ECサイトにおけるセキュリティ対策の実態調査報告

平成１５年３月

電子商取引推進協議会
財団法人日本情報処理開発協会
電子商取引推進センター

電子商取引推進協議会
財団法人日本情報処理開発協会 電子商取引推進センター

はじめに

本報告書は、インターネット上で商品の販売を行っている国内のECサイトが、実態としてどの程度まで情報セキュリティ対策を行っているのかを把握するための調査を実施し、その結果を纏めたものである。

これまで、国内で報告されているセキュリティ対策に関する実態調査報告では、セキュリティ対策を行うための機器やソフトの導入状況、あるいは体制の整備状況等について等の調査が主流であったが、本報告書では、セキュリティマネジメントの観点から対策実態を把握し、その実施の程度についても把握しようとしている点に大きな特徴がある。

今回の調査は、電子商取引推進協議会（ECOM）で行った第1回目のセキュリティ対策実態調査であり、予備調査としての位置付けで調査・分析を行っているが、その分析結果より大まかな実態の傾向は把握できるものと考え、この報告書を通じて結果を報告することとした。

また、付録として、セキュリティ対策の調査票を添付しているが、その中では調査アンケートの回答者へのセキュリティ対策への啓蒙の意味を含め、セキュリティ対策として行うべきことについても解説している。ECサイトばかりでなく、インターネットを利用したシステムの開発者、運営者にも是非ご一読いただき、EC サイトの安全と信頼を守ることへの理解への一助となれば幸いである。

平成１５年３月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

目　次

1 調査の概要

1.1 調査の背景

ECOM では、EC サイトの情報セキュリティ推進に向け、これまでに EC サイト向けのセキュリティ対策ガイドラインを開発している。このガイドラインは、EC サイトが行うべきセキュリティ対策の考え方を、システムへの脅威に対する防御と、トラブル発生時への備えとの両面についてまとめたものである。詳細については、平成 13 年度の ECOM 報告書「EC サイト向けセキュリティ対策ガイドライン 第 2 版」の解説編および実施の手引きを参照されたい。

ECOM では、ガイドライン開発の次のステップとして、ガイドラインの普及およびガイドラインの考え方に立った EC サイトにおけるセキュリティ対策の普及啓蒙を行うことが重要であると認識し、そのための第一段階として、日本国内の EC サイトにおけるセキュリティ対策の実態を把握することとした。

1.2 調査の目的

本調査では、以下の 3点を目的としている。

- 現在捉えられていない EC サイトにおけるセキュリティ対策の実態を示すデータの把握
- 把握したデータの分析による EC サイトにおけるセキュリティ対策の問題点の整理
- EC サイトのセキュリティレベルの向上へ向けた提言

1.3 調査の特徴

本調査では、これまでセキュリティ対策について他の機関等で行われてきた調査とは異なり、

- セキュリティマネジメントの考え方に基づいた質問構成
- 単に何を実施しているのかを調査するのではなく、その実施の程度についてまで踏込んだ調査
- 調査の回答者が自サイトのセキュリティ対策度を自己評価できるための工夫

という点に大きな特徴がある。

セキュリティ対策は、サイトの運営の実態に合った技術面の対応とサイト運営上のマネジメントが一体となってはじめて実現するものであり、そのためには技術面での対応やセキュリティに関わる諸活動が常にサイトの運営実態に合ったものとして維持されなければならないという考えのもとに、以下の観点に立ってセキュリティマネジメントの実態について質問を構成している。

- 脅威およびセキュリティ対策の推進についての認識度
- セキュリティ対策としてなすべきことへの理解度

- セキュリティ対策の要求事項の指定の程度
- 指定された要求事項のシステムへの実装やシステム運用および業務運用への反映の程度
- 計画されたセキュリティ対策の実行の徹底度

また、質問体系は、セキュリティ対策ガイドラインの体系をベースとし、情報セキュリティの専門化をアドバイザに加えたセキュリティWG のメンバーの研究により作成した。

以下に、その体系の大枠を示す。

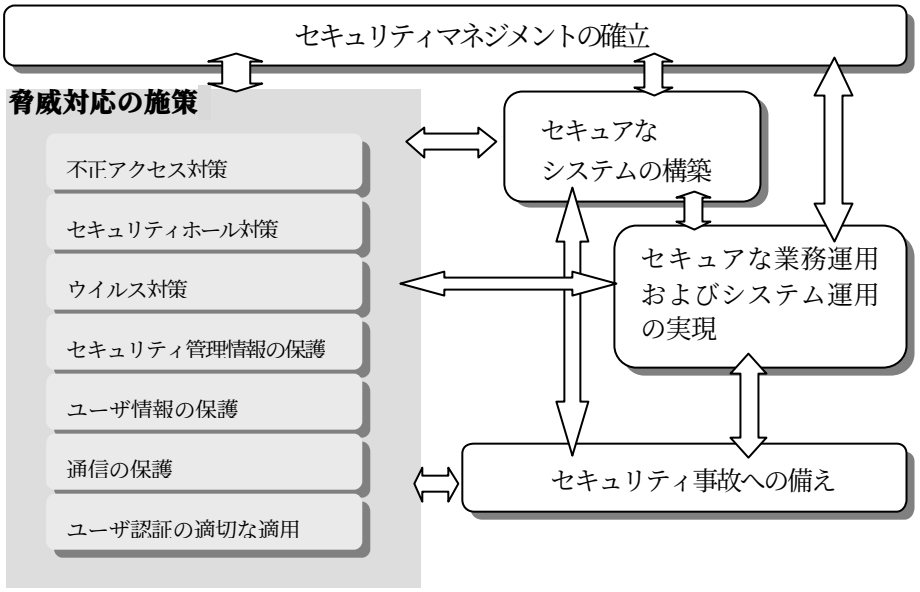


図 1-1　質問項目の体系

この中で、“セキュアなシステムの構築”と“セキュアな業務運用およびシステム運用の実現”は、“脅威対応の施策”や“セキュリティ事故への備え”をシステムの構成や業務およびシステム運用へ反映するものである。

なお、具体的な質問区分と質問数は、下表の通りである。具体的な質問については、添付の「セキュリティ対策の実施状況についての質問」を参照されたい。

表 1-1　質問区分と質問数

質問区分	質問数	質問区分	質問数
セキュリティマネジメントの確立	21	通信の保護	6
不正アクセス対策	12	ユーザ認証	15
セキュリティホール対策	10	セキュアなシステムの構築	24
ウイルス対策	10	ｼｽﾃﾑ運用と業務現場におけるｾｷｭﾘﾃｨ対策	21
セキュリティ管理情報の保護	11	セキュリティ事故への備え	17
ユーザ情報の保護	12	総合評価	14

1.4　調査方法

本調査では、バーチャルショップを運営する EC サイトを抽出し、そのサイトに対してアンケート票を郵送して、サイトより回答を返送していただく方法により調査を行った。

アンケートの発送数と回答の回収状況については下表の通りであり、結果として十分なサンプル数を確保することはできなかったが、それでもおおよその傾向を見ることは可能であると判断し、予備調査的な位置付けとして、回答の分析を行った。

表 1-2　アンケートの発送数・回収数

	発送数	回収数	回収率
バーチャルショップ	1722	37	2.1%

2　調査対象サイトのプロフィール

ここでは、調査対象となったバーチャルショップのプロフィールより、

- サイトの規模に関するもの
- システムの運営形態
- 取扱商品

について示す。

2.1　サイトの規模に関するもの

サイトの規模については、売上規模、システムに関する要員数、および使用しているサーバ台数について調査を行った。

なお、今回の調査では、対象となるサイトの規模を「大規模」「中規模」「小規模」の別に分類して分析を行っているが、分類方法としては売上規模を基準として考え、サーバ数と要員数を勘案して修正を加えて分類を行っている。

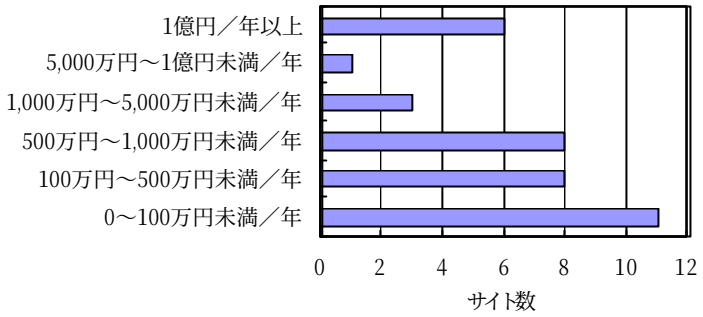
分析対象サイトすべてについての規模分類した結果を下表に示す。

表 2-1　分析対象サイトの規模分類

サイト規模	売上規模	サーバ数	ｼｽﾃﾑ要員数
大規模	1億円／年以上	50	25
大規模	1億円／年以上	8	15
大規模	1億円／年以上	4	2.5
大規模	1億円／年以上	1	7
大規模	1億円／年以上	0	9
大規模	5000万円～1億円未満／年	1	5
大規模	1000万円～5000万円未満／年	0	0
大規模	500万円～1000万円未満／年	0	4
大規模	500万円～1000万円未満／年	0	0
中規模	1億円／年以上	2	0
中規模	1000万円～5000万円未満／年	2	3
中規模	1000万円～5000万円未満／年	1	4
中規模	500万円～1000万円未満／年	1	2
中規模	500万円～1000万円未満／年	1	2
中規模	500万円～1000万円未満／年	1	2
中規模	500万円～1000万円未満／年	1	0
中規模	500万円～1000万円未満／年	1	0
中規模	500万円～1000万円未満／年	0	2
中規模	100万円～500万円未満／年	2	5
中規模	100万円～500万円未満／年	1	6
中規模	100万円～500万円未満／年	1	4
中規模	100万円～500万円未満／年	1	4
中規模	100万円～500万円未満／年	1	2
中規模	0～100万円未満／年	3	0
中規模	0～100万円未満／年	1	4
中規模	0～100万円未満／年	1	4
小規模	100万円～500万円未満／年	1	2
小規模	100万円～500万円未満／年	1	1
小規模	100万円～500万円未満／年	1	0
小規模	0～100万円未満／年	1	2
小規模	0～100万円未満／年	1	2
小規模	0～100万円未満／年	1	1
小規模	0～100万円未満／年	1	1
小規模	0～100万円未満／年	0	1
小規模	0～100万円未満／年	0	1
小規模	0～100万円未満／年	0	0
小規模	0～100万円未満／年	0	0

2.1.1　売上規模（年商）

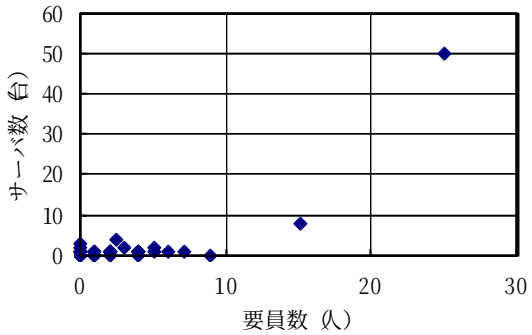
売上高から見ると、年商 1,000 万円以下のサイトが多い。



2.1.2　システムに関する要員数と使用しているサーバ台数

※　システムに関する要員数は、システム開発・保守およびシステム運用に関する要員を合わせた数

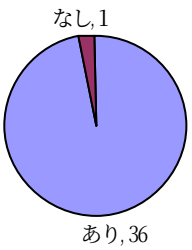
一部のサイトを除いて、要員数、サーバ数とも少なく、小規模なサイトが多い。



2.2　システムの運営形態

2.2.1　自社サイトの有無

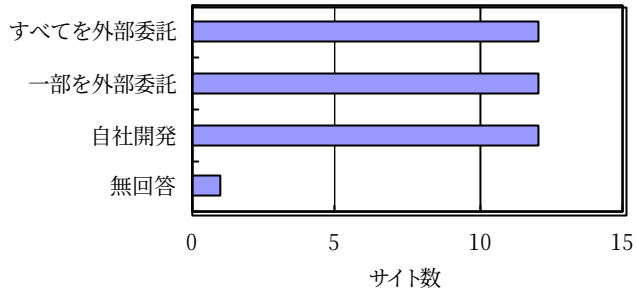
ほとんどのサイトが、自社サイトを持っている。



（サイト数）

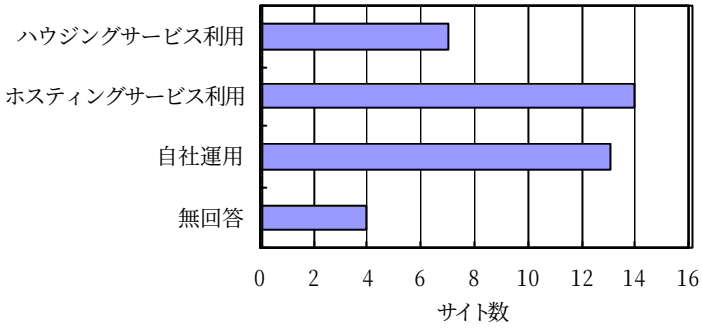
2.2.2　システム開発の形態

何らかの形で外部にシステム開発を委託しているサイトは2／3であり、バーチャルショップにおいても外部に開発を委託する傾向がある。



2.2.3　システム運用の形態

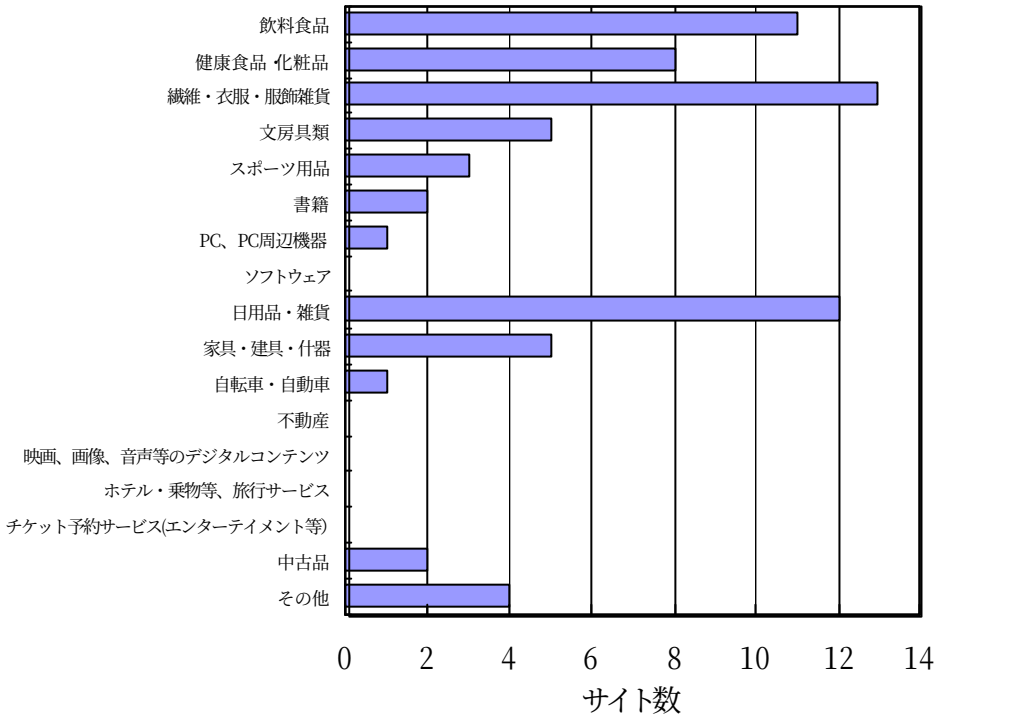
システムを自社運用しているサイトは1／3程度で、多くは社外に置かれたサーバを利用して運用サービスを受けている。



※ 複数回答あり

2.3　取扱商品

高価な商品を取り扱うサイトは少なく、服飾や日用品、雑貨など、小規模サイトでも比較的取り扱いやすいと思われる低価格帯の商品を扱うサイトが多い。



※ 複数回答あり

3 セキュリティマネジメントの確立

本章では、EC サイトがセキュリティ対策を計画的、組織的に行うための基盤確立の実施状況について分析を行う。

分析項目については、以下の通り。

- セキュリティポリシー（セキュリティ対策基本方針）の確立
- セキュリティ対策の推進体制
- セキュリティ対策予算の確保
- 運営関係者の管理状況
- 業務委託先との連携
- セキュリティ監査の実施状況

3.1 “セキュリティマネジメントの確立”全体を通しての傾向

セキュリティの脅威および脅威のサイトに対する影響はほぼ十分に認識されているが、セキュリティポリシーの確立や体制の整備、セキュリティ教育、監査の実施等のマネジメント面の確立という点では、全体的に十分とは言えない。

また、サイトの規模による傾向の違いが明確に見られ、特に小規模サイトにおけるセキュリティマネジメントは不十分であると言える。

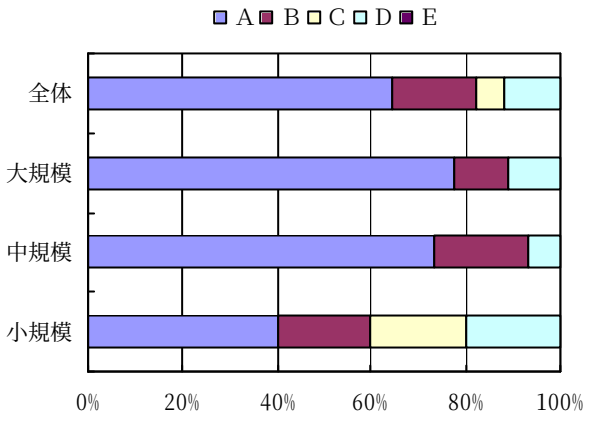
3.2 設問ごとの分析結果

3.2.1 セキュリティポリシーの確立

分析結果から見た傾向は、以下の通り。

- 全体的にセキュリティポリシーの確立は十分とは言えず、サイトの規模が小さくなるほど不十分な状況にある。
- 脅威に対する認識は持っているが、予算・体制の許される範囲でのセキュリティ対策に取組むという方針に止まっている。
- 認識している脅威としては、システムへの侵入およびコンピュータウィルスなどによるシステム破壊と、他社サイトへのウイルス配布および踏み台などがある。
- セキュリティ事故としては、情報の漏えい、企業およびサイトの信用の失墜およびデータの復元などについての影響の大きさを意識している。

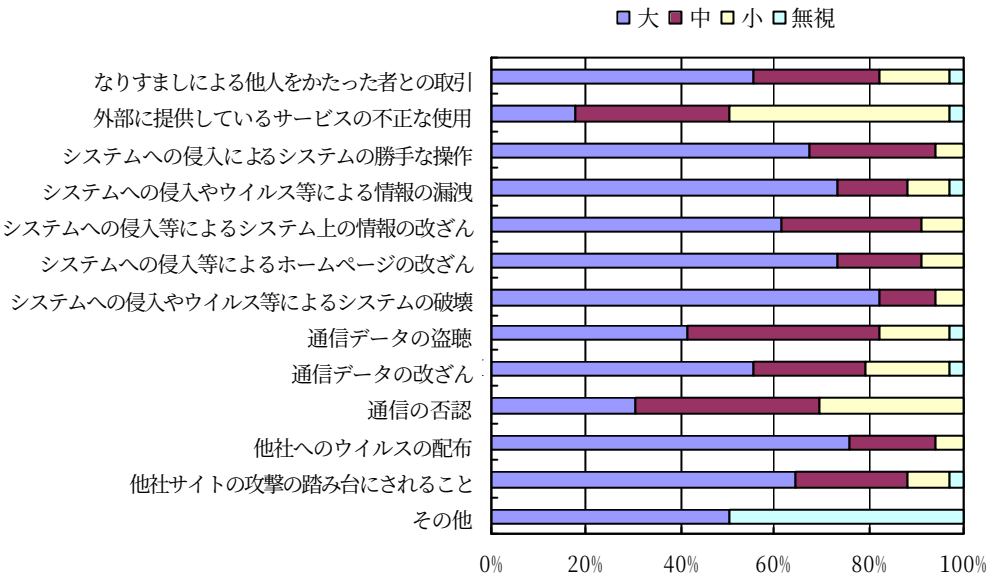
(1) 脅威に対する認識



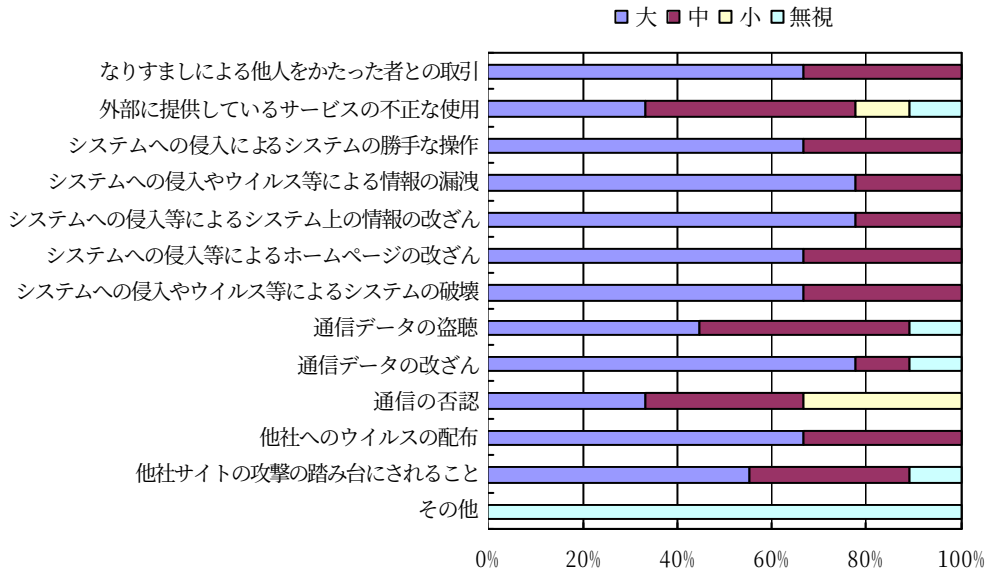
(A) サイトは攻撃の対象になり易く、セキュリティにかかわる事故は事業や企業イメージに致命的な打撃を与える恐れもあり、重大な脅威と考えている
(B) サイトは攻撃の対象になり易い。ただし、セキュリティ事故が発生しても事業や企業イメージに直接的な影響が出るとは考えていないものの、業務に混乱をきたす恐れもあり、相当の脅威と考えている
(C) 特別に攻撃の対象となるサイトでもなく、業務やサイトの運営形態からみて、セキュリティ事故の影響はそれほど重大視していない
(D) 業務やサイトの運営形態からみてあまり重大視していないが、脅威は意識している
(E) 特に気にしていない

(2) 認識している脅威とそのレベルについての認識

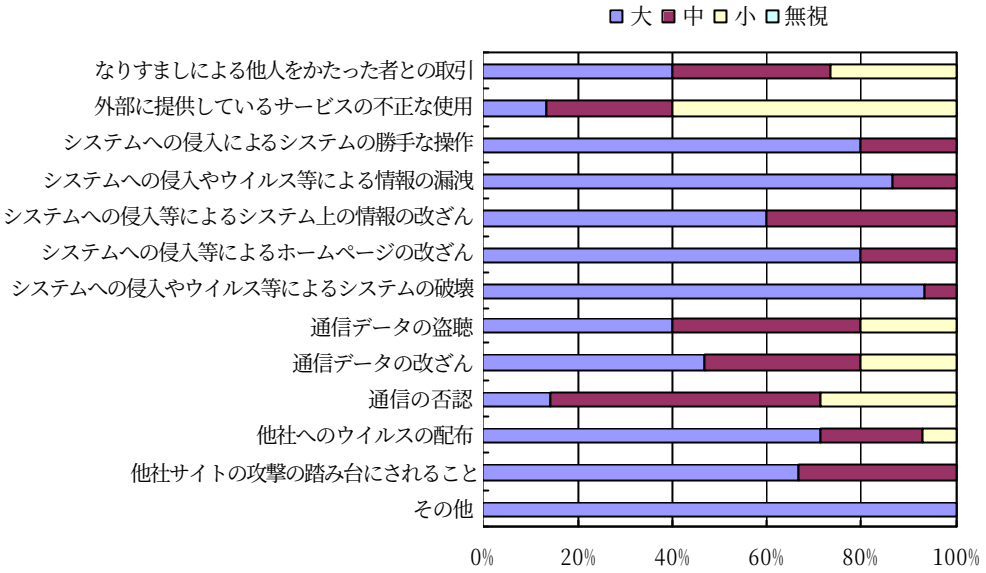
【全体】



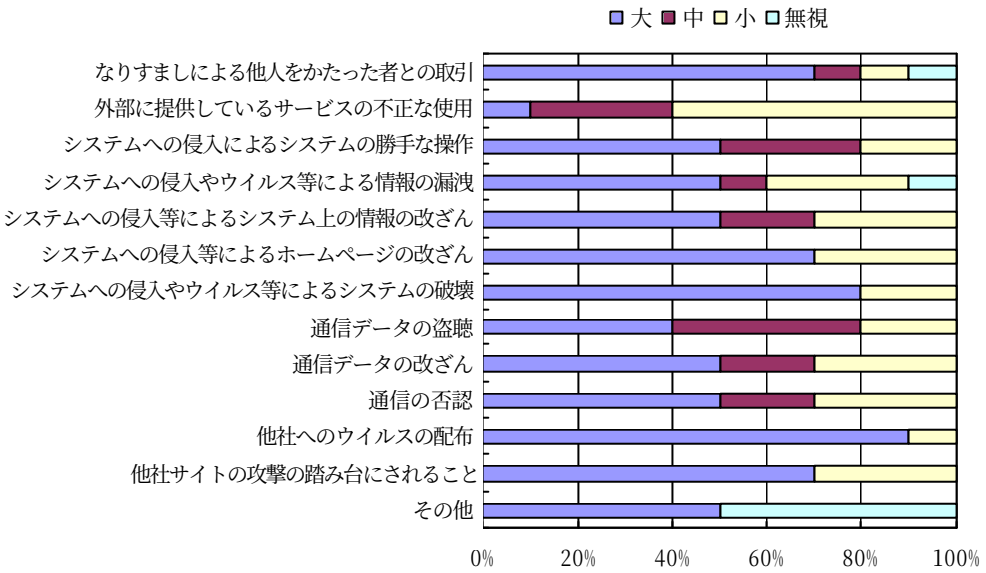
【大規模】



【中規模】

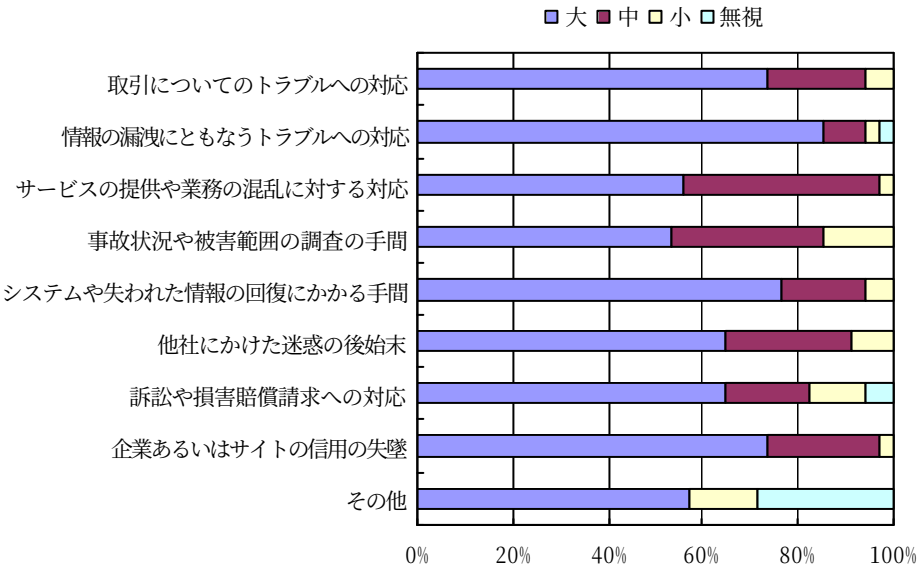


【小規模】

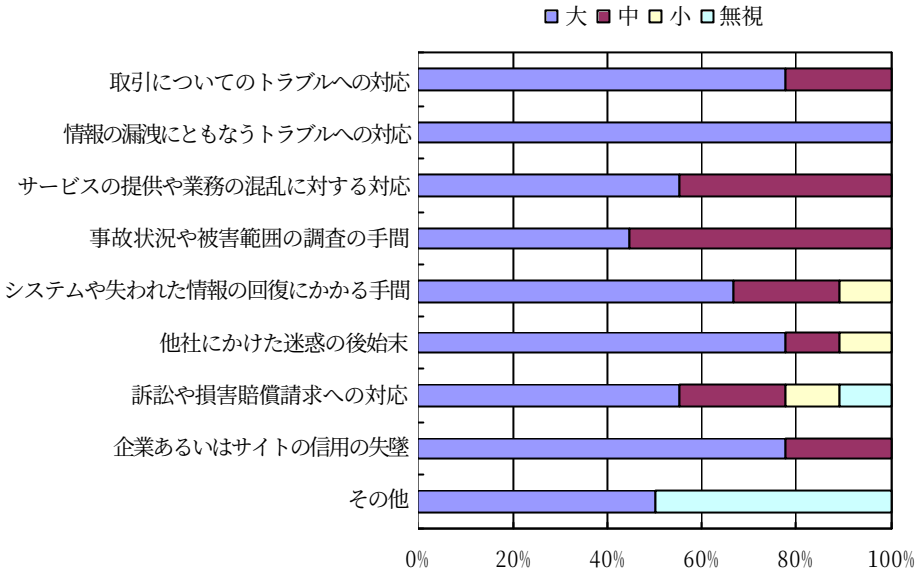


(3) 想定されるセキュリティ事故の影響の度合いについての認識

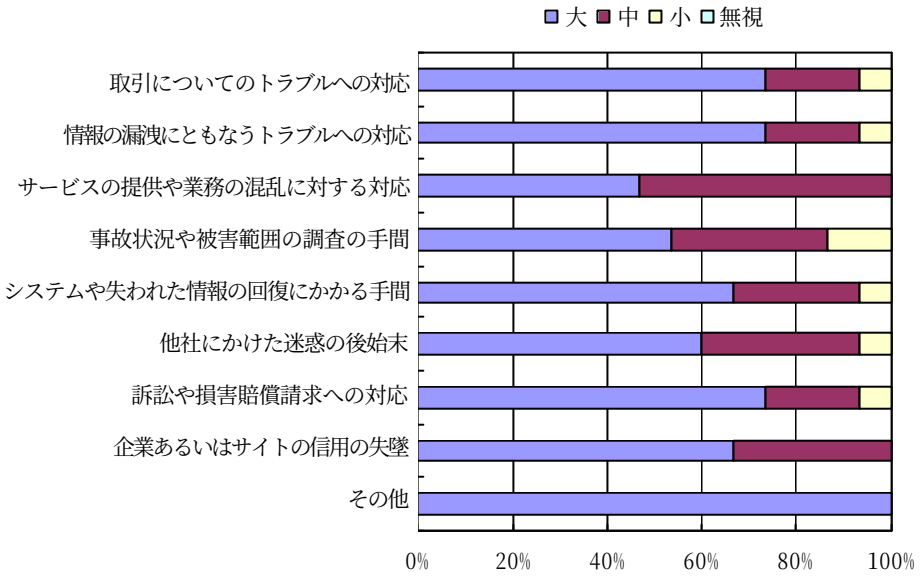
【全体】



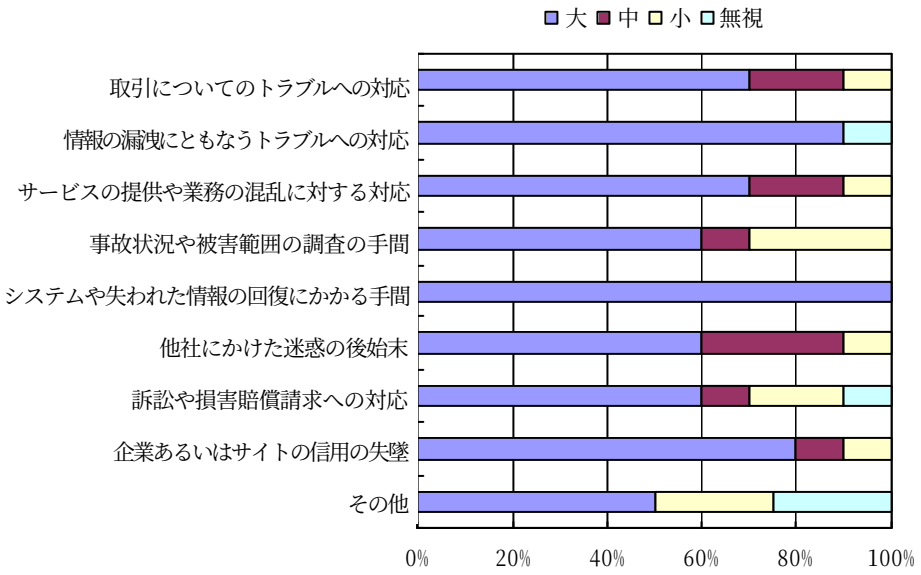
【大規模】


大
中
小
無視
取引についてのトラブルへの対応
情報の漏洩にともなうトラブルへの対応
サービスの提供や業務の混乱に対する対応
事故状況や被害範囲の調査の手間
システムや失われた情報の回復にかかる手間
他社にかけた迷惑の後始末
訴訟や損害賠償請求への対応
企業あるいはサイトの信用の失墜
その他
0%
20%
40%
60%
80%
100%

【中規模】

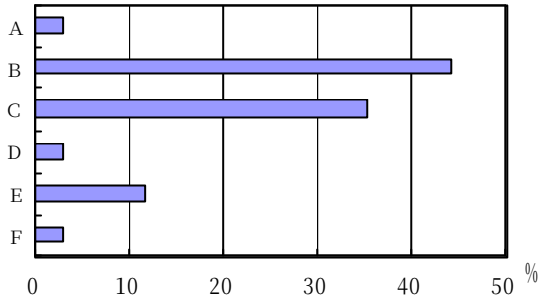

大
中
小
無視
取引についてのトラブルへの対応
情報の漏洩にともなうトラブルへの対応
サービスの提供や業務の混乱に対する対応
事故状況や被害範囲の調査の手間
システムや失われた情報の回復にかかる手間
他社にかけた迷惑の後始末
訴訟や損害賠償請求への対応
企業あるいはサイトの信用の失墜
その他
0%
20%
40%
60%
80%
100%

【小規模】

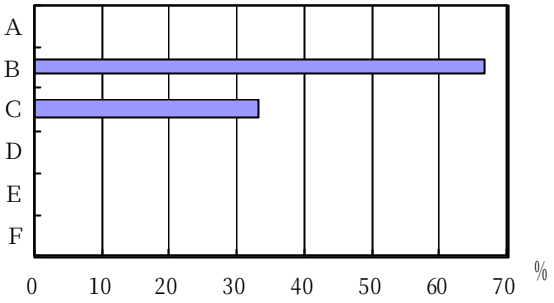

大
中
小
無視
取引についてのトラブルへの対応
情報の漏洩にともなうトラブルへの対応
サービスの提供や業務の混乱に対する対応
事故状況や被害範囲の調査の手間
システムや失われた情報の回復にかかる手間
他社にかけた迷惑の後始末
訴訟や損害賠償請求への対応
企業あるいはサイトの信用の失墜
その他
0%
20%
40%
60%
80%
100%

(4) 脅威への対応についての基本方針

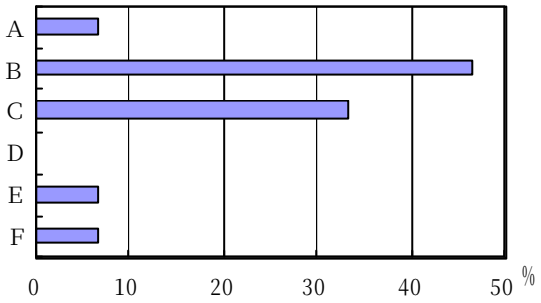
【全体】



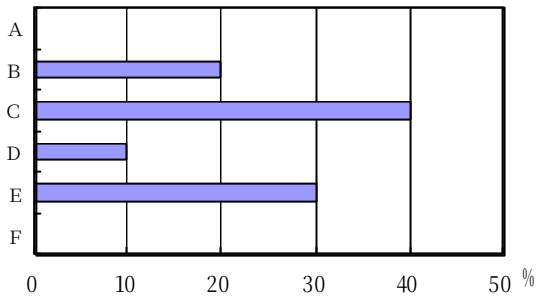
【大規模】



【中規模】

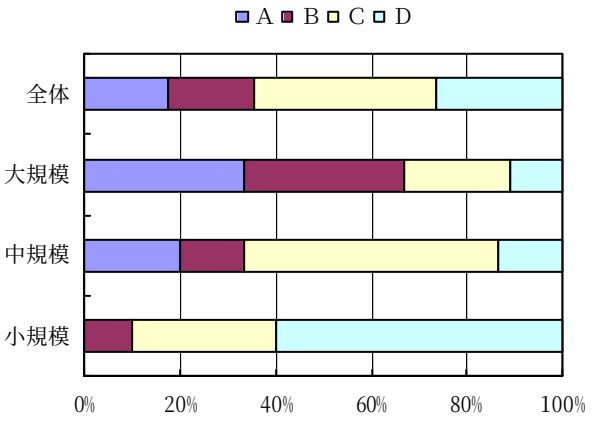


【小規模】



(A) セキュリティ対策は事業の基盤と考え、必要な予算および体制を確保し、可能な限りの対策を実施する
(B) 予算、体制に限界はあるができる限りのセキュリティ対策を実施する
(C) ファイアウォールの設置やウイルス対策ソフトの導入等の一般的な対策は実施するが、セキュリティ対策に特に注力はしていない
(D) 実際問題としての脅威は感じないため特に対策はしない
(E) 保護が必要なところはネットワークから切り離し、セキュリティ対策は不要なシステムとする
(F) その他

(5) セキュリティポリシーへの取組み



(A) サイトの運営実態を適切に反映した実効的なセキュリティポリシーが経営レベルから宣言されている
(B) 宣言されたセキュリティポリシーはあるが形式的であり、実効的なものにするためには内容、記述とも見直しが必要
(C) 担当者レベルでのセキュリティへの取組みについての共通認識はあるが、セキュリティポリシーとして定義したものはない
(D) セキュリティに対する取組みが明確でない

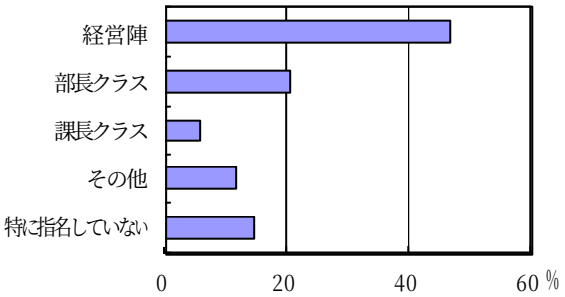
3.2.2　セキュリティ対策の推進体制

分析結果から見た傾向は、以下の通り。

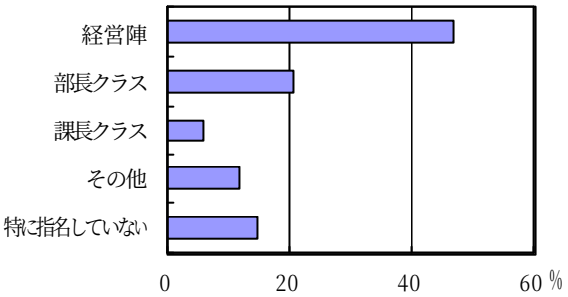
- セキュリティ対策の推進体制は、全体的に経営陣の参画は見られるものの責任者の立場がサイトの規模によって大きく異なっている。また、体制の整備状況については、小規模サイトの不十分さが目立ち、全体的にも強化の必要性があると言える。
- セキュリティ対策の担当者の技術レベルは運営には大きな支障のない状況であると判断されている。
- 外部の依頼先としては、システム構築支援の延長でのシステムベンダーのサポートが一番多い。
- 外部支援依頼の中心は、システム構築・維持管理の技術指導とセキュリティ情報の入手、侵入監視、事故処理支援などが中心となっている。

(1) 責任者の存在

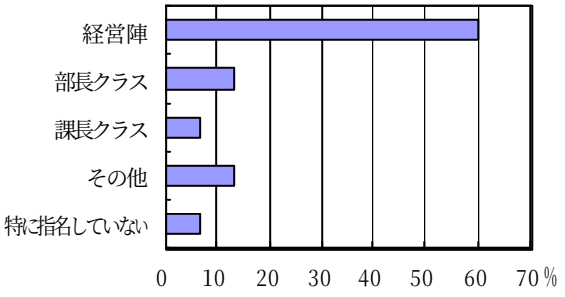
【全体】



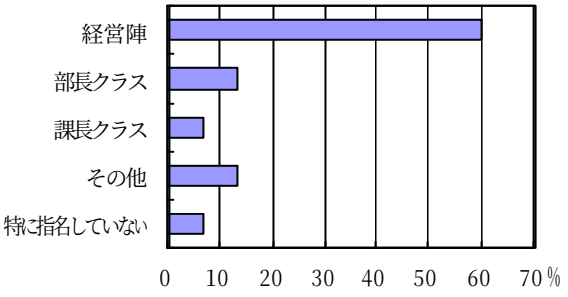
【大規模】



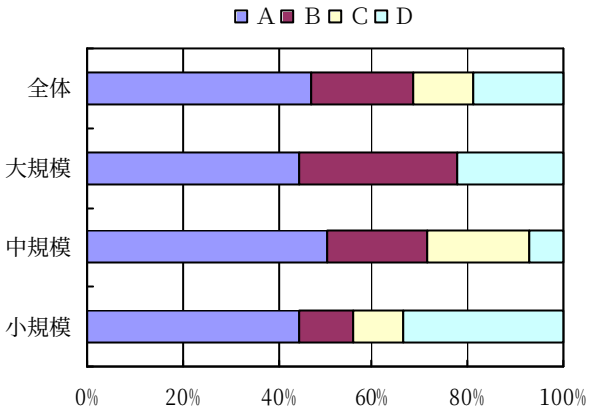
【中規模】



【小規模】

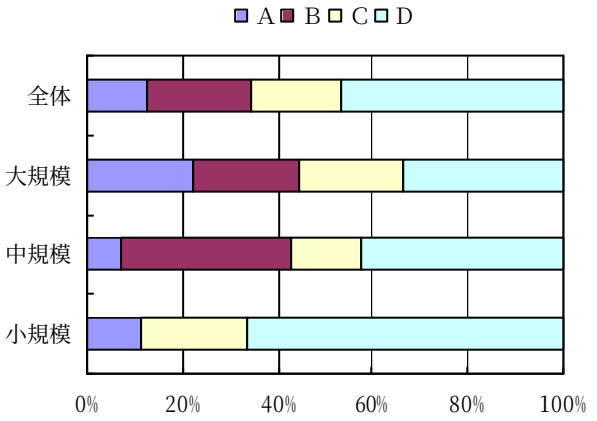


(2) 経営陣の推進体制への参画



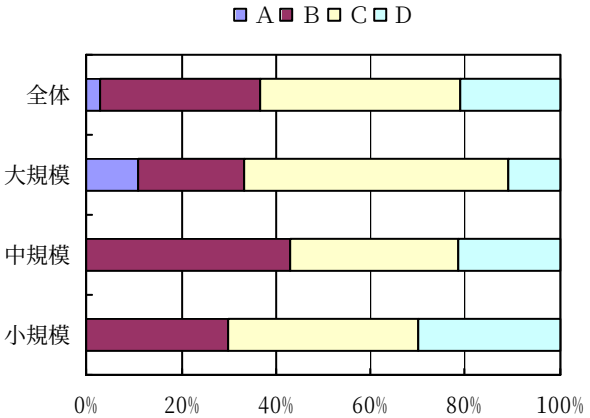
(A) セキュリティについて十分な認識がある経営陣が参加しており、適切な指導を行っている
(B) 報告を受け経営レベルの問題には対処するが、チェックや指導を行うまでには至っていない
(C) 体制の中には含まれているが、形式的であり実際上機能はしていない
(D) 経営陣は推進体制に参画していない

(3) セキュリティ対策推進体制の整備状況



(A) 確立した体制が組まれており、関係者は自分のタスクを承知し、体制は十分に機能している。また、適宜、見直しも行われ、常にサイトの運営実態に適合したものになっている
(B) 十分に検討された体制やタスクの定義はあるが、見直しはあまり行われておらず、運営実態に適合しないところもある
(C) セキュリティ推進体制は形作られてはいるが、タスクの定義や担当者の認識等は不十分で形式的なレベルである
(D) セキュリティ対策推進のための体制はない。それぞれの担当が自分の責務の範囲で対応している

(4) セキュリティ対策担当者の技術レベルとスキル向上への取組み

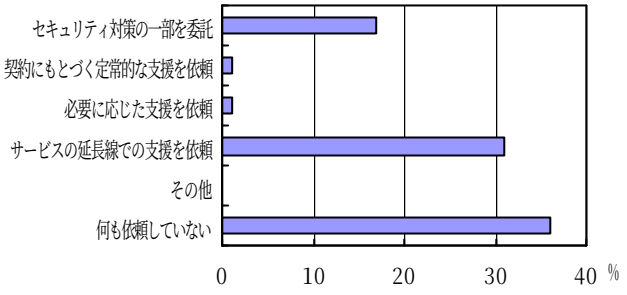


(A) 積極的に教育を行っており、必要な知識、スキルを十分に有している。問題があってもほとんど独力で対応可能である
(B) 教育等の実施により一通りの知識、スキルを有しているが、十分とは感じていない。問題が生じた場合、外部の専門家と連携することにしている
(C) 担当者の自主的な学習に依存しており、知識やスキルは基本的なレベル。外部の支援に頼るところが多い
(D) セキュリティに関する知識、スキルはほとんど有していない。セキュリティ対策のすべてを外部からの支援に依存している

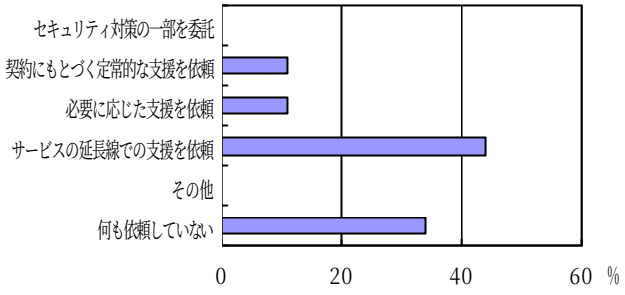
(5) 外部の支援の活用状況

① 支援依頼の形態

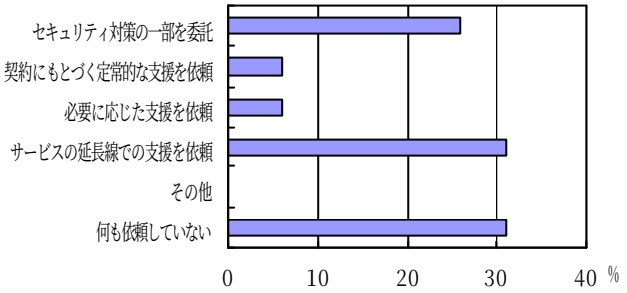
【全体】



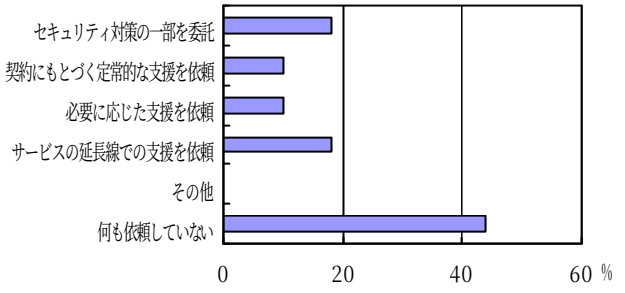
【大規模】



【中規模】

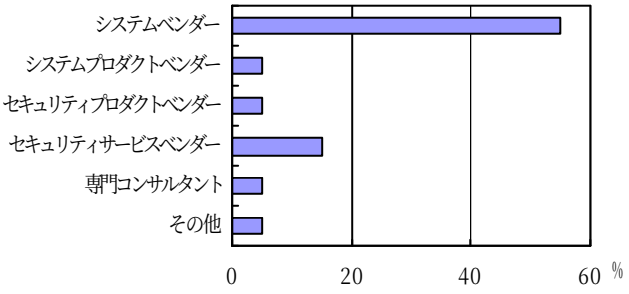


【小規模】

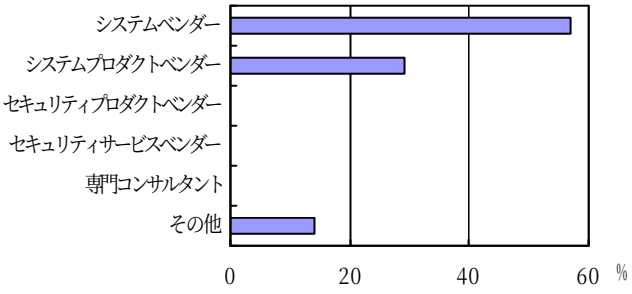


② 支援依頼先

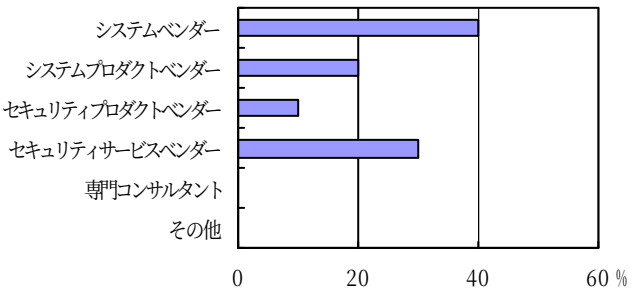
【全体】



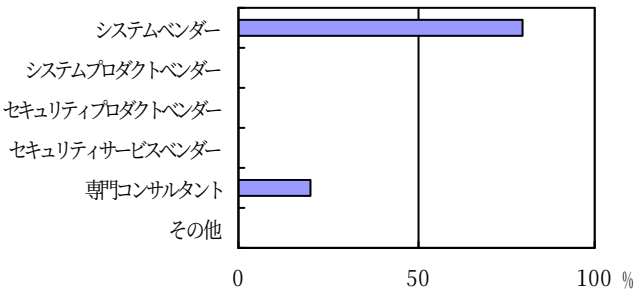
【大規模】



【中規模】

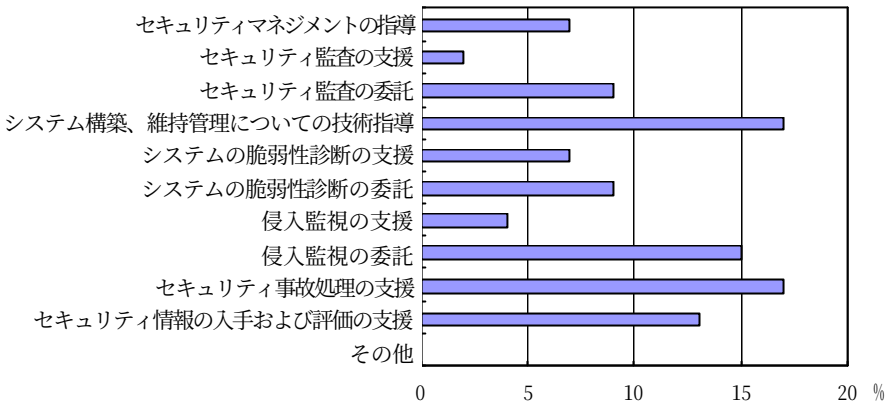


【小規模】

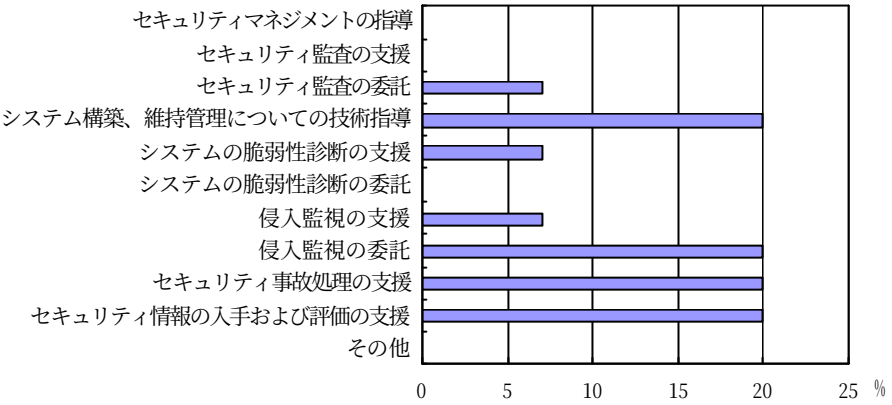


③ 支援依頼事項

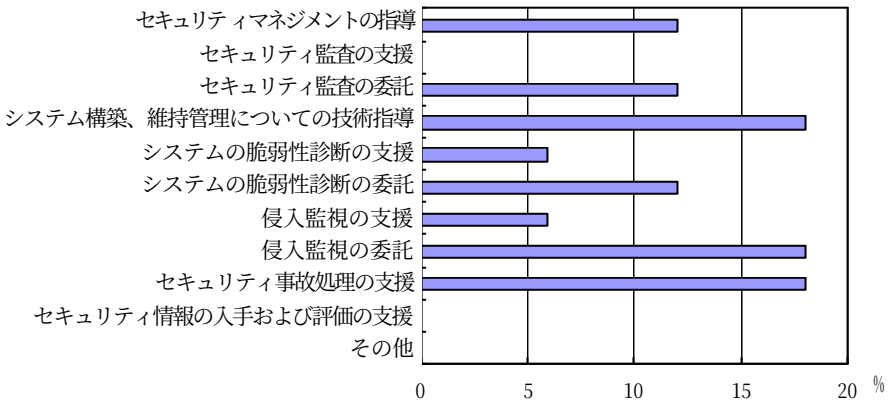
【全体】



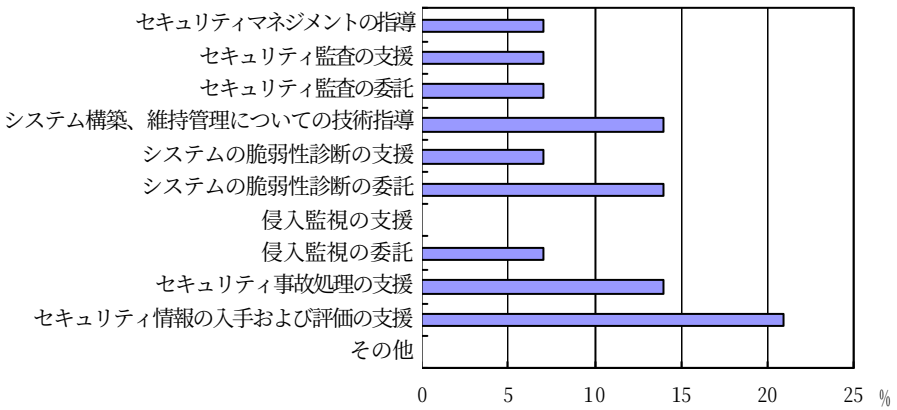
【大規模】



【中規模】

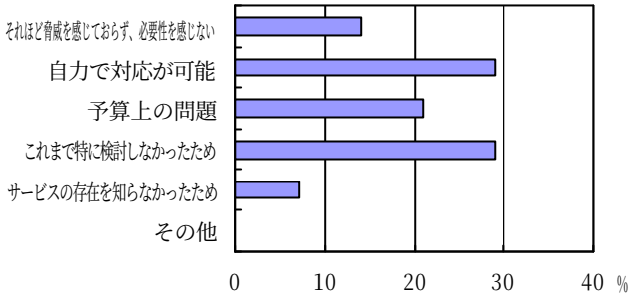


【小規模】

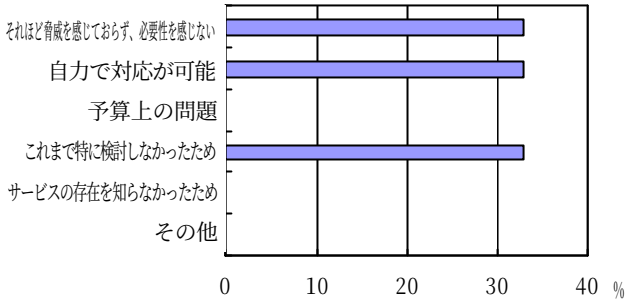


④　支援を得ていない理由

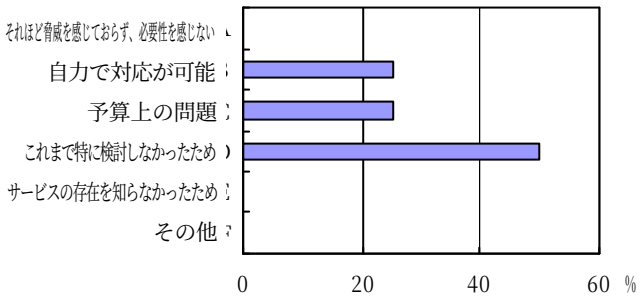
【全体】



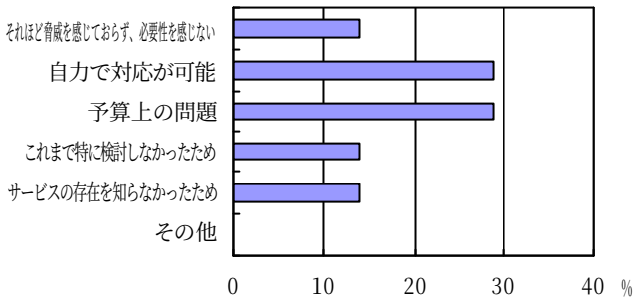
【大規模】



【中規模】

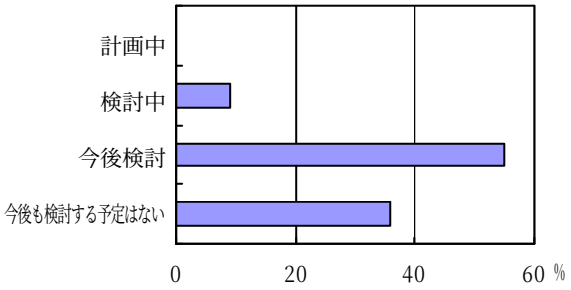


【小規模】

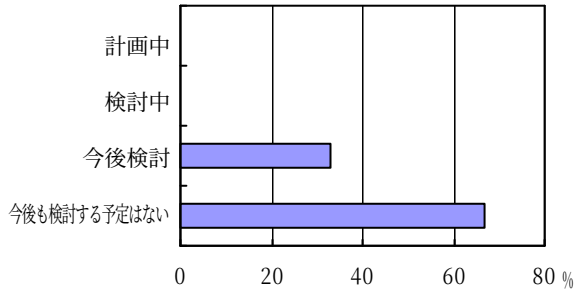


⑤　外部の支援サービスの今後の利用

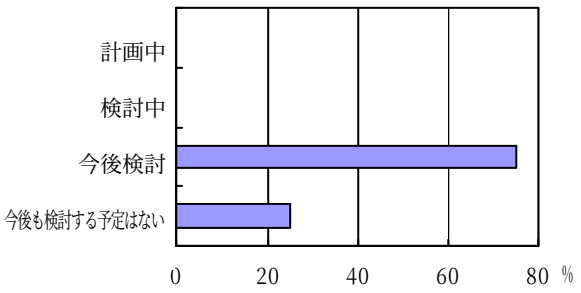
【全体】



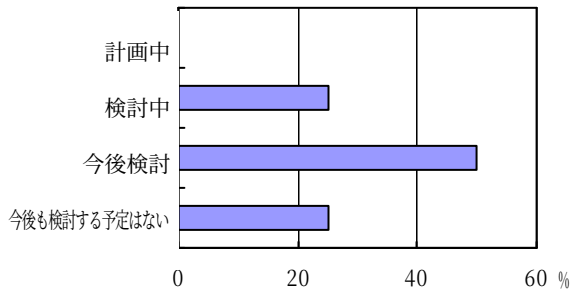
【大規模】



【中規模】

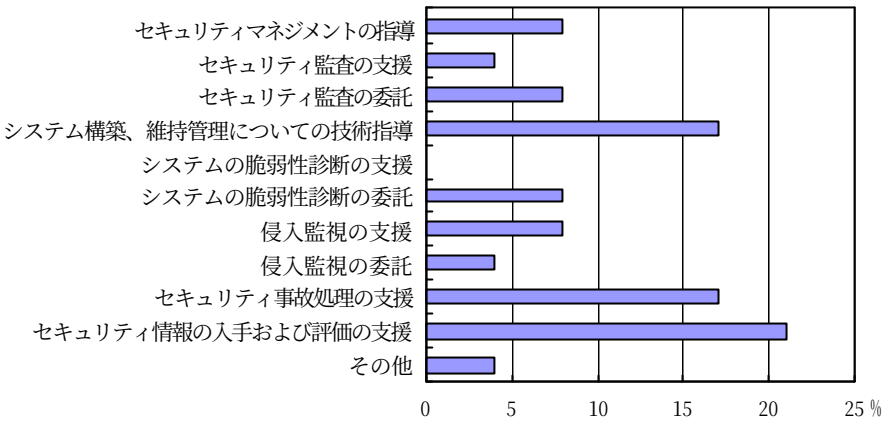


【小規模】

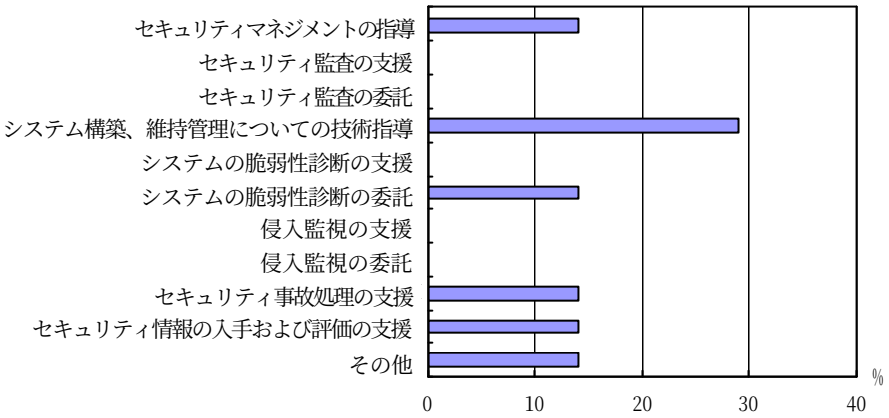


⑥ 外部の支援サービスで考えている利用サービス

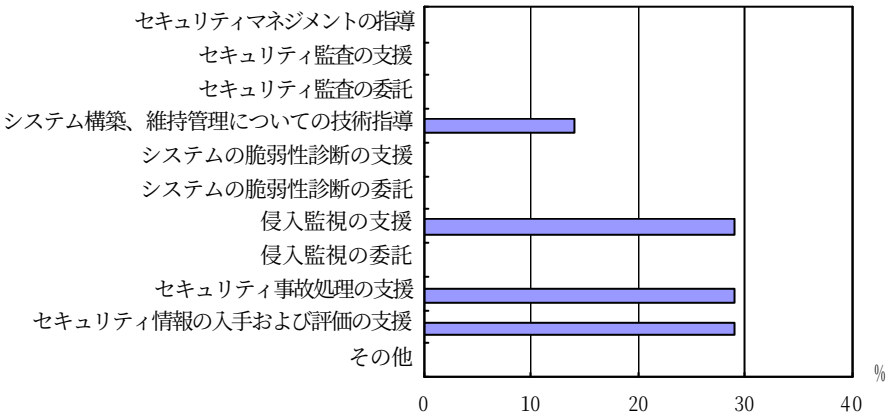
【全体】



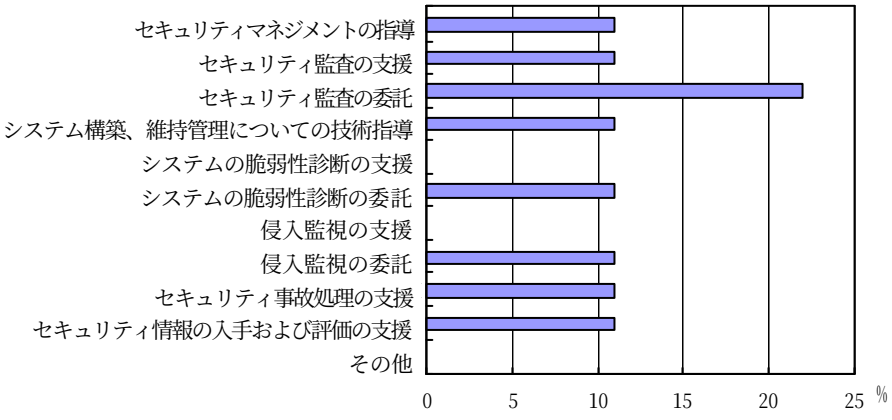
【大規模】



【中規模】



【小規模】

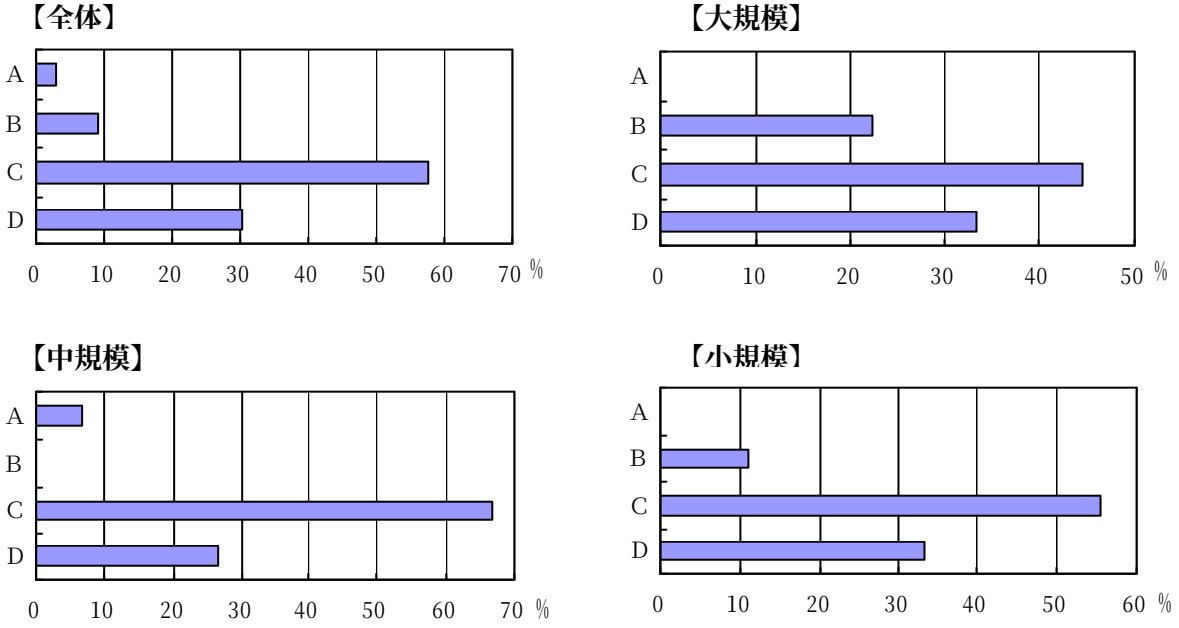


3.2.3　セキュリティ対策予算の確保

分析結果から見た傾向は、以下の通り。

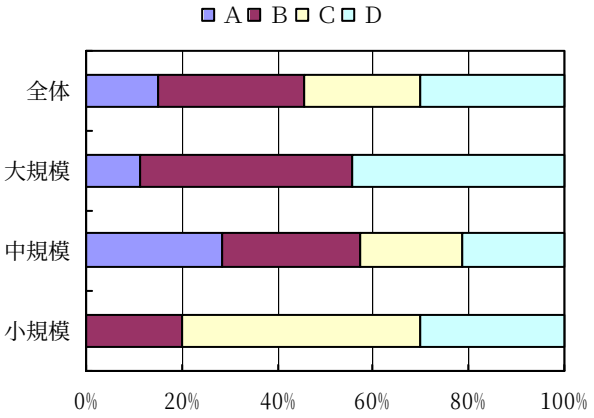
- 全体的にセキュリティ対策予算の確保は別立てで計上されてはおらず、システム運用予算に含めて計上されている。また、セキュリティ対策予算の意識を持たないサイトが 30%もある。
- 脅威に対する認識は持っているが、予算・体制の許される範囲でのセキュリティ対策に取組むという方針に止まっている。

(1) セキュリティ予算の計上方法



（A）セキュリティ対策のための予算は他の費用とは別立てで計上され審議されている
(B) 他の予算と別立てで計上するまでは至っていないが、セキュリティ予算として審議されている
（C）セキュリティ対策に必要な予算は、システムの導入や維持管理あるいは運用予算に含まれて計上、審議されており、セキュリティ対策に焦点をあてた予算の検討は行われていない
（D）セキュリティ対策予算としての意識はない

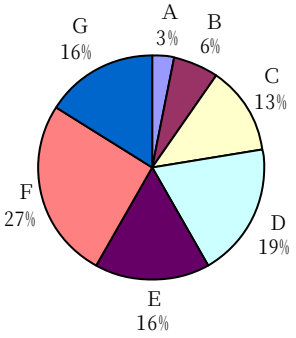
(2) 予算の確保状況



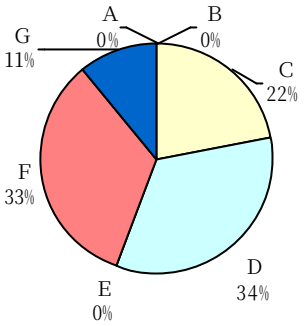
(A) 実施したいセキュリティ対策に必要な予算はほとんど割当てている
(B) 実施したいセキュリティ対策に必要な予算は要求通りではないが、おおむね割当てている
(C) 予算不足のため実施したいセキュリティ対策が十分に実施できない
（D）セキュリティ対策の予算はほとんど確保していない

(3) サイトの運用予算全体に占めるセキュリティ予算の割合

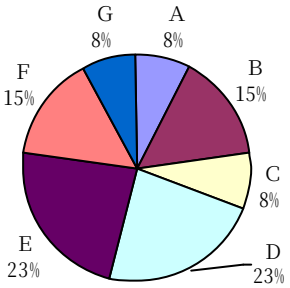
【全体】



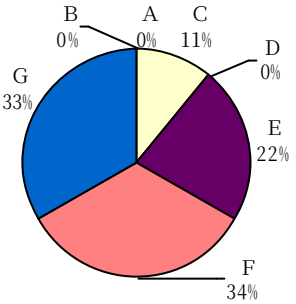
【大規模】



【中規模】



【小規模】



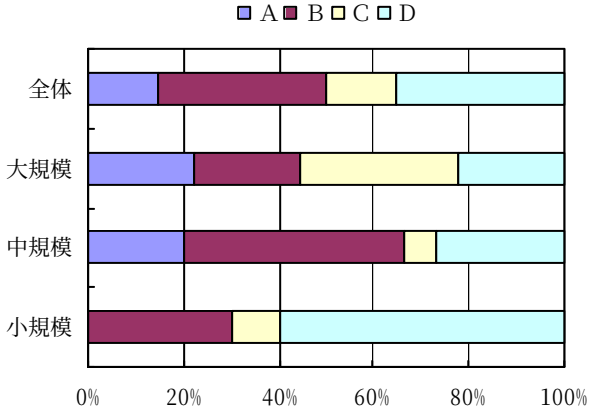
Ⓐ 15%超　Ⓑ 10%～15%　Ⓒ 5%～10%　Ⓓ 3～5%
Ⓔ 1～3%　Ⓕ 1%未満　Ⓖ ゼロ

3.2.4 運営関係者の管理状況

分析結果から見た傾向は、以下の通り。

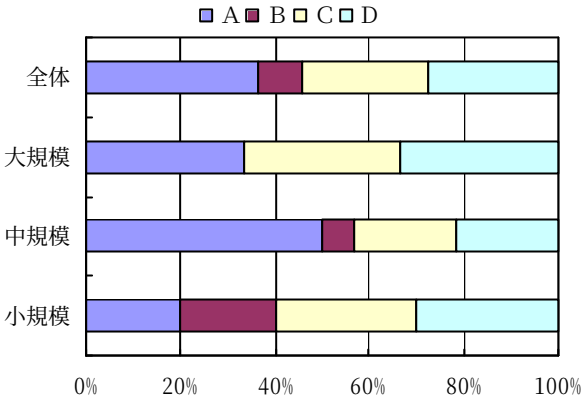
- 全体的に関係者に対するセキュリティに関する指導や管理はだいたい行われているが、小規模サイトでは少し不十分と言える。
- サイト内に立ち入るものに対するセキュリティ上の管理について何も行っていないサイトも約30%もあり不十分と言える。

(1) 運営関係者へのセキュリティ面での指導や管理



Ⓐ 必要なルールも確立しており、必要な管理も業務プロセスの中に組込まれており、厳格に運用されている。また、関係者に対する教育指導も徹底している
Ⓑ ルールは確立しているがその運用は厳格でなく、十分な管理が行われているとは言い難い
Ⓒ 基本的な教育や指導は一通り行っているが、管理はほとんど行っていない
Ⓓ 特に何も行っていない

(2) 一時的にサイト内に立入る者に対するセキュリティ上の管理



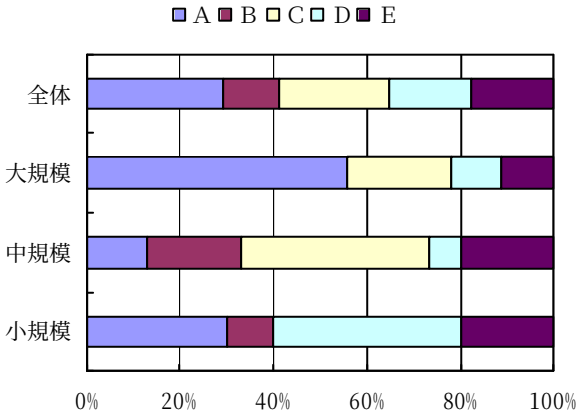
Ⓐ サイトへの一時立入り者に対する管理ルールが確立しており、厳格に運用されている
Ⓑ サイトへの一時立入り者に対する管理ルールは確立しているが、それほど厳格に運用されていない
Ⓒ 問題意識はあり関係者に注意を うながしているが、ルールの確立までには至っていない。管理は関係者の注意に依存している
Ⓓ特に何も行っていない

3.2.5 業務委託先との連携

分析結果から見た傾向は、以下の通り。

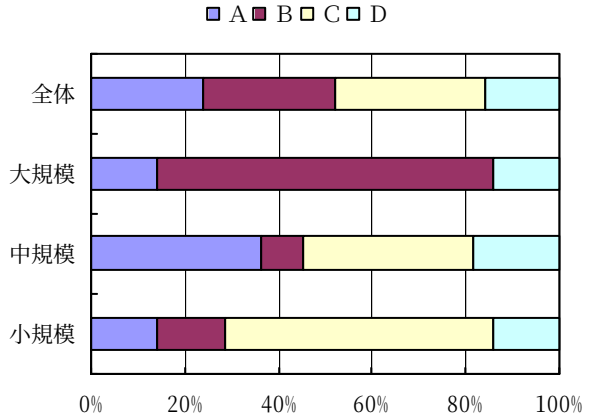
- 全体的には、業務委託先との責任が契約等で明確になっていないサイトも半分程度ある。
- 大規模サイトにおいては、業務委託先の管理はほぼ行われているが、小規模サイトでは不十分な状況である。

(1) 業務委託先との間でのセキュリティに関する責任の明確化



Ⓐ 業務委託契約の中で委託先の責任が明記されており、業務委託先がこの点に関して十分に認識していることも確認している
Ⓑ 業務委託契約の中で委託先の責任を記載しているが、この点に関し業務委託先との間での共通認識については不十分
Ⓒ 双方の担当者間での意思疎通はあるものの、契約書や覚書等での明示は行っていない
Ⓓ 特に何も行っていない
Ⓔ 外部に委託している業務はない

(2) 業務委託先に管理や指導の実施



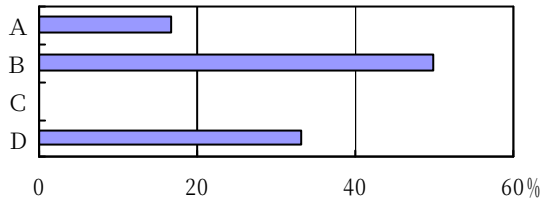
Ⓐ 業務委託先の協力を得て十分な管理や指導を行っている
Ⓑ 業務委託先との間で決められたルールにもとづき連携をとっているが、管理や指導は十分とは言えない
Ⓒ 担当者レベルの注意に依存しており、組織的な管理、指導は行っていない
Ⓓ 特に何も行っていない

分析結果から見た傾向は、以下の通り。

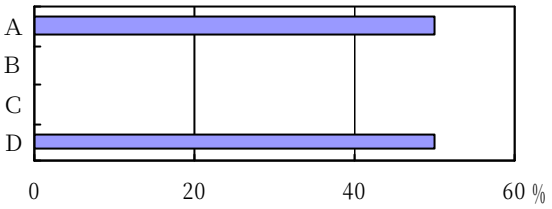
- 本格的な監査はほとんど行われておらず、担当者レベルの自主チェックのレベルに止まっている。
- 監査を実施している中では、外部または別部門の者による監査が実施されており、実施内容もだいたい評価できるものとなっている。

(1) 内部監査の実施状況

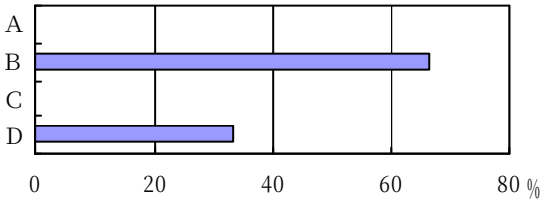
【全体】



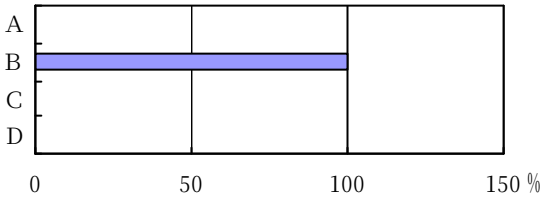
【大規模】



【中規模】



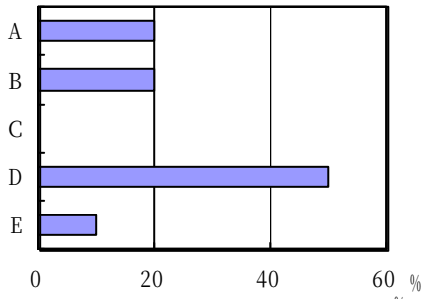
【小規模】



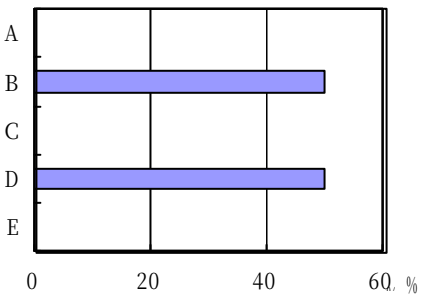
(A) 十分に計画された組織的な監査を年に1回以上実施している
(B) 組織的な監査が年に1回以上行われているが、十分に計画されたものとは言い難い
(C) 担当者レベルで自主的なチェックが年に1回程度行われているが、組織的な監査としては行っていない
(D) 定期的なチェックは特に行っていない

(2) 監査の実施体制

【全体】

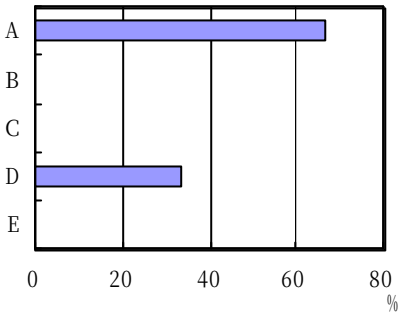


【大規模】

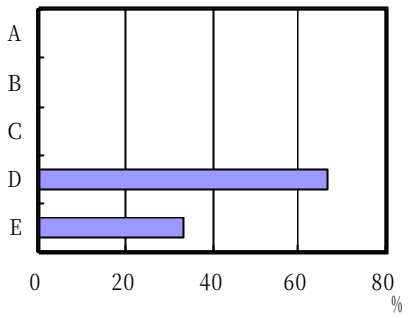


(A) 監査を外部に委託
(B) 別部門の者も含む自社内の監査体制で実施
(C) 外部の専門家の支援を得て自社内の特別体制で実施
(D) サイト関係者により実施
(E) 外部の専門家の支援を得てサイト内の関係者により実施

【中規模】

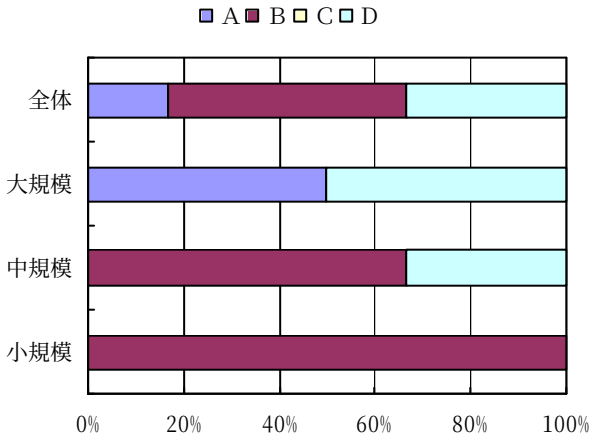


【小規模】



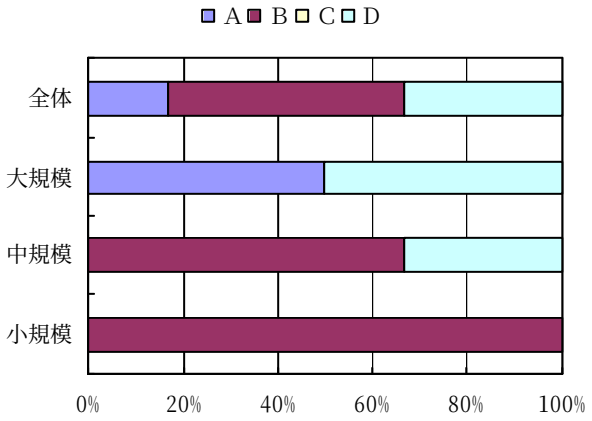
(A) 監査を外部に委託
(B) 別部門の者も含む自社内の監査体制で実施
(C) 外部の専門家の支援を得て自社内の特別体制で実施
(D) サイト関係者により実施
(E) 外部の専門家の支援を得てサイト内の関係者により実施

(3) 監査の内容



(A) 必要な事項はすべてカバーしており、充実したものである
(B) おおむね十分なものと考えているがまだ改善する余地はある
(C) 一通りの項目はカバーしているが、監査としては、さらなる充実が必要である
(D) 断片的で、全体的な再構築が必要である

(4) 監査結果の活用状況



(A) 問題点の指摘も十分で、指摘事項に対しては迅速に改善が行われている
(B) 問題点の指摘や指摘された問題点のフィードバックには不満な点があるが、監査は有効に機能している
(C) 指摘された問題点に対するフィードバックは不十分で、チェックの実施が活かされているとは言い難い
(D) 問題点もそれほど指摘されず、あまり機能していない

4 不正アクセス対策

本章では、EC サイトにおける不正アクセス（侵入）対策の実施状況について分析を行う。
分析項目については、以下の通り。

- アクセス制御
- 機器へのサービス・ソフトウェア搭載の管理
- 不正アクセスの監視

4.1 “不正アクセス対策”全体を通しての傾向

不正アクセス対策の必要性は、十分認識されている。ファイアウォール等の機器の設置レベルでの対策は一通り行われているようであるが、要求事項の指定や実装のレベルになると組織的な取組みはまだまだ不十分である。

また、小規模サイトでは組織的な管理ができていない傾向にあり、大規模サイトでは対策全般はできているようだが、ログの保管については組織的なルールがないところも見受けられる。

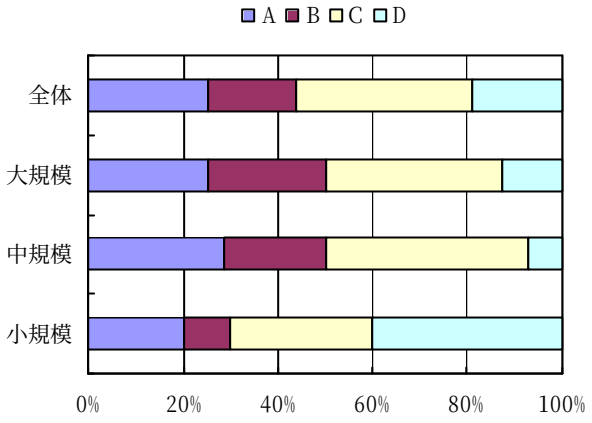
4.2 設問ごとの分析結果

4.2.1 アクセス制御

分析結果から見た傾向は、以下の通り。

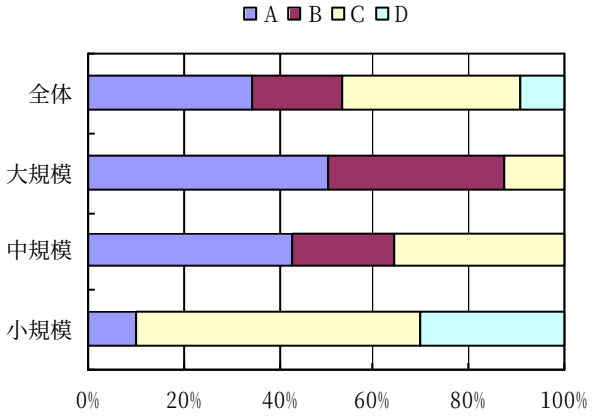
- 全体を通じて、小規模サイトの多くでは、組織的な取組みが行われておらず、全サイトで見ても半数程度のサイトしか組織的な管理がなされていない。
- アカウント指定の管理については、規模が大きなサイトほどよく管理されている。
- ルータ、ファイアウォール、プロキシの通信制御要件の指定と実装については、大規模サイトでは組織的な管理がよくなされている。一方、小規模サイトでは、担当者に依存していたり、または管理がなされていない場合が多い。

(1) アクセス制御要件の指定



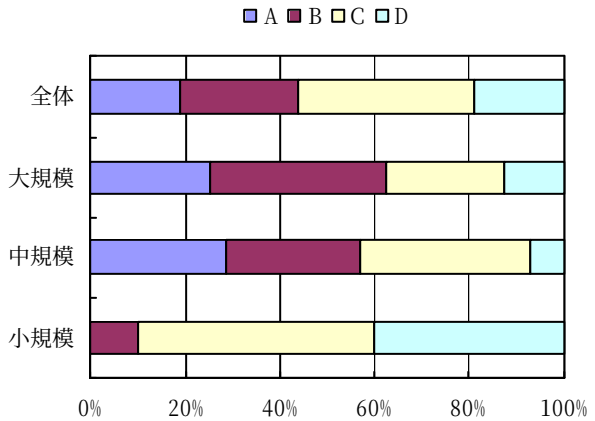
Ⓐ 各機器におけるサービスや機能に対するアクセス制御要件の指定時のレビューや定期的な見直しも、組織的に厳格に行われていて、すべてにわたり指定の妥当性は維持されている
（Ⓑ）アクセス制御要件の指定時のレビューや定期的な見直しが組織的に行われることになっているが、厳格に運用されておらず、妥当性を欠くところが見逃されている可能性もある
Ⓒ 担当者レベルでの指定にあたってのレビューや見直しは行われているが、これらは担当者の注意に依存している
Ⓓ 指定時のレビューや見直しはあまり行われていなく、実質的に無管理状態に近い

(2) アカウント指定の管理



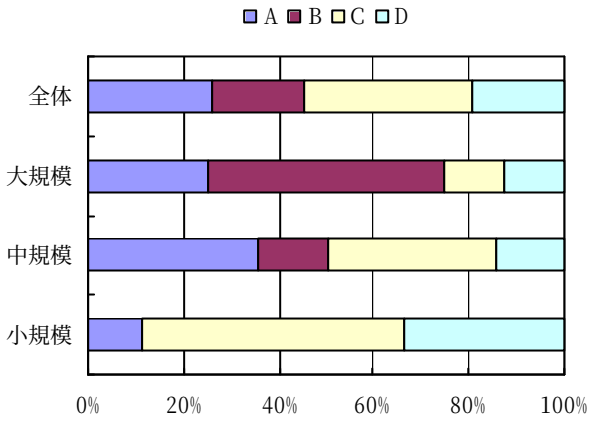
Ⓐ 確立したルールのもとで組織的な管理が厳格に行われている
Ⓑ ルールにそった組織的な管理が行われることになっているが、その運用は厳格でなく、不適切なところが見過ごされている可能性もある
Ⓒ ルールは確立していないが、担当者レベルで一通りの管理は行われている
Ⓓ 担当者レベルでの管理も行われてなく、ほとんど無管理状態である

(3) アクセス制御要件の機器への設定の反映



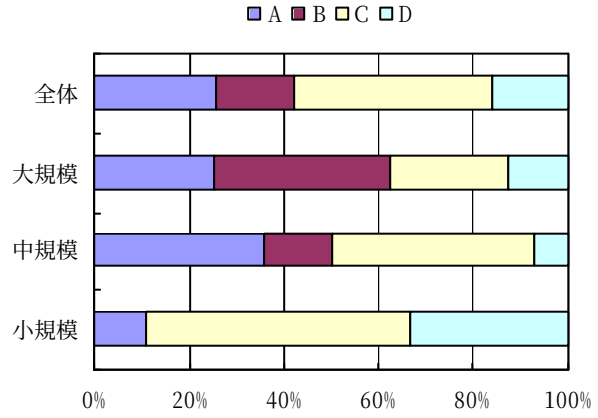
Ⓐ 設定時の確認や定期的な見直しも、組織的に厳格に行われていて、すべてにわたり設定の妥当性は確認されている
Ⓑ 設定時の確認や定期的な見直しは組織的に行われることになっているが、厳格に運用されておらず、設定のミスや要件の変更への追随が見逃されている可能性もある
Ⓒ 担当者レベルでの設定の確認や見直しは行われているが、これらは担当者の注意に依存している
Ⓓ 設定時の確認や見直しはあまり行われていない

(4) ルータ、ファイアウォール、プロキシ等の通信制御要件の指定



(A) これらの機器における通信に対する制御要件の指定時のレビューや定期的な見直しも、組織的に厳格に行われていて、すべてにわたり指定の妥当性は維持されている
(B) アクセス制御要件の指定時のレビューや定期的な見直しが組織的に行われることになっているが、厳格に運用されておらず、妥当性を欠くところが見逃されている可能性もある
(C) 担当者レベルでの指定にあたってのレビューや見直しは行われているが、これらは担当者の注意に依存している
(D) 指定時のレビューや見直しはあまり行われていなく、実質的に無管理状態に近い

(5) 通信制御要件のルータ、ファイアウォール、プロキシへの設定の反映



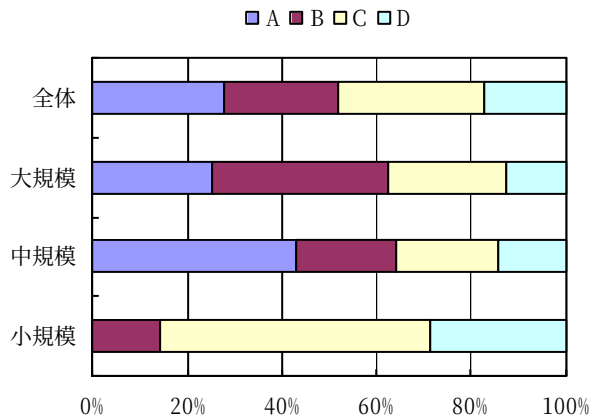
(A) 設定時の確認や定期的な見直しも、組織的に厳格に行われていて、すべてにわたり設定の妥当性は確認されている
(B) 設定時の確認や定期的な見直しは組織的に行われることになっているが、厳格に運用されておらず、設定のミスや要件の変更への追随が見逃されている可能性もある
(C) 担当者レベルでの設定の確認や見直しは行われているが、これらは担当者の注意に依存している
(D) 担当者レベルでの設定時の確認や見直しはあまり行われてなく、実質的に無管理状態に近い

4.2.2 機器へのサービス・ソフトウェア搭載の管理

分析結果から見た傾向は、以下の通り。

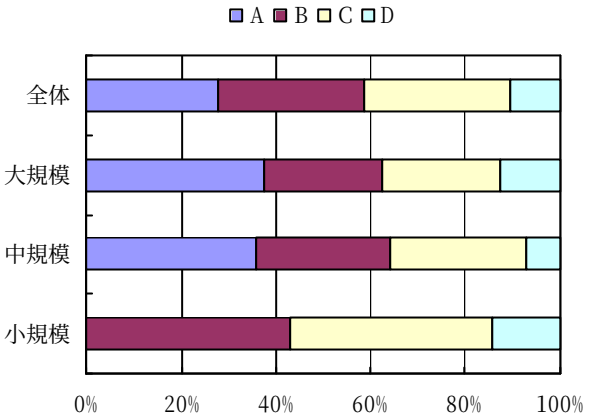
- 小規模サイトの多くでは、組織的な取組みが行われていない傾向にある。

(1) 搭載制限の指定



(A) 各機器における搭載できるサービスとその条件の指定時のレビューや定期的な見直しも、組織的に厳格に行われていて、すべてにわたり指定の妥当性は維持されている
(B) これらについての指定時のレビューや定期的な見直しが組織的に行われることになっているが、厳格に運用されておらず、妥当性を欠くところが見逃されている可能性もある
(C) 担当者レベルでの指定にあたってのレビューや見直しは行われているが、これらは担当者の注意に依存している
(D) 指定時のレビューや見直しはあまり行われていなく、実質的に無管理状態に近い

(2) 搭載されたサービス・ソフトウェアの管理状況



(A) 当初設定時や変更時の確認および定期的な見直しも、組織的に厳格に行われていて、すべてにわたり設定の妥当性は確認されている
(B) 当初設定時や変更時の確認および定期的な見直しは、組織的に行われることになっているが、厳格に運用されておらず、設定のミスや要件の変更への追随が見逃されている可能性もある
(C) 担当者レベルでの設定の確認や見直しは行われているが、これらは担当者の注意に依存している
(D) 担当者レベルでの設定時の確認や見直しはあまり行われてなく、実質的に無管理状態に近い

4.2.3 不正アクセスの監視

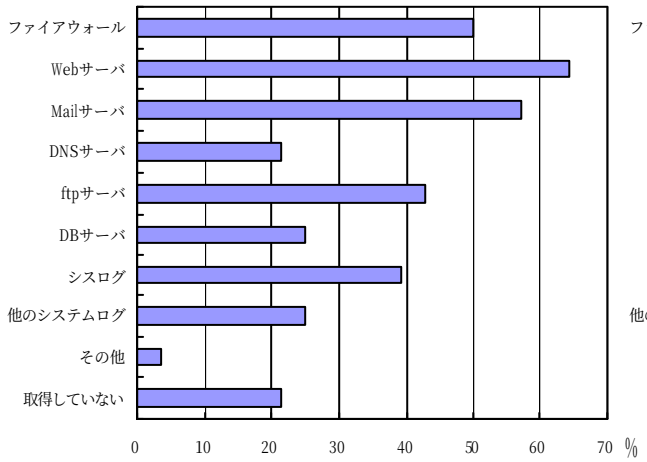
分析結果から見た傾向は、以下の通り。

- 大規模サイトでは、アクセスログは取っていてもログの保管については管理できていない傾向にある。
- 小規模サイトでは、ログの分析が十分にできていない。
- 取得したアクセスログの保管に関しては、大規模のサイトであっても必ずしも組織的に管理されておらず、全サイトを見ても半数程度しか組織的に実施していない。
- ログ分析の活用については、大規模サイトでは十分行っているようであるが、小規模サイトでは、十分な活用はできていない傾向にある。
- 大規模サイトでは、侵入監視を実施した結果が、侵入発見・被害拡大防止に結びついている。

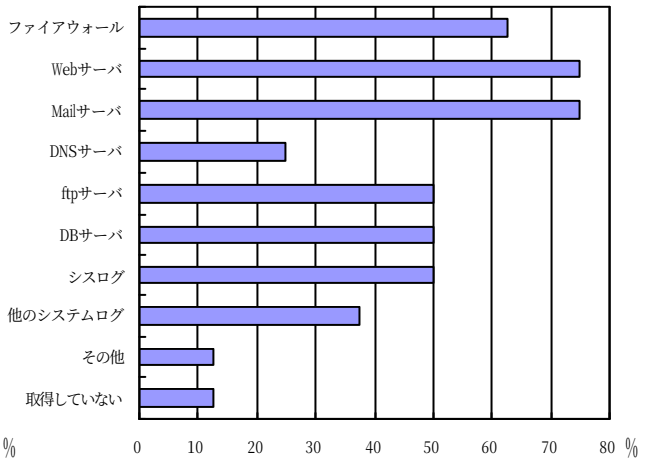
(1) ログの適切な取得

① 取得しているログ

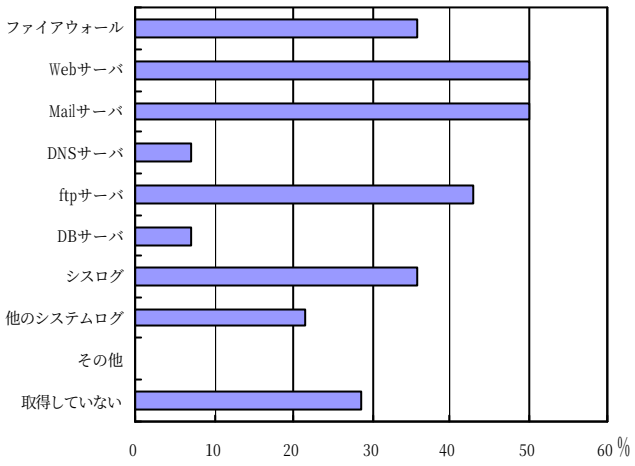
【全体】



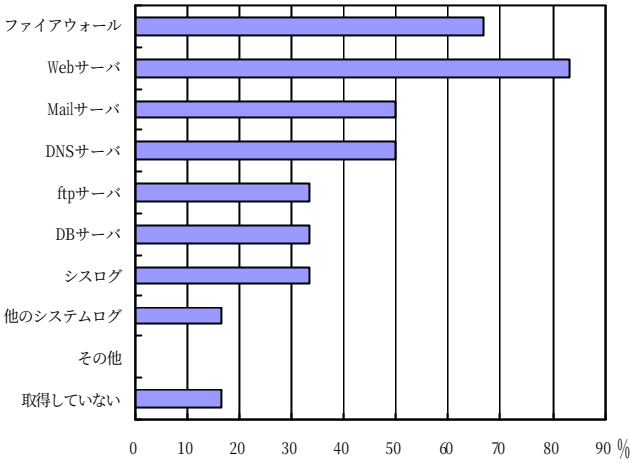
【大規模】



【中規模】

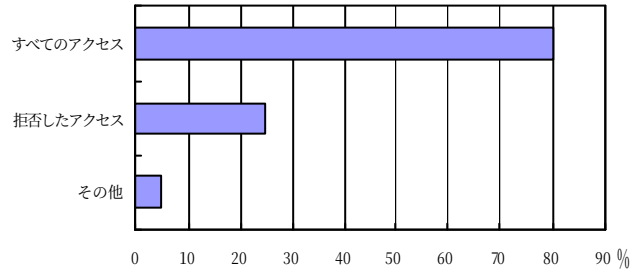


【小規模】

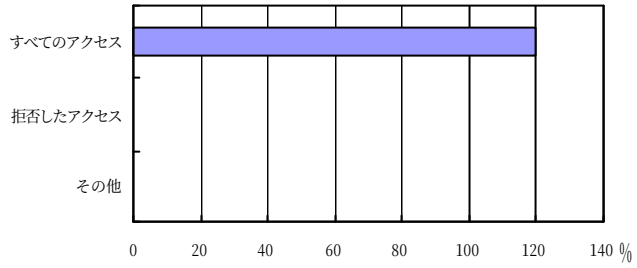


② ログ取得の対象としているイベント

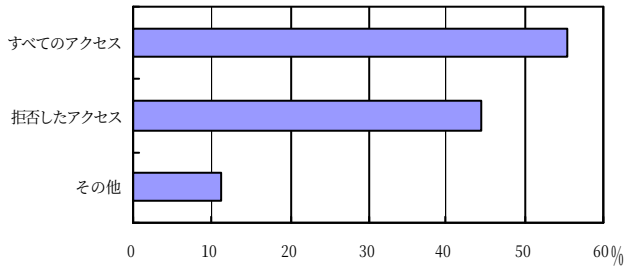
【全体】



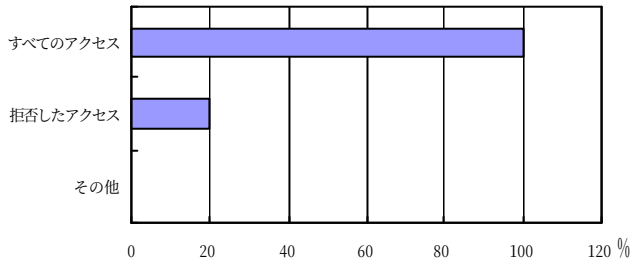
【大規模】



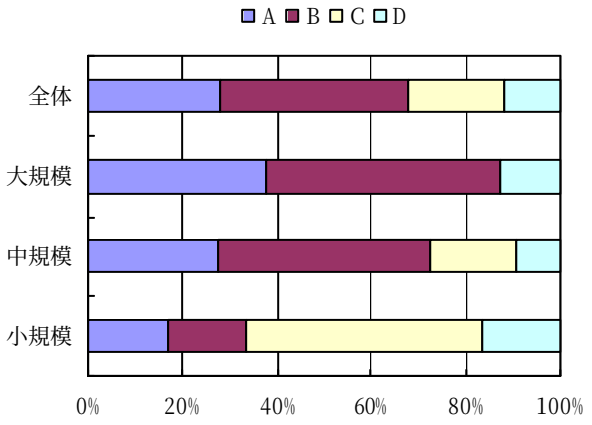
【中規模】



【小規模】



③ アクセスログ取得の実施



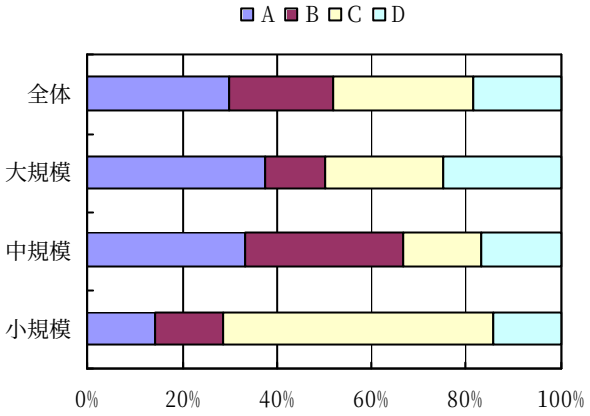
(A) ほとんどすべてのログを取得している。また、十分な取得領域の確保と取得したログの安全な保管も十分に管理されている

(B) サイト内の通信や重要なサービスへのログは取得している。すべてを対象としてはいないが、サイトの運営形態から見て、おおむね必要なログは取得している。取得領域の確保や取得ログの安全な保管も行われることになっている

(C) ログ取得は行っているがその指定は担当者レベルであり、取得したログの保管等も担当者任せとなっている

(D) 計画的なログの取得は行っていない、もしくは行っていても計画的なものではない

(2) 取得したアクセスログの保管

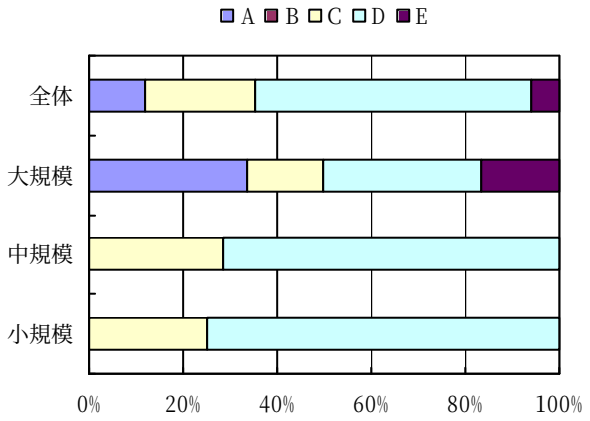


Ⓐ 指定したログの取得および取得したログに対する安全措置ならびに保管は、十分な計画のもとに行っており、またその管理も十分である
Ⓑ 指定したログ取得および取得したログに対する安全措置ならびに保管は十分な計画にもとづいているが、管理は十分でない
Ⓒ 担当者レベルでの管理は行っているが、十分とは言えない
Ⓓ担当者任せとなっていて、ほとんど管理はされていない

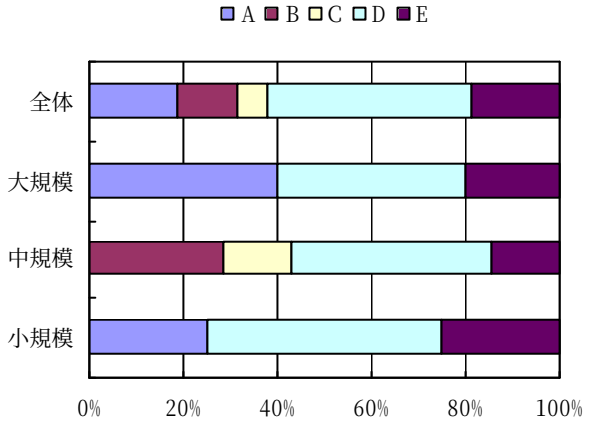
(3) 取得したログの分析

① ログ分析の実施状況

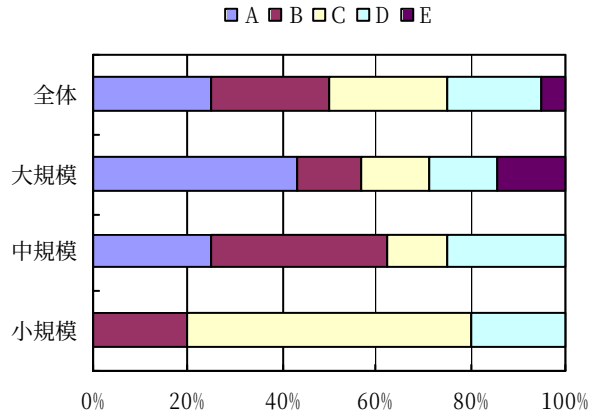
(a) シスログ



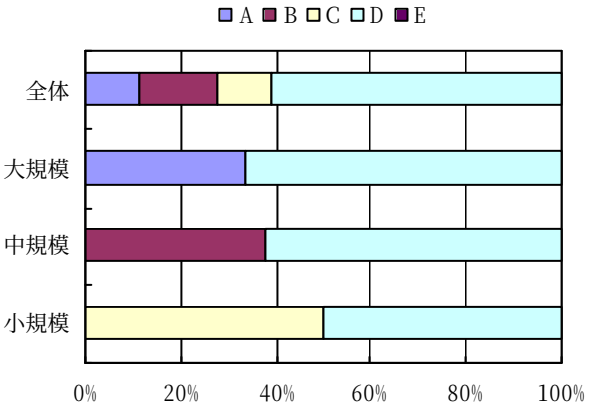
(b) シスログ以外のシステムログ



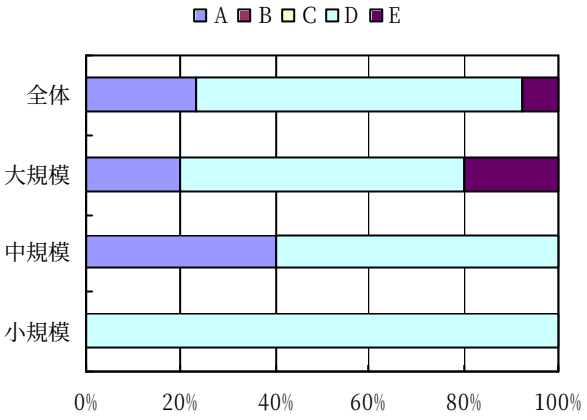
(c) Web のログ



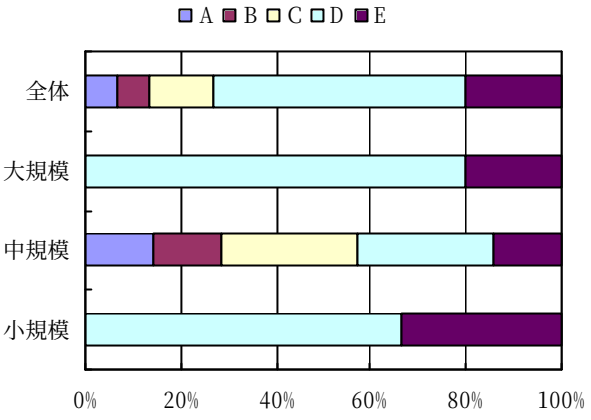
(d) Mail のログ



(e) DB のログ

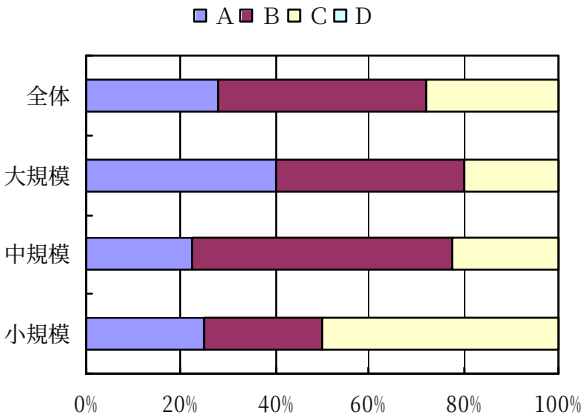


(f) ftp のログ



(A) 毎日　(B) 毎週　(C) 毎月　(D) 必要の都度　(E) あまり行っていない

② ログ分析の効果

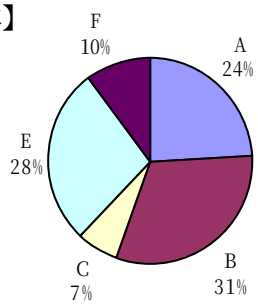


(A) 十分な分析が行われて大いに有効である
(B) 一通りの分析は行っているが効果をあげるためにはさらに綿密な分析が必要
(C) 分析は形式的であまり効果的とは思えない
(D) 有効な分析になっていない

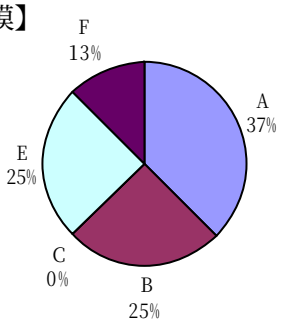
(4) 侵入監視の実施

① 実施の有無

【全体】

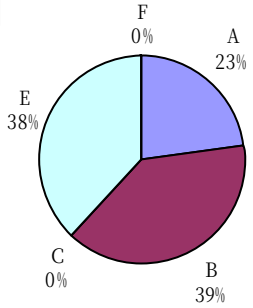


【大規模】

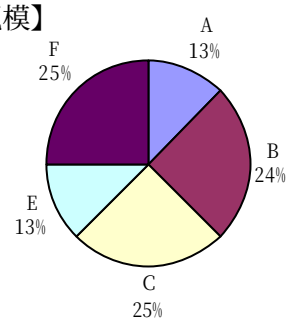


（A）ツールを装備し自社で侵入監視を行っている
(B) ベンダーの侵入監視サービスを利用している
(C) 侵入監視の実施を計画中
(D) 実施していないが、今後検討したい
(E) 実施しておらず、今後も実施する予定はない

【中規模】



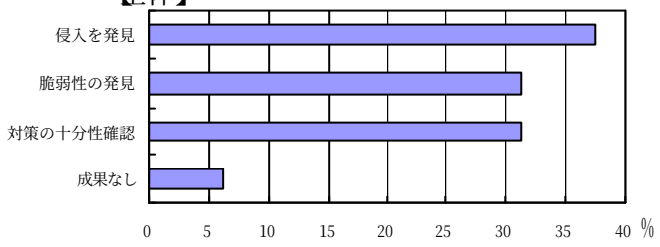
【小規模】



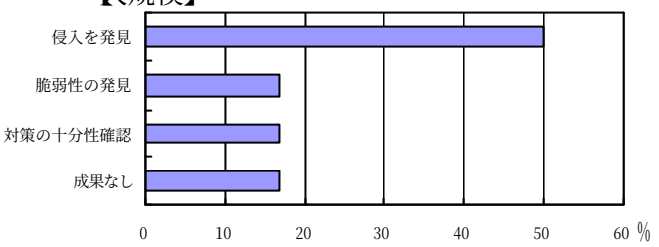
（A）ツールを装備し自社で侵入監視を行っている
(B) ベンダーの侵入監視サービスを利用している
(C) 侵入監視の実施を計画中
(D) 実施していないが、今後検討したい
(E) 実施しておらず、今後も実施する予定はない

② 実施の効果

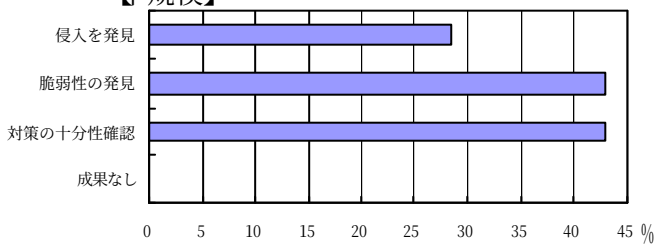
【全体】



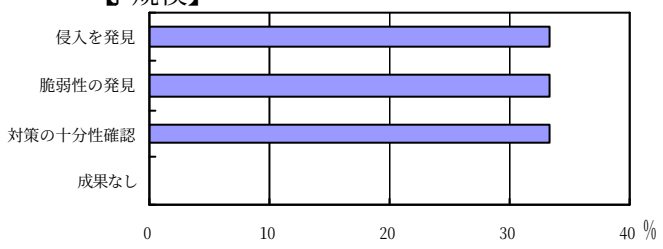
【大規模】



【中規模】

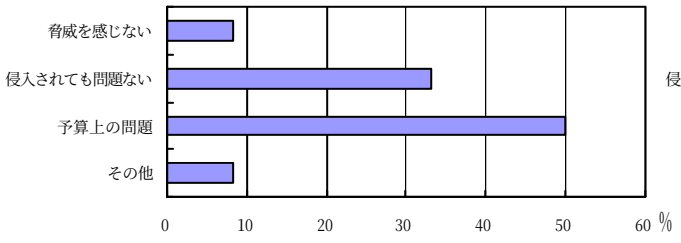


【小規模】

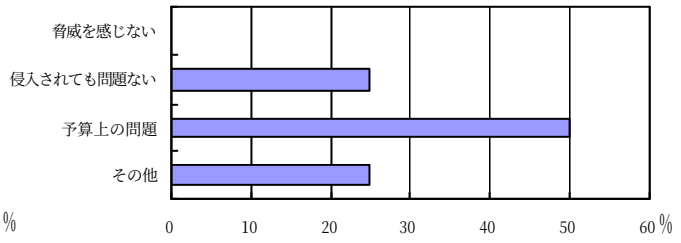


③ 実施していないサイトの未実施理由

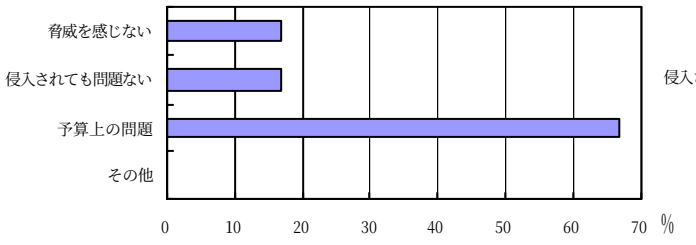
【全体】



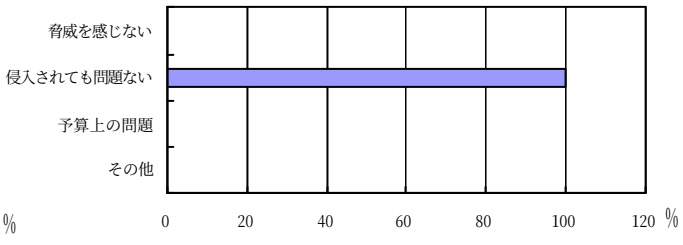
【大規模】



【中規模】

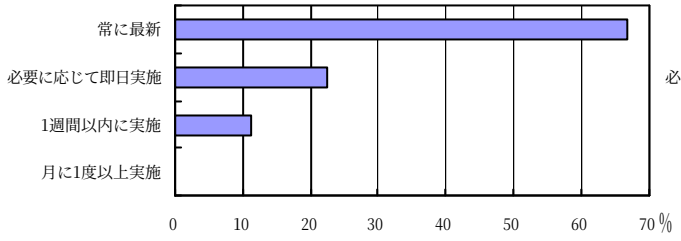


【小規模】

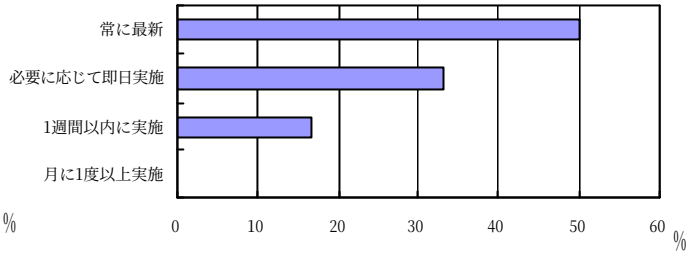


(5) 侵入監視ツールのメンテナンス実施状況

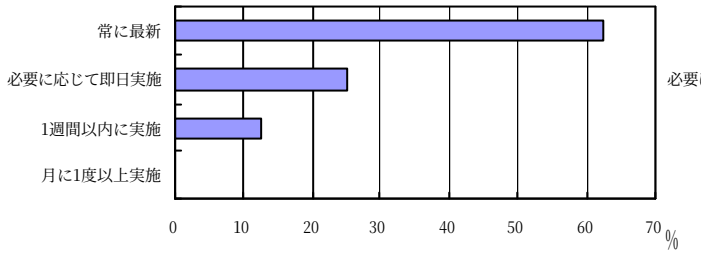
【全体】



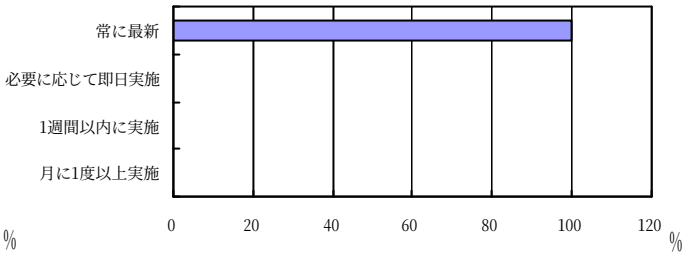
【大規模】



【中規模】



【小規模】



5 セキュリティホール対策

本章では、EC サイトのシステムに内在するセキュリティホールに対する取組みについて分析を行う。

分析項目については、以下の通り。

- セキュリティホールに対する取組方針の確立
- セキュリティホールに関する最新情報の収集と分析への取組み
- システムに対するセキュリティホール検査の実施
- セキュリティホール対策の実施

5.1 “セキュリティホール対策”全体を通しての傾向

セキュリティホール対策は、ほとんどのサイトで実施されているが、セキュリティホール検査の実施については定期的に検査を実施していてもルールに基づいて組織的な検査を実施しているサイトは少なく、全体として担当者の行動に依存した状況にある。

また、積極的に対策に取組んでいるサイトとまったく取組んでいないサイトの 2 極分化がうかがえる。

5.2 設問ごとの分析結果

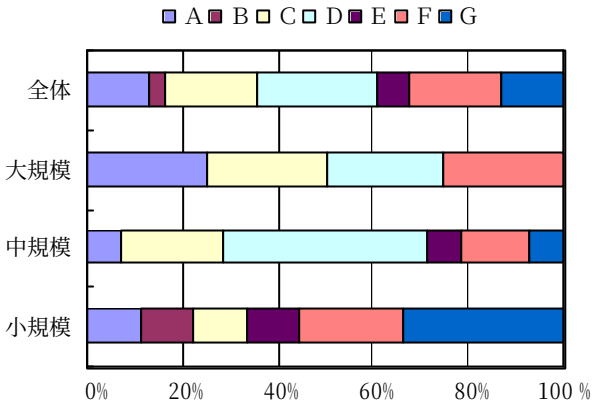
5.2.1 セキュリティホールに対する取組方針の確立

分析結果から見た傾向は、以下の通り。

- セキュリティホール対策の取組方針としては、外部からアクセス可能なマシンに限定して実施するサイトが多い一方で、システムメンテナンス時まで何も対策を実施しないサイトも見受けられる。
- 対策を実施しているサイトの半数は、現在実施しているセキュリティホール対策に問題があると感じている。

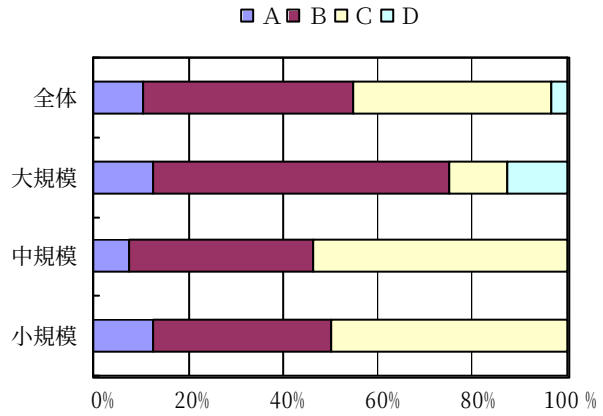
(1) 基本方針

① 取組方針の内容



(A)全ての機器を対象に既知のセキュリティホールゼロを目標
(B) 全ての機器を対象に危険と判断されたセキュリティホールゼロを目標
(C) 外部からアクセス可能なマシンに限定し、既知のセキュリティホールゼロを目標
(D)外部からアクセス可能なマシンにおける危険と判断されたセキュリティホールは、運用の都合に優先して対策
(E) 外部からアクセス可能なマシンにおける危険と判断されたセキュリティホールは、運用の都合がつき次第できるだけ早い時機に対策
(F) 通常は特に対策せず、システムのメンテナンスに合わせて対策
(G) 特に方針は持っていない

② 方針の評価



(A) 万全と考えている
(B) 万全ではないが、サイトの運営実態から見てこれで十分と考えている
(C) 多少問題はあるがサイトの運営上からこのような取組みが限界
(D) 問題と考えており、このような対応は脅威であると感じている

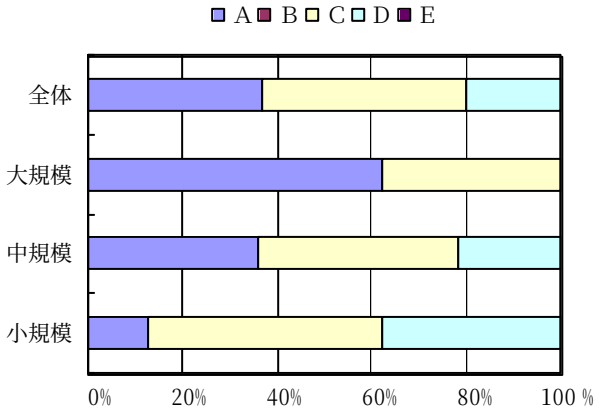
5.2.2 セキュリティホールに関する最新情報の収集と分析への取組み

分析結果から見た傾向は、以下の通り。

- 大規模サイトの全てにおいてセキュリティホールに関する情報収集が業務として実施されているが、サイトの規模が小さくなるに従って収集を行わないサイトが多くなる。

(1) セキュリティホールについての情報収集

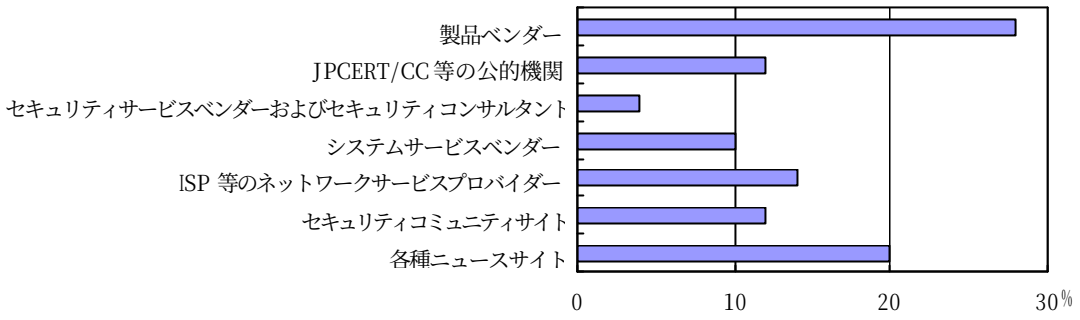
① セキュリティホールに関する情報収集状況



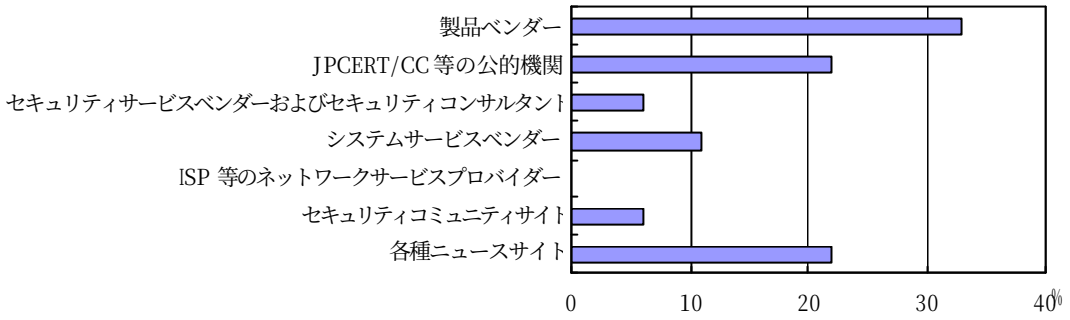
(A) セキュリティホールに関する情報の入手についてのルールや責任者も決められており、定期的に情報を入手している
(B)セキュリティホールに関する情報の入手についてのルールや責任者も決められているが、励行されていない
(C) 特に話題となった場合に行われることもあるが、日常は担当者の意識に依存
(D) 特に意識して情報の収集は行っていない
(E) かつては収集していたが現在では行っていない

② 情報の収集元

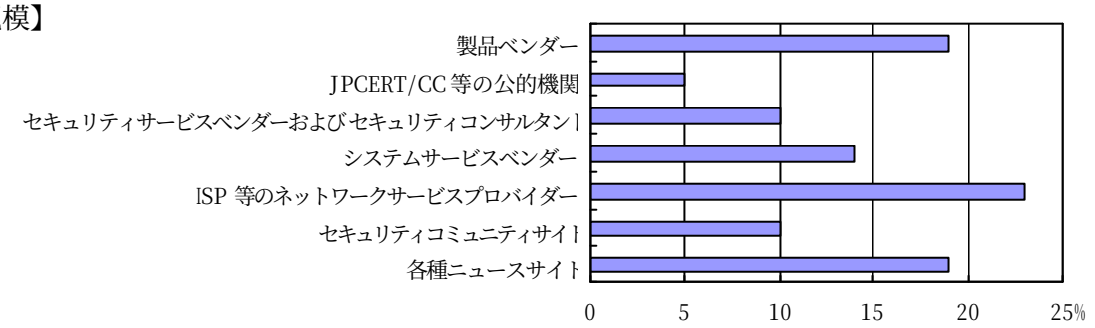
【全体】



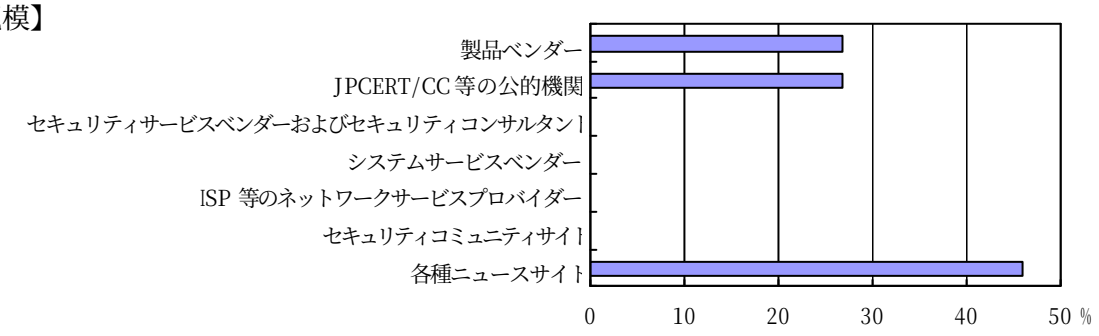
【大規模】



【中規模】

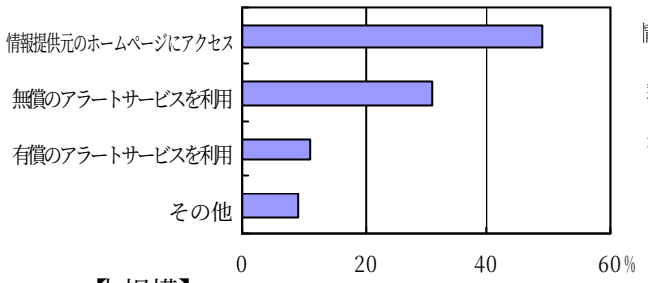


【小規模】

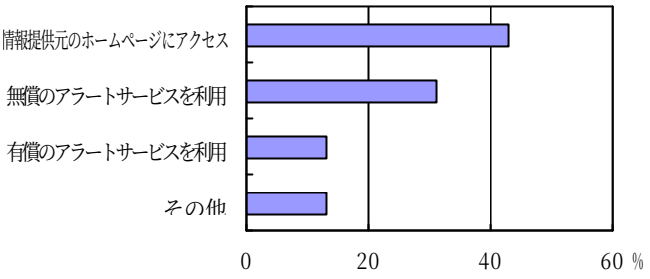


③ 情報の収集方法

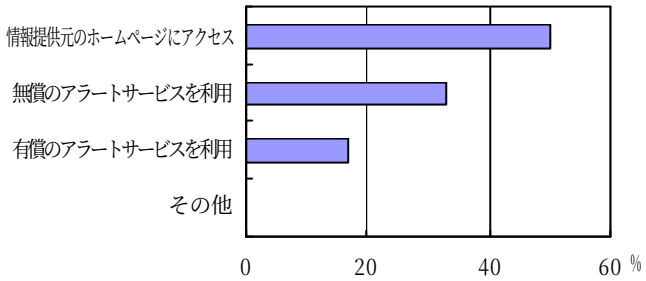
【全体】



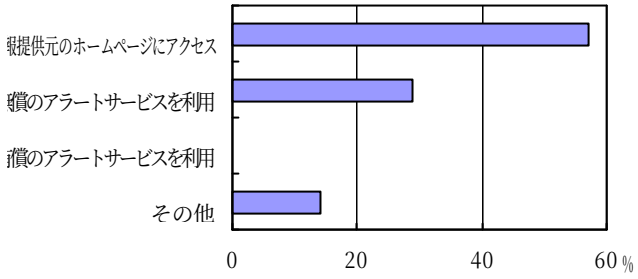
【大規模】



【中規模】

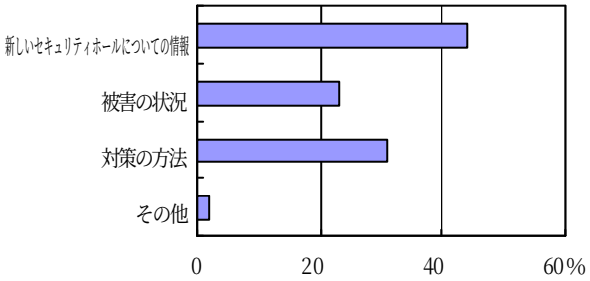


【小規模】

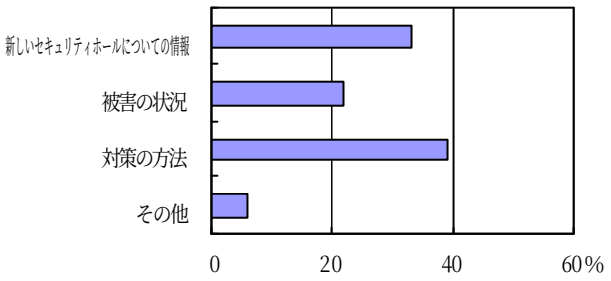


④ 収集している情報

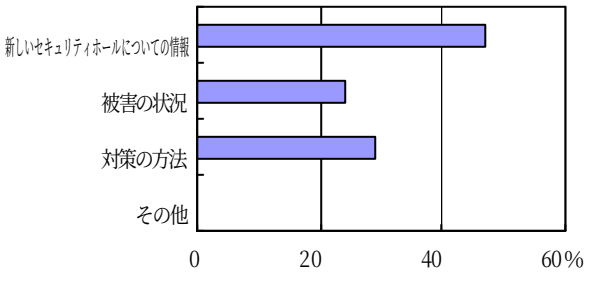
【全体】



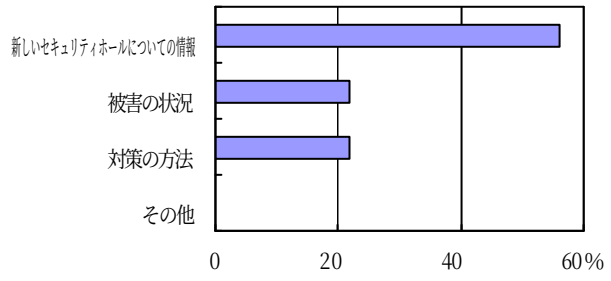
【大規模】



【中規模】

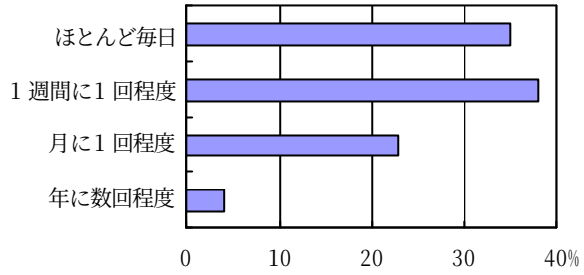


【小規模】

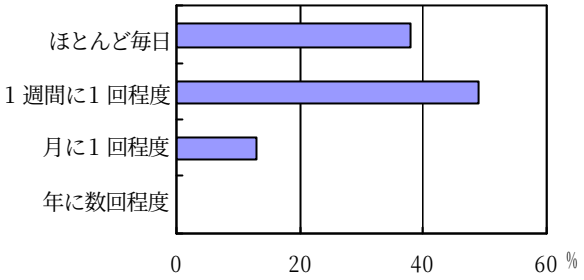


⑤　収集活動の頻度

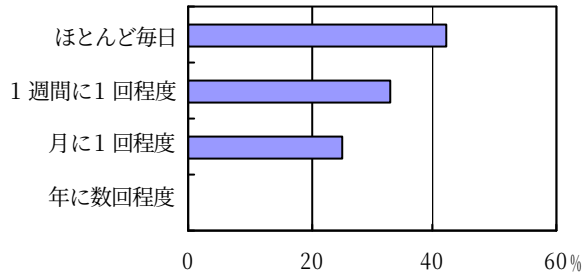
【全体】



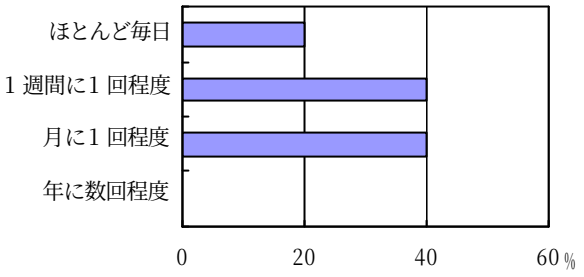
【大規模】



【中規模】

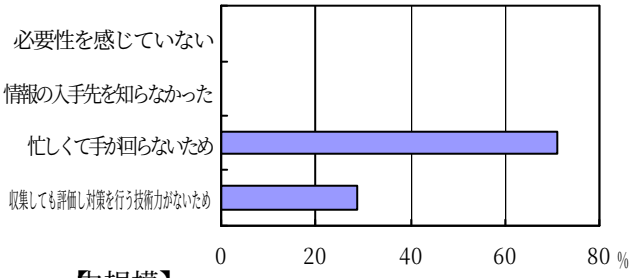


【小規模】

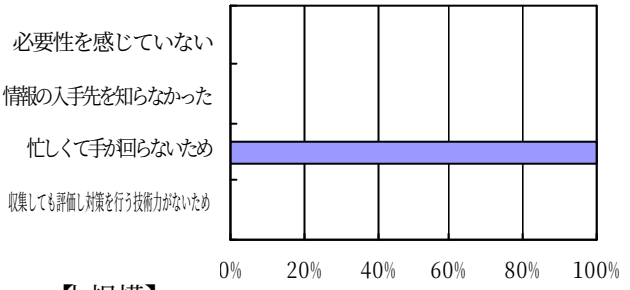


⑥　積極的に収集を行っていない理由

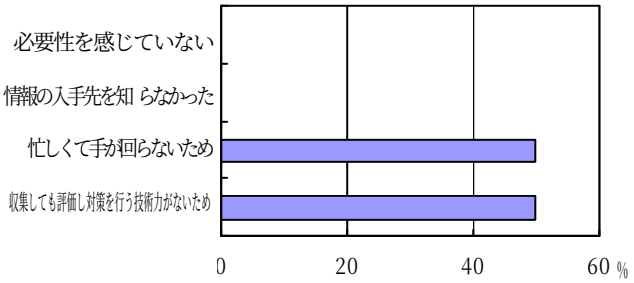
【全体】



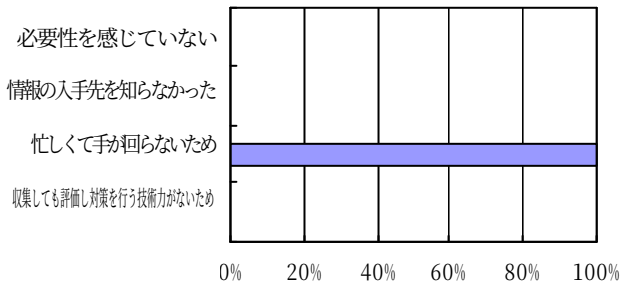
【大規模】



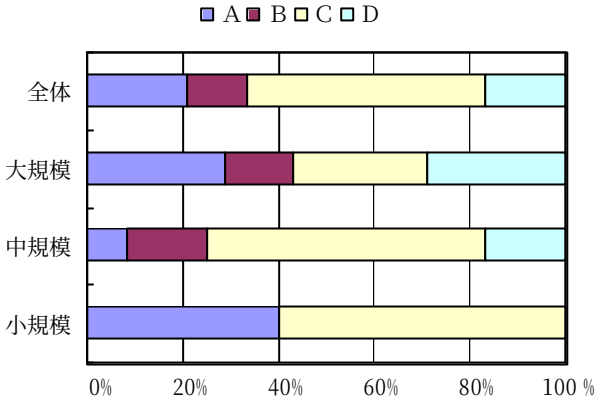
【中規模】



【小規模】



(2) 収集されたセキュリティホールについての情報の評価



(A) 収集した情報のすべてについて対策の要否やその緊急度についての評価、判断は組織的に行われ、対策に適切に反映されている
(B) 収集した情報に対する対策の要否やその緊急度についての評価、判断は組織的に行われることになっているが徹底さに欠けるところもあり、対策への反映は十分とは言えない
(C) 担当者レベルで一通りの対応は行われているが、管理はされていない
(D) 収集はしているが、分析や対策への反映等はほとんど行われていない

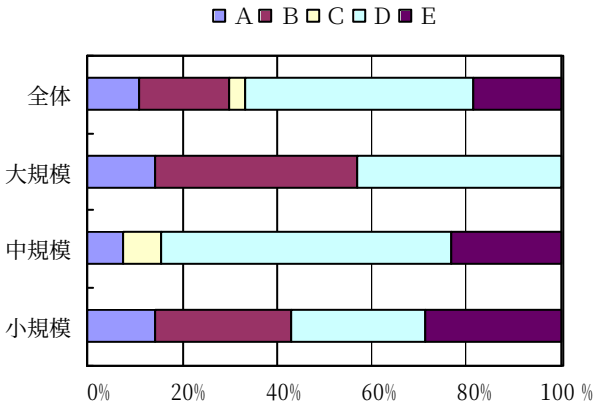
5.2.3 システムに対するセキュリティホール検査の実施

分析結果から見た傾向は、以下の通り。

- 約半数にあたるサイトがセキュリティホール検査を定期的に行っているが、システムに対するセキュリティホール検査を組織的に行っているサイトは 1／3程度と少ない。
- 何らかの形でセキュリティホール検査を行っているサイトのうち、検査の対象とすべきすべての機器に対して検査を行っているのは半数以下。

(1) システムに対するセキュリティホール検査

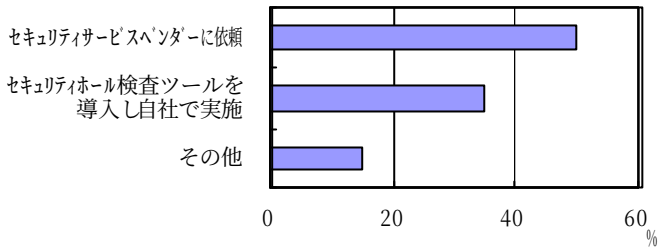
① 評価



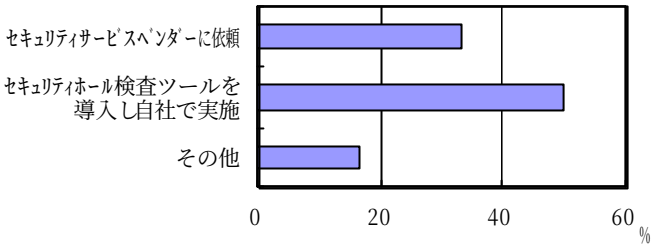
（A）プログラム化され自動的に実施している
（B）システム運用者による検査がルールに沿って励行されている
(C) 検査実施についてのルールは決められているが、あまり励行されていない
(D) 特にルールは決められておらず、運用担当者の任されている
（E）ほとんど行われていない

② 実施の方法

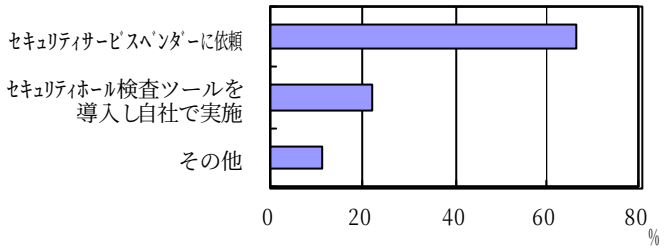
【全体】



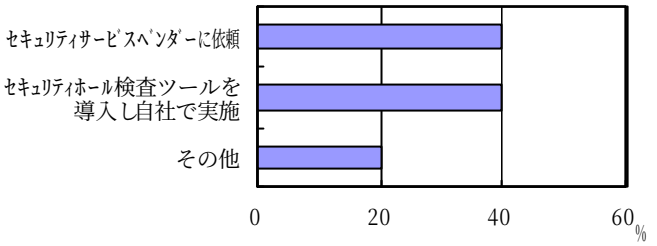
【大規模】



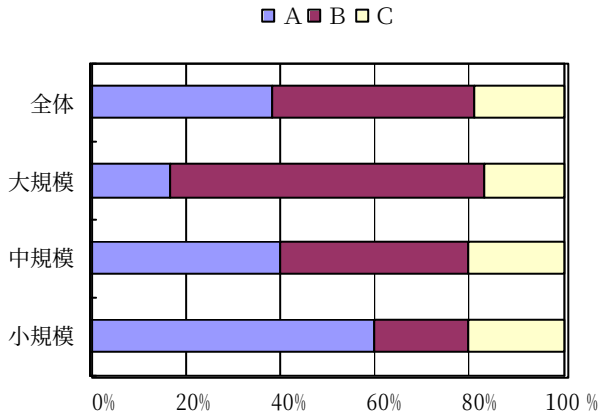
【中規模】



【小規模】



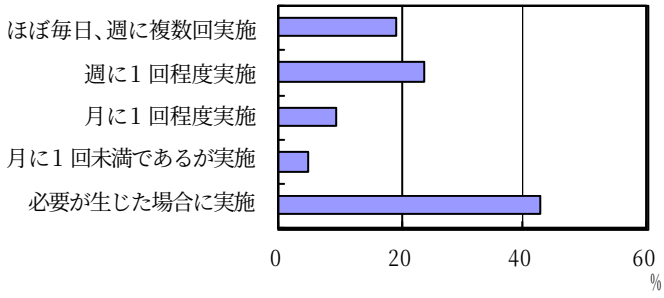
③ 検査の対象



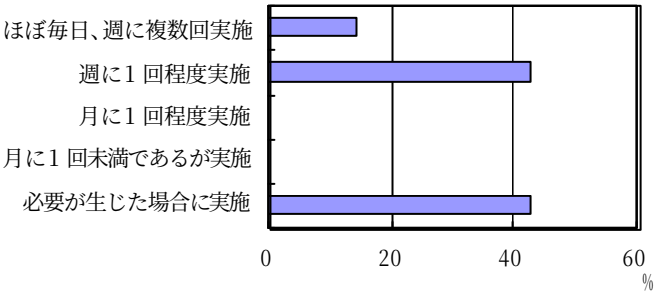
（A）セキュリティホール対策の対象となるすべての機器を対象
(B) 外部からアクセス可能な機器すべてを対象
(C) 特定の機器のみ

④ 検査の頻度

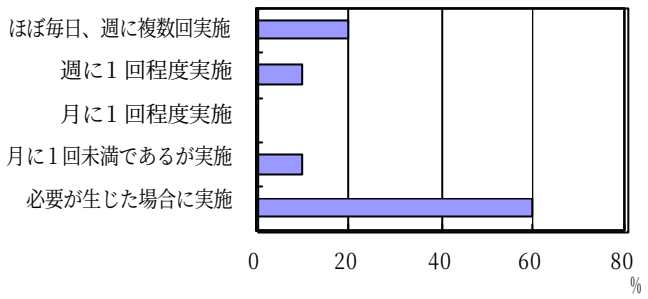
【全体】



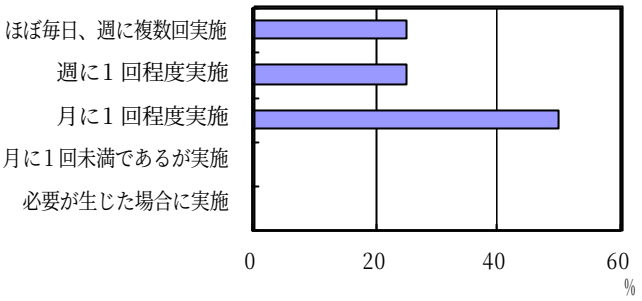
【大規模】



【中規模】

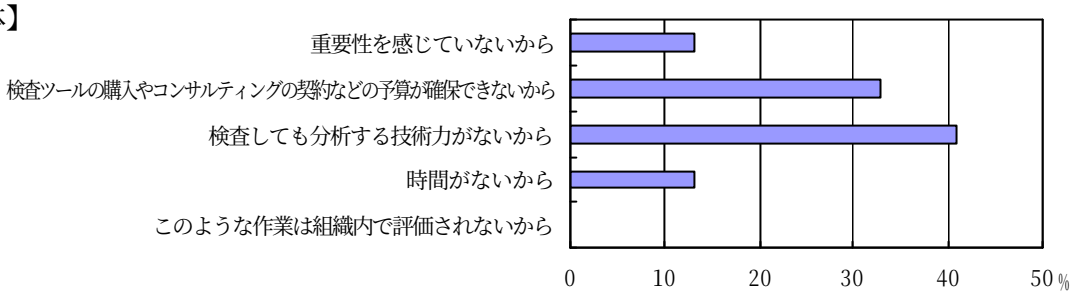


【小規模】

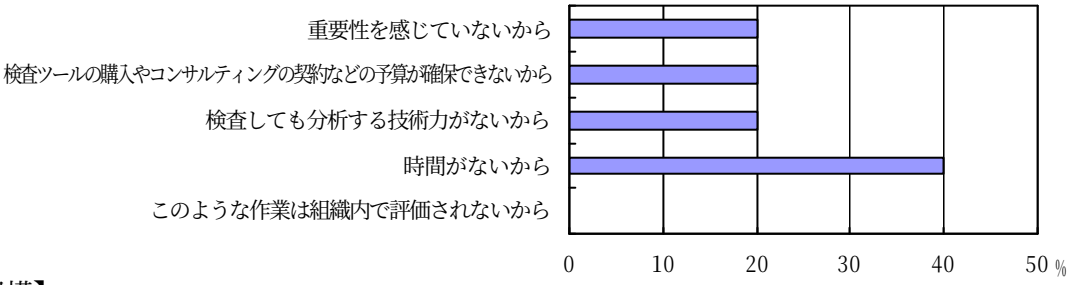


⑤ 十分に検査を行っていない理由

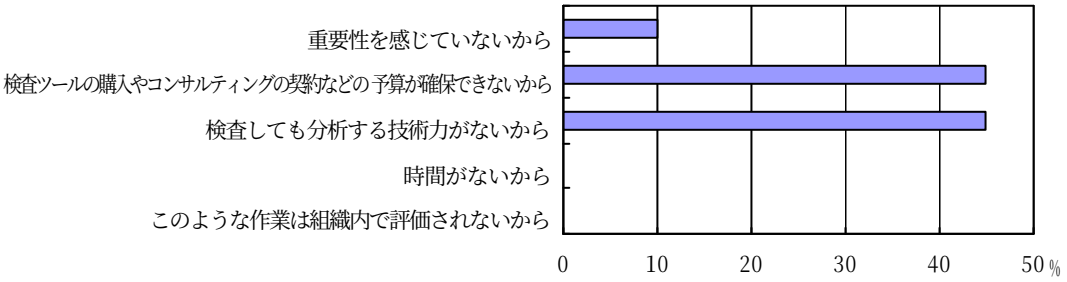
【全体】



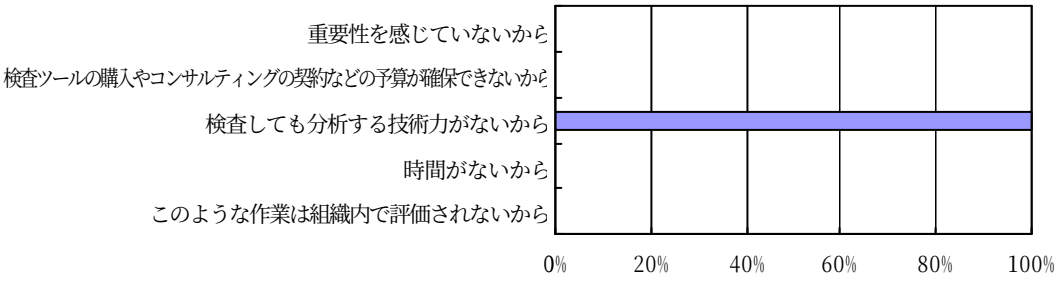
【大規模】



【中規模】

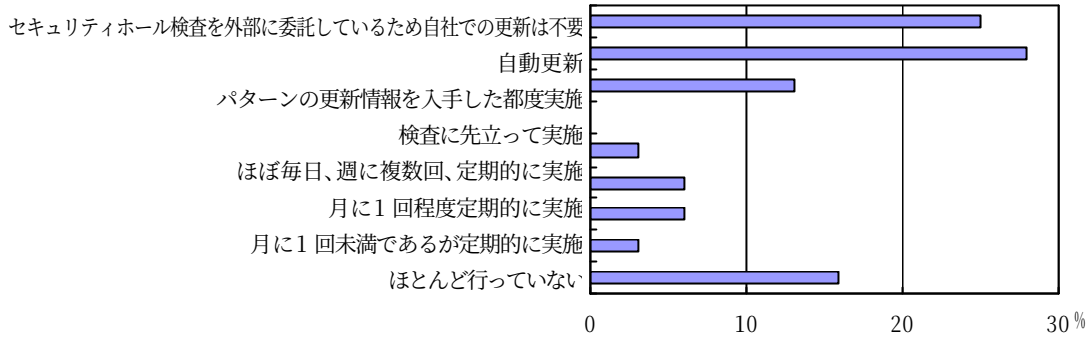


【小規模】

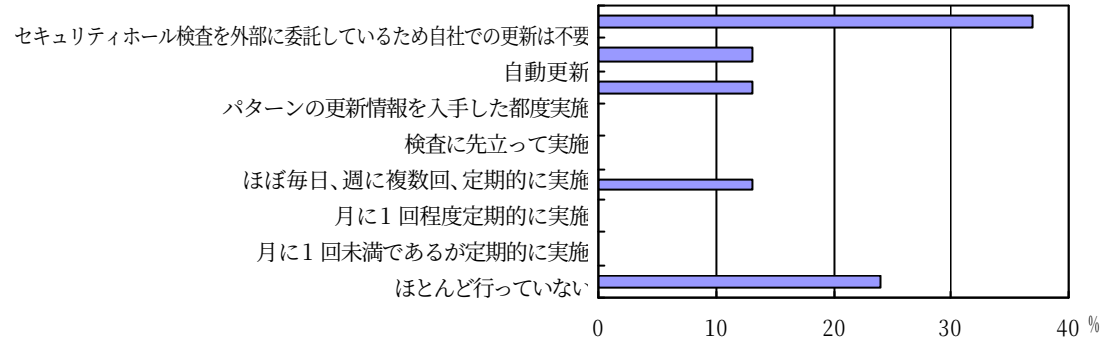


(2) セキュリティホール検査に用いるパターンファイルの更新頻度

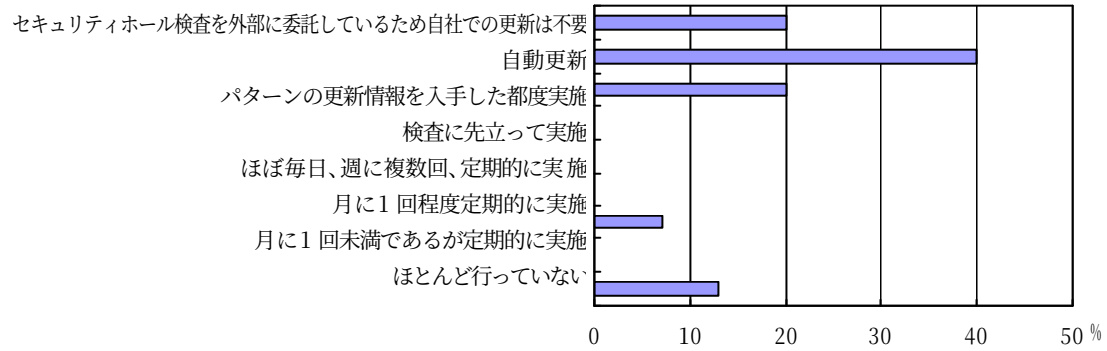
【全体】



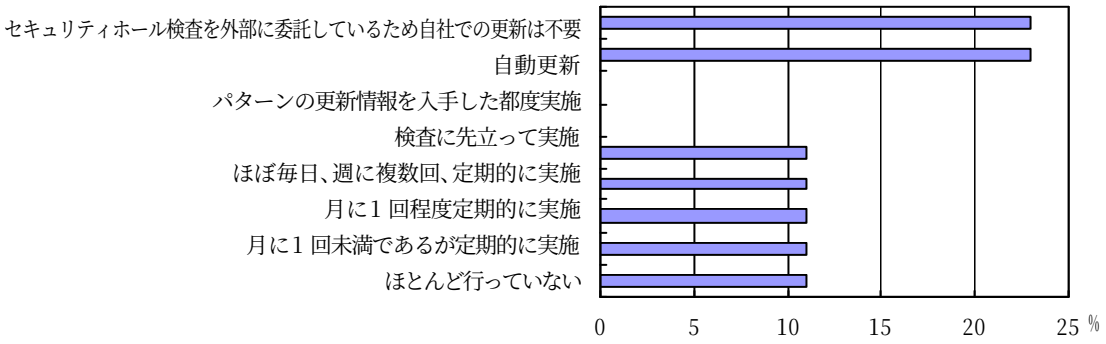
【大規模】



【中規模】



【小規模】



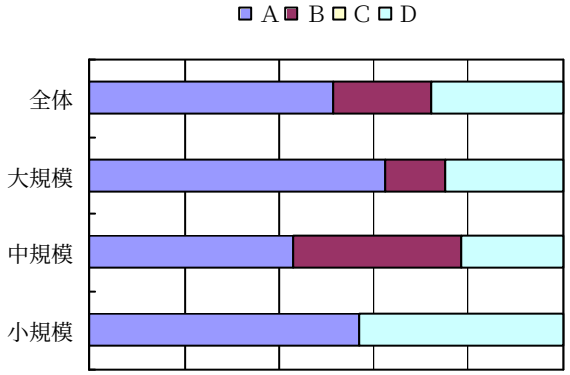
5.2.4　セキュリティホール対策の実施

分析結果から見た傾向は、以下の通り。

- セキュリティホールに対する重大な脅威を認識した場合はショップの規模に関わらず迅速な行動を行える体制が整っているものと思われる。
- 全体としてセキュリティホールに対する対策手順に関する明確な手順が定められておらず、業務担当者の経験と注意への依存度が高いと思われる。

(1) セキュリティホール対策実施の迅速度

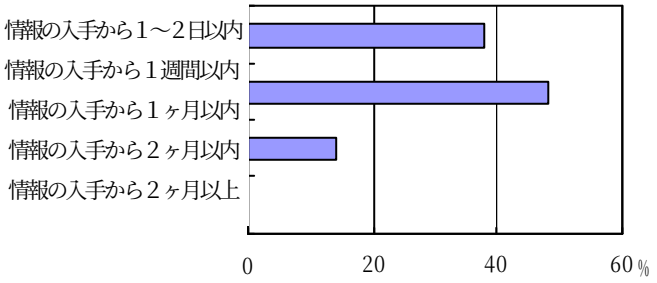
①　評価



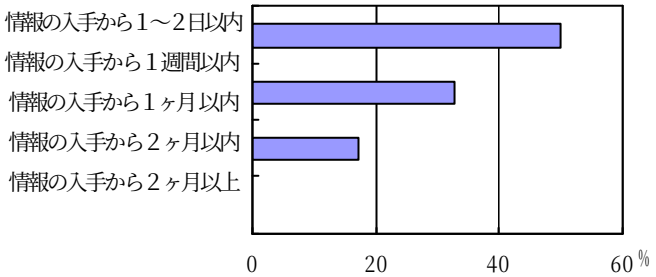
(A) 脅威の程度にもよるが、重大な脅威に対しては遅滞なく対策を行っている
(B) 迅速に実施できるよう努めているが遅れ気味
(C) 対策が迅速に行われることは少ない
(D) 対策はほとんど行っていない

②　平均的なタイムラグ

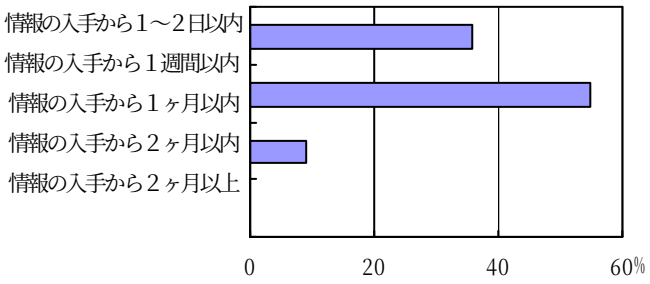
【全体】



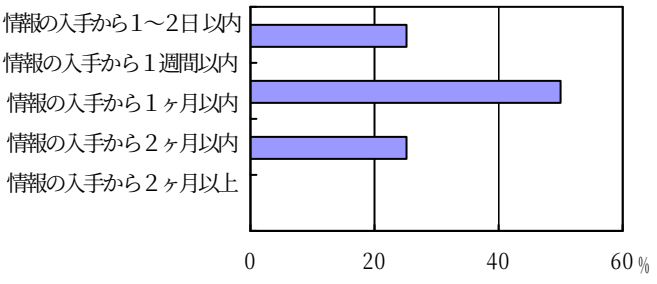
【大規模】



【中規模】

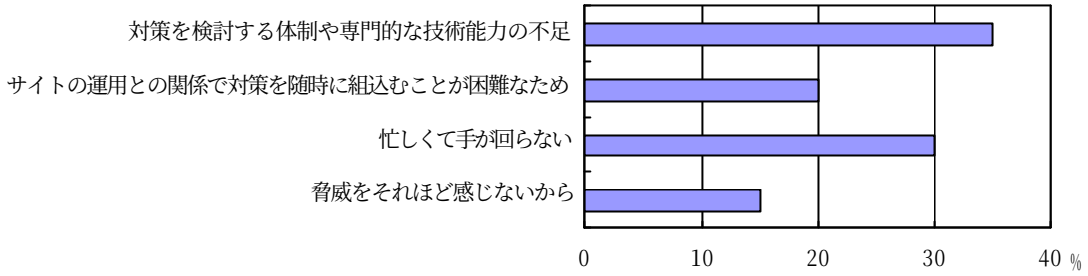


【小規模】

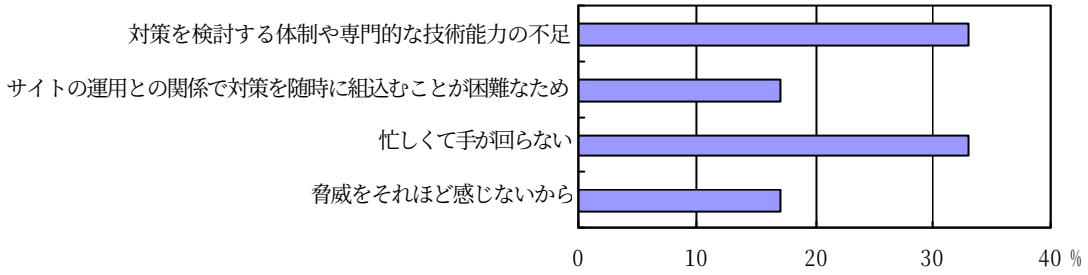


③　対策を迅速に行っていない理由

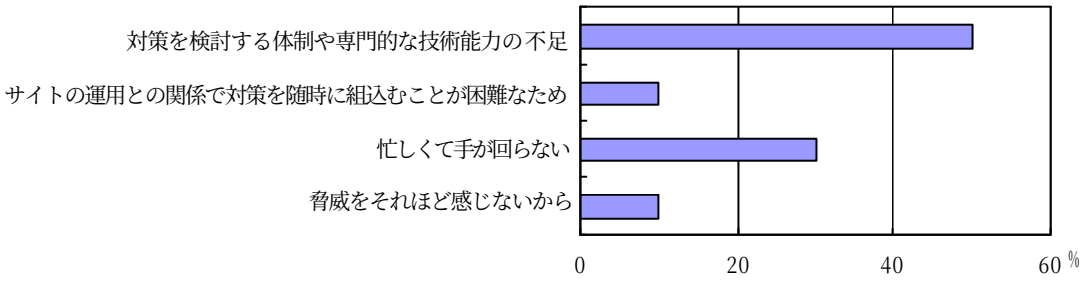
【全体】



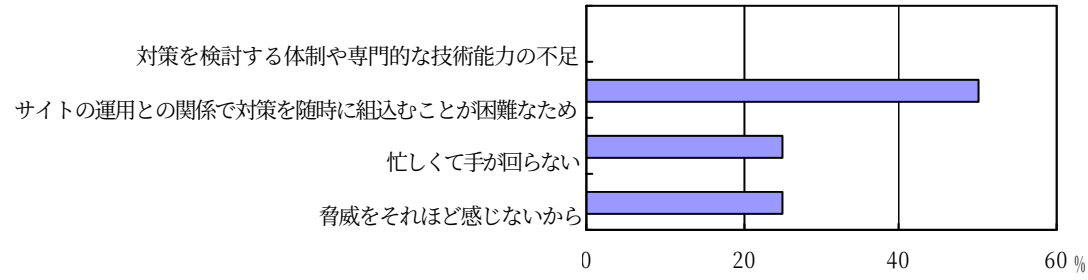
【大規模】



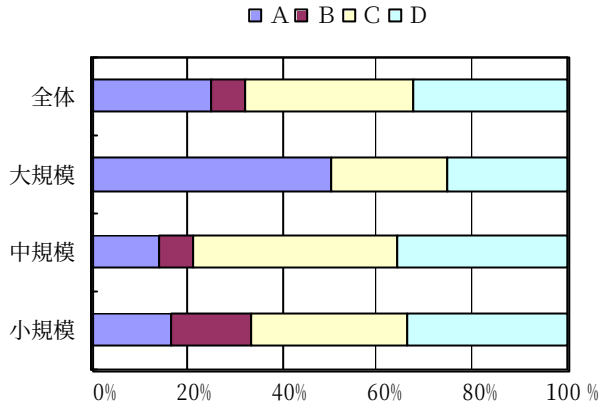
【中規模】



【小規模】

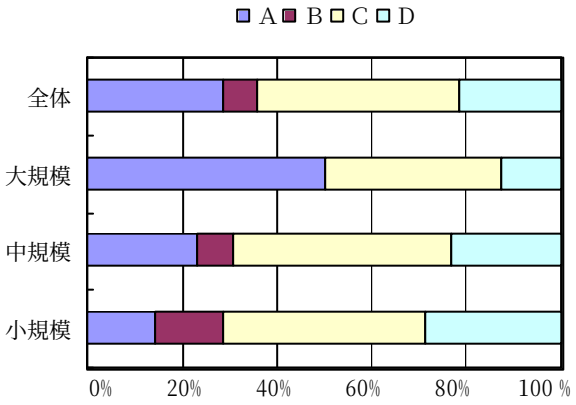


(2) セキュリティホール対策実施の慎重度



Ⓐ 手順が定められており、この手順に沿って厳格な管理下で行っている
Ⓑ 手順は定められているが必ずしも守られておらず、危険がないことはない
Ⓒ 手順は確立していないが、習 慣的に必要な処置はおおむねとっている
Ⓓ 担当者の注意に依存している

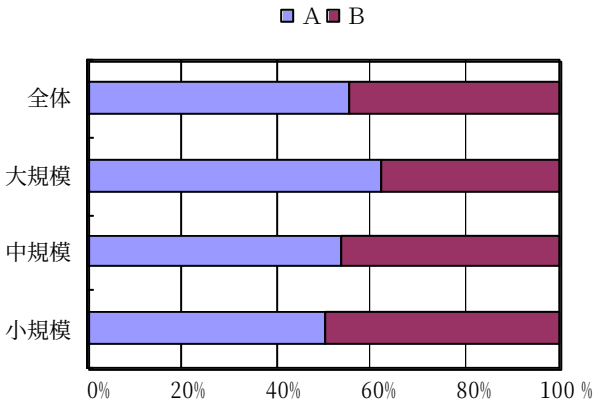
(3) 未対策セキュリティホールの把握



Ⓐ おおむね正確な把握、管理が行われており、特に危険性の高い未対策セキュ リティホールについては完全に把握している
（B）システム上の未対策セキュリティホールの把握はルール化されているが、励行されてなく、その情報は正確とは言えない
Ⓒ 担当者レベルである程度は把握している
Ⓓ 特に把握、管理は行われていない

(4) セキュリティホールをついた攻撃の監視

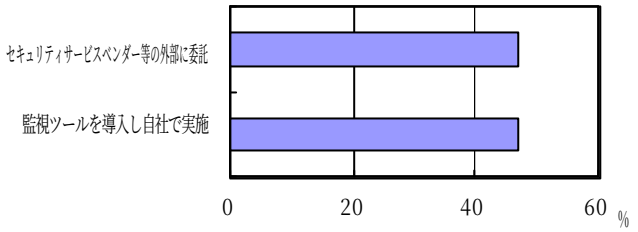
① 監視の実施状況



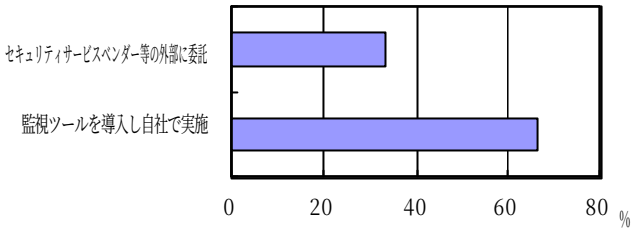
Ⓐ 攻撃の監視を常に行っている
Ⓑ 実施していない

② 監視の実施形態

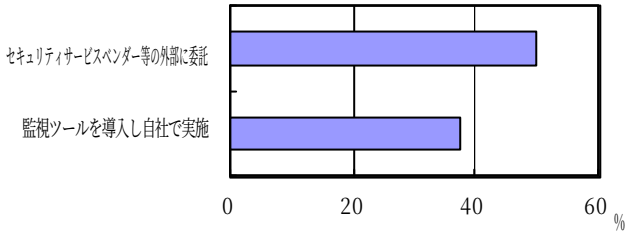
【全体】



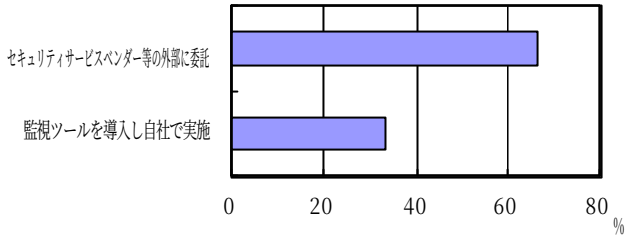
【大規模】



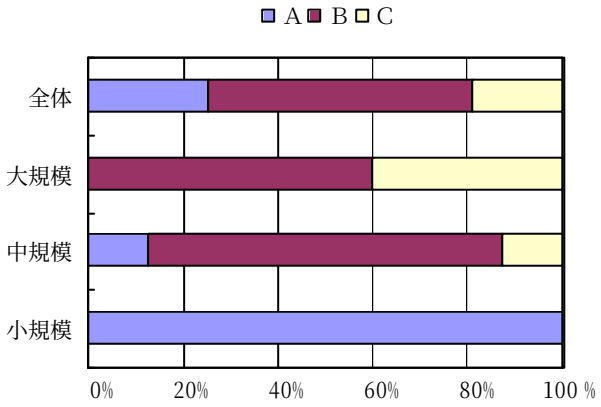
【中規模】



【小規模】



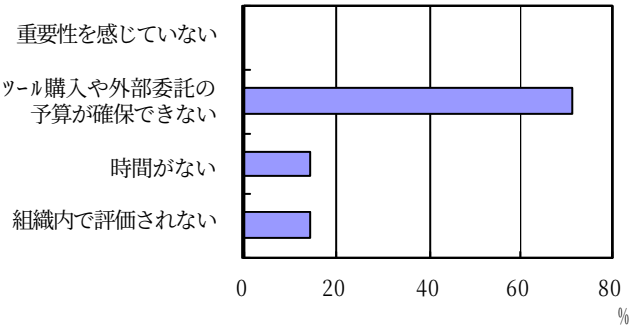
③ 監視の対象



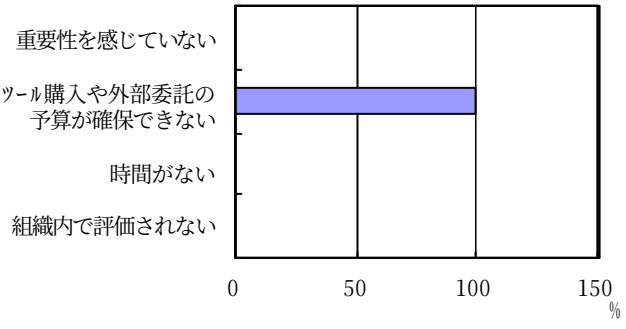
(A) すべての機器を対象
(B) 外部からアクセス可能な機器のみを対象
(C) 特定の機器のみ

④ 監視を行っていない理由

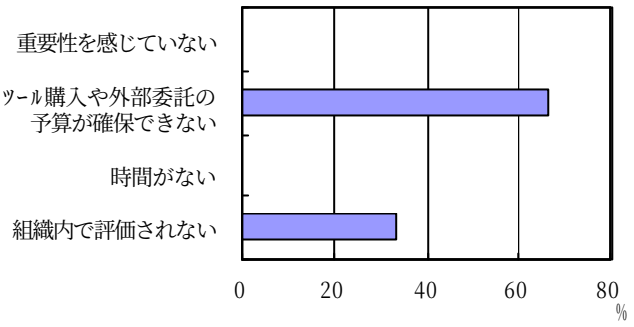
【全体】



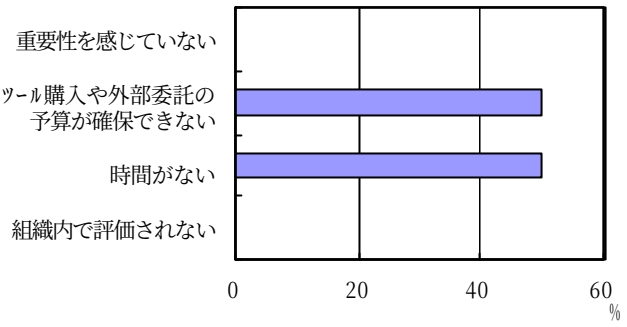
【大規模】



【中規模】

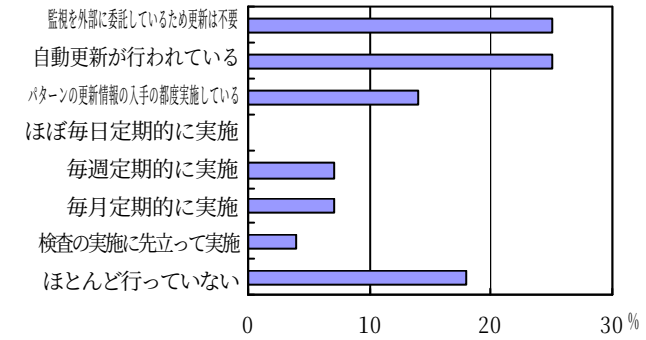


【小規模】

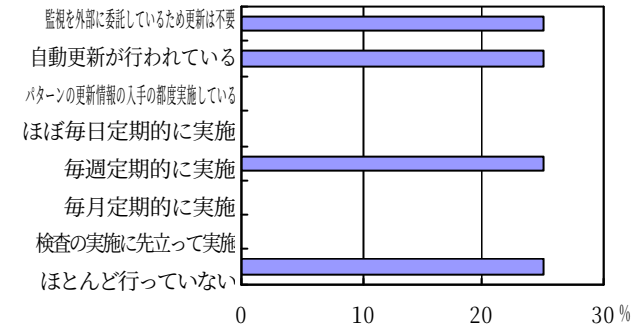


(5) セキュリティホール攻撃監視用パターンファイルのメンテナンス状況

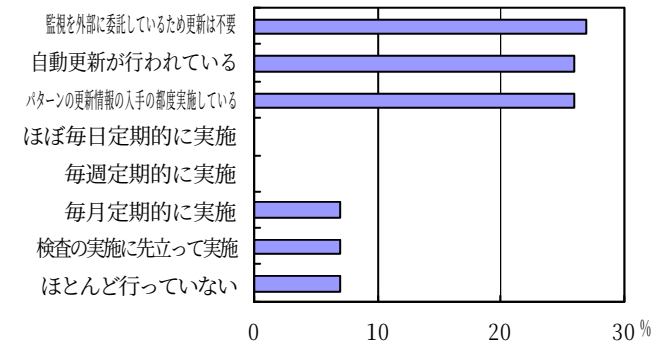
【全体】



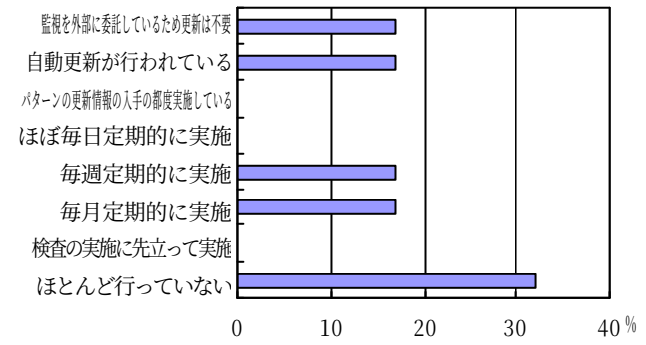
【大規模】



【中規模】



【小規模】



6　ウイルス対策

本章では、EC サイトのシステムに対するウイルスやトロイの木馬の侵入を阻止するための対策および侵入による被害を限定的なものにするための対策への取組みについて分析を行う。

分析項目については、以下の通り。

- ウイルスに対する取組方針の確立
- ウイルスに関する最新情報の収集
- ネットワーク経由でのウイルス侵入の阻止
- ソフトウェアインストールにともなう侵入の阻止
- 持込まれた PC からのウイルス侵入の阻止
- システムに対するウイルス検査の実施

6.1　“ウイルス対策”全体を通しての傾向

すべてのサイトが何らかの形でウイルス対策ソフトを導入しており、ウイルスの脅威に対する認識と対策の実施が他のセキュリティ対策に比べて進んでいる。

クライアント全てにウイルス対策ソフトを導入しているサイトは約半数であり、ゲートウェイなどによる対策をしているサイトが見られる反面、PC の持込みやソフトウェアインストール時におけるウイルス検査が正しく行われているサイトは少なく、ゲートウェイだけでは対応できないウイルスの流行が懸念される。

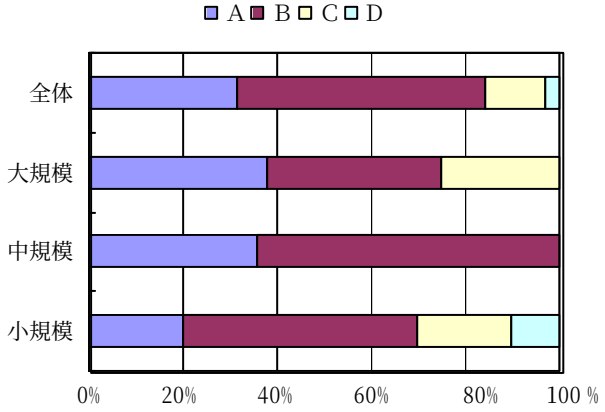
6.2　設問ごとの分析結果

6.2.1　ウイルスに対する取組方針の確立

分析結果から見た傾向は、以下の通り。

- ウイルス対策への取組みに対する認識は非常に高い。

(1) ウイルスに対する基本姿勢



（A）ウイルスの侵入を阻止するための手段を尽くすとともに、システムの管理を行う者だけでなく、システムに触れる者全員による取組みを行う
（B）ウイルス対策ソフトの導入によるウイルスの侵入阻止を行う
（C）ネットワークサービスベンダーのウイルスチェックサービスを利用することにより、サイトでの対策は行わない
（D）特に対策は行わない

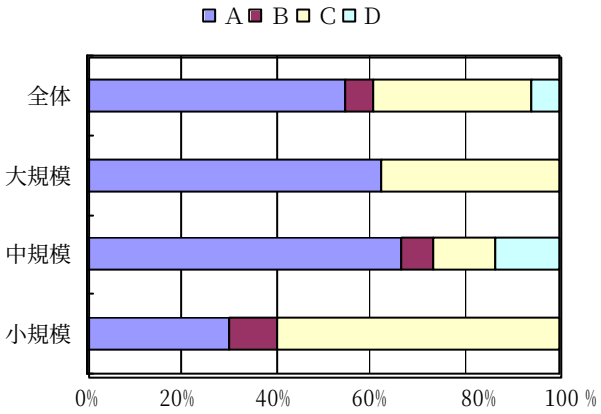
6.2.2　ウイルスに関する最新情報の収集

分析結果から見た傾向は、以下の通り。

- 情報の収集と分析に関してはサイト規模との相関性は薄いように思われる。これはウイルス対策ソフトによる自動パラメータ更新機能への依存が高いためではないかと推測される。

(1) ウイルス情報の収集

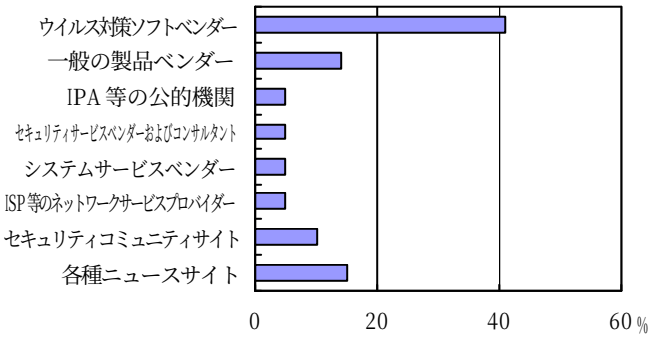
①　ウイルスについての情報の収集状況



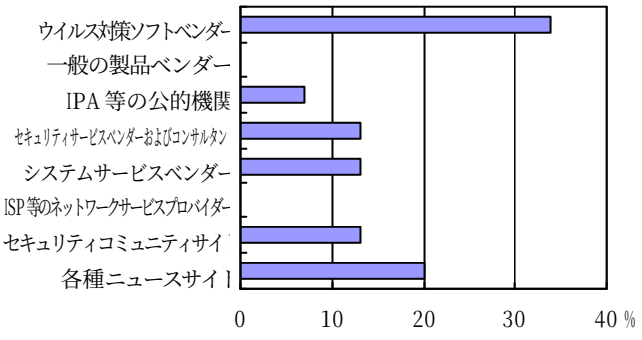
（A）ウイルスに関する情報の入手についてのルールや責任者も決められていて、定期的に情報を入手している
（B）ウイルスに関する情報の入手についてのルールや責任者も決められているが、励行されてはいない
(C) 特に話題となったウイルスについては行われることもあるが、日常は担当者の意識に依存
(D) 特に意識して情報の収集は行っていない

②　情報の収集元

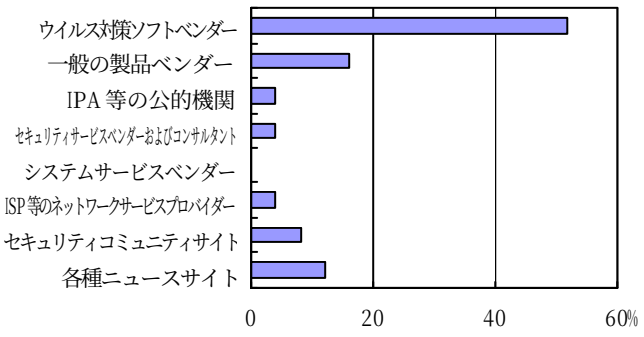
【全体】



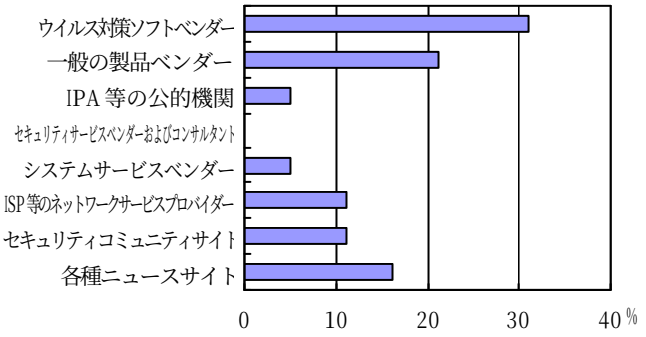
【大規模】



【中規模】

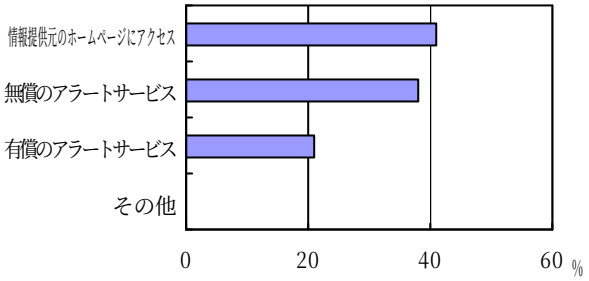


【小規模】

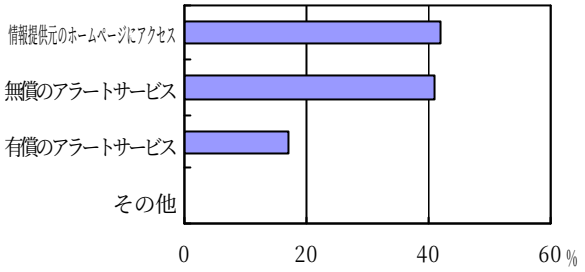


③　情報の収集ルート

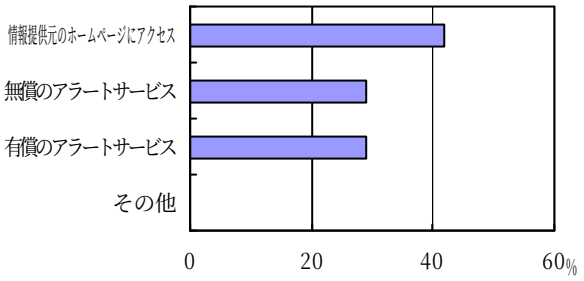
【全体】



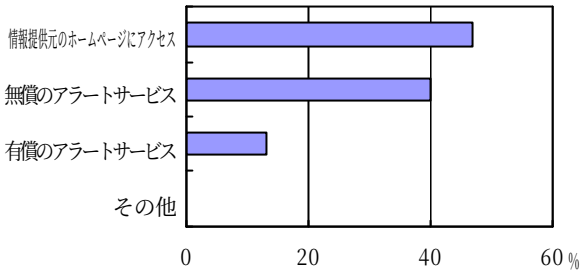
【大規模】



【中規模】

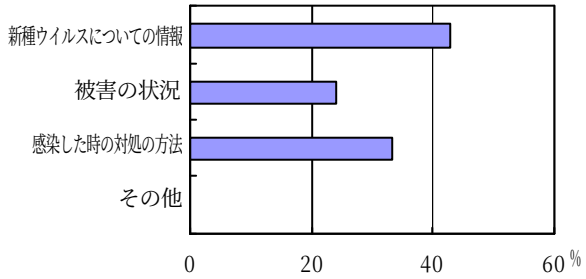


【小規模】

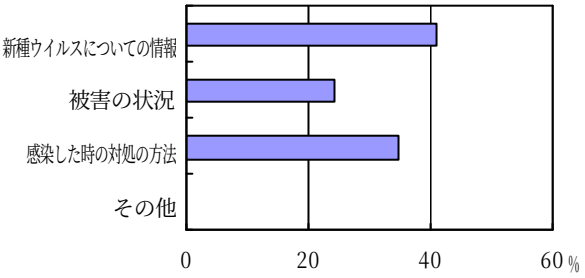


④　収集している情報

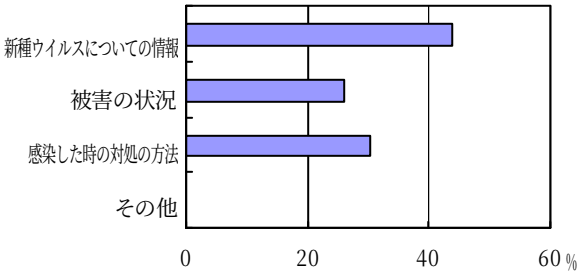
【全体】



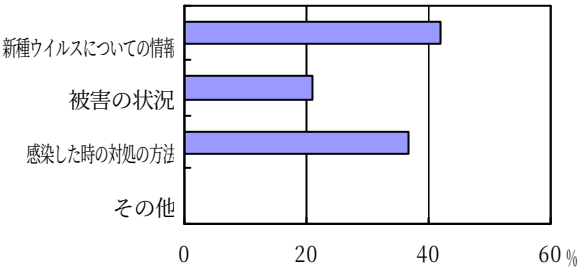
【大規模】



【中規模】

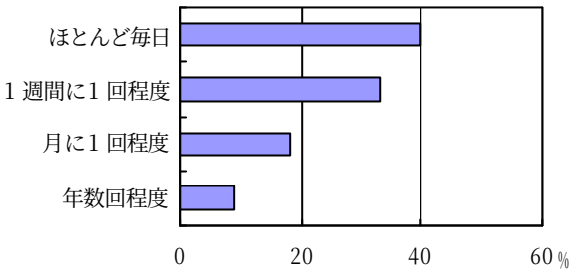


【小規模】

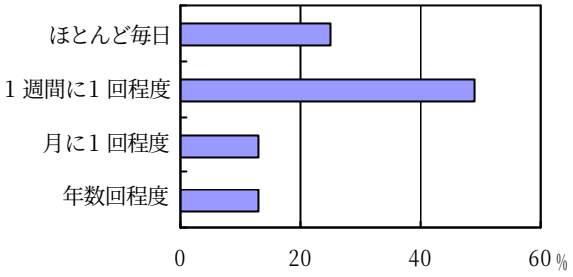


⑤ 収集の頻度

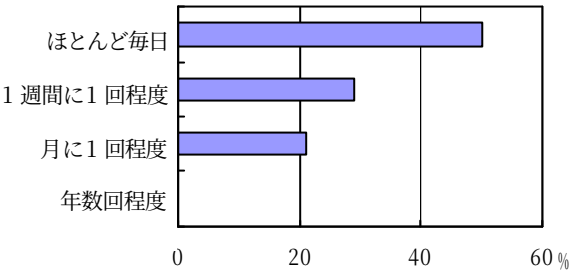
【全体】



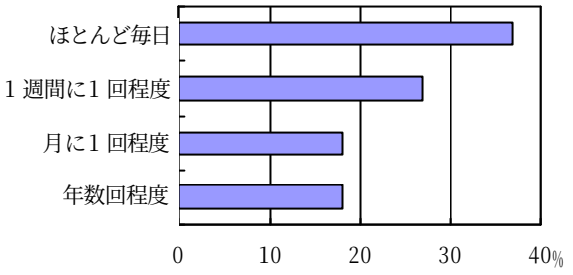
【大規模】



【中規模】

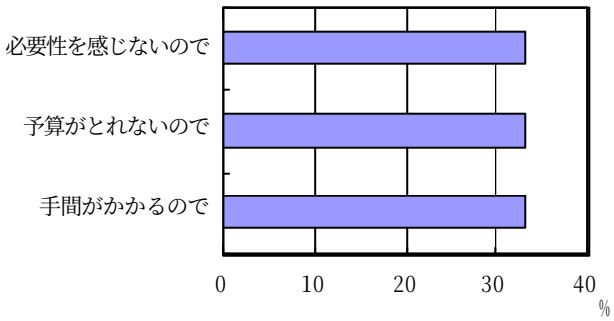


【小規模】

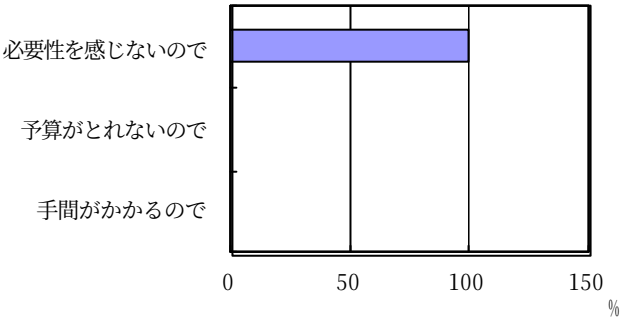


⑥ 収集していない場合、その理由

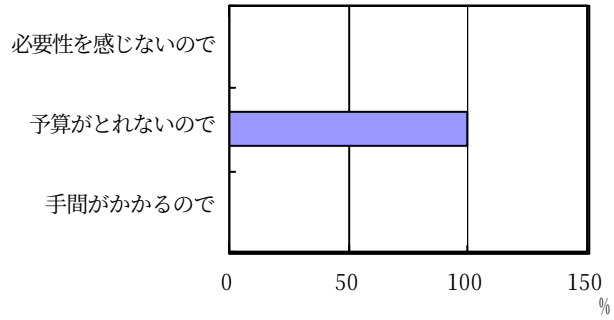
【全体】



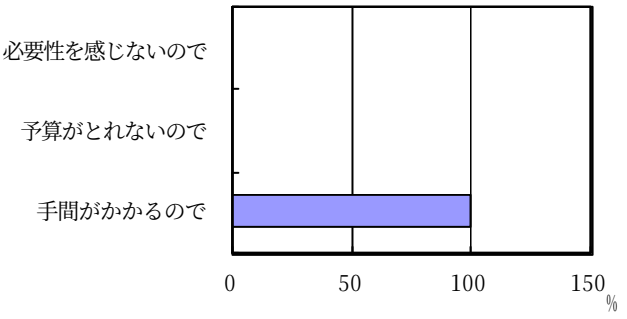
【大規模】



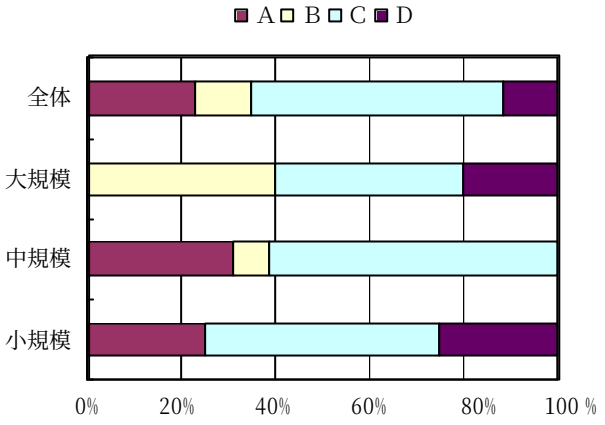
【中規模】



【小規模】



(2) 収集されたウイルスの情報の活用状況



Ⓐ 収集した情報のすべてについて臨時ウイルス検査の実施等の対策の要否やその緊急度についての評価、判断は組織的に行われ、対策に適切に反映されている
Ⓑ 収集した情報に対する対策の要否やその緊急度についての評価、判断は組織的に行われることになっているが徹底さに欠けており、情報収集は十分に活かされているとは言えない
Ⓒ 担当者レベルで一通りの分析、評価は行われているが、管理はされてなく担当者任せとなっている
Ⓓ 収集はしているが、分析や対策への反映等はほとんど行われていない

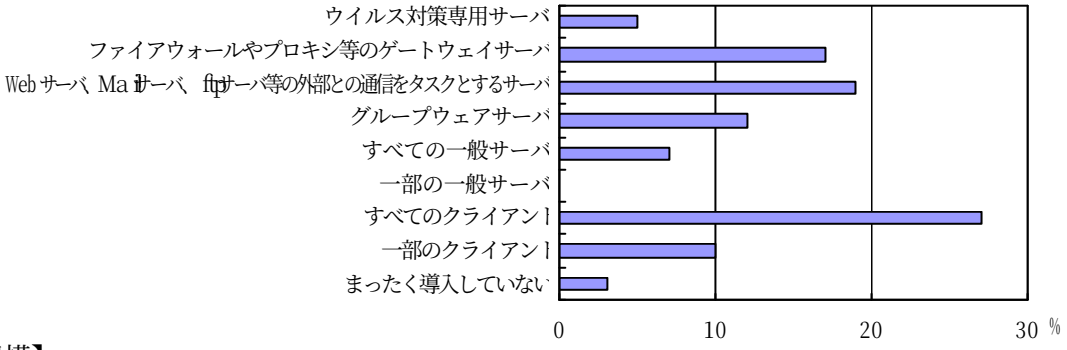
6.2.3 ネットワーク経由でのウイルス侵入の阻止

分析結果から見た傾向は、以下の通り。

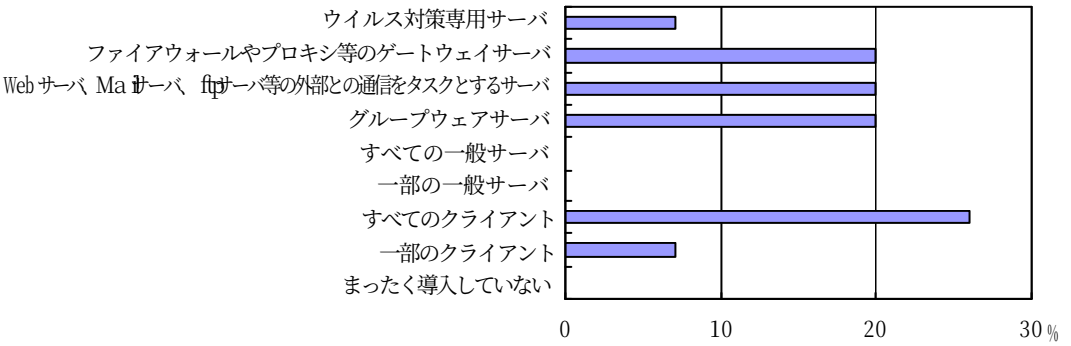
- 全クライアントへ対策ソフトを導入しているのは半数程度に止まり、ゲートウェイにおける対策への依存性がうかがわれる。

(1) ウイルス対策ソフトを搭載しているマシンの配置

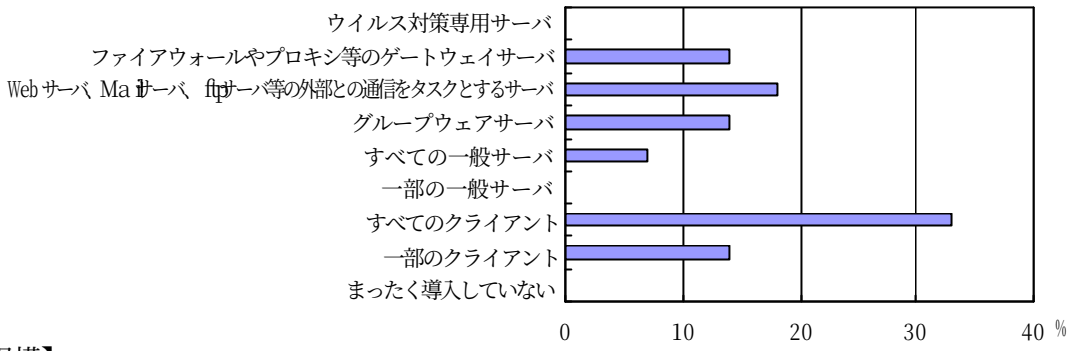
【全体】



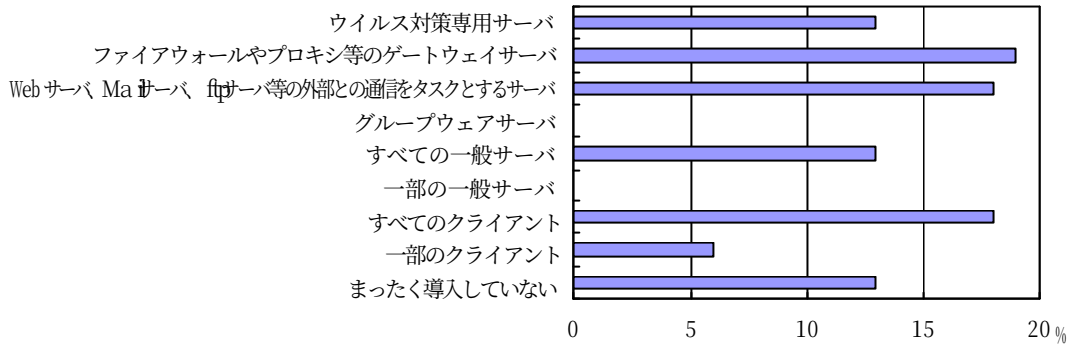
【大規模】



【中規模】

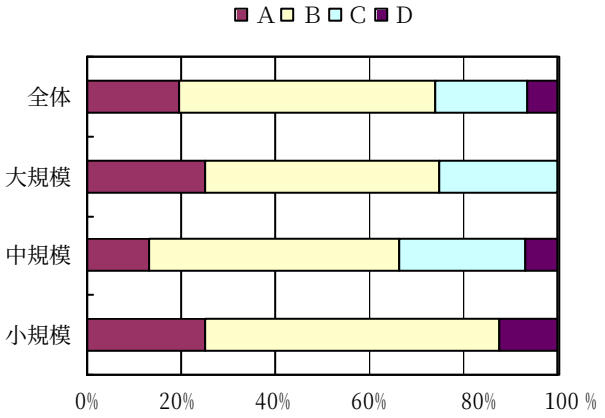


【小規模】



(2) ウイルス対策ソフトの配置に対する評価

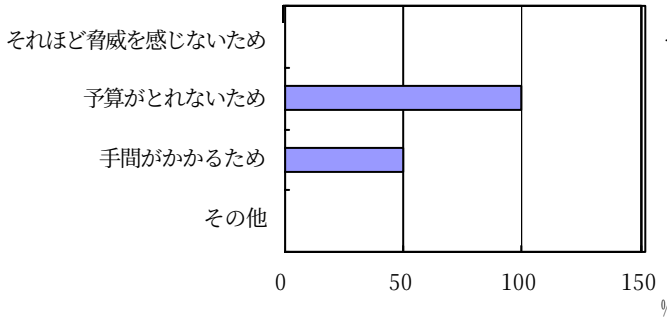
① 評価



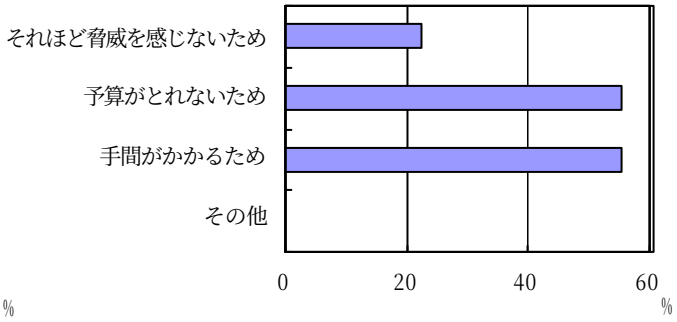
(A) サイトの実態と要求するセキュリティレベルから見て十分と考えている
(B) サイトの運営実態から見ておおむね十分な配置と考えている
(C) まだ最低限のレベルであり、強化が必要と考えている
(D) 適切とは言えない

② 不十分と判断している場合、そのような配置になっている理由

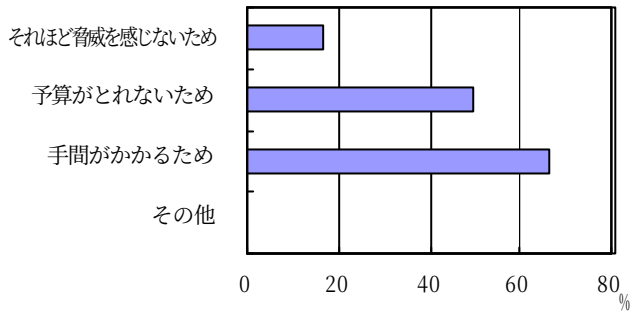
【全体】



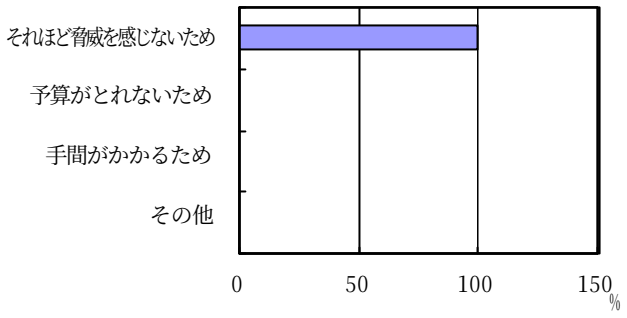
【大規模】



【中規模】

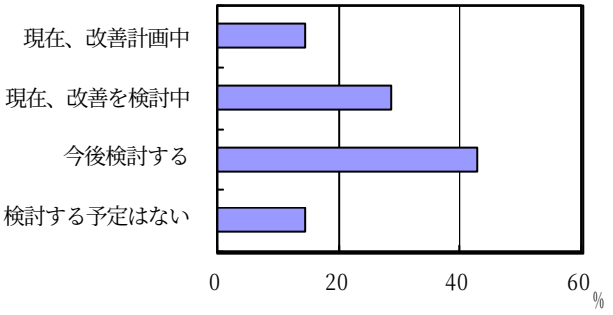


【小規模】

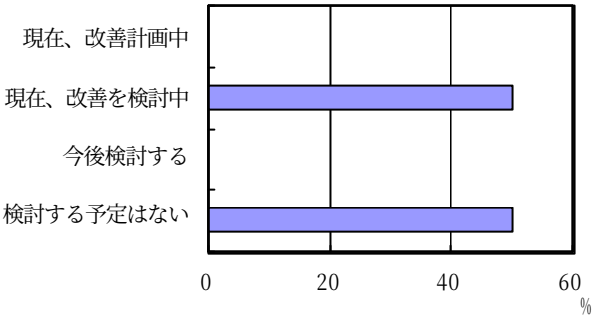


③　不十分と判断している場合の今後の対応

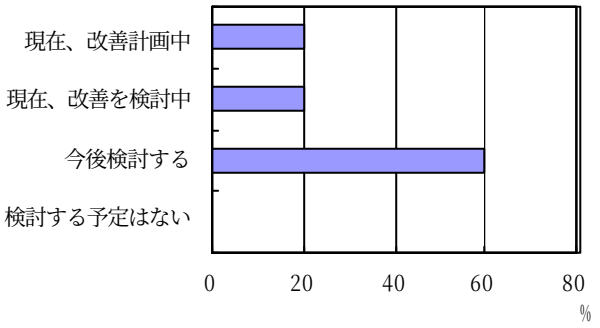
【全体】



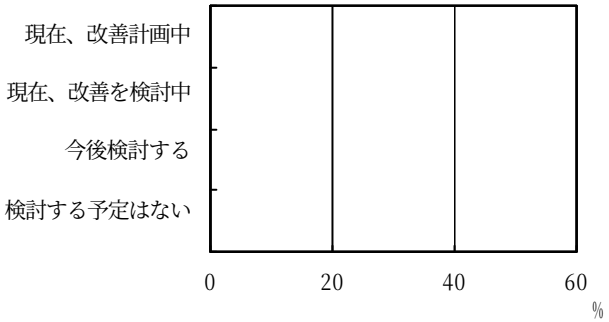
【大規模】



【中規模】



【小規模】



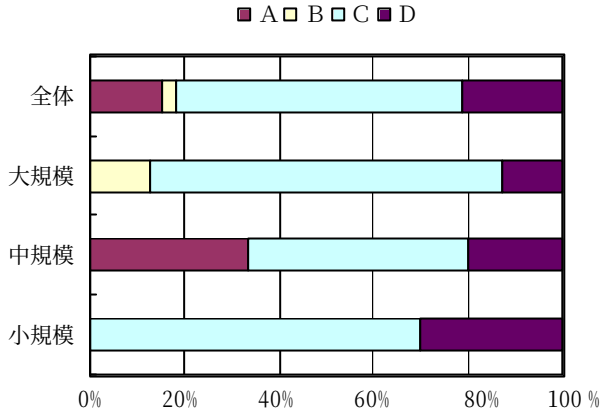
6.2.4　ソフトウェアインストールにともなう侵入の阻止

分析結果から見た傾向は、以下の通り。

- ソフトウェアのインストール時にウイルス検査を行っているサイトはかなり少ない。
- その理由として、素性のはっきりしないソフトは使わないという方針を持っていることがあげられている。

(1) インストールするソフトウェアに対するウイルス検査の実施状況

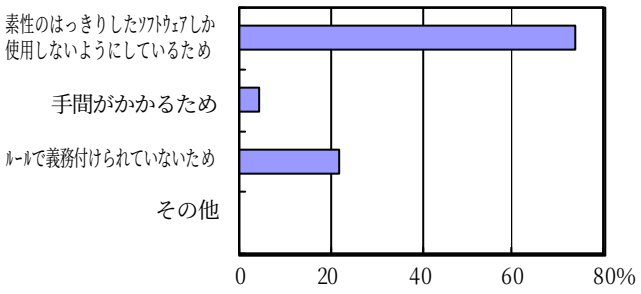
① 評価



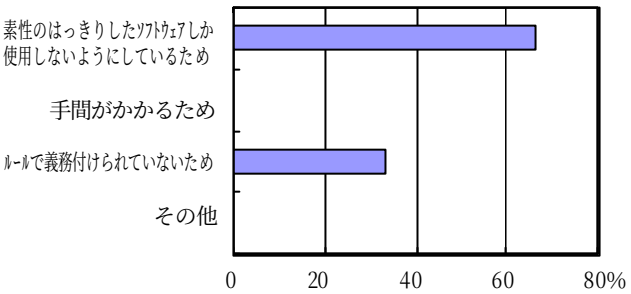
(A) ルールにもとづいた検査が厳格に行われている
(B) ルールに沿った検査が行われることになっているが、励行されていない
(C) インストールするソフトウェアに対するウイルス検査についてのルールはなく、インストール担当者の判断に委ねられている
(D) ほとんど実行していない

② 不十分と判断している場合、その理由

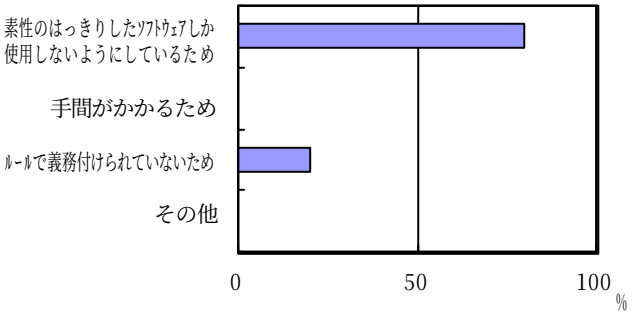
【全体】



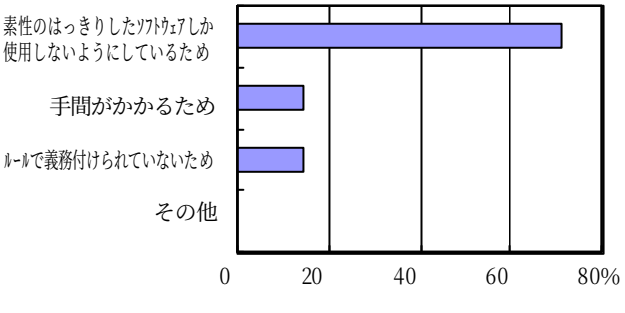
【大規模】



【中規模】



【小規模】



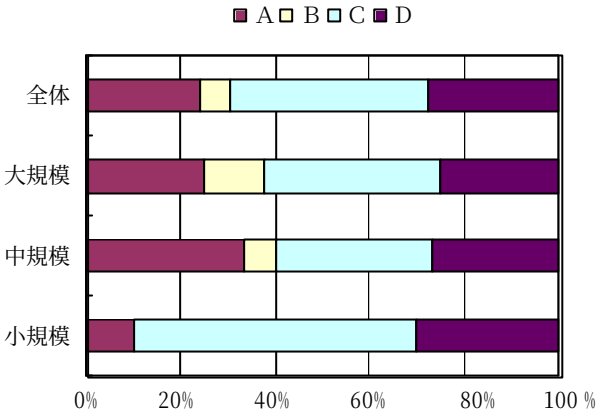
6.2.5 持込まれた PC からのウイルス侵入の阻止

分析結果から見た傾向は、以下の通り。

- 持込まれた PC への対策実施は 30%以下に止まり、ＰＣの持込み によるウイルス感染の媒介が懸念される。

(1) 持込まれた PC に対するウイルス検査の実施状況

① 評価



(A) 外部から持込まれたり外部から持帰ったりした PC に対しては、サイトシステムへの接続に先立ち、ウイルス検査を行うことが義務付けられており、厳格に運用されている

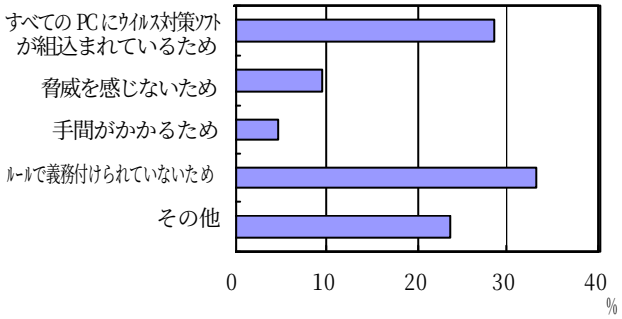
(B) これらの PC に対してサイトシ ステムへの接続に先立ちウイルス検査を行うことが義務付けられているが、厳格には運用されていない

(C) PC の管理者や使用者に対する指導は行われているが、当事者の注意に任されている

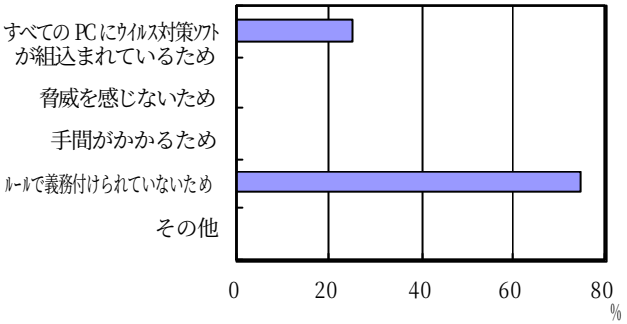
(D) ほとんど行っていない

② 行っていない場合、その理由

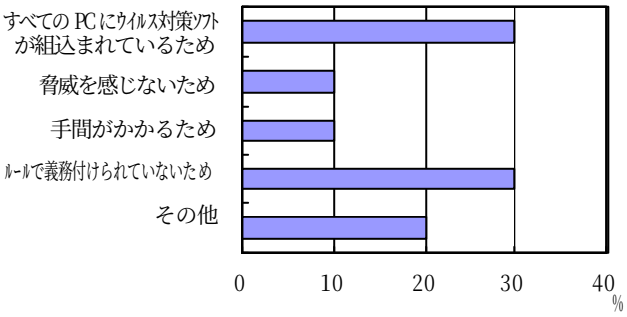
【全体】



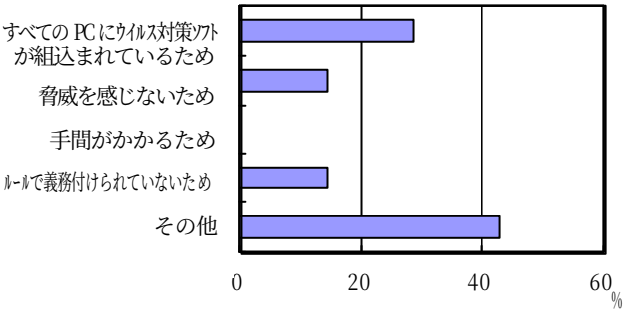
【大規模】



【中規模】



【小規模】



6.2.6 システムに対するウイルス検査の実施

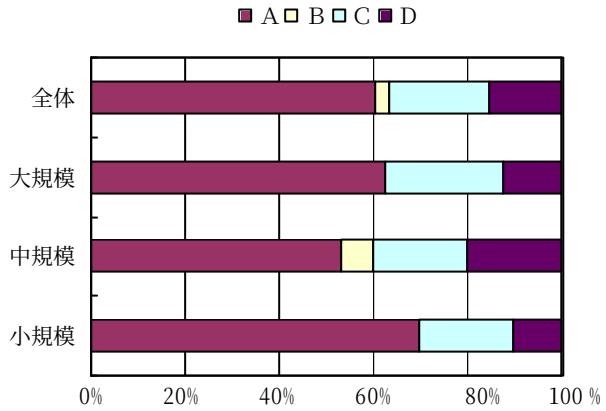
分析結果から見た傾向は、以下の通り。

- 外部との通信に用いられるサーバでは、ある程度ウイルス検査が行われているようだが、クライアントでは、１／５のサイトがほとんどウイルス検査の実施を行っておらず、この点は問題であると言える。

- ウイルス検査の頻度については、かなり高い頻度で行われるようになってきているようにも見えるが、実際のウイルス被害発生状況からすると、もっと頻度を高める必要があるものと思われる。

(1) Web サーバ、Mail サーバ、ftp サーバ等外部との通信に用いられるサーバに対するウイルス検査の実施

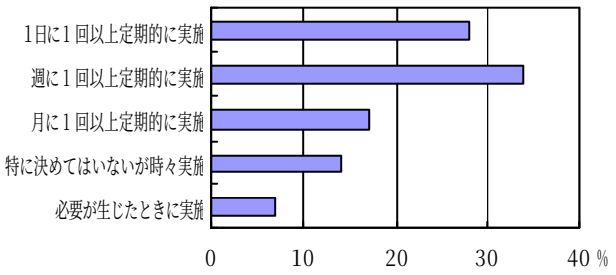
① ウイルス検査の実施方法



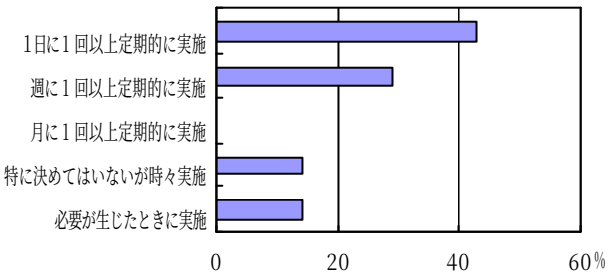
(A) 自動的に行われるようになっている
(B) ルールに沿った検査をシステム運用者の手で励行している
(C) 特にルールは決められておらず、担当者の判断で適宜行っている
(D) ほとんど行っていない

② 検査の頻度

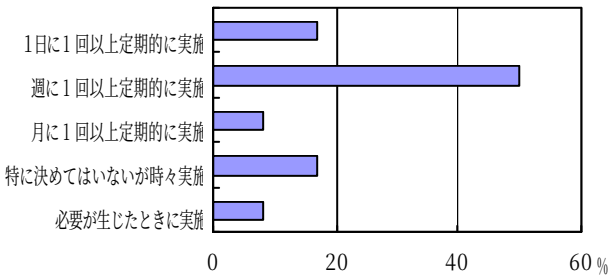
【全体】



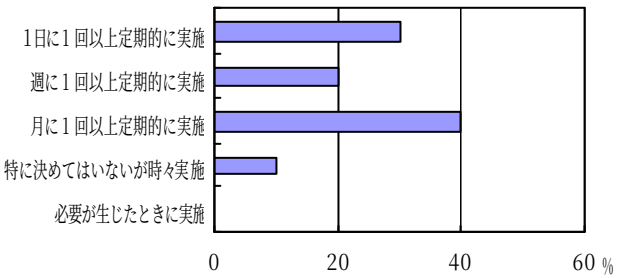
【大規模】



【中規模】

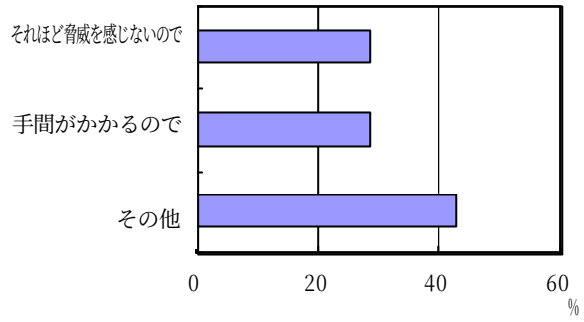


【小規模】

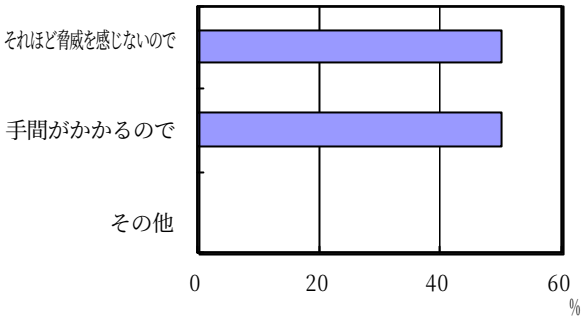


③　実施頻度が低い場合、その理由

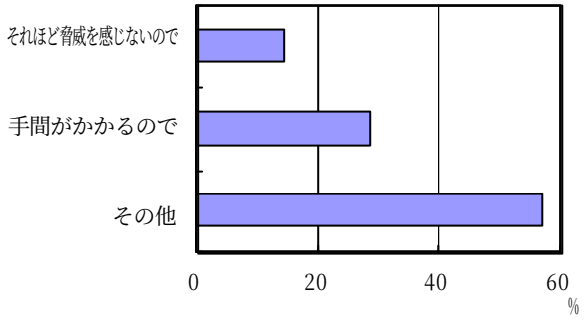
【全体】



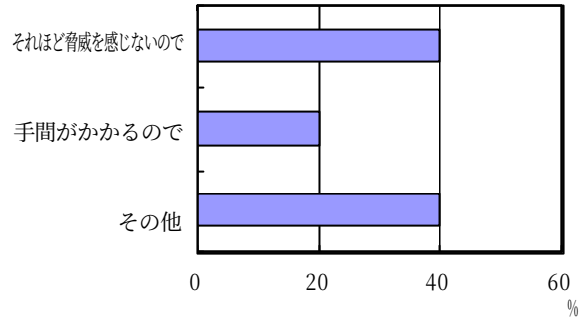
【大規模】



【中規模】

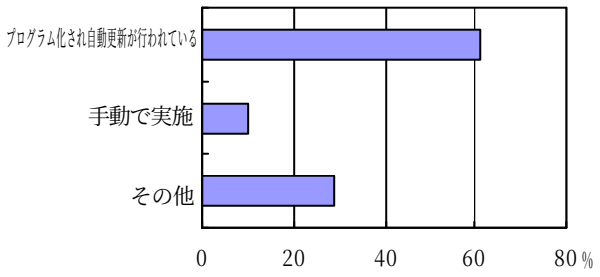


【小規模】

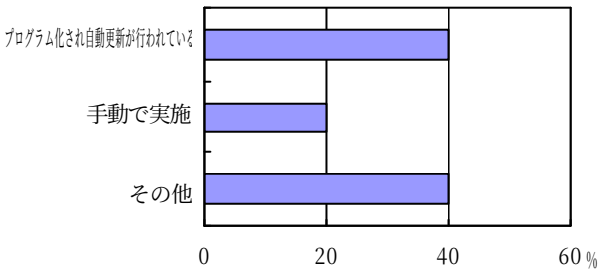


④　検査に用いるパターンファイルの更新方法

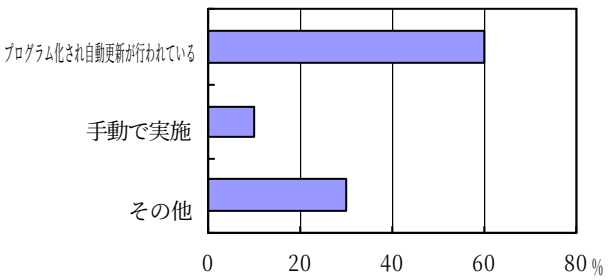
【全体】



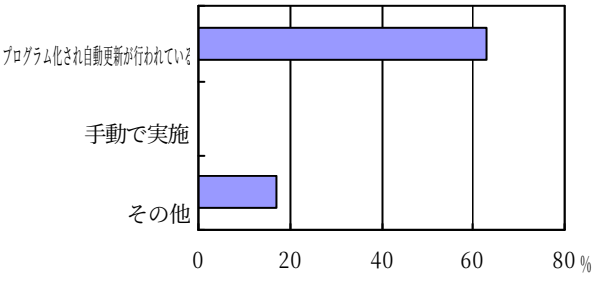
【大規模】



【中規模】

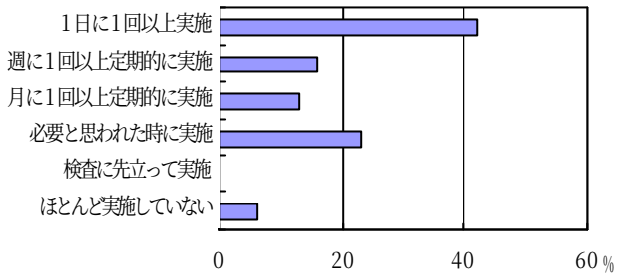


【小規模】

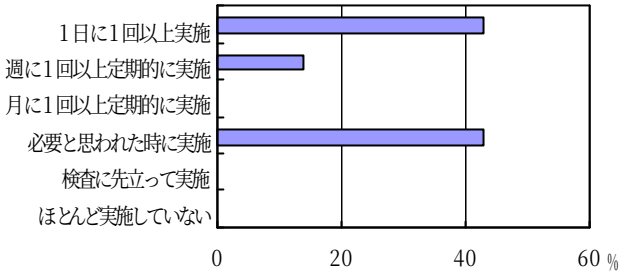


⑤ パターンファイルの更新頻度

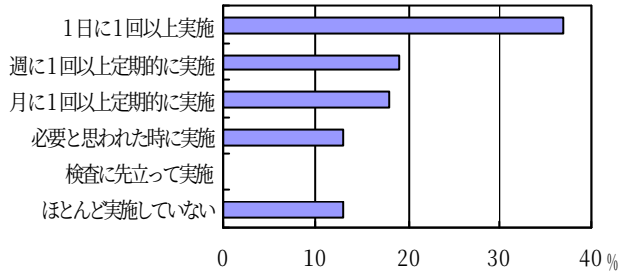
【全体】



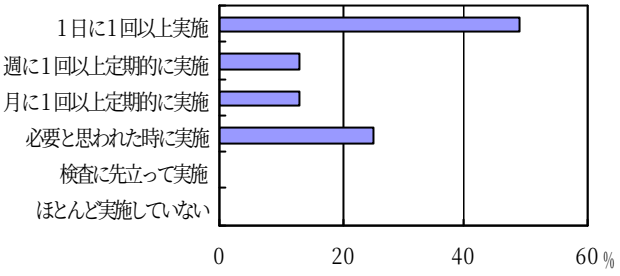
【大規模】



【中規模】

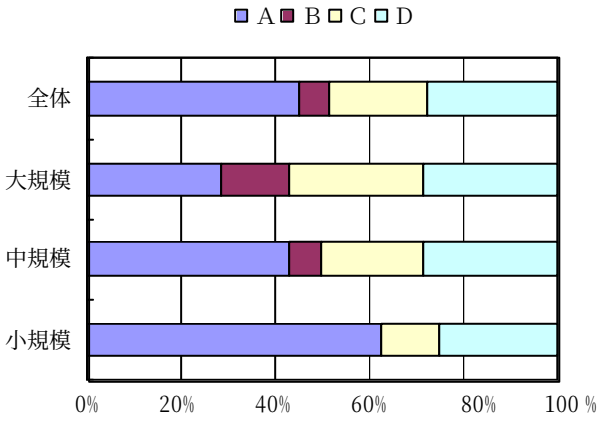


【小規模】



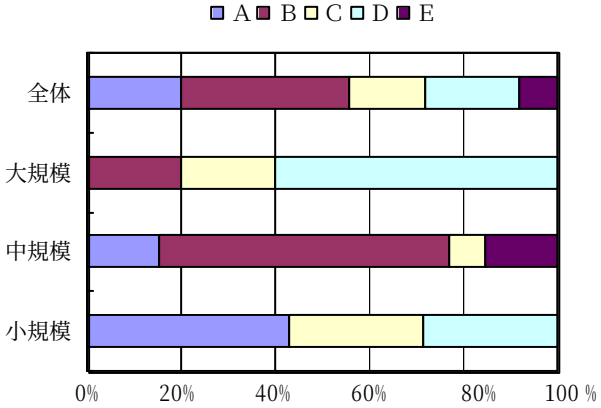
(2) 一般のサーバに対するウイルス検査の実施

① ウイルス検査の実施方法



(A) 自動的に行われるようになっている
(B) ルールに沿った検査をシステム運用者の手で励行している
(C) 特にルールは決められておらず、担 当者の判断で適宜行っている
(D) ほとんど行っていない

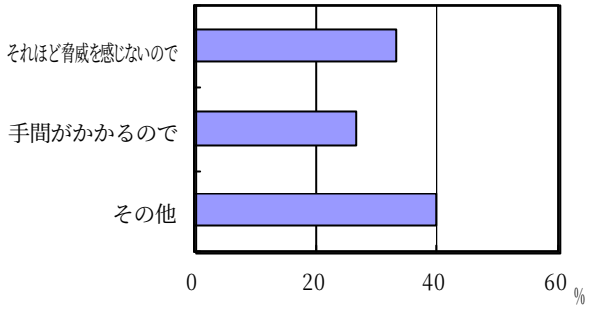
② 検査の頻度



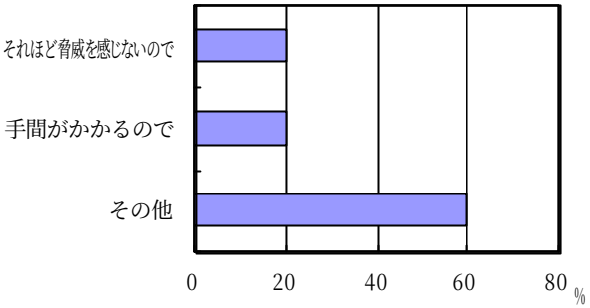
(A)1 日に 1 回以上実施
(B) 週に 1 回以上定期的に実施
(C) 月に 1 回以上定期的に実施
(D) 特には決めていないが必要と思われた時に実施
(E) 検査に先立って実施

③ 実施頻度が低い場合、その理由

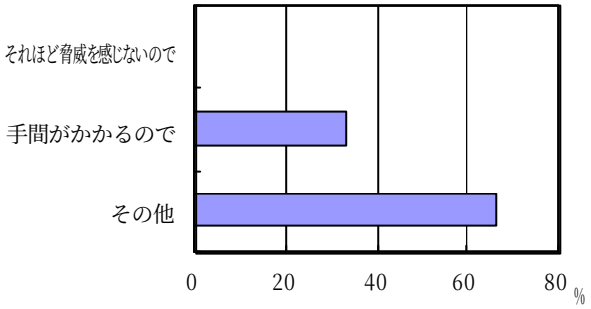
【全体】



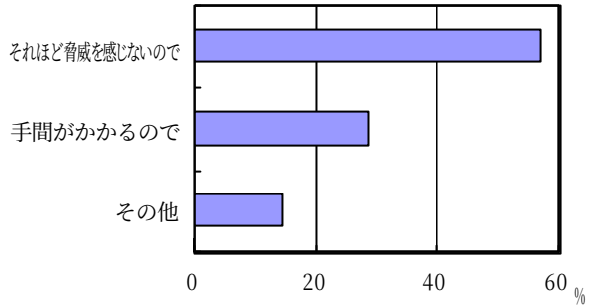
【大規模】



【中規模】

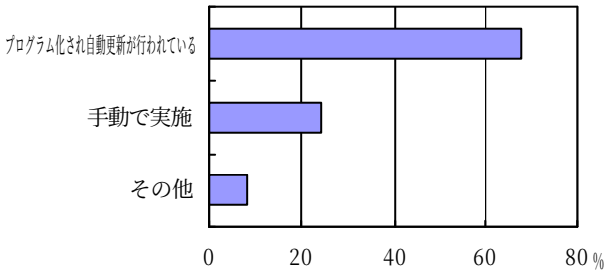


【小規模】

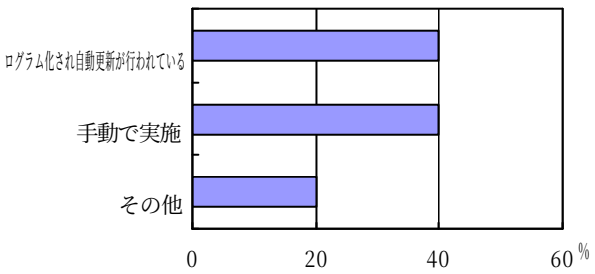


④ 検査に用いるパターンファイルの更新方法

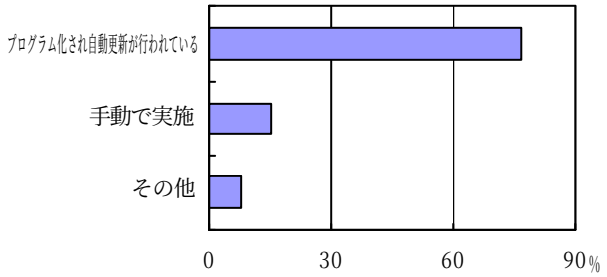
【全体】



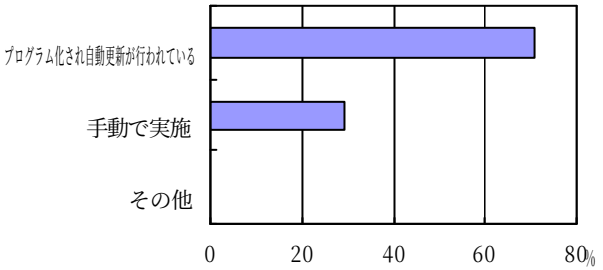
【大規模】



【中規模】

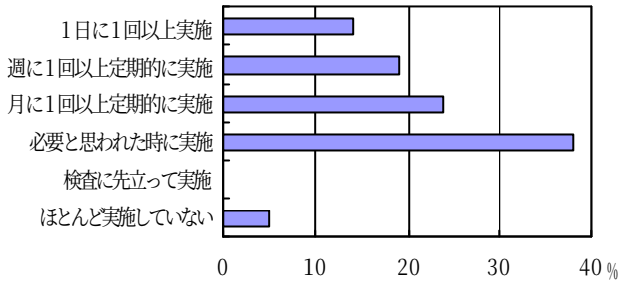


【小規模】

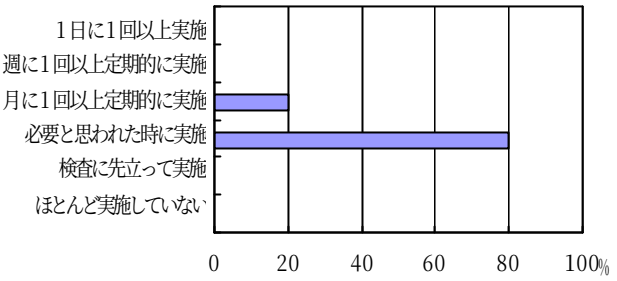


⑤ パターンファイルの更新頻度

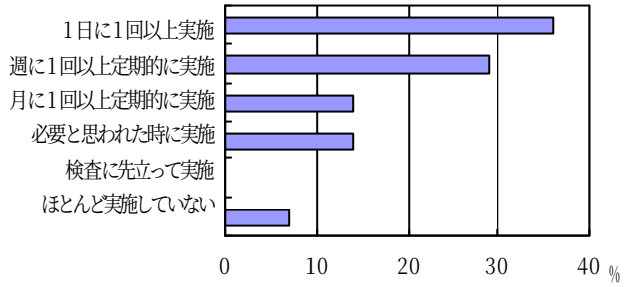
【全体】



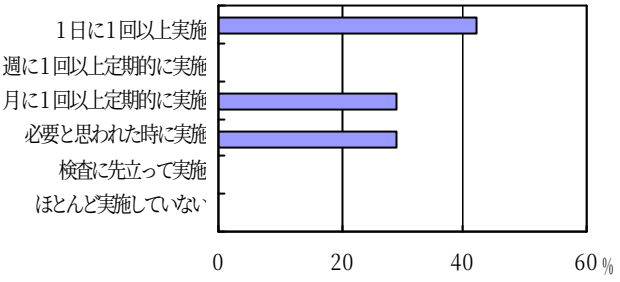
【大規模】



【中規模】

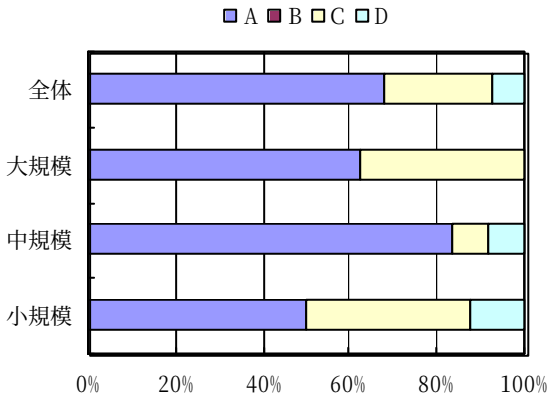


【小規模】



(3) クライアントに対するウイルス検査の実施

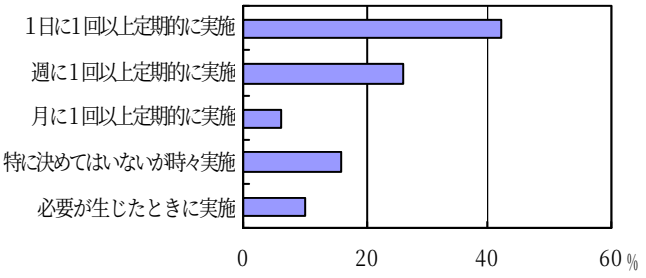
① ウイルス検査の実施方法



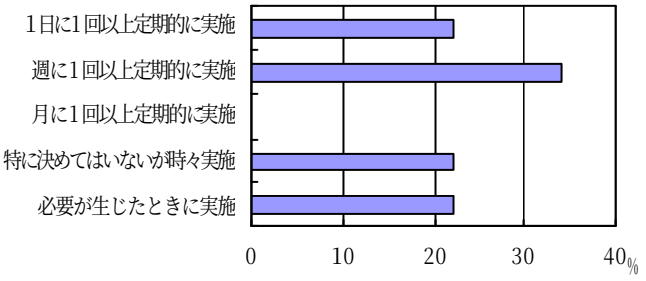
(A) 自動的に行われるようになっている
(B) ルールに沿った検査をシステム運用者の手で励行している
(C) 特にルールは決められておらず、担当者の判断で適宜行っている
(D) ほとんど行っていない

② 検査の頻度

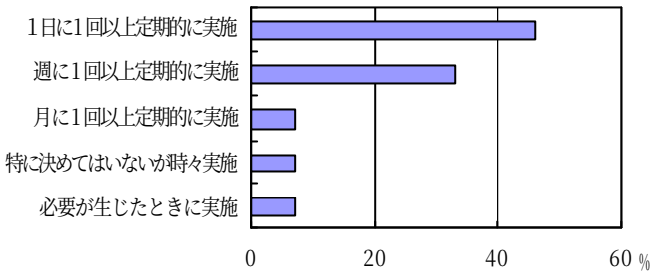
【全体】



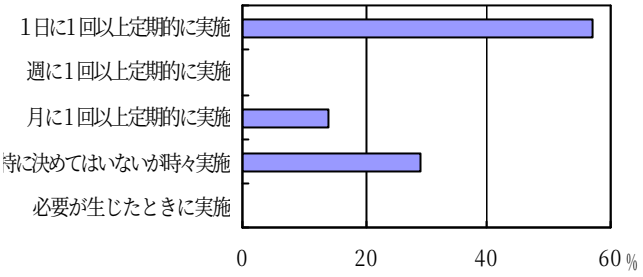
【大規模】



【中規模】

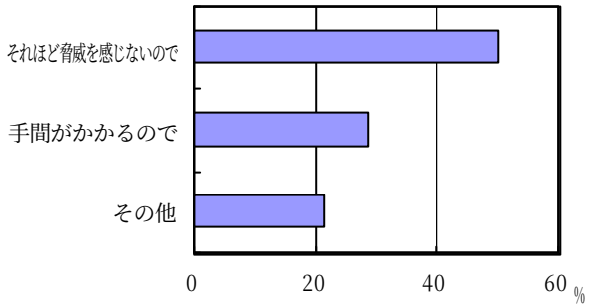


【小規模】

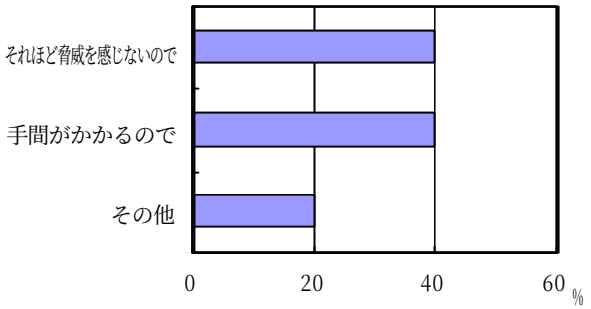


③ 実施頻度が低い場合、その理由

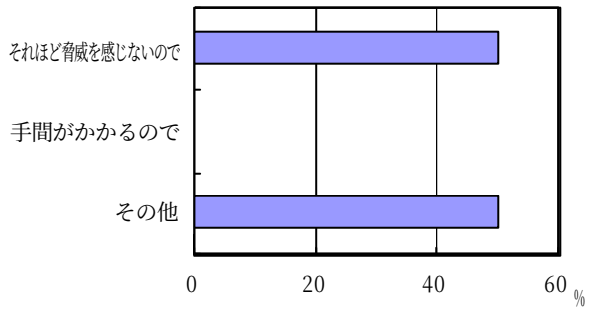
【中規模】



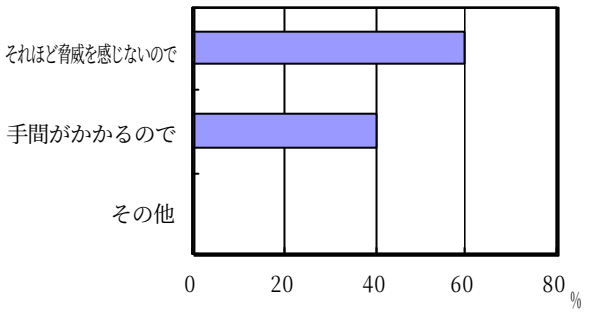
【小規模】



【中規模】

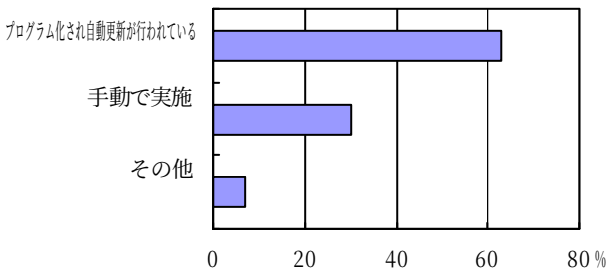


【小規模】

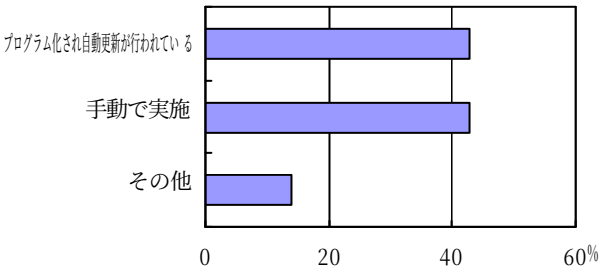


④ 検査に用いるパターンファイルの更新方法

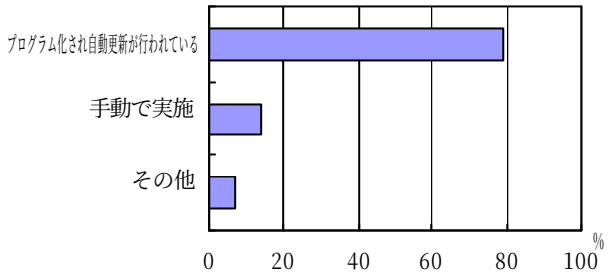
【全体】



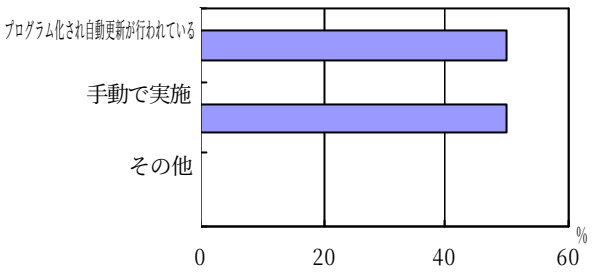
【大規模】



【中規模】

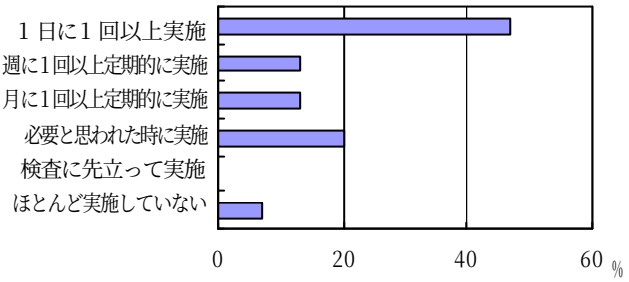


【小規模】

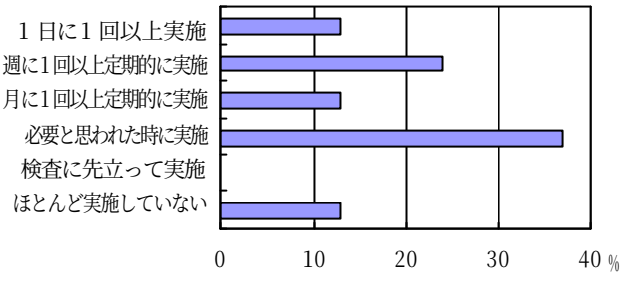


⑤ パターンファイルの更新頻度

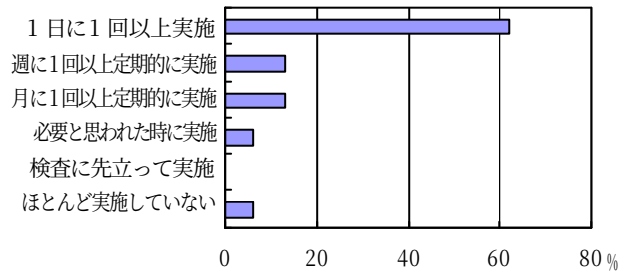
【全体】



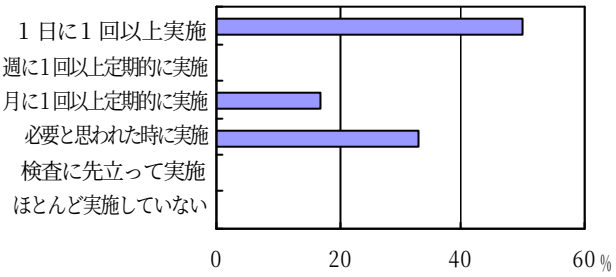
【大規模】



【中規模】



【小規模】



7　セキュリティ管理情報の保護

本章では、EC サイトがセキュリティ管理情報の漏洩や改ざんあるいは破壊に対する対策としての保護管理策への取組状況について分析を行う。

分析項目については、以下の通り。

- 保護対象のセキュリティ管理情報の把握と保護要件の指定
- システム上の保護対象ファイルに対する保護管理の実施
- 業務現場やシステム運用の現場におけるセキュリティ管理情報の取扱い

7.1　“セキュリティ管理情報の保護”全体を通しての傾向

セキュリティ管理情報の把握と保護に関して認識しているサイトはまだ少なく、対策は不十分である。

また、セキュリティ管理情報の保護要件やアクセス権の指定に関する認識、アクセス管理の実施についても不十分である。これらの点がサイトのセキュリティを脆弱にしている要因の一つだと言える。

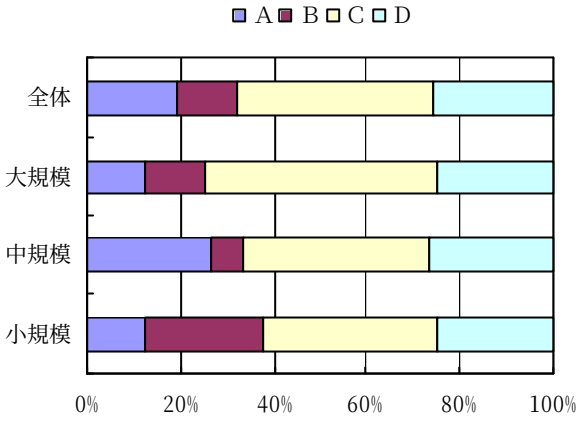
7.2　設問ごとの分析結果

7.2.1　保護対象のセキュリティ管理情報の把握と保護要件の指定

分析結果から見た傾向は、以下の通り。

- セキュリティ管理情報の把握と保護の指定を実施しているサイトは 3／4 程度あり、一応、セキュリティ管理情報に関し意識していることがうかがえる。ただし、組織的にセキュリティ管理情報の把握と保護の指定を行っているサイトは 1／3 程度であり、サイトの規模には依存していない。
- セキュリティ管理情報の保護要件の指定は全体的に見ると 2／3 程度のサイトで実施している。組織的にセキュリティ管理情報の保護要件の指定を実施しているサイトは半分以下となっている。小規模サイトでは組織的にセキュリティ管理情報の保護要件の指定を実施しているのは 1／3 以下となっており、ほとんど担当者まかせとなっている。
- アクセス権の指定についてはセキュリティ管理情報の保護要件の指定と同じ傾向を示している。全体的の 4／5 程度のサイトでアクセス権の指定を実施している。しかし、組織的にアクセス権の指定を実施しているサイトは半分以下となっている。

(1) セキュリティ管理情報の把握と保護の指定状況



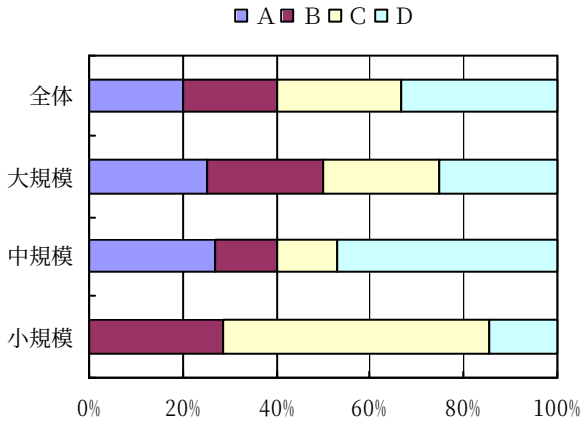
（A）セキュリティ管理情報の把握やそれぞれに求められる保護についての指定は組織的にレビューされている。また、その見直しも適宜行われていて、セキュリティ管理情報の把握とそれぞれに対する保護についての指定の妥当性は常に維持されている

（B）セキュリティ管理情報の把握やそれぞれに求められる保護についての指定は組織的にレビューされることになっているが、レビューや見直しは厳格であると言えず、セキュリティ管理情報の把握とそれぞれに対する保護についての指定の一部に妥当性を欠くところもありうる

(C) 担当者レベルでのセキュリティ管理情報の把握とそれぞれに対する保護についての指定は行われているが、組織的なレビューや管理は行われていない

（D）セキュリティ管理情報の保護は担当者に任されており、セキュリティ管理情報の把握やその保護についての指定等は特に行われていない

(2) セキュリティ管理情報の保護要件の指定状況



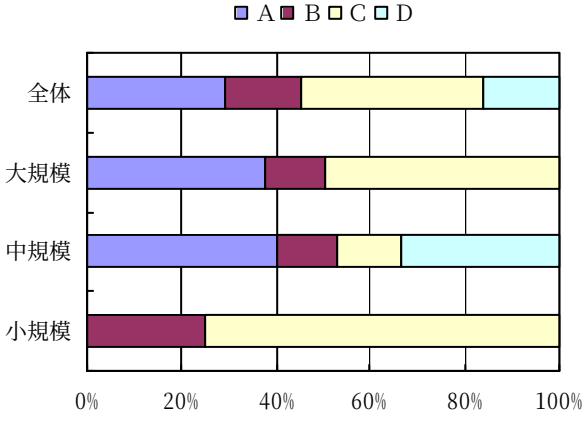
（A）セキュリティ管理情報に対する保護要件の指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持され、ドキュメントも整備されている

（B）セキュリティ管理情報に対する保護要件の指定は、決められた手順に沿って行われることになっており、ドキュメントも整備されているが、組織的な検討やレビューおよび見直しは厳格ではなく、指定の一部に妥当性を欠いていることもありうる

(C) 管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメントもあまり整備されていない

(D) 担当者任せにしており、特に管理は行っていない

(3) アクセス権限保有者の指定と付与するアクセス権の指定



(A) これらの指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持され、ドキュメントも整備されている

(B) これらの指定は、決められた手順に沿って行われることになっており、ドキュメントも整備されているが、組織的な検討やレビューおよび見直しは厳格ではなく、指定の一部に妥当性を欠いていることもありうる

(C) 管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメントもあまり整備されていない

(D) 担当者任せにしており、特に管理は行っていない

7.2.2　システム上の保護対象ファイルに対する保護管理の実施

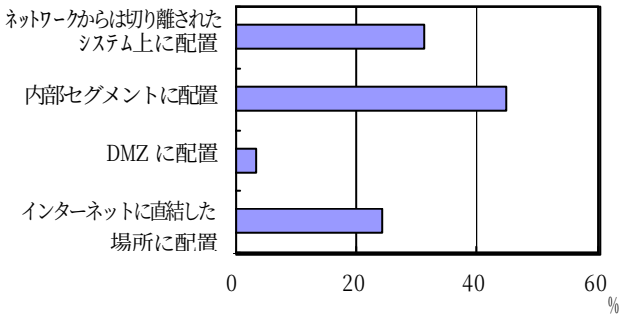
分析結果から見た傾向は、以下の通り。

- 保護対象ファイルの配置場所と配置については、3／4 程度のサイトが配置に注意を払っている。
- 保護対象ファイルの格納上の施策としてはディレクトリを分けて格納しているサイトが大部分を占めている。また、暗号化して格納しているサイトは 1／5 以下であった。
- セキュリティ管理情報に対する必要なアクセス制御機能の組込みおよび保護管理は約 3／4 のサイトで実施している。また、組織的に行っているサイトは半分以下となっている。管理されていないサイトも 1／4 程度あり、改善が必要である。
- セキュリティ管理情報に対するアクセス監視は約 2／3 のサイトで実施している。組織的にアクセス監視を行っているサイトは 2／5 程度ある。
- セキュリティ管理情報に対する改ざん検知は約 2／3 のサイトで実施している。必要と判断したときのみ実施するサイトが 1／3 以上となっている。

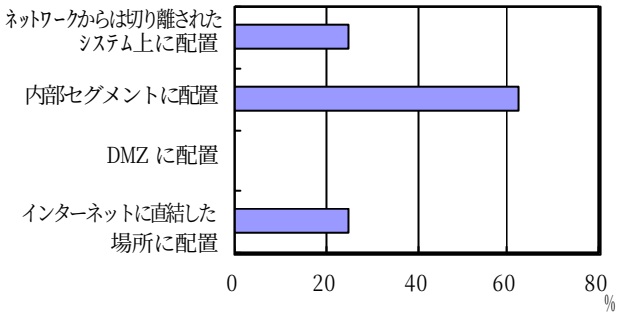
(1) システム構成上でのセキュリティ管理情報の配置の工夫

① 保護対象ファイルの配置場所

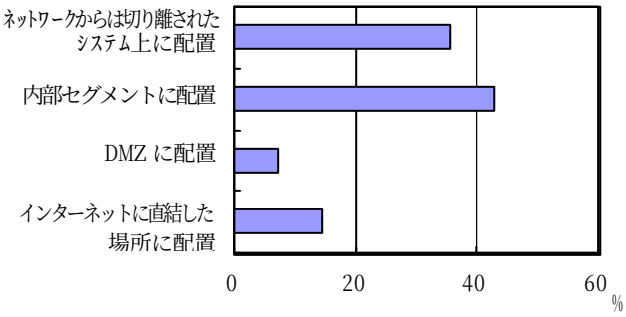
【全体】



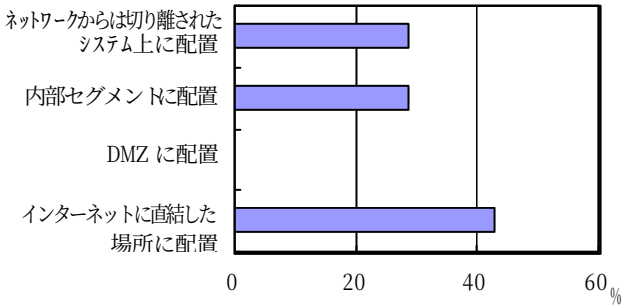
【大規模】



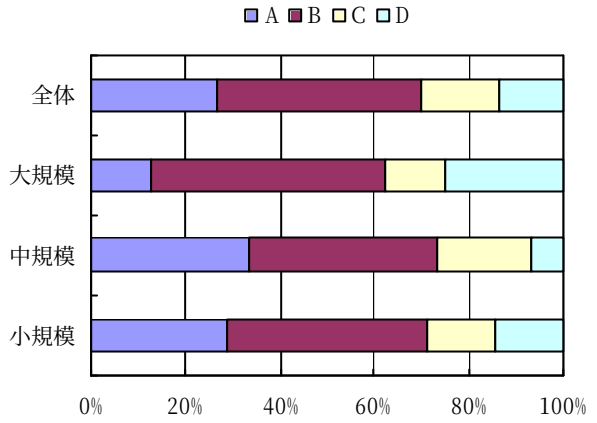
【中規模】



【小規模】



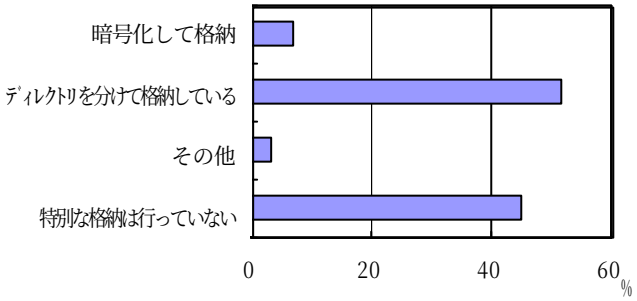
② 保護対象ファイルの配置についての評価



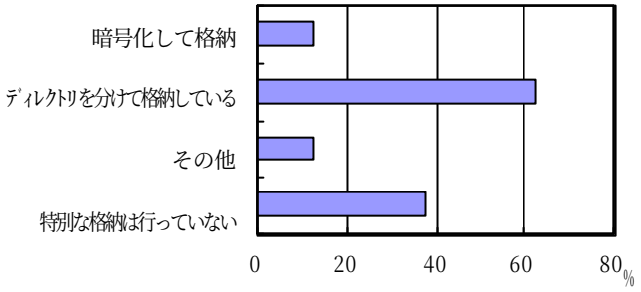
(A) 保護対象ファイルは外部からのアクセスから完全に隔離されている
(B) 外部のアクセスから完全には隔離されていないが、保護要件を満たす安全な場所に配置されている
(C) 一部のファイルは危険な領域にあると認識している
(D) 配置場所については見当が不十分で危険な領域に置かれているものがある

(2) システム上での格納の工夫

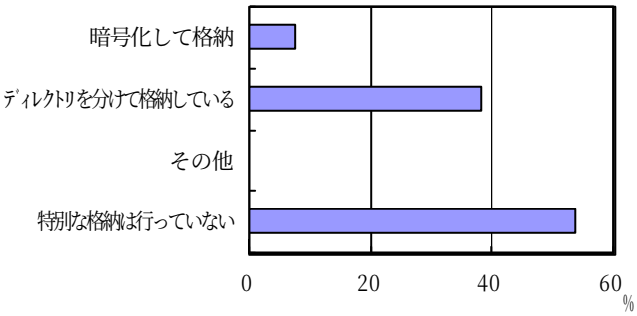
【全体】



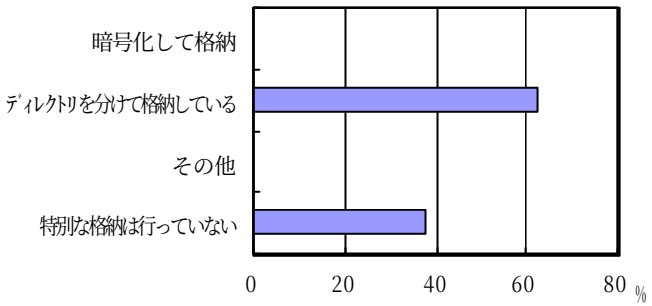
【大規模】



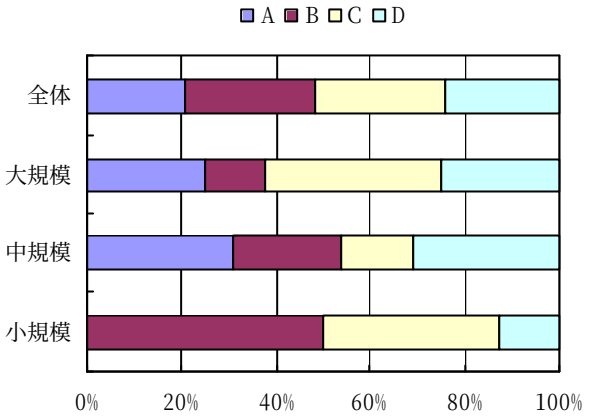
【中規模】



【小規模】

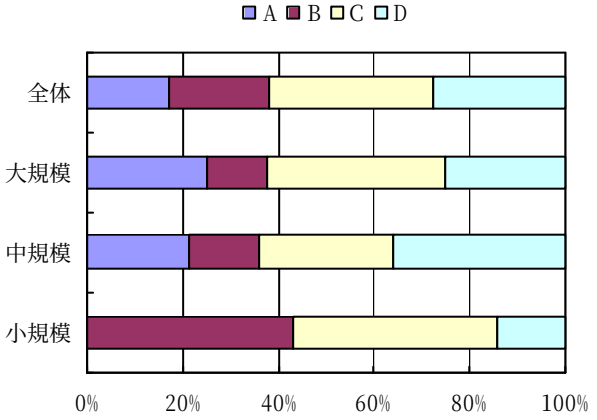


(3) セキュリティ管理情報に対する必要なアクセス制御機能の組込状況



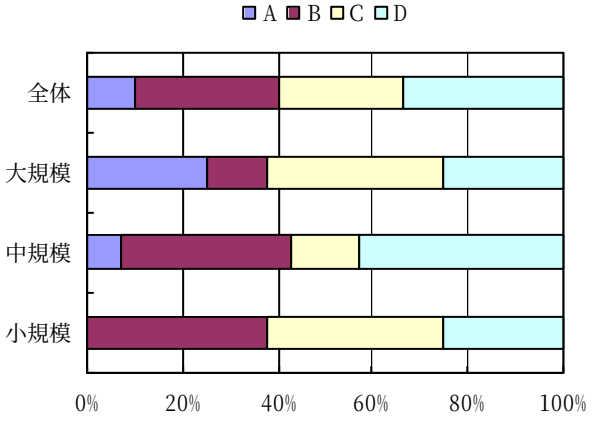
(A) 当初組込み時だけでなく変更時においても、決められたプロセスに従った組織的なチェックが厳密に行われており、不備が存在する余地はほとんどない
(B) 当初組込み時だけでなく変更時においても、決められたプロセスに従った組織的なチェックが行われることになっているが、厳格に運用されてなく、不備が見過ごされている可能性もある
(C) 確認プロセスはあるが形式的で、組織的な管理は行われていない。担当者の注意に依存しているが、一応管理されている
(D) 確認プロセスも確立されておらず、担当者任せであまり確認は行われていない

(4) セキュリティ管理情報に対するアクセス制御や認証に用いる情報の設定



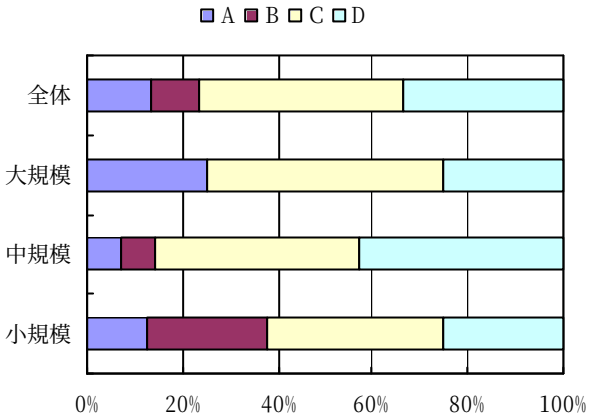
(A) この設定は決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている。またドキュメントもよく整備されている
(B) この設定は決められた手順に沿って行われることになっており、ドキュメントも整備されているが、組織的な検討やレビューおよび見直しは厳格ではなく、設定の一部に妥当性を欠いていることもありうる
(C) 設定およびその管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメント化も不十分である
(D) 担当者任せにしており、特に管理は行っていない

(5) セキュリティ管理情報に対するアクセス監視の有無



(A) アクセスの監視が必要な情報の洗出しと監視要件の指定は十分に検討されている。また、アクセスログの分析もルーチン化されており、必要な監視は励行している
(B) アクセスの監視が必要な情報の洗出しと監視要件の指定、これらの指定にもとづいたアクセスログの取得と分析も行われているが、監視対象の洗出しや監視要件の指定やアクセスログの分析は十分とは言えない
(C) 一部の情報に対してアクセスログの取得と分析が行われているが、監視が必要な情報の洗出しやそれらに対する監視要件の指定等は組織的に検討されていない
(D) 行っていない

(6) セキュリティ管理情報に対する改ざん検知



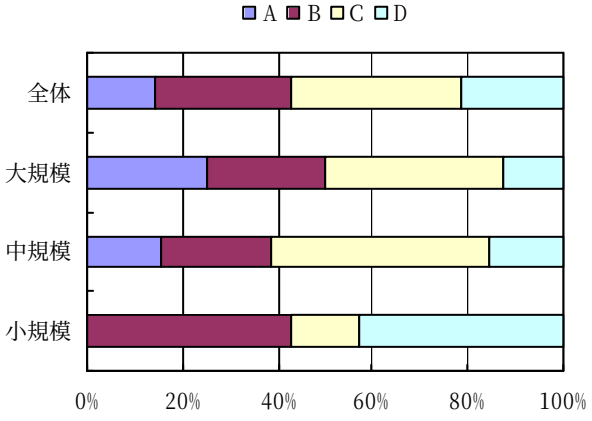
(A) セキュリティ管理情報のほとんどに対し改ざん検知を行う仕組みを組込んでいる
(B) 特に重要と思われるセキュリティ管理情報に対してのみ定期的に改ざん検知を行っている
(C) システムへの侵入の形跡が発見された場合等、必要と判断された場合のみ実施
(D) 行っていない

7.2.3 業務現場やシステム運用の現場におけるセキュリティ管理情報の取扱い

分析結果から見た傾向は、以下の通り。

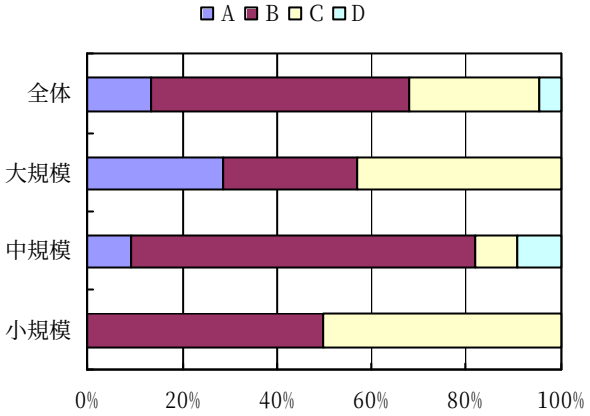
- セキュリティ管理情報の取扱いルールが確立しているサイトは 4／5 程度あり、厳密に見ると半分以下となっている。小規模サイトにおいては約半分のサイトにおいてルールが確立されていない。
- セキュリティ管理情報の取扱いルールの遵守状況はほとんどのサイトで遵守されているという回答があった。個人の意識に依存というのが 1／4 程度あり、小規模サイトでは半分もあった。

(1) セキュリティ管理情報の取扱いルール確立状況



(A) システム運用現場における保護対象のセキュリティ管理情報が記録された印刷物や電磁媒体の洗出し、それぞれに求められる取扱いルールの指定は組織的な管理のもとで行われている。また、その見直しも含め管理プロセスも確立している
(B) システム運用現場における保護対象のセキュリティ管理情報が記録された電磁媒体等の洗出しやそれぞれに求められる取扱いルールの指定は、決められた手順に沿って組織的には行われているが検討は十分とは言えない
(C) 特に重要なもの についてのみ取扱いルールが決められている
(D) 保護対象の電磁媒体等の保護は特に考えてはいない

(2) システム運用現場や業務現場における PC・電磁媒体に対する取扱い状況



(A) 取扱いルールはシステムの運用現場や業務現場に徹底されており、厳格に運用されている
(B) おおむね取扱いルールにもとづいた保護が行われているが厳格とはいえない
(C) 取扱いルールが示されているが管理や指導はほとんど行われておらず、個人の意識に依存している
(D) ほとんど守られていない

8 ユーザ情報の保護

本章では EC サイトに対し、ユーザ情報を含むデータやファイル等の漏洩、改ざん、破壊等の保護管理策への取組状況について分析を行う。

分析項目については、以下の通り。

- 保護対象のユーザ情報の把握と保護要件の指定
- システム上の保護対象ファイルに対する保護の実施
- 保護対象のユーザ情報がかかわる印刷物の取扱い
- 保護対象のユーザ情報がかかわる PC や電磁媒体の取扱い

8.1 “ユーザ情報の保護 ”全体を通しての傾向

ユーザ情報の保護についての認識は浸透しており、全体の半数程度のサイトで、保護対象ファイルに対する保護要件の指定が適切に行われているようであるが、管理の厳格さについては疑問である。これはアクセス管理の仕組みや、アクセス管理の実行についても同様である。

システム運用現場や業務現場における印刷物や電磁媒体等の取扱いまでに配慮が行われているところは半数程度であり、運用上の問題もかなりあるものと思われる。

ユーザ情報の保護に関しては実務的な方法論の開発が必要である。

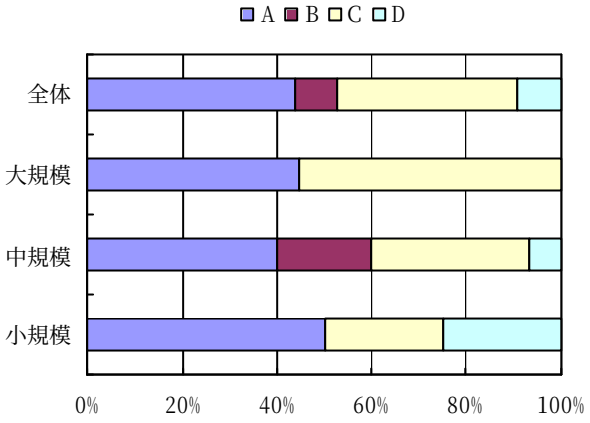
8.2 設問ごとの分析結果

8.2.1 保護対象のユーザ情報の把握と保護要件の指定

分析結果から見た傾向は、以下の通り。

- ユーザ情報の把握と保護の指定を実施しているサイトは 9／10 程度あり、ユーザ情報に関し意識していることがうかがえる。ただし、組織的にユーザ情報の把握と保護の指定を行っているサイトは半分以下となっている。
- 保護対象ファイルに対する保護要件は約 4／5 のサイトで指定を行っている。しかし、組織的に実施しているサイトは半分以下となっている。小規模サイトにおいてはおよそ半分のサイトが保護対象ファイルに対する保護要件の指定が行われていない。
- アクセス権限保有者の指定と付与するアクセス権の指定は 4／5 以上のサイトで実施している。しかし、組織的にアクセス権の指定を実施しているサイトは半分以下となっている。

(1) ユーザ情報の把握と保護の指定状況



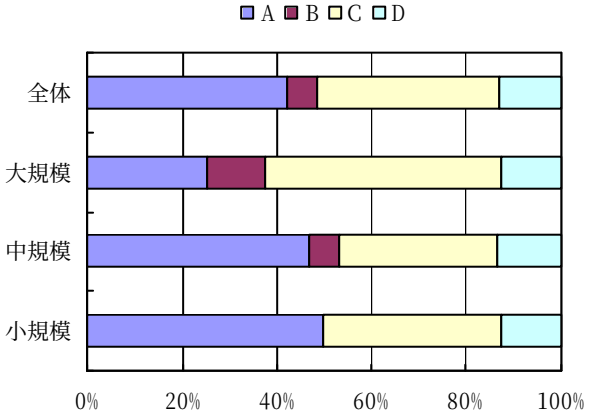
(A) サイトが取扱うすべてのユーザ情報は洗出され、それぞれに求められる保護についての指定は組織的に検討、レビューされている。また、その見直しも適宜行われていて、保護対象のユーザ情報の把握とそれぞれに対する保護についての指定の妥当性は常に維持されている

(B) この指定は組織的にレビューされることになっているが、レビューや見直しは厳格であると言えず、保護すべきユーザ情報の把握とそれぞれに対する保護についての指定に漏れや一部に妥当性を欠くところもありうる

(C) 担当者レベルの作業ではあるが、保護対象とすべきユーザ情報の洗出しやそれぞれに対する保護についての指定が行われている。組織的なレビューや管理は行われていない

(D) 保護対象のユーザ情報の洗出しやその保護についての指定等は行われていない

(2) 保護対象ユーザの情報の存在場所の把握状況



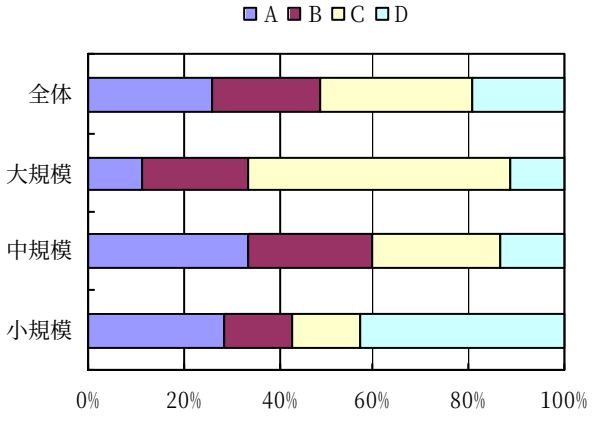
(A) 保護の対象となるユーザ情報の存在場所の洗出しは、組織的にレビューされている。また、その見直しも適宜行われておりドキュメント化も十分で、保護対象のユーザ情報の存在場所は常に正確に把握されている

(B) 保護対象のユーザ情報の存在場所の指定は組織的にレビューされることになっており、ドキュメント化も行われているが、レビューや見直しは厳格であると言えず、保護対象のユーザ情報の存在場所の把握に漏れもありうる

(C) 担当者レベルの作業ではあるが、保護対象のユーザ情報の存在場所の洗出しが行われている。組織的なレビューや管理は行われていない。ドキュメント化も十分ではない

(D) 保護対象のファイルやメッセージの把握は行っていない

(3) 保護対象ファイルに対する保護要件の指定状況



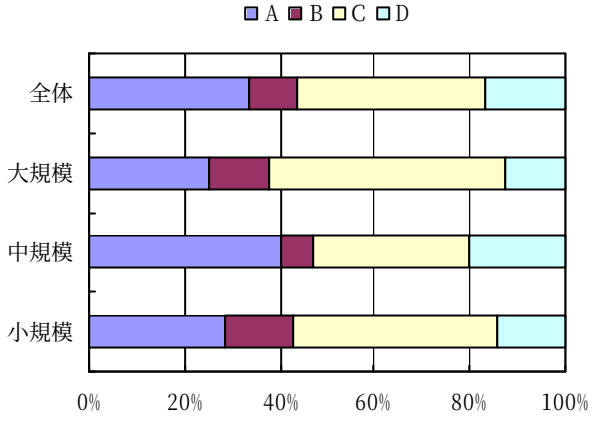
(A) 保護対象ファイルに対する保護要件の指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われおり、見直しも適宜行われ、ドキュメント化も十分で、常に、その妥当性は維持されている

(B) 保護対象ファイルに対する保護要件の指定は、決められた手順に沿って行われることになっておりドキュメント化も行われているが、組織的な検討やレビューおよび見直しやドキュメント化は厳格ではなく、指定の一部に妥当性を欠いていることもありうる

(C) 管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメント化も不十分である

(D) 保護対象ファイルに対する保護要件の指定は行われていない

(4) アクセス権限保有者の指定と付与するアクセス権の指定



(A) これらの指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている。また、ドキュメントもよく整備されている

(B) これらの指定は、決められた手順に沿って行われることになっており、ドキュメント化も行われているが、組織的な検討やレビューおよび見直しやドキュメント化は厳格ではなく、指定の一部に妥当性を欠いていることもありうる

(C) 管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメント化も不十分

(D) 担当者任せにしており、特に管理は行われていない

8.2.2 システム上の保護対象ファイルに対する保護の実施

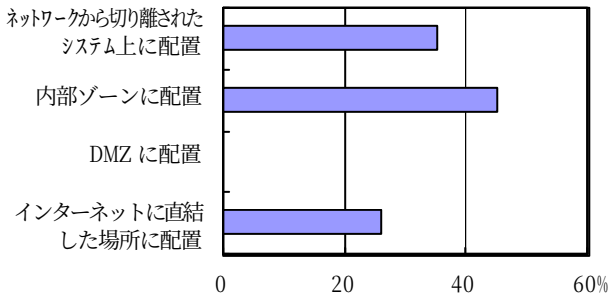
分析結果から見た傾向は、以下の通り。

- 保護対象ファイルの配置場所と配置についての評価を見ると 3／4 程度のサイトが配置に注意を払っている。
- 保護対象ファイルの格納上の施策としてはディレクトリを分けて格納しているサイトが大部分を占めている。小規模サイトでは 4／5 以上のサイトで対策が行われていない。
- 保護対象ファイルに対する必要なアクセス制御機能の組込状況は 7／10 のサイトで実施しているが、組織的に行っているサイトは 3／10 以下となっている。
- 保護対象ファイルに対するアクセス制御や認証に用いる設定情報の管理状況は 3／4 以上のサイトで実施しているが、組織的に行っているサイトは 1／3 以下となっている。

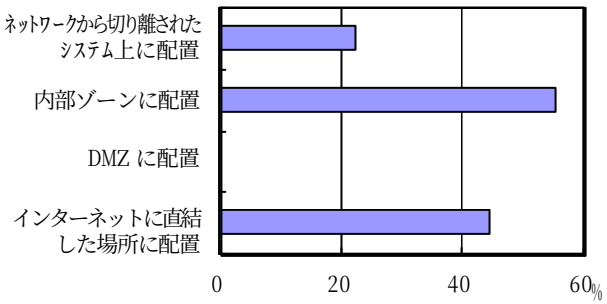
(1) システム構成上でのユーザ情報の配置の工夫

① 保護対象ファイルの配置場所

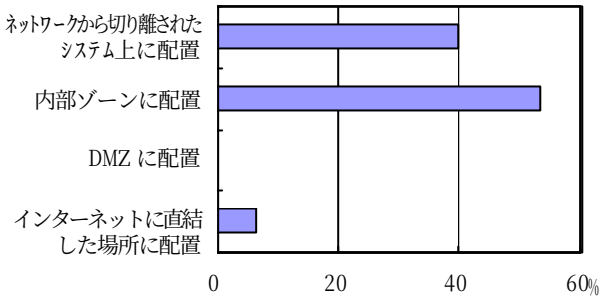
【全体】



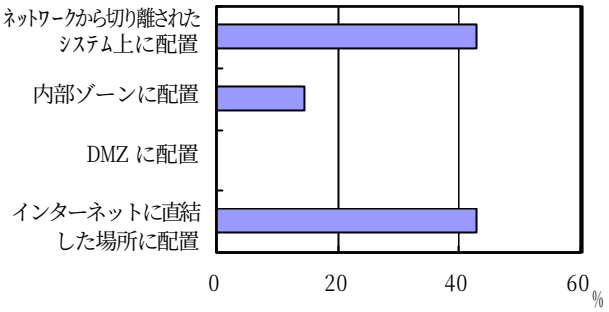
【大規模】



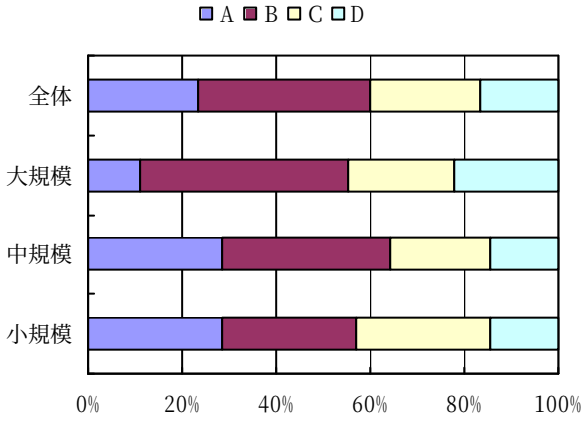
【中規模】



【小規模】

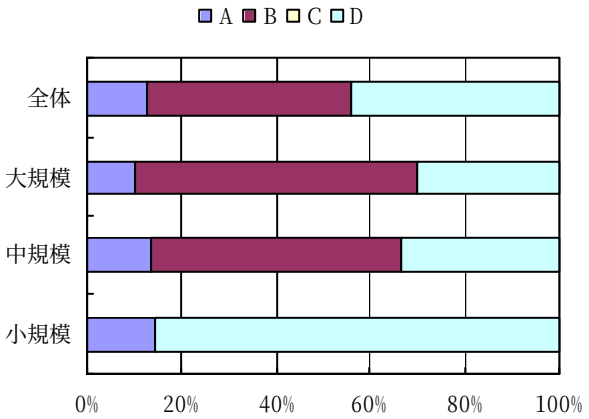


② 保護対象ファイルの配置についての評価



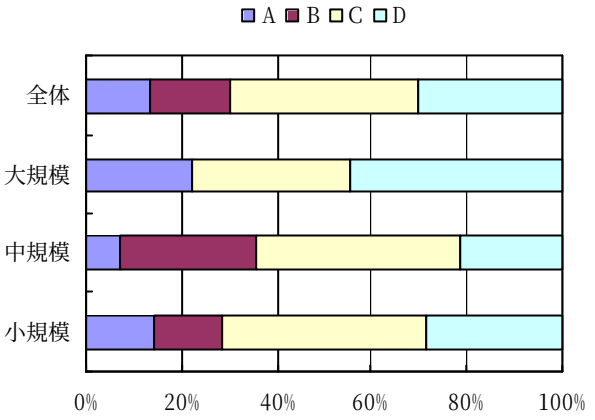
(A) すべての保護対象ファイルは外部からの完全に隔離されている
(B) 外部からアクセス可能な領域に置かれているものもあるが、すべては保護要件を満たす位置にある
(C) おおむね適切な配置であるが、一部は危険な場所に置かれている
(D) 配置場所についての検討が不十分で、全体として不適切な配置といえる

(2) 保護対象ファイルの格納上の工夫



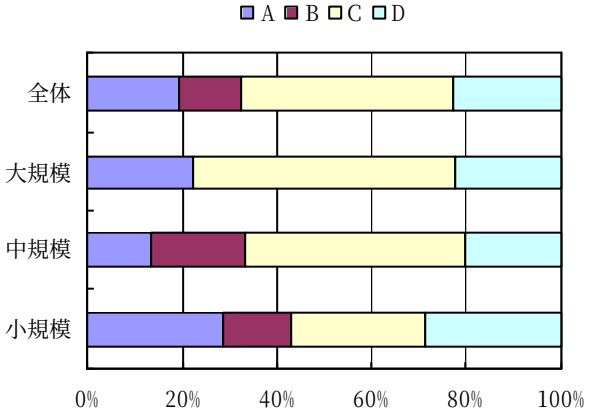
(A) 暗号化して格納
(B) Web等で直接参照できないディレクトリの下に格納
(C) その他
(D) 特別な格納は行っていない

(3) 保護対象ファイルに対する必要なアクセス制御機能の組込状況



(A) 当初組込み時だけでなく変更時においても、決められたプロセスに従った組織的なチェックが厳密に行われており、不備が存在する余地はほとんどない
(B) 当初組込み時だけでなく変更時においても、決められたプロセスに従った組織的なチェックが行われることになっているが、厳格に運用されてなく、不備が見過ごされている可能性もある
(C) 確認プロセスはあるが形式的で、組織的な管理は行われていない。担当者の注意に依存しているが、一応管理されている
(D) 確認プロセスも確立されておらず、担当者任せであまり確認は行われていない

(4) 保護対象ファイルに対するアクセス制御や認証に用いる情報の設定



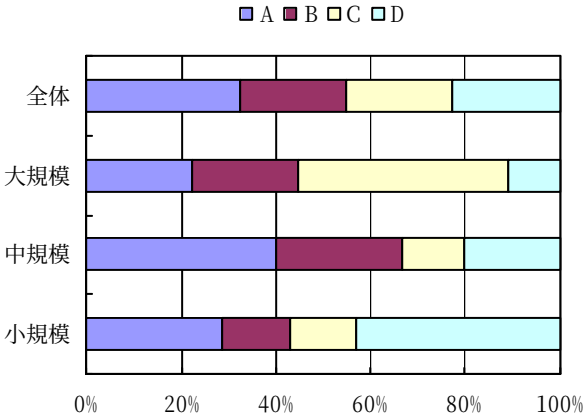
(A) この設定は決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている
(B) この設定は決められた手順に沿って行われることになっているが、組織的な検討やレビューおよび見直しは厳格ではなく、設定の一部に妥当性を欠いていることもありうる
(C) 設定およびその管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている
(D) 担当者任せにしており、特に管理は行っていない

8.2.3 保護対象のユーザ情報がかかわる印刷物の取扱い

分析結果から見た傾向は、以下の通り。

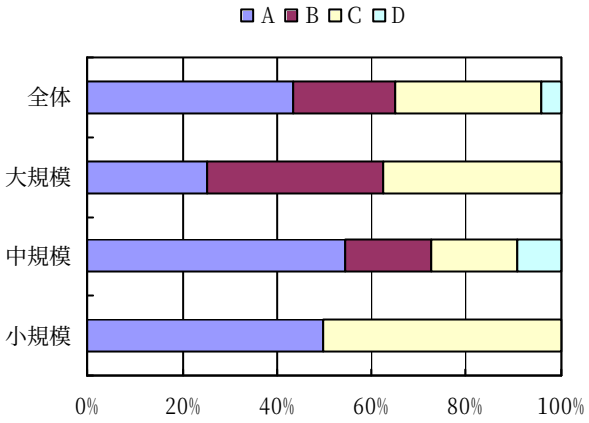
- 関係印刷物の把握とそれらに対する取扱いルールは 3／4 以上のサイトで確立しており、ルールの確立しているサイトではほとんどのサイトがルールを遵守している。

(1) 関係印刷物の把握とそれらに対する取扱いルールの確立状況



(A) 十分に検討された印刷物の取扱いルール確立しており、関係者にも徹底されている
(B) 印刷物に対する取扱いルールは決められているが、検討が十分とはいえない
(C) 特に重要なものについてのみ取扱いルールが決められている
(D) 印刷物についての保護は特に考えてはいない

(2) 印刷物に対する取扱い状況



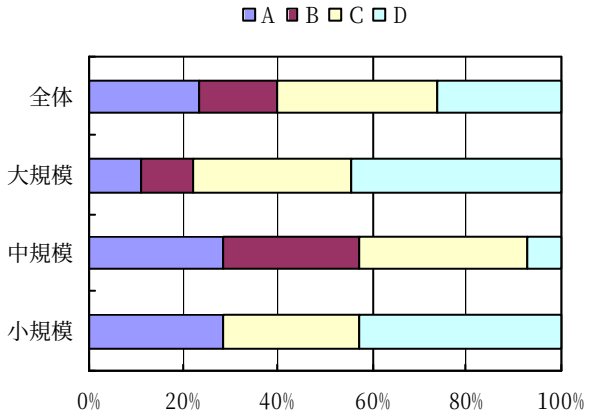
(A) 取扱いルールはシステムの運用現場や業務現場に徹底されており、厳格に運用されている
(B) おおむね取扱いルールにもとづいた保護が行われているが厳格とはいえない
(C) 取扱いルールが示されているが管理や指導はほとんど行われておらず、個人の意識に依存している
(D) ほとんど守られていない

8.2.4 保護対象のユーザ情報がかかわるPCや電磁媒体の取扱い

分析結果から見た傾向は、以下の通り。

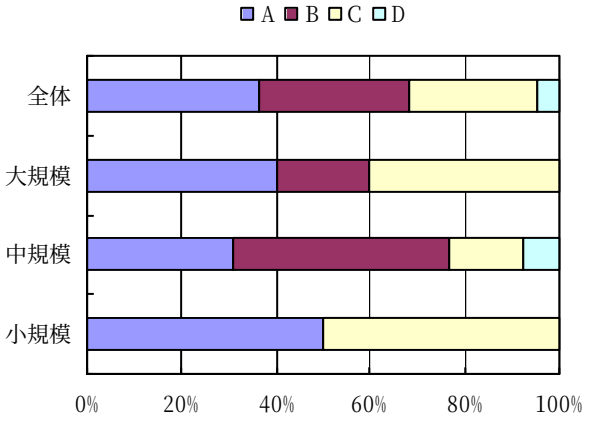
- PCや電磁媒体に関する取扱いルールは3／4程度のサイトで確立しており、ルールの確立しているサイトではほとんどのサイトがルールを遵守している。

(1) PCや電磁媒体の把握とそれらに対する取扱いルールの確立状況



(A) 電磁媒体の取扱いについての十分に検討されたルールが確立しており、関係者にも徹底されている
(B) 電磁媒体等に対する取扱いルールは決められているが、検討が十分とはいえない
(C) 特に重要なものについてのみ取扱いルールが決められている
(D) 電磁媒体等に対する保護は特に考えてはいない

(2) PCや電磁媒体に対する取扱状況



(A) 取扱いルールはシステムの運用現場や業務現場に徹底されており、厳格に運用されている
(B) おおむね取扱いルールにもとづいた保護が行われているが厳格とはいえない
(C) 取扱いルールが示されているが管理や指導はほとんど行われておらず、個人の意識に依存している
(D) ほとんど守られていない

9 通信の保護

本章では EC サイトの外部との通信に対し、通信路上での情報の漏洩、改ざんの防止や、意図した相手でない者との通信の防止、さらには否認防止等の保護管理策への取組状況について分析を行う。

分析項目については、以下の通り。

- 保護対象の通信の把握と保護要件の指定
- 通信に対する保護の実施

9.1 “通信の保護”全体を通しての傾向

通信の保護の認識はほぼ浸透しており、全体的には問題はほとんどないが、保護対象となる通信の把握と保護要件の指定については組織的な取組みが不足しているようである。

保護対象になる通信に対する Web 通信への SSL の適用は半数程度とほぼ浸透しており、保護が必要なメールに対して暗号化等の対策を行っているサイトも見受けられる。

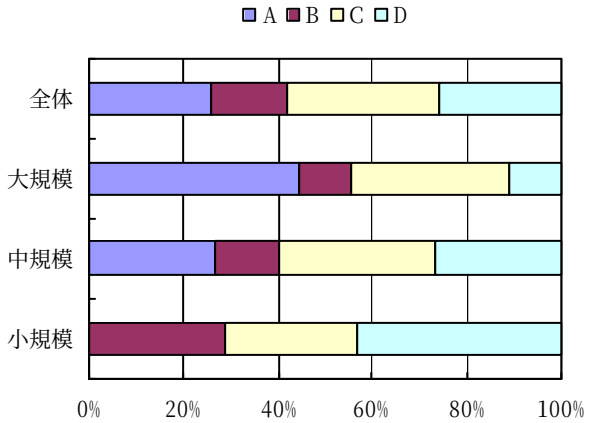
9.2 設問ごとの分析結果

9.2.1 保護対象の通信の把握と保護要件の指定

分析結果から見た傾向は、以下の通り。

- 保護対象となる通信の把握と保護要件の指定は 3／4 程度のサイトで実施されているが、厳格に見ると半分以下のサイトとなる。
- 小規模サイトでは半分程度のサイトが通信の保護を行っていない。

(1) 保護対象となる通信の把握と保護要件の指定状況



Ⓐ 保護対象となる通信の洗出しやそれぞれに対する保護要件の指定は、組織的な管理のもとで行われている。また、その見直しも含め管理プロセスも確立している

Ⓑ 保護対象となる通信の洗出しやそれぞれに対する保護要件の指定は、決められた手順に沿って組織的には行われているが検討は十分とは言えない

Ⓒ 保護対象となる通信の特定とその保護要件の指定は担当者の意識に任されており、その十分性についてはチェックされていない

Ⓓ 通信の保護は行っていない

9.2.2　通信に対する保護の実施

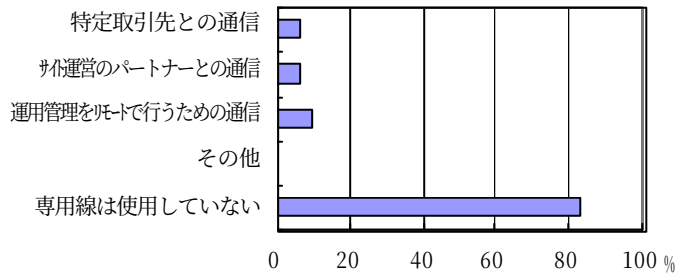
分析結果から見た傾向は、以下の通り。

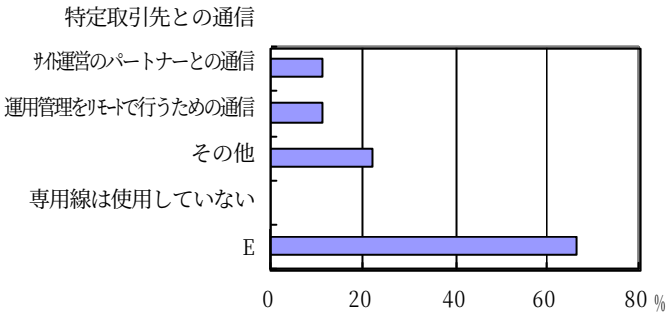
- 専用線の使用目的は特定取引先との通信やサイト運営のパートナーとの通信に使用しているのが全サイトの１／8である。また、ＶＰＮの使用目的は特定取引先との通信やサイト運営のパートナーとの通信に使用しているのが全体で1／10程度であった。
- Web 通信に対する保護手段として半数程度のサイトがＳＳＬを使用している。また、脅威を感じていないというサイトが 1／3 程度もあり、小規模サイトになると約半数になる。
- メール使用についてのルールは約 3／4 のサイトで持っているが、厳格なルールを持っているサイトは 1／3 以下と少ない。ほとんどが一般的な注意に止まっている。
- メールに対する保護は 4／5 のサイトで適用されている。厳格に見ると、1／4 である。
- 否認に対する対抗策を組込んでいるサイトは 1／10 以下と少ない。現段階では否認に対する問題意識が低いように思える。
- 無線 LAN を導入しているサイトでは、脆弱性に対する処置を実施しているサイトが 2／3 という結果であり、これは対策が十分であるかのように 見えるが、調査サンプル数の少なさや導入率の低さから、この結果をそのまま受取ることはできないと考える。

(1) 専用線や VPN 等のセキュアな通信路の使用状況

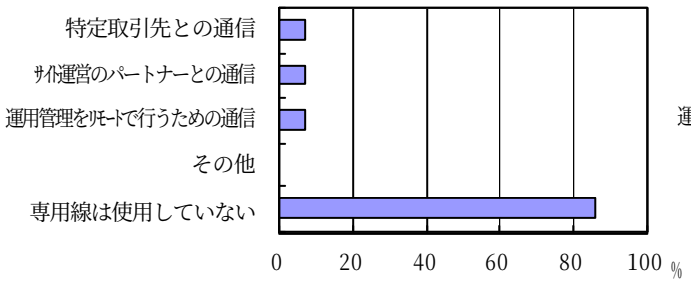
① 専用線

【全体】

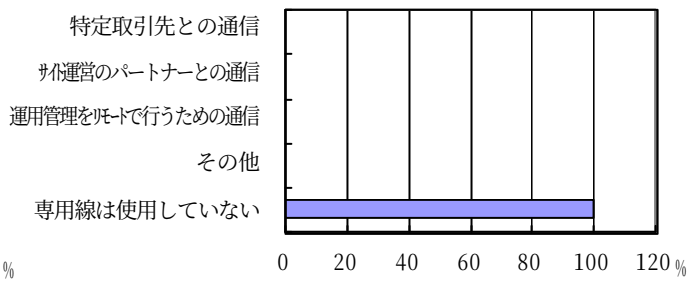




【中規模】

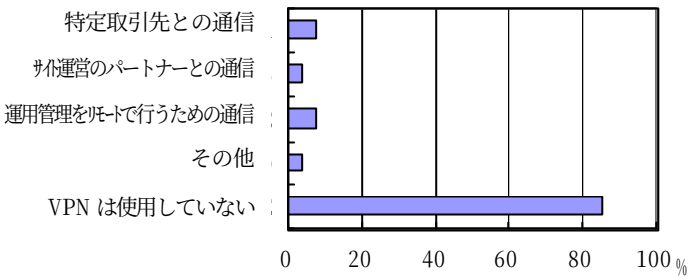


【小規模】

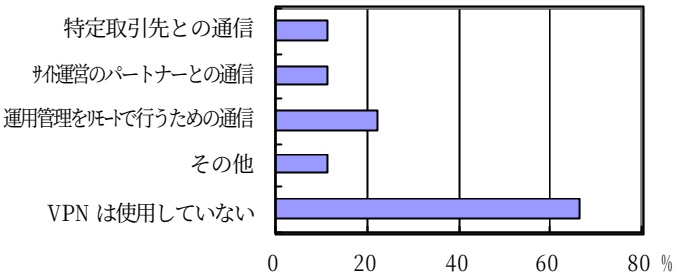


② VPN

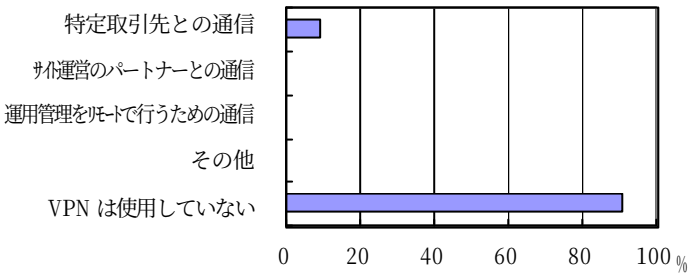
【全体】



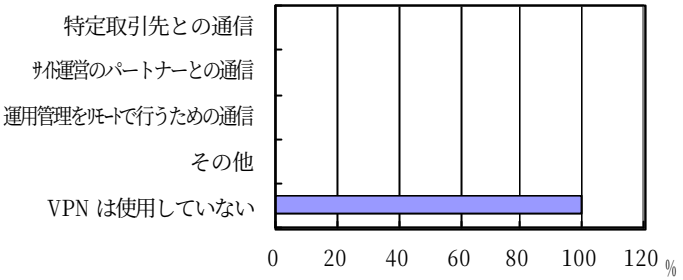
【大規模】



【中規模】

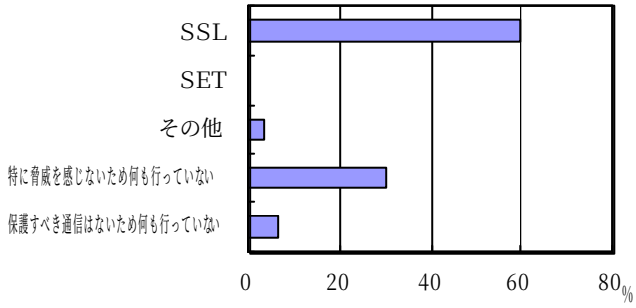


【小規模】

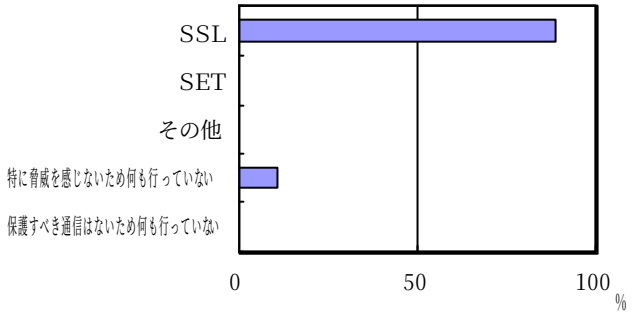


(2) Web 通信に対する保護の適用状況

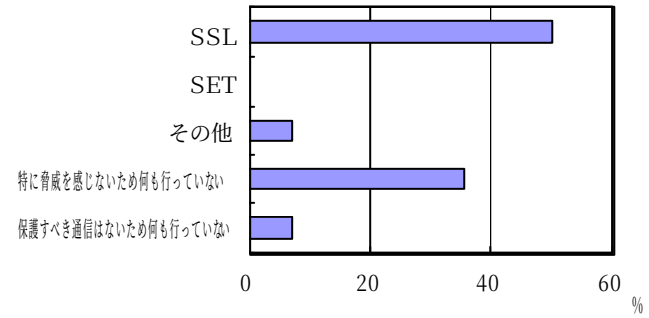
【全体】



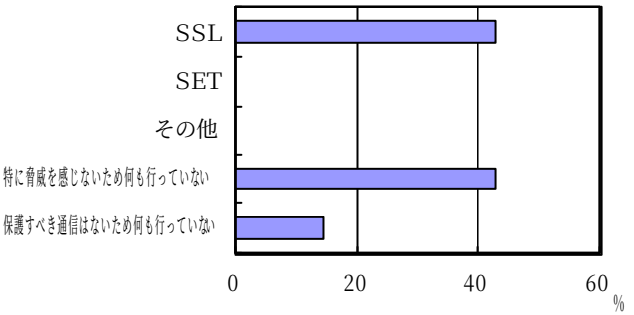
【大規模】



【中規模】

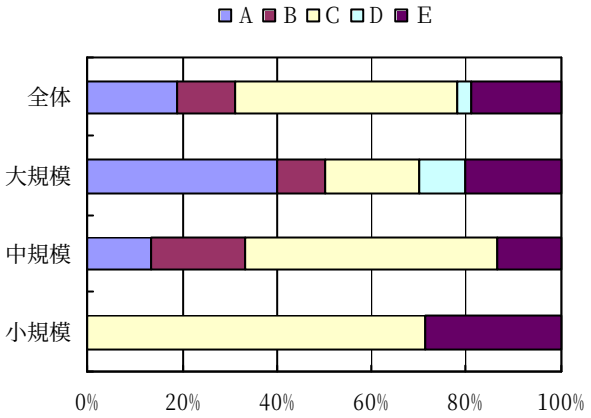


【小規模】



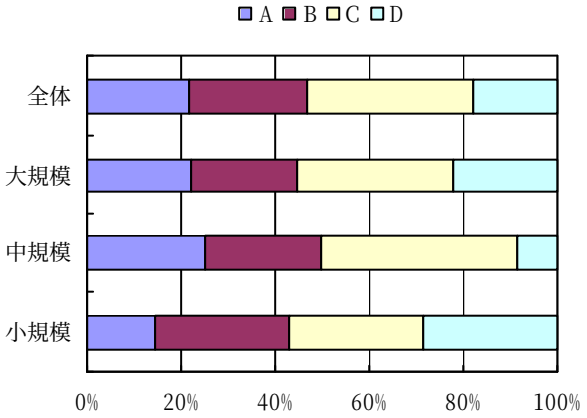
(3) メール通信に対する保護の適用状況

① メール使用についてのルール



Ⓐ 外部に対し秘匿が必要な情報のメールによる連絡は禁止している
Ⓑ 情報内容の暗号化を行えば、外部に対し秘匿が必要な情報もメールにより連絡することも可としている
Ⓒ 一般的な注意に止まっている
Ⓓ その他
Ⓔ 特別な配慮はしていない

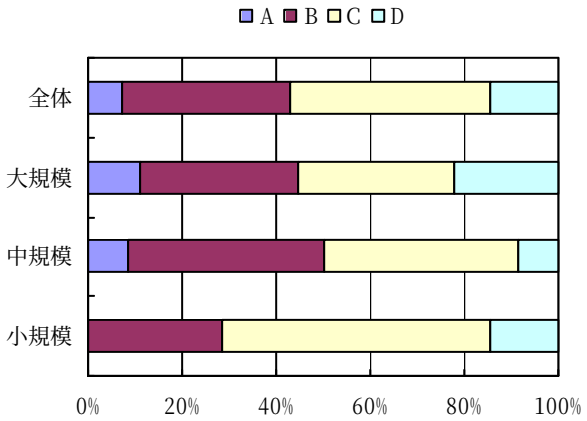
② メールに対する保護の適用状況の評価



Ⓐ ルールは関係者に徹底されて、その実行状況も厳しく管理されている
Ⓑ ルールは決められているが、実行状況についての管理は甘く、問題を起こす可能性もある
Ⓒ 関係者に注意を喚起しているが、実行状況についてのチェックは行っていない
Ⓓ 無管理状態である

(4) 否認に対する対抗策の実施状況

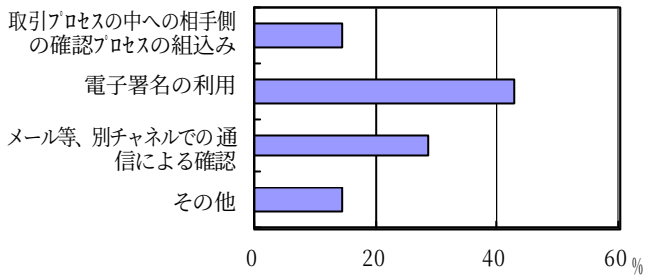
① 否認に対する対抗策の実施状況



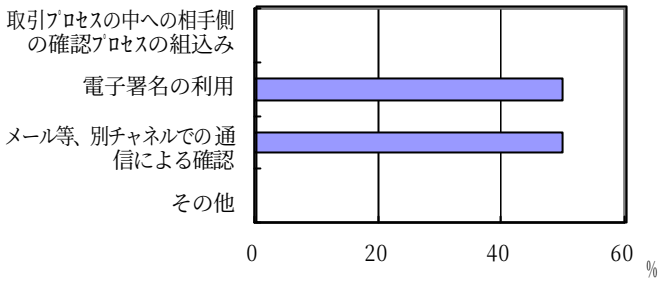
Ⓐ 組込んでいる
Ⓑ 気になっているが適当な方法がわからないため対策はしていない
Ⓒ 特に脅威を感じないため何も行っていない
Ⓓ 考えたことはない

② 否認防止策の組込方法

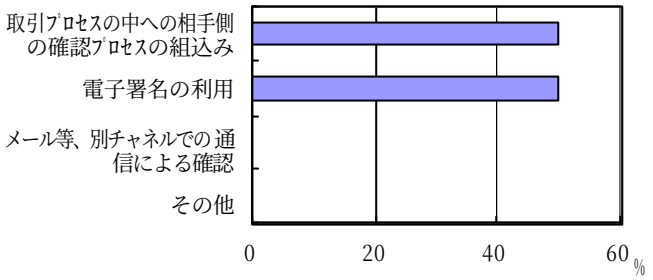
【全体】



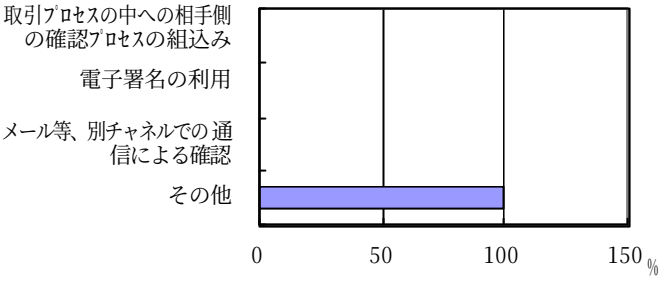
【大規模】



【中規模】

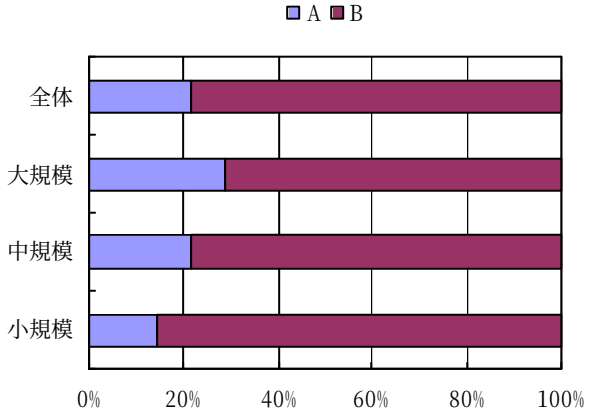


【小規模】



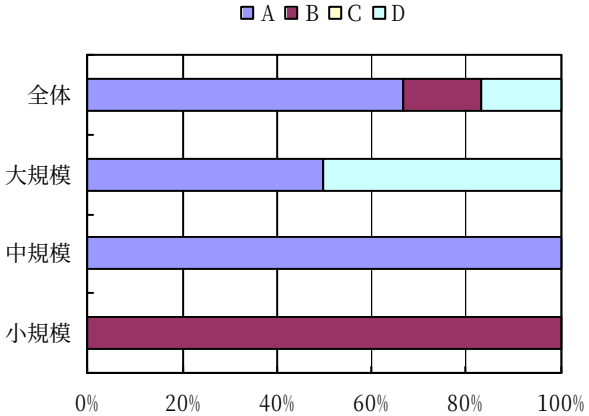
(5) 無線 LAN の脆弱性に対する処置の実施状況

① 無線 LAN の導入状況



Ⓐ 無線ＬＡＮを導入している
Ⓑ 無線ＬＡＮは導入していない

② 無線 LAN の脆弱性に対する処置の実施状況



Ⓐ 十分な検討のもと、無線ＬＡＮの脆弱性が問題にならないようにする対策が講じられている
Ⓑ 十分な検討のもとに対策が決められ実行されているが、その安全性は十分とは言えない
Ⓒ 問題点の認識はあり、注意はしているが、実質的な対策にはなっていない
Ⓓ 特に対策をしていない

10 ユーザ認証

本章では、EC サイトが外部に提供している様々なサービスのうち、対象者を限定しているサービスの提供に際して行われるユーザ認証の実施状況について分析を行う。

分析項目については、以下の通り。

- ユーザ認証への取組み
- 個々の認証場面に対する認証要件の指定
- ユーザの管理

10.1 “ユーザ認証 ”全体を通しての傾向

ユーザ認証を実施している組織はほとんどなく、脅威に対する認識が薄い。また、特に問題であるとは思われないが、定期的なパスワードの更新やパスワードの強度についての更なる取組みが望まれる。

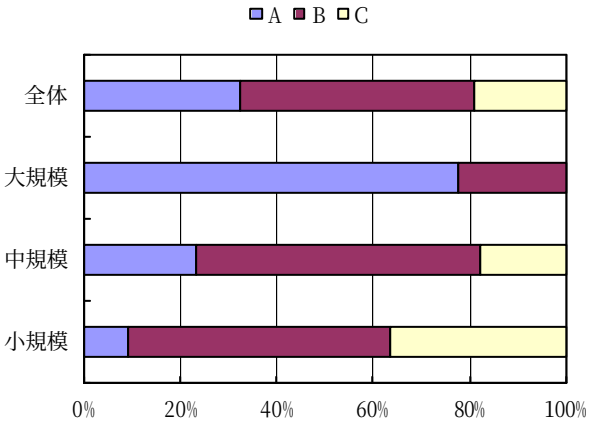
10.2 設問ごとの分析結果

10.2.1 ユーザ認証への取組み

分析結果から見た傾向は、以下の通り。

- 30%程度しかユーザ認証を実施していない。規模別では、大規模では 80%近くのサイトでユーザ認証を行っており、大規模では脅威に対する認識が高い。

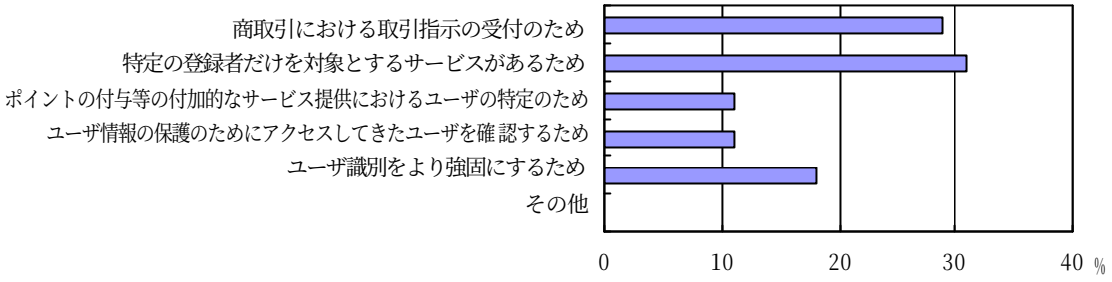
(1) ユーザ認証の実施の有無



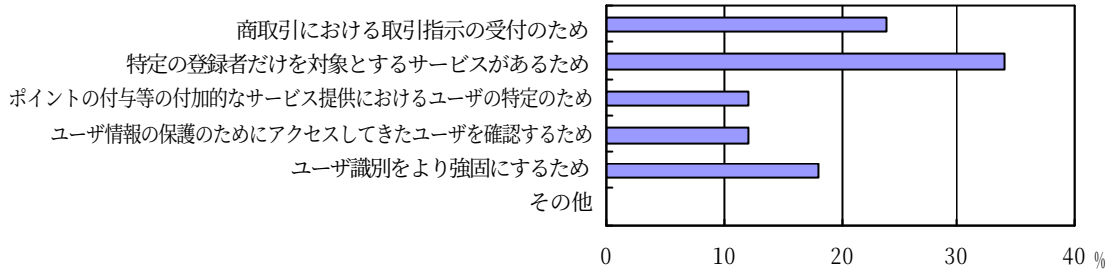
(A) ユーザ認証を行っている
(B) ユーザ認証は行っていない
(C) 回答なし

(2) ユーザ認証の利用目的

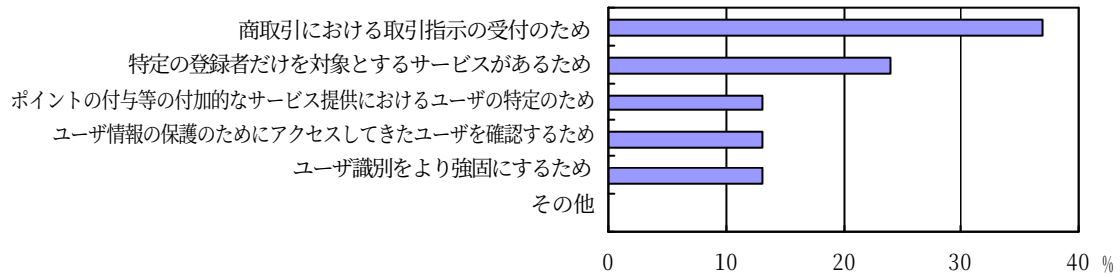
【全体】



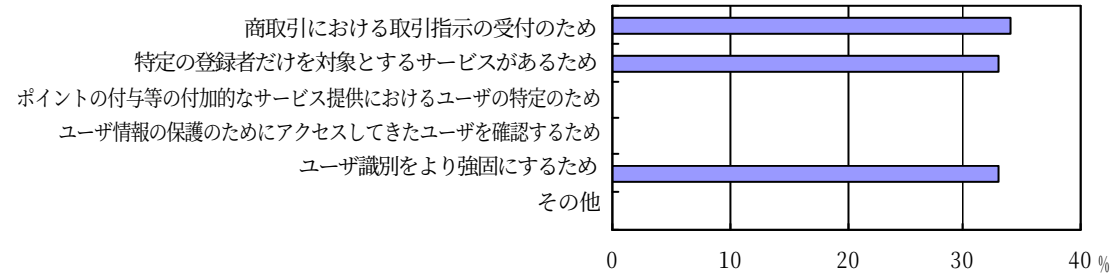
【大規模】



【中規模】



【小規模】

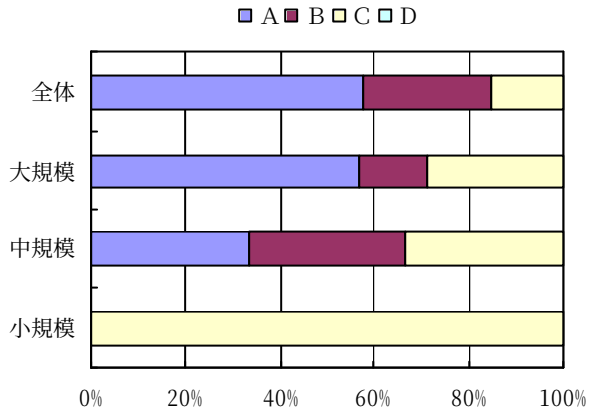


10.2.2 個々の認証場面に対する認証要件の指定

分析結果から見た傾向は、以下の通り。

- ユーザ認証の要件を十分検討しているサイトが約半数とかなり多い。
- 認証方式としては、パスワード／ID 方式がほとんどを占めている。

(1) ユーザ認証要件の指定状況

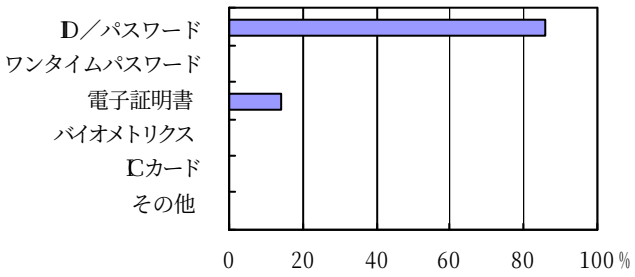


(A) 関係者による指定されたプロセスに沿った十分な検討にもとづいたものであり、すべての認証に対し適切な認証要件が指定されている
(B) ユーザ認証の要件定義は指定されたプロセスに沿って行われることになっているが、すべての認証に対して関係者による十分な検討が行われていない
(C) 認証要件は示されているが、定義の内容や検討プロセスは十分とは言えない
(D) 認証要件は明確でない

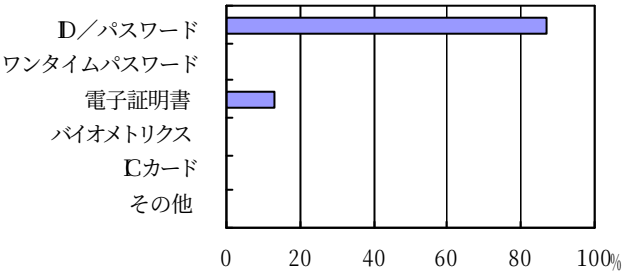
(2) ユーザ認証方式

① 採用している認証方式

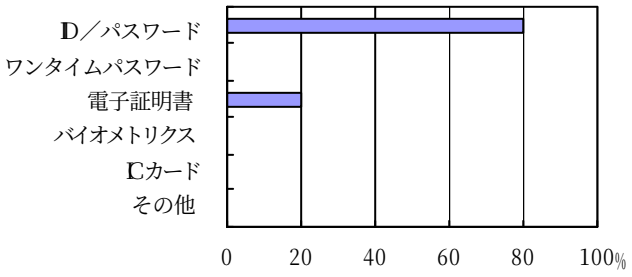
【全体】



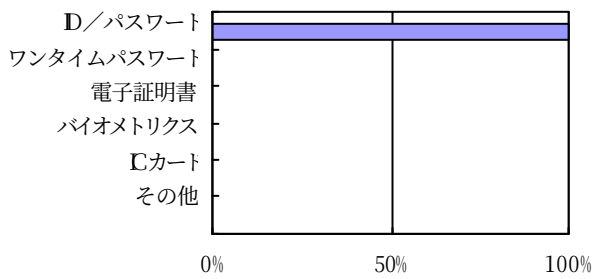
【大規模】



【中規模】

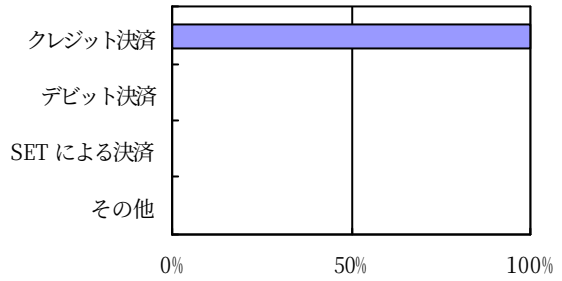


【小規模】

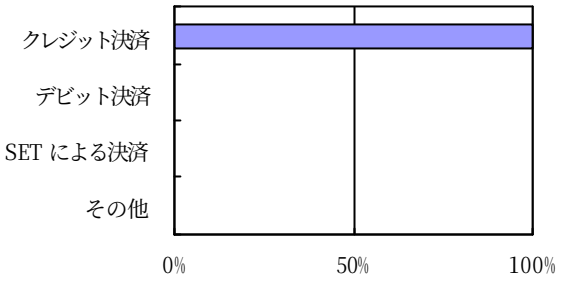


② 電子証明書によるユーザ認証の適用サービス

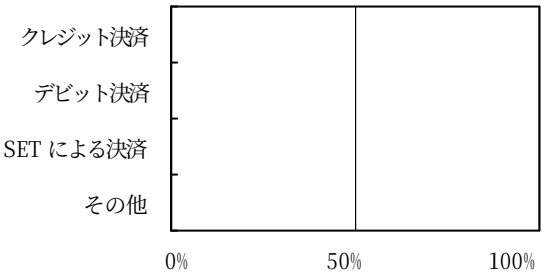
【全体】



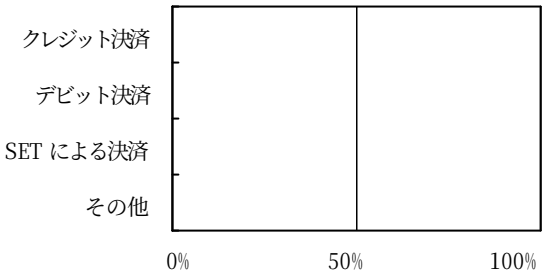
【大規模】



【中規模】



【小規模】



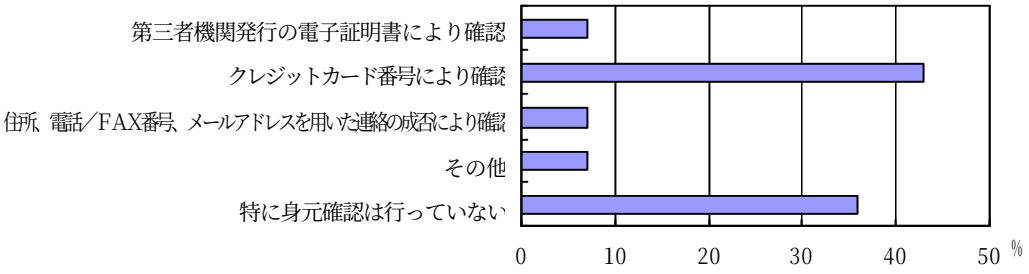
10.2.3 ユーザの管理

分析結果から見た傾向は、以下の通り。

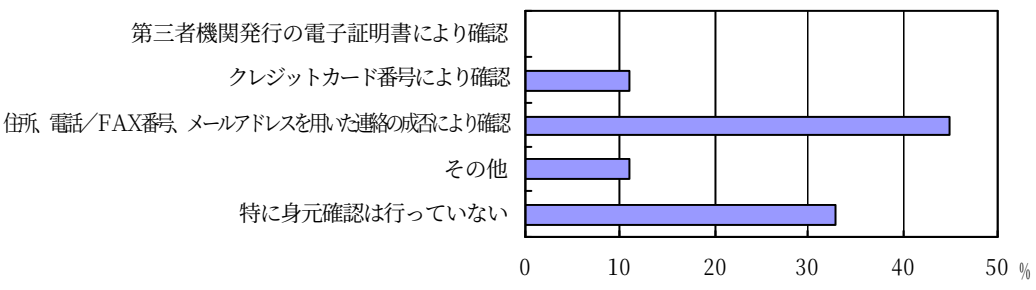
- バーチャルショップの利用者の身元確認は、メールや郵便、電話などの手段で本人に確認をとることにより行われるケースが多い。また、約半数が身元確認を行なっていない。
- 登録された利用者の情報は、ほとんどのサイトでルールを決めて管理されている。

(1) ユーザ登録時における身元確認方法

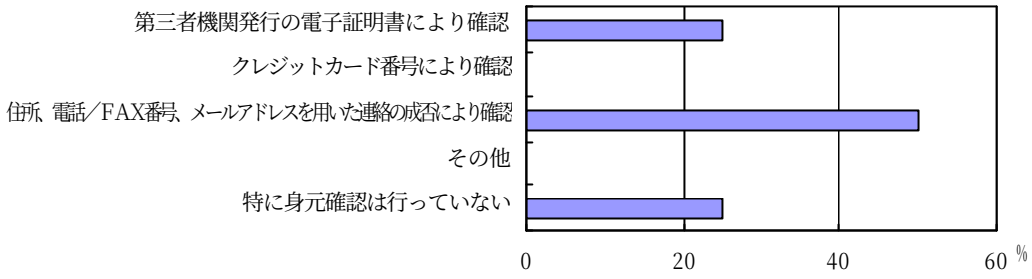
【全体】



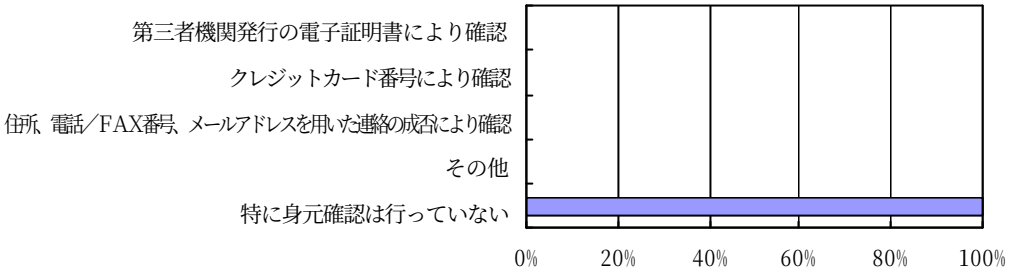
【大規模】



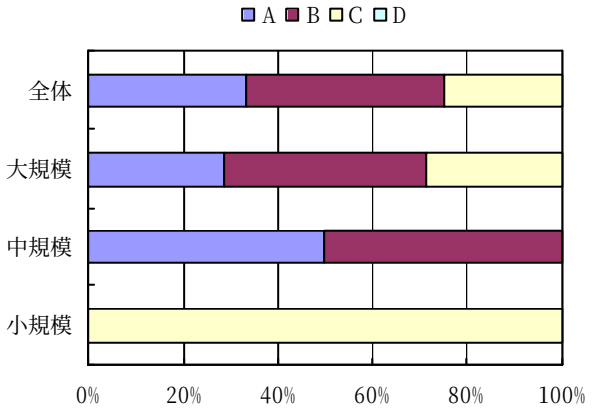
【中規模】



【小規模】

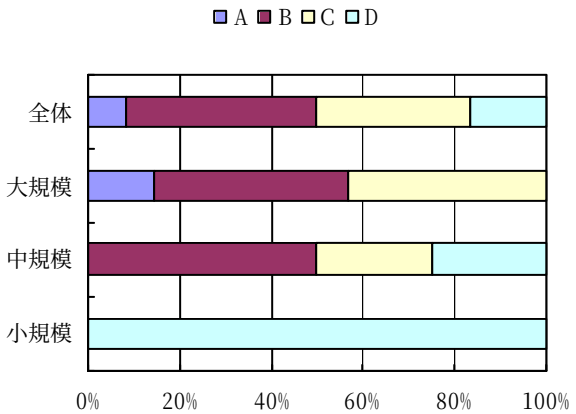


(2) 登録ユーザの管理状況



Ⓐ 管理ルールが確立しており、管理ルールに沿った日常的な管理に加え、定期的なチェックも行っており、ユーザ管理は万全と言える
Ⓑ 管理ルールは決められているが実行に徹底を欠き、ユーザ管理に不手際が生じる可能性もある
Ⓒ 管理ルールは決められているが、担当者まかせで組織的な管理は行われておらず、管理に問題があると言える
Ⓓ 管理ルールも明確でなく管理はずさん

(3) パスワードや IC カードなどの管理に関するユーザへの指導状況



Ⓐ 登録時だけでなく定期的に注意を喚起している
Ⓑ 登録プロセスの中で注意を喚起している
Ⓒ 登録に関する文書に記載してはいるが、積極的な指導は行っていない
Ⓓ 行っていない

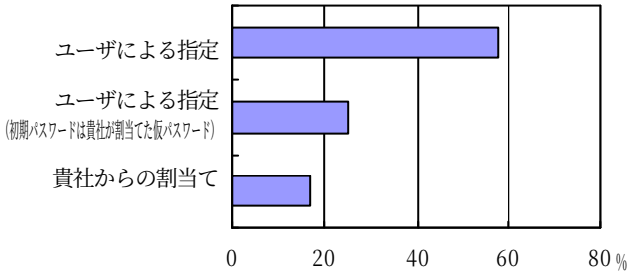
10.2.4 パスワードの管理

分析結果から見た傾向は、以下の通り。

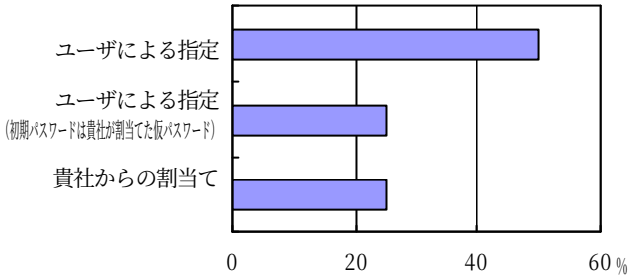
- パスワードの交付は、全サイトが、Web またはメールを利用して行っている。
- 仮パスワードを使用する場合の脆弱性に対する配慮は十分になされていないサイトが多く、なりすましの可能性が残されている。
- パスワードの更新を定期的に行っているサイトは少ない。また、パスワードのクラック対策を施しているサイトは、ほとんどないと言ってよい。

(1) パスワードの設定方法

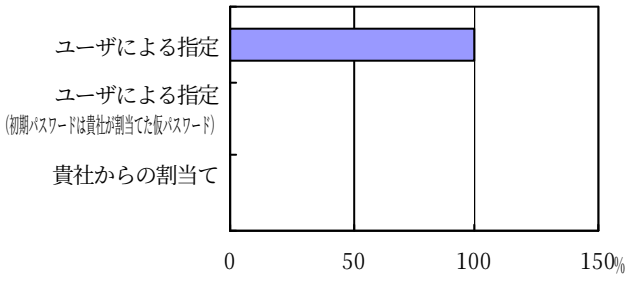
【全体】



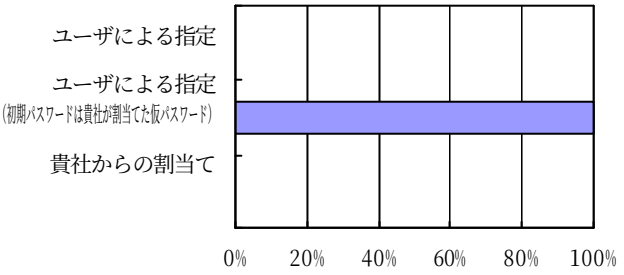
【大規模】



【中規模】

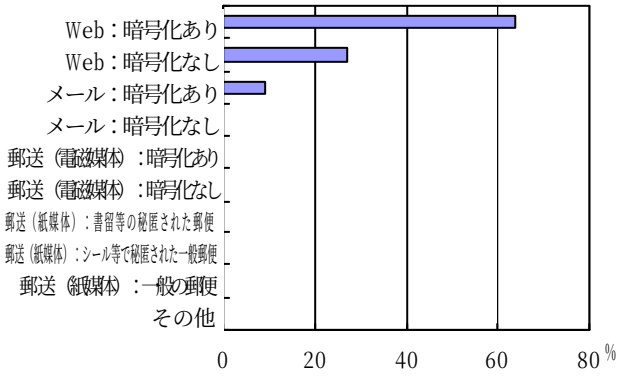


【小規模】

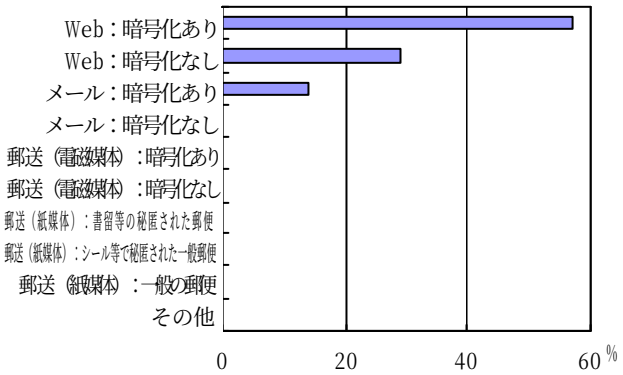


(2) ユーザの指定したパスワードの受理方法

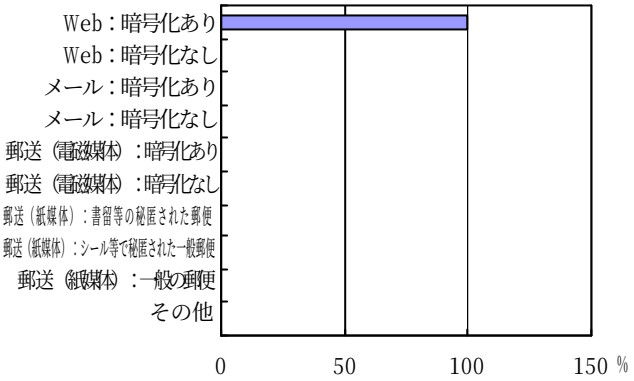
【全体】



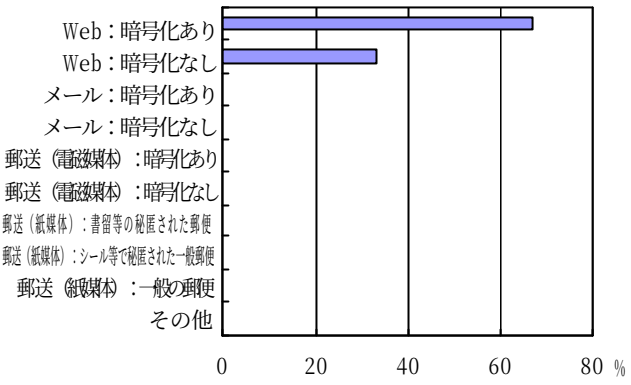
【大規模】



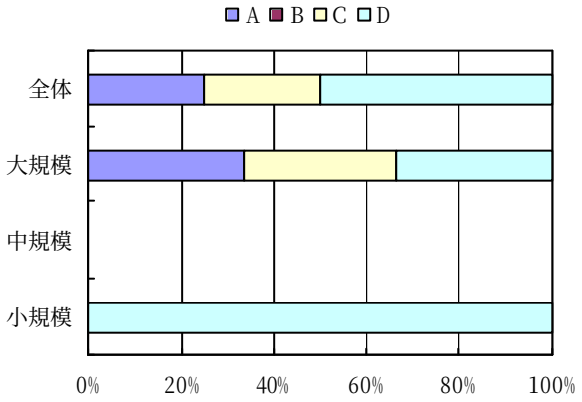
【中規模】



【小規模】



(3) 仮パスワード使用の脆弱性を補う工夫



Ⓐ 仮パスワードの引渡し方法への配慮や、1 回目のログインで正式なパスワードに変更する等、仮パスワードの使用がなりすましを誘う危険性を封じている

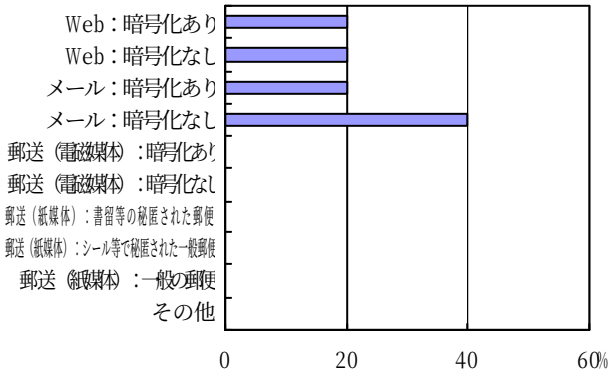
Ⓑ 仮パスワードを強度の高いものにするとともに引渡し方法にも配慮しているため、そのまま使われてもなりすましを誘う危険性は小さくしている

Ⓒ 仮パスワードを強度の高いものにするとともにユーザに対し正式なパスワードへの変更を要求しているが、そのまま使うこともできる。そのまま使われた場合、なりすましを誘う危険性は少なくない

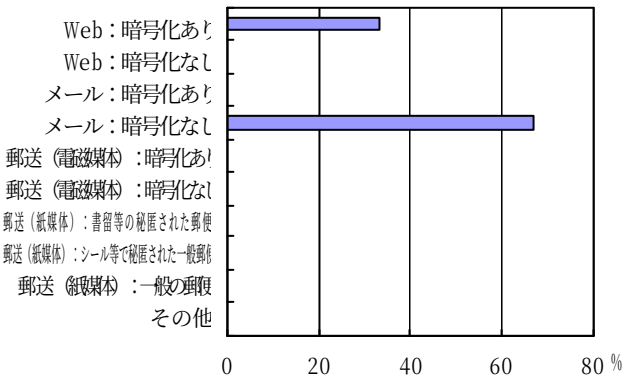
Ⓓ そのままユーザのパスワードとして使うこともでき、特別な配慮はされてないため、そのまま使われた場合、なりすましを誘う危険性が高い

(4) パスワード等のユーザへの交付方法

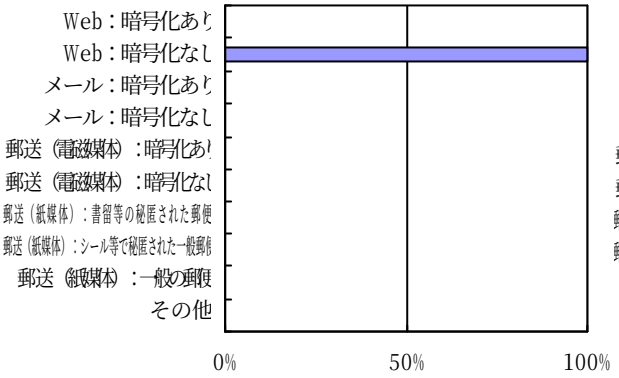
【全体】



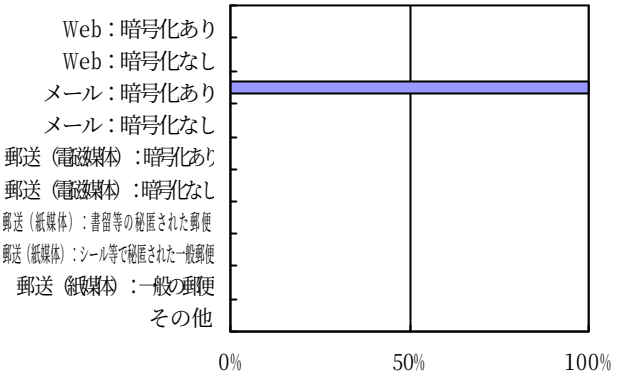
【大規模】



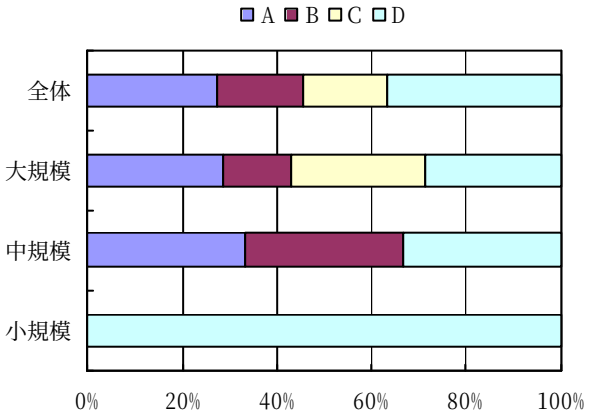
【中規模】



【小規模】



(5) パスワードの強度確保への工夫



(A) パスワードについての基準があり、ユーザに対する周知および指導を行っている。さらに、パスワード設定時にチェックを行い、不適切なパスワードは拒否している

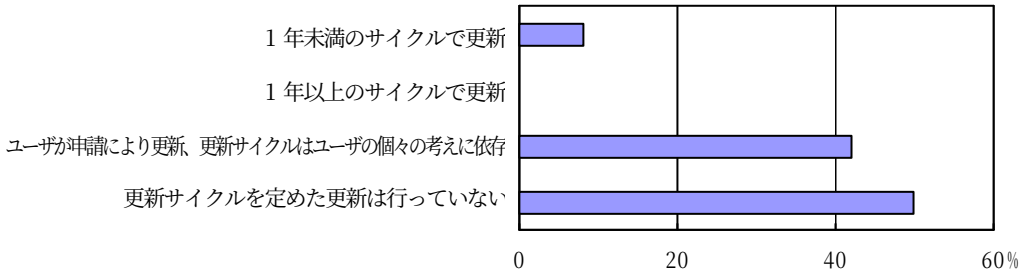
(B) パスワードについての基準があり、ユーザに対する指導を行っているが、徹底さには欠け、問題のあるパスワードが使われている可能性もある

（C）ユーザに対し推測されにくいパスワードの設定を呼びかけているが、受付時のチェックに関するチェック等は行われていない

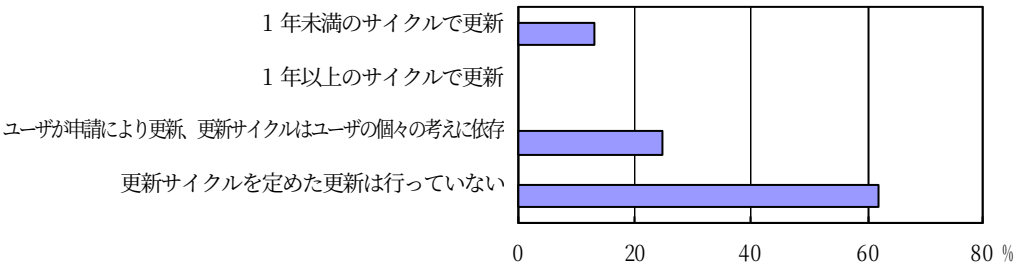
(D) 特に対策は講じていない

(6) パスワード等の更新サイクル

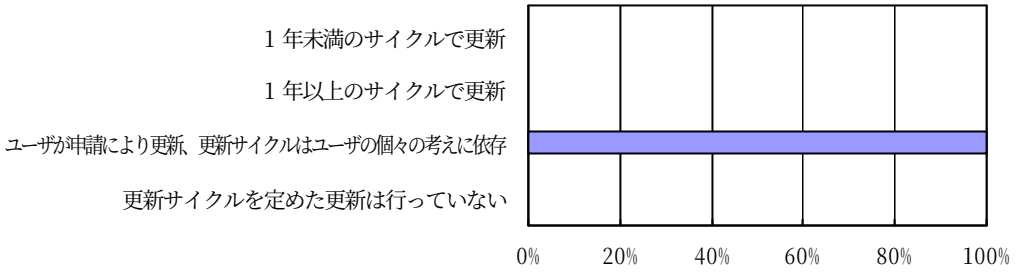
【全体】



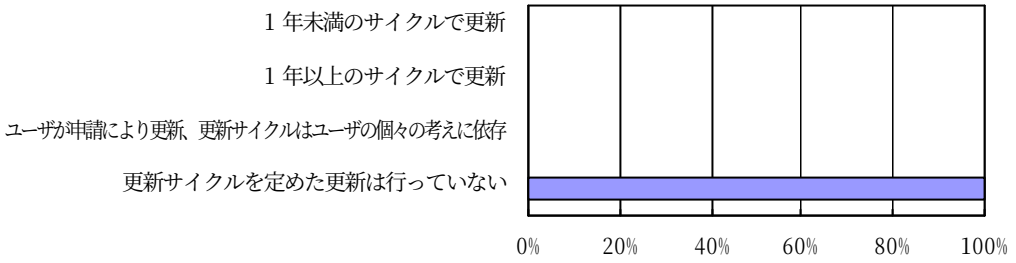
【大規模】



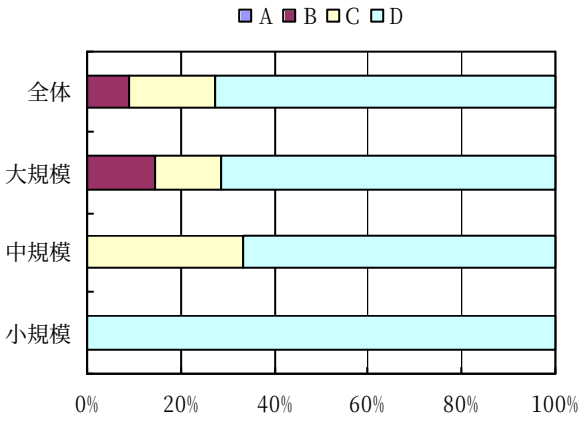
【中規模】



【小規模】



(7) パスワードクラックに対する対策



Ⓐ すべてのパスワード認証に、パスワードクラックの試みに対する対策を組込むことになっており、その組込みも確認されている
Ⓑ 重要なパスワード認証には、パスワードクラックの試みに対する対策を組込むことになっており、その組込みも確認されている
Ⓒ 一部のパスワード認証に対しては、担当者の判断でパスワードクラックの試みに対する対策が組込まれているが、組織的な管理は行われていない
Ⓓ パスワードクラックの試みに対する対策は組込んでいない

11 セキュアなシステム構築

本章では、EC サイトにおけるシステム構築上のセキュリティ対策の実施状況について分析を行う。

分析項目については、以下の通り。

- セキュリティ面からのシステム構成についての検討
- 各サーバのシステム構成上の配置とセキュリティ対策についての配慮
  - Web サーバ
  - Mail サーバ
  - ftp サーバ
  - DB サーバ
  - ファイルサーバ
- 開発環境のシステム構成上の配置とセキュリティ対策についての配慮
- 自社で開発するソフトウェアへの必要なセキュリティ機能の実装
- 自社で開発するソフトウェアに対する保護

11.1 “セキュアなシステム構築”全体を通しての傾向

システムをセキュアなものにし、運用環境の変化に追随していくための努力が不足している傾向にある。

また、小規模なサイトでは、システム構築上のセキュリティ対策を行うための体制をとることが難しく、システム構成からいっても、予算あるいはスペースの問題等により決して十分な対策がとられていない。

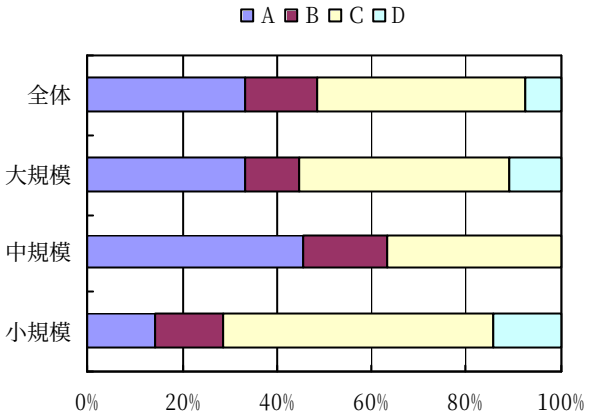
11.2 設問ごとの分析結果

11.2.1 セキュリティ面からのシステム構成についての検討

分析結果から見た傾向は、以下の通り。

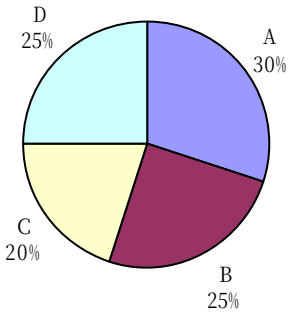
- 組織的に対策を行っているサイトは、全体の半数にすぎない。特に小規模サイトでは、専門家を交えた検討体制さえとることが難しそうである。
- システム構築時のセキュリティ検討を組織的に行っているサイトは、小規模サイトで 1／3弱に止まっており、大規模サイトでさえも約半数しかない。
- システム構成のセキュリティ検討体制については、サイト規模が大きいほど、外部の専門家を活用している傾向がある。一方小規模サイトでは、社内の要員だけで取組まざるを得ない状況がうかがえる。

(1) システム構築時におけるセキュリティ面からの 検討状況



(A)専門的な技術の裏付けのもと組織的に検討が十分に行われており、セキュリティ対策面からの要求はすべて適切に反映されており、セキュアな構成として自信がある
(B) 組織的な検討は行われたが、サイトのセキュリティポリシーや個別対策を完全に反映しているとは言い難い
(C) 担当者レベルで一通りの検討が行われているが、専門家の指導やチェックは受けておらず、十分な検討が行われているとは言えない
(D) セキュリティ面はほとんど考慮していない

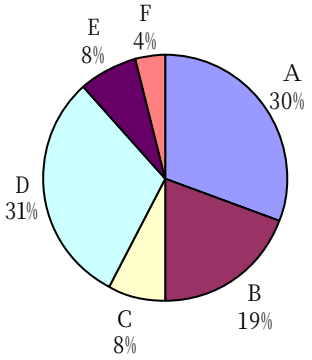
【検討が不十分な理由】



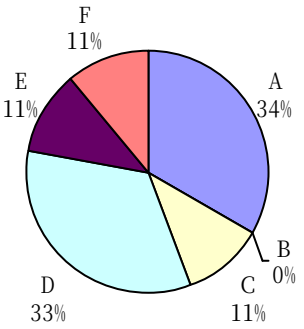
(A) セキュリティについての意識が低く、検討が行われなかったため
(B) 実際の脅威は少ないと見てセキュリティ対策を重要視しなかったため
(C) 検討を実施できる人材がいないため
(D) 予算に制限があるため

(2) サイトシステム構成の検討体制

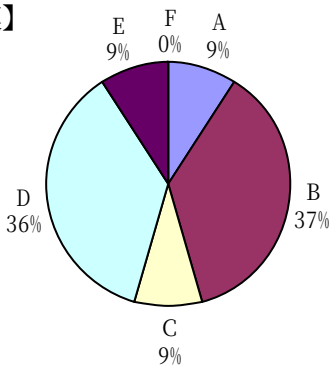
【全体】



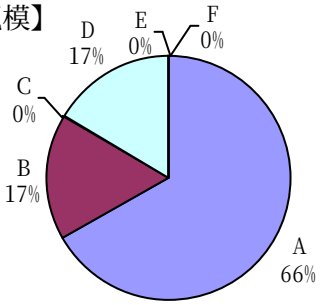
【大規模】



【中規模】



【小規模】

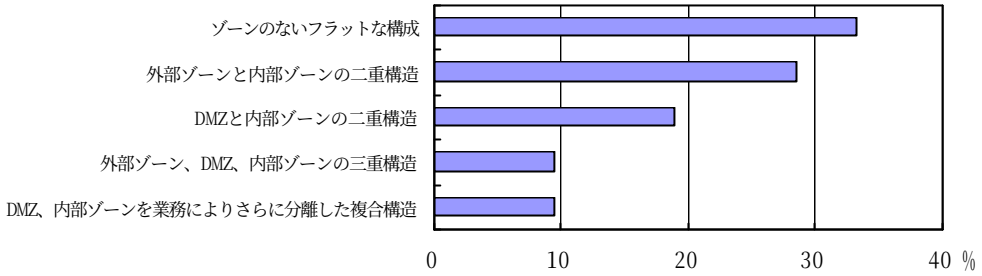


(A) 自社の要員だけで実施　　(B) システムベンダーの助言を得て自社要員で実施
(C) セキュリティ専門コンサルタントの助言を得て自社要員で実施　(D) システムベンダーの提案を採用
(E) セキュリティ専門コンサルタントの提案を採用
(F) システムベンダーに加え、セキュリティ専門コンサルタントも参画

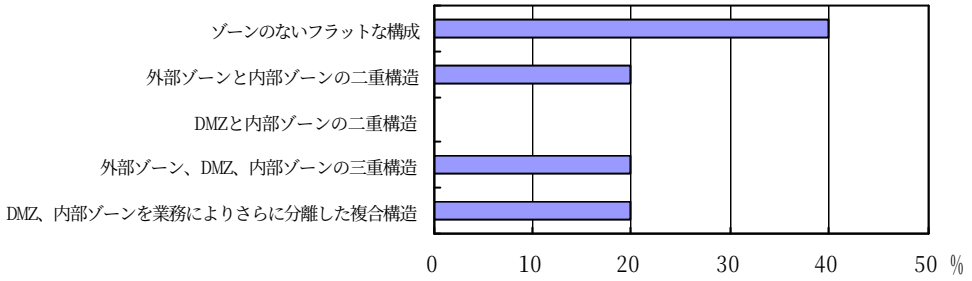
(3) ゾーン分割

① サイトシステムの構成

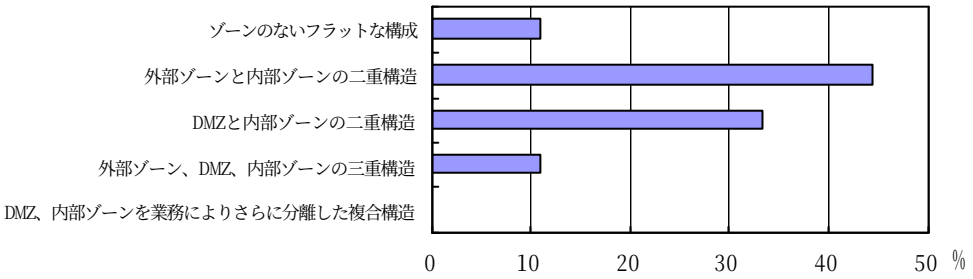
【全体】



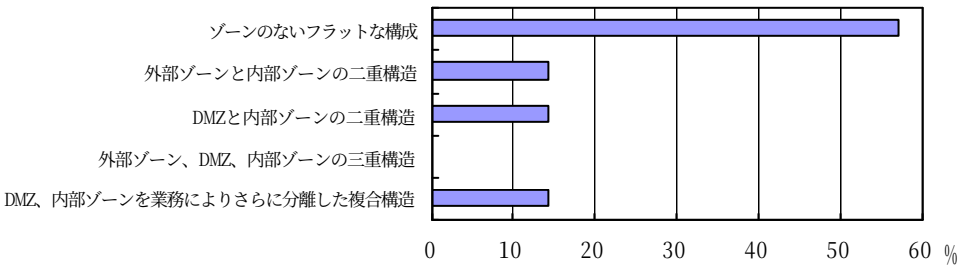
【大規模】



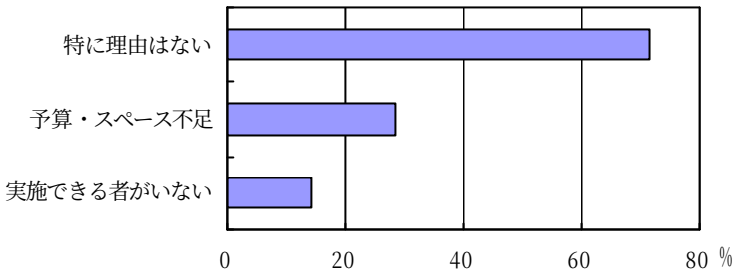
【中規模】



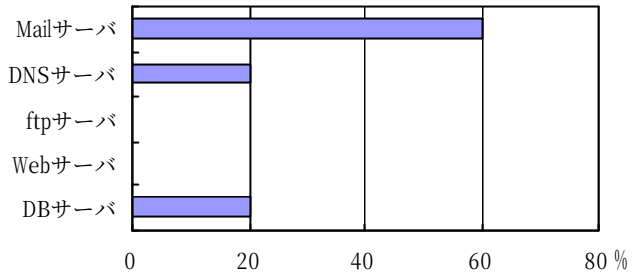
【小規模】



② ゾーンを構成しない場合の理由



③ DMZ に配置しているサーバ



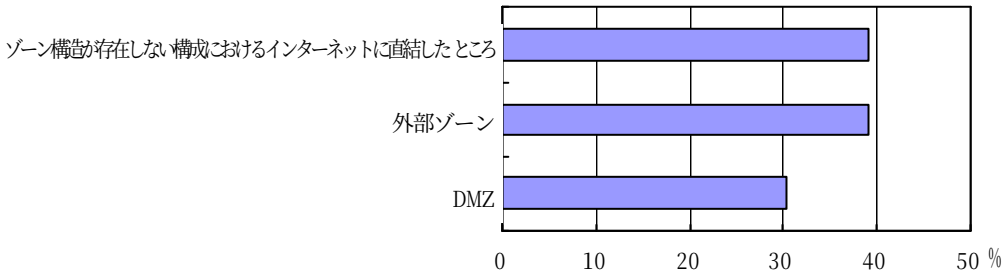
11.2.2 Web サーバのシステム構成上の配置とセキュリティ対策についての配慮

分析結果から見た傾向は、以下の通り。

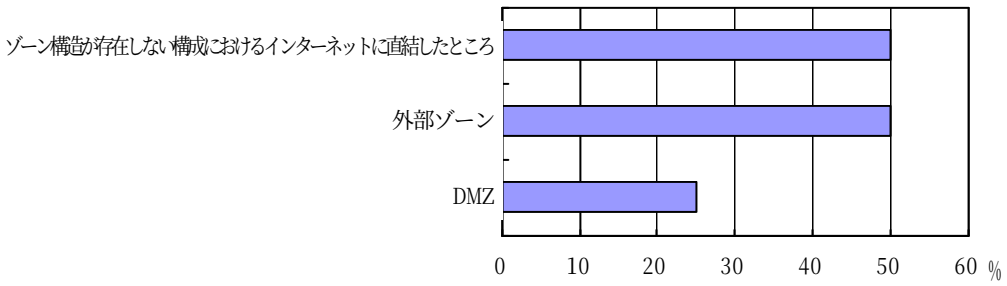
- Web サーバの他サービスからの隔離状況を見ると、Web サーバが攻撃されることによるシステム全体への影響よりも、サーバ運営の利便性の方が重視されている。
- サーバ構築上のセキュリティに関する配慮は大体なされているようである。一方、配慮が十分になされていない場合の理由としては、サーバ構築上のセキュリティ対策方法がわからないことがトップである。

(1) システム構成上の位置

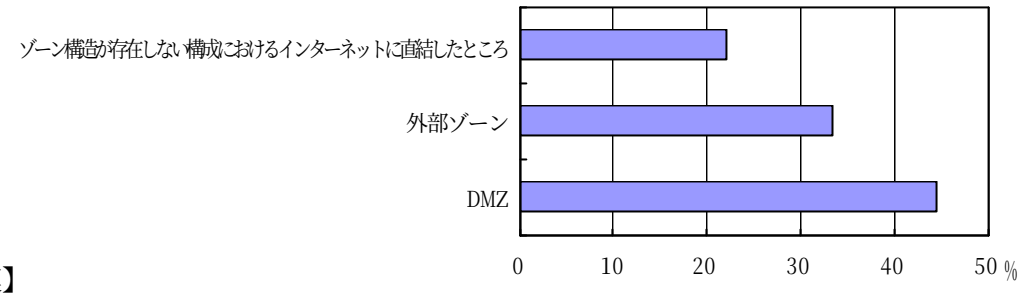
【全体】



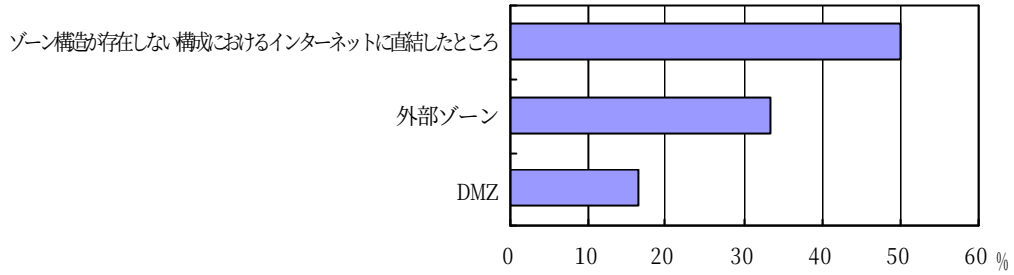
【大規模】



【中規模】

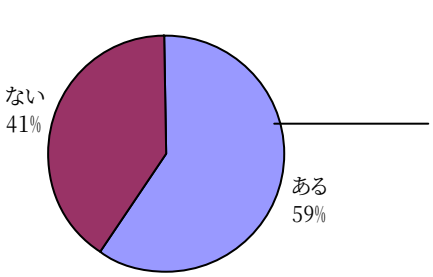


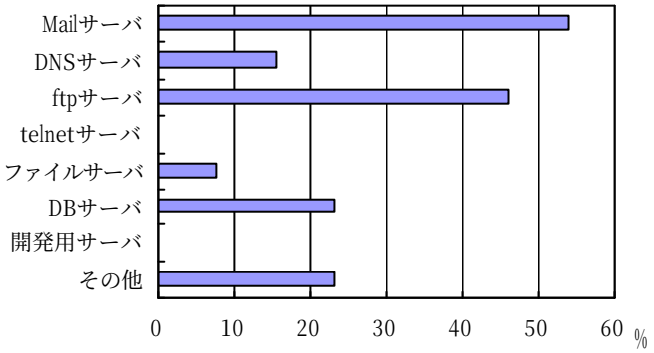
【小規模】



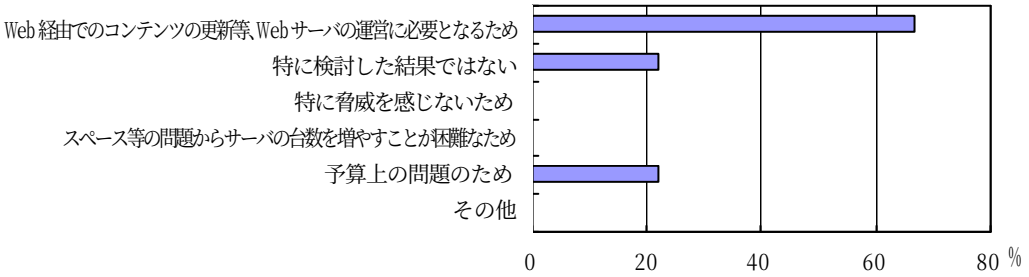
(2) 他のサービスからの隔離状況

① Web サーバに搭載しているサービス

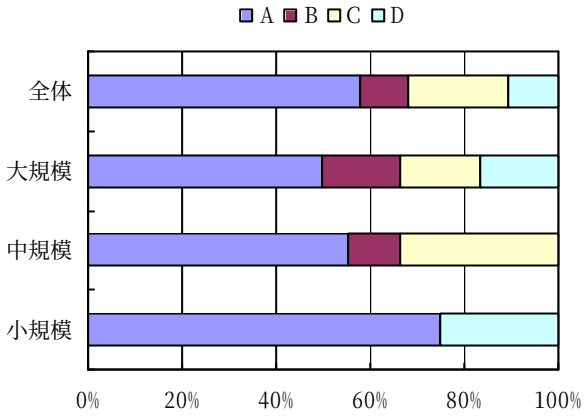




【搭載している理由】

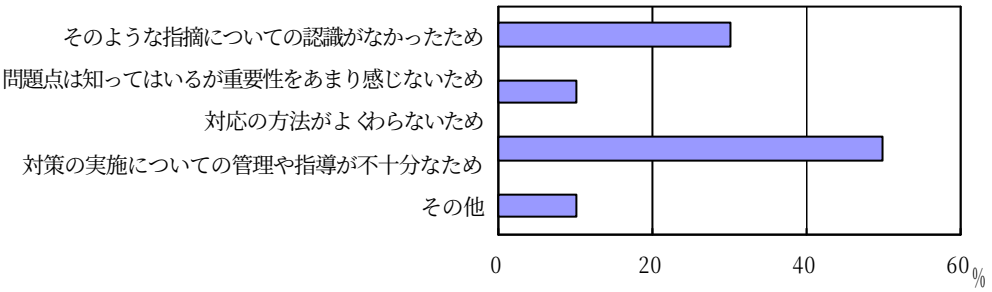


② サーバ構築上のセキュリティ上の配慮



（A）システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
(B) 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
(C) 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
(D) 特に対策は考えていない

【上で(C)または（D）を選択した理由】



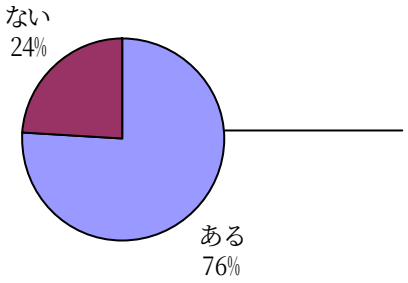
11.2.3 Mail サーバのシステム構成上の配置とセキュリティ対策についての配慮

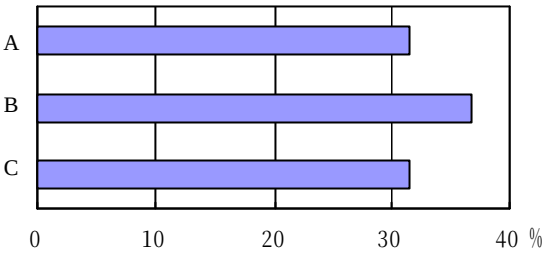
分析結果から見た傾向は、以下の通り。

- 多くのサイトがセキュリティ上の配慮を行っている。
- サーバ構築上のセキュリティに関する配慮はおおよそなされているようである。一方、配慮が十分になされていない場合の理由としては、サーバ構築上のセキュリティ対策方法がわからないことがトップである。

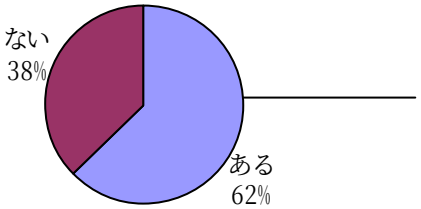
(1) システム構成上の位置

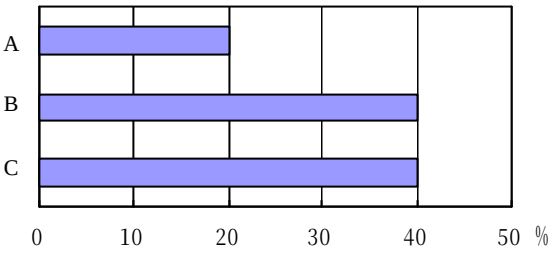
【全体】



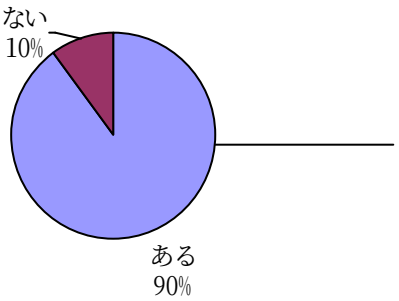


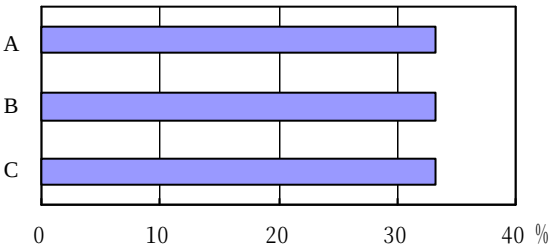
【大規模】



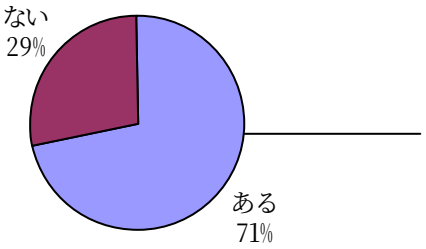


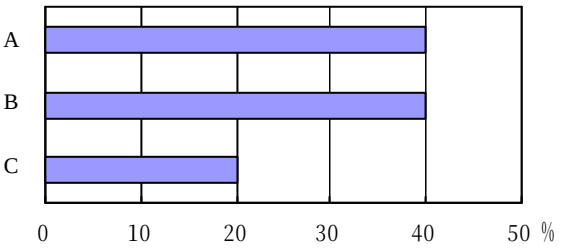
【中規模】





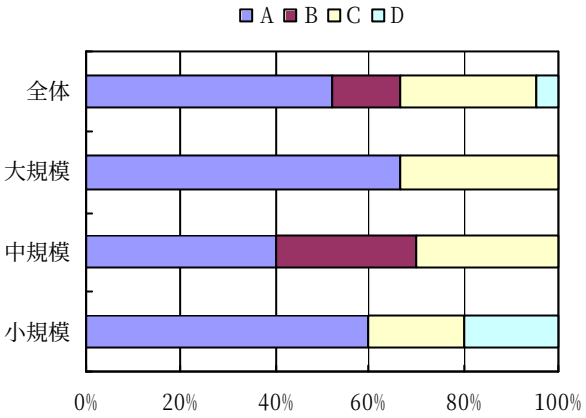
【小規模】





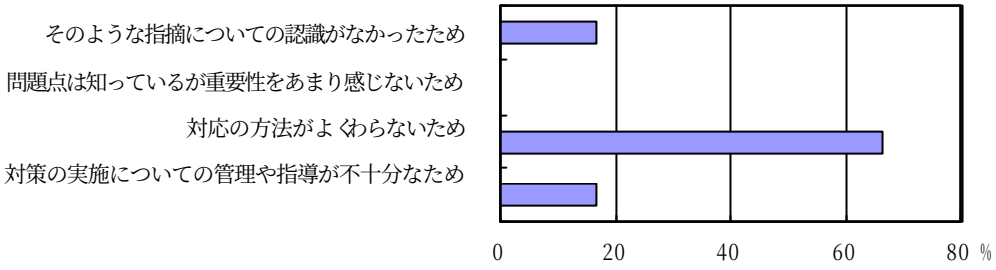
(A) ゾーン構造が存在しない構成におけるインターネットに直結したところ
(B) 外部ゾーン
(C) DMZ

(2) サーバ構築上のセキュリティ上の配慮



（A）システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
(B) 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
(C) 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
(D) 特に対策は考えていない

【上で(C)または (D)を選択した理由】



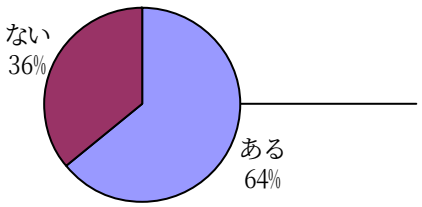
11.2.4 ftp サーバのシステム構成上の配置とセキュリティ対策についての配慮

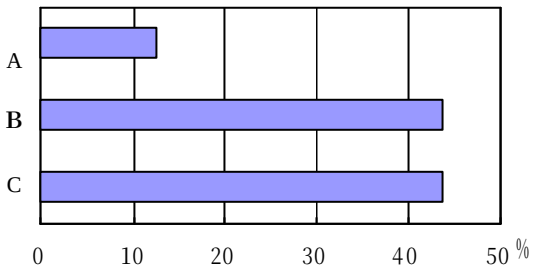
分析結果から見た傾向は、以下の通り。

- 多くのサイトがセキュリティ上の配慮を行っている。

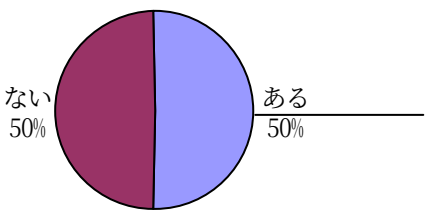
(1) システム構成上の位置

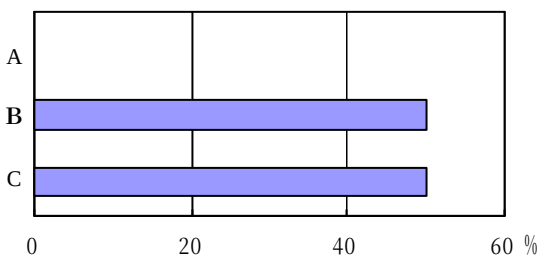
【全体】





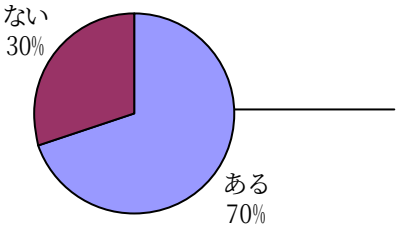
【大規模】

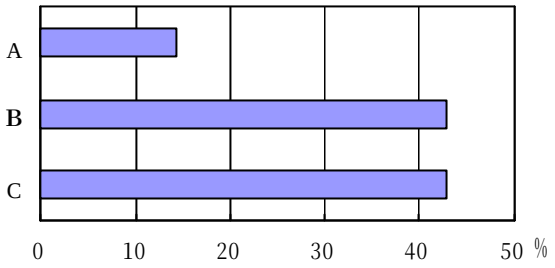




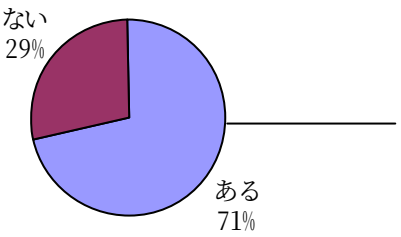
（A）ゾーン構造が存在しない構成におけるインターネットに直結したところ
(B) 外部ゾーン
(C) DMZ

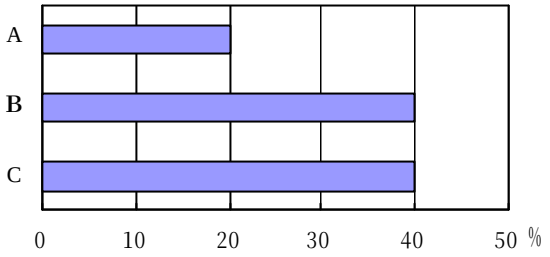
【中規模】





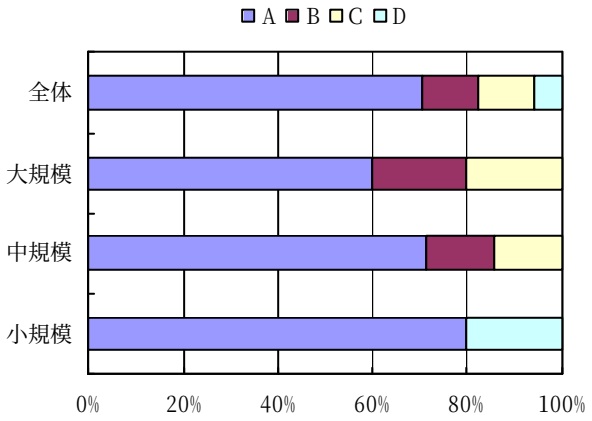
【小規模】





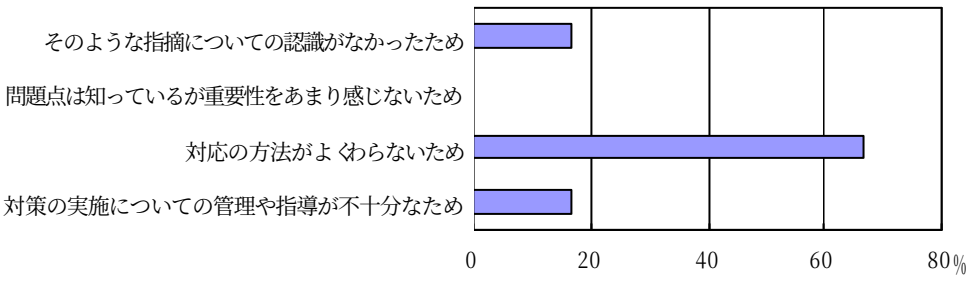
(A) ゾーン構造が存在しない構成におけるインターネットに直結したところ
(B) 外部ゾーン
(C) DMZ

(2) サーバ構築上のセキュリティ上の配慮



(A) システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
(B) 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
(C) 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
(D) 特に対策は考えていない

【上で(C)または(D)を選択した理由】



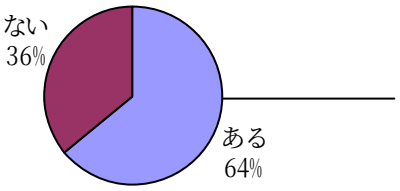
11.2.5 DB サーバのシステム構成上の配置とセキュリティ対策についての配慮

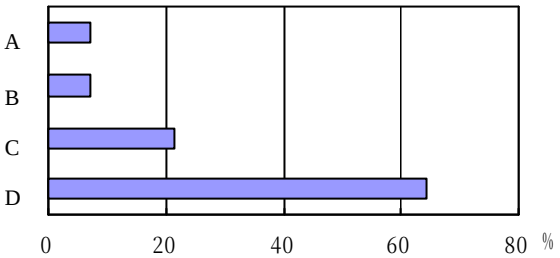
分析結果から見た傾向は、以下の通り。

- 脅威は認識されており、やむを得ない理由がない限り、対策はとられている。
- 他サービスからの隔離状況に関しては、他サービスと同居しないようにしているか、または脅威を認識した上でスペース・予算等の問題でやむを得ず同居させているという結果となっている。
- サーバ構築上のセキュリティ上の配慮はかなりなされているようである。

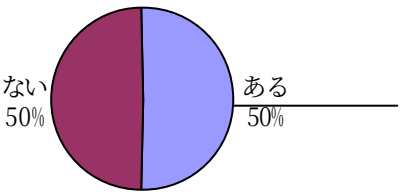
(1) システム構成上の位置

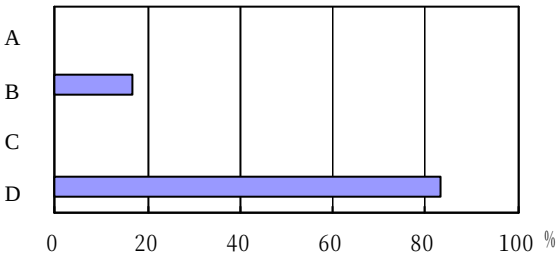
【全体】



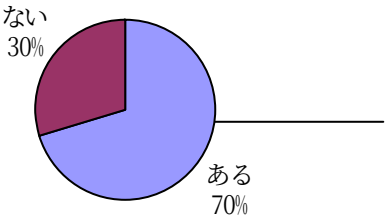


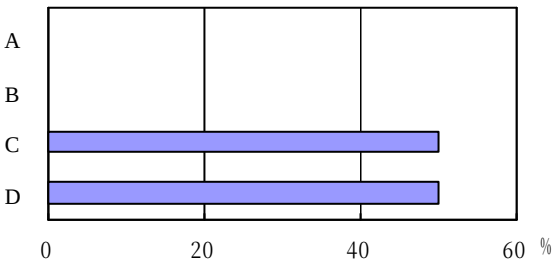
【大規模】



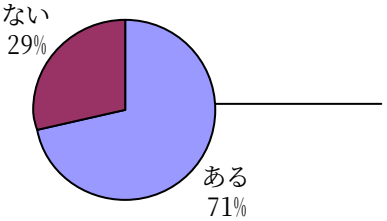


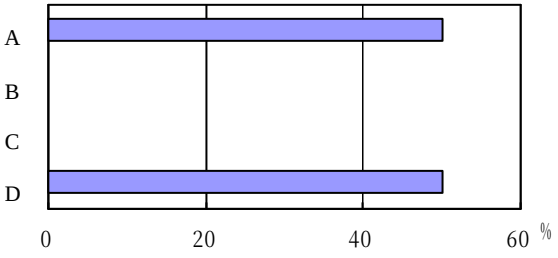
【中規模】





【小規模】

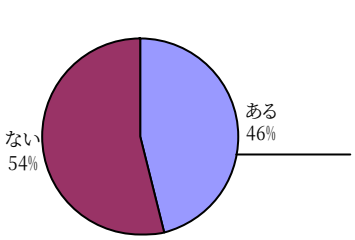


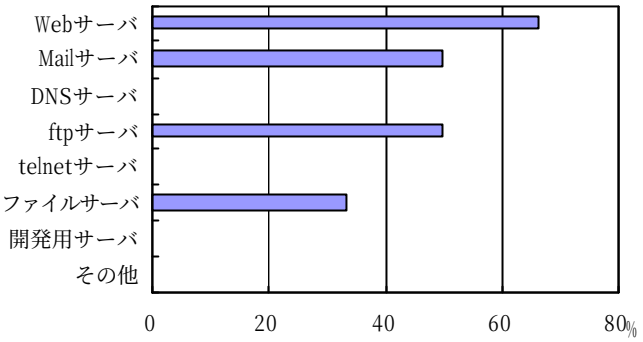


（A）ゾーン構造が存在しない構成におけるインターネットに直結したところ
(B) 外部ゾーン
(C) DMZ
(D) 内部ゾーン

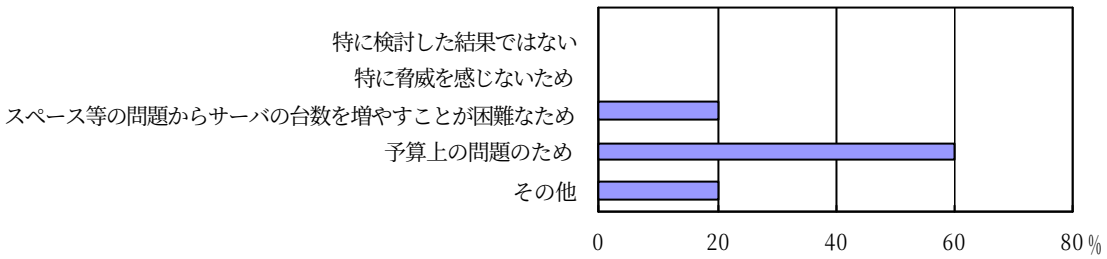
(2) 他のサービスからの隔離状況

① DB サーバに搭載しているサービス

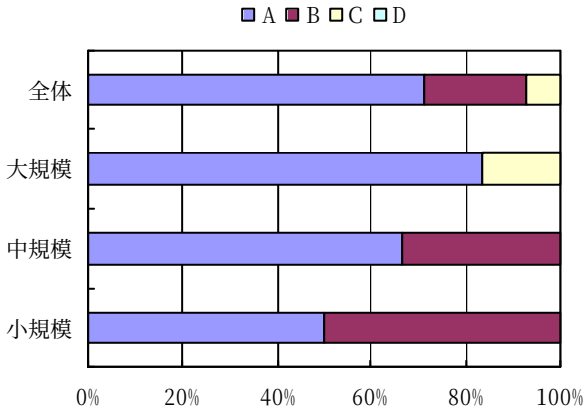




【搭載している理由】

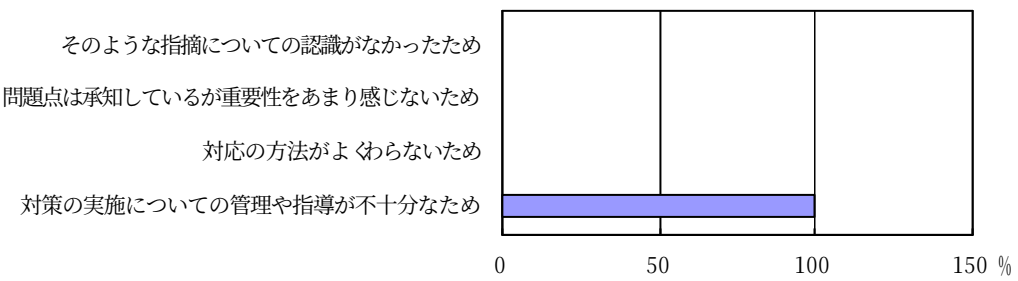


(3) サーバ構築上のセキュリティ上の配慮



（A）システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
(B) 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
(C) 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
(D) 特に対策は考えていない

【上で(C)または（D）を選択した理由】



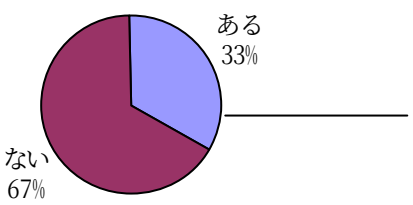
11.2.6 ファイルサーバのシステム構成上の配置とセキュリティ対策についての配慮

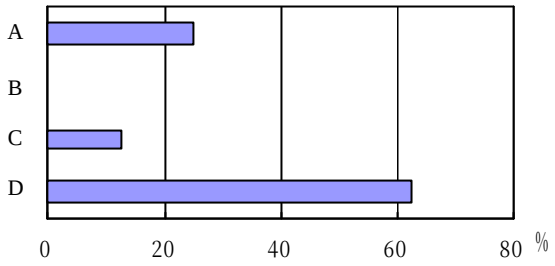
分析結果から見た傾向は、以下の通り。

- ゾーン構成をとっているところについては、内部ゾーンあるいは DMZ に配置している。

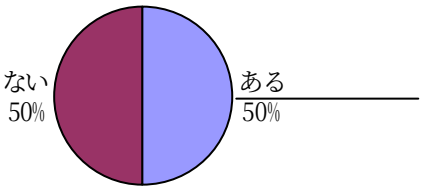
(1) システム構成上の位置

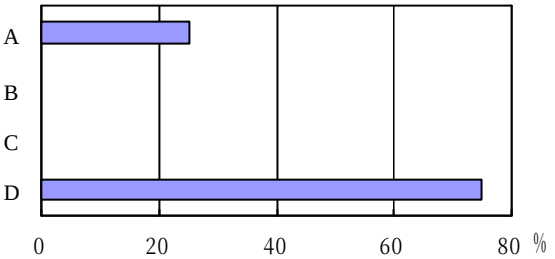
全体



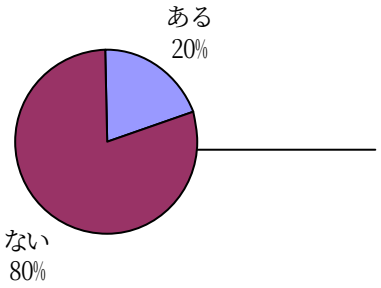


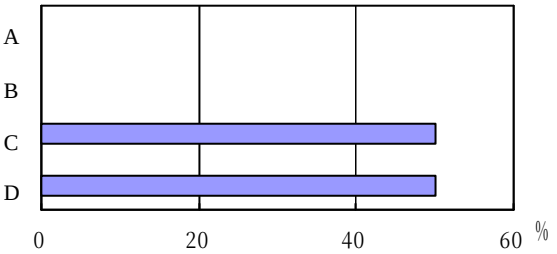
大規模



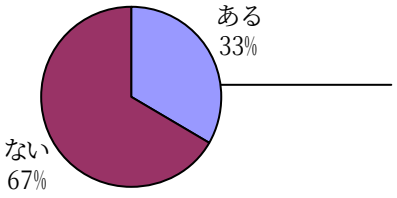


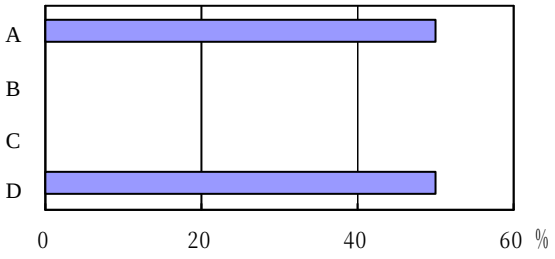
中規模





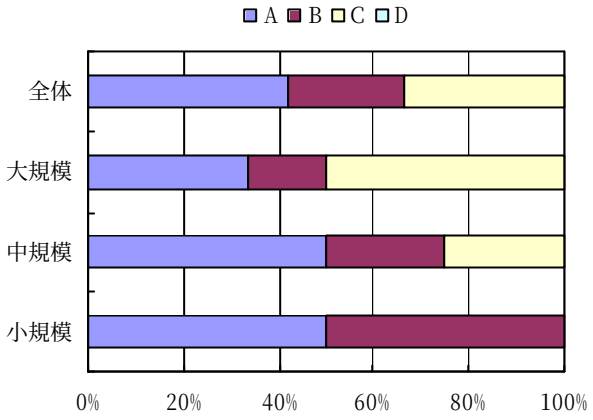
小規模





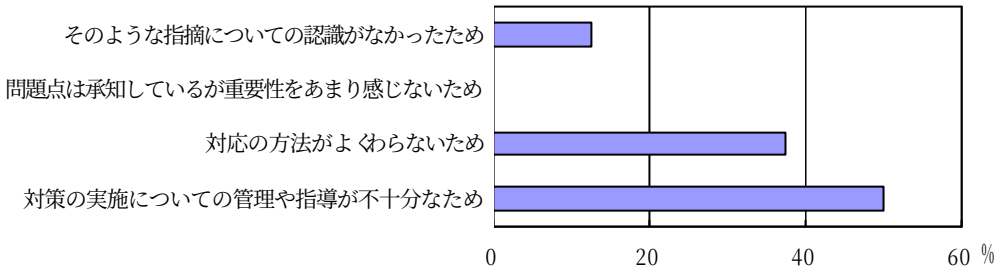
(A) ゾーン構造が存在しない構成におけるインターネットに直結したところ
(B) 外部ゾーン
(C) DMZ
(D) 内部ゾーン

(2) サーバ構築上のセキュリティ上の配慮



（A）システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
(B) 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
(C) 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
(D) 特に対策は考えていない

【上で(C)または(D)を選択した理由】



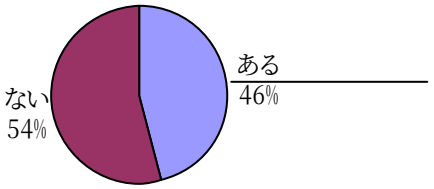
11.2.7 開発環境のシステム構成上の配置とセキュリティ対策についての配慮

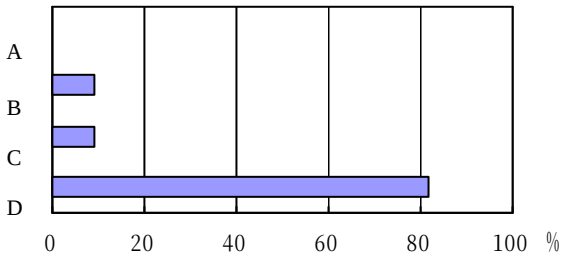
分析結果から見た傾向は、以下の通り。

- 小規模サイトでは、開発環境を運用環境と分けることの難しさがうかがえる。
- 一方、大規模サイトでは十分な対策がとられている。

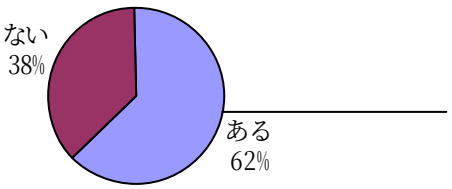
(1) システム構成上の位置

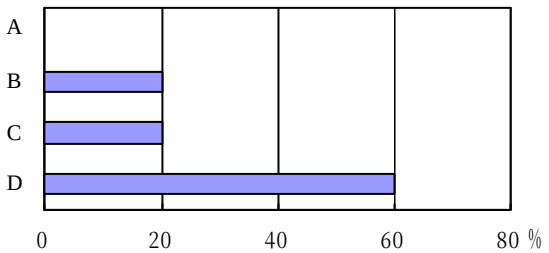
【全体】





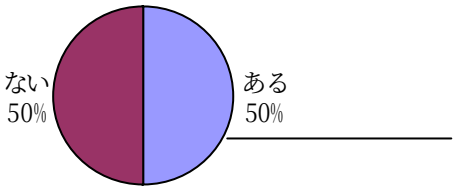
【大規模】

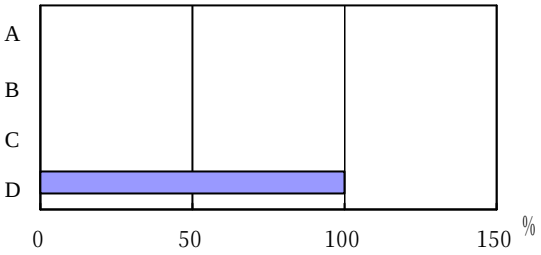




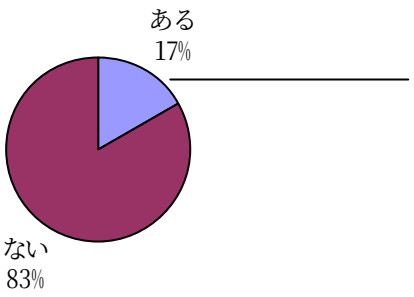
（A）ゾーン構造が存在しない構成におけるインターネットに直結したところ
(B) 外部ゾーン　　(C)DMZ　　(D) 内部ゾーン

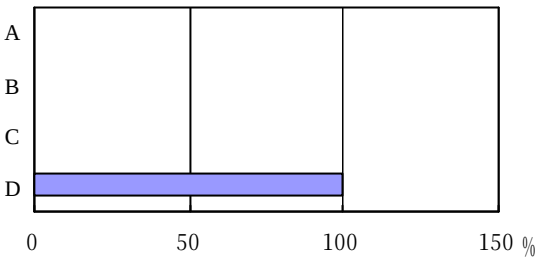
【中規模】





【小規模】



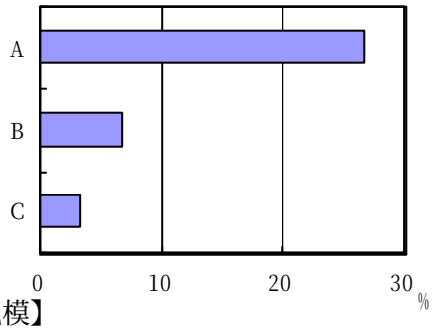


（A）ゾーン構造が存在しない構成におけるインターネットに直結したところ
（B）外部ゾーン　　（C）DMZ　　（D）内部ゾーン

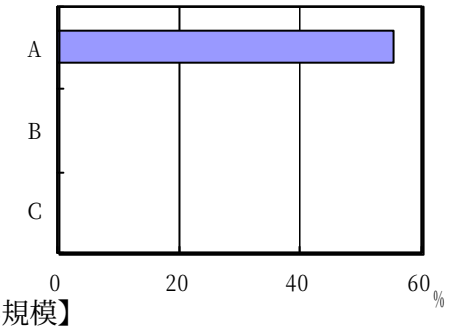
(2) 運用環境からの隔離状況

① 開発環境と運用環境の位置関係

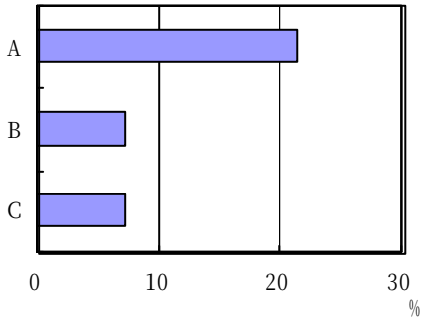
【全体】



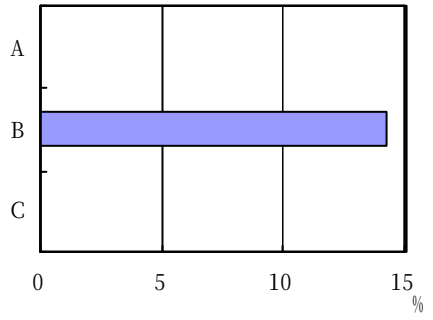
【大規模】



【中規模】

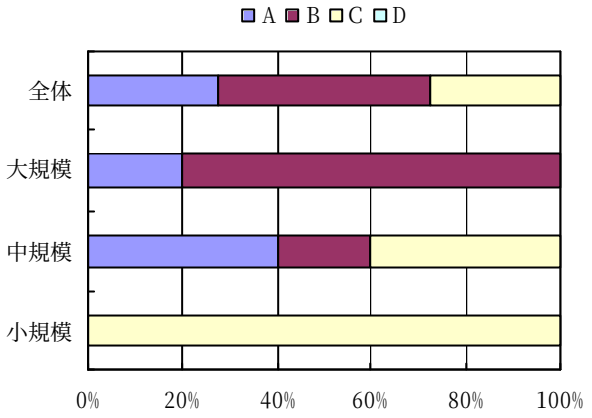


【小規模】



（A）運用環境は開発環境とネットワークレベルで隔離（異なったゾーンに配置）
（B）開発環境と運用環境は同じゾーンに置かれているがマシンは分離
（C）開発環境は、運用で用いられている（一部の）サービスと同一マシン上に同居

② 隔離状況



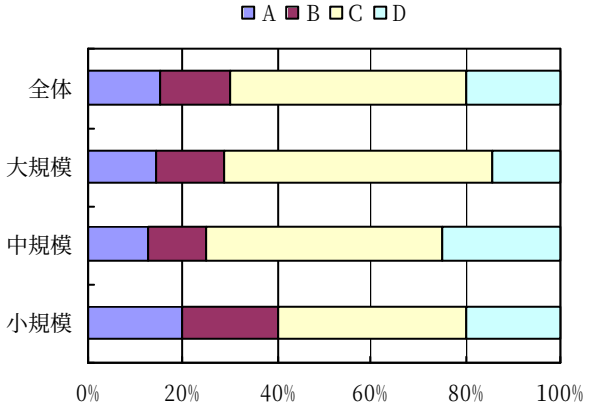
(A) 開発環境と運用環境間の通信はできず、開発環境は運用環境から完全に隔離されている
(B) 開発環境と運用環境間の一般の通信は制限され、必要な通信も厳格な管理のもとに行っており、問題が生じる可能性は低い
(C) 開発環境と運用環境間の通信の制限は厳格でなく、担当者の注意に依存しているところもあり、問題を起こす可能性も低くはない
(D) 開発環境と運用環境間の通信に対する特別の管理は行っていない

11.2.8 自社で開発するソフトウェアへの必要なセキュリティ機能の実装

分析結果から見た傾向は、以下の通り。

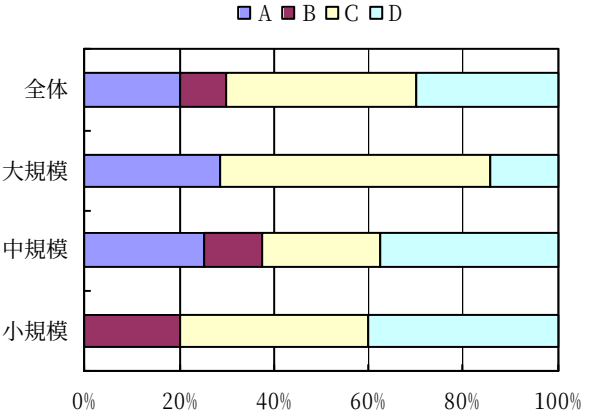
- 全般的に十分な対応がとれていない。

(1) セキュリティ機能の指定



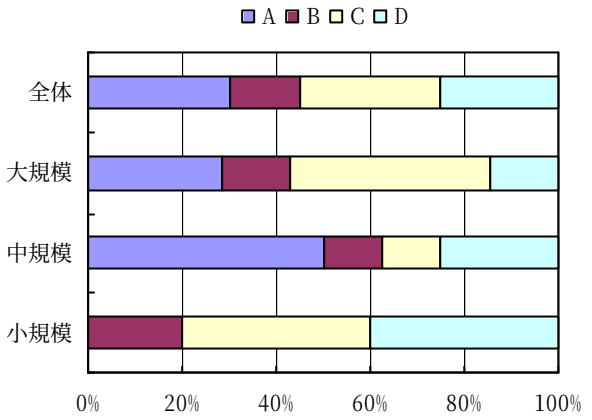
(A) 設計レビューの中に必要となるセキュリティ機能についての第三者チェックが行われており、すべてのソフトウェアに必要なセキュリティ機能は適切に指定されている
(B) 設計レビューの中で必要となるセキュリティ機能についての第三者チェックは義務付けられているが、厳格には運用されてなく、問題が見過ごされている可能性もある
(C) ソフトウェアの設計担当者レベルでのチェックは義務付けられているが、第三者的なチェックは行われていない
(D) チェック実施も義務付けられてなく、実質的に無管理の状態

(2) セキュリティ機能の実装



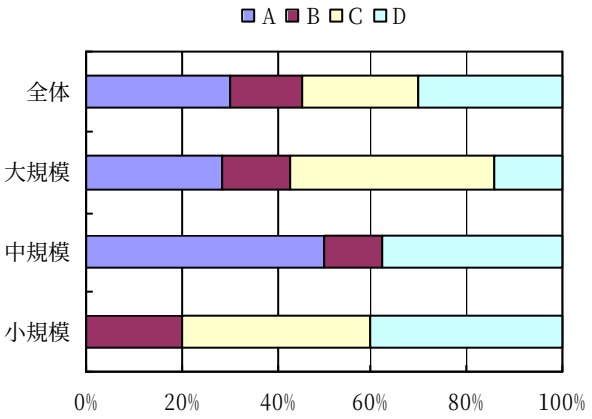
(A) 組織的なチェックが行われており、ミスが見逃される余地はほとんどない
(B) 確認プロセスおよびチェックの体制もあるが、チェックに厳密さを欠き、ミスが見逃されている可能性もある
(C) 担当者レベルでのチェックは義務付けられているが、第三者的なチェックは行っていない
(D) 担当者任せで、特に管理は行われていない

(3) セキュリティ機能の動作環境確保状況



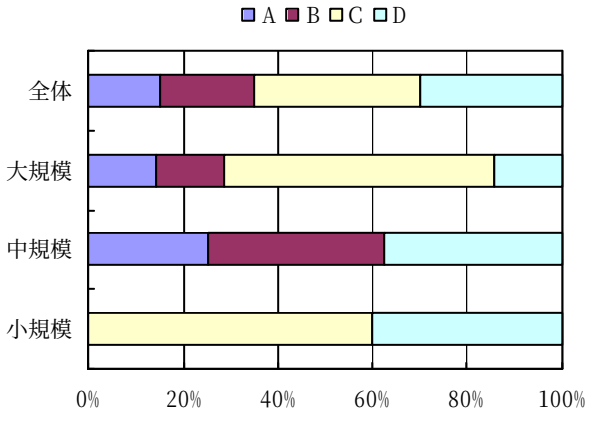
（A）システムの維持管理業務にルーチン作業として組込まれており、組織的な管理が十分に行われている
（B）システムの維持管理業務にルーチン作業として組込まれているが、厳格に運用されてなく、不備が見逃される可能性もある
(C) 担当者レベルでの管理は行われているが、組織的な管理は行われていない
(D) 担当者任せで、特に管理は行われていない

(4) 業務、システム構成の変更にともなうセキュリティ機能変更への取組状況



（A）システムの維持管理業務にルーチン作業として組込まれており、組織的な管理が十分に行われている
（B）システムの維持管理業務にルーチン作業として組込まれているが、厳格に運用されてなく、不備が見逃される可能性もある
(C) 担当者レベルでの管理は行われているが、組織的な管理は行われていない
(D) 担当者任せで、特に管理は行われていない

(5) 開発時に脆弱性を残さないための配慮



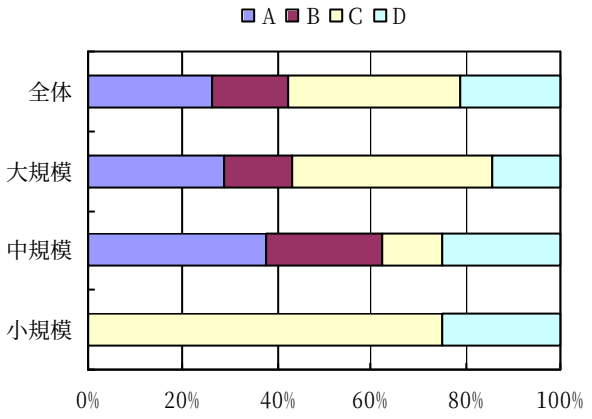
(A) これらの脆弱性を検知するプロセスがシステムの維持管理業務にルーチン作業として組込まれており、厳格に運用されていて、不備が見逃されている可能性はほとんどない
(B) これらの脆弱性を検知するプロセスがシステムの維持管理業務にルーチン作業として行われることになっているが、厳格に運用されてなく、不備が見過ごされている可能性もある
(C) 担当者に地位を喚起しており、担当者レベルでのレビューは行われているが、組織的な管理は行われていない
(D) 担当者任せで、特に管理はされていない

11.2.9 自社で開発するソフトウェアに対する保護

分析結果から見た傾向は、以下の通り。

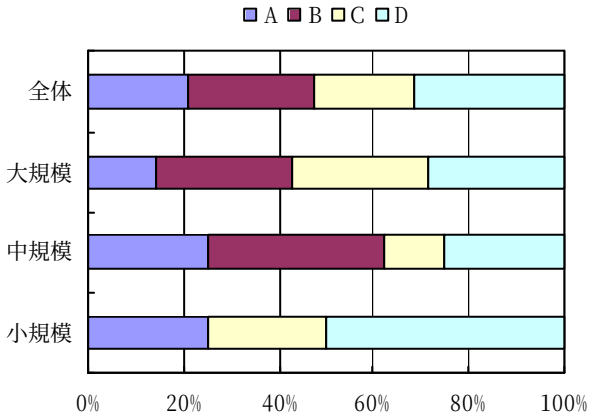
- やはり、小規模サイトでは組織的な管理ができていない。

(1) 開発プロセスの管理



Ⓐ 必要な管理はすべて開発プロセスに組込んでおり、厳格に運用している
Ⓑ 必要な管理はすべて開発プロセスに組込んでいるが、厳格に運用されていないため、問題が見逃されている可能性もある
Ⓒ 問題意識はあるが、その実行は開発担当者に任されている
Ⓓ 特に行っていない

(2) 開発を外部委託する場合の、委託先でのセキュリティ管理



Ⓐ 必要な事項は契約あるいはそれに準ずる文書で明示しており、また、適宜必要な監督や指導を行っている
Ⓑ 必要な事項は契約あるいはそれに準ずる文書で明示しているが、監督や指導までは行っていない
Ⓒ 問題意識はあるが、開発担当者の意識に任されている
Ⓓ 特に行っていない

12 システムの運用と業務現場におけるセキュリティ対策

本章では、EC サイトにおけるシステムの運用と業務現場におけるセキュリティ確保への取組状況について分析を行う。

分析項目については、以下の通り。

- システム運用における不手際防止への取組み
- システム構成の維持管理
- 攻撃への備え
- 脆弱点の把握および対策
- 業務における不手際防止への取組み
- システムの物理的な保護

12.1 “システムの運用と業務現場におけるセキュリティ対策”全体を通しての傾向

システムの運用や業務現場での運用については全般的にセキュリティに対する認識が薄く、この点は改善が必要である。

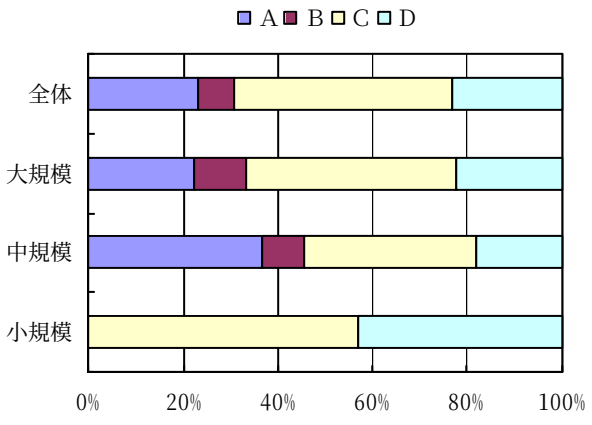
12.2 設問ごとの分析結果

12.2.1 システム運用における不手際防止への取組み

分析結果から見た傾向は、以下の通り。

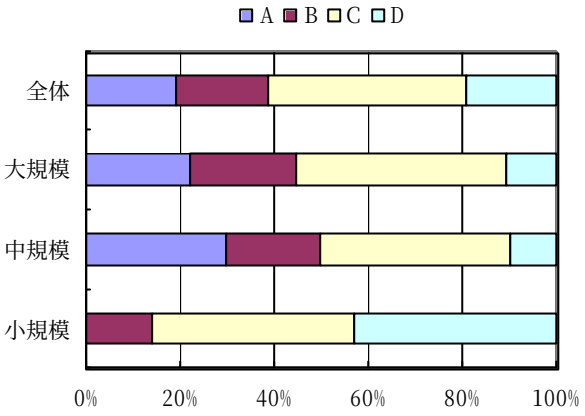
- セキュリティ要求事項は運用規程や運用マニュアルに反映されておらず、組織的な取組みが薄い。
- 実施面を見ても、運用面でのセキュリティ対策としての工夫は少なく、担当者の教育についても不十分である。

(1) システムの運用に係るセキュリティ要求事項の指定状況



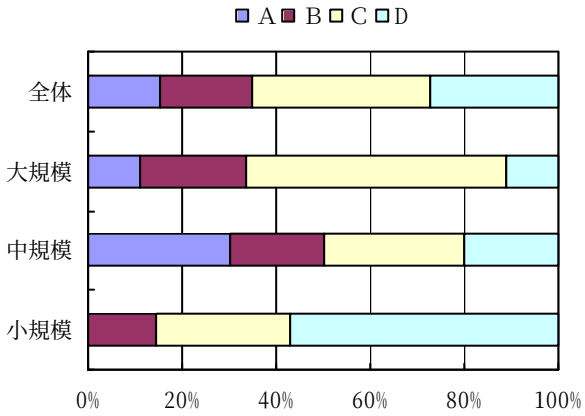
（A）システム運用に対するセキュリティ要求事項の指定は、関係者によりレビューされており、運用規程や運用マニュアルも常にサイトの運用環境やセキュリティ対策を反映したものが維持されている
（B）システム運用に対するセキュリティ要求事項の指定は、関係者によりレビューされるとともに、運用規程や運用マニュアルへのセキュリティ対策の反映も、確立したプロセスの中で行われることになっているが、その運用は厳格でなく、セキュリティ対策のシステム運用への反映に漏れが生じている可能性もある
(C) 担当者レベルの努力に依存しているが、システム運用へのセキュリティ対策の反映についての確立したプロセスや、運用規程や運用マニュアルについてのセキュリティ面からの組織的な管理は行われていない
（D）セキュリティ対策とシステム運用の連携はあまりとられていない

(2) システム運用を確実なものにするための施策



(A) さまざまな工夫がシステム運用の中に組込まれ、その実行も厳格に管理されており、システム運用上不手際が発生あるいは見逃される可能性はほとんどない
(B) さまざまな工夫がシステム運用の中に組込まれているが、その実行は徹底しているとは言い難く、不手際を発生させたり見逃したりする可能性もある
(C) 担当者レベルでの工夫は見られるが、組織的な管理は行われておらず、不手際を発生させそれが見逃されていても不思議ではない
(D) 特別な工夫はなされていない

(3) システム運用者へのセキュリティ教育



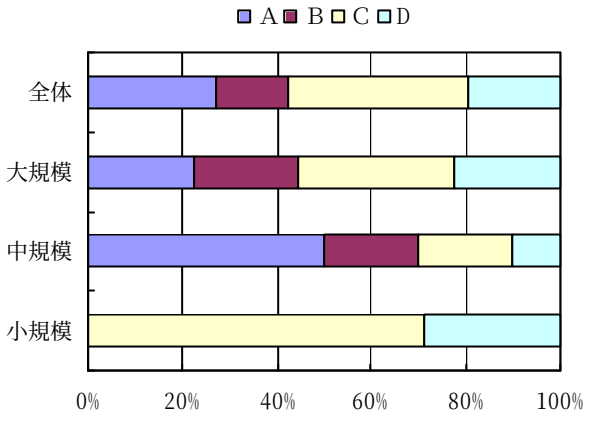
(A) 検討された計画のもとで教育を行っており、システム運用関係者の責任意識ならびに要求事項についての理解は十分である
(B) 教育を行っているが、関係者の責任意識ならびに要求事項に対する理解については十分とは言い難い
(C) 特別に教育は行われていないが、関係者にセキュリティはおおむね責任意識ならびに要求事項に対する理解を有していると考えている
(D) 特に行われておらず、関係者の責任意識ならびに要求事項に対する理解については不安がある

12.2.2 システム構成の維持管理

分析結果から見た傾向は、以下の通り。

- 個別の脅威対策等で決定された要求事項のシステムや機器設定への反映状況を見ると、組織的に手順が決められているサイトは多くない。小規模なサイトほどこの傾向が強い。
- 開発されたプログラムライブラリの管理についても、ほぼ同じ傾向である。

(1) セキュリティ要求事項のシステム構成への反映状況



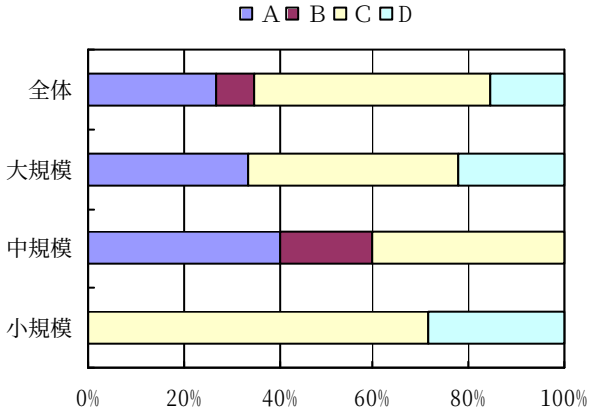
(A)十分な検討の下で設計されており、運用環境への適合性についての定期的なチェックも行われており、常に、システム構成方針に沿っており、セキュリティ対策面からの要求を完全に満たしているものとして維持されている

(B)当初の設計は十分な検討のもとに行われたが、システム構成の変更に際してのレビューは厳格でなく、部分的にシステム構成方針からずれたところも出る可能性がある

(C)明示されたシステム構成方針はないが、システム構成はサイトの運営実態から見て、おおむねセキュリティ対策面からの要求を満たしている

(D)セキュリティ面からのシステム構成の評価は行っていない

(2) セキュリティ要求事項の機器設定への反映状況



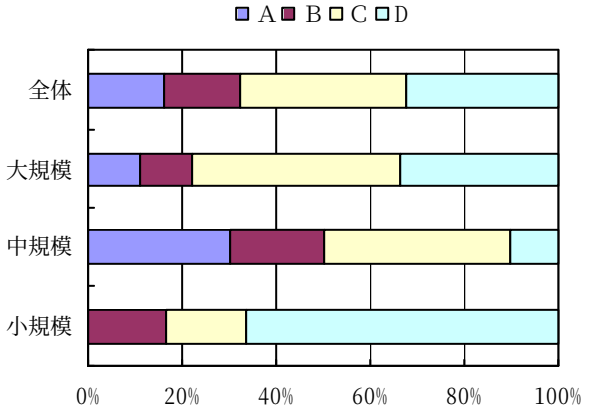
(A) 各機器に対する諸設定は確立した手順に沿って行い、厳格なチェックも行っている。ミスが見逃されている可能性はほとんどない

(B)各機器に対する諸設定は確立した手順に沿って行い、組織的なチェックを行うことになっているが、その運用が厳格でなく、ミスが見逃されている可能性もある

(C) 確立した手順や組織的なチェックはなく、担当者の注意と努力に依存しているが、おおむね適切に行われている

(D) 各機器に対する諸設定はほとんど管理されておらず、設定内容の把握も十分でない

(3) システム構成および機器設定の把握状況



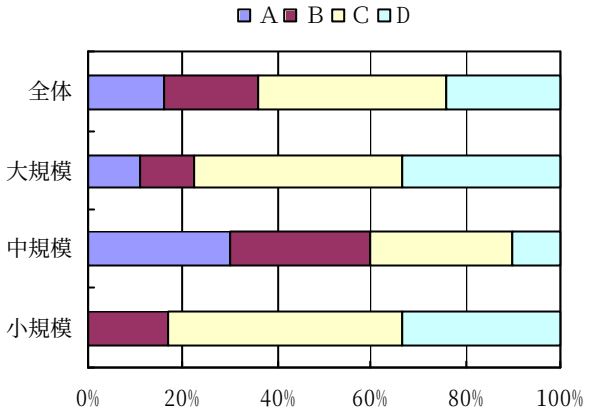
(A) 正確なドキュメントが漏れなく整備されている

(B) ドキュメントは作成されているが、メンテナンスが十分に行われておらず、正確さについては多少疑問がある

(C) ドキュメント化は一部に止まっており、全体としてのドキュメント化は行われていない

(D) ドキュメント化はほとんど行われていない

(4) 各種プログラムライブラリの管理



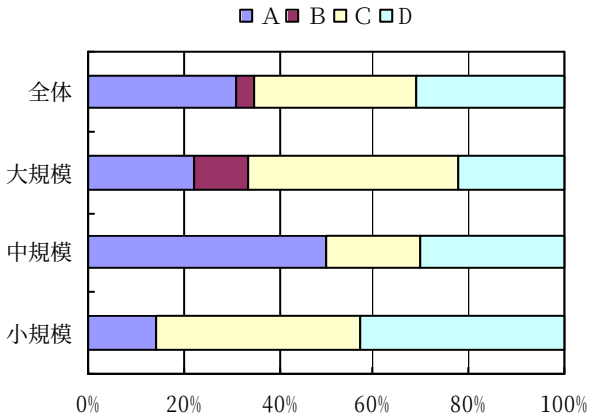
Ⓐ 確立した管理手順に沿って厳格に運用されている。問題が発生する可能性はほとんどない
Ⓑ 確立した管理手順に沿って行われることになっているが、厳格には運用されておらず、問題が発生する隙がある
Ⓒ 担当者レベルである程度の管理は行われている
Ⓓ プログラムライブラリの管理は実質的に行われていない

12.2.3 攻撃への備え

分析結果から見た傾向は、以下の通り。

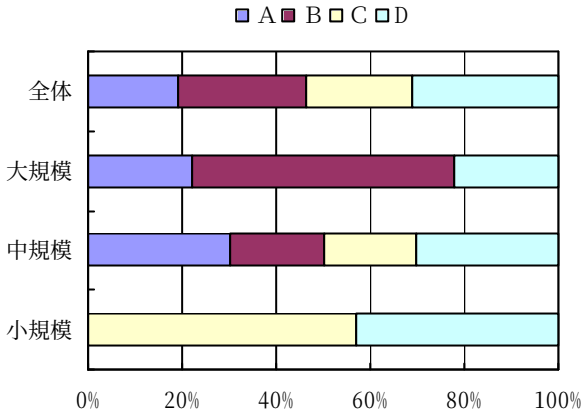
- 攻撃に対する検知については、多くのサイトで実施はされているようであるが、組織的に手順を決めて取組んでいるところは、半数にも満たない。
- Web コンテンツの改ざん検知を自動で行っているところは、全体の 1／5程度のサイトのみであり、あまり意識は高くないようである。

(1) 攻撃検知時の対応



Ⓐ 決められた手順に沿って、常に適切に行われている
Ⓑ 手順は決められているが手順通りに行われていないこともある。対応内容はおおむね適切である
Ⓒ 手順は確定していないが、担当者は習慣的に必要な処置を行っている。
Ⓓ 手順も確定しておらず、必要な処置は行われていない

(2) Web コンテンツの改ざん検知



(A) Ｗｅｂコンテンツに対し改ざん検知や自動復旧等を行う仕組みを組込んでいる。
（B）システムへの侵入の形跡が発見された場合等、必 要と判断された場合のみ改ざん検知を実施している
(C) 高い頻度でＷｅｂコンテンツを更新しており、改ざんされても大きな影響が出ないと考えているため、改ざん検知を行っていない
(D) 単に行っていない

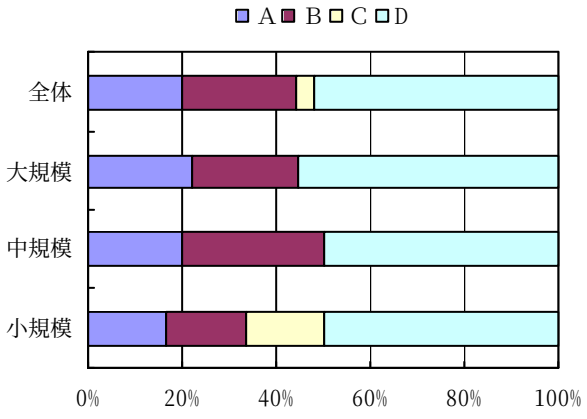
12.2.4 脆弱点の把握および対策

分析結果から見た傾向は、以下の通り。

- 脆弱性診断の実施は半数程度のサイトでしか実施されておらず、その実施結果についてほぼ活用しているサイトはまたその半数にも満たない。
- 脅威に関する情報収集を行っていないサイトは、1／3に上り、その理由として、専門的な技術能力の不足をあげているサイトが多い。
- また、脆弱点を認知した後の対応の早さについては、多くのサイトが1ヶ月以内には対処しており、この点についてはほぼ十分といえる。

(1) 脆弱性診断の実施および活用状況

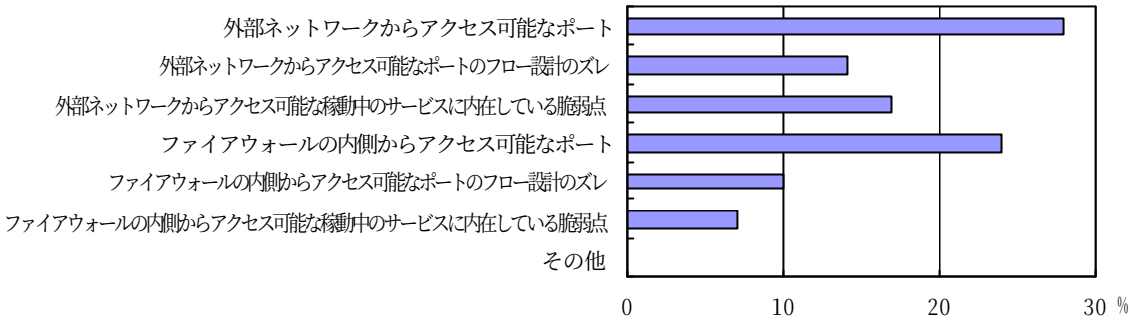
① 脆弱性診断の実施有無と形態



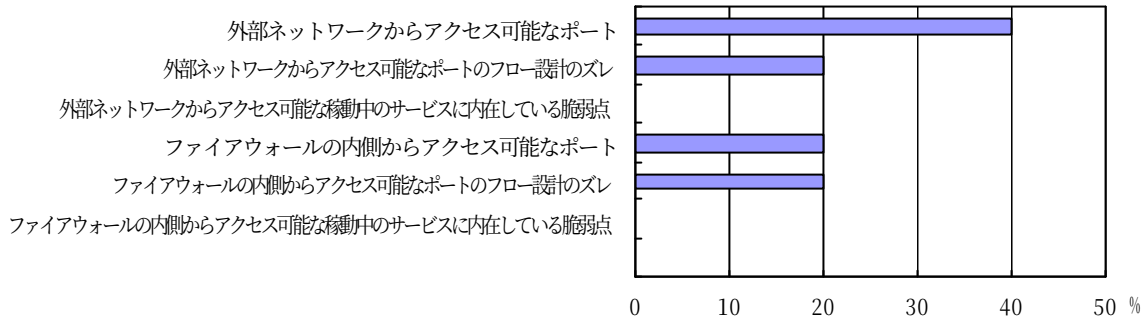
(A) 導入したツールを用い自社で実施
（B）セキュリティサービスベンダーの診断サービスを利用
(C) 無料サービスを利用
(D) 脆弱性診断は行っていない

② 実施している診断事項

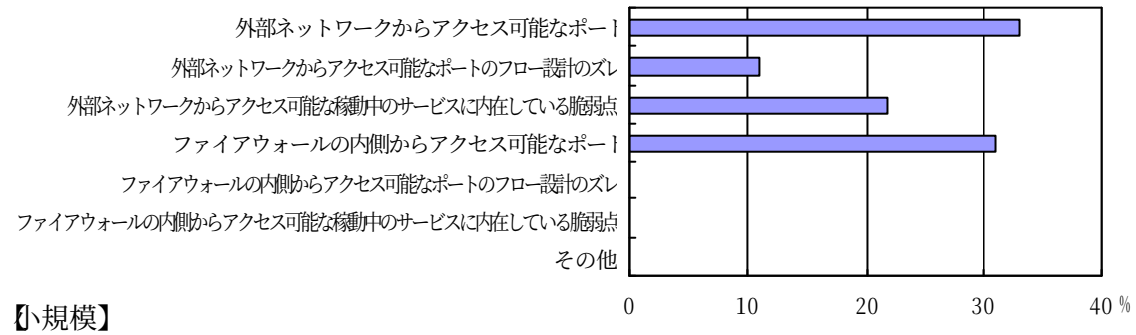
【全体】



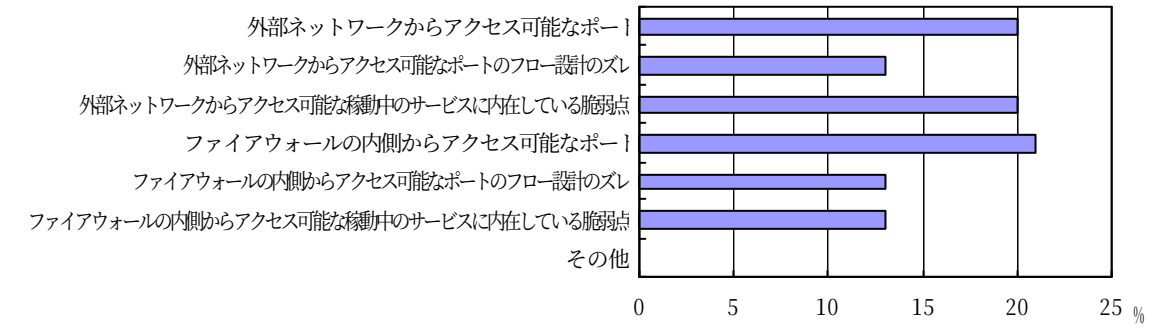
【大規模】



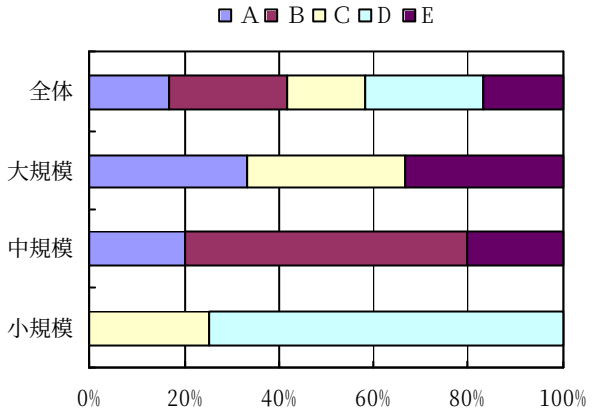
【中規模】



【小規模】



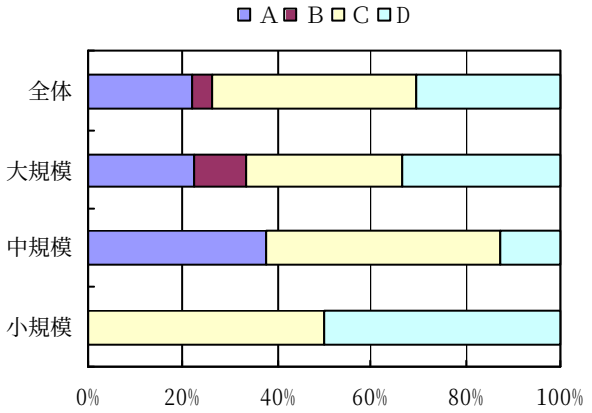
(2) 脆弱性診断結果の活用状況



Ⓐ 思わぬ問題点が指摘されておりフィードバックも迅速に行われていて、セキュリティの維持に不可欠である
Ⓑ 問題点の分析や発見した問題点の対策へのフィードバックには不満な点があるが、おおむね有効に活用されている
Ⓒ 発見された問題点への対応は一応行われているが、十分ではない
Ⓓ 診断結果は報告されているが分析や対策へのフィードバックはほとんど行われていない
Ⓔ 診断結果は十分にチェックされているが、これまでのところ問題点は見つかっていない

(3) 新たな脅威に関する情報の把握

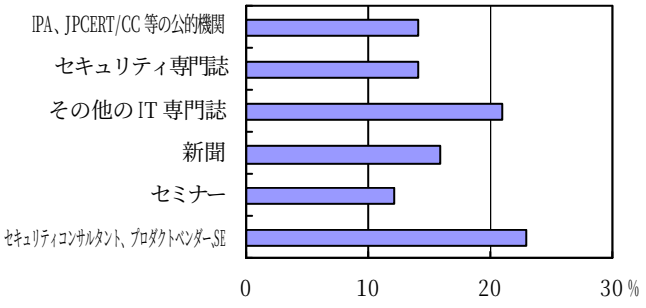
① 情報の収集状況



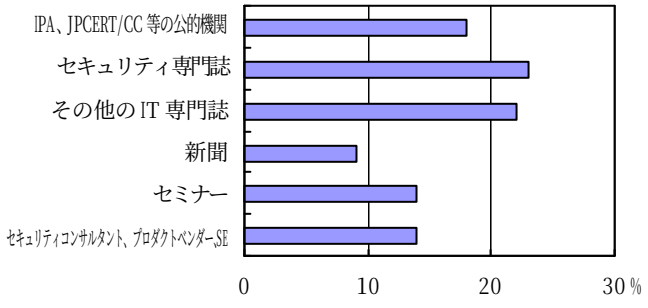
Ⓐ 情報の収集についてのルールが確立しており、ルールに沿った情報の収集を行っている
Ⓑ 情報の収集および収集した情報の取り扱いについてのルールは確立しているが、厳格に運用されておらず、情報の収集は十分には行われていない
Ⓒ 情報の収集は担当者レベルであり組織的には取組んでいない。主にセキュリティコンサルタントや SE からの警告に依存している
（D）このような情報の収集はほとんど行っていない

② 情報の収集源

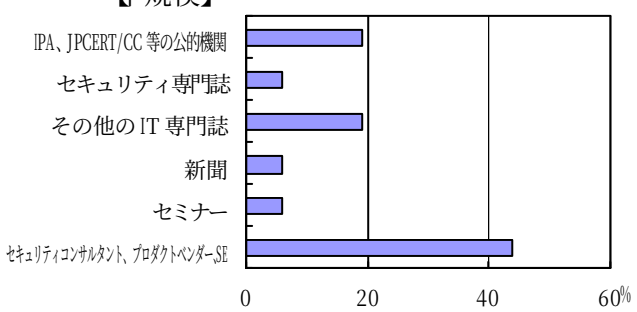
【全体】



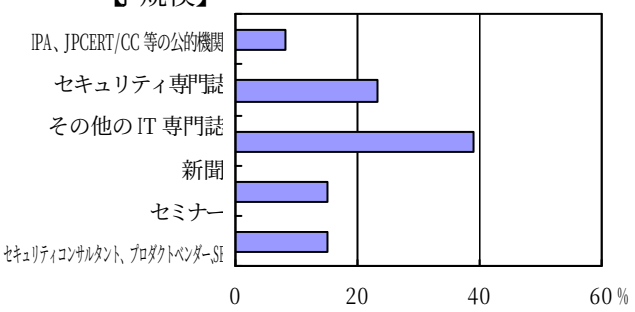
【大規模】



【中規模】

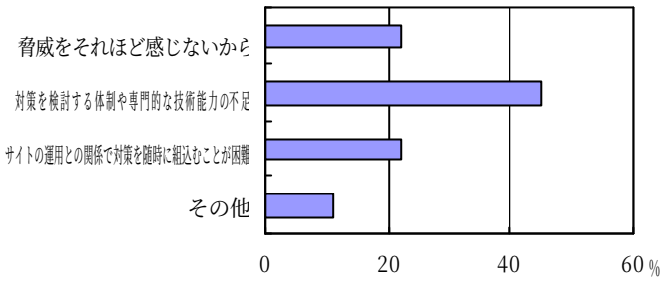


【小規模】

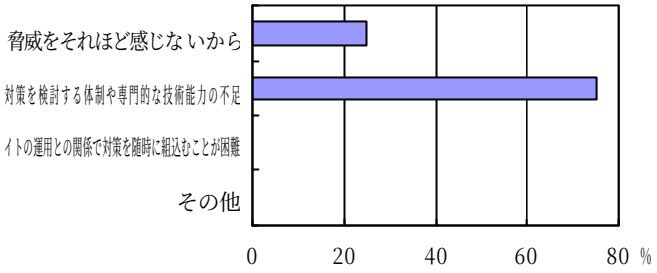


③ 情報収集を実施していない理由

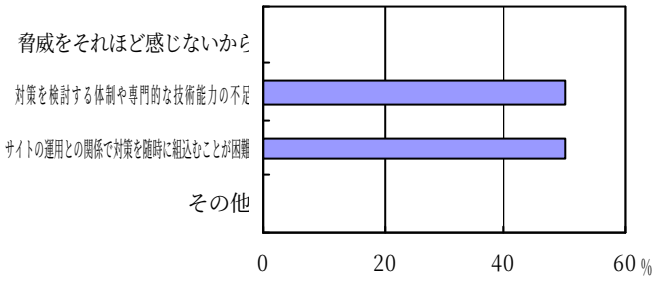
【全体】



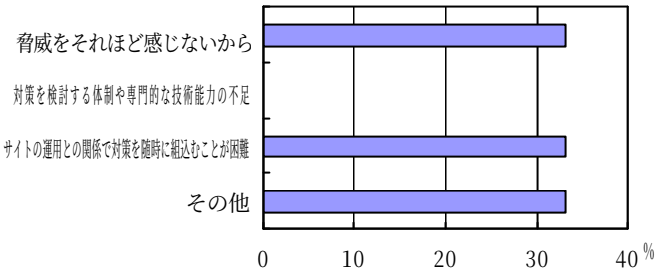
【大規模】



【中規模】

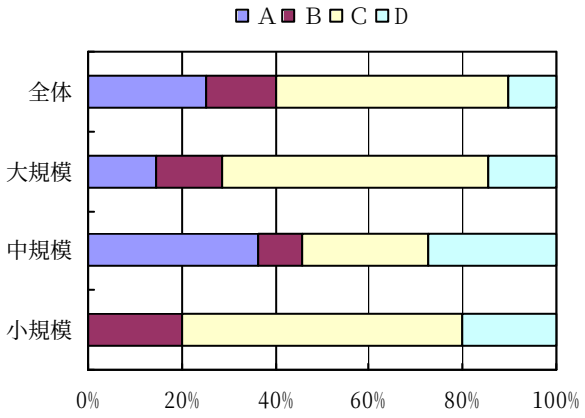


【小規模】



(4) 収集した情報への対応

① 情報の取扱状況



(A) 収集した情報の処理についての手順が確立しており、この手順に沿って情報の評価および必要な対応の検討を行っている

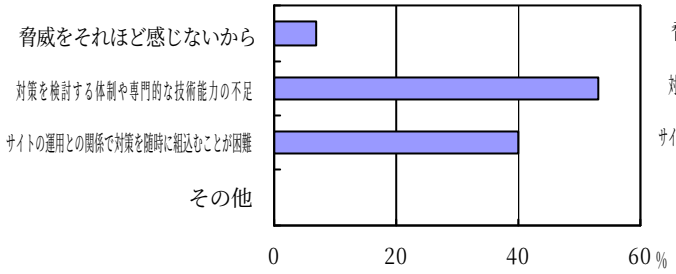
(B) 収集した情報の処理についての手順は確立しているが、収集した情報に対する評価や必要な対応の検討は十分とは言えない

(C) 担当者レベルは努力しているが、担当者の任せであり組織的な対応はできていない

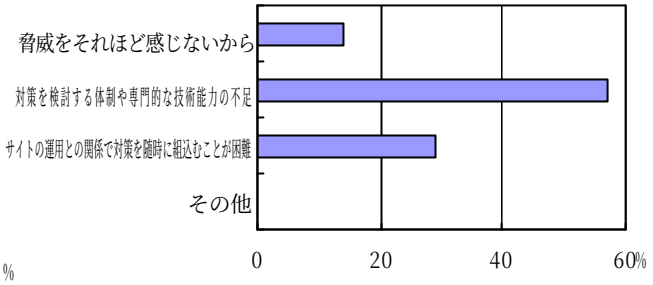
(D) 情報を入手してもほとんど対応していない

② 収集した情報への対応が不十分な場合の理由

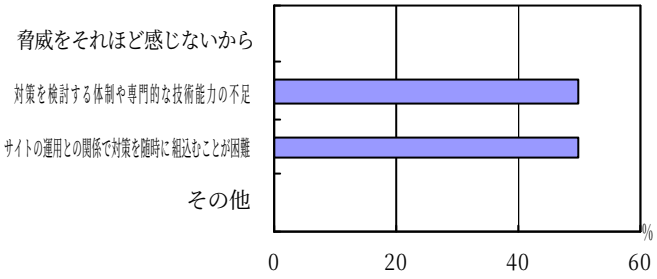
【全体】



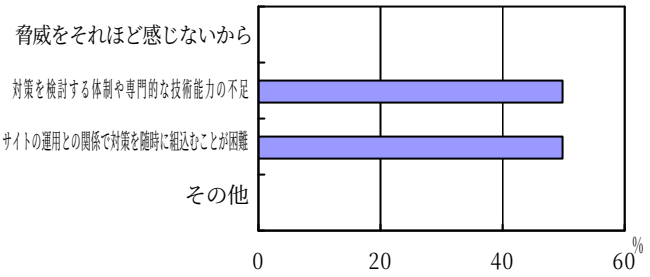
【大規模】



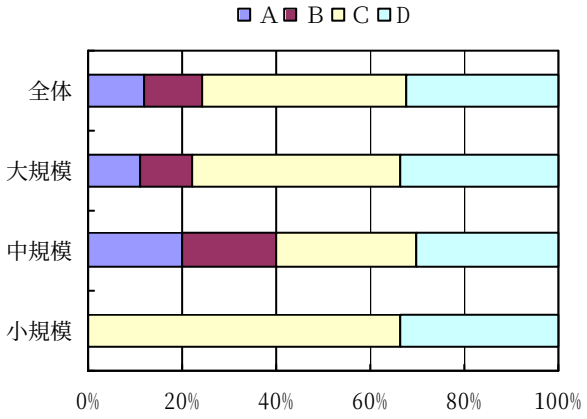
【中規模】



【小規模】



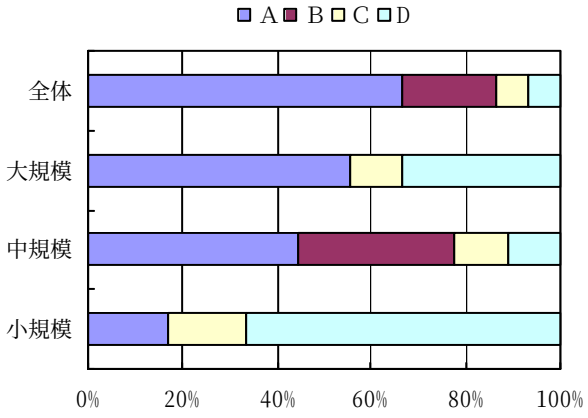
(5) 脆弱点の把握状況



(A) これらの情報の把握と整理についての手順が確立しており、決められた手順に従った管理を行っている。また、関係ドキュメントも整備されている
(B) これらの情報の把握と整理についての手順は確立しているが、厳格に運用されておらず、その確実性に不安がある
(C) 担当者レベルでの把握は行われているが、組織的な管理は行われていない
(D) 特に把握は行われていない

(6) 認知した脆弱性への対策

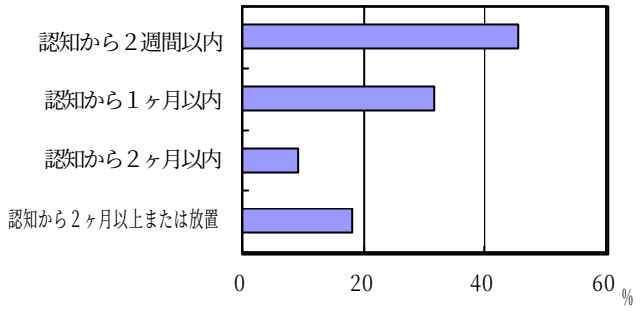
① 新しい脅威への取組状況



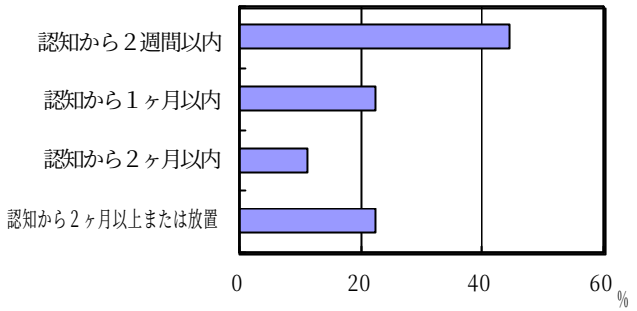
(A) 脅威の程度の判断にもとづき、重大な脅威に対しては迅速に対策を実施している
(B) 迅速化に努力しているが遅れ気味である
(C) あまり積極的に対応していない
(D) 特に対処は行っていない

② 認知した脆弱性への対応のタイムラグ

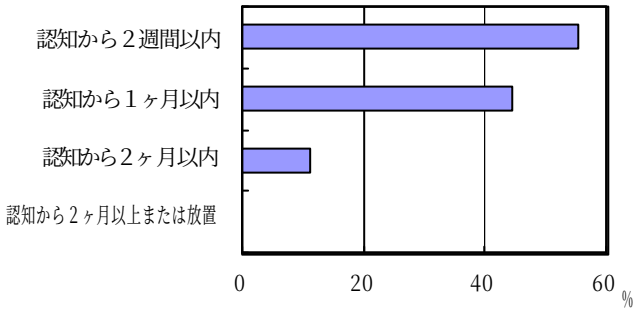
【全体】



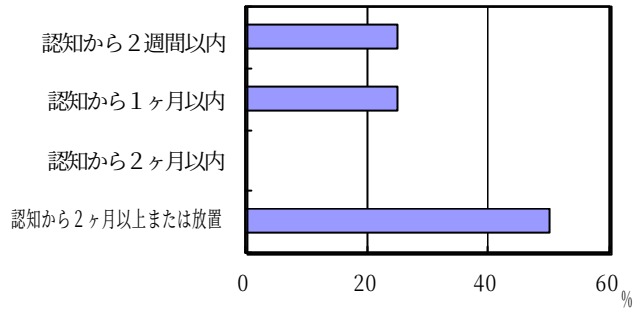
【大規模】



【全体】

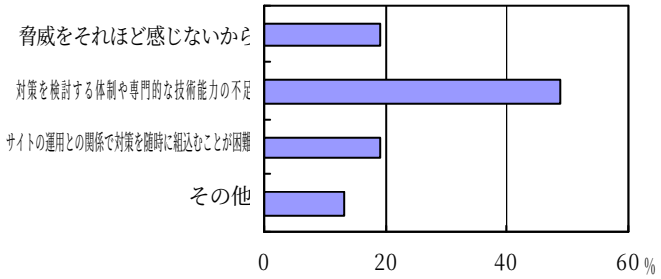


【大規模】

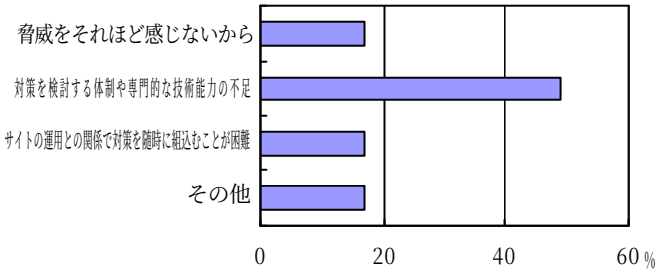


③ 認知した脆弱性への対応が遅い場合の理由

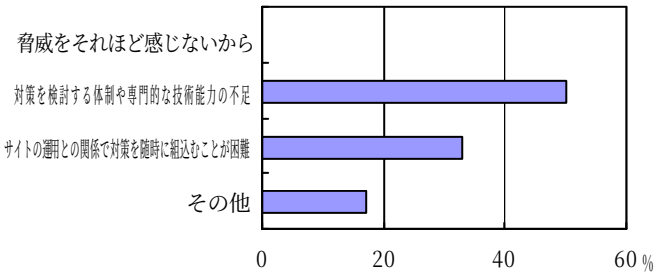
【全体】



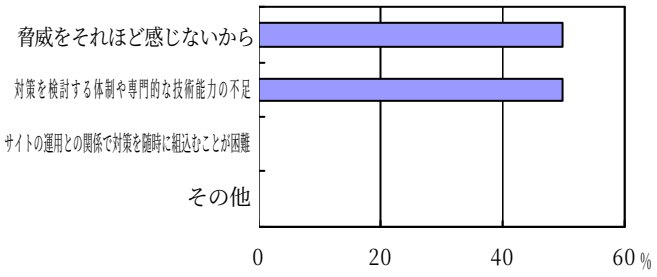
【大規模】



【中規模】



【小規模】

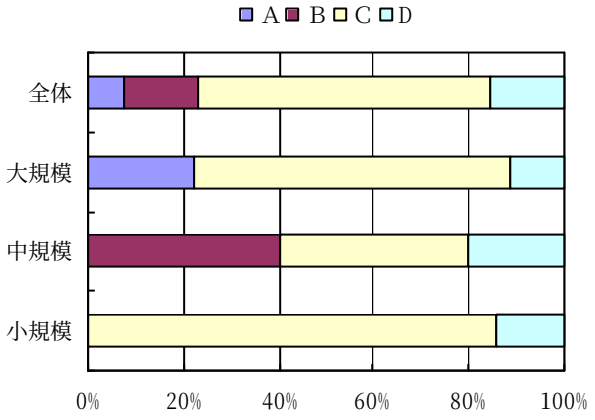


12.2.5 業務における不手際防止への取組み

分析結果から見た傾向は、以下の通り。

- 業務運用についてのセキュリティ要求事項については、指定、実施面ともかなり不十分。
- 運用者への教育も行き届いていない傾向がある。

(1) 業務の運用に係るセキュリティ要求事項の指定状況



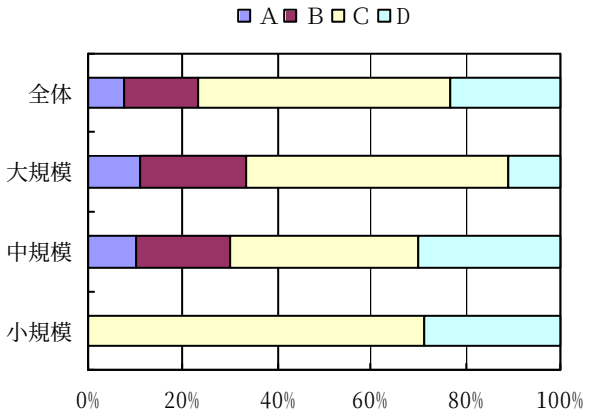
(A) 業務現場に対するセキュリティ要求事項の指定は、関係者によりレビューされており、業務規程や業務マニュアルも常にサイトの運営環境やセキュリティ対策を反映したものが維持されている

(B) 業務現場に対するセキュリティ要求事項の指定は、関係者によりレビューされるとともに、業務規程や業務マニュアルへのセキュリティ対策の反映も、確立したプロセスの中で行われることになっているが、その運用は厳格でなく、セキュリティ対策のシステム運用への反映に漏れが生じている可能性もある

(C) 担当者レベルの努力に依存しているが、業務現場へのセキュリティ対策の反映についての確立したプロセスや、業務規程や業務マニュアルについてのセキュリティ面からの組織的な管理は行われていない

(D) セキュリティ対策と業務現場の連携はあまりとられていない

(2) 業務の運用を確実なものにするための施策



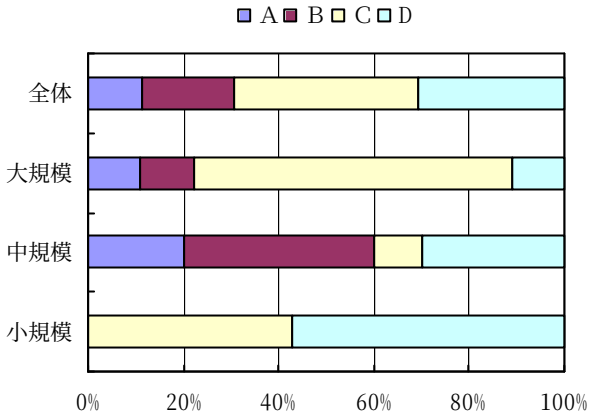
（A）さまざまな工夫が業務プロセスの中に組込まれ、その実行も厳格に管理されており、業務上で不手際が発生あるいは見逃される可能性はほとんどない

（B）さまざまな工夫が業務プロセスの中に組込まれているが、その実行は徹底しているとは言い難く、不手際を発生させたり見逃したりする可能性もある

(C) 担当者レベルでの工夫には見られるが、組織的な管理は行われておらず、不手際が発生したり見逃されていても不思議ではない

(D) 特別な工夫はなされていない

(3) 業務関係者へのセキュリティ教育の実施状況



Ⓐ 検討された計画のもとで教育を行っており、業務関係者の責任意識ならびに要求事項についての理解は十分
Ⓑ 教育を行っているが、関係者の責任意識ならびに要求事項に対する理解については十分とは言い難い
Ⓒ 特別に教育は行われていないが、関係者はセキュリティについての責任意識ならびに要求事項に対する理解をおおむね有していると考えている
Ⓓ 特に行われておらず、関係者の責任意識ならびに要求事項に対する理解については不安

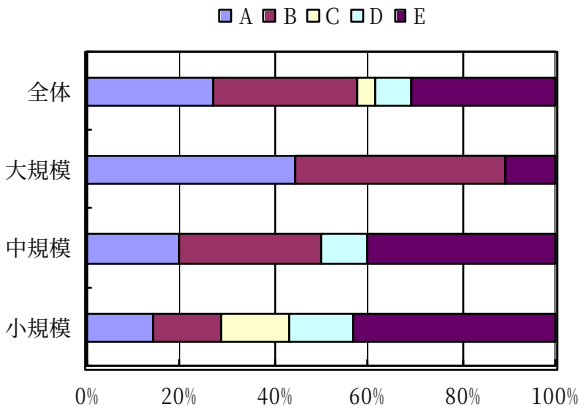
12.2.6 システムの物理的な保護

分析結果から見た傾向は、以下の通り。

- システムの設置場所については、規模の大きなサイトでは、セキュリティを考慮した場所に設置されているが、小さなサイトでは半数弱のサイトが物理的な保護についての意識を持っていない。
- システムに対する物理的なアクセスの管理状態も十分でなく、半数以上のサイトでルール化されていない。

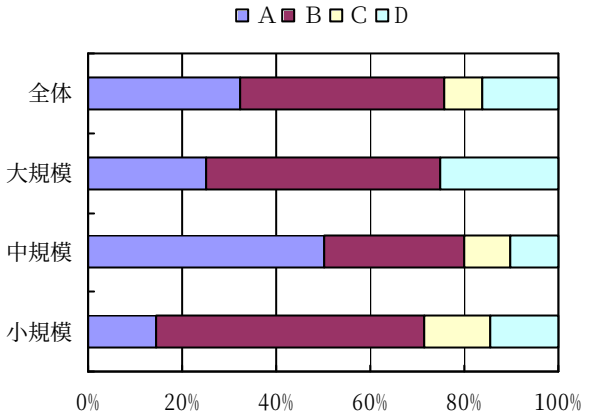
(1) システムおよび関係設備の設置場所

① システムおよび関係設備の設置場所



Ⓐ 常時施錠された扉で物理的に隔離された場所
Ⓑ 常時施錠はされていないが、他とは隔離された独立した場所
Ⓒ パーティション等の移動可能な家具で囲われた場所
Ⓓ 囲われた場所ではないが、保護領域として明示された場所
Ⓔ 特別に保護領域は設けていない

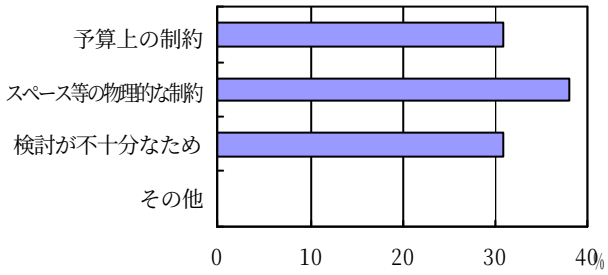
② 設置場所の評価



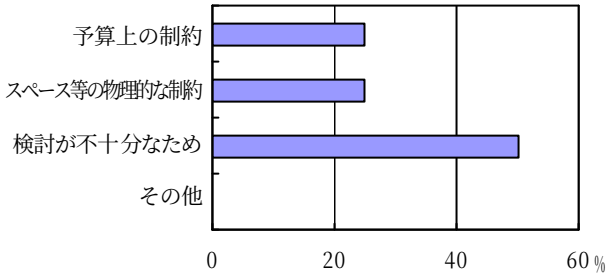
(A) サイトの運営実態とセキュリティポリシーに照らし十分
(B) 十分とはいえないまでも、サイトの運営実態およびセキュリティポリシーに照らしおおむね適切
(C) セキュリティポリシーに照らし十分とは言えず改善が必要
(D) サイトの運営実態やセキュリティポリシーから見て無対策に近く早急に対策が必要

③ 設置場所が不十分と評価した場合の理由

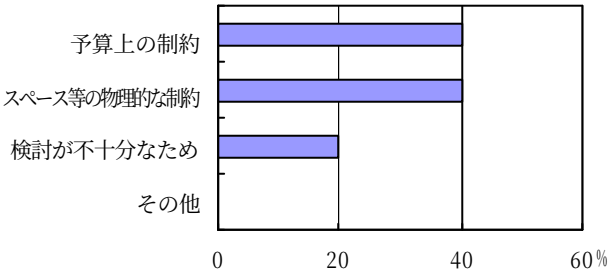
【全体】



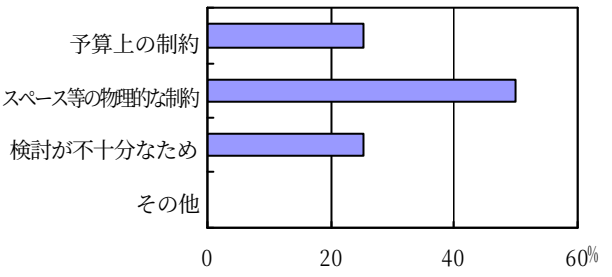
【大規模】



【中規模】

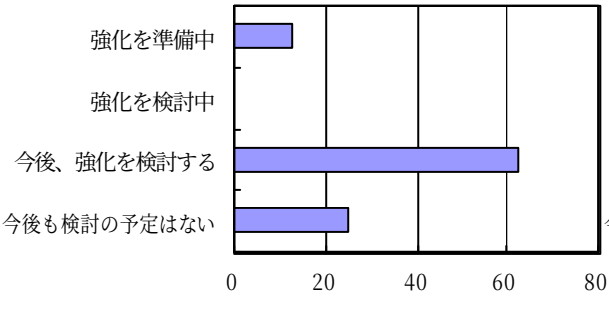


【小規模】

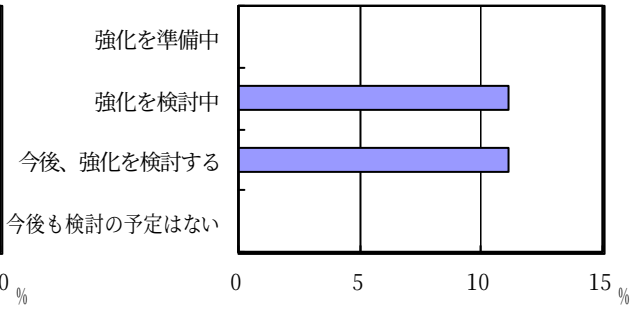


④ 設置場所に関する今後の計画

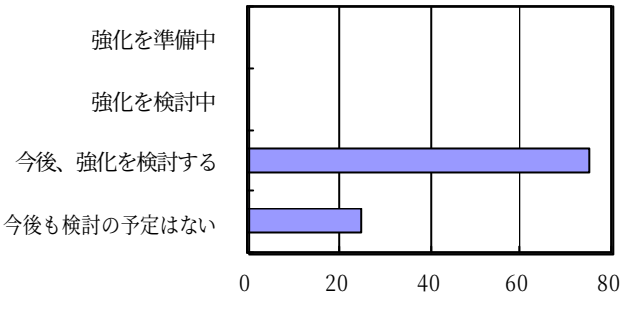
【全体】



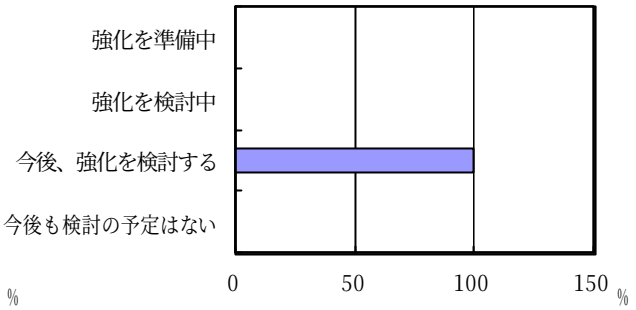
【大規模】



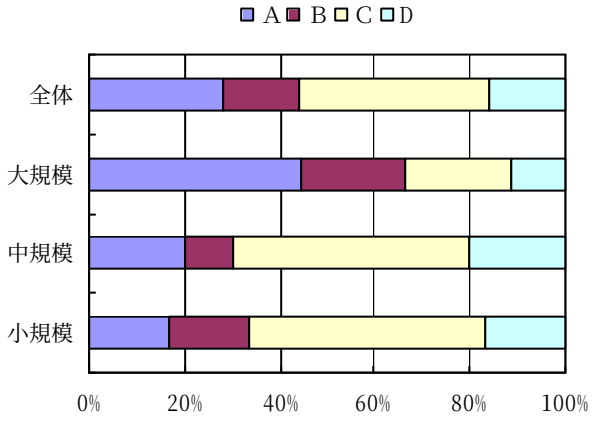
【中規模】



【小規模】



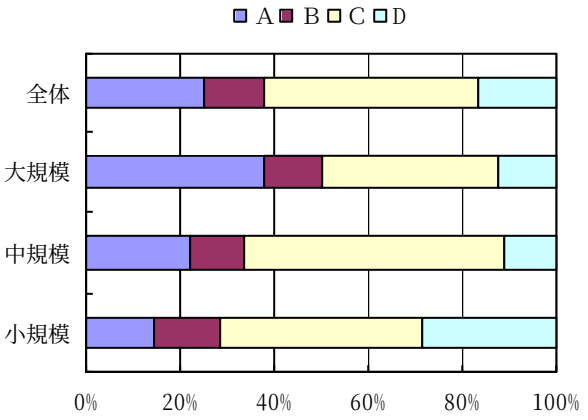
(2) システムおよび関係設備に対する物理的なアクセス管理の実施状況



Ⓐ 設備にあった管理ルールが決められ、厳格に運用されている
Ⓑ 設備にあった管理ルールが決められているが、厳格に運用されていない
Ⓒ ルールは明確でないが、周辺にいる者が注意して運用している
Ⓓ 特に管理していない

(3) 業務現場における物理的な保護領域の設定状況

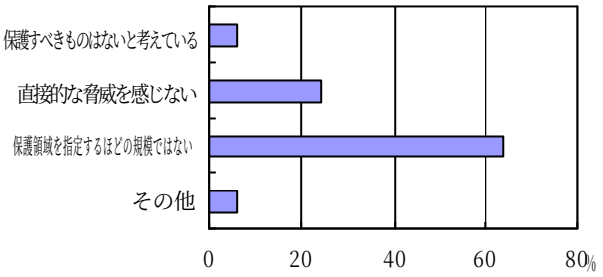
① 業務現場における保護領域の設置



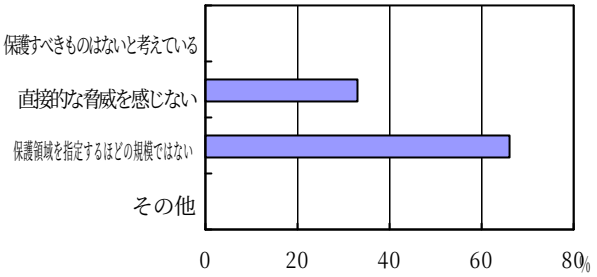
Ⓐ 保護領域は他の職場あるいは外部と隔離されており、厳重なアクセス管理が行われている
Ⓑ 保護領域の隔離とアクセスの管理は行われているが、保護領域の設定やアクセス管理の運用は厳格とは言えない
Ⓒ 保護領域の認識はあるが、物理的な隔離は行われておらず、職場の注意に依存している
Ⓓ 特に保護領域についての認識はない

② 職場に保護領域を設定していない場合の理由

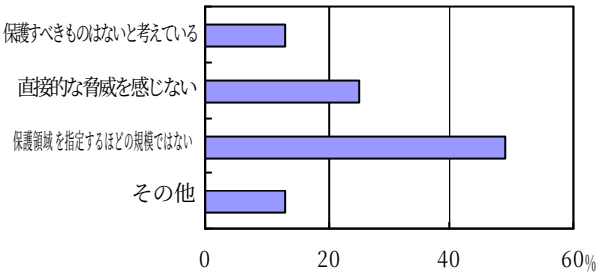
【全体】



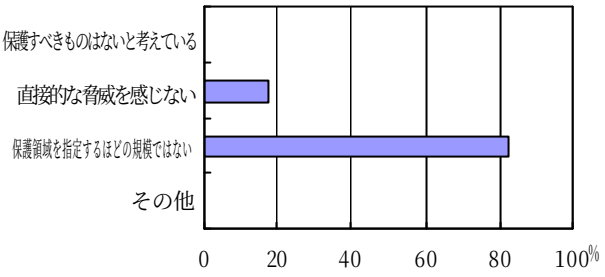
【大規模】



【中規模】



【小規模】



13 セキュリティ事故への備え

本章では、EC サイトが実施しているセキュリティ事故への備えについて分析を行う。
分析項目については、以下の通り。

- セキュリティ事故対策方針の確立状況と体制
- セキュリティ事故処理手順の確立
- 日常におけるセキュリティ事故への備え
- セキュリティ事故遭遇の経験と対応
- セキュリティ事故対応の反省点
- セキュリティ事故対応能力の自己評価

13.1 “セキュリティ事故への備え”全体を通しての傾向

セキュリティ事故への備えについては、かなり認識が薄い。また、組織としての対応方針さえ持たないサイトが多い。

セキュリティ事故への対策方針・体制の明文化と確立は、サイト規模の大きさに比例しており、小規模のサイトほど対策ができていない。

また、セキュリティ事故（インシデント）遭遇の経験としてはウイルス感染を筆頭に DoS 攻撃、不正侵入、情報漏洩による被害の順で多く回答されている。

インシデントに対する技術者スキルの程度については全体的に不十分であり、インシデントに備えての訓練実施は全般に低調である。

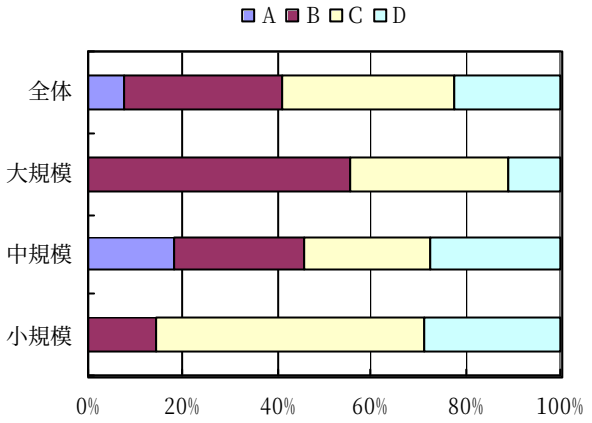
13.2 設問ごとの分析結果

13.2.1 セキュリティ事故対策方針の確立状況と体制

分析結果から見た傾向は、以下の通り。

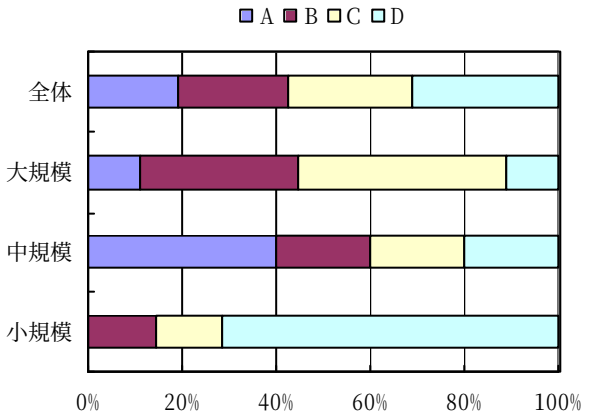
- シェア的にはまだまだその数は少ないが、組織的なセキュリティ事故対策の方針・体制の確立はサイト規模の大きさに比例して整備されている。
- 事故遭遇を想定した定期的な訓練は規模の大きいサイトのごく少数を除き、大半のサイトでは未実施である。
- セキュリティ事故遭遇時の手順の整備状況については、「組織的に必ずしも明確になっていない」が、セキュリティ対策関係者レベルで手順と対応をおこなっている状況にある。

(1) セキュリティ事故対応方針の確立



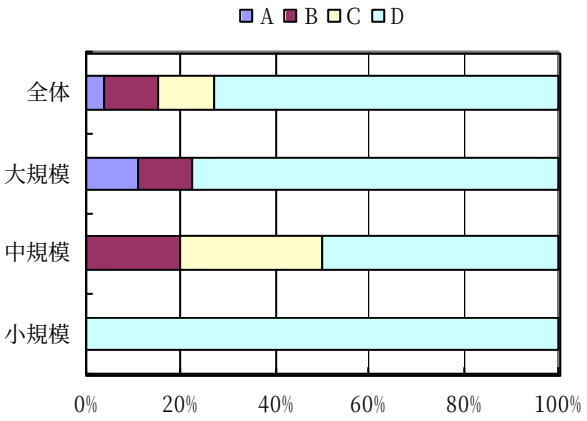
Ⓐ 十分に検討されたものがあり、関係者に明示されている
Ⓑ 原則は示されているが、内容的に十分とは言えない
Ⓒ 担当者レベルでは考えられているが、組織的には検討されていない
Ⓓ 検討されていない

(2) セキュリティ事故対策体制の整備



Ⓐ 必要な体制を確立しており、常時、即応できる
Ⓑ 体制は決められているが、常時、即応体制にあるとは言い難い
Ⓒ 事故処理体制としては明確にはなっていないが、セキュリティ対策関係者が対応することになっている
(D) セキュリティ事故に対応できる体制はない

(3) セキュリティ事故対応訓練の実施状況



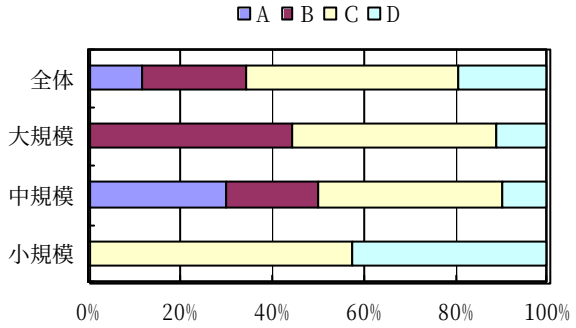
Ⓐ 十分に検討された訓練計画があり、この計画に従った訓練を定期的に行っている
Ⓑ 確立した訓練計画はないが、定期的に訓練を行っている
Ⓒ 担当者レベルで事故処理訓練が行われることもある
Ⓓ 事故処理訓練は行っていない

13.2.2 セキュリティ事故処理手順の確立

分析結果から見た傾向は、以下の通り。

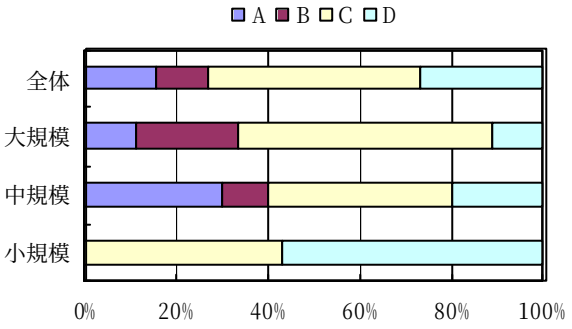
- 事故処理に関する手順および事故発生時の処置手順については、十分には確立しておらず、特に小規模サイトにおいては、組織的な検討がほとんどなされていない。

(1) 事故処理手順の確立状況



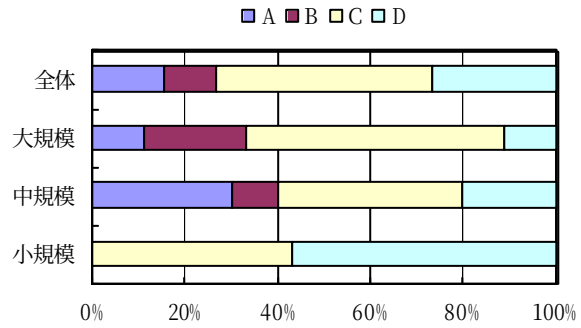
(A) 十分に検討された手順が確立しており、関係者に徹底されている
(B) 一通りのことは決められているが、内容的にも十分といえず、さらに検討が必要である
(C) 担当者レベルでは考えられているが、組織的には検討されていない
(D) 検討していない

(2) 事故発生時のとっさの処置



(A) 十分に検討された手順が確立しており、関係者に徹底されていて、何時でも迅速に対応ができる
(B) 必要な処置や手順は示されているが、内容的にも十分といえず改善が必要である
(C) 担当者は必要な処置を心得ており、ある程度の対応は可能とみているが、組織として対応できるようにはなっていない
(D) 何も準備がなく、即応できる状態にはない

(3) パスワードの漏洩や IC カード等の盗難、偽造に対する処置



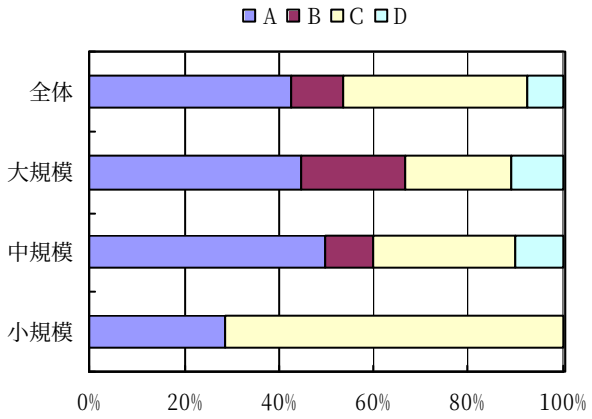
(A) 十分に検討された手順が確立しており、関係者に徹底されていて、何時でも迅速に対応ができる
(B) 手順は確立しているが、問題の発生に際して期待通り機能するかどうかに不安が残る
(C) 手順としては確立していないが、関係者は必要な処置についての知識をある程度有している
(D) 特に準備されていない

13.2.3 日常におけるセキュリティ事故への備え

分析結果から見た傾向は、以下の通り。

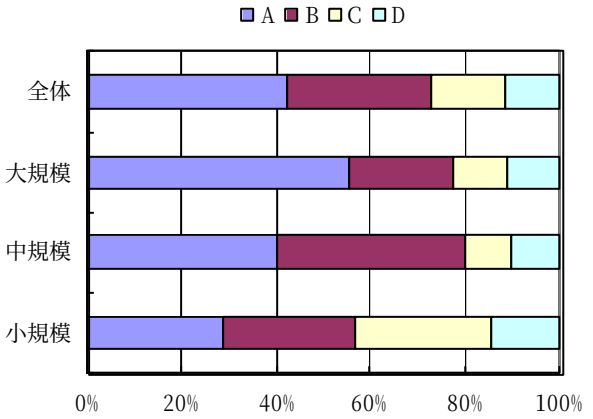
- セキュリティ事故からの復旧手段（措置）として、最も認知度の高い「バックアップ」の実施であるが、組織的管理のもと着実に実施できているのは規模の大きなサイトということが言える。
- 運用記録（保管）は、一般に低調である。
- 事故処理ツールの整備は規模の大きさに比して取り揃えが充実している。しかし、全般的にツールの質としては「ファイル回復ツール」のレベルでそれ以上のツールにはまだ手が回らない状況にある。

(1) バックアップのルール化



(A) これらの指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている。また、ドキュメントもよく整備されている
(B) これらの指定は、決められた手順に沿って行われることになっており、ドキュメント化も行われているが、組織的な検討やレビューおよび見直しやドキュメント化は厳格ではなく、指定の一部に妥当性を欠いていることもありうる
(C) 担当者任せで組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。
(D) 計画的なバックアップの取得、保管は行われていない

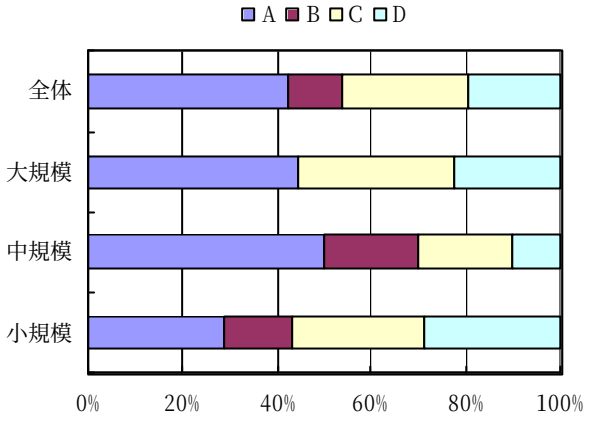
(2) バックアップの実施状況



(A) 指定に従ったバックアップの取得および保管は十分な管理下で励行されている
(B) 指定に従ったバックアップの取得および保管は行われていることになっているが管理は徹底していない
(C) バックアップの取得や保管は行われているが、運用チームの意識に依存している
(D) バックアップの取得は計画的には行っていない

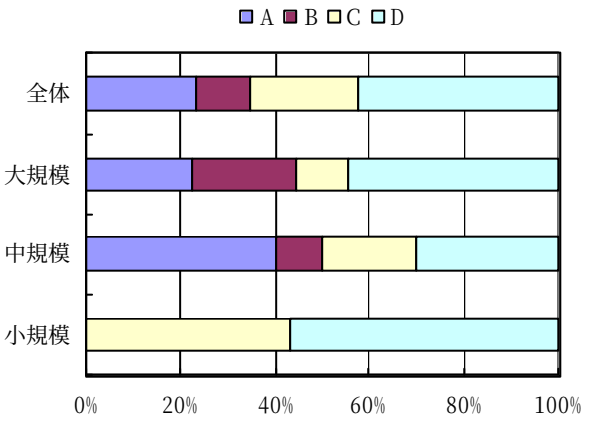
【補足】大規模サイトかつ自社運営のサイトでは、実施者としての自覚から「確立した手順と管理の実施」を明確に回答しているが、中・小規模サイトではホスティング運営の状況を反映してか、「回答なし」としている。

(3) 運用記録の確保



(A) 十分に検討された記録の取得、保管要領が確立しており、必要な記録の取得ならびに保管はシステムの運用の中に組込まれ、確実に運用されている
(B) 必要な記録の取得、保管要領が確立しているが、厳格に運用されていると言えない。また、現時点での確保の対象としている記録は、サイトの運用実態から見て妥当であるかどうかの確認はされていない
(C) 一部の記録はとられているが、必要な記録の取得、保管についての組織的な検討は行われていない
(D) セキュリティ事故に備えた記録の取得、保管は行われていない

(4) ツールのメンテナンス状況



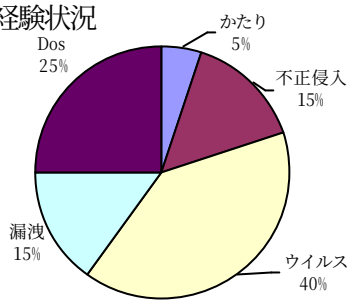
(A) 必要なツールはすべて揃えられており、メンテナンスも適切に行われ定期的な動作確認も行われている
(B) 必要なツールは揃えられているが、メンテナンスや定期的な動作確認は十分に行われていない
(C) ファイルの回復のためのツールが準備されている程度で、十分な検討は行われていない
(D) セキュリティ事故に備えたツールの整備は行っていない

13.2.4 セキュリティ事故遭遇の経験と対応

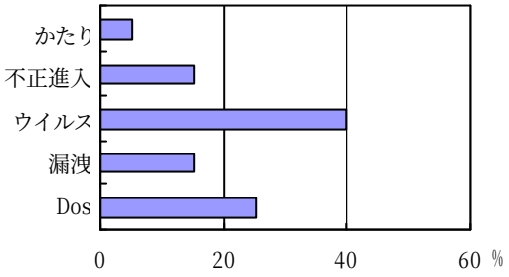
分析結果から見た傾向は、以下の通り。

- 多くのサイトで「ウイルスの感染」、「DoS攻撃」、「不正侵入」、「情報漏洩」の順で不名誉な洗礼を受けている。
- セキュリティ事故による被害規模として、ウイルス感染で大きいダメージを受けたと回答があり、情報漏洩では中規模程度の影響、そのほかでは、おおよそ軽微な被害に収まったと回答している。
- ウイルス等によるセキュリティ事故被害状況報告の実施は「その義務を認知していなかった」、「報告への抵抗感（メリットがないと判断）」という理由から積極的に届け出を行わなかったと回答されている。

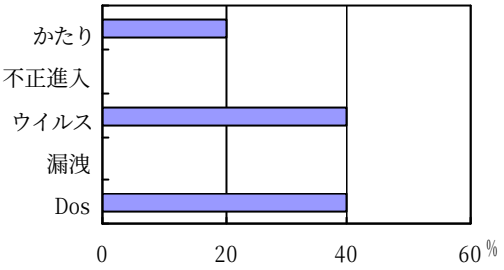
(1) セキュリティ事故遭遇経験状況



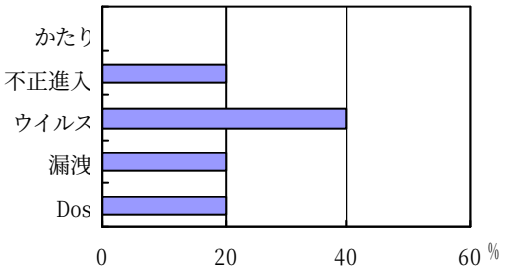
【全体】



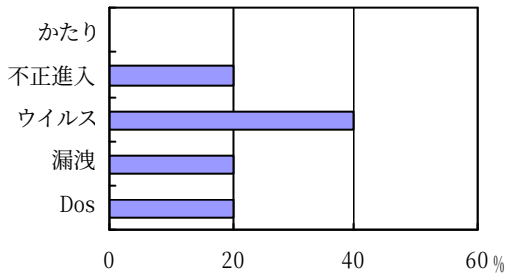
【大規模】



【中規模】

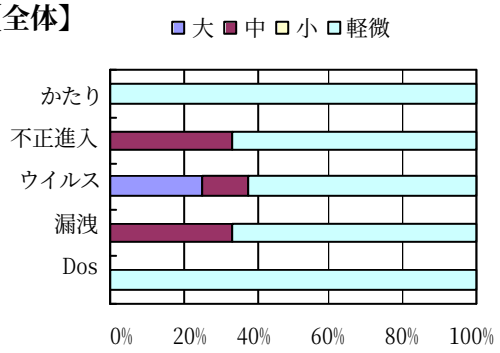


【小規模】

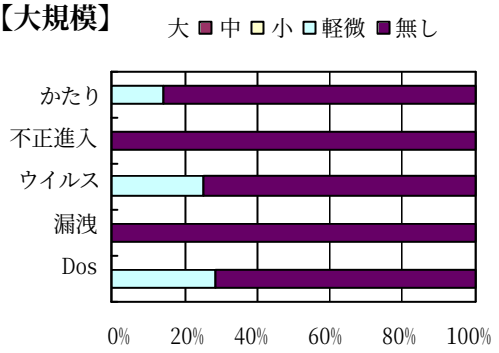


(2) 被害規模状況

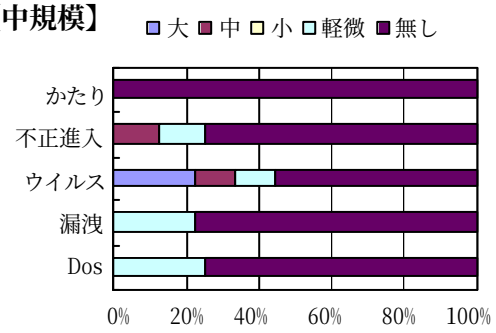
【全体】



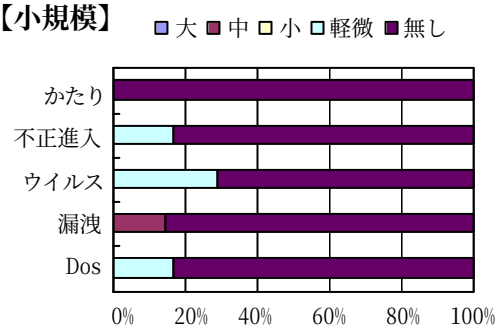
【大規模】



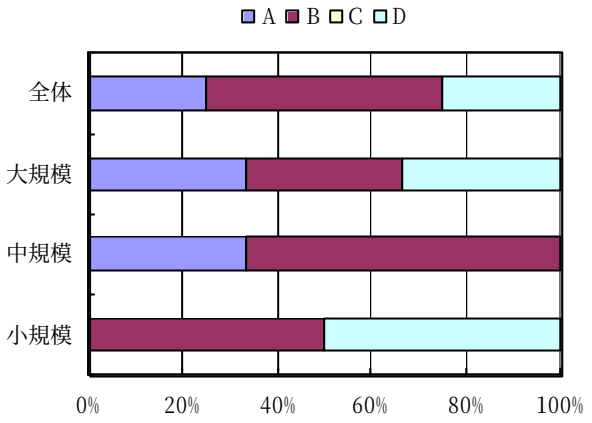
【中規模】



【小規模】



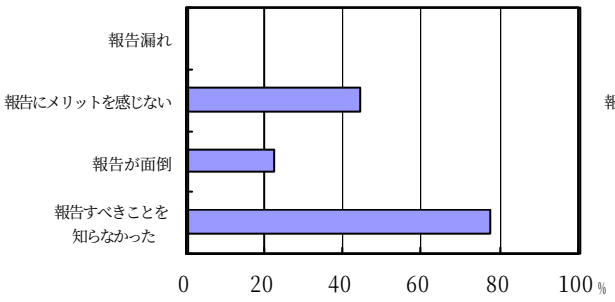
(3) IPA等への被害報告実施状況



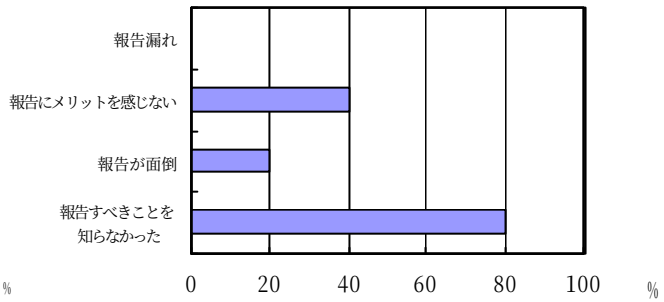
(A) すべて報告している
(B) 報告することを原則にしているが、報告しないこともある
(C) 報告することを原則にはしていないが、報告することもある
(D) ほとんど報告しない
(E) 報告したことがない

(4) 報告阻害要因

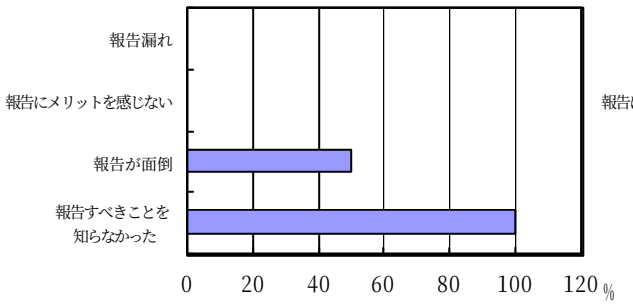
【全体】



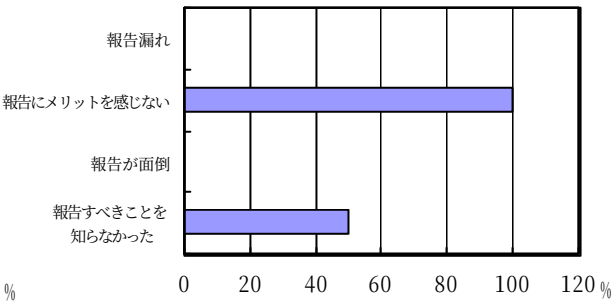
【大規模】



【中規模】



【小規模】

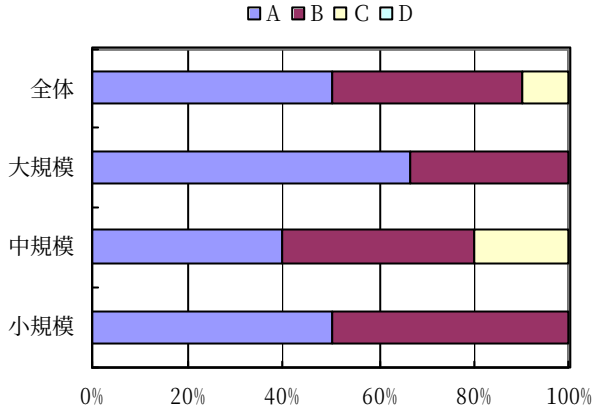


13.2.5 セキュリティ事故対応への反省点

分析結果からみた“事故対応への反省点”の傾向は、以下の通り。

- セキュリティ事故処理の課題として、「業務の復旧」、「他社対応」、「再発防止」に問題を残したとしており、そのほかにも同率で、「事態の把握」、「被害範囲の特定」、「情報公開」と「訴訟・賠償へ対応」の難しさをあげる回答が目立った。しかし、実際にセキュリティ事故による被害を受けたサイトの管理者が、事故処理対応状況を振り返り、「おおむね適切に対処できた」と回答している。

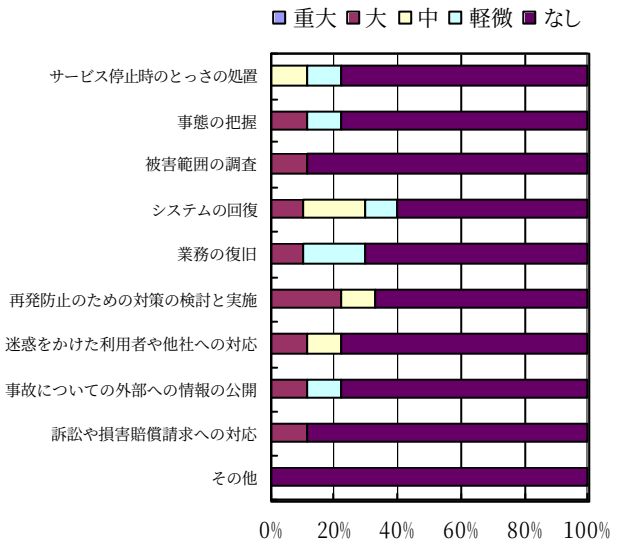
(1) 対応の自己評価



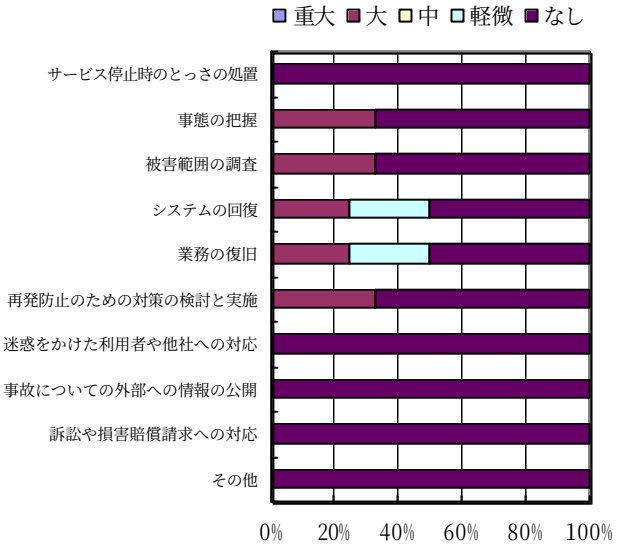
Ⓐ 必要な処置はすべて適切かつ迅速に行われた
Ⓑ 必要な処置はおおむね適切に行われたが、改善すべきところもある
（C）なんとか処置はすませたが、多くの問題を残した
Ⓓ 必要な処置が適切に行われず混乱が発生した

(2) 発生事故に対する問題の程度

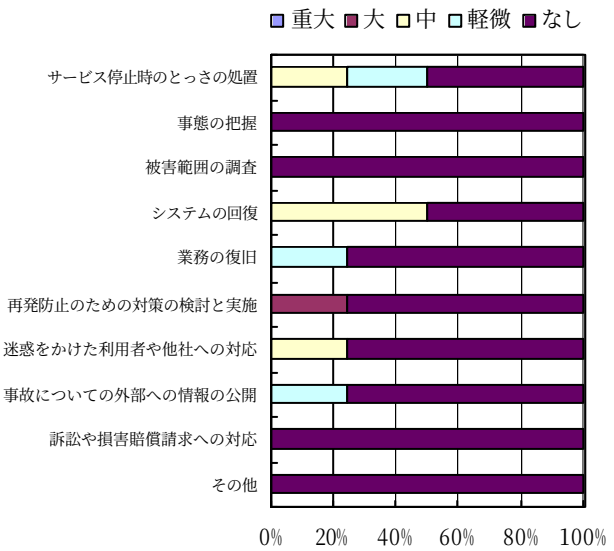
【全体】



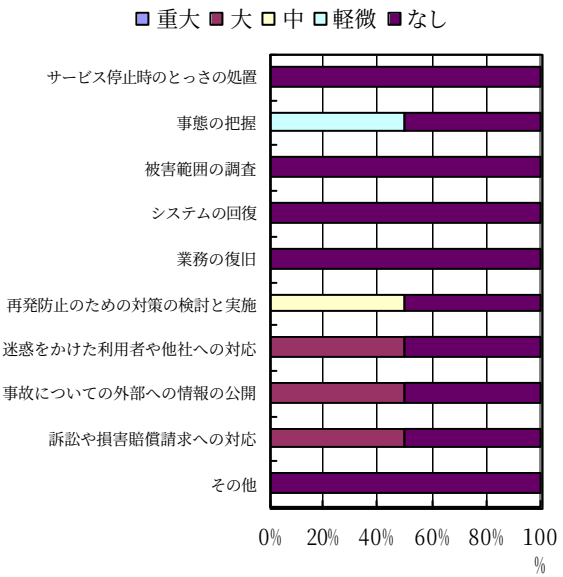
【大規模】



【中規模】



【小規模】

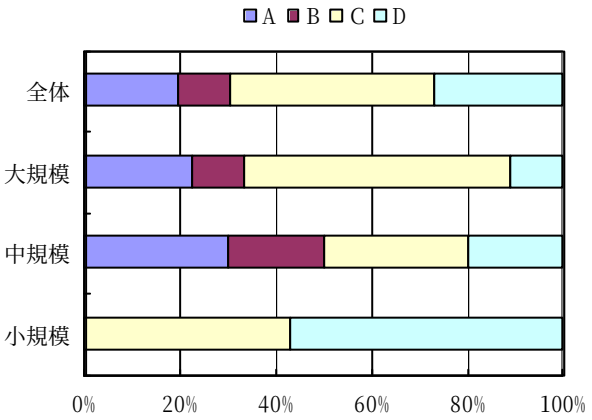


13.2.6 セキュリティ事故対応能力の自己評価

分析結果から見た傾向は、以下の通り。

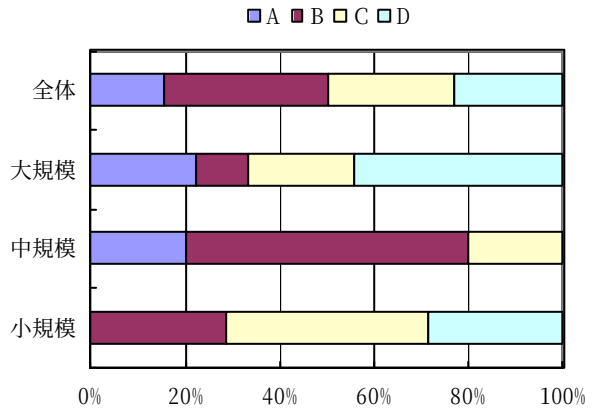
- 規模の大きなサイトには、「それなりのスキルの要員」を抱えていることがうかがえるが、小規模サイトでは「事故処理できる要員はなし」と回答しており、厳しい運営状況が浮き彫りになった。「事故処理要員なし」としたサイトでは、外部機関を採用（ベンダ等のコンサルタントとの連携など）し、「必要に応じ支援を要請」するなどして、弱点を補完する傾向がうかがえる。

(1) 担当者スキルレベルの自己評価



Ⓐ 必要なスキルを十分に有している
Ⓑ 一通りのスキルはあると考えているが十分とは言えない
（C）ある程度のスキルは有するが不安がある
Ⓓ 事故処理ができる要員はいない

(2) 外部機関の利用状況



Ⓐ 事故処理体制の中に組込まれており、常時、連絡をとっている
Ⓑ 事故処理体制に中に組込むまでには至ってないが、必要に応じ応援をもらえるようになっている
Ⓒ 特に準備はしていないが、必要に応じて支援を依頼するつもりである
Ⓓ 外部からの支援は特に考えていない

14 総合評価

本章では、各 EC サイトが実施しているセキュリティ対策についてどのような自己評価を行っているかについて分析を行う。

14.1 分析結果から見た全般的傾向

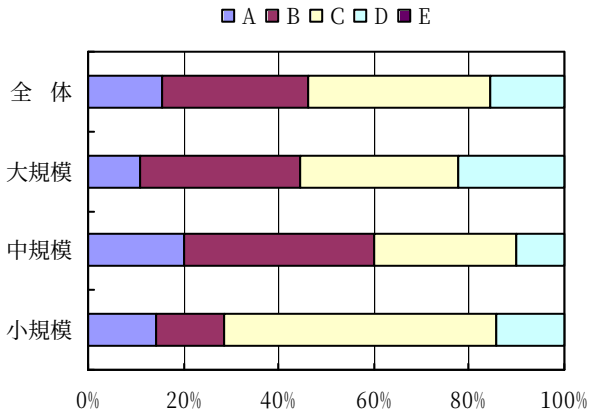
情報セキュリティの脅威の認識は、EC サイトの規模によらずサイト運営者に広く行きわたっているが、セキュリティ対策や実施すべき内容については自信をもてないままサイト運営を行っているという実態がうかがえる。組織的なセキュリティ対策が整備できているサイトは有効回答数の１／３に止まっている。

その他、傾向として気づいた点は、以下の通り。

- 全体評価で十分と評価しているサイトの大部分は技術面での対策も十分としているが、プロセス、運用面、ドキュメント化については十分と評価しているところは半分以下である。
- セキュリティ対策が不十分と評価していながら、速やかな対策を検討していないサイトがかなりある。

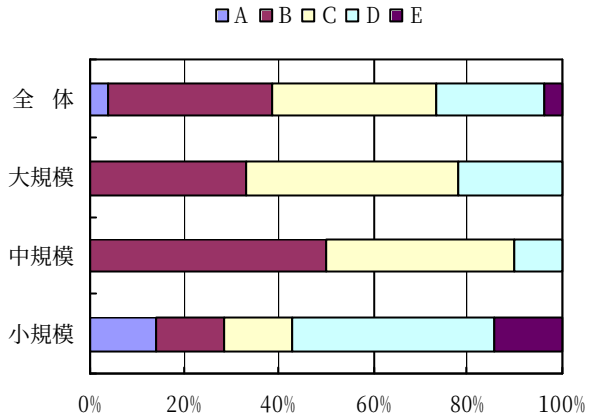
14.2 設問ごとの分析結果

(1) 技術面に対する評価



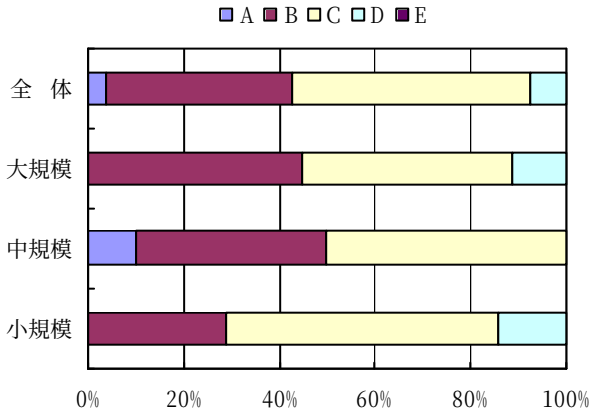
(A) サイトの運営実態に照らし十分と考えている
(B) 一通りの対策は講じられているが十分とは言えない。改善すべき点がある
(C) 最低限の対策の範囲を出てない
(D) 実質的な対策になっていない
(E) わからない

(2) サイト運営へのセキュリティ要求事項のプロセス化に対する評価



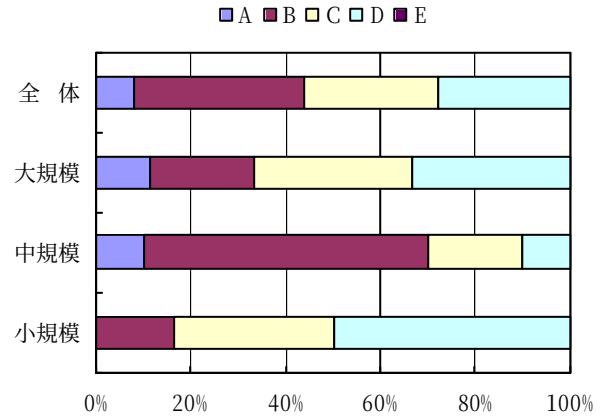
Ⓐ 十分と考えている
Ⓑ おおむね十分と考えている
Ⓒ 一部しかできていない
(D) ほとんどできていない
(E) わからない

(3) サイト運営におけるセキュリティ要求事項実行の管理に対する評価



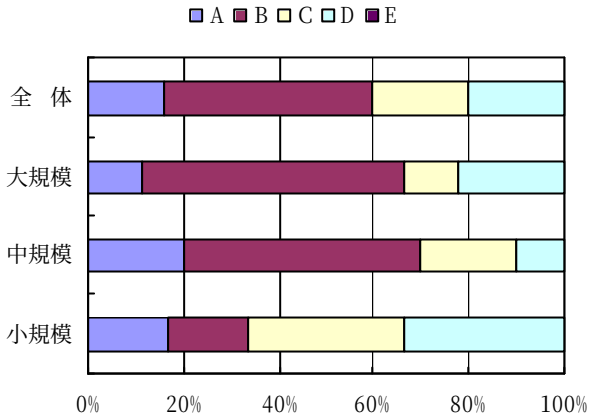
(A) セキュリティ要求事項の実行に対する管理はルール化されており、このルールに沿った管理が厳格に行われている
(B) セキュリティ要求事項の実行に対する管理はルール化されているが、このルールに沿った管理が厳格には行われていない
(C) セキュリティ要求事項の実行に対する管理についてのルールはなく、部分的にしか管理されていない
(D) ほとんど管理されていない
(E) わからない

(4) セキュリティ対策についてのドキュメント化に対する評価



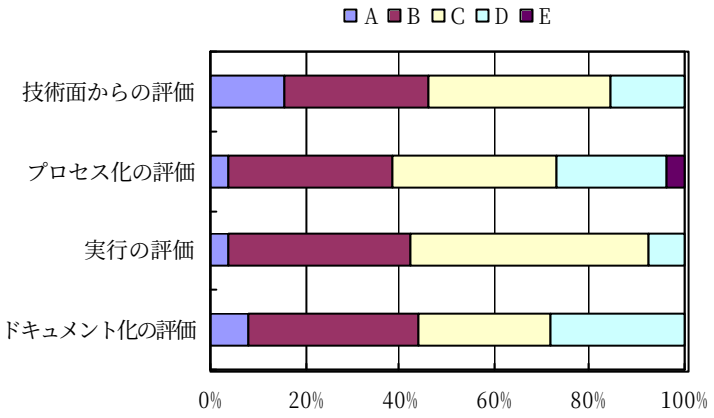
Ⓐ ルールに沿ったドキュメント化が行われており、常に関係ドキュメントの正確性は維持されている
Ⓑ ルールに沿ってドキュメント化が行われることになっているが、厳格に運用されているとは言えず、関係ドキュメントのすべてについて正確かどうかは疑問
Ⓒ 担当者レベルで行っている一部を除き、すべてにわたりドキュメント化は行われていない
(D) ドキュメントの整備はほとんど行われていない
(E) わからない

(5) セキュリティ対策全体の評価



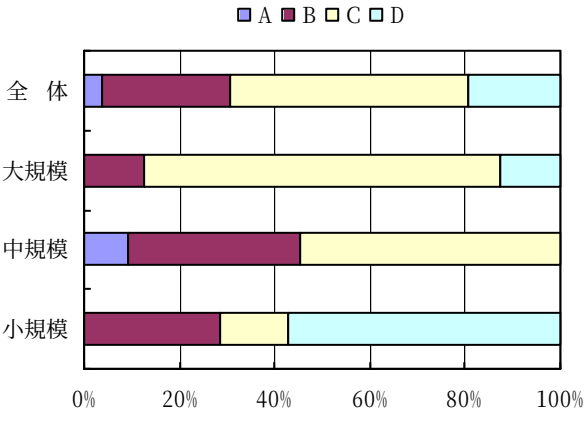
(A) サイトの運営形態から見て十分な対策が講じられていると考えている
(B) 一通りの対策は講じているものの、技術面でも管理面でも十分とは言えない
(C) ある程度の対策は講じられているものの、組織的戦略的には程遠く、不十分
(D) 実質的な対策はほとんどなされていない
(E) わからない

※　項目ごとの評価の相関

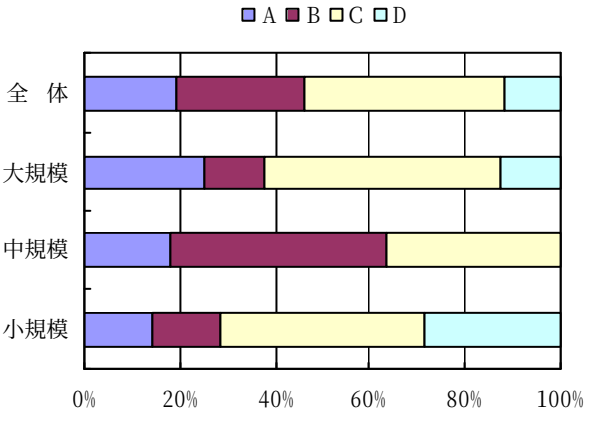


(6) 個々の対策についての評価

①　セキュリティマネジメントの確立

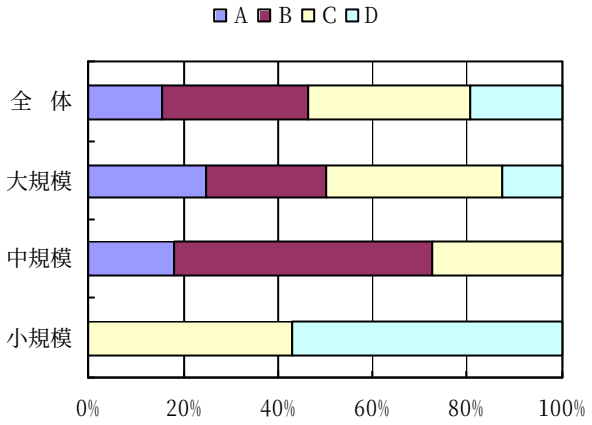


②　不正アクセス対策

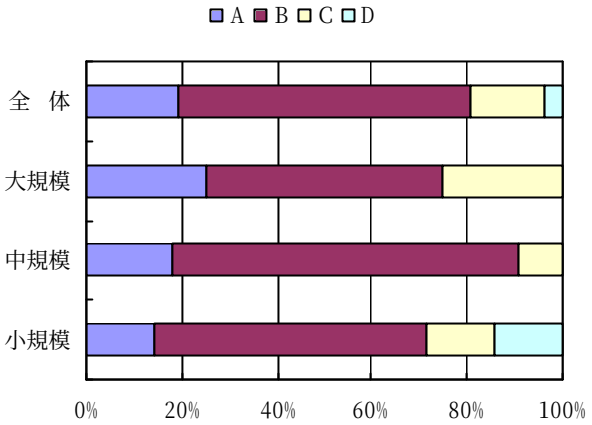


(A) 十分　　(B) おおむね十分　　(C) 改善が必要　　(D) 未対策

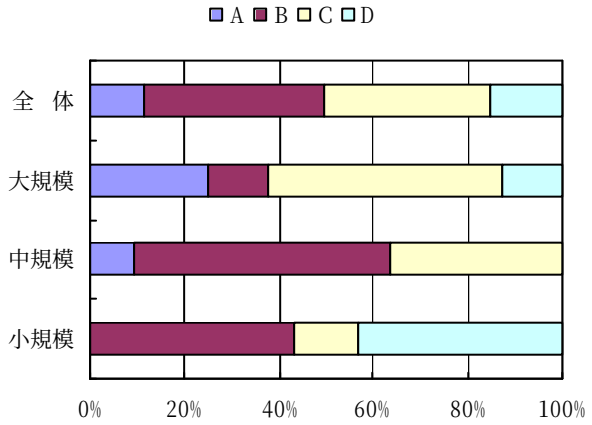
③ セキュリティホール対策



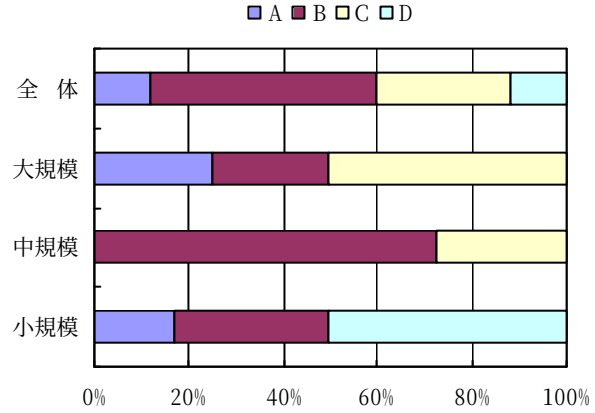
④ ウイルス対策



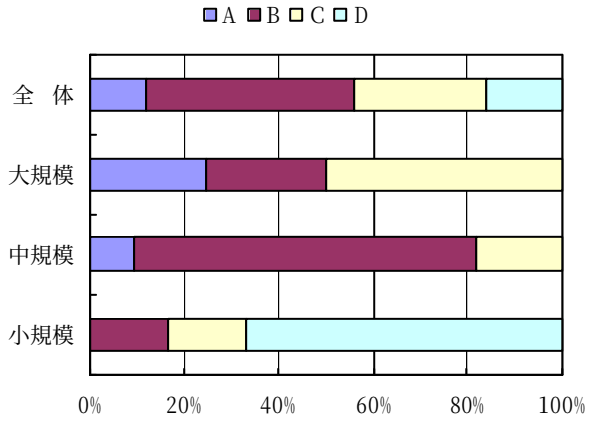
⑤ セキュリティ管理情報の保護管理



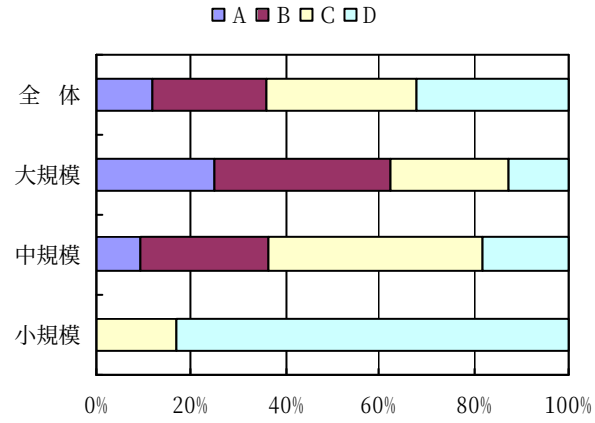
⑥ ユーザ情報の保護管理



⑦ 通信の保護

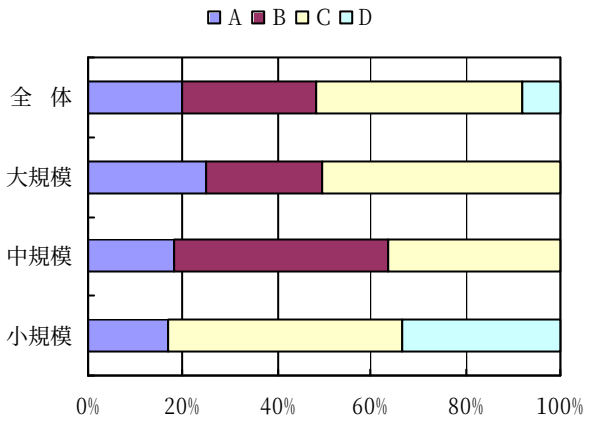


⑧ ユーザ認証の管理

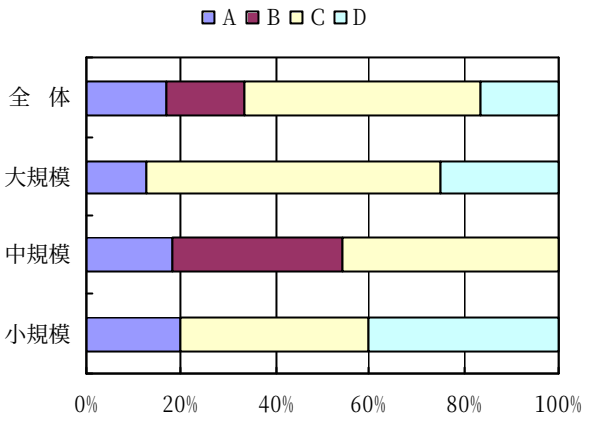


Ⓐ 十分　　Ⓑ おおむね十分　　Ⓒ 改善が必要　　Ⓓ 未対策

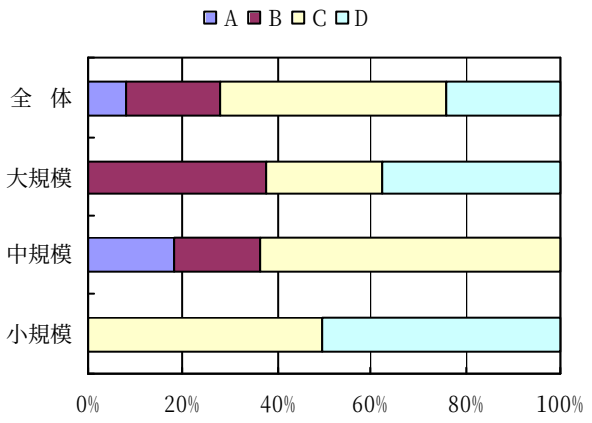
⑨ システム構成の管理



⑩ システム運用や業務運用の管理



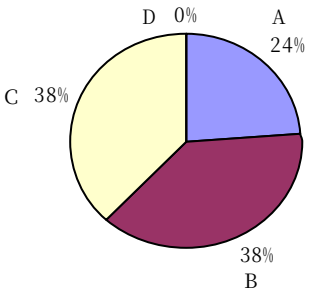
⑪ セキュリティ事故への備え



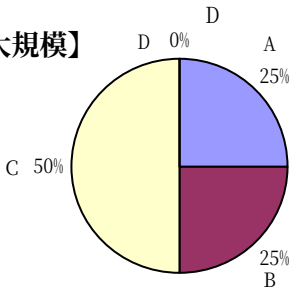
(A) 十分
(B) おおむね十分
(C) 改善が必要
(D) 未対策

(7) セキュリティ対策が不十分のままにしている理由

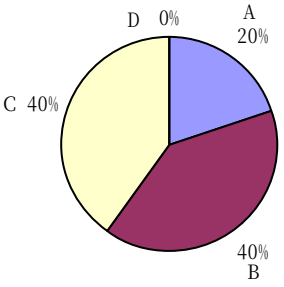
【全体】



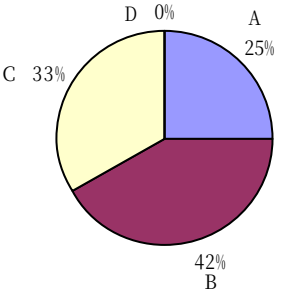
【大規模】



【中規模】



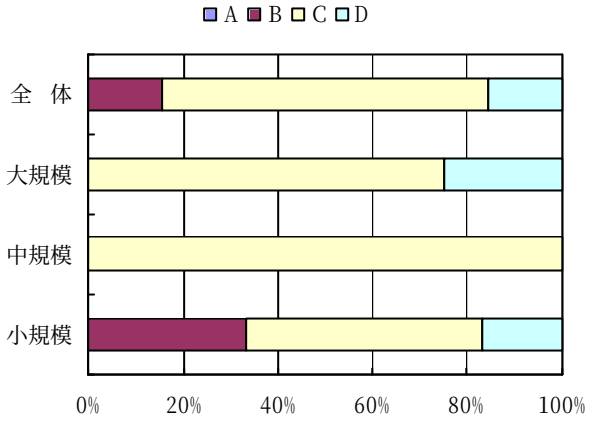
【小規模】



(A) 十分とは考えていないが、脅威に対する現実感が薄いため
(B) 予算面での制約が大きいため　　(C) 技術的な対応力が不足しているため　　(D) その他

(8) セキュリティ対策の向上についての計画

（組織的に取組んでいる場合について）



Ⓐ 強化を準備中
Ⓑ 強化を検討中
Ⓒ 当面は現状のままとするが、今後、強化を検討する
Ⓓ 今後も強化を検討する予定はない

15 分析全体を通しての傾向と今後必要になると思われる施策

今回実施した EC サイトにおけるセキュリティ対策実態調査は、結果的に調査対象サイト数が僅かであったが、おおよその傾向を把握することができた。

この分析結果については、これまでの章で述べているが、分析全体を通した傾向と今後必要となるであろう施策について触れておく。

なお、本格的な実態調査については、今回の予備調査の方法をもとに、対象数を増やして再度実施したいと考える。

15.1 分析全体を通しての傾向

分析全体を通しての傾向は、以下の通りである。

- **ほとんどの EC サイトでは、脅威に対する認識について、ある程度十分なレベルにある。**
- **多くのＥＣサイトでは、自サイトのセキュリティ対策について自信を持っていない。**
- **多くのＥＣサイトでは、セキュリティ対策について組織的なマネジメントができていない。**
- **セキュリティ対策として定めたことについての実施を徹底する姿勢に欠けており、セキュリティ対策の実行レベルは当事者が考えているものより低い可能性がある。**
- **多くのＥＣサイトでは、担当者のスキルレベルが不足していると感じている。**

15.2 今後必要になると思われる施策

今回の分析の傾向から、以下のような施策が今後必要なると考えられる。

(1) 技術面・マネジメント面の両面から具体的な対策実施方法を示した、中小サイト向けの”セキュリティ対策モデル”の検討

中規模から小規模のサイトでは、セキュリティ対策を実施するために十分なスキルを持った者のいるサイトは決して多くはないであろう。このようなサイトでは、“少なくともこれぐらいの対策を行っておけば、大体のセキュリティ対策はカバーできる”といったセキュリティ対策モデルが必要とされていると考える。

(2) 特に小規模サイトを対象としたセキュリティ対策についての実践的な指導

単にセキュリティ対策モデルが示されても、それを実現するだけの体制がとれない小規模サイトも少なくはないであろう。このようなサイトに対しては、実践的な指導を行うことが必

要である。

(3) 実施しているセキュリティ対策についての第三者チェックによる診断の普及および自己評価の指導

監査等の第三者による客観的な診断を行うことにより、日頃のセキュリティ対策の妥当性を確認することができ、運用環境・システム環境の変化を反映したセキュリティ対策の見直しをより確実に行うことが可能となる。そのためには、EC サイトに対して第三者によるチェックを実施することの指導が必要であり、また常日頃より自己評価を行うことによってマネジメントサイクルを適切に回していくことも合わせて指導していくことが必要であると考える。

(4) 実施しているセキュリティ対策の実行レベルについての評価モデルの確立

第三者あるいは自己評価を行う上では、何か評価の基準となるものがなければその評価結果も曖昧なものとなってしまう可能性がある。そこで、セキュリティ対策の実行レベルについての評価尺度を与えるような評価モデルを確立し、世の中に広めていくことが重要であると考える。

【付録】

セキュリティ対策に関するアンケート調査票

― セキュリティ対策の実施状況についての質問 ―

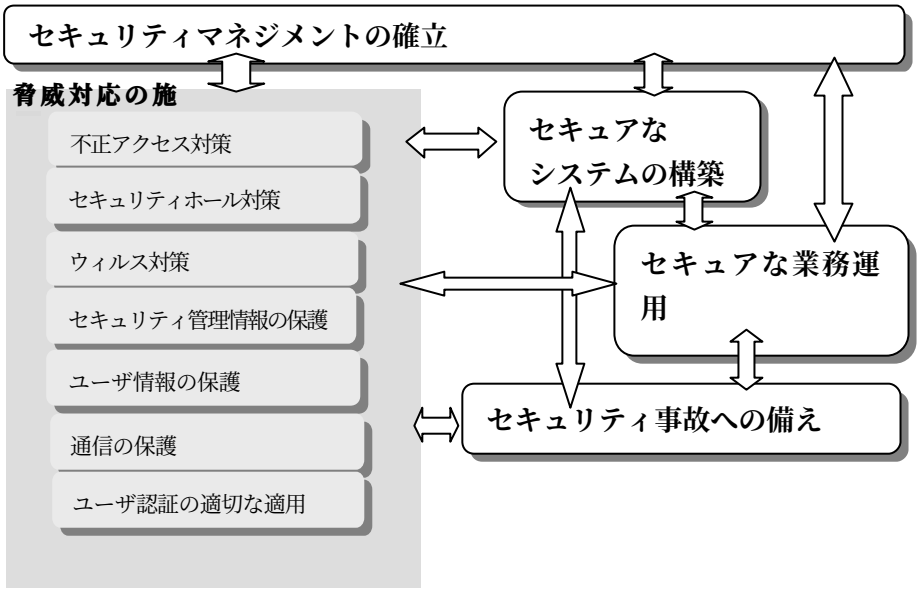
目　次

はじめに

本冊は、貴社サイトにおけるセキュリティ対策の実施状況をお訊ねするものです。いささか分厚く取付きにくい感がありますが、これは、回答を通じて貴社サイトにおけるセキュリティ対策の実施状況についての自己評価ができるように工夫したのと、個々の質問についてその主旨を付加したためです。質問事項は、全部で 130 項目です。

本調査の質問に答えることによって、貴社サイトにおけるセキュリティ対策の問題点が把握でき、セキュリティの強化につながれば幸いです。

質問は、ECOM が昨年開発した「EC サイト向けのセキュリティ対策ガイドライン」(注)が示す EC サイト運営におけるセキュリティ要求事項の体系（下図参照）をベースに、情報セキュリティの専門家をアドバイザーに加えた ECOM のセキュリティ WG のメンバーの研究により作成されたものです。



この中で、“セキュアなシステムの構築”と“セキュアな業務運用およびシステム運用の実現”は、“脅威対応の施策”や“セキュリティ事故への備え”をシステムの構成やシ業務やステム運用へ反映するものです。また、“セキュリティマネジメントの確立”は、これらの施策を戦略的かつ組織的な取組みにするためのものです。

セキュリティ対策は、サイト運営の実態に合った技術面での対応とサイト運営上のマネジメントが一体となってはじめて実現するものであり、このためには技術面での対応やセキュリティにかかわる諸活動が、常に、サイトの運営実態に合ったものとして維持されなければならないと考えます。このため、本調査における質問は、技術面での対応よりマネジメント面での質問が中心になっています。

回答にあたっての留意事項

1　回答の作成にあたって

- 回答は、本冊とは別紙の解答用紙にご記入下さい。
- 本冊にも回答を記入し、回答について当協会からの質問に対する控えとして下さい。

2　“セキュリティ対策についての質問“への回答について

- 本質問は、実際にサイトの運営およびサイトシステムの運用に責任を持っている立場の方からお答え頂きたいと考えています。このため、サイトシステムの運営のすべてあるいは一部を外部に委託しているような場合は、関係する質問に関しての回答は委託先に依頼または問合わせを行って下さい。
- 本調査は、貴社サイトで実施されているセキュリティ対策についての自己評価をお伺いすることを中心に組立てていますので、回答者の現在の認識をそのままお答え下さい。特に【評価】についての質問は、AからDまでの４段階に分かれていますが、A、B、C、Dはおおよそ以下の評価を意味しています。

  A：十分
  B：おおむね十分
  C：一通りの対策は実施しているが十分にはほど遠い
  D：未対策、あるいは対策はしていても形だけで実効的ではない

  各質問に付加したA、B、C、Dについての記述は、当該質問における評価の目安を参考として示したものです。
- 本調査は、対象とするシステムの範囲を EC サイトシステムに限定します。このため、セキュリティ対策の実施状況についての評価にあたっては、セキュリティ面から見てファイアウオール等で EC サイトシステムから隔離されたバックヤードシステムやオフィスシステムはその対象外として下さい。EC サイトシステムがこれらのシステムと渾然一体となっているシステムの構成をとっている場合は、これらに対応するシステムの構成や業務およびシステムの運用も評価に含まれなければなりません。

用語の定義

- **セキュリティ管理情報とユーザ情報**

本冊においては、保護すべき情報を、暗号鍵、パスワード、アクセス権限情報といったセキュリティのための機能がそのよりどころとする情報と、取引情報や個人情報等のユーザ情報を分け、前者をセキュリティ管理情報、後者をユーザ情報と呼び、その保護管理は別立てとし、それぞれについての対応を訊ねています（第 5 章、第 6 章参照）。

これは、セキュリティ管理情報の保護の不備は、サイトのセキュリティ全体を危うくするものであるという認識から、その保護管理はユーザ情報より一段と厳格であるべきで、同じレベルで対策を評価するのは妥当ではないとの考えにもとづくものです。

- **機器、サーバ**

第 9 章のシステム構成の考え方の質問の中で用いられている“機器”とは、サーバマシン、PC 等を指し、ハードウエアとそれに搭載されるソフトウェアのすべてを含みます。

なお、Web サーバ、Mail サーバ等の表現におけるサーバは、特定の機能を指す場合と、特定のサービスのために準備された機器を指す場合があります。

第 1章　セキュリティマネジメントの確立

EC サイトが必要なレベルのセキュリティを確保するには、まず、セキュリティ対策を計画的、組織的に行うための基盤の確立が必要で、このためには以下のようなことが必要となります。

- サイト運営関係者間でのセキュリティについての意識の徹底
- セキュリティ対策の目標の明確化
- セキュリティ対策のフレームワークの適切な確立
- セキュリティ対策の実施体制の確立
- セキュリティ対策の実施を指導、管理する仕組みの確立
- 適切な予算の確保
- 関係者の必要なスキルの確保

ここでは、貴社サイトにおけるこれらについての取組みについてお聞かせ下さい。

(1) セキュリティポリシー（セキュリティ対策基本方針）の確立

サイト運営上のセキュリティポリシーとは、サイト運営にかかる脅威についての認識の確立とセキュリティの確保に向けた取組方針を示すものです。このセキュリティポリシーはサポートしている業務の特性やシステムの構成、規模等のサイトの運営実態を反映したものでなければなりません。また、このセキュリティポリシーはサイトの運営関係者全員に徹底され、セキュリティ対策の基盤として機能していなければなりません。

(注)　“サイトの運営関係者”とは、EC サイトにおける業務担当者やシステムの構築、運用を含む、サイト運営に携わるすべての者（外部からの派遣要員も含む）を指します。

設問①〕

脅威をどのように認識していますか？

貴社ではセキュリティにかかる脅威の程度をどのように認識していますか。

【脅威に対する認識】
- Ⓐ）サイトは攻撃の対象になり易く、セキュリティにかかわる事故は事業や企業イメージに致命的な打撃を与える恐れもあり、重大な脅威と考えている
- Ⓑ）サイトは攻撃の対象になり易い。ただし、セキュリティ事故が発生しても事業や企業イメージに直接的な影響が出るとは考えていないものの、業務に混乱をきたす恐れもあり、相当の脅威と考えている
- Ⓒ）特別に攻撃の対象となるサイトでもなく、業務やサイトの運営形態からみて、セキュリティ事故の影響はそれほど重大視していない
- Ⓓ）業務やサイトの運営形態からみてあまり重大視していないが、脅威は意識している
- Ⓔ）特に気にしていない

設問②〕

問題視している脅威はどんなものですか？

以下にあげる EC サイトの運営上考えられる脅威のそれぞれについて、感じている脅威はどの程度ですか。

【認識している脅威とそのレベルについての認識】

(A) なりすましによる他人をかたった者との取引	大、中、小、無視）
(B) 外部に提供しているサービスの不正な使用	大、中、小、無視）
(C) システムへの侵入によるシステムの勝手な操作	大、中、小、無視）
(D) システムへの侵入やウイルス等による情報の漏洩	大、中、小、無視）
(E) システムへの侵入等によるシステム上の情報の改ざん	大、中、小、無視）
(F) システムへの侵入等によるホームページの改ざん	大、中、小、無視）
(G) システムへの侵入やウイルス等によるシステムの破壊	大、中、小、無視）
(H) 通信データの盗聴	大、中、小、無視）
(I) 通信データの改ざん	大、中、小、無視）
(J) 通信の否認	大、中、小、無視）
(K) 他社へのウイルスの配布	大、中、小、無視）
(L) 他社サイトの攻撃の踏み台にされること	大、中、小、無視）
(M) その他（　　）	大、中、小、無視）

設問③】

セキュリティ事故の事業や業務への影響で懸念していることはどんなことですか？

以下にあげるセキュリティ事故が貴社の事業や業務に及ぼしうる影響の大きさをどの程度と考えていますか。

【想定されるセキュリティ事故の影響の度合いについての認識】

(A) 取引についてのトラブルへの対応	大、中、小、無視レベル）
(B) 情報の漏洩にともなうトラブルへの対応	大、中、小、無視レベル）
(C) サービスの提供や業務の混乱に対する対応	大、中、小、無視レベル）
(D) 事故状況や被害範囲の調査の手間	大、中、小、無視レベル）
(E) システムや失われた情報の回復にかかる手間	大、中、小、無視レベル）
(F) 他社にかけた迷惑の後始末	大、中、小、無視レベル）
(G) 訴訟や損害賠償請求への対応	大、中、小、無視レベル）
(H) 企業あるいはサイトの信用の失墜	大、中、小、無視レベル）
(I) その他（　　）	大、中、小、無視レベル）

設問④】

貴社での脅威への対応についての基本方針は？

貴社でのセキュリティ対策の基本方針に最も近いものを、下 記の中から選んで下さい。

【脅威への対応についての基本方針】

(A) セキュリティ対策は事業の基盤と考え、必要な予算および体制を確保し、可能な限りの対策を実施する

(B) 予算、体制に限界はあるができる限りのセキュリティ対策を実施する

（C）ファイアウォールの設置やウイルス対策ソフトの導入等の一般的な対策は実施するが、セキュリティ対策に特に注力はしていない

(D) 実際問題としての脅威は感じないため特に対策はしない

(E) 保護が必要なところはネットワークから切り離し、セキュリティ対策は不要なシステムとする

(F) その他（　　）

設問⑤〕

サイトの運営全体にかかるセキュリティポリシーは宣言されていますか？

脅威についての認識ならびに脅威への対応についての基本方針を示すものとして、セキュリティポリシーを確立し宣言することが望ましいとされています。その内容としては以下に示すようなものが求められます。セキュリティポリシーの求めるところや記述の範囲やレベルはサイトの運営実態によって異なり、対象業務の特性やシステムの規模、構成、および運営体制等のサイトの運営実態に合ったものでなければなりません。

- サイト運営上でのセキュリティポリシーの位置付け
- 対象となる組織、業務、システム等
- セキュリティ確保についての基本方針
- セキュリティ対策の組立て

貴社サイトにおけるセキュリティポリシーについて評価して下さい。

【評価】

Ⓐ)サイトの運営実態を適切に反映した実効的なセキュリティポリシーが経営レベルから宣言されている

Ⓑ)宣言されたセキュリティポリシーはあるが形式的であり、実効的なものにするためには内容、記述とも見直しが必要

Ⓒ)担当者レベルでのセキュリティへの取組みについての共通認識はあるが、セキュリティポリシーとして定義したものはない

Ⓓ)セキュリティに対する取組みが明確でない

②セキュリティ対策の推進体制

サイトのセキュリティ対策は、さまざまな活動の集合体であり、多くの関係者の総合力に依存します。このため、セキュリティの確保に関し、組織の誰がどのような責任を持っているかが明確になっていなければなりません。そのためには、関係者それぞれが、自己の責務を周知しその遂行に必要なスキルを有していることが必要となるとともに、これら関係責任者間の連携体制の確立も重要です。

また、セキュリティ対策の実施には高度の技術も必要となることから、外部の専門家の有効活用もそのポイントの一つです。

設問①〕

セキュリティ対策を統括する責任者は存在しますか？

セキュリティの確保にはサイトのセキュリティ対策を統括する人の存在が必要となります。貴社サイトでは、どのような立場の方がセキュリティ対策を統括していますか。

【責任者の立場】
Ａ)経営陣
Ｂ)部長クラス
Ｃ)課長クラス
Ｄ)その他（　　）
Ｅ)責任者は特に指名していない

設問②】

経営陣は推進体制に参画していますか？

セキュリティの確保は経営レベルの課題です。このため、経営に責任を持つ人がセキュリティ対策の推進体制の指導者として参画することが望ましいとされています。

貴社サイトにおけるセキュリティ対策の推進体制への経営陣の参画状況を評価して下さい。

【評価】
Ａ)セキュリティについて十分な認識がある経営陣が参加しており、適切な指導を行っている
Ｂ)報告を受け経営レベルの問題には対処するが、チェックや指導を行うまでには至っていない
Ｃ)体制の中には含まれているが、形式的であり実際上機能はしていない
Ｄ)経営陣は推進体制に参画していない

設問③】

セキュリティ対策の推進体制は整備されていますか？

セキュリティ対策が決められていても、セキュリティ対策にかかるさまざまなタスクの担当者が明確にされ、担当者の一人一人が自己の責務を承知していなければ、セキュリティ対策は機能しません。

貴社サイトにおけるセキュリティ対策推進体制の整備状況について評価して下さい。

【評価】
Ａ)確立した体制が組まれており、関係者は自分のタスクを承知し、体制は十分に機能している。また、適宜、見直しも行われ、常にサイトの運営実態に適合したものになっている
Ｂ)十分に検討された体制やタスクの定義はあるが、見直しはあまり行われておらず、運営実態に適合しないところもある
Ｃ)セキュリティ推進体制は形作られてはいるが、タスクの定義や担当者の認識等は不十分で形式的なレベルである
Ｄ)セキュリティ対策推進のための体制はない。それぞれの担当が自分の責務の範囲で対応している

参考)セキュリティ対策の推進体制の確立には、先にあげた統括責任者の指名とその責任の明確化に加え、以下のようなタスクの実行に責任を持つ者の指名が必要となります。また、関係者が連携できるような仕組みの構築も必要となります。

・不正アクセス対策の実施
・セキュリティホール対策の実施

・ ウイルス対策の実施
・ セキュリティ管理情報の保護管理の実施
・ ユーザ情報の保護管理の実施
・ 通信にかかるリスク対策の実施
・ ユーザ認証の管理の実施
・ セキュアなシステムの構築
・ セキュアなシステム運用の実現
・ セキュリティ事故への対応
・ 関係者に対するセキュリティ教育とセキュリティ面での管理の実施
・ セキュリティ監査の実施

設問④】

セキュリティ対策を担当する者の技術レベルは十分ですか、また必要な技術の習得のための努力は行われていますか？

セキュリティ対策を担当する者が必要なスキルを有していなければセキュリティ対策は適切に実行できません。組織がセキュリティ対策に必要なスキルを確保するためには、以下に示すような施策も必要となります。

- 必要な知識やスキルの把握
- 関係者に対する必要な知識やスキルの習得についての動機や機会の付与
- 関係者における必要な知識やスキルの習得状況の把握

貴社サイトにおけるセキュリティ対策にかかるスキルの向上に向けた努力を評価して下さい。

【評価】
Ⓐ)積極的に教育を行っており、必要な知識、スキルを十分に有している。問題があってもほとんど独力で対応可能である
Ⓑ)教育等の実施により一通りの知識、スキルを有しているが、十分とは感じていない。問題が生じた場合、外部の専門家と連携することにしている
Ⓒ)担当者の自主的な学習に依存しており、知識やスキルは基本的なレベル。外部の支援に頼るところが多い
Ⓓ)セキュリティに関する知識、スキルはほとんど有していない。セキュリティ対策のすべてを外部からの支援に依存している

設問⑤】

システムベンダー、セキュリティサービスベンダー、コンサルタントの支援を活用していますか？

強固なセキュリティ対策を実施するには専門的な知識、技術が必要となります。このため、外部のサービスや専門家を活用することも有効な手段となります。

貴社におけるセキュリティ対策の実施にあたっての外部の支援の活用状況をお訊ねします。

【支援依頼の形態】複数回答）
Ⓐ セキュリティ対策の一部を委託
Ⓑ 契約にもとづく定常的な支援を依頼
Ⓒ 必要に応じた支援を依頼
Ⓓ システム構築支援他のサービスの延長線での支援を依頼
Ⓔ その他（　　）
Ⓕ 何も依頼していない

【支援依頼先】前問で F 以外を回答した方のみお答え下さい。複数回答）

Ⓐ システムベンダー
Ⓑ システムプロダクトベンダー
Ⓒ セキュリティプロダクトベンダー
Ⓓ セキュリティサービスベンダー
Ⓔ 専門コンサルタント
Ⓕ その他（　　）

【支援依頼事項】最初の質問で F 以外を回答した方のみお答え下さい。複数回答）

Ⓐ セキュリティマネジメントの指導
Ⓑ セキュリティ監査（セキュリティ対策の実施状況のチェック）の支援
Ⓒ セキュリティ監査（セキュリティ対策の実施状況のチェック）の委託
Ⓓ システム構築、維持管理についての技術指導
Ⓔ システムの脆弱性診断の支援
Ⓕ システムの脆弱性診断の委託
Ⓖ 侵入監視の支援
Ⓗ 侵入監視の委託
Ⓘ セキュリティ事故処理の支援
Ⓙ セキュリティ情報の入手および評価の支援
Ⓚ その他（　　）

【支援を得ていない理由】
最初の質問で F を回答した方のみお答え下さい。複数回答）

Ⓐ それほど脅威を感じておらず、必要性を感じない
Ⓑ 自力で対応が可能
Ⓒ 予算上の問題
Ⓓ これまで特に検討しなかったため
Ⓔ サービスの存在を知らなかったため
Ⓕ その他（　　）

【今後の外部の支援サービスの利用について】
最初の質問で F を回答した方のみお答え下さい。複数回答）

Ⓐ 計画中
Ⓑ 検討中
Ⓒ 今後検討
Ⓓ 今後も考えない

【今後、外部の支援サービスの利用を考えている場合その対象サービス】
前問で A、B、C を回答した方のみお答下さい。複数回答）

Ⓐ セキュリティマネジメントの指導
Ⓑ セキュリティ監査（セキュリティ対策の実施状況のチェック）の支援
Ⓒ セキュリティ監査（セキュリティ対策の実施状況のチェック）の委託
Ⓓ システム構築、維持管理についての技術指導
Ⓔ システムの脆弱性診断の支援
Ⓕ システムの脆弱性診断の委託
Ⓖ 侵入監視の支援
Ⓗ 侵入監視の委託
Ⓘ セキュリティ事故処理の支援
Ⓙ セキュリティ情報の入手および評価の支援
Ⓚ その他（　　）

③セキュリティ対策予算の確保

セキュリティ対策にはコストがかかります。セキュリティポリシーを具現化するための具体策の実施に必要な予算は確保されなければなりません。このためには、経営コストの中でセキュリティ対策費が意識され適切に審議されるべきです。

設問①〕

セキュリティ対策予算は適切に検討されていますか？

セキュリティ対策にかかる費用としては参考に示すようなものがあげられます。

貴社サイトにおけるセキュリティ予算の位置付けについてお訊ねします。

【セキュリティ予算の位置付け】

Ⓐ セキュリティ対策のための予算は他の費用とは別立てで計上され審議されている

Ⓑ 他の予算と別立てで計上するまでは至っていないが、セキュリティ予算として審議されている

Ⓒ セキュリティ対策に必要な予算は、システムの導入や維持管理あるいは運用予算に含まれて計上、審議されており、セキュリティ対策に焦点をあてた予算の検討は行われていない

Ⓓ セキュリティ対策予算としての意識はない

参考）セキュリティ対策予算として計上すべき費用

- ファイアウォールやウイルス対策ソフト等のセキュリティ対策に使用する設備やソフトウェア等にかかる費用
- セキュリティ対策にかかるシステムの維持管理ならびに運用にかかる費用
- セキュリティサービスの利用等外部に委託している支援にかかる費用
- セキュリティ事故対策に必要な費用

設問②〕

セキュリティ対策に必要な費用は投入されていますか？

貴社サイトにおけるセキュリティ対策にかかる予算の確保状況を評価して下さい。

【評価】

Ⓐ 実施したいセキュリティ対策に必要な予算はほとんど割当てている

Ⓑ 実施したいセキュリティ対策に必要な予算は要求通りではないが、おおむね割当てている

Ⓒ 予算不足のため実施したいセキュリティ対策が十分に実施できない

Ⓓ セキュリティ対策の予算はほとんど確保していない

設問③〕

貴社サイトのセキュリティ予算の規模はどのくらいですか？

貴社サイトの運営にかかるコストのうちセキュリティ予算の示すおおよその割合はどのくらいですか。なお、セキュリティ予算とは、設問①の 参考）に示した項目の予算の総額とします。

【サイトの運用予算全体に占めるセキュリティ予算の割合】
Ⓐ 15%超
Ⓑ 10%～15%
Ⓒ 5%～10%
Ⓓ 3～5%
Ⓔ 1～3%
Ⓕ 1%未満
Ⓖ ゼロ

⑷運営関係者に対するセキュリティの確保と教育

サイトのセキュリティは、サイトの運営にかかわる従業員や外部から派遣された要員等の日常の業務活動やセキュリティ対策にかかる活動に依存するところが少なくありません。サイトの運営にかかわる者のすべてが、セキュリティ要求事項を遵守し、これらの者がサイトのセキュリティ上の脅威にならないようにするためには、サイトの運営関係者に対するセキュリティ面での管理も重要な課題となります。

設問①】

業務やシステムの運用に携わる者（外部要員も含む）に対するセキュリティ面での指導や管理は適切に行われていますか？

業務やシステムの運用に携わる者（常勤者）がセキュリティ上の脅威にならないようにするためには、サイトの運営にかかわる者に対する以下に示すような施策が必要となります。

- 関係者に対する一般的なセキュリティ教育等の実施によるセキュリティについての認識の徹底
- 業務遂行上での各人のセキュリティにかかる責務の明確化とその遵守の指導
- 業務規程や雇用契約等の中で、セキュリティの脅威になる行為の牽制
- 業務プロセスの中への不正な行為を抑止するための手続きの組込み
- 関係者の行動に対するセキュリティ面からのチェックの実施

貴社サイトの運営にかかわる者に対するセキュリティ面での指導や管理を評価して下さい。

【評価】
Ⓐ 必要なルールも確立しており、必要な管理も業務プロセスの中に組込まれており、厳格に運用されている。また、関係者に対する教育指導も徹底している
Ⓑ ルールは確立しているがその運用は厳格でなく、十分な管理が行われているとは言い難い
Ⓒ 基本的な教育や指導は一通り行っているが、管理はほとんど行っていない
Ⓓ 特に何も行っていない

設問②】

一時的にサイト内に立入る者に対しセキュリティ上の管理がなされていますか？

外部の者がサイト内に（一時的に）立入ることもあります。これらの者がサイトのセキュリティ上の脅威にならないようにするためには、以下に示すようなことが必要とされています。

- サイトに立ち入る者の資格についてルールの確立
- 一時的にサイトに立ち入る者に対する行動制限についてルールの確立
- それらのルールの厳格な運用

貴社サイトにおける、サイトへの一時立入り者に対するセキュリティ面での管理状況を評価して下さい。

【評価】
Ⓐ サイトへの一時立入り者に対する管理のルールが確立しており、厳格に運用されている
Ⓑ サイトへの一時立入り者に対する管理のルールは確立しているが、それほど厳格に運用されていない
Ⓒ 問題意識はあり関係者に注意をうながしているが、ルールの確立までには至っていない。管理は関係者の注意に依存している
Ⓓ 特に何も行っていない

⑤業務委託先との連携

サイト運営上、業務を外部に委託していたり、外部からの派遣要員を受け入れたりすることもあります。業務の外部委託や外部からの派遣要員が、サイトのセキュリティ上の脅威にならないようにするためには、業務の委託先や派遣元に対するセキュリティ面での責任を明確にするとともに、適切な指導や管理も必要となります。

設問①〕
業務委託先との間でのセキュリティに関する責任は明確になっていますか？

サイトの運営にかかる業務を外部に委託している場合、業務委託先に対するセキュリティ面での責任を明確にしておく必要があります。

貴社がサイトの運営にかかる業務を外部に委託したり、外部から要員を受け入れている場合、業務委託先に対するセキュリティ面での責任の明示について評価して下さい。

【評価】
Ⓐ 業務委託契約の中で委託先の責任が明記されており、業務委託先がこの点に関して十分に認識していることも確認している
Ⓑ 業務委託契約の中で委託先の責任を記載しているが、この点に関し業務委託先との間での共通認識については不十分
Ⓒ 双方の担当者間での意思疎通はあるものの、契約書や覚書等での明示は行っていない
Ⓓ 特に何も行っていない
Ⓔ 外部に委託している業務はない

設問②〕設問①でA、B、Cを回答した方のみお答え下さい）
業務委託先に対するセキュリティ要求事項についての管理や指導は行われていますか？

業務の委託先や要員の派遣元に対し、セキュリティ要求事項についての適切な管理や指導も必要となります。

貴社サイトにおける業務委託先や要員の派遣元に対するセキュリティにかかる管理についての取組状況を評価して下さい。

【評価】
Ⓐ 業務委託先の協力を得て十分な管理や指導を行っている
Ⓑ 業務委託先との間で決められたルールにもとづき連携をとっているが、管理や指導は十分とは言えない
Ⓒ 担当者レベルの注意に依存しており、組織的な管理、指導は行っていない
Ⓓ 特に何も行っていない

⑹ セキュリティ監査の実施

サイトのセキュリティの確保は、計画されたセキュリティ対策の妥当性と、求められているセキュリティ対策の確実な実行により達成されものです。しかし、十分に検討したセキュリティ対策も、サイトの運営方法やサイトシステムの変更等の運営環境の変化に対応して、その妥当性を維持して行くこと、ならびに、日々の業務の運営やシステムの運用が、常にセキュリティの確保に関し求められていることに対応できているようにすることは、なかなか難しいと考えなければなりません。

このため、セキュリティ対策の妥当性とサイトの運営現場でのそれらの実施状況についての内部監査を定期的に行い、問題点の発見と必要な是正処置の実施も、サイト運営におけるセキュリティの確保には欠かせないものです。

（注）ここで言う内部監査とは、組織的で総合的なチェックを指し、正式に監査という形にはとらわれないものとします。

設問①】

セキュリティ対策の実施状況についての内部監査は行われていますか？

貴社サイトにおける、サイトの運営全体を対象としたセキュリティ対策の実施状況についての内部監査の実施状況を評価して下さい。

【評価】
Ⓐ 十分に計画された組織的な監査を年に１回以上実施している
Ⓑ 組織的な監査が年に１回以上行われているが、十分に計画されたものとは言い難い
Ⓒ 担当者レベルで自主的なチェックが年に１回程度行われているが、組織的な監査としては行っていない
Ⓓ 定期的なチェックは特に行っていない

設問②】設問①で A、B を回答した方のみお答え下さい）

セキュリティ対策の実施状況についての監査はどのような体制で行っていますか？

セキュリティ対策の実施状況について組織的な監査やチェックを定期的に行っている場合、どのような体制でチェックを実施していますか。

【監査の実施体制】
Ⓐ 監査を外部の組織に委託
Ⓑ 別部門の者も含む自社内の監査体制で実施
Ⓒ 外部の専門家の支援を得て自社内の特別体制で実施
Ⓓ サイト関係者により実施
Ⓔ 外部の専門家の支援を得てサイト内の関係者により実施

設問③〕設問①で A、B を回答した方のみお答え下さい）
セキュリティ対策の実施状況についての監査の内容は十分ですか？

セキュリティ対策の実施状況についての監査としては、以下に示すような事項についてのチェックが必要となります。

- セキュリティマネジメントの確立および展開状況
- 不正アクセス対策の実施状況
- セキュリティホール対策の実施状況
- ウイルス対策の実施状況
- セキュリティ管理情報の保護管理の実施状況
- ユーザ情報の保護管理の実施状況
- 通信に対するリスク対策の実施状況
- ユーザ認証の適用および管理状況
- システムの構成および管理におけるセキュリティ要求事項の反映状況
- システム運用におけるセキュリティ要求事項の反映状況
- セキュリティ事故への備えの状況

貴社サイトが行っているセキュリティ対策の実施状況について監査の内容を評価して下さい。

【評価】
Ⓐ 必要な事項はすべてカバーしており、充実したものである
Ⓑ おおむね十分なものと考えているがまだ改善する余地はある
Ⓒ 一通りの項目はカバーしているが、監査としては、さらなる充実が必要である
Ⓓ 断片的で、全体的な再構築が必要である

設問④〕設問①で A、B を回答した方のみお答え下さい）
セキュリティ対策の実施状況についての監査は有効ですか？

貴社サイトにおけるセキュリティ対策の実施状況について監査を評価して下さい。

【評価】
Ⓐ 問題点の指摘も十分で、指摘事項に対しては迅速に改善が行われている
Ⓑ 問題点の指摘や指摘された問題点のフィードバックには不満な点があるが、監査は有効的で機能している
Ⓒ 指摘された問題点に対するフィードバックは不十分で、チェックの実施が活かされているとは言い難い
Ⓓ 問題点もそれほど指摘されず、あまり機能していない

第 2章　不正アクセス対策

不正アクセス対策とは、EC サイトシステムへのアクセスに対し、正規の者（許可された者）がその権限範囲内で行うアクセスに限定しそれ以外のアクセスを排除すること、および不審なアクセスを監視し、サイトの外部および内部からのシステムへの侵入を防ごうとするものです。

ここでは、貴社サイトシステムにおける不正アクセス（侵入）対策の実施状況についてお聞かせ下さい。

⑴ アクセス制御

EC サイト内に置かれた機器やサービスへの不正なアクセスを防ぐためには、サイトと外部ネットワークの通信やサイト内の機器間の通信の制御を適切に行うとともに、各機器およびサービスにおけるアクセス制御を適切に行うことが必要となります。

設問①〕

サービスあるいは機能ごとに必要なアクセス制御要件が適切に指定されていますか？

サービスや機能に対するアクセス制御要件の指定には、以下のような事項についての指定が必要となります。

- アクセス権限保有者の範囲
- アクセス権限保有者の識別および認証要件
- 必要に応じたアクセス要求ポイントの制限
- 接続時間の制限
- システムユーティリティの使用についての要件

貴社サイトにおける各システムに搭載されているサービスや機能に対するアクセス制御要件の指定を評価して下さい。

【評価】

Ⓐ 各機器におけるサービスや機能に対するアクセス制御要件の指定時のレビューや定期的な見直しも、組織的に厳格に行われていて、すべてにわたり指定の妥当性は維持されている

Ⓑ アクセス制御要件の指定時のレビューや定期的な見直しが組織的に行われることになっているが、厳格に運用されておらず、妥当性を欠くところが見逃されている可能性もある

Ⓒ 担当者レベルでの指定にあたってのレビューや見直しは行われているが、これらは担当者の注意に依存している

Ⓓ 指定時のレビューや見直しはあまり行われていなく、実質的に無管理状態に近い

設問②〕

アカウントの指定は適切に管理されていますか？

アクセス制御要件が確立していても、アカウントの指定の管理がずさんであれば、アクセス制御は無意味になります。このため、アカウントについては以下のような管理が必要となります。

- ルールにもとづいたアクセス権限保有者の指定とアカウントの割当て
- 使用するアカウントの登録、付与、抹消等のライフサイクル管理
- 認証情報の保護管理

貴社サイトにおけるアカウントの管理を評価して下さい。

【評価】
Ⓐ 確立した管理ルールのもとで組織的な管理が厳格に行われている
Ⓑ ルールにそった組織的な管理が行われることになっているが、その運用は厳格でなく、不適切なところが見過ごされている可能性もある
Ⓒ 管理ルールは確立していないが、担当者レベルで一通りの管理は行われている
Ⓓ 担当者レベルでの管理も行われてなく、ほとんど無管理状態である

設問③〕

各機器におけるアクセス制御についての設定は、指定されたアクセス制御要件を正しく反映していると確認されていますか？

機器ごとに組込まれたアクセス制御についての諸設定は、当該機器におけるアクセス制御要件を満足するものでなければなりません。

貴社サイトにおけるこの点についての確認状況を評価して下さい。

【評価】
Ⓐ 設定時の確認や定期的な見直しも、組織的に厳格に行われていて、すべてにわたり設定の妥当性は確認されている
Ⓑ 設定時の確認や定期的な見直しは組織的に行われることになっているが、厳格に運用されておらず、設定のミスや要件の変更への追随が見逃されている可能性もある
Ⓒ 担当者レベルでの設定の確認や見直しは行われているが、これらは担当者の注意に依存している
Ⓓ 設定時の確認や見直しはあまり行われていない

設問④〕

ルータ、ファイアウォール、プロキシ等を用いている場合、これらに求める通信の制御についての要件の指定は適切なものになっていることが確認されていますか？

ルータやファイアウォールやプロキシ等を用い、サイトと外部ネットワーク間の通信やサイト内のサーバやクライアント間の通信の制御を行う場合、これらにおける通信の制御についての要件指定は、各機器における各サービスのアクセス制御要件や、サイトのネットワークの構成および各機器でのアクセス制御についての役割分担により決まります。

ルータやファイアウォールやプロキシ等の通信を制御する機器が、期待通りの働きをするためには、これらの機器に対して指定された制御要件が、各機器における各サービスのアクセス制御要件や、サイトのネットワークの構成および各機器でのアクセス制御についての役割分担を的確に反映したものでなければなりません。

貴社サイトにおけるこれらの機器に対する通信の制御要件の指定についての妥当性の確認

状況を評価して下さい。

【評価】
- Ⓐ これらの機器における通信に対する制御要件の指定時のレビューや定期的な見直しも、組織的に厳格に行われていて、すべてにわたり指定の妥当性は維持されている
- Ⓑ アクセス制御要件の指定時のレビューや定期的な見直しが組織的に行われることになっているが、厳格に運用されておらず、妥当性を欠くところが見逃されている可能性もある
- Ⓒ 担当者レベルでの指定にあたってのレビューや見直しは行われているが、これらは担当者の注意に依存している
- Ⓓ 指定時のレビューや見直しはあまり行われていなく、実質的に無管理状態に近い

設問⑤〕

外部およびサイト内の各ネットワークセグメント間の通信の制御に関する諸設定は、指定された通信に対する制御要件を正しく反映していると確認されていますか?

貴社サイトにおけるルータやファイアウォール、プロキシ等における通信の制御にかかる機能の選択や諸設定の確認状況を評価して下さい。

【評価】
- Ⓐ 設定時の確認や定期的な見直しも、組織的に厳格に行われていて、すべてにわたり設定の妥当性は確認されている
- Ⓑ 設定時の確認や定期的な見直しは組織的に行われることになっているが、厳格に運用されておらず、設定のミスや要件の変更への追随が見逃されている可能性もある
- Ⓒ 担当者レベルでの設定の確認や見直しは行われているが、これらは担当者の注意に依存している
- Ⓓ 担当者レベルでの設定時の確認や見直しはあまり行われてなく、実質的に無管理状態に近い

(2) 個々のサーバ(システム)に対する搭載サービスの管理

各機器に搭載しているサービス(アプリケーション)やソフトウェアが、システムへの不正アクセスの足掛かりに使われないようにするためには、使用しないサービスやスクリプト、および内容の不明なサービスやスクリプトは除去または停止して、システム上に動作できる状態で放置されないようにすることが必要です。

設問①〕

各機器に対するサービスやソフトウェアの搭載制限は適切に指定されていますか?

個々の機器におけるサービスやソフトウェアの搭載が適切なものであるためには、以下に示すようなことを明確にしておくことが必要です。

- 通常使用するサービスやソフトウェアの指定
- 通常使用しないが稼動状態で搭載しておくサービス
- 停止状態にして搭載しておくサービス
- 削除すべきサービスやソフトウェア

貴社サイトにおける、機器に対する搭載するサービスやソフトウェアについての制限の指定状況を評価して下さい。

【評価】
Ⓐ 各機器における搭載できるサービスとその条件の指定時のレビューや定期的な見直しも、組織的に厳格に行われていて、すべてにわたり指定の妥当性は維持されている
Ⓑ これらについての指定時のレビューや定期的な見直しが組織的に行われることになっているが、厳格に運用されておらず、妥当性を欠くところが見逃されている可能性もある
Ⓒ 担当者レベルでの指定にあたってのレビューや見直しは行われているが、これらは担当者の注意に依存している
Ⓓ 指定時のレビューや見直しはあまり行われていなく、実質的に無管理状態に近い

参考）
各機器へのサービスの搭載に関し注意すべき事項としては、以下のようなものがあります。
・必要なスクリプトについては検証を行うこと
・デフォルトでインストールされるサンプルプログラムの要否判定を厳格に行うこと
・telnet や ftp 等のサービスについては、特別なシステム（サーバ）を除いては、除去するか停止状態にしておくことが望ましいが、どうしても使用する必要がある場合は、そのアクセスについての厳重な制限を行うこと
・外部公開用 Web サーバにおいては以下に示すようなプログラムは原則として除去または停止すること
  －apache の phf 等のサンプルプログラム（CGI のサンプルファイルで、セキュリティホールがあることが知られている）
  －Windows NT/IIS における不要なサンプルプログラム
  －CGI ディレクトリにおけるsh、perl などのインタープリタ
  －また、文字を入力させる場合、ユーザが任意のコマンドを実行できないようになっているかをテストで確認しておくことが必要なプログラム（CGI のサンプルファイルで、セキュリティホールがあることが知られている）

設問②〕

各サーバ（システム）における動作中のサービスやソフトウェアは指定通りであることが確認されていますか？

貴社サイトにおける各サーバ（システム）に搭載されているサービスやソフトウェアの管理状況を評価して下さい。

【評価】
Ⓐ 当初設定時や変更時の確認および定期的な見直しも、組織的に厳格に行われていて、すべてにわたり設定の妥当性は確認されている
Ⓑ 当初設定時や変更時の確認および定期的な見直しは、組織的に行われることになっているが、厳格に運用されておらず、設定のミスや要件の変更への追随が見逃されている可能性もある
Ⓒ 担当者レベルでの設定の確認や見直しは行われているが、これらは担当者の注意に依存している
Ⓓ 担当者レベルでの設定時の確認や見直しはあまり行われてなく、実質的に無管理状態に近い

❸不正アクセスの監視

外部との通信やサイト内部の通信やサーバ（システム）およびサービスへのアクセス（要求）についてのログを取得し分析することも、不審なアクセスをチェックするためは必要となります。また、最近では、侵入監視システム（IDS）を用い、システムへの侵入の試みを監視し排除することも普及してきました。

設問①】

不正アクセスのチェック等に必要なログの取得は適切に行われていますか？

必要なログの取得が適切に行われるためには、以下のことが必要になります。

- ログ取得の対象となる通信やアクセスの対象（サービス）
- ログ取得の対象となるイベント
- 取得する情報
- 必要な取得領域の確保

貴社サイトにおけるログ取得状況を評価して下さい。

【取得しているログ】（複数回答）
（A）ファイアウォール、プロキシ等へのアクセスログ
（B）Web サーバへのアクセスログ
（C）Mail サーバへのアクセスログ
（D）DNS サーバへのアクセスログ
（E）ftpサーバへのアクセスログ
（F）DB サーバへのアクセスログ
（G）シスログ
（H）コマンド履歴等のシスログ以外のシステムログ
（I）その他（　　）
（J）ログの取得は行っていない

【対象としているイベント】（前問でJ以外を回答した方のみ回答下さい。複数回答）
（A）すべてのアクセス
（B）拒否したアクセス（不審なアクセス）
（C）その他（　　）

【アクセスログの取得についての評価】
（A）ほとんどすべてのログを取得している。また、十分な取得領域の確保と取得したログの安全な保管も十分に管理されている
（B）サイト内の通信や重要なサービスへのログは取得している。すべてを対象としてはいないが、サイトの運営形態から見て、おおむね必要なログは取得している。取得領域の確保や取得ログの安全な保管も行われることになっている
（C）ログ取得は行っているがその指定は担当者レベルであり、取得したログの保管等も担当者任せとなっている
（D）計画的なログの取得は行っていない、もしくは行っていても計画的なものではない

設問②〕

ログの取得と取得したログの安全な保管は適切に行われていますか？

必要なログの取得とその安全な保管にあたっては、ログ取得の失敗や取得したログ情報が削除、改ざんされないような安全措置と、必要な時に何時でも使用できるよう適切に保管することが重要です。このため、ログの取得にあたっては、以下のことが必要になります。

- 必要に応じたログ取得の二重化
- ログ取得に関する的確な設定とその確認
- ログ取得領域のオーバーフローによるログ喪失を防ぐための十分な取得領域の確保
- 必要なタイミングでの取得ログのアーカイブ
- 保管期間や保管場所等の取得ログの保管ルールの確立と保管ルールにもとづく保管の実施

貴社サイトにおけるログの取得およびその保管を評価して下さい。

【実施の有無について】
Ⓐ 指定したログの取得および取得したログに対する安全措置ならびに保管は、十分な計画のもとに行っており、またその管理も十分である
Ⓑ 指定したログ取得および取得したログに対する安全措置ならびに保管は十分な計画にもとづいているが、管理は十分でない
Ⓒ 担当者レベルでの管理は行っているが、十分とは言えない
Ⓓ 担当者任せとなっていて、ほとんど管理はされていない

設問③〕

取得したログの分析は適切に行われていますか？

貴社サイトにおける取得したログの分析状況についてお訊ねします。

【主要なアクセスログの分析実施状況】（それぞれにお答え下さい）
Ⓐ シスログ　　（毎日、毎週、毎月、必要の都度、あまり行っていない、ログの取得なし）
Ⓑ シスログ以外のシステムログ
（毎日、毎週、毎月、必要の都度、あまり行っていない、ログの取得なし）
Ⓒ Web のログ　（毎日、毎週、毎月、必要の都度、あまり行っていない、ログの取得なし）
Ⓓ Mail のログ　（毎日、毎週、毎月、必要の都度、あまり行っていない、ログの取得なし）
Ⓔ DB のログ　（毎日、毎週、毎月、必要の都度、あまり行っていない、ログの取得なし）
Ⓕ ftpのログ　（毎日、毎週、毎月、必要の都度、あまり行っていない、ログの取得なし）

【ログの分析の評価】（ログの取得を行っている場合のみお答えください）
Ⓐ 十分な分析が行われて大いに有効である
Ⓑ 一通りの分析は行っているが効果をあげるためにはさらに綿密な分析が必要
Ⓒ 分析は形式的であまり効果的とは思えない
Ⓓ 有効な分析になっていない

設問④〕

サイトシステムに対する侵入監視を行っていますか？

ツールの導入や外部サービスの活用等により、侵入監視を行っている場合、その実施状況についてお訊ねします。

【実施の有無について】
Ⓐ ツールを装備し自社で侵入監視を行っている
Ⓑ ベンダーの侵入監視サービスを利用している
Ⓒ 侵入監視の実施を計画中
Ⓓ 実施していないが、今後検討したい
Ⓔ 実施しておらず、今後も実施するつもりはない

【実施の効果について】（最初の質問で A、B と回答された方のみお答え下さい）
Ⓐ 現実に侵入を発見でき被害の拡大を防げた
Ⓑ 脆弱性の発見によりセキュリティの強化に寄与している
Ⓒ セキュリティ対策の十分性が確認できている
Ⓓ 現段階ではコスト手間に見合う成果はあげていない

【実施しない理由】（最初の質問で D、E と回答された方のみお答えください）
Ⓐ 脅威を感じてない
Ⓑ 業務やサイトの構成等の特性から侵入されても問題ではない
Ⓒ 採用したいが予算上の問題
Ⓓ その他（　　）

参考）
・侵入検知のための監視機能
　－ IDS と呼ばれる侵入監視システム
　－攻撃を能動的におびき寄せるハニーポットシステム
・侵入監視のための診断機能
　－アクセス履歴や稼動状態履歴の分析等のためのログ診断
　－ネットワークを介した診断
　－対象システム上で実施するホストベース診断
・外部からの侵入監視サービス
　－24 時間 365 日監視、監視レポート作成、侵入兆候の発見時の通知、
　　リモート／オンサイトによるアタック撃退

設問⑤〕（設問④で実施していると回答した方のみお答え下さい）
侵入監視ツールのメンテナンスは適切に行われていますか？

侵入監視ツールは新しい攻撃手段の登場に対応して、常に、最新のものにしておく必要があります。

貴社サイトにおける侵入監視ツールのメンテナンスの状況についてお訊ねします。

【実施状況】
Ⓐ ベンダーのサービスを利用しているので常に最新のものであると考えている
Ⓑ 原則として必要が生じた場合即日実施
Ⓒ1 週間以内に実施
Ⓓ 月に 1 度以上実施
Ⓔ それ以外（おおよその実施サイクル：　　）

第3章　セキュリティホール対策

サイトシステムを構成する機器やソフトウェアには、外部からサイトに攻撃を試みる者にとって攻撃の足掛かりとなるセキュリティホール（セキュリティ上の欠陥）が必ずと言ってよいくらい存在していると考えなければなりません。サイトシステムを構成する機器やソフトウェアに内在するセキュリティホールへの対策を徹底することもセキュアなシステムを維持するために不可欠なものです。

ここでは、貴社サイトにおけるセキュリティホール対策への取組みについてお聞かせ下さい。

(注)セキュリティホール対策としては、ソフトウェアをセキュリティホールのないものと取換える、セキュリティホールを塞ぐためのパッチを当てる等によるセキュリティホールの除去や、セキュリティホールのあるソフトウェアの動作を停止させたり、関係する機能の使用を控える等の運用面からの攻撃の無効化等があります。

⑴ セキュリティホールに対する取組方針の確立

サイトの運営実態に合ったセキュリティホール対策が適切に行われるためには、セキュリティホール対策をどのような考えのもとで行うのかが明確になっていなければなりません。

設問①〕

セキュリティホールに対してはどのような方針を持っていますか？

現在、貴社サイトにおいてはセキュリティホールに対してどのような方針で臨んでいますか。また、その方針を評価して下さい。

【セキュリティホールに対する取組方針】

Ⓐ 全ての機器を対象に既知のセキュリティホールゼロを目標
Ⓑ 全ての機器を対象に危険と判断されたセキュリティホールゼロを目標
Ⓒ 外部からアクセス可能なマシンに限定し、既知のセキュリティホールゼロを目標
Ⓓ 外部からアクセス可能なマシンにおける危険と判断されたセキュリティホールは、運用の都合に優先して対策
Ⓔ 外部からアクセス可能なマシンにおける危険と判断されたセキュリティホールは、運用の都合がつき次第できるだけ早い時機に対策
Ⓕ 通常は特に対策せず、システムのメンテナンスに合わせて対策
Ⓖ 特に方針は持っていない

【この方針の評価】

Ⓐ 万全と考えている
Ⓑ 万全ではないが、サイトの運営実態に照らせばこれで十分と考えている
Ⓒ 多少問題はあるがサイトの運営上からこのような取組みが限界
Ⓓ 問題と考えており、このような対応は脅威であると感じている

②セキュリティホールに関する最新情報の収集と分析への取組み

セキュリティホールに関する最新の情報が把握できていないと必要なセキュリティホール対策に漏れが生じることになります。このため、さまざまな情報源からセキュリティホールに関する最新情報の収集に努めるとともに、収集した情報をもとに対策の要否やその緊急度についての評価を行い、セキュリティホール対策に反映することが必要となります。

設問①〕

使用しているソフトウェア製品のセキュリティホールについての情報を収集していますか？

貴社サイトシステムにおいて使用しているソフトウェア製品に関するセキュリティホール情報の収集状況についてお訊ねします。

【セキュリティホールについての情報の収集状況】

Ⓐ セキュリティホールに関する情報の入手についてのルールや責任者も決められており、定期的に情報を入手している
Ⓑ セキュリティホールに関する情報の入手についてのルールや責任者も決められているが、励行されていない
Ⓒ 特に話題となった場合に行われることもあるが、日常は担当者の意識に依存
Ⓓ 特に意識して情報の収集は行っていない
Ⓔ かつては収集していたが現在では行っていない

【情報の収集元】

最初の質問で D、E 以外を回答した方のみお答え下さい。複数回答）

Ⓐ 製品ベンダー
ⒷJPCERT/CC 等の公的機関
Ⓒ セキュリティサービスベンダーおよびセキュリティコンサルタント
Ⓓ システムサービスベンダー
ⒺISP 等のネットワークサービスプロバイダー
Ⓕ セキュリティコミュニティサイト
Ⓖ 各種ニュースサイト

【情報の収集方法】

最初の質問で D、E 以外を回答した方のみお答え下さい。複数回答）

Ⓐ 情報提供元のホームページにアクセス
Ⓑ 無償のアラートサービス（メール，専用ウェブなど）を利用
Ⓒ 有償のアラートサービス（メール，専用ウェブなど）を利用
Ⓓ その他（　　）

【収集している情報】

最初の質問で D、E 以外を回答した方のみお答え下さい。複数回答）

Ⓐ 新しいセキュリティホールについての情報
Ⓑ 被害の状況
Ⓒ 対策の方法
Ⓓ その他（　　）

【収集している場合、その頻度】
最初の質問でD以外を回答した方のみお答え下さい。複数回答）
Ⓐ）ほとんど毎日
Ⓑ）1 週間に 1 回程度
Ⓒ）月に 1 回程度
Ⓓ）年に数回程度

【積極的に収集を行っていない場合その理由】
最初の質問で D、Eを回答した方のみお答え下さい。複数回答）
Ⓐ 必要性を感じていない
Ⓑ 情報の入手先を知らなかった
Ⓒ 忙しくて手が回らないため
Ⓓ 収集しても評価し対策を行う技術力がないため

設問②〕

収集されたセキュリティホールについての情報はセキュリティホール対策に活かされていますか？

貴社サイトにおける収集したセキュリティホール情報に対する危険度の評価や対策の要否、緊急度の判断、および対策実施への反映状況について評価して下さい。

【評価】
Ⓐ 収集した情報のすべてについて対策の要否やその緊急度についての評価、判断は組織的に行われ、対策に適切に反映されている
Ⓑ 収集した情報に対する対策の要否やその緊急度についての評価、判断は組織的に行われることになっているが徹底さに欠けるところもあり、対策への反映は十分とは言えない
Ⓒ 担当者レベルで一通りの対応は行われているが、管理はされていない
Ⓓ 収集はしているが、分析や対策への反映等はほとんど行われていない

③ システムに対するセキュリティホール検査は行っていますか？

セキュリティホール対策を行っていても対策の漏れや新しいセキュリティホールの登場等で、システムにはセキュリティホールが残存していることは、ごく普通のことと言えます。このため、システムに残されている未対策のセキュリティホールを発見するためのセキュリティホール検査は、セキュリティホール対策の要の一つとも言えます。

設問①〕

セキュリティホール対策対象機器に対し求められるセキュリティホール検査を行っていますか？

貴社サイトにおけるセキュリティホール検査の実施状況を評価して下さい。また、実施方法についてもお訊ねします。

【評価】複数回答）
Ⓐ プログラム化され自動的に実施している
Ⓑ ステム運用者による検査がルールに沿って励行されている
Ⓒ 検査実施についてのルールは決められているが、あまり励行されていない
Ⓓ 特にルールは決められておらず、運用担当者の任されている
Ⓔ ほとんど行われていない

【実施の方法】（最初の質問でＥ以外を回答した方のみお答え下さい）
Ⓐセキュリティサービスベンダーに依頼
Ⓑセキュリティホール検査ツールを導入し検査を自社で実施
Ⓒその他（　　）

【検査の対象】（最初の質問でＥ以外を回答した方のみお答え下さい）
Ⓐセキュリティホール対策の対象となるすべての機器を対象
Ⓑ外部からアクセス可能な機器すべてを対象
Ⓒ特定の機器のみ

【検査の頻度】
（最初の質問でＥ以外を回答した方のみお答え下さい。また、機器によって対応が異なる場合は、該当するものをすべて選んで下さい。）
Ⓐほぼ毎日、週に複数回、定期的に実施
Ⓑ週に１回程度定期的に実施
Ⓒ月に１回程度定期的に実施
Ⓓ月に１回未満であるが定期的に実施
Ⓔ必要が生じた場合に実施

【十分に行っていない場合、その理由】
（最初の質問でＡ、Ｂ以外を回答した方のみお答え下さい。複数回答）
Ⓐ重要性を感じていないから
Ⓑ検査ツールの購入やコンサルティングの契約などの予算が確保できないから
Ⓒ検査しても分析する技術力がないから
Ⓓ時間がないから
Ⓔ このような作業は組織内で評価されないから

設問②】

セキュリティホール検査に用いるパターンファイルのメンテナンスは適切に行われていますか？

セキュリティホール検査を行うツールには、セキュリティホールに関するパターンファイルが存在し、これは日々更新されるため、サイトにおいても常に最新のものに更新していかなければセキュリティホール検査の結果が信頼のおけないものとなります。またベンダーが公開している修正プログラム適用検査ツールにも同様のことが言えます。

貴社サイトにおけるセキュリティホールの検査に用いるパターンファイルの更新頻度についてお訊ねします。

【更新頻度】（複数回答）
Ⓐセキュリティホール検査を外部に委託しているため自社での更新は不要
Ⓑ自動更新
Ⓒパターンの更新情報を入手した都度実施
Ⓓ検査に先立って実施
Ⓔほぼ毎日、週に複数回、定期的に実施
Ⓕ週に１回程度定期的に実施
Ⓖ月に１回程度定期的に実施
Ⓗ月に１回未満であるが定期的に実施
Ⓘほとんど行っていない

④セキュリティホールの対策（除去）の実施

設問①】

対策の実施が必要と判断されたセキュリティホールに対しては、対策（除去）が迅速に行われていますか？

新しいセキュリティホールに対する評価が行われて、必要な対応が決められても、サイトの運営上の都合から、すぐに対策を実施できるとは限りません。運用とのバランスを取りながら、いかに迅速に対策を実施するかが、サイトをセキュアなものにするためのポイントの一つとも言えます。

貴社サイトにおける対策が必要と判断されたセキュリティホールに対する対策の実施状況を評価して下さい。

【評価】
- Ⓐ 脅威の程度にもよるが、重大な脅威に対しては遅滞なく対策を行っている
- Ⓑ 迅速に実施できるよう努めているが遅れ気味
- Ⓒ 対策が迅速に行われることは少ない
- Ⓓ 対策はほとんど行っていない

【重大な脅威に対する対応の平均的なタイムラグ】
（システムのメンテナンスに合わせて行っている場合は、そのサイクルでお答え下さい。また、機器によって対応が異なる場合は、該当するものをすべて選んで下さい。）
- Ⓐ 新しいセキュリティホールの情報の入手から 1～ 2日以内
- Ⓑ 新しいセキュリティホールの情報の入手から 1週間以内
- Ⓒ 新しいセキュリティホールの情報の入手から 1ヶ月以内
- Ⓓ 新しいセキュリティホールの情報の入手から 2ヶ月以内
- Ⓔ 新しいセキュリティホールの情報の入手から 2ヶ月以上

【対策を迅速に行っていない理由】
（評価で A 以外を回答した方のみお答え下さい。複数回答）
- Ⓐ 対策を検討する体制や専門的な技術能力の不足
- Ⓑ サイトの運用との関係で対策を随時に組込むことが困難なため
- Ⓒ 忙しくて手が回らない
- Ⓓ 脅威をそれほど感じないから

設問②】

セキュリティホール対策の実施は慎重に行われていますか？

OS 等のサイトシステムの基盤ともいえるソフトの入替えやこれらに対するパッチの実施によるセキュリティホール対策の実施に慎重を欠くと、システムの円滑な運用に重大な支障を与えることになります。このようなセキュリティホール対策の実施にあたっては、以下に示すような手順を組込むことが必要です。

- 対策方法の選択
- 当該対策がシステムに与える影響の調査
- ロールバックの準備
- 事前テストの実施

貴サイトにおけるセキュリティホール対策の実施手順について評価して下さい。

【評価】
Ⓐ 手順が定められており、この手順に沿って厳格な管理下で行っている
Ⓑ 手順は定められているが必ずしも守られておらず、危険がないことはない
Ⓒ 手順は確立していないが、習慣的に必要な処置はおおむねとっている
Ⓓ 担当者の注意に依存している

設問③】

システムに残された未対策のセキュリティホールは常に把握されていますか？

セキュリティホール対策はシステムの基盤となるソフトウェアのメンテナンスでもあり、対策の実施にあたっては十分な事前テストも必要であるため、運用との関係で簡単に実施するわけにはいかないのが現実です。このため、対策実施が待たされ、その間、セキュリティホールは未対策のまま残ることになります。また、当面の対策は不要と判断されたセキュリティホールも、当然、未対策のままシステムに残されています。システムに残されている未対策のセキュリティホールは、サイトの脅威として、常に正確に把握されていることが望まれます。

貴社サイトにおけるシステム上の未対策セキュリティホールの把握状況を評価して下さい。

【評価】
Ⓐ おおむね正確な把握、管理が行われており、特に危険性の高い未対策セキュリティホールについては完全に把握している
Ⓑ システム上の未対策セキュリティホールの把握はルール化されているが、励行されてなく、その情報は正確とは言えない
Ⓒ 担当者レベルである程度は把握している
Ⓓ 特に把握、管理は行われていない

設問④】

セキュリティホールをついた攻撃に対する監視を行っていますか？

システムへのセキュリティ攻撃の内容を把握することは、システムが脅威にさらされている状況を把握するためにも有効な手段です。

貴社サイトにおける攻撃監視の実施状況を評価して下さい。

【監視の実施状況】
Ⓐ攻撃の監視を常に行っている
Ⓑ 実施していない

【監視の実施形態】（前問でＣ以外を回答した方のみお答え下さい）
Ⓐ セキュリティサービスベンダー等の外部に委託
Ⓑ 監視ツールを導入し自社で実施

【監視の対象】（最初の質問でＣ以外を回答した方のみお答え下さい）
Ⓐ すべての機器を対象
Ⓑ 外部からアクセス可能な機器のみを対象
Ⓒ 特定の機器のみ

【行っていない場合その理由】最初の質問で C を回答した方のみお答え下さい）
Ⓐ重要性を感じていない
Ⓑ監視ツールの購入や外部に委託する予算が確保できない
Ⓒ時間がない
Ⓓ このような作業は組織内で評価されないから

設問⑤】

セキュリティホール攻撃の監視に用いるパターンファイルのメンテナンスは適切に行われていますか？

攻撃を監視するツールでは、日々更新される新しいセキュリティホールに関するパターンファイルが存在します。これらのパターンファイルを常に最新のものに更新しなければ悪用されるセキュリティホールの内容が把握できません。

監視ツールで利用するパターンファイルのメンテナンスの実施状況についてお訊ねします。

【パターンファイルのメンテナンス状況】複数回答）
Ⓐ セキュリティホール攻撃の監視を外部に委託しているため自社での更新は不要
Ⓑ 自動更新が行われている
Ⓒ パターンの更新情報の入手の都度実施している
Ⓓ ほぼ毎日定期的に実施
Ⓔ 毎週定期的に実施
Ⓕ 毎月定期的に実施
Ⓖ 検査の実施にあたって実施
Ⓗ ほとんど行っていない

第4章　ウイルス対策

サイトシステムにウイルスが侵入することの阻止を図るとともに、ウイルスの侵入による被害を限定的なものにするためには組織的な取組みが必要です。

ここでは、貴社サイトにおけるウイルス対策についてお聞かせ下さい。

⑴ ウイルスに対する取組方針の確立

ウイルス対策が適切に行われるためには、ウイルス対策をどのような考えで，またどのような方法で実施するかを明らかにするウイルスに対する取組方針が確立していなければなりません。

設問①〕

ウイルスに対してはどのような基本方針で臨んでいますか？

ウイルスに対する基本方針をお訊ねします。

【ウイルスに対する基本姿勢】

Ⓐ ウイルスの侵入を阻止するための手段を尽くすとともに、システムの管理を行う者だけでなく、システムに触れる者全員による取組みを行う

Ⓑ ウイルス対策ソフトの導入によるウイルスの侵入阻止は行う

Ⓒ ネットワークサービスベンダーのウイルスチェックサービスを利用することにより、サイトでの対策は行わない

Ⓓ 特に対策は行わない

⑵ ウイルスに関する最新情報の収集

ウイルスに関する最新の情報が把握できていないと必要なウイルス対策に漏れが生じることになります。このため、さまざまな情報源からウイルスに関する最新情報の収集を努めるとともに、収集した情報の分析を適切に行いウイルス対策に反映することが必要となります。

設問①〕

ウイルスについての最新情報を収集していますか？

貴社サイトにおけるウイルス情報の収集状況についてお訊ねします。

【ウイルスについての情報の収集状況】

Ⓐ ウイルスに関する情報の入手についてのルールや責任者も決められていて、定期的に情報を入手している

Ⓑ ウイルスに関する情報の入手についてのルールや責任者も決められているが、励行されてはいない

Ⓒ 特に話題となった場合に行われることもあるが、日常は担当者の意識に依存

Ⓓ 特に意識して情報の収集は行っていない

【情報の収集元】
前問でD以外を回答した方のみお答え下さい。複数回答）
Ⓐ ウイルス対策ソフトベンダー
Ⓑ 一般の製品ベンダー
ⓒIPA 等の公的機関
Ⓓ セキュリティサービスベンダーおよびコンサルタント
Ⓔ システムサービスベンダー
ⓕISP 等のネットワークサービスプロバイダー
Ⓖ セキュリティコミュニティサイト
（Ⅰ）各種ニュースサイト

【情報の収集ルート】
最初の質問でD以外を回答した方のみお答え下さい。複数回答）
Ⓐ 情報提供元のホームページにアクセス
Ⓑ 無償のアラートサービス（メール，専用ウェブなど）
Ⓒ 有償のアラートサービス（メール，専用ウェブなど）
Ⓓ その他（　　）

【収集している情報】
最初の質問でD以外を回答した方のみお答え下さい。複数回答）
Ⓐ 新種ウイルスについての情報
Ⓑ 被害の状況
Ⓒ 感染した時の対処の方法
Ⓓ その他（　　）

【収集の頻度】
最初の質問でD以外を回答した方のみお答え下さい。複数回答）
Ⓐ ほとんど毎日
Ⓑ1 週間に 1 回程度
Ⓒ 月に 1 回程度
Ⓓ 年数回程度

【収集していない場合、その理由】
最初の質問でDを回答した方のみお答え下さい。複数回答）
Ⓐ）必要性を感じないので
Ⓑ）予算がとれないので
Ⓒ）手間がかかるので

設問②】

収集されたウイルスについての情報はウイルス対策に活かされていますか？

貴社サイトにおける収集したウイルス情報に対する危険度の評価や対策の要否、緊急度の判断、および対策実施への反映状況について評価して下さい。

【評価】
(A) 収集した情報のすべてについて臨時ウイルス検査の実施等の対策の要否やその緊急度についての評価、判断は組織的に行われ、対策に適切に反映されている
(B) 収集した情報に対する対策の要否やその緊急度についての評価、判断は組織的に行われることになっているが徹底さに欠けており、情報収集は十分に活かされているとは言えない
(C) 担当者レベルで一通りの分析、評価は行われているが、管理はされてなく担当者任せとなっている
(D) 収集はしているが、分析や対策への反映等はほとんど行われていない

(3) ネットワークからのウイルスの侵入の阻止

サイトシステムへのウイルスの侵入のほとんどは、メールやメール添付ファイルあるいはダウンロードするデータやソフトウェアに付着したウイルスによるものです。このため、外部ネットワークとの接点や内部ネットワークに流れるデータやサービスの入口での受信データに対する監視によりウイルスの侵入を阻止することは、ウイルス対策の基本となるものです。

ネットワークからのウイルス侵入の阻止を適切に行うためには、ウイルス対策ソフトの配置についての方針が適切に決められ、この方針に沿ったウイルス対策ソフトの配置等が適切に行われなければなりません。

設問①】

ウイルス対策ソフトをどのように配置していますか？

貴社サイトシステムにおいてウイルス対策ソフトを配置している場所をお訊ねします。

【ウイルス対策ソフトを搭載しているマシン】（複数回答）
(A) ウイルス対策専用サーバ（ウイルスゲートウェー）
(B) ファイアウォールやプロキシ等のゲートウェイサーバ
(C) Web サーバ、Mail サーバ、ftp サーバ等の外部との通信をタスクとするサーバ
(D) グループウェアサーバ
(E) すべての一般サーバ
(F) 一部の一般サーバ
(G) すべてのクライアント
(H) 一部のクライアント
(I) まったく導入していない

設問②】（設問①で I 以外を回答した方のみお答え下さい）

現在のウイルス対策ソフトの配置をどのように評価していますか？

貴社サイトシステムにおける現在のウイルス対策ソフトの配置を評価して下さい。

【評価】
Ⓐ サイトの実態と要求するセキュリティレベルに照らして十分と考えている
Ⓑ サイトの運営実態から見ておおむね十分な配置と考えている
（C）まだ最低限のレベルであり、強化が必要と考えている
Ⓓ 適切とは言えない

【不十分と判断している場合、そのような配置になっている理由】
前問でA、B以外を回答した方のみお答え下さい。複数回答）
Ⓐ それほど脅威を感じないため
Ⓑ 予算がとれないため
Ⓒ 手間がかかるため
Ⓓ その他（　　）

【不十分と判断している場合、今後の対応】
最初の質問でA、B 以外を回答した方のみお答え下さい）
Ⓐ 現在、改善計画中
Ⓑ 現在、改善を検討中
Ⓒ 今後検討する
Ⓓ 今後も考えない

4) インストールするソフトウェアからのウイルス侵入の阻止

ウイルス対策の第一歩は、ウイルスに感染したソフトウェアをシステムにインストールしないことです。このためには、システムにインストールするソフトウェアに対しては、そのインストールにあたってウイルス検査を必ず実施し、ウイルスに感染していないことを確認しなければなりません。

設問①〕

インストールするソフトウェアに対するウイルス検査は実施されていますか？

貴社サイトにおけるインストールするソフトウェアに対するウイルス検査の実施状況を評価して下さい。

【評価】
Ⓐ ルールにもとづいた検査が厳格に行われている
Ⓑ ルールに沿った検査が行われることになっているが、励行されていない
Ⓒ インストールするソフトウェアに対するウイルス検査についてのルールはなく、インストール担当者の判断に委ねられている
Ⓓ ほとんど実行していない

【不十分と判断している場合、その理由】
前問で C、D を回答した方のみお答え下さい。複数回答）
Ⓐ 素性のはっきりしたソフトウェアしか使用しないようにしているため、必要性を感じない
Ⓑ 手間がかかるため
Ⓒ ルールで義務付けられていないため
Ⓓ その他（　　）

⑸持込まれたPCからのウイルスの侵入の阻止

感染したPCをサイト内のネットワークに接続することにより、サイトがウイルスに感染することもあります。このため、外部から持込まれるPCをサイト内のネットワークに接続するにあたっては、当該PCに対するウイルス検査を必ず行い、感染していないことを確認しなければなりません。

設問①〕

持込まれたPCに対するウイルス検査は実施されていますか？

貴社サイトにおける外部から持込まれるPCに対するウイルス検査の実施状況を評価して下さい。

【評価】

Ⓐ 外部から持込まれたり外部から持帰ったりしたPCに対しては、サイトシステムへの接続に先立ち、ウイルス検査を行うことが義務付けられており、厳格に運用されている

Ⓑ これらのPCに対してサイトシステムへの接続に先立ちウイルス検査を行うことが義務付けられているが、厳格には運用されていない

Ⓒ PCの管理者や使用者に対する指導は行われているが、当事者の注意に任されている

Ⓓ ほとんど行っていない

【行っていない場合その理由】（前問でA以外を回答した方のみお答え下さい。複数回答）

Ⓐ すべてのPCにウイルス対策ソフトが組込まれているため

Ⓑ 脅威を感じないため

Ⓒ 手間がかかるため

Ⓓ ルールで義務付けられていないため

Ⓔ その他（　　）

⑹システムに対するウイルス検査の実施

外部との通信やサイト内部の通信、サイトに持込まれるソフトウェア、ＰＣや電磁媒体等に対するウイルスの監視を行っていても、新しいウイルスの登場に対する検査パターンの更新遅れや監視の漏れ等で、システムにウイルスが侵入してしまうことがあります。このような場合、被害の発生を阻止したり、被害が拡大しないようにするためには、ウイルス感染の事実を早期に発見することが重要です。このためには、システム内の各機器に対し、できる限り高い頻度でウイルス検査を行うことが求められます。

設問①〕

Web サーバ、Mail サーバ、ftpサーバ等外部との通信に用いられるサーバに対するウイルス検査は実施されていますか？

貴社サイトにおける外部との通信に用いられるサーバに対するウイルス検査についてお訊ねします。

【ウイルス検査の実施方法】
Ⓐ 自動的に行われるようになっている
Ⓑ ルールに沿った検査をシステム運用者の手で励行している
Ⓒ 特にルールは決められておらず、担当者の判断で適宜行っている
Ⓓ ほとんど行っていない

【検査の頻度】（前問で D 以外をお答えになった方のみお答え下さい。複数回答）
Ⓐ 1日に 1 回以上定期的に実施
Ⓑ 週に 1 回以上定期的に実施
Ⓒ 月に 1 回以上定期的に実施
Ⓓ 特に決めてはいないが時々実施
Ⓔ 必要が生じたときに実施

【実施頻度が低い場合その理由】
（前問で A、B 以外を回答した方のみ回答下さい）
Ⓐ それほど脅威を感じないので
Ⓑ 手間がかかるので
Ⓒ その他（　　）

【検査に用いるパターンファイルの更新方法】
(最初の質問で E 以外を回答した方のみお答え下さい)
Ⓐ プログラム化され自動更新が行われている
Ⓑ 手動（マニュアル）で実施
Ⓒ その他（　　）

【パターンファイルの更新頻度】
(最初の質問で D 以外を回答した方のみお答え下さい。複数回答)
Ⓐ1 日に 1 回以上実施
Ⓑ 週に 1 回以上定期的に実施
Ⓒ 月に 1 回以上定期的に実施
Ⓓ 特には決めていないが必要と思われた時に実施
Ⓔ 検査に先立って実施
Ⓕ ほとんど実施していない

設問②】

一般のサーバに対するウイルス検査は実施されていますか？

貴社サイトにおける一般のサーバに対するウイルス検査についてお訊ねします。

【ウイルス検査の実施方法】
Ⓐ 自動的に行われるようになっている
Ⓑ ルールに沿った検査をシステム運用者の手で励行している
Ⓒ 特にルールは決められておらず、担当者の判断で適宜行っている
Ⓓ ほとんど行っていない

【検査の頻度】（前問で D 以外をお答えになった方のみお答え下さい。複数回答）
Ⓐ 1日に 1 回以上定期的に実施
Ⓑ 週に 1 回以上定期的に実施
Ⓒ 月に 1 回以上定期的に実施
Ⓓ 特に決めてはいないが時々実施
Ⓔ 必要が生じたときに実施

【実施頻度が低い場合その理由】
（前問で A、B 以外を回答した方のみ回答下さい）
Ⓐ それほど脅威を感じないので
Ⓑ 手間がかかるので
Ⓒ その他（　　）

【検査に用いるパターンファイルの更新方法】
(最初の質問で E 以外を回答した方のみお答え下さい)
Ⓐ プログラム化され自動更新が行われている
Ⓑ 手動（マニュアル）で実施
Ⓒ その他（　　）

【パターンファイルの更新頻度】
(最初の質問で D 以外を回答した方のみお答え下さい。複数回答)
Ⓐ1 日に 1 回以上実施
Ⓑ 週に 1 回以上定期的に実施
Ⓒ 月に 1 回以上定期的に実施
Ⓓ 特には決めていないが必要と思われた時に実施
Ⓔ 検査に先立って実施
Ⓕ ほとんど実施していない

設問③〕

クライアント対するウイルス検査は実施されていますか？

貴社サイトにおける一般のサーバに対するウイルス検査についてお訊ねします。

【ウイルス検査の実施方法】
Ⓐ 自動的に行われるようになっている
Ⓑ ルールに沿った検査をシステム運用者の手で励行している
Ⓒ 特にルールは決められておらず、担当者の判断で適宜行っている
Ⓓ ほとんど行っていない

【検査の頻度】（前問で D 以外をお答えになった方のみお答え下さい。複数回答）
Ⓐ 1日に 1 回以上定期的に実施
Ⓑ 週に 1 回以上定期的に実施
Ⓒ 月に 1 回以上定期的に実施
Ⓓ 特に決めてはいないが時々実施
Ⓔ 必要が生じたときに実施

【実施頻度が低い場合その理由】
前問で A、B 以外を回答した方のみ回答下さい）

Ⓐ それほど脅威を感じないので
Ⓑ 手間がかかるので
Ⓒ その他（　　）

【検査に用いるパターンファイルの更新方法】
(最初の質問で E 以外を回答した方のみお答え下さい)

Ⓐ プログラム化され自動更新が行われている
Ⓑ 手動（マニュアル）で実施
Ⓒ その他（　　）

【パターンファイルの更新頻度】
(最初の質問で D 以外を回答した方のみお答え下さい。複数回答)

Ⓐ1 日に 1 回以上実施
Ⓑ 週に 1 回以上定期的に実施
Ⓒ 月に 1 回以上定期的に実施
Ⓓ 特には決めていないが必要と思われた時に実施
Ⓔ 検査に先立って実施
Ⓕ ほとんど実施していない

第5章　セキュリティ管理情報の保護

セキュリティ管理情報（注）の漏洩や改ざんあるいは破壊は、サイトのセキュリティ対策の無力化やサイト運用の混乱に直結します。このため、これらの情報については特に厳格な保護管理が求められます。

ここでは、貴社サイトにおけるセキュリティ管理情報の保護管理策への取組みについてお聞かせ下さい。

（注）セキュリティ管理情報とは、管理者権限情報、システム構成情報、アクセス制御に用いられる情報、電子証明書、暗号鍵等のセキュリティを守るための機能がそのベースとする情報を指します。

(1) サイトで用いられるセキュリティ管理情報と保護ポイントの把握

セキュリティ管理情報が適切な保護を受けるためには、まず、システムが取扱っているセキュリティ管理情報が漏れなく把握され、それぞれについてどのような保護が求められるかが明確にされていなければなりません。

設問①】

システムが扱うセキュリティ管理情報は洗出され、それぞれに求められる保護が適切に決められていますか？

貴社サイトにおけるセキュリティ管理情報の把握とそのそれぞれに求められる保護の指定状況を評価して下さい。

【評価】

Ⓐ セキュリティ管理情報の把握やそれぞれに求められる保護についての指定は組織的にレビューされている。また、その見直しも適宜行われていて、セキュリティ管理情報の把握とそれぞれに対する保護についての指定の妥当性は常に維持されている

Ⓑ セキュリティ管理情報の把握やそれぞれに求められる保護についての指定は組織的にレビューされることになっているが、レビューや見直しは厳格であると言えず、セキュリティ管理情報の把握とそれぞれに対する保護についての指定の一部に妥当性を欠くところもありうる

Ⓒ 担当者レベルでのセキュリティ管理情報の把握とそれぞれに対する保護についての指定は行われているが、組織的なレビューや管理は行われていない

Ⓓ セキュリティ管理情報の保護は担当者に任されており、セキュリティ管理情報の把握

(2) システム上のセキュリティ管理情報に対する保護管理要件の指定

セキュリティ管理情報の個々に対しては、具体的な保護管理要件が適切に指定されていなければなりません。

設問①〕

セキュリティ管理情報のそれぞれに保護管理要件が適切に指定されていますか？

セキュリティ管理情報に対する保護管理要件の指定には、以下のような事項についての指定が必要となります。

- 当該セキュリティ管理情報に対するシステム操作のアクセス権限保有者の範囲
- アクセス権限保有者の指定登録方法
- 適用するアクセス管理方式
- 不審なアクセスに対する処置
- アクセス監視対象
- アクセス監視方法

貴社サイトにおけるセキュリティ管理情報に対する保護管理要件の指定状況を評価して下さい。

【評価】

Ⓐ セキュリティ管理情報に対する保護要件の指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持され、ドキュメントも整備されている

Ⓑ セキュリティ管理情報に対する保護要件の指定は、決められた手順に沿って行われることになっており、ドキュメントも整備されているが、組織的な検討やレビューおよび見直しは厳格ではなく、指定の一部に妥当性を欠いていることもありうる

Ⓒ 管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメントもあまり整備されていない

Ⓓ 担当者任せにしており、特に管理は行っていない

設問②〕

アクセス権限保有者の指定とアクセス権限保有者に付与するアクセス権の付与は適切に行われていますか？

保護管理要件が適切に指定されていても、アクセス権限保有者の指定とアクセス権限保有者に付与するアクセス権の指定が適切でなければ、適切な保護は実現しません。

貴社サイトにおける保護対象ファイルに対するアクセス権限保有者とアクセス権限保有者に付与するアクセス権の範囲の指定について評価して下さい。

【評価】

Ⓐ これらの指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている。また、ドキュメントもよく整備されている

Ⓑ これらの指定は、決められた手順に沿って行われることになっており、ドキュメント化も行われているが、組織的な検討やレビューおよび見直しやドキュメント化は厳格ではなく、指定の一部に妥当性を欠いていることもありうる

Ⓒ 管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメント化も不十分である

Ⓓ 担当者任せにしており、特に管理は行っていない

参考）アクセス権限保有者に付与するアクセス権とは、アクセス権限保有者に許されるファイルに対する操作権限を指し、厳密に言えば以下のすべてについてその可否が指定さ

れなければなりません。

・セキュリティ管理情報の生成・登録・参照・更新・削除
・セキュリティ管理情報の印刷、他の電子媒体へのコピー
・システム上のセキュリティ管理情報に対する二次加工
・セキュリティ管理情報のバックアップの取得

③ システム上の保護対象ファイルに対する保護管理の実施

システム上のセキュリティ管理情報が格納されたファイルに対して指定通りの保護が行われるためには、関係する機能がシステムに適切に組込まれ、これらの機能が使用する情報も正しく登録されていなければなりません。

設問①】

セキュリティ管理情報は保護対象要件を満足する場所に置かれていますか？

セキュリティ管理情報は論理的にアクセスする権限のない者からは容易にアクセスできない場所に保管されていることが必要です。

貴社サイトシステムでは、セキュリティ管理情報をどのような場所に格納していますか。

【保護対象の配置場所】（複数回答）
Ⓐ ネットワークからは切り離されたシステム上に配置
Ⓑ 内部セグメントに配置
Ⓒ DMZ に配置
Ⓓ インターネットに直結した場所に配置

【保護対象ファイルの配置についての評価】（複数回答）
Ⓐ 保護対象ファイルは外部からのアクセスから完全に隔離されている
Ⓑ 外部のアクセスから完全には隔離されていないが、保護要件を満たす安全な場所に配置されている
Ⓒ 一部のファイルは危険な領域にあると認識している
Ⓓ 配置場所については見当が不十分で危険な領域に置かれているものがある

設問②】

セキュリティ管理情報のメモリやハードディスク等への格納は、それらの保護についての要求を満足する形で格納されていますか？

セキュリティ管理情報のメモリやハードディスクへの格納にあたって以下に示すような格納方法を適用していますか。適用している格納方法をお訊ねします。

【適用している施策】（複数回答）
Ⓐ）暗号化して格納
Ⓑ）ディレクトリを分けて格納している
Ⓒ）その他（　　）
Ⓓ）特別な格納は行っていない

設問③〕

セキュリティ管理情報が格納されているファイルへのアクセスには、保護管理要件を満足するアクセス管理機能が的確に組込まれていることが確認されていますか？

セキュリティ管理情報が格納されているファイルに対して適用するアクセス制御やアクセス監視の機能は、的確にシステムに組込まれていなければなりません。

貴社サイトシステムにおけるセキュリティ管理情報に対する保護機能の組込みについての確認状況を評価して下さい。

【評価】

Ⓐ 当初組込み時だけでなく変更時においても、決められたプロセスに従った組織的なチェックが厳密に行われており、不備が存在する余地はほとんどない

Ⓑ 当初組込み時だけでなく変更時においても、決められたプロセスに従った組織的なチェックが行われることになっているが、厳格に運用されてなく、不備が見過ごされている可能性もある

Ⓒ 確認プロセスはあるが形式的で、組織的な管理は行われていない。担当者の注意に依存しているが、一応管理されている

Ⓓ 確認プロセスも確立されておらず、担当者任せであまり確認は行われていない

設問④〕

アクセス管理や認証に用いられる情報は常に正しく設定されていることが確認されていますか？

セキュリティ管理情報を保護するための機能がシステムに適切に組込まれていても、これらの機能が用いるアクセス権限保有者の指定やそれぞれに対するアクセス権の指定に不備があれば、保護は機能しません。アクセス管理や認証に用いられる情報の正しい設定の実現には、以下のようなことが必要です。

- 指定内容についての関係者による厳格なチェックの実施
- システムに対する指定についての十分な確認の実施
- システムの構成の変更や前提とするプラットフォームの変更、あるいは保護管理要件の見直しに伴う指定の見直しと変更の実施
- 指定状況についての正確なドキュメントの作成

貴社サイトシステムにおけるこれらの情報の設定の管理状況を評価して下さい。

【評価】

（A）この設定は決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている。またドキュメントもよく整備されている

Ⓑ この設定は決められた手順に沿って行われることになっており、ドキュメントも整備されているが、組織的な検討やレビューおよび見直しは厳格ではなく、設定の一部に妥当性を欠いていることもありうる

Ⓒ 設定およびその管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメント化も不十分である

Ⓓ 担当者任せにしており、特に管理は行っていない

設問⑤〕

システム上のセキュリティ管理情報に対するアクセスの監視を行っていますか？

システム上のセキュリティ管理情報の保護をより強固なものにするためには、セキュリティ管理情報へのアクセスに対する監視も求められます。

貴社サイトシステムにおけるシステム上のセキュリティ管理情報に対するアクセスの監視を評価して下さい。

【評価】

Ⓐ アクセスの監視が必要な情報の洗出しと監視要件の指定は十分に検討されている。また、アクセスログの分析もルーチン化されており、必要な監視は励行している

Ⓑ アクセスの監視が必要な情報の洗出しと監視要件の指定、これらの指定にもとづいたアクセスログの取得と分析も行われているが、監視対象の洗出しや監視要件の指定やアクセスログの分析は十分とは言えない

Ⓒ 一部の情報に対してアクセスログの取得と分析が行われているが、監視が必要な情報の洗出しやそれらに対する監視要件の指定等は組織的に検討されていない

Ⓓ 行っていない

設問⑥〕

定期的にセキュリティ管理情報の改ざん検知は行われていますか？

万一セキュリティ管理情報が改ざんされたような場合、被害の拡大を防ぐためには改ざんの事実が早期に発見されなければなりません。

貴社サイトにおけるセキュリティ管理情報の改ざん検知を評価して下さい。

【評価】

Ⓐ セキュリティ管理情報のほとんどに対し改ざん検知を行う仕組みを組込んでいる。

Ⓑ 特に重要と思われるセキュリティ管理情報に対してのみ定期的に改ざん検知を行っている

Ⓒ システムへの侵入の形跡が発見された場合等、必要と判断された場合のみ実施

Ⓓ 行っていない

⑷ 業務現場やシステムの運用現場におけるセキュリティ管理情報の適切な取扱い

セキュリティ管理情報の保護は、業務現場やシステム運用の現場における取扱いにも依存します。セキュリティ管理情報が記録された印刷物や電磁媒体（注）についての慎重な取扱いに加え、スクリーンにこれらを表示したまま放置しないといったような、これらの情報にアクセスする時の操作においても注意が必要です。

(注)電磁媒体とは、磁気テープや磁気ディスク、光ディスク、パソコン、サーバ、携帯端末等の本体内蔵の記憶装置・ディスク類を指します。

設問①〕

システム運用現場や業務現場におけるセキュリティ管理情報の取扱いについてのルールは決められていますか？

システム運用の現場や業務現場におけるセキュリティ管理情報の取扱いについては、以下に示すようなことについてのルールが決められていなければなりません。

- セキュリティ管理情報のオーナーシップ
- 対象となる印刷物や電磁媒体の特定
- システム上のこれらの情報へのアクセスやその操作上のルール
- セキュリティ管理情報が記載された印刷物の取扱い
- セキュリティ管理情報が記録された電磁媒体や PC の取扱い

貴社サイトのおけるセキュリティ管理情報の取扱いについてのルールの確立状況を評価して下さい。

【評価】

Ⓐ システム運用現場における保護対象のセキュリティ管理情報が記録された印刷物や電磁媒体の洗出し、それぞれに求められる取扱いルールの指定は組織的な管理のもとで行われている。また、その見直しも含め管理プロセスも確立している

Ⓑ システム運用現場における保護対象のセキュリティ管理情報が記録された電磁媒体等の洗出しやそれぞれに求められる取扱いルールの指定は、決められた手順に沿って組織的には行われているが検討は十分とは言えない

Ⓒ 特に重要なものについてのみ取扱いルールが決められている

Ⓓ 保護対象の電磁媒体等の保護は特に考えてはいない

参考 1) セキュリティ管理情報を記載した印刷物および電磁媒体に対する取扱いルールで規定すべき事項

- 作成手順や作成が許される者等の作成に関する制限
- 参照、コピー、二次加工等の使用上の制限
- 外部への持出しについての制限
- 外部への提供についての制限
- 保管場所、保管責任者等の保管要件
- 廃棄の方法
- 上記についての記録の作成と保管

設問②) (設問①で D 以外を解答した場合のみお答えください)

システム運用の現場や業務現場において保護対象となるセキュリティ管理情報が記録された PC や電磁媒体に対する取扱いルールは守られていますか？

業務の現場におけるセキュリティ管理情報が記録された PC や電磁媒体の取扱い状況を評価して下さい。

【評価】

Ⓐ 取扱いルールはシステムの運用現場や業務現場に徹底されており、厳格に運用されている

Ⓑ おおむね取扱いルールにもとづいた保護が行われているが厳格とはいえない

Ⓒ 取扱いルールが示されているが管理や指導はほとんど行われておらず、個人の意識に依存している

Ⓓ ほとんど守られていない

第 6 章　ユーザ情報の保護

顧客の個人情報、取引先の商業秘密情報、取引情報等のユーザ情報の漏洩は、消費者のプライバシーの侵害や取引先のビジネスの妨害につながります。また、これらの情報に対する改ざん、破壊は、業務の運営を混乱させることにもなります。

ユーザ情報の保護管理とは、消費者のプライバシー侵害や取引先のビジネス妨害に加担することのないよう、これらの情報を含むデータやファイル等に、漏洩、改ざん、破壊が生じないようにするための施策を総称するものです。

ここでは、貴社サイトにおけるユーザ情報の保護管理策への取組みについてお聞かせ下さい。

⑴ 保護対象のユーザ情報と保護ポイントの把握

ユーザ情報が適切な保護を受けるためには、まず、システムが取扱っているユーザ情報が洗出され、そのうち保護の対象となるものについては、どのような保護が求められるかが明確にされていなければなりません。

設問①〕

システムが扱うユーザ情報は洗出され、それぞれに求められる保護が適切に決められていますか？

貴社サイトにおける保護対象ユーザ情報の洗出しとそれぞれに求められる保護の指定状況を評価して下さい。

【評価】

Ⓐ サイトが取扱うすべてのユーザ情報は洗出され、それぞれに求められる保護についての指定は組織的に検討、レビューされている。また、その見直しも適宜行われていて、保護対象のユーザ情報の把握とそれぞれに対する保護についての指定の妥当性は常に維持されている

Ⓑ この指定は組織的にレビューされることになっているが、レビューや見直しは厳格であると言えず、保護すべきユーザ情報の把握とそれぞれに対する保護についての指定に漏れや一部に妥当性を欠くところもありうる

Ⓒ 担当者レベルの作業ではあるが、保護対象とすべきユーザ情報の洗出しやそれぞれに対する保護についての指定が行われている。組織的なレビューや管理は行われていない

Ⓓ 保護対象のユーザ情報の洗出しやその保護についての指定等は行われていない

参考）一般には、以下のような保護対象となるユーザ情報があります。

個人情報、経営情報、取引情報、信用情報、設計情報、等々

設問②〕

保護対象となる情報が含まれるファイルやメッセージは正確に把握されていますか？

ユーザ情報の保護が適切に行われるためには、保護の対象となる情報が含まれるファイルやメッセージ等が正確に把握されていなければなりません。

貴社サイトシステムにおける保護対象情報の存在場所の把握状況を評価して下さい。

【評価】

Ⓐ 保護の対象となるユーザ情報の存在場所の洗出しは、組織的にレビューされている。また、その見直しも適宜行われておりドキュメント化も十分で、保護対象のユーザ情報の存在場所は常に正確に把握されている

Ⓑ 保護対象のユーザ情報の存在場所の指定は組織的にレビューされることになっており、ドキュメント化も行われているが、レビューや見直しは厳格であると言えず、保護対象のユーザ情報の存在場所の把握に漏れもありうる

Ⓒ 担当者レベルの作業ではあるが、保護対象のユーザ情報の存在場所の洗出しが行われている。組織的なレビューや管理は行われていない。ドキュメント化も十分ではない

Ⓓ 保護対象のファイルやメッセージの把握は行っていない

② システム上の保護対象ファイルに対する保護管理要件の指定

保護対象のファイルの個々に対しては、具体的な保護管理要件が適切に指定されていなければなりません。

設問①〕

保護対象ファイルごとに保護管理要件が適切に指定されていますか？

ファイルに対する保護管理要件の指定には以下のような事項についての指定が必要となります。

- 当該保護対象ファイルに対するシステム操作のアクセス権限保有者の範囲
- アクセス権限保有者の指定手順
- アクセス管理方式
- アクセス監視の要件と不審アクセスに対する処置

貴社サイトにおける保護対象ファイルに対する保護管理要件の指定状況を評価して下さい。

【評価】

Ⓐ 保護対象ファイルに対する保護要件の指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われおり、見直しも適宜行われ、ドキュメント化も十分で、常に、その妥当性は維持されている

Ⓑ 保護対象ファイルに対する保護要件の指定は、決められた手順に沿って行われることになっておりドキュメント化も行われているが、組織的な検討やレビューおよび見直しやドキュメント化は厳格ではなく、指定の一部に妥当性を欠いていることもありうる

Ⓒ 管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメント化も不十分である

Ⓓ 保護対象ファイルに対する保護管理要件の指定は行われていない

設問②〕

アクセス権限保有者の指定と付与するアクセス権の指定は適切に行われていますか？

保護管理要件が適切に指定されていても、アクセス権限保有者の指定とアクセス権限保有者の個々に付与するアクセス権の指定が適切でなければ、適切な保護は実現しません。

貴社サイトにおける保護対象ファイルに対するアクセス権限保有者とアクセス権限保有者に

付与するアクセス権の範囲の指定状況を評価して下さい。

【評価】
- Ⓐ これらの指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている。また、ドキュメントもよく整備されている
- Ⓑ これらの指定は、決められた手順に沿って行われることになっており、ドキュメント化も行われているが、組織的な検討やレビューおよび見直しやドキュメント化は厳格ではなく、指定の一部に妥当性を欠いていることもありうる
- Ⓒ 管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。ドキュメント化も不十分
- Ⓓ 担当者任せにしており、特に管理は行われていない

参考）アクセス権限保有者に付与するアクセス権とは、アクセス権限保有者に許されるファイルに対する操作を指し、厳密に言えば以下のすべてについてその可否が指定されなければなりません。

- 保護対象ファイルの生成・登録・参照・更新・削除
- 保護対象ファイルの印刷、他の電子媒体へのコピー
- システム上の保護対象ファイルに対する二次加工
- 保護対象ファイルのバックアップの取得
- 保護対象ファイルの再編成

③ システム上の保護対象ファイルの保護

システム上の保護対象ファイルに指定通りの保護が行われるためには、関係する機能がシステムに適切に組込まれ、これらの機能が使用する情報も正しく登録されていなければなりません。

設問①〕

保護対象のファイルは保護対象要件を満足する場所に置かれていますか？

保護対象ファイルは論理的に容易にアクセスできない場所に保管されていることが必要です。貴社サイトシステムにおいて保護対象ファイルをどのような場所に配置していますか。また、その配置を評価して下さい。

【保護対象の配置場所】（複数回答）
- Ⓐ ネットワークから切り離されたシステム上に配置
- Ⓑ 内部ゾーンに配置
- Ⓒ DMZ に配置
- Ⓓ インターネットに直結した場所に配置

【保護対象ファイルの配置についての評価】
- Ⓐ すべての保護対象ファイルは外部からの完全に隔離されている
- Ⓑ 外部からアクセス可能な領域に置かれているものもあるが、すべては保護管理要件を満たす位置にある
- Ⓒ おおむね適切な配置であるが、一部は危険な場所に置かれている
- Ⓓ 配置場所についての検討が不十分で、全体として不適切な配置といえる

設問②〕

メモリやハードディスク等への格納について特別な配慮が求められるファイルについては、その要求を満足する形で格納されていますか？

保護対象ファイルの格納にあたって以下に示すような施策を適用していますか。適用している施策を答えて下さい。

【適用している施策】（複数回答）
Ａ）暗号化して格納
Ｂ）Ｗｅｂ等で直接参照できないディレクトリの下に格納
Ｃ）その他（　　）
Ｄ）特別な格納は行っていない

設問③〕

保護対象ファイルへのアクセスには、保護管理要件を満足する適切なアクセス管理機能が組込まれていますか？

保護対象のユーザ情報が格納されているファイルに対して適用するアクセス制御やアクセス監視の機能は、的確にシステムに組込まれていなければなりません。

貴社サイトシステムにおけるユーザ情報にかかわる保護対象ファイルに対する保護機能の組込みについての確認状況を評価して下さい。

【評価】
Ａ）当初組込み時だけでなく変更時においても、決められたプロセスに従った組織的なチェックが厳密に行われており、不備が存在する余地はほとんどない
Ｂ）当初組込み時だけでなく変更時においても、決められたプロセスに従った組織的なチェックが行われることになっているが、厳格に運用されてなく、不備が見過ごされている可能性もある
Ｃ）確認プロセスはあるが形式的で、組織的な管理は行われていない。担当者の注意に依存しているが、一応管理されている
Ｄ）確認プロセスも確立されておらず、担当者任せであまり確認は行われていない

設問④〕

アクセス管理や認証に用いられる情報は常に正しく設定されていることが確認されていますか？

ファイルを保護するための機能がシステムに適切に組込まれていても、これらの機能が用いるアクセス権限保有者の指定やそれぞれに対するアクセス権の指定に不備があれば、保護は機能しません。アクセス管理や認証に用いられる情報の正しい設定の実現には、以下のようなことが必要です。

- 設定内容についての関係者による厳格なチェックの実施
- システムに対する指定についての十分な確認の実施
- システムの構成の変更や前提とするプラットフォームの変更、あるいは保護管理要件の見直しに伴う指定の見直しと変更の実施

貴社サイトにおけるこれらの情報の設定についての管理状況を評価して下さい。

【評価】
（A）この設定は決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている
Ⓑ この設定は決められた手順に沿って行われることになっているが、組織的な検討やレビューおよび見直しは厳格ではなく、設定の一部に妥当性を欠いていることもありうる
Ⓒ 設定およびその管理の手順は決められてなく、組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている
Ⓓ 担当者任せにしており、特に管理は行っていない

⑷保護対象のユーザ情報がかかわる印刷物に対する適切な取扱い

保護対象のユーザ情報が記載されている印刷物についても適切な保護管理が必要となります。このためには、対応するユーザ情報に適用される保護管理要件に従った保護管理が日常の業務やシステムの運営で常に行われるようになっていることが求められています。

設問①〕

保護の対象とすべきユーザ情報にかかわる印刷物は洗出され、それぞれに取扱いルールが決められていますか？

保護の対象となる印刷物が適切な保護を受けるためには、まず、サイト業務に用いられている保護対象のユーザ情報が記載されている印刷物が洗出され、そのそれぞれに対して取扱いルールが決められていなければなりません。

貴社サイトにおけるユーザ情報にかかわる印刷物の把握とそのそれぞれに求められる保護の指定状況を評価して下さい。

【評価】
Ⓐ 十分に検討された印刷物の取扱いルール確立しており、関係者にも徹底されている
Ⓑ 印刷物に対する取扱いルールは決められているが、検討が十分とはいえない
Ⓒ 特に重要なものについてのみ取扱いルールが決められている
Ⓓ 印刷物についての保護は特に考えてはいない

参考）保護対象の印刷物に対する取扱いルールで規定すべき事項
- 作成手順や作成が許される者等の作成に関する制限
- 参照、コピー、二次加工等の使用上の制限
- 外部への持出しについての制限
- 外部への提供についての制限
- 保管場所、保管期間他の保管要件
- 廃棄の方法
- 上記についての記録の作成と管理

設問②〕質問①でＤ以外を回答した方のみお答え下さい）

業務の現場において保護対象の印刷物に対する取扱いルールは守られていますか？

保護対象の印刷物の取扱いルールは業務現場に徹底していて励行されていますか。

貴社サイトにおける保護対象の印刷物の取扱い状況を評価して下さい。

【評価】

Ⓐ 取扱いルールはシステムの運用現場や業務現場に徹底されており、厳格に運用されている

Ⓑ おおむね取扱いルールにもとづいた保護が行われているが厳格とはいえない

Ⓒ 取扱いルールが示されているが管理や指導はほとんど行われておらず、個人の意識に依存している

Ⓓ ほとんど守られていない

⑤保護対象のユーザ情報が記録されたPCや電磁媒体の適切な取扱い

保護対象のユーザ情報が記録されているＰＣや電磁媒体 注）についても適切な保護管理が必要となります。

ＰＣや電磁媒体は、その記録情報量が多量であるだけでなく、証跡を残さず複写や改ざんすることが容易であり、また簡単に転々流通させることが可能で、印刷物と比べ情報の漏洩、流出時の影響は格段に大きいため、ＰＣや電磁媒体やの保護管理は特に厳格に行う必要があります。

(注)電磁媒体とは、磁気テープや磁気ディスク、光ディスク、PC、サーバ、携帯端末等の本体内蔵の記憶装置・ディスク類を指します。

設問①〕

保護の対象とすべきユーザ情報が記録されているＰＣや電磁媒体は洗出され、それぞれに取扱いルールが決められていますか？

保護の対象となるＰＣや電磁媒体等が適切な保護を受けるためには、まず、サイトシステムの運営や業務で用いられている保護対象のユーザ情報が記録されているＰＣや電磁媒体が洗出され、そのそれぞれに対して取扱いルールが決められていなければなりません。

貴社サイトにおけるユーザ情報にかかわるＰＣや電磁媒体の把握とそのそれぞれに求められる保護の指定状況について評価して下さい。

【評価】

Ⓐ 電磁媒体の取扱いについての十分に検討されたルールが確立しており、関係者にも徹底されている

Ⓑ 電磁媒体等に対する取扱いルールは決められているが、検討が十分とはいえない

Ⓒ 特に重要なものについてのみ取扱いルールが決められている

Ⓓ 電磁媒体等に対する保護は特に考えてはいない

参考）保護対象のユーザ情報がかかわる電磁媒体等に対する取扱いルールで規定すべき事項

・作成手順や作成が許される者等の作成に関する制限
・参照、コピー、二次加工等の使用上の制限
・外部への持出しについての制限
・外部への提供についての制限
・保管場所、保管機関他の保管要件
・廃棄の方法
・上記についての記録の作成と管理

設問②〕設問①でＤ以外を回答した方のみお答え下さい）

業務現場において保護対象のユーザ情報がかかわるＰＣや電磁媒体に対する取扱いルールは守られていますか？

保護対象のユーザ情報がかかわる電磁媒体等の取扱いルールは業務現場に徹底していて励行されていますか。

貴社サイトにおけるこれらの電磁媒体等の取扱いを評価して下さい。

【評価】
Ａ）取扱いルールはシステムの運用現場や業務現場に徹底されており、厳格に運用されている
Ｂ）おおむね取扱いルールにもとづいた保護が行われているが厳格とはいえない
Ｃ）取扱いルールが示されているが管理や指導はほとんど行われておらず、個人の意識に依存している
Ｄ）ほとんど守られていない

第 7章　通信の保護

サイトの外部との通信に対しては、通信路上での情報の漏洩、改ざんの防止や、意図した相手でない者との通信の防止、さらには否認防止等の保護が必要になります。

ここでは、貴社サイトにおける通信の保護についての取組みについてお聞かせ下さい。

⑴保護対象となる通信の把握と保護管理要件の指定

通信に対する保護が適切に行われるためには、まず、保護対象の通信の洗出しと、個々の保護対象の通信に対する保護管理要件の適切な指定が必要となります。

設問①〕

保護対象の通信は洗出され、そのそれぞれに対し保護管理要件が適切に指定されていますか？

通信の保護を実現するためには、まず、保護の対象となる通信が洗出され、それぞれに対して以下のような事項が適切に指定されていなければなりません。

- 使用する通信路についての要件
- 通信相手の識別、認証についての要件
- メッセージの暗号化についての要件
- メッセージの真正性の確認についての要件
- 否認への備えについての要件
- ログの確保についての要件

貴社サイトにおける保護対象の通信に対する保護管理要件の指定状況を評価して下さい。

【評価】

Ⓐ 保護対象の通信の洗出しやそれぞれに対する保護管理要件の指定は、組織的な管理のもとで行われている。また、その見直しも含め管理プロセスも確立している

Ⓑ 保護対象の通信の洗出しやそれぞれに対する保護管理要件の指定は、決められた手順に沿って組織的には行われているが検討は十分とは言えない

Ⓒ 保護対象の通信の特定とその保護管理要件の指定は担当者の意識に任されており、その十分性についてはチェックされていない

Ⓓ 通信の保護は行っていない

⑵　通信に対する保護管理の実施

設問①〕

専用線やＶＰＮ等のセキュアな通信路を使用していますか？

専用線や VPN 等のセキュアな通信路を使用していますか。使用している場合、どのような通信に適用されていますか。

貴社サイトシステムにおける専用線およびＶＰＮの使用状況についてお訊ねします。

【どのような通信に専用線を用いていますか】複数回答）
Ⓐ 仕入れ先等商取引上の特定取引先との通信
Ⓑ 出店企業やコンテンツ作成企業等のサイト運営のパートナーとの通信
Ⓒ サイトの保守等の運用管理をリモートで行うための通信
Ⓓ その他（　　）
Ⓔ 専用線は使用していない

【どのような通信にＶＰＮを用いていますか】複数回答）
Ⓐ 仕入れ先等商取引上の特定取引先との通信
Ⓑ 出店企業やコンテンツ作成企業等のサイト運営のパートナーとの通信
Ⓒ サイトの保守等の運用管理をリモートで行うための通信
Ⓓ その他（　　）
Ⓔ VPNは使用していない

設問②】

Web 通信の保護はどのような方法で行っていますか？

貴社サイトシステムにおいては通信路上での情報の漏洩や改ざんを防ぐため、保護対象の Web 通信に対する保護にどのような方法を用いていますか。

【Web 通信の保護に用いている方法】(複数回答)
Ⓐ SSL
Ⓑ SET
Ⓒ その他（　　）
Ⓓ 特に脅威を感じないため何も行っていない
Ⓔ 保護すべき通信はないため何も行っていない

設問③】

メールによる通信に対する安全対策は行っていますか？

メールは盗聴される可能性が高いと考えなければなりません。

業務上の連絡のメール使用に対する貴社でのルールやその実行状況の評価をお訊ねします。

【メールの使用についてのルール】複数回答）
Ⓐ 外部に対し秘匿が必要な情報のメールによる連絡は禁止している
Ⓑ 情報内容の暗号化を行えば、外部に対し秘匿が必要な情報もメールにより連絡することも可としている
Ⓒ 一般的な注意に止まっている
Ⓓ その他（　　）
Ⓔ 特別な配慮はしていない

【評価】
Ⓐ ルールは関係者に徹底されて、その実行状況も厳しく管理されている
Ⓑ ルールは決められているが、実行状況についての管理は甘く、問題を起こす可能性もある
Ⓒ 関係者に注意を喚起しているが、実行状況についてのチェックは行っていない
Ⓓ 無管理状態である

設問④】

否認防止策を組込んでいますか。組込んでいる場合どのような方法を用いていますか？

貴社サイトシステムでは否認対策を組込んでいますか。否認対策を組込んでいる場合、その方法をお聞かせ下さい。

【否認防止策の実施の有無】
- Ⓐ 組込んでいる
- Ⓑ 気になっているが適当な方法がわからないため対策はしていない
- Ⓒ 特に脅威を感じないため何も行っていない
- Ⓓ 考えたことはない

【否認防止策の実施の有無】（前問でＡを回答した方のみお答え下さい）
- Ⓐ 取引プロセスの中への相手側の確認プロセスの組込み
- Ⓑ 電子署名の利用（ＳＥＴの使用を含む）
- Ⓒ メール等の別チャネルでの通信による確認
- Ⓓ その他（　　）

設問⑤】

無線ＬＡＮの脆弱性についての対策は行っていますか？

無線ＬＡＮは、うかつに導入すると攻撃者を容易に貴社サイトシステムのＬＡＮ内の通信に参加させることになります。貴社サイトにおける無線ＬＡＮの導入の有無と、導入している場合その脆弱性に対する対策を評価して下さい。

【無線ＬＡＮの導入の有無】
- Ⓐ 無線LANを導入している
- Ⓑ 無線ＬＡＮは導入していない

【評価】（前問でＡを回答した方のみお答え下さい）
- Ⓐ 十分な検討のもと、無線ＬＡＮの脆弱性が問題にならないようにする対策が講じられている
- Ⓑ 十分な検討のもとに対策が決められ実行されているが、その安全性は十分とは言えない
- Ⓒ 問題点の認識はあり、注意はしているが、実質的な対策にはなっていない
- Ⓓ 特に対策していない

第 8章　ユーザ認証

サイトが外部に提供しているさまざまなサービスのうち対象者を限定しているサービスの提供に際して行われるユーザ認証については、以下が適切に行われなければなりません。

- 対象者の管理
- 求められる認証機能のシステムへの組込み
- パスワード等のユーザ認証に用いる情報の管理

ここでは、貴社サイトが外部に提供するサービスで行っている認証について**お聞かせ下さい**。

⑴ ユーザ認証の実施の有無および目的

設問①】

ユーザ認証を行っていますか？

【ユーザ認証の有無】
Ⓐ ユーザ認証を行っている
Ⓑ ユーザ認証は行っていない

⇨ **Ⓑ の“ユーザ認証を行っていない“と回答された方は、本章（第 8 章）の以降の設問に回答する必要はありません。**

設問②】

ユーザ認証をどのような目的に使っていますか？

貴社サイトでユーザ認証を行っている理由をお訊ねします。

【ユーザ認証を行っている理由】複数回答）
Ⓐ 商取引における取引指示の受付のため
Ⓑ 特定の登録者だけを対象とするサービスがあるため
Ⓒ ポイントの付与等の付加的なサービス提供におけるユーザの特定のため
Ⓓ ユーザ情報の保護のためにアクセスしてきたユーザを確認するため
Ⓔ ユーザ識別をより強固にするため
Ⓕ その他（　　）

⑵ 個々の認証場面に対する認証要件の指定

ユーザ認証についての要件は、求められる厳格さや運用上の負担等により、個々の場面によって異なったものになります。ユーザ認証が適切なものであるためには、まず、個々の場面に対する認証要件が、その利用目的に照らして適切に決められていなければなりません。

設問①】

ユーザ認証が必要な個々の場面に対してユーザ認証要件が適切に指定されていますか？

ユーザ認証の要件の設定にあたっては、一般に以下についての検討が必要となります。

- ユーザ認証に求められる厳格さ
- アクセス権の付与者とアクセス権を付与した者へのアクセス権の範囲
- アクセス権の付与の管理方法
- ユーザ認証に求められる厳格さ、運用上の負担、利用者の操作性等を配慮した認証方式

貴社サイトにおけるユーザ認証要件の指定状況を評価して下さい。

【評価】
Ⓐ 関係者による指定されたプロセスに沿った十分な検討にもとづいたものであり、すべての認証に対し適切な認証要件が指定されている
Ⓑ ユーザ認証の要件定義は指定されたプロセスに沿って行われることになっているが、すべての認証に対して関係者による十分な検討が行われていない
Ⓒ 認証要件は示されているが、定義の内容や検討プロセスは十分とは言えない
Ⓓ 認証要件は明確でない

設問②〕

どのような認証方式を採用していますか？

貴社サイトシステムで用いているユーザ認証方式をお訊ねします。

【採用している認証方式】（複数回答）
Ⓐ ID／パスワード
Ⓑ ワンタイムパスワード
Ⓒ 電子証明書
Ⓓ バイオメトリクス
Ⓔ ICカード
Ⓕ その他（　　）

設問③〕 設問②でCを回答した方のみお答えください）

電子証明書をユーザ認証に採用している場合、どのようなサービスに適用していますか？

電子証明書を認証に用いている場合、対象としているサービスをお訊ねします。

【電子認証適用サービス】（複数回答）
Ⓐ クレジット決済
Ⓑ デビット決済
Ⓒ SETによる決済
Ⓓ その他（　　）

❸ユーザの管理

ユーザ認証を行う場合は、ユーザの認定、権限の付与、システムへの登録から、指定内容の変更や登録の抹消等の対象ユーザに対する一連の管理が必要となります。

設問①〕

登録時にユーザの身元確認や付与の妥当性についての確認をどのような方法で行っていますか？

サービスによってはアクセス権を付与する際に、ユーザの身元や付与の妥当性をチェックする必要があります。

ユーザ登録に際して貴社が行っているユーザの身元確認方法をお聞かせ下さい。

【身元確認方法】（複数回答）
- Ⓐ 第三者機関発行の電子証明書により確認
- Ⓑ クレジットカード番号により確認
- Ⓒ 住所、電話／ＦＡＸ番号、メールアドレスを用いた連絡の成否により確認
- Ⓓ その他（　　）
- Ⓔ 特に身元確認は行っていない

設問②〕

登録ユーザの管理は適切に行われていますか？

ユーザ認証の対象となっているユーザについては、継続的な管理が必要であり、登録ユーザがアクセス権を失った場合は、当該ユーザに付与したアクセス権を無効にする処置が迅速にとられなければなりません。

貴社サイトにおける登録ユーザに対する管理の状況を評価して下さい。

【評価】
- Ⓐ 管理ルールが確立しており、管理ルールに沿った日常的な管理に加え、定期的なチェックも行っており、ユーザ管理は万全と言える
- Ⓑ 管理ルールは決められているが実行に徹底を欠き、ユーザ管理に不手際が生じる可能性もある
- Ⓒ 管理ルールは決められているが、担当者まかせで組織的な管理は行われておらず、管理に問題があると言える
- Ⓓ 管理ルールも明確でなく管理はずさん

設問③〕

ユーザに対しユーザIDやパスワード、ICカード等の保護についての指導は行っていますか？

ユーザにおけるユーザIDやパスワード、ICカード等のずさんな管理は、これらの盗難に結びつく恐れがあります。このような被害を防ぐためは、ユーザ登録時だけでなく、ユーザに対し適宜これらの管理についての指導を行うことも必要となります。

貴社におけるこの点についての努力を評価して下さい。

【評価】
- Ⓐ 登録時だけでなく定期的に注意を喚起している
- Ⓑ 登録プロセスの中で注意を喚起している
- Ⓒ 登録に関する文書に記載してはいるが、積極的な指導は行っていない
- Ⓓ 行っていない

⑷ パスワードの管理

ユーザ認証に（固定）パスワードを用いている場合のみ、以下の質問にお答え下さい。

設問①】

パスワードの設定をどのような方法で行っていますか？

貴社でのパスワードの設定方法を下記から選んで下さい。

【設定方法】（複数回答）
- (A)ユーザによる指定
- (B)ユーザによる指定（ただし、初期パスワードは貴社が割当てた仮パスワード）
- (C)貴社からの割当て

設問②】（設問①でA、Bを回答した方のみお答え下さい）

ユーザが指定したパスワードを、貴社サイトはどのような方法で受取っていますか？

貴社でのパスワードの受取り方法を下記から選んで下さい。

【受取り方法】（複数回答）
- (A)Web：暗号化あり
- (B)Web：暗号化なし
- (C)メール：暗号化あり
- (D)メール：暗号化なし
- (E)郵送（電磁媒体）：暗号化あり
- (F)郵送（電磁媒体）：暗号化なし
- (G)郵送（紙媒体）：書留等の秘匿された郵便
- (H)郵送（紙媒体）：シール等で秘匿された一般郵便
- (I)郵送（紙媒体）：一般の郵便
- (J)その他（　　）

設問③】（設問①でBを回答した方のみお答え下さい）

仮パスワードを用いている場合、仮パスワード使用にかかる脆弱性を補う工夫はされていますか？

パスワードの登録用に仮パスワードを用いている場合、この仮パスワードが悪用されるのを防ぐための対策が必要となります。

貴社サイトシステムにおける仮パスワード使用上の脆弱性対策を評価して下さい。

【評価】
- (A)仮パスワードの引渡し方法への配慮や、1回目のログインで正式なパスワードに変更するようにしていること等、仮パスワードの使用がなりすましを誘う危険性を封じている
- (B)仮パスワードを強度の高いものにするとともに引渡し方法にも配慮しているため、そのまま使われてもなりすましを誘う危険性は小さくしている
- (C)仮パスワードを強度の高いものにするとともにユーザに対し正式なパスワードへの変更を要求しているが、そのまま使うこともできる。そのまま使われた場合、なりすましを誘う危険性は少なくない
- (D)そのままユーザのパスワードとして使うこともでき、特別な配慮はされてないため、そのまま使われた場合、なりすましを誘う危険性が高い

設問④〕 設問①で B、C を回答した方のみお答え下さい）

パスワード等の認証に用いる情報を、どのような方法でユーザに交付していますか？

パスワードおよび仮パスワードの交付に際しては、その内容が他人に渡らないようにする手段を講じなければなりません。

貴社では、パスワード等の認証に用いる情報を、どのような方法で交付していますか。

【認証情報の交付】複数回答）
- ㈀Web :暗号化あり
- ㈁Web :暗号化なし
- ㈂ メール :暗号化あり
- ㈃ メール :暗号化なし
- ㈄ 郵便（電磁媒体）:暗号化あり
- ㈅ 郵便（電磁媒体）:暗号化なし
- ㈆ 郵便（紙媒体）:書留等の秘匿された郵便
- ㈇ 郵便（紙媒体）:シール等で秘匿された一般郵便
- ㈈ 郵便（紙媒体）:一般の郵便
- ㈉ その他（　　）

設問⑤〕

パスワードは推測されにくいものにしていますか？

パスワードを推測されにくいものにするために、貴社ではどのような対策を講じていますか。

【評価】
- ㈀ パスワードについての基準があり、ユーザに対する周知および指導を行っている。さらに、パスワード設定時にチェックを行い、不適切なパスワードは拒否している
- ㈁ パスワードについての基準があり、ユーザに対する指導を行っているが、徹底さには欠け、問題のあるパスワードが使われている可能性もある
- ㈂ ユーザに対し推測されにくいパスワードの設定を呼びかけているが、受付時のチェックに関するチェック等は行われていない
- ㈃ 特に対策は講じていない

設問⑥〕

パスワード等の認証に用いる情報は適切なサイクルで更新していますか？

パスワードは有効期限を定め、定期的に更新すべきとされています。

貴社が用いているパスワードの更新サイクルをお聞か下さい。

【更新状況】複数回答）
- ㈀1 年未満のサイクルで更新
- ㈁1 年以上のサイクルで更新
- ㈂ ユーザが申請により更新、更新サイクルはユーザの個々の考えに依存
- ㈃ 更新サイクルを定めた更新行っていない

設問⑦〕

パスワードクラックに対する対策は講じていますか？

システムでの認証プロセスの中に、パスワードクラックと見られる操作があった場合（認証の失敗が続いた場合など）、当該ユーザの認証を停止したり、ユーザと連絡をとるような機能を組込んでおくことも必要です。

貴社サイトシステムにおけるパスワードクラック対策を評価して下さい。

【評価】

Ⓐ すべてのパスワード認証に、パスワードクラックの試みに対する対策を組込むことになっており、その組込みも確認されている

Ⓑ 重要なパスワード認証には、パスワードクラックの試みに対する対策を組込むことになっており、その組込みも確認されている

Ⓒ 一部のパスワード認証に対しては、担当者の判断でパスワードクラックの試みに対する対策が組込まれているが、組織的な管理は行われていない

Ⓓ パスワードクラックの試みに対する対策は組込んでいない

第 9章　セキュアなシステム構築

EC サイトにおけるセキュリティ対策の実施は、巧みに設計されたシステムの構成とシステムを構成する各機器に組込まれたさまざまなセキュリティサービス機能、および、各機器に対するセキュリティ要件に対応した諸設定を基盤としています。このため、システムの構成ならびにセキュリティサービス機能および各機器における諸設定は、脅威別に定められた対策が求めていることを的確に反映したものでなければなりません。

セキュアなシステムの構築とは、サイト構成の設計や各機器における諸設定を適切に行い、攻撃を受けにくく、かつ、攻撃を受けても被害は限定的なものに止めることができるよう、攻撃に対して堅固なシステムを構築することを言います。

サイトシステムの構築や各機器におけるセキュリティ対策にかかわる諸設定を、脅威別に定められた対策が求められていることを的確に反映したものにするためには、システムの構成や使用する技術の組込みとその使用方法についての十分な検討と適切な管理が必要となります。

ここでは、貴社サイトにおけるセキュアなシステム構築への取組みについてお訊ねします。

⑴ セキュリティ面からのシステム構成についての検討

システムを、攻撃を防ぎ易くまた攻撃を受けてもその被害を限定的なものにするためには、システムの構築およびその維持管理について、セキュリティ対策面からのさまざまな視点から検討することが必要です。

設問①〕

システム構成の設計にあたって、セキュリティ面からの検討は十分に行われましたか？

システムの構成の検討にあたっては、一般に以下に示すような点をセキュリティ面から考慮する必要があります。

- サポートしている業務の特性からのリスクの評価
- ゾーン分割の要否とゾーン分割を行う場合の分割の方式と各ゾーンの位置付け
- 各サービスのシステム構成上での配置
- サービスの分散の要否と、必要な場合の分散の方式
- 一つのマシン上でのサービスの同居の是非と、同居させる場合の問題点への対策
- 保護対象資産の配置
- バックアップの配置
- データフロー管理、ウイルス検査、侵入監視等のセキュリティサービス機能の配置

貴社サイトのシステムの構築およびその変更にあたってのセキュリティ面からの検討を評価して下さい。

【評価】
Ⓐ 専門的な技術の裏付けのもと組織的に検討が十分に行われており、セキュリティ対策面からの要求はすべて適切に反映されており、セキュアな構成として自信がある
Ⓑ 組織的な検討は行われたが、サイトのセキュリティポリシーや個別対策を完全に反映しているとは言い難い
Ⓒ 担当者レベルで一通りの検討が行われているが、専門家の指導やチェックは受けておらず、十分な検討が行われているとは言えない
Ⓓ セキュリティ面はほとんど考慮していない

【検討が不十分である場合その理由】（前問で C、D を回答した方のみお答え下さい）
Ⓐ セキュリティについての意識が低く、検討が行われなかったため
Ⓑ 実際の脅威は少ないと見てセキュリティ対策を重要視しなかったため
Ⓒ 検討を実施できる人材がいないため
Ⓓ 予算に制限があるため

設問②】

システム構成へのセキュリティ要求事項の反映はどのような体制で行われましたか？

システム構成へのセキュリティ要求事項の反映には専門的な知識が必要となります。
貴社のサイトシステムの構成を検討した体制をお訊ねします。

【サイトシステム構成の検討体制】
Ⓐ 自社の要員だけで実施
Ⓑ システムベンダーの助言を得て自社要員で実施
Ⓒ セキュリティ専門コンサルタントの助言を得て自社要員で実施
Ⓓ システムベンダーの提案を採用
Ⓔ セキュリティ専門コンサルタントの提案を採用
Ⓕ システムベンダーに加え、セキュリティ専門コンサルタントも参画

設問③】

ゾーン分割を行っていますか？

インターネットに接続するサイトシステムでは内部、外部、DMZにゾーン分割を行い、外部にサービスを提供するサーバはDMZへ、顧客データ、社内の機密性の高いデータ、メールなどのサーバを内部ゾーンに配置することが望ましいとされています。
貴社サイトシステムにおけるゾーン分割とその考え方をお訊ねします。

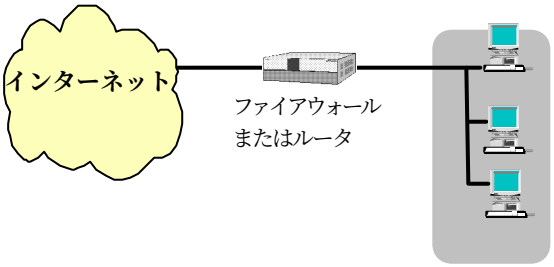
【サイトシステムの構成】
下記の構成パターンの中から、貴社サイトの構成に最も近いものを選んで下さい。
Ⓐ ゾーン構成のないフラットな構成で、サイトの機器のすべてがインターネットに直結
Ⓑ 外部ゾーンと内部ゾーンの２層構造
Ⓒ DMZと内部ゾーンの2層構造
Ⓓ 外部ゾーン、DMZ、内部ゾーンの３層構造
Ⓔ DMZ、内部ゾーンをビジネスによりさらに分離した複合構造
＊各構成パターンのイメージについては、（参考）を参照して下さい。

【ゾーン分割を行っていない場合その理由】
前問でＡを回答した方のみお答下さい。複数回答）
ゾーン分割を行わなかった理由を以下の中から選んで下さい。
Ⓐ 特に理由はない。よく検討した結果ではない
Ⓑ 分割による防御が必要ないため
Ⓒ サイトのセキュリティは、各サーバのセキュリティ対策を強固なものにすることで実現することを構成方針としているため
Ⓓ 分割を実施するために必要な予算や設置スペースがない
Ⓔ 分割を実施できる者がいない
Ⓕ その他（　　）

【DMZ の位置付け】最初の質問でA、B 以外を回答した方のみお答下さい。複数回答）
DMZをどのように位置付けていますか。以下のサーバの中からDMZに配置しているものを選んで下さい。
Ⓐ Mail サーバ
Ⓑ DNS サーバ
Ⓒ ftp サーバ
Ⓓ Webサーバ
Ⓔ DBサーバ
Ⓕ その他（　　）

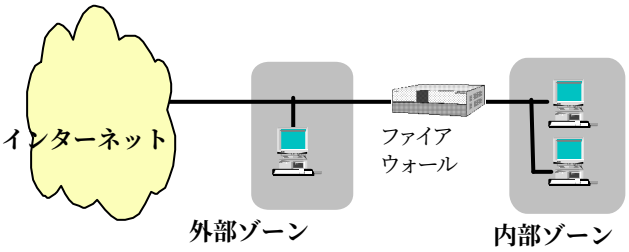
参考）サイトシステムの構成パターンのイメージ

Ⓐ ゾーン構成のないフラットな構成



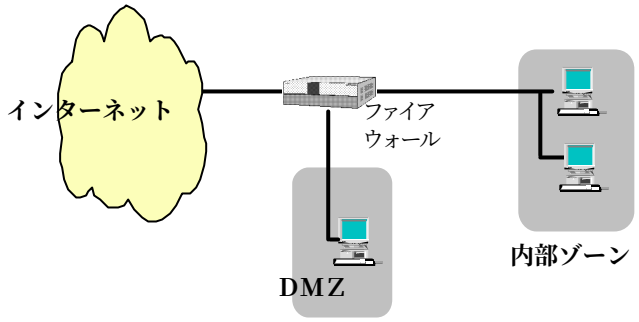
外部公開サーバと同一ゾーン内に業務サーバ等を設置する形態であるため、公開サーバを経由して業務サーバが攻撃される危険性の高い形態

Ⓑ 外部ゾーンと内部ゾーンの２層構造



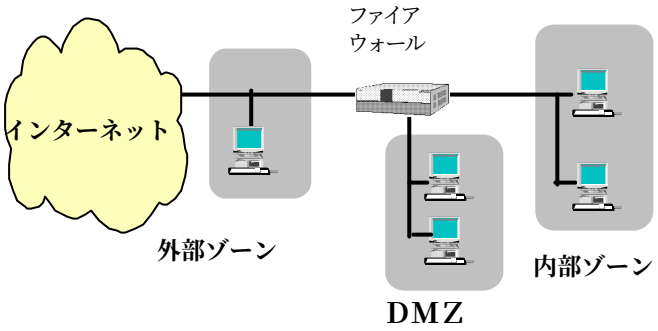
公開サーバ（例：Web サーバ）と業務用サーバ群を別ゾーンに配置する形態、（A）よりセキュアな構成

(C) DMZと内部ゾーンの2層構造



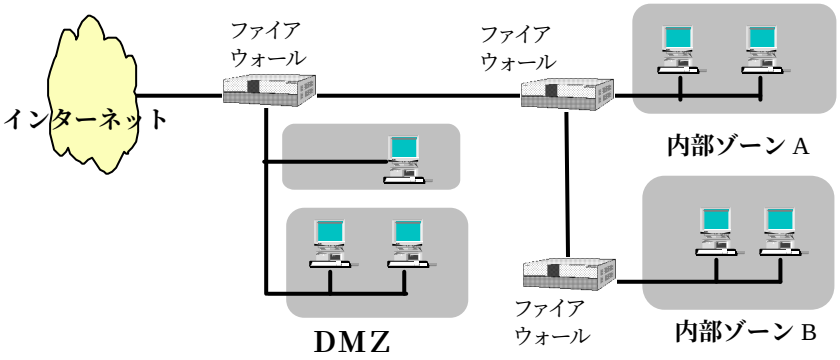
ファイアウォールを隔て公開用サーバ（例：Webサーバ）をDMZに配置、非公開サーバ群を内部ゾーンに設置する形態、ファイアウォールの介在により公開サーバへの不正アクセス監視（ロギング）、IDS装置との連携などが可能なセキュアなゾーン構成

(D) 外部ゾーン、DMZ、内部ゾーンの3層構造



ファイアウォールを境界に外部、DMZ、非公開サーバ群を設置する内部ゾーンの3区画にゾーン分割を行う形態、ファイアウォールの介在によりDMZ上のサーバへの不正アクセス監視（ロギング）、IDS装置との連携が可能なセキュアなゾーン構成

(E) DMZ、内部ゾーンをビジネスによりさらに分離した複合構造



(C)の形態をビジネス用途により各区画内でさらにゾーン分割し、排他すべき業務間のアクセスを厳しく制限した形態、よりセキュアなゾーン構成

②Webサーバのシステム構成上の配置とセキュリティ対策についての配慮

設問①〕

Webサーバはサイトのシステム構成上の適切な位置にありますか？

システム構成上でのWebサーバの配置についてお訊ねします。

【Web サーバの位置】複数回答）
Ⓐ ゾーン構造が存在しない構成におけるインターネットに直結したところ
Ⓑ 外部ゾーン
ⒸDMZ

設問②］

Web サーバは他のサービスとは隔離されていますか？

外部のネットワークに公開されているWeb サーバは、攻撃を受け易いため、その被害が他のサービスに影響を及ぼさないよう、同じマシン上に他のサービスは置かないことが望ましいとされています。

Web サーバが置かれた機器上への他のサービスの搭載状況をお訊ねします。

【Web サーバに搭載しているサービス】複数回答）
Ⓐ 同居サービスは存在しない
ⒷMail サーバ
ⒸDNS サーバ
Ⓓftp サーバ
Ⓔtelnet サーバ
Ⓕ ファイルサーバ
ⒼDB サーバ
Ⓗ 開発用サーバ
Ⓘその他　（　　）

【他のサービスを搭載している場合その理由】
前問で A 以外を回答した方のみお答え下さい）
ⒶWeb 経由でのコンテンツの更新等、Web サーバの運営に必要となるため
Ⓑ 特に検討した結果ではない
Ⓒ 特に脅威を感じないため
Ⓓ スペース等の問題からサーバの台数を増やすことが困難なため
Ⓔ 予算上の問題のため
Ⓕ その他理由（　　）

設問③］

Ｗｅｂサーバの構築にあたってそのセキュリティ上の特性に対する配慮は行われていますか？

Ｗｅｂサーバはその特性から、その構築にあたって、セキュリティ面で配慮すべき事項として以下にあげるようなことが必要であると指摘されています。

- IIS 等のソフトウェアを常に最新のものにする
- ディレクトリの一覧の取得許可を必要最小限にする
- URL でアクセス可能な場所に重要なファイルを置かない
- HTTP メソッドの制限を行う
- OS 上でコンテンツへのアクセス制限を行う
- CGI プログラムの種類、配置位置等を管理する
- コンピュータにログオンできるユーザを制限する

- 暗号化（SSL）を行う
- Java、Java スクリプト、ActiveX、CGI の脆弱性に対する対策を行う

Web サーバについてのこれらの指摘に対し、貴社サイトシステムで行っている対策を評価して下さい。

（注）なお、ここでは Web サーバの特性からくるセキュリティ問題に焦点をあててください。Web アプリケーションの開発にかかるセキュリティ問題については、 ⑧の“自社で開発するソフトウェアへの必要なセキュリティ機能の確実な実装”を参照ください。

【評価】
- Ⓐ システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
- Ⓑ 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
- Ⓒ 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
- Ⓓ 特に対策は考えていない

【不十分と回答した場合その理由】（評価で C、D を回答した方のみお答下さい）
- Ⓐ そのような指摘についての認識がなかったため
- Ⓑ 問題点は知ってはいるが重要性をあまり感じないため
- Ⓒ 対応の方法がよくわらないため
- Ⓓ 対策の実施についての管理や指導が不十分なため
- Ⓔ その他（　　）

③Mail サーバのシステム構成上の配置とセキュリティ対策についての配慮

設問①】

Mail サーバはサイトのシステム構成上の適切な位置にありますか？

システム構成上での Mail サーバの配置についてお訊ねします。

【Mail サーバの配置】（複数回答）
- Ⓐ Mail サーバは設置していない　（→ ④へ進んでください）
- Ⓑ ゾーン構造が存在しない構成におけるインターネットに直結したところ
- Ⓒ 外部ゾーン
- Ⓓ DMZ

設問②】

Mail サーバの構築にあたってそのセキュリティ上の特性に対する配慮は行われていますか？

Mail サーバはその特性から、その構築にあたって、セキュリティ面で配慮すべき事項として以下にあげるようなことが必要であると指摘されています。

- 自ドメイン宛のメールあるいは、自ドメイン内から外部に送信するメール以外の中継を禁止する

- メール発信者制限を行う（SMTP AUTH や POP before SMTP 等）
- SMTP の EXPN 機能の制限を行う
- POP や IMAP の認証の安全強化を行う（APOP や POP3、IMAP SSL 認証や IMAPS 等）
- メール一通のサイズ制限を設ける

Mail サーバについてのこれらの指摘に対する貴社サイトで行っている対策を評価して下さい。

【評価】
- (A) システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
- (B) 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
- (C) 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
- (D) 特に対策は考えていない

【不十分と回答した場合その理由】（評価で C、D を回答した方のみお答え下さい）
- (A) そのような指摘についての認識がなかったため
- (B) 問題点は知っているが重要性をあまり感じないため
- (C) 対応の方法がよくわらないため
- (D) 対策の実施についての管理や指導が不十分なため
- (E) その他（　　）

⑷ftp サーバのシステム構成上の配置とセキュリティ対策についての配慮

設問①】

ftpサーバはサイトのシステム構成上の適切な位置にありますか？

システム構成上での ftpサーバの配置についてお訊ねします。

【サーバの配置】（複数回答）
- (A) ftp サーバが存在しない　（→ (5) へ進んでください）
- (B) ゾーン構造が存在しない構成におけるインターネットに直結したところ
- (C) 外部ゾーン
- (D) DMZ

設問②】

ftpサーバの構築にあたってそのセキュリティ上の特性に対する配慮は行われていますか？

ftpサービスはその特性から、その構築にあたって、セキュリティ面で配慮すべき事項として以下にあげるようなことが必要であると指摘されています。

- OS 上のアクセス制限
- ファイルのパーミッションの適用
- anonymous ftp を用いない場合における他人のファイルにアクセスできないような制限
- passive モードを用いる場合における利用可能な port の制限

● アクセスクライアント数（セッション接続数）の制限

ftpサーバに対するこれらの指摘に対し、貴社サイトで行っている対策を評価して下さい。

【評価】
Ⓐ システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
Ⓑ 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
Ⓒ 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
Ⓓ 特に対策は考えていない

【不十分と回答した場合その理由】（評価でC、Dを回答した方のみお答え下さい）
Ⓐ そのような指摘についての認識がなかったため
Ⓑ 問題点は知っているが重要性をあまり感じないため
Ⓒ 対応の方法がよくわらないため
Ⓓ 対策の実施についての管理や指導が不十分なため
Ⓔ その他（　　）

⑸DB サーバのシステム構成上の配置とセキュリティ対策についての配慮

設問①］

DB サーバはサイトのシステム構成上の適切な位置にありますか？

DB サーバが攻撃され情報の漏洩や改ざん、破壊が生じた場合の被害は甚大なため、保護対象の情報が格納されているDBサーバは厳重な保護が必要となります。このため、DBサーバは外部ネットワークから隔離された内部ゾーンに配置するのが一般的ですが、サイトの業務の特性や予算上の問題等によりシステム構成の考え方によりさまざまな選択肢があります。

システム構成上のDB サーバの配置についてお訊ねします。

【ＤＢサーバの配置】（複数回答）
Ⓐ DB サーバが存在しない　（→ ⑹へ進んでください）
Ⓑ ゾーン構造が存在しない構成におけるインターネットに直結したところ
Ⓒ 外部ゾーン
Ⓓ DMZ（非武装ゾーン）
Ⓔ 内部ゾーン

【ＤＢサーバを外部ゾーンあるいはDMZに置いている場合その理由】
（
）

設問②］

DB サーバは他のサービスとは隔離されていますか？

DB サーバが攻撃され情報の漏洩や改ざん、破壊が生じた場合の被害は甚大なため、保護対象の情報が格納されているDBサーバは厳重な保護が必要となります。このため、DBサーバ

は比較的対策が緩やかな他のサービスのセキュリティ事故の影響を受けないよう、同じマシン上に他のサービスは置かないことが望ましいとされています。

DB サーバが置かれたマシン上への他のサービスの搭載状況をお訊ねします。

【DB サーバに搭載しているサービス】複数回答）

Ⓐ 同居サービスは存在しない
Ⓑ Web サーバ
Ⓒ Mail サーバ
Ⓓ DNS サーバ
Ⓔ ftp サーバ
Ⓕ telnet サーバ
Ⓖ ファイルサーバ
Ⓗ 開発用サーバ
Ⓘ その他　（　　）

【他のサービスを搭載している場合その理由】
前問で A 以外を回答した方のみお答え下さい。複数回答）

Ⓐ 特に検討した結果ではない
Ⓑ 特に脅威を感じないため
Ⓒ スペース等の問題からサーバの台数を増やすことが困難なため
Ⓓ 予算上の問題のため
Ⓔ その他　（　　）

設問③］

DB サーバの構築にあたってそのセキュリティ上の特性に対する配慮は行われていますか？

DB サーバはその特性から、その構築にあたって、セキュリティ面で配慮すべき事項として以下にあげるようなことが必要であると指摘されています。

- 適切なアクセス制御の組込み
- 機密情報への通信の暗号化
- データベース管理者のパスワードの適切な設定

DB サーバについてのこれらの指摘に対し貴社サイトで行っている対策を評価して下さい。

【評価】

Ⓐ システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
Ⓑ 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
Ⓒ 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
Ⓓ 特に対策は考えていない

【不十分と回答した場合その理由】評価で C、D を回答した方のみお答え下さい。複数回答）

Ⓐ そのような指摘についての認識がなかったため
Ⓑ 問題点は承知しているが重要性をあまり感じないため
Ⓒ 対応の方法がよくわらないため
Ⓓ 対策の実施についての管理や指導が不十分なため
Ⓔ その他（　　）

⑹ ファイルサーバのシステム構成上の配置とセキュリティ対策についての配慮

設問①】

ファイルサーバはサイトのシステム構成上の適切な位置にありますか？

EC サイトにおいて、冗長構成を行う際の共有ディスクやネットワークストレージ等に用いられるファイルサーバが攻撃され情報の漏洩や改ざん、破壊が生じた場合、被害を受けた情報によっては被害は甚大となるため、顧客情報等の保護すべき情報が格納されているファイルサーバは厳重な保護が必要となります。このため、ファイルサーバは外部ネットワークから隔離された内部ゾーンに配置するのが一般的ですが、サイトの業務の特性や予算上の問題等によりシステム構成の考え方よりさまざまな選択肢があります。

貴社サイトにおけるシステム構成上でのファイルサーバの配置についてお訊ねします。

【ファイルサーバの配置】複数回答）
- Ⓐ ファイルサーバが存在しない　（→ (7) へ進んでください）
- Ⓑ ゾーン構造が存在しない構成におけるインターネットに直結したところ
- Ⓒ 外部ゾーン
- Ⓓ DMZ（非武装ゾーン）
- Ⓔ 内部ゾーン

【ファイルサーバを外部ゾーンあるいは DMZ に置いている場合その理由】
（
）

設問②】

ファイルサーバの構築にあたってそのセキュリティ上の特性に対する配慮は行われていますか？

ファイルサーバはその特性から、その構築にあたって、セキュリティ面で配慮すべき事項として以下にあげるようなことが必要であると指摘されています。

- ファイルサーバの利用が可能なホストの制限
- OS 上のアクセス制限、ファイルのアクセス許可(パーミッション)の管理
- 他人のファイルへのアクセスの制限
- 利用可能な容量の制限

ファイルサーバについてのこれらの指摘に対し、貴社サイトで行っている対策を評価して下さい。

【評価】
- Ⓐ システムには関係者により十分に検討された対策を組込んでおり、必要な対応はとられている
- Ⓑ 対策についての組織的な検討やその結果のシステムへの組込みはチェックされることになっているが、レビューは十分とは言えず、問題が見逃されている可能性もある
- Ⓒ 担当者が気がついた範囲で対策が行われているが、組織的なレビューは行われていない
- Ⓓ 特に対策は考えていない

【不十分と回答した場合その理由】（評価で C、D を回答した方のみお答え下さい）
Ⓐ そのような指摘についての認識がなかったため
Ⓑ 問題点は承知しているが重要性をあまり感じないため
Ⓒ 対応の方法がよくわらないため
Ⓓ 対策の実施についての管理や指導が不十分なため
Ⓔ その他（　　）

(7) 開発環境のシステム構成上の配置とセキュリティ対策についての配慮

設問①】

開発環境はシステム構成上の適切な位置にありますか？

開発環境サーバは開発時の事故から現用システムへの影響を遮断する意味合いからも運用中のネットワークから隔離された内部ゾーンに配置するのが一般的ですが、サイトの業務の特性や予算上の問題等によりシステム構成の考え方よってさまざまな選択肢があります。

システム構成上の開発環境サーバの配置についてお訊ねします。

【開発環境の配置】
Ⓐ 開発環境サーバが存在しない　（→ (8) へ進んでください）
Ⓑ ゾーン構造が存在しない構成におけるインターネットに直結したところ
Ⓒ 外部ゾーン
Ⓓ DMZ（非武装ゾーン）
Ⓔ 内部ゾーン

【開発環境サーバを外部ゾーンあるいは DMZ に置いている場合その理由】
（　　）

設問②】

開発環境は運用環境から隔離されていますか？

開発中のシステムではさまざまなトラブルが発生するのは避けられません。開発環境に発生したトラブルが運用中のシステムに影響を与えないようにするため、運用システムからは隔離されなければなりません。

貴社サイトにおける運用環境と開発環境の隔離状況を評価して下さい。

【運用環境と開発環境の位置関係】
Ⓐ 運用環境は開発環境とネットワークレベルで隔離（異なったゾーンに配置）
Ⓑ 開発環境と運用環境は同じゾーンに置かれているがマシンは分離
Ⓒ 開発環境は、運用で用いられている（一部の）サービスと同一マシン上に同居

【評価】
Ⓐ 開発環境と運用環境間の通信はできず、開発環境は運用環境から完全に隔離されている
Ⓑ 開発環境と運用環境間の一般の通信は制限され、必要な通信も厳格な管理のもとに行っており、問題が生じる可能性は低い
Ⓒ 開発環境と運用環境間の通信の制限は厳格でなく、担当者の注意に依存しているところもあり、問題を起こす可能性も低くはない
Ⓓ 開発環境と運用環境間の通信に対する特別の管理は行っていない

⑧自社で開発するソフトウェアへの必要なセキュリティ機能の確実な実装

アプリケーションレベルでのアクセス制御やアクセス監視、Web 通信に対する暗号化等は、ネットワークレベルでのバリアやシステムレベルでの防御をかいくぐってくる不正なアクセスからシステムの機能の不正な使用や情報の不正取得や改ざん、破壊の試みに対する最後の砦であり、自社で開発するソフトウェアへのセキュリティ機能の確実な実装が必要となります。

設問①〕

自社で開発する（外部に委託する場合を含む）ソフトウェアに対する必要なセキュリティ機能は適切に指定されていますか？

自社で開発するソフトウェアに対しては、具備すべきアクセス制御機能や、アクセス監視機能、アクセス者の識別および認証機能、暗号化や特殊な格納などのデータの保護機能、データの真正性の検証機能等の必要なセキュリティ機能が明示されなければなりません。また、この要求は、常に、その時々のサイトの運営環境に照らしたセキュリティ要求事項を満足するものでなければなりません。

貴社サイトにおける自社開発ソフトウェアに対する必要なセキュリティ機能の指定状況を評価して下さい。

【評価】

Ⓐ 設計レビューの中に必要となるセキュリティ機能についての第三者チェックが行われており、すべてのソフトウェアに必要なセキュリティ機能は適切に指定されている

Ⓑ 設計レビューの中で必要となるセキュリティ機能についての第三者チェックは義務付けられているが、厳格には運用されてなく、問題が見過ごされている可能性もある

（C）ソフトウェアの設計担当者レベルでのチェックは義務付けられているが、第三者的なチェックは行われていない

Ⓓ チェック実施も義務付けられてなく、実質的に無管理の状態

設問②〕

指定されたセキュリティ機能が開発ソフトウェアに確実に組込まれていることは確認されていますか？

各アプリケーションに要求されたセキュリティ機能は、期待通りに動作することが確認されてなければなりません。このためには、開発プロセスに対する適切な管理が必要となります。

貴社サイトにおける開発ソフトウェアに対するセキュリティ機能の組込みについての確認状況を評価して下さい。

【評価】

Ⓐ 組織的なチェックが行われており、ミスが見逃される余地はほとんどない

Ⓑ 確認プロセスおよびチェックの体制もあるが、チェックに厳密さを欠き、ミスが見逃されている可能性もある

Ⓒ 担当者レベルでのチェックは義務付けられているが、第三者的なチェックは行っていない

Ⓓ 担当者任せで、特に管理は行われていない

設問③〕

開発ソフトウェアに組み込まれたセキュリティ機能の動作に必要な環境は確保されていますか？

開発するソフトウェアに組み込まれたセキュリティ機能が正しく動作するためには、以下に示すようなさまざまな環境整備が必要となります。そして、これらの環境は維持し続けなければなりません。

- SSL 通信、暗号化、電子署名等で必要となる電子証明書期限が無効にならないよう管理
- 使用ソフトウェアのライセンス期限が無効・使用不可能にならないよう管理
- ブラウザバージョンの指定管理と指導（機能対応のない旧版利用の禁止）
- サーバの秘密鍵、電子証明書の秘匿管理
- ソフトウェアのバージョン指定および管理、指導（機能対応のない旧版利用の禁止）

貴社サイトにおける、この点についての取組状況を評価して下さい。

【評価】

Ⓐ システムの維持管理業務にルーチン作業として組込まれており、組織的な管理が十分に行われている
Ⓑ システムの維持管理業務にルーチン作業として組込まれているが、厳格に運用されてなく、不備が見逃される可能性もある
Ⓒ 担当者レベルでの管理は行われているが、組織的な管理は行われていない
Ⓓ 担当者任せで、特に管理は行われていない

設問④〕

業務やセキュリティ対策の変更、システム構成の変更のアプリケーションに組込んでいるセキュリティ機能や必要な動作環境の指定に適切に反映されていますか？

業務の変更、セキュリティ対策の変更に伴うセキュリティ要求事項の変更、プラットフォームの変更、新規機能追加・変更に際しては、アプリケーションに組込んでいるセキュリティ機能やその動作環境の指定に変更の要否の確認を行い、必要な変更を実施しなければなりません。

貴社サイトにおける、この点についての取組状況を評価して下さい。

【評価】

Ⓐ システムの維持管理業務にルーチン作業として組込まれており、組織的な管理が十分に行われている
Ⓑ システムの維持管理業務にルーチン作業として組込まれているが、厳格に運用されてなく、不備が見逃される可能性もある
Ⓒ 担当者レベルでの管理は行われているが、組織的な管理は行われていない
Ⓓ 担当者任せで、特に管理は行われていない

設問⑤〕

開発するソフトウェアに脆弱性を残さないようにするための配慮は払われていますか？

ソフトウェアの脆弱性を生む原因についてはよく知られたいくつかのパターンがあり、これらが繰り返し発生していることが知られています。この質問はよく知られた脆弱性への配慮を開発段階で考慮するプロセスが存在するかどうかをお訊ねします。

貴社サイトにおけるこの点についての取組みを評価して下さい。

【評価】

Ⓐ これらの脆弱性を検知するプロセスがシステムの維持管理業務にルーチン作業として組込まれており、厳格に運用されていて、不備が見逃されている可能性はほとんどない

Ⓑ これらの脆弱性を検知するプロセスがシステムの維持管理業務にルーチン作業として行われることになっているが、厳格に運用されてなく、不備が見過ごされている可能性もある

Ⓒ 担当者に地位を喚起しており、担当者レベルでのレビューは行われているが、組織的な管理は行われていない

参考）問題となっている脆弱性の一例

- クロスサイトスクリプティングにおける脆弱性
- cookie の持つ脆弱性
- バッファオーバフローの脅威

⑨ ソフトウェアに対する適切な保護の実施

開発したソフトウェアにトロイの木馬やコバート通信路（隠れチャネル）が埋め込まれたり、プログラムが他のものとすり替えられたりすることもセキュリティの脅威の一つです。これらのことを防ぐためにはソフトウェア開発プロセスに対する適切な管理とプログラムライブラリに対する適切な保護管理が必要となります。ここでは開発の過程でセキュリティを確保する適切なプロセスが存在するかを確認します。

設問①】

自社で開発するソフトウェアの開発プロセスに対するセキュリティ面での管理は行われていますか？

開発するソフトウェアにセキュリティ面において問題がないものにするためには、開発プロセスに対し以下に示すようなセキュリティ面で適切な管理が必要となります。

- ソフトウェア開発プロジェクトにおける開発体制や開発環境からくるセキュリティ面のリスクの評価
- ソフトウェア開発プロセスに対するセキュリティ管理の実施
- 開発記録の作成と保管
- 開発参加者に対する開発作業上でのセキュリティ面での要求の明示
- ソフトウェアの検収にあたってのセキュリティ面からのチェック
- 開発要員に対する管理（外部委託開発員を利用する場合の取り決め）

貴社サイトにおけるソフトウェア開発におけるセキュリティ面からの管理状況を評価して下さい。

【評価】
Ⓐ 必要な管理はすべて開発プロセスに組込んでおり、厳格に運用している
Ⓑ 必要な管理はすべて開発プロセスに組込んでいるが、厳格に運用されていないため、問題が見逃されている可能性もある
Ⓒ 問題意識はあるが、その実行は開発担当者に任されている
Ⓓ 特に行っていない

設問②〕

ソフトウェアの開発を外部に委託している場合、開発委託先での開発プロセスに対するセキュリティ面での管理を要求していますか？

外部に開発を委託したソフトウェアにセキュリティ面において問題がないものにするためには、開発委託先における開発プロセスに対し、以下に示すようなセキュリティ面での適切な管理が必要となります。

- 開発委託先における開発プロジェクトにかかるセキュリティ面からのリスクの評価
- 開発プロセスならびに納入ソフトウェアに対するセキュリティ面からの要求の明示
- 契約書等による、セキュリティ面からの管理と、納入するソフトウェアがセキュリティ面で問題がないこと等に関する開発委託先の責任の明確化
- ソフトウェアの検収にあたってのセキュリティ面からのチェックの実施
- 必要に応じた開発委託先の開発プロセスに対する管理や指導

貴社サイトにおけるソフトウェアの開発委託についてのセキュリティ面からの管理を評価して下さい。

【評価】
Ⓐ）必要な事項は契約あるいはそれに準ずる文書で明示しており、また、適宜必要な監督や指導を行っている
Ⓑ）必要な事項は契約あるいはそれに準ずる文書で明示しているが、監督や指導までは行っていない
Ⓒ）問題意識はあるが、開発担当者の意識に任されている
Ⓓ）特に行っていない

第 10章　システムの運用と業務現場におけるセキュリティ対策

日々のシステムや業務の運用に対するセキュリティ要求事項が適切に実行され、システムの運用や業務運用上の不手際がセキュリティの脅威にならないようにするためには、システム運用や業務現場に対してもセキュリティ面からの適切な管理が必要となります。

ここでは、貴社サイトにおけるシステムの運用と業務現場におけるセキュリティ確保への取組みについてお訊ねします。

⑴ セキュリティ事故につながるシステム運用の不手際の防止策の実施

セキュリティ事故につながるシステム運用の不手際の発生を防止するためには、セキュリティ対策がシステムの運用に求めていることが確実に実行されるようにするための工夫が必要となります。

設問①〕

システムの運用に対するセキュリティ面からの要求は明確になっていますか？

セキュリティ面からのシステム運用に対する要求は明確にされ、システム運用規程や運用マニュアルに適切に反映されていなければなりません。

貴社サイトにおけるシステム運用に対するセキュリティ要求事項の指定について評価して下さい。

【評価】

Ⓐ システム運用に対するセキュリティ要求事項の指定は、関係者によりレビューされており、運用規程や運用マニュアルも常にサイトの運用環境やセキュリティ対策を反映したものが維持されている

Ⓑ システム運用に対するセキュリティ要求事項の指定は、関係者によりレビューされるとともに、運用規程や運用マニュアルへのセキュリティ対策の反映も、確立したプロセスの中で行われることになっているが、その運用は厳格でなく、セキュリティ対策のシステム運用への反映に漏れが生じている可能性もある

Ⓒ 担当者レベルの努力に依存しているが、システム運用へのセキュリティ対策の反映についての確立したプロセスや、運用規程や運用マニュアルについてのセキュリティ面からの組織的な管理は行われていない

Ⓓ セキュリティ対策とシステム運用の連携はあまりとられていない

設問②〕

セキュリティ対策にかかわるシステム運用を確実にするための施策は講じられていますか？

セキュリティ対策にかかわるシステム運用を確実なものにするためには、以下のような施策の実施が求められます。

- システム運用にかかるセキュリティ要求事項の運用関係者への明示
- 関係ルーチン作業のスケジュール化
- チェックリスト等を用いた実行確認および管理の励行

貴社サイトにおけるセキュリティにかかわるシステム運用上の不手際の防止についての取組みを評価して下さい。

【評価】
（A）さまざまな工夫がシステム運用の中に組込まれ、その実行も厳格に管理されており、システム運用上不手際が発生あるいは見逃される可能性はほとんどない
（B）さまざまな工夫がシステム運用の中に組込まれているが、その実行は徹底しているとは言い難く、不手際を発生させたり見逃したりする可能性もある
(C) 担当者レベルでの工夫は見られるが、組織的な管理は行われておらず、不手際を発生させそれが見逃されていても不思議ではない
(D) 特別な工夫はなされていない

設問③〕

システム運用者および関係者に対するセキュリティ教育は行われていますか？

システム運用時におけるセキュリティ対策を確実なものにするためには、システム運用関係者に対する以下のような教育も必要となります。

- サイトシステムの運用におけるセキュリティリスクと脅威の認識
- サイトにおけるセキュリティ対策の概要
- 日々の運用におけるセキュリティ要求事項

貴社サイトにおけるシステム運用関係者に対するセキュリティ教育への取組みを評価して下さい。

【評価】
(A) 検討された計画のもとで教育を行っており、システム運用関係者の責任意識ならびに要求事項についての理解は十分である
(B) 教育を行っているが、関係者の責任意識ならびに要求事項に対する理解については十分とは言い難い
(C) 特別に教育は行われていないが、関係者にセキュリティはおおむね責任意識ならびに要求事項に対する理解を有していると考えている
(D) 特に行われておらず、関係者の責任意識ならびに要求事項に対する理解については不安がある

② システム構成の維持管理

サイトのシステム構成や各機器における諸設定は、常に、その時々のサイトの運用環境に適合し、セキュリティ要求事項を満足するものでなければなりません。

設問①〕

システムの構成はその構成方針を反映しセキュリティ面からの要求を満たすものとして維持されていますか？

サイトのシステム構成は、常に、その構成方針を反映し、システムの構成に対するセキュリティ要求事項を満足するものでなければなりません。

貴社サイトにおける現在のシステム構成は、構成方針に沿った適切なものですか。

【評価】
Ⓐ 十分な検討の下で設計されており、運用環境への適合性についての定期的なチェックも行われており、常に、システム構成方針に沿っており、セキュリティ対策面からの要求を完全に満たしているものとして維持されている
Ⓑ 当初の設計は十分な検討のもとに行われたが、システム構成の変更に際してのレビューは厳格でなく、部分的にシステム構成方針からずれたところも出る可能性がある
Ⓒ 明示されたシステム構成方針はないが、システム構成はサイトの運営実態に照らし、おおむねセキュリティ対策面からの要求を満たしている
Ⓓ セキュリティ面からのシステム構成の評価は行っていない

設問②〕

各機器は、常に、それぞれに対するセキュリティ要求事項を満足していますか？

各機器における諸設定は、さまざまなセキュリティ要求事項を的確に反映したものでなければなりません。このためには、ソフトウェアのレベルアップ等の適切な実施や、サイトの運営環境の変更に際しての見直しが必要です。また、各機器における諸設定の正確な把握とその妥当性についての定期的なチェックの実施も必要となります。

貴社サイトにおけるシステム構成機器における諸機能の設定の妥当性維持への取組みを評価して下さい。

【評価】
Ⓐ 各機器に対する諸設定は確立した手順に沿って行い、厳格なチェックも行っている。ミスが見逃されている可能性はほとんどない
Ⓑ 各機器に対する諸設定は確立した手順に沿って行い、組織的なチェックを行うことになっているが、その運用が厳格でなく、ミスが見逃されている可能性もある
Ⓒ 確立した手順や組織的なチェックはなく、担当者の注意と努力に依存しているが、おおむね適切に行われている
Ⓓ 各機器に対する諸設定はほとんど管理されておらず、設定内容の把握も十分でない

参考）各機器に対するセキュリティ要求事項の例
- 使用 OS やサービス用ソフトウェアのバージョンレベル
- 不要なアカウントおよびサービス等の処置、OS の使用権限認証、ポートの管理等の必要な不正アクセス対策の実施
- 必要なセキュリティホール対策
- 必要なウイルス対策

設問③〕

システム構成や各機器における諸機能の設定は正確に把握されていますか？

システムの構成や各機器におけるセキュリティに関係する諸設定は、常に正確に把握されていなければなりません。このためには、これらに関するドキュメント化とその正確性の維持が必要になります。

貴社サイトにおけるシステムの構成や各機器におけるセキュリティに関係する諸設定についてドキュメント化の状況を評価して下さい。

【評価】
Ⓐ 正確なドキュメントが漏れなく整備されている
Ⓑ ドキュメントは作成されているが、メンテナンスが十分に行われておらず、正確さについては多少疑問がある
Ⓒ ドキュメント化は一部に止まっており、全体としてのドキュメント化は行われていない
Ⓓ ドキュメント化はほとんど行われていない

設問④〕

各種プログラムライブラリの管理は適切に行われていますか？

ソフトウェアの保護管理のためには、以下のような施策も必要となります。

- ソースライブラリへのアクセス制限
- 実行ライブラリへのアクセス制限
- ソースライブラリの変更ルールの確立とルールにもとづく変更の実施
- 実行ライブラリの変更ルールの確立とルールにもとづく変更の実施

貴社サイトにおける各種プログラムライブラリの管理状況を評価して下さい。

【評価】
Ⓐ 確立した管理手順に沿って厳格に運用されている。問題が発生する可能性はほとんどない
Ⓑ 確立した管理手順に沿って行われることになっているが、厳格には運用されておらず、問題が発生する隙がある
Ⓒ 担当者レベルである程度の管理は行われている
Ⓓ プログラムライブラリの管理は実質的に行われていない

❸攻撃への備え

セキュリティ事故の発生は早期に発見しないと被害を大きくしてしまいます。このため、サイトに対し行われた攻撃あるいは不審なアクセスについては、適切な対応が必要となります。

設問①〕

監視により攻撃が行われたことが発見された場合、適切な処置は行われていますか？

不審なアクセスや攻撃の形跡が発見された場合は、以下にあげるような処置を適切に行わなければなりません。

- 発生している事象の正確な把握
- 被害の発生の有無のチェックと被害が確認された場合における組織的な事故処理の立上げ
- システムの脆弱性のチェックと必要な対策の検討と実施

攻撃を受けた形跡がある場合に対する貴社サイトでの対応を評価して下さい。

【評価】
Ⓐ 決められた手順に沿って、常に適切に行われている
Ⓑ 手順は決められているが手順通りに行われていないこともある。対応内容はおおむね適切である
Ⓒ 手順は確定していないが、担当者は習慣的に必要な処置を行っている。
Ⓓ 手順も確定しておらず、必要な処置は行われていない

設問②】

Ｗｅｂコンテンツの改ざん検知は行われていますか？

万一、Ｗｅｂコンテンツが改ざんされたような場合、被害の拡大を防ぐためには改ざんの事実が早期に発見されなければなりません。貴社サイトにおけるＷｅｂコンテンツの改ざん検知を評価して下さい。

【評価】
Ⓐ Ｗｅｂコンテンツに対し改ざん検知や自動復旧等を行う仕組みを組込んでいる。
Ⓑ システムへの侵入の形跡が発見された場合等、必要と判断された場合のみ改ざん検知を実施している
Ⓒ 高い頻度で更新をしており、改ざんされても大きな影響が出ないと考えている
Ⓓ 行っていない

⑷ システムの脆弱点の把握とそれらへの対応

セキュリティ対策の実施にあたっては、対策実施上のタイムラグや漏れおよび新しい攻撃手段の登場によりシステムに生じた脆弱点を常に把握し、万一の場合に必要な対応が迅速にとれるようになっていなければなりません。

設問①】

サイトシステムに対する脆弱性診断は行われていますか？

セキュリティ対策の不備が見過ごされないようにするためには、サイトシステムに対する技術的な脆弱性の診断を定期的または必要に応じて実施することも有効な手段の一つです。

貴社サイトシステムに対する脆弱性診断の実施状況についてお訊ねします。

【脆弱性診断の実施有無とその形態】
Ⓐ 導入したツールを用い自社で実施
Ⓑ セキュリティサービスベンダーの診断サービスを利用
Ⓒ 無料サービスを利用
Ⓓ 脆弱性診断は行っていない

【実施している場合の診断事項】（上でＤ以外を回答した方のみお答下さい）
Ⓐ 外部ネットワークからアクセス可能なポートの検査
Ⓑ 外部ネットワークからアクセス可能なポートのフロー設計との照合
Ⓒ 外部ネットワークからアクセス可能な稼動中のサービスに内在している脆弱点
（Ｄ）ファイアウォールの内側からアクセス可能なポートの検査
（Ｅ）ファイアウォールの内側からアクセス可能なポートのフロー設計との照合
（Ｆ）ファイアウォールの内側からアクセス可能な稼動中のサービスに内在している脆弱点
Ⓖ その他（　　）

設問②〕 設問①の 脆弱性診断の実施有無とその形態】でD以外を回答した方のみお答え下さい）

脆弱性診断は有効に活用されていますか？

貴社サイトシステムで実施している脆弱性診断の結果の活用状況を評価して下さい。

【評価】

Ⓐ 思わぬ問題点が指摘されておりフィードバックも迅速に行われていて、セキュリティの維持に不可欠である

Ⓑ 問題点の分析や発見した問題点の対策へのフィードバックには不満な点があるが、おおむね有効に活用されている

Ⓒ 発見された問題点への対応は一応行われているが、十分ではない

Ⓓ 診断結果は報告されているが分析や対策へのフィードバックはほとんど行われていない

Ⓔ 診断結果は十分にチェックされているが、これまでのところ問題点は見つかっていない

設問③〕

新しい脅威について情報の把握は行われていますか？

クロスサイトスクリプティングの脅威やｃｏｏｋｉeの利用上の脅威等の報告されている脅威や、他社における大きな被害が報告されている攻撃手段による被害を防ぐためには、まず、情報サイトやメーリングリスト、専門誌、新聞報道等から、新しい脅威（攻撃手段）や他社における被害報告等の情報に関心を持ち、そのような攻撃に対する自社のサイトの対策状況をチェックし、必要な対策を講じ、自社のサイトが次の被害サイトにならないようにする努力も必要です。

貴社における新しい脅威についての情報の収集状況を評価して下さい。

【評価】

Ⓐ）情報の収集についてのルールが確立しており、ルールに沿った情報の収集を行っている

Ⓑ）情報の収集および収集した情報の取り扱いについてのルールは確立しているが、厳格に運用されておらず、情報の収集は十分には行われていない

Ⓒ）情報の収集は担当者レベルであり組織的には取組んでいない。主にセキュリティコンサルタントや SE からの警告に依存している

Ⓓ） このような情報の収集はほとんど行っていない

【情報の収集を行っている場合その情報源】（評価で D 以外を回答した方のみお答え下さい。複数回答）

Ⓐ IPA、JPCERT/CC 等の公的機関

Ⓑ セキュリティ専門誌

Ⓒ その他の IT 専門誌

Ⓓ 新聞

Ⓔ セミナー

Ⓕ セキュリティコンサルタント、プロダクトベンダー、SE

Ⓖ その他（ ）

【行っていないと回答した場合その理由】（評価でDを回答した方のみお答え下さい）
Ⓐ 脅威をそれほど感じないから
Ⓑ 対策を検討する体制や専門的な技術能力の不足
Ⓒ サイトの運用との関係で対策を随時に組込むことが困難なため
Ⓓ その他（　　）

設問④〕（設問③の【評価】でD以外を回答した方のみお答え下さい）

新しい脅威についての情報に対する対応の要否等についての評価は適切に行われていますか？

入手した情報に対しては、それらの脅威が自社のサイトにも該当するかどうか、該当する場合どのような対応が必要かどうか、またその緊急度はどうか等についての正しい評価が行われなければなりません。この評価を適切に行うためには、以下のような施策が必要になります。

- 収集した情報の評価手順の確立
- 評価体制の確立および評価能力の確保
- 最終判断責任者の明確化
- 必要に応じた外部の専門家の意見の反映

貴社における新しい脅威についての情報の取扱い状況を評価して下さい。

【評価】
Ⓐ）収集した情報の処理についての手順が確立しており、この手順に沿って情報の評価および必要な対応の検討を行っている
Ⓑ）収集した情報の処理についての手順は確立しているが、収集した情報に対する評価や必要な対応の検討は十分とは言えない
Ⓒ）担当者レベルは努力しているが、担当者の任せであり組織的な対応はできていない
Ⓓ）情報を入手してもほとんど対応していない

【不十分と回答した場合その理由】（前問でA以外を回答した方のみお答下さい。複数回答）
Ⓐ 脅威をそれほど感じないから
Ⓑ 対策を検討する体制や専門的な技術能力の不足
Ⓒ サイトの運用との関係で対策を随時に組込むことが困難なため
Ⓓ その他（　　）

設問⑤〕

サイトシステムに内在している脆弱性は正確に把握していますか？

サイトシステムに内在している脆弱性に対し、対策方法の検討に時間を要したり、対策が決まってもサイトの運用上の都合から、すべてに迅速に対処できるわけではありません。このため、サイトシステムに内在する脆弱性について正確に把握し、運用上で特別の注意を払う等、これらの脆弱性を補完する手段を講じる必要があります。

貴社サイトにおけるサイトシステムに内在する脆弱性の把握についての取組みを評価して下さい。

【評価】
Ⓐ これらの情報の把握と整理についての手順が確立しており、決められた手順に従った管理を行っている。また、関係ドキュメントも整備されている
Ⓑ これらの情報の把握と整理についての手順は確立しているが、厳格に運用されておらず、その確実性に不安がある
Ⓒ 担当者レベルでの把握は行われているが、組織的な管理は行われていない
Ⓓ 特に整理は行われていない

参考）サイトシステムに内在しうる脆弱点
- サイトシステムに対する脆弱性診断で指摘された脆弱点
- システム構成に関し認識されている脆弱点
- システムの実装上認識されている脆弱点
- 未対策のセキュリティホール
- 未対策のウイルス
- 新しく報告された脅威への対応

設問⑥】

認知したシステムの脆弱点に対する対策は迅速に行われていますか？

新しい脅威に対する評価が行われて、必要な対応が決められても、サイトの運営上の都合から、それらの対策がすぐに実施できるとは限りません。サイトの運営とのバランスを取りながら、如何に迅速にこれらへの対応を実施できるかが、サイトをセキュアなものにするためのポイントの一つとも言えます。

貴社サイトにおける新しい脅威への取組みについて評価して下さい。

【評価】
Ⓐ 脅威の程度の判断にもとづき、重大な脅威に対しては迅速に対策を実施している
Ⓑ 迅速化に努力しているが遅れ気味である
Ⓒ あまり積極的に対応していない
Ⓓ 特に対処は行っていない

【重大な脅威に対する対策実施の平均的なタイムラグ】
Ⓐ 認知から２週間以内
Ⓑ 認知から１ヶ月以内
Ⓒ 認知から２ヶ月以内
Ⓓ 認知から２ヶ月以上または放置

【対応が遅い場合その理由】（前問で A 以外を回答した方のみお答え下さい。複数回答）
Ⓐ 脅威をそれほど感じないから
Ⓑ 対策を検討する体制や専門的な技術能力の不足
Ⓒ サイトの運用との関係で対策を随時に組込むことが困難なため
Ⓓ その他（　　）

⑤業務現場におけるセキュリティ事故につながる不手際の防止策の実施

セキュリティ事故につながる業務の不手際の発生を防止するためには、セキュリティ対策が業務現場に求めていることが確実に実行されるようにするための工夫が必要となります。

設問①】

業務現場に対するセキュリティ面からの要求は明確になっていますか？

セキュリティ面からの業務現場に対する要求は明確にされ、業務規程や業務マニュアルに適切に反映されていなければなりません。

貴社サイトにおける業務現場に対するセキュリティ要求事項の指定について評価して下さい。

【評価】

Ⓐ 業務現場に対するセキュリティ要求事項の指定は、関係者によりレビューされており、業務規程や業務マニュアルも常にサイトの運営環境やセキュリティ対策を反映したものが維持されている

Ⓑ 業務現場に対するセキュリティ要求事項の指定は、関係者によりレビューされるとともに、業務規程や業務マニュアルへのセキュリティ対策の反映も、確立したプロセスの中で行われることになっているが、その運用は厳格でなく、セキュリティ対策のシステム運用への反映にもれが生じている可能性もある

Ⓒ 担当者レベルの努力に依存しているが、業務現場へのセキュリティ対策の反映についての確立したプロセスや、業務規程や業務マニュアルについてのセキュリティ面からの組織的な管理は行われていない

Ⓓ セキュリティ対策と業務運用の連携はあまりとられていない

設問②】

セキュリティ対策にかかわる業務運用を確実にするための施策は講じられていますか？

セキュリティ対策にかかわる業務の運用を確実なものにするためには、以下のようなことが求められます。

- 業務の運用にかかるセキュリティ要求事項の運用関係者への明示
- 関係ルーチン作業のスケジュール化
- チェックリスト等を用いた実行確認および管理の励行

貴社サイトにおけるセキュリティにかかわる業務上の不手際の防止について取組みを評価して下さい。

【評価】

（A）さまざまな工夫が業務プロセスの中に組込まれ、その実行も厳格に管理されており、業務上で不手際が発生あるいは見逃される可能性はほとんどない

（B）さまざまな工夫が業務プロセスの中に組込まれているが、その実行は徹底しているとは言い難く、不手際を発生させたり見逃したりする可能性もある

Ⓒ 担当者レベルでの工夫には見られるが、組織的な管理は行われておらず、不手際が発生したり見逃されていても不思議ではない

Ⓓ 特別な工夫はなされていない

設問③〕

業務担当者に対するセキュリティ教育は行われていますか？

業務現場におけるセキュリティ要求事項への対応を確実なものにするためには、業務担当者に対する以下のような教育も必要となります。

- 業務におけるセキュリティリスクと脅威の認識
- サイトにおけるセキュリティ対策の概要
- 日々の業務におけるセキュリテ ィ要求事項

貴社サイ トにおける業務担当者に対するセキュリティ教育への取組みを評価して下さい。

【評価】

Ⓐ 検討された計画のもとで教育を行っており、業務担当者の責任意識ならびに要求事項についての理解は十分
Ⓑ 教育を行っているが、関係者の責任意識ならびに要求事項に対する理解については十分とは言い難い
Ⓒ 特別に教育は行われていないが、関係者はセキュリティについての責任意識ならびに要求事項に対する理解をおおむね有していると考えている
Ⓓ 特に行われておらず、関係者の責任意識ならびに要求事項に対する理解については不安

⑹ 物理的な保護領域の確保と保護領域へのアクセス管理の実施

サイトシステムの物理的な保護や、システムへの不正なアクセスの防止あるいは職場にある情報の保護のためには、サイトシステムが置かれている場所や職場へのアクセスは適切に管理されなければなりません。

設問①〕

システムおよび関係設備が置かれた場所は他から物理的に隔離されていますか？

システムおよび関係設備が置かれた場所は、許可されない者に容易にアクセスを許さないようにするため、他と物理的に隔離されていることが望ましいとされています。

貴社サイトにおける、システムおよび関係設備がおかれている場所についてお訊ねします。また、その配置についても評価して下さい。

【システムおよび関係設備が置かれた場所について】

Ⓐ 常時施錠された扉で物理的に隔離された場所
Ⓑ 常時施錠はされていないが、他とは隔離された独立した場所
Ⓒ パーティション等の移動可能な家具で囲われた場所
Ⓓ 囲われた場所ではないが、保護領域として明示された場所
Ⓔ 特別に保護領域は設けていない

【評価】

Ⓐ サイトの運営実態とセキュリティポリシーに照らし十分
Ⓑ 十分とはいえないまでも、サイトの運営実態およびセキュリティポリシーに照らしおおむね適切
Ⓒ セキュリティポリシーに照らし十分とは言えず改善が必要
Ⓓ サイトの運営実態やセキュリティポリシーに照らし無対策に近く早急に対策が必要

【不十分な状態におかれている理由】
（評価でＣまたはＤを回答した方のみお答え下さい。複数回答）
Ⓐ 予算上の制約
Ⓑ スペース等の物理的な制約
Ⓒ 検討が不十分なため
Ⓓ その他（　　）

【今後の計画】（評価でＣまたはＤと回答した方のみお答え下さい）
Ⓐ 強化を準備中
Ⓑ 強化を検討中
Ⓒ 今後、強化を検討する
Ⓓ 今後も検討の予定はない

設問②〕

システムおよび関係設備が置かれた場所に対するアクセスは適切に管理されていますか？

システムおよび関係設備が置かれた場所に対するアクセスは制限されるだけではなく、アクセスは正しく管理が行われることが必要です。これらの場所に対しては、一般に以下のような管理が必要とされています。

- 設備に見合ったルールの確立
- ルールにもとづく入退室管理の実施
- アクセスを認められた者に対するルールに従った管理の実施

貴社サイトにおけるこのような場所へのアクセス管理の実状を評価して下さい。

【評価】
Ⓐ）設備にあった管理ルールが決められ、厳格に運用されている
Ⓑ）設備にあった管理ルールが決められているが、厳格に運用されていない
Ⓒ）ルールは明確でないが、周辺にいる者が注意して運用している
Ⓓ）特に管理していない

設問③〕

業務の現場にセキュリティ面からの物理的な保護領域は設けられていますか？

保護の対象となる情報が扱われる職場やシステム運用にかかわる職場も、保護領域として適切なアクセス管理が要求されます。

貴社サイトにおける業務現場における物理的保護領域の設定状況を評価して下さい。

【評価】
Ⓐ 保護領域は他の職場あるいは外部と隔離されており、厳重なアクセス管理が行われている
Ⓑ 保護領域の隔離とアクセスの管理は行われているが、保護領域の設定やアクセス管理の運用は厳格とは言えない
Ⓒ 保護領域の認識はあるが、物理的な隔離は行われておらず、職場の注意に依存している
Ⓓ 特に保護領域についての認識はない

【保護領域を設定していない理由】評価でＣまたはＤを回答した方のみお答え下さい。複数回答）

Ⓐ 保護すべきものはないと考えている
Ⓑ 直接的な脅威を感じない
Ⓒ 保護領域を指定するほどの規模ではない
Ⓓ その他（　　）

第11章　セキュリティ事故への備え

セキュリティ事故の予防に努めていても、新たに登場した攻撃手段や、対策実施上の不備を考えると、セキュリティ事故の阻止を保証することは不可能と考えなければなりません。このため、セキュリティ対策を尽くしたとしても、セキュリティ事故は発生するものとしてとらえ、その事故が事業や業務に大きな影響を及ぼさないようにするための備えをすることが必要となります。

セキュリティ事故の発生に際して、以下が重要となります。

- 事故発生の早期発見
- 事態の正確な把握、被害の拡大防止のために必要となる処置の迅速な実施
- 事故原因の把握と除去
- システムの回復と業務の復旧
- 再発防止策の実施や報告等の事後処理の適切な実施

セキュリティ事故への備えとは、セキュリティ事故の発生に際して、これらのことが適切に実行されるための日頃からの準備を言います。

ここでは、貴社サイトにおけるセキュリティ事故への備えについてお訊ねします。

⑴ セキュリティ事故への対応方針の確立

セキュリティ事故への対応を適切に行うためには、セキュリティ事故の発生に際してどのような対応をするのかについての基本方針が確立していることが必要となります。

設問①〕

セキュリティ事故発生時における業務の中断や復旧についての方針は適切に定められていますか？

セキュリティ事故への対応を決めるためには、セキュリティ事故等による業務の中断はどの程度許されるのか等の業務の継続に関し、以下に示すようなことが明確になっていなければなりません。

- 業務の中断が止むをえない場合
- 業務の中断の許容時間
- 業務の中断実行の手順
- 影響を与えた他社等への対応
- 関係機関への報告

貴社におけるセキュリティ事故への対応についての方針の確立状況を評価して下さい。

【評価】

Ⓐ 十分に検討されたものがあり、関係者に明示されている
Ⓑ 原則は示されているが、内容的に十分とは言えない
Ⓒ 担当者レベルでは考えられているが、組織的には検討されていない
Ⓓ 検討されていない

設問②〕

影響を与えた他社等に対する対応は適切に定められていますか？

セキュリティ事故が他社等社外に影響を及ぼしている場合、社外に被害を拡大させないためには、関係する他社等への連絡や、事後処理を迅速かつ適切に行わなければなりません。セキュリティ事故によっては、事故の発生やその影響を外部に公開することも必要になります。これらが適切に行われるようにするためには、以下のような備えが必要となります。

- 被害を及ぼしているあるいは及ぼす恐れのある他社や顧客への連絡や、公開についての原則の確立
- 他社への連絡や公開の手順の確立

貴社におけるこの点についての取組状況を評価して下さい。

【評価】
Ⓐ 十分に検討された手順が確立しており、関係者にも徹底されている
Ⓑ 原則は決められているが、詳細は検討していない
Ⓒ 担当者レベルでは考えられているが、組織的には検討されていない
Ⓓ 検討されていない

⑵ セキュリティ事故に対する即応体制の確立

設問①〕

事故処理即応体制は確立していますか？

発生したセキュリティ事故には迅速な対応が要求されます。このため、事故処理体制をあらかじめ決めておき、いつでも機能するようにしておかなければなりません。

セキュリティ事故への即応体制の確立に関しては、以下のようなことが求められます。

- 事故処理についての総責任者の明確化
- 事故処理にかかるさまざまなタスクの定義とその実行責任者の明確化
- 関係者の事故処理にかかわる自己の責務についての認識と必要なスキルの確保
- 運用環境の変更に際したこれらの見直し

貴社サイトにおける事故処理即応体制の確立状況を評価して下さい。

【評価】
Ⓐ 必要な体制を確立しており、常時、即応できる
Ⓑ 体制は決められているが、常時、即応体制にあるとは言い難い
Ⓒ 事故処理体制としては明確にはなっていないが、セキュリティ対策関係者が対応することになっている
Ⓓ セキュリティ事故に対応できる体制はない

参考）一般には、以下のようなタスクについての定義と実行に責任を持つ者の指名が必要となります。

・事故処理の統括
・技術面からの対応
・業務面からの対応、外部の専門家との連携
・影響を与えた社外や関係機関との対応

設問②〕

セキュリティ事故を担当する者の技術レベルは十分ですか、また必要な技術教育が行われていますか？

セキュリティ事故への対処には、以下に示すような専門的な技術が必要となる場合があります。

- とっさに必要となる処置についての判断
- 事故原因の分析と対策
- 影響範囲の調査

貴社サイトにおけるセキュリティ事故対応力を評価して下さい。

【評価】
Ⓐ 必要なスキルを十分に有している
Ⓑ 一通りのスキルはあると考えているが十分とは言えない
Ⓒ ある程度のスキルは有するが不安がある
Ⓓ 事故処理ができる要員はいない

設問③〕

システムベンダー、セキュリティサービスベンダー、コンサルタントとの連携体制はとれていますか？

セキュリティ事故への対応には専門的な知識や技術が必要となるため、場合によっては外部のサービスや専門家の応援も必要となります。

貴社サイトにおける、事故処理にあたってのシステムベンダーやセキュリティサービスベンダー、コンサルタントの活用状況をお訊ねします。

【事故処理における外部の専門家の活用状況】
Ⓐ 事故処理体制の中に組込まれており、常時、連絡をとっている
Ⓑ 事故処理体制に中に組込むまでには至ってないが、必要に応じ応援をもらえるようになっている
Ⓒ 特に準備はしていないが、必要に応じて支援を依頼するつもりである
Ⓓ 外部からの支援は特に考えていない

③セキュリティ事故処理手順の確立

発生したセキュリティ事故に対して必要な処置が迅速かつ適切に実行されるためには、さまざまなセキュリティ事故を想定した事故処理についての手順があらかじめ確立しており、関係者にこれが周知されていることが必要となります。

設問①〕

適切な事故処理の手順は存在していますか？

事故処理手順として明示されなければならないことは、以下に示すような事項です。

- サービスの一時停止等の事故発生時におけるとっさに行うべき処置
- 関係者への報告、事故処理体制の発動

- 発生事象の確認、原因の分析、被害範囲の特定等の事態の把握
- 原因の排除
- システムの回復と業務の復旧
- 他社に与えた被害等への対応や影響を与えうる他社への警告
- 警察、IPA、JPCERT/CC 等の関係する機関への報告や外部への情報の公開
- 事故処理の経緯の記録

貴社サイトにおける事故処理手順の整備状況を評価して下さい。

【評価】
Ⓐ 十分に検討された手順が確立しており、関係者に徹底されている
Ⓑ 一通りのことは決められているが、内容的にも十分といえず、さらに検討が必要である
Ⓒ 担当者レベルでは考えられているが、組織的には検討されていない
Ⓓ 検討していない

設問②】

セキュリティ事故が発生した時まず行わなければならない処置は適切に行えるようになっていますか？

サイトシステムへの不正アクセスやウイルスの侵入等が発生した場合は、被害の拡大を防ぐための処置が迅速に行われなければなりません。このためには、以下のような備えが必要とされています。

- ネットワークの切り離し等のセキュリティ事故のタイプごとに事故発生時にとりあえず実行すべき処置の明確化とその手順の野明確化
- 運用環境の変更にともなうこれらの手順の見直しの実施
- 関係者への周知徹底

貴社サイトにおけるセキュリティ事故に対する初期処理への備えについて評価して下さい。

【評価】
Ⓐ 十分に検討された手順が確立しており、関係者に徹底されていて、何時でも迅速に対応ができる
Ⓑ 必要な処置や手順は示されているが、内容的にも十分といえず改善が必要である
Ⓒ 担当者は必要な処置を描いており、ある程度の対応は可能とみているが、組織として対応できるようにはなっていない
Ⓓ 何も準備がなく、即応できる状態にはない

設問③】

パスワードの漏洩や IC カード等の盗難、偽造に対する処置は適切にとられるようになっていますか？

なりすましの発生や、パスワードの漏洩や IC カードの盗難、偽造が発見された場合は、以下のような処置が迅速に行われる必要があります。

- 当該ユーザとの情報交換
- パスワードや IC カードなどの無効化と再設定
- なりすましによる被害状況の把握と必要な対応

貴社サイトにおけるこの点について評価して下さい。

【評価】
Ⓐ 十分に検討された手順が確立しており、関係者に徹底されていて、何時でも迅速に対応ができる
Ⓑ 手順は確立しているが、問題の発生に際して期待通り機能するかどうかに不安が残る
Ⓒ 手順としては確立しはいないが、関係者は必要な処置についての知識をある程度有している
Ⓓ 特に準備されていない

⑷ 事故処理に必要なツールの整備

システムの復旧に備えたバックアップの取得や、事故の影響範囲の調査やシステムの復旧等、事故処理を適切に行うためには、被害調査のためのツール、システムの回復に用いるツール、さらには中断した業務を再開するためのツール等のさまざまなツールを必要とします。これらのツールは、何時でも期待通りに機能するようになっていなければなりません。

設問①】

セキュリティ事故の処理に必要となるツールや機能は整備されていますか？

セキュリティ事故の処理にツールは準備されていても、普段は使われないため、これらが必要な時に円滑に動作するためには、諸設定が適切に行われていることと、変動するシステム環境への対応が確実に行われていることが必要となります。

貴社サイトにおけるセキュリティ事故の処理に必要となるツールの整備状況を評価して下さい。

【評価】
Ⓐ 必要なツールはすべて揃えられており、メンテナンスも適切に行われ定期的な動作確認も行われている
Ⓑ 必要なツールは揃えられているが、メンテナンスや定期的な動作確認は十分に行われていない
Ⓒ ファイルの回復のためのツールが準備されている程度で、十分な検討は行われていない
Ⓓ セキュリティ事故に備えたツールの整備は行っていない

⑸ バックアップと必要な記録の確保

セキュリティ事故の影響範囲の調査や被害からのシステムの回復には、ソフトウェアやデータのバックアップだけでなく、業務や実施したさまざまなセキュリティ対策についての記録も必要となります。このため、必要となるバックアップや業務やセキュリティ対策関連処理についての記録の確保も重要になります。

設問①】

バックアップの取得と保管についての指定は適切に行われていますか？

システムの回復に必要となるバックアップが確保されるためには、以下のようなことが必要となります。

- 取得すべきバックアップとその取得条件の適切な指定
- 取得したバックアップに対する保管期間、保管手段等、保管の方法の指定
- 運用環境の変更に際してのバックアップ取得ルールの見直しの実施
- システム運用へのバックアップの取得、保管作業の組込み

貴社サイトにおけるバックアップの取得計画の整備状況を評価して下さい。

【評価】

(A) これらの指定は、決められた手順に沿って行われ、組織的な検討やレビューが行われている。見直しも適宜行われ、常に、その妥当性は維持されている。また、ドキュメントもよく整備されている

(B) これらの指定は、決められた手順に沿って行われることになっており、ドキュメント化も行われているが、組織的な検討やレビューおよび見直しやドキュメント化は厳格ではなく、指定の一部に妥当性を欠いていることもありうる

(C) 担当者任せで組織的なレビューも行われていないが、担当者レベルでは十分に検討、管理が行われている。

(D) 計画的なバックアップの取得、保管は行われていない

設問②〕

バックアップの取得、保管はルールに従って適切に行われていますか？

貴社サイトにおけるシステム運用におけるバックアップの取得状況を評価して下さい。

【評価】

(A) 指定に従ったバックアップの取得および保管は十分な管理下で励行されている

(B) 指定に従ったバックアップの取得および保管は行われていることになっているが管理は徹底していない

(C) バックアップの取得や保管は行われているが、運用チームの意識に依存

(D) バックアップの取得は計画的には行っていない

設問③〕

事故処理に必要となるシステム運用の記録は確保されていますか？

セキュリティ事故に際して必要となる記録の確保のためには、以下のようなことが必要になります。

- 必要な記録の洗出しと取得についてのルールの確立
- システムの運用プロセスの中へのシステム運用についての記録の確保の組込み
- システムの運用プロセスの中へのアクセス権限付与の変更等のセキュリティ対策にかかわる処理についての記録の確保の組込み
- ルールに従った記録確保についての管理
- 取得した記録の適切な保管・管理

貴社サイトにおけるこれらの記録の取得、保管の状況を評価して下さい。

【評価】
Ⓐ 十分に検討された記録の取得、保管要領が確立しており、必要な記録の取得ならびに保管はシステムの運用の中に組込まれ、確実に運用されている
Ⓑ 必要な記録の取得、保管要領が確立しているが、厳格に運用されていると言えない。また、現時点での確保の対象としている記録は、サイトの運用実態に照らして妥当であるかどうかの確認はされていない
Ⓒ 一部の記録はとられているが、必要な記録の取得、保管についての組織的な検討は行われていない
Ⓓ セキュリティ事故に備えた記録の取得、保管は行われていない

⑹ 事故処理訓練の実施

セキュリティ事故はめったに起きるものではないため、たとえ、事故処理に対する手順が確立しており、必要なバックアップや記録が準備され、ツールも整備されていたとしても、対応する者の不慣れから、その実行に迅速性や正確性を欠き、被害を大きくしてしまうこともあります。セキュリティ事故の発生に際して、関係者が決められた処置を的確かつ迅速に行えるようにするためにはセキュリティ事故を想定した事故処理訓練の実施も必要となります。

設問①】

セキュリティ事故を想定した事故処理訓練は行われていますか？

有効な事故処理訓練を行うためには、以下のようなことも必要となります。

- 訓練内容、訓練手順、訓練サイクル等を示した事故処理訓練計画の確立
- 事故処理訓練の実施の管理
- 訓練結果の評価と問題点の事故処理計画へのフィードバック

貴社サイトにおけるセキュリティ事故を想定した事故処理訓練の実施状況を評価して下さい。

【評価】
Ⓐ 十分に検討された訓練計画があり、この計画に従った訓練を定期的に行っている
Ⓑ 確立した訓練計画はないが、定期的に訓練を行っている
Ⓒ 担当者レベルで事故処理訓練が行われることもある
Ⓓ 事故処理訓練は行っていない

(7) 実際に発生したセキュリティ事故とその対応についての評価

ここでは、貴社サイトにおいて最近発生したセキュリティ事故と事故発生に際して行った処置についてお訊ねします。

設問①】

貴社サイトで最近セキュリティ事故を経験しましたか。またそれはどんな事故でしたか？

【この 1 年以内に発生したセキュリティ事故と被害の程度】

(A) 他人をかたった者との取引　無、有 :被害の程度 重大、大、中、軽微）
(B) システムへの侵入　無、有 :被害の程度 重大、大、中、軽微）
(C) ウイルスの感染　無、有 :被害の程度 重大、大、中、軽微）
(D) 情報の漏洩　無、有 :被害の程度 重大、大、中、軽微）
(E) DoS 攻撃　無、有 :被害の程度 重大、大、中、軽微）
(F) その他（　　）　無、有 :被害の程度 重大、大、中、軽微）
(G) とりたててあげるようなセキュリティ事故は発生しなかった

設問②】質問①で G 以外を回答した方のみお答え下さい）

事故発生時、必要な処置は適切に行われましたか？

先にあげたセキュリティ事故が発生した時に行われた事故処理について評価して下さい。

【評価】

(A) 必要な処置はすべて適切かつ迅速に行われた
(B) 必要な処置はおおむね適切に行われたが、改善すべきところもある
(C) なんとか処置はすませたが、多くの問題を残した
(D) 必要な処置が適切に行われず混乱が発生した

設問③】質問②で A 以外を回答した方のみお答え下さい）

事故処理のどこに問題がありましたか？

発生したセキュリティ事故の処理で問題が発生したところと、その程度についてお訊ねします。問題を感じたものすべてをあげて下さい。

【問題が発生したところとその程度】複数回答）

(A) サービスの停止等の事故の拡大を防ぐためのとっさの処置
　無、有 :問題の程度 重大、大、中、軽）
(B) 事態の把握　無、有 :問題の程度 重大、大、中、軽）
(C) 被害範囲の調査　無、有 :問題の程度 重大、大、中、軽）
(D) システムの回復　無、有 :問題の程度 重大、大、中、軽）
(E) 業務の復旧　無、有 :問題の程度 重大、大、中、軽）
(G) 再発防止のための対策の検討と実施　無、有 :問題の程度 重大、大、中、軽）
(H) 迷惑をかけた利用者や他社への対応　無、有 :問題の程度 重大、大、中、軽）
(I) 事故についての外部への情報の公開　無、有 :問題の程度 重大、大、中、軽）
(J) 訴訟や損害賠償請求　無、有 :問題の程度 重大、大、中、軽）
(K) その他（　　）　無、有 :問題の程度 重大、大、中、軽）

設問④〕

発生したセキュリティ事故について関係機関に報告しましたか？

システムが不正なアクセスを受けたりウイルスに感染した場合は、IPA や JPCERT/ＣＣや警察等に報告することが義務付けられています。

貴社におけるこれら機関への報告状況についての対応をお訊ねします。

【関係機関への報告の状況】

Ⓐ すべて報告している
Ⓑ 報告することを原則にしているが、報告しないこともある
Ⓒ 報告することを原則にはしていないが、報告することもある
Ⓓ ほとんど報告しない
Ⓔ 報告したことがない

【報告を積極的に行っていない場合その理由】

前問で C、D、E を回答した方のみお答下さい。複数回答）

Ⓐ 管理が不十分で報告が漏れているため
Ⓑ 報告にメリットを感じないため
Ⓒ 報告するのが面倒なため
Ⓓ 報告すべきことを知らなかったため

第12章 総合評価および要望事項

ここでは、貴社サイトにおけるセキュリティ対策についての総合的な自己評価をお訊ねします。

(1) セキュリティ対策についての総合評価

設問①〕

実施しているセキュリティ対策を技術面ではどのように評価していますか？

貴社サイトのセキュリティ対策を技術面から評価して下さい。

【評価】
- (A) サイトの運営実態に照らし十分と考えている
- (B) 一通りの対策は講じられているが十分とは言えない。改善すべき点がある
- (C) 最低限の対策の範囲を出てない
- (D) 実質的な対策になっていない
- (E) わからない

設問②〕

サイト運営へのセキュリティ要求事項のプロセス化をどのように評価していますか？

計画したセキュリティ対策が確実に実行されるようにするためには、システムの管理や運用、業務現場に対するセキュリティ要求事項が、業務のプロセスに適切に組込まれていなければなりません。

貴社サイトにおけるこの点についての評価として最も近いものを選んで下さい。

【評価】
- (A) 十分と考えている
- (B) おおむね十分と考えている
- (C) 一部しかできていない
- (D) ほとんどできていない
- (E) わからない

設問③〕

サイト運営におけるセキュリティ要求事項の実行は十分に管理されていますか？

計画したセキュリティ対策が確実に実行されるようにするためには、システムの管理や運用、および業務現場に対するセキュリティ要求事項の実行が常にチェックされていることも必要です。

貴社サイトにおけるこの点について評価して下さい。

【評価】
- (A) セキュリティ要求事項の実行に対する管理はルール化されており、このルールに沿った管理が厳格に行われている
- (B) セキュリティ要求事項の実行に対する管理はルール化されているが、このルールに沿った管理が厳格には行われていない
- (C) セキュリティ要求事項の実行に対する管理についてのルールはなく、部分的にしか管理されていない
- (D) ほとんど管理されていない
- (E) わからない

設問④】

セキュリティ対策についてのドキュメント化の状況をどのように評価していますか？

実施されているセキュリティ対策の的確性の確認や、問題が生じた場合の調査や対策の実施には、セキュリティ要求事項やその実施についての正確な情報が必要になります。このためには、以下のようなものについてのドキュメンテーションの整備が必要となります。

- セキュリティ対策にかかる基準やルール
- セキュリティ対策の各種要件
- セキュリティ対策に関係する各種要件の指定
- システムの構成やセキュリティ機能の設定に関する情報
- セキュリティ対策にかかるシステム運用についての記録

貴社サイトにおけるセキュリティ対策に関係するドキュメントの整備状況を評価して下さい。

【評価】

(A) ルールに沿ったドキュメント化が行われており、常に関係ドキュメントの正確性は維持されている
(B) ルールに沿ってドキュメント化が行われることになっているが、厳格に運用されているとは言えず、関係ドキュメントのすべてについて正確かどうかは疑問
(C) 担当者レベルで行っている一部を除き、すべてにわたりドキュメント化は行われていない
(D) ドキュメントの整備はほとんど行われていない
(E) わからない

設問⑤】

実施しているセキュリティ対策全体をどのように評価していますか？

下記の中から、貴社サイトで実施しているセキュリティ対策の評価として最も近いものを選んで下さい。

【セキュリティ対策全体に対する評価】

(A) サイトの運営形態に照らし十分な対策が講じられていると考えている
(B) 一通りの対策は講じているものの、技術面でも管理面でも十分とは言えない
(C) ある程度の対策は講じられているものの、組織的戦略的には程遠く、不十分
(D) 実質的な対策はほとんどなされていない
(E) わからない

設問⑥〕

個々の対策について評価して下さい。

下記にあげる個々の対策についての、貴社なりの評価をお訊ねします。

【セキュリティ対策全体に対する評価】(それぞれにお答えください)

Ⓐ セキュリティマネジメントの確立	(十分、おおむね十分、改善が必要、不在)
Ⓑ 不正アクセス対策	(十分、おおむね十分、改善が必要、未対策)
Ⓒ セキュリティホール対策	(十分、おおむね十分、改善が必要、未対策)
Ⓓ ウイルス対策	(十分、おおむね十分、改善が必要、未対策)
Ⓔ セキュリティ管理情報の保護管理	(十分、おおむね十分、改善が必要、未対策)
Ⓕ ユーザ情報の保護管理	(十分、おおむね十分、改善が必要、未対策)
Ⓖ 通信の保護	(十分、おおむね十分、改善が必要、未対策)
Ⓗ ユーザ認証の管理	(十分、おおむね十分、改善が必要、未対策)
Ⓘ システムの構成の管理	(十分、おおむね十分、改善が必要、未対策)
Ⓙ システムや業務の運用の管理	(十分、おおむね十分、改善が必要、未対策)
Ⓚ セキュリティ事故への備え	(十分、おおむね十分、改善が必要、不在)

設問⑦〕設問⑤で、A、B 以外を回答した方のみお答え下さい)

セキュリティ対策が不十分なままにされている理由は何ですか？

下記の中から、その理由を選択して下さい。

【セキュリティ対策を不十分なままにしている理由】

Ⓐ 十分とは考えていないが、脅威に対する現実感が薄いため
Ⓑ 予算面での制約が大きいため
Ⓒ 技術的な対応力が不足しているため
Ⓓ その他（　　）

設問⑧〕設問⑤で、A、B 以外を回答した方のみお答え下さい)

セキュリティ対策の向上についての今後の計画はどのようになっていますか？

今後のセキュリティの強化についてお訊ねします。

【今後の取組み】

Ⓐ 強化を準備中
Ⓑ 強化を検討中
Ⓒ 当面は現状のままとするが、今後、強化を検討する
Ⓓ 今後も強化を検討する予定はない

②要望事項

ここでは、セキュリティ向上のため、貴社が考えている政府機関やシステムベンダー、セキュリティサービスベンダーに対するご要望があればお聞かせ下さい。

設問①〕

政府系機関等に対し何か要望はありますか？

【要望事項】

参考）情報セキュリティにかかる政府系機関としては、以下があげられます。

・各省庁、地方自治体、警察

・IPA や JPCERT／ＣＣ等のセキュリティに関する機関

設問②〕

IT プロダクトベンダーやシステムソリューションベンダーに対し何か要望はありますか？

【要望事項】

設問③〕

セキュリティサービスベンダーやセキュリティコンサルタントに対し何か要望はありますか？

【要望事項】

設問④〕（モールに出店しているショップの方のみお答え下さい）

セキュリティに関し出店先のモールに対し何か要望はありますか？

【要望事項】

設問⑤〕（モールの方のみお答下さい）

セキュリティに関し出店ショップに対し何か要望はありますか？

【要望事項】

設問⑥〕

サイトのセキュリティの確保について何か悩んでいることはありますか？

【悩み】

ECサイトにおけるセキュリティ対策の実態調査報告

平成　１５年　3月　発行

発行所　　財団法人　日本情報処理開発協会
　　電子商取引推進センター
　　東京都港区芝公園３丁目５番８号
　　機械振興会館　３階
　　TEL：０３（３４３６）７５００
印刷所　　株式会社　美行企画
　　東京都千代田区神田錦町２丁目５番地
　　鈴木第２ビル
　　TEL：０３（３２１９）２９７１

この資料は再生紙を使用しています。