ECサイト向けセキュリティ対策ガイドライン

― 実施の手引き ―

平成１３年３月

電子商取引推進協議会
セキュリティWG

はじめに

本書は、「EC サイト向けのセキュリティ対策ガイドライン」の第二分冊として、EC サイトにおけるセキュリティ対策として求められる施策の個々について、

- その主旨
- 実施すべき具体的事項
- 実施上のポイント

を示したものである。

個々のセキュリティ対策の背景となっている、EC サイトにおけるセキュリティに関する問題とセキュリティ対策の組立てについての考え方に関しては、本ガイドラインの第一分冊である「EC サイト向けセキュリティ対策ガイドライン－解説編」を参照されたい。

本書は、セキュリティ対策として EC サイトの運営管理上で求められることを体系化し、その個々について解説したものであり、実施現場における具体的な解を示したものではない。個々の脅威に対し求める対策のレベルや、サイト内におけるデータフロー制御ルール、システムへのアクセス監視のルール、情報に対するアクセス権限の付与ルール等の具体的な定義は、サイトが対象としている業務やシステム構成等のサイトの運営形態や、経営レベルでの当該サイトにおけるセキュリティについての基本的な姿勢により異なるものであり、それぞれのサイトの実情に合わせ、サイトの責任で検討決定すべきものである。

本書は、これらの検討において、検討すべきことを体系化して示すとともに、それらの検討についてのガイドとなるものと考えている。

本書が、EC サイトにおけるセキュリティ対策の検討に役に立ち、セキュアなサイト運営の確立に貢献することを期待している。

目 次

1 EC サイトに求められるセキュリティ対策の体系と概要

1.1 セキュリティ対策の体系

本ガイドラインでは、セキュリティ対策は、

- 不正アクセス対策
- セキュリティホール対策
- ウイルス対策
- セキュリティ管理情報の保護管理
- ユーザデータの保護管理
- 通信にかかるリスク対策
- ユーザ認証の適切な適用

といった個々の脅威に対する対策と、これらの対策の実施を支えるものとしてのセキュアなシステムの構築とセキュアなシステム運用の実現、およびこれらの施策全体を統括するサイト運営におけるセキュリティマネジメントの 10 の対策テーマから組立てられるとしている。

これらの対策テーマの相対的な位置付けを、図 1-1 に示す。また、対策テーマ間の関連を表 1-1 に示す。

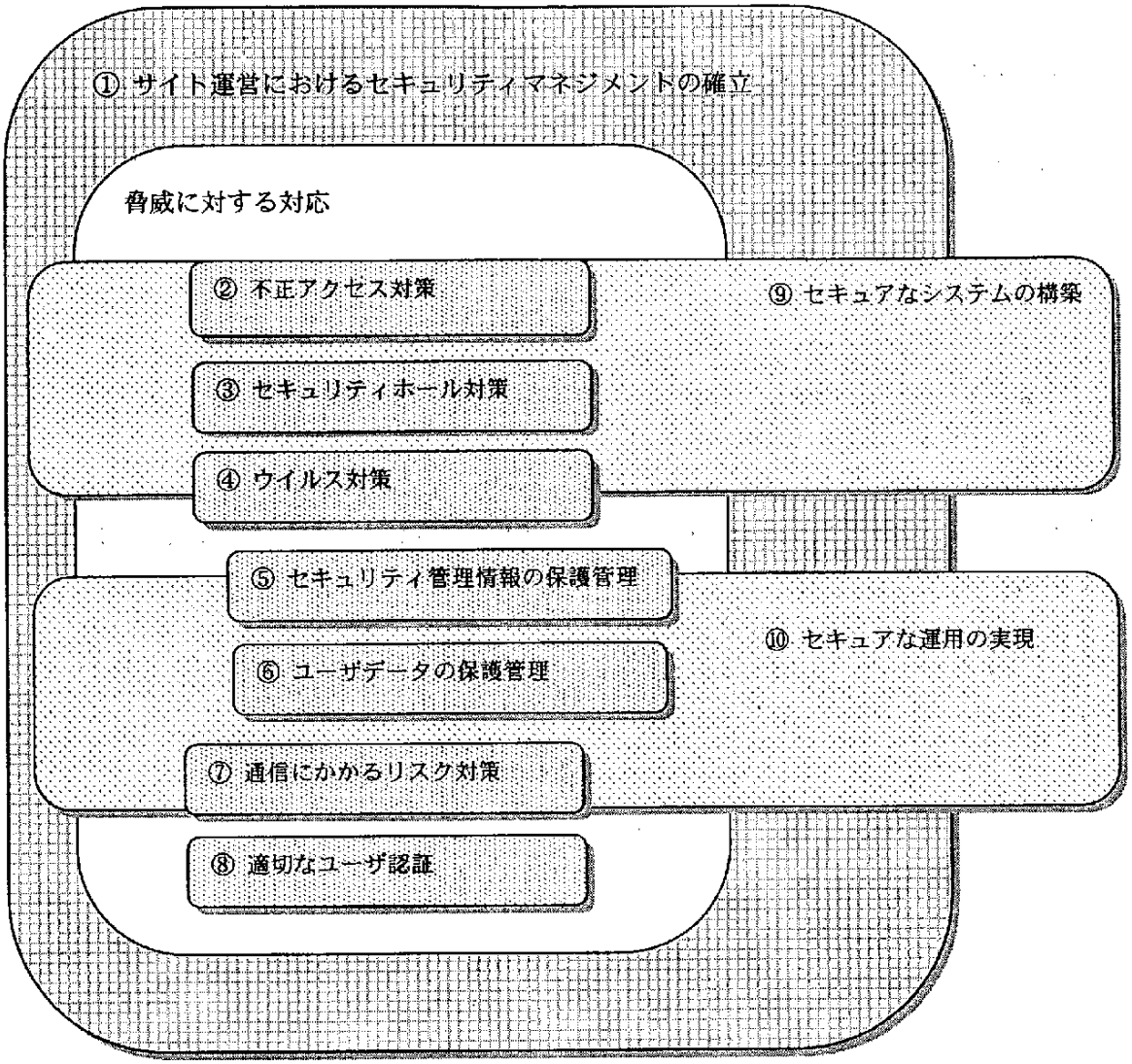


図 1-1　本ガイドラインにおける対策テーマの体系

表 1-1　セキュリティ対策における対策テーマの相関

項番		1 セキュリティマネジメントの確立	2 システムへの不正アクセス対策	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 ユーザデータの保護管理	7 通信にかかるリスク対策	8 ユーザ認証の適切な適用	9 セキュアなシステムの構築	10 セキュアな運用の確保	備考
1	セキュリティマネジメントの確立	＝＝＝										
2	システムへの不正アクセス対策	⇦	＝＝＝			⇦			⇦	⇦	⇦	
3	セキュリティホール対策の実施	⇦	⇦	＝＝＝						⇦	⇦	
4	ウイルス対策の実施	⇦			＝＝＝					⇦	⇦	
5	セキュリティ管理情報の保護管理の実施	⇦	⇦	⇦	⇦	＝＝＝		⇦	⇦	⇦	⇦	
6	ユーザデータの保護管理の実施	⇦	⇦	⇦	⇦	⇦	＝＝＝	⇦	⇦	⇦	⇦	
7	通信にかかるリスク対策の実施	⇦						＝＝＝	⇦	⇦	⇦	
8	ユーザ認証の適切な適用	⇦	⇦			⇦			＝＝＝			
9	セキュアなシステムの構築	⇦	⇦	⇦	⇦	⇦	⇦	⇦	⇦	＝＝＝	⇦	
10	セキュアな運用の確保	⇦	⇦	⇦	⇦	⇦	⇦	⇦	⇦	⇦	＝＝＝	

⇦ 指針の付与　　⇦ 要求(当該施策の一要素として関与)　　⇦ 影響（当該施策の不備は、矢印の先の施策を脆弱

1.2 サイト運営におけるセキュリティマネジメントの確立

1.2.1 サイト運営におけるセキュリティマネジメント確立とは

ECサイトシステムが必要なレベルのセキュリティを確保するためには、以下のことが必要となる。

- 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醸成
- セキュリティ対策の目標の明確化
- セキュリティ対策をどのような組立てで行うかというセキュリティ対策の組立て
- 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

セキュリティマネジメントの確立とは、これらに対する取組方針を明確にし、セキュリティ対策を計画的、組織的に実施する基盤を確立するための施策を総称するものである。

1.2.2 サイト運営におけるセキュリティマネジメント確立のための施策

本ガイドラインでは、サイト運営におけるセキュリティマネジメントの確立のための施策を、以下で構成する。

(1) サイト運営上のセキュリティポリシーの確立
(2) セキュリティ対策の実施にあたっての責任体制の確立
(3) 関係者に対するセキュリティに関する教育、管理の実施
(4) サイト運営に対するセキュリティ監査の実施

1.3 不正アクセス対策の概要

1.3.1 不正アクセス対策とは

権限のない者によるサイトシステムへのアクセスは、システム機能の不正使用による業務やシステム運用の混乱を引き起したり、ソフトウェアおよびセキュリティ管理情報やユーザ情報等のシステム資産の破壊、改ざん、不正取得等につながる攻撃を可能にする。

システムへの不正アクセス対策は、システムをこのような被害から守るため、外部ならびに内部からの保護対象領域へのアクセスを、正規のもの(許可された者がその権限の範囲でのアクセス)に限定し、それ以外のアクセスを排除し、

- 権限のない者によるシステムへの不正なアクセスの阻止
- システムへの侵入を許したときの被害の極小化

を行うものである。

1.3.2 不正アクセス対策の構成

本ガイドラインでは、サイトシステムへの不正アクセス対策を、以下の施策で構成する。

(1) システムへの不正アクセスに対する取組方針の確立
(2) 不正アクセス対策についての責任体制の確立
(3) アクセス管理ポリシーの確立
(4) 各サーバにおける不要サービスの除去または停止
(5) アクセス管理ポリシーに沿ったデータフロー制御の実施
(6) 個々のサービスに対するアクセス管理要件の確立
(7) 個々のサービスに対する指定されたアクセス管理の実施
(8) サイト外との通信ならびにサイト内のデータフローの監視の実施
(9) 不正アクセス対策に用いる機能の適切な実装
(10) 不正アクセスによる事故への備えの実施
(11) 不正アクセス対策にかかる施策のシステム運用への反映
(12) 関係者に対する不正アクセス対策についての教育の実施
(13) 不正アクセス対策の実施状況についての監査の実施

1.4 セキュリティホール対策の概要

1.4.1 セキュリティホール対策とは

サイトシステムに対するセキュリティホールをついた攻撃は、システム機能の不正使用、ソフトウェアの不正取得、改ざん、破壊、セキュリティ管理情報の破壊、改ざん、不正取得、ユーザ情報の破壊、改ざん、不正取得等の被害につながる。

セキュリティホール対策とは、このような被害からシステムを守るため、

- 既知のセキュリティホールの除去
- 残留セキュリティホールによる被害発生の抑止
- セキュリティホールをついた攻撃を受けた時の被害の極小化

を行うための施策の総称である。

1.4.2 セキュリティホール対策の構成

本ガイドラインでは、セキュリティホール対策を、以下の施策で構成する。

(1) セキュリティホールに対する取組方針の確立
(2) セキュリティホール対策についての責任体制の確立
(3) セキュリティホールに関する情報の収集と収集情報に対する適切な処理の実施
(4) 対策実施単位の個々に対する対策要件の指定
(5) インストールするソフトウェアに対するセキュリティホール検査の実施
(6) システムに対するセキュリティホール検査の実施
(7) システムに対するセキュリティホールをついた攻撃に対する監視の実施
(8) セキュリティホール対策に用いる機能の適切な実装
(9) セキュリティホールをついた攻撃による事故への備えの実施
(10) セキュリティホール対策にかかる施策のシステムの運用への反映
(11) 関係者に対するセキュリティホール対策についての教育の実施
(12) セキュリティホール対策の実施状況についての監査の実施

1.5 ウイルス対策の概要

1.5.1 ウイルス対策とは

ウイルス対策とは、サイトのシステムへのウイルス感染による被害を防ぐため、

- ウイルス感染の防止
- ウイルス感染時の被害の極小化

のための諸施策を総称をいう。

1.5.2 ウイルス対策の構成

本ガイドラインでは、ウイルス対策を、以下の施策で構成する。

(1) ウイルスに対する取組方針の確立
(2) ウイルス対策についての責任体制の確立
(3) ウイルスに関する情報の収集と収集情報の適切な処理の実施
(4) 対策実施単位個々に対する対策要件の指定
(5) 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
(6) データに対すウイルス検査の実施

(7) システムに対するウイルス検査の実施
(8) ウイルス感染ファイルの外部への持出しの防止
(9) ウイルス対策に用いる機能の適切な実装
(10) ウイルス感染事故への備えの実施
(11) ウイルス対策にかかる施策のシステム運用への反映
(12) 関係者に対するウイルス対策についての教育の実施
(13) ウイルス対策の実施状況についての監査の実施

1.6 セキュリティ管理情報保護管理策の概要

1.6.1 セキュリティ管理情報保護管理とは

セキュリティ管理情報の漏洩や改ざんは、なりすましによる不正取引の実行、他サイト攻撃への加担、システム機能の不正利用、業務やシステム運用の混乱、システムの破壊や改ざん等につながる。

セキュリティ管理情報保護管理とは、セキュリティ管理情報を攻撃から守り、

- 外部への漏洩
- 改ざん
- 破壊

を受けないようにするための施策と、万一、攻撃を受けたとしてもその被害を限定的なものにするための施策の総称を指す。

1.6.2 セキュリティ管理情報保護管理策の構成

本ガイドラインでは、セキュリティ管理情報の保護管理を、以下の施策で構成する。
(1) セキュリティ管理情報の保護管理についての取組方針の確立
(2) セキュリティ管理情報の保護管理についての責任体制の確立
(3) 個々のセキュリティ管理情報に対する保護管理要件の指定
(4) セキュリティ管理情報の適切なシステムへの格納
(5) 個々のセキュリティ管理情報に対する指定されたアクセス制限の実施
(6) 個々のセキュリティ管理情報に対する指定されたアクセス監視の実施
(7) セキュリティ管理情報にかかわる印刷物、電磁媒体等の適切な取扱いの実施
(8) 業務委託先に対するセキュリティ管理情報の保護管理についての指導、管理の実施
(9) セキュリティ管理情報の保護管理に用いる機能の適切な実装

(10)セキュリティ管理情報の漏洩、改ざん、破壊事故への備えの実施
(11)セキュリティ管理情報の保護管理にかかる施策のシステム運用への反映
(12)関係者に対するセキュリティ管理情報の保護管理についての教育の実施
(13)セキュリティ管理情報の保護管理の実施状況についての監査の実施

1.7 ユーザデータの保護管理策の概要

1.7.1 ユーザデータの保護管理とは

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流出は、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る。また、これらの情報に対する改ざん、破壊行為は、業務の運営を混乱させることにもなる。ユーザデータの保護管理とは、消費者のプライバシー侵害や取引先のビジネスの妨害に加担しないよう、これらの情報を含むデータやファイル等を外部の攻撃から守り、

- 漏洩
- 改ざん
- 破壊

等を受けないようにするための施策と、万一、攻撃を受けたとしてもその被害を限定的なものにするための施策の総称を指す。

1.7.2 ユーザデータの保護管理策の構成

本ガイドラインでは、ユーザデータの保護管理を、以下の施策で構成する。
(1) ユーザデータの保護管理についての取組方針の確立
(2) ユーザデータの保護管理についての責任体制の確立
(3) システム上の個々のユーザデータに対する保護管理要件の指定
(4) ユーザデータの適切なシステムへの格納
(5) 個々のユーザデータに対する指定されたアクセス制限の実施
(6) 個々のユーザデータに対する指定されたアクセス監視の実施
(7) ユーザ情報にかかわる印刷物、電磁媒体等の適切な取扱いの実施
(8) 業務委託先に対するユーザ情報の保護管理についての指導、管理の実施
(9) ユーザデータの保護管理に用いる機能の適切な実装
(10) ユーザデータの漏洩、改ざん、破壊事故への備えの実施

(11) ユーザデータの保護管理にかかる施策のシステム運用への反映
(12) 関係者に対するユーザデータの保護管理についての教育の実施
(13) ユーザデータの保護管理の実施状況についての監査の実施

1.8 通信にかかるリスク対策の概要

1.8.1 通信にかかるリスク対策とは

通信にかかるリスク対策とは、

- 通信路上のデータに含まれる顧客のID、パスワード等のセキュリティ管理情報、および顧客の個人情報や取引先の商業秘密情報に対する盗聴、改ざん、破壊行為
- 通信の否認

等を防ぐための施策と、このような攻撃を受けた時への備えを総称するものである。

1.8.2 通信にかかるリスク対策の構成

本ガイドラインでは、通信にかかるリスク対策を、以下の施策で構成する。
(1) 通信にかかるリスクについての取組方針の確立
(2) 通信にかかるリスク対策実施についての責任体制の確立
(3) 個々の通信に対するリスク対策要件の指定
(4) 操作に依存する対策おけるその厳格な運用についての指導の実施
(5) 通信にかかるリスク対策に用いる機能の適切な実装
(6) 通信にかかるセキュリティ事故への備えの実施
(7) 通信にかかるリスク対策のシステム運用への反映
(8) 通信にかかるリスク対策の実施状況についての監査の実施

1.9 ユーザ認証の適切な適用の概要

1.9.1 ユーザ認証の適切な適用とは

ユーザ認証の適切な適用とは、ECサイトがその業務上、ネットを介して通信する相手の認証を適切に行い、

- 意図しない相手へのシステムの機能へのアクセスの阻止

- 意図しない相手との取引の拒否
- 意図しない相手への情報の提供の拒否

を実現するための施策と、問題が生じた場合の備えを総称するものである。

1.9.2 ユーザ認証の適切な適用のための施策の構成

本ガイドラインでは、ユーザ認証の適用を適切に行うための施策を、以下で構成する。

(1) ユーザ認証についての取組方針の確立
(2) ユーザ認証の適切な適用についての責任体制の確立
(3) 個々の認証場面に対する認証要件の適切な指定
(4) パスワードに対するの適切な管理の実施
(5) ユーザ認証とその管理に用いる機能の適切な実装
(6) ユーザ認証に関する事故への備えの実施
(7) ユーザ認証にかかる施策のシステム運用への的確な反映
(8) ユーザ認証の適用状況についての監査の実施

1.10 セキュアなシステムの構築についての概要

1.10.1 セキュアなシステムの構築とは

サイトシステムのセキュリティ対策は、セキュアなシステムの構成の上に置かれた各機器に組込んださまざまなセキュリティサービス機能や、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る。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、個々の脅威に対するセキュリティ対策が求めていることを的確に対応したものでなければならない。

セキュアなシステムの構築とは、サイトの構成の設計やその実装を適切に行い、

- 攻撃を受付けにくい
- 攻撃を受けても被害は限られる

と言えるような、攻撃に対して堅固なシステムを構築することをいう。

サイトシステムの構成や各構成機器におけるセキュリティ対策にかかわる機能を、セキュリティ対策が求めていることを的確に反映したものにするためには、システムの構成管理面からの十分な対応が必要となる。

これまでに述べてきた各脅威に対応するセキュリティ対策のところでも、必要な機能の適切な実装については求めてきたが、ここでは、実際のシステム構成や各機器における機能の実装が、サイ

トのセキュリティ確保のために定められた諸施策を的確に反映したものにし、サイトシステムをセキュリティに強いシステムにするよう、システム構成の管理に求めることを纏めている。

1.10.2 セキュアなシステムの構築に必要な施策の構成

本ガイドラインでは、セキュアなシステムの構築を実現するための施策を、以下で構成する。

(1) セキュアなシステムの構築についての責任体制の確立
(2) サイトのセキュリティポリシーに沿ったシステム構成方針の確立
(3) 構成方針に沿ったシステム構成の構築
(4) 各機器に対するセキュリティ要件の的確な実装
(5) システム構成と機能の実装の管理についての監査の実施

1.11 セキュアなシステム運用の実現についての概要

1.11.1 セキュアなシステム運用の実現とは

セキュリティ対策におけるさまざまな施策は、システムの運用に依存しているところが多い。

システムの構成や諸機能がセキュリティについて十分に配慮されていたとしても、システムの運用がずさんであれば、システムのセキュリティは危険にさらされ、システムの構築で施したせっかくの苦心も無に帰しかねない。

特に、システムの運用においては、日常の多忙なシステム運用の中にセキュリティにかかる運用処理が埋もれ易いことと、セキュリティについては専門家でない多くの要員が関係するため、不手際も生じ易い。

各脅威に対応したセキュリティ対策においても、対応したシステム運用の的確な実施に実現について述べてきたが、ここでは、システムの運用上におけるセキュリティ対策にかかわる事項が、的確に実施されるように、運用サイドに求められることを纏めたものである。

1.11.2 セキュアな運用の実現に向けた施策の構成

本ガイドラインでは、セキュアな運用を実現するための施策を、以下で構成する。

(1) セキュアなシステム運用の実現に向けた取組方針の確立
(2) セキュアなシステム運用の実現のための責任体制の確立
(3) セキュリティ対策にかかる諸施策の運用規定、運用マニュアルへ適切な反映

(4) 日々のセキュリティ対応運用に対する適切な管理の実施
(5) システムへの物理アクセスについての適切な管理の実施
(6) サイトシステムにおけるセキュリティ事故への備えの実施
(7) 運用関係者に対するセキュリティ教育の実施
(8) セキュリティ対策にかかるシステム運用についての監査の実施

2 サイト運営におけるセキュリティマネジメントの確立

2.1 セキュリティマネジメント確立のための施策一覧

表 2-1 に、サイトのセキュリティマネジメント確立に必要な具体的実施事項の一覧を示す。

表 2-1 セキュリティマネジメント確立のための具体的実施事項

施策名	具体的実施事項
(1) サイト運営上のセキュリティポリシーの確立	① 不正アクセス対策の目標の明確化 ② 不正アクセス対策の適用範囲の明確化 ③ 不正アクセス対策実施基準の確立 ④ 不正アクセス対策の組立ての明確化 ⑤ 不正アクセス対策についての取組方針の関係者への周知
(2) セキュリティ対策の実施にあたっての管理体制を確立する	① 不正アクセス対策についての責任体制の明確化 ② 不正アクセス対策関係者間の連絡体制の構築
(3) 関係者に対するセキュリティに関する教育、管理を行う	① 不正アクセス対策についての責任体制の明確化 ② 不正アクセス対策関係者間の連絡体制の構築
(4) サイト運営に対するセキュリティ監査を行う	① 不正アクセス対策についての責任体制の明確化 ② 不正アクセス対策関係者間の連絡体制の構築

2.2 個別具体策

(1) サイト運営上のセキュリティポリシーを確立する

【主旨】

サイトのセキュリティは、サイト運営にかかわる多くの関係者が一体となった、セキュリティ対策にかかる諸施策ついての継続的な努力があって始めて達成されるものである。

サイトのセキュリティを目標とするレベルで実現するための第一歩は、サイトにおけるセキュリティ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について、関係者に共通の基盤を与えるための、以下に示すようなことを明確にしたサイト運営にかかわる全体的なセキュリティポリシーが確立していなければならない。

- 目標とするセキュリティのレベル
- セキュリティ対策の組立て

【具体的な実施事項】

(1) セキュリティ確保への取組み方針の確立と宣言

サイトにおけるセキュリティ確保の取組方針として、以下を明確にし、宣言文にする。

- セキュリティ対策の目指すところ
- セキュリティ対策が対象とする脅威
- セキュリティ対策にかかる施策の組立て
- セキュリティ対策の推進体制
- セキュリティ対策についての予算の考え方

(2) セキュリティへの取組み宣言の関係者への徹底

さまざまな機会や方法を用いて、作成したセキュリティ確保についての宣言が、サイトの構築、運用関係者に浸透するようにする。

このための方法としては、以下のようなことが考えられる。

- ポスター化する等してサイトに掲示する
- 関係者全員に配布する
- 朝礼等の機会を通じて、関係者への定期的な再確認

【対策実施上のポイント】

(1) セキュリティ対策の目指すところの定義について

セキュリティ対策の目指すところとしては、以下があげられる。

- 円滑な業務の運営を阻害されないこと

- 円滑なサイトシステムの運用を阻害されないこと
- 消費者を、サイトのセキュリティ問題からトラブルに巻き込まないこと
- サイトのセキュリティ問題から、取引先とのトラブルを生じる事態を起こさない

(2) セキュリティ対策が対象とする攻撃について

セキュリティ対策がどのような攻撃を前提としているかを示すもので、以下のようなものがあげられる。

- 取引等におけるなりすまし
- システムへの不正アクセスおよびシステムへの侵入
- セキュリティホールをついた攻撃
- ウイルスによる攻撃
- セキュリティ管理情報の不正取得、改ざん、破壊
- ユーザデータの不正取得、改ざん、破壊
- 通信路上での情報の不正取得、改ざん、破壊
- 通信における事後否認

(3) セキュリティ対策にかかる施策の組立て

セキュリティ対策をどのように行うのかを示すもので、

- セキュリティ対策のテーマと対策テーマ間の関連
- セキュリティ対策実施のための基準

を明確にする必要がある。

本ガイドラインは、**1.1** 節に示すようなセキュリティ対策テーマの組立てに立って、個別対策を展開している。また、各種の対策実施基準については、各セキュリティ対策テーマにおける当該対策テーマに対する取組方針の中で考え方が示されている。

(2) セキュリティ対策の実施にあたっての管理体制を確立する

【主旨】

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ている。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を明確にするとともに、関係者それぞれが、自分に求められることを周知しておくことが必要となる。

また、これら関係責任者間の連携体制の確立も求められる。

【具体的な実施事項】

(1) セキュリティにかかる責任者と責任分担の確立

サイトのセキュリティ確保に関し、その責任を明確にしておく責任者としては、以下があげられる。

- セキュリティ総括責任者
- 不正アクセス対策責任者
- セキュリティホール対策責任者
- ウイルス対策責任者
- セキュリティ管理情報の保護管理責任者
- ユーザデータの保護管理責任者
- 通信にかかるリスク対策責任者
- ユーザ認証管理責任者
- システム管理者
- システム運用責任者

セキュリティ総括責任者の責任については、「対策実施上のポイント」を参照。また、その他の責任者の責任については、第3～10章参照。

(2) 関係者間の連携体制の確立

関係責任者間および担当者間の連携を円滑にするため、以下のようなことも明確にしておくべきである。

- 方向ルートと報告手続き
- 各種連絡会議の設定

【対策実施上のポイント】

(1) セキュリティ総括責任者の責任

サイトのセキュリティ確保の全体責任者で、以下のことに責任を持つ。

- セキュリティポリシーの宣言と、関係者への徹底
- セキュリティ対策にかかる各種の基準の発行

- セキュリティ確保のための各種施策実施の監督
- セキュリティにかかる問題が発生した場合の対象の統括
- セキュリティ対策にかかる予算の確保と管理

サイトのセキュリティ統括責任者は、サイトの運営責任者またはそれの準じる者である事が望ましい。

(2) 組織が小さい場合、一人が多くを兼務しても構わないが、その責任を明確にするため、それぞれの責任者として明確にしておくべきである。

(3) サイト運営関係者に対するセキュリティに関する教育、管理を行う

【主旨】

サイトのセキュリティは、サイト運用関係者のセキュリティに対する意識と、それぞれに求められていることについての正確な理解と、その律儀な遂行に依存する。

このため、セキュリティマネジメントの一環として、サイト運用関係者には、これらに関する教育を行うとともに、業務の遂行に関する必要な躾を行うこと必要となる。

また、サイト運営関係者の作為による情報の漏洩や、攻撃者の便宜を図るようなことがないようにするための要員管理上の施策も必要となる。

【具体的実施事項】

(1) セキュリティ教育の実施

サイト運営関係者に対しては、定期的な教育の実施を行うべきである。

サイト運営関係者全員に対しては、

- セキュリティリスクとサイトのセキュリティに対する取組みについての教育

また、セキュリティ対策関係者には、それぞれのサイト運営上の業務に対応して、以下のような教育が必要となる。

- システムへの不正アクセス対策についての教育
- セキュリティホール対策についての教育
- ウイルス対策についての教育
- セキュリティ管理情報の保護管理についての教育
- ユーザデータの保護管理についての教育
- システム運用関者に対するセキュリティ教育

これらの教育は、計画されたカリキュラムに従い、整備されたテキストの下で行われることが望ましい。

(2) セキュリティ面からの要員管理の実施

サイト運営にかかわる要員による意図的およびミスによる、サイト運営にかかくわるセキュリティ事故を防止するためには、以下ような配慮が必要となる。

- 不安要員のサイト運営からの排除
- サイト運営要員に対するセキュリティにかかわる責務の明示
- セキュリティについての意識の醸成
- 必要なスキルの確保の支援とスキルレベルの把握

【対策実施上のポイント】

(1) セキュリティ教育カリキュラムの確立

関係者へのセキュリティ教育が行き届くようにするためには、セキュリティ教育に関するカリキュラムを確立しておくことが望ましい。

教育カリキュラムとして規定すべき事項は以下のようなものとなる。

- セキュリティ教育の体系
- 教育テーマ毎の教育対象者
- 教育テーマ毎の教育内容とそのレベル
- 教育テーマ毎の教育の実施サイクル、実施時点
- 教育テーマ毎の講師、テキスト等の実施要領

(2) サイト運営関係者全員を対象としたセキュリティ教育について

サイト運営の関係者全員を対象としたセキュリティリスクとセキュリティ教育のイメージを、表 2-2 示す。

(3) セキュリティ教育の一部を外部の専門家に依頼するのも有効であるが、取組み姿勢等サイトのセキュリティポリシー等サイト運営上の基本事項については、内部の者が行うべきである。

表 2-2 サイトの関係者全員を対象としたセキュリティ教育のイメージ

項番	項目	概要
1	目的	・サイトの運営関係者全てに対するセキュリティについての啓蒙 ・サイトにおけるセキュリティ対策の組立ての理解
2	対象	・サイトの運営関係者全員 ーシステム設計関係者者、システム管理関係者、システム運用関係者、サイトの業務関係者 等
3	教育内容	・サイトにおける保護資産とセキュリティリスクの概要 ・サイトにおけるセキュリティへの取組み方針 ・サイトの構築、運用に関係する各種セキュリティ基準の概要 ・業務遂行上の留意事項 ・セキュリティ事故の事例
4	実施サイクル	・定期教育として、年１回以上 ・組織の改定、人事異動に伴い、新たな関係者が登場する場合

(4) サイト運営に対するセキュリティ監査を行う

【主旨】

サイトのセキュリティは、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ある。しかし、十分に検討されたと考えられる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、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らない。

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の実施状況をチェックする、サイト運営全体に対するセキュリティ監査の定期的な実施は、サイト運営におけるセキュリティの確保して行くためには欠かせない。

なお、サイト運営におけるセキュリティ監査は、

- サイト運営におけるセキュリティマネジメントについての監査
- 脅威への対応を中心として組立てられたセキュリティ対策テーマごとの対策の実施状況についての監査

から構成される。

【具体的な実施事項】

(1) サイト運営おけるセキュリティマネジメントについての監査の実施

サイト運営におけるセキュリティ確保のための具体的な諸施策の適切な実施のための管理環境の整備に関する監査で、以下のような事項についてのチェックを行う。

ベースとなる所対策を全体的な立場からチェックし、サイトの堅牢性を評価するもので、以下のような項目がチェック対象となる。

- サイト運営全体に対して定義されたセキュリティポリシーの妥当性
- サイトのセキュリティ確保のための施策の組立ての妥当性
- セキュリティマネジメントの仕組みの確立状況
- 関係者におけるセキュリティとセキュリティマネジメントについての認識
- セキュリティマネジメントの実施状況
- セキュリティ事故への対応状況

(2) 対策テーマ別のセキュリティ対策の実施状況についての監査の実施

セキュリティ対策として具体的に定めていることの妥当性、ならびに定められている対策の実施状況についてのチェックを行うもので、第3～10 章までに示されているようなセキュリティ対策テーマごとに実施する。

この監査は、以下に示すような監査で構成される。

- 不正アクセス対策の実施状況についての監査

- セキュリティホール対策の実施状況についての監査
- ウイルス対策の実施状況についての監査
- セキュリティ管理情報の保護管理の実施状況についての監査
- ユーザデータの保護管理の実施状況についての監査
- 通信にかかるリスク対策の実施状況についての監査
- ユーザ認証の適用についての監査
- システムの構成管理についての監査
- システム運用についての監査

それぞれの監査内容とそのポイントについては、該当の章を参照。

(3) セキュリティ監査実施要領の確立

セキュリティ監査が適切に実施され、その実効をあげるためには、それぞれの監査について、監査実施要領が確立されマニュアル化されていることが望ましい。

セキュリティ監査実施要領で、定義すべき事項は以下のようになる。

- 監査の狙いと監査のポイント
- 監査の実施サイクル
- 監査実施体制
- 監査メンバーの要件
- 監査項目

(4) セキュリティ監査体制の確立

セキュリティ監査が適切に実施され、その実効をあげるためには、監査体制をあらかじめ決定しておくことが望ましい。

- 監査長および監査担当者は、関係者以外の第三者が当てられるのが望ましい。
- 監査担当者にはある程度のセキュリティに関する技術知識が必要である。
- システムベンダーの SE 等外部の要員を監査担当として用いることも一つの方法である。ただし、この場合は契約相手の身元確認や契約内容による情報漏洩防止策実施等を別途定めた規定に従って行う。

3 不正アクセス対策

3.1 必要な施策項目

図 3-1 に、セキュリティホール対策の組立てを示す。

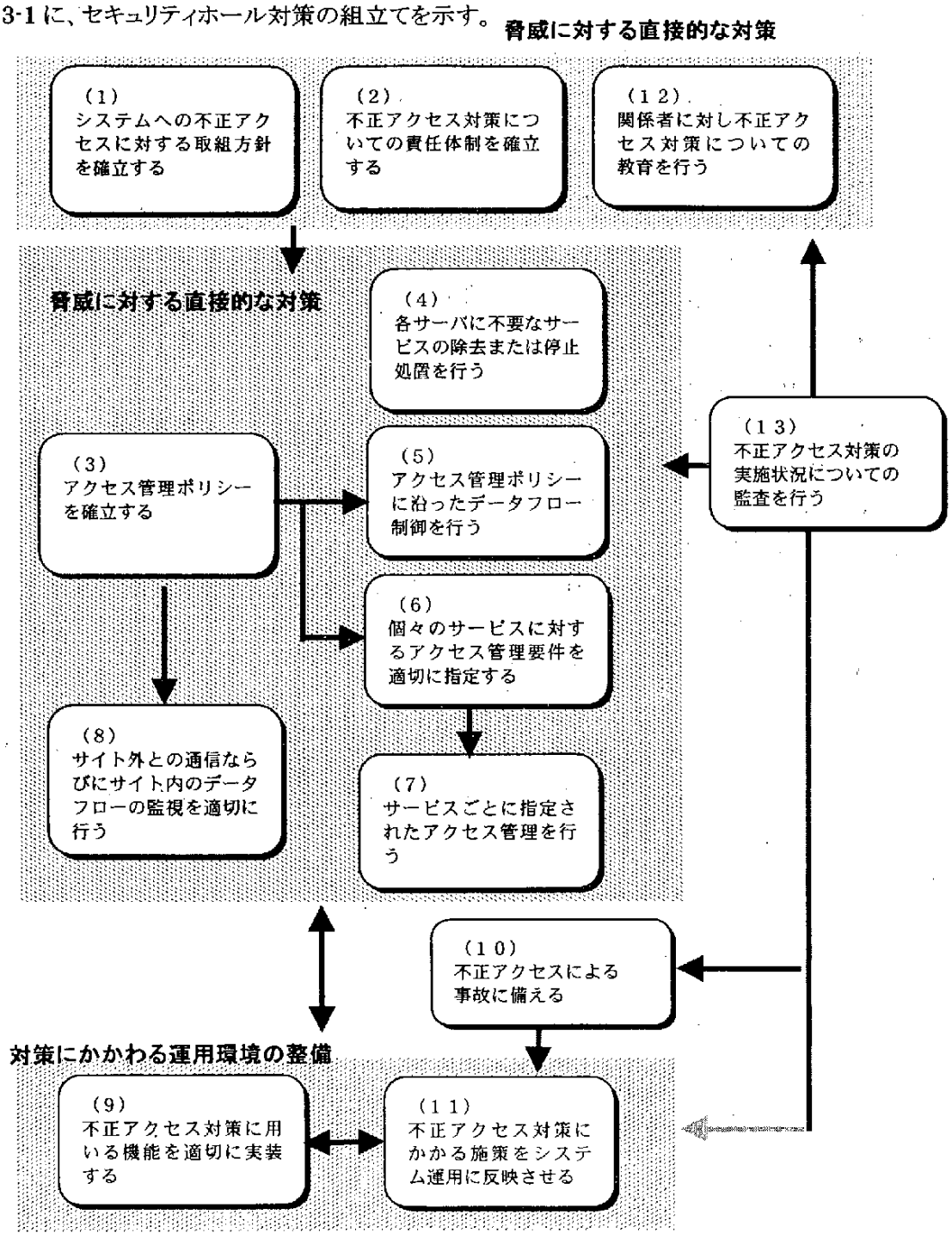


図 3-1 不正アクセス対策の組立て

また、表 3-1 に各施策における実施事項の一覧を示す。

表 3-1　不正アクセス対策としての具体的実施事項一覧

施策名	具体的実施事項
(1) システムへの不正アクセスに対する取組方針を確立する	① 不正アクセス対策の目標の明確化 ② 適用範囲の明確化 ③ 不正アクセス対策実施基準の確立 ④ 不正アクセス対策の組立ての明確化 ⑤ 不正アクセス対策についての取組方針の関係者への周知
(2) 不正アクセス対策についての責任体制を確立する	① 不正アクセス対策についての責任体制の明確化 ② 不正アクセス対策関係者間の連携体制の確立
(3) アクセス管理ポリシーを確立する	① アクセス管理についての基本方針の確立 ② サイトシステムにおけるデータフロー制御ルールの確立 ③ 求めるデータフロー制御の実現方法の確立 ④ 各サーバにおけるアクセス管理の実施原則の明確化 ⑤ アクセス監視要件の確立
(4) 各サーバに不要なサービスの除去または停止処置を行う	① 個々のサーバに必要なサービスの確認 ② 個々のサーバにおける不要サービスの除去又は停止処理の実施 ③ 不要サービス残留チェックの実施 ④ 個々のサーバにおけるサービスの搭載についてのドキュメントの整備
(5) アクセス管理ポリシーに沿ったデータフロー制御を行う	① 必要なシステム構成の構築 ② データフロー制御にかかわる機能の適切な設定と実装 ③ 使用する機能に対するパラメータ等の指定の適切な設定とその正確なインストール
(6) 個々のサービスに対するアクセス管理要件を適切に指定する	① アクセス管理実行単位ごとのアクセス管理要件の指定 ② 個々のサービスに指定したアクセス管理要件のドキュメントの整備
(7) サービスごとに指定されたアクセス管理を行う	① アクセス管理に用いる機能の的確な実装 ② アクセス管理に必要な情報の的確な登録 ③ 各サービスに対するアクセス管理の実施に関する記録の作成と保管
(8) サイト外との通信ならびにサイト内のデータフローの監視を適切に行う	① 外部ネットワークとの接点でのデータフローの監視の実施 ② サイト内におけるデータフローの監視の実施 ③ 各サーバおよび各サービスに対するアクセス監視の実施 ④ データフローの監視に必要な機能の適切な実装 ⑤ アクセスログの適切な取扱いの実施

表 3-1　不正アクセス対策としての具体的実施事項一覧

施策名	具体的実施事項
(9) 不正アクセス対策に用いる機能を適切に実装する	① 適切な技術と機能の選択 ② 組込み場所の適切な選択 ③ 選択した機能の適切なインストール ④ 必要な運用環境の整備 ⑤ 使用機能の実装についてのドキュメントの整備
(10) 不正アクセスによる事故に備える	① システムへの不正アクセスによる事故に対する対処要領の確立 ② システムへの不正アクセスによる事故への対処に必要な情報の整備 ③ システムへの不正アクセスによる事故による被害に備えたシステムの保全 ④ システムへの不正アクセスによる事故を想定した事故処理訓練の実施 ⑤ 必要なツールの整備
(11) 不正アクセス対策にかかる施策をシステム運用に反映させる	① 不正アクセス対策にかかる施策の運用規定、運用マニュアルへの反映 ② 運用環境の変更の適切な反映 ③ 不正アクセス対策にかかる定期作業のスケジュール化 ④ 運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行 ⑤ 不正アクセス対策にかかわる運用処理についての記録とその管理
(12) 関係者に対し不正アクセス対策についての教育を行う	① 関係者に対する不正アクセス対策についての教育の実施 ② 不正アクセス対策についての教育カリキュラムの確立 ③ 不正アクセス対策に関する教育テキストの整備
(13) 不正アクセス対策の実施状況についての監査を行う	① 不正アクセス対策の実施状況についての定期的な監査の実施 ② 監査実施要領の確立 ③ 監査指摘事項に対するフォローの実施

3.2 個別具体策

(1) システムへの不正アクセスに対する取組方針を確立する

【主旨】

外部からのサイトシステムに対する不正なアクセスの阻止を図るとともに、侵入を許した時の被害を限定的なものにすることに組織的に取組むには、不正アクセスへの対策を、どのような考えで、またどのような方法で実施するかを示す不正アクセスに対する取組方針を確立し、これを、不正アクセス対策に直接かかわる者だけでなく、システムの構築や運用に関係する者等、サイトにおける不正アクセス対策の実施に関係する者のすべてに周知させておくことが必要となる。

【具体的な実施事項】

(1) 不正アクセス対策の目標の明確化

不正アクセス対策が目標とするところを明確にし、不正アクセス対策に関する諸施策の意図を明確にする。不正アクセス対策の目標としては、以下があげられる。

- システムが提供するサービス(機能)の不正使用の阻止
- システムに不正にアクセスした者によるコマンド操作やプログラムの実行の阻止
- システムへの侵入を許した時の被害の極小化

(2) 適用範囲の明確化

不正アクセス対策の適用範囲として、以下を明確にする。

- サイトのシステム構成上の対象ゾーン(ネットワーク領域)および対象サーバ等の機器
- 利用者とアクセス制限の対象となるサービス(機能)、操作コマンド、プログラム、情報等の関係

(3) 不正アクセス対策実施基準の確立

不正アクセス対策の基本となるサイトにおけるシステムのサービスに対するアクセス制限やアクセス監視は、外部ネットワークとの接点だけでなく、サイト内のゾーンの境界や各サービスの入口で行われるアクセス制限やアクセス監視により行われる。

サイトの随所に組込むこれらの機能を、統制のとれたものとし、サイト全体として求めるものとするためには、アクセス管理についての考え方を中心とする、不正アクセス対策実施基準を確立しておく必要がある。

不正アクセス対策実施基準で定義すべき事項としては、以下をあげることができる。

- サービスの実装に関する原則

外部に公開するサービスは、外部からの侵入の試みに足がかりを与えることになるため、その存在だけで脅威となる。このため、外部に開放するサービスのシステムへの実装についての考え方と、その管理の方針を明らかにする。

- サイトシステムならびに各サービスへのアクセス管理の実施原則

  インターネットならびにイントラネットからのサイトシステムおよび各サービスへのアクセスには、厳格なアクセス管理が必要となる。このアクセス管理についての考え方と、その実施についての方針を明らかにする。

(4) 不正アクセス対策の組立ての明確化

不正アクセス対策をどのように行うかを明らかにするもので、実施する施策の構成とその施策間の関係を示す。

本ガイドラインにおける不正アクセス対策にかかる諸施策の組立てについては、3.1 節参照。

(5) 不正アクセス対策についての取組方針の関係者への周知

作成された不正アクセス対策についての取組方針は文書化され、不正アクセス対策に直接かかわる者の他、サイトの構築ならびに運用関係者等、不正アクセス対策に関係する者のすべてに周知させておかなければならない。このためには、

- システムへの不正アクセスに対する取組方針の配布や掲示
- 定期的な関係者間での不正アクセスに対する取組方針の再確認

も必要となる。

【対策実施上のポイント】

(1) サービスの実装に関する実施原則

サービスの実装に関する原則としては、以下のようなことがあげられる。

- 各サーバからは、業務に必要のないサービスはすべて除去または停止処理を行い、管理されていないサービスがサーバに残り、外部からアクセスできるような状態を作らない
- 各サーバにおける不要サービスの除去または停止は、別途に定める不要サービスの除去または停止要領に準じて実施する。

(2) サイトシステムへのアクセス管理の実施原則

サイトシステムへのアクセス管理の実施原則としては、以下のようなことがあげられる。

① サイトへのアクセス制限の原則

サイトへのアクセス制限は、以下の原則による。

- サイトシステムへのアクセスが許されない者の、サイトシステムへのアクセスの排除
- サイトシステムへのアクセスが許される者であっても、サイトシステムの操作コマンド等を勝手に行うことの排除
- サイトシステムへのアクセスが許される者であっても、その者が許されたサービス以外のサービスにアクセスすることの排除
- サイトシステムへのアクセスが許される者であっても、その者に許されていない情報へのアクセスまたは更新等の操作を行うことの排除

② サイトへのアクセス管理の実施方針

サイトへのアクセスに対する管理は、先にあげたサイトシステムへのアクセス制限の原則に従った、

- 各サーバにおけるサービスごとに定義されるアクセス権の設定
- 設定されたアクセス権に対応したアクセス制限の実施
- 設定されたアクセス権を前提とした不正アクセスの監視

により構成する。

アクセス権の設定とアクセス制限の実施、ならびに不正アクセスの監視は、それぞれ、別途に定めるシステムへのアクセス制限要件およびアクセス監視要件に従う。

(3) 不正アクセスに対する取組方針は、システム構成やその運用形態等、システム運用の実環境の変化に対応して必要な修正が加えられるべきであり、必要に応じて見直しを行うこと。

(4) 不正アクセスに対する取組方針は、定期的に関係者間で再確認することをルーチン化しておくことが望ましい。

(2) 不正アクセス対策についての責任体制を確立する

【主旨】

不正アクセス対策をその取組方針に沿って機能させるためには、システムへの不正アクセス対策として定められていることがシステムの構築や運用に適切に反映されるよう、指導、管理する責任体制の確立が必要となる。

このためには、不正アクセス対策にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) 不正アクセス対策についての責任体制の明確化

不正アクセス対策についての責任体制に関し、明確にしておくべきこととしては、以下があげられる。

- 不正アクセス対策の責任者とその責任
- 不正アクセス対策実施担当者の責任
- システム開発者の不正アクセス対策に関する責任
- システム管理者の不正アクセス対策に関する責任
- システム運用者の不正アクセス対策に関する責任

(2) 不正アクセス対策関係者の連携体制の確立

不正アクセス対策に関する責任体制が有効に機能するためには、関係者間の連携が重要となる。

【対策実施上のポイント】

(1) 不正アクセス対策関係者の責任分担表 3-2 に、不正アクセス対策関係者の責任区分の定義例を示す。

(2) 不正アクセス対策にかかる責任体制は、不正アクセス対策を変更したり、サイトの運営環境に変更が生じた場合は、見直しを行い、必要な変更を行うこと。

表 3-2　不正アクセス対策関係者の責任分担

責任区分	タスク
不正アクセス対策の責任者	・不正アクセスに対する取組方針の確立と関係者への周知 ・不正アクセス対策実施基準の発行 ・不正アクセス対策全体の妥当性の維持 ・不正アクセス対策の実施状態のチェック ・対策実施基準に沿った不正アクセス対策の実施の指導 システムへの侵入事故発生時における事故処理の指揮
不正アクセス対策実施担当者	・不正アクセス対策の詳細の検討 ・不要サービスの除去または停止処理の実施 ・外部へのネットワークサービスの提供状況の管理 ・システムへのアクセス制限ルールの詳細の決定 ・システムへのアクセス制限機能の適切な実装と必要な環境整備 ・システムへのアクセス制限に用いる情報の設定管理 ・システムへのアクセス制限に用いる情報のシステムへの的確な設定 ・システムに対するアクセス監視の詳細の決定 ・システムに対するアクセス監視機能の適切な実装と必要な環境整備 ・システムに対するアクセス監視に用いる情報の設定管理 ・システムに対するアクセス監視に用いる情報のシステムへの的確な設定 ・システムに対するアクセス監視ログの分析等、侵入監視結果のチェック ・システムへの侵入事故発生時における事故処理と再発防止策の検討
システム開発者	・開発システムにおける関係機能の適切な組込み －設計の妥当性の確認 －正確な実装の確認
システム管理者	・システムにおけるサービスの制限および、アクセス制限、アクセス監視機能の維持 －必要なシステム構成の変更の反映の管理 －アクセス制限、アクセス監視機能の動作環境の維持管理 ・システムにおける対応技術や機能の実装状況の正確な把握
システム運用者	・アクセス制限、アクセス監視に用いる情報のシステムへの的確な設定等、対応機能が必要とするシステム運用環境の整備 ・アクセス監視結果の分析

(3) アクセス管理ポリシーを確立する

【主旨】

不正アクセス対策の中心となるアクセス管理を適切に行うためには、どのような考えの下で、サイトシステムのどこで、どのようなアクセス管理を行うのかを明確にしたアクセス管理ポリシーが確立していなければならない。

アクセス管理ポリシーは、以下で構成される。

- アクセス管理の基本方針
- サイト内におけるデータフロー制御ルール
- データフロー制御の実現方式
- 各サーバにおけるアクセス管理の実施原則
- アクセス監視の実現方式

このアクセス管理ポリシーは、サイトの運営実態とサイト全体に対するセキュリティポリシーを反映したものでなければならない。

(注) ここでいうデータフローとは、サービスへのアクセス、サービスにかかわるコマンドやデータの授受等のサーバ間における通信を指す。

【具体的な実施事項】

(1) アクセス管理についての基本方針の確立

アクセス管理をどのような考えで行うのかを示すもので、以下のようなことを明確にする。

- データフロー制御と各サーバにおけるアクセス制限の分担と連携
- 求めるアクセス監視のレベル

(2) サイトシステムにおけるデータフロー制御ルールの確立

サイトシステムにおけるデータフロー制御が適切に行われるためには、サイトシステム内におけるデータフロー制御ルールの定義として、以下にあげることが適切に決められていなくてはならない。

- ゾーン分割と各ゾーンに許されるデータフロー
- 各ゾーンに配置するサーバと各サーバに搭載するサービス
- 各サーバが前提とするデータフロー

システムの構成やサイトの運営方法等に、このデータフロー制御ルールに影響を与えるような変更が生じた場合は、その見直しを行い、必要な変更を行わなければならない。

(3) 求めるデータフロー制御の実現方式の確立

前項で設定したサイトシステム内におけるデータフロー制御ルールを実現するためには、データフロー制御にかかわるファイアウォール等使用する機能の配置や役割分担が適切に決められていなくてはならない。

(4) 各サーバにおけるアクセス管理の実施原則の明確化

各サーバにおいては、どのようなアクセス管理を行うべきかについて、以下のようなことを明確にする。

- 外部公開サービスを除いた全てのサービスや管理機能に対するアクセス制限の実施
- サーバ単位で行うアクセス管理

(5) アクセス監視要件の確立

不正アクセスの監視をどのように行うのかを示すもので、以下のようなことを明確にする。

- 外部からのアクセスに対する監視に用いる機能とその配置
- サイト内のデータフロー監視に用いる機能とその配置
- 監視対象イベントの定義等各サーバにおけるアクセス監視の内容

【対策実施上のポイント】

(1) データフロー制御と各サーバにおけるアクセス制限の分担と連携

ファイアウォール等でサイト内のデータフロー制御が行われ、サーバに対するアクセスが制限されていたとしても、各サーバの各サービスにおいても、以下に示すアクセス管理を行わなければならない。

- サービス単位でのアクセス制限の実施
- サービス単位のアクセス制限の実施状況の確認
- サービス単位でのアプリケーションレベルのアクセス制限の実施

(2) 求めるアクセス監視レベルの定義について

システムに対する不正アクセスの監視を有効に行うためには、システムのどこで、どのような方法で、何を監視するかといった、サイトにおけるデータフローに対する監視要件が確立していなければならない。サイトにおけるデータフローの監視要件として定義すべき事項としては、以下があげられる。

- 外部からのサイトへのアクセスおよびサイト内のデータフローの監視についての基本方針
- 監視対象となるイベントと監視ポイント
- 監視手段
- 取得ログの保管方法
- 取得ログの分析サイクル、手順等の監視の運用
- 不正アクセスまたは不正アクセスの試みを検知した場合の処理要領

このデータフロー監視要件は、サイトにおけるアクセス管理方法の変更が、適宜反映されたものでなければならない。

(3) データフロー制御ルールの定義要領

表 3-3 に、データフロー制御ルールの定義で指定すべき事項を示す。

表 3-3　データフロー制御ルール定義における指定事項

項番	定義項目	定義の内容
1	ゾーン分割と各ゾーンに許されるデータフロー	・サイトのゾーン構成と各ゾーンの定義 ・ゾーン間のデータフローの制約 ・ゾーン内のデータフローの制約
2	各ゾーンに配置する機器とサービス	・各ゾーンに配置するサーバ ・各サーバに搭載するサービス
3	各サーバが前提とするデータフロー	・当該サーバにデータやコマンドを転送できるサーバとその条件 ・当該サーバからデータやコマンドを転送できるサーバとその条件 ・受取ったデータの転送に関するルール

(4) アクセス監視要件の定義要領

表 3-4 に、アクセス監視要件定義で指定すべき事項を示す。

表 3-4　アクセス監視要件定義における指定事項

項番	項目	内容
1	アクセス監視についての基本方針	・監視の狙い(どのような問題の抑止を目標にするのか) ・実施のレベル(監視の密度)
2	監視対象となるイベントと監視のポイント	・取得、監視対象ログとそのレベル ・ログの取得に使用するツールとその機能 ・監視のポイント
3	監視の実施方法	・取得ログの分析方法と使用するツール ・IDS(侵入検知システム)を用いる場合、その使用方法 ・データ分析サイクル、分析評価手順等の監視の運用
4	取得ログの保管、管理	・ログの 2 重化の適用 ・保全措置としての他の媒体へのコピー
5	異常検知時の処理手順	・侵入の形跡または侵入の試みの形跡を検知した場合の処理手順

【参考】

データフロー制御ルールの例

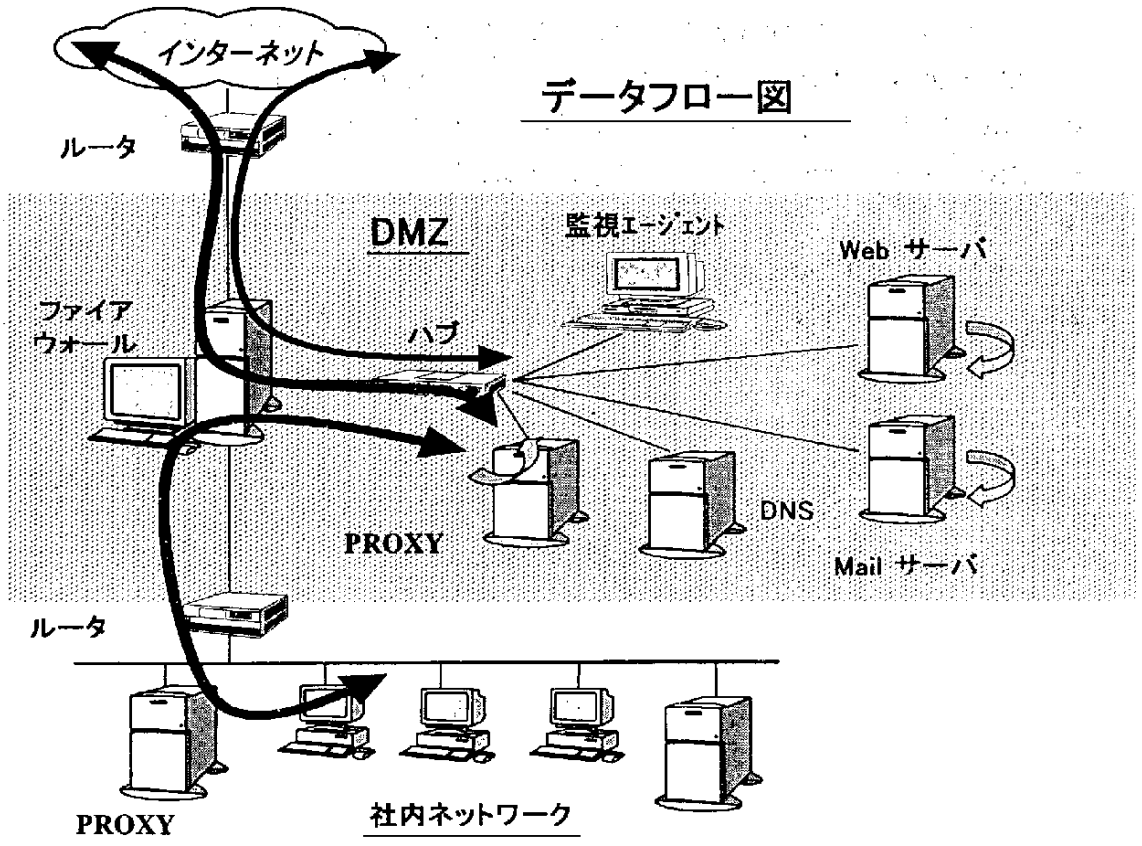


図 3-2 に、一般的なサイトの構成におけるデータフロー制御ルールの例を以下に示す。

図 3-2 データフロー制御ルールのイメージ

① サイトのゾーンは、次の三つに分類される。

- インターネットゾーン
- DMZ (Demilitalized Zone： 非武装ゾーン)
- イントラネットゾーン (企業内ネットワーク)

② 各ゾーンに配置する機器とサービス

ルータ: ネットワークとネットワークの間に設置し、適切にデータの伝送経路を決定

ファイアウォール: 内部と外部のコンピュータ間で安全な通信を各種アクセス制御機能で実現

プロキシー: ネットワークの内部から外部のサーバにアクセスする時のデータ中継の実施

DNS (Domain Name Service): 通信相手を名前で指定すると IP アドレスに変換

Web サーバ: インターネットで情報を受発信するサーバ

(IIS (WindowsNT) やApache (Linux) などで構築)

Mail サーバ: 電子メール用のサーバ (POP3 や IMAP4 のプロトコルがある)

監視エージェント: リモート監視用の機器

③ 各サーバが前提とするデータフロー

- インターネットからのアクセスはルータからファイアウォールへの経路のみ許可
- ファイアウォールでは外部から可能なアクセス(例えばメール SMTP、Web の HTTP および SSL/SHTTP 等)の設定、ログ取得、リアルタイム監視等を実施
- PROXY サーバは、イントラネットからの外部アクセス時に内部アドレスを変換
- DNS サーバに対するゾーン転送の禁止等の設定
- Web サーバに対する一般利用者によるファイルの更新・削除の禁止、パスワードファイル、ロギングファイル等のシステム関連ファイルへの操作禁止
- Mail サーバでの SPAM メール中継禁止、コンピュータウイルス診断ソフトでの自動チェック

(4) 各サーバに不要なサービスの除去または停止処置を行う

【主旨】

外部の利用者が利用できるサービスは、適切なアクセス制限がなされていないと、攻撃者にシステムへの不正アクセスの足掛かりを与える。

システムをデフォルト設定で構築すると、ベンダーが設定したいろいろなサービスがそのまま動作することになる。このようなサービスや、使われなくなったサービスやテスト用のサービス等、業務やシステムの運用管理で用いられないサービスについては、システム管理者や運用者が管理の対象としていないところから、アクセス管理の対象外におかれるため、まず無防備になっていると考えなければならない。

このため、これらの業務やシステム運用に不要なサービスについては、除去するか停止状態にして、サイトシステムに不正アクセスを試みる者に、成功の足掛かりを与えないようにしなければならない。

【具体的な実施事項】

(1) 個々のサーバに必要なサービスの確認

各サーバに不要なサービスを残さないためには、個々のサーバに必要となるサービスの特定が必要となる。各サーバが必要とするサービスについては、その使用の必然性についての説明を必要とする。

また、使用するサービスについては、その個々にアクセス管理要件の指定が必要となる。個々のサービスに対するアクセス管理要件については、**"(6)個々のサービスに対するアクセス管理要件を適切に設定する"**参照。

(2) 個々のサーバにおける不要サービスの除去または停止処置の実施

個々のサーバごとに、必要と指定されたサービス以外のサービスのすべてについて、除去または停止処置を行う。

除去または停止指定の処理については、それが確実に行われたかどうかの点検が、厳密に行わなければならない。

(3) 不要サービス残留チェックの実施

個々のサーバに対する、不要なサービスが稼動状態になっていないかどうかのチェックを、定期的およびシステム環境変更時に実施する。

(4) 個々のサーバにおけるサービスの搭載についてのドキュメントの整備

個々のサーバにおけるサービスの搭載が適切に行われているかどうかについての管理が適切に行えるように、個々のサーバに搭載されているサービスについて、稼動中または停止扱いといった状態についてのドキュメントの整備を行い、何時でも正確に把握できるようにしておくことも必要である。

また、このドキュメントは、システムの構成や運用方法の変更に伴う搭載サービスの変更が適切に反映されるようになっていなければならない。

【対策実施上のポイント】

(1) サーバから不要なサービスの除去または停止について

- 未使用または使用しないサービスやスクリプトや内容が不明なサービスやスクリプトは、削除または停止する。この時、以下に留意すること。
  - 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は、その全てに対し、要否の判定を厳格に行う
- 以下のサービスについては、特別なサーバを除いては、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が必要となる。
  - telnet
  - ftp
- 外部公開用 Web サーバにおける以下に示すような不要なプログラムは、除去するか停止状態にすること。
  - 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 ASP
  - 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、文字入力をさせる場合、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も必要である。

(2) 不要サービスの除去や停止についての定期的な確認の実施

以下のような方法により、各サーバにおいて不要なサービスの除去や停止処理に不備がないかどうかについての確認を、システム環境の変更時はもちろん定期的にも行うこと。

- システムコマンドや監査ツールを用いた稼動サービスのチェック
- システムへの侵入事例、セキュリティホールやウイルス関係情報等、セキュリティに関する情報を下にした、特定サービスの状態の確認

(3) 各サーバにおけるサービスの稼動状態の管理に関するドキュメント例

表 3-5 に、各サーバにおけるサービスの稼動状態の管理に関するドキュメントの様式例を示す。

表 3-5　サービスの稼動状態管理表の例

サービス名	状態	管理の重要度	使用上の留意事項
1. 外部からTCPコネクションを許すサービス		(注)	
(1)HTTP	□削除□停止□実行		
(2)HTTPS	□削除□停止□実行		
(3)DNS	□削除□停止□実行		
・・・・・・	□削除□停止□実行		
2. ネットワークサービス			
(1)telnet	□削除□停止□実行		
(2)ftp	□削除□停止□実行		
(3)finger	□削除□停止□実行		
・・・・・・	□削除□停止□実行		
3. 起動するプロセスの制限			
(1)システムのセットアップ	□削除□停止□実行		
(2)nfsサーバ停止	□削除□停止□実行		
・・・・・・	□削除□停止□実行		

(注)管理の重要度は、最重要、重要、注意、必要なしで区分する。

(5) アクセス管理ポリシーに沿ったデータフロー制御を行う

【主旨】

適切なシステム構成の構築、データフロー制御に用いる機能の適切な組込み、必要な環境の整備等により、アクセス管理ポリシーで定められたデータフローの制御を実現する。

【具体的な実施事項】

(1) 必要なシステム構成の構築

前項で設定したサイトシステム内におけるデータフロー制御ルールに沿ったデータフローの制御を実現するためには、サイトシステムの構成において、

- ゾーン分割を行う機器の配置
- データフロー制御にかかわる機器のデータフロー制御にかかる役割分担

が適切でなければならない。

(2) データフロー制御にかかわる機能の適切な設定と実装

ルータ、ファイアウォール、プロキシ等、サイトにおけるデータフローの制御にかかわる機器における機能の選択は、それぞれの役割に沿って適切に行われていなければならない。

また、これらの機能は指定通りにシステムに組込まれていなければならない。

(3) 使用する機能に対するパラメータ等の指定の適切な設定とその正確なインストール

データフローの制御機能が動作上使用するパラメータ等の設定、ならびそのシステムへのインストールは正確でなければならない。

このことを実現するためには、

- パラメータ等の諸設定のレビューの徹底
- インストールの内容の確認の徹底

が必要となる。

また、これらは、システム構成の変更やサイトの運営方法の変更等が反映されるようになっていなければばならない。このため、システム構成の変更やサイトの運営方法の変更手続きに中に、サイトのデータフロー制御の見直しを組込んでおくことも必要である。

【対策実施上のポイント】

(1) サイトのネットワーク構成の設計について

サイトのネットワーク構成の考え方については、"10 章 セキュアなシステムの構築"参照。

(2) 用いる機能の的確な実装について

サイトシステムにおけるデータフロー制御に用いるルータやファイアウォールの実装の管理については、"(9) 不正アクセス対策に用いる機能を適切に実装する"参照。

(3) ルータやファイアウォールの使用について

ルータやファイアウォールの使用にあたっての考え方については、**“10章 セキュアなシステムの構築”**参照。

(6) 個々のサービスに対するアクセス管理要件を適切に指定する

【主旨】

不正アクセス対策を適切に行うためには、アクセス制限やアクセス監視等のアクセス管理の実行単位としての個々のサーバにおけるサービスごとに、これらをどのような条件の下にどのように行うのかが、適切に決められていなくてはならない。

【具体的な実施事項】

(1) アクセス管理実行単位ごとのアクセス管理要件の設定

システムの管理機能やアプリケーション等、アクセス管理の実行単位となるサービスごとに、これらをどのように行うのかについて、以下に示すようなことを指定する。

- 対象サーバ
- 対象サービス
- 当該サービスに対するアクセス管理についての基本要件
- アクセス権限者とアクセス権
- アクセス権限者の認証要件
- アクセス監視要件
- アクセス権限者とアクセス権の登録手続き

この要件の設定は、サーバ単位に行わなければならない。

また、システムの構成やサイトの運営体制や運営方法等に、個々のサービスに対するアクセス管理要件の設定に影響を与えるような変更が生じた場合は、その見直しを行い、必要な変更を行わなければならない。

(2) 個々のサービスに指定したアクセス管理要件についてのドキュメントの整備

個々のサービスに対するアクセス管理が適切に行われているかどうかについて、管理が適切に行えるように、個々のサービスごとに定めたアクセス管理要件についてのドキュメントの整備を行い、何時でもその内容が正確に把握できるようにしておくことも必要である。

このドキュメントで明らかにしておくべき事項は、アクセス管理の実行単位に対する、(1)項であげた項目となる。

また、このドキュメントは、システムの構成やサイトの運営体制や運営方法の変更に伴う管理要件の変更が適切に反映されるるようになっていなければならない。

【対策実施上のポイント】

(1) 個々のサービスに対するアクセス管理要件の定義要領

表 3-6 に個々のサービスに対するアクセス管理要件定義で指定すべき事項を示す。

表 3-6　個々のサービスに対するアクセス管理要件の定義における指定項目

項番	定義項目	定義の内容
1	対象サーバ	・サービスが搭載されているサーバ名
2	対象サービス(注1)	・アクセス管理の対象となるサービス名称 ・当該サービスの機能概要
3	当該サービスに対する アクセス管理についての 基本要件	・当該サービスのアクセス権限者の範囲(注2) ・アクセス権限者に対するアクセス権の制限(注3) ・アクセス権限者とアクセス権の見直しが必要な場合 ・求める認証レベル(注4) ・アクセス監視の要否
4	アクセス権限者とアクセス権	・アクセス権限者のリスト ・各アクセス権限者がアクセスできる当該サービスにおける機能の指定
5	アクセス権限者の認証要件	・当該サービスのアクセス権限者の認証方法 ・認証用情報のメンテナンス要件 等 (認証要件については、**第 9 章"ユーザ認証の適切な適用"**における認証要件定義による)
6	アクセス監視要件	・アクセス監視の対象 ・当該サービスに対するアクセス監視に用いる技術 ・アクセス監視結果の取扱い
7	アクセス権限者とアクセス権の指定手続き	・アクセス権限者とアクセス権の管理責任者 ・アクセス権とアクセス権の設定、承認、指定の確認手順

(注1)ここでいうサービスとは、システムの持つ機能を指し、以下のように分類することができる。
－OS のシステム管理機能
－各サービスにおける運用管理機能
－外部利用者からアクセスできるネットワークサービス
－外部利用者には隠蔽されている内部処理用アプリケーション
(注2)アクセス権限者の範囲としては、以下のようなものがある。
－システム管理者(ルート管理者、ドメイン管理者)
－運用管理者、運用担当者
－業務管理者、業務担当者
－特定外部利用者(会員登録した特定サービス利用者)
－一般外部利用者
(注3)一つのサービスが多くの機能を提供している場合、アクセス権限者すべてが、全ての機能にアクセスできるとは限らない。
(注4)認証の厳格さについての要求の指定。詳細は第 9 章 "ユーザ認証の適切な適用"参照

(2) システム管理者や運用管理者向けサービスに対するアクセス管理について

システムファイル等へのアクセス、システム管理者や運用管理者向けのサービスについては、特に厳重なアクセス管理が必要である。これらのサービスに対するアクセス管理要件の設定にあたっては、以下に留意する。

- 機能単位の木目細かいアクセス管理の設定
- 認証の強化(例えば、スマートカードやバイオメトリクス認証等も考慮する)
- 常時使用しないサービスの使用時におけるインストールと使用後の除去の励行
- リモートメンテナンス用等のダイアルアップ接続の排除

(7) サービスごとに指定されたアクセス管理を行う

【主旨】

すべてのサービスに対し、当該サービスに定義されているアクセス管理要件に従ったアクセス管理を行う。

各サービスに対するアクセス管理が適切に行なわれるためには、アクセス管理要件に指定されたアクセス権限者情報や、それぞれのアクセス権限者に付与されたアクセス権に関する情報、アクセス権限者の認証情報のシステムへの登録を的確に行うこと、およびアクセス制限に用いる機能の確認が必要となる。

【具体的な実施事項】

(1) アクセス管理に用いる機能の的確な実装

システムに改めてアクセス管理を行う機能の組込みが必要な場合は、必要な機能の的確な実装が必要となる。実装の管理については、"(9)不正アクセス対策に用いる機能を適切に実装する"を参照。

(2) アクセス管理に必要な情報の的確な登録

アクセス管理を行う機能が必要とするアクセス管理に関する情報を、当該サービスに対して定義されているアクセス管理要件に従って、正確にシステムに登録する。

アクセス管理に関する情報としては、以下があげられる。

- アクセス権限者
- アクセス権限者ごとの当該サービスに対するアクセス権(利用できる機能の範囲)
- アクセス権限者の認証情報
- 監視対象イベントに関する情報

なお、この登録は、システムの構成変更や運営体制や運営方法の変更等に伴うアクセス制限要件の変更が、その都度正確に反映されなければならない。

(3) 各サービスに対するアクセス制限の実施に関する記録の作成と保管

システムにおけるアクセス制限の管理のため、アクセス管理の実行にかかるシステムの運用処理については、記録を行い保管すること。

【対策実施上のポイント】

(1) アクセス管理の実施にかかるシステム運用処理の記録について

その実行について記録を取り保管すべきサービスに対するアクセス管理の実行にかかるシステムの運用処理としては、以下をあげることができる。

- アクセス制限にかかる機能の新規導入およびその変更
- アクセス制限にかかる情報の変更

(8) サイト外との通信ならびにサイト内のデータフローの監視を適切に行う

【主旨】

システムへの不正アクセスの阻止に、万全はありえず、不正アクセスを許してしまうことも考えられる。このような場合、不正アクセスを許したことを早期に発見し、被害が大きくならないうちに、必要な対策を実施できるようにしておかなければならない。

また、侵入の成否を問わず、システムへの侵入が試みについては、その状況を把握しておくことは、システムへの不正アクセス対策をより強化するためにも必要なことである。

このため、システムへの侵入または侵入の試みを監視し、侵入の証拠の確保や侵入の再発防止策の検討資料収得のための、外部からデータやサイト内のネットワークに流れるデータについてのログの収集とその解析は、システムへの不正アクセス対策の一環として重要である。

ログの収集対象、保存方法、解析方法は、サイトにおけるデータフロー監視についての考え方に依存し、サイトごとに異なる。適切なログの運用管理が行われるためには、ショップの運用形態、取引内容やタイプを勘案し、自サイトおいて適用するログの運用管理を確立しておく必要がある。

【具体的な実施事項】

(1) 外部ネットワークとの接点でのデータフローに対する監視の実施

データフロー制御ルールに従って、ルータまたは外部に向けたファイアウォール等で、サイトと外部との通信についての監視を行う。

この実施にあたっては、

- 監視対象イベントの設定
- 監視機能の適切な実装
- 取得ログの分析や管理
- 問題事象に対する処置

等が、別途に定めるところに従って、適切に行わなければならない。

(2) サイト内におけるデータフローの監視の実施

データフロー制御ルールに従って、ファイアウォール等を用いて、ゾーンの境界やゾーン内で更新される通信についての監視を行う。

この実施にあたっては、

- 監視対象イベントの設定
- 監視機能の適切な実装
- 取得ログの分析や管理
- 問題事象に対する処置

等が、別途に定めるところに従って、適切に行わなければならない。

(3) 各サーバおよび各サービスに対するアクセスの監視の実施

データフロー制御ルールに従って、各サーバおよびサービスの個々に対するアクセスについ

ての監視を行う。

この実施にあたっては、

- 監視対象イベントの設定
- 監視機能の適切な実装
- 取得ログの分析や管理
- 問題事象に対する処置

等が、別途に定めるところに従って、適切に行わなければならない。

(4) データフローの監視に必要な機能の適切な実装

データフローの監視に用いる機能については、以下が適切に行われていなければならない。

- データフローを監視するツールの決定
- 使用ツールの機能の設定
- ログの記録と可視化機能の設定

(5) アクセスログの適切な取扱いの実施

取得したログは監視要件に従い、所定の場所で所定の期間、保管されなければならない。

また、取得したログに対しては、基準に従い分析を行い、侵入や侵入の試みの有無についての確認を行わなければならない。

【対策実施上のポイント】

(1) 可能な範囲で、自動的にアクセスログを分析し、不正アクセスの警告情報を発することができるようにしておくことが望ましい。

(2) 実際に取得するログの例

ログに記録すべき情報としては、以下のようなものがあげられる。

- システムの起動、終了時刻
- サービスプログラムの起動終了時刻
- ユーザ(正規、非正規)のログインユーザー認証の成否時刻、ログイン名、アクセス元
- サービス要求ごとの成功/失敗時刻、サービス内容、アクセス元
- 詳細なシステム利用履歴
- システム内の重要ファイルの変更履歴

(3) ログ保全方法例

ログの保全方法としては、以下のようなものがあげられる。

- ログファイルを保存しているファイル、ディレクトリへのアクセス許可を必要最低限にする
- ログをテープ、光ディスクといったリモートアクセスできない媒体に格納する
- ログを追記不可能なメディアに保存する
- ハッシュ関数(MD5)等を用いたログの改ざん検出

(4) ログの解析方法を、CERT 等の専門機関に委託することも検討の対象である。

(5) ログ保存媒体は、記録データに安全で施錠可能な場所や監視可能な場所に保管することが望ましい。

【参考】

(1) 外部サービスの利用によるアクセス監視について

サイトの監視は 24 時間 365 日の監視が必要であり、要員体制の確保が困難になるケースも多い。最近では、ネットワーク監視センターを持ち専門家による監視サービスを提供しているセキュリティサービスベンダーもあるので、これを利用することも可能である。

監視サービスにおけるサービスメニュとしては、以下のようなものがある。

- 24 時間 365 日の監視
- 監視レポートの作成
- 侵入兆候の発見、通知
- リモート／オンサイトによるアタック撃退

(9) 不正アクセス対策に用いる機能を適切に実装する

【主旨】

システムへの不正アクセス対策に用いる機能としては、

- データフロー制御機能
- アクセス制限に用いる機能
- アクセス管理の脆弱性の検査に用いる機能
- アクセス監視に用いる機能

等があり、その実現方法としては、

- 専用機器の使用
- OSの機能や、データベース管理の機能や、アプリケーションに組込まれた汎用機能の使用
- 独自の仕様による実現

を選択することができるが、いずれの場合においても、期待通りに機能し、使用目的を満足するものでなければならない。

このためには、適切な技術の選択と選択した技術における使用機能の選択、インストール時の設定等を的確に行うとともに、そのインストールに対する検査も十分に行うことが必要となる。

また、データフロー制御のためのパラメータやアクセス制限やアクセス監視の実行に必要な権限情報や利用者の認証情報等、使用する技術が前提とする運用環境の整備に不備がないようにしなければならない。

本節の、**"(5)アクセス管理ポリシーの沿ったデータフロー制御を行う"**、**"(7)サービスごとに指定されたアクセス管理を行う"**、および**"(8)サイト外との通信ならびにサイト内のデータフローの監視を適切に行う"**においても、必要とする機能の適切な実装を求めている。ここでは、システムへの不正アクセス対策全体の立場から、関連機能の実装管理の徹底を求めたものである。

【具体的な実施事項】

適用する技術の個々に対し、以下のことが求められる。

(1) 適切な技術と機能の選択

システムへの不正アクセス対策のためにシステムに組込む機能は、以下を満足していなければならない。

- 使用する技術(製品や方式)は、アクセス制限やアクセス監視を行う個々の場面ごとに設定されているアクセス制限やアクセス監視についての要件を満足するものでなければならない。
- 一般に機器やソフトウェアにはさまざまな機能が準備されており、同じ技術でもその使い方次第で機能も異なってくる。使用する技術そのものは妥当であっても、その機能設定が、対応する管理要件に対して不適切であってはならない。

(2) 組込み場所の適切な選択

選択した技術を期待通りに機能させるためには、選択した技術のシステム構成上の配置を適切なものにしなければならない。使用する技術のシステム構成上での組込み位置は、以下により決められる。

- システム構成上の適用範囲等、不正アクセス対策における当該技術の役割
- 当該技術の機能特性および前提とする環境条件

(3) 選択した機能の適切なインストール

選択した技術を期待通りに機能させるためには、技術のシステムへのインストールが適切に行われていなければならない。このためには、以下のことが求められる。

- 選択機能の的確な組込み
- テストによる動作確認の実行

  システムへのインストールが終了したら、十分な機能検査を必ず実施し、インストールにミスがないことを確認すること。

(4) 必要な運用環境の整備

システムの構成管理やシステムの運用において、OS やネットワークの環境設定、アクセス権限テーブルや認証情報の整備等、適用した技術が前提とする環境整備に不備がないようにしなければならない。

これには、システムの導入時だけでなく、定期的な更新といったその維持管理についての処理も必要となる。

(5) 使用機能の実装についてのドキュメントの整備

使用機能の実装については、いつでもその設定仕様や実装状況の把握ができるようドキュメント化されていなければならない。

また、このドキュメントは、機能の新規導入時に作成するだけでなく、実装についての変更が行われたときも、適切にメンテナンスされるようになっていなければならない。

【対策実施上のポイント】

(1) 採用した技術における機能の選択にあたっては、十分な検討を行うこと。使用する技術のデフォルト機能を安易に用いないこと。

(2) 独自仕様の技術を用いる場合、当該機能またはシステムの設計と実装に対し、ISO15408 に準拠した、機能の評価および実装の検査を行うことが望ましい。

(3) 使用技術の実装状況についてのドキュメント化すべき事項としては、以下のようなものがある。

- システム構成上の組込み場所
- 設定機能等の各種の指定内容
- 運用上の留意点
- 実装確認テストの内容と結果
- 新規組込みまたはメンテナンス日時

（10）不正アクセスによる事故に備える

【主旨】

サービス制限やアクセス制限等のシステムへの不正アクセス対策を綿密に計画していても、設定のミスや運用の手違いといった対策実施上の不備から、システムへの不正アクセスを許してしまう危険性は残る。

システムへの不正アクセスを許した場合、

- 被害状況の把握
- 改ざんまたは破壊されたシステムやデータの復旧

が適切に行われなければならない。

影響範囲を見逃して、復旧が完全でなかったり、二次被害に対する対応が不十分であったりすると、被害の拡大を招くことになる。また、システムへの不正アクセスがあったことについての関係機関への届出も、漏れないようににしなければならない。

システムへの不正アクセスによる事故が発生した場合における必要な処置が、適切かつ迅速に行われるようにするためには、システムへの不正アクセスを許した時の対処要領を確立しておくとともに、常日頃から、事故処理に必要となる情報やツールの整備を行っておかねばならない。

【具体的な実施事項】

(1) システムへの不正アクセスによる事故に対する対処要領の確立

システムへの不正アクセスによる事故発生時における必要な処置を円滑に行えるようにするためには、事故時の対処要領を確立しておくことが必要である。

システムへの不正アクセスに対する対処要領として明確にしておくべき事項としては、以下があげられる。

- 対策チームの編成
- サービスの停止の検討と実施
- 関係者へのシステムへの侵入を許したことの告知
- 侵入により実行された不正な処理の内容の把握
- 影響範囲の特定
- 改ざん、破壊されたソフト資産、情報資産の復旧
- 二次被害の調査と対策の検討、実施
- 原因の分析と再発防止策の検討とその実施
- 処理経緯の記録と保管
- 関係機関への報告

(2) システムへの不正アクセスによる事故への対処に必要な情報の整備

システムの構成情報や、日常の運用状況に関する情報等、システムへの不正アクセスによる

事故に対する処理に必要な情報は、適切に記録、保管されていなければならない。

(3) システムへの不正アクセスによる事故による被害に備えたシステムの保全

システムへの不正アクセスによる事故による被害が発生した場合、被害から迅速にシステムや情報の復旧を実現するためには、必要なソフト資産および情報資産のバックアップが必要となる。システムや情報の復旧に必要となるバックアップの取得とその管理を適切に行うためには、このような事故による被害を想定した保全要領を確立しておくことが必要となる。

システムへの不正アクセスによる被害に備えたシステムの保全要領の中で明確にすべき事項としては、以下があげられる。

- バックアップを取得する対象情報
- バックアップ取得サイクル
- バックアップデータからの復旧手順
- バックアップデータの管理手順（保管場所、持出手順、保管期限、保管期限等）
- 保全基準の実行に必要な機能
- 復旧訓練の実施基準

(4) システムへの不正アクセスによる被害を想定した事故処理訓練の実施

バックアップデータが保管されていても、復旧機能の実装の不備、運用環境の変化、処理手順への不慣れからくる操作の不手際等から、必要な時に復旧がうまくできないといった事態が起こりうる。

このため、さまざまな形態の不正アクセスによる被害を想定した事故処理訓練を、定期的に行うことが望ましい。

また、運用訓練で事故処理の手順、システムの保全、バックアップの取得、システムの機能、対応運用規定、運用マニュアル等の不備が発見された場合には、遅滞なく改善を行わなければならない。

(5) 必要なツールの整備

バックアップの取得に用いるツールや、システムへの侵入事故発生時における被害範囲の調査や、破壊されたシステムや情報の復旧等の事故処理に用いるツールは、期待通り機能しなければならない。

このためには、

- 適切なツールの選択とその適切なシステムへの組込み
- 運用環境の変更への対応
- ツール使用上のマニュアルの整備

等に不備がないようにしておかなければならない。

【対策実施上のポイント】

(1) システムへの侵入を把握する方法

システムへの侵入を把握する方法としては、以下のようなものがある。

- システム利用履歴の解析
- ファイル改ざん検出
- 最新のバックアップとの比較によるファイル改ざん検出

(2) システムへの侵入の影響調査のポイント

- システムへの侵入の形跡を発見した場合には、まず、システム上の情報の改ざん、偽造の有無を確認する。(ただし、侵入者がトラップを仕掛けている場合があるので、各種コマンドの使用には十分な注意が必要である。)
- 各種ログを調査し、侵入者による影響範囲(対象サーバ、対象ファイル等)を調査する。

(3) システムへの不正アクセスへの対処に必要な情報

システムへの不正アクセスを許した時の処理に必要な情報としては、以下のようなものがあげられる。

- システム構成を示す情報
- システムにおける情報資産の格納状況を示す情報
- システム構成の変更履歴を示す情報
- システムにおける情報資産の更新履歴を示す情報
- 実施しているシステムへのアクセス制限に関する外部情報

これらは、いずれも運用規定に準じて記録、保管されていなければならない。

(4) システムへの侵入を許した原因調査と復旧の手順

- システムへ侵入された場合、各種ログから侵入ルートおよび手口を調査し特定する。これには、専門知識が必要とされることが多く、JPCERT／CC の指導や、専門の業者へ委託するなどが必要になる場合もある。特に、攻撃者の特定にあたっては、アクセスしてきたIPアドレスが必ずしも攻撃者のものとは限らない場合が多く、注意が必要。
- 何も対策せずにサービスを再開することは決してしてはならない。対策の実施に、時間とコストが必要になる場合は応急処置をしてサービスを再開することも考えられるが、このような場合でも、これまで以上に監視を強化する必要がある。
- 再発防止策をとった後、必要に応じてバックアップデータなどからシステム復旧を行う。

(5) システムへの侵入事故への対処におけるその他の留意事項

- システムを緊急に停止する場合でも、メモリイメージを保存するなど、可能な限りシステムの情報を保持できるような起動(UNIX ではシングルユーザモードでの起動)で再起動した後に、分析作業に入ると良い。これは、その後の事後対応の原因解明において重要な情報となりえる。
- 他組織からの連絡の場合も、その連絡そのものが偽りの可能性も考えられる。対応をとりつつも、その連絡先と、その内容の正当性を確認することが重要である。

- 原因の追求や対応に時間のかかる場合は、システムの運用の一時停止やネットワークの切断といった、システムへの侵入が実際に起こっていても、その侵攻を押さえる対策を実施後、原因追及を行う。

(6) 関係機関への報告

システムへ侵入され、被害にあった場合は警察へ被害届けを提出すること。(国内でも2000年2月13日よりいわゆる不正アクセス禁止法が施行されたため、システム上の情報の改ざんがなくとも、不正アクセスは処罰されることとなった。)

この場合、捜査のため各種ログの提供を求められる場合がある。また、場合によっては被害にあったサーバのハードディスクの提出を求められる場合もある。

また、他のサイトの同様な被害を未然に防止する観点からも、JPCERT／CC や IPA への報告を行うことが望ましい。

【参考情報】

(1) 届出先

- IPA　http://www.ipa.go.jp/SECURITY
- JPCERT/CC　http://www.jpcert.or.jp/
- 警察関係　http://www.npa.go.jp/(/police_j.htm)

（11）不正アクセス対策にかかる施策をシステム運用に反映させる

【主旨】

不正アクセス対策にかかる諸施策が有効に機能するためには、不正アクセス対策がシステム運用に求めていることが、実際のシステム運用で適切に実行されなければならない。

システムの運用においても、アクセス制限に関する設定の管理や、アクセス監視結果の分析、不正アクセス対策に関係してシステムにインストールしている諸機能に対する、ネットワークや機器の増設や変更、OS やアプリケーションソフトのレベルアップ等のシステムの運用環境の変更にともなう対応等、不正アクセス対策にかかわる作業は多い。

これらの作業を確実なものにするためには、不正アクセス対策が運用に委ねていることが、日々の運用において的確に実施されるようにする管理上の仕組みを工夫し、これらを日常の運用に組込んでおくことが必要となる。

【具体的な実施事項】

(1) 不正アクセス対策にかかる施策の運用規定、運用マニュアルへの適切な反映

不正アクセス対策にかかる諸施策がシステムの運用に求めていることは、システムの運用規定、運用マニュアルに適切に反映されていなければならない。

(2) 運用環境の変更の適切な反映

運用環境に以下に示すような変更が行われた場合は、不正アクセス対策にかかるシステム運用に変更の必要がないかどうかのチェックを行う。

- システムへのアクセス管理ルール、アクセス管理方法等、不正アクセス対策にかかる具体的手段の変更
- システム構成の変更
- システムの運用形態の変更
- 不正アクセス対策に用いている機能の変更

このチェックにより、システム運用に変更が必要となった場合は、以下の対応を適切に行わなければならない。

- 運用規定、運用マニュアルに対する必要な変更
- 必要な場合における運用スケジュールの変更等、システム運用の組立ての変更
- システム運用の変更の運用関係者への徹底

(3) 不正アクセス対策にかかる定期作業のスケジュール化

不正アクセス対策にかかる運用処理の実行を漏れないようするためのシステム運用上定期的に実施すべき作業は、予めスケジュール化しておくことが有効である。

不正アクセス対策に関連して、定期的な作業としてスケジュール化しておくべき作業としては、以下のようなものがあげられる。

- システムの運用要件の変更に伴うサービス制限やアクセス制限の変更の実施
- システム構成の変更に伴うサービス制限やアクセス制限の変更の実施
- 定期的なサービス制限やアクセス制限の実態検査の実施
- 必要に応じた、サービス制限やアクセス制限の実態検査の実施
- 定期的なアクセスログの保全処理
- 定期的なアクセス監視の分析の実施
- 使用ツールの機能確認と定期メンテナンス

(4) 運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行

不正アクセス対策にかかる運用作業についてのチェックリストを作成し、運用実績を記入、報告し、個々の作業が的確に実行されたことの確認を常に行うようにすることも、運用上から必要な処理が漏れないようにするための工夫の一つである。

(5) 不正アクセス対策にかかわる運用処理についての記録とその管理

以下に示すような不正アクセス対策にかかわる運用上の処理については、その記録を残し管理する。この運用処理に関する記録と管理を確実なものにするためには、該当する運用処理についての記録・管理要領を定めておくことも必要となる。

- アクセス管理ツールや監視ツールの新規導入、機種変更、機能変更および設定変更
- サービス制限やアクセス制限の変更
- サービス制限やアクセス制限の実態検査とその結果に対する処理
- アクセスログの分析とその結果に対する処理
- システムへの侵入事故に備えたシステムの保全処理
- アクセスログの保全処理
- 不正アクセス対策にかかるシステム運用の変更

【実施対策上のポイント】

(1) 不正アクセス対策にかかる施策の運用規定や運用マニュアルへの反映手順の確立

不正アクセス対策にかかる諸施策の運用規定や運用マニュアルへの反映を確実にするためには、これらの施策の運用規定や運用マニュアルへの反映手順を確立しておくことも必要となる。

これらの手順については、11.2 節の“(4)セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに適切に反映する”の項参照。

(2) 不正アクセス対策に関する運用処理のチェックリストについて

日々の運用における不正アクセス対策にかかる諸施策の運用処理を、確実なものにするための実行チェックリストにあげるべき処理としては、以下のようなものがあげられる。

- システムの運用要件の変更に伴うサービス制限やアクセス制限の変更の実施
- システム構成の変更に伴うサービス制限やアクセス制限の変更の実施

- 定期的なサービス制限やアクセス制限の実態検査の実施
- 必要に応じた、サービス制限やアクセス制限の実態検査の実施
- 定期的なアクセスログの保全処理
- 定期的なアクセス監視の分析の実施
- 使用ツールの機能確認と定期メンテナンス
- アクセスログの保全処理
- アクセスログの分析とその事後処理
- 関係する規準やその運用の変更

（12）関係者に対し不正アクセス対策についての教育を行う

【主旨】

不正アクセス対策が適切に定められていても、これらが機能するためには、システムの管理や運用にかかわる者に、これらについての十分な理解を必要とする。

このためには、不正アクセス対策に直接かかわる者だけでなく、システムの構築、管理、運用にかかわる者にも、以下に示すような不正アクセス対策とその実施に必要なスキルについての教育を適切に実施することが必要となる。

【具体的な実施事項】

(1) 関係者に対する不正アクセス対策についての教育の実施

① 不正アクセス対策に関する定期的教育の実施

不正アクセス対策に関する関係者への教育は、定期的に行われなければならない。

② 必要に応じた臨時教育の実施

以下のような場合は、その都度、該当者に対し実施することが必要である。

- 異動等により不正アクセス対策関係者の入替えがあった場合
- 不正アクセス対策にかかる基準やその運用が変更された時
- 不正アクセス対策に問題が生じた場合

(2) 不正アクセス対策についての教育カリキュラムの確立

不正アクセス対策についての教育を効果的に行うためには、教育科目とその内容、対象者と受講サイクル、実施時期等を定めた教育カリキュラムを、確立しておくことが望ましい。

教育すべき内容としては、以下があげられる。

- 不正アクセスの手口と対策の概要
- 不正アクセス対策の詳細とその実施要領
- 不正アクセス対策に用いる技術とその運用
- システムへの侵入事故事例

また教育内容は、サイトの運営形態やシステム構成、運用形態、さらには技術環境の進化を反映した、運用対象システムの実態に合ったものであるように、適時、更新すべきである。

(3) 不正アクセス対策に関する教育テキストの整備

関係者への不正アクセス対策に関する教育をより効果的にするために、サイトの運営実態に合ったテキストを準備する必要がある。

また、このテキストについてもサイトの運営環境の変更を反映するよう定期的な見直しを行うことが望ましい。

【対策実施上のポイント】

(1) 不正アクセス対策に関する教育カリキュラム例

表 3-7 に、不正アクセス対策に関する教育カリキュラムの一例を示す。

表 3-7 不正アクセス対策に関する教育カリキュラム例

項番	教育項目	教育対象者	頻度
1	不正アクセスの手口と対策の概要 ・ システムへの侵入の手口とその脅威の概要 ・ サイトにおけるシステムへの不正アクセス対策についての取組み ・ 不正アクセス対策の概要	・不正アクセス対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	1回／年
2	不正アクセス対策の詳細とその実施要領 ・ 関係基準 ・ 運用規定、運用マニュアル上の関係事項 ・ その他注意事項	・不正アクセス対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	1回／年
3	不正アクセス対策に用いる技術とその運用 ・ アドレス管理技術 ・ ポート管理技術 ・ アクセス制限技術 ・ アクセス制限管理技術 ・ アクセス監視技術 ・ 不正アクセス追跡技術	・不正アクセス対策関係者 ・システム開発関係者 ・システム管理関係者	1回／年
4	システムへの侵入事故事例	・不正アクセス対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	1回／年 + 随時

(13) 不正アクセス対策の実施状況についての監査を行う

【主旨】

不正アクセスに対する諸施策が決められその実施についての管理が行われていても、完全は期待できない。一方、不正アクセス対策の不備は、サイトのセキュリティに直接的な脅威となるため、不正アクセス対策の不備が問題をおこす前に、問題点を発見し適切な改善策を講じることができるようにしておくことも重要である。

このため、定められている不正アクセス対策は、サイトの運営実態に照らして適切かどうか、また、不正アクセス対策として定められていることが適切に実施されているかどうか等をチェックし、問題点の摘出と必要な改善の指導を行う、不正アクセス対策の実施状況についての監査を行うことも必要である。

また日常の運用の中で、実施した不正アクセス対策に関する運用についての記録の保管等、この監査のための準備を組込んでおくことも必要となる。

特に、EC サイトサービスを事業として提供しているモール等では、その責任からみても、この不正アクセス対策の実施状況に関する監査の実施は必須である。

(注)正式な監査という形はとらなくとも、ここに示すよう不正アクセス対策の実施状況についてのチェックは、組織的に行われるべきものである。

【具体的な実施事項】

(1) 不正アクセス対策の実施状況についての定期的な監査の実施

最低でも年1回は、不正アクセス対策の実施状況について、以下に示すような事項をチェックする監査を行う。

- 不正アクセス対策についての責任体制の整備状況とその機能状況
- 不正アクセス対策実施基準の妥当性
- 不要なサービスの除去または停止処理の実施状況
- ネットワークサービスに対するアクセス制限の実施状況
- ネットワークサービスに対するアクセス監視の実施状況
- 不正アクセス対策に使用している機能の実装状況
- システムへの侵入事故への備えの状況
- 不正アクセス対策にかかる施策のシステム運用への反映状況
- 関係者の不正アクセス対策に関する認識とスキルレベル

(2) 監査実施要領の確立

不正アクセス対策の実施状況についての定期的な監査が、円滑に実施され、かつ実効的なものにするためには、この監査についての実施要領が確立されていることが望ましい。

この監査実施要領で規定しておく事項については、1.2.2 節の(4)項を参照。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。

このためには、監査指摘事項に対する改善措置が実際にとられたかどうかについての確認を行うことも必要であり、監査指摘事項についてのフォローの仕組みも、監査要領の中に組込んでおくことも有効である。

【対策実施上のポイント】

(1) 監査内容例

表 3-8 に、不正アクセス対策の実施状況についての監査において、監査すべき事項の例を示す。

(2) 監査の報告

監査結果は、不正アクセス対策総括責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告されなければならない。

表 3-8 不正アクセス対策の実施状況に関する監査項目

項番	監査項目	監査の内容等
1	不正アクセス対策についての責任体制の整備状況とその機能状況	・不正アクセス対策についての責任体制は、サイトの運営実態に照らして適切か ・不正アクセス対策についてかかわる責任者の自己の責任についての認識は十分か ・不正アクセス対策について責任体制は機能しているか
2	不正アクセス対策実施基準の妥当性	・不正アクセス対策実施基準は、サイトの技術環境、運用環境等のサイトの運営実態に照らして適切か
3	不要なサービスの除去または停止処理の実施状況	・システムで稼動中のサービスはすべて正確に把握されているか ・個々のサーバから不要なサービスは除去または停止されているか ・除去または停止されていない危険なサービスの当該サーバでの使用は妥当か ・サイトの運営上、止むをえず稼動させている危険なサービスについての運用上の制約は確立しており、かつそれらは確実に実施されているか

表 3-8　不正アクセス対策の実施状況に関する監査項目

項番	監査項目	監査の内容等
4	ネットワークサービスに対するアクセス制限の実施状況	・各サーバにおけるアクセス制限要件はシステムへの侵入防止実施基準に沿って適切に設定されているか ・各サーバにおけるネットワークサービスに対するアクセス制限は、それぞれのサービスに対するアクセス制限要件通りに機能していることが確認されているか
5	ネットワークサービスに対するアクセス監視の実施状況	・アクセス監視要件はアクセス監視基準に沿って適切に設定されているか ・各サーバにおけるネットワークサービスに対するアクセス監視機能は、侵入防止実施基準に沿って適切な場所に適切に組込まれているか ・監視結果は適切に処理されているか
6	不正アクセス対策に使用している機能の実装状況	・不正アクセス対策に用いる技術およびその機能選択は妥当か ・その実装の正確性は確認されているか （実装すべき場所に正確に実装されているか） ・運用環境の変更時における対応機能の実装の見直しは行われているか ・必要な運用環境の整備状況についてのチェックは適切に行われているか
7	システムへの侵入事故への備えの状況	・システムに侵入を許した時に備えた保全要領が、サイトの運営実態に照らして適切に決められているか ・必要な保全処理は適切に行われているか ・システムへの侵入事故への対処要領は適切に決められているか ・監査期間中におけるシステムへの侵入事故が発生した時の処理は妥当であったか
8	不正アクセス対策にかかる諸施策のシステム運用への反映状況	・不正アクセス対策にかかる諸施策は運用規定、運用マニュアルに適切に反映されているか ・これらの運用は、日々の運用において確実に実行されているか、また、そのことは管理されているか ・不正アクセス対策にかかわるシステム運用の適切な実行を実現するための工夫は十分か
9	関係者の不正アクセス対策に関する認識とスキルのレベル	・不正アクセスならびにこれらへの対策の実施についての認識は十分か ・不正アクセス対策にかかわる者のスキルは十分か ・関係者へのシステムへの侵入防止策に関する教育は適切か

4 セキュリティホール対策の徹底

4.1 必要な施策項目

図 4-1 に、セキュリティホール対策の組立て示す。

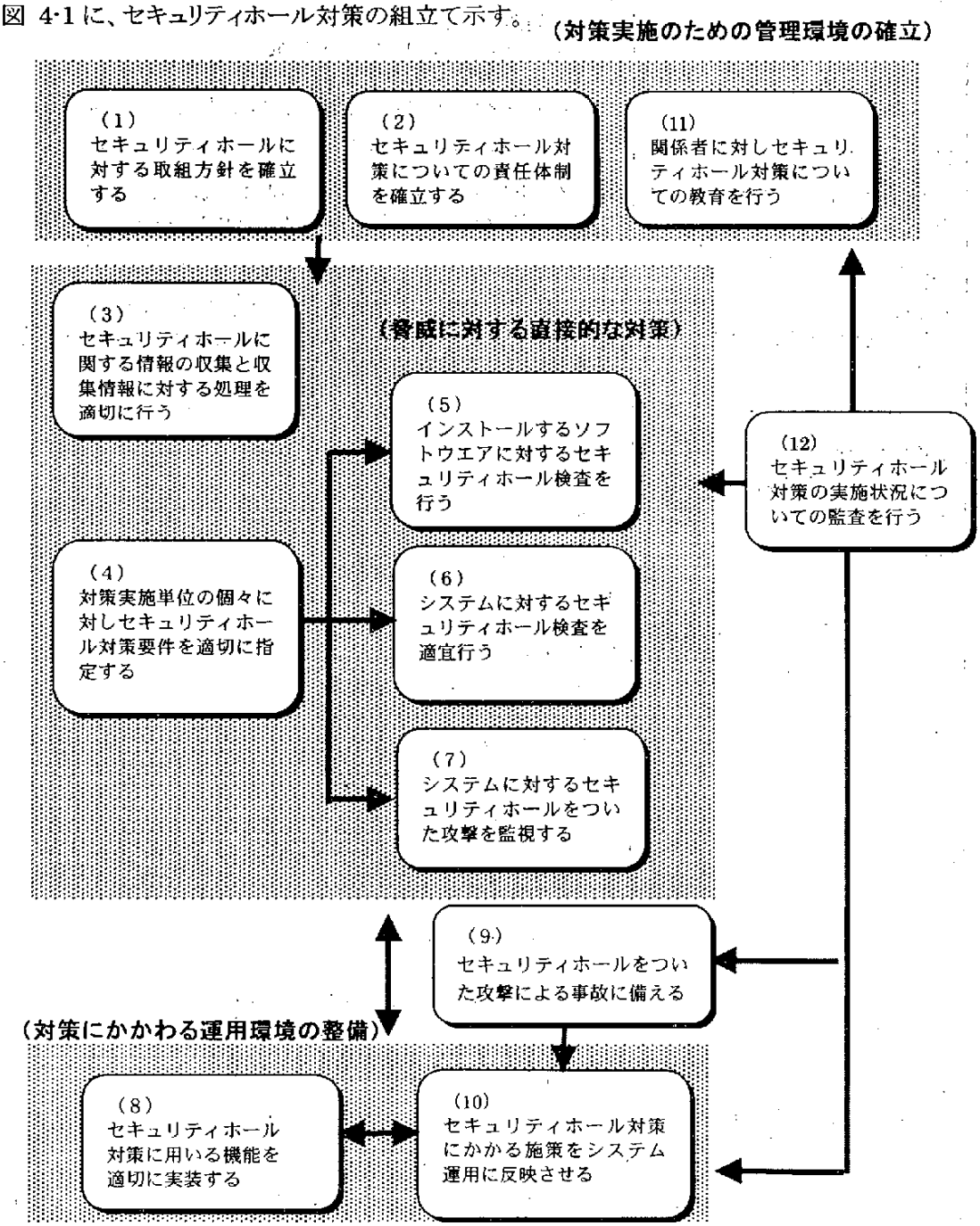


図 4-1 セキュリティホール対策の組立て

また、各施策における実施事項の一覧を示す。

表 4-1　セキュリティホール対策としての具体的実施事項一覧

施策名	具体的実施事項
(1) セキュリティホールに対する取組方針を確立する	① セキュリティホール対策の目標の明確化 ② 適用範囲の明確化 ③ セキュリティホール対策実施基準の確立 ④ セキュリティホール対策の組立ての明確化 ⑤ セキュリティホールに対する取組方針の関係者への周知
(2) セキュリティホール対策についての責任体制を確立する	① セキュリティホール対策についての責任体制の明確化 ② セキュリティホール対策関係者間の連携体制の確立
(3) セキュリティホールに関する情報の収集と収集情報に対する処理を適切に行う.	① セキュリティホールに関する情報の収集とその処理要領の確立 ② セキュリティホールに関する情報の収集と収集情報に対する適切な処理の実施
(4) 対策実施単位の個々に対しセキュリティホール対策要件を適切に指定する	① 対策処理単位の個々に対するセキュリティホール対策要件の指定 ② 対策処理単位の個々に指定した対策要件についてのドキュメントの整備
(5) インストールするソフトウェアに対するセキュリティホール検査を行う	① セキュリティホール対策の視点からのソフトウェアの導入に関するルールの確立 ② 最適バージョンの使用 ③ 新しくシステムにインストールするソフトウェアに関するセキュリティホール情報の把握 ④ 新しくシステムにインストールするソフトウェアに対するセキュリティホール検査の実施 ⑤ 新しくシステムにインストールするソフトウェアに対するセキュリティホール検査についての記録とその保管 ⑥ セキュリティホール発見時の適切な処置の実施
(6) システムに対するセキュリティホール検査を適宜行う	① 定期的なセキュリティホール検査の実施 ② 必要に応じた臨時セキュリティホール検査の実施 ③ 実施したセキュリティホール検査についての記録とその保管 ④ セキュリティホール発見時の適切な処置の実施
(7) システムに対するセキュリティホールをついた攻撃を監視する	① セキュリティホールをついた攻撃監視機能の適切な適用 ② 監視結果に対する適切な処置の実施 ③ 監視結果についての記録とその保管 ④ セキュリティホールをついた攻撃の試みまたはその痕跡発見時における適切な処置の実施

表 4-1　セキュリティホール対策としての具体的実施事項一覧

施策名	具体的実施事項
(8) セキュリティホール対策に用いる機能を適切に実装する	① 適切な技術と使用する機能の選択 ② 組込み場所の適切な選択 ③ 選択した技術、機能の適切な組込み ④ パターンファイルの適切なメンテナンス等の必要な運用環境の整備 ⑤ 使用技術の実装についてのドキュメントの整備
(9) セキュリティホールをついた攻撃による事故に備える	① セキュリティホールをついた攻撃を許した時における対処要領の確立 ② セキュリティホールをついた攻撃による被害への対処に必要な情報の整備 ③ セキュリティホールをついた攻撃に備えたシステムの保全 ④ セキュリティホールをついた攻撃による被害を想定した事故処理訓練の実施 ⑤ 必要なツールの整備
(10) セキュリティホール対策にかかる施策をシステム運用に反映させる	① セキュリティホール対策にかかる施策の運用規定、運用マニュアルへの反映 ② 運用環境の変更への適切な対応 ③ セキュリティホール対策にかかる定期作業のスケジュール化 ④ 関係する運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行 ⑤ セキュリティホール対策にかかる運用処理についての記録とその管理
(11) 関係者に対しセキュリティホール対策についての教育を行う	① 関係者に対するセキュリティホール対策についての教育の実施 ② セキュリティホール対策についての教育カリキュラムの確立 ③ セキュリティホール対策に関する教育テキストの整備
(12) セキュリティホール対策の実施状況についての監査を行う	① セキュリティホール対策の実施状況についての定期的な監査の実施 ② 監査実施要領の確立 ③ 監査指摘事項に対するフォローの実施

4.2 個別具体策

(1) セキュリティホールに対する取組方針を確立する

【主旨】

セキュリティホールをついた攻撃により、外部からシステムを不正に操作されたり、情報を不正に取得されたり、ソフトウェアや情報を改ざん、破壊されたりすることを防ぐとともに、万一、セキュリティホールをついた攻撃を許しても、その被害を限定的なものにすることに組織的に取組むには、セキュリティホール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示すセキュリティホールに対する取組方針確立し、これを、セキュリティホール対策に直接かかわる者だけでなく、システムの構築や運用に関係する者、さらにはサイトにおけるセキュリティホール対策に関係する者すべてに周知させておくことが必要となる。

【具体的な実施事項】

(1) セキュリティホール対策の目標の明確化

セキュリティホール対策が目指すところを明確にし、セキュリティホール対策にかかる諸施策の意図を明確にする。セキュリティホール対策の目標としては、以下があげられる。

- セキュリティホールをついた攻撃の阻止
- セキュリティホールをついた攻撃を許した時の被害の極小化

(2) 適用範囲の明確化

セキュリティホール対策の適用範囲として、下記を明確にする。

- サイトのシステム構成上の対象となる領域および対象サーバ等の機器
- 対象とするソフトウェア

(3) セキュリティホール対策実施基準の確立

セキュリティホール対策の基本は、セキュリティホールを有するソフトウェアに対し、それらが除去された新しいバージョンに交換したり、対策パッチを施したりして、既知のセキュリティホールの除去をすることにある。その効果はセキュリティホールの検査と除去の実施密度に依存する。

しかし、サイト全体に対し密度の高い対策を一律に行うことは、運用上相当の負担が伴う。このため、セキュリティホール対策の実施が疎かになり、その結果として、危険度の高いセキュリティホールを外部にさらされているサーバに残し、セキュリティホールをついた攻撃を許すことになる。

実際に実施するセキュリティホール対策は、サーバまたはソフトウェア単位に決めなければならないが、これらを運用負担とバランスが取れた実効的なものにするとともに、サイト全体で整合性のあるものにすることが必要である。このためには、実施するセキュリティホール対策に厳格さによるレベル分けを行い、それぞれのレベルに対する標準的な対策要件を定義したセキュリティ

ホール対策実施基準を確立しておき、対象サーバまたはソフトウェアごとに適用する対策レベルを割当て、そのレベルに指定されている対策要件に従った対策を実施するような工夫も必要となる。

セキュリティホール実施基準として、定義すべき事項としては以下をあげることができる。

- 対策レベル名称
- 当該レベルに求める対策の実施密度
- 当該レベルの適用範囲
- セキュリティホール検査の実施要件
- セキュリティホール除去の実施要件

セキュリティホール対策は、このセキュリティホール対策実施基準に準じて実施されなければならない。

(4) セキュリティホール対策の組立ての明確化

セキュリティホール対策をどのように行うかを明らかにするもので、実施する施策の構成とその施策間の関係を示す。

本ガイドラインにおけるセキュリティホール対策にかかる諸施策の組立てについては、4.1 節参照。

(5) セキュリティホールに対する取組方針の関係者への周知

作成されたセキュリティホールへの取組方針は文書化され、セキュリティホール対策に直接かかわる者だけでなく、システムの構築ならびに運用関係者等、セキュリティ対策に関係する者のすべてに周知させておかなければならない。このためには、

- セキュリティホールに対する取組方針配布や掲示
- 関係者間でのセキュリティホールに対する取組方針の定期的な再確認

も必要となる。

【対策実施上のポイント】

(1) セキュリティホール対策実施基準の定義要領

表 4-2 に、セキュリティホール対策実施基準で定義すべき事項を示す。

表 4-2　セキュリティホール対策実施基準の定義内容

項番	定義項目	定義内容
1	対策レベル名称	・ 当該対策レベルの名称と ID
2	当該レベルに求めるセキュリティホール対策の実施密度	・ 対象領域における既存のセキュリティホールの存在についての容認の程度で表わす目標とするセキュリティホール対策の成果 (注1)
3	当該レベルの適用対象	・ 当該レベルを適用するサーバ、あるいはソフト
4	セキュリティホール検査の実施要件	・ 当該レベルに求められるセキュリティホール検査の実施サイクル ・ 使用する検査パターンに関する要件(注2)
5	セキュリティホール除去の実施要件	・ 検出されたセキュリティホールの除去実施のタイミング (注3)

(注1) セキュリティホール対策の実施密度の定義例
- 常時、既知のセキュリティホールはすべて除去または運用対策済
- 危険度の高いセキュリティホールは、すべて常時対策済とするが、それ以外のセキュリティホールについては、二週間以内に限り未対策を容認
- 除去していないセキュリティホールのすべてについて、1ヶ月以内は存在を容認

(注2) 使用するセキュリティホール対策検査パターンについての要件の定義例
- 既知のセキュリティホールすべてに対応
- 危険度の高いセキュリティホールについてはすべて対応、それ以外のセキュリティホールについては、二週間前のパターンで可
- 定期メンテナンスで更新された最新パターンであれば可

(注3) セキュリティホール除去の実施要件の定義例
- 存在が確認されているセキュリティホールのすべてに対し即時除去の実施
- 危険度の高いセキュリティホールに対しては、即時除去を実施、それ以外の存在が確認されているセキュリティホールに対しては、二週間以内に除去を実施
- 未対策のセキュリティホール全てについて、毎月の定期メンテナンスで対策

(2) セキュリティホールの危険度クラスについて

セキュリティホールの危険度とは、個々のセキュリティホールの存在がサイトシステムに与える脅威のレベルであり、求めるセキュリティホール対策レベルを決める時の判断材料となるものである。セキュリティホールの危険度は、その構造的な特性とサイトシステムの構成の組合せからく

る、攻撃を受ける確率と、そのセキュリティホールにより可能となる攻撃の種類により異なる。

このセキュリティホールの危険度についてクラス化を行い、各対策対象機器(サーバ)またはソフトにおけるセキュリティホール対策実施の要否の判断に用いるようにすることも、サイト全体におけるセキュリティホール対策を整合性のあるものにすることに有効である。

表 4-3 に、セキュリティホールの危険度クラスの定義例を示す。

表 4-3 セキュリティホールの危険度クラスの定義例

項番	危険度クラス	危険の程度
1	クラスA	・当該セキュリティホールをついた攻撃を受けた時の被害は大きく、かつ、当該サイトの特性から、機器によっては攻撃を受ける可能性の高いセキュリティホール
2	クラスB	・当該セキュリティホールをついた攻撃を受けた時被害は大きいものの、当該サイトの特性から、攻撃を受ける可能性は、そう高くないセキュリティホール
3	クラスC	・当該セキュリティホールをついた攻撃を受けても、その被害は限定的であるが、当該サイトの特性から、機器によっては、攻撃を受ける可能性が高いセキュリティホール
4	クラスD	・当該セキュリティホールをついた攻撃を受けても、被害は限定的で、かつ、攻撃を受ける可能性も低いセキュリティホール

(3) セキュリティホール対策実施基準の定義例

表 4-4 に、セキュリティホール対策実施基準の定義例を示す。

表 4-4 セキュリティホール対策実施基準例

項番	対策レベル	当該対策レベルにおける標準的な対策要件
1	レベルA	・対策実施密度・・・・・・・・・・・常時、既知のセキュリティホールは全く存在しない ・適用範囲・・・・・・・・・・・・・・サイト全体に直接大きな影響を与えるサーバ 他社に影響を与える可能性のあるサーバ ・セキュリティホール検査の実施要件 ・・・・・・・最新パターンによる月2回以上のセキュリティホール検査の実施 新しいセキュリティホールが報告された都度、そのセキュリティホールに対する臨時検査の実施 ・セキュリティホール除去の実施要件 ・・・・・・・・セキュリティホール発見時に即時に実施 ・セキュリティホール攻撃監視要件 ・・・・・・・・入力データに対し、常時実施 検査パターンは常に最新情報を反映

表 4-4　セキュリティホール対策実施基準例

項番	実施レベル	当該対策レベルにおける標準的な対策要件
2	レベルB	・対策実施密度……2週間の定期検査期間中は、危険度クラスA、B、Cを除く新しく報告されたセキュリティホールの存在は容認 ・適用範囲……サイト全体への影響が比較的大きいサーバ ・セキュリティホール検査の実施要件 ……最新パターンによる月2回以上のセキュリティホール検査の実施 危険度A, B, Cの新しいセキュリティホールが報告された都度、そのセキュリティホールに対する臨時検査の実施 ・セキュリティホール除去の実施要件 ……セキュリティホール検出時に即時に実施 ・セキュリティホール攻撃監視要件 ……入力データに対し、常時実施 検査パターンは、新しく報告された危険度A, B, Cのセキュリティホールに対応
3	レベルC	・対策実施密度……2週間の定期検査サイクル間は、新しいセキュリティホールに対しては容認 ・適用範囲……外部へは影響を及ぼさないものの、業務やサイトの運用への影響が大きいことが懸念されるサーバ ・セキュリティホール検査の実施要件 ……最新パターンによる月2回以上のセキュリティホール検査の実施 特別の場合を除いては、臨時検査は不要 ・セキュリティホール除去の実施要件 ……セキュリティホール検出後、1ヶ月以内に実施 ・セキュリティホール攻撃監視要件……特に不要
4	レベルD	・対策実施密度……1ヶ月間の定期検査サイクル間は、新しいセキュリティホールに対しては、容認 ・適用範囲……外部へは影響を及ぼさないものの、業務やサイトの運用への影響が大きいことが懸念されるサーバ ・セキュリティホール検査の実施要件 ……最新パターンによる月1回以上のセキュリティホール検査の実施 特別の場合を除いては、臨時検査は不要 ・セキュリティホール除去の実施要件 ……セキュリティホール検出後、1ヶ月以内に実施 ・セキュリティホール攻撃監視要件……特に不要

(4) セキュリティホール対策実施基準の適用について

セキュリティホールの検査や除去の実施は、保護対象のソフトやファイルごとに検討しなければならない。ただし、各ソフトやファイルに求められるセキュリティホール対策密度は、それがイン

ストールされるマシンに同居している他のサービスへの影響も配慮して決めなければならない。このため、同じソフトやファイルでも、インストールされるマシンによって異なったものになることがある。

(5) セキュリティホールに対する取組み方針は、システムの構成やその運用形態等システム運用の実環境の変化に対応して必要な修正が加えられるべきであり、必要に応じて見直しを行うこと。

(6) セキュリティホールに対する取組み方針については、定期的に関係者間で再確認することをルーチン化しておくことが望ましい。

(2) セキュリティホール対策についての責任体制を確立する

【主旨】

セキュリティホール対策をその取組方針に沿って機能させるためには、セキュリティホール対策として定められていることが、システムの構築や運用に適切に反映されるよう、指導、管理する責任体制の確立が必要となる。

このためには、セキュリティホール対策にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) セキュリティホール対策についての責任体制の明確化

セキュリティホール対策の責任体制に関し、明確にしておくべきこととしては、以下があげられる。

- セキュリティホール対策責任者とその責任
- セキュリティホール対策の実施担当者の責任
- システム開発者のセキュリティホール対策に関する責任
- システム管理者のセキュリティホール対策に関する責任
- システム運用者のセキュリティホール対策に関する責任

(2) セキュリティホール対策関係者間の連携体制の確立

セキュリティホール対策に関する責任体制が有効に機能するためには、関係者間の連携が重要となる。

【対策実施上のポイント】

(1) セキュリティホール対策関係者の責任分担

表 4-5 に、セキュリティホール対策関係者の責任分担の定義例を示す。

(2) セキュリティホール対策にかかる責任体制は、セキュリティホール対策を変更したり、サイトの運営環境に変更が生じた場合は、見直しを行い、必要な変更を行うこと。

表 4-5　セキュリティホール対策関係者の責任分担

責任区分	タスク
セキュリティホール対策責任者	・セキュリティホールに対する取組方針の確立と関係者への周知 ・セキュリティホール対策実施基準の発行 ・セキュリティホール対策全体の妥当性の維持 ・セキュリティホール対策の実施状態のチェック ・対策実施基準に沿ったセキュリティホール対策の実施の指導 ・セキュリティホールをついた攻撃を許した時の対策の指揮
セキュリティホール対策の実施担当者	・セキュリティホール対策の詳細の検討 ・セキュリティホールに関する最新情報の入手とその処理 ・セキュリティホール対策の実施状況の把握 ・システム上の未対策セキュリティホールの把握 ・セキュリティホール検査に用いる機能の適切なシステムへの組込みと必要な環境整備 ・検査パターンのメンテナンスの管理 ・検査結果の確認と検査結果に対する適切な処理の決定 ・セキュリティホール除去計画の決定と指示および実行確認 ・セキュリティホールをついた攻撃の監視 ・セキュリティホールをついた攻撃を許した場合の対処と再発防止策の検討
システム開発者	・開発システムにおけるセキュリティホール対策関係機能の適切な組込み －設計の妥当性の確認 －正確な実装の確認
システム管理者	・セキュリティホール除去作業の実施 ・セキュリティホール対策に用いる機能の維持 －必要なシステム構成の変更の反映の管理 －使用機能の動作環境の維持管理 ・セキュリティホール検査に用いる検査パターンのメンテナンス ・システムにおける対応機能の実装状況の正確な把握
システム運用者	・セキュリティホール対策に用いる機能が必要とするシステム運用環境の整備 ・実施基準に沿った定期セキュリティホール検査の実施 ・実施基準に沿った臨時セキュリティホール検査の実施

(3) セキュリティホールに関する情報の収集と収集情報に対する処理を適切に行う

【主旨】

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を見逃すことになる。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、入手した情報の分析を行い、セキュリティホール対策に適切に反映することが必要である。

このため、最新のセキュリティホール情報の収集と、収集した情報の処理を適切に行うための仕組みを確立しておくことが必要となる。

【具体的な実施事項】

(1) セキュリティホールに関する情報の収集とその処理要領の確立

セキュリティホールに関する最新情報を漏れなく収集し、これらの情報が有効かつタイムリーに活用されるようにするためには、以下のようなことを定めたセキュリティホールに関する情報の収集とその処理要領を確立しておく必要がある。

- 情報の収集とその処理に関する責任者
- 情報収集源
- 収集サイクル
- 収集すべき情報の内容
- 収集した情報の処理手順
- 収集した情報とその処理に関する記録とその管理

(2) セキュリティホールに関する情報の収集と収集情報に対する適切な処理の実施

セキュリティホールに関する情報の収集とその処理要領に従って、セキュリティホールに関する最新の情報を収集するとともに、指定された手順に従い、収集した情報に対する処理を行い、必要な場合は、セキュリティホール対策実施基準に従ったセキュリティホール対策を実施しなければならない。

これらの処置の確実な実行を管理する仕組みを、日々のシステム運用の中に組込んでおくことも必要である。

【対策実施上のポイント】

(1) 収集したセキュリティホールに関する情報の処理手順の定義

収集情報に対する処理手順の中で、その考え方と進め方を示しておくべきこととしては、以下があげられる。

- 収集した情報に対する処理についての責任者

- 新しく報告されたセキュリティホールに対する検査、除去実施の要否の判断
- 問題となるセキュリティホールの検査、除去が実施されるまでの間の運用制限の要否と、必要な場合の運用制限の範囲設定、およびその実施
- 必要なセキュリティホール検査、除去の実施計画の立案
- 計画されたセキュリティホール検査、除去の実行確認

(2) セキュリティホールに関する情報の収集は、可能な限り短いサイクルで行うべきである。できれば、毎日、新しい情報がないかどうかのチェックを行うことが望ましい。

(3) 収集した情報から、セキュリティホール検査および除去処理の実行が必要と判断されても、運用上の都合等により、すぐに対策できない場合もある。このような場合、対策が実施されるまでの期間、システムに脆弱性が存在していることを認識し、運用制限等の運用上の処置を適切に施さなければならない。

【参考情報】

セキュリティホール情報入手先例

- メーカ、ソフトウェア製造者及び取り扱い業者

Microsoft Security Bulletin(英語)	http://www.microsoft.com/security/
Microsoft Security Bulletin(日本語)	http://www.asia.microsoft.com/japan/security/
Sun Security Bulletin	http://sunsolve.sun.com/pub-cgi/secBulletin.pl

- 中立的第3者機関

CERT/CC	http://www.cert.org/
CIAC	http://ciac.llnl.gov/
JPCERT/CC	http://www.jpcert.or.jp/
IPA	http://www.ipa.go.jp/SECURITY/

- 書籍、雑誌、インターネットのセキュリティサイト
- BUGTRAQ等のメーリングリスト

これらの情報源から得たセキュリティホールに関する情報のうち、自サイトに影響があると判断されるセキュリティホールの情報についてはセキュリティ担当者がセキュリティホール管理簿に情報を載せて以後管理する。

(4) 対策実施単位の個々に対しセキュリティホール対策要件を適切に指定する

【主旨】

セキュリティホール対策を適切に行うためには、セキュリティホール検査や発見したセキュリティホールの除去等のセキュリティホール対策処理を行う単位としてのサーバやソフト(群)ごとに、どのような対策を行うのかが、セキュリティホールに対する取組方針の中で定めたセキュリティホール対策実施基準に沿って適切に決められていなくてはならない。

この対策要件の設定にあたっては、対策処理の実施単位ごとに、セキュリティホール攻撃を受けた時の影響の大きさを考慮する。

【具体的な実施事項】

(1) 対策実施単位個々に対するセキュリティホール対策要件の指定

セキュリティホールの検査、攻撃の監視、除去等のセキュリティホール対策処理の実行単位となるマシンやソフトウェア(群)ごとに、これらをどのように行うのかについて、以下に示すようなことを指定する。

- 対策対象の名称
- 対策対象に含まれるソフトウェア
- 適用する対策レベル
- セキュリティホール検査に関する要件
- セキュリティホール攻撃の監視に関する要件
- セキュリティホール発見時の対応方法
- 保全要件

また、この個々の対策実施単位に定められたセキュリティホール対策要件は、システムの構成やセキュリティホール対策実施基準等にセキュリティホール対策の実施方法に影響を与えるような変更が生じた場合は、その見直しを行い、必要な変更を行わなければならない。

(2) 対策実施単位の個々に指定した対策要件についてのドキュメントの整備

セキュリティホール対策が適切に行われているかどうかについて、管理が適切に行えるように、個々のセキュリティホール対策対象単位ごとに定めた対策要件についてのドキュメントの整備を行い、何時でも正確にその内容が把握できるようにしておくことも必要である。

このドキュメントに記載しておくべき事項は、個々のセキュリティホール対策の実施単位に対する、(1)項であげた項目となる。

また、このドキュメントは、システムの構成やセキュリティホール対策実施基準等の変更に伴う対策要件の変更が、適切に反映されたものであるようになってなければならない。

【対策実施上のポイント】

(1) 個々の対策実施単位に指定するセキュリティホール対策実施要件の定義要領

表 4-6 に個々の対策実施単位に指定するセキュリティホール対策実施要件で指定すべき事項を示す。

表 4-6 対策実施単位に指定するセキュリティホール対策要件定義における指定項目

項番	定義項目	定義内容
1	対策対象名称	・当該対策対象単位の名称、ID
2	対策対象に含まれるソフトウェア	・当該対策対象単位に含まれるソフトウエア ・それぞれの構成ソフトウェアに求められるセキュリティホール対策レベル
3	対策対象に適用する対策レベル (注1)	・当該対策対象単位に適用するセキュリティホール対策レベル (当該対策対象単位に含まれるソフトウェア個々に求められる対策レベルのうち最も高いレベルを指定)
4	セキュリティホール検査に関する要件 (注2)	・定期セキュリティホール検査の実施サイクル ・臨時セキュリティホール検査が必要な条件 ・これらのセキュリティホール検査に用いる検査パターンの条件
5	セキュリティホール攻撃監視に関する要件 (注3)	・セキュリティホール侵入監視の内容(どのような内容の監視を行うかを明示) ・使用技術と使用する機能(使用する技術の概要と、その機能設定要件) ・セキュリティホールの侵入監視に用いる検査パターンの条件
6	セキュリティホール発見時の対応方法 (注4)	・発見セキュリティホールの除去実施のタイミング
7	保全要件	・バックアップの取得要件 ・バックアップの取得サイクル ・バックアップ管理要件

(注1) セキュリティホール対策実施基準参照

(注2) セキュリティホール対策実施基準に定める、当該対策レベルに対するセキュリティホール検査に関する要件を基準に決定

(注3) セキュリティホール対策実施基準に定める、当該対策レベルに対するセキュリティホール攻撃監視に関する要件を基準に決定

(注4) セキュリティホール対策実施基準に定める、当該対策レベルに対する発見セキュリティホールの除去実施に関する要件を基準に決定

(2) セキュリティホール対策実施単位の編成

求めるレベルのセキュリティホール対策を効率的に行うためには、セキュリティホール対策実施単位が適切に編成されていなくてはならない。セキュリティホール対策実施単位の編成にあたって考慮することをあげると以下のようになる。

- ツールの機能範囲と性能
- 対策対象ソフトウェアに求められる対策レベルの組合せ
- 運用負担

(3) バックアップについての考え方

セキュリティホールをついた攻撃に備えたバックアップについての考え方については、“(9)セキュリティホールをついた攻撃による事故に備える”を参照のこと。

(5)インストールするソフトウェアに対するセキュリティホール検査を行う

【主旨】

セキュリティホール対策の第一歩は、セキュリティホールのないソフトウェアを用いることにある。

このためには、システムに新たにインストールするソフトウェアについては、当該ソフトウェアに関するセキュリティホール情報を参考に、セキュリティホール対策の最も進んだバージョンを選択するとともに、システムへのインストールにあたっては、改めてセキュリティホール検査を行い必要な対策を実施する等、システムに既知のセキュリティホールを無管理のまま持込まないようにする努力をしなければならない。

【具体的な実施事項】

(1) セキュリティホール対策面からのソフトウェアの導入に関するルールの確立

危険性の高いセキュリティホールを持つソフトウェアをシステムにインストールしてしまわないようにするためには、セキュリティホール対策の視点からの新しいソフトウェアの導入に関するルールを確立しておくことが必要となる。

このルールの中で明確にしておくべきこととしては、以下をあげることができる。

- 適用対象ソフトウェア
- 最新バージョンの使用
- 使用ソフトウェアのセキュリティホールに関する情報の把握
- 使用にあたっての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パッチの実施等、その使用上の条件
- 導入の承認
- 導入時検査に関する記録とその保管

(2) 最新バージョンの使用

新しくシステムにインストールするソフトウェアに対しては、特に問題がない場合は、最新バージョンを採用する。

(3) 新しくシステムにインストールするソフトウェアに関するセキュリティホール情報の把握

新しくシステムにインストールするソフトウェアに対しては、セキュリティホール対策責任者による、

- 当該ソフトウェアのセキュリティホールに関する情報の確認
- 使用にあたっての条件の確立
- 使用の承認

を行わなければならない。

(4) 新しくシステムにインストールするソフトウェアに対するセキュリティホール検査の実施

選択したソフトウェア(バージョン)に対して、システムへのインストールに先立ってセキュリティ

ホール検査を実施し、検査に用いたパターンの範囲ではセキュリティホールがないことを確認する。

この検査で用いる検査パターンは、当該ソフトウェアがインストールされるマシンまたはソフトウェア群であらわされるセキュリティホール対策実施単位に指定されている対策要件に従ったものでなければならない。

(5) 新しくシステムにインストールするソフトウェアに対するセキュリティホール検査についての記録とその保管

セキュリティホール検査にパスしてシステムにインストールされるソフトウェアについては、"セキュリティ対策の視点からのソフトウェアの導入についてのルール"に従い、これらの審査、検査についての記録を行い、適切に保管する。

(6) セキュリティホール発見時の適切な処置の実施

セキュリティホールが発見された場合は、別バージョンの選択あるいはパッチ等によるセキュリティホール対策の実施を行い、当該マシンあるいはソフト(群)に指定されている対策レベルを満足するレベルにした後、システムへのインストールを行う。

【対策実施上のポイント】

(1) "セキュリティホール対策面からのソフトウェアの導入についてのルール"の適用対象について

このルールは、一つのアプリケーション全体、アプリケーションの一モジュール、マクロ等その構造を問わず、サイトシステムにインストールするすべてのソフトウェアに対し、以下のような場合に適用しなければならない。

- 新しい機器をシステムにインストールする場合、もしくは一部を交換する場合
- 新しいソフト(パッケージソフト、開発ソフト)一式をシステムにインストールする場合、もしくは一部を交換する場合

また、このルールは、自社開発ソフト、外部に開発委託を行ったソフト、購入ソフトのすべてを対象とする。

(2) 導入審査についての記録について

導入時のバージョンの選択やセキュリティホール検査についての記録に記載すべき事項としては、以下があげられる。

- 素性審査の日時、内容、評価および実施責任者
- 導入時セキュリティホール検査実施日
- 使用した検査ツールと検査結果
- 導入時セキュリティホール検査に用いたパターンファイルに関する情報(メンテナンス日等)

(6) システムに対するセキュリティホール検査を適宜行う

【主旨】

セキュリティホールの除去に努力しても、その実施上の不備や報告されていないセキュリティホール等の潜在等で、セキュリティホールがないシステムを構築することは難しい。このような状況の下、セキュリティホールをついた攻撃による被害を受けないようにするためには、最新の検査パターンを用いたセキュリティホール検査を頻繁に行い、システムに残されているセキュリティホールの発見に努め、発見したセキュリティホールの除去を速やかに行い、攻撃者に対する足掛かりを少しでも少なくする努力が必要となる。

システムに残されている既知のセキュリティホールの発見と除去を適切に行うためには、セキュリティホール対策実施単位に定められている対策要件に沿って、適宜、セキュリティホール検査を実施する必要がある。

【具体的な実施事項】

(1) 定期的なセキュリティホール検査の実施

マシン、あるいはソフトウェア(群)に対しては、セキュリティホール対策実施単位ごとに定められたセキュリティホール対策要件に従って、定期的にセキュリティホール検査を実施する。

検査サイクル、検査方法、検査パターンに関する条件は、それぞれに定められている対策要件の指定による。

(2) 必要に応じた臨時のセキュリティホール検査の実施

マシン、あるいはソフトウェア(群)については、セキュリティホール対策実施単位ごとに定められたセキュリティホール対策要件において、臨時セキュリティホール検査が必要と指定されている状況が発生した場合は、その指定に従って、臨時セキュリティホール検査を実施しなければならない。

検査方法、検査パターンに関する条件は、それぞれに定められている対策要件の指定による。

(3) 実施したセキュリティホール検査についての記録とその保管

定期、臨時を問わず、実施したセキュリティホール検査については、セキュリティホール対策実施基準に沿った実施に関する記録の作成とその保管を行わなければならない。

(4) セキュリティホール発見時の適切な処置の実施

セキュリティホールが発見された場合は、その除去を行うとともに、このセキュリティホールをついた攻撃を受けていないかどうかの調査を行い、必要な場合は、セキュリティホール攻撃による事故処理を行う。セキュリティホールをついた攻撃による事故の処理については、"(9)セキュリティホールをついた攻撃による事故に備える"の項を参照。

【対策実施上のポイント】

(1) 臨時セキュリティホール検査の実施が必要なケース

- 新しい危険度の高いセキュリティホールが報告され、セキュリティホール検査パターンがこのセキュリティホールに対応した時(対応する検査パターンが更新された時)
- 検査パターンの不備等、実施した定期検査に不備が発見された場合

(7) システムに対するセキュリティホールをついた攻撃を監視する

【主旨】

セキュリティホールの除去や運用制限等のセキュリティホール対策を徹底したつもりでも、その対策実施上の不備や報告されていないセキュリティホール等の潜在等で、セキュリティホールがないシステムを構築することは難しい。このような状況の下、セキュリティホールをついた攻撃による被害を受けないようにするためには、セキュリティホールをついた攻撃を監視する機能を用いた攻撃の監視と、セキュリティホールをついた攻撃と思われる不審なアクセスを拒否する機能をシステムに組込んでおくことも必要である。

【具体的な実施事項】

(1) セキュリティホールをついた攻撃監視機能の適切な適用

必要な範囲で、セキュリティホール攻撃監視機能を適用して、システムへのアクセスに対しセキュリティホール攻撃の監視を行う。

このセキュリティホールをついた攻撃の監視の適用は、マシン、あるいはソフトウェア(群)に対しては、セキュリティホール対策実施単位ごとに定められた対策要件の指定による。

セキュリティホールをついた攻撃の監視を行うためには、

- 必要な監視機能の適切な実装
- 監視条件の設定等必要な環境の適切な設定

等が必要となる。

これらの実装の管理については、**"(8)セキュリティホール対策に用いる機能を適切に実装する"**を参照。

(2) 監視結果に対する適切な処置の実施

監視機能は、セキュリティホールをついた攻撃と考えられる不審なアクセスに対し、アクセスを拒否する場合と、警告の報告に止まるものがある。このため、これらの機能を用いる場合は、システムの運用において監視結果についてのチェックを適切に行わなければ、せっかくの機能を活かせず、必要な処置を見逃すことになる。

(3) 監視結果ついての記録とその保管

セキュリティホール監視の結果については、監視要件の定めるところに従い、結果の分析や実施した処置等に関する記録の作成とその保管を行わなければならない。

(4) セキュリティホールをついた攻撃の試みまたは痕跡発見時における適切な処置の実施

セキュリティホール攻撃の痕跡が発見された場合は、その攻撃により被害が発生していないかどうかの調査を行い、必要な場合は、セキュリティホール攻撃による事故処理を行う。セキュリティホール攻撃による事故の処理については、**"(9)セキュリティホールをついた攻撃による事故に備える"**の項を参照。

【対策実施上のポイント】

(1) 外部サービスの利用によるセキュリティホールをついた攻撃の監視

セキュリティサービスベンダーによっては、リモート監視による、セキュリティホールをついた攻撃の監視サービスを提供しているところある。このようなサービスを利用することにより、レベルの高い監視を行うことができる。

（8）セキュリティホール対策に用いる機能を適切に実装する

【主旨】

セキュリティホール対策に用いられる機能としては、

- システム上のセキュリティホールを検査する機能
- セキュリティホールをついた攻撃を監視する機能

等があるが、使用する機能については、期待通りに機能し、その使用目的を満足するものでなければならない。

そのためには、技術の選択と選択した技術における使用機能の選択、インストール時の設定等を的確に行うとともに、そのインストールに対する検査も十分に行うことが必要となる。

また、セキュリティホールの検査や攻撃の監視に用いる検査パターンの適切な整備も必要となる。

また、セキュリティホール検査を外部のサービスに委託する場合においては、当該サービスの検査が、適切に機能するようにするための環境整備に不備があってはならない

【具体的な実施事項】

適用する技術の個々に対し、以下のことが求められる。

（1）適切な技術と使用する機能の選択

セキュリティホール対策のためシステムに組込む機能は、以下を満足していなければならない。

- 使用する技術（製品や方式や外部のサービス）は、検査対象ごとのセキュリティホール検査についての要件を満足するものでなければならない。
- 一般にソフトウェアや外部のサービスにはさまざまな機能が準備されており、その使い方次第で機能も異なってくる。使用するソフトウェアやサービスそのものは妥当であっても、その機能設定が、使用目的に対して不適切であってはならない。

（2）組込み場所の適切な選択

選択した技術を期待通りに機能させるためには、選択した技術のシステム構成上の配置は適切なものでなければならない。使用する技術のシステム構成上での組込み場所は、以下により決められる。

- 検査対象範囲等、セキュリティホール対策における当該技術の役割
- 当該技術の機能特性および前提とする環境条件

（3）選択した技術、機能の適切な組込み

選択した技術を期待通りに機能させるためには、技術のシステムへのインストールが適切に行われていなければならない。このためには、以下のことが求められる。

- 選択機能の的確な組込み
- テストによる動作確認の実行

システムへのインストールが終了したら、十分な機能検査を必ず実施し、インストールに不備がないことを確認すること。

(4) パターンファイルの適切なメンテナンス等の必要な運用環境の整備

システムの構成管理やシステムの運用において、OS やネットワークの環境設定等、適用した技術が前提とする環境整備に不備がないようにしなければならない。

これには、システムの導入時だけでなく、定期的な更新といったその維持管理についての処理も必要となる。

このなかでも、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メンテナンスは、特に重要となる。

セキュリティホールを使った攻撃は、日々新しい手口がどこかで創り出されていると考えなければならない。既知のセキュリティホールをついた攻撃を許さないようにするためには、検査パターンを常に最新の状態に保っておく必要がある。最新の検査パターンは、通常ファイルの形で検査ツールベンダーから提供される。検査ツールベンダーからの情報を常にチェックし、パターンファイルの更新があった場合は、速やかに対応する必要がある。

このことが適切に行われるためには、以下のことが適切に行われなければならない。

- 基準に準じたパターンファイルの更新情報の入手
- 所定の入手先から、基準に準じたサイクルでのパターンファイルの更新情報の入手
- 基準に準じたパターンファイルのメンテナンスの実施
- パターンファイル更新の記録とその保管

  パターンファイルの更新については、その記録とその保管を行い、個々のセキュリティホール検査に用いられた検査パターンの内容が、後日でも正確に把握できるようにしておく。

(5) 使用技術の実装についてのドキュメントの整備

使用技術の実装については、いつでもその設定仕様や実装の状況の把握できるようドキュメント化されていなければならない。

また、このドキュメントは、機能の新規導入時に作成するだけでなく、実装についての変更が行われたときも、適切にメンテナンスたものになっているようになっていなければならない。

【対策実施上のポイント】

(1) 採用した技術における機能の選択にあたっては、十分な検討を行うこと。使用する技術のデフォルト機能を安易に用いないこと。

(2) 独自仕様の技術を用いる場合、当該機能またはシステムの設計と実装に対し、機能の評価および実装の検査を行うことが望ましい。

(3) 使用技術の実装状況についてのドキュメントに記載すべき事項としては、以下のようなものがある。

- システム構成上の組込み場所
- 設定機能等の各種の指定内容
- 運用上の留意点
- 実装確認テストの内容と結果
- 新規組込みまたはメンテナンス日時

(9) セキュリティホールをついた攻撃による事故に備える

【主旨】

セキュリティホールの除去に努力していても、未知のセキュリティホールに対しては対処できず、また対策実施上の不備も合わせると、セキュリティホールをシステムから皆無にすることは難しく、セキュリティホールをついた攻撃を受ける可能性は、常にあると考えなければならない。

システムがセキュリティホールをついた攻撃を受けた場合、

- システムに組込まれた不正プログラムの除去
- 攻撃により改ざんまたは破壊されたシステムの復旧
- 攻撃により他サイトの攻撃の踏み台にされたような場合等における二次被害の把握と必要な対策の実施

等が適切に行われなければならない。

不正プログラムの除去が不完全だったり、影響範囲を見逃して、復旧が完全でなかったり、二次被害に対する対応が不十分であったりすると、思わぬ被害の拡大を招くことになる。また、セキュリティホールをついた攻撃を受けたことについての関係機関への届出も、漏れないようににしなければならない。

システムがセキュリティホールをついた攻撃を受けた場合における必要な処置が、適切かつ迅速に行われるようにするためには、システムがセキュリティホールをついた攻撃を受けた時の対処要領を確立しておくとともに、常日頃から、事故処理に必要となる情報やツールの整備を行っておかねばならない。

【具体的な実施事項】

(1) セキュリティホールをついた攻撃を許した時における対処要領の確立

セキュリティホールをついた攻撃を許した時における必要な処置を円滑に行えるようにするためには、事故時の対処要領を確立しておくことが必要となる。

セキュリティホールをついた攻撃を許した時の対処要領として明確にしておくべき事項としては、以下があげられる。

- 対策チームの編成
- サービスの停止の検討と実施
- 関係者へのセキュリティホールをついた攻撃を受けたことの告知
- 攻撃内容の把握
- 影響範囲の特定
- 不正プログラムの除去
- 改ざん、破壊されたソフト資産、情報資産の復旧
- 二次被害の調査と対策の検討、実施

- 原因の分析と再発防止策の検討とその実施
- 処理経緯の記録とその保管
- 関係機関への報告

(2) セキュリティホールをついた攻撃による被害への対処に必要な情報の整備

システムの構成情報や、日常のセキュリティホール対策の実施状況に関する情報等、セキュリティホールをついた攻撃による被害を受けた時の処理に必要な情報は、適切に記録、保管されていなければならない。

(3) セキュリティホールをついた攻撃による被害に備えたシステムの保全

セキュリティホールをついた攻撃による被害が発生した場合、被害から迅速にシステムや情報の復旧を実現するためには、必要なソフト資産および情報資産のバックアップが必要となる。システムや情報の復旧に必要となるバックアップの取得とその管理を適切に行うためには、セキュリティホールをついた攻撃による被害を想定したシステムの保全要領を確立しておくことが必要となる。

セキュリティホールをついた攻撃による被害に備えたシステムの保全要領の中で明確にすべき事項としては、以下があげられる。

- バックアップを取得する対象情報
- バックアップ取得サイクル
- バックアップデータからの復旧手順
- バックアップデータからの復旧手順の確立と、必要な機能の実装を行い、運用規定に反映する。なお、定められた手順通りに確実に復旧できることを確認しておくこと。
- バックアップデータの管理手順
- バックアップデータの保管場所、保管場所からの持出し手順、保管期限、保管期限経過後の処置(バックアップデータの消去ルールや方法等)を決定し、運用規定に反映する。
- 保全に必要な機能
- 事故処理訓練の実施

(4) セキュリティホールをついた攻撃による被害を想定した事故処理訓練の実施

バックアップデータを保管していても、復旧のための機能の実装不備や、運用環境の変化や、なれないことからくる操作の不手際等から、必要な時に復旧がうまく出来ないといった事態が起こりうる。このため、さまざまなセキュリティホールをついた攻撃による被害を想定した事故処理訓練を、定期的に行うことが望ましい。

また、運用訓練で発見された、セキュリティホールをついた攻撃を許した場合に備えた保全に関する処置や、システムの機能、対応運用規定，運用マニュアルの不備については、遅滞なく改善を行わなければならない。

(5) 必要なツールの整備

バックアップの取得に用いるツールや、セキュリティホールをついた攻撃を許した時の被害範囲の調査や、破壊されたシステムや情報の復旧等の処理に用いるツールは、期待通り機能しな

ければならない。

このためには、

- 適切なツールの選択とその適切なシステムへの組込み
- 運用環境の変更への対応
- ツール使用上のマニュアルの整備

等に不備がないようにしておかなければならない。

【対策実施上のポイント】

(1) セキュリティホールをついた攻撃を許した場合の対処要領における指定事項

表 4-7 に、セキュリティホールをついた攻撃を許した場合の処理手順として規定しておくべきことの内容を示す。

表 4-7 セキュリティホールをついた攻撃を許した場合の処理要領の内容

項番	項目	内容
1	処理の実施手順	・標準的な処理の流れ
2	対策チームの編成	・対策チームの編成
3	サービスの停止	・ファイルの公開停止、サービスの停止等についての考え方 ・サービス停止の手順
4	セキュリティホール攻撃を受けた事実の告知	・関係者への告知の内容、手順
5	攻撃内容の把握	・攻撃に使われたセキュリティホールの特定 ・攻撃に使われたプログラムの特性の分析による被害範囲の推定
6	被害範囲の特定	・被害範囲の調査手順 ・被害範囲の確定手順
7	システムの復旧	・改ざん、破壊されたソフト資産の復旧手順 ・改ざん、破壊された情報資産の復旧手順
8	二次被害の調査	・二次被害の調査、確定方法 ・二次被害への対処手順
9	原因の分析と再発防止策の実施	・セキュリティホールをついた攻撃の原因調査、確認手順 ・再発防止策の検討手順 ・再発防止策の実施手順
１０	処理経緯の記録	・報告書様式、内容 ・報告手順
１１	関係機関への報告	・ＩＰＡ報告への適用基準 ・ＩＰＡへの報告要領

(2) セキュリティホールをついた攻撃を把握する方法

セキュリティホールをついた攻撃を把握する方法としては、以下のようなものがある。

- システム利用履歴の解析
- ファイル改ざん検出(MD5 など)
- 最新のバックアップとの比較によるファイル改ざん検出

(3) システムへの侵入の影響調査

- システムへの侵入の形跡を発見した場合には、まず、システム上の情報の改ざん、破壊の有無を確認する。ただし、侵入者がトラップを仕掛けている場合があるので、各種コマンドの使用には十分な注意が必要である。
- 次に、各種ログを調査し、Web サーバだけなのか、DB サーバ等にも影響があるのか、情報を盗まれた形跡があるかといったような侵入者による影響範囲を調査する。
- この調査にあたっては、ログの改ざんの有無についての調査も必要である。

(4) 事故処理に必要な情報

セキュリティホールをついた攻撃による事故処理に必要な情報としては、 以下のようなものがあげられる。

- システム構成を示す情報
- システムにおける情報資産の格納状況を示す情報
- システム構成の変更履歴を示す情報
- システムにおける情報資産の更新履歴を示す情報
- セキュリティホールに関する外部情報
- 過去におけるセキュリティホール検査の実施に関する情報
- 過去におけるセキュリティホール除去の実施に関する情報

これらは、いずれも運用規定に準じて記録、保管されていなければならない。

(5) バックアップデータの取得について考え方

- バックアップ取得サイクルの決定にあたっては、復旧時間のみでなく扱うデータ量、更新頻度等も考慮の上決定すること
- バックアップの取得を行う際は、対象ファイルに対するウイルス検査を、事前に実施する
- バックアップ媒体は、安全な方法で、決められた期間保管する
- バックアップの頻度については、システムの可用性により判断する
- バックアップした日付、内容、媒体などを記録しておく
- 複数世代のバックアップデータを保存する
- 廃棄についてのルールを確立しておく

(6) セキュリティホールをついた攻撃を許した時の処置についてのその他の留意事項

- システムを緊急に停止する場合でも、メモリイメージを保存するなど、可能な限りシステムの情報を保持できるような起動(UNIX ではシングルユーザモードでの起動)で再起動した後に、分析作業に入る。これは、その後の事後対応の原因解明において重要な情報と

なりえる。

- 他組織からの事故の発生を知らされた場合、その連絡そのものが偽りの可能性も考えられる。対応をとりつつも、その連絡先と、その内容の正当性を確する作業を並行して行うこと。
- 原因の追求や対応に時間のかかる場合は、システムの運用の一時停止やネットワークの切断といった、システムへの反復攻撃を抑止するための措置を講じた上で、原因追及を行う。

(7) 関係機関への報告について

セキュリティホールをついた攻撃への対応が完了したら、その報告を行う。報告書は保管する。また経済産業大臣が指定する者へ、不正アクセスの届出を行う。

他のサイトにおける同様な被害を未然に防止するという観点からも、セキュリティホールをついた攻撃が発見された場合は、指定機関に、所定の報告を行うことが望ましい。

【参考情報】

(1) 届け出事項と連絡先

- IPA

  http://www.ipa.go.jp/SECURITY

  Security@adm.ipa.go.jp

(10) セキュリティホール対策にかかる施策をシステム運用に反映させる

【趣旨】

セキュリティホール対策にかかる諸施策が有効に機能するためには、セキュリティホール検査や、発見したセキュリティホールに対する適切な処置等、セキュリティホール対策がシステム運用に求めていることが、実際のシステム運用で適切に実行されなければならない。

このことを確実にするためには、セキュリティホール対策が運用に委ねていることが、日々の運用において的確に実施されるようにする管理上の仕組みを工夫し、これらを日常の運用に組込んでおくことが必要となる。

【具体的な実施事項】

(1) セキュリティホール対策にかかる施策の運用規定、運用マニュアルへの適切な反映

セキュリティホール対策にかかる諸施策がシステムの運用に求めていることは、システムの運用規定、運用マニュアルに適切に反映されていなければならない。

(2) 運用環境の変更への適切な対応

運用環境に以下に示すような変更が行われた場合は、セキュリティホール対策にかかるシステム運用に変更の必要がないかどうかのチェックを行う。

- セキュリティホール検査についての実施ルールや実施方法等、セキュリティホール対策にかかる具体的手段の変更
- 関係するシステム構成の変更
- システムの運用形態の変更
- セキュリティホール対策に用いている機能の変更

このチェックにより、システム運用に変更が必要となった場合は、以下の対応を適切に行わなければならない。

- 運用規定、運用マニュアルに対する必要な変更
- 必要な場合における運用スケジュールの変更等、システム運用の組立ての変更
- システム運用の変更の運用関係者への徹底

(3) セキュリティホール対策にかかる定期作業のスケジュール化

セキュリティホール対策にかかる運用処理の実行を漏れないようするためには、システム運用上定期的に実施すべき作業は、予めスケジュール化しておくことが有効である。

セキュリティホール対策に関連して、定期的な作業としてスケジュール化しておくべき作業としては、以下のようなものがあげられる。

- セキュリティホール検査ツールの見直し
- セキュリティホールに関する最新情報の反映とその実施状況のチェック
- セキュリティホール検査パターンのメンテナンスとその実施状況のチェック

- セキュリティホール検査の実施
- 各サーバに対するセキュリティホール検査実施状況のチェック
- セキュリティホール攻撃に備えたシステムの保全処理

(4) 関係する運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行

セキュリティホール対策にかかる運用作業についてのチェックリストを作成し、運用実績を記入、報告し、個々の作業が的確に実行されたことの確認を常に行うようにすることも、システムの運用から必要な処理が漏れないようにするための工夫の一つである。

(5) セキュリティホール対策にかかわる運用処理についての記録とその管理

以下に示すようなセキュリティホール対策にかかわるシステム運用上の処理については、その記録を残し管理する。

- セキュリティホール対策ツールの新規導入、機種変更、機能変更および設定の変更
- パターンファイルの更新
- セキュリティホール検査の実施とその結果に対する処理
- セキュリティホール対策にかかるシステム運用の変更

【実施対策上のポイント】

(1) セキュリティホール対策にかかる施策の運用規定や運用マニュアルへの反映手順の確立

セキュリティホール対策にかかる諸施策の運用規定や運用マニュアルへの反映を確実にするためには、これらの施策の運用規定や運用マニュアルへの反映手順を確立しておくことも必要となる。

これらの手順については、11.2 節の**"(4)セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに適切に反映する"**の項参照。

(2) セキュリティホール対策に関する運用処理のチェックリストについて

日々の運用におけるセキュリティホール対策にかかる諸施策の運用処理を、確実なものにするための実行チェックリストにあげるべき処理としては、以下のようなものがあげられる。

- セキュリティホールに関する最新情報の収集とその処理
- 検査パターンファイルの更新
- 定期セキュリティホール検査の実施
- システム構成の変更時のセキュリティホール検査
- バックアップファイルの取得

(11) 関係者に対しセキュリティホール対策についての教育を行う

【主旨】

セキュリティホール対策についての諸施策が適切に定められていても、それらが機能するためには、システムの管理や運用にかかわる者に、セキュリティホールに対する知識とその対策についての十分な理解を必要とする。

このため、セキュリティホール対策にかかわる者に対し、以下に示すようなセキュリティホール対策についての必要な教育を適切に実施することが必要となる。

【具体的な実施事項】

(1) 関係者に対するセキュリティホール対策についての教育の実施

① 定期的なセキュリティホール対策教育の実施

セキュリティホールならびにセキュリティホール対策についての教育は、定期的に行われなければならない。

② 必要に応じた臨時セキュリティホール対策教育の実施

以下のような場合は、その都度、該当者に対し実施することが必要である。

- 異動によりセキュリティホール対策関係者の入れ替えが合った場合
- セキュリティ対策の規準やその運用が変更された時
- セキュリティホール対策に問題が生じた場合

(2) セキュリティホール対策についての教育カリキュラムの確立

セキュリティホールとセキュリティホール対策についての教育を効果的に行うためには、教育科目とその内容、対象者と受講サイクル、実施時期等を定めた教育カリキュラムを確立しておくことが望ましい。

教育すべき内容としては、以下があげられる。

- セキュリティホールとセキュリティホール対策の概要
- セキュリティホール対策の詳細とその実施要領
- セキュリティホール対策に用いる技術とその運用
- セキュリティホールに関する事故事例

また、教育内容は、サイトの運営形態やシステム構成、運用形態、さらには技術環境の進化を反映した、運用対象システムの実態に合ったものであるよう、適時更新がなされなければならない。

(3) セキュリティホール対策に関する教育テキストの整備

セキュリティホール対策に関する教育をより効果的にするためには、サイトの運営環境に合ったテキストを準備することが望ましい。

また、このテキストについてもサイトの運営形態の変更を反映するよう定期的な見直しを行うこ

とが望ましい。

【対策実施上のポイント】

(1) セキュリティホール対策についてのカリキュラム例

表 4-8 に、セキュリティホール対策についての教育カリキュラムの一例を示す。

表 4-8 セキュリティホール対策についての教育カリキュラム例

項番	教育項目	教育対象者	頻度
1	セキュリティホールとセキュリティホール対策の概要 ・セキュリティホールとその脅威の概要 ・セキュリティホール対策についての取組み ・セキュリティホール対策の概要	・セキュリティホール対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	1回／年
2	セキュリティホール対策の詳細とその実施要領 ・各種関係基準 ・運用規定、運用マニュアル上の関係事項 ・その他注意事項	・セキュリティホール対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	1回／年
3	セキュリティホール対策に用いる技術とその運用 ・セキュリティホール検査技法（含むツールの操作） ・セキュリティホール除去技法（含むツールの操作） ・セキュリティホール対策ツールのメンテナンス	・セキュリティホール対策関係者 ・システム開発関係者 ・システム管理関係者	1回／年
4	セキュリティホールに関する事故事例	・セキュリティホール対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	1回／年 ＋ 随時

(12) セキュリティホール対策の実施状況についての監査を行う

【主旨】

セキュリティホール対策にかかる施策が定められその実施についての管理が行われていても、完全はありえない。一方、セキュリティホール対策の不備は、サイトのセキュリティに直接的な脅威となるため、セキュリティホール対策の不備が問題をおこす前に、問題点を発見し適切な改善策を講じることができるようにしておくことも重要である。

このため、セキュリティホール対策として定められていることが、サイトの運営実態に照らして適切かどうか、また、セキュリティホール対策として定められている諸施策が適切に実施されているかどうか等についてのチェックを行し、問題点の摘出と必要な改善を指導するセキュリティホール対策の実施状況についての監査を行うことも必要である。

また日常の運用の中で、実施したセキュリティホール対策に関する運用についての記録の保管等、この監査のための準備を組込んでおくことも必要となる。

特に、EC サイトサービスを事業として提供しているモール等では、その責任からみても、セキュリティホール対策の実施状況に関する監査の実施は必須である。

(注) 正式な監査という形はとらなくとも、ここに示すようなセキュリティホール対策の実施状況についてのチェックは、組織的に行われるべきものである。

【具体的な実施事項】

(1) セキュリティホール対策の実施状況についての定期的な監査の実施

最低でも年1回は、以下に示すような事項をチェックする、セキュリティホール対策の実施状況についての監査を行う。

- セキュリティホール対策についての責任体制の整備状況とその機能状況
- セキュリティホール対策実施基準の妥当性
- セキュリティホールに関する最新情報の収集とその処理の状況
- 定期的なセキュリティホール検査の実施状況
- 必要に応じた臨時セキュリティホール検査の実施状況
- セキュリティホール対策に使用している機能の実装状況
- セキュリティホールをついた攻撃による事故への備えの状況
- セキュリティホール対策にかかる施策のシステム運用への反映状況
- 関係者のセキュリティホールとセキュリティホール対策についての認識とスキルレベル

(2) 監査実施要領の確立

セキュリティホール対策の実施状況についての定期的な監査が、円滑に実施され、かつ実効的なものにするためには、監査についての実施要領が確立されていることが望ましい。

監査実施要領で規定しておく事項については、1.2.2 節の(4)項を参照。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。

このためには、監査指摘事項に対する改善措置が実際にとられたか否かについての確認を行うことも必要であり、監査指摘事項についてのフォローの仕組みも、監査要領の中に組込んでおくことも有効である。

【対策実施上のポイント】

(1) 監査内容例

表 4-9 に、セキュリティホール対策の実施状況についての監査において、監査すべき事項の例を示す。

表 4-9 セキュリティホール対策の実施状況に関する監査におけるチェック事項

項番	監査項目	監査の内容等
1	セキュリティホール対策についての責任体制の整備状況とその機能状況	・セキュリティホール対策に関する責任体制は、サイトの運営実態に照らして適切か ・セキュリティホール対策に関する責任者の自己の責任についての認識は十分か ・セキュリティホール対策に関する責任体制は機能しているか
2	セキュリティホール対策実施基準の妥当性	・セキュリティホール対策実施基準は、サイトの技術環境、運用環境等のサイトの運営実態に照らして適切か
3	セキュリティホールに関する最新情報の収集とその処理状況	・セキュリティホールに関する最新情報の収集とその処理についての適切なルールは確立しているか ・セキュリティホールに関する最新情報の収集は、ルールに沿って適切に行われいるか ・収集した情報に対する処理は適切に行われているか
4	定期的セキュリティホール検査の実施状況	・定期セキュリティホール検査は、セキュリティホール対策基準に沿って適切に行われているか （対象範囲すべてに対する漏れない実施の確認） ・セキュリティホール検査結果に対する処置は適切に行われているか

表 4-9　セキュリティホール対策の実施状況に関する監査におけるチェック事項

項番	監査項目	監査の内容等
5	必要に応じた臨時セキュリティホール検査の実施状況	・必要な場合における臨時セキュリティホール検査は、セキュリティホール対策基準の沿って行われているか（必要時における、対象範囲すべてに対する漏れない実施の確認） ・検査結果は適切に処理されているか
6	セキュリティホール検査に使用している機能の実装状況	・セキュリティホール対策に用いる技術およびその機能選択は妥当か ・その実装の正確性は確認されているか（実装すべき場所に正確に実装されているか） ・運用環境の変更時における対応機能の実装の見直しは行われているか ・必要な運用環境の整備状況についてのチェックは適切に行われているか
7	セキュリティホールをついた攻撃による事故への備えの状況	・セキュリティホールをついた攻撃を受けた時に備えた保全要領が、サイトの運営実態に照らして適切に決められているか ・必要な保全処理は適切に行われているか ・セキュリティホールをついた攻撃を受けた時の対処要領は適切に決められているか ・監査期間中におけるセキュリティホールをついた攻撃を受けた時の処理は妥当であったか
8	セキュリティホール対策に関する施策のシステム運用への反映状況	・セキュリティホール対策にかかる諸施策は運用規定、運用マニュアルに適切に反映されているか ・これらの運用は、日々の運用において確実に実行されているか、また、そのことは管理されているか ・セキュリティホール対策にかかわるシステム運用の適切な実行を実現するための工夫は十分か
9	関係者のセキュリティホールとセキュリティホール対策に関する認識とスキルレベル	・セキュリティホールならびにセキュリティホール対策についての認識は十分か ・セキュリティホール対策担当者のセキュリティホール対策にかかわるスキルは十分か ・関係者へのセキュリティホール対策教育は適切か

(2) 監査の報告

監査結果は、セキュリティホール対策責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告されなければならない。

5 ウイルス対策の徹底

5.1 必要な施策項目

図 5-1 に、ウイルス対策としての施策の体系を示す。

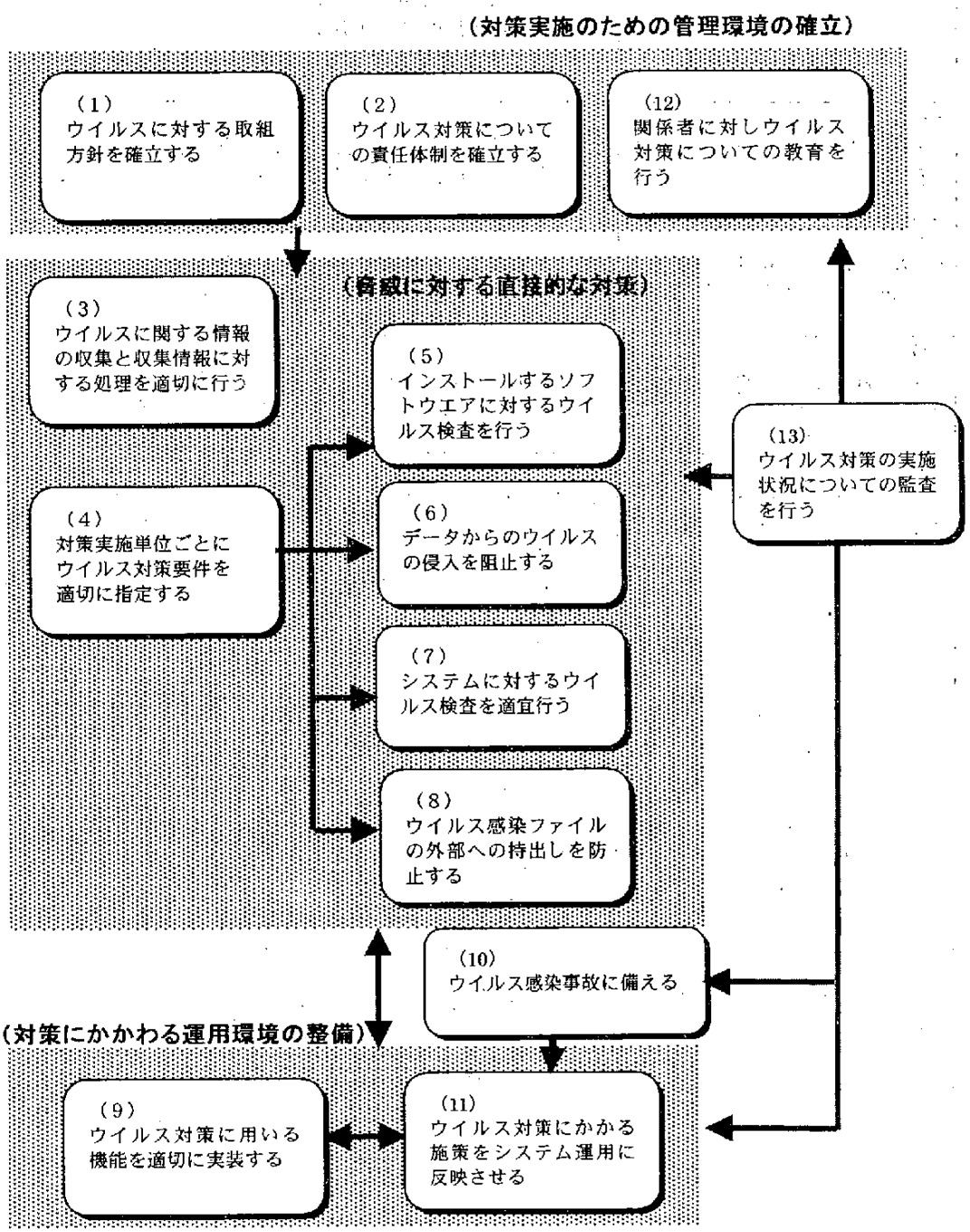


図 5-1 ウイルス対策の組立て

また、表 5-1 に各施策における実施事項の一覧を示す。

表 5-1　ウイルス対策としての具体的実施事項一覧

施策名	具体的実施事項
(1) ウイルスに対する取組方針を確立する	① ウイルス対策の目標の明確化 ② 適用範囲を明確化 ③ ウイルス対策実施基準の確立 ④ ウイルス対策の組立て明確化 ⑤ ウイルスに対する取組み方針の関係者への周知
(2) ウイルス対策についての責任体制を確立する	① ウイルス対策についての責任体制の明確化 ② ウイルス対策関係者間の連携体制の確立
(3) ウイルスに関する情報の収集と収集情報に対する処理を適切に行う	① ウイルスに関する情報の収集とその処理要領の確立 ② ウイルスに関する情報の収集と収集情報に対する処理の実施
(4) 対策実施単位ごとにウイルス対策要件を適切に指定する	① 対策実施単位ごとのウイルス対策要件の指定 ② ウイルス対策要件の指定に関するドキュメントの整備
(5) インストールするソフトウェアに対するウイルス検査を行う	① ウイルス対策の視点からのソフトウェアの採用に関するルールの確立 ② 新しくシステムにインストールするソフトウェアに対する素性確認の実施 ③ 新しくシステムに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 ④ 実施したウイルス検査についての記録と保管 ⑤ ウイルス発見時の適切な処置の実施
(6) データからのウイルスの侵入を阻止する	① ウイルス対策の視点からの外部からの受取りデータの取扱いに関するルールの確立 ② 外部からの受取りデータに対する素性確認の実施 ③ 外部からの受取りデータに対するウイルス検査の実施 ④ 実施したウイルス検査についての記録と保管 ⑤ ウイルス発見時の適切な処置の実施
(7) システムに対するウイルス検査を適宜行う	① 定期的なウイルス検査の実施 ② 必要に応じた臨時ウイルス検査の実施 ③ 実施したウイルス検査についての記録と保管 ④ ウイルス発見時の適切な処置の実施

表 5-1　ウイルス対策としての具体的実施事項一覧

施策名	具体的実施事項
(8) ウイルス感染ファイルの外部への持出しを防止する	① ウイルス対策の視点からの外部持出しデータの取扱いに関するルールの確立 ② 外部に持出すデータに対するウイルス検査の実施 ③ 実施したウイルス検査についての記録と保管 ④ ウイルス発見時の適切な処置の実施
(9) ウイルス対策に用いる機能を適切に実装する	① 適切な技術と使用機能の選択 ② 組込み場所の適切な選択 ③ 選択した機能の的確なインストール ④ ウイルスパターンファイルのメンテナンス等の必要な運用環境の整備 ⑤ 使用技術の実装についてのドキュメントの整備
(10) ウイルス感染事故に備える	① ウイルス感染事故に対する対処要領の確立 ② ウイルス感染事故への対処に必要な情報の整備 ③ ウイルス感染事故による被害に備えたシステムの保全 ④ ウイルス感染事故を想定した事故処理訓練の実施 ⑤ 必要なツールの整備
(11) ウイルス対策にかかる施策をシステム運用に反映させる	① ウイルス対策にかかる施策の運用規定、運用マニュアルへの反映 ② 運用環境の変更への適切な対応の実施 ③ ウイルス対策にかかる定期作業のスケジュール化 ④ 関係運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行 ⑤ ウイルス対策にかかる運用処理についての記録と保管
(12) 関係者に対しウイルス対策についての教育を行う	① ウイルス対策教育の実施 ② ウイルス対策に関する教育カリキュラムの確立 ③ ウイルス対策教育テキストの整備
(13) ウイルス対策の実施状況についての監査を行う	① ウイルス対策の実施状況についての定期的な監査の実施 ② 監査実施要領の確立 ③ 監査指摘事項に対するフォローの実施

5.2 個別具体策

(1) ウイルスに対する取組方針を確立する

【主旨】

サイトシステムのウイルス感染の阻止を図るとともに、ウイルス感染時の被害を限定的なものにすることに組織的に取組むには、関係者がウイルスに関する必要な知識を持つとともに、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確立し、これを、ウイルス対策に直接関係する者だけでなく、システムの構築や運営に関係する者、さらにはシステムに触れる者すべてに周知させておくことが必要となる。

【具体的な実施事項】

(1) ウイルス対策の目標の明確化

ウイルス対策が目標とするところを明確にし、ウイルス対策に関する施策の意図を明確にする。ウイルス対策の目標としては、以下があげられる。

- サイトシステムのウイルス感染の防止
- ウイルス感染事故発生時の被害の極小化
- 一般消費者や他サイト等外部のシステムへのウイルスの伝染の阻止

(2) 適用範囲の明確化

ウイルス対策の適用範囲として、以下を明確にする。

- サイトのシステム構成上の対象となる領域及び対象サーバ等の機器
- 対象とするファイル
- 対象とする通信
- 対象とする組織

ウイルス対策は、サイトシステムを構成する機器だけでなく、サイトシステムで用いらる電子媒体等も関係するため、その規定が及ぶ範囲の明確化は重要である。

(3) ウイルス対策実施基準の確立

ウイルス対策の基本は、ワクチン等ウイルス対策ソフトの活用によるウイルスの感染防止と、感染防止策をかいくぐって感染してきたウイルスの早期発見や駆除にある。これらは、対象とするソフトやファイルに対する漏れのないウイルス検査や、検査が使用するウイルスパターンファイルのきめ細かいメンテナンスの実施密度に依存している。

しかし、サイト全体に対し密度の高い対策を一律に行うことは、運用上相当の負担が伴う。このため、運用現場が運用上の負担に負けて、その実行を疎かにし、その結果として、ウイルスの感染を許したり、感染したウイルスを見逃したりして、ウイルス被害を拡大させてしまうことが多い。

実際に実施するウイルス対策は、機器(サーバ)またはソフトウェア単位に決めなければならないが、これらを運用負担とバランスが取れた実効的なものにするとともに、サイト全体で整合性のあるものにしなければならない。このためには、実施するウイルス対策に厳格さによるレベル分けを行い、それぞれのレベルに対する標準的な対策要件を定義したウイルス対策実施基準を確立しておき、対象機器(サーバ)またはソフトウェアの個々に適用する対策レベルを割当て、そのレベルに指定されている対策要件に準じた対策を実施するような工夫も必要となる。

このウイルス対策実施基準は、後述のウイルス検査のベースとなる。

ウイルス対策実施基準として、定義すべき事項としては、以下をあげることができる。

- 対策レベル名称
- 当該対策レベルが求める対策実施密度
- 当該対策レベルの適用範囲
- ウイルス検査の実施要件
- ウイルス駆除の実施要件

ウイルス検査や駆除の実施要件は、対象とする機器等のサイト運営上の重要度に依存する。ウイルス対策は、このウイルス対策実施基準に準じて実施されなければならない。

(4) ウイルス対策の組立ての明確化

ウイルス対策をどのように行うかを明らかにするもので、実施する施策の構成と、施策間の関係を示す。

本ガイドラインにおけるウイルス対策に関する施策の組立てについては、は、5.1 節参照。

(5) ウイルスに対する取組方針の関係者への周知

ウイルスに対する取組方針は文書化されるとともに、ウイルス対策に直接かかわる者の他、システムの構築ならびに運用関係者、さらには業務でシステムに触れる者のすべてに周知させておかなければならない。このためには、

- ウイルスに対する取組方針の掲示や配布
- 関係者間での定期的なウイルスに対する取組方針の再確認

が必要となる。

【対策実施上のポイント】

(1) ウイルス対策実施基準の定義要領

ウイルス対策実施基準を定義するにあたって指定すべき事項を、表 5-2 に示す。

表 5-2　ウイルス対策実施基準における定義項目

項番	定義項目	定義内容
1	対策レベル名称	・当該対策レベルの名称とID
2	当該対策レベルに求めるウイルス対策の実施密度	・対象領域におけるウイルスの存在についての容認の程度で表わす目標とするウイルス対策の成果(注1)
3	当該対策レベルの適用範囲	・当該対策レベルを適用する機器、あるいはソフト、ファイル
4	ウイルス検査の実施要件	・当該対策レベルに求められるウイルス検査の時点またはサイクル ・ウイルス検査パターンの要件(注2)
5	ウイルス駆除の実施要件	・報告されたウイルスの駆除実施のタイミング(注3)

(注1) ウイルス対策の実施密度の定義方法例
- 常時、既知のウイルスはすべて対策済
- 危険度の高いウイルスは、すべて常時対策済とするが、それ以外のウイルスについては、二週間以内に限りその存在を容認
- 未対策のウイルスすべてについて、1ヶ月はその存在を容認

(注2) 使用するウイルス対策検査パターンについての要件の定義例
- 既知のウイルスすべてに対応
- 危険度の高いウイルスについてはすべて対応、それ以外のウイルスについては、二週間前のパターンで可
- 定期メンテナンスのパターンで可

(注3) ウイルス除去の実施要件の定義例
- 発見したウイルスの全てに対し即時駆除の実施
- 危険度の高いウイルスに対しては、即時駆除を実施、それ以外の未対策ウイルスに対しては二週間以内に対策実施
- 未対策ウイルスのすべてについて、毎月の定期メンテナンスで対策

(2) ウイルスの危険度についての考え方

ウイルスの危険度とは、そのウイルスが侵入した場合の、サイトに与える影響の大きさの尺度を示すもので、求めるウイルス対策レベルを決める時の判断材料となるものである。ウイルスの危険度は、その構造的な特性とサイトシステムの構成の組合せからくる、攻撃を受ける確率と、そのウイルスがもたらしうる被害による。

このウイルスの危険度についてクラス化を行い、各対策対象機器(サーバ)またはソフトにおけるウイルス対策実施の要否および実施タイミングの判断の基準として用いるようにすることも、サイト全体におけるウイルス対策を整合性のあるものにすることに有効である。

表 5-3 に、ウイルスの危険度クラスの定義例を示す。

表 5-3　ウイルスの危険度クラスの定義例

項番	危険度クラス	危険の程度
1	クラスA	・感染したときの被害は大きく、かつ、当該サイトの特性から、 機器によっては感染の可能性の高いウイルス
2	クラスB	・感染したときの被害は大きいものの、当該サイトの特性から、感染の可能性は、そう高くないウイルス
3	クラスC	・感染してもその被害は限定的であるが、当該サイトの特性から、機器によっては、感染の可能性が高いウイルス
4	クラスD	・感染しても被害は限定的で、かつ、感染の可能性も低いウイルス
5	クラスE	・感染しても実害はないが、感染の可能性の高いウイルス
6	クラスF	・感染しても実害はないし、感染の可能性も低いウイルス

(3) ウイルス対策実施基準の定義例

表 5-4 に、ウイルス対策実施基準の定義例を示す。

(4) ウイルス対策実施基準の適用について

ウイルスの検査や駆除のウイルス対策の実施は、保護対象のソフトやファイル毎に検討しなければならない。ただし、各ソフトやファイルにおいて、求められるウイルス対策密度は、それが配置される機器に同居している他のサービスへの影響も配慮して決めなければならない。このため、同じソフトやファイルでも、配置される機器によって異なったものになることがある。

(5) ウイルスに対する取組方針は、システム構成やその運用形態等、システム運用の実環境の変化に対応して必要な修正が加えられるべきであり、必要に応じて見直しを行うこと。

(6) ウイルスに対する取組方針は、定期的に関係者間で再確認することをルーチン化しおくことが望ましい。

表 5-4　ウイルス対策実施基準の定義例

項番	対策レベル	当該対策レベルにおける標準的な対策要件
1	レベルA	・対策の実施密度・・・・・・・・・常時、すべての既知のウイルスは存在しない ・適用対象・・・・・・・・・・・・・・・サイト全体に直接大きな影響を与えるサーバ 外部に影響を与える可能性のあるサーバ ・ウイルス検査の実施要件・・最新パターンによる月2回以上のウイルス検査の実施 新しいウイルスが報告された都度、そのウイルスに対する臨時検査の実施 ・ウイルス駆除の実施要件・・ウイルス検出時に即時に実施 ・ウイルス侵入監視用件・・・・入力データに対し、常時実施 検査パターンは常に最新情報を反映
2	レベルB	・対策の実施密度・・・・・・・・・新しく報告されたウイルスに関しては、危険度クラスA、B、Cを除いては、2週間の定期検査期間中は容認 ・適用対象・・・・・・・・・・・・・・・サイト全体への影響が比較的大きいサーバ ・ウイルス検査の実施要件・・最新パターンによる月2回以上のウイルス検査の実施 危険度A, B, Cの新しいウイルスが報告された都度、そのウイルスに対する臨時検査の実施 ・ウイルス駆除の実施要件・・ウイルス検出時に即時に実施 ・ウイルス侵入監視用件・・・・入力データに対し、常時実施 検査パターンは、危険度A, B, Cの新しいウイルスには対応
3	レベルC	・対策の実施密度・・・・・・・・・すべての新しいウイルスに対しては、2週間の定期検査サイクル間は容認 ・適用対象・・・・・・・・・・・・・・・外部へは影響を及ぼさないものの、業務やサイトの運用への影響が大きいことが懸念されるサーバ ・ウイルス検査の実施要件・・最新パターンによる月2回以上のウイルス検査の実施 特別の場合を除いては、臨時検査は不要 ・ウイルス駆除の実施要件・・ウイルス検出時に即時に実施 ・ウイルス侵入監視用件・・・・できれば、入力データに対し常時実施 検査パターンは最低2週間ごとに最新版に更新
4	レベルD	・対策の実施密度・・・・・・・・・すべての新しいウイルスに対しては、1ヶ月の定期検査サイクル間は容認 ・適用対象・・・・・・・・・・・・・・・外部への影響はなく、業務やサイトの運用への影響も大きくないもサーバ ・ウイルス検査の実施要件・・最新パターンによる月1回以上のウイルス検査の実施 特別の場合を除いては、臨時検査は不要 ・ウイルス駆除の実施要件・・ウイルス検出時に即時に実施 場合によっては、2週間の猶予可 ・ウイルス侵入監視用件・・・・特に不要

(2) ウイルス対策についての責任体制を確立する

【主旨】

ウイルス対策をその取組方針に沿って機能させるためには、ウイルス対策として定められていることが、システムの構築や運用に適切に反映されるよう、指導、管理する責任体制の確立が必要となる。

このためには、ウイルス対策にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) ウイルス対策についての責任体制の明確化

ウイルス対策についての責任体制に関し、明確にしておくべきこととしては以下があげられる。

- ウイルス対策の責任者とその責任
- ウイルス対策実施担当者の責任
- システム開発者のウイルス対策に関する責任
- システム管理者のウイルス対策に関する責任
- システム運用者のウイルス対策に関する責任

(2) ウイルス対策関係者間の連携体制の確立

ウイルス対策に関する責任体制を有効に機能させるためには、関係者間の連携が重要となる。

【対策実施上のポイント】

(1) ウイルス対策関係者の責任分担

表 5-5 に、ウイルス対策関係者の責任分担の定義例を示す。

(2) ウイルス対策にかかる責任体制は、ウイルス対策を変更したり、サイトの運営境に変更が生じた場合は、見直しを行い、必要な変更を行うこと。

表 5-5　ウイルス対策関係者の責任分担

責任区分	タスク
ウイルス対策責任者	・ウイルスに対する取組方針の確立と関係者への周知 ・ウイルス対策実施基準の発行 ・ウイルス対策全体の妥当性の維持 ・ウイルス対策の実施状態のチェック ・対策実施基準に沿ったウイルス対策の実施の指導 ・ウイルス感染事故発生時の事故処理の指揮
ウイルス対策実施担当者	・ウイルス対策の詳細の検討 ・ウイルスに関する最新情報の入手とその処理 ・ウイルス対策の実施状況の把握 ・システム上の未対策ウイルスの把握 ・ウイルス検査に用いる機能の適切なシステムへの組込みと必要な環境整備 ・ウイルス検査パターンのメンテナンスの管理 ・ウイルス検査結果の確認と検査結果に対する適切な処理の決定 ・ウイルス駆除計画の決定と指示および実行確認 ・ウイルス攻撃の監視 ・ウイルス感染事故発生時における事故処理と再発防止策の検討
システム開発者	・開発システムにおけるウイルス対策関係機能の適切な組込み 　－設計の妥当性の確認 　－正確な実装の確認 ・開発ソフトにおけるウイルス不在の保証
システム管理者	・ウイルス駆除作業の実施 ・ウイルス対策に用いる機能の維持 　－必要なシステム構成の変更の反映の管理 　－使用機能の動作環境の維持管理 ・ウイルス検査に用いるパターンファイルのメンテナンス ・システムにおける対応機能の実装状況の正確な把握
システム運用者	・ウイルス対策に用いる機能が必要とするシステム運用環境の整備 ・システムへの導入機器、ソフトにに対するウイルス対策実施基準に沿ったウイルス検査の実施 ・受取ファイルに対するウイルス検査の実施 ・外部持出しファイルに対するウイルス検査の実施 ・必要な場合における臨時ウイルス検査の実施

(3) ウイルスに関する情報の収集と収集情報に対する処理を適切に行う

【主旨】

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を見逃すことになるため、さまざま情報源からウイルスに関する最新情報の収集に努めるとともに、収集した情報の分析を適切に行い、ウイルス対策に適切に反映することが重要である。

このため、ウイルスに関する最新情報の収集と、入手した情報に対する処理を適切に行うための仕組みを確立しておくことも必要となる。

【具体的な実施事項】

(1) ウイルスに関する情報の収集とその処理要領の確立

ウイルスに関する最新情報を漏れなく収集し、これらの情報が有効かつタイムリーに活用されるようにするためには、以下に示すようなことを定めたウイルスに関する情報の収集とその処理要領を確立しておく必要がある。

- 情報の収集とその処理に関する責任者
- 情報収集源
- 収集サイクル
- 収集すべき情報の内容
- 収集した情報の処理手順
- 収集した情報とその処理に関する記録とその保管

(2) ウイルスに関する情報の収集と収集情報に対する適切な処理の実施

ウイルスに関する情報の収集とその処理要領に従って、ウイルス関連情報の情報を収集するとともに、指定された手順に従い、収集した情報に対する処理を行い、必要な場合は、ウイルス対策実施基準に従ったウイルス対策を実施しなければならない。

これらの処置の確実な実行を管理する仕組みを、日々のシステム運用の中に組込んでおくことも必要である。

【対策実施上のポイント】

(1) 収集したウイルス関する情報の処理手順の定義

収集情報に対する処理手順の中でその考え方と進め方を明確にしておくべきこととしては、以下があげられる。

- 収集した情報に対する対応(評価、検査、駆除)実施の責任者
- 新しく報告されたウイルスに対する検査、駆除実施の要否の判断
- 問題となるウイルスを評価、検査、駆除するまでの間のサービスの制限等の運用制限の

要否と、実施範囲の設定、及びその実施

- 問題となるウイルスの検査、駆除の実施計画の立案
- 計画されたウイルス検査、除去の実行確認

(2) ウイルスに関する情報の収集は、可能な限り短いサイクルで行うべきである。できれば、毎日新しい情報がないかどうかのチェックを行うことが望ましい。

(3) 収集した情報から、ウイルス検査及び駆除処理の実行が必要と判断されても、運用上の都合等により、すぐに対策できない場合もある。このような場合、対策が実施されるまでの期間、システムに脆弱性が存在していることを認識し、サービスの制限等の運用上処置を適切に施さなければならない。

【参考情報】

ウイルス関連情報の入手先を、以下に例示する。

① 公的機関

- 情報処理振興事業協会(IPA)
  http://www.ipa.go.jp/security/index.html
  - パソコン・ユーザのためのコンピュータウイルス対策7箇条
    http://www.ipa.go.jp/security/antivirus/7kajo.html
  - コンピュータウイルス対策基準(通商産業省第952号)
    http://www.ipa.go.jp/security/antivirus/kijun535.html

② セキュリティサービスベンダー

- 株式会社シマンテック・・・・・・・・・・・・・・・・・・http://www.symantec.co.jp/
- コンピュータ・アソシエイツ株式会社・・・・・・・http://www.caj.co.jp/
- トレンドマイクロ株式会社・・・・・・・・・・・・・・・http://www.trendmicro.co.jp/
- 日本エフ・セキュア株式会社・・・・・・・・・・・・http://www.f-secure.co.jp/
- 日本ネットワークアソシエイツ株式会社・・・・・http://www.nai.com/japan/

③ 民間団体

- ワクチンバンク・・・・・・・・・・・・・・・・・・・・・・・・http://www.vaccinebank.or.jp/
- 日本コンピュータセキュリティ協会(JCSA)・・・http://www.jcsa.or.jp/

(4) 対策実施単位ごとにウイルス対策要件を適切に指定する

【主旨】

ウイルス対策を適切に行うためには、ウイルス検査や発見したウイルスの駆除等のウイルス対策処理を行う単位としての機器、ソフト、ファイル(群)ごとに、これらをどのような条件の下にどのように行うのかが、ウイルスに対する取組方針の中で定められたウイルス対策実施基準に沿って適切に決められていなくてはならない。

この対策要件の設定にあたっては、対策処理の実施単位ごとにウイルス感染事故が発生した時の影響の大きさを考慮する。

【具体的な実施事項】

(1) 対策実施理単位ごとのウイルス対策要件の設定

ウイルスの検査、侵入監視、駆除等のウイルス対策処理の実行単位となる機器やソフトウェア(群)やファイル(群)ごとに、これらをどのように行うのかについて、以下に示すようなことを指定する。

- 対策対象名称
- 対策対象に含まれるソフトウェア、ファイル
- 対策対象に適用する対策レベル
- ウイルス検査の実施に関する要件
- ウイルス侵入監視に関する要件
- ウイルス発見時の対応方法
- 保全要件

また、この個々の対策実施単位に決められたウイルス対策要件は、システムの構成やウイルス対策実施基準等にウイルス対策の実施方法に影響を与えるような変更が生じた場合は、その見直しを行い、必要な変更を行わなければならない。

(2) ウイルス対策要件の指定に関するドキュメントの整備

ウイルス対策が適切に行われているかどうかについて、管理が適切に行えるように、個々のウイルス対策対象単位ごとに定めた対策要件についてのドキュメントの整備を行い、何時でも正確にその指定内容が把握できるようにしておくことも必要である。

このドキュメントに記載すべき事項は、個々のウイルス対策の実施単位に対する、(1)項であげた項目となる。

また、このドキュメントは、システムの構成やウイルス対策実施基準等の変更に伴う対策要件の変更が、適切に反映されたものになっているようになっていなければならない。

【対策実施上のポイント】

(1) 個々の対策実施単位に指定するウイルス対策要件の定義要領

表 5-6 に個々の対策実施単位に指定するウイルス対策要件で指定すべき事項を示す。

表 5-6 個々の対策実施単位に指定するウイルス対策要件定義における指定項目

項番	定義項目	定義内容
1	対策対象名称	・当該対策対象単位の名称、ID
2	対策対象に含まれるソフトウェア、ファイル	・当該対策対象単位に含まれるソフトウエア、ファイル名 ・それぞれの構成ソフトウェア、ファイルに求められるウイルス対策レベル
3	対策対象に適用する対策レベル (注1)	・当該対策対象単に適用するウイルス対策レベル (当該対策対象単位に含まれるソフトウェア、ファイル個々に求められる対策レベルのうち最も高いレベルを指定)
4	ウイルス検査の実施に関する要件 (注2)	・定期ウイルス検査の実施サイクル ・臨時ウイルス検査が必要な場合 ・これらのウイルス検査に用いる検査パターンの条件
5	ウイルス侵入監視に関する要件 (注3)	・ウイルス侵入監視の内容(どのような内容の監視を行うかを明示) ・使用技術と使用する機能(使用する技術の概要と、その機能設定要件) ・ウイルスの侵入監視に用いる検査パターンの条件
6	ウイルス発見時の対応方法 (注4)	・発見ウイルスの駆除実施のタイミング
7	保全要件	・バックアップの取得要件 ・バックアップの取得サイクル ・バックアップ管理要件

(注1) ウイルス対策実施基準参照

(注2) ウイルス対策実施基準に定める、当該対策レベルに対するウイルス検査に関する要件を基準に決定

(注3) ウイルス対策実施基準に定める、当該対策レベルに対するウイルス侵入監視に関する要件を基準に決定

(注4) ウイルス対策実施基準に定める、当該対策レベルに対する発見ウイルスの駆除実施に関する要件を基準に決定

(2) ウイルス対策実施単位の編成

求めるレベルのウイルス対策を効率的に行うためには、ウイルス対策実施単位が適切に編成されていなくてはならない。ウイルス対策実施単位の編成にあたって考慮することをあげると以下のようになる。

- ツールの機能範囲と性能
- 対策対象ソフトウェア、ファイルに求められる対策レベルの組合せ
- 運用負担

(3) バックアップデータの取扱いについて考え方

- バックアップバックアップ取得サイクルの決定にあたっては、復旧時間のみでなく扱うデータ量、更新頻度等も考慮の上決定すること
- バックアップ媒体は、安全な方法で、決められた期間保管する
- バックアップの頻度については、システムの可用性により判断する
- バックアップした日付、内容、媒体などを記録しておく
- 複数世代のバックアップデータを保存する
- 廃棄の手順を明確にしておく

(5) インストールするソフトウェアに対するウイルス検査を行う

【主旨】

ウイルス対策の第一歩は、ウイルスに感染したソフトをシステムにインストールしないことにある。

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らない。また、ワクチンを用いたウイルス検査では発見が難しいトロイの木馬的なウイルスの侵入を阻止するため、素性のはっきりしないソフトウェアの導入を避ける措置も重要となる。

【具体的な実施事項】

(1) ウイルス対策の視点からのソフトウェアの採用に関するルールの確立

危険性の高い出所のはっきりしないソフトウェアをシステムに組込んでしまうことを避けるための措置が確実に行われるようにするためには、ウイルス対策の視点からの新しいソフトウェアの導入に関するルールを確立しておくことが必要となる。

このルールの中で明確にしておくべきこととしては、以下をあげることができる。

- 適用対象
- ソフトウェアの素性の審査と評価
- ウイルス検査済みの確認
- 導入の承認
- 導入前のウイルス検査の実施
- 導入時検査に関する記録とその保管

(2) 新しくシステムにインストールするソフトウェアに対する素性確認の実施

新しくシステムに組込むソフトウェアに対しては、前項で示すウイルス対策の視点からのソフトウェアの導入についてのルールに従い、ウイルス対策責任者による、

- ソフトウェアの素性の確認と評価
- ウイルス検査済みの確認
- システムへの導入の承認

を行わなければならない。

(3) 新しくシステムに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

(2)の素性確認をパスしたソフトウェアに対して、システムへのインストールに先立ってウイルス検査を実施し、検査に用いたパターンの範囲ではウイルスがないことを確認する。

この検査で用いる検査パターンは、当該ソフトウェアがインストールされる機器またはソフトウェア群であらわされるウイルス対策実施単位に求められる対策レベルに対し定められているところに従うものとする。

(4) 実施したウイルス検査についての記録と保管

素性審査やウイルス検査にパスしてシステムにインストールされるソフトウェアについては、ウイルス対策の視点からのソフトウェアの導入についてのルールに従い、これらの審査、検査についての記録を行い、保管する。

(5) ウイルス発見時の適切な処置の実施

ウイルスが発見された場合は、そのソフトウェアのシステムのインストールを拒否し、破棄を行う。発見ウイルスを駆除してインストールし使用することは避け、ウイルスに感染していないソフトウェアを、開発元から新たに入手すべきである。

【対策実施上のポイント】

(1) ウイルス対策の視点からのソフトウェアの導入についてのルールの適用対象について

このルールは、一つのアプリケーション全体、アプリケーションの一モジュール、マクロ等その構造を問わず、サイトシステムに組込まれるすべてのソフトウェアに対し、以下のような場合に適用しなければならない。

- 新しい機器をシステムに組込む場合、もしくは一部を交換する場合
- 新しいソフト(パッケージソフト、開発ソフト)一式をシステムにインストールする場合、もしくは一部を交換する場合

また、このルールは、自社開発ソフト、外部に開発委託を行ったソフト、購入ソフトのすべてを対象とする。

(2) 導入ソフトウェアの素性審査について

導入ソフトに対する素性審査におけるチェックポイントとしては、以下があげられる。

- 開発元ははっきりしているか
- 開発元は信頼できるか

開発元がはっきりしないソフトウェアや、開発元がはっきりしていてもその信頼性に確信が持てない場合、そのソフトウェアの採用は避けるのが望ましい。

そのような不安を超えて採用する場合は、導入時のウイルス検査を特に入念に行うべきである。

(3) 導入時検査についての記録について

導入時の素性審査やウイルス検査についての記録に記載すべき事項としては、以下があげられる。

- 素性審査の日時、内容、評価および実施責任者
- 導入時ウイルス検査実施日
- 使用した検査ツールと検査結果
- 導入時ウイルス検査に用いたパターンファイルに関する情報(メンテナンス日等)

(6) データからのウイルスの侵入を阻止する

【主旨】

受信メールに添付されたデータや、ダウンロードしたデータなどはウイルスに感染している危険性がある。このため、ウイルスが付着したデータから、システムがウイルスに感染しないよう、外部から受取ったデータに対しては、受取時やその処理に先立って必ずウイルス検査を行い、ウイルスに感染していないことを確認しなければならない。

この検査でウイルスが発見された場合は、ウイルスの駆除、またはデータそのものの破棄等を行なわなければならない。

【具体的な実施事項】

(1) ウイルス対策の視点からの外部からの受取りデータの取扱いに関するルールの確立

外部から受取ったデータから、システムがウイルスに感染することを阻止するための措置が適切に行われるためには、外部からの受取りデータの取扱いに関し、ウイルス対策の視点からのルールを確立しておくことが必要となる。

このルールの中で明確にしておくべきこととしては、以下をあげることができる。

- ルールの適用範囲
- データの素性の審査と評価
- 受取時または処理前のウイルス検査の実施
- 実施したウイルス検査に関する記録とその保管

(2) 外部からの受取データに対する素性確認の実施

外部からの受取ったデータに対しては、その受取時または処理前等、当該データに対するウイルス対策要件で指定された時点で、前項で示す**ウイルス対策の視点からの外部からのデータの受取りに関するルール**に従い、

- 発信者の確認と評価
- 作成者の確認と評価
- ウイルス検査済みの確認

を行う。

この素性確認で、不審と判断されるデータに対しては、受取の拒否、破棄等を行い処理しないことを原則とするが、どうしても処理する必要がある場合は、厳重なウイルス検査を行うこと。

(3) 外部からの受取データに対するウイルス検査の実施

(2)の素性確認をパスの有無を問わず、外部から受取ったデータについては、システムで処理に先立ってウイルス検査を実施し、検査に用いたパターンの範囲ではウイルスがないことを確認する。

このウイルス検査の実施方法としては、以下があげられる。

- データ受取後におけるオフライン処理でのウイルス検査
- ゲートウェイ型ワクチンによる受信データに対する動的検査
- 特定アプリケーション対応型ワクチンによる受信データに対する動的検査

この検査で用いる検査パターンは、当該データの処理が行われる機器(群)に求められる対策レベルに対し定められているところに従うものとする。

(4) 実施したウイルス検査についての記録と保管

外部から受取ったデータに対するウイルス検査等については、**外部からの持込みデータに対するウイルス対策の視点の取扱いルール**に従い、これらの審査、検査についての記録を行い、保管する。

(5) ウイルス発見時の適切な処置の実施

ウイルスが発見された場合は、当該データの受取りや処理を拒否し、当該データの破棄を行う。またこの時、他への感染他の問題が既に生じていないかどうかのチェックを行い、必要な場合はウイルス感染事故処理を適切に行わなければならない。

ウイルス感染事故処理については、**"(10)ウイルス感染事故に備える"**参照。

【対策実施上のポイント】

(1) 外部からの受取りデータについて

サイトシステムが扱う外部からのデータがサイトに持込まれる形態としては、以下のようなものがあげられる。

- FD や CD 等の可搬電子記憶媒体により持込まれるデータ
- メールに添付されたデータ
- インターネット等の外部組織から ftp 等でダウンロードしたデータ

(2) 外部からの受取りデータの素性審査について

外部からの受取りデータに対する素性チェックのチェックポイントとしては、以下があげられる。

- 発信元ははっきりしていて、かつ信頼できるか
- 作成元ははっきりしており、かつ信頼できるか

発信元が信頼できても、作成元に信頼がおけない場合は、不審データとして認識すべきである。転送メールに添付ファイル等は、要注意である。

(3) 圧縮データの扱い

圧縮されているデータについても、ウイルス検査を実施すること。

(4) ゲートウェイ型ワクチンによる動的ウイルス検査の実施

ファイアウォールへやプロキシサーバ上で動作するワクチンを利用すると、ファイアウォール等を通過するデータに対して、ウイルス検査を実施することが可能である。

(5) 特定アプリケーション対応型ワクチンによる動的ウイルス検査の実施

メールサーバ等に常駐するワクチンを使用すると、メールサーバ等で処理するデータに対して

ウイルス検査を実施することが可能である。

(6) ウイルス検査の多重化

システムが処理する外部からのデータに対しては、さまざまなウイルス検査を複数組み合わせて実施するようにすることも有効である。

(7) システムに対するウイルス検査を適宜行う

【主旨】

ソフトウェアに対するウイルス検査や外部から持込まれたデータに対するウイルス検査等の感染防止策の実施上の不備や、新種ウイルスの登場等で、ウイルス感染を完全に防止することは困難と考えていなければならない。ウイルス感染による被害の発生や被害拡大を未然に防ぐためには、ウイルス感染防止策をかいくぐってウイルスが侵入したことをできるだけ早期に発見する必要がある。

ウイルス感染を早期に発見するには、ウイルス対策実施単位ごとに定められているウイルス対策要件に沿って、適宜、ワクチン等を利用したウイルス検査を実施する必要がある。

【具体的な実施事項】

(1) 定期的なウイルス検査の実施

サーバ、あるいはソフトウェア(群)やデータベース(群)等に対しては、ウイルス対策実施単位ごとに定められたウイルス対策要件に従って、定期的にウイルス検査を実施する。

検査サイクル、検査方法、検査パターンに関する要件は、それぞれに定められているウイルス対策要件の指定による。

(2) 必要に応じた臨時のウイルス検査の実施

サーバ、あるいはソフトウェア(群)やデータベース(群)等については、ウイルス対策実施単位ごとに定められたウイルス対策要件において、臨時のウイルス検査が必要と指定されている状況が発生した場合は、その指定に従って、臨時ウイルス検査を実施しなければならない。

検査方法、検査パターンに関する要検討は、それぞれに定められているウイルス対策要件の指定による。

(3) 実施したウイルス検査についての記録と保管

定期、臨時を問わず、実施したウイルス検査については、ウイルス対策実施基準に沿った実施に関する記録の作成とその保管を行わなければならない。

(4) ウイルス発見時の適切な処置の実施

ウイルスが発見された場合は、その駆除を行うとともに、ウイルス感染事故処理を行う。ウイルスク感染事故の処理については、**"(10)ウイルス感染事故に備える"**の項を参照。

【対策実施上のポイント】

(1) 臨時ウイルス検査の実施が必要なケース

以下のようなケースは、臨時ウイルス検査の実施を検討しなければならない。

- 新しい危険度の高いウイルスが報告され、このウイルスに対応するワクチンが登場した時(対応する検査パターンが更新された時)
- 定期ウイルス検査に不備が発見された場合

(8) ウイルス感染ファイルの外部への持出しを防止する

【主旨】

自サイトが感染源となって外部のシステムをウイルスに感染させるようなことがあってはならない。サイトの顧客や取引先にウイルスを感染させることは、サイトの信用を失うばかりでなく、感染先とのトラブルに発展する危険性もある。このため、自システムが新たな感染源になることを阻止するための施策を実施する必要がある。

【具体的な実施事項】

(1) ウイルス対策の視点からの外部持出しデータの取扱いに関するルールの確立

ウイルスに感染したデータを外部に持出さないようにするためには、外部に持出すデータに対するウイルス対策の視点からの取扱いルールを確立しておくことが必要となる。

このルールの中で明確にしておくべきこととしては、以下をあげることができる。

- 適用範囲
- データの素性の確認
- 外部持出し前のウイルス検査の実施
- 実施したウイルス検査に関する記録とその保管

(2) 外部に持出すデータに対するウイルス検査の実施

外部に持出すデータについては、発信や発送処理に先立ってウイルス検査を実施し、検査に用いたパターンの範囲ではウイルスがないことを確認する。

このウイルス検査の実施方法としては、以下があげられる。

- データ作成時あるいは持出し処理に先立った、当該ファイルに対するオフライン処理でのウイルス検査
- ゲートウェイ型ワクチンによる送信データに対する動的検査
- 特定アプリケーション対応型ワクチンによる送信データに対する動的検査

この検査で用いる検査パターンは、当該データに対して求められる対策レベルに対し定められているところに従うものとする。

(3) 実施したウイルス検査についての記録と保管

外部から受取ったデータに対するウイルス検査等については、外部に持出すデータについてのウイルス対策の視点からの取扱いルールに従い、これらの審査、検査についての記録を行い、保管する。

(4) ウイルス発見時の適切な処置の実施

ウイルスが発見された場合は、当該データの発信等の処理を拒否し、当該データの破棄を行う。また、この時、他への感染他の問題が既に生じていないかどうかのチェックを行い、必要な場合はウイルス感染事故処理を適切に行わなければならない。

ウイルス感染事故処理については、“(10)ウイルス感染事故に備える”参照。

【対策実施上のポイント】

(1) データの外部への持出しについて

サイトから外部へデータの持出す形態としては、以下のようなものがあげられる。

- FD や CD 等の可搬電子記憶媒体の外部への引渡し
- ファイルを添付したメールの発信
- ftp によるファイルの送信
- Web コンテンツのアップロード

(2) 外部に持出すデータに対する素性確認の実施

自サイトで作成したもの以外が含まれているデータに対しては、その受取時または処理前にウイルス検査が義務つけられているはずであるが、外部持出しに際しては、改めて問題がないかどうかのチェックを行うことが望ましい。

この素性確認で、不審と判断されるデータに対しては、外部への持出しを中止し、破棄等を行い処理しないことを原則とするが、どうしても処理する必要がある場合は、必ず厳重なウイルス検査を行うこと。

(3) ゲートウェイ型ワクチンによる動的ウイルス検査の実施

ファイアウォールへやプロキシーサーバ上で動作するワクチンを利用すると、ファイアウォール等を通過するデータに対して、ウイルス検査を実施することが可能である。

(4) 特定アプリケーション対応型ワクチンによる動的ウイルス検査の実施

メールサーバ等に常駐するワクチンを使用すると、メールサーバ等で処理するデータに対してウイルス検査を実施することが可能である。

(5) ウイルス検査の多重化

システムが処理する外部からのデータに対しては、さまざまなウイルス検査を複数組み合わせて実施するようにすることも有効である。

(9) ウイルス対策に用いる機能を適切に実装する

【主旨】

ウイルス対策に用いられる機能としては、

- ワクチン等のシステムまたはファイル上のウイルスを検査、駆除する機能
- 外部とのデータのやり取りにおけるウイルスを監視する機能

等があるが、使用する機能については、期待通りに機能し使用目的を満足すものでなければならない。

このためには、技術の選択と選択した技術における使用機能の選択、インストール時の設定等を的確に行うとともに、そのインストールに対する検査も十分に行うことが必要となる。

また、ウイルスの検査に用いる検査パターンの適切な整備が必要となる。

【具体的な実施事項】

適用する技術の個々に対し、以下のことが求められる。

(1) 適切な技術と使用する機能の選択

ワクチン等のウイルス対策のためシステムに組込む機能は、以下を満足していなければならない。

- 使用する技術(製品や方式)は、その使用場面ごとに求めるウイルス対策のレベルを満足するものでなければならない。
- 一般に機器やソフトウェアにはさまざまな機能が準備されており、同じ技術でもその使い方次第で機能も異なってくる。使用する技術そのものは妥当であっても、その機能設定が、使用目的に対して不適切であってはならない。

(2) 組込み場所の適切な選択

ワクチン等の選択した技術を期待通りに機能させるためには、選択した技術のシステム構成上の配置を適切に行わなければならない。使用する技術のシステム構成上での組込み場所は、以下により決められる。

- ウイルス対策における当該技術の役割および適用範囲
- 当該技術の機能特性および前提とする環境条件

(3) 選択した機能の的確なインストール

選択した技術を期待通りに機能させるためには、技術のシステムへのインストールが適切に行われていなければならない。このためには、以下のことが求められる。

- 選択機能の的確な組込み
- テストによる動作確認の実行

  システムへのインストールが終了したら、十分な機能検査を必ず実施し、インストールに不備がないことを確認すること。

(4) ウイルスパターンファイルのメンテナンス等の必要な運用環境の整備

システムの構成管理やシステムの運用において、OSやネットワークの環境設定、ウイルスパターンファイルの最新化等、適用した技術が前提とする環境整備に不備がないようにしなければならない。

これには、システムの導入時だけでなく、定期的な更新といったその維持管理についての処理も必要となる。

この中でも、ウイルスパターンファイルのメンテナンスは，特に重要である。

ウイルスは日々新種が発見されており、これに対応するためには、ワクチンおよびウイルスパターンファイルを常に最新の状態に保っておく必要がある。最新の状態のワクチンおよびウイルスパターンファイルは、通常ワクチンベンダーから提供される。ワクチンベンダーからの情報を常にチェックし、ウイルスパターンファイルの更新があった場合は、速やかに対応する必要がある。

このことが適切に行われるためには、以下の事項が適切に行われていなければならない。

- ベンダーからの情報をチェックし、ウイルスパターンファイルの更新状況を把握する
- ウイルスパターンファイルが更新されていた場合は、自ワクチンのウイルスパターンファイルを速やかに更新する
- ウイルスパターンファイルの更新について記録と保管を行い、個々のウイルス検査に用いられたウイルスパターンファイルの内容が、正確に把握できるようにしておく

(5) 使用技術の実装についてのドキュメントの整備

使用技術の実装については、いつでもその設定仕様や実装の状況の把握ができるようドキュメント化されるようになっていなければならない。

また、このドキュメントは、機能の新規導入時に作成するだけでなく、実装についての変更が行われたときも、適切にメンテナンスされていなければならない。

【対策実施上のポイント】

(1) 採用した技術における機能の選択にあたっては、十分な検討を行うこと。使用する技術のデフォルト機能を安易に用いないこと。

(2) ワクチンにはさまざまな導入形態がある。システムに適した方式のワクチンを選択すること。

(3) ウイルスパターンファイルの更新は、ウイルス感染防止にとって、非常に大切な作業である。ワクチンベンダーにより様々なウイルスパターンファイル更新形態が用意されている。ワクチンベンダーからウイルスパターンファイルの更新情報が届き、システム管理者がウイルスパターンファイルをダウンロードする形態等が、一般的である。可能ならば、ウイルスパターンファイルが更新されたことを自動で検出し、自動でウイルスパターンファイルをダウンロードしてくるような仕組みを導入することが望ましい。

(4) 使用技術の実装状況についてのドキュメント化すべき事項としては、以下のようなものがある。

- システム構成上の組込み場所

- 設定機能等の各種の指定内容
- 運用上の留意点
- 実装確認テストの内容と結果
- 新規組込みまたはメンテナンス日時

(10) ウイルス感染事故に備える

【主旨】

感染防止に努めても、感染防止処理の不備や、新しいウイルスの登場等で、ウイルス感染防止に完全はなく、システムは常にウイルス感染にさらされていると考えなければならない。

システムがウイルスに感染した場合、以下の処置を適切に実施しなければならない。

- システム全体からの感染ウイルスの完全な駆除
- ウイルス被害からのシステムや情報の迅速な復旧
- 二次被害の把握と必要な対策の実施

ウイルスの駆除が不完全だったり、影響範囲を見逃して復旧が完全でなかったり、二次感染に対する対応が不十分であったりすると、思わぬ被害の拡大を招くことになる。また、ウイルスに感染についての関係機関への届出も、漏れないようににしなければならない。

ウイルス感染事故発生時に必要な処置が、適切かつ迅速に行われるようにするためには、ウイルス感染事故発生時の対処要領を確立しておくとともに、常日頃から、事故処理に必要となる情報やツールの整備を行っておかねばならない。

【具体的な実施事項】

(1) ウイルス感染事故に対する対処要領の確立

ウイルス感染事故が発生した場合、必要な処置を円滑に行えるようにするためには、事故時の対処要領を確立しておくことが必要である。

ウイルス感染事故に対する対処要領として明確にしておくべき事項としては、以下があげられる。

- 対策チームの編成
- サービスの停止の検討と実施
- 関係者へのウイルス感染の告知
- 改ざん、破壊の内容、範囲等その状況の把握
- 改ざん、破壊されたソフト資産、情報資産の復旧
- 二次被害の調査と対策の検討、実施
- 原因の分析と再発防止策の検討とその実施
- 処理経緯の記録と保管

(2) ウイルス感染事故への対処に必要な情報の整備

日常のウイルス対策の運用状況に関する情報等、ウイルス感染事故の処理に必要となる情報は、適切に記録、保管しなければならない。

(3) ウイルス感染事故による被害に備えたシステムの保全

ウイルス感染事故による被害が発生した場合、被害から迅速にシステムや情報の復旧を実現

するためには、必要なソフト資産および情報資産のバックアップが必要となる。システムや情報の復旧に必要となるバックアップの取得とその管理を適切に行うためには、ウイルス感染事故による被害を想定したシステムの保全要領を確立しておくことが必要となる。

ウイルス感染事故による被害に備えたシステムの保全要領の中で明確にすべき事項としては、以下があげられる。

- バックアップを取得する対象
- バックアップ取得サイクル
- バックアップ取得方法
- バックアップデータからの復旧手順
- バックアップデータの管理手順
- バックアップデータの保管場所、保管場所からの持出し手順、保管期限、保管期限経過後の処置(バックアップデータの消去ルール)等。
- バックアップデータからの復旧訓練

(4) ウイルス感染事故を想定した事故処理の実施

バックアップデータが正常に保管されていても、復旧のための機能実装不備や、運用環境の変化、操作の不手際等から、必要な時に確実に復旧できない事態が起こりうる。このため、さまざまな形のウイルス感染による被害を想定した事故処理訓練を、定期的に行うことが望ましい。

また運用訓練で、事故処理の手順、システムの保全、事故対策を支援するツール、対応する運用規定や運用マニュアル等に不備が発見された場合は、遅滞なく必要な改善を行わなければならない。

(5) 必要なツールの整備

ウイルス感染事故に備えたバックアップの取得に用いるツールや、ウイルス感染事故発生時の被害範囲の調査や、破壊されたシステムや情報の回復等の事故処理に用いるツールは、期待通り機能しなければならない。

このためには、

- 適切なツールの選択とその適切なシステムへの組込み
- 運用環境の変更への対応
- ツール使用上のマニュアルの整備

等に不備がないようにしておかなければならない。

【対策実施上のポイント】

(1) ウイルス感染事故発生時の処理手順

ウイルス感染事故発生時の一般的な処理手順を、図 5-2 に示す。

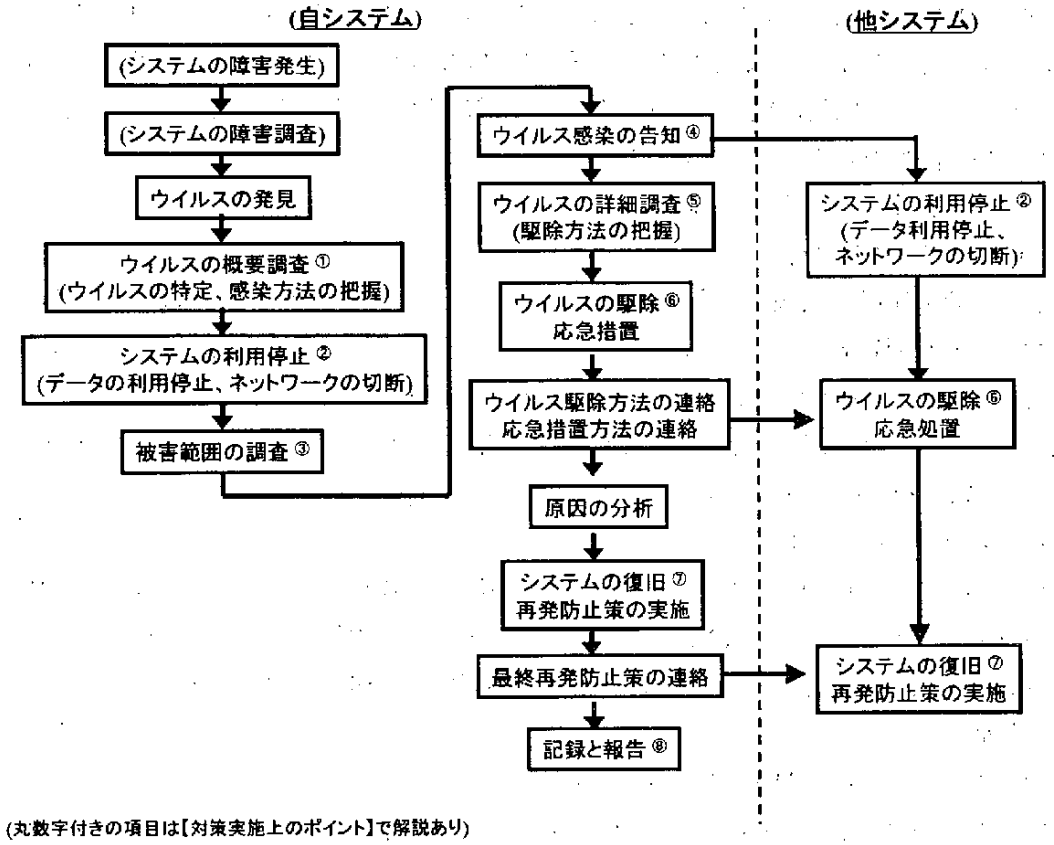


図 5-2 ウイルス感染時の対処手順

① ウイルスの概要調査(ウイルスの特定、感染方法の把握)

感染したウイルスの種類を特定し、その感染方法を調査、把握する。これにより、ウイルスの二次感染範囲をしぼり込むことができる。

② システムの利用停止(データの利用停止、ネットワークの切断)

システムにウイルスが感染していることを発見した場合は、これ以上ウイルス感染が広がらないようにするために、速やかにシステムの利用を停止する。ネットワークの特性や感染システムの状態により、感染データのみの利用停止、ネットワークの切断など、適切な対応を取る。ホストをシャットダウンする場合、可能な限り現状を保存できるよう工夫してシャットダウン・再起動を行う。不用意にシャットダウンすると、ウイルスの影響で起動しなくなる危険性があるので、十分注意すること。

③ 被害範囲の調査

ウイルスの特性から、二次感染を含めた感染の可能性を探り、ウイルス検査を実施し、その範囲を特定する。またウイルスの特性からデータの破壊等システムが被った被害範囲の特定を行う。

④ ウイルス感染の告知

二次感染の危険性がある場合は、二次感染の疑いのある対象者に対して、ウイルス感染の事実を連絡し、三次感染を未然に防ぐ。以後の作業において、現状以上の情報が入手できた場合、随時、二次感染の疑いのある対象者に、情報を連絡するのが望ましい。

⑤ ウイルスの詳細調査(駆除方法の把握)

ウイルスの駆除方法を調査、把握する。

⑥ ウイルスの駆除、応急措置

ワクチン等を利用して、発見したウイルスのすべてをシステムから駆除する。駆除作業終了後、再度ウイルス検査を行い、駆除が完了していることを確認することが重要である。場合によっては、ウイルス駆除だけではデータが復旧しない場合もある。

また、ウイルスの被害を受けた部分に対する応急措置を行う。さらに、再発防止策を実施するまでは、監視を強化することも必要である。

⑦ システムやデータの復旧

システムやデータの復旧を行う。この復旧が適切に行われるためには、システムの保全処置が適切に行われていなければならない。システムやデータの復旧にはこのバックアップデータを用いる。しかし、場合によっては、システムを再インストールする必要もある。

⑧ 記録と報告

ウイルス感染の対応結果を記録し、保管する。

ウイルス感染対応が完了したら、「ウイルス対策基準」(通商産業省告示第 692 号)に従い、指定された届出先にウイルス感染の届出を行う。

(2) ウイルス感染時の対処に必要な情報

ウイルス感染発見時における感染範囲や被害範囲の調査に必要な情報を、以下に示す。これらは、記録、保管されていなければならない。

- システム構成を示す情報
- システム上での情報資産の格納状況を示す情報
- システム構成の変更履歴を示す情報
- システムにおける情報資産の更新履歴を示す情報
- 業務処理の情報資産の流れを示す情報
- 外部システムとの情報の交換履歴を示す情報
- ワクチンのウイルスパターンファイルの更新履歴を示す情報
- 過去のウイルス検査実施に関する情報
- 過去のウイルス駆除実施に関する情報

(3) バックアップの取得とその保管についての留意事項

- バックアップ取得サイクルの決定にあたっては、復旧時間のみでなく、扱うデータ量や更新頻度等も考慮の上決定すること。
- バックアップの取得を行う際は、対象データに対するウイルス検査を、事前に実施する。

- バックアップ媒体は、安全な方法で、決められた期間保管する。
- ウイルスはプログラムを書き換えて感染するため、オリジナルプログラムには、ライトプロテクトを施す。
- 複数世代のバックアップデータを保存する。
- バックアップデータによる復旧を行う場合、バックアップデータはウイルス検査を実施した後、回復処理を行う。もしバックアップデータがウイルスに感染していた場合は、感染していない世代のバックアップデータまでさかのぼって、復旧処理を行う。

【参考情報】

「ウイルス対策基準」(通商産業省告示第 692 号)に示されているウイルス感染の届出先を、以下に示す。

- 情報処理振興事業協会(IPA)

  http://www.ipa.go.jp/security/

  - コンピュータウイルスに関する届出についての概要

    http://www.ipa.go.jp/security/outline/todokede-j.html

（11）ウイルス対策にかかる施策をシステム運用に反映させる

【基準の趣旨】

ウイルス対策にかかる諸施策が有効に機能するためには、ウイルス検査の実施や、発見したウイルスに対する適切な処置の実施等において、ウイルス対策がシステム運用に求めていることが適切に実行されなければならない。

このことを確実にするためには、ウイルス対策がシステム運用に委ねていることが、日々の運用において的確に実施されるようにする管理上の仕組みを工夫し、これらを日常の運用に組込んでおくことが必要となる。

【具体的な実施事項】

(1) ウイルス対策にかかる施策の運用規定、運用マニュアルへの反映

ウイルス対策にかかわる施策が運用に求めていることは、すべてシステムの運用規定や運用マニュアルに適切に反映されていなければならない。

(2) 運用環境の変更への適切な対応

運用環境に以下に示すような変更が行われた場合は、ウイルス対策にかかるシステム運用に変更の必要がないかどうかのチェックを行う。

- ウイルスに関する情報の収集とその処理、ウイルス検査についてのルール、ウイルス検査の方法、ウイルスの侵入監視の方法等、ウイルス対策にかかる具体的手段の変更
- 関係するシステム構成の変更
- システムの運用形態の変更
- ウイルス対策に用いている機能の変更

このチェックにより、システム運用に変更が必要となった場合は、以下の対応を適切に行わなければならない。

- 運用規定、運用マニュアルに対する必要な変更
- 必要な場合における運用スケジュールの変更等、システム運用の組立ての変更
- システム運用の変更の運用関係者への徹底

(3) ウイルス対策にかかる定期作業のスケジュール化

ウイルス対策にかかる運用処理の実行を漏れないようするためには、システム運用上定期的に実施すべき作業は、予めスケジュール化しておくことが有効である。

ウイルス対策に関連して、定期的な作業としてスケジュール化しておくべき作業としては、以下のようなものがあげられる。

- ウイルス検査ツールの見直し
- ウイルスに関する最新情報の入手
- ウイルスパターンファイルのメンテナンス

- 定期ウイルス検査の実施
- 各サーバに対するウイルス検査実施状況のチェック
- ウイルス感染に備えたシステムの保全処理

(4) 関係運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行

ウイルス対策にかかる運用作業についてのチェックリストを作成し、運用実績を記入、報告し、個々の作業が的確に実行されたことの確認を常に行うようにすることも、運用上から必要な処理が漏れないようにするための工夫の一つである。

(5) ウイルス対策にかかる運用処理についての記録と保管

以下に示すようなウイルス対策にかかわる運用上の処理については、その記録を残し管理する。ワクチンの新規導入、機種変更、機能変更及び設定の変更

- ウイルスパターンファイルの更新
- ウイルス検査の実施とその結果に対する処理
- ウイルス侵入監視の分析とその結果に対する処理
- ウイルス感染事故に備えたシステムの保全処理
- ウイルス対策にかかるシステム運用の変更

【実施対策上のポイント】

(1) ウイルス対策の運用規定や運用マニュアルへの反映手順の確立

ウイルス対策にかかる諸施策の運用規定や運用マニュアルへの反映を確実にするためには、これらの施策の運用規定や運用マニュアルへの反映手順を確立しておくことも必要となる。

これらの手順については、11.2 節の"**(4)セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに適切に反映する**"の項参照。

(2) ウイルス対策に関する運用処理のチェックリストについて

日々の運用におけるウイルス対策にかかる諸施策の運用処理を、確実なものにするための実行チェックリストにあげるべき処理としては、以下のようなものがあげられる。

- ウイルスに関する情報の収集とその処理
- ウイルスパターンファイルの更新
- 定期ウイルス検査の実施
- システム構成の変更時のウイルス検査
- バックアップデータの取得

(12) 関係者に対しウイルス対策についての教育を行う

【主旨】

ウイルス対策についての諸施策が適切に定められていても、それらが機能するためには、システムの管理や運用にかかわる担当者のウイルスに対する知識とその対策についての十分な理解を必要とする。

このため、ウイルス対策に直接かかわる者だけでなく、システムの構築や運用関係者や、システムに触れる者のすべてに対して、以下に示すようなウイルスとウイルス対策についての教育を適切に実施することが必要となる。

【具体的な実施事項】

(1) ウイルス対策教育の実施

① 定期的なウイルス対策教育の実施

システムの関係者に対する、ウイルスならびにウイルス対策に関する教育は、定期的に行われなければならない。

② 必要に応じた臨時ウイルス対策教育の実施

以下のような場合は、その都度、該当者に対する臨時教育を実施することが必要である。

- 異動によりウイルス対策関係者の交代があった場合
- ウイルス対策に関する基準やその運用が変更された場合
- ウイルス対策に問題が生じた場合

(2) ウイルス対策に関する教育カリキュラムの確立

ウイルスとウイルス対策についての教育を効果的に行うためには、教育科目とその内容、対象者と受講サイクル、実施時期等を定めた教育カリキュラムを確立しておくことが望ましい。

教育すべき内容としては、以下があげられる。

- ウイルスとウイルス対策の概要
- ウイルス対策の詳細とその実施要領
- ウイルス対策に用いる技術とその運用
- ウイルスの動向と最新のウイルス
- ウイルス感染事故事例

また教育内容は、サイトの運営形態やシステム構成、運用形態、さらには技術環境の進化を反映した、運用対象システムの実態に合ったものであるよう、適時見直しを行うこと。

(3) ウイルス対策教育テキストの整備

ウイルス対策に関する教育をより効果的にするためには、サイトの運営環境に合ったテキストを準備することが望ましい。

また、このテキストについてもサイトの運営形態の変更を反映するよう定期的な見直しを行うこ

とが望ましい。

【対策実施上のポイント】

(1) ウイルス対策に関する教育カリキュラムのを、表 5-7 に例示する。

表 5-7　ウイルス対策に関する教育カリキュラム例

項番	教育項目	教育対象者	頻度
1	ウイルスとウイルス対策の概要 ・ウイルスとその脅威の概要 ・ウイルス対策についての取り組み ・ウイルス対策の概要	・ウイルス対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者 ・業務上サイトシステムに触れる者(サイトシステムユーザ等)	1 回／年
2	ウイルス対策の詳細とその実施要領 ・各種基準 ・運用規定、運用マニュアル上の関係事項 ・その他注意事項	・ウイルス対策対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	1 回／年
3	ウイルス対策に用いる技術とその運用 ・ウイルス検査技法（含むツールの操作） ・ウイルス駆除技法（含むツールの操作） ・ウイルス対策ツールのメンテナンス	・ウイルス対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	1 回／年
4	ウイルスの動向と最新のウイルス ・流行しているウイルス ・サイトに感染したウイルス	・ウイルス対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者	随時
5	ウイルス感染事故事例	・ウイルス対策関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者 ・業務上サイトシステムに触れる者(サイトシステムユーザ等)	1 回／年

(2) ウイルスは日々新しい種類が作成されており、中には世界的な大流行を起こし、社会問題となるような場合もある。そのような事態が生じた場合、そのウイルスに関する情報や対策方法を関係者に周知するための教育を随時行う必要がある。

（13）ウイルス対策の実施状況についての監査を行う

【主旨】

ウイルス対策についての施策が決められその実施についての管理が行われていても、完全はありえない。一方、ウイルス対策の不備は、サイトのセキュリティに直接的な脅威となるため、ウイルス対策の不備によって問題が起きる前に、問題点を発見し適切な改善策を講じることができるようにしておくことが重要である。

このため、サイトの運営におけるウイルス対策として定められていることが、サイトの運営実態に照らして適切かどうか、またウイルス対策として定められていることが適切に実施されているかどうか等についてのチェックを行い、問題点の摘出と必要な改善を指導する、ウイルス対策の実施状況についての監査を行うことも必要である。

また日常の運用の中で、実施したウイルス対策に関する運用についての記録の保管等、この監査のための準備を組込んでおくことも必要となる。

特に、EC サイトサービスを事業として提供しているモール等では、その責任からみても、ウイルス対策の実施状況に関する監査の実施も必要となる。

（注）正式な監査という形はとらなくとも、ここに示すようなウイルス対策の実施状況についてのチェックは、組織的に行われるべきものである。

【具体的な実施事項】

（1）ウイルス対策の実施状況についての定期的な監査の実施

最低でも年1回は、以下に示すような事項をチェックする、ウイルス対策の実施状況についての監査を行う。

- ウイルス対策についての責任体制の整備状況とその機能状況
- ウイルス対策実施基準の妥当性
- ウイルスに関する最新情報の把握とその処理の状況
- ウイルス感染防止策の実施状況
- 定期的なウイルス感染検査の実施状況
- 必要に応じた臨時ウイルス感染検査の実施状況
- 外部持出しファイルに対するウイルス検査の実施状況
- ウイルス対策に使用している機能の実装状況
- ウイルス感染事故への備えの状況
- ウイルス対策にかかる施策のシステム運用への反映状況
- 関係者のウイルスとウイルス対策についての認識とスキルレベル

（2）監査実施要領の確立

ウイルス対策の実施状況についての定期的な監査が、円滑に実施され実効的なものにする

ためには、この監査についての実施要領が確立しておくことが望ましい。

この監査実施要領で規定しておく事項については、2.2 節の(4)項参照のこと。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。このためには、監査指摘事項に対する改善措置が実際にとられたかどうかについてのチェックを行うことが必要であり、監査要領の中に、指摘事項についてのフォローの仕組みを組み込んでおくことも有効である。

【対策実施上のポイント】

(1) 監査内容例

ウイルス対策の実施状況についての監査において、チェックすべき事項一覧を、表 5-8 に例示する。

(2) 監査の報告

監査結果は、ウイルス対策責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告しなければならない。

(3) 臨時監査の実施

適用しているウイルス対策やその実施の妥当性に疑問が持たれる場合は、その時点で監査を行うべきである。

表 5-8 ウイルス対策の実施状況に関する監査におけるチェック事項

項番	監査項目	監査の内容等
1	ウイルス対策についての責任体制の整備状況とその機能状況	・ウイルス対策に関する責任体制は、サイトの運営実態に照らして適切か ・ウイルス対策に関する責任者の自己の責任についての認識は十分か ・ウイルス対策に関する責任体制は機能しているか
2	ウイルス対策実施基準の妥当性	・ウイルス対策実施基準は、サイトの技術環境、運用環境等のサイトの運営実態に照らして適切か
3	ウイルスに関する最新情報の把握とその処理状況	・ウイルスに関する最新情報の収集とその処理についての適切なルールは確立しているか ・ウイルスに関する最新情報の収集は、ルールに沿って適切に行われいるか ・収集した情報に対する処理は適切に行われているか

表 5-8　ウイルス対策の実施状況に関する監査におけるチェック事項

項番	監査項目	監査の内容等
4	ウイルス感染防止策の実施状況	・ネットワークの入口におけるウイルス監視は、基準に沿って適切に行われているか ・メーラ等のアプリケーション対応ウイルス監視は、基準に沿って適切に行われているか ・機器やソフトのシステムへの組込み時点におけるウイルス検査は、基準に沿って適切に行われているか ・外部からの受取りデータに対するウイルス検査は、基準に沿って適切に行われているか
5	定期ウイルス検査の実施状況	・定期ウイルス検査はウイルス検査実施基準に沿って適切に実施されているか （対象範囲全てに対する漏れのない実施の確認） ・検査結果は適切に処理されているか
6	必要に応じた臨時ウイルス検査の実施状況	・必要な場合における臨時ウイルス検査は基準の沿って行われているか （必要時における、対象範囲すべてに対する漏れない実施の確認） ・ウイルス検査結果は適切に処理されているか
7	外部持出しファイルに対するウイルス検査の実施状況	・外部持出しデータに対するウイルス検査は規準に沿って適切に行われているか （対象範囲すべてに対する漏れない実施の確認） ・外部持出しファイルに対する検査結果は適切に処理されているか
8	ウイルス対策に使用している機能の実装状況	・ウイルス対策に用いる技術およびその機能選択は妥当か ・その実装の正確性は確認されているか （実装すべき場所に正確に実装されているか） ・運用環境の変更時における対応機能の実装の見直しは行われているか ・必要な運用環境の整備状況についてのチェックは適切に行われているか
9	ウイルス感染事故への備えの状況	・ウイルス感染に備えた保全要領が、サイトの運営実態に照らして適切に決められているか ・必要な保全処理は適切に行われているか ・ウイルス感染に対する対処要領は適切に決められているか ・監査期間中におけるウイルス感染事故に対する処理は妥当であったか

表 5-8　ウイルス対策の実施状況に関する監査におけるチェック事項

項番	監査項目	監査の内容等
10	ウイルス対策に関する施策のシステム運用への反映状況	・ウイルス対策にかかる諸施策は運用規定、運用マニュアルに適切に反映されているか ・これらの運用は、日々の運用において確実に実行されているか、また、そのことは管理されているか ・ウイルス対策にかかわるシステム運用の適切な実行を実現するための工夫は十分か
11	関係者のウイルスとウイルス対策に関する認識とスキルのレベル	・ウイルスならびにウイルス対策についての認識は十分か ・ウイルス対策担当者のウイルス対策にかかわるスキルは十分か ・関係者へのウイルス教育は適切か

6 セキュリティ管理情報の保護管理の徹底

6.1 実施すべき施策

図 6-1 に、セキュリティ管理情報の保護管理策の体系を示す。

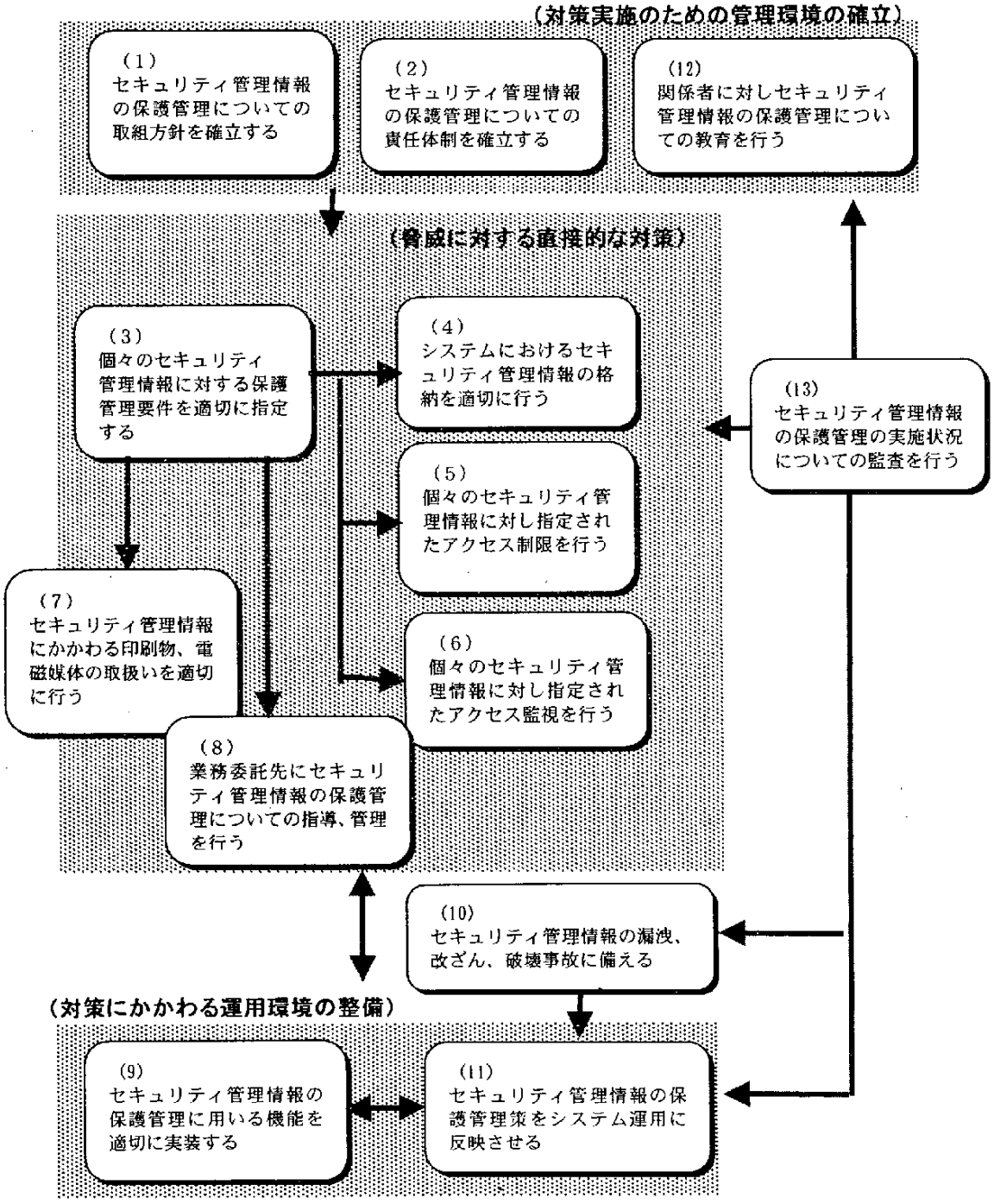


図 6-1 セキュリティ管理情報の保護管理策の組立て

また、表 6-1 に各施策における実施事項の一覧を示す。

表 6-1　セキュリティ管理情報の保護管理策としての具体的実施事項一覧

施策名	具体的実施事項
(1) セキュリティ管理情報の保護管理についての取組方針を確立する	① セキュリティ管理情報の保護管理の目標の明確化 ② 適用範囲の明確化 ③ セキュリティ管理情報の保護管理基準の確立 ④ セキュリティ管理情報の保護管理策の組立ての明確化 ⑤ セキュリティ管理情報の保護管理についての取組方針の関係者への周知
(2) セキュリティ管理情報の保護管理についての責任体制を確立する	① セキュリティ管理情報の保護管理についての責任体制の明確化 ② セキュリティ管理情報の保護管理関係者間の連携体制の確立
(3) 個々のセキュリティ管理情報に対する保護管理要件を適切に指定する	① 個々のセキュリティ管理情報に対する保護管理要件の指定 ② 個々のセキュリティ管理情報に指定した保護管理要件に関するドキュメントの整備
(4) システムにおけるセキュリティ管理情報の格納を適切に行う	① 指定された格納(ストア)の実践 ② システム上でのセキュリティ管理情報の格納状況の正確な把握 ③ セキュリティ管理情報のシステムへの格納にかかる運用の適切な実行
(5) 個々のセキュリティ管理情報に対し指定されたアクセス制限を行う	① 指定されたアクセス制限の実践 ② アクセス制限に用いる権限情報等の適切な管理の実施 ③ アクセス制限の実施状況の正確な把握
(6) 個々のセキュリティ管理情報に対し指定されたアクセス監視を行う	① 指定されたアクセス監視の実施 ② アクセス監視にかかる運用管理の確立 ③ 検知した不審なアクセスに対する適切な処置の実施 ④ アクセス監視の実施状況の正確な把握
(7) セキュリティ管理情報にかかわる印刷物、電磁媒体の取扱いを適切に行う	① セキュリティ管理情報を含む印刷物や電磁媒体の個々に対する保護管理要件の確立 ② 関係者の教育の実施 ③ 保護管理要件に従った保護管理の実践

表 6-1　セキュリティ管理情報の保護管理策としての具体的実施事項一覧

施策名	具体的実施事項
(8) 業務委託先にセキュリティ管理情報の保護管理についての指導、管理を行う	① 適切な業務委託先の選定 ② 業務委託先における保護責任の明確化 ③ 業務委託先における保護管理状況の把握と必要な指導の実施
(9) セキュリティ管理情報の保護管理に用いる機能を適切に実装する	① 適切な技術と使用する機能の選択 ② 組込み場所の適切な設定 ③ 選択した機能の適切な組込み ④ 必要な運用環境の整備 ⑤ 使用技術の実装についてのドキュメントの整備
(10) セキュリティ管理情報の漏洩、改ざん、破壊事故に備える	① セキュリティ管理情報にかかる事故に対する対処要領の確立 ② セキュリティ管理情報にかかる事故の処理に必要な情報の整備 ③ セキュリティ管理情報にかかる事故による被害に備えたセキュリティ管理情報の保全 ④ セキュリティ管理情報にかかる事故を想定した事故処理訓練の実施 ⑤ 必要なツールの整備
(11) セキュリティ管理情報の保護管理にかかる施策をシステム運用に反映させる	① セキュリティ管理情報の保護管理にかかる施策の運用規定、運用マニュアルへの反映 ② 運用環境の変更への適切な対応 ③ セキュリティ管理情報の保護管理にかかる定期作業のスケジュール化 ④ 関係運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行 ⑤ セキュリティ管理情報の管理にかかる運用処理の記録と保管
(12) 関係者に対しセキュリティ管理情報の保護管理についての教育を行う	① 関係者に対するセキュリティ管理情報の保護管理についての教育の実施 ② セキュリティ管理情報の保護管理についての教育カリキュラムの確立 ③ セキュリティ管理情報の保護管理に関する教育テキストの整備
(13) セキュリティ管理情報の保護管理の実施状況についての監査を行う	① セキュリティ管理情報の保護管理の実施状況についての監査の定期的な実施 ② 監査実施要領の確立 ③ 監査指摘事項に対するフォローの実施

6.2 個別具体策

(1) セキュリティ管理情報の保護管理についての取組方針を確立する

【主旨】

サイトセキュリティ確保の要の一つであるセキュリティ管理情報の保護管理を徹底し、その漏洩等の事故の防止を図るとともに、万一このような事故が発生しても、その被害を限定的なものにすることに組織的に取組むには、セキュリティ管理情報の保護管理をどのような考えで、またどのような方法で実施するかといったセキュリティ管理情報の保護管理についての取組方針を確立し、これを、セキュリティ管理情報の保護管理に直接かかわる者だけでなく、システムの構築や運用に関係する者、さらにはサイトやショップの運営上、セキュリティ管理情報に触れる者のすべてに、周知させておくことが必要となる。

【具体的な実施事項】

(1) セキュリティ管理情報の保護管理の目標の明確化

セキュリティ管理情報の保護管理が目指すところを明確にし、セキュリティ管理情報の保護管理に関する諸施策の意図を明確にする。セキュリティ管理情報の保護管理の目標としては、以下があげられる。

- セキュリティ管理情報の漏洩の防止
- セキュリティ管理情報の改ざん、破壊の阻止
- セキュリティ管理情報に関する事故発生時における被害の極小化

(2) 適用範囲の明確化

セキュリティ管理情報の保護管理策の適用範囲として、以下を明確にする。

- システム構成上の対象領域および対象サーバ等の機器
- 対象とする電磁媒体
- 対象とする印刷物
- 対象とする組織
- 対象とする業務、作業

セキュリティ管理情報の保護管理は、システム上に格納されている情報だけでなく、これらの情報が含まれる電子媒体や印刷物も対象となるため、その規定が及ぶところの明確化は特に重要である。

(3) セキュリティ管理情報の保護管理基準の確立

セキュリティ管理情報に求められる保護管理は、対象とする情報のライフサイクル特性、システム上での保管形態、漏洩や破壊等の事故が発生した場合の影響の大きさ等により異なる。このため、すべてに一律の保護管理策を適用することは、運用上現実的でない。

実際に実施する保護管理策は、個々の情報ごとに決めなければならないが、それぞれは全体として統制のとれたものでなければならない。このことを実現するためには、保護管理に厳格さによるレベル分けを行い、それぞれのレベルに対する標準的な保護管理要件を定義したセキュリティ管理情報の保護管理基準を確立しておき、対象情報ごとに適用する保護管理レベルを割り当て、そのレベルに対し規定されている保護管理要件に基づいた保護管理を実施するような工夫も必要となる。

セキュリティ管理情報の保護管理基準として定義すべき事項をあげると、以下のようになる。

- 保護管理レベルの名称
- 当該レベルの適用範囲
- システム上の対象情報に対し操作単位に定めるアクセス権限条件
- 電磁媒体、印刷物の取扱いについての要件
- 業務上での取扱い条件
- システムへの格納についての要件
- アクセス監視についての要件
- メンテナンスについての要件
- 保全要件

保護管理にかかる諸要件は、当該レベルが適用される情報の重要度に依存する。

(4) セキュリティ管理情報の保護管理策の組立ての明確化

セキュリティ管理情報の保護管理をどのように行うかについて明らかにするもので、実施する施策の構成と施策間の関係を示す。

本ガイドラインにおけるセキュリティ管理情報の保護管理にかかる諸施策の組立てについては、6.1 節参照。

(5) セキュリティ管理情報の保護管理についての取組方針の関係者への周知

作成されたセキュリティ管理情報の保護管理についての取組方針は文書化され、セキュリティ管理情報の保護管理に直接かかわる者の他、サイトの構築ならびに運用関係者や、業務上これらの情報に触れる者のすべてに周知させておかなければならない。このためには、

- セキュリティ管理情報の保護管理についての取組方針の掲示や配布
- 定期的なセキュリティ管理情報の保護管理の取組方針についての関係者間での再確認

が必要となる。

【対策実施上のポイント】

(1) セキュリティ管理情報の保護管理基準の定義要領

セキュリティ管理情報の保護管理基準を定義するにあたって定義すべき項目を表 6-2 に示す。

表 6-2　セキュリティ管理情報の保護管理基準における定義項目

項番	定義項目	定義の内容
1	保護管理レベルの名称	・当該保護管理レベルの名称、ID
2	当該レベルの適用範囲	・当該レベルが適用対象となるセキュリティ管理情報の重要度クラス(注1)
3	システム上の対象情報に対し操作単位に定める権限条件	・対象情報の登録、更新、削除等そのライフサイクルにかかわる個々の操作に対する権限の対象範囲 (例)－当該情報の保護管理責任者 －当該情報の保護管理担当チーム員 ・当該情報の登録、更新、削除等そのライフサイクルにかかわらない照合のための読取り等その使用のためのアクセスについての権限の対象範囲 (例)－当該情報の保護管理責任者 －当該情報の保護管理チームの一員 －業務で当該情報へのアクセスが必要な者、あるいはプログラム －システムのメンテナンスにかかわる者 －システムの運用管理者 －システムの運用担当者
4	電磁媒体や印刷物の取扱いについての要件	・セキュリティ管理情報を含む電磁媒体や印刷物について取得、保管、利用権限を持つ者を指定 (例)－当該電磁媒体や印刷物の保護管理責任者 －当該情報の保護管理チームの一員 －当該情報にかかわる業務の管理に従事している者 －システムのメンテナンスにかかわる者 －システムの運用管理者 －システムの運用担当者
5	業務上での取扱い制限	・当該情報の生成、登録、更新、削除等そのライフサイクルにかかわる処理の手続き上、当該情報およびその操作に触れることできる者の対象範囲 (例)－当該情報の保護管理責任者 －当該情報の保護管理チームの一員 －当該情報にかかわる業務の管理に従事している者 －システムのメンテナンスにかかわる者 －システムの運用管理者 －システムの運用担当者 ・当該情報の秘匿にかかる注意事項等
6	システムへの格納についての要件	・システム上での当該情報の格納方法についての指定 (例)－専用の装置またはシステムで格納 －OS等のシステムの機能に依存し、一般的にはブラックボックス化した状態での格納 －暗号化して格納 －一般ファイルとしての格納

表 6-2　セキュリティ管理情報の保護管理基準における定義項目

項番	定義項目	定義の内容
7	アクセス監視についての条件	・当該情報についてのアクセス監視の要否および実施密度 (例)－動的アクセス監視を適用 －月１回以上の頻度全てのアクセスをチェック －アクセス監視対象外
8	メンテナンスについての要件	・パスワード等その内容の定期的なメンテナンスサイクル (例)－年2回以上、年１回以上、複数年に１度 －特に定期更新なし ・運用環境の変更への対応速度 (例)－リアルタイムで反映 －数日レベルの遅れ容認 －月単位でのメンテナンス ・実施したメンテナンスについての記録とその保管の要領
9	保全要件	・バックアアップの取得サイクル ・バックアアップの保管世代 ・バックアアップの保管期間 ・バックアアップの物理的な保管要件

(注1) (2)項の“セキュリティ管理情報の重要度についての考え方”参照。

(2) セキュリティ管理情報の重要度についての考え方

セキュリティ管理情報の重要度とは、漏洩や改ざん、破壊等の事故が発生した場合における影響の大きさの尺度を示すもので、当該情報に求められる保護管理の厳格さを決める時の判断材料となるものである。

重要度についてクラス化を行い、対象情報に対する保護管理レベルの割当ては、対象情報に指定された重要度クラスによるようにすることも、セキュリティ管理情報に対する保護管理をサイト全体として統制にあるものにするためには有効である。

表 6-3 にセキュリティ管理情報の重要度クラスの定義例を示す。

表 6-3 セキュリティ管理情報の重要度クラスの定義例

項番	重要度クラス	重要度の尺度	情報例
1	クラスA	その漏洩、改ざんは、サイトのセキュリティ全体を極度に危うくするもの	・ルート権限 ・ACL ・ファイアウォールの設定情報 ・証明書の秘密鍵
2	クラスB	その漏洩、改ざんは、サイトのセキュリティを危うくするものの、セキュリティ全体に対しては、影響が限定的なもの	・アカウント情報 ・システム設定情報 ・ネットワーク設定情報 ・アプリケーション設定情報
3	クラスC	その漏洩、改ざん、破壊の影響は、特定業務に限定されるものの、被害が甚大になる可能性のあるもの	・セキュリティが特に重要なアプリケーションレベルのパスワード
4	クラスD	その漏洩、改ざん、破壊の影響は、特定業務に限定され、かつ、その被害が限定的なもの	・セキュリティがそう重要でないアプリケーションレベルのパスワード

(3) セキュリティ管理情報の保護管理基準の定義例

表 6-4 に、セキュリティ管理情報の保護管理基準の定義例を示す。

(4) セキュリティ管理情報の保護管理についての取組方針は、システム構成やその運用形態等、システム運用の実環境の変化に対応して必要な修正が加えられるべきであり、必要に応じて見直すこと。

(5) セキュリティ管理情報の保護管理についての取組方針は、定期的に関係者間で再確認することをルーチン化しておくことが望ましい。

表 6-4　セキュリティ管理情報の保護管理基準の定義例

項番	保護管理レベル	当該クラスにおけるセキュリティ管理情報の保護管理の実施基準
1	レベル A	・適用条件……重要度クラス A の情報 ・特定操作の権限条件……当該情報の保護管理担当者 ・使用権限条件……業務上での取扱い担当者 ・印刷物、電子媒体の取扱い条件……(省略) ・業務上の取扱い制限……業務上での取扱い担当者 ・システムへの格納についての要件……専用機器、システムで保管 ・アクセス監視要件……月 1 回以上アクセス状況をチェック ・メンテナンス要件……年1回以上の頻度で変更 当該情報の取扱い条件の変更は即時反映
2	レベル B	・適用条件……重要度クラス B の情報 ・特定操作の権限条件……当該情報の保管管理責任者 ・使用権限条件……当該情報の保管管理責任者 ・印刷物、電子媒体の取扱い条件……(省略) ・業務上の取扱い制限……当該情報の保管管理責任者のみ ・システムへの格納についての要件…OS等システム機能に依存 ・アクセス監視要件……月 1 回以上アクセス状況をチェック ・メンテナンス要件……年 2 回以上の頻度で変更 担当者の変更等の運用環境は即時反映
3	レベルD	・適用条件……重要度クラス D の情報 ・特定操作の権限条件……当該情報の保管管理担当者 ・使用権限条件……利用権限を有するユーザあるいはプログラム ・印刷物、電子媒体の取扱い条件……(省略) ・業務上の取扱い制限……業務上の関係者 ・システムへの格納についての要件…一般ファイルとして保管 ・アクセス監視要件……不要 ・メンテナンス要件……定期更新なし、 利用権限の変更は 1 週間以内に反映

(2) セキュリティ管理情報の保護管理についての責任体制を確立する

【主旨】

セキュリティ管理情報の保護管理策をその取組み方針に沿って機能させるためには、セキュリティ管理情報の保護管理策として定められていることが、システムの構築や運用に適切に反映されるよう、指導、管理する責任体制の確立が必要となる。

このためには、セキュリティ管理情報の保護管理にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) セキュリティ管理情報の保護管理についての責任体制の明確化

セキュリティ管理情報の保護管理の責任体制に関し、明確にしておくべきこととしては、以下のものがあげられる。

- セキュリティ管理情報の保護管理責任者とその責任
- システム上のセキュリティ管理情報の保護管理実施担当者の責任
- システム開発者のセキュリティ管理情報の保護管理に関する責任
- システム管理者のセキュリティ管理情報の保護管理に関する責任
- システム運用者のセキュリティ管理情報の保護管理に関する責任
- 業務現場におけるセキュリティ管理情報の取扱い責任者の責任
- セキュリティ管理情報の取扱いがかかわる業務の外部への業務委託責任者の責任

(2) セキュリティ管理情報の保護管理関係者間の連携体制の確立

セキュリティ管理情報の保護管理についての責任体制が有効に機能するためには、関係者間での連携が重要となる。

【対策実施上のポイント】

(1) セキュリティ管理情報の保護管理関係者の責任分担

表 6-5 に、セキュリティ管理情報の保護管理関係者の責任分担の定義例を示す。

(2) セキュリティ管理情報の保護管理にかかる責任体制は、セキュリティ管理情報の保護管理策を変更したり、サイトの運営環境に変更が生じた場合は、見直しを行い、必要な変更を行うこと。

表 6-5　セキュリティ管理情報の保護管理関係者の責任分担

責任者区分	タスク
セキュリティ管理情報の保護管理責任者	・セキュリティ管理情報の保護管理についての取組方針の確立と関係者への周知 ・セキュリティ管理情報の保護管理基準の発行 ・セキュリティ管理情報の保護管理全体の妥当性の維持 ・セキュリティ管理情報の保護管理の実施状態のチェック ・保護管理基準に従ったセキュリティ管理情報の保護管理の実施についての指導 ・セキュリティ管理情報の歩が管理にかかる事故発生時における事故処理の指揮
システム上のセキュリティ管理情報の保護管理実施担当者	・システム管理に関するセキュリティ管理情報の把握 ・システム管理に関するセキュリティ管理情報の保護の監督、管理 ・必要な機能の的確な実装 ・システム管理に関するセキュリティ管理情報の保護管理に関する事故処理と再発防止策の検討
システム開発者	・開発システムにおける関係機能の適切な組込み －設計の妥当性の確認 －正確な実装の確認
システム管理者	・システムにおけるセキュリティ管理情報の保護管理機能の維持 －システム構成の変更の反映の管理 －セキュリティ管理情報の保護管理支援機能の動作環境の維持管理 ・システムにおける対応機能の実装状況の正確な把握
システム運用者	・セキュリティ管理情報の保護管理にかかる適切なシステム運用環境の整備 ・セキュリティ管理情報の保護管理にかかる運用のチェックと指導
業務現場におけるセキュリティ管理情報の取扱い責任者	・業務現場でのセキュリティ管理情報の取扱い状況の把握 ・業務現場で取扱われるセキュリティ管理情報の保護の監督、管理 ・必要な機能の的確な実装 ・セキュリティ管理情報の保護管理に関する事故に対する業務現場サイドでの対処
セキュリティ管理情報の取扱いにかかわる業務の外部への業務委託責任者	・委託先におけるセキュリティ管理情報の保護管理責任の明確化 ・委託先におけるセキュリティ管理情報の保護管理の実施状態のチェック ・基準に従ったセキュリティ管理情報の保護管理の実施についての指導

（3）個々のセキュリティ管理情報に対する保護管理要件を適切に指定する

【主旨】

セキュリティ管理情報の保護管理を適切に行うためには、個々のセキュリティ管理情報に対しどのような保護をどのように行うかを定めた保護管理要件が、当該情報に適用される保護管理レベルに指定されている保護管理基準に沿って適切に決められていなければならない。

この要件の設定にあたっては、それぞれの保護対象情報ごとにそのライフサイクルを意識して、考えられる脅威を考慮しなければならない。

セキュリティ管理情報はシステム上だけでなく印刷物や電磁媒体上にも置かれることがあるが、これらについては保護管理の手段がシステム上のものと大きく異なるため、その扱いについては別項で述べる。"(7)セキュリティ管理情報にかかわる印刷物、電磁媒体の取扱いを適切に行う"参照。

【具体的な実施事項】

(1) 個々のセキュリティ管理情報に対する保護管理要件の設定

個々のセキュリティ管理情報に対し、どのような保護管理をどのような方法で行うかについて、以下に示すようなことを指定する。

- 当該情報のサイトのセキュリティとの関係
- 当該情報に適用する重要度クラス
- 当該情報に適用する保護管理レベル
- 適用するアクセス制限の詳細
- システム上での格納方法
- 適用するアクセス監視の詳細
- システムへの格納、アクセス制限、アクセス監視に使用する技術とその使用条件
- 当該セキュリティ管理情報のメンテナンスについての要件
- バックアップの取得とその保管についての要件

(2) 個々のセキュリティ管理情報に指定した保護管理要件に関するドキュメントの整備

セキュリティ管理情報に対する保護管理が、適切に行われているかどうかについての、管理が行えるように、当該サイトおよびショップの運営において用いられているセキュリティ管理情報の保護管理の実態を一覧できるドキュメントの整備を行い、何時でもその実態が正確に把握できるようにしておくことも必要である。

このドキュメントで明らかにすべき事項は、保護管理の対象となるセキュリティ管理情報すべてに対する、(1)項であげた項目となる。

また、このドキュメントは、業務やシステムの運用管理におけるセキュリティ管理情報の取扱い方法、システムの上でのセキュリティ管理情報の取扱い方式、システムの運用環境等の変更等

にともなう保護管理要件の変更が、適切に反映されたものになっているようになっていなければならない。

【対策実施上のポイント】

(1) 個々のセキュリティ管理情報に対する保護管理要件の定義要領

表 6-6 に個々のセキュリティ管理情報に対する保護管理要件で指定すべき事項を示す。

表 6-6 個々のセキュリティ管理情報に対する保護管理要件の定義における定義項目

項番	定義項目	定義内容
1	サイトのセキュリティとの関係	・当該セキュリティ管理情報がサイトのセキュリティに関する役割 ・当該セキュリティ管理情報に漏洩、改ざん、破壊事故が発生した場合に考えられる影響
2	適用する重要度クラス	・当該情報に適用される重要度クラス
3	適用する保護管理レベル	・当該セキュリティ管理情報に割り当てるセキュリティ管理情報の保護管理基準で定義されている保護管理レベル
4	適用するアクセス制限の詳細	・当該セキュリティ管理情報に適用するアクセス制限を定義する アクセス制限の要件定義の詳細は、(2)項参照
5	システム上での格納方法	・保護管理上から特別な格納を行う場合、その要件を定義する －暗号化の要否と必要な場合の暗号化の要件 －特殊な専用装置の使用 －他データとの隔離についての要件 ・更新、収容変え等の保管にかかる運用の実施手順
6	適用するアクセス監視の詳細	・アクセス監視の要否 ・必要な場合における、アクセス監視の要件 アクセス監視の要件定義の詳細については、(3)参照
7	システムへの格納アクセス制限、アクセス監視に使用する技術とその使用方法	・システム上での保管に用いる技術と使用機能 ・アクセス制限に用いる技術と使用機能 ・アクセス監視に用いる技術と使用機能

表 6-6　個々のセキュリティ管理情報に対する保護管理要件の定義における定義項目

項番	定義項目	定義内容
8	当該セキュリティ管理情報のメンテナンス要件	・パスワード等アクセス管理に用いる情報等のメンテナンスサイクル ・計画、承認、実行、確認等のメンテナンスの実行手順 ・実施したメンテナンスの記録要領
9	保全要件	・バックアップの取得等当該セキュリティ管理情報の保全に関する以下に示すような事項についての指定 －バックアップの取得サイクル －バックアップの保存機関、保存世代、保管場所等のバックアップの保管に関する要件 －バックアップからの回復手順

(2) セキュリティ管理情報に対するアクセス制限要件の定義要領

セキュリティ管理情報へのアクセス制限要件定義において指定すべき事項を、表 6-7 に示す。

表 6-7　セキュリティ管理情報へのアクセス制限要件定義における定義事項

項番	定義項目	定義内容
1	当該セキュリティ管理情報に対するシステム操作の権限保有者	・システム上の当該セキュリティ管理情報に対する操作の権限保有者を、下記の操作単位に指定する。 －個別情報の生成 －個別情報の登録 －個別情報の参照 －個別情報の印刷、他の電子媒体へのコピー －個別情報の更新 －個別情報の削除 －システム上の当該情報の二次加工 －情報全体の印刷 －情報全体のコピー －情報全体の抹消 －情報のバックアップの取得 －収容ファイルの再編成 ・権限保有者(人またはプログラム)はその資格名を指定する
2	権限保有者の指定登録方法	・権限保有者の登録管理方法権限情報の管理方法

表 6-7　セキュリティ管理情報へのアクセス制限要件定義における定義事項

項番	定義項目	定義内容
3	適用するアクセス管理方式	・適用する技術または方式の指定 （例） －OSやデータベース管理の持つ機能の使用 －特殊な専用装置の使用 －独自仕様の適用 ・使用機能の使用方法（機能設定等）の指定
4	不審アクセスに対する処置	・アクセス管理で不審アクセスが検知された場合のシステムならびに業務上での処置を定義

(3) アクセス監視についての要件定義要領

セキュリティ管理情報へのアクセス監視の要件定義において指定すべき事項を、表 6-8 に示す。

表 6-8　セキュリティ管理情報へのアクセス監視の要件定義における定義内容

項番	定義項目	定義内容
1	監視対象	・監視すべきイベント ・不審アクセスの定義
2	監視方法	・監視に用いる技術とその機能の設定 ・監視ポイント ・不審アクセス検知時の報告方法
3	監視の運用	・不審アクセス監視責任者の指定 ・定期的なチェック実施についての指定 ・不審アクセスが報告されたときの対処要領

(4) バックアップデータの取扱いについて考え方

- バックアップバックアップ取得サイクルの決定にあたっては、復旧時間のみでなく扱うデータ量、更新頻度等も考慮の上決定する
- バックアップ媒体は、安全な方法で、決められた期間保管する
- バックアップの頻度については、システムの可用性により判断する
- バックアップした日付、内容、媒体などを記録しておく
- 複数世代のバックアップデータを保存する
- 廃棄の手順を明確にしておく

(5) システムで取扱うセキュリティ管理情報の把握について

システム上の個々のセキュリティ管理情報に対する保護管理要件の設定が適切に行われるようにするためには、システムの扱っているセキュリティ管理情報の取扱い状況が正確に把握されていなければならない。

このためには、以下の情報は常に整理把握されていなければならない。

- システムの処理対象となっているセキュリティ管理情報の体系
- システムにおけるセキュリティ管理情報の配置状況
- ユーザデータとプログラムとの関係
- 個々のセキュリティ管理情報のライフサイクル
  - 生成、登録、参照、更新、抹消等が、業務との関係でどのような形態で行われているか
  - 変動特性(更新頻度、参照頻度、寿命等)

(6) システム上でのセキュリティ管理情報の保護管理方式の検討について

システム上のセキュリティ管理情報の個々に対するシステムへの格納、アクセス制限、アクセス監視に適用する方式の選択に当っては、保護管理要件と、ユーザの使い勝手、コスト、運用環境の手間等のバランスを考慮すること。

(7) セキュリティ管理情報に対する脅威について

個々のセキュリティ管理情報に対する保護管理要件の設定にあたっては、当該セキュリティ管理情報に対する脅威の分析が必要となる。この脅威の分析では、当該セキュリティ管理情報のライフサイクルの各ステージにおける、考えられる脅威とその影響および脅威の抑止を検討する。

検討対象の脅威をあげると以下のようになる。

- 外部ネットワークからの不正アクセス
- 情報の電子的交換時の盗聴、改ざん、漏洩
- 保管状態にある物理的媒体(印刷物、電磁媒体等)の盗難・紛失
- 機器のメンテナンス、媒体の廃棄処分等に起因する無権限者による閲覧、コピー
- 媒体のデリバリー途上の盗難・紛失
- オペレーションに起因するファイル等システムの破壊・破損・不正コピー

(4) システムにおけるセキュリティ管理情報の格納を適切に行う

【主旨】

システム上でのセキュリティ管理情報の格納場所や格納方法は、それぞれのセキュリティ管理情報に指定された保護管理要件に従っていなければならない。特に、専用保管装置の使用や暗号化等の特別な格納方法が指示されている場合は、その実現方法については十分な検討と管理が必要となる。

【具体的な実施事項】

(1) 指定された格納(ストア)の実践

セキュリティ管理情報はシステムにおいて、当該情報の保護管理要件で指定された方法により格納しなければならない。

このためには、必要な装置や機能のシステムへの組込みや、これらに必要とされる設定が適切なものでなければならない。

これらの機能の実装の管理については、(9)項**"セキュリティ管理情報の保護管理に用いる機能を適切に実装する"**の項参照。

(2) システム上でのセキュリティ管理情報の格納状況の正確な把握

システムにおけるセキュリティ管理情報の格納状況は、常に正確に把握されていなければならない。一覧表等のドキュメントの整備が求められる。

セキュリティ管理情報の格納状況に関して把握しておくべき情報としては、以下のようなものがあげられる。

- システム上での格納場所(使用装置、アドレス等)
- 格納方式(使用データベース管理ソフトおよびその使用法、暗号化方法等)
- 当該情報を使用するアプリケーションまたはシステム管理機能

(3) セキュリティ管理情報のシステムへの格納に関する運用処理の適切な実行

システム上のセキュリティ管理情報についての、

- 新規登録または更新
- 収容方式、収容場所等システムにおける格納形態の変更
- ファイルの再編集等の編成変え

等の保管にかかる運用処理の実行にあたっては、

- 決められた手順に従った計画、承認、実行、事後処理
- 処理の記録

を適切に行わなければならない。

(5) 個々のセキュリティ管理情報に対し指定されたアクセス制限を行う

【主旨】

システム上のセキュリティ管理情報には、個々のセキュリティ管理情報ごとに設定されたアクセス制限要件に従ったアクセス制限が、的確に行われていなければならない。

【具体的な実施事項】

(1) 指定されたアクセス制限の実践

システム上のセキュリティ管理情報には、当該情報に対する保護管理要件で指定されたアクセス制限が、的確行われていなければならない。

このためには、必要な装置や機能のシステムへの組込みや、これらに必要とされる設定は適切なものでなければならない。

これらの機能の実装の管理については、(9)項**"セキュリティ管理情報の保護管理に用いる機能を適切に実装する"**の項参照。

(2) アクセス制限に用いる権限情報等の適切な管理の実施

セキュリティ管理情報に対するアクセス制限をサポートする機能は、当該セキュリティ管理情報に対するアクセス権限情報と、アクセスしようとしているユーザまたはプログラムの認証に基づいている。このため、セキュリティ管理情報に対するアクセス制限が期待通り機能するためには、当該情報に対して定められている保護管理要件に従った、

- アクセス権限情報の適切な設定
- 決められた手順に沿ったアクセス権限情報のシステムへの登録
- アクセス権限者の認証情報の適切な設定
- 決められた手順に従ったアクセス権限者の認証情報の登録

が適切に行われるようになっていなければならない。

(3) アクセス制限の実施状況の正確な把握

システムにおけるセキュリティ管理情報に対するアクセス制限の実施状況は、常に正確に把握されていなければならない。一覧表等のドキュメントの整備が求められる。

セキュリティ管理情報に対するアクセス制限の実施状況に関し、把握しておくべき情報としては、以下のようなものがあげられる。

- 適用方式、使用機能
- 個別アクセスにおけるアクセス制限の設定状況
- 認証用情報、権限情報等の取り扱い状況

(6) 個々のセキュリティ管理情報に対し指定されたアクセス監視を行う

【主旨】

セキュリティ管理情報に対する権限のない者による不正なアクセスは、サイトのセキュリティ全体に対する脅威となるため、セキュリティ管理情報への不正アクセスは見逃さないようにしなければならない。

セキュリティ管理情報に対する不正なアクセスの試みが、どのような形でどの程度行われているかをチェックするセキュリティ管理情報を対象としたアクセス監視は、セキュティ管理情報の漏洩や改ざん、破壊事故の早期発見のためにも、セキュリティ管理情報の保護管理策の脆弱性を発見するためにも重要である。

このため、セキュリティ管理情報に対しては、当該情報に対する保護管理要件の指定するところに従ったアクセス監視が適切に行われなければならない。

【具体的な実施事項】

(1) 指定されたアクセス監視の実施

アクセス監視が指定されたセキュリティ管理情報については、保護管理要件で指定されたアクセス監視が適切に行われなければならない。このためには、

- セキュリティ管理情報に対するアクセス監視に必要な機能のシステムへの実装
- アクセス監視ログの適切な分析

を適切に行うことが必要となる。

① システムへのアクセス監視に必要な機能の適切な実装

アクセス監視のためにシステムに実装すべきものとしては、

- セキュリティ管理情報へのアクセスを監視する機能
- セキュリティ管理情報へのアクセスの記録機能と表示機能
- アクセス監視条件の設定

がある。

これらの機能の実装の管理については、(9)項**"セキュリティ管理情報の保護管理に用いる機能を適切に実装する"**の項参照。

② アクセスログの分析の実施

アクセスログについては、当該情報の保護管理で定義された頻度で、指定されたチェックを行う。

(2) アクセス監視にかかる運用管理の確立

実装した機能およびその実行環境に基づき、アクセス監視に関する運用について下記のような事項を明確にするとともに、システムの運用に反映させる。

- セキュリティ管理情報へのアクセス記録の定期的なチェック

- セキュリティ管理情報へのアクセス記録の保管期間の設定
- 不審アクセスを検知した場合の処理

(3) 検知した不審なアクセスに対する適切な処置の実施

不審なアクセスを検知した場合の処置は、以下の処置を適切に行わなければならない。

- 不正アクセスの成功の有無
- 成功している場合における被害の確認
- 不正アクセスを許した原因の調査と再発防止策の検討、実施

また、不正アクセスが成功していない場合にも、検知された不審アクセスに対し、脆弱点はないかどうかのチェックも行うことが望ましい。

(4) アクセス監視の実施状況の正確な把握

システムにおけるセキュリティ管理情報に対するアクセス監視の実施状況は、常に正確に把握されていなければならない。一覧表等のドキュメントの整備が求められる。

セキュリティ管理情報に対するアクセス監視の実施状況に関し、把握しておくべき情報としては、以下のようなものがあげられる。

- アクセス監視に用いる技術とその使用方法
- 個別アクセスにおけるアクセス監視条件の設定状況
- アクセス監視の結果
- 不審アクセスに対し実施した処置

(7) セキュリティ管理情報にかかわる印刷物、電磁媒体の取扱いを適切に行う

【主旨】

セキュリティ管理情報にかかわる印刷物等、セキュリティ管理情報が可視できる状態にあるものや、セキュリティ管理情報が記録された電磁媒体等については、システム上の情報とは別に、保護管理策を確立する必要がある。従って、システム上のセキュリティ管理情報と同様、これらの印刷物や電磁媒体それぞれについても保護管理要件を定めておく必要がある。

セキュリティ管理情報が記録された電磁媒体等は、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。このため、電磁媒体の保護管理は特に厳格に行う必要がある。

(注) 電磁媒体等とは、磁気テープや磁気ディスク、光ディスク等々の他、パソコン、サーバ、携帯端末等の本体内蔵の記憶装置・ディスク類を指す。

【具体的な実施事項】

(1) セキュリティ管理情報にかかわる印刷物や電磁媒体の個々に対する保護管理要件の確立

セキュリティ管理情報にかかわる印刷物や電磁媒体等に対しては、システム上のこれらの情報をとは別の保護管理要件が必要となる。

これらに対する保護管理要件で定義しておくべき事項としては、以下のようなものがあげられる。

- 作成に関する制約
- 外部との授受に関する条件
- 保管、保有に関する制限
- 使用に関する制限コピー
- 廃棄に関する要件
- 表示に関する条件

(2) 関係者の教育の実施

業務上、セキュリティ管理情報にかかわる印刷物や電磁媒体を取扱う者にう対しては、その保護管理についての教育を定期的に実施し、周知徹底を図る必要がある。

(3) 保護管理要件に従った保護管理の実践

日常の業務の運営において、これらの規定は厳格に守られなければならないが、現実には実行が伴わないことが多い。このため、その実行について常にチェックを行い、問題点の指摘を行う管理、指導を行い、これらの運用が習慣化するようにする管理上の努力が必要となる。

【対策実施上のポイント】

(1) セキュリティ管理情報を含む印刷物、電磁媒体に対する保護管理要件の定義

表 6-9に、セキュリティ管理情報を含む印刷物、電磁媒体に対する保護管理要件で定義すべき事項を示す。

表 6-9 ｾｷｭﾘﾃｨ管理情報を含む印刷物, 電磁媒体に対する保護管理要件定義における定義事項

項番	定義事項	定義内容
1	作成に関する制約	・作成者に関する条件 ・使用目的の限定等、作成にあたっての条件 ・作成の手続き ・作成についての記録とその保管
2	外部との授受についての条件	・授受の相手に関する条件 ・授受にあたっての条件の指定 ・授受に関する手続き ・授受についての記録とその保管
3	保管、保有に関する制限	・保管可能条件(使用目的、権限保有者の範囲) ・保管期間に関する条件 ・保管場所、保管管理の方法についての条件
4	使用に関する制限コピー	・参照にあたっての条件 ・二次加工にあたっての条件 ・更新等内容に対する操作の条件
5	廃棄に関する要件	・廃棄方法の明示 (特に電磁媒体等については、内容の消去方法、その確認についての指定も必要)
6	表示に関する条件	・保護対象物であることの表示 ・作成者、保管者の表示 ・作成日、廃棄予定日の表示

(2) セキュリティ管理情報を含む印刷物や電磁媒体の管理についての基本的な考え方

セキュリティ管理情報を含む印刷物や電磁媒体の管理についての基本的な考え方としては、以下のようなことをあげることができる。

- システム上のセキュリティ管理情報の印刷や外部記憶媒体へのコピーを制限する

これらの管理に漏れがないようにするための基本は、セキュリティ管理情報についての印刷物や、これらの内容をコピーした電磁媒体を必要最小限とし、管理対象を絞り込むことにある。システム上のセキュリティ管理情報の印刷や外部記録媒体へのコピーは、許さ

れた目的に限り、権限を持つものだけが実行できるようにしておかなければならない。

- セキュリティ管理情報を含む印刷物等については、極力保管せずに速やかに廃棄するようにする

(3) これらに対する基準は、社内の文書管理規定と連携を取っておくことが望ましい。場合によっては、社内文書管理規定に含ませることも考えられる。

(8) 業務委託先にセキュリティ管理情報の保護管理についての指導、管理を行う

【主旨】

ショップ運営あるいはサイト運営にかかる業務のすべてまたは一部を外部に委託しているような場合には、セキュリティ管理情報の取扱いにこの委託先がかかわることもある。このような場合、セキュリティ管理情報の保護管理の実現には、委託先においてもセキュリティ管理情報の保護管理が適切に行われることが必要となる。

このためには、業務委託先の選定を適切に行うとともに、業務委託先に対するセキュリティ管理情報の保護管理についての管理、指導の実施が必要となる。

【具体的な実施事項】

(1) 適切な業務委託先の選定

業務委託先におけるセキュリティ管理情報の適切な保護管理を期待するための第一歩は、信頼できる委託先を選ぶことにある。

このため、業務委託先の選定にあたっては、

- 企業の経営体質
- 情報の保護についての取組み

を確認することが必要である。

(2) 業務委託先における保護管理責任の明確化

セキュリティ管理情報を扱う業務を委託する場合は、業務委託契約等でセキュリティ管理情報の取扱いについて規定を設け、委託先におけるセキュリティ管理情報の保護管理についての履行義務と責任を明確にしておくことが必要である。

(3) 業務委託先における保護管理状況の把握と必要な指導の実施

業務委託先において、業務委託契約等で定めたセキュリティ管理情報の保護管理が適切に行われているかどうかのチェックを定期的に行い、問題があれば指導を行う必要がある。

これらのことを適切に行うためには、

- 業務委託先におけるセキュリティ管理情報の保護管理の状況についての情報の収集
- 適切な保護管理の実施のための連絡体制の構築

等も必要となる。

【対策実施上のポイント】

(1) 業務委託先の選定時における適格性の判断基準としては、以下のようなものをあげることができる。

- 情報保護に関し、従業員の義務が就業規則等で規定されているか

- 情報保護についての従業員の教育は行われているか
- 情報保護の責任者は明確になっているか
- 業務規定で、情報保護についての適切な規定があり、かつ、それらは実務上で実際に守られているか

プライバシマークの取得は、安心材料の一つになる。

(2) 業務委託にあたって、契約書等でセキュリティ管理情報の保護管理の責務の定義として取り決めておきたい事項としては、以下のようなものがあげられる。

- 委託先の責任の範囲
- 保護管理責任者の指定
- 保護管理基準の制定
- 保護管理の運用の励行
- 保護管理についての関係者の教育
- 保護管理の実施状況についての報告
- 保護管理上の事故の報告と適切な処置

(9) セキュリティ管理情報の保護管理に用いる機能を適切に実装する

【主旨】

セキュリティ管理情報の保護管理に用いられる機能としては、

- 特殊な格納のための機能
- アクセス制限に用いる機能
- アクセス監視に用いる機能

があり、その実現方法としては、

- 専用機器の使用
- OS の機能や、データベース管理の機能や、アプリケーションに組込まれた機能の使用
- 独自の仕様による実現

を選択することができるが、いずれの場合においても、期待通りに機能し、対象情報の保護管理要件に沿った保護管理が実現できるものでなければならない。

このためには、技術の選択と選択した技術における使用機能の選択、インストール時の設定等を的確に行うとともに、そのインストールに対する検査を十分に行うことが必要となる。

また、これらのデータへのアクセス制限の実行に必要な権限情報や利用者の認証情報等、使用する技術が前提とする運用環境の整備にも漏れがないようにしなければならない。

【具体的な実施事項】

適用する技術の個々に対し、以下のことが求められる。

(1) 適切な技術と使用する機能の選択

セキュリティ管理情報の保護管理のためにシステムに組込む機能は、以下を満足していなければならない。

- 使用する技術、製品、方式は対象とする情報について指定されているシステムへの格納やアクセス管理やアクセス監視についての要件を満足するものでなければならない。
- 一般に機器やソフトウェアにはさまざまな機能が準備されており、その使い方次第で機能も異なってくる。使用する技術そのものは妥当であっても、その機能設定が、対応する保護管理要件に対して不適切であってはならない。

(2) 組込み場所の適切な設定

セキュリティ管理情報の保護管理ツールとして選択した技術を期待通りに機能させるためには、選択した技術のシステム構成上の配置は適切なものでなければならない。使用する技術のシステム構成上での組込み場所は、以下により決められる。

- セキュリティ管理情報の保護管理における当該技術の役割および適用範囲
- 当該技術の機能特性および前提とする環境条件

(3) 選択した機能の適切な組込み

選択した技術を期待通りに機能させるためには、技術のシステムへのインストールが適切に行われていなければならない。このためには、以下のことが求められる。

- 選択機能の的確な組込み
- テストによる動作確認の実行

システムへのインストールが終了したら、十分な機能検査を必ず実施し、インストールに不備がないことを確認すること。

(4) 必要な運用環境の整備

システムの構成管理やシステムの運用において、OS やネットワークの環境設定、アクセス権限テーブルの整備や、ファイルの暗号化を行った時の暗号鍵の整備等、適用した技術が前提としている環境整備に不備がないようにしなければならない。

これには、システムの導入時だけでなく定期的な更新といった維持管理も必要となる。

(5) 使用技術の実装についてのドキュメントの整備

使用技術の実装については、いつでもその設定仕様や実装の状況の把握ができるようドキュメント化されていなければならない。

また、このドキュメントは機能の新規導入時に作成するだけでなく、実装についての変更が行われたときも適切にメンテナンスされたものになっているようになっていなければならない。

【対策実施上のポイント】

(1) 採用した技術における機能の選択にあたっては、十分な検討を行うこと。使用する技術のデフォルト機能を安易に用いないこと。

(2) 独自仕様の技術を用いる場合は、当該機能またはシステムに対し、ISO15408 に準拠した機能の評価および実装の評価を行うことも望ましい。

(3) 使用技術の実装状況に関しドキュメンに記載すべき事項としては、以下のようなものがある。

- システム構成上の組込み場所
- 設定機能等の指定内容
- 運用上の留意点
- 実装確認テストの内容と結果
- 新規組込みまたはメンテナンス日時

(10) セキュリティ管理情報の漏洩、改ざん、破壊事故に備える

【主旨】

セキュリティ管理情報の保護管理に努めていても、運用上の不備や新しい攻撃手段の登場等で、セキュリティ管理情報が改ざんされたり、破壊される可能性も考えておかなければならない。このような場合において、被害の拡大を防ぎ、業務やシステムの運用の混乱を極小化するためには、事故に対する処置が適切かつ迅速でなければならない。

事故時の対処が適切かつ迅速に行われるようにするためには、セキュリティ管理情報にかかわるセキュリティ事故が発生した時の対処要領を確立しておくとともに、常日頃から、事故処理に必要となる情報やツールの整備を行っておくことが求められる。

【具体的な実施事項】

(1) セキュリティ管理情報に関するセキュリティ事故に対する対処要領の確立

セキュリティ管理情報の漏洩、改ざん、破壊等、セキュリティ管理情報に関する事故が発生した場合、必要な処置を円滑に行えるようにするためには、事故に対する対処要領を確立しておくことが必要である。

セキュリティ管理情報に関する事故に対する対処要領として明確にしておくべき事項としては、以下があげられる。

- 対策チームの編成
- サービス停止の検討と実施
- 関係者へのセキュリティ管理情報の改ざん、破壊事故発生告知
- 改ざん、破壊の内容や範囲等の状況の把握
- 改ざん、破壊された資産の復旧
- 二次被害の調査と対策の検討、実施
- 原因の分析と再発防止策の検討とその実施
- 処理経緯の記録と保管

(2) セキュリティ管理情報にかかる事故の処理に必要な情報の整備

セキュリティ管理情報に関する運用処理の記録等、セキュリティ管理情報に関する事故の処理に必要な情報は、適切に記録、保管されていなければならない。

(3) セキュリティ管理情報にかかる事故による被害に備えたセキュリティ管理情報の保全

個々のセキュリティ管理情報の設定されている保護管理要件の定められたところに従い、日々の運用の中でバックアップの取得とその管理を行う。

(4) セキュリティ管理情報に関する事故を想定した事故処理訓練の実施

バックアップデータが保管されていても、復旧機能の実装の不備、運用環境の変化、処理手順への不慣れからくる操作の不手際等から、必要な時に復旧がうまくできないといった事態が起

こりうる。

このため、さまざまな形のセキュリティ管理情報に関する事故を想定した事故処理訓練を、定期的に行うことが望ましい。

また、運用訓練で事故処理の手順、システムの保全、バックアップの取得システムの機能、対応運用規定、運用マニュアル等の不備が発見された場合には、遅滞なく改善を行わなければならない。

(5) 必要なツールの整備

セキュリティ管理情報にかかわる事故に備えたバックアップの取得に用いるツールや、セキュリティ管理情報にかかわる事故発生時の被害範囲の調査や、破壊されたシステムや情報の復旧等、事故処理に用いるツールは、期待通り機能しなければならない。

このためには、

- 適切なツールの選択とその適切なシステムへの組込み
- 運用環境の変更への対応
- ツール使用上のマニュアルの整備

等に不備がないようにしておかなければならない。

【対策実施上のポイント】

(1) セキュリティ管理情報にかかるセキュリティ事故発生時の被害の調査と復旧に必要な情報

セキュリティ管理情報の改ざん、破壊事故発生時における被害範囲の調査と復旧処理に必要な情報としては、以下のようなものがあげられる。

- システム構成を示す情報
- システムにおけるセキュリティ管理情報の保有状況を示す情報
- システムにおけるセキュリティ管理情報の処理に関する運用を示す情報
- システムにおけるセキュリティ管理情報の更新履歴を示す情報
- ショップ業務におけるセキュリティ管理情報の使用状況

（11）セキュリティ管理情報の保護管理にかかる施策をシステム運用に反映させる

【主旨】

セキュリティ管理情報の保護管理にかかる諸施策が有効に機能するためには、対象情報についてのシステム上での安全な格納、アクセス制限、アクセス監視、情報の保全等において、セキュリティ管理情報の保護管理策がシステム運用に求めていることが、実際のシステム運用において適切に実行されなければならない。

このことを確実にするためには、セキュリティ管理情報の保護管理策がシステムの運用に委ねていることが、日々のシステム運用において的確に実施されるようにする管理上の仕組みを工夫し、これらを日常の運用に組込んでおくことが必要となる。

【具体的な実施事項】

(1) セキュリティ管理情報の保護管理にかかる施策の運用規定、運用マニュアルへの反映

セキュリティ管理情報の保護管理にかかる諸施策が運用に求めていることは、すべてシステムの運用規定や運用マニュアルに適切に反映されていなければならない。

(2) 運用環境の変更への適切な対応

運用環境に以下に示すような変更が行われた場合は、セキュリティ管理情報の保護管理策にかかるシステムの運用に変更の必要がないかどうかのチェックを行う。

- セキュリティ管理情報の保護管理ルール、格納方法、アクセス管理方法等、セキュリティ管理情報の保護管理にかかる具体的手段の変更
- 関係するシステム構成の変更
- システムの運用形態の変更
- セキュリティ管理情報の保護管理に用いている機能の変更

このチェックにより、システム運用に変更が必要となった場合は、以下の対応を適切に行わなければならない。

- 運用規定、運用マニュアルに対する必要な変更
- 必要な場合における運用スケジュールの変更等、システム運用の組立ての変更
- システム運用の変更の運用関係者への徹底

(3) セキュリティ管理情報の保護管理にかかる定期作業のスケジュール化

セキュリティ管理情報の保護管理にかかる運用処理の実行を漏れないようするためには、システム運用上定期的に実施すべき作業は、予めスケジュール化しておくことが有効である。

セキュリティ管理情報の保護管理に関連して、定期的な作業としてスケジュール化しておくべき作業としては、以下のようなものがあげられる。

- システムが保有しているセキュリティ管理情報の保管状態の確認
- システムが保有しているセキュリティ管理情報の改ざん、破壊の監視

- セキュリティ管理情報に対する不正アクセスの監視
- セキュリティ管理情報の定期メンテナンス
- セキュリティ管理情報にかかる事故に備えた情報の保全処理
- 事故処理の訓練

(4) 関係運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行

セキュリティ管理情報の保護管理にかかる運用作業についてのチェックリストを作成し、運用実績を記入、報告し、個々の作業が的確に実行されたことの確認を常に行うようにすることも、運用上から必要な処理が漏れないようにするための工夫の一つである。

(5) セキュリティ管理情報の管理にかかる運用処理についての記録と保管

以下に示すようなセキュリティ管理情報の保護管理にかかわる運用上の処理については、その記録を残し管理する。

- セキュリティ管理情報の登録、変更、削除、コピー等当該ファイルに対して行った操作
- セキュリティ管理情報の収容方法の変更
- セキュリティ管理情報に対するアクセス監視の分析とその結果に対する処理
- セキュリティ管理情報の保全処理
- セキュリティ管理情報の保護管理にかかるシステム運用の変更

【実施対策上のポイント】

(1) セキュリティ管理情報の保護管理策にかかる施策の運用規定や運用マニュアルへの反映手順の確立

セキュリティ管理情報の保護管理策にかかる諸施策の運用規定や運用マニュアルへの反映を確実にするためには、これらの施策の運用規定や運用マニュアルへの反映手順を確立しておくことも必要となる。

これらの手順については、11.2 節の"**(4)セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに適切に反映する**"の項参照。

(2) セキュリティ管理情報の保護管理に関する運用処理に関するチェックリストについて

日々の運用におけるセキュリティ管理情報の保護管理にかかる運用処理を、確実なものにするための実行チェックリストにあげるべき処理としては、以下のようなものがあげられる。

- システムが保有しているセキュリティ管理情報の保管状態の確認
- システムが保有しているセキュリティ管理情報の改ざん、破壊監視
- セキュリティ管理情報に対する不正アクセス監視
- セキュリティ管理情報にかかわる事故に備えた情報の保全処理
- 事故処理の訓練

（12） 関係者に対しセキュリティ管理情報の保護管理についての教育を行う

【主旨】

セキュリティ管理情報の保護管理についての諸施策が適切に定められていても、それらが機能するためには、システムの管理や運用に携わる者に、セキュリティ管理情報とその保護管理についての十分な理解が必要となる。

このため、セキュリティ管理情報の保護管理に直接かかわる者ものだけでなく、システムの構築や運用関係者やセキュリティ管理情報に触れる者すべてに対し、以下に示すようなセキュリティ管理情報の保護管理に関する教育を適切に実施することが必要となる。

【具体的な実施事項】

(1) 関係者に対するセキュリティ管理情報の保護管理についての教育の実施

① セキュリティ管理情報の保護管理についての定期的な教育の実施

セキュリティ管理情報の保護管理についての教育は、定期的に行われなければならない。

② 必要に応じたセキュリティ管理情報の保護管理についての臨時教育の実施

以下のような場合は、その都度、該当者に対する教育を行うことが必要となる。

- 異動等によりセキュリティ管理情報にかかわる者に入替えが合った場合
- セキュリティ管理情報の保護管理基準やその運用が変更された時
- セキュリティ管理情報の保護管理に問題が生じた場合

(2) セキュリティ管理情報の保護管理についての教育カリキュラムの確立

セキュリティ管理情報の保護管理についての教育を効果的に行うためには、教育科目とその内容、対象者と受講サイクル、実施時期等を定めた教育カリキュラムを確立しておくことが望ましい。

教育すべき内容としては、以下があげられる。

- セキュリティ管理情報とその保護管理の概要
- セキュリティ管理情報の保護管理策の詳細とその実施要領
- セキュリティ管理情報の保護管理に用いる技術とその運用
- セキュリティ管理情報に関する事故事例

教育内容は、サイトの運営形態やシステム構成、運用形態、さらには技術環境の進化を反映した、運用対象システムの実態に合ったものであるよう、随時見直しを行うこと。

(3) セキュリティ管理情報の保護管理に関する教育テキストの整備

セキュリティ管理情報の保護管理に関する教育をより効果的にするためには、サイトの運営実態に合ったセキュリティ管理情報の保護管理についてのテキストを準備することが望ましい。

また、このテキストについても、サイトの運営環境の変更を反映するよう定期的な見直しを行うことが望ましい。

【対策実施上のポイント】

(1) セキュリティ管理情報の保護管理についての教育カリキュラム例

表 6-10 に、セキュリティ管理情報の保護管理についての教育カリキュラムの一例を示す。

表 6-10 セキュリティ管理情報の保護管理についての教育カリキュラム例

項番	教育項目	教育対象者	頻度
1	セキュリティ管理情報とその保護管理の概要 ・セキュリティ管理情報に関する事故の脅威 ・セキュリティ管理情報の保護管理についての取組み ・セキュリティ管理情報の保護管理策の概要	・セキュリティ管理情報の保護関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者 ・業務上でのセキュリティ管理情報取扱い責任者	1回／年
2	セキュリティ管理情報の保護管理策の詳細とその実施要領 ・セキュリティ管理情報保護管理基準 ・運用規定、運用マニュアル上の関係事項 ・その他注意事項	・セキュリティ管理情報の保護関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者 ・業務上でのセキュリティ管理情報取扱い責任者	1回／年
3	セキュリティ管理情報の保護管理に用いる技術とその運用 ・サイトにおけるセキュリティ管理情報の保有状況 ・対象情報の保護技術 ・対象情報へのアクセス監視技術	・セキュリティ管理情報の保護関係者 ・システム開発関係者 ・システム管理関係者	1回／年
4	セキュリティ管理情報に関する事故事例	・セキュリティ管理情報の保護関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者 ・業務上でのセキュリティ管理情報取扱い責任者	1回／年

(13) セキュリティ管理情報の保護管理の実施状況についての監査を行う

【主旨】

セキュリティ管理情報の漏洩、改ざん、破壊は、サイトのセキュリティに直接的な脅威となるので、セキュリティ管理情報の保護管理の不備が問題をおこす前に、問題点を発見し適切な改善策を講じることができるようにしておくことも重要である。

このため、定められているセキュリティ管理情報の保護管理策がサイト運営の実態に照らして適切かどうか、また、セキュリティ管理情報の保護管理策として定められていることが適切に実施されているかどうか等についてのチェックを行い、問題点の摘出と必要な改善の指導を行う、セキュリティ管理情報の保護管理の実施状況についての監査を行うことも必要である。

また日常の運用の中で、実施したセキュリティ管理情報の保護管理にかかわる運用についての記録の保管等、この監査のための準備を組込んでおくことも必要となる。

(注) 正式な監査という形はとらなくとも、ここに示すようなセキュリティ管理情報の保護管理の実施状況についてのチェックは、組織的に行われるべきものである。

【具体的な実施事項】

(1) セキュリティ管理情報の保護管理の実施状況についての定期的な監査の実施

最低でも年1回は、以下に示すようなことをチェックする、セキュリティ管理情報の保護管理の実施状況についての監査を行う。

- セキュリティ管理情報の保護管理についての責任体制の整備状況とその機能状況
- セキュリティ管理情報保護管理基準の妥当性
- セキュリティ管理情報の個々に設定している保護管理要件の妥当性
- 個々のセキュリティ管理情報に対する保護管理の実施状況
- セキュリティ管理情報の保護管理に用いている機能の実装状況
- セキュリティ管理情報の漏洩、改ざん、破壊事故への備えの状況
- セキュリティ管理情報の保護管理にかかる施策のシステム運用への反映状況
- 業務運営上におけるセキュリティ管理情報にかかわる印刷物や電磁媒体の取扱い状況
- 業務委託先に対するセキュリティ管理情報の取扱いに対する指導、管理の実施状況
- 関係者のセキュリティ管理情報の保護管理についての認識

(2) 監査実施要領の確立

セキュリティ管理情報の保護管理についての定期的な監査が円滑に実施され、実効的なものになるようにするためには、この監査についての実施要領が確立されていることが望ましい。

監査実施要領で規定しておく事項については、2.2 節の(4)項参照のこと。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。

このためには、監査指摘事項に対する改善措置が実際にとられたかどうかについての確認を行うことも必要であり、指摘事項についてのフォローの仕組みも、監査要領の中に組込んでおくことも有効である。

【対策実施上のポイント】

(1) 監査内容例

表 6-11に、セキュリティ管理情報の保護管理の実施状況についての監査において監査すべき事項の例を示す。

(2) 監査結果は、セキュリティ管理情報の保護管理責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告しなければならない。

表 6-11 セキュリティ管理情報の保護管理の実施状況に関する監査内容例

項番	監査項目	監査の内容等
1	セキュリティ管理情報の保護管理についての責任体制の整備状況とその機能状況	・セキュリティ管理情報の保護管理についての責任体制は、サイトの運営実態に照らして適切か ・該当責任者における自己の責任についての認識は十分か ・セキュリティ管理情報の保護管理に関する責任体制は機能しているか
2	セキュリティ管理情報保護管理基準の妥当性	・セキュリティ管理情報の保護管理基準は、サイトの運営に照らして適切か
3	セキュリティ管理情報の個々に設定している保護管理要件の妥当性	・セキュリティ管理情報すべてに対して保護管理要件が定義されているか ・セキュリティ管理情報個々に設定されている保護管理要件は、保護管理基準やシステムの運営実態に照らして適切か
4	個々のセキュリティ管理情報に対する保護管理の実施状況	・システムにおけるセキュリティ管理情報の格納状況は、正確に把握されているか ・システム上での個々のセキュリティ管理情報の格納は、当該セキュリティ管理情報に指定されている保護管理要件を満足しているか ・システム上の個々のセキュリティ管理情報に対するアクセス制限は、当該セキュリティ管理情報に対する保護管理要件に指定されていることを満足しているか ・システム上の個々のセキュリティ管理情報に対するアクセス監視は、当該セキュリティ管理情報に対する保護管理要件に指定されていることを満足しているか ・システム上のセキュリティ管理情報に対する運用上の操作は記録されているか

表 6-11　セキュリティ管理情報の保護管理の実施状況に関する監査内容例

項番	監査項目	監査の内容等
5	セキュリティ管理情報の保護管理に用いている機能の実装状況	・セキュリティ管理情報の保護管理に使用する技術およびその機能選択は妥当か ・その実装の正確性は確認されているか（実装すべき場所に正確に実装されているか） ・運用環境の変更時における対応機能の実装の見直しは行われているか ・必要な運用環境の整備状況についてのチェックは適切に行われているか
6	セキュリティ管理情報の漏洩、改ざん、破壊事故への備えの状況	・セキュリティ管理情報の保護管理にかかる事故に対する対処要領は適切に決められているか ・監査期間における事故対策は妥当であったか
7	セキュリティ管理情報の保護管理にかかる施策のシステム運用への反映状況	・セキュリティ管理情報の保護管理にかかる諸施策がシステム運用に求めていることは、運用規定、運用マニュアルに適切に反映されているか ・これらの運用は、日々の運用において確実に実行されているか、またそのことが管理されているか ・セキュリティ管理情報の保護管理にかかる諸施策に関係するシステム運用の適切な実行の実現のための工夫は十分か
8	業務運営上におけるセキュリティ管理情報にかかわる印刷物や電子媒体や印刷物の取扱い状況	・セキュリティ管理情報をにかかわる印刷物や電子媒体の取扱い規定の確立状況 ・日常の業務運営上におけるこれらの取扱状況 ・日常の業務運営におけるこれらの取扱いについての指導、管理の実施状況
9	業務委託先に対するセキュリティ管理情報の取扱いについての指導、管理の実施状況	・業務委託先に対するセキュリティ管理情報の取扱いについての適切な取決めの締結状況 ・業務委託先に対するセキュリティ管理情報の保護管理に対する指導状況 ・業務委託先におけるセキュリティ管理情報の取扱いの妥当性 ・業務委託先に業務運営上でのセキュリティ管理情報の取扱いについての管理状況
10	関係者におけるセキュリティ管理情報の保護管理にかかる認識	・セキュリティ管理情報の保護管理の必要性についての認識は十分か ・セキュリティ管理情報の保護管理に用いている技術についての理解は十分か ・設定している保護管理基準についての理解は十分か ・セキュリティ管理情報の保護管理策とその運用についての理解は十分か

7 ユーザデータの保護管理の徹底

7.1 実施すべき施策

図 7-1 に、ユーザデータの保護管理策の体系を示す。

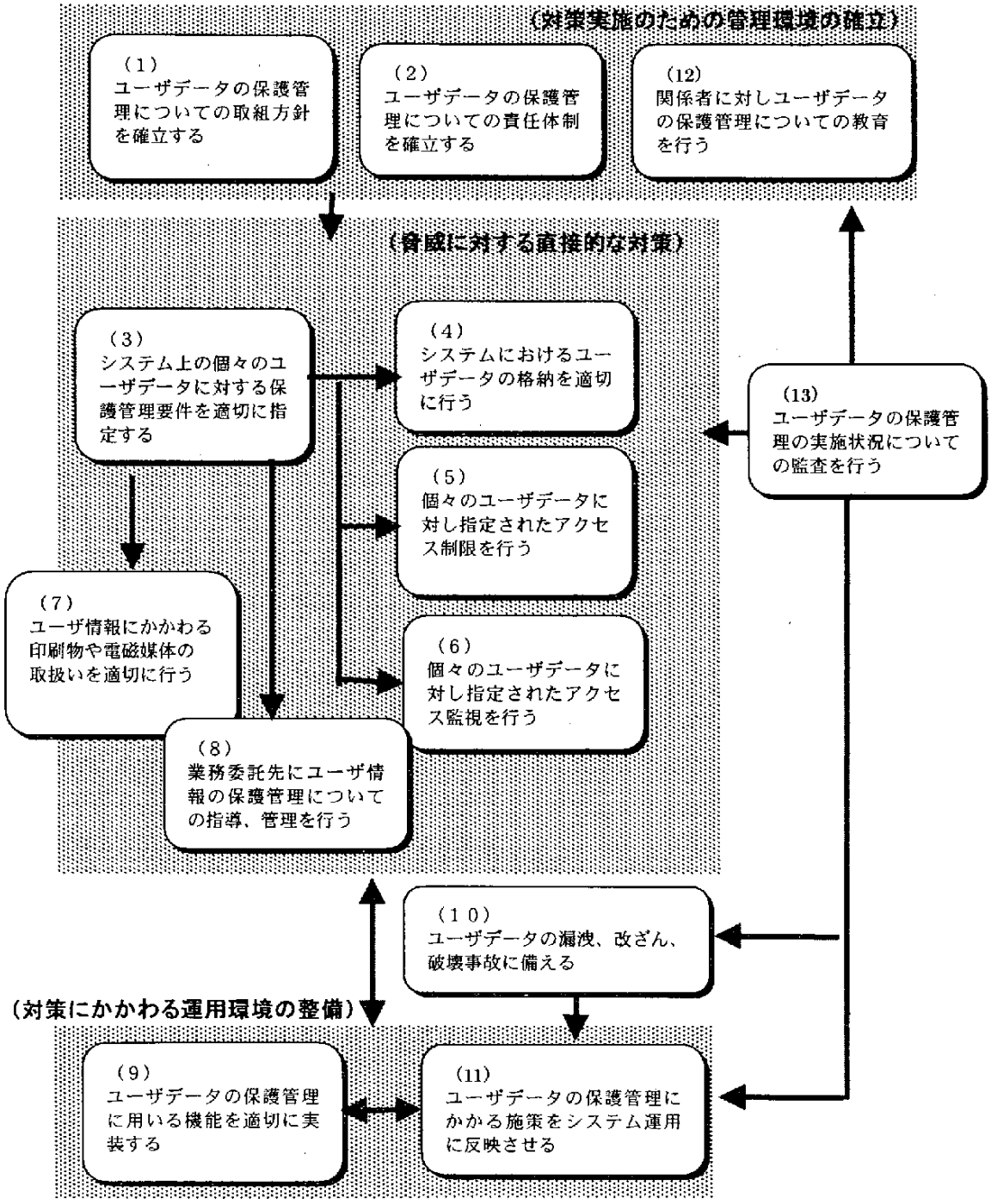


図 7-1 ユーザデータの保護管理策の組立て

また、表 7-1 に各施策における実施事項の一覧を示す。

表 7-1　ユーザデータの保護管理策としての具体的実施事項一覧

施策名	具体的実施事項
(1) ユーザデータの保護管理についての取組方針を確立する	① ユーザデータの保護管理の目標の明確化 ② 適用範囲の明確化 ③ ユーザデータの保護管理基準の確立 ④ ユーザデータの保護管理策の組立ての明確化 ⑤ ユーザデータの保護管理についての取組方針の関係者への周知
(2) ユーザデータの保護管理についての責任体制を確立する	① ユーザデータの保護管理についての責任体制の明確化 ② ユーザデータの保護管理関係者間の連携体制の確立
(3) システム上の個々のユーザデータに対する保護管理要件を適切に指定する	① 個々の保護対象ユーザデータに対する保護管理要件の指定 ② 個々のユーザデータに指定した保護管理要件に関するドキュメントの整備
(4) システムにおけるユーザデータの格納を適切に行う	① 指定された格納の実施 ② システム上でのユーザデータの格納状況の正確な把握 ③ ユーザデータの格納に関する運用処理の適切な実行
(5) 個々のユーザデータに対し指定されたアクセス制限を行う	① 指定されたアクセス制限の実施 ② アクセス制限に用いる権限情報等の適切な管理の実施 ③ アクセス制限の実施状況の正確な把握
(6) 個々のユーザデータに対し指定されたアクセス監視を行う	① 指定されたアクセス監視の実施 ② アクセス監視にかかる運用管理の確立 ③ 検知した不審なアクセスに対する適切な処置の実施 ④ アクセス監視の実施状況の正確な把握
(7) ユーザ情報にかかわる印刷物や電磁媒体の取扱いを適切に行う	① ユーザ情報にかかわる印刷物や電磁媒体の個々に対する保護管理要件の確立 ② 関係者の教育の実施 ③ 保護管理要件に従った保護管理の実施
(8) 業務委託先にユーザ情報の保護管理についての指導、管理を行う	① 適切な業務委託先の選定 ② 業務委託先における保護管理責任の明確化 ③ 業務委託先における保護管理状況の把握と必要な指導の実施

表 7-1　ユーザデータの保護管理策としての具体的実施事項一覧

施策名	具体的実施事項
(9) ユーザデータの保護管理に用いる機能を適切に実装する	① 適切な技術と使用する機能の選択 ② 組込み場所の適切な設定 ③ 選択した機能の適切な組込み ④ 必要な運用環境の整備 ⑤ 使用技術の実装についてのドキュメントの整備
(10) ユーザデータの漏洩、改ざん、破壊事故に備える	① ユーザデータに関するセキュリティ事故に対する処理要領の確立 ② ユーザデータに関するセキュリティ事故の処理に必要な情報の整備 ③ ユーザデータに関するセキュリティ事故による被害に備えたユーザデータの保全 ④ ユーザデータに関するセキュリティ事故を想定した事故処理訓練の実施 ⑤ 必要なツールの整備
(11) ユーザデータの保護管理にかかる施策をシステム運用に反映させる	① ユーザデータの保護管理にかかる施策の運用規定、運用マニュアルへの反映 ② 運用環境の変更への適切な対応の実施 ③ ユーザデータの保護管理にかかる定期作業のスケジュール化 ④ 関係運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行 ⑤ ユーザデータの保護管理にかかる運用処理についての記録と保管
(12) 関係者に対しユーザデータの保護管理についての教育を行う	① 関係者に対するユーザデータの保護管理についての教育の実施 ② ユーザデータの保護管理についての教育カリキュラムの確立 ③ ユーザデータの管理に関する教育テキストの整備
(13) ユーザデータの保護管理策の実施状況についての監査を行う	① ユーザデータの保護管理の実施状況についての監査の実施 ② 監査実施要領の確立 ③ 監査指摘事項に対するフォローの実施

7.2 個別具体策

(1) ユーザデータの保護管理についての取組方針を確立する

【主旨】

その取扱い上の問題が、ショップならびにサイトの信用に大きくかかわる、消費者や取引先に関する情報を含むユーザデータの保護管理を徹底し、その漏洩等の事故の防止を図るとともに、万一、このような事故が発生しても、その被害を限定的なものにすることに組織的に取組むには、ユーザデータの保護管理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示すユーザデータの保護管理についての取組方針を確立し、これを、ユーザデータの保護管理に直接かかわる者だけでなく、システムの構築や運用に関係する者、さらにはサイトやショップの運営上ユーザ情報に触れる者のすべてに、周知させておくことが必要となる。

【具体的な実施事項】

(1) ユーザデータの保護管理の目標の明確化

ユーザデータの保護管理が目指すところを明確にし、ユーザ情報の保護管理に関する諸施策の意図を明確にする。ユーザデータの保護管理の目標としては、以下があげられる。

- ユーザデータの漏洩の防止
- ユーザデータの改ざん、破壊の阻止
- ユーザデータに関するセキュリティ事故発生時の被害の極小化

(2) 適用範囲の明確化

ユーザデータの保護管理策の適用範囲として、以下を明確にする。

- システム構成上の対象領域および対象サーバ等の機器
- 対象とする電磁媒体
- 対象とする印刷物
- 対象とする組織
- 対象とする業務、作業

ユーザデータの保護管理は、システム上に格納された情報だけでなく、これらの情報が含まれる電子媒体や印刷物も対象となるため、その規定が及ぶところの明確化は重要である。

(3) ユーザデータの保護管理基準の確立

ユーザデータに求められる保護管理は、対象とするユーザデータのライフサイクルやシステム上での保管形態や、漏洩や破壊等の保護管理上の事故が発生した場合の影響の大きさ等により異なる。このため、すべてのユーザデータに同じような保護管理を適用することは、運用上現実的でない。

実際に実施する保護管理策は、個々の情報ごとに決めなければならないが、それぞれは全

体として統制のとれたものでなければならない。このことを実現するためには、保護管理に厳格さによるレベル分けを行い、それぞれのレベルに対する標準的な保護管理要件を定義したユーザデータの保護管理基準を確立しておき、対象情報ごとに適用する保護管理レベルを割り当て、そのレベルに対し規定されている保護管理要件に基づいた保護管理を実施するような工夫も必要となる。

ユーザデータの保護管理基準として定義すべき事項をあげると以下のようになる。

- 保護管理レベルの名称
- 当該レベルの適用範囲
- システム上の対象ユーザデータに対する操作単位で規定するアクセス権限条件
- 電磁媒体、印刷物の取扱いについての要件
- 業務上の取扱い制限
- システムへの格納についての要件
- アクセス監視についての要件
- 保全についての要件

保護管理の要件は、当該レベルが適用されるデータが保有する情報の重要度に依存する。

(4) ユーザデータ保護管理策の組立ての明確化

ユーザ情報の保護管理をどのように行うかを明らかにするため、実施する施策の構成とその施策間の関係を示す。

本ガイドラインにおけるユーザデータの保護管理に関する諸施策の構成については、7.1 節参照。

(5) ユーザデータの保護管理についての取組方針の関係者への周知

作成されたユーザデータの保護管理についての取組方針は文書化され、ユーザデータの保護管理に直接かかわる者だけでなく、サイトの構築ならびに運用関係者、業務上ユーザデータに触れる者等の関係者に周知させておかなければならない。このためには、

- ユーザデータの保護管理についての取組方針の掲示や配布
- 関係者間での定期的なユーザデータの保護管理の取組方針についての確認

も必要となる。

【対策実施上のポイント】

(1)ユーザデータの保護管理基準の定義要領

ユーザデータの保護管理基準を定義するにあたって指定すべき事項を表 7-2 に示す。

表 7-2　ユーザデータの保護管理基準における定義項目

項番	定義項目	定義内容
1	保護管理レベルの名称	・当該保護管理レベルの名称、ID
2	当該レベルの適用範囲	・当該レベルが適用の対象となるユーザ情報の重要度クラス
3	システム上の対象ユーザデータに対する操作単位に定めるアクセス制限	・対象ユーザデータの登録、更新、削除等そのライフサイクルにかかわる操作に対する権限の対象範囲 （例）－当該情報の保護管理責任者 －当該情報の保護管理担当チーム員 ・当該ユーザデータの登録、更新、削除等そのライフサイクルにかかわらない照合のための読取り等その使用に限定したアクセスについての権限の対象範囲 （例）－当該情報の保護管理責任者 －当該情報の保護管理チームの一員 －業務で当該情報へのアクセスが必要な者、あるいはプログラム －システムのメンテナンスにかかわる者 －システムの運用管理者 －システムの運用担当者
4	電磁媒体や印刷物の取扱いについての要件	・対象ユーザデータの電磁媒体や印刷物について取得、保管、利用権限を持つ者を指定 （例）－当該電磁媒体や印刷物の保護管理責任者 －当該情報の保護管理チームの一員 －当該情報にかかわる業務の管理に従事している者 －システムのメンテナンスにかかわる者 －システムの運用管理者 －システムの運用担当者
5	業務上での取扱い制限	・当該ユーザデータの生成、登録、更新、削除等そのライフサイクルにかかわる処理の手続き上、当該情報およびその操作に触れることできる者の対象範囲 （例）－当該情報の保護管理責任者 －当該情報の保護管理チームの一員 －当該情報にかかわる業務の管理に従事している者 －システムのメンテナンスにかかわる者 －システムの運用管理者 －システムの運用担当者 ・対象ユーザデータの内容の秘匿にかかる注意事項等
6	対象ユーザデータのシステムへの格納についての要件	・システム上での当該情報の格納方法についての指定 （例）－暗号化して保管 －一般ファイルとしての保管

表 7-2　ユーザデータの保護管理基準における定義項目

項番	定義項目	定義内容
7	当該ユーザデータに対するアクセス監視についての条件	・当該ユーザデータに対するアクセス監視の要否および実施についての以下に示すような事項に関する指定 －動的アクセス監視を適用 －月１回以上の頻度全てのアクセスをチェック －アクセス監視対象外
8	保全要件	・当該ユーザデータのバックアップの取得と、その保管に関する以下に示すような事項についての指定 －バックアップの取得サイクル －バックアップの保管世代 －バックアップの保管期間 －バックアップの物理的な保管要件

(2) ユーザデータの重要度についての考え方

ユーザデータの重要度とは、漏洩や改ざん、破壊等の事故が発生した場合における影響の大きさの尺度を示すもので、当該情報に求められる保護管理の厳格さを決める時の判断材料となるものである。

ユーザデータについての重要度についてクラス化を行い、対象情報に対する保護管理レベルの割当は、対象ユーザデータに指定された重要度クラスによるようにすることも、ユーザデータに対する保護管理がサイト全体として統制あるものにするためには有効である。

表 7-3 にユーザデータの重要度クラスの定義例を示す。

表 7-3　ユーザデータの重要度クラスの定義例

項番	重要度クラス	重要度の尺度	情報例
1	クラスA	その漏洩、改ざんは、ユーザに直接的な損害を与える可能性があり、かつ損害も大きなものになる可能性のある情報を含むデータ	個人特定情報 信用情報 経営情報
2	クラスB	その漏洩、改ざんは、ユーザに直接的な損害を与える可能性はあるが、その損害の規模は限定的なもの	個人健康情報 取引情報
3	クラスC	その漏洩、改ざんは、ユーザに直接的な損害は与えないものの、ユーザとの間でトラブルになる恐れのあるもの	一般属性情報
4	クラスD	その漏洩、改ざんは、ユーザに直接的な損害を与えはしないものの、業務に一時的なトラブルを生じたり、サイトやショップの信頼を傷つける恐れのあるもの	ショッピング情報 個人活動情報

(3) ユーザデータの保護管理基準の定義例

表 7-4 に、ユーザデータの保護管理基準の定義例を示す。

表 7-4 ユーザデータの保護管理基準の定義例

項番	保護管理レベル	当該レベルにおけるユーザデータの保護管理要件
1	レベルA	・適用対象・・・・・・・・・・・・・・・・・・・・・・・・重要度クラスAのユーザデータ ・特定操作の権限条件・・・・・・・・・・・・・・当該情報の保護管理担当者 ・使用権限条件・・・・・・・・・・・・・・・・・・・・業務上での取扱い責任者 ・電子媒体等の取扱い要件・・・・・・・・・・(省略) ・業務上の取扱い制限・・・・・・・・・・・・・・業務上での取扱い担当者 ・システムへの格納についての要件・・・暗号化して保管 ・アクセス監視要件・・・・・・・・・・・・・・・・すべてのアクセスをチェック ・保全要件・・・・・・・・・・・・・・・・・・・・・・更新の都度バックアップを取得
2	レベルB	・適用対象・・・・・・・・・・・・・・・・・・・・・・・・重要度クラスBのユーザデータ ・特定操作の権限の付与・・・・・・・・・・・・当該情報の保管管理担当者 ・使用権限の付与条件・・・・・・・・・・・・・業務上での取扱い担当者 ・電子媒体等の取扱い要件・・・・・・・・・・(省略) ・業務上の取扱い制限・・・・・・・・・・・・・・業務上での取扱い担当者 ・システムへの格納についての要件・・・一般ファイルとして保管 ・アクセス監視要件・・・・・・・・・・・・・・・・月1回以上アクセス状況をチェック ・保全要件・・・・・・・・・・・・・・・・・・・・・・月次処理実行後に取得

(4) ユーザデータの保護管理についての取組方針は、システム構成やその運用形態等、システム運用の実環境の変化に対応して必要な修正が加えられるべきであり、必要に応じて見直しを行うこと。

(5) ユーザデータの保護管理についての取組方針は、定期的に関係者間で再確認することをルーチン化しておくことが望ましい。

(2) ユーザデータの保護管理についての責任体制を確立する

【主旨】

ユーザデータの保護管理策を、その取組方針に沿って機能させるためには、ユーザデータの保護管理策として定められていることが、システムの構築や運用に適切に反映されるよう、指導、管理する責任体制の確立が必要となる。

このためには、ユーザデータの保護管理にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) ユーザデータの保護管理についての責任体制の明確化

ユーザデータの保護管理についての責任体制に関し、明確にしておくべきこととしては、以下があげられる。

- ユーザデータの保護管理責任者とその責任
- システム上のユーザデータに対する保護管理実施担当者の責任
- システム開発者のユーザデータの保護管理に関する責任
- システム管理者のユーザデータの保護管理に関する責任
- システム運用者のユーザデータの保護管理に関する責任
- 業務現場におけるユーザ情報の取扱い責任者の責任
- ユーザ情報の取扱いにかかわる業務の外部への業務委託責任者の責任

(2) ユーザデータの保護管理関係者間の連携体制の確立

ユーザデータの保護管理に関する責任体制が有効に機能するためには、関係者間の連携が必要となる。

【対策実施上のポイント】

(1) ユーザデータの保護管理にかかる責任者の責任分担

表 7-5 に、ユーザデータの保護管理にかかる責任者の責任分担の定義例を示す。

(2) ユーザデータの保護管理に関する責任体制は、ユーザデータの保護管理策が変更になったり、サイトの運営形態に変更に生じた場合は、見直しを行い、必要な変更を行うこと。

表 7-5　ユーザデータの保護管理関係者の責任分担

責任区分	タスク
ユーザデータの保護管理責任者	・ユーザデータの保護管理についての取組方針の確立の関係者への周知 ・ユーザデータ保護管理基準の発行 ・ユーザデータの保護管理策全体の妥当性の維持 ・ユーザデータの保護管理の実施状態のチェック ・保護管理基準に従ったユーザデータの保護管理の実施についての指導 ・ユーザデータにかかるセキュリティ事故発生時の対処の指揮
システム上のユーザデータの保護管理担当者	・システムが保有しているユーザデータの現状把握 ・システムが保有しているユーザデータの保護の監督、管理 ・必要な機能の的確な実装 ・ユーザデータの保護管理に関する事故発生時における事故処理と、再発防止策の検討
システム開発者	・開発システムにおける関係機能の適切な組込み －設計の妥当性の確認 －正確な実装の確認
システム管理者	・システムにおけるユーザデータの保護管理機能の維持 －システム構成の変更の反映の管理 －ユーザデータの保護管理支援機能の動作環境の維持管理 ・システムにおける対応機能の実装状況の正確な把握
システム運用者	・ユーザデータの保護管理にかかる適切なシステム運用環境の整備 ・ユーザデータの保護管理にかかる運用のチェックと指導
業務現場におけるユーザ情報の取扱い責任者	・業務現場でのユーザ情報の取扱い状況の把握 ・業務現場で取扱われるユーザ情報の適切な取扱いについての監督、管理 ・ユーザ情報に関する事故発生時における業務現場サイドでの対処
ユーザ情報の取扱いにかかわる業務の外部への業務委託責任者	・委託先におけるユーザ情報の保護管理責任の明確化 ・委託先におけるユーザ情報の保護管理の実施状態のチェック ・基準に従ったユーザ情報の保護管理の実施についての指導

(3) システム上の個々のユーザデータに対する保護管理要件を適切に指定する

【主旨】

ユーザデータの保護管理を適切に行うためには、個々の保護対象情報に対し、どのような保護をどのように行うかを定めた保護管理要件が、当該ユーザデータに適用される保護管理レベルに指定されている保護管理基準に沿って適切に決められていなければならない。

この要件の定義にあたっては、保護対象情報ごとに、そのライフサイクルを意識して、考えられる脅威を考慮しなければならない。

ユーザデータは、システム上だけでなく、印刷物や電磁媒体上にも置かれるが、これらについては保護管理の手段がシステム上のものと大きく異なるため、その扱いについては別項で述べる。
"(7)ユーザ情報を含む印刷物や電磁媒体の取扱いを適切に行う"参照

【具体的な実施事項】

(1) 個々の保護対象ユーザデータに対する保護管理要件の指定

個々の保護対象ユーザデータに対し、どのような保護管理を、どのような方法で行うかについて、以下に示すようなことを指定する。

- 当該ユーザデータが保有する保護対象ユーザ情報
- 当該ユーザデータに適用する重要度クラス
- 適用する保護管理レベル
- 適用するアクセス制限の詳細
- システム上での格納方法
- 適用するアクセス監視の詳細
- システムへの格納、アクセス制限、アクセス監視に使用する技術とその使用条件
- 保全に関する要件

(2) 個々のユーザデータに指定した保護管理要件に関するドキュメントの整備

ユーザデータに対する保護管理が、適切に行われているかどうかについての管理が行えるように、当該サイトで実施されているユーザデータの保護管理の実施状況が一覧できるドキュメントの整備を行い、何時でも正確にその内容が把握できるようにしておくことも必要となる。

このドキュメントで明らかにすべき事項は、保護管理対象ユーザデータのすべてに対する(1)項であげた項目となる。

また、このドキュメントは、業務におけるユーザ情報の取扱い方法の変更、システムにおけるユーザデータの取扱い方式の変更、システムの運用環境等に変更等にともなう保護管理要件の変更が適切に反映されたものになっているようになっていなければならない。

【対策実施上のポイント】

(1) 個々の保護対象ユーザデータに対する保護管理要件の定義要領

表 7-6 に、個々の保護対象ユーザデータに対する保護管理要件の定義で指定すべき事項を示す。

表 7-6 ユーザデータに対する保護管理要件定義におけるの定義項目

項番	定義項目	定義内容
1	当該ユーザデータが保有する保護対象ユーザ情報	・当該ユーザデータに含まれる保護対象となるユーザ情報 （例）個人情報、資産経営情報、取引情報 ・対象としたユーザ情報が漏洩、改ざん、破壊された時の影響
2	適用する重要度クラス	・当該ユーザデータに割当てるユーザデータの重要度クラス
3	適用する保護管理レベル	・当該ユーザデータに割当てるユーザデータの保護管理基準で定義されている保護管理レベル
3	適用するアクセス制限の詳細	・当該ユーザデータに適用するアクセス制限を指定する （注）保護対象ユーザデータに対するアクセス権限の定義については(2)参照
4	システム上での格納方法	・保護管理上から特別の格納を行う場合、以下に示すような事項についての指定を行う －暗号化の要否と必要な場合の暗号化の要件 －特殊な専用装置の使用 －他データとの隔離についての要件
5	適用するアクセス監視	・アクセス監視の要否 ・必要な場合における、アクセス監視の要件 (注)アクセス監視の要件の定義については(3)参照
6	システムへの格納、アクセス制限、アクセス監視に使用する技術とその使用方法	・システム上での保管に用いる技術と使用機能 ・アクセス制限に用いる技術と使用機能 ・アクセス監視に用いる技術と使用機能
7	保全要件	・バックアップの取得等当該ユーザ情報の保全に関する以下に示すような事項についての指定 －バックアップの取得サイクル －保管期間、保管世代、保管場所等のバックアップの保管に関する要件 －バックアップからの回復手順

(2) ユーザデータに対するアクセス制限の要件定義要領

ユーザデータへのアクセス制限についての要件定義において指定すべき事項を、表 7-7 に示す。

表 7-7 ユーザデータへのアクセス制限に対する要件定義における定義事項

項番	定義項目	定義内容
1	当該ユーザデータに対するシステム操作の権限保有者	・システム上の当該ユーザデータに対する操作の権限保有者を、下記の操作単位に指定する。 －個別データの登録 －個別データの参照 －個別データの印刷、他の電子媒体へのコピー －個別データの更新 －個別データの削除 －システム上の当該情報の二次加工 －データ全体の印刷 －データ全体のコピー －データ全体の抹消 －データのバックアップの取得 －データの再編集 ・権限保有者(人またはプログラム)はその資格名を指定する
2	権限保有者の指定登録方法	・権限保有者の登録管理方法 ・権限情報の管理方法
3	適用するアクセス管理方式	・適用する技術または方式の指定 (例) －OSやデータベース管理の持つ機能の使用 －特殊な専用装置の使用 －独自仕様の適用 ・使用機能の使用方法(機能設定等)の指定
4	不審アクセスに対する処置	・アクセス管理で不審アクセスが検知された場合のシステムならびに業務上での処置を定義

(注1)ユーザデータのアクセス制限に用いられる権限情報は、特別の管理が求められるセキュリティ管理情報のひとつである。その保護管理については、第 6 章の**"セキュリティ管理情報の保護管理"**参照。

(3) アクセス監視についての要件定義要領

ユーザデータへのアクセス監視の要件定義において指定すべき事項を、表 7-8 に示す。

表 7-8　ユーザデータへのアクセス監視の要件定義における定義事項

項番	定義項目	定義内容
1	監視対象	・監視すべきイベントを定義 ・不審アクセスの定義
2	監視方法	・監視に用いる技術とその機能の設定 ・監視ポイント ・不審アクセス検知時の報告方法
3	監視の運用	・不審アクセス監視責任者の指定 ・定期的なチェック実施についての指定 ・不審アクセスが報告されたときの対処要領

(4) バックアップデータの取扱いについて考え方

- バックアップバックアップ取得サイクルの決定にあたっては、復旧時間のみでなく扱うデータ量、更新頻度等も考慮の上決定する
- バックアップ媒体は、安全な方法で、決められた期間保管する
- バックアップの頻度については、システムの可用性により判断する
- バックアップした日付、内容、媒体などを記録しておく
- 複数世代のバックアップデータを保存する
- 廃棄の手順を明確にしておく

(5) システムが扱うユーザデータの把握について

システム上の個々のユーザデータに対する保護管理要件の設定が適切に行われるようにするためには、システムが扱っているユーザデータの取扱い状況が正確に把握されていなければならない。

このためには、以下の情報は常に整理把握されていなければならない。

- システムの処理対象となっているユーザデータの体系
- システムにおけるユーザデータの配置状況
- ユーザデータとプログラムとの関係
- 個々のユーザデータのライフサイクル
  - －生成、登録、参照、更新、抹消等が、業務との関係でどのような形態で行われているか
  - －変動特性(更新頻度、参照頻度、寿命等)

(6) システム上のユーザデータの保護管理に適用する方式の検討について

システム上のユーザデータ個々に対する格納、アクセス制限、アクセス監視に適用する方式の選択に当っては、保護管理要件と、ユーザの使い勝手、コスト、運用環境の手間等のバランス

を考慮すること。

(7) システム上のユーザデータに対する脅威について

個々のユーザデータに対する保護管理要件の設定にあたっては、当該ユーザデータに対する脅威の分析が必要である。この脅威の分析では、当該ユーザデータのライフサイクルの各ステージにおける、考えられる脅威とその影響および脅威の抑止を検討する。

検討対象の脅威をあげると以下のようになる。

- 外部ネットワークからの不正アクセス
- 情報の電子的交換時の盗聴、改ざん、漏洩
- 保管状態にある物理的媒体(印刷物、電磁媒体等)の盗難・紛失
- 機器のメンテナンス、媒体の廃棄処分等に起因する無権限者による閲覧、コピー
- 媒体のデリバリー途上の盗難・紛失
- オペレーションに起因するファイル等システムの破壊・破損・不正コピー

(4) システムにおけるユーザデータの格納を適切に行う

【主旨】

システム上でのユーザデータ格納場所や格納方法は、それぞれのユーザデータに指定された保護管理要件に従っていなければならない。特に専用保管装置の使用や暗号化等の特別な格納方法が指示されている場合は、その実現方法について十分な検討と管理が必要となる。

【具体的な実施事項】

(1) 指定された格納の実施

ユーザデータはシステムにおいて、当該情報の保護管理要件で指定された方法により格納しなければならない。

このためには、必要な装置や機能のシステムへの組込みや、これらに必要とされる設定は適切なものでなければならない。

これらの機能の実装の管理については、**(9)項"ユーザデータの保護管理に用いる機能を適切に実装する"**の項参照。

(2) システム上でのユーザデータの格納状況の正確な把握

システムにおけるユーザデータの格納状況は、常に正確に把握されていなければならない。一覧表等のドキュメントの整備が求められる。

ユーザデータの格納状況に関して把握しておくべき情報としては、以下のようなものがあげられる。

- システム上での格納場所(使用装置、アドレス等)
- 格納方式(使用データベース管理ソフトおよびその使用法、暗号化方法等)
- 当該情報を使用するアプリケーションまたはシステム管理機能

(3) ユーザデータの格納に関する運用処理の適切な実行

システム上のユーザデータについての、

- 新規登録または更新
- 収容方式、収容場所等システムにおける格納形態の変更
- ファイルの再編集等の編成変え

等の保管にかかる運用処理の実行にあたっては、

- 決められた手順に従った計画、承認、実行、事後処理
- 処理の記録

を適切に行わなければならない。

(5) 個々のユーザデータに対し指定されたアクセス制限を行う

【主旨】

システム上のユーザデータには、個々のユーザデータごとに設定されたアクセス制限要件に従ったアクセス制限が、的確に行われていなければならない。

【具体的な実施事項】

(1) 指定されたアクセス制限の実施

システム上のユーザデータには、当該情報に対する保護管理要件で指定されたアクセス制限が、的確行われていなければならない。

このためには、必要な装置や機能のシステムへの組込みや、これらに必要とされる設定が適切なものでなければならない。

これらの機能の実装の管理については、**(9)項"ユーザデータの保護管理に用いる機能を適切に実装する"**の項参照。

(2) アクセス制限に用いる権限情報等の適切な管理の実施

ユーザデータに対するアクセス制限をサポートする機能は、当該ユーザデータに対するアクセス権限情報と、アクセスしようとしているユーザまたはプログラムの認証に基づいている。このため、ユーザデータに対するアクセス制限が期待通り機能するためには、当該情報に対して定められている保護管理要件に従った、

- アクセス権限情報の適切な設定
- 決められた手順に沿ったアクセス権限情報のシステムへの登録
- アクセス権限者の認証情報の適切な設定
- 決められた手順に従ったアクセス権限者の認証情報の登録

が適切に行われるようになっていなければならない。

(3) アクセス制限の実施状況の正確な把握

システムにおけるユーザデータに対するアクセス制限の実施状況は、常に正確に把握されていなければならない。一覧表等のドキュメントの整備が求められる。

ユーザデータに対するアクセス制限の実施状況に関し、把握しておくべき情報としては、以下のようなものがあげられる。

- 適用方式、使用機能
- 個別アクセスにおけるアクセス制限の設定状況
- 認証用情報、権限情報等の取扱い状況

(6) 個々のユーザデータに対し指定されたアクセス監視を行う

【主旨】

ユーザデータに対する権限のない者による不正なアクセスは、サイトのセキュリティ全体に対する脅威となるため、セキュリティ管理情報への不正アクセスは見逃さないようにしなければならない。

ユーザデータに対する不正なアクセスの試みが、どのような形でどの程度行われているかをチェックするユーザデータを対象としたアクセス監視は、ユーザデータの漏洩や改ざん、破壊事故の早期発見のためにも、ユーザデータの保護管理策の脆弱性を発見するためにも重要である。

このため、保護管理要件でアクセス監視の実行が指定されているユーザデータに対しては、指定に沿ったアクセス監視が適切に行われなければならない。

【具体的な実施事項】

(1) 指定されたアクセス監視の実施

アクセス監視が指定されたユーザデータについては、保護管理要件で指定されたアクセス監視が適切に行われなければならない。このためには、

- ユーザデータに対するアクセス監視に必要な機能のシステムへの実装
- アクセス監視ログの適切な分析

を適切に行うことが必要となる。

① システムへのアクセス監視に必要な機能の適切な実装

アクセス監視のためにシステムに実装すべきものとしては、

- セキュリティ管理情報へのアクセスを監視する機能
- セキュリティ管理情報へのアクセスの記録機能と表示機能
- アクセス監視条件の設定

がある。

これらの機能の実装の管理については、**(9)項"ユーザデータの保護管理に用いる機能を適切に実装する"**の項参照。

② アクセスログの分析の実施

アクセスログについては、当該情報の保護管理で定義された頻度で、指定されたチェックを行う。

(2) アクセス監視にかかる運用管理の確立

実装した機能およびその実行環境に基づき、アクセス監視に関する運用について下記のような事項を明確にするとともに、システムの運用に反映させる。

- ユーザデータへのアクセス記録の定期的なチェック
- ユーザデータへのアクセス記録の保管期間の設定
- 不審アクセスを検知した場合の処理

(3) 検知した不審なアクセスに対する適切な処置の実施

不審なアクセスを検知した場合の処置は、以下の処置を適切に行わなければならない。

- 不正アクセスの成功の有無
- 成功している場合における被害の確認
- 不正アクセスを許した原因の調査と再発防止策の検討、実施

また、不正アクセスが成功していない場合にも、検知された不審アクセスに対し、脆弱点はないかどうかのチェックも行うことが望ましい。

(4) アクセス監視の実施状況の正確な把握

システムにおけるユーザデータに対するアクセス監視の実施状況は、常に正確に把握されていなければならない。一覧表等のドキュメントの整備が求められる。

ユーザデータに対するアクセス監視の実施状況に関し、把握しておくべき情報としては、以下のようなものがあげられる。

- アクセス監視に用いる技術とその使用方法
- 個別アクセスにおけるアクセス監視条件の設定状況
- アクセス監視の結果
- 不審アクセスに対し実施した処置

(7)ユーザ情報がかかわる印刷物や電磁媒体の取扱いを適切に行う

【主旨】

ユーザデータにかかわる印刷物等ユーザデータそのものが可視できる状態にあるものや、ユーザデータが記録された電磁媒体等については、システム上のデータとは別の保護対策を確立しておく必要がある。従って、システム上のユーザデータに対する保護管理と同様、これらの印刷物や電磁媒体それぞれについても保護管理要件を確立する必要がある。

ユーザデータが記録された電磁媒体等は、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、更に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。このため、電磁媒体等の保護管理は特に厳格に行う必要がある。

(注)電磁媒体等とは、磁気テープや磁気ディスク、光ディスク等々の他、パソコン、サーバ、携帯端末等の本体内蔵の記憶装置・ディスク類を指す。

【具体的な実施事項】

(1) ユーザ情報にかかわる印刷物や電磁媒体の個々に対する保護管理要件の確立

ユーザ情報が関係する印刷物や電磁媒体等に対しては、システム上のこれらの情報を含むデータとは別の保護管理要件が必要となる。

これらに指定する保護管理要件として定義しておくべき事項としては、以下のようなものがあげられる。

- 作成に関する制約
- 外部との授受に関する条件
- 保管、保有に関する制限
- 使用に関する制限コピー
- 廃棄に関する要件
- 表示に関する条件

(2) 関係者の教育の実施

業務上、ユーザ情報に記載した印刷物やユーザデータが記録された電磁媒体を取扱う者に対しては、その保護管理の教育を定期的に実施し、周知徹底を図る必要がある。

(3) 保護管理要件に従った保護管理の実施

日常の業務の運営において、ユーザデータに対し定められた保護管理は厳格に守られなければならないが、現実には、実行が伴わないことが多い。

このため、その実行について、常にチェックを行い、問題点の指摘を行う管理、指導を行い、これらの運用が習慣化するようにする管理面での努力も必要である。

【対策実施上のポイント】

(1) ユーザ情報がかかわる印刷物、電磁媒体に対する保護管理要件の定義要領

表 7-9 に、ユーザ情報がかかわる印刷物、電磁媒体に対する保護管理要件で定義すべき事項を示す。

表 7-9 ユーザ情報がかかわる印刷物、電磁媒体に対する保護管理要件における定義項目

項番	定義事項	定義内容
1	作成に関する制約	・作成者に関する条件 ・使用目的の限定等、作成にあたっての条件 ・作成の手続き ・作成についての記録とその保管
2	外部との授受についての条件	・授受の相手に関する条件 ・授受にあたっての条件の指定 ・授受に関する手続き ・授受についての記録とその保管
3	保管、保有に関する制限	・保管可能条件(使用目的、権限保有者の範囲) ・保管期間に関する条件 ・保管場所、保管管理の方法についての条件
4	使用に関する制限コピー	・参照にあたっての条件 ・2次加工にあたっての条件 ・更新等内容に対する操作の条件
5	廃棄に関する要件	・廃棄方法の明示 (特に電磁媒体等については、内容の消去方法、その確認についての指定も必要)
6	表示に関する条件	・保護対象物であることの表示 ・作成者、保管者の表示 ・作成日、廃棄予定日の表示

(2)ユーザ情報がかかわる印刷物や電磁媒体の管理についての基本的な考え方

ユーザ情報がかかわる印刷物や電磁媒体の管理についての基本的な考え方としては、以下のようなことをあげることができる。

- システム上のユーザデータの印刷や外部記憶媒体へのコピーを制限する

  これらの管理に漏れがないようにするための基本は、ユーザデータについての印刷物や、これらの内容をコピーした電磁媒体を必要最小限とし、管理対象を絞り込むことにある。

システム上のユーザデータの印刷や外部記録媒体へのコピーは、許された目的に限り、権限を持つものだけが実行できるようにしておかなければならない。

- ユーザに関する印刷物等については、極力保管せずに速やかに廃棄するようにする

(3) これらに対する基準は、社内の文書管理規定と連携を取っておくことが望ましい。場合によっては、社内文書管理規定に含ませることも考えられる。

(8) 業務委託先にユーザ情報の保護管理についての指導、管理を行う

【主旨】

ショップ運営あるいはサイト運営にかかる業務のすべてまたは一部を外部に委託しているような場合、保護対象ユーザ情報の取扱いに、この委託先がかかわることもある。このような場合、ユーザ情報の保護管理の実現には、委託先においてもユーザ情報の保護管理が適切に行われることが必要となる。

このためには、適切な業務委託先を選定するとともに、業務委託先に対するユーザ情報の保護管理について管理、指導の実施が必要となる。

【具体的な実施事項】

(1) 適切な業務委託先の選定

業務委託先におけるユーザデータの適切な保護管理を期待するための第 1 歩は、信頼できる委託先を選ぶことにある。

このため、業務委託先の選定にあたっては、

- 企業の経営体質
- ユーザ情報の保護についての取組み

をチェックすることが必要である。

(2) 業務委託先における保護管理責任の明確化

ユーザ情報を扱う業務を委託する場合は、業務委託契約の中等で、ユーザ情報の取扱いについて規定を設け、委託先におけるユーザ情報の保護管理についての履行義務と責任を明確にしておくことが必要である。

(3) 業務委託先における保護管理状況の把握と必要な指導の実施

業務委託先において、業務委託契約等で定めたユーザ情報の保護管理が適切に行われているかどうかのチェックを定期的に行い、問題があれば指導を行う必要がある。

これらのことを適切に行うためには、

- 業務委託先におけるユーザ情報の保護管理の状況についての情報の収集
- 適切な保護管理の実施のための連絡体制の構築

等も必要となる。

【対策実施上のポイント】

(1) 業務委託先の選定時における適格性の判断基準としては、以下のようなものをあげることができる。

- 情報保護に関し、従業員の義務が就業規則等で規定されているか

- 情報保護についての従業員の教育は行われているか
- 情報保護の責任者は明確になっているか
- 業務規定で、情報保護についての適切な規定があり、かつ、それらは実務上で実際にまもられているか

プライバシマークの取得は、安心材料の一つとなる。

(2) 業務委託にあたって、契約書等で、ユーザ情報の保護管理の責務の定義として取り決めておきたい事項としては、以下のようなものがあげられる。

- 委託先の責任の範囲
- 保護管理責任者の指定
- 保護管理基準の制定
- 保護管理の運用の励行
- 保護管理についての関係者の教育
- 保護管理の実施状況についての報告
- 保護管理上の事故の報告と適切な処理

(9) ユーザデータの保護管理に用いる機能を適切に実装する

【主旨】

ユーザデータの保護管理に用いられる技術としては、

- 特殊な格納のために用いる機能
- アクセス制限に用いる機能
- アクセス監視に用いる機能

があり、その実現方法としては、

- 専用機器の使用
- OS の機能や、データベース管理の機能や、アプリケーションに組込まれた機能の使用
- 独自の仕様による実現

を選択することができるが、いずれの場合においても、期待通りに機能し、対象とするユーザデータの保護管理要件に準じた保護管理を実現するものでなければならない。

このためには、技術の選択と選択した技術における使用機能の選択、インストール時の設定等を的確に行うとともに、そのインストールに対する検査も十分に行うことが必要となる。

また、これらのデータへのアクセス制限の実行に必要な権限情報や利用者の認証情報等、使用する技術が前提とする運用環境の整備にも漏れがないようにしなければならない。

【具体的な実施事項】

適用する技術の個々に対し、以下のことが求められる。

(1) 適切な技術と使用する機能の選択

ユーザデータの保護管理のためシステムに組込む機能は、以下を満足していなければならない。

- 使用する技術(製品や方式)は、対象とするユーザデータについて指定されている格納やアクセス管理やアクセス監視についての要件を満足するものでなければならない。
- 一般に機器やソフトウェアにはさまざまな機能が準備されており、同じ技術でもその使い方次第で機能も異なってくる。使用する技術そのものは妥当であっても、その機能設定が、対応する保護管理要件に対して不適切であってはならない。

(2) 組込み場所の適切な設定

ユーザデータの保護管理ツールとして選択した技術を期待通りに機能させるためには、選択した技術のシステム構成上での配置は適切なものでなければならない。使用する技術のシステム構成上での組込み場所は、以下により決められる。

- ユーザデータの保護にかかる当該技術の役割および適用範囲
- 当該技術の機能特性および前提とする環境条件

(3) 選択した機能の適切な組込み

選択した技術を期待通りに機能させるためには、技術のシステムへのインストールが適切に行われていなければならない。このためには、以下のことが求められる。

- 選択機能の的確な組込み
- テストによる動作確認の実行

システムへのインストールが終了したら、十分な機能検査を必ず実施し、インストールに不備がないことを確認すること。

(4) 必要な運用環境の整備

システムの構成管理やシステムの運用において、OS やネットワーク環境の整備、アクセス権限テーブルの整備や、ファイルの暗号化を行った時の暗号鍵の整備等、適用した技術が前提としている環境の整備に不備がないようにしなければならない。

これには、システムの導入時だけでなく、定期的な更新といったその維持管理についての処理も必要となる。

(5) 使用技術の実装についてのドキュメントの整備

使用技術の実装については、いつでもその設定仕様や実装の状況の確認ができるようドキュメント化されていなければならない。

また、このドキュメントは、機能の新規導入時に作成するだけでなく、実装についての変更が行われたときも、適切にメンテナンスされたものになってるようになっていなければならない。

【対策実施上のポイント】

(1) 採用した技術における、機能の選択にあたっては、十分な検討を行うこと。使用する技術のデフォルト機能を安易に用いないこと。

(2) 独自仕様の技術を用いる場合、当該機能またはシステムの設計と実装に対し、ISO15408 に準拠した、機能の評価および実装の評価を行うことも望ましい。

(3) 使用技術の実装状況に関するドキュメントに記載すべき事項としては、以下のようなものがある。

- システム構成上の組込み場所
- 設定機能等の各種の指定内容
- 運用上の留意点
- 実装確認テストの内容と結果
- 新規組込みまたはメンテナンス日時

(10) ユーザデータの漏洩、改ざん、破壊事故に備える

【主旨】

ユーザデータの保護管理に努めていても、運用上の不備や新しい攻撃手段の登場等で、ユーザデータが改ざん、破壊を受ける可能性も考えておかなければならない。このような場合において被害の拡大を防ぎ、業務やシステムの運用の混乱を極小化するためには、事故に対する処置が適切かつ迅速でなければならない。

事故時の対処が適切かつ迅速に行われるようにするためには、ユーザデータにかかわるセキュリティ事故が発生した時の対処要領を確立しておくとともに、常日頃から、事故処理に必要となる情報やツールの整備を行っておくことが求められる。

【具体的な実施事項】

(1) ユーザデータに関するセキュリティ事故に対する対処要領の確立

ユーザデータの漏洩、改ざん、破壊等ユーザデータに関するセキュリティ事故の発生に際して、必要な処置を適切に行わなければ、被害を拡大することになる。このため、このような場合における対処要領を確立しておくことが必要である。

ユーザデータに関するセキュリティ事故に対する対処要領として明確にしておくべき事項としては、以下があげられる。

- 対策チームの編成
- サービスの停止の検討と実施
- 関係者へのユーザデータの改ざん、破壊事故発生告知
- 改ざん、破壊の内容,範囲等その状況の把握
- 改ざん、破壊されたソフト資産、情報資産の復旧
- 二次被害の調査と対策の検討、実施
- 原因の分析と再発防止策の検討とその実施
- 処理経緯の記録と保管

(2) ユーザデータに関するセキュリティ事故の処理に必要な情報の整備

ユーザデータに関する運用処理の記録等、ユーザデータに関するセキュリティ事故の処理に必要な情報は、適切に記録、保管されていなければならない。

(3) ユーザデータに関するセキュリティ事故による被害に備えたユーザデータの保全

個々のユーザデータに対する保護管理要件の定めるところに従い、バックアップの取得とその管理を行う。

(4) ユーザデータに関するセキュリティ事故を想定した事故処理訓練の実施

バックアップデータが保管されていても、復旧のための機能の実装の不備や、運用環境の変化や、慣れないことからくる操作の不手際等から、必要な時に復旧がうまくできないといった事態

が起こりうる。

このため、ユーザデータに関するセキュリティ事故を想定した、事故処理訓練を定期的に行うことが望ましい。

また、運用訓練で発見された、ユーザデータの改ざん、破壊事故発生に備えたユーザ情報の保全に関する処置や、システムの機能、対応運用規定、運用マニュアルに不備については、遅滞なく改善を行わなければならない。

(5) 必要なツールの整備

ユーザデータにかかわるセキュリティ事故に備えたバックアップの取得に用いるツールや、事故発生時における被害範囲の調査や、破壊されたシステムや情報の復旧等の事故処理に用いるツールは、期待通り機能しなければならない。

このためには、

- 適切なツールの選択とその適切なシステムへの組込み
- 運用環境の変更への対応
- ツール使用上のマニュアルの整備

等に不備がないようにしておかなければならない。

【対策実施上のポイント】

(1) ユーザデータにかかわるセキュリティ事故発生時の調査や復旧処理に必要な情報

ユーザデータの漏洩、改ざん、破壊事故発生時における被害範囲の調査や復旧処理に必要な情報としては、以下のようなものがあげられる。

- システム構成を示す情報
- システムにおけるユーザ情報の保有状況を示す情報
- システムにおけるユーザ情報の処理に関する運用を示す情報
- システムにおけるユーザ情報の更新履歴を示す情報
- ショップ業務におけるユーザ情報の使用状況

（11）ユーザデータの保護管理にかかる施策をシステム運用に反映させる

【主旨】

ユーザデータの保護管理にかかる諸施策が有効に機能するためには、対象情報についてのシステムへの格納、アクセス制限、アクセス監視、データの保全等において、ユーザデータの保護管理策がシステム運用に求めていることが、実際のシステム運用において、適切に実行されなければならない。

このことを確実にするためには、ユーザデータの保護管理策がシステムの運用に委ねていることが、日々のシステム運用において的確に実施されるようにする管理上の仕組みを工夫し、これらを日常の運用に組込んでおくことが必要となる。

【具体的な実施事項】

(1) ユーザデータの保護管理にかかる施策の運用規定、運用マニュアルへの反映

ユーザデータの保護管理にかかる諸施策が運用に求めていることは、すべてシステムの運用規定や運用マニュアルに適切に反映されていなければならない。

(2) 運用環境の変更への適切な対応の実施

運用環境に以下に示すような変更が行われた場合は、ユーザデータの保護管理策にかかるシステムの運用に変更の必要がないかどうかのチェックを行う。

- ユーザデータの保護管理ルール、格納方法、アクセス管理方法等、ユーザデータの保護管理にかかる具体的手段の変更
- 関係するシステム構成の変更
- システムの運用形態の変更
- ユーザデータの保護管理に用いている機能の変更

このチェックにより、システム運用に変更が必要となった場合は、以下の対応を適切に行わなければならない。

- 運用規定、運用マニュアルに対する必要な変更
- 必要な場合における運用スケジュールの変更等、システム運用の組立ての変更
- システム運用の変更の運用関係者への徹底

(3) ユーザデータの保護管理にかかる定期作業のスケジュール化

ユーザデータの保護管理の保護管理にかかる運用処理の実行を漏れないようするためには、システム運用上定期的に実施すべき作業は、予めスケジュール化しておくことが有効である。

ユーザデータの保護管理に関連して、定期的な作業としてスケジュール化しておくべき作業としては、以下があげられる。

- システムが保有しているユーザデータの保管状態の確認
- システムが保有しているユーザデータの改ざん、破壊の監視

- ユーザデータに対する不正アクセスの監視
- ユーザデータの定期メンテナンス
- ユーザデータに関する事故に備えた情報の保全処理
- 事故処理の訓練

(4) 関係運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行

ユーザデータの保護管理にかかる運用作業についてのチェックリストを作成し、運用実績を記入、報告し、個々の作業が的確に実行されたことの確認を常に行うようにすることも、運用上から必要な処理が漏れないようにするための工夫の一つである。

(5) ユーザデータの管理にかかる運用処理についての記録と保管

以下に示すようなユーザデータの保護管理にかかわる運用上の処理については、その記録を残し管理する。

- ユーザデータの登録、変更、削除、コピー等当該ファイルに対して行った操作
- ユーザデータの収容方法の変更
- ユーザデータに対するアクセス監視の分析とその結果に対する処理
- ユーザデータの保全処理
- ユーザデータの保護管理にかかるシステム運用の変更

【実施対策上のポイント】

(1) ユーザデータの保護管理策にかかる施策の運用規定や運用マニュアルへの反映手順の確立

ユーザデータの保護管理策にかかる諸施策の運用規定や運用マニュアルへの反映を確実にするためには、これらの施策の運用規定や運用マニュアルへの反映手順を確立しておくことも必要となる。

これらの手順については、11.2 節の**"(4)セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに適切に反映する"**の項参照。

(2) ユーザデータの保護管理に関する運用処理に関するチェックリストについて

日々の運用におけるユーザデータの保護管理にかかる運用処理を、確実なものにするための実行チェックリストにあげるべき処理としては、以下のようなものがあげられる。

- システムが保有しているユーザデータの保管状態の確認
- システムが保有しているユーザデータの改ざん、破壊監視
- ユーザデータに対する不正アクセス監視
- ユーザデータに関する事故に備えた保全処理
- 事故処理の訓練

(12) 関係者に対しユーザデータの保護管理についての教育を行う

【主旨】

ユーザデータの保護管理についての諸施策が適切に定められていても、それらが機能するためには、システムの管理や運用に携わる担当者に、ユーザデータの保護管理についての知識と対応施策についての十分な理解を必要とする。

このため、ユーザデータの保護管理を直接かかわる者だけでなく、システムの構築や運用に携わる者や、業務上ユーザ情報に触れる者のすべてに対し、以下に示すようなユーザデータの保護管理についての教育を適切に実施することが必要となる。

【具体的な実施事項】

(1) 関係者に対するユーザデータの保護管理についての教育の実施

① ユーザデータの保護管理についての定期的な教育の実施

ユーザデータの保護管理に関する教育は、定期的に行われなければならない。

② 必要に応じたユーザデータの保護管理についての臨時教育の実施

以下のような場合は、その都度、該当者に対する教育を実施することが必要となる。

- 異動等によりユーザデータの取扱い関係者の入替えが合った場合
- ユーザデータの保護管理にかかる諸施策やその運用が変更された時
- ユーザデータの保護管理にかかる技術とその運用
- ユーザデータの保護管理に問題が生じた場合

(2) ユーザデータの保護管理についての教育カリキュラムの確立

ユーザデータの保護管理についての教育を効果的に行うためには、教育科目とその内容、対象者と受講サイクル、実施時期等を定めた教育カリキュラムを確立しておくことが望ましい。

教育すべき内容としては、以下があげられる。

- ユーザデータの保護管理の概要
- ユーザデータの保護管理策の詳細とその実施要領
- ユーザデータの保護管理に用いる技術とその運用
- ユーザデータの保護管理に関する事故事例

また教育内容は、サイトの運営形態やシステム構成、運用形態、さらには技術環境の進化を反映した、運用対象システムの実態に合ったものであるよう、適時、見直しを行うべきである。

(3) ユーザデータの保護管理に関する教育テキストの整備

ユーザデータの保護管理に関する教育をより効果的にするためには、サイトの運営環境に合ったテキストを準備することが望ましい。

また、このテキストについても、サイトの運営形態の変更を反映するよう定期的な見直しを行うことが望ましい。

【対策実施上のポイント】

(1) ユーザデータの保護管理についての教育カリキュラム例

表 7-10 に、ユーザデータの保護管理についての教育カリキュラムの一例を示す。

表 7-10 ユーザデータの保護管理についての教育カリキュラム例

項番	教育項目	教育対象者	頻度
1	ユーザデータの保護管理の概要 ・ユーザデータの保護管理義務について ・ユーザデータの保護管理についての取組み	・ユーザデータの保護関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者 ・業務上でのユーザデータ取扱い責任者	1回／年
2	ユーザデータの保護管理策の詳細とその実施要領 ・ユーザデータの保護管理基準 ・保護管理基準の個々のユーザデータに対する適用状況 ・運用規定、運用マニュアル上の関係事項 ・その他注意事項	・ユーザデータの保護関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者 ・業務上でのユーザデータ取扱い責任者	1回／年
3	ユーザデータの保護管理に用いる技術とその運用 ・サイトにおけるユーザデータの保有状況 ・対象情報の保護技術 ・対象情報へのアクセス監視技術	・ユーザデータの保護関係者 ・システム開発関係者 ・システム管理関係者	1回／年
4	ユーザデータの保護管理に関する事故事例	・ユーザデータの保護関係者 ・システム開発関係者 ・システム管理関係者 ・システム運用関係者 ・業務上でのユーザデータ取扱い責任者	1回／年

(13) ユーザデータの保護管理の実施状況についての監査を行う

【主旨】

ユーザデータの漏洩、改ざん、破壊は、プライバシーの侵害や他社の業務に混乱を招く恐れがあるため、ユーザデータの保護管理の不備が問題をおこす前に、問題点を発見し適切な改善策を講じることができるようにしておくことも重要である。

このため、定められているユーザデータの保護管理策がサイト運営の実態に照らして適切かどうか、また、ユーザデータの保護管理策として定められていることが適切に実施されているかどうか等についてのチェックを行い、問題点の摘出と必要な改善の指導を行う、ユーザデータの保護管理の実施状況についての監査を行うことも必要である。

また日常の運用の中で、実施したユーザデータの保護管理にかかわる運用についての記録の保管等、この監査のための準備を組込んでおくことも必要となる。

(注) 正式な監査という形はとらなくとも、ここに示すようなユーザデータの保護管理の実施状況についてのチェックは、組織的に行われるべきものである。

【具体的な実施事項】

(1) ユーザデータの保護管理の実施状況についての定期的な監査の実施

最低でも年1回は、以下に示すような事項をチェックする、ユーザデータの保護管理の実施状況についての監査を行う。

- ユーザデータの保護管理についての責任体制の整備状況とその機能状況
- ユーザデータ保護管理基準の妥当性
- 保護管理対象ユーザデータの個々に指定している保護管理要件の妥当性
- 個々の保護対象ユーザデータに対する保護管理の実施状況
- ユーザデータの保護管理に使用している機能の実装状況
- ユーザデータの漏洩、改ざん、破壊事故への備えの状況
- ユーザデータの保護管理にかかる施策のシステム運用への反映状況
- 業務運営上におけるユーザ情報にかかわる印刷物や電磁媒体の取扱い状況
- 業務委託先に対するユーザ情報の取扱いについての指導、管理の実施状況
- 関係者におけるユーザデータの保護管理についての認識

(2) 監査実施要領の確立

ユーザデータの保護管理についての定期的な監査が、円滑に実施され実効的なものになるようにするためには、この監査についての実施要領が確立されていることが望ましい。

この監査実施要領で規定しておく事項については、1.2.2 節の(4)項を参照。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。

このためには、監査指摘事項に対する改善措置が実際にとられたかどうかについてのチェックを行うことも必要であり、監査要領の中に、指摘事項についてのフォローの仕組みも組込んでおくことも有効である。

【対策実施上のポイント】

(1) 監査内容例

表 7-11 に、ユーザデータの保護管理の実施状況についての監査において、監査すべき事項の例を示す。

(2) 監査結果は、ユーザデータの保護管理責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告しなければならない。

表 7-11 ユーザデータの保護管理の実施状況に関する監査内容例

項番	監査項目	監査の内容等
1	ユーザデータの保護管理についての責任体制の整備状況とその機能状況	・ユーザデータの保護管理についての責任体制は、サイトの運営実態に照らして適切か ・該当責任者における自己の責任についての認識は十分か ・ユーザデータの保護管理に関する責任体制は機能しているか
2	ユーザデータ保護管理基準の妥当性	・ユーザデータの保護管理基準は、サイトの運営に照らして適切か
3	保護対象ユーザデータ個々に指定している保護管理要件の妥当性	・保護対象とすべきユーザデータすべてに対して保護管理要件が定義されているか ・保護対象ユーザデータ個々に設定されている保護管理要件は、保護管理基準やシステムの運営実態に照らして適切か
4	個々の保護管理対象ユーザデータに対する保護管理の実施状況	・システムにおける保護対象ユーザデータの格納状況は、正確に把握されているか ・システム上での個々の保護対象ユーザデータの格納は、当該ユーザデータに指定されている保護管理要件を満足しているか ・システム上の個々のユーザデータに対するアクセス制限は、当該ユーザデータに対する保護管理要件に指定されていることを満足しているか ・システム上の個々のユーザデータに対するアクセス監視は、当該ユーザデータに対する保護管理要件に指定されていることを満足しているか ・システム上の保護管理対象ユーザデータファイルに対する再編正等の運用上の操作は記録されているか

表 7-11 ユーザデータの保護管理の実施状況に関する監査内容例

項番	監査項目	監査の内容等
5	ユーザデータの保護管理に使用している機能の実装状況	・ユーザデータの保護管理に使用する技術およびその機能選択は妥当か ・その実装の正確性は確認されているか （実装すべき場所に正確に実装されているか） ・運用環境の変更時における対応機能の実装の見直しは行われているか ・必要な運用環境の整備状況についてのチェックは適切に行われているか
6	ユーザデータの漏洩、改ざん、破壊事故への備えの状況	・ユーザデータにかかるセキュリティ事故に対する対処要領は適切に決められているか ・監査期間における事故対策は妥当であったか
7	ユーザデータの保護管理にかかる施策のシステム運用への反映状況	・ユーザデータの保護管理にかかる諸施策がシステム運用に求めていることは、運用規定、運用マニュアルに適切に反映されているか ・これらの運用は、日々の運用において確実に実行されているか、またそのことが管理されているか ・ユーザデータの保護管理にかかる諸施策に関係するシステム運用の適切な実行の実現のための工夫は十分か
8	業務運営上におけるユーザ情報にかかわる印刷物や電磁媒体の取扱い状況	・ユーザ情報にかかわる印刷物や電磁媒体の取扱い規定の確立状況 ・日常の業務運営上におけるこれらの取扱い状況 ・日常の業務運営におけるこれらの取扱いについての指導、管理の実施状況
9	業務委託先に対するユーザ情報の取扱いについての指導、管理の実施状況	・業務委託先に対するユーザ情報の取扱いについての適切な取決めの締結状況 ・業務委託先に対するユーザ情報の保護管理に対する指導状況 ・業務委託先におけるユーザ情報の取扱いの妥当性 ・業務委託先に業務運営上でのユーザ情報の取扱いについての管理状況
10	関係者におけるユーザデータの保護管理にかかる認識	・ユーザデータの保護管理の必要性についての認識は十分か ・ユーザデータの保護管理に用いている技術についての理解は十分か ・設定している保護管理基準についての理解は十分か ・ユーザデータの保護管理策とその運用についての理解は十分か

8 通信にかかるリスク対策の適切な実施―秘密通信の適用等

8.1 必要な施策

図 8-1 に通信にかかるリスク対策の組立てを示す。

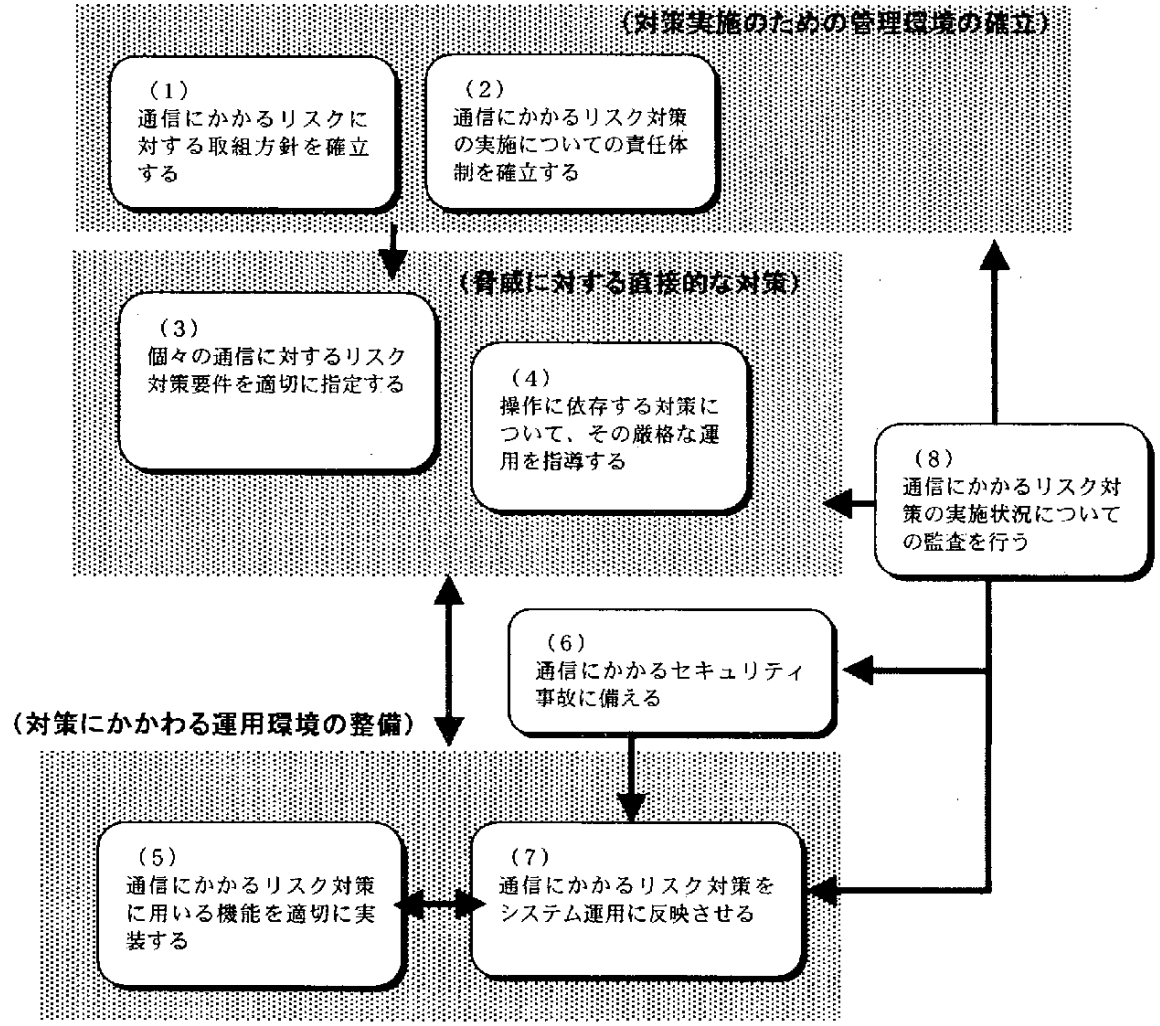


図 8-1 通信にかかるリスク対策の組立て

また、表 8-1 に各施策における実施事項の一覧を示す。

表 8-1　通信にかかるリスク対策としての具体的実施事項一覧

施策名	具体的実施事項
(1) 通信にかかるリスクに対する取組方針を確立する	① 通信にかかるリスク対策の目標の明確化 ② 適用範囲の明確化 ③ 通信にかかるリスク対策実施基準の確立 ④ 通信にかかるリスク対策の組立ての明確化 ⑤ 取組方針の関係者への周知
(2) 通信にかかるリスク対策の実施についての責任体制を確立する	① 通信にかかるリスク対策実施についての責任体制の明確化 ② 通信にかかるリスク対策関係者間の連携体制の確立
(3) 個々の通信に対するリスク対策要件を適切に指定する	① 個々の通信に対するリスク対策要件の指定 ② 個々の通信に設定したリスク対策要件についてのドキュメントの整備
(4) 操作に依存する対策について、その厳格な運用を指導する	① 消費者も含む関係者への必要な操作の要求 ② 適用状況の監視と改善の指導
(5) 通信にかかるリスク対策に用いる機能を適切に実装する	① 適切な技術と使用する機能の選択 ② 組込み場所の適切な設定 ③ 選択した技術、機能の適切なインストール ④ 必要な運用環境の整備 ⑤ 使用技術の実装についてのドキュメントの整備
(6) 通信にかかるセキュリティ事故に備える	① 通信にかかるセキュリティ事故に対する対処要領の確立 ② 通信にかかるセキュリティ事故の対処に必要となる情報の整備 ③ 通信ログの保全 ④ 通信にかかるセキュリティ事故を想定した事故処理訓練の実施 ⑤ 必要なツールの整備
(7) 通信にかかるリスク対策をシステム運用に反映させる	① 通信にかかるリスク対策の運用規定、運用マニュアルへの反映 ② 運用環境の変更への適切な対応 ③ 通信にかかるリスク対策に関する定期作業のスケジュール化 ④ 関係する運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行 ⑤ 通信にかかるリスク対策に関係する運用処理についての記録と保管
(8) 通信にかかるリスク対策の実施状況についての監査を行う	① 通信にかかるリスク対策の実施状況についての定期的な監査の実施 ② 監査実施要領の整備 ③ 監査指摘事項に対するフォローの実施

8.2 個別具体策

(1) 通信にかかるリスクに対する取組方針を確立する

【主旨】

通信路上での情報の漏洩、改ざん、破壊、通信相手による事後否認等の通信にかかるセキュリティ事故の防止を図るとともに、事故が生じた時の被害を限定的なものにすることに組織的に取組むには、通信にかかるリスクへの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示す通信にかかるリスクに対する取組方針を確立し、これを、その対策に直接かかわる者だけでなく、システムの構築や運用に関係する者、さらにはユーザも含むサイトとの通信にかかわる者のすべてに、周知させておくことが必要となる。

【具体的な実施事項】

(1) 通信にかかるリスク対策の目標の明確化

通信にかかるリスク対策が目標とするところを明確にし、関係する施策の意図を明確にする。通信にかかるリスク対策の目標としては、以下があげられる。

- 通信路上での情報の漏洩の防止
- 通信路上での情報の改ざん、破壊からの防御
- 通信にかかるセキュリティ事故発生時の被害の極小化

(2) 適用範囲を明確化

通信にかかるリスク対策の適用範囲として、以下を明確にする。

- 対象となる通信
- 対象とする組織
- 対象とする業務、作業

(3) 通信にかかるリスク対策実施基準の確立

通信にかかるリスク対策は、通信情報の漏洩や破壊等の事故が発生した場合の影響の大きさにより異なる。このため、全ての通信に同じようなリスク対策を適用することは、運用上現実的でない。

実際に実施する通信にかかるリスク対策は、個々の通信ごとに決めなければならないが、それらはサイト全体として統制のとれたものでなければならない。このことを実現するためには、実施するリスク対策に、その厳格さによるレベル分けを行い、それぞれのレベルに対する標準的な対策要件を定義した通信にかかるリスク対策実施基準を確立しておき、保護対象通信ごとに適用する対策レベルを割当て、そのレベルに指定された標準的な対策要件に基づいた対策を実施するような工夫も必要となる。

通信にかかるリスク対策実施基準として定義すべき事項をあげると、以下のようになる。

- 対策レベルの名称
- 当該対策レベルの適用範囲
- 通信路についての要件
- 相手確認についての要件
- 暗号化についての要件
- ログの取得およびその保管に関する要件

対策要件は、当該クラスが対象としている通信の保護の重要度クラスに依存する。

(4) 通信にかかるリスク対策の組立ての明確化

通信にかかるリスク対策をどのように行うかについて明らかにするもので、実施する施策と施策間の関係を示す。

本ガイドラインにおける通信にかかるリスク対策としての施策の組立てについては、8.1 節参照。

(5) 通信にかかるリスクに対する取組方針の関係者への周知

通信にかかるリスクについての取組方針は文書化されるとともに、通信にかかるリスク対策に直接かかわる者だけでなく、システムの構築ならびに運用関係者、さらには業務上で通信にかかわる者のすべてに周知させておかねければならない。このためには、

- 通信にかかるリスクに対する取組方針の掲示や配布
- 関係者間での通信路上のリスクに対する取組方針の定期的な再確認

が必要となる。

【対策実施上のポイント】

(1) 通信にかかるリスク対策実施基準の策定にあたってのポイント

通信にかかるリスク対策実施基準は、対策の厳格さのレベル分けと、各対策レベルに求められる対策要件の定義からなり、これらは、以下のような視点から決められる。

- 問題が生じた場合の影響の大きさ
- 対象とする脅威の発生頻度
- 使用するネットワークや通信方式といった通信の形態

また、対策のレベル分けは、システムの対象業務やその運用形態等、そのシステムの特性に合わせて決めればよく、必要以上の細分化は不要である。

(2) 通信かかるリスク対策実施基準の定義について

通信にかかるリスク対策実施基準の定義で、規定すべき事項をあげると、表 8-2 のようになる。

表 8-2　通信にかかるリスク対策実施基準の定義内容

項番	定義項目	内容
1	対策レベルの名称	・当該対策レベルの ID、名称
2	当該対策レベル適用範囲	・当該対策レベルの適用対象となる通信の重要度クラス
3	通信路についての要件	・通信路の選定についての要件（当該対策レベルの要求に対応する通信路の要件と、採用が可能な通信路の例示） （例）－完全な隔離されたクローズトな通信路の使用 －VPN等擬似的なクローズトな通信路の使用 －インターネットを使用 －その他のオープンな通信路を使用
4	相手確認についての要件	・当該通信において必要とする相手認証のレベルと、採用が可能な認証方式の例示 （例）－電子認証等、法的に有効な認証の使用 －ローカルな電子認証を使用 －ワンタイムパスワード等信頼性の高いパスワード使用 －一般的なパスワード使用 －認証不要
5	暗号化についての要件	・暗号化の要否と、求める暗号化のレベルと、採用が可能な暗号ツールの例示 （例）－システム固有の暗号化の適用を要求 －アプリケーションがサポートしている暗号化を適用 －暗号化不要
6	真正性確認についての要件	・情報が改ざんされていないことの確認の要否と、求める真正性確認方式についての要件 （例）－システム固有の方法による真正性の確認を要求 －電子署名等普及ソフトによる真正性の確認を要求
7	ログの取得および保管要件	・取得対象 （例）－通信レベルのログの完全取得 －特定な通信イベントについての通信ログの取得 ・ログの取得方法 （例）－二重化等の特別な保全処置を要求 －二重化等の特別な保全処置は不要 ・取得ログの保管要件 （例）－別途に指定する期間の保管 －ログの容量の範囲での保管

(3) 通信にかかるリスク対策実施基準の定義例

表 8-3 に、通信にかかるリスク対策実施基準の定義例を示す。

表 8-3 通信にかかるリスク対策実施基準の定義例

項番	対策実施レベル	当該レベルにおける対策要件等
1	レベルA	・適用対象通信・・・・・・・・・・・・・・・当該対策レベルの適用対象となる通信の重要度クラス（表 8-4 参照） ・通信路についての要件・・・・・・・・完全に隔離された通信路を使用 ・相手確認についての要件・・・・・・端末と使用者の確認 ・暗号化についての要件・・・・・・・・業務固有の暗号化を適用 ・真正性の確認についての要件・・電子署名レベルの確認が必要 ・ログの取得、保管に関する要件・・通信レベルのログの完全取得 保管期間は2年以上
2	レベルB	・適用対象通信・・・・・・・・・・・・・・・当該対策レベルの適用対象となる通信の重要度クラス（表 8-4 参照） ・通信路についての要件・・・・・・・・VPNを使用 ・相手確認についての要件・・・・・・端末と使用者の確認 ・暗号化についての要件・・・・・・・・業務固有の暗号化を適用 ・真正性の確認についての要件・・電子署名レベルの確認が必要 ・ログの取得、保管に関する要件・・通信レベルのログの完全取得 保管期間は1年以上
3	レベルC	・適用対象通信・・・・・・・・・・・・・・・当該対策レベルの適用対象となる通信の重要度クラス（表 8-4 参照） ・通信路についての要件・・・・・・・・インターネットを使用 ・相手確認についての要件・・・・・・公的な電子認証を適用 ・暗号化についての要件・・・・・・・・電子認証に含まれる暗号化使用 ・真正性の確認についての要件・・電子署名による確認の適用 ・ログの取得、保管に関する要件・・通信レベルのログの完全取得 保管期間は 6 ヶ月以上
4	レベルD	・適用対象通信・・・・・・・・・・・・・・・当該対策レベルの適用対象となる通信の重要度クラス（表 8-4 参照） ・通信路についての要件・・・・・・・・インターネットを使用 ・相手確認についての要件・・・・・・一般的なパスワードを使用 ・暗号化についての要件・・・・・・・・アプリケーションソフトに組込まれた暗号化の使用 ・真正性の確認についての要件・・不要 ・ログの取得、保管に関する要件・・アプリケーションレベルのログの保管 保管期間は 3 年以上
5	レベルE	・適用対象通信・・・・・・・・・・・・・・・当該対策レベルの適用対象となる通信の重要度クラス（表 8-4 参照） ・通信路についての要件・・・・・・・・インターネットを使用 ・相手確認についての要件・・・・・・不要 ・暗号化についての要件・・・・・・・・アプリケーションソフトに組込まれた暗号化の使用 ・真正性の確認についての要件・・不要 ・ログの取得、保管に関する要件・・アプリケーションレベルのログの保管 保管期間は2週間以上

(4) 通信の重要度についての考え方と重要度クラスの設定

通信の重要度とは、漏洩や改ざん、破壊等の事故が発生した場合における影響の大きさの尺度を示すもので、当該通信に求められるリスク対策の厳格さを決める時の判断材料となるものである。

この重要度についてクラス化を行い、対象通信に対する対策レベルの割当てを、対象通信に指定された重要度クラスによるようにすることも、通信にかかるリスク対策をサイト全体として統制のあるものにするためには有効である。

表 8-4 に、通信の重要度クラスの定義例を示す。

表 8-4 通信の重要度クラスの定義例

項番	重要度クラス	通信の重要度	備考 (対象となる通信例)
1	クラスA	その漏洩、改ざんは、ユーザに直接的な損害を与える可能性のあり、かつ、その損害も大きなものになる可能性のあるもの	・パスワードの登録データ等のセキュリティ管理情報に属する情報を含む通信 ・ユーザの商業秘密情報を含む通信
2	クラスB	その漏洩、改ざんは、ユーザに直接的な損害を与える可能性はあるが、その損害の規模は限定的なもの	・クラス A 相当の情報であるが利用が制限され、問題が生じても被害も被害の範囲が限定されるような情報を含む通信
3	クラスC	その漏洩、改ざんは、ユーザに直接的な損害は与えないにしても、ユーザとの間でトラブルになる恐れのあるもの	・プライバシー情報を含む通信
4	クラスD	その漏洩、改ざん、破壊は、業務に一時的なトラブルを生じるもの	・公開されている情報であっても取引条件に関する情報等、取引の実行に影響を与える通信
5	クラスE	その漏洩、改ざん、破壊は、ユーザに直接的な損害を与えたり、業務に影響を与えたりはしないものの、サイトやショップの信頼を傷つける恐れのあるもの	・取引に関係しない公開情報だけを扱う通信

(5) 通信にかかるリスク対策についての信頼性について

通信にかかるリスク対策として採用する方式については、その方式の信頼性についての認識も必要となる。

通信にかかるリスク対策の信頼性についての考え方の一例を、下記に示す。

- 環境整備に遺漏がなければ 100%信頼してよいもの
- 個々の場面毎に対策の組込みが必要で、対策漏れの可能性を持つもの

- 個々の場面毎に特別な操作が必要で、その漏れない運用は期待しがたいもの

(6) 通信にかかるリスクへの取組方針は、システム構成やその運用形態等、システム運用の実環境の変化に対応して必要な修正が加えられるべきであり、必要に応じて見直しを行うこと。

(7) 通信にかかるリスクへの取組方針は、定期的に関係者間で再確認することをルーチン化しておくことが望ましい。

(2) 通信にかかるリスク対策の実施についての責任体制を確立する

【主旨】

通信にかかるリスク対策をその取組方針に沿って機能させるためには、通信にかかるリスク対策として定められていることが、システムの構築や運用に適切に反映されるよう、指導、管理する責任体制の確立が必要となる。

このためには、通信にかかるリスク対策にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) 通信にかかるリスク対策実施についての責任体制の明確化

通信にかかるリスク対策の実施についての責任体制に関し、明確にしておくべきこととしては以下があげられる。

- 通信にかかるリスク対策責任者とその責任
- 通信にかかるリスク対策実施担当者の責任
- 業務現場における通信にかかるリスク対策実施推進者の責任
- システム開発者の通信にかかるリスク対策に関する責任
- システム管理者の通信にかかるリスク対策に関する責任
- システム運用者の通信にかかるリスク対策に関する責任

(2) 通信にかかるリスク対策関係者間での連携体制の確立

通信にかかるリスク対策に関する責任体制が有効に機能するためには、関係者間の連携が重要となる。

【対策実施上のポイント】

(1) 通信にかかるリスク対策関係者の責任分担

表 8-5 に、通信にかかるリスク対策関係者の責任分担の定義例を示す。

(2) 通信にかかるリスク対策についての責任体制は、通信にかかるリスク対策が変更されたり、サイトの運営形態に変更が生じた場合は、見直しを行い、必要な変更を行うこと。

表 8-5　通信にかかるリスク対策関係者の責任分担

責任区分	タスク
通信にかかるリスク対策責任者	・通信にかかるリスク対策についての取組方針の確立と関係者への周知 ・通信にかかるリスク対策実施基準の承認と発行 ・通信にかかるリスク対策全体の妥当性の維持 ・通信にかかるリスク対策の実施状況の把握 ・対策基準に従った通信にかかるリスク対策の実施についての指導 ・通信にかかるセキュリティ事故発生時における事故処理の指揮
通信にかかるリスク対策の実施担当者	・通信にかかるリスク対策基準の検討および見直し ・通信にかかるリスク対策の実施状況の把握 ・対策基準に従った通信にかかるリスク対策の監督、管理 ・通信にかかるセキュリティ事故発生時における事故処理と再発防止策の検討
業務現場における通信にかかるリスク対策実施推進責任者	・業務現場における通信にかかるリスク対策についての妥当性のチェックと改善の提案 ・業務現場における通信にかかるリスク対策の実施状況の把握 ・業務現場における、対策基準に従った通信にかかるリスク対策の監督、管理 ・通信にかかるリスク対策でユーザに依存する事項についての啓蒙と指導およびその実行監視と指導 ・通信にかかるセキュリティ事故に対する現場サイドの対処
システム開発者	・開発システムにおける通信にかかるリスク対策要件の的確なインストール －設計の妥当性の確認 －漏れの的確な実装の確認
システム管理者	・システムにおける通信にかかるリスク対策対応機能の維持管理 －システム構成変更の反映の管理 －通信にかかるリスク対策対応機能の維持管理 ・システムにおける対応機能の実装状況の正確な把握
システム運用者	・システム運用における通信にかかるリスク対策対応機能の動作環境の整備 ・通信にかかるリスク対策にかかるシステム運用のチェックと指導

(3) 個々の通信に対するリスク対策要件を適切に指定する

【主旨】

求められる通信にかかるリスク対策が機能するようにするには、対策が必要な個々の通信に対して、適用する対策レベル、適用する方式とその実装、および当該機能の使用にからむ運用上の要件等が、通信にかかるリスクに対する取組方針の中で定められている対策実施基準に従い適切に設定されていなければならない。

対策手段が厳格になればなるほど、運用面での負担が大きくなるのが一般である。対策手段の選択にあたっては、目的を損なわないようにしながら、運用面での負担とのバランスがとれるようにしなければならない。

また、どの通信にどのような対策が、どのように適用されているかが、常に正確に把握されていなければならない。

【具体的な実施事項】

(1) 個々の通信に対するリスク対策要件の指定

通信にかかるリスク対策実施基準に従い、保護対象通信の洗出しを行い、その個々に対し、その通信の特性から、対策の要否と、対策が必要な場合適用する対策要件を設定する。

通信ににかかるリスク対策要件として、指定すべき事項をあげるとし、以下のようになる。

- 当該通信の重要度クラス
- 当該通信に対するリスク対策要件
- 適用する技術
- 適用上の留意事項

(2) 個々の通信に設定したリスク対策要件についてのドキュメントの整備

個々の通信に対するリスク対策が適切に行われているかどうかについての管理ができるように、当該サイトにおける外部との通信のすべてに対し、適用しているリスク対策を一覧できるドキュメントを整備しておくことも必要である。

このドキュメントには、対策の対象としない通信についても記載の対象とし、対策不要の旨を含む記述をしておくことが望ましい。

【対策実施上のポイント】

(1) 個々の通信に対するリスク対策要件の定義要領

表 8-6 に、個々の通信に対するリスク対策の定義にあたっての定義すべき事項を示す。

表 8-6 個々の通信に対するリスク対策要件定義における定義事項

項番	定義事項	定義内容
1	当該通信の 重要度クラス	・当該通信に適用する重要度クラス －当該通信に求められる保護要件は、この重要度クラスによって決められる。
2	当該通信に対する リスク対策要件	・当該通信に対し、リスク対策として求められることとして、下記項目についての要件を明確にする －ユーザ認証のレベル －暗号化の要否とそのレベル －真正性確認の要否 －法的証拠性確保の要否 －通信ログ保管の要否とそのレベル
3	適用する技術	・当該通信に対して、リスク対策要件を満足するために適用する技術の指定として、下記事項を明確にする －適用技術 －適用技術の使用条件(機能設定条件他)
4	適用上の留意事項	・対応機能の実装上の留意事項 ・当該方式の適用にあたっての運用管理上の留意事項

(2) リスク対策実施対象通信の洗出しについて

通信にかかるリスク対策においては、保護対象通信の洗出しに漏れがあってはならない。

以下に示す通信は、すべてリスク対策対象として検討の対象にならなければならない。

- 一般データ通信におけるデータ群のすべて
- Web を介して交換されるメッセージの全て
- 保護対象情報が含まれるメールの全て

(3) 個々の場面への適用方式の選択に当っては、リスク対策要件と、ユーザの使い勝手、コスト、運用環境の手間等のバランスを考慮しなければならない。

(4) 操作に依存する対策について、その厳格な運用を指導する

【主旨】

暗号化メールを用いるような場合、暗号化の実行は発信者の操作に依存する。通信にかかるリスク対策をこのような技術に依存している場合、その適用が漏れないようにする指導が必要となる。

このためには、消費者等のサイトとの通信相手に対し、操作要領を配布する、その運用に漏れがあったような場合の改善の指導を行う等の措置が必要となる。

【具体的な実施事項】

(1) 消費者も含む関係者への必要な操作の要求

消費者をはじめとする通信相手に対し、

- 通信の安全確保についての解説
- 通信時に必要な操作の励行の要求
- 操作要領

を説明した文書の配布を行い、その適用の徹底を図る努力をする。

(2) 適用状況の監視と改善の指導

暗号化等の求められる処置が、実際に行われているかどうかのチェックを行い、問題がある場合は、対象者に必要な指導を行う。

このためには、

- システムへの監視機能の組込み
- 業務運用上の監視の義務づけ

等について工夫が必要である。

(5) 通信にかかるリスク対策に用いる機能を適切に実装する

【主旨】

通信にかかるリスク対策技術としては、

- 他の通信と隔離する専用の通信路の使用
- オープンな通信路を用いる通信に対する暗号化通信等のセキュア通信の適用

等がある。

また、その実現方法としては、

- VPN、SSL、SET／SECE、暗号化メール等、使用する通信形態に対応した汎用技術の使用
- 独自仕様のよる実現

等があるが、いずれの場合においても、期待通りに機能し、その使用目的を満足するものでなければなければならない。

このためには、技術の選択と選択した技術における使用機能の選択、インストール時の設定等を適切に行うとともに、そのインストールに対する検査を十分に行うことが必要となる。

また、SSL 適用時における証明書の取得と管理、暗号鍵の管理等、使用する技術に必要な運用環境の整備にも不備がないようにしなければならない。

【具体的な実施事項】

適用する技術の個々に対し、以下のことが求められる。

(1) 適切な技術と使用する機能の選択

- 使用する技術(製品や方式)は、対象とする通信に対するリスク対策要件を満足するものでなければならない。
- 一般に機器やソフトウェアにはさまざまな機能が準備されており、同じ技術でもその使い方次第で機能も異なってくる。使用する技術そのものは妥当であっても、その機能設定が対象とする使用場面における要求に対して不適切であってはならない。

これらのことが、適切であるかどうかについては十分なチェックを必要とする。

(2) 組込み場所の適切な設定

通信にかかるリスク対策ツールとして選択した技術を期待通りに機能させるためには、選択した技術をシステム構成上の配置を適切なものにしなければならない。システム構成上での、使用する技術を組込む場所は、以下により決められる。

- 通信の保護にかかる当該技術の役割および適用範囲
- 当該技術の機能特性および前提とする環境条件

(3) 選択した技術、機能の適切なインストール

選択した技術を期待通りに機能させるためには、技術のシステムへのインストールが適切に行

われていなければならない。このためには、以下のことが求められる。

- 選択機能の的確なインストール
- テストによる動作確認の実行

システムへのインストールが終了したら、十分な機能検査を必ず実施し、インストールに不備がないことを確認すること。

(4) 必要な運用環境の整備

SSL の適用の場合は、認証局への登録と証明書の取得とそのシステムへの実装が必要となる。このように、適用した技術によっては、それが機能するために運用上で準備すべきことがある。また、システムの構成管理やシステムの運用において、OS やネットワーク環境の整備、アクセス権限テーブルの整備や、ファイルの暗号化を行った時の暗号鍵の整備等、適用した技術が前提としている環境の整備に不備がないようにしなければならない。

これには、システムの導入時だけでなく、定期的な更新といったその維持管理についての処理も必要となる。

(5) 使用技術の実装についてのドキュメントの整備

使用技術の実装については、いつでもその設定仕様や実装の状況の把握ができるようドキュメント化されていなければならない。

また、このドキュメントは、機能の新規導入時に作成するだけでなく、実装の変更が行われたときも、適切にメンテナンスされるようになっていなければならない。

【対策実施上のポイント】

(1) 採用した技術における機能の選択につては、よく検討すること。使用する技術のデフォルト機能を安易に用いないこと。

(2) 独自技術使用時の留意点

独自仕様の技術を用いる場合、当該機能または、当該機能を含むシステムまたはシステム機能の設計と実装に対し、ISO15408 に準拠した機能の評価および実装の評価を行うことが望ましい。

(3) 専用回線を使用するにあたっての留意点

専用回線を使っているからといって安心してはならない。サービスに対する通信回線の指定ミス等で、実際にはオープンな回線が使われているようなことがないよう、以下の点についての留意が必要となる。

- 指定の通信が、この専用線が使われていることの確認
- 指定以外の通信が、この専用線上で通信されていないことの確認
- 暗号化の要否の検討と必要な場合のその適切な組込み
  - アプリケーション等における通信回線の指定ミスの排除

(4) SSL 使用時の留意点

SSL を使用する場合、以下の点についての留意が必要となる。

- コンテンツへの SSL 機能の漏れない設定

  SSLの場合個々のコンテンツへのSSL機能の設定が必要であり、多くのコンテンツをからなるショップにおいては、その指定に漏れをおこしやすい。このため、指定が必要なコンテンツの漏れのない把握と、対象コンテンツへの SSL 機能の指定確認が確実に行われるようにする仕組みの確立も必要となる。
- 証明書の有効期限管理
- 秘密鍵の管理

(5) SET／SECE使用時の留意点

SET／SECEを用いる場合、以下の点についての十分な検討が必要となる。

- SET／SECE 適用アプリケーションの適切な設計と実装

  SET／SECEは、EC ショッピングにおけるクレジットおよび銀行決済を伴う処理における標準プロトコルであり、この標準プロトコルに対応するソフトウェア部品も製品として提供されている。これらの取引における通信路上でのリスク対策にこの技術を用いる場合、サイトは、この標準部品を組み込み、このプロトコルを前提と処理を実装しなければならない。この実装にあたっては、適切な設計と、適切な実装を必要とする。
- 証明書の有効期限管理
- 秘密鍵の管理
- ペイメントゲートウエイとの適切な連携
- クライアントユーザとの適切な連携

(6) 使用技術のドキュメンテーションについての留意点

使用技術の実装状況についてのドキュメントに記載すべき事項としては、以下のようなものがある。

- 当該技術がサポートする認証とそのレベル
- システム構成上の組込み場所
- 設定機能等の各種の指定内容
- 運用上の留意点
- 実装確認テストの内容と結果
- 新規組込みまたはメンテナンス日時

(6) 通信にかかるセキュリティ事故に備える

【主旨】

通信にかかるリスク対策に努力していても、新たな手法による盗聴等の攻撃により、通信路上で情報の漏洩や情報の改ざん等が行われる可能性も、常に考えておく必要がある。

通信路上でこのよう行為が行なわれたことが発見された場合における被害の拡大を防ぎ、業務やシステムの運用の混乱を極小化するためには、対象情報とその処理に関わる問題を対処するだけではなく、二次的な被害について調査し、必要な処置を適切かつ迅速に行わなければならない。

事故時における対処が適切かつ迅速に行われるようにするためには、通信にかかるセキュリティ事故が発生した時の対処要領を確立しておくとともに、常日頃から、事故処理に必要となる情報やツールの整備を行っておくことが求められる。

【具体的な実施事項】

(1) 通信にかかるセキュリティ事故に対する対処要領の確立

通信路上で情報の漏洩、改ざん、破壊等、通信にかかるセキュリティ事故が発生した場合、必要な処置を円滑に行えるようにするためには、事故時の対処要領を確立しておくことが必要である。

通信にかかるセキュリティ事故に対する対処要領として明確にしておくべき事項としては、以下があげられる。

- 対策チームの編成
- サービスの停止の検討と実施
- 関係者への情報の漏洩、改ざん、破壊事故発生の告知
- 漏洩、改ざん、破壊の内容、範囲等その状況の把握
- 攻撃を受けた処理に対する再実行等の必要な処理の実施
- 二次被害の調査と対策の検討、実施
- 原因の分析と再発防止策の検討とその実施
- 処理経緯の記録と保管

(2) 通信にかかるセキュリティ事故の対処に必要となる情報の整備

システムの構成情報や、システムが取扱っている通信に関する情報等、通信路上での情報の漏洩、改ざん、破壊事故の事故処理に必要な情報は、適切に記録、保管されていなければならない。

(3) 通信ログの保全

日々の運用の中で、個々の通信に対し指定されている通信にかかるリスク対策要件で指定されている通信ログの取得および保管を行う。

(4) 通信にかかるセキュリティ事故を想定した事故処理訓練を行う

バックアップデータが保管されていても、復旧のための機能の実装の不備や、運用環境の変化や、慣れないことからくる操作の不手際等から、必要な時に復旧がうまくできないといった事態が起こりうる。

このため、通信にかかるさまざまな事故を想定した事故処理訓練を、定期的に行うことが望ましい。

また、事故処理訓練で発見された、事故発生に備えた情報の保全に関する処置や、システムの機能、対応運用規定、運用マニュアルに不備については、遅滞なく改善を行わなければならない。

(5) 必要なツールの整備

通信にかかるセキュリティ事故に備えたバックアップの取得、通信にかかるセキュリティ事故発生時の被害範囲の調査、破壊されたシステムや情報の回復等の事故処理に用いるツールは、期待通り機能しなければならない。

このためには、

- 適切なツールの選択とその適切なシステムへのインストール
- 運用環境の変更への対応
- ツール使用上のマニュアルの整備

等に不備がないようにしておかなければならない。

【対策実施上のポイント】

(1) 通信にかかるセキュリティ事故の被害範囲の調査に必要な情報

通信路上での情報の漏洩、改ざん、破壊等、通信にかかるセキュリティ事故発生時における被害範囲の調査に必要な情報としては、以下のようなものがあげられる。

- システムにおける当該データの取扱いを示す情報
- 業務における当該データの取扱いを示す情報
- システムにおける当該通信に適用している保護手段とその実装状況に関する情報
- 当該処理における処理経緯を記録した情報

これらは、いずれも運用規定に従い記録、保管されていなければならない。

(7) 通信にかかるリスク対策をシステム運用に反映させる

【趣旨】

通信にかかるリスク対策にかかる諸施策が有効に機能するためには、これらがシステム運用に求めていることが、実際のシステム運用において適切に実行されなければならない。

このことを確実なものにするためには、これらが、日々のシステム運用において的確に実施されるようにする管理上の仕組みを工夫し、日常の運用に組込んでおくことが必要となる。

【具体的な実施事項】

(1) 通信にかかるリスク対策の運用規定、運用マニュアルへの反映

通信にかかるリスク対策にかかる諸施策が運用に求めていることは、すべてシステムの運用規定や運用マニュアルに適切に反映されていなければならない。

(2) 運用環境の変更への適切な対応

運用環境に以下に示すような変更が行われた場合は、通信にかかるリスク対策のシステム運用に変更の必要がないかどうかのチェックを行う。

- 通信に対するリスク対策実施基準、個々の通信に対する対策要件、暗号化の方法、改ざん検知の方法等、通信にかかるリスク対策にかかる具体的手段の変更
- 関係するシステム構成の変更
- システムの運用形態の変更
- 通信にかかるリスク対策に用いている機能の変更

このチェックにより、システム運用に変更が必要となった場合は、以下の対応を適切に行わなければならない。

- 運用規定、運用マニュアルに対する必要な変更
- 必要な場合における運用スケジュールの変更等、システム運用の組立ての変更
- システム運用の変更の運用関係者への徹底

(3) 通信にかかるリスク対策に関する定期作業のスケジュール化

通信にかかるリスク対策にかかわる運用処理の実行を漏れないようするためには、システム運用上定期的に実施すべき作業は、予めスケジュール化しておくことが有効である。

通信にかかるリスク対策に関連し、定期的な作業としてスケジュール化しておくべき作業としては、以下があげられる。

- サイトにおける商取引にかかる外部との通信実態の正確な把握
- 通信にかかるリスク対策に用いる機能の実装ならびにその動作環境の定期メンテナンス
- 通信にかかるリスク対策に用いる機能の実装ならびにその動作環境の定期点検
- メールの暗号化等操作に依存する対策の実行状況のチェック
- 通信の安全に関係するセキュリティ管理情報の定期メンテナンス
- 通信ログ、通信情報の保全に関する定期的な処理

(4) 関係する運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行

通信にかかるリスク対策にかかわる運用処理についてのチェックリストを作成し、運用実績を記入、報告し、個々の作業が的確に実行されたことの確認を常に行うようにすることも、運用上から必要な処理が漏れないようにするための工夫の一つである。

(5) 通信にかかるリスク対策に関係する運用処理についての記録と管理

以下に示すような通信にかかわるリスク対策にかかわる運用上の処理については、その記録を残し管理する。

- 関係機能の実装の変更
- 機器やソフトの機種等の入替え変更、バージョンの変更
- 機器やソフトのシステム構成上の配置や接続方法の変更
- 機器やソフトの設定の変更　他

- 暗号鍵、パスワード、認証局の証明書の更新等、通信路上のリスク対策に用いる情報の変更
- 通信データの保全処理
- 通信にかかるリスク対策に関するシステム運用の変更

【実施対策上のポイント】

(1) 通信にかかるリスク対策の運用規定や運用マニュアルへの反映手順の確立

通信にかかるリスク対策にかかわる諸施策の運用規定や運用マニュアルへの反映を確実にするためには、これらの施策の運用規定や運用マニュアルへの反映手順を確立しておくことも必要となる。

これらの手順については、11.2 節の**“(4)セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに適切に反映する”**の項参照。

(2) 通信にかかるリスク対策にかかわる運用処理に関するチェックリストについて

日々の運用における通信にかかるリスク対策にかかわる運用処理を、確実なものにするための実行チェックリストにあげるべき処理としては、以下のようなものがあげられる。

- サイトにおける商取引にかかる外部との通信の正確な把握の確認
- 通信路上のリスク対策機能の実装ならびにその動作環境の状況の確認
- 通信路上のリスク対策機能の実装ならびにその動作環境の定期メンテナンス
- サイトの運営環境の変更に伴う、通信路上のリスク対策機能の実装ならびにその動作環境の見直し
- メールの暗号化等操作に依存する対策の実行状況のチェック
- 通信路上のリスク対策に関する監視のチェック
- 暗号鍵、パスワード、認証局の証明書等のセキュリティ管理情報の定期メンテナンス
- 通信路上の情報保護に関する事故に備えた通信ログ、通信情報の保全に関する定期的な処理

(8) 通信にかかるリスク対策の実施状況についての監査を行う

【主旨】

通信にかかるリスク対策は、個々の通信毎に、機能の実装あるいは操作が必要となるため、対策要件は適切に決められていても、実行上で漏れが生じ易い。そして、この実装または操作上で必要な措置の漏れは、攻撃者に対し、保護されるべき通信に対し盗聴や改ざん等の攻撃のチャンスを与えることになり、セキュリティ管理情報やユーザ情報に対する保護管理にかかる努力を無にすることにつながりかねない。このため、対応機能の実装と、通信上で必要となる操作の実施の徹底を図る努力は欠かせない。

このため、通信にかかるリスク対策の実施状況についての監査を定期的に行い、通信にかかる事故が発生する前に、問題点を発見し適切な改善策を講じることができるようにしておくことも必要である。

また日常の運用の中で、実施した通信にかかるリスク対策に関する処理についての記録の保管等、この監査のための準備を組込んでおくことも必要となる。

(注) 正式な監査という形はとらなくとも、ここに示すような通信にかかるリスク対策の実施状況についてのチェックは、組織的に行われるべきものである。

【具体的な実施事項】

(1) 通信にかかるリスク対策の実施状況についての定期的な監査の実施

最低でも年1回は、以下に示すようなことをチェックする、通信にかかるリスク対策の実施状況についての監査を行う。

- 通信にかかるリスク対策についての責任体制の整備状況とその機能状況
- 通信にかかるリスク対策実施基準の妥当性
- 保護対象の通信個々に設定している対策要件の妥当性
- 個々の通信に定めた対策要件の実施状況
- 通信にかかるリスク対策に用いる機能の実装状況
- 通信にかかるリスク対策で操作に依存する通信における、運用現場での実行状況
- 通信にかかるセキュリティ事故への備えの状況
- 通信にかかるリスク対策のシステム運用への反映状況
- 関係者における通信にかかるリスクとリスク対策についての認識

(2) 監査実施要領の確立

通信にかかるリスク対策の実施状況についての定期的な監査が、円滑に実施され、かつ実効的なものにするためには、この監査についての実施要領が確立されていることが望ましい。

この監査実施要領で規定しておく事項については、1.2.2 節の(4)項を参照。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。このためには、監査指摘事項に対する改善措置が実際にとられたかどうかについてのチェックを行うことも必要であり、監査要領の中に、指摘事項についてのフォローの仕組みも組込んでおくことも必要である。

【対策実施上のポイント】

(1) 監査内容例

表 8-7 に、通信にかかるリスク対策の実施状況についての監査において、チェックすべきことの例を示す。

(2) 監査の報告

監査結果は、通信にかかるリスク対策責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告されなければならない。

表 8-7 通信にかかるリスク対策の実施状況に関する監査内容例

項番	監査項目	監査の内容等
1	通信にかかるリスク対策についての責任体制の整備状況とその機能状況	・通信にかかるリスク対策についての責任体制は、サイトの運営実態に照らして適切か ・該当責任者における自己の責任についての認識は十分か ・通信にかかるリスク対策に関する責任体制は機能しているか
2	通信にかかるリスク対策実施基準の妥当性	・通信にかかるリスク対策実施基準は、サイトの運営に照らして適切か
3	保護対象の通信個々に設定している対策要件の妥当性	・保護対象とすべき通信すべてに対してリスク対策要件が定義されているか ・保護対象通信個々に設定されているリスク対策要件は、対策実施基準やシステムの運営実態に照らして適切か
4	個々の通信に定められている対策要件の実施状況	・個々の通信に定められているリスク対策要件の実行は管理されているか

項番	監査項目	監査の内容等
5	通信にかかるリスク対策に用いる機能の実装状況	・個々の通信に適用する技術およびその機能選択は妥当か ・その実装の正確性は確認されているか （実装すべき場所に正確に実装されているか） ・運用環境の変更時における対応機能の実装の見直しは行われているか ・必要な運用環境の整備状況についてのチェックは適切に行われているか
6	通信路上のリスク対策で、操作に依存する通信における、運用現場での実行状況	・該当通信についての運用規定、操作マニュアルは整備されているか ・関係者に対する徹底努力は適切に行われているか ・実務において、定められた保護操作の実行は、きちんと行われているか（実運用でどの程度守られているか） ・定められた保護操作の実行についてのチェック、指導は適切に行われているか
7	通信にかかるセキュリティ事故への備えの状況	・通信にかかるセキュリティ事故に対する対処要領は適切に決められているか ・監査期間における事故対策は妥当であったか
8	通信にかかるリスク対策のシステム運用への反映状況	・通信にかかるリスク対策がシステム運用に求めていることは、運用規定、運用マニュアルに適切に反映されているか ・これらの運用は、日々の運用において確実に実行されているか、またそのことが管理されているか ・通信にかかるリスク対策に関係するシステム運用の適切な実行の実現のための工夫は十分か
9	関係者における通信にかかるリスクとリスク対策についての認識	・通信にかかるリスクについての認識は十分か ・通信にかかるリスク対策に用いている技術についての理解は十分か ・設定している対策基準についての理解は十分か ・保護対象通信の個々に適用しているリスク対策とその運用についての理解は十分か

9 ユーザ認証の適切な適用

9.1 必要な施策

図 9-1 に、適切なユーザ認証の実施のための施策の構成を示す。

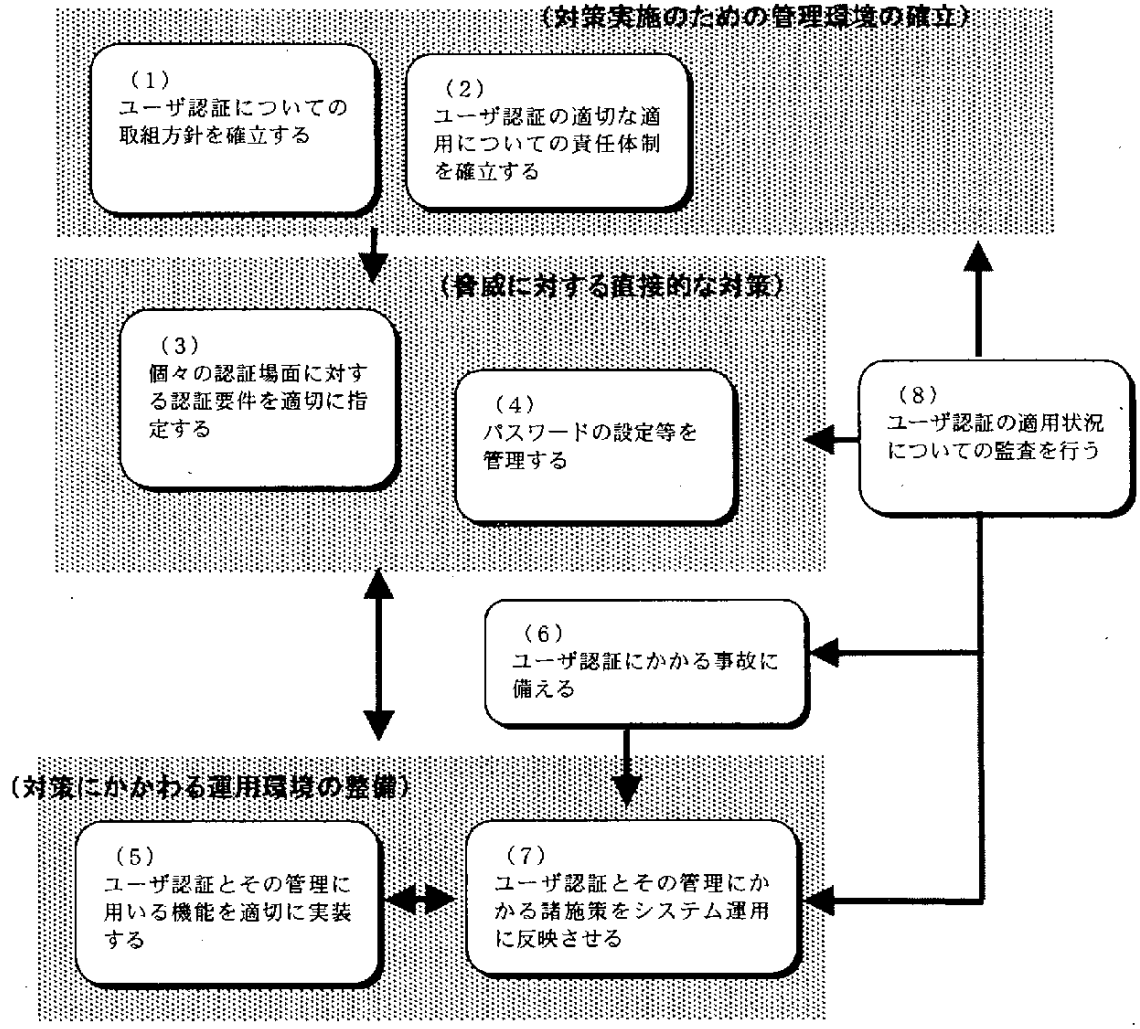


図 9-1 ユーザ認証の適切な適用のための施策の組立て

また、表 9-1 に各施策における実施事項の一覧を示す。

表 9-1　ユーザ認証の適用にかかる施策における具体的実施事項

施策名	具体的実施事項
(1) ユーザ認証についての取組方針を確立する	① ユーザ認証の適用に関する管理目標の明確化 ② 適用範囲の明確化 ③ ユーザ認証適用基準の確立 ④ ユーザ認証の適切な適用の実現に向けた施策の組立ての明確化 ⑤ 取組方針の関係者への 周知
(2) ユーザ認証の適切な適用についての責任体制を確立する	① ユーザ認証の適切な適用についての責任体制の明確化 ② ユーザ認証管理関係者間の連絡体制の確立
(3) 個々の認証場面に対する認証要件を適切に指定する	① 個々の認証場面に対する認証方式とその運用方式の指定 ② 個々の認証場面に適用している認証についてのドキュメントの整備
(4) パスワードの設定等を管理する	① パスワード管理基準の確立 ② パスワード管理基準の関係者への周知 ③ パスワードの登録受付時における適正性チェックの実施
(5) ユーザ認証とその管理に用いる機能を適切に実装する	① 適切な技術と使用する機能の選択 ② 組込み場所の適切な設定 ③ 選択した技術、機能の的確なインストール ④ 必要な運用環境の整備 ⑤ 使用技術の実装についてのドキュメントの整備
(6) ユーザ認証にかかる事故に備える	① ユーザ認証事故への対処要領の確立 ② ユーザ認証に関する事故の処理に必要となる情報の整備 ③ 必要なツールの準備
(7) ユーザ認証とその管理にかかる施策をシステム運用に反映させる	① ユーザ認証にかかる諸施策の運用規定、運用マニュアルへの適切な反映 ② 運用環境の変更への適切な対応 ③ ユーザ認証の管理にかかる定期作業のスケジュール化 ④ 関係する運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行 ⑤ ユーザ認証の管理にかかる運用処理についての記録とその保管
(8) ユーザ認証の適用状況についての監査を行う	① ユーザ認証の適用状況についての定期的な監査の実施 ② 監査実施要領の整備 ③ 監査指摘事項に対するフォローの実施

9.2 個別具体策

(1) ユーザ認証についての取組方針を確立する

【主旨】

他人をかたった者との取引の実行等、意図した相手と異なる者との処理の実行は、業務の混乱や、保護すべき情報の流出等の事故を招く。このようなユーザ認証にかかる事故の防止を図るとともに、万一事故が発生しても、その被害を限定的なものにすることに組織的に取組むには、ユーザ認証をどのような考えで、またどのような方法で実施するかについての取組方針を確立しておくとともに、これをユーザ認証の管理に直接かかわる者だけでなく、システムの構築や運用に関係する者に加え、業務上ユーザ認証が付随している処理や、ユーザ認証に用いるパスワード等の情報に触れる者のすべてに、周知させておくことが必要となる。

(注)本ガイドラインでは、ショップ業務運営上の処理に適用されるユーザ認証のみを対象にする。システム管理にかかわる処理におけるユーザ認証(管理者権限の確認等)は、システムへのアクセス管理、セキュリティ管理情報へのアクセス管理、ユーザ情報へのアクセス管理の問題とする。

【具体的な実施事項】

(1) ユーザ認証の適用に関する管理目標の明確化

ユーザ認証の適用に関する管理が目標とするところを明確にし、対応する施策の意図を明確にする。ユーザ認証の適用にかかる管理施策の目標としては、以下があげられる。

- ユーザ認証にかかる事故の抑止
- ユーザ認証にかかる事故発生時の被害の極小化

(2) 適用範囲の明確化

ユーザ認証の適用に関する管理施策の適用範囲として、以下を明確にする。

- 対象業務
- 対象組織

(3) ユーザ認証適用基準の確立

認証の厳密さに対する要求は、対象とする業務によって異なってくる。適用する認証方式もそれぞれの認証場面の要求にあったものでなければならない。

個々の認証場面におけるユーザ認証が不適切であったり、ショップ運営全体の中でばらつきが生じたりすることを防ぐためには、認証に、その厳格さによるレベル分けを行い、それぞれのレベルに対する標準的な認証方式や運用上の条件等の認証要件を定義したユーザ認証適用基準を確立しておき、ユーザ認証が必要な個々の場面ごとに、適切な認証レベルを割当て、その認証レベルに指定されている認証要件に基づいた認証方式を適用するような工夫も必要となる。

ユーザ認証適用基準として定義すべき事項をあげると、以下のようになる。

- ユーザ認証レベルの名称
- 当該レベルに求められる認証のレベル
- 当該レベルの適用範囲
- 認証方式についての要件
- 適用技術
- 認証用の情報についての要件
- 運用上の要件

ユーザ認証が必要な個々の処理に対し適用されるユーザ認証の方式は、この基準に従っていなければならない。

(4) ユーザ認証の適切な適用の実現に向けた施策の組立ての明確化

ユーザ認証の適切な適用をどのように実現するかを明らかにするもので、実施する施策の構成と施策間の関係を示す。

本ガイドラインにおける適切なユーザ認証の実現のための施策の構成については、9.1 節、参照。

(5) 関係者への取組方針の組織内への周知

作成されたユーザ認証の適切な適用についての取組方針は文書化され、ユーザ認証の管理に直接かかわる者だけでなく、システムの構築ならびに運用関係者や、業務上ユーザ認証にかかわるに者のすべてに周知させておかなければならない。このためには、

- ユーザ認証の適切な適用についての取組方針の掲示や配布
- ユーザ認証の適切な適用についての取組方針の再確認の定期的な実施

も必要となる。

【対策実施上のポイント】

(1) ユーザ認証適用基準の定義要領

ユーザ認証の適用基準を定義するにあたって明示すべき事項の内容を、表 9-2 に示す。

表 9-2 ユーザ認証適用基準の定義内容

項番	定義項目	内容
1	ユーザ認証レベルの名称	・当該レベルの ID、名称
2	当該レベルに求める認証のレベル	・当該認証レベルに求める認証の厳密さ(注1)
3	当該レベルの適用範囲	・ユーザ認証の重要度クラスで表す当該クラスが適用されるユーザ認証の場面
4	認証方式についての要件	・ 当該認証レベルに対し適用が可能な認証方式の範囲(注2)
5	適用技術	・ 適用する製品・技術の指定 ・ 認証に用いる技術についての制約
6	認証用情報についての要件	・ パスワードの設定上の制約 ・ 有効期間等メンテナンスに関する要件
7	運用上の要件	・ 保管上の要件 －暗号化等の保管上の要件 －バックアップ取得に関する要件

(注1) 求める認証レベルの定義例

- 運用に依存せず100%近い制度が期待でき、法的にも保障される
- 運用に依存せず100%近い制度が期待できるが、法的に保障されるものではない
- 運用に依存するところはあるが、100%近い制度を期待することができる
- サイト側の運用が厳密であれば、かなり高い精度を期待できる
- ユーザの運用に依存するところが多いが、ある程度の精度を期待できる
- ユーザの運用に依存するところが多く、精度の低いもの

(注2) 一般に EC サイトで適用が考えられるユーザ認証方式

- 公的に認められた認証局による証明書を使用
- 私的な認証局による証明書を使用
- 厳密な運用(頻度の高い更新が行われる)のパスワードを使用
- 一般的なパスワードを使用
- 生体認証を使用
- 機器の ID を使用
- 申告をそのまま信用:識別だけで認証は不要

(2) ユーザ認証の重要度クラスについて

ユーザ認証の重要度とは、相手の誤認やなりすましを許した場合における影響の大きさの尺度を示すもので、ユーザ認証が必要な個々の場面に対するユーザ認証の厳格さを決める時の

判断材料となるものである。

この重要度についてクラス化を行い、個々の認証場面に割当てる認証レベルは、当該認証場面に指定された重要度クラスにより決定するようにすることも、ユーザ認証をサイト全体として統制のあるものにすることに有効である。

表 9-3 に、ユーザ認証の重要度クラスの定義例を示す。

表 9-3 ユーザ認証の重要度クラスの定義例

項番	重要度クラス	ユーザ認証の重要度
1	クラスA	その処理が本来のユーザと異なる者と行われた場合、本来のユーザに直接的な損害を与える可能性のあり、かつ、その損害も大きなものになる可能性のあるもの
2	クラスB	その処理が本来のユーザと異なる者と行われた場合、本来のユーザに直接的な損害を与える可能性はあるが、その損害の規模は限定的なもの
3	クラスC	その処理が本来のユーザと異なる者と行われた場合、本来のユーザに直接的な損害は与えないにしても、ユーザとの間でトラブルになる恐れのあるもの
4	クラスD	その処理が本来のユーザと異なる者と行われた場合、業務に一時的なトラブルを生じるもの
5	クラスE	その処理が本来のユーザと異なる者と行われた場合、本来のユーザに損害を与えたり、業務に影響を与えたりはしないものの、サイトやショップの信頼を傷つける恐れのあるもの

(3) 認証レベルの設定について

認証のレベル分けを行う時の検討要素としては、以下があげられる。レベル分けは、システムの特性に合わせて決めればよく、必要以上の細分化は不要である。

- 認証の対象(個人か、マシンか？)
- 認証対象者の範囲(不特定多数か、特定者か？)
- 認証対象者の特性(事前審査の有無等)
- 対象者に対するサービスの内容(なりすましが行なわれた場合の被害のレベル)
- システムの運用形態
- 適用技術のレベル

(4) 各認証レベルに対する認証要件、適用技術、運用条件等の検討要素

対象システムにおける、それぞれの認証レベルに対し適用する技術とその運用の原則について、以下の事項を明確にしておかねければならない。

- 求める認証の精度のレベル
- 適用できる技術の信頼性、導入の容易性、導入コスト、運用コスト
- 適用できる技術の運用性(環境整備、運用管理の容易性)
- 認証を要する処理における操作性

(5) ユーザ認証適用基準の定義例

表 9-4 に、ユーザ認証の適用基準の定義例を示す。

表 9-4　ユーザ認証の適用基準の定義例

項番	対象重要度クラス	適用対象	認証要件等
1	クラスA	・重要度クラスAの認証に適用 ・対象業務 　－金融取引処理	・認証方式についての要件・・・・・・・ 　－公的認証機関による証明書によるサイト確認＋生体認証による操作者の本人確認 ・使用技術・・・・・・・・・・・・・・・・・・・・(略) ・認証用情報についての要件・・・・・ 　－設定についての特定条件 　－暗号化して保存 ・運用上の要件・・・・・・・・・・・・・・・・

(6) 取組方針の見直しについて

ユーザ認証の適切な使用についての取組方針は、システム構成やその運用形態等、システム運用の実環境の変化に対応して必要な修正が加えられるべきであり、必要に応じて見直しを行うこと。また、ユーザ認証の適切な使用についての取組方針は、定期的に関係者間で再確認することをルーチン化しておくことが望ましい。

(2) ユーザ認証の適切な適用についての責任体制を確立する

【主旨】

業務やサイトの運用で用いられるユーザ認証を適切なものにするための諸施策を、その取組方針に沿って機能させるためには、ユーザ認証の適用について定められていることが、システムの構築や運用に適切に反映されるよう、指導、管理する責任体制の確立が必要となる。

このためには、ユーザ認証の適用にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) ユーザ認証の適切な適用についての責任体制の明確化

ユーザ認証の管理にかかる責任体制に関し、明確にしておくべきこととしては、以下があげられる。

- ユーザ認証管理責任者とその責任
- ユーザ認証の管理担当者の責任
- 業務現場でのユーザ認証またはユーザ認証に用いる情報の取扱責任者とその責任
- システム開発者のユーザ認証に関する責任
- システム管理者のユーザ認証に関する責任
- システム運用者のユーザ認証に関する責任

(2) ユーザ認証管理関係者間の連携体制の確立

ユーザ認証の管理についての責任体制が有効に機能するためには、関係者間の連携が重要となる。

【対策実施上のポイント】

(1) ユーザ認証管理関係者の責任分担

表 9-5 に、ユーザ認証の管理にかかわる者の責任分担の定義例を示す。

(2) ユーザ認証の管理に関する責任体制は、ユーザ認証の取扱いを変更したり、業務やサイトのの運営形態に変更が生じた場合は、見直しを行い、必要な変更を行うこと。

表 9-5　ユーザ認証の管理関係者の責任分担

責任区分	タスク
ユーザ認証管理責任者	・ユーザ認証の適用についての取組方針の確立と関係者への周知 ・ユーザ認証の適用基準の発行 ・ユーザ認証の適用全体の妥当性の維持 ・ユーザ認証の適用状況の把握 ・ユーザ認証適用基準に従ったユーザ認証の適用についての指導 ・ユーザ認証に関する事故発生時における事故処理の指導
ユーザ認証の管理担当者	・ユーザ認証適用基準の検討、見直し ・ユーザ認証の適用の実施状況の把握 ・基準に従ったユーザ認証の適用の監督、管理 ・ユーザ認証に関する事故発生時における事故処理と再発防止策の検討
業務現場におけるユーザ認証ならびに認証情報の取扱い責任者	・業務現場におけるユーザ認証ならびに認証情報の取扱い規定の妥当性のチェックと改善の提案 ・業務現場における、ユーザ認証ならびに認証情報の取扱い状況の把握 ・業務現場における、ユーザ認証適用基準に従ったユーザ認証ならびに認証情報の取扱いの監督、管理 ・ユーザ認証に関する事故発生時における業務サイドにおける事故処理
システム開発責任者	・各認証場面に対するユーザ認証要件に必要な機能の的確な組込み －設計の妥当性の確認 －漏れの的確な実装の確認
システム管理責任者	・システムにおけるユーザ認証にかかわる機能の維持管理 －システム構成変更の反映の管理 －ユーザ認証関係機能の維持管理 ・システムにおける対応機能の実装状況の正確な把握
システム運用責任者	・システム運用におけるユーザ認証支援機能の動作環境の整備 ・ユーザ認証にかかる運用のチェックと指導

(3) 個々の認証場面に対する認証要件を適切に指定する

【主旨】

求めるユーザ認証が適切に機能するようにするためには、ユーザ認証が必要な個々の場面において、適用される認証のレベル、その認証レベルを満足するための認証方式、そのために実装すべき機能、および当該機能にからむ運用上の要件等が、ユーザ認証ついての取組方針の中で定められているユーザ認証適用基準に沿って適切に決められていなければならない。

認証手段が厳格になればなるほど、取引実行上の操作や運用管理面での負担が大きくなるのが一般である。ユーザ認証の方式の選択に当っては、目的を損なわないようにしながら、これらのことについてバランスがとれるようにしなければならない。

また、どの場面にどのような認証がどのように適用されているかを、常に正確に把握できているようにしておくことも重要である。

【具体的な実施事項】

(1) 個々の認証場面に対する認証方式とその運用方式の適切な指定

当該サイトやショップの運営においてユーザ認証が必要な場面の洗出しを行い、個々のユーザ認証ごとに適用する認証方式と必要な運用上の条件等、下記項目を明確にする。

- ユーザ認証場面の定義
- 認証対象ユーザの定義
- 適用する重要度クラス
- 適用認証クラス
- 適用する技術とその使用条件
- 認証用情報の扱い等当該ユーザ認証にかかるサイト運用上の要件

(2) 個々の認証場面に適用している認証についてのドキュメントの整備

ユーザ認証が適切に行われているかどうかについての管理が適切に行えるように、当該サイトおよびショップの運営で用いているユーザ認証の実態を一覧できるドキュメントを整備しておくことも必要である。

【対策実施上のポイント】

(1) 個々のユーザ認証に対する認証要件の定義要領

表 9-6 に、個々のユーザ認証に対する認証要件の定義にあたって、指定すべき事項を示す。

表 9-6　個々のユーザ認証に対する認証要件定義における指定事項

項番	指定項目	指定内容
1	ユーザ認証場面	・対象とするユーザ認証の場面を、下記事項等で定義する －対象とする業務 －対象処理
2	認証対象ユーザと認証の要件	・認証の対象となるユーザの範囲を指定する(注1) ・認証により与えられる権限(注2) ・必要な資格(注3)
3	適用重要度クラス	・当該認証に割当てる重要度クラスを指定
4	適用認証レベル	・当該認証に割当てるユーザ認証適用基準における認証レベルを指定する
5	適用する技術とその使用条件	・適用する技術(製品等)または方式の指定 ・適用する技術における機能選定
6	運用上の要件	・当該技術の使用環境(注4) ・パスワードの更新サイクル等認証用情報に関する条件 ・パスワード等の認証用情報の取扱い上の要件

(注1)特定会員、社員等認証の対象となるものの身分、資格等
(注2)アクセスできるサービスや情報等、その認証により与えられる権限
(注3)権限の取得または付与の方法
(注4)認証局の選定等、当該認証技術が前提とする環境

(2) 個々の場面々々への適用方式の選択に当っては、認証の重要度クラスと、ユーザの使い勝手、コスト、運用環境の手間等のバランスを考慮しなければならない。

(3) システム全体におけるユーザ認証の適用状況の整理

ユーザ認証が求められる個々の場面毎に設定された認証に関する要件を、一表に纏め、サイトにおけるユーザ認証の実施状況が正確に把握できるようにしておかなければならない。

この表で明らかにしておくべき事項は、(1)で規定した項目となる。

(4) ユーザ認証用の情報の取扱いについては、**"7.1 セキュリティ管理情報の保護管理"参照。**

(5) ライフサイクル管理の徹底

ユーザ認証に用いられる情報については、その登録、更新、廃棄等ライフサイクル上のそれぞれのイベントごとに、その取扱いのルールが決められていなければならない。

また、その取扱いはこのルールに従って実行されていることが管理されてなければならない。

(6) 認証用情報の保護管理の徹底

システム上やDB上に置かれたユーザ認証に用いられる情報や、印刷物等別媒体上のこれらの情報の取扱いについても、厳正な保護管理が実施されなければならない。

これらについての具対策については、「適切なセキュリティ管理情報の保護管理の実施」の項参照。

(4) パスワードの設定等を管理する

【主旨】

パスワードをユーザ認証に用いる場合、盗まれ易い設定は避けなければならない。

このため、パスワードの設定についての基準を設け、パスワードの登録者に対する啓蒙を行なったり、パスワードの登録受付にあたって盗まれ易い設定を排除することが必要である。

また、その定期的な更新の実施も重要である。

【具体的な実施事項】

(1) パスワード管理基準の確立

パスワードを盗まれにくいものにするため、個々のパスワードについて、パスワードの設定とその管理についての基準を定めておく。基準として定めるべき事項としては、以下があげられる。

- パスワードの設定原則
  - －文字の組合せに関する原則
  - －使用を避ける設定
- パスワードのメンテナンス要件

  同じパスワードの長期使用は、攻撃者に解読のチャンスをそれだけ多く与えることになるため、定期的に新たなものにすることが望ましい。必要とされる更新頻度は、運用負担とその認証の重要度による。
- パスワードの設定手順

  以下に示すようなパスワードの設定に関する手順を明確にする。
  - －パスワードの設定者(使用設定か、管理者設定か)
  - －パスワードの承認手続き
- システムへの登録手順
- 使用者への連絡手順

  パスワード等の入手や、対象者への通知にあたっては、これらの情報の連絡過程において、第三者に漏洩しないような配慮を施さなければならない。このためには、以下についての検討が必要となる。
  - －収集ルートの適切な設定
  - －配布ルートの設定
  - －連絡相手の確認の実施
  - －収集・配布ルート上の漏洩防止策の実施

(2) パスワード管理基準の関係者への周知

パスワードの登録手順を示す画面や文書等の上に、パスワードの管理基準を明示し、パスワードの登録者に対し、その基準に従った設定を行うように指導する。

(3) パスワードの登録受付け時における適正性チェックの実施

パスワードの登録受付けにあたっては、申請されたパスワードが基準に従っており、盗まれにくいものであるかどうかのチェックを行い、比較的盗まれ破られ易いと判断されるものについては、受付を拒否し、改善を指導するような仕組みを、パスワードの受付処理の中に組込んでおくことも必要である。

【対策実施上のポイント】

(1) パスワードの設定原則としては、以下のようなものがあげられる。

- 一定数以上の桁数とする
- 英文字、数字、特定の特殊記号のランダムな組合せとする
- 以下に示すような何らかの意味を有するパスワードは避ける
  - 辞書の出てくるような言葉、人名・地名、事象、歴史上の事実等普遍的な固有名詞、誕生日、電話番号等個人の属性に関する情報と同じになるもの 他

(2) パスワードの登録要求には、この設定原則の明示と、原則に従った設定を要求する記述があることを確認すること。

(3) パスワードの登録受付け機能に、パスワードの脆弱性チェック機能の組込みを行うのも有効である。

(5) ユーザ認証とその管理に用いる機能を適切に実装する

【主旨】

個々のユーザ認証場面に適用するユーザ認証の実現方法としては、

- OS の機能や、SSL 等通信形態に組込まれた機能や、認証用の専用機器等の使用といった汎用技術の使用
- 独自仕様のよる実現

等があるが、いずれの場合においても、期待通りに機能し、その使用目的を満足するものでなければならない。このためには、選択した技術とその技術が提供する機能の選択、インストール時の設定を適切に行うとともに、そのインストールに対する検査を十分に行うことが必要となる。

また、SSL 適用時における認証書の取得および認証情報のシステムへの登録等、使用する技術が前提とする運用環境の整備に不備がないようにしなければならない。

【具体的な実施事項】

適用する技術の個々に対し、以下のことが求められる。

(1) 適切な技術と使用する機能の選択

- 使用する技術(製品や方式)は、対象処理における認証についての要件を満足するものでなければならない。
- 一般に機器やソフトウェアにはさまざまな機能が準備されており、同じ技術でもその使い方次第で機能も異なってくる。使用する技術そのものは妥当であっても、その機能設定が対象とする使用場面における要件に対して不適切であってはならない。

これらのことが、適切であるかどうかについては十分なチェックを必要とする。

(2) 組込み場所の適切な設定

ユーザ認証とその管理に用いるツールとして選択した技術を期待通りに機能させるためには、選択した技術のシステム構成上の配置を適切なものにしなければならない。使用する技術のシステム構成上での組込み場所は、以下により決められる。

- ユーザ認証の適用にかかる当該技術の役割および適用範囲
- 当該技術の機能特性および前提とする環境条件

(3) 選択した技術、機能の的確なインストール

選択した技術を期待通りに機能させるためには、技術のシステムへのインストールが適切に行われていなければならない。このためには、以下のことが求められる。

- 選択機能の的確なインストール
- テストによる動作確認の実行

  システムへの組込みが終了したら、十分な機能検査を必ず実施し、インストールに不備がないことを確認すること。

(4) 必要な運用環境の整備

SSL の適用の場合は、認証局への登録と証明書の取得とそのシステムへの実装が必要となる。このように、適用した技術によっては、それが機能するために運用上で準備すべきことがある。また、システムの構成管理やシステムの運用において、OS やネットワーク環境の整備、アクセス権限テーブルの整備や、ファイルの暗号化を行った時の暗号鍵の整備等、適用した技術が前提としている環境の整備に不備がないようにしなければならない。

これには、システムの導入時だけでなく、定期的な更新といったその維持管理についての処理も必要となる。

(5) 使用技術の実装についてのドキュメントの整備

使用技術の実装については、いつでもその設定や実装の状況の把握ができるようドキュメント化されていなければならない。

また、このドキュメントは、機能の新規導入時に作成するだけでなく、実装についての変更が行われたときも更新される等、適切にメンテナンスされるようになっていなければならない。

【対策実施上のポイント】

(1) 採用した技術における機能の選択は十分検討すること。使用する技術のデフォルト機能を安易に用いないこと。

(2) 独自仕様の技術を用いる場合、当該機能または、当該機能を含むシステムまたはシステム機能の設計と実装に対し、ISO15408 に準拠した機能の評価および実装の評価を行うことが望ましい。

(3) 使用技術についてのドキュメンテーションに関する留意点

使用技術の実装状況についてのドキュメントに記載すべき事項としては、以下のようなものが ある。

- 当該技術がサポートする認証とそのレベル
- システム構成上の組込み場所
- 設定機能等の各種の指定内容
- 運用上の留意点
- 実装確認テストの内容と結果
- 新規組込みまたはメンテナンス日時

(6) ユーザ認証にかかる事故に備える

【主旨】

個々のユーザ認証場面に対する認証要件の設定が適切であっても、システム構築上のミスや運用における誤り等その実施上の不備や、新たな手法によるなりすまし等により、意識している相手とは異なる者と処理を行ってしまう可能性も、常に考えておく必要がある。

このような事態が発生した場合における被害の拡大を防ぐとともに、業務やシステムの運用の混乱を極小化するためには、不当に処理された取引に対する業務およびシステム面での対処だけでなく、この不当処理に伴う情報の漏洩等からくる二次的な被害についても調査し、必要な処置を迅速に適切に行わなければならない。

事故時の対処が適切かつ迅速に行われるようにするためには、ユーザ認証にかかるセキュリティ事故が発生した時の対処要領を確立しておくとともに、常日頃から、事故処理に必要となる情報やツールの整備を行っておくことが求められる。

また、ユーザ認証に関する事故の原因が、サイトシステムに対する不正なアクセスや、セキュリティ管理情報の漏洩にある場合は、システムへの不正アクセス対策やセキュリティ管理情報の保護管理策等、関係するセキュリティ対策の見直しも必要となる。

【具体的な実施事項】

(1) ユーザ認証事故への対処要領の確立

ユーザ認証にかかる事故が発生した場合における必要な処置を円滑に行えるようにするためには、事故時の対処要領を確立しておくことが必要である。

ユーザ認証にかかる事故に対する対処要領として明確にしておくべき事項としては、以下があげられる。

- 対策チームの編成
- サービスの停止等取りあえずの措置
- 当該処理についての被害範囲の調査、特定
- 対象処理に対する業務上ならびにシステム処理上の対処方法の扱いの決定
- 二次被害の調査、特定
- 二次被害に対する対応方法の決定
- 二次被害への対処
- 原因の分析と再発防止策の検討とその実施
- 処理経緯の記録と保管
- 事故対策訓練の実施基準
- 事故対策に必要な環境の整備

(2) ユーザ認証に関する事故の処理に必要となる情報の整備

ユーザ認証の管理についての運用の記録等ユーザ認証に関する事故の処理に必要な情報は、適切に記録、保管されていなければならない。

(3) 必要なツールの整備

ユーザ認証にかかるセキュリティ事故発生時における被害範囲の調査等の事故への対処に用いるツールは、期待通り機能しなければならない。

このためには、

- 適切なツールの選択とその適切なシステムへのインストール
- 運用環境の変更への対応
- ツール使用上のマニュアルの整備

等に不備がないようにしておかなければならない。

【対策実施上のポイント】

(1) ユーザ認証に関する事故の被害範囲の調査に必要な情報

ユーザ認証に関する事故の被害範囲の調査に必要な情報としては、以下のようなものがあげられる。

- システム構成を示す情報
- システムにおける当該処理の位置付けを示す情報
- 業務における当該処理の取扱いを示す情報
- システムにおける当該処理に適用している認証手段とその実装ならびに運用状況に関する情報
- 当該処理における処理経緯を記録した情報

これらは、いずれも運用規定に従い記録、保管されていなければならない。

(7) ユーザ認証とその管理にかかる施策をシステム運用に反映させる

【主旨】

ユーザ認証の適切な適用のための諸施策が有効に機能するためには、ユーザ認証の管理がシステムの運用に求めていることが、実際のシステム運用において適切に実行されなければならない。

このことを確実なものにするためには、これらが日々のシステム運用において的確に実施されるようにする管理上の仕組みを工夫し、これらを日常の運用に組込んでおくことが必要となる。

【具体的な実施事項】

(1) ユーザ認証にかかる諸施策の運用規定、運用マニュアルへの適切な反映

ユーザ認証の適用にかかる諸施策が運用に求めていることは、すべてシステムの運用規定や運用マニュアルに適切に反映されていなければならない。

(2) 運用環境の変更への適切な対応

運用環境に以下に示すような変更が行われた場合は、ユーザ認証の管理にかかるシステムの運用に変更の必要がないかどうかのチェックを行う。

- ユーザ認証ルール、認証方法、認証情報の保護管理方法等、ユーザ認証の管理にかかる具体的手段の変更
- 関係するシステム構成の変更
- システムの運用形態の変更
- ユーザ認証に用いている機能の変更

このチェックにより、システム運用に変更が必要となった場合は、以下の対応を適切に行わなければならない。

- 運用規定、運用マニュアルに対する必要な変更
- 必要な場合における運用スケジュールの変更等、システム運用の組立ての変更
- システム運用の変更の運用関係者への徹底

(3) ユーザ認証の管理にかかる定期作業のスケジュール化

ユーザ認証の適切な適用に運用処理の実行を漏れないようするためには、システム運用上定期的に実施すべき作業は、予めスケジュール化しておくことが有効である。

ユーザ認証の管理に関連して、定期的な作業としてスケジュール化しておくべき作業としては、以下があげられる。

- ユーザ認証に用いる機能の実装ならびにその動作環境についての定期点検
- ユーザ認証に用いる機能の実装ならびにその動作環境の定期メンテナンス
- パスワード等ユーザ認証に用いる情報の定期メンテナンス
- ユーザ認証に関する事故に備えた情報の保全処理

(4) 関係する運用作業についてのチェックリストの作成とチェックリストに基づく実行確認の励行

ユーザ認証の管理にかかる運用作業についてのチェックリストを作成し、運用実績を記入、報告し、個々の作業が的確に実行されたことの確認を常に行うようにすることも、運用上から必要な処理が漏れないようにするための工夫の一つである。

(5) ユーザ認証の管理にかかる運用処理についての記録とその管理

以下に示すようなユーザ認証の適用にかかわる運用上の処置については、その記録を残し管理する。

- 関係機能の実装の変更
  - 機器やソフトの機種等の入替え変更、バージョンの変更
  - 機器やソフトのシステム構成上の配置や接続方法の変更
  - 機器やソフトの設定の変更 他
- 暗号鍵、パスワード、認証局の証明書の更新等、通信路上のリスク対策に用いる情報の変更
- ユーザ認証の管理にかかるシステム運用の変更

【実施対策上のポイント】

(1) ユーザ認証の適用に関する諸施策の運用規定や運用マニュアルへの反映手順の確立

ユーザ認証の適用に関する諸施策の運用規定や運用マニュアルへの反映を確実にするためには、これらの施策の運用規定や運用マニュアルへの反映手順を確立しておくことも必要となる。

これらの手順については、11.2 節の**"(4)セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに適切に反映する"**の項参照。

(2) ユーザ認証の適用に関する運用処理のチェックリストについて

日々の運用におけるユーザ認証の適用にかかる運用処理を、確実なものにするための実行チェックリストにあげるべき処理としては、以下のようなものがあげられる。

- サイト運営におけるユーザ認証が必要な処理の把握状況の確認
- ユーザ認証に用いる機能の実装ならびにその動作環境の定期メンテナンス
- サイトの運営環境の変更に伴う、ユーザ認証に用いる機能の実装ならびにその動作環境の見直し
- パスワード等のユーザ認証用情報の定期メンテナンス
- パスワード等認証用情報を含む電子媒体や印刷物に関する処理
- ユーザ認証に関する事故に備えた通信ログ、通信情報の保全に関する定期的な処理

(8) ユーザ認証の適用状況についての監査を行う

【基準の主旨】

ユーザ認証とその管理がずさんであれば、攻撃者にとってなりすましは容易なものとなる。ユーザ認証の適用の不備が問題をおこす前に、問題点を発見し適切な改善を講じることができるようにしておくことも重要である。

このためには、ユーザ認証の適用を適切にするために定められている諸施策が、サイト運営の実態に照らして適切かどうか、また、定められていることが適切に実施されているかどうか等についてのチェックを行い、問題点の摘出と必要な改善を指導する、ユーザ認証の適用状況についての監査を定期的に行うことも必要である。

また日常の運用の中で、実施したユーザ認証の管理にかかわる運用についての記録の保管等、この監査のための準備を組込んでおくことも必要となる。

(注)正式な監査という形はとらなくとも、ここに示すようなユーザ認証の適用状況についてのチェックは、組織的に行われるべきものである。

【具体的な実施事項】

(1) ユーザ認証の適用状況についての定期的な監査の実施

最低でも年1回は、以下に示すようなことをチェックする、ユーザ認証の適用状況についての監査を行う。

- ユーザ認証の管理についての責任体制の整備状況とその機能状況
- ユーザ認証適用基準の妥当性
- 個々のユーザ認証場面に対し設定している認証要件の妥当性
- 個々のユーザ認証場面に対するユーザ認証の適用状況
- ユーザ認証に用いる機能の実装状況
- パスワード等の認証用情報の取扱い状況
- ユーザ認証事故への備えの状況
- 適切なユーザ認証の実現に向けた諸施策のシステム運用への反映状況
- 関係者におけるユーザ認証の厳格な運用についての認識

(2) 監査実施要領の確立

ユーザ認証の適用状況についての定期的な監査が、円滑に実施され、かつ実効的なものにするためには、この監査についての実施要領が確立されていることが望ましい。

この監査実施要領で規定しておく事項については、1.2.2節の(4)項を参照。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。

このためには、監査指摘事項に対する改善措置が実際にとられたかどうかについての確認を

行うことも必要であり、監査指摘事項についてのフォローの仕組みも、監査要領の中に組込んでおくことも有効である。

【対策実施上のポイント】

(1) 監査内容例

表 9-7 に、ユーザ認証の適用状況についての監査において、チェックすべき事項の例を示す。

(2) 監査の報告

監査結果は、ユーザ認証についての責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告されなければならない。

表 9-7 ユーザ認証の適用状況に関する監査内容例

項番	監査項目	監査の内容等
1	ユーザ認証についての責任体制の整備状況とその機能状況	・ユーザ認証に関する責任体制は、サイトの運営実態に照らして適切か ・ユーザ認証に関する責任者の自己の責任についての認識は十分か ・ユーザ認証に関する責任体制は機能しているか
2	ユーザ認証適用基準の妥当性	・設定されているユーザ認証適用基準は、サイトの運営実態に照らして適切か ・パスワード等ユーザ認証に用いる情報の管理基準は、妥当に定められているか
3	個々のユーザ認証場面に対し設定している認証要件の妥当性	・個々の認証が必要な処理に適用している保護方式は、ユーザ認証適用基準およびシステムの運営実態に照らして適切か ・ユーザ認証が必要な場面の洗出しはできているか ・個々のユーザ認証場面に適用している認証方式と必要な運用についての指定は明確になっているか ・個々のユーザ認証場面に適用している認証方式および対応して指定されている運用は、ユーザ認証適用基準に照らして適切か
4	個々のユーザ認証場面に対するユーザ認証の適用状況	・個々のユーザ認証場面に対し適用されているユーザ認証は、指定された要件通りか ・個々のユーザ認証場面に適用されているユーザ認証が必要とする運用（証明書やパスワードの更新等）は適切に行われいるか

表 9-7　ユーザ認証の適用状況に関する監査内容例

項番	監査項目	監査の内容等
5	ユーザ認証に用いる機能の実装状況	・ユーザ認証に用いる技術およびその機能選択は妥当か ・その実装の正確性は確認されているか （実装すべき場所に正確に実装されているか） ・運用環境の変更時における対応機能の実装の見直しは行われているか ・必要な運用環境の整備状況についてのチェックは適切に行われているか
6	パスワード等の認証用情報の取扱い状況	・認証用情報の設定についての監督、指導は適切におこなわれているか ・サイト運営上における認証用情報の取扱いは妥当か、またそのことは適切に管理されているか ・システム上での認証用情報の保護管理は妥当か（注１） ・認証情報を含む電子媒体や印刷物の取扱いは妥当か ・またそのことは適切に管理されているか（注１） ・認証情報を含む通信データの保護は適切に行われているか（注２）
7	ユーザ認証事故への備えの状況	・関係事故に備えた保全要領が、ユーザ認証の実態に照らして適切に決められているか ・必要な保全処理は適切に行われているか ・ユーザ認証事故に対する対処要領は適切に決められているか ・監査期間中におけるユーザ認証事故に対する処理は妥当であったか
8	適切なユーザ認証の実現に向けた諸施策のシステム運用への反映状況	・ユーザ認証にかかる施策は運用規定、運用マニュアルに適切に反映されているか ・これらの運用は、日々の運用において確実に実行されているか、また、そのことは管理されているか ・ユーザ認証に関する運用の適切な実行を実現するための工夫は十分か
9	関係者におけるユーザ認証の厳格な運用についての認識	・ユーザ認証適用基準についての認識は十分か ・個々の処理に適用されている認証方式についての理解は十分か ・ユーザ認証の適切な運用についての自己の責任についての認識は十分か

（注１）セキュリティ管理情報の保護管理でも指定
（注２）通信にかかるリスク対策でも指定

10 セキュアなシステム構成の確保

第3～9 章に述べてきた各脅威に対応するセキュリティ対策でも、必要とする機能の的確な実装についての要求がなされている。ここでは、システムの構築に関する者に、セキュアなシステムを構築するために求められるマネジメントを纏めたものである。

10.1 必要な施策の一覧

図 10-1 に、セキュアなシステムの構築実現のための施策の組立てを示す。

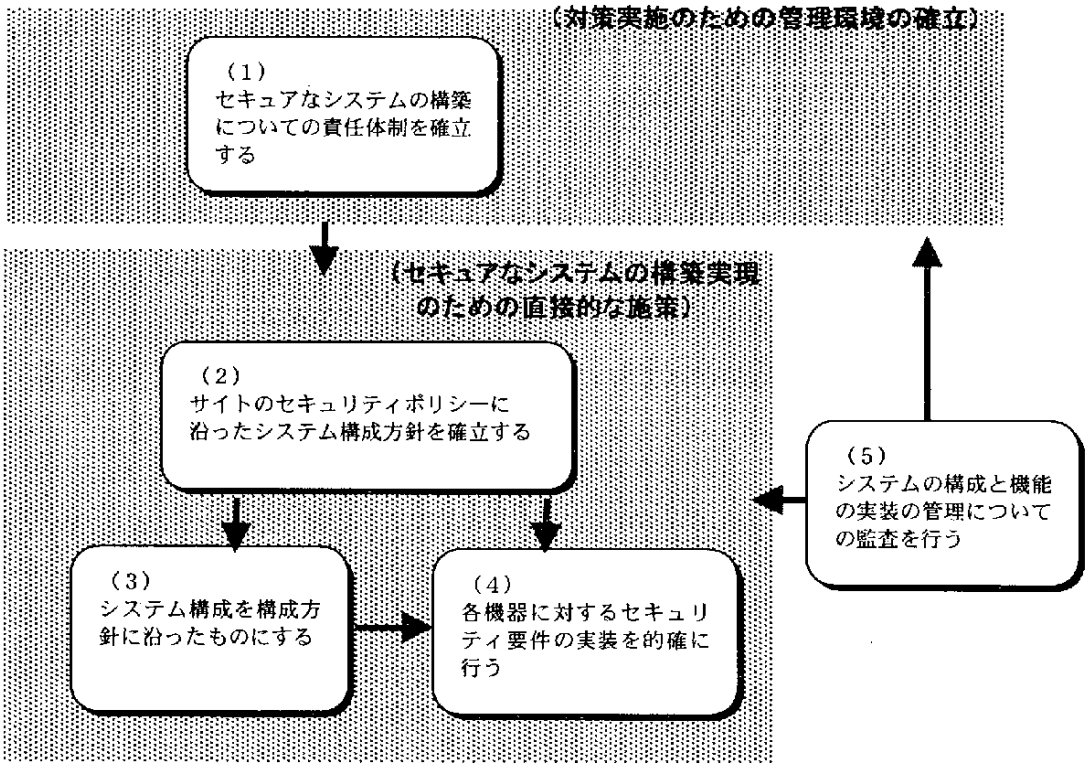


図 10-1 セキュアなシステムの構築実現のための施策の組立て

また、表 10-1 に各施策における実施事項の一覧を示す。

表 10-1　セキュアなシステム構築のための具体的実施事項

施策名	具体的実施事項
(1) セキュアなシステムの構築についての責任体制を確立する	① システム構成の管理についての責任体制の明確化 ② システム構成の管理にかかわる関係者間の連絡体制の確立
(2) サイトのセキュリティポリシーに沿ったシステム構成方針を確立する	① システム構成の組立てについての基本的な考え方の確立 ② システム構成のフレームワークの確立 ③ システム構成方針の関係者への周知
(3) システムの構成を構成方針に沿ったものにする	① 構成方針に沿ったシステム構成の設計 ② 設計を的確に反映したシステム構成の構築 ③ サイトの運用形態やセキュリティ対策の変更のシステム構成への適切な反映 ④ システム構成に関するドキュメントの整備
(4) 各機器に対するセキュリティ要件の実装を的確に行う	① セキュリティサービス機能の的確な実装 ② 各機器に対するセキュリティ要件の的確な実装 ③ サイトの運用形態やセキュリティ対策の変更の適切な反映 ④ 各機器におけるセキュリティ関係機能の実装に関するドキュメントの整備
(5) システム構成と機能の実装の管理についての監査を行う	① システム構成と各機器へのセキュリティ対策にかかわる機能の実装に関する管理の実施状況についての定期的な監査の実施 ② 監査実施要領の確立 ③ 監査指摘事項に対するフォローの実施

10.2 個別具対策

(1) セキュアなシステムの構築についての責任体制を確立する

【主旨】

システムの構成や各機能の実装を、サイトのセキュリティ対策が求めるものにするためには、

- サイトにおけるさまざまなセキュリティ対策に照らした適切なシステムの構成方針の確立
- システムの構成への構成方針の的確な反映
- セキュリティ対策にかかる諸施策の各機器における関係機能の実装への反映と
- システム構成や各機器における諸機能の実装への運用環境の変化の的確な反映

を指導、管理する責任体制の確立が必要となる。

このためには、セキュアなシステムの構築にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) セキュアなシステムの構築についての責任体制の明確化

システムの構成や関係機能の実装が適切に行われるためには、システムの構築およびその維持管理ににかかる者の責任分担を明確にしておくことが必要となる。システムの構成管理に関する責任体制として、その責任を明確にしておくべきこととしては以下があげられる。

- システムの構成管理に関する責任者とその責任
- システムの構成管理担当者の責任
- システム開発責任者のセキュアなシステム構成の構築にかかる責任
- システム運用責任者のシステム構成の管理にかかる責任

(2) システム構成の管理にかかわる関係者間の連絡体制の確立

システムの構成管理に、セキュリティ対策面から定められていることが的確に反映されるようにするためには、システムの構築とその維持にかかわる者の間での連携も重要となる。

関係者間での連絡対策の確立については、2.2 節参照。

また、以下にあげる者は、システムの構築及びその維持管理には直接かかわらないものの、この連絡体制に組込むべきである。

- システムへの不正アクセス対策責任者
- セキュリティホール対策責任者
- ウイルス対策責任者
- セキュリティ管理情報の保護管理責任者
- ユーザデータの保護管理責任者
- 通信にかかるリスク対策責任者

【対策実施上のポイント】

(1) システムの構成およびその維持管理にかかわる者の責任区分

表 10-2 に、システムの構成およびその維持管理にかかわる者の責任区分の定義例を示す。

(2) サイトの運営形態や体制等の変更に際しては、この責任体制についての見直しも行うこと。

表 10-2　システムの構成管理にかかる責任者のタスク

責任区分	タスク
システムの構成管理責任者	・システム構成指針の妥当性の維持 ・システムの構成、各機器における機能の実装状況の管理 ・的確なシステム構成と実装の実現についての管理と指導
システムの構成管理担当者	・システムの構成方針に沿ったシステム構成の実現 ・各機器における的確な機能の指定、各種設定 ・システム構成、各機器における機能の実装状況の把握 ・運用環境の変更時の、システムの構成や各機器の機能の実装への反映 ・ウイルス検査のパターンファイル等のセキュリティ機能の実行に必要な環境の整備
システム開発責任者	・独自開発システムにおける各種セキュリティ要件の的確な組込み －設計の妥当性の確認 －漏れの的確な実装の確認 －対応機能の実装状況の正確な把握
システム運用責任者	・システム運用におけるセキュリティ機能の動作環境の整備 ・システム構成や各機器における実装の変更の運用への反映

(2) サイトのセキュリティポリシーに沿ったシステム構成方針を確立する

【主旨】

セキュアなシステムを構築する第一歩は、システム構成をサイトのセキュリティポリシーにあったものにすることである。システム構成の検討にあたっては、セキュリティ面から、以下についての考え方が確立していなければならない。

- 考えられる脅威に対し、どこにどのような対策を配置するか
- 問題が生じても、被害を最小限に押さえるためにはどうすればよいか

これらは、システムの構成を決めたり、各機器におけるセキュリティ対応機能の実装を検討する時のベースとなるものである。

セキュリティ面からのサイトシステム構成の妥当性は、サイトにおけるセキュリティ対策の巧拙に直結する。サイトシステムの構成を、サイトにおけるさまざまなセキュリティ対策を反映した適切なものにするためには、まず、セキュリティ対策面からのシステム構成方針を確立しておくことが必要となる。

セキュリティ面からのシステム構成方針として検討しなければならない事項としては、以下があげられる。

- 構成の組立てについての基本的な考え方
- 各機能のサイト内ネットワーク上での配置
- 各機器におけるサイトセキュリティ確保のための機能分担
- これらを反映したネットワーク構成のフレームワーク

【具体的な実施事項】

(1) システム構成の組立てについての基本的な考え方の確立

サイトのネットワーク構成と、各機器の機能の分担、およびサイトのセキュリティ確保のための機能の分担を決めるための考え方を示すもので、システムのネットワーク構成や各機器への機能の配置等は、この考え方に基づいて行われなければならない。

このシステム構成についての基本的な考え方として明確にすべきこととしては、以下があげられる。

- ゾーン分割の考え方

  外部接続ゾーン、DMZ(非武装ゾーン)、内部ゾーン等、セキュリティ対策面からのサイトのネットワーク構成上のゾーン分割を行い、各ゾーンのセキュリティ対策面での性格や、ネットワーク的なアクセス制限等で示す各ゾーンを定義する。

- ネットワーク上の各機器の配置に対する考え方

  ファイアウォールや各種サーバ等の機器を、どのゾーンにどのように配置するかについての考え方を定義する。

- セキュリティサービス機能の配置についての考え方

  アクセス制限や、アクセス監視、ウイルス検査等、サイトのセキュリティ確保のための機能をネットワーク上にどのように配置するかについての考え方を明確にする。

このシステム構成にの組立てについての考え方は、サイトのセキュリティ確保のための諸施策を反映したものでなければならない。

(2) システム構成のフレームワークの確立

実際にシステムを構築するためのシステム構成のフレームワーク設計を、システム構成の基本的な考え方に沿って適切に行う。

この設計においては、以下の点が明確にされていなければならない。

- サイトのネットワーク構成
- サイトのネットワーク構成上における各機器の配置(接続図)
- 各接続機器への機能配置
  - 当該機器に配置する本来機能
  - 当該機器に格納するDB等で示す収容するファイル
  - 当該機器がサポートするサイトのセキュリティ確保のための機能
- 各構成機器に求められるセキュリティ要件
  - アクセス制限等の当該機器に求められるセキュリティ対策

(3) システム構成方針の関係者への周知

システムの構成や各機器のおけるセキュリティにかかわる機能の実装が的確に行われるようにするには、このシステム構成方針を、文書化するとともに、システムの構築およびシステムの維持管理にかかわる者によく周知させていなければならない。

【実施上のポイント】

(1) セキュリティ面からのサイトのシステム構成の検討における主要検討事項

サイトのシステム構成を組立てるにあたって、セキュリティ面からの構成方針として確立すべき点をあげると、以下のようになる。

特に、システムに組込むセキュリティサービス機能については、全体的に見て確実に、かつ効率的に機能するようにするとともに、それらの実装に漏れが生じにくくするための工夫も加えなければならない。

- ゾーンの分割
- サービスの分散
- 一つのサーバにおける異なるサービスの共存
- 各サービスのネットワーク上での配置
- アクセス制御の分担と配置
- アクセス監視機能の分担と配置

- ウイルス対策範囲の明確化と監視機能の分担と配置
- 保護対象情報資産の配置
- 保全データの配置

(2) セキュアなシステム構成検討の視点

サイトシステムをセキュアなものにするために、その構成の検討にあたって考慮すべき事項としては、以下をあげることができる。

- システムに組込むセキュリティサービス機能が、効率的に所期の役割を果たすようにする
- システムに組込むセキュリティサービス機能の実装に漏れを生じにくくする
- セキュリティに関する事故が生じても、その影響は出来るだけ局所化されるようにする
- 性能等、システムの本来機能の提供とのバランスをとる
- システムの構築やその維持管理が複雑になり過ぎないようにする

(3) ゾーン(セグメント)分割についての考え方

一般にサイトのネットワーク構成上におけるセキュリティ面からいうゾーンには、以下のものがある。非武装ゾーンの要否とその使い方については、特に十分な検討を要する。

- 外部接続ゾーン

  外部から直接アクセスすることができる領域で、ファイアウォールの外側に置かれるため、このゾーンに置かれるサーバは不正アクセスの脅威が大きい。

- DMZ(非武装ゾーン)

  外部ゾーンと内部ゾーンの中間に位置付けられるゾーンで、外部に公開する情報を格納するサーバ等を設置する。このゾーンに置かれたサーバは、外部からも内部からもアクセスができるため、公開用サーバの情報の更新等が、内部システム側から可能になる。しかし、サイトの運用上の便利を保持しながら、外部から内部システムへの直接的なアクセスが遮断されるため、内部システムが保護されている。このため、万一、サイトシステムに侵入があっても、その影響を内部システムに及ぼすことを防ぐことができる。

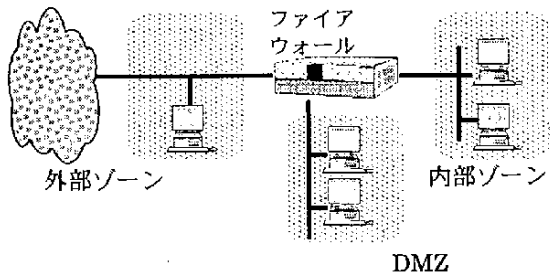
  DMZ は、図 10-2(a)に示すように、DMZ を構成できるファイアウォールを用いるか、(b)に示すように、外部ネットワーク向けのファイアウォールと内部ネットワーク向けファイアウォールを別個に置くことにより設けることができる。

- 内部ゾーン

  外部に公開する必要のないサーバを設置する。ファイアウォールの内側にサーバを設置するため不正アクセスに対する脅威は小さくなる。

これらの考え方を用い、万一、公開サーバが侵入され乗っ取られても、被害が内部ネットワーク全体におよばないよう、また、サーバの配置によっては、被害が他のサーバアプリケーションに及ばないようにすることができる。

（a）DMZ が構成できるファイアウォールを用いた DMZ の設置



（b）ファイアウォールを組合せて構成した DMZ

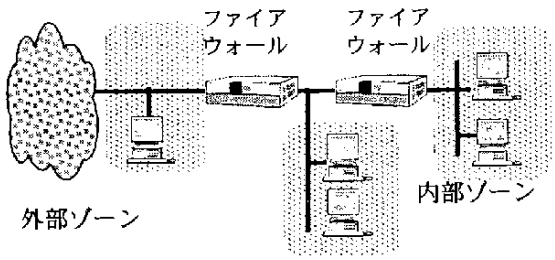


図 10-2　DMZ の構築パターン

ネットワーク上の分割されたゾーンはセキュリティ面で異なる特性を持つ。そのため、ネットワーク上におけるサービスの配置の検討と、ネットワークのゾーン分割の検討は並行して行う必要がある。

(4) サービスの分散についての考え方

Web サーバ、ショッピングや決済をサービスするアプリケーションサーバ、さらに消費者情報等を格納する DB サーバ等を、その負荷分散や事故時における影響範囲の局所化といった観点から、複数の機器に分散して配置することも検討の対象である。

サービスの分散についての検討ポイントをあげると、以下のようになる。

- 分散を検討すべきサービス
  - －分散の目的と期待効果
  - －目的に添った分散のあり方とその有効性
- 分散方式
  - －分散のメッシュ
  - －分散処理の方式と、分散されたものの間での連携の方式
- システムの維持管理等システム運用上の負担
- コスト負担

- ネットワークの負担等のシステムの性能問題

(5) 同一機器への異なるサービスの配置についての考え方

コストや運用上の問題から一つの機器にいろいろなサービスを同居させることも多い。一つのサーバへの異なるサービスの配置は、一つのサービスにおけるセキュリティに関係する問題が、そのサービスの特性や問題の内容によっては、同居している他のサービスにもセキュリティ問題を波及させる可能性もある。

できれば異なるサービスは同一機器に配置しないことが望ましいが、システムの構築およびその維持管理の手間、コスト等とのバランスから、どうしても一つの機器に複数のサービスを同居させなければならない場合は、運用面でのカバーも含め、他への影響をなくすためのシステム運用上の配慮について十分に検討を行うことが必要である。

以下のサービスについては、できれば同一機器に配置しないことが望ましい。

- DNS サーバ
- Web サーバ
- メールサーバ
- ftp サーバ

(6) ネットワーク上へのサービスの配置についてのポイント

システムに組込む各種のサービスをどのゾーンへどう配置(接続)するかを決めるものであり、その検討にあたって配慮すべきこととしては、以下をあげることができる。

- 当該サービスに求められるアクセス制限
- 異なるサービスとの同一機器上での共存の可否と、共存が必要な場合の条件
- 被害の発生等に備えた分散配置の要否と、分散が必要な場合の分散の方法

(7) アクセス制限の配置と機能分担についてのポイント

サイトにおける各サーバへのアクセス制御は、ファイアウォールのアクセス制御機能や各機器におけるアクセス制御機能を用いて行われる。個々の機能の使用上の不備や、機能間の連携の不備により、アクセス制御に漏れがないよう、その配置と機能分担については十分な検討と点検が必要となる。

アクセス制御機能の配置と機能の分担に関し、特に検討すべき点としては、以下をあげることができる。

- ファイアウォールを複数用いる場合の役割分担
- ファイアウォールと各サーバのアクセス制御機能間の役割分担と連携

(8) アクセス監視機能の配置と機能分担について

アクセス監視機能についても、アクセス監視機能の配置と、アクセス監視をサポートしている機器間での機能の分担が、適切に行われていなければならない。

この点に関し、検討すべき事項としては、以下をあげることができる。

- アクセス監視の対象範囲
  - 全てのアクセスを監視にするのか、特定対象だけの監視にするのか

- 監視装置等監視サービスの機能と各サーバ、各サービスが独自に行う監視機能との役割分担

(9) ウイルス対策範囲の明確化と監視機能の配置と機能分担について

ウイルス対策を行うシステム構成上の範囲を明確にする。ウイルス監視機能は、ウイルス対策の対象とする範囲に対して、最適な位置に配置する。また、ウイルス監視機能についても、そのサポートしている機能間での機能の分担が適切に行われていなければならない。

ウイルス監視機能の配置と機能の分担に関し、特に検討すべき点としては、以下をあげることができる。

- 全体監視にするか特定対象だけの部分監視にするか
- 監視装置等監視サービスの機能と各サーバ、各サービスが独自に行う監視機能との役割分担

(10) 保護対象の情報資産の配置についての考え方

セキュリティ管理情報やユーザデータ等の保護対象とすべき情報資産のシステム構成上の配置については、特に慎重な検討を必要とする。

保護対象の情報資産については、情報ごとに個別にアクセス制限が行われているはずであるが、収容されているサーバ自体が攻撃を受けるとその影響を受けることも考えられるため、ネットワーク的に見てアクセスが制限されている位置に配置すべきである。

また、その保護が特に重要なものについては、他とは隔離されたサーバへの配置も検討すべきである。

保護対象情報資産のシステム構成上での配置は、その情報の保護の重要度により決められるものであるが、その配置に関し、検討すべき点とは以下のようになる。

- 配置ゾーン
- 外部から直接的なアクセスを排除する多重配置
- 当該サーバへの外部からのアクセスと、当該サーバから内部サーバへのアクセスのタイプを別々に分離することにより、外部から内部サーバへの直接アクセスを防止する。
- 他のサービス、情報資産との分離
- サイトのネットワーク上で配置する位置の限定

特に、外部から直接アクセスが可能なサーバへの保護対象情報の配置は危険である。

(11) 保全データの配置

セキュリティにかかる事故に備えたシステムの保全は、脅威に対応して検討されるが、システム構成の検討にあたっては、これらの保全処置がサイト全体として適切に行われるように配慮しなければならない。

検討すべき事項としては、以下があげられる。

- サイト全体としての保全ファイルの構成
- 保全ファイルの配置

【実施例】

(1) ファイアウォールの設置形態

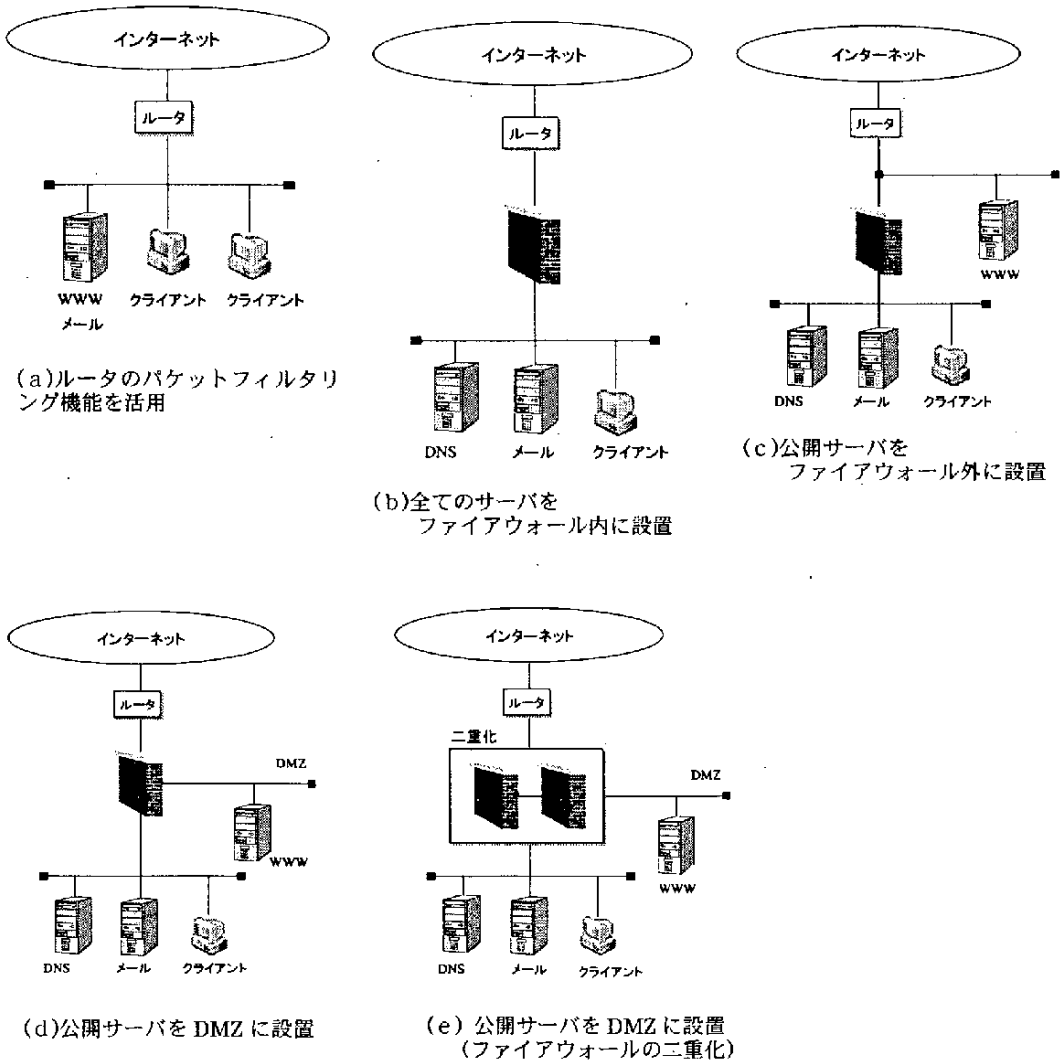


図 10-3 ファイアウォールの設置形態

図 10-3 に、サイトのネットワーク構成における典型的なファイアウォールの設置形態を示す。それぞれの形態の特徴は、以下の通り。

① ファイアウォールを導入せず、ルータのパケットフィルタリング機能を活用(図a)

コストが安くてすむ反面、ファイアウォールを設置するケースに比較して、細かなアクセス制御が困難である。しかしルータの備えている機能がサイトが必要とするセキュリティ機能をカバーしていれば運用上支障はないと考えられる。

② すべてのサーバをファイアウォールの内側に設置(図b)

DMZ を設置する場合に比較して、公開サーバに侵入され、乗っ取られた場合に被害が社内システム全体に及ぶ危険性が高くなる。提供するサービスの種類が多くなると(ファイアウォールを通過するサービスが多くなると)それだけ内部に侵入される危険性が増すため、サービスの検討と合わせて、DMZ の設置を検討するべきである。

③ 内部システムをファイアウォールの内側、公開サーバをファイアウォールの外側に設置(図c)

公開サーバが乗っ取られても、内部システムにまで被害が及ぶ危険性が少ない。一方、公開サーバをインターネットに直結するため、公開サーバに十分なセキュリティ対策を施す必要がある。

このような場合、公開サーバが攻撃を受けやすいことを認識し、攻撃された場合問題となるような情報を置かない等の配慮が必要となる。

④ 公開サーバを DMZ(非武装地帯)に設置(図d)

公開サーバが乗っ取られても、内部システムにまで被害が及ぶ危険性が低く、かつ全てのサーバをファイアウォールで防御可能な構成を構築できる。3つのゾーンを管理するため、ファイアウォールの設定・管理が煩雑になるが、通常最も適用されている構成である。

この場合、以下についてのルールも決めておく必要がある。

- インターネットーDMZ 間におけるデータフロー制御ルール
- インターネットー内部ゾーン間におけるデータフロー制御ルール
- DMZ ー 内部ゾーン間におけるデータフロー制御ルール

⑤ ファイアウォールを二重化し、公開サーバを DMZ に設置(図e)

④の特徴に加え、ファイアウォールの信頼性が向上する。ファイアウォールを2台必要とするためコストが大きくなるが、信頼性を重視するバーチャルショップシステムではこの方式の適用も検討すべきである。

(3) システムの構成を構成方針に沿ったものにする

【主旨】

サイトにおけるシステムの構成は、

- サイトシステムとしてのネットワークの接続構成
- ファイアウォールやサーバ等のシステム構成機器のネットワーク上への配置
- サーバ等への各機能やデータベースの配置

からなる。

これらを、先に述べたセキュリティ面から見た構成方針を的確に反映したものにする。

【具体的な実施事項】

(1) 構成方針に沿ったシステム構成の設計

構成方針に従い、

- サイトシステムとしてのネットワークの接続構成
- ファイアウォールやサーバ等のシステム構成機器のネットワーク上への配置
- サーバ等への各機能やデータベースの配置

を決める。

(2) 設計を的確に反映したシステム構成の構築

サイトのシステム構成は、設計通りに構築されていなければならない。特に、セキュリティ面からの要件は、すべて満足されていることが確認されなければならない。

(3) サイトの運営形態やセキュリティ対策の変更のシステム構成への適切な反映

サイトの運営形態に

- セキュリティ対策の方式の変更
- システム構成の変更

等が生じた場合は、セキュリティ確保に関するシステムの構成方針に沿って、サイトのシステム構成におけるセキュリティ面からの見直しを行い、セキュリティレベルの維持のため、必要な場合は、構成の変更を行わなければない。

見直しの範囲としては、以下のものがあげられる。

- ゾーンの分割
- サービスの分散
- 一つのサーバにおける異なるサービスの共存
- 各サービスのネットワーク上での配置
- アクセス制御の分担と配置
- アクセス監視機能の分担と配置
- ウイルス対策範囲の明確化と監視機能の分担と配置

- 保護対象情報資産の配置
- 保全対策

(4) システム構成に関するドキュメンテートの整備

システム構成の妥当性の確認、その的確な実装の確認、問題が生じた場合の調査や対策の実施等のためにも、サイトのシステム構成については、正確なドキュメンテーションが整備されていなければならない。

【対策実施上のポイント】

(1) 運用に適したシステム構成の設計

構成方針に従いネットワークの接続構成、機器のネットワーク上への配置を設計する際に、セキュリティに関する構成方針を満足するだけでなく、運用に適したものにしなければならない。

また、ネットワークの設計や機器の配置を設計する際には、トラフィックを考慮した性能やネットワーク管理についての運用性についても考慮しなければならない。

(2) システム構成の変更時の対処

セキュリティ対策やシステム構成の変更にあたっては、システムの構成設計を見直す必要がある。当初のシステム設計は、システム全体を対象として設計しているため、一部分の変更であっても全体に影響する場合があるため、必ず見直しを実施しなければならない。

(3) システム構成の変更の移行期間における注意事項

運用形態やセキュリティ対策の変更によりシステム構成の変更が必要となった場合には迅速に実施する必要があるが、ある移行期間を設けざるを得ない場合も考えられる。

その場合には、一時的にセキュリティ要件が満たされていない状態になるため、このような移行期間中には特にセキュリティについての監視を十分行い、不正アクセス等の攻撃に備える必要がある。

(4) 各機器に対するセキュリティ要件の実装を的確に行う

【主旨】

セキュリティ対策が適切に決められていても、各機器におけるセキュリティにかかわる機能のインストールや諸設定の登録が的確なものでなければ、定められているセキュリティ対策は機能しない。

このため、システムの構築ならびに維持管理にあたる者は、全ての機器がそれぞれに与えられているセキュリティ要件を常に満足していることを保証しなければならない。

それぞれの機器に求められているセキュリティ要件としては、

- 当該機器に与えられたサイトのセキュリティ確保のためのサービスの完全な提供
- 当該機器に対する不正アクセス対策
- 当該機器に対するセキュリティホール対策
- 当該機器に対するウイルス対策
- 当該機器におけるセキュリティ管理情報の保護管理策
- 当該機器におけるユーザデータの保護管理策
- 当該機器における通信にかかるリスク対策

からなる。これらの詳細については、第3～9章までの該当のセキュリティ対策を参照のこと。

【具体的な実施事項】

(1) セキュリティサービス機能の的確な実装

当該機器が、アクセス管理やアクセス監視機能等を、サイトシステムのセキュリティ確保のためのサービスとして提供している場合、これらは求められていることを満足するものでなければならない。

(2) 各機器に対するセキュリティ要件の的確な実装

サイトの構成要素の一つとしてサイトのネットワークに接続される機器の機能の実装や諸設定の登録は、機器自身のセキュリティ確保のために要求されていることを的確に反映したものでなければならない。

このことは、組込み当初だけでなく、常時、十分な点検が行われなければならない。この点に関する管理のポイントとしては、以下をあげることができる。

- OS 等プラットフォームソフトのバージョンの妥当性
- 管理者権限の適切な設定
- 不要なサービスやコマンドの除去または停止
- アクセス制限の的確な設定
- アクセス制限に用いる情報の的確な設定
- アクセス監視の的確な設定

- 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対応機能の的確な組込みと実装
- セキュリティ管理情報の的確な格納
- ユーザデータの保護管理対応機能の的確な組込みと実装
- ユーザデータの的確な格納
- ユーザ認証機能の的確な組込み
- 通信路上のリスク対策の的確な組込み
- 個別サービスにおけるセキュリティ要件の的確な反映

(3) サイトの運用形態やセキュリティ対策の変更の適切な反映

サイトの運用形態に

- セキュリティ対策の方針の変更
- システム構成の変更

等が生じた場合は、各機器におけるセキュリティ要件の見直しを行い、必要なセキュリティレベルの維持のため、必要な場合は、構成や設定の変更を行わなければない。

見直しの範囲としては、以下のものがあげられる。

- ゾーンの分割
- サービスの分散
- 一つのサーバにおける異なるサービスの共存
- 各サービスのネットワーク上での配置
- アクセス制御の分担と配置
- アクセス監視機能の分担と配置
- ウイルス対策範囲の明確化と監視機能の分担と配置
- 保護対象情報資産の配置
- 保全対策

(4) 各機器におけるセキュリティ関係機能の実装に関するドキュメンテートの整備

各機器におけるセキュリティ関係機能の実装の確認や、問題が生じた場合の調査や対策の実施等のためにも、各機器におけるセキュリティにかかわる機能の実装については、正確なドキュメンテーションが整備されていなければならない。

【対策実施上のポイント】

(1) 個別サービスに固有なセキュリティ要件の反映について

Web サーバやメールサーバ等のネットワークサービスは、その機能実現のための構造的な特性から、セキュリティ面で他とは異なる脆弱性を有する。これらの点をついた攻撃を受けないようにするためには、それぞれにその脆弱性を補う対策の実施が必要となる。

代表的な機器におけるセキュリティ面での配慮については、後述の(参考)を参照のこと。

(5) システム構成と機能の実装の管理についての監査を行う

【主旨】

システム構成や各機器へのセキュリティ対策の実装の不備は、サイトのセキュリティ対策を破綻させることになるため、これらについて見逃しがないようにしなければならない。このためには、システムの構成や各機器へのセキュリティ対策にかかる機能が適切に実装されているかどうかについての管理が、適切に行われている必要がある。

このため、システムの構成や各機器へのセキュリティ対策の実装が適切であり、かつ、それらについての管理が適切に行われているかどうかについてチェックする監査を行うことも必要である。

また、実施したセキュリティ対策にかかわるシステムの構成管理に関する運用についての記録とその保管等のこの監査のための準備を、日常の運用の中に組込んでおくことも必要となる。

(注) 正式な監査という形はとらなくとも、以下に示すような構成管理に関するチェックは、組織的に行われるべきである。

【具体的な実施事項】

(1) システム構成と各機器へのセキュリティ対策にかかわる機能の実装に関する管理の実施状況についての定期的な監査の実施

最低でも年1回は、システム構成と各機器へのセキュリティ対策の実装に関する管理についての監査を行い、以下に示すような事項をチェックする。

- システムの構成管理に関する責任体制とその機能状況
- システム構成方針の妥当性
- システムの構成や各機器に対するセキュリティ対策にかかわる機能の適切な実装に対する管理の実施状況
- システムの構成や各機器に対するセキュリティ対策にかかわる機能の実装の把握
- 運用環境の変更の反映とその管理についての管理状況
- セキュリティ対策基準の変更の反映とその管理の状況

(2) 監査要領の確立

システム構成や各機器へのセキュリティ対策の実装に関する管理の状況についての定期的な監査が、円滑に実施され実効的なものになるようにするためには、この監査についての実施要領が確立されていることが望ましい。

この監査実施要領で規定しておく事項については、1.2.2 節の(4)項を参照。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。

このためには、監査指摘事項に対する改善措置が実際にとられたかどうかについての確認を行うことも必要であり、監査指摘事項についてのフォローの仕組みも、監査要領の中に組込んで

おく必要がある。

【対策実施上のポイント】

(1) 監査内容例

表 10-3 に、システム構成や各機器へのセキュリティ対策の実装に関する管理の状況についての監査において、チェックすべき事項の例を示す。

(2) 監査の報告

監査結果は、システム構成管理責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告されなければならない。

表 10-3 システムの構成と機能の実装についての監査内容例

項番	監査項目	監査の内容
1	システムの構成管理に関する責任体制とその機能状況	・システムの構成管理に関する責任体制は、サイトの運営実態に照らして適切か ・システムの構成管理に関する責任者の自己の責任についての認識のレベルは適切か ・システムの構成管理に関する責任体制は機能しているか
2	システム構成方針の妥当性	・設定されているシステム構成方針は、サイトの運営実態と設定されているセキュリティ対策に照らして適切か
3	システムの構成や各機器に対するセキュリティ対策にかかわる機能の実装に対する管理の実施状況	・システムの構成や各機器に対するセキュリティ対策にかかわる機能の実装時のチェックは適切に行われているか ・システムの構成や各機器に対するセキュリティ対策にかかわる機能の実装についての定期的なチェックは適切に行われているか
4	システムの構成や各機器に対するセキュリティ対策にかかわる機能の実装の把握	・システム構成は最新状態のものが、正確に把握されているか ・各機器に対するセキュリティ対策にかかわる機能の実装は最新状態を反映したものが、正確に把握されているか
5	運用環境の変更の反映とその管理の状況	・運用環境の変更のシステム構成や各機器のセキュリティ対応機能の実装への反映は、適切に管理されているか

表 10-3　システムの構成管理に関する監査内容例

項番	監査項目	監査の内容
6	セキュリティ対策基準の変更の反映とその管理の状況	・セキュリティ対策基準のシステム構成や各機器のセキュリティ対応機能の実装への反映は、適切に管理されているか

(参考1) ファイアウォール構築のポイント

ファイアウォールは、ネットワークの中にあってデータの流れをルールに従って中継するものであり、ネットワークとのアクセス管理の中核をなすものであり、一般に次の機能を提供している。

- アクセス制御機能

  ファイアウォールの内側と外側との間で転送されるデータ、プロトコル、利用ユーザ・ホストの制限を実施する

- 認証機能

  サービスの利用を許可する前に、ユーザやIPアドレス等でアクセスを認証する。

- 監査機能

  ファイアウォールを通過しようとするパケットの情報を監視するとともに、アクセスログとして蓄積する。また、指定された監視条件に合ったパケットが見つかったら、不審パケットとして、接続を拒否したり、その情報を警告メッセージとして管理者に通知する。

- 暗号化(VPN)機能

  オプション的機能で、VPN モジュールをアドオンすることにより暗号化通信を可能にする。

ファイアウォールをサイトのセキュリティ対策の要として機能させるためには、サイトのセキュリティ対策が求めるところに合ったファイアウォールの選択を行い、サイトのネットワーク上の適切な場所に、適切な設定のもとで実装しなければならない。

また、ファイアウォールを選定する場合、以下の事項を明確にした上で選定しなければならない。

- ファイアウォールに求める機能範囲

  －アクセス制御機能に対する要求

  －詳細ログ採取機能に対する要求

  －暗号化機能に対する要求

  －監査機能に対する要求

- 運用するアプリケーションとの整合性

  導入予定のファイアウォールが、現在使用しているまたは使用予定のアプリケーションに対応しているかどうかの確認

- システム構成との整合性

  システムへの不正アクセスの防止のための諸施策が求めていることに対応でき、システムの構成にフィットできるかどうかの確認

【ファイアウォール構築上の留意事項】

(1) アクセス制限に関する要件の検討

サイトにおけるシステムへのアクセス制限基準に基づくネットワークとの接続ルールに従って、ファイアウォールに対する要件を明確化し、構築の考え方をドキュメント化する。使用するファイアウォール製品の仕様に従って、構築時に設定する項目等を決定していく。また、ファイアウォールを設置する位置や、運用におけるセキュリティ面での考え方も、この段階で明確にする。

この要件定義での主な指定事項は、以下のようなものとなる。

- 許可する送信元アドレス
- 許可する宛先アドレス
- 許可する利用者
- 許可するサービス
- システム管理者
- ルールに応じたパケット受信時の動作

(2) 侵入監視要件の検討

侵入監視を行う場合、監視条件として、以下を検討しなければならない。

- 監視の対象とする不審アクセスの定義
- 接続の拒否を行う条件
- 不審アクセスの報告要領

(3) ファイアウォールの選定

ファイアウォールの選定にあたって考慮すべきこととして、以下をあげることができる。

- 外部公開用サーバやウイルスチェックサーバの設置にあたっての DMZ の要否
- 外部からのアクセスだけでなく、内部からのアクセスについての制御の要否
- アクセス制限要件、侵入監視要件の実現等、サイトにおけるシステムへの不正アクセス対策がファイアウォールに求める機能
- サイトのシステム構成との整合性

(4) ファイアウォールの設定

事前に作成したファイアウォール構築の考え方のドキュメントに従って設定作業を行う。

ファイアウォールの構築では以下の項目について設定が必要となる。

- ネットワーク設定

  ルーティング情報、IP アドレス情報、アドレス変換等
- 各種ログファイルディレクトリ情報設定
- ルールベース

これらはいずれも、サイトにおけるアクセス制限基準に基づく個々のアクセス制限要件に沿って決められる。

(5) 構築したファイアウォールの実装の確認

ファイアウォールの実装については、テストも入れた厳格なチェックを行う。

【ファイアウォールの運用に欠かしてはならないこと】

ファイアウォールが所期の機能を果たすためには、その適切な運用が不可欠となる。ファイアウォールの運用に関してのチェックポイントをあげると、以下のようになる。

(1) メンテナンスは適切に実施されているか

- 適切なメンテナンスの実施の有無(実施サイクル)
- メンテナンス後の機能検査実施の有無(実施の有無とそのチェック内容)

(2) メンテナンス管理は適切に行われているか

- メンテナンス基準は確立しているか
- メンテナンスは適切な管理の下に行われているか
  - 実施管理、実施の権限のある者で行われているか
  - 実施は適切な手順に基づいているか

(3) 権限の設定が適切に行われているか

(4) 適切なアクセス制限が行われているか

- 管理者権限(root 等)によるリモートアクセスは禁止されているか

(5) 不正アクセス監視(日常のログ監査、セキュリティアラート調査)

各種ログ、システムから通知されるセキュリティアラートを監視することにより、不正アクセスの事実を確認する。

このためには、ログの取得とその管理を適切に行なわなければならない。常に、以下についての確認を行うこと。

- アクセスログは適切に取得されているか
- 取得ログについて二重化や改ざん防止の保護は行っているか

(6) 定期的なバックアップの取得

定期的なフルバックアップの採取、差分バックアップの採取を実施する。これは障害時およびセキュリティ上の問題(破壊等)があった場合に必要となる。

(7) 最新のセキュリティ情報の収集

ファイアウォールソフトウェアの最新バージョンに関する、セキュリティホールに関する情報を監視し、必要であれば最新バージョンへの入替え等必要な処置を検討する。

(8) ファイアウォール自体に対するセキュリティ対策の実施

ファイアウォール自体が、外部からの攻撃を許したり、サイト内の他のサーバや他社システムの攻撃の踏台にされたりするようなことがあってはならない。

このためには、ファイアウォール自身に対し以下のようなセキュリティ対策を怠ってはならない。

- 不要なデフオルトアカウントの削除
- 不要なデーモン(ネットワークサービス)の削除または停止処理
- 定期的なセキュリティホール検査の実施等のセキュリティホール対策の実施
- ウイルス対策の実施

- 他のサーバソフトの同居の排除

【堅固なファイアウォールシステムの構築について】

外部からの攻撃に対してサイトをさらに堅固なものにする方法として、以下のようなファイアウォールシステムの構成も検討の対象となる。

(1) ファイアウォールの複数構成

異なるファイアウォールを直列的に設置することにより、簡単には侵入できないようなシステムの構成を検討する。

(2) ルータとの連携

必要であれば、ルータと連携することにより、不正アクセスを検知した場合、自動的にコネクションを切断したり、パケットを破棄したりするシステム構成の検討も行う。

(3) 他のセキュリティ製品との連携

他のセキュリティ製品との連携により、トータル的なセキュリティの強化実現を検討する。

【参考】

ファイアウォールはその実現方式によって、表 10-4 に示すように 2 つのタイプに分類することができる。

表 10-4 ファイアウォールのタイプ

項番	実現方式	機能概要と特徴
1	パケットフィルタリング	IP アドレス、ポート番号によるフィルタリングによりアクセス制御を実現する。 ＜特徴＞ ・ アプリケーションに依存しない ・ 優れたパフォーマンスを持つ
2	アプリケーションゲートウェイ	アプリケーションのコネクションをアプリケーション層で相互接続するとともに、データ転送に関するアクセス制御を実現する。 ＜特徴＞ ・ 詳細なログ情報を採取できる ・ プロキシ型ファイアウォール

(参考2) DNS サーバ構築のポイント

インターネットで提供される各種サービスへのアクセスには DNS(Domain Name System)サーバの設置が必要となる。

DNS サーバを設置するにあたっては、DNS 情報が不正利用されないようにするためのセキュリティ対策が必要となる。

この時、考慮すべき脅威としては以下があげられる。

- named サーバプログラムを利用した攻撃
- バージョンの古い BIND を利用した攻撃
- ゾーン転送、DNS 情報の流れを利用した情報の不正取得

【システム構築時のセキュリティ対策】

(1) 外部公開用 DNS サーバの DMZ への設置

外部に公開する DNS サーバは、ファイアウォールの許可するサービスとして外部ネットワークからの参照を許す DMZ に設置する。

DMZ を構成できないファイアウォールを使用する場合は、外部公開用 DNS サーバはルータとファイアウォールの間の外部セグメントに設置する。この場合、ルータのフィルタリング機能を使用し、セキュリティを強化する必要がある。

(2) DNS 情報公開ルールの確立

ファイアウォールを設置する場合に、ファイアウォールの外部と内部に対する DNS 情報の公開についてのルールの確立が必要がある。

この時の一般的な考え方は、以下の通り。

- ファイアウォールの内側に対する DNS 情報の外部への隠蔽

  ファイアウォールの内側に対する DNS 情報については、外部ネットワークから参照できないようにしなければならない。
- 外部公開 DNS サーバと内部用 DNS サーバの別機器への配置

  外部公開用 DNS サーバと内部用 DNS サーバを別個に設ける場合は、物理的に異なるマシン上に配置することが望ましい。もし、同一機器上に配置する場合は、外部ネットワークから内部 DNS サーバの情報を参照できないように設定し、その設定を確認することが必要である。
- DNS サーバはファイアウォールとは別機器上に配置する

  推奨するシステム構成としては、ファイアウォールとは別マシンに配置することが望ましい。同一マシンへの配置はセキュリティホールの存在等を考慮した場合、リスクが高い。

(3) 外部公開用 DNS サーバへのゾーン転送の禁止

外部公開用 DNS サーバと内部用 DNS の間でのゾーン転送を許可してはならない。

(4) DNS サーバ自体のセキュリティ対策の徹底

DNS サーバが、外部からの攻撃を許したり、サイト内の他のサーバや他サイト攻撃の踏台にされたりするようなことがあってはならない。

このためには、DNS サーバに対し、**"(参考7)の各サーバに共通な運用上の留意事項"**に示すようなセキュリティ対策を怠ってはならない。

また、DNS にあっては、ゾーン間転送を許可する条件の明確化と、必要な場合におけるゾーン間転送については、特に留意すること。

【実施例】

サイトのネットワーク構成における、DNS サーバの一般的な設置位置を、図 10-4 に示す。

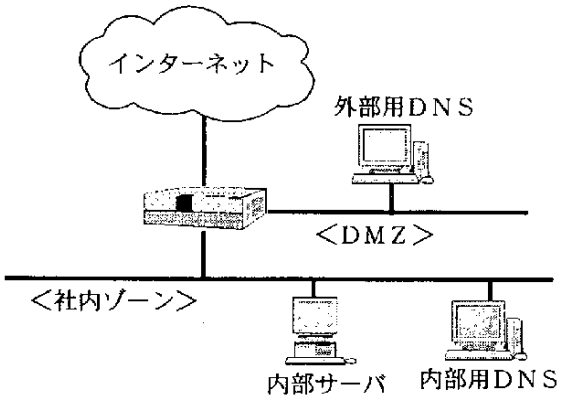


図 10-4 DNS サーバの設置位置

【参考情報】

(1) SecureDNS

TSIG、DNSSEC 等 DNS サーバ間、DNS サーバークライアント間通信に認証や暗号化を適用する SecureDNS 機能がある。将来的には、これら機能の使用も重要になるかもしれない。

(2) DynamicDNS

DHCP 等との連携により、DNS 情報をダイナミックに更新する DynamicDNS サーバ機能がある。DNS 情報の自動更新機能の悪用により、不正情報をエントリされないような配慮が必要となる。

(参考3) Web サーバ構築のポイント

Web サーバ上では以下の脅威が存在する。

- CGI を利用したサーバ内のコマンド実行による攻撃
- CGI を利用したバッファオーバフローをついた攻撃

Web サーバを外部からのこのような攻撃から保護するためには、適切な動作環境の構築および適切な運用が必要となってくる。

【構築上の留意事項】

(1) 外部公開用 Web サーバの DMZ への設置

外部公開用として設置する Web サーバは DMZ に設置する。こうことにより、不正アクセスにより Web サーバに侵入されたとしても、ファイアウォールの内側のネットワークにまで侵入されることはなく、被害を最小限に抑えることができる。

DMZ を設けない場合は、外部公開用 Web サーバはルータとファイアウォールの間の外部ゾーンに配置する。この場合、ルータのフィルタリング機能を使用し、セキュリティの強化を図る必要がある。

(2) CGI プログラムの管理

CGI プログラムの実行権を認識しておく必要がある。CGI の実装については、組み込むスクリプトは全てソースレベルで理解し、管理することが基本であり、把握できない内容を含むプログラムは登録しないことが必要である。またその利用は、常に監視・制御されるべきであり、チェックされない入力を受信しない、外部から動作する問題のあるプログラムはすべて、メタキャラクタを含まない形にするなどの措置を必要とする。これらのことは CGI の使用上のルールとして文書化され、関係者に配布、徹底されることが望ましい。

(3) コンテンツファイルへのアクセス制限の実施

公開するコンテンツファイルへのアクセスはサーバ管理者にのみ許可することとする。また、ファイルごとに管理者が異なる場合には、ファイル単位でのパーミッションを設定するべきである。

(4) HTTP メソッドの制限

基本的には GET のみ許可する設定とする。PUT メソッドが必要な場合には、アクセス権限者を明確にするとともにアクセス制御について管理する必要がある。

(5) ファイル・転送データの暗号化

Web サーバにおいては、外部のネットワークおよび内部ネットワークにある他のサーバとの間で、ファイルやデータのやり取りが行われる。このファイルやデータの転送においても、重要なデータ、機密データに関しては、

- 暗号化による秘匿性の確保
- 改ざん検知

等の通信にかかるリスク対策を考えるべきである。

通信にかかるリスク対策については、第 8 章参照。

(6) ファイルの暗号化

Web サーバへの侵入による Web サーバ管理下のファイルへの不正アクセスに備えて、使用ファイルについて必要に応じた暗号化も検討対象の一つである。

(7) ディレクトリの自動インデックス機能の使用の禁止

ディレクトリの自動インデックス機能は、当該ディレクトリ内のファイル構造を公開することで、ファイルの所有者、パーミッション情報の漏洩につながる可能性があるため、使用しないことが望ましい。

ダウンロードファイルの一覧の表示を行う場合でも、Web サーバの機能を利用して、ディレクトリ単位でのリスト表示を行う等して、自動インデックス機能の使用は避ける工夫が必要となる。

(8) Web サーバの管理機能へのアクセス制限の実施

Web サーバの管理機能へアクセスについては、適切なアクセス制限の実施が必要である。

Web サーバの管理機能へのアクセスの制限の設定においては、以下が重要な要素となる。

- ドメイン名称
- IP アドレス
- ユーザ認証

(9) コンテンツ書換え監視の実施

コンテンツに書かれている価格情報等の改ざんを発見するために、ファイルの更新日時等を自動的にチェック・監視する監視用ソフトウェアの適用も検討すべきことの一つである。

(10) Web サーバ自体のセキュリティ対策の実施

Web サーバが、外部からの攻撃を許したり、サイト内の他のサーバや他サイト攻撃の踏台されたりするようなことがあってはならない。

このためには、Web サーバに対し、**"(参考7)の各サーバに共通な運用上の留意事項"**に示すようなセキュリティ対策を怠ってはならない。

また、Web にあっては、

- 不要な CGI プログラムの削除

については、特に徹底を期すること。

(11) Web サーバ上で使用を制限したいサービス

- DNS、SMTP 等
- finger、systat 等・・・・マシン情報を盗まれて侵入の足掛かりになる
- chargen、echo 等・・・・攻撃に利用される
- TFTP、Berkely コマンド(rlogin、rsh、rsist 等)
  ・・・・認証機能がない、または認証機能が貧弱
- telnet、ftp等・・・・・・・・・パスワードがそのままネットワーク上を流れる

【実施例】

サイトのネットワーク構成における、Web サーバの一般的な設置位置を図 10-5 に示す。

- 公開用 Web サーバの DMZ への設置
- 内部用（イントラネット用）Web サーバの内部ゾーンへの設置

を原則とする。

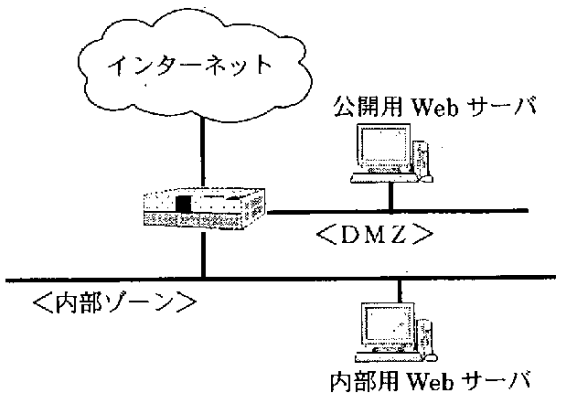


図 10-5 Web サーバの設置位置

(参考4) Mail サーバ構築のポイント

メールシステムには以下の脅威が存在する。

- 添付ファイルに潜むウイルス
- SPAM メール

メールサーバをこれらの攻撃から保護するためには、適切な動作環境の構築と運用が必要となる。

【構築時の留意事項】

(1) メールアカウントを持つ(外部公開)メールサーバの DMZ への設置

実際のユーザのメールアカウントを登録し、メールボックスを持つメールサーバは、DMZ に設置すべきである。

(2) ウイルスチェックサーバの DMZ への設置

外部ネットワークからのウイルスの侵入を防止するため、また、内部ネットワークからのウイルスの外部への流出を防止するため、ウイルスチェック専用のサーバを DMZ に設置し、チェックするようにする。

このウイルスチェックサーバはメール転送サーバと連携して動作するようにルーティング情報を設定する。

(3) smtp サーバに対する SPAM メール対策の実施

- 中継サーバからのメール受信の拒否

  ORBS(Open Relay Blocking System)を利用する。SPAM メールの受信をメールサーバにおいて拒否するための対策である。しかし、個々のメールに関して、それが SPAM であるか否かの判断は難しく、上記 ORBS の利用はそのひとつの解決策ではあるが、すべての SPAM メールを拒否できるわけではない。SPAM メール受信被害に関しては、根本的な解決は無いのが実情である。

- メール中継の制限

  SPAM による脅威のもうひとつの側面は、自サイトのメールサーバを不正に経由され、SPAM メールを他へ配送することにより、SPAM メールの配送元とされてしまう、いわゆる踏台攻撃である。

  この攻撃に対しては、メールサーバの中継機能に制限をかけ、宛先が自サイトになっているメールと、送信元が自サイトであるメールのみを処理する設定を行うことが有効である。

- メール中継不要なメールサーバではメール中継機能を停止する

  メールを中継することがないとわかっているメールサーバでは、メールの中継機能そのものを停止する。

- SMTP サーバへの送信におけるユーザ認証の実施

  メールサーバによっては、各ユーザがメーラ上で作成したメールメッセージを送信する前に POP でのユーザ認証を行うように設定できるものがある。これを設定することにより正式なアカウントを持たないものからメールサーバを悪用されることを防止できる。

(4) 一般公開用メールサーバと内部者用メールサーバの分離

消費者等不特定多数をサービス対象としたメールは、ウイルス他の攻撃の糸口になることが多いことから、外部公開用メールサーバは社内用メールサーバと分離することが望ましい。

(5) POP 認証の強化

POP サーバアクセス時の認証にワンタイム・パスワードを用いる APOP プロトコルの利用によりメールサーバのアクセス管理が強化される。特にモバイルユーザが外部からメールサーバにアクセスする場合等に有効となる。ただし、この場合メーラも APOP 対応のものを使用する。

(6) Mail サーバ自体のセキュリティ対策

Mail サーバが、外部からの攻撃を許したり、サイト内の他のサーバや他社システムの攻撃の踏台されたりするようなことがあってはならない。

このためには、Mail サーバに対し、**(参考7)の各サーバに共通な運用上の留意事項**に示すようなセキュリティ対策を怠ってはならない。

(7) メールサーバの SPAM メールへの対応

- SPAM メールを外部から不当に中継されないために、sendmail8.9 以降を使用、それ以前のバージョンでは OpenRelay を No に設定する。または qmail を使用する
- SPAM メールを受取らないようにするために、SPAM メール発信元情報を入手(http://www.orbs.org/ などから入手できる)し、メールを受信しないように設定を行なう

【実施例】

サイトのネットワーク構成における、一般的な Mail サーバの設置位置を、図 10-6 に示す。

- メールボックスを持たない転送用メールボックスの DMZ への設置
- ユーザのメールボックスを持つ社内メールサーバの内部ゾーンへの設置

がポイント。

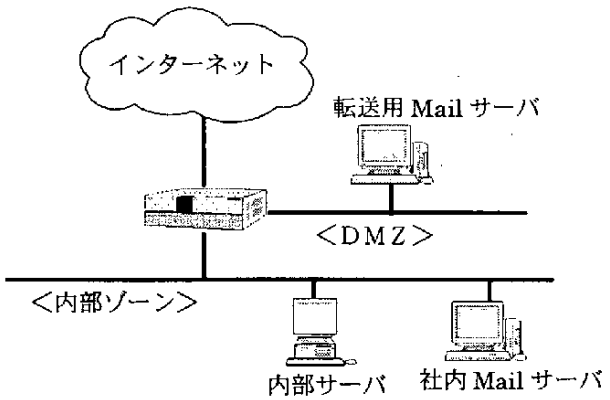


図 10-6　Mailサーバの設置位置

(参考5) DB サーバ、アプリケーションサーバ構築のポイント

インターネット上でバーチャルショップを運営する場合には、商品情報、顧客情報等のデータベースやサービスを提供するアプリケーションサーバの設置が必要となる。小規模なシステムの場合、DB サーバとアプリケーションサーバを同一のサーバ上で稼働させることが普通である。一方大規模なシステムでは専用の DB サーバを設置することも行われる。

このようなサーバについても、他のインターネット上のサービスを提供するサーバと同様に、セキュリティに関して適切な運用を行う必要がある。

【構築上の留意事項】

(1) DB サーバやアプリケーションサーバサーバの内部ネットワークへの設置

DB サーバやアプリケーションサーバは外部ネットワークから直接アクセスできないように、内部ネットワークに設置すること。

公開用 Web サーバとの通信がある場合には、外部からのアクセス制限とは別に、ファイアウォールにて、通信プロトコルや IP アドレスを見たアクセスを制限する必要がある。

(2) 必要に応じたファイルや転送データの暗号化

重要データ、機密データに関しては暗号化した上でデータ転送するような仕掛け、機構を導入する。

(3) DB サーバ、アプリケーションサーバ自体のセキュリティ対策

DB サーバ、アプリケーションサーバが、外部からの攻撃を許したり、サイト内の他のサーバや他社システムの攻撃の踏台されたりするようなことがあってはならない。

このためには、DB サーバ、アプリケーションサーバに対し、**"(参考7)の各サーバに共通な運用上の留意事項"**に示すようなセキュリティ対策を怠ってはならない。

【実施例】

サイトのネットワーク構成における、DB サーバやアプリケーションサーバの一般的な設置位置を、図 10-7 に示す。

なお、この図においては、DB サーバは二重化されている。

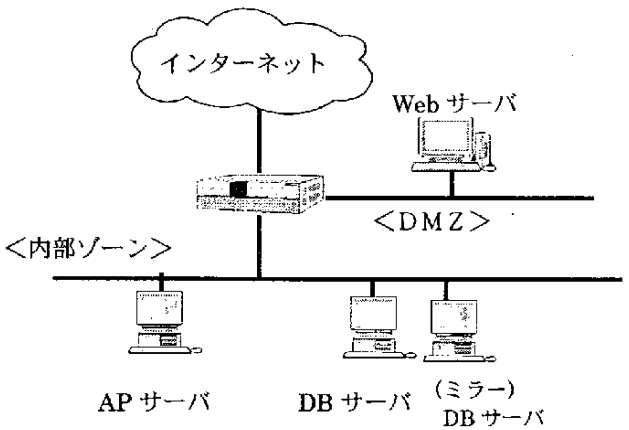


図 10-7　DB サーバやアプリケーションサーバの設置位置

(参考6) ftp サーバ構築のポイント

ネットワークを介して他サイトとファイルの送受信を行う場合に ftp サーバを設置し、ftp サービスを提供することが行われる。ftp サービスは、システムへの侵入やウイルスの侵入の温床ともなるサービスであり、EC サイトでは原則として使用しないことが望ましい。しかし、モール等において出店ショップ側との間で、コンテンツの授受を行うような場合、ftp サービスを使用せざるを得ないこともある。

ftp サービスを用いる場合は、以下の脅威を含めた対策を実施する必要がある。

- ftp サーバ上でのコマンド実行
- 不正なログインの実行
- ファイルパーミッション

【実装上の留意事項】

(1) ftp サービスへのアクセス権限や管理方法の設定

ftp によるサーバへのアクセスは、サイトの管理者、出店者等のサイト運営関係者以外に許可しない等、サイトの運営に直接関係するものにだけ許し、それ以外の者の使用を許してはならない。

このためには、アクセスについて識別と認証を厳格に行う必要がある。

また、この場合、ユーザ ID、パスワードが盗聴されないような仕組みを工夫しなければならない。

(2) ファイルや転送データの暗号化について

重要データ、機密データに関しては暗号化した上でデータ転送するような仕組みを導入する。

(3) バーチャルショップ利用者からのftpへのアクセスの排除

(4) ftp サーバ自体のセキュリティ対策

ftp サーバが、外部からの攻撃を許したり、サイト内の他のサーバや他社システムの攻撃の踏台されたりするようなことがあってはならない。

このためには、ftp サーバに対し、"(参考7)の各サーバに共通な運用上の留意事項"に示すようなセキュリティ対策を怠ってはならない。

【実施例】

サイトのネットワーク構成における、ftp サーバの一般的な設置位置を、図 10-8 に示す。

ftp サーバは、DMZ に設置することを原則とする。

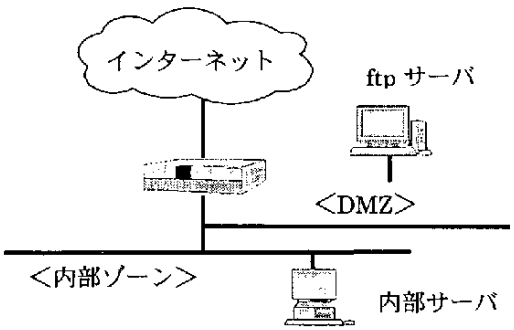


図 10-8 ftp サーバの設置位置

(参考7) 各サーバに共通な運用上の留意事項

サイトに置かれたサーバは、外部からの攻撃を許したり、サイト内の他のサーバや他社システムの攻撃の踏台にされたりするようなことがあってはならない。

ここでは、システムの構成管理の立場から、各サーバに求められるセキュリティ対策をまとめてみた。

(1) 不要なデフォルトアカウントの削除

(2) 不要なデーモン(ネットワークサービス)の削除または起動の抑止

(3) 管理理機能へのアクセス制限の徹底

- アカウントの確認、パスワードの定期的な更新

  各アカウントに対し、パスワードが適正に設定されているかどうかの確認は重要である。また、アクセス権限者(アカウント)は、必要最小限にし、パスワードも定期的に更新すべきである。

(4) 最新バージョンのプログラムの使用

セキュリティ上の弱点を含むバージョンのプログラムの使用は避けるべきで、運用上可能な限り最新バージョンへの入替えを励行すべきである。

このためには、最新のセキュリティ情報についての監視が必要がある。

また、メンテナンス作業は、実施権限のある管理者のもとで、ドキュメント化された適切な手順にもとづいて実施するようにする。

(5) セキュリティホール対策の徹底

(6) ウイルス対策の徹底

(7) 侵入監視の実施

システムの運用ログ、アクセスログを検証し、不正アクセスの痕跡がないかを、常にチェック、監視する必要がある。この確認のため、アクセスログは適切に採取されるべきであり、ログに対する改ざん防止や二重化を実施することが望ましい。

(8) バックアップ取得の管理

定期的なフルバックアップの採取、差分バックアップの採取を実施する。これらはサーバ上のソフツェアやデータが改ざんされたり破壊されたりするようなセキュリティ事故への対処で必要となる。

(9) セキュリティ事故に対する対処方法の確立

万が一、サーバ内に侵入された場合の対処を、迅速かつ適切に行うためには、対処方法を明確にしておく必要がある。

11 セキュアなシステム運用の確保

セキュリティ対策にかかる諸施策でシステムの運用に求めていることが、サイトにおける日々のシステム運用に的確に反映されるようにするためには、システムの運用サイドからも適切な管理が必要となる。

本章では、これまで脅威対応に述べてきたセキュリティ対策に関し、システムの運用サイドに求められう管理を整理したものである。

11.1 必要な施策の一覧

図 11-1 に、セキュアなシステム運用の実現のための施策の組立てを示す。

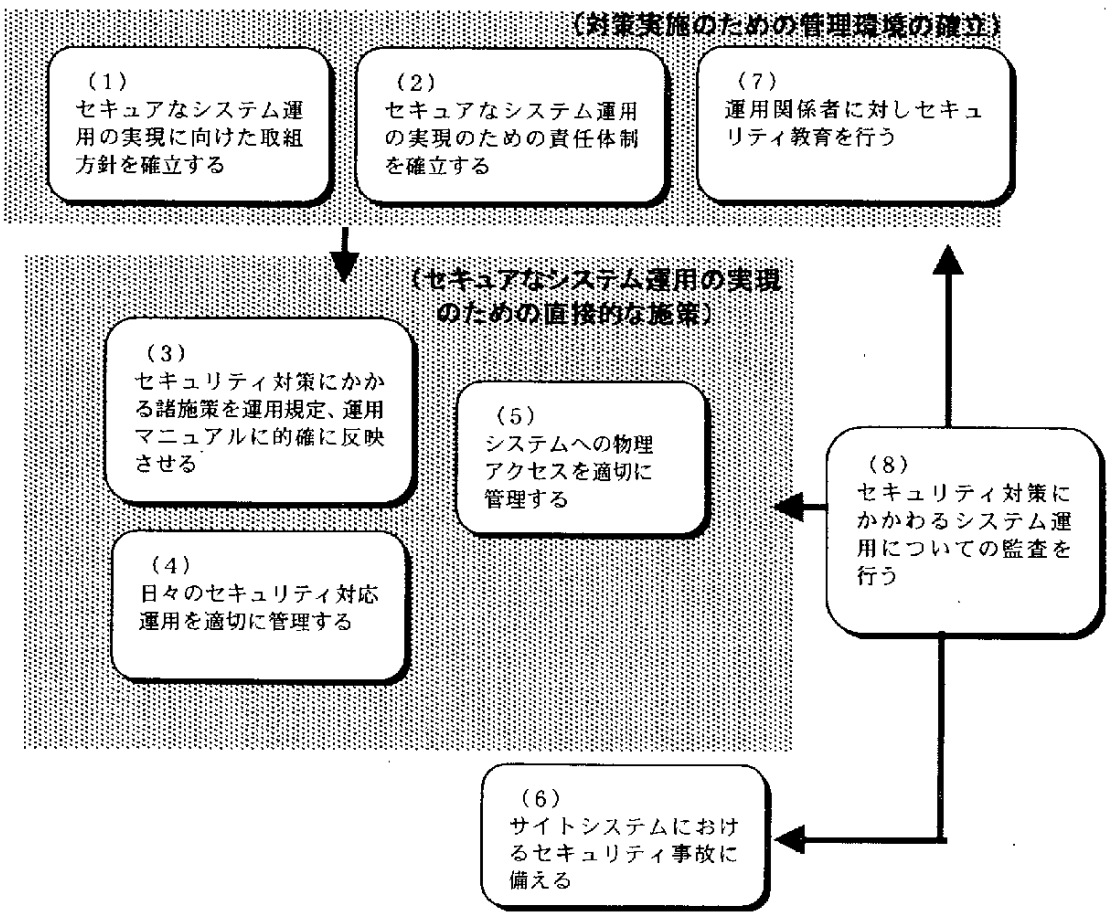


図 11-1 セキュアな運用の実現のための施策の組立て

また、表 11-1 に各施策における実施事項の一覧を示す。

表 11-1　セキュアな運用実現のための具体的実施事項

施策名	具体的実施事項
(1) セキュアなシステム運用の実現に向けた取組方針を確立する	① セキュアなシステム運用の実現に向けた運用サイドの責任の明示とシステム運営上のテーマの確立 ② 適用範囲の明確化 ③ セキュアな運用の実現に向けた施策の組立ての明確化 ④ セキュアな運用の実現に向けた取組方針の関係者への周知
(2) セキュアなシステム運用のための責任体制を確立する	① セキュアなシステム運用についての責任体制の明確化 ② セキュアな運用の確保に関係する者の間での連携体制の構築
(3) セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに的確に反映させる	① セキュリティ対策にかかる諸施策の運用規定、運用マニュアルへの反映手順の確立 ② セキュリティ対策の新規策定や変更の運用規定、運用マニュアルへの的確な反映 ③ 運用環境の変更に対する運用規定や運用マニュアルの見直しの実施 ④ 運用規定や運用マニュアルの定期的な点検の実施
(4) 日々のセキュリティ対応運用を適切に管理する	① セキュリティ対策に関連して定期的に実施すべき運用処理の定期スケジュール化 ② 日々の運用におけるセキュリティ対策に関係する運用処理の実行チェックリストの作成と、チェックリストに基づく実行確認の励行 ③ 日々の運用におけるセキュリティ関連処理の記録の作成と保管
(5) システムへの物理アクセスを適切に管理する	① システムへの物理アクセス管理基準の確立 ② システムへの物理アクセス管理に必要な環境の整備 ③ システムへの物理アクセス管理基準の運用規定への反映 ④ 管理基準に準じたシステムへの物理アクセス管理の実施とその実行管理の実施
(6) サイトシステムにおけるセキュリティ事故に備える	① サイト全体としてのシステム保全要領の確立 ② サイト全体に対するシステム保全要領の運用規定、運用マニュアルへの反映 ③ システムの保全要領に従った保全処理の実施 ④ 事故発生時の処理を円滑かつ的確に行うための環境の整備
(7) 運用関係者に対しセキュリティ教育を行う	① 運用関係者に対するセキュリティ対策教育の実施 ② 教育カリキュラムの確立 ③ 運用関係者に対するセキュリティ教育に用いるテキストの整備

表 11-1 セキュアな運用実現のための具体的実施事項

施策名	具体的実施事項
(8) セキュリティ対策にかかわるシステム運用についての監査を行う	① セキュリティ対策ににかかるシステム運用の実施状況についての定期的な監査の実施 ② システム運用についての監査要領の整備 ③ 監査指摘事項に対するフォローの実施

11.2 個別具対策

(1) セキュアなシステム運用の実現に向けた取組方針を確立する

【主旨】

セキュアなシステム運用の実現に組織的に取組むには、サイトのセキュリティ確保についての運用サイドの責任を明らかにするとともに、運用チームとして、これにどのように取組むかを示す取組方針を確立し、これらをシステムの運用関係者に周知させておくことが必要となる。

【具体的な実施事項】

(1) セキュアな運用の実現に向けた運用サイドの責任の明示とシステム運用上のテーマの確立

システムの運用サイドには、サイトにおけるセキュリティ確保に関し、

- セキュリティ確保のための諸施策がシステムの運用に求めていることの完全な実施
- 運用そのものをサイトのセキュリティの脅威にしないこと

に責任を持たなければならない。

セキュアな運用の実現に向けたシステム運用上のテーマとしては、以下のようなものが上げられる。

- セキュリティ確保のための諸施策の運用規定への完全な反映
- 運用規定に基づいたセキュアな運用の実践
- サイトシステムに脅威となるような運用の不手際の排除
- 他システムへの脅威を生じるような運用上の不手際の排除
- 運用上知り得た保護対象情報の保護の徹底

(2) 適用範囲の明確化

セキュアな運用の実現に向けた諸施策の適用範囲として、以下のようなことを明確にする。

- サイトのシステム構成上の対象となる領域および対象サーバ等の機器
- 対象とする組織
- 対象とする業務、作業

(3) セキュアな運用の実現に向けた施策の組立ての明確化

セキュアな運用の確保をどのように実現するかを示す。

本ガイドラインにおけるセキュアな運用実現のための施策の組立てについては、11.1 節参照。

(4) セキュアな運用の実現に向けた取組方針の関係者への周知

作成されたセキュアな運用の実現に向けた取組方針は、システム運用関係者に周知されなければならない。このためには、

- 取組方針の掲示や配布
- 関係者間での取組方針の定期的な再確認

等が必要となる。

(2) セキュアなシステム運用の実現のための責任体制を確立する

【主旨】

サイト運営におけるセキュリティ対策がシステム運用に求めていることは多いが、これらが、日々のシステム運用において確実に実行されるようにするためには、

- セキュリティ対策が運用に求めていることをの日々のシステム運用への的確な反映
- セキュアなシステム運用を実現するに必要な運用環境の整備
- 運用要員におけるセキュアなシステム運用実現に必要なセキュリティについての理解と、必要なスキルの確保

を指導、管理する責任体制の確立が必要となる。

このためには、セキュアな運用の実現にかかわる関係者の責任の明確化と、関係者間での連携体制の確立が必要となる。

【具体的な実施事項】

(1) セキュアなシステム運用の確保についての責任体制の明確化

セキュアなシステム運用の実現のための責任体制について、明確にしておくべきこととしては、以下があげられる。

- システム運用におけるセキュリティ責任者とその責任
- システム運用におけるセキュリティ管理者
- システム(構成)管理者

(2) セキュアな運用の確保に関係する者の間での連絡体制の確立

セキュアな運用の確保するためには、関係者間での連携が必要となる。このため、システムの運用に関係する責任者間での連絡体制の構築も重要となる。

【対策実施上のポイント】

(1) システムの運用にかかる責任者のタスク

表 11-2 に、システムの運用にかかる責任者のタスクを示す。

(2) 業務の運営形態やサイトの運営形態や体制等の変更に際しては、この責任体制についての見直しも行うこと。

表 11-2　システムの運用にかかる責任者のタスク

責任区分	タスク
システム運用における セキュリティ責任者	・運用関係者におけるセキュリティへの取組方針の確立と関係者への周知 ・セキュアな運用環境の整備の監督、指導 －運用規定、運用マニュアルにおける諸セキュリティ対策の反映の確認 －日々のセキュリティ運用の妥当性についてのチェックの監督、指導 －事故への備えについての監督、指導
システム運用における セキュリティ管理者	・運用関係者に対するセキュリティへの取組みについての指導 ・セキュアな運用環境の整備の実行管理 －運用規定、運用マニュアルにおける諸セキュリティ対策の反映 －日々のセキュリティ運用の妥当性についてのチェック －事故への備えの実施監督 ・セキュリティ対策の変更の運用への反映 ・システムの構成、セキュリティ対応機能の変更等の運用への反映
システム(構成)管理者	・システムの構成や各機器における機能の実装の管理 ・システム構成や各機器のセキュリティ関係機能の変更管理

(3) セキュリティ対策にかかる諸施策を運用規定、運用マニュアルに的確に反映させる

【主旨】

脅威対応に検討されてきたセキュリティ確保のための施策において、日々の運用に委ねられていることが、運用規定や、運用マニュアルに的確に反映されていないと、実際の運用から漏れる可能性があり、セキュリティ確保に破綻をきたす恐れが生じる。

(注) セキュリティ対策にかかる諸施策の運用規定、運用マニュアルへの適切な反映については、これまで述べてきたそれぞれの脅威に対応したセキュリティ対策においても求められているが、ここでは、これらセキュリティ対策にかかる諸施策が、確実に運用規定や運用マニュアルに反映している様にすることを、運用者側の立場から保証しようとするものである。

【具体的な実施事項】

(1) セキュリティ対策にかかる諸施策の運用規定、運用マニュアルへの反映手順の確立

セキュリティ対策にかかる諸施策の運用規定、運用マニュアルへの反映を確実なものにするためには、これらについての手順を確立しておくことが必要となる。

この手順で明確にしておくべきこととしては、以下があげられる。

- 運用規定、運用マニュアルへのセキュリティ対策の反映を行うべき場合
- 運用規定、運用マニュアルにおける関係する記述内容の起草、レビュー、承認要領
- 運用規定、運用マニュアルにおける関係する記述についての関係セキュリティ対策責任者との連携
- 運用規定、運用マニュアル変更時における変更内容の関係者への周知手順
- 変更履歴の作製と保管

(2) セキュリティ対策の新規策定や変更の運用規定、運用マニュアルへの的確な反映

以下に示すような場合においては、規定された手順に従い、新しく策定されたセキュリティ対策がシステム運用に求めていることを、運用規定、運用マニュアルに的確に反映するような修正を行わなければならない。

運用責任者ならびに当該対策責任者は、セキュリティ対策の新規策定あるいは変更に伴い必要となるシステム運用の変更が、運用規定、運用マニュアルに的確に反映されたことを確認しなければならない。

- セキュリティ対策にかかる諸施策の新規制定時
- セキュリティ対策にかかる諸施策の変更時

(3) 運用環境の変更に対する運用規定や運用マニュアルの見直しの実施

運用環境の変更に伴い、システム運用にセキュリティ対策にかかる処理が変更される場合は、運用規定、運用マニュアルにおけるセキュリティ対策関連事項について、その見直しを行い、必要な変更を行うこと。

(4) 運用規定、運用マニュアルの定期的な点検の実施

セキュリティ対策にかかる諸施策の変更や、セキュリティ環境、運用環境の変更等の運用規定や運用マニュアルへの反映に漏れが生じたまま放置されないようにするため、運用規定や運用マニュアルにおけるセキュリティ対応事項について、以下の点からの点検を定期的に行うことが望ましい。

- セキュリティ対策にかかる諸施策との整合性
- システム構成との整合性
- システムの運用との整合性

【対策実施上のポイント】

(1) チェックリストの作成による管理

以下に示す脅威対応のセキュリティ対策における諸施策が、的確に運用規定や運用マニュアルに反映されていることが、確認できるよう、それぞれの施策の中に、運用規定や、運用マニュアルへの反映を裏付けるチェックリストを作成、管理するよう規定しておくことも望ましい。

- システムへの侵入対策
- セキュリティホール対策
- コンピュータウイルス対策
- セキュリティ管理情報の保護管理策
- ユーザ情報の保護管理策
- 通信路上のリスク対策
- ユーザ認証の適用

(4) 日々のセキュリティ対応運用を適切に管理する

【主旨】

日々のシステム運用においてセキュリティ確保のために定められていることが的確に行われ、必要な処理の実行に不備がでないようにするためには、サイトの運営形態にあったシステム運用対する管理方法に工夫を行い、これらを組込んだ、日々のセキュリティ対策にかかるシステム運用に対する管理の仕組みを確立することも必要となる。

【具体的な実施事項】

(1) セキュリティ対策に関連して定期的に実施すべき運用処理の定期スケジュール化

脅威対応のセキュリティ対策の中で示されているスケジュール化すべきセキュリティ対策にかかわる運用事項をまとめ、実運用にあった形で再編成をし、これをスケジュール化する。

このスケジュールは、セキュリティ対策にかかる運用の原点になるものであるため、漏れがないことの確認と、セキュリティ対策やシステムの運用環境の変更が的確に反映されるようになっていなければならない。

(2) 日々の運用におけるセキュリティ対策に関係する運用処理の実行チェックリストの作成と実行確認の励行

日々の運用におけるセキュリティ対策にかかる運用が漏れなく的確に行われるようにするためには、

- 個別処理に対する運用チェックリストの作成
- チェックリストに基づく実行確認と処理結果の確認

を励行することが望ましい。

(3) 日々の運用におけるセキュリティ関係処理の記録の作成と保管

日々の運用における問題点の分析や、事故が発生した場合の調査等の必要性から、セキュリティ対策にかかわる運用上の処理は、規程に従って記録、保管しなければならない。

この点ついても、その実施状況の管理、指導が必要である。

【対策実施上のポイント】

(1) 特にその実行管理が必要なシステム運用におけるセキュリティ対応処理

特にその実行管理が必要なシステム運用におけるセキュリティ対応処理としては、以下があげられる。

- セキュリティ管理情報の更新
- セキュリティ管理情報ファイルに対する再編成等の運用操作
- 警告に対する処理、ログの分析、ログファイルのアーカイブ等システムへの侵入監視にか

かわる運用処理

- 警告に対する処理、監視データの分析、監視ファイルのアーカイブ等、ウイルス監視に関する運用処理
- 保全にかかわる処理

（注）構成の変更やセキュリティ関係機能の変更や、セキュリティホール検査やウイルス検査のためのパターンファイルの更新等は、セキュアなシステムの構築の範疇とする。

(2) セキュリティトラブルについての報告と記録について

日々の運用におけるセキュリティ対策対応処理のチェックリストに基づき、異常が発見された場合は、運用責任者に報告しなければならない。

(5) システムへの物理アクセスを適切に管理する

【主旨】

システムへの物理アクセスとは、EC サイトの運営にかかわるソフトウェアや情報がインストールされている機器に直接触れて利用することを言う。サイトのセキュリティ確保に向けてさまざまな施策が実施されていても、サイトシステムが物理的な観点から、不正に利用されるような環境に置かれていては、サイトのセキュリティは危ういと考えなければならない。 また、機器や記録媒体の盗難にも留意しなければならない。機器や記録媒体の盗難は、それらの中に記録されているソフトウェアやセキュリティ管理情報、ユーザ情報の漏洩につながるため、サイトシステムのセキュリティには大きな脅威となる。

実施しているセキュリティ対策を十分に活かすためにも、サイトシステムは正規の運用者のみが利用できるような環境に置き、適切な管理下に置くことが必要である。

このため、サイトシステムを構成する機器や記録媒体等を、可能な限り関係者以外から隔離することを図るとともに、これらへの物理的なアクセスが限定されるような管理の仕組みを作ることが必要である。

【具体的な実施事項】

(1) システムへの物理アクセス管理基準の確立

システムに対するアクセス管理を的確に行うためには、サイトシステムの適用業務、規模、運用形態に応じた適切なアクセス管理基準が確立していなければならない。

システムへの物理的アクセス管理基準で規定しておくべき事項としては、以下があげられる。

- 保護対象機器等の範囲
- 管理区域区分
  - アクセス権限が異なる区域
    (例:特定の運用管理者のみアクセスが許される領域、運用関係者のみ等)
- 管理区域毎のアクセス管理方法
  - 施錠隔離またはパーティションレベルの隔離
  - 電子ロック等の装置による管理、警備員による管理、入退室管理簿といった記録による管理と自主規制の組合わせ

(2) システムへの物理アクセスの管理に必要な環境の整備

システムへの物理アクセスの管理の実施に必要な環境は、採用した管理手段によって異なってくるが、検討対象としては、一般に以下のようなものがあげられる。

① 必要な設備

管理区域を物理的に隔離する場合は、以下の設備が必要となる。

- 特定管理対象区域であることを示すパーティション化

- 管理区域の隔離および入退室を制限する装置

② その他

- 入退室管理に用いられるIDカード等
- 警備員を用いる場合における、警備員およびその作業環境

(3) システムへの物理アクセス管理基準の運用規定への反映

システムへの物理アクセス管理基準は、運用規定に的確に反映されていなければならない。

(4) 基準に従ったシステムへの物理アクセスの管理の実施とその実行管理

システムに対するアクセスについての管理は、規定があってもその履行はルーズになりがちであるため、(1)で定めた基準に従い励行されるよう、その実行管理も的確に行わなければならない。

このためには、その実行管理に対するチェックリストの作成等の工夫も必要となる。

【対策実施上のポイント】

(1) システムへの物理アクセスの管理についての考え方

システムへの物理アクセスの管理は、システムの規模や取扱っている業務の性格やシステムの規模等により、異なったものとなる。採用する管理手段は、その主旨に照らし、システムの規模やコスト等を考慮して、システムの運用形態に合ったものにする必要がある。

ただし、規模の大小に関わらず、何らかの管理は必須であり、部外者がシステムに近づけないようにする規制は重要である。

できれば、専用マシン室などを設けて、専用マシン室等への入退室を管理する。

この場合の管理の方法としては、

- 警備員をおき入室許可証を確認、入退室の記録する
- 入退室カード(磁気カード、ICカード)による入退室管理
- 必要に応じた所持品の検査

システムを物理的に完全に隔離できない場合でも、システムが置かれている区域に部外者が簡単に入室することができないようにしておく必要がある。入室権限者の指定、入室権限者の認識方法についての工夫に加え、部外者が入室した場合にすぐに発見できるようにする工夫や、入室権限者が不在の場合は施錠する等の工夫も必要となる。また、システムを物理的に完全に隔離できない場合、システムをセキュリティ管理者に隣接させ、正規利用者以外が利用できないように監視するようにすることも、一つの工夫である。

(注) 以上で述べたシステムへの物理アクセスの管理の対象としてのシステムには、記録媒体も含む。記録媒体に対しても、物理アクセスの管理についての十分な配慮が必要である。

(6) サイトシステムにおけるセキュリティ事故に備える

【主旨】

個々の脅威に対応したセキュリティ対策において、対象とした脅威による事故や被害が発生した時の備えとして、

- 保全要件の設定と保全要件に従った保全の実行
- 事故発生時の処理要領の確立
- 事故発生時の対応を円滑に行うための環境の整備

が要求されている。

これらを確実にかつ効率よく実行するためには、運用チームは、それぞれの施策テーマの要求で重複しているところを纏めるとともに、全体の運用スケジュールの中に上手に組込むための工夫が必要となる。

【具体的な実施事項】

(1) サイト全体としてのシステムの保全要領の確立

個別セキュリティ対策からの要求を統合し、サイト全体としての保全要領を確立する。

サイト全体としてのシステムの保全要領として明確にすべき事項としては、以下があげられる。

- 保全対象システム資産
- 保全対象システム資産ごとのバックアップの取得ルール
- バックアップの保管ルール
- 保全処理についての記録のルール

また、この要領は、サイトの運営形態やシステムの構成および個別セキュリティ対策に変更が加えられた時、それらの変更が的確に反映するようになっていなければならない。

(2) サイト全体に対するシステム保全要領の運用規定、運用マニュアルへの反映

定められたシステム保全要領は、的確に運用規定や運用マニュアルに反映しなければならない。

また、システムの保全要領の変更も、運用規定や運用マニュアルに的確に反映されていなければならない。

(3) システムの保全要領に従った保全処理の実施

システムの保全要領に基づく、運用規定や運用マニュアルに従い、日々の運用において、バックアップの取得やその保管といった、所定の保全処理を的確に実行する。

これらの処理についても、その実行管理は的確に行われなければならない。

(4) 事故発生時の処理を円滑かつ的確に行うための環境の整備

事故発生時の対応が円滑にかつ的確に行われるようにするための環境の整備としては、以下のことが必要になる。

① セキュリティ対策テーマ毎に定めているセキュリティ事故への対処要領の集大成

② 想定しているそれぞれの事故への対処に必要な運用についてのマニュアルの集大成

③ 事故発生時の処理に必要なシステム環境の整備

想定しているさまざまなセキュリティ事故への対処に用いるシステムの機能は、何時でも使えるようになっていなければならない。

このためには、事故時の対処に用いる機能に関し、

- 機能の動作確認
- 的確な実装の確認
- 必要な動作環境の整備

等について、定期的な点検が必要となる。

④ 事故発生に備えた復旧訓練等の実施

事故は発生頻度が低いため、事故対応は、運用関係者が不慣れであったり、必要な機能が予定したように機能しなかったりで、円滑に行かないことが多い。

事故対処に慣れることと問題点摘出のため、想定しているそれぞれの事故への対処について、定期的な訓練を行うことが望ましい。

【対策実施上のポイント】

(1) セキュリティに関する事故の被害範囲の調査に必要な情報

サイトシステムにおけるセキュリティに関連する事故の被害範囲の調査に必要な運用サイドの情報としては、以下のようなものがあげられる。

- システムの運用記録(対象機関における実行ジョブとその如けジュール等)
- セキュリティ対策対応運用処理の実行記録
- セキュリティ対策にかかる監視データ等の処理に関する記録

これらは、いずれも運用規定に準じて記録、保管されていなければならない。

(2) 事故調査、復旧訓練の実施サイクルについて

事故調査や事故による被害からの復旧は、日常的な作業ではないため、必要な環境の整備や、対処に必要なスキルの保持等に齟齬をきたし易い。このため、事故調査や復旧訓練は、最小でも年に1回は実施すべきである。

(7) 運用関係者に対しセキュリティ教育を行う

【主旨】

運用関係者において、セキュリティについての意識や理解が不十分であれば、セキュリティ確保のための諸施策が整備され、これらが運用規定や運用マニュアルに的確に反映されていたとしても、その的確な実行は期待できない。

このため、システムの運用関係者に対し、セキュアな運用ができるようにするための必要な教育を実施することが必要となる。

【具体的な実施事項】

(1) 運用関係者に対するサイトのセキュリティ対策教育の実施

① 定期セキュリティ教育の実施

運用関係者に対するセキュリティ教育は、定期的に行わなければならない。

② 必要に応じた運用関係者に対する臨時セキュリティ教育の実施

以下のような場合は、その都度、該当者に対する教育を行う必要がある。

- 異動等により運用にかかわる者に入替えが合った場合
- セキュリ対策にかかる運用に大きな変更が発生した場合
- 運用上でセキュリティに関し問題が生じた場合

(2) 教育カリキュラムの確立

運用関係者に対するセキュリティ教育を効果的に行うためには、サイトの運営実態に応じた、教育科目とその内容、対象者と受講サイクル、実施時期等を定めた教育カリキュラムを、確立しておくことが望ましい。

教育すべき内容としては、以下があげられる。

- サイト運営におけるセキュリティリスクとセキュリティ対応技術の概要
- サイトのセキュリティ対策の概要
- セキュリティ対策にかかる運用規定と日々の運用におけるセキュリティ対応処理
- システム運用にかかるセキュリティ事故事例

この教育内容は、サイトの運営形態やシステム構成、運用形態、及び技術環境の進化を反映した、運用対象システムの実態に合ったものであるよう、適時更新がなされなければならない。

(3) 運用関係者に対するセキュリティ教育に用いるテキストの整備

運用関係者に対するセキュリティ教育をより効果的にするためには、サイトの運営実態に合ったテキストを準備することが望ましい。

また、このテキストも、サイトの運営形態の変更を反映するよう、定期的に見直すことが望ましい。

【対策実施上のポイント】

(1) 運用関係者に対するセキュリティ教育のカリキュラム例

表 11-3 に、運用関係者に対するセキュリティ教育のカリキュラムの一例を示す。

表 11-3 運用関係者に対するセキュリティ教育のカリキュラム例

項番	教育項目	教育対象者	頻度
1	サイト運営におけるセキュリティリスクとセキュリティ対応技術の概要 ・脅威とセキュリティ対策の概要 ・個別セキュリティ対策技術の概要 ・適用新技術の概要	・システム運用関係者の全員	1回／年
2	サイトのセキュリティ対策の概要 ・サイト全体としてのセキュリティへの取組み方針 ・システムへの侵入防止策と対応システム運用 ・セキュリティ対策と対応システム運用 ・ウイルス対策と対応システム運用 ・セキュリティ管理情報の保護管理策と対応システム運用 ・ユーザデータの保護管理策と対応システム運用 ・通信にかかるリスク対策と対応システム運用 ユーザ認証と対応システム運用	・システム運用関係者の全員	1回／年
3	セキュリティ対策にかかる運用規定と日々の運用におけるセキュリティ対応処理 ・サイトのセキュリティ対策にかかわる運用に関する規定 ・セキュリティ対策にかかわる日常運用の実行要領 ・セキュアな運用に関する責任体制 ・運用上の留意事項	・システム運用関係者の全員	2回／年
4	システム運用におけるセキュリティ事故事例 ・セキュアな運用に関する新しい工夫 ・運用上の問題点 ・事故事例	・システム運用関係者の全員	1回／年

(2) 運用関係者については、セキュリティ教育の履修は管理すべきである。

(3) 外部の講習会への参加も、セキュリティ教育の一環として有効である。上手な活用を検討されたい。

(8) セキュリティ対策にかかわるシステム運用についての監査を行う

【主旨】

サイトのセキュリティ確保におけるシステム運用の比重の大きさを考えると、システム運用に問題が発生する前に、問題点を発見し適切な改善策を講じることができるようにしておくことも重要である。

このため、セキュリティ対策にかかる諸施策がシステム運用に求めていることが適切に実行されているかどうかについてチェックを行ない、問題点の摘出と必要な改善の実施の指導を行う、システム運用におけるセキュリティ対策の実施状況についての監査を行うことも必要である。

また日常の運用の中で、実施したセキュリティ対策にかかる運用についての記録の保管等、この監査のための準備を組込んでおくことも必要となる。

(注)正式な監査という形はとらなくとも、以下に示すようなシステム運用におけるセキュリティ対策にかかわる処理の実施状況についてのチェックは、組織的に行なわれるべきである。

【具体的な実施事項】

(1) セキュリティ対策にかかる運用の実施状況についての定期的な監査の実施

最低でも年1回は、日々の運用におけるセキュリティ対策にかかるシステム運用の実施状況についての定期的な監査を行い、以下に示すような事項をチェックする。

- セキュアな運用の実現についての責任体制の整備とその機能状況
- セキュリティ対策にかかる諸施策の運用規定、運用マニュアルへの反映状況
- システム運用におけるセキュリティ対応処理の正確性を期するための工夫の状況
- 情報保護の実施状況
- セキュリティにかかる事故への備え
- セキュリティ対策対応運用の変更の実運用への反映状況
- 運用関係者のセキュリティとセキュリティ対策についての認識

(2) 監査要領の確立

システム構成や各機器へのセキュリティ対策の実装に関する管理の状況についての定期的な監査が、円滑に実施され実効的なものになるようにするためには、この監査についての実施要領が確立されていることが望ましい。

この監査実施要領で規定しておく事項については、1.2.2 節の(4)項を参照。

(3) 監査指摘事項に対するフォローの実施

監査で指摘された問題点については、適切な改善がなされなければならない。

このためには、監査指摘事項に対する改善措置が実際にとられたかどうかについての確認を行うことも必要であり、監査指摘事項についてのフォローの仕組みも、監査要領の中に組込んでおくことも有効である。

【対策実施上のポイント】

(1) 監査内容例

表 11-4 に、日々の運用におけるセキュリティ対策にかかわるシステム運用の実施状況に関する管理の状況についての監査において、チェックすべき事項の例を示す。

(2) 監査の報告

監査結果は、運用責任者の承認を経て、サイトのセキュリティ対策総括責任者に報告されなければならない。

表 11-4 セキュリティ対策にかかわるシステム運用の実施状況に関する監査内容例

項番	監査項目	監査の内容等
1	セキュアな運用の実現についての責任体制の整備状況とその機能状況	・セキュアな運用に確保についての責任体制は、サイトの運営実態に照らして適切か ・セキュアな運用に確保に関する責任者の自己の責任についての認識は十分か ・セキュアな運用に確保についての責任体制は機能しているか
2	セキュリティ対策にかかわる諸施策の運用規定、運用マニュアルへの反映状況	・セキュリティ対策にかかる諸施策の、運用規定、運用マニュアルへ反映状況はチェックされているか ・運用環境の変化やセキュリティ対策の変更が、運用規定や運用マニュアルに的確に反映される仕組みがあり、機能しているか ・運用規定や運用マニュアルの変更は、関係者に徹底されているか
3	システム運用におけるセキュリティ対応処理の正確性を期するための工夫の状況	・セキュリティ対策にかかる定期的な運用は、予めスケジュールされているか ・日々の運用におけるセキュリティ対策に関する作業は、チェックリスト等にに基づき、その実行が管理されているか ・セキュリティにかかる運用上の処理について、適切な記録がなされているか
4	情報保護の実施状況	・保護対象情報を含む印刷物や電子媒体の扱いは適切か ・運用上知り得た保護対象情報は守られているか

表 11-4　セキュリティ対策にかかわるシステム運用の実施状況に関する監査内容例

項番	監査項目	監査の内容等
5	セキュリティにかかる事故への備え	・サイトシステム全体としてのセキュリティ事故に備えた保全は適切に決められているか ・保全処理は、規定通り的確に行われているか ・セキュリティ事故に対する処理要領は整備されているか ・事故処理に必要な処理についての操作マニュアル等は整備されているか ・事故処理に必要なスキルは整備されているか
6	セキュリティ対策対応運用の変更の実運用への反映の状況	・セキュリティ対策の変更や運用環境の変更等でセキュリティ対策にかかわるシステム運用が変更になった場合における、これらの運用規定や運用マニュアルへの変更は適切に行われ、そのかとが管理されているか ・これらの変更は、実際の運用に的確に反映されているか
7	運用関係者のセキュリティとセキュリティ対策についての認識	・運用関係者におけるセキュリティについての認識は十分か ・各運用関係者は、サイトのセキュリティ確保についての自分の責任についての認識は十分か

本ガイドラインの開発に参画したWGメンバー

重松　孝明　電子商取引推進協議会
小川　修身　電子商取引推進協議会

浅野陽一郎　日本信販(株)　管理本部セキュリティ情報部 マネージャ
天野　大緑　富士通(株)ソフトウェア事業本部
アプリケーションサーバソフトウェア事業部 第4開発部 担当部長
一村　政司　(株)日立システムアンドサービス ネットワークビジネス本部
ネットワークソリューション部 主任技師
岩立　誠　(株)三菱総合研究所　応用システム部 研究員
印丸　哲　コンピュータ・アソシエイツ(株)　フィールドサービスグループ
eTrust フィールドサービス プロジェクトマネージャ
大林　素生　川鉄情報システム(株)ネットワークソリューション事業部
EC/EDI 技術部 EC/EDI グループ インターネット EDI チーム 課長
尾崎　孝彦　富士電機情報サービス(株)情報 SI 事業部
データ・ネットワークセンター 情報通信部 課長補佐
佐藤　勝彦　三菱電機(株)情報システム製作所
流通・サービス・通信システム部 EC 事業推進グループ 専任
佐藤　亮介　日本電信電話(株)情報流通プラットフォーム研究所
情報セキュリティプロジェクト
柴田　利幸　(株)日立情報ネットワーク システムインテグレーション本部
セキュリテイソリューション部 ユニットリーダー
東海林 健　(株)アニモ　営業部 主任
末延　忠昭　富士通(株)システムサポート本部 主席部長
高取　敏夫　(財)日本情報処理開発協会 情報セキュリティプロジェクト
中村　信次　(株)日立製作所 公共システム事業部 電子政府プロジェクト部 主任
支倉　健一　日本電気(株)インターネットソフトウェア開発本部
セキュリティ技術センター 主任
平川　真　(株)日立製作所 公共システム事業部 電子政府プロジェクト部 課長
藤本　正代　(株)住友海上リスク総合研究所 調査第四部 副主任研究員
松永　和男　(株)日立製作所 ソフトウェア事業部
ネットワーク管理ソフト設計部 チーフプロジェクトマネージャ
山田　朝彦　(株)東芝e－ソリューション社　SI 技術開発センター　主査

平成１３年３月発行
発行：電子商取引推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel　03-5500-3600
E-mail　info@ecom.or.jp