ECサイト向け
セキュリティ対策ガイドライン

― 解 説 編 ―

第2版

平成１４年３月

電子商取引推進協議会

セキュリティWG

H13－セキュリティWG－3
ECサイト向けセキュリティ対策ガイドライン（解説編）第2版
平成14年3月
電子商取引推進協議会セキュリティWG

はじめに

インターネットのセキュリティについては、いろいろ論じられているが、個々の対策についての専門的なものが多く、バーチャルショップ事業者やECサイトの運用者にとって、なすべきことを判りやすく網羅的に解説したものは見当たらない。このためか、何をすべきかがよく判らないとか、ECサイトのセキュリティは専門的でかつコストのかかるものという思い込み等で、できることも実施せずセキュリティリスクに対し無防備なままにされているサイトも少なくはない。EC サイトの多くが、基本的なセキュリティ対策が実施されたものにするためには、バーチャルショップの運営者等 EC サイトの運営にかかわる者が、容易に理解できかつ着実に実施できるような指針、マニュアルが必要となる。

本ガイドラインはこのような背景から、EC サイトシステムの構築、維持、運用にあたって、実施が求められるセキュリティ対策についての実務的ガイドラインを提案するものである。

目　次

1 概要

1.1 本ガイドラインの目的

本ガイドラインは、EC サイトシステムに求められるセキュリティ対策についての考え方と、実施上での手引きを示すことにより、バーチャルショップ事業者ならびに EC サイトの運営者が、サイトのセキュリティ対策を考えるにあたっての、

- EC サイトにおけるセキュリティ問題についての認識
- セキュリティ対策として、何をどのように行えばいいのか

という疑問に応えようとするものである。

本ガイドラインは、EC サイトにおけるセキュリティについての認識を醸成するとともに、セキュリティ対策の目標とその実施およびその管理についてガイドを与えている。

本ガイドラインを提示することにより、関係者にセキュリティとセキュリティ対策についての理解を深めるとともに、多くの EC サイトのセキュリティレベルの向上を期待するものである。

1.2 本ガイドラインの検討方針

サイトのセキュリティは、なすべきことに対しての充分な理解と、対策実施についての計画とその実行管理の存在の上に、それらの正確な実装および的確な運用があって確保されるものと考える。

したがって、本ガイドラインの開発に当っては、以下を基本方針とした。

(1) セキュリティ対策として認識すべきこと、組織的に計画、管理されるべきことを中心に、基本的に必要な対策を盛込むものとする。(ただし、あまり専門的かつ細かくならないように留意する)

(2) 本ガイドラインにおいては、サイトのセキュリティを堅固なものにするための基本は、

- セキュリティ対策として決めるべきことを適切に定めること
- セキュリティ対策として決めたことの的確な実施を管理すること

にあると考えて、本ガイドラインは、

- 決めるべきこととその考え方の提示
- 決めたことの的確な実施の管理方法

を示すものとする。

したがって、実施するセキュリティ対策のレベルは、個々のサイトの実情に沿って適切に決めるべきものとして、上記の考え方に沿っていれば良しとし、その絶対尺度については特に問題としない。

(3) セキュリティ機能の実装についての記述は、目的ならびに実装上のポイントだけで、実装の詳細については、本ガイドラインの外とする。

(4) 実施を求める個々の対策は、システムの規模にかかわらず、必要でかつ現実的に実施可能なものとする。

(5) 個々の対策については、以下のことを明示する。

- その考え方（対応するリスクと対策についての解説）
- 具体的に実施すべき事項
- 実施上の留意点

(6) セキュリティ対策の実施状況についての自己診断に用いるチェックリストも添付する。

(7) 経営者や管理者層が理解し、計画・管理に実際に使用できるよう、記述は専門的なものに陥らないようにする。

(8) セキュリティに関する国際標準や国内標準と整合性のあるものとする。

1.3 本ガイドラインの構成

本ガイドラインは、図 1-1 に示すような内容で構成されている。

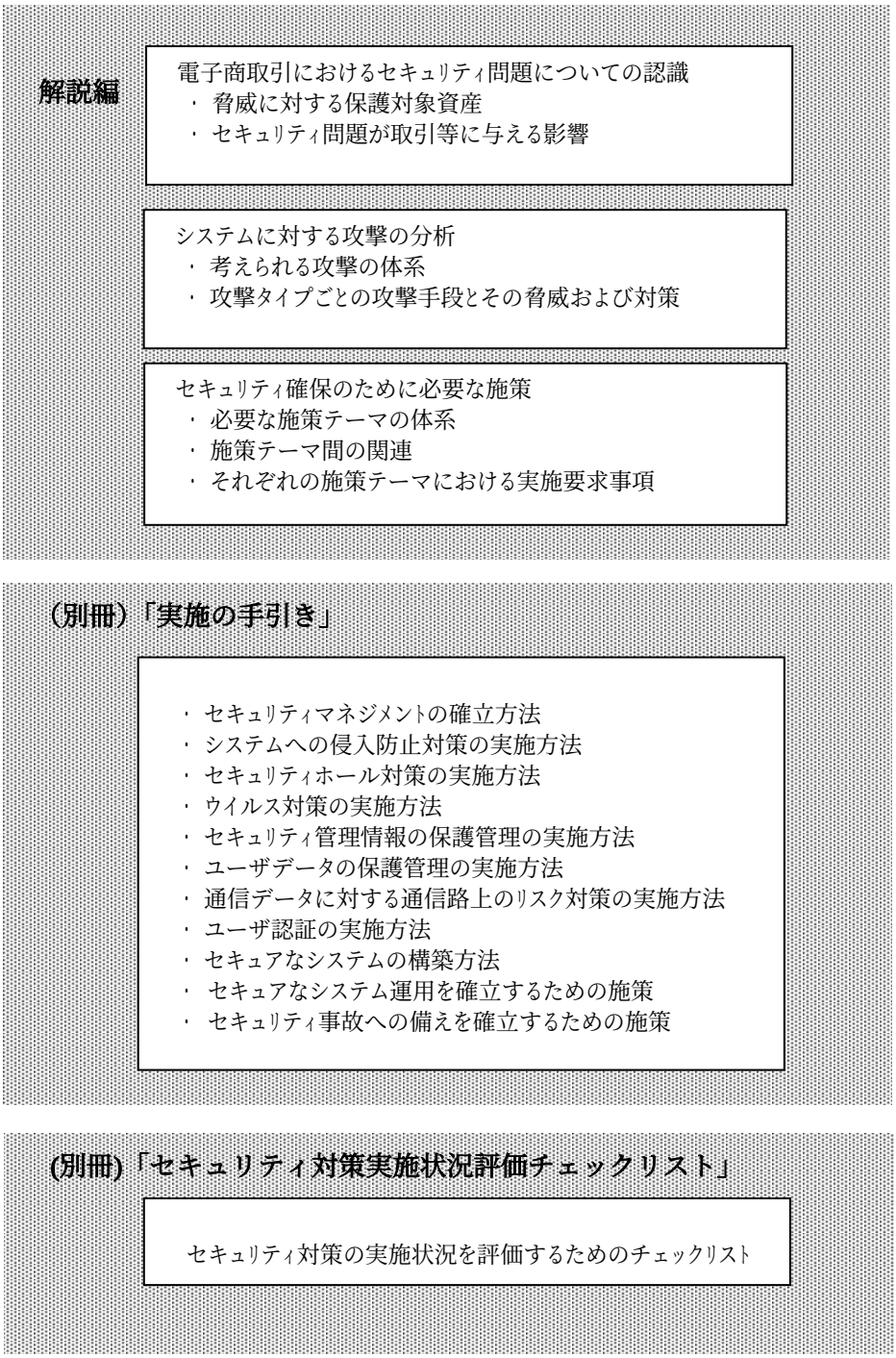

図 1-1 本ガイドラインの構成

1.4 本ガイドラインの適用範囲

本ガイドラインが対象とする脅威は、サイトならびにシステムが扱う情報資産に対する意図的な攻撃とし、システムの構成要素の故障、操作上のミス、災害等によるシステムの動作不良や破壊は含まないものとする。これらは、システム設計上の信頼性設計や性能設計あるいはソフトウエアの品質確保問題として、本ガイドラインではセキュリティ問題の外と考える。

従って、本ガイドラインが対象とするところは、以下の範囲とし、そのイメージを図 1-2 に示す。

- バーチャルショップの運営にかかるシステムのインターネット接続セグメントの構成、仕様、運用
- その他の領域については、バーチャルショップの運営にかかる個人情報、取引情報、セキュリティ管理情報の保護管理

従って、図 1-2 に示すファイアウォール等で外部からは隔離された内部セグメントにあるバックヤードシステムは、対象としない。

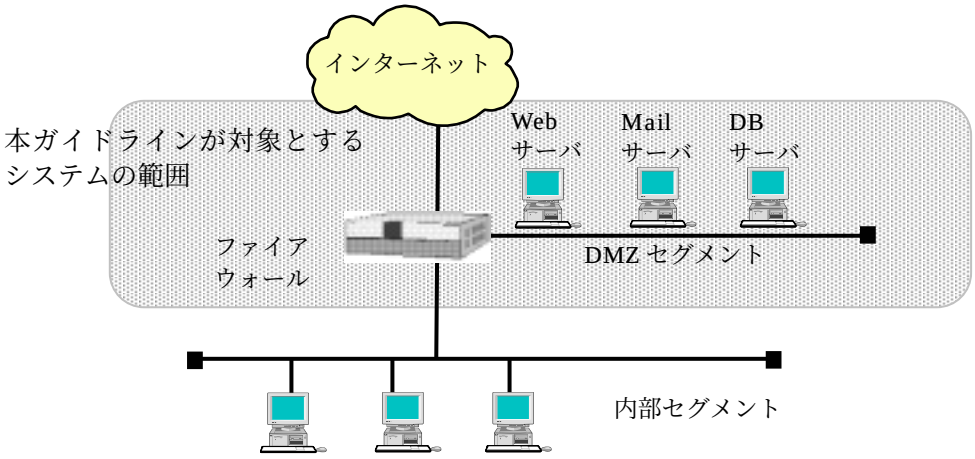

図 1-2 本ガイドラインが対象とするシステムの範囲

1.5 本ガイドラインの利用方法

本ガイドラインは、EC サイトのセキュリティを確保するために、実施しなければならないことを体系化し、その個々について解説したものである。

本ガイドラインは、以下に示すような場合の参考にされたい。

- EC サイトにおけるセキュリティ問題の基本を理解したい時
- EC サイトにおけるセキュリティ対策の概要を理解したい時
- EC サイトにおけるセキュリティ対策の構築あるいは現行セキュリティ対策の評価、再構築をしたい時
- EC サイトにおけるセキュリティ対策の実施状況を評価したい時

それぞれの場合における、本ガイドラインの利用についての考え方を以下に示す。

(1) セキュリティ問題の基本を理解したい場合

セキュリティ対策についての検討にあたっては、EC サイトの運営にかかる脅威や、脅威に対する基本的な対応策等、EC サイトにおけるセキュリティ問題についての基本的な理解が必要となる。情報システムのセキュリティ問題について理解が不充分と考えている方、およびこの際、この点についての理解を再整理したい方は、本書の第 1～3 章を参照されたい。ここでは、EC サイトにおけるセキュリティ上の脅威についての解説と、攻撃を受けた場合に考えられる EC サイト運営上の影響、ならびに脅威に対する対抗策の基本が示されている。ショップ経営者やサイト運営の責任者は、自分がかかわる EC サイトのセキュリティの最終責任者として、これらについての十分な理解が求められる。

(2) セキュリティ対策の組立てを理解したい場合

EC サイトのセキュリティ対策を構築するにあたっては、まず、具体的な実施事項とその実施方法についての検討が必要となるが、その検討の基盤として、セキュリティ対策をどう組立てるかを確立しなければならない。EC サイトにおけるセキュリティ対策の組立ての検討にあたっては、本書の第 4 章を参照されたい。ここには、求められる施策の体系とそれぞれの施策の主旨と必要な事項が列挙されているので、考え方の整理と、検討すべき事項の洗出しの参考になるはずである。

(3) セキュリティ対策の新規構築、あるいは現行セキュリティ対策の評価、再構築をしたい場合

サイトにおけるセキュリティ対策を新規に構築したい場合、あるいは既に実施しているセキュリティ対策の評価、見直しを行いたい場合は、別冊の「EC サイトにおけるセキュリティ対策ガイドライン－対策実施の手引き」を参照されたい。

この対策実施の手引きには、個々の求める施策に対し、行うべきことについての説明と、その実施上のポイントが示されているので、セキュリティ対策の詳細を検討するガイドになるはずである。実際のセキュリティ対策は、本ガイドラインがセキュリティ対策として求めていることに対する回答で構成される。これらについては文書化が必要となるが、その文書化については、各サイトの運営実態に合った適切な様式化等の工夫が必要である。

また、セキュリティ対策にかかるシステムの構成と実装の設計についての記述は、その考え方と管理のポイントを示すに止め、その詳細については触れていない。これは、技術や対応製品が日進月歩であることと、これらはセキュリティ対策への取組みやサイトの運営形態の違いにより千差万別であるところから、このようなガイドラインで示すのは困難であるという理由だけでなく、セキュリティマネジメント上は、これらが“サイトのセキュリティ対策が求めていることを満足するようにする”ということに尽きるので、特にそこまで触れる必要はないとの考えによるものである。

セキュアなシステム構築の具体的なことについては、別途専門家の相談を受けることをお薦めする。

(4) セキュリティ対策の実施状況を評価したい場合

運営する EC サイトのセキュリティ対策が十分かどうか、どこかに欠陥はないかについて定期的なチェックを行い、見つけた問題に対し適切な処置を講じ、サイトのセキュリティを一歩一歩進化させる努力は欠かせない。

別冊の「EC サイト向けセキュリティ対策実施状況評価要領」は、セキュリティ対策として求められていることに対し、どのくらいの対応ができているかを知りたい場合、チェックする項目を施策単位で示すとともに、その対策の十分性についての評価尺度を示している。サイトのセキュリティ監査等、サイトのセキュリティ対策の実施状況の評価を行う場合の参考にされたい。

1.6 用語の定義

- EC サイト

  インターネットに接続され、消費者等に電子商取引サービスを提供する Web サイトを指し、本ガイドラインでは、システムだけでなく、システムの運営、対象業務であるバーチャルショップの運営を含めたサイト運営の全てを指す。

  EC サイトには、バーチャルショップが単独で運営するサイトや、複数のショップの集合体であるモールがある。また、IDC 等でショップやモールの運営代行が行われている場合、これらのシステムも、本ガイドラインの言う EC サイトに入る。
  なお、直接取引をサポートしていないポータルサイトやインターネットプロバイダーのシステムは、本ガイドラインの EC サイトには含まれない。

  なお、EC サイトが指すシステムの範囲については、EC サイトシステムの定義を参照のこと

- EC サイトシステム、サイトシステム、システム

  本ガイドラインでは、EC サイトにおけるシステムのうち、インターネットからアクセスできる範囲を指す。そのイメージについては、1.4 節を参照。

- DoS 攻撃

  Denial of Service の略で、システムへの技術的な介入でシステムの運用を妨害する行為

- 保護対象情報

  EC サイトが扱う情報のうち、外部への漏洩、改ざん、破壊から守るべき情報の総称。本ガイドラインでは、その役割、サイト運営上の取扱いの違い、EC サイトにおけるセキュリティ確保等との係わり合いから、さらにこれらを、セキュリティ管理情報とユーザ情報に分類している。

- セキュリティサービス機能

  ファイアウォールにおけるアクセス制御機能、侵入監視装置における侵入監視機

能、ウイルス検査機能、システムの脆弱性診断機能等、サイトシステムのセキュリティ確保のためのサービスを指す。

- セキュリティ管理情報

  ユーザ認証に用いる情報、アクセス権限に関する情報、システム構成情報等、その情報の漏洩や改ざんが、サイトのセキュリティを直接的な脅威になるような情報。これらについては、特に厳格な保護管理が必要である。

- ユーザ情報（ユーザデータ）

  EC サイトが、業務の運営にあたって取扱う消費者や取引先にかかわる情報、および EC サイトが扱う取引情報の総称。プライバシーにかかわる個人情報、取引先の企業秘密にかかわる情報の漏洩、改ざん等は、当該情報の主権者との間でトラブルとなる恐れがあるので、その保護管理は、サイトのセキュリティに関する重要なテーマの一つである。

  なお、本ガイドラインでは、ユーザ情報を含むファイル等を、ユーザデータと呼んでいる。

2 EC サイトにおけるセキュリティにかかる脅威

2.1 電子商取引におけるセキュリティ問題とは

インターネット経由の非対面取引という形態をベースとする電子商取引においては、基盤としている技術環境の特徴から、第三者の攻撃を受けやすく、システムの構成や運用がずさんであれば、

- システムへの不正アクセス
- 通信データの盗聴
- DoS 攻撃

等を許し、その結果として、取引上の混乱、消費者のカード情報等の重要情報や個人情報の流出による問題、サイト運営の妨害というトラブルに見舞われることになる。

セキュリティ問題とは、このようなセキュリティにかかるトラブルを排除し、電子商取引を消費者にとっても、ショップ事業者にとっても、安全で信頼できるものにするための課題である。

2.2 想定される EC サイトにおけるセキュリティトラブル

EC サイトシステムのセキュリティ面の問題から生じるバーチャルショップ運営上のトラブルとしては、以下のようなものが考えられる。このトラブルには、個々の取引にかかわるものと、個々の取引には影響が現れないものの、後日、まったく別な場面で違った形態でトラブルを発生させるものがある。

⑴ 悪意の業者による他ショップへのなりすまし

消費者になじみの深いショップを装うもので、このショップのホームページ等を盗用して、消費者に対しあたかもそのショップと取引をしているように錯覚させ、消費者が意識していない相手と消費者の意図しない取引を成立させてしまう手口である。

⑵ 悪意の者による他の消費者へのなりすまし

購買者が他人のパスワード等を利用して他人を装い、商品の詐取等を行なおうとするもので、クレジット決済等の決済方法次第では、第三者を巻き込むトラブルとなる。

⑶ 商品表示･取引条件表示の改ざん

第三者の介入による商品や取引条件の画面表示の改ざんは、ショップ側にとっても消費者側双方にとって意図しない取引を成立させてしまう結果、商品に対するクレームや代金等の取引条件についてのトラブルを招く。

⑷ 取引メッセージの改ざん

第三者の介入による取引メッセージの改ざんは、消費者の購入申し込みとは異なった購入指

示がショップ側に届けられたことにより、商品に対するクレームや数量や代金等の取引条件についてのトラブルを招く。

⑸ 取引の否認

- ショップ側による購入申込み受付けの否認

  購入申込みを受付けながら、その受付けの事実を否認し、取引を実行しない行為であり、消費者にとっては確保できたはずの商品を入手できないというようなことを生じることが考えられる。

- 消費者側による購入申込みの否認

  購入の申込みを行いながらその事実を否認し、ショップが準備した取引を拒否するもので、商品の詐取等にはつながらないものの、ショップには商品の準備等を無駄にし、場合によっては実害も招くこともありうる。

⑹ 個人情報や取引情報の漏洩

第三者による取引の申込みにかかるメッセージのやり取りの盗聴や、EC サイトのずさんな運用管理につけこんだ内部犯行による個人情報の不正な取得等により、本来秘匿されなければならない個人情報や取引に関する情報が第三者に漏れることであり、これらの情報が不正使用されると、消費者には後日、以下のような問題が生じる。

- パスワード等の漏洩による当人へのなりすましによる商品や預金の搾取
- 保護されるべき個人情報の第三者への不正開示または漏洩
- 取引情報の競争相手への漏洩によるビジネスにおける不利

⑺ システムの破壊および運用の妨害

システムやデータベース（以降ＤＢと略す）を破壊したり、システムの業務運用ができなくなってしまうような事態を生じさせるもので、コンピュータウイルスの侵入を許したり、ＤｏＳ攻撃に対する備えがなかったりした場合、このような事態を招くことがある。

2.3 保護対象の資産と保護対象資産に対する脅威

EC サイトシステムおいて脅威として意識すべきものとしては、以下があげられる。

- 個別取引の妨害
- 業務の運用妨害
- 保護対象情報の不正取得
- システムの運用に対する妨害
- ネットワークでつながる他サイトもしくはユーザ端末攻撃への加担

2.3.1 個別取引の妨害

個別取引に対する妨害とは、電子商取引における個々の取引の円滑な処理を妨げるものであり、表 2-1 に示すようなケースが考えられる。

表 2-1 個別取引に対する妨害とその手段

項番	妨害のタイプ	想定される手段
1	他の消費者へのなりすましによる取引の実行	・ユーザ認証を行っていないことを利用 ・ユーザ認証の不備
2	商品や取引条件の表示内容の改ざん	・商品や取引条件を示すコンテンツの改ざん ・業務 DB 上の業務情報の改ざん
3	取引データの改ざん、破壊	・通信路上での取引指示データ、取引確認データの改ざん、破壊 ・業務 DB 上の業務情報の改ざん、破壊
4	取引の否認 ・消費者のよる購入申込みの否認 ・ショップによる購入申込受付けの否認	・取引指示の事実確認の困難さを利用した意図的な否認

2.3.2 業務の運用妨害

個別取引に対する妨害ではなく、電子商取引という業務の全体的な運営を脅かすもので、表 2-2 に示すようなケースが考えられる。

なお、サイトシステムの運用妨害は、結果として業務の運用妨害につながるが、システムの運用妨害については、2.3.4 節参照。

表 2-2　業務の運用妨害とその手段

項番	妨害のタイプ	想定される手段
1	業務運営に関する機能の不正使用 （業務の運営に関する指示等の機能を不正に使用し、業務運営管理者の意図とは異なる運営を強いること）	・該当機能へのアクセス制限の不備をついたシステムの機能への不正なアクセス ・該当機能へのアクセス制御情報への細工によるシステムの機能への不正アクセス ・業務運営指示者の権限の不正取得によるシステムの機能への不正アクセス
2	システム上の情報の改ざん、破壊 ・セキュリティ管理情報の改ざん、破壊 ・ユーザ情報の改ざん、破壊	・該当機能へのアクセス制限の不備をついたシステムの機能への不正なアクセス ・該当機能へのアクセス制限情報への細工によるシステムの機能への不正アクセス ・業務運営指示者の権限の不正取得によるシステムの機能への不正アクセス ・管理者権限の不正取得によるファイルへのアクセス ・セキュリティホールをついた攻撃によるファイルへのアクセス ・ウイルスを用いたファイルの破壊
3	関係ソフトウエアの改ざん ・HTML ファイルの改ざん ・システム上にあるその他のプログラムの改ざん	・管理者権限の不正取得によるソフトウエアの置換え(書換え) ・セキュリティホールをついた攻撃によるソフトウエアの置換え(書換え)

2.3.3 保護対象情報の不正取得

個人情報等サイト運営上保護しなければならない情報が、外部の者に不正に取得されることで、商取引そのものには直接的な影響はないものの、関係者に多大な迷惑を生じるもので、表 2-3 に示すようなケースが考えられる。

表 2-3　保護対象情報の不正取得とその手段

項番	妨害のタイプ	想定される手段
1	システム上の保護対象情報の不正取得	・該当情報へのアクセス制限の不備をついた情報への不正アクセス ・該当情報アクセス制御情報への細工による情報への不正アクセス ・当該情報へのアクセス権限の不正取得による情報不正アクセス
2	通信データの保護対象情報の不正取得	・通信路上での該当情報を含む通信データの盗聴
3	業務運営上での情報の取扱いの不備からくる漏洩、流出	・保護対象情報を含む電子媒体や印刷物のずさんな取扱いをついた入手 ・内部関係者の意図的な外部への持出し

2.3.4 システム運用に対する妨害

サイトシステムの円滑なシステム運用を妨害するもので、表 2-4 に示すようなケースが考えられる。

表 2-4　システム運用の妨害とその手段

項番	妨害のタイプ	想定される手段
1	システム運用に関する機能の不正使用 システム運用に関する指示等の機能を不正に使用し、運用管理者の意図とは異なる運営を強いる	・システムの運用にかかるアクセス制限の不備をついた機能への不正なアクセス ・システムの運用にかかるアクセス制御情報への細工による機能への不正アクセス ・システム運用管理者の権限の不正取得によるシステムの機能への不正アクセス
2	システム上の情報やソフトウェアの改ざん、破壊 ・メモリ上のプログラムや情報の改ざん、破壊 ・ＤＢ上のプログラムや情報の改ざん、破壊	・管理者権限の不正取得によるプログラム、制御情報、ＤＢの置換え(書換え) ・セキュリティホールをついた攻撃によるプログラム、制御情報、ＤＢの置換え(書換え) ・ウイルスによるプログラム、制御情報、ＤＢの破壊
3	サービスの妨害	・DoS 攻撃

3　システムにおける脅威と対策―セキュリティ対策

3.1　システムに対する脅威の分析

3.1.1　システムに対する脅威の体系

システムにおける脅威の体系を図 3-1 に示す。

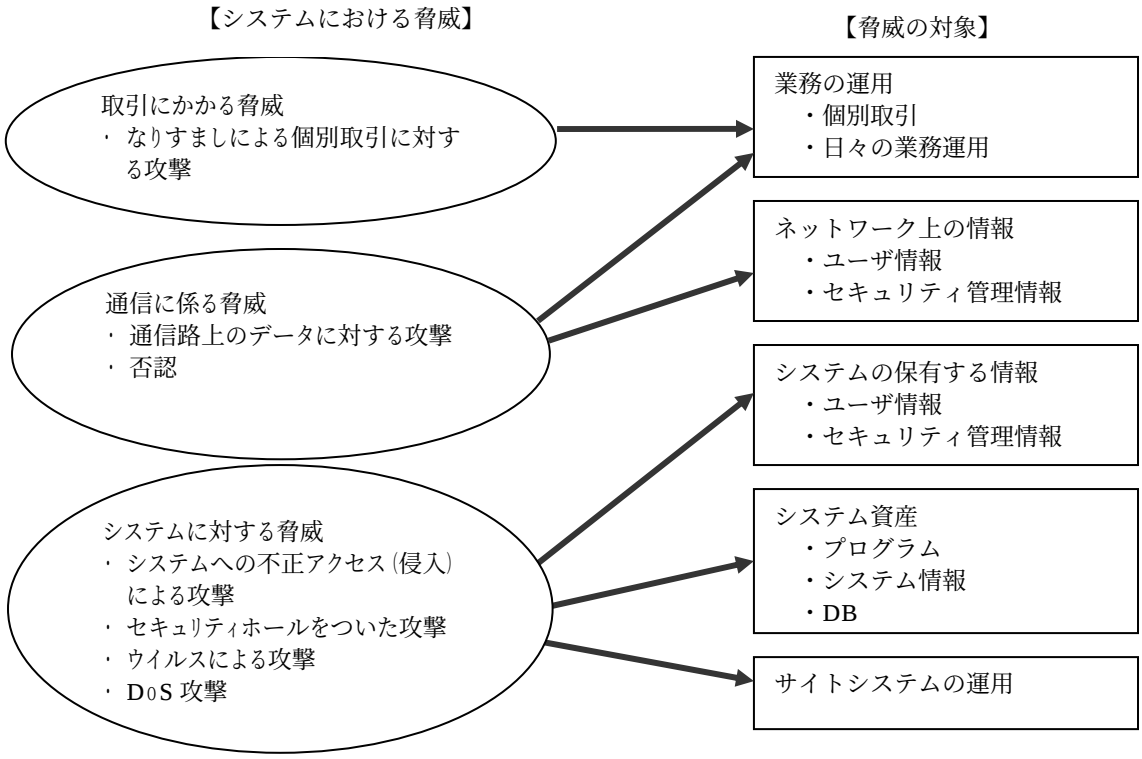

図 3-1 サイトシステムにおける脅威の体系

3.1.2　システムに対する攻撃の連鎖

システムに対する攻撃は、一つの攻撃が、新たな攻撃の手がかりを与え、別な攻撃を誘うといったように相互に関連するものがある。この関係を図 3-2 に示す。攻撃に対する対抗策としてのセキュリティ対策の検討にあたっては、これらの関係にも十分注意を払う必要がある。

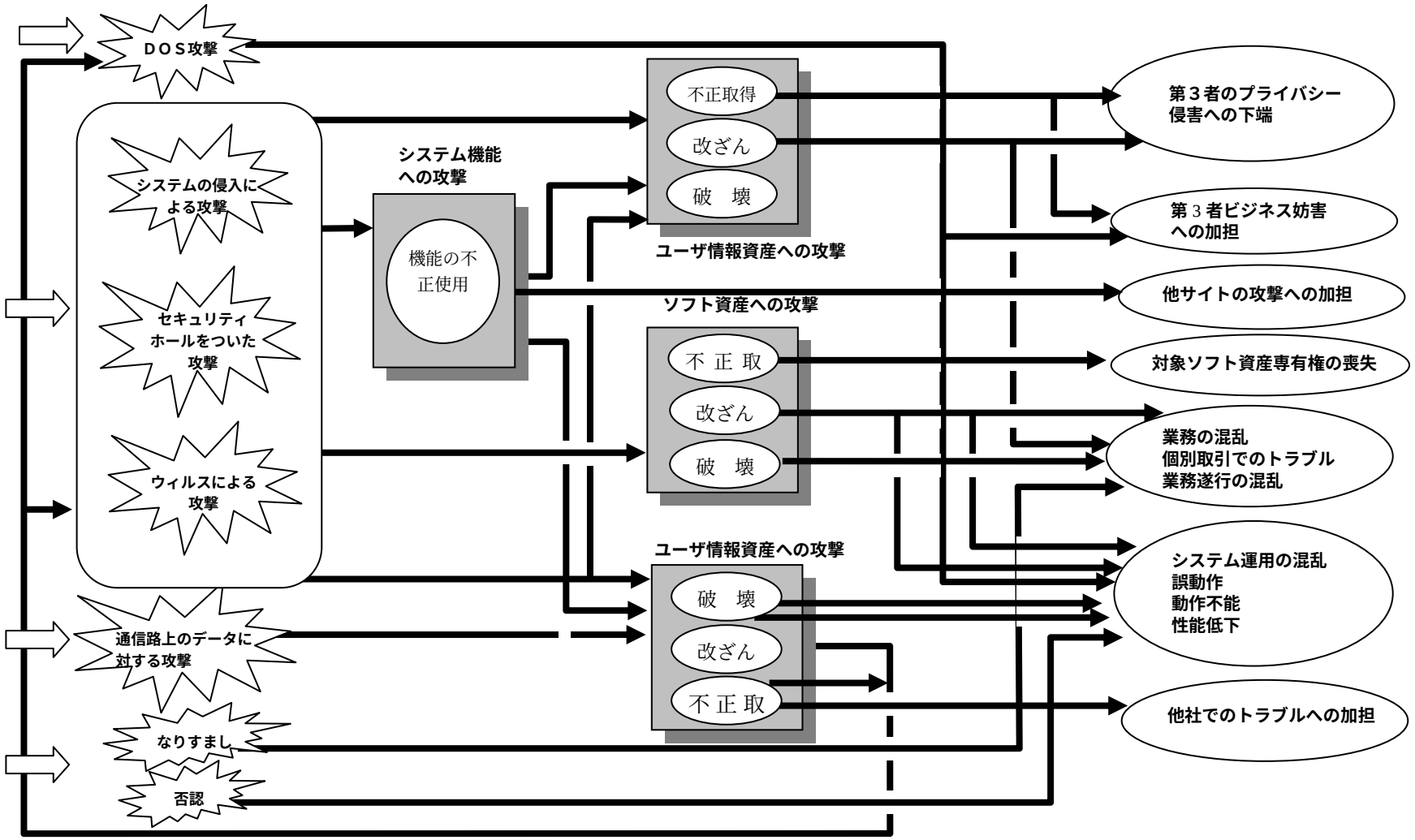

図 3-2 サイトシステムに対する攻撃の連鎖

3.2 個々の攻撃の分析

3.2.1 なりすましによる個別取引に対する攻撃

⑴ なりすましによる攻撃とは

なりすましによる個別取引に対する攻撃とは、

- オンラインショッピング等、一般に開放されている業務機能に他人になりすまして不正にアクセスし、他人名義で商品の購入等を行うこと
- 登録していないものが登録者をかたり、登録者に限定されたサービスを受けること

を指す。

本来的には、一般には開放されておらず、権限が付与された者しかアクセスできない内部管理機能等、サービスへの不正なアクセスは、本ガイドラインでは、システムへの侵入と捕らえ、3.2.2 節で議論する。

⑵ なりすましによる個別取引に対する攻撃とその影響

なりすましによる個別取引への攻撃により発生が懸念される問題を、表 3-1 に示す。

表 3-1 なりすましによる個別取引への攻撃の影響

項番	アクセスの対象	攻撃の内容	発生が懸念される問題
1	一般公開サービスへのアクセス	・ 他人名義での取引の実行	・取引の混乱 －架空取引の惹起 －商品の搾取 －他人へのつけまわし ・情報の不正取得
2	限定的公開サービスへのアクセス	・ 限定サービスの不正利用	・権利のないものへの不当な利益、利便の提供 ・利権者の権利侵害 ・情報の不正取得

⑶ なりすましの手段と対抗策

なりすましの手段と、それらの手段に対する対策を、表 3-2 に示す。

表 3-2　なりすましの手段と対抗策

項番	なりすましの手段	対抗策
1	ずさんなユーザ認証をついたなりすまし	・強度の高い認証方式の採用
2	認証情報の解読	・パスワード等認証用情報の適切な設定 （解読されにくい情報の設定）
3	認証情報の漏洩 ・システムへの侵入による不正取得 ・セキュリティ管理情報への不正アクセスによる不正取得 ・認証用情報のずさんな取扱いをついた不正取得	・システムへの不正アクセス対策の徹底 ・セキュリティホール対策の徹底 ・セキュリティ管理情報へのアクセス制限の徹底 ・運用上でのセキュリティ管理情報の厳正な取扱い
4	認証情報、権限情報の改ざん ・システムへの侵入による不正取得 ・セキュリティ管理情報への不正アクセスによる不正取得	・システムへの不正アクセス対策の徹底 ・セキュリティホール対策の徹底 ・セキュリティ管理情報へのアクセス制限の徹底

⑷ なりすまし対策の構成

なりすましに対する対策の基本は、

- 適切な認証方式の採用
- 認証用情報の保護管理の徹底

からなる。

それぞれの対策のポイントを、表 3-3 に示す。

表 3-3　なりすまし対策のポイント

項番	対策項目	ポイント	備考
1	適切な認証方式の採用	・ニーズに合わせた適切な認証方式の適用 ・パスワード等認証に用いる情報の適切な設定	
2	認証用情報の保護管理の徹底	・システムへの不正アクセス対策の徹底 ・セキュリティホール対策の徹底 ・認証用情報の保護管理の徹底 定期的な更新の実施	セキュリティ管理情報の保護管理に含む

また、表 3-3 に示すように、なりすましの阻止は、ユーザ認証の適切な適用に加え、システムへの侵入防止、セキュリティホール対策、セキュリティ管理情報の保護管理、伝送路上のリスク対策がそれぞれ機能しなければならない。

(注) システムへの侵入防止、セキュリティホール対策、セキュリティ管理情報の保護管理、伝送路上のリスク対策についいては、該当の節参照。

3.2.2 システムへの不正アクセス(侵入)の脅威と侵入防御策

(1) システムへの不正アクセス(侵入)とは

システムへの不正アクセス(侵入)とは、権限のない者がシステムにアクセスし、

- システムのサービス(機能)の不正使用
- システムの動作妨害
- システム上の情報の破壊、改ざん、不正入手
- ソフトウエア資産の破壊、改ざん

といった行為を行うことである。

(2) システムへの不正アクセス(侵入)による攻撃とその影響

システムへの不正アクセス(侵入)による攻撃にもいろいろなものがある。想定される攻撃とそれによりもたらされる影響を、表 3-4 に示す。

表 3-4 システムへの不正アクセス（侵入）による攻撃とその影響

項番	システムへの侵入による攻撃	発生が懸念されるトラブル
1	システムのサービス(機能)の不正使用	・サービス提供の課金もれ ・不正取引処理の実行 ・情報の不正入手 ・認証用情報、アクセス権限情報の入手によるシステム資源へのアクセスによる新たな攻撃の実行 ・他システムの攻撃への踏み台
2	システムの運用妨害	・システムの(一時的な)動作不能 ・システムの(一時的な)性能低下 ・システムの暴走

表 3-4　システムへの不正アクセス（侵入）による攻撃とその影響

項番	システムへの侵入による攻撃	発生が懸念されるトラブル
3	プログラム等システム資産の破壊、改ざん	・ アクセス制御機能の変更による他の攻撃の実行 ・ システムの動作不能 ・ システムの性能低下 ・ システムの暴走
4	システム上の情報の不正入手、情報資産の破壊、改ざん	・ 取引情報の漏洩、改ざん、破壊 ・ 商業秘密情報の漏洩、改ざん、破壊 ・ 個人情報の漏洩、改ざん、破壊

(3) システムへの不正アクセス(侵入)の手段と対抗策

システムへの不正アクセス(侵入)にはいろいろな手段があるが、いずれもアクセス管理の不備をついたものである。考えられるシステムへの侵入の手段とそれぞれの手段への対抗策を、表 3-5 に示す。

表 3-5　システムへの不正アクセス攻撃の手段とそれぞれの攻撃手段への対抗策

項番	システムへの侵入手段 (侵入を許すアクセス管理上の不備)	当該手段への対抗策
1	不要なサービスの放置をついた侵入 (業務上、特に必要のないサービスをネットワークに開放したままにしておくと、管理対象外のサービスのため、アクセス制限に漏れが生じ易く、攻撃者に窓口を与えることにつながる)	・ 不要サービスの除去または停止
2	アクセス管理の不備をついた侵入 ・ アクセス制限のルールの不備 ・ 具体的なアクセス制限の指定の不備 ・ 指定されたアクセス制限の実装の不備 等により生じたアクセス管理すべき窓口に本来のアクセス管理が行われていないようなアクセス管理の穴は、攻撃者に侵入の窓口を与える。	・ アクセス制限の的確な実施
3	なりすましによる侵入 ・ 権限者の認証の不備をついたなりすまし ・ アクセス制御情報の不正入手によるなりすまし	・ ユーザ認証の適切な適用 ・ セキュリティ管理情報の保護管理の徹底

(注) セキュリティホールをついた攻撃やウイルスによる攻撃は、システムへの正規のアクセスによっても行われることから、本ガイドラインでは、システムへの侵入とは別と考える。

(4) システムへの不正アクセス(侵入)対策の構成

システムへの不正アクセス(侵入)による攻撃への対策としては、以下があげられる。

- サイトにおけるデータフローに対する適切な制御および監視の実施
- システム(サーバ)へのアクセスに対する適切なアクセス制御および監視の実施
- 個々のサービスに対する的確なアクセス制限の徹底
- 不要なサービスの削除または停止
- 適切なユーザ認証の実施
- アクセス管理情報の保護管理の徹底
- システムへの侵入事故に対する備えの実施

それぞれの対策のポイントを、表 3-6 に示す。

表 3-6　システムへの侵入対策のポイント

項番	対策項目	ポイント	備考
1	サイトにおけるデータフローに対する制御および監視の実施	・データフロー制御・監視ポリシーの確立 ・データフロー制御・監視ポリシーの沿った外部ネットワークとのデータフローおよびサイト内部のデータフローに対する適切な制御と監視の実施	
2	システム（サーバ）へのアクセスに対する制御と監視の実施	・OS のアクセス制御ならびに監視機能の適切な利用	
3	個々のサービスに対する的確なアクセス管理の実施	・個々のサービスに対するアクセス制限の徹底 ・アクセス監視の徹底	
4	不要なサービスの停止	・システムが有しているサービスの正確な把握と、不要なサービスの停止の厳格な実施	
5	アクセス制御にかかる情報の保護管理の徹底	・セキュリティ管理情報の保護管理の徹底	(注１)
6	ユーザ認証の適切な実施	・適切なユーザ認証ルールの確立 ・場面場面にあった適切なユーザ認証方式の適用 ・ユーザ認証に用いる機能の整備 ・ユーザ認証に用いる情報の保護管理の徹底	(注２)
7	システムへの侵入事故に対する備えの実施	・対処要領の整備 ・システムの復旧手段の整備	

(注1) セキュリティ管理情報の保護管理は、セキュリティ対策の中でも大きなテーマであるため、本ガイドラインでは、独立テーマとしてシステムへの侵入対策とは別個に扱う。

(注2) ユーザ認証の適切な適用は、セキュリティ対策の中でも大きなテーマであるため、本ガイドラインでは、独立テーマとしてシステムへの侵入対策とは別個に扱う。

3.2.3 セキュリティホールをついた攻撃への防御

(1) セキュリティホールとは

セキュリティホールとは、攻撃者がターゲットとしたシステムにおいて、自分の好みのプログラムを埋込み、かつ動作出来るようにすることが可能になるようなプログラム上の欠陥を言う。

攻撃者は、このシステム上の欠陥を活用して、ターゲットとしたシステムに、任意のプログラムを送り込み、自分の意図した動作を実行させることにより、ターゲットとしたシステムに、表 3-7 に示したような問題を発生させることができる。

(2) セキュリティホールを突いた攻撃とその影響

セキュリティホールを突いた攻撃と、その攻撃により発生が懸念されるトラブルを、表 3-7 に示す。

表 3-7 セキュリティホールを突いた攻撃とその影響

項番	攻撃対象	攻撃の内容	発生が懸念されるトラブル
1	ソフトウェア資産	システムの機能の不正使用	・利用権限のない者へのサービスの提供 ・予定外のシステム機能の発動による業務の混乱 ・システムの運用の混乱 ・システム上の情報の不正取得 ・他システム攻撃への加担
2		システムの改ざん、破壊	・業務プログラムの改ざんによる業務の混乱 ・業務プログラムの破壊による業務の混乱 ・システムの破壊によるシステム運用の混乱
3	情報資産	情報資産の不正取得	・取引の混乱 ・プライバシー侵害への加担 ・商業秘密悪用への加担 ・なりすましの手がかりの付与 ・システム運用の混乱
4		情報資産の改ざん、破壊	・取引の混乱 ・システム運用の混乱
5	システム機能	運用妨害	・システム運用の混乱

(3) セキュリティホールをついた攻撃からの防御(セキュリティホール対策)

セキュリティホールをついた攻撃は、セキュリティホールの存在が前提となる。このため、セキュリティホールをついた攻撃からシステムを守るセキュリティホール対策の基本は、システムにセキュリティホールを残さないことにある。しかし、ソフトウェアにセキュリティホールが存在しないことを保証することは困難なため、一般ユーザにとって、この点に関してできることは、システムが使用しているソフトウェアについて報告されているセキュリティホールを除去することに限られる。従って、システムに既に報告されているセキュリティホールがないことを常に確認することと、セキュリティホールに関する情報を集め、新しく報告されたセキュリティホールの除去を如何にこまめに行うかがそのポイントとなる。

一方、既に報告されているセキュリティホールの除去の徹底に努めても、報告されていないセキュリティホールがあれば、セキュリティホールをついた攻撃を許してもおかしくはない。このため、セキュリティホール対策としては、攻撃を許した時への備えも重要な要素となる。

以上のことより、セキュリティホール対策のポイントは、

- 最新の情報に基づく既報告セキュリティホールの検査、除去の徹底
- 被害の極小化するためのセキュリティホールをついた攻撃を受けた時への備えの実施

となる。

3.2.4 ウイルスによる攻撃とその対策

(1) ウイルスとは

ウイルスとは、コンピュータに感染し、ユーザの意図しない動作(操作妨害、ファイル破壊等)を行う悪質なコンピュータプログラムまたはデータのことであり、その振舞いがインフルエンザ等の病原性のウイルスによく似ているために、“コンピュータウイルス”もしくは単に“ウイルス”と呼ばれている(本ガイドラインでは「ウイルス」と呼ぶ)。

ウイルスには、その構造的な特性により、ブートセクタ感染型ウイルス、ファイル感染型ウイルス、マクロウイルス、ネットワーク言語型ウイルス等に分類されている。感染時の症状も、感染経路もそれぞれに特徴がある。ウイルス対策は、これらのウイルスの特性を踏まえて行わなければならない。

(参考) ウイルスの定義

「コンピュータウイルス対策基準」(通商産業省告示第 952 号)では、ウイルスを以下のように定義している。

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

① 自己伝染機能
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

② 潜伏機能
　発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能
③ 発病機能
　プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

本ガイドラインでは、この定義を広義のウイルスととらえ、狭義のウイルスに対して対策を述べる。広義のウイルス対策は、狭義のウイルス対策に加え、別途に示すシステムへの侵入防止策やセキュリティホール対策などの対策を施すことにより、対応が可能と考える。なお、広義のウイルスとは、トロイの木馬やブラウザクラッシャー、メールボム等を指す。

(2) ウイルスによる攻撃とその影響

ウイルスによる攻撃の対象と、その攻撃により発生が懸念されるトラブルを、表 3-8 に示す。

表 3-8 ウイルスによる攻撃とその影響

項番	攻撃対象	攻撃の内容	発生が懸念されるトラブル
1	ソフトウエア資産	システムの機能の不正使用	・利用権限のない者へのサービスの提供 ・予定外のシステム機能の発動による業務の混乱 ・システムの運用の混乱 ・システム上の情報の不正取得 ・他システム攻撃への加担
2		システムの破壊	・業務プログラムの改ざんによる業務の混乱 ・業務プログラムの破壊による業務の混乱 ・システムの破壊によるシステム運用の混乱
3	情報資産	情報資産の不正取得	・取引の混乱 ・プライバシー侵害への加担 ・商業秘密悪用への加担 ・なりすましの手がかりの付与 ・システム運用の混乱
4		情報資産の破壊	・取引の混乱 ・システム運用の混乱
5	システム機能	運用妨害	・システム運用の混乱

(注) ウイルスによる攻撃は、セキュリティホールをついた攻撃と比べると、攻撃手段が異なるだけで、その影響は同じ。

(3) ウイルス対策の構成

ウイルスに対する対策は、

- ウイルス感染防止策
- ウイルス感染の早期発見
- ウイルスの外部への持出しの阻止
- ウイルス感染事故時の被害の極小化

からなる。

それぞれの対策のポイントを、表 3-9 に示す。

表 3-9　ウイルス対策のポイント

項番	対策項目	ポイント
1	ウイルスの感染防止	・機器、ソフトのシステム組込み時におけるウイルス検査の徹底 ・入出力の取込み時におけるウイルス検査の徹底
2	ウイルス感染の早期発見	・定期ウイルス検査の励行 ・新しい脅威が発見された場合の対象ウイルスに関する検査の励行
3	ウイルスの外部への持出しの阻止	・外部持出しファイルに対するウイルス検査の徹底
4	ウイルス感染事故時の被害の極小化	・感染範囲の正確な把握と感染ウイルスの完全除去 ・被害範囲の正確な把握 ・感染時の適切な対応 ・回復手段の整備

(4) ウイルス対策に関する技術

① ワクチンのウイルス検出技術

ウイルス検出技術には主に、以下のような方式がある。

- 過去に発見されたウイルスの特徴をデータベース化し、そのデータベースと比較することによって、ウイルスの感染を検査･検出する方式。ウイルスを特定できる可能性が高く、誤検出の可能性が少ない。その反面、常に最新のウイルスパターンファイルを保つ必要があり、未知のウイルスは検出できない。現在のワクチン製品は、比較的この方式を採用するものが多い。
- ファイルのチェックサムを事前に保存しておき、過去のチェックサムと現在のチェックサムを比較し、ウイルスによるファイルの改ざんを検出する方式。未知のウイルスに対応することができる。その反面、データ更新や設定変更の度にチェックサムを更新する必要があり、誤検出の可能性が高い。

② ワクチンの適用方法

ワクチンの適用方法の代表的な形態としては、以下のようなものがある。

- 外部からのウイルス感染を防止する目的で、組織外部との接点となるゲートウエイにワクチンを適用する。これにより、組織外部からのウイルス感染を防止することができる。
- コンピュータ自身のウイルス感染を防止するために、ワクチンを適用する、これにより自身のコンピュータシステムや保持するデータへのウイルス感染を防止できる
- 共有されているデータへのウイルス感染を防止するためにワクチンを適用する。これにより共有ファイルサーバ上のデータへのウイルス感染を防止でき、共有ファイルサーバを経由したウイルス感染も防止できる。ワクチンベンダーによっては、特定のグループウェア専用のワクチンを提供している場合もある。
- 特定のアプリケーション機能を利用した場合のウイルス感染を防止するためにワクチンを適用する。特に、メールサーバ用のワクチンを提供しているものが多い。これにより、メールの送受信によるウイルス感染を防止することができる。

③ ウイルス対策関連の製品とサービス

ワクチンによるウイルス検出率は、日ごろのワクチンベンダーの努力により、高い確率でウイルスを検出できるようになってきており、概ねどのワクチンも一定レベルのウイルス検出能力を持っていると考えることができる。ここ数年のウイルス対策関連の傾向は以下の通りである。

- ウイルス対策関連製品の統合化
- 外部ベンダーによるアウトソーシングサービスの提供

前者は、ウイルス対策関連製品の統合化である。ウイルス検出率の優劣より、運用性を重視したものである。異なるシステム適用方式のワクチンを統合し、集中管理できるようにした仕組みである。後者は、外部ベンダーによるアウトソーシングサービスである。ウイルス検査やウイルス発見時の対応、ウイルスパターンファイルのアップデートなどを管理者に代わり実施してくれるサービスである。

これらの製品やサービスを、適宜採用することにより、より効果的にウイルス対策が実施できるものと考える。

3.3 システム上の情報資産に対する攻撃の分析

3.3.1 システム上のセキュリティ管理情報に対する攻撃とその対策

(1) セキュリティ管理情報とは

セキュリティ管理情報とは、表 3-10 に例示するような、パスワードや暗号鍵、アクセス制御リスト等、サイトのセキュリティをサポートする機能がその動作に用いるパラメータ類を指す。

システムへの侵入を許したり、システムの運用の不手際から、この情報の外部への漏洩や、改ざんが発生すれば、サイトのセキュリティは一気に崩壊しかねない。このため、これらの情報は保

護管理すべき情報としては最重要なものであり、

- 外部への漏洩、流出
- 改ざん
- 破壊

の防止には徹底を期さなければならない。

セキュリティ管理情報には、OS 等サイトのシステムを構成するプラットフォームに固有のものと、業務に関係したアプリケーションレベルのものがある。

（注） 認証用のユーザ ID やパスワード等も個人情報には属するが、これらは個人に関する情報というよりは、サービスの提供に当ってのセキュリティ確保のための特別に付与されるものであり、その機能と運用面での取扱いが一般の情報と異なるため、本ガイドラインでは、これらの情報はセキュリティ管理情報に区分する。

表 3-10 EC サイトが扱うセキュリティ管理情報例

区分	情報の主権者	情報例
システム構成情報	・ サイト運用者	・ OS 設定情報 ・ ネットワーク設定情報 ・ ファイアウォール等各機能における各種設定情報
システム管理情報	・ サイト運用者	・ システム管理者権限 ・ ログ情報
アクセス権限情報	・ サイト運用者	・ アクセスコントールリスト
認証用情報	・ サイト運用者 ・ 利用者	・ ユーザ ID ・ パスワード ・ 指紋データ等特殊認証用情報
暗号関係情報	・ サイト運用者	・ 認証局証明書 ・ 暗号鍵

(2) セキュリティ管理情報に対する攻撃とその影響

EC サイトのセキュリティ対策が考慮すべき、表 3-10 に示すようなセキュリティ管理情報に対する攻撃手段とその攻撃により発生が懸念されるトラブルを、表 3-11 に示す。

表 3-11 EC サイト上のセキュリティ管理情報に対する攻撃とその影響

項番	攻撃のタイプ	発生が懸念されるトラブル
1	漏洩 (外部の者による不正入手)	・新たなシステムへの不正アクセス －システムの機能の不正使用 －システム資産の改ざん、破壊 －別なセキュリティ管理の不正取得、改ざん、破壊 －ユーザ情報の不正取得、改ざん、破壊 －システムの運用妨害 －他システム攻撃の踏み台
2	改ざん	・システムへの不正アクセスの踏み台 －システムの機能の不正使用 －システム資産の改ざん、破壊 －別なセキュリティ管理の不正取得、改ざん、破壊 －ユーザ情報の不正取得、改ざん、破壊 －システムの運用妨害 －他システム攻撃の踏み台
3	破壊	・システムの運用妨害

(3) セキュリティ管理情報への攻撃に対する対策

EC サイトが取扱うセキュリティ管理情報への攻撃に対する対策を、表 3-12 に示す。

表 3-12 EC サイト上のセキュリティ管理情報への攻撃と対抗策

項番	対象とする攻撃	対策
1	なりすましによるセキュリティ管理情報への不正アクセス	・ユーザ認証の適切な適用 ・セキュリティ管理情報の保護管理の徹底
2	アクセス管理の不備を突いたセキュリティ管理情報への不正アクセス	・システムへの不正アクセス対策の徹底 ・セキュリティホール対策の徹底 ・セキュリティ管理情報に対するアクセス制限の徹底
3	ウイルスによる攻撃	・ウイルス対策の徹底
4	業務上でのセキュリティ管理情報の取扱いの不備をついた攻撃	・サイト運用におけるセキュリティ管理情報の厳正な取扱い
5	通信路上での攻撃	・通信路上のリスク対策の徹底

3.3.2 システム上のユーザ情報に対する攻撃とその対策

(1) ユーザ情報とその保護について

ユーザデータとは、表 3-13 に例示するような個人情報や、そのサイトにおける商取引の実行に関わる取引情報を指す。

認証用のユーザ ID やパスワード等も個人情報には属するが、これらは個人に関する情報というよりは、サービスの提供に当ってのセキュリティ確保のために特別に付与されるものであり、その機能と運用面での取扱いが一般の情報と異なるため、本ガイドラインでは、これらの情報は、3.3.1 節にあげたセキュリティ管理情報に区分する。

表 3-13 EC サイトが扱うユーザ情報の代表例

区分	情報の主権者	情報例
個人情報	・ 消費者	・ 以下に示すようなプライバシーに関わる情報 －個人属性情報 －信用情報 －一部の取引情報
商業秘密情報	・ 出店者 ・ 取引先（企業）	・ 関係者外秘の事業にかかわる情報 －企業属性情報 －商品情報 －技術情報 －経営情報
一般取引情報	・ 消費者 ・ 出店者 ・ 取引先（企業）	・ 以下のもののうち個人情報、商業秘密情報に該当しない情報 －取引指示情報 －取引付属情報

(2) ユーザ情報に対する脅威とその影響

EC サイトのセキュリティ対策が考慮すべき、表 3-13 に示すようなユーザ情報に対する攻撃手段と攻撃により発生が懸念されるトラブルを、表 3-14 に示す。

表 3-14 EC サイト上のユーザ情報対する攻撃とその影響

項番	脅威	発生が懸念されるトラブル
1	漏洩 (外部の者による不正入手)	・プライバシー侵害への加担 ・商業秘密情報の悪用への加担
2	改ざん	・プライバシー侵害への加担 ・取引の混乱
3	破壊	・取引の混乱 ・サイト運用の混乱

(3) ユーザ情報への攻撃に対する対策

EC サイトが保有するユーザ情報への攻撃に対する対策を、表 3-15 に示す。

表 3-15 EC サイト上のユーザ情報への攻撃に対する対策

項番	対象とする攻撃	対抗策
1	なりすましによるユーザ情報への不正アクセス	・ユーザ認証の適切な適用 ・セキュリティ管理情報の保護管理の徹底
2	アクセス管理の不備を突いたユーザ情報への不正アクセス	・システムへの不正アクセス対策の徹底 ・セキュリティホール対策の徹底 ・ユーザ情報に対するアクセス制限の徹底
3	ウイルスによる攻撃	・ウイルス対策の徹底
4	業務やシステム運用上でのユーザ情報の取扱いの不備を突いた攻撃	・ユーザ情報の取扱いの厳正な運用
5	通信路上での攻撃	・通信路上のリスク対策の徹底

(参考) 個人情報の保護について

個人情報の取扱いに関しては、(注) に示すような各種のガイドライン等に以下に示すような制約が設けられている。

(1) 個人情報の収集に関する制約

「収集範囲の制限」「収集方法の制限」「特定機微な個人情報の収集の禁止」「情報主体から直接収集する場合の措置」「情報主体から間接的に収集する場合の措置」

(2) 個人情報の利用に関する制約

「利用の範囲の制限」「目的内の利用の場合の措置」「目的外の利用の場合の措置」

(3) 個人情報の提供に関する措置

「提供範囲の制限」「目的内の提供の場合の措置」「目的外の提供の場合の措置」

(4) 個人情報の適正管理義務

「個人情報の正確性の確保」「個人情報の利用の安全性の確保」「個人情報の秘密保持に関する従事者の責務」「個人情報の委託処理に関する措置」

(5) 管理体制の確立

「管理者の指名」「管理者の責務」

(注1) 個人情報の範囲について

個人情報とは、その法益として守られているプライバシー権の対象として捉える場合、その範囲は、『個人を識別し得る全ての情報』を指すことができる。

しかし、極めて広範な定義の中で、その情報が個人の私的領域に属する情報か否かの判別は非常に困難であるため、プライバシー権として保護される対象の範囲は、特定の産業や業種・業態によって、収集される情報の範囲で決定する必要がある。

例えば、平成 10 年 3 月に、ECOM が策定した「民間部門における電子商取引に係る個人情報の保護に関するガイドライン」によれば、「個人情報」の定義を以下の通り定めている。

「個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号、画像若しくは音声により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む）をいう。」

その他、消費者信用産業においては、与信審査に必要な収集情報を「個人信用情報」と定義し、その範囲を規定していたり、銀行・保険・証券等金融業界や電気事業連合会、（社）全国学習塾協会等　様々な分野の業種でそのガイドラインが設けられている。

(注2) 個人情報保護の背景

平成 10 年 11 月に内閣に設置された高度情報通信社会推進本部によって取りまとめられた「高度情報通信社会推進に向けた基本方針」の中で、個人情報保護について以下の通り記述されている。

「情報通信関連技術の発展により、電子化された情報を情報通信ネットワークを介して大量かつ迅速に処理することが可能となっており、また、蓄積、検索、利用、改竄も容易であることから、プライバシー保護の必要性が以前にも増して急速に高まっている。電子商取引等の発展には自由な情報流通が不可欠であるが、その前提として、プライバシーについては確実な保護が図られなければならない。」

(注3) 個人情報の保護を規定しているもの

① ＯＥＣＤ（Organization for Economic Co-operation and Development：経済協力開発機構）理事会勧告

－ プライバシー保護と個人データの国際流通についての理事会勧告（1980）

勧告は加盟国に対し、8原則（ガイドライン）を各国国内法の中で考慮することを求める一方、個人情報の国際流通に対する不当な阻害の回避を求めている。

② 国レベル

－ 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（1988）
公的部門（国の行政機関）のみを対象。

－ 個人情報保護法（法制化に向け検討中）
国、地方公共団体及びこれらに準ずる一定の者以外の事業を営む者を対象。

③ 地方公共団体レベル

都道府県、政令指定都市をはじめとして、各地方公共団体毎に個人情報条例が制定されている。

④ 自主規制（主なもの）

－ 民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン（1997 通産省）
－ 電気通信事業における個人情報保護に関するガイドライン（1998 郵政省）
－ 民間部門における電子商取引に係る個人情報の保護に関するガイドライン（1998 電子商取引実証推進協議会（ECOM））
－ 日本工業規格 個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001）
－ プライバシーマーク制度における監査ガイドライン（2000 （財）日本情報処理開発協会（JIPDEC））

（注4）ユーザデータの漏洩の事例

- A社（銀行）における顧客データ流出
  情報検索システムを開発していた派遣社員によって、氏名や勤務先など約2万人分の顧客情報が名簿業者に流れていた。
- B社（人材派遣会社）における派遣社員リスト流出
  業務委託先の社員によって、人材派遣会社に登録した女性派遣スタッフ約9万人分のデータが外部に漏洩した。
- C社（百貨店）における顧客データ流出
  友の会へ加入していた約50万人分の氏名や住所等顧客情報が、同社システム部社員によって持ち出され、名簿業者へ売り渡されていた。
- D社（製造業）ホームページ上で個人情報が閲覧可能
  商品の予約販売をインターネットで受付けたが、注文者に割り振った「受付番号」で、他人の個人情報が閲覧できる状態になっていた。

3.4 通信に対する攻撃の分析

3.4.1 通信路上のデータに対する攻撃とその対策

（1）通信路上の送受信データとは

表 3-16 に示すような、EC サイトがその業務運営上、外部とネットワークを介して授受するデータで、これらのデータは、伝送路や中継システム等の通信路上での

- 盗聴による情報の漏洩

- 情報の改ざん
- 通信事実の否認

から保護されなければならない。

表 3-16 EC サイトが扱う外部との送受信データの代表例

通信区分	情報の主権者	情報例
消費者－モール、ショップ間	取引情報	・商品情報 ・取引条件情報 ・発注情報 ・受注確認情報、契約情報
消費者－モール、ショップ間	その他情報	・会員登録等登録情報 ・パスワード等認証用情報 ・問い合わせ情報等一般情報
モール－ショップ間	取引情報	・商品情報 ・取引条件情報 ・受注確認情報、契約情報
	取引の管理に用いる情報	・会員登録等登録情報 ・パスワード等認証用情報 ・問い合わせ情報等一般情報
	ショップ運営情報	・HTML コンテンツ
ショップ－仕入先、物流業者等の業務取引先間	取引情報	・発注情報 ・受注確認情報、契約情報 ・その他取引付帯情報
	その他情報	・認証用情報

(2) ネットワークを介したデータの送受信にかかる脅威とその影響

表 3-17 にネットワークを介したデータの送受信に対する、攻撃手段と攻撃により発生が懸念されるトラブルを示す。

表 3-17　通信路上の送受信データに対する攻撃とその影響

項番	脅威	攻撃手段	発生が懸念されるトラブル
1	なりすまし	（3.2.1 節 参照）	（3.2.1 節 参照）
2	盗聴	・タッピング等通信路線信号の傍受 ・中継サイト内ネットワークでの盗聴 ・中継システムへの侵入による情報の不正入手 ・中継システムにおけるずさんな運用管理をついた情報の不正入手	・個人情報の漏洩 ・商業秘密情報の漏洩 ・パスワード等の流出によるなりすましによる不正取引等の発生
3	通信内容の改ざん（注１）	・中継システムへの不正アクセスによる情報の改ざん	・取引上の行き違いによるトラブルの発生
4	送信事実の否認（注２）	・送信側の悪意	・取引上のトラブルの発生（取引の有無に関わるトラブル）
5	受信事実の否認（注３）	・送信側の悪意	・取引上の行き違いによるトラブルの発生

(注1) 攻撃にはあたらないが、通信路の技術的なトラブルや運用の問題で、通信内容がこわれ、結果として通信内容が改ざんされることもある。
(注2) 攻撃にはあたらないが、送信側の誤解により、送信事実の否認が行われることもある。
(注3) 攻撃にはあたらないが、受信側の誤解により、受信事実の否認が行われることもある。

(3) ネットワークを介したデータの送受信にかかる脅威への対策

ネットワークを介したデータの送受にかかる脅威への対策を、表 3-18 に示す。

表 3-18　ネットワークを介したデータの送受にかかる脅威への対策

項番	脅威	対策	使用できる技術等
1	なりすまし	・相手認証の適切な適用 （3.2.1 節 参照）	（3.2.1 節 参照）
2	盗聴	・通信の暗号化 ・通信経路の専用線化	・SSL ・SET/SECE ・各種暗号ライブラリ ・暗号化メール ・VPN
3	通信内容の改ざん	・電子署名他の等改ざん検出機能の適用	・SSL
4	通信事実の否認	・通信ログの保管 ・否認防止技術の使用	・ルータ、ファイヤウォール、OS 等の通信路ログ取得機能 ・電子署名技術 ・SET/SECE ・暗号化メール

3.5 セキュリティ対策の構成と攻撃との関連

3.1 節、3.2 節、3.3 節、3.4 節の分析より、サイト運営上の脅威として検討の対象とすべき攻撃と、その対策との関連を整理すると表 3-19 のようになる。

表 3-19 攻撃と対策の関連

項番	攻撃の対象区分	攻撃の種類	セキュリティ対策としての施策テーマ
1	個々の商取引に対する攻撃	なりすましによる個別取引に対する攻撃	・ ユーザ認証の適切な適用
2	通信に対する攻撃	通信データに対する攻撃	・通信にかかるリスク対策 －通信路上のデータの保護 －否認対策
3		通信事実の否認	
4	システムに対する攻撃	システムへの侵入による攻撃	・ 不正アクセス対策
5		セキュリティホールをついた攻撃	・ セキュリティホール対策
6		ウイルスによる攻撃	・ ウイルス対策
7		DoS 攻撃	・DoS 攻撃対策(注1)
8	情報資産に対する攻撃	セキュリティ管理情報に対する攻撃	セキュリティ管理情報の保護管理
9		ユーザデータに対する攻撃	ユーザデータの保護管理

システムの運用を阻害するような攻撃は全て DoS 攻撃といえるが、ここでは SYN 攻撃等の狭義の DoS 攻撃と定義する。DoS 攻撃に対しての効果的な対策は、今後の課題とする。

4 EC サイトに求められるセキュリティ対策の体系と概要

4.1 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”、“セキュリティ事故への備え”に加えて、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確立”の合計11の施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 4-1 に示す。また、対策テーマ間の関連を表 4-1 に示す。

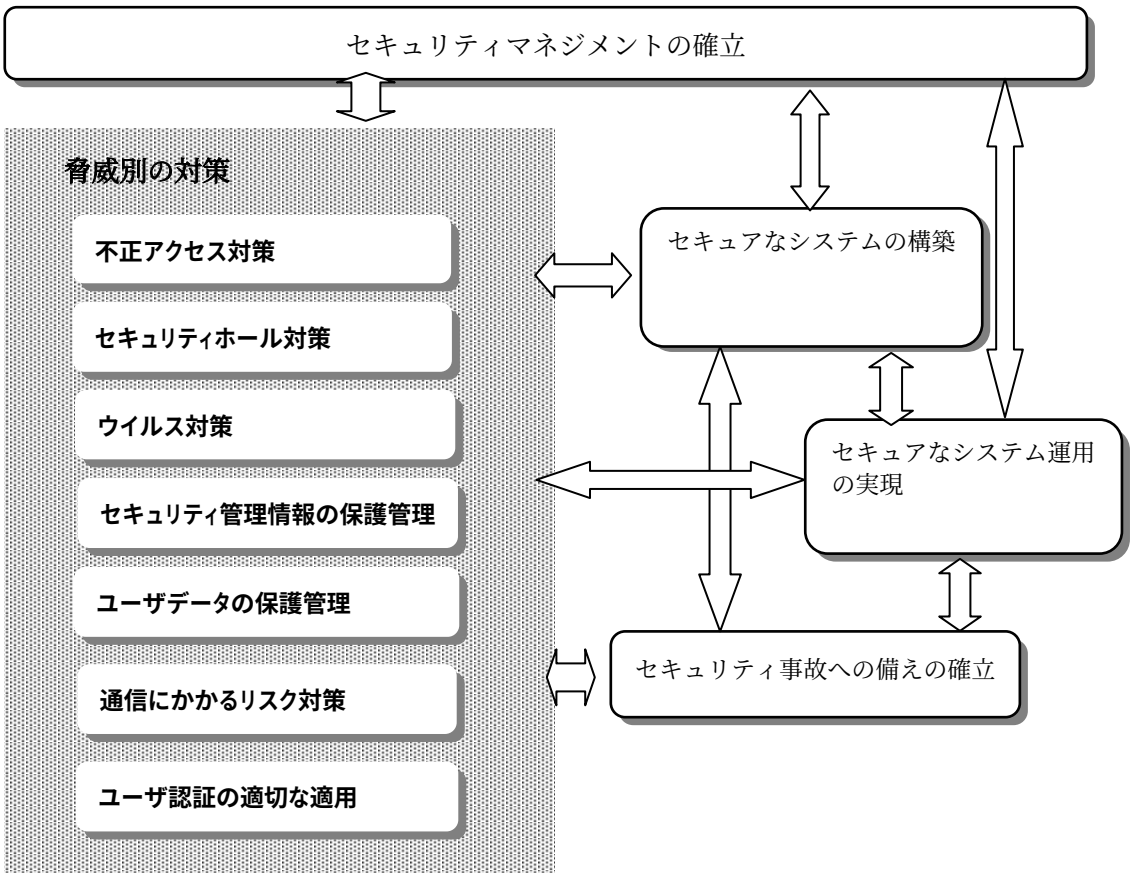

図 4-1　本ガイドラインにおける対策テーマの体系

表 4-1　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 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 セキュアなシステム運用の実現	11 セキュリティ事故への備えの確立	備考
1	セキュリティマネジメントの確立	＝＝＝											
2	不正アクセス対策	⇦	＝＝＝			⬅			⬅	⬅	⬅		
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	セキュアなシステム運用の実現	⇦	⇦	⇦	⇦	⇦	⇦	⇦	⇦	⇐	＝＝＝	⇦	
11	セキュリティ事故への備えの確立	⇦	⇦	⇦	⇦	⇦	⇦	⇦	⇦	⇐	⇐	＝＝＝	

⇦ 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

4.2 セキュリティマネジメントの確立

4.2.1 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
- 適切なセキュリティ対策の構築
- 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。

4.2.2 セキュリティマネジメント確立のための施策の構成

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) セキュリティ対策推進体制の確立
(3) スタッフのセキュリティの確立
(4) サイト運営にかかわる外部組織の協力の確保
(5) セキュリティ対策予算の確保
(6) サイト運営関係者に対するセキュリティ教育の実施
(7) サイト運営に対するセキュリティ監査の実施

4.2.3 各施策の概要

4.2.3.1 サイト運営上のセキュリティポリシーの確立

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、さまざまな活動の積上げがあって始めて達成されるものである。

これらの活動を組織的に計画されたものにするためには、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を示したサイトに運営全体にかかわるセキュリティポリシーが確立されていなければならない。また、このセキュリティポリシーは、サイトの運営にかかわる者全員に徹底されていなければならない。

(1) サイト運営上のセキュリティポリシーの確立と宣言
(2) セキュリティポリシーの発行とその見直しプロセスの確立
(3) セキュリティポリシーの見直しの実施
(4) セキュリティポリシーの関係者への徹底

4.2.3.2 セキュリティ対策推進体制の確立

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。

(1) 経営陣の参画とその責任の明確化
(2) セキュリティ対策の実施責任者とその責任の明確化
(3) 関係者間の連携体制の確立

4.2.3.3 スタッフのセキュリティの確立

サイトのセキュリティは、従業員や外部からの派遣要員等のサイトの運営にかかわる日常の業務における行動や、セキュリティ対策にかかる活動に依存している。サイトの運営にかかわるスタッフが、サイトにおけるセキュリティ要求事項を遵守し、スタッフがサイトのセキュリティの脅威にならないようにするためには、スタッフについてのセキュリティの確立も重要な課題である。

(1) サイトの運営関係者から不適格者の排除
(2) サイト運営にかかわる者に対するセキュリティポリシー遵守についての徹底
(3) セキュリティ要求事項違反に対する懲戒制度の導入
(4) サイトへの一時立入り要員に対するセキュリティの確保

4.2.3.4　サイト運営にかかわる外部組織の協力の確保

一部業務の委託、サポート要員の派遣等、サイトの運営に他社のサポートがかかわっていることが多い。このよう場合、これらの関係他社に対しても、業務の委託や派遣要員の受入れが、サイトのセキュリティ上の脅威にならないようにするための必要な協力を得なければならない。

(1) 業務委託先に対するセキュリティ要求事項とその責任の明確化
(2) 業務委託先に対するセキュリティ要求事項への対応状況についての監督、指導の実施
(3) 要員派遣元に対する責任の明確化
(4) 問題が生じた場合における責任の追及の実施

4.2.3.5　セキュリティ対策予算の確保

セキュリティ対策にはコストがかかる。定めれれたセキュリティ対策にかかる諸施策が機能するようにするためには、セキュリティポリシーを実現するための具体策の実施に必要な予算は確保されなければならない。

このためには、サイトの経営コストの中でセキュリティ対策費が意識され、適切に審議されるようになっていなければならない。

(注) 現時点ではセキュリティ対策予算は、システムの導入費やシステム運用費の中に含まれ計上されているのが一般で、セキュリティ対策にかかる予算をまとめ、個別審議している組織は、少ないと見られている。

(1) セキュリティ対策予算の明確化
(2) セキュリティ対策予算の審議プロセスの確立

4.2.3.6　サイト運営関係者に対するセキュリティ教育の実施

サイト運営におけるセキュリティの確保は、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、その確実な遂行に依存する。

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が必要となる。

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にかかる施策も必要となる。

(1) サイト運営関係者全員に対する定期的なセキュリティ教育の実施

(2) 管理者に対するセキュリティマネジメント教育の実施
(3) 新規参加者に対する就業前のセキュリティ教育の実施

4.2.3.7 サイト運営に対するセキュリティ監査の実施

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。

(1) 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の実施
(2) セキュリティ要求事項の実施状況についての監査の実施
(3) セキュリティ監査実施要領の確立
(4) セキュリティ監査実施体制の確立

4.3 不正アクセス対策の概要

4.3.1 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、業務やシステム運用の混乱につながるシステムの機能の不正な使用、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に対する破壊、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、

- 万一、システムへの不正なアクセス（侵入）を許したときの被害の極小化

を行うものである。

4.3.2 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）不正アクセス対策ポリシーの確立
（2）不正アクセス対策についての責任体制の確立
（3）データフロー制御・監視要件とその実現方式の適切な指定
（4）個々のシステム（サーバ）に対するアクセス制御・監視要件の適切な指定
（5）個々のサービスに対するアクセス制御・監視要件の適切な指定
（6）個々のシステム（サーバ）に対するサービス搭載要件の適切な指定
（7）システムの構成や機能の実装への不正アクセス対策の反映
（8）不正アクセス事故への備えの確立
（9）システム運用への不正アクセス対策の反映
（10）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
（11）不正アクセス対策の実施状況についての定期的なチェックの実施

4.3.3 求める施策の概要

4.3.3.1 不正アクセス対策ポリシーの確立

システムへの不正なアクセスの阻止を図るとともに、万一、不正なアクセス（侵入）を許した時の被害を限定的なものにするためには、実施する不正アクセス対策が効果的なものでなければならない。このためには、戦略的で組織的な取組みが必要であり、不正アクセス対策を、どのような考えで、またどのような方法で実施するのかを明らかにする不正アクセス対策ポリシーが確立され、関係者にこれが周知されていなければならない。

不正アクセス対策ポリシーの中で明らかにすべき事項としては、以下があげられる。

- 不正アクセス対策についての基本方針
- 不正アクセス対策の組立て
- 対策の適用範囲
- アクセス制御・監視ポリシーとアクセス制御や監視の実施についての基準
- システム（サーバ）に対するサービスの搭載についての基準

(注) サイトへの不正アクセスとは、サイトの利用を許されていない者によるネットワークおよびシステム（サーバ）へのアクセス、またはサイトの利用者に与えられた権限によって許された範囲を超えた(本来許されない)システムの利用等の行為を、ネットワークを介して意図的に行うことをいう。

(1) 不正アクセス対策についての基本方針の明確化
(2) 不正アクセス対策の組立ての明確化
(3) 適用範囲の明確化
(4) アクセス制御・監視ポリシーの確立
(5) データフロー制御・監視基準の確立
(6) システム（サーバ）に対するアクセス制御・監視基準の確立
(7) サービス（アプリケーション）におけるアクセス制御・監視基準の確立
(8) システム(サーバ)に対するサービス搭載基準の確立
(9) 不正アクセス対策ポリシーの関係者への周知
(10) 必要に応じた不正アクセス対策ポリシーの見直しの実施

4.3.3.2 不正アクセス対策についての責任体制の確立

不正アクセス対策が期待通りに機能するためには、不正アクセス対策として定められたことが、ネットワークやシステムの構築およびシステムの運用に確実に反映されるようにするための体制が必要となる。

このためには、不正アクセス対策にかかわるさまざまなタスクとその実施に責任を持つ者を明確にするとともに、関係者間の連携体制を確立しておくことが必要となる。

(1) 不正アクセス対策にかかるタスクの明確化
(2) 不正アクセス対策にかかるタスクの実施責任者の明確化
(3) 不正アクセス対策関係者間の連携の確立
(4) 責任体制の周知徹底
(5) 必要に応じた責任体制についての見直しの実施

4.3.3.3 データフロー制御・監視要件とその実現方式の適切な指定

サイトと外部ネットワークとのデータフローならびにサイト内のデータフローに対する制御や監視は、サイト内に置かれたシステム（サーバ）への不正なアクセスを防ぐための第一のバリアである。

サイトが扱うデータフローに対する制御や監視を適切に行うためには、データフローに対する制御および監視についての具体的な要求を、データフロー制御・監視ポリシーに沿って適切に指定しなければならない。

(1) データフロー制御・監視要件の指定
(2) データフローの制御および監視の実現方式の指定
(3) 使用するデータフロー制御機能や監視機能におけるパラメータ等についての設定要件の指定
(4) 必要に応じたデータフロー制御・監視要件や実現方式の指定の見直しの実施

4.3.3.4 個々のシステム(サーバ)に対するアクセス制御・監視要件の適切な指定

自システム(サーバ)に置かれている機能や情報等のシステム資産への不正なアクセスを防ぐためには、各システムは権限のない者に対しログインの拒否を行わなければならない。このことを適切に行うためには、ＯＳレベルのアクセス制御機能やアクセス監視機能をどのように用いるかを適切に指定しなければならない。

このためには、サイトに置かれるシステムの個々に対し、システム使用権限やシステムリソースに対するアクセス権の設定やアクセス要求者の認証等についての要求を適切に指定しなければならない。

(1) 個々のシステムに対するアクセス制御・監視要件の指定
(2) 必要に応じた個々のシステムに指定したアクセス制御・監視要件の見直しの実施

4.3.3.5 個々のサービスに対するアクセス制御・監視要件の適切な指定

ネットワークレベルやＯＳレベルでのアクセス制御では対応できないサービス特有の(アプリケーションレベルでの)の当該サービスに対するきめの細かいアクセスの制御や監視は、各サービス(アプリケーション)が自らの手で行わなければならない。このため、アプリケーションレベルでのアクセス制御やアクセス監視が必要なサービスに対しては、個別サービスにおけるアクセス制御・監視基準にもとづき、サービス個々に必要なアクセス制御やアクセス監視を指定しなければならない。

(1) 個々のサービスに対するアクセス制御・監視要件の指定
(2) 必要に応じたサービスの個々に指定したアクセス制御・監視要件の見直しの実施

4.3.3.6 個々のシステム（サーバ）に対するサービス搭載要件の適切な指定

システム（サーバ）に搭載しているサービス（アプリケーション）やソフトウェアがシステムへの不正なアクセスの足掛かりに使われないようにしなければならない。アクセス制御やアクセス監視の管理対象外の運用に使用されないサービスやソフトウェアが管理されずに稼動状態におかれたままシステムに放置されないようにすることと、その機能や構造的な特徴から攻撃の足掛かりになり易いサービスやソフトウェアは、その使用にあたっては厳重な管理が必要がある。

これらのことを適切に行うためには、システムに対するサービス搭載基準にもとづき、サイトシステムに置かれるシステムの個々に対し、そのサイト内での役割やネットワーク上での位置等を配慮した搭載するサービスについての制限に関する指定を適切にを行わなければならない。

また、各システムでこの指定にもとづきサービスの搭載が管理されなければならない。

（1）個々のシステムに対する搭載するサービスやソフトウェアについての要件の指定
（2）使用しないサービスやソフトウェアの除去または停止処理の点検の実施
（3）必要に応じたサービス搭載要件の指定の見直しの実施

4.3.3.7 システムの構成や機能の実装への不正アクセス対策の反映

不正アクセス対策の実行には、以下に示すような技術（プロダクト）・機能が用いられる。

- データフローの制御する技術・機能
- システム(サーバ)へのアクセスを制限する技術・機能
- アクセス管理の脆弱性を検査する技術・機能
- データフローやサイトシステムへのアクセスを監視する技術・機能

これらが、不正アクセス対策が求める役割を果たすようにするためには、不正アクセス対策の実施に必要な技術・機能についての要件が適切に指定され、開発、導入、維持管理を担当する者にに伝えられ、それらの機能の配置等のシステム構成や諸機能の実装に的確に反映されなければならない。

このため、不正アクセス対策の立場からも、それらがシステムに的確に実装され期待通りに機能するようになっていることについて確認することも必要である。

(注) ここで指定された使用する技術・機能のシステムへの実装は、システムの構築と維持管理の問題となる。第9章の**“セキュアなシステムの構築”**を参照。

（1）不正アクセス対策に用いる技術・機能要件の指定
（2）指定した技術・機能の実装についての確認の実施

(3) 必要に応じた技術･機能要件の指定の見直しの実施

4.3.3.8 不正アクセス事故への備えの確立

サイトシステムへの不正アクセスの阻止に努力していても、対策実施上の不備や新しい攻撃手段を考えると、不正アクセスの阻止に保証はなく、サイトシステムが侵入を許す可能性は常にあると考えておかなければならない。

システムへの不正アクセス事故(侵入事故)が発生した場合は、

- システムへの不正アクセスにより改ざんまたは破壊されたシステムの復旧
- 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処置の実施
- 不正アクセスを許した原因の除去
- 関係機関への連絡

等が適切に行われなければならない。

システムへの不正アクセス事故が発生した場合、これらのことが迅速かつ適切に行われるようにするためには、このような事故に対して必要となる処置についての十分な研究にもとづいた手順の確立や、その実行のために必要となるシステムのバックアップやシステムの運用記録の確保、必要なツールの準備等の備えが必要となる。

このため、不正アクセス事故の処理に必要となる備えについての要求を明確にするとともに、それらがシステムの構成や運用に適切に反映されていることを確認することも必要となる。

(注) ここで指定される不正アクセス事故への備えについての要求は、第12章に示す**“サイト全体としてのセキュリティ事故対策への備え”**に対する要求となり、他の脅威に対する事故への備えと統合され、システムの構成や運用へ反映される。

(1) 不正アクセス事故の処理に必要な備えについての要求の明確化
(2) 要求事項のシステム構成やシステム運用への反映状況について確認の実施
(3) 必要に応じた要求事項についての見直しの実施

4.3.3.9 システム運用への不正アクセス対策の反映

不正アクセス対策として定めた諸施策が有効に機能するためには、それらがシステムの構成やシステムの運用に的確に反映されなければならない。

不正アクセス対策からのシステム運用への要求が、日々の運用において的確に実施されるようにするためには、不正アクセス対策がシステム運用に求めていることを明確にし、それらがシステム

運用の中に適切に組込まれるようにしなければならない。

⑴ 不正アクセス対策からのシステム運用への要求の明確化
⑵ 要求事項のシステム運用への組込みについての確認の実施
⑶ システム運用における要求事項の実行状況についてのチェックの実施
⑷ 必要に応じたシステム運用への要求についての見直しの実施

4.3.3.10 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

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、不正アクセス対策を担当する者やシステムの管理や運用にかかわる者が、これらについての十分な認識と理解を持っていることが必要となる。

このため、不正アクセス対策に責任を持つ者だけでなく、システムの構築、管理、運用等で不正アクセス対策にかかわる業務に携わる者に対しても、不正アクセスの脅威とその対策について必要な教育を行うことが求められる。

⑴ 不正アクセス対策についての教育の実施
⑵ 関係者の不正アクセス対策の実施に必要なスキルの確保

4.3.3.11 不正アクセス対策の実施状況についての定期的なチェックの実施

不正アクセス対策が定められていても、それらがサイトの運営実態に照らして適切であり、かつ、確実に実行されていなければ、期待した不正アクセス対策は実現しない。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、不正アクセス対策として定められていることが確実に実施されているかどうか等について定期的にチェックを行い、問題点の発掘と指摘された問題に対する改善を行うことが必要である。

⑴ 不正アクセス対策の実施状況についての定期的なチェックの実施
⑵ 必要に応じた不正アクセス対策の実施状況についての臨時チェックの実施
⑶ 指摘事項のフィードバックの実施

4.4 セキュリティホール対策の概要

4.4.1 セキュリティホール対策とは

サイトシステムのソフトウェアにあるセキュリティホールは、システムの機能の不正な使用、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をついた攻撃を呼ぶ。

セキュリティホール対策とは、このような被害を生じさせかねないセキュリティホール攻撃からサイトシステムを守るため、

- システムからの既知のセキュリティホールの除去
- システムに残された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。

4.4.2 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対策ポリシーの確立
(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セキュリティホール対策要件の適切な指定
(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) 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) システムの構成や機能の実装へのセキュリティホール対策の反映
(9) セキュリティホール攻撃による事故への備えの確立
(10) システム運用へのセキュリティホール対策の反映
(11) 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チェックの実施

4.4.3 求める施策の概要

4.4.3.1 セキュリティホール対策ポリシーの確立

セキュリティホールをついた攻撃による外部からのシステムの不正な操作、情報の不正な取得、

ソフトウェアや情報の改ざん、破壊被害を防ぐとともに、万一、このようなセキュリティホール攻撃を許したとしても、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明らかにするセキュリティホール対策ポリシーが確立され、関係者にこれが周知されていなければならない。

- セキュリティホール対策についての基本方針
- セキュリティホール対策の組立て
- 対策の適用範囲

(1) セキュリティホール対策についての基本方針の明確化
(2) セキュリティホール対策の組立ての明確化
(3) 適用範囲の明確化
(4) セキュリティホール対策実施基準の確立
(5) セキュリティホール対策ポリシーの関係者への周知
(6) 必要に応じたセキュリティホール対策ポリシーの見直しの実施

4.4.3.2 セキュリティホール対策についての責任体制の確立

セキュリティホール対策が期待通りに機能するためには、セキュリティホール対策として定められたことが、ネットワークやシステムの構築およびシステムの運用に確実に反映されるようにするための体制が必要となる。

このためには、セキュリティホール対策にかかわるさまざまなタスクとその実施に責任を持つ者を明確にするとともに、関係者間の連携体制を確立しておくことが必要となる。

(1) セキュリティホール対策にかかるタスクの明確化
(2) セキュリティホール対策にかかるタスクの実施責任者の明確化
(3) セキュリティホール対策関係者間の連携の確立
(4) 責任体制の周知徹底
(5) 必要に応じた責任体制の見直しの実施

4.4.3.3 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

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。

このことが適切に行われるようにするためには、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も必要となる。

(1) セキュリティホールに関する情報の収集・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
(3) 必要に応じたセキュリティホールに関する情報の収集とその処理についての見直しの実施

4.4.3.4 対策実施単位の個々に対するセキュリティホール対策要件の適切な指定

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ウェア(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。

(1) 対策実施単位の編成
(2) 対策実施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
(3) 必要に応じたセキュリティホール対策実施単位の編成や対策実施単位の個々に指定したセキュリティ対策要件の見直しの実施

4.4.3.5 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

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。

(1) セキュリティホール対策からのソフトウェアのインストールに関するルールの確立
(2) 適切なバージョンの選択
(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
(6) セキュリティホール発見時の適切な処置の実施

4.4.3.6 システムに対するセキュリティホール検査の実施

セキュリティホール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減らす努力が必要となる。

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。

(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

4.4.3.7 セキュリティホールをついた攻撃に対する監視の実施

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でセキュリティホールを見逃し、セキュリティホールをついた攻撃による被害を受ける可能性もある。

このような被害を受けないためには、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監視し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。

(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

4.4.3.8 システムの構成や機能の実装へのセキュリティホール対策の反映

セキュリティホール対策の実行には、以下に示すような技術（プロダクト）・機能が用いられる。

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

これらが、セキュリティホール対策が求める役割を果たすようにするためには、セキュリティホール対策の実施に必要な技術・機能についての要件が適切に指定され、開発、導入、維持管理チームに伝えられ、それらの機能の配置等のシステム構成や諸機能の実装に的確に反映されなければならない。

このため、セキュリティホール対策の立場からも、それらがシステムに的確に実装され期待通りに機能するようになっていることについて確認することも必要である。

(注) ここで指定された使用する技術・機能のシステムへの実装は、システムの構築と維持管理の問題となる。第9章の**“セキュアなシステムの構築”**を参照。

(1) セキュリティホール対策に用いる技術・機能要件の明確化
(2) 指定した技術・機能の実装についての確認の実施
(3) 必要に応じた技術・機能要件の指定についての見直しの実施

4.4.3.9 セキュリティホール攻撃による事故への備えの確立

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有害プログラムの除去
- 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。

セキュリティホール攻撃によりシステム埋込まれた有害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、これらのことが迅速かつ適切に行われるようにするためには、このような事故に対して必要となる処置についての十分な研究にもとづ

いた手順の確立や、その実行のために必要となるシステムのバックアップやシステムの運用記録の確保、必要なツールの準備等の備えが必要となる。

このため、このような事故の処理に必要となる備えについての要求を明確にするとともに、それらがシステムの構成や運用に適切に反映されていることを確認することも必要となる。

(注) ここで指定されるセキュリティホール攻撃による事故への備えについての要求は、第12章に示す**“サイト全体としてのセキュリティ事故対策への備え”**に対する要求となり、他の脅威に対する事故への備えと統合され、システムの構成や運用へ反映される。

(1) セキュリティホール攻撃による事故の処理に必要な備えについての要求の明確化
(2) 必要に応じた要求事項についての見直しの実施

4.4.3.10 システム運用へのセキュリティホール対策の反映

セキュリティホール対策として定めた諸施策が有効に機能するためには、それらがシステムの構成やシステムの運用に的確に反映されなければならない。

セキュリティホール対策からのシステム運用への要求が、日々の運用において的確に実施されるようにするためには、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を明確にし、それらがシステム運用の中に適切に組込まれるようにしなければならない。

(1) セキュリティホール対策からのシステム運用への要求の明確化
(2) 要求事項のシステム運用への組込みについての確認の実施
(3) システム運用におけるセキュリティホール対策の実行状況についてのチェックの実施
(4) 必要に応じたシステム運用への要求の見直しの実施

4.4.3.11 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チェックの実施

セキュリティホール対策が定められていても、それらがサイトの運営実態に照らして適切であり、かつ、確実に実行されていなければ、期待したセキュリティホール対策は実現しない。このため、定められているセキュリティホール対策がサイトの運営実態に照らして適切かどうか、セキュリティホール対策として定められていることが確実に実施されているかどうか等について定期的にチェックを行い、問題点の発掘と指摘された問題に対する改善を行うことが必要である。

(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チェックの実施
(2) 必要に応じたセキュリティホール対策の実施状況についての臨時チェックの実施
(3) 指摘事項のフィードバックの実施

4.5 ウイルス対策の概要

4.5.1 ウイルス対策とは

ウイルス対策とはシステム上のソフトウェアや情報の破壊や、勝手な処理の実行による業務やシステムの運用の混乱、さらには他サイトへのウイルスの伝染等につながるウイルス感染からサイトシステムを守るための、

- サイトシステムのウイルス感染の防止
- ウイルス感染時の被害の極小化

を行う施策の総称をいう。

4.5.2 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) ウイルス対策ポリシーの確立
(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) ネットワークからのウイルスの侵入の阻止
(5) インストールするソフトウェアからのウイルスの侵入の阻止
(6) FD 等の持込みファイルからのウイルス侵入の阻止
(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) システムの構成や機能の実装へのウイルス対策の反映
(10) ウイルス感染事故への備えの確立
(11) システム運用へのウイルス対策の反映
(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定期的なチェックの実施

4.5.3 求める施策の概要

4.5.3.1 ウイルス対策ポリシーの確立

サイトシステムにウイルスが侵入したりトロイの木馬が持込まれたりすることの阻止を図るとともに、これらの有害プログラムの侵入による被害を限定的なものにすることに組織的に取組むには、ウイルス対策(注)をどのような考えで、またどのような方法で実施するかを明らかにするウイルス対策ポリシーが確立され、ウイルス対策を担当する者だけでなく、システムの管理者や内部利用者等サイト内部でシステムに触れる者のすべてにこれが周知されていなければならない。

ウイルス対策ポリシーで明らかにしておくべき事項としては、以下があげられる。

- ウイルス対策についての基本方針
- ウイルス対策の組立てについての考え方
- 対策の適用範囲

(注) 本ガイドラインでのウイルス対策にはトロイの木馬等のシステムに持込まれる有害プログラムのすべてをその対象とする。ただし、セキュリティホールをついた有害プログラムのシステムの埋込みについては、第 4 章の**“セキュリティホール対策”**で取扱っている。

(1) ウイルス対策についての基本方針の明確化
(2) ウイルス対策の組立ての明確化
(3) 適用範囲の明確化
(4) ウイルス対策ポリシーの関係者への周知
(5) 必要に応じたウイルス対策ポリシーの見直しの実施

4.5.3.2 ウイルス対策についての責任体制の確立

ウイルス対策が期待通りに機能するためには、ウイルス対策として定められたことが、ネットワークやシステムの構築およびシステムの運用に確実に反映されるようにするための体制が必要となる。

このためには、ウイルス対策にかかわるさまざまなタスクとその実施に責任を持つ者を明確にするとともに、関係者間の連携体制を確立しておくことが必要となる。

(1) ウイルス対策にかかるタスクの明確化
(2) ウイルス対策にかかるタスクの実施責任者の明確化
(3) ウイルス対策関係者間の連携の確立
(4) 責任体制の周知徹底

⑸ 必要に応じた責任体制についての見直しの実施

4.5.3.3 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必要となる。

このことを適切に行うためには、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。

⑴ ウイルスに関する情報の収集・処理要領の確立
⑵ 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
⑶ 必要に応じたウイルスに関する情報の収集とその処理についての見直しの実施

4.5.3.4 ネットワークからのウイルスの侵入の阻止

サイトシステムへのウイルスの侵入は、メールやメールの添付ファイルあるいはダウンロードするデータやソフトウェアに付着したウイルスによることが多い。このため、外部ネットワークとの接点や内部ネットワークを流れるデータに対するウイルスの監視や、サービスの入口での受信データに対するウイルスの監視によるウイルスの侵入阻止は、ウイルス対策の基本となるものである。

ネットワークからのウイルスの侵入の阻止を適切に行うためには、侵入を試みるウイルスに対し、監視と排除を行うバリアの構成方針が適切に決められ、このバリアの構成方針に沿ったウイルス対策ソフトウェアの配置等が適切に行われなければならない。

⑴ ウイルス侵入監視バリア構成の確立
⑵ 各バリアに対するウイルス監視要件の指定
⑶ 各バリアに指定したウイルス監視要件の実装の確認の実施
⑷ 必要に応じたバリア構成と各バリアに指定したウイルス監視要件の見直しの実施

4.5.3.5 インストールするソフトウェアからのウイルスの侵入の阻止

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

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、ウイルス対策ソフトウェア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有害プログラムがシステムに持込まれるのを阻止するため、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。

(1) ウイルス対策の視点からのソフトウェアのインストール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) 必要に応じたソフトウェアのインストールについてのルールの見直しの実施
(6) ウイルス発見時の適切な処置の実施

4.5.3.6 FD 等の持込みファイルからのウイルスの侵入の阻止

電子媒体上のデータ等ネットワーク以外のルートからでもウイルスに感染する危険性がある。このため、ウイルスが付着したファイルから、システムにウイルスが侵入しないよう、FD 等により外部からの持込みファイルに対しては、受取時やその処理を行う前に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、またはファイルそのものの破棄等を行わなければならない。

(1) ウイルス対策の視点での外部からの持込みファイルの取扱いについてのルールの確立
(2) 外部から持込まれたファイルに対する素性確認の実施
(3) 外部から持込まれたファイル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) 必要に応じた持込みファイルに対するウイルス対策についての見直しの実施
(6) ウイルス発見時の適切な処置の実施

4.5.3.7 システムに対するウイルス検査の実施

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ファイル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、サイトの全領域を対象に定期的あるいは必要が生じた都度ウイルス検査を実施する必要がある。このとき一箇所でも感染を見逃すと、再度サイト全域が感染の脅威にさらされ、せっかくの検査や駆除等の対策を無意味なものにするため、この検査は綿密な計画ももとに十分に管理されて行わなければならない。

(1) ウイルス検査実施単位の編成
(2) 個々の検査実施理単位に対するウイルス検査要件の指定
(3) 検査実施単位ごとに指定したウイルス検査要件のシステム構成やシステムの運用への反映状況についての確認の実施
(4) 定期的なウイルス検査の実施
(5) 必要に応じた臨時のウイルス検査の実施
(6) 実施したウイルス検査についての記録と保管
(7) 必要に応じたウイルス検査実施単位の編成や個々の実施単位に指定した検査要件の見直しの実施
(8) ウイルス発見時の適切な処置の実施

4.5.3.8 ウイルス感染ファイルの外部への持出しの防止

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。

(1) ウイルス対策の視点からの外部持出しファイルの取扱いに関するルールの確立
(2) 外部に持出すファイル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) 必要に応じた外部持出しファイルに対するウイルス検査についてのルールの見直しの実施
(5) ウイルス発見時の適切な処置の実施

4.5.3.9 システムの構成や機能の実装へのウイルス対策の反映

ウイルス対策の実行には、以下に示すような技術(プロダクト)・機能が用いられる。

- 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、駆除する技術･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技術･機能

これらが、ウイルス対策が求める役割を果たすようにするためには、ウイルス対策の実施に必要な技術･機能についての要件が適切に指定され、開発、導入、維持管理チームに伝えられ、それらの機能の配置等のシステム構成や諸機能の実装に的確に反映されなければならない。

このため、ウイルス対策の立場からも、それらがシステムに的確に実装され期待通りに機能するようになっていることについて確認することも必要である。

(注) ここで指定された使用する技術･機能のシステムへの実装は、システムの構築と維持管理の問題となる。第9章の**“セキュアなシステムの構築”**を参照。

⑴ ウイルス対策に用いる技術･機能要件の指定
⑵ 指定した技術･機能の実装についての確認の実施
⑶ 必要に応じたウイルス対策に用いる技術･機能要件の指定の見直しの実施

4.5.3.10 ウイルス感染事故への備えの確立

ウイルスの侵入の阻止に努めていても、侵入阻止策やその実施上の不備や、新しいウイルスの登場等で、ウイルスの侵入阻止に完全はなく、システムはいつでもウイルスに侵入されうると考えておかなければならない。

システムにウイルスが侵入した場合は、

- 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

等が適切に行われなければならない。

システムにウイルス感染事故が発生した場合、これらのことが迅速かつ適切に行われるようにするためには、このような事故に対して必要となる処置についての十分な研究にもとづいた手順の確立や、その実行のために必要となるシステムのバックアップやシステムの運用記録の確保、必要なツールの準備等の備えが必要となる。

このため、システムのウイルス感染事故の処理に必要となる備えについての要求を明確にするとともに、それらがシステムの構成や運用に適切に反映されていることを確認することも必要となる。

(注) ここで指定されるウイルス感染事故への備えについての要求は、第12章に示す**“サイト全体としてのセキュリティ事故対策への備え”**に対する要求となり、他の脅威に対する事故への備えと統合され、システムの構成や運用へ反映される。

⑴ ウイルス感染事故の処理に必要な備えについての要求の明確化

⑵ 要求事項のシステム構成やシステム運用への反映状況についての確認の実施
⑶ 必要に応じた要求事項についての見直しの実施

4.5.3.11 システム運用へのウイルス対策の反映

ウイルス対策として定めた諸施策が有効に機能するためには、それらがシステムの構成やシステムの運用に的確に反映されなければならない。

ウイルス対策からのシステム運用への要求が、日々の運用において的確に実施されるようにするためには、ウイルス対策がシステム運用に求めていることを明確にし、それらがシステム運用の中に適切に組込まれるようにしなければならない。

⑴ ウイルス対策からのシステム運用への要求の明確化
⑵ 要求事項のシステム運用への組込みについての確認の実施
⑶ システム運用における要求事項の実行状況についてのチェックの実施
⑷ 必要に応じたシステム運用への要求についての見直しの実施

4.5.3.12 関係者に対するウイルス対策についての教育の実施

ウイル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、ウイルス対策を担当する者やシステムの管理や運用にかかわる者に加え、業務等でシステムにアクセスする内部ユーザにおいても、これらについての十分な認識と理解が必要となる。

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、管理、運用にかかわる者、およびシステムの内部利用者のすべてに対し、ウイルスの脅威とその対策について必要な教育を行うことが求められる。

⑴ ウイルス対策についての教育の実施
⑵ 関係者のウイルス対策の実施に必要なスキルの確保

4.5.3.13 ウイルス対策の実施状況についての定期的なチェックの実施

ウイルス対策が定められていても、それらがサイトの運営実態に照らして適切であり、かつ、確実に実行されていなければ、期待したウイルス対策は実現しない。このため、定められているウイルス対策はサイトの運営実態に照らして適切かどうか、ウイルス対策として定められていることが確実に

実施されているかどうか等について定期的にチェックを行い、問題点の発掘と指摘された問題に対する改善を行うことが必要である。

⑴ ウイルス対策の実施状況についての定期的なチェックの実施
⑵ 必要に応じたウイルス対策の実施状況についての臨時チェックの実施
⑶ 指摘事項のフィードバックの実施

4.6 セキュリティ管理情報保護管理策の概要

4.6.1 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、サイトのセキュリティ確保の要でもあるセキュリティ管理情報に、

- 漏洩
- 改ざん
- 破壊

が生じないようにする施策と、万一、漏洩、改ざん、破壊事故が発生し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。

4.6.2 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。

⑴ セキュリティ管理情報の保護管理ポリシーの確立
⑵ 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
⑶ 個々のセキュリティ管理情報に対する保護管理要件の適切な指定
⑷ システムの構成や機能の実装へのセキュリティ管理情報保護管理策の反映
⑸ 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確立
⑹ 業務やシステムの運用へのセキュリティ管理情報保護管理策の反映
⑺ 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
⑻ 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
⑼ 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

(10) 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チェックの実施

4.6.3 求める施策の概要

4.6.3.1 セキュリティ管理情報の保護管理ポリシーの確立

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な取組みを行うには、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に関し、以下のような事項を明らかにするセキュリティ管理情報保護管理ポリシーが確立され、関係者にこれが周知されていなければならない。

- セキュリティ管理情報の保護管理についての基本方針
- セキュリティ管理情報の保護管理策の組立て
- 保護管理策の適用範囲
- セキュリティ管理情報の保護管理実施基準

(1) セキュリティ管理情報の保護管理についての基本方針の明確化
(2) セキュリティ管理情報の保護管理策の組立ての明確化
(3) 適用範囲の明確化
(4) セキュリティ管理情報の保護管理実施基準の確立
(5) セキュリティ管理情報の保護管理ポリシーの関係者への周知
(6) 必要に応じたセキュリティ管理情報の保護管理ポリシーの見直しの実施

4.6.3.2 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

セキュリティ管理情報の保護管理策が期待通りに機能するためには、セキュリティ管理情報の保護管理策として定められたたことが、ネットワークやシステムの構築およびシステムの運用に確実に反映されるようにするための体制が必要となる。

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さまざまなタスクとその実施に責任を持つ者を明確にするとともに、関係者間の連携体制を確立しておくことが必要となる。

(1) セキュリティ管理情報の保護管理にかかるタスクの明確化
(2) セキュリティ管理情報の保護管理にかかるタスクの実施責任者の明確化
(3) セキュリティ管理情報の保護管理関係者間の連携の確立

(4) 責任体制の周知徹底
(5) 必要に応じた責任体制についての見直しの実施

4.6.3.3 個々のセキュリティ管理情報に対する保護管理要件の適切な指定

セキュリティ管理情報の保護管理実施基準に従って適用される保護管理レベル、その保護管理レベルを満足するための方式、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を指定する。

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。4.6.3.7 節**“セキュリティ管理情報にかかわる印刷物、電磁媒体の適切な取扱いの実施”**を参照。

(1) 保護対象のセキュリティ管理情報の洗出し
(2) 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
(3) 必要に応じたセキュリティ管理情報の個々に指定した保護管理要件の見直しの実施

4.6.3.4 システムの構成や機能の実装へのｾｷｭﾘﾃｨ管理情報保護管理策の反映

セキュリティ管理情報の保護管理の実行には、以下に示すような技術（プロダクト）・機能が用いられる。

- 特殊な格納のために用いる技術・機能
- アクセス制限に用いる技術・機能
- アクセス監視に用いる技術・機能

これらが、セキュリティ管理情報の保護管理策が求める役割を果たすようにするためには、セキュリティ管理情報の保護管理策の実施に必要な技術・機能についての要件が適切に指定され、開発、導入、維持管理チームに伝えられ、それらの機能の配置等のシステム構成や諸機能の実装に的確に反映されなければならない。

このため、セキュリティ管理情報の保護管理の立場からも、それらがシステムに的確に実装され期待通りに機能するようになっていることについて確認することも必要である。

(注) ここで指定された使用する技術・機能のシステムへの実装は、システムの構築と維持管理の問題となる。第9章の**“セキュアなシステムの構築”**を参照。

(1) セキュリティ管理情報の保護管理に用いる技術・機能要件の明確化

(2) 指定した技術･機能の実装についての確認の実施
(3) 必要に応じた技術･機能要件の指定の見直しの実施

4.6.3.5 セキュリティ管理情報の漏洩、改ざん、破壊事故への備への確立

セキュリティ管理情報の保護管理に努力していても、対策実施上の不備や新しい攻撃手段の登場やにより、セキュリティ管理情報の保護を保証することは難しく、セキュリティ管理情報にかかわる事故が発生する可能性は常にあると考えておかなければならない。

セキュリティ管理情報に漏洩、改ざん、破壊等の事故が発生した場合は、

- 漏洩、改ざん、破壊されたセキュリティ管理情報の無効化と再設定
- 改ざんまたは破壊された情報の復旧
- 改ざんされた情報が用いられたことによる被害の把握と必要な対策の実施
- 事故原因の除去

等が適切に行われなければならない。

セキュリティ管理情報にかかわる事故が発生した場合、これらのことが迅速かつ適切に行われるようにするためには、このような事故に対して必要となる処置についての十分な研究にもとづいた手順の確立や、その実行のために必要となるシステムのバックアップやシステムの運用記録の確保、必要なツールの準備等の備えが必要となる。

このため、セキュリティ管理情報にかかわる事故の処理に必要となる備えについての要求を明確にするとともに、それらがシステムの構成や運用に適切に反映されていることを確認することも必要となる。

(注) ここで指定されるセキュリティ管理情報にかかわる事故への備えについての要求は、第12章に示す**“サイト全体としてのセキュリティ事故対策への備え”**に対する要求となり、他の脅威に対する事故への備えと統合され、システムの構成や運用へ反映される。

(1) セキュリティ管理情報にかかる事故の処理に必要な備えについての要求の明確化
(2) 要求事項のシステム構成やシステム運用への反映状況についての定期的なチェックの実施
(3) 必要に応じた要求事項についての見直しの実施

4.6.3.6 業務やシステムの運用へのセキュリティ管理情報保護管理策の反映

セキュリティ管理情報の保護管理策として定めた諸施策が有効に機能するためには、それらがセキュリティ管理情報を扱う業務やシステムの構成やシステムの運用に的確に反映されなければならない。

セキュリティ管理情報の保護管理策からのシステム運用への要求が、日々の運用において的確に実施されるようにするためには、セキュリティ管理情報の保護管理策が業務やシステム運用に求めていることを明確にし、それらが業務運用システム運用の中に適切に組込まれるようにしなければならない。

(1) セキュリティ管理情報の保護管理策からの業務運用への要求の明確化
(2) 業務運用に対する要求事項の業務運用への組込み確認
(3) セキュリティ管理情報の保護管理策からのシステム運用への要求の明確化
(4) システム運用に対する要求事項のシステム運用への組込みの確認
(5) 業務運用やシステム運用に対する要求事項の実行状況についてのチェックの実施
(6) 必要に応じた業務やシステムの運用への要求についての見直しの実施

4.6.3.7 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

セキュリティ管理情報が記載あるいは記録されている印刷物等、電磁媒体、およびPC等の装置についても適切な保護管理が必要となる。このためには、これらについても、該当するセキュリティ管理情報に適用される保護管理要件に沿った保護管理要件を定め、指定された要件に従った保護管理が日常の業務やシステムの運営で習慣的に行われるようになっていることが求められる。

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

(1) 保護対象の印刷物や電磁媒体等の洗出し
(2) 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指定
(3) 関係者の教育の実施
(4) 業務現場やシステム運用における指定された保護管理要件に従った保護管理の実施

4.6.3.8 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

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、この委託先がセキュリティ管理情報の取扱いに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。

(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

4.6.3.9 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

セキュリティ管理情報の保護管理が適切に定められていても、これらが機能するためには、セキュリティ管理情報の保護管理に責任を持つ者やシステムの管理や運用にかかわる者に加え、業務等でセキュリティ管理情報に触れる者においても、これらについての十分な認識と理解が必要となる。

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だけでなく、システムの構築、管理、運用にかかわる者、および業務上でセキュリティ管理情報に触れる者のすべてに対し、セキュリティ管理情報の保護管理についての必要な教育を行うことが求められる。

(1) 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) 関係者のセキュリティ管理情報の保護管理に必要なスキルの確保

4.6.3.10 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ﾁｪｯｸの実施

セキュリティ管理情報の保護管理策が定められていても、それらがサイトの運営実態に照らして適切であり、かつ、確実に実行されていなければ、期待したセキュリティ管理情報の保護管理は実現しない。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はサイトの運営実態に照らして適切かどうか、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確実に実施されているかどうか等について定期的にチェックを行い、問題点の発掘と指摘された問題に対する改善を行うことが必要である。

(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チェックの実施
(2) 必要に応じた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臨時チェックの実施
(3) 指摘事項のフィードバックの実施

4.7 ユーザデータの保護管理策の概要

4.7.1 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に、

- 漏洩
- 改ざん
- 破壊

が生じないようにするための施策と、万一、ユーザデータに漏洩、改ざん、破壊事故が発生し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。

4.7.2 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ポリシーの確立
(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) 個々のユーザデータに対する保護管理要件の適切な指定
(4) システムの構成や機能の実装へのユーザデータの保護管理策の反映
(5) ユーザデータの漏洩、改ざん、破壊事故への備えの確立
(6) 業務やシステムの運用へのユーザデータの保護管理策の反映
(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) 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
(10) 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チェックの実施

4.7.3 求める施策の概要

4.7.3.1 ユーザデータ保護管理ポリシーの確立

取扱いに問題を起こせば、ショップならびにサイトの信頼に大きくかかわる、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な取組みを行うには、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に関し、以下のような事項を明らかにするユーザデータ保護管理ポリシーが確立され、関係者にこれが周知されていなければならない。

- ユーザデータの保護管理についての基本方針
- ユーザデータの保護管理策の組立て
- ユーザデータの保護管理策の適用範囲
- ユーザデータの保護管理実施基準

(1) ユーザデータの保護管理についての基本方針の明確化
(2) ユーザデータの保護管理策の組立ての明確化
(3) 適用範囲の明確化
(4) ユーザデータの保護管理基準の確立
(5) ユーザデータの保護管理ポリシーの関係者への周知
(6) 必要に応じたユーザデータの保護管理ポリシーの見直しの実施

4.7.3.2 ユーザデータの保護管理についての責任体制の確立

ユーザデータの保護管理策が期待通りに機能するためには、ユーザデータの保護管理策として定められたことが、ネットワークやシステムの構築およびシステムの運用に確実に反映されるようにするための体制が必要となる。

このためには、ユーザデータの保護管理にかかわるさまざまなタスクとその実施に責任を持つ者を明確にするとともに、関係者間の連携体制を確立しておくことが必要となる。

(1) ユーザデータの保護管理にかかるタスクの明確化
(2) ユーザデータの保護管理にかかるタスクの実施責任者の明確化
(3) ユーザデータの保護管理関係者間の連携の確立
(4) 責任体制の周知徹底
(5) 必要に応じた責任体制についての見直しの実施

4.7.3.3　個々のユーザデータに対する保護管理要件の適切な指定

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実施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、4.7.3.7 節**“ユーザ情報にかかわる印刷物や電磁媒体の適切な取扱いの実施”**を参照。

⑴ 保護対象のユーザデータの洗出し
⑵ 個々のユーザデータに対する保護管理要件の指定
⑶ 必要に応じた個々のユーザデータに指定した保護管理要件の見直しの実施

4.7.3.4　システムの構成や機能の実装へのユーザデータ保護管理策の反映

ユーザデータの保護管理の実行には、以下に示すような技術（プロダクト）・機能が用いられる。

- 特殊な格納のために用いる技術・機能
- アクセス制限に用いる技術・機能
- アクセス監視に用いる技術・機能

これらが、ユーザデータの保護管理策が求める役割を果たすようにするためには、ユーザデータの保護管理策の実施に必要な技術・機能についての要件が適切に指定され、開発、導入、維持管理チームに伝えられ、それらの機能の配置等のシステム構成や諸機能の実装に的確に反映されなければならない。

このため、ユーザデータの保護管理の立場からも、それらがシステムに的確に実装され期待通りに機能するようになっていることについて確認することも必要である。

(注) ここで指定された使用する技術・機能のシステムへの実装は、システムの構築と維持管理の問題となる。第9章の**“セキュアなシステムの構築”**を参照。

⑴ ユーザデータの保護管理に用いる技術・機能要件の指定
⑵ 要求した技術・機能の実装についての確認の実施

(3) 必要に応じた技術･機能要件の指定の見直しの実施

4.7.3.5 ユーザデータの漏洩、改ざん、破壊事故への備えの確立

ユーザデータの保護管理に努力していても、対策実施上の不備や新しい攻撃手段の登場やにより、ユーザデータの保護を保証することは難しく、ユーザデータにかかわる事故が発生する可能性は常にあると考えておかなければならない。

ユーザデータに漏洩、改ざん、破壊等の事故が発生した場合は、

- 改ざんまたは破壊された情報の復旧
- 改ざんされた情報が用いられたことによる被害の把握と必要な対策の実施
- 事故原因の除去

等が適切に行われなければならない。

ユーザデータにかかわる事故が発生した場合、これらのことが迅速かつ適切に行われるようにするためには、このような事故に対して必要となる処置についての十分な研究にもとづいた手順の確立や、その実行のために必要となるシステムのバックアップやシステムの運用記録の確保、必要なツールの準備等の備えが必要となる。

このため、ユーザデータにかかわる事故の処理に必要となる備えについての要求を明確にするとともに、それらがシステムの構成や運用に適切に反映されていることを確認することも必要となる。

(注) ここで指定されるユーザjデータにかかわる事故への備えについての要求は、第12章に示す**“サイト全体としてのセキュリティ事故対策への備え”**に対する要求となり、他の脅威に対する事故への備えと統合され、システムの構成や運用へ反映される。

(1) ユーザデータにかかる事故の処理に必要な備えについての要求の明確化
(2) 要求事項のシステム構成やシステム運用への反映状況についての定期的なチェックの実施
(3) 必要に応じた要求についての見直しの実施

4.7.3.6 業務やシステムの運用へのユーザデータ保護管理策の反映

ユーザデータの保護管理策として定めた諸施策が有効に機能するためには、それらがセキュリティ管理情報を扱う業務やシステムの構成やシステムの運用に的確に反映されなければならない。

ユーザデータの保護管理策からのシステム運用への要求が、日々の運用において的確に実施されるようにするためには、ユーザデータの保護管理策が業務やシステム運用に求めていることを

明確にし、それらが業務運用システム運用の中に適切に組込まれるようにしなければならない。

⑴ ユーザデータの保護管理策からの業務運用への要求の明確化
⑵ 業務運用に対する要求事項の業務運用への組込みの確認
⑶ ユーザデータの保護管理策からのシステム運用への要求の明確化
⑷ システム運用に対する要求事項のシステム運用への組込みの確認
⑸ 業務運用やシステム運用に対する要求事項の実行状況についてのチェックの実施
⑹ 必要に応じた業務やシステム運用への要求についての見直しの実施

4.7.3.7 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

保護対象のユーザ情報が記載あるいは記録されている印刷物等、電磁媒体、およびPC等の装置についても適切な保護管理が必要となる。このためには、これらについても、対応するユーザデータに適用される保護管理要件に沿った保護管理要件を定め、指定された要件に従った保護管理が日常の業務やシステムの運営で常に行われるようになっていることが求められる。

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。

⑴ 保護対象の印刷物や電磁媒体の洗出し
⑵ 保護対象の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指定
⑶ 関係者の教育の実施
⑷ 業務現場やシステム運用における指定された保護管理要件に従った保護管理の実施

4.7.3.8 業務委託先に対するﾕｰｻﾞﾃﾞｰﾀの保護管理についての指導、管理の実施

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、この委託先がユーザデータの取扱いにかかわることもある。このような場合、ユーザデータの保護管理の実現には、委託先においてもユーザデータの保護管理が適切に行われることが必要となる。

⑴ 適切な業務委託先の選定
⑵ 業務委託先における保護管理責任の明確化
⑶ 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

4.7.3.9 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

ユーザデータの保護管理が適切に定められていても、これらが機能するためには、ユーザデータの保護管理に責任を持つ者やシステムの管理や運用にかかわる者に加え、業務等でユーザデータに触れる者においても、これらについての十分な認識と理解が必要となる。

このため、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、管理、運用にかかわる者、および業務上でユーザデータに触れる者のすべてに対し、ユーザデータの保護管理についての必要な教育を行うことが求められる。

⑴ ユーザデータの保護管理についての教育の実施
⑵ 関係者のユーザデータの保護管理に必要なスキルの確保

4.7.3.10 ﾕｰｻﾞﾃﾞｰﾀの保護管理の実施状況についての定期的なチェックの実施

ユーザデータの保護管理策が定められていても、それらがサイトの運営実態に照らして適切であり、かつ、確実に実行されていなければ、期待したユーザデータの保護管理は実現しない。このため、定められているユーザデータの保護管理策はサイトの運営実態に照らして適切かどうか、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確実に実施されているかどうか等について定期的にチェックを行い、問題点の摘出と指摘された問題に対する改善を行うことが必要である。

⑴ 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チェックの実施
⑵ 必要に応じたユーザデータの保護管理の実施状況についての臨時チェックの実施
⑶ 指摘事項のフィードバックの実施

4.8 通信にかかるリスク対策の概要

4.8.1 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、このような事故やトラブル攻撃が生じた時への備えを総称するものである。

4.8.2 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対策ポリシーの確立
(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適切な指定
(4) システムの構成や機能の実装への通信にかかるリスク対策の反映
(5) 通信にかかるセキュリティ事故への備えの確立
(6) システム運用への通信にかかるリスク対策の反映
(7) 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チェックの実施

4.8.3 求める施策の概要

4.8.3.1 通信にかかるリスク対策ポリシーの確立

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ため通信にかかるリスク対策を効果的なものにするためには、戦略的で組織的な取組みが必要であり、このためには通信にかかるリスク対策をどのような考えで、またどのような方法で実施するかを明らかにする等の通信にかかるリスク対策ポリシーが確立され、関係者にこれが周知されていなければならない。

通信にかかる対策ポリシーの中で明らかにすべき事項としては、以下があげられる。

- 通信にかかる脅威への対応についての基本方針
- 通信にかかるリスク対策の組立てについての考え方

- 対策の適用範囲
- 通信にかかるリスク対策の実施基準

(1) 通信にかかる脅威への対応についての基本方針の明確化
(2) 通信にかかるリスク対策の組立ての明確化
(3) 適用範囲の明確化
(4) 通信にかかるリスク対策基準の確立
(5) 通信にかかるリスク対策ポリシーの関係者への周知
(6) 必要に応じたの通信にかかるリスク対策ポリシーの見直しの実施

4.8.3.2 通信にかかるリスク対策についての責任体制の確立

通信にかかるリスク対策が期待通りに機能するためには、通信にかかるリスク対策として定められたことが、ネットワークやシステムの構築およびシステムの運用に確実に反映されるようにするための体制が必要となる。

このためには、通信にかかるリスク対策についてのさまざまなタスクとその実施に責任を持つ者を明確にするとともに、関係者間の連携体制を確立しておくことが必要となる。

(1) 通信にかかるリスク対策についてのタスクの明確化
(2) 通信にかかるリスク対策についてのタスクの実施責任者の明確化
(3) 通信にかかるリスク対策関係者間の連携の確立
(4) 責任体制の周知徹底
(5) 必要に応じた責任体制についての見直しの実施

4.8.3.3 個々の通信に対するリスク対策要件の適切な指定

求められる通信にかかるリスク対策が機能するためには、リスク対策ポリシーで定めたリスク対策実施基準に沿って、個々の保護対象通信ごとのリスク対策要件と対策レベルを明確にし、それを実現するための適用する通信方式や技術、および運用管理上の留意事項等が適切に指定されなければならない。

対策レベルが厳格になればなるほど、コストや運用面での負担が大きくなるのが一般的であり、適用する通信方式や技術の選択にあたっては、目的を損なわないように運用面での負担とのバランスがとれたものにする必要がある。

(1) 保護対象通信の洗出し
(2) 保護対象通信の個々に対するリスク対策要件の指定
(3) 必要に応じた個々の通信に指定したリスク対策要件の見直しの実施

4.8.3.4 システムの構成や機能の実装への通信にかかるリスク対策の反映

通信にかかるリスク対策の実行には、以下に示すような技術（プロダクト）・機能が用いられる。

- 通信の秘匿を行う技術・機能
- 通信メッセージの改ざんをチェックする技術・機能
- 通信の記録をとる技術・機能
- 特定の通信をチェックする機能

これらが、通信にかかるリスク対策が求める役割を果たすようにするためには、通信にかかるリスク対策の実施に必要な技術・機能についての要件が適切に指定され、開発、導入、維持管理チームに伝えられ、それらの機能の配置等のシステム構成や諸機能の実装に的確に反映されなければならない。

このため、通信にかかるリスク対策の立場からも、それらがシステムに的確に実装され期待通りに機能するようになっていることについて確認することも必要である。

(注) ここで指定された使用する技術・機能のシステムへの実装は、システムの構築と維持管理の問題となる。第9章の**“セキュアなシステムの構築”**を参照。

(1) 通信にかかるリスク対策に用いる技術・機能要件の指定
(2) 指定した技術・機能の実装についての確認の実施
(3) 必要に応じた技術・機能要件の指定の見直しの実施

4.8.3.5 通信にかかるセキュリティ事故への備えの確立

通信にかかるリスク対策に努力していても、対策実施上の不備や新しい攻撃手段の登場により、保護を保証することは難しく、通信にかかる事故が発生する可能性は常にあると考えておかなければならない。

通信の監視、通信メッセージの漏洩、改ざん、破壊等の事故や、通信の否認が発生した場合は、

- 改ざんされた情報が用いられたことによる被害の把握と必要な対策の実施
- 否認に対する通信事実の証明

- 事故原因の除去

等が適切に行われなければならない。

通信にかかるセキュリティ事故が発生した場合、これらのことが迅速かつ適切に行われるようにするためには、このような事故に対して必要となる処置についての十分な研究にもとづいた手順の確立や、その実行のために必要となるシステムのバックアップやシステムの運用記録の確保、必要なツールの準備等の備えが必要となる。

このため、通信にかかるセキュリティ事故の処理に必要となる備えについての要求を明確にするとともに、それらがシステムの構成や運用に適切に反映されていることを確認することも必要となる。

(注) ここで指定される通信にかかるセキュリティ事故への備えについての要求は、第12章に示す**“サイト全体としてのセキュリティ事故対策への備え”**に対する要求となり、他の脅威に対する事故への備えと統合され、システムの構成や運用へ反映される。

(1) 通信にかかるセキュリティ事故の処理に必要な備えについての要求の明確化
(2) 要求事項のシステム構成やシステム運用への反映状況についての定期的なチェックの実施
(3) 指定した要求事項についての見直しの実施

4.8.3.6 システムの運用への通信にかかるリスク対策の反映

通信にかかるリスク対策として定められた諸施策が有効に機能するためには、それらがシステムの構成やシステムの運用に的確に反映されなければならない。

通信にかかるリスク対策からのシステム運用への要求が、日々の運用において的確に実施されるようにするためには、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を明確にし、それらがシステム運用の中に適切に組込まれるようにしなければならない。

(1) 通信にかかるリスク対策からのシステム運用への要求の明確化
(2) 要求事項のシステム運用への組込みの確認の実施
(3) システム運用に対する要求事項の実行状況についてのチェックの実施
(4) 必要に応じたシステム運用への要求についての見直しの実施

4.8.3.7 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チェックの実施

通信にかかるリスク対策が定められていても、それらがサイトの運営実態に照らして適切であり、かつ、確実に実行されていなければ、期待した通信にかかるリスク対策は実現しない。このため、定められている通信にかかるリスク対策はサイトの運営実態に照らして適切かどうか、通信にかか

るリスク対策として定められていることが確実に実施されているかどうか等について定期的にチェックを行い、問題点の摘出と指摘された問題点に対する改善を行うことが必要である。

(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チェックの実施
(2) 必要に応じた通信にかかるリスク対策の実施状況についての臨時チェックの実施
(3) 指摘事項のフィードバックの実施

4.9 ユーザ認証の適切な適用の概要

4.9.1 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、問題が生じた時への備えを総称するものである。

4.9.2 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) ユーザ認証ポリシーの確立
(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) 適切なパスワード管理の実施
(5) システムの構成や機能の実装へのユーザ認証の運用の反映
(6) ユーザ認証にかかる事故への備えの確立
(7) 業務やシステムの運用へのユーザ認証の運用にかかる施策の反映
(8) ユーザ認証の適用とその管理の実施状況についての定期的なチェックの実施

4.9.3 求める施策の概要

4.9.3.1 ユーザ認証ポリシーの確立

サイトが提供するサービスの不正な利用につながる他人になりすましたサービスへのアクセスを防ぐとともに、万一、なりすましによるサービスの不正な使用等の事故が発生しても、その被害を限定的なものにすることに組織的な取組みを行うには、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等に関し、以下に示すような事項を明らかにするユーザ認証ポリシーが確立され、関係者がこれが周知されていなければならない。

- ユーザ認証の適用と管理についての基本方針
- ユーザ認証の適用管理の組立て
- 施策の適用範囲
- ユーザ認証適用基準

(注) 本章が対象にする**“ユーザ認証”**とは、サイトの外部や内部からサイトシステムのサービスを利用しようとする者からの当該サービスへのアクセス要求についての認証を指す。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し、本ガイドラインでは、第3章の**“不正アクセス対策”**の範疇としている。

(1) ユーザ認証の適用と管理についての基本方針の明確化
(2) ユーザ認証の適用と管理にかかる施策の組立ての明確化
(3) 適用範囲の明確化
(4) ユーザ認証適用基準の確立
(5) ユーザ認証適用ポリシーの関係者への周知
(6) 必要に応じたユーザ認証ポリシーの見直しの実施

4.9.3.2 ユーザ認証の適切な適用についての責任体制の確立

業務やサイトの運用で用いられるユーザ認証が適切に行われるためには、ユーザ認証の適用について定められていることが、ネットワークやシステムの構築およびシステムや業務の運用に確実に反映されるようにするための体制が必要となる。

このためには、ユーザ認証の適用についての管理にかかわるさまざまなタスクとその実施に責任を持つ者を明確にするとともに、関係者間の連携体制を確立しておくことが必要となる。

(1) ユーザ認証の管理にかかるタスクの明確化
(2) ユーザ認証の管理にかかるタスクの実施責任者の明確化

(3) ユーザ認証の管理関係者間の連携の確立
(4) 責任体制の周知徹底
(5) 必要に応じた責任体制についての見直しの実施

4.9.3.3 個々のユーザ認証場面に対する認証要件の適切な指定

求めるユーザ認証が適切に機能するようにするには、ユーザ認証が必要な個々の場面において、適用される認証レベル、その認証レベルを満足するため適用する認証方式と、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。

(1) サイト運営におけるユーザ認証場面の洗出し
(2) 個々のユーザ認証場面に対する認証要件の指定
(3) 必要に応じた個々のユーザ認証場面に指定した認証要件の見直しの実施

4.9.3.4 適切なパスワードの管理の実施

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。

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。

(1) 関係者へのパスワード管理基準の周知
(2) 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
(3) パスワード使用者に対する教育の実施
(4) 必要に応じたパスワード管理の実施状況についての定期的なチェックの実施

4.9.3.5　システムの構成や機能の実装へユーザ認証の運用の反映

ユーザ認証の適用とその管理の実行には、以下に示すような技術（プロダクト）・機能が用いられる。

- 認証の各場面における認証に用いる技術・機能
- 認証情報の管理に用いる技術・機能

これらが、ユーザ認証の運用が求める役割を果たすようにするためには、ユーザ認証の運用にかかる施策の実施に必要な技術・機能についての要件が適切に指定され、開発、導入、維持管理チームに伝えられ、それらの機能の配置等のシステム構成や諸機能の実装に的確に反映されなければならない。

このため、ユーザ認証の運用管理の立場からも、それらがシステムに的確に実装され期待通りに機能するようになっていることについて確認することも必要である。

(注) ここで指定された使用する技術・機能のシステムへの実装は、システムの構築と維持管理の問題となる。第9章の**“セキュアなシステムの構築”**を参照。

(1) ユーザ認証の運用とその管理に用いる技術・機能についての要件の指定
(2) 指定した技術・機能の実装についての確認の実施
(3) 必要に応じた技術・機能要件についての指定の見直しの実施

4.9.3.6　ユーザ認証にかかる事故への備えの確立

ユーザ認証の運用や管理に努力していても、対策実施上の不備や新しい攻撃手段の登場により、ユーザ認証にかかる事故が発生する可能性は常にあると考えておかなければならない。

ユーザ認証にかかる事故が発生した場合は、

- なりすましによる被害の把握と必要な対策の実施
- 被害の発生には至っていないが対策すべき範囲の把握と必要な処置の実施
- 事故原因の除去

等が適切に行われなければならない。

ユーザ認証にかかる事故が発生した場合、これらのことが迅速かつ適切に行われるようにするためには、このような事故に対して必要となる処置についての十分な研究にもとづいた手順の確立や、その実行のために必要となるシステムのバックアップやシステムの運用記録の確保、必要なツールの準備等の備えが必要となる。

このため、ユーザ認証にかかる事故の処理に必要となる備えについての要求を明確にするとともに、それらがシステムの構成や運用に適切に反映されていることを確認することも必要となる。

(注) ここで指定されるユーザ認証にかかる事故への備えについての要求は、第12章に示す

“サイト全体としてのセキュリティ事故対策への備え”に対する要求となり、他の脅威に対する事故への備えと統合され、システムの構成や運用へ反映される。

(1) ユーザ認証にかかる事故の処理に必要な備えについての要求の明確化
(2) 要求事項のシステム構成やシステム運用への反映状況についての定期的なチェックの実施
(3) 必要に応じた要求事項についての見直しの実施

4.9.3.7 システムの運用へのユーザ認証の運用にかかる施策の反映

ユーザ認証の適用を適切なものにするために定められた諸施策が有効に機能するためには、それらがユーザ認証とその管理にかかわる業務やシステムの構成やシステムの運用に的確に反映されなければならない。

ユーザ認証の管理からのシステム運用への要求が、日々の運用において的確に実施されるようにするためには、ユーザ認証とその管理が業務やシステム運用に求めていることを明確にし、それらが業務運用やシステム運用の中に適切に組込まれるようにしなければならない。

(1) ユーザ認証の運用が業務の運用に求めていることの明確化
(2) 業務運用に対する要求事項の業務運用への組込みの確認の実施
(3) ユーザ認証の運用がシステム運用に求めていることの明確化
(4) システム運用に対する要求事項のシステム運用への組込みの確認の実施
(5) 業務運用やシステム運用における要求事項の実行状況についてのチェックの実施
(6) 必要に応じた業務やシステム運用への要求についての見直しの実施

4.9.3.8 ユーザ認証の適用とその管理の実施状況についての定期的なチェックの実施

ユーザ認証を適切に行うための施策が定められていても、それらがサイトの運営実態に照らして適切であり、かつ、確実に実行されていなければ、期待した適切なユーザ認証通信は実現しない。このため、定められているユーザ認証にかかる諸管理策はサイトの運営実態に照らして適切かどうか、ユーザ認証の適用について定められていることが確実に実施されているかどうか等について定期的にチェックを行い、問題点の摘出と指摘された問題点に対する改善を行うことが必要である。

(1) ユーザ認証の適用とその管理の実施状況についての定期的なチェックの実施
(2) 必要に応じたユーザ認証の実施状況についての臨時チェックの実施

(3) 指摘事項のフィードバックの実施

4.10 セキュアなシステムの構築についての概要

4.10.1 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の実施は、巧みな設計されたシステムの構成と、システムを構成する各機器に組込まれたさまざまなセキュリティサービス機能や、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、脅威別に定められた対策が求めていることに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、

- 攻撃を受付けにくく、
- 攻撃を受けても被害は限定的な者に止めることができる

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、脅威別に定められた対策が求めていることを的確に反映したものにするためには、システムの構成や使用する技術・機能の実装とその使用法についての十分な検討と適切な管理が必要となる。

4.10.2 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実現
(4) セキュリティ対策ツールの的確な実装
(5) 各システム(サーバ)の実装へのセキュリティ要求事項の適切な実装
(6) アプリケーションへの必要なセキュリティ機能の適切な実装
(7) ソフトウェアに対する適切な保護の実施
(8) セキュリティ対策のシステムの構成や機能の実装への管理についての定期的なチェックの実施

4.10.3 求める施策の概要

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。

4.10.3.1 セキュアなシステムの構築についての責任体制の確立

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。

(1) セキュアなシステムの構築にかかるタスクの明確化
(2) セキュアなシステムの構築にかかるタスクの実施責任者の明確化
(3) セキュアなシステムの構築にかかる関係者間の連携の確立
(4) 責任体制の周知徹底
(5) 必要に応じた責任体制についての見直しの実施

4.10.3.2 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

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、被害を最小限に抑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

(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

4.10.3.3 構成方針に沿ったシステム構成の実現

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。

(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
(4) システム構成に関するドキュメントの整備

4.10.3.4 セキュリティ対策ツールの的確な実装

システムの構成の中には、データフローの制御や監視あるいはウイルスの検査等、サイトのセキュリティ確保のツールとして組込まれている技術(プロダクト)や機能がある。策定されたセキュリティ対策が機能するためには、セキュリティ対策の要ともいえるこれらの機能がセキュリティ対策からの要求に応えようにシステムに実装されていなければならない。

このため、セキュリティ対策のツールの組込みについての十分なレビューと実装についての確認

が必要となる。

(1) セキュリティ対策ツールへの要求についての確認の実施
(2) セキュリティ対策ツールの的確な実装
(3) サイトの運営形態やセキュリティ対策の変更のセキュリティ対策ツールの実装への適切な反映
(4) セキュリティ対策ツールの実装状況に関するドキュメントの整備

4.10.3.5 各システム（サーバ）の実装へのセキュリティ要求事項の適切な反映

脅威別に策定されたセキュリティ対策は、その実行の一部を各システム(サーバ)におけるさまざま攻撃に対して自分自身を守るためのセキュリティ対策の実装に依存している。このため、各システムはその内部構成や機能や各種パラメータの設定等の実装において、セキュリティ要求に対しそれぞれのサイト内の位置、役割、搭載機能等に対応して、セキュリティ対策からの要求を適切に反映させなければならない。

(1) 各システム(サーバ)に対するセキュリティ要求事項についての確認の実施
(2) 各システム(サーバ)におけるセキュリティ要求事項の的確な実装
(3) サイトの運用形態やセキュリティ対策の変更の各システムにおけるセキュリティ要求事項の実装への適切な反映
(4) 各アプリケーションにおけるセキュリティ対応機能の実装に関するドキュメントの整備

4.10.3.6 アプリケーションへの必要なセキュリティ機能の適切な実装

アプリケーションソフトウェアに組込むアクセス制御やアクセス監視は、機能(サービス)の不正使用や情報への不正なアクセスの最後の砦といえる。また、ネットワークレベルでのバリアやシステムレベルでのバリアをかいくぐってくる不正なアクセスへのアプリケーションレベルでの防御や、Web通信に対する暗号化等は必要な機能のアプリケーションプログラムに組込みに依存する。

このため、アプリケーションに組込むべきセキュリティ機能の適切な設定とその的確な実装を実現するための施策の実施が必要となる。

(1) 各アプリケーションに求められるセキュリティ機能な適切な指定
(2) アプリケーションに要求したセキュリティ機能の的確な実装
(3) サイトの運用形態やセキュリティ対策の変更の各アプリケーションに実装したセキュリティ機能への適切な反映

(4) 各アプリケーションにおけるセキュリティ対応機能の実装に関するドキュメントの整備

4.10.3.7 ソフトウェアに対する適切な保護の実施

開発したソフトウェアにトロイの木馬やコバート通信路(隠れチャネル)が埋込れたり、プログラムが他のものとすり返られたりすることもセキュリティの脅威の一つである。これらのことを防ぐためには、ソフトウェアの開発プロセスに対する適切な管理と、ソフトウェアライブラリに対する適切な保護管理が必要となる。

(1) ソフトウェア開発プロセスに対する適切な管理の実施
(2) ソフトウェアに対する保護管理の実施

4.10.3.8 セキュリティ対策のシステムの構成や機能の実装への反映の管理についての定期的なチェックの実施

サイトシステムの作りにセキュリティ上の欠陥がないようにするためには、システム構成と機能の実装へのセキュリティ対策の反映についての適切な管理が不可欠である。

サイトシステムが、構成方針に沿った構成となっているか、セキュリティ対策にかかわる機能の実装についての管理が適切に行われているかについてのチェックを定期的に行い、問題が顕在化する前に問題点の発掘と適切な改善が行えるようにしておくことも必要である。

(1) セキュリティ対策のシステム構成や機能の実装への反映の管理の実施状況についての定期的なチェックの実施
(2) 必要に応じたセキュリティ対策のシステム構成や機能の実装への反映の管理の実施状況について臨時チェックの実施
(3) 指摘事項のフィードバックの実施

4.11 セキュアなシステム運用の実現についての概要

4.11.1 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駄となる。

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。

セキュアなシステム運用の実現とは、セキュリティ対策がシステムの運用に求めていることが、日々のシステム運用の中で的確に実行されることをいう。このことを実現するためには、日々のシステム運用においてセキュリティ対策にかかわる作業や処理が適切に行われるようにするための仕組み作りや適切な管理が必要となる。

4.11.2 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) システム運用にかかるセキュリティポリシーの確立
(2) セキュアなシステム運用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程や運用マニュアルへ的確な反映
(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) サイトシステムへの物理アクセスに対する適切な管理の実施
(6) 運用関係者に対するセキュリティ教育の実施
(7) システム運用におけるセキュリティ対策への対応についての定期的なチェックの実施

4.11.3 求める施策の概要

4.11.3.1 システム運用にかかるセキュリティポリシーの確立

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運用チームとしてどのように取組むかに関し、以下に示すような事項を明らかにするシステム運用にかかるセキュリティポリシーが確立され、運用にかかわる者にこれが周知されていなければならない。

- システム運用におけるセキュリティに対する基本方針
- セキュアなシステム運用の実現のための施策の組立て
- 施策の適用範囲

(1) システム運用におけるセキュリティに対する基本方針の明確化
(2) セキュアなシステム運用の実現のための施策の組立ての明確化

(3) 適用範囲の明確化
(4) システム運用におけるセキュリティポリシーの関係者への周知

4.11.3.2 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

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。

(1) セキュアなシステム運用の実現にかかるタスクの明確化
(2) セキュアなシステム運用の実現にかかるタスクの実施責任者の明確化
(3) システム運用関係者間での連携の確立
(4) 責任体制の周知徹底
(5) 必要に応じた責任体制についての見直しの実施

4.11.3.3 セキュリティ対策にかかる諸施策の運用規程や運用マニュアルへの的確な反映

システム運用が脅威対応に検討されてきたセキュリティ対策からの要求に応えるためには、まず、セキュリティ対策が日々のシステム運用に求めていることが運用規程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。

(注) セキュリティ対策にかかる諸施策の運用規程、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、確実に運用規程や運用マニュアルに反映しているようにすることを、運用者側の立場から保証しようとするものである。

(1) セキュリティ対策にかかる諸施策の運用規程、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程、運用マニュアルへの的確な反映
(3) 必要に応じた運用規程や運用マニュアルの見直しの実施

⑷ 運用規程や運用マニュアルについての定期的なチェックの実施

4.11.3.4 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

日々のシステム運用においてセキュリティ対策求めている作業や処理が的確に行われ、その実行に不備がでないようにするためには、セキュリティ要求事項の確実な実施についての工夫を織り込んだ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。

⑴ セキュリティ対策に関連して定期的に実施すべき作業や処理の定期スケジュール化
⑵ 日々のシステム運用におけるセキュリティ対策に関係する作業や処理の実行チェックリストの作成と予定作業･処理の実行確認の励行
⑶ 日々のシステム運用におけるセキュリティ対策に関係する作業や処理についての記録の確保
⑷ 必要に応じたシステム運用におけるセキュリティ対策に関係した作業や処理の実行方法や管理の方法についての見直しの実施
⑸ システム運用におけるセキュリティ対策に関係した作業や処理の実行方法や管理の方法についての定期的なチェックの実施

4.11.3.5 サイトシステムへの物理アクセスに対する適切な管理の実施

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、システムの機能の使用やシステムの運用や機器等のメンテナンスで、直接触れることを言う。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、不正に使用あるいは操作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、それらの中に記憶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。

脅威対応に研究されたセキュリティ対策が思わぬところから破綻しないよう、サイトシステムは正規の運用者のみがアクセスできるような環境に置き、適切な管理下にお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。

⑴ システムへの物理アクセスに対する管理ルールの確立
⑵ システムへの物理アクセスに対する管理に必要な環境の整備

(3) ルールに従ったシステムへの物理アクセスに対する管理の実施
(4) 必要に応じたシステムへの物理アクセスに対する管理についての見直しの実施

4.11.3.6 運用関係者に対するセキュリティ教育の実施

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、これらが運用規程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。

(1) システム運用関係者に対するセキュリティ教育の実施
(2) 運用関係者におけるセキュリティ対策の実施に必要なスキルの確保

4.11.3.7 システム運用おけるセキュリティ対策への対応についての定期的なチェックの実施

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い、問題点の発掘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。

(1) システム運用におけるセキュリティ対策への対応についての定期的なチェックの実施
(2) 必要に応じたシステム運用におけるセキュリティ対策への対応についての臨時チェックの実施
(3) 指摘事項のフィードバックの実施

4.12 セキュリティ事故への備え

4.12.1 セキュリティ事故への備えとは

さまざまなセキュリティ対策を実施していたとしても、すべての攻撃を排除することは保証できず、システムはいつか攻撃による被害を受けるものと考えておかなければならない。このため、セキュリティにかかる事故が発生しても、サイトにおける業務の運用やシステムの運用が大きな影響が及ばないようにしておかなければならない。このことを実現するためには、セキュリティ事故の発生に際して、被害の拡大を防ぐと共に、システムの被害からの回復と業務の再開が迅速かつ的確に行われなければならない。セキュリティ事故への備えとは、事故の処理が円滑に行えるようにするための日頃からの準備を総称するものであり、セキュリティ事故の予防にかかわる諸施策とサイトのセキュリティ対策の両輪をなすものである。

4.12.2 セキュリティ事故への備えのための施策の構成

本ガイドラインでは、セキュリティ事故への備えとして必要な施策を、以下で構成する。

(1) セキュリティ事故対応ポリシーの確立
(2) セキュリティ事故への対応についての責任体制の確立
(3) 事故処理単位個々に対する事故への備えの確立
(4) サイと全体としてのセキュリティ事故対応計画の確立
(5) セキュリティ事故への対応に必要な技術･機能要件のシステムの構成や機能の実装への反映
(6) システム運用へのセキュリティ事故への備えの反映
(7) 事故処理訓練の実施
(8) セキュリティ事故の備えのについての定期的なチェックの実施

4.12.3 求める施策の概要

4.12.3.1 セキュリティ事故対応ポリシーの確立

さまざまなセキュリティ対策を実施していたとしても、すべての攻撃を排除することは保証できず、システムはいつでも攻撃による被害を受けるものと考えておかなければならない。セキュリティ事故が発生しても、サイトにおける業務の運用やシステムの運用が大きな影響が及ばないようにするためには、日頃から、セキュリティ事故の発生に際して被害からの迅速かつ的確な回復を実現するための備えができていなくてはならない。

また、セキュリティ事故への備えは、業務（サービス）の継続確保に対する要求のレベルによって大きく異なり、その運用への負担も大きく異なる。このため、セキュリティ事故への備えを適切に行うためには、セキュリティ事故への対応についての基本的な考え方を示すため、以下のようなことを明確にするセキュリティ事故対応ポリシーが確立されていることが必要となる。

- セキュリティ事故への対応についての基本方針
- セキュリティ事故への対応の組立て

（1）セキュリティ事故への対応についての基本方針の明確化
（2）セキュリティ事故への対応策の組立ての明確化
（3）セキュリティ事故対応ポリシーの関係者への周知
（4）必要に応じたセキュリティ事故対応ポリシーの見直しの実施

4.12.3.2 セキュリティ事故への対応についての責任体制の確立

日常のシステム運用におけるセキュリティ事故への備えや、発生した事故に対する処理が適切に行われるようにするためには、セキュリティ事故の備えと事故発生時の処理についての適切な計画の確立し実行する体制が必要となる。

このためには、セキュリティ事故への備えと発生した事故の処理にかかるさまざまなタスクとその実施に責任を持つ者を明らかにするとともに、関係者間での連携体制を確立しておくことが必要となる。

（1）セキュリティ事故への対応にかかるタスクの明確化
（2）セキュリティ事故への対応にかかるタスクの実施責任者の明確化
（3）セキュリティ事故対応関係者間の連携の確立
（4）責任体制の周知徹底
（5）必要の応じた責任体制についての見直しの実施

4.12.3.3 事故処理単位個々に対する事故への備えの確立

事故発生時の被害範囲の調査や被害からの回復に必要な処理は、被害を受けたまたは受けた可能性のある業務(アプリケーション)や、行われた攻撃のタイプ等の事故の特性により異なってくる。このため、発生した事故に対して、どのような処理を行うかは、業務を主体に検討しなければならない。このとき、取扱いが共通となる業務については、一緒に検討することができる。

したがって、セキュリティ事故発生時における処置を適切に行うためには、まず、サイトにおける

業務の構成およびシステムの構成や運用の組立て等から事故処理の計画単位を適切に決め、そのそれぞれに対し必要な処理やその手順を示す事故処理要領を確立しておくことが必要となる。

またこの時、合わせて、指定した事故の処理に必要なバックアップの取得や必要な情報の確保等の日頃からの備えについての要求も明確にしておく必要がある。

(1) 事故処理単位の指定
(2) 事故処理単位の個々に対する事故処理要領の確立
(3) 事故処理単位の個々に対する必要なバックアップの確保についての要件の指定
(4) 事故処理単位の個々に対する事故処理に必要な情報や記録の確保についての要件の指定
(5) 事故処理単位個々における事故への対応に必要なシステム環境についての要件の指定
(6) 事故処理単位個々における事故処理訓練の実施についての要求の指定
(7) 必要に応じた事故処理単位の個々に指定した事故への対応についての見直しの実施

4.12.3.4 サイト全体としてのセキュリティ事故対応計画の確立

事故処理への備えや実際の事故処理の手順等は、事故処理単位に検討定義されなければならないが、事故への備えには重複したものがあるだけでなく、事故によってはその影響は複数の業務にわたる場合がある。このため、実運用上は、事故への備えや発生した事故に対する処置は、サイト全体として考える必要がある。

このため、個々の事故処理単位に指定された事故処理要領や事故処理に必要な備えについての要求を統合した、

- サイト全体としてのセキュリティ事故対応計画
- サイト全体としてのバックアップの取得要領
- サイト全体としての事故発生時の処置に必要となる情報の確保容量

を纏めておく必要がある。バックアップの取得や必要な情報の確保、ならびに事故発生時における処置はこれらの要領にそって行われる。

(1) サイト全体としてのセキュリティ事故対応計画の確立
(2) サイト全体としてのバックアップの確保要領の確立
(3) サイト全体としての事故処理に必要となる情報や記録の確保についての要領の確立
(4) 必要に応じたサイト全体としてセキュリティ事故対応計画や事故への備えについての見直しの実施

(注) 統合事故処理要領における事故処理手順は、一般にはに示されるようなものになる。

4.12.3.5 セキュリティ事故への対応に必要な技術・機能のシステムの構成や機能の実装への反映

セキュリティ事故への備え、ならびに事故時における被害状況の調査や事故による被害からの復旧の実行は、以下に示すような技術（プロダクト）・機能が用いられる。

- バックアップの取得とその保管に用いる技術・機能
- 被害状況の調査に用いる技術・機能
- データの回復等システムの回復に用いる技術・機能
- 業務（サービス）の再開に用いる技術・機能

セキュリティ事故への迅速で適切な処置が意図したように行われるためには、システムでセキュリティ事故への備えや事故処理に用いられる技術（プロダクト）・機能についての要件が適切に指定され、システム構成チームに明示されなければならない。また、それらがシステムに的確に実装され期待通りに機能するようになっていることについて確認することも必要となる。

（1）セキュリティ事故への備えならびに事故の処理に用いる技術・機能について要件の適切な指定
（2）指定した技術・機能の実装についての確認の実施
（3）必要に応じた技術・機能要件についての指定の見直しの実施

4.12.3.6 システム運用へのセキュリティ事故への備えの反映

セキュリティ事故への備えとしてシステム運用に求めていることは、システム運用に適切に反映されなければならない。

日々の運用において、セキュリティ事故への備えとして必要な処理が、的確に実施されるようにするためには、セキュリティ事故への備えとしてシステム運用に求めていることを明確にするとともに、それらがシステム運用の中に適切に組込まれているかどうかを確認することも必要である。

（1）システム運用上でのセキュリティ事故への備えにかかる作業や処理の明確化
（2）セキュリティ事故への備えが求めるシステム運用のシステム運用規程や運用マニュアルへの適切な反映の確認の実施
（3）必要なバックアップの確保の実施状況についてのチェックの実施
（4）必要な記録の確保の実施状況についてのチェックの実施
（5）必要に応じたシステム運用への要求についての見直しの実施

4.12.3.7 事故処理訓練の実施

セキュリティ事故発生時における必要な処理の迅速かつ的確な実行は、発生事故に対する事故処理要領の妥当性、使用する機能の妥当性とその適切な実装、必要なバックアップや運用の記録の準備、さらには事故処理を行うスタッフのスキルや慣れに依存する。そして、これらは普段使用されないため、問題が潜在化しやすく、事故発生時に機能せず、被害を大きくすることが多い。このため、これらについての問題点を洗出したり、事故処理にあたるスタッフに対する事故処理に必要なスキルを確保するためには、想定されるセキュリティ事故を対象とした事故処理訓練を、定期的に実施しなければならない。

(1) サイト全体としての事故処理訓練計画の確立
(2) 個々の事故処理訓練についての訓練実施要領の確立
(3) 事故処理訓練計画にもとづいた事故処理訓練の実施
(4) 訓練結果の評価とフィードバック
(5) 必要に応じた事故処理訓練計画や個々の訓練実施要領についての見直しの実施

4.12.3.8 セキュリティ事故への備えについての定期的なチェックの実施

セキュリティ事故発生時に、セキュリティ事故への備えが期待通りに機能するためには、定められているセキュリティ事故への備えはサイトの運営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を定期的にチェックし、問題点の発掘と必要な改善の指導を行うことも必要である。

(1) セキュリティ事故への備えの実施状況についての定期的なチェックの実施
(2) 必要に応じたセキュリティ事故への備えについての臨時チェックの実施
(3) 指摘事項のフィードバックの実施

■ 本報告書の執筆に携わったメンバー（50 音順）

電子商取引推進協議会		重松　孝明
電子商取引推進協議会		川村　尚哉
日本電気株式会社	IT 基盤システム開発事業部	石田　文治
株式会社日立ｼｽﾃﾑｱﾝﾄﾞｻｰﾋﾞｽ	ネットワークビジネス本部	一村　政司
株式会社日立情報システムズ	システムインテグレーション本部	柴田　利幸
富士通ｻﾎﾟｰﾄ&ｻｰﾋﾞｽ株式会社	カストマリレーション本部	末延　忠昭
松下電器産業株式会社	本社 情報企画グループ	東本　謙治
株式会社日立製作所	ソフトウェア事業部	松永　和男

平成 14 年 3 月発行
発行：電子商取引推進協議会
東京都港区芝公園 3-5-8
機械振興会館 3F
Tel　03-3436-7500
e-mail　info@ecom.jp

この資料は再生紙を使用しています。