H13－セキュリティWG－4

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　－

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

本書は、「EC サイト向けのセキュリティ対策ガイドライン」の第二分冊であり、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、

- 施策の趣旨
- 実施要求事項
- 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。個々の脅威に対して求める対策のレベルや、サイト内におけるデータフローの制御や監視についてのルール、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ことにより、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”、“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 1-1に示す。また、対策テーマ間の関連を表1-1に示す。

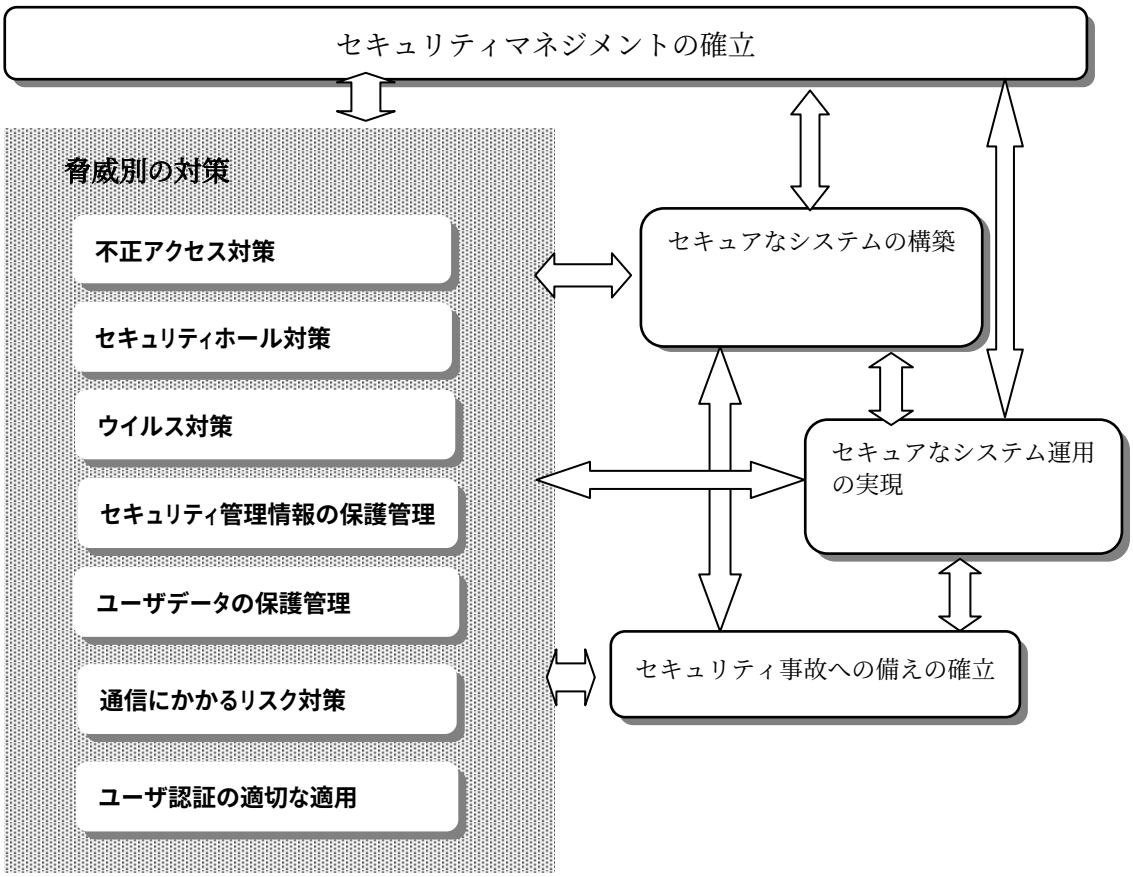

図 1-1　本ガイドラインにおける対策テーマの体系

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	2	3	4	5	6	7	8	9	10	11	備考
		セキュリティマネジメントの確立	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	セキュアなシステムの構築	セキュアなシステム運用の実現	セキュリティ事故への備えの確立	
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

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
- 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。

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。

⑴ サイト運営上のセキュリティポリシーの確立
⑵ セキュリティ対策推進体制の確立
⑶ スタッフのセキュリティの確立
⑷ サイト運営にかかわる外部組織の協力の確保
⑸ セキュリティ対策予算の確保
⑹ サイト運営関係者に対するセキュリティ教育の実施
⑺ 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、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。

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) 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

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。

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

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、

- 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

のための施策の総称をいう。

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

⑶ 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
⑷ ネットワークからのウイルスの侵入の阻止
⑸ 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
⑹ FD 等の持込みファイルからのウイルス侵入の阻止
⑺ システムに対するウイルス検査の実施
⑻ ウイルス感染ファイルの外部への持出しの防止
⑼ システムの構成や機能の実装へのウイルス対策の反映
⑽ ウイルス感染事故への備えの確立
⑾ システム運用へのウイルス対策の反映
⑿ 関係者に対するウイルス対策についての教育の実施
⒀ 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

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、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。

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。
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
⑽ 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

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。

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。
⑴ ユーザデータの保護管理ポリシーの確立
⑵ ユーザデータの保護管理についての責任体制の確立
⑶ 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
⑷ 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
⑸ ユーザデータの漏洩、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ユーザデータの保護管理策の反映
⑺ 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
⑻ 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
⑼ 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

⑽ 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

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。

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。

⑴ 通信にかかるリスク対策ポリシーの確立
⑵ 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
⑶ 個々の通信に対するリスク対策要件の適切な指定
⑷ 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
⑸ 通信にかかるセキュリティ事故への備えの確立
⑹ システム運用への通信にかかるリスク対策の反映
⑺ 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

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、問題が生じた時へ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

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、脅威対応の施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、行為対応の施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。

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

⑶ 構成方針に沿ったシステム構成の実現
⑷ セキュリティ対策ツールの的確な実装
⑸ 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
⑹ 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
⑺ ソフトウェアに対する適切な保護の実施
⑻ 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

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。

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。
⑴ システム運用にかかるセキュリティポリシーの確立
⑵ セキュアなシステム運用実現のための責任体制の確立
⑶ 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
⑷ 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
⑸ 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
⑹ 運用関係者に対するセキュリティ教育の実施
⑺ 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

1.12　セキュリティ事故への備えの確立の概要

1.12.1　セキュリティ事故への備えの確立とは

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。

1.12.2　セキュリティ事故への備えの確立ための施策の構成

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。

⑴ セキュリティ事故対応ポリシーの確立
⑵ セキュリティ事故への対応についての責任体制の確立
⑶ 事故処理単位個々に対する事故への備えの確立
⑷ サイと全体としてのセキュリティ事故対応計画の確立
⑸ 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
⑹ システム運用へのセキュリティ事故への備えの反映
⑺ 事故処理訓練の実施
⑻ 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

■ 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