THE POSSIBILITIES ARE INFINITE FUJITSU

富士通のエンタープライズセキュリティアーキテクチャー 別冊

富士通規準セキュリティポリシー 2007

2007 年 5 月

富士通株式会社

情報セキュリティセンター

目次

1. 規準セキュリティポリシーのコンセプト

1. 富士通規準セキュリティポリシーとは

「富士通のエンタープライズセキュリティアーキテクチャー」本編で述べたように、組織の情報セキュリティガバナンスを達成するためには、運用面の基盤であるセキュリティマネジメントフレームワークと、技術面の基盤であるエンタープライズセキュリティアーキテクチャーの 2 つの基盤が相互に連携して整備されることが必要です。また、この両者を繋ぐ位置にあるものが一連のセキュリティ管理策であり、セキュリティ管理策がエンタープライズセキュリティアーキテクチャー検討のインプットとなります。

本書「富士通規準セキュリティポリシー 2007」は、エンタープライズセキュリティアーキテクチャーの前提となる、セキュリティ管理策のサンプルを提供するものです。本書は一般的なセキュリティポリシーの様式で記述されているので、これ自身をセキュリティポリシーのサンプルとして利用することもできます。

2. 富士通規準セキュリティポリシーの特長

(1) 富士通が独自開発したセキュリティポリシーの規準

富士通が独自のノウハウに基づいて、どのお客様にも必要となる最小限の内容を、無理なく適用できるように作成された公開セキュリティポリシーです。

(2) 組織ポリシーから製品/サービスまでをカバー

規準セキュリティポリシーおよび機能セキュリティポリシーに含まれるセキュリティ対策は、富士通がご提供するセキュリティ関連サービス (セキュリティ監視サービス、アタックテストサービス、ウィルス対策サービス等) 及びセキュリティ製品 (各種ファイアウォール、ウィルス対策ソフト、 侵入検知システム等) で実現されています。これにより、上位の組織ポリシーから実装レベルまでシームレスなセキュリティ対策が可能です。

(3) 国際/国内標準ベース

ISO/IEC 27000（BS7799）シリーズ、ISO/IEC15408、ISO/IEC TR 13335、旧郵政省の情報通信ネットワーク安全・信頼性基準など、国内外の代表的なセキュリティ標準を基にして作成されており、安心してお使いいただけます。

3. 本書の構成

本書は、富士通が考えるセキュリティ分野ごとにセキュリティポリシーを記載しています。また、それぞれの要求事項について、ISO/IEC 27001(JIS Q 27001)の付録 A に記載されている管理策の中で関連が深いものの番号を[A.4.1.1]のような形で記載しています。

2. 用語定義

1. 対象システム

本セキュリティポリシーの適用対象となる情報システム。ポリシーの適用範囲があいまいにならないように、対象システムの範囲は可能な限り具体的な記述で明文化されている必要がある。

2. システム運用責任者

対象システムのセキュリティ維持および本セキュリティポリシーの実施に関して責任を負い、システム管理者を管理する立場にあることが明文化されている者。対象システムにはかならずシステム運用責任者を置かなければならない。
なお、本セキュリティポリシーにおいては、特に明記していない限り、主語として「システム運用責任者は」が省略されていると解釈するべきである。

3. システム管理者

対象システムのセキュリティ維持に関する運用を主体的に行う立場にあり、その立場が明文化されている者。対象システムにはかならずシステム管理者を置かなければならない。原則としてシステム運用責任者とシステム管理者を兼ねることは認めない。システム管理者は、システム運用責任者の指示に従い、本セキュリティポリシーを実施するための各種作業を行う。

4. 明文化

組織内で必要な承認手続きを経た文書に記載されており、かつそれを知る必要がある者がいつでもその記載を確認できる状況に置くこと。

5. 権限

システムの資源や情報を利用することについて、組織の公式な意思決定によりその正当性が認められていること。

6. セキュリティ

対象システムに求められるシステムの機密性、完全性、可用性などを実現するための装置、設備、活動、組織などを概念的に総称したもの。

7. リッチコンテンツ

情報の密度が高いコンテンツの総称。例えば、画像や音声などを含むコンテンツなど。

3. セキュリティ統制

第1章　共通

社内の各業務に共通して実施すべきセキュリティ対策

1. 情報資産管理

(1) 情報管理区分に従った資産管理を行うこと。[A.7.2.1][A.7.2.2]

- 文書、保管媒体への表示
- 社外への開示方法
- 廃棄方法

2. 文書・可搬記憶媒体管理

(1) 文書・可搬記憶媒体の管理について、マニュアルを作成し、管理手順を明確にすること。[A.7.2.2][A.10.7.1]

(2) 文書・可搬記憶媒体の廃棄について、以下の対策を実施すること。 [A.7.2.2][A.10.7.1]

- 廃棄マニュアルを作成する
- 焼却、溶解処理等、記載情報が判読できない形で廃棄する

3. 情報システム機器管理

(1) 情報機器について、財産目録を作成すること。 [A.7.1.1]

(2) 情報機器について、盗難防止策を講じること。 [A.9.2.1]

4. 情報セキュリティ監査

(1) 適切な情報セキュリティ監査を定期的に行うこと。 [A.15.3.1]

5. 業務継続計画

(1) コンピュータシステムにトラブルが発生し、利用が不可能となっても、業務の継続が可能となるように、業務継続計画を作成すること。 [A.14.1.1]

第2章　人事総務

従業員、外部委託および施設に対して実施すべきセキュリティ対策

6. 従業員・外部委託管理

(1) 従業員採用時には「採用審査」を行うこと。 [A.8.1.2]
(2) 従業員の情報セキュリティに対する責任と守秘義務を明確にすること。 [A.8.1.1]
(3) 外部委託契約時、以下の項目を明確にすること。 [A.8.1.3]
- 外部委託先のスタッフの守秘義務

7. 施設管理

(1) 従業員の入館時には、身分証明書を提示させ、施設内では常に身分証明書を携帯させること。 [A.9.1.2]
(2) マシンルームは施錠可能とし、必要に応じて入退管理装置を設置すること。 [A.9.1.1][A.9.1.2]

第3章　情報システム構築

情報システムを構築する際に実施すべきセキュリティ対策

8. セキュリティ機能設計

(1) 情報システムの利用に先立ち、利用者 ID や利用者カードにて一意に利用者の識別を行うことができること。 [A.11.5.2]
(2) パスワードを入力する時に、非表示または伏せ字にして、入力したパスワードを画面上に表示させないようにできること。 [A.11.5.1]
(3) パスワードで使用する文字列に対して、下記に示す機能を採用し、パスワードの強度を情報システムで確保できるようにすること。 [A.11.5.3]
- 最少文字数を設定できること
- 連続した同一文字列を禁止できること
- ユーザ ID と同一の文字列を禁止できること

(4) 利用者の権限に応じて、資源へのアクセスを制限できること。 [A.11.1.1]
(5) 情報の重要度に応じて、格納されるデータの暗号化ができること [A.12.3.1]

9. 開発品質保証管理

(1) ソースコード、オブジェクトコード、情報システム設計書等については、構成管理を行うこと。 [A.12.5.1]
(2) テスト計画を作成し、セキュリティ機能の正常動作を確認すること。 [A.12.1.1]

10. 開発環境管理

(1) 本番システムと開発システムを分離すること。 [A.10.1.4]

(2) 本番システムの実データをテストデータとして使用しないこと。[A.12.4.2]

第4章　情報システム運用

情報システムを運用する際に実施すべきセキュリティ対策

11. 情報システム運用管理

(1) 情報システムの運用マニュアルを作成し、文書化すること。 [A.10.1.1]
(2) システムの変更を行う場合は、管理者の承認を得ること。 [A.10.1.2][A.12.5.2][A.12.5.3]
(3) システム運用における事故管理の責任を明確にすること。 [A.13.1.1]
(4) 定期的にバックアップを行い、そのバックアップデータを保護すること。 [A.10.5.1]
(5) 運用に関する作業記録を作成すること。 [A.10.10.4]

12. 利用者登録管理

(1) 利用者ＩＤを一意に割り当てること。（ひとつの利用者ＩＤに対して、複数の利用者を割り当てないこと。） [A.11.5.2]

13. ホストおよびサーバ管理

(1) 各ホストおよびサーバは、不必要なサービスを提供しないよう管理すること。
(2) 各ホストおよびサーバの監査ログを取得し、不正アクセスの兆候を発見すること。 [A.10.10.1][A.10.10.2]

14. ウィルス対策

(1) パソコンにウィルス対策ソフトを導入すること。 [A.10.4.1]
(2) ウィルス対策ソフトのパターンファイルを最新の状態に保つための環境を整備すること。 [A.10.4.1]

15. ソフトウェア管理

(1) 管理者に無断でソフトウェアをインストールしないこと。 [A.12.5.1]
(2) ソフトウェアの違法コピーを行わないこと。 [A.15.1.2]

第5章　ネットワーク

ネットワークを構築･運用する際に実施すべきセキュリティ対策

16. ネットワーク管理

(1) 外部ネットワークと内部ネットワークを接続する場合、その接続口を管理された箇所に

限定すること。 [A.11.4.7]

(2) 外部ネットワークと内部ネットワークを接続する場合、その接続口にファイアーウォール機構を設けること。 [A.11.4.7]

17. リモートアクセス管理

(1) モバイル用のパソコンには、必要に応じて以下の保護対策を行うこと。

- BIOSパスワードの設定 [A.11.5.1]
- 情報の暗号化 [A.12.3.1]

(2) インターネット経由でリモートアクセスを行う場合、リモートアクセスを行うパソコンとリモートアクセスサーバ間の通信を暗号化すること。 [A.10.8.4]

第6章　利用者管理

情報システムの利用者に対して実施すべきセキュリティ対策

18. 利用者セキュリティ

(1) 利用者ＩＤ、利用者カード等を他人に貸与させないこと。[A.11.3.1]

(2) パスワードを定期的に変更させること。[A.11.3.1]

(3) 離席時には、次の対策をとらせること。[A.11.3.3]

- 一旦ログオフして、システムの利用を中断する
- パスワード付きスクリーンセイバーを利用する

19. 電子メールセキュリティ

(1) 業務以外の電子メールの私的利用を禁止すること。 [A.15.1.5]

(2) 大容量ファイルを添付したメールの送信を禁止すること。

20. パソコン管理セキュリティ

(1) 許可なくパソコンにデバイスを増設することを禁止すること。

(2) 個人所有のパソコンを、会社に持ち込むことを禁止すること。

21. 情報セキュリティ教育

(1) 新規採用者に対して、情報セキュリティ教育を実施すること。 [A.8.2.2]

(2) 従業員に対して、定期的に情報セキュリティ教育を実施すること [A.8.2.2]

4. 不正アクセス対策

目標

組織内の情報資産（システムおよび情報）を社外に存在する不正アクセスを企図する者から防御し、その完全性、機密性、可用性を業務上必要なレベルで保持する。

第1章　不正アクセス対策の基本方針

(1) 【基本方針】 システム管理者は、不正アクセスを企図する者からシステムを防御するための予防、検知、および回復の方針を明確にすること。

第2章　不正アクセスの予防

1. インターネット接続とファイアウォール

(1) 【インターネット接続点の限定】 組織内のネットワーク（以降「内部ネットワーク」と呼ぶ）と、インターネットの接続点は原則として一ヵ所に限定すること。業務上やむを得ない場合は複数の接続点を持つことを認めるが、この場合はすべての接続点で同じ強度のセキュリティ対策を実施しなければならない。 [A.11.4.7]

(2) 【DMZ の構築】 内部ネットワークの資源を不正アクセスの脅威から守るため、ファイアウォールを用いて中立のセグメント（以降「DMZ」と呼ぶ）を構築すること。 [A.11.4.5]

(3) 【内外直結アクセスの禁止】 内部ネットワークとインターネットの間の通信は、例外なく DMZ 上の機器で中継を行うこと。ファイアウォールで内部ネットワークとインターネット間の直接の通信を許可することはいかなる理由があっても禁止する。

(4) 【通過プロトコルの限定】 ファイアウォールを通過する通信は、業務上必要であると公式に認められた通信プロトコルに限定すること。不特定多数のプロトコルの通過を許可するルールを設定してはならない。 [A.11.4.1]

2. 公開サーバ

(1) 【DMZ 設置】 インターネットに何らかのサービスを一次的に提供するサーバを以降「公開サーバ」と呼ぶ。公開サーバの例を以下に示す。公開サーバは（ファイアウォール自身を除き）DMZ に設置すること。

- ファイアウォール、ウェブ（http）サーバ、DNS サーバ、メール(smtp)サーバ、プロキシサーバ、リモートアクセス（radius）サーバ

(2) 【非公開ポートのクローズ】 公開サーバでは、提供するべきサービス以外の TCP/UDP サービスポートを常時クローズしておくこと。

(3) 【アクセス権限の制限】 公開サーバでは、ディレクトリ／ファイルのアクセス権限を、可能な限り制限すること。不特定多数にアクセスを許可する性質のアカウント（ゲストアカウント）は OS レベルでは提供してはならない。

(4) 【セキュリティ情報の収集と対処】 公開サーバにおいては、構成するソフトウェアのセキュリティ情報を可能な限り収集すること。収集したセキュリティ情報については、その重大性を分析し、そのリスクに見合った対処を速やかに実施すること。 [A.12.6.1]

(5) 【セキュリティ強度の検証】 公開サーバのセキュリティ強度を、客観的な方法で定期的に検証すること。 [A.12.6.1][A.13.1.2]

3. 運用監査

(1) 【運用監査】 システムの運用にセキュリティ上の問題がないかどうか、定期的に客観的な監査を実施すること。 [A.15.2.1][A.15.2.2]

(2) 【是正処置】 監査の結果、判明した問題点については、そのリスクの大きさを評価し、リスクに見合った適切な対処を実施すること。 [A.15.2.1][A.15.2.2]

第3章　不正アクセスの検知

4. ログチェック

(1) 【ログ異常の検出】 システム管理者、およびサーバ管理者は、管理対象の機器のログを定期的にチェックし、異常値があった場合に検出できるようにすること。 [A.10.10.2]

(2) 【異常調査】 ログチェックの結果、異常がみられた場合はその原因を調査すること。不正アクセスの兆候など、重大なリスクを示唆する場合は、速やかにシステム運用責任者に報告し、適切な対処を行うこと。 [A.10.10.2]

5. 侵入検知

(1) 【侵入検知システムの導入】 特に重要な業務を実施しているシステム、および特に不正侵入のリスクが高いシステムにおいては、侵入検知システムを導入し、休日・夜間も含め無停止運用すること。 [A.10.10.2]

(2) 【侵入分析】 侵入検知の結果、異常がみられた場合はその内容を分析すること。不正アクセスの兆候など、重大なリスクを示唆する場合は、適切な対処を行うこと。また可能な限り速やかにシステム運用責任者に報告すること。 [A.10.10.2]

第4章　不正アクセスからの回復

6. 侵入発見時の対応

(1) 【報告義務】 不正侵入の事実または明確な兆候を検知した者は、速やかにシステム運用責任者に報告すること。 [A.13.1.1]

(2) 【現状把握】 システム管理者は、不正侵入の事実または兆候を知った場合は、ただちに以下の状況を把握すること。 [A.13.1.1]

- 不正侵入かどうかの判断
- 被害範囲
- 被害の大きさ
- 被害拡大の可能性

(3) 【一次対応】 不正侵入であると判断された場合は、一次対応として速やかに以下の対処を取ること。 [A.13.2.1]

- 被害拡大の防止（インターネットを含むネットワークからのシステム切り離し）
- 現状維持（リブートなど、その場の対処の禁止）
- システム運用責任者への連絡
- 関係各部門、上位部門への連絡
- 捜査機関（警察）への連絡（必要と判断された場合）

(4) 【復旧計画】 システム運用責任者は、関係者を招集し、復旧計画を決定すること。復旧計画には、以下の内容を記載すること。計画策定後は、計画に従って復旧作業を行うこと。 [A.13.2.1]

- 被害規模の推定
- 現状復帰計画
- 原因となったセキュリティ問題の除去計画
- 再稼動前のセキュリティ検証の計画

(5) 【アクセス制御の維持】 対応中および復旧作業中においても、通常運用時に実施されているアクセス制御を維持すること。運用継続や作業上の都合を理由としてセキュリティレベルを下げることは認めない。

(6) 【復旧検証】 復旧完了後再稼動する前に、再度の侵入がないことを保証するため、客観的なシステムのセキュリティ検証を実施すること。

5. 情報漏洩対策

目標

組織内に存在する機密性情報を適切に保護し、権限のない者がこれらの情報にアクセスすること、およびこれらの情報が意図した範囲から外へ漏洩することを防止する。

第1章　機密性情報の制御方針

1. 機密性情報の識別

(1) 【機密性ランクの定義】 組織内における情報の機密性ランクを定義すること。一般的に「秘」「極秘」「部外秘」などの用語で呼ばれるものでもよい。機密性ランク同士は互いに独立な関係でもよいが、「通常」－「重要」－「最重要」のように互いに順序を持つものがより理解しやすい。 [A.7.2.1]

(2) 【アクセス権限の定義】 それぞれの機密性ランクに対して、どのような権限を持った者がその機密性ランクを持った情報にアクセス可能とするかを明確に定義すること。[A.7.2.1]

(3) 【機密性情報の明確化】 組織内において機密性を必要とするすべての情報に対して、機密性ランクを明確に指定すること。このとき、必要以上に機密性を高く指定することは、コスト増加要因となることに十分留意すること。 [A.7.2.1]

(4) 【識別の見直し】 機密性ランク、アクセス権限、機密性情報などの指定について、定期的に見直しを実施すること。 [A.7.2.1]

2. 機密性情報の制御原則

(1) 【機密性情報の制御】 機密性情報は、いかなる場面においても権限を持つ者以外はアクセスできないように保護されていること。これは機密性情報のライフサイクル全体を通して実現されていなければならない。例えばシステム上に保存されている機密性情報は、プリントアウトされた後は文書として同等のアクセス制御の対象にならなければならない。[A.11.1.1]

(2) 【システムによる保護】 システム上にある機密性情報は、システムが装備するアクセス制御機能により、アクセス制御されることが保証されていること。システムがアクセス制御機能を提供できない場合は、システム自身の利用を権限を持つものだけに制限すること。[A.11.6.1]

(3) 【情報媒体の保護】 文書、磁気媒体などの情報媒体は、権限を持つ者だけが情報にアクセスできるように、物理的に保護すること。 [A.10.7.3]

3. 機密性保護対策

(1) 【機密性保護対策の明確化】 各機密性ランクに対して、最低限要求される保護対策を明確に規定すること。 [A.7.2.2]

第2章　保護対策

4. 暗号化

(1) 【暗号化】 情報の機密性に応じて、暗号化を行うこと。 [A.12.3.1]
(2) 【鍵管理】 暗号化のための秘密鍵は、権限のない者がアクセスできないように管理すること。 [A.12.3.2]
(3) 【鍵の預託】 暗号化のための秘密鍵は、万一の喪失に備え、本人以外の預託者にコピーを預けるか、またはマスターキーを預託すること。この場合、預託者は対象となる情報へのアクセス権限を持つ者でなければならない。 [A.12.3.2]
(4) 【預託鍵の使用】 預託された鍵の使用は、あらかじめ定められた手続きに従って行うこと。預託者は、預託鍵を使用した事実を記録すること。[A.12.3.2]
(5) 【暗号方式】 使用する暗号の方式は、情報の機密性に応じた強度を持つものであること。一般に、広く公開されて強度の議論を経た方式以外は採用するべきではない。また、鍵長についても同様に強度を評価し決定すること。 [A.12.3.1]

5. インターネットアクセス

(1) 【インターネット監視】 情報の機密性に応じて、情報漏洩を検知できるようにインターネットと組織間の情報を監視すること。さらに必要であれば、特定のキーワードを含む情報の流出を検知できる機構を装備すること。 [A.10.10.2]
(2) 【インターネットログ】 情報の機密性に応じて、インターネットと組織間を流通する情報を記録すること。 [A.10.10.2]
(3) 【インターネットアクセス制御】 特に FTP、HTTP などのプロトコルに対して、業務上必要のない通信先との接続を禁止すること。 [A.11.4.1]

6. 機密性対策機器

(1) 【機密性対策機器】 情報の機密性に応じて、特殊な情報漏洩対策を施した機器を利用すること。例えば、以下のような機器の利用が考えられる。
- 起動に暗証番号を要求するコンピュータ
- アクセスに暗証番号を要求する記録メディア

第3章　定常運用

7. 教育

(1) 【利用者教育】 部門の責任者は、機密性情報の取り扱いおよび機密性情報を扱うシステムの操作についての教育を必要に応じて実施すること。 [A.8.2.2]

8. 監査

(1) 【トレースログ】 機密性情報を扱うシステムにおいては、不正な利用や過失による事故を追跡できるように、利用者の行為をトレースログとして常に記録すること。 [A.10.10.1][A.10.10.4]

(2) 【トレースログの監査】 トレースログの定期的なチェックを必要に応じて実施すること。 [A.10.10.2]

第4章　非定常運用

9. 保守と廃棄

(1) 【保守時の機密保持】 機密性情報を持つ機器の修理・保守は、信頼できる業者に依頼すること。必要に応じて、守秘義務の契約を締結すること。また、可能な限り機密性情報の削除や暗号化などの対処を行うこと。 [A.10.2.1]

(2) 【機器廃棄】 機密性情報を扱った機器を廃棄する場合、機器内に機密性情報が残存しないように次のような対処すること。 [A.9.2.6]

- ディスクのフォーマット（わずかだが残存磁気が残ることがある）
- 消磁ツールの利用
- 暗号化ツールの利用（データを暗号化してから捨てる）
- 安全な廃棄処分サービスの利用

(3) 【媒体廃棄】 機密性情報を扱った媒体を廃棄する場合、媒体内に機密性情報が残存しないように対処すること。媒体を再利用する場合もこれに準じること。一部の媒体は、ファイルを削除してもデータ自身は媒体に残っている場合があるので留意すること。 [A.10.7.2]

10. セキュリティインシデント

(1) 【インシデントの報告】 セキュリティ上の問題点や事故を発見した利用者は、所定の手続きに従ってその事実を報告すること。 [A.13.1.1]

(2) 【インシデントの対処】 セキュリティインシデントに対して、適切に処理を行い、被害を最小限に抑えること。対処には以下のような作業が含まれる。 [A.13.2.1]

- 当面の問題回避
- 被害拡大の防止（被害の極小化）
- 原因の特定と再発防止処置の実施

6. ウイルス対策

目標

社内の情報資産（システムおよび情報）をコンピュータウイルスから防御し、その完全性、機密性、可用性を業務上必要なレベルで保持する。

第1章　ウイルス対策の基本方針

(1) 【基本方針】 システム管理者は、システムをウイルスから防御するための予防および回復の方針を明確にすること。 [A.10.4.1]

第2章　ウイルスの予防

1. 1. 機器ベース対策

(1) 【ウイルス対策ソフトウェア】 組織内で使用する情報機器は、以下のいずれかに相当する場合を除き、必ずウイルス対策ソフトウェアを導入すること。なお、以下の場合に該当した場合でも、可能な限りのウイルス対策を実施すること。 [A.10.4.1]

- 特殊な用途に使用されるシステムで、ウイルスの侵入がないことが合理的に説明できる場合。
- 特殊なアーキテクチャや OS を使用しており、一般的なウイルスに対して脆弱性がないと認められる場合。
- 特殊なアーキテクチャや OS を使用しており、有効なウイルス対策ソフトウェアが提供されていない場合。

(2) 【パターンファイルの更新】 ウイルス対策ソフトウェアのパターンファイルは、アップデートがベンダーから提供されたとき、あらかじめ定めた許容期間内に確実に更新を行うこと。可能であれば、これを保証するシステムを構築すること。 [A.10.4.1]

(3) 【更新状況の把握】 パターンファイルの更新状況を把握できる仕組みがあり、更新されていないクライアントに対して適切な処置ができること。 [A.10.4.1]

2. サーバベース対策

(1) 【メールスクリーニング】 組織内部とインターネット間で交換されるメールにウイルスが混入することを阻止するため、メールサーバと連携して動作するウイルスフイルタリン

グソフトウェアを導入すること。 [A.10.4.1]

(2) 【Web スクリーニング】 組織内部からインターネットに対する Web アクセスにより組織内にウイルスが侵入することを予防するため、必要に応じてプロキシサーバと連携して動作するウイルスフイルタリングソフトウェアを導入すること。 [A.10.4.1]

3. 運用対策

(1) 【利用者の意識向上】 利用者に対してウイルスの危険性と予防方法を周知するための意識向上のための活動を実施すること。周知内容には以下の項目を含むこと。 [A.8.2.2][A.10.4.1]

- 不審な添付ファイルを開かない
- 不審なマクロを実行しない
- 不審なソフトウェアをインターネットからダウンロードしない
- 信用できない ActiveX 等のプログラムをインターネット上の Web から受け取らない
- ブラウザや OS のセキュリテイホールに対処しておく

(2) 【媒体交換】 組織外部から受け取った媒体および組織外部に送り出す媒体については、必ず最新のパターンファイルを装備したウイルス対策ソフトウェアを利用してウイルスチェックを実施すること。 [A.10.4.1]

4. 復旧のための準備

(1) 【復旧のための準備】 システム管理者は、万一ウイルスが侵入した場合に迅速に復旧できるよう準備を実施しておくこと。例えば以下のような項目が考えられる。 [A.13.2.1]

- 環境の標準化
- 機器の構成管理
- バックアップ

第3章　ウイルス侵入時の対処

5. 侵入発見時の対応

(1) 【侵入報告】 ウイルス侵入の事実または兆候を検知した者は、該当の機器をネットワークから切り離し、速やかにシステム管理者に報告し、その指示に従って対処すること。 [A.13.1.1]

(2) 【現状把握】 システム管理者は、ウイルス侵入の事実または兆候を知った場合は、ただちに以下の状況を把握し、システム運用責任者に報告すること。 [A.13.1.1]

- 被害範囲
- 被害の大きさ
- 被害拡大の可能性

(3) 【復旧】 ウイルス侵入の被害が大規模である場合、システム運用責任者は、関係者を招集し、復旧計画を決定すること。復旧計画には、以下の内容を記載すること。計画策定後は、計画に従って復旧作業を行うこと。 [A.13.2.1]

- 被害規模の推定
- 現状復帰計画
- 原因となったウイルス対策上の問題の除去計画

参考資料

この分野のセキュリテイポリシー整備にあたり、以下の資料を参考にするとよい。

「コンピュータウイルス対策基準」通商産業省告示第 429 号

7. コンテンツセキュリティ

目標

リッチコンテンツを安全に公開することを目標とし、公開コンテンツの不正利用抑制を実現する。

第1章　不正利用抑制方針(情報資産管理対策の明確化)

(1) 【情報資産管理対策の明確化】 公開対象とするリッチコンテンツにおいて、下記ポリシーに基づき、情報資産管理対策を明確に規定すること。リッチコンテンツの管理に関して、公開対象とするリッチコンテンツに対する以下責任を明確にすることにより、適正な保護対策を実現する。 [A.15.1.2]

- リッチコンテンツの作成者は、作成したコンテンツの所有者(著作権など)を明確にすること。
- 所有者は、リッチコンテンツの管理責任者を割り当て、適切な保護対策を実施させること。
- 管理責任者は、電子透かしなど、リッチコンテンツの不正利用を検出・防止する仕組みを導入すること。
- 管理責任者は、必要に応じ、コンテンツ利用者に対し、不正利用検出・防止の仕組みが導入されていることを告知すること。

第2章　不正利用抑制、不正利用による事故時の対応

(1) 【不正利用抑制と不正利用による事故時の対応】 管理責任者は、情報資産管理対策に関する下記ポリシーに基づき、不正利用抑制と事故対応すること。 [A.13.2.1]

- コンテンツ、利用者を識別し、コンテンツ利用環境を設定すること。
- 事故発生時の管理体制の明確化、事故発生を想定した対応手順の作成、手順の確認を行う。
- 情報資産の不正利用状態を確認し、内容改竄、内容破壊、複製状態を判定する。
- 事故発生が確認できた場合は、事前に作成した手順に従い対応を行うこと。

8. フィジカルセキュリティ

目標

業務施設及び業務情報に対する認可されていないアクセス、損傷及び妨害を防止する

第1章　フィジカルセキュリティ対策の基本方針

(1) 【基本方針】 システム管理者は、フィジカルセキュリティ対策のための管理および作業の方針を明確にすること。

第2章　センタの管理

1. 物理的セキュリティ境界

(1) 【セキュリティ境界の定義】セキュリティ境界を明確に定義すること。 [A.9.1.1]

(2) 【セキュリティ境界】情報処理設備を収容した建物又は敷地の境界は、物理的に頑丈（境界には間げきがない又は容易に侵入できる領域がない）であること。敷地の外周壁を堅固な構造物とすること、及びすべての外部扉を認可されていないアクセスから開閉制御の仕組み（かんぬき、警報装置、錠など）で適切に保護すること。 [A.9.1.1] [A.9.1.2]

(3) 【アクセスの管理】敷地又は建物への物理的アクセスを管理するために、有人の受付又はその他の手段を設けること。敷地及び建物へのアクセスは、認可された職員だけに制限すること。 [A.9.1.1]

(4) 【壁】物理的な壁は、認可されていない立ち入り、並びに火災及び洪水が引き起こす環境への悪影響を防止するために、必要ならば、床から天井にわたる構造で設けること。 [A.9.1.1]

(5) 【防火扉】セキュリティ境界上にあるすべての防火扉は、警報装置付き及び密閉式であること。 [A.9.1.1]

2. 物理的入退管理策

(1) 【入退の管理】セキュリティが保たれた領域への訪問者を監視し、又は立入り許可を求めさせること、及びその入退の日付・時刻を記録すること。その訪問者には、認可された特定の目的に限ってのアクセスを認めること、並びにその領域のセキュリティ要求事項及び非常時の手段を説明した文書を渡すこと。 [A9.1.2]

(2) 【アクセスの管理】取扱いに慎重を要する情報及び情報処理設備へのアクセスを管理して、認可された者だけに制限すること。アクセスをすべて認可して、妥当性を確認するために、例えば、暗証番号付きの磁気カードといった認証管理策を用いること。すべてのアクセスの監査証跡は、安全に保管しておくこと。 [A.9.1.2]

(3) 【身分証明の着用】すべての要員に、目に見える何らかの形状をした身分証明の着用を要求すること、並びに付添いを伴わない見知らぬ人及び目に見える身分証明を着用していない人に対しては、誰であるか問い掛けるよう奨励すること。 [A.9.1.5]

(4) 【アクセス管理の保守】セキュリティが保たれた領域へのアクセス権は、定期的に見直し及び更新すること。 [A.8.3.3]

3. オフィス、部屋及び施設のセキュリティ

(1) 【設置場所】主要な設備は、一般の人のアクセスが避けられる場所に設置すること。 [A.9.2.1]

(2) 【用途の表示】建物は目立たせず、その用途を示す表示は最小限とすること、さらに、情報処理作業の存在を示すものは建物の内外を問わず一切表示しないこと。 [A.9.1.6]

(3) 【支援装置】例えば、複写機、ファクシミリといった支援機能及び装置は、情報漏洩などをもたらすおそれがあるアクセスを避けるために、セキュリティの保たれた領域内の適切な場所に設置すること。 [A.9.2.1]

(4) 【不在時の施錠】要員が不在のときは扉及び窓に施錠すること。特に一階の窓については、外部に対する防御を考慮すること。 [A.9.1.3]

(5) 【遮へい手段】すべての外部扉及びアクセス可能な窓を遮へいするためには、専門の標準類に従って取り付けられ、かつ、定期的に点検する、適切な侵入者の検知システムを設置すること。無人の領域には常に警報装置を稼動させること。例えば、コンピュータ室又は通信室といった他の領域においても、このような仕組みを設置すること。 [A.9.1.3]

(6) 【設備の保護】組織自ら管理する情報処理設備は、第三者が管理するものから物理的に分離しておくこと [A.9.1.6]

(7) 【文書の保護】取扱いに慎重を要する情報処理設備の所在を掲げた職員録及び社内電話帳は、一般の人に容易に見られないようにすること。 [A.9.1.6]

(8) 【危険物との分離】危険物又は可燃物は、セキュリティが保たれた領域から十分に離れた場所に、安全に保管すること。セキュリティが保たれた領域には、事務用品などを、必要もないのに大量に保管しないこと。 [A.9.1.4]

(9) 【バックアップ媒体】緊急時に用いる代替装置及びバックアップされた媒体は、主事業所で起きた災害によって損傷しないように、主事業所から十分に離れた場所に置くこと。 [A.10.5.1]

第3章　センタでの作業

4. セキュリティが保たれた領域での作業

(1) 【作業領域の存在】セキュリティが保たれた領域の存在又はそこでの作業は、知る必要がある要員だけに知らせるという基本に沿って、その必要がある要員だけが知っていること。 [A.9.1.3]

(2) 【未監視下での作業】セキュリティが保たれた領域において監視もなく作業することは、安全のため及び悪意のある行動を防ぐために、避けること。 [A.9.1.5]

(3) 【無人領域の施錠】セキュリティが保たれた領域を無人にするときは、物理的な施錠を行うこと、及び定期的に検査すること。 [A.9.1.2]

(4) 【外部者の作業】セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスを許可するときは、アクセスができる範囲を限定し、アクセスが必要な場合に限ること。このアクセスは認可のもとにおくこと、及び監視下におくこと。あるセキュリティ境界の中にセキュリティ要求事項の異なる領域が存在するときは、その領域の間に、物理的アクセスを管理するための障壁及び境界を追加することが必要な場合がある。 [A.9.1.5]

(5) 【作業装置の管理】認可なしの、写真機、ビデオカメラ、録音機、又はその他の記録装置の使用は、許さないこと。 [A.9.1.5]

5. 受渡し場所の隔離

(1) 【受渡し要員】建物の外から一時保管場所へのアクセスは、本人の確認及び認可を受けた要員に限定すること。 [A.9.1.6]

(2) 【受渡し場所】一時保管場所については、建物内の他の場所にアクセスすることなく受渡しの要員が荷おろしできるように、設計を行うこと。 [A.9.1.6]

(3) 【受渡し場所の扉】一時保管場所の内部扉を開いているときは、外部扉を閉めること。 [A.9.1.6]

(4) 【搬入品の検査】一時保管場所から使用場所に搬入品を移送する前に、危険の可能性がないかどうか、その品物を検査すること。 [A.9.1.6]

(5) 【搬入品の管理】敷地内に搬入するときには、適切ならは、搬入品の登録を行うこと。 [A.9.1.6]

9. 電子認証基盤

目標

システムにおける識別と認証の方針を明確化し、システムの機密性、完全性、可用性、真正性を維持するための基盤を確立する。

第1章　原則

1. 識別と認証

(1) 【一意識別】 権限を持つシステムの利用者は、一意に識別されること。 [A.11.5.2]

(2) 【利用者 ID の交付】システムにおいて利用者の識別に ID を用いる場合は、権限を持つすべての利用者に対して、一意の利用者 ID を交付すること。 [A.11.5.2]

(3) 【認証】 システムは、そのシステムに要求されるセキュリティ強度に相応する方法で、必ず利用前に利用者の認証を実施すること。システム運用責任者は、管理するシステムにおいて、必要な強度を満たすセキュリティ認証方法を決定すること。 [A.11.5.2]

(4) 【高強度認証】 高いセキュリティ強度が必要なシステムの認証には、以下に示すような強度の高いセキュリティ認証方式を使用すること。 [A.11.5.2]

- 生体認証（指紋認証、網膜認証、光彩認証、筆跡認証、掌紋認証など）
- 所持物による認証（磁気カード、IC カードなど）と暗証の組み合わせ

(5) 【リモート認証】 安全でない伝送路（インターネットなど）を経由して遠隔地からシステムを利用するために認証を行う場合は、認証情報の漏洩に考慮した認証方式（ワンタイムパスワード、チャレンジレスポンス方式など）を使用すること。 [A.11.4.2]

2. 真正性維持

(1) 【真正性維持対象の明確化】 業務上真正性の維持が必要とされる情報を明確にすること。 [A.10.8.5]

(2) 【電子署名】 真正性維持が必要な情報に対しては、電子署名を付与し、情報の出自および完全性を保証すること。 [A.10.8.5]

(3) 【電子証明書システム】 以下のような要件がある場合は、必要に応じて電子証明書システムを導入すること。 [A.10.8.5]

- 第三者に対して信頼性の高い電子署名を提供する。
- 電子署名の運用を簡略化し、信頼性を向上させる。

第2章　識別と認証の要件

3. 利用者 ID

(1) 【利用者 ID の再利用の禁止】 利用者 ID の再利用はしないこと。 [A.11.2.1]

(2) 【利用者 ID の削除】 権限を失った利用者の利用者 ID はすみやかに削除すること。 [A.11.2.1]

(3) 【利用者 ID の管理】 利用者がどのような権限を持つか、システム上どのような権限が与えられているかなどの情報は、システム管理者によって管理されていること。必要に応じてこの管理を支援する機構を導入すること。 [A.11.2.1]

4. パスワード認証

(1) 【パスワード強度】 利用者は、既知のパスワード解読技術（辞書攻撃、ブルートフォースなど）に対して十分な耐性を持つパスワードを選択すること。システム管理者は、利用者がそのようなパスワードを選択するよう、周知および教育を行うこと。必要に応じて、脆弱なパスワードの選択を許さないようにシステムの環境を設定すること。 [A.11.3.1]

(2) 【連続試行の禁止】 ブルートフォースを禁止するため、パスワードによる認証に一定回数連続して失敗した場合は、セッションを切断し、一定時間認証の試行を禁止すること。 [A.11.5.1]

(3) 【パスワードの更新】 利用者は、一定期間のうちに最低 1 回はパスワードを変更すること。必要に応じて、システムが利用者にこれを強制できること。これを実現するために、システムはパスワード変更後一定期間はさらに変更することを禁止できること。 [A.11.5.1]

(4) 【パスワードの再利用制限】 利用者は、以前使用したパスワードを一定期間は使用しないこと。必要に応じて、システムがこれを利用者に強制できること。これを実現するために、システムはパスワードの履歴を管理できること。 [A.11.5.1]

5. 利用者の注意義務

(1) 【利用者の注意義務】 前項の他、システム管理者は、以下のような利用者 ID／パスワードに関する注意事項を利用者に周知徹底し、実行させること。 [A.11.2.3]

- 利用者 ID、あるいは認証目的に利用される媒体（IC カードなど）の貸し借りをしない。
- パスワードを人目に付く場所に記録しない。

6. 生体認証

(1) 【代替手段】 生体認証を用いて認証を行う場合は、認識装置の誤差を勘案し、正当な利用者が認証に失敗したときに備えてパスワードによる認証など代替の認証手段を用意しておくこと。 [A.11.5.2]

第3章　電子証明書システムの要件

7. 証明書認証

(1) 【認証局の運用規定の明確化】 社内において認証局を運用して証明書を発行する場合は(自社構築、アウトソーシングいずれも)、その運用規定(CP/CPS:Certificate Policy / Certificate Practice Statement)をあらかじめ策定すること。その中で、認証対象の審査基準、証明書の失効手順等を規定すること。

(2) 【利用者による秘密鍵の管理】 利用者が秘密鍵の保管に関し、以下のような点に留意するように周知すること。 [A.12.3.2]

- 他人に貸与しない。
- IC カード等のハードトークンに保管することが望ましい。
- ファイルトークンに保管する場合は、PC は id/パスワード管理できる OS を使用する。

10. 電子文書保証

目標

情報に対して業務上必要な信頼性を付与し、かつ第三者に対してその信頼性を証明できる運用機構を確立する。

第1章　電子文書保証方針

1. 保証対象情報の識別

(1) 【保証対象情報の明確化】 組織内において、高度なセキュリティ保証を必要とするすべての文書情報を明確に指定すること。ここでいう高度なセキュリティ保証とは、例えば以下のようなものが含まれる。 [A.7.2.2][A.10.8.5]

- セキュリティの確保に対して第三者の検証が可能であること。
- 文書の改ざんを検出できること。
- 文書配信時の送達状況を確認できること。

(2) 【対象情報の厳選】必要以上に指定することは、コスト増加要因となることに十分留意すること。

2. 保証対策

(1) 【保証対策の明確化】 保証対象情報に対して、最低限要求される保護対策を明確に規定すること。 [A.7.2.2][A.10.8.5]

第2章　電子文書の配信

3. 安全な電子文書配信

(1) 【状況確認】 保証対象情報を配信するときは、配信情報の現況（到達状況など）が常に確認できるようにしておくこと。必要に応じてこの要件を実現する仕組みを導入すること。

(2) 【漏洩の防止】 保証対象情報を組織外部へ配信するとき、あるいはインターネットなど組織外部の伝送路を利用して配信するときは、必要に応じて以下のような方法で情報を暗号化するなど、外部への情報漏洩を防止する対策を取ること。 [A.10.8.4]

- アプリケーションによる情報の暗号化
- PGP（Pretty Good Privacy）などの暗号化ツールの利用

- SSL（Secure Socket Layer）などの暗号化プロトコルの利用
- VPN（Virtual Private Network）の利用

(3) 【ウィルスチェック】 保証対象情報を配信するときは、配信データにウィルスが混入しないよう、適切な対策を実施すること。 [A.10.4.1]

(4) 【高度な本人認証】 保証対象情報を配信するときは、必要に応じて ID／パスワードによる認証よりも強度が高い認証方式を導入すること。 [A.11.5.2]

第3章　電子文書の保管

4. 安全な電子文書保管

(1) 【安全な電子文書保管】 保証対象情報は、必要に応じて以下の要件のいずれか、またはその組み合わせを満たす方法で保管すること。また、要件が満たされる状況で保管されていたことを第三者に証明できるようにしておくこと。 [A.7.2.2][A.10.8.5]

- 存在証明：過去のある時点においてその情報が存在したことを証明できること。
- 機密性の維持：権限のある利用者だけがその情報を知ることができること。
- 改ざんの検知：情報に対して改変が行われたことを知ることができること。
- 見読性の維持：必要なときにはいつでも情報を読み取ることができること。

(2) 【原本性保証】 原本性保証を必要とする情報は、前項の「機密性の維持」「改ざんの検知」「見読性の維持」をすべて満たすように保管すること。[注] 一般に文書の原本性という場合は、「唯一性」（原本は一つしか存在しないこと）の保証が含まれるが、電子文書の原本性保証の要件には通常含まれない。 [A.7.2.2][A.10.8.5]

(3) 【出力】 保証対象情報を出力するときに、文書の保証レベルが損なわれないような考慮をすること。 [A.7.2.2]

11. Web アプリケーションセキュリティ

目標

組織が独自で開発する Web アプリケーションプログラムの安全性を確保し、保証する。

第1章　設計および開発時の留意事項

1. 基本方針

(1) Web アプリケーションを設計する場合は、以下の項目について十分に考慮すること。 [A.12.1.1]

- 悪意を持った利用者または第三者の操作から、適切な強度をもってシステムとデータを保護すること。
- アプリケーションの欠陥や脆弱性を悪用されることで、善意の第三者（利用者またはサイト）に危害を及ぼさないように考慮すること。
- 利用者の個人情報や、操作履歴などプライバシーに関わる情報が漏洩しないように適切に管理すること。
- 業務の処理や、利用者の操作などに関する記録を適切に取得し、保存できること。

2. 認証とセッション管理

(1) アプリケーションの利用者の正当性を確認するため、利用者の識別と認証を適切に行うこと。認証方式は、システムに求められる強度と、可能な技術的選択肢を考慮して決定すること。 [A.11.5.2]

(2) 適切なセッション管理を実施すること。セッション管理技術の選択にあたっては、第三者によるセッションの乗っ取り(ハイジャック)に対して十分な耐性を持つものを選ぶこと。セッション管理の設計にあたっては、以下の項目を考慮対象に含めること。 [A.11.6.1]

- セッショントークン(Cookie など)の暗号化
- 十分なセッショントークンの鍵空間(桁数)の確保
- セッションタイムアウト
- セッション総当り攻撃の検知とロックアウト
- セッションの再認証
- ログアウト時のセッショントークン処理

3. 入出力検証

(1) アプリケーション入出力の検証機能を実装すること。実装にあたっては、以下の原則を適用すること。 [A.12.1.1][A.12.2.1][A.12.2.2]

- 有効かつ既知のデータのみを許可する。
- クライアントから送られて来るすべてのデータは、検証するまで信頼しない。

(2) 以下の攻撃を防御する観点から、十分な入力データの検証と無害化（サニタイジング)を実施すること。 [A.12.2.4]

- クロスサイトスクリプティング
- ダイレクト SQL コマンドの実行
- ダイレクト OS コマンドの実行
- パスの横断（トラバース）とパスの開示
- ヌルバイト入力
- Cookie 操作
- HTTP ヘッダ操作
- HTML フォームフィールド操作
- URL 操作

第2章　セキュリティ検証

4. セキュリティチェック

(1) システム管理者、およびサーバ管理者は、システム完成時、および本稼働後定期的に Web アプリケーションのセキュリティ安全性についてチェックを実施すること。 [A.12.6.1][A.13.1.2]

第3章　運用上の留意

5. 脆弱性発見時の対応

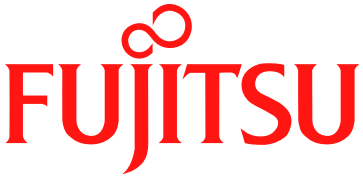
(1) Web アプリケーションにセキュリティ上の問題点または脆弱性が存在することが判明したときは、以下の対処を実施すること。 [A.13.1.2]

- 発生しうる被害の大きさの判定
- すでに発生している被害の調査と特定
- Web アプリケーションによるサービス提供停止の判断
- 利用者を含む関係者への告知
- 脆弱性の一時回避手段の検討と適用

- 脆弱性の根本的な除去の検討と実施

富士通のエンタープライズセキュリティアーキテクチャー 別冊
富士通規準セキュリティポリシー 2007

2007 年 5 月　　初版発行
著　　者　　富士通株式会社 情報セキュリティセンター ESA プロジェクト
編集・発行　　富士通株式会社 情報セキュリティセンター
東京都大田区新蒲田 1－17－25 富士通ソリューションスクエア



THE POSSIBILITIES ARE INFINITE