

広島県情報セキュリティポリシー

はじめに.....	- 1 -
第1章 広島県情報セキュリティ基本方針.....	- 2 -
第1 目的.....	- 2 -
第2 対象機関.....	- 2 -
第3 用語の定義.....	- 2 -
第4 職員の遵守義務.....	- 3 -
第5 情報セキュリティ管理体制.....	- 3 -
第6 情報資産の分類.....	- 3 -
第7 情報資産への脅威.....	- 3 -
第8 情報セキュリティ対策.....	- 3 -
第9 対策基準の策定.....	- 4 -
第10 実施手順の策定.....	- 4 -
第11 情報セキュリティ監査及び自己点検の実施.....	- 4 -
第12 評価及び見直し.....	- 4 -
第2章 広島県情報セキュリティ対策基準.....	- 1 -
第1 目的.....	- 1 -
第2 組織・体制.....	- 1 -
第3 情報資産の管理等.....	- 3 -
第4 物理的セキュリティ.....	- 5 -
第5 人的セキュリティ.....	- 7 -
第6 技術的セキュリティ.....	- 11 -
第7 運用.....	- 21 -
第8 例外措置.....	- 24 -
第9 法令遵守.....	- 24 -
第10 情報セキュリティに関する違反への対応.....	- 24 -
第11 評価及び見直し.....	- 25 -
第12 個人番号利用事務システムにおける特則.....	- 25 -
第13 L G W A Nに接続するシステムにおける特則.....	- 26 -
付 録.....	- 28 -

はじめに	1
------	---

第1章 広島県情報セキュリティ基本方針	2
----------------------------	----------

第1 目的	2
第2 対象機関	2
第3 用語の定義	2
第4 職員の遵守義務	3
第5 情報セキュリティ管理体制	3
第6 情報資産の分類	3
第7 情報資産への脅威	3
第8 情報セキュリティ対策	3
第9 対策基準の策定	4
第10 実施手順の策定	4
第11 情報セキュリティ監査及び自己点検の実施	4
第12 評価及び見直し	4

第2章 広島県情報セキュリティ対策基準	5
----------------------------	----------

第1 目的	5
第2 組織・体制	5
第3 情報資産の管理等	7
第4 物理的セキュリティ	9
第5 人的セキュリティ	11
第6 技術的セキュリティ	14
第7 運用	23
第8 例外措置	26
第9 法令遵守	26
第10 情報セキュリティに関する違反への対応	27
第11 評価及び見直し	27
第12 個人番号利用事務システムにおける特則	28
付録 用語解説	30
〃 情報資産への脅威の例	31

はじめに

【情報セキュリティポリシーの必要性】

情報通信技術の飛躍的な進展を背景に、本県のような業務に情報システムの導入が進んでいる中で、社会的な問題として、情報資産の無許可持出しやシステム誤操作等の故意・過失による情報漏えい、ウイルス感染や悪意を持った者による不正アクセスなどによるデータ改ざん及びシステムトラブル等による業務停止など、情報セキュリティ侵害に関する危険性は絶えることなく、常に顕在化している。

これらの問題に対し、個々の情報システムが安全かつ均質的なセキュリティレベルを確保するとともに、情報システム利用者の情報セキュリティに対する意識の向上を図るため、組織として統一された情報セキュリティポリシーを策定するものである。

【広島県情報セキュリティポリシーの構成】

広島県情報セキュリティポリシー（以下「セキュリティポリシー」という。）は、本県の保有する情報資産に関する情報セキュリティ対策について、総合的にまとめたものであり、図1のとおり、広島県情報セキュリティ基本方針（以下「基本方針」という。）及び広島県情報セキュリティ対策基準（以下「対策基準」という。）から構成されている。

なお、情報セキュリティ実施手順（以下「実施手順」という。）については、個々の情報システムを所管する部局等において策定することとする。

基本方針	情報セキュリティ対策に関する統一的・基本的な方針
対策基準	基本方針を実行に移すためのすべての情報システムに共通の情報セキュリティ対策の基準
実施手順	情報システムごとに定める、対策基準に基づいた具体的なセキュリティ対策のための実施手順

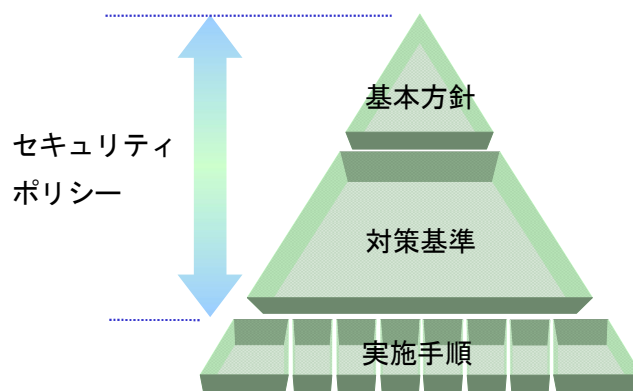


図1 セキュリティポリシーの構成

第1章 広島県情報セキュリティ基本方針

第1 目的

基本方針は、県が保有する情報資産の機密性、完全性及び可用性を維持するため、情報資産の取扱い及び情報セキュリティ対策の基本的な考え方及び方策を定め、本県における情報資産の管理を徹底することを目的とする。

第2 対象機関

対象となる機関は、知事部局、上下水道部、議会事務局、各行政委員会及び警察本部とする。なお、知事部局以外の機関については、知事部局が管理運用する情報システムを利用する部署のみとする。

第3 用語の定義

1 情報

情報システムで取り扱う電磁的データをいう。

2 情報資産

情報及び情報を管理する仕組み（情報システム並びに情報システムの開発、運用及び保守のための資料等を含む。）をいう。

3 情報システム

コンピュータのハードウェア・ソフトウェア、ネットワーク及び記録媒体等で構成されるものであって、これら全体で業務処理を行うための情報処理の体系をいう。

4 ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

5 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

6 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

7 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

8 可用性

情報にアクセスすることを認められた者が、必要なときに、情報にアクセスできる状態を確保することをいう。

9 内部ネットワーク

単一の情報システム及びそれを構成するネットワークをいう。

1 0 外部ネットワーク

単一の情報システムを中心とした際の内部ネットワーク以外の全ての領域をいう。

1 1 庁内ネットワーク

行政LAN・WANネットワーク及びそれと接続された情報システムを構成するネットワークのうち、オンプレミスで構築されたもの（クラウドサービスに構築されたものは除く。）をいう。

1 2 庁外ネットワーク

庁内ネットワーク以外の全ての領域をいう。

1 3 閉域接続系

行政LAN・WANネットワーク及びそれと閉域接続された情報システム（クラウドサービスに構築されたものを含む。）を構成するネットワークをいう。

第4 職員の遵守義務

県の保有する情報資産に関する業務に携わるすべての職員（再任用職員、非常勤職員、臨時職員及び市町等からの派遣職員等を含む）は、情報セキュリティの重要性についての共通の認識を持つとともに、業務の遂行に当たってはセキュリティポリシー及び実施手順を遵守する義務を負う。

第5 情報セキュリティ管理体制

県の保有する情報資産について、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

第6 情報資産の分類

情報資産については、機密性、完全性及び可用性に応じて分類し、その分類に応じた情報セキュリティ対策を行うものとする。

第7 情報資産への脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施するものとする。

- 1 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去等
- 2 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作ミス、故障等の非意図的な要因による情報資産の漏えい・破壊・消去等
- 3 地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

第8 情報セキュリティ対策

第7で示した脅威から情報資産を保護するために、次の情報セキュリティ対策を講じるものとする。

1 物理的セキュリティ対策

情報システムを設置する施設への不正な立入りの防止や、情報資産を損傷・妨害等から保護するために物理的な対策を講じる。

2 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、職員に基本方針及び情報セキュリティに関する法令等の内容を周知徹底するなど、十分な教育及び啓発が行われるよう必要な対策を講じる。

3 技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、アクセス制御、不正プログラム対策等の技術的な対策を講じる。

4 運用

各種対策の実施状況を確認するため、情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等の運用面の対策を講じる。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

第9 対策基準の策定

第8の情報セキュリティ対策を講じるに当たって、遵守すべき行為、判断等の基準を統一的に定めるため、必要となる基本的な要件を明記した対策基準を策定するものとする。

なお、対策基準は公にすることにより本県の行政運営に重大な支障を及ぼすことがあることから非公開とする。

第10 実施手順の策定

セキュリティポリシーを遵守して情報セキュリティ対策を実施するため、個々の情報システムについて具体的な手順を明記した実施手順を策定するものとする。

なお、実施手順は公にすることにより本県の行政運営に重大な支障を及ぼすことがあることから非公開とする。

第11 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

第12 評価及び見直し

情報セキュリティ監査及び自己点検の実施による検証結果等を踏まえるとともに、情報セキュリティを取り巻く状況の変化に対応するため、セキュリティポリシー及び実施手順の見直しを適宜行うこととする。

第2章 広島県情報セキュリティ対策基準

第1 目的

対策基準は、情報セキュリティに関し本県が達成すべき基準を示すものであり、情報セキュリティ確保のために、遵守すべき行為及び判断基準を明らかにすることを目的とする。

第2 組織・体制

情報セキュリティ対策は、次に掲げる管理体制に基づいて実施するものとする。

- 1 最高情報セキュリティ責任者（CISO：Chief Information Security Officer、以下「CISO」という。）
 - (1) 副知事（総務局所掌）を CISO とする。
 - (2) 本県の情報セキュリティに関するすべての責任及び権限を有する。
 - (3) CISO は、情報セキュリティ事案に対処するための体制（CSIRT：Computer Security Incident Response Team）として、情報セキュリティ統括部門を置く。
 - (4) CISO は、CISO を助けて本県における情報セキュリティに関する事務を整理し、CISO の命を受けて本県の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。） 1 人を必要に応じて置く。
 - (5) CISO は、セキュリティポリシーに定められた自らの担務を、副 CISO その他のセキュリティポリシーに定める責任者に担わせることができる。
- 2 情報セキュリティ総括管理者（以下「総括管理者」という。）
 - (1) DX 審議官を総括管理者とする。
 - (2) 情報セキュリティ統括部門を総括する。
 - (3) CISO の指示の下、情報セキュリティの運営を行う。
 - (4) 総括管理者は、情報セキュリティの運営に関する専門的な助言を得るため、必要に応じ情報戦略担当部長をその任に置くものとする。
 - (5) 総括管理者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。
- 3 情報セキュリティ統括部門（以下「統括部門」という。）
 - (1) 総務局デジタル基盤整備課を統括部門とする。
 - (2) 総括管理者の指示の下、情報セキュリティの実際の運用を行う。
 - (3) 情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署とし、また、外部の事業者等との情報共有を行う。
 - (4) 庁内で情報セキュリティ事案が発生した場合、当該事案の対処に係る指示、助言を行う。

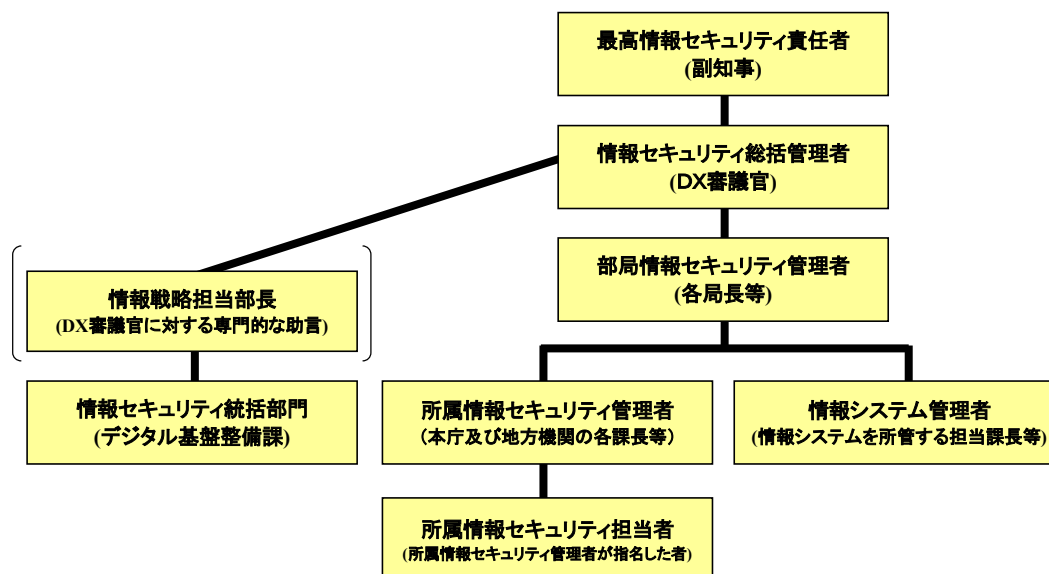


図2 情報セキュリティ管理体制図

- 4 部局情報セキュリティ管理者（以下「部局管理者」という。）
 - (1) 各局長等及び各地方事務所長を部局管理者とする。
 - (2) 所管部局（地方事務所を含む。以下同じ。）における情報セキュリティに関する責任及び権限を有する。
- 5 所属情報セキュリティ管理者（以下「所属管理者」という。）
 - (1) 本庁、地方事務所及びその他の地方機関の各課長等を所属管理者とする。
 - (2) 所属（本庁、地方事務所及びその他の地方機関の各課等をいう。以下同じ。）における情報セキュリティに関する責任及び権限を有する。
 - (3) 所属において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害の恐れがある場合には、統括部門に報告する。
- 6 所属情報セキュリティ担当者（以下「所属担当者」という。）
 - (1) 所属担当者は、所属管理者が当該所属の職員のうちから正担当者1名及び副担当者1名を指名する。
 - (2) 所属担当者は、所属管理者の指示の下、所属における情報セキュリティ活動を行う。
 - (3) 所属において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害の恐れがある場合には、統括部門に報告する。
- 7 情報システム管理者
 - (1) 情報システム管理者は、所管する情報システムの情報セキュリティに関する権限及び責任並びに開発、設定の変更、運用、更新等を行う権限及び責任を有する者

で、各情報システムの担当課長等（地方機関にあっては、地方事務所及びその他の地方機関の各課長等）が当たる。

- (2) 情報システム管理者は、所管する情報システムにおいて、セキュリティポリシーを運用するための具体的な実施手順を作成することとする。

8 兼務の禁止

- (1) 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
- (2) 情報セキュリティ監査の実施において、やむを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

第3 情報資産の管理等

1 情報資産の管理責任

情報資産は、当該情報資産を作成・入手した各部局が管理責任を有し、その重要度に応じて情報セキュリティ対策を行うものとする。特に、個人情報については、漏えい、滅失及びき損の防止等に留意し、適切な管理を行うものとする。

2 情報資産の重要度分類

情報資産については、その重要度を次の分類区分により分類し、その分類に応じて取扱いを制限するなど、適正な管理を行うものとする。

機密性分類区分

分類区分	分類基準
<u>機密性 3 A</u>	<u>秘密文書に相当するもの</u>
<u>機密性 3 B</u>	<u>漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべきもの</u>
<u>機密性 3 C</u>	<u>自治体機密性 3 B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべきもの</u>
機密性 2	直ちに外部への公開を予定していないもの
機密性 1	上記のいずれにも該当しないもの

完全性分類区分

分類区分	分類基準
完全性 2	改ざんや破損により、県民の権利が侵害される、又は行政事務の執行等に重大な支障を及ぼすおそれがあるもの
完全性 1	上記に該当しないもの

可用性分類区分

分類区分	分類基準
可用性 2	滅失、紛失又は当該情報資産が利用不可能であることにより、県民の権利が侵害される、又は行政事務の執行等に重大な支障を及ぼすおそれがあるもの
可用性 1	上記に該当しないもの

3 情報資産の管理方法

情報資産へのアクセスについては、情報資産ごとにその権限を定め、次のとおり取扱うものとする。

(1) 情報の作成

ア 職員は、業務上必要のない情報を作成してはならない。

イ 情報資産を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、作成途上で不要になった場合は、当該情報を消去しなければならない。

(2) 情報資産の利用

ア 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

イ 情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

ウ 情報資産を利用する者は、記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

(3) 情報資産の保管

ア 最終的に確定した情報を記録した記録媒体は、必要に応じて書込禁止措置を行った上で保管するものとする。

イ 記録媒体に納められた情報は、必要に応じ別の記録媒体に複製し保管するものとする。

ウ 機密性 2 以上、完全性 2 又は可用性 2 の情報を記録した記録媒体は、施錠可能な場所に保管し、可能な限り耐火、耐熱、耐水、耐湿の対策及び電磁波対策を講じる。

(4) 情報資産の廃棄

ア 情報を記録した記録媒体を廃棄する場合、所属管理者の許可を得るとともに、記録されている情報の機密性に応じ、記録媒体に含まれる情報を復元できないよう消去した上で、これを行うこととする。

また、当該記録媒体の廃棄においては、日時、処理担当者及び処理内容を記録することとする。

なお、廃棄の作業を委託した場合は、委託先が確実に廃棄したことについて、証明書等文書による確認を行うこととする。

イ クラウドサービスを利用する際は、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理すること。

ウ 情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「文書プロパティ」¹や、文書の作成履歴、PDF ファイルの「しおり」等に残留した不要な情報を除去すること。

また、ソフトウェアを用いて文書の特定部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合は、黒塗りした部分の情報の削除や置換を行うなど、黒塗り部分の復元が行えないよう適切に措置すること。

第4 物理的セキュリティ

1 機器等の管理

情報システム管理者は、機器等の管理において、次の措置を講じる。

(1) サーバ等重要な情報システム関連機器の取付け

ア 外部からの侵入が容易にできない場所に設置する。

イ 火災、水、ほこり、振動等の影響を可能な限り排除し、消火装置及び空調設備を完備した場所に設置する。

ウ 盗難、倒壊防止のため、必要に応じ、容易に取り外せないように、固定等の措置を講じる。

エ 電磁波による情報漏えいを防止するため、必要に応じて適切な措置を講じる。

(2) 電源

ア サーバ等重要な情報システム関連機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を設置する。また、重要かつ高い可用性を要するシステムは、可能な限り非常用電源を設置する。

イ 落雷等による過電流に対してサーバ等の機器を保護するため、サージプロテクト等の措置を施す。

(3) 通信ケーブル等の配線

ア 通信ケーブル及び電源ケーブルの損傷等を防止するために、必要に応じて配線収納管等により保護する。

イ サーバ等重要な情報システム関連機器については、配線の損傷等について、必要に応じて定期的な点検を行う。

ウ ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等、適切に管理する。

(4) パソコン等の機器及び記録媒体等の管理

ア 盗難防止のため、必要に応じて執務室等で利用するパソコンのワイヤーによる固定、モバイル端末（携帯電話、スマートフォンを含む。以下同じ。）及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じる。モバイル端末について

¹ Office データの場合「ファイル」→「情報」から、文書プロパティが参照できます。プロパティを削除する際は「ファイル」→「情報」→「ドキュメント検査」から削除対象を選択して削除をおこなうことが可能です。

は、パスワード等による端末ロックを設定する。記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去する。

イ 情報システムへのログインパスワードの入力を必要とするように設定する。

ウ 取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用する。

エ 必要に応じてパソコンやモバイル端末等におけるデータの暗号化等の機能や端末にセキュリティチップが搭載されている場合はその機能を有効に活用する。同様に、記録媒体についてもデータ暗号化機能を備える媒体を使用する。

オ 執務室等で利用するパソコンや、モバイル端末の庁外での業務利用の際は、アからエまでの対策に加え、遠隔消去機能を利用する等の措置を講じる。

(5) 機器等の保守

ア 可用性 2 のサーバ等重要な情報システム関連機器については、必要に応じて保守対策を講じる

イ 記録媒体を内蔵する機器を外部の事業者修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、外部の事業者修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

(6) 庁舎の敷地外に設置する機器等

庁舎の敷地外に機器等を設置する（機器等の運用を、外部受託者に委託し、その者の敷地に機器等が設置される等）場合は、庁内と同等程度以上の物理的セキュリティ対策を講じる。

(7) 機器の廃棄等

機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべての情報を消去の上、物理的又は論理的方法により、復元不可能な状態にする措置を講じる。

2 入退室管理

情報システム管理者は、サーバ等重要な情報システム関連機器の設置場所への入退室については、次の措置を講じる。

(1) 許可を受けていない者が入室できないように、鍵、カードゲート等の機能により入室者を管理する。

(2) 入退室の記録を管理簿等に残しておく。

(3) 職員等が入室する際には、名札を着用させるとともに、必要に応じて、身分証明書等の提示を求める。

(4) 機器等の搬入の際は、当該機器の安全性とともに、搬入する機器等の既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認をする。

- (5) 外部受託者等による機器等の搬出入時には、所属担当者等が現場に立ち会う。なお、サーバ等重要な情報システム関連機器の設置場所以外においても、情報資産の重要度に応じ、部外者等の入室を制限するなどの対策を講じる。
- (6) 機密性 2 以上の情報資産を扱うシステムを設置している管理区域には、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を原則として持ち込ませないようにする。

3 通信回線及び通信回線装置の管理

情報システム管理者は、通信回線、通信回線装置の管理においては、次の措置を講じる。

- (1) 庁内の通信回線及び通信回線装置を、適切に管理し、また、通信回線及び通信回線装置に関連する文書を適切に保管する。
- (2) 外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らす。
- (3) 通信回線を接続する場合、機密性及び可用性を踏まえ必要なセキュリティ水準を検討の上、適切な回線を選択する。また、必要に応じて次の措置を行う。
 - ア 送受信される情報の暗号化を行う。
 - イ 伝送途上の情報が破壊、盗聴、改ざん、消去等が生じないように対策を実施する。
 - ウ 可用性 2 の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

第 5 人的セキュリティ

1 職員の責務

- (1) 職員は、法令、セキュリティポリシー及び実施手順に定められている事項を遵守しなければならない。また、セキュリティポリシーに対する違反行為を発見した場合、直ちに所属管理者に報告を行わなければならない。なお、職員は、情報セキュリティ対策について不明な点、遵守が困難な点等については、所属管理者に相談し、指示を受けなければならない。
- (2) 職員は、情報資産を適正に利用・管理し、盗難、紛失、電子メールの誤送信による意図しない情報流出等を未然に防止するとともに、業務以外の目的での情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスなど業務遂行の妨げとなる情報資産の私的利用等を行ってはならない。

なお、情報システム管理者は、職員による業務に関係がないと思われる情報資産の利用を発見した場合は、所属管理者に通知を行うものとする。

- (3) パソコン等の機器、記録媒体等の情報資産（記憶装置を有しないパソコン等を除く。）については、持ち出し及び持込みを原則禁止とし、持ち出し及び持込みを行う場合は、所属管理者又は情報システム管理者の許可を得なければならない。

なお、所属管理者又は情報システム管理者は、パソコン等の機器、記録媒体等の情報資産の持ち出し及び持込みについて、記録を作成し、保管しなければならない。

- (4) 職員は、業務を処理するにあたり、私物のパソコン及び記録媒体を利用してはならない。
- (5) 職員は、業務上付与された情報システム（クラウドサービスを含む。）のアカウント等を私的利用しているアカウント等と紐付けてはならない。
- (6) 職員は、パソコン等の機器のソフトウェアに関するセキュリティ機能の設定を情報システム管理者の許可なく変更してはならない。
- (7) 職員は、パソコン等の機器や記録媒体等について、使用権限のない者に使用されること、又は許可なく情報を閲覧されることがないように、離席時の端末のロックや記録媒体等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。
- (8) 情報システム管理者は、機密性 2 以上、可用性 2、完全性 2 の情報資産を外部で処理する場合の安全管理措置を定めなければならない。また、職員は情報システム管理者が定めた安全管理措置を遵守しなければならない。
- (9) 退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

2 教育・訓練

- (1) 総括管理者は、情報セキュリティ対策を総合的に推進するため、職員に対して、情報セキュリティの教育・訓練を計画的かつ継続的に実施するとともに、職員が情報セキュリティに関する知識を習得できるようにするため、研修、教材等を準備する。

また、新規採用の職員を対象とする情報セキュリティに関する研修を実施する。

- (2) 総括管理者は、緊急時を想定した訓練を定期的の実施する。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。
- (3) 情報システム管理者は、当該情報システムの利用者に対して、情報システム利用にかかわる教育を実施する。
- (4) 職員は、情報セキュリティ研修を受けるとともに、自ら意欲的に習得し、業務の中で実践する。

3 ID、ICカード等の管理

I D、I Cカード等を管理する職員は、次に掲げる事項を遵守しなければならない。

(1) I Dの管理

ア 自分に付与又は貸与されたものではないI Dを利用しないこと。

イ 共用I Dを利用する場合は、共用I Dの利用者以外に利用させないこと。

(2) I Cカード等の管理

ア I Cカード等認証に用いるカード類は、職員等間で共有しないこと。

イ I Cカード等は、カードリーダ等に常時挿入したままにしないこと。

ウ I Cカード等は、紛失、盗難及び不正使用等の事故のないように、厳重に保管及び管理すること。

エ I Cカード等を紛失した場合には、速やかに当該情報システム管理者に通報し、指示を受けること。

オ 情報システム管理者は、紛失の通報があった場合は、速やかに当該I Cカード等を使用したアクセス等を停止すること。

カ 情報システム管理者は、I Cカードを廃棄する場合、破砕するなど復元不可能な処理を行わなければならない。

4 パスワードの管理

情報システムを利用する職員は、割り当てられたユーザI Dのパスワードの管理について、次に掲げる事項を遵守しなければならない。

(1) パスワードは決して他人に漏らさないこと。

(2) パスワードのメモを作成し、机上、ディスプレイ周辺等にメモを置かないこと。作成した場合、特定の場所に施錠して保存する等により他人が容易に見ることができないような措置を講じること。

(3) パスワードが流出した恐れがある場合には、所属管理者及び当該情報システム管理者に速やかに報告するとともに、パスワードを変更すること。

(4) 複数の情報システムを利用する職員は、同一のパスワードをシステム間で使用してはならない。

(5) 共用I Dを利用する場合、パスワードは定期的に変更すること。特に人事異動の際等、共用I Dの利用者が変更になった場合は必ず変更すること。

(6) パスワードを変更する場合、以前に使用したパスワードを再利用しないこと。

(7) 割り当てられたユーザI Dに係る初期値パスワードは、速やかに変更すること。

(8) サーバ、ネットワーク機器及びパソコン等の設定を変更することによって、パスワードの入力なしに認証を可能とする等、認証を回避する設定を行わないこと。

(9) 共用I Dを利用する場合を除き、職員等間でパスワードを共有しないこと。

(10) パスワードの長さは原則として、英大文字小文字の両方を用いた、数字や記号を織り交ぜた8桁以上の容易に推測できないものを選択すること。

5 電子メールの適正利用

電子メールを利用する職員は、次に掲げる事項を遵守しなければならない。

- (1) 業務上必要のない送信先に電子メールを送信しないこと。
- (2) 外部の複数人に電子メールを送信する際は、必要がある場合を除き、B c c で送信するなど他の送信先の電子メールアドレスが分からないようにすること。
- (3) 重要な電子メールを誤送信した場合、所属管理者に報告すること。

6 電子署名・暗号化

職員は、外部に送るデータの機密性又は完全性を確保することが必要な場合には、電子署名、暗号化又はパスワードの設定を行わなければならない。

7 インターネットサービスの利用制限

職員は、インターネットサービスのうち、責任ある管理者の所在が不明確なクラウドサービス（ウェブメールやネットワークストレージサービス等）を使用してはならない。

8 外部委託に関する管理

外部受託者との委託契約について権限を有する者は、当該委託契約の締結に関し、次の事項を遵守しなければならない。

- (1) 外部受託者の選定に係る相手方の情報セキュリティ実施状況、経営の信頼度、情報セキュリティ意識等の確認
- (2) 外部受託者との間で必要に応じて次の情報セキュリティ要件を明記した契約の締結

ア セキュリティポリシー及び実施手順のうち外部受託者が守るべき内容の遵守

イ 外部受託者の責任者、委託内容、作業者、作業場所の特定

ウ 提供されるサービスレベルの保証

エ 外部受託者にアクセスを許可する情報の種類と範囲、アクセス方法

オ 従業員に対する教育の実施

カ 県が提供した情報の目的外利用及び外部受託者以外の者への提供の禁止

キ 業務上知り得た情報の守秘義務

ク 再委託に関する制限事項の遵守

ケ 委託業務終了時の情報資産の返還、廃棄等

コ 委託業務の定期報告及び緊急時報告義務

サ 県による監査、検査

シ 情報セキュリティインシデント発生時の県による公表

ス 情報セキュリティ対策の履行が不十分な場合の規定

- (3) システム開発を委託する場合のソースコードの提出、システム導入前の検査要求事項等の契約への明記

- (4) 契約期間が3か月以上の場合、契約相手方に係る契約終了までの情報セキュリティ実施状況等を契約相手方から定期的に報告を受けること

9 無許可ソフトウェアの導入禁止

- (1) 職員は、情報システム管理者の許可なく、新規にソフトウェアを導入してはならない。ただし、業務上必要がある場合は、情報システム管理者（複数の情報システムに関係する場合は、関係するすべての情報システム管理者）の許可を得て導入することができる。
- (2) 職員は、不正にコピーしたソフトウェアを利用してはならない。

10 機器及びネットワーク構成の管理

- (1) 職員は、情報システム管理者の許可なくパソコン等の機器の構成を増設又は交換してはならない。また、機器を増設して他の環境へのネットワーク接続を行い、外部からのアクセスを可能とする仕組みを構築してはならない。
ただし、業務上必要がある場合は、情報システム管理者（複数の情報システムに関係する場合は、関係するすべての情報システム管理者）の許可を得て増設等することができる。
- (2) 職員は、情報システム管理者の許可なく、パソコン等の機器を情報システム管理者が認めていないネットワークに接続してはならない。

第6 技術的セキュリティ

1 コンピュータ及びネットワークの管理

(1) ログの取得

情報システム管理者は、当該情報システムのログについて次のとおり実施する。

ア 当該情報システムのログ及びセキュリティ関連事案に関する記録を取得し、一定期間保存する。

イ ログが漏えい、改ざん、消去されないように必要な措置をとる。

ウ 必要に応じて、取得したログを定期的に点検又は分析する機能を設け、悪意のある第三者等からの不正侵入、不正操作等の有無について点検又は分析を行う。

(2) 障害記録

情報システム管理者は、情報システムの障害等に対する処理を行った場合は、障害記録として記録し、常に活用できるよう保存する。

(3) 情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図及び情報システム仕様書を業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理する。

(4) バックアップの実施

ア 情報システム管理者は、サーバ等に記録された情報について、サーバの冗長化対策にかかわらず、必要に応じて定期的にバックアップをとることとする。

イ 情報システム管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

ウ バックアップの適切な世代管理を実施すること。また、保存場所については、論理的に切り離されたネットワークに保存すること。もしくは、物理的な媒体に保管すること。²

エ 情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

(5) 電子メール

ア 情報システム管理者は、メールの不正中継を防止するため、情報システムに必要な設定をする。

イ 情報システム管理者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止する等、必要な措置を講じる。

ウ 情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可とするとともに、電子メールの送受信上限容量及び上限を超えた場合の対応を職員に周知する。

(6) 外部の者が利用できるシステムの分離等

情報システム管理者は、外部の者が利用できるシステムについては、必要に応じ他のネットワーク及び情報システムと物理的又は論理的に分離する等の措置を講じなければならない。

(7) 無線 LAN の利用制限

情報システム管理者は、無線 LAN を利用する場合、解読が困難な暗号化及び認証技術を使用すること。

(8) 複合機のセキュリティ管理

ア 所属管理者は、運用中の複合機に対するセキュリティ対策を講じる。

イ 所属管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じる。

(9) 特定用途機器

情報システム管理者は、特定用途機器（テレビ会議システム、IP電話システム、ネットワークカメラシステム等をいう。）について、取り扱う情報、利用方法、通信回線への接続形態等により何らかの脅威が想定される場合は、当該機器の特性に応じた対策を所属管理者に実施させる。

2 アクセス制御

情報システム管理者は、当該情報システムへのアクセス制御について次の事項を遵守しなければならない。

² バックアップを保存する電磁的記録媒体等の種類、バックアップの周期、世代管理の方法、バックアップデータを保存した記録媒体を端末及びサーバ装置やネットワークから切り離して保管すること等を考慮して対策を講じること。

(1) アクセス制御

情報システム管理者が所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないよう、必要最小限の範囲で適切に設定をすること。

(2) 利用者権限の管理

ア 利用者権限が付与された I D については、利用者の登録、変更及び抹消等の情報管理、並びに、職員等の異動等における取扱い等の方法を定めること。

イ 利用されていない I D が放置されないよう、点検を行うこと。

ウ 主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

(3) 管理者権限の管理

情報システムの管理者権限が付与された I D については、必要最小限の者に与え、当該 I D 及びパスワードを厳重に管理すること。また、当該 I D を初期設定以外のものとする。

(4) ネットワークのアクセス制御

ア ファイアウォール等の設置により、外部からの内部ネットワーク又は内部から外部ネットワークへのアクセスを適切に制御すること。

イ 不要なネットワークサービスを使用不可にすること。

ウ 外部から内部ネットワークにアクセスを認める場合、セキュリティ確保のために必要な措置を講じること。

(5) 庁外ネットワークからのアクセス制御

ア 職員が庁外ネットワークから県の保有するネットワーク又は情報システムにアクセスする場合は、当該情報システム管理者の許可を得ること。

イ 庁外ネットワークからのアクセスに関する許可は、必要最小限の者に限定すること。

ウ 庁外ネットワークからのアクセスにおいては、システム上、利用者の本人確認を行う機能を確保すること。

エ 庁外ネットワークからのアクセスにおいては、通信途上の盗聴を防御するために暗号化等の措置を講じること。

(6) 庁外ネットワークとの接続

ア 他の自治体又は民間企業等のネットワークとの接続は、業務上必要がある場合のみに限定すること。

イ 他の自治体又は民間企業等のネットワークと接続する場合は、当該ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を確認し、県の保有するネットワークや情報システム等の情報資産に影響が生じないことを確認すること。

ウ ウェブサーバ等をインターネットに公開する場合は、次のセキュリティ対策を実施しなければならない。

(ア) 所管するネットワークへの侵入を防御するために、所管するネットワークと外部ネットワークとの境界にファイアウォールを設置すること。

(イ) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じること。

(ウ) 情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定すること。

(エ) 必要に応じて、不正アクセスによるウェブページの改ざんを防止するため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。

エ 接続した外部ネットワークのセキュリティに問題が認められ、所管する情報資産に脅威を及ぼす可能性が生じた場合は、速やかに当該外部ネットワークから物理的に切断すること。

オ 公衆通信回線（公衆無線 LAN）等の庁外通信回線を通じて庁内ネットワークに接続を認める場合は、多要素認証方式を利用すること。³ また、通信内容の暗号化やログ取得の実施など、セキュリティ確保のために必要な措置を講じること。

カ クラウドサービス等庁外のネットワーク上に構築された情報システムとの接続を行う場合、暗号化を実施した上で、原則として専用回線を利用すること。

キ 専用回線が利用できない際には、通信事業者が提供する閉域網を利用した VPN（IP-VPN）を利用し閉域接続を行うこと。

ク 専用回線等により庁内ネットワークと閉域接続をした庁外ネットワークは、その領域を閉域接続系として扱い、他のネットワークと物理的・論理的に分離を行うこと。

ケ 総括管理者が認めた場合に限り、パブリック認証局が発行したサーバ証明書を使用した HTTPS 通信については、専用回線等を用いた閉域接続を必須としない。

コ インターネット VPN は閉域接続として採用しないこと。

(7) 自動識別の設定

ネットワークで使用される機器については、可能な限り機器固有情報によって、アクセスの可否を自動的に決定するシステムを導入すること。

(8) ログイン制御

ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等、正当なアクセス権を持つ職員がログインしたことを確認することができるよう、必要に応じてシステムを設定すること。また、複数回連続でパスワード認証に失敗した場合、強制的にアカウントをロック（使用不可）する仕組みを設けること。

³ ID、パスワードのような知識認証だけでなく、所持認証（セキュリティカード等）、生体認証（顔、指紋等）の2つ以上を組み合わせた認証方法のこと。

(9) パスワードの管理方法

ア 職員のパスワードに関する情報は、アクセス制御等により厳重に管理すること。

イ 職員のパスワードを発行する場合は、仮のパスワードを発行し、職員に、直ちに
変更させるなど、必要に応じて適切な措置を講じること。

ウ パスワードが第三者に読まれることのないよう、パスワードの暗号化等の措置を
とること。

3 外部サービスの利用

(1) 情報システム管理者は、民間企業等が提供する情報システムサービスをネットワー
クを通じて利用する場合、利用するサービスのシステム構成及びセキュリティ対
策等を確認し、所管する情報資産に影響を及ぼす可能性が無いこと及び提供される
サービスの可用性について、調査し、利用にあたってのリスクが許容できることを
確認した上でサービスを利用すること。

(2) 所属管理者は、クラウドサービス（民間事業者が提供するものに限らず、本県が
自ら提供するもの等を含む。以下同じ。）を利用しようとする場合は、次の事項に
ついて、検討・検証を実施し、情報戦略担当部長に利用の申請をしなければならない。
い。

ア 取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取り扱いを
委ねることの可否

イ 取り扱う情報の可用性区分に応じて、次の事項を検討すること。

(イ) クラウドサービスの中断や終了時に円滑に業務を移行するための対策及び委託
先の選定

(イ) クラウドサービスの中断時の復旧要件

(ウ) クラウドサービスの終了又は変更の際の事前告知の方法、期限及びデータ移行
方法

ウ 取り扱う情報の機密性区分に応じて、次の事項を確認すること。

(ア) 機密性 2 または 3 C の情報を取り扱う場合、ISMS（ISO/IEC 27001）を取得し
ていることに加え、次のいずれかを満たしていること。

a ISMAP クラウドサービスリストに登録されていること。

b ISMAP-LIU クラウドサービスリストに登録されていること。

c クラウドサービスにおける第三者認証として ISO/IEC 27017 を取得している
こと。

(イ) 機密性 3 B の情報を取り扱う場合、ISMS（ISO/IEC 27001）を取得しているこ
とに加え、次のいずれかを満たしていること。

a ISMAP クラウドサービスリストに登録されていること。

b クラウドサービスにおける第三者認証として ISO/IEC 27017 及び ISO/IEC
27018 を取得していること。

- c クラウドサービスにおける第三者認証として ISO/IEC 27017 及び ISO/IEC 27701 を取得していること。
- ウ 機密性 3 A の情報はクラウドサービスで取り扱わないこと。
- エ 国の行政機関がクラウドサービス提供者となるシステムの利用においては、
(ア)～(ウ)の定めにかかわらず、情報戦略担当部長が別に指示する事項を確認する
こと。
- エ クラウドサービスに保存する情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されるリスクが懸念されるため、原則としてクラウドサービスの情報保存先は国内データセンターを採用すること。
- オ 不正アクセスを防止するためのアクセス制御を実施すること。
- カ クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、クラウドサービスにアクセスする際は、多要素認証を用いて認証させること。
- キ クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）において定めること。
- ク クラウドサービスに保存される情報の利用終了後の取り扱いを定めること。
- ケ クラウドサービスの利用終了後等に、クラウドサービスで取り扱った情報を消去する場合には、暗号鍵を削除するなどの簡易かつ確実な対応により、保存した情報を復元困難とする管理を行うこと。
- コ クラウドサービスで機密性 3 C 以上の情報を扱う場合は、機密性保護のため暗号化すること。また、利用終了後には情報を消去すること。
- サ 庁内システムと外部のアプリケーションを連携する場合や、複数のクラウドサービスを連携して用いる場合、API 連携で使用するユーザアプリケーションやデバイスの範囲は最小限に限定し、API 接続時の認証やログ管理など、不正な API 操作を防止するため、WAAP 技術による保護やアクセス制御を実施すること。⁴
- シ クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し得る情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等の確認
- 情報戦略担当部長は、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形で、上記ア～シの事項について検討し、利用の可否を判断しなければならない。
- (3) 情報システム管理者は、ソーシャルメディアサービスを利用する場合、次の事項を遵守すること。
- ア ソーシャルメディアサービスの提供事業者が「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合は、これを利用すること。

⁴ アプリケーション間でのデータ引き渡しのため、API（Application Programming Interface）連携の利用増加が想定される。WAAP（Web Application and API Protection）による API と Web アプリケーションの包括的な保護や、API 接続時のトークン認証によるアクセス制御などについて検討すること。

- イ パスワード等、認証情報を適切に管理すること。
- ウ 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。
- エ 機密性 2 以上の情報はソーシャルメディアで発信しないこと。
- オ 利用するソーシャルメディアサービスごとに責任者を定めなければならない。
- カ アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

4 システム開発、導入、保守等

情報システム管理者は、当該システムの開発、導入及び保守に際して、次の事項を遵守しなければならない。

(1) 機器等及び情報システムの調達

ア 情報システムの調達に当たっては、一般に公開する調達仕様書が情報セキュリティ確保の上で問題が生じないようにすること。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載すること。

イ 情報システムの開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記すること。

ウ 機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上、問題が無いことを確認すること。

エ ネットワーク及び情報システムの開発、導入、保守等を外部受託者から調達する場合、情報セキュリティに関して外部受託者が遵守すべき事項等を説明すること。

(2) 情報システムの開発、保守

ア 責任者及び監督者を定め、作業への立会い又は現場との連絡調整、作業の終了確認などを行わせること。

イ 作業者及び作業範囲を明確にすること。

ウ システム運用環境を利用して、システム開発・保守を行う場合は、システム運用に問題を生じさせないこと。

エ 開発、保守に際しては、ソースコードの提出を求めるとともに、提出されたソースコードは適切な方法で保管すること。

オ 開発、保守に際しては、セキュリティ上問題となるおそれのあるソフトウェアを使用しないこと。

カ 開発、保守記録の提出を義務付けること。

キ 開発、保守に関連する資料等は、適切な方法で保管すること。

ク 開発、保守作業において作業者等が使用する ID は、必要最少限に限定し、当該作業終了後、不要となった時点で速やかに抹消すること。

また、作業者等が使用する ID のアクセス権限は適正に設定すること。

(3) 情報システムの導入

- ア 重要な情報システムについては、必要に応じて、テスト環境とシステム運用環境の分離を行うこと。
- イ 重要な情報システムについては、必要に応じて、テスト環境からシステム運用環境への移行について、システム開発・保守等計画の作成時に手順を明確にすること。
- ウ 移行の際、情報システムに記録されている情報資産の保存を確実に行之、移行に伴う情報システムの停止等の影響が最小限になるよう配慮すること。
- エ 導入するシステムやサービスの可用性が確保されていることを確認した上で導入すること。
- オ 新しいシステムを導入する際には、原則として既に稼動しているシステムに接続する前に、十分な試験を行うこと。
- カ 重要な情報システムについては、必要に応じて、あらかじめ擬似環境による操作確認を行うこと。
- キ 試験時の使用データには、原則として運用データ（特に個人情報）は使用しないこと。
- ク 試験に使用したデータ及びその結果は厳重に管理すること。
- ケ 脆弱性が存在する可能性が増大することを防止するため、サーバ等が備える機能のうち、必要な機能のみを利用すること。
- コ ウェブアプリケーション・コンテンツを開発する際は、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。⁵
- サ ウェブサイトを新たに構築する際は「pref.hiroshima.lg.jp」等「lg.jp」のサブドメイン、もしくはサブディレクトリの使用について仕様書に含めること。
「pref.hiroshima.lg.jp」ドメインの使用が困難なサービスを利用する場合は、本県が提供するサービスであることを、閲覧者が容易に確認できるようにすること。
- シ インターネットに公開するウェブサイトにおいては、情報の盗聴及び改ざん防止のため、すべての情報に対する暗号化及び電子証明書による認証の対策（常時SSL）を講じること。
- ス 利用を終えた「lg.jp」以外のドメイン名を廃止する際は、すぐに廃止するのではなく、悪意のある第三者に不正利用されないよう、廃止ドメインを一定期間保持（数年間）すること。⁶

(4) 情報システムの変更管理

⁵ 適正なセキュリティを考慮したウェブサイト等を構築するための注意点については、「安全なウェブサイトの作り方」（情報処理推進機構）を参照すること。

⁶ 廃止ドメインへのアクセスがあった際に、移転先サイト（移転先サイトが存在しない場合はサービス終了を告知したページ等）へHTTP 応答コード 301 を用いた転送を行うなど、誤誘導への防止策を講じること。

- ア 情報システム管理者は、当該情報システムに対して変更を実施する場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。
 - イ システムを追加、変更等した場合は、その際の設定、構成等の履歴を記録し、保存すること。
 - ウ 当該情報システムに対して実施した作業履歴を記録し、適切に管理すること。
- (5) ソフトウェアの保守及び更新
- ア ソフトウェアについて、管理簿等を作成し、定期的にインストール状況及び保管状況を確認すること。
 - イ ソフトウェア（独自開発ソフトウェア及び汎用ソフトウェア）を更新し、又は修正プログラムを導入する場合は、不具合等について確認を行った上で、導入すること。
 - ウ 導入したソフトウェアのライセンスを管理すること。
- (6) リモートアクセスによる保守等
- 情報システム管理者は、庁外のネットワークから県の保有するシステムの保守又は診断のためのリモートアクセスを行う場合は、次の対策を講じるものとする。
- ア リモートアクセス端末の識別コード等によるアクセス制御
 - イ 公衆通信回線（公衆無線LAN）等を通じて、県の保有するシステム又はネットワークに接続を行う場合は、多要素認証を採用すること。また、ログ取得の実施や通信内容の暗号化などセキュリティ確保のために必要な措置を講じること。
 - ウ 情報システムの保守においては、保守担当者が作業中に権限外の情報にアクセスできないよう、アクセス制御や権限管理を考慮すること。
- ただし、全庁的なネットワーク（行政LAN・WAN等）の基盤上で稼働するシステムについては、外部のネットワークからのリモートアクセスによる保守、診断を行ってはならない。
- 5 コンピュータウイルス等不正プログラム対策
- (1) 総括管理者の遵守事項
- ア コンピュータウイルス等不正プログラム（以下「ウイルス」という。）の情報について職員に対する注意喚起を行うこと。
 - イ ウイルス関連情報の収集に努め、最新のウイルス検査ソフトウェア及びそのパターンファイルを配布すること。
- (2) 情報システム管理者の遵守事項
- ア ウイルスの感染の予防、発見、駆除、復旧等のウイルス対策を行うため、ウイルス検査ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施すること。また、内部に侵入したウイルスを早期検知して対処するために、通信をチェックする等の内部対策を講じること。

- イ インターネットを通じて受信したファイルは、インターネットのゲートウェイにおいてウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止すること。
- ウ 庄外ネットワークに送信するファイルは、インターネットのゲートウェイにおいてウイルス等不正プログラムのチェックを行い、不正プログラムの組織外への拡散を防止すること。
- エ 業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用しないこと。
- オ 重要なシステムの設定に係るファイル等について、必要に応じて改ざんの有無をチェックすること。

(3) 職員の遵守事項

- ア 外部から取得したファイル又はソフトウェアは、ウイルス検査後に使用すること。
- イ 出所不明のファイル又はソフトウェアは使用しないこと。
- ウ プログラム及びファイル媒体等を他者に提供する際には、事前にウイルス検査を実施すること。
- エ 利用する機器に対して最新のウイルス検査ソフトウェアを利用して定期的にウイルス検査を実施すること。
- オ 差出人が不明又は不自然なメールを受信した場合は、速やかに削除すること。
- カ ウイルスに感染した場合又は疑われる場合は、次の対応をとること。
 - パソコン等の端末の場合、速やかにLANケーブルの取り外し、無線LAN及びSIMによる通信機能を停止させる等、すべての通信を停止させる措置をとること。
- キ ウイルスの感染を発見した場合は、直ちに所属担当者に報告すること。

6 セキュリティ情報の収集

情報システム管理者は、セキュリティに関する情報について、次のとおり収集し、必要に応じて対処すること。

- (1) 情報収集先（外部受託者、IRTサイト、ベンダーのサイト等）を定める。
- (2) 使用しているソフトウェアのバージョン情報を管理し、得られた情報との確認ができるようにする。
- (3) セキュリティに重大な影響を及ぼす不具合が公開された場合は、緊急度に応じてパッチの適用や回避策等の対応を速やかに行う。
- (4) 緊急の場合には、総括管理者の判断により全庁内に連絡を行う。
- (5) 収集した情報のうち、職員にとって必要な事項は、これを周知する。

7 専門家の支援体制

総括管理者は、実施している不正プログラム対策等のセキュリティ対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

第7 運用

1 情報システムの監視

情報システム管理者は、次に掲げる事項を実施することにより、当該情報システムに対するセキュリティに関する事案の検知に努めるものとする。

- (1) セキュリティ侵害を検出するための監視項目の設定及び当該監視項目に基づく情報システムの監視
- (2) 外部と接続する情報システムへの侵入検知装置(Intrusion Detection System)等の設置による監視
- (3) 監視により得られた結果に対する消去、改ざん等の防止に必要な措置の実施
- (4) 監視結果の正確性を確保するための各機器間での時刻同期の実施
- (5) 取得したログの内容を定期的に確認することによる、不正アクセスの検知

2 運用管理における留意点

- (1) 総括管理者又は部局管理者は、セキュリティ上問題があると認められる場合は、CISO の許可を得てメール等個人のプライバシーに係る情報を閲覧することができる。ただし、他の法令等で定められた個人情報保護に関する情報の閲覧に関しては、他の法令等に定められた手続に従う。

なお、閲覧の許可を受けた場合であっても、CISO 又はその指名する者の立会がない場合は閲覧することができない。

- (2) 総括管理者、部局管理者、所属管理者及び情報システム管理者は、職員等が常にセキュリティポリシー及び実施手順を参照できるよう配慮するものとする。

3 侵害時の対応

情報システム管理者は、当該情報システムにおける緊急時対応計画を作成し、セキュリティ侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じる。

(1) 連絡経路

セキュリティ侵害時の庁内連絡経路は、図3のとおりとする。

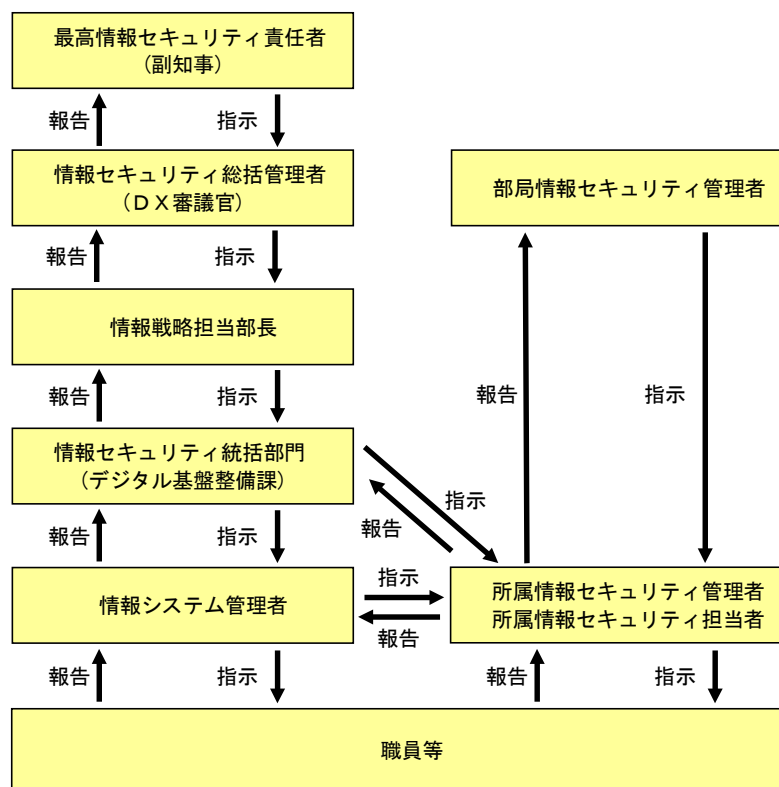


図3 連絡経路

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定める。

- ア 庁内外関係者の連絡先
- イ 発生した事案に係る報告すべき事項
- ウ 発生した事案への対応措置
- エ 再発防止措置の策定

(3) 緊急時対応計画の見直し

情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じて、必要に応じて緊急時対応計画の規定を見直さなければならない。

(4) 事案の報告

- ア 職員は、セキュリティ事故、情報システム上の欠陥及び誤作動を発見、若しくは県民等から報告を受けた場合には、速やかに連絡経路に従って報告し、指示を受けなければならない。
- イ 職員は、情報セキュリティに関する事案を報告する際、次の事項を調査の上、報告しなければならない。

(ア) 事案の内容

(イ) 事案が発生した原因として想定される行為

(ウ) 確認した被害・影響範囲

ウ 総括管理者は、重要な事案の詳細な調査を行い、CISO へ報告するものとする。

(5) 事案への対処

ア 総括管理者は、次に掲げる場合は、必要に応じて国及び関係機関へ連絡するものとする。

(ア) サイバーテロその他国民に重大な被害が生じるおそれがあるとき。

(イ) 不正アクセスその他犯罪と思慮されるとき。

(ウ) 部外者が県の保有する情報資産を経由し、他の第三者に被害を与えるおそれがあるとき。

(エ) 個人情報・特定個人情報の漏えい等が発生したとき。

イ 情報システム管理者は、次に掲げる場合においては、直ちに当該情報システムのネットワークの切断及びシステムの停止を行うことができる。

なお、切断及び停止により他のシステムの運用に影響を及ぼす場合は、当該情報システム管理者へその旨を直ちに連絡することとする。

(ア) 不正アクセスが継続しているとき。

(イ) D o S 攻撃等のシステムの運用に著しい支障を来たす攻撃が継続しているとき。

(ウ) ウイルスがネットワーク経由で拡がっているとき。

(エ) ウイルスが情報資産に深刻な被害を及ぼしているとき。

(オ) 災害等により電源を供給することが危険又は困難なとき。

(カ) その他情報資産に係る重大な被害が発生しているとき。

ウ 情報システム管理者は、セキュリティ侵害によりネットワークを切断又はシステムを停止した場合は、迅速に原因究明を行い、被害拡大（再発）防止の暫定措置を講じた後、復旧するものとする。

エ 情報システム管理者は、情報セキュリティ事案が発生した場合、統括部門に報告する。また、重要な情報セキュリティ事案については、部局管理者、総括管理者及びCISOに報告する。

(6) 再発防止の措置

ア 情報システム管理者は、セキュリティ侵害が発生したときは当該事案の分析を行い、再発防止に係る対応策を策定し、総括管理者に協議しなければならない。

イ 総括管理者は、前記アの対応策が適当であると認めた場合は、これを承認するものとする。

ウ 情報システム管理者は、当該対応策に従い、必要な措置を講じなければならない。

4 情報システムの運用継続

非常時にも情報システムの運用を継続させる必要があるシステムを所管する情報システム管理者は、当該情報システムの運用継続のための措置を講じるものとする。

5 セキュリティポリシー等遵守状況の確認等

総括管理者及び情報システム管理者は、セキュリティポリシー及び実施手順の遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処するものとする。

第8 例外措置

1 例外措置の許可

所属管理者及び情報システム管理者は、基本方針及び対策基準を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、総括管理者の許可を得て、例外措置を取ることができる。

2 緊急時の例外措置

所属管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに総括管理者に報告しなければならない。

3 例外措置の申請書の管理

総括管理者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

第9 法令遵守

職員は、職務の遂行において情報資産を使用する場合は、次の法令等を遵守しなければならない。

- 1 地方公務員法（昭和25年法律第261号）
- 2 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
- 3 著作権法（昭和45年法律第48号）
- 4 個人情報の保護に関する法律（平成15年法律第57号）
- 5 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）
- 6 サイバーセキュリティ基本法（平成28年法律第31号）

第10 情報セキュリティに関する違反への対応

- 1 情報セキュリティの保持に関して、地方公務員法第29条に規定する懲戒事由に該当すると認められる行為を行った職員については、その内容、程度に応じて、懲戒処分等の人事管理上必要な措置を講じる。

- 2 情報システム管理者は、職員等の情報セキュリティポリシーに違反する行動を確認した場合には、当該職員等が属する所属の所属管理者に通知し、適切な措置を求めるものとする。
- 3 前項の規定による通知等にも かかわらず、改善が認められないと情報システム管理者が判断した場合、情報システム管理者は、該当する職員のネットワークまたは情報システムを使用する権利を停止または剥奪することができる。

第 1 1 評価及び見直し

1 監査

- (1) 情報システム管理者は、法令並びにセキュリティポリシー及びこれに関連する規程・規準等の遵守状況及び運用実態について、定期的又は必要に応じて監査を受けるものとする。
- (2) 総括管理者は、特に必要と認められる情報システムに対して、監査を行うものとする。
- (3) 情報システム管理者は、監査結果を基に改善措置をとる。
- (4) 監査を実施する場合は、被監査部門から独立し、監査及び情報セキュリティに関する専門知識を有する者に対して、監査の実施を依頼する。
- (5) 外部受託者に委託している場合、セキュリティ対策の履行状況について監査を定期的に又は必要に応じて行わなければならない。
- (6) 情報システム管理者は、監査結果及び改善措置を総括管理者に報告する。

2 自己点検

- (1) 情報システム管理者は、所管する情報システムについて、定期的に又は必要に応じて自己点検を実施する。
- (2) 総括管理者は、情報システム管理者が行う自己点検に対して、支援を行う。
- (3) 情報システム管理者は、点検結果を基に改善措置をとる。
- (4) 情報システム管理者は、点検結果及び改善措置を総括管理者に報告する。

3 セキュリティポリシーの見直し

CISO は、新たな対策を講じる必要が発生した場合又は監査及び自己点検の結果等を基にセキュリティポリシーを改正する必要がある場合は、セキュリティポリシーの実効性を確保するため、必要な見直しを行う。

第 1 2 個人番号利用事務システムにおける特則

当分の間、個人番号利用事務システム（行政手続における特定の個人を識別するための番号の利用等に関する法律第 9 条において個人番号を利用することができると規定されている事務を取り扱うシステムをいう）においては、次の措置をとらなくてはならない。

- 1 個人番号利用事務システム専用のネットワークセグメントとする。
- 2 個人番号利用事務システムのネットワーク以外との通信は、アクセスしても安全と認められる特定通信限定とする。特定通信に限定する際は、通信経路の限定（MAC アドレス、IP アドレスに加えて、アプリケーションプロトコル（ポート番号）のレベルでの限定も行う。特定通信先のサーバや端末はインターネットとの通信ができないことを確認する。）を行う。
- 3 ID、パスワードの他に認証方法を導入し二要素認証とする。
- 4 ログを記録、及び一定期間保存し、定期的に又は随時に分析を行い、不正アクセス等の有無を確認する。
- 5 USBメモリ等の外部記憶媒体による端末からの情報持出しができないように設定する。やむを得ず情報持出しの必要が生じた場合は、管理者権限を持つ職員によってその都度、持出し不可設定を解除する、又は管理者権限を持つ職員のみ持出しができる設定とする。
- 6 情報システムの不正な構成変更（許可されていない電子媒体、機器の接続、ソフトウェアのインストール等）を防止するために必要な設定を行う。
- 7 個人番号利用事務系においては、無線 LAN は利用しないこと。
- 8 クラウドサービス上で個人番号利用事務系の標準準拠システム等を利用する場合は、そのクラウドサービスの領域を閉域として扱い、他のネットワークと物理的及び論理的に分離を行うこと。閉域間の接続は暗号化を実施したうえで、専用回線を用いて接続すること。
- 9 クラウドサービスの管理コンソールに対して、例外的にインターネット経由でアクセスする場合は、多要素認証によるアクセスとログ取得を行うこと。また、許可された端末からのアクセスに限定する必要があるため、端末認証（MAC アドレス、シリアル番号及び電子証明書等）又は接続する機器や拠点の IP アドレス等の認証情報を利用し端末を制限すること。

第 13 LGWANに接続するシステムにおける特則

LGWANに接続する情報システムにおいては、次の措置を取らなくてはならない。

- 1 行政 LAN・WANとのネットワーク分離を行う。
- 2 行政 LAN・WANに接続された情報システムとの通信は、必要な通信のみ許可する設定を行う。

平成 14 年 7 月 23 日 施行
平成 15 年 4 月 1 日 一部改正（組織名称の変更）
平成 17 年 4 月 1 日 一部改正（組織名称の変更）
平成 18 年 4 月 1 日 一部改正（組織名称、法令名の変更）
平成 20 年 4 月 1 日 一部改正（組織名称の変更）
平成 21 年 4 月 1 日 一部改正（組織名称の変更）
平成 22 年 4 月 1 日 一部改正（内容の変更）
平成 23 年 4 月 1 日 一部改正（組織名称の変更）
平成 24 年 3 月 31 日 一部改正（内容の変更）
平成 26 年 4 月 1 日 一部改正（組織名称の変更）
平成 28 年 6 月 1 日 一部改正（組織名称の変更）
平成 29 年 4 月 1 日 一部改正（内容の変更）
平成 31 年 4 月 1 日 一部改正（内容の変更）
令和 2 年 4 月 1 日 一部改正（内容の変更）
令和 2 年 5 月 8 日 一部改正（組織名称の変更）
令和 3 年 4 月 1 日 一部改正（内容の変更）
令和 4 年 9 月 1 日 一部改正（内容の変更）
令和 5 年 5 月 16 日 一部改正（組織、役職名称の変更）
令和 6 年 3 月 19 日 一部改正（内容の変更、クラウドサービス利用の変更）
令和 7 年 4 月 1 日 一部改正（内容の変更）

付 録

《 用 語 解 説 》

用 語	解 説
I C カード	薄い半導体集積回路（I C チップ）を埋め込み、情報を記録できるようにしたカードのこと。
アクセス記録	サーバの理由状況を記録すること。利用者の I P アドレス利用された日時と時刻、利用されたファイル名などを記録する。
アクセス権限	情報、情報システム及び情報システムで提供しているサービスを利用する権限をいう。
アクセス制御	情報、情報システム及び情報システムで提供しているサービスに対して、利用できる者を制限するハードウェア又はソフトウェアで実現する機能をいう。
暗号化	インターネットなどのネットワークを通じて文書や画像などのデジタルデータをやり取りする際に、通信途中で第三者に盗み見られたり改ざんされたりしないよう、決まった規則に従ってデータを変換すること。
インストール	ソフトウェアをコンピュータの記憶装置にコピーして、実行可能な状態にする行為をいう。
外部からのアクセス	インターネット等を通じて組織外のネットワークから組織内のネットワークに接続すること。
記録媒体	情報を記憶するための媒体（メディア）のこと。例えば、ハードディスク、USBメモリ、CD-R、DVD-R、MO、SDカードなど
サイバーテロ	ネットワークを通じて各国の国防、治安等をはじめとする各種情報システムに侵入し、データを破壊、改ざんするなどの手段で国家又は社会の重要な基盤を機能不全に陥れるテロ行為をいう。
サージプロテクト	雷により瞬間的に発生する異常な電圧・電流の変動から、半導体集積回路が破壊されることを防護するための装置をいう。
サーバ	サービスを提供するソフトウェア又はハードウェアをいう。
侵入検知装置 (Intrusion Detection System)	あらかじめ定義された攻撃パターンにもとづいて、情報システムに対するセキュリティ侵害を未然に防止する装置又はソフトウェアをいう。
ソースコード	プログラミング言語で記述されたプログラムの原本をいう。
ネットワークストレージサービス	ネットワーク上でファイル保管用のディスクスペースにデータを保存することが出来るサービス
パッチ	ソフトウェアの不具合を修正するための追加プログラムをいう。
パターンファイル	ウイルスを特定するための定義情報
不正アクセス	不正アクセス禁止法第3条第2項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセスをいう。
ファイアウォール	外部からの不正なアクセスから社内（内部）ネットワークを守るため、外部ネットワークと内部ネットワークの境界となる部分に設置され、意図していないデータの通過を防ぐソフトウェア又はハードウェアをいう。
フリーメール	インターネットを通じて無料で提供される電子メールサービスのこと。申し込めば無料でメールアドレスを開設し、電子メールの送受信が行えるようになる。
プロトコル	コンピュータ間において、データを送受信するときの通信及びデータの形式に関する規約をいう。
ポート	I P アドレスの下に設けられた番号のこと。
モール	床上に配線した通信線等を保護する樹脂性のケーブル保護材
リスク	情報や情報システムがセキュリティ侵害を受ける危険性をいう。
ログイン	情報システムにおいて提供されているサービスを利用するときに、利用者本人を証明して、サービスを利用するための権限を得ることをいう。
I D	利用者を特定するために割り振られた文字列をいう。（Identification）
I R T サイト	Incident Response Team(緊急対応チーム)がセキュリティ侵害に影響を及ぼすような情報を公開するW e b サイト

《 情 報 資 産 へ の 脅 威 の 例 》

ウイルス

他のファイルに隠れた自己増殖型プログラムをいう。ウイルスに感染したファイルを実行などすると、

他のファイルに自身をコピーし、際限なく増殖する。さまざまなタイプ・効果のウイルスがあり、中にはシステムの破壊やホームページの初期化など恐ろしい結果を引き起こすものもある。

サービス停止

D o S (Denial of Service) アタックと呼ばれ、標的の機器（サーバやルータ、クライアントのマシン等）を動作不能に陥らせたり、ネットワークのトラフィックを増大させたりなどしてネットワークの機能を麻痺させること。

サービス妨害

ホームページ領域乗っ取り・掲示板荒らしなど、サイトのオーナーが提供するサービスを正常に実行できなくする。

S P A Mメール

ネズミ講の勧誘・広告など無駄、あるいは意味のない内容のメール。メール受信のアクセス費用・時間が浪費される。数によってはメール爆弾同様の効果を引き起こす。

スパイウェア

スパイウェアとはウイルスの一種であり、コンピュータ内部からインターネットに対して情報を送り出すソフトウェアの総称。一般的には、そのようなソフトウェアがインストールされていることや動作していることにユーザーが気付いていない状態で、自動的に情報を送信するソフトウェアをスパイウェアと呼ぶ。

盗難・盗聴

I D情報・パスワードファイル・機密データなどを盗難し、不正閲覧・利用する。ユーザ情報の売買などが引き起こされる。

ファイル共有ソフト (P 2 P)

ファイル共有ソフトとは、インターネットで不特定多数のユーザーとファイルをやり取りするためのソフトウェア。現在では、ファイル共有ソフトをターゲットにしたウイルスにより企業や組織の機密情報がインターネット上に漏洩する事件が数多く発生。

不正侵入 (アクセス)

サーバソフト及びO Sのバグによるセキュリティホールを悪用したり、盗難I Dなどの不正なアカウントを利用してサーバにログインすること。ここからプログラム実行やホームページの消費などのリソース（資源）消費、侵害を受けたサイトを踏み台とした、機密情報への不正アクセスなどが行われる。

踏み台・不正中継

他サイトへの攻撃・S P A Mメールの中継など。攻撃された側からは、踏み台にされたサイトが攻撃したように見える。

メール爆弾

同一内容のメールを多数送り付けたり、大容量のメールを送り付けたりして標的者のメールボックスを溢れさせ、正常にメール受信できなくする。