社会福祉法人世田谷区社会福祉事業団
情報セキュリティポリシー

平成２４年１０月１８日

社会福祉法人世田谷区社会福祉事業団

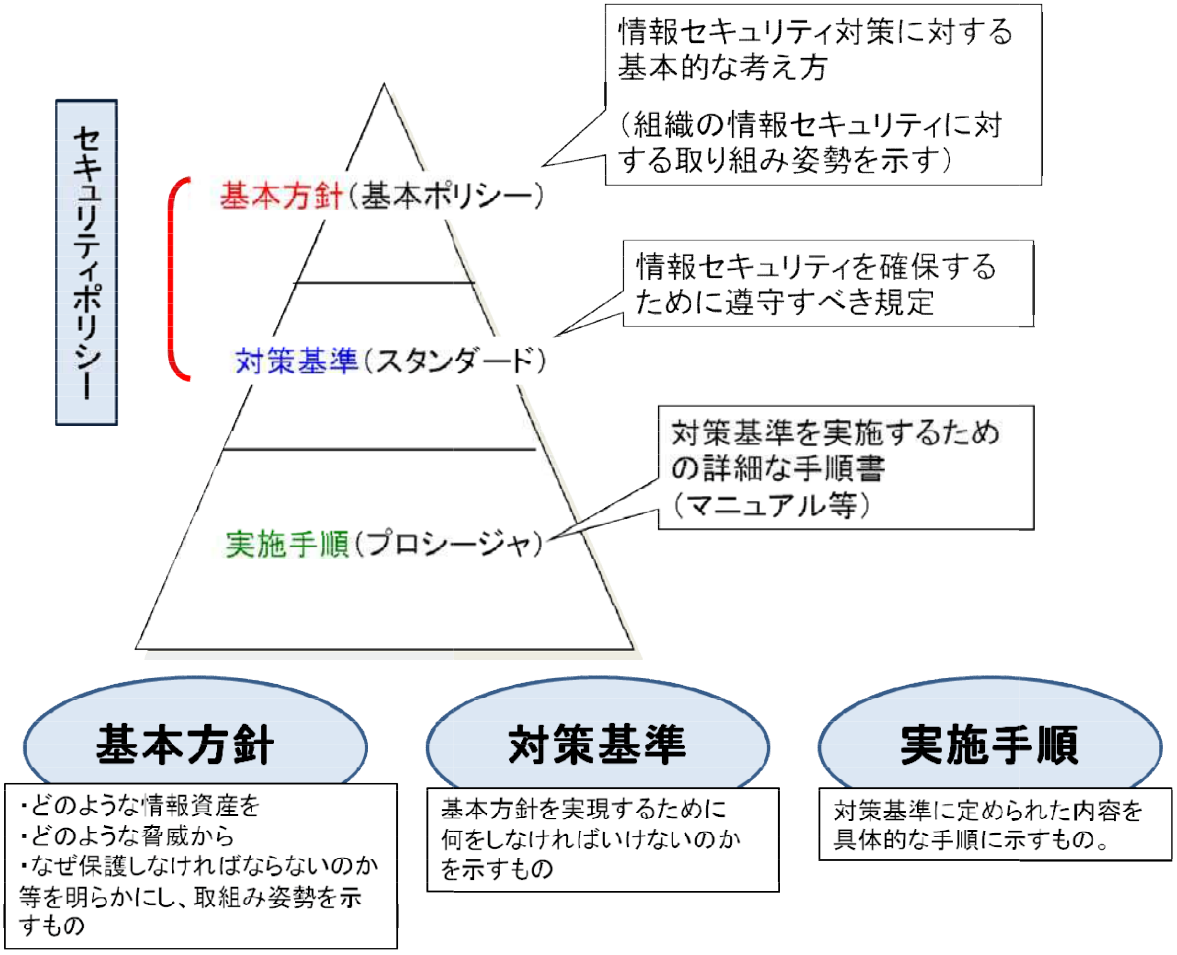
１．はじめに

インターネットを利用した情報提供及び収集が一般的になるにつれて、より高密度な情報がより高速にやりとりすることが可能となり、利便性はますます向上している。

しかし、ＩＴ化による利便性の向上は、同時に大きな危険性を抱え持つことにも繋がり、組織における情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつと考えなければならない。

組織として一貫したセキュリティ対策を行うため、事業団における組織のセキュリティ方針と対策の基準を示した情報セキュリティポリシーを策定することとした。

２．情報セキュリティポリシーの階層



３．情報セキュリティポリシーの具体的内容

（１）　責任の所在がどこにあるのか。

（２）　どの情報を誰が読み取れるようにするか。

（３）　どの操作を誰に対して許可するか。

（４）　ウィルスや外部からの侵入に対して、どのような防御体制を整えるか。

（５）　システムの停止、データの喪失等に対してどう対処するか。

（６）　それらが正常に機能していることをどのように確認し、維持管理していくか。　等

社会福祉法人世田谷区社会福祉事業団
情報セキュリティ基本方針

目　次

社会福祉法人世田谷区社会福祉事業団情報セキュリティ基本方針

1　目的

情報セキュリティ基本方針（以下「本基本方針」という。）は、社会福祉法人世田谷区社会福祉事業団（以下「本事業団」という。）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、本事業団が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2　定義

（1）　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。

（2）　情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（3）　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。

（4）　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5）　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。

（6）　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。

（7）　可用性

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

3　対象とする脅威

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。

（1）　サイバー攻撃をはじめとする部外者の侵入、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、重要情報の詐取、内部不正等

（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、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去

（3）　地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５） 電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

４ 適用範囲

（１） 対象者の範囲

本基本方針が対象とする対象者の範囲は、次のとおりとする。

① 雇用形態、職位、勤務地を問わず、本事業団の就労者

② 本基本方針の対象となる業務を外部に委託する場合の外部委託業者

（２） 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

５ 職員等の遵守義務

本事業団の就労者（以下「職員」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

６ 情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１） 組織体制

本事業団の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（２） 情報資産の分類と管理

本事業団の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（３） 物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

（４） 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（５） 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（６） 運用

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、情報セキュリティポリシーの運用面の対策を講じるものとする。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。

7　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。

8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより本事業団の事業運営に重大な支障を及ぼすおそれがあることから非公開とする。

社会福祉法人世田谷区社会福祉事業団
情報セキュリティ対策基準

目　次

社会福祉法人世田谷区社会福祉事業団情報セキュリティ対策基準

1　目的

情報セキュリティ対策基準（以下「本対策基準」という。）は、社会福祉法人世田谷区社会福祉事業団（以下「本事業団」という。）の情報セキュリティ基本方針９項に基づき、本事業団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事項を定めることにより、本事業団の有する情報資源を適正に保護、活用し並びに情報システムの信頼性、安全性及び効率性の向上に資することを目的とする。

2　対象範囲

（１）　対象者の範囲

本対策基準が対象とする対象者の範囲は、次のとおりとする。

①　雇用形態、職位、勤務地を問わず、本事業団の就労者

②　本基本方針の対象となる業務を外部に委託する場合の外部委託業者

（２）　情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

①　ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

②　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③　情報システムの仕様書及びネットワーク図等のシステム関連文書

3　組織体制

（１）　最高情報統括責任者

事務局長を、最高情報統括責任者とする。最高情報統括責任者は、本事業団における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（２）　情報統括責任者

①　総務課長を、最高情報統括責任者直属の情報統括責任者とする。情報統括責任者は最高情報統括責任者を補佐しなければならない。

②　情報統括責任者は、本事業団の全てのネットワーク及び情報システムにおける導入、設定の変更、運用、見直し等を行う権限及び責任を有する。

③　情報統括責任者は、本事業団の全てのネットワーク及び情報システムにおける情報セキュリティ対策に関する権限及び責任を有する。

④　情報統括責任者は、情報セキュリティ責任者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤　情報統括責任者は、本事業団の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、最高情報統括責任者の指示に従い、最高情報統括責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

⑥　情報統括責任者は、本事業団の共通的なネットワーク、情報システム及び情報資

産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑦　情報統括責任者は、緊急時等の円滑な情報共有を図るため、最高情報統括責任者、情報統括責任者、情報セキュリティ責任者、情報システム担当者を網羅する連絡体制を整備しなければならない。

⑧　情報統括責任者は、情報システム等について、情報セキュリティポリシーの遵守に関する意見の集約及び本事業団の職員（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

（３）　情報セキュリティ責任者

①　各課長を情報セキュリティ責任者とする。

②　情報セキュリティ責任者はその所管する課等の情報セキュリティ対策に関する権限及び責任を有する。

③　情報セキュリティ責任者は、その所掌する課等において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報統括責任者及び最高情報統括責任者へ速やかに報告を行い、指示を仰がなければならない。

（４）　情報セキュリティ管理者

①　課長等が同一建物に不在の事業所及び施設については、事業所長または施設長を情報セキュリティ管理者とする。

　情報セキュリティ管理者は、情報セキュリティ責任者を補佐する。

②　情報セキュリティ管理者はその所管する係等の情報セキュリティ管理を行う責任を有する。

③　情報セキュリティ管理者は、その所掌する係等において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（５）　情報システム担当者

①　情報統括責任者の指示等に従い、情報システムの導入、設定の変更、運用、更新等の作業を行う。

②　情報統括責任者の指示等に従い、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う。

（６）　情報セキュリティ委員会

①　本事業団の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

②　委員会は、会長及び委員をもって組織する。

③　会長は、理事長とする。

④　委員は、幹部職員とする。

（７）　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　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

4　情報資産の分類と管理方法

（1）　情報資産の分類

本事業団における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

【機密性による情報資産の分類】

分類	分類基準	取扱制限
機密性２	秘密文書に相当する機密性を要する情報資産	①必要以上の複製及び配付禁止 ②保管場所の制限 ③情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ④復元不可能な処理を施しての廃棄 ⑤信頼のできるネットワーク回線の選択 ⑥外部で情報処理を行う際の安全管理措置の規定 ⑦外部記録媒体の施錠可能な場所への保管
機密性１	機密性２以外の情報資産	

【完全性による情報資産の分類】

分類	分類基準	取扱制限
完全性２	改ざん、誤びゅう又は破損により、職員及び利用者等の権利が侵害される、又は事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	①バックアップ ②外部で情報処理を行う際の安全管理措置の規定 ③外部記録媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

【可用性による情報資産の分類】

分類	分類基準	取扱制限
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、職員用及び利用者等の権利が侵害される、又は事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	①バックアップ ②外部記録媒体の施錠可能な場所への保管
可用性１	可用性２情報資産以外の情報資産	

（２） 情報資産の管理

① 管理責任

ア 情報セキュリティ管理者及び情報セキュリティ責任者は、その所管する情報資産について管理責任を有する。

イ 情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

② 情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する記録媒体（CD-R のラベル等）、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

③ 情報の作成

ア 職員等は、業務上必要のない情報を作成してはならない。

イ 情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ 情報を作成する者は、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、情報の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。

④ 情報資産の入手

ア 職員が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

イ 職員以外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ責任者に判断を仰がなければならない。

⑤ 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。

⑥　情報資産の保管

ア　情報セキュリティ管理者及び情報セキュリティ責任者は、情報資産の分類に従って、所管する課等の情報資産を適切に保管しなければならない。

イ　情報セキュリティ管理者及び情報セキュリティ責任者は、情報資産を記録した外部記録媒体を長期保管する場合は、情報統括責任者の指示を仰ぎ、必要な措置を講じなければならない。

ウ　情報セキュリティ管理者及び情報セキュリティ責任者は、機密性２、完全性２又は可用性２の情報を記録した外部記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

エ　情報統括責任者は、情報システムのバックアップで取得したデータを記録する外部記録媒体等を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

⑦　情報の送信

電子メール等により機密性２の情報を送信する者は、必要に応じてパスワード設定を行わなければならない。

⑧　情報資産の運搬

ア　車両等により機密性２の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

イ　機密性２の情報資産を運搬する者は、情報セキュリティ責任者に許可を得なければならない。

⑨　情報資産の提供・公表

ア　機密性２の情報資産を外部に提供する者は、必要に応じてパスワードの設定を行わなければならない。

イ　機密性２の情報資産を外部に提供する者は、情報セキュリティ責任者に許可を得なければならない。

ウ　情報セキュリティ責任者は、公開する情報資産について、完全性を確保しなければならない。

⑩　情報資産の廃棄

ア　機密性２の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

イ　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

ウ　情報資産の廃棄を行う者は、情報セキュリティ責任者の許可を得なければならない。

5　物理的セキュリティ

（1）　サーバ等の管理

①　機器の取付け

情報統括責任者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

②　サーバの冗長化

ア　情報統括責任者は、重要情報を格納しているサーバ等を冗長化し、同一データを保持しなければならない。

イ　情報統括責任者は、メインサーバに障害が発生した場合に、システムの運用停止時間を最小限にするよう必要な措置を講じなければならない。

③　機器の電源

ア　情報統括責任者は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が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備え付けなければならない。

イ　情報統括責任者は、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の措置を講じなければならない。

④　通信ケーブル等の配線

ア　情報統括責任者は、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、配線収納管を使用する等必要な措置を講じなければならない。

イ　情報統括責任者は、主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合、連携して対応しなければならない。

ウ　情報統括責任者は、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しなければならない。

⑤　機器の定期保守及び修理

ア　情報統括責任者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

イ　情報統括責任者は、記録媒体を内蔵する機器を外部の事業者に修理させる場合、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他、秘密保持体制の確認などを行わなければならない。

⑥　敷地外への機器の設置

情報統括責任者は、本事業団内の敷地外にサーバ等の機器を設置する場合、最高情報統括責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

⑦　機器の廃棄等

情報統括責任者は、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、復元不可能な状態にする措置を講じなければならない。

（2）　管理区域（情報システム室等）の管理

①　管理区域の構造等

ア　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

イ　情報統括責任者は、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

ウ　情報統括責任者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

エ　情報統括責任者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び記録媒体に影響を与えないようにしなければならない。

②　管理区域の入退室管理等

ア　情報統括責任者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。

イ　職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

ウ　情報統括責任者は、外部からの訪問者が管理区域に入る場合には、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

エ　情報統括責任者は、機密性２の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、通信回線装置、外部記録媒体等を持ち込ませないようにしなければならない。

③　機器等の搬入出

ア　情報統括責任者は、搬入する機器等が、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行わせなければならない。

イ　情報統括責任者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

（３）　通信回線及び通信回線装置の管理

①　情報統括責任者は、本事業団内の通信回線及び通信回線装置を適切に管理しなければならない。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しなければならない。

②　情報統括責任者は、 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さなければならない。

③　情報統括責任者は、機密性２の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

④　情報統括責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

（４）　職員等のパソコン等の管理

①　情報統括責任者は、執務室等のパソコン等の端末について、盗難防止のため、ワ

イヤーによる固定等の物理的措置を講じなければならない。

② 情報統括責任者は、パソコン等の端末及び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しなければならない。

③ 情報統括責任者は、パソコン等の端末について、必要に応じてＢＩＯＳパスワード、ハードディスクパスワード等を併用しなければならない。

6 人的セキュリティ

（1） 職員等の遵守事項

① 職員等の遵守事項

ア 情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者及び情報セキュリティ責任者に相談し、指示を仰がなければならない。

イ 業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、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を行ってはならない。

ウ パソコン等の端末の持ち出し及び外部における情報処理作業の制限

ａ．職員等は、本事業団のパソコン等の端末、記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ責任者の許可を得なければならない。

ｂ．職員等は、外部で情報処理業務を行う場合には、情報セキュリティ責任者の許可を得なければならない。

エ パソコン等の端末等の持込

職員等は、私物のパソコン及び記録媒体を本事業団内に持ち込んではならない。

オ 持ち出し及び持ち込みの記録

情報セキュリティ管理者及び情報セキュリティ責任者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

カ パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコン等の端末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統括責任者の許可なく変更してはならない。

キ 机上の端末等の管理

職員等は、パソコン等の端末や記録媒体、情報が印刷された文書等について、第三者に使用されること、又は情報セキュリティ責任者の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、文書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。

ク 退職時等の遵守事項

職員等は、異動、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）　研修・訓練

①　情報セキュリティに関する研修・訓練

情報統括責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

②　研修計画の立案及び実施

ア　情報統括責任者は、幹部を含めすべての職員等に対する情報セキュリティに関する研修計画を定期的に立案し、情報セキュリティ委員会の承認を得なければならない。

イ　新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

ウ　情報統括責任者は、毎年度１回、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

③　緊急時対応訓練

情報統括責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。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。

④　研修・訓練への参加

幹部を含めたすべての職員等は、定められた研修・訓練に参加しなければならない。

（３）　事故、欠陥等の報告

①　本事業団内からの事故等の報告

ア　職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、速やかに情報セキュリティ管理者及び情報セキュリティ責任者に報告しなければならない。

イ　報告を受けた情報セキュリティ責任者は、速やかに情報統括責任者に報告しなければならない。

ウ　情報セキュリティ責任者は、報告のあった事故等について、必要に応じて最高情報統括責任者に報告しなければならない。

②　住民等外部からの事故等の報告

ア　職員等は、本事業団が管理するネットワーク及び情報システム等の情報資産に関する事故、欠陥について、住民等外部から報告を受けた場合、情報セキュリティ管理者及び情報セキュリティ責任者に報告しなければならない。

イ　報告を受けた情報セキュリティ責任者は、速やかに情報統括責任者に報告しなければならない。

ウ　情報セキュリティ責任者は、当該事故等について、必要に応じて最高情報統括責任者に報告しなければならない。

③　事故等の分析・記録等

情報統括責任者は、事故等を引き起こした部門の情報セキュリティ管理者、情報セキュリティ責任者及び情報システム管理者と連携し、これらの事故等を分析し、記録を保存しなければならない。

（４） ID 及びパスワード等の管理

① ID の取扱い

職員等は、自己の管理するID に関し、次の事項を遵守しなければならない。

ア 自己が利用しているID は、他人に利用させてはならない。

イ 共用ID を利用する場合は、共用ID の利用者以外に利用させてはならない。

② パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア パスワードは、他者に知られないように管理しなければならない。

イ パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

エ パスワードが流出したおそれがある場合には、情報セキュリティ管理者及び情報セキュリティ責任者に速やかに報告し、パスワードを速やかに変更しなければならない。

オ パスワードは定期的に変更し、古いパスワードを再利用してはならない。

カ 仮のパスワードは、最初のログイン時点で変更しなければならない。

キ パソコン等の端末にパスワードを記憶させてはならない。

ク 職員等間でパスワードを共有してはならない。

7 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 文書サーバの設定等

ア 情報統括責任者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

イ 情報統括責任者は、文書サーバを課等の単位で構成し、職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

ウ 情報統括責任者は、個人情報、人事記録等、特定の職員等しか取扱えないデータについて、同一課等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

② バックアップの実施

情報統括責任者は、ファイル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関わらず、必要に応じて定期的にバックアップを実施しなければならない。

③ 他団体との情報システムに関する情報等の交換

情報統括責任者は、他の団体と情報システムに関する情報等を交換する場合、その取扱いに関する事項をあらかじめ定めなければならない。

④ システム管理記録及び作業の確認

ア 情報統括責任者は、情報システムの運用において実施した作業について、作業記録を作成しなければならない。

イ 情報統括責任者は、情報システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に

管理しなければならない。

ウ　情報統括責任者又は情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

⑤　情報システム仕様書等の管理

情報統括責任者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者の閲覧や、紛失等がないよう、適切に管理しなければならない。

⑥　アクセス記録の取得等

ア　情報統括責任者は、各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

イ　情報統括責任者は、アクセス記録等が詐取改ざん、誤消去等されないように必要な措置を講じなければならない。

⑦　障害記録

情報統括責任者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

⑧　ネットワークの接続制御、経路制御等

ア　情報統括責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

イ　情報統括責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑨　外部ネットワークとの接続制限等

ア　情報統括責任者は、ウェブサーバ等をインターネットに公開する場合、本事業団内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置したうえで接続しなければならない。

イ　情報統括責任者は、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、情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑩　無線LAN 及びネットワークの盗聴対策

ア　情報統括責任者は、無線LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

イ　情報統括責任者は、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

⑪　電子メールのセキュリティ管理

ア　情報統括責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

イ　情報統括責任者は、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しなければならない。

ウ　情報統括責任者は、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能にしなければならない。

⑫　電子メールの利用制限

ア　職員等は、自動転送機能を用いて、電子メールを転送してはならない。

イ　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

ウ　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

エ　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者及び情報セキュリティ責任者に報告しなければならない。

オ　職員等は、ウェブで利用できるフリーメール、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。

⑬　電子署名・暗号化

職員等は、情報資産の分類により定めた取扱制限に従い、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、パスワードを設定して、送信しなければならない。

⑭　無許可ソフトウェアの導入等の禁止

ア　職員等は、パソコン等の端末に無断でソフトウェアを導入してはならない。

イ　職員等は、業務上の必要がある場合は、情報統括責任者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報統括責任者は、ソフトウェアのライセンスを管理しなければならない。

ウ　職員等は、不正にコピーしたソフトウェアを利用してはならない。

⑮　機器構成の変更の制限

ア　職員等は、パソコン等の端末に対し機器の改造及び増設・交換を行ってはならない。

イ　職員等は、業務上、パソコン等の端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報統括責任者の許可を得なければならない。

⑯　無許可でのネットワーク接続の禁止

職員等は、情報統括責任者なくパソコン等の端末をネットワークに接続してはならない。

⑰　業務以外の目的でのウェブ閲覧の禁止

ア　職員等は、業務以外の目的でウェブを閲覧してはならない。

イ　情報統括責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者及び情報セキュリティ責任者に通知し適切な措置を求めなければならない。

（２）　アクセス制御

①　アクセス制御

ア　アクセス制御

情報統括責任者は、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に、システム上制限しなければならない。

イ　利用者ID の取扱い

ａ．情報統括責任者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者IDの取扱い等の方法を定めなければならない。

ｂ．職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報統括責任者に通知しなければならない。

ｃ．情報統括責任者は、利用されていないIDが放置されないよう、点検しなければならない。

ウ　特権を付与されたID の管理等

ａ．情報統括責任者は、管理者権限等の特権を付与されたID を利用する者を必要最小限にし、当該ID のパスワードの漏えい等が発生しないよう、当該ID 及びパスワードを厳重に管理しなければならない。

ｂ．情報統括責任者の特権を代行する者は、情報統括責任者が指名し、最高情報統括責任者が認めた者でなければならない。

ｃ．最高情報統括責任者は、代行者を認めた場合、速やかに情報セキュリティ責任者に通知しなければならない。

ｄ．情報統括責任者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

②　職員等による外部からのアクセス等の制限

ア　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、情報統括責任者及び情報セキュリティ責任者の許可を得なければならない。

イ　情報統括責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

ウ　情報統括責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

エ　情報統括責任者は、外部からのアクセスを認める場合、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なければならない。

オ　情報統括責任者は、外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

カ　職員等は、外部から持ち帰ったパソコン等の端末を本事業団内のネットワークに接続する前に、コンピュータウイルスに感染していないこと等を確認しなければならない。

③　パスワードに関する情報の管理

情報統括責任者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

④　特権による接続時間の制限

情報統括責任者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

（３）　システム導入、保守等

① 情報システムの調達

ア 情報統括責任者は、情報システム導入、保守等の調達に当たっては、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しなければならない。

イ 情報統括責任者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

② 情報システムの導入

ア 情報統括責任者は、システムの移行について、手順を明確にしなければならない。

イ 情報統括責任者は、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い、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しなければならない。

③ システム導入、保守等に関連する資料等の保管

情報統括責任者は、システム導入、保守等に関連する資料及び文書を適切な方法で保管しなければならない。

④ 情報システムの変更管理

情報統括責任者は、情報システムを変更した場合、仕様書等の変更履歴を保管しなければならない。

⑤ ソフトウェアの更新等

情報統括責任者は、ソフトウェア等を更新等する場合、他の情報システムとの整合性を確認しなければならない。

⑥ システム更新又は統合時の検証等

情報統括責任者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

（4） 不正プログラム対策

① 情報統括責任者の措置事項

情報統括責任者は、不正プログラム対策として、次の事項を措置しなければならない。

ア 外部ネットワークから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コンピュータ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しなければならない。

イ 外部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コンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

ウ コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

エ 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

オ 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

カ　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

キ　記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、本事業団が管理している媒体以外を職員等に利用させてはならない。

②　職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

ア　パソコン等の端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

イ　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

ウ　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

エ　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

オ　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

カ　情報統括責任者が提供するウイルス情報を、常に確認しなければならない。

キ　コンピュータウイルス等の不正プログラムに感染した場合は、LAN ケーブルの即時取り外しを行わなければならない。

③　専門家の支援体制

情報統括責任者は、実施している不正プログラム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。

（５）　不正アクセス対策

①　情報統括責任者の措置事項

情報統括責任者は、不正アクセス対策として、使用されていないポートの閉鎖、改ざん見地ウェアの利用等の必要な措置を講じなければならない。

②　攻撃の予告

最高情報統括責任者及び情報統括責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

③　記録の保存

最高情報統括責任者及び情報統括責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

④　内部からの攻撃

情報統括責任者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの本事業団内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

⑤　職員等による不正アクセス

情報統括責任者は、職員等による不正アクセスを発見した場合は、当該職員等が所

属する課室等の情報セキュリティ管理者及び情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

（6） セキュリティ情報の収集

① セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

情報統括責任者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

② 不正プログラム等のセキュリティ情報の収集・周知

情報統括責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

③ 情報セキュリティに関する情報の収集及び共有

情報統括責任者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

8 運用

（1） 情報システムの監視

① 情報統括責任者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

② 情報統括責任者は、重要なアクセスログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置等を講じなければならない。

（2） 情報セキュリティポリシーの遵守状況の確認

① 遵守状況の確認及び対処

ア 情報セキュリティ管理者及び情報セキュリティ責任者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに最高情報統括責任者及び情報統括責任者に報告しなければならない。

イ 最高情報統括責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

ウ 情報統括責任者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシー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しなければならない。

② 端末及び記録媒体等の利用状況調査

最高情報統括責任者及び最高情報統括責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

③ 職員等の報告義務

ア 職員等は、情報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、直ちに情報セキュリティ管理者及び情報セキュリティ責任者に報告を行わなければならない。

イ　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報統括責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

（３）　侵害時の対応

①　緊急時対応計画の策定

最高情報統括責任者又は情報セキュリティ委員会は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、侵害時には当該計画に従って適切に対処しなければならない。

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、以下の内容を定めなければならない。

ア　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　業務継続計画との整合性確保

本事業団が自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

④　緊急時対応計画の見直し

最高情報統括責任者又は情報セキュリティ委員会は、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、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）　外部委託

①　外部委託先の選定基準

情報統括責任者は、外部委託先の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②　契約項目

情報システムの運用、保守等を外部委託する場合には、委託事業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を締結しなければならない。

ア　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

イ　委託先の責任者、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　従業員に対する教育の実施

オ　提供された情報の目的外利用及び受託者以外の者への提供の禁止

カ　業務上知り得た情報の守秘義務

キ　再委託に関する制限事項の遵守

ク　委託業務終了時の情報資産の返還、廃棄等

ケ　委託業務の定期報告及び緊急時報告義務

コ　本事業団による監査、検査

サ　本事業団による事故時等の公表

シ　情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

③　確認・措置等

情報統括責任者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、②の契約に基づき措置しなければならない。

（５）　例外措置

①　例外措置の許可

情報セキュリティ責任者は、情報セキュリティ関係規定を遵守することが困難な状況で、業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、最高情報統括責任者及び情報統括責任者の許可を得て、例外措置を取ることができる。

②　緊急時の例外措置

情報セキュリティ責任者は、業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、事後速やかに最高情報統括責任者及び情報統括責任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

最高情報統括責任者は、例外措置の審査結果等の記録を適切に保管しなければならない。

（６）　法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、関係法令を遵守し、これに従わなければならない。

（７）　懲戒処分等

①　懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、規程等による懲戒処分の対象とする。

②　違反時の対応

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、速やかに次の措置を講じなければならない。

ア　情報統括責任者が違反を確認した場合は、情報統括責任者は当該職員等が所属する課等の情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

イ　情報セキュリティ責任者の指導によっても改善されない場合、情報統括責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、情報統括責任者は、職員等の権利を停止あるいは剥奪した旨を最高情報統括責任者及び当該職員等が所属する課等の情報セキュリティ責任者に通知しなければならない。

９　評価・見直し

（１）　監査

① 実施方法

情報セキュリティ委員会は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

② 監査を行う者の要件

ア 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

イ 監査を行う者は、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でなければならない。

③ 監査実施計画の立案及び実施への協力

ア 情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

イ 被監査部門は、監査の実施に協力しなければならない。

④ 外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。

⑤ 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

⑥ 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

⑦ 監査結果への対応

最高情報統括責任者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ責任者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

⑧ 情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（２） 自己点検

① 実施方法

ア 情報統括責任者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

イ 情報セキュリティ責任者は、所管する課等における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

② 報告

情報統括責任者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

③　自己点検結果の活用

ア　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　情報セキュリティ委員会は、この点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（3）　情報セキュリティポリシーの見直し

情報セキュリティ委員会は、情報セキュリティポリシーについて情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、毎年度評価を行い、必要があると認めた場合、改善を行うものとする。

事業団セキュリティポリシー権限及び責任イメージ図

最高情報統括責任者
（事務局長）

ネットワーク・システム等の管理
情報セキュリティ対策
最終決定権限及び責任

報告

情報セキュリティ委員会
会長：理事長
委員：幹部

情報セキュリティポリシー
情報セキュリティに関する重要な
事項の決定

報告等　管理・指示等

情報統括責任者
（総務課長）

最高情報統括責任者の補佐
管理・情報セキュリティ対策
権限及び責任

報告　指名・監査依頼

情報セキュリティ
監査責任者
（総務課長）

情報セキュリティ対策状況につい
ての監査実施

報告等
指示等

システム担当者
（経営企画職員）

情報統括責任者の指示のもと
情報システム導入
実施手順の維持・管理　等

申請・報告・確認等　管理・指示・許可等

管理等

情報セキュリティ責任者
（各課長）

所管課の情報セキュリティに関す
る権限及び責任

補佐

情報セキュリティ管理者
（各係長・所長）

所管係の情報セキュリティ管理

外部委託
（委託企業）

申請・報告
・確認等

管理・指示
・許可等

報告・確認等

管理・指示等

職員等
（各課職員）

セキュリティポリシーの遵守

権限・責任等一覧表

※　記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分					項目	情報セキュリティ委員会	最高情報統括責任者	情報統括責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム担当者	職員等の義務	情報セキュリティ監査責任者	外部委託
3. 組織体制	(1)最高情報統括責任者	①			最高情報統括責任者の設置		○							
	(2)情報統括責任者	①			情報統括責任者の設置		△	○						
		②			ネットワーク及び情報システムにおける導入等の権限及び責任			○						
		③			ネットワーク及び情報システムにおける情報セキュリティ対策に関する権限及び責任			○						
		④			情報セキュリティ責任者及び管理者に対する指導及び助言			○	△		△			
		⑤			情報資産に対する侵害が発生した場合等の権限及び責任		△	○						
		⑥			情報セキュリティ及びシステム実施手順の維持・管理の権限及び責任			○			○			
		⑦			最高情報統括責任者等との連絡体制の整備		△	○	△	△	△			
		⑧			情報システムにおける意見集約、教育等			○				△		
	(3)情報セキュリティ責任者	①			情報セキュリティ責任者の設置				○					
		②			課等の情報セキュリティ対策に関する権限及び責任				○					
		③			情報資産に対する侵害が発生した場合等の報告等				○					
	(4)情報セキュリティ管理者	①			情報セキュリティ管理者の設置				△	○				
		②			係等の情報セキュリティ管理を行う責任					○				
		③			情報資産に対する侵害が発生した場合等の報告等					○				
	(5)情報システム担当者				情報システム担当者の設置						○			
	(6)情報セキュリティ委員会	①			情報セキュリティ委員会の設置	○								
4. 情報資産の分類	(2)情報資産の管理	①	ア		情報資産の管理責任				○	○				
			イ		複製等された情報資産の管理責任				○	○				
		②			情報資産の分類の表示							○		
		③	ア		業務上必要のない情報の作成の禁止							○		
			イ		情報作成時の情報の分類と取扱制限の設定							○		
			ウ		作成途上の情報の取扱							○		
		④	ア		職員が作成した情報資産の取扱							○		
			イ		職員以外が作成した情報資産の取扱							○		
			ウ		分類が不明な情報資産を入手した際の対応							○		
		⑤	ア		情報資産の業務外目的の利用の禁止							○		
			イ		情報資産の分類に応じた適切な取扱							○		
			ウ		情報資産の分類が異なる記録媒体の取扱							○		
		⑥	ア		情報分類に応じた適切な保管				○	○				
			イ		長期保管する情報資産を記録した外部記録媒体の保管				○	○				
			ウ		外部記録媒体の施錠可能な場所への保管				○	○				
			エ		情報システムのバックアップデータの保管			○						
		⑦			電子メール等での送信時の対策							○		
		⑧	ア		車両などでの情報資産運搬時の対策							○		
			イ		情報資産運搬時の許可				許			○		
		⑨	ア		情報資産の外部への提供の対策							○		
			イ		情報資産の外部への提供の許可				許			○		
			ウ		公開する情報資産の取扱				○					
		⑩	ア		情報資産廃棄時の対策							○		
			イ		情報資産廃棄時の処理の記録							○		
			ウ		情報資産廃棄時の許可				許			○		
		①			サーバ等取付時の必要な措置			○						
		②	ア		サーバの冗長化			○						
			イ		システム運用停止時間の最小化			○						

権限・責任等一覧表

※　記号:「〇」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分					項目	情報セキュリティ委員会	最高情報統括責任者	情報統括責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム担当者	職員等の義務	情報セキュリティ監査責任者	外部委託
5. 物理的セキュリティ	(1)サーバ等の管理	③	ア		予備電源の設備			〇						
			イ		過電流に対する機器の保護措置			〇						
		④	ア		通信ケーブル等の損傷防止措置			〇						
			イ		通信ケーブル等の損傷等時の対応			〇						
			ウ		ネットワーク接続口の管理			〇						
		⑤	ア		機器の定期保守の実施			〇						
			イ		修理時における外部業者からの情報漏えい防止措置			〇						△
		⑥			敷地外への機器の設置		承	〇						
		⑦			機器の廃棄等の措置			〇						
	(2)管理区域(情報システム室)の管理	①	イ		管理区域への立ち入り制限等			〇						
			ウ		耐震対策等の対策			〇						
			エ		消化薬剤等の設置方法			〇						
		②	ア		入室管理方法			〇				〇		〇
			イ		入室時の身分証明書等の携帯及び提示							〇		〇
			ウ		外部からの訪問者に対する入室管理			〇				△		
			エ		上布おシステムに関連しないコンピュータ等の持ち込み禁止			〇						
		③	ア		搬入する機器の既存情報システムへの影響確認			〇				△		△
			イ		機器などの搬入時の職員立ち会い			〇				△		
	(3)通信回線及び通信回線措置の管理	①			事業団内の通信回線等の適切な管理等			〇						
		②			外部へのネットワーク接続の限定措置			〇						
		③			通信回線に利用する回線の選択等			〇						
		④			回線に十分なセキュリティ対策の実施			〇						
	(4)職員等のパソコン等の管理	①			ノートパソコン等の盗難防止措置			〇						
		②			情報システムへのログインパスワードの設定			〇						
		③			BIOSパスワードの設定等措置			〇						
6. 人的セキュリティ	(1)職員などの遵守事項	①	ア		情報セキュリティポリシー等の遵守				△	△		〇		
			イ		情報資産の業務目的以外での使用の禁止							〇		
			ウ	a	情報資産の外部での処理時の安全管理措置				許					
				b	端末等の持ち出しの許可				許			〇		
			エ		私物パソコンの事業団内への持ち込み禁止等				許			〇		
			オ		端末等の持出及び持込の記録等				〇	〇				
			カ		パソコン等のセキュリティ設定変更の禁止							〇		
			キ		机上の端末等の管理				許			〇		
			ク		退職時の遵守事項							〇		
	(2)研修・訓練	①			情報セキュリティに関する研修・訓練の実施			〇						
		②	ア		研修計画の立案など	承		〇						
			イ		新規採用の職員等に対する研修の設定			〇				△		
			ウ		研修受講状況の報告	△		〇						
		③			緊急時対応訓練の実施			〇						
		④			研修・訓練の参加義務							〇		
	(3)事故、欠陥等の報告	①	ア		事故等の報告				△	△		〇		
			イ		情報システムに関連する事故等の報告			△	〇					
			ウ		事故等の必要に応じた報告		△	△	〇					
		②	ア		住民等外部からの報告時の対応				△	△		〇		
			イ		情報システム又はネットワークに関連する事故等の報告			△	〇					
			ウ		事故等の必要に応じた報告		△	〇						
		③			事故等の分析・記録等			〇	△	△				

権限・責任等一覧表

※　記号：「〇」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分					項目	情報セキュリティ委員会	最高情報統括責任者	情報統括責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム担当者	職員等の義務	情報セキュリティ監査責任者	外部委託
	(4)ID及びパスワード等の管理	①	ア		自己のIDの他人による利用の禁止							〇		
			イ		共用ID利用者以外による共用ID利用禁止							〇		
		②	ア		パスワードの管理							〇		
			イ		パスワードの秘密保持							〇		
			ウ		パスワードの文字の選択							〇		
			エ		パスワードの流出したおそれのある時の措置				△	△		〇		
			オ		パスワードの定期的な更新							〇		
			カ		仮パスワードの変更							〇		
			キ		パスワードの記憶機能の利用禁止							〇		
			ク		職員等間でのパスワード共有禁止							〇		
	(1)コンピュータ及びネットワークの管理	①	ア		文書サーバの容量の設定			〇						
			イ		文書サーバの課等単位での設定			〇						
			ウ		特定の情報のためのディレクトリ設定			〇						
		②			バックアップの実施			〇						
		③			他団体との情報システムに関する情報等の交換の許可等			〇						
		④	ア		情報システムの運用に係る作業記録の作成			〇						
			イ		システム変更等時の作業内容記録作成等			〇						
			ウ		システム変更の作業方法			〇			〇			〇
		⑤			ネットワーク構成図等の保管			〇						
		⑥	ア		アクセス記録等の取得等			〇						
			イ		アクセス記録等の管理			〇						
		⑦			システム障害等の記録、保存			〇						
		⑧	ア		通信ソフトウェア等の設定情報の管理			〇						
			イ		ネットワークのアクセス制御			〇						
		⑨	ア		ファイアウォール等の設置			〇						
			イ		問題発生時の物理的な遮断			〇						
		⑩	ア		無線LAN利用時の暗号化等の使用義務設定			〇						
			イ		機密性の高いネットワークへの暗号化等の措置			〇						
		⑪	ア		電子メールの中継処理禁止の設定			〇						
			イ		スパムメール等を検知した際のサーバ運用停止			〇						
			ウ		電子メールの送受信容量の上限設定等			〇						
		⑫	ア		自動転送機能の禁止							〇		
			イ		業務上必要のない送信先への送信禁止							〇		
			ウ		複数人に電子メールを送信する際の方法							〇		
			エ		重要メールの誤送信時の報告				△	△		〇		
			オ		ウェブ上のフリーメール等の使用禁止							〇		
		⑬			パスワードによる送信							〇		
		⑭	ア		ソフトウェアの無断導入禁止							〇		
			イ		ソフトウェアの導入の許可の取得			許				〇		
			ウ		不正コピーしたソフトウェアの利用禁止							〇		
		⑮	ア		機器の改造及び増設・交換の禁止							〇		
			イ		機器の改造等の禁止			許				〇		
		⑯			無許可でのネットワーク接続の禁止			許				〇		
		⑰	ア		業務目的外のウェブ閲覧の禁止							〇		
			イ		業務目的外のウェブ閲覧発見時の対応			〇	△	△				
		①	ア		アクセス制御			〇						
			イ	a	利用者の情報管理やIDの取扱い等の設定			〇						

権限・責任等一覧表

※　記号:「〇」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分					項目	情報セキュリティ委員会	最高情報統括責任者	情報統括責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム担当者	職員等の義務	情報セキュリティ監査責任者	外部委託
7. 技術的セキュリティ	(2)アクセス制御			b	利用者登録抹消の申請			△				〇		
				c	利用されるIDの点検			〇						
			ウ	a	ID及びパスワードの管理			〇						
				b	情報システム責任者等の特許を代行する者の要件		〇	〇						
				c	特許代行者の通知		〇	〇	△					
				d	特許付与されたID等の変更の外部事業者への委託禁止			〇						〇
		②	ア		外部からの内部ネットワーク等へのアクセスの許可			許	許			〇		
			イ		外部からのアクセス可能人数の制限			〇						
			ウ		外部からのアクセス時の本人確認の機能の確保			〇						
			エ		外部からのアクセス時の暗号化等の措置			〇						
			オ		外部アクセス用端末等付与時のセキュリティの確保			〇						
			カ		外部から持ち込んだ端末等のウィルスの確認等							〇		
		③			職員等のパスワード情報の管理等			〇						
		④			特許によるネットワーク等への接続時間の制限			〇						
	(3)システム導入、保守等	①	ア		仕様書への技術的なセキュリティ機能の明記			〇						
			イ		調達時のセキュリティ機能の調査等			〇						
		②	ア		システム移行の手順の明確化			〇						
			イ		移行に伴うシステム停止等の影響の最小化			〇						
		③			システム開発等の資料等の保管			〇						
		④			プログラム仕様書等の変更履歴の作成、保管			〇						
		⑤			ソフトウェア更新時の他の情報システムとの整合性確認			〇						
		⑥			システム更新又は結合時の検証等の実施			〇						
	(4)不正プログラム対策	①	ア		不正プログラムのシステムへの侵入防止措置			〇						
			イ		不正プログラムの外部への拡散防止措置			〇						
			ウ		不正プログラム情報の収集、職員等への注意喚起			〇						
			エ		不正プログラム対策ソフトウェアの常駐			〇						
			オ		不正プログラム対策ソフトウェアのパターンファイルの更新			〇						
			カ		不正プログラム対策ソフトウェアの更新			〇						
			キ		記録媒体の制限及び不正プログラム対策ソフトウェアの導入等			〇						
		②	ア		不正プログラム対策ソフトウェアの設定変更の禁止							〇		
			イ		外部からのデータ取込時のウィルスチェックの実施							〇		
			ウ		差出人が不明等のファイルの削減							〇		
			エ		不正プログラム対策ソフトウェアによる定期的なフルチェックの実施							〇		
			オ		添付ファイル送受信時のウィルスチェックの実施							〇		
			カ		ウィルス情報の確認			△				〇		
			キ		ウィルス感染時の対処方法							〇		
		③			外部の専門家の支援体制の整備			〇						
	(5)不正アクセス対策	①			使用されていないポートの閉鎖			〇						
		②			攻撃の予告時の対策		〇	〇						
		③			攻撃を受けた時の対策		〇	〇						
		④			内部からの攻撃等の監視			〇						
		⑤			職員等による不正アクセス時の対応			〇	△	△				
	(6)セキュリティ情報の収集	①			セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等			〇						
		②			不正プログラム等のセキュリティ情報の収集・周知			〇						
		③			情報セキュリティに関するグ術情報の収集及び共有			〇						
	(1)情報システムの監視	①			情報システムの監視			〇						
		②			サーバの正確な時刻設定等の措置			〇						

権限・責任等一覧表

※　記号:「〇」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分					項目	情報セキュリティ委員会	最高情報統括責任者	情報統括責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム担当者	職員等の義務	情報セキュリティ監査責任者	外部委託
8. 運用	(2)情報セキュリティポリシーの遵守状況の確認	①	ア		情報セキュリティポリシーの遵守状況の確認等		△	△	〇	〇				
			イ		問題発生時の対処		〇							
			ウ		システム設定等における情報セキュリティポリシーの遵守状況の確認等			〇						
		②			端末及び記録媒体等の利用状況調査		〇							
		③	ア		違反行為の発見時の報告			△	△	△		〇		
			イ		緊急時対策計画に従った対応			〇						
	(3)侵害時の対応	①			緊急時対応計画の策定	〇	〇							
		②			緊急時対応計画に盛り込むべき内容	〇	〇							
		③			業務継続計画と情報セキュリティポリシーの整合性の確保	〇								
		④			緊急対応計画の見直し	〇	〇							
	(4)外部委託	①			外部委託先の選定時の確認事項			〇						〇
		②			契約項目									〇
		③			委託先事業所のセキュリティ確保の確認等		△	〇						〇
	(5)例外措置	①			例外措置の許可		許	許	〇					
		②			緊急時の例外措置		△	△	〇					
		③			例外措置の申請書の管理		〇							
	(6)法令順守				主要な法令順守							〇		
	(7)懲戒処分等	①			懲戒処分							〇		
		②	ア		違反時の対応			〇	△					
			イ		違反を改善しない職員等のシステム使用の権利の停止等		△	〇	△					
9. 評価・見直し	(1)監査	①			情報セキュリティ対策状況について監査の実施	〇							△	
		②	ア		被監査部門から独立した者への監査の実施依頼								〇	
			イ		監査を行う者の要件									
		③	ア		監査実施計画の立案等	承							〇	
			イ		監査の実施に対する協力									
		④			外部委託事業者に対する監査								〇	〇
		⑤			監査結果の報告	△							〇	
		⑥			監査証拠等の保管								〇	
		⑦			監査結果への対応		〇	△	△					
		⑧			監査結果の情報セキュリティポリシー見直し等への活用	〇								
	(2)自己点検	①	ア		ネットワーク等の自己点検の実施			〇						
			イ		情報セキュリティ対策状況の自己点検			〇	〇					
		②			点検結果と改善策の報告	△		〇	〇					
		③	ア		自己の権限の範囲内での改善							〇		
			イ		点検結果の情報セキュリティポリシー見直し等への活用	〇								
	(3)情報セキュリティポリシーの見直し				情報セキュリティポリシーの見直しに関する規定	〇								