

第1 総則

1 目的

呉市水道局情報セキュリティポリシー（以下「ポリシー」という。）は、呉市水道局電算処理業務管理規程（平成20年呉市水道局規程第9号）第6条の規定に基づき、局の電算処理システムに係る情報の漏えいを防止するための基本的考え方及び具体的方法を定めることにより、その管理を徹底し、もって、事務の効率性及び適正性を確保するとともに、情報資産の保護に資することを目的とする。

2 用語の定義

このポリシーにおいて、次の各号に掲げる用語の定義は当該各号の定めるところによる。

(1) ネットワーク

コンピュータ相互の情報の伝送及びこれに伴うコンピュータの多目的利用を目的として、コンピュータ、関連機器等を相互に接続するために構築された情報通信基盤をいう。

(2) 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、電子記録媒体等で構成される情報処理体系により特定の業務を処理する仕組み（以下「プログラム」という。）及びその物理的構成要素をいう。

(3) 情報資産

情報システム及び情報システムにおいて取り扱う電磁的記録（以下「データ」という。）並びに情報システムの開発、運用、保守等に当たって必要となる紙媒体の資料等をいう。

(4) 情報資産の機密性

情報資産の使用、利用、操作、改変、持ち出し等（以下「アクセス」という。）を行う正当な権限を有する者（以下「アクセス権者」という。）以外の者には、当該情報資産のアクセスを行わせないことを確実にすることをいう。

(5) 情報資産の完全性

情報資産の内容の遺漏（情報システムの誤処理を含む。）がないことを確実にすることをいう。

(6) 情報資産の可用性

アクセス権者が、情報資産のアクセスを行うことが必要なときに、当該アクセスを行うことを確実にすることをいう。

(7) 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。

(8) 情報セキュリティ対策

情報セキュリティを実現するための具体的方法をいう。

3 ポリシーの構成

ポリシーは、主として情報セキュリティに係る基本的考え方について定める「情報セキュリティ基本方針」と、主として情報セキュリティ対策の一般的基準について定める「情報セキュリティ対策基準」により構成する。

また、「情報セキュリティ対策基準」に基づき、各個別の情報資産ごとの情報セキュリティ対策の実施手順として「情報セキュリティ実施手順」を、必要に応じて別に定めることとする。

4 対象機関

ポリシーの適用の対象となる機関は、局及び局が所管する情報システムを利用する機関とする。

第2 情報セキュリティ基本方針

1 職員等の義務

情報資産の取扱いを伴う業務に携わるすべての職員（以下「職員」という。）及び情報資産の取扱いを伴う業務を受託したもの（以下「外部受託者」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つとともに、当該業務の遂行に当たってポリシーを遵守しなければならない。

2 情報セキュリティ管理体制

情報セキュリティ対策の実施及び推進並びに実効性の担保を図るため、局全体の情報セキュリティ管理体制を確立するものとする。

3 情報資産の分類

情報資産は、それぞれの重要性を踏まえて分類をし、当該分類に応じた情報セキュリティ対策を行うものとする。

4 情報システムに係る情報資産に対する脅威

職員及び外部受託者（以下「職員等」という。）は、情報システムに係る情報資産に対する次に掲げる脅威については、その発生頻度、発生した場合の影響の大きさ等を考慮し、その危険性を特に認識するものとする。

(1) 部外者による故意の不正アクセスを原因とするデータの持ち出し、盗聴、改ざん、消去、機器及び媒体の盗取等

(2) 職員等による意図しない誤操作又は故意の不正アクセスを原因とするデータの持ち出し、盗聴、改ざん、消去、機器及び媒体の盗取等及び職員等が指定外のコンピュータ、機器等を接続することにより発生するデータの漏えい等

(3) 地震、落雷、火災その他の災害、事故、故障等を原因とする行政サービス又は業務の停止

5 情報セキュリティ対策

前項各号に掲げる脅威その他の情報資産に対する脅威から情報資産を保護するため、次に掲げるセキュリティ対策の種別に応じ、当該各号に定める措置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，情報資産の損傷の防止その他の物理的な対策を講じる。

(2) 人的セキュリティ対策

情報セキュリティ対策に関する職員等の権限や責任を定めるとともに，ポリシー，法令その他の情報セキュリティを実現するための遵守事項を周知徹底するため，職員等に必要な研修・啓発を行うなど，人的な対策を講じる。

(3) 技術的・運用的セキュリティ対策

情報システムへの不正アクセス等による脅威から情報資産を適切に保護するため，アクセスの制御，ネットワークの監視等の技術・運用面における対策を講じる。また，災害等が発生した場合における迅速かつ適切な情報セキュリティの実現を図るため，技術・運用面における対策を講じる。

6 情報セキュリティ対策基準の策定内容

情報セキュリティ対策基準においては，情報セキュリティ対策を講じるに当たっての具体的行為，判断の基準等を明記するものとする。

7 情報セキュリティ実施手順の策定

情報セキュリティ実施手順においては，各個別の情報資産の特性に応じ，その情報セキュリティ対策について，より具体的な実施手順を明記するものとする。

8 情報セキュリティ監査等の実施

ポリシーが遵守されていることを検証するため，随時に，又は定期的に情報セキュリティに関する監査，自己点検等（以下「情報セキュリティ監査等」という。）を実施するものとする。

9 評価及び見直し

情報セキュリティ監査等の実施による検証結果等を踏まえ，ポリシー及び実施手順の見直しを適宜行うこととする。なお，昨今，ネットワーク，情報システム，情報セキュリティ等に関する技術の進展は目覚ましく，かつ，当該進展内容について予測困難であることにかんがみ，情報資産を取り巻く状況の変化に迅速かつ適切に対応するため，当分の間，「情報セキュリティ対策基準」については，見直しの必要性を特に重点的に検討するものとする。

第3 情報セキュリティ対策基準

1 情報セキュリティ管理体制

情報セキュリティ管理体制は，次のとおりとする。

(1) 情報セキュリティ統括責任者

ア 局における情報セキュリティ対策を掌理するため，情報セキュリティ統括責任者（以下「統括責任者」という。）を置き，管理部長をもってこれに充てる。

イ 統括責任者は，次に掲げる職務を行う。

(ア) 各個別の情報システム間の調整

- (イ) ネットワークへの接続設定に関する基本協議
 - (ウ) 情報セキュリティに係る重要事案に関する対応の検討
 - (エ) 情報セキュリティに関する研修の企画・実施
- (2) 情報セキュリティ副統括責任者
- ア 情報セキュリティ統括責任者を補佐するため、情報セキュリティ副統括責任者(以下「副統括責任者」という。)を置き、総務企画課総務係長をもってこれに充てる。
 - イ 副統括責任者は、統括責任者の指示、命令又は委任(以下「委任等」という。)に基づき、統括責任者の職務のうち当該委任等をされた職務を行う。
- (3) 情報セキュリティ管理責任者
- ア 個別の情報資産に係る情報セキュリティの管理責任者として情報セキュリティ管理責任者(以下「管理責任者」という。)を置き、当該各情報資産を主管する課(課に準じる組織を含む。以下「課等」という。)の長をもってこれに充てる。ただし、庁内LANにおいては、庁内LANシステム管理者設置規程(平成16年呉市水道局規程第10号)第1条に規定する庁内LANシステム管理者(以下同じ。)を管理責任者とする。
 - イ 管理責任者は、次に掲げる職務を行う。
 - (ア) 情報セキュリティ実施手順の作成及びその統括責任者への報告
 - (イ) 情報セキュリティ対策の実施(職員等に対する当該実施の指示を含む。次号において同じ。)及び改善の提案
 - (ウ) 統括責任者との連絡調整
- (4) 情報システム利用責任者
- ア 個別の情報システムについて、当該情報システムを主管する課等以外の課等が、その利用のみを行う場合の当該利用に係る情報セキュリティの責任者として情報システム利用責任者(以下「利用責任者」という。)を置き、当該システムの利用を行う課等の長をもってこれに充てる。
 - イ 利用責任者は、次に掲げる職務を行う。
 - (ア) 情報セキュリティ対策の実施
 - (イ) 管理責任者との連絡調整
- 2 情報資産の分類
- 情報資産は、重要性が高いと認められる次に掲げる情報資産(以下「重要情報資産」という。)とそれ以外の情報資産とに分類し、重要情報資産については、これを取り扱う権限を有する者を定めて、適正な管理を行う。
- (1) 個人情報(呉市個人情報保護条例(平成19年呉市条例第2号)第6条第1項の規定により、同項の個人情報取扱事務として登録する事務に係る個人情報に限る。以下同じ。)の取扱いを伴う情報資産(インターネットその他の外部ネットワークに接続している情報システムに関するものに限る。)
 - (2) 管理責任者が特に重要と認める情報資産
- 3 情報資産の管理責任
- 管理責任者及び利用責任者は、主管及び利用する情報資産について、管理責

任を有する。

4 重要情報資産のセキュリティ対策

重要情報資産について、共通して実施すべきセキュリティ対策は、次に掲げるとおりとする。

(1) 物理的セキュリティ対策

ア サーバ等の設置管理

サーバ,その関連機器等,情報システムの構成要素のうち重要なもの(以下「サーバ等」という。)の取付けに当たっては,次の措置を講じる。

(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,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) ノートパソコンや携帯情報端末については,盗難防止のため,必要に応じ,ワイヤーによる固定等の措置を講じる。

イ 電源管理

(ア) サーバ等の電源については,当該サーバ等を正常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。

(イ) 高い可用性を要する情報システムのサーバ等については,可能な限り非常用電源を設置する。

(ウ) 落雷等による過電流の発生に際して,サーバ等を保護するための措置を講じる。

ウ 入退室管理

(ア) サーバ等の設置場所(以下「サーバ室等」という。)は,部外者による不正行為を防止するため,鍵,カードゲート等により入室が制限された場所とし,外部受託者等が作業を行う場合には,必要に応じて呉市水道局電算処理業務管理規程(平成20年呉市水道局規程第9号)第4条に規定する業務責任者(以下同じ。)が指名した職員が作業に立ち会う。また,サーバ室等以外の場所においても,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措置を講じる。

(イ) サーバ室等への外部受託者等による情報資産の搬出入時には,業務責任者が指名した職員が実地に立ち会う。

(ウ) サーバ室等への入退室については,入退室管理簿等により,確実に記録する。

(エ) 定期点検などのためにサーバ室等に外部受託者等を入室させる場合は,管理責任者は,外部受託者から作業を行う従業員の所属,氏名,作業内容等をあらかじめ連絡させる。

エ 共用設備の管理

プリンタ,ファクシミリ,コピー機等の共用設備は,出力した紙媒体の回収漏れによる情報漏えいを防ぐため,可能な限り,出入口,通路付近等には設置せず,職員の目の届く場所に設置する。利用責任者は,定期的に,紙媒体の回収漏れが無いことを確認する。

オ 機器の廃棄等

サーバ等の機器を自ら廃棄し，又はリース業者へ返却する場合等においては，機器内部の記憶装置に記録された情報をすべて消去し，復元不可能な状態にする。

(2) 人的セキュリティ対策

ア 職員の責務

職員は，コンピュータ，ネットワーク等の利用において次に掲げる事項を遵守しなければならない。

(ア) コンピュータ，電子記録媒体等の適正な利用・管理をし，盗難，紛失等を防止するため，管理責任者及び利用責任者の許可なくこれらを庁舎外に持ち出さない。また，個人所有のコンピュータ，電子記録媒体等を許可なく持ち込まない。

(イ) 自分に付与されたユーザID以外は，利用しない。

(ウ) アクセス権を有さない情報資産へのアクセス（データの盗聴，改ざん等を含む。以下「不正アクセス」という。）を行わない。

(エ) 名札等の記名票を常時携帯し，見えやすい場所に掲示する。

(オ) 業務終了後又は長時間コンピュータの操作を行わない場合は，必ず電源を切る。

(カ) 席を離れる場合は，短時間であってもログオフ，画面のロック，パスワードで保護されたスクリーンセーバーを有効にする等，他人が容易に操作できないような措置を講じる。

(キ) ディスプレイの表示角度を可能な限り通路から見えないように設定する。

(ク) 管理責任者の許可なく，新規にソフトウェアを導入しない。

(ケ) 業務目的以外でパソコン，ネットワーク又はインターネットへのアクセス（電子メールの使用を含む。）を使用しない。

(コ) 管理責任者の許可なく，情報システムを構成する機器等（以下「機器等」という。）の増設，改造等を行わない。

(サ) 管理責任者の許可なく，機器等の設定を変更しない。

イ パスワードの管理

職員等は，アクセス権に基づき付与されたユーザIDのパスワード（以下「パスワード」という。）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。

(ア) パスワードを適正に管理し，定期的に変更する。

(イ) パスワードを他人に教えない。

(ウ) パスワードのメモを作らない。

(エ) パスワードを共用しない。ただし，情報システムの仕様上，個人ごとのパスワードの設定が困難な場合は，管理責任者又は利用責任者が，共用のパスワードを作成し，可能な限り操作者が判別できるよう管理する。

(オ) パスワード保存機能を使用しない。

(カ) 類推しやすいパスワードは使用しない。

ウ 電子メールの利用

職員は、インターネットを経由する電子メールの利用に当たり、次に掲げる事項を遵守しなければならない。

(ア) 誤送信等によるデータの漏えいに留意する。

(イ) ファイルを添付する場合は、事前にウイルス対策ソフトウェア又はウイルス検査ソフトウェア等により、コンピュータウイルスその他の情報システムを損傷することを目的とする不正なプログラム（以下「ウイルス」という。）に感染していないことを確認する。

(ウ) 管理責任者の許可なく、電子メールの自動転送機能を使用しない。

エ 外部委託に関する管理

管理責任者は、重要情報資産の取扱いを伴う業務を外部に委託する場合、次の事項を遵守する。

(ア) 外部受託者に対して、当該業務により知り得た個人情報等を保護するために、次の事項について契約書に明記する。なお、年度更新契約を締結する場合は、不足している事項を特記事項として追加することとする。

a 個人情報保護条例の遵守

b ポリシーの遵守

c 契約に係る権利義務譲渡及び再委託先の報告義務又は制限に関する事項

d 情報資産の収受、搬送、保管、返還又は廃棄に関する事項

e 情報資産の目的外使用、複製・複写及び第三者提供の制限に関する事項

f 情報の機密保持に関する事項

g 事案（違反）等の報告に関する事項

h 成果物の所有権、著作権等に関する事項

i 損害賠償に関する事項

j 作業者に対する遵守事項の説明及び説明を受けた旨の記録

(イ) 保守作業を行う外部受託者の従業員のメールアドレスの利用について、外部受託者との間で利用方法を取り決める。

(ウ) 次に掲げる事項については、必要に応じて契約書に明記し、又は契約前に外部受託者に取扱基準を提出させる等の措置を講じるものとする。

a 作業場所、作業範囲、作業内容及び作業責任区分に関する事項

b aに掲げる事項の変更に関する事項

c 作業を行う従業員の氏名等の通知に関する事項

オ ポリシー等の掲示

統括責任者及び管理責任者は、ポリシー及び実施手順を職員等に配付し、又は事務室に掲示する等して、職員がいつでも閲覧できるようにする。

カ 研修・啓発

統括責任者は、職員を対象とした情報セキュリティに関する研修、啓発

等を随時に，又は定期に実施する。

(3) 技術的セキュリティ対策

ア アクセス制御

管理責任者は，当該主管する情報システムへのアクセスの制御について次の事項を遵守しなければならない。

(ア) 情報システムのアクセス制御

a 情報システムへのアクセス権は，必要最少限の者に付与することとし，厳重に管理する。

b 情報システムの管理者権限登録は個人のユーザIDとし，操作者を操作記録から判別できない共用のユーザID（例：Administrator）には設定しない。

(イ) ネットワークのアクセス制御

ファイアウォール等の設置により，外部から内部のネットワークへのアクセスを適切に制御する。

イ ファイアウォール

(ア) 基本的事項

a ファイアウォールに記録されたアクセスの記録その他の情報セキュリティに関する記録を取得し，一定期間保存する。

b 必要に応じ，aにより取得した記録のバックアップを行う。

(イ) 外部ネットワーク接続用ファイアウォールに係る特記事項

内部ネットワークからインターネット等外部ネットワークへの接続を確保しつつ，そのアクセスは，必要最少限のデータのみを透過させるように設定を行う。

ウ Webサーバ，DNSサーバ，メールサーバ及びファイルサーバ

(ア) インターネット等外部ネットワークを経由してアクセス可能なすべてのサーバ（以下「Webサーバ等」という。）は，ファイアウォール等で保護する。

(イ) Webサーバ等に記録されたアクセスの記録その他の情報セキュリティに関する記録を取得し，一定期間保存する。

(ウ) 不要なアプリケーション等は，一切起動しないよう設定する。

(エ) Webサーバは，HTTP，HTTPS等必要最少限の通信のみ許可し，不要なネットワークサービスの停止を行うように設定する。

(オ) DNSサーバは，第三者へのドメイン情報の漏えいを防止するため，無許可のゾーン転送を禁止するよう設定する。

(カ) メールサーバは，電子メールの不正中継を防止するため，必要のない中継を一切行わないよう設定する。

(キ) ファイルサーバは，ユーザIDごとに適正なアクセス権を設定する。

エ ウイルス対策

(ア) 管理責任者の遵守事項

a ウイルスについての情報について職員に対する注意喚起を行う。

- b ウイルスに関する情報の収集を行い，最新のウイルス対策ソフトウェアを導入し，かつ，最新のパターンファイルが使用されていることを定期的に確認する。
- c ウイルスの感染の予防，発見，駆除，復旧等の対策を行う。
- d 情報システムがインターネット等外部ネットワークに接続している場合には，ウイルス対策ソフトウェアを機器等に導入する。

(1) 職員の遵守事項

- a 外部から取得したファイル及び内部で共有する電子記録媒体は，ウイルス検査後に使用する。
- b プログラムやファイルを格納した電子記録媒体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。
- c ウイルスの感染を発見した場合は，直ちに管理責任者及び利用責任者に報告するとともに，LAN ケーブルの即時取外し又は機器等の電源遮断を行わなければならない。

オ 情報セキュリティに関する知識・情報の収集

管理責任者は，日ごろから情報セキュリティに関する知識・情報を収集し，必要に応じ，次のとおり情報セキュリティの実現を図る。

(ア) 情報システムに関する情報セキュリティの維持に重大な影響を及ぼす不具合が公開された場合は，修正用のプログラムの適用や回避策等の対応を速やかに行う。

(イ) 情報収集先（外部受託者，自治体向けセキュリティ関係機関，ベンダーのサイト等）を定める。

(ウ) 情報システムのバージョン情報を管理し，得られた情報と照合する。

(エ) 緊急を要すると判断される場合には，当該知り得た知識・情報を局内に通知し，統括責任者に報告する。

カ 住民への公開情報

ホームページその他の住民への情報提供手段として管理する情報システムについては，改ざん防止の措置を講じる等その完全性を確保する。

(4) 運用的セキュリティ対策

管理責任者及び利用責任者は，次に掲げる事項を職員等に周知し，遵守させる。

ア 所属において対応することが困難と認められるセキュリティ事案（ウイルス感染，不正アクセス等に係る事案をいう。以下「重要事案」という。）が発生した場合並びに情報システムの欠陥及び誤作動を発見した場合には，直ちに統括責任者に報告し，その指示を受ける。

イ 重要事案を報告する際は，その内容，原因，被害及び影響範囲並びに対処内容を調査の上，報告する。

(ア) 県等への報告

管理責任者は，次に掲げる重要事案が発生した場合は，統括責任者に報告し，統括責任者は，広島県情報セキュリティ主管課及び関係機関に

報告する。

- a 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。
- b 不正アクセスその他法令に違反するものと思慮されるとき。

(イ) 事案の再発防止の措置

管理責任者は、重要事案の再発防止に関して、必要な措置を講じる。

ウ 情報セキュリティに関するチェック

管理責任者及び利用責任者は、職員がポリシー及び実施手順に基づき、適切に情報システムを利用していることを定期的に確認する。

5 個人情報を取り扱う重要情報資産の管理方法

前項に定める情報セキュリティ対策のほか、個人情報を取り扱う重要情報資産の情報セキュリティ対策は、次に掲げるとおりである。

(1) 物理的セキュリティ対策

ア 基本的管理事項

(ア) 重要な情報を含む電子記録媒体は、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界対策を講じる。

(イ) 最終的に確定した電子記録媒体は、書き込み禁止措置を講じた上で、必要に応じて別の電子記録媒体に複製して保管する。

(ウ) 重要な情報資産を目的外利用し、又は庁舎外に持ち出す場合は、管理責任者及び利用責任者の承認を得る。

(エ) 重要な情報資産を外部で利用し、保管し、又は外部提供（電子メールなど、ネットワークを経由して行う提供を含む。）をする場合は、管理責任者の承認を得る。この場合において、相手方が局の機関以外のものである場合は、管理責任者は、利用、保管又は提供の理由、その期間、保管及び受渡しに関する手続及び方法その他必要な事項を定め、ポリシーを遵守することを書面で確認し、統括責任者の承認を得る。

イ 重要情報資産の廃棄

(ア) 個人情報を含む電子記録媒体を廃棄する場合は、管理責任者又は利用責任者の許可を得るとともに、当該電子記録媒体に含まれる情報を復元できないような措置を講じる。この場合において、管理責任者は、適切に廃棄されたことを廃棄証明書等により確認する。

(イ) 個人情報を含む紙媒体の資料等を廃棄する場合は、管理責任者又は利用責任者の許可を得るとともに、焼却・溶解をする等の措置を講じる。この場合において、廃棄の決定から現に廃棄するまでの期間にあっては、当該紙媒体を施錠可能な場所に保管する。

ウ 外部委託に関する措置

情報システムの開発等の外部委託を行うに際しては、次に掲げる事項を遵守しなければならない。

(ア) 外部受託者に対して、当該業務の中で知り得た個人情報等を保護するために、情報システムを開発する場合のソースコードの提出及び情報システム導入前後の検査要求事項等について契約書に明記する。なお、年

度更新契約を締結する場合は、不足している事項を特記事項として追加することとする。

(イ) 外部受託者に対して当該業務範囲外の情報資産の利用，操作等を行わせないよう指示をする。

(ウ) 外部受託者の選定に当たっては，契約相手方候補者の情報セキュリティ実施状況，経営の信頼度，実績，情報セキュリティ意識等を確認する。

(2) 技術的セキュリティ対策

ア 機器等及びネットワークの管理

管理責任者は，所管する機器等及びネットワークの管理について次の事項を遵守しなければならない。

(ア) 障害記録

情報システムの障害等が発生した場合は，障害記録として発生状況，処理状況等を記録し，常に活用できるよう保存する。

(イ) 仕様書等の管理

ネットワーク構成図，システム仕様書等の紙媒体の情報資産を部外者が無断で閲覧できないよう必要な措置を講じる。

(ウ) バックアップ

サーバ等及び機器等に記録された情報について，情報の重要度に応じて期間を設定し，定期的にバックアップを行う。

イ アクセス制御

管理責任者及び利用責任者は，当該主管する情報システムへのアクセスの制御について次の事項を遵守しなければならない。

(ア) 利用登録申請

a 管理責任者は，当該主管する情報システムのアクセス権者の登録，変更，抹消等の状況を常に把握していなければならない。

b 利用責任者は，当該利用する情報システムのアクセス権者をその所属職員のうちから選定し，当該職員の氏名その他当該情報システムを適正に利用するために必要な事項を記載した利用登録申請書を，管理責任者に提出しなければならない。

c 情報システムの仕様上又は運用上，アクセス権者ごとのユーザIDの設定が困難な場合は，共用のユーザIDを設定した上で，管理責任者において，アクセス権者以外の者が当該情報システムを利用することのないよう必要な措置を講じるものとする。

d 利用登録申請書の書式，記載事項等については，各情報システムの内容に応じ，管理責任者が別に定める。

(イ) ネットワークのアクセス制御

a 不要なネットワークサービスを使用不可にする。

b 外部ネットワークへのアクセスを適切に制御する。

(ウ) 外部からのアクセス制御

持ち出したパソコン等からのアクセスの許可は，必要最少限とする。

この場合におけるアクセス方法，使用方法等は，利用者の真正性を確保できる方法とする。

ウ ファイアウォール

他の情報システムとネットワークで接続する場合には，次に掲げる事項を遵守して，ファイアウォールを設置する。

- (ア) 当該他の情報システムを管理する者と，十分な事前協議を行った上で，相互の接続点にファイアウォールを設置する。
- (イ) 必要最小限のデータのみ透過させるように設定する。
- (ウ) 新たなアプリケーションの導入等により，ファイアウォールを透過するデータを追加する必要がある場合は，管理責任者は，統括責任者の許可を得るものとする。

エ 情報システムの調達，開発，保守，導入等

管理責任者は，新たな情報システムの調達，開発，導入及び保守に際して，次に掲げる事項を遵守しなければならない。

(ア) 調達

- a 調達に当たって一般に公開することとなる仕様書の内容が，情報セキュリティの実現に支障を生じさせることのないようにする。
- b 機器等及びソフトウェアを購入する場合等は，これらが，情報セキュリティの実現に支障を生じさせることのないものであることをあらかじめ確認する。

(イ) 開発及び保守

- a 情報システムの開発及び保守を外部委託する場合は，必要に応じて管理責任者が指名した職員を実地に立ち合わせる。
- b 作業を行う従業員及び作業範囲を明確にする。
- c 情報セキュリティの実現に支障を生じさせるおそれのあるソフトウェア等（例：セキュリティホールが指摘され，パッチ対処がされていないアプリケーション等）を使用させない。
- d 外部受託者に，開発及び保守に係る記録の提出を義務付ける。

(ウ) 導入

- a 既に稼動している情報システムに接続する場合は，あらかじめ，十分な動作試験を行う。
- b 動作試験においては，現に使用し，又は作成したデータは，これに個人情報が入り混ざるおそれがあるため，原則として使用しない。
- c 動作試験に使用したデータ及び動作試験の結果は，厳重に管理する。

(イ) 変更

情報システムを追加，変更等する場合は，その設定，機器等の構成等変更内容の履歴を記録し，保存する。

(オ) 保守及び更新

ソフトウェア（独自開発ソフトウェア，汎用ソフトウェアその他一切のソフトウェアをいう。）を更新し，又は修正プログラムを導入する場合

は、不具合の有無及び他の情報システムとの相性の確認を行い、計画的に導入する。

オ 無線 LAN

無線 LAN は、情報セキュリティの実現に支障を生じさせるおそれがないことを確認した上で、統括責任者の承認を得て利用する。

(3) 運用的セキュリティ対策

ア 情報システムの監視

管理責任者は、情報システムに対する不正アクセスを検知し、情報システムの安定した運用を確保するため、取得したアクセスの記録の内容を定期的に確認する。

イ 日常の動作確認試験

管理責任者は、情報システムの安定した運用を確保するため、次に掲げる事項を実施する。

(ア) ネットワークにおけるサーバ等及び機器等の相互の疎通確認を毎日行う。

(イ) 重要なサーバ等に関しては、毎日バックアップを取得する。

ウ 事案対応

管理責任者は、長期間にわたり情報システムを停止する必要があると判断される次に掲げる重要事案が発生した場合、継続的なネットワークの切断、情報システムの停止等の措置を講じ、統括責任者に報告する。

(ア) 不正アクセスが継続しているとき。

(イ) ウイルスがネットワーク経由で拡大しているとき。

(ウ) その他情報資産に係る重大な被害が発生しているとき。

6 情報セキュリティの実現に支障を来す行為への対応

情報セキュリティの実現に支障を来す行為を行った職員に対しては、その内容、程度に応じて、情報システムを利用することを禁じるなど、必要な措置を講じる。この場合において、地方公務員法（昭和25年法律第261号）第29条に規定する懲戒事由に該当すると認められるときは、当該行為を行った職員の氏名、行為の内容等を、総務企画課長に報告するものとする。

7 評価及び見直し

(1) 監査等

ア 管理責任者は、法令並びにポリシー及びこれに関連する規程等の遵守状況並びにこれらの運用実態について、随時に、又は定期的に監査等を実施する。この場合において、統括責任者が必要と認めるときは、統括責任者又は副統括責任者において別に監査を行う。

イ 監査を行った者は、その監査等の結果に基づき、必要な改善措置を講じる。この場合において、監査を行った管理責任者によって改善が図れない場合は、統括責任者に報告し、その命に従う。

ウ 管理責任者は、監査等の実施及び改善状況について統括責任者に報告する。

エ 管理責任者及び利用責任者は、監査等に協力し、関係書類を提出する。

(2) ポリシーの見直し

統括責任者は、新たなセキュリティ対策を講じる必要が発生した場合又は監査等が終了した場合は、ポリシーを改正する必要性を検討するものとする。

付 則

この要綱は、平成20年8月28日から実施する。

付 則

この要綱は、平成21年4月1日から実施する。