学校における情報セキュリティについて

平成25年7月

文部科学省

目　次

1．本資料の位置づけ

学校における教育の情報化が進みつつある中で、教員一人一台の校務用コンピュータの整備や校務支援システムの導入等、校務の情報化を推進することにより、教員の業務負担を軽減し、子どもと向き合う時間の確保に取り組む地方公共団体の事例が見られます。その一方で、学校現場における情報漏えいなど、情報セキュリティ対策が徹底されていないことを要因とする事故が発生しています。こうしたことへの対応として、学校が保有する情報資産の取扱いを定め、一人ひとりの教員がその取扱いを確実に遵守するため、すべての学校において情報セキュリティポリシーの策定とその適切な運用が必要となります。しかし、学校におけるICT環境の導入は設置主体である教育委員会が行っており、学校現場単独でICT環境が関連する情報セキュリティポリシーを整備することは困難であると考えられます。このため、教育委員会における情報セキュリティポリシーを準用する例や、教育委員会が中心となった体制の下に、所管する学校に共通の情報セキュリティポリシーを策定する例が見られます。その一方で、情報セキュリティポリシーの策定及び適切な運用の重要性や具体的な進め方について教育委員会や学校に共有されておらず、情報セキュリティポリシーが未整備の学校があります。

こうした状況を踏まえ、本資料では、まず、２．１にて、学校における情報セキュリティポリシーの策定に向けて、教育委員会が中心となってどのように進めればよいかについて、先進的な取組を実施する地方公共団体の実例等を踏まえ分かりやすく記載しました。２．２では、学校現場の情報セキュリティの確保のための具体的な実施方法を記載する情報セキュリティ実施手順について、特に学校現場と密接に関係する情報資産の分類（「情報区分」）及び情報資産の具体的な取扱方法（「日常の留意事項」）についてポイントを整理しました。また、２．３では、学校における情報セキュリティポリシーの運用と普及啓発について解説しています。

学校における情報セキュリティポリシーに対して、禁止事項を定めた文書であるという教職員の意識が強い傾向があるといった指摘もありますが、実際には、学校において教職員や児童生徒が、校務の情報化を含め安心してICTを活用し様々な活動を行うために必要となる事項を整理した文書であることから、可能な限りこの点について考慮した上で本資料を作成しました。

本資料の普及を通じて、学校における情報セキュリティポリシーの策定が促進され、すべての学校において適切に運用されることにより、学校における情報セキュリティの確保につながることが期待されます。

2. 学校における情報セキュリティポリシーの整備について

2.1. 学校における情報セキュリティポリシーの全体像

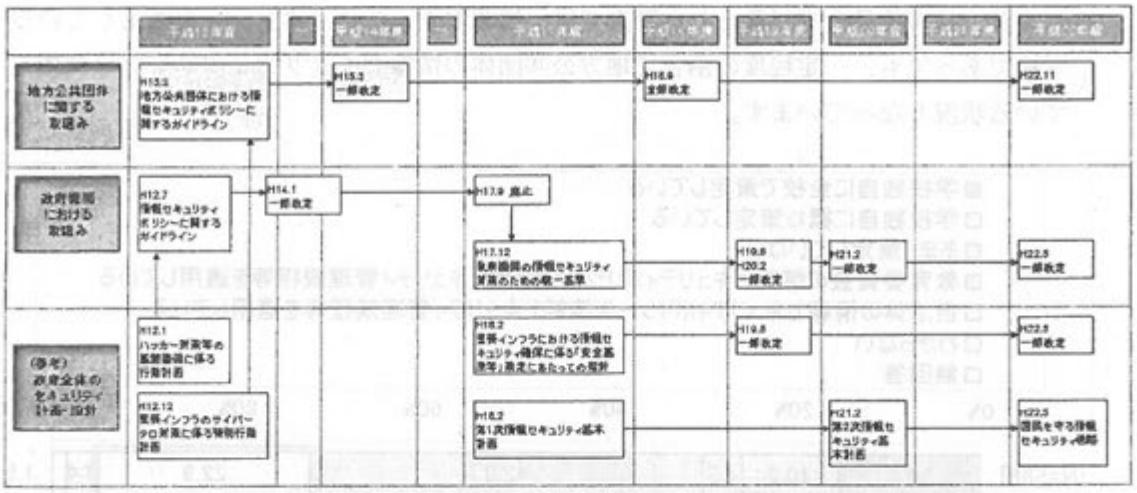
(1) 地方公共団体における情報セキュリティポリシーの整備の流れ

地方公共団体は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、他に代替することができない行政サービスを提供しています。また、地方公共団体の業務においても情報化が推進されており、快適な住民生活を保障するため、情報セキュリティ対策を講じて、その保有する情報を守ることが必要となっています。こうした状況から、すべての地方公共団体において、情報セキュリティ対策の実効性を高めるとともに、対策レベルを一層強化していくことが必要となっています。また、情報セキュリティの確保に絶対の安全はないため、情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止・迅速な対応や再発防止の対策を講じていくことが求められます。

行政手続き等における情報通信の技術の利用に関する法律（平成14年法律第151号）第9条第1項では、「地方公共団体は、地方公共団体にかかる申請、届出その他の手続きにおける情報通信の技術の利用の促進を図るため、この法律の趣旨にのっとり、当該手続きにかかる情報システムの整備及び条例又は規則に基づく手続きについて必要な措置を講ずること」に努めなければならないと規定されており、条例等に基づく手続きについては、同法第8条第2項（安全性及び信頼性の確保）において、地方公共団体は情報セキュリティポリシーの策定や見直しを行うことが定められています。

これに対応して、地方公共団体における情報セキュリティポリシーの策定を推進するため、平成13年3月30日に「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）が策定されました。その後、新たな対策技術の動向、政府の情報セキュリティ政策会議等における政策の改定等を踏まえ、これまでに3回の改訂が行われています。（http://www.soumu.go.jp/denshijiti/jyouhou_policy/）

地方公共団体では、当該ガイドラインに基づき情報セキュリティポリシーの策定が進められており、「地方自治情報管理概要」（平成21年10月公表）によれば、その策定状況は、平成21年4月時点で都道府県では100%、市区町村では97.1%となっています。



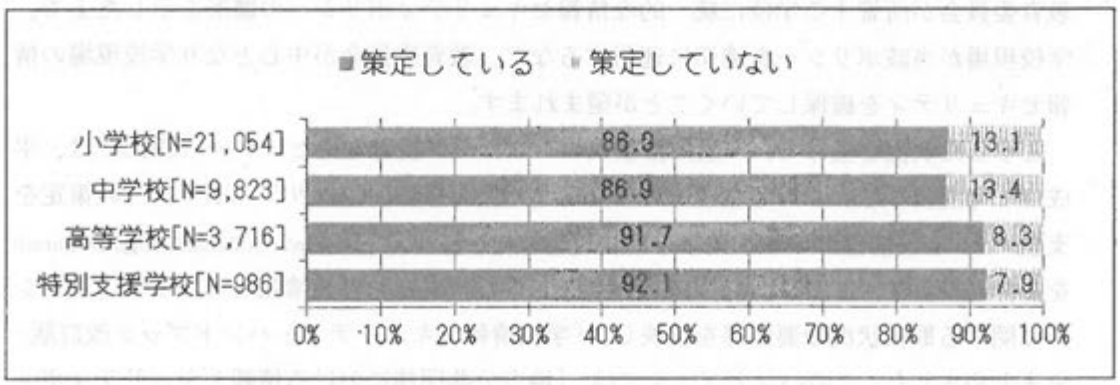
図表 1　情報セキュリティポリシー等に関する取組の推移

（出典:「地方公共団体における情報セキュリティポリシーに関するガイドライン」(総務省)）

(2) 学校における情報セキュリティポリシーの必要性

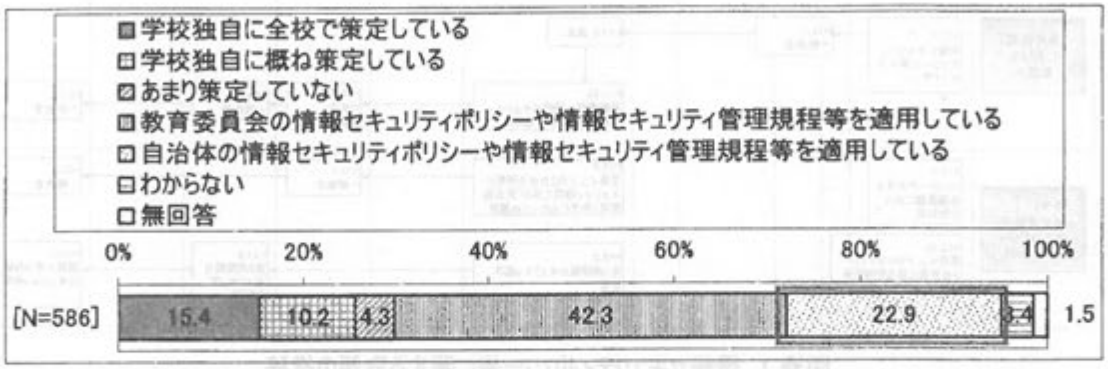
地方公共団体における情報セキュリティポリシーの整備が進む中で、学校現場において、学校情報や児童生徒の個人情報が流出する等の事故が発生するなど、学校における情報管理の重要性が高まっています。このようなことから、校務の情報化を含め、学校における ICT の活用を推進する上で、情報セキュリティの確保は極めて重要です。このため、学校が保有する具体的な情報資産の取扱いを定め一人ひとりの教員がその取扱いを確実に遵守するため、教育委員会が中心となり、学校現場の状況に応じた情報セキュリティポリシーを策定し、すべての学校において適切に運用することが望まれます。

しかし、学校における教育の情報化の実態等に関する調査（平成 23 年度　文部科学省）では、「学校における情報セキュリティポリシーを策定していない」と回答した学校は、小・中学校で 13%程度、高等学校及び特別支援学校では 8%程度となっており、早急な対応が必要となっています。



図表 2　学校における情報セキュリティポリシーの策定状況

また、教育委員会を対象とした調査では、情報セキュリティポリシーを策定している学校であっても、一定程度の割合で地方公共団体の情報セキュリティポリシーを準用している状況となっています。



図表 3 所管する学校における学校における情報セキュリティポリシーの策定状況（教育委員会が回答）

（平成 24 年 3 月　株式会社三菱総合研究所）

学校現場は、児童生徒が教室や職員室に自由に出入りできるなど、地方公共団体や民間企業とは情報を管理する場の特性が異なっていること、また、学校で守るべき情報資産は、学籍や成績の情報など、個人情報に関係するものが多いことから、情報セキュリティの確保についても、地方公共団体や民間企業とは異なる取扱が求められます。

したがって、地方公共団体の情報セキュリティポリシーを準用している学校においても、当該学校が保有する情報資産の特性を踏まえた情報セキュリティポリシーを教育委員会が策定し、適切に運用することが望まれます。

しかしながら、一般的に学校におけるネットワーク環境や情報機器の整備主体は当該学校を所管する教育委員会であり、整備されたネットワーク環境等の運用も学校単独で行うのではなく教育委員会が主導的に行っていることから、学校情報や児童生徒に関する情報等の管理に関しても教育委員会が一定の責任を担うこととなります。したがって、学校現場において独自に情報セキュリティポリシーを策定することは現実的ではなく、教育委員会が所管する学校に統一的な情報セキュリティポリシーの雛形を示した上で、学校現場が当該ポリシーを適切に運用するなど、教育委員会が中心となり学校現場の情報セキュリティを確保していくことが望まれます。

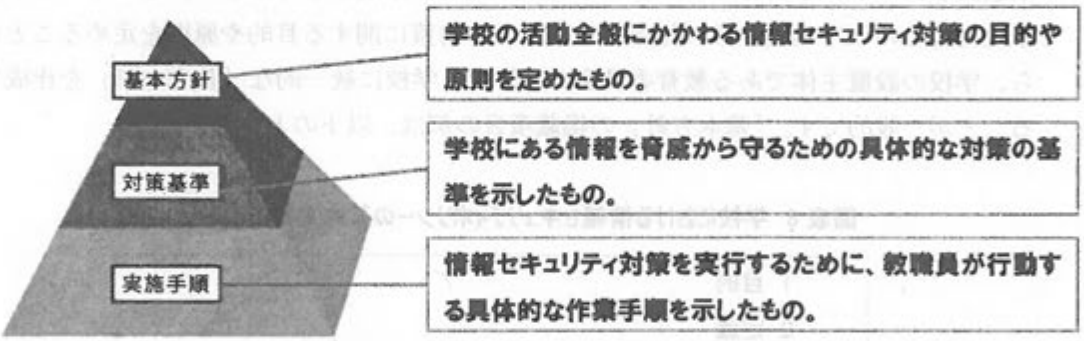
こうした状況を受けて、一般財団法人コンピュータ教育推進センター（CEC）は、平成 17 年度に学校における情報セキュリティ対策と情報セキュリティポリシーの策定を支援する「学校情報セキュリティ・ハンドブック」(http://www.cec.or.jp/seculib/haifu/18gjhaifu.html) を発行しました。さらに、平成 18 年度には、学校現場における情報セキュリティポリシーに関する取組状況や要望等を反映し、「学校情報セキュリティ・ハンドブック改訂版」をまとめました。このハンドブックでは、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）の方針に基づき、学校現場の特殊性を反映した学

校情報セキュリティポリシーの策定方法について解説するとともに、ハンドブック改訂版では、改訂前のハンドブックを活用して情報セキュリティポリシーの策定と運用を試みた教育委員会や学校の報告をまとめています。このハンドブックを参考として、学校情報セキュリティポリシーの策定と運用に取り組んでいる学校現場がみられるとともに、教育委員会にて雛形を作成し、その一部を学校が加筆・修正して「学校情報セキュリティポリシー」を整備している地域もみられます。

なお、学校が保有する情報資産は、例えば、指導要録や出席簿など、各学校に共通するものが多いため、情報資産の分類や取扱制限等も各学校共通のものとすることが適切です。このため、学校における情報セキュリティポリシーは教育委員会と学校とが連携してその内容を整理することが望ましく、その際、情報セキュリティポリシーの継続性の観点から、教職員の人事異動を考慮し、都道府県と市区町村とが連携協力することが望ましいと考えられます。

(3) 学校における情報セキュリティポリシーの概要

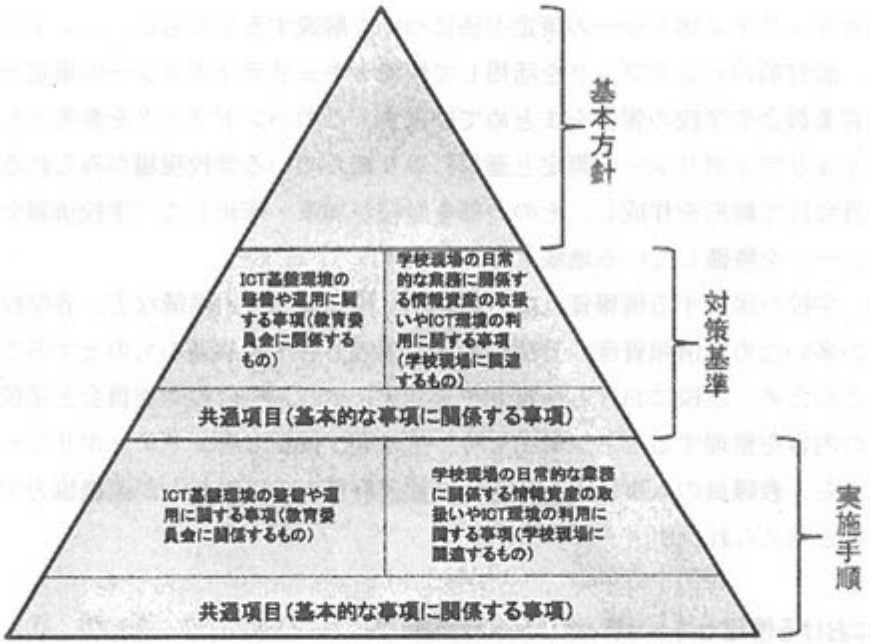
一般的に、情報セキュリティポリシーは、「基本方針」「対策基準」「実施手順」の 3 つから構成されます。「基本方針」「対策基準」を狭義の情報セキュリティポリシー、「実施手順」を含めたものを広義の情報セキュリティポリシーと呼ぶこともあります。



図表 4 情報セキュリティポリシーの概要

（出典：「教育の情報化に関する手引」（文部科学省））

既に述べたとおり、一般的に学校におけるネットワーク環境や情報機器の整備主体は当該学校を所管する教育委員会であり、整備されたネットワーク環境等の運用は教育委員会が主導的に行いながら学校現場にて実施されることとなります。したがって、対策基準や実施手順の記載内容は、大別すると、教育委員会と学校現場の両方に関連する共通事項、教育委員会に関係する ICT 基盤環境の整備や運用に関する事項、学校現場の日常的な業務に関係する情報資産の取扱いや ICT 環境の利用に関する事項の三つに分けて記載することが望ましいです。



図表 5　対策基準と実施手順の記載内容イメージ

① 基本方針と対策基準の記載事項

「教育の情報化に関する手引き」（文部科学省）では、「基本方針」について「学校の活動全般にかかわる情報セキュリティ対策の目的や原則を定めたもの」としています。学校現場でのICT環境全般の情報セキュリティ対策に関する目的や原則を定めることから、学校の設置主体である教育委員会が所管する学校に統一的な「基本方針」を作成することが一般的です。「基本方針」の掲載項目の例は、以下のとおりです。

図表 6　学校における情報セキュリティポリシーの基本方針項目例

1 目的
2 定義
3 対象とする脅威
4 適用範囲
5 教職員等の遵守義務
6 情報セキュリティ対策
7 情報セキュリティ監査及び自己点検の実施
8 情報セキュリティポリシーの見直し
9 情報セキュリティ対策基準の策定
10 情報セキュリティ実施手順の策定

（出典：「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省））

この「基本方針」に基づき、具体的な遵守事項や情報資産の重要度の区分と取扱制限等について「対策基準」で示します。「対策基準」では具体的な情報セキュリティ対策が示されますが、各学校に共通する内容であることから、「基本方針」と同様に教育委員会が統一的に作成することが一般的です。「対策基準」の掲載項目の例は、以下のとおりです。

図表 7 学校における情報セキュリティポリシーの対策基準項目例

1 対象範囲
2 組織体制
3 情報資産の分類と管理方法
4 物理的セキュリティ
5 人的セキュリティ
6 技術的セキュリティ
7 運用
8 評価・見直

（出典:「地方公共団体における情報セキュリティポリシーに関するガイドライン」(総務省)）

図表 7 の「3 情報資産の分類と管理方法」では、情報資産が学校の外に流出した場合、消失した場合、又は、書き換えられた場合に、学校に対してどのような影響が生じるか等を考慮して、情報資産の重要度の定義を明確にします。「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）では、情報セキュリティの確保に当たっては、「情報資産の機密性（許可された人だけが情報にアクセスできること）、完全性（情報が破壊、改ざん又は消去されないこと）、可用性（必要時に中断することなく情報にアクセスできること）を考慮し情報資産の重要度を定義した上で、重要度に応じた情報資産の分類及びその取扱制限を定める必要がある」とされていますが、あわせて、「職員の理解等に応じ、情報漏えいにより想定される被害の程度等を勘案して重要度を定義することもありうる」とされています。例えば、大分県教育委員会では、個人情報の有無、情報漏えい時の被害の大きさなどを基準として、情報の重要度を A～D の 4 段階に分類し、その定義を記載しています。

図表 8 情報の重要度の定義（例）

重要度	定義
A	プライバシー性が非常に高く、漏えいした場合の被害が非常に大きい
B	プライバシー性が高く、漏えいした場合の被害が非常に大きい
C	配布もしくは公開されてもよい情報のうち、個人情報を含むもの
D	配布もしくは公開されてもよい情報のうち、個人情報を含まないもの

【その他の事例】（P10：事例 2-1-1 及び P11：事例 2-1-2 参照）

一般的には、学校における情報セキュリティの確保に当たっては、完全性及び可用性よりも機密性が重視される傾向があります。この場合、教職員による情報資産の取扱いに柔軟性がなくなり、結果として規定が遵守されず情報セキュリティが確保されない状況に陥る可能性があります。このため、学校における情報セキュリティポリシーの策定・運用に当たっても、可用性及び完全性を十分に考慮し、教職員が学校において安心・安全に情報資産を取り扱えるようにすることが重要であり、このことが結果として教職員を情報セキュリティに関する事故から守ることに繋がります。

② 実施手順の記載事項

「対策基準」で示した情報資産の重要度の定義等に基づき、学校が保有する具体的な情報資産の分類とその取扱方法について、「何を」「どのようにするか」など学校現場に密接に関係する内容を「実施手順」で示します。

「実施手順」において、特に学校現場との関係が非常に深い内容として、「情報資産の洗い出しとそれぞれの情報資産が該当する区分（分類）の決定」及び「当該区分に応じた情報資産の取扱いの明確化」があげられます。

このことについて、「基本方針」では、情報資産を機密性、完全性、可用性に応じて分類を行うという情報セキュリティの基本的な方針を示し、「対策基準」では、情報資産を分類する際の重要度について、プライバシー性や情報漏えい時の児童生徒、保護者、教職員への影響の大きさに従って重要度を決定することとなります。そして、「実施手順」では、「対策基準」で定められた重要度ごとに、どの情報資産が該当するかを整理するとともに、整理した情報資産の取扱方法について具体的に記載します。（図表９参照）

実際には、教育委員会が中心となり学校現場の情報資産の状況を十分に把握した上で、「対策基準」で示された重要度に応じて個々の情報資産の分類を決定し、その取扱方法を明確にするとともに、学校現場においては、教職員が規定を遵守し適切に運用することが求められます。

基本方針

学校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。

対策基準

基本方針に従って対策基準で情報資産の分類の定義を明確化

重要度	定義
A	指導要録や評定一覧表、定期考査素点表、教職員等の給与関係書類や手当関係書類等、プライバシー性が非常に高く、情報が漏えいした場合、生徒や保護者、教職員等にとって経済的な損失や精神的な苦痛が非常に大きい校務情報。
B	生徒の通知表や定期考査答案用紙、住所録や緊急連絡先等のプライバシー性が高く、情報が漏えいした場合、生徒や保護者、教職員等に経済的な損失や精神的な苦痛が大きい校務情報。また、情報が漏えいした場合、学校運営に支障をきたす校務情報。
C	学校紹介パンフレット、PTA 資料等の配布もしくは公開されてもよい校務情報のうち、個人情報を含むもの。
D	実施後の未使用考査問題、職員会議資料等の配布もしくは公開されてもよい校務情報のうち、個人情報を含まないもの。

実施手順

対策基準で定めた重要度毎に対象となる情報資産とその取扱方法を明確化

	情報資産	取扱方法
重要度A	生徒等の障がいの状況、事件・事故、指導記録、保護者の収入等の情報等、プライバシー性が高い情報並びに指導要録や成績一覧表等、児童・生徒の情報が高度に集積している帳票や電子データ等 <学籍関係> ○指導要録(学籍に関する記録)その写し及び抄本 ○出席簿 ○卒業証書授与台帳 ○転退学受付(整理)簿 ○転入学受付(整理)簿 ○就学児童・生徒異動報告 ○休学・退学願等受付(整理)簿 ○教科用図書給付児童・生徒名簿 ○要・準要保護児童・生徒認定台帳 ○その他校内就学援助関係書類 <成績関係> ○指導要録(指導に関する記録) その写し及び抄本 ○評定一覧 ○進級・卒業判定会議録・会議資料 ○定期考査素点表 ○成績に関する個票等 <生徒指導関係> ○事故報告書・記録簿 ○生徒指導・特別指導等記録簿 ○児童・生徒等の個人写真 <進路関係> ○卒業生進路先一覧等 ○進路希望調査 ○進路指導記録 ○入学者選抜に関する表簿(願書等) <教務関係> ○高校入試関連資料(合否判定資料等含む。) <健康関係> ○健康診断に関する表簿・歯の検査表 ○心臓管理等医療情報 ○保健日誌 <事務関係> ○住民票・戸籍謄本・抄本など ○監査調書 ○叙位・叙勲書類 ○卒業生台帳 ○授業料関連書類 ○給与関係書類 ○手当関係書類	・持ち出し禁止 ・電子データは、教育委員会が設置するアクセス権限の設定ができる装置に保存 ・リモートアクセスシステムを利用して、自宅のパソコンからアクセス可能 ・簿冊等の紙文書は施錠可能な場所に保管

図表 9 情報資産の重要度の定義、重要度に応じた情報資産の分類及び取扱方法に関する記載例

「実施手順」の具体的な記載事項については、２．２にて詳細に記載します。

●学校で取り扱う情報資産の機密レベルを対策基準において明確化（杉並区）

事例 2-1-1

学校で取り扱う情報資産については、情報セキュリティポリシーの中の対策基準にて機密レベルを３段階（「高」「中」「低」）で定め、管理しています。

図表 10 情報の重要度の定義

機密レベル	定義（影響度）	定義（共有範囲）
高	・漏えいすることにより、児童・生徒・保護者に重大な影響を及ぼす情報 ・漏えいすることにより、社会的非難が大きく、信用を著しく失墜する情報 ・漏えいすることにより、法律・条例に違反する情報 ・個人情報（入学予定者・児童生徒・教職員・卒業生）	・限られた関係者のみが知り得る情報 ・原則として、学校外への持ち出しを禁止とする情報
中	・漏えいすることにより、児童・生徒・保護者に影響を及ぼす情報 ・漏えいすることにより、社会的非難がある程度発生する情報	・教育委員会・学校内で共有している情報 ・管理職の許可を得ることで、学校外へ持ち出せる情報
低	・漏えいしても、影響はない情報	・公開されている情報 ・十分な注意を払うことで、学校外への持ち出しができる情報

その上で、学校で取り扱う情報資産 228 項目について、情報資産台帳でどの機密レベルにあたる情報なのかを明記しました。児童生徒の出欠・成績管理、指導要録情報、保健情報等の機密レベル「中」「高」のものは校務ネットワークでのみ扱うことと対策基準で定め、教材や生徒の作品等の機密レベル「低」の情報については、教育用ネットワークで扱うこととしました。情報資産台帳の情報項目について、教育委員会が設定した 228 項目以外の情報が学校現場に存在する場合は、学校現場にて情報資産台帳に追加を行い、機密レベルとの関係を明確にした上で運用を行っています。

情報を個人情報とその他の情報の2種類に分類（横浜市）　事例 2-1-2

学校における情報セキュリティポリシーの基本方針の中で、学校で扱う情報については、「個人情報」及び「その他の情報」の２種に区分して管理しています。それぞれの区分ごとに情報の取扱いに関する通知により、情報の取扱いについて明確に定めています。

通知の中では、電子データと紙データを分けて、取扱方法について定めており、電子データについては、「学校の組織として対応すること」、「教職員として対応すること」の2 つに分けて取扱方法について定めています。なお、情報の学校外への持ち出しについては、個人情報は原則として校長の承認制とし、その他の情報は校長への届出制としています。

2.2. 実施手順の内容

(1) 「実施手順」における記載事項の概要

「実施手順」は、学校現場において教職員（非常勤職員、臨時職員を含む）が具体的に対応する事項を定める文書であることから、分かりやすく、現実的な内容とすることが必要です。「対策基準」の内容を「実施手順」において具体化するポイントとしては、以下の事項が考えられます。

＜具体化のポイント＞

- 「実施手順」を遵守するべき者が誰なのかを明確にする。
- 用語の定義を明確にして、読み手によって解釈が異ならないようにする。
- 情報資産の重要度の区分（分類）に当たっては、どの情報資産がどの重要度に該当するか一覧表等で明確にする。
- いつ、何を、どのように実施するかを具体的に分かりやすく記載する。例えば、出勤から退校までに携わる業務の流れに沿って、出勤時、システム利用時、離席時、退校時等の場面ごとに実施すべき手順を記載する、あるいは、E メール、校務支援システム、USB メモリ、クラウド等、利用するシステムごとに実施すべき手順を記載する。
- 禁止すべき事項と、留意すべき事項に分けて記載する。
- PC の操作方法等、多くの教職員に関係する内容については、図等を使用して分かりやすく記載する。
- 許可、申請、記録、報告で使用する書式等は、どのような場合に必要になるかを明示するとともに、具体的な記入例を示す。
- 事故が発生したときの連絡系統等の体制を明確に定め、図にして分かりやすく示す。

以下では、大分県教育委員会の事例を参考にしながら、「実施手順」に記載する主な内容について解説します。

＜大分県学校情報セキュリティ実施手順における主な記載事項＞

1 目的

「基本方針」、「対策基準」との関係性を明確にしながら、「実施手順」を作成する主旨と目的について具体的に記載します。

2 適用者

情報資産を取扱う対象者が、教職員等の学校関係者におけるどの者であるかを具体的に記載します。

3 用語の定義

「実施手順」に記載される用語について定義を明確にし、「実施手順」に対する学校現場の解釈の統一を図り、「実施手順」の運用が適正に行われるようにします。

4 管理体制

「基本方針」及び「実施手順」の周知及び遵守状況を確認するために、各学校における管理体制等について記載します。

5 情報区分

「実施手順」に定める情報資産の範囲を明確にした上で、「対策基準」で決定した重要度ごとに情報資産を整理し、重要度ごとの取扱方法を明確に示します。

6 日常の留意事項

5で示した取扱方法に関連して、教職員が遵守すべき具体的な手順を、学校での日常的な業務に関連付けて、分かりやすく記載します。

7 ネットワークの利用・管理

情報資産の取扱いをネットワーク上で行う場合に、サービスごとの利用に関する遵守事項について明確に定めます。

8 緊急時及び障害発生時の対応

障害や事故等が発生した際、被害の拡大防止や復旧に向けた手順等、教職員等が対応しなければならない事項を記載します。

9 情報セキュリティ研修等

情報セキュリティに関する教職員等を対象とした研修を実施する場合は、具体的な研修内容、参加対象者等について明確に記載します。

上記に加えて、「情報セキュリティ検証（監査）」や「人事異動時の注意事項」等についても、具体的な留意事項を記載します。

以下、（2）、（3）では、特に学校現場との関係が深く、多くの教職員に関係する「5 情報区分」と「6 日常の留意事項」における記載事項の詳細について示します。

(2) 「5 情報区分」における記載事項

「実施手順」では、「対策基準」において決定した重要度に基づき、個々の情報資産がどの重要度の区分に当てはまるかを整理します。そして、重要度ごとに、それぞれの情報資産に対する取扱方法について規定します。

図表 11 重要度 A での情報資産とその取扱方法(大分県教育委員会の例)

情報資産	取扱方法
指導要録(学籍に関する記録)その写し及び抄本、出席簿、卒業証書授与台帳、転退学受付(整理)簿、転入学受付(整理)簿、就学児童・生徒異動報告書、休学・退学願等受付(整理)簿、教科用図書給付児童・生徒名簿、要・準要保護児童・生徒認定台帳、その他校内就学援助関係書類	・持ち出し禁止 ・電子データは、教育委員会が設置するアクセス権限の設定ができる装置に保存 ・リモートアクセスシステムを利用して、自宅のパソコンからアクセス可能 ・簿冊等の紙文書は施錠可能な場所に保管

※重要度 B、C、D の例は、P18:事例 2-2-1 を参照のこと。

なお、学校が保有する情報資産を、学校の業務に関連付けて、「学籍関連」「児童生徒指導関連」「成績関連」「進路関連」「保健関連」「学校運営関連」「事務関連」等の観点からあらかじめ整理しておくと、個々の情報資産の分類を円滑に行えます。

図表 12 学校が保有する情報資産の分類の例

分類	項目例
学籍情報	指導要録、出席簿、卒業証書授与台帳、転退学受付簿、転入学受付簿、就学児童・生徒異動報告書、休学・退学願等受付簿等
指導関連	事故報告書・記録簿、生徒指導・特別指導等記録簿、児童・生徒等の個人写真、児童生徒個人調査票、教育相談・面接の記録、個別の教育支援計画、個別の指導計画、児童生徒指導計画、児童生徒指導のしおり等
成績情報	指導要録、評定一覧表、進級・卒業判定会議資料、定期考査素点表、通知表、定期考査答案用紙、児童・生徒作品・作文・レポート等
進路関連	卒業生進路先一覧、進路希望調査票、進路指導記録簿、入学者選抜に関する表簿、調査書、推薦書、受験報告書、進路のしおり等
教務関係・保健関係	高校入試関連資料、健康診断に関する資料、保健日誌、教務手帳、指導計画、児童・生徒等健康調査票、健康保険証の写、考査問題等
学校運営関連	学級費会計簿、児童・生徒等名簿、住所録、緊急連絡先・学級の緊急連絡網、職員会議資料、学校要覧、学校紹介パンフレット、PTA 資料、ホームページ情報、学校行事のしおり、卒業アルバム・集合写真等、職員会議資料等

分類	項目例
事務関連	住民票・戸籍謄本・抄本等、監査調書、卒業生台帳、授業料関連書類、給与関係書類、手当関係書類、各種証明書関係書類、収入調定書、各種点検報告書、服務管理関連書類、授業用教材、教材研究資料、学級(学年)通信、宿題プリント、動画等

(3)「6 日常の留意事項」における記載事項

「実施手順」において、学校現場における個々の情報資産を重要度に応じて分類し、その取扱方法について規定しますが、取扱方法の記載内容として、実際にいつ、どのように当該情報資産を取り扱うかという学校現場に関連付けた内容が含まれておらず、教職員にとって学校の日常業務の中で実際にどのように情報資産を取扱えばよいかが分かりにくい場合があります。そこで、そのような取扱方法をあらかじめ洗い出し、教職員が遵守すべき具体的な手順を学校での日常的な業務に関連させた上で分かりやすく記載します。

図表 13 学校での日常的な業務に関連させた情報資産の取扱い(例)

日常的な情報資産の取扱い	場面ごとの情報資産の取扱い
・校務情報の取扱い ・校内・校外でのパソコンの利用 ・電子記録媒体の利用 ・ソフトウェアの利用 ・リモートアクセスシステム(※)の利用 ・ログイン ID 及びパスワードの管理 ・職員室内や事務室内の整備と行動 等	・出勤時の情報資産の利用 ・離席時の情報資産の利用 ・退校時の情報資産の利用 等

※教職員が自宅などの学校外において、安心・安全に職員室内と同様の業務を行える環境

さらに、学校での日常的な業務に関連させた情報資産の取扱いについて、留意事項(取扱い時に気を付けないといけないこと)と禁止事項(禁止されていること)に分けて記載します。

例えば、「5 情報区分」では、重要度 A(指導要録、出席簿、評定一覧表等)の取扱方法として「電子データは、教育委員会が設置するアクセス権限の設定ができる装置に保存すること。」と定めますが、ここには、教職員が実際にどのように情報資産を取り扱うかという学校現場に関連付けた内容が十分に含まれていません。そこで、「6 日常の留意事項」では、「退校時には、保存する必要のない情報(一時ファイル)は確実に消去すること。」(留意事項)、「退校時には、重要度 A、B の電子データは文書管理システム又は統合ファイルサーバの学校フォルダに移行し、校務用パソコンのローカルハードディスクに電子データを保存したまま退校することを禁止する。」(禁止事項)のように、

分類	項目例
事務関連	住民票・戸籍謄本・抄本等、監査調書、卒業生台帳、授業料関連書類、給与関係書類、手当関係書類、各種証明書関係書類、収入調定書、各種点検報告書、服務管理関連書類、授業用教材、教材研究資料、学級(学年)通信、宿題プリント、動画等

(3)「6 日常の留意事項」における記載事項

「実施手順」において、学校現場における個々の情報資産を重要度に応じて分類し、その取扱方法について規定しますが、取扱方法の記載内容として、実際にいつ、どのように当該情報資産を取り扱うかという学校現場に関連付けた内容が含まれておらず、教職員にとって学校の日常業務の中で実際にどのように情報資産を取扱えばよいかが分かりにくい場合があります。そこで、そのような取扱方法をあらかじめ洗い出し、教職員が遵守すべき具体的な手順を学校での日常的な業務に関連させた上で分かりやすく記載します。

図表 13 学校での日常的な業務に関連させた情報資産の取扱い(例)

日常的な情報資産の取扱い	場面ごとの情報資産の取扱い
・校務情報の取扱い ・校内・校外でのパソコンの利用 ・電子記録媒体の利用 ・ソフトウェアの利用 ・リモートアクセスシステム(※)の利用 ・ログイン ID 及びパスワードの管理 ・職員室内や事務室内の整備と行動 等	・出勤時の情報資産の利用 ・離席時の情報資産の利用 ・退校時の情報資産の利用 等

※教職員が自宅などの学校外において、安心・安全に職員室内と同様の業務を行える環境

さらに、学校での日常的な業務に関連させた情報資産の取扱いについて、留意事項(取扱い時に気を付けないといけないこと)と禁止事項(禁止されていること)に分けて記載します。

例えば、「5 情報区分」では、重要度 A(指導要録、出席簿、評定一覧表等)の取扱方法として「電子データは、教育委員会が設置するアクセス権限の設定ができる装置に保存すること。」と定めますが、ここには、教職員が実際にどのように情報資産を取り扱うかという学校現場に関連付けた内容が十分に含まれていません。そこで、「6 日常の留意事項」では、「退校時には、保存する必要のない情報(一時ファイル)は確実に消去すること。」(留意事項)、「退校時には、重要度 A、B の電子データは文書管理システム又は統合ファイルサーバの学校フォルダに移行し、校務用パソコンのローカルハードディスクに電子データを保存したまま退校することを禁止する。」(禁止事項)のように、

図表 15 場面ごとの情報資産の取扱い(例)

場面	留意事項	禁止事項
出勤時の情報資産の利用	・業務中は名札を着用するように心掛ける。 ・校務用パソコンや電子記録媒体、文書等が帰宅時と相違がないか確認すること。	なし
離席時の情報資産の利用	・ログインしたまま、離席しないようにすること。自分でログオフ又はコンピュータのロックをすること。 ・席を離れる場合には、画面を覗かれたり、不正に操作されたりすることのないように必ずふたを閉めるなどの対策を行うこと。 ・文書は机の中等に入れて他人が直接見えないように管理すること。	・重要度 B 以上の電子データを含む公用 USB メモリや文書を机上に放置すること。
退校時の情報資産の利用	・保存する必要のない情報(一時ファイル)は確実に消去すること。 ・校務用パソコンは必ずシャットダウンを行ったうえで、退校すること。 ・最終退校者は、建物が施錠されていることを確認すること。	・校務用パソコンのローカルハードディスクに重要度 A、B の電子データを保存したまま退校すること。(重要度A、Bの電子データは、文書管理システム又は統合ファイルサーバの学校フォルダに移行した上で退校すること。) ・重要度 B の電子データを保存した電子記録媒体や紙文書を机上に放置したまま退校すること。(重要度Bの電子データを保存した電子記録媒体や紙文書は、原則として施錠できるキャビネットに保管して退校すること。)

※離席時及び退校時などの不在時のパソコンの保管については、別途「校内・校外でのパソコンの利用」の項目の中で施錠できる場所に保管するなどの運用を定める必要があります。

● 情報の重要度に応じた取扱方法を、学校における情報セキュリティポリシーにおいて明確化（大分県）

事例 2-2-1

県の情報セキュリティポリシーでは、職場で作成した資料の持ち出しを原則禁止していますが、学校現場では児童生徒に資料を渡して持ち帰らせることが多いため、学校現場の実態に沿っていませんでした。そこで、学校現場の実態に合うように、教育委員会で「基本方針」、「対策基準」、「実施手順」からなる「大分県立学校情報セキュリティポリシー」を独自に作成しました。この中で、情報資産の重要度を A（指導要録、定期考査素点表等）、B（通知表、住所録等）、C（学校パンフレット、PTA 資料等）、D（授業用教材、課題プリント等）の 4 段階に分類しました。

重要度 A

学籍情報	生徒指導関連	成績情報
指導要録（学籍に関する記録） その写し及び抄本 出席簿 卒業証書授与台帳 転退学受付（整理）簿 転入学受付（整理）簿 就学児童・生徒異動報告書 休学・退学願等受付（整理）簿 教科用図書給付児童・生徒名簿 要・準要保護児童・生徒認定台帳 その他校内就学援助関係書類	事故報告書・記録簿 生徒指導・特別指導等記録簿 児童・生徒等の個人写真	指導要録（指導に関する記録）その写し及び抄本 評定一覧表 進級・卒業判定会議録・会議資料 定期考査素点表 成績に関する個票等
進路関連	**教務関係・保健関係**	**事務関連**
卒業生進路先一覧等 進路希望調査 進路指導記録簿 入学者選抜に関する表簿（願書等）	高校入試関連資料（合否判定資料等含む。） 健康診断に関する表簿・歯の検査表 心臓管理等医療情報 保健日誌	住民票・戸籍謄本・抄本等 監査調書 卒業生台帳 授業料関連書類 給与関係書類 手当関係書類
＜取扱方法＞ ・持ち出し禁止 ・電子データは、教育委員会が設置するアクセス権限の設定ができる装置に保存 ・リモートアクセスシステムを利用して、自宅のパソコンからアクセス可能 ・簿冊等の紙文書は施錠可能な場所に保管		

重要度 B

学校運営・学校経営・その他	生徒指導関連	成績情報
不審者対策等マニュアル 学級費会計簿 児童・生徒等名簿 住所録 緊急連絡先・学級の緊急連絡網 職員会議資料	生徒個人調査票 指導カード（児童・生徒等理解カード） 教育相談・面接の記録・カード等 個別の教育支援計画 個別の指導計画 自転車等通学生一覧表	通知表 定期考査答案用紙 児童・生徒作品・作文・レポート等
進路関連	**教務関係・保健関係**	**事務関連**
調査書 推薦書 受験報告書	教務手帳 週ごとの指導計画（個人情報が含まれるもの。） 児童・生徒等健康調査票 健康保険証の写し	各種証明書関係書類 収入調定書 旅行関係書類 運転免許・教員免許状等の写し 各種点検報告書 休暇欠勤簿等の服務管理関連書類

＜取扱方法＞

・原則持ち出し禁止

・持ち出す都度、校長等の書面による許可が必要

・電子データを校外へ持ち出す場合は、公用 USB メモリで取り扱い暗号化等のセキュリティ対策を施すこと。

・校外でパソコンを使用する場合は、校務用パソコンと公用 USB メモリで処理を行うこと。

・電子データは、教育委員会が設置するアクセス権限の設定ができる装置で取り扱うこと。

・リモートアクセスを利用して、自宅の私的に所有するパソコンで、サーバ内の電子データを操作することができる。

・紙文書を校外へ持ち出す場合は、外部から見えない鞄等に入れ、寄り道をせずに目的地まで、厳重に管理して運搬すること。

重要度 C

学校運営・学校経営・その他	生徒指導関連	成績情報
学校要覧 学校紹介パンフレット PTA 資料 ホームページのバックアップ	生徒指導計画や生徒指導のしおり等	

データ 学校行事のしおり(修学旅行・キャンプ・合宿等) 卒業アルバム・集合写真等		
進路関連	教務関係・保健関係	事務関連
進路のしおり等	考査問題	
＜取扱方法＞ ・包括的承認 ・持ち出す都度、又は一括して校長等の口頭による許可が必要 ・電子データを校外へ持ち出す場合は、公用 USB メモリ又は教育委員会が許可するクラウドサービスで取り扱うこと。 ・紙文書を持ち出す場合は、適切に管理を行うこと。		

重要度 D

学校運営・学校経営・その他	生徒指導関連	成績情報
職員会議資料(個人情報を含まないもの。) 求人一覧		
進路関連	教務関係・保健関係	事務関連
進路のしおり等	考査問題 ※実施後の未使用の考査等	授業用教材 教材研究資料 学級(学年)通信 宿題プリント(※解答後の取扱いは、重要度 B と同様。) 動画等
＜取扱方法＞ ・包括的承認 ・電子データを校外へ持ち出す場合には、原則公用 USB メモリ又は教育委員会が許可するクラウドサービスで取り扱うこと。 ・紙文書を持ち出す場合は、適切に管理を行うこと。		

次に、システムや媒体ごとに、扱える情報はどれかを情報セキュリティ実施手順にて明確化しました。クラウドで扱う情報については同様の区分で扱いを明確化して、重要度 C、D の情報をパブリッククラウド上でのみ扱うこととし、重要度 A、B の情報をプライベートクラウド上でのみ扱うこととしました。このような対応により、現場の教職員が、電子化されたデータの取扱いについて迷うことなく適切に判断することができるようになり、情報漏えいの事故も少なくなりました。

図表 16 情報の重要度と情報を扱う環境・機器との関係

情報の重要度	情報の説明	資料例	個人情報有無	クラウド		校内サーバ(学習系)	校務用PC	リモートアクセス	メモリなど
				プライベート	パブリック				
A	プライバシー性が非常に高く、情報が漏洩した場合、経済的な損失や精神的な苦痛が非常に大きい校務情報	指導要録、定期考査素点表等	有	○				○	
B	プライバシー性が高く、情報が漏洩した場合、経済的な損失や精神的な苦痛が大きい校務情報	通知表、住所録等	有	○				○	
C	配布または公開されてもよい校務情報のうち、個人情報を含むもの	学校パンフレット、PTA資料等	有		○		○	○	○
D	配布または公開されてもよい校務情報のうち、個人情報を含まないもの	授業用教材、課題プリント等	無		○	○	○	○	○

2.3.学校における情報セキュリティポリシーの策定と適切な運用に向けて

(1) 学校における情報セキュリティポリシーの策定

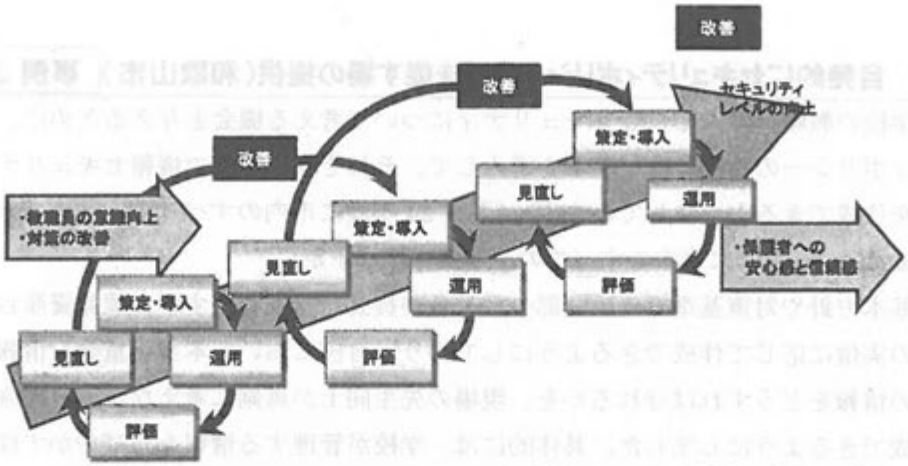
教育委員会における情報セキュリティポリシーは、地方公共団体の情報セキュリティポリシー（多くの場合、基本方針と対策基準）を準用する場合が多いですが、2.1(2)において記したとおり、学校現場の特性を踏まえ、学校現場において地方公共団体の情報セキュリティポリシーを準用することは適切ではないと考えられます。このため、教育委員会が所管する学校に統一的な情報セキュリティポリシーの「基本方針」と「対策基準」を定める例が多くみられます。そして、教育委員会がその内容について学校現場での理解を図りながら、「実施手順」の雛形を作成し、それを基に各学校が実情に応じて微修正を加える形や、教育委員会が域内の学校向けに統一の「実施手順」を作成する例も見られます。

「実施手順」は、学校現場で教職員がどのように情報セキュリティ対策を行うかについて具体的に記載し、教職員が学校で情報資産を管理するための共通理解を持つことにより、統一的な対応を徹底するための文書であることから、教職員自身が「実施手順」の作成にかかわることが必要であると考えられます。（P24：事例 2-3-1 参照）この場合も、教育委員会が定期的にその内容を把握し、必要に応じて指導することが求められます。また、学校現場における「実施手順」の普及・啓発のため、教職員が「実施手順」の内容をすぐに参照できるように工夫することも効果的です。（P25：事例 2-3-2 及び P26：事例 2-3-3 参照）

(2) 学校における情報セキュリティポリシーの適切な運用

情報セキュリティ対策の実施は、情報セキュリティポリシーを整備するだけでは実現することはできず、整備した情報セキュリティポリシーを学校現場で適切に運用していく必要があります。このことに関することについて、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）では「PDCA サイクル」として指摘しています。情報セキュリティ対策の運用は、策定・導入（Plan）、運用（Do）、評価（Check）、見直し（Action）の 4 段階に分けるとともに、この実施サイクルを繰り返すことによって情報セキュリティが確保されるとしています。

情報セキュリティを取り巻く脅威や求められる対策は常に変化しており、上記の PDCA サイクルは、一度限りではなく定期的に繰り返すことで、環境の変化に対応しつつ情報セキュリティ対策の水準の向上を図っていくことが必要であると考えられます。



図表 17 PDCA サイクルの繰り返しによる情報セキュリティ対策の水準の向上

（出典:地方公共団体における情報セキュリティポリシーに関するガイドライン(総務省)）

PDCA の考え方に基づき、情報セキュリティポリシーを策定・導入（Plan）し、運用（Do）した後は、あらかじめ定められた期間ごとに、又は社会状況が大きく変化した場合に、適切性、妥当性及び有効性について確認するために評価（Check）することが必要です。

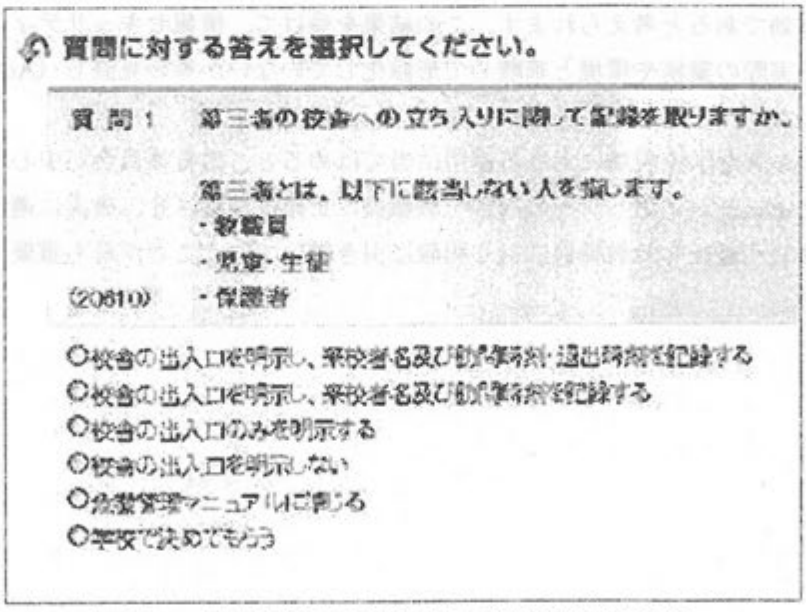
そして、情報セキュリティポリシーの有効性を定期的に確認するため、リスク分析や自己点検、情報セキュリティ監査を定期的に受けることも情報セキュリティを確保する上で有効であると考えられます。この結果を受けて、情報セキュリティポリシーの要求事項が実際の業務や環境と乖離して形骸化していないか等の見直し（Action）を行うことにつながると考えられます。

このことを学校現場における運用に当てはめると、教育委員会が中心となり策定した情報セキュリティポリシーの内容を教職員に正確に理解させ、確実に遵守させるとともに、新しく赴任した教職員に対し明確に引き継いでいくことが最も重要であると考えられます。

自発的にセキュリティポリシー作成を促す場の提供(和歌山市) 事例 2-3-1

学校の教職員に対し自らセキュリティについて考える機会を与えるために、セキュリティポリシーの作成支援ソフトを導入して、それぞれの学校で情報セキュリティポリシーを作成できるようにしています。(平成 24 年度に市内のすべての中学校で作成済み、平成 25・26 年度に市内のすべての小学校で作成予定)

基本方針や対策基準等の原則部分は教育委員会が作成しますが、情報資産台帳は各学校の実情に応じて作成できるようにしており、自校において本当に重要な情報は何か、その情報をどうすれば守れるかを、現場の先生同士が真剣に考えながら「実施手順」を作成できるようにしました。具体的には、学校が管理する情報をおびやかす様々な脅威に対しどのような対策を行うべきか、表示された質問に対して複数の選択肢から選んでいく形で作業を進めます。どの対策が自校にとって望ましいか、画面に表示されるヒントを参考に選択していき、そこで選んだ内容に基づいて、最終的に情報セキュリティポリシーの「基本方針/対策基準」「実施手順」が自動作成される仕組みとなっています。情報セキュリティポリシーを全く白紙の状態から作成するのは難しいですが、質問に答えていくだけでポリシーを作成することが可能なため、専門的な知識を持たない学校の教職員でも簡単に作業を行えるとともに、自ら重要な情報を守るためには何をすべきかを考える場となっています。



図表 18 質問形式にて「実施手順」で作成する画面の例

ハンドブックの作成による普及啓発活動の実施(大分県)

事例 2-3-2

学校現場での教職員による情報資産の取扱いは、「実施手順」に定められた内容に従って実施しますが、「実施手順」は分量があり、教職員が気軽に読めるものではないことから、「実施手順」の中で特に重要で、日常の業務で参照することが多い項目をコンパクトに整理した冊子として、「学校情報セキュリティハンドブック」を作成しました。ハンドブックは「実施手順」の 1/3 程度のページ数で、携帯しやすい B5 版の冊子としており、情報セキュリティチェックシートを付ける等、現場の職員が情報セキュリティについて疑問が生じた場合に手軽に参照できるものにしています。また、イントラネット上のサーバからダウンロードできるようにして、手軽に使えるように利便性にも配慮しています。

図表 19 情報セキュリティハンドブックの表紙

教員の意識に働きかける情報セキュリティポリシーの作成（仙台市）

事例 2-3-3

事故防止を目的とした「ルール」を定めても、その必要性が理解され、教員一人一人の気持ちに変化が生じなければ実効性が薄いものとなってしまいます。

仙台市では「適切な情報管理が実現されるように」という願いのもと「仙台市立学校における個人情報の管理に関する指針（情報管理指針）」を定めています。セキュリティポリシーを堅い条文で記すのではなく、「わかりやすさ」を大切にしているのが特徴です。

まず、基本方針では、項目を絞って宣言文形式で表すことにより、「何を大切にするのか」「実行するのか」を一般の教員にもわかりやすく示しています。

また、文意のわかりにくさや手続きの煩わしさが先に立ってしまいがちな実施手順の部分では、情報資産の具体的な活用場面を取り上げ、場面毎に「注意すべきポイント」「管理・運用上の注意点」「活用の流れ」を解説するスタイルで記述しています。

さらに、50 頁以上に及ぶ情報管理指針の内容をコンパクトにまとめたリーフレットも配布するなど、セキュリティ意識に働きかけることを大切にしています。

単にルールを定めるだけでなく、セキュリティポリシーに研修資料としての性格も持たせ、教員一人ひとりの意識変革を促すようにしているのが工夫点と言えます。

図表 20　情報管理指針の表紙とリーフレット

2.4. 参考資料

・情報セキュリティ基本方針（P28～P31）
・情報セキュリティ対策基準の例文（P32～P63）
（総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」
http://www.soumu.go.jp/denshijiti/jyouhou_policy/ ）

情報セキュリティ基本方針

情報セキュリティ基本方針

1 目的

本基本方針は、本市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、本市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・消去等

（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）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

（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

職員、非常勤職員及び臨時職員（以下「職員等」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

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（2）情報資産の分類と管理

本市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市の行政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。

情報セキュリティ対策基準の例文

3.1. 対象範囲

（1）行政機関の範囲

本対策基準が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

（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

3.2. 組織体制

（1）最高情報統括責任者

①副市長を、最高情報統括責任者とする。最高情報統括責任者は、本市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最高情報統括責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家をアドバイザーとして置くものとする。【推奨事項】

（2）統括情報セキュリティ責任者

①情報政策担当部長を、最高情報統括責任者直属の統括情報セキュリティ責任者とする。統括情報セキュリティ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統括情報セキュリティ責任者は、本市の全てのネットワークにおける開発、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統括情報セキュリティ責任者は、本市の全てのネットワーク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統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理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統括情報セキュリティ責任者は、本市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統括情報セキュリティ責任者は、本市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統括情報セキュリティ責任者は、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、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、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。

（3）情報セキュリティ責任者

①内部部局の長、行政委員会事務局の長、消防長及び地方公営企業の局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、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、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職員等（職員、非常勤職員及び臨時職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

（4）情報セキュリティ管理者

①内部部局の課室長、内部部局の出張所等出先機関の長、行政委員会事務局の課室長、消防本部の課室長及び地方公営企業の課室長を、情報セキュリティ管理者とする。

②情報セキュリティ管理者はその所管する課室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情報セキュリティ管理者は、その所掌する課室等において、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、統括情報セキュリティ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。

（5）情報システム管理者

①各情報システムの担当課室長等を、当該情報システムに関する情報システム管理者とする。

②情報システム管理者は、所管する情報システムにおける開発、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情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

④情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（6）情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を、情報システム担当者とする。

（7）情報セキュリティ委員会

①本市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情報セキュリティ委員会は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。【推奨事項】

（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。

3.3. 情報資産の分類と管理方法

（1）情報資産の分類

本市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３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・私物パソコンでの作業禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の外部記録媒体等の持ち込み禁止 ・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 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・外部記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

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	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政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	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・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	行政事務で取り扱う情報資産のうち、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、住民の権利が侵害される、又は行政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	・バックアップ、指定する時間以内の復旧 ・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の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）庁内の者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）庁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、情報セキュリティ管理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又は情報システム管理者は、情報資産の分類に従って、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又は情報システム管理者は、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、書込禁止の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又は情報システム管理者は、利用頻度が低い外部記録媒体や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。【推奨事項】

（エ）情報セキュリティ管理者又は情報システム管理者は、機密性２以上、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。

⑦情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又は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以上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以上の情報資産を運搬する者は、情報セキュリティ管理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以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（イ）機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

（ウ）情報セキュリティ管理者は、住民に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以上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、情報セキュリティ管理者の許可を得なければならない。

3.4. 物理的セキュリティ

3.4.1. サーバ等の管理

（１）機器の取付け

情報システム管理者は、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

①情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。【推奨事項】

②情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。【推奨事項】

（３）機器の電源

①情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、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。

②情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、

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

①統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、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。

②統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から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。

③統括情報セキュリティ責任者及び情報システム管理者は、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。

④統括情報セキュリティ責任者、情報システム管理者は、自ら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以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

（5）機器の定期保守及び修理

①情報システム管理者は、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。

②情報システム管理者は、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、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、情報システム管理者は、外部の業者に故障を修理させるに当たり、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

統括情報セキュリティ責任者及び情報システム管理者は、庁舎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

情報システム管理者は、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。

3.4.2. 管理区域（情報システム室等）の管理

（1）管理区域の構造等

①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」いう。）や電磁的記録媒体の保管庫をいう。

②統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は１階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。【推奨事項】

③統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、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。

④統括情報セキュリティ責任者及び情報システム管理者は、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。

⑤統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部をすべて塞がなければならない。【推奨事項】

⑥統括情報セキュリティ責任者及び情報システム管理者は、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

①情報システム管理者は、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。

②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。

③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、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。【推奨事項】

④情報システム管理者は、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。【推奨事項】

（3）機器等の搬入出

①情報システム管理者は、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。

②情報システム管理者は、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。

3.4.3. 通信回線及び通信回線装置の管理

①統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、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統括情報セキュリティ責任者は、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統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

④統括情報セキュリティ責任者は、機密性２以上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。

⑤統括情報セキュリティ責任者は、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。

3.4.4. 職員等のパソコン等の管理

①情報システム管理者は、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情報システム管理者は、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情報システム管理者は、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。【推奨事項】

④情報システム管理者は、パスワード以外に指紋認証等の生体認証を併用しなければならない。【推奨事項】

⑤情報システム管理者は、パソコン等の端末のディスクデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。【推奨事項】

3.5. 人的セキュリティ

3.5.1. 職員等の遵守事項

（1）職員等の遵守事項

①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に相談し、指示を仰がなければならない。

②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。

③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

（ア）最高情報統括責任者は、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における安全管理措置を定めなければならない。

（イ）職員等は、本市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、情報セキュリティ管理者の許可を得なければならない。

（ウ）職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

（エ）職員等は、外部で情報処理作業を行う際、私物パソコンを用いる場合には、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性３の情報資産については、私物パソコンによる情報処理を行ってはならない。

④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庁舎内に持ち込んではならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て、これらを持ち込むことができる。

⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、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。

⑥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セキュリティ管理者の許可なく変更してはならない。

⑦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管理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。

⑧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）非常勤及び臨時職員への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び臨時職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び臨時職員にパソコン等の端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（3）情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（4）外部委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

3.5.2. 研修・訓練

（1）情報セキュリティに関する研修・訓練

最高情報統括責任者は、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

①最高情報統括責任者は、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。

②研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。【推奨事項】

③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。

④研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤最高情報統括責任者は、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

最高情報統括責任者は、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。

3.5.3. 事故、欠陥等の報告

（１）庁内からの事故等の報告

①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に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③情報セキュリティ管理者は、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。

（２）住民等外部からの事故等の報告

①職員等は、本市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に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③情報セキュリティ管理者は、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。

④最高情報統括責任者は、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るための窓口を設置し、当該窓口への連絡手段を公表しなければならない。【推奨事項】

（3）事故等の分析・記録等

統括情報セキュリティ責任者は、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。

3.5.4. ID及びパスワード等の管理

（1）ICカード等の取扱い

①職員等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。

（ア）認証に用いるICカード等を、職員等間で共有してはならない。

（イ）業務上必要のないときは、ICカード等をカードリーダ若しくはパソコン等の端末のスロット等から抜いておかなければならない。

（ウ）ICカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、ICカード等の紛失等の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、ICカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（2）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。

①自己が利用しているIDは、他人に利用させてはならない。

②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。

（3）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。

①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。

②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。

③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。
④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。
⑤パスワードは定期的に、又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。
⑥複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑦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。
⑧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。
⑨職員等間でパスワードを共有してはならない。

3.6. 技術的セキュリティ

3.6.1. 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

①情報システム管理者は、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。
②情報システム管理者は、文書サーバを課室等の単位で構成し、職員等が他課室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。
③情報システム管理者は、住民の個人情報、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、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、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

統括情報セキュリティ責任者及び情報システム管理者は、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

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ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。

（4）システム管理記録及び作業の確認

①情報システム管理者は、所管する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。
②統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、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。

③統括情報セキュリティ責任者、情報システム管理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

統括情報セキュリティ責任者及び情報システム管理者は、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が閲覧したり、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

①統括情報セキュリティ責任者及び情報システム管理者は、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。

②統括情報セキュリティ責任者及び情報システム管理者は、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。

③統括情報セキュリティ責任者及び情報システム管理者は、システムから自動出力したアクセス記録等について、必要に応じ、外部記録媒体にバックアップしなければならない。【推奨事項】

（7）障害記録

統括情報セキュリティ責任者及び情報システム管理者は、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

①統括情報セキュリティ責任者は、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。

②統括情報セキュリティ責任者は、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、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、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に分離する等の措置を講じなければならない。

（１０）外部ネットワークとの接続制限等

①情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、最高情報統括責任者及び統括情報セキュリティ責任者の許可を得なければならない。

②情報システム管理者は、接続しようとする外部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詳細に調査し、庁内のすべてのネットワーク、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しなければならない。

③情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁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。

⑤情報システム管理者は、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、統括情報セキュリティ責任者の判断に従い、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。

（１１）無線 LAN 及びネットワークの盗聴対策

①統括情報セキュリティ責任者は、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。

②統括情報セキュリティ責任者は、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。【推奨事項】

（１２）電子メールのセキュリティ管理

①統括情報セキュリティ責任者は、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。

②統括情報セキュリティ責任者は、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。

③統括情報セキュリティ責任者は、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。

④統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、委託先

との間で利用方法を取り決めなければならない。

⑥統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように、添付ファイルの監視等によりシステム上措置しなければならない。【推奨事項】

（１３）電子メールの利用制限

①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。

②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。

③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。

④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に報告しなければならない。

⑤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。

（１４）電子署名・暗号化

①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、最高情報統括責任者が定めた電子署名、暗号化又はパスワード設定の方法を使用して、送信しなければならない。

②職員等は、暗号化を行う場合に最高情報統括責任者が定める以外の方法を用いてはならない。また、最高情報統括責任者が定めた方法で暗号のための鍵を管理しなければならない。

（１５）無許可ソフトウェアの導入等の禁止

①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。

②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、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、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③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。

（１６）機器構成の変更の制限

①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。

②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、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

（１７）無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可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。

（１８）業務以外の目的でのウェブ閲覧の禁止

①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。

②統括情報セキュリティ責任者は、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に通知し適切な措置を求めなければならない。

3.6.2. アクセス制御

（１）アクセス制御

①アクセス制御

統括情報セキュリティ責任者又は情報システム管理者は、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に、システム上制限しなければならない。

②利用者 ID の取扱い

（ア）統括情報セキュリティ責任者及び情報システム管理者は、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。

（イ）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、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

（ウ）統括情報セキュリティ責任者及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

③特権を付与された ID の管理等

（ア）統括情報セキュリティ責任者及び情報システム管理者は、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。

（イ）統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、最高情報統括責任者が認めた者でなければならない。

（ウ）最高情報統括責任者は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

（エ）統括情報セキュリティ責任者及び情報システム管理者は、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。

（オ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたID及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（2）職員等による外部からのアクセス等の制限

①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、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

②統括情報セキュリティ責任者は、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。

③統括情報セキュリティ責任者は、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。

④統括情報セキュリティ責任者は、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。

⑤統括情報セキュリティ責任者及び情報システム管理者は、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。

⑥職員等は、持ち込んだ又は外部から持ち帰ったパソコン等の端末を庁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、パッチの適用状況等を確認しなければならない。

（3）自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。【推奨事項】

（4）ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。【推奨事項】

（5）パスワードに関する情報の管理

①統括情報セキュリティ責任者又は情報システム管理者は、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。

②統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

（6）特権による接続時間の制限

情報システム管理者は、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。

3.6.3. システム開発、導入、保守等

（1）情報システムの調達

①統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、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。

②統括情報セキュリティ責任者及び情報システム管理者は、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）情報システムの開発

①システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。

②システム開発における責任者、作業者のＩＤの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（イ）情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

（イ）情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。【推奨事項】

（3）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。【推奨事項】

（イ）情報システム管理者は、システム開発・保守及び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・保守計画の策定時に手順を明確にしなければならない。

（ウ）情報システム管理者は、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。

②テスト

（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ）情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ）情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（4）システム開発・保守に関連する資料等の保管

①情報システム管理者は、システム開発・保守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。

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（5）情報システムにおける入出力データの正確性の確保

①情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（6）情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（7）開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、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。

（8）システム更新又は統合時の検証等

情報システム管理者は、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。

3.6.4. 不正プログラム対策

（1）統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、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。

①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。

②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。

③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。

④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。

⑤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。

⑥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。

（2）情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

①情報システム管理者は、その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システムに常駐させなければならない。

②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。

③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。

④インターネットに接続していないシステムにおいて、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、市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。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策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しなければならない。

（3）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。

①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。

②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。

③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。

④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。

⑤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。

⑥統括情報セキュリティ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。

⑦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。

（4）専門家の支援体制

統括情報セキュリティ責任者は、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。【推奨事項】

3.6.5. 不正アクセス対策

（1）統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポートを閉鎖しなければならない。

②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に、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定

しなければならない。

③重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。【推奨事項】

（2）攻撃の予告

最高情報統括責任者及び統括情報セキュリティ責任者は、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統括情報セキュリティ責任者は、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

統括情報セキュリティ責任者及び情報システム管理者は、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庁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

統括情報セキュリティ責任者及び情報システム管理者は、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に通知し、適切な処置を求めなければならない。

3.6.6. 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

統括情報セキュリティ責任者及び情報システム管理者は、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

統括情報セキュリティ責任者は、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

統括情報セキュリティ責任者及び情報システム管理者は、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。

3.7. 運用

3.7.1. 情報システムの監視

①統括情報セキュリティ責任者及び情報システム管理者は、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統括情報セキュリティ責任者及び情報システム管理者は、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を講じなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

3.7.2. 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

①情報セキュリティ責任者及び情報セキュリティ管理者は、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統括情報セキュリティ責任者に報告しなければならない。

②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。

③統括情報セキュリティ責任者及び情報システム管理者は、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

①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、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

②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統括情報

セキュリティ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。

3.7.3 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。

①関係者の連絡先

②発生した事案に係る報告すべき事項

③発生した事案への対応措置

④再発防止措置の策定

（3）業務継続計画との整合性確保

本市が自然災害、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。

3.7.4. 外部委託

（1）外部委託先の選定基準

①情報セキュリティ管理者は、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情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。【推奨事項】

（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。

・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
・委託先の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・従業員に対する教育の実施
・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
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による事故時等の公表
・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

情報セキュリティ管理者は、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。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度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。

3.7.5. 例外措置

（1）例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、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、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、最高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、事後速やかに最高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、例外措置の申請書及び審査結果を適切に保管しなければならない。

3.7.6. 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、次の法令のほか関係法令を遵守し、これに従わなければならない。

①地方公務員法（昭和二十五年十二月十三日法律第二百六十一号）

②著作権法（昭和四十五年法律第四十八号）

③不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）

④個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）

⑤○○市個人情報保護条例（平成○○年条例第○○号）

3.7.7. 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、地方公務員法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。

①統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者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に通知し、適切な措置を求めなければならない。

②情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び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に通知し、適切な措置を求めなければならない。

③情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、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、統括情報セキュリティ責任者は、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室等の情報セキュリティ管理者に通知しなければならない。

3.8. 評価・見直し

3.8.1. 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

①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。

②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

①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。

②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定期的に又は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管理者に対し、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管理者に対しても、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。

3.8.2. 自己点検

（1）実施方法

①統括情報セキュリティ責任者及び情報システム管理者は、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。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局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

統括情報セキュリティ責任者、情報システム管理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

①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。

②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。

3.8.3. 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。