平成 27 年度　行政監査結果報告

情報セキュリティについて

監　査　報　告　第　２　号

平成２８年３月１６日

行　政　監　査　結　果　報　告

神戸市監査委員	谷　口　時　寛
同	吉　田　基　毅
同	むらの　誠　一
同	藤　本　浩　二

地方自治法第 199 条第 2 項の規定に基づき実施した平成 27 年度行政監査について，同条第 9 項の規定によりその結果に関する報告を次のとおり決定した。

Ⅰ　監査の概要

第１　監査の対象

１　監査のテーマ

情報セキュリティについて

２　選定理由

近年，事務処理におけるコンピュータやネットワークを利用した情報システムの活用は欠かせないものであるが，そのトラブルは，組織内部にとどまらず，市民に多大な影響を及ぼす。特に神戸市（以下「本市」という。）をはじめ地方自治体の事務処理では，大量の個人情報を処理するため，不正アクセス又は職員や委託業者による情報漏洩等により大量の個人情報が外部に流出する危険性がある。

平成 27 年 5 月に，日本年金機構における外部からのウイルスメールによる不正アクセスによって，大量の個人情報が流出するという事件（参考１　参照）が発生した。この事件における個人情報の取扱いに関する問題点は，①電子メールの添付ファイルを安易に開封した，②個人情報が記録されたデータファイルにパスワードを設定していなかった，③基幹系システムのデータを情報系システム上で取り扱っていた，などといわれている。

また，行政手続における特定の個人を識別するための番号の利用等に関する法律（いわゆるマイナンバー法）が平成 27 年 10 月に施行されたことに伴い，平成 28 年 1 月から国の行政機関や地方自治体における税・社会保障・災害対策の３分野での個人番号の利用が開始され，順次，その利用方法も拡大される計画であることから，一層の情報セキュリティ対策の維持・向上が重要である。

このような状況のなか，本市の個人情報を処理する業務系システム及び情報系ネットワークシステムについて，神戸市情報セキュリティ基本方針及び神戸市情報セキュリティ対策基準等に照らして，情報セキュリティを維持・管理する仕組みが適切に整

備・運用されているか，特に業務系システムの個人情報の一部を編集加工して他のシステムで利用する場合の運用が適切であるかを検証し，情報セキュリティ対策の維持・向上を図ることを目的として，監査を実施する。

3　監査対象部局

全ての局区室

第２　監査の期間

平成 27 年 8 月 19 日から平成 28 年 3 月 16 日

第３　監査の方法

1　事前調査

企画調整局情報化推進部から情報システム台帳を入手し，このうち個人情報を処理している全ての業務系情報システム及びこのシステムを運用している所属の情報系ネットワークシステムを監査対象システムとして特定した。

対象局区室別の対象システム数及び主なシステム名は，第１表のとおりである。

監査対象システムのシステム管理者及び区役所・市税事務所のシステムの整備・運用状況等を関係書類等により把握した。

第１表　監査対象システムの局区室別内訳

対象局区室	対象システム数	主なシステム名	
		基幹業務系	その他
危機管理室	1	－	自動通報装置
企画調整局	29	財務会計，共通基盤 老人保健福祉医療，介護保険，国民健康保険 税務，住民基本台帳ネットワーク，選挙	ＰＣ統合管理，文書管理・電子決裁 新財務会計 公的個人認証
行財政局	19	新税収滞納	庶務事務，公有財産管理
市民参画推進局	18	新住民記録，戸籍，諸証明自動交付	パイオネット，情報ﾗｲﾌﾞﾗﾘｰ図書管理
保健福祉局	44	福祉情報，生活保護，介護保険認定管理 精神保健福祉手帳	災害援護資金貸付償還事務，後期高齢者医療 墓園管理，学務（看護大）
こども家庭局	10	児童相談	私立幼稚園就学援助助成，母子保健情報
環境局	13	－	大型ごみ受付，資源集団回収活動助成
産業振興局	4		農業共済ﾈｯﾄﾜｰｸ化情報，ものづくり復興工場使用料
建設局	17	道路占用料調定収納	下水道事業財務会計，排水設備台帳
住宅都市局	10	新市営住宅総合管理	耐震診断台帳
みなと総局	4	－	港湾EDIｼｽﾃﾑ運営，ﾗﾝﾊﾟｽ発行，ｽﾎﾟｯﾄ管理
区役所	2	－	市民課（垂水）
消防局	3	－	非常伝達，防災情報
水道局	4	－	営業ｵﾝﾗｲﾝ，開閉栓等受付，給水設計台帳管理
交通局	7	－	ﾄﾞﾗｲﾌﾞﾚｺｰﾀﾞ，地下鉄駅防犯対策
教育委員会事務局	18	同和奨学金	準公費会計事務支援，就学援助，図書館情報ﾈｯﾄﾜｰｸ
選挙管理委員会	2	期日前不在者投票	裁判員制度用名簿調整支援
農業委員会	1	－	農地基本台帳
市会事務局	4	－	市会会議録検索，市会図書室総合管理
合計	210		

2　実地調査

事前調査に基づき，182 システムの管理者及び区役所・市税事務所の 83 所属において，関係書類の審査，関係職員への質問等の方法により，各システムの情報セキュリティ対策及びその運用状況を調査した。

第４　監査の項目

監査項目，着眼点並びに実施方法は，下表のとおりである。

監査項目	着眼点	実施方法
1. 情報セキュリティの仕組み (1)情報資産の管理 ①情報資産の管理方法	①機密性 3 の情報資産（個人情報に関するデータ等）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っているか。	関係職員への質問 等により検証
(2)物理的セキュリティ ①サーバ等の管理	①情報基盤管理者及び業務システム管理者は，重要性（機密性，完全性，可用性）分類 3 のデータが記録されている電子記録媒体及びコンピュータ設置場所の入退出について，適切な管理を行っているか。	情報資産管理台帳 入退室管理簿 等により検証
②端末等の管理	①情報基盤管理者及び業務システム管理者は，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ているか。	関係職員への質問 等により検証
(3)人的セキュリティ ①職員等の責務 （データの取扱）	①職員等は，使用する端末に，コンピュータウイルス等対策ソフトウェアを常駐させ，定義ファイルを常に最新のものにしているか。 ②職員等がパソコン等の端末，USB 等の記録媒体などの情報資産を外部に持ち出す場合，情報管理者等の許可を得ているか。	抽出した端末の定義ファイル更新日 抽出した端末を使用する職員への質問 端末等持出・持込申請書/承認書 等により検証
②アクセスのための認証情報及びパスワードの管理	①職員等は，ID カード，ID，パスワードを適切に管理しているか。	抽出した端末を使用する職員への質問 等により検証
③外部委託に関する管理	①情報システムの運用，保守等を外部委託する場合，当該委託事業者との間で，必要	委託契約書，報告書 等により検証

	な事項を明記した契約を締結しているか。締結される契約書に，必要に応じた情報セキュリティ要件が明記されているか。 ②情報基盤管理者及び業務システム管理者は，当該委託先事業者の情報セキュリティ確保への取組みの実施状況等について，定期的若しくは随時，調査を行っているか。	
(4)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情報基盤管理者及び業務システム管理者は，アクセス記録の取得，情報資産のバックアップなどを適切に行っているか。	関係職員への質問 等により検証
②アクセス制御	①情報基盤管理者及び業務システム管理者は，利用者の識別及び認証，利用者登録，特権管理，外部からのアクセス，内部ネットワーク間の接続，外部ネットワークとの接続などを，適切に行っているか。	利用者の登録・変更・抹消に関する記録， 関係職員への質問 等により検証
③コンピュータウイルス等不正プログラム対策	①情報基盤管理者，業務システム管理者及び情報セキュリティ管理者は，所管するサーバ及び端末に，コンピュータウイルス等対策ソフトウェアを常駐させ，定義ファイルを常に最新のものにしているか。	定義ファイル更新日 等により検証
④不正アクセス対策	①情報基盤管理者及び業務システム管理者は，内部からの不正アクセスの監視等を適切に行っているか。	関係職員への質問 等により検証
(5)運用 ①情報システムの監視	①情報基盤管理者及び業務システム管理者は外部と接続するシステムを稼働中，常時監視しているか。	関係職員への質問 等により検証
②緊急時の対応	①情報基盤管理者及び業務システム管理者は，緊急時対応計画を策定しているか。	緊急時対応計画 を検証
2. 業務系システム個人情報の二次利用	業務系システムの個人情報の一部を編集加工して他のシステムで利用する場合の運用が適切であるか。	関係職員への質問 等により検証

※下線部は，日本年金機構の事件を踏まえ，重点的に監査する事項

Ⅱ　監査の結果

監査の結果，事務処理はおおむね適正に行われているものと認められた。

しかし，事務の一部について改善を要する事例があったので，今後，適正な事務処理に努められたい。

特に，情報セキュリティの確保と情報資産の活用を図るため，情報系ネットワーク上の外部記憶装置（NAS：Network Attached Storage，以下「NAS」という。）を利用してデータの保存，活用する場合のセキュリティ対策の徹底を図るとともに，情報セキュリティ侵害が発生した場合又は侵害の恐れがある場合の組織全体の適切な初動対応を確保するため，情報セキュリティ責任者（企画調整局情報化推進部長）のリーダーシップの下，迅速に組織全体で対応（連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置）する仕組みを強化することを検討されたい。

１　監査項目に係る事業の調査結果

本市の情報セキュリティ対策について，（１）情報システムに係る動向，（２）情報セキュリティ対策の仕組み，（３）情報セキュリティ対策の運用状況について，調査・検証を行った結果は，次のとおりである。

なお，セキュリティへの脅威とセキュリティ対策については参考５，情報セキュリティに関連する専門的用語については参考６を参照されたい。

（１）情報システムに係る動向

①情報システムネットワーク

本市では，昭和 61 年に住民記録オンラインシステムを導入し，順次，税務，印鑑，国民健康保険などの庁内事務のオンライン化に取り組むとともに，平成６年に市のホームページを開設し，平成９年には庁内インターネット・イントラネットの運用を開始するなど，情報通信技術の発達やインターネットの普及など社会を取り巻く情報通信環境の変化に対応した情報化を進めてきた。

特に電子市役所の実現においては，システムの信頼性やセキュリティの確保に留意した上で，内部事務処理の効率化を図るとともに，より質の高い市民サービスを提供している。

本市の情報システムネットワークは，主に住民情報など機密情報を取り扱うシステム群を配置した「基幹業務系ネットワーク」と，電子自治体のバックオフィス基盤として，事務効率化や情報共有を目的としたシステム群を配置した「情報系ネットワーク」の２つのネットワークで構成されている。なお，基幹業務系ネットワークは，取り扱う情報の特性上，原則，他のネットワークと接続しない「クローズされたネットワーク」であり，インターネットには情報系ネットワークのみが接続されている。

ネットワーク概念図は第１図のとおりである。

（ア）基幹業務系ネットワーク

基幹業務系ネットワークは，住民基本台帳，税，国民健康保険，介護保険，福祉情報等の大量の個人情報を利用するための汎用機及び窓口用端末等が接続するネットワークである。

（イ）情報系ネットワーク（イントラネット）

情報系ネットワークは，統合管理された事務処理用パソコン（文書作成，表計算，データベース管理用等の市販のソフトウェアを標準装備）（以下「事務処理用 PC」という。）が接続され，職員ポータルシステム，文書管理・電子決裁システム，財務会計システム，メールシステム等が構築されている。

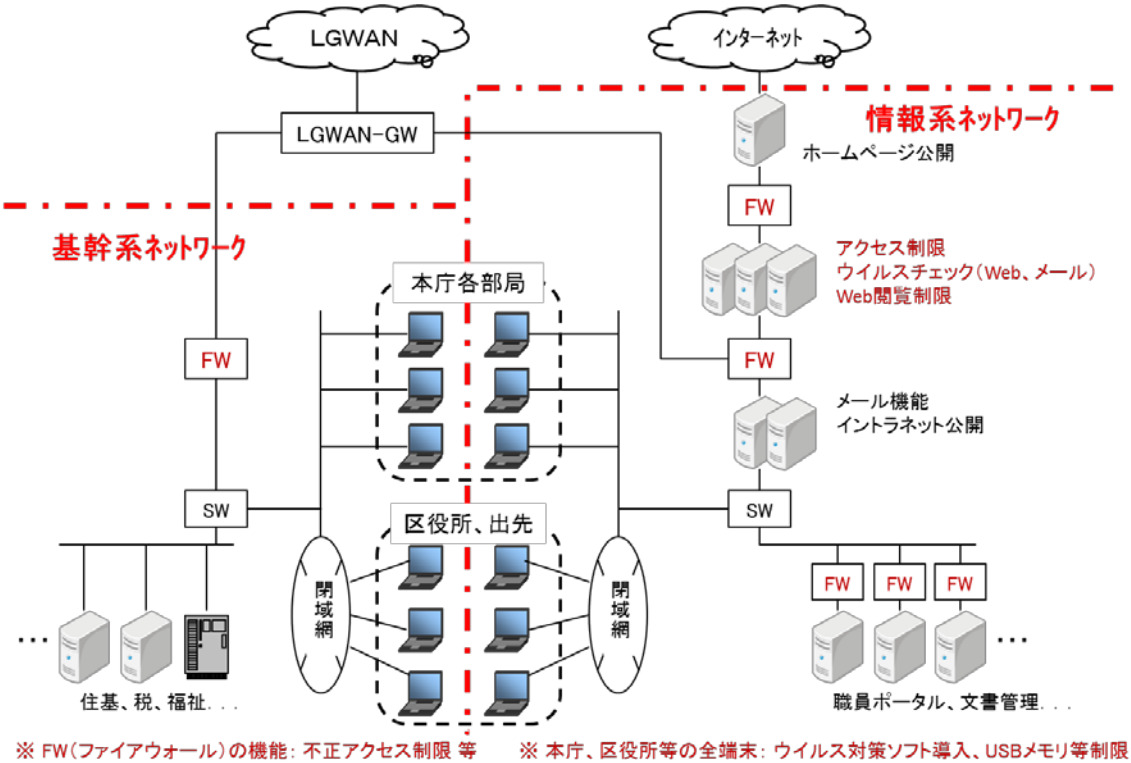
情報系ネットワークは「本庁」を中心に「区役所・支所・出張所・連絡所」（25 か所），「その他拠点」（約 200 か所）が WAN（Wide Area Network：広域通信網）で接続されている。

また，インターネット，総合行政ネットワーク（以下「LGWAN」という。），その他専用システムと接続されており，複数のシステムで独自のセグメントを構築している。

（ウ）業務系ネットワーク

(ア)(イ)以外の独立したネットワークで，神戸教育情報ネットワーク（KIIF）等の独自ネットワークシステムやスタンドアロン（端末単体）のシステム等が構築されている。

第１図　神戸市ネットワーク概念図



②情報化推進方針

近年のコンピュータやネットワークを利用して大量の個人情報が扱われている状況の中では，国や自治体等の公的機関，事業者における個人情報の保護とセキュリティの確保に万全を期していく必要がある。

このため，本市では，平成 15 年 1 月，情報システムに関する情報セキュリティ水準の向上や職員の意識向上を目的に「神戸市情報セキュリティ基本方針」（以下，「基本方針」という。参考２　参照）を制定し，平成 17 年 6 月には「物理的」「人的」「技術的」「運用面」の４つの観点から構成される「神戸市情報セキュリティ対策基準」（以下，「対策基準」という。参考３　参照）を制定した。この基本方針と対策基準を「神戸市情報セキュリティポリシー」（以下，「情報セキュリティポリシー」という。）として扱い，マネジメントシステム及び対策を運用している。

また，情報セキュリティの目標を設定し，情報環境の変化に迅速に対応できる実効性のある情報セキュリティ対策を，策定・導入（Plan）・運用（Do）・評価（Check）・見直し（Action）の PDCA サイクルで実施し，マネジメントシステムを確立することで，より一層のセキュリティ水準の向上を図っている。

以上の方針のもと，平成 18 年 11 月に「神戸市情報化推進方針」として，次の３点に取り組むことを市長が宣言し，全庁的に取組を進めている。

ア）情報システムの導入・開発及び運用にあたっては，関係法令をはじめ，神戸市個人情報保護条例，コンプライアンス条例，神戸市情報セキュリティポリシー等を遵守するとともに，手続きの明確化と透明性を確保し，システム全体にわたって効率的に行う。

イ）情報セキュリティ対策を適切に実施するために，役割と責任を明確にした全庁的な体制を構築し，必要な啓発・研修を定期的に行うとともに，事故等が発生した場合の緊急的対応計画を定め，速やかに対処する。

ウ）情報システムの運営状況や情報セキュリティ対策の実施状況について定期的・継続的にモニタリングを行い，対策の有効性を点検し，監査することにより，改善に努める。

③マイナンバー法等への対応

マイナンバー制度（社会保障・税番号制度）のもと，平成 27 年 10 月から住民票を有する者全員にマイナンバーが通知され，全国で平成 28 年 1 月からマイナンバーカード（個人番号カード）の交付が開始された。

国の行政機関や地方公共団体等が，特定個人情報ファイル（個人番号をその内容に含む個人情報ファイル）を保有しようとするときは，保有する前に，特定個人情報保護評価（PIA）を実施することを原則として義務付けられており，平成 28 年 2 月 1 日現在，31 件の特定個人情報保護評価を得ている。

また，マイナンバーカードを活用して，コンビニエンスストア（全国の約 48,000 店舗で利用可能）で，住民票の写し及び印鑑登録証明書の交付サービスが平成 28 年 1 月に開始された。さらに，平成 28 年 5 月頃に戸籍謄抄本（戸籍記録事項証明書）と戸籍の附票の写しの交付サービスも追加される予定であり，所得・課税証明書の発行（平成 29 年 3 月予定）の準備も進められている。なお，証明書コンビニ交付サービスが開始されたことに伴い，平成 28 年 2 月末で市内すべて（12 か所）の証明書自動交付機のサービスが終了された。

④ホストコンピュータからの移行

本市では，昭和 39 年に大型のホストコンピュータを導入して以降，現在に至るまで長年にわたり基幹系業務システムに利用しており，企画調整局情報化推進部（以下「情報化推進部」という。）が一元的に管理・運用してきた。

しかし，近年の情報通信技術の進展を踏まえ，平成 24 年の住民記録システムを皮切りに，オープンな技術を用いた小型のサーバシステムへの移行を順次進めており，平成 28 年度末にホストコンピュータを廃止する予定である。

ホストコンピュータシステムからクライアント・サーバ・システムへの移行後は，これまでの情報化推進部が一元的にホストコンピュータを管理・運用する体制ではなく，業務所管課がそれぞれ情報システムを管理・運用し，情報化推進部は基幹業務系ネットワーク回線を管理・運用する。

また，情報化推進部は，従来は情報システムの調達工程における支援が中心であったが，現在は開発工程における支援についても積極的に実施している。

（２）情報セキュリティ対策の仕組み

①個人情報保護審議会

本市では，「個人情報保護条例」（平成 9 年制定）や「電子計算機処理に係るデータ保護管理規程」（昭和 61 年制定）に基づき個人情報やデータの保護を図っている。

実施機関（市長，公営企業管理者，教育委員会等）は，新たに個人情報の電子計算機処理を行おうとするときは，個人情報の内容及び利用目的，システム概要，個人情報保護対策等について，あらかじめ個人情報保護審議会（以下「審議会」という。）の意見を聴かなければならない（個人情報保護条例第 11 条第 1 項）。

また，実施機関は，個人情報を取り扱う事務の目的以外の目的のために，個人情報を当該実施機関の内部において利用し，又は当該実施機関以外のものに提供してはならないが，例外として，法令等に規定があるとき，本人の同意があるとき等以外に，実施機関が審議会の意見を聴いて公益上特に必要があると認めるときは，実施機関の内部利用等が認められている（個人情報保護条例第 9 条第 1 項）。

なお，実施機関の職員又は職員であった者の人事，給与，服務，福利厚生その他これらに準ずる事項に関する個人情報については，新たに個人情報の電子計算機処理を行おうとするときは，個人情報保護条例第 11 条の規定は適用除外となり，審議会の意見は不要となる（個人情報保護条例第 35 条第 3 項）。

②情報セキュリティポリシー

基本方針と対策基準から成る情報セキュリティポリシーは，その下位規程類として個別対策基準や実施手順書も定めており，実態に合わせた効果的な取組の実行を図っている（情報セキュリティポリシー等の構成は第２表のとおり)。

これらの規程に基づくマネジメントシステムの運用の一環として，情報セキュリティポリシー自体も毎年度１回見直しを行い，必要に応じて改正している。

なお，基本方針は本市組織全体の共通方針であるが，教育委員会学校園（小学校・中学校・高等学校・高等専門学校・特別支援学校・幼稚園）及び市立看護大学における業務や組織の特殊性を考慮し，「神戸市情報セキュリティ対策基準（学校編)」（平成 23 年 4 月制定)，「神戸市情報セキュリティ対策基準（工業高等専門学校編)」（平成 23 年 6 月制定）及び「神戸市情報セキュリティ対策基準（看護大学編)」（平成 24 年 4 月制定）を順次別途制定し，より実効性のある管理体制を整えている。

第２表　神戸市情報セキュリティポリシー等の構成

１．神戸市情報セキュリティポリシー
(1)　神戸市情報セキュリティ基本方針(4.1版)
(2)　神戸市情報セキュリティ対策基準（4.4版）
２．個別対策基準
(1)　情報セキュリティに係る文書管理基準(1.2版)
(2)　監査・自己点検基準（2.0版）
(3)　研修・訓練基準（1.3版）
(4)　ソフトウェア資産管理基準(2.1版)
(5)　物理的・技術的セキュリティ管理基準(1.4版)
(6)　情報セキュリティ事件・事故等緊急時対応基準(1.0版)
３．情報セキュリティ実施手順
(1)　ソフトウェア資産管理手順書(2.0版)
(2)　情報漏えい等発生時の対応手順書(1.0版)
(3)　情報漏えい事件・事故報告書（速報用）
(4)　情報漏えい事件・事故報告書（最終報告用）

③情報セキュリティ管理体制

適切に情報セキュリティ対策を推進･管理するため,情報セキュリティポリシーに基づき，神戸市情報化推進体制の整備に関する要綱に定める情報化統括責任者（情報化の推進を所管する実施組織を担任する副市長）を情報セキュリティ最高責任者とし，対策基準において，第３表のとおり，必要な体制，役割，権限等を定めている。

第３表　情報セキュリティ管理体制

体　　制	役　　職	主な権限と責任
情報セキュリティ最高責任者	副市長	本市における全てのネットワーク，情報システム，データ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。
情報セキュリティ統括責任者	企画調整局長	情報セキュリティ最高責任者を補佐し，全ての情報資産における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。
情報セキュリティ責任者	企画調整局 情報化推進部長	情報セキュリティ統括責任者を補佐し，情報セキュリティ管理者，情報基盤管理者，基幹業務系ネットワーク管理者，情報系ネットワーク管理者，情報責任者，情報管理者，業務システム責任者，業務システム管理者，大型汎用機器管理者に対して，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。
情報セキュリティ管理者	企画調整局 ICT計画推進担当課長	情報セキュリティ統括責任者及び情報セキュリティ責任者を補佐し，その実務を担当する。
情報基盤管理者	企画調整局 電子市役所担当課長	共通的なネットワーク，情報システム，データ等の情報資産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。
基幹業務系ネットワーク管理者	企画調整局 基幹業務ｼｽﾃﾑ担当課長	共通的なネットワーク，情報システム，データ等の情報資産に関する情報基盤管理者の権限及び責任のうち，基幹業務系ネットワークに関する部分については情報基盤管理者と同等の権限及び責任を有する。
情報系ネットワーク管理者	企画調整局 電子市役所担当課長	共通的なネットワーク，情報システム，データ等の情報資産に関する情報基盤管理者の権限及び責任のうち，情報系ネットワークに関する部分については情報基盤管理者と同等の権限及び責任を有する。
情報責任者	局室区等の長	所管する局室区等における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。
情報管理者	情報資産を取り扱う課の長	所管課内におけるデータ等の情報資産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。
業務システム責任者	業務システムを所管する局室区等の情報責任者	当該業務システム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。
業務システム管理者	業務システムを所管する課の長	当該業務システム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。
大型汎用機器管理者	企画調整局 基幹業務ｼｽﾃﾑ担当課長	各業務システムに関する業務システム管理者の権限及び責任のうち，大型汎用機器に関する部分については業務システム管理者と同等の権限及び責任を有する。

④情報セキュリティ対策

基本方針では，情報資産に対する脅威から情報資産を保護するため，次の情報セキュリティ対策を講ずるものとし，対策基準において，情報セキュリティ対策等を実施するために，適用範囲における共通の基準としての具体的な遵守事項及び判断基準を定めている。なお，対策基準において監査の着眼点に関する主なセキュリティ対策は，参考３のとおりである。

（ア）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実施することとする。

（イ）物理的セキュリティ

コンピュータ設置場所への入退室，サーバ等の管理，通信回線及び端末等への物理的な対策を講じる。

（ウ）人的セキュリティ

情報セキュリティに関し，職員等情報取扱者が遵守すべき事項を定めるとともに，十分な研修・訓練及び啓発を実施するなど人的な対策を講じる。

（エ）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，コンピュータウイルス等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。

（オ）運用面のセキュリティ

情報システムに関し，情報セキュリティポリシーの遵守状況の確認等，情報セキュリティポリシーの運用面の対策を講じる。また，情報資産への侵害が発生した場合等に，迅速かつ適切に対応するため，緊急時対応計画を策定する。

⑤本市の情報資産

（ア）パソコンソフトウェアの管理

平成21年度に「ソフトウェア資産管理基準」,「ソフトウェア資産管理手順書」を策定し，「パソコンソフトウェア管理システム」を導入して，①設置，撤去など保有するパソコン（以下「PC」という。）の管理（ハードウェア台帳），②インストール先の変更など保有するPCとインストールされているソフトウェアの管理（インストール台帳），③購入，廃棄など保有するソフトウェアとライセンス数の管理（ライセンス台帳）を行っている。

台帳の正確性を担保するため，年１回の棚卸（各所属で現物と台帳の突合）を行うとともに，台帳間に齟齬があれば，日々，同システムより情報管理者（所属長）に通知して是正させる仕組みになっている。

平成27年3月末現在，ハードウェア台帳にPC等が16,697件(事務処理用PC：10,400件，専用システムPC：6,297件)，ライセンス台帳に有償ソフトが7,432件，インストール管理台帳に18,855件の登録がある。

（イ）情報システム台帳

平成21年度に，庁内に設置する全てのPC・サーバについて，情報セキュリティ対策の実施者とその実施内容を明確にするため，用途毎に情報システムコードを付与し，情報システムの概要，構成，管理情報やセキュリティ対策の状況等について台帳化している。

情報システム台帳に登録されているシステムは，平成26年7月に行った情報化推進部の照会の結果では，平成27年3月末現在，570システムであり（廃止されたものを除く），このうち個人情報を処理しているものは210システムであった。

登録された210システムの所管課に調査を実施したところ，システムの改廃があったにもかかわらず台帳データが更新されていなかったもの，システムが重複して登録されていたもの，個人情報を処理していなかったもの等があり，監査時点で実際に個人情報を処理していたものは182システムであった。

この182システムについて，使用する端末，使用するネットワーク，センシティブ情報の有無，特定個人情報の有無は，第４表のとおりである。

第４表　個人情報を処理するシステムの概要

使用する端末		使用するネットワーク		センシティブ情報		特定個人情報	
事務処理用	24	基幹系	44	有	71	有	20
専用端末	157	独自	50	無	111	無	162
併用	1	イントラ	22				
		外部	7				
		ｽﾀﾝﾄﾞｱﾛﾝ	54				
		その他	5				
計	182	計	182	計	182	計	182

各システムで使用する端末は，情報系ネットワークの事務処理用PCを使用しているシステムが24システム，事務処理用PCと専用PCを併用しているシステムが１システムであった。

各システムで使用するネットワークでは，基幹業務系ネットワークが44システム，独自ネットワーク（基幹系及び情報系以外で独自に構築したネットワーク）が50システム，外部ネットトーク（国・県など外部の機関が構築・管理しているネットワーク）が7システム，スタンドアロン（PC単体でネットワークに接続しないもの）が54システムあり，これらのシステムはいずれも情報系ネットワークから分離されているが，情報系ネットワークを使用するイントラは22システムであった。

センシティブ情報（個人情報保護条例第7条第3項に規定する内容が含まれているもの）を処理しているシステムは71システム，特定個人情報（マイナンバー制度における個人情報）を処理しているシステムは20システムであった。

（３）情報システムの運用状況

実地監査により確認した，個人情報を取り扱っている情報システムの運用状況は，次のとおりである。

①個人情報保護審議会

個人情報保護条例に基づき，システムの構築時及び再構築時，業務の目的以外の目的のために他システムに個人情報を提供する場合は，審議会の意見を聴かなければならないため，その運用状況について

・システムの構築時または再構築時に審議会に諮問しているか
・システムで処理する個人情報を他の業務での目的外利用又は提供する場合に審議会に諮問しているか

の観点から，審議会の諮問状況の確認を行った。

その結果は第５表のとおりであった。

なお，事務処理用 PC において標準搭載されているソフトウェアを利用して名簿等の作成管理することは審議会で類型承認されており諮問を要しないが，センシティブ情報が含まれる場合は個別に審議会の諮問が必要である。また，個人情報を含む電子データについては，暗証番号を設定する必要がある（個人情報保護審議会平成 20 年 12 月 10 日諮問時の情報化推進部作成資料，参考４　参照)。

第５表　個人情報保護審議会の諮問状況

		使用するネットワークの種類						合計
		基幹系	独自	イントラ	外部	スタンドアロン	その他	
システム数		44	50	22	7	54	5	182
システム構築時等	諮問　有	34	23	10	2	21	3	93
	諮問　無	0	5	3	0	9	1	18
	適用除外	10	22	9	5	24	1	71
他システムへの情報提供	提供　無	21	38	16	5	43	4	127
	提供　有	23	12	6	2	11	1	55
	諮問　有	16	7	2	0	3	0	28
	諮問　無	1	1	0	1	2	0	5
	適用除外	6	4	4	1	6	1	22

構築時または再構築時の諮問については，概ね適正に行われていたが，独自ネットワークの一部（こども家庭センターシステム，博物館内システムなど)，イントラネットの一部（ライオンズ奨学金システムなど）やスタンドアロンシステムの一部（特定不妊治療助成システムなど）で審議会への諮問が行われていなかった。

個人情報を他システムへ提供しているシステム数は 55 システムであった。このうち，法令の規定等により審議会への諮問が不要となるシステムが 22 システム，審議会に諮問していたシステム数は 28 システムであり，諮問していないシステムが 5 システム（同和奨学金システム，地域改善対策奨学金システムなど）あったが，目的外利用又は提供する場合にはあたらず，いずれもシステム所管課内で情報の共有を図るためのものであった。

②情報セキュリティ対策

審議会で承認されたセキュリティ対策等の運用状況について，

・PC 及びサーバのウイルス対策について，対策ソフトウェアの常駐，ウイルス定義ファイルの更新が適切か。また，その更新方法はどのように行っているのか。

・他システムへ個人情報を提供する際に，管理者の許可，記録簿の記載など適正な手続きをとっているのか。

・その他のセキュリティ対策の運用状況は適正か。

の観点から確認を行った。

特にデータ処理，システム保守・改修を外部委託する場合，委託契約書約款及び情報セキュリティ遵守特記事項が遵守されていること，情報資産の持ち出し管理が徹底しているかの確認も行った。

その結果は，第６表のとおりである。

第６表　セキュリティ対策の運用状況

		使用するネットワーク						計
		基幹系	独自	イントラ	外部	ｽﾀﾝﾄﾞｱﾛﾝ	その他	
システム数		44	50	22	7	54	5	182
PC・サーバのウイルス対策	適正	43	32	21	6	27	5	134
	一部不適	0	1	0	0	0	0	1
	不適	1	17	1	1	27	0	47
他システムへの情報提供	提供なし	21	34	16	5	42	4	122
	提供あり	23	16	6	2	12	1	60
	適正	22	16	6	2	12	1	59
	一部不適	1	0	0	0	0	0	1
	不適	0	0	0	0	0	0	0
その他のセキュリティ対策	適正	39	47	21	7	52	5	171
	一部不適	3	2	1	0	1	0	7
	不適	2	1	0	0	1	0	4

PC・サーバのウイルス対策について，独自ネットワークを使用するシステム及びスタンドアロンのシステムにおいて，インターネット等の外部のネットワークに接続しないことを理由に，ウイルス対策ソフトを常駐させていなかったり，定義ファイルを更新していないシステムが，それぞれ 17 システム，27 システムあった。

他システムへの情報提供については，60 システムにおいて情報提供している。生活保護版レセプト管理システムにおいて，所管課が管理する他システムへデータを提供する際の記録簿の記載が漏れている事例があったものの，その他のシステムでは，個人情報を提供する際には，管理者の許可，記録簿の記載など適正な手続きをとっていた。

その他のセキュリティ対策については，福祉情報システム（基幹系）及び生活保護システム（基幹系）において，区役所に設置するセグメントサーバが施錠可能な区画を設けずに執務区域に設置され，また，サーバをラック等に収納して容易に取り外せないよう固定が行われていない事例や，同和奨学金システム（基幹系）及び地域改善対策奨学金システム（スタ

ンドアロン）において，同システムから抽出した個人情報データを事務処理用 PC で編集加工して奨学生一覧等を作成し，NAS に保存して課内の関係職員で滞納整理事務等を行うために共有化していた事例等があったものの，ほとんどのシステムは適正な対策がとられていた。

③業務系システム個人情報の情報系ネットワークでの二次利用

（ア）二次利用の現状

業務分析及び管理のためのデータ整理，国等への業務報告，他システムへのデータ提供のための編集加工など，業務システムの個人情報の一部を情報系ネットワークに接続する事務処理用 PC に取り込んで二次利用する場合がある。

業務システムの個人情報を他システムに提供する場合には，提供課は電子記録媒体（CD-R，USB，DVD-R など）のファイルにパスワードを設定して受領課等に手渡さなければならないが，受領課が受け取った個人情報を編集加工しこのデータを保存する場合や，業務システムを運用管理する所属内で業務システムの個人情報を事務処理用 PC で保存する場合の現場でのルールの徹底が十分でない。

このため，システム管理者の所属における業務系システム個人情報の事務処理用 PC での二次利用の状況について，

・業務システムの個人情報や他のシステムから提供された個人情報を，事務処理用 PC で編集・加工することがあるか。
・編集加工した個人情報データを事務処理用 PC 又は情報系ネットワーク上の共有サーバ等に保存しているか。
・個人情報を含むファイルを保存する場合，パスワード設定などどのような保存方法を行っているか。

の観点から，その運用状況（事務処理用 PC の確認は各システムを管理する所属で 2 台抽出）について確認したところ，その結果は第 7 表のとおりであった。

第 7 表　業務系システム個人情報の情報系ネットワークでの二次利用（システム管理者）

	二次利用	データ保存	抽出したファイルのデータの保存方法	
無	153 システム	159 システム		
有	29 システム	23 システム	全てのファイルにパスワード設定又は暗号化あり	17
			全てのファイルにパスワード設定及び暗号化なし	4
			一部のファイルにパスワード設定及び暗号化とも無	2
計	182 システム	182 システム	計	23

システム管理者においては，業務システムの個人情報を情報系ネットワークで編集加工して二次利用しているシステムは 29 システムあり，データを保存しているものは 23 システムであった。このうち，抽出した全てのファイルでパスワード設定又は暗号化が行われていたものは 17 システムであったが，全てのファイルにパスワード設定及び暗号化がされていなかったものは 4 システム（同和奨学金システム，地域改善対策奨学金システムなど），一部のファイルにパスワード設定及び暗号化とも行なわれていなかったものは 2 システム（生活

保護システムなど）であった。

また各区役所及び市税事務所等における個人情報の情報系ネットワークでの取り扱い状況について，

・各所属において，個人情報（業務システムの個人情報を含む）を事務処理用 PC で編集・加工することがあるか。
・編集加工した個人情報データを事務処理用 PC 又は情報系ネットワーク上の共有サーバ等に保存しているか。
・個人情報を含むファイルを保存する場合，パスワード設定などどのような保存方法を行っているか。

の観点から，その運用状況について，各区の総務課，まちづくり課，市民課，保険年金医療課，市税事務所，健康福祉課，こども家庭支援課，保護課，北須磨支所，北神出張所，西神出張所の 83 所属で確認（事務処理用 PC の確認は各所属で 2 台抽出）したところ，その結果は第８表のとおりであった。

第８表　個人情報の情報系ネットワークでの取り扱い（区役所及び市税事務所）

	個人情報	データ保存	抽出したファイルのデータの保存方法	
無	6 所属	10 所属		
有	77 所属	73 所属	全てのファイルにパスワード設定又は暗号化あり	53
			全てのファイルにパスワード設定及び暗号化なし	9
			一部のファイルにパスワード設定及び暗号化とも無	11
計	83 所属	83 所属	計	73

区役所及び市税事務所においては，事務処理用 PC を利用して個人情報を編集加工している所属は 77 所属あり，データを事務処理用 PC 又は情報系ネットワーク上の共有サーバに保存しているものは 73 所属であった。このうち，抽出した全てのファイルでパスワード設定又は暗号化が行われていたものは 53 所属であったが，全てのファイルにパスワード設定及び暗号化のいずれも行われていなかったものは 9 所属，一部のファイルにパスワード設定及び暗号化のいずれも行われていなかったものは 11 所属であった。

（イ）基幹系ネットワークから情報系ネットワークへの個人情報データの移し替えの禁止

平成 27 年 8 月 7 日に，総務省より「社会保障・税番号制度の施行に伴う既存住基システム及び団体内統合宛名システムのインターネットを介した不特定の外部との通信について（通知)」が発出されたことに伴い，本市においても，平成 27 年 10 月 28 日，「基幹系ネットワークから情報系ネットワークへの個人情報データの移し替えの禁止および情報漏えい防止対策について」が通知された。

これに伴い本市では，以下の対策を可能な限り速やかに実施し，平成 28 年度中を目途に情報漏えい対策を完了することとしている。

◎基幹系ネットワーク上で稼働するシステム上の個人情報データを情報系ネットワーク（事務処理用 PC）に移動させることの禁止

◎基幹系ネットワーク上のシステムから可搬媒体へ情報を書き出す際には

・可搬記録媒体への書き出しが可能な端末，ユーザ権限は，必要最小限にすること

・可搬記録媒体へ個人情報等の機密性の高い情報を書き出す際は，暗号化，パスワードロック等の処置をとること

・可搬記録媒体へ個人情報等の機密性の高い情報を書き出す際は，記録に残すこと

市税システム，国民健康保険システム等において，本来業務の一環として，国等への報告，業務分析等を行うため，ホストコンピュータからデータを抽出し，これを本庁又は各区役所の事務処理用 PC で編集加工し，情報系ネットワーク上の NAS で保存している。

現在，平成 28 年度末にホストコンピュータを廃止し，クライアント・サーバ・システムへの移行作業が進められている。これらのシステムがクライアント・サーバ・システム化されれば，このような作業は同システムの専用 PC で処理され，そのデータも同システムのサーバで保存されるようになり，各業務システムの本来業務に付随した個人情報データの利用は，各業務システム内で完結することになる。

また，情報化推進部では，新たにクライアント・サーバ・システム化しないシステムであっても，基幹系ネットワーク上のシステムから提供を受けた個人情報データを事務処理用 PC で取り扱う場合は，各データ利用課にインターネットに接続できない環境を構築し，その環境に接続する事務処理用 PC を配布することを検討している。

④情報セキュリティ対策の徹底

（ア）副市長（情報化統括責任者）通知

日本年金機構の個人情報大量流出事件を受け，本市では，平成 27 年 6 月 5 日，副市長（情報化統括責任者）が，「情報セキュリティ対策の徹底について」を局室区長に通知し，所属職員に対して電子メールの取扱い，個人情報など機密性の高い重要データの取扱い，住民情報を取り扱う業務，ウイルス感染時等の対応の再度確認と周知徹底を図っている。

特に，この通知には，チェックリストが添付されており，情報セキュリティ対策の重要な事項の確認作業を速やかに行うことを指示している。

個人情報を処理する 182 の業務システムを管理する所属並びに各区役所及び市税事務所の 83 所属において，

- 上記副市長通知に基づき，課内で情報セキュリティ対策の周知徹底を行っているか。
- 通知に添付されたチェックリストに基づく情報セキュリティ対策の確認作業を行っているか。
- PC 等の端末，USB 等の記録媒体などの情報資産を外部に持ち出す場合，情報管理者の許可を得ているか。
- 事務処理用 PC にウイルス対策ソフトを常駐させるとともに，定義ファイルを最新のものにし，完全スキャン等を確実に実行しているか。

について，その実施状況を確認（事務処理用 PC は各所属で 2 台抽出）したところ，その結果は，第 9 表のとおりであった。

第 9 表　副市長（情報化統括責任者）通知の実施状況

	周知徹底	チェエクリストの活用		情報資産の持ち出し	ウイルス対策
システム管理者分					
済	181	181	適正	180	126
未済	1	1	不適	2	56
計	182	182	計	182	182
区役所・支所・出張所分					
済	83	83	適正	77	59
未済	0	0	不適	5	24
			該当なし	1	－
計	83	83	計	83	83

システム管理者及び区役所等とも，ほとんどの所属で，周知徹底及びチェックリストの活用が図られていた。

情報資産の持ち出しについては，持ち出し管理簿を作成し情報資産を外部に持ち出す場合には情報管理者の許可を得ていたものの，一部のシステムで，持ち出し管理簿を作成していない事例があった。

事務処理用 PC のウイルス対策については，システム管理者分では 56 システムの所属，区役所及び市税事務所分では 24 の所属で不適であった。抽出した PC には，ウイルス対策ソフト「Symantec」及び「Acrobat Reader」，「Flash Player」が常駐していたが，「Symantec」のウイルス定義ファイル及び「Acrobat Reader」については自動更新されるものの，「Flash

Player」については情報基盤管理者からの更新通知に基づき利用者が手動で更新作業を行うため，一部の PC で最新バージョンに更新されていなかった。

なお，情報基盤管理者は，平成 27 年 11 月 26 日に「イントラネット掲載ソフトウェアの脆弱性対策について（依頼）」を通知し，平成 27 年 12 月 25 日までに「Flash Player（Firefox 用）」，「Shockwave Player」，「Java(JRE)」，「Firefox」のソフトウェアを原則アンインストールし，「Flash Player（IE 用）」のソフトウェアのアンインストールを推奨することとし，ソフトウェアの脆弱性対策の強化を図った。

（イ）全庁ウイルス感染対応訓練

日本年金機構の個人情報大量流出事件を受け，本市では，平成 27 年 7 月 13 日に標的型メール攻撃による事務処理用 PC へのコンピュータウイルス感染を想定した全庁情報伝達訓練を実施し，事案発生時の初動対応の確認を行っている。

⑤情報セキュリティ監査及び自己点検

本市では，情報セキュリティ対策の実施状況を把握するため，定期的及び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している。

平成 26 年度及び平成 27 年度の実施状況は，第 10 表のとおりである。

特に，平成 26 年度から，第三者による独立かつ専門的な立場から助言型の情報セキュリティシステム外部監査を行っている。

第 10 表　情報セキュリティ監査及び自己点検の実施状況

年　度	種　別	実施時期	監査目的	監査対象	実施方法
平成26年度	自己点検	8月～9月	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ遵守状況の確認	全所属	所属職員が全市共通のチェックリストにより点検
	内部監査	12月～3月	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ遵守状況の確認	27所属	ヒアリング 実地視察
	外部監査（システム）	10月～1月	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ遵守状況の確認	（２システム） ・戸籍システム ・市営住宅総合管理システム	ヒアリング 実地視察
	外部監査（ソフトウェア）	2月	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ遵守状況の確認	（６所属） ・環境局事業系廃棄物対策室 ・市民参画推進局参画推進部市民情報サービス課 ・教育委員会事務局博物館小磯記念美術館 ・建設局下水道河川部計画課 ・こども家庭局こども企画育成部総合療育センター ・建設局中部建設事務所	ヒアリング 実地視察
平成27年度	自己点検	6月	日本年金機構の個人情報流出事件に伴うデータの取扱い等の確認	全所属	情報セキュリティチェックリストによる点検
		8月～9月	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ遵守状況の確認	全所属	所属職員が全市共通のチェックリストにより点検
	内部監査	1月～2月	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ遵守状況の確認	平成27年度は外部監査（システム）と一緒に実施	
	外部監査	1月～2月	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ遵守状況の確認	（１システム４利用課） ・情報系ネットワークシステム ※利用課として，こども家庭局子育て支援部振興課古湊保育所，市民参画推進局市民生活部消費生活課生活情報センター，西区まちづくり推進部総務課，行財政局職員部総務事務センターにもヒアリングを実施	ヒアリング 実地視察

２　指　摘　事　項

（１）情報資産の管理

①情報資産の管理方法

事務処理用 PC に標準装備されている市販の文書作成，表計算又はデータベース管理用のソフトウェアを使用して，職員が他の職員とは電磁記録を共有せずに単独で行う個人情報の電子計算機処理については，個人情報の保護対策として，電子メールでのデータ送信時の添付ファイルのパスワードの設定，職員ごとの ID と暗証番号の設定と共有の禁止，個人情報を含む電子データの暗証番号の設定などを行うこととし，また，その情報に，個人情報保護条例第 7 条第 3 項に規定するセンシティブ情報が含まれる場合には，審議会に諮問するとされている。(個人情報保護審議会平成 20 年 12 月 10 日諮問時の情報化推進部作成資料，参考４　参照)。

しかし，次のような事例があった。

（ア）情報系ネットワーク上でのNAS利用による個人情報の保存

事務処理用 PC で作成したデータの保存及び所属での情報共有を図るため，情報系ネットワーク上に外部記憶装置 NAS(Network Attached Storage)を設置し，各種の名簿や刊行物の送付先などの個人情報を含むファイルが保存されている事例が散見された。また，事務処理用 PC を職員が共用で使用している所属では，作成したデータを USB で個人ごとに保存管理するために，共用の事務処理用 PC のデバイス制御を解除した上で，各担当者に USB を配付している事例があった。

情報化推進部においては，NAS にデータを保存する場合の職員のアクセス制限やファイルへのパスワード設定を呼びかけているものの，情報セキュリティポリシー上では，NAS 等による個人情報の保存方法について規定されていない。

NAS 等を利用して個人情報を保存し活用する場合の個人情報の保護対策について，その対策を情報セキュリティポリシーで明記し，その徹底を図るべきである。

（企画調整局情報化推進部）

（イ）生活保護業務における査察指導台帳の作成保存

各区の生活保護業務では，担当係長が，被保護世帯に対するケースワークの査察指導の進行管理を行うため，生活保護システムから被保護世帯に関する必要な情報を事務処理用 PC に取り込み，データを編集加工して「査察指導台帳」を作成保存しているが，「査察指導台帳」ファイルにパスワード設定が行われていない事例があった。また，「査察指導台帳」の事務処理用 PC による作成保管は，審議会に諮問されていなかった。

「査察指導台帳」のデータには個人情報保護条例第 7 条第 3 項に規定するセンシティブ情報が含まれる場合があることから，適正な情報セキュリティ対策を講じるべきである。

（保健福祉局総務部保護課）

（ウ）同和奨学金・地域改善対策奨学金システムの個人情報の情報系ネットワーク上での保存

同和奨学金システム（ホストシステム）及び地域改善対策奨学金システム（スタンドアロンシステム）では，国庫返還事務や滞納整理事務を行うため，同システムから抽出した個人情報データを事務処理用 PC で編集加工して状況別の奨学生一覧等を作成し，NAS に保存して課内の関係職員で奨学生や返還金の情報を共有化していた。

同和奨学金に関する情報はセンシティブ情報にあたることから，適正な情報セキュリティ対策を講じるべきである。

（教育委員会事務局指導部人権教育課）

（２）物理的セキュリティ

①サーバの管理

福祉情報システム及び生活保護システムの区役所に設置するセグメントサーバ，精神障害者保健福祉手帳システム及びこども家庭センター(児童虐待対応ナビ)システムのサーバの管理について，下表のとおり，施錠可能な区画を設置せずに執務室内にサーバを設置し，また，ラック等に収納して容易に取り外せないよう固定が行われていない事例があった。なお，こども家庭センターシステムは，構築時に，審議会の諮問を受けていなかった。

サーバを施錠可能な区画に設置し，容易に取り外せないように固定して取り付けるなど適正な管理を行うべきである。

（保健福祉局総務部計画調整課，保護課，障害福祉部こころの健康センター，
こども家庭局こども家庭センター）

サーバ等の管理が不適正なシステム

システム名 （サーバ種類）	サーバの設置場所													
	管理者	東灘	灘	中央	兵庫	北	北神	長田	須磨	北須磨	垂水	西	西神	その他
福祉情報 （区等セグメントサーバ）	－	×	▽	×	×	×	×	×	×	×	×	×	－	×
生活保護 （区セグメントサーバ）	－	▽	▽	×	▽	×	×	▽	▽	×	▽	×	－	－
精神障害者保健福祉手帳	×	－	－	－	－	－	－	－	－	－	－	－	－	－
こども家庭センター （児童虐待対応ナビ）	×	－	－	－	－	－	－	－	－	－	－	－	－	－

○：サーバを施錠可能な区画に設置し，容易に取り外せないようラック等に適切に固定している。
△：サーバが執務区域に設置されている。
▽：サーバが容易に取り外せないようラック等に適切な固定を行っていない。
×：サーバを執務区域に設置し，ラック等に適切な固定を行っていない。
－：サーバ未設置。

3　意　　見

本市では，ホストコンピュータが廃止され，業務システムごとのクライアント・サーバ・システムに移行されると，各システム管理者がそれぞれのシステムの管理・運用に一元的な責任を負うことになるが，その一方で，情報システムに関する全庁的な調整，人材育成及び情報セキュリティに関する全庁的な対応機能の低下が懸念される。

また，日本年金機構の事案では組織全体の不適切な初動対応が被害を拡大し，個別システムのインシデントであっても複雑に連携したネットワークでは直ちに全体のインシデントに拡大する恐れがある。

このため，情報セキュリティ責任者（企画調整局情報化推進部長）のリーダーシップの下に，平常時から，情報セキュリティ監査及び自己点検の更なる充実を図るとともに，インシデント発生時には，迅速に組織全体で対応（連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置）する仕組みを強化する必要がある。

重要な情報システムは，外部のインターネット環境と切り離されており，外部から接続できない独立した仕組みなので，安全だと信じられてきた。しかし，米国で開催されたハッカーの国際大会では，隔離したはずのシステムをインターネット経由で攻撃する手法が多数報告されており，インターネットと独立したシステムといえども複数の段階を経由すれば侵入し，ハッキングによるデータの破壊・改ざんや取得をすることができる。（日経新聞　平成27年9月2日朝刊記事）

また，標的型攻撃等は巧妙かつ複雑多様化してきており，最新のウイルス対策ソフトを常駐していても，これを入り口で完全に防御しきるのは困難である。

このため，感染後の事態をいち早く把握し，影響範囲を特定し封じ込め，システムを迅速に復旧させることを前提に，標的型攻撃等の脅威からの防御・検出だけでなく，内部での侵入拡大の防止や情報の持ち出しの防止などと組み合わせた多重防御の考え方が不可欠である。

堺市において，平成23年大阪府知事選の市内の全有権者約68万人分の氏名，年齢，生年月日，住所などの個人情報が，職員の内部不正行為により，外部に流出，インターネット上で一時公開されたという事件があった。

内部犯罪・内部不正行為による個人情報の漏えいの発生件数は，外部からの攻撃によるものと比較すると少ないものの，1回あたりの漏えいする個人情報の被害件数は大きく，また関係者に対する信頼を著しく損なうものである。

職員や委託業者の従業員の不正行為による個人情報の流出を防止するためには，職員等の情報セキュリティ研修の継続的な実施だけでなく，過度に職員等を信頼（放任）するのではなく，定められた管理や監視の証跡を確実に確認することによって，職員等の不正行為の動機や機会を抑制するとともに情報漏えいの早期発見,被害の最小化を図ることが重要である。

情報セキュリティの向上だけでなく，ICT を活用した業務の効率化，市民サービスの向上には，職員の ICT 能力の向上が不可欠である。このため，一般職員への基礎的な ICT 研修を継続的に実施するだけでなく，特に ICT システムの構築や運用などに関する知識を有し，ICT サービスの立案，設計，導入，継続的改善を行うことのできる職員の戦略的な人材育成が必要である。

情報セキュリティ対策の導入にあたっては，冷静なリスク評価に基づき，リスク対策が生み出す新たなリスクや対策のコストを考慮しつつ，各リスクを受け入れ可能な範囲にまで下げるための効果的な対策を組み合わせることが重要である。

このような ICT リスクへの基本的な認識のもと，特に以下の点について改善を検討されたい。

（１）情報資産の管理

①情報システム台帳

情報システム台帳は，本市の情報資産の管理及び情報システムの全容を把握する上で基本となる台帳である。今回の監査もこの台帳情報をもとに実施したが，台帳記載内容と実際が異なる事例が散見されたので，次の事項について検討されたい。

（企画調整局情報化推進部）

（ア）台帳の定期的な更新

情報システム台帳については，情報化推進部が本市の情報システムを把握するため任意で作成したものである。情報資産の管理の観点から，この台帳の作成を情報セキュリティポリシー等で義務化し，定期的に情報を更新する仕組みを検討されたい。

（イ）登録すべき情報システムの明確化

登録されているシステムの中には，インターネットと接続していない PC や他の事業所でも同様に使用されているのではないかと推測されるシステム，国等の他機関が管理運営するシステムのネットワーク機器等があった。

本市の管理するシステムの全容を正確に把握するため，この台帳に登録すべきシステムの定義の明確化を検討されたい。

②情報資産の保管方法

（ア）機密性３のデータの保存方法

対策基準では，機密性３のデータ（個人情報など）について，電子メールによる送信を行う場合及び外部に提供する場合には，パスワード等による情報漏えい対策を行わなければならないとされているが（対策基準 4.2.3 エ(3)及びカ(1)），データの保存については，「情報資産管理責任者は，情報資産の重要性分類に従って，情報資産の保管を適切に行わなければならない。」（対策基準 4.2.3 オ(1)）と規定するのみで，具体的な保存方法は規定されていない。

抽出した事務処理用 PC の個人情報を含むファイルについて，そのデータの保存方法を確認したところ，次のとおり，多くの所属では全てのファイルにパスワード設定又は暗号化のいずれかが行われていたものの，全てのファイルに両方とも行われていなかった事例や一部のファイルに両方とも行われていなかった事例があった。

情報漏えい対策を強化するため，対策基準等に機密性３のデータの具体的な保存方法を明記し，その方法を徹底することを検討されたい。

（企画調整局情報化推進部）

システム管理者

	二次利用	データ保存	抽出したファイルのデータの保存方法	
無	153 システム	159 システム		
有	29 システム	23 システム	全てのファイルにパスワード設定又は暗号化あり	17
			全てのファイルにパスワード設定及び暗号化なし	4
			一部のファイルにパスワード設定及び暗号化とも無	2
計	182 システム	182 システム	計	23

区役所及び市税事務所

	個人情報	データ保存	抽出したファイルのデータの保存方法	
無	6 所属	10 所属		
有	77 所属	73 所属	全てのファイルにパスワード設定又は暗号化あり	53
			全てのファイルにパスワード設定及び暗号化なし	9
			一部のファイルにパスワード設定及び暗号化とも無	11
計	83 所属	83 所属	計	73

（イ）家庭内暴力（DV）・ストーカー等の被害者の証明書発行制限に関する情報共有

各区市民課では，DV・ストーカー行為等の被害者について，証明書の発行を制限する支援を行っており，住民記録システムでも，発行制限等の処理ができるようになっている。しかし実務上の必要から，各区市民課で，担当係長又は担当者が情報系ネットワーク上の事務処理用 PC を使用して独自に DV・ストーカー行為等の被害者の氏名，生年月日，住所，証明書の発行制限に関する情報等を記録した対象者リストを作成するとともに NAS を利用して係長と担当者が情報を共有している事例があった。

これらの情報は機密性の高い情報であるが，事務処理の効率化の観点から，セキュリティに十分注意した上で，事務処理用 PC を利用した情報共有のあり方について検討されたい。

（市民参画推進局参画推進部区政振興課）

（２）物理的セキュリティ

①コンピュータの設置場所

ホストコンピュータ及び住民記録，福祉情報等の基幹業務系システムのサーバは，セキュリティカードにより一般職員が入退室不能なマシンルームに設置されているが，市税のサブシステム等のサーバが民間ビルの事務室スペースを改修して設置されていた。

いずれのシステムもセキュリティポリシー上問題はないものの，セキュリティレベルの向上の観点から，ホストコンピュータのクライアント・サーバ・システムへの移行後に，ホストコンピュータの設置場所，ホストデータ入力室等を活用して，サーバの集約化を検討されたい。

（企画調整局情報化推進部）

②スタンドアロンシステムのあり方

システム台帳では，個人情報を取り扱っているスタンドアロンシステム（PC 単体で稼働しているシステム）が 54 システムあった。

いずれもアクセス制限のための ID とパスワードの設定は行われていたものの，その多くが，ネットワークに接続していないことを理由にウイルス対策ソフトの常駐がないか，ウイルス対策ソフトを導入していても定義ファイルを更新していなかった。また，審議会の諮問を経ずにシステムを構築したり，施錠可能な管理区域に PC を設置していないシステムも多数あった。さらに，情報の共有化及び業務の効率化を図るため，スタンドアロンのシステムの情報を情報系ネットワーク上で課内共有し，データを編集加工している事例もあった。

インターネット接続がなく，USB 等による外部接続が完全に行われず，当該 PC 内だけで情報の閲覧・処理が行われるのであれば，ウイルス対策ソフトの常駐までは必要ないといえなくはないが，当該 PC に個人情報が保存されている以上，端末本体の盗難等による情報流出に備え，不利用時に施錠できる書庫等へ保管することや業務担当者以外のアクセス制御の徹底などのセキュリティ対策の確実な実施が必要である。

スタンドアロンシステムについて，情報系ネットワークのイントラで処理することも含めて，よりセキュリティ対策の確実なあり方を検討されたい。

（企画調整局情報化推進部）

（３）技術的セキュリティ

①不正アクセス対策の強化

第三者からのサービス不能攻撃や標的型攻撃の発生事例が，国及び他地方自治体，企業で多数報告されている。本市においても同様の攻撃を受けることが懸念されるが，第三者からのサービス不能攻撃を受けた場合でも情報システムの可用性を維持し，標的型攻撃による外部からの本市システムへの侵入を防ぐ必要がある。

不正アクセス対策について，総務省が策定した「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」（平成 27 年 3 月一部改訂）では，サービス不能攻撃及び標

的型攻撃の項目が追加され，その対策が明記されている。

不正アクセス対策をより明確にするため,本市でも,総務省のガイドラインも参考にして，対策基準を見直し，サービス不能攻撃及び標的型攻撃への対策を明記することを検討されたい。

（企画調整局情報化推進部）

（４）運　用

①情報システムの監視

（ア）ログ解析

ログは，OS，アプリケーション，通信機器などが，稼働状態，処理の実行状況，障害・異常の発生状況などについて出力した記録であり，ログの解析結果に基づいて問題箇所を修正することで発生中のトラブルを解決したり，未然に防止したりすることができる。また外部からの不正アクセスや内部の不正利用を検知することができるため，ネットワークを構成する各システム管理者は，ファイアウォールなどネットワーク機器や端末のログの収集を行っている。

しかし，収集したログの解析については，各システム管理者によって，その頻度，対象機器等が大きく異なっていた。

ログ解析は，不正アクセス・不正利用の早期発見，被害拡大の防止に資することから，システムの重要性に鑑み，特に基幹業務系システムについては，ログ解析の実施水準を標準化することを検討されたい。

（企画調整局情報化推進部）

②情報セキュリティインシデントへの対応

（ア）ＣＳＩＲＴの設置

近年，相次ぐサイバー攻撃による重大な情報セキュリティインシデントの発生や，それに伴うサイバーセキュリティへの関心の高まりを背景として，CSIRT（シーサート：Computer Security Incident Response Team）を設置する企業や組織が増加している。

CSIRT は，初動対応，原因究明，対応策等のインシデント発生時の対応を主導し，現場組織等に適時対応を指示するとともに，日常的な活動としてインシデントの検知，個別の対応手順の策定などインシデント発生に備えた各種対応を行う。

本市の対策基準等では，情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に備え，情報セキュリティ総括責任者（企画調整局長）は，緊急時の円滑な情報提供を図るため関係者の連絡体制を整備し，情報基盤管理者及び業務システム管理者は，緊急時対応計画（緊急時の対応手順，緊急連絡網）を策定する，とされている。しかし，複数の業務システム又は全庁的に影響を及ぼすインシデントに対する対応手順は明らかでない。また主要な業務システム以外では，必ずしも情報通信技術に詳しい職員が運用しているわけでないため緊急時対応計画を策定することが困難なシステムもある。

一方で，ホストコンピュータからクライアント・サーバ・システムへの移行により業務所管課がそれぞれ情報システムを管理・運用するようになること，マイナンバー法の施行と個人番号の利用拡大といった情勢を踏まえれば，個別システムのインシデントを全体の被害に拡大させないためにも，緊急時により実践的な初動対応が要求されるようになっている。

インシデントに備えた全庁的な各種対応やインシデント発生時に主導的に適時対応(連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置）を指示する仕組みを明確にし，初動対応力の強化を図るため，情報セキュリティ責任者（企画調整局情報化推進部長）を中心に，情報セキュリティ管理者，情報基盤管理者，基幹業務系ネットワーク管理者，情報系ネットワーク管理者，主要な業務システム管理者並びに情報セキュリティに関する事務局で構成する CSIRT の設置を検討されたい。

（企画調整局情報化推進部）

参考１　日本年金機構における不正アクセスによる情報流出事案に関する調査結果報告

（概要）

日本年金機構の不正アクセスによる情報流出事案に関する調査委員会による「不正アクセスによる情報流出事案に関する調査結果報告」（平成 27 年 8 月 20 日）及び厚生労働省の日本年金機構における不正アクセスによる情報流出事案検証委員会による「検証報告書」（平成 27 年 8 月 21 日）に基づき，監査事務局が作成。

１．事案の概要

- 5 月 8 日（金）以降，標的型メールを合計 124 通受信。メール添付ファイル等を開封した機構職員は 5 名。感染した端末は合計 31 台。
- 5 月 21 日（木）～23 日（土）までの間に約 125 万件（約 101 万人）の個人情報が流出した。そのうち約 55 万件のデータは，パスワード未設定。

２．日本年金機構の個人情報流出事件の対応等

	何が起こったのか	何をしたか	どのように対応すればよかったのか
H27.4.22	厚生労働省年金局等に標的型メールが届き端末が感染。	URL ブロックを行い，通信を遮断した。	機構も含めたネットワークでドメイン単位のブロック。
H27.5.8	・年金機構の公開メールアドレス宛てに標的型メールが届き端末が感染。 ・内閣サイバーセキュリティセンター（NISC）から「不審な通信を検知した」と連絡あり。	不審通信を検知した端末を特定して抜線した。	・送信元のメールアドレスの受信拒否設定。 ・感染端末のフォレンジック調査。
H27.5.18	・年金機構の非公開の個人メールアドレス宛てに約100件の標的型メールが届き端末が感染。 ・認証サーバの管理権限が盗まれる。	不審メールの送信元のメールアドレスの受信拒否設定を実施した。	・メールが届いた職員にファイル開封の確認。 ・機構全体のインターネット接続の遮断。
H27.5.21～23	年金機構から情報流出	不審通信を検知した端末を特定して抜線した。	

３．日本年金機構の問題認識と対応策

問題認識	対応策
個人情報を扱う端末がインターネットにつながっていた。	個人情報のインターネット接続環境からの完全遮断を行う。
インターネット接続環境下にある共有ファイルサーバに個人情報を置くというリスクへの認識が甘かった。	共有ファイルサーバの管理業務を情報セキュリティ管理担当部署に移行し，ルールの遵守状況などの確認を徹底する。
基本的な対応が担当者任せとなっていた。	情報セキュリティ対策の司令塔として一元的に管理する「情報管理対策本部（仮称）」を新設する。
情報セキュリティポリシーの改正に遅れがあり，標的型メール攻撃に対する基本的対策事項等に関する記載が不足していた。	情報セキュリティポリシーを改正するとともに，標的型メール攻撃に対する具体的対処手順を整備し，職員への周知徹底を図る。

参考２　神戸市情報セキュリティ基本方針

１．目的

本市の情報システムが取り扱う情報には，市民の個人情報や行政運営上重要な情報が多数含まれており，情報資産を人的脅威や災害，事故等様々な脅威から防御することは，市民の財産，プライバシー等を守るためにも，また，継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

このため，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ことを目的として神戸市情報セキュリティ基本方針（以下「情報セキュリティ基本方針」という）を定める。神戸市の情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものである。

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及びその構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム

コンピュータ及びネットワークで構成され，情報処理を行う仕組みをいう。

（３）データ

電子計算機処理に係る入出力帳票，磁気テープ，磁気ディスク，パンチカードその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

（４）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。

（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。

（８）情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

３．情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは，本市が保有する情報資産に関する情報セキュリティ対策について総合的かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり，情報セキュリティ基本方針及び情報セキュリティ対策基準から構成される。

情報セキュリティ対策基準は，情報セキュリティ基本方針に基づき，情報セキュリティ対策等を実施するために最低限必要な水準として，職員等が遵守すべき事項及び判断基準をまとめたものである。本市では，組織等の状況に合わせた情報セキュリティ対策基準を策定する。

４．適用範囲

（１）組織の範囲

神戸市事務分掌条例(平成15年10月条例第19号)第1条に規定する局及び室，区役所，会計室，消防局，水道局，交通局，教育委員会，選挙管理委員会事務局，人事委員会事務局，監査事務局，農業委員会事務局，市会事務局とする。

（２）情報資産の範囲

情報セキュリティ基本方針が対象とする情報資産は次のとおりとする。

ア 物理資産

コンピュータ・ネットワーク・記録媒体等物理的な形状を有する資産でありかつ，情報を利用するのに必要な資産

イ データ資産

データ及び情報システムの設計等に関する情報

ウ ソフトウェア資産

コンピュータ等の情報機器において稼動するプログラム

エ サービス資産

電源，メールサービス等契約により提供される情報システムに関連する業務

５．職員等の義務

職員（再任用職員，任期付職員を含む。以下同じ），教員，臨時的任用職員，非常勤嘱託職員及び委託業務等従事者（以下「職員等情報取扱者」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，業務の遂行にあたっては情報セキュリティポリシーを遵守するものとする。

６．情報セキュリティ管理体制

本市の情報資産について，適切に情報セキュリティ対策を推進・管理するため，神戸市情報化推進体制の整備に関する要綱に定める情報化統括責任者（情報化の推進を所管する実施組織を担任する副市長）を情報セキュリティ最高責任者とし，その下に全庁的な組織体制を確立する。

必要な体制，役割，権限等については情報セキュリティ対策基準にて定める。

７．情報資産への脅威

情報セキュリティ対策を講じるうえでは，情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に次の脅威については，十分な措置を講じるものとする。

（１）部外者による不正アクセス又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去，機器及び媒体の盗難等

（２）職員等情報取扱者による意図しない操作，不正アクセス又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去，機器及び媒体の盗難，規定外の端末接続によるデータ漏えい等

（３）地震，落雷，火災等の災害，事故，故障等によるサービス及び業務の停止

８．情報セキュリティ対策

情報資産に対する脅威から情報資産を保護するため，次の情報セキュリティ対策を講ずるものとする。

（１）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実施することとする。

（２）物理的セキュリティ

コンピュータ設置場所への入退室，サーバ等の管理，通信回線及び端末等への物理的な対策を講じる。

（３）人的セキュリティ

情報セキュリティに関し，職員等情報取扱者が遵守すべき事項を定めるとともに，十分な研修・訓練及び啓発を実施するなど人的な対策を講じる。

（4）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,コンピュータウイルス等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。

（5）運用面のセキュリティ

情報システムに関し，情報セキュリティポリシーの遵守状況の確認等，情報セキュリティポリシーの運用面の対策を講じる。また，情報資産への侵害が発生した場合等に，迅速かつ適切に対応するため，緊急時対応計画を策定する。

9．情報セキュリティ個別基準の策定

情報セキュリティポリシーを補完するために必要な内容に関して，具体的な内容を定める情報セキュリティ個別基準を策定するものとする。

１０．情報セキュリティ実施手順の策定

情報セキュリティポリシー及び情報セキュリティ個別基準に基づき，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。

１１．情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況を評価するため，定期的及び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。

１２．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，情報セキュリティに関する状況の変化等を踏まえ，必要に応じ適宜情報セキュリティポリシーの見直しを行う。

参考３　神戸市情報セキュリティ対策基準（概要）

１.目的

神戸市情報セキュリティ対策基準とは，神戸市情報セキュリティ基本方針に基づき情報セキュリティ対策等を実施するために適用範囲における共通の基準として具体的な遵守事項及び判断基準を定めたものである。

２.適用範囲

神戸市事務分掌条例第 1 条に規定する局（保健福祉局看護大学を除く）及び室，区役所，会計室，消防局，水道局，交通局，教育委員会（小学校，中学校，高等学校，高等専門学校，特別支援学校，幼稚園を除く），選挙管理委員会事務局，人事委員会事務局，監査事務局，農業委員会事務局，市会事務局とする。

３.情報セキュリティ管理体制

(ア)　情報資産の分類と管理

4.2.1 情報資産の分類

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，第 11-1 表のとおり分類し，当該分類に基づき情報セキュリティ対策を実施している。

情報資産の機密性，完全性，可用性のいずれかの重要性分類２以上に分類される情報資産は，この対策基準の対象としている。

第 11-1 表　情報資産の分類

分類	機密性	完全性	可用性
3	行政事務で取り扱う情報資産のうち、特に機密性を要するもの （次のデータだけではなくそれらが含まれる電子記録媒体、パーソナルコンピュータ、システム等も同様） ・特定個人情報に関するデータ ・個人情報に関するデータ ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に行政の信頼を著しく害する可能性があるデータ ・公開することでセキュリティ侵害が生じる可能性があるデータ	行政事務で取り扱う情報資産のうち、特に完全性を要するもの （次のデータだけではなくそれらが含まれる電子記録媒体、パーソナルコンピュータ、システム等も同様） ・改ざん、誤びゅう又は破損が生じると住民の権利が侵害される可能性があるデータ ・改ざん、誤びゅう又は破損が生じると行政事務の適確な遂行に著しい支障を及ぼす可能性があるデータ	行政事務で取り扱う情報資産のうち、特に可用性を要するもの （次のデータだけではなくそれらが含まれる電子記録媒体、パーソナルコンピュータ、システム等も同様） ・利用できないと住民の権利が侵害される可能性があるデータ ・利用できないと行政事務の安定的な遂行に著しい支障を及ぼす可能性があるデータ
2	直ちに一般に公表することを前提としていないもの （機密性３には当てはまらないが、広報等は行っていないデータ及びそれらが含まれる電子記録媒体、パーソナルコンピュータ、システム等）	改ざん、誤びゅう又は破損が生じると行政事務の適確な遂行に支障を及ぼす可能性があるもの	利用できないと行政事務の安定的な遂行に支障を及ぼす可能性があるもの
1	機密性２又は機密性３以外の情報資産	完全性２又は完全性３以外の情報資産	可用性２又は可用性３以外の情報資産

4.2.3　情報資産の管理方法

情報資産の管理，データの作成，情報資産の入手，利用，保管，提供・公表，廃棄について，その方法が定められている。主な管理方法は，第 11-2 表のとおりである。

第 11-2 表　情報資産の管理方法

主な項目	主な対策
4.2情報資産の分類と管理方法	
4.2.3 情報資産の管理方法	ア 情報資産の管理 (2) すべての情報資産を明確に識別し、重要な情報資産に対しては必要に応じて目録を作成して管理しなければならない。 エ 情報資産の利用 (2) 情報資産の利用においては、情報資産の分類に応じ、利用者並びにアクセス権限を定めなければならない。 (3) 機密性３のデータは、情報資産管理責任者の許可を得た場合、複写、複製、送付、送信を行うことができる。ただし、パスワード等による情報漏えい対策を施さなければ電子メールによる送信を行ってはならない。 (4) 電子メールにより機密性２のデータを送信する者は、必要に応じパスワード等による情報漏えい対策を施さなければならない。 オ 情報資産の保管 (2) 最終的に確定したデータを記録した電子記録媒体は、書込禁止措置を行ったうえで保管しなければならない。 (3) 情報資産管理責任者は、持ち運び可能な電子記録媒体を耐火、耐熱、耐水及び耐湿対策を講じたうえ施錠可能な場所への保管等適切な管理を行わなければならない。 (4) 情報資産管理責任者は、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電子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への保管を考慮しなければならない。 (5) 機密性２以上の情報資産が保管された電子記録媒体の搬送にあたっては、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施さなければならない。 カ 情報資産の提供・公表 (1) 機密性３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。 (2) 機密性３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事前に許可を得たうえで、日時・担当者及び提供概要を記録しなければならない。 キ 情報資産の廃棄 (1) 電子記録媒体が不要となった場合は、当該媒体に含まれるデータの消去を行ったうえで裁断、溶解等により物理的に破壊し、復元不可能な状態にして廃棄しなければならない。

(イ) 物理的セキュリティ

コンピュータ設置場所への入退室，サーバ等の管理，通信回線及び端末等への物理的な対策を講じている。主な対策は，第 11-3 表のとおりである。

第 11-3 表　物理的セキュリティ対策

主な項目	主な対策
5.1サーバ等の管理	
5.1.1　入退室の管理	情報資産管理責任者は、重要性分類３のデータが記録されている電子記録媒体及び紙媒体の保管場所並びにそれを取扱うコンピュータ設置場所の入退室について、適正な管理を行わなければならない。 中でも、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、当該機器の管理及び運用を行う部屋（以下「管理区域」という）については、次の事項に従い厳重な管理を行わなければならない。 ア 管理区域を新設する場合は、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しなければならない。 イ 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。 ウ 管理区域への入退室は、許可された者のみに制限し、ＩＤカード等による認証及び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。 エ 職員等情報取扱者は、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。 オ 外部からの訪問者が管理区域に入室する場合には、必要に応じて立ち入り区域を制限したうえで、管理区域への入退室を許可された職員が付き添うものとし、外見上職員と区別できる措置を施さなければならない。 カ 管理区域については、当該システムに関連しないコンピュータ、通信回線装置、電子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。
5.3　端末等の管理	
5.3.2　ログインパスワード	情報基盤管理者及び業務システム管理者は、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。また、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。

（ウ） 人的セキュリティ

情報システムにアクセスするための認証情報及びパスワードの管理，外部委託に関する管理など職員等情報取扱者が遵守すべき事項などの人的な対策を講じている。主な対策は，第 11-4 表のとおりである。

第 11-4 表　主な人的セキュリティ対策

主な項目	主な対策
6.1　職員等の責務	
6.1.5 情報資産の持ち出し及びＷｅｂサイト等による送信禁止	職員は情報資産を取り扱う場合、次の行為を行ってはならない。 ア 所属外への持ち出し ただし、情報資産のバックアップ等、合理的理由のある場合、かつ情報管理者等管理権限のある者の許可を得た場合に限り、記録を作成したうえで所属外への持ち出しができるものとする。
6.4 アクセスのための認証情報及びパスワードの管理	
6.4.1 ＩＤカード等の管理	イ 職員等情報取扱者は、次の事項を遵守しなければならない。 (1) ＩＤカード等は、職員等情報取扱者間で共有しない。ただし、所属等ごとに配布されたＩＤカード等については除く。 (2) ＩＤカード等は、カードリーダ若しくは端末のスロット等に必要な時以外は挿入しない。 (3) ＩＤカード等を紛失した場合には、速やかに情報基盤管理者及び業務システム管理者等権限のある者に通報し、指示を仰ぐ。
6.4.2 ＩＤの管理	ア 職員等情報取扱者は、他人に自己が利用しているＩＤを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。
6.4.3 パスワードの管理	ア 職員等情報取扱者は、自己のパスワードに関し、次の事項を遵守しなければならない。 (1) パスワードは秘密にし、パスワードの照会等には一切応じない。 (2) 情報システム又はパスワードに対する危険のおそれがある場合には、情報基盤管理者及び業務システム管理者等権限のある者に速やかに報告し、パスワードを速やかに変更する。 (3) 原則として、パスワードを記載したメモを作成しない。やむを得ずメモを作成する場合は、他人にわからない場所に保管をする。 (4) 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とする。 (5) パスワードは定期的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ない。 (6) 複数の情報システムを扱う場合は、同一のパスワードを複数のシステムで用いない。 (7) 仮のパスワードは、最初のログイン時点で変更する。 (8) パーソナルコンピュータ等のパスワードの記憶機能を利用しない。 (9) 職員等情報取扱者の間でパスワードを共有しない。
6.5 外部委託に関する管理	
6.5.1 委託先事業者の選定	特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、委託先の選定にあたり、委託内容に応じた情報セキュリティ対策の実施が確保されることを確認しなければならない。
6.5.2 契約書の記載事項	ア 特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、当該委託先事業者との間で、下記事項を明記した契約を締結しなければならない。
6.5.3 情報セキュリティ確保への取組みの実施状況等の調査	情報基盤管理者及び業務システム管理者は、契約締結後においても、当該委託先事業者の情報セキュリティ確保への取組みの実施状況等について、定期的若しくは随時、調査を行い、安全を確保しなければならない。情報セキュリティ責任者から内容の報告を求められた場合には、報告を行わなければならない。
6.5.4 再委託等	再委託（再々委託を含む）を受ける事業者がある場合、6.5.2 及び6.5.3 に定める事項は再委託（再々委託を含む）を受ける事業者にも適用する。
7.4 コンピュータウイルス等不正プログラム対策	
7.4.3 職員等情報取扱者の遵守事項	職員等情報取扱者は、次の事項を遵守しなければならない。 ア 端末において、コンピュータウイルス等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ない。 オ 端末に対して、コンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

(エ) 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,コンピュータウイルス等不正プログラム対策，不正アクセス対策などの技術的対策を講じている。主な対策は,第 11-5 表のとおりである。

第 11-5 表　主な技術的セキュリティ対策

主な項目	主な対策
7.1 コンピュータ及びネットワークの管理	
7.1.3 アクセス記録の取得等	ア 情報基盤管理者及び業務システム管理者は、所管するシステムにおいて、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、窃取、改ざん、誤消去等を防止する措置を施したうえで一定期間保存する。また、不正アクセスの兆候を発見するために定期的にそれらを分析することとする。 イ 情報基盤管理者及び業務システム管理者は、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。
7.1.5 情報資産のバックアップ	情報基盤管理者及び業務システム管理者は、所管するシステムにおいて、必要なものはサーバの二重化対策実施の有無に関わらず、定期的に情報資産のバックアップのための対応を行うものとする。
7.2 アクセス制御	
7.2.1 利用者の識別及び認証	情報基盤管理者及び業務システム管理者は、所管するネットワーク又はシステムに権限がない職員等情報取扱者がアクセスすることが不可能となるように、利用者の識別及び認証等適切な対応を行わなければならない。
7.2.2 利用者登録	ア 情報基盤管理者及び業務システム管理者は、利用者の登録、変更、抹消、登録した情報資産の管理、異動、出向及び退職時における利用者ＩＤの取り扱い等については、定められた方法に従って行わなければならない。 必要な利用者登録・変更・抹消は、情報基盤管理者及び業務システム管理者に対する申請により行う。ただし、所属等ごとに配布されたＩＤ等については除く。 イ 情報基盤管理者及び業務システム管理者は、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。 ウ 情報基盤管理者及び業務システム管理者は、ＩＤに割り当てているアクセス権の正当性を確保するために、定められた方法に従って点検しなければならない。
7.2.3 特権管理等	ア 情報基盤管理者及び業務システム管理者は、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 情報基盤管理者及び業務システム管理者の特権を代行する者は、当該管理者が指名し、情報セキュリティ統括責任者が認めた者でなければならない。 ウ 情報基盤管理者及び業務システム管理者は、特権を付与されたＩＤ及びパスワードの変更について、原則として外部委託事業者に行わせてはならない。 エ 情報基盤管理者及び業務システム管理者は、特権を付与されたＩＤ及びパスワードについて、職員等情報取扱者の端末等のパスワードと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。 オ 情報基盤管理者及び業務システム管理者は、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。
7.2.4 ネットワークにおけるアクセス制御	情報基盤管理者及び業務システム管理者は、アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また、ネットワークサービスを利用する権限を有しない職員等情報取扱者が当該サービスを利用できるようにしてはならない。
7.2.5 強制的な接続制御、経路制御	ア 情報基盤管理者及び業務システム管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。 イ 情報基盤管理者及び業務システム管理者は、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、ルータ等に搭載されている通信ソフトウェア等を設定しなければならない。
7.2.6 無人状態にある装置の管理	情報基盤管理者及び業務システム管理者は、サーバ又は端末等の装置が無人の状態になる場合、適切なセキュリティ対策を施さなければならない。
7.2.7 外部からのアクセス	ア 情報基盤管理者及び業務システム管理者は、外部からのアクセスを許可する場合、合理的理由を有する必要最低限のものに限定しなければならない。 イ 内部ネットワーク及び情報システムへのアクセス方法及び利用方法等は、通信途上の機密性及び利用者の真正性が確保できるものでなければならない。 ウ 職員等情報取扱者は、外部から持ち帰ったパーソナルコンピュータ等の端末を内部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。

7.2.8 内部ネットワーク間の接続	情報基盤管理者及び業務システム管理者は、他の内部ネットワークとの接続については、あらかじめ接続先の内部ネットワークの管理者と協議し、以下の内容を確認したうえで、接続しなければならない。 ア 接続によりそれぞれの情報資産に影響が生じないこと イ 接続した場合のそれぞれの情報システムの責任範囲 ウ 障害発生時の対応体制
7.2.9 外部ネットワークとの接続	ア 情報基盤管理者及び業務システム管理者は、外部ネットワークとの接続にあたり、当該外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、適用範囲における情報資産に影響が生じないことを確認したうえで、情報セキュリティ管理者の許可に基づき接続しなければならない。 イ 情報基盤管理者及び業務システム管理者は、接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。情報基盤管理者及び業務システム管理者は、当該外部ネットワークの瑕疵により本市のデータの漏えい、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応するため、必要に応じて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するよう努めなければならない。 ウ 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、適用範囲における情報資産に脅威が生じるおそれがある場合には、情報基盤管理者及び業務システム管理者は当該外部ネットワークとの接続を物理的に遮断することができるものとする。
7.2.10 ネットワーク機器の自動識別	情報基盤管理者及び業務システム管理者は、適用範囲におけるネットワークで使用される機器について、機器固有情報等によって端末とネットワークとのアクセスの可否が自動的に識別されるよう必要に応じてシステムを設定しなければならない。
7.2.11 ログイン試行回数の制限等	情報基盤管理者及び業務システム管理者は、ログイン試行回数の制限及びアクセスタイムアウトの設定等により、正当なアクセス権を持たない職員等情報取扱者が利用できないようにシステムを設定するよう考慮しなければならない。
7.2.12 パスワードに関する情報の管理	ア 情報基盤管理者及び業務システム管理者は、職員等情報取扱者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。また、職員等情報取扱者のパスワードを発行する場合において、仮のパスワードを発行する場合、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。 イ 情報基盤管理者及び業務システム管理者は、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、これを活用しなければならない。 ウ 情報基盤管理者及び業務システム管理者は、仮のパスワードも含めパスワードを発行する場合、パスワードの長さは十分な長さとし、文字列は他者が想像しにくいものとする。 エ 情報基盤管理者及び業務システム管理者は、パスワードは定期的又は一定のアクセス回数経過後に変更しなければならない。その場合には古いパスワードの再利用は行わないようにしなければならない。
7.4 コンピュータウイルス等不正プログラム対策	
7.4.2 情報基盤管理者等の実施事項	情報基盤管理者、業務システム管理者及び情報管理者は、次の事項を実施しなければならない。 ア 所管するサーバ及び端末に、コンピュータウイルス等対策ソフトウェアを常駐させる。 イ 情報システムにおいて電子記録媒体を使用する場合、本市が管理しているものを職員等情報取扱者に使用させるとともに、当該媒体の使用にあたり、ウイルスチェックを行わせる。 ウ コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保つ。インターネットに接続していないシステムにおいても、定期的に当該ソフトウェア及び定義ファイルの更新を行う。
7.5.4 内部からの不正アクセスの監視	情報基盤管理者及び業務システム管理者は、職員等情報取扱者が使用している端末からの庁内のサーバ等に対する不正アクセスや外部のサイトに対する不正アクセスを監視しなければならない。
7.5.5 職員等による不正アクセス時の措置	職員等情報取扱者による不正アクセスがあった場合、情報基盤管理者及び業務システム管理者は当該職員等情報取扱者が所属する課の情報管理者に通知し、適切な措置を求めなければならない。

(オ) 運用面のセキュリティ

情報セキュリティポリシーの遵守状況の確認等，情報セキュリティポリシーの運用面の対策を講じている。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。主な対策は，第 11-6 表のとおりである。

第 11-6 表　主な運用面のセキュリティ対策

主な項目	主な対策
8.1 情報システムの監視	
8.1.3 常時監視	情報基盤管理者及び業務システム管理者は、外部と接続するシステムを稼働中、常時監視しなければならない。
8.4 緊急時の対応	
8.4.1 緊急時対応計画の策定	情報基盤管理者及び業務システム管理者は、情報資産への重大な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、緊急時対応計画を策定しなければならない。
8.4.2 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、次の内容を定めなければならない。 ア 関係者の連絡先 イ 意思決定の所在 ウ 発生した事象に係る報告すべき事項 エ 発生した事象への対応措置 オ 再発防止措置の策定
8.4.3 緊急時対応計画の見直し	情報基盤管理者及び業務システム管理者は、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を見直さなければならない。

参考４　「ＰＣ統合管理システム」登録パーソナルコンピュータでの事務処理用ソフトウェアの使用について（平成 20 年 12 月 10 日　個人情報保護審議会諮問時の情報化推進部作成資料）

【参　考】

庁内における「ＰＣ統合管理システム」と今回諮問類型の位置づけについて

〔Ａ〕特定業務専用パソコン…以下の３種類に分類される。

- （Ａ１）特定業務用パソコン…特定の業務のみを遂行するために構築されたシステムとして特化され利用されるパソコン
- （Ａ２）設備管理用パソコン…各種施設・設備等を制御・管理するため，それら施設・設備等の一部として利用されるパソコン
- （Ａ３）市民用パソコン……もっぱら市民の方に利用していただくパソコン

〔Ｂ〕事務処理用汎用パソコン…特定業務専用として利用されるパソコン以外の全てのパソコンであり，不特定多数の業務に使用できるように市販の文書作成，表計算及びデータベース・ソフトウェアが標準装備されている。更に，ＰＣ統合管理システム上で稼働する各種特定業務用システムにも利用される。

ＰＣ統合管理システム	対象		対象外		
パソコン分類	Ｂ		Ａ１	Ａ２	Ａ３
機能・用途	不特定多数の業務に係る一般的な事務処理	特定業務用システム（汎用）	特定業務用システム（特化）	設備管理用システム	市民が利用するために設置
個人情報の電子計算機処理の形態	市販の文書作成，表計算又はデータベース管理用のソフトウェアを使用して，職員が他の職員とは電磁的記録を共有せずに単独で行う	特定の業務処理に特化した専用のソフトウェアを導入して，業務所管課の複数の職員が電磁的記録を共有しながら行う		個人情報は取扱わない	
電子計算機処理の例	研修・講座等の講師・受講生，審議会等の委員，刊行物の送付先，表彰の対象者，寄付等の申出者，アンケートの応募者等の名簿の作成・管理	・データやプログラムを格納したサーバへアクセスして処理を行うシステム（広聴事務システム，母子保健情報システム等） ・パソコン自体にデータやプログラムを持ち，当該パソコンを直接操作して処理を行うシステム	住民基本台帳システム，税務システム，介護保険システム等	プラント制御や地下鉄運行管理，研究所における試料分析・測定装置の制御・分析	各種案内等の閲覧・申し込み，パソコン研修等の利用
今後の取扱案	類型承認により今後は個別の諮問は不要	これまでどおり個別に審議会に諮問		審議会の諮問対象外	

参考５　セキュリティへの脅威とセキュリティ対策

セキュリティへの脅威		セキュリティ対策			
		直接的対策	効果	間接的対策	効果
第三者からの脅威	(1)機密性の喪失	アクセス管理 暗号化	防止	ワクチンプログラム セキュリティ監視 セキュリティ監査　他	検知 予防
	(2)完全性の喪失	アクセス管理 暗号化	防止	ワクチンプログラム セキュリティ監視 セキュリティ監査　他	検知 予防
	(3)可用性の喪失	アクセス管理	防止	ワクチンプログラム セキュリティ監視 セキュリティ監査　他	検知 予防
取引相手からの脅威	(4)証拠性の喪失	デジタル署名 (電子捺印)	防止 検知		
	(5)不正コピー			電子透かし	検知 予防

（出典）佐々木良一「インターネットセキュリティ入門」（岩波新書）

１．アクセス管理

(1)ユーザ認証

ユーザ ID，パスワードなどによってユーザの識別，認証を行い，ホストやアプリケーションシステムへのアクセス（ログイン）を制御する。

（ユーザ認証技術）

ア)本人の知識を利用するもの　　：暗証番号，パスワードなど

イ)本人の持ち物を利用するもの　　：磁気カード，ＩＣカードなど

ウ)本人の身体的特徴を利用するもの：指紋，声紋，虹彩，網膜パターン，筆跡，DNA など

(2)アクセス制御

何らかの識別情報に基づいて情報資産に対する権限がある者とない者とを区別し，前者に対してのみそれを許可する仕組み。

ただし，ユーザ認証に失敗し他人に成りすまされたり，セキュリティホールを利用して侵入された場合は無力となる。

①アクセス制御技術（任意，強制）

セキュリティレベルの異なる複数のネットワークセグメント間において，設定されたルールに基づいて通過（中継）を許可あるいは拒否するパケットやフレームを判別し，制御する。

ア）ファイアウォール（サブネットワークの入り口でブロック）

インターネットからの攻撃や不正アクセスから組織内部のネットワークを保護するためのシステムで，あらかじめ設定されたルールに従い，パケットの中継可否を制御するとともに，結果をログに記録する。

○アクセス制御

組織外と組織内との間で転送されるデータや，利用ユーザ，アクセス対象コンピュータなどの制限を実施する。

○認　証

利用ユーザやパソコンなどが，アクセスが認められたユーザやコンピュータであるかを確認する。

○監　視

ネットワーク上のトラフィック量や，ルータ，コンピュータの使用状況，アクセスログなどを監視する。

○暗号化

近年，転送データやパスワードの暗号化を行う製品もある。ファイアウォール間を暗号化して安全に通信することにより，インターネットをあたかも専用網のように使う機能をＶＰＮ（Virtual Private Network）という。

２．暗号化

何らかの意味のある文字や記号などを，①「ある定められた約束事」（暗号アルゴリズム）に従い，②「固有の値」（暗号鍵，復号鍵）を用いて，他の文字や記号などに変換（暗号化）する。

ファイル内のデータを暗号化したり，通信上（ネットワーク上）のデータを暗号化したりする。

(1)主な暗号方式

ア)共通鍵暗号

暗号化用の鍵と復元用の鍵が同じか容易に類推できる暗号方式

イ)公開鍵暗号

暗号化用の鍵と復元用の鍵が異なり，同時に生成された一対の鍵のうち一方を公開鍵として公開し，他方を秘密鍵として厳重に管理する。一方から他方への類推が実質的に不可能な暗号方式

３．ワクチンプログラム

システム管理者は，最新のワクチンプログラムの自動配布，企業情報ネットワーク入り口での侵入防止，社内におけるウイルス被害の監視などを行う。

(1)ワクチンプログラムの適切な実行

ア)基本機能

・ウイルス検査機能：既知ウイルスの検出

・ファイルの変更チェック機能：未知ウイルスの検出

・修復機能：発見したウイルスの駆除

・百科事典機能：発見したウイルスの詳細の調査

(2)OS や応用ソフトのセキュリティパッチ対策

パッチ（ソフトウェアの出荷後に発見された問題などを修正するためのプログラム）の適用

４．セキュリティ監視

(1)セキュリティ監視

ア)ログ解析

OS，アプリケーション，通信機器などが，稼働状態，処理の実行状況，障害・異常の発生状況などについて出力した記録（ログ）を解析し，問題箇所を修正する。

イ)侵入検知システム（IDS）

ネットワークやホストで発生している事象をリアルタイムに監視して侵入や攻撃を検知し，管理者に通知するなどのアクションを実行する。

①ネットワーク型侵入検知システム（NIDS：通信路の稼働状態を監視）

監視専用の機器（センサ）を監視対象となるネットワークセグメントに接続して使用する。センサは，接続されたネットワークを流れるパケットをリアルタイムに監視し，あらかじめ設定されたルールに基づいて不正アクセスや不審な事象を検知する。

②ホスト型侵入検知システム（HIDS：コンピュータの稼働状態を監視)）

監視対象となるホスト（Web サーバ，DB サーバ，メールサーバ等）にインストールして使用する。インストールされたホストに常駐して発生している事象をリアルタイムに監視し，あらかじめ設定されたルールに基づいて不正な操作やファイルの改ざんなどを検知する。

ウ)侵入防御システム（IPS）

従来の NIDS をインライン接続することで，NIDS と同等の侵入検知機能と，NIDS よりも強力な防御機能を備えたシステムである。

(2)セキュリティ検査

ネットワークを介して擬似的な侵入や攻撃を試みて，OS，アプリケーション，ネットワークを含めたサイト全体の脆弱性(セキュリティホール等)の有無やその内容を確認する。

専用のサーバを用いて外部から実施するものと対象となるコンピュータの中に検査機能を持つソフトを載せて検査を実施するものがある。

５．セキュリティ監査

システム監査をセキュリティに特化したもので，セキュリティ管理基準で決められた対策をきちんとやっているかどうかをチェックするものである。

監査法人が実施したり，専門のセキュリティ監査組織が実施したりする。

参考６　用語解説

出典）総務省　国民のための情報セキュリティサイト　用語辞典
情報セキュリティスペシャリスト 2016 年度版　　など

アクセス制御

コンピュータセキュリティにおいて，ユーザがコンピュータシステムの資源にアクセスすることができる権限・認可をコントロールすることをいい，典型的にはオペレーティングシステムにおいてアクセスコントロールリストとして実装される。

ゲートウェイ（gateway：GW）

通信手順（プロトコル）が異なる二者間やネットワーク間の通信を中継する機器やソフトウェア，システムの一種で，最上位層のプロトコルの違いに対応できるもの。

脆弱性（ぜいじゃくせい）

コンピュータやネットワークにおいて，情報セキュリティ上の問題となる可能性がある弱点のこと。 多くの場合は，OS やソフトウェアのセキュリティホールが脆弱性となる。また，設定ミスや管理体制の不備なども脆弱性のひとつとなることがある。これらの脆弱性が具体的な脅威と結び付くと，情報セキュリティのインシデント（事件・事故）が発生してしまうことになる。

セキュリティホール

OS やソフトウェアにおいて，情報セキュリティ上の欠陥となる不具合のこと。脆弱性とも呼ばれる。

デジタル署名

PKI 技術を用いて文書ファイルなどに電子的な署名を行うことで，その文書が間違いなく本人が発信したものであり，かつ途中で改ざんされていないことを証明する技術。

ドメイン

ネットワーク上の複数のコンピュータを管理するためのグループや組織を表す言葉。

パッチ

完成したプログラムに対して，脆弱性などをなくすために後から配布される修正プログラムのこと。 メーカーのホームページなどで提供される。

ファイアウォール（Fire Wall）

外部のネットワークと内部のネットワークを結ぶ箇所に導入することで，外部からの不正な侵入を防ぐことができるシステムのこと。またはシステムが導入された機器。

ファイルサーバ（File server）

ファイルを保存して，ファイル共有の機能を提供するコンピュータのこと。 企業や組織では，共有する

文書ファイルを保管するために利用している。

フォレンジック調査

PC のハードディスクから犯罪の証拠となるメールやドキュメントファイルを特定したり，サーバのログファイルから不正アクセスの記録を見つけ出すこと。

マルウェア

マルウェアとは，「Malicious Software」（悪意のあるソフトウェア）を略したもので，さまざまな脆弱性や情報を利用して攻撃をするソフトウェア（コード）の総称。コンピュータウイルスと同じ意味で使われているが，厳密にはさらに広義な用語として使われている。

（マルウェアの主な種類）

ウイルス

他のコンピュータに勝手に入り込んで，意図的に何らかの被害を及ぼすように作られたプログラムのこと。

ワーム

他のファイルに寄生して増殖するのではなく，自分自身がファイルやメモリを使って自己増殖を行うタイプのウイルスのこと。

スパイウェア

利用者の使用するコンピュータから，インターネットに対して個人情報やコンピュータの情報などを送信するソフトウェアのこと。

ボット

コンピュータを外部から遠隔操作するためのコンピュータウイルスの一種。

キーロガー

キーボードからの入力を記録するソフトウェア。

トロイの木馬

コンピュータの内部に潜伏して，システムを破壊したり，外部からの不正侵入を助けたり，そのコンピュータの情報を外部に発信したりするプログラム。

ルータ

セグメントと呼ばれるネットワークの単位にネットワークを分割する装置のこと。もしくは，別のセグメントのネットワークへ通信する際の経路情報の管理を行う装置のこと。 ルータは，ネットワークをセグメントに分割することで，セグメント外に不要な通信を流さない役割を担う。また，個々のコンピュータ自身で通信する相手の経路情報を管理させないため，ルータを使うことで，効率的な通信が実現される。

ログ

コンピュータが保有するユーザの接続時刻や処理内容などを記録したファイル。 通常は，ログを参照することで，コンピュータが正常に動作しているかどうかを管理することができる。