成田市情報セキュリティポリシー

平成１６年４月１日　策定

成田市 IT 推進本部

＜ 目　　次 ＞

序　成田市情報セキュリティポリシーの構成

情報セキュリティポリシーとは、成田市が所掌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、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、成田市が所掌する情報資産に関する業務に携わる全職員、非常勤、臨時職員(以下、「職員等」という。)及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

情報セキュリティ基本方針

情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする(下表参照)。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

第１章　成田市情報セキュリティ基本方針

１　目的

成田市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産及び情報資産を取り扱うネットワーク及び情報システムを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、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが成田市に対する市民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなっている。成田市が電子自治体を構築するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、成田市の情報資産の機密性、完全性及び可用性(注)を維持するための対策(情報セキュリティ対策)を整備するために成田市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については成田市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

(注)：国際標準化機構(ISO)が定めるもの(ISO7498-2：1989)

機密性(confidentiality)：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性(integrity)：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性(availability)：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２　定義

(1) ネットワーク

成田市における各部課、各行政委員会、消防、及び各関連施設等を相互に接続するための通信網、その構成機器(ハードウエア及びソフトウエア)及び記録媒体で構成され、処理を行う仕組みをいう。

(2) 情報システム

電子計算機(ネットワーク、ハードウェア及びソフトウェア)及び記録媒体で構成され、処理を行う仕組みをいう。

(3) 情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及

び情報システムで取り扱う全ての情報をいう。

なお、情報資産には紙等の有体物に出力された情報も含むものとする。

(4) 情報セキュリティ

情報資産の機密の保持及び正確性､完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

３　情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

情報セキュリティポリシーは、成田市が所掌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、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、成田市長をはじめとして成田市が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

４　情報セキュリティ管理体制

成田市の情報資産について、幹部が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

５　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

６　情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

・ 部外者の侵入による機器又は情報資産の破壊・盗難、故意の不正アクセス又は不正操作による機器又は情報資産の破壊・盗聴・改ざん・消去等

・職員等又は外部委託事業者による機器又は情報資産の持出、誤操作、アクセスのための認証情報又はパスワードの不適切管理、故意の不正アクセス又は不正行為による破壊・盗聴・改ざん・消去等、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏洩等

・コンピュータウイルス、地震、落雷、火災等の災害並びに事故、故障等によるサービ

ス及び業務の停止

７　情報セキュリティ対策

上記６で示した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ずるものとする。

(1) 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

(2) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め､全ての職員等及び外部委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

(3) 技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため､情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

８　情報セキュリティ対策基準の策定

成田市の様々な情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

９　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を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、各部課等の長が、所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより成田市の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。

10　評価及び見直しの実施

情報セキュリティ対策基準に定める事項の検証及び評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシー対策基準の見直しを実施する。

第２章　成田市情報セキュリティ対策基準

成田市情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための成田市行政全般の情報資産に関する情報セキュリティ対策の基準である。

１　対象範囲

この情報セキュリティポリシーが対象とする行政機関の範囲は、成田市役所各部課、各行政委員会、消防及び関連各施設等のネットワーク接続機関とする。

２　組織・体制

成田市の情報セキュリティ管理については、以下の組織・体制とする。

- 最高情報統括責任者　【助　役】
- ネットワーク管理者　【総務部長】
- 統括情報セキュリティ責任者　【各部長】
- 情報セキュリティ責任者　【各課等の長】
- 情報システム管理者　【情報システム担当課長】
- 情報システム担当者　【情報システム担当課の職員】
- 成田市 IT 推進本部

３　情報資産の分類と管理

(1) 情報資産の管理責任

ア　管理責任

・情報資産は、当該情報資産を作成した各課等の情報セキュリティ責任者が管理責任を有する。

イ　利用者の責任

・情報資産を利用する者は、情報資産の分類に従い利用する責任を有する。

ウ　重要性の効力

・情報資産が複製又は伝送された場合には、当該複製等も分類に基づき管理しなければならない。

(2) 情報資産の分類と管理方法

ア　情報資産の分類

・対象となるネットワーク及び情報システムの情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

重　要　性　分　類	
レベル　IV	個人情報及びセキュリティ侵害が本市の住民の生命、財産等へ重大な影響を及ぼす情報
レベル　III	公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
レベル　II	外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に軽微な影響を及ぼす情報。
レベル　I	上記以外の情報。

イ　情報資産の管理方法

(ｱ) 行政情報の管理及び取扱い

・行政情報の重要性分類に従い、パスワード等によるアクセス制限及び暗号等による通信内容の秘匿を行わなければならない。

・重要性分類レベルIII以上の行政情報は、原則として複製や、送付・送信は行ってはならない。但し、業務上必要な場合には、情報セキュリティ責任者の許可を得た上で行政情報の複製・送付・送信を行わなければならない。

(ｲ) 記録媒体の管理

・重要性分類レベルIII以上の行政情報を記録した取り外し可能な記録媒体は、外部からの脅威にさらされないよう施錠ができるなど特に安全な場所に保管しなければならない。また、保管状況等を記録しなければならない。

・重要性分類III以上の行政情報を記録した記録媒体を送る場合は、職員又は守秘義務を明記した契約を締結した外部業者に行わせるとともに、記録媒体の物理的な保護措置を講じなければならない。

(ｳ) 情報資産の変更又は廃棄の管理

・記録媒体が不要となった場合は、当該媒体に含まれる重要な情報資産(重要性分類レベルIII以上)は、情報資産を復元できないように消去を行ったうえで廃棄しなければならない。

・重要な情報資産(重要性分類レベルIII以上)を記録した記録媒体の廃棄は、情報セキュリティ責任者の許可を得ることとし、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。

４　物理的セキュリティ

(1) サーバ等

ア　装置の取付け等

・ネットワーク及び情報システムの取付けを行う場合は、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な固定等必要な措置を施さなければならない。
・重要な情報資産(重要性分類レベルIII以上)を格納しているサーバは、ミラーリング等によるデータの二重化を図るなど、障害発生時に対応できるよう措置を講じなければならない。
・ネットワーク管理者、情報システム管理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容易に操作できないように、利用者の ID、パスワードの設定等の措置を施さなければならない。
・無線 LAN の導入に当たっては、重要性分類レベルIII以上の情報資産を送信する際には経路を暗号化する等、十分な漏洩防止策を実施しなければならない。

イ　電源

・サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。
・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施さなければならない。

ウ　配線

・配線は、損傷等を受けることがないように可能な限り必要な措置を施さなければならない。
・主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。
・ネットワーク接続口(ハブのポート等)は、他の者が容易に発見できない場所に設置しなければならない。

エ　外部に設置する装置

・外部に設置する装置は、最高情報統括責任者の承認を受けたものでなければならない。また、最高情報統括責任者は、必要に応じて当該装置の情報セキュリティの水準について確認しなければならない。

(2) 管理区域

ア　管理区域

・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、当該機器等又は重要性分類レベルIII以上の情報資産の管理並びに運用を行うための部屋(以下「管理区域」と

いう。)は、水害対策及び確実な入退室管理を行えるような場所に設置しなければならない。また、外部からの侵入が容易にできないような管理区域としなければならない。

・管理区域は、鍵、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。

・管理区域内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を施さなければならない。なお、管理区域内の機器類の配置は、緊急時に職員等が円滑に避難できるように配慮しなければならない。

・消火剤は機器及び記録媒体に影響を与えるものであってはならない。

イ　管理区域の入退室管理

・管理区域の入退室は許可された者のみとし、IC カード等による入退室管理又は入退室管理簿の記載を行い、職員等及び外部委託事業者は身分証明書等を携帯し、求めにより提示しなければならない。

ウ　機器等の搬入・搬出

・管理区域へ機器等を搬入する場合は、あらかじめ当該機器等の安全性について、職員による確認を行わなければならない。

・機器等の搬入には職員が同行する等の必要な措置を施さなければならない。

(3) ネットワーク

・外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

・ネットワークに使用する回線は、伝送途上において破壊、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が実施されたものでなければならない。

(4) 職員等の端末等

・情報システムの執務室等の端末については、盗難防止のためのワイヤーによる固定等、盗難防止のための物理的措置を施さなければならない。

5　人的セキュリティ

(1) 役割・責任

ア　最高情報統括責任者

・最高情報統括責任者は、成田市における全てのネットワーク、情報システム、情報資産及び情報セキュリティに関する最終決定権限及び責任を有する。

イ　ネットワーク管理者

・ネットワーク管理者は、成田市のすべてのネットワークにおける情報セキュリティに関する責任者である。

・ネットワーク管理者は、成田市の全てのネットワークにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

・ネットワーク管理者は、成田市の情報資産に対する侵害又は侵害のおそれのある場合には、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全ての措置を行う権限及び責任を有する。

・ネットワーク管理者は、成田市の全てのネットワーク、情報システム及び情報資産に関する情報セキュリティ対策基準の維持・管理を行う。

ウ　統括情報セキュリティ責任者

・各部の長、各行政委員会等事務局の長、消防長を、その部等の情報セキュリティに関する総括的な権限及び責任を有する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、所掌に属する部等における情報セキュリティに関する統括的な権限及び責任を有する。

・統括情報セキュリティ責任者は、所掌に属する部等において担当している情報システムの追加・変更の承認等を行う。

・統括情報セキュリティ責任者は、所掌に属する部等において情報セキュリティポリシーの遵守に関し、教育、指示及び助言を行う。

エ　情報セキュリティ責任者

・各課等の長、各出先機関の長、各行政委員会事務局の長及び消防本部の各課の長を、その所管組織の情報セキュリティに関する権限及び責任を有する情報セキュリティ責任者とする。

・情報セキュリティ責任者は、統括情報セキュリティ責任者の下、所管組織内における情報セキュリティポリシーの遵守に関する権限と責任を有する。

・情報セキュリティ責任者は、所掌する事務の情報セキュリティ維持のため実施手順を定める。

・情報セキュリティ責任者は、所掌に属する課室等における情報資産に対する侵害又は侵害の恐れのある場合には、最高情報統括責任者及びネットワーク管理者へ速やかに報告を行い、指示を仰がなければならない。

この場合、最高情報統括責任者及びネットワーク管理者に報告した後、速やかに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。

オ　情報システム管理者

・情報システムの担当課長を情報システム管理者とする。

・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、更新等を行う権限及び責任を有する。

・情報システム管理者は、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。

カ　情報システム担当者

・情報システム担当者は、担当する情報システムに関して、情報システム管理者の指示等に従い、開発、設定の変更、運用、更新等の作業を行う。

キ　成田市 IT 推進本部

・成田市の情報セキュリティの維持管理を統一的な視点で行うため、IT 推進本部において、情報セキュリティポリシーの策定等の情報セキュリティに関する重要な事項を審議する。

ク　職員

(ｱ) 情報セキュリティ対策の遵守義務

・全ての職員は、情報セキュリティポリシー及び職員向け実施手順に定められている事項を遵守しなければならない。

・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については、速やかに情報セキュリティ責任者に相談し、指示等を仰がなければならない。

(ｲ) その他

・全ての職員は、使用する端末や記録媒体について、第三者に使用されること、又は許可なく情報資産を閲覧されることがないように、適切な措置を施さなければならない。

・全ての職員は、情報セキュリティ責任者の許可を得ず、端末等を執務室外に持ち出してはならない。

・全ての職員は、異動、退職等により業務を離れる場合には、知り得た情報資産を秘匿しなければならない。

ケ　非常勤及び臨時職員

(ｱ) 情報セキュリティ対策の遵守義務

・全ての非常勤及び臨時職員は、情報セキュリティポリシー及び職員向け実施手順に定められている事項を遵守しなければならない。

・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については、速やかに情報セキュリティ責任者に相談し、指示等を仰がなければならない。

(ｲ) 非常勤及び臨時職員の雇用及び契約

・非常勤及び臨時職員には、雇用及び契約時に必ず情報セキュリティポリシーのうち、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。

・非常勤及び臨時職員には、雇用及び契約の際、必要な場合は情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。

(ｳ) その他

・全ての非常勤及び臨時職員は、使用する端末や記録媒体について、第三者に使用されること又は許可なく情報資産を閲覧されることがないように、適切な措置を施さなければならない。

・全ての非常勤及び臨時職員は、情報セキュリティ責任者の許可を得ず、端末等を執務室外に持ち出してはならない。

・全ての非常勤及び臨時職員は、異動、退職等により業務を離れる場合には、知り得た情報資産を秘匿しなければならない。

コ　外部委託に関する管理

・情報システムの開発・保守・運用管理等を外部事業者に委託する場合は、情報セキュリティポリシーのうち外部委託事業者が守るべき内容の遵守及びその守秘義務を明記した契約を締結し、その遵守を管理しなければならない。

・重要性分類レベルIII以上の情報資産に関しては、情報システムにおける取り扱いのみでなく、外部施設との搬入出時においても情報資産を暗号化、又は認証等アクセス制限を施したうえで、盗難、不正コピー等の防止を厳重に実施する旨を契約書に明記しなければならない。

(2) 研修

・最高情報統括責任者は、全ての職員等及び関係する者に対し情報セキュリティポリシーについて研修しなければならない。

・最高情報統括責任者は、一般職員とは別に、ネットワーク管理者、統括情報セキュリティ責任者、情報セキュリティ責任者、情報システム管理者及び情報システム担当者に対して、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研修を実施しなければならない。

・情報システム管理者及び情報システム担当者は、情報システムに関する研修を受けなければならない。

・職員等は、定められた研修に参加し情報セキュリティポリシー及び実施手順を理解し、情報セキュリティ上の問題が生じないようにしなければならない。

(3) 事故、欠陥に対する報告

・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には、速やかにネットワーク管理者に報告し、ネットワーク管理者の指示に従い必要な措置を講じなければならない。また、別途、職員等は、情報セキュリティ責任者に報告し、情報セキュリティ責任者は、報告のあった事故等について全て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。

・職員等は、成田市が管理するネットワーク及び情報システムに関する事故、欠陥に関する住民からの報告・連絡を受けた場合には、速やかにネットワーク管理者に報告し、ネットワーク管理者の指示に従い必要な措置を講じなければならない。また、職員等は、情報セキュリティ責任者に報告し、情報セキュリティ責任者は、報告のあった事故等について全て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。

・ネットワーク管理者は、これらの事故等を分析し、再発防止のための情報資産として記録を保存しなければならない。

(4) アクセスのための認証情報及びパスワードの管理

ア　IC カード等の管理

・職員等は、自己の管理する IC カード等について、所有者本人が厳重に保管しなければならない。

イ　パスワードの管理

・職員は、自己の保有するパスワードについて、不用意にもらしたりメモを作ったりしないようにするなど、パスワードの秘密保持に努めなければならない。

・職員は、ＩＤカードを他の者の目に触れないようにするなど、適切に管理しなければならない。

６　技術的セキュリティ

(1) ネットワーク、情報システム及び情報資産の管理

・情報資産の重要性分類に従ってネットワーク、情報システム及び情報資産を以下のとおり管理する。

ア　情報資産の重要性分類レベルIII以上

・情報システム管理者は、重要性分類レベルIII以上の情報資産が記録されたサーバ等について、アクセス記録及びセキュリティ関連障害に関する記録を取得し、一定の期間保存しなければならない。

・ネットワーク管理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等に関し、記録媒体の形態に関わりなく適切な保管をしなければならない。

・重要性分類レベルIII以上に属する情報資産は、暗号化、又は認証等のアクセス制限により、適切な管理を行わなければならない。特に、外部へ送信又は搬出する際には、必ずいずれかの方法をとらねばならない。

・緊急時に直ちに対処できるようにするため、最高情報統括責任者が定めた特に重要な情報システムは、ミラーリング等により常時バックアップしなければならない。また、最高情報統括責任者が定めた重要なネットワーク及び情報システムは、システムを二重化しなければならない。

・情報システム管理者は、情報システムのミラーリング等に関わりなく情報資産の重要度に応じて期間を設定し、定期的に情報資産のバックアップ用の複製を取らなければならない。

・情報システム管理者は、閲覧権限がない職員等が所管するシステムにアクセスすることが不可能となるように、システム上制限しなければならない。

・外部の者が利用できるシステムにおいては、必要に応じ他のネットワーク及び情報システムと物理的に分ける等、情報セキュリティ対策について特に強固に対策をとらなければならない。

イ　情報資産の重要度分類レベルII以下

・原則、重要性分類レベルIII以上に分類される情報資産の管理に準拠するが、重要性分類レベルII以下の情報資産は公開を前提としているため、この範囲において基準を緩和することができる。

・Web サイトにより情報を公開・提供する場合には、当該サイトに係るシステムにおいて盗難、改ざん、消去、踏み台、DoS 等を防止しなければならない。

・メールシステム等においても、他のシステムに対する攻撃の踏み台とならないように

適切な管理を実施しなければならない。

(2) ネットワーク及び情報システムを使用する際の規定

ア　業務目的以外の使用の原則禁止

・職員等によるネットワーク及び情報システム等の使用は、業務目的に沿ったもののみが許可される。業務目的以外での情報システムへのアクセス、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。

イ　情報資産の持ち出し及びインターネット等による情報資産の送信禁止

・職員等は、重要性分類上レベルIII以上に該当する情報資産を取り扱う場合、原則として、下記の行為を行ってはならない。特に、重要性分類レベルIII以上に該当する情報資産のインターネットへの自動転送は厳禁する。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、かつ最高情報統括責任者の事前の了解を得た場合に限り、庁外への持ち出し又は庁外との送受信ができるものとする。

＊庁外への持ち出し
＊インターネット等による庁外との送受信
＊個人の所有する情報が記録された媒体の管理区域への持ち込み

ウ　無許可ソフトウエアの導入の禁止

・職員等は、各自に供用された端末等に対して、ネットワーク管理者が定める以外のソフトウエアの導入を行ってはならない。但し、外部からソフトウェアを取り入れる必要が生じた場合は，事前にネットワーク管理者の承認を受けることにより可能とする。

エ　機器構成の変更の禁止

・職員等は、情報システムの機器について、原則として改造又は機器の増設・交換を行ってはならない。但し、情報システムの機器について業務を遂行するため機器の増設・交換を行う必要がある場合には、情報システム管理者の許可を得なければならない。

・職員等は、モデム等の機器を増設して、他のネットワークへ接続を行う場合及び他のネットワークからアクセスを可能とする仕組みを構築する場合には、情報システム管理者の許可を得なければならない。情報システム管理者は、許可に当たって情報システム及び他の情報システムにセキュリティ上の問題を生じさせてはならない。

オ　情報及びソフトウエアの交換

・組織間において、情報システムに関する情報及びソフトウエアを交換する場合は、そ

の取扱いに関する事項をあらかじめ定め、ネットワーク管理者の許可を得なければならない。

カ　メール

・職員等は，メールの自動転送機能を用いて，業務上必要な者へ職場のメールを転送してはならない。

・職員等は，チェーンメールや不審メールを他者に転送してはならない。

・職員等は,差出人が不明なメールを受信した場合は,直ちに廃棄しなければならない。

キ　情報システムの入出力データ

・情報システムに入力されるデータは、適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

・情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されることを確認しなければならない。

ク 暗号化

・暗号化については、最高情報統括責任者が定める方法を用いなければならない。

・暗号のための鍵は、重要性分類レベルIVの行政情報として厳重に管理しなければならない。

ケ 職員以外の者が利用できる情報システム

・ネットワーク管理者は、職員以外の者が利用できる情報システムについては、特に強固な対策を取らなければならない。

コ その他

・職員等が利用できるプロトコルは、業務上必要最低限のものとする。

(3) アクセス制御

ア　利用者登録

・ネットワーク管理者及び情報システム管理者は、利用者の登録、変更、抹消、登録した情報資産の管理、異動や成田市外への出向等の職員等及び退職者における利用者 ID の取扱い等については、各情報システム毎に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・変更は、ネットワーク管理者に対する申請により行う。

イ　管理者権限

・ネットワークの管理者権限は、1 人の者に与え厳重に管理しなければならない。

・ネットワーク管理者の権限を代行する者は、ネットワーク管理者が指名し、最高情報統括責任者が認めた者でなければならない。代行者を認めた場合、最高情報統括責任者は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及び情報システム管理者に周知しなければならない。

・情報システムの管理者権限は、必要最小限の者に与え、厳重に管理しなければならない。

・情報システム管理者の権限を代行する者は、情報システム管理者が指名し、ネットワーク管理者が認めた者でなければならない。代行者を認めた場合、ネットワーク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セキュリティ責任者に周知しなければならない。

ウ　インターネット以外の外部ネットワークにおけるアクセス制御

・ネットワーク管理者は、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出来る者を定めなければならない。

・ネットワーク管理者は、外部ネットワークのサービスを使用する権限を有しない職員等が当該サービスを使用できるようにしてはならない。

エ　強制的な経路制御

・ネットワーク管理者は、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。

オ　外部からのアクセス

・外部からのアクセスの許可は、必要最低限にしなければならない。

カ　総合行政ネットワーク及び住民基本台帳ネットワークシステムとの接続

・総合行政ネットワーク及び住民基本台帳ネットワークシステムについては、当該接続において取り扱う情報資産の重要性を考慮し、適切なアクセス制御を実施する。

キ　外部ネットワークとの接続

・外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成及び情報セキュリティレベル等を詳細に検討し、本市の情報資産に影響が生じないことを明確に確認したうえで、ネットワーク管理者の許可に基づき接続しなければならない。

・ネットワーク管理者は、外部ネットワークとの接続を行うことでネットワークの安全性が脅かされることの無いようにセキュリティ対策に努めなければならない。
・接続した外部ネットワークの情報セキュリティに問題が認められた場合には、ネットワーク管理者は、速やかに当該外部ネットワークを物理的に遮断しなければならない。
・ネットワークの情報セキュリティに問題が認められた場合には、ネットワーク管理者は速やかに当該内部ネットワークを、外部ネットワークから遮断しなければならない。

ク　パスワードの管理方法

・ネットワーク管理者及びシステム管理者は、情報機器の ID、パスワードを厳重に管理しなければならない。
・ネットワーク管理者及びシステム管理者は、ネットワーク並びにネットワーク上で利用する各種サービスの ID、パスワードを適切に管理しなければならない。

(4) システム開発、導入、保守等

ア　情報システムの開発導入

・情報システム管理者は、情報システムのソフトウェアを開発・導入する場合は、情報セキュリティ上問題にならないかどうか、確認しなければならない。
・情報システム管理者は、情報システムのソフトウェアを開発する場合は、ソフトウェアの仕様書、ネットワーク構成図等を整備しなければならない。
・情報システム管理者は、開発したソフトウェアを情報システムに取り入れる場合は、既に稼動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　ネットワーク及び情報システムの更新

・ネットワークを更新する際は、更新の内容、必要性、計画等をネットワーク管理者に提出し承認を得なければならない。
・情報システムを更新する際は、更新の内容、必要性、計画等を情報システム管理者に提出し承認を得なければならない。
・重要な更新にあったては、それぞれ最高情報統括責任者に承認を得なければならない。

ウ　ソフトウエアの保守及び更新

・ソフトウエア等を更新、又は修正プログラムを導入する場合は、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。
・情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、速やかな対応を行うこととし、その他のソフトウエアの更新等については、計画的に実施しなければならない。

エ　機器の修理及び廃棄

・記憶媒体の含まれる機器について、外部の事業者に修理させ又は廃棄する場合は、可能な範囲でバックアップをとり、その内容が消去された状態で行わなければならない。

・故障を外部の事業者に修理させる際、情報資産を消去することが難しい場合は、修理を委託する事業者に対し秘密を守ることを契約に定めなければならない。また重要な機器については、復元不可能な廃棄を行わなければならない。

(5) コンピュータウイルス対策

ア　ネットワーク管理者は、次の事項を実施しなければならない。

・ウイルス情報について職員等に対する注意喚起を行うこと。

・常時ウイルスに関する情報収集に努めること。

・サーバ及び端末において、ウイルスチェックを行うこと。

・ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

イ　職員等は、次の事項を遵守しなければならない。

・外部からデータ又はソフトウエアを取り入れる場合には、必ずウイルスチェックを行うこと。

・差出人が不明又は不自然に添付されたファイルは速やかに削除すること。

・ウイルスチェックの実行を途中で止めないこと。

・ネットワーク管理者が提供するウイルス情報を常に確認すること。

・添付ファイルのあるメールを送受信する場合は、ウイルスチェックを行うこと。

(6) 不正アクセス対策

・攻撃を受けることが明確な場合には、ネットワーク管理者は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、関係機関との連絡を密にして情報の収集に努めなければならない。

・攻撃を受け、当該攻撃が不正アクセス禁止法違反等犯罪の可能性がある場合には記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

・職員等による不正アクセスがあった場合、ネットワーク管理者又は情報システム管理者は当該職員等が所属する課等の情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

(7) セキュリティ情報の収集

・ネットワーク管理者は、情報セキュリティに関する情報を収集し、成田市の全てのネ

ットワーク及び情報システムについてソフトウエアにパッチを当てる等、セキュリティ対策上必要な措置を講じなければならない。

・最高情報統括責任者は、これらの情報を定期的に取りまとめ、関係部課等に通知する。

7　運用

(1) 情報システムの監視

・情報システム管理者は、情報システムの運用にあたっては、常に情報システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。

(2) 情報セキュリティポリシーの遵守状況の確認

・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は、所管する部課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、また、運用上支障が生じていないかについて確認を行わなければならない。

(3) 障害時の対応

セキュリティ障害が発生した場合には、ネットワーク管理者及び情報システム管理者はすみやかに対応するとともに、再発防止の措置を講じなければならない。

ア　障害拡大の防止措置

・情報システム管理者は、故意の不正アクセス又は不正操作により情報システムに障害を及ぼすことが明らかな場合には、情報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。

・情報システム管理者は、情報システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録の保存に努めなければならない。

イ　障害の調査

(ｱ) 情報システム管理者は、セキュリティ障害が発生した場合、障害の発生を速やかにネットワーク管理者へ報告するとともに、次の項目について調査をしなければならない。

・障害の内容

・障害が発生した原因

・確認した被害、影響範囲

(ｲ) 調査した内容は速やかにネットワーク管理者へ報告しなければならない。ただし、障害の程度が軽微なものについては報告を要しないものとする

ウ　障害への対応

・情報システム管理者は、ネットワーク管理者の指示の下に速やかにセキュリティ障害を復旧し、その措置についてネットワーク管理者に報告しなければならない。
・障害が外部に重大な影響を及ぼすおそれがある場合には、ネットワーク管理者は速やかに最高情報統括責任者に報告のうえ必要な指示を仰がなければならない。

エ　再発防止の措置

・ネットワーク管理者は、必要な再発防止の措置を講じるとともに、その結果を最高情報統括責任者に報告しなければならない

８　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について、次の法令等を遵守しこれに従わなければならない。

○ 不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)
○ 著作権法(昭和 45 年法律第 48 号)
○ 個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）
○ 行政機関の保有する個人情報の保護に関する法律
（平成 15 年 5 月 30 日法律第 58 号）
○ 成田市情報公開及び個人情報保護に関する条例(平成 10 年 9 月 29 日条例第 24 号)

９　情報セキュリティに関する違反に対する対応

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に対しては、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。

なお、職員等に情報セキュリティポリシーに違反する行動がみられた場合には、速やかに次の措置を講じなければならない。

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

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ネットワーク管理者及び当該職員等が所属する課等の情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

情報セキュリティ責任者の指導によっても改善されない場合、ネットワーク管理者は、当該職員等のネットワーク又は情報システムの使用に関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、ネットワーク管理者は、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責任者に通知しなければならない。

10 評価・見直し

・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は、当該部課の情報セキュリティが確保されていることを確認するため、自主点検を行い、必要に応じ改善措置を講じなければならない。

・最高統括情報管理者は、評価及び見直しが必要となる事象が発生した場合には、「成田市ＩＴ推進本部」に諮り必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。