別紙２

新宿区情報セキュリティ対策基準

平成15年8月22日
15新企情第294号
改正　平成17年3月30日16新企情第1029号
平成18年3月30日17新総情第2275号
平成19年3月23日総情第2605号
平成19年5月24日19新総情第493号
平成20年2月26日19新総情第2815号
平成20年6月23日20新総合情第868号
平成24年4月30日24新総合情第141号
平成26年3月24日25新総合情第3605号
平成27年11月20日27新総合情第2678号

第1　総則

1　目的

この基準は、新宿区情報セキュリティ規則(平成15年新宿区規則第98号)に基づき情報セキュリティ対策を実施するに当たり、統一的に遵守すべき行為、判断等の基準を定めることを目的とする。

2　用語の定義

この基準において使用する用語の意義は、次に定めるものを除くほか、新宿区情報セキュリティ規則において使用する用語の例による。

(1)　課等　新宿区情報セキュリティ規則第8条第1項に規定する課等をいう。

(2)　庁舎　新宿区庁舎管理規則(昭和59年新宿区規則第39号)第2条に規定する庁舎、教育センター、中央図書館又は区立の学校をいう。

(3)　コンピュータウイルス　第三者のプログラム又はデータベースに対して、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等で、自己伝染機能、潜伏機能又は発病機能を有するものをいう。

(4)　情報セキュリティインシデント　情報セキュリティに関する障害、事故、故障及びシステム上の欠陥をいう。

3　情報資産に対する脅威

情報セキュリティ対策を行う上で、特に留意すべき情報資産に対する脅威は、次に掲

げる事項とする。

(1)　不正なアクセス又は誤操作による情報資産の破壊、持ち出し、盗聴、改ざん若しくは消去

(2)　構成機器、記録媒体又は帳票の破壊、紛失若しくは盗難

(3)　故意又は過失による情報の漏えい

(4)　コンピュータウイルス、地震、落雷、火災等による災害、情報セキュリティインシデント等による情報システムの停止

第2　情報資産の管理責任、重要性分類及び管理方法

1　情報資産の管理責任

(1)　情報資産の管理責任

情報資産を作成した課等の情報セキュリティ責任者は、当該情報資産を管理する責任を有する。

(2)　管理責任の及ぶ範囲

情報資産を複製し、又は伝送した場合においては、当該複製され、又は伝送された情報資産を保有することとなった課等の情報セキュリティ責任者が管理する責任を有する。

(3)　利用者の利用責任

情報資産を利用する者(以下「利用者」という。)は、当該情報資産を3の情報資産の重要性分類に基づき利用する責任を有する。

2　リスク管理

情報資産を管理し、又は利用する課等の情報セキュリティ責任者は、その情報資産に対する脅威を分析し、当該脅威に係る影響を評価し、並びに当該脅威の顕在化を予防するための対策及び当該脅威が顕在化した場合に被害を最小化するための手順を定めるものとする。

3　情報資産の重要性分類

情報資産を作成した課等の情報セキュリティ責任者は、当該情報資産の機密性、完全性及び可用性(利用者が必要なときに情報資産にアクセスできることを確実にすること。)を踏まえ、当該情報資産を次に掲げる重要性分類に基づき分類し、目録を作成するものとする。

(1)　重要性分類Ⅰ

ア　区民の財産及びプライバシー等に重大な影響を及ぼす情報資産

イ　法令又は区の条例等により守秘されるものと規定されている情報資産

ウ　漏えいした場合、個人又は法人その他の団体の利益を害する等区に対する信頼を害するおそれのある情報資産

エ　滅失し、又はき損した場合、その復元が困難となり、区の円滑な執行を妨げるおそれのある情報資産

オ　情報システムに係るパスワード及び情報システムの設定情報

(2)　重要性分類Ⅱ

重要性分類Ⅰに分類される情報資産以外の情報資産

4　情報資産の管理方法

(1)　情報資産の重要性分類の表示

情報セキュリティ責任者は、情報資産の重要性分類の表示をしなければならない。この場合において、第三者が重要性分類の識別を容易にすることができないよう留意しなければならない。

(2)　情報資産の管理

ア　情報セキュリティ責任者は、2の情報資産の重要性分類に基づき、情報資産にアクセスする権限を有する者を定めなければならない。

イ　職員は、重要性分類Ⅰに属する情報資産を当該課等の情報資産が所在する場所から外部へ持ち出し、又は送信してはならない。ただし、当該情報資産の内容、使用目的、持出し方法、管理方法等を明確にした上で、当該情報資産を管理する情報セキュリティ責任者の承認を受けたときは、この限りでない。

ウ　職員は、支給されたもの以外の電子計算機、記録媒体等において、重要性分類Ⅰに属する情報資産を記録し、又は使用してはならない。

(3)　記録媒体の管理

ア　情報セキュリティ責任者は、情報資産を記録した媒体を適切に管理しなければならない。

イ　情報セキュリティ責任者は、最終的に確定した情報資産を記録した媒体については、書き込み禁止措置を講じた上で保管しなければならない。

ウ　情報セキュリティ責任者は、重要性分類Ⅰに分類される情報資産については、記録した媒体を施錠可能な場所に保管しなければならない。

(4)　情報資産の廃棄

職員は、重要性分類Ⅰに分類される情報資産が不要となった場合は、速やかに廃棄

しなければならない。この場合において、当該情報資産を記録した媒体を廃棄するときは、情報セキュリティ責任者の承認を受け、当該情報資産を完全に消去する等復元できないようにした上で、廃棄しなければならない。

第3　物理的な対策

1　サーバ等

(1)　機器等

ア　情報システム管理者は、ネットワーク及び情報システムの障害が発生した場合に情報システムの運用が停止しないよう、回線、機器等を冗長構成とする等の措置を講じるように努めなければならない。

イ　情報セキュリティ責任者は、ネットワーク管理者又は情報システム管理者が指定した職員並びに外部委託事業者及びその従業員以外の者が容易にネットワーク及び情報システムを操作できないような措置を講じなければならない。

ウ　サーバ等の重要な機器を設置する場合は、当該サーバ等について、次に掲げる情報セキュリティ対策を行わなければならない。

(ア)　設置及び利用場所が確定している電子計算機及び通信回線装置については、所定の設置場所から移動できない措置を講ずること。

(イ)　電子計算機及び通信回線装置については、不正操作されないための措置を講ずること。

(2)　配線

情報セキュリティ責任者は、配線について、損傷、盗聴、侵入等をされることがないように可能な限り必要な措置を講じなければならない。

(3)　庁舎以外の場所に設置する機器等

ア　情報セキュリティ責任者は、所管するネットワークに係る構成機器及び情報システムに係る電子計算機(以下「機器等」という。)を庁舎以外の場所に設置する場合は、新宿区情報化の推進に関する規則(平成20年新宿区規則第92号)第8条第1項の情報化統括管理者(以下「情報化統括管理者」という。)の承認を受けなければならない。

イ　ネットワーク管理者は、定期的に機器等における情報セキュリティについて確認しなければならない。

2　管理区域

(1)　管理区域の指定

情報セキュリティ責任者は、ネットワークに係る構成機器、重要な情報システム及び重要性分類Ⅰに分類される情報資産を適正に管理するために、次の表に定めるとおり、事務室等を指定する。

管理区域の区分	管理区域
管理区域Ⅰ	重要な電子計算機、通信回線装置等を設置するために独立して設けられた部屋又は区画で、関係者以外の侵入や自然災害の発生等を原因とする情報資産に対するセキュリティ侵害(以下「侵害」という。)に対して、施設及び環境面から対策が講じられているもの
管理区域Ⅱ	事務室等又はその内部であって、関係者以外の侵入や自然災害の発生等を原因とする侵害に対して施設及び環境面から対策が必要な区域で、管理区域Ⅰ以外のもの

(2) 管理区域の管理

ア 管理区域Ⅰを定めた情報セキュリティ責任者は、当該管理区域について、次の各号に掲げる措置を講じなければならない。

(ア) 入退室を、許可を受けた者に制限すること。

(イ) 鍵又は認証装置等により、入退室管理を行うこと。

(ウ) 入退室管理簿等により、入退室の記録を行うこと。

(エ) その他管理区域の情報セキュリティを保つために必要な措置

イ 管理区域Ⅱを定めた情報セキュリティ責任者は、管理区域に係る職員並びに外部委託事業者及びその従業員の出入りを適正に管理しなければならない。

ウ ア及びイのほか、情報セキュリティ責任者は、管理区域内における情報資産及び機器等に係る適切な情報セキュリティ対策を行わなければならない。

(3) 機器等の取得及び搬入等

ア 情報セキュリティ責任者は、機器等を取得する場合には、あらかじめ当該機器等のシステムとの適合性に関し、職員をもって確認しなければならない。

イ 情報セキュリティ責任者は、管理区域に機器等を搬入し、又は管理区域から機器等を搬出するときは、職員を立ち会わせる等必要な措置を講じなければならない。

3 ネットワーク

(1) 情報セキュリティ責任者は、実施機関等以外へのネットワークの接続をする場合は、情報化統括管理者の許可を得なければならない。この場合において、当該ネット

ワークの接続は、必要最低限のものにしなければならない。

(2) 情報セキュリティ責任者は、ネットワークを使用して情報資産を伝送するとき、その伝送の途上において当該情報資産に破壊、盗聴、改ざん、消去等の被害が生じないように情報セキュリティ対策を行わなければならない。

第4 人的な対策

1 職員の役割及び責任

(1) 職員は、使用する端末又は記録媒体を第三者に使用されること及び情報セキュリティ責任者の許可なく情報資産を第三者に閲覧されることがないように、適切な措置を講じなければならない。

(2) 職員は、情報セキュリティ責任者の承認を得ずに、機器等を庁舎外に持ち出してはならない。

(3) 職員は、他の組織に異動した場合においても、異動前の組織での業務において知り得た情報資産を他に譲渡し、若しくは貸与し、又は使用させてはならない。職員が退職等により職を離れた場合においても、同様とする。

第5 技術的な対策

1 ネットワーク、情報システム及び情報資産

(1) ネットワーク管理者は、重要性分類Ⅰに分類されるログ及び情報セキュリティの確保に必要な記録(以下「ログ等」という。)について、必要があると認める場合には、当該ログ等を所管している情報システム管理者に提出させるとともに、当該ログ等について、盗難、改ざん又は消去等を防止する措置を講じ、適切に保存しなければならない。

(2) ネットワーク管理者は、記録される媒体の形態にかかわらず、重要性分類Ⅰに分類されるネットワーク構成図及び情報システム仕様書等(以下「ネットワーク構成図等」という。)を適切に保管しなければならない。

(3) 情報システム管理者は、重要性分類Ⅰに分類される情報資産について、定期的にバックアップ用のデータを作製しなければならない。

2 ネットワーク、情報システム及び情報資産を使用する際の禁止等

(1) 業務目的以外の使用禁止

職員は、業務の目的以外のためにネットワーク又は情報システムを使用してはならない。

(2) 情報資産の持ち出し及びインターネットによる伝送の禁止等

ア　職員は、重要性分類Ⅰに分類される情報資産を取り扱う場合には、次に掲げる行為を行ってはならない。

(ア)　庁舎から庁舎以外の場所への持ち出し(ただし、当該情報資産を管理する情報セキュリティ責任者が許可したときは、この限りでない。)

(イ)　インターネットによる実施機関等以外への伝送(ただし、情報化統括管理者が許可したときは、この限りでない。)

イ　ア(イ)ただし書の規定による情報化統括管理者の許可に基づき情報資産を実施機関等以外へ伝送する場合は、電子署名、通信経路の暗号化、本人認証、パスワード設定等高度なセキュリティ対策を講じなければならない。

ウ　職員は、原則として、支給されたもの以外の記録媒体を管理区域Ⅰに持ち込んではならない。

(3)　無許可ソフトウェアの導入の禁止

ア　職員は、自己に供用された端末等に対し、情報システム管理者が定めるソフトウェア以外のソフトウェアを導入してはならない。

イ　職員は、情報システム管理者が定めるソフトウェアを導入する場合においても、その提供元の信頼性が確保できることを確認した上で、ソフトウェアを入手しなければならない。

(4)　構成機器の変更の禁止

職員は、自己に供用された端末等について、構成機器の増設又は改造を行ってはならない。

(5)　情報システムに関するネットワーク構成図等及びソフトウェアの貸与

情報セキュリティ責任者は、所管する情報システムに関するネットワーク構成図等又はソフトウェアを他の課等の情報セキュリティ責任者に貸与する場合には、当該貸与が著作権法その他の法令に抵触しないことを確認した上で行わなければならない。この場合において、当該情報セキュリティ責任者は、当該ネットワーク構成図等又はソフトウェアの取扱に関し、当該他の課等の情報セキュリティ責任者と協議の上、必要な事項について定めなければならない。

3　アクセス制御等

(1)　利用者登録

情報セキュリティ責任者は、所管する利用者の登録、変更又は抹消を記録した情報資産を適切に管理しなければならない。

(2)　ネットワークに対するアクセスの制限

ネットワーク管理者は、利用する権限を有しない職員によって不正にネットワークのサービスが利用されることがないよう適切にネットワークの管理を行わなければならない。

(3)　適切なネットワークの経路の制御

ネットワーク管理者は、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。以下「法」という。)第2条第4項に規定する不正アクセス行為を防止するため、ネットワークの経路を適切に制御しなければならない。

(4)　実施機関等以外からのアクセス

ネットワーク管理者は、実施機関等以外からのアクセスの許可を必要最低限にしなければならない。

(5)　実施機関等以外のネットワークとの接続

ネットワーク管理者は、実施機関等以外のネットワークと接続しようとする場合には、当該実施機関等以外のネットワークの構成、情報セキュリティのレベル等を詳細に検討し、情報資産及び機器等に影響が生じないことを確認しなければならない。

(6)　パスワード

情報セキュリティ責任者は、職員が使用するパスワードを、想像することが困難な文字列にする等適切な措置を講じなければならない。

(7)　特権を付与されたID

情報システム管理者は、特権を付与されたIDについて、可能な限り初期設定以外のものに変更しなければならない。

4　ネットワークの導入、開発、保守等

(1)　ネットワークの導入

ア　ネットワーク管理者は、既存のネットワークを新たに拡張し、又は他のネットワークに接続しようとする場合には、既存のネットワークに影響が生じないよう拡張又は接続する前に十分な試験を行わなければならない。

イ　ネットワーク管理者は、アの試験による結果の記録のうち重要なものを厳重に保管しなければならない。

(2)　ソフトウェアの導入及び変更

ア　ネットワーク管理者は、ソフトウェアを計画的に導入するとともに、導入に当たっては、当該ソフトウェアの適格性及び他のネットワークとの適合性について確認

しなければならない。

イ　ネットワーク管理者は、ソフトウェアについて情報セキュリティに重大な影響を及ぼすおそれのある不具合が発見された場合には、速やかに当該ソフトウェアの変更を行う等適切に対応しなければならない。

ウ　ネットワーク管理者は、イの場合のほか、ソフトウェアの変更については計画的に行わなければならない。

(3)　ネットワークの情報セキュリティインシデント及び不正行為への対策

ネットワーク管理者は、ネットワークの開発若しくは保守時の情報セキュリティインシデント又は不正行為に対する対策のため、必要な事項を別に定めなければならない。

(4)　ネットワークに関する外部委託事業者

ア　ネットワーク管理者は、新たにネットワークの開発を事業者に委託する場合は、情報の機密性に応じたセキュリティレベルが確保されていることを確認した上で、総務部契約管財課契約係に対し、当該事業者の経営状況等の調査を依頼し、当該開発の契約を適正に履行することが可能であるかどうかを確認しなければならない。

イ　ネットワーク管理者は、外部委託事業者の従業員が委託した業務に従事するときには、当該外部委託事業者の従業員であることを証する身分証明書を事前に提示させなければならない。

(5)　ネットワークの変更

ネットワーク管理者は、ネットワークに重要な変更を加える場合は、情報化統括管理者の承認を得なければならない。

(6)　構成機器の廃棄、返却及び修理

ア　ネットワーク管理者は、情報資産を記録した媒体が含まれる構成機器を廃棄する場合は、当該媒体に記録された情報資産を完全に消去する等復元できないようにした上で行わなければならない。賃貸業者に対し、賃貸した構成機器を返却する場合も、同様とする。

イ　ネットワーク管理者は、情報資産を記録した媒体が含まれる構成機器の故障について、事業者に委託して修理させる場合は、可能な限り当該媒体に記録された情報資産を消去するものとする。

(7)　管理記録

ネットワーク管理者は、ネットワークについて行った変更及び修理等の作業につい

ては、それらの作業記録を作成し、適切に管理しなければならない。

5　情報システムの導入、開発、保守等

(1)　情報システムの導入

ア　情報システム管理者は、既存の情報システムを新たに拡張し、又は他の情報システムに接続しようとする場合には、既存の情報システムに影響が生じないよう拡張又は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、アの試験による結果の記録のうち重要なものを厳重に保管しなければならない。

(2)　ソフトウェアの導入及び変更

ア　情報システム管理者は、ソフトウェアを計画的に導入するとともに、導入に当たっては、当該ソフトウェアの適格性及び他の情報システムとの適合性について確認しなければならない。

イ　情報システム管理者は、ソフトウェアについて情報セキュリティに重大な影響を及ぼすおそれのある不具合が発見された場合には、速やかに当該ソフトウェアの変更を行う等適切に対応しなければならない。

ウ　情報システム管理者は、イの場合のほか、ソフトウェアの変更については計画的に行わなければならない。

(3)　情報システムの情報セキュリティインシデント及び不正行為への対策

情報システム管理者は、情報システムの開発若しくは保守時の情報セキュリティインシデント又は不正行為に対する対策のため、必要な事項を別に定めなければならない。

(4)　情報システムに関する外部委託事業者

ア　情報システム管理者は、新たに情報システムの開発を事業者に委託する場合は、情報の機密性に応じたセキュリティレベルが確保されていることを確認した上で、総務部契約管財課契約係に対し、当該事業者の経営状況等の調査を依頼し、当該開発の契約を適正に履行することが可能であるかどうかを確認しなければならない。

イ　情報システム管理者は、外部委託事業者の従業員が委託した業務に従事するときには、当該外部委託事業者の従業員であることを証する身分証明書等を事前に提示させなければならない。

(5)　電子計算機の廃棄、返却及び修理

ア　情報システム管理者は、情報資産を記録した媒体が含まれる電子計算機等を廃棄

する場合は、当該媒体に記録された情報資産を完全に消去する等復元できないようにした上でしなければならない。賃貸業者に対し、賃貸した構成機器を返却する場合も、同様とする。

イ　情報システム管理者は、情報資産を記録した媒体が含まれる電子計算機の故障について、事業者に委託して修理させる場合は、可能な限り当該媒体に記録された情報資産を消去するものとする。

(6)　管理記録

情報システム管理者は、情報システムについて行った変更及び修理等の作業については、それらの作業記録を作成し、適切に管理しなければならない。

6　コンピュータウイルスの対策

(1)　ネットワーク管理者及び情報システム管理者は、コンピュータウイルスをチェックするパターンファイルを常時、最新のものに保たなければならない。

(2)　情報システム管理者は、所管する情報システムに対し、コンピュータウイルスの対策のためのソフトウェア等を導入しなければならない。

(3)　職員は、データ又はソフトウェアを取り入れる場合及び執務室外にデータ又はソフトウェアを持ち出す場合には、必ずコンピュータウイルスのチェックを行わなければならない。

(4)　職員は、コンピュータウイルスに関する情報については、常時、確認しなければならない。

(5)　職員は、自己の端末等において差出人の不明なメール又は不自然に添付されたファイルを発見したときは、速やかにそれらを削除しなければならない。

(6)　職員は、ファイルが添付されたメールを送信し、又は受信する場合は、コンピュータウイルスのチェックを併せて行わなければならない。

(7)　職員は、特に必要な場合を除き、コンピュータウイルスのチェックを中断してはならない。

7　不正なアクセスの対策

(1)　情報システム管理者は、情報セキュリティホール(ソフトウェアに関する情報セキュリティ上の抜け穴をいう。以下同じ。)の発見に努め、情報システムの製造業者等から修正ソフトウェアの提供があった場合には、業務に支障がないことを確認の上、速やかに当該情報セキュリティホールを除去しなければならない。

(2)　情報システム管理者は、情報セキュリティホールが発見された場合において、情

報システムの製造業者等から修正ソフトウェアの提供がない段階においても、サーバ、端末及び通信回線上で採り得る対策を可能な限り講じなければならない。

(3)　情報システム管理者は、重要な情報システムの設定に係るファイルの改ざんの有無について定期的に検査しなければならない。

(4)　情報システム管理者は、侵害を受ける可能性がある場合には、情報システムの停止等必要な措置を講じなければならない。

(5)　情報システム管理者は、侵害が法に違反する可能性がある場合には、当該侵害の記録の保存に努めるとともに、その旨をネットワーク管理者に報告しなければならない。

(6)　ネットワーク管理者は、(5)の報告があった場合は、警察署及び関係機関との緊密な連携に努めなければならない。

(7)　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、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(8)　ネットワーク管理者は、情報システムにおいて、標的型攻撃による内部への侵入又は外部への情報漏えいを防止するために必要な人的対策及び技術的対策を講じるとともに、内部に侵入した攻撃を早期探知し、通信をチェックする等の内部対策を講じなければならない。

(9)　ネットワーク管理者は、実施している不正なアクセス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体制を整備しておかなければならない。

8　情報セキュリティに関する情報の収集等

(1)　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、ネットワーク及び情報システムについて、情報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。

(2)　情報化統括管理者は、(1)の情報を定期的に取りまとめ、実施機関等にその結果を通知しなければならない。

(3)　ネットワーク管理者は、別に定める緊急時対応計画に掲げる緊急に連絡すべき情報を入手した場合は、当該緊急時対応計画に定める連絡先に連絡しなければならない。

第6　運用

1　情報システムの監視

(1)　情報システム管理者は、情報セキュリティを確保するため、常時、情報システムの監視を行わなければならない。

(2)　情報システム管理者は、(1)の監視により得られた結果を記録した媒体について、盗難、改ざん、消去等を防止するために必要な措置を講じ、安全な場所に保管しなければならない。

2　情報セキュリティポリシーの遵守状況等

(1)　統括情報セキュリティ責任者は、情報セキュリティポリシーの遵守状況及び情報資産の管理に関する問題の有無について、常時、確認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、(1)の確認により、情報セキュリティポリシーの遵守状況又は情報資産の管理に関する問題が発生していた場合には、速やかに情報化統括管理者及びネットワーク管理者にその旨を報告しなければならない。

(3)　情報化統括管理者は、(2)の報告があった場合は、速やかに当該問題に対する適切な措置を講じなければならない。

3　情報セキュリティ障害

(1)　情報セキュリティ障害の調査

ア　ネットワーク若しくは情報システムの障害又は侵害(以下これらを「情報セキュリティ障害」という。)を確認した職員は、その内容を速やかに情報セキュリティ責任者に報告しなければならない。

イ　アの報告を受けた情報セキュリティ責任者は、その内容を速やかに情報化統括管理者及びネットワーク管理者に報告しなければならない。

ウ　ネットワーク管理者は、イの報告があった場合は、当該情報セキュリティ障害に関して詳細に調査を行い、その調査結果を新宿区情報化の推進に関する規則第2条に規定する情報化戦略本部(以下「情報化戦略本部」という。)へ報告しなければならない。

(2)　情報セキュリティ障害の拡大の防止

ア　ネットワーク管理者は、次に掲げる場合には、ネットワーク、情報システム及び情報資産の保護のためにネットワークを切断する措置を講じるものとする。

(ア)　情報システムの運用に著しい支障が生じる等異常なアクセスが継続しているとき、又は不正なアクセスが判明したとき。

(イ)　コンピュータウイルス等不正なプログラムがネットワークを経由して拡大

しているとき。

(ウ)　災害等により、ネットワークを稼動させる電力の供給を受けることが危険又は困難であるとき。

(エ)　コンピュータウイルス等の不正なプログラムに感染したとき、又は当該感染が疑われるとき。

(オ)　その他ネットワーク、情報システム及び情報資産に係る被害が想定されるとき。

イ　情報システム管理者は、次に掲げる場合には、ネットワーク、情報システム及び情報資産の保護のために所管する情報システムを停止する措置を講じるものとする。

(ア)　コンピュータウイルス等不正なソフトウェアが情報資産に危害を及ぼしているとき。

(イ)　災害等により、情報システムを稼動させる電力の供給を受けることが危険又は困難であるとき。

(ウ)　コンピュータウイルス等の不正なプログラムに感染したとき、又は当該感染が疑われるとき。

(エ)　その他ネットワーク、情報システム及び情報資産に係る被害が想定されるとき。

ウ　職員は、自己の端末等をネットワークから離脱させる場合には、事前にネットワーク管理者の許可を受けなければならない。ただし、ネットワーク、情報システム及び情報資産への危害を防止するため、直ちに離脱させる必要がある場合には、事後において、ネットワーク管理者にその旨を報告するものとする。

(3)　情報セキュリティ障害への対応

ネットワーク管理者は、情報セキュリティ障害が発生した場合には、次に掲げる措置を迅速かつ円滑に講じなければならない。

ア　緊急時対応計画により定められた連絡先への連絡

イ　情報セキュリティ障害に係る現状及び対処した経過の記録

ウ　情報セキュリティ障害に係る証拠保全の実施

エ　情報セキュリティ障害の再発を防止するための暫定的な措置

オ　エの暫定的な措置を講じた後の復旧作業

カ　オの復旧作業後必要と認められる期間内における情報セキュリティ障害の再発

に関する監視

(4)　情報セキュリティ障害の再発防止の措置

ア　ネットワーク管理者は、情報セキュリティ障害に関するリスクを分析し、情報セキュリティ障害の再発を防止するために必要な措置を検討し、情報化戦略本部にその旨を報告しなければならない。

イ　情報化戦略本部は、アの報告があった場合は、これを審議する。

ウ　情報化統括管理者は、アの情報セキュリティ障害の概要とともに情報セキュリティポリシーが見直されたときは、見直し後の情報セキュリティポリシーを職員に周知しなければならない。

4　情報セキュリティに関する違反への対応

(1)　ネットワーク管理者は、職員の情報セキュリティポリシーに違反する行為を確認した場合には、当該職員が所属する課等の情報セキュリティ責任者にその旨を通知しなければならない。

(2)　(1)の通知を受けた情報セキュリティ責任者は、当該職員に対し適切な措置を講じなければならない。

(3)　ネットワーク管理者は、(2)の措置によっても当該職員の情報セキュリティポリシーに違反する行動が改善されない場合には、当該職員によるネットワーク又は情報システムの使用を停止させることができる。

(4)　ネットワーク管理者は、(3)により使用を停止させた場合には、情報化統括管理者及び当該職員が所属する課等の情報セキュリティ責任者にその旨を通知しなければならない。

5　外部委託に関する管理

事業者に情報業務を委託する場合には、次に掲げる事項を契約書に明記しなければならない。

(1)　情報セキュリティポリシーの主旨の遵守に関すること。

(2)　受託した情報業務上知り得た情報の守秘義務に関すること。

(3)　受託した情報業務上提供された情報の目的外利用又は第三者への提供の禁止に関すること。

(4)　受託した情報業務上提供された情報の適切な管理に関すること。

(5)　受託した情報業務上提供された情報の複写等の禁止に関すること。

(6)　受託した情報業務の再委託の禁止に関すること。

(7)　受託した情報業務上提供された情報の返還義務に関すること。

(8)　区の求めにより受託した情報業務に関する報告を定期的に行うこと。

(9)　区の監査に応じること。

(10)　当該事業者の従業員に対する情報セキュリティに関する教育の実施に関すること。

(11)　情報セキュリティインシデント発生時等における報告に関すること。

(12)　前各号に掲げる事項に違反した場合の措置に関すること。

6　派遣労働者に情報業務を行わせる場合

派遣労働者に情報業務を行わせる場合には、労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律(昭和60年法律第88号)第26条第1項に規定する労働者派遣契約に係る書面に、次に掲げる事項を明記しなければならない。

(1)　当該派遣労働者の情報セキュリティポリシーの遵守に関すること。

(2)　情報業務上知り得た情報の守秘義務に関すること。

(3)　区の監査に応じること。

(4)　前3号に掲げる事項に違反した場合の措置に関すること。

7　例外措置

(1)　情報セキュリティ責任者及び情報システム管理者は、情報セキュリティ関連規程を順守することが困難な状況下において、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、情報化統括管理者の許可を得て、例外措置を採ることができる。

(2)　情報セキュリティ責任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、事後速やかに情報化統括管理者に報告しなければならない。

(3)　情報化統括管理者は、例外措置の申請及び審査結果を適切に保管し、必要に応じて、申請状況や例外措置実施状況を確認しなければならない。

第7　監査、点検、評価及び見直し

1　監査

(1)　情報化統括管理者は、監査の結果を情報化戦略本部へ報告しなければならない。

(2)　情報化戦略本部は、(1)の報告を、情報セキュリティポリシー及び関連規程等の見直しに関する審議の際に、活用するものとする。

2　点検

(1)　統括情報セキュリティ責任者は、所管する情報資産について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が行われているかどうか点検を行い、ネットワーク管理者に当該点検の結果を報告しなければならない。

(2)　ネットワーク管理者は、(1)の点検の結果をとりまとめ、情報化戦略本部へ報告しなければならない。

3　評価

情報化統括管理者は、1の監査及び2の点検の結果及び情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティ対策の実効性を定期的に評価しなければならない。

4　情報セキュリティポリシー及び関連規程等の見直し

情報化戦略本部は、3の評価に基づき、情報セキュリティポリシー及び関連規程等の必要な見直しに関し、審議する。

附　則

この基準は、平成15年8月25日から施行する。

附　則(平成17年3月30日16新企情第1029号)

この基準は、平成17年4月1日から施行する。

附　則(平成18年3月30日17新総情第2275号)

この基準は、平成18年4月1日から施行する。

附　則(平成19年3月23日総情第2605号)

この基準は、平成19年4月1日から施行する。

附　則(平成19年5月24日19新総情第493号)

この基準は、平成19年5月31日から施行する。

附　則(平成20年2月26日19新総情第2815号)

この基準は、平成20年4月1日から施行する。

附　則(平成20年6月23日20新総合情第868号)

この基準は、平成20年6月26日から施行する。

附　則(平成24年4月30日24新総合情第141号)

この基準は、平成24年5月1日から施行する。

附　則(平成26年3月24日25新総合情第3605号)

この基準は、平成26年3月25日から施行する。

附　則(平成27年11月20日27新総合情第2678号)

この基準は、平成28年1月1日から施行する。