立川市情報セキュリティ対策基準
～概要版～

≪　目　次　≫

第2.0版対応
令和元年７月

1　総則

1.1.　目的

この対策基準（以下「対策基準」という。）は、立川市（以下「市」という。）が保有する情報資産に係る情報セキュリティ対策を実施するために、立川市情報セキュリティ基本方針（以下「基本方針」という。）第 10 条の規定に基づき、具体的な遵守事項及び判断基準等を定めることを目的とする。

1.2.　用語の定義

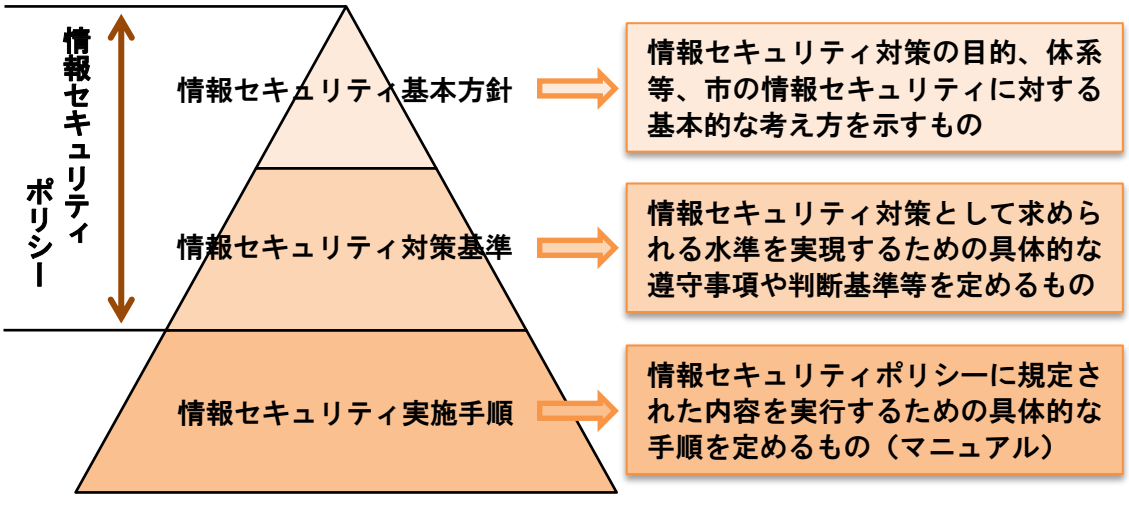
基本方針第２条の規定によるほか、次のとおりとする。

用語	定義
情報セキュリティインシデント	情報セキュリティを侵害する事象又は事故
個人情報	立川市個人情報保護条例第２条第２号に掲げる個人情報
番号法	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（平成25年法律第27号）
個人番号	住民票を持つ全ての者に付される12桁の番号（番号法第２条第５項）
特定個人情報	個人番号をその内容に含む個人情報（番号法第２条第８項）
特定個人情報等	個人番号及び特定個人情報
個人情報等	個人情報及び特定個人情報等
端末	情報システム等（図表 1.5-1 参照）の構成要素である機器のうち、情報処理を行うために直接操作するもの。具体的にはパソコン等を指し、搭載されるソフトウェアを含むものとする。
外部委託事業者	市との契約・協定等に基づいて市の業務を担う外部の者

1.3.　情報セキュリティ対策に関する規程

市の情報セキュリティ対策に関する規程は次の体系で構成されており、基本方針と対策基準を併せて「情報セキュリティポリシー」と称するものとする。

図表 1.3-1　情報セキュリティポリシーの体系図



1.4. 個人情報等の取扱い

個人情報等については、情報セキュリティポリシーのほか、立川市個人情報保護条例をはじめとする関連法令（8.5.参照）を遵守した取扱いを徹底するものとする。

1.5. 対象範囲

（１）実施機関の範囲

対策基準が適用される市の機関は、市長部局、会計課、教育委員会事務局、図書館、選挙管理委員会事務局、監査委員事務局、農業委員会事務局、議会事務局とする。

（２）対象者の範囲

① 対策基準が適用される者は、市長、副市長、教育長、常勤の一般職、再任用職員、嘱託職員及び臨時職員（以下「職員」という。）とする。

② 委託等により、業務において市が保有する情報資産を利用する職員以外の者は、職員に準じて情報セキュリティポリシーを遵守するものとする。

（３）情報資産の範囲

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、情報システム及びこれらに関する設備並びに電磁的記録媒体（以下「情報システム等」という。）

② 紙文書

③ 情報システム等及び紙文書で取り扱う情報

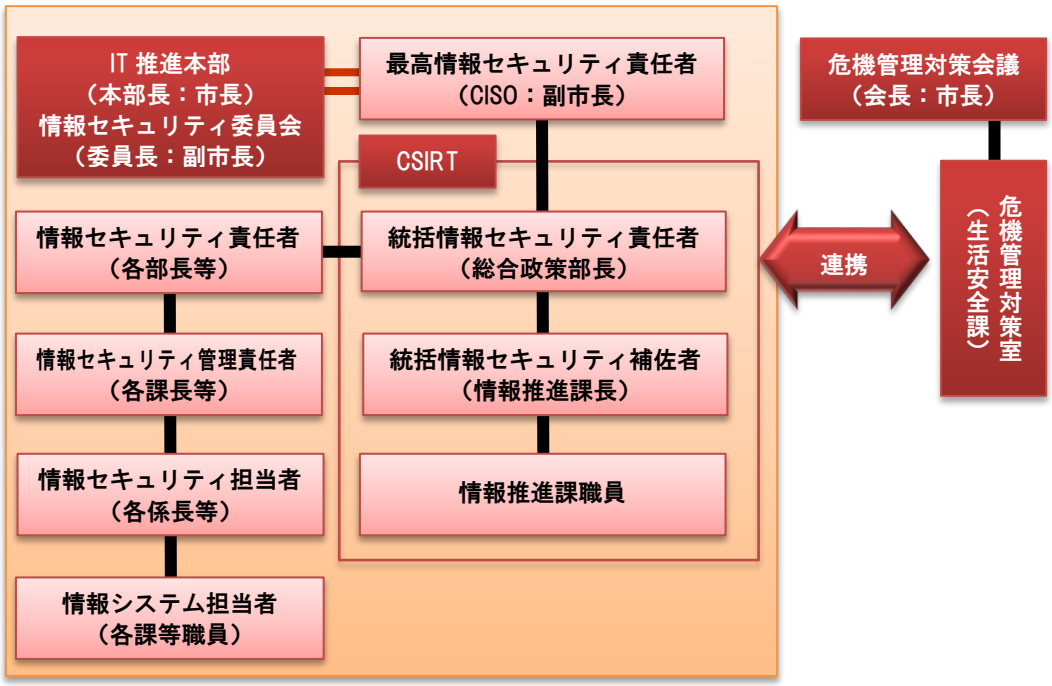
図表 1.5-1 情報資産の種類と例

情報資産の種類		情報資産の例
情報システム等	ネットワーク	通信回線、ルータ等の通信機器
	情報システム	サーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア等
	これらに関する設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
	電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される電磁的記録媒体、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体
紙文書		紙文書全般
情報システム等及び紙文書で取り扱う情報		あらゆる媒体に記録されたすべての行政情報

2　組織体制

情報セキュリティ対策を組織的かつ効果的に実施するため、次のとおり体制を整備する。

図表 2-1　情報セキュリティに関する組織体系図



3　情報資産の管理

3.1.　情報資産の分類・記録

情報資産は重要性に応じて次のとおり分類して記録し、当該分類に基づいて取扱制限の措置を講じるものとする。

分類	分類基準	取扱制限
Ⅰ	情報セキュリティの侵害があった場合に、市民等に損害が生じるおそれ又は行政事務の執行に重大な影響を及ぼすおそれのある情報（個人情報をはじめとする重要情報）	最小限の者のみが取り扱うこととし、権限を有しない者の利用・接触等が絶対にないよう、特段の取扱制限を行う。
Ⅱ	情報セキュリティの侵害があった場合に、行政事務の執行等に影響を及ぼすおそれのある情報	関係者以外の利用・接触等がないよう、取扱制限を行う。
Ⅲ	上記以外の情報	特になし。

3.2.　管理責任

情報セキュリティ管理責任者は、所管する情報資産について管理責任を有するものとし、当該情報資産の取扱状況について把握しなければならない。

3.3. 管理方法

情報資産のライフサイクルには、「作成」「入手」「利用」「保管」「送信」「持ち出し・運搬」「提供・公表」「廃棄」の局面がある。情報資産の取扱いについて遵守すべき事項は、これらの局面ごとに重要性分類に応じて次のとおり定めるものとする。

3.3.1. 情報の作成

分類	遵守事項
Ⅰ	✓ 情報の作成にあたっては、情報セキュリティ管理責任者の許可を得なければならない。 ✓ 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。 ✓ 作成する情報は最小限の項目及び件数としなければならない。
Ⅱ	✓ 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。 ✓ 作成する情報は最小限の項目及び件数としなければならない。
共通	✓ 業務上必要のない情報を作成してはならない。 ✓ 情報は正確に作成し、内容に誤り等を発見した場合には、必要に応じて訂正等を行わなければならない。

3.3.2. 情報の入手

分類	遵守事項
Ⅰ	✓ 情報の入手にあたっては、情報セキュリティ管理責任者の許可を得なければならない。 ✓ 入手する情報は最小限の項目及び件数としなければならない。
Ⅱ	✓ 入手する情報は最小限の項目及び件数としなければならない。
共通	✓ 業務上必要のない情報を入手してはならない。

3.3.3. 情報資産の利用

分類	遵守事項
Ⅰ	✓ 情報資産を取り扱う区域を明確にし、安全管理措置を講じなければならない。 ✓ 情報の利用中に、離席、退室等でその場を離れ、情報を管理する者がいなくなるときは、情報を書庫等に戻し施錠するか、部屋に施錠しなければならない。 ✓ 利用開始時点と終了時点で、紛失等がないか情報の内容を確認しなければならない。
共通	✓ 業務以外の目的に情報資産を利用してはならない。 ✓ 情報を必要以上に複製してはならない。

3.3.4. 情報資産の保管

分類	遵守事項
I	✓ 施錠された場所に保管する等の安全管理措置を講じるとともに、必要に応じて耐火金庫等に保管しなければならない。 ✓ 情報にアクセスできる者は最小限としなければならない。 ✓ 電子ファイルには、必要に応じて暗号化又はパスワード設定等の措置を講じなければならない。
共通	✓ 情報資産を保管する媒体には、紛失、破損等を防止するための措置を講じなければならない。

3.3.5. 情報の送信

分類	遵守事項
I II	✓ 業務上の必要から情報を送信等する場合は、情報セキュリティ管理責任者の許可を得なければならない（個人情報等の電子メール又はFAXによる送信は原則禁止）。 ✓ 電子メールで送信する情報には、暗号化又はパスワード設定等の措置を講じなければならない。 ✓ 郵送・使送する情報は、封筒等を利用して第三者が内容を見ることができないようにしなければならない。 ✓ 電磁的記録媒体で送付する情報には、暗号化又はパスワード設定等の措置を講じなければならない。
共通	✓ 誤送信等を防止する適切な措置を講じなければならない。

3.3.6. 情報資産の持ち出し・運搬

分類	遵守事項
I	✓ 情報資産を持ち出す場合は、情報セキュリティ管理責任者の許可を得なければならない。 ✓ 電磁的記録媒体で持ち出す情報には、暗号化又はパスワード設定等の措置を講じなければならない。 ✓ 車両等により運搬する場合は、必要に応じて鍵付のケース等に格納するなど、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。
共通	✓ 情報資産は、業務上の必要がある場合に限って最小限の範囲で持ち出すことができる。 ✓ 持ち帰った際に、全て揃っているか確認しなければならない。

3.3.7. 情報の提供・公表

分類	遵守事項
Ⅰ Ⅱ	✓ 情報を提供・公表する場合は、情報セキュリティ管理責任者の許可を得なければならない。 ✓ 情報の提供は、「3.3.5.情報の送信」の遵守事項に準じて行わなければならない。
共通	✓ 提供・公表する情報については誤りのないようにしなければならない。

3.3.8. 情報資産の廃棄

分類	遵守事項
Ⅰ	✓ 情報資産を廃棄する場合は、情報セキュリティ管理責任者の許可を得なければならない。 ✓ 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。
Ⅱ	✓ 必要に応じて、重要性Ⅰに準じて廃棄しなければならない。
共通	✓ 業務上必要のなくなった情報は速やかに廃棄しなければならない。

3.4. USB メモリ等の取扱い

USB メモリ等（持ち運び可能な小型の電磁的記録媒体）の取扱いに当たっては、紛失、盗難、ウイルス感染及びデータ漏えい等を防止するための対策を講じなければならない。

4 特定個人情報等の取扱い

特定個人情報等の取扱いは重要性Ⅰの遵守事項によるほか、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（個人情報保護委員会）」に基づく安全管理措置を講じなければならない。

5　物理的セキュリティ対策

5.1.　サーバ等の管理

サーバ等の機器の管理が不十分な場合、情報システム全体に悪影響が及んだり、業務の継続性に支障が生じたりするおそれがある。そのため、機器の取付け、バックアップの保管、電源・配線等についてセキュリティ対策を講じなければならない。

5.2.　管理区域（情報システム室等）の管理

情報システム室等が適切に管理されていない場合、盗難、損傷等により重大な被害が発生するおそれがある。そのため、構造、入退室管理、機器等の搬入出等についてセキュリティ対策を講じなければならない。

5.3.　通信回線及び通信回線装置の管理

ネットワーク利用における通信回線及び通信回線装置が適切に管理されていない場合、ネットワークそれ自体のみならず、ネットワークに接続している情報システム等に対しても損傷や不正アクセス等が及ぶおそれがある。そのため、通信回線等の管理、ネットワークの接続制限、回線の選択等についてセキュリティ対策を講じなければならない。

5.4.　端末及び電磁的記録媒体等の管理

端末及び電磁的記録媒体等が適切に管理されていない場合、不正利用、紛失、盗難、情報漏えい等の被害を及ぼすおそれがある。そのため、盗難防止、認証機能等についてセキュリティ対策を講じなければならない。

6　人的セキュリティ対策

6.1.　職員の遵守事項

職員が情報資産を不正に利用したり、適正な取扱いを怠ったりした場合、コンピュータウイルス等の感染、情報漏えい等の被害が発生し得る。そのため、情報資産の取扱いに関する遵守事項（目的外使用の禁止、私物端末の利用制限等）を定めて実施しなければならない。

6.2.　嘱託職員等への対応

嘱託職員及び臨時職員（以下「嘱託職員等」という。）に対し、情報セキュリティポリシーのうち嘱託職員等が守るべき内容の遵守及びその機密事項を採用時に説明しなければならない。

6.3.　外部委託事業者に対する説明

重要性Ⅰ・Ⅱの情報の取扱い又は情報システム等の開発・運用・保守等を外部委託する場合には、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機密事項を説明しなければならない。

6.4.　研修・訓練

職員に対して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。

6.5.　情報セキュリティインシデントの報告

情報セキュリティインシデントを認知した場合における責任者等への報告体制を整備し、適切かつ速やかな対応が図られるようにしておかなければならない。

6.6.　ID 及びパスワード等の管理

情報システム等を利用する際のID・パスワード、生体等の認証情報及びこれを記録した媒体（IC カード等）の管理が適切に行われない場合、情報システム等を不正に利用されるおそれがある。そのため、ID 及びパスワード等の管理についてセキュリティ対策を講じなければならない。

6.7.　インターネット及び各種機器等の取扱い制限

インターネット、電子メール、端末、FAX 及び印刷機器を利用する際には、情報漏えい等を防ぐためのセキュリティ対策を講じなければならない。

7　技術的セキュリティ対策

7.1.　コンピュータ及びネットワークの管理

情報システム等の管理が不十分な場合、不正利用によるサイバー攻撃、情報漏えい、損傷、改ざん、重要情報の詐取、内部不正等の被害が生じるおそれがある。

これらの被害を防いで証拠を保全するため、バックアップの実施、ログの取得、ネットワークの接続制御、無許可ソフトウェアの導入禁止、機器構成の変更制限等のセキュリティ対策を講じなければならない。

7.2.　アクセス制御

アクセス権限のない者が情報システム等を利用できる状態にしておくと、情報漏えいや情報資産の不正利用等の被害が発生し得る。そのため、権限のない者が情報システム等にアクセスできないよう、権限識別機能（ID・パスワード、生体認証、ICカード等）の設定等によりアクセス制御の措置を講じなければならない。

7.3.　システム開発、導入、保守等

システム開発、導入、保守等において、技術的なセキュリティ対策が十分に行われない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。そのため、システム開発、導入、保守等のそれぞれの段階においてセキュリティ対策を講じなければならない。

7.4.　不正プログラム対策

情報システム等にコンピュータウイルス等の不正プログラム対策が十分に行われていない場合、システムの損傷、情報漏えい等の情報セキュリティインシデントが発生するおそれがある。そのため、不正プログラム対策ソフトウェアの導入などによって、コンピュータウイルス等の感染を予防するとともに、感染時に適切に対応するためのセキュリティ対策を講じなければならない。

7.5.　不正アクセス対策

情報システム等に不正アクセス対策が十分に行われていない場合、システムへの攻撃、情報漏えい、損傷、改ざん等の被害を及ぼすおそれがある。そのため、ファイアウォールの設定による経路制御等のセキュリティ対策を講じるとともに、攻撃を受けた際の対処及び関係機関との連携等について体制を構築しなければならない。

7.6.　セキュリティ情報の収集

情報セキュリティに関する情報を収集し、必要に応じて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、セキュリティ侵害を未然に防止するための対策を講じなければならない。

8　運用

8.1.　情報システムの監視

情報セキュリティに関する事案を検知するため、情報システムを監視しなければならない。

8.2.　情報セキュリティポリシーの遵守状況の確認

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。

8.3.　侵害時の対応等

情報資産に対するセキュリティ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、セキュリティ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。

8.4.　例外措置

情報セキュリティポリシー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、CISO 又は統括情報セキュリティ責任者の許可を得て例外措置を取ることができる。

8.5.　法令遵守

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 25 年法律第 261 号)
（２）著作権法（昭和 45 年法律第 48 号）
（３）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）
（４）個人情報の保護に関する法律（平成 15 年法律第 57 号）
（５）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（平成 25 年法律第 27 号）
（６）サイバーセキュリティ基本法（平成 26 年法律第 104 号）
（７）特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（平成 26 年特定個人情報保護委員会告示第６号）
（８）立川市個人情報保護条例（平成元年立川市条例第 55 号）
（９）立川市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に関する条例（平成 27 年立川市条例第 54 号）
（10）立川市職員服務規程（昭和 24 年立川市規程第８号）
（11）立川市文書規程（昭和 36 年立川市訓令甲第６号）

8.6. 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及びその監督責任者は、「立川市職員の懲戒処分の指針」に基づき、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なる。

（２）違反時の対応

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、責任者等に通知して適切な措置を求めなければならない。

9 外部サービスの利用

9.1. 外部委託

（１）外部委託事業者の選定基準

① 外部委託事業者の選定にあたり、業務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 必要に応じて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。

（２）契約項目

重要性Ⅰ・Ⅱの情報の取扱い又は情報システム等の開発・運用・保守等を外部委託する場合には、情報セキュリティポリシーと同等以上の水準での情報セキュリティを確保できるよう、必要に応じて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。

（３）確認・措置等

情報セキュリティ管理責任者は、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必要に応じて確認し、適切な措置を講じさせなければならない。

9.2. 約款による外部サービスの利用

約款への同意及び簡易なアカウント登録により利用可能なサービス（電子メール、ファイルストレージサービス等）を使用してはならない。業務上の必要からやむを得ず使用する場合は、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責任者の許可を得なければならない。

9.3. ソーシャルメディアサービスの利用

市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する運用手順を定めなければならない。また、重要性Ⅰ・Ⅱの情報をソーシャルメディアサービスで発信してはならない（個人のアカウントでの情報発信を含む。）。

10　評価・見直し

10.1.　監査

CISOは、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を実施しなければならない。

10.2.　自己点検

情報セキュリティ管理責任者は、所管する課等の情報セキュリティ対策の実施状況について、定期的又は必要に応じて自己点検を実施しなければならない。

10.3.　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、情報セキュリティポリシーについて毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合は改善・見直しを行うものとする。

10.4.　情報セキュリティ実施手順の策定

情報資産を取り扱うに当たって、どのような手順で情報セキュリティポリシーに記述された内容を実行していくかを定めるマニュアルに該当するものとして、情報セキュリティ実施手順を策定するものとする。

以上