情報セキュリティ基本方針

施行日：平成 19 年 4 月 1 日

世田谷区

改訂履歴

年月日	版番号	改訂理由・内容
平成 21 年 4 月 1 日	1.2	世田谷区電子計算組織の運営に関する規則の一部改正に対応するため。
平成 23 年 4 月 1 日	1.3	平成 22 年 11 月に一部改訂された「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」（総務省策定）の改訂内容等を踏まえ、一部改訂する。
平成 24 年 4 月 1 日	1.4	世田谷区電子計算組織の運営に関する規則の一部改正に対応するため。
平成 27 年 12 月 28 日（平成 28 年 1 月 1 日施行）	1.5	平成 27 年 3 月に一部改訂された「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」（総務省策定）の改訂内容に対応するため。
平成 31 年 3 月 8 日（平成 31 年 4 月 1 日施行）	1.6	平成 30 年 9 月に一部改訂された「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」（総務省策定）の改訂内容に対応するため。
令和 2 年 4 月 1 日	1.7	会計年度任用職員制度の導入に対応するため。
令和 4 年 6 月 15 日（令和 4 年 6 月 16 日施行）	1.8	世田谷区電子計算組織の運営に関する規則の一部改正に対応するため。
令和 5 年 3 月 20 日（令和 5 年 4 月 1 日施行）	1.9	「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」（総務省策定）の改訂内容に対応するため。
令和 7 年 3 月 31 日（令和 7 年 4 月 1 日施行）	2.0	「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」（総務省策定）の改訂内容に対応するため。

目次

1　目　的 ..... - 1 -
2　定　義 ..... - 1 -
(1)　情報セキュリティポリシー ..... - 1 -
(2)　ネットワーク ..... - 1 -
(3)　情報システム ..... - 1 -
(4)　情報セキュリティ ..... - 2 -
(5)　機密性 ..... - 2 -
(6)　完全性 ..... - 2 -
(7)　可用性 ..... - 2 -
(8)マイナンバー利用事務系（個人番号利用事務系） ..... - 2 -
(9)ＬGWAN接続系 ..... - 2 -
(10)インターネット接続系 ..... - 2 -
(11)通信経路の分割 ..... - 2 -
(12)無害化通信 ..... - 2 -
3　対象とする脅威 ..... - 2 -
4　適用範囲 ..... - 3 -
(1)　行政機関の範囲 ..... - 3 -
(2)　情報資産の範囲 ..... - 3 -
5　職員の義務 ..... - 3 -
6　情報セキュリティ対策 ..... - 4 -
(1)　組織体制 ..... - 4 -
(2)　情報資産の分類 ..... - 4 -
(3)情報システム全体の強靭性の向上 ..... - 4 -
(4)物理的セキュリティ対策 ..... - 4 -
(5)人的セキュリティ対策 ..... - 4 -
(6)技術及び運用におけるセキュリティ対策 ..... - 5 -
(7) 外部委託と外部サービスの利用 ..... - 5 -
7　情報セキュリティ監査及び自己点検の実施 ..... - 5 -
8　情報セキュリティポリシーの見直し ..... - 5 -
9　確認及び見直しと承認 ..... - 5 -
10　情報セキュリティ対策基準の策定 ..... - 6 -
11　情報セキュリティ実施手順の策定 ..... - 6 -

1　目　的

世田谷区の各情報システムが取扱う情報には、区民の個人情報のみならず行政運営上重要な情報など、部外に漏洩等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。

従って、これらの情報及び情報を取扱う情報システムを様々な脅威から防御することは、区民の財産、プライバシー等を保護し、事務の安定的な運営のためにも必要不可欠である。

また、近年の情報化の急激な進展により、より徹底した行政の情報化が期待されているところである。世田谷区がこれらに積極的に対応するためには、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。

さらに、セキュリティに関わる職員の役割及び責任の所在を明確にし、日々の取り組み結果を区民に対して説明できるよう努めていく必要がある。ひいては、これらが、世田谷区に対する区民からの信頼の維持向上に寄与するものである。

そのため、世田谷区の情報資産の機密性、完全性及び可用性を維持し、説明責任を果たすための対策（情報セキュリティ対策）として情報セキュリティ基本方針と情報セキュリティ対策基準を定める。このうち、情報セキュリティ基本方針については、世田谷区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) 情報セキュリティポリシー

情報セキュリティポリシーは、世田谷区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とりまとめたものであり、情報セキュリティ基本方針と情報セキュリティ対策基準を合わせて、情報セキュリティポリシーとする。

(2) 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（ハードウエア及びソフトウエア）をいう。

(3) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(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)マイナンバー利用事務系（個人番号利用事務系）
　個人番号利用事務（社会保障、地方税もしくは防災に関する事務）又は戸籍事務等に関わる情報システム及びその情報システムで取り扱うデータをいう。

(9)ＬGWAN接続系
　ＬGWANに接続された情報システム及びその情報システムで取り扱うデータをいう。

(10)インターネット接続系
　インターネットメール、ホームページ管理システム、一部の内部事務等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11)通信経路の分割
　ＬGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12)無害化通信
　インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

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)不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入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、無許可ソフトウエ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インフラ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、区長部局、行政委員会及び議会事務局とする。

(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。(ただし、教育委員会における学校教育に係るものを除く。)

- ネットワーク及び情報システム並びにこれらを構成する設備や設置場所
- ネットワーク及び情報システムで取扱う情報(これらを印刷したものを含む）や電磁的記録媒体
- 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　職員の義務

職員（再任用職員及び会計年度任用職員を含む。以下同じ。）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対策を遵守する義務を負うものとする。

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

本区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。

情報セキュリティに関する重要事項を審議する機関として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は統括情報化責任者を中心として構成する。

(2) 情報資産の分類

世田谷区の保有する情報資産は、各々の機密性、完全性及び可用性を踏まえ、その重要度に応じた情報セキュリティ対策を講じるものとする。

(3)情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②ＬGWAN接続系においては、ＬGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、インターネット接続系とLGWAN接続系間でメールやデータを取り込む場合は、無害化通信を実施する。

③インターネット接続系においては、クラウドサービスを含めた不正通信の監視機能の強化、通信の遮断及び自治体情報セキュリティの導入等を組み合わせ、高度な情報セキュリティ対策を実施する。

(4)物理的セキュリティ対策

サーバ等、情報システム室等、通信回線等及び職員のパソコン等の管理について、物理的な対策を講じる。

(5)人的セキュリティ対策

情報セキュリティに関し、職員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。

(6)技術及び運用におけるセキュリティ対策

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及び不正アクセス対策等の技術的対策を講じる。

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及び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、区の業務の根幹となる住民情報や特定個人情報ファイルを取り扱うシステム等、特に重要な情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、基幹システム及び特定個人情報を取り扱うシステム等について、緊急時対応計画を策定する。

(7) 外部委託と外部サービスの利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。

約款による外部サービスを利用する場合には、利用にかかる規程を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーの見直しを実施する。

9　確認及び見直しと承認

世田谷区の情報セキュリティレベルの維持、向上を図るため、上記７及び８の情報セキュリティ対策を講じるにあたっては、情報セキュリティ委員会によって確認及び見直しを実施し、最高情報セキュリティ責任者の承認を得るものとする。

10 情報セキュリティ対策基準の策定

世田谷区の様々な情報資産について、上記 6、7 及び 8 の情報セキュリティ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。

なお、情報セキュリティ対策基準は、公にすることにより世田谷区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。

11 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世田谷区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。