

サイバーセキュリティ基本方針

1. 目的	2
2. 定義	2
3. 対象とする脅威.....	3
4. 適用範囲	4
(1) 行政機関の範囲	4
(2) 情報資産の範囲	4
5. 関係団体等への指導.....	4
6. 職員等の遵守義務	4
7. サイバーセキュリティ対策	4
(1) 組織体制の確立	4
(2) 情報資産の分類と管理	4
(3) 情報システム全体の強じん性の向上	5
(4) 物理的セキュリティ対策	5
(5) 人的セキュリティ対策	5
(6) 技術的セキュリティ対策	5
(7) 運用面での対策	5
(8) 業務委託及びクラウドサービスの利用に係る対策	5
8. リスク評価の実施及び計画の策定.....	5
9. 自己点検及びサイバーセキュリティに関する監査の実施	5
10. サイバーセキュリティポリシーの見直し.....	6
11. サイバーセキュリティ対策基準の策定	6
12. サイバーセキュリティ実施手順の策定	6

1. 目的

江戸川区（以下「区」という。）は、行政運営上、個人情報などの重要な情報を多数取り扱っているだけでなく、公共インフラ事業を担うことにより、区民生活及び社会経済活動に必要不可欠なサービスを提供している。よって、これらを支える情報システムに加え、これらで取り扱う重要な情報などの情報資産を様々な脅威から守り、安全性を確保することは、行政及び公共インフラ事業の安定的・継続的な運営を実現するために、区に課せられた責務である。

そのため、区が実施するサイバーセキュリティ対策に関する基本的な事項を定め、サイバー攻撃等の様々な脅威から、区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本基本方針の目的とする。

また、全ての職員等は、区が保有する情報資産に対する脅威への対応が重大かつ喫緊の課題であることを改めて認識し、区におけるサイバーセキュリティ対策の推進に積極的に取り組むこととする。

2. 定義

この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

- (1) ネットワーク 区がコンピュータを相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）及び記録媒体により構成され、情報処理を行う仕組みをいう。
- (2) 情報システム コンピュータ（ハードウェア及びソフトウェア）、その周辺機器、ネットワーク及び記録媒体の全部又は一部により構成され、これを使用して業務を処理する仕組みをいう。
- (3) サイバーセキュリティ 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。
- (4) サイバーセキュリティポリシー 本基本方針及びサイバーセキュリティ対策基準（区情報セキュリティポリシーに包含）をいう。
- (5) 職員等 区が所管する情報資産に関する業務に携わる正規職員、再任用職員、会計年度任用職員、委託事業者等及び労働者派遣契約に基づき区の業務の処理に従事する派遣労働者をいう。
- (6) 機密性 情報資産にアクセスすることを認可されていない個人、実体又はプロセスに対して、情報資産を使用不可又は非公開にする特性又はその程度をいう。
- (7) 完全性 情報資産の正確さ及び完全さを保護する特性又はその程度をいう。
- (8) 可用性 情報資産にアクセスすることを許可されたものが要求したときに、アクセス及び使用が可能である特性又はその程度をいう。
- (9) マイナンバー利用事務（個人番号利用事務）系の情報システム 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。定められている個人番号利用事務（社会保障、地方税

又は防災に関するその他の事務)又は戸籍事務等に関わる情報システムをいう。

- (10) L G W A N接続系の情報システム 業務用システムをいう。
- (11) インターネット接続系の情報システム インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システムをいう。
- (12) 業務用端末 職員等に対し、業務上利用することが許可されたパソコン及びスマートフォン、タブレット等のモバイル端末等をいう。
- (13) 業務用外部記録端末 職員等に対し、業務上利用することが許可されたU S Bメモリや光ディスク等の外部記録媒体をいう。
- (14) 管理区域 サーバ室(ネットワークの基幹機器及び重要な情報システム等に係る機器等を設置し、専ら当該機器等の管理及び運用を行うための部屋)及び業務用外部記録媒体の保管に使用する保管庫を設置している区域をいう。
- (15) 外部サービス(クラウドサービス、以下「クラウドサービス」という。) 業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。
- (16) サイバーセキュリティ事象(以下「イベント」という。) 以下の「3で定める脅威」により業務の遂行及びサイバーセキュリティに影響を与える事象の全てをいう。
- (17) サイバーセキュリティインシデント イベントのうち、業務の遂行を危うくする確率及びサイバーセキュリティを脅かす確率が高い事象をいう。
- (18) 関係団体 区が出資その他財政上の援助等を行う法人又は団体のうち、公益財団法人えどがわ環境財団、公益社団法人シルバー人材センター江戸川区高齢者事業団、社会福祉法人江戸川区社会福祉協議会、認定N P O法人えどがわエコセンター、公益財団法人えどがわボランティアセンター、一般社団法人みんなの就労センター及び江戸川区職員厚生会をいう。

3. 対象とする脅威

情報資産に対する脅威として、以下のものを想定し、サイバーセキュリティ対策を実施するほか、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応する。

- (1) サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、無許可ソフトウェ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、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、風水害、事故等の災害によるサービス及び業務の停止。
- (4) 電力供給の途絶、通信の途絶等の提供サービスの障害からの波及。
- (5) 公共ネットワークにおける職員等による公序良俗に反する発言又はいわれのない外部からの誹謗中傷等による社会的信用の低下。

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、教育委員会、監査委員、選挙管理委員会、農業委員会、区議会事務局の所管するものとする。

(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。

- ① ネットワーク、情報システム、これらに関する設備、電磁的記録媒体。
- ② ネットワーク及び情報システムで取り扱う情報。（これらを印刷した文書を含む。）
- ③ 情報システムの仕様書、ネットワーク図等のシステム関連文書。
- ④ 江戸川区学校教育情報管理安全対策要綱の適用を受ける情報資産（情報システム等を含む。）は対象外とし、対象外となる学校の情報システム等は、この基本方針の対象となる情報システムと物理的に分けなければならない。

5. 関係団体等への指導

関係団体等においては、本基本方針等を参考に、各団体等においてサイバーセキュリティ対策に係る基本方針等を策定するなど、必要なサイバーセキュリティ対策を実施するよう、適正に指導を行うこととする。

6. 職員等の遵守義務

職員等は、区が保有する情報資産に対する脅威への対応の重要性について共通の認識を持ち、業務の遂行に当たって、サイバーセキュリティポリシー及びサイバーセキュリティ実施手順等を遵守しなければならない。

7. サイバーセキュリティ対策

3の脅威から情報資産を保護するために、以下のサイバーセキュリティ対策を講じる。

(1) 組織体制の確立

区の情報資産についてサイバー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。

(2) 情報資産の分類と管理

区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、サイバーセキュリティ対策を講じる。

(3) 情報システム全体の強じん性の向上

情報システム全体に対し、マイナンバー利用事務（個人番号利用事務）系の情報システム、L G W A N 接続系の情報システム及びインターネット接続系の情報システムという三層の情報システムからなる強じん性向上対策を講じる。

(4) 物理的セキュリティ対策

サーバ、管理区域、通信回線、業務用端末等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ対策

サイバーセキュリティに関し、職員等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) 技術的セキュリティ対策

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、不正アクセス対策等の技術的対策を講じる。

(7) 運用面での対策

情報システムの監視及びサイバーセキュリティポリシー等の遵守状況の確認のほか、(8)の業務委託及びクラウドサービスを利用する際のセキュリティ確保等、サイバーセキュリティポリシーの運用面での対策を講じるものとする。

また、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、緊急時対応体制を整備する。

(8) 業務委託及びクラウドサービスの利用に係る対策

区の業務を受託する事業者（当該事業者から派遣されている者を含む。）及び公的施設の管理を行う指定管理者等（以下併せて「委託事業者等」という。）に当該業務を行わせる場合には、区が定めるサイバーセキュリティ要件等、セキュリティ対策上、遵守させるべき事項を、委託事業者等の選定要件として提示する。

さらに、契約や協定等（以下「契約等」という。）の締結時等に、区が定めるサイバーセキュリティ要件を契約等事項に明記し、委託事業者等において要件を満たすセキュリティ対策が確保されていることを確認、又は、別途、書面による提出を求める等の措置を講じる。

なお、クラウドサービスの利用に当たっては、利用に関する手順等を定めるとともに、必要に応じて、当該利用の対象とする情報について定める等、規定を整備し、対策を講じる。

8. リスク評価の実施及び計画の策定

サイバーセキュリティに係る内部環境及び外部環境の変化を踏まえ、区が保有する情報資産のサイバーセキュリティ上のリスクを評価し、リスク対応方針を策定する。

また、策定したリスク対応方針に基づき、リスク対応計画を策定する。

9. 自己点検及びサイバーセキュリティに関する監査の実施

サイバー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、自己点検及びサイバーセキュリティに関する監査を実施する。

10. サイバーセキュリティポリシーの見直し

自己点検及びサイバーセキュリティに関する監査の結果、サイバーセキュリティポリシーの見直しが必要となった場合、又は、サイバーセキュリティに関する状況の変化に対応するため、新たに対策が必要となった場合には、サイバーセキュリティポリシーを見直す。

11. サイバーセキュリティ対策基準の策定

7から10までに示す対策等を実施するため、具体的な遵守事項及び判断基準等を定めるサイバーセキュリティ対策基準を策定する。

なお、当該対策基準は、区におけるサイバーセキュリティ対策の基準を定めるものであり、公にすることにより、区行政の運営に重大な支障を及ぼすおそれがあることから、当該対策基準については、4(1)に定める行政機関の適用範囲以外に対しては非公開とする。

12. サイバーセキュリティ実施手順の策定

11に定めるサイバーセキュリティ対策基準を踏まえ、サイバー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サイバーセキュリティ実施手順を策定するものとする。

なお、当該実施手順は、関連する情報システム等のサイバーセキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務の運営に重大な支障を及ぼすおそれがあることから、4(1)に定める行政機関の適用範囲以外に対しては非公開とする。

付 則

(施行期日)

この基本方針は、令和7年9月1日から施行する。