大田区サイバーセキュリティ基本方針

令和８年４月１日

大　田　区
大田区議会

改定履歴

年　月　日	内　容
令和８年４月１日	初版

目　次

１　目的

大田区及び大田区議会（以下「区」という。）は、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、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、区の安定的・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

(1)　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

区の運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

(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)　情報セキュリティポリシー

本基本方針、大田区セキュリティ基本方針及び大田区情報セキュリティ対策基準をいう。

(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、会計年度任用職員、臨時的任用職員、行政委員会委員、大田区議会議員、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。

(7)　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。

(8)　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。

(9)　区民情報系システム

住民サービスの提供等を目的として、主に住民の個人情報及び特定個人情報を取り扱うシステム及びこれらのシステムとデータを連携するシステムをいう。

(10)　内部情報系システム

文書や財務など内部事務での利用を目的として、主に内部事務情報及び職員の認証に関わる情報を取り扱うシステムをいう。

(11)　外部接続システム

インターネットに接続し、外部との情報交換等を行うことを目的としたシステムをいう。

(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（仮想クライアント含む。）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)　管理区域

指定機器やネットワークの重要機器を設置し、当該機器等の管理及び運用を行うための部屋や機器収納庫、収納スペース、並びに外部記録媒体の保管庫等をいう。

(14)　取扱区域

個人番号及び特定個人情報を取り扱う事務を実施する区域をいう。

(15)　クラウドサービス

従来は手元のコンピュータに導入して利用していたソフトウェアやデータ、それらを提供するための技術基盤等を、インターネットなどのネットワークを通じて、利用できるサービスをいう。

(16)　ソーシャルメディアサービス

インターネット上で展開される情報メディアであって、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアである、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のサービスをいう。

(17)　外部サービス

自組織以外の者が一般向けに情報システムの一部又は全部の機能を提供するクラウ

ドサービス、Ｗｅｂ会議サービス、ソーシャルメディアサービス、検索サービス、翻訳サービス、地図サービス、ホスティングサービス等をいう。

(18)　関係団体

大田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、以下に掲げるものをいう。

ア　公益財団法人大田区産業振興協会

イ　大田区土地開発公社

ウ　公益財団法人大田区文化振興協会

エ　一般財団法人国際都市おおた協会

オ　一般財団法人大田区環境公社

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)　不正アクセス、ウイルス攻撃、ランサムウェア攻撃、サービス不能攻撃等のサイバー攻撃及び侵入等の意図的な要因による区が保有する情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、サービス及び業務の停止のほか、内部管理の欠陥など職員等による不正行為等

(2)　区が保有する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、外部サービス設定等の不備、メンテナンスの不備、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、メールの誤送信等の非意図的要因による情報資産の漏えい・破壊・消去、重要情報の詐取、サービス及び業務の停止、不正行為等

(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

４　適用範囲

(1)　実施機関の適用範囲

本基本方針が適用される範囲は、大田区長、大田区教育委員会、大田区監査委員、大田区選挙管理委員会、大田区議会の所管するものとする。

(2)　情報資産の適用範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　情報システム等

イ　個人情報のほか、情報システム等で取り扱うデータ
ウ　情報システム等に関するシステム設計書、ネットワーク図等のシステム関連文書

５　関係団体への指導

大田区は、関係団体に対して、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を含む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、情報セキュリティポリシー及び各所属が策定するセキュリティ実施手順（以下「セキュリティ実施手順」という。）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、情報セキュリティポリシーに基づき、サイバーセキュリティ対策を含む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。

(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含む情報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、区民情報系システム、内部情報系システム、外部接続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、取扱区域、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情報セキュリティポリシーの遵守状況の確認のほか、(8)の業務委託及び外部サービスを利用する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、緊急時対応体制を情報セキュリティポリシーに基づき整備する。

(8)　業務委託及び外部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、区が定めるセキュリティ要件等、サイバーセキュリティを含む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、外部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　セキュリティに関する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、セキュリティに関する監査及び自己点検を実施する。

９　情報セキュリティポリシーの見直し

自己点検及びセキュリティに関する監査の結果、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、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、情報セキュリティポリシーを見直す。

10　セキュリティ対策基準及びセキュリティ実施手順の適用

７から９までに示す対策等の実施にあたり、具体的な遵守事項及び判断基準等は、大田区情報セキュリティ対策基準及びセキュリティ実施手順を適用する。

なお、当該対策基準及びセキュリティ実施手順は、区における情報セキュリティ対

策の基準及び具体的かつ詳細な手順を定めるものであり、公にすることにより、区の運営に重大な支障を及ぼすおそれがあることから、当該対策基準及びセキュリティ実施手順については、４(1)に定める実施機関の適用範囲以外に対しては非公開とする。

付　則

本基本方針は、令和８年４月１日から施行する。