情報セキュリティ基本方針

1.0版

長崎県　交通局

■新規発行／改定記録

発行／改定年月日	版数	文書の新規発行／改定内容	備考
令和８年４月１日	１．０	新規発行	

情報セキュリティ基本方針 目次

１．目的 …… P1

２．定義 …… P1

３．対象とする脅威 …… P2

４．適用範囲 …… P2

５．職員等の遵守義務 …… P2

６．情報セキュリティ対策 …… P2

７．情報セキュリティ監査及び自己点検の実施 …… P3

８．情報セキュリティポリシーの見直し …… P3

９．情報セキュリティ対策基準の策定 …… P4

10．情報セキュリティ実施手順の策定 …… P4

長崎県交通局　情報セキュリティ基本方針

1．目的

本基本方針は、長崎県交通局（以下「交通局」という。）が保有する情報資産の機密性、完全性及び可用性を維持し、情報資産を事故、災害、不正侵入、漏えい、改ざん、サービス利用妨害等の様々な脅威から保護するための必要な対策について、組織的かつ継続的に取り組むための基本的な考え方を定め、交通局における情報セキュリティ水準の維持、向上を目的とする。

2．定義

（１）職員等

交通局の情報資産を取り扱う全ての者（会計年度任用職員及び委託契約により常駐する者等を含む。）をいう。

（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（ハードウェア及びソフトウェア）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）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（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）県庁ＬＡＮ

スマート県庁推進課が管理し、主に一般行政事務用に使用される閉鎖されたネットワークをいう（スマート県庁推進課以外が独自に管理するネットワークは含まない。）。交通局の一部職員が、県庁ＬＡＮに接続したパソコンを利用している。

（10）ＬＧＷＡＮ 接続系

県庁ＬＡＮにおけるネットワークの一つであり、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（マイナンバー利用事務系を除く。）。インターネット環境からの通信は無害化されている。

（11）インターネット接続系

県庁ＬＡＮにおけるネットワークの一つであり、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及びその情報システムで取り扱うデータをいう。ＬＧＷＡＮ接続系からは分離されており、仮想ブラウザ等により分離環境を経由してアクセスすることができる。

(12)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。

(13)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無い等、安全が確保された通信をいう。

(14)外部サービス(クラウドサービス)

ＳａａＳ（Software as a Service)、ＰａａＳ（Platform as a Service)、ＩａａＳ（Infrastructure as a Service）等、事業者等が情報システムの一部又は全部の機能を提供するものをいう。

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

(６)その他、交通局の情報資産の機密性、完全性、可用性を脅かす脅威

４．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。ただし、知事部局で管理するLGWAN接続系、インターネット接続系のネットワークに接続して利用する情報資産は除く。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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及びネットワーク図等のシステム関連文書

５．職員等の遵守義務

職員等は、情報セキュリティ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情報セキュリティ実施手順を遵守しなければならない。

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。ただし、

県庁ＬＡＮにおけるＬＧＷＡＮ接続系、インターネット接続系の対策については、知事部局の方針に準ずる。

（１）組織体制

交通局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。

（２）情報資産の分類と管理

交通局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、当該分類に基づき情報セキュリティ対策を実施する。

（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対策を講じる。

（４）物理的セキュリティ

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

（５）人的セキュリティ情報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

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

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、業務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、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は、迅速かつ適正に対応するものとする。

（８）業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、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、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。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定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を見直す。

９．情報セキュリティ対策基準の策定

上記６、７及び８に規定する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交通局の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。

10．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交通局の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。