公開可

情報通信技術の利用における安全性及び信頼性の確保に関する基本要綱（群馬県情報セキュリティポリシー）

令和７年１月１６日

群　馬　県

公開可

（目次）

公開可

本県のネットワーク、情報システム、コンピュータ等が取り扱う情報には、県民の個人情報のみならず、外部に漏えい、消失した場合には県民生活に重大な影響を及ぼす行政運営上重要な情報等が多数含まれている。

これらの情報並びに情報を取り扱うネットワーク、情報システム、コンピュータ等を様々な脅威から防御することは、県民の財産、プライバシー等を守るためにも、安定的な行政運営のためにも必要不可欠である。ひいては、このことが本県に対する県民からの信頼の維持・向上に寄与する。

このことから、本県が所有する情報資産の機密性、完全性及び可用性を維持するため、本県が実施する対策の基本的な方針及び基準として、情報通信技術の利用における安全性及び信頼性の確保に関する基本要綱（群馬県情報セキュリティポリシー）（以下「群馬県情報セキュリティポリシー」という。）を定める。

群馬県情報セキュリティポリシーは、情報セキュリティ基本方針及び情報セキュリティ対策基準の二階層で構成する。

第１章　情報セキュリティ基本方針

1.　目的

本基本方針は、本県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ため、本県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）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。

（２）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。

（３）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。

（４）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。

（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、地方税若しくは防災に関する事務）に関わる情報システム及びデータをいう。

（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（マイナンバー利用事務系を除く。）。

（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無い等、安全が確保された通信をいう。

（１３）自治体情報セキュリティクラウド

インターネットとの通信の常時監視及びログの分析・解析を始め高度なセキュリティ対策を実施するものをいう。

（１４）クラウドサービス

事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。この構成要素として、SaaS（Software as a Service）[1]、PaaS（Platform as aService）[2]、IaaS（Infrastructure as a Service）[3]が存在する。

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

[1] SaaS：クラウド上のソフトウェア／アプリケーションを利用するサービスであり、利用者には CSP（クラウドサービスプロバイダ）のインフラストラクチャ上で稼動している ASP（アプリケーションサービスプロバイダ）由来のアプリケーションが提供される。

[2] PaaS：クラウド上の OS やミドルウェアなどのプラットフォームを利用するサービスであり、利用者には演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースが提供される。

[3] IaaS：クラウド上のネットワーク、CPU、メモリ、ストレージなどのコンピューティングリソースを利用するサービスとして提供されるインフラストラクチャであり、利用者には演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースが提供される。

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

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、知事部局、企業局、病院局、議会事務局、人事委員会事務局、選挙管理委員会、監査委員事務局、労働委員会事務局、収用委員会、内水面漁場管理委員会、教育委員会事務局及び教育機関、並びに警察本部とする。

（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。

なお、病院局、教育委員会事務局及び教育機関、並びに警察本部において独自に管理する情報資産については、対象外とする。

①ネットワーク[4]及び情報システム[5]並びにこれらに関する設備[6]及び電磁的記録媒体[7]

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[8]

5. 職員等の遵守義務

（１）職員[9]及び派遣労働者（以下「職員等」という。）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並びにネットワーク及び情報システムごとに定める情報セキュリティ実施手順を遵守しなければならない。

（２）職員は、委託事業者に対し、契約等により群馬県情報セキュリティポリシー並びに関係するネットワーク及び情報システムごとに定める情報セキュリティ実施手順を遵守

---

[4] ネットワークの情報資産の例：通信回線、ルータ等の通信機器等

[5] 情報システムの情報資産の例：サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等

[6] これらに関する設備の情報資産の例：コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等

[7] 電磁的記録媒体の情報資産の例：サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、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等

[8] 関連文書の情報資産の例：システム設計書、プログラム仕様書、操作マニュアル、端末管理マニュアル、ネットワーク構成図等

[9] 職員とは、会計年度任用職員を含む全ての職員をいう。

する義務を負わせなければならない。

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。

（１）組織体制

本県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体制を確立する。

（２）情報資産の分類と管理

本県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、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、他の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、両システム間で通信する場合には、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、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、県及び市町村等のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドを利用する。

（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

情報資産を不正なアクセス等から適正に保護するため、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

ネットワーク及び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迅速かつ適正に対応するため、緊急時対応計画を策定する。

（８）業務委託と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。

クラウドサービスを利用する場合には、利用にかか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及び情報セキュリティ実施手順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及び情報セキュリティ実施手順を見直す。

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。

また、情報セキュリティ対策基準は、公にすることにより本県の情報セキュリティ対策に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

ネットワーク及び情報システムを所管する者は、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ネットワーク及び情報システムごとに策定するものとする。

なお、情報セキュリティ実施手順には必ず緊急時対応計画を明記するものとする。

また、情報セキュリティ実施手順は、公にすることにより本県の情報セキュリティ対策に支障を及ぼすおそれがあることから非公開とする。