

議案第 21 号

大野市情報セキュリティポリシー基本方針の改訂（共同策定）について

令和 8 年 3 月 26 日提出

大野教育委員会

教育長 久保俊岳

提案理由

地方自治法の一部改正に伴い、サイバーセキュリティを確保するための方針を定める対象が委員会まで拡大することを受けて、市長等と統一した基本方針を共同策定するもの

(案)

大野市情報セキュリティポリシー (情報セキュリティ基本方針)

大野市
大野市議会
大野市教育委員会
大野市選挙管理委員会
大野市監査委員
大野市農業委員会
大野市固定資産評価審査委員会

令和8年 3月 日 策定

〈 目 次 〉

1	目的	1
2	定義	1
3	対象とする脅威	2
4	適用範囲	2
5	職員等の遵守義務	3
6	情報セキュリティ対策	3
7	情報セキュリティ監査及び自己点検の実施	4
8	情報セキュリティポリシーの見直し	5
9	情報セキュリティ対策基準の策定	5
10	情報セキュリティ実施手順の策定	5

1 目的

本基本方針は、大野市（以下「市」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するため、市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。また、本基本方針は、サイバーセキュリティ基本法（平成26年法律第104号）の趣旨に則り、市におけるサイバーセキュリティの確保に関する施策を総合的かつ効果的に推進するための基本方針としても位置づけるものである。

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、基幹系）

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）又は戸籍事務等に関わる情報システム及びデータをいう。

(9) LGWAN 接続系（内務系）

人事給与、財務会計及び文書管理等 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。

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、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な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) 適用される機関の範囲

本基本方針は、市長（補助機関を含む）、市議会、教育委員会、選挙管理委員会、監査委員、農業委員会及び固定資産評価審査委員会に適用する。

(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、情報システム及び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、会計年度任用職員等（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。

(1) 組織体制

市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

市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靱性の向上

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、都道

府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

サーバ類、サーバ室等、通信回線等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、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、情報資産への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。

(9) 評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

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、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。

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市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。

地方公共団体におけるサイバーセキュリティを確保するための方針の共同策定について①

(大野市情報セキュリティポリシー改訂の概要)

経緯

①地方公共団体におけるサイバーセキュリティを確保するための方針策定の義務づけ

- ・ 地方自治法の一部を改正する法律の改正に伴い、国指針を踏まえた基本方針及び対策基準を策定する必要有り
- ・ **既存情報セキュリティポリシーの見直し**を行ったものをもって方針に**位置付けることが可能**
- ・ 市だけでなく、議会、委員会等も執行機関等対象（一つの方針を**複数機関**で**共同策定可能**）
- ・ **基本方針のみ、R8.4.1までに公表する必要あり**

サイバーセキュリティを確保するための方針
自治体間のネットワーク連携が進み、一団体の不備が他へ影響する恐れが高まったため、法改正で方針策定が義務化。方針は、脅威への備えや事故拡大防止に必要な、統一的で継続的な取組の基本的な考え方を示すもの。

策定の概要

①既存情報セキュリティポリシーに位置付けて共同策定

②改訂1 構成の変更

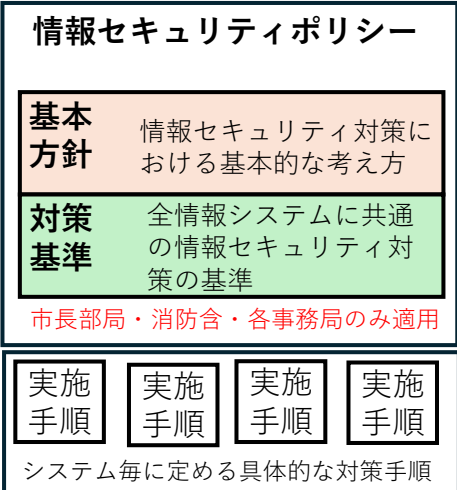
位置づけに必要な見直しの実施

公表義務は基本方針のみ。対策基準の具体項目が未定 ⇒ **基本方針と対策基準を分離**、今回は**基本方針のみを改訂（共同策定）**し、**対策基準**は国が示す具体項目の公表を待って**R9年度末までに改訂（共同策定）**

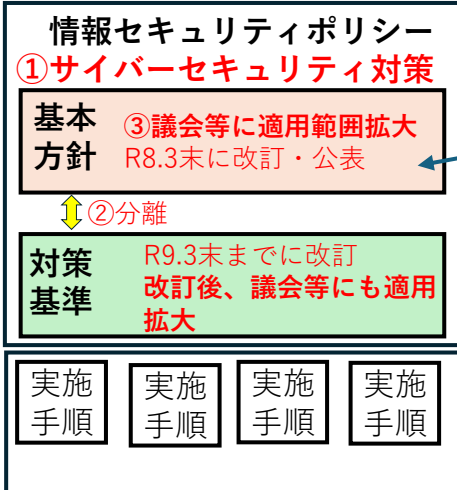
③改訂2 適用範囲を拡大

《改定前》 市長部局、教育委員会**事務局**、議会**事務局**、その他の各行政委員会**事務局**及び消防本部
《改定後》 **市長**（補助機関含む）、**議会**、**教育委員会**、**選挙管理委員会**、**監査委員**、**農業委員会**及び**固定資産評価審査委員会**

<改訂前>



<改訂後>



改訂スケジュール

R8.3末	【市】既存ポリシーを国指針に基づき方針に位置付け、「基本方針」のみ公表	対策基準は、体裁のみの改訂
R8.6頃	【国】地方自治体が必ず実施すべきサイバーセキュリティ対策の具体項目を公表	R9.4.1施行予定
R8.6～R9.3	【市】具体項目を反映し、対策基準を改訂	
R9.3末	【市】セキュリティポリシーの改訂完了	対策基準完全適用

今回の改訂

地方公共団体におけるサイバーセキュリティを確保するための方針の共同策定について② (大野市情報セキュリティポリシーの概要・基本方針改訂後)

議員・各委員が関係する箇所

基本方針

1.情報セキュリティポリシーとは

市の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取りまとめたものの総称。
「情報セキュリティ基本方針（普遍的な考え方）」+「情報セキュリティ対策基準（具体的な対策）」

2.適用範囲

市長（補助機関含む）、**議会、各行政委員会**

3.対象となる情報資産

情報システム **(市・議会・委員会貸与タブレットなど)**、ネットワーク、データなど

対策基準

4.組織体制

情報セキュリティ対策を推進する全庁的な組織体制

- ・CISO（最高責任者）：副市長
- ・統括情報セキュリティ責任者：情報政策担当部長
- ・各部局長：情報セキュリティ責任者
- ・課室長：情報セキュリティ管理者
- ・CSIRT（インシデント対応）

7.システム構造の基本（3領域分離）

- ・マイナンバー系：分離、多要素認証、USB持ち出し禁止
- ・LWAN系：インターネット系と分離、無害化通信で取込
- ・インターネット系：不正通信監視、セキュリティクラウド

10.人的対策（職員等の遵守事項）

- ・情報セキュリティポリシー・手順の遵守
- ・業務外利用・私物端末利用・無断持ち出しの禁止
- ・文書／媒体の適切保管
- ・ID・パスワードの厳格管理・不共有
- ・インシデント・不審事象の速やかな報告
- ・研修受講

5.想定する脅威

- ・不正アクセス、ウイルス、標的型攻撃
- ・誤操作・設定ミス・機器故障
- ・災害、停電・通信障害
- ・大規模疾病等による業務停止

8.技術的対策

- ・アクセス制御、特権ID管理、
- ・ログ取得・分析
- ・ウイルス対策ソフトの最新保持
- ・無許可ソフト・機器禁止、暗号化利用

11.外部委託・外部サービス

- ・委託先のセキュリティ確認
- ・守秘義務・再委託制限など契約明記

6.情報資産の分類と管理

- ・機密性（1～3）／完全性（1～2）／可用性（1～2）に分類
- ・暗号化・持ち出し制限・バックアップ等を分類に応じて実施

9.物理的対策

- ・サーバ室入退室管理
- ・耐震・防火・防水対策
- ・機器持ち出し
- ・廃棄時のデータ消去

12.監査・点検・見直し

- ・内部監査、部局の自己点検
- ・必要に応じポリシー見直し

➡ **対策基準が議員及び各委員に適用されるのは、R9.3末の見込み**

※国が示す対策基準の細目（R8.6公表、R9.4制定見込み）を踏まえつつ、各執行機関の実情に沿った改訂を実施後