古河市情報セキュリティポリシー

平成 17 年 9 月 12 日　策定
平成 20 年 4 月　　全部改正
平成 22 年 8 月　　一部改正
令和元年 12 月　　一部改正
令和 6 年 3 月　　一部改定
令和 8 年 3 月　　一部改定

古　　河　　市
古河市情報セキュリティ委員会

情報セキュリティ及び特定個人情報の安全管理に関する基本方針

1. 目的

本基本方針は、本市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とともに、特定個人情報の適正な取扱いを確保するため、市が講ずる安全管理措置の基本的な事項を定めることを目的とする。

2. 定義

本書における用語の意義は、行政手続における特定の個人を識別する番号の利用等に関する法律（平成 25 年法律第 27 号、以下「番号法」という。）及び古河市個人情報保護条例（平成 17 年条例第 20 号）において使用する用語の例によるほか、巻末の「用語解説／索引」にて定義する。

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（DoS 攻撃及び DDoS 攻撃)、標的型攻撃、ランサムウェア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、内部部局、行政委員会、議会事務局及び地方公営企業とする。

（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、情報システムで取り扱う情報及びこれらを印刷した文書

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

④番号法及び古河市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に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成 27 年条例第 42 号、以下「番号条例」という。）に基づき、市が取り扱う特定個人情報

5. 特定個人情報の安全管理措置

市は、特定個人情報の適正な取扱いを確保するため、上記 3 の脅威に対する情報セキュリティ対策を実施するほか、特定個人情報に係る次に掲げる事項その他の適切な管理のために必要な措置を講ずるものとする。

（１）漏えい、滅失及び毀損の防止

（２）番号法及び番号条例に定められた事務のうち、あらかじめ本人に通知した利用目的の達成に必要な範囲内での適正な収集、保管、利用及び提供並びに不要となった際の速やかな廃棄

（３）目的外利用の防止

6. 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。

7. 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

本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行う。

（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、次の三層の対策を講じる。

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、都道府県及び市区町村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の導入等を実施する。

（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

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、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切に対応するため、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する。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ずる。

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、発信する情報の担当課室長等を責任者として定める。

（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、適宜情報セキュリティポリシーの見直しを行う。

8. 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。

9. 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対策並びに特定個人情報の安全管理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、リスクを検討した上で、情報セキュリティポリシーを見直す。

10. 情報セキュリティ対策基準の策定

上記 7、8 及び 9 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並びに特定個人情報の安全管理に関する基準を策定する。

11. 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及び特定個人情報の安全管理に関する基準に基づき、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とともに特定個人情報の適正な取扱いを確保するための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、本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。

用語解説／索引

（戻る）

BCP（Business Continuity Plan：事業継続計画）

組織において特定する事業の継続に支障を来すと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適正に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。

CRYPTREC（Cryptography Research and Evaluation Committees）

電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。

CSIRT（Computer Security Incident Response Team）

コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う組織の総称。

SLA（Service Level Agreement）

サービス提供者と利用者との間でサービス内容に関し明示的になされた合意であり、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、サービス提供者に保証させることをいう。

URL（Uniform Resource Locator）

インターネット上の情報資源の場所とその属性を指定する記述方式。情報資源の種類やアクセス方法、情報を提供するウェブサーバの識別名、ファイルの所在を指定するパス名などで構成される。

VPN（Virtual Private Network）

暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術である。

Web（ウェブ）会議サービス

専用のアプリケーションやWeb ブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。

暗号化消去

情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。

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）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）が存在する。

クラウドサービス管理者

クラウドサービスの利用における利用申請の許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う者をいう。

クラウドサービス提供者

クラウドサービスを提供する事業者をいう。クラウドサービスを利用して自組織に向けて独自のサービスを提供する事業者は含まれない。

クラウドサービス利用者

クラウドサービスを利用する自組織の職員等又は業務委託した委託先においてクラウドサービスを利用する場合の委託先の従業員をいう。

供給者

サプライチェーンの一部を構成し、データの処理やサービス等で連携する組織をいう。

サプライチェーン

部品やサービス等の供給に多種多様な主体が係わった取引の連鎖をいう。

情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

情報セキュリティ事象

情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

シンクライアント
サーバ側に仮想的なクライアント環境を設けた上で、当該クライアント環境にパソコンやモバイル端末が専用のアプリケーションを使用してアクセスし、パソコンやモバイル端末にデータを保存せずに、データの閲覧や編集を行うことを可能とする機能をいう。

送信ドメイン認証技術
メール送信者情報のドメインが正しいものかどうかを検証することができる仕組みをいう。現在のメール送信においては、送信者情報を詐称することが可能で、実際、多くの迷惑メールは他のアドレスになりすまして送られているため、成りすまし対策として用いられる。

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の在り方で、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のことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったWeb サイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

多要素認証
システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせて認証する方式をいう。認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。それぞれの認証手段には各々異なった利点と欠点があり、複数の認証方式を組み合わせることが利用者認証の信頼性を高める意味でも有効である。

端末
情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、地方公共団体が調達又は開発するものをいう。

庁内ネットワーク
地方公共団体の庁舎・出先機関を含めた団体が管理主体となるネットワーク及び同ネットワークを委託しているデータセンターに設置している情報システムをいう。

電子署名
情報の正当性を保証するための電子的な署名情報をいう。

特権 ID
サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常の ID よりもシステムに対するより高いレベルでの操作が可能な ID をいう。

ドメイン名
国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。

パソコン

端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

標的型攻撃

明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

モバイル端末

端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

リスク分析

リスク特定、リスク分析、リスク評価を網羅するプロセス全体を指す。リスク分析を行った後、リスク対応を行う。リスク対応の手段には、リスク源の除去、起こりやすさの変更、結果の変更、他者とのリスクの共有、リスクの保有などがある。

遠隔消去機能

携帯電話などに記録してあるデータを、当該端末から操作するのではなく離れた場所から、遠隔操作（リモート）で、消去、無効化する機能をいう。携帯電話を紛失・盗難にあった場合の、情報漏えいを防ぐ目的で利用される。

機器等

情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等)、外部電磁的記録媒体等の総称をいう。

＜情報システムの基盤を管理又は制御するソフトウェアの例＞

- 端末やサーバ装置、通信回線装置等を制御するソフトウェア
- 統合的な主体認証を管理するソフトウェア
- ネットワークを制御・管理するソフトウェア
- 資産を管理するソフトウェア
- 監視に関連するソフトウェア
- 情報システムのセキュリティ機能として使用するソフトウェア

令和８年３月

古河市役所　企画政策部　デジタル推進課
〒306-0291　茨城県古河市下大野２２４８
TEL　0280-92-3111（内線 2243・2244）
FAX　0280-92-3225
メール　jouhou@city.ibaraki-koga.lg.jp
HP　　http://www.city.ibaraki-koga.lg.jp