別冊３

豊橋市情報セキュリティに関する対策基準

豊橋市

変更履歴

版数	変更年月日	変更内容
1	平成 15 年 8 月 18 日	策定
2	平成 19 年 4 月 1 日	改定
3	平成 21 年 4 月 1 日	改定
4	平成 23 年 4 月 1 日	改定
5	平成 24 年 4 月 1 日	改定
6	平成 27 年 4 月 1 日	改定
7	平成 28 年 1 月 1 日	改定
8	平成 31 年 4 月 1 日	改定
9	令和 2 年 4 月 1 日	改定
10	令和 2 年 9 月 1 日	改定
11	令和 3 年 4 月 1 日	改定
12	令和 6 年 4 月 1 日	改定
13	令和 7 年 4 月 1 日	改定
14	令和 8 年 4 月 1 日	改定

豊橋市情報セキュリティに関する対策基準

この対策基準は、豊橋市情報セキュリティに関する基本方針（以下「基本方針」という。）を実行に移すための市が所管する情報資産に共通する情報セキュリティ対策の基準を総合的かつ具体的に定めるものである。

ただし、次に掲げる情報資産は対象範囲としない。

(1) 豊橋市民病院が所管する情報資産(行政情報管理システムに係るものを除く。)

(2) 豊橋市議会が所管し、豊橋市議会議員が取り扱う情報資産

第１　組織体制

情報セキュリティを確保するために、次に掲げる管理体制を整備する。

１　最高情報セキュリティ責任者（CISO: Chief Information Security Officer 、以下「CISO」という。）CISO は、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティに関する最終決定権限及び責任を有する者とし、豊橋市副市長事務分担規則第 2 条第 1 項第 1 号に掲げる副市長をもって充てる。

２　統括情報セキュリティ責任者

(1) 統括情報セキュリティ責任者は、本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する者とし、総務部長をもって充てる。

(2) 統括情報セキュリティ責任者は、市が所管する情報資産に共通する情報セキュリティに関する実施手順書（以下「セキュリティ手順書」という。）の作成、維持及び管理を行うとともに、職員等にセキュリティ手順書を遵守させるものとする。

(3) 総務部情報企画課長は、統括情報セキュリティ責任者を補佐するものとする。

３　情報セキュリティ責任者

情報セキュリティ責任者は、部等（豊橋市の政策推進における部等の役割を定める条例（平成 16 年豊橋市条例第 4 号）第 2 条に掲げる組織並びに会計課、監査委員事務局、選挙管理委員会事務局、農業委員会事務局及び議会局をいう。以下同じ。）における情報セキュリティに関する統括的な権限及び責任を有する者とし、部等の長（ただし、市民病院においては事務局長、選挙管理委員会事務局においては総務部長、農業委員会事務局においては産業部長とする。以下同じ。）をもって充てる。

４　情報セキュリティ管理者

(1) 情報セキュリティ管理者は、情報資産（ハードウェア及びソフトウェアを除く。）の情報セキュリティに関する権限及び責任を有する者とし、当該情報資産を所管する課等の長をもって充てる。

(2) 情報セキュリティ管理者は、自己が管理する情報資産へのアクセス権限を有する者を定め、許可した者以外の者が当該情報資産を利用し、又は閲覧することのないよう、適正に管理するものとする。

(3) 情報セキュリティ管理者は、自己が不在の場合に情報資産（ハードウェア及びソフトウェアを除く。）の情報セキュリティに関する権限及び責任を有する者を情報セキュリティ管理者の代理者として指名するものとする。なお、セキュリティ管理者の代理者は、原則として、課長補佐等の管理職から指名するものとする。

5　情報システム管理者

情報システム管理者は、情報システムの情報セキュリティに関する権限及び責任を有する者とし、当該情報システムを所管する課等の長をもって充てる。

(1) 情報システム管理者は、自己が管理する情報システムの開発、設定の変更、運用、更新等の権限及び責任を有するものとする。

(2) 情報システム管理者は、自己が管理する情報システムの情報セキュリティに関する実施手順書（以下「システム手順書」という。）の作成、維持及び管理を行うとともに、当該情報システムへのアクセス権限を付与した職員等にシステム手順書を遵守させるものとする。

(3) 情報システム管理者は、自己が管理する情報システムへのアクセス権限を有する者を定め、許可した者以外の者が当該情報システムを利用することのないよう、適正に管理するものとする。

(4) 情報システム管理者は、所管する情報システムに接続する端末装置の日常管理並びに利用者承認に関する権限及び責任の一部を当該情報システムで取り扱う情報資産を所管する情報セキュリティ管理者に委任することができる。

(5) 住民情報システム及び行政情報管理システムを管理する情報システム管理者は、当該情報システムに接続する他の情報システム間の、ネットワークの構築、設定の変更、運用及び更新等並びに相互調整に関する権限及び責任を有するものとする。

6　情報システム担当者

情報システム担当者は情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者とする。

7　情報セキュリティ委員会

本市の情報セキュリティ対策を統一的に行うため、豊橋市情報化推進会議に情報セキュリティ委員会を設置する。

8　ＣＳＩＲＴ

インシデントに対して迅速かつ適正に対応するため、豊橋市ＣＳＩＲＴ（Computer Security Incident Response Team：シーサート）を設置する。ＣＳＩＲＴは、インシデントの可能性がある事案について、庁内の統合的な窓口として報告を受け、インシデントであるかの評価を行い、関係機関と連携しながら対応するものとする。なお、ＣＳＩＲＴ責任者は統括情報セキュリティ責任者を、ＣＳＩＲＴ副責任者は情報セキュリティ責任者を、ＣＳＩＲＴ管理者は総務部情報企画課長をもって充てる。

第２　情報資産の分類と管理方法

１　重要性による情報資産の分類

本市における情報資産は、次のとおり分類するものとする。

（1）重要性分類Ⅰ

個人情報及びセキュリティ侵害が市民の生命、財産等へ重大な影響を及ぼす情報

ア　行政事務で取り扱う情報資産のうち漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産

イ　「行政文書の管理に関するガイドライン」（平成２３年４月１日内閣総理大臣決定）に定める機密文書に相当する文書

（2）重要性分類Ⅱ

公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報

ア　行政事務で取り扱う情報資産のうち、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産

（3）重要性分類Ⅲ

外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報

（4）重要性分類Ⅳ

重要性分類Ⅰ、重要性分類Ⅱ又は重要性分類Ⅲの情報以外の情報

２　記録媒体の管理

(1) 記録媒体の複製の作成及び適正な保管等により、情報資産の安全を確保するものとする。

(2) 重要性分類Ⅰ、重要性分類Ⅱ又は重要性分類Ⅲに該当する情報資産を記録した記録媒体を保管等のために移送する場合は、受払い及び保管に関する必要事項を記録し、職員等又は委託事業者等に行わせるとともに、記録媒体の物理的な保護措置を講ずるものとする。

(3) 不要となった記録媒体を廃棄処分又は賃借期間満了により返却するときは、当該記録媒体に記録されている重要性分類Ⅰ、重要性分類Ⅱ又は重要性分類Ⅲに該当する情報資産を復元不可能な状態にするものとする。

第3　情報システム全体の強靭性の向上

1　マイナンバー利用事務系

(1) マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

(2) 情報のアクセス及び持ち出しにおける対策

ア　情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

イ　情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

(3) マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

(4) マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

2 LGWAN 接続系

(1) LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、原則、次の実現方法等により、無害化通信を図らなければならない。

ア インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

イ インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

ウ 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(2) LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

3 インターネット接続系

(1) インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

(2) 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する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

第４　物理的セキュリティ

１　主要機器の管理

情報システム管理者は、所管する情報システムの主要機器の管理に関して、次に掲げる物理的セキュリティ対策を実施するものとする。

(1) 主要機器の設置

ア　火災、水害、埃、振動、温度、湿度、静電気及び電磁波等の影響を可能な限り排除した場所に、施錠可能なラックに固定する等の措置を講じたうえで、主要機器の保守を行うために必要なスペースを十分確保して設置するものとする。

イ　電気容量や空調能力の不足等により、主要機器の運用に支障が生じないことを事前に確認するものとする。

ウ　主要機器は、緊急時において円滑に避難できるよう配慮して設置するものとする。

(2) サーバの二重化等

停止した場合に著しく業務に支障の生じる情報システムは、サーバの二重化等の措置を講ずるものとする。

(3) 電源の保護

ア　停電時に安全に主要機器を停止するまでの間、必要な電力を供給できる予備電源を備え付けるものとする。

イ　主要機器や記録されている情報を落雷等による過電流から保護するための措置を講ずるものとする。

(4) 配線の保護

ア　傍受、電磁波障害又は物理的損傷等を受けることがないよう、必要な措置を講ずるものとする。

イ　権限のない者がネットワーク配線の変更、追加を行うことができないように、ネットワーク機器には必要な措置を講ずるものとする。

２　情報システム室の整備

(1) 情報システム室の要件

ア　水害を防止し、確実な入退室管理を行えるよう、２階以上のフロアに設置するものとする。

イ　ドア、窓等の開口部は必要最小限にとどめ、鍵、警報装置等を設置して不正な立入りを防止できるようにするとともに、換気口等の開口部は小動物が侵入できないような措置を講ずるものとする。

ウ　内装に不燃材を使用する等の防火対策を講ずるものとし、主要機器の設置に当たっては、地震等による災害対策を考慮するものとする。

エ　主要機器、周辺装置及び記録媒体に損傷を与えるおそれのない消火剤を備えるものとする。

オ　監視装置等を設置するものとする。

カ　非常用の照明器具等を備えるものとする。

(2) 情報システム室の入退室管理

ア　入室を許可した者以外の者は、入室させないものとする。

イ　入退室管理簿、ＩＣカード等による入退室管理を行うものとする。

(3) 機器等の搬入出

主要機器の搬入出を行う場合は、職員等が立会う等の措置を講ずるものとする。

3　通信回線及び通信回線装置の管理

(1) 庁舎間を結ぶネットワーク回線は、専用回線又は暗号化等の措置を講じた公衆回線等により、十分なセキュリティを確保できるものとする。

(2) 他の情報システム管理者が管理するネットワークとの接続は必要最小限にし、接続ポイントには、ファイアウォール機能を有するネットワーク機器を設置する等、必要な措置を講ずるものとする。

4　端末装置の管理

情報システム管理者は、所管する情報システムに接続する端末装置に盗難防止のための措置を講ずるものとする。

5　その他

情報セキュリティ管理者は、情報システム管理者の例により、適正な物理的セキュリティ対策を講ずるものとする。

第５　人的セキュリティ

1　職員等の遵守事項

(1) 職員等は、業務目的以外で情報資産を使用しないものとする。

(2) 職員等は、端末装置、周辺装置及び記録媒体を庁舎外（市の施設以外）に持ち出す場合、情報システム管理者又は情報セキュリティ管理者の承認を得るものとする。

2　個人端末の業務利用

(1) 職員等が個人で所有する端末を業務利用する場合、自己が管理するシステムに関するアクセスについては情報システム管理者、情報資産へのアクセス等については情報セキュリティ管理者が認めた場合に限り利用できるものとする。

(2) 個人端末利用に当たっては、次に掲げるセキュリティ対策を実施するものとする。

ア　端末内に情報資産を保存しないこと。

イ　アカウント管理を適切に行うこと。

ウ　端末にウイルス対策やパスワードロック等を施し、十分なセキュリティを確保すること。机上の端末等の管理

(3) 机上の端末等の管理

職員等は、自己が使用中の端末装置、周辺装置及び記録媒体を第三者が無断で使用又は情報資産を閲覧できないよう、適正に管理するものとする。

3　研修の実施等

(1) CISO は、研修の計画を策定し、職員等に対して情報セキュリティに関する研修を行うものとする。

(2) CISO は、職員等に対して基本方針及びこの対策基準の啓発を行うとともに、職員等が常に基本方針及びこの対策基準を参照できるよう適正な措置を講ずるものとする。

(3) 情報システム管理者及び情報セキュリティ管理者は、研修の計画を策定し、関係職員等に情報資産（サービスを除く。）の管理に必要な研修を行う等、必要な措置を講ずるものとする。

(4) CISO は、緊急時対応を想定した訓練を定期的に実施することとする。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施するものとする。

4　事故発生時等の対応

(1) 職員等は、情報セキュリティに係る事故又は不正行為、情報システムの欠陥、障害又は誤動作を発見した場合には、その内容に応じて、速やかに情報システム管理者又は情報セキュリティ管理者に報告し、その指示に従って必要な措置を講ずるものとする。

(2) 情報システム管理者は、情報システムの事故等の対応について、緊急連絡体制の整備、被害の拡大防止、復旧、原因究明等の必要な措置を講ずるものとする。

(3) 情報システム管理者は、発生した事故等が重大であると判断した場合は、情報セキュリティ委員会に報告するものとする。

5　ID 及びパスワード等の管理

(1) 職員等の認証等に用いるＩＣカード等の管理

ア　原則として、職員間で共有させないものとする。

イ　業務上の必要によりやむをえず共有させる場合は、管理簿の作成等により適正に管理するものとする。

ウ　職員等は、ユーザ認証に用いるＩＣカード等を保有する場合は、他の者の目に触れないように保管する等、適正に管理するものとする。また、ＩＣカード等を紛失又は破損した場合は、速やかに情報システム管理者又は情報セキュリティ管理者に報告し、その指示に従って適正な措置を講ずるものとする。

(2) パスワード等の管理

ア　職員等は、パスワードを秘密にし、他の者に知られないように適正に管理するものとする。

イ　パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。

ウ　職員等は、パスワードを忘れた場合、他の者に知られた場合又はその恐れがある場合は、情報システム管理者又は情報セキュリティ管理者に報告し、その指示に従ってパスワードを変更する等、適正な措置を講ずるものとする。

エ　機密性の非常に高い複数のシステム間で同一パスワードの使い回しを行わせないものとする。

オ　ＩＤ及びパスワードの共有が認められている情報システムを除き、職員間でＩＤ及びパスワードを共有させないものとする。

カ　ＩＤ及びパスワードを保管するファイルは、情報システム管理者があらかじめ指定した者以外の者が入手できないように、適正に管理するものとする。

第６　技術的セキュリティ

１　コンピュータ及びネットワークの管理

(1) バックアップの作成

サーバに記録された情報については、定期的に記録媒体又は周辺装置によりバックアップ用の複製を作成し、一定の期間保存するものとする。

(2) 技術情報又はソフトウェアの受け渡し

外部と情報システムに関する技術情報又はソフトウェアの受け渡しを行う場合には、あらかじめ統括情報セキュリティ責任者の承認を得るものとする。

(3) メンテナンスの記録等

情報システムのメンテナンスを行う場合には、その作業内容を記録し、一定の期間保存するものとする。

(4) ドキュメントの管理

ドキュメントについては、業務上必要とする者のみが閲覧できることとし、施錠をした書庫に保管する等適正に管理するものとする。

(5) 情報システムへのアクセス記録の取得等

ア　情報セキュリティの確保に必要なアクセス記録を取得し、一定の期間保存するものとする。

イ　アクセス記録の窃取、改ざん及び消去等を防止するため、必要な措置を講ずるものとする。

(6) ネットワークの接続制御、経路制御等

ルータの設置等により適正なネットワーク経路制御を施すものとする。

(7) 他のネットワークとの接続管理

市が所管するネットワーク以外のネットワークとの接続に当たっては、当該ネットワークの構成及びセキュリティレベル等を検討し、市が所管するネットワークの情報セキュリティに支障が生じないことを確認した上で、統括情報セキュリティ責任者の承認を得るものとする。

(8) 無線 LAN の盗聴対策

庁舎内のネットワークに無線回線を使用する場合には、暗号化等の措置を講ずるものとする。

(9) 電子メールの送受信

ア　職員等は、情報システム管理者又は情報セキュリティ管理者が定めるメールボックスの容量及び送受信の容量の制限を遵守するものとする。

イ　職員等は、業務上必要がある場合で、送信する電子情報の安全性が確保できる場合を除いて、電子メールの自動転送機能を使用しないものとする。

ウ　職員等は、電子メールを複数の相手に同時送信する場合、受信者間で電子メールアドレスを秘匿する必要がない場合を除き、受信者間で電子メールアドレスが閲覧できないようにするものとする。

エ　職員等は、重要性分類Ⅰ、重要性分類Ⅱ又は重要性分類Ⅲに該当する電子情報を電子メールで外部に送信する場合は、情報システム管理者又は情報セキュリティ管理者が定める方法で送信するものとする。

(10) 電磁的情報の暗号化等

ア　外部に送る電子情報が完全なものであることを担保する事が必要な場合には、定められたパスワードによる保護又は暗号化を行い送信するものとする。

イ　電磁的情報は、必要に応じて、暗号化を施して管理するものとする。

ウ　暗号化のための鍵は、定められた方法により管理するものとする。

(11) ソフトウェアの追加インストール

情報セキュリティ管理者は、業務上必要なソフトウェアを情報システムに追加インストールする場合には、情報システム管理者の承認を得るものとする。

(12) 機器構成の変更

情報セキュリティ管理者は、情報システムに接続する機器構成の変更、端末装置又は周辺装置の交換、増設等を行う場合には、情報システム管理者の承認を得るものとする。

(13) 不要プロトコルの利用禁止

業務に必要のないプロトコルについては、利用できないよう措置するものとする。

(14) その他

職員等及び委託事業者以外の者が利用する情報システムは、他の情報システムと独立した情報システムとする等、定められた情報セキュリティ対策を実施するものとする。

2　アクセス制御等

(1) アクセス制御

ア　ユーザの認証及び登録等

①　パスワード等によるユーザの認証を行うものとする。

②　ユーザの登録、変更又は抹消の手続き、ユーザに関する登録情報の管理を適正に行うものとする。

イ　ログインに関する設定

ログインの試行回数の制限、アクセスタイムアウトの設定の措置を講ずるものとする。

(2) 特権を付与された ID の管理等

管理者権限（サーバの管理を行うための操作権限をいう。以下同じ。）は、情報システム管理者があらかじめ指定する必要最小限の者に与えるものとする。

(3) 市が所管するネットワークへの外部からのアクセス

ア　市が所管するネットワークへの外部からのアクセスを認める情報システムは最小限に限定するものとする。

イ　市が所管するネットワークへの外部からのアクセスは、適正なアクセスであることを確認できる措置をとるものとする。

ウ　市が所管するネットワークへの外部からのアクセスは、原則として、ファイアウォール等で区切られたサーバのみ認めるものとする。

(4) 端末装置の接続管理

情報システムに接続する端末装置に関し、機器固有情報等の識別コードで自動的に識別する等の措置をネットワーク機器に講ずることにより、不正接続を防止するものとする。

(5) 認証情報の管理

パスワードを職員等自身に設定させる場合には、仮のパスワードを発行し、ログイン後、直ちに職員等に正規のパスワードを設定させるものとする。

(6) 特権による接続時間の制限

管理者権限によるサーバへのアクセス時間は、必要最小限に制限するものとする。

3　情報システムの開発、導入、保守等

情報システム管理者は、情報システムの開発、導入、保守等に当たっては、基本方針及びこの対策基準に従い、適正な情報セキュリティ対策を講ずるものとする。

(1) 情報システムの入出力データのチェック

ア　電子情報の改ざん、操作ミス等による入出力誤り等を速やかに検出するため、入出力データの二重チェックを行う等の適正な対策を施すものとする。

イ　必要に応じて、情報システムにデータチェック機能を組み込むものとする。

4　コンピュータウイルス対策

(1) 情報システム管理者の措置事項

ア　ウイルスに関する情報の収集に努め、職員等に対して、最新の情報を提供するものとする。

イ　定期的なウイルスチェックが行える環境を整備するものとする。

ウ　ウイルスチェックに用いるパターンファイルを常に最新の状態に保つものとする。

(2) 職員等の遵守事項

ア　職員等は、ウイルス対策ソフトを常に有効な状態に保つとともに、最新のパターンファイルでウイルスチェックを行うものとする。

イ　職員等は、電子メールにファイルを添付して送信する場合は、事前にウイルスチェックを行うものとする。

ウ　職員等は、情報システム管理者又は情報セキュリティ管理者が提供するウイルス情報に常に注意するものとする。

エ　職員等は、情報システムに接続する端末装置、周辺装置及び電子媒体がウイルスに感染した恐れがある場合は、直ちにネットワークから切断した上で、情報システム管理者又は情報セキュリティ管理者に報告し、その指示に従って適正な措置を講ずるものとする。

5　不正アクセス対策

(1) 情報システムの設定に係る重要なドキュメントについては、当該ドキュメントが改ざんされていないことを定期的に確認するものとする。

(2) 情報システムに接続する端末装置からの不正アクセスが発見された場合、直ちに情報セキュリティ管理者に通知し、端末装置の情報システムからの切断、不正アクセスを行った者の特定等、適正な処置を求めるものとする。

(3) 不正アクセスによる被害を受けた場合には、その記録を保存するとともに、犯罪の可能性がある場合には、警察等との緊密な連携に努め、再発の防止を図るものとする。

(4) セキュリティホールに関する情報の収集及びセキュリティ診断等の実施によるセキュリティホールの発見に努め、製造元等から提供される修正プログラム等を現行の情報システムへの影響が無いことを確認の上適用するものとする。

6　セキュリティ情報の収集及び提供

(1) 統括情報セキュリティ責任者は、情報セキュリティに関する情報の収集に努め、必要に応じて情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者に提供するものとする。

(2) 情報システム管理者は、情報セキュリティに関する必要な情報を関係職員等に提供するものとする。

第7　運用

1　庁内での情報共有化

情報システム管理者は、庁内で情報の共有化を図る場合、アクセス権限を明確にした上で行うものとする。

2　情報システムの監視

(1) 情報システム管理者は、情報システムが適正に運用されているかを、定期的に監視するものとし、必要に応じてログの分析等を実施する。

(2) 情報システム管理者は、不正なアクセスやサーバの故障等の障害を検知するため、常に情報システムの監視に努めるものとする。

(3) アクセス記録の正確性を確保するため、主要機器等の時刻設定は正確に保つものとする。

(4) 情報システム管理者は、所管する情報システムのインターネットへの常時接続に関し、ネットワークへの侵入を防止するネットワーク機器を設置し、24時間監視を行うものとする。

3　情報セキュリティポリシーの遵守状況の確認

統括情報セキュリティ責任者は、セキュリティ手順書の遵守状況の確認を行うものとし、確認結果を CISO に報告するとともに、遵守されていない事項については速やかに適正な措置を講ずるものとする。

4　その他

情報セキュリティ管理者は、情報システム管理者の例により、適正な運用におけるセキュリティ対策を講ずるものとする。

第8　業務委託と外部サービス（クラウドサービス）の利用

1　委託事業者等に対するセキュリティ対策

(1) 業務委託に関する事項

情報システム管理者及び情報セキュリティ管理者は、委託事業者等（市との契約により、市の情報資産を取り扱う業務又は市の情報システムに係る開発、導入、保守、修理等の業務に携わる者をいう。以下同じ。）との契約に当たっては、情報の守秘義務等の情報セキュリティに関する遵守事項及びこれに違反した場合の措置等を契約書に記載する。また、委託事業者には、業務委託中及び終了時にも情報セキュリティ対策を適切に実施させなければならない。

(2) 氏名等の掲示

情報システム管理者及び情報セキュリティ管理者は、委託事業者等が市の施設内で作業を行う場合は、氏名、委託事業者名等が記載された名札等を常に着用させるものとする。

2　外部サービス（クラウドサービス）の利用（重要性分類Ⅰ・Ⅱの情報を取り扱う場合）

(1) クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は、重要性分類Ⅰ・Ⅱの情報を取り扱う場合、以下を含むクラウドサービスの利用に関する規定を整備しなくてはならない。

ア　クラウドサービスの利用可否を判断する基準（以下、「クラウドサービス利用判断基準」という。）

イ　クラウドサービス提供者の選定基準

ウ　クラウドサービスの利用申請の許可権限者と利用手続

エ　クラウドサービスの利用状況の管理

(2) クラウドサービスの選定

ア　情報システム管理者は、取り扱う情報の格付及び取扱制限を踏まえ、以下に示すクラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。

① 国内法適用

② データの国内保管

③ 画一的な約款の制限

④ 庁外通信回線からのアクセス制限

⑤ 庁外通信回線からのアクセスに対するセキュリティ対策

イ　情報システム管理者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、以下に示す情報セキュリティ対策の選定基準に従って、クラウドサービス提供者を選定すること。また、必要に応じて、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

① クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止

② クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制

③ クラウドサービスの提供に当たり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

④ クラウドサービス提供者及び提供に従事する者の実績・専門性（情報セキュリティに係る資格・実績等）

⑤ 情報セキュリティインシデントへの対処方法、連絡方法及びクラウドサービス提供者との責任分担

⑥ 情報セキュリティ対策その他の契約の履行状況の確認方法

⑦ 情報セキュリティ対策の履行が不十分な場合の対処方法

⑧ 情報セキュリティ監査の受入れ

⑨ サービスレベルの保証

⑩ 再委託における安全担保

⑪ クラウドサービスの終了又は変更時における事前通知等の取り決め及び情報資産の移行方法

⑫　クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティ対策

ウ　情報セキュリティ責任者は、利用するクラウドサービスが、本市が定めたクラウドサービスの利用に関する規定に適合するか評価しなければならない。

(3) クラウドサービスの利用に係る調達・契約

ア　情報システム管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者の利用判断基準及び選定基準並びにその他セキュリティ要件を、必要に応じて調達仕様に含めなければならない。

イ　情報システム管理者は、調達仕様の内容を契約に含めなければならない。

(4) クラウドサービスの利用承認

ア　情報システム管理者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

イ　利用申請の許可権限者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。

(5) クラウドサービスを利用した情報システムの導入・構築時の対策

ア　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

①　不正なアクセスを防止するためのアクセス制御

②　取り扱う情報の機密性保護のための暗号化

③　開発時におけるセキュリティ対策

④　設計・設定時の誤りの防止

⑤　クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

イ　情報システム管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳に記録しなければならない。

ウ　情報システム管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

①　クラウドサービスの情報セキュリティ水準の維持に関する手順

②　クラウドサービスの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

エ　情報システム管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築がなされているか、クラウドサービス事業者に情報を求め、実施状況を確認すること。

(6) クラウドサービスを利用した情報システムの運用・保守時の対策

ア　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

①　クラウドサービス利用に必要な教育

②　不正アクセスを防止するためのアクセス制御

③　クラウドサービスを利用した情報システムの事業継続

④　設計・設定変更時の情報や変更履歴の管理

⑤　インシデント対応

⑥　新たな脅威等に対する見直し

イ　情報システム管理者は、情報セキュリティに配慮した運用・保守がなされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認すること。

(7) クラウドサービスを利用した情報システムの更改・廃棄時の対策

ア　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。

①　クラウドサービスの利用終了時における対策

②　クラウドサービスで取り扱った情報の廃棄

③　クラウドサービスの利用のために作成したアカウントの廃棄

イ　情報システム管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認すること。

3　外部サービス（クラウドサービス）の利用（重要性分類Ⅰ・Ⅱの情報を取り扱わない場合）

(1) クラウドサービスの利用に係る規定の整備

統括情報セキュリティ責任者は、重要性分類Ⅰ・Ⅱの情報を取り扱わない場合のクラウドサービスの利用に関する規定を整備しなければならない。

(2) クラウドサービスの利用における対策の実施

職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で重要性分類Ⅰ・Ⅱの情報を取り扱わない場合のクラウドサービスの利用について、行政デジタル推進室長へ届

け出なければならない。また、情報システム管理者は、当該クラウドサービスの利用において適切な措置を講じなければならない。

第９　監査の実施

この対策基準に定めるもののほか、監査の実施については「豊橋市情報セキュリティ監査実施要綱」により、定める。

第１０　評価及び見直しの実施

１　情報セキュリティ委員会は、基本方針及びこの対策基準の実効性を評価するものとする。

２　情報セキュリティ委員会の長は、評価の結果、基本方針及びこの対策基準の見直しが必要と判断した時は、CISO に報告するものとする。

３　統括情報セキュリティ責任者は、基本方針及びこの対策基準の改正に伴いセキュリティ手順書を修正するとき、又はセキュリティ手順書の実効性の評価の結果必要な見直しを行うときは、CISO の承認を得るものとする。

第１１　実施手順書の作成、維持及び管理

１　統括情報セキュリティ責任者は、第１の２の（２)の規定により作成するセキュリティ手順書には、次に掲げる事項を定めるものとする。

(1) 情報資産を利用する職員等が遵守すべき事項

(2) 情報セキュリティ管理者が留意すべき事項

(3) 前各号に定めるものの他、情報セキュリティを確保するために必要な事項

２　統括情報セキュリティ責任者は、セキュリティ手順書を作成するときは、CISO の承認を得るものとする。

３　統括情報セキュリティ責任者は、職員等が常にセキュリティ手順書を参照できるよう適正な措置を講ずるとともに、第三者が許可なく閲覧できないようにするものとする。

４　情報システム管理者は、第１の５の(２)の規定により作成するシステム手順書には、次に掲げる事項を定めるものとする。

(1) 情報システムへのアクセス権限に関する事項

(2) 情報システムを利用する職員等が遵守すべき事項

(3) 情報セキュリティ管理者が留意すべき事項

(4) 前各号に定めるものの他、情報システムにおいて情報セキュリティを確保するために必要な事項

5　情報システム管理者は、システム手順書を作成するときは、情報セキュリティ責任者の承認を得るものとする。

6　情報システム管理者は、システム手順書の遵守状況の確認を行うものとし、確認結果を情報セキュリティ責任者に報告するとともに、遵守されていない事項については速やかに適正な措置を講ずるものとする。

7　情報システム管理者は、基本方針及びこの対策基準の改正に伴いシステム手順書を修正するとき、又はシステム手順書の実効性の評価の結果必要な見直しを行うときは、情報セキュリティ責任者の承認を得るものとする。

8　情報システム管理者は、自己が管理する情報システムへのアクセス権限を付与した職員等が、常にシステム手順書を参照できるよう適正な措置を講ずるとともに、第三者が許可なく閲覧できないようにするものとする。

第１２　対策基準の取扱い

この対策基準は、職員等以外の者が知ることにより、情報セキュリティに重大な支障が発生する可能性があるため、みだりに職員等以外の者が知り得る状態においてはならない。

第１３　特定個人情報等の取扱い

この対策基準に定めるもののほか、特定個人情報等の取扱いについては「豊橋市特定個人情報等の取扱いに関する管理要綱」により、定める。

第１４　委任

この対策基準に定めるもののほか必要な事項は、別に定める。