京都府情報セキュリティ対策基準

１　目的

京都府情報セキュリティ対策基準（以下「対策基準」という。）は、京都府情報セキュリティ基本方針（以下「基本方針」という。）を実施する上で必要な情報セキュリティ対策の基準を定めることを目的とする。

２　組織・体制

府の情報セキュリティ管理の組織・体制は次のとおりとする。

(1) 最高情報セキュリティ責任者

ア　全ての情報資産の管理及び情報セキュリティ対策に関する権限及び責任を有する最高情報セキュリティ責任者（Chief Information Security Officer 以下「CISO」という。）を置く。

イ　CISOは、政策企画部情報政策統括監の職にある者をもって充てる。

ウ　CISOは、基本方針や対策基準の改正等の情報セキュリティ対策に関する重要事項について、京都府IT推進本部へ報告し、了承を得るものとする。

(2) 最高情報統括責任者

ア　京都府における情報通信技術の活用による府民サービスの向上や業務改革のための施策の推進を統括する最高情報統括責任者（Chief Information Officer 以下「CIO」という。）を置く。

イ　CIOは、政策企画部情報政策統括監の職にある者をもって充てる。

ウ　CIOは、情報通信技術の活用による府民サービスの向上や業務改革のための施策の推進に関する重要事項について、京都府IT推進本部へ報告し、了承を得るものとする。

(3) 情報セキュリティ責任者

ア　本庁の課（室）又は地方機関の長（以下「所属長」という。）を、当該組織の情報セキュリティ対策に関する権限及び責任を有する情報セキュリティ責任者とする。

なお、大規模な地方機関等については、CISOの承認を得て、当該地方機関の長が指定する職にある者を情報セキュリティ責任者とすることができる。

イ　情報セキュリティ責任者は、各所属において、対策基準及び情報システム管理者が定める情報セキュリティ対策の実施手順（以下「実施手順」という。）が遵守されるよう必要な措置を講じるものとする。

ウ　情報セキュリティ責任者は、IT推進員及び専門知識を取得した情報セキュリティ操作認定者（CISOが定めるセキュリティ対策に関する研修を修了した者をいう。以下同じ。）に情報セキュリティに関する事務を補佐させることができる。

(4) 情報システム管理者

ア　各情報システムを所管する所属長を、当該情報システムに係る情報システム管理者とする。

イ　情報システム管理者は、実施手順を策定するとともに、その維持・管理を行うものとする。

ウ　情報システム管理者は、所管する情報システムに係る開発、設定の変更、運用、更新等を行う権限及び責任を有する。

エ　情報システム管理者は、所管する情報システムに係る情報セキュリティ対策に関する権限及び責任を有する。

(5) 情報セキュリティインシデント対応チーム

ア　CISOは、次に掲げる措置等を行うため、情報セキュリティインシデント対応チーム（Computer Security Incident Response Team 以下「CSIRT」という。）を置く。

① 発生した情報セキュリティインシデント（ウイルス感染、不正アクセス、情報漏えい等の情報資産のセキュリティを脅かす事象。以下「インシデント」という。）の正確な把握及び分析

② 発生したインシデントに対する、迅速かつ的確な被害拡大防止、復旧、再発防止等の措置

③ インシデントが発生し、又は発生するおそれがある場合に備えた、緊急時対応計画（以下「緊急時対応計画」という。）の策定及び変更

④ 情報システムにおける情報セキュリティ対策に関する監査

⑤ その他情報セキュリティに関する必要な措置

イ　CSIRTのチーム員は、次に掲げる職員をもって充てる。

① 政策企画部情報政策課の職員

② 知事部局、議会事務局、各行政委員（会）及び警察本部の推薦に基づきCISOが指名する者

③ ②の他、チーム員として適当と認められるもののうち、CISOが指名する者

ウ　CSIRTにチーム責任者を置き、チーム員のうちから、CISOが指名する。

エ　CSIRTの事務局は、政策企画部情報政策課に置く。

3　適用機関

対策基準の適用機関は、府の知事部局、議会事務局、各行政委員（会）及び警察本部とする。

なお、個別の事情を考慮した情報セキュリティ対策に関する規程を策定し、CISOの承認を得た場合は、対策基準は適用しないものとする。

4　物理的セキュリティ対策

(1) 情報システム

ア　機器の設置等

機器の設置等に当たっては、次に掲げる措置を講じるものとする。

(ｱ) 重要な情報システムのサーバー等については、原則としてデータセンターに設置し、他のシステムのサーバー等については庁舎内の専用の管理区域（ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等又は情報資産の管理並びに運用を行うための区画をいう。以下同じ。）に設置すること。なお、これらの場所に設置できないやむを得ない事由がある場合にあっては、温度、湿度、ほこり等の環境の影響を可能な限り排除した場所に設置すること。

(ｲ) 必要に応じ、容易に取り外せないようにするなど適切な措置を講じること。

(ｳ) 情報システムの重要度に応じて、機器の二重化や地震対策等運用環境を考慮すること。

(ｴ) ネットワークに接続できない等の事由で情報セキュリティを維持できない機器については、USBポート等の外部機器と接続可能なインターフェイスを封印すること。

イ　電源

(ｱ) サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けること。

(ｲ) 落雷等による過電流に対してサーバ等の機器を保護するための措置を講じること。

ウ　ネットワーク

(ｱ) ネットワーク回線は、傍受・損傷等を受けることがないよう、可能な限りの措置を講じること。

(ｲ) CISOの許可なく、庁舎内、庁舎間及び庁舎と外部機関等との間のネットワーク回線を追加又は変更してはならない。

() 行政目的のネットワークにおける無線LAN機器の設置を禁止する。ただし、災害・防災対策や府民サービスの向上等の目的で無線LAN機器を設置しようとする場合は、予算要求前に使用するネットワーク、強固な暗号化方式、認証方法、アクセスログ取得、災害時においてセキュリティを解除する要件等を記載した計画書を作成し、CISOに協議しなければならない。

(2) 管理区域

ア　管理区域は、水害対策及び確実な入退室管理を行うために、地階又は１階に設けることは可能な限り避けること。

また、外部からの侵入が容易にできないように管理区域は可能な限り無窓の外壁等に囲まれた区画とすること。

イ　管理区域から外部に通じる出入口は１箇所のみとし、ICカード等による入退室管理、入退室管理簿の記載、監視機能、鍵、警報装置等によって許可されていない立入りを防止すること。

ウ　管理区域には、ビデオカメラ等の監視機能を設置すること。

エ　管理区域内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を

講じること。

なお、管理区域内の機器類の配置は、緊急時に円滑に避難できるように配慮すること。

オ　管理区域を囲む外壁等の床下開口部はすべて塞ぐこと。

カ　消火剤は、機器及び記録媒体に影響を与えないものであること。

(3) 情報システムを庁舎外に設置又はクラウドサービスを利用しようとする場合

情報システム管理者は、情報システムを庁舎外に設置又はクラウドサービスを利用しようとする場合は、あらかじめCISOの承認を受けるものとする。

(4) 情報資産の管理方法

ア　情報資産に関する業務に携わるすべての職員（非常勤職員等を含む。）及び情報資産に関する業務の受託者又は機器のリースを行う者（以下「受託・リース事業者」という。）（以下合わせて「職員等」という。）は、情報セキュリティの確保のため、電子計算機のハードウェアのうちハードディスク、ＳＳＤ等の記憶保持動作を要することなくデータを記憶する装置（以下「記憶装置」という。）及び記録媒体について、暗号化等の必要な措置を講じるものとする。

イ　職員等は、業務上やむを得ず記憶装置及び記録媒体を持ち出す場合、情報セキュリティ責任者は管理簿を設けるなど適切に管理するものとする。

ウ　記憶装置及び記録媒体の管理

(ｱ) 取り出しが可能な記録媒体は、盗難や損傷、ウイルス被害防止等のためウイルスチェックを行うなど適切な管理を行うこと。

(ｲ) 記憶装置及び記録媒体に納められた情報資産のうち、重要な情報資産は、別の記録媒体に複製し、当該記録媒体は自然災害を被る可能性が低い地域に別途保管すること。

(ｳ) 重要な情報資産を記録した記憶装置及び記録媒体は、耐火、耐熱、耐水及び耐湿対策を講じた施錠可能な場所に管理又は保管すること。

(ｴ) 記憶装置及び記録媒体が不要となり廃棄する場合又はリース期間満了等により返却する場合、情報セキュリティ責任者から指名された職員又は受託・リース事業者はデータを復元できない方法で消去しなければならない。

データ消去を行う者は、処理日時、処理者及び処理内容を記録し、情報セキュリティ責任者へ報告すること。

ただし、特定個人情報又は大量の個人情報を取り扱う記憶装置及び記録媒体については、物理的又は磁気的な破壊を行った上で廃棄することとする。

なお、受託・リース事業者がこれらの処理を行った場合は、処理前後の画像を含む記録とともに、機器の破壊、データの消去及び廃棄した旨の証明書を提出すること。

５　人的セキュリティ対策

(1) 職員等の責任

ア　情報セキュリティ対策の遵守義務

(ｱ) 職員等は、基本方針及び対策基準に定められている事項を遵守すること。

(ｲ) 情報セキュリティ対策について不明な点、遵守することが困難な点が発生したときは、速やかに情報セキュリティ責任者に連絡すること。

(ｳ) 情報システム管理者は、次のイに該当する行為が行われていると認める場合は、当該職員等に対して情報システムの利用を停止することができる。

イ　情報システム利用上の注意事項

職員等は、情報システムの利用に当たって次の行為を行ってはならない。

(ｱ) 業務目的以外で情報システムを利用すること。

(ｲ) 情報資産を執務室外に持ち出すこと。ただし、情報資産を別の記録媒体に保存するなどやむを得ない理由のある場合で、かつ情報セキュリティ責任者の事前の了解を得た場合を除く。

(ｳ) 情報システム管理者の許可を得ずにソフトウェアを導入すること。

(ｴ) 利用する端末や記録媒体について、許可のない第三者に利用又は閲覧され得る状態にすること。

(ｵ) 府の情報システム以外の端末を業務目的で使用すること。

(ｶ) 府の情報システムに記録媒体を接続すること。ただし、CISOが必要と認めた場合であって、CISOが指示した方法による接続を除く。

(ｷ) 府の情報システムの端末を公衆無線LANに接続すること。ただし、CISOが必要と認めた場合であって、CISOが指示した方法による接続を除く。

ウ　受託・リース事業者が管理区域へ入る場合は、必要に応じて職員（非常勤職員等を除く。）が立ち会うこと。

エ　特定個人情報を取り扱うシステムの作業については、職員の立会の下で行うか、又は管理区域内にあらかじめ定められた監視カメラが設置されている場所で行わなければならない。

オ　その他

職員等は、知り得た情報資産を漏えいしてはならない。その職を退いた後も、また、同様とする。

(2) パスワード及びICカードの管理

ア　職員等は、パスワード等に関し、次に掲げる事項を遵守すること。

(ｱ) 他の職員等のユーザ名を使わないこと。

(ｲ) パスワードを秘密にし、パスワードの照会等には一切応じないこと。

(ｳ) パスワードは８桁以上とし、文字列はアルファベット、数字及び記号を混在させるなど容易に推定できないものとすること。

ただし、特定個人情報を取り扱うシステムについては、１１桁以上とすること。

(ｴ) パスワードは定期的に変更し、古いパスワードの再利用はしないこと。

(ｵ) パスワードの盗用や漏えいがあった場合は、直ちに情報システム管理者に報告し、パスワードを変更すること。

(ｶ) その他、ユーザ名及びパスワードの適正な管理を行うこと。

イ　情報システム管理者のパスワード管理

情報システム管理者は、職員等のパスワードに関する情報を厳重に管理するものとする。

ウ　ICカード等の管理

(ｱ) 職員等は、ICカード等を紛失した場合には、速やかに情報セキュリティ責任者及び情報システム管理者に報告すること。

(ｲ) 情報システム管理者は、(ｱ)の規定により報告があり次第速やかに当該ICカード等を利用したアクセス等を停止すること。

(3) 教育・訓練

ア　CISOは、情報セキュリティに対する意識を醸成し保つため、職員等に対し普及啓発するとともに、情報セキュリティに関する理解が深まるよう教育・訓練を行うものとする。

イ　情報システム管理者は、情報システムに不測の事態が発生した場合に備えた訓練を行うものとする。

ウ　情報セキュリティ責任者、IT推進員及び情報セキュリティ操作認定者は、毎年定められたセキュリティ対策に関する研修を修了しなければならない。

なお、情報セキュリティ操作認定者が研修を修了しなかった場合、そのを取り消すものとする。

(4) 事故、欠陥に対する報告

ア　職員等は、インシデントの発生及び発生のおそれがある場合には、直ちに情報セキュリティ責任者に報告し、その指示に従い必要な措置を講じるものとする。

イ　情報セキュリティ責任者は、インシデントの報告を受けた場合は、直ちに当該インシデントの内容を情報システム管理者及びCSIRTに報告するとともに受託・リース事業者等の関係者（以下「関係者」という。）に連絡するものとする。

(5) 外部委託に関する管理

ネットワーク及び情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から再委託等を受ける事業者も含めて、下記の事項を明記した契約を締結するものとする。

ア　基本方針及び対策基準の遵守

イ　業務上知り得た情報の守秘義務

ウ　府から提供された情報の目的外利用及び受託者以外の者への提供の禁止

エ　府から提供された情報の返還及び廃棄義務

オ　外部委託事業者の責任者や業務に携わる社員の名簿の提出

カ　基本方針及び対策基準が遵守されなかった場合の損害賠償等の規定
キ　府の監査を受ける義務

６　技術的セキュリティ対策

(1) アクセス記録の取得等

ア　情報システム管理者は、重要な情報システムについて、各種アクセス記録及び情報セキュリティ対策に必要な記録を取得し、１年以上の期間を定めて、保存するものとする。

イ　情報システム管理者は、重要な情報システムについて、定期的にアクセス記録等を分析、監視するものとする。

ウ　情報システム管理者は、アクセス記録等が窃盗、改ざん、消去されないように必要な措置を講じるものとする。

(2) 機器構成変更の禁止

職員等は、情報システムの端末等に対して機器の増設又は改造等を行わないものとする。

ただし、次のいずれかに該当する場合を除く。

ア　業務を円滑に遂行するためやむを得ない理由がある場合で、かつ情報システム管理者に事前に申請し、了解を得た場合

イ　特定個人情報を取り扱うシステムにおいては、業務を円滑に遂行するためやむを得ない理由がある場合で、かつ情報システム管理者及びCISOに事前に申請し、了解を得た場合

(3) アクセス制御

ア　情報システム管理者は、情報システムにおけるアクセス制御について次の事項を遵守するものとする。

(ｱ) アクセス権限の許可は必要最小限にすること。

(ｲ) 不正アクセスを防止するため、ユーザ認証、論理的なネットワークの分割、ファイアウォールの設置等の適切なネットワーク経路制御を講じること。

(ｳ) アクセス方法等は職員等の真正性が確保できるものにすること。

(ｴ) 特定個人情報を取り扱うシステムについては、ID、パスワードに加えて生体認証、ICカード等の認証方法を導入し、二要素認証とすること。

イ　職員は庁舎外から府の情報システムにアクセスしようとする場合は、あらかじめCISO及び情報セキュリティ責任者の許可を得なければならない。

また、許可に当たってCISOは、以下の措置を講じなければならない。

(ｱ) システム上利用者の本人確認を行う機能を確保すること。

(ｲ) 通信途上の盗聴を防御するため暗号化等の措置を講じること。

(ｳ) 特定個人情報を取り扱うシステムにはアクセスできない仕組みを構築すること。

ウ　接続した情報通信機器についてセキュリティ上の問題があり、情報資産を脅かすおそれがあると認められる場合には、速やかに当該情報通信機器をネットワークから物理的に隔離するものとする。

(4) 外部ネットワークとの接続

府の情報システムと府以外の機関の情報システム（以下「外部ネットワーク」という。）との接続については、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を検討し、府の情報資産に影響が生じないことをCISOが確認した上で接続を認めるものとする。

なお、接続に当たって、情報システム管理者は、次の事項を遵守するものとする。

ア　不正アクセスを防止するためのファイアウォールの設置や職員等の認証、論理的なネットワークの分割等適切なネットワーク経路制御を講じること。

イ　外部ネットワークとの接続により情報システムの運用及び情報資産の保持に支障が生じるおそれがある場合は、直ちに当該情報システムと外部ネットワークとの接続を物理的に遮断すること。

(5) システム開発、導入、保守等

ア　情報システムの調達

(ｱ) 情報システムの調達（更新を含む。）を実施する場合、情報システム管理者は予算要求前、調達実施前、運用開始前の各段階で、セキュリティ確保方策等についてCISO及びCIOと協議し、承認を受けなければならない。

なお、協議の結果、CISO又はCIOから指導があった場合、情報システム管理者はその指導を遵守するものとする。

(ｲ) 情報システム管理者は、情報システムの機器及びソフトウェアの調達に伴う仕様書の作成については、情報セキュリティ対策上支障が生じるおそれのある内容を記載しないようにすること。

(ｳ) 情報システム管理者は、機器及びソフトウェアを調達する場合は、当該製品の安全性及び信頼性を確認すること。

イ　情報システムの開発

情報システム管理者は、情報システムの開発を行う場合、次の事項を実施するものとする。

(ｱ) 情報システムの開発、保守等に関するインシデント発生のリスク（危険性）について十分検討を行うこと。

(ｲ) 情報システムの開発環境及びテスト環境と運用環境を分離し、開発環境及びテスト環境から運用環境への移行について、その手順を明確にすること。

(ｳ) システム開発時に使用するID、パスワード等を適切に管理し、開発終了後、不要になったID、パスワード等は、速やかに抹消すること。

ウ　情報システムの導入

情報システム管理者は、情報システムの導入を行う場合、次の事項を実施するもの

とする。

(ｱ) 既に稼働している情報システムとの整合性を確認する等十分なテストを行い、その結果を適切に保管すること。

(ｲ) 情報システムの開発及び保守に係る記録を作成し、適切に保管すること。

エ　ソフトウェアの更新及び保守

(ｱ) 情報システム管理者は、OS等を更新又は修正プログラムを適用する場合は、不具合がないこと及び他のシステムとの適合性の確認を行った上で、計画的に更新又は適用すること。

オ　システム変更等の記録管理

(ｱ) 情報システム管理者は、所管する情報システムにおいて、システム変更等の作業を行う場合、その内容について事前に確認するものとする。

(ｲ) 情報システム管理者は、システム変更等の作業を行った場合は、その内容について記録を作成し、適切に保管するものとする。

(6) 不正プログラム対策

ア　情報システム管理者は、コンピュータウイルス等の不正プログラム対策として、次の事項を実施しなければならない。

(ｱ) 外部ネットワークからデータを受け入れる際には、ファイアウォールを適切に設定するとともに、ウイルスチェックサーバ等においてコンピュータウイルス等の不正プログラムのチェックを行い、コンピュータウイルス等の不正プログラムのシステムへの侵入を防止すること。

(ｲ) 外部ネットワークへデータを送信する際にも、(ｱ)と同様のコンピュータウイルス等の不正プログラムのチェックを行い、外部へのコンピュータウイルス等の不正プログラムの拡散を防止すること。

(ｳ) コンピュータウイルス等の不正プログラム情報を収集し、必要に応じて職員等に対する注意喚起を行うこと。

(ｴ) 端末においてコンピュータウイルス等の不正プログラム対策用のソフトウェアを導入し、常に稼働させること。

(ｵ) コンピュータウイルス等の不正プログラム対策用ソフトウェアは、常に最新の状態に保つこと。

(ｶ) コンピュータウイルス等の不正プログラム対策用ソフトウェアのパターンファイルは、常に最新の状態に保つこと。

(ｷ) セキュリティホール等に対する修正プログラムを入手し、サーバ及び端末に速やかに適用すること。

イ　職員等は、次の事項を遵守しなければならない。

(ｱ) 端末に導入されているコンピュータウイルス等の不正プログラム対策用ソフトウェアの設定を変更してはならない。

(ｲ) 外部からデータまたはソフトウェアを取り入れる場合には、必ずコンピュータウイルス等の不正プログラム対策用ソフトウェアによるチェックを行うこと。

(ｳ) 差出人が不明または差出人に心当たりがないメールに添付されたファイルやリンクは、開かず速やかに削除すること。

(ｴ) 情報システム管理者が提供するウイルス情報を常に確認すること。

(ｵ) コンピュータウイルス等の不正プログラムに感染し、又は感染したおそれがある場合は、直ちに端末の電源を切るとともに、端末のLANケーブルを取り外し、情報セキュリティ責任者及びCSIRTに報告するとともに、関係者に連絡するものとする。

ウ　情報セキュリティ責任者は、イの(ｵ)の規定による報告を受けた場合は、直ちにその内容を情報システム管理者及びCSIRTに報告するとともに、関係者に連絡を行い、情報の復旧等必要な措置を講じなければならない。

(7) 不正アクセス対策

ア　情報システム管理者は、不正アクセスを防止するため、次に掲げる対策を講じるものとする。

(ｱ) ソフトウェアの不備に伴うセキュリティホールに対しては、速やかに修正プログラムを適用すること。

(ｲ) 情報システム上の不要なユーザ名は、速やかに削除すること。

(ｳ) 重要な情報システムの設定に係るファイル等について、当該ファイルの改ざんの有無を検査すること。

(ｴ) 不正アクセスを受けるおそれが認められる場合には、情報システムの停止を含む必要な措置を講じること。

(ｵ) 利用終了又は利用される予定のない不要なポートは閉めること。

イ　職員等は、不正アクセスを受け、又は受けたおそれがある場合は、直ちに情報セキュリティ責任者及びCSIRTに報告するものとする。

ウ　情報セキュリティ責任者は、イの規定による報告を受けた場合は、直ちにその内容を情報システム管理者及びCSIRTに報告するとともに、関係者に連絡を行い、情報の復旧等必要な措置を講じなければならない。

エ　情報システム管理者は、不正アクセスを受け、又は受けたおそれがある場合は、CSIRTに報告するとともに関係者に連絡を行い、情報の復旧等必要な措置を講じなければならない。

(8) セキュリティ情報の収集

ア　情報システム管理者は、情報セキュリティに関する情報を収集し、情報システムについてソフトウェアに修正プログラムを適用する等、セキュリティ対策上必要な措置を講じるものとする。

イ　CSIRTは、前項の情報を情報システム管理者及び情報セキュリティ責任者に通知するものとする。

7　運用及び緊急時におけるセキュリティ対策

(1) 情報システムの監視

ア　情報システム管理者は、情報システムの円滑な運用を確保するため、情報システムを定期的に監視し、障害が起きた際は速やかに対応するものとする。

イ　情報システム管理者は、外部ネットワークと常時接続するシステムについては、ネットワーク侵入監視装置を設置する等厳重な監視を行うものとする。

ウ　情報システム管理者は、情報システム内部において、適正なアクセス制御を行い、運用状況について監視されないよう必要な措置を講じ、安全な場所に保管するものとする。

(2) 対策基準の遵守状況の確認

ア　職員等は、この対策基準に違反した場合又は違反事実を確認した場合は、直ちに情報セキュリティ責任者に報告するものとする。

イ　情報セキュリティ責任者は、対策基準の遵守状況及び情報資産の管理状況について定期的に確認を行い、支障を認めた場合には速やかに情報システム管理者及びCSIRTに報告するものとする。

　なお、情報システム管理者が支障を確認した場合には、迅速かつ適切に対処するものとする。

ウ　CISO及びCISOが指名した者は、不正アクセス、不正プログラムの調査を行うため、必要に応じて職員等が使用している端末及び記録媒体のログ、電子メールの送受信記録等の利用状況を調査することができる。

(3) 緊急時の対応等

ア　情報セキュリティ責任者は、インシデント発生等の場合に備えて、あらかじめ所管するシステムにおける関係者との連絡体制を整備するものとする。

イ 情報システム管理者は、インシデント発生等の場合、緊急時対応計画に基づき、CSIRTと連携、共同してインシデントへの対応措置を行うものとする。

ウ 情報システム管理者は、インシデントが発生又は発生するおそれがあり、情報資産の保持のために情報システムの停止がやむを得ないと認められる場合は、CSIRTと協議の上、ネットワークを遮断することができる。

エ　情報システム管理者は、ウの規定によるネットワークの遮断又は自然災害等により、所管する情報システムが停止した場合において、所管する業務を継続して行うことができるよう、あらかじめ業務継続計画を策定するものとする。

(4) 例外措置

ア　情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、CISOの許可を得た上で、例外措置を取ることができる。

イ　情報セキュリティ責任者及び情報システム管理者は、大規模災害等に起因する行政

事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにCISOに報告すること。

ウ　CISOは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

８　監査、評価及び見直し

(1) 内部監査

ア　CISOは、CSIRTのチーム員のうちから、次に掲げる要件を全て満たす職員を情報セキュリティ監査統括責任者（以下「監査責任者」という。）に指名し、情報システムにおける情報セキュリティ対策について、必要に応じて監査を行わせるものとする。

① 監査対象所属以外の職員

② 監査対象所属と業務上の関連を有する所属以外の職員

③ 監査及び情報セキュリティに関する専門知識を有する職員

イ　監査責任者は、監査を実施するに当たっては、監査実施計画を作成し、CISOの承認を得なければならない。

ウ　監査対象所属は、監査の実施に協力しなければならない。

エ　委託事業者に委託している場合、監査責任者は、委託事業者から再委託等を受けている事業者も含めて、監査を行わなければならない。

オ　監査責任者は、監査結果を取りまとめの上、CISOに報告する。

カ　監査責任者は、監査の実施に当たって監査対象所属の情報セキュリティ責任者から提出された監査調書や監査責任者が収集した証拠資料等については、紛失等することのないよう、適切に保管しなければならない。

キ　CISOは、監査結果を踏まえ、監査対象所属の情報セキュリティ責任者に対しての指摘事項を通知し、当該事項への対処を指示しなければならない。

ク　キの規定による指示を受けた情報セキュリティ責任者は、当該指示に対する措置を講じたときは、速やかにCISOに報告しなければならない。

なお、当該指示に対する措置を講じるまでの間については、その進捗状況を少なくとも年１回、CISOに報告しなければならない。

(2) 外部監査

ア　CISOは、必要に応じて、情報システムにおける監査及び情報セキュリティに関する専門知識を有する者を外部監査人に指名し、情報セキュリティ対策について、監査を行わせることができる。

イ　監査の実施に当たっては、(1)のイからクまでの規定を準用する。

(3) 評価

情報システム管理者は、この対策基準を踏まえた情報セキュリティ対策の遵守状況について定期的に検証し、その結果をCISOに報告するものとする。

(4) 対策基準の見直し

CISOは、監査の結果及び情報セキュリティに関する状況の変化等を踏まえた評価の結果、必要があると認めた場合、対策基準の見直しを行い、その内容をIT推進本部に報告し、了解を得るものとする。