地方独立行政法人大阪市民病院機構

情報セキュリティ対策基準

直近改定：令和８年３月17日

制　定：平成26年10月１日

[目次]

7.5 法令遵守

8. 業務委託と外部サービスの利用

8.1 業務委託

（1）委託事業者の選定基準

（2）契約項目

（3）確認・措置等

8.2 外部サービスの利用 （機密性2以上の情報を取り扱う場合）

9. 評価・見直し

9.1 監査

（1）実施方法

（2）監査を行う者の要件

（3）監査実施計画の立案及び実施への協力

（4）委託事業者に対する監査

（5）報告

（6）監査結果への対応

（7）情報セキュリティポリシー及び関係規程等の見直し等への活用

9.2 自己点検

（1）実施方法

（2）報告

（3）自己点検結果の活用

9.3 情報セキュリティポリシー及び関係規程等の見直し

本対策基準は、情報セキュリティ管理要綱を実行に移すための、地方独立行政法人大阪市民病院機構（以下、「法人」という。）における情報資産に関する情報セキュリティ対策の基準を定めたものである。

1. 組織体制

（1）最高情報セキュリティ責任者

① 法人に最高情報セキュリティ責任者を置き、理事長をもって充てる。

② 最高情報セキュリティ責任者は、法人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対策に関する最終決定権限と責任を有する。

③ 最高情報セキュリティ責任者は、本対策基準に定められた自らの担務を、統括情報セキュリティ責任者及び本対策基準に定める責任者に担わせることができる。

（2）統括情報セキュリティ責任者

① 法人に統括情報セキュリティ責任者を置き、法人運営本部医事企画部長をもって充てる。

② 統括情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐し、情報セキュリティに関する企画、実施及び運用に係る事務を統括する。

③ 統括情報セキュリティ責任者は、情報セキュリティ責任者、システム管理責任者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

④ 統括情報セキュリティ責任者は、法人の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

⑤ 統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、システム管理責任者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑥ 統括情報セキュリティ責任者は、緊急時には最高情報セキュリティ責任者に早急に報告を行うとともに、回復のための対策を講じなければならない。

⑦ 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告しなければならない。

（3）情報セキュリティ責任者

① 病院等に次のとおり情報セキュリティ責任者を置く。総合医療センターの情報セキュリティ責任者は病院長、十三市民病院の情報セキュリティ責任者は病院長、住之江診療所の情報セキュリティ責任者は所長をもって充てる。

② 情報セキュリティ責任者は、当該施設における情報セキュリティ対策及びネットワークの運用に関する権限と責任を有する。

③ 情報セキュリティ責任者は、当該施設において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、統括情報セキュリティ責任者及び最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（4）システム管理責任者

① 各情報システムにシステム管理責任者を置き、当該システムを所管する課長等をもって充てる。

② システム管理責任者は、所管するシステムにおける仕様、運用を定め、適切に管理する権限と責任を有する。

③ システム管理責任者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（5）システム管理担当者

システム管理責任者の指示等に従い、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をシステム管理担当者とする。

【責任体制図】

最高情報セキュリティ責任者	理事長	法人の全情報資産管理及び情報セキュリティ対策の最終決定権限及び責任
統括情報セキュリティ責任者	法人運営本部医事企画部長	法人の情報セキュリティの企画、実施及び運用事務統括
情報セキュリティ責任者 総合医療センター 十三市民病院 住之江診療所	 病院長 病院長 所長	当該施設における情報セキュリティ及びネットワークに関する権限及び責任
システム管理責任者	所管する課長等	所管する部門の情報セキュリティ対策に関する権限及び責任 所管するシステムの仕様、運用を定め、適切に管理する権限及び責任
システム管理担当者		情報システムの開発、設定の変更、運用、更新等の作業

2. 情報資産の分類と管理

（1）情報資産の分類

情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行う。

① 機密性による分類

分類	分類基準	取扱制限
機密性３	個人情報及び人事情報等、機密性を要する情報資産	・貸与された端末以外での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止
機密性２	公開を前提としていない情報資産	

		・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性１	機密性２又は機密性３の情報資産以外の情報資産	―

② 完全性による分類

分類	分類基準	取扱制限
完全性２	改ざん、誤びゅう又は破損により、第三者の権利が侵害される又は法人内部の事務の遂行に重大な支障を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２の情報資産以外の情報資産	―

③ 可用性による分類

分類	分類基準	取扱制限
可用性２	滅失、紛失又は当該情報資産が利用不可能であることにより、第三者の権利が侵害される又は法人内部の事務の遂行に重大な支障を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	―

(２) 情報資産の管理

① 管理責任

(ア) システム管理責任者は、その所管する情報資産について管理責任を有する。

(イ) システム管理責任者は、情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

② 情報資産の分類の表示

職員等は、必要に応じて情報資産の分類の表示、取扱制限の明示等適正な管理を行わなければならない。

③ 情報資産の作成

(ア) 職員等は、業務上必要のない情報資産を作成してはならない。

(イ) 情報資産を作成する者は、その作成時に（1）の分類に基づき、当該情報資産の分類と取扱制限を定めなければならない。

（ウ）情報資産を作成する者は、作成途上のものについても、紛失や流出等を防止しなければならない。また、作成途上で不要になった場合は、当該情報資産を消去しなければならない。

④　情報資産の入手

（ア）情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）入手した情報資産の分類が不明な場合は、システム管理責任者に判断を仰がなければならない。

⑤　情報資産の利用

（ア）情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ）情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なるものが複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥　情報資産の保管

（ア）システム管理責任者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）システム管理責任者は、機密性２以上、完全性２又は可用性２の内容を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦　メールの送信

電子メール等により機密性２以上のものを送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

⑧　情報資産の運搬

（ア）車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）機密性２以上の情報資産を運搬する者は、システム管理責任者に許可を得なければならない。

⑨　情報資産の提供・公表

（ア）機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）機密性２以上の情報資産を外部に提供する場合は、システム管理責任者及び個人情報保護責任者の許可を得なければならない。

（ウ）システム管理責任者は、公開する情報資産について、完全性を確保しなければならない。

⑩　情報資産の廃棄等

（ア）情報資産の廃棄やリース返却等を行う者は電子データを記録している電磁的記録媒体について、その機密性に応じ、復元できないように処置しなければならない。

（イ）情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

（ウ）情報資産の廃棄やリース返却等を行う者は、システム管理責任者の許可を得なければならない。

3. 情報システム全体の強靭性の向上

（1）病院情報システム

① 病院情報システム（以下「ＨＩＳ」という。）と他の領域との分離

ＨＩＳと他の領域を通信できないように分離しなければならない。ＨＩＳと外部との通信をする必要がある場合は、通信経路の限定や認証を行い、安全性を確保しなければならない。

② 情報資産のアクセス及び持ち出しにおける対策

（ア）情報資産のアクセス対策

情報システムの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）情報資産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への電子データの持ち出しができないように設定しなければならない。

（2）病院事業ネットワークシステム

① 病院事業ネットワークシステム（以下「庁内ＮＷ」という。）は、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。

② インターネット環境で受信したインターネットメールは、危険因子をファイルから除去するソフトを通して受信しなければならない。

③ 庁内ＮＷにおいては、可能な限り、通信パケットの監視、ふるまい検知等の不正通信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。

（3）医学情報収集用ネットワークシステム

① 医学情報収集用ネットワークシステム（以下「医学ＮＷ」という。）は、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。

② インターネット環境で受信したインターネットメールは、危険因子をファイルから除去するソフトを通して受信しなければならない。

③ 医学ＮＷにおいては、可能な限り、通信パケットの監視、ふるまい検知等の不正通信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。

4. 物理的セキュリティ

4.1 サーバ等の管理

（1）サーバ等の取付け

① サーバ等の機器は、火災、水害、ほこり、振動等の影響を可能な限り排除した場所に設置しなければならない。

② システムのサーバ等については、施錠された区域に設置しなければならない。

（2）機器の電源

① システム管理責任者は、情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正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なければならない。

② システム管理責任者は、情報セキュリティ責任者及び施設管理部門と連携し、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なければならない。

（3）通信ケーブル等の配線

① 情報セキュリティ責任者及びシステム管理責任者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

② 情報セキュリティ責任者及びシステム管理責任者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③ 情報セキュリティ責任者及びシステム管理責任者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④ 情報セキュリティ責任者及びシステム管理責任者は、自ら又はシステム管理担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

（4）機器の定期保守及び修理

① システム管理責任者は、サーバ等の機器の定期保守を実施しなければならない。

② システム管理責任者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、システム管理責任者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（5）法人の施設外への機器の設置

情報セキュリティ責任者及びシステム管理責任者は、法人の施設外にサーバ等の機器を設置する場合、最高情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（6）機器の廃棄等

システム管理責任者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての電子データを消去の上、復元不可能な状態にする措置を講じなければならない。

4.2 コンピュータ室の管理

（1）コンピュータ室の入退室管理等

① 情報セキュリティ責任者は、コンピュータ室への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

② 職員等及び委託事業者は、コンピュータ室に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③　情報セキュリティ責任者は、外部からの訪問者がコンピュータ室に入る場合には、必要に応じて立ち入り区域を制限した上で、コンピュータ室への入退室を許可された職員等を付き添わせるものとし、外見上職員等と区別できる措置を講じなければならない。

（2）機器等の搬入出

①　情報セキュリティ責任者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等に確認を行わせなければならない。

②　情報セキュリティ責任者は、コンピュータ室の機器等の搬入出について、職員等を立ち会わせなければならない。

4.3 ネットワーク及びネットワーク装置の管理

①　統括情報セキュリティ責任者及び情報セキュリティ責任者は、施設内のネットワーク及びネットワーク装置を、施設管理部門と連携し、適正に管理しなければならない。また、ネットワーク及びネットワーク装置に関連する文書を適正に保管しなければならない。

②　統括情報セキュリティ責任者及び情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③　統括情報セキュリティ責任者及び情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送信する電子データの暗号化を行わなければならない。

④　統括情報セキュリティ責任者及び情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に電子データが破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑤　統括情報セキュリティ責任者及び情報セキュリティ責任者は、可用性２の内容を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

4.4 職員等の利用するパソコンや電磁的記録媒体等の管理

①　システム管理責任者は、執務室等で利用するパソコン等について、盗難防止のための物理的措置を講じなければならない。電磁的記録媒体については、電子データが保存される必要がなくなった時点で速やかに記録した電子データを消去しなければならない。

②　システム管理責任者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

5. 人的セキュリティ

5.1 職員等の遵守事項

（1）職員等の遵守事項

①　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、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等がある場合は、速やかにシステム管理責任者に相談し、指示を仰がなければならない。

② 業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③ パソコンや電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

(ア) 最高情報セキュリティ責任者は、機密性２以上、可用性２、完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

(イ) 職員等は、法人のパソコンや電磁的記録媒体等の情報資産を外部に持ち出す場合には、システム管理責任者の許可を得なければならない。

(ウ) 職員等は、外部で情報処理業務を行う場合には、システム管理責任者の許可を得なければならない。

④ 貸与以外のパソコンや電磁的記録媒体等の業務利用

(ア) 職員等は、貸与以外のパソコンや電磁的記録媒体等を原則業務に利用してはならない。ただし、貸与以外の端末の業務利用の可否判断を情報セキュリティ責任者が行った後に、業務上必要な場合は、システム管理責任者の許可を得て利用することができる。

(イ) 職員等は、貸与以外のパソコンや電磁的記録媒体等を用いる場合には、システム管理責任者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑤ 持ち出し及び持ち込みの記録

システム管理責任者は、パソコン等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥ パソコン等におけるセキュリティ設定変更の禁止

職員等は、パソコン等のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ責任者の許可なく変更してはならない。

⑦ 机上のパソコン等の管理

職員等は、取扱う情報資産について、第三者に使用されること又はシステム管理責任者の許可なく閲覧されることがないように、離席時のパソコン等をロックしたり、電磁的記録媒体や文書等を容易に閲覧されない場所に保管する等、適正な措置を講じなければならない。

⑧ 退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た機密情報を漏らしてはならない。

(２) 情報資産を取扱う外部職員等への対応

① 情報セキュリティポリシー等の遵守

システム管理責任者は、業務委託、労働者派遣契約に基づき業務に従事する者、その他法人の情報資産を取扱う法人の役職員以外の者（以下、「外部職員等」という。）に対し、入職時に情報セキュリティポリシー等のうち、情報資産を取扱う外部職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

② 情報セキュリティポリシー等の遵守に対する同意

システム管理責任者は、情報資産を取扱う外部職員等の入職の際、必要に応じ、情報セキュリティポリシー等の遵守を求めるものとする。

③ インターネット接続及び電子メール使用等の制限

システム管理責任者は、情報資産を取扱う外部職員等にパソコン等による作業を行わせる場合、必要のないインターネット接続や電子メールの使用を制限させなければならない。

(3) 情報セキュリティポリシー等の掲示

システム管理責任者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

(4) システム委託事業者に対する説明

システム管理責任者は、ネットワーク及び情報システムの導入・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうちシステム委託事業者が守るべき内容の遵守について説明しなければならない。

5.2 研修・訓練

(1) 情報セキュリティに関する研修

最高情報セキュリティ責任者は、定期的に情報セキュリティに関する研修を実施しなければならない。

(2) 研修計画の策定及び実施

① 最高情報セキュリティ責任者は、役員を含めた全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

② 職員等が、毎年度最低1回は情報セキュリティ研修を受講できるよう研修計画を作成しなければならない。

③ 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

(3) 緊急時対応訓練

最高情報セキュリティ責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。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、効果的に実施できるようにしなければならない。

(4) 研修・訓練への参加

役員を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

5.3 情報セキュリティインシデントの報告

① 職員等は、情報セキュリティインシデントを認知した場合、速やかにシステム管理責任者に報告しなければならない。

② 報告を受けたシステム管理責任者は、速やかに情報セキュリティ責任者に報告しなければならない。

③ 情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、必要に応じて、統括情報セキュリティ責任者及び最高情報セキュリティ責任者に報告しなければならない。

5.4 ID 及びパスワード等の管理

（1）IC カード等の取扱い

① 職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。

（ア）認証に用いる IC カード等を、職員等の間で共有してはならない。

（イ）業務上必要のないときは、IC カード等をカードリーダ又はパソコン等のスロット等から抜いておかなければならない。

（ウ）IC カード等を紛失した場合には、速やかにシステム管理責任者に通報し、指示に従わなければならない。

② 情報セキュリティ責任者及びシステム管理責任者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

③ 情報セキュリティ責任者及びシステム管理責任者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（2）ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

① 自己が利用している ID は、他人に利用させてはならない。

② 共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

（3）パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① パスワードは、他者に知られないように管理しなければならない。

② 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てはならない。

③ 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。

④ パスワードが流出したおそれがある場合には、情報セキュリティ責任者及びシステム管理責任者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤ 複数の情報システムを扱う職員等は、同一のパスワードを複数のシステムで使いまわしてはならない。

⑥ 仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

⑦ サーバ、ネットワーク機器及びパソコン等にパスワードを記憶させてはならない。

⑧ 職員等の間でパスワードを共有してはならない（ただし、共用 ID に対するパスワードは除く）。

6. 技術的セキュリティ

6.1 コンピュータ及びネットワークの管理

（1）ファイルサーバの設定等

① 情報セキュリティ責任者は、職員等が使用できるファイルサーバの容量を設定しなければならない。

② 情報セキュリティ責任者は、ファイルサーバを部署等の単位で構成し、職員等が他部署等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

（2）バックアップの実施

情報セキュリティ責任者及びシステム管理責任者は、情報システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策の有無にかかわらず、必要に応じて定期的にバックアップを実施しなければならない。

（3）システム管理記録及び作業の確認

① 情報セキュリティ責任者及びシステム管理責任者は、所管する情報システムで実施した作業の作業記録を作成しなければならない。

② 情報セキュリティ責任者及びシステム管理責任者は、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

（4）情報システム仕様書等の管理

情報セキュリティ責任者及びシステム管理責任者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

（5）ログの取得等

① 情報セキュリティ責任者及びシステム管理責任者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② 情報セキュリティ責任者及びシステム管理責任者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

（6）障害記録

情報セキュリティ責任者及びシステム管理責任者はシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

（7）ネットワークの接続制御、経路制御等

① 統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

② 統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

（8）外部ネットワークとの接続制限等

① システム管理責任者は所管するネットワークを外部ネットワークと接続しようとする場合には、統括情報セキュリティ責任者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。

② システム管理責任者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③ システム管理責任者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当

該外部ネットワークの管理責任者による責任分界点を契約上明らかにしなければならない。

④ 統括情報セキュリティ責任者及びシステム管理責任者は、Web サーバ等をインターネットに公開する場合、法人のネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤ システム管理責任者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（9）複合機のセキュリティ管理

① 情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

② システム管理責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③ システム管理責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての電子データを抹消する又は再利用できないようにする対策を講じなければならない。

（１０） IoT 機器を含む特定用途機器のセキュリティ管理

システム管理責任者は、特定用途機器について、取扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（１１） 無線 LAN 及びネットワークの盗聴対策

① 統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

② 統括情報セキュリティ責任者は、機密性の高い内容を取扱うネットワークについて、盗聴等を防ぐため、電子データの暗号化等の措置を講じなければならない。

（１２） 電子メールのセキュリティ管理

① 統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

② 統括情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

③ 統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④ 統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤ 統括情報セキュリティ責任者は、システム導入や運用、保守等のため施設内に常駐している委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。

（１３）　電子メールの利用制限

①　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

②　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

③　職員等は、機密性の高い電子メールを誤送信した場合、システム管理責任者に報告しなければならない。

（１４）　電子署名・暗号化

職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

（１５）　無許可ソフトウェアの導入等の禁止

①　職員等は、パソコン等に無断でソフトウェアを導入してはならない。

②　職員等は、業務上の必要がある場合は、情報セキュリティ責任者及びシステム管理責任者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、システム管理責任者は、ソフトウェアのライセンスを管理しなければならない。

③　職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１６）　機器構成の変更の制限

①　職員等は、パソコン等に対し機器の改造及び増設・交換を行ってはならない。

②　職員等は、業務上、パソコン等に対し機器の改造及び増設・交換を行う必要がある場合には、情報セキュリティ責任者及びシステム管理責任者の許可を得なければならない。

（１７）　業務外ネットワークへの接続の禁止

①　職員等は、貸与されたパソコン等を、有線・無線を問わず、統括情報セキュリティ責任者によって定められたネットワークと異なるネットワークに接続してはならない。

②　統括情報セキュリティ責任者は、貸与した端末について、搭載された OS のポリシー設定等により、異なるネットワークに接続できないよう技術的に制限することが望ましい。

（１８）　業務以外の目的での Web 閲覧の禁止

①　職員等は、業務以外の目的で Web を閲覧してはならない。

②　情報セキュリティ責任者は、職員等の Web 利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、システム管理責任者に通知し適正な措置を求めなければならない。

（１９）　Web 会議サービスの利用時の対策

①　情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。

②　職員等は、利用手順に従い、Web 会議の参加者や取扱う内容に応じた情報セキュリティ対策を実施すること。

③　職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

④　職員等は、外部から Web 会議に招待される場合は、機密性２以上の内容を含んだ資料の共有や保存をさせない等、情報漏洩に注意すること。

（２０）　ソーシャルメディアサービスの利用

①　情報セキュリティ責任者は、法人が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を厳守させなければならない。

（ア）アカウントによる情報発信が、実際の法人のものであることを明らかにするために、法人の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

（イ）パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

②　機密性２以上の内容はソーシャルメディアサービスで発信してはならない。

③　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なければならない。

④　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

⑤　可用性２の情報発信にソーシャルメディアサービスを用いる場合は、法人の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

6.2 アクセス制御

（１）アクセス制御等

①　アクセス制御

情報セキュリティ責任者又はシステム管理責任者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

②　利用者 ID の取扱い

（ア）情報セキュリティ責任者及びシステム管理責任者は、利用者の登録、変更、停止等の情報管理、職員等の異動、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

（イ）職員等は、業務上必要がなくなった場合は、利用者 ID を停止するよう、システム管理責任者に通知しなければならない。

（ウ）情報セキュリティ責任者及びシステム管理責任者は、利用されていない ID が放置されないよう総務課と連携し、点検しなければならない。

③　特権を付与された ID の管理等

（ア）情報セキュリティ責任者及びシステム管理責任者は、特権を付与されたアカウントを利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう管理しなければならない。

（イ）情報セキュリティ責任者及びシステム管理責任者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

（ウ）情報セキュリティ責任者及びシステム管理責任者は、特権を付与された ID 及びパスワードについて、定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

(エ) 情報セキュリティ責任者及びシステム管理責任者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

(2) 職員等による外部からのアクセス等の制限

① 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、情報セキュリティ責任者及びシステムを管理するシステム管理責任者の許可を得なければならない。

② 情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③ 情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④ 情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤ 情報セキュリティ責任者及びシステム管理責任者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥ 職員等は、外部から持ち込んだ又は外部から持ち帰ったモバイル端末を法人のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、システム管理責任者及び情報セキュリティ責任者の承認を得たうえで、接続しなければならない。

⑦ 情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。

ただし、止むを得ず接続を許可する場合は、情報セキュリティ確保のために必要な措置を講じなければならない。

(3) ログイン時の表示等

システム管理責任者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

(4) 認証情報の管理

① 情報セキュリティ責任者又はシステム管理責任者は、職員等の認証情報を厳重に管理し、認証情報ファイルを不正利用から保護しなければならない。

② 情報セキュリティ責任者又はシステム管理責任者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

③ 情報セキュリティ責任者又はシステム管理責任者は、認証情報の不正利用を防止するための措置を講じなければならない。

(5) 特権による接続時間の制限

情報セキュリティ責任者又はシステム管理責任者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

6.3 システム開発・導入・保守等

(1) 情報システムの調達

① 情報セキュリティ責任者及びシステム管理責任者システム管理責任者は、情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② 情報セキュリティ責任者及びシステム管理責任者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(2) 情報システムの開発

① システム開発における責任者及び作業者の特定

システム管理責任者は、システム開発の責任者及び作業者を特定しなければならない。

また、システム開発のための規則を確立しなければならない。

② システム開発における責任者、作業者の ID の管理

(ア) システム管理責任者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

(イ) システム管理責任者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③ システム開発に用いるハードウェア及びソフトウェアの管理

(ア) システム管理責任者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(イ) システム管理責任者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

(3) 情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

(ア) システム管理責任者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

(イ) 情報セキュリティ責任者及びシステム管理責任者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(ウ) システム管理責任者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(エ) システム管理責任者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

② テスト

(ア) システム管理責任者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

(イ) システム管理責任者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(ウ) システム管理責任者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

(エ) システム管理責任者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

(4) システム開発・保守に関連する資料等の整備・保管

① システム管理責任者は、システム導入・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

② システム管理責任者は、テスト結果を一定期間保管しなければならない。

③ システム管理責任者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

(5) 情報システムにおける入出力データの正確性の確保

① システム管理責任者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

② システム管理責任者は、故意又は過失により電子データが改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③ システム管理責任者は、情報システムから出力されるデータについて、処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6) 情報システムの変更管理

システム管理責任者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(7) 導入・保守用のソフトウェアの更新等

システム管理責任者は、導入・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(8) システム更新又は統合時の検証等

システム管理責任者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

6.4 不正プログラム対策

(1) 情報セキュリティ責任者の措置事項

情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

① 外部ネットワークから受信したファイルは、インターネットのゲートウェイ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、不正プログラムのシステムへの侵入を防止しなければならない。

② 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③ 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、必要に応じ職員等に対して注意喚起しなければならない。

④　所掌するサーバやパソコン等の情報資産に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
⑤　不正プログラム対策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たなければならない。
⑥　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
⑦　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

（2）システム管理責任者の措置事項

システム管理責任者は、不正プログラム対策に関し、次の事項を措置しなければならない。

①　システム管理責任者は、その所掌するサーバやパソコン等の情報資産に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。
②　不正プログラム対策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たなければならない。
③　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
④　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、法人が許可している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。
⑤　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、システム管理責任者が許可した職員を除く職員等に当該権限を付与してはならない。

（3）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①　パソコン等において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
②　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
③　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
④　パソコン等に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。
⑤　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネットメール又はインターネット経由で入手したファイルを HIS に取り込む場合は無害化しなければならない。
⑥　情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑦　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

（4）専門家の支援体制

情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

6.5.不正アクセス対策

（1）情報セキュリティ責任者の措置事項

情報セキュリティ責任者及びは、不正アクセス対策として、以下の事項を措置しなければならない。

①　使用されていないポートを閉鎖しなければならない。

②　不要なサービスについて、機能を削除又は停止しなければならない。

③　不正アクセスによる Web ページの改ざんを防止するために、データの書換えを検出し、情報セキュリティ責任者及びシステム管理責任者へ通報するよう、設定しなければならない。

④　情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2）攻撃への対処

最高情報セキュリティ責任者及び情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、厚生労働省、大阪市等と連絡を密にして情報収集に努めなければならない。

（3）記録の保存

最高情報セキュリティ責任者及び情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（4）内部からの攻撃

情報セキュリティ責任者及びシステム管理責任者は、職員等及び委託事業者が使用しているパソコン等からの法人のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）職員等による不正アクセス

情報セキュリティ責任者及びシステム管理責任者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の責任者に通知し、適正な処置を求めなければならない。

（6）サービス不能攻撃

情報セキュリティ責任者及びシステム管理責任者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（7）標的型攻撃

情報セキュリティ責任者及びシステム管理責任者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6.6 セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

情報セキュリティ責任者及びシステム管理責任者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（2）不正プログラム等のセキュリティ情報の収集・周知

情報セキュリティ責任者及びシステム管理責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（3）情報セキュリティに関する情報収集及び共有

情報セキュリティ責任者及びシステム管理責任者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

7. 運用

7.1 情報システムの監視

① 情報セキュリティ責任者及びシステム管理責任者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

② 情報セキュリティ責任者及びシステム管理責任者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③ 情報セキュリティ責任者及びシステム管理責任者は、外部と常時接続するシステムを監視しなければならない。

7.2 情報セキュリティポリシーの遵守状況の確認

（1）遵守状況の確認及び対処

① 情報セキュリティ責任者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告しなければならない。

② 最高情報セキュリティ責任者は、発生した問題について、適正かつ速やかに対処しなければならない。

③　統括情報セキュリティ責任者及び情報セキュリティ責任者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（2）パソコンや電磁的記録媒体等の利用状況調査

最高情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコンや電磁的記録媒体等のログ、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）職員等の報告義務

①　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報セキュリティ責任者及びシステム管理責任者に報告を行わなければならない。

②　当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると最高情報セキュリティ責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

7.3 侵害時の対応等

（1）システム BCP の策定

最高情報セキュリティ責任者は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

（2）システム BCP に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①　関係者の連絡先

②　発生した事案に係る報告すべき事項

③　発生した事案への対応措置

④　再発防止措置の策定

（3）事業継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途事業継続計画を策定し、情報セキュリティ責任者は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（4）システム BCP の見直し

情報セキュリティ責任者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

7.4 例外措置

（1）例外措置の許可

情報セキュリティ責任者及びシステム管理責任者は、情報セキュリティ関係規定を遵守することが困難な状況で、法人業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する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、最高情報セキュリティ責任者の許可を得て、例外措置を講じることができる。

（2）緊急時の例外措置

情報セキュリティ責任者及びシステム管理責任者は、法人業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、事後速やかに最高情報セキュリティ責任者に報告しなければならない。

7.5 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、関係法令を遵守し、これに従わなければならない。

8. 業務委託と外部サービスの利用

8.1 業務委託

（1）委託事業者の選定基準

① システム管理責任者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

② システム管理責任者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

（2）契約項目

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・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
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報資産の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・提供された情報資産の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た機密情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・法人よる監査、検査
・法人による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（3）確認・措置等

システム管理責任者は、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定期的に確認し、必要に応じ、(2)の契約に基づき措置を実施しなければならない。また、その内容を情報セキュリティ責任者に報告しなければならない。

8.2 外部サービスの利用 （機密性２以上の内容を取り扱う場合）

クラウドサービスなどの情報システムの一部又は全部の機能を提供するサービス（以下「外部サービス」という。）の利用については、法人の定める利用基準に基づいて行うこととする。

9. 評価・見直し

9.1 監査

（1）実施方法

最高情報セキュリティ責任者は、システム監査責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的に監査を行わせなければならない

（2）監査を行う者の要件

① システム監査責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

② 監査を行う者は、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でなければならない。

（3）監査実施計画の立案及び実施への協力

① システム監査責任者は、監査を行うに当たって、監査実施計画を立案しなければならない。

② 被監査部門は、監査の実施に協力しなければならない。

（4）委託事業者に対する監査

事業者に業務委託を行っている場合、システム監査責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（5）報告

システム監査責任者は、監査結果を取りまとめ、最高情報セキュリティ責任者に報告する。

（6）監査結果への対応

最高情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管するシステム管理責任者に対し、当該事項への対処を指示しなければならない。また、その他のシステム管理責任者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、法人内で横断的に改善が必要な事項については、情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

（7）情報セキュリティポリシー及び関係規程等の見直し等への活用

最高情報セキュリティ責任者は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

9.2 自己点検

（1）実施方法

システム管理責任者は、所管するネットワーク及び情報システムについて、定期的に自己点検を実施しなければならない。

（2）報告

システム管理責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ責任者に報告しなければならない。

（3）自己点検結果の活用

① 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

② 最高情報セキュリティ責任者は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

9.3 情報セキュリティポリシー及び関係規程等の見直し

最高情報セキュリティ責任者は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

附　則

この対策基準は平成 26 年 10 月 1 日より施行する。

この改定対策基準は令和 8 年 3 月 17 日より施行する。