別紙９

新図書館等複合施設
情報セキュリティポリシー（案）

目　次

第1章　総則

第１条（趣旨）

新図書館等複合施設情報セキュリティポリシー（以下、「本ポリシー」という。）は、高知県および高知市が共同設置する新図書館等複合施設（以下、「複合施設」という。）の情報セキュリティを確保し、情報資産を適正に取り扱うため、必要な事項を定めるものとする。

第２条（定義）

この規則において、次の各号に掲げる用語の定義は、それぞれ当該各号に定めるところによる。

(1) 組織　新図書館等複合施設に入居する4つの組織（「高知県立図書館」「高知市立市民図書館」「高知市立高知点字図書館」「高知市立こども科学館（仮称）」）
(2) 情報資産　組織の業務において使用するコンピュータ及び記録媒体に記録されたデータ並びに記録されたデータが処理されて出力されたもの
(3) 情報システム　コンピュータ、ネットワーク及びそれらを制御するソフトウェア、並びに記録媒体で構成された情報処理を行う仕組み
(4) 資源　情報システムを構成するハードウェア、ソフトウェア、ネットワーク等
(5) 電子機器　情報を処理する機器（コンピュータ、サーバ、パソコンだけでなく、カードリーダー等）
(6) 脅威　情報資産に対して、障害や影響を与える原因となるもの
(7) 情報セキュリティ　複合施設が管理する情報資産を脅威から保護し、機密性、完全性、可用性を確保すること
(8) 情報統括責任者　複合施設の情報資産について、管理を統括する者
(9) 職員　高知県立図書館、高知市立市民図書館、高知市立高知点字図書館、高知市立こども科学館（仮称）のいずれかに所属する者
(10) 管理責任者　複合施設の各組織の長の職にある者
(11) 担当者　各組織において管理責任者を補助し、各組織における情報セキュリティ対策を円滑に行う者で、各組織の中から各管理責任者が指名する者
(12) ネットワーク管理者　複合施設内の各ネットワークを所管する組織の長の職にある者
(13) リスクアセスメント　守るべき対象である情報資産で発生する可能性のある脅威と、脅威の発生確率や発生した場合の影響度等を評価する方法
(14) 可用性　権限のある者に対し、いつでも情報資産の利用を可能とすること
(15) 完全性　情報資産の改ざん、破壊による被害を防止すること
(16) 悪意のあるコード　情報システムが提供するサービスを妨害するプログラム
(17) 特権　管理者権限等の特別な権限

第３条（適用範囲）

複合施設が管理する情報資産（委託事業者等に管理を委託しているものを含む。）について適用する。ただし、高知県セキュリティポリシー及び高知県教育情報ネットワークシステム管理要綱並びに高知市情報セキュリティ規程の適用範囲となる情報資産については、それぞれの規定を適用する。

第2章　運用管理体制

第４条（運用管理体制）

情報セキュリティ対策を実施するため、次の事項を定める。

1 情報統括責任者

(1) 情報セキュリティ対策を統括する責任者として、情報統括責任者を置き、〇〇をもって充てる。
(2) 情報セキュリティ対策の目的及び情報セキュリティ方針を承認し、定期的に見直す。
(3) 情報セキュリティ方針の実装について有効性を見直す。
(4) 情報セキュリティに必要な資源を提供する。

2 情報セキュリティ委員会

(1) 情報セキュリティ対策を総合的に推進するため、情報セキュリティ委員会を置く。情報セキュリティ委員会は、各組織の代表者で構成し、組織間の問題について調整する。
(2) 情報セキュリティ委員長は情報統括責任者をもって充てる。
(3) 情報セキュリティ委員長は、必要に応じて委員会に専門的な知識を有する者又は委員以外の職員の参画を求めることができる。

3 情報処理設備の許可プロセス

情報処理設備の新規導入の際には、情報セキュリティ委員会による許可を必要とする。

4 関係当局との連絡

(1) 各管理責任者及び情報セキュリティ委員会は、それぞれが関係する上部組織や外部の機関、事業者等との関係を維持する。
(2) 管理責任者は、上部組織や外部機関、事業者等から情報セキュリティに関する情報を入手した場合は、各組織内に周知する。

5 職員の責務

(1) 職員は、法令及び本ポリシーを守り、情報資産の適切な管理に努めなければならない。
(2) 職員は、情報資産を取り扱う事務の全部又は一部を事業者に委託する場合は、法令及び本ポリシーを守らせるために必要な措置を講ずるものとする。

第3章 情報資産の管理

第５条（情報資産の分類）

情報資産の適切なレベルでの保護を確実にするため、次の事項を定める。

(1) 1 分類の指針管理責任者は、組織で管理している情報資産を、組織に対しての価値、法的要求事項、取扱いに慎重を要する度合い及び重要性の観点から分類する。
(2) 情報資産の分類基準は、別途設ける。
(3) 情報資産の分類基準は、情報セキュリティ委員会が承認し、維持する。
(4) 職員は、分類基準に従って情報資産を適切に分類しなければならない。

2 情報資産の取扱い

(1) 管理責任者は、複合施設が採用した分類体系に従って情報資産の取扱いの手順を策定し、実施する。
(2) 職員は、情報資産の取扱いの手順に沿って、情報資産を取り扱わなければならない。

第 6 条（情報資産に対する責任）

組織の情報資産を適切に保護し、維持するため、次の事項を定める。

1 情報資産に対する責任の割当て

(1) 管理責任者は、組織のすべての情報資産に対する責任を明確に定めること。

(2) 管理責任者は、組織のすべての重要な情報資産について、担当者を定められなければならない。

(3) 管理責任者は各組織における情報資産の管理責任を有する。

(4) 管理責任者と担当者は原則、兼務を認めない。

2 情報資産目録

(1) 管理責任者は、すべての情報資産を明確に分類し、また、重要な情報資産を情報資産管理表に記載し、維持する。

(2) 管理責任者は、情報資産に追加および変更がある場合は遅滞なく情報資産管理表を更新しなければならない。また、定期的に見直しを行わなければならない。

3 情報資産利用の許容範囲

管理責任者は、情報資産利用の許容範囲を情報資産管理表に記載し、維持する。

第4章 人的な情報セキュリティ対策

第 7 条（職員）

職員によるコンピュータの誤操作や不正行為等の脅威から情報資産を保護するため、次の事項を定める。

1 職員の管理責任

(1) 職員は、与えられた利用者ＩＤ、パスワード及び認証に用いるカード等を厳重に管理し、他の者による不正アクセスや不正利用を未然に防止しなければならない。

(2) 職員は、不適切な情報の発信、不正アクセス等、自らが加害者になる行為を行ってはならない。

(3) 職員は、業務以外の目的でインターネットを利用してはならない。

(4) 職員は、コンピュータを複合施設外に持ち出してはならない。
ただし、業務上必要であって、かつ、情報セキュリティの確保上支障がないと管理責任者が認めた場合はこの限りでない。

(5) 職員は、自己が所有するコンピュータ及び記録媒体を複合施設内の室（組織がその分掌事務を行うために使用する部屋等の区域、以下「室」という。）に持ち込み、かつ、使用してはならない。
ただし、業務上必要であって、かつ、情報セキュリティの確保上支障がないと管理責任者が認めた場合はこの限りでない。

(6) 職員は、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速やかに返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

(7) その他、組織別の職員の管理責任に関する規定は、別途定める。

2 職員への教育

(1) 管理責任者は、本ポリシーについての啓発・教育資料を用意し、職員が本ポリシーを遵守できるように、教育・訓練を実施しなければならない。

(2) 本ポリシー及び関連する手順等の教育・訓練は定期的に実施しなければならない。

第 8 条（委託事業者）

1 委託事業者への周知

管理責任者は、委託事業者に対して、本ポリシーに規定する事項を周知させる。

2 契約書への記載事項

管理責任者は、委託事業者が守るべき内容について、次に掲げるもののうち必要な事項を契約書に明記する。

(1) 再委託の禁止及び制限に関する事項
(2) 委託事業者の守秘義務に関する事項
(3) 情報及び関連資料の保管、返還及び廃棄に関する事項
(4) 責任者、従業者、作業範囲、作業場所の指定に関する事項
(5) 情報及び関連資料の目的外の使用、複製及び複写の禁止に関する事項
(6) 情報セキュリティに関する事案が発生した時の報告に関する事項
(7) 知的財産権の保護及び著作権の帰属に関する事項
(8) 業務記録等の定期報告に関する事項
(9) 委託事業者における情報資産の保護に関する管理体制や情報セキュリティ対策の実施状況等の調査に関する事項
(10)遵守されなかった場合の規定(損害賠償等)
(11)その他情報セキュリティを確保するために必要な事項

3 個人情報の取扱い

個人情報に関する情報資産を取り扱う事務については、各組織で別途定める。

第 9 条（職員及び委託事業者以外の者への対応）

職員は、職員及び委託事業者以外の者が情報資産を利用する場合は、その取扱いに関して適切な指導を行う。

第5章　物理的な情報セキュリティ対策

第 10 条（セキュリティを保つべき領域）

複合施設及び情報資産に対する許可されていない物理的アクセス、損傷及び妨害を阻止するため、次の事項を定める。

1 物理的セキュリティ境界

(1) 情報システムを構成する機器等（以下、「機器等」という。）のある領域（以下、「セキュリティ領域」という。）を保護するために、壁、カード制御等電子機器による入口、有人の受付等の複数の物理的セキュリティ境界を設定する。
(2) 物理的セキュリティ境界は、明確に定義する。
(3) セキュリティ領域は、重要度と用途に応じた設置条件により適切に保護する。
(4) 重要なセキュリティ領域は、物理的、環境的に保護する。

2 物理的入退管理策

(1) 重要なセキュリティ領域は、物理的な入退室管理により制御する。
(2) 重要なセキュリティ領域への入退室は、組織の長の許可を得た必要最小限の対象者に限定する。

(3) 入退室は、期間を限定して許可する。
(4) 管理責任者は、重要なセキュリティ領域への入退室の日付・時間を個人単位で記録し、期間を定めて保管する。

3 室及び施設のセキュリティ
(1) 管理責任者は、自らが管理する室及び施設に設置する機器等に対して、盗難防止のために必要な措置を講じる。
(2) 管理責任者は、重要なセキュリティ領域に、情報資産を保護する措置を講じなければならない。

4 自然災害及び人的災害からの保護
　火災、洪水、地震等の自然災害や、爆発、暴力行為等の人的災害に対する物理的セキュリティ対策を設計し、適用する。
(1) 自然災害及び人的災害に対する物理的セキュリティ対策については、別途定める。ただし、他の対策等の適用により保護が可能であれば、他の対策等により保護する。
(2) 警報装置の設置については、リスクアセスメントに基づき、情報セキュリティ委員会が決定する。

5 セキュリティ領域での作業
(1) セキュリティ領域での作業規定は、別途定める。
(2) セキュリティ領域では、作業規定に従って作業を行わなければならない。
(3) 管理責任者は、所管するセキュリティ領域において、作業規定に従い作業が行われていることを確認しなければならない。

第 11 条（機器等の管理）

情報資産の損失、損傷、盗難若しくは劣化、又は複合施設の活動に対する妨害を防止するため、次の事項を定める。

1 機器等の設置及び保護
(1) 管理責任者は、重要度、用途等に応じて、機器等の設置条件を定め、設置する。
(2) 機器等は、不必要なアクセスが最小限に抑えられる場所に設置する。
(3) 管理責任者は、機器等周辺の環境の状態が、情報処理設備の運用に悪影響を及ぼさないことを確認する。
(4) 機器等に関する機密度の高いドキュメントや媒体についても保護の対象とする。

2 ケーブル配線の保護
(1) 管理責任者は、通信傍受、通信ケーブルの損傷等を防止するため、必要な措置を講ずる。
(2) 管理責任者は、電源ケーブルによる通信ケーブルへの干渉を防止するための措置を講ずる。
(3) 管理責任者は、情報サービスに使用する電源ケーブルを損傷から保護する措置を講ずる。

3 機器等の保守
　可用性及び完全性を継続的に維持するために、適正に機器等を保守する。
(1) 管理責任者は、機器等の製造業者から提供される取扱方法に従い、機器等の保守点検を行う。
(2) 機器等の保守点検を保守業者に委託する場合は、保守契約を締結し、管理責任者が適切に管理する。

(3) 保守のために機器等をセキュリティ領域の外部に搬出する場合は、情報資産を適切に保護する措置を講ずる。

4 複合施設の敷地外にある機器等のセキュリティ

複合施設の敷地外にある機器等に対しては、敷地内での作業とは異なるリスクを考慮に入れて、情報セキュリティ対策を適用する。

(1) 管理責任者の許可を得ずに、機器等を複合施設の敷地外で使用してはならない。
(2) 機器等を複合施設の敷地外で使用する場合、セキュリティを保護するための適切な措置を講ずる。
(3) 管理責任者は、複合施設の敷地外に設置している機器等を、定期的に点検しなければならない。

5 機器等の安全な処分又は再利用

(1) 管理責任者は、記憶媒体を内蔵した機器等を処分する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又は問題が起きないように上書きしていることを確認する。
(2) 管理責任者は、機器等を廃棄する場合、取扱いに慎重を要する情報やライセンス供与されたソフトウェアの読み出しができないように処理をしなければならない。
(3) 管理責任者は、借用していた電子機器等を返却する場合、取扱いに慎重を要する情報の読み出しができないように処理をしなければならない。

6 機器等の移動

機器等又は情報資産ソフトウェアは、管理責任者の許可なしに複合施設の敷地外に持ち出さないこと。

(1) 複合施設の特定された領域に使用が限定されている機器等や情報資産、ソフトウェア等を、管理責任者の許可を得ずに移動又は持ち出しをしてはならない。
(2) 管理責任者は、機器等の所在を定期的に点検しなければならない。

第6章 通信及び運用管理

第 12 条（運用の手順及び責任）

情報システム及び情報処理設備を適正に管理するため、次の事項を定める。

1 操作手順書

(1) 管理責任者は、所管する情報システムごとに操作手順書を作成し、維持しなければならない。また、その手順書は、必要とするすべての利用者が利用できるものとする。
(2) 操作手順書の決定又は変更の際は、情報セキュリティ委員会の承認を得なければならない。

2 変更管理

(1) 情報システムや情報処理設備の運用に関する変更を行う場合は、情報セキュリティ委員会の承認を得なければならない。
(2) 管理責任者は、変更作業の手順書を作成し、情報セキュリティ委員会の承認を得なければならない。
(3) 変更作業は手順書に従って実施し、作業内容を記録しなければならない。

第 13 条（情報システムの計画作成及び受入れ）

情報システムの故障のリスクを最小限に抑えるため、次の事項を定める。

1 容量・能力の管理

管理責任者は、システム資源の使用状況及び仕様傾向を把握し、システム資源の利用を調整するとともに、将来必要となる容量・能力を予測する。

2 システムの受入れ

管理責任者は、新しいシステムを受け入れるに当たり、開発中及び受入れ前に適切なシステム試験を実施し、要求事項が満たされていることを確認する。

第 14 条（悪意のあるコードからの保護）

悪意のあるコードからソフトウェア及び情報を保護するために、次の事項を定める。また、利用者向けの手順を明文化し、周知する。

(1) 管理責任者は、電子メールを扱うコンピュータにウィルス検出対策を実施する。
(2) 管理責任者は、不正ソフトウェアの購入防止及びダウンロード防止の措置を講ずる。
(3) 管理責任者は、サーバ、パソコンに関する不正ソフトウェア利用の防止及び検出措置を講ずる。
(4) 管理責任者は、フリーソフトウェアの安全性について、確認及び使用を制限する措置を講ずる。
(5) 管理責任者は、不正ソフトウェア対策として利用者が守るべき事項を明確にする。

第 15 条（バックアップ）

(1) 管理責任者は、重要な情報について、定期的にバックアップを取得し、安全に保管する。
(2) バックアップは災害や盗難等から防止するための手段を講じた場所で保管する。
(3) 管理責任者は、長期にわたり保管されるバックアップについて、緊急の場合に確実に使用できるように、定期的に有効性を検査する。

第 16 条（ネットワークセキュリティ管理）

ネットワークを脅威から保護するために、また、処理中の情報を含め、ネットワークを用いた業務用システム及び業務用ソフトウェアのセキュリティを維持するため、次の事項を定める。

(1) ネットワーク管理者は、適切にネットワークの維持管理を行い、セキュリティの保護に努める。
(2) 職員は、複合施設のネットワークに関する重要な情報を適切に保護しなければならない。

第 17 条（媒体の取扱い）

情報資産の改ざん、除去及び破壊、許可されていない情報資産の開示、並びに業務活動の中断を防止するため、次の事項を定める。

1 取り外し可能な媒体の管理

(1) 職員は、機密情報の記録された取り外し可能な媒体又は印刷物を適切に管理し、保管しなければならない。
(2) 職員は、重要な情報の記録された媒体を持ち出す場合は、管理責任者の許可を得なければならない。

2 媒体の処分

媒体が不要になった場合、管理責任者は、安全かつ確実な方法で媒体を処分する。

3 媒体の取扱い

許可されていない情報資産の開示又は情報資産の誤用を防止するために、職員は、記録された情報の重要度に応じた媒体の取扱いと保管を行う。

第 18 条（情報システム文書のセキュリティ）

(1) 管理責任者は、重要な情報システム文書のアクセス範囲、保管の手順を定め、情報システム文書を保護しなければならない。
(2) 情報システム文書のアクセス権限の対象者は必要最小限としなければならない。

第 19 条（情報の交換）

複合施設内外で交換した、情報及びソフトウェアのセキュリティを維持するため、次の事項を定める。

1 情報交換の方針及び手順
(1) 管理責任者は、あらゆる形式の通信設備を利用して交換される情報及びソフトウェアを保護するための交換方針、手順及び管理策を備えること。
(2) 管理責任者は、取扱いに慎重を要する情報をファクシミリ又は電話で送受信又は通話を行う場合の手順を定め、徹底する。
(3) ファクシミリ及び電話を使用して情報及びソフトウェアを交換しようとする者は、機密を保護するために、別途定めた注意事項に従わなければならない。

2 情報交換に関する合意
(1) 取扱いに慎重を要する情報及びソフトウェアの交換については、その取扱い方法について外部組織等と合意の元に取り扱う。
(2) 取扱い方法については、情報及びソフトウェアの重要度を考慮しなければならない。

3 配送中の媒体の保護

情報を格納した媒体は、複合施設の敷地外での配送の途中における、管理責任者に許可されていないアクセス、不正使用又は破損から保護する。
(1) 配送中の媒体は、その種類に応じ物理的な損傷や開封から保護しなければならない。
(2) 具体的な配送方法は配送相手先との個別の取り決めによる。

4 電子メール
(1) 管理責任者は、電子メールに含まれる情報を適切に保護するため、電子メールの利用に関する指針を定め、教育等により利用者全員に徹底する。
(2) 管理責任者は、電子メールによる情報セキュリティ侵害等の形跡や証跡を発見するための措置を講じなければならない。

5 情報システム

管理責任者は、情報システムの相互接続と関連がある情報を保護しなければならない。

第 20 条（監視）

許可されていない情報処理活動を検知するため、次の事項を定める。

1 監査ログ取得

管理責任者は、利用者の活動、例外処理、情報セキュリティインシデントなど、セキュリティに関連して取得する監査ログの項目を定め、取得する。また、将来の調査及びアクセス制御の監視を補うために、一定期間安全に保管しなければならない。

２ システム使用状況の監視

管理責任者は、情報システム及び情報処理装置の監視対象及び監視方法を定め、監視手順に従って監視を行う。

３ ログ情報の保護

管理責任者は、ログ情報の、改ざん及び許可されていないアクセスからログ情報を保護する。

４ 担当者の作業記録

(1) 情報システムの作業を行う場合、担当者は、作業記録を記入しなければならない。
(2) 作業記録には、作業の経過のほか、異常があった場合はその内容を明確に示さなければならない。
(3) 管理責任者は、作業の種類ごとに作業記録の保管期間を定め、適切に保管する。

５ 障害のログ取得

障害のログを取得し、分析し、また、障害に対する適切な処置を講じること。

(1) 職員は、障害が発生した場合は、別途作成する連絡網に従って直ちに報告し、適切な復旧措置をとる。
(2) 管理責任者は、障害の規模に応じて、責任者を定め、復旧の指揮、復旧の確認を行う。
(3) 管理責任者は、障害の原因及び復旧措置を記録し、必要に応じて情報セキュリティ委員会に報告する。

６ 時計の同期

(1) 管理責任者は、同期の基準とするコンピュータを特定し、時計を同期させることとする。
(2) 時計の同期は、その方法と手順を定めて行うものとする。

第7章　アクセス制御

第 21 条（アクセス制御に対する業務上の要求事項）

情報へのアクセスを制御するため、次の事項を定める。

(1) 管理責任者は、アクセス制御によって情報システムのセキュリティを保護することとし、アクセス制御を行うに当たっての方針を定める。
(2) 機器等及び情報はすべてアクセス制御方針に従ったアクセス制御をしなければならない。
(3) 情報へのアクセスはアクセス制御方針に従って、利用者を制御しなければならない。

第 22 条（利用者アクセスの管理）

情報システムへのアクセス許可された利用者のアクセスを確実にし、許可されていないアクセスを防止するため、次の事項を定める。

１ 利用者登録

(1) 管理責任者は、情報システムごとに利用者の登録の条件を明確にする。
(2) 管理責任者は、担当者が異動した場合、又は職務に変更があった場合、アクセス権限を取り消す。
(3) 管理責任者は、情報セキュリティを侵害する行為を行った利用者に対し、アクセス権限の停止又は取り消しを行う。

２ 情報システムの特権の管理

(1) 管理責任者は、情報システムの特権の割当て及び利用を制限し、管理する。

(2) 情報システムの特権の割当て及び使用は、情報システムや装置を厳重に保護するものでなければならない。

３ 利用者パスワードの管理

利用者パスワードは機密が保たれ、有効でなければならない。利用者パスワードの管理方法や発行手順については、別途定める。

４ 利用者アクセス権限の見直し

(1) 管理責任者は、利用者のアクセス権限の必要性及びアクセスの範囲について、定期的に見直しを行わなければならない。

(2) アクセス権限の割当ては定期的に見直さなければならない。

第 23 条（利用者の責任）

１ 利用者パスワードの利用

職員は、利用者パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うことを、利用者に要求する。

(1) 管理責任者は、利用者パスワードが有効であるように、利用者パスワードの取り扱いに関する規定を定める。

(2) 利用者は、利用者パスワードの取扱いに関する規定に従い、パスワードを秘匿する責任を有することを認識しなければならない。

２ 無人状態にある利用者用機器等

(1) 管理責任者は、無人状態にある利用者用機器等を保護するための取り扱いを定め、利用者に徹底する。

(2) 管理責任者は、無人状態にある利用者用機器等の利用者による保護が困難な場合、保護できる環境を用意しなければならない。

３ クリアデスク・クリアスクリーン方針

(1) 利用者は、取り扱っている情報の機密保持のために、監視のない状態で情報や媒体を放置してはならない。

(2) 利用者は、離席時や帰宅時は、書類及び媒体を盗難や火災等の脅威から保護することとし、適切に保管しなければならない。

第 24 条（ネットワークのアクセス制御）

ネットワークを利用したサービスへの許可されていないアクセスを防止するため、次の事項を定める。

１ ネットワークサービスの利用についての方針

(1) ネットワーク管理者は、ネットワークサービスの種類別にアクセス権限の許可の手続きを定め、許可された利用者にのみアクセス権限を付与する。

(2) 利用者は、複合施設内ネットワークを経由するいかなるサービスも、定められた手続きに従って許可を得ないかぎりアクセスすることができないものとする。

２ 外部から接続する利用者の認証

管理責任者は、遠隔利用者のアクセスを管理するために、適切な認証方法を決定する。

３ ネットワークにおける機器等の識別

ネットワーク管理者は、特定の場所及び機器等からの接続を認証するための手段として、自動的な装置識別を考慮する。

(1) 自動的な端末識別は、その機能がコンピュータ及び端末に備わっている場合に使用する。

(2) 自動的な端末識別の機能がないが、セキュリティ保護に対し確実な識別が必要と判断される場合、その他の技術的な手段により識別する。

４ 遠隔診断用及び環境設定用ポートの保護

ネットワーク管理者は、診断用及び環境設定用ポートへの物理的及び論理的なアクセスを制御する。

５ ネットワークの領域分割

(1) ネットワーク管理者は、ネットワークが同一であることにより、取扱いに慎重を要する情報への脅威などがある場合、ネットワークを分離し情報を保護する。

(2) 規模の大きなネットワークで、通信の制御が必要であれば、ネットワークを論理的に分割し領域間の通信を制御する。

６ ネットワークの接続制御

ネットワーク管理者は、共有ネットワーク、特に、各組織の境界を越えて広がっているネットワークについて、必要に応じて利用者を制限する。

７ ネットワークルーティング制御

ネットワーク管理者は、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないために、ネットワークに対してルーティング制御の管理策を実施する。

第 25 条（オペレーティングシステムのアクセス制御）

オペレーティングシステムへの、許可されていないアクセスを防止するため、次の事項を定める。

１ セキュリティに配慮したログオン手順

管理責任者は、オペレーティングシステムへのアクセスに関して、セキュリティに配慮したログオン手順を定め、制御する。

２ 利用者の識別及び認証

すべての利用者は、個人ごとに一意な識別子（利用者ID）を保有する。また、利用者が主張する同一性を検証するために、適切な認証技術を選択する。

(1) 認証は利用者本人であることを証明し、利用者を一意に識別するものとする。

(2) 情報システムのすべての利用者は、利用者IDとパスワードの組合せ、または真正性を証明する他の確実な手段によって認証を行う。

３ パスワード管理システム

パスワードを管理するシステムは、対話式とすること。また、有効なパスワード設定を行えるものであること。

(1) 職員は、パスワードの設定、変更を行う場合、可能であれば有効なパスワードを設定するための対話的機能を利用者に提供する。

(2) システムの制約等から対話式の機能を備えられない場合、有効なパスワードを設定するための手段を講じなければならない。

(3) パスワードは、その有効性を維持するための管理を行わなければならない。

4 システムユーティリティの使用

管理責任者は、システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用を厳正に管理しなければならない。

5 セッションのタイムアウト

一定の使用中断時間経過時は、使用が中断しているセッションを遮断する。

(1) 管理責任者は、不正利用時のリスクの高い環境で、機密情報等を取り扱う端末が活動停止状態にある場合、端末のタイムアウト機能等により第三者のアクセスを防止する措置を講じなければならない。

(2) 端末のタイムアウト機能が利用できない場合、代替手段を講ずる。

6 接続時間の制限

機密情報等を取り扱う業務用ソフトウェアを、不正利用等のリスクの高い環境で使用する場合は、接続時間を制限する。

第 26 条（業務用ソフトウェア及び情報のアクセス制御）

業務用ソフトウェアが保有する情報への許可されていないアクセスを防止するため、次の事項を定める。

1 情報へのアクセス制限

管理責任者は、アクセス制御方針及び業務用システムの要求事項に従い、業務用ソフトウェアのアクセス制御を行うものとし、許可された者だけにアクセスを限定しなければならない。

2 取扱いに慎重を要するシステムの隔離

管理責任者は、取扱いに慎重を要する業務システムのセキュリティ保護の条件を明確にし、必要に応じ隔離された環境を用意するものとする。

第 27 条（モバイルコンピューティング（無線LANを含む））

モバイルコンピューティング及び無線LAN設備を用いた場合のリスクから保護するため、次の事項を定める。

(1) 管理責任者は、携帯用のコンピュータ又は情報機器の利用環境によるリスクを明確にし、適切な管理を行わなければならない。

(2) 管理責任者は、公共の場所、会議室、その他複合施設の敷地外などセキュリティの保護されていない場所でコンピュータを利用する場合の手順を定め、利用者に徹底する。

(3) 管理責任者は、公衆ネットワークを経由した複合施設内の業務へのアクセスについて、識別及び認証を厳重に行わなければならない。

第 28 条（技術的ぜい弱性管理）

管理責任者は、利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、それと関連するリスクに対処するために、適切な手段を講じること。

第8章　情報セキュリティインシデント対策

第 29 条（情報セキュリティインシデントの報告）

情報システムに関連する情報セキュリティインシデントが発生した場合に、時機を失さずに是正処置を講じるため、次の事項を定める。

1 情報セキュリティインシデントの報告

情報セキュリティインシデントは、管理責任者への連絡を通じて、できるだけ速やかに情報統括責任者に報告する。

(1) 情報セキュリティインシデント発生時の報告、連絡網を定め、対象者に周知させる。
(2) 情報セキュリティインシデントが発生した場合には、別途定める連絡網に従ってできる限り速やかに報告しなければならない。
(3) 連絡網は常に最新の状態に維持しなければならない。
(4) 可用性への影響の軽微なものは管理責任者が処置するものとする。

2 セキュリティ弱点の報告

管理責任者は、すべての職員、第三者の情報システム及びサービスの利用者に、システム又はサービスの中で発見した又は疑いを持ったセキュリティ弱点について、どのようなものでも報告するように要求する。

(1) 情報セキュリティの弱点を発見、又は発見したと思われる場合、発見者は直ちに連絡網に従って報告しなければならない。
(2) 管理責任者は、教育等の機会ごとに報告義務を徹底する。

第 30 条（情報セキュリティインシデントへの対応及び改善）

情報セキュリティインシデントの管理に、一貫性のある効果的な取組み方法を用いることを確実にするため、次の事項を定める。

1 責任及び手順

(1) 情報統括責任者は、セキュリティ事件・事故に対し、迅速に対処するための体制を定める。
(2) 管理責任者は、セキュリティ事件・事故を分析し、類似の事件・事故を防止するための手順を定める。
(3) 管理責任者は、セキュリティ事件・事故に対応する手順に関する教育を行い、有効性を確認しなければならない。

2 情報セキュリティインシデントからの学習

情報セキュリティインシデントの形態、規模及び復旧に要した費用を定量化し監視できるようにする仕組みを備えること。

(1) 管理責任者は事故調査チームを組織し、事故の調査を行う。
(2) 事故が組織をまたがる場合には情報統括責任者が事故調査の責任者を指名し、事故調査チームを組織する。
(3) 管理責任者は事故の原因を究明し、復旧に要した概算費用、再発防止策等をとりまとめ、その規模や重要性に応じ情報セキュリティ委員会に報告する。
(4) 情報セキュリティ委員会は、報告内容を審査し、類似の事件・事故を予防する措置を講ずる。

3 証拠の収集

情報セキュリティインシデント発生後の個人又は組織の事後処理が法的処理（民事又は刑事）に及ぶ場合には、関係する法令に従い、証拠を収集、保全し、提出する。

第9章　コンプライアンス

第 31 条（法的要求事項の遵守）

法令や契約上のあらゆる義務、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため、次の事項を定める。

1　適用法令の識別

各情報システム及び組織について、すべての関連する法令及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組み方を明確に定め、また、最新に保つこと。

(1) 適用法令等の識別及び改廃等の影響調査はそれぞれの組織で行い、調査結果を共有する。

(2) 管理責任者は、適用法令等の遵守事項を文書化し、教育等により対象者に徹底する。

2　知的財産権（IPR）

知的財産権が存在する可能性があるものを利用するとき、及び権利関係のあるソフトウェア製品を利用するときは、法令及び契約上の要求事項を遵守するための適切な手順を導入する。

(1) 管理責任者は、知的所有権の対象や遵守事項を明確にし、対象者に徹底する。

(2) 管理責任者は、ソフトウェア製品の取得及び取扱い手順と利用者の責務を定め、利用者に徹底する。

(3) 管理責任者は、定期的にソフトウェア製品の利用状況を調査し、知的所有権に違反していないことを確認する。

3　組織の記録の保護

管理責任者は、法令で定められた記録、訴訟等の証跡となる記録、事業活動に不可欠な記録など、組織として重要な記録について安全に保護する。また、重要な記録は、法令及び契約及び事業上の要求事項に従って、消失、破壊及び改ざんから保護する。

4　情報処理設備の誤用防止

情報システムは個人ごとに許可された権限の範囲内で使用するものとし、不適切な情報処理設備の使用を防止しなければならない。

5　暗号化機能に対する規則

暗号化機能は、関連するすべての協定、法令を遵守して用いること。

第 32 条（情報セキュリティ対策の遵守及び技術的コンプライアンス）

情報セキュリティ対策の遵守を確実にするため、次の事項を定める。

1　情報セキュリティ対策の遵守

(1) 管理責任者は、その組織の情報セキュリティ対策が正しく実行されていることを確認するために、内部監査を受けなければならない。

(2) 管理責任者は、情報システムが本ポリシーに適合していることを定期的に確認しなければならない。

2　技術的コンプライアンスの点検

(1) 管理責任者は、情報システムの実行環境が本ポリシーに適合していることを定期的に確認しなければならない。

(2) 管理責任者は、ハードウェア及びソフトウェアの管理策が正しく実行されていることを確認するため、定期的に情報システムの検査を行う。
(3) ネットワーク管理者は、ネットワーク装置の設定及び動作が、本ポリシーに適合していることを定期的に確認しなければならない。
(4) ネットワーク管理者は、分離されたネットワーク等について、セキュリティ境界が有効であることを定期的に確認する。
(5) 管理責任者は、ウィルス定義ファイルは最新版の状態が維持されているか随時確認する。