情報セキュリティ遵守特記事項

令和２年８月

西宮市　産業文化局　産業部　労政課

情報安全都市をめざして

～西宮市情報セキュリティ方針～

すべての人が安心して西宮市で「暮らす」「学ぶ」「働く」「過ごす」ためには、西宮市は一人ひとりについての情報および行政運営上の重要な情報を適切に管理・維持・使用しなければなりません。情報技術の進展に伴い、多くの業務が情報システムやネットワークに依存している中で、これらの情報や情報システム等を情報資産として適切に取り扱い、個人情報等の漏えいを防ぐとともに様々な脅威から防御し、情報セキュリティを維持することは、西宮市の重大な責務です。

西宮市がこの課せられた責任を真摯に果たすため、ここに情報セキュリティ方針を定めます。すべての対象者はこの方針に従い、行動しなければなりません。

（目的）

西宮市は情報資産において、

- 機密性を維持し、情報の漏洩等を発生させないこと
- 完全性を維持し、不正侵入、破壊等から守ること
- 可用性を維持し、事故、災害等によるサービス停止を防ぐこと

を目的とします。

目的実現のため、以下の取組みを実施します。

1．情報セキュリティ活動を推進するため、市長を最高情報セキュリティ責任者（CISO）とする情報セキュリティ委員会を設置します。また、情報の管理に関する役割と責任を明確にして情報セキュリティを維持します。

2．本市の職員は、西宮市情報セキュリティポリシー、個人情報の保護に関する法律、西宮市個人情報保護条例等の関連法令等を遵守し、責任をもって行動します。

3．本市の保有する情報資産の機密性、完全性、可用性の維持を脅かすリスクを評価し、リスク対応を実施します。

4．本市の保有する情報資産を守り、円滑な行政サービスを継続するために、関連施設および関連設備を事故・災害および外部の脅威・妨害から厳重に保護し、業務継続性を備えた強固な情報セキュリティ基盤を構築・維持します。

5．情報の機密性・完全性・可用性に影響を及ぼすような事故や災害等が発生した場合の対策を定めるとともに、速やかに機密性・完全性・可用性を回復させます。

6．情報セキュリティ活動が西宮市情報セキュリティポリシーに適合しているかどうかについて内部監査及び自己点検等を計画的に実施し、確認するとともに、本市の情報資産を取り扱う全職員等に対し、西宮市情報セキュリティポリシー等について教育及び訓練を実施します。

7．住民記録等システム、住民基本台帳ネットワーク、税務システム、税務外部接続システム、電子カルテ等業務管理システムにおいて、情報セキュリティマネジメントシステム（ＩＳＭＳ）を構築するとともに、定期的に見直し、継続的に改善します。また、定められた基準に適合しているかどうかについて、定期的な監査により確認するとともに、適用範囲の情報資産に関わるすべての職員等に対し、ＩＳＭＳの運用に関係する基準、手順について定期的に教育及び訓練を実施します。

令和元年１０月１日

西宮市長

石井登志郎

西宮市情報セキュリティ対策基準書

【０１】セキュリティ組織に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、セキュリティ組織に関し必要な事項を定めるものとする。

（対象範囲）
第２条　この基準は、西宮市情報公開条例第２条第１号に規定する実施機関に対して適用する。

第２章　情報セキュリティのための役割と責任

（最高情報セキュリティ責任者（ＣＩＳＯ）：A7.2.1）
第３条　市長を本市における最高情報セキュリティ責任者（以下、「ＣＩＳＯ」という。）とする。
ＣＩＳＯは本市における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最終決定権限及び責任を有する。
２　副市長を、副ＣＩＳＯとし、ＣＩＳＯが不在または欠けた場合はＣＩＳＯを代行する。
３　ＣＩＳＯは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家をアドバイザーとして置くことができる。

（ＣＩＳＯの役割：A5.1.2、A7.2.1）
第４条　ＣＩＳＯは、次の事項を実施する責任と権限を有する。
（１）本市の情報セキュリティ目的に則った情報セキュリティ方針を定めること
（２）情報セキュリティ方針を実現するためのＩＳＭＳ（情報セキュリティマネジメントシステム）を構築、運用し、そのために必要な役割及び責任の割当を行うとともに、必要な資源を提供すること
（３）情報セキュリティ委員会を主催すること
（４）マネジメントレビューを行い、本市のＩＳＭＳ実施状況をレビューすること
（５）情報セキュリティ委員会に対して、日々のポリシーの遵守状況確認、問題点の調査及び見直し、並びに教育・啓発活動を行う役割を担わせること

（ＩＳＭＳ統括責任者：A6.1.1）
第５条　総務局長をＩＳＭＳ統括責任者とする。
２　情報管理部長は、ＩＳＭＳ統括責任者を補佐し、ＩＳＭＳ統括責任者が不在または欠けた場合はＩＳＭＳ統括責任者を代行する。

（ＩＳＭＳ統括責任者の役割：A6.1.1）
第６条　ＩＳＭＳ統括責任者は、次の事項を実施する責任と権限を有する。
（１）ＩＳＭＳ統括責任者は、本市の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、ＣＩＳＯの指示に従い必要かつ十分な措置を行うこと
（２）本市の全ての情報セキュリティ実施プロセスの維持・管理を行うこと
（３）本市の全ての開発、変更、運用、見直し等に必要な対策等を行うこと
（４）本市の全ての組織、職員等に対して、情報セキュリティに関する指導及び助言を行うこと

（５）情報セキュリティ推進部会を主催すること

（教育長、水道事業管理者、局長級職員の役割：A6.1.1）
第７条　教育長、水道事業管理者、局長級職員は、次の事項を実施する責任と権限を有する。
（１）ＣＩＳＯの命を受け、当該部局または局の情報セキュリティ管理に関し、所属職員を指揮監督するとともに、ＣＩＳＯ及びＩＳＭＳ統括責任者を補佐すること
（２）当該局の所属職員に情報セキュリティ意識を周知徹底させるとともに、局内の統制及び調整を行うこと
（３）つねに当該局の情報セキュリティ状況を確認し、情報セキュリティの維持について改善を行うこと

（部長級職員の役割：A6.1.1）
第８条　部長等は、次の事項を実施する責任と権限を有する。
（１）所属上司の命を受け、当該部の情報セキュリティ管理に関し、所属職員を指揮監督すること
（２）当該部の所属職員に情報セキュリティ意識を周知徹底させるとともに、部内の統制及び調整を行うこと
（３）つねに当該部の情報セキュリティ状況を確認し、情報セキュリティの維持について改善を行うように努めること

（セキュリティ管理者・配備管理者・課長級職員の役割：A6.1.1）
第９条　課等の長を、当該課等の所管する全ての情報資産に対するセキュリティ管理者とする。
２　セキュリティ管理者は次の事項を実施する責任と権限を有する。
（１）所属上司の命を受け、情報セキュリティを適切に管理して所掌事務を実施すること
（２）課等内で管理している情報資産について、適切に管理し、情報セキュリティを維持すること
（３）セキュリティ管理に必要な実施手順を、情報セキュリティ事務局の審査後に承認し、所属職員に周知徹底させるとともに、手順実施にあたっては、課等内の統制及び調整を行う。
（４）所属職員に情報セキュリティ意識を周知徹底させ、セキュリティポリシーに基づいてセキュリティを維持するよう指導教育すること
（５）つねに課等内の情報セキュリティ状況を確認し、情報セキュリティの維持について改善を行うように努めること
３　情報機器等を調達・配備する課等の長を配備管理者とする。他部署に情報機器等を配備する場合、配備を受けた課等の長を当該情報機器等のセキュリティ管理者とする。

（セキュリティ担当者の役割：A6.1.1）
第１０条　セキュリティ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職員をセキュリティ担当者（ICT 調達担当者）とする。

（兼務の禁止：A6.1.2）
第１１条　セキュリティ管理者とセキュリティ担当者は同じ者が兼務してはならない。

（課等の所属職員の役割：A6.1.1）
第１２条　課等の所属職員は、セキュリティ管理者の指揮監督を受け、その職務上の命令に従い情報セキュリティの維持に努めなければならない。
２　課等の所属職員は情報セキュリティの懸念、問題点、改善点等があれば、そのつどセキュリティ管理者に報告し、その指示を受けなければならない。
３　本市関連業務に従事し、本市の情報資産を取り扱う外部関係者・事業者等についても、職員

と同様の義務を負う。

第３章　情報セキュリティのための組織

（情報セキュリティ委員会）

第１３条　ＣＩＳＯは情報セキュリティに関する、組織全体の調整を行うことを目的として、情報セキュリティ委員会を主催し、年１回以上開催しなければならない。ただし、ＣＩＳＯが必要と判断した場合には随時開催することができる。

２　情報セキュリティ委員会の委員長はＣＩＳＯとし、副委員長は副ＣＩＳＯとする。

３　情報セキュリティ委員会の構成員は、西宮市情報化推進本部会議設置規則に定める情報化推進本部会議の構成員とする。

４　情報セキュリティ委員会は、次の事項を実施する。

（１）情報セキュリティ方針を遵守したセキュリティ活動の確実な履行

（２）情報セキュリティ方針を遵守していない事項の扱い方の特定

（３）情報セキュリティのための方法及びプロセスの承認

（４）重要な脅威の変化の特定、並びに情報及び情報処理施設への脅威の露呈の特定

（５）毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認

（６）情報セキュリティの管理策の妥当性のアセスメント及びその実施の調整

（７）組織全体にわたる情報セキュリティの教育、訓練及び意識向上の効果的な促進

（８）情報セキュリティ事件・事故及びレビューによって得た情報の評価、並びに特定された情報セキュリティ事件・事故に応じた適切な処置の推奨

（９）庁内の関係者、専門家及び外部専門家に対する、情報セキュリティ委員会への必要に応じた出席要請

（１０）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を行う

（１１）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ふまえ、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

（情報セキュリティ推進部会）

第１４条　ＩＳＭＳ統括責任者は、情報セキュリティの実施を組織全体で行うための調整を目的として、情報セキュリティ推進部会を主催し、年１回以上開催しなければならない。ただし、ＩＳＭＳ統括責任者が必要と判断した場合には随時開催することができる。

２　情報セキュリティ推進部会長は総務局長（ＩＳＭＳ統括責任者）とし、副部会長は情報管理部長とする。

３　情報セキュリティ推進部会の構成員は、西宮市情報化推進本部会議設置規則に定める情報化推進本部幹事会の構成員とする。

４　情報セキュリティ推進部会は、次の事項を実施する。

（１）情報セキュリティ委員会の決定に基づき、情報セキュリティの実施を組織全体で行うための調整

（２）情報セキュリティに関して必要な事項について、情報セキュリティ委員会に対する報告もしくは意見具申

（３）セキュリティ内部監査委員長および委員の選出

（情報セキュリティ事務局：A6.1.4、A18.2.1）

第１５条　情報セキュリティ委員会、情報セキュリティ推進部会の活動における事務手続を担当し、活動を支援するため、情報管理部内に情報セキュリティ事務局を設置する。

2　情報セキュリティ事務局長は、情報企画課長とする。
3　情報セキュリティ事務局の構成員は、情報管理部職員とする。
4　情報セキュリティ事務局は、次の事項を実施する。
（1）情報セキュリティ委員会、情報セキュリティ推進部会の活動補助
（2）マネジメントレビューに必要な情報の提供
（3）情報セキュリティに関する連絡・調整・助言等
（4）情報セキュリティ事件・事故発生時の連絡窓口
（5）情報セキュリティに関する専門組織等との協力・調整・情報共有・連絡
（6）その他の情報セキュリティに関する事務取扱
（7）セキュリティの実施に重要な変化が生じた場合の独立したレビューの実施

第４章　セキュリティ教育・訓練

（情報セキュリティ維持に必要な力量と教育方法：A7.2.2）
第１６条　情報セキュリティに関する責任を割り当てられたすべての職員等に必要な力量をもたせるために、情報セキュリティ教育を実施しなければならない。
2　職員に必要な力量は次の通りとする。

業務種類	必要な力量
一般職員	一般職員に求められる責任を理解すること 情報セキュリティの重要性を理解し、意識を持つこと 情報セキュリティポリシーのしくみを理解すること 緊急時の対応について理解すること 法的要求事項について理解すること
セキュリティ管理者	一般職員の力量に加え、 セキュリティ管理者の権限と責任を理解すること セキュリティ区画管理について理解すること 情報資産の管理について理解すること 所掌部門におけるリスク分析と改善について理解すること
局長級・部長級職員	セキュリティ管理者の力量に加え、 局長級・部長級職員の権限と責任を理解すること セキュリティ内部監査のしくみを理解すること
ＩＳＭＳ統括責任者	局長級職員の力量に加え、 ＩＳＭＳ統括責任者の権限と責任を理解すること 情報セキュリティにかかる危機管理のしくみを理解すること
セキュリティ内部監査委員	部長級職員の力量に加え、 セキュリティ内部監査のしくみを理解すること ISO27001 の構造について理解すること

（情報セキュリティに関する教育：A7.2.2）
第１７条　情報セキュリティ事務局は、すべての職員等に情報セキュリティ維持に必要な力量を持たせるため、情報セキュリティに関する年度教育計画を立案し、情報セキュリティ委員会の承認を得なければならない。
2　教育計画において、職員等は毎年度最低１回は情報セキュリティ教育を受講できるようにしなければならない。

３　教育終了後は、その有効性を評価し、受講歴とともに記録しなければならない。

第５章　懲戒手続

（懲戒手続：A7.2.3）

第１８条　職員等が情報セキュリティポリシーに違反する行動を確認した場合には、セキュリティ管理者は速やかに次の措置を講じなければならない。

（１）直ちに違反行動の中止を指示すること

（２）必要に応じてセキュリティ区画からの退出と情報資産の使用停止を命じること

２　前項の措置によっても改善されない場合、ＩＳＭＳ統括責任者は、当該職員等の情報資産の使用を強制的に停止することができる。この場合は、職員等の情報資産の使用を停止した旨をＣＩＳＯ及びセキュリティ管理者に通知しなければならない。

３　セキュリティ違反を犯した職員等及びその監督責任者、並びにセキュリティ管理者は、その重大性、発生した事案の状況等に応じて、地方公務員法に従った懲戒処分の対象とする。

第６章　マネジメントレビュー

（マネジメントレビュー：A5.1.2）

第１９条　情報セキュリティ方針および、組織のＩＳＭＳの適切性、妥当性及び有効性を確保するため、年一回以上、又は重大な変化が発生した場合に、ＣＩＳＯはマネジメントレビューを実施しなければならない。

２　マネジメントレビューでは、情報セキュリティの方針及び目的を含め、ＩＳＭＳに対する改善の機会及び変更の必要性のアセスメントも行わなければならない。

３　マネジメントレビューの結果は、明確に文書化し、記録を維持しなければならない。

（マネジメントレビューへのインプット：A5.1.2）

第２０条　情報セキュリティ事務局は、マネジメントレビューに際しては、以下の情報をＣＩＳＯに提供しなければならない。

（１）ＩＳＭＳ監査及びレビューの結果

（２）利害関係者からのフィードバック

（３）ＩＳＭＳのパフォーマンス及び有効性を改善するために組織の中で利用可能な技術、製品又は手順

（４）予防処置及び是正処置の状況

（５）前回までのリスクアセスメントが十分に取り上げていなかった脆弱性又は脅威

（６）有効性測定の結果

（７）前回までのマネジメントレビューの結果に対するフォローアップ

（８）ＩＳＭＳに影響を及ぼす可能性がある、あらゆる変化

（９）改善のための提案

（マネジメントレビューからのアウトプット：A5.1.2）

第２１条　ＣＩＳＯは、マネジメントレビューからのアウトプットとして、以下の決定及び措置を含めなければならない。

（１）ＩＳＭＳの有効性の改善

（２）リスクアセスメント及びリスク対応計画の更新

（３）ＩＳＭＳに影響を与える可能性がある内外の事象に対応するために、必要に応じた、情報セキュリティを実現する手順及び管理策の修正。

（４）必要となる経営資源
（５）管理策の有効性測定方法の改善

【０２】コンプライアンスに関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、法令、規制又は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（以下、「法的要求事項」という。）に関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

第２章　順守

（適用法令の識別と個人情報保護：A18.1.1、A18.1.4）
第３条　職員等は、法的要求事項を順守しなければならない。
２　個人情報に関しては、個人情報の保護に関する法律及び西宮市個人情報保護条例の規定を遵守しなければならない。
３　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、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。
４　その他、共通に留意すべき法令及び関連規定については、表１「ＩＳＭＳ関係法令等一覧」に示す。

（知的財産権：A18.1.2）
第４条　職員等は、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、以下の事項を順守しなければならない。
（１）法的要求事項で認められる範囲で利用しなければならない。
（２）本市が正式に使用許諾されているソフトウェア製品以外は使用してはならない。
（３）ソフトウェア製品の使用にあたっては、使用許諾を得ていることの証明及び証拠、並びにマスタディスク、インストール数、手引き等を維持管理しなければならない。

（例外措置）
第５条　セキュリティ管理者は、以下の場合には例外措置の対応ができる。
（１）例外措置の許可
　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、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の許可を得て、例外措置を取ることができる。
（２）緊急時の例外措置
　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に報告しなければならない。
（３）例外措置の申請書の管理
　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。

第３章　契約

（外部事業者等との契約：A15.1.1、A15.2.1、A14.2.7）

第６条　情報システムや機器、サービス等の利用に関し、外部事業者等と契約する場合は、セキュリティ管理策、サービス管理について確認し、要求仕様として記述しなければならない。

２　セキュリティ管理者が外部事業者と業務委託契約を締結する時には、原則として「情報処理関連業務委託に関する一般仕様書」（以下、「一般仕様書」という。）を使用しなければならない。

３　情報管理部は、業務委託契約のための一般的なセキュリティ要求事項を記載した「一般仕様書」を作成し、庁内に公開しなければならない。

４　業務委託以外の契約であっても、作業等を含む場合には「一般仕様書」の必要事項を考慮して仕様書に記載しなければならない。

５　セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（約款による外部サービスの利用：A15.1.1、A15.1.3）

第７条　セキュリティ管理者は、以下を含む約款による外部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。また、当該サービスの利用において、重要性分類がＢ以上の情報は、法令で定められた場合を除いては取扱われないように規定しなければならない。

（１）約款によるサービスを利用してよい範囲

（２）業務により利用する約款による外部サービス

（３）利用手続及び運用手順

２　職員等は、利用するサービスの約款、その他提供条件から、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約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

（ソーシャルメディアサービスの利用：A13.2.3）

第８条　セキュリティ管理者は、本市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含めたソーシャルメディアサービス運用手順を定めなければならない。

（１）本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブ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行うこと。

（２）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（IC カード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと

２　重要性分類がＡまたはＢの情報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。

表１．ＩＳＭＳ関係法令等一覧

法令等の種類	法令の名称及び主な参考条項	遵守方法
契約に関する法令	民法　全般（第四編、第五編を除く）	<基準②-02>第 5 条 <基準②-06>第 4 条
コンピュータ犯罪に関する法令	刑法 第 7 条の２　電磁的記録の定義 第 157 条　公正証書原本不実記載等 第 158 条　偽造公文書行使等 第 161 条の２　電磁的記録不正作出・不正作出電磁的記録供用 第 234 条の２　電子計算機損壊等業務妨害罪 第 236 条の２　電子計算機使用詐欺罪 第 258 条　公用文書等毀棄罪 第 259 条　私用文書等毀棄罪	入所時研修、力量研修における遵法教育 その他、 <基準②-04>第 4 条 <基準②-04>第 10 条 <基準②-08>全般 <基準②-07>全般
	不正アクセス行為の禁止等に関する法令　全般	<基準②-04>第 13 条 <基準②-09>全般
知的財産権等に関する法令	著作権法 第 2 条　定義 第 10 条　著作物の例示 第 12 条の２　データベースの著作物 第 20 条　同一性保持権 第 47 条の２　ﾌﾟﾛｸﾞﾗﾑの著作物の複製物の所有者による複製等 第 76 条の２　創作年月日の登録 第 113 条　侵害とみなす行為	入所時研修、力量研修における遵法教育。 ライセンス管理実施。 その他、 <基準②-02>第 4 条 <基準②-02>第 5 条 <基準②-04>第 4 条
	特許法　全般	
営業秘密の不正取得・利用行為等に関する法律 ドメイン名の不正取得・保有・使用する行為に関する法律	不正競争防止法	<基準②-04>第 4 条
個人情報保護に関する法令及び要求事項	OECD8 原則（プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告） 個人情報の保護に関する法律 行政機関の保有する個人情報の保護に関する法律 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	入所時研修、力量研修における遵法教育 その他、 <基準②-04>第 4 条
設備に関する法令	建築基準法 建築基準法施行令 消防法 消防法施行令 消防法施行規則	<基準②-05>全般
地方公務員に関する法律	地方公務員法	入所時研修、力量研修における遵法教育 その他、 <基準②-04>第3条 <基準②-04>第5条 <基準②-04>第15条 <基準②-04>第16条 <基準②-04>第17条
関連する庁内規則	西宮市情報公開条例 西宮市情報公開条例施行規則 西宮市個人情報保護条例 西宮市個人情報保護条例施行規則 西宮市行政手続等における情報通信の技術の利用に関する条例 西宮市行政手続等における情報通信の技術の利用に関する条例施行規則	入所時研修、力量研修における遵法教育 その他、 <基準②-04>第 4 条 <基準②-06>第 16 条
個別業務に関連する法令	住民基本台帳法 その他、行政事務にかかわる各種根拠法令	力量教育における遵法教育

サイバーセキュリティに関する法令	サイバーセキュリティ基本法	

【０３】情報資産管理に関する基準

第１章　総則

（趣旨）

第１条　この基準は、西宮市情報セキュリティ方針に基づき、情報資産管理に関して必要な事項を定めるものとする。

（対象者・対象範囲）

第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

２　対策基準が対象とする情報資産の範囲は、次のとおりとする。

（１）ネットワーク、情報システム、これらに関する設備、電磁的記録媒体、紙媒体

（２）ネットワーク及び情報システムで取り扱う情報

（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）公文書（紙媒体及び電子データ）

第２章　情報資産の管理

（情報資産台帳：A8.1.1、A8.1.2）

第３条　セキュリティ管理者は、その所管する情報資産について管理責任を有する。

２　セキュリティ管理者は、システムに関連する重要性分類Ｂ以上（後述）の情報資産について、情報資産台帳を作成し、情報資産の種類、形式、所在、管理者等について明確にしなければならない。

３　セキュリティ管理者は、システムに関連する重要性分類 Ｂ 以上（後述）の情報資産の追加、変更、廃止等があった場合には、速やかに情報資産台帳を改訂しなければならない。

（情報資産の分類：A8.2.1）

第４条　本市における情報資産は、機密性、完全性、可用性及び法的要求事項等を考慮して、次のとおり分類する。

分類	項目	内容
重要性分類Ａ	定義	情報セキュリティの侵害が、業務の１日以上の停止、もしくは市民生活に重大な影響を及ぼすもの ※個人情報が含まれる情報は、重要性分類Ａとしなければならない。
	要件	個人情報、及び下記の情報のうち業務上必要とする最小限の者のみが扱うべき情報（極秘情報） ・法令などの定めにより守秘義務が課せられている情報 ・外部に知られることを適当としない法人等に関する情報 ・漏洩した場合、市政に対する信頼を著しく阻害するおそれのある情報
	例示	住民基本台帳情報、市民税情報、国民健康保険情報、図書館の利用者情報、職員名簿情報、特定個人情報、業務で利用するメールアドレス等
重要性分類Ｂ	定義	情報セキュリティの侵害が、業務の半日程度の停止、もしくは市民生活に軽微な影響を及ぼすもの ※非公開・部分公開の公文書は、重要性分類Ｂ以上としなければならない。

	要件	（1）法令若しくは条例の定めるところにより又は実施機関が法律上従う義務を有する国の機関等の指示により、公にすることができない情報 （2）通常他人に知られたくないと望むことが正当であると認められる個人に関する情報で、特定の個人が識別されうるもの。ただし、事業を営む個人の当該事業に関する情報を除く。 （3）法人その他の団体（国及び地方公共団体を除く。以下「法人等」という。）に関する情報又は事業を営む個人の当該事業に関する情報で、公開することにより、当該法人等又は当該個人の競争上の地位その他正当な利益を害すると認められるもの。ただし、人の生命、身体若しくは健康に危害を及ぼすおそれのある事業活動又は人の財産若しくは生活若しくは環境に重大な影響を及ぼすおそれのある違法若しくは著しく不当な事業活動に関する情報を除く。 （4）市と国、地方公共団体その他公共団体（以下「国等」という。）との間の協議依頼等に基づいて作成し、又は取得した情報で、公開することにより、当該国等との協力関係又は信頼関係を著しく害すると認められるもの （5）市の内部又は市と国等との間における調査、検討、審議、企画等の意思形成過程に関する情報で、公開することにより、率直な意見の交換若しくは意思決定の中立性が不当に損なわれるおそれ、不当に市民の間に混乱を生じさせるおそれ又は特定の者に不当に利益を与え、若しくは不利益を及ぼすおそれがあるもの （6）市又は国等が行う立入検査、試験、入札、交渉、渉外、争訟、人事その他の事務事業に関する情報で、公開することにより、当該事務事業又はこれと同種の事務事業の公正かつ円滑な執行に著しい支障が生じるおそれのあるもの （7）公開することにより、人の生命、身体若しくは財産等の保護、公共の安全又は秩序の維持に支障を及ぼすと認められる情報
	例示	指定統計調査票、取引先・得意先の経営、運営等に関する情報、新開発技術内容、商品の検査又は調査結果、立入検査、技術指導、評価、工事に係る評価、各種政策に関する情報　各種試験問題、用地取得の計画、用地買収の交渉経過、調達予定価格情報、設計単価、争訟の方針等（キャビネット「情報公開制度の手引き」参照）
重要性分類 C	定義	情報セキュリティの侵害によっても、業務停止や市民生活への影響がほとんどないもの
	要件	重要性分類Ａ、Ｂ以外の情報
	例示	重要性分類Ａ及びＢに該当しないもの

（情報のラベル付け：A8.2.2、A8.2.3）

第５条　セキュリティ管理者は、情報資産の重要性分類に従って、情報資産を適切に保管しなければならない。

２　セキュリティ管理者は、容易に移動、持出が可能な記録媒体（ＦＤ、ＣＤ、ＵＳＢメモリ等）には、第三者には容易に重要性を認識できないような記号等により、重要性分類を表示しなければならない。ただし、端末機、サーバ機器、ネットワーク機器等は重要性が高いことが周知の事実であるため、重要性分類の表示対象から除外する。

第３章　情報資産の取扱い

（情報資産の作成：A8.1.1）

第６条　職員等は、業務上必要のない情報を作成、入手等してはならない。個人情報の取得、管理については西宮市個人情報保護条例を遵守しなければならない。

２　作成、入手した情報を保管するときは、重要性分類に基づいた取扱いをしなければならない。庁内の他部門が作成した情報を入手した者は、入手元の重要性分類に基づいた取扱いをしなければならない。

３　作成、入手した情報の重要性分類が不明な場合、セキュリティ管理者に判断を仰がなければならない。

（情報資産の保管：A8.2.2）

第７条　重要性分類Ａの情報を保管する場合、耐火、耐熱、耐水及び耐湿を考慮した施錠可能な場所に保管しなければならない。

２　重要性分類Ｂの情報を保管する場合、施錠可能な場所に保管しなければならない。

３　情報資産は西宮市文書取扱規程、契約書、その他の定められた保存年限に応じて処理されなければならない。

４　職員等は、パソコンや記録媒体等にやむを得ず重要性分類Ｂ以上の情報を一時的保管する場合は、暗号化かつパスワードをしなければならない。

（記録媒体の管理：A8.3.1）

第８条　セキュリティ管理者の許可なしに、記録媒体を使用してはならない。

２　記録媒体は、セキュリティが保たれた環境に保管しなければならない。

３　記録媒体に重要性分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

４　記録媒体に格納した情報が不要となったときは、再利用不可能な形で消去しなければならない。

（情報資産の持出し等：A8.2.2、A11.2.5、A8.3.3、A18.1.5）

第９条　重要性分類Ｂ以上の情報は、法令で定められた場合を除いては、外部に提供、交付、送信等をおこなってはならない。

２　重要性分類Ｂ以上の情報は、セキュリティ管理者の許可なく、外部に持ち出してはならない。

３　重要性分類Ｂ以上の情報を、許可を得て持ち出す場合は、データ持ち出しについて記録するとともに、ケースの施錠、暗号化など情報の不正利用を防止するために必要な措置を講じなければならない。

４　重要性分類Ｂ以上の情報を郵便等により配送する必要がある場合は、信頼できる輸送機関を用いるとともに、必要に応じて施錠したコンテナの使用、開封防止包装などの情報の不正利用を防止するために必要な措置を講じなければならない。

５　暗号機能を有する情報機器等の国外への持ち出し等は行ってはならない。

６　セキュリティ管理者は、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、あらかじめ職員又は委託した業者に確認を行わせなければならない。

７　セキュリティ管理者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

※暗号技術を使用した暗号装置を日本国外へ持ち出す場合、またはそれらの暗号技術を国内外の非居住者に提供する場合には、「外国為替および外国貿易法」に基づく輸出許可又は役務取引許可の手続きが原則必要となります。

（電子署名・暗号化：A13.2.1）

第１０条　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、情報システム課長が定めた電子署名、暗号化又はパスワード設定の方法を使用して、送信しなければならない。
２　職員等は、暗号化を行う場合に情報システム課長が定める以外の方法を用いてはならない。また、情報システム課長が定めた方法で暗号のための鍵を管理しなければならない。

（情報のバックアップ：A12.3.1）
第１１条　重要性分類Aの電子データおよびソフトウェアについては、定期的にバックアップを取得しなければならない。
２　前項のバックアップは、保管場所のセキュリティ状況を考慮し、必要に応じて自然災害を被る可能性が低い地域に保管しなければならない。

（記録の保存、証拠保全：A16.1.7、A18.1.3）
第１２条　業務の重要な記録、サーバ等の利用記録等は法的要求事項にしたがって、消失、破壊及び改ざんから保護しなければならない。これらの記録の法的な証拠能力を確保するため、原本は厳重に保管しなければならない。

（クロックの同期：A12.4.4）
第１３条　セキュリティ管理者は、その所有する情報機器について、正確な時刻設定ができる措置を講じなければならない。

第４章　情報資産の廃棄

（媒体の処分：A8.3.2）
第１４条　重要性分類Ｂ以上の情報を記録している記録媒体が不要になった場合、媒体の物理的破壊など、情報を復元できないように処置した上で廃棄しなければならない。
２　情報資産の廃棄を行うときは、セキュリティ管理者の許可を得るとともに、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。

（情報機器の内部の記憶装置の取扱い：A11.2.7、A8.3.2）
第１５条　セキュリティ管理者は、情報機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべての情報及びソフトウェアを消去の上、復元不可能な状態にする措置を講じなければならない。
２　セキュリティ管理者は、記憶媒体を内蔵する機器を外部の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、セキュリティ管理者は、外部の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、守秘義務について合意の上、秘密保持体制の確認などを行わなければならない。
※情報機器は、コピー機、複合機等の機器を含む。

【０４】職員等の情報資産使用に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、職員等が情報資産を使用する際に遵守すべき内容に関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

第２章　情報資産の利用要件

（情報資産の利用資格：A7.1.1、A7.1.2）
第３条　本市の情報資産を利用できるのは以下の者とする。
（１）身元確認を受けて採用され、採用にあたって誓約書を提出した職員。情報資産へのアクセス権限については、西宮市事務分掌条例等に定められた事務分掌と、事務分担表により管理しなければならない。
（２）身元と経歴が明らかであり、セキュリティに関する要求事項の順守を誓約した外部委託要員。

（秘密保持誓約：A13.2.4）
第４条　職員は西宮市処務規則に従い、採用時の誓約書の提出をもって、地方公務員法に定められた守秘義務を負う。
２　職員以外の第三者が、本市の情報資産を使用する場合は、秘密保持誓約書をＣＩＳＯに提出しなければならない。
３　セキュリティ管理者は、秘密保持誓約書の提出を確認し、適切に管理しなければならない。

（雇用・契約の終了時等の責任：A7.3.1）
第５条　職員等は、異動、退職等により業務を離れた後も業務上知り得た情報を漏らしてはならず、関連する情報セキュリティに関する責任を負わねばならない。

（資産の返却：A8.1.4）
第６条　職員等は、退職時もしくは契約終了時に、貸与等を受けていた情報資産すべてを返却しなければならない。
２　職員は、異動時に、所属のセキュリティ管理者より貸与等を受けていた情報資産がある場合は、すべてを返却しなければならない。

第３章　情報資産の取り扱い

（情報資産の利用：A8.1.3、A11.2.8）
第７条　すべての情報資産は、業務目的以外のために使用してはならない。
２　取扱いに慎重を要する情報資産は、必要のないときや職員の不在時には、施錠等を行い、管

理しなければならない。

（情報資産の取扱い：A8.1.3）
第８条　各種情報資産は、配備管理者が定める手順にしたがって使用しなければならない。
２　セキュリティ管理者は、手順に従い当該情報資産を厳重に管理し、適正な使用に努めなければならない。
３　配備管理者は、配備した情報機器が適正に管理、使用されていないと判断したとき、または緊急の必要があると判断したときには、情報機器の使用停止、機器撤去を命じることができる。

（機微情報の取扱い：A8.1.3）
第９条　個人情報等の機微情報の取り扱いについては、各種法令に従い、適切に取り扱わなければならない。
２　端末等の画面の写し（以下、「ハードコピー」という）は、画面表示の確認目的以外に出力してはならない。また、交付等は行ってはならない。
３　ハードコピーは、確認終了後再利用不可能な方法で速やかに廃棄しなければならない。

第４章　情報機器の利用

（システム装置の適正使用：A6.1.1）
第１０条　職員等は、システム装置の故障、誤作動等を招来する行為等を行ってはならない。

（設定変更の禁止：A12.1.2、A14.2.4）
第１１条　職員等は、パソコン等のソフトウエアに関するセキュリティ機能の設定をセキュリティ管理者または配備管理者の許可なく変更してはならない。
２　セキュリティ管理者または配備管理者が定めた以外のソフトウエアを許可なく利用してはならない。業務上やむを得ない場合は、所属のセキュリティ管理者の承認を得た上で、配備管理者の許可を得なければならない。

（クリアデスク・クリアスクリーン：A11.2.9）
第１２条　端末等の画面は、離席時や使用していないときには取扱いに慎重を要する情報が表示されない状態にしなければならない。
２　取扱いに慎重を要する文書等は、机上・プリンタ・スキャナ等に放置してはならない。

（パスワードの利用：A9.3.1）
第１３条　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）業務上やむを得ず共用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。
２　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）パスワードを秘密にしなければならない。
（２）パスワードを記載したメモを放置してはならない。
（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、セキュリティ管理者または配備管理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）パスワードは定期的に変更するよう努めなければならない。
（６）パスワードは他のシステムのパスワードを使い回してはならない。
（７）仮のパスワードは、最初のログイン時点で変更しなければならない。

（８）パソコン等の端末のパスワードの記憶機能を利用してはならない。
（９）職員等間でパスワードを共有してはならない。

（マルウェアに関する順守事項：A12.2.1）
第１４条　職員等は、マルウェア対策に関し、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、マルウェア対策ソフトウエアが導入されている場合は、当該ソフトウエ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エアを取り入れる場合には、必ずマルウェア対策ソフトウエ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）情報セキュリティ事務局が提供するマルウェア関連情報を、常に確認しなければならない。
（５）マルウェアへの感染が疑われる場合には、ネットワークからの遮断等の措置を講じた上で、情報セキュリティ事務局及びセキュリティ管理者に速やかに報告しなければならない。

※マルウェア（Malware）とは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称

（私物パソコンの使用禁止：A7.1.2）
第１５条　職員等は私物パソコンを持ち込んではならず、また、それを利用して業務情報の処理を行ってはならない。

第５章　ネットワーク利用

（電子メール等の利用制限：A7.1.2）
第１６条　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、重要な電子メールを誤送信した場合、情報セキュリティ事務局及びセキュリティ管理者に報告しなければならない。
４　職員等は、インターネット上で利用できるフリーメール、ネットワークストレージサービス、Ｐ２Ｐサービス等を原則として業務で使用してはならない。ただし、ほかの方法をもって所期の目的を果たすことができないと認められる場合は、情報セキュリティ事務局と協議の上、これを認めるものとする。

※フリーメール（free mail）とは、インターネット接続サービスに加入していなくても、必要な事項（希望のメールアドレス、パスワードなど）を入力すれば無料で電子メールアカウントが取得できるサービスのこと
※ネットワークストレージサービス（network storage service）とは、インターネット上でファイル保管用のディスクスペースにデータを保存することができるサービスのこと
※Ｐ２Ｐサービス（Peer to Peer service）とは、不特定多数の個人間で直接情報のやり取りを行なうインターネットの利用形態またはそのためのアプリケーションのこと

（業務以外の目的でのウェブ閲覧の禁止：A7.1.2）
第１７条　職員等は、業務以外の目的でウェブを閲覧してはならない。
２　ＩＳＭＳ統括責任者は、職員等のウェブ利用について、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、セキュリティ管理者に通知し適切な措置を求めなければ

ならない。
３　ネットワーク管理者は業務以外の目的でウェブ閲覧が行われることを抑止するための対策を講じなければならない。

（無許可でのネットワーク接続の禁止：A11.2.1）
第１８条　職員等は、ネットワーク管理者の許可なくパソコン等の機器をネットワークに接続してはならない。

第６章　情報セキュリティに関する報告

（職員等の報告義務：A16.1.2）
第１９条　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、直ちにセキュリティ管理者に報告を行わなければならない。
２　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セキュリティ管理者が判断した場合は、「情報セキュリティ事件・事故に関する基準」に従って適切に対処しなければならない。

（セキュリティ弱点の報告：A16.1.2）
第２０条　職員等はセキュリティ事故を防止するため、発見もしくは疑いをもったセキュリティ弱点について、セキュリティ管理者に連絡しなければならない。
２　職員等は、疑いをもった弱点について、自ら立証しようと試みてはならない。

【０５】セキュリティ区画管理に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、セキュリティ区画管理に関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

（定義）
第３条　この基準において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
（１）セキュリティ区画　情報資産を用いて業務を行うとともに物理的な管理を行う区域
（２）高度セキュリティ区画　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、当該機器等の管理並びに運用を行うための施設等の区域。

第２章　セキュリティ区画

（セキュリティ区画：A11.1.1）
第４条　セキュリティ管理者は、管理下にある事務室、部屋及び施設等（以下、「事務室等」という。）について、セキュリティ区画を明確に定め、適切に管理しなければならない。
２　セキュリティ区画を定めるにあたっては、事務室等で管理する情報資産やリスクなどを総合的に勘案して決定しなければならない。
３　セキュリティ管理者は、セキュリティ区画を物理的な障壁もしくは表示等により明確に区分し、第三者が誤って立ち入ることのないようにしなければならない。
４　セキュリティ区画内には、職員及びセキュリティ管理者が許可した者以外は立ち入ることはできない。
５　事務室等の移転・変更、情報資産の追加や変更、リスク要因の変動等が生じた場合は、セキュリティ区画の妥当性について検討し、必要な場合には速やかにセキュリティ区画を変更しなければならない。

（セキュリティ区画の入退管理策：A11.1.2）
第５条　セキュリティ管理者は、許可された者だけがセキュリティ区画に入室できるよう、下記の入退管理策を定め、実施しなければならない。
（１）外部訪問者の入退日時、訪問目的、訪問者氏名等の確認
（２）外部訪問者に対するセキュリティ区画内での注意事項の指示
２　セキュリティ管理者が入室許可証等の標識を定めている場合は、セキュリティ区画への入室が認められた者はこれを着用しなければならない。ただし西宮市職員については、正規の名札の着用をもって入室許可証の着用に代えることができる。

（セキュリティ区画の外部及び環境の脅威からの保護：A11.1.4）
第６条　セキュリティ管理者は、セキュリティ区画を火災、自然災害、事故、犯罪行為等の脅威による損傷から保護するために、必要な対策を実施しなければならない。

2　職員等が専用で使用する端末機、プリンタ、ファクシミリ、コピー機等を設置するときは、セキュリティ区画内に設置しなければならない。
3　前項の機器類を設置するときは、外部の者が出力物を簡単に持ち去ることができないよう配慮しなければならない。
4　セキュリティ区画が無人になる場合には、施錠、巡回警備、遠隔監視等により第三者の潜入を防止しなければならない。

（セキュリティ区画での作業、業務用情報システム：A11.1.5）
第７条　セキュリティ管理者の許可なく、外部から情報機器、写真機、ビデオカメラ、記憶媒体等をセキュリティ区画内に持ち込んではならない。
2　市が配備した以外の情報機器、写真機、ビデオカメラ、記憶媒体等を業務に使用してはならない。

（一般の人の立寄り場所及び受渡場所：A11.1.6）
第８条　窓口対応や荷物などの受け渡しは、セキュリティ区画外で行わなければならない。
2　前項についてセキュリティ区画内で行う必要がある場合は、必要最小限度に留め、所定の入退管理策を実施しなければならない。

第３章　高度セキュリティ区画

（高度セキュリティ区画：A11.1.1、A11.1.3）
第９条　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、当該機器等の管理並びに運用を行うための施設等のセキュリティ管理者は、当該管理区域について高度セキュリティ区画を明確に定め、適切に管理しなければならない。
2　高度セキュリティ区画は一般の人のアクセスが避けられる場所に設置し、高度セキュリティ区画であることを示す表示は、必要最小限度にとどめなければならない。
3　高度セキュリティ区画のセキュリティ管理者は、高度セキュリティ区画への入室経路は必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。
4　高度セキュリティ区画が無人になるときには、最終退出者が施設、機器、情報資産等の確認と施錠等を行い、その内容について退出記録簿に記入しなければならない。
5　高度セキュリティ区画に関する脅威やリスク要因の変動等が生じた場合は、高度セキュリティ区画の妥当性について検討し、必要な場合には速やかに高度セキュリティ区画を変更しなければならない。
6　高度セキュリティ区画を変更する場合は、レイアウト図を速やかに情報セキュリティ事務局に提出し、情報セキュリティ委員会の承認を得なければならない。

（高度セキュリティ区画の入退管理策：A11.1.2）
第１０条　高度セキュリティ区画のセキュリティ管理者は、高度セキュリティ区画への入退室は許可された者のみに制限しなければならない。
2　高度セキュリティ区画のセキュリティ管理者は、下記の入退管理策を定め、実施しなければならない。
（１）入退室時認証装置の設置と利用記録の管理
（２）外部訪問者の入退日時、訪問目的、訪問者氏名等の確認と入退室管理簿への記載
（３）外部訪問者に対するセキュリティ区画内での注意事項の指示
3　高度セキュリティ区画への入室が認められた訪問者は、セキュリティ管理者が定めた入室許可証を着用しなければならない。ただし西宮市職員については、正規の名札の着用をもって入

室許可証の着用に代えることができる。

（高度セキュリティ区画の外部及び環境の脅威からの保護：A11.1.4）

第１１条　高度セキュリティ区画のセキュリティ管理者は、区画を火災、自然災害、事故、犯罪行為等の脅威による損傷から保護するために、必要な対策を実施しなければならない。

２　高度セキュリティ区画に設置する消火薬剤や消防用設備等は、それらを使用したときに機器等及び記録媒体に影響を与えないよう配慮しなければならない。

３　高度セキュリティ区画に設置している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なければならない。

４　高度セキュリティ区画には、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。

第４章　セキュリティ区画外

（セキュリティ区画外にある装置のセキュリティ：A11.2.6）

第１２条　情報機器は、原則としてセキュリティ区画外で使用してはならない。やむを得ず使用が認められていないセキュリティ区画外（特に庁舎外）で使用する場合には、配備管理者および情報セキュリティ事務局の許可を得なければならない。

２　業務上の必要性に基づき、情報機器を新たにセキュリティ区画外に設置等する場合は、ＩＳＭＳ統括責任者の許可を得なければならない。

３　前項について、許可を得て設置する場合は、セキュリティ区画内とは異なるリスクを考慮して、必要なセキュリティ対策を実施しなければならない。

【０６】ＩＣＴ関連調達に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、情報システムの開発・導入に関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

第２章　導入前プロセス

（情報システム等導入の承認プロセス）
第３条　情報システム・設備・サービス等の購入、賃借、開発、使用、改修等（以下、「ＩＣＴ調達」という。）を行おうとするときは、その目的及び用途について所管のセキュリティ管理者の承認を受けるとともに、情報管理部の確認を受けなければならない。
２　前項を実施するため、情報管理部長は、ＩＣＴ調達手順に関するガイドラインを別途定める。

（仕様の作成：A14.1.1、A14.2.7）
第４条　ＩＣＴ調達に関する仕様書を作成する際には、本市が実施する情報セキュリティ要求事項に関する内容を含めなければならない。
２　ソフトウェア開発を外部に委託するときは、ソフトウェアに関する諸権利および、納品物の確認および必要な監査についての規定を含めなければならない。

（業務用ソフトウェアに関する要求事項：A14.2.5）
第５条　セキュリティ管理者は、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　セキュリティ管理者は、故意又は過失により情報が破壊、改ざん又は漏えい等の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　コンピュータウイルス、不正侵入等を使った破壊行為によりメッセージが変更されるリスクが想定されるときには、メッセージの完全性の必要性について判断し、必要な対策を実装しなければならない。
４　セキュリティ管理者は、情報システムから出力されるデータについて、情報の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。

第３章　開発・変更の管理手順

（管理手順：A12.1.2、A15.2.2、A14.2.9、A12.5.1）
第６条　大規模なＩＣＴ調達にあたっては、下記の手順で管理し、実施するとともに、文書化しなければならない。

（１）責任者及び作業者を特定
（２）責任者、作業者のＩＤの管理
ア　セキュリティ管理者は、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を削除する
イ　セキュリティ管理者は、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する
（３）重要な変更等の特定及び記録を作成し、一定期間保管
（４）変更等作業の計画策定及びテスト実施
（５）変更等により生じる影響のアセスメント
（６）変更等の承認手順（管理者の承認は必須）
（７）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
（８）すべての関係者に対する、変更等に関する必要事項の通知
（９）変更等作業を中断等する場合の手順（必要ならば代替手順）
２　前項について、外部業者等に作業を実施させる場合も同様の管理を実施させるとともに、進捗状況等について報告させなければならない。

（オペレーションシステム変更時のレビュー：A14.2.3）
第７条　オペレーションシステム（以下、「ＯＳ」という。）を変更するときは、情報システムの運用またはセキュリティに影響がないように確認しなければならない。
２　前項の確認手順は、第６条の手順に準じて管理しなければならない。

（パッケージソフトウェアの変更：A14.2.4）
第８条　パッケージソフトウェアを導入する場合は、原則として変更（カスタマイズ）を加えずに導入、使用しなければならない。
２　パッケージソフトウェアを変更して使用しようとする場合は、以下の点について考慮しなければならない。
（１）処理の完全性や、セキュリティ面が損なわれるリスク
（２）パッケージソフトウェアの供給元（以下、「ベンダー」という。）の同意
（３）ベンダーからの継続的なサポートの有無
３　パッケージソフトウェアを変更して使用しようとするときは、第６条の手順に準じて管理しなければならない。

第４章　開発・導入の作業

（開発環境と本番環境の分離：A12.1.4）
第９条　セキュリティ管理者は、システム開発（またはテスト）環境とシステム本番環境を分離しなければならない。
２　セキュリティ管理者は、システム開発及びテスト環境からシステム本番環境への移行について、システム開発計画の策定時に手順を明確にしなければならない。
３　セキュリティ管理者は、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。

（システム試験データの保護：A14.3.1）
第１０条　情報システム・ＯＳ等の導入または変更時に使用する試験データは、厳重に管理しなければならない。
２　やむを得ず本番データを試験目的で使用する場合は、以下の手順を実施しなければならない。
（１）本番データを複写し、試験に使用することについて、データを所管するセキュリティ管

理者に許可を受けること
（２）本番システムと同様のアクセス制御手順で管理すること
（３）試験が完了した後、本番データは速やかに消去すること
（４）本番データの複製及び利用のログを取得すること

【０７】システム運用・保守に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、情報システムの運用・保守に関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

第２章　運用・保守管理

（操作手順書：A12.1.1）
第３条　情報システムの操作手順は文書化し、維持しなければならない。
２　操作手順書は必要とするすべての利用者に対して利用可能としなければならない。

（保守記録：A11.2.4、A6.1.2）
第４条　システムの保守に関する記録は、文書化し、保存しなければならない。
２　システム保守契約を締結した業者は、保守に関する報告書を定期的に提出しなければならない。
３　セキュリティ管理者は、保守に関する記録を定期的に確認しなければならない。
４　意図しない変更または誤用を防止するために、作業、確認、承認の職務を分割しなければならない。

（システム文書のセキュリティ）
第５条　情報システム関連の文書・記録等（以下、「システム文書」という。）は、当該業務のセキュリティ管理者が責任をもって保管しなければならない。
２　システム文書へのアクセスは、最小限度に抑えなければならない。

第３章　装置のセキュリティ

（装置の設置及び保護：A11.2.1）
第６条　システム装置は、環境上の脅威及び災害からのリスク並びに許可されていないアクセスが発生しないように配慮して、設置又は保護しなければならない。
２　システム装置は、原則としてセキュリティ区画に設置しなければならない。また、設置にあたっては、システム装置の盗難・持ち去りを防ぐ手立てを講じるとともに、設置場所、設置方向等を考慮し、覗き見・許可されていないアクセスを防がなければならない。

（サポートユーティリティー：A11.2.2）
第７条　システム稼働中に発生した停電により致命的な障害を受ける可能性のあるシステム装置に対しては、無停電電源装置（UPS）を設置しなければならない。

２　長時間にわたる停電の場合に処理の継続が要求されるシステム装置に対しては、自家発電装置を設置しなければならない。
３　システム装置からの発熱により、安定稼動が損なわれる可能性があるシステム装置に対しては、空調設備を設置しなければならない。
４　これらのサポートユーティリティーに対しては、適切な保守契約を締結し、定期的に点検を実施しなければならない。
５　セキュリティ管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。

（装置の保守：A11.2.4）
第８条　システム装置はその機能を維持するため、適切な保守を実施しなければならない。
２　装置の保守にあたっては、以下に留意しなければならない。
（１）装置は、供給者の推奨する保守間隔及び仕様にしたがって保守すること
（２）許可された保守要員だけが作業を行うこと
（３）保守についての記録を保管すること
３　保守を外部委託するときは、前項の内容および必要なセキュリティ要求事項を仕様に含めなければならない。

第４章　オペレーティングシステム管理

（ログオン手順：A9.4.2）
第９条　オペレーティングシステム（以下、「ＯＳ」という。）へのアクセスは、セキュリティに配慮したログオン手順によって制御しなければならない。
２　ログオン手順においては、不正アクセスの参考となるような情報を表示もしくは示唆することのないよう配慮しなければならない。
３　セキュリティ管理者は、取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用しなければならない。

（利用者の識別及び認証：A9.4.2）
第１０条　情報システムへのアクセスを行おうとする利用者は、各個人に付与された利用者ＩＤを使用しなければならない。
２　業務上やむを得ず共有ＩＤを使用する場合は、所属のセキュリティ管理者および配備管理者の承認を得なければならない。

（パスワード管理システム：A9.4.3）
第１１条　パスワードの管理システムは、以下の事項を考慮しなければならない。
（１）セキュリティ強度の低いパスワードは使用できないようにする。
（２）パスワード入力時に、画面に表示しないようにする。
（３）定期的にパスワードの変更を要求する。

（システムユーティリティー：A9.4.4）
第１２条　セキュリティ管理者は、システム及び業務用ソフトウエアによる制御を無効にするようなユーティリティプログラムの使用を制限しなければならない。
２　やむを得ず使用するときは、システム変更手順に従い許可を得るとともに、要求事項に沿った作業を行わなければならない。

（セッションのタイムアウト：A9.4.2）

第１３条　一定の使用中断時間が経過したときは、原則として使用が中断しているセッションを遮断しなければならない。

（接続時間の制限：A9.4.2）

第１４条　取扱いに慎重を要する業務用ソフトウエアに対しては、接続時間を限定し、やむを得ない場合を除き、接続時間を通常の就業時間内に制限しなければならない。

第５章　システムのセキュリティ機能

（マルウェア：A12.2.1）

第１５条　コンピュータウイルス等の不正プログラム（以下、「マルウェア」という。）から情報システムを保護するために、マルウェア対策ソフトウエアを導入し、動作保障の範囲において最新状態に保たなければならない。

２　インターネット経由で受信するファイルは、インターネットのゲートウェイにおいてマルウェアチェックを行い、システムへの侵入を防止しなければならない。

３　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マルウェアチェックを行い、外部への拡散を防止しなければならない。

４　情報セキュリティ事務局はマルウェア情報を収集し、必要に応じて職員等に注意喚起しなければならない。

５　セキュリティ管理者は所管するサーバ及びパソコン等の端末に、マルウェア対策ソフトウエアを常駐させなければならない。

６　ネットワークに接続していないシステムにおいて、記録媒体を使う場合は、マルウェア感染を防止するために、市が管理している媒体以外を使用してはならない。

７　ネットワークに接続していないシステムに導入したマルウェア対策ソフトウエアは市が管理している媒体を用いて最新の状態に保たなければならない。

※ゲートウェイ（Gateway）とはネットワーク間の接続を中継する機器またはソフトウエアのことであり、ここではインターネットと庁内ネットワークを接続している中継機器等のこと

（モバイルコード：A12.2.1）

第１６条　情報システムが許可されていない動作を防止するため、原則としてモバイルコードの利用を行ってはならない。

２　業務上、モバイルコードの利用が必要不可欠な場合は、セキュリティ管理者の許可を得るとともに、分離した環境での実施などの対策を行わなければならない。

※モバイルコード（mobile code）とは、ユーザーが意識することなく、自動的にダウンロードして実行されるプログラムのこと

（ログの取得：A12.4.1、A12.4.2、A12.4.3）

第１７条　セキュリティ管理者は、セキュリティに関する事案を検知するため、利用者の活動、例外処理及びセキュリティ事象を記録した監査ログ、システムの管理者及び担当者の作業ログ等の記録（以下、「ログ」という。）を取得しなければならない。

２　ログには、次の事項を含めなければならない。

（１）利用者

（２）主要な事象の日時及び内容

（３）データ等へのアクセスの成功及び失敗した記録

（４）アクセスされたファイル及びアクセスの種類
（５）システム構成の変更
（６）特権の利用
（７）システムが発した警報やエラー
３　将来の調査及びアクセス制御の監視を補うために必要なログは、３ヶ月以上保持しなければならない。ただし、法令等によって保持期間が別途定められている場合は、その期間とする。
４　ログは、以下のような許可されていない変更及び運用上の問題から保護されていなければならない。
（１）ログの変更または削除
（２）容量不足等に起因する意図しないログの上書き、またはシステム停止
５　セキュリティ管理者は、不正アクセス、不正プログラム等の調査のために、ログを随時調査できる。調査できる対象には職員等が使用しているパソコンおよび端末等の利用状況、記録媒体のアクセス記録、電子メールの送受信記録、インターネット利用状況、プリンタへの出力状況等を含み、これらを本人の同意なく調査することができる。

（障害のログ取得：A12.4.1）
第１８条　セキュリティ管理者は、情報システムに関連する障害が発生した場合は、可能ならばログを取得し、確認のうえ、適切な処置をとらねばならない。

（外部委託事業者の監視とレビュー：A15.2.1）
第１９条　セキュリティ管理者は、外部委託事業者が提供するサービス、報告及び記録を定期的にレビューしなければならない。
２　レビューの結果、必要な場合は契約に基づく措置を行わなければならない。

（技術的遵守点検：A12.1.3、A12.4.1、A18.2.3）
第２０条　セキュリティ管理者は、所管の情報システムに関し作業報告書および侵入検知報告書、技術的脆弱性報告書等により技術的遵守点検を、定期的に行わなければならない。
２　セキュリティ管理者は、前項の点検において以下の項目について確認しなければならない。
（１）許可されているアクセスの状況
（２）許可されていないアクセスの状況
（３）システムの警告又は不具合
３　セキュリティ管理者は、要求されるシステム性能を満たすため、資源の利用状況を監視・調整し、また、将来必要とする容量・能力を予測しなければならない。

（暗号の利用方針：A10.1.1）
第２１条　暗号を使用するときは、十分な強度を持った暗号を使用しなければならない。
２　情報システム課長は予め定めた暗号化方法の中から、または必要に応じて新たに利用可能な暗号化方式を定め、用途に応じて強度及び品質等を考慮した推奨暗号方式を指定することができる。

（暗号鍵管理：A10.1.1）
第２２条　安全に暗号技術を利用するため、管理者は適切な暗号鍵の管理を行わなければならない。
２　暗号鍵の保管、変更、更新、無効化については、セキュリティ管理者がこれを実施する。
３　暗号鍵の管理について、記録を残さなければならない。

（情報漏洩リスクの抑止）
第２３条　隠れチャネル等による情報漏洩を抑止するため、システムの利用状況について定期的

に確認しなければならない。

（技術的脆弱性の管理：A12.6.1）

第２４条　利用中の情報システムの技術的脆弱性に関する情報を速やかに入手するとともに、適切な手段で対処しなければならない。

２　セキュリティパッチが公開された際は、リスクと既存業務への影響を検討したうえで、適用を検討しなければならない。

３　セキュリティ管理者は技術的脆弱性の対策記録を管理しなければならない。

【０８】ネットワークに関する基準

第１章　総則

（趣旨）

第１条　この基準は、西宮市情報セキュリティ方針に基づき、ネットワークの利用・管理に関し必要な事項を定めるものとする。

（対象者）

第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

第２章　ネットワーク利用方針

（ネットワーク利用方針： A9.1.2）

第３条　庁内において許可されるネットワーク利用は、原則として情報管理部が運用する庁内ネットワーク基盤（以下、「ネット基盤」という。）のみとする。

２　前項以外のネットワーク構築、ネットワークサービス等（以下、「独自ネットワーク」という。）の利用を行おうとするときは、情報システム課長の許可を得なければならない。

３　ネットワーク管理者は、ネット基盤においては情報システム課長、独自ネットワークにおいては当該業務の所管課長とする。

４　独自ネットワークをネット基盤に接続しようとするとき、及び独自ネットワーク同士を接続しようとするときは、情報システム課長の許可を得なければならない。また、独自ネットワークのネットワーク管理者は、ネット基盤との境界に、責任分解点としてファイアウォール等のネットワーク装置を設置しなければならない。

５　ネット基盤における各種サービスは、原則として住民情報を扱う情報システムにおいては行政系の住民情報（ＪＪ）系、LGWAN に接続する情報システムにおいては LGWAN 系を利用し、その他の情報システムは行政系の職員ネット系を利用し NAIS-NET に集約することを検討しなければならない。

６　住民情報（ＪＪ）系及び LGWAN 系は、他のネットワークとこれを分離しなければならない。

７　メールやデータを LGWAN 系に取り込む場合は、無害化措置を図らなければならない。

８　情報システム課長は、NAIS-NET を利用できる職員、サービス内容を適切に制御する手段を講じなければならない。

（ネットワークの管理：A13.1.1、A13.1.2）

第４条　ネットワーク管理者は、ネットワーク利用に関し、適切なログを取得するとともに、監視を行わなければならない。

２　ネットワーク管理者は、ネットワークサービス仕様作成時にネットワークセキュリティについての要求事項を設定し、定期的に実施状況を確認しなければならない。

３　ネットワーク管理者は、職員等及び外部委託事業者、その他の利用者が使用しているパソコン等からの庁内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。

４　ネットワーク管理者は、ネットワーク監視システムからのアラートを監視し、事故の兆候をできるだけ速く察知するよう努めなければならない。

５　ネットワーク管理者は、１年に１度以上ネットワーク機器等の性能評価を行い、性能上の問題の発見に努めなければならない。

6　ネットワーク管理者は、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等のセキュリティ管理者に通知し、適切な処置を求めなければならない。
7　ネットワーク管理者は、緊急時にはネットワーク機器等の構成情報をすぐに取り出せるように保管しなければならない。
8　ネットワーク管理者は、IP アドレス等のネットワーク構成情報等を、関係者以外に公表してはならない。

（ケーブル配線のセキュリティ：A11.2.3）
第５条　ネットワーク管理者は、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　ネットワーク管理者は、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　ネットワーク管理者は、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切に管理しなければならない。
4　ネットワーク管理者は、自ら又はセキュリティ担当者及び契約により操作を認められた外部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施さなければならない。

（ネットワーク装置の管理：A11.2.1）
第６条　ネットワーク管理者は、庁内の通信ケーブル及びネットワーク装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信ケーブル及びネットワーク装置に関連する文書を適切に保管しなければならない。
2　ネットワーク管理者は、新たな情報資産をネットワークに接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。
3　ネットワーク管理者は、ネットワークに使用する通信ケーブル及びネットワーク装置について、伝送途上に情報が破壊、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。

（外部から接続する利用者の認証：A13.1.1）
第７条　職員等は、外部公開している装置を除き、原則として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してはならない。
2　業務上やむを得ない理由で、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必要が生じた場合は、ネットワーク管理者、当該情報システムを所管するセキュリティ管理者の許可を得なければならない。
3　ネットワーク管理者は、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、合理的理由を有する必要最小限の者に限定し、管理しなければならない。
4　ネットワーク管理者は、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するとともに、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。また、使用する端末について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。

（ネットワークにおける装置の識別：A13.1.1）
第８条　ネットワーク管理者は、ネットワーク上で使用される機器について、機器固有情報（ＭＡＣアドレス、ＩＰアドレス、電子証明書等）によってパソコンとネットワークとの接続の可否が自動的に識別される等の方法により、許可しない機器の不正接続を防止する措置を考慮しなければならない。

（遠隔診断用及び環境設定用ポートの保護：A13.1.1）
第９条　ネットワーク管理者およびサーバ等のセキュリティ管理者は、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しなければならない。

（ネットワークの領域分割：A13.1.3）
第１０条　ネットワーク管理者は、情報サービス、利用者及び情報システムのセキュリティ水準に応じて、物理的または論理的にネットワークを分割し、境界にはファイアウォールやルータ等を設置し、適切にネットワークの領域を分割管理しなければならない。

（外部ネットワークとの接続制限等：A13.1.3）
第１１条　ネットワーク管理者は、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、情報システム課長の許可を得なければならない。
２　ネットワーク管理者は、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、庁内のすべてのネットワーク、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　ネットワーク管理者は、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損害賠償責任を契約上担保しなければならない。
４　ネットワーク管理者は、サーバ等を外部に公開する場合、庁内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うえで接続しなければならない。
５　ネットワーク管理者は、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、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。
６　実施機関の異なる情報システムで個人情報を扱うものを接続する場合は、西宮市個人情報保護条例第１６条の規定に従わなければならない。

（ネットワークの接続制御：A13.1.3）
第１２条　ネットワーク管理者は、ネットワークに接続された機器が、許可されたネットワークサービス、情報資産及び情報システムにのみ接続されるように、物理的及び論理的管理を行わなければならない。

（ネットワークのルーティング制御：A13.1.3）
第１３条　ネットワーク管理者は、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、ルータ等の設定を管理しなければならない。
２　ネットワーク管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（無線 LAN 及びネットワークの盗聴対策：A13.2.1）
第１４条　無線 LAN を新たに導入しようとする場合は情報システム課長の許可を得なければならない。
２　情報システム課長は、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づけなければならない。
３　ネットワーク管理者は、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（他団体との情報システムに関する情報等の交換：A13.2.2）
第１５条　ネットワーク管理者は、他の団体と情報資産を交換する仕組みを構築する場合には、その取扱いに関する事項をあらかじめ定め、ＩＳＭＳ統括責任者の許可を得なければならない。

（電子メールのセキュリティ管理：A13.2.3）
第１６条　電子メールシステムを運用している情報システムのセキュリティ管理者は、権限のない利用者により、電子メールの中継処理（踏み台としての利用）が行われないように、サーバの設定を行わなければならない。
２　電子メールシステムを運用している情報システムのセキュリティ管理者は、大量のスパムメール等の受信又は送信を検知した場合は、電子メールサーバの運用を停止する等の適切な処理を講じなければならない。
３　電子メールシステムを運用している情報システムのセキュリティ管理者は、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。
４　電子メールシステムを運用している情報システムのセキュリティ管理者は、外部委託事業者の作業員の電子メール利用について、委託先との間で利用アドレス等を取り決めなければならない。
５　電子メールシステムを運用している情報システムのセキュリティ管理者は、職員等が電子メールを外部に送信することにより、情報資産が無断で持ち出されることに対して追跡調査が可能なように、メールおよび操作ログの保存等の措置を講じなければならない。

（公開情報：A14.1.2）
第１７条　ウェブサーバ・外部サービス等を利用してホームページ等（以下、「ホームページ等」という。）を構築し情報公開を行おうとする場合は、適切な手段でソフトウェア、データ等を保護しなければならない。
２　ホームページ等を新規に公開しようとする際は、情報企画課長の承認を受けなければならない。

（クロックの同期：A12.4.4）
第１８条　ネット基盤上で運用する情報システムのために、ネットワーク管理者は時刻同期のための機器を用意しなければならない。
２　ネットワーク管理者は重要なアクセス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。

（モバイル機器：A6.2.1）
第１９条　セキュリティ区画外に持ち出し可能な端末等（以下、「モバイル機器」という。）は、通常以上のセキュリティ対策が必要であることを考慮し、使用にあたっての手順を定めなければならない。
２　モバイル機器からのネットワークへの接続は、識別及び認証が正しくなされ、かつ適切なアクセス制御がなされている場合以外は、実行できないようにしなければならない。

（テレワーキング：A6.2.2）
第２０条　ＩＳＭＳ統括責任者の許可なく、テレワーキング活動を実施してはならない。
２　前項の許可を得てテレワーキングを実施する場合、ＩＳＭＳ統括責任者はセキュリティ要求仕様を踏まえた、適切な管理手順を定め、順守させなければならない。

第３章　オンラインサービス

（オンラインサービス検討時の考慮事項：A14.1.2）
第２１条　セキュリティ管理者は電子申請・電子入札等のインターネット上で提供するサービス（以下、「オンラインサービス」という。）を実施しようとするときは、以下の事項について考

慮した管理策を実施しなければならない。
（１）本人認証の必要性、レベル
（２）申請時における、重要性に応じた機密性、完全性及び発送・受領の証明と、契約の否認防止に関する要求事項
（３）申請に関する各種データ、処理状況等に関する機密性、完全性の確保
（４）不正、エラー時の対処方法

（オンラインサービスのセキュリティ：A14.1.2、A14.1.3）
第２２条　セキュリティ管理者はオンラインサービスのためのセキュリティには、次の事項について検討し、必要に応じて実施しなければならない。
（１）電子署名の利用
（２）通信経路の暗号化
（３）データ保管環境の安全性

【０９】アクセス権限管理に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、情報資産に対するアクセス権限管理に関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

第２章　アクセス制御方針

（アクセス制御方針： A6.1.5、A9.2.6、A9.1.1、A9.4.1）
第３条　正当な職務権限に基づいてアクセス許可を受けた場合を除き、本市の情報資産にアクセスしてはならない。
２　セキュリティ管理者は、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。
３　情報資産へのアクセス権限は、当該情報資産の重要性、リスク等を考慮し、原則として業務上必要な部分・機能についてのみ、セキュリティ管理者がこれを付与する。
４　セキュリティ管理者は、職員等の異動時や契約の終了時には、アクセス権限を速やかに削除もしくは変更しなければならない。
５　プロジェクト実施者は、情報セキュリティの配慮をしなければならない。

（利用者登録：A9.2.1）
第４条　セキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者ＩＤの取扱い等の方法を定めなければならない。
２　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、セキュリティ管理者に通知しなければならない。
３　セキュリティ管理者は、利用されていないＩＤが放置されないよう、定期的に点検しなければならない。

（特権管理：A6.1.2、A9.2.3）
第５条　セキュリティ管理者は、管理者権限等の特権を付与されたＩＤ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、当該ＩＤ及びパスワードを厳重に管理しなければならない。
２　セキュリティ管理者は、特権を付与されたＩＤ及びパスワードについて、一般利用者よりも定期変更、入力回数制限等のセキュリティ機能を強化するよう考慮しなければならない。
３　セキュリティ管理者は、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するよう考慮しなければならない。
４　セキュリティ管理者は、情報資産に対する許可されていない、もしくは意図しない変更又は不正使用を避けるため、特権ＩＤと一般ＩＤは原則として分割しなければならない。これが困難な場合であっても、特権ＩＤを通常業務に使用してはならない。

（ＩＤ・パスワードの管理：A9.2.4）

第６条　セキュリティ管理者は、職員等のＩＤ・パスワードに関する情報を厳重に管理しなければならない。不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

２　個人情報等の取扱いに慎重を要する情報を取り扱うシステムは、物理認証キーを併用しなければならない。

３　セキュリティ管理者は、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、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。

４　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。

（１）認証に用いる IC カード等を、職員等間で共有してはならない。

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

（３）IC カード等を紛失した場合には、速やかにセキュリティ管理者に通報し、指示に従わなければならない。

５　セキュリティ管理者は、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。

６　セキュリティ管理者は、IC カード等を切り替えるまたは返却の場合、情報管理部が IC カード等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。

（情報処理施設の不正使用防止：A9.2.5）

第７条　セキュリティ管理者は、使用記録（ログ）を取得し、必要な期間、これを保存しなければならない。

２　セキュリティ管理者は、利用者のアクセス権を少なくとも半年に一回以上棚卸しなければならない。

第３章　不適正使用予防措置

（外部利用者のアクセス：A5.1.1）

第８条　権限を与えられた職員等以外（以下、「外部組織」という。）は、原則としてセキュリティ管理者の許可なく本市の重要性分類Ｂ以上の情報資産にアクセスしてはならない。

２　セキュリティ管理者は、外部組織から本市の情報資産へのアクセス申請があった場合には、以下の件を考慮のうえ、判断しなければならない。

（１）外部組織がアクセスする必要がある情報資産

（２）アクセスの必要性と業務における重要度

（３）アクセス制御を行うための管理策

（４）利用施設、利用機器、利用ネットワーク等の特定

（５）情報資産を取り扱う外部組織の要員

（６）法的要求事項及び契約上の義務

３　利用が許可された外部利用者は、法的要求事項、情報セキュリティポリシーおよび配備管理者が定める手順、指示等に従わなければならず、従わない場合には配備管理者およびセキュリティ管理者はアクセス権限の停止、失効を命じることができる。

（取扱いに慎重を要するシステムの隔離：A9.4.1）

第９条　取扱いに慎重を要するシステムを共有環境で実行する場合は、資源を共有する業務用ソフトウェアを識別して、それぞれのセキュリティ管理者の合意を得なければならない。

（プログラムソースコードへのアクセス制御：A9.4.5）

第１０条　プログラムソースコード（以下、「プログラム」という。）へのアクセスは、制限されたものとして管理しなければならない。
２　プログラムは、管理者の承認を受け、手順にしたがって管理しなければならない。

【１０】情報セキュリティ事件・事故に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、情報セキュリティに関する事件・事故及び弱点を速やかに把握し、必要な対処及び是正処置をとることに関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

（情報セキュリティ事件・事故の識別）
第３条　情報セキュリティ事件・事故（以下、「セキュリティ事故」という。）とは、情報システム及び関連機器・ネットワーク等の不具合・異常動作・故障・誤操作・不正使用・ウイルス等の感染・不法な攻撃・盗難等、あるいは紙媒体の紛失・盗難・誤廃棄・誤交付等に起因し、業務継続やサービス提供、セキュリティ確保に支障が生じる事態又はそのおそれがある事態をさす。

（セキュリティ事故対応の基本方針）
第４条　セキュリティ事故対応の基本方針は次の通りとする。
（１）セキュリティの確保（セキュリティが損なわれた場合においては被害の拡大防止）
（２）業務・サービスの継続（業務・サービスが停止した場合においては速やかな復旧）

（セキュリティ事故レベル決定基準：A16.1.2）
第５条　セキュリティ事故レベルの決定基準は「情報セキュリティ事件・事故(システム障害・情報漏洩等)対策マニュアル」の「２．危機管理の組織と体制」のとおりとする。

第２章　セキュリティ事故の報告

（セキュリティ事故の報告：A16.1.2）
第６条　職員等は、セキュリティ事故と思われる事象を発見した場合、「情報セキュリティ事件・事故(システム障害・情報漏洩等)対策マニュアル」の「４．応急対策（危機が発生した場合等の対策）」に従って情報セキュリティ事務局及びセキュリティ管理者に報告しなければならない。

（セキュリティ事故の報告書式等：A16.1.2）
第７条　連絡を受けたセキュリティ管理者は「情報セキュリティ事件・事故(システム障害・情報漏洩等)対策マニュアル」の「４．応急対策（危機が発生した場合等の対策）」に従って報告書の速報を作成し速やかに情報セキュリティ事務局に報告しなければならない。

第３章　セキュリティ事故の管理及び改善

（危機管理体制：A16.1.1）

第８条　セキュリティ事故が発生した場合の、危機管理体制は「情報セキュリティ事件・事故(システム障害・情報漏洩等)対策マニュアル」の「２．危機管理の組織と体制」のとおりとする。

（関係当局との連絡：A6.1.3）

第９条　セキュリティ事故が発生もしくは疑われる場合にセキュリティ管理者もしくは情報セキュリティ事務局は、「情報セキュリティ事件・事故(システム障害・情報漏洩等)対策マニュアル」の「４．応急対策（危機が発生した場合等の対策)」に従って、必要な報告を関係当局に実施しなければならない。

２　事象毎に連絡を要する関係当局の例を下記に示す。

（１）サイバーテロ等犯罪性が疑われる場合　兵庫県警サイバーテロ対策室

（２）マルウェア感染の場合　IPA（独立行政法人情報処理推進機構）セキュリティセンター

（３）業務関連システムに関する事故の場合　各システムの監督官庁、機関

（セキュリティ事故報告書：A16.1.2、A16.1.6）

第１０条　当該セキュリティ事故を所管するセキュリティ管理者は「情報セキュリティ事件・事故(システム障害・情報漏洩等)対策マニュアル」の「５．事後対策（復旧・復興及び再発防止対策)」に従って報告書の顛末を作成しセキュリティ事務局に提出しなければならない。

２　報告書等によるセキュリティ事故の公開は「情報セキュリティ事件・事故(システム障害・情報漏洩等)対策マニュアル」の「４．応急対策（危機が発生した場合等の対策)」のとおりとする。

【１１】業務継続管理に関する基準

第１章　総則

（趣旨）

第１条　この基準は、西宮市情報セキュリティ方針に基づき、危機的状況における事業活動の中断に対処するとともに、危機における重要な業務手続を保護するための業務継続計画に関し必要な事項を定めるものとする。

（対象者）

第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

（業務継続管理手続：A17.1.1）

第３条　ＣＩＳＯは、組織全体を通じた業務継続計画を審査、承認し、業務継続計画に必要な経営資源を提供しなければならない。

２　情報セキュリティ委員会及び同推進部会は、業務継続計画の実施と維持に必要な調整及び取り纏めを行わなければならない。

３　セキュリティ管理者は、業務継続計画の手順を文書化するとともに、定期的に試験し、更新し、維持しなければならない。

（業務継続のためのリスク分析：A17.1.1）

第４条　情報セキュリティ事務局は、業務継続に影響を及ぼしうる事象、発生確率、影響、事業中断が情報セキュテリィに及ぼす結果等のリスクを特定しなければならない。その上で、重要な資源、中断の影響、受容可能な停止時間及び回復の優先順位を織り込んだリスク分析を行わなければならない。

２　前項のリスク分析結果を踏まえ、セキュリティ管理者は業務継続戦略を策定し、ＣＩＳＯの承認を受けなければならない。

（業務継続計画の策定：A16.1.1、A17.1.1）

第５条　セキュリティ管理者は、業務継続戦略に基づいて所管事務における業務継続計画を策定、管理しなければならない。

２　業務継続計画の策定にあたっては、以下の点を考慮なければならない。

（１）すべての責任及び業務継続手順の特定

（２）受容可能な情報の損失及びサービスの停止の特定

（３）業務の運用並びに情報の可用性の回復及び復旧を、要求された時間内で可能にする手順

（４）損傷を受けたプロセスが回復もしくは復旧するまでの、損傷を受けなかったプロセスにおける運用手順

（業務継続計画策定の枠組み）

第６条　業務継続計画には、以下の事項を記載しなければならない。

（１）業務継続計画の対象となる業務手続およびシステム

（２）重大な障害又は災害の事業に及ぼす脅威の明確化及びリスク分析

（３）重大な障害又は災害による影響を許容可能なレベルに抑えるための管理方法

（４）緊急事態に対応するための体制、連絡先

（業務継続計画の試験、維持及び再評価：A17.1.3）

第７条　セキュリティ管理者は、業務継続計画が最新で効果的なものであることを確実にするために、定期的に試験を行い、更新しなければならない。

２　試験の結果は記録し、必要な場合は業務継続計画の改善を行わなければならない。

３　以下のような変更があった場合は、業務継続計画の再検討を行わなければならない。

（１）運用システムの変更

（２）要員・組織の変更

（３）契約相手、関係者、その他連絡先の変更

（４）所在地、施設、装置等の変更

（５）法的要求事項の変更

（６）業務内容、手続等の変更

（７）リスク内容の変化

（業務継続計画の試験：A17.1.3）

第８条　業務継続計画が最新で効果的なものであることを確実にするために、年に一回以上、試験しなければならない。

２　業務継続計画の試験は、以下の方法等について計画する。

（１）具体的な障害例に対する机上試験。

（２）事件・事故が発生した場合の連絡体制及び要員の役割についての模擬訓練。

（３）バックアップ等から復旧できることを技術的に確認する試験。

３　業務継続計画は、計画の有効性を維持するために、定期的に見直し及び更新を行う。

（１）業務継続計画の試験において問題が発生した場合、見直しを行う。

（２）定期的な見直しには環境条件の変化及び、いまだ事業計画に反映されていない新たな情報システムや設備・施設の重要性の識別を含めるものとする。

（３）見直しの内容は、情報セキュリティ委員会に報告する。

（４）情報セキュリティ推進部会は、問題の確認及び業務継続計画の見直し内容について評価する。

（５）見直し内容の評価に基づき、業務継続計画を更新し、維持する。

【１２】セキュリティ監査に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、セキュリティ監査・レビュー等に関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

第２章　セキュリティ内部監査

（情報セキュリティ監査委員会：A18.2.1）
第３条　ＣＩＳＯは、本市のすべてのネットワーク及び情報システムの監査業務（以下、「内部監査」という。）を統括するため、情報セキュリティ監査委員会を設置する。
２　情報セキュリティ監査委員会は、委員長及び委員、監査従事者をもって組織する。
３　委員長は、総務総括室長をもって充てる。
４　委員長は、監査業務を統括し、情報セキュリティ監査委員会を代表する。
５　委員長に事故があるとき、又は委員長が欠けたときは、委員の互選により、その職務を代理する者を決める。
６　委員は、委員長が情報セキュリティ推進部会員のなかから指名する。
７　情報セキュリティ監査委員会は、内部監査を実施する場合は、職員のなかから監査従事者を指名する。ただし、監査従事者は被監査部門から独立していなければならない。
８　監査従事者は、内部監査業務に従事し、その結果を情報セキュリティ監査委員会に報告しなければならない。

（内部監査の実施方法：A12.7.1）
第４条　情報セキュリティ監査委員会は、毎年内部監査を実施しなければならない。
２　情報セキュリティ監査委員会は、内部監査を行うに当たって、監査実施計画を立案し、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　情報セキュリティ監査委員会は、内部監査によって次の事項を判断しなければならない。
（１）法令・規則・セキュリティポリシーへの適合性
（２）特定された情報セキュリティポリシーへの適合性
（３）有効に実施され、維持されているか
（４）期待したように実施されているか
４　被監査部門は、内部監査の実施に協力しなければならない。

（システム監査資料等の保護：A9.4.4）
第５条　内部監査で使用する調査票や各種資料等については、誤用又は悪用を防止するため、情報セキュリティ事務局が一般の職員等がアクセスできないように管理しなければならない。

（内部監査報告書の提出：A12.7.1）
第６条　情報セキュリティ監査委員会は、内部監査結果を取りまとめ、ＣＩＳＯに報告しなけれ

ばならない。

（監査結果への対応：A16.1.6）

第７条　ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管するセキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していないセキュリティ管理者に対しても、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。

【１３】情報セキュリティ改善に関する基準

第１章　総則

（趣旨）
第１条　この基準は、西宮市情報セキュリティ方針に基づき、情報セキュリティの不備等の改善を行うことに関し必要な事項を定めるものとする。

（対象者）
第２条　この基準は、本市の情報資産を取り扱う全職員及び全ての関係者（以下、「職員等」という。）に適用する。

（継続的改善）
第３条　すべての関係者は、リスク分析、監査結果、監視した事情の分析、情報セキュリティ事件・事故、関係者からの通報、マネジメントレビュー等を利用して、情報セキュリティの改善に努めなければならない。

（セキュリティポリシー遵守状況の確認：A18.2.2）
第４条　セキュリティ管理者は、管理している情報システムについて、日々のポリシー遵守状況を定期的に確認しなければならない。
２　確認の結果、何らかの非遵守を発見した場合は、管理者はその原因を特定するとともに、再発防止のための処置をとらなければならない。

（是正計画の作成及び承認：A16.1.6、A18.2.2）
第５条　セキュリティ管理者は、下記に該当する場合は情報セキュリティ是正計画（以下、「是正計画」という。）を作成し、情報セキュリティ事務局に提出しなければならない。ただし、情報セキュリティ事務局が不要と判断した場合はこの限りではない。
（１）リスク分析の結果、リスク値が「大きい」と判定されリスク対応を行う場合
（２）情報セキュリティ監査で不適合の指摘を受けた場合
（３）レベル２以上の情報セキュリティ事件・事故が発生した場合
（４）セキュリティポリシー非順守を発見し、計画的に再発防止策を実施する場合
（５）計画的に情報セキュリティ改善（予防措置含む）に取り組む必要があると判断した場合
（６）その他、情報セキュリティ事務局より是正計画作成の指示を受けた場合
２　情報セキュリティ事務局は、提出された是正計画に不備等がある場合は、是正計画の修正を指示することができる。この場合、セキュリティ管理者は是正計画の修正指示に速やかに対応しなければならない。
３　情報セキュリティ事務局は、提出された是正計画についてＣＩＳＯの判断を要すると判断した場合は、セキュリティ推進部会、セキュリティ委員会の議題として提出しなければならない。

（是正計画の記載事項：A16.1.1、A16.1.6）
第６条　是正計画には、以下の内容を記載しなければならない。
（１）是正計画の内容
（２）是正計画の担当者名およびセキュリティ管理者名
（２）必要な費用
（３）実施予定時期

２　セキュリティ管理者は、同時に複数の是正計画を作成する場合は、その重要度、必要な資源等を勘案して、優先順位をつけなければならない。
３　是正計画の完了までに時間がかかる場合は、セキュリティ管理者は暫定措置を実施し、完了までの期間、リスクの低減に努めなければならない。

（是正計画の進捗確認：A16.1.1、A16.1.6）
第７条　セキュリティ管理者は、是正計画に沿って情報セキュリティの改善を実施しなければならない。
２　セキュリティ管理者は、継続中の是正計画の進捗状況について、４半期ごとに情報セキュリティ事務局に報告しなければならない。

（是正計画の完了確認：A16.1.1、A16.1.6、A18.2.2）
第８条　セキュリティ管理者は、是正計画が完了したときは速やかに情報セキュリティ事務局に報告し、確認を受けなければならない。

（マネジメントレビューでの報告：A16.1.1、A16.1.6）
第９条　セキュリティ事務局は、是正計画の進捗状況について、マネジメントレビューで報告しなければならない。