| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| **第1編　基本編**<br>**第1.5部　情報システムに対する基本的な対策**<br>**1.5.1　情報システムのセキュリティ要件**<br>**1.5.1.1　情報システムのセキュリティ要件**<br>**(1)　情報システムの計画** | | | | | | | | |
| 1.5.1.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、情報システムを統括する責任者に求めること。 | **○設計・開発時における情報システムのセキュリティ維持の体制**<br>・情報システムを統括する責任者（情報化統括責任者（CIO）等を想定）が、当該情報システムの設計・開発について、セキュリティの検討及び維持の側面から実施可能な体制（人員、機材、予算等）を確保する。 | **○運用・保守時における情報システムのセキュリティ維持の体制**<br>・情報システムを統括する責任者（情報化統括責任者（CIO）等を想定）が、当該情報システムの運用・保守について、セキュリティの検討及び維持の側面から実施可能な体制（人員、機材、予算等）を確保する。 | （該当せず） | | | |
| 1.5.1.1(1)(b) | 基本 | 情報システムセキュリティ責任者は、情報システムのセキュリティ要件を決定すること。 | **○情報システムのセキュリティ要件の決定**<br>・情報システムに求められる要求事項のうち、セキュリティに関わる要求事項について検討し、その中で必要と判断する要求事項を当該情報システムのセキュリティ要件として決定する。決定したセキュリティ要件は、システム要件定義書や仕様書などの形式で明確化し、実装等の際に確実に考慮されるようにする。 | （該当せず） | （該当せず） | | | |
| 1.5.1.1(1)(c) | 基本 | 情報システムセキュリティ責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。 | **○情報システムのセキュリティ要件を満たす為の構成要素についての対策**<br>・定めた情報システムのセキュリティ要件（1.5.1.1(1)(b)を参照のこと）を満たすために、設計・開発段階（機器等の購入や、機能の設定等を含む）において必要な対策を定める。具体的には、省庁対策基準における情報システムに関わる遵守事項について、該当するもの該当しないものを判断した上で、該当するもののうち設計・開発段階で実施するものを明確化する（本点検リストの活用等による）。セキュリティ要件を満たすために、前記の遵守事項以外の対策が必要な場合には、その対策も含めて定める必要がある。 | **○情報システムのセキュリティ要件を満たす為の構成要素についての対策**<br>・定めた情報システムのセキュリティ要件（1.5.1.1(1)(b)を参照のこと）を満たすために、運用・保守段階において必要な対策を定める。具体的には、省庁対策基準における情報システムに関わる遵守事項について、該当するもの該当しないものを判断した上で、該当するもののうち運用・保守段階で実施するものを明確化する（本点検リストの活用等による）。セキュリティ要件を満たすために、前記の遵守事項以外の対策が必要な場合には、その対策も含めて定める必要がある。 | （該当せず） | | | |
| 1.5.1.1(1)(d) | 基本 | 情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST評価・ST確認を受けること。ただし、情報システムを更改し、又は構築中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。 | **○重要なセキュリティ要件がある場合のST評価・ST確認**<br>・重要なセキュリティ要件がある情報システムについて、セキュリティ機能が確実に実装されることを目的として、第三者機関により、ISO/IEC 15408に基づいたセキュリティ設計仕様書のST評価・ST確認を受ける。 | （該当せず） | （該当せず） | | | |
| 1.5.1.1(1)(e) | 基本 | 情報システムセキュリティ責任者は、情報システムについて、情報セキュリティの侵害又はそのおそれのある事象の発生を監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定めること。 | **○情報セキュリティの侵害又はおそれのある事象の発生を監視する必要性の判断と、監視のための機能の導入等**<br>・情報システム及び取り扱う情報等を考慮して、情報システムの各所において監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定める。監視の対象としては、府省庁の外部から通信回線を通してなされる不正アクセス、不正侵入、情報システムの管理者・運用者又は利用者の誤操作又は不正操作、サーバ装置等機器の動作、及び、許可されていない者の安全区域への立ち入り等が考えられる。監視のために必要な措置としては、(1)必要な監視機能の導入、(2)運用時における監視の体制の確立・手順書の策定、(3)監視対象となりうる職員等への説明、がある。 | （該当せず） | （該当せず） | | | |
| 1.5.1.1(1)(f) | 基本 | 情報システムセキュリティ責任者は、構築した情報システムを運用段階へ導入するに当たって、情報セキュリティの観点から実施する導入のための手順及び環境を定めること。 | **○情報システムを導入する際の手順及び環境**<br>・セキュリティの観点での試験の実施により、当該情報システムがセキュリティ要件を満たすことを確認すると共に、運用段階への導入に際して、その方法、体制、作業手順、スケジュール、期間、教育やトラブル対処についてセキュリティの観点から手順書等を整備する。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 1.5.1.1(1)(g) | 強化 | 情報システムセキュリティ責任者は、構築する情報システムの構成要素については、重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合であって、その中に当該セキュリティ機能に関してITセキュリティ評価及び認証制度に基づく認証を取得している製品がある場合には、当該製品を情報システムの構成要素として選択すること。 | **○重要なセキュリティ要件がある場合のITセキュリティ評価及び認証制度による評価**<br>・セキュリティ機能の実現において重要とみなされる機器等の購入において（認証提供製品や、ファイアウォール等のネットワークセキュリティ製品等）、要求する機能を有する製品に選択肢がある場合、IS0/IEC 15408に基づくITセキュリティ評価及び認証制度による認証を取得しているものを優先的に選択する。 | （該当せず） | （該当せず） | | | |
| **(2) 情報システムの構築・運用** | | | | | | | | |
| 1.5.1.1(2)(a) | 基本 | 情報システムセキュリティ責任者は、情報システムの構築、運用に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行うこと。 | **○情報システムの構築に際してのセキュリティ対策の実施**<br>・情報システムのセキュリティ要件に基づいて定めた設計・開発時の対策（1.5.1.1(1)(c)を参照のこと）及び監視のための措置（1.5.1.1(1)(e)を参照のこと）に従って、設計・開発において必要な対策を実施する。 | **○情報システムの運用・監視に際してのセキュリティ対策の実施**<br>・情報システムのセキュリティ要件に基づいて定めた運用・保守時の対策（1.5.1(1)(c)を参照のこと）及び監視のための措置（1.5.1.1(1)(e)を参照のこと）に従って、運用・保守において必要な対策を実施する。 | （該当せず） | | | |
| **(3) 情報システムの移行・廃棄** | | | | | | | | |
| 1.5.1.1(3)(a) | 基本 | 情報システムセキュリティ責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を講ずること。 | （該当せず） | **○情報システムの移行及び廃棄時の適切な措置**<br>・情報システムの移行及び廃棄を行う場合に、情報システムを構成する機器の扱い、情報の格付け等を考慮して、機器及び情報に関して廃棄、保存、消去等の適切な措置を講ずる。 | （該当せず） | | （該当せず） | （該当せず） |
| **(4) 情報システムの見直し** | | | | | | | | |
| 1.5.1.1(4)(a) | 基本 | 情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。 | （該当せず） | **○情報システムのセキュリティ対策の見直し**<br>・情報システムのセキュリティ対策について、必要に応じて見直しとそれに必要な措置を行う。見直しを行う時期は、新たなセキュリティ脅威の出現や、運用・監視等の状況により判断する。 | （該当せず） | | （該当せず） | （該当せず） |
| **1.5.2 情報システムに係る規定の整備と遵守**<br>**1.5.2.1 情報システムに係る文書及び台帳整備**<br>**(1) 情報システムの文書整備** | | | | | | | | |
| 1.5.2.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、所管する情報システムについて以下の事項を記載した文書を整備すること。<br>（ア）当該情報システムを構成する電子計算機関連事項<br>・電子計算機を管理する行政事務従事者及び利用者を特定する情報<br>・電子計算機の機種並びに利用しているソフトウェアの種類及びバージョン<br>・電子計算機の仕様書又は設計書<br>（イ）当該情報システムを構成する通信回線及び通信回線装置関連事項<br>・通信回線及び通信回線装置を管理する行政事務従事者を特定する情報<br>・通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン<br>・通信回線及び通信回線装置の仕様書又は設計書<br>・通信回線の構成<br>・通信回線装置におけるアクセス制御の設定<br>・通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応<br>・通信回線の利用部署<br>（ウ）情報システムの構成要素のセキュリティ維持に関する手順<br>・電子計算機のセキュリティ維持に関する手順<br>・通信回線を介して提供するサービスのセキュリティ維持に関する手順<br>・通信回線及び通信回線装置のセキュリティ維持に関する手順<br>（エ）障害・事故等が発生した際の対処手順 | **○情報システムの文書整備**<br>・所管する情報システムにおいて、適切な情報セキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うため、情報システムの管理に必要な情報として遵守事項の（ア）から（エ）の内容について把握し、文書として整備する。文書の整備にあたっては、維持管理が容易になるように適切な単位で整備することが望ましい。また、文書は書面ではなく電磁的記録媒体として整備してもよい。<br>所管する情報システムに変更があった場合、また想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しを行う。 | **○情報システムの文書の更新**<br>・所管する情報システムに変更があった場合、また想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しを行う。 | （該当せず） | | | |
| 1.5.2.1(1)(b) | 基本 | 情報システムセキュリティ管理者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理において情報セキュリティ対策を行うこと。 | （該当せず） | **○情報システムの文書に基づく運用管理**<br>・所管する情報システムの運用管理において、整備した情報システムの文書に基づき、適切な情報セキュリティ対策を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| **(2) 情報システムの台帳整備** | | | | | | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 1.5.2.1(2)(a) | 基本 | 統括情報セキュリティ責任者は、すべての情報システムに対して、当該情報システムに係る以下の事項を記載した台帳を整備すること。<br>（ア）情報システム名、管理課室及び管理責任者の氏名・連絡先<br>（イ）システム構成<br>（ウ）接続する府省庁外通信回線の種別<br>（エ）取り扱う情報の格付け及び取扱制限に関する事項<br>（オ）当該情報システムの設計・開発、運用、保守に関する事項 | （該当せず） | （該当せず） | **組織内セキュリティ管理の確認** | | （該当せず） | （該当せず） |
| 1.5.2.1(2)(b) | 基本 | 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システムの台帳の記載事項について統括情報セキュリティ責任者に報告すること。 | （該当せず） | **○情報システム台帳の記載事項に関する報告**<br>・情報システム係る台帳に記載の事項について統括情報セキュリティ責任者に報告する。 | **組織内セキュリティ管理の確認** | | （該当せず） | （該当せず） |
| **1.5.2.2 機器等の購入**<br>**(1) 機器等の購入に係る規定の整備** | | | | | | | | |
| 1.5.2.2(1)(a) | 基本 | 統括情報セキュリティ責任者は、機器等の選定基準を整備すること。 | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |
| 1.5.2.2(1)(b) | 基本 | 統括情報セキュリティ責任者は、機器等の購入において、セキュリティ機能の要求仕様があり、総合評価落札方式により購入を行う際には、ITセキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用することを選定基準として定めること。 | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |
| 1.5.2.2(1)(c) | 基本 | 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。 | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |
| **(2) 機器等の購入に係る規定の運守** | | | | | | | | |
| 1.5.2.2(2)(a) | 基本 | 情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の候補の選定における判断の一要素として活用すること。 | **○機器等の選定時の適合性確認**<br>・府省庁で整備されている選定基準に従って、機器等に必要なセキュリティ機能が実装されていること等を確認し、これを機器等の選定における判断の一要素として利用する。 | （該当せず） | （該当せず） | | | |
| 1.5.2.2(2)(b) | 基本 | 情報システムセキュリティ責任者は、機器等の納入時において、定められた確認・検査手続に従って、納品検査を実施すること。 | **○納品検査の実施**<br>・確認・検査手続に従って、納入された機器等が定められた選定基準を満たすことを確認し、その結果を納入検査における確認の判断に加える。具体的な確認・検査の方法として、必要なセキュリティ機能の実装状況（機器等に最新のパッチが適用されているかどうか、アンチウイルスソフトウェア等が最新の脆弱性に対応しているかどうか等にも留意）及び機器等に不正プログラムが混入していないことを、購入先からの報告で確認すること等がある。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| **1.5.2.3 ソフトウェア開発**<br>**(1) ソフトウェア開発に係る規定の整備** | | | | | | | | |
| 1.5.2.3(1)(a) | 基本 | 統括情報セキュリティ責任者は、ソフトウェア開発について、セキュリティに係る以下の対策事項を情報システムセキュリティ責任者に求めるための規定を整備すること。<br>(ア) 情報システムセキュリティ責任者は、セキュリティに係る対策事項（本項(ウ)から(セ)の遵守事項）を満たすことが可能な開発体制を確保すること。<br>(イ) 情報システムセキュリティ責任者は、ソフトウェア開発を外部委託する場合には、セキュリティに係る対策事項（本項(ウ)から(セ)の遵守事項）の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。<br>(ウ) 情報システムセキュリティ責任者は、ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。<br>(エ) 情報システムセキュリティ責任者は、ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムと分離する必要性の有無を検討し、必要と認めたときは分離すること。<br>(オ) 情報システムセキュリティ責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付け及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。<br>(カ) 情報システムセキュリティ責任者は、開発するソフトウェアが運用される際に利用されるセキュリティ機能についての管理機能の必要性の有無を検討し、必要と認めたときは、管理機能を適切に設計し、設計書に明確に記述すること。<br>(キ) 情報システムセキュリティ責任者は、ソフトウェアの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。<br>(ク) 情報システムセキュリティ責任者は、開発するソフトウェアにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要と認めたときは、その<br>(ケ) 情報システムセキュリティ責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST評価・ST 確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書のST 評価・ST 確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。<br>(コ) 情報システムセキュリティ責任者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスから保護するとともに、バックアップを取得すること。<br>(サ) 情報システムセキュリティ責任者は、情報セキュリティの観点からコーディングに関する規定を整備すること。<br>(シ) 情報システムセキュリティ責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの必要性の有無を検討し、必要と認めたときは、ソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。<br>(ス) 情報システムセキュリティ責任者は、セキュリティの観点から実施する試験の必要性の有無を検討し、必要と認めたときは実施する試験項目及び試験方法を定め、これに基づいて試験を実施すること。<br>(セ) 情報システムセキュリティ責任者は、情報セキュリティの観点から | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |
| **(2) ソフトウェア開発に係る規定の遵守** | | | | | | | | |
| 1.5.2.3(2)(a) | 基本 | 情報システムセキュリティ責任者は、ソフトウェア開発に係る規定に基づいて、ソフトウェアの開発を行うこと。 | **○ソフトウェア開発規定の遵守**<br>・府省庁で整備されたソフトウェア開発に係る規定を遵守して、ソフトウェア開発を行う。 | （該当せず） | （該当せず） | | | |
| **1.5.2.4 暗号と電子署名の標準手順**<br>**(1) 暗号と電子署名に係る規定の整備** | | | | | | | | |
| 1.5.2.4(1)(a) | 基本 | 統括情報セキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズム及び方法を、以下の事項を含めて定めること。<br>（ア）電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。<br>（イ）情報システムの新規構築又は更新に伴い暗号化又は電子署名を導入する場合には、電子政府推奨暗号リストに記載されたアルゴリズムを使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。 | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 1.5.2.4(1)(b) | 基本 | 統括情報セキュリティ責任者は、暗号化された情報（書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の（ア）及び（イ）の手順（以下「鍵の管理手順等」という。）を定めること。<br>（ア）鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等<br>（イ）鍵の保存手順 | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |
| 1.5.2.4(1)(c) | 強化 | 統括情報セキュリティ責任者は、暗号化された情報の復号に用いる鍵のバックアップの取得手順又は鍵の預託手順（以下「鍵のバックアップ手順等」という。）を定めること。 | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |
| **(2) 暗号化及び電子署名に係る管理** | | | | | | | | |
| 1.5.2.4(2)(a) | 基本 | 行政事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 1.5.2.4(2)(b) | 基本 | 行政事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順に従い、これを適切に管理すること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 1.5.2.4(2)(c) | 強化 | 行政事務従事者は、暗号化された情報の復号に用いる鍵について、定められた鍵のバックアップ手順等に従い、そのバックアップを取得すること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| **1.5.2.5 府省庁外の情報セキュリティ水準の低下を招く行為の防止**<br>**(1) 措置についての規定の整備** | | | | | | | | |
| 1.5.2.5(1)(a) | 基本 | 統括情報セキュリティ責任者は、府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備すること。 | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| **(2) 規定の遵守** | | | | | | | | |
| 1.5.2.5(2)(a) | 基本 | 行政事務従事者は、府省庁外の情報セキュリティ水準の低下を招く行為の防止の規定に基づいて、必要な措置を講ずること。 | **○府省庁外の情報セキュリティ水準の低下を招く行為の防止に対する情報システム構築時の対策**<br>・広く国民等に対してサービスを提供する情報システムの構築において、利用者である国民等の端末等に対して情報セキュリティ水準の低下を招くような行為を明示的又は暗黙的に求めないように配慮する。<br>具体的には、国民がサービスを利用する際に、その利用端末等において、（ア）不適切なソフトウェア（構築時点でセキュリティホールのあるソフトウェアや、そのバージョン）の使用を求めてはならず、（イ）主にセキュリティ対策の観点から実施されているソフトウェアの設定を無効化するような不適切な設定を要求してはならず、（ウ）セキュリティ対策のために導入されているソフトウェアの削除又は無効化を求めてはならない。<br>情報システムの構築においては、上記の禁止事項に配慮して、利用するソフトウェアの選定及び推奨設定の定めを行う必要がある。また、上記の事項は、情報システムの運用期間中において、新たなセキュリティホールに関する情報等が公開されるリスクに配慮し、構築時点でより適切と判断するソフトウェア等を選定することが望ましい。 | **○府省庁外の情報セキュリティ水準の低下を招く行為の防止に対する措置**<br>・広く国民等に対してサービスを提供する情報システムの運用において、利用者である国民等の端末等に対して情報セキュリティ水準の低下を招くような行為を明示的又は暗黙的に求めないように配慮する。<br>具体的には、国民がサービスを利用する際に、その利用端末等において、（ア）不適切なソフトウェア（構築時点でセキュリティホールのあるソフトウェアや、そのバージョン）の使用を求めてはならず、（イ）主にセキュリティ対策の観点から実施されているソフトウェアの設定を無効化するような不適切な設定を要求してはならず、（ウ）セキュリティ対策のために導入されているソフトウェアの削除又は無効化を求めてはならない。<br>情報システムの運用においては、特に、構築後に公開されたセキュリティホールに関する情報や、ソフトウェアのサポート終了等に留意して、上記の禁止事項に反する状態が生じないよう、使用する又はその使用が前提となるソフトウェア（OS,ミドルウェア他）の更新・修正への対応（試験や、開発ソフトウェアの修正等）を行う必要がある。 | **利用者向け手順書への反映、若しくは利用者への周知** | | | |
| **1.5.2.6 ドメイン名の使用についての対策**<br>**(1) ドメイン名の使用についての規定の整備** | | | | | | | | |
| 1.5.2.6(1)(a) | 基本 | 統括情報セキュリティ責任者は、ドメインネームシステムによるドメイン名（以下「ドメイン名」と言う。）の使用について、以下の事項を行政事務従事者に求める規定を整備すること。<br>（ア）行政事務従事者は、府省庁外の者（国外在住の者を除く。以下、本項において同じ。）に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、以下の政府機関のドメイン名であることが保証されるドメイン名（以下「政府ドメイン名」という。）を使用すること。<br>・go.jpで終わるドメイン名<br>・日本語ドメイン名の中で行政等に関するものとして予約されたドメイン名<br>ただし、電子メール送信又は政府ドメイン名のウェブページでの掲載に限り以下の条件を満たす場合には、政府ドメイン名以外のドメイン名を府省庁以外のものとして告知してもよい。具体的には、電子メールの送信においては以下の条件をすべて満たすことが必要である。<br>・告知内容についての問い合わせ先として政府ドメイン名による電子メールアドレスを明記しているか、又は政府ドメイン名による電子署名をしていること。<br>・告知するドメイン名を管理する組織名を明記すること。<br>・告知するドメイン名の有効性を確認した時期又は有効性を保証する期間について明記していること。<br>また、政府ドメイン名のウェブページでの掲載においては以下の条件をすべて満たすことが必要である。<br>・告知するドメイン名を管理する組織名を明記すること。<br>・告知するドメイン名の有効性を確認した時期又は有効性を保証する期間について明記していること。<br>（イ）行政事務従事者は、府省庁外の者に対して、電子メールの送信元としてドメイン名を使用する場合には、政府ドメイン名を使用すること。ただし、当該府省庁外の者にとって、当該行政事務従事者が既知の者である場合を除く。<br>（ウ）行政事務従事者は、府省庁外の者に対して、アクセスさせることを | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |
| **(2) ドメイン名の使用についての規定の遵守** | | | | | | | | |
| 1.5.2.6(2)(a) | 基本 | 行政事務従事者は、ドメイン名の使用についての規定に基づいて、必要な措置を講ずること。 | **○ドメイン名の利用に対する対策**<br>・インターネットを経由して広く国民等にサービスを提供する情報システム（ウェブサーバ、電子メール、その他の情報システム）の構築において、サービスを利用する国民等が、当該サービスが実際の府省庁のものであると信頼できるための一要素として、当該情報システムが本遵守事項に照らして適切なドメイン名を使用するように設計及び設定を行う。 | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| **1.5.2.7　不正プログラム感染防止のための日常的実施事項** | | | | | | | | |
| **(1)　不正プログラム対策に係る規定の整備** | | | | | | | | |
| 1.5.2.7(1)(a) | 基本 | 統括情報セキュリティ責任者は、不正プログラム感染の回避を目的として、以下の措置を行政事務従事者に求める規定を整備すること。<br>(ア) 行政事務従事者は、アンチウイルスソフトウェア等により不正プログラムとして検知された実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。<br>(イ) 行政事務従事者は、アンチウイルスソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。<br>(ウ) 行政事務従事者は、アンチウイルスソフトウェア等による不正プログラムの自動検査機能を有効にすること。<br>(エ) 行政事務従事者は、アンチウイルスソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること。<br>(オ) 行政事務従事者は、外部からデータやソフトウェアを電子計算機等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。<br>(カ) 行政事務従事者は、不正プログラム感染の予防に努めること。<br>(キ) 行政事務従事者は、不正プログラムに感染した恐れのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講じること。 | （該当せず） | （該当せず） | **情報セキュリティ関係規程の確認** | | （該当せず） | （該当せず） |
| **(2)　不正プログラム対策に係る規定の遵守** | | | | | | | | |
| 1.5.2.7(2)(a) | 基本 | 行政事務従事者は、定められた不正プログラム対策に係る規定に基づいて、不正プログラムの感染を防止するための対策を行うこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| **第2編　情報システム編** | | | | | | | | |
| **第2.1部　情報セキュリティ要件の明確化に基づく対策** | | | | | | | | |
| **2.1.1　情報セキュリティについての機能** | | | | | | | | |
| **2.1.1.1　主体認証機能** | | | | | | | | |
| **(1)　主体認証機能の導入** | | | | | | | | |
| 2.1.1.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断すること。 | **○情報システムへの主体認証機能の必要性判断**<br>・情報システムで取り扱う情報と、当該情報にアクセスする主体（利用者、システム管理者等）を整理した上で、アクセスする主体に対して主体認証を行う必要性の有無を検討する。要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断する。<br><br>（「主体」とは、情報システムにアクセスする者や、他の情報システム及び装置等をいう。<br>「識別」とは、情報システムにアクセスする主体を特定することをいう。「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。具体的な識別コードとして、ユーザID等がある。<br>「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。具体的な主体認証情報として、パスワード等がある。<br>「要保護情報」とは、要機密情報（機密性２情報及び機密性３情報）、要保全情報（保全性２情報）及び要安定情報（可用性２情報）をいう。） | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(b) | 基本 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、識別及び主体認証を行う機能を設けること。 | **○情報システムへの識別及び主体認証機能の導入**<br>・主体認証を行う必要があると認めたシステム（2.1.1.1(1)(a)を参照のこと）について、識別及び主体認証を行う機能（主体認証機能）を設ける。<br>・主体認証の方式として、知識、所有、生体情報の３つの方法が代表的である。「知識」による主体認証は、パスワード等の本人のみが知りうる情報を提示することにより本人性を検証する方式である。「所有」による主体認証は、ICカードや磁気ストライプカード等、本人のみが所有する機器の利用により検証する方式である。「生体情報」による主体認証は、指紋や虹彩等、本人の生体的な特徴により、検証する方式である。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.1(1)(c) | 基本 | 情報システムセキュリティ管理者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。<br>（ア）主体認証情報を保存する場合には、その内容の暗号化を行うこと。<br>（イ）主体認証情報を通信する場合には、その内容の暗号化を行うこと。<br>（ウ）保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更、提供（入力）させる際に、暗号化が行われない旨を通知すること。 | **○情報システムにおける主体認証情報の秘密管理**<br>・主体認証情報の漏えいにより不正利用等の危険が発生する場合において、主体認証情報の保存時および通信時に、その内容の暗号化が行われるよう情報システムの機能を構築する。<br>・やむをえず、主体認証情報の暗号化ができない場合には、利用者が他のシステムと主体認証情報を共有しないように、その旨を利用者等に通知するよう情報システムの機能を構築する（漏えいした主体認証情報の二次利用による被害の拡散を防止するため。）。<br>・漏えい等により危険が発生する主体認証情報としては、「知識」による主体認証でのパスワードが代表的であるが、採用する主体認証の方式及び主体認証情報により、それぞれ判断すべきである。 | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(d) | 基本 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。<br>（ア）利用者が定期的に変更しているか否かを確認する機能<br>（イ）利用者が定期的に変更しなければ、情報システムの利用を継続させない機能 | **○主体認証情報の定期的変更を促す機能の導入**<br>・利用者に主体認証情報の定期的な変更を求める場合に、利用者に対して定期的な変更を促す機能に加え、その定期的な変更がなされているか否かを確認する機能、又は、定期的に変更していない場合に情報システムの利用を停止する機能、のいずれかを設ける。 | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(e) | 基本 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報又は主体認証情報格納装置を他者に使用され、又は使用される危険性を認識した場合に、直ちに当該主体認証情報若しくは主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けること。 | **○主体認証情報、主体認証情報格納装置の他者利用発生時の利用を停止する機能の導入**<br>・主体認証情報自体の露呈、主体認証情報に関連する情報の露呈又はそれらが露呈した可能性について報告を受けた場合に、主体認証の停止、識別コードによる情報システムの利用停止や主体認証情報の強制変更などの対策を講じられるよう情報システムの機能を構築する。 | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(f) | 基本 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識による主体認証方式を用いる場合には、以下の機能を設けること。<br>（ア）利用者が自らの主体認証情報を設定する機能<br>（イ）利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能 | **○本人による主体認証情報設定機能の導入**<br>・知識による主体認証方式を用いる場合に、主体認証情報の忘却の防止や、本人以外による主体認証情報のなりすましの防止のため、知識による主体認証方式の場合に、本人による主体認証情報の設定を可能とする機能を設ける。<br>・情報漏えいや不正利用の防止の観点から、情報システムの管理者であっても本人が設定した主体認証情報を知ることができないよう、暗号化等により主体認証情報が容易に知ることができないための機能を設ける。 | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(g) | 基本 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項が適用可能かどうかを検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。<br>（ア）正当な主体以外の主体認証を受諾しないこと。（誤認の防止）<br>（イ）正当な主体が本人の責任ではない理由で主体認証を拒否されないこと（誤否の防止）<br>（ウ）正当な主体が容易に他者に主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）及び貸与ができないこと。（代理の防止）<br>（エ）主体認証情報が容易に複製できないこと。（複製の防止）<br>（オ）情報システムセキュリティ管理者の判断により、ログオンを個々に無効化できる手段があること。（無効化の確保）<br>（カ）必要時に中断することなく主体認証が可能であること。（可用性の確保）<br>（キ）新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）<br>（ク）主体に付与した主体認証情報を使用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保） | **○知識、所有、生体以外の主体認証方式の満たすべき要件**<br>・代表的な方式である「知識」、「所有」、「生体情報」による主体認証方式以外の方法を用いる場合の検討事項として、本遵守事項の（ア）～（ク）の要件を検討する。セキュリティ上の求められる強度や利便性なども考慮して、方式を決定する。なお、（ア）～（ク）の要件は、必ずしもすべて充足することを求めるものではない。知識、所有、生体以外の主体認証方式として、例えば、機器や回線等に紐づけられた固有の識別子（ID）で、その識別子が容易に偽装できないものの送信（発信電話番号表示や、携帯電話の機器固有IDの通知等）による認証、位置情報による認証、RFIDによる認証等が考えられるが、その採用については本遵守事項の要件を検討した上で判断する必要がある。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.1(1)(h) | 基本 | 情報システムセキュリティ責任者は、生体情報による主体認証方式を用いる場合には、当該生体情報を本人から事前に同意を得た目的以外の目的で使用しないこと。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。 | **○生体情報による主体認証情報の取り扱い（目的外利用禁止とプライバシーへの留意）**<br>・利用者の指紋情報など、主体認証情報として生体情報を取り扱う場合に、個人のプライバシーに配慮し、個人情報として厳格な管理を求める。本人の同意を前提とせずに生体情報を主体認証以外の目的で使用することになっていないことや、生体情報を管理者以外が参照・変更等できないこと（アクセス制御の実施等）、使用する必要が無くなった生体情報を管理者が消去できること、等を確認する。 | **○生体情報による主体認証情報の取り扱い（目的外利用禁止とプライバシーへの留意）**<br>・利用者の指紋情報など、主体認証情報として生体情報を取り扱う場合に、情報システムの運用期間中において、個人のプライバシーに配慮し、個人情報として厳格な管理を行う。 | （該当せず） | | | |
| 2.1.1.1(1)(i) | 強化 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、複数要素（複合）主体認証方式を行う機能を設けること。 | **○情報システムへの複数要素の主体認証機能の導入**<br>・複数要素（複合）による主体認証方式を用いることにより、より強固な主体認証を実現する。（一つの方式における主体認証情報が万が一露呈した場合に、残りの主体認証方式が情報システムへのアクセスを保護することで、不正にログイン等される可能性を軽減する。） | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(j) | 強化 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、ログオンした利用者に対して、前回のログオンに関する情報を通知する機能を設けること。 | **○前回ログオン情報の通知機能の導入**<br>・本人の識別コードが他者によって不正に使われた場合に、本人が気づく機会が得られるよう、識別コードによる前回のログオンに関する情報（ログイン日時や、アクセスに用いた端末のIPアドレス等）を通知する機能を設ける。 | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(k) | 強化 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、不正にログオンしようとする行為を検知し、又は防止する機能を設けること。 | **○不正ログオン又は試行の検知もしくは防止機能の導入**<br>・識別コードによるログインについて、指定回数以上の主体認証情報の誤入力が検知された場合に、その旨を通知する、あるいは、当該識別コードによる情報システムへの以後のログインを無効にする（アカウントロックする）機能を設ける。 | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(l) | 強化 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能を設けること。 | **○システムログイン時の利用に関する通知メッセージの表示機能の導入**<br>・利用者がシステムにログインする前に、当該情報システムの利用に関し、次のような通知メッセージを表示する機能を設ける。（利用者が政府機関の情報システムへアクセスしようとしていること／情報システムの使用が監視、記録される場合があり、監査対象となること／情報システムの不正使用は禁止されており、刑法の罰則対象となること） | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(m) | 強化 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、以前に設定した主体認証情報と同じものを再設定することを防止する機能を設けること。 | **○以前に設定された主体認証情報の再設定の防止機能の導入**<br>・一度使用した主体認証情報（パスワードなど）の再利用を禁止する機能を設ける。 | （該当せず） | （該当せず） | | | |
| 2.1.1.1(1)(n) | 強化 | 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能を設けること。 | **○管理者権限の共有時に事前個別識別コードでログオンさせる機能の導入**<br>・管理者権限を有した識別コードを管理者グループで共用した場合に、実際に作業をした管理者を個人単位で特定する目的で、非管理者権限の識別コードを本人に付与した上、その識別コードで最初にログオンした後に限り、管理者権限を有する共用識別コードに切り替えて管理者作業を実施することを可能とするための機能を設ける。<br>・当該情報システムのオペレーションシステムがUnixの場合には、一般利用者でログオンした後にsuコマンドでrootに切り替えるという手順により、上記のことが達成可能であり、更に、rootによるログオンを禁止する設定により、その手順を強制することができる。 | （該当せず） | （該当せず） | | | |
| **(2) 識別コードの管理** | | | | | | | | |
| 2.1.1.2(a) | 基本 | 行政事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて、情報システムを利用しないこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.1(2)(b) | 基本 | 行政事務従事者は、自己に付与された識別コードを他者に主体認証に用いる目的のために付与及び貸与しないこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.1.1.1(2)(c) | 基本 | 行政事務従事者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.1.1.1(2)(d) | 基本 | 行政事務従事者は、行政事務のために識別コードを利用する必要がなくなった場合は、その旨を情報システムセキュリティ管理者に届け出ること。ただし、個別の届出が必要ないと、情報システムセキュリティ責任者が定めている場合は、この限りでない。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.1.1.1(2)(e) | 強化 | 行政事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| **(3) 主体認証情報の管理** | | | | | | | | |
| 2.1.1.1(3)(a) | 基本 | 行政事務従事者は、主体認証情報が他者に使用され、又はその危険が発生した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.1.1.1(3)(b) | 基本 | 情報システムセキュリティ責任者又は情報システムセキュリティ管理者は、主体認証情報が他者に使用され、又はその危険が発生したことの報告を受けた場合には、必要な措置を講ずること。 | （該当せず） | **○盗用の報告を受けた場合の措置**<br>・主体認証情報自体の露呈、主体認証情報に関連する情報の露呈又はそれらが露呈した可能性について報告を受けた場合に、主体認証の停止、識別コードによる情報システムの利用停止や主体認証情報の強制変更などの対策を、情報システム機能の利用を含めて、実施する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.1(3)(c) | 基本 | 行政事務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。<br>(ア)自己の主体認証情報を他者に知られないように管理すること。<br>(イ)自己の主体認証情報を他者に教えないこと。<br>(ウ)主体認証情報を忘却しないように努めること。<br>(エ)主体認証情報を設定するに際しては、容易に推測されないものにすること。<br>(オ)情報システムセキュリティ管理者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更すること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.1.1.1(3)(d) | 基本 | 行政事務従事者は、所有による主体認証を用いる場合には、以下の管理を徹底すること。<br>(ア)主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理すること。<br>(イ)主体認証情報格納装置を他者に付与及び貸与しないこと。<br>(ウ)主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。<br>(エ)主体認証情報格納装置を利用する必要がなくなった場合には、これを情報システムセキュリティ責任者又は情報システムセキュリティ管理者に返還すること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |

**2.1.1.2 アクセス制御機能**
**(1) アクセス制御機能の導入**

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.2(1)(a) | 基本 | 情報システムセキュリティ責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。 | **○情報システムへのアクセス制御機能の必要性の判断**<br>・アクセス制御を行う必要性の有無を検討する。複数の主体（利用者、システム管理者等）が情報システムを利用する場合で、主体毎にアクセス可能な情報が異なる場合には、どの主体がどの情報にアクセス可能かを定め、その定めに従って情報へのアクセスを制御するためのアクセス制御機能が必要となる。 | （該当せず） | （該当せず） | | | |
| 2.1.1.2(1)(b) | 基本 | 情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設けること。 | **○情報システムへのアクセス制御機能の導入**<br>・アクセス制御を行う必要があると認めた情報システム（2.1.1.2(1)(a)を参照のこと）について、アクセス制御を行う機能（アクセス制御機能）を設ける。 | （該当せず） | （該当せず） | | | |
| 2.1.1.2(1)(c) | 強化 | 情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、利用者及び所属するグループの属性以外に基づくアクセス制御の機能を追加すること。 | **○利用者及びグループ属性以外に基づくアクセス制御機能の追加**<br>・次のような、利用者及びグループ属性以外によるアクセス制御の必要性を検討し、必要性があれば導入する。（利用時間の上限／利用可能時間帯／同時利用者数の上限／同一ＩＤによる複数ログインの禁止／接続ＩＰアドレスの制限） | （該当せず） | （該当せず） | | | |
| 2.1.1.2(1)(d) | 強化 | 情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、強制アクセス制御機能を設けること。 | **○強制アクセス制御機能の導入**<br>・情報システムのオペレーティングシステム（OS）として、強制アクセス制御の機能を持ったトラステッドOSやセキュアOS等を採用する。 | （該当せず） | （該当せず） | | | |
| **(2) 適正なアクセス制御** | | | | | | | | |
| 2.1.1.2(2)(a) | 基本 | 情報システムセキュリティ責任者は、行政事務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付け及び取扱制限に従って、アクセス制御を行うこと。 | **○システム導入時のアクセス制御設定**<br>・情報システムに格納される情報に対して適切なアクセス制御がなされるよう、必要なアクセス制御の設定を行う。導入時においては、情報システムの運用開始前に保管される情報、及び運用時に情報システムによって自動的に追加される情報に対して、その格付けと取扱制限に従って、確実にアクセス制御がなされるよう設定する必要がある。 | **○システム運用時のアクセス制御設定**<br>・運用時においては、業務等の必要に応じて運用中に追加される情報に対して、その格付けと取扱制限に従って、確実にアクセス制御がなされるよう必要な設定を行う。 | （該当せず） | | | |
| **2.1.1.3 権限管理機能**<br>**(1) 権限管理機能の導入** | | | | | | | | |
| 2.1.1.3(1)(a) | 基本 | 情報システムセキュリティ責任者は、すべての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。 | **○情報システムへの権限管理機能の必要性の判断**<br>・権限管理を行う必要性の有無を検討する。権限管理とは、識別コード及び主体認証情報の付与管理（払い出し等）や、主体毎のアクセス許可を管理する行為をいう。特定の主体（システム管理者等）に管理者権限を付与することも含む。 | （該当せず） | （該当せず） | | | |
| 2.1.1.3(1)(b) | 基本 | 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。 | **○情報システムへの権限管理機能の導入**<br>・権限管理を行う必要があると認めたシステム（2.1.1.3(1)(a)を参照のこと）について、権限管理を行う機能（権限管理機能）を設ける。 | （該当せず） | （該当せず） | | | |
| 2.1.1.3(1)(c) | 強化 | 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、最少特権機能を設けること。 | **○情報システムの最少特権機能の導入**<br>・情報システムの権限管理において、最少特権機能を設ける必要性を検討し、必要がある場合には導入する。<br><br>（「最少特権機能」とは、管理者権限を実行できる範囲を管理作業に必要な最少の範囲に制限する機能をいう。） | （該当せず） | （該当せず） | | | |
| 2.1.1.3(1)(d) | 強化 | 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、主体認証情報の再発行を自動で行う機能を設けること。 | **○情報システムへの主体認証機能の自動再発行機能の導入**<br>・利用者が主体認証情報の再発行を求めた場合に、その再発行処理を自動化することで、システム管理者を含む他の者がその主体認証情報を知り得ないようにするための機能を導入する。新規の利用者に比べ、既存の利用者は情報システムに重要な情報を保存している可能性が高いため、更なる安全性を確保するための措置として実施する。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.3(1)(e) | 強化 | 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、デュアルロック機能を設けること。 | **○情報システムのデュアルロック機能の導入**<br>・不正操作及び誤操作を防止するため、情報システムにデュアルロック機能を設ける。デュアルロック機能により、ある行為を、少なくとも２名の者が操作しなければ行為を完遂できないようにすることが可能となる。 | （該当せず） | （該当せず） | | | |
| **(2) 識別コードと主体認証情報の付与管理** | | | | | | | | |
| 2.1.1.3(2)(a) | 基本 | 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、共用識別コードの利用許可については、情報システムごとにその必要性を判断すること。 | （該当せず） | **○情報システムにおける共有識別コードの利用許可の決定**<br>・当該情報システムにおいて、識別コードの共有を許可するかどうかを判断する。原則として、識別コードは主体毎に個別に付与されるべきであるが、情報システムの機能上の制約や利用状況を考慮して、１つの識別コードを複数の主体で共用する必要がある場合には、共用識別コードの利用を許可することを明確化する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(b) | 基本 | 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、以下の事項を含む手続を定めること。<br>(ア)主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続<br>(イ)主体認証情報の初期配布方法及び変更管理手続<br>(ウ)アクセス制御情報の設定方法及び変更管理手続 | （該当せず） | **○権限管理に関する手続の決定**<br>・情報システムへアクセスする主体（利用者、システム管理者等）に対して、識別コード及び主体認証情報を付与する際の関連手続を明確に定める。また、関連手続として、主体毎にアクセス制御情報を設定・変更するための手続を定める。具体的な手続は、2.1.1.3(2)(c)～2.1.1.3(3)(b)の遵守事項にも配慮して決める。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(c) | 基本 | 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。 | （該当せず） | **○権限管理者の任命**<br>・権限管理の手続（2.1.1.3(2)(b)を参照のこと）において、その権限管理を行う役割の者（権限管理者）を定める。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(d) | 基本 | 権限管理を行う者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を発行すること。 | （該当せず） | **○許可を得た主体への識別コードと主体認証情報の発行**<br>・情報システムを利用する許可を得た主体に対してのみ識別コードと主体認証情報を発行するため、申請時に本人を確認する方法や、配布時に確実に本人に届ける方法を定め、厳格に運用する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(e) | 基本 | 権限管理を行う者は、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。 | （該当せず） | **○共有識別コードの区別の利用者への通知**<br>・識別コードを利用者に発行する際に、その識別コードが共用識別コードかそうでないかを明確に分かるように通知することで、利用者による誤用（他人に使わせる等）を防止する。ただし、共用識別コードの利用は、その利用が許可された情報システム（2.1.1.3(2)(a)を参照のこと）に限られる。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(f) | 基本 | 権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与（発行、更新及び変更を含む。以下この項において同じ。）すること。 | （該当せず） | **○業務又は業務上の責務に即した管理者権限割り当て**<br>・管理者権限を持つ識別コードは、業務又は業務上の責務に即して最小限の者に付与する。業務上必要が無い者には、管理者権限を持つ識別コードを付与しない。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(g) | 基本 | 権限管理を行う者は、行政事務従事者が情報システムを利用する必要がなくなった場合には、当該行政事務従事者の識別コードを無効にすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不要な識別コードの有無を点検すること。 | （該当せず） | **○情報システムを利用する必要が無くなった場合の識別コードの無効化及び不要な識別コードの有無点検**<br>・本人からの届出（2.1.1.1(2)(d)を参照のこと）に基づき、異動や退職等により不要になった識別コードを無効にする。また、人事異動等の時期に照らして、定期的又は必要に応じて不要な識別コードがないか確認し、もし不要な識別コードがあった場合には、それを無効化する。 | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.3(2)(h) | 基本 | 権限管理を行う者は、行政事務従事者が情報システムを利用する必要がなくなった場合には、当該行政事務従事者に交付した主体認証情報格納装置を返還させること。 | （該当せず） | **○情報システムを利用する必要が無くなった場合の主体認証情報格納装置の返却**<br>・本人からの届出（2.1.1.1(2)(d)を参照のこと）に基づき、異動や退職等により不要になった主体認証情報格納装置（ICカードや、ワンタイムパスワード用トークン等）を回収する。また、人事異動等の時期における確認（2.1.1.3(2)(g)を参照のこと）において、不要となった主体認証情報格納装置が存在すると判断される場合には、交付した行政事務従事者からそれらを回収する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(i) | 基本 | 権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与えるようにアクセス制御の設定をすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不適切なアクセス制御設定の有無を点検すること。 | （該当せず） | **○業務上必要最小限に限定されたアクセス制御の設定及び不適切なアクセス制御設定の有無点検**<br>・情報システムにアクセスする主体（利用者、システム管理者等）に対し、業務又は業務上の責務に即して、最小限のアクセス許可を与える。また、識別コードの追加や削除時に、不適切なアクセス許可がないか確認し、不適切なアクセス許可があった場合には是正する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(j) | 強化 | 権限管理を行う者は、単一の情報システムにおいては、１人の行政事務従事者に対して単一の識別コードのみを付与すること。 | （該当せず） | **○一意の識別コードの付与**<br>・１人の行政事務従事者に対して、２つ以上の識別コードを付与しないよう権限管理を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(k) | 強化 | 権限管理を行う者は、識別コードをどの主体に付与したかについて記録すること。当該記録を消去する場合には、情報セキュリティ責任者からの事前の承認を得ること。 | （該当せず） | **○識別コードの付与記録の維持**<br>・障害・事故等の原因調査に備えて、識別コードの付与に係る記録を不用意に消去しないようにする。もし消去する必要が生じた場合には、必ず事前の承認を得る。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(2)(l) | 強化 | 権限管理を行う者は、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。 | （該当せず） | **○識別コードの再利用禁止**<br>・一度付与した識別コードを、再利用して他の主体に付与しないよう権限管理を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| **(3) 識別コードと主体認証情報における代替手段等の適用** | | | | | | | | |
| 2.1.1.3(3)(a) | 基本 | 情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった行政事務従事者から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。 | （該当せず） | **○識別コードと主体認証情報における代替手段の提供**<br>・利用者が何らかの理由で識別コードや主体認証情報が使えなくなった場合に備え、代替手段及び代替手段を提供する手続きを用意する。使えなくなる場合には、パスワードの忘却や、主体認証格納装置の携帯忘れ、指紋認証の際の指の怪我等が考えられる。また、代替手段としては、当日限り有効な暫定識別コードの提供や代替PCの貸与等が考えられる。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.3(3)(b) | 基本 | 情報システムセキュリティ責任者及び情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、識別コードの不正使用の報告を受けた場合には、直ちに当該識別コードによる使用を停止させること。 | （該当せず） | **○不正使用の報告を受けた際の識別コードの停止**<br>・識別コードの不正使用の報告を受けた際には、直ちに当該識別コードの使用を停止する措置を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.1.1.4 証跡管理機能**<br>**(1) 証跡管理機能の導入** | | | | | | | | |
| 2.1.1.4(1)(a) | 基本 | 情報システムセキュリティ責任者は、すべての情報システムについて、証跡管理を行う必要性の有無を検討すること。 | **○情報システムへの証跡管理機能の必要性の判断**<br>・証跡（ログ）を取得して管理する必要性の有無について検討する。証跡（ログ）の取得及び管理は、情報システムの動作及びその他必要な事象を記録することで、当該情報システムの管理の実効性を高めると共に、もし情報セキュリティに関する問題が発生した場合に、事後にこれを調査することを可能とする。<br>・具体的には次のような記録を取得することを検討する。（利用者によるログイン・ログオフ及び操作／管理者・運用者によるログイン・ログオフ及び操作／プログラムの動作／ファイアウォール・侵入検知システム等の通信回線装置上の通信記録） | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.4(1)(b) | 基本 | 情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。 | **○情報システムへの証跡管理機能の導入**<br>・2.1.1.4(1)(a)で証跡管理を行う必要があると認めたシステムについて、証跡管理を行う機能（証跡管理機能）を設ける。 | （該当せず） | （該当せず） | | | |
| 2.1.1.4(1)(c) | 基本 | 情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡として取得する情報項目及び証跡の保存期間を定めること。 | **○証跡に記録する事象毎の情報項目の選択**<br>・証跡（ログ）に含める情報項目として、次のようなものを検討する。（行為者又は発生元の機器の識別コード等／事象の種別／対象となった情報やプログラム／日付・時刻／成功・失敗の区別／通信パケットのヘッダ／電子メールのヘッダ）<br>・情報セキュリティに関する問題を事後に調査するという目的にも照らして、証跡の保存期間を定める。 | （該当せず） | （該当せず） | | | |
| 2.1.1.4(1)(d) | 基本 | 情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。 | **○証跡が取得できない場合の対処方法の決定、及び、必要な対処機能の導入**<br>・証跡を保存する情報システムのデータ領域において用意したファイル容量を使い切った場合等の証跡が取得できない場合の対処方法を定め、その対処を行うために機能の導入が必要であれば、それらを検討して導入する。具体的な対処方法としては、用意したファイル容量を使い切った場合に証跡の取得を中止する、古い証跡に上書きすることで取得を継続する、ファイル容量を使い切る前に管理者等に通知する、等が考えられる。 | （該当せず） | （該当せず） | | | |
| 2.1.1.4(1)(e) | 基本 | 情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。 | **○証跡の消去・改ざん・不正アクセスからの保護**<br>・証跡が不当に消去、改ざん、漏えいすることがないよう適切な格付け及び取扱制限を定め、それに従ってアクセス制御が行われるよう設定を行う。具体的なアクセス制御の機能および設定については、「2.1.1.2　アクセス制御機能」項の遵守事項も考慮する。 | （該当せず） | （該当せず） | | | |
| 2.1.1.4(1)(f) | 強化 | 情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。 | **○情報システムへの証跡の点検、分析、報告支援の自動化機能の導入**<br>・大量にある証跡情報の点検、分析、及び報告の作業を効率化するため、証跡の内容をソフトウェア等により集積し、時系列表示し、報告書を作成するなどの自動化機能を検討して導入する。なお、規模の大きい情報システムにおいては、複数の装置で取得した証跡を集積して管理するためのシステムの必要性の有無も合わせて検討し、必要があれば導入する。 | （該当せず） | （該当せず） | | | |
| 2.1.1.4(1)(g) | 強化 | 情報システムセキュリティ責任者は、取得した証跡の内容により、情報セキュリティの侵害の可能性を示す事象を検知した場合に、監視する者等にその旨を即時に通知する機能を情報システムに設けること。 | **○セキュリティ侵害を示す事象を検知した際の監視要員への通知機能の導入**<br>・府省庁外からの不正侵入の可能性、府省庁における持ち込みPCの情報システムへの接続など、監視する者等へ通知すべき事象を定め、これらの事象を通知する機能を情報システムに設置する。 | （該当せず） | （該当せず） | | | |
| **(2)　証跡の取得と保存** | | | | | | | | |
| 2.1.1.4(2)(a) | 基本 | 情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、情報システムセキュリティ責任者が情報システムに設けた機能を利用して、証跡を記録すること。 | （該当せず） | **○情報システム機能を利用した証跡の記録**<br>・証跡（ログ）を取得及び管理するため、情報システムに設けられた証跡管理機能(2.1.1.4(1)(b)を参照のこと）を用いて、予め定めた情報項目（2.1.1.4(1)(c)を参照のこと）を証跡として取得するために必要な設定を行い、当該機能を継続的に動作させる。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.1.4(2)(b) | 基本 | 情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。 | （該当せず） | **○証跡の保存期間満了時までの保存**<br>・定めた保存期間に従って、証跡（ログ）の保存及び、保存期間が完了した際の消去を行う。 | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.4(2)(c) | 基本 | 情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処方法に基づいて対処すること。 | （該当せず） | **○証跡を取得できない場合の対処**<br>・証跡を取得できない場合の対処方法に従って、必要な操作を行う。例えば、用意したファイル容量の残りが少ないことを通知された場合に、証跡ファイルを外部電磁的記録媒体に移し変えてファイル容量を開放する操作を行う等。 | （該当せず） | | （該当せず） | （該当せず） |
| **(3) 取得した証跡の点検、分析及び報告** | | | | | | | | |
| 2.1.1.4(3)(a) | 強化 | 情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又は情報セキュリティ責任者に報告すること。 | （該当せず） | **○証跡の検査と必要なセキュリティ対策の実施**<br>・取得した証跡を用いて、定期的に又は何らかの兆候を契機に点検及び分析を行い、その結果に応じて必要な情報セキュリティ対策を講じ、又は情報セキュリティ責任者に報告する。 | （該当せず） | | （該当せず） | （該当せず） |
| **(4) 証跡管理に関する利用者への周知** | | | | | | | | |
| 2.1.1.4(4)(a) | 基本 | 情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、情報システムセキュリティ管理者及び利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。 | （該当せず） | **○証跡の取得、保存、点検及び分析を行う可能性があることのあらかじめの説明**<br>・利用者等に対するプライバシーへの配慮、および不正利用の防止の観点から、利用者及び情報システムセキュリティ管理者に対し、情報システムの利用や操作等について証跡を取得、保存、点検及び分析する可能性があることを、あらかじめ説明しておく。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.1.1.5 保証のための機能**<br>**(1) 保証のための機能の導入** | | | | | | | | |
| 2.1.1.5(1)(a) | 基本 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについて、保証のための対策を行う必要性の有無を検討すること。 | **○情報システムへの保証機能の必要性の判断**<br>・要保護情報を扱う情報システムについて、2.1.1.1～2.1.1.4で示した遵守事項に限らない情報及び情報システムの安全性をより確実にするための機能として、保証のための機能を導入する必要性の有無を検討する。保証のための機能としては、（ア）2.1.1.1～2.1.1.4の機能とは異なる観点で保護を高める機能、（イ）2.1.1.1～2.1.1.4の機能及び前記（ア）の機能が適正に動作していることを確認するための機能、の２種類がある。具体的には、例えば（ア）は、データの機密性保護のために情報を分解して分散保管する機能や、完全性保護のためにタイムスタンプの処理を施す機能、（イ）は、証跡管理機能が正常に働いているかどうかを監視し、異常が検知された場合に警報を鳴らす機能、が考えられる。 | （該当せず） | （該当せず） | | | |
| 2.1.1.5(1)(b) | 基本 | 情報システムセキュリティ責任者は、保証のための対策を行う必要があると認めた情報システムにおいて、保証のための機能を設けること。 | **○情報システムへの保証機能の導入**<br>・保証のための対策を行う必要があると認めた情報システム（2.1.1.5(1)(a)を参照のこと）について、保証のための機能（保証機能）を設ける。 | （該当せず） | （該当せず） | | | |
| **2.1.1.6 暗号と電子署名**<br>**(1) 暗号化機能及び電子署名機能の導入** | | | | | | | | |
| 2.1.1.6(1)(a) | 基本 | 情報システムセキュリティ責任者は、要機密情報（書面を除く。以下この項において同じ。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。 | **○情報システムにおける暗号化の必要性の検討**<br>・情報システムで取り扱う要機密情報について、その保存や通信といった取り扱い方法に照らして、情報（データ、ファイル、電子メール等）の暗号化や、情報を送受信する通信の暗号化を行う必要性の有無を検討する。 | （該当せず） | （該当せず） | | | |
| 2.1.1.6(1)(b) | 基本 | 情報システムセキュリティ責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。 | **○情報システムにおける暗号化機能の導入**<br>・暗号化を行う必要があると認めたシステム（2.1.1.6(1)(a)を参照のこと）について、暗号化を行う機能（暗号化機能）を設ける。本機能における暗号化のためのアルゴリズム及び方法について、府省庁における定めがある場合は、それに準拠する(1.5.2.4(1)(a)を参照のこと)。また、暗号化のための鍵の管理手順等、鍵のバックアップ手順等の定めがある場合には、それを考慮した暗号化機能を設ける(1.5.2.4(1)(b)～(c)を参照のこと）。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.6(1)(c) | 基本 | 情報システムセキュリティ責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与及び検証を行う機能を付加する必要性の有無を検討すること。 | **○情報システムにおける電子署名の必要性の検討**<br>・情報システムについて、取り扱う情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与及び検証を行う機能の必要性の有無を検討する。 | （該当せず） | （該当せず） | | | |
| 2.1.1.6(1)(d) | 基本 | 情報システムセキュリティ責任者は、電子署名の付与又は検証を行う必要があると認めた情報システムには、電子署名の付与又は検証を行う機能を設けること。 | **○情報システムにおける電子署名機能の導入**<br>・電子署名の付与又は検証を行う必要があると認めた情報システム（2.1.1.6(1)(c)を参照のこと）について、電子署名を付与又は検証する機能（電子署名機能）を設ける。本機能における電子署名のアルゴリズム及び方法について、府省庁における定めがある場合は、それに準拠する(1.5.2.4(1)(a)を参照のこと)。また、電子署名付与のための鍵の管理手順等、鍵のバックアップ手順等の定めがある場合には、それを考慮した電子署名機能を設ける(1.5.2.4(1)(b)～(c)を参照のこと）。 | （該当せず） | （該当せず） | | | |
| 2.1.1.6(1)(e) | 強化 | 情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。 | **○暗号モジュールを交換可能なコンポーネントとして構成**<br>・暗号化又は電子署名付与又は検証のために選択したアルゴリズムが危殆化した場合（暗号の安全性が確保されない状態）を想定し、機能の中で暗号モジュールが交換可能なコンポーネントとなるように、暗号化又は電子署名付与又は検証のための機能を設計する。そのためには、暗号モジュールのアプリケーションインタフェースを統一しておく等の配慮が必要となる。 | （該当せず） | （該当せず） | | | |
| 2.1.1.6(1)(f) | 強化 | 情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、複数のアルゴリズムを選択可能とすること。 | **○複数のアルゴリズムを選択可能な構成**<br>・暗号化又は電子署名付与又は検証のために選択したアルゴリズムが危殆化した場合（暗号の安全性が確保されない状態）を想定し、当該アルゴリズムを他のアルゴリズムへ直ちに変更できる機能等を、情報システムに設ける。予め、別個のアルゴリズムを利用する暗号モジュールを複数導入しておき、設定により、それらの選択・変更を可能とする方法が考えられる。 | （該当せず） | （該当せず） | | | |
| 2.1.1.6(1)(g) | 強化 | 情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択すること。 | **○認証を取得している暗号利用製品の選択**<br>・ISO/IEC 19790に基づく暗号モジュール試験及び認証制度による認証を取得している製品を選択する。日本国内においては、独立行政法人情報処理推進機構（IPA）により運用されている暗号モジュール試験及び認証制度（JCMVP: Japan Cryptographic Module Validation Program）が利用可能である。 | （該当せず） | （該当せず） | | | |
| 2.1.1.6(1)(h) | 強化 | 情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵を、第三者による物理的な攻撃から保護するために、耐タンパー性を有する暗号モジュールへ格納すること。 | **○耐タンパー性を有する暗号モジュールへの鍵の格納**<br>・暗号化及び電子署名付与に用いる鍵について、電磁的記録媒体が盗難される等の物理的な手段によっても鍵情報が外部に漏えいしないよう、セキュリティ的に強固な電磁的記録媒体（ICカード等）に格納する。 | （該当せず） | （該当せず） | | | |
| **(2) 暗号化及び電子署名に係る管理** | | | | | | | | |
| 2.1.1.6(2)(a) | 基本 | 情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムにおいて、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供すること。 | （該当せず） | **○署名検証者への電子署名の正当性を検証する為の情報又は手段の提供**<br>・電子署名が付与された情報の受け取り者に対し、当該電子署名が正当であることを検証するための情報又は手段を提供する。具体的には、電子署名を付与する際に使用した署名鍵に対応する検証鍵を、情報の受け取り者に提供する必要があるが、更に、その検証鍵自体の真正性を保証するために、信頼できる機関による電子証明書の発行や、窓口による検証鍵の直接提供、検証鍵に付随する固有の情報（フィンガープリント等）を公開する等の措置を合わせて行う必要もある。<br>（検証鍵の真正性が担保されず、例えば偽装された検証鍵が提供された場合には、なりすましによる電子署名を、本人によるものと誤って認識してしまう恐れがあるため。） | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.1.6(2)(b) | 強化 | 情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。 | （該当せず） | **○アルゴリズムの危殆化に関する情報の入手**<br>・暗号化又は電子署名のために選択したアルゴリズムについて、CRYPTREC等の様々な機関から提供される情報を適宜入手し、アルゴリズムの危殆化（暗号の安全性が確保されない状態）に備える。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.1.2 情報セキュリティについての脅威** | | | | | | | | |
| **2.1.2.1 セキュリティホール対策** | | | | | | | | |
| **(1) 情報システムの構築時** | | | | | | | | |
| 2.1.2.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、電子計算機及び通信回線装置（公開されたセキュリティホールの情報がない電子計算機及び通信回線装置を除く。以下この項において同じ。）の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。 | **○電子計算機及び通信回線装置の公開されたセキュリティホールへの対応**<br>・情報システムを構成する電子計算機及び通信回線装置について、情報システムの導入時点までに公開されたセキュリティホールへの対策を検討し、実施する。 | （該当せず） | （該当せず） | | | |
| 2.1.2.1(1)(b) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、セキュリティホール対策中にサービス提供が中断しないように、電子計算機及び通信回線装置を冗長構成にすること。 | **○要安定情報システムにおける電子計算機及び通信回線装置の冗長構成**<br>・情報システムが、そのサービス提供を中断できない場合において、セキュリティホール対策を実施する際にサービスが中断しないよう、電子計算機及び通信回線装置を冗長構成にする。この場合、一方の電子計算機又は通信回線装置のセキュリティホール対策を実施する場合で、それに伴い、サービスが中断する可能性が有る場合には、冗長化された他方の電子計算機又は通信回線装置によりサービス提供が継続できるように情報システムを構成する。 | （該当せず） | （該当せず） | | | |
| 2.1.2.1(1)(c) | 強化 | 情報システムセキュリティ責任者は、公開されたセキュリティホールの情報がない段階においても電子計算機及び通信回線装置上で採り得る対策を実施すること。 | **○公開されたセキュリティホール情報がない場合の電子計算機及び通信回線装置への対策機能の導入**<br>・公開されたセキュリティホールへの対策に加え、明らかになっていないセキュリティホールについても何らかの対策が可能となる措置を実施する。具体的には、特定のメモリ上の実行権限を削除する措置、又は、バッファオーバーフローの発生検知を行い、検知時にアプリケーションの実行を停止等させる機能の導入が考えられる。 | （該当せず） | （該当せず） | | | |
| **(2) 情報システムの運用時** | | | | | | | | |
| 2.1.2.1(2)(a) | 基本 | 情報システムセキュリティ管理者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、公開されたセキュリティホールに関連する情報を適宜入手すること。 | （該当せず） | **○電子計算機及び通信回線装置のセキュリティ情報の適宜入手**<br>・当該電子計算機又は通信回線装置を販売・提供等する事業者又は組織、並びに、セキュリティホールに関連する情報を継続的に提供する組織等から、セキュリティホールに関連する情報や、セキュリティパッチのリリース情報、ソフトウェアの更新情報等を適宜収集する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.2.1(2)(b) | 基本 | 情報システムセキュリティ責任者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、セキュリティホールに関連する情報を入手した場合には、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を作成すること。<br>(ア)対策の必要性<br>(イ)対策方法<br>(ウ)対策方法が存在しない場合の一時的な回避方法<br>(エ)対策方法又は回避方法が情報システムに与える影響<br>(オ)対策の実施予定<br>(カ)対策試験の必要性<br>(キ)対策試験の方法<br>(ク)対策試験の実施予定 | （該当せず） | **○セキュリティホール情報に基づく対策計画の策定**<br>・セキュリティホールに関連する情報等（2.1.2.1(2)(a)を参照のこと）を入手した場合に、対策の必要性を検討した上で、対策方法等を含めたセキュリティホール対策計画を策定する。実施予定の対策方法が情報システムの機能や安定性に支障を及ぼす恐れが高い場合や、要安定情報を扱う情報システムの場合には、対策試験（予備システム等を用いた対策の事前確認試験）の実施を含めた慎重なセキュリティホール対策計画が求められる。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.2.1(2)(c) | 基本 | 情報システムセキュリティ管理者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。 | （該当せず） | **○セキュリティホール対策計画に基づく対策の実施**<br>・セキュリティホール対策計画（2.1.2.1(2)(b)を参照のこと）に基づき、セキュリティホール対策を実施する。 | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.2.1(2)(d) | 基本 | 情報システムセキュリティ管理者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者を含む事項を記録すること。 | （該当せず） | **○セキュリティホール対策の実施結果の記録**<br>・セキュリティホール対策の実施の記録として、実施日、実施内容、実施者、並びに、その他の必要事項を記載する。予め、情報システムについて、セキュリティホール対策の実施を記録する記録簿の様式を定めておくことが望ましい。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.2.1(2)(e) | 基本 | 情報システムセキュリティ管理者は、信頼できる方法でパッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイル（以下、「対策用ファイル」という。）を入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。 | （該当せず） | **○信頼できる対策用ファイルの入手と完全性検証**<br>・対策用ファイルとして提供された情報について、第三者により悪意のあるコードが混入されている危険性を考慮し、対策用ファイルを信頼できる方法で入手する。具体的には、ソフトウェアの開発元等が公開するウェブサイトから直接ダウンロードすることや、開発元・販売元から郵送された外部電磁的記録媒体から対策ファイルを入手すること等が考えられる。また、対策用ファイルの改ざんを検知する手段が提供されている場合（電子署名の付与やフィンガープリントの提供等）には、それらの検証作業を実施する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.2.1(2)(f) | 基本 | 情報システムセキュリティ管理者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。 | （該当せず） | **○セキュリティホール対策状況及びソフトウェア構成の定期的状況確認**<br>・電子計算機及び通信回線装置に導入されているソフトウェアの種類及びバージョンと、それらに対するセキュリティホール対策の実施状況を定期的に確認する。セキュリティホールの存在する古いソフトウェアのバージョンを使用している場合や、適切なパッチが適用されていない等、不適切な状態が確認された場合は、その是正を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.2.1(2)(g) | 基本 | 情報システムセキュリティ責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、他の情報システムセキュリティ責任者と共有すること。 | （該当せず） | **○セキュリティホール情報と対策方法の情報共有**<br>・セキュリティホールに関連する情報の入手や、セキュリティホール対策計画の作成を効率的に行うため、情報システムセキュリティ責任者間で適宜、情報共有を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.1.2.2 不正プログラム対策**<br>**(1) 情報システムの構築時** | | | | | | | | |
| 2.1.2.2(1)(a) | 基本 | 情報システムセキュリティ責任者は、電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。以下この項において同じ。）にアンチウイルスソフトウェア等を導入すること。 | **○電子計算機へのアンチウィルスソフトウェアの導入**<br>・情報システムを構成する電子計算機（端末、サーバ装置）に、導入可能なアンチウィルスソフトウェアが存在する場合に、当該電子計算機にアンチウィルスソフトウェアを導入する。<br>・端末には、アンチウィルスソフトウェアを導入する（導入可能なアンチウィルスソフトウェアが無い場合や、ネットワークに接続されない等により装置外からデータを取り込む可能性のないものは除く。）。<br>・サーバ装置は、ファイル提供サーバ（いわゆる共有ファイルサーバや、ウェブサーバ）には、アンチウィルスソフトウェア等を導入する必要があるが、データを中継する目的のサーバ（電子メールサーバ等）等その他については、2.1.2.2(1)(b)も含めて必要性の有無を検討し、必要があると認める場合には導入する。 | （該当せず） | （該当せず） | | | |
| 2.1.2.2(1)(b) | 基本 | 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路のすべてにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。 | **○想定される感染経路への不正プログラム対策**<br>・不正プログラムの感染経路として考えられる、電子メール、ウェブのネットワーク経路において、アンチウィルスソフトウェア等の導入による不正プログラム対策を実施する。また、外部電磁的記録媒体（USBやCD-ROM，DVD等）を扱う可能性のある電子計算機（端末、サーバ装置）にて、適切な不正プログラム対策を実施する。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.2.2(1)(c) | 強化 | 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、複数の種類のアンチウイルスソフトウェア等を組み合わせ、導入すること。 | **○異なる業者のアンチウィルスソフトウェアの組み合わせ導入**<br>・電子メール、ウェブ、ファイル共有といった不正プログラムの感染経路において、複数のアンチウィルスソフトウェアを導入すると共に、それらのアンチウィルスソフトウェアをそれぞれ別の種類のソフトウェアとする。これにより、個別のアンチウィルスソフトウェア製品の事情による定義ファイルの提供遅れや検知漏れ等のリスクに対応して、効果的な不正プログラム対策を可能とする。 | （該当せず） | （該当せず） | | | |
| 2.1.2.2(1)(d) | 強化 | 情報システムセキュリティ責任者は、不正プログラムが通信により拡散することを防止するための対策を実施すること。 | **○不正プログラムの通信による拡散禁止機能の導入**<br>・不正プログラムが通信により短時間かつ大規模に感染することを防止するため、定義ファイルやパッチ適用が最新化されていない端末を接続させないネットワークの機能や、通信に不正プログラムが含まれていることを検知した場合に、その通信の送信元と想定される端末やネットワークからの通信を遮断する機能を導入する（いわゆる検疫ネットワーク機能の導入）。 | （該当せず） | （該当せず） | | | |
| **(2) 情報システムの運用時** | | | | | | | | |
| 2.1.2.2(2)(a) | 基本 | 情報システムセキュリティ管理者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、行政事務従事者にその対処の実施に関する指示を行うこと。 | （該当せず） | **○不正プログラム回避の為の特別な対処の実施**<br>・新たな不正プログラムの存在が明らかになったにも関わらず、利用中のアンチウィルスソフトウェアにおいて、定義ファイルがすぐには更新されないなど、日常行っている不正プログラム対策では不正プログラムによる影響の回避が困難と判断される場合における特別な対処を実施する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.1.2.2(2)(b) | 基本 | 情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。 | （該当せず） | **○不正プログラム対策状況の把握**<br>・1.5.2.7(1)(a)の規定による統括情報セキュリティ責任者が整備する規程に基づいた対策の状況及び本項の対策の状況を適宜把握し、問題点が発見された場合は改善する。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.1.2.3 サービス不能攻撃対策**<br>**(1) 情報システムの構築時** | | | | | | | | |
| 2.1.2.3(1)(a) | 基本 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける電子計算機、通信回線装置又は通信回線を有する情報システムに限る。以下この項において同じ。）については、サービス提供に必要な電子計算機及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。 | **○要安定情報システムにおけるサーバ装置及び通信回線装置の機能を活用したサービス不能攻撃への対策**<br>・インターネットからアクセスを受ける電子計算機又は通信回線装置において、サービス不能攻撃への対策を行うため、電子計算機又は通信回線装置が装備している対策機能を有効にする。具体的には、サーバ装置におけるSYN Cookie対策機能や、通信回線装置におけるSYN Flood対策機能、その他のサービス不能攻撃対策機能を有効化する。 | （該当せず） | （該当せず） | | | |
| 2.1.2.3(1)(b) | 強化 | 情報システムセキュリティ責任者は、情報システムがサービス不能攻撃を受けた場合に影響が最小となるように情報システムを構築すること。 | **○他のサービスへの影響を考慮した通信回線の構築**<br>・サービス不能攻撃による、通信回線の帯域圧迫によるアクセス障害や、サーバの処理能力低下等の悪影響を最小化するため、サービス不能攻撃を検出した場合に直ちに情報システムを外部ネットワークから切断する機能や、通信回線を流れる通信量に制限を加える機能等を導入する。 | （該当せず） | （該当せず） | | | |
| 2.1.2.3(1)(c) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受ける電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法及び監視記録の保存期間を定めること。 | **○サービス不能攻撃に対する監視対象の特定と監視方法の策定、及び監視機能の導入**<br>・情報システムによるサービス提供を継続する目的で、インターネットからアクセスを受ける電子計算機及び通信回線装置の中から、監視が必要となる対象を定め、その対象において適切な監視方法を定める。具体的には、サーバ装置の死活や負荷状況を監視するサーバ監視機能や、ネットワークの利用状況を監視するネットワーク監視機能、サービス不能攻撃を含めた不正アクセスを監視する侵入検知システム（IDS）の導入が考えられる。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.2.3(1)(d) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響を排除し、又は低減する対策装置を導入すること。 | **○対策装置によるサービス不能攻撃の抑止**<br>・サービス不能攻撃の影響を排除し、又は低減するための対策装置として、通信回線を流れる通信量に制限を加える機能や、侵入検知システム（IDS）及びそれと連動可能なファイアウォール機能、侵入防御システム（IPS）等を導入する。 | （該当せず） | （該当せず） | | | |
| 2.1.2.3(1)(e) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保しておくこと。 | **○サービス不能攻撃への対策を実施できる手段の確保**<br>・サービス不能攻撃への対策装置（2.1.2.3(1)(d)を参照のこと）の操作について、大量アクセスによるサービス不能攻撃が発生している状態においても、情報システムの運用者が正常に実施できるような手段を確保する。具体的な手段としては、運用者が対策装置を操作するための電子計算機、通信回線装置又は通信回線を、サービス提供のための電子計算機、通信回線装置又は通信回線とは別に用意すること等が考えられる。 | （該当せず） | （該当せず） | | | |
| 2.1.2.3(1)(f) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機、通信回線装置又は通信回線を冗長構成にすること。 | **○要安定情報システムにおける電子計算機、通信回線装置又は通信回線の冗長構成**<br>・サービス不能攻撃が発生した場合、サービスを提供する電子計算機、通信回線装置及び通信回線を代替のものに切り替えることにより、サービスが中断しないように、情報システムを構成する。この場合、代替機器等への切替処理が短時間に出来るようにすることが望ましい。 | （該当せず） | （該当せず） | | | |
| 2.1.2.3(1)(g) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機や通信回線装置における対策だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を整備すること。 | **○要安定情報システムに対するサービス不能攻撃発生時の、事業者との対処手順及び連絡体制の整備**<br>・インターネットに接続している通信回線を提供する通信事業者との間で、予め、サービス不能攻撃が発生した場合の対処手順や連絡方法を定める。これにより、情報システムの機能だけでは、発生したサービス不能攻撃の影響を防げない場合にも、当該攻撃による影響を排除し、また低減できる可能性が高まる。 | （該当せず） | （該当せず） | | | |
| **(2) 情報システムの運用時** | | | | | | | | |
| 2.1.2.3(2)(a) | 強化 | 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。 | （該当せず） | **○電子計算機、通信回線及び通信回線装置の監視と記録**<br>・情報システムによるサービス提供を継続する目的で、サービス不能攻撃を想定して定めた監視方法（2.1.2.3(1)(c)を参照のこと）により、電子計算機、通信回線又は通信回線装置を監視し、取得した監視記録を保存する。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.1.2.4 踏み台対策** | | | | | | | | |
| **(1) 情報システムの構築時** | | | | | | | | |
| 2.1.2.4(1)(a) | 基本 | 情報システムセキュリティ責任者は、情報システム（インターネット等の府省庁外の通信回線に接続される電子計算機、通信回線装置又は通信回線を有する情報システムに限る。以下この項において同じ。）が踏み台として使われることを防止するための措置を講ずること。 | **○府省庁外通信回線に接続される電子計算機、通信回線装置又は通信回線に対する踏み台攻撃への対策**<br>・インターネットからアクセスを受ける電子計算機又は通信回線装置において、踏み台になることを避けるために必要な対策を行う。具体的な対策としては、アンチウィルスソフトウェアの導入、セキュリティホールへの対策、不要なサービスの削除、フィルタリング機能の有効化、不審なプログラムの実行禁止、ボット通信の監視等が考えられる。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.1.2.4(1)(b) | 基本 | 情報システムセキュリティ責任者は、情報システムを踏み台として使われた場合の影響が最小となるように情報システムを構築すること。 | **○他のサービスへの影響を考慮した通信回線の構築**<br>・情報システムが踏み台として使われた場合の影響が最少となるよう、府省庁外から直接アクセスされる可能性のある電子計算機を、その他の電子計算機とは別のグループとして通信回線上で分離し（DMZ（DeMilitalized Zone：非武装地帯）の設置）、それ以外の電子計算機が府省庁外からアクセスできないようにアクセス制御を実施する、あるいは、府省庁内で踏み台とされる可能性がある電子計算機から府省庁外や他のグループの電子計算機への通信が必要最小限のものとなるようにアクセス制御を実施する等の措置を行う。また、通信回線の監視（侵入検知システム等の利用）によって踏み台攻撃の発生が疑われる場合に、府省庁外との通信回線の接続を自動で切断したり、問題を引き起こしている電子計算機等をネットワークから自動で切り離すための機能の導入等も考えられる。 | （該当せず） | （該当せず） | | | |
| 2.1.2.4(1)(c) | 強化 | 情報システムセキュリティ責任者は、情報システムが踏み台になっているか否かを監視するための監視方法及び監視記録の保存期間を定めること。 | **○踏み台攻撃に対する監視対象の特定と監視方法の策定、及び監視機能の導入**<br>・情報システムが踏み台として使われる場合に備え、電子計算機における意図しない稼働負荷や、意図しないインターネットへの通信、踏み台を動作させるための外部からの通信等を監視する方法を定め、その監視のために必要な機能を導入する。 | （該当せず） | （該当せず） | | | |
| **(2) 情報システムの運用時** | | | | | | | | |
| 2.1.2.4(2)(a) | 強化 | 情報システムセキュリティ管理者は、定められた監視方法に従って情報システムを監視し、その記録を保存すること。 | （該当せず） | **○電子計算機、通信回線及び通信回線装置の監視と記録**<br>・踏み台攻撃への対策として定めた監視方法（2.1.2.4(1)(c)を参照のこと）に従って、必要な情報システムの監視を行い、監視の記録を保存する。 | （該当せず） | | （該当せず） | （該当せず） |
| **第2.2部 情報システムの構成要素についての対策** | | | | | | | | |
| **2.2.1 施設と環境** | | | | | | | | |
| **2.2.1.1 電子計算機及び通信回線装置を設置する安全区域** | | | | | | | | |
| **(1) 立入り及び退出の管理** | | | | | | | | |
| 2.2.1.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、安全区域に不審者を立ち入らせない措置を講ずること。 | （該当せず） | **○安全区域への不審者の立ち入り制限措置**<br>・安全区域への不審者の立入りを防止するための措置として、身分を確認できる物の提示の義務化や、安全区域の所在表示の制限等を行う。<br>（「安全区域」とは、電子計算機及び通信回線装置を設置した事務室又はサーバルーム等の内部であって、部外者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。） | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(1)(b) | 基本 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、安全区域を物理的に隔離し、立入り及び退出を管理するための措置を講ずること。 | （該当せず） | **○安全区域とセキュリティの低いエリアとの物理的隔離**<br>・要保護情報を取り扱う情報システムを設置する安全区域において、物理的隔離及び立入り及び退出の管理によりセキュリティを確保する。物理的隔離としては、壁、施錠可能な扉、パーティション等で囲むことが考えられ、また、立入り及び退出の管理としては、安全区域が無人になる際は扉を施錠する、当該鍵の貸し出しを管理するといった措置が挙げられる。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(1)(c) | 強化 | 情報システムセキュリティ責任者は、安全区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置を講ずること。 | （該当せず） | **○安全区域へ入室する者の確認**<br>・安全区域へ立ち入る者の確認を実施することで、許可されていない者の立入りを排除する。なお、立入りを許可された者であるかの確認のために主体認証を行う機能を設けた場合には、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読み取り防止のための措置等を実施することが望ましい。 | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.1.1(1)(d) | 強化 | 情報システムセキュリティ責任者は、安全区域から退出する者が立入りを許可された者であるかの確認を行うための措置を講ずること。 | （該当せず） | **○安全区域から退出する者の確認**<br>・安全区域へ立ち入る者の確認に加え、立ち入った者が退出する際にも確認を行うことで、退室についても把握し、記録等がなされるようにする。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(1)(e) | 強化 | 情報システムセキュリティ責任者は、立入りを許可された者が、立入りを許可されていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。 | （該当せず） | **○許可された行政事務従事者のみへの入退出の限定**<br>・安全区域への立入り及び退出時における確認を確実に実施するため、一人づつでないと立入り及び退出が不可能な入退室装置（ゲート等）の設置、警備員の配置による目視確認等を実施する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(1)(f) | 強化 | 情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を許可する手続を整備すること。また、その者の氏名、所属、立入許可日、立入期間及び許可事由を含む事項を記載するための文書を整備すること。 | （該当せず） | **○安全区域への継続的入退室対象者の許可手続と文書の整備**<br>・安全区域へ継続的に立ち入る者を、業務又は業務上の責務に照らして必要な範囲とし、また、その者を確実に把握するための、許可手続および管理簿を作成する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(1)(g) | 強化 | 情報システムセキュリティ責任者は、安全区域へ立入りを許可された者に変更がある場合には、当該変更の内容を前事項の文書へ反映させること。また、当該変更の記録を保存すること。 | （該当せず） | **○入退室対象者の変更管理と記録の保存**<br>・安全区域へ継続的に立ち入る者を管理するための管理簿（2.2.1.1(1)(f)を参照のこと）を常に最新化するとともに、その変更履歴を保存する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(1)(h) | 強化 | 情報システムセキュリティ責任者は、安全区域へのすべての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。 | （該当せず） | **○安全区域への立入り及び退出の記録と監視**<br>・安全区域への立入り及び当該区域からの退出について、警備員又は監視カメラ等による記録及び監視を行う、又は、入退室装置により当該入退室のすべての記録を保存し、それらの記録を定期的に確認すること等を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| **(2) 訪問者及び受渡業者の管理** | | | | | | | | |
| 2.2.1.1(2)(a) | 強化 | 情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置を講ずること。 | （該当せず） | **○訪問者の安全区域への入室時の身元等の確認**<br>・訪問者を確認するため、訪問者に所定の事項を記入させると共に、本人の身元を名刺や社員証等により確認する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(2)(b) | 強化 | 情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置を講ずること。 | （該当せず） | **○訪問者の訪問内容の記録**<br>・訪問者の記録を保存するため、訪問者に所定の事項を記入させた用紙や記録簿等を適切に保管する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(2)(c) | 強化 | 情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問相手の行政事務従事者が訪問者の安全区域への立入りについて審査するための手続を整備すること。 | （該当せず） | **○訪問相手の行政事務従事者による訪問者の立ち入りの審査**<br>・訪問者について、訪問先の担当者が立ち入りの審査を行うため、例えば、出入口に駐在する警備員が訪問先担当者に連絡して確認する、担当者が出入口まで迎えにいく、等の手続きを定める。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(2)(d) | 強化 | 情報システムセキュリティ責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。 | （該当せず） | **○訪問者の立ち入る区域の制限**<br>・訪問者が許可されていない区域へ立ち入らないようにするため、区域毎に許可されていない者の立入りを禁止するためのゲート装置の配備等を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(2)(e) | 強化 | 情報システムセキュリティ責任者は、安全区域内において訪問相手の行政事務従事者が訪問者に付き添うための措置を講ずること。 | （該当せず） | **○訪問者への付き添い措置**<br>・訪問者が許可されていない区域に立ち入らないよう、安全区域内において、必ず訪問先担当者等の行政事務従事者が付き添うような措置を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(2)(f) | 強化 | 情報システムセキュリティ責任者は、訪問者と継続的に立入りを許可された者とを外見上判断できる措置を講ずること。 | （該当せず） | **○訪問者の外見上の識別**<br>・訪問者を、継続的に入退室を許可された職員と区別するため、訪問者用の入館カード（ゲストカード等）を作成し提示を求めたり、訪問者用の入館カード用ストラップの色を変える等の措置を行う。 | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.1.1(2)(g) | 強化 | 情報システムセキュリティ責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。<br>(ア)安全区域外で受渡しを行うこと。<br>(イ)業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、記録媒体に触れることができない場所に限定し、行政事務従事者が立ち会うこと。 | （該当せず） | **○業者との受け渡し**<br>・受渡業者と物品の受渡しを行う際に、業者が許可なく情報システム機器や記録媒体（電磁的記録媒体や印刷物等）に接触することがないよう、必要な措置を講じる。 | （該当せず） | | （該当せず） | （該当せず） |

**(3) 電子計算機及び通信回線装置のセキュリティ確保**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2.1.1(3)(a) | 基本 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している電子計算機の盗難及び当該場所からの不正な持出しを防止するための措置を講ずること。 | （該当せず） | **○設置場所が確定した電子計算機の移動防止措置**<br>・設置場所が確定している電子計算機（サーバ装置及び据置き型PC等）について、盗難及び不正な持出しを防止するため、設置場所からの移動を防止するための措置を行う。具体的には、端末であればセキュリティワイヤの固定、サーバ装置であればサーバラックへの設置及び当該サーバラックの施錠、端末及びサーバ装置について施設からの退出時における持ち物検査等の実施がある。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(3)(b) | 強化 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置を他の情報システムから物理的に隔離し、安全区域を共用しないこと。 | （該当せず） | **○電子計算機及び通信回線装置の物理的隔離**<br>・他の情報システムと共用の安全区域に設置することで安全性が確保できないと判断する場合に、当該情報システムの電子計算機及び通信回線装置を他の情報システムから物理的に隔離する措置を行う。具体的には、独自の施錠等を行う別室を用意する、一つの室の中でパーティションを区切り、他との往来を制限する等が考えられる。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(3)(c) | 強化 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している通信回線装置の盗難及び当該場所からの不正な持出しを防止するための措置を講ずること。 | （該当せず） | **○設置場所が確定した通信回線措置の移動防止措置**<br>・設置場所が確定している通信回線装置について、盗難及び不正な持出しを防止するため、設置場所からの移動を防止するための措置を行う。具体的には、基幹の通信回線装置であればサーバラックへの設置及び当該サーバラックの施錠、終端の通信回線装置であれば床下への埋設等がある。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(3)(d) | 強化 | 情報システムセキュリティ責任者は、行政事務従事者が離席時に電子計算機及び通信回線装置を不正操作から保護するための措置を講ずること。 | **○電子計算機及び通信回線装置の不正操作からの保護機能の導入**<br>・行政事務従事者の離席時に、電子計算機及び通信回線装置を第三者による不正操作から保護するための機能を導入する。具体的な対策としては、スクリーンロック機能の導入に加え、そのスクリーンロック機能について、一定時間操作がないと自動的にロックし、かつロック解除にパスワード等による主体認証等が必要となる設定をする等がある。 | **○電子計算機及び通信回線装置の不正操作からの保護の徹底**<br>・電子計算機及び通信回線装置の運用において、行政事務従事者の離席時に、第三者による不正操作から保護するための対策を行う。具体的な対策としては、例えば、行政事務従事者の端末についてスクリーンロック機能を導入している場合には、その設定を実施する。 | （該当せず） | | | |
| 2.2.1.1(3)(e) | 強化 | 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置を講ずること。 | （該当せず） | **○表示用デバイスの盗み見からの保護**<br>・電子計算機に接続されたディスプレイや、通信回線装置のメッセージ表示用ディスプレイ等を、許可のない第三者に見られないような対策を実施する。具体的には、ディスプレイに偏向フィルタを取り付ける等がある。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(3)(f) | 強化 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、情報システムで利用する電源ケーブル及び通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置を講ずること。 | （該当せず） | **○要保護情報を取り扱う情報システムにおける電源ケーブルと通信ケーブルの保護**<br>・電源ケーブルの損傷や、通信ケーブルの損傷及び物理的な手段による通信の盗聴等（盗聴器の挿入等）の脅威から保護するための対策を実施する。具体的には、ケーブルの床下への埋設等がある。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(3)(g) | 強化 | 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、電磁波による情報漏えい対策の措置を講ずること。 | （該当せず） | **○電磁波からの情報漏えい対策**<br>・ディスプレイケーブル等から生じる電磁波による情報漏えいのリスクについての対策を講ずる。具体的には、ディスプレイケーブルへの電磁波軽減フィルタの取り付け等がある。 | （該当せず） | | （該当せず） | （該当せず） |

**(4) 安全区域内のセキュリティ管理**

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.1.1(4)(a) | 基本 | 行政事務従事者は、安全区域内において、身分証明書を他の職員から常時視認することが可能な状態にすること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.1.1(4)(b) | 強化 | 行政事務従事者は、情報システムセキュリティ責任者の許可を得た上で、要保護情報を取り扱う情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しを行うこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.1.1(4)(c) | 強化 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しに係る記録を取得すること。 | （該当せず） | **○安全区域への物品の持込み及び持出しの記録**<br>・情報システムを構成する物品等を適正に管理するため、関連する物品の持込み及び持出しを記録する。記録する事項としては、持込み及び持出しを行う者の名前及び所属、日時、対象物品、事由等が考えられる。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(4)(d) | 強化 | 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の安全区域への持込みについて制限すること。 | （該当せず） | **○情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体、映像／画像記憶装置の安全区域への持ち込み制限**<br>・情報漏えいの原因となる恐れがある電子計算機、通信回線装置、電磁的記録媒体（以上、当該情報システムに関連しないもの）及び、音声や映像・画像を記録するための装置（カメラ、録音機等）の安全区域への持込みを制限する。具体的には、安全区域に立ち入る職員自身が注意する、訪問者については付き添え者が注意を促す、持込制限対象の物品を一時的に保管するロッカーや場所等を設置する、等の措置がある。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(4)(e) | 強化 | 情報システムセキュリティ責任者は、安全区域内での作業を監視するための措置を講ずること。 | （該当せず） | **○安全区域内における作業の監視**<br>・安全区域での作業を監視するため、第三者による立ち会いを義務化することや、監視カメラの導入等を実施する。 | （該当せず） | | （該当せず） | （該当せず） |
| **(5) 災害及び障害への対策** | | | | | | | | |
| 2.2.1.1(5)(a) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。 | （該当せず） | **○自然災害及び人為的災害からの電子計算機及び通信回線装置の物理的保護**<br>・地震、火災、水害、停電、爆発及び騒じょう等の災害から電子計算機及び通信回線装置を保護するための対策を行う。具体的には、サーバラックの利用のほか、ハロゲン化物消火設備、無停電電源装置等の設備、空調設備、耐震又は免震設備、非常口及び非常灯等の設置又は確保がある。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.1.1(5)(b) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、安全区域内において災害又は障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。 | （該当せず） | **○非常時の電子計算機と通信回線装置の電源遮断**<br>・作業者が災害等により安全区域に設置された電子計算機及び通信回線装置に近づくことができない場合に、作業者の安全性を確保した上で電子計算機及び通信回線装置の電源を遮断できるための措置を講じておく。具体的には、非常時に即座に電源を切ることができるように、電源を切るための緊急スイッチを設備室の非常口近くに設置しておく等の措置を行う等がある。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.2.2 電子計算機**<br>**2.2.2.1 電子計算機共通対策**<br>**(1) 電子計算機の設置時** | | | | | | | | |
| 2.2.2.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を将来の見通しを含め検討し、確保すること。 | **○電子計算機に求められるシステム性能の検討と確保**<br>・要安定情報を取り扱う電子計算機において、当該電子計算機の運用上求められるシステム性能を確保するため、想定される処理負荷及び処理容量を見積もり、それらに備えた性能設計を行った上で、ハードウェア・ソフトウェア製品の選択や、処理機能の実装、性能試験等に反映させる。将来にわたっても十分なシステム性能を確保できるように、拡張性や余裕を持たせる。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.2.1(1)(b) | 基本 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機を安全区域に設置すること。ただし、モバイルPCについて情報セキュリティ責任者の承認を得た場合は、この限りでない。 | （該当せず） | **○電子計算機の安全区域への設置**<br>・部外者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策を講じるため、要保護情報を取り扱う情報システムについて、電子計算機を安全区域に設置する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.2.1(1)(c) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機を冗長構成にすること。 | **○要安定情報システムにおける電子計算機の冗長構成**<br>・サービスを提供する電子計算機に障害・事故等が発生した場合に、代替電子計算機へ切り替えることでサービスが継続されるように、当該電子計算機を冗長構成とする。なお、災害等を想定して冗長構成にする場合には、代替電子計算機を遠隔地に設置して、災害時等に利用できるようにすることが望ましい。 | （該当せず） | （該当せず） | | | |
| **(2) 電子計算機の運用時** | | | | | | | | |
| 2.2.2.1(2)(a) | 基本 | 行政事務従事者は、行政事務の遂行以外の目的で電子計算機を利用しないこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.2.1(2)(b) | 強化 | 情報システムセキュリティ責任者は、所管する範囲の電子計算機で利用されているすべてのソフトウェアの状態を定期的に調査し、不適切な状態にある電子計算機を検出した場合には、当該不適切な状態の改善を図ること。 | （該当せず） | **○電子計算機のソフトウェアの定期的調査及びその改善**<br>・電子計算機で利用しているソフトウェアについて定期的に調査し、利用が許可されていないソフトウェアがインストールされている、ソフトウェアがセキュリティの観点で望ましくない設定になっている等の不適切な状態にある電子計算機が存在する場合に、その状態の改善を図る。具体的な対策の一つとして、行政事務従事者が利用する端末等を対象にインベントリ管理のためのシステムを導入し、それにより管理対象の電子計算機上のソフトウェアやその設定を定期的に確認する等も考えられる。 | （該当せず） | | （該当せず） | （該当せず） |
| **(3) 電子計算機の運用終了時** | | | | | | | | |
| 2.2.2.1(3)(a) | 基本 | 情報システムセキュリティ責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体のすべての情報を抹消すること。 | （該当せず） | **○電子計算機の電磁的記録の確実な消去**<br>・電子計算機の運用を終了する場合に、当該電子計算機に含まれる電磁的記録媒体から、すべての情報を抹消する。情報の抹消にあたり、単純に「ファイル削除」の操作をしただけでは、ファイルの情報自体が電磁的に残存する可能性があり、抹消ツールの使用や媒体の物理的破壊等の、電磁的記録を完全に読めなくするための対策を実施する。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.2.2.2 端末**<br>**(1) 端末の設置時** | | | | | | | | |
| 2.2.2.2(1)(a) | 基本 | 情報システムセキュリティ責任者は、端末で利用可能なソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙し、又は両者を併用することができる。 | **○端末で利用可能なソフトウェアの定義**<br>・セキュリティの観点で利用が危険なソフトウェアの排除や、多様なソフトウェアの利用に伴うセキュリティホール等のリスクの低減のため、端末で利用可能なソフトウェアを予め定め、それ以外のソフトウェアの利用を禁止する。利用可能なソフトウェアは、業務上及び端末運用管理上の必要性に照らして検討することが必要である。利用可能なソフトウェアをリストアップすることが困難な場合には、利用を禁止するソフトウェアを具体的に定め、それらのソフトウェアの利用禁止を徹底することでもよい。<br><br>（「端末」とは、端末を利用する行政事務従事者が直接操作を行う電子計算機（オペレーティングシステム及び接続される周辺機器を含む。）であり、いわゆるPCのほか、PDA等も該当する。） | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.2.2(1)(b) | 基本 | 情報システムセキュリティ責任者は、要保護情報を取り扱うモバイルPCについては、府省庁外で使われる際にも、府省庁内で利用される端末と同等の保護手段が有効に機能するように構成すること。 | **○モバイルPCの庁舎外での利用時の保護のための機能及び設定**<br>・府省庁外で利用されるモバイルPCについて、府省庁内で利用される端末とは異なる環境下で使用されることに留意し、府省庁内の端末と同等のセキュリティの保護がなされるように機能の導入や設定を行う。具体的には、主体認証やアクセス制御、証跡管理、監視といった機能が、府省庁内のネットワークに接続されない状態でも同等に機能する必要があり、そのための対策としてパーソナルファイアウォールの導入や、端末セキュリティポリシーの設定等を行う。<br><br>（「モバイルPC」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用するノート型PCは、モバイルPCには含まれない。） | （該当せず） | （該当せず） | | | |
| 2.2.2.2(1)(c) | 基本 | 行政事務従事者は、モバイルPCを利用する必要がある場合には、情報システムセキュリティ責任者の承認を得ること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.2.2(1)(d) | 基本 | 情報システムセキュリティ責任者は、要機密情報を取り扱うモバイルPCについては、電磁的記録媒体に保存される情報の暗号化を行う機能を設けること。 | **○モバイルPCの暗号化を行う機能の実装**<br>・モバイルPCが盗難等により外部の者の手に渡った場合に、モバイルPCから取り外された電磁的記録媒体から他の電子計算機を利用して情報が解読される恐れがあることから、端末に格納される要保護情報をすべて暗号化できるよう、モバイルPCに暗号化機能を導入する。 | （該当せず） | （該当せず） | | | |
| 2.2.2.2(1)(e) | 基本 | 情報システムセキュリティ責任者は、要保護情報を取り扱うモバイルPCについては、盗難を防止するための措置を定めること。 | （該当せず） | **○モバイルPCの盗難防止措置の定め**<br>・モバイルPCが盗難又は紛失されないように、府省庁内での保管・使用においてはセキュリティワイヤで固定し、又は施錠可能なキャビネットに保管することや、持ち出し時には、常に身近に置き、目を離さない等の措置を定める。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.2.2(1)(f) | 強化 | 情報システムセキュリティ責任者は、行政事務従事者が情報を保存できない端末を用いて情報システムを構築すること。 | **○情報を保存できない端末の利用環境の構築**<br>・端末が盗難・紛失、不正な持ち出し等が行われた場合に、端末から情報が漏えいしないよう、端末内の電磁的記録媒体には情報が保存できない端末（シンクライアント端末）を利用することとし、そのような端末を利用可能にするために必要なサーバやネットワークを含めたシンクライアント端末環境を構築する。 | （該当せず） | （該当せず） | | | |
| **(2) 端末の運用時** | | | | | | | | |
| 2.2.2.2(2)(a) | 基本 | 行政事務従事者は、端末で利用可能と定められたソフトウェアを除いて、ソフトウェアを利用しないこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.2.2(2)(b) | 基本 | 行政事務従事者は、要保護情報を取り扱うモバイルPCを利用する場合には、盗難防止措置を行うこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.2.2(2)(c) | 基本 | 行政事務従事者は、要機密情報を取り扱うモバイルPCについては、モバイルPCを府省庁外に持ち出す場合に、当該モバイルPCで利用する電磁的記録媒体に保存されている要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.2.2(2)(d) | 基本 | 行政事務従事者は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に端末を接続しないこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.2.2(2)(e) | 強化 | 情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、端末の時刻を同期すること。 | **○端末への時刻同期機能の導入**<br>・情報システムを構成する各機器に時刻情報を配信するための機能を導入(ntpサーバの導入等）し、端末の時刻を同期させるために必要な機能の導入及び設定(ntpクライアントとしての設定等）を行う。 | **○端末の時刻同期**<br>・端末の時刻を同期させるための機能を有効化し、継続的に時刻の同期がなされるようにする。 | （該当せず） | | | |

**2.2.2.3 サーバ装置**
**(1) サーバ装置の設置時**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2.2.3(1)(a) | 基本 | 情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報を暗号化するための機能を設けること。 | **○サーバ装置への保守作業時の通信の暗号化**<br>・サーバ装置の保守作業において、保守する者が通信回線を経由してサーバ装置にログオンして作業することが想定される場合に、通信上で送受信する情報を暗号化する必要性を検討し、必要があると判断する場合には、情報を暗号化するための機能を設ける。特に、インターネット等の信頼できない府省庁外通信回線を経由して遠隔保守作業を行う場合には、暗号化をする必要があると判断する。具体的には、暗号通信を行うリモートターミナルサービス用ソフトウェア(ssh等）を導入する等が考えられる。<br><br>（「サーバ装置」とは、通信回線等を経由して接続してきた電子計算機に対して、自らが保持しているサービスを提供する電子計算機をいう。） | （該当せず） | （該当せず） | | | |
| 2.2.2.3(1)(b) | 基本 | 情報システムセキュリティ責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。 | **○サーバ装置で利用するソフトウェアの定義**<br>・不要なサーバアプリケーションが稼働している又は導入されていることによるセキュリティホールや不適切な設定等のセキュリティリスクを軽減するため、サーバ装置で利用するソフトウェアについて、サービスの提供及びサーバ装置の運用管理での必要性の観点からリストアップし、予め定める。 | （該当せず） | （該当せず） | | | |
| 2.2.2.3(1)(c) | 基本 | 情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動すること。 | **○不要なサーバアプリケーションの無効化**<br>・不要なサーバアプリケーションが稼働していることによるセキュリティホールや不適切な設定等のセキュリティリスクを軽減するため、利用が定められたソフトウェア（2.2.2.3(1)(b)を参照のこと）に該当しないサーバアプリケーションが稼働している場合に、当該サーバアプリケーションを停止する措置を行う。また、利用が定められたソフトウェア（前述）に該当するサーバアプリケーションであっても、サービスの提供又はサーバ装置の運用管理において利用しない機能がある場合は、当該機能を無効化する措置を行う。 | （該当せず） | （該当せず） | | | |
| 2.2.2.3(1)(d) | 強化 | 情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないソフトウェアをサーバ装置から削除すること。 | **○不要なサーバアプリケーションの削除**<br>・不要なサーバアプリケーションが導入されていることによるセキュリティホールや不適切な設定等のセキュリティリスクを軽減するため、利用が定められたソフトウェア（2.2.2.3(1)(b)を参照のこと）に該当しないソフトウェアを、サーバ装置から削除する。または、OSのインストール（一般的にOSにバンドルされた複数ソフトウェアが含まれる）や、パッケージ製品に含まれる複数のソフトウェアをインストールする際に、不要なソフトウェアが導入されないように配慮して導入を行う。 | （該当せず） | （該当せず） | | | |
| 2.2.2.3(1)(e) | 強化 | 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置の内、サービス提供に必要なサーバ装置については、負荷を複数のサーバ装置に分散又はサーバ装置を冗長構成とすること。 | **○サーバ装置の負荷分散又は冗長化**<br>・障害・事故等や過度のアクセス集中等によりサービスが提供できなくなる事態を防止するため、複数のサーバ装置による負荷分散、負荷分散装置の設置、DNSによる負荷分散や、サーバ装置の冗長化等を検討し、そのために必要な装置や機能の導入や設定等を行う。 | （該当せず） | （該当せず） | | | |

**(2) サーバ装置の運用時**

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.2.3(2)(a) | 基本 | 情報システムセキュリティ責任者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対処すること。 | （該当せず） | **○サーバ装置構成変更時の確認とセキュリティへの影響の特定**<br>・サーバ装置の構成（ソフトウェア及びハードウェア等）が変更されていないか定期的に確認する。変更がある場合に、その変更事項によりサーバ装置のセキュリティレベル低下等の悪影響が発生していないかどうか確認し、悪影響がある場合には、変更事項を元に戻す等の是正を行う。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.2.3(2)(b) | 基本 | 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置については、サーバ装置の運用状態を復元するために必要な措置を講ずること。 | **○サーバ装置内情報の定期バックアップ機能の導入**<br>・サーバ装置に保存されている情報及びその情報を用いたサービスの可用性を確保するため、サーバ装置の運用状態を復元するための措置として、保存されている情報を定期的にバックアップする必要性を検討し、必要があると判断する場合には、情報の定期的なバックアップのために必要な機能を導入する。 | **○サーバ装置の運用状態を復元するための措置の実施**<br>・サーバ装置の運用状態を復元するための措置を定め、実施する。具体的には、サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく、サーバ装置に導入された機能を用いて定期的にバックアップを取得する、バックアップデータ等を利用してサーバ装置の運用状態を回復する手段を確保しておく、等がある。 | （該当せず） | | | |
| 2.2.2.3(2)(c) | 基本 | 情報システムセキュリティ管理者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。 | （該当せず） | **○サーバ装置運用管理作業の記録**<br>・サーバ装置において障害等のトラブルが発生した際の原因究明につなげる目的で、サーバ装置に対して行われる日々の運用管理作業の記録を残すため、予め運用管理作業を記録する様式等を定めておき、それに基づき運用管理作業を記録する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2].2.3(2)(d) | 基本 | 情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。 | **○サーバ装置への時刻同期機能の導入**<br>・情報システムを構成する各機器に時刻情報を配信するための機能を導入(ntpサーバの導入等）し、サーバ装置の時刻を同期させるために必要な機能の導入及び設定(ntpクライアントとしての設定等）を行う。 | **○サーバ装置の時刻同期**<br>・サーバ装置の時刻を同期させるための機能を有効化し、継続的に時刻の同期がなされるようにする。 | （該当せず） | | | |
| 2.2.2.3(2)(e) | 強化 | 情報システムセキュリティ管理者は、サーバ装置のセキュリティ状態を監視し、不正行為及び不正利用を含む事象の発生を検知すること。 | **○サーバ装置への不正行為、不正利用の発生検知機能の導入**<br>・サーバ装置上での不正な行為及び要機密情報への不正なアクセス等の発生を監視するため、侵入検知システム、ファイル完全性チェックツール、プロセス監視ツール等を導入する。 | **○サーバ装置への不正行為、不正利用の発生検知**<br>・サーバ装置上での不正な行為及び要機密情報への不正なアクセス等の発生を監視するため、アクセスログを定期的に確認することや、導入した侵入検知システム、ファイル完全性チェックツール、プロセス監視ツール等の機能を用いて監視を行う。 | （該当せず） | | | |
| 2.2.2.3(2)(f) | 強化 | 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視し、当該サーバ装置に関する障害等の発生を検知すること。 | **○サーバ装置のシステム状態の監視とトラブルの検知機能の導入**<br>・サーバ装置において障害等のトラブルが発生した際に早期に発見するため、サーバ装置のシステム状態を監視する機能を導入する。サーバ装置を遠隔から監視、又は複数のサーバ装置を集中的に監視する場合には、SNMP等を用いたシステム監視ツールを導入する。 | **○サーバ装置のシステム状態の監視とトラブルの検知**<br>・サーバ装置において障害等のトラブルが発生した際に早期に発見する目的で、サーバ装置のシステム状態を把握するため、導入した機能等を用いてサーバ装置のシステム状態を監視する。 | （該当せず） | | | |

**2.2.3 アプリケーションソフトウェア**
**2.2.3.1 電子メール**
**(1) 電子メールの導入時**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2.3.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。 | **○電子メールサーバへの不正中継防止設定**<br>・迷惑メールの送信等の踏み台に使われることを回避するために、電子メールを不正に中継しないように電子メールサーバを設定する。具体的には、交換用電子メールサーバ(MTA)で、府省庁外からの電子メールの中継について、自ドメインあての電子メールのみを府省庁内部の電子メールサーバ等に転送し、他のドメインあての中継は拒否する。更に、送信用電子メールサーバ(MSA)で、府省庁LAN上に接続された電子計算機から送信された電子メールのみを送信し、府省庁外からの送信要求は拒否する等の対策も考えられる。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.3.1(1)(b) | 基本 | 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に行政事務従事者の主体認証を行う機能を備えること。 | **○電子メールサーバとメールクライアント間の送受信時の主体認証**<br>・送受信用電子メールサーバにおいて、各利用者用のメールボックスにアクセスして電子メールを受信する処理について、必ず利用者の主体認証を行うことに加え、電子メールの送信についても、SMTP認証等により送信者の主体認証が行われるように、電子メールサーバを設定する。なお、送信者の主体認証については、端末がボット等の不正プログラムに感染し、不正な操作により電子メールを送信させられるような踏み台攻撃への対策としても有効である。 | （該当せず） | （該当せず） | | | |
| **(2) 電子メールの運用時** | | | | | | | | |
| 2.2.3.1(2)(a) | 基本 | 行政事務従事者は、業務遂行に係る情報を含む電子メールを送受信する場合には、各府省庁が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。ただし、府省庁支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.3.1(2)(b) | 基本 | 行政事務従事者は、受信した電子メールにより、スクリプトが電子計算機で実行されないように電子メールの内容を表示させること。 | （該当せず） | **○電子メールクライアントにおいてスクリプトが実行されないための電子メールの表示の設定**<br>・電子メールクライアントの運用において、例えばHTML形式の電子メールを元の形式のまま表示すると、偽のホームページに誘導するために表示が偽造されること、意図しないファイルが外部から取り込まれること等の問題が発生するため、これらの問題の原因となる不正なスクリプトが電子メールクライアントで実行されないように電子メールの表示の設定を行う。<br>「スクリプト」とは、ここではJavaScript等の電子計算機にて簡易に実行することができるプログラムをいう。「スクリプトが電子計算機で実行されないように表示させる」とは、表示をテキスト形式のみに設定して表示することや端末でスクリプトの実行を禁止された情報システムを用いて表示することが挙げられる。 | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| **2.2.3.2 ウェブ**<br>**(1) ウェブの導入時** | | | | | | | | |
| 2.2.3.2(1)(a) | 基本 | 情報システムセキュリティ責任者は、ウェブサーバを用いて提供するサービスが利用者からの文字列等の入力を受ける場合には、特殊文字の無害化を実施すること。 | **○ウェブサーバにおける利用者からの特殊文字入力の無害化**<br>・ウェブサービスの提供において、フォーム等により利用者が入力するページを提供する場合に、その入力される文字列等に特殊文字を挿入されることにより、ウェブサーバが意図しない動作をさせられる（SQLインジェクションやファイル・トラバーサルと呼ばれる攻撃等）ことを防止するため、特殊文字の無害化が確実に行われるようにウェブサーバを設計し、実装する。 | （該当せず） | （該当せず） | | | |
| 2.2.3.2(1)(b) | 基本 | 情報システムセキュリティ責任者は、ウェブサーバからウェブクライアントに攻撃の糸口になり得る情報を送信しないように情報システムを構築すること。 | **○攻撃の糸口となる情報の送信禁止**<br>・ウェブサービスを提供するウェブアプリケーションやデータベース等について、利用者からの要求に対する応答等として、稼働している製品名及びそのバージョン、登録されているユーザID、各種の詳細な情報が記載されたエラーメッセージ等の不要な情報を送信してしまうと、攻撃を試みる者に攻撃の糸口になり得る情報を与えてしまうため、これらの不要な情報を利用者に対して送信しないように、ウェブサーバを設計し、実装する。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.3.2(1)(c) | 基本 | 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバを用いて提供するサービスにおいて、通信の盗聴から保護すべき情報を特定し、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化する機能を設けること。 | **○ウェブサーバの通信の暗号化の必要性の検討と暗号化**<br>・ウェブサーバにおいて、特定の利用者にのみ提供することを目的とした要機密情報や個人情報を提供する場合、または、利用者から要機密情報や個人情報を入力させる場合等について、それらの情報が流れる通信を暗号化する必要性を検討し、必要があると判断する場合には通信暗号化のための機能を導入する。具体的には、ウェブサーバにサーバ証明書を導入し、httpsによる情報の提供及び入力により、通信を暗号化する等の措置を行う。 | （該当せず） | （該当せず） | | | |
| 2.2.3.2(1)(d) | 強化 | 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバに保存する情報を特定し、当該サーバに要機密情報が含まれないことを確認すること。 | **○ウェブサーバへ保存する情報の特定**<br>・万が一、不正侵入等された場合の被害を最小化するため、ウェブサーバ自体に保存する情報について、要機密情報が含まれないように、情報システムを構築し、導入する。ウェブサービスにおいて特定の利用者に要機密情報を提供する場合には、それらの要機密情報を外部からアクセス可能なウェブサーバ自体ではなく、内部のネットワークに設置した基幹サーバ等に保存し、ウェブサーバは情報提供の中継のみ行うようなシステム構成とすることが考えられる。 | （該当せず） | （該当せず） | | | |
| 2.2.3.2(1)(e) | 強化 | 情報システムセキュリティ責任者は、ウェブサーバの正当性を保証するために電子証明書を利用すること。 | **○ウェブサーバの正当性を保証する電子証明書の利用**<br>・ウェブサーバをなりすました偽のホームページが立ち上げられ、そこに誘導されることでアクセスする者等に重大な被害が出ることが想定される場合には、ウェブサーバにサーバ証明書を導入し、httpsでサービスを提供することで、利用者がサーバ証明書の確認によりウェブサーバの正当性を確認できるようにシステムを構成する。 | （該当せず） | （該当せず） | | | |

**(2) ウェブの運用時**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2.3.2(2)(a) | 基本 | 行政事務従事者は、情報セキュリティの確保がなされるよう適切にウェブクライアントのセキュリティ設定をすること。 | （該当せず） | **○ウェブクライアントのセキュリティ設定**<br>・ウェブクライアントの運用において、行政事務従事者が意図しない悪意のあるソフトウェアが電子計算機において実行されること等により、情報が漏えいしてしまうことや他の電子計算機を攻撃してしまうこと等を防止するため、ウェブクライアントのセキュリティ設定を適切に行う。<br>具体的には、閲覧するホームページの信頼性やウェブクライアントが動作する電子計算機にて扱う情報の機密性等に応じて、次のようなセキュリティ設定項目について適切な値を選択する。（ActiveXコントロールの実行／JavaScriptの実行／Javaの実行／Cookieの保存　等） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.3.2(2)(b) | 基本 | 行政事務従事者は、ウェブクライアントが動作する電子計算機にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.3.2(2)(c) | 基本 | 行政事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。<br>（ア）送信内容が暗号化されること<br>（イ）当該ウェブサイトが送信先として想定している組織のものであること。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.3.2(2)(d) | 強化 | 情報システムセキュリティ責任者は、行政事務従事者が閲覧することが可能な府省庁外のホームページを制限し、定期的にその見直しを行うこと。 | **○行政事務従事者が閲覧可能なホームページを制限する機能の導入**<br>・府省庁外部のホームページの閲覧を通じて、不適切なソフトウェアがダウンロードされたり、要機密情報が流出したりする問題を最小限とするため、閲覧可能な外部ホームページの範囲を制限するためのコンテンツフィルタ機能を導入する。コンテンツフィルタ機能としては、ウェブクライアントに導入するもの、ウェブプロキシーに導入するものやその他装置によるものが存在するため、そのうち適切なものを選択し、導入する必要がある。 | **○行政事務従事者が閲覧可能なホームページの制限と定期的見直し**<br>・閲覧可能な外部のホームページの範囲を制限するためのコンテンツフィルタ機能について、その閲覧可能な範囲を定期的に見直し、必要に応じてコンテンツフィルタ機能の設定等を更新する。 | （該当せず） | | | |

**2.2.3.3 ドメインネームシステム（DNS）**

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| **(1) DNSの導入時** | | | | | | | | |
| 2.2.3.3(1)(a) | 基本 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するDNSのコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。 | **○DNSのコンテンツサーバにおいて、名前解決を停止させないための措置**<br>・要安定情報を取り扱う情報システムの名前解決を提供するDNSのコンテンツサーバにおいて、名前解決を停止させないために冗長化等の対策を実施する。DNSのコンテンツサーバの冗長化としては、府省庁内にプライマリDNS、セカンダリDNSを合わせて複数のDNSのコンテンツサーバを設置して運用することの他、例えば、ISPが提供するセカンダリDNSを利用することも含まれる。要求される可用性の度合いに応じて、保守作業による復旧対策等の、冗長化以外の措置を実施することも考えられる。<br><br>（「名前解決」とは、ドメイン名やホスト名とIPアドレスを変換することをいう。<br>「DNSサーバ」とは、名前解決のサービス提供するアプリケーション及びそのアプリケーションを動作させる電子計算機をいう。DNSサーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の二種類に分けることができる。） | （該当せず） | （該当せず） | | | |
| 2.2.3.3(1)(b) | 基本 | 情報システムセキュリティ責任者は、DNSのコンテンツサーバにおいて管理するドメインに関する情報を運用管理するための手続を定めること。 | （該当せず） | **○DNSのコンテンツサーバにおいて、管理するドメインに関する情報を運用管理するための手続**<br>・DNSのコンテンツサーバにおいて管理するドメインに関する情報（ゾーン情報）を運用管理するための情報として、管理するドメインの構成範囲を明確化するとともに、ドメイン情報の設定や更新の手続、正確性の維持のための手順等を整備する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.3.3(1)(c) | 基本 | 情報システムセキュリティ責任者は、DNSのキャッシュサーバにおいて、府省庁外からの名前解決の要求には応じず、府省庁内からの名前解決の要求のみに回答を行なうための措置を講ずること。 | **○DNSのキャッシュサーバにおいて、府省庁外からの名前解決の要求に応じないための措置**<br>・DNSのキャッシュサーバの第三者による不正利用やキュッシュ情報の汚染等を防止するための措置として、DNSサーバの設定やファイアウォール等によるアクセス制御を実施する。 | （該当せず） | （該当せず） | | | |
| 2.2.3.3(1)(d) | 基本 | 情報システムセキュリティ責任者は、DNSのコンテンツサーバにおいて、府省庁内のみで使用する名前の解決を提供する場合、当該情報が外部に漏えいしないための措置を講ずること。 | **○DNSのコンテンツサーバにおいて、内部のみで使用する名前に関する情報を漏えいしないための措置**<br>・DNSのコンテンツサーバにおいて、府省庁内のみで使用する名前情報の解決を提供する場合、府省庁外の者が内部のみで使用している名前情報を取得できないようにするための対策を実施する。具体的には、府省庁内向けの名前解決を提供するコンテンツサーバを府省庁外向けのコンテンツサーバと別々に設置する、DNSサーバの設定やファイアウォール等によりアクセス制御を行う、等が考えられる。 | （該当せず） | （該当せず） | | | |
| 2.2.3.3(1)(e) | 強化 | 情報システムセキュリティ責任者は、重要な情報システムの名前解決を提供するDNSのコンテンツサーバにおいて、管理するドメインに関する情報に電子署名を付与すること。 | **○DNSのコンテンツサーバにおいて、管理するドメインに関する情報の電子署名を付与する措置**<br>・DNSサーバのなりすましや管理するドメインに関する情報（ゾーン情報）の改ざんを検出するため、ドメイン情報に電子署名を付与するための機能をDNSサーバに導入し、管理するドメイン情報に電子署名を付与する。TSIGやDNSSECの利用が考えられる。 | （該当せず） | （該当せず） | | | |
| **(2) DNSの運用時** | | | | | | | | |
| 2.2.3.3(2)(a) | 基本 | 情報システムセキュリティ管理者は、DNSのコンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。 | （該当せず） | **○DNSのコンテンツサーバにおいて、管理するドメインに関する情報を複数のサーバ間で整合性を維持する措置**<br>・管理するドメインに関する情報を扱う複数台のDNSのコンテンツサーバがある場合に、複数のサーバ間でドメイン情報の整合性を維持するための措置を行う。例えば、主系統のコンテンツサーバのドメイン情報が変更された場合に、ゾーン転送機能の利用により、適切なタイミングで副系統のコンテンツサーバのドメイン情報を更新する。 | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.3.3(2)(b) | 基本 | 情報システムセキュリティ管理者は、DNSのコンテンツサーバにおいて管理するドメインに関する情報を運用管理するための手続に基づいて、当該情報が正確であることを適宜確認すること。 | （該当せず） | **○運用管理手続に基づいた、管理するドメインに関する情報が正確であることの確認**<br>・DNSのコンテンツサーバにおいて管理するドメインに関する情報（ゾーン情報）を運用管理するための手続（2.2.3.3(1)(b)を参照のこと）に基づき、管理するドメインに関する情報の正確性を維持するための手順を実施する。 | （該当せず） | | （該当せず） | （該当せず） |

**2.2.4 通信回線**
**2.2.4.1 通信回線共通対策**
**(1) 通信回線の構築時**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2.4.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、通信回線構築によるリスクを検討し、通信回線を構築すること。 | **○リスクを検討した通信回線の構築**<br>・通信回線を構築する場合に、必ず通信回線構築による情報セキュリティのリスクを検討した上で、情報セキュリティ対策の観点から適切となるように通信回線を設計し、構築する。特に、インターネット等の府省庁外の通信回線との接続や、府省庁内の他の情報システムの通信回線との接続又は共用について、情報セキュリティ対策の観点からメリット・デメリットを整理した上で実施等を判断し、実施する場合には必要な対策が講じられるように通信回線を設計し、構築する。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(b) | 基本 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。 | **○通信回線及び通信回線装置の通信性能を発揮する能力の検討と確保**<br>・要安定情報を取り扱う通信回線及び通信回線装置において、当該通信回線及び装置の運用上求められるシステム性能を確保するため、想定される処理負荷及び通信容量を見積もり、それらに備えた性能設計を行った上で、回線及びハードウェア・ソフトウェア製品の選択や、処理機能の実装、性能試験等に反映させる。将来にわたっても十分なシステム性能を確保できるように、拡張性や余裕を持たせる。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(c) | 基本 | 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定めること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。 | **○通信回線装置が動作するために必要なソフトウェアの定め**<br>・不要なソフトウェアが稼働している又は導入されていることによるセキュリティホールや不適切な設定等のセキュリティリスクを軽減するため、通信回線装置が利用するソフトウェアについて、通信回線装置の動作及び運用管理の必要性の観点からリストアップし、予め定める。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(d) | 基本 | 情報システムセキュリティ責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。 | **○電子計算機のグループ化と通信回線上での分離**<br>・電子計算機が接続されている通信回線の境界で、効果的にアクセス制御を行うために、電子計算機をグループ化し通信回線上で分離する。インターネット等の府省庁外通信回線と接続する府省庁内通信回線の場合には、府省庁外から直接アクセスされる可能性のある電子計算機を、その他の電子計算機とは別のグループとし、分離する必要がある（DMZ（DeMilitalized Zone：非武装地帯）の設置）。その他の場合についても、複数の電子計算機を、その利用目的や求められるセキュリティレベル、管理部署等の違いから分離する必要があると判断する場合には、それぞれ必要な単位にグループ化し、通信回線上で分離して接続する。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(e) | 基本 | 情報システムセキュリティ責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用しアクセス制御及び経路制御を行うこと。 | **○アクセス制御と経路制御の実施**<br>・グループ化された電子計算機（2.2.4.1(1)(d)を参照のこと）の間の通信制御を行うことにより、各グループの電子計算機について必要なセキュリティレベルを確保する。具体的には例えば、グループ化された電子計算機間で情報システムの運用上必要となる通信をすべて確認し、それら必要最小限の通信を通信要件として定め、定めた通信のみを許可するように、通信回線装置（ルータ、ファイアウォール等）を利用してアクセス制御及び経路制御を行う。 | （該当せず） | （該当せず） | | | |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.4.1(1)(f) | 基本 | 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化するための機能を設けること。 | **○要機密情報を取り扱う情報システムの暗号化**<br>・情報システムが通信回線を用いて要機密情報の送受信を行う場合に、その送受信を行う通信回線について盗聴等のリスクから保護する必要性を検討し、それらのリスクから保護するために通信回線を流れる情報を暗号化する必要性があると判断する場合には、通信路を暗号化するための機能を導入する。具体的には、暗号化を行うVPN装置又はVPN機能を通信回線の両端又は電子計算機に導入し、VPN装置又は電子計算機との間の通信を暗号化する。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(g) | 基本 | 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、適切な回線を選択すること。 | **○物理的通信回線のセキュリティの検討と選択**<br>・通信回線に利用する物理的な回線の種別によって（例えば、有線LANと無線LAN等）、盗聴、改ざん等の脅威及びそれらに対する有効なセキュリティ措置が異なることから、適切な物理的な回線を選択する。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(h) | 基本 | 情報システムセキュリティ責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。 | **○遠隔地からの通信回線装置の保守に関するセキュリティ確保のための機能の導入**<br>・通信回線装置について遠隔からの保守又は診断を想定する場合に、通信回線装置で動作する保守又は診断のための機能についてセキュリティ確保のための対策を実施する。具体的には、保守作業のためのログオン機能についての主体認証の導入、接続元である電子計算機の識別コード（IPアドレス等）によるアクセス制御の実施、通信暗号化の実施等の機密性の確保に加えて、通信回線が利用できない状況での代替接続手段の確保（電話回線による接続）といった可用性の確保も考えられる。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(i) | 基本 | 情報システムセキュリティ責任者は、通信回線装置を安全区域に設置すること。 | （該当せず） | **○通信回線装置の安全区域への設置**<br>・部外者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策を講じるため、通信回線装置を安全区域に設置する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.4.1(1)(j) | 基本 | 情報システムセキュリティ責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。 | **○通信事業者のサービスの利用時の契約上の留意事項**<br>・異なる拠点にある府省庁内通信回線同士を専用線で接続する場合に、当該専用線のセキュリティレベル及びサービスレベルを確保するため、当該専用線を提供する通信事業者との契約時に、それらに関する事項を定めておく。なお、セキュリティレベル及びサービスレベルが、通信事業者の約款で定められていれば、それで代替してもよい。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(k) | 強化 | 情報システムセキュリティ責任者は、通信を行う電子計算機の主体認証を行うこと。 | **○通信を行う電子計算機の主体認証を行う機能の導入**<br>・通信相手の電子計算機が正しい相手であることを確認するため、通信を行う電子計算機の主体認証を行う機能を設ける。具体的には、例えば、IPsec通信の鍵交換プロトコルにおける、電子計算機に保管されたパスワード、鍵情報又は電子証明書を用いた電子計算機間の相互認証や、それに類似した方式の採用が考えられる。 | （該当せず） | （該当せず） | | | |
| 2.2.4.1(1)(l) | 強化 | 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な通信回線又は通信回線装置を冗長構成にすること。 | **○要安定情報システムにおける通信回線又は通信回線装置の冗長化**<br>・障害・事故等によりサービスを提供できない状態が発生した場合、サービスを提供する通信回線又は通信回線装置を代替回線又は代替通信回線装置に切り替えること等により、サービスが中断しないように、情報システムを構成する。災害等を想定して冗長構成にする場合には、被災時にも冗長構成のうち少なくとも一系統が存続可能な構成にすることが望ましい。 | （該当せず） | （該当せず） | | | |
| **(2) 通信回線の運用時** | | | | | | | | |
| 2.2.4.1(2)(a) | 基本 | 情報システムセキュリティ管理者は、通信回線装置のソフトウェアを変更する場合には、情報システムセキュリティ責任者の許可を得ること。 | （該当せず） | **○通信回線装置で利用するソフトウェアの変更**<br>・予め定めた通信回線装置のソフトウェア（2.2.4.1(1)(c)も参照のこと）について、それらのソフトウェアを変更する場合には、情報システムセキュリティ責任者の許可を得る。 | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.4.1(2)(b) | 基本 | 情報システムセキュリティ管理者は、通信回線及び通信回線装置の運用管理について、作業日、作業を行った通信回線及び通信回線装置並びに作業内容及び作業者を含む事項を記録すること。 | （該当せず） | **○通信回線及び通信回線装置の運用管理の記録**<br>・通信回線及び通信回線装置において障害等のトラブルが発生した際の原因究明につなげる目的で、通信回線及び通信回線装置に対して行われる日々の運用管理作業の記録を残すため、予め運用管理作業を記録する様式等を定めておき、それに基づき運用管理作業を記録する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.4.1(2)(c) | 基本 | 情報システムセキュリティ責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更すること。 | （該当せず） | **○他の情報システムが利用する通信回線から独立した情報システム**<br>・当該情報システムが他の情報システムと通信回線を共有している場合において、通信回線の共有によって当該情報システムのセキュリティの確保が困難であると判断する事由が発生した場合に、それらの共有を行わないように情報システムの構成を変更する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.4.1(2)(d) | 基本 | 行政事務従事者は、情報システムセキュリティ責任者の許可を受けていない電子計算機及び通信回線装置を通信回線に接続しないこと。 | （該当せず） | （該当せず） | **利用者向け手順書への反映、若しくは利用者への周知** | | （該当せず） | （該当せず） |
| 2.2.4.1(2)(e) | 基本 | 情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、通信回線装置の時刻を同期すること。 | **○通信回線装置への時刻同期機能の導入**<br>・情報システムを構成する各機器に時刻情報を配信するための機能を導入(ntpサーバの導入等）し、通信回線装置の時刻を同期させるために必要な機能の導入及び設定(ntpクライアントとしての設定等）を行う。 | **○通信回線装置の時刻同期**<br>・通信回線装置の時刻を同期させるための機能を有効化し、継続的に時刻の同期がなされるようにする。 | （該当せず） | | | |
| 2.2.4.1(2)(f) | 強化 | 情報システムセキュリティ責任者は、所管する範囲の通信回線装置が動作するために必要なすべてのソフトウェアの状態を定期的に調査し、不適切な状態にある通信回線装置を検出した場合には、当該不適切な状態の改善を図ること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。 | （該当せず） | **○通信回線装置のソフトウェアの定期的な調査と、不適切な場合の改善**<br>・通信回線装置で利用しているソフトウェアについて定期的に調査し、利用が許可されていないソフトウェアがインストールされている、ソフトウェアがセキュリティの観点で望ましくない設定になっている等の不適切な状態にある通信回線装置が存在する場合に、その状態の改善を図る。 | （該当せず） | | （該当せず） | （該当せず） |
| **(3) 通信回線の運用終了時** | | | | | | | | |
| 2.2.4.1(3)(a) | 基本 | 情報システムセキュリティ責任者は、通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体のすべての情報を抹消すること。 | （該当せず） | **○通信回線装置の内蔵記録媒体からの情報の確実な消去**<br>・通信回線装置の運用を終了する場合に、当該通信回線装置に含まれる電磁的記録媒体から、すべての情報を抹消する。抹消の方法としては、通信回線装置の初期化、内蔵電磁的記録媒体の物理的な破壊等の方法がある。 | （該当せず） | | （該当せず） | （該当せず） |
| **2.2.4.2 府省庁内通信回線の管理**<br>**(1) 府省庁内通信回線の構築時** | | | | | | | | |
| 2.2.4.2(1)(a) | 強化 | 情報システムセキュリティ責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続することを許可されたものであることを確認するための措置を講ずること。 | **○通信回線に接続する電子計算機の許可確認機能の導入**<br>・電子計算機が通信回線に論理的に接続する際に、許可された電子計算機であることを確認するための機能を、通信回線に導入する。具体的には、電子計算機固有の情報による主体認証や、IEEE 802.1xを用いた端末利用者による主体認証が考えられる。 | （該当せず） | （該当せず） | | | |
| **(2) 府省庁内通信回線の運用時** | | | | | | | | |
| 2.2.4.2(2)(a) | 強化 | 情報システムセキュリティ責任者は、通信要件の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。 | （該当せず） | **○通信要件変更の際又は定期的なアクセス制御設定の見直し**<br>・グループ化された電子計算機（2.2.4.1(1)(d)を参照のこと）の間の通信において、各グループの電子計算機について必要なセキュリティレベルを確保するために実施しているアクセス制御及び経路制御（2.2.4.1(1)(e)を参照のこと）について、通信要件（グループ間で最小限必要な通信の定め等）に変更があった場合に、あるいは定期的に（６ヶ月～１年程度）、見直しを行う。 | （該当せず） | | （該当せず） | （該当せず） |

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.4.2(2)(b) | 強化 | 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。 | **○通信回線の利用状況及び状態確認と分析、性能低下、異常の検知のための機能の導入**<br>・通信回線において想定外の大量の通信が流れることによる性能低下や通信不能、あるいは通信回線装置や通信ケーブルの障害等による通信不能等により、要安定情報を取り扱う情報システムの可用性が損なわれる事態を可能な限り回避するため、通信回線の利用状況及び状態の確認、あるいは異常等の検知を行うための機能を、通信回線に導入する。具体的には、トラフィック監視ツールの導入や、通信回線装置の状態を監視可能なシステム監視ツールの導入等が考えられる。 | **○通信回線の利用状況及び状態確認と分析、性能低下、異常の検知**<br>・通信回線において想定外の大量の通信が流れることによる性能低下や通信不能、あるいは通信回線装置や通信ケーブルの障害等による通信不能等により、要安定情報を取り扱う情報システムの可用性が損なわれる事態を可能な限り回避するため、通信回線に設置した利用状況及び状態を監視するための機能を利用して、通信回線の利用状況及び状態の監視・分析を行う。 | （該当せず） | | | |
| 2.2.4.2(2)(c) | 強化 | 情報システムセキュリティ管理者は、府省庁内通信回線上を送受信される通信内容を監視すること。 | **○府省庁内通信回線の通信内容の監視機能の導入**<br>・通信回線上を流れる情報から、不正アクセス行為の発生等を検知するため、府省庁内通信回線において侵入検知システム等の通信監視機能を導入する。 | **○府省庁内通信回線の通信内容の監視**<br>・通信回線上を流れる情報から、不正アクセス行為の発生等を検知するため、府省庁内通信回線に設置した侵入検知システム等を用いて、通信内容の監視を行う。 | （該当せず） | | | |
| **(3) 回線の対策** | | | | | | | | |
| 2.2.4.2(3)(a) | 基本 | 情報システムセキュリティ責任者は、VPN環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。<br>(ア)利用開始及び利用停止時の申請手続の整備<br>(イ)通信内容の暗号化<br>(ウ)通信を行う電子計算機の識別又は利用者の主体認証<br>(エ)主体認証記録の取得及び管理<br>(オ)VPN経由でアクセスすることが可能な通信回線の範囲の制限<br>(カ)VPN接続方法の機密性の確保<br>(キ)VPNを利用する電子計算機の管理 | **○VPN環境の構築時の対策**<br>・VPNを利用して論理的な府省庁通信回線を構築する場合に、VPNに関わる環境においてセキュリティを確保するための機能の導入や設定を行う。VPNとしては、インターネットVPN、IP-VPN、SSL-VPN，SoftEther等が考えられる。通信路の暗号化や、VPN接続利用者の主体認証等の機能の導入の他、VPNをアクセス可能な通信回線の範囲の設定や、VPN接続端末の識別コード(IPアドレス、MACアドレス等）の登録等を実施する。 | **○VPN環境の運用手続の整備と実施**<br>・VPNを利用して論理的な府省庁通信回線を構築している場合に、VPNの利用に関してセキュリティを確保するために、必要な手続を定め、実施する。具体的には、利用者のVPN接続申請及び許可の手続、識別コード及び主体認証情報の付与等の手続、識別コードに対応するアクセス制御の設定の手続等を定め、実施する必要がある。 | **利用者向け手順書への反映、若しくは利用者への周知** | | | |
| 2.2.4.2(3)(b) | 基本 | 情報システムセキュリティ責任者は、無線LAN環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。この場合、要機密情報を取り扱う無線LAN環境については、通信内容の暗号化を行う必要性があると判断すること。<br>(ア)利用開始及び利用停止時の申請手続の整備<br>(イ)通信内容の暗号化<br>(ウ)通信を行う電子計算機の識別又は利用者の主体認証<br>(エ)主体認証記録の取得及び管理<br>(オ)無線LAN経由でアクセスすることが可能な通信回線の範囲の制限<br>(カ)無線LANに接続中に他の通信回線との接続の禁止<br>(キ)無線LAN接続方法の機密性の確保<br>(ク)無線LANに接続する電子計算機の管理 | **○無線LAN環境の構築時の対策**<br>・無線LANを利用して論理的な府省庁通信回線を構築する場合に、無線LANに関わる環境においてセキュリティを確保するための機能の導入や設定を行う。無線通信路の暗号化や、無線LAN接続利用者の主体認証等の機能の導入の他、無線LAN接続端末の識別コード(MACアドレス等）の登録等を実施する。<br>なお、要機密情報を取り扱う無線LAN環境については、通信内容を暗号化する必要があるが、WEP(Wired Equivlent Privacy)等は、比較的容易に解読できるという脆弱性が報告されており、また同様の問題が起こる可能性があるため、最新の情報に従い適切な方式や設定値を選択する。この場合、暗号化については暗号と電子署名の標準手順に従う。 | **○無線LAN環境の運用手続の整備と実施**<br>・無線LANを利用して論理的な府省庁通信回線を構築している場合に、無線LANの利用に関してセキュリティを確保するために、必要な手続を定め、実施する。具体的には、利用者の無線LAN接続申請及び許可の手続、識別コード及び主体認証情報の付与等の手続、識別コードに対応するアクセス制御の設定の手続等を定め、実施する必要がある。 | **利用者向け手順書への反映、若しくは利用者への周知** | | | |
| 2.2.4.2(3)(c) | 基本 | 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。<br>(ア)利用開始及び利用停止時の申請手続の整備<br>(イ)通信を行う者又は発信者番号による識別及び主体認証<br>(ウ)主体認証記録の取得及び管理<br>(エ)リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限<br>(オ)リモートアクセス中に他の通信回線との接続の禁止<br>(カ)リモートアクセス方法の機密性の確保<br>(キ)リモートアクセスする電子計算機の管理 | **○リモートアクセス環境の構築時の対策**<br>・公衆電話網を経由したリモートアクセスを利用して論理的な府省庁通信回線を構築する場合に、リモートアクセスに関わる環境においてセキュリティを確保するための機能の導入や設定を行う。リモートアクセス接続利用者の主体認証等の機能の導入の他、リモートアクセス接続回線の登録、リモートアクセス接続端末の識別コード(MACアドレス等）の登録等を実施する。 | **○リモートアクセス環境の運用手続の整備と実施**<br>・リモートアクセスを利用して論理的な府省庁通信回線を構築している場合に、リモートアクセスの利用に関してセキュリティを確保するために、必要な手続を定め、実施する。具体的には、利用者のリモートアクセス接続申請及び許可の手続、識別コード及び主体認証情報の付与等の手続、識別コードに対応するアクセス制御の設定の手続等を定め、実施する必要がある。 | **利用者向け手順書への反映、若しくは利用者への周知** | | | |

**2.2.4.3 府省庁外通信回線との接続**
**(1) 府省庁内通信回線と府省庁外通信回線との接続時**

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.2.4.3(1)(a) | 基本 | 情報システムセキュリティ責任者は、情報セキュリティ責任者の承認を得た上で、府省庁内通信回線を府省庁外通信回線と接続すること。 | **○府省庁外通信回線との接続時の情報セキュリティ責任者からの承認**<br>・府省庁内通信回線をインターネット等の府省庁外通信回線と接続して構築する場合には、情報セキュリティ責任者の承認を得る。 | （該当せず） | （該当せず） | | | |
| 2.2.4.3(1)(b) | 基本 | 情報システムセキュリティ責任者は、府省庁内通信回線を府省庁外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線として府省庁内通信回線を構築すること。 | **○他の情報システムから独立した通信回線の構成**<br>・構築しようとする通信回線において、インターネット等の府省庁外通信回線と接続することにより情報システムのセキュリティ確保が困難な場合には、他の情報システムと共有している府省庁内通信回線から独立した通信回線として構成するか、府省庁外通信回線から切断した通信回線として構築する。 | （該当せず） | （該当せず） | | | |
| **(2) 府省庁外通信回線と接続している府省庁内通信回線の運用時** | | | | | | | | |
| 2.2.4.3(2)(a) | 基本 | 情報システムセキュリティ責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線に構成を変更すること。 | （該当せず） | **○他の情報システムから独立した通信回線構成への変更**<br>・当該情報システムが他の情報システムと通信回線を共有している場合あるいはインターネット等の府省庁外通信回線と接続している場合において、通信回線の共有によって当該情報システムのセキュリティの確保が困難であると判断する事由が発生した場合に、それらの共有又は府省庁外通信回線との接続を行わないように情報システムの構成を変更する。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.4.3(2)(b) | 基本 | 情報システムセキュリティ責任者は、通信回線の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。 | （該当せず） | **○通信回線変更の際のアクセス制御設定の見直し、及び、定期的な見直し**<br>・インターネット等の府省庁外通信回線と、府省庁内の電子計算機との間の通信において、府省庁内の電子計算機について必要なセキュリティレベルを確保するために実施している通信回線装置（ルータ、ファイアウォール等）上でのアクセス制御及び経路制御（2.2.4.1(1)(e)を参照のこと）について、通信要件（府省庁外通信回線との間で最小限必要な通信の定め等）に変更があった場合に、あるいは定期的に（６ヶ月～１年程度）、見直しを行う。 | （該当せず） | | （該当せず） | （該当せず） |
| 2.2.4.3(2)(c) | 基本 | 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。 | **○通信回線の利用状況及び状態確認と分析、性能低下と異常の検知の機能の導入**<br>・通信回線において想定外の大量の通信が流れることによる性能低下や通信不能、あるいは通信回線装置や通信ケーブルの障害等による通信不能等により、要安定情報を取り扱う情報システムの可用性が損なわれる事態を可能な限り回避するため、特に、府省庁外通信回線と直結する通信回線の利用状況及び状態の確認、あるいは異常等の検知を行うための機能を、通信回線に導入する。具体的には、トラフィック監視ツールの導入や、通信回線装置の状態を監視可能なシステム監視ツールの導入等が考えられる。 | **○通信回線の利用状況及び状態確認と分析、性能低下と異常の検知**<br>・通信回線において想定外の大量の通信が流れることによる性能低下や通信不能、あるいは通信回線装置や通信ケーブルの障害等による通信不能等により、要安定情報を取り扱う情報システムの可用性が損なわれる事態を可能な限り回避するため、特に、府省庁外通信回線と直結する通信回線に設置した利用状況及び状態を監視するための機能を利用して、通信回線の利用状況及び状態の監視・分析を行う。 | （該当せず） | | | |
| 2.2.4.3(2)(d) | 基本 | 情報システムセキュリティ管理者は、府省庁内通信回線と府省庁外通信回線との間で送受信される通信内容を監視すること。 | **○府省庁内通信回線と府省庁外通信回線間の通信内容の監視機能の導入**<br>・府省庁内通信回線と府省庁外通信回線間を流れる情報から、不正アクセス行為の発生等を検知するため、侵入検知システム等の通信監視機能を導入する。 | **○府省庁内通信回線と府省庁外通信回線間の通信内容の監視**<br>・府省庁内通信回線と府省庁外通信回線間を流れる情報から、不正アクセス行為の発生等を検知するため、通信回線に設置した侵入検知システム等を用いて、通信内容の監視を行う。 | （該当せず） | | | |

**第2.3部 個別事項についての対策**
**2.3.1 その他**
**2.3.1.1 情報システムへのIPv6技術の導入における対策**
**(1) IPv6移行機構がもたらす脆弱性対策**

| 統一基準項番 | 基本／強化 | 遵守事項 | 情報システムのライフサイクルへの適用に関わる解説 | | | 当該情報システムの評価 | | |
|---|---|---|---|---|---|---|---|---|
| | | | 設計・開発に関わる解説 | 運用・保守に関わる解説 | 他（利用者による対策、省庁対策基準等） | 本遵守事項の該当性（○：該当する ×：該当しない） | 採用する対策内容（調達者が定める場合及び自ら設計する場合に記入） | 納品時・作業完了時の確認結果（○：十分 ×：不十分） |
| 2.3.1.1(1)(a) | 基本 | 情報システムセキュリティ責任者は、情報システムにIPv6技術を利用する通信（以下「IPv6通信」という。）の機能を導入する場合には、IPv6移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。 | **○IPv6移行機構が他の情報システムに脅威を及ぼすことの防止**<br>・IPv6通信プロトコルに対応している端末やサーバ装置には、多様なIPv6移行機構（デュアルスタック機構、IPv4-IPv6トンネル機構等）が実装されている。それらのIPv6移行機構は、それぞれが想定する使用方法と要件に基づき設計されていることから、その選定と利用にあたっては、セキュリティホールの原因をつくらないよう十分な検討と措置が必要である。<br>例えば、デュアルスタック機構を運用する場合には、IPv4のプライベートアドレスを利用したイントラネットの情報システムであっても外部ネットワークとのIPv6通信が可能となるため、デュアルスタック機構を導入した電子計算機を経由した当該外部ネットワークからの攻撃について対策を講ずる必要がある。また、IPv6-IPv4トンネル機構を運用する場合、トンネルの終端が適切に管理されないと本来通信を想定しないネットワーク間のIPv6通信が既設のIPv4ネットワークを使って可能となるため、府省庁内のネットワークが外部から攻撃される危険性がある。管理された電子計算機以外のトンネル通信を当該IPv4ネットワークに設置されたファイアウォールにて遮断する等、不適切なIPv6通信を制御する対策が必要である。 | （該当せず） | （該当せず） | | | |
| **(2) 意図しないIPv6通信の抑止と監視** | | | | | | | | |
| 2.3.1.1(2)(a) | 基本 | 情報システムセキュリティ責任者は、IPv6通信を想定していない通信回線に接続されるすべての電子計算機及び通信回線装置に対して、IPv6通信を抑止するための措置を講ずること。 | **○IPv6通信を想定しない通信回線での、IPv6通信の抑止の措置**<br>・通信回線がIPv6通信を想定していない場合に、当該通信回線に接続される端末等のIPv6通信の機能を停止する措置を行う。<br>IPv6通信を想定していない通信回線においては、ファイアウォールや侵入検知システム等のセキュリティ機能に不正なIPv6通信を制御する措置が講じられず、悪意ある者によるIPv6通信を使った攻撃に対して無防備となるおそれがある。さらに、IPv6通信が可能な電子計算機においては、IPv4ネットワークに接続している時でもIPv6通信による当該電子計算機への接続を可能とする自動トンネリング機能を提供するものがある。この機能を利用すると、電子計算機と外部のネットワークとの間に利用者や管理者が気づかないうちに意図しない経路が自動生成され、これがセキュリティを損なうバックドアとなりかねないことから、自動トンネリング機能を動作させないよう電子計算機を設定する必要がある。また、ルータ等の通信回線装置についてもIPv6通信をしないよう設定し、意図しないIPv6通信を制限することが求められる。 | （該当せず） | （該当せず） | | | |
| 2.3.1.1(2)(b) | 強化 | 情報システムセキュリティ責任者は、IPv6通信を想定していない通信回線を監視し、IPv6通信が検知された場合には通信している装置を特定し、IPv6通信を遮断するための措置を講ずること。 | **○IPv6通信を想定しない通信回線での、IPv6通信の監視及び検知時の遮断のための機能の導入**<br>・意図しないIPv6通信が情報システムに与える脅威から情報システムを守るため、通信回線上でのIPv6通信を監視する機能と、IPv6通信が検知された場合に通信している装置を特定し、IPv6通信を遮断する機能を導入する。<br>IPv6技術にはアドレスの自動構成機構が提供されている。電子計算機から送出されるアドレスの自動構成を要求する通信パケットや、ルータから送出されるアドレスの自動構成を提供する通信パケットが府省庁内通信回線を流れている場合には、管理者や利用者が気づかないうちにIPv6技術のアドレス自動構成機構が利用されていることを示唆している。また、IPv6通信を想定していない府省庁内通信回線において、IPv6-IPv4トンネル機構で使用する通信パケットが検知された場合には、IPv6技術を使った悪意のある通信がなされているおそれがある。府省庁内通信回線を管理する者は、このような通信の有無を監視して、IPv6通信が検知された場合は、当該通信の遮断等の措置を講ずる必要があることから、当該通信回線において必要な機能を導入する。 | **○IPv6通信を想定しない通信回線での、IPv6通信の監視及び検知時の遮断の実施**<br>・意図しないIPv6通信が情報システムに与える脅威から情報システムを守るため、通信回線に導入したIPv6通信を監視する機能と、IPv6通信が検知された場合に通信している装置を特定し、IPv6通信を遮断する機能を利用して、必要な監視及び措置を行う。 | （該当せず） | | | |