【付録Ｂ．統一基準対応表】　※令和３年度版統一基準に対応

※本対応表は、オンプレミスの情報システムを調達する際に活用することを想定しているため、4.2外部サービスは未対

本付録は、対策要件集の「対策要件」の「実施レベル」ごとに対応する統一基準の遵守事項を「統一基準」欄に示したものである。

ID	実施レベル	仕様記載例	統一基準
AT-1-1	低位		
	中位	不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。	7.3.1(1)(a)
	高位	不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。	6.2.4(1)(b) 7.2.2(1)(a)(エ) 7.3.1(1)(a) 7.3.1(1)(b) 7.3.1(1)(j) 7.3.1(4)(a) 8.1.3(2)(a)
AT-1-2	低位		
	中位	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。	6.2.4(1)(a) 7.2.1(1)(a) 7.2.1(1)(c) 7.3.1(1)(a) 7.3.1(1)(g) 7.3.2(1)(b)(ア) 7.3.2(1)(b)(イ) 7.3.2(1)(b)(ウ) 7.3.2(1)(b)(エ) 7.3.2(2)(a)
	高位	（↑　同様）	（↑　同様）
AT-1-3	低位		
	中位	情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えること。	6.3.2(1)(a) 6.3.2(2)(a) 7.2.1(1)(c) 7.2.2(1)(a)(オ)
	高位	情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。	6.3.2(1)(a) 6.3.2(2)(a) 7.2.1(1)(c) 7.2.2(1)(a)(オ) 7.3.1(1)(d) 7.3.1(1)(j) 7.3.1(4)(a) 8.1.3(2)(a)
AT-1-4	低位		
	中位	サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。	6.2.3(1)(a)
	高位	サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。	6.2.3(1)(a) 6.2.3(1)(b)
AT-2-1	低位	不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。	6.2.2(1)(a) 6.2.2(1)(b) 6.2.4(1)(a) 6.3.1(2)(a)(ア)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）
AT-2-2	低位		
	中位		
	高位	システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。	6.2.2(1)(c)
AT-3-1	低位	情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。	6.2.1(1)(a) 6.2.1(1)(b) 6.2.4(1)(a) 6.3.1(2)(a)(イ) 7.2.2(1)(a)(ア) 7.2.2(2)(a) 7.2.4(1)(d) 7.3.2(1)(b)(イ) 7.3.2(1)(b)(ウ) 7.3.2(1)(b)(エ) 7.3.2(2)(a)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）

ID	実施レベル	仕様記載例	統一基準
AT-3-2	低位	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を行う方法（手順等）を備えること。	6.2.1(1)(d) 7.1.1(1)(b) 7.1.2(1)(c) 7.2.2(2)(a) 7.3.1(1)(i)
	中位	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。	6.2.1(1)(d) 7.1.1(1)(b) 7.1.2(1)(c) 7.2.2(2)(a) 7.3.1(1)(i)
	高位	（↑ 同様）	（↑ 同様）
AU-1-1	低位	情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、【　　】の期間保管すること。	6.1.4(1)(a) 6.1.4(1)(b) 6.2.3(1)(c) 6.2.4(1)(a) 6.2.4(1)(b) 7.1.2(2)(c) 7.3.1(1)(e) 7.3.1(1)(h) 8.1.3(2)(a)
	中位	情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、【　　】の期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。	6.1.4(1)(a) 6.1.4(1)(b) 6.1.4(1)(c) 6.2.3(1)(c) 6.2.4(1)(a) 6.2.4(1)(b) 7.1.2(2)(c) 7.3.1(1)(e) 7.3.1(1)(h) 8.1.3(2)(a)
	高位	（↑ 同様）	（↑ 同様）
AU-1-2	低位	ログの不正な改ざんや削除を防止するため、ログに関するアクセス制御機能を備えること。	6.1.4(1)(b)
	中位	ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざん等の脅威の軽減）のための措置を含む設計とすること。	6.1.4(1)(b) 6.1.5(1)(a)(ア)
	高位	ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。	6.1.4(1)(b) 6.1.5(1)(a)(ア) 6.1.5(1)(a)(イ)
AU-1-3	低位	情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。	6.1.4(1)(a)
	中位	（↑ 同様）	（↑ 同様）
	高位	（↑ 同様）	（↑ 同様）
AU-2-1	低位		
	中位	不正行為に迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。	6.2.4(1)(a) 7.3.1(1)(g) 7.3.1(1)(h)
	高位	不正行為に迅速に対処するため、府省庁内外で送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。	6.2.4(1)(a) 6.2.4(1)(b) 7.1.2(2)(c) 7.3.1(1)(g) 7.3.1(1)(h)
AU-2-2	低位		
	中位		
	高位	サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。	6.2.3(1)(c) 7.1.2(2)(c) 7.3.1(1)(f) 7.3.1(1)(g)

ID	実施レベル	仕様記載例	統一基準
AC-1-1	低位		
	中位	情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち【　　】の認証を行う機能として、【　】の方式を採用すること。	6.1.1(1)(a) 6.1.1(1)(b) 6.1.1(1)(c) 6.1.1(2)(a) 6.1.1(2)(b) 7.2.1(1)(b) 7.3.1(1)(j) 7.3.1(4)(a) 8.1.3(2)(a)
	高位	情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち【　　】の認証を行う機能として、【　】の方式を採用し、主体認証情報の推測や盗難等のリスクの軽減を行う機能として、【　　】の条件を満たすこと。	6.1.1(1)(a) 6.1.1(1)(b) 6.1.1(1)(c) 6.1.1(2)(a) 6.1.1(2)(b) 7.2.1(1)(b) 7.3.1(1)(j) 7.3.1(4)(a) 8.1.3(2)(a)
AC-2-1	低位		
	中位	主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。	6.1.1(2)(a) 6.1.1(2)(b)
	高位	（↑　同様）	（↑　同様）
AC-2-2	低位		
	中位		
	高位	情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。	6.1.2(1)(a) 6.1.2(1)(b) 6.1.3(1)(a) 7.3.1(1)(j) 7.3.1(4)(a) 8.1.3(2)(a)
AC-2-3	低位	特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。	6.1.3(1)(a) 6.1.3(1)(b) 6.2.4(1)(b)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）
PR-1-1	低位		
	中位	通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。	6.1.5(1)(a)(ア) 6.1.5(1)(b)(ア) 6.1.5(1)(b)(イ) 6.1.5(1)(b)(ウ) 6.1.5(1)(b)(エ) 6.1.5(1)(c) 6.1.5(2)(a)(イ) 7.1.2(1)(d) 7.2.1(1)(d) 7.2.2(1)(a)(オ) 7.3.1(1)(c) 7.3.1(1)(j) 7.3.1(4)(a) 8.1.3(2)(a)
	高位	（↑　同様）	（↑　同様）
PR-1-2	低位		
	中位	情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、外部との接続のある情報システムにおいて保護すべき情報を利用者が直接アクセス可能な機器に保存しないこと。	6.1.2(1)(a) 6.3.1(2)(a)(カ) 7.2.2(1)(b)
	高位	情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存しないことに加えて、保存された情報を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。	6.1.2(1)(a) 6.1.5(1)(a)(ア) 6.1.5(1)(b)(ア) 6.1.5(1)(b)(イ) 6.1.5(1)(b)(ウ) 6.1.5(1)(b)(エ) 6.1.5(1)(c) 6.1.5(2)(a)(イ) 6.3.1(2)(a)(カ) 7.1.1(4)(b) 7.1.1(5)(d) 7.2.2(1)(b)

ID	実施レベル	仕様記載例	統一基準
PR-1-3	低位		
	中位		
	高位	情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。	6.1.5(1)(a)(イ) 6.1.5(1)(b)(ア) 6.1.5(1)(b)(イ) 6.1.5(1)(b)(ウ) 6.1.5(1)(b)(エ) 6.1.5(1)(c) 6.1.5(2)(a)(ア) 6.1.5(2)(a)(イ) 6.3.1(2)(a)(エ) 7.2.2(1)(a)(オ)
PH-1-1	低位	情報の漏えいを防止するため、【　　】等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。	3.2.1(2)(b) 7.1.1(1)(a) 7.1.1(4)(b) 7.1.1(5)(d) 7.1.2(1)(a) 7.3.1(1)(e)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）
PH-1-2	低位	物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。	3.2.1(2)(b) 7.1.1(1)(a) 7.1.2(1)(a) 7.3.1(1)(e)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）
DA-1-1	低位	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに、文書どおりの構成とすること。	5.1.1(1)(b) 5.1.1(2)(a)(ア) 5.1.1(2)(a)(イ) 5.1.1(2)(a)(ウ)
	中位	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。	5.1.1(1)(b) 5.1.1(2)(a)(ア) 5.1.1(2)(a)(イ) 5.1.1(2)(a)(ウ)
	高位	（↑　同様）	（↑　同様）
DA-2-1	低位	サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として【　　】を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。	3.2.1(3)(b) 4.1.1(2)(c)(イ) 6.2.3(1)(a) 6.2.3(1)(b) 6.2.3(1)(c) 7.1.2(1)(b) 7.1.2(2)(d) 7.2.3(1)(a) 7.2.3(1)(b) 7.2.3(1)(c) 7.3.1(1)(f)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）
SC-1-1	低位	情報システムの構築において、府省庁が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、府省庁が情報セキュリティ監査の実施を必要と判断した場合は、受託者は情報セキュリティ監査を受け入れること。 また、役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して、情報セキュリティを確保すること。	4.1.1(2)(b)(ア) 4.1.1(2)(b)(イ) 4.1.1(2)(b)(ウ) 4.1.1(2)(b)(エ) 4.1.1(2)(b)(オ) 4.1.1(2)(b)(カ) 4.1.1(2)(b)(キ) 4.1.1(2)(c)(ア) 4.1.1(2)(d)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）
SC-2-1	低位	機器等の製造工程において、府省庁が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。	5.1.2(1)(a)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）

ID	実施レベル	仕様記載例	統一基準
UP-1-1	低位		
	中位	情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。	6.3.1(2)(a)(ウ) 6.3.1(2)(a)(オ) 6.3.2(1)(a) 6.3.2(1)(b)
	高位	（↑ 同様）	（↑ 同様）
UP-2-1	低位		
	中位	情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。	6.3.1(2)(a)(カ)
	高位	（↑ 同様）	（↑ 同様）