【パブリックコメント】

情報システムに係る政府調達における
セキュリティ要件策定マニュアル（案）

【付録B. 政府機関統一基準群対応表】

2011 年 1 月 31 日

【パブリックコメント】

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群の遵守事項を「統一基準群」欄に示したものである。なお、「統一基準群」欄では、下位の実施レベルには含まれない遵守事項を下線で表している。

ID	実施レベル	仕様書記載（例）	統一基準群
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、所属する府省庁の外部と通信を行う電子計算機及び内部のみと通信を行う電子計算機を通信回線上で分離すること。	2.3.4.1(1)(a) 2.3.4.1(1)(d)
	高位	不正の防止及び発生時の影響範囲を限定するため、所属する府省庁の外部との通信の有無に加えて、業務目的、情報の管理体制に応じて電子計算機を通信回線上で分離すること。	2.3.4.1(1)(a) 2.3.4.1(1)(d) 2.3.4.1(1)(e) 2.3.4.1(1)(h) 2.3.4.2(3)(a)(オ) 2.3.4.2(3)(b)(オ) 2.3.4.2(3)(b)(カ) 2.3.4.2(3)(c)(エ) 2.3.4.2(3)(c)(オ) 2.3.4.3(1)(b)
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。	2.2.2.2(1)(d) 2.2.2.4(1)(a) 2.2.2.4(1)(b) 2.3.3.1(1)(a) 2.3.3.1(1)(c) 2.3.4.1(1)(a) 2.4.1.1(1)(a) 2.4.1.1(2)(a) 2.4.1.1(2)(b)
	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、サーバの認証機能を備えること。	2.3.3.2(1)(a)(エ)

【パブリックコメント】

ID	実施レベル	仕様書記載（例）	統一基準群
	高位	情報システムのなりすましを防止するために、サーバの認証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、通信回線装置の接続を防止する機能を備えること。	2.3.3.2(1)(a)(エ) 2.3.4.1(1)(h) 2.3.4.1(1)(l) 2.3.4.2(1)(a) 2.3.4.2(3)(a)(ウ) 2.3.4.2(3)(b)(ウ) 2.3.4.2(3)(c)(イ)
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。	2.2.2.3(1)(a) 2.2.2.3(1)(b)
	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または処理量の抑制を行う等のサービス停止の脅威を軽減する対策装置を導入して情報システムを構成すること。	2.2.2.3(1)(a) 2.2.2.3(1)(b) 2.2.2.3(1)(e) 2.2.2.3(1)(f)
AT-2-1	低位	マルウェア（ウィルス、ワーム、ボット等）による脅威に備えるため、マルウェアの感染を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。	2.2.2.2(1)(a) 2.2.2.2(1)(b) 2.2.2.2(1)(c) 2.2.2.4(1)(a)
	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マルウェア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。	2.2.2.2(1)(d)

【パブリックコメント】

ID	実施レベル	仕様書記載（例）	統一基準群
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に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。	1.5.2.3(1)(a)(ス) 1.5.2.3(1)(a)(セ) 2.2.2.1(1)(a) 2.2.2.4(1)(a) 2.3.3.2(1)(a)(イ) 2.3.3.2(1)(a)(ウ) 2.3.3.2(2)(a)(ア) 2.3.3.2(2)(a)(イ) 2.3.3.2(2)(a)(ウ) 2.3.3.2(2)(a)(エ) 2.3.3.2(2)(a)(オ) 2.3.3.2(2)(a)(カ)
	中位	（↑ 同様）	（↑ 同様）
	高位	（↑ 同様）	（↑ 同様）
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。	2.2.2.1(2)(a) 2.2.2.1(2)(b)(ア) 2.2.2.1(2)(b)(イ) 2.2.2.1(2)(b)(ウ) 2.2.2.1(2)(b)(エ) 2.2.2.1(2)(b)(オ) 2.2.2.1(2)(b)(カ) 2.2.2.1(2)(b)(キ) 2.2.2.1(2)(b)(ク)
	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。	2.2.2.1(2)(a) 2.2.2.1(2)(b)(ア) 2.2.2.1(2)(b)(イ) 2.2.2.1(2)(b)(ウ) 2.2.2.1(2)(b)(エ) 2.2.2.1(2)(b)(オ) 2.2.2.1(2)(b)(カ) 2.2.2.1(2)(b)(キ) 2.2.2.1(2)(b)(ク) 2.3.2.1(2)(c)
	高位	（↑ 同様）	（↑ 同様）

【パブリックコメント】

ID	実施レベル	仕様書記載（例）	統一基準群
AU-1-1	低位	情報システムに対する不正の検知、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証跡を蓄積し、【　　】の期間保管すること。	1.5.2.4(1)(a)(オ) 2.2.1.4(1)(a) 2.2.2.3(1)(c) 2.2.2.4(1)(c) 2.3.4.2(3)(a)(エ) 2.3.4.2(3)(b)(エ) 2.3.4.2(3)(c)(ウ)
	中位	情報システムに対する不正の検知、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証跡を蓄積し、【　　】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（証跡の検索機能、証跡の蓄積不能時の対処機能等）を備えること。	1.5.2.4(1)(a)(オ) 2.2.1.4(1)(a) 2.2.1.4(1)(b) 2.2.1.4(1)(d) 2.2.2.3(1)(c) 2.2.2.4(1)(c) 2.3.4.2(3)(a)(エ) 2.3.4.2(3)(b)(エ) 2.3.4.2(3)(c)(ウ)
	高位	（↑　同様）	（↑　同様）
AU-1-2	低位	証跡の不当な消去や改ざんを防止するため、証跡に関するアクセス制御機能を備えること。	2.2.1.4(1)(c)
	中位	証跡の不当な消去や改ざんを防止するため、証跡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の脅威の軽減）のための措置を含む設計とすること。	2.2.1.4(1)(c) 2.2.1.6(1)(b)
	高位	証跡の不当な消去や改ざんを防止するため、証跡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。	2.2.1.4(1)(c) 2.2.1.6(1)(b) 2.2.1.6(1)(d)
AU-1-3	低位	不正行為の追跡や情報セキュリティ侵害時において証跡の解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。	2.3.2.2(2)(e) 2.3.2.3(2)(d) 2.3.4.1(2)(e)
	中位	（↑　同様）	（↑　同様）
	高位	（↑　同様）	（↑　同様）
AU-2-1	低位	－	－
	中位	不正行為を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。	1.5.1.1(1)(e) 2.2.2.4(1)(a) 2.3.4.2(2)(c)

【パブリックコメント】

ID	実施レベル	仕様書記載（例）	統一基準群
	高位	不正行為を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。	1.5.1.1(1)(e) 2.2.1.4(1)(e) 2.2.2.4(1)(a) 2.3.2.3(2)(e) 2.3.2.3(2)(f) 2.3.4.2(2)(c)
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。	2.3.4.2(2)(b)
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、【　　】の条件を満たす方式を採用すること。	2.2.1.1(1)(a) 2.2.1.1(1)(f)(ア) 2.2.1.1(1)(f)(イ) 2.2.1.1(1)(f)(カ) 2.2.1.1(1)(f)(キ) 2.3.3.1(1)(b) 2.3.4.1(1)(h) 2.3.4.2(3)(a)(ウ) 2.3.4.2(3)(b)(ウ) 2.3.4.2(3)(c)(イ)

【パブリックコメント】

ID	実施レベル	仕様書記載（例）	統一基準群
	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【　　】の認証を行う機能及び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、【　　】の条件を満たす方式を採用すること。	2.2.1.1(1)(a) 2.2.1.1(1)(b)(ア) 2.2.1.1(1)(b)(イ) 2.2.1.1(1)(b)(ウ) 2.2.1.1(1)(c) 2.2.1.1(1)(c)(ア) 2.2.1.1(1)(c)(イ) 2.2.1.1(1)(e)(イ) 2.2.1.1(1)(f)(ア) 2.2.1.1(1)(f)(イ) 2.2.1.1(1)(f)(ウ) 2.2.1.1(1)(f)(エ) 2.2.1.1(1)(f)(カ) 2.2.1.1(1)(f)(キ) 2.2.1.1(1)(g) 2.2.1.1(1)(h) 2.2.1.1(1)(i) 2.2.1.1(1)(j) 2.2.1.1(1)(k) 2.3.3.1(1)(b) 2.3.4.1(1)(h) 2.3.4.2(3)(a)(ウ) 2.3.4.2(3)(b)(ウ) 2.3.4.2(3)(c)(イ)
AC-2-1	低位	―	―
	中位	主体のアクセス権を適格に管理するため、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。	2.2.1.1(1)(c)(ア) 2.2.1.1(1)(c)(イ) 2.2.1.1(1)(d) 2.2.1.1(1)(e)(ア) 2.2.1.1(1)(f)(オ) 2.2.1.1(1)(f)(ク)
	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こと。	2.2.1.2(1)(a) 2.2.1.2(1)(b) 2.2.1.2(1)(c) 2.2.1.2(2)(a) 2.2.1.3(1)(a)

【パブリックコメント】

ID	実施レベル	仕様書記載（例）	統一基準群
AC-2-3	低位	アカウント管理者による不正を防止するため、アカウントの管理権限を制御する機能を備えること。	2.2.1.1(1)(l) 2.2.1.3(1)(b)
	中位	－	－
	高位	－	－
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。	2.2.1.6(1)(b) 2.3.2.3(1)(a) 2.3.3.2(1)(a)(エ) 2.3.4.1(1)(f) 2.3.4.2(3)(a)(イ) 2.3.4.2(3)(b)(イ)
	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搾取や漏えいを防止するため、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管しないこと。	2.3.3.2(1)(b)
	高位	情報システムに蓄積された情報の搾取や漏えいを防止するため、保管された情報を暗号化する機能を備えること。	2.2.1.6(1)(b) 2.3.2.2(1)(d) 2.3.3.2(1)(b)
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。	2.2.1.6(1)(d) 2.2.1.6(2)(a)
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搾取行為を防止・検知するための機能を備えること。	2.3.1.1(3)(a) 2.3.1.1(3)(c) 2.3.1.1(3)(d) 2.3.1.1(3)(e) 2.3.1.1(3)(f) 2.3.1.1(4)(d) 2.3.2.1(1)(d) 2.3.2.2(1)(e) 2.3.2.2(1)(f) 2.3.4.1(1)(g)
	中位	（↑ 同様）	（↑ 同様）
	高位	（↑ 同様）	（↑ 同様）

【パブリックコメント】

ID	実施レベル	仕様書記載（例）	統一基準群
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、安全区域に設置可能な設計とすること。	2.3.1.1(1)(a) 2.3.1.1(1)(b) 2.3.1.1(1)(c) 2.3.1.1(1)(d) 2.3.1.1(1)(e) 2.3.1.1(1)(h) 2.3.1.1(2)(a) 2.3.1.1(2)(b) 2.3.1.1(3)(b) 2.3.1.1(4)(e) 2.3.2.1(1)(b) 2.3.4.1(1)(i)
	中位	（↑ 同様）	（↑ 同様）
	高位	（↑ 同様）	（↑ 同様）
DA-1-1	低位	障害・事故等の発生要因を減らすとともに、障害・事故等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。	1.5.2.1(1)(a)(ア) 1.5.2.1(1)(a)(イ) 1.5.2.1(1)(a)(ウ) 2.2.2.4(1)(a) 2.3.2.2(1)(a) 2.3.2.3(1)(b) 2.3.2.3(1)(c) 2.3.3.2(1)(a)(ア)
	中位	障害・事故等の発生要因を減らすとともに、障害・事故等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。	1.5.2.1(1)(a)(ア) 1.5.2.1(1)(a)(イ) 1.5.2.1(1)(a)(ウ) 2.2.2.4(1)(a) 2.3.2.2(1)(a) 2.3.2.3(1)(b) 2.3.2.3(1)(c) 2.3.2.3(2)(a) 2.3.3.2(1)(a)(ア)
	高位	（↑ 同様）	（↑ 同様）

【パブリックコメント】

ID	実施レベル	仕様書記載（例）	統一基準群
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。	2.2.2.3(1)(g) 2.2.2.4(1)(b) 2.3.1.1(5)(a) 2.3.1.1(5)(b) 2.3.2.1(1)(c) 2.3.2.3(1)(e) 2.3.2.3(2)(b) 2.3.3.3(1)(a) 2.3.4.1(1)(h) 2.3.4.1(1)(k)
	中位	（↑ 同様）	（↑ 同様）
	高位	（↑ 同様）	（↑ 同様）
その他	マニュアルの利用により統一基準の遵守事項を満足する項目		1.5.1.1(1)(b) 1.5.1.1(1)(c) 1.5.1.1(1)(d) 1.5.1.1(1)(g) 1.5.2.4(1)(a)(ア) 1.5.2.4(1)(a)(イ) 1.5.2.4(1)(a)(ウ) 1.5.2.4(1)(a)(エ) 1.5.2.4(1)(a)(キ) 2.2.1.5(1)(a) 2.2.1.6(1)(a) 2.2.1.6(1)(c)