

情報システムに係る政府調達における情報セキュリティ要件策定マニュアル用ワークシート(1/4)

■ ステップ1: 目的及び業務の洗い出し (⇒ マニュアル4.1節)

【ワークシート1】

項目	内容
名称	行政情報提供システム
目的	インターネットを経由してA省の行政情報を、国民に提供するしくみを確立すること
業務	(1) 「国民」が、「行政情報提供システム」から行政情報を取得 (2) 「事務局」が、「行政情報提供システム」に行政情報を登録 (3) 「事務局」が、「行政情報提供システム」の閲覧傾向の把握と、システムの運用と管理

■ ステップ2: 業務の特徴の整理 (⇒ マニュアル4.2節)

【ワークシート2】

主体	業務	業務(細分化後)	業務(細分化後)の概要	情報	利用環境・手段
国民	行政情報の閲覧	閲覧	行政情報を表示し、内容を確認する。	「行政情報」	インターネット、PC、携帯電話、スマートフォン、タブレット端末
事務局	行政情報の登録	登録	サーバにコンテンツ(行政情報)を登録する。	「行政情報」	内部ネットワーク、業務用PC
		管理	サーバに登録済みのコンテンツ(行政情報)を更新及び削除する。	「行政情報」	
システム管理者	閲覧傾向の把握と、システムの運用と管理	利用状況の把握	利用者のアクセスした日時及び対象に関するログ等の集計を行う。	「利用統計」 (Web サイトのページ毎のアクセス)	管理用LAN、管理用PC
		不正利用及び障害の監視、追跡	アクセス状況の監視及びログ等を元にした原因究明を行う。	「アクセスログ」	
		システムのバックアップと復旧	システムのデータを定期的にバックアップ及び障害時の復旧を行う。	「システムデータ」	

情報システムに係る政府調達における情報セキュリティ要件策定マニュアル用ワークシート(2/4)

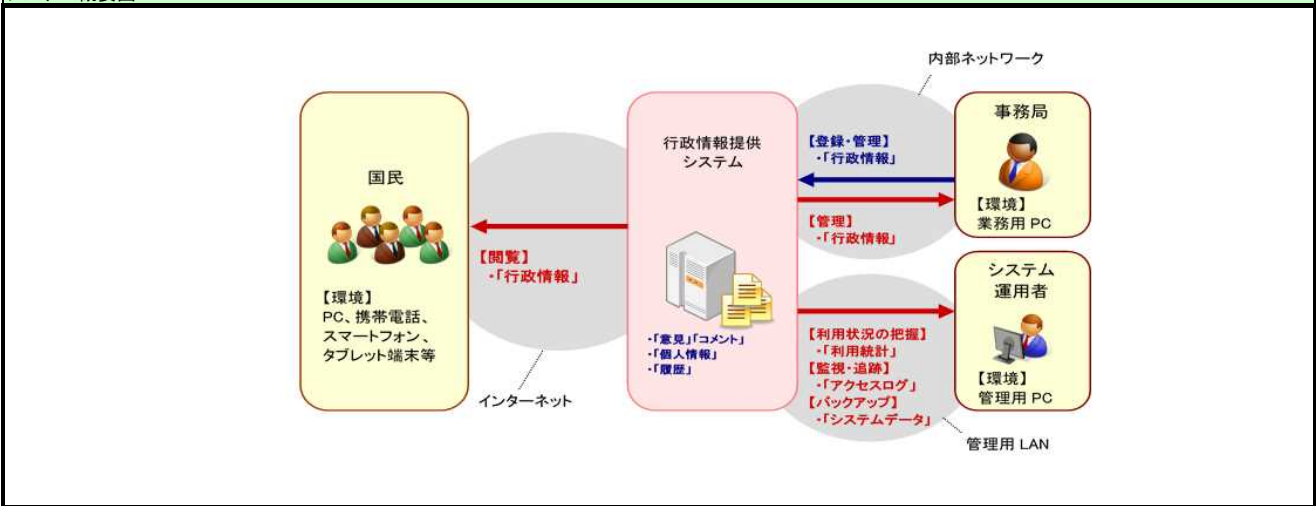
■ ステップ3: システム概要図の作成 (⇒ マニュアル4.3節)

【ワークシート3】

表記ルール

1	主体(人やシステム)を表す図形を決定する。
2	調達対象となる情報システムを図の中央付近に記載する。
3	業務(情報のやりとり)が発生する主体の間を矢印で結ぶ。
4	矢印の向きと情報の流れができるだけ一致するように業務及び情報の名称(または略称)を記載する。
5	利用環境・手段のうち、機器は機器を用いる主体の付近に記載し、ネットワークは情報のやりとりを表す矢印の付近(背景部分)に記載する。
6	サーバや端末等の機器が情報を蓄積する場合、その付近にその情報の名称を記載する。
7	すべての情報を書き込み切れない場合は各ステップの検討結果を別表に整理して採番し、図には番号等を記載する。
8	異なる主体であっても情報や利用環境・手段等に共通点がある場合には、一括して記載するなどして、図が難解にならないように工夫する。

システム概要図



■ ステップ4: 定型設問による業務要件の詳細化 (⇒ マニュアル4.4節)

【ワークシート4】

※ 必要に応じてワークシートを複数コピーして使用すること。

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	100万人程度
A-2		【主体分類】 主体の分類は？	国民
A-3		【集合特性】 特定か不特定か？	不特定(匿名性あり)
A-4		【所属】 システム所管部署との関係は？	府省庁外
A-5		【頻度】 1人あたりのアクセス頻度は？	年に数回程度
A-6		【利用時間】 1日の主な利用時間帯は？	特定できない(24時間)
A-7		【信頼性】 役割どおりに振る舞えるか？	誤操作が発生しやすい(マニュアル等を読まない)
B-1	情報	【数量】 おおよそのデータ量は？	「行政情報」: 数百KB~数十MB程度
B-2		【所有者】 情報の所有者は誰か？	「行政情報」: システム所管部署
B-3		【範囲】 公開・提供可能な範囲は？	「行政情報」: 公開
B-4		【漏えい】 漏えい時の影響度は？	「行政情報」: なし
B-5		【改変】 不正改変時の影響度は？	「行政情報」: 行政の信頼が損なわれる
B-6		【取扱】 閲覧のみか？変更が発生するか？	変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存(保存期限あり)
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	Webブラウザ
C-2		【処理環境】 サーバ又は端末の種類は？	PC、携帯電話、スマートフォン等
C-3		【通信環境】 利用するネットワークは？	インターネット
C-4		【通信環境】 外部からの遠隔利用は必要か？	必要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

情報システムに係る政府調達における情報セキュリティ要件策定マニュアル用ワークシート(3/4)

■ ステップ5: 判断条件による対策方針の検討 (⇒ マニュアル5.1節)

【ワークシート5】				
名称	観点分類	判断条件	解説	判断結果
A. 外部アクセスの有無	利用環境・手段	インターネット等の通信回線を介して(情報の管理ポリシーが異なる)外部から情報システムにアクセスしてサービスの利用、業務の遂行、情報システムの管理等を行うか。	情報システムを所管する組織の外部(情報管理ポリシーが異なる外部)からアクセスを受ける可能性を検討する。判断にあたっては、ステップ2の利用環境・手段の検討結果、定型設問C-3、C-4等を参考にすると良い。	○
B. 情報の重要度	情報	漏えいした場合、正常にアクセスできない場合或いは消失した場合に、深刻な損害を被る可能性がある重要な高い情報を取り扱うか。	漏えい、改ざん、消失等によって発生するプライバシー侵害や金銭的被害等の損害の度合いを見極め、情報の重要性を検討する。判断にあたっては、例えば、定型設問B-3の情報の取り扱い範囲、B-4、B-5の損害度合の回答を参考にすると良い。	×
C. 情報保存時の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	情報の重要性が非常に高く物理対策が突破されることも想定する必要がある場合、あるいはモバイルPCによる情報処理が必要な場合などは追加的対策が重要になる。判断にあたっては、定型設問B-7にてシステム内に保存することを確認している場合かつ定型設問B-4、B-5の想定被害の程度を考慮すると良い。	×
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	情報システムのサービスや業務機能を、特定の利用者や運用者のみに提供するか否かを検討する。判断にあたっては、定型設問A-3にて確認された主体の集合特性を参考にすると良い。	×
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	利用者や運用者に応じてアクセス権を管理し、アクセス権に応じてサービスや業務機能の提供内容を制御する必要があるか否かを検討する。例えば、ステップ2にて情報システムの利用者として多様な主体が洗い出され、主体の種類ごとに提供する機能やサービスを切り替える等の制御が必要である場合には本判断条件に合致する可能性がある。	×
F. 複数部局による利用	主体	情報の取り扱い方や利用目的等が異なる複数の部局等の中で共用されるか。	情報システムを広く共用するが、情報システム内の情報管理体制の異なる部局ごとに分け、互いにアクセスできない状態を保つ必要があるか否かを検討する。例えば、ステップ2にて情報システムを利用する主体として多様な主体が洗い出され、各主体の所属が情報管理ポリシーの異なる部局である場合に本判断条件に合致する可能性がある。	×

■ ステップ6: 対策要件の決定 (⇒ マニュアル5.2節)

「推奨レベル」はワークシート5の記入内容に従って自動的に変化します。推奨レベルを参考にして「検討結果」に実施レベルを入力してください。対策を省略する対策要件については、検討結果を空欄にしてください。

【ワークシート6】					
対策区分	対策方針	対策要件	判断条件 対応関係	実施レベル	
				推奨レベル	検討結果
侵害対策 (AT: Attack)	通信回線対策(AT-1)	AT-1-1 通信経路の分離	A or F	中位 or 高位	中位
		AT-1-2 不正通信の遮断	A	中位	中位
		AT-1-3 通信のなりすまし防止	A	中位 or 高位	中位
		AT-1-4 サービス不能化の防止	A	中位 or 高位	中位
	不正プログラム対策(AT-2)	AT-2-1 マルウェアの感染防止	-	低位	低位
		AT-2-2 マルウェア対策の管理	A or B	省略 or 高位	
	セキュリティホール対策(AT-3)	AT-3-1 構築時の脆弱性対策	-	低位	低位
AT-3-2 運用時の脆弱性対策		A	中位	中位	
不正監視・追跡 (AU: Audit)	証跡管理(AU-1)	AU-1-1 証跡の蓄積・管理	B or C	低位	低位
		AU-1-2 証跡の保護	B or C	低位	低位
		AU-1-3 時刻の正確性確保	-	低位	低位
	不正監視(AU-2)	AU-2-1 侵入検知	A	中位 or 高位	中位
		AU-2-2 サービス不能化の検知	A	省略 or 高位	
アクセス・利用制限 (AC: Access)	主体認証(AC-1)	AC-1-1 主体認証	D	省略	
		AC-2-1 ライフサイクル管理	D	省略	
	アカウント管理(AC-2)	AC-2-2 アクセス権管理	E	省略	
		管理者権限の保護	-	低位	低位
データ保護 (PR: Protect)	機密性・完全性の確保(PR-1)	PR-1-1 通信経路上の盗聴防止	B or C	省略	
		PR-1-2 保存情報の機密性確保	B or C	省略	
		PR-1-3 保存情報の完全性確保	B or C	省略	
			-	低位	低位
物理対策 (PH: Physical)	情報搾取・侵入対策(PH-1)	PH-1-1 情報の物理的保護	-	低位	低位
		PH-1-2 侵入の物理的対策	-	低位	低位
障害対策(事業継続対応) (DA: Damage)	構成管理(DA-1)	DA-1-1 システムの構成管理	B	低位	低位
		DA-2-1 システムの可用性確保	-	低位	低位
サプライチェーン・リスク対策 (SC: Supply Chain)	情報システムの構築等の外部委託における対策(SC-1)	SC-1-1 委託先において不正プログラム等が組み込まれることへの対策	-	低位	低位
		機器等の調達における対策(SC-2)	SC-2-1 調達する機器等に不正プログラム等が組み込まれることへの対策	-	低位
利用者保護 (UP: User Protect)	情報セキュリティ水準低下の防止(UP-1)	UP-1-1 情報セキュリティ水準低下の防止	A	中位	中位
		UP-2-1 プライバシー保護	A	中位	中位

情報システムに係る政府調達における情報セキュリティ要件策定マニュアル用ワークシート(4/4)

■ ステップ7: 調達仕様書記載内容の整理 (⇒ マニュアル5.3節)

各項目の「記載内容」はワークシート1及びワークシート6の内容に従って自動的に変化します。

【ワークシート7】			
大項目	小項目	記載内容	
ア 調達案件の概要	(1) 調達背景		
	(2) 目的	インターネットを経由してA省の行政情報を、国民に提供するしくみを確立すること	
	(3) 期待する効果		
	(4) 業務・情報システムの概要	(※ ステップ2及びステップ4の結果を反映)	
	(5) 契約期間		
	(6) 作業スケジュール等		
イ 調達案件及び関連調達案件の調達単位、調達の方式等	(1) 調達案件及びこれと関連する調達案件の調達単位		
	(2) 調達の方式		
	(3) 実施時期等		
ウ 情報システムに業務要件求める要件	機能要件	(1) 業務実施手順	
		(2) 規模	
		(3) 時期・時間	
		(4) 場所等	
		(5) 管理すべき指標	
		(6) 情報システム化の範囲	
		(7) 業務の継続の方針等	
		(8) 情報セキュリティ	
	非機能要件	(1) ユーザビリティ及びアクセシビリティ	
		(2) システム方式	
	(3) 規模		
	(4) 性能		
	(5) 信頼性	DA-2-1 システムの可用性確保 ・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。	
	(6) 拡張性		
	(7) 上位互換性		
	(8) 中立性		
	(9) 継続性		
	(10) 情報セキュリティ	AT-1-1 通信経路の分離 ・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。 AT-1-2 不正通信の遮断 ・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にて遮断する機能を備えること。 AT-1-3 通信のなりすまし防止 ・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。 AT-1-4 サービス不能化の防止 ・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。 AT-2-1 不正プログラムの感染防止 ・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。	
		AU-1-1 ログの蓄積・管理 ・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。	
		AU-1-2 ログの保護 ・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。	
		AU-1-3 時刻の正確性確保 ・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。	
		AU-2-1 侵入検知 ・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。	

大項目	小項目	記載内容
		AC-2-3 管理者権限の保護 ・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。
		DA-1-1 システムの構成管理 ・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。
		SC-2-1 調達する機器等に不正プログラム等が組み込まれることへの対策 ・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。
		UP-1-1 情報セキュリティ水準低下の防止 ・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。
		UP-2-1 プライバシー保護 ・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。
	(11) 情報システム稼働環境	(※ ステップ3にて作成したシステム概要図を記載)
	(12) テスト	AT-3-1 構築時の脆弱性対策 ・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。
	(13) 移行	-
	(14) 引継ぎ	-
	(15) 教育	-
	(16) 運用	PH-1-1 情報の物理的保護 ・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。
		PH-1-2 侵入の物理的対策 ・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。
	(17) 保守	AT-3-2 運用時の脆弱性対策 ・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。
エ 作業の実施内容	(1) 作業の内容 (2) 成果物の範囲 (3) 納品期日等	-
オ 作業の実施体制・方法	(1) 作業実施体制	SC-1-1 委託先において不正プログラム等が組み込まれることへの対策 ・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。
	(2) 作業要員に求める資格要件 (3) 作業の管理に関する要領等	-
カ 作業の実施	(1) 機密保持 (2) 資料の取扱い (3) 遵守する法令等	-
キ 成果物の取扱い	(1) 知的財産権の帰属 (2) 瑕疵担保責任 (3) 検取等	-
ク 入札参加資格	(1) 入札参加要件 (2) 入札制限	-
ケ 再委託	(1) 再委託の制限並びに再委託を認める場合の条件 (2) 承認手続 (3) 監査及び再委託先の契約違反等に関する責任についての定め等	-
コ その他特記事項	(前提条件、制約条件、要件定義、調達仕様書の変更手順等)	-
サ 附属文書	(1) 要件定義書 (2) 参考資料 (3) 事業者が閲覧できる資料一覧表 (4) 閲覧要領 (5) 提案書等の審査要領 (6) その他事業者の提案に必要な資料	-

※ 二重下線(青字)の箇所については、仕様書に記載する際には具体化が必要な箇所である。

対策区分	対策方針	対策要件の名称	判断条件 対応関係	目的	実施レベル選定の考え方	仕様書記載時の注意事項	実施 レベル	想定脅威	対策の効果	仕様記載例	対策の提案例	
AT 侵害対策	AT-1 通信回線対策	AT-1-1 通信経路の分離	A or F	不正行為の影響範囲を限定的にするため、業務に応じて通信経路(ネットワーク)の分離を行うこと。	・ネットワークを情報の管理体制が異なる(情報の共有があってはならない)複数部局で共用する場合、あるいは利用部局が多岐に渡り統制が取りづらい場合等では、不正アクセス等の危険性が高まるため、「高位」の実施レベルが必要となる可能性がある。 ・分離の方法によってはコストが高まることから、「(AC)アクセス・利用制限」等の他の対策を行い、本対策は「中位」に留める方法が考えられる。	・仕様書記載例をそのまま調達仕様書に記載する場合、提案によっては多大な費用を要する場合があるため、分離の条件(分離単位、分離方法等)をできるだけ具体的に記載すること。	低位	通信回線を介して外部からアクセス可能な機器等が仮に繋がれたとしても内部ネットワークの他の機器等に被害が及ぶ可能性を低くすることができる。	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。	・DMZの構築による外部アクセス向けネットワークの分離		
							中位	なんらかの高度な攻撃手法、あるいは内部関係者によって、内部ネットワークの機器等に不正行為が行われる。	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。	・VLAN、専用回線等による提供サービス、利用目的、部局等に応じたネットワークの分離 ・重要な情報を保有するサーバ装置等のネットワークと他のネットワークの分離とアクセス制御 ・情報システムの運用または管理に用いる端末専用ネットワークの構築 ・VPN、無線LAN、公衆電話網を介したアクセスが可能なネットワークの制限		
							高位	(1 同様)	(1 同様)	(1 同様)	(1 同様)	
		AT-1-2	A	許可されていない不正な通信を防止するため、特定の通信を遮断すること。	(特になし)	(特になし)	低位	通信プロトコルの脆弱性やサーバ装置等の既定不備を悪用して、不正行為が行われる。	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以上に遮断する機能を備えること。	・ファイアウォール、WAF、リバースプロキシ等による通信制御 ・通信回線装置による特定の通信プロトコルの利用制限 ・IDS/IPSによる不正アクセスの検知・遮断 ・UTM(統合脅威管理)の導入 ・サーバ装置による不要な通信プロトコルの停止 ・サーバ装置による不正なメールの検疫及び中継の遮断		
		AT-1-3	A	通信回線を介したなりすましによる不正を防止すること。	・高位レベルの対策は、情報システムを構成する機器(端末、サーバ装置、通信回線装置)が多い場合、多大なコスト増加を招くおそれがある。	(特になし)	低位	(1 同様)	(1 同様)	(1 同様)	(1 同様)	
		AT-1-4	A	トラフィック集中によるサービス不能化の防止	・高位レベルが求めるDDoS対策機能を備えた専用装置の導入費用は、中小規模の情報システムにとって負担が大きいため、情報システムの停止した場合の利用者への影響が許容できる場合は中位レベルに留めることが考えられる。	(特になし)	低位	大量のアクセス等によってサービス提供が不能な状態または困難な状態に陥る。	情報システム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。	・機器等の通信機能の設定の最適化(パケットフィルタリング、タイムアウト時間の短縮等)		
		AT-2	AT-2-1 不正プログラムの感染防止	-	不正プログラムによる情報漏えい等の被害を防止するため、不正プログラムの感染防止の対策を行うこと。	(特になし)	(特になし)	低位	情報システムが不正プログラム(ウイルス、ワーム、ボット等)に感染し、情報漏えい等の被害を受ける。	不正プログラムの感染防止、感染時の被害拡大の防止が可能になる。	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。	・不正プログラム対策ソフトウェアの導入 ・不正プログラム検出パターンファイル等の手動または自動更新 ・検査方式が異なる複数の不正プログラム対策ソフトウェアの導入 ・ふるまい検知型の不正プログラム対策ソフトウェアの導入 ・検疫ネットワークの導入
		中位						(1 同様)	(1 同様)	(1 同様)	(1 同様)	
		高位						(1 同様)	(1 同様)	(1 同様)	(1 同様)	
		AT-2-2	A or B	不正プログラム対策の最新化を確実にするため、不正プログラムの対策状況を管理すること。	・情報システムを構成する各機器において不正プログラム対策機能の自動更新が可能である場合や、管理する機器が少なく更新漏れが発生する可能性が低い場合には、高位レベルの対策は必要性が低い。	(特になし)	低位	情報システムの一部の構成機器について、不正プログラム対策機能が最新化されていないことが原因で不正プログラムに感染してしまう。	情報システム全体について、不正プログラム対策機能の稼働状況を把握し、感染のおそれがある機器を検出し、改善できる。	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。	・情報システムを構成する各装置における不正プログラム対策ソフトウェアの統合管理機能	
		AT-3	AT-3-1 構築時の脆弱性対策	-	情報システムの脆弱性をついた攻撃を予め防ぐため、脆弱性の有無を確認し対処すること。	(特になし)	・脆弱性の有無の点検方法については、「対策の提案例」を参考にするなどして、最低限満たすことを求める条件を具体的に記載することが望ましい。	低位	開発時の脆弱性の混入、ソフトウェアの更新漏れ、設定誤り等によって安全ではない状態で構築された情報システムに対して不正行為が行われる。	開発時や構築時の脆弱性の混入や残存を防止、より安全な情報システムを調達することができる。	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。	・コーディング規約によるセキュアコーディングの徹底 ・リリース済みのパッチの適用及びソフトウェアの最新化 ・利用するソフトウェアのサポート期間の考慮 ・不審なプログラムの実行の禁止 ・不要なサービス、機能等の停止 ・不要な通信の制限 ・IPv6を考慮した実装 ・ツール等によるサーバ装置、通信回線装置、ウェブアプリケーション、データベース管理システム等の脆弱性診断(内部検査又は第三者検査)の実施 ・WAF等によるSQLインジェクションの脆弱性対策
		中位						(1 同様)	(1 同様)	(1 同様)	(1 同様)	
高位	(1 同様)	(1 同様)						(1 同様)	(1 同様)			
AT-3-2	A	運用開始後に発見される脆弱性について、その改善を行うための対策を実施すること。	・管理すべきハードウェアやソフトウェアの数が多いため、脆弱性の対処漏れが発生する可能性が高くなるため、中位レベルの対策が望ましい。 ・管理対象が少ない場合でも、使用しているハードウェアやソフトウェアの脆弱性の発見頻度が高い場合、あるいは取り扱う情報の重要度が高い場合には、中位レベルの対策によって脆弱性の対処漏れを防止すると良い。	(特になし)	低位	情報システムの運用開始後に発見された新たな脆弱性を利用して、不正行為が行われる。	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(手続等)を備えること。	・情報システムを構成する各装置に対するパッチ適用、バージョンアップ及び管理方法の手順化 ・ツール等によるサーバ装置、通信回線装置、ウェブアプリケーション等の定期的な脆弱性診断(内部検査又は第三者検査)の実施 ・情報システムを構成する各装置に対するパッチ適用、バージョンアップの更新機能の導入 ・情報システム全体の更新状況の一元管理				
中位	情報システムの一部の構成機器について、新たに発見された脆弱性の対処が漏れたことが原因で、不正行為が行われる。	情報システム全体について、脆弱性の対処状況を把握し、悪用されるおそれがある脆弱性については漏れなく対処できる。	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。	(1 同様)								
高位	(1 同様)	(1 同様)	(1 同様)	(1 同様)								

対策区分	対策方針	対策要件の名称	判断条件 対応関係	目的	実施レベル選定の考え方	仕様書記載時の注意事項	実施 レベル	想定脅威	対策の効果	仕様記載例	対策の提案例		
AU 不正監視・追跡	AU-1 ログ管理	AU-1-1 ログの蓄積・管理	B or C	不正行為の検知、原因追 求を行うため、情報シス テムのログの収集・蓄 積・保管を行うこと。	・ログ管理は、情報システムの利用頻度、不正行為の発生頻度及び 侵害発生時の影響を想定し、費用対効果を踏まえた実施レベルを導 入することが望ましい。	・ログ管理は、情報システムのストレージで も、不正行為の検知、発生原因の特定及び 被害内容の把握等が困難になる。また、 費用面での負担は大きい。ログの保存内容・ 期間は、情報システムへの不正行為の検知・ 原因追跡に必要な内容等を考慮した期間を【 】の箇所に記載すること。	低位	アクセス記録等のログがないことによ って、不正行為の検知、発生原因の特定及び 被害内容の把握等が困難になる。また、不 正行為への対応が可能となる。	必要な情報をログとして確保することで、 不正行為の検知、発生原因の特定及び被害 内容の把握等の一助となり、不正行為への 対応が可能となる。	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。	・サーバ装置のアクセス記録、主体認証のログ、操作ロ グ及び通信回線装置の通信ログの取得		
							中位	アクセス記録等のログが蓄積されているに も関わらず、ログの管理機能に不足がある ことで、不正行為に対する対応の即時性・的 確性が向上することで、被害防止や低減を図 れる。	適切に管理されたログから不正行為を迅速 かつ的確に把握することが可能になり、不 正行為に対する対応の即時性・的確性が向 上することで、被害防止や低減を図れる。	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。	・ログ管理サーバによるログの一元管理 ・ログの検索、集計、追跡等の分析機能 ・ログ及び分析結果の表示・通知機能 ・ログの蓄積不能時の対処機能 ・外部ログサーバへの出力機能		
							高位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）		
		AU-1-2 ログの保護	B or C	不正行為のログに対する 改ざんや削除を防止する ため、ログの保護を行う こと。	・ログの保護は、本対策区分以外（侵害対策、アクセス/利用制限 等）の対策状況を踏まえて、実施レベルを選定するのが望ましい。	（特になし）	低位	情報システムの運用者または管理者による 悪意や誤操作によって、ログの改ざんや削 除が行われる。	ログにアクセス可能な者を必要最小限に絞 ることによって、ログの改ざんや削除が行 われる可能性を低減できる。	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。	（【 】 同様）	（【 】 同様）	・サーバ装置や通信回線装置のログに対するアクセス制 御
							中位	外部記憶媒体等に保存したログのアーカイ ブデータのように、情報システムのアクセ ス制御外になったログに対し、改ざんや削 除が行われる。	情報システムのアクセス制御外になったロ グのアーカイブデータに対して、改ざんや 削除が行われる可能性を低減できる。	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。	・ログのアーカイブデータの暗号化 ・ログの定期的なアーカイブ（ログのローテーション及 び圧縮等を含む） ・ログ保存メディアのライトワンス（1回書込、追記不 可）メディア使用 ・鍵付きロッカーによる保管		
							高位	不正アクセスによるログの改ざんや削除が 行われる。また、ログ管理装置の障害に よって、ログが破損・消失される。	不正アクセスによるログの改ざんや削除を 検知することで、不正行為に対する対応の 即時性が向上する。また、装置故障による ログの破損・消失する可能性を低減でき、 ログの信頼性向上も図れる。	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追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。	・信頼性の高い記憶装置の導入、ログ管理装置の冗長化 ・電子署名、タイムスタンプ等によるログの完全性保証 ・改ざん検知システムによるログの監視		
	AU-1-3 時刻の正確性 確保	-	ログの発生時刻を正確に 把握することで正確な分 析を行うため、システ ム全体の時刻を同期させ ること。	（特になし）	低位	標準時刻に対し、情報システムのシステム 時刻が不正確であったり、各構成機器間の システム時刻が不整合であることで、ログ の内容を正しく解釈できなくなる。	情報システムのシステム時刻を正確かつ整 合をとることで、情報システム内部（ア クセス制御内）の各種ログ及び、外部保存 （アクセス制御外）の各種ログについて、 事象及び関係性を正しく解釈でき、正確な 分析を行える。	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。	・NTPによる時刻同期 ・GPS等の正確な時刻ソースの利用				
					中位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）				
					高位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）				
	AU-2 不正監視	AU-2-1 侵入検知	A	外部ネットワークから侵 入による情報セキュリ ティの侵害を防止するた め、不正侵入の検知を行 うこと。	・高レベルの対策を実施する場合、装置の数に応じて費用が増大 するため、費用対効果を踏まえた実施優先度を定めることが望まし い。 ・情報システムの運用者や利用者が多岐に渡り、運用の統制やセ キュリティ確保が困難な場合などには、中レベルでは迅速に対応 できない可能性があるため、高レベルの対策が有効に働く場合 がある。	（特になし）	低位	通信回線を介した外部からの不正アクセ スに気づくことができず、対処が遅れる。	外部からの不正アクセスを検知することで 迅速な対応が可能となり、侵入被害を抑制 することができる。	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。	・IDS/IPSによる通信回線の上の不正な通信パケットの検 知やファイアウォールの連携による通信制御 ・マルウェアによって発生する不審な通信の検知		
							高位	高度な通信の擬装によって通信の監視では 不正を検知できず、侵入を許してしまう。	サーバ装置における監視によって、高度な 通信の擬装や内部機器を介した攻撃に対 しても、不正検知の可能性が高まる。	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。	・IDS/IPSによるサーバ装置等の通信ポートの監視 ・システムの負荷、リソースの使用状況の監視		
		AU-2-2 サービス不能 化の検知	A	トラフィック集中による サービス不能化を検知す ること。	・高レベルが求める検知機能の導入は、情報システムが停止した 場合の影響度（利用者へのサービス停止が許容可能かどうか等） と、費用対効果を十分に踏まえた上で検討することが望ましい。	（特になし）	低位	サービス不能化を目的とした攻撃の検知が 遅れ被害が深刻化し、サービス提供が困 難になる。	攻撃の検知の可能性が高まり、早期対応に よって被害を抑制できる。	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。	・IDS/IPSまたは通信回線装置による異常トラフィック の監視、検知 ・システムの負荷、リソースの使用状況の監視		
高位							（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）			
AC アクセス・利 用制限	AC-1 主体認証	AC-1-1 主体認証	D	許可されていない利用者 のアクセスを防止するた め、アクセス主体を認証 するための機能を備える こと。	・主体認証の安全性は、利便性やコストとトレードオフの関係にあ るため、「行政手続におけるオンラインによる本人確認の手法に関 するガイドライン（平成31年2月25日 各府省情報化統括責任者 （CIO）連絡会議決定）」を参考にして、合理的に対策要件を決定 する。	・仕様書記載例の【 】の箇所に 関して、「行政手続におけるオンラインによる本人確認の手法に関 するガイドライン」を参考とする等して認証が必要な主体ごとに認証方 式の条件を具体的に明記すること。	低位	許可されていない利用者が情報システムに アクセスすることを許してしまう。	正当な利用者のみアクセスを許可し、無 許可の利用者のアクセスを禁止できる。	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。	・識別コード（ID）とパスワードによる主体認証 ・パスワード規則の設定（文字列の長さの規定、文字種 の規定等） ・送信又は保存時の主体認証情報の暗号化 ・保存された主体認証情報へのアクセス制御		
							中位	他人の主体認証情報（パスワード等）の推 測や盗難等によって不正アクセスが行われ る。	主体認証情報の推測、盗難等によるリスク を軽減し、主体認証機能の安全性が高ま る。	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 とし、 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。	・ワンタイムパスワードによる主体認証 ・耐タタビ性を備えたICカード認証 ・生体認証（指紋、顔、静脈、虹彩等） ・2つ以上の主体認証方式を用いて認証を行う多要素主 体認証方式 ・情報システムの認証履歴の記録と通知 ・指定回数以上の認証失敗時のアクセス拒否 ・大規模な録書を用いたパスワード鑑折への耐性		
							高位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）		
		AC-2 アカウント管 理	AC-2-1 ライフサイク ル管理	D	不要なアカウントによる 不正な操作等を防止す るため、適切に識別コー ド、認証情報等のライフ サイクルを管理するこ と。	（特になし）	低位	不要アカウントの残存、不正なアカウント 登録や変更等が原因で、情報システムに 対する不正アクセスが引き起こされる。	厳格なアカウント管理が可能となり、許可 されていない利用者によって情報システム が利用される可能性を低減できる。	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。	・アカウントを一元的に管理する機能 ・識別コード（ID）、主体認証情報の作成、配付機能 ・主体認証情報の変更状況を把握する機能 ・特定の識別コード（ID）による認証を停止する機能		
							中位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）		
							高位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）		
	AC-2-2 アクセス権管 理	E	許可されている情報のみ にアクセスできるように 、職務等に応じたアク セス権の管理を行うこ と。	・情報システムの利用者の職務（情報システムが提供するサービ スの内容）が一定である場合には主体認証のみで対応可能であるが、 利用者（主体）によってアクセスする情報や利用するサービスが異 なる場合には高レベルの対策要件が必要になる。	（特になし）	低位	不要な情報やサービスに誤って又は意図 的にアクセスされ、情報漏えいや情報の不正 な操作が行われる。	職務に応じて必要最小限のアクセス権を利 用者に与えることによって、不正の防止や 侵害時の被害を抑制できる。	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。	・利用時間や利用時間帯によるアクセス制御 ・同一IDによる複数アクセスの禁止 ・IPアドレスによる端末の制限 ・ネットワークセグメントの分割によるアクセス制御 ・情報の格付及び取扱制限によるアクセス制御			
						中位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）			
						高位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）			
	AC-2-3 管理者権限の 保護	-	管理者権限の悪用による 不正行為を防止するた め、管理者権限を適切に 保護すること。	（特になし）	低位	情報システムの管理者権限が悪用され、通 常の利用者ではアクセスできない情報の窃 取等の不正行為が行われる。	管理者権限を正当な者のみに与えて悪用を 防止するとともに、管理者権限の内容を必 要最小限に絞って被害を抑制できる。	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。	・システムの管理、運用に用いるシステムアカウントを一 元的かつ厳格に管理する機能 ・最小限の特権の付与 ・複数名による操作が必要なデュアルロック機能の導入				
					中位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）				
					高位	（【 】 同様）	（【 】 同様）	（【 】 同様）	（【 】 同様）				

対策区分	対策方針	対策要件の名称	判断条件 対応関係	目的	実施レベル選定の考え方	仕様書記載時の注意事項	実施 レベル	想定脅威	対策の効果	仕様記載例	対策の提案例			
PR	データ保護	機密性・完全性の確保	PR-1-1	通信経路上の盗聴防止	B or C	通信経路上に流れるデータが盗聴された場合でも影響を低減させるための措置を行うこと。	(特になし)	低位 中位	通信回線に流れるデータの盗聴によって、情報が窃取される。	通信回線の暗号化によって、仮に通信が盗聴されたとしても、意味のある情報が取得される可能性を低減できる。	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。	・IPsecによるIPレベルでの暗号化 ・SSL-VPN等のVPNによる仮想的な専用回線での接続 ・SSL/TLSによるHTTP通信の暗号化 ・情報の暗号化を行う製品の導入 ・S/MIME等のセキュアメールシステム		
			PR-1-2	保存情報の機密性確保	B or C	保存されているデータの窃取を防止するため処置及び窃取された場合に影響を低減させるための措置を行うこと。	・取り扱う情報の機密性の高さを考慮して、高度な攻撃手法により情報の保存場所に直接アクセスされ、情報が窃取される脅威や、内部犯行により情報が漏えいする脅威を想定する必要がある場合に高位の対策を講ずることが考えられる。 ・端末に保護すべき情報を保存する必要がある場合、端末に保存する情報についても上記と同様の対策要件を求める必要がある。	・保護すべき情報の保存場所が複数想定される場合には、保存場所ごとに対策要件を定めること。	低位 中位	情報にアクセスする必要の無い利用者がアクセスし、情報が窃取される。また、外部との接続のある情報システムにおいて、通信回線を介した外部からの不正アクセスによって情報が窃取される。	アクセス権に関する対策により情報にアクセスする必要の無い利用者が、アクセスすることを制限すること、また、外部との接続のある情報システムにおいては外部から直接アクセス可能な機器には保護すべき情報を保存しないことにより、不正アクセスによる情報漏えいの被害を抑制できる。	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、また、外部からの高度な攻撃手法により情報の保存場所に直接アクセスされ、情報が窃取される。また、内部犯行により情報が窃取される。	・情報へのアクセス権を制御する機能 ・情報を保存する機器の内部ネットワークへの設置	
			PR-1-3	保存情報の完全性確保	B or C	情報が不正に改ざんされることを防止するため、システムが取り扱う情報の完全性を確保すること。	・通信回線を流れる情報の完全性の確保についてはPR-1-1の対策要件でも効果があり、本対策の必要性は高くない。 ・サーバ機器、端末等に保存された情報の完全性の確保については、PR-1-2と同様に利用者の信用度、利用環境を考慮し、必要性が認められる場合にのみ高位レベルの対策を採用すると良い。	(特になし)	低位 中位 高位	情報システムに不正アクセスし、情報システムが保存する情報が改ざんされる。	情報が改ざんされた場合にその事実を検知し、早期に対処することができる。	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。	・デジタル署名又はタイムスタンプ ・原本性保証システム ・S/MIME等のセキュアメールシステム	
			PH	物理対策	PH-1	情報窃取・侵入対策	PH-1-1	情報の物理的保護	-	画面の盗み見や機器の盗難等を防止するための措置を講じること。	(特になし)	・仕様書記載例のままでは費用見積もりが困難であるため、提案例も参考にした上で仕様書記載例の【 】に条件をできるだけ具体的に記すこと。	低位 中位 高位	機器の盗難、ディスプレイの盗み見、許可されていない持ち出し等の物理的な手段によって情報が窃取される。
PH-1-2	侵入の物理的対策	-	情報システムの設置場所への不正侵入を防止するための措置を行うこと。	(特になし)	・仕様書記載例のままでは費用見積もりが困難であるため、提案例も参考にした上で条件をできるだけ具体的に記すこと。	低位 中位 高位	情報システムの設置場所に対する物理的な侵入を受け、保護すべき情報の窃取や削除・破壊等の被害を受ける。	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。	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。	・入室の制限及び記録 ・遠隔映像監視 ・侵入警報 ・所在表示の制限				
DA	障害対策 (事業継続対応)	構成管理	DA-1-1	システムの構成管理	B	必要な機器のみによって必要なサービスのみを提供するように情報システムの構成及び稼働状況の管理を行うこと。	(特になし)	低位 中位 高位	情報システムを構成するハードウェアやソフトウェア及びサービスの構成を正確に把握できず、侵害の原因究明や適切な対応が困難になる。	情報システムの機器やサービス構成の情報に基づいて、侵害の原因を迅速に究明し、被害拡大を防止できる。また、侵害の原因となる構成要素を点検し、排除することができる。	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。	・システム設計書等の文書による構成の定義 ・システム設計書等の文書によるサービス構成（端末やサーバ等の機器の不要な機能の停止又は制限等も含む）の定義		
			DA-2	可用性確保	DA-2-1	システムの可用性確保	-	システムの異常停止を防止するとともに障害時のシステムの迅速な復旧を行うこと。	(特になし)	低位	情報システムの異常停止、あるいは異常停止状態の長期化によって、サービスの利用者や提供者が被害を被る。	情報システムが異常停止した場合でも、復旧目標時間の範囲内で復旧できる可能性が高まる。	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。	・構成情報を管理するシステムの導入 ・端末にインストールされているソフトウェアを管理するツールの導入 ・端末の利用者へはユーザ権限のみを付与
			DA-1-2	システムの構成管理	B	必要な機器のみによって必要なサービスのみを提供するように情報システムの構成及び稼働状況の管理を行うこと。	(特になし)	低位 中位 高位	運用開始後の情報システムの機器やサービス構成の変更によって把握していた構成情報が無効となり、侵害発生時に適切な対応ができない。	情報システムの機器やサービス構成に変更が発生しても、正確に構成情報を更新することが可能であるため、侵害発生時の対応の確実性が増す。	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。	・構成情報を管理するシステムの導入 ・端末にインストールされているソフトウェアを管理するツールの導入 ・端末の利用者へはユーザ権限のみを付与		
			DA-2-2	システムの可用性確保	-	システムの異常停止を防止するとともに障害時のシステムの迅速な復旧を行うこと。	(特になし)	低位 中位 高位	情報システムの異常停止、あるいは異常停止状態の長期化によって、サービスの利用者や提供者が被害を被る。	情報システムが異常停止した場合でも、復旧目標時間の範囲内で復旧できる可能性が高まる。	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。	・装置及びネットワークの冗長化（ホットスタンバイ、コールドスタンバイ等） ・信頼性の高いハードウェア及びソフトウェアの採用 ・DNS等の基盤サービスの信頼性確保 ・オンライン又はオフラインバックアップ ・システムのリカバリ方法の手順化 ・災害時の対処方法の手順化		

