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（情報の共有がされてはならない）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。 ・「高位」であっても、情報システムの運用又は管理に用いる通信経路（ネットワーク）のみ分離する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				
									中位	通信回線を介して情報の管理ポリシーの異なる外部からのアクセスによって、情報窃取等の不正行為が行われる。	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乗っ取ら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
									高位	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。	内部ネットワークの機器等に対する不正行為の影響範囲をネットワークの一部に限定することができる。	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。	・通信が必要な単位でセグメントを分割し、セグメント間の通信を必要最小限とするアクセス制御（マイクロセグメンテーションの観点を踏まえた対策） ・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
				AT-1-2	不正通信の遮断	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				
									中位	通信プロトコルの脆弱性やサーバ装置等の設定不備を悪用して、不正行為が行われる。	脆弱な通信プロトコルや不要な通信プロトコルやアプリケーションの通信の利用を制限することで、不正行為が行われる可能性を低減することができる。	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やアプリケーションの通信を通信回線上にて遮断する機能を備えること。	・ファイアウォール、WAF、プロキシやリバースプロキシ、次世代ファイアウォール等による通信制御 ・不審なメールの受信や不審なウェブサイトへのアクセスを遮断 ・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
									高位	（↑ 同様）		（↑ 同様）	（↑ 同様）
				AT-1-3	通信のなりすまし防止	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、通信回線装置等）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				
									中位	利用者が気づかぬまま、偽の情報システムにアクセスしてしまい、個人情報等の保護すべき情報が漏えいしてしまう。	利用者は、情報システムの利用時にアクセス先の正当性を確認することができる。	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。	・TLSによるサーバの認証 ・政府ドメイン名（.go.jpで終わるドメイン名）の利用 ・検索エンジン最適化措置（SEO対策）の実施 ・送信ドメイン認証（DMARC）による不正なメール受信の遮断
									高位	許可されていない機器等（端末、サーバ装置、通信回線装置等）がネットワークに接続されることによって、情報窃取等が行われる。	情報システムに対してアクセス可能な機器等を正当なもののみに制限できる。	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。	・情報システムの機器番号等による接続機器の識別 ・クライアント証明書による接続機器の認証 ・無線LANの認証プロトコル、IPSec、IEEE 802.1x、等
				AT-1-4	サービス不能化の防止	A	トラフィック集中によるサービス不能化の脅威を軽減すること。	・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				
									中位	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。	情報システムに対するDDoS攻撃による被害を抑制することができる。	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。	・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）
									高位	構成機器の設定程度では対処困難な攻撃によって、サービス提供が不能な状態または困難な状態に陥る。	情報システムに対する広範囲かつ多様なDDoS攻撃に対処可能になる。	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。	・負荷分散装置による処理性能の確保 ・代替となる機器等の設置 ・サービス不能化攻撃の元アドレス及び通信パケットの特徴に基づく通信の制限又は遮断 ・通信回線装置及び通信回線において、大量アクセス発生時に帯域を一時的に拡大 ・情報システムの管理に用いる端末、サーバ及び通信回線をサービス提供に用いるものと分離
		AT-2	不正プログラム対策	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や感染拡大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用パターンファイル等の手動または自動更新 ・ 振る舞い検知方式、機械学習検索方式、およびサンドボックス方式の不正プログラム対策ソフトウェア等を組み合わせた多重防御の導入 ・ EDRソフトウェアの導入 ・検疫ネットワークの導入
									中位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
									高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
				AT-2-2	不正プログラム対策の管理	A or B	不正プログラム対策の最新化を確実に行うため、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				
									中位				
									高位	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	脆弱性対策	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ぎ、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 ・脆弱性を検査するための専用ツールや事業者が提供するサービス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 ・ペネトレーションテストによる脆弱性診断 ・WAF等によるSQLインジェクションの脆弱性対策
									中位	（↑ 同様）	（↑ 同様）	（↑ 同様）	
									高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
				AT-3-2	運用時の脆弱性対策	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場合、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。	情報システムの構成機器において、運用開始後に新たに発見される脆弱性についての対策が可能になる。	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（手順等）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 ・脆弱性を検査するための専用ツールや事業者が提供するサービス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
									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。	・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
									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
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、不正行為に気づかないことで被害のさらなる拡大を招く。	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かかわらず、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に遅れや場当たり的な対処が発生し、被害の拡大・長期化を招く。	適切に管理されたログや様々なログを組み合わせた相関分析等により、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、様々なログを組み合わせた相関分析に有効な管理機能、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 ・外部ログサーバへの出力機能 ・リアルタイムでのログの調査・分析を行うための機能（SIEM）
										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。	・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	外部記録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。	・信頼性の高い記録装置の導入、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えるため、システム全体の時刻を同期させること。	（特になし）	（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。	・高位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決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、中位レベルでは迅速に対応できない可能性があるため、高位レベルの対策が有効に働く場合がある。	（特になし）	低位				
										中位	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処が可能となり、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による通信回線上の不正な通信パケットの検知やファイアウォールと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 ・内部ネットワーク内の機器同士における普段は起こりえない通信の監視 ・システムの負荷、リソースの使用状況の監視 ・ユーザ、グループ、システム管理者の追加、変更の有無の監視 ・管理者、ユーザのパスワード漏洩の有無、大量のログオン失敗や、通常とは異なる時間帯やアクセス元IPアドレスからのログインがないかの監視
				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。	・高位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				
										中位				
										高位	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、早期対処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 ・脅威情報の収集、サービス不能攻撃を受ける可能性のCSIRT等への通知
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」を参考に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				
										中位	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。	正当な利用者のみにアクセスを許可し、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限
										高位	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やFIDO認証による主体認証 ・耐タンパ性を備えたICカード又はUSBトークン認証 ・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 ・大規模な辞書を用いたパスワード解析への耐性（パスフレーズ等）
		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）	（特になし）	低位				
										中位	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
										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位レベルの対策要件が必要になる。	・本対策要件を調達仕様書に記載する場合には、業務要件の一環として、情報システムのアクセス元となる主体及び主体ごとの業務（アクセス権）の関係を具体的に記載すること。	低位				
										中位				
										高位	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。	利用者の職務や信用情報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や信用情報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や信用情報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 ・認証・認可の統合管理基盤 ・動的なアクセス制御
				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）	（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やワークフロー機能の導入
										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	PR-1	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）	（特になし）	低位				
									中位	通信回線上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及び鍵長については、「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 ・VPNによる仮想的な専用回線での接続 ・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
									高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
				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り端末の利用環境が安全ではない（他人に操作される可能性がある）場合には、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。	・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
									高位	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。	情報の保存場所から情報が窃取されても、情報の内容が読み取られる可能性を低減できる。	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、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及び鍵長については、「電子政府推奨暗号リスト」を参照し決定すること。	・ファイル暗号化システム（ソフト、機能） ・暗号化機能を備える記録装置（USBメモリ、HDD、モバイルPC等） ・情報漏えい対策（DLP）ソリューション全般 ・S/MIME等のセキュアメールシステム
				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 ・ウェブアプリケーションやウェブコンテンツの更新時に保存するハッシュ値を比較する機能
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	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。	物理的な手段による情報窃取の可能性を低減することができる。	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。	・端末の離席対策（自動スクリーンロック等） ・端末のワイヤーロック ・施錠可能なサーバラックの採用 ・ディスプレイの盗み見防止フィルタ ・記録装置のパスワードロック、暗号化 ・データ消去ソフトや物理的破壊等による情報の完全廃棄 ・携帯電話、メモリデバイス等の持込みの監視及び制限 ・物品持ち出し管理システム ・通信ケーブル及び通信回線装置の物理的保護（床下への埋設等） ・シンクライアントによる端末に情報を保存させない仕組み ・セキュアブラウザによる端末に情報を保存させない仕組み ・遠隔データ消去による盗難・紛失対策 ・テンペスト（電磁波盗聴）対策システム
									中位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
									高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
				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	情報システムの設置場所に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。	情報システムの設置場所に対する物理的な侵入の防止及び検知が可能になり、侵入された場合にも早期対処が可能になる。	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。	・入退室の制限及び記録 ・遠隔映像監視 ・侵入警報 ・所在表示の制限
									中位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
									高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
DA	障害対策（事業継続対応）	DA-1	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）	（特になし）	低位	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処が困難になる。	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
									中位	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、侵害発生時の対処の確実性が増す。	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
									高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
		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）	・情報システムが扱う各業務の復旧時間について利用者への影響度合い等を考慮し、【　　】の箇所に明記する必要がある。	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損害を被る。	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
									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
SC	サプライチェーン・リスク対策	SC-1	情報システムの構築等の外部委託における対策	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等の委託先における従業員等の情報セキュリティ管理体制を確認することで、不正プログラム等が組み込まれた情報システムが納入されないようにする。	（特になし）	・構築する情報システムが機密性の高い情報を扱わず他の情報システムとも接続しない場合等、情報漏えいリスク対策に高い水準の要件を求める必要がない場合は、除外することも考えられる。	低位	情報システムの構築を受託した事業者の従業員が、情報システムへの侵入経路（いわゆるバックドア）等の不正プログラム等を開発時に悪意を持って組み込むことにより、情報システムの稼働開始後に情報システムで取り扱われる情報を窃取する。 再委託をすることにより、再委託先事業者の従業員等が、情報システムへの侵入経路（いわゆるバックドア）等の不正プログラム等を開発時に悪意を持って組み込むことにより、情報システムの稼働開始後に情報システムで取り扱われる情報を窃取する。	情報システムの構築等の外部委託において、構築する情報システムに意図せざる変更が加えられないための十分な管理体制が採られている事業者を選定条件とすることで、情報窃取の可能性を低減する。再委託先にも委託事業者と同様の管理体制を求めることにより、再委託先からの、情報窃取の可能性を低減する。	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。	・委託事業者の資本関係や役員等の情報を含めた基本情報の提出 ・委託事業の実施場所の提示 ・委託事業従事者の所属、専門性、実績や国籍情報を含めた体制図の提示 ・委託先における監査の受け入れの事前合意（契約時） ・委託先における情報の適正な取扱いのための情報セキュリティ対策の実施内容及び管理体制 ・再委託先事業者の資本関係や役員等の情報を含めた基本情報の提出 ・再委託先委託事業の実施場所の提示 ・再委託先委託事業従事者の所属、専門性、実績や国籍情報を含めた体制図の提示
										中位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
										高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
		SC-2	機器等の調達における対策	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	－	製造過程における情報セキュリティ対策を確認することで、不正プログラム等が組み込まれた機器等が納入されないようにする。	（特になし）	・機器を調達しない場合、調達する機器が機密性の高い情報を扱う情報システムに接続しない場合等、情報漏えいリスク対策に高い水準の要件を求める必要がない場合は、除外することも考えられる。	低位	機器の製造過程において、製造事業者の従業員が、機器が構成する情報システムへの侵入経路（いわゆるバックドア）等の不正プログラム等を悪意を持って組み込むことにより、情報システムの稼働開始後に情報システムで取り扱われる情報を窃取する。	製造機器等に不正な変更が加えられないよう努めている事業者から機器等を調達することで、情報窃取の可能性低減することができる。	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。	・製造過程における情報セキュリティ管理体制や管理手順等が記載された書類の提出
										中位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
										高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
UP	利用者保護	UP-1	情報セキュリティ水準低下の防止	UP-1-1	情報セキュリティ水準低下の防止	A	利用者が情報システムによって提供されるアプリケーションプログラムやウェブコンテンツ等を利用する際に、利用者の情報セキュリティ水準が低下しないよう対策を行うこと。	（特になし）	（特になし）	低位				
										中位	政府機関が提供するアプリケーションプログラムやウェブコンテンツ等を利用することによって、利用者の情報セキュリティ水準が低下し、不正プログラムへの感染等が発生する。	利用者の情報セキュリティ水準が維持されることで、不正プログラム等への感染を防止することができる。	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。	・実行プログラム形式（拡張子が「.exe」等で終わるもの）でのコンテンツ提供の禁止 ・サポート期限が切れた、又は情報システムの提供期間中にサポート期限が切れる予定にあるバージョンのOSやソフトウェア等の利用を前提とすることの禁止 ・複数のウェブブラウザで動作するよう設計・構築 ・政府ドメイン名（.go.jpで終わるドメイン名）の利用
										高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）
		UP-2	プライバシー保護	UP-2-1	プライバシー保護	A	情報システムの利用者に関する情報が本人の意思に反して第三者に提供されないよう対策を行うこと。	（特になし）	（特になし）	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することによって、利用者のプライバシーを侵害する。	利用者のアクセス履歴、入力情報等が第三者に送信されないことで、利用者のプライバシーを保護することができる。	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。	・府省庁外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを検証 ・府省庁外のウェブサイト等のサーバへ自動的にアクセスが発生する機能を含める場合は、当該府省庁外へのアクセスが情報セキュリティ上安全なものであることを検証 ・本来のサービス提供に必要のない府省庁外へのアクセスを自動的に発生させる機能の禁止
										高位	（↑ 同様）	（↑ 同様）	（↑ 同様）	（↑ 同様）

【目的】
・対策要件を満たす対策を実施することの目的

【実施レベル選定の考え方】
・中位レベル及び高位レベルの対策要件があり得る場合の選定の考え方

【仕様記載時の注意事項】
・調達する情報システムの特性に応じて調達仕様書の記載内容を具体化すべき事項

【想定脅威】
・対策要件の各実施レベルにおいて想定され解決を試みようとする脅威の内容

【対策の効果】
・各実施レベルの対策要件に対応する対策を実施した場合に得られる効果

【仕様書記載例】
・各実施レベルの対策要件に対応する仕様書の記載例

【対策の提案例】
・各実施レベルの対策要件に対して想定される一般的な対策の提案例（実現例）
・実施レベル毎に対策の提案例を記載しているが、上位の実施レベルを選択する場合は、同一対策要件の下位の対策の提案例も参照すること。

※対策は「想定する脅威の具体的内容」等に強く依存するため、対策の提案例をレベル分けせずに低位に一括記載している場合がある。

【備考】
・本対策要件集は、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が、クラウドサービスを調達する際にも活用することは可能である。
なお、クラウドサービスを調達する際は、本対策要件集に記載の内容の他にもクラウドサービス提供者へ求めるサービスレベル等の要件も考慮する必要がある。