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

【付録D. 用語解説】

2019 年9月 24 日

用語	語義
DDoS	【ディー・ドス、Distributed Denial of Service】複数のネットワークに分散する大量の端末が、一斉に特定のサーバ装置にアクセスし、通信経路を溢れさせて機能を停止させてしまう攻撃のこと。
DKIM	【ディー・キム、Domain Keys Identified Mail】電子署名を利用した電子メールの送信ドメイン認証技術の一つ。スパムメール、フィッシングメールなどの迷惑メールへの対策の一つとして利用可能。
DMARC	【ディー・マーク、Domain-based Message Authentication, Reporting & Conformance】電子メールにおける送信ドメイン認証技術の一つであり、SPF・DKIM のドメイン認証技術を利用し、メールの正当性を送信者と受信者間で確認する仕組み。
DMZ	【ディー・エム・ゼット、Demilitarized Zone】インターネットと接続された通信回線において、セキュリティを維持することを目的に、ファイアウォールによって外部からも内部からも分離された区域のこと。
DNS	【ディー・エヌ・エス、Domain Name System】ドメイン名（電子計算機を識別する名称）を IP アドレスに自動的に変換するシステムのこと。
GPS	【ジー・ピー・エス、Global Positioning System】人工衛星と地上の制御局を利用して、位置を測定するシステムのこと。
HDD	【ハードディスクドライブ、Hard Disk Drive】電子計算機における記憶装置の一つで、磁気記憶方式によって情報を読み書きする装置のこと。
HTTP	【エイチ・ティ・ティ・ピー、Hyper Text Transfer Protocol】端末上のブラウザとサーバ装置の間で、データを送受信するために使われるプロトコルのこと。
IC カード認証	極めて薄い IC（Integrated Circuit＝集積回路）を埋め込んだカードによる認証方式のこと。
IDS	【アイ・ディー・エス、Intrusion Detection System】通信回線を監視し、ネットワークへの侵入を検知して管理者に通報するシステムのこと。
ID パスワード認証	操作者が特定のユーザであることを確認するために、文字列を使って認証を行う方式のこと。
IEEE802.1x	【アイ・トリプルイー・ハチマルニ・テン・イチ・エックス】IEEE（Institute of Electrical and Electronic Engineers：米国電気電子協会）が定めた LAN 上でのユーザ認証とアクセス制御に関する規格のこと。
IP	【アイ・ピー、Internet Protocol】電子計算機を通信回線で相互接続するための通信プロトコルのこと。
IPS	【アイ・ピー・エス、Intrusion Prevention System】サーバ装置や通信回線に対する攻撃や侵入等の不正行為を検知して阻止する仕組みのこと。

用語	語義
IPSec	【アイ・ピー・セック、Security Architecture for Internet Protocol】暗号技術を使って IP パケットの完全性や機密性を実現する仕組みのこと。
LAN	【ラン、Local Area Network】一つの施設内程度の規模で用いられる通信回線のこと。
NTP	【エヌ・ティ・ピー、Network Time Protocol】ネットワークを使って電子計算機内の時計を正確に保つための通信方式のこと。
S/MIME	【エス・マイム、Secure Multipurpose Internet Mail Extensions】電子メールで利用される暗号化／電子署名利用の国際規格の一つ。
SPF	【エス・ピー・エフ、Sender Policy Framework】メールの送信元アドレスの偽装を防止するための送信ドメインを認証する方式の一つ。
SSL/TLS	【エス・エス・エル、Secure Socket Layer / ティ・エル・エス、Transport Layer Security】インターネット上で、データを暗号化して送受信する方法のこと。TLS は SSL を元に標準化させたもの。
SQL インジェクション	【エス・キュー・エル・インジェクション、SQL Injection】ウェブアプリケーションのプログラムが SQL 言語を用いている場合に、アプリケーションの不備を悪用して外部から攻撃用の文字列を SQL 文に不正に混入（インジェクション）させることにより、データベースを不正に操作しようとする攻撃のこと。
USB メモリ	【ユー・エス・ビー・メモリ、Universal Serial Bus メモリ】サーバ装置や端末に接続してデータの読み書きを行う補助記憶装置のこと。
UTM	【ユー・ティー・エム、Unified Threat Management】複数の異なるセキュリティ機能を、一つの装置に統合し、集中的にネットワーク管理を行う仕組みのこと。
VLAN	【ブイ・ラン、Virtual Local Area Network】物理的な一つの LAN 上に、仮想的に複数の LAN に分離する、或いは、物理的に分離している LAN を仮想的な一つの LAN として利用する仕組みのこと。
VPN	【ブイ・ピー・エヌ、Virtual Private Network】インターネット回線や共有通信回線を仮想的に専用線のように利用する仕組みのこと。
WAF	【ワフ、Web Application Firewall】Web アプリケーションに対する外部からの攻撃や侵入を検知及び防止する仕組みのこと。
アーカイブ アーカイブデータ	情報システムが運用時に蓄積する情報のうち、業務上不要となった情報を情報システムの記憶装置の負担を軽減するため、ひとまとめにして外部に取り出して保存すること及び保存されるひとまとめの情報のこと。
アカウント	情報システムを利用するための資格や権限のことであり、情報システムの運用者によって対象となる利用者に割り当てられる。

用語	語義
アクセスログ	サーバ装置における接続や操作の履歴のこと。
アクセス主体	通信回線を経由して、サーバ装置のサービスを利用するユーザ、及び電子計算機に連接する装置等の総称のこと。
アクセス制御 アクセス制御機能	アクセス元（利用者、運用者、管理者、装置等）に応じて情報システムが管理する情報資産に対するアクセスの内容（例えば、情報の読み出し、書き込み、変更等）を許可又は拒否すること及びそのための機能のこと。
アドレス	通信回線上の存在場所を表す識別子のこと。
アプライアンス	特定用途向けにカスタマイズされた専用のハードウェアとソフトウェアの総称のこと。
アンチウイルスソフトウェア	ウイルスを検出及び除去するためのソフトウェアのこと。
イベント	電子計算機内で発生する様々な動作のこと。
ウイルス	電子計算機に感染して破壊活動を行い、または、トラブルを引き起こすプログラムのこと。
オンラインバックアップ オフラインバックアップ	サーバ装置や端末のデータの複製を別の場所に保存し、問題が起きても、データ復旧できるように備えておくこと。特に、通信回線を利用したものをオンラインバックアップといい、外部記憶媒体に直接接続によるものをオフラインバックアップという。
コーディング規約	プログラミング言語の文法とは異なり、様々な書き方が可能な場合にどのような書き方にするかを集団内の約束として決めたもの。
コールドスタンバイ	電子計算機や通信回線を、全く同じ構成や設置の予備のマシンの電源を入れない状態で待機させておく状態で多重化して信頼性を向上させる手法の一つ。
サーバ装置	通信回線を通じて、端末からのアクセスを受けて、自身のもっている機能やデータを提供する装置のこと。
サービス サービス構成	情報システムが、利用者又はその端末等からのアクセスに対して提供する機能及び機能構成のこと。
サービス不能化	情報システムが利用者に対して機能を正常に提供することが困難な状態になること。
しきい値	通信監視装置などで、どの程度のエラーが発生した場合に障害とみなすかを設定した値のこと。
システムアカウント	情報システムを管理、運用、保守する目的のためにアクセス可能なアカウントのこと。
システムの負荷	電子計算機において、内部の処理待ち状態を示すもの。
システム設計書	システム全般を網羅した機能実現のために必要な文書の一つ。

用語	語義
システム設定	システム設置時において、機能実現のために登録・設定が必要な事項のこと。
シンクライアント	利用者が使う端末に必要最小限の処理をさせ、ほとんどの処理をサーバ装置側に集中させた仕組みのこと。
ストレージ（情報システムのストレージ）	電子計算機内でデータやプログラムを記録する装置の総称のこと。
スパイウェア	ユーザが気付かぬうちに電子計算機にて動作し、操作記録、個人情報、処理結果等をスパイウェアの作成元に送り、情報を不正に収集したり、電子計算機を不正に利用したりするソフトウェアのこと。
セキュアコーディング	脆弱性に繋がる恐れのあるコーディング作法や未定義の動作を極力減らすためのコーディング手法のこと。
セキュアメールシステム	S/MIME 等の採用により、通信を暗号化し安全にメールを送信するシステムのこと。
セキュリティの専門家	外部において、セキュリティ領域における十分な専門知識と経験を発揮できる有識者のこと。
セキュリティホール	ソフトウェアの不具合や設計上のミスが原因で発生するセキュリティ上の欠陥のこと。
セキュリティ状態（サーバ装置のセキュリティ状態）	サーバ装置に対する、第三者による侵害行為やウイルス等による不正アクセスの事象の有無のこと。
セキュリティ侵害	利用する権限を持たない第三者により、不正にデータが利用されること。
セキュリティ要件	情報セキュリティを確保するために満たすべき条件のこと。
ソフトウェア	電子計算機を動作させる手順及び命令を電子計算機が理解できる形式で記述したもの。
タイムスタンプ	特定の電子文書が、ある時刻から存在したこと、及びその時刻から検証した時刻までの間に変更・改ざんされていないことを証明するための手段のこと。
データ消去ソフト	HDD に書き込まれた内容（データやファイルや画像）を完全に消去するためのソフトウェアのこと。
デジタル署名	電子文書の正当性を保証するために付けられる、暗号化された署名情報のこと。
テンペスト	電子計算機等の電子機器から漏れ出す電磁波をキャッチし、そこから情報を盗み出す手口のこと。
トラフィック	通信回線を流れるデータそのもののこと、或いはそのデータ量のこと。
なりすまし	自身ではない他人のふりをして何らかの行為を行うこと。

用語	語義
バージョンアップ	ソフトウェアやハードウェアにおいて、新しい機能の追加やバグの修正、仕様の変更などにより改良や改善が加えられ機能が強化されること。
ハードウェア	電子計算機を物理的に構成している回路や筐体、周辺危機といった装置の総称のこと。
パスワードロック	HDD 自体にパスワードを掛けて、第三者にアクセスできなくする機能、或いは、スクリーンセーバーからの復帰にログオン時のパスワード入力を求めることで、離席中の第三者に操作されることを防ぐ機能のこと。
パターンファイル	ウイルスに感染したファイルや、通信回線上で自己複製を繰り返すワームの特徴を収録したファイルのことで、アンチウイルスソフト(ワクチンソフト)がウイルスやワームを検出するために使うもの。
パッチ	コンピュータのプログラムの一部分を更新して障害修正や機能変更を行うための追加ファイルのこと。
ファイアウォール	組織内の通信回線に外部から侵入されるのを防ぐ仕組みのこと。
ファイル暗号化システム	ファイルの内容を第三者に分からなくするための機能及びシステムのこと。
フィルタ処理	不要なものを取り除き、 目的とする情報を取り出す処理のこと。
プロトコル	電子計算機同士が通信を行う上で、相互に決められた約束事の集合のこと。
ボット	インターネットを通じて悪意を持った第三者が、電子計算機を外部から遠隔操作することを目的として作成された悪意のあるプログラムのこと。
ホットスタンバイ	電子計算機や通信回線を、データの同期などを絶えず行った状態で多重化して信頼性を向上させる手法の一つ。
マルウェア	ウイルス、ワーム、スパイウェア、ボット等の不正プログラムの総称であり、コンピュータ上で利用者の意図しないような悪意のある動作を行うことができるプログラムのこと。
モバイル PC	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のこと
ライトワンスメディア	書き込みが一度しかできないデバイスのこと。
ライフサイクル管理	情報システムの企画・設計段階から、開発及び運用までのすべての過程を管理する手法のこと。
リカバリ	障害が発生したシステムを復旧或いは復元すること。
リスク	脅威が情報資産の脆弱性を利用して、情報資産への損失又は損害を与える可能性のこと。ちなみに、脅威とは、情報システムに対して悪い影響を与える要因のことであり，自然災害，システム障害，人為的過失及び不正行為等がある。

用語	語義
リソース	電子計算機を構成し、稼動させるためのハードウェア・ソフトウェアの総称のこと。
リバースプロキシ	特定のサーバ装置に代わってアクセスを受け付けて中継するサーバ装置であり、特にアクセスの内容を検証の上で中継する場合にはセキュリティの強化が可能となるサーバ装置のこと。
ローテーション（ログのローテーション）	蓄積された証跡情報を管理する上で、システム管理ポリシーで定められた保存期間に基づき、参照しやすいファイル名やサイズで保存すること。
ロードバランサ	外部ネットワークからの大量のアクセスを一元的に管理し、複数のサーバに割り振り負荷を軽減する装置のこと。
ロール（ユーザのロール）	情報システムにおいて、共通の役割(権限)を持つユーザから構成するグループのこと。
ログ	情報システムの利用状況、動作状況を記録すること及び記録される情報のこと。
ワーム	電子計算機に悪害を与えるプログラムとしての広義のウイルスの中でも、インターネットを通じて自己増殖を行う性質を持つもの。
ワイヤーロック	盗難防止のために、端末をワイヤーで固定すること。
ワンタイムパスワード	一度限りしか使えないパスワードを生成することで、パスワード認証の弱点を克服した認証方式のこと。
安全区域	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、第三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のこと。
暗号 暗号アルゴリズム	情報を第三者に知られることがないように、情報に何らかの変換処理を行うこと及び変換処理の方式のこと。
一元管理	一つの手段やツールを使って、サーバ装置や端末を統一的に管理すること。
運用 （情報システムの運用）	電子計算機及び通信回線を稼働する際に発生する様々な業務の総称のこと。
運用者	電子計算機及び通信回線を稼働する際に発生する日常的な業務を担当し、その業務の遂行に必要な権限が与えられている担当者のこと。
遠隔映像監視	監視対象となる遠隔地の状況を、カメラで撮影し、通信回線を通じて、その映像を監視すること。
可用性	情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。

用語	語義
改ざん	通信回線を通じて、電子計算機に不正侵入し、内部の情報を管理者の許可を得ずに書き換える行為のこと。
改ざん検知システム	システムファイルや Web コンテンツの内容、またはその特徴を記録し、対象となるファイルが改ざんされていないかどうかを検知する仕組みのこと。
外部アクセス(外部アクセス向けネットワーク)	特定の領域の関係者のみが利用することができるネットワーク(内部ネットワーク)から、不特定多数の人が利用する可能性のあるネットワーク(外部ネットワーク)向けに通信の流れを発生させること。
外部ネットワーク	インターネット等の不特定多数の人が利用する可能性のあるネットワークのこと。
各府省情報化統括責任者(CIO)連絡会議	高度情報通信ネットワーク社会推進戦略本部令(平成 12 年政令第 555 号)第 4 条の規定に基づき、関係行政機関相互の緊密な連携の下、政府全体として情報化推進体制を確立し、行政の情報化等を一層推進することにより、国民の利便性の向上を図るとともに、行政運営の簡素化、効率化、信頼性及び透明性の向上に資するため、高度情報通信ネットワーク社会推進戦略本部に設置された連絡会議のこと。 (http://www.kantei.go.jp/jp/singi/it2/cio/konkyo.html)
完全性	情報が破壊、改ざん又は消去されていない状態を確保すること。
管理者	電子計算機及び通信回線を稼働に関する責任を持ち、想定外の事象に対応しうる権限を持っている担当者のこと。
管理者権限	電子計算機等のシステム、ユーザ、ファイル等の追加、変更、削除をすることなどができる権限のこと。
機密性	情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保すること。
記憶媒体	データやプログラムを記録する装置或いはデバイスのこと。
業務要件	なんらかの目的を達成するために実施する各業務の内容及びその遂行にあたって満たすことが求められる条件のこと。どのようなルールに従って、誰が何をどのようにして処理するのかを条件としてまとめたもの。
検疫ネットワーク	端末を組織内 LAN に接続する際に、一旦、LAN とは隔離された検査専用のネットワークに接続し、問題がないことを確認してから組織内のネットワークへ接続する仕組みのこと。
権限管理	主体認証に係る情報(識別コード及び主体認証情報を含む。)及びアクセス制御における許可情報を管理すること。
検索エンジン最適化(SEO)	対象とするウェブサイトが検索サイトで上位に現れるよう、サイトの内容等に工夫を施すこと。SEO…Search Engine Optimization

用語	語義
原本性保証	電子文書を管理及び保存する際、紙文書と同等の有効性を保証すること。
公衆電話網（公衆交換電話網）	一般固定電話回線の電話網のこと。
構成機器	システムの中で機能或いは装置毎に分けられる機器のこと。
構成情報	ハードウェアやソフトウェアの情報、関連ドキュメント、契約情報、保守情報のこと。
構築（情報システムの構築）	システムの設計からテスト・評価に至るまでの作業のこと。
構文解析（ログの構文解析）	蓄積された証跡情報における文字列の構造を明らかにし、その意味構造を理解可能な状態にする技術こと。
最少特権機能	管理者権限を持つ識別コードを付与された者が、管理者としての業務遂行時に限定してその識別コードを利用させる機能のこと。
時刻ソース	信頼できる時刻情報の提供主体のこと。
識別コード	主体を識別するために用いられる、情報システムが認識するコード（符号）のこと。ユーザ ID 等がある。
実施レベル	セキュリティ対策の実施の程度（強度）を「低位」「中位」「高位」の 3 段階にて表す本マニュアル独自の尺度のこと。
主体	行政サービスの利用や提供を行う情報システム、あるいは当該業務を実施する者のこと。主体は利用者、運用者及びシステム管理者等の人間以外に、装置、システム等の場合もある。（マニュアル本編 4 章参照）
主体認証	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正当な主体であるか否かを検証すること。
主体認証情報	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のこと。代表的な主体認証情報として、パスワード等がある。
証跡	情報システムの処理内容が時系列に沿って記録され、情報システムを用いて業務が定められた手順に従って実施されているかどうかの追跡、確認等に用いられる情報のこと。
証跡の管理装置	業務が定められた手順に従って実施されているかどうかを記録として残し、管理するための措置のこと。
証跡管理	業務が定められた手順に従って実施されているかどうかを記録として残し、管理すること。
冗長化	複数の装置を用意しておき、1 つの装置が故障しても他の装置がサービスを続行できるようにすること。
情報システム	情報処理及び通信に係るシステムのこと。

用語	語義
情報の管理ポリシー	情報セキュリティに関する基本方針のうち、情報の管理について定めたもの。各府省庁において策定した基準などにより規定される。
情報漏えい	内部の機密情報が何からの形で外部に流出してしまうこと。
生体認証	指紋や眼球の虹彩、声紋などの身体的特徴によって本人確認を行う認証方式のこと。
脆弱性	電子計算機において、第三者がセキュリティ脅威となる行為に利用可能となる、システムの欠陥や問題点のこと。
脆弱性診断（内部検査及び第三者検査）	電子計算機や通信回線などにおける各種装置において、システムの乗っ取りや機密情報の漏洩などを第三者に利用される可能性のある欠陥や仕様上の問題点を検出すること。
専用回線	利用者が自分専用として使用できる回線のこと。
送信ドメイン	メールの送信者が名乗るメールアドレスのドメイン（コンピュータを識別するために付与される名前）部分のこと。
属性（ユーザの属性）	情報システムのサービスを利用するユーザ固有 ID、所属部署、氏名、職員番号、システム利用の有効期間等の情報のこと。
対策要件 対策要件集 対策区分 対策方針	「対策要件」は、情報セキュリティ対策のために情報システムが備えるべき機能に求められる条件のことであり、「対策要件集」は、対策要件を本マニュアルにて独自に一覧化したもののこと。対策要件集は、「対策区分」と呼ぶ8種類の区分及び対策区分の中の小区分である「対策方針」によって対策要件を整理している。（マニュアル本編 5 章参照）
耐タンパ性（耐タンパ性を備えた IC カード認証）	IC カードに記録されているデータに対する解析や偽造に対して物理的にデータを保護する性質のこと。
帯域	通信回線において、一定時間に通信可能なデータ量のこと。
端末	端末を利用する者が直接操作を行う、PC や PDA 等の電子計算機のこと。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。
通信パケット	通信回線において、流れるデータの通信単位を表すもの。
通信プロトコル	通信回線上で、データを通信するために必要な規約のこと。
通信ポート（サーバ装置の等の通信ポート）	電子計算機が、通信回線を通じて、他の装置と接続をするために必要となる接続器（コネクタ）のことで、特定の識別情報が付与されているもの。
通信回線	複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みのこと。
通信回線装置	回線の接続のために設置され、電子計算機により回線上を送受信される情報の制御を行うための装置のこと。
通信経路	通信回線においてデータが流れる道筋のこと。

用語	語義
通信遮断	通信経路において、データの流れを止めること
通信制御	通信回線に流れるデータの量や送出速度の制御や、通信回線の変更等すること。
定型設問	情報システムに関する共通的な業務要件について本マニュアルが独自に定めた設問のこと。調達担当者が設問の回答を検討することによって業務要件の詳細化を促すために用いられる。（マニュアル本編 4.4 節参照）
電子計算機	コンピュータ全般のことを指し、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サーバ装置及び端末のこと。
電子署名	電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。 ・ 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 ・ 当該情報について改変が行われていないかどうかを確認することができるものであること。
盗聴	他人のやりとりの内容を気づかれないように聞いたり、通信の内容を傍受したりすること。
統一基準	「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）（平成 30 年7月 25 日サイバーセキュリティ戦略本部決定）」のこと。
内部ネットワーク	特定の領域の関係者のみが利用することができるネットワークのこと。
認証	自分しか持ち得ない情報などに基づく確認及び本人認証のこと。
認証プロトコル	電子通信装置間で、相手の正当性を確認するために定められた手順や規約のこと。
認証情報	本人証明可能で、自分しか持ち得ない情報のこと。
判断条件	業務要件をあてはめて、優先すべきセキュリティ対策の方向性を導出するための条件のこと。（マニュアル本編 5 章参照）
標準ガイドライン	「デジタル・ガバメント推進標準ガイドライン（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）」のこと。
不正アクセス	電子計算機に対して、正規の権限を持たない者が、ソフトウェアの不具合や設定ミスを悪用して、不正に電子計算機を利用する、或いは、試みること。
不正プログラム	意図しない結果を電子計算機にもたらすソフトウェアの総称のこと。コンピュータウイルス、スパイウェアということが多い。

用語	語義
府省庁外	行政事務従事者の各々が所属する府省庁が管理する組織又は庁舎の外のこと。
府省庁内外	行政事務従事者の各々が所属する府省庁が管理する組織又は庁舎の内及び外のこと。
復旧目標時間	情報システムの異常停止後、対象業務が復旧及び再開するまでの目標時間のこと。
利用環境・手段	主体が、情報を処理（作成、保存、送受信等）するために用いる環境・手段のこと。（マニュアル本編 4 章参照）
利用者	情報システムが提供するサービスを利用する主体のこと。