令和7年3月

「港湾分野における情報セキュリティ確保に係る安全ガイドライン（第2版）」 専門用語集

本ガイドラインにおける専門用語を以下に掲載する。

1. 多要素認証機能

多要素認証とは、以下の認証方式を複数組み合わせた認証方式のことである。

- 対象者の知識を利用したもの（ID/パスワード、暗証番号、事前に登録した質問事項への回答など）
- 対象者の持ち物を利用したもの（セキュリティトークン、ICカードなど）
- 対象者の身体の特徴を利用したもの（指紋認証、静脈認証など）

2. ウェブアプリケーションの脆弱性

本章は、一般的なセキュリティ用語の解説であるため、解説中の「利用者」については特定の重要インフラに限らない、一般的な情報システムの利用者を指す。

（1）SQL インジェクション脆弱性

ウェブアプリケーションのプログラムがデータベースを操作する手段として SQL 言語を用いている場合に、プログラムが SQL 文を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が SQL 文に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、データベースを破壊されたり、データベース内の情報を盗まれたりするなどの被害が生じ得る。このような欠陥は一般に「SQL インジェクション脆弱性」と呼ばれている。SQLインジェクション脆弱性を排除するには、SQL 文の組み立てにプレースホルダを用いる実装方法を採用することを徹底するなどの対策が考えられる。

（2）OS コマンドインジェクション脆弱性

ウェブアプリケーションのプログラムが OS のコマンドを操作する必要がある場合に、プログラムが OS のシェルのコマンドラインを用いてコマンド呼出しをする構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列がコマンドラインに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、サーバに侵入される被害が生じ得る。このような欠陥は一般に「OS コマンドインジェクション脆弱性」と呼ばれている。OS コマンドインジェクション脆弱性を排除するには、OS コマンドの操作にシェルのコマンドラインを用いない実装方法を採用することを徹底するなどの対策が考えられる。

（3）ディレクトリトラバーサル脆弱性

ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっている場合に、指定されたパス名をプログラムがそのまま使用する構造になっていると、

公開を想定しないファイルが参照されて、その内容が外部から閲覧され得る欠陥となる場合がある。このような欠陥は一般に「ディレクトリトラバーサル脆弱性」と呼ばれている。ディレクトリトラバーサル脆弱性を排除するには、外部のパラメータからパス名を指定する仕様を排除する対策、それができない場合には、ファイルにアクセスする直前に、使用するパス名の妥当性検査を行う方法、又は、ファイルのディレクトリと識別子を固定にしてアクセスするなどの対策が考えられる。

(4) セッション管理の脆弱性

ウェブアプリケーションのプログラムがログイン機能を有するなど、セッション管理の仕組みを持つ場合に、そのセッション管理の実装方法に欠陥がある場合がある。例えば、セッション管理に用いられるセッション ID が推測可能な値となっている場合、セッション ID を URL パラメータに格納している場合、TLS(SSL)を使用しているセッションの管理に用いる cookie に secure 属性がセットされていない場合等が、この脆弱性に該当する。この欠陥を攻撃されると、正規の利用者がログイン中に、その利用者になりすまして不正にアクセスする「セッションハイジャック」の被害が生じ得る。この脆弱性を排除するには、暗号論的疑似乱数生成器(CSPRNG)で生成する十分な長さの文字列をセッション ID として推測困難なものとし、secure 属性のセットされた cookie にこれを格納することでセッション ID の漏えいを防ぐ対策方法が考えられる。

(5) アクセス制御欠如と認可処理欠如の脆弱性

ウェブアプリケーションがログイン機能を有し、ログイン中の利用者にのみ利用を許可すべき機能がある場合に、ログインしていない利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「アクセス制御欠如の脆弱性」と呼ばれる。また、ログイン中の利用者のうち、一部の利用者にのみ利用を許可すべき機能がある場合に、それ以外の利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「認可処理欠如の脆弱性」と呼ばれる。これらの欠陥を攻撃されると、秘密情報の漏えい、なりすまし操作等の被害が生じ得る。これらの脆弱性を排除するには、アクセス制御と認可処理が必要な画面の仕様を明確にし、仕様に沿った実装を徹底するなどの対策が考えられる。

(6) クロスサイトスクリプティング脆弱性

ウェブアプリケーションのプログラムが HTML ページを出力する場合に、プログラムが HTML を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が HTML に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、cookie の値を盗まれてセッションハイジャックされるほか、画面の内容を改ざんされるなどの被害が生じ得る。このような欠陥は一般に「クロスサイトスクリプティング脆弱性」と呼ばれている。クロスサイトスクリプティング脆弱性を排除するには、以下を含む対策が考えられる。

- HTML の出力に際して HTML タグの出力以外の全ての出力において文字列を HTML エスケープ処理することを徹底する。
- URL を出力するときは「http://」又は「https://」で始まる URL のみを許可する。
- SCRIPT 要素の内容を動的に生成しないようにする。
- スタイルシートを任意のサイトから取り込める仕様を排除する。
- 全てのページについて HTTP レスポンスヘッダの「Content-Type」フィールドの「charset」に文字コードの指定を行う。

ただし、当該ウェブアプリケーションの仕様の都合で、これらだけでは解決できない場合もあり、その場合には追加的な対策が必要となる。

(7) クロスサイトリクエストフォージェリ脆弱性

ウェブアプリケーションが、ログイン中の利用者にのみ利用を許可する機能を有している場合に、その機能のウェブページに「アクセス制御欠如と認可処理欠如の脆弱性」の対策が施されている場合であっても、外部のサイトから当該ウェブページにリンクを張る方法により、利用者本人にそのリンクをたどらせることで、当該利用者の意図に反して当該機能が利用されてしまうという構造になっている場合がある。このような欠陥は一般に「クロスサイトリクエストフォージェリ脆弱性」と呼ばれている。この欠陥を攻撃されると、悪意ある者が仕掛けたリンクによって、不正に当該機能を操作される被害(具体的には、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害)が生じ得る。この脆弱性を排除するには、外部からのリンクによって機能が作動してはならないウェブページは、処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行するように実装するなどの対策方法が考えられる。

(8) クリックジャッキング脆弱性

ウェブアプリケーションが、サイト内のボタンやリンクをクリックするだけで作動する機能を有している場合に、悪意ある者が、当該サイトを透明化した(透明色で表示して利用者の目に見えないように設定された)フレームとして外部のサイト上に表示するようにし、利用者を当該外部サイトへ誘導して、当該ボタンやリンクの表示された画面上の位置をクリックさせるよう誘導することで、利用者の意図に反して当該機能を作動させることができてしまう場合がある。このような欠陥は一般に「クリックジャッキング脆弱性」と呼ばれている。この欠陥を攻撃されると、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害が生じ得る。この脆弱性を排除するには、ウェブサーバの設定で、HTTP レスポンスに「X-Frame-Options」ヘッダを出力するようにし、そのフィールド値に「deny」又は「sameorigin」の値をセットすることで、当該ウェブページが外部のサイトにフレームとして表示されることを拒否するよう利用者のブラウザに指示する機能を用いるといった対策方法が考えられる。

(9) メールヘッダインジェクション脆弱性

ウェブアプリケーションが電子メールを送信する機能を有し、その宛先となる電子メールアドレスをウェブアプリケーションのパラメータから指定する構造になっている場合に、悪意ある者により任意の電子メールアドレスが当該パラメータに与えられ、迷惑メールの送信のために当該ウェブアプリケーションが悪用されてしまうという被害が生じ得る。この欠陥を排除するには、電子メールの送信先電子メールアドレスはプログラム中に固定的に記述する実装方法(又は設定ファイルから読み込む実装方法)を採用して、ウェブアプリケーションのパラメータを用いるのを避けるなどの対策方法が考えられる。

(10) HTTP ヘッダインジェクション脆弱性

ウェブアプリケーションが HTTP レスポンスヘッダの「Location」や「Set-Cookie」のフィールド値を動的に出力する構造になっている場合、外部から悪意ある者によって与えられた改行文字を含む攻撃用の文字列が HTTP レスポンスヘッダに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、クロスサイトスクリプティング脆弱性の場合と同じ被害が生じ得る。このような欠陥は一般に「HTTP ヘッダインジェクション脆弱性」と呼ばれている。HTTP ヘッダインジェクション脆弱性を排除するには、HTTP レスポンスヘッダを出力する際に、直接にヘッダ文字列を出力するのではなく、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する実装方法を採用するなどの対策が考えられる。

(11) eval インジェクション脆弱性

ウェブアプリケーションのプログラムを作成する言語が、「eval」等、文字列をプログラムとして実行する機能を持つ言語である場合に、プログラムがこの機能を使用していると、外部から悪意ある者によって与えられた攻撃用の文字列が、その eval に与える文字列に混入し得る欠陥となることがある。この欠陥を攻撃されると、任意のプログラムがサーバで実行されることとなり、様々な被害が生じ得る。このような欠陥は一般に「eval インジェクション脆弱性」と呼ばれる。この脆弱性を排除するには、eval 機能を一切使用しない実装方法を採用するなどの対策が考えられる。

(12) レースコンディション脆弱性

ウェブアプリケーションの機能を複数の利用者が全く同時に利用したときに、一方の利用者向けの処理ともう一方の利用者向けの処理を途中で取り違えてしまう事態が一定の確率で発生する場合がある。このような欠陥は一般に「レースコンディション脆弱性」と呼ばれる。この欠陥により、利用者の秘密にすべき情報が第三者に閲覧される被害が生じる。この被害は、攻撃者がいなくても偶然に発生する場合もあれば、攻撃者が大量のアクセスをすることで意図的に引き起こされる場合もある。この脆弱性を排除するには、ソースコードレビューによってレースコンディションが起きえない構造にプログラムが記述されていることを確認する方法や、大量のアクセスを同時に発生させて異常が発生しないことを十分に確認するテストを行うなどの対策方法が考えられる。

(13) バッファオーバーフロー及び整数オーバーフロー脆弱性

ウェブアプリケーションのプログラムを作成する言語として、バッファオーバーフロー脆弱性等が生じない言語を採用することが望ましいが、その場合であっても、ウェブアプリケーションが、内部で C 言語等を用いて独自に作成されたプログラムを呼び出す構造になっている場合がある。その呼び出されるプログラムにバッファオーバーフロー脆弱性や整数オーバーフロー脆弱性が存在し、ウェブアプリケーションに外部から与えた文字列が当該プログラムに引き渡される構造になっていると、それらの欠陥を攻撃されて、サーバに侵入される被害が生じ得る。このような脆弱性を排除するためには、C 言語等のバッファオーバーフロー脆弱性等が生じ得る言語により作成されたプログラムが内部で呼び出されることを避けるなどの対策が考えられる。

3. その他

(1) アプリケーション・コンテンツ

アプリケーションプログラム、ウェブコンテンツ等の総称をいう。

(2) ドメインネームシステム(DNS)

インターネットを使った階層的な分散型システムで、主としてインターネット上のホスト名や電子メールに使われるドメイン名と、IP アドレスとの対応づけ(正引き、逆引き)を管理するために使用されるものをいう。DNS では、端末等のクライアント(DNS クライアント)からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係等について回答を行う。

(3) データベース

データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものをいう。

要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び取扱者の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

(4) IPv6(Internet Protocol Version 6) 通信回線

従来の IPv4 にかわるものとして設計された、次世代のインターネットプロトコルのことをいう。従来よりも IP アドレスを多く作成することにより、より多くのユーザやデバイスがインターネット上で通信できるようになった。

サーバ装置、端末及び通信回線装置等に、IPv6 技術を利用する通信(以下「IPv6 通信」)の機能が標準で備わっているものが多く出荷されているが、運用者が意図しない IPv6 通信が通信ネットワーク上で動作している可能性がある。これらは、不正アクセスの手口として悪用されるおそれもあることから、不正アクセスを検知する対策等を講じていく必要がある。

(5) HSE

健康（Health）、安全（Safety）及び環境（Environment）を指す。産業用オートメーション及び制御システムを対象としたサイバーセキュリティのマネジメントシステムである CSMS 認証基準（Ver.2.0）では、物理的リスクのアセスメントの結果、HSE 上のリスクのアセスメントの結果及びサイバーセキュリティリスクのアセスメントの結果の統合を要求している。

（6）MDM

Mobile Device Management の略称。スマートフォン等のセキュリティ設定を統合的に管理するためのツール。

（7）VDI

Virtual Desktop Infrastructure の略称。サーバ上に仮想の PC を複数台用意し、サーバに接続した利用者からはあたかも個別に PC が用意されているような使い勝手で利用できるようにする環境のこと。

（8）VPN

Virtual Private Network の略称。主にインターネット上で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。

（9）ゼロトラストセキュリティ

ゼロトラストセキュリティとは、外部ネットワーク（インターネット）と、内部ネットワーク（LAN）との境界による防御（境界型セキュリティ）には限界があり、内部ネットワーク内にも脅威が存在しうるという考えのもと、データや機器等の単位でのセキュリティ強化をうたった考え方を指す。

（10）ランサムウェア

感染した端末上のデータを勝手に暗号化してしまうマルウェア。攻撃者はその端末の利用者に対し暗号化を解除する見返りに金銭等を要求して利益を得ること。

（11）リモートデスクトップ

自らの手元にある機器から、ネットワークを経由して他の端末を操作するための仕組みのこと。

（12）ローカルブレイクアウト

オフィスネットワークやデータセンター等の拠点を介することなく、端末から直接インターネットへアクセスするネットワーク構成のこと。

（13）オンプレミス

従来型のシステム構築手法で、自組織の施設内（事務所内や自組織で保有するデータセンター内等）にシステムを設置する方式のこと。

(14) クラウドサービス

ネットワークに接続されたコンピュータ資源(計算能力、記録装置、情報システム等)を、ネットワーク(インターネット)を介して必要なときに必要な分だけ利用できるようなサービスを指す。クラウドサービス事業者が利用者に提供する資源の範囲(レベル)によって、SaaS・PaaS・IaaS という分類がある。

(15) IaaS(Infrastructure as a Service)

クラウドサービスモデルの一つ。利用者に CPU、ストレージ、メモリ等のコンピュータリソースが提供される。利用者はそのリソース上に OS 等を構築することができる。

(16) PaaS(Platform as a Service)

クラウドサービスモデルの一つ。IaaS に加えて、OS、基本機能、開発環境等もサービスとして提供される。利用者はそれらを組み合わせて情報システムを構築することができる。

(17) SaaS(Software as a Service)

クラウドサービスモデルの一つ。PaaS に加えて、利用者に特定のアプリケーション(メールサービスやファイルサービス、グループウェア等)の機能がサービスとして提供されるもの。

(18) 5G

4G など従来の移動通信システムと比較して、「超高速」、「超低遅延」、「多数同時接続」であるという特長を有しており、IoT 時代の基盤技術として、様々な産業分野での利活用が期待されている。

(19) ローカル 5G

地域の企業や自治体等の様々な主体が自らの建物や敷地内でスポット的に柔軟に構築し利用することのできる 5G のこと。

(20) テレワーク

テレワークの形態として「在宅勤務」、「サテライトオフィス勤務」、「モバイル勤務」があげられる。テレワークにおいて情報資産を守るためには、「ルール」・「人」・「技術」のバランスがとれた対策を実施し、全体のレベルを落とさないようにすることが重要である。

(21) バックドア

外部からコンピュータに侵入しやすいように、“裏口”を開ける行為、または裏口を開けるプログラムのこと。このプログラムが実行されてしまうと、インターネットからコンピュータを操作されてしまう可能性がある。なお、一部のウイルスでは、感染時にバックドアを埋め込むことがある。

（22）CVE 情報

CVE（Common Vulnerabilities and Exposures）とは、共通脆弱性識別子。個別製品中の脆弱性を対象として米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子。個別製品中の脆弱性に一意の識別番号「CVE 識別番号（CVE-ID）」を付与することにより、組織Ａの発行する脆弱性対策情報と、組織Ｘの発行する脆弱性対策情報とが同じ脆弱性に関する対策情報であることを判断したり、対策情報同士の相互参照や関連付に利用したりできる。

（23）JVN iPedia

IPA が運営する脆弱性対策情報データベース。

（24）サイバーハイジーン

インターネットの利用環境など、ICT 環境を健全なセキュリティ状態に保っておくこと。

（25）EDR

EDR（Endpoint Detection and Response）とは、組織内のネットワークに接続されているエンドポイントからログデータを収集し、解析サーバーで相関解析、不審な挙動・サイバー攻撃を検知し、管理者に通知する、エンドポイント・セキュリティ・ソリューション。

（26）フォレンジック（デジタルフォレンジック）

不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。