用語解説

API

Application Programming Interface の略。オペレーティングシステムや各種ソフトウェア製品が提供する種々の機能を、アプリケーションプログラムから直接呼び出して利用できるよう用意された一連の処理手続きの入口、およびそれらの呼び出しの仕様。

Cookie

HTTP プロトコルの通信において、Web サーバが Web クライアントに預けておくと、Web クライアントから Web サーバへ自動送信される小さなデータ。Cookie は、1 つの「名前＝値」の対、およびいくつかの属性からなる。Web サーバは、HTTP レスポンス電文中に含める形で Cookie を発行し、Web クライアントはそれを一定期間預かる。Web クライアントは、HTTP リクエスト電文中に含める形で Cookie の値を Web サーバへ返送する。Web クライアントは、複数の Web サーバからそれぞれ複数の Cookie を預かることができる。Cookie の返送は、Web クライアントが HTTP リクエストを送信するたびに行なわれるが、どの Cookie をどの Web サーバ宛の HTTP リクエストに含めるかは、Cookie を預かった際に与えられていた属性によってきまる。Cookie は、発行した Web サーバそのものへ返送される形で用いられることが多いが、それ以外の使われ方をすることもある。

hidden 項目

hidden フィールドとも呼ばれる。Web ページのフォームの項目の一種であって、画面には描画されない項目。hidden 項目もまた、他のフォーム項目と同様、項目名（name）と値（value）の対からなる。hidden 項目は、フォームを含むページを出力したプログラムが、フォームのデータを受け取るプログラムへパラメータ値を受け渡す目的で用いられる。hidden 項目は画面にこそ描画されないが、ユーザはブラウザを操作して容易にその内容を見、書き換えることができる。

HTTP リクエスト

HTTP プロトコルの、Web クライアントから Web サーバへ送られる通信メッセージ。この通信メッセージは、HTTP リクエストヘッダと HTTP リクエストボディの 2 つの部分からなる。HTTP リクエストは、Web サーバ内のリソースを URL を用いて単純に呼び出す場合と、Web サーバ内のプログラムを呼び出すとともに、そのプログラムにパラメータ渡す場合とがある。プログラムに渡すパラメータを HTTP リクエストに含める方法には、HTTP リクエストヘッダに含めるものと、HTTP リクエストボディに含めるものとがある。後者は、HTTP リクエストにおいて「POST」というメソッドを用いるケースである。

HTTP レスポンス

HTTP プロトコルの、Web サーバから Web クライアントへ送られる通信メッセージ。この通信メッセージは、HTTP レスポンスヘッダと HTTP レスポンスボディの２つの部分から構成される。HTTP レスポンスボディは多くの場合、HTML で記述された Web ページを含むが、それ以外に、スタイルシート、画像、PDF、音声、動画等、あらゆる種類のファイルを含み得る。HTTP レスポンスの内容は、キャッシュサーバやプロキシサーバといった中計設備において暫くの間保持され、Web クライアントは、本来の Web サーバではなくこれらの設備から HTTP レスポンスを受け取る場合がある。これは、同じ HTTP リクエストに対して常に同じ HTTP レスポンスが返されるような場合には、Web サーバやネットワーク通信の負荷を軽減でき、有効である。

HTTP レスポンスによるキャッシュ偽造

別名「HTTP レスポンス分割」、英文 HTTP response splitting。Web アプリケーションが出力する HTTP レスポンスヘッダに不正な内容が挿入されるよう計らい、それがネットワーク上のキャッシュ設備に記録されるようにし、そのキャッシュ設備を利用するすべてのユーザに偽造されたコンテンツを見せる攻撃、およびそれを防ぐことができない脆弱性。「HTTP レスポンスによるキャッシュ偽造」は、IPA の「セキュア・プログラミング講座」（2007 年版）で用いられる用語である。

HTTP 認証

HTTP プロトコルに定められている、ユーザ認証のしくみ。HTTP 認証にはベーシック認証、ダイジェスト認証、PAKE 認証等があるが、現在広く用いられているものは、ベーシック認証である。ベーシック認証は、ブラウザが Web サーバへリクエストを送るたびに、そこにユーザ ID とパスワードを平文で含める方法であるが、毎回パスワードがネットワーク上を流れることには問題がある。ダイジェスト認証および PAKE 認証は、basic 認証の強化を意図したものである。ただし、現時点では普及しておらず、実験的な性格が強い。

SQL 注入

別名「SQL インジェクション」、英文 SQL injetion。プログラム中で SQL ステートメントの文字列を組み立てている箇所に外部から別の SQL ステートメントの断片を送り込み、不正にデータベースにアクセスする攻撃、およびそれを防ぐことができない脆弱性。「SQL 注入」は、IPA の「セキュア・プログラミング講座」（2007 年版）で用いられる用語である。

URL リライティング

Web アプリケーションのセッションの維持のために複数 Web ページ間でセッション ID を受け渡す方法のひとつ。Web サーバ側がページの内容を送信する際、ページの中の URL を参照している箇所をすべてセッション ID パラメータが付加された形の URL に書き換えて送信する方法。セッション ID を受け渡す方法にはほかに、Cookie を用いる方法、フォームの不可視フィールド（hidden 項目）を用いる方法がある。

Web アプリケーション

ユーザインタフェースに Web ブラウザを用い、Web サーバでデータベースや主要なデータ処理ロジックを動作させる、クライアント／サーバ型のアプリケーションプログラム。最近では Ajax 等、Web ブラウザ上で高度な処理を行う Web アプリケーションも増えてきた。

アカウント

Web コンテンツを提供しているひとつのホスト、もしくはそこで提供されているコンテンツのこと。http(s)://ホスト名/ の形の URL で識別される。最近の公報媒体では、Web サイトを示す際にたんにホスト名を書き、www.example.com のように示すことも増えている。

アカウントのロックアウト

攻撃ツールを用いて辞書に載っている単語あるいは総当たりパターンを試すことで、正しいパスワードを見つけ出し、アカウントに入り込む攻撃が存在する。この種の攻撃に対抗する目的で、短時間に一定回数ログイン失敗が連続すると、そのアカウントにおけるログイン受付を一定時間停止させる措置のこと。ロックアウト（施錠して閉め出すこと）が本来の名称の由来であるが、短く、アカウントの「ロック」と呼ばれることもある。

アクセス制御

意図したユーザのみが特定のコンピュータリソースにアクセスでき、他者はアクセスできないことを強制する、システムの仕組み。アクセス制御は、アクセスしようとしているのが本人であることを確認する「ユーザ認証」（Authentication）手続きと、認証済みのユーザにコンピュータリソースへのアクセスの許可・禁止の制御を行う「アクセス認可」（Authorization）の２段階から構成される。

アプリケーション

→ アプリケーションプログラム

アプリケーションプログラム

アプリケーションソフトウェア、あるいはたんにアプリケーションとも呼ぶ。他のプログラムを稼働させる環境を提供するのではなく、それ自体を用いて各種領域の問題解決に役立てることを目的としたプログラム。ワードプロセッサ、会計ソフトウェア、作図ソフトウェア、通信クライアント等、多数のものがある。World Wide Web システム上で動作するアプリケーションプログラムのことを、Web アプリケーションと呼ぶ。

拡張子

ファイル名の末尾にあるピリオド（.）以降の文字列で、ファイルの種類を示すもの。例えば、.gif .html .jpg .properties .txt 等がある。

コマンド注入

別名「コマンドインジェクション」、英文 command injection。ステルスコマンディング stealth commanding と呼ばれることもある。プログラム中でシェルコマンドの文字列を組み立てている箇所に外部から別のシェルコマンドの断片を送り込み、不正にサーバコンピュータを操る攻撃、およびそれを防ぐことができない脆弱性。「コマンド注入」は、IPA の「セキュア・プログラミング講座」（2007 年版）で用いられる用語である。

コンテンツ

ひとまとまりの情報やデータのこと。ニュース、画像、音楽、動画、ゲーム等、それ自体が閲覧・再生・鑑賞の対象となり得るものを指すことが多い。

サニタイズ

→ 無害化

スクリプト

あらかじめコンパイルすることなく、その場で実行できる、テキストで書かれたプログラム。スクリプトは、インタプリタと呼ばれるソフトウェアによって解釈実行される。スクリプトのプログラミング言語には、例えば、JavaScript、Perl、PHP、シェルスクリプト等がある。

スクリプト注入

別名「クロスサイトスクリプティング」、英文 cross-site scripting、略称 XSS。Web サイトの正規ユーザのブラウザに JavaScript 等で記述した悪意のスクリプトプログラムを送りつけ、偽のページを描画してフィッシング詐欺の被害に遭わせる、セッション ID の値を盗み出してセッション乗っ取りを起こす等に利用される攻撃手口、およびそれを防ぐことができない脆弱性。「スクリプト注入」は、IPA の「セキュア・プログラミング講座」（2007 年版）で用いられる用語である。

セッション

Web クライアントと Web サーバの会話が維持されている状態のこと。すなわち、複数の Web ページの前後関係の文脈が正しく維持されている状態のことである。Web アプリケーションにおけるセッションには、ページの前後関係の維持、ログイン状態の維持、リクエスト強要（CSRF）対策の３つのレベルがあり得る。Web アプリケーションは、セッション ID と呼ばれる識別子を発行して個々の Web クライアントを識別し、それぞれとのセッションを維持するのが通常である。

セッション ID の強制

別名「セッションフィクセーション」、英文 session fixation。Web アプリケーションの「セッション乗っ取り」を行う手口のひとつ。攻撃者は自ら確保したセッション ID を「スクリプト注入」等の手口を用いて被害者のブラウザに植え付け、被害者に既知のセッション ID を使わせるというものである。セッション ID の強制を、セッション乗っ取りとは別のものに分類する考え方もあるが、本書ではセッション ID の強制はセッション乗っ取りを行うための一手口であるという立場をとる。「セッション ID の強制」は、IPA の「セキュア・プログラミング講座」（2007 年版）においては「セッション ID のお膳立て」と呼んでいる。

セッション乗っ取り

別名「セッションハイジャック」、英文 session hijack。Web アプリケーションの正規ユーザのセッション、とくにログインセッションに別人が接続し、本人の権限で不正 Web サイトを使用する行為。「セッション乗っ取り」は、IPA の「セキュア・プログラミング講座」（2007 年版）で用いられる用語である。

トランザクション

情報システムに投入されるデータ更新処理の単位。データベースシステムにおいては、そっくり取り消しが可能な更新処理の単位のことを指すが、Web システムにおいてはかならずしもその限りではない。Web アプリケーションが受け取る HTTP リクエストの１つ１つを、それぞれトランザクションであるとみなすことができる。

ハッシュ関数

メッセージダイジェスト関数とも呼ばれる。任意の長さのバイト列を入力としてとり一定のビット数の値を出力する関数であり、わずかな違いしかない二つの値を処理したとき、それぞれに対して生成される値どうしは大きく異なるよう、アルゴリズムが工夫されている。一般に、ハッシュ関数の出力値からその入力値を推定することは困難である。ただし、コンピュータ処理速度の向上に伴い、出力ビット数の少ない MD5、SHA1 等の古典的なハッシュ関数は今後容易に破られるおそれがある。

パスワード

ユーザ認証の際、いまシステムと会話しているのがユーザ本人であることを証明する目的でユーザがシステムに提示する秘密のデータ。

パスワードリマインダ

パスワードを忘れたユーザを救済するためのしくみ。ユーザは、あらかじめシステムに登録しておいた本人確認用の秘密データを提示することによって本人であることの確認を受け、システムからパスワードを通知してもらうか、または再設定の機会を得る。

平文

ひらぶん、と読む。暗号化されていない、読み取りが容易なデータ。一見暗号化されているように見える文字列であっても、特定のエンコード方法で表現されているのみである場合は、それも平文である。

無害化

アプリケーションプログラムからデータベースシステム、スクリプトのインタプリタ、Web ブラウザ等に指令の文字列を渡す場面で、その文字列中に意図せぬ特殊記号が混入されていると指令の意味が変わり、セキュリティ被害を生じるおそれがある。無害化は、そのような特殊記号を別の表現に置き換えてから相手先に渡すことによって、好ましくない事態を避ける措置である。無害化は、「エスケープ」「フィルタ」「サニタイズ」とも呼ばれる。

リクエスト強要

別名「クロスサイトリクエストフォージェリ」、英文 cross-site request forgery、略称 CSRF。Web アプリケーションの正規ユーザを悪意のコンテンツで誘導して、本人の望まないトランザクションを投入させる攻撃、およびそれを防ぐことができない脆弱性。「リクエスト強要」は、IPA の「セキュア・プログラミング講座」（2007 年版）で用いられる用語である。

ログイン

本人であることを確認し、システムの利用を開始する手続き。ログイン手続きの中の本人であることを確認する部分は、アクセス制御の「ユーザ認証」手続きに相当する。システムを操作しているのが本人であることを確認する目的で、システム利用途中に再度ユーザ認証を行うような設計があり得るので厳密には、ログイン≠ユーザ認証 であるが、多くの場合この二つを同一視してもあまり支障はない。システムの利用を終了する手続きが「ログアウト」である。「ログイン」と「ログアウト」の語を用いているのは主に UNIX、GNU/Linux のオペレーティングシステムである。Windows オペレーティングシステムでは、「ログオン」と「ログオフ」の語が用いられている。