

用語集（技術コース 標準編 / 専門編）

Cookie（クッキー）

ウェブサーバとウェブブラウザの間で行う通信において利用される仕組みの一つ。Cookie の発行は通常、ウェブサーバが行う。ウェブブラウザは、受け取った Cookie 情報を自身に保存し、発行したウェブサーバにアクセスする度に、そのウェブサーバに対して保存した Cookie 情報を送り返す。この特徴により、Cookie は、ユーザ情報やセッション ID の格納に用いられるケースが多い。利用にはセキュリティ上の注意が必要である。

DNS（Domain Name System）

インターネットにおけるホスト名と IP アドレスとを対応させるシステムのこと。インターネット上にある全世界の DNS サーバが協調して動作する、階層的な分散型データベースシステムである。

IDS（Intrusion Detection System / 侵入検知システム）

システムに対する侵入 / 侵害を検出・通知するシステムのこと。システムを監視し、セキュリティポリシーを侵害するような行為を検出した場合に、その行為を可能な限り早く管理者に伝えるとともに、調査分析の作業を支援するために必要な情報を保存・提供することが目的である。

IPS（Intrusion Prevention System / 侵入防止システム）

システムに対する侵入 / 侵害を阻止するシステムのこと。異常を検知した際に自動的に通信を停止する機能を有したものであり、一般的には IDS の発展形と言える。

LAME delegation（レイムデレゲーション）

DNS サーバにおいて、上位サーバに登録したサーバが正しく動作していない、設定に誤りがあるなどの要因で、ドメイン名に関する情報の委任が正しく行われていない状態。

SQL（Structured Query Language）

リレーショナルデータベースマネジメントシステム（RDBMS）において、データの操作や定義を行うための問合せ言語のこと。構造化問い合わせ言語とも言う。元々は IBM 社が作った言語であるが、現在ではアメリカ規格協会（ANSI）や JIS で標準化されている、世界標準規格。

SQL インジェクション（SQL Injection）

データベースアクセスのために SQL 文を用いるプログラムにおいては、SQL 文を構成する際、プログラム中の式の値を SQL 文に埋め込む場合には、引用符で括られる文字列について、引用符が含まれているならばそれをエスケープ処理しなければならない。これを怠ると、

正当なデータに対して SQL 文の実行がエラーとなる不具合が生じる。このバグが悪意ある者によって与えられ得る文字列を扱う箇所に存在すると、それはセキュリティ上の脆弱性となる。攻撃者が悪意あるコマンドを与えると、データベースの内容を改ざんされたり、情報を盗み出されるなどの被害が生じる。このような攻撃を SQL インジェクション攻撃と呼び、その原因箇所を同脆弱性と呼ぶ。

SSH (Secure SHell)

ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。通信上のデータはすべて暗号化されるため、Telnet のようにデータが平文で通信されるプロトコルに比べて、安全性が高い。SSH の利用に際しては、いくつかの認証方式を選択することが可能だが、パスワード認証はブルートフォース攻撃などにより認証を突破されてしまう可能性があるため、公開鍵認証を用いることが推奨される。

WAF (Web Application Firewall)

ファイアウォール的一种で、特にウェブアプリケーションによる通信を管理するもの。従来からのファイアウォールは基本的にネットワーク層で管理するが、WAF は基本的にアプリケーション層で管理する。

エスケープ処理

処理系によって特別な意味を持つ文字（記号文字など）に対し、別の文字に置換するなどして、特別な意味を持たない文字に変換する処理のこと。

クロスサイト・スクリプティング (Cross-Site Scripting / XSS)

ウェブアプリケーションで HTML ページを出力するプログラムにおいては、文字列を出力する際、それがテキストとして出力する部分なのか、それとも HTML タグとして出力する部分なのかによって、本来、文字列に対して行うべき処理が異なる。テキストとして処理する部分では、「<」「>」「&」がタグ等として解釈されないよう「<」「>」「&」に変換する必要があり、また、引用符で括った部分に出力する場合は、埋め込む文字列中に含まれる同じ引用符をエスケープ処理しなくてはならない。これを怠ると、開発者の意図に反して画面が崩れるといった不具合が生ずる。このバグが外部から与えられ得る文字列を表示する箇所に存在すると、それはセキュリティ上の問題即ち脆弱性となる。攻撃者がスクリプトを含む文字列を与えた場合、スクリプトの同ドメインルールのセキュリティモデルが破られ、利用者の cookie を盗まれたり、本物サイト上に偽のページを表示させられフィッシング詐欺につながるといった危険をもたらす。このような攻撃をクロスサイト・スクリプティング攻撃と呼び、その原因箇所を同脆弱性と呼ぶ。

公開鍵認証

公開鍵暗号を用いた、認証方式のこと。

(参考) 公開鍵暗号方式

秘密鍵と公開鍵との鍵のペアを使用して、暗号化と復号を行う方式のこと。公開鍵を使用して暗号化した場合、復号には、それとペアを成す秘密鍵が必要。

(参考) 共通鍵暗号方式

暗号化と復号に同一の(共通の)鍵を用いる暗号方式のこと。

標的型攻撃 (targeted attack)

特定の組織や個人を狙って行われる攻撃のこと。不特定多数を狙って行われる攻撃と区別して、このように呼ばれている。この攻撃では、攻撃者は攻撃対象のことを十分に調査した上で攻撃を仕掛けるため成功率が高く、攻撃の範囲が狭いため大きな話題になりにくいのが特徴。

フィッシング詐欺 (Phishing)

「銀行からのお知らせメール」などと嘘をついて偽のウェブサイトに誘導し、口座番号やパスワードを利用者に入力させて盗む、詐欺の手法。

ボット (Bot)

コンピュータを遠隔操作することを目的に作成されたソフトウェアで、ウイルスのように他のコンピュータに感染する機能のあるもの。ボットに感染したコンピュータは、外部からの指示に従い、他のサイトへの攻撃や、スパイウェアとしての活動などを行う。