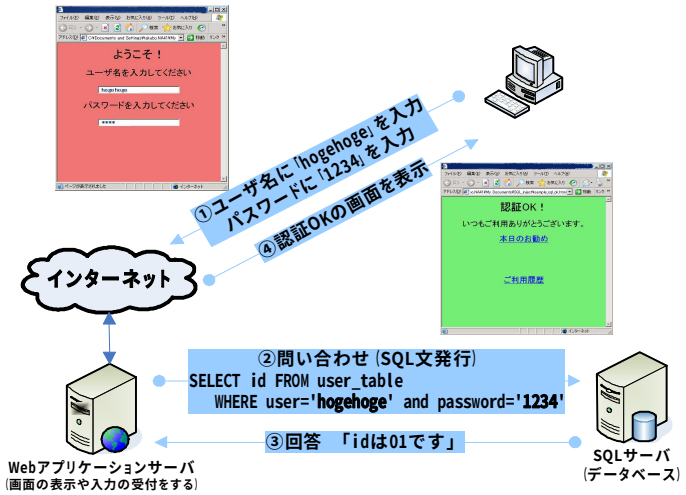
ネットエージェント株式会社

One Point Wall の SQL Injection ルールについて

OnePointWall の SQL Injection ルールは、Web アプリケーションサーバもしくはデータベースクライアントソフトからデータベースサーバへのネットワークを介した通信において SQL Injection 攻撃で利用される特徴のある SQL 文があった場合、該当通信を検知･遮断します。

※ 対応している SQL Injection パターンは一般的な文献にある方法のみです。脆弱性検査のプロフェッショナルによるマニュアルオペレーションに対しては防ぐことができません。具体的な攻撃方法についてはご購入後ユーザー専用ページより完全なホワイトペーパーをご覧ください。

SQL Injection とは、データベースと連動している Web サイトなどで、アプリケーションが想定していない**データベース操作言語 (SQL: Simple Query language)** を故意に**注入 (Injection)** することで、データベースを不正に操作する攻撃手法を言います。



データベースと連動している Web サイトの例

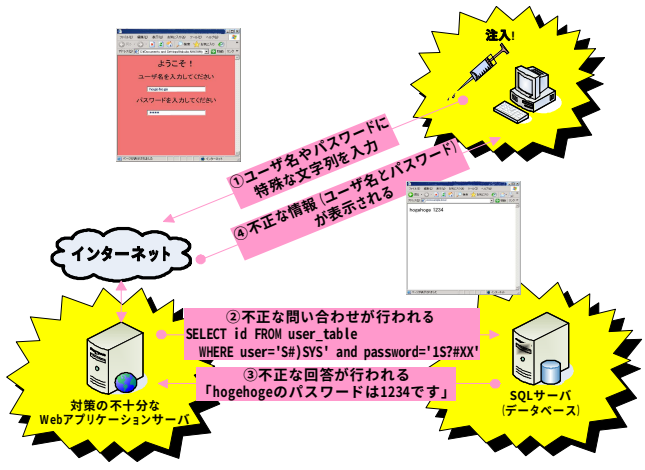
最新の調査によると **2005 年後半以降、SQL Injection による攻撃件数が急増**し、被害内容も深刻化しています。

例えば、多くの通販サイトでは左図のように顧客や商品情報等を保持する SQL サーバ（データベース）と連携して動作しています。

この場合 **Web アプリケーションサーバ**が画面表示やユーザからの入力受付を担当し、ユーザの要求を SQL 文に加工して **SQL サーバ**へ問い合わせを行います。

SQL Injection 攻撃は、通常、ユーザ名や商品名などが想定さている入力に **SQL に特異な文字列**を挟み込むことで不正に情報を引き出したり、データベースへの侵入や改ざんを行います。

実際の SQL Injection による攻撃は右図のように、**①雑誌や Web サイトで公開されている特殊な文字列を Web のフォームにコピーアンドペーストして不正にアクセスを試みる**ような単純な方法から、**②Web サーバの反応を見ながら様々な SQL 文を直接サーバに発行しデータベースを操作する**高度な方法、さらに**③それらを自動的に行うツール**など、手法も攻撃者のレベルも様々です。



SQL インジェクションの例

（具体的な攻撃手法は入れていません）

ネットエージェント株式会社

昨今のセキュリティ意識の高まりにより、多くの Web サイトでは SQL Injection への対策が施されつつありますが、**一方で①や③のような手軽で技術力を要しない攻撃を好む「スクリプトキディ」と呼ばれる層による攻撃量は膨大**で、メンテナンス作業中の一瞬のすきやケアレスミスが重大な情報漏洩事件の引き金となることも多いようです。

今回の SQL Injection ルールで対応するのは主に**①のような攻撃**になりますが、②や③のような攻撃も初期には①のような手法を用いている可能性もあり OPW 導入による効果が見込まれます。

【対応データベースについて】

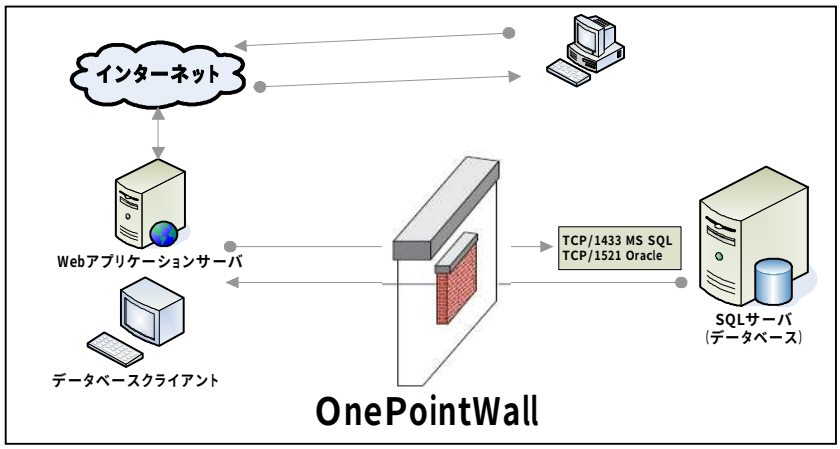
SQL エンジンは実装によってパケットの構造がかわるため、個別にルールが必要になります。今回対応したのは**Microsoft と Oracle の SQL サーバ**になります。対応バージョンは下記のとおりです。その他のバージョンの詳細についてはテクニカルサポートまでお問い合わせください。

MSSQL：SQL Server 2000 および 2005、SQL Server 2000 Desktop Engine (MSDE)

Oracle：Oracle 8i、9i、10g

【設置場所について】

今回のルールは Web アプリケーション (またはデータベースクライアント) とデータベースサーバの間の通信に特化したものです。データベースへの接続ポートが**固定されている (MS SQL は TCP/1433、TCP/Oracle は 1521) 必要があります**。特に MS SQL 2005 はデフォルトでポートが動的になっていますのでご注意ください。



【注意事項】

このルールは SQL のクライアント・サーバ間の通信に特化したものです。既存の環境に適用した場合、誤検知率が高くなる可能性があります。ご利用の際は SQL Injection ルールのみを適用した OnePointWall を別途設置することを推奨いたします。

データベースへのアクセスを取りまとめるミドルウェアを利用してデータベースサーバと通信していた場合 TCP セッションがいったん途切れるため、他の通信が停止する場合があります。

SQL 文送信時に SQL のコメントを使用すると誤検知する可能性があります。使用している SQL 文にコメントがある場合はコメントを抜いてから利用してください、抜けない場合は comment と入ったルールのチェックを外してください。外した場合はいくつかの SQL Injection 手法での攻撃を受け付けるようになってしまいます。

OnePointWall の SQL Injection ルールを全て適応した場合でも完全にデータベースサーバへの攻撃を防げるものではありません。