公開サーバのセキュリティ対策

総合情報処理センター　堀川慎一

平成 22 年度は、特に公開サーバを対象として、現有機器のセキュリティ対策を強化するとともに、新たに WAF（Web Application Firewall）の導入を行いました。以下では、その概要について述べさせていただきます。

当センターでは前年度末より、スタンドアロン型の侵入検知防御システム（IPS）を運用しています。この IPS では、FTP のパスワード総当たり攻撃をほぼ完全に防御できることから、本学では巷を賑わせたいわゆる「Gumblar」の被害は一件も発生していません。ところが、実際に防御した攻撃の内訳を調べてみますと、FTP や SSH といったリモートアクセス関連よりも、Web サーバを直接狙ったものが大半を占めることがわかりました。具体的には、PHP の脆弱性を突いて不正にコマンドを実行させようとしたり、SQL データベースから不正に情報を引き出そうとするものです。インターネットに公開されたサーバの場合、アドレスが広く知られているため狙い撃ちは防ぎようがありませんが、ポートスキャン（アドレススイープ）によって探し出したサーバに対し無差別に攻撃を行う活動も依然として多く観測されていました。そこで、少しでも危険度を下げるべく、Web サーバで用いられる HTTP の TCP 80 番ポートや HTTPS の TCP 443 番ポートについて、探索的なアクセスを行ってきたホストを一定時間遮断するよう対策を施しました。

しかしながら、新たな Web アプリケーションが日々生み出される現状においては、それらに応じてよりきめ細やかに通信内容を精査することが求められつつあります。このため、数ヶ月間の評価を経て、その名の通り Web に特化したファイアウォールである WAF を導入することとしました。これにより、現有 IPS では処理能力の問題からカバーしきれなかった Web 関連の非常に多岐に渡る攻撃にも対応可能となり、セキュリティ対策の強化が図れることを期待しています。

このように当センターでは各種セキュリティ対策を年々強化していますが、インターネットからのアクセスを許可した時点で 100%の安全はなく、時には思わぬ隙を突かれることがあります。その代表例が、HTTP の PUT メソッドにより不正なファイルを挿入するというものでした。PUT メソッドは、通常の Web サーバでは許可されていないはずなのですが、一部の環境では標準で受け付けてしまうことがあるようです。本学の侵入検知システム（IDS）では、現在でも Web サーバに対して継続的に「PUT /indonesia.htm」なるアク

セスを観測しています。最悪の場合にはこのファイルを目印として、サーバが乗っ取られる危険のあることが明らかとなっていますので、Web サーバを管理されている方は少なくとも DocumentRoot 直下に見知らぬファイルが存在しないか、定期的に確認されることを強くおすすめします。