Scan 覆面座談会
「いい WAF とは」

株式会社イード

目次

謝辞

情報セキュリティのプロフェッショナルの皆様に役に立つ情報をお届けするために、ScanNetSecurityでは2012年新春、専門家をお招きして、都内某所で座談会形式でディスカッションを実施しました。テーマは「いいWAFとは何か」です。

WAF（Web Application Firewall）の技術や運用に詳しい識者をお招きし、フリーディスカッションを行うことで、WAF導入の一助となることを目的としています。趣旨にご賛同いただいた参加者の皆様は、国内外の第一線で活躍する方ばかりです。

本座談会は、さまざまな団体や企業の枠を超えて、自由闊達な本音のご意見を頂戴するため、氏名はもちろん、所属組織の商号や名称一切を誌面非公開とする、覆面形式でのディスカッションとさせていただきました。

なお、座談会冒頭では、専門家としてのプロ意識を新たにするために、ビールによる乾杯が行われました。

ご参加いただいた有志諸氏へ心より感謝申しあげます。

ScanNetSecurity 発行人
高橋潤哉

参加者一覧(敬称略)

●参加者一覧(敬称略)

・クワガタ情報ソリューションズ株式会社　桑田　健二
略歴:同社エンジニアとして多数のWAFの導入、運用支援を行った実績を持ち、国内のほとんどの商用WAFに精通する。

・株式会社ビートルシステム　兜　隆一
略歴:コンサルタントとして、WAFの導入運用に関わる一方で、Webアプリケーションの脆弱性に詳しい。

・ヤンマインテリジェンス株式会社　鬼塚　昌宏
略歴:セキュリティコンサル会社経営者。主に中小企業を対象に多数のコンサル実績を持つ。

※註:参加者一覧の社名、商品名及び氏名は仮名であり実在しません

・司会進行　ScanNetSecurity編集長　上野　宣

いいWAFとは

●WAFの導入について

--導入のエピソードはありますか？

クワガタ情報　桑田：
　セキュリティ診断が入ると「アクセス抜けたけど何なの？」と聞かれることがあります。文字列型のところにシングルコードなしに「or1=1」とか検出するのですが、それは攻撃ではなくただの文字列ですと説明することは多いですね。そこにupdateやdeleteなど入ってくれば攻撃と思われるので止めますと説明します。

ビートルシステム　兜：
今はそうですよね。昔はそういったものも全部止めていました。今でもありますが……。あと、導入で思い出すのはImpervaですね。結構導入したのですが、ことごとく初期不良で大変な目に遭いました。Impervaでなくてもチューニングは大変ですが。

クワガタ情報　桑田：
WAFは導入が大変というイメージを持っているお客さんが多いです。導入した当日から使えるくらいでないといけませんね。

ビートルシステム　兜：
バラクーダの宣伝はそうですね。箱から出して30分で運用を開始できると謳っています。最近はよく売れています。

クワガタ情報　桑田：
導入のしやすさを売りにしていますね。誤検知が気になる人に対しては、ひとまずスルーして後でログをチェックして修正していく。

上野：
最近のWAF製品は、わりと簡単に導入できるようになっているんですか？

クワガタ情報　桑田：

Intentionally blank

Scan 覆面座談会「いいペンテストとは」

発行　株式会社イード
発行人　高橋潤哉
頒価　10,000 円(税抜)
発行年月日　2013 年 5 月 1 日

編集･製作　株式会社イード
ScanNetSecurity 編集部
〒164-001　東京都中野区中央一丁目 38 番 1 号
TEL　03-6304-0217　／　FAX　03-5332-5760
MAIL　info@netsecurity.ne.jp　／　URL　scan.netsecurity.ne.jp