

インターネットセキュリティ インサイト

WatchGuard 脅威ラボ

2017年第2四半期

敵の行動を知らずに、
攻撃から自らの身を守る術を知るのは困難です。

脅威のトレンド

Firebox フィードが記録
した脅威データは

33,590 台の
Firebox アプライアンス か
ら収集

21% の増加

ゲートウェイアンチウイル
スサービスがブロックした
マルウェアの数は

10,919,403

35% の増加

さらに、APT Blockerが
防御したマルウェアの数

5,484,320

53% の増加

47%
のマルウェアは

ゼロデイ攻撃

53%
のマルウェアは

既知のマルウェア

継続したWebを標的とした攻撃

マルウェアの検知は

41%

増加 (Q1, 2017との比較)

上位10種類の攻撃がWebサービスを
ターゲットとして、**サーバー側**と**クライアント側**
の両方から攻撃

従来のファイアウォールによる
防御は最新の脅威に対して
十分ではありません。

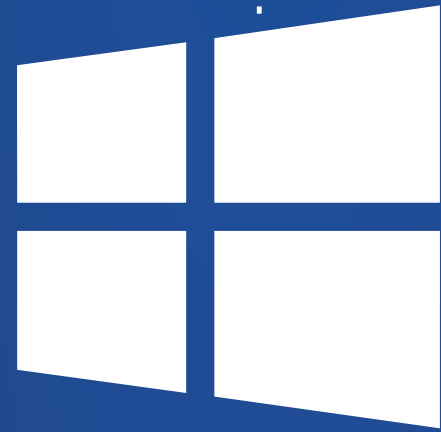
Webアクセスを許可するには、ファイアウォール上のポートを開放
することになるため、**IPS** などのセキュリティ機能を追加して、
Web 攻撃を検知する必要があります。

脅威のトレンド

ログイン/パスワード

Webアプリケーションの
認証に対する攻撃

認証システムに対する2種類の攻撃手法
1. ブルートフォース攻撃
2. Linuxシステムのパスワードファイルへの
リモートからのハッキング



Windowsの認証情報
への攻撃

Web(HTTP)接続を介して配信されたマルウ
ェアの半分以上が、Mimikatzという名前の
ツールに結び付けられる「SCGeneric」
シグネチャのパリエーションでした。



メール経由でのJavaScript

SMTPやPOP3などの電子メールプロトコルを
使用して配信されるマルウェアの大部分は、
JavaScriptベースのものです。
前回のJavaScriptダウンロードに新たにトップ
10の脅威であるJS/Phishシグネチャが加わりま
した。

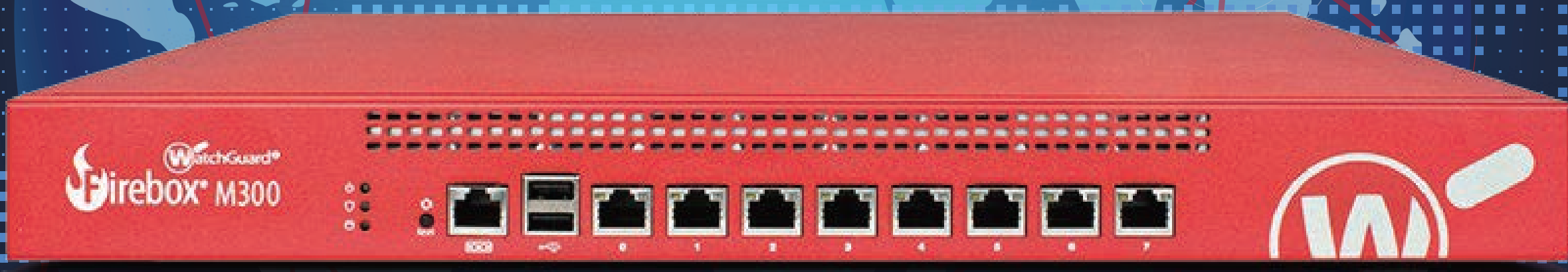
ウォッチガードによる防御

2,902,984

件のネットワーク攻撃をブロック
(Q2 2017)

86 件の攻撃

平均防御数(1台のアプライアンス)



16,403,723

ウォッチガードがブロックしたマルウェアの数
(Q2 2017)

488 件のマルウェア数

平均ブロック数(1台のアプライアンス)

インターネットセキュリティレポート(フルバージョン)は以下よりダウンロード

www.watchguard.co.jp

