

Q1 2017 インターネット脅威レポート サマリー

WatchGuard Threat Lab

インターネットを活用して安全にビジネスを推進するには、セキュリティの脅威と攻撃の傾向を理解し、最適な防御方法を策定する必要があります。WatchGuard Threat Labによるインターネット脅威レポートをご活用下さい。

マルウェアのトレンド

Linuxマルウェアが
増加傾向

36%

検知されたマルウェアの中
でのLinuxへの攻撃の割合

LinuxサーバーとIoTデバイスを標的とした
攻撃が増加。多層防御による対策が有効

従来のアンチウイルスによる
未知のマルウェア検知率が高い

38%

シグネチャベースのアンチウイルスが
検知しなかったマルウェアの比率

シグネチャベースの検知技術は必要だが、
さらに、高度な脅威の検知を可能にする
サービスによる強化が必要

サイバーセキュリティの戦場が Webサービスに移行

ドライブバイダウンロードと ブラウザベース攻撃 の増加

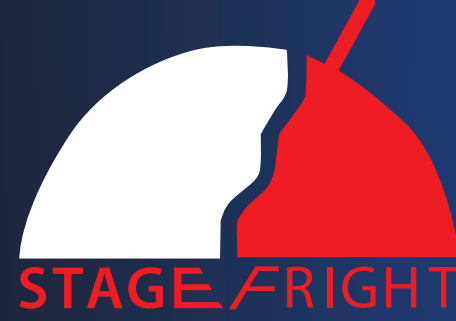
82%

Webサーバ(または他のWeb
ベースのサービス)が標的に
(ネットワーク攻撃の上位82%)

Webサーバの防御の強化項目

- アクセス許可の厳格化
- リソースの公開制限の実施
- アプリケーションのパッチ適用

脅威のトレンド



Android StageFright

攻撃者は
Android Stage-
Fright の脆弱性を悪用



ビットコインのマイニングに
関係するトロイの木馬

FTP経由での
トロイの木馬の配信



不正なJavaScript

97.2% の不正なJavaScript
が電子メールにて拡散

WatchGuard の実績

250万

ウォッチガードがブロックした
ネットワーク攻撃の数(2017年1-3月)

156

1台のFireboxが
防御した攻撃の数



700万

ウォッチガードがブロックした
マルウェアの数(2017年1-3月)

266

1台のFireboxがブロックしたマルウェアの数

インターネット脅威レポートは以下よりダウンロード頂けます。
www.watchguard.co.jp/whitepaper

