第66回スクエアfreeセミナー

可視化から始めるサイバー攻撃対策

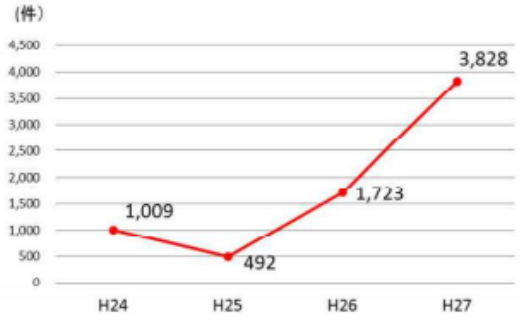
サイバー攻撃の状況を可視化する無料サービスのご紹介

株式会社OPENスクエア
田中　昭造
三好　文樹

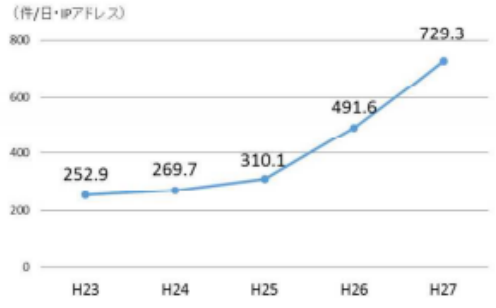
IoTの普及により深刻かするサイバー攻撃

「平成27年におけるサイバー空間をめぐる脅威の情勢について」 2016年3月17日警視庁発表より

平成27年中に警察が連携事業者等から報告を受けた標的型メール攻撃は 3,828件と過去最多。Word文書形式のファイルを添付したものが急増、過半数 を占める。



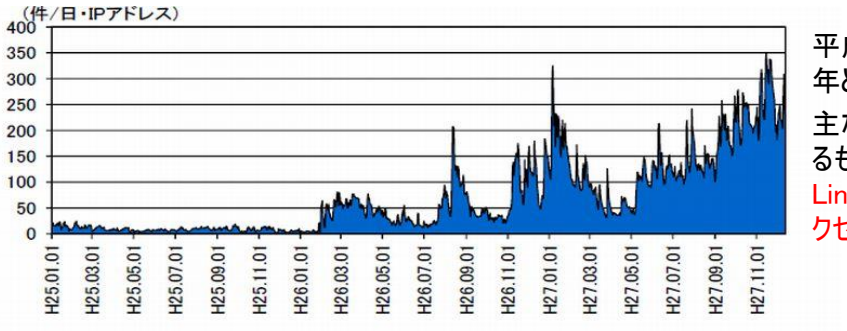
【標的型メール攻撃の件数】



【センサーに対するアクセス件数】

サイバー空間における探索行為

- インターネットとの接続点に設置したセンサーに対するアクセス件数は、１ 日１IPアドレス当たり729.3件。
- ルータや監視カメラ等の組込み機器を標的とした探索行為等が増加。



平成27年のセンサーに対するアクセス件数は、１日・1IPアドレス当たり729.3件で、前年と比べ約1.5倍に増加した。

主な増加の要因は、宛先ポート23/TCPに対するアクセスが大幅に増加したことによるものであり、IoTの普及に伴い脅威の増加が懸念されるルータ、監視カメラ等のLinux系のOSが組み込まれた機器を標的とする探索行為や同機器を踏み台としたアクセスが多数確認されている。

総務省も2020年東京オリンピック開催に向けて、IoTの増加を視野に入れた情報セキュリティ対策を推進

可視化で分かるサイバー攻撃状況

そうは言っても、、、
サイバー攻撃はそんなに多いの？　日本は他の国に比べたら安全でしょう？
言葉だけでは良く分からないんだけど。

では、実際の世界のサイバー攻撃状況を見てみましょう

CYBERTHREAT REAL-TIME　MAP　https://cybermap.kaspersky.com/

ロシアのセキュリティソフト会社であるカスペルスキーが運営するサイバー攻撃の可視化サイトです。

Digital Attack Map　http://www.digitalattackmap.com/

あの有名なGoogleが運営する『DDoS攻撃』の可視化サイトです。

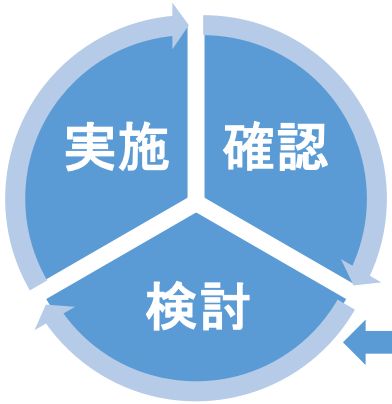
日本も結構攻撃されてようだけど、うちのサーバは大丈夫だよ。
うちのサーバのサイバー攻撃状況までは見れないでしょう？

攻撃見えるくんを利用して自社サーバへのサイバー攻撃状況を可視化できます。
また、可視化だけでなく、サイバー攻撃を遮断する攻撃遮断くんもご利用頂けます。

攻撃見えるくん/攻撃遮断くんサービス概要

攻撃遮断くん

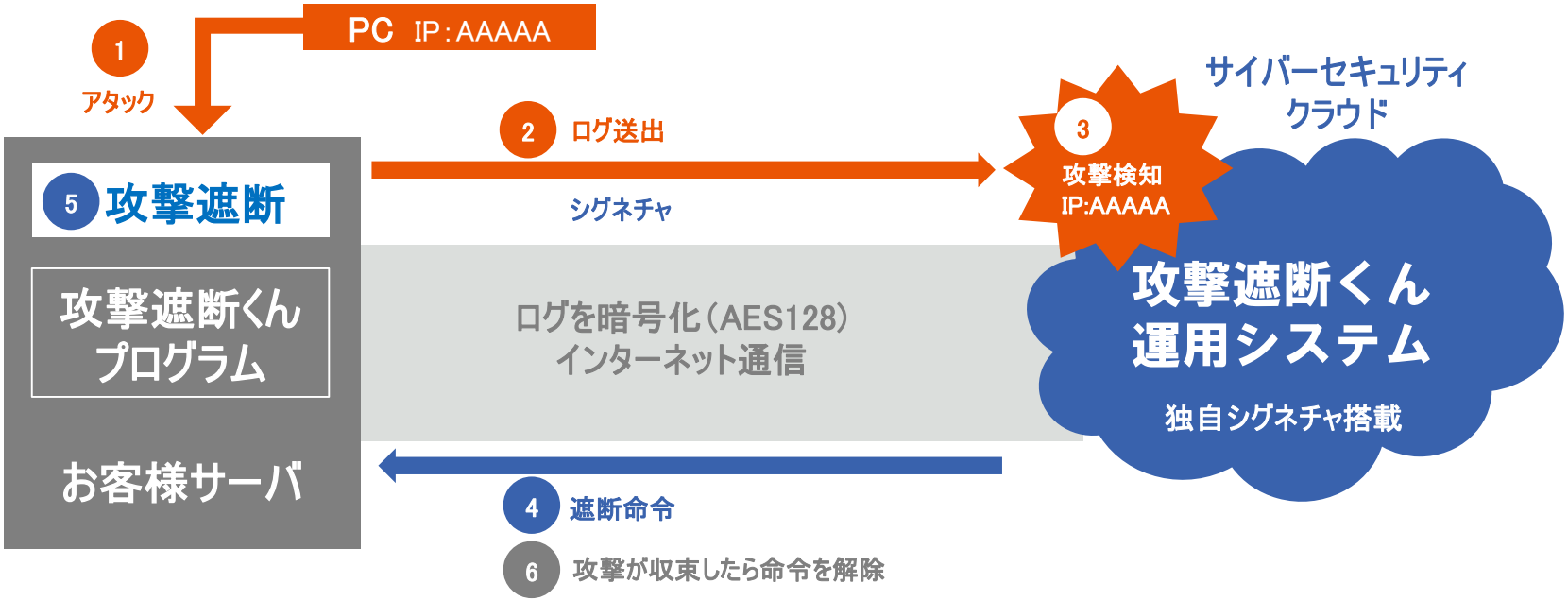
検討結果に合わせて対策を実施します。
対策としてはネットワーク、サーバの設定変更や製品の導入などが考えられます。
「攻撃遮断くん」は迅速で簡単に対策が可能です。



攻撃見えるくん

お客様のサーバがどこからどの程度の攻撃を受けているかを容易に確認できます。

攻撃状況のログから脅威レベルの確認してサイバー攻撃対策の検討を支援します。



攻撃見えるくん/攻撃遮断くんは株式会社サイバーセキュリティクラウド社(CSC社)の製品です。

攻撃見えるくん/攻撃遮断くん比較

	攻撃見えるくん	攻撃遮断くん
攻撃の検知	○	○
攻撃の遮断	×	○
攻撃元IPアドレスの閲覧	○	○
攻撃の種類の閲覧	○	○
攻撃元のログの閲覧	○（1000攻撃ログ）	○（10000攻撃ログ）
アラートメールの送信	○（攻撃検知メール）	○（防御証明メール）
費用	無料	有料

攻撃見えるくん/攻撃遮断くん　特長１

攻撃可視化でリアルタイムに確認
お客様ごとの管理画面で、お客様に対する攻撃の閲覧が可能。リアルタイムで確認が出来ます。

24時間365日攻撃遮断くん／攻撃見えるくん申請可能
いつでも好きなときに攻撃遮断くん／攻撃見えるくんの申し込みが可能です。

24時間以内で攻撃遮断くん／攻撃見えるくん開始可能
最短5分、24時間以内で攻撃遮断くん／攻撃見えるくんの開始が可能です。

過去の攻撃データから分析
過去のデータにより、攻撃の傾向を分析可能です。

安心の国内データセンター運用
攻撃遮断くん／攻撃見えるくんは安心安全の国内データセンターにて運用を行っています。

監視センターとの接続状況確認も可能
監視センターとの接続状況の確認が管理画面で可能。

お客様に合わせたフルカスタマイズ機能（攻撃遮断くんのみ）
サービス毎に貴社専用監視センターを構築しています。クラウドとアプライアンスのハイブリッド構成となっております。

攻撃見えるくん/攻撃遮断くん　特長２

国内開発

攻撃見えるくん／攻撃遮断くんは国内開発製品です。開発、販売、サポートを一貫してCSCが行うため、安心してご利用いただけます。管理画面、マニュアル、サポートなども日本語で提供。難しいセキュリティ専門用語を苦にすることなく、操作・運用を行うことが出来ます。

ご担当者様での保守・運用作業は一切必要なし

管理が難しいシステムの保守・運用作業は全てCSCで行います。
ご担当者様の保守・運用作業は一切発生しませんので、専門的な技術者がいなくても、問題なくサービスをご利用する事ができます。

シグネチャは自動で最新にアップデート（高速更新機能）

専門技術者がクラウド上でシグネチャを常に最新バージョンへアップデートしています。
ご担当者様で煩雑なチューニングをすることなく、常に最新の脅威に対応することができます。

クラウド環境（IaaS）への対応

エージェントプログラムを埋め込むだけのクラウド型（SaaS）のため、各社様のクラウドサーバ（IaaS）にも対応しております。

ほぼすべてのOSに対応

導入サーバのOSは問いません。
Linux、Windowsはもちろんの事、ほぼ全てのOSに対応しているので、ご利用中のサーバにすぐご導入頂けます。

サーバへの負荷は１％以下

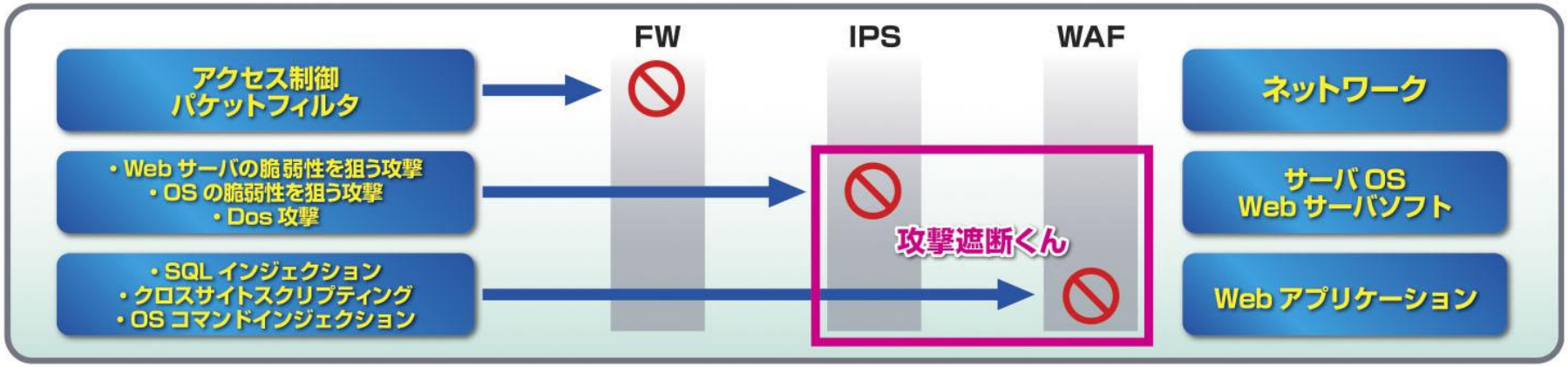
攻撃の検知・遮断の最中でもサーバへの負荷は1%を超えません。
導入によりサーバやサービス性能への影響はほとんどありません。

ネットワーク構成の変更やサーバ停止の必要なし

専用ハードウェアは必要なく、エージェントをインストールするのみ。サーバの一時停止やネットワーク構成を変更することなく、
サービスを開始する事ができます。

対応する主なサイバー攻撃

IPS+WAF（幅広いレイヤーをカバー）



対応可能な主な攻撃手法

- ブルートフォースアタック
- SQLインジェクション
- SSLインジェクション
- クロスサイトスクリプティング
- ディレクトリトラバーサル
- OSコマンドインジェクション
- 改行コードインジェクション
- LDAPインジェクション
- ファイルインクルード
- URLエンコード攻撃
- 各種OSやミドルウェアなどの脆弱性を突いた攻撃
- その他のWEB攻撃全般
- パスワードリスト攻撃（抑制）
- Apache Struts2の脆弱性を利用した攻撃

※攻撃見えるくんで可視化可能な攻撃手法も同様です。

攻撃見えるくんデモンストレーション

当社でも攻撃見えるくんを利用してみました！！

実際に当社のサーバに「攻撃見えるくん」を導入しましたので、当社サーバへの攻撃状況を可視化してご覧頂きます。

デモンストレーションの全体の流れ

- **管理画面へのログイン**
  Webサイトでログインして管理画面を表示
- **管理画面説明**
  管理画面の説明、攻撃情報の見方
- **攻撃内容の説明**
  当社で多かった攻撃の説明
- **攻撃検知実演**
  実際に当社サーバに対する攻撃と検知の実演

最後に

ご清聴ありがとうございました。

ＯＰＥＮスクエア社は
可視化から始めるサイバー攻撃対策　をご提案します。

お問合せ先：
株式会社OPENスクエア
電話　：　03-6413-1840
E-Mail：　sales_os@opensquare.co.jp