攻撃者の動向を踏まえた
2018年セキュリティ予測

ファイアアイ株式会社

執行役副社長　岩間優仁

2月　2018年

ファイア・アイ会社概要

CEO（最高経営責任者）兼取締役
ケビン・マンディア
（前Mandiant CEO）

プレジデント
トラヴィス・リース

グローバル・サービス＆
インテリジェンス担当
エグゼクティブ・バイス・
プレジデント
ジョン・ウォッターズ

エグゼクティブ・バイス・
プレジデント兼
CTO（最高技術責任者）
グレイディ・サマーズ

ワールドワイド・セールス担当
エグゼクティブ・バイス・プレジデント
ビル・ロビンズ

本社：米国カリフォルニア州ミルピタス
2004年創業、2013年9月　NASDAQ上場
2014年1月　Mandiant買収
2016年1月　iSight Partners買収
2016年2月　Invotas買収
社員：約2,900名
67カ国・6,000社を超えるユーザー企業

代表取締役社長
西村 隆行

ファイア・アイ株式会社（日本法人）

- 設立: 2012年
- 拠点: 東京、大阪、名古屋
- 従業員数:約100名（日本国内）

FireEye

FIREEYEインテリジェンス

すべてのフェーズにおいて「価値ある・使える」インテリジェンス

iSIGHTPARTNERS

攻撃グループの追跡から補足される
攻撃側の動機や目的に関する
インテリジェンス

将来の脅威への準備

- 攻撃手法
- マルウェア
- ツール
- 目的
- 攻撃対象
- 脅威の動向
- 漏洩情報の行方

16,000の攻撃者を監視

300以上の専門家

29言語**18**ヶ国

FireEye

センサーがリアルタイムに収集する
脆弱性やマルウェアに関する
インテリジェンス

脅威を検知・防御

- IPアドレス
- ドメイン
- URL
- ハッシュ値
- メールアドレス
- ルール

1,400万仮想実行空間

10億以上のマルウェア

100ヶ国以上

MANDIANT

インシデント対応の現場から得られる
侵入後の攻撃者の活動に関する
インテリジェンス

脅威への対策を最適化

- 侵入経路• 漏洩情報
- 侵入方法
- 侵入期間
- 侵害されたシステム

10万時間以上*

46ヶ国以上

＊年間

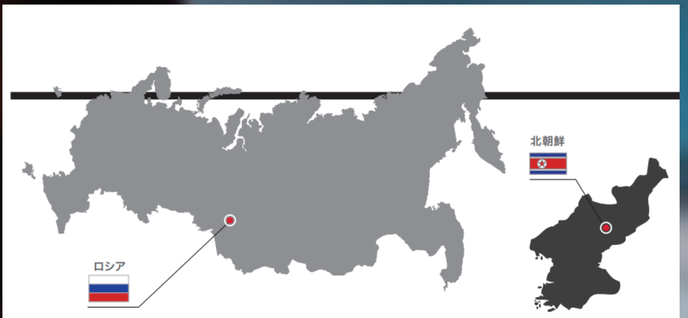
2018セキュリティ動向予測レポート

1. 国家によるサイバー脅威の拡大
2. 主要脅威としてのイランや北朝鮮の台頭
3. クラウドへの広範な移行によって紡ぎだされたセキュリティ問題
4. 従業員をサイバー攻撃から守る為の組織への圧力が高まっている
5. ソーシャルメディアや電子メールアカウントに対する攻撃のリスクが高まっている
6. サイバー攻撃に対するGDPRの影響
7. 主要なサイバー脅威の支援者が、味方を訓練し、装備を施し、危険を広げる仕組み
8. 中国による経済サイバースパイ活動の継続的な影 響
9. 北朝鮮によるサイバー攻撃の増加が予想される
10. 熟練労働者の不足が如何にして自動化の増加につながっているか
11. 産業制御システムに直面するリスク
12. ランサムウェアの継続的な役割と、IoTへの攻撃の増加

*GDPR=General Data Protection Regulation

国家支援の標的型攻撃グループの活動が増加

- ✓ 新たに課せられた貿易や経済制裁に対抗する目的でサイバー攻撃が発生
- ✓ 世界中の多くに国々にサイバー攻撃ツールと技術が普及、拡大しており、リスクが高くなっている
- ✓ 北朝鮮、中国、ロシア、イランの活動が増加する
- ✓ 中国の標的型攻撃グループは、インドや香港など、グローバルマーケットに照準を変えてきつつある



過去数年間で最も大きな経済的被害を出したサイバー攻撃

過去数年間で最も大きな経済的被害を出したサイバー攻撃は、米国など西側諸国による制裁を契機に発生しています。今後も、多くのサイバー大国が、自国に課せられた貿易制裁や経済制裁に対し、米国企業に対するサイバー攻撃で報復しようとするでしょう。ロシアや北朝鮮など、西側諸国の制裁対象となった一部の国々は、グローバル経済全体に悪影響をもたらすサイバー攻撃によって、そのような制裁に対抗できることを実証しています。

サイバー犯罪は巧妙さが今までにないレベルに達する

- ✓ 偵察目的のソフトウェアを使用した情報窃取や、非公開のバグを突いた攻撃が増加する
- ✓ ワームや、急速に拡散できるコモディティマルウェアの使用が増加する
- ✓ 2017年8月から11月で、HTTPSドメインのフィッシング攻撃が186%増加しており、更に拡大する

大規模侵害

- ✓ 金銭目的のグループによるインシデントの数が増加
- ✓ 個人情報の大規模な捜索活動が継続

Copyright © 2017, FireEye, Inc. All rights reserved.

新しい規制が組織のより良いデータ防御に功を奏する

- ✓ GDPRやDFSによる規制が主要なトピックになる
- ✓ GDPR他の規制に絡んだ人質行為やゆすりの類の攻撃が増加する

FireEye
SECURITY REIMAGINED

クラウドベースの攻撃と回避テクニック

- ✓ 攻撃者がよりクラウド環境を意識するようになり、手口に採用することが増えていく

IoTの脆弱性を突いた攻撃の増加

- ✓ コネクテッドデバイスの数の増大に伴い、新しく特定された脆弱性を素早く突いてくる攻撃が増加する
- ✓ 特定のIoTデバイスがランサムウェアの標的になる

FireEye

仮想通貨をターゲットとした マルウェアの増加と不正な拡散

- ✓ 仮想通貨を標的とするマルウェアが多く見込まれる
- ✓ 資格情報の盗難やパッシュパスなどを活用したマルウェアの自動拡散が一般的になる

向かいくる戦い

- ✓ システムとアカウントで二要素認証を使用する
- ✓ パスワード管理ツールにより、システムとアカウントを保護する
- ✓ ランサムウェア感染やデータ侵害の際に自動的にデータをバックアップできるようにする

ご清聴ありがとうございました

FireEye