CyberDefense

# サイバー攻撃対策と組織体制のこれまでと現状

2016年11月17日

サイバーディフェンス研究所
鎌田 敬介

# サイバー攻撃の変遷

技術者の趣味または愉快犯などが中心

ハッカー集団などの主義/主張が目的の攻撃

金銭を目的としたサイバー攻撃

情報を目的としたサイバー攻撃
国家によるサイバー攻撃・サイバー戦争

攻撃者の裾野が広がり若者がゲーム感覚で
本格的なサイバー攻撃を実施できる時代

# 脅威認識：昨今の主要な攻撃

DDoS攻撃

脆弱性攻撃

標的型攻撃（APT）

アカウント不正利用

マルウエア感染

Web改ざん

ランサム

不正送金

# サイバー攻撃対応の変遷

ホームページの改ざん対応、スローな脆弱性対応
（セキュリティ対応の必要性の認知）

情報漏えいを意識したポリシーやルールの整備
USBメモリ使用禁止（クライアント環境の制限）

Webアプリケーションへの攻撃の対応
（サーバ環境のセキュリティ対策の進化）

標的型攻撃（APT攻撃）、DDoS攻撃、不正送金など高度化された攻撃への場当たり的な対応

情報資産の特定、リスク分析、リスクベースアプローチ、インテリジェンスや脅威動向の活用、危機管理

# サイバー攻撃対応の昨今の変化

# 組織体制の変遷

ITの管理機能を司る部門（IT部門や総務部門に組み込まれている）が技術に特化したセキュリティ対策を実施

情報セキュリティ部門やコンプライアンス部門などが情報漏えい対策の観点からセキュリティ対策を強化

侵入前提型の対策の必要性や、インシデント対応体制としてのCSIRTの設置の必要性が考慮される（CSIRTの位置付けは企業によって異なることに注意）

1.「特定、防御、検知、対応、復旧」の考え方
2. インシデント対応体制を発展させた危機管理体制へ
3. 組織外の情報収集、組織間連携、インテリジェンスの活用

# 1.「特定、防御、検知、対応、復旧」の考え方

- 「特定」の観点の乏しさ
  - **自社の弱点を知る**
  - 自社の情報資産の特定
  - 脅威動向の特定
  - リスクの特定
  - リスク管理戦略の策定
- 「復旧」の観点の乏しさ(次ページ)
- 様々なフレームワークを活用した網羅性の確保
  - NISTのCybersecurity Framework
  - FFIECのCAT
  - CISのCritical Security Controls
  - PCI-DSS
    など

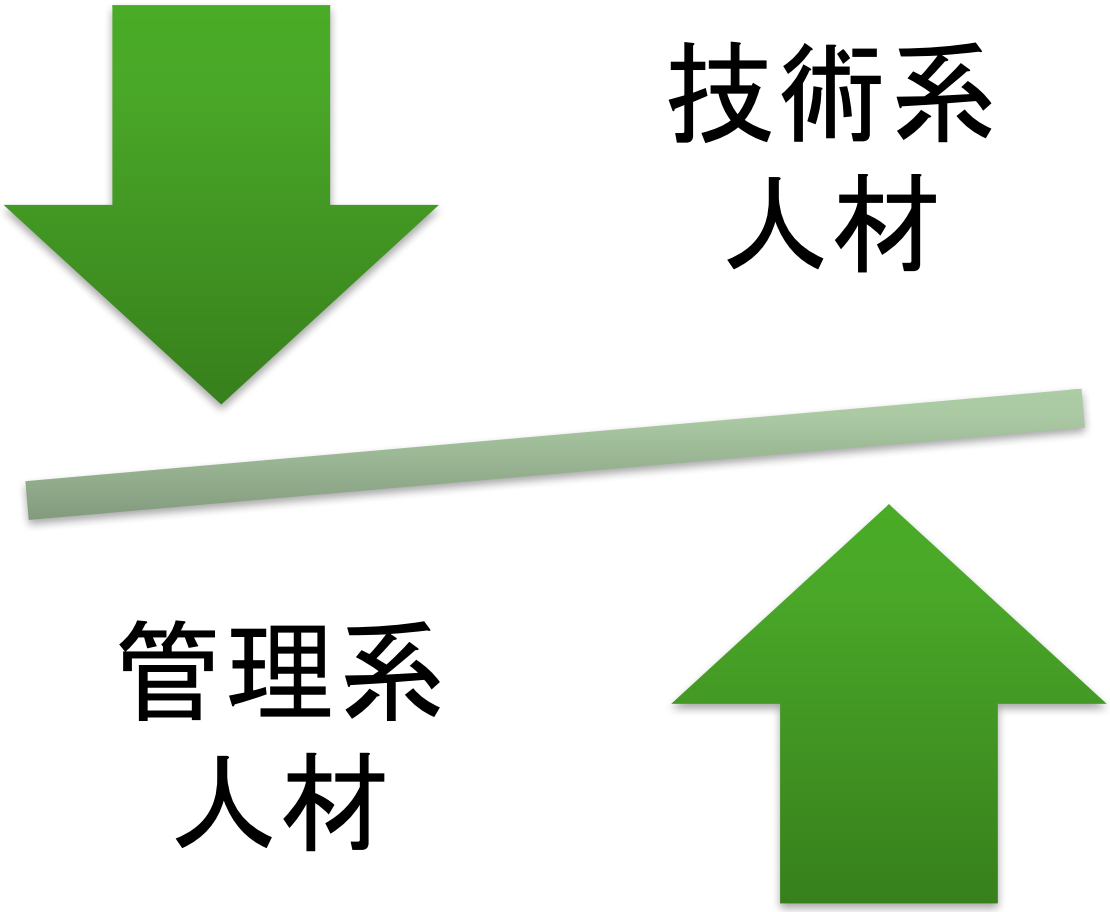
# 2. 危機管理体制上のよくある問題点

- ガバナンス
  - 危機管理体制の整備
  - 社内規定や各種文書の整備（作りすぎは×）
  - 部署間連携、情報の適時エスカレーション
  - サイバー攻撃発生時の危機対応の流れ（技術vs管理）
  - 対策本部(CSIRT)の立ち上げとスムーズな意志決定
- コンプライアンス
  - サイバー攻撃発生時の現場の対応方針
  - 悪い報告が上がりやすい組織作り
  - 法令遵守＋倫理的な問題
- サイバー攻撃対応訓練の実施
  - 自組織にとって最悪のサイバー攻撃被害を想定したものを
  - 組織トップが記者会見で謝罪するようなシナリオは？
  - 標的型メール訓練はもはやアリバイ作り程度の意味
  - 対策のできないサイバー攻撃があることを認知しているか

# 3. 組織間連携、情報収集、インテリジェンス

- 組織間連携
  - 1組織の限られたリソースでの対応の限界
  - 同じ目的に向かって他組織と協力し合う事で、対応のためのリソースを共有し効率化を図る
- 情報収集活動
  - 世の中の状況を的確に把握できているのか？
  - 他社はどのようにやっているのか？
  - 脅威動向、リスク管理策、セキュリティ対策、人材育成
  - 一方で「情報過多」という問題も起きている
  - 複数の情報ルートを持つことの重要性
- インテリジェンス
  - 情報を収集し、分析し、アクションに繋げる
  - 得られた情報を元に何を読み解くのか？
  - 短期的に使う情報、長期的な戦略に関わる情報
  - セキュリティオペレーションの考え方
- 「自動収集・自動分析・自動適用」などの自動化

# セキュリティ人材育成について



# CISOは必要か？

- 国内大企業においてCIOがCISOを兼務しているケースが多い
- ITを前に進める仕事と、セキュリティを前に進める仕事は両立しうるのか？
- 米国ではCISOはCIO直下もしくはリスク所管のCRO直下のケースが増えてきているように見受けられる
- CISOは役員である必要はなく、「セキュリティの仕事をフルタイムでしている最上位の役職」と考えれば良い
- ただし、CISO相当の人間は役員と直接会話できる位置にいることが必要

# 経営層の関与を得るには人材育成のアプローチが必要

- 多くの場合、経営層はサイバーセキュリティのことをよく理解していない（平均的には恐らく新聞レベル）
- 経営層のサイバーセキュリティの理解が進み、積極的な関与を得られた組織体は体制整備・対策が進む傾向にある（金融庁の調査結果でもそう出ている）
- 数年単位の覚悟で経営層にサイバーセキュリティのリスクを認知してもらうためのレクチャーをすること
- 日常的なコミュニケーションを怠らないこと

# 組織内に技術の専門家は必要か？

- 1人の専門家が全てをこなす時代はとっくに終わっている
- 技術だけでなく、危機管理、組織管理、リスク分析、法律、情報分析など様々な分野の知見が必要、チーム戦である
- 各領域に詳しい人間が組織内にいることが望ましいが、難しい場合は気軽に質問が出来る距離感で外部関係を持つことが重要

# 管理系人材の育成

- 金融機関にまず必要なのは技術系人材ではなく管理系人材
- 経営感覚と現場感覚の両方を持ち合わせる
- 「橋渡し人材」という言葉もあるが…
- サイバーセキュリティの専門能力以外に
  - 対人能力
  - 組織内調整力
  - 構造化能力
  - 抽象化能力
    などが必要になってくる
- 育成方法は模索中だが、システムの素養は必要

# 最後に

- 世の中の変化に追いつけているか
- 外の世界を見ているか
- 限られた情報に振り回されていないか
- セキュリティの仕事が進みやすい組織に
- 遊び心もわすれずに