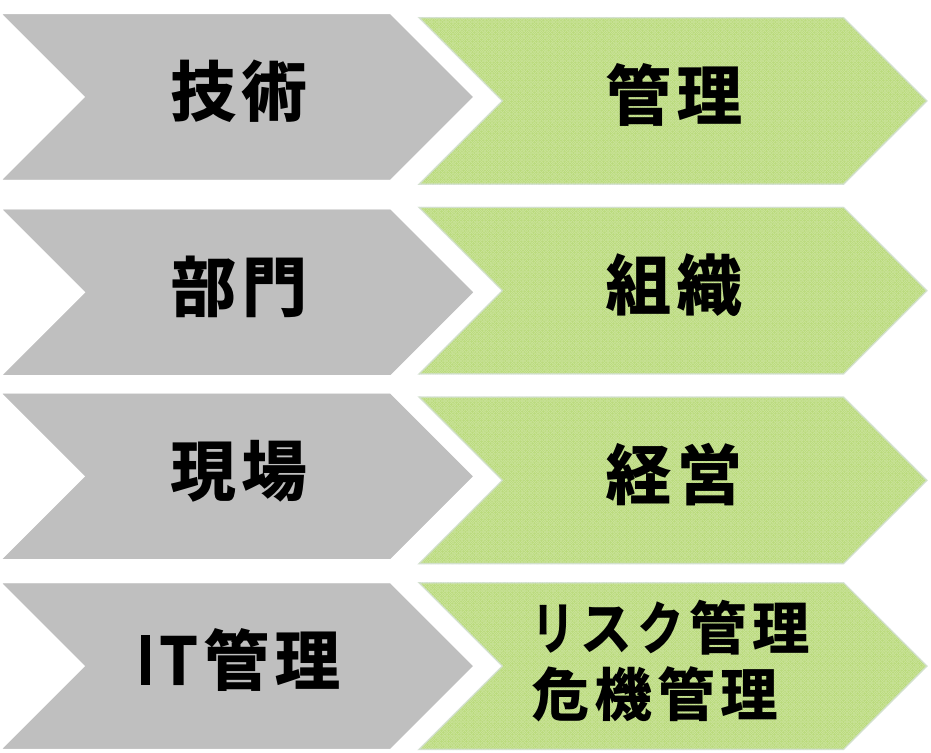
組織管理者のための
見えないサイバー攻撃リスクへの心構え

2017年12月11日

金融ISAC
鎌田 敬介
kamata@f-isac.jp

サイバー攻撃対応における考え方の変化



昨今のサイバー攻撃の概観

攻撃者は誰なのか？

趣味と興味：ハッカー

主義主張をサイバー攻撃で：
ハクティビスト

金銭取得が目的：犯罪者？国家？

情報取得が目的：スパイ？国家？

サイバー戦争：国家

子供の遊び：十代からの子供たち

サイバー攻撃の実害とは？

情報漏えい

- 個人情報
- 知的財産
- 企業秘密
- 金銭被害

サービス停止や業務への影響

- 業務影響の大きさ
- 顧客影響
- 人命への影響

参考資料：昨今の主要な攻撃でよく使われる用語

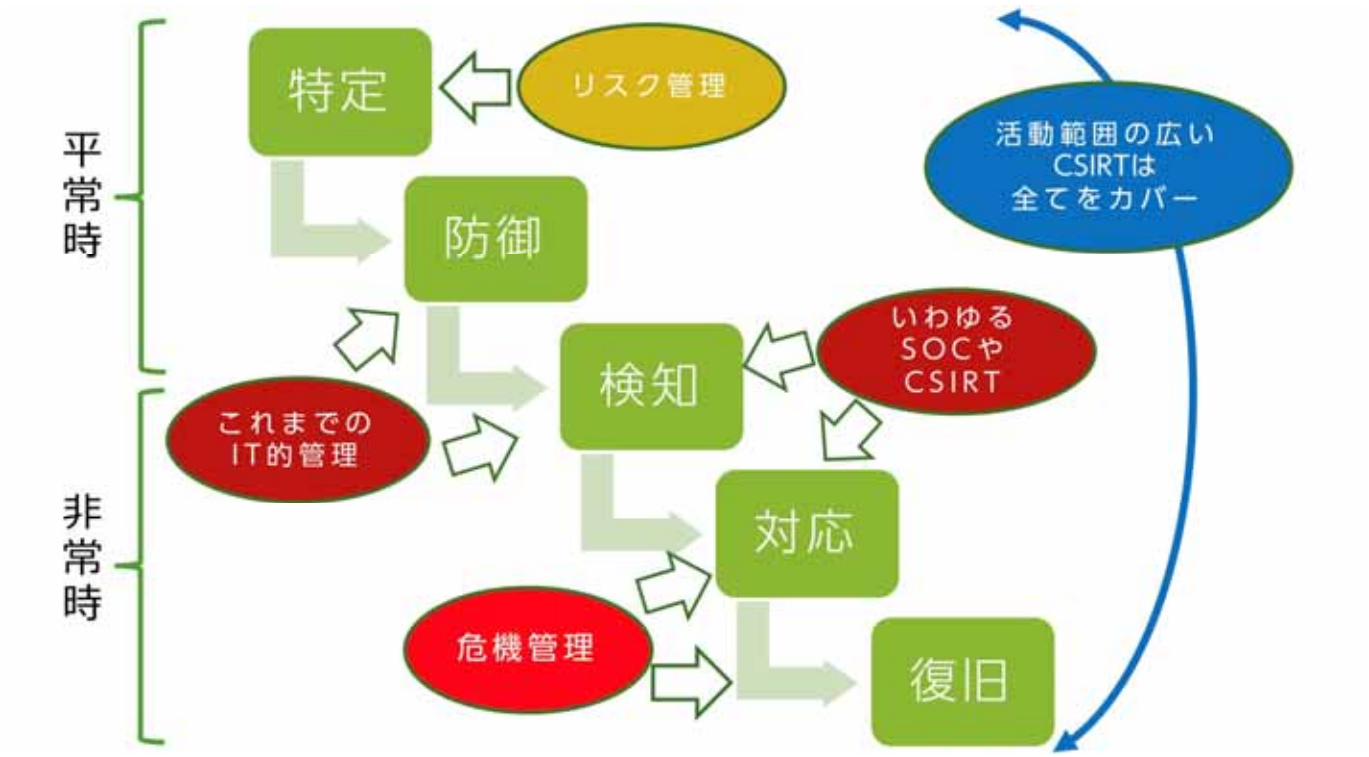
- DDoS攻撃
- 脆弱性攻撃
- 標的型攻撃（APT）
- アカウント不正利用
- マルウエア感染
- Web改ざん
- ランサムウエア（破壊型？）
- 不正送金

サイバーセキュリティマネジメントの概観

5つの重要な観点

1. 「特定、防御、検知、対応、復旧」の観点
2. リスク管理の観点
3. 危機管理・危機対応の観点
4. インシデント対応の観点
5. 組織間連携、情報収集、インテリジェンスの観点

1.「特定、防御、検知、対応、復旧」の考え方



平常時と非常時の組織的役割分担

	平常時	非常時
経営層	・リスク認識 ・リスクの決定と優先順位付け ・リソースの割り当て	組織としての意思決定
管理層 (企画)	・ガバナンス（PPP/PPT） ・コンプライアンス ・リスク管理 ・演習や訓練の実施 ・経営層への報告 ・現場との連携	インシデント対応の 司令塔（トリアージ）
技術層 (現場/運用)	・インフラの保護（監視/検知） ・リスク管理策の実行	インシデント対応の 技術的対応・現場対応

PPP = Policy, Process, Procedure, PPT = People, Process, Technology

2．リスク管理に関するよくある問題点

- **「特定」の観点が不足**
  - 自社の弱点を知ること
  - 自社の情報資産（と重要性）を特定すること
  - 世の中の変化（脅威動向）にリアルタイムで追いつくこと
- **リスク管理の視点が不足**
  - 想定外リスクの考慮と対応
  - リスク影響評価、リスク管理戦略の策定と実行
  - アウトソースリスクの考慮
  - 「自分の知らない脅威や脆弱性がある」というリスクの認識
- **体系的・網羅的な考慮の不足**
  - 国際的に認知されたスタンダードを活用する
    - NIST の Cybersecurity Framework
    - CIS の Critical Security Controls　　など
  - 個別の攻撃方法への対応の検討にもスタンダードやガイドの活用を

想定外リスクへの対応

情報漏えいリスクは
コスト算出可能か？

企業を対象としたサイバーエスピオナージの目的

企業秘密	・M&Aに関する情報 ・海外投資に関する情報
知的財産	・研究開発の優位性確保 ・新製品の開発
企業戦略	・新規市場参入 ・戦略的事業提携 ・製品やサービスなどの利用情報
財務戦略	・政府入札案件に関わる競合情報 ・再委託、外部委託のための情報 ・重要インフラ関連事業者の設備情報

最先端の攻撃者はどのように侵入を試みるか？

正規のアクセス権限

物理侵入

内部侵入

内部犯行

事案発生時にこれらの可能性を考慮することができるか？

想定外リスクへの対応のために最悪の事態を想定する

- 想定外リスクの対応能力向上
- 最悪の事態を想定した対応をシミュレーションすると、組織上の課題が非常に多く洗い出される
- リアリティを追求すればするほど現実的な課題が浮かび上がり、机上の議論で終わらせれば実践力は身につかない
- サイバー攻撃起因の最悪のシナリオを想像可能か？
- 攻撃側にまわることを（あえて）想定してみる

3. 危機管理・危機対応上のよくある問題点

- **ガバナンス**
  - 危機管理体制にサイバー攻撃起因の事案を想定する
  - サイバー事案発生時の対策本部の立ち上げとスムーズな意志決定
  - 社内規定や文書を整備しすぎないこと（作りすぎで実効性がない）
  - 部署間連携や情報の適時エスカレーション
  - ITに偏ったサイバー攻撃対応プランからの脱却
- **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が曖昧
  - 悪い報告が上がりやすい組織作り
  - 良くも悪くも法令遵守＋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危機対応訓練を
  - 演習・訓練は失敗を経験する場として捉える
  - 組織トップが記者会見で謝罪するようなシナリオ
  - 対策のできないサイバー攻撃があることを認知すること

インシデント対応とフォレンジック

4．事案発生時の対応の心得とよくある問題点

- **適切かつ効率的なインシデント対応のために**
  - 事案発生時に、発生事象から「何が起きていそうか」を的確に推測するためには、世の中のトレンドを理解していることが重要
  - 大抵の事案には脆弱性が関わっており「どの脆弱性が原因なのか？」をいち早く推測することが重要。組織の弱点を把握しておく
  - ある程度以上の難易度の事案になると、自組織のみでの対応は困難。外部組織との連携が必須なので、見えなければ見えないほど外部を頼った方が良い
- **攻撃者の目的を理解する**
  - 攻撃者は誰なのか？遊びなのか？本気なのか？
  - 攻撃者の目的は？金銭？情報？破壊？
- **セキュリティ対策に100%は存在しない**
  - 「○○があるから大丈夫」といった「安全である」という思い込みが最も危険
  - 間違った思い込みが横行しているのが現実（知識が古い、など）
  - セキュリティ機構がどう破られるのか（破られたのか）を考える
  - 他組織事例を自組織に置き換えるシミュレーションはとても有効
- **事案対応の中でよく問題になるポイント**
  - 認知バイアスが起こる
  - システム運用会社も最先端の攻撃には素人である
  - インシデント調査会社がリソース一杯で3ヶ月先まで来られない
  - セキュリティ専門家ではあるが業界の常識を知らない

リスク認識の課題となる視点の違い

昨今のフォレンジック調査に必要な観点

- ログが残っていない、不十分である
- 攻撃者が正規のアクセス権限のみを利用して情報を窃取
- 完全な分析にかかる時間vs意思決定に必要な情報
- 「フォレンジックはしない」という選択肢
- 攻撃の全体像・フローを理解する
- 技術的に完璧であることを求めることの難しさ

組織の限界をこえるために

5．組織間連携、情報収集、インテリジェンス

- **組織間連携**
  - こんなの自組織では無理だ、と思いませんか？それは正しい認識
  - 1組織の限られたリソースでの全方位の対応はもう限界
  - 組織を越えて対応のためのリソースを共有し効率化を図る時代に
- **情報収集**
  - 世の中の状況を把握できているのか？認識は古くないか？
  - 他社はどうしているのか？
  - 自社で起きている事象はどの程度広範囲に起きているのか？
  - 「情報過多」という問題もすぐに直面する
  - 複数の情報ルートを持つことが重要
  - 一次情報源に当たることの重要性
- **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き、何に繋げるのか？
  - セキュリティ運用の中核を担う役割
  - カウンターインテリジェンス

インテリジェンスの3つの文脈を理解する

情報利用者	情報利用サイクル	情報の利用目的	情報の例
経営・戦略	長期的 (数年～数ヶ月)	リスク管理戦略の優先度判断	• 投資情報が狙われている • 政府入札の妨害目的のサイバー攻撃が報告された • 成長・高収益事業への新規参入目的のサイバー攻撃が発生 • 経営活動の秘密情報を知る人物の個人情報が狙われる
管理・企画	中期的 (数ヶ月～数週間)	• リスク評価 • 計画立案と実行	• 脆弱性情報 • 攻撃情報 • 被害情報 • 攻撃予告 • 国内外動向 • 製品・サービス情報
技術・運用	短期的 (数日～数時間)	セキュリティ運用	• マルウエアのハッシュ値 • 攻撃元IPアドレス • 不正利用されるドメイン • 攻撃ツール • 漏えいデータ

最後に

- サイバー攻撃への対応は、組織全体としてのリスク管理･危機管理として考える。１００％は目指すもの
- 深刻なインシデント発生は想定外の塊である
- 数値化できない、被害額の算出不能なリスクの想定と対応は？
- サイバーに見せかけた内部犯行？
- 一般公開情報と一次情報の間の大きな乖離
- 注：他にも見えないものはたくさんあります
  –例）ハードウェア系とか