CyberDefense

日本企業における CSIRT 構築ノウハウ

日本シーサート協議会（CDI-CIRT）
乾　奈津子

アジェンダ

1. ここ1年における FACT と CSIRTに関する Findings と Lessons Learned

2. CSIRTの構築経験からの Findings と Lessons Learned

3. 今後の方向性と課題

トピック1

ここ1年における FACT と CSIRT（インシデントレスポンス体制）に関する FINDINGS と LESSONS LEARNED

サイバー脅威の変異（2005～2007年頃）

- 内部から外部への情報流出
  - USBメモリ等の外部記録媒体からの情報漏えいの多発
    - 大手印刷会社の800万件以上の個人情報漏えい
    - 大手保険会社のクレジットカード番号が含まれる150万件の個人情報漏洩
    - その他、地方銀行や多くの大手企業の情報漏えいの多発
  - Winnyによる情報流出事件の多発
    - 職員のパソコン（職場及び個人）からの機密情報の情報流出
- 個人情報の保護に関する法律の全面施行
  - 2003年5月23日に成立した個人情報保護法が、2005年4月1日に全面施行
- ISMS（情報セキュリティマネージメントシステム）、プライバシーマークの認証取得の急増

サイバー脅威の変異（2008年頃）

- スパムメールや（弱い）標的型攻撃メールによるマルウェア感染の増加
  - 社内パソコンでのインシデント
  - システムやアンチウィルスの導入で対策が可能

- SQLインジェクション
  - サーバのインシデント
  - 脆弱性情報流通で対応が可能

- フィッシング詐欺サイト
  - 自らがコントロールできないところでのインシデント
  - コンソーシアム等で対応可能だった

サイバー脅威の変異(現在)

- **目的型の攻撃**が増えている
  - 内部の**重要情報の搾取**目的
  - **明確な意図**をもっている
  - 特定の人しか喜ばない、**特定の情報**を狙ってきている

- 攻撃手法の**高度化、巧妙化、執拗化**
  - 粘着型標的型攻撃
  - ウィルス検知ソフトでは検知し切れない場合や、アップデートが追いつかないこともある
  - 手を変え、品を変え、どんどん回して攻撃してくる

- 見つからないような高度な技術
  - 自分の姿を消すための工作


衆院にサイバー攻撃

サーバーがウイルス

議員パスワード

1カ月盗み見可能状態


日経コンピュータReport

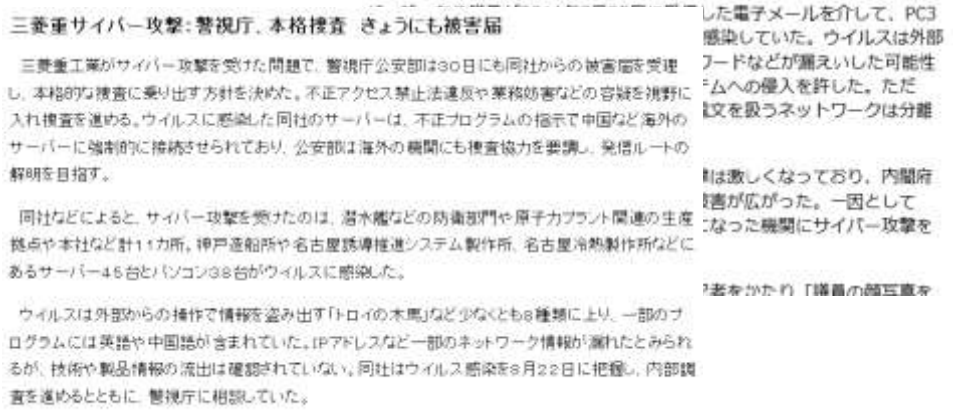
今度は政府機関、止まらないサイバー攻撃

官民連携の情報共有体制がスタート

2011/11/17

日本へのサイバー攻撃が止まらない。三菱重工業などの防衛産業に続き、今度は国会や政府機関が大規模なサイバー攻撃を受けていた。新たに判明したのは、衆議院や外務省、国土地理院などだ。

衆議院への攻撃で狙われたのは、議員に貸与したPCや情報共有用のサー


三菱重サイバー攻撃:警視庁、本格捜査 きょうにも被害届

三菱重工業がサイバー攻撃を受けた問題で、警視庁公安部は30日にも同社からの被害届を受理し、本格的な捜査に乗り出す方針を決めた。不正アクセス禁止法違反や業務妨害などの容疑を視野に入れ捜査を進める。ウイルスに感染した同社のサーバーは、不正プログラムの指示で中国など海外のサーバーに強制的に接続させられており、公安部は海外の機関にも捜査協力を要請し、発信ルートの解明を目指す。

同社などによると、サイバー攻撃を受けたのは、潜水艦などの防衛部門や原子力プラント関連の生産拠点や本社など計11カ所。神戸造船所や名古屋誘導推進システム製作所、名古屋冷熱製作所などにあるサーバー46台とパソコン38台がウイルスに感染した。

ウイルスは外部からの操作で情報を盗み出す「トロイの木馬」など少なくとも8種類に上り、一部のプログラムには英語や中国語が含まれていた。IPアドレスなど一部のネットワーク情報が漏れたとみられるが、技術や製品情報の流出は確認されていない。同社はウイルス感染を8月22日に把握し、内部調査を進めるとともに、警視庁に相談していた。

毎日新聞 2011年9月30日 中部夕刊

脅威と対策手法の変化

- 脅威は、内部から外部の流出から、**外部から内部への意図を持った攻撃**へと変わり続けている
  - 追いかけていくのが面倒、先回りが難しい
    - 攻撃者の気持ちは攻撃者にしかわからない
  - 攻撃技術の変わるスピードの高速化、手法の多様化
  - より簡単、お手軽に、スピーディーに攻撃できるようになった

- 次のような従来の対策（技術および運用）では不十分になった
  - フィシング詐欺やSQLインジェクションからシステムを守る
  - 内部の教育や運用ルールの徹底
  - 対策手法も使用する技術も変わった

- 情報搾取に対する対策がされてきていない

業務プロセスとITの役割の変化

- 業務プロセスの変化
  - やや画一した仕組みから多様化
    - 競争の激化、インターネットの普及による新しいビジネスの出現で、業務の仕組みが多様化している（各社の独自性が生まれている）
    - 同業他社でも、同じ対策が当てはまらない

- 業務とITの関わり合いの変化
  - 以前は、業務の効率化目的でのIT導入
  - 現在は、業務遂行がITに依存している

対策をするには

- セキュリティサービスベンダーの提案をそのまま導入できない
  - 自分の業務のすべてをセキュリティベンダーに理解してもらえるとは限らない
  - 業務の仕組みが多様化したため、対策も同様である

- 自分が、どのような脅威にさらされているかを知る必要がある
  - 業務の仕組みが多様化したため、各組織に対する脅威も多様化した

- 適切な対策には、内部と業務の仕組みの熟知が必要である
  - ITと業務が一体化している
  - 経営層にしか分からないことも多い

レスポンスオペレーションからの経験則から – 1

インシデントレスポンスを担当してきたのは、**IT部門**

- インシデントに気付くのはITの現場の担当者
  - リスクにさらされている対象を守っている上に、対応範囲が広いため、事実上対策の窓口がIT部門になることが多い
- 痛みを知らない人には、わからない
- そのため、IT部門がインシデントレスポンスを担当する場合が多い

レスポンスオペレーションからの経験則から – 2

クイックレスポンスが難しい

- 他部門は管轄外のため、強い要請が出来ず、「依頼」止まりになる
- 絶えずエスカレーションをして、部署間の合意形成をしなければならない
- 会社全体のプロセスを把握する必要がある
  - 基本的には、経営層に近い人しかわからない
  - 経営層に近いところ（例：CISOやCSOの直下）に、部署間の連携を推進させる権限や体制が必要

トピック2

CSIRT の構築経験からの FINDINGS & LESSONS LEARNED

構築経験からのLessons Learned と Findings

CSIRTや事故前提社会、事後対応・レスポンスなどの関連する**概念の理解がまず必要**である。また、勉強するアイテムとマテリアルが日本に欠けている。

1. セキュリティの担当者は分散化していなく、特定の人に依存していることが多い。その特定の人へのヒアリングで充分である。
2. 会社全体ではなく、部門や**特定の業務範囲内などCSIRTの適用範囲が限定的**である。

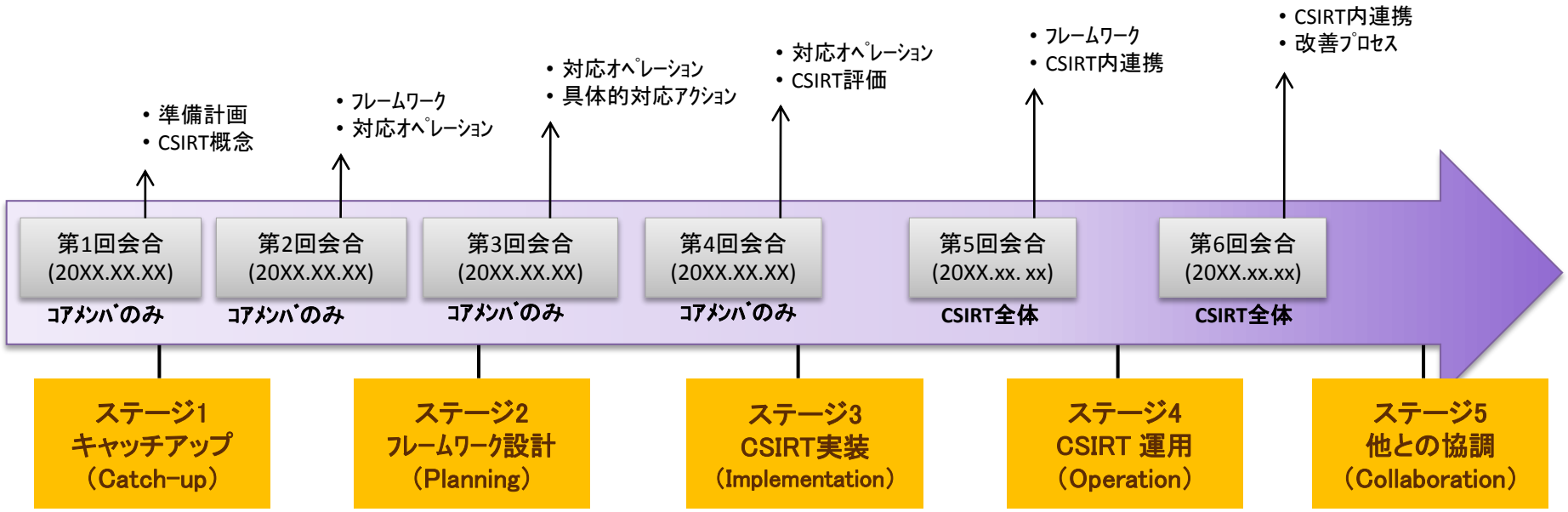
CSIRTの実装では、機器購入やリソースのアサインメントを想定していたが、**既存の仕組みの中で運用体制を作り上げる**ことが多い。そのため、説明会で人の理解が得られれば、すぐに実装が可能である。

社内や組織内の情報共有を、**概念図やモデル図を用いて**、目的や位置づけを説明することが重要である。文字のみでは、見てもらえない。

見出した構築プロセス

- ステージ1：キャッチアップ（CSIRT概念及びインシデント対応概論の理解 等）
- ステージ2: フレームワーク設計（CSIRT運用に必要な骨組み固め）
- ステージ3: CSIRT実装（対応オペレーション及びCSIRT評価の確立）
- ステージ4：CSIRT運用（関係部署の周知と理解獲得）
- ステージ5: 他との連携（内部他部門及び外部組織とのシームレスな連携）

導入スケジュールの例：



トピック3

今後の方向性と課題

CSIRT構築を考える上で必要なこと

- コンセプトノートの重要性

- 整理整頓
  - **全体を見渡せる**ようになる
  - 現場は経営層を、経営層は現場を
  - **現場と経営層の間のギャップを埋める**ことができた
  - 両方のアスペクトが出揃うこと
  - 経営層と現場、**双方の認識を 気付き（realise）、認識すること**
  - **既存のインシデントレスポンス担当との連携を密にしておくこと**
  - **分かりやすさを常に意識**すること

CSIRT効力の維持の難しさ

- 経営層などのトップマネージメントの交代時の難しさ
- 既存のインシデントレスポンス担当との連携を密に行なっていくこと
- 実際に運用開始してからも**動くのは「分かる人」**であることを認める
  - 在職歴の長い社員/職員
  - システムを熟知している者

今後の方向性と課題

- **事前の連携準備**の重要性

- **既存のインシデントレスポンス担当との連携**を密に行なっていくこと

- 実際に運用開始してからも、**動くのは「分かる人」**
  - 在職歴の長い社員/職員
  - システムを熟知している社員/職員

ご清聴ありがとうございました。

以下お気軽に相談ください。

CSIRTに関する相談: csirt-pr@nca.gr.jp
NCAおよび加盟に関して: nca-sec@nca.gr.jp