MALWARE CONTAINMENT

ゲームを終えて…

MALWARE CONTAINMENT

ゲームを終えて…

無事、封じ込めはできましたでしょうか？

今回、皆さんは発生したセキュリティインシデントに対して、
「報告を受け取り」「調査し」「対応活動」といった初動対応を行いました。

世間では情報漏えいに関するニュースが報道されていますが、CSIRT は、
こういったサイバー攻撃被害に対応するだけの組織ではありません。

起こりうるサイバー攻撃を未然に防ぎ、被害があってもいち早く発見し、
その被害を極小化することも CSIRT の役割になります。

ゲームを終えて…

CSIRT とは

CSIRT (Computer Security Incident Response Team)

“サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対応するための組織”

「サイバーセキュリティ経営ガイドライン ver 1.0」より

インシデントの例

- 情報漏えい
- Web サイト改ざん
- サービス妨害
- マルウエア感染

- **未然に防ぐ**
- **迅速に気付く**
- **効率よく対応する**
- **被害を最小化する**

例えば…

外部からの情報受付窓口を持つ
外部機関と連携を行う

組織のシステム環境を整備して
調査が迅速に行えるようにする

インシデント発生時の体制を整え
内部調整・外部連携を行う

MALWARE CONTAINMENT

ゲームを終えて…

インシデント例について

Web サイト改ざん

サービス妨害

Web サイトにアクセスが集中し、Web サイトが利用できなくなってしまう

Web サイトが改ざんされ、マルウェアを配布するように書き換えられてしまう

マルウエア感染

情報漏えい

【金銭等を要求する、設定情報を窃取する攻撃】

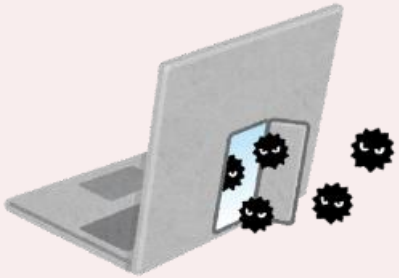
- ランサムウェア
  端末を「ロック」したり暗号化して使えなくして元に戻すことを条件に金銭を要求する
- スパイウェア
  ユーザに関する情報を収集(アカウント情報など)し、外部に送信する

MALWARE CONTAINMENT

ゲームを終えて…

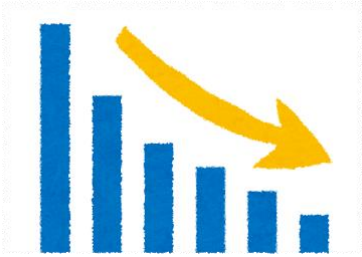
インシデント例について

マルウエア感染　情報漏えい



【機密情報を狙った攻撃】
- 遠隔操作マルウェア / バックドア型マルウェア
  端末を組織以外の人間が操作できるよう設定し
  組織内の端末を調査、機密情報を盗み出す

対応できないと…



サービスが運用できず
業績が低下する

なりすまされて
不正にお金が使われる

お客様の個人情報が
盗まれ、責任問題になる

MALWARE CONTAINMENT

ゲームを終えて…

CSIRT のメンバー

プレイしてもらった役職

コマンダー

CSIRT チームの統括を行う。
また、組織としての意思決定
を行う経営陣や CISO と
情報連携をして支援する。

リサーチャー

インシデントの情報を収集する。
セキュリティ製品を用いて、異常
がないか確認する。攻撃に関する
プロファイリングも行う。

フォレンジックエンジニア

感染した端末の証拠保全を行う
と共に、システム的な鑑識や、
精密な検査や解析を行う。
消されたデータの復元したりも。

ノーティフィケーション

インシデント発生の際に関連部署
のハブとなり情報を発信する。
社内システムに影響が及ぶ場合は、
IT 部門と調整を行ったりもする。

MALWARE CONTAINMENT

ゲームを終えて…

他にもいます！ CSIRTメンバー

PoC (Point of Contact)

社外窓口として、情報連携を行う。（JPCERT/CC, 経産省, 警察など…）
社内窓口として、IT 部門だけでなく、法務や広報などとも情報連携する。
情報を正しく、さじ加減が分かったトークスキルが重要。

ソリューションアナリスト

自社組織のビジネス計画に合わせてセキュリティ戦略を決定する。
「リスク」を評価し、導入するソリューションの有効性を確認する。
確認した結果から、その改善計画を考える。

脆弱性診断士

ネットワークやアプリケーション、ソフトウェアがセキュリティに
考慮したプログラミングがされているかの検査を行い、評価する。

インシデントハンドラー

インシデント対応時に、調査等を行うメンバーに指示を出し、
報告を受け取って、対応状況を把握する。対応履歴を確認すると共に
コマンダーへ状況を報告する。

MALWARE CONTAINMENT

ゲームを終えて…

CSIRT チームの例

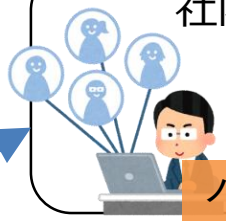
外部組織

社内システム
関連システム

社内・社外への
説明

POC

社内関連部署への
連絡

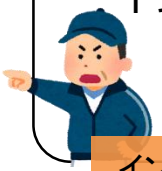


ノーティフィケーション

全体統括

コマンダー

インシデント管理
状況分析



インシデントハンドラー

システムセキュリティ設計
リスクを考え
対策の検討

ソリューションアナリスト

情報収集・調査

フォレンジックエンジニア

リサーチャー

脆弱性診断

脆弱性診断士

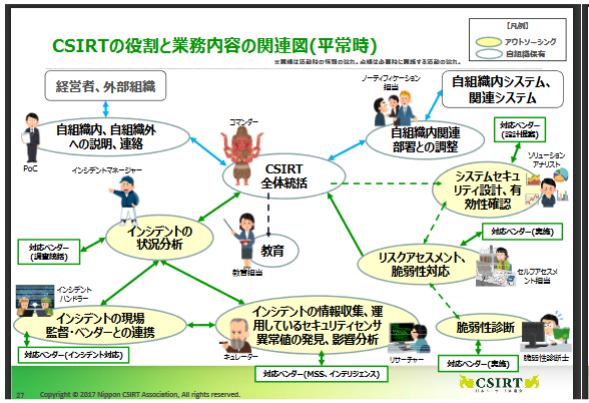
MALWARE CONTAINMENT

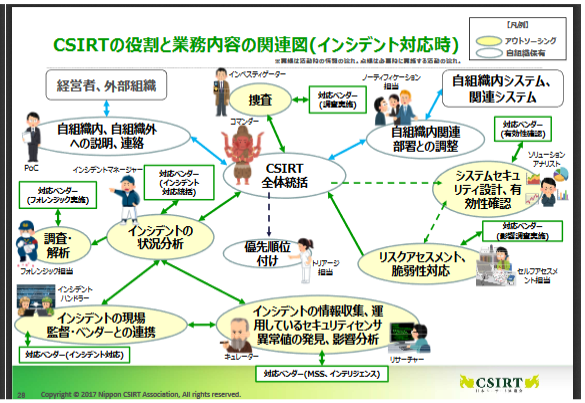
ゲームを終えて…

参考資料

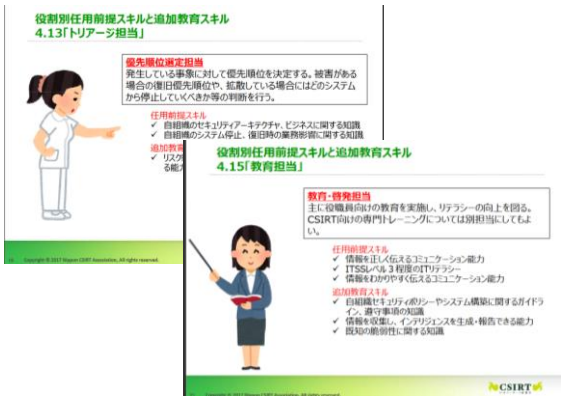
日本シーサート協議会　CSIRT 人材の定義と確保 (ver, 1.5)

- **CSIRT に求められる役割と実現に必要な人材のスキル、育成についてまとめられた資料**
- CSIRT における課題と解決に向けた方向性や、CSIRT が持つ役割と業務内容について紹介
- 役割別での、メンバー紹介資料
- 企業で実際に行う場合のモデルケースなど
- 付録には、「募集要項」のサンプルなども





平常時とインシデント対応時の対応体制に関する図



ゲームに出なかった役割も

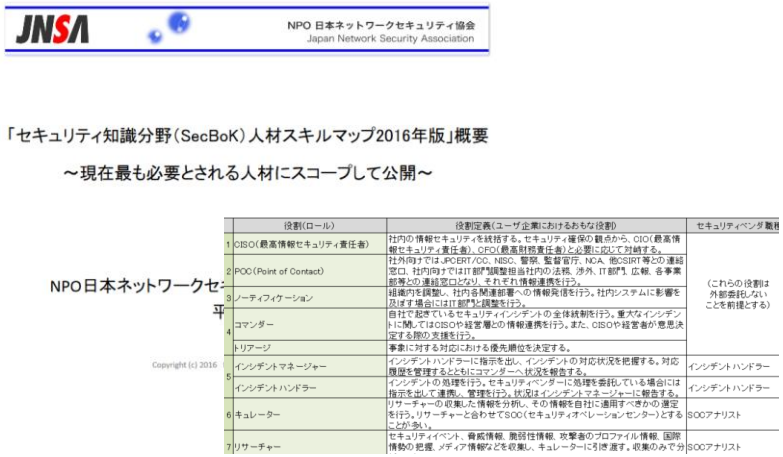
MALWARE CONTAINMENT

ゲームを終えて…

参考資料

JNSA

セキュリティ知識分野(SecBoK)
人材スキルマップ 2016年度版



- **情報セキュリティに関わる人材が、身につけるべき知識とスキルを整理したもの**
- セキュリティ人材が担うべき業務を、職種単位ではなく、役割ごとに定義
- 学習すべき事項についても役割ごとに整理してまとめられている

セキュリティ対応組織の教科書
第1.0版

図 6　セキュリティ対応の役割分担

- **SOC(Security Operation Center) やCSIRT (Computer Security Incident Respose Team) においてどのような機能、役割、人材が必要となるかまとめたもの**
- 役割分担の考え方や、組織パターン、対応体制（人員など）にも言及されている

ゲームを終えて…

感染経緯①

メールに添付されている不審な添付ファイルの開封

不審なメールの例

件名：請求書をお送りします
本文：お疲れ様です。遅くなりました。
ご依頼の請求書をお送りします。

ご確認の上、お手配よろしくお願いします。また、こちらの URL でも確認が可能です。

http[:]//www.example.com/~~

不審な添付ファイルの例

見積もり用写真.xlxs**.exe**

アイコンを偽装している
実は exe ファイル

アイコンを誤解させやすいよう、
ファイル名もわかりにくく

宛先や差出人、内容に見覚えのない不審なメールには注意しましょう。
少しでも不審に思ったら添付ファイルは開封しないようにしましょう。

ゲームを終えて…

感染経緯②

改ざんされた Web サイト経由での感染

攻撃者によって改ざんされた Web サイト

①日常的に利用しているウェブサイトを閲覧

ユーザー端末

②意図せず、別サイトに誘導される

攻撃者の用意した Web サイト

③マルウエアをダウンロードさせる

使用している製品やソフトウェアのバージョンアップデートを適切に行いましょう

IE などのブラウザ / Java / Flash Player 等

脆弱性が未修正のままだと
マルウエアに感染する可能性がある