サイバーセキュリティ動向について

私立大学情報教育協会
情報セキュリティ対策問題研究小委員会 アドバイザー

東京大学大学院情報学環　特任准教授
JPCERT/CC 早期警戒グループ技術アドバイザー
満永　拓邦

プロフィール

- 名前：満永　拓邦(みつなが　たくほう)
- 所属：東京大学情報学環 セキュア情報化社会寄付講座(SiSOC)
  特任准教授

  JPCERTコーディネーションセンター
  早期警戒グループ 技術アドバイザー
- 業務：・セキュリティに関する情報の収集・分析・発信
  ・外部の組織や企業の経営層やシステム管理部門との連携
  ・セミナーや大学などでの講演活動
  ・セキュリティ関連調査のレポート執筆

「サイバー攻撃からビジネスを守る」
監修/共著

「情報セキュリティ白書　2013」
分担執筆

HTML5 を利用したWebアプリケーションの
セキュリティ問題に関する調査報告書

情報セキュリティを取り巻く現状

JPCERT/CCとは

一般社団法人JPCERTコーディネーションセンター
（JPCERT/CC (ジェーピーサート・コーディネーションセンター)）

JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

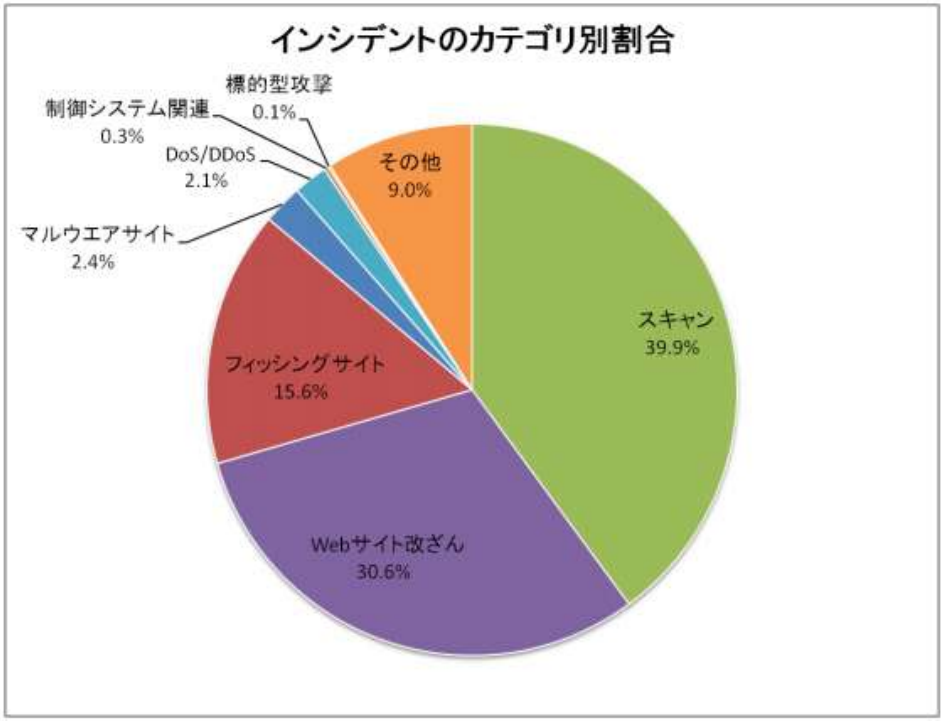
- https://www.jpcert.or.jp/
- サービス対象: 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**我が国の窓口となる　CSIRT**

※各国に同様の窓口となる　CSIRTが存在する
(例えば、米国のUS-CERT,CERT/CC、中国のCNCERT, 韓国のKrCERT/CC、など)

- 経済産業省からの委託事業として、コンピュータセキュリティ早期警戒体制構築運用事業を実施

2015年度のJPCERT/CCにおける インシデント対応状況

- JPCERT/CCへの報告
  - 全インシデント件数
    17,342件
- JPCERT/CCからの連絡
  - 全調整件数
    7,606件
    うち標的型
    148件



インシデント件数のカテゴリ別割合
（2015年4月～2016年3月）

昨年度の報告件数は ２２，２５５件であり、やや減少傾向

JPCERT/CC インシデント報告対応レポート https://www.jpcert.or.jp/ir/report.html より

インシデント数増加の背景

ITの社会インフラ化

- 企業活動のIT化
- 電子商取引の発展
- 制御系システムへの利用

インターネットの世界的な普及

- ボーダレスの通信
- 物理的な追跡困難性

攻撃用インフラの整備

- 攻撃ツールの進歩
- 分業化された攻撃集団

今後、サイバー攻撃の増加が予想されるため、各組織においても対応体制が必要！

攻撃者の分類(再掲)

- 攻撃の目的をもとに攻撃者を分類すると、それぞれの攻撃手法や技術力が異なることが推察できる

	愉快犯/ハクティビスト	**金銭目的の攻撃者**	**標的型攻撃の実行者**
攻撃の目的	- 政治的な主張 - 技術力のアピール	- 金銭の獲得(不正送金)	- 標的とする組織内の重要情報窃取やシステム破壊
主な攻撃手法	- Web サイトに対するDoS - 政治的な主張を目的とするWeb サイトの改ざん - SNS アカウント乗っ取り	-マルウエアが添付されたメールの送付 -Web サイト改ざんによるマルウエアの配布	-マルウエアが添付されたメールの送付 - Web サイト改ざんによるマルウエアの配布 (ただし攻撃対象のみに限定)
技術力	低		高

JPCERT/CC 早期警戒グループにて独自に分類

歴史的特異日に関連する攻撃(1/2)

- 政治的な主張を行うため、歴史的特異日に Web サイトへ対して改ざんや DDoS 攻撃を行うことがある。

  (歴史的特異日例)
  - ９月１８日(満州事変)
  - ３月　 １日(独立運動)

ニュース詳細

最高裁のHP改ざん 「尖閣諸島は中国」

最高裁が運営する全国の裁判所のホームページ(HP)が14日、改ざんされ、中国名で沖縄県・尖閣諸島を意味する「釣魚島は中国である」との文章などが表示されて閲覧できない状態になった。最高裁は復旧を急いでいる。

改ざんされたHPには、島に中国国旗を立てたイラストとともに、日本語で「釣魚島は中国であり、日本は釣魚島から抜け出す」と表示された。中国語と英語の文章もあった。

改ざんされた最高裁のホームページ

[引用 47NEWS] http://www.47news.jp/CN/201209/CN2012091401001932.html

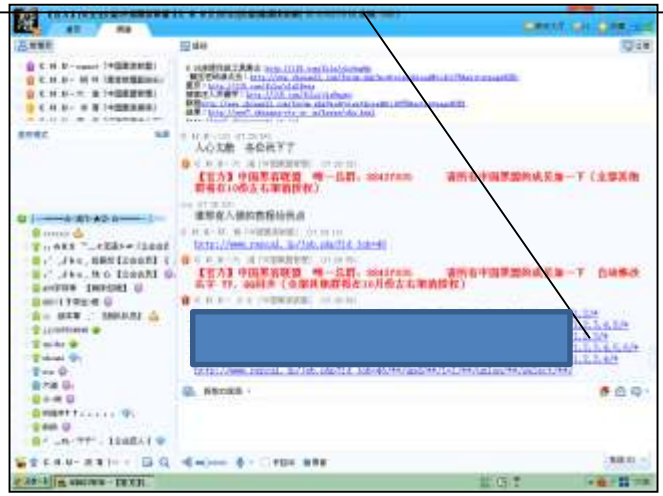
歴史的特異日に関連する攻撃(2/2)

- 高度な技術力を持つ攻撃者ではなく、一般のインターネットユーザが、お祭り騒ぎのようにチャットに集い、日本のWebサイトに対して攻撃を行う
- チャットルームでは、攻撃に関連する情報の交換や攻撃ツールの配布が行われている

攻撃用ツール

あるサイトに SQL Injection の脆弱性が見つかった旨の発言

/**/1=1/**/and/**/union/


チャットルームの様子

ハクティビストによる攻撃例

SiSOC TOKYO

#OpKillingBay

- 捕鯨活動に関する抗議や動物愛護を目的とする抗議活動
- Tweet Storm と呼ばれる Twitter を使用したメッセージの発信が主な活動であるが、アノニマス系の攻撃者により、サイバー攻撃に発展することもある
- 主な対象
  - 捕鯨に関連する自治体
  - 水族館や水族館関連組織
  - 国内の民間企業や**大学等研究機関**
    （捕鯨とは関係なく、注目を浴びる攻撃対象を選定している）

攻撃者の分類(再掲)

- 攻撃の目的をもとに攻撃者を分類すると、それぞれの攻撃手法や技術力が異なることが推察できる

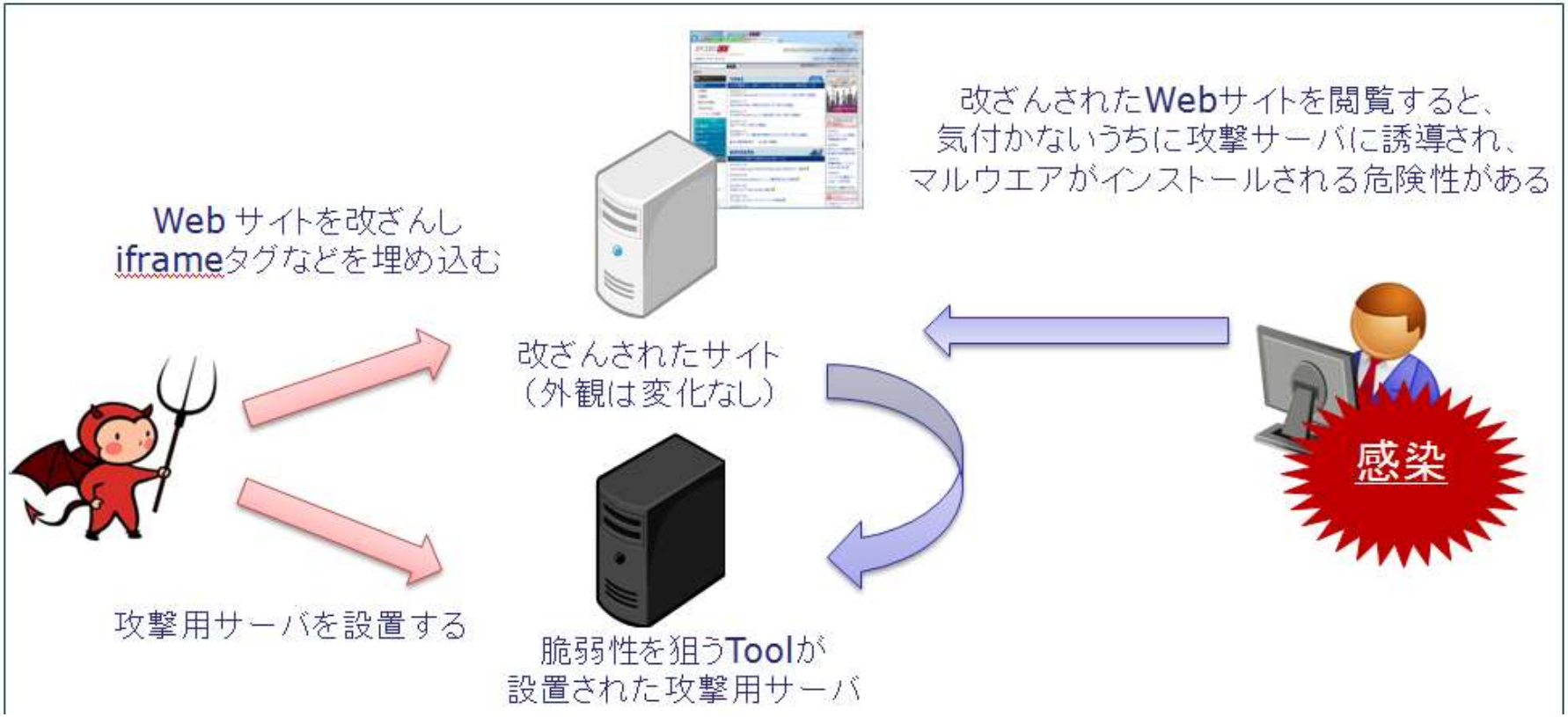
	愉快犯/ハクティビスト	**金銭目的の攻撃者**	**標的型攻撃の実行者**
攻撃の目的	- 政治的な主張 - 技術力のアピール	- 金銭の獲得(不正送金)	- 標的とする組織内の重要情報窃取やシステム破壊
主な攻撃手法	- Web サイトに対するDoS - 政治的な主張を目的とするWeb サイトの改ざん - SNS アカウント乗っ取り	-マルウエアが添付されたメールの送付 -Web サイト改ざんによるマルウエアの配布	-マルウエアが添付されたメールの送付 - Web サイト改ざんによるマルウエアの配布 (ただし攻撃対象のみに限定)
技術力	低		高

JPCERT/CC 早期警戒グループにて独自に分類

Webサイト閲覧によるマルウエア感染

- メールの添付ファイル以外にも、マルウエア感染の経路として、改ざんされたWebサイト閲覧がある
- 攻撃者は、マルウエアに感染した端末を不正に操作したり(不正送金)、情報を窃取することで金銭的な利益を得る

・Web サイト閲覧によるマルウエア感染の概要



不正送金の被害とツール

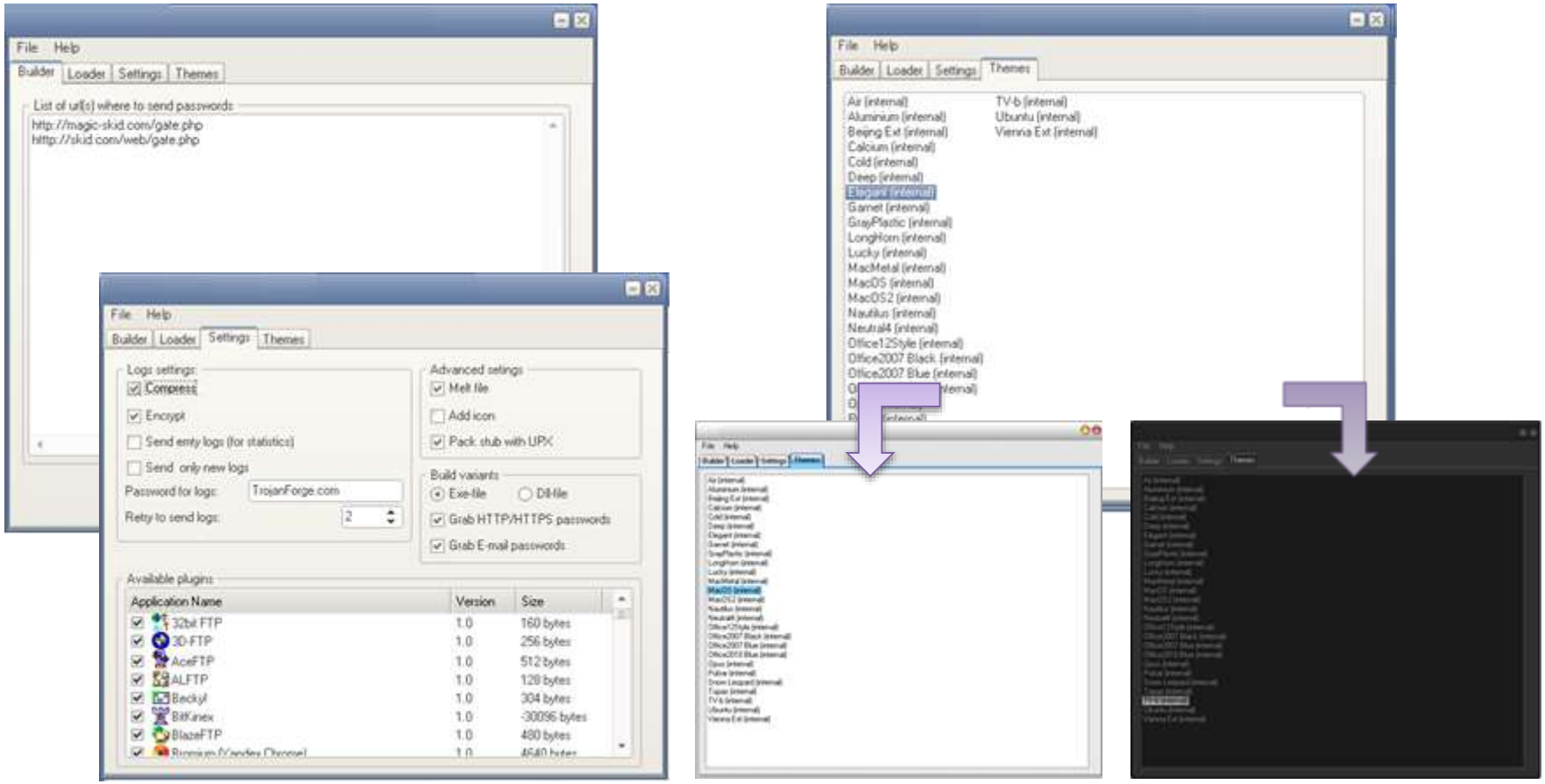
- マルウエア感染による不正送金の被害(2015年)
  - 被害件数　　1,495件
  - 被害金額　　**約30億7300万円**

インターネットバンキングに関する不正送金の発生件数と被害額の推移
(引用) http://itpro.nikkeibp.co.jp/atcl/news/16/030300664/?rt=nocnt

突然、銀行口座から預金が消えることに・・。法人口座も攻撃対象
cf. 法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方
http://www.zenginkyo.or.jp/abstract/news/detail/nid/3349/

増加の背景

いわゆるブラックマーケットにおいて、マルウエアを生成するためのビルダーや管理ツールの普及が進む



マルウエア生成用ビルダーの画面

増加の背景

情報送信先(Web管理パネル)

メイン画面

レポート画面

マルウエア管理用ツールの画面

金銭を要求するマルウエア(ランサムウエア)

- 2016年2月、米国医療機関Hollywood Presbyterian Medical Center にて院内の端末がランサムウエアに感染するインシデントが発生した
- 緊急処置室のシステムをはじめ、ＣＴスキャン、電子文書などが影響を受け、一部の患者が他の医療機関に運ばれる事態となったとのこと
- 医療機関は復号鍵のため40BitCoin(約17,000ドル)を支払い、システムは復旧した（**<u>システムやファイルのバックアップは極めて重要</u>**）

Hollywood Presbyterian Medical Center

経緯と対応についてのプレス発表
http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf

攻撃者の分類(再掲)

- 攻撃の目的をもとに攻撃者を分類すると、それぞれの攻撃手法や技術力が異なることが推察できる

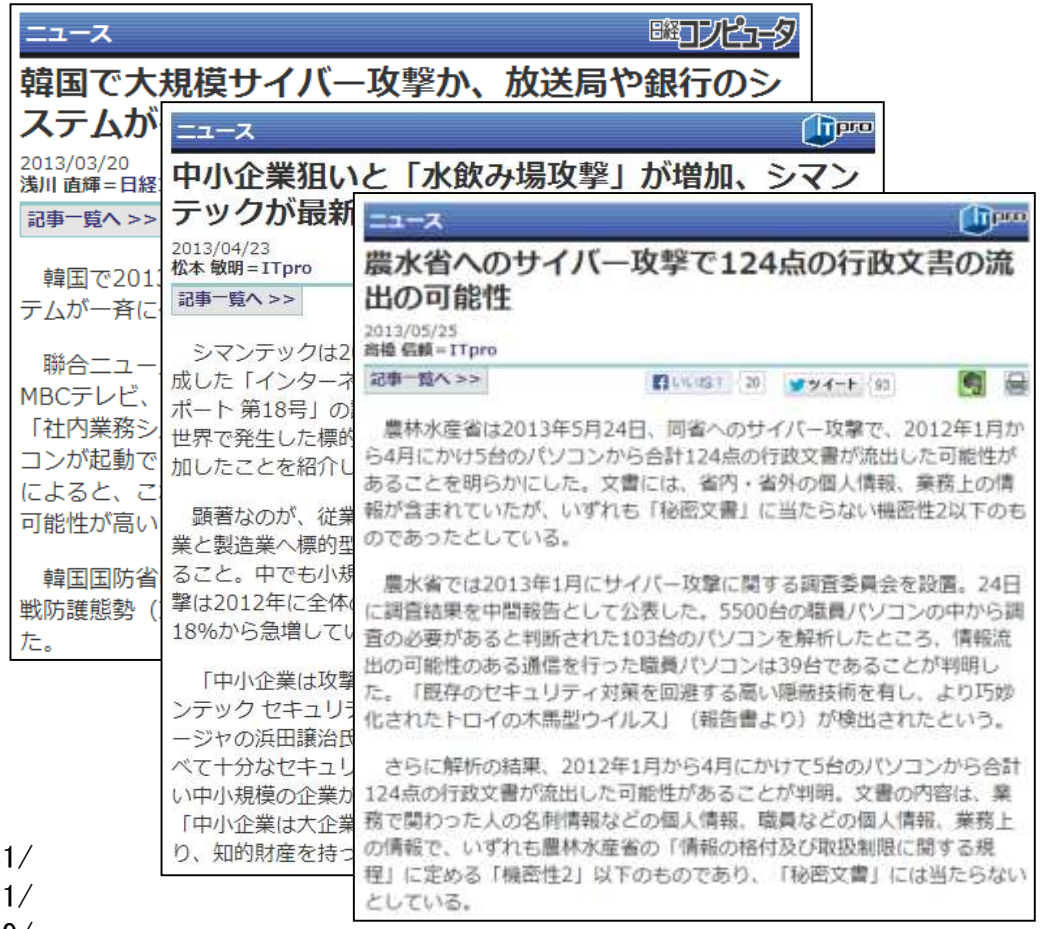
	愉快犯/ハクティビスト	**金銭目的の攻撃者**	**標的型攻撃の実行者**
攻撃の目的	- 政治的な主張 - 技術力のアピール	- 金銭の獲得(不正送金)	- 標的とする組織内の重要情報窃取やシステム破壊
主な攻撃手法	- Web サイトに対するDoS - 政治的な主張を目的とするWeb サイトの改ざん - SNS アカウント乗っ取り	-マルウエアが添付されたメールの送付 -Web サイト改ざんによるマルウエアの配布	-マルウエアが添付されたメールの送付 - Web サイト改ざんによるマルウエアの配布 (ただし攻撃対象のみに限定)
技術力	低		高

JPCERT/CC 早期警戒グループにて独自に分類

増加する標的型攻撃の脅威

SiSOC TOKYO

- 国内外を問わず、ここ数年で被害が増加
- 対象
  - ・政府系組織
  - ・重要インフラ事業者
  - ・研究機関
  - ・社会に大きな影響をもつ組織
  - ・機密情報を保有する組織



（引用）
http://itpro.nikkeibp.co.jp/article/NEWS/20130320/464581/
http://itpro.nikkeibp.co.jp/article/NEWS/20130525/479521/
http://itpro.nikkeibp.co.jp/article/NEWS/20130423/472869/

標的型攻撃(APTによる攻撃)について

SiSOC TOKYO

【先進的】
攻撃者は目的達成のために必要な最小限のツールしか使用しない。そのため、一連のイベント自体が「先進的」と見なされる。

【執拗な】
攻撃者は ネットワーク上に長期にわたって居座り続ける。例えば、繰り返しアクセスを図り、複数年にわたってアクセスを維持することもある。

【脅威】
攻撃者は長期的な 活動を実施するために技術だけではなくリソースが必要である。そのため、攻撃者には国家が支援する能力者や先進的なサイバー犯罪者が含まれる場合がある。

- 攻撃者は、先進的なツールとテクニックを用いて高度に組織化された活動を展開する。
- 標的を攻略し、アクセスを維持するために、複数の手法、ツールやテクニックを組み合わせることが多い。

- 攻撃者は長期的に活動することに集中し、侵入に成功した組織内の足場の構築・維持を図る。
- 機密情報などデータの収集に集中する。
- 長期に活動可能なインフラを構築する。
- アプローチ方法は、目立たず、ゆっくり。

先進的で（Advanced） **執拗な（Persistent）** **脅威（Threat）**

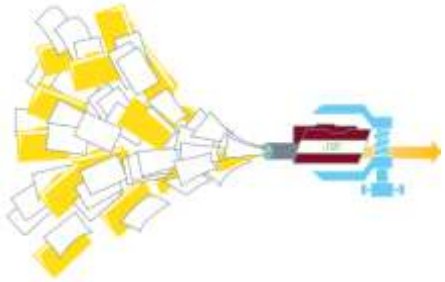
APT攻撃者は、明確な攻撃の目的とその能力を有しており、その活動は組織化されて資金も十分で、また経験も豊富に有した人たちが連携することで行われる。

リスク	想定される攻撃者
●評判を失う	●競合他社
●競争優位性を失う -IDの窃盗 -交渉内容の漏洩	●国家スパイ、産業スパイ
●内部情報の売買	●犯罪組織
●事業能力の低下	●競合他社、国家が後押しする団体

APTによる攻撃の特徴

- 米セキュリティ企業 Mandiant 社のレポートによると APT による攻撃の特徴は以下の通り、
  - 組織的かつ体系的な攻撃により、20業種141組織から数百テラバイトの情報を窃取された
  - 侵入を発見するきっかけは、 94%が外部からの通知による
  - 組織内に侵入されていた平均の期間は、356日であり、期間が長い場合では1764日であった
  - 組織内ネットワークに一度侵入を許すと、数カ月から数年の期間に渡って、組織内に保管されている技術文書、財務資料、経営計画、契約書など様々に渡るカテゴリーの情報、ならびにEメールアドレスなどの外部の連絡先を窃取した

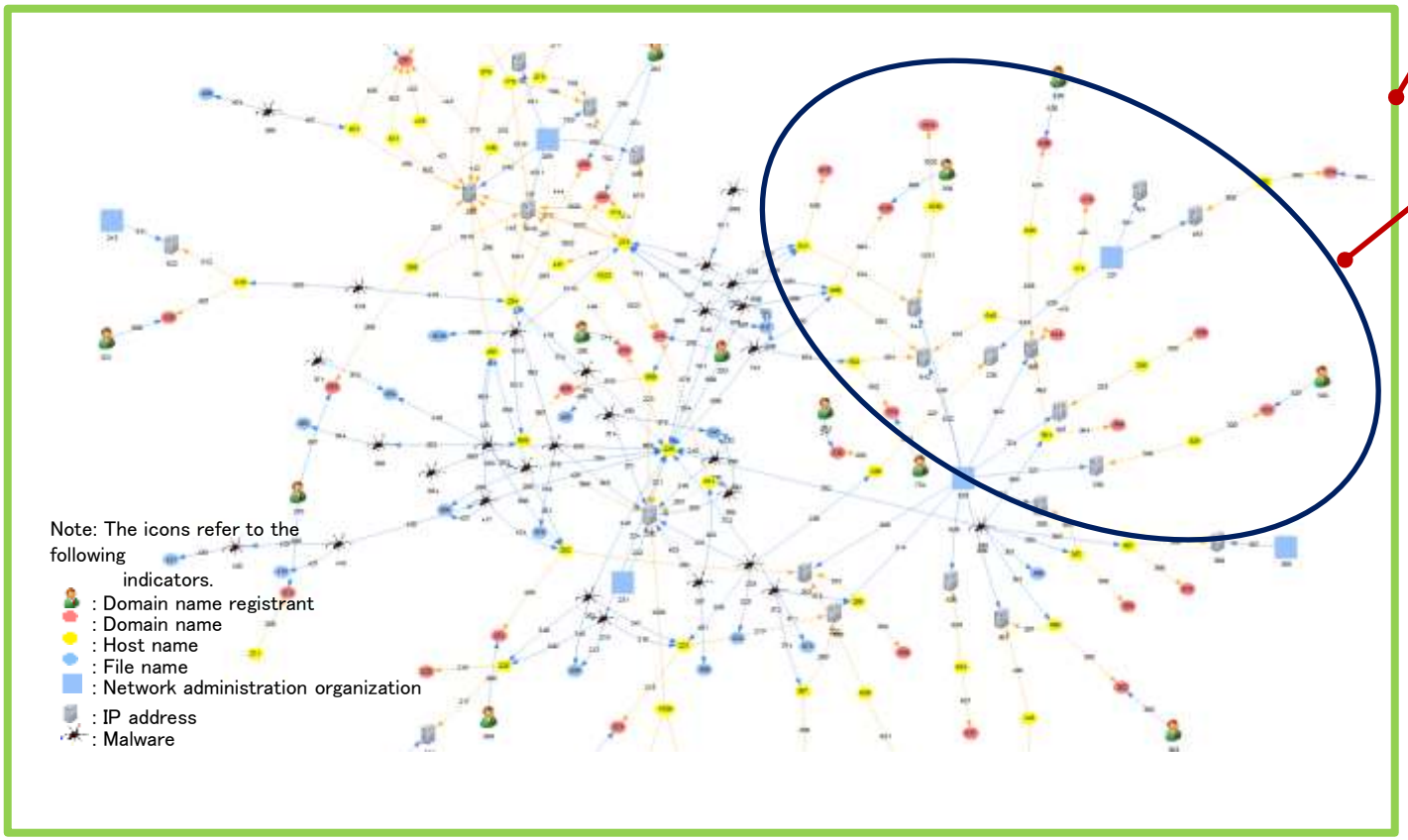
(参考)
Mandiant Intelligence Center Report
http://intelreport.mandiant.com/



高度サイバー攻撃のインフラ分析事例

SiSOC TOKYO

Emvidi攻撃に関して、共有情報や複数のオンサイト調査などを通じて得た攻撃関連情報（マルウエア、C2サーバなど）を可視化



ある時点で判明した全貌

ひとつの調査で判明した攻撃（イメージ）

- 攻撃被害者に見えたものが全てではない
- 攻撃全貌の解明努力は氷山の一角から
- 全貌と局所の乖離は復旧・封じ込め見落としにつながる

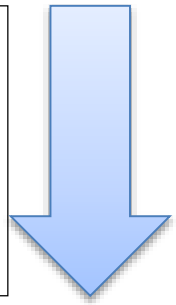
社会環境の変化

「通知」におけるコミュニケーション

- 「御社は標的型攻撃の被害にあっているようだ」と外部組織から連絡を受けた際に、迅速な対応が実施できる体制を構築できているか
- リスク・コミュニケーションという観点からは、「面識がない人から突然連絡を受け、リスク(脅威)を説明されたとしても信頼や理解しずらい」とされる。むしろ疑うのが自然。

→日常的にリスクへの理解や信頼構築を行う必要性がある

1. **C**redibility(信頼の確立)	価値観の共有を通じた信頼の確立
2. **A**wareness(気づき・意識)	リスクに気づき、意識する
3. **U**nderstanding(理解)	リスクについて理解を深める
4. **S**olution(解決策)	リスクに対する解決策を理解、検討する
5. **E**nactment(対処行動)	リスクへの対処行動を起こす



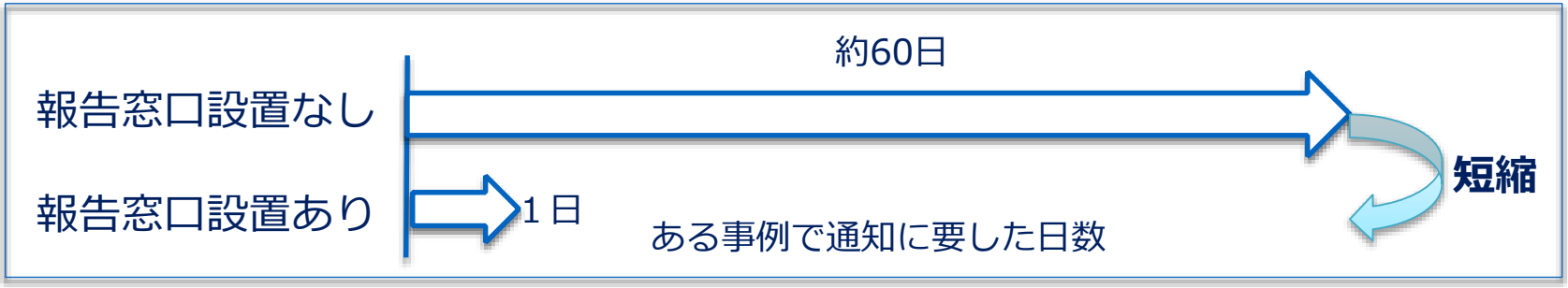
信頼醸成と
リスクへの対処

リスク・コミュニケーションにおけるCAUSEモデルの段階
(参考)KE Rowan: “Why Rules for Risk Communication Are Not Enough”

初動開始までの時間の違い

- 報告窓口に通知できない場合、セキュリティ担当部門に届くまでに約60日を要した事例がある(設置後は即日通知が可能になった)

→セキュリティに関する外部組織との連絡窓口を設置し、また組織内部で実効的な調整を行える体制が必要（組織内CSIRTの必要性）



- 代表電話番号や一般の問い合わせ窓口からセキュリティ担当部門までの情報伝達が、必ずしもスムーズが行われるわけではない
- そのため、セキュリティ担当部門への報告窓口を設置している組織への通知と、設置していない組織への通知は必要な日数は異なることが多い
- リスク・コミュニケーションという観点からは、「面識がない人から突然連絡を受け、リスク(脅威)を説明されたとしても信頼や理解しずらい」とされる。むしろ疑うのが自然。

サイバーセキュリティは経営課題に

SiSOC TOKYO

- セキュリティインシデント発生は**株価にネガティブな影響**を与える
  cf.「サイバー・セキュリティ・インシデントが企業価値に与える影響」
  田中秀幸・中野邦彦(2016)

- 重大なインシデントの場合には**膨大な対応費用**が発生する
  ex. Sony(PSN)、ベネッセ、JTB 等

- 企業の信頼低下による顧客離れや、業務提携先への影響する可能が
  ex. JTB の件では NTT docomo、Yahoo Japan にも影響

https://www.nttdocomo.co.jp/info/notice/page/160614_00_m.html

http://blogs.yahoo.co.jp/yjtravel_staff/20970682.html

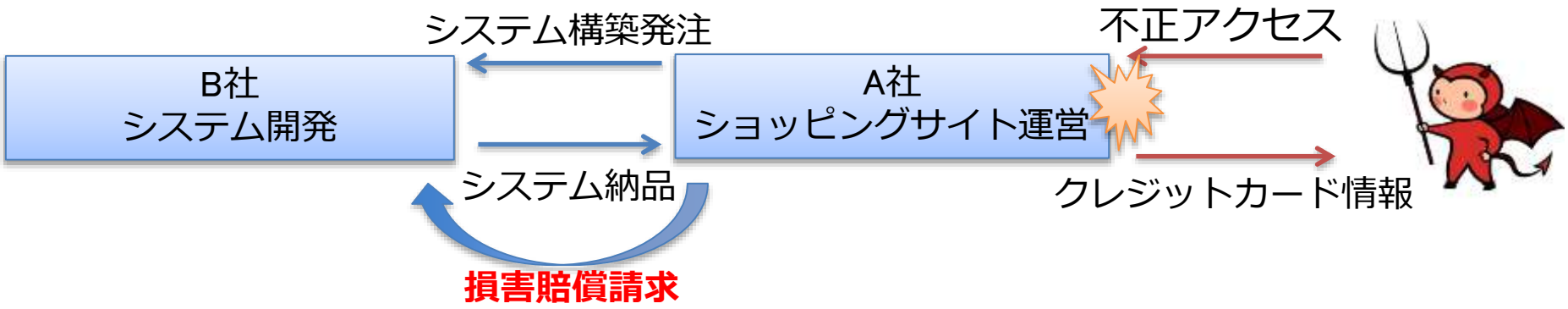
サイバーセキュリティ経営ガイドライン

２０１５年に経済産業省とIPAが経営者に向けてサイバーセキュリティの考え方と重要項目を定めたガイドラインを公開。本ガイドラインには**「サイバーセキュリティは経営問題」**と明記されている。

No.	重要項目
1	サイバーセキュリティリスクの認識、組織全体での対応の策定
2	サイバーセキュリティリスク管理体制の構築
3	サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
4	サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
5	系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握
6	サイバーセキュリティ対策のための資源（予算、人材等）確保
7	IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
8	情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
9	緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
１０	被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

サイバー攻撃により生じた損害の賠償請求

- 2009年、A社はB社にショッピングサイトのシステム構築を発注
- 2011年、A社のサイトに対して不正アクセス(SQLインジェクションの脆弱性を利用)が行われて、クレジットカード情報が漏えい
- 2011年、A社はB社に対して、対応調査の費用、売上減少による損害等について、委託契約の債務不履行に基づき1億円余りの損害賠償を請求
- 2014年、東京地裁はB社に対して約2262万円の損害賠償金を支払うように命じた（確定）



ポイント！
契約書、仕様書にはセキュリティ対策に関する記載はなかったが、
経産省等が「SQLインジェクション」に関する注意喚起を出しており、
対策は「専門家として当然果たすべき責務」であったと判断された

インシデント対応プロセス

SiSOC TOKYO

マネージメントの積極的関与

外部との情報連携

外部からの情報で
インシデントが発覚する
ケースが多い

インディケータ

ここが
最も重要

一般的に
ここが起点になる

外部と共有

準備 | **検知・分析** | 封じ込め | 根絶 | 修復 | **教訓**

平常時の備え

有事における対応

原因追及、**全容把握**、**フィードバック**のために多種のデータを利用

- ✓通信ログ（ファイアウオール、プロキシ等: 内部⇒外部や内部⇒内部）
- ✓証跡データ（IT資産管理システム等）
- ✓IT資産管理情報など

セキュリティに関する対応体制

SiSOC TOKYO

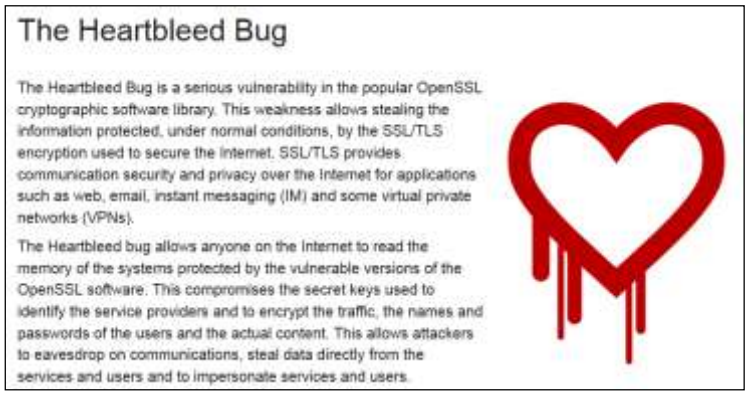
- インシデント(*)発生時の対応体制
  - ユーザ部門、システム管理、営業、法務、広報などの関連部署間で情報の共有及び対策の一元化
  - システム責任者、対応フローの明確化(例：誰がサーバを止めれるか？)

インシデント(*)・・IT システムの正常な運用または利用を阻害するマルウエア感染、不正アクセス、情報漏えい、DoS 攻撃などの事案や現象の発生をいう

例えば・・・

- ２０１４年に、 SSLなどを利用するためのライブラリ「OpenSSL」に関する情報漏えいの脆弱性が公開された。攻撃手法も公開されており、いつ攻撃を受けてもおかしくない状況であった。緊急度が高い状況で、例えば以下の様な対応体制を事前に関係者間で確認しておく事で、迅速な対応が可能になる。
  - 管理サーバが、当該脆弱性の影響を受けるかの担当者と確認フロー
  - 影響を受ける場合、サービス停止を決定する社内プロセス
  - 脆弱性情報や対応状況に関する社内の情報共有体制
  - 被害を受けた場合の対応手順、顧客への連絡、プレスリリース

JPCERT/CC OpenSSL の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140013.html



The Heartbleed Bug
http://heartbleed.com/

完全なセキュリティ予防策はない

SiSOC TOKYO

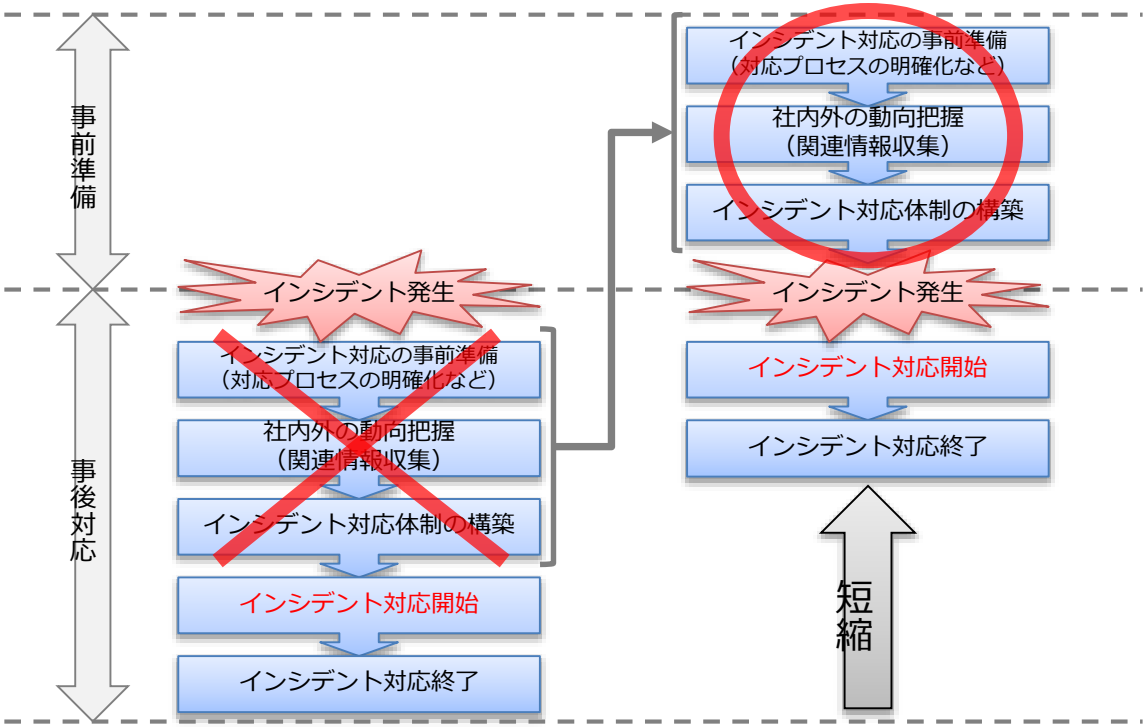
- インシデント対応活動
  - インシデントを検知し、或いはその報告を受けることにより認知し、影響の拡大を防ぐとともに、情報を収集して分析を加え、インシデントの全体像や原因について把握し、復旧措置や再発防止のための措置を取る
- 「コンピュータセキュリティ」で思い描くイメージ
  - 「いかにしてインシデントの発生を未然に防ぐか」を主眼に置かれることが多い
- コンピュータセキュリティを取り巻く状況を見ると．．．
  - 人為的ミス（パッチの適用忘れなど）
  - 未知（公知になっていない）の脆弱性の悪用
  - 技術的な対応の限界　等

インシデントの発生を「完全に回避する」ための予防策はない
（事故前提の対応体制が必要）

（発生確率を低下させ、発生時の影響や被害を低減するための予防策はある）

事前準備の重要性

- インシデント発生後、その対応方法を考え始め、対応体制をとるのは、被害を拡大させる一因となるため、できるだけ**事前に** 対応体制等を整えておく必要がある



対応体制構築、マニュアル整備に加え、
情報セキュリティに関する”避難訓練(対応訓練)”を実施してみる

まとめ

- サイバー攻撃は突然無くなることはなく、今後も継続して発生すると考えられる

- 経済産業省のガイドラインにある通り、サイバーセキュリティ対策は経営問題であり、対岸の火事ではない
（損害賠償請求裁判となる事例も）

- １００%の防御手法がないため、万が一、被害が発生した時に備える必要がある(CSIRT)

- 外部リソースを活用しつつ、基本的な対策から始める
まずは、サイバーセキュリティの避難訓練から！

東京大学 情報学環

CSIRT と消防署の役割の比較例

CSIRT の場合（例）

- 発生したインシデント対応
  - 連絡先の提供：　Email アドレス／電話
  - 連絡目的：　対応や技術支援などの要請
  - CSIRT　での活動
    - インシデントの分類、優先度の判断と対応方法の決定
    - 適切な（技術的）対応を取る人への連絡調整
    - 被害の極限化策の実施（ネットワークからの切り離し、システムの設定変更等）
    - インシデント原因の排除（脆弱性箇所へのパッチ適用、ウィルス除去、Phishing サイト停止等）
- インシデントの発生予防
  - ユーザへのセキュリティ啓発活動
  - インシデント脅威情報の提供

消防署の場合（例）

- 発生した火事や事故への対応
  - 連絡先の提供：　電話（１１９番）
  - 連絡目的：　消火依頼、救出要請など
  - 消防署での活動
    - 火災規模、症状等の判断と対応方法の決定
    - 最寄の消防車や救難器材の手配に関する連絡
    - 火事の拡散防止や救出等の緊急避難等のための一部破壊
    - 消火活動及び救出活動
- 火事や事故の発生予防
  - 防火訓練や救出講習等の啓発活動
  - 火災／乾燥注意報による注意の呼びかけ

参考資料

- JPCERT/CC　における関連文書
  - 組織内 CSIRT 構築支援マテリアル
    - http://www.jpcert.or.jp/csirt_material/
  - コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック
    - http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf

- その他の参考資料
  - CERT/CC – “Creating a Computer Security Incident Response Team: A Process for Getting Started”
    - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - TERENA – “CSIRT Starter Kit”
    - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - AusCERT – “Forming an Incident Response Team”
    - http://www.auscert.org.au/render.html?it=2252
  - RFC 2350 – “Expectations for Computer Security Incident Response”
    - http://www.ietf.org/rfc/rfc2350.txt