高度化するサイバー攻撃の脅威

-2017年前半に発生した攻撃を例として-

2017年9月26日

JPCERT/CC 早期警戒グループ
洞田 慎一

はじめに

「JPCERT/CCをご存知ですか？」

JPCERT/CC とは

■ **一般社団法人 JPCERT コーディネーションセンター**

Japan Computer Emergency Response Team / Coordination Center

- 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　**我が国における「セキュリティ向上を推進する活動」**を実施
- **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）**
- 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、米国のUS-CERT, CERT/CC, 中国のCNCERT, 韓国のKrCERT/CC)

■ 経済産業省からの委託事業として、
サイバー攻撃等国際連携対応調整事業を実施

「JPCERT/CCをご存知ですか？」

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

脆弱性情報ハンドリング

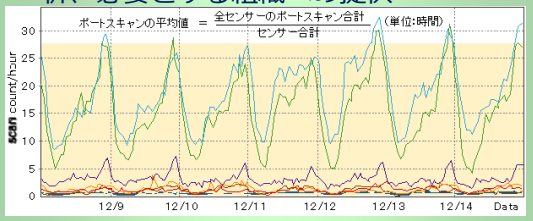
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

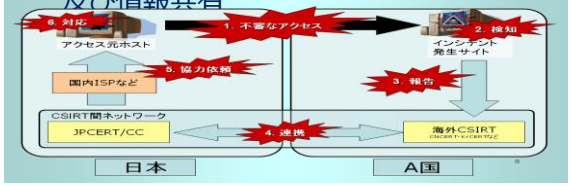
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応調整支援）

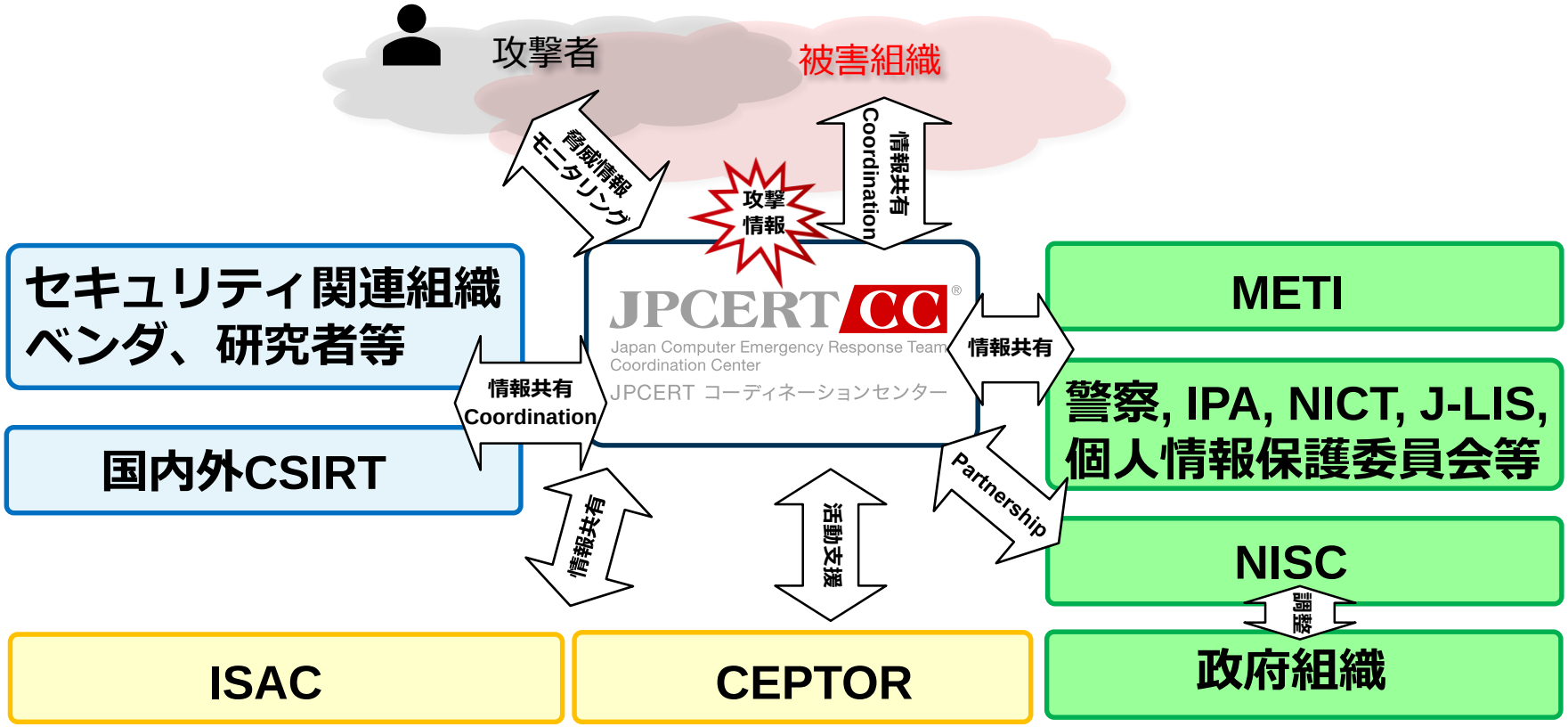
- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング/情報収集,分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

コーディネーションセンターとしての役割

■ 様々なパートナーとの調整



インシデントに関する調整 (coordination) 期間として、問題解決に向けて、必要な人に必要な情報を届ける業務を行っています

JPCERT/CC の活用

コーディネーションセンターの役割と活用

- インシデントレスポンス
- 脆弱性・脅威情報に関する情報流通
  - 脆弱性情報 | JVN
  - 脅威情報 | 注意喚起、早期警戒情報他
- アーティファクト分析
- 国内外 CSIRT 連携

“インシデント”に沿った活動を展開しています

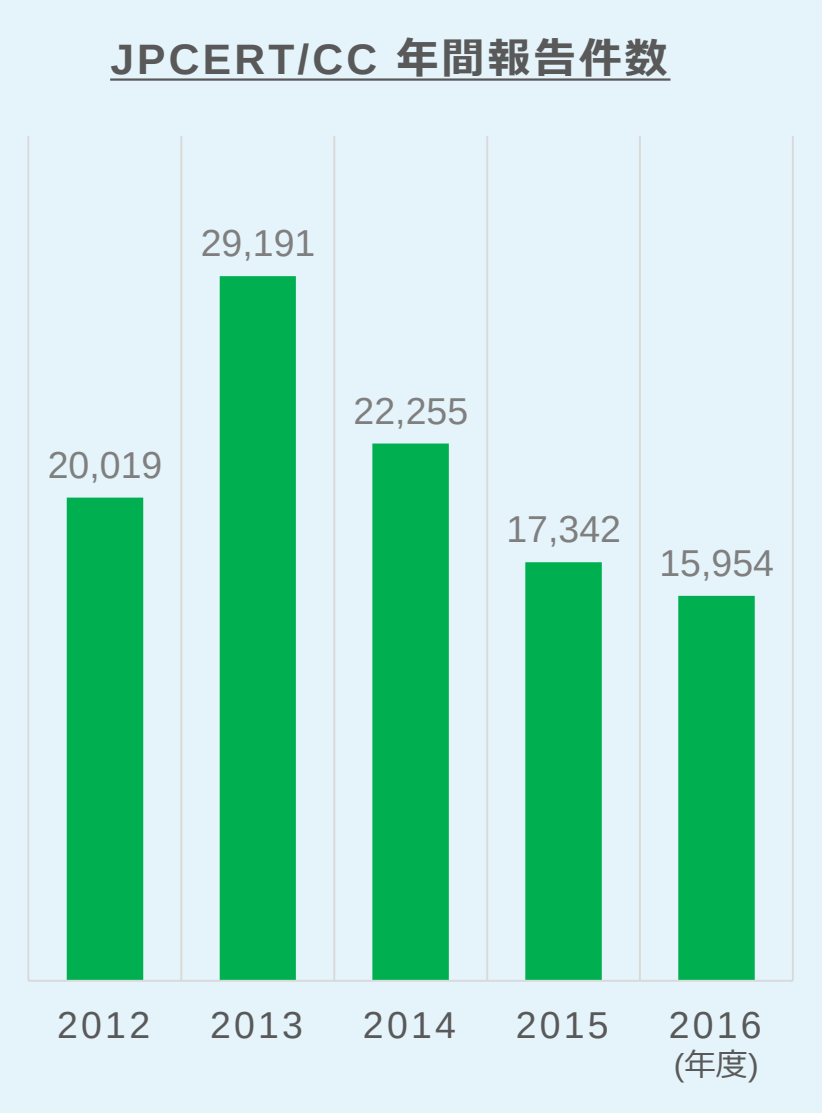
例えば、こんなときにお役立てください

- インシデントが発生し、初動対応での技術的な支援や情報が必要となるケース
- 日々の対策を進める上で、脆弱性や脅威に関する情報が必要となるケース
- その他、よろずお気軽にご相談ください

コンピュータセキュリティインシデントとは

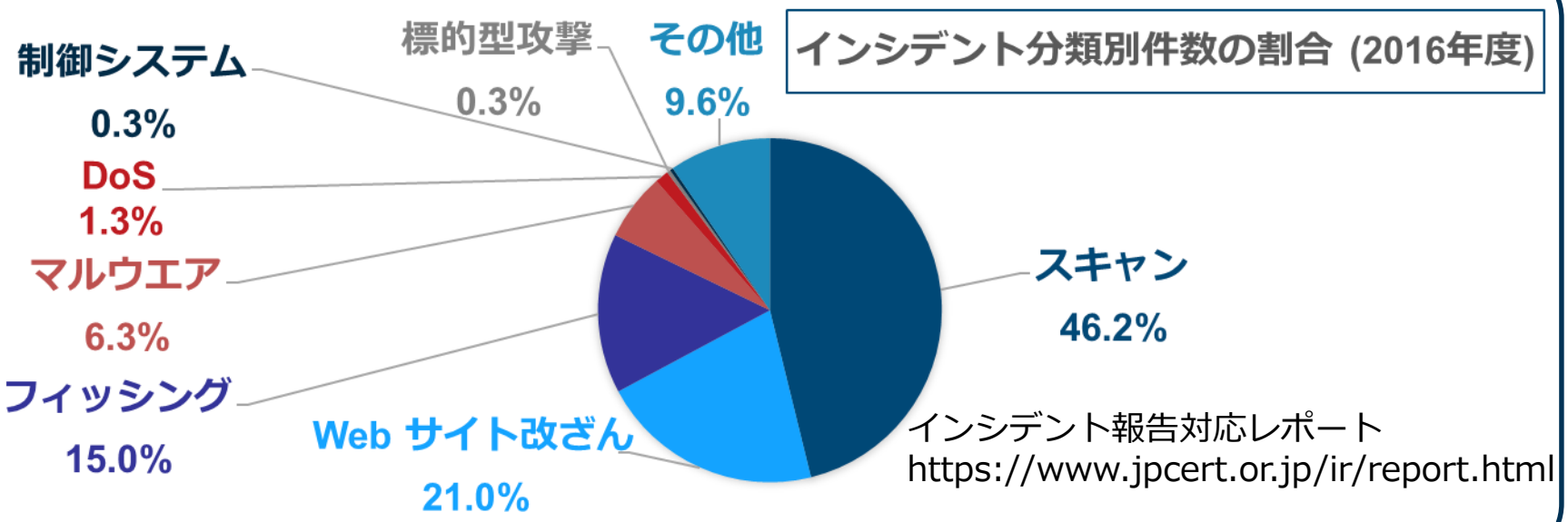
- コンピュータセキュリティインシデント・・・
  - **コンピュータセキュリティに関わる事象（事件・事故）**
  - **必ずしも自組織だけが被害をこうむるとは限らない**
- 年間 1万件以上のインシデント報告・・・
  - **2016年度 15,954 件**
  - **氷山の一角**

- **組織における「インシデント」の一要素でしかない**
- **組織によって温度感が異なる**



様々な種類のインシデントが発生

■ 様々な要因でインシデントは発生しています



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

■ サイバーインシデントがなくなるその日まで

— JPCERT/CC では、インシデントや、その原因・背景にある脆弱性に対する調整を行っています

2017年前半に発生したサイバー攻撃から

2017年前半に発生した主なサイバー攻撃

- 2016年6月～ “Datper” を用いた標的型攻撃
- 2017年2月 WordPress 脆弱性を悪用したサイト改ざん
- 2017年3月 Apache Struts2 脆弱性を悪用した情報窃取

本日取り上げる内容

- **2017年5月～ ランサムウエア “WannaCrypt” による攻撃**
- **2017年6月　その他のランサムウエアの出現**

Armada Collective による DDoS 攻撃

- 2017年8月 OpKillingBay 2017　ターゲットリスト公開
- 2017年9月 FX / 証券事業者等への DDoS 攻撃

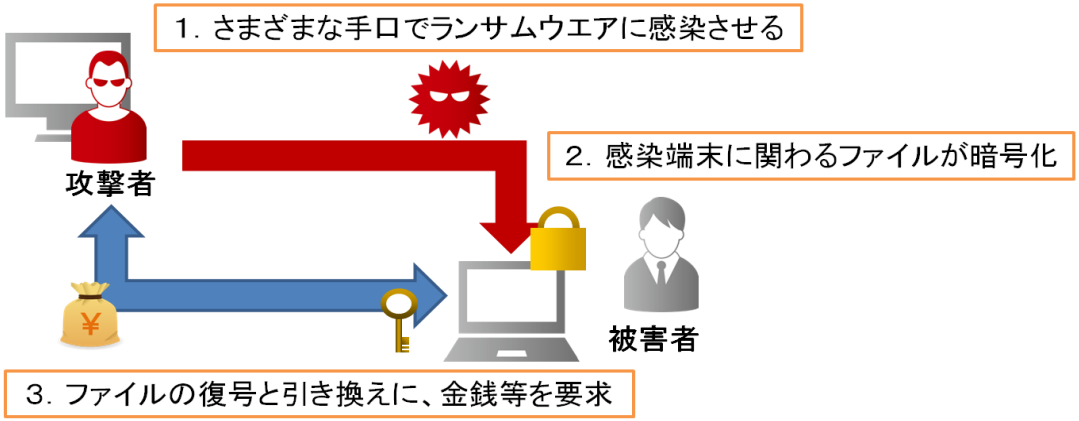
ランサムウエア

ランサムウエア

— マルウエアの一種。感染したコンピュータでは、システムやファイルを暗号化され、復号のための金銭を要求される。

2015年に日本語に文面を対応したランサムウエアが登場

— **海外では**ランサムウエアの被害が大きく、組織全体が影響を受けるほどの被害も報道されている
（例：サンフランシスコ私営鉄道、ロサンゼルスHPMC等）



WannaCryptの感染拡大

- **2017年5月12日頃以降、国内外にてWannaCryptの動向に関する情報が公開**

Multiple Ransomware Infections Reported
https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported

ランサムウエア "WannaCrypt" に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170020.html

世界的な感染拡大

- **その後も、WannaCryptによる影響とみられる事案が継続**
  - その後、WannaCrypt の亜種も登場し、現在も感染は続く
    - 2017年6月19日
      - 日本マクドナルドがランサムウエア感染によりシステム障害が発生と発表
    - 2017年6月21日
      - ホンダ狭山工場がランサムウェア感染により操業停止になったと報じられる

WannaCryptについて

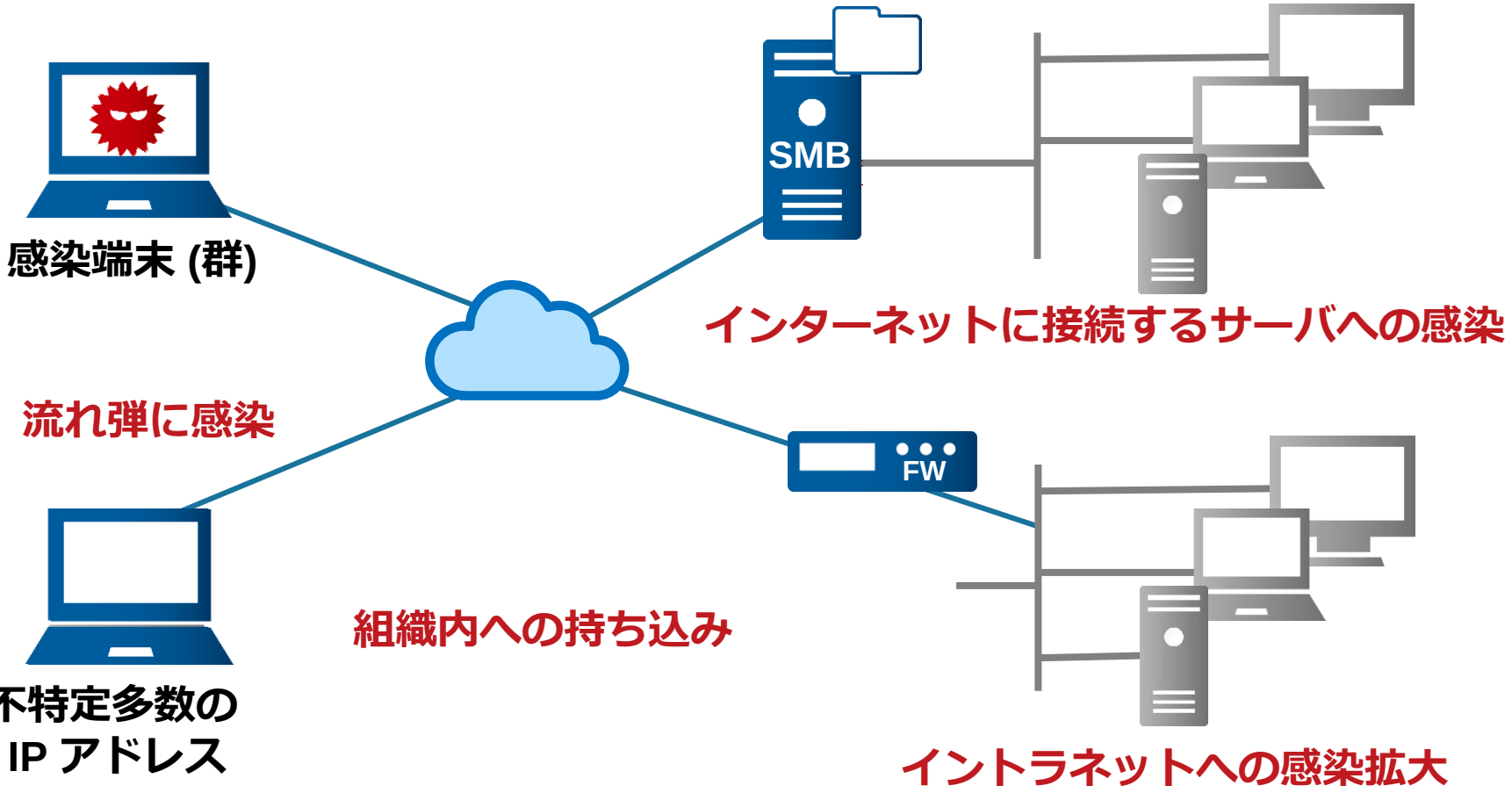
- **Wanna Decryptor、WanaCrypt0r 2.0、Wcryなどとして知られるランサムウエア**

- **他のランサムウエアと異なる特徴としては2点**
  - Shadow Browkers が公開したツールを使用
    - 「EternalBlue」と呼ばれるMS17-010を悪用
    - 「DoublePulsar」と呼ばれるコードを悪用
  - 動作を制御する機能「通称: Kill Switch」が実装されている

- **侵入経路について断定されていない**
  - JPCERT/CCでは、ネットワーク経由での感染に関する事例を確認

WannaCrypt 感染までの流れ

- 脆弱性 (CVE-2017-0147) を悪用し感染拡大
  - 通信ポート (445/tcp, ファイル共有) を介して感染拡大



検体を実行した場合の動作

1. 通信の可否の確認（Kill Switch）

- C:¥Windows¥直下にファイルの作成を試みるため管理者権限が必要

2. 感染端末外への感染活動（MS17-010の悪用）

[対象]
- ローカルIPアドレス
- グローバルIPアドレス（ランダム）

3. ランサムウエアの動作

- レジストリを変更し、再起動時も感染活動が実行される

脆弱性 (MS17-010) の悪用

- SMB トラフィックを処理するドライバにおけるバッファエラーを悪用

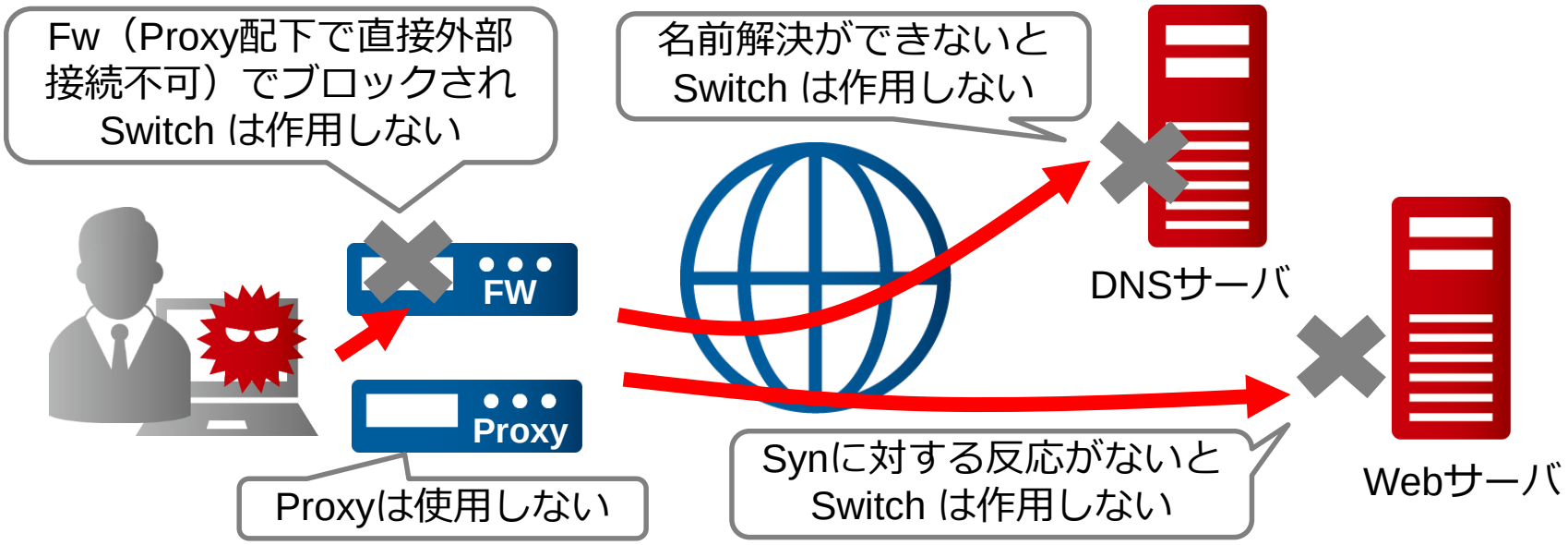
- EthernalBlue (FUZZBUNCH) がはじまり？
  - 細工した SMB トラフィックを送る
  - DEP / ASLR バイパス
  - 32bit / 64bit 両対応

- 侵入後は、lsass.exe (システム権限) を通じて実行
  - DoublePulser
  - 実行されて以後は、管理者権限で動作

Kill Switch の動作概要

- 検体の動作を制御するためのSwitch
- Proxyを使用しないで直接外部への接続を試みる
- 作用する条件

- ドメインの名前解決が可能
- サーバと接続が可能（通信の確立が可能）



WannaCrypt 亜種（2017年6月以降）

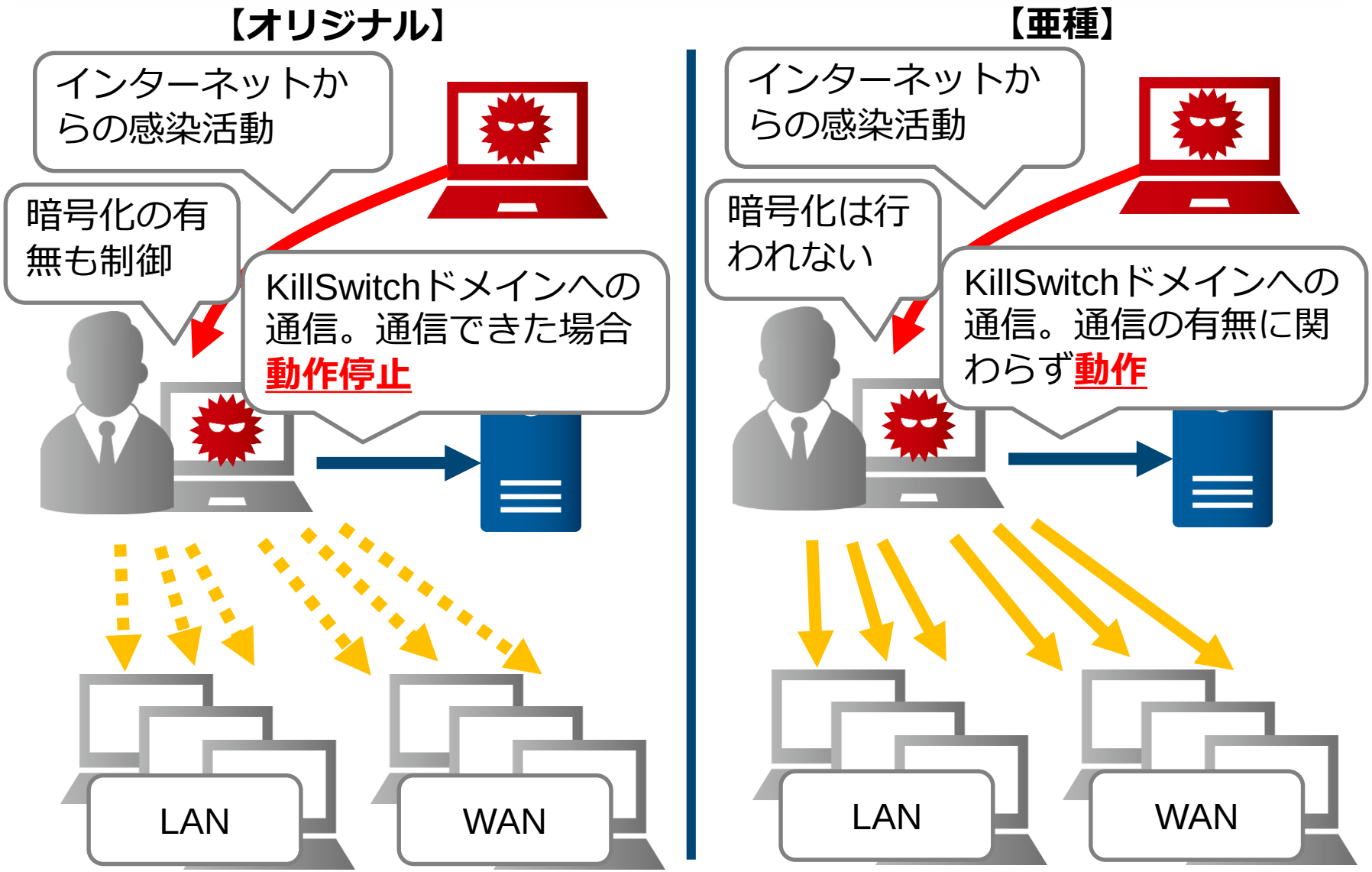
- オリジナルと違う点
  - ランサムウエアの挙動がない
  - KillSwitchによる動作の制御がない

- 同じ点
  - 内部・外部ネットワークへの感染活動を行う

起こり得る事象

- 感染に気付きづらい
- 内部・外部への感染拡大が行われる

WannaCrypt 亜種の動作



ランサムウエアの侵入経路が変わりつつある

- **従来 (2015年に日本語ランサムメッセージの表示から)**
  - メールによるばらまきや誘導
  - Web サイト改ざんからの誘導

- **最近みかけるようになってきたもの**
  - 脆弱性を悪用したワーム感染 (例: WannaCrypt)
  - Remote Desktop Protocol や RAT 経由による感染

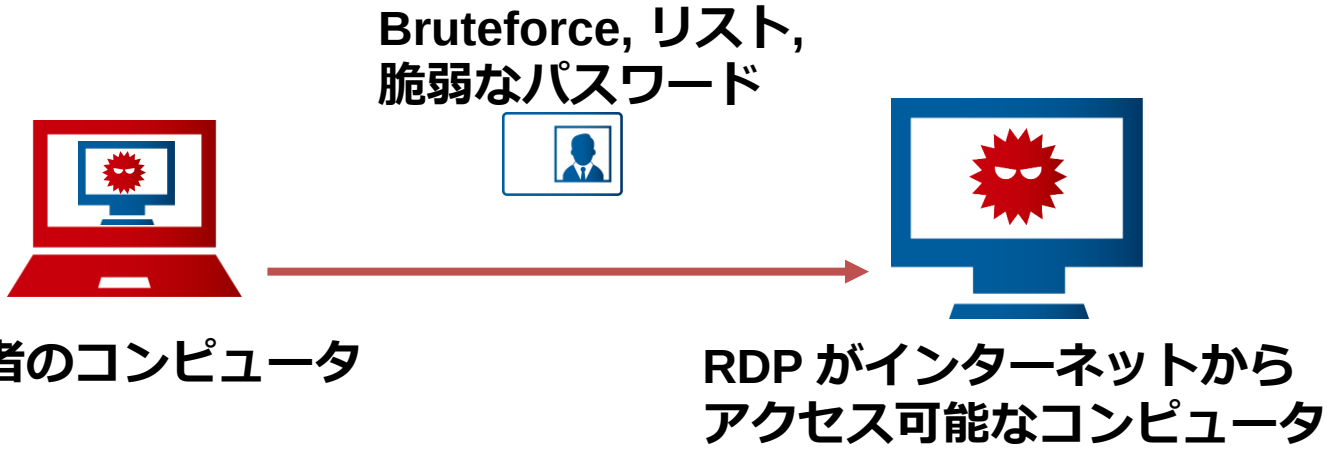
システム単独
(感染は数台レベル)

範囲の拡大
（感染がネットワークレベル）

メールや Web 閲覧に加えて、
ネットワークからの侵入にも備える必要

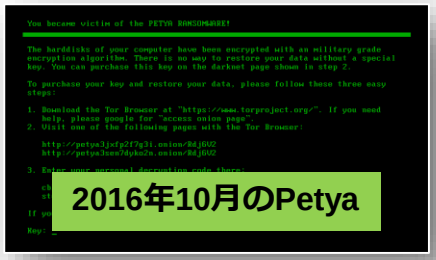
他にもあるランサムウエアの侵入経路

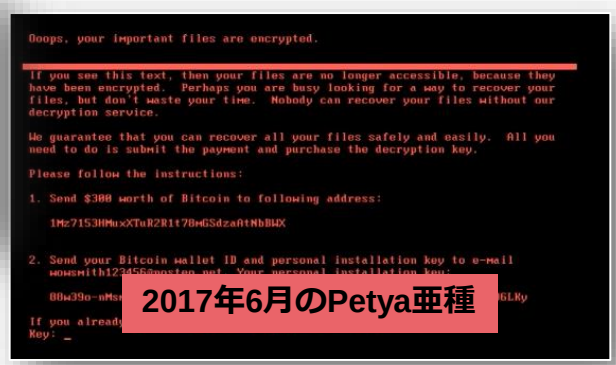
- RDP (Remote Desktop Protocol) から侵入しランサムウエアを設置するケースも観測されている

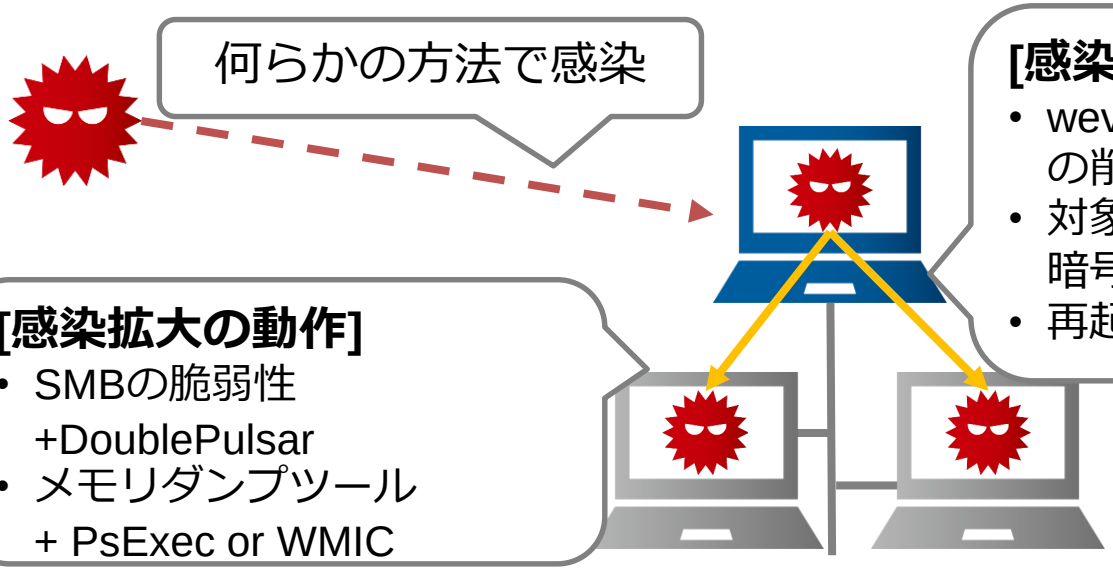


その他のランサムウエアの例 ①

- **2017年 6月、Petya 亜種がウクライナを中心に感染拡大**
- Petya 亜種
  - 特徴
    - LAN内への感染活動
    - MBRの書き換え
  - 感染経路
    - 会計ソフトウエアの更新サービスを経由し感染？

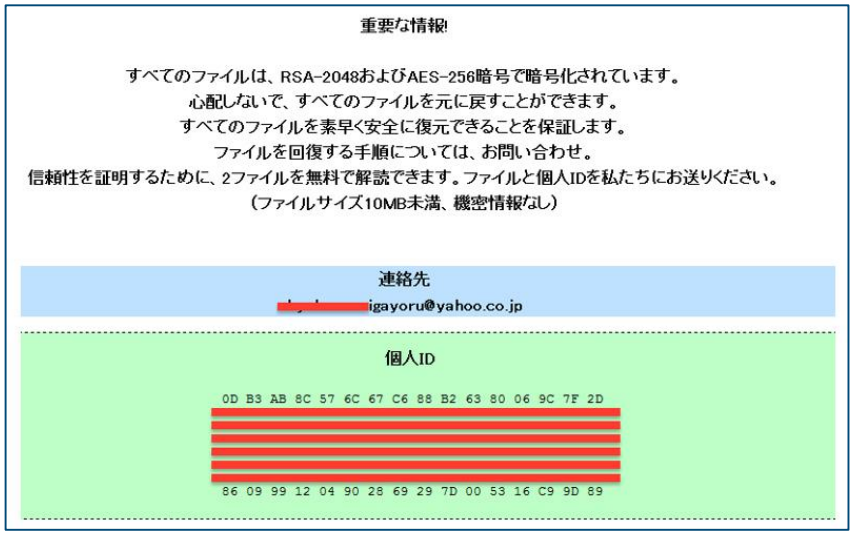






その他のランサムウエアの例 ②

- **2017年6月、国内にて “ONI” ランサムウエアによる被害が発生**



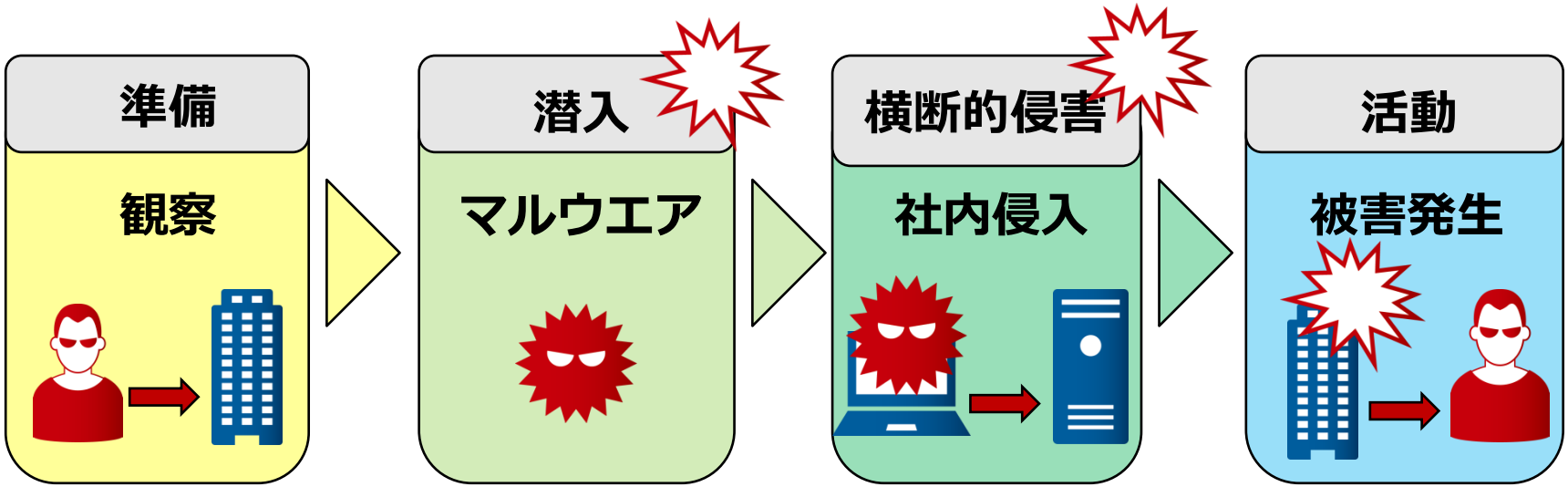
【引用元】Cylance Japan株式会社
日本をターゲットにしたGlobeImposterの亜種(”ONI”の正体)
https://www.cylance.com/ja_jp/blog/jp-oni-ransomware-globeimposter.html

- 暗号化だけでなくログが消されるなど、フォレンジックや原因調査が困難な状態に
- 組織内の複数のシステムが感染
- 背景に標的型メール攻撃、リモートからの端末操作

高度サイバー攻撃 (標的型攻撃) の流れ

攻撃は複数の段階に区分できる (サイバーキルチェーン)

- マルウエアの感染がすべてではない
- 大きな被害発生に気が付くのは最後のフェーズ



製品の脆弱性を利用した攻撃もよくみられる
① マルウエアの感染時
② 横断的侵害時の権限昇格や感染拡大

まとめ

まとめ

■ 確実に発生しているインシデント

- ✓ JPCERT/CC では、多様なサイバー攻撃を確認しています
- ✓ 毎週のように**新しい脆弱性**や**事例**が報告されています

■ 脆弱性を悪用された攻撃の被害を防ぐために

- ✓ **悪用されやすい脆弱性は、数日のうちに悪用され、しばらく悪用が続く**こともあります
- ✓ 早期のうちにアップデートが望まれます

■ 標的型攻撃は、対岸の火事ではありません

- ✓ **「ウチは狙われない」**という意識を捨てましょう
- ✓ 攻撃を防止するだけでなく、**早期検知**、**復旧**、**追跡調査**ができる準備をしておくことも大切です。

ランサムウエアへの対策

- **適切タイミングでのバックアップの取得**
  - 重要なデータについては1日一回取得を行う
  - リビジョン管理を使用する（手元のデータをマスターデータとしない）

  など

- **取得したバックアップの世代管理の実施**
  - バックアップ先も暗号化の対象となるため

  暗号化されたとき**最小限の被害**に抑える対応を行う

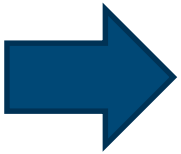
- **初動対応や範囲特定などのインシデント対応**
  - ランサムウエアの感染のみがインシデントであったのか？

  感染経路や原因を**追究できる体制やしくみ**を整える

目的に応じた情報共有のススメ

- **「目的をもった攻撃」を意識する**
  - 様々な手段を用いて達成しようとする
  - 複数の攻撃先、繰り返される攻撃
  - 内部ネットワークまで到達できれば

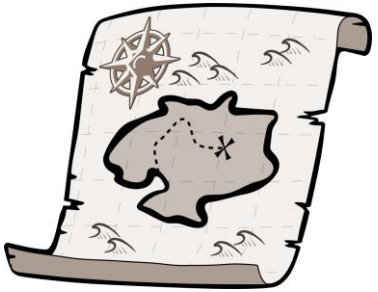
- **「見えていないもの」に気付くための手段を確保する**
  - 各組織内においてデータを保全・共有する
    ログ / インシデント対応履歴 / 対処方法
  - 他組織との間でデータを突合させる
    これって、ウチだけ？？？



「知見の集約」がキーワード
経営課題としてのセキュリティを意識

原因を探る上での情報の重要性

- **インシデントへの対応において「情報＝地図」**
  - 対応チームを効果的に動かすにも重要



- **ただし、必ずしも一つのポイントやルートのみが記されているとは限らない**
  - 原因もトラブルシュートも一つではない
  - たくさんの情報があふれている

  → **対応チームを混乱させたり、パニックを引き起こす引き金になることも**

- **どのよう「今必要な情報」をトリアージするか？が鍵**
  - 情報をどうやって活用するか？普段からの事前の備え

パニックは事態を複雑にする

- **WannaCrypt 休暇明けの5月15日での対応**
  注意喚起や報道等をきっかけとして、多くの組織で、休暇明けに対応が実施される
- **「自組織は大丈夫か？アップデートは大丈夫か？ランサムウエア感染がある？どういうことだ？」**
  - **パニックに至っていなかっただろうか？**
- **2017年6月27日、Petya 亜種への対応**
  - **様々な情報が錯そう→混乱**
- **必要以上の情報があふれることはかえって混乱を生む**
  - 災害時での情報の取扱いと同じ性格をもつ

脅威に関する情報に踊らされないようにするには？

■ 様々な情報が世の中にあふれています

- 脅威に関する様々な情報、共有される情報、レポート、商材
- **「情報」に振り回されていませんか？**

■ 情報の収集と消化をこころがけてください

- **自組織に「必要な情報」は何かを見極めることとを心がける**
- 自組織では何を守るべきか、何が強く、何が弱いかをしっかりと見極めておく

■ 信頼できる相談窓口を設けてください

- **「得た情報」から、いま何をするべきかを考えられるようにする**
- 対策の全てを自社リソースで補うことは難しい
- 「餅は餅屋」と言われる通り、専門家やベンダーなどの外部リソースを活用する
- ただし、丸投げではない自立的に判断ができる状態を維持する

CSIRTの「R」は？

- **CSIRTは事後の対応のためだけのチーム？**
  - 事前の準備を用意周到にしておくこともCSIRTの機能

- **CSIRTはマネジメントだけのセキュリティ機能？**
  - マネジメントだけではなくハンドリング
  - そのためには技術的な知見も必須（検知・分析などの監視、フォレンジック、情報収集、トリアージetc

事前（Readiness & Proactive)と事後（Response)

技術・マネジメント・運用・渉外などさまざまな知見を有する対応チームを目指しましょう（成熟度を上げ、組織文化を醸成）

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form