セキュリティインシデントから学べること

日本コンピュータセキュリティ
インシデント対応チーム協議会
運営委員長　寺田　真敏
2017年12月11日

目次

サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team（CSIRT、シーサート）体制による活動への期待が高まっています。日本シーサート協議会では、連携と問題解決の場の提供を通して、シーサート活動を支援しています。本講演では、日本シーサート協議会の活動ならびに、これまでに発生したセキュリティインシデントを題材に、セキュリティインシデントから学べることと、組織におけるシーサートの役割を一緒に考えてみたいと思います。

- セキュリティインシデントから学べること
- 日本シーサート協議会とは
- 組織におけるシーサートの役割

1 実世界との対比（感染症と病原体）

- **大規模感染マルウェア**

	約15年前（2000-2003）	現在（2017）
種類	W32/CodeRed I/II(2001年7月) W32/Nimda(2001年9月) W32/SQLSlammer(2003年1月) W32/MSBlaster(2003年8月)	WannaCry(2017年5月) NotPetya(2017年6月) Bad Rabbit(2017年10月)
機能	ワーム 感染	ワーム 感染 ランサムによるファイル暗号化 システム破壊型
対応	ワーム駆除	ワーム駆除 バックアップからのファイル復旧 システム復旧

1 実世界との対比（感染症と病原体）

- **コンピュータウイルス**
  - **自己伝搬の有無による分類**

マルウエア（Malicious Software）
＝有害な機能を持ったプログラム ≒ 広義のコンピュータウイルス

Wildlife 自分自身で増殖することが出来るプログラム

ウイルス
狭義のコンピュータウイルス
単独のファイルでは動作せず、ほかのファイルに寄生するプログラムであり、ファイル、USBやネットワークを通じて増殖するプログラム

ワーム
ネットワーク上のコンピュータからコンピュータへ自分自身を拡散させるプログラム（ウイルスと異なりワームは、ファイル、プログラムに感染しない）

ファイルに感染する　ファイルに感染しない

トロイの木馬
有益な効果を持つように見えながら、予想できない悪意のある動作を引き起こすプログラム（ウイルスのように拡散せずに、プログラムが実行された場合に悪意ある動作を引き起こす）

自己伝搬する　自己伝搬しない

1 実世界との対比（感染症と病原体）

- **感染症**
  - **感染症の予防及び感染症の患者に対する医療に関する法律（平成十年十月二日法律第百十四号）**

    - **第六条**　この法律において「感染症」とは、一類感染症、二類感染症、三類感染症、四類感染症、五類感染症、新型インフルエンザ等感染症、指定感染症及び新感染症をいう。

    - **１９**　この法律において「特定病原体等」とは、一種病原体等、二種病原体等、三種病原体等及び四種病原体等をいう。

出典：感染症の予防及び感染症の患者に対する医療に関する法律
http://law.e-gov.go.jp/htmldata/H10/H10HO114.html
感染症の範囲及び類型について
http://www.mhlw.go.jp/file/05-Shingikai-10601000-Daijinkanboukouseikagakuka-Kouseikagakuka/0000040509.pdf

1 実世界との対比（感染症と病原体）

- **感染症の類別**
  - **感染症患者の適切な治療と感染症の予防、蔓延の防止**

分類	感染性の疾病（しっぺい）	分類の考え方	既／未知
一類感染症	エボラ出血熱、クリミア・コンゴ出血熱、痘そう（とうそう）など	感染力と罹患（りかん）した場合の重篤（じゅうとく）性等に基づく総合的観点から見た危険性の程度に応じて分類	既知
二類感染症	急性灰白髄炎（きゅうせいかいはくずいえん）、結核、ジフテリアなど		
三類感染症	コレラ、細菌性赤痢など		
四類感染症	E型肝炎、A型肝炎、黄熱など	主に動物等を介してヒトに感染	
五類感染症	インフルエンザ、ウイルス性肝炎、クリプトスポリジウム症など	国民や医療関係者への情報提供が必要	
新型インフルエンザ等感染症	新型インフルエンザ 再興型インフルエンザ	新たに人から人に伝染する能力を有するインフルエンザ	未知 既知
指定感染症		一類から三類と同等の措置を必要とする既知の感染症	既知
新感染症	既に知られている感染性の疾病とその病状又は治療の結果が明らかに異なるもの	ヒトからヒトに伝染する未知の感染症	未知

1 実世界との対比（感染症と病原体）

- 病原体の分類
  - 病原体の適正な取扱いの徹底

分類	規制	分類の考え方	病原体等
一種病原体等	所持等の禁止	現在、我が国に存在していないもので、治療法が確立していない病原体。	エボラウイルス、クリミア・コンゴ出血熱、ウイルス痘そうウイルスなど
二種病原体等	所持等の許可	一種病原体等ほどの病原性は強くないが、国民の生命及び健康に重大な影響を与えるもの。	SARSコロナウイルス、炭疽菌、野兎病菌、ペスト菌、ボツリヌス菌など
三種病原体等	所持等の届出	人為的な感染症の発生を防止する観点から、届出対象として、その所持状況を常時把握する必要がある病原体等。	Q熱コクシエラ、狂犬病ウイルス、多剤耐性結核菌など
四種病原体等	基準の遵守	A型インフルエンザウイルスなど、病原体の保管・所持は可能であるが、人為的な感染症の発生を防止するため、保管等の基準の遵守を行う必要がある病原体等。	インフルエンザウイルス、新型インフルエンザ等感染症の病原体、黄熱ウイルスなど

1 実世界との対比(感染症と病原体)

- サイバー攻撃との対比
  - 感染症の類別
    - 一類感染症
    - 二類感染症
    - 三類感染症
    - 四類感染症
    - 五類感染症
    - 新型インフルエンザ等感染症
    - 指定感染症
    - 新感染症

・・・防御側
コンピュータウイルス
対策の分類

  - 病原体の分類
    - 一種病原体等
    - 二種病原体等
    - 三種病原体等
    - 四種病原体等

・・・攻撃側
コンピュータウイルスの
分類

1 実世界との対比（感染症と病原体）

● インフルエンザと感染経路の種類

分類	説明	サイバー攻撃での事例
接触感染	皮膚と粘膜・創の直接的な接触、あるいは中間に介在する環境などを介する間接的な接触による感染経路を指す。	● **USBメモリ型マルウエア**
飛沫感染	病原体を含んだ大きな粒子（５ミクロンより大きい飛沫）が飛散し、他の人の鼻や口の粘膜あるいは結膜に接触することにより発生する。飛沫は咳・くしゃみ・会話などにより生じる。飛沫は空気中を漂わず、空気中で短距離（1～2メートル以内）しか到達しない。	● **マルウエアを添付した電子メール** ● **ウェブ経由のマルウエア感染**
空気感染	病原体を含む小さな粒子（５ミクロン以下の飛沫核）が拡散され、これを吸い込むことによる感染経路を指す。医療現場においては気管内吸引や気管支鏡検査などの手技に伴い発生する。飛沫核は空気中に浮遊するため、この除去には特殊な換気（陰圧室など）とフィルターが必要になる。	● **ネットワーク型ワーム** ● **マルウエアによるDDoS（Distributed Denial of Service）攻撃**

出典：医療施設等における感染対策ガイドライン(新型インフルエンザ専門家会議)
http://www.mhlw.go.jp/bunya/kenkou/kekkaku-kansenshou04/pdf/09-07.pdf

1 実世界との対比（感染症と病原体）

● サイバー攻撃における感染経路の種類

分類	物理的接触	利用者の介入	利用する脆弱性	サイバー攻撃での事例
接触感染	必要（USBメモリの接続）	必要（USBメモリの接続）	利用者の脆弱性 プログラムの脆弱性	● **USBメモリ型マルウエア**
飛沫感染	不要	必要（電子メール添付ファイル参照、ウェブサーフィンなど）	利用者の脆弱性 プログラムの脆弱性	● **マルウエアを添付した電子メール** ● **ウェブ経由のマルウエア感染**
空気感染	不要	不要	プログラムの脆弱性設定（IDやパスワードが既定値、安易で推定可能）の脆弱性	● **ネットワーク型ワーム** ● **マルウエアによるDDoS（Distributed Denial of Service）攻撃**

目次

サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team（CSIRT、シーサート）体制による活動への期待が高まっています。日本シーサート協議会では、連携と問題解決の場の提供を通して、シーサート活動を支援しています。本講演では、日本シーサート協議会の活動ならびに、これまでに発生したセキュリティインシデントを題材に、セキュリティインシデントから学べることと、組織におけるシーサートの役割を一緒に考えてみたいと思います。

- **セキュリティインシデントから学べること**
- **日本シーサート協議会とは**
- **組織におけるシーサートの役割**

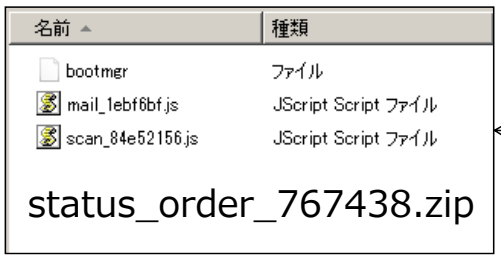
2 ランサムウエアの変遷

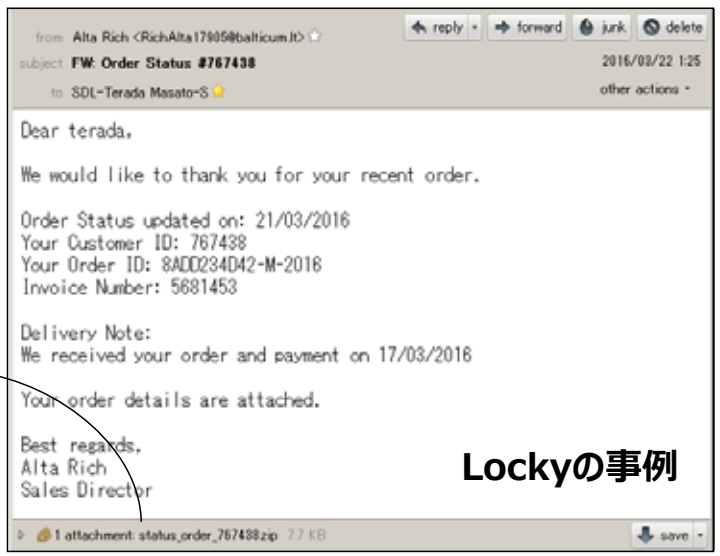
1991-2000	2001-2010	2011-2020
●**対称鍵暗号型** AIDS/PC Cyborg(1989)	●**公開鍵暗号型** Gpcode(2006) Archiveus(2006)	●**公開鍵暗号型** CryptoLocker(2013) Cryptowall(2014) CBT-Locker(2014) TeslaCrypt(2015) Locky(2016)
	●**ロック型** Winlock(2010)	●**ハードドライブ暗号型** Petya(2016)
		●**ネットワーク型ワーム** WannaCry(2017) NotPetya(2017) Bad Rabbit(2017)

ランサムウエアは、パソコン内のファイルを人質にとる不正プログラムの総称である。
特に、パソコン内のファイルを暗号化し、その暗号解除と引き換えに金銭を要求するランサムウエアは急増している。

2 ランサムウエアの変遷

- **2016年までの感染経路【飛沫感染】**
  - 電子メール本文中に記載された不正なURLにアクセスしてしまう
  - 電子メールに添付された不正なファイルを開いてしまう
  - 改ざんされた正規サイトを閲覧してしまう（不正サイトへの誘導）
    など





Lockyの事例

2 ランサムウエアの変遷

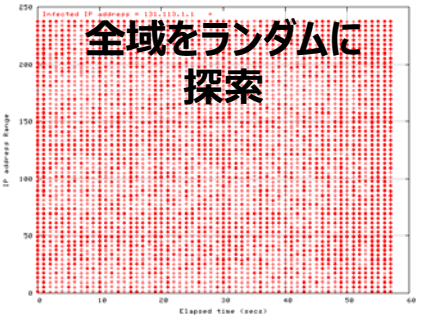
- **2017年、突然変異による感染経路拡大【空気感染】**
  - ネットワーク型ワームの機能を持ったランサムウエアWannaCry

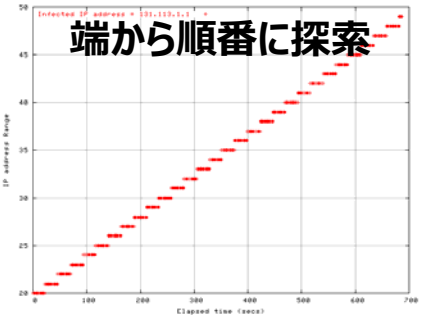
ランサムウエア WannaCryの特徴

- **拡散活動（ネットワーク型ワームの機能）**
  SMB1脆弱性（MS17-010）を利用したネットワーク経由での自己増殖
- **ランサム活動**
  ファイルを暗号化し、ファイル拡張子をWNCRYに変更
  脅迫状ダイアログを表示（復号にあたり金銭（仮想通貨ビットコイン）を要求）。

2 WannaCryインパクト（再興型への対応）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - ネットワーク型ワーム感染先探索特性



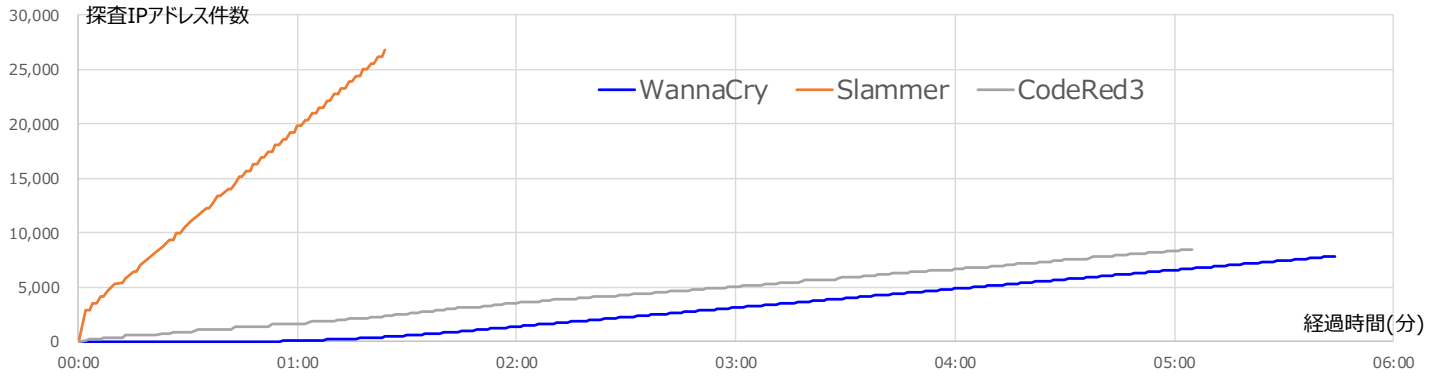


横軸：経過時間(秒)
縦軸：探索IPアドレス範囲

WannaCryの探索は、
Slammer（全域をランダムに探索）と
MSBlaster（端から順番に探索）の組合せ

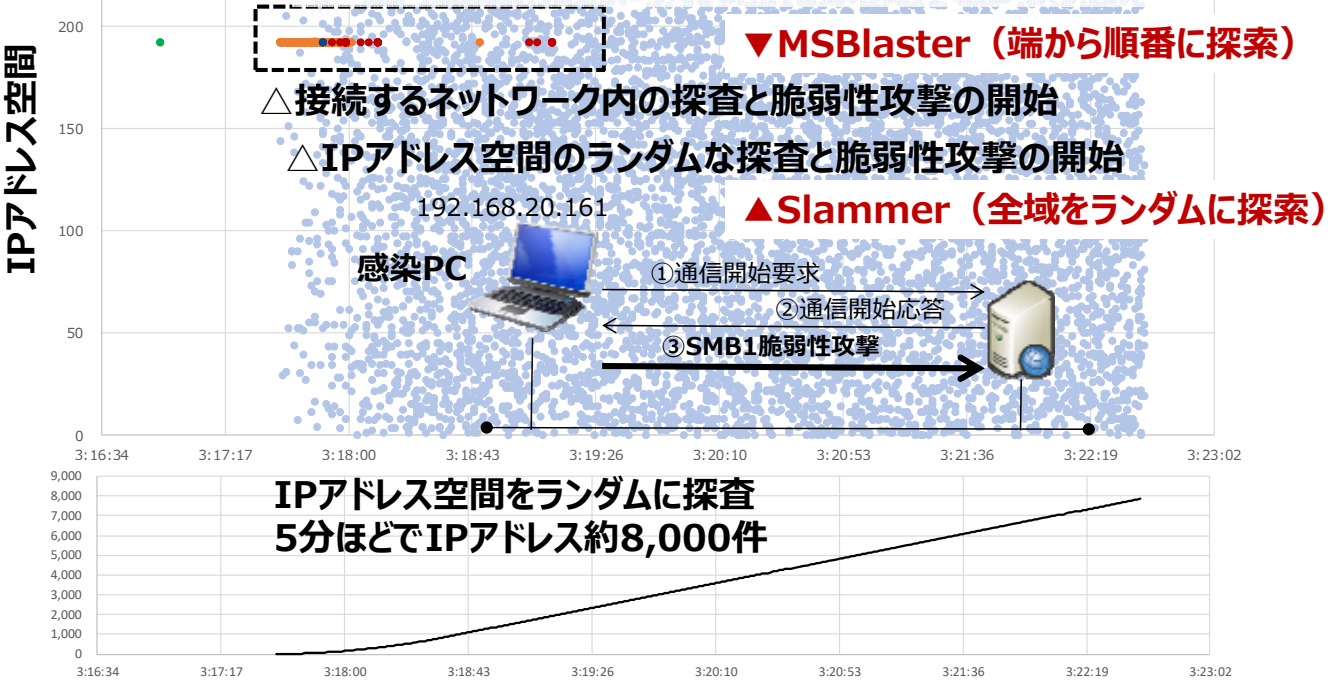
2 WannaCryインパクト（再興型への対応）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - ネットワーク型ワーム感染先探索特性
    - WannaCryの探査は、過去のワームに比べても遅いわけではないが、
    - イントラネットでの活動を想定した動作とすることで、拡散活動速度を上げている。

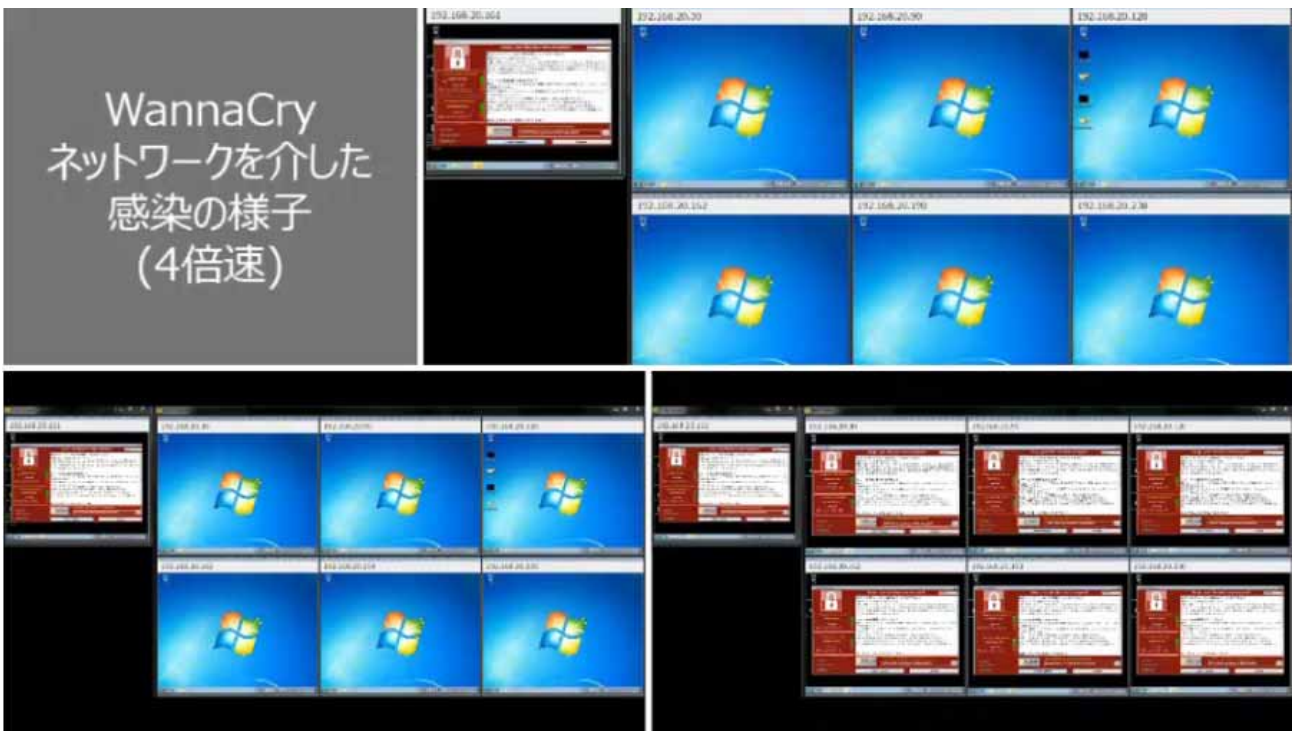


2 WannaCryインパクト（再興型への対応）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - ランサムウエアWannaCryの拡散活動（ネットワーク型ワームの機能）

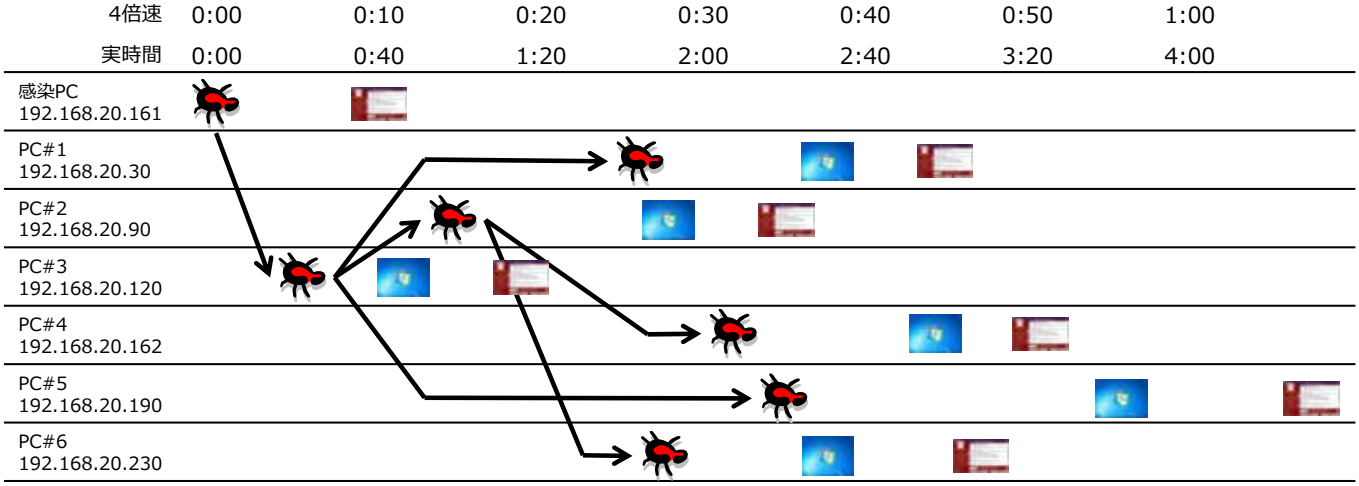


2 WannaCryインパクト（再興型への対応）



2 WannaCryインパクト（再興型への対応）

- **4倍速のMP4ファイルのムービーで、6台のPCが感染してしまうまでの時間は約1分10秒ほど、実時間にすると5分ほど**



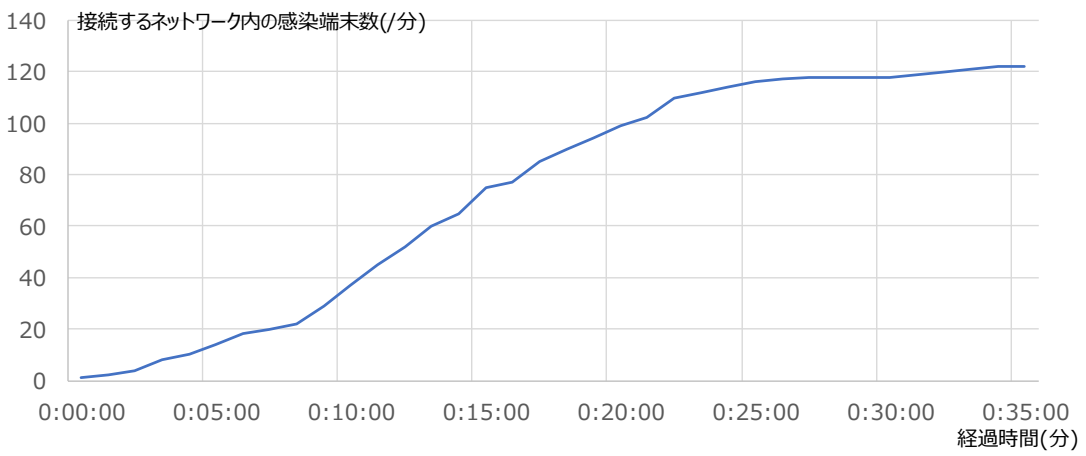
ネットワークを介して感染 (通信データを解析して得られた感染タイミング)

ネットワークを介して感染 (画面表示上、感染を確認したタイミング)

ランサム活動が発症したダイアログ表示

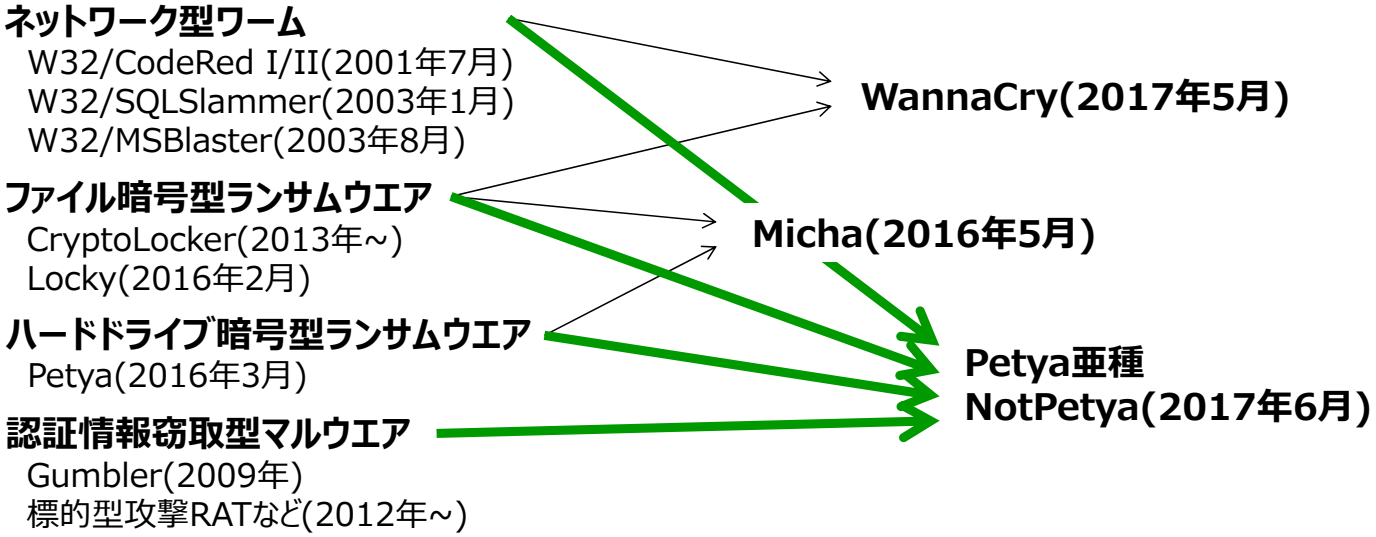
2 WannaCryインパクト（再興型への対応）

- **同一ネットワーク内に124台のPCを用意した実験では、要した時間は30分ほど**



2 NotPetyaインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - ネットワーク型ワーム**プラスアルファ**の機能を持ったランサムウエアPetya亜種

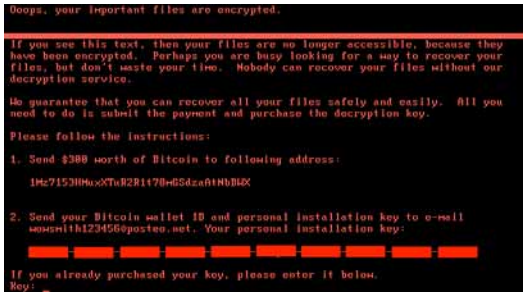


2 NotPetyaインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - ネットワーク型ワーム**プラスアルファ**の機能を持ったランサムウエアPetya亜種

ランサムウエア
NotPetyaの特徴

- **拡散活動（ネットワーク型ワームの機能）**
  SMB1脆弱性（MS17-010）を利用した自己増殖や、Windows管理ツール（PsExec、WMIC）を利用
- **ランサム活動**
  ファイルの暗号化、NTFSパーティションのMFT（Master File Table）の上書き、MBR（Master Boot Record）の改ざん



ランサムウェアという名の付いた
破壊型マルウェア

Copyright © 2017 CSIRT Association, All rights reserved.

2 NotPetyaインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - NotPetyaの探査＝潜伏活動に転用可能な検知されにくい探査

	接続するネットワーク内の探査	左記以外のネットワークの探査	自己増殖（感染）
WnnaCry	MSBlaster（端から順番に探査）方式	Slammer（全域をランダムに探索）方式	SMB1脆弱性（MS17-010）を利用
NotPetya	同上	既接続情報（現在ネットワーク接続しているIPアドレスなど）を活用	SMB1脆弱性（MS17-010）を利用 窃取した認証情報を利用

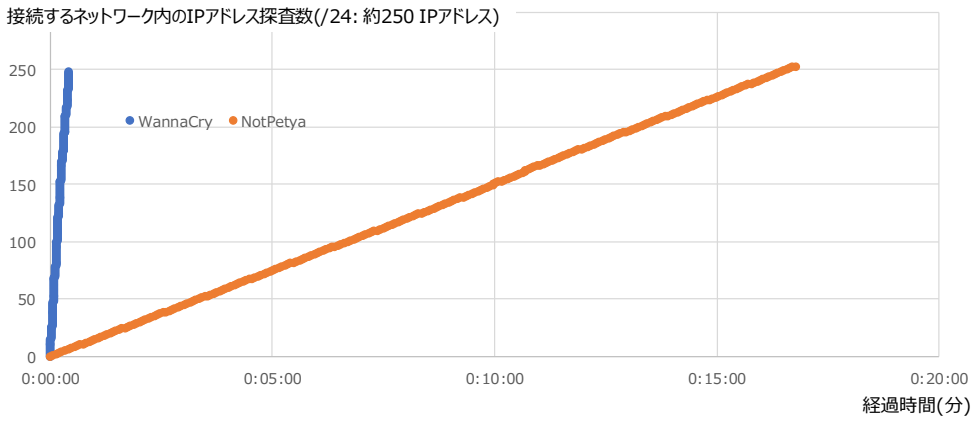
NotPetyaの探査手法≠WannaCryの探査手法

2 NotPetyaインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - NotPetyaの探査＝潜伏活動に転用可能な検知されにくい探査

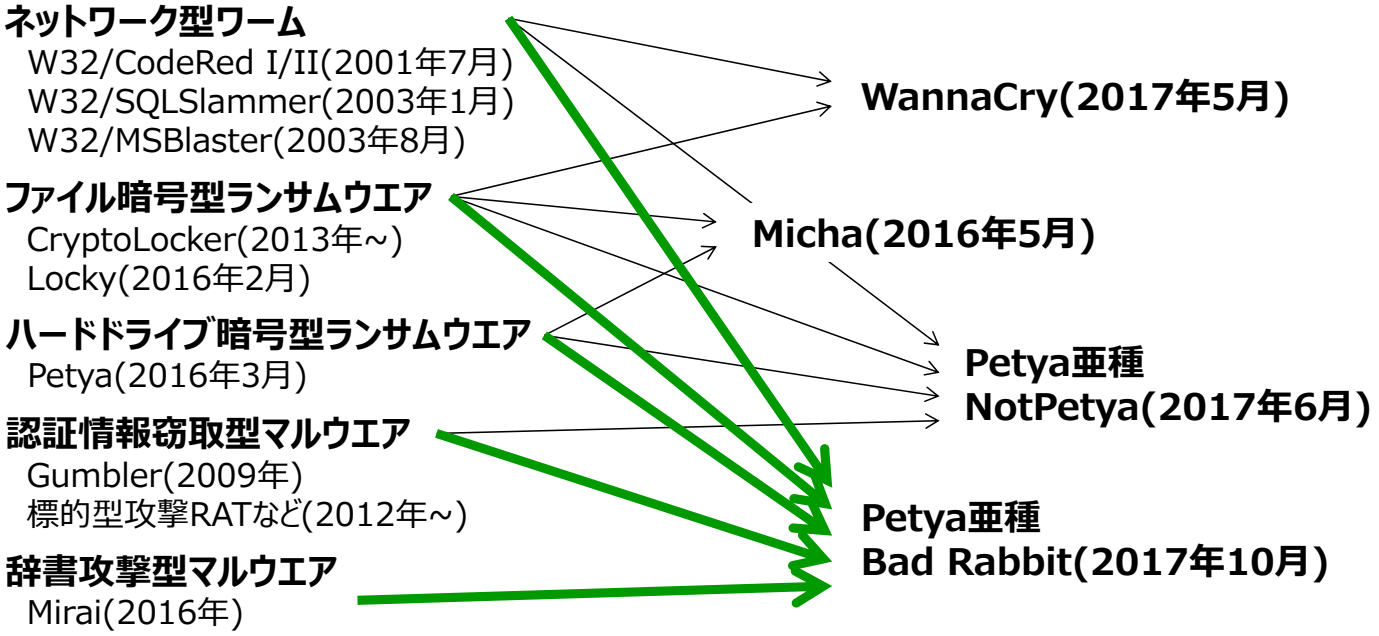
接続するネットワーク内の探査

- WannaCryと同様に、MSBlaster（端から順番に探査）方式を採用しつつも、低速度探査を実施
  探査時間（/24）：WannaCry（約30秒）、NotPetya（約15分）



2 Bad Rabbitインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - ネットワーク型ワーム**プラスアルファ**の機能を持ったランサムウエアPetya亜種

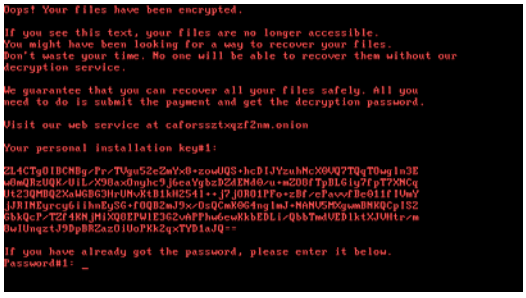


2 Bad Rabbitインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - ネットワーク型ワーム**プラスアルファ**の機能を持ったランサムウエアPetya亜種

ランサムウエアBad Rabbitの特徴

- **拡散活動(ネットワーク型ワームの機能)**
  窃取した認証情報や、ハードコーディングされたユーザ名／パスワードを用いた辞書攻撃を利用した自己増殖
- **ランサム活動**
  ファイルの暗号化、NTFSパーティションのMFT（Master File Table）の上書き



Copyright © 2017 CSIRT Association, All rights reserved.

2 Bad Rabbitインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - Bad Rabbitの探査＝潜伏活動に転用可能な検知されにくい探査

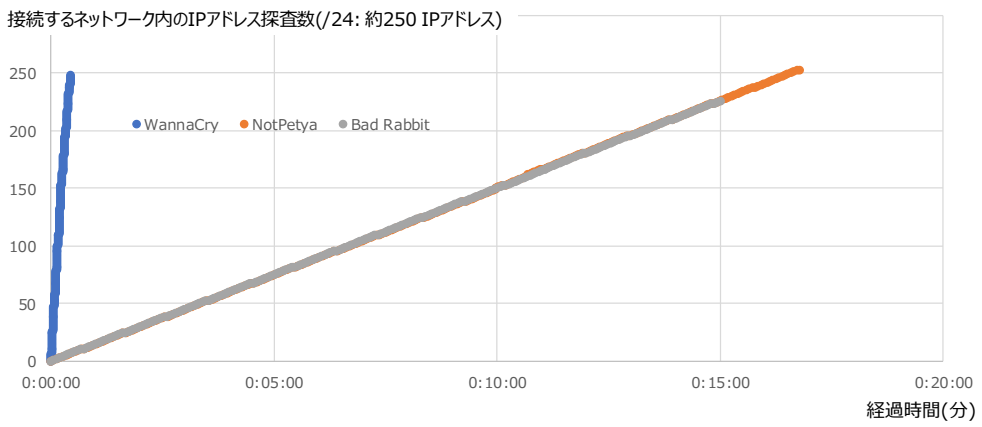
	接続するネットワーク内の探査	左記以外のネットワークの探査	自己増殖（感染）
WnnaCry	MSBlaster（端から順番に探査）方式	Slammer（全域をランダムに探索）方式	SMB1脆弱性（MS17-010）を利用
NotPetya	同上	既接続情報（現在ネットワーク接続しているIPアドレスなど）を活用	SMB1脆弱性（MS17-010）を利用 窃取した認証情報を利用
Bad Rabbit	同上	同上	窃取した認証情報を利用 辞書攻撃を利用

2 Bad Rabbitインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**
  - Bad Rabbitの探査＝潜伏活動に転用可能な検知されにくい探査

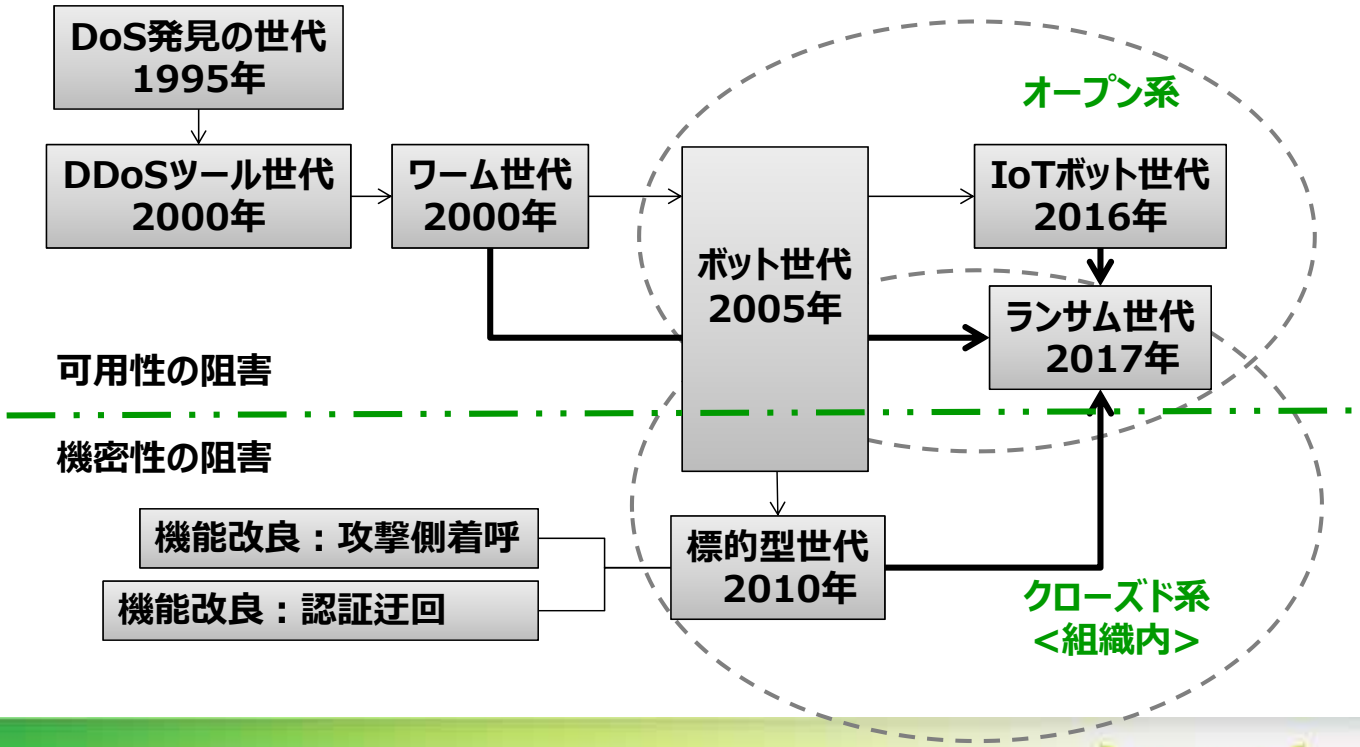
接続するネットワーク内の探査

- WannaCryと同様に、MSBlaster（端から順番に探査）方式を採用しつつも、低速度探査を実施
  探査時間（/24）：WannaCry（約30秒）、Bad Rabbit（約15分）



2 Bad Rabbitインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**



2 Bad Rabbitインパクト（潜伏型の進化）

- **2017年、突然変異による感染経路拡大【空気感染】**

  - **破壊型マルウェアへの対応**
    - バックアップからのリストアだけでなくシステム復旧検討
    - NotPetyaの他にもサービス停止や運用妨害を目的としたPDoS（Permanent Denial-of-Service）も発生
      例：BrickerBot（2017/04～）
  - **認証情報窃取への対策**
    - 個人のパスワード管理、システムやIoTで利用するパスワード管理の設計運用
  - **潜伏活動に転用可能な技術への対応**
  - **経験値の継承**
    - 継続的に進化する攻撃への追従
    - 世代交代後、10年後への経験値の継承

目次

サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team（CSIRT、シーサート）体制による活動への期待が高まっています。日本シーサート協議会では、連携と問題解決の場の提供を通して、シーサート活動を支援しています。本講演では、日本シーサート協議会の活動ならびに、これまでに発生したセキュリティインシデントを題材に、セキュリティインシデントから学べることと、組織におけるシーサートの役割を一緒に考えてみたいと思います。

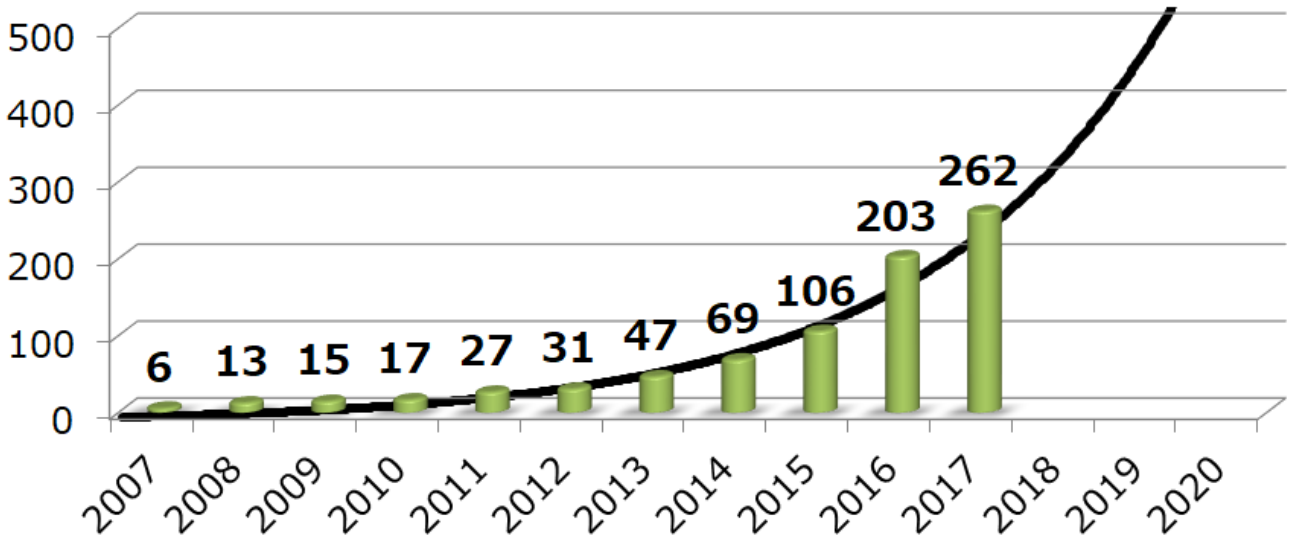
- セキュリティインシデントから学べること
- **日本シーサート協議会とは**
- 組織におけるシーサートの役割

3 日本シーサート協議会の組織概要

- **設立**
  - 2007年3月
- **名称**
  - 名称：日本コンピュータセキュリティインシデント対応チーム協議会
  - 略称：日本シーサート協議会
  - 英語名：NIPPON CSIRT ASSOCIATION
  - ウェブ： http://www.nca.gr.jp/
- **使命**
  - 本協議会の全会員による緊密な連携体制等の実現を追及することにより、会員間に共通する課題の解決を目指す
  - 社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る

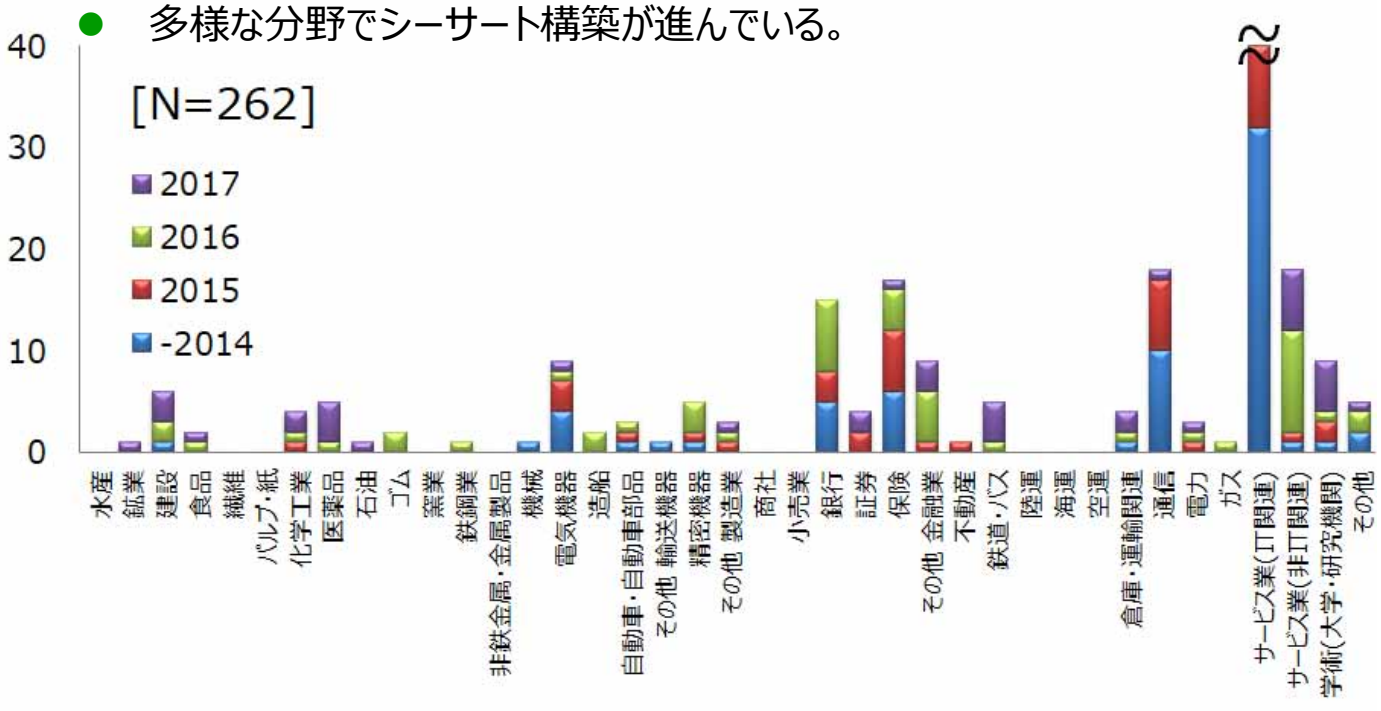
日本シーサート協議会の組織概要
～データからみた日本シーサート協議会～

- **加盟数（累積）の推移**
  - 262チーム（2017年10月31日現在）
  - 2020年には、500チームに到達する勢い



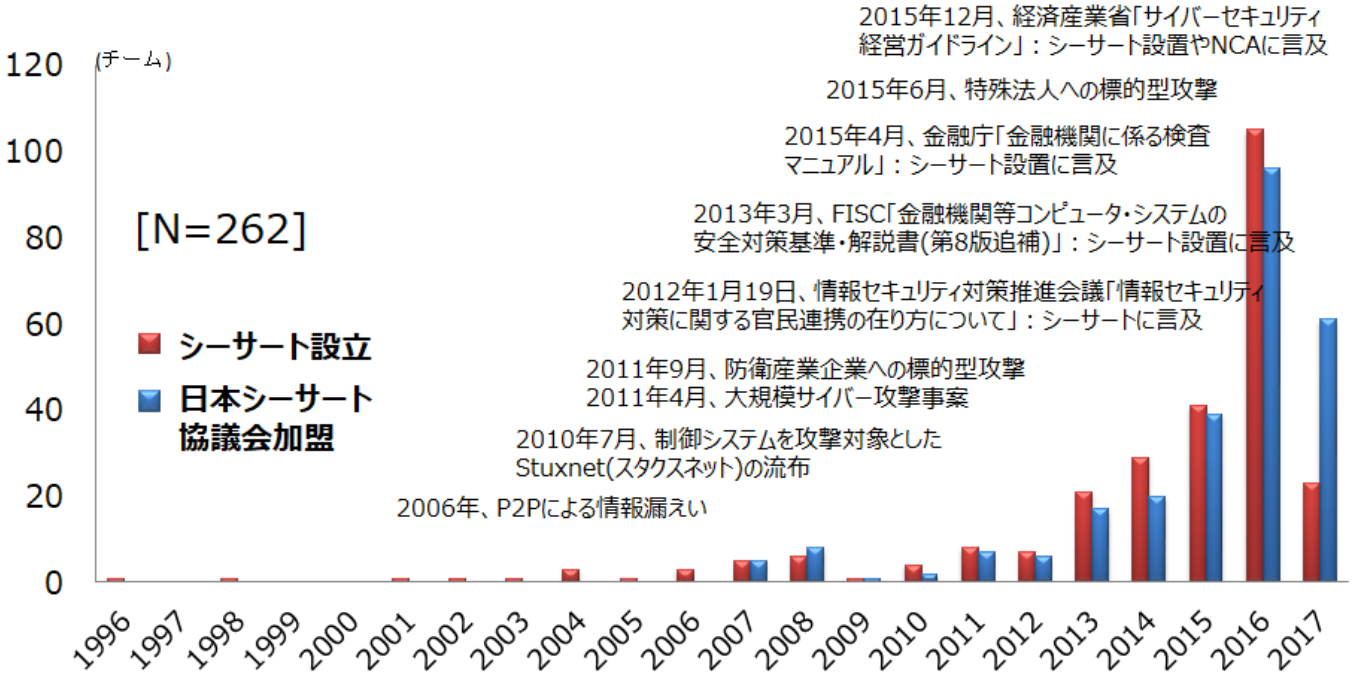
日本シーサート協議会の組織概要
～データからみた日本シーサート協議会～

- **業種による分類**
  - 多様な分野でシーサート構築が進んでいる。



3 日本シーサート協議会の組織概要
～データからみた日本シーサート協議会～

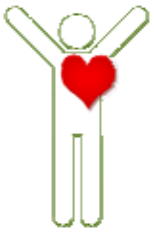
- **シーサート設立年と加盟年の推移**
  - 2013年以降、シーサート設立と加盟が急速に進んでいる。



3 日本シーサート協議会の特色

- **ボランタリーな活動**
  - 問題提起と解決のためのワーキンググループ活動
  - MLサービス、ドメイン、ウェブ運用
  - 事務局
  - 運営委員

- **マインド、モチベーションの高い仲間**



- **多様性**
  - 情報関連企業だけでなく
  - 製造（自動車、家電）
  - 金融、建設、流通　他

3 日本シーサート協議会の特色

- **日本シーサート協議会の行動指針**

正義の味方	社会貢献、トラブルをさっそうと解決する有志による無償の提供、積極的な姿勢、強制的にさせられている訳ではない、という事を端的に示す。
自由と責務	信頼関係を築くためには積極的な連携、情報提供が必要。黙って聞いているだけでは信頼は得られない。情報を提供した分だけ、信頼感があがると考えよ。
チャレンジと自己研鑽	常に自分を自己研鑽し、プロフェッショナルであること、新しい事、だれも手をつけていない事に積極的にチャレンジすべし。そして、メンバはその人を否定するのではなく、全力でフォローする事。
Open Door	協議会内、WG間で垣根を作らない事。どのメンバも参加、見学に対しては温かく迎える事。

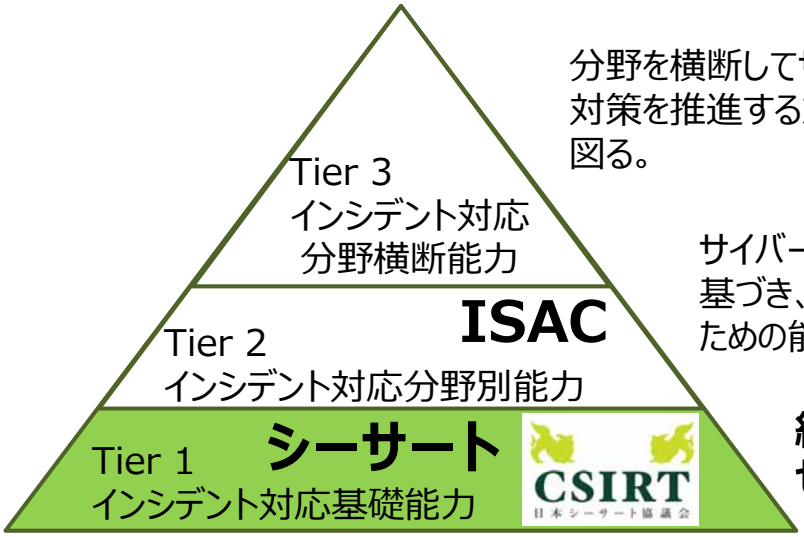
3 日本シーサート協議会の役割

- **国内のシーサートコミュニティの急速な拡大への対応**
  - **｛組織間の協力×（事前対処＋事後対処）｝に向けた場の提供**
    - 分野横断的な場の提供
    - セキュリティ業界のパイプ役
    - 地区毎で顔の見える活動の場の提供
  - **｛組織間の協力×（事前対処＋事後対処）｝に向けた場の整備**
    - アドレス帳（日本シーサート協議会加盟組織一覧）の整備
    - シーサート活動の暗黙知（慣習）の明文化
    - 地区毎で顔の見える活動の場の整備

国内のシーサートコミュニティが、いざというときに協力して活動できるための場の提供と整備

3 日本シーサート協議会の役割

- **協力して活動するための場の提供と整備**
  - **{組織間の協力×（事前対処＋事後対処）}に向けた場**
    - 組織自身が自主的に「インシデント対応基礎能力」の向上を図れる場



分野を横断してサイバーセキュリティ対策を推進するための能力向上を図る。

サイバーセキュリティ基礎能力に基づき、分野対策を推進するための能力向上を図る。

組織自身が自主的にサイバーセキュリティ基礎能力の向上を図る

目次

サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team（CSIRT、シーサート）体制による活動への期待が高まっています。日本シーサート協議会では、連携と問題解決の場の提供を通して、シーサート活動を支援しています。本講演では、日本シーサート協議会の活動ならびに、これまでに発生したセキュリティインシデントを題材に、セキュリティインシデントから学べることと、組織におけるシーサートの役割を一緒に考えてみたいと思います。

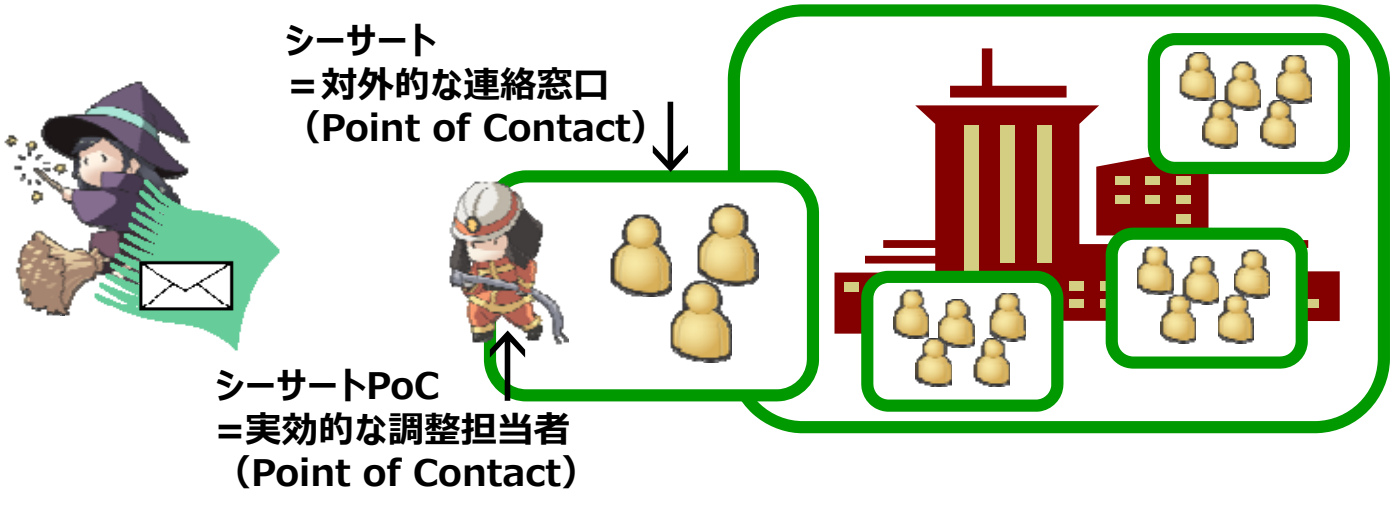
4 組織におけるシーサートの役割

- **シーサート活動から導かれる組織におけるシーサートの役割**
  - 対外的な連絡窓口であること
  - 技術的な問合せに関して対応が可能であること
  - インシデントレスポンス（事後対処）だけではなく、インシデントレスポンスなどの実践的な活動経験を元に、インシデントレディネス（事前対処）を進めていること
  - 部署間を横断した組織体制をとっていること

組織間（あるいは部署間）で情報を活用したサイバー攻撃対策を実現する仕組みの基本機能

4 対外的な連絡窓口

- **対外的な連絡窓口が明らかになっていることの利点**
  - ［通知側］ 脆弱性ハンドリングやインシデントハンドリングの通知先を探さずに済む。通知の背景説明を省略できる。通知をたらい回しにされない。
  - ［受領側］ 通知をトリガに、脆弱性ハンドリングやインシデントハンドリングをベストエフォートで動かし始めることができる。



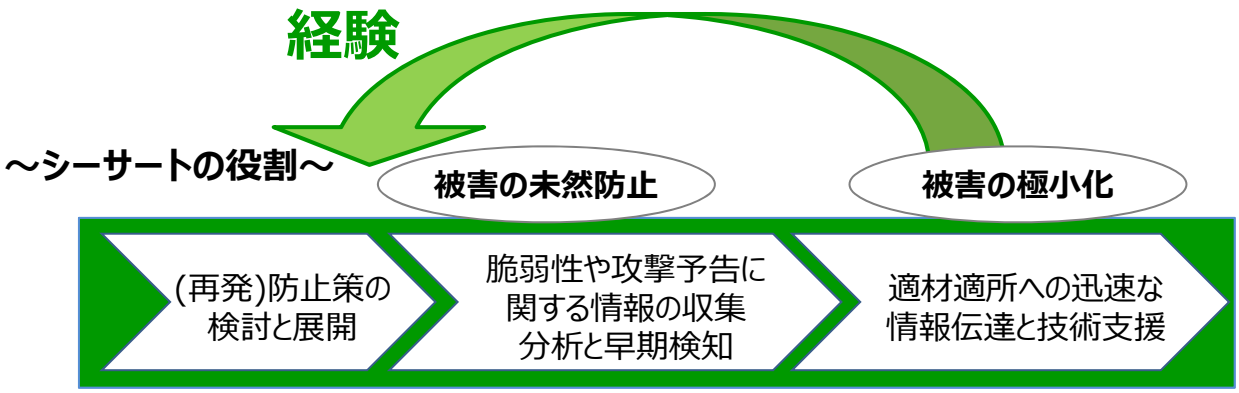
4 技術的な問合せに対応可

- **対外的な連絡窓口が、技術的な問合せに関しても対応可能であることの利点**
  - ［通知側］ 脆弱性対策やインシデント対応の技術的な通知をたらい回しにされない。
- **連絡窓口（シーサート）に期待したい要件**
  - 技術的な視点で脅威を推し量り、伝達できること
  - 技術的な調整活動ができること
  - 技術面での対外的な協力ができること

技術的な通知や依頼に対して対処してくれることを期待しているのであり、必ずしも、シーサート内に技術的な専門家が必要であるという指摘ではない。
まず重要なのは技術力ではなく、「コミュニケーション能力」

4 インシデントレディネス（事前対処）

- **インシデントレスポンス（事後対処）などの実践的な活動経験を元に、インシデントレディネス（事前対処）を進めることの重要性**



- 経験があるからこそ、「問題解決」に向けての想像力も働く。
- 経験ができないならば、他のインシデントレスポンス（事後対処）の疑似体験を通して、「問題解決」に向けての想像力を養う。

4 部署間を横断した組織体制

- **シーサート実装の多くは、専任のシーサート要員を抱えた部署を核とした部署横断型**
  - 部署間を横断した組織体制の構築、すなわち、組織内の横断的な協力体制整備への期待

サイバーセキュリティ対策の推進
特定の部署だけが頑張れば良い（お任せ）モデルから
組織全体で頑張る（連帯）モデルへ

シーサートは万能薬ではない。
組織のセキュリティ文化そのもの。

ご清聴ありがとうございました。

CSIRT同士の積極的なコミュニケーションを図ることによって、より良いセキュリティ対応を考え、そして、実現していきます。

CSIRTに関して： csirt-pr@nca.gr.jp
加盟に関して： nca-sec@nca.gr.jp

CSIRT
日本シーサート協議会

http://www.nca.gr.jp/