HITACHI
Inspire the Next

企業における
サイバー攻撃対策の再考

2012/05/25
Hitachi Incident Response Team
寺田　真敏

HITACHI
Inspire the Next

サイバー攻撃活動を振り返り、新たに見えてきた脅威や課題を、企業における、これまでの施策、これからの施策という視点から報告する。

1. APT (Advanced Persistent Threat)
2. 攻撃技術の変遷
3. 対策のアプローチ

Hitachi Incident Response Team

情報窃取を目的とした攻撃

- 2010年1月　通称、オーロラ攻撃

  グーグル、アドビ、ヤフーなど、30におよぶ企業を標的とした攻撃
  知的財産の窃取

- 2011年2月　通称、ナイトドラゴン

  ウェスタンオイル社など、石油、エネルギー、石油化学会社大手5社を標的とした攻撃
  油田やガス田の運営、入札や資金調達といった機密情報の窃取

- 2011年3月　米EMC社からのRSA SecurIDに関する情報窃取

  5月中旬、米ロッキード・マーティン社に対して、窃取された
  RSA SecurID関連情報を悪用した侵害活動が発生

- 2011年8月　通称、シャディラット攻撃

  70以上におよぶ各国の企業や政府機関を標的とした攻撃

Hitachi Incident Response Team

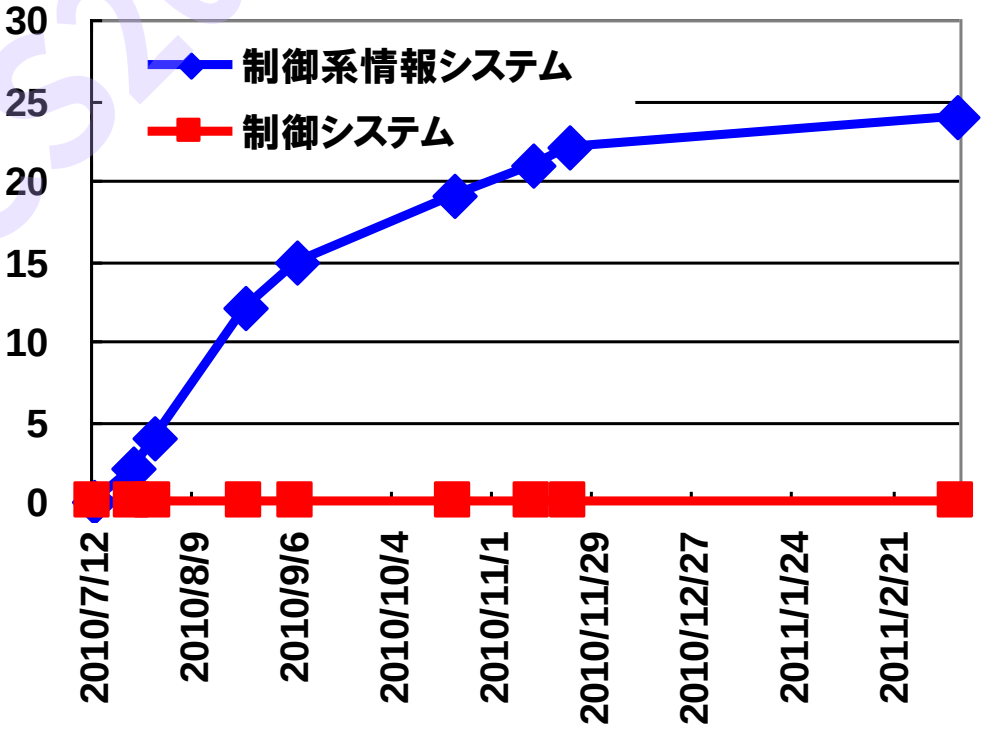
サービス停止や運用妨害を目的とした攻撃

- 2010年7月　イランの原子力施設を狙った攻撃 (スタクスネット)

  独シーメンス社製SCADAソフトウェアを通じて制御装置の動作に異常をきたすことに特化したマルウェア

2011年3月末時点で、独シーメンス社製SCADAソフトウェアのインストールされたWindowsシステムで24件の感染報告 (実被害なし)

一般のWindowsシステムでは日本を含む世界各地で数百万台規模での感染報道あり



【初出】オンライン誌Bloomberg Businessweek（2008年4月）

- An Evolving Crisis - BYZANTINE FOOTHOLD

  BYZANTINE FOOTHOLD は、2006年頃から始まった米国政府や米国軍事関連企業を標的とした攻撃活動のこと

  2007. A new form of attack, using sophisticated technology, deluges outfits from the State Dept. to Boeing. Military cyber security specialists find the "resources of a nation-state behind it" and call the type of attack an "advanced persistent threat." ・・・

【普及】 マカフィー　レポート (2010年1月)

- **重要資産の保護**

  オーロラ攻撃など、標的型サイバー攻撃からの防護方法を詳述

  APT (Advanced Persistent Threat) と呼ばれる高度でしつこい脅威は、ますます一般的な攻撃の手法となってきています。これは、権限があるシステムをターゲットとして脆弱性を利用して侵入し、目的を達成するまで攻撃をしかけ、アクセス権を奪取・保持し続ける複雑な標的型攻撃です。

Hitachi Incident Response Team

【モデル】 Exploitation Life Cycle

- MANDIANT 「M-Trends」 レポート (2010年1月)
  - 【定義】
    MANDIANT defines the APT as a group of sophisticated, determined and coordinated attackers that have been systematically compromising U.S. government and commercial computer networks for years.
  - 【モデル】
    ① Reconnaissance (偵察)
    ② Initial Intrusion into the network (侵入)
    ③ Establish a Backdoor into the network (遠隔制御)
    ④ Obtain user Credentials (権限取得)
    ⑤ Install Various utilities (インストール)
    ⑥ Privilege escalation/Lateral Movement/Data Exfiltration (実行)
    ⑦ Maintain Persistence (潜伏)

APT (Advanced Persistent Threat) のモデル化

【モデル】 Intrusion Kill Chain (Cyber Kill Chain)

- Lockheed Martin 「Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (ICIW2011)」 レポート (2011年3月)
  - 【定義】
    "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information.
  - 【モデル】
    ① Reconnaissance (偵察)
    ② Weaponization (武器化)
    ③ Delivery (配送)
    ④ Exploitation (攻撃)
    ⑤ Installation (インストール)
    ⑥ Command and Control (C2) (遠隔制御)
    ⑦ Actions on Objectives (実行)

APT (Advanced Persistent Threat) のモデル化

【モデル】 簡易モデル

- 特定組織を対象とし (標的型) 、組織内ネットワークを活動基点とした (潜伏型) 侵害活動

A	**Step1 (侵入) :ソーシャルエンジニアリングを用いた攻撃** ● 標的型メール ● 悪意あるウェブサイトへの誘導 (⇒マルウェア:Gumblar) ● USB経由 (⇒マルウェア:Conficker)	共通攻撃
P	**Step2 (潜伏) :潜伏中は外部との通信環境を維持** ● 攻撃指令管理ホストとの接続 ● 新たな機能や自身の更新のためファイルダウンロード	
T	**Step3 (窃取や妨害) :最終目標 (脅威) に合わせて変更** ● ソフトウェア構成管理システムへの攻撃 (⇒オーロラ攻撃) ● 機密情報の窃取 (⇒ナイトドラゴン、米EMC社) ● 制御システムの動作妨害 (⇒スタクスネット)	個別攻撃

攻撃技術の変遷：DDoS攻撃からAPT攻撃へ

DDoS攻撃

HIRT Hitachi Incident Response Team

攻撃指令管理と配備の体系化

発見の世代　1996年～1998年

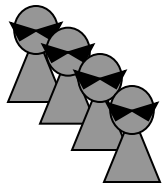
UDP Echo Flood、TCP SYN Floodなど
DoS攻撃を実現する攻撃手法の発見

攻撃者ひとり

① ツール世代・・・攻撃指令管理：階層型＋配備：手動

2000年2月　ヤフー、アマゾンなど有名サイトへの攻撃

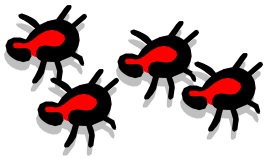
攻撃者の分身（手動）



②ワーム世代・・・攻撃指令管理：水平型＋配備：自動

2001年7月　CodeRedによるホワイトハウスへの攻撃
2004年1月　Mydoomによるマイクロソフトへの攻撃

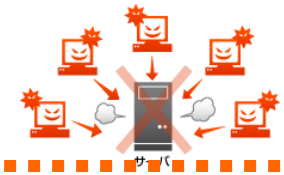
攻撃者の分身（自動）



③ボット世代・・・攻撃指令管理：階層型＋配備：自動

2007年5月　エストニアに対する攻撃
2009年7月　米国ならびに韓国政府サイトへの攻撃

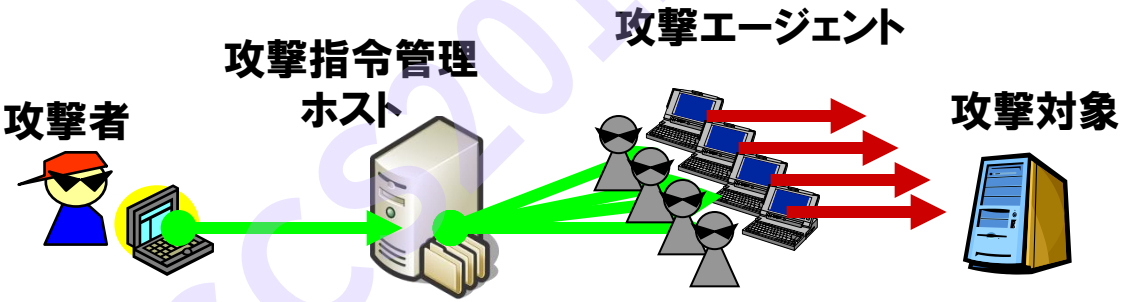
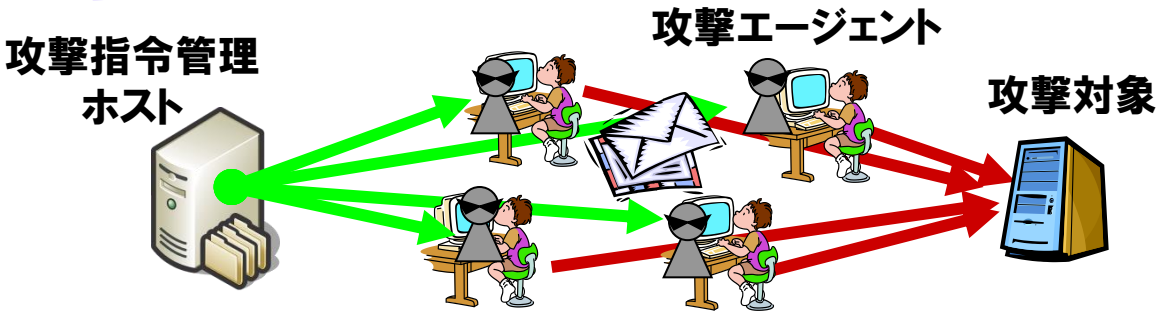
ボット（体系化）



2 攻撃技術の変遷：DDoS攻撃からAPT攻撃へ

DDoS攻撃（①ツール世代、②ワーム世代）

⇒ 攻撃指令管理技術の確立

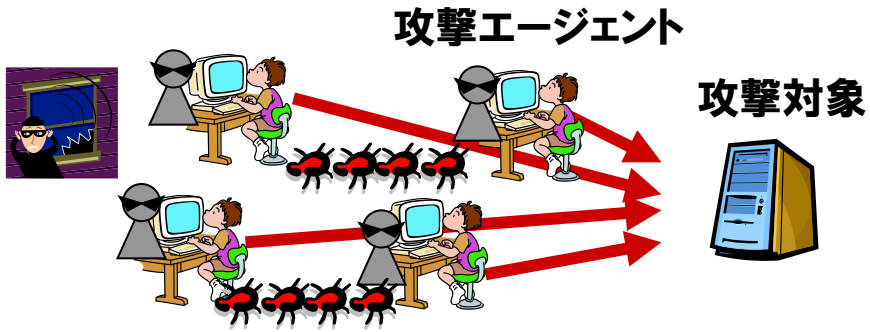
①ツール世代 Trin00 TFN TFN2K Stacheldraht 1999年	攻撃指令管理：階層型 攻撃エージェント配備：手動 
②ワーム世代 Sobig.F 2003年09月	攻撃指令管理：階層型 攻撃エージェント配備：自動（メールを利用したワーム感染技術） 

攻撃技術の変遷：DDoS攻撃からAPT攻撃へ

DDoS攻撃（①ツール世代、②ワーム世代）

Hitachi Incident Response Team

⇒ 攻撃エージェント配備技術の確立

②ワーム世代 Blaster 2003年8月	攻撃指令管理：水平型 攻撃エージェント配備：自動（脆弱性を利用したワーム感染技術） 0 2003年8月16日 
②ワーム世代 Doomjuice 2004年2月	攻撃指令管理：水平型 攻撃エージェント配備：自動（バックドアを利用したワーム感染技術） 0 2004年2月9日 

攻撃技術の変遷：DDoS攻撃からAPT攻撃へ

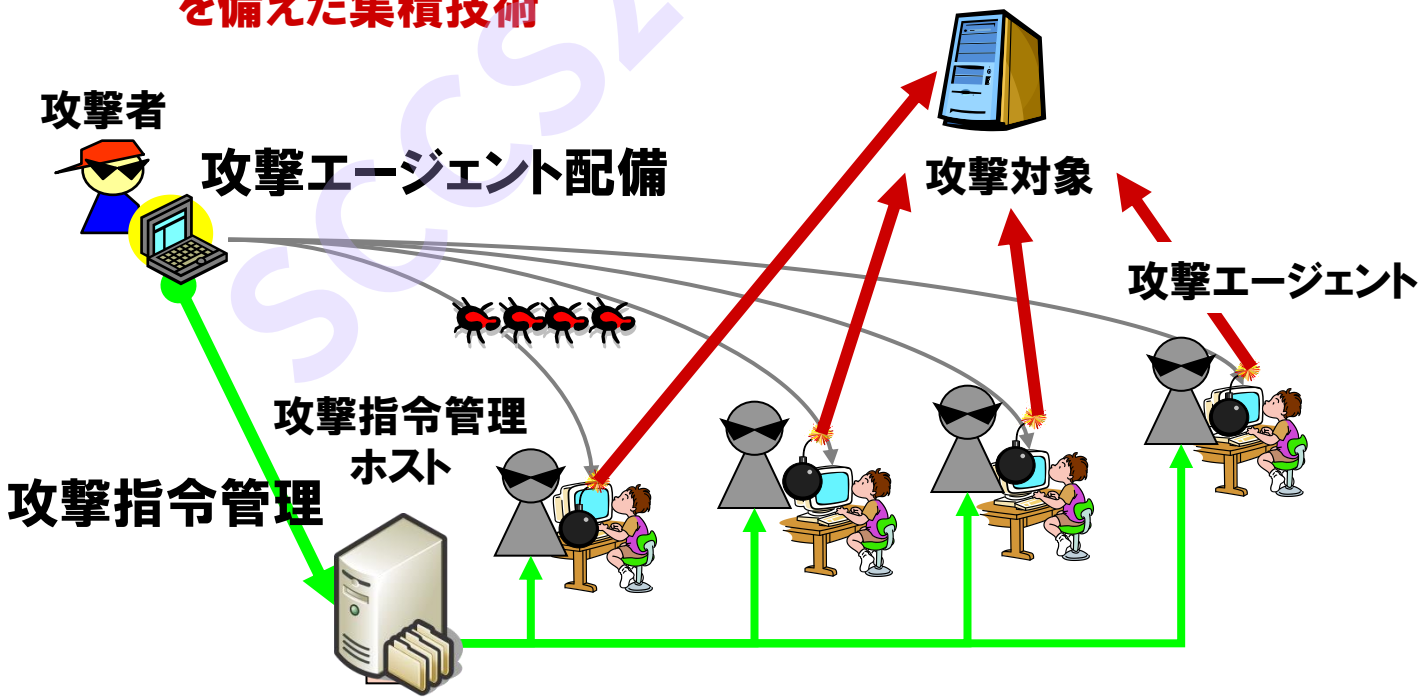
DDoS攻撃⇒③ボット世代

攻撃指令管理と配備の体系化

③ボット世代
＝①ツール世代
＋②ワーム世代

攻撃指令管理：階層型
攻撃エージェント配備：自動（脆弱性を利用したワーム感染技術）

ボットネット＝攻撃エージェント配備（分身を増やす技術）
＋攻撃指令管理（攻撃エージェントの活動を制御する技術）
を備えた集積技術



攻撃技術の変遷：DDoS攻撃からAPT攻撃へ

③ボット世代⇒④APT世代

Hitachi Incident Response Team

⇒ APT攻撃に向けた進化（1）

④APT世代	攻撃指令管理：階層型＋HTTPなどの汎用プロトコルの使用 攻撃エージェント配備：自動＋標的型メール、ウェブ感染型の使用 **組織内ネットワークを活動基点とした（潜伏型）侵害活動へ**

APT: Advanced Persistent Threat

攻撃技術の変遷：DDoS攻撃からAPT攻撃へ

④APT世代

⇒ APT攻撃に向けた進化（2）

- **遠隔操作ツール（RAT）の進化**
  侵入したシステムを遠隔から操作するためのプログラム
  潜伏活動や窃取活動で利用されている

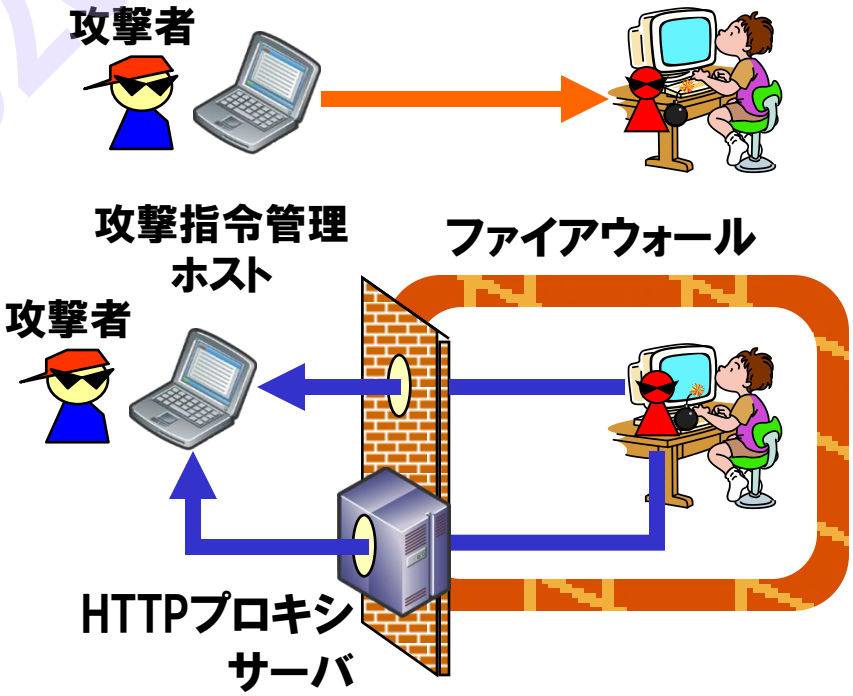
攻撃側発呼型から

- 2000年前後 BackOrifice、SubSeven など

攻撃側着呼型へ

- 2010年前後 Poison Ivy （米EMC社）
  MFC Hunter （三菱重工業）

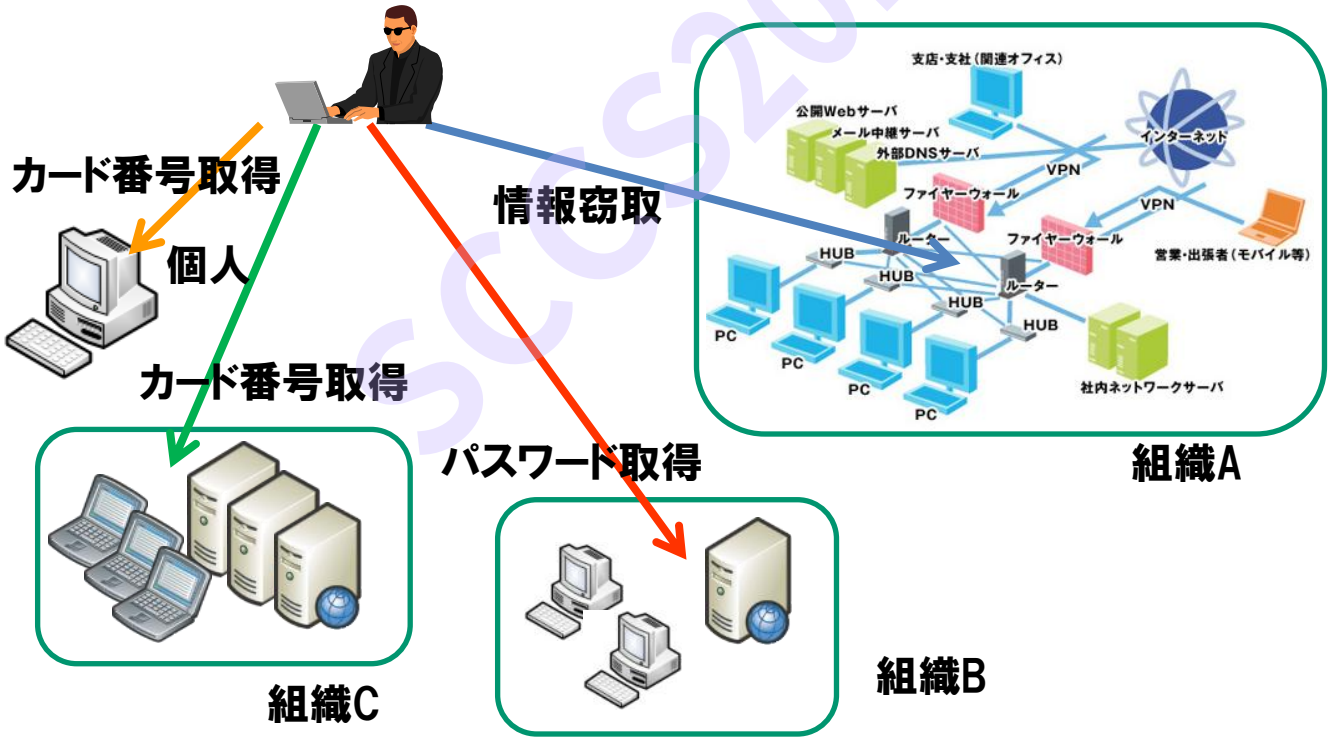
⇒潜伏中、ファイアウォールを介した
外部接続可能な通信環境を実現



RAT: Remote Access Trojan / Remote Administration Tool

単独型の標的型攻撃

- 【事例】アカウント、パスワード、カード番号などの情報収集、情報窃取、動作阻害など、個々の機器に侵入した後、用途毎のツールをインストールして遠隔操作

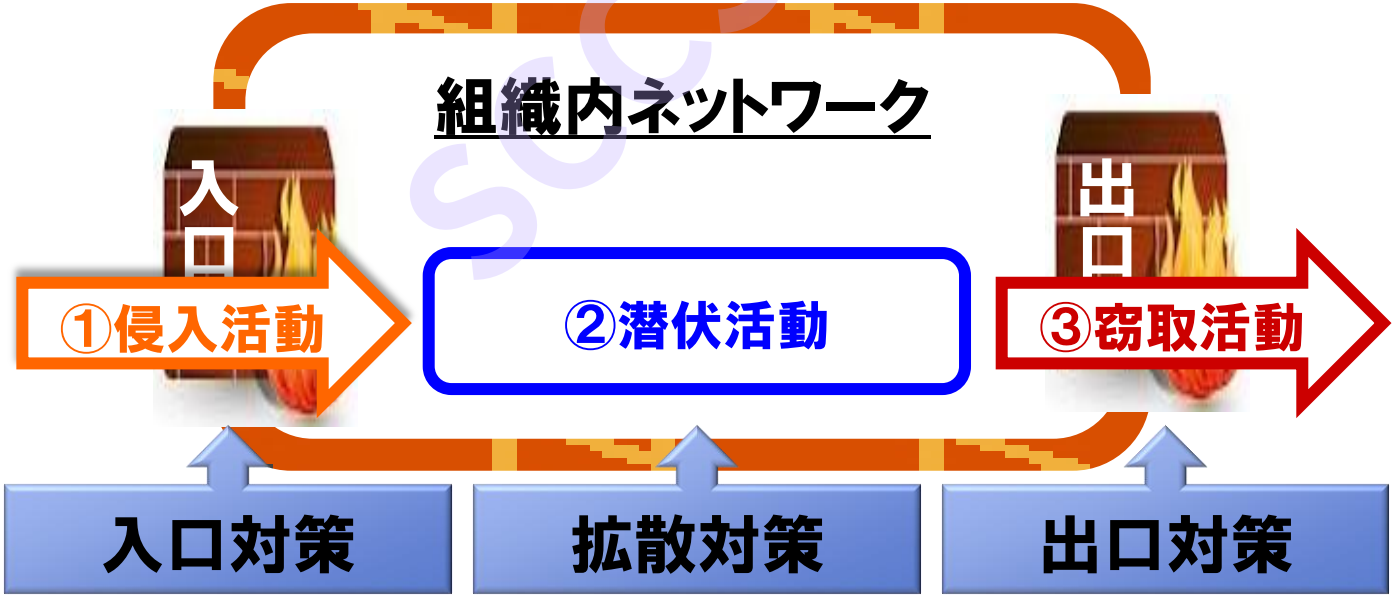


対策のアプローチ

簡易モデル

入口での侵入防止策へのてこ入れ ⇒ 多層防御

- 攻撃を防げず、侵入を許してしまう可能性は高まっている
  - ゼロディ脆弱性が狙われる
  - 様々なソフトウェアの脆弱性が狙われる
  - 次々とウイルスの亜種が出てくる等、対策ソフトで検知できない
  - 教育や啓発をしても徹底されず、不審な添付ファイルを開いたり、リンクをクリックしてしまう



対策のアプローチ

簡易モデル

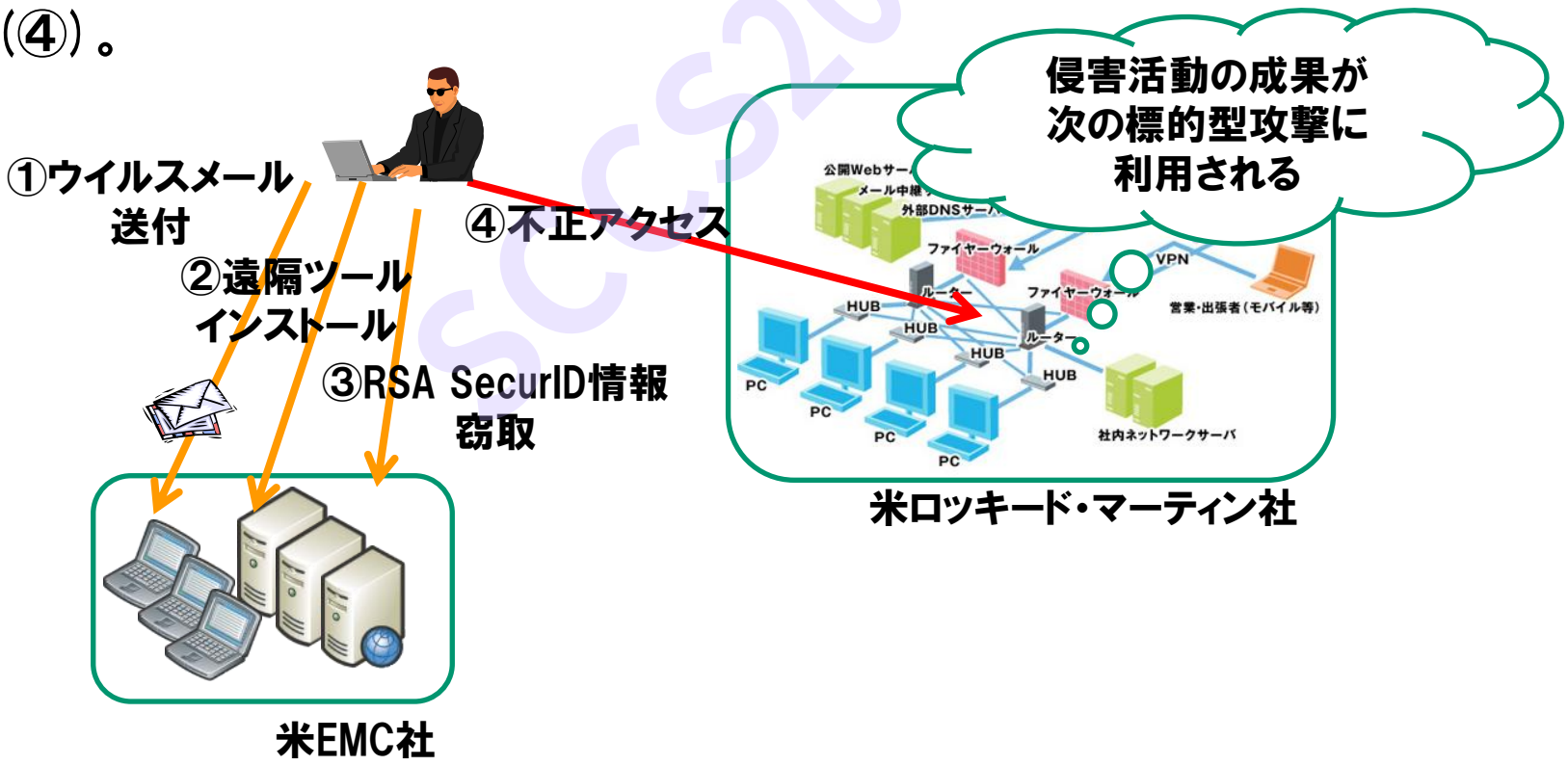
Hitachi Incident Response Team

多層防御（構成視点）の推進

	ネットワーク	メール	ウェブ	PC・サーバ他
入口対策 侵入を阻止（妨害）する施策	セキュリティポリシー／教育・啓発			
	FW／IPS・IDS	スパムフィルタ	URLフィルタ	外部メディア利用制限
	ウイルス対策ソフト			
	脆弱性診断（セキュリティホール診断・ウェブアプリケーション診断）			
	脆弱性情報の収集／セキュリティパッチの適用			
			ウェブプログラミング	
			WAF	
拡散対策 潜伏を阻止（妨害）する施策	ネットワーク設計			ユーザ認証
	通信の制限			アクセス制御、権限管理
	ログ取得・分析			プログラム認証
	通信路の暗号化			ログ取得・分析
				アクセスログ監査
出口対策 侵入されることを前提に、情報漏えいを阻止（妨害）する施策	ネットワークの監視			重要資産の隔離
	経路制御			暗号化
	プロキシ認証			コンテンツフィルタ
	コンティンジェンシープランの作成			

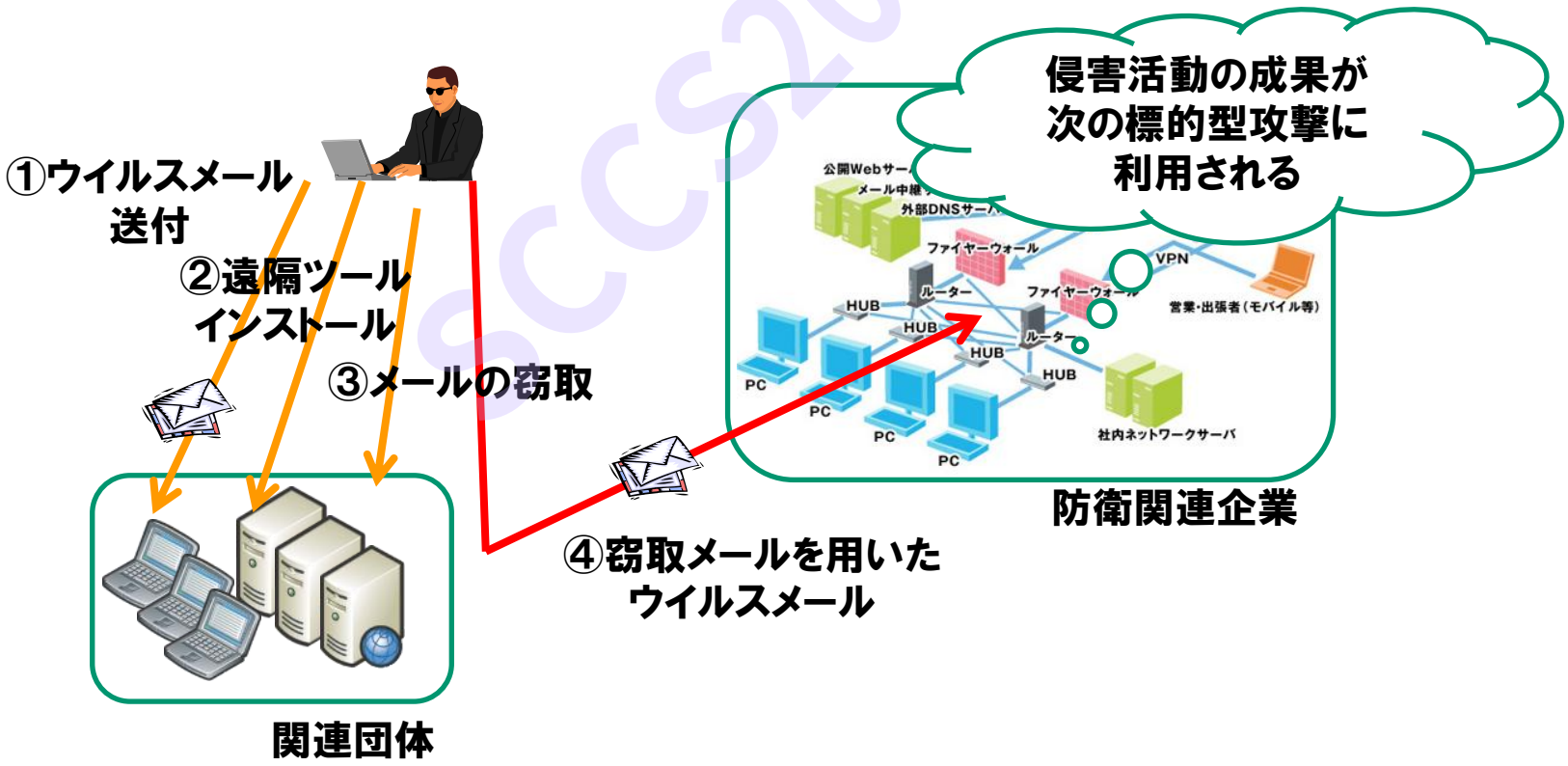
連鎖型の標的型攻撃（1）

- 【事例】2011年3月中旬、米EMC社のセキュリティ部門RSAの情報システムから二要素認証製品であるRSA SecurIDに関する情報の一部が盗まれた（①～③）。2011年5月中旬、米ロッキード・マーティン社に対して、3月に米EMC社から盗まれたRSA SecurID関連情報を悪用した不正アクセスが発生した（④）。



連鎖型の標的型攻撃（2）

- 【事例】2011年10月、関連団体のコンピュータが、情報を窃取するタイプのウイルスに感染していた（①～③）。さらに、窃取されたメールにウイルスが仕込まれ、会員企業に対する標的型攻撃メールに転用されていた（④）。



Cyber Kill Chain

- Kill Chain (F2T2EA)
  米国空軍の軍事コンセプトで、発見 (Find) ⇒ 固定 (Fix) ⇒ 照準 (Targeting) ⇒ 追跡 (Track) ⇒ 交戦 (Engage または Employ) ⇒ 査定 (Access) の6段階からなるサイクル

- Cyber Kill Chain＝Kill Chainのコンセプトをサイバー攻撃に応用
  ① Reconnaissance (偵察)
  ② Weaponization (武器化)
  ③ Delivery (配送)
  ④ Exploitation (攻撃)
  ⑤ Installation (インストール)
  ⑥ Command and Control (C2) (遠隔制御)
  ⑦ Actions on Objectives (実行)

①Reconnaissance (偵察)、②Weaponization (武器化)、③Delivery (配送)、
④Exploitation/ Installation (攻撃/インストール)、⑤Command and Control (C2) (遠隔制御)、
⑥Actions to achieve objectives (実行)、⑦Maintenance (潜伏維持) とするモデルもある。

対策のアプローチ
Cyber Kill Chain モデル

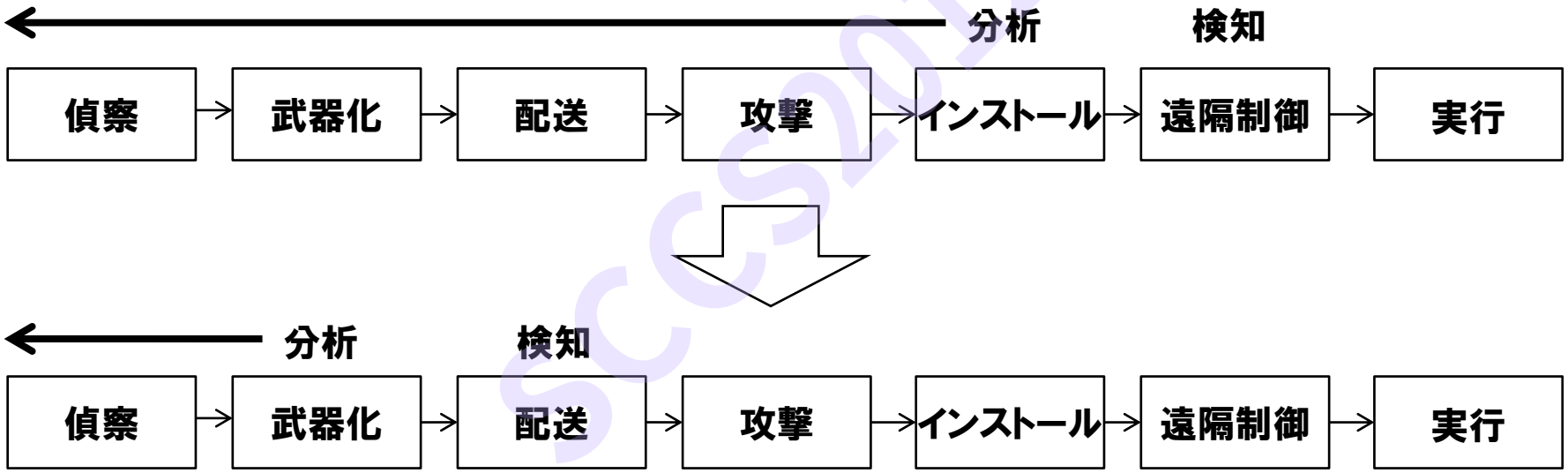
多層防御（アクション視点）の推進

	DOD Information Operations（軍事的な情報作戦）の目的					
フェーズ	検出	拒否	中断	低下	欺き	破壊
偵察	Web分析	ファイアウォールACL				
武器化	NIDS	NIPS				
配送	慎重なユーザ	プロキシフィルタ	ウイルス対策	キューイング（遅延転送）		
攻撃	HIDS	パッチ	DEP			
インストール	HIDS		ウイルス対策			
遠隔制御	NIDS	ファイアウォールACL	NIPS	Tarpit（遅延）	DNSリダイレクト	
実行	ログ監査			QoS	ハニーポット	

IOの目的には、Destroy（破壊）、Disrupt（中断）、Degrade（低下）、Deny（拒否）、Deceive（欺き）、Exploit（攻撃）、Influence（影響）、Protect（防護）、Detect（検知）、Restore（回復）、Respond（対応）がある。

Cyber Kill Chain モデルでの分析

- 初期段階での分析ならびに検知へ（入口対策の強化）
  - 攻撃観測事象（Observable）、攻撃検知事象（Indicator）の活用



- 攻撃活動分析（Campaign Analysis）
  - 攻撃者のパタン、行動、TTP（Tactics, Techniques and Procedures：戦術、技術及び手順）を明らかにする。
  - 攻撃者の意図を明らかにする。

CybOX (Cyber Observable eXpression)

- サイバー攻撃観測記述言語
  MITREが中心となり仕様策定を進めてきたもので、MandiantのOpenIOCの仕様を踏まえた、サイバー攻撃活動での観測事象を記述するためのXML仕様
- 経緯
  - 2009年9月: CAPECの延長で検討開始
  - 2010年6月: CAPEC、 MAEC、CEEとの連携検討開始
  - 2010年12月: スキーマVer0.4完成、Mandiant OpenIOCとの連携検討
  - 2011年5月: CEEとの連携、CybOXリリース
  - 2012年1月: CybOXスキーマVer0.7リリース (MAEC Ver2.0との連携)
  - 2012年4月: CybOXスキーマVer1.0リリース
- 利用例
  - 標的型攻撃メールの表記
  - ダウンロードサイトURLの表記　など

CAPEC (Common Attack Pattern Enumeration and Classification:共通攻撃パターン一覧)
MAEC (Malware Attribute Enumeration and Characterization:マルウェア特徴属性一覧)
CEE (Common Event Expression:共通イベント記述)

HITACHI
Inspire the Next

END

企業における
サイバー攻撃対策の再考