ICTイノベーションフォーラム2016
発表資料

国際連携によるサイバー攻撃の予知技術の研究開発

研究期間　平成23年度～平成27年度

KDDI(株)，(公財)九州先端科学技術研究所，(株)セキュアブレイン
(大)横浜国立大学，(株)KDDI総合研究所，ジャパンデータコム(株)

平成28年10月4日

KDDI株式会社 セキュリティ オペレーション センター
千賀　渉

目次

- 背景
- 研究開発の目的
- 研究開発の概要
- 研究開発課題と分担
- プロジェクト成果概要
- 予兆解析/早期攻撃把握からアラート導出
  - DRDOSハニーポットによるアラート
  - サンドボックスによるアラート
  - ダークネット解析によるアラート
- 攻撃情報収集と情報共有基盤の構築
  - 通信事業者データの活用・運用技術
  - 海外拠点との連携による攻撃把握と技術連携
  - 情報共有基盤の構築と実アラート提供
- 特許・論文等に関する成果
- 研究開発成果の引継・社会展開について
- まとめ

背景

- 総務省・経済産業省連携ボット対策プロジェクトであるサイバークリーンセンター（CCC)活動（2006-2010年）等により、マルウェアに関する情報を収集し、国内のマルウェア感染PCを減少させることを通じ、サイバー攻撃への脅威を低下させる試みを行ってきた。
- 一方、ガンブラー攻撃、標的型攻撃、ソーシャルネットワークにおける脅威など、サイバー攻撃の多様化も進んでいる．また、海外では依然マルウェア感染PCが多い国があり、そのような国を経由し、サイバー攻撃は国境を越えて行われるようになっている。
- これまで、事案情報・脆弱性情報の共有やスパムメール、フィッシング等、特定目的の活動団体への参加等を通じて、情報セキュリティ脅威に対する国際連携や情報共有が図られているものの、サイバー攻撃に関する観測・解析・情報共有に関しては、法制度やネットワーク環境、言語といった様々な違いがあり、迅速かつ適切な対応が行えているとはいえない。

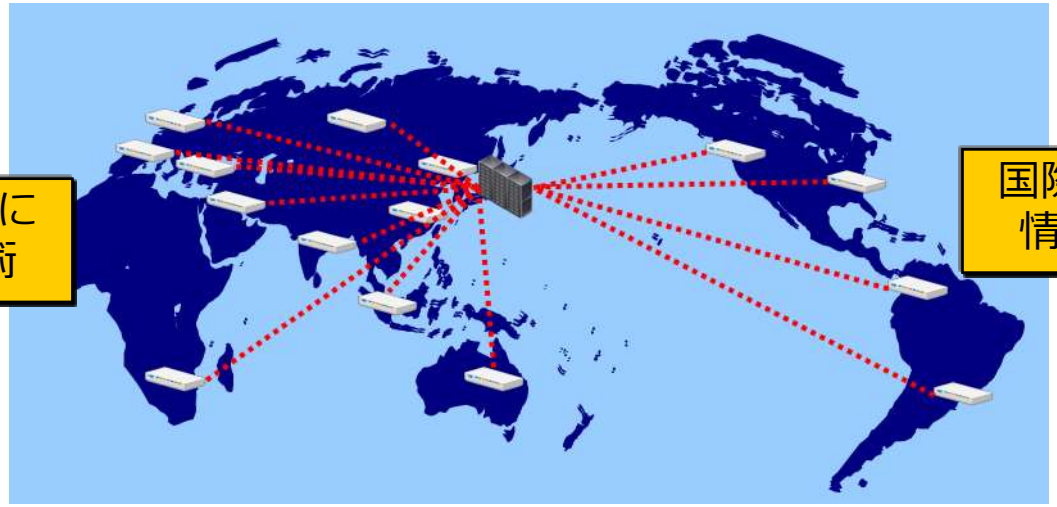
ボット等のマルウェアによる脅威、ソーシャルエンジニアリングを駆使した脅威等が深刻な問題となっており、サイバー攻撃への迅速かつ適切な対応の必要性が高まっている。

研究開発の目的

目的

サイバー攻撃に起因する脅威情報の収集ネットワークを国際的に構築し、収集した情報をISP、大学等と協力して分析することにより、サイバー攻撃の脅威を速やかに把握・捕捉する技術及び、早い段階で捕捉できるサイバー攻撃の予兆現象を実践的なセキュリティ対応に生かす技術を確立すること

国内外の多様な情報に基づく攻撃予知技術



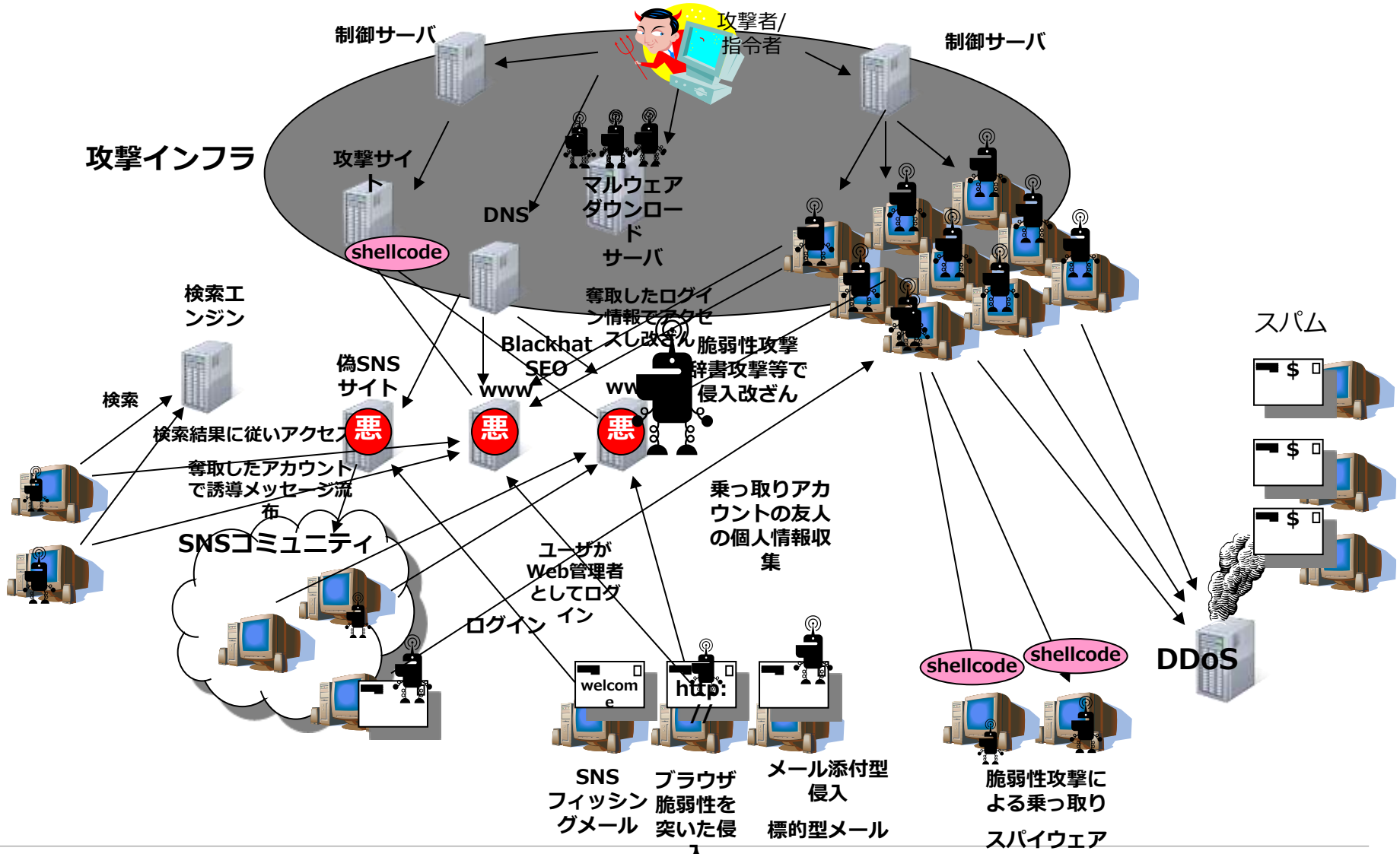
国際的なサイバー攻撃情報収集・共有技術

PRACTICE

Proactive **R**esponse **A**gainst **C**yber-attacks
Through **I**nternational **C**ollaborative **E**xchange

研究開発の概要：サイバー攻撃のための攻撃インフラ

攻撃者は様々なサイバー攻撃を効率的に実施するための「攻撃インフラ」を構築・運用



サイバー攻撃予知のための前提：

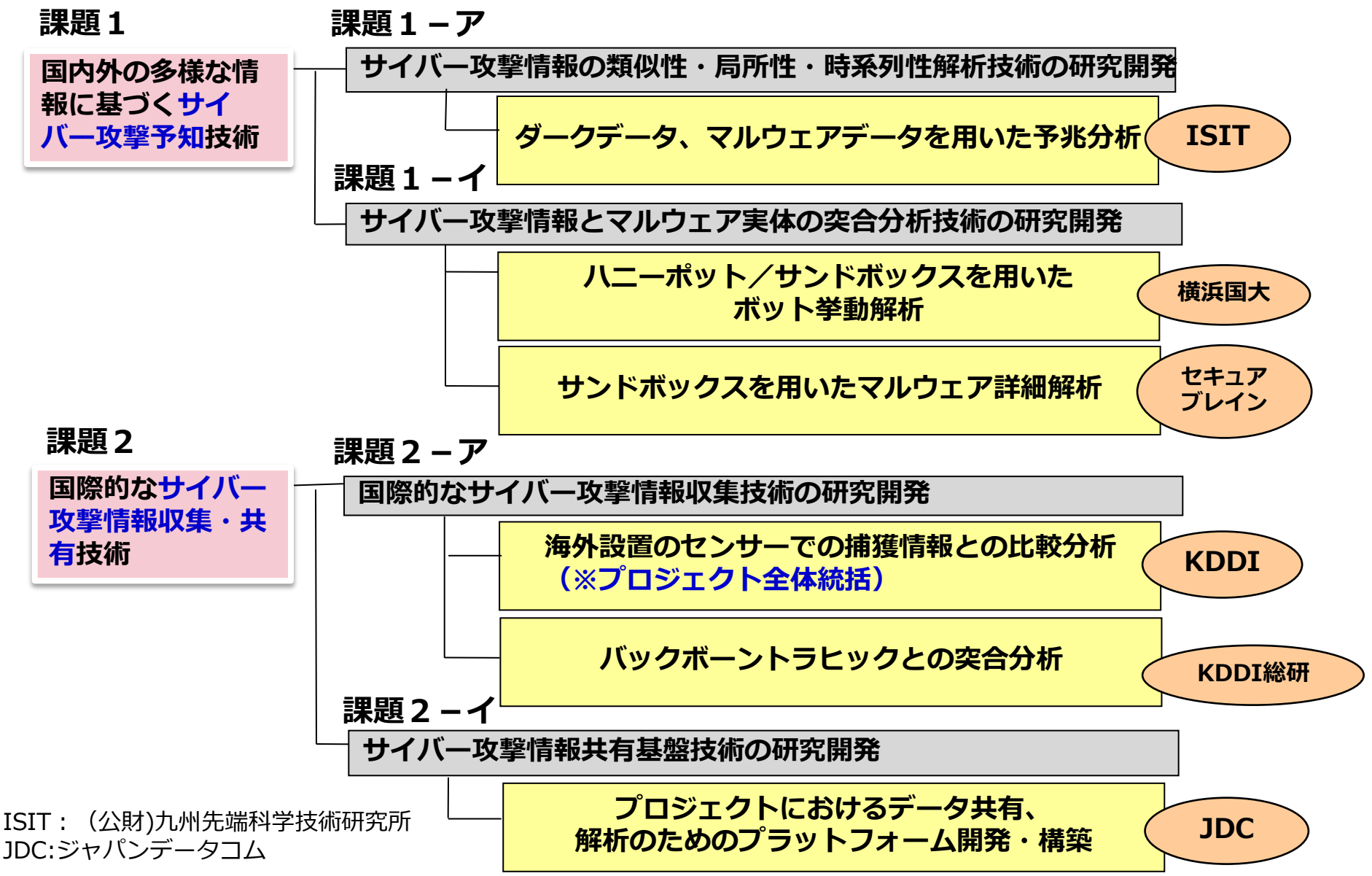
サイバー攻撃が実施される前には
ボットネットを用いた攻撃インフラにおいて
何らかの予兆(攻撃者による準備行動)が現れる

予知の基本アプローチ：

予兆把握（＝ボットネットの活動を把握する）の仕組みを構築し、早期対策に役立てる

研究開発課題と分担

2016年10月4日



ISIT：（公財)九州先端科学技術研究所
JDC:ジャパンデータコム

プロジェクト成果概要（１）

１．予兆解析/早期攻撃把握からアラート導出

- **ハニーポット技術（横浜国大）**
  世界初で開発したハニーポット技術を早期攻撃把握に活用する技術をベースに、変遷を続ける脅威に対応した研究を展開し、サイバー攻撃の実態を明らかにすると共に、ISPの運用に資する即時アラート等、実用性の高い予知・即応技術を確立。

- **サンドボックス技術（セキュアブレイン）**
  マルウエアの時間軸での挙動変化を観測できるといった利点のある長期観測用マルウェア動的解析とTaint解析を組み合わせた大規模なサンドボックス環境構築に成功し、C2, 悪性IP情報などのアラート発行を実現。

- **ダークネットデータ解析技術（ISIT）**
  調査系トラヒックが多く存在するダークネットにおいて、不要な雑音トラヒックを除去し、Morto初期挙動や韓国内の大量感染などの不正挙動をダークネットから抽出することが可能となる解析エンジン群の開発に成功。

プロジェクト成果概要（２）

2. 海外拠点との連携による攻撃情報収集と情報共有基盤の構築

- **通信事業者データの活用･運用技術（KDDI総合研究所）**
  公に観測したハニーポットなどの観測データとあわせ、通信事業者のデータをいかに活用し、実被害情報などとの突合を行うことで、アラート情報の精度・有効性の向上ができることを確認。

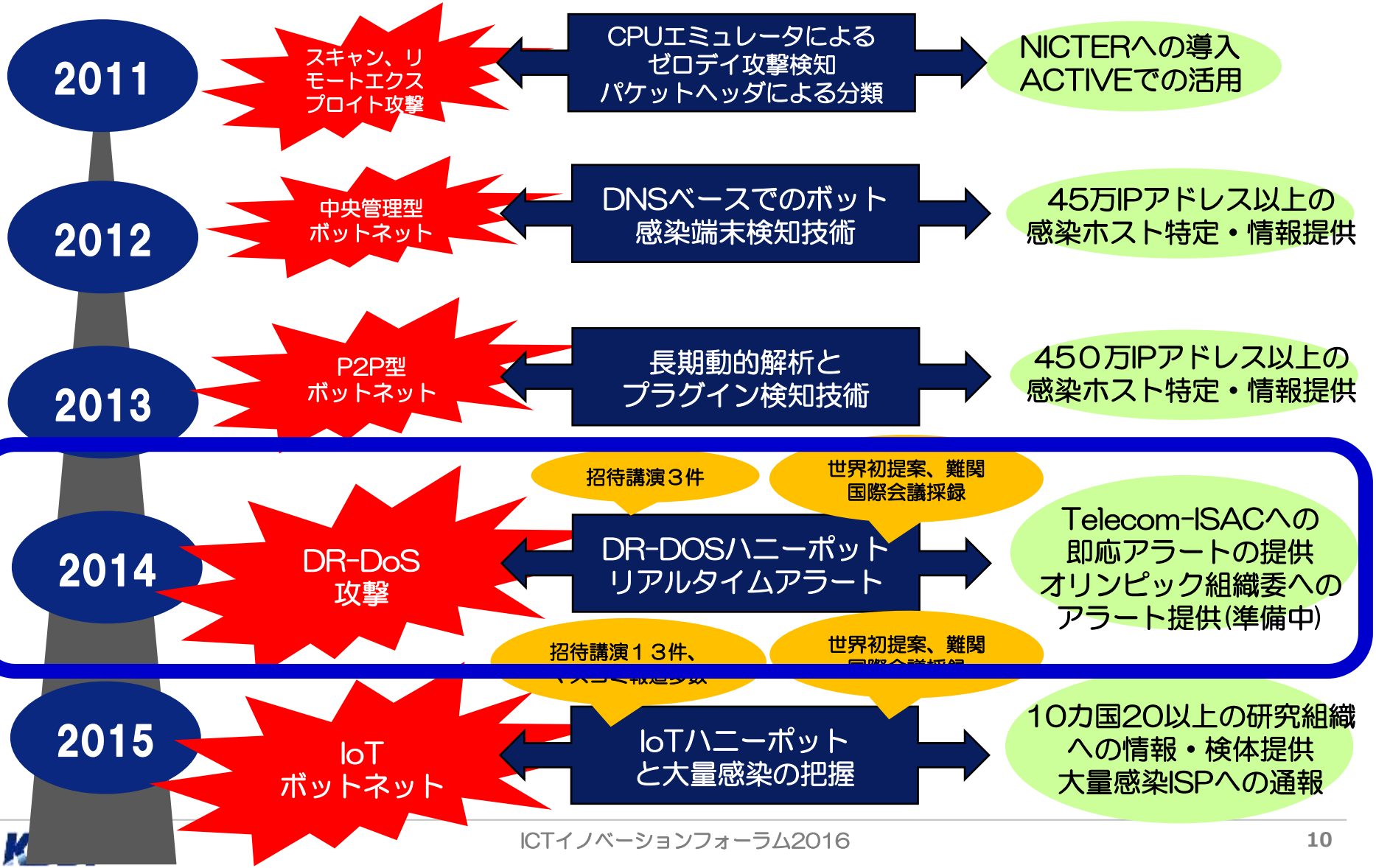
- **海外拠点との国際連携による攻撃把握と技術連携（ＫＤＤＩ）**
  海外10拠点の観測センサー設置を完了し、海外連携国から得られた観測データに基づく解析を実施した。収集したデータや解析結果を閲覧できるＷｅｂポータルを構築し、連携国との間でポータル情報を共有し、アラート情報やマルウェア感染IPなどを実時間で参照できる環境を構築。

- **情報共有基盤の構築と活用（JDC）**
  異なる関連研究機関が観測収集したデータを共有しながら分析研究を行うためのプラットフォームを構築し、機微情報の扱いも含め、連携研究のための基盤を開発。PRACTICEの解析における各種データの相関分析に貢献。

予兆解析/早期攻撃把握からアラート導出：DRDoSハニーポットによるアラート

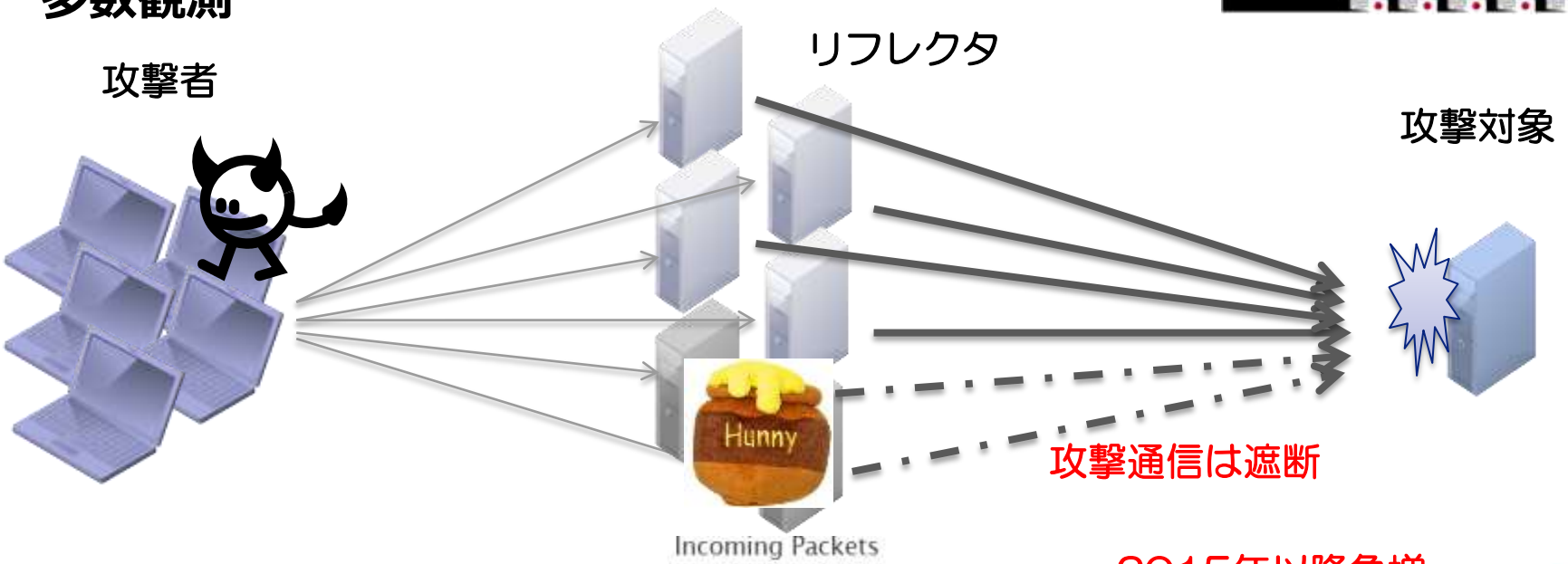
2016年10月4日

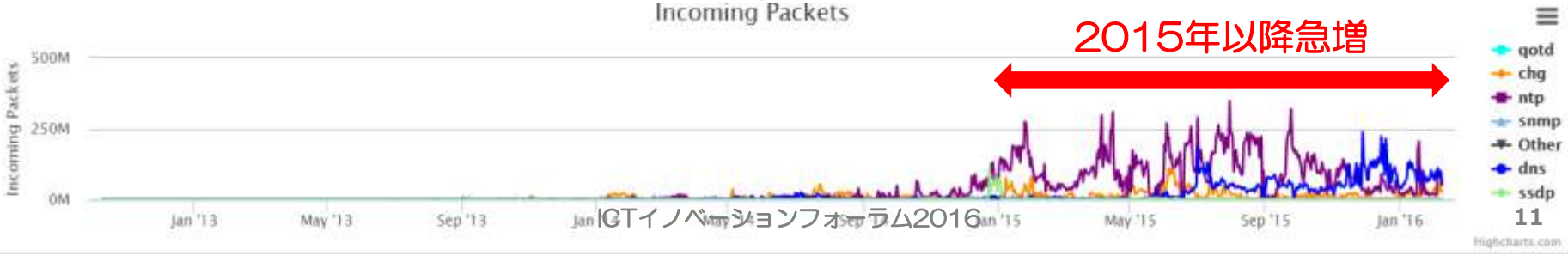
変遷を続ける脅威に対応した観測・即応技術を確立



予兆解析/早期攻撃把握からアラート導出：DRDoSハニーポットによるアラート

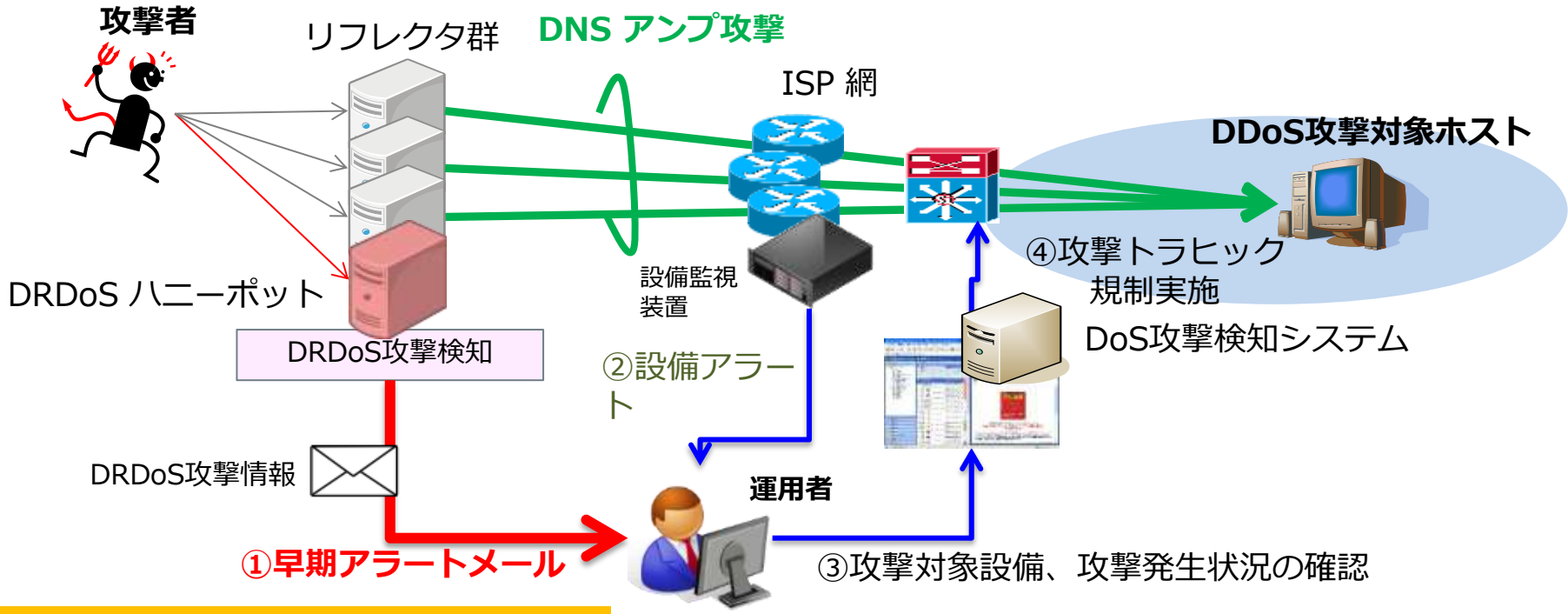
- 超大規模サービス妨害攻撃の原因である反射型サービス妨害攻撃を観測するためのハニーポット技術を世界で初めて提案
- Telecom-ISACから国内ISPに即時アラートを発行
- 中央省庁、オリンピック組織委等を狙った攻撃等を多数観測





早期警戒アラートのISPにおける活用（１）

■ DRDoSハニーポットのパラメータをISP運用の立場からチューニングを行い、既存のDoS攻撃対策システムとの連携により攻撃対応の早期化を実現した。



早期警戒アラート利活用の評価結果

大量通信に対するアラート活用の効果（2015/4/1～11/30）

1) 発生検知までの時間：設備アラート発生の約**3分前**に本アラートを運用者へ配信
2) アラート配信時の対応時間：アラート非配信時と比較してDoS攻撃対応時間が**30秒以上**短縮
3) 精度（大量通信の検知精度）：配信されたアラートの約**90%**が実際に大量通信（DoS攻撃）と合致

早期警戒アラートのISPにおける活用（２）

■ DRDoSハニーポットによるアラート例

アラートメールの例：攻撃開始通知

XXXX網宛DRDoS攻撃を観測しましたので、お知らせします。

[攻撃対象IP]
YYY.YYY.YYY.YYY

[検知時刻]
2015-ZZ-ZZ ZZ:ZZ:ZZ

[プロトコル]
NTP：port 123

[DRDoS Honeypot 詳細データ]
AS番号："AS???? XXXX"
country："Japan"
pps(最大)：2.183333333333333
pps(平均)：1.1583333333333334

[ドメイン]

(end)

アラートメールの例：攻撃終了通知

XXXX網宛DRDoS攻撃観測結果について、以下の通りお知らせします。

[攻撃対象IP]
YYY.YYY.YYY.YYY

[検知時刻/終了時刻]
2015-ZZ-ZZ ZZ:ZZ:ZZ/2015-ZZ-ZZ zz:zz:zz

[プロトコル]
NTP：port 123

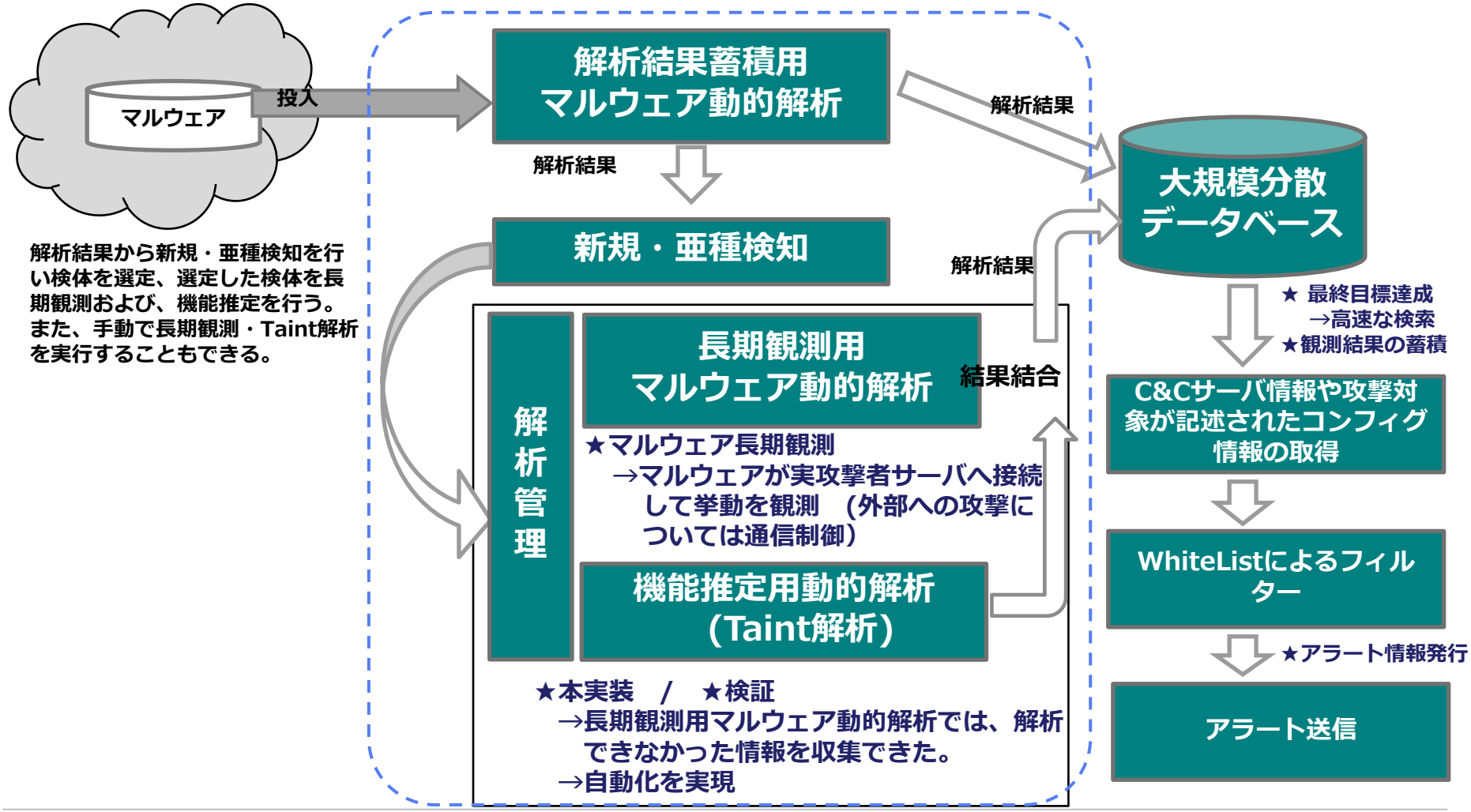
[DRDoS Honeypot 詳細データ]
AS番号："AS???? XXXX"
country："Japan"
pps(最大)：71.68333333333334
pps(平均)：58.96875
総パケット数：28305

[ドメイン]

(end)

予兆解析/早期攻撃把握からアラート導出：サンドボックスによるアラート

■ 以下のサンドボックスに関連するすべてのサブシステムの実装を完了し、120実検体（マルウェア）を並行観測し、マルウェア挙動に関する多くのアラートを導出した。

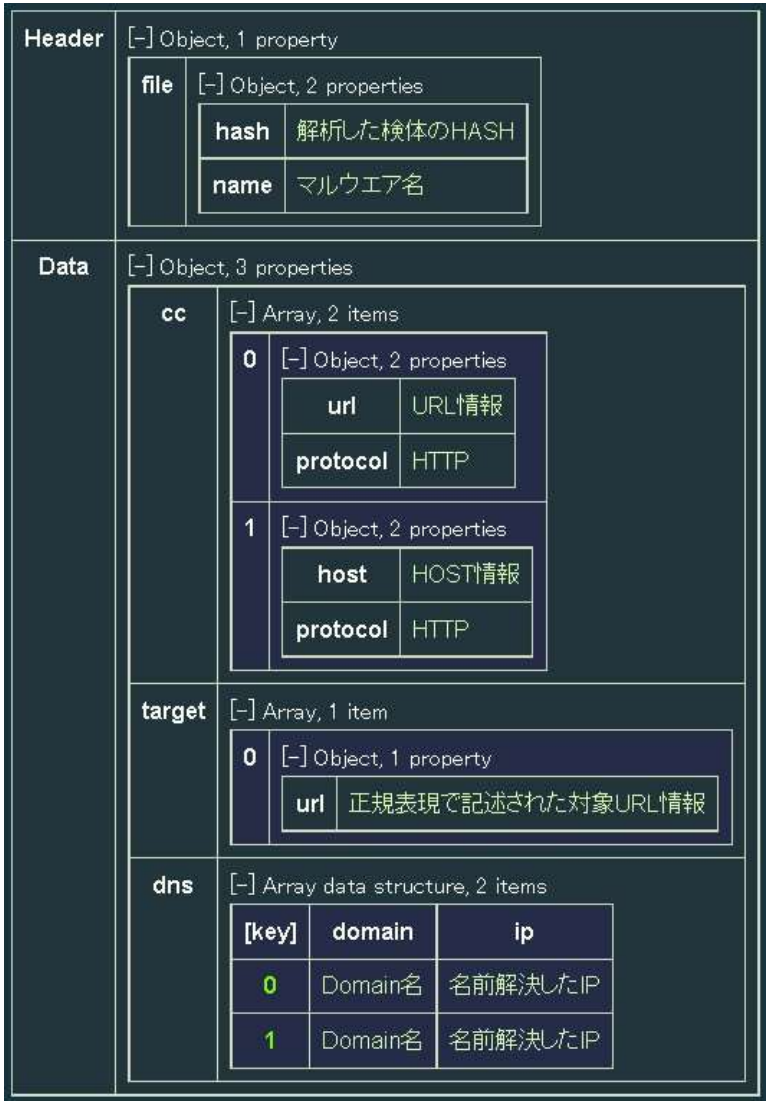


長期観測用マルウェア動的解析　金融系マルウェア群（評価検体例）

検体ファイルハッシュ値sha1	VirusTotal McAfee	VirusTotal Symantec	VirusTotal TrendMicro
fc39b596b851dc2d2262d6b393c7b80b56c366bd	Win32/Injector.CMUF	Suspicious.Cloud.9	TROJ_GEN.R021C0DKK15
0ad35377c36376f7fb57ac5802ec294493499084	Win32/Spy.Zbot.YW	Trojan.Gen.2	TROJ_GEN.R00JC0DL115
445030dcf9d211365a641f53be1286ea2ceb58be	Win32/Injector.BRDF	Suspicious.Cloud.7.L	TROJ_MALKRYP.SM7
445030dcf9d211365a641f53be1286ea2ceb58be	Win32/Injector.BRDF	Suspicious.Cloud.7.L	TROJ_MALKRYP.SM7
2d108ac35247d007cfc10659f29bd75c52c02cf5	VBA/TrojanDownloader.Agent.AJQ	W97M.Downloader	W2KM_DRIDEX.YYSPB
7e31255da225871d0c93ab7b7dd8df23f9c12e69	VBA/TrojanDownloader.Agent.AJZ	W97M.Downloader	W2KM_DRIDEX.SPE
02492bcc7fb9d13e95ef949af34f126f486fe458	VBA/TrojanDownloader.Agent.AKO	W97M.Downloader	W2KM_DRIDEX.NC
c25afc2bb36c91deeee5cf59e55a6996ea2b46df	VBA/TrojanDownloader.Agent.AKZ	W97M.Downloader	W2KM_DRIDEX.AM
694ad860d0752e7f8080			DEX.AM
f0e522523e11694fd0c0			DEX.YYSPI
a18f3d7e48860d5d5e63			DEX.YYSPJ
83ce3a255a6fdb64f316			DEX.YYSQB
fdcf8d452da9320f19e16			DEX.CP
c2f1579afd235d92aeff29841fff18d1a20ed201	VBA/TrojanDownloader.Agent.AKB	W97M.Downloader	W2KM_DRIDEX.VF
70301e32628e8a0e3f5d865863248d89f7df1836	a variant of Win32/Battdil.AL	該当なし	TROJ_GEN.R047C0DK315
a3ade010374df07a9497df0cceda8916a336eede	a variant of Win32/Battdil.AL	Infostealer	TSPY_DYRE.YYSPG
81a9f4e71d929b7d1d200d5bf09f88fa3ca8d940	Win32/Farfli.AFV	Suspicious.MH690.A	TROJ_ZEGOST_EE290078.UVPA
7c35f7c59b9f83def6a8877ed7bff3e29b059d40	Win32/Farfli.BWM	Trojan.Skintrim	TROJ_GEN.R028C0DKQ15
c6bd5827938e46486c85bcaf0de454eb86aed933	Win32/Farfli.BWM	Downloader.Tandfuy	TROJ_GEN.R00XC0CL315
88c2d2b3c1a4d610ac6e8ce2a54875675c279669	Win32/Farfli.MJ	Backdoor.Trojan	TROJ_AGENT_046407.TOMB
7b0bd448378280ba69713ac5a1cc61e1523a852b	Win32/Farfli.AWG	SMG.Heur!cg1	BKDR_FARFLI.SMNB

金融系マルウェア検体の長期動的解析を実行し、そこから検出されたC2サーバや悪性URL情報をアラートとして生成した

JSON 形式のマルウェア長期動的解析アラート（例）



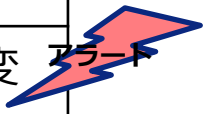
- ヘッダ部
  - 検体ハッシュ値
  - マルウェア名
- データ部
  - C&Cサーバ情報
  - アクセス先URL
  - DNS情報

等

金融系マルウェア　VAWTRAKの観測状況

■ 期間 2014/07/10 ～

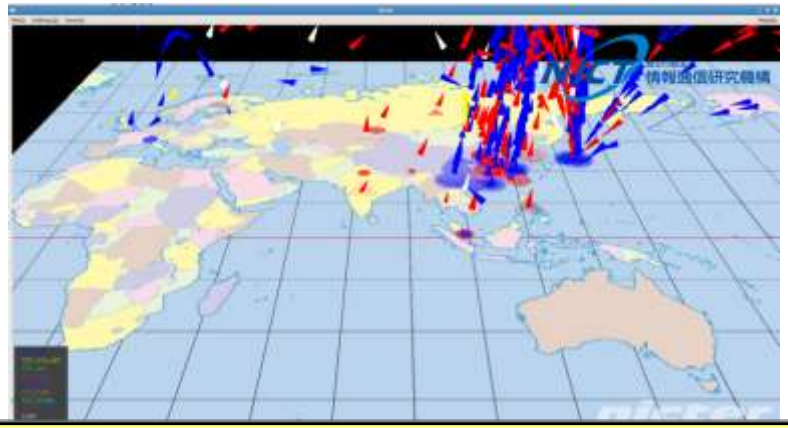
設定情報の更新確認日	外部サーバから更新された情報
2014年7月初旬	VAWTRAK観測開始
2014年7月15日	国内カード会社20社をターゲットとした設定情報
2014年7月18日	国内地銀11行をターゲッとした設定情報
2014年7月29日、31日	某不正送金対策ソフトの機能を無効化する情報
2014年8月13日	マルウェアが通信する外部サーバのホスト（ドメイン）の変更情報
2014年8月13日	国内カード会社への攻撃の削除（銀行は攻撃対象のまま）
2014年9月19日	ヤフオクと大手通販サイトをターゲットとした設定情報

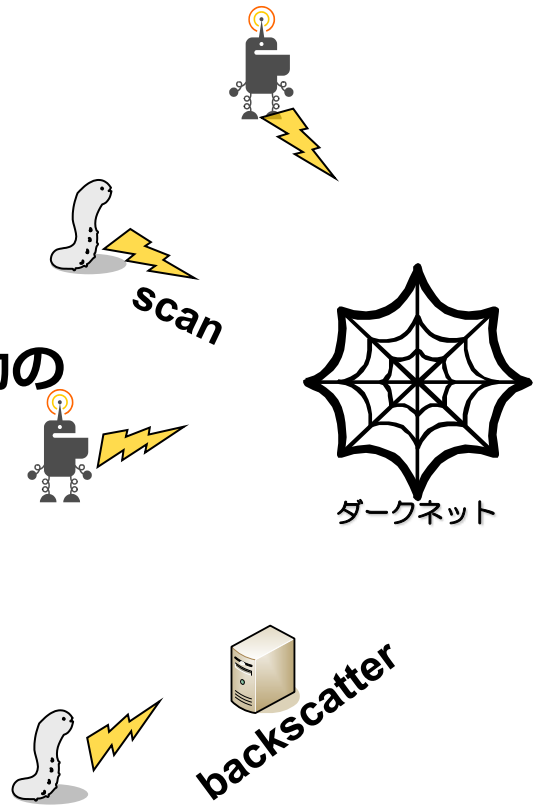


■ ダークネット： 未使用のIPアドレス（空間）
サーバーやホストPCが接続されていないIPアドレス。

■ ダークネットに到達するパケット：
- マルウェアによるスキャン
- マルウェア感染端末の挙動
- DDoS攻撃の跳ね返り（バックスキャッタ）
- 設定ミス

■ ダークネット観測はインターネット上での攻撃挙動の把握に有効であり、多くの研究が行われている。





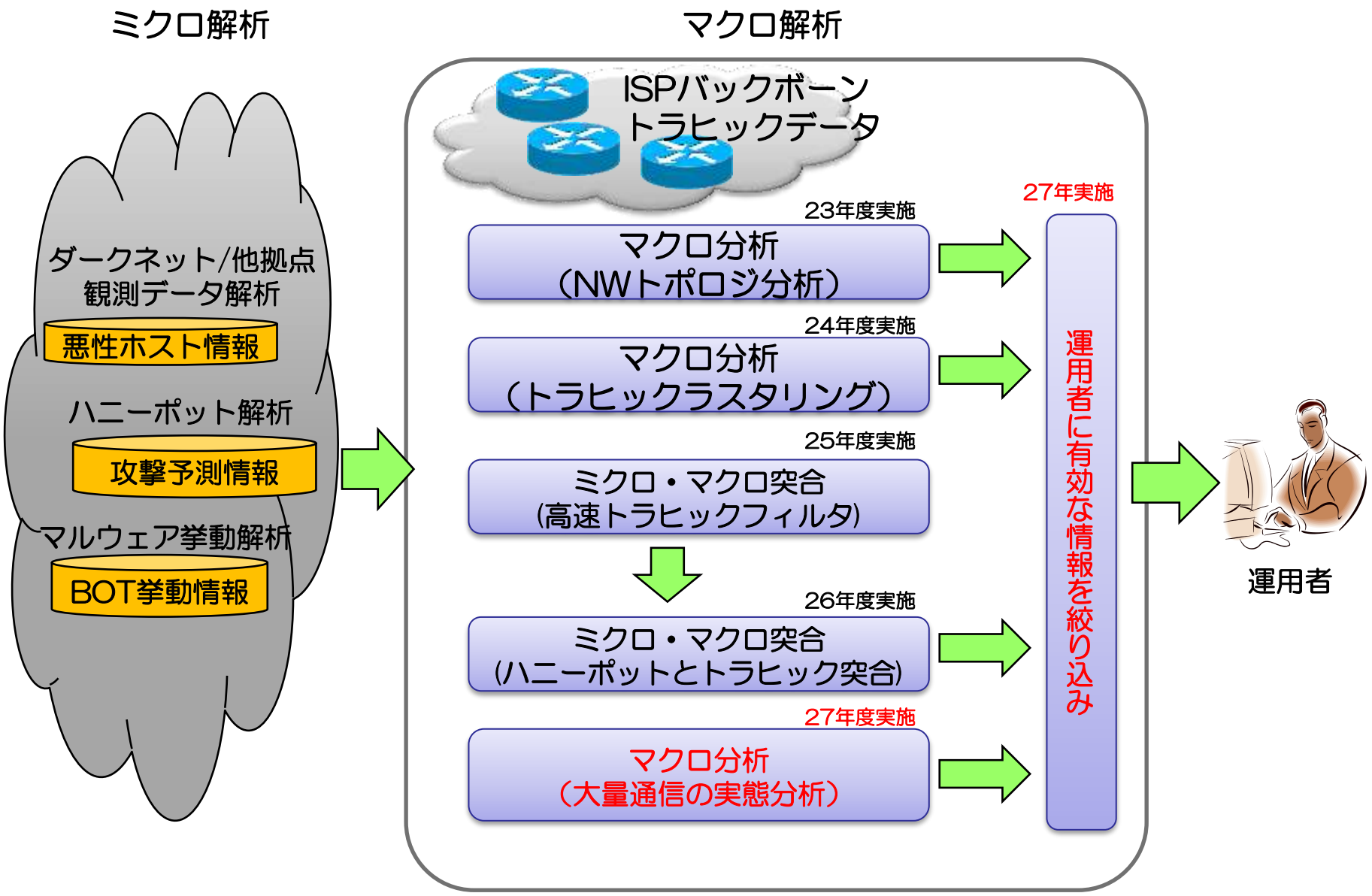
本プロジェクトにて、NICT （情報通信研究機構）の開発したNICTER技術をベースに海外１０拠点のダークネット観測センサーを構築し、NICTの持つ国内センサーと合わせたダークネット解析を実施した。

予兆解析/早期攻撃把握からアラート導出：ダークネット解析によるアラート

- ダークネットをベースとした複数の解析エンジンを開発した。
- 国際連携国の発出する複数国からの捕捉される変化（例えば、送信元IP数の増加等）を把握するために、以下のエンジン群を活用した。

解析エンジン	出力	解析粒度(タイムスパン)	特徴	成果
テンソル分解/NMFエンジン	ボット疑いホスト群の活動パタン	分～時間	始点ホストから終点ホストの対応パタン分析を行う	DRDoS関連ポートへのスキャンを検知（2015/1, 4）。20カ国に分布する端末群が33434/udp (traceroute)をスキャンする異常な事象を検知(2015/11)。
glassoエンジン	ボット疑いホスト群	数分～時間	ホスト間の協調関係をとらえ、ボットネットを検知。NMFよりロバスト	同一のマルウェアに大量感染した韓国内のホスト群を早期検知（2015/11）。JPCERTを経由しKRCERTに通知済み。事態収束に貢献。
高リスクポート検知エンジン(グラフベース変化点検知+分散型攻撃検知)	攻撃リスクが高まりつつあるポートのリスト	時間	数時間単位の変動を捉える異常検知	早期脅威検知事例：攻撃コードを含む53473/udp*宛てのパケットを、2014/9に検知。*2014/8/27にトレンドマイクロの脆弱性報告。

攻撃情報収集と情報共有基盤の構築：通信事業者データの活用・運用技術



大量通信アラートから重要度の高いアラートを選別

ハニーポットアラートを活用して大量通信アラートを分類

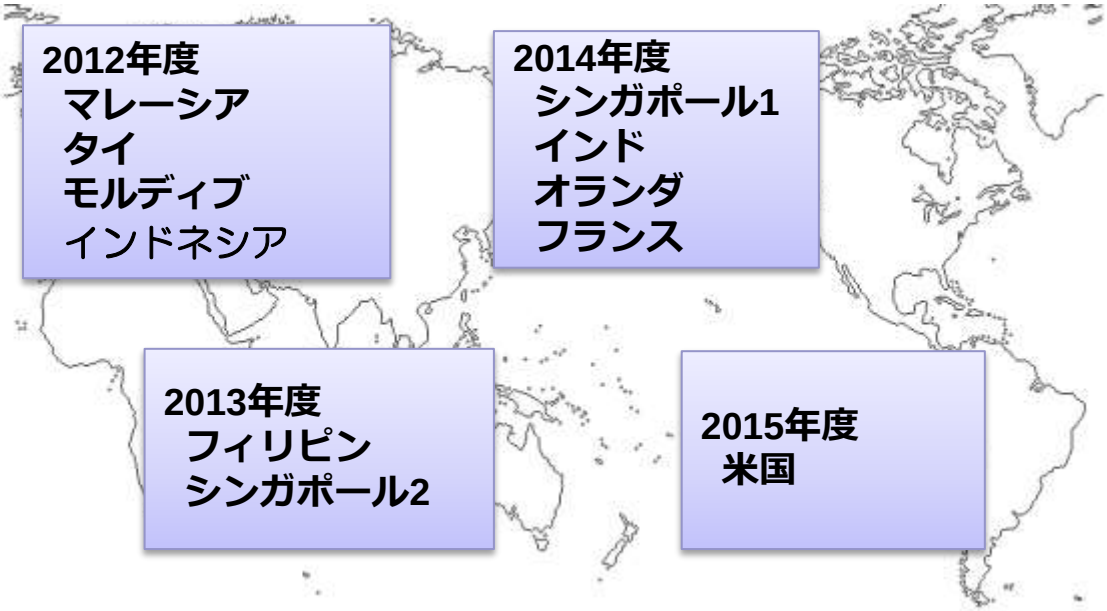
- 手法：ハニーポットアラートとオペレータ対応ログを活用して、機械学習により大量通信アラートを分類
  - 目的：重要度の低いアラートの削減、重要度の高いアラートの抽出
- 検証データ：
  - 学習セット：2015年1月-2月（重要・非重要件数：7866件）
  - テストセット：2015年3月（重要：1509件、非重要：15038件）

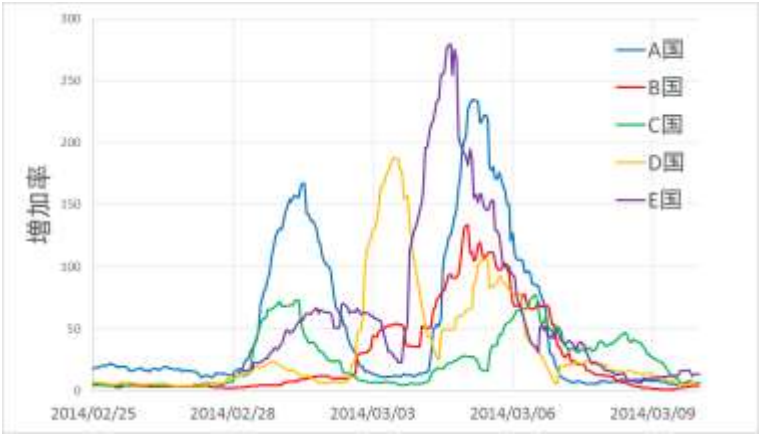
1．重要アラートの見落としなく、重要度の低いアラートを53%削減可能*1
2．重要度の高いアラートを9.9%抽出可能（※ 誤検知を0.1%に抑制可能）*2

*1 重要アラートの見落としが最小となるよう閾値を設定した場合
*2 誤判定する確率が最小となるように閾値を設定した場合

攻撃情報収集と情報共有基盤の構築：海外拠点との連携による攻撃把握と技術連携

- 国際連携により海外10カ国11拠点にダークネット観測センサーを展開
- 連携機関向けにWebポータルを公開し、収集したデータの統計情報や、リアルタイムアラート情報等をフィードバック
- 複数国・拠点で収集したサイバー攻撃情報を用いて、全世界的に行われる攻撃活動を検知するシステムを開発し、アラートが早期警戒に役立つことを確認





Webポータルによる連携先への情報提供

■ PRACTICE成果の連携先への共有を目的としてWebポータルを構築

<サイバー攻撃観測網>

A国 ダークネットt

B国 ダークネット

・・・

F国 ダークネット

日本国内 ダークネット

ダークネット網

DRDoS ハニーポット

マルウェア サンドボックス

国内サイバー攻撃観測網

各種解析エンジン群

情報共有基盤

PRACTICE　Webポータル

公開

サイバー攻撃1次情報

自国のダークネット情報	・攻撃元ホストリスト情報 ・攻撃元国分布情報 ・感染疑いホストリスト情報 ・宛先ポート分布情報
連携国内のダークネット情報	上記一次情報を連携国間で共有し、他国のセンサで観測される自国の攻撃元ホスト、感染疑いホストの情報を取得

サイバー攻撃解析情報

DRDoS ハニーポット	・自国のDRDoS攻撃被害ホスト
マルウェア サンドボックス	・マルウェアのC＆C情報
tkiwa	・独自シグネチャに基づくマルウェア感染ホスト等検知結果
複数情報の相関	・DRDoS ハニーポット、ダークネットの両観測網から得られるDRDoS攻撃に使用されるリフレクタ群情報等

連携国における活用イメージ

サイバー攻撃1次情報

・自国内攻撃元・感染疑いホストの確認
・自国、他国への攻撃傾向の把握
・自国への攻撃元分布に基づき、特定の国の送信元ホスト急増等の変化や傾向を把握

自国のサイバー攻撃情報をリアルタイムで可視化する事で、迅速な情報の活用に役立てる。

サイバー攻撃解析情報（感染疑い、被害ホスト情報）

・自国内のDRDoS攻撃被害ホストの確認、国内ISP等への展開
・自国内の感染ホスト把握、国内ISP等への展開

早期警戒アラートを共有する事により、自国に対するサイバー攻撃への即応に役立てる。

サイバー攻撃解析情報（C&C情報等）

・ 自国内のC&Cやマルウェア感染ホストを把握し、国内ISPやIP利用者等への注意喚起等へ活用

解析の結果得られた攻撃関連情報（C&C等）情報を可視化して共有する事により、攻撃被害軽減、被害の未然防止に役立てる。

Webポータル提供情報例：DRDoS攻撃アラート

2016-02-16 12:28:32	185.62.188.62	hosted-by.blazingfast.io	dns		9349 Dotsi, Unipessoal Lda.	defcon.org ANY IN":40727
20 -16 12:28:28	185.62 .62	hosted- lazingfast.io	dns	171	AS49349 Dotsi, Unipessoal Lda.	defcon.org ANY IN":40754
	18		dns	172	AS49349 Dotsi, Unipessoal Lda.	defcon.org ANY IN":40891
	185	hosted-by.blazingfast.io	dns	172	AS49349 Dotsi, Unipessoal Lda.	defcon.org ANY IN":40841
2016-02-16 12:27:03	185.62.188.62	hosted-by.blazingfast.io	dns	7	ipessoal Lda.	defcon.org ANY IN":1035
2016-02-16 12:27:03	185.62.188.62	hosted-by.blazingfast.io	dns	7	ipessoal Lda.	defcon.org ANY IN":1020
2016-02-16 12:27:03	185.62.188.62	hosted-by.blazingfast.io	dns	7	AS49349 Dotsi, Unipessoal Lda.	defcon.org ANY IN":1035
2016-02-16 12:27:03	185.62.188.62	hosted-by.blazingfast.io	dns	7	AS49 tsi, Unipessoal Lda.	defcon.org ANY IN":1035
2016-02-16 12:00:19	108.61.103.168	108.61.103.168.vultr.com	dns	60		httrack.com ANY IN":708
2016-02-16 12:00:19	108.61.103.168	108.61.103.168.vultr.com	dns	60	AS20473 Choopa, LLC	.com ANY IN":696
2016-02-16 12:00:19	108.61.103.168	108.61.103.168.vultr.com	dns	59	AS20473 Choopa, LLC	
2016-02-16 11:36:11	178.84.156.94	178-84-156-94.dynamic.upc.nl	dns	21	AS6830 Liberty Global Opera B.V.	
2016-02-16 11:12:02	92.109.211.33	92.109.211.33	dns	300	AS6830 Liberty Global Operations B.V.	httrack.com ANY IN":4374
2016-02-16 10:43:47	84.31.147.186	541F93BA.cm-5-8c.dynamic.ziggo.nl	ntp	2109	AS9143 Ziggo B.V.	null":0

攻撃時刻

被害IP

被害ホスト名

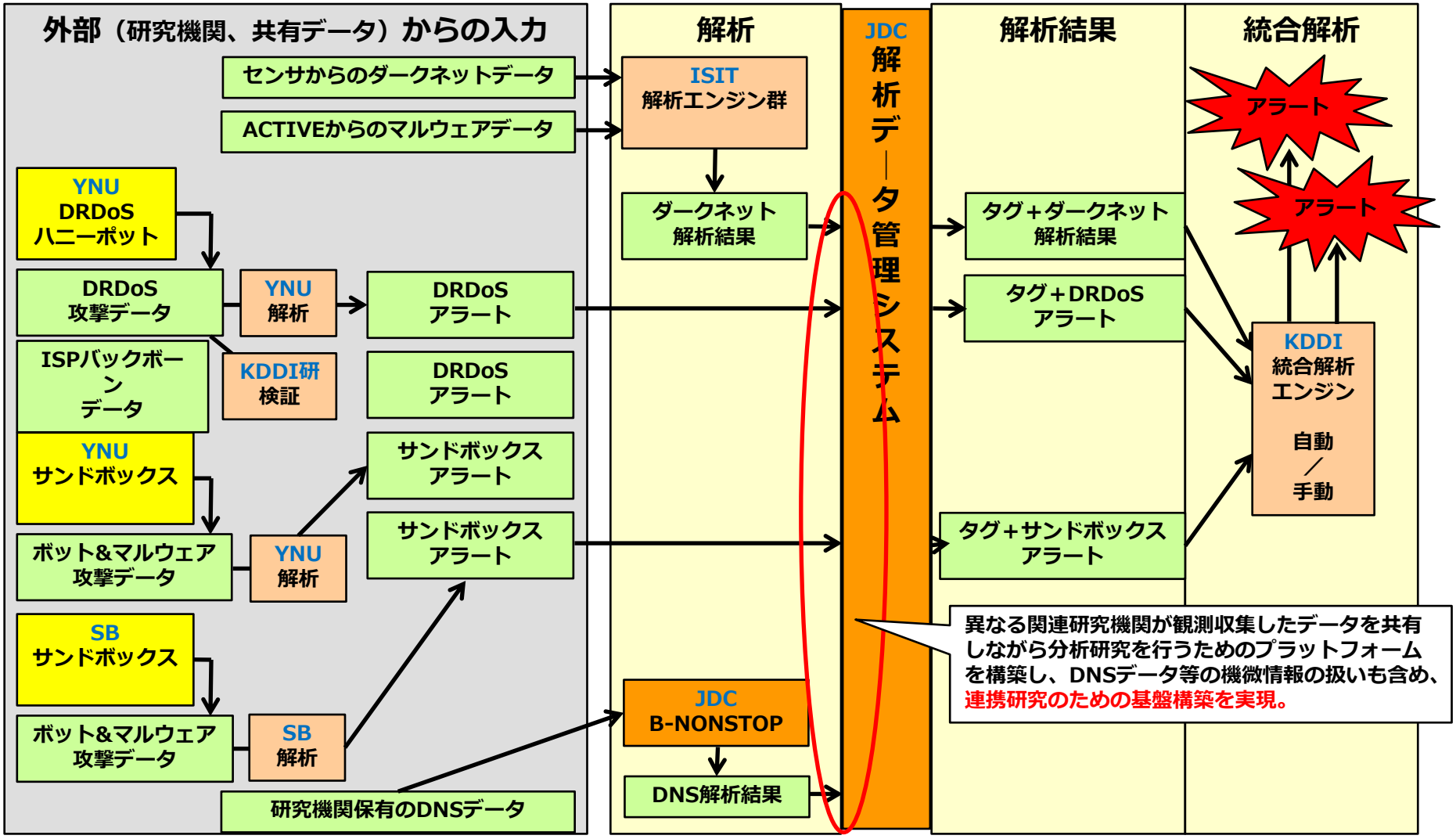
攻撃種類

総パケット数

AS情報

ドメイン（DNS Amp攻撃の場合のみ）

■ 情報共有基盤システムのアーキテクチャおよび実装状況



研究開発成果の引継・社会展開について

- ダークネット解析エンジン：
  NICT（情報通信研究機構）におけるNICTERシステムのダークネット分析エンジンを補完する解析エンジンとして動作させており、今後NICTのサイバーセキュリティ研究基盤の一部として活用される予定。

- DR-DoSハニーポット：
  NICTと連携して引続き横浜国立大学で運用を継続し、ICT-ISAC（旧Telecom-ISAC Japan）を経由して各ISPへのアラート配信を継続する。

- マルウェアの長期サンドボックス解析：
  サンドボックスの運用をセキュアブレインにて継続し、解析結果（C2情報や悪性URLなど）を総務省の「官民連携による国民のマルウェア対策支援プロジェクト（通称ACTIVE）」に提供する。

- 国際連携（ダークネットセンサー）：
  構築したダークネット観測センサーの管理運用を含め、全ての海外連携窓口をNICTへ移管済み。NICTを通じて情報共有等の連携を継続する。

まとめ

- 平成23年度から27年度にかけて実施された「国際連携によるサイバー攻撃の予知技術の研究開発」プロジェクトの報告を行った。

- 5年間の取り組みの中で、ボット型攻撃に加えてP2Pマルウェア、リフレクション型のDDoS攻撃や、金融系のマルウェア等、多様化する新たな攻撃にも対応した研究開発を実施し、脅威の変化に追随する研究開発を推進することができた。

- 世界初で開発したハニーポット技術や、長期サンドボックス解析技術などを用いて早期に攻撃を把握するための技術基盤を確立でき、実用性の高い予知・即応技術・基盤を確立することができたことは大きな成果である。

- 2020年の東京オリンピック・パラリンピックを含めた近未来における高度な脅威（攻撃）観測基盤、及び分析基盤の構築は必達の課題であり、それらにおいて本研究開発が有効的に利活用され、今後の日本の安心安全に向けて大きく貢献できることを期待したい。