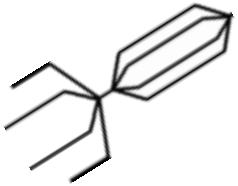
サイバー攻撃に対する NICTの最新の取り組みと今後の課題

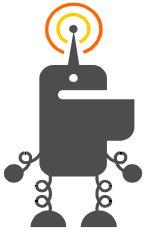
独立行政法人 情報通信研究機構（NICT）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室
井上 大介

サイバー攻撃のツール：マルウェア

- **Malware = Malicious(悪意のある)+ Software**
  - 情報漏えいやデータの破壊・改竄、他のコンピュータへの攻撃など、ユーザの望まない不正な活動を行うソフトウェアの総称



ウイルス



ボット

ワーム

マルウェア関連用語

～ マルウェアの感染形態に着目した分類～

- **ウイルス（狭義のウイルス）**
  - ✓ 単体動作せず，自分自身を他のファイルやプログラムに寄生
  - ✓ ブートセクタ感染型：ハードディスクなどのシステム領域に感染
  - ✓ ファイル感染型：実行可能ファイルを主な感染対象

- **ワーム**
  - ✓ 単体で動作し自己増殖を行う
  - ✓ ウイルスに比べ高い感染力を有し，大規模感染を引き起こす
  - ✓ 電子メールやリムーバブルメディア（USBメモリ等）を媒体とするもの
  - ✓ Windowsのファイル共有やメッセージング機能を利用するもの
  - ✓ OSやアプリケーションの脆弱性に対する攻撃コードを用いるもの

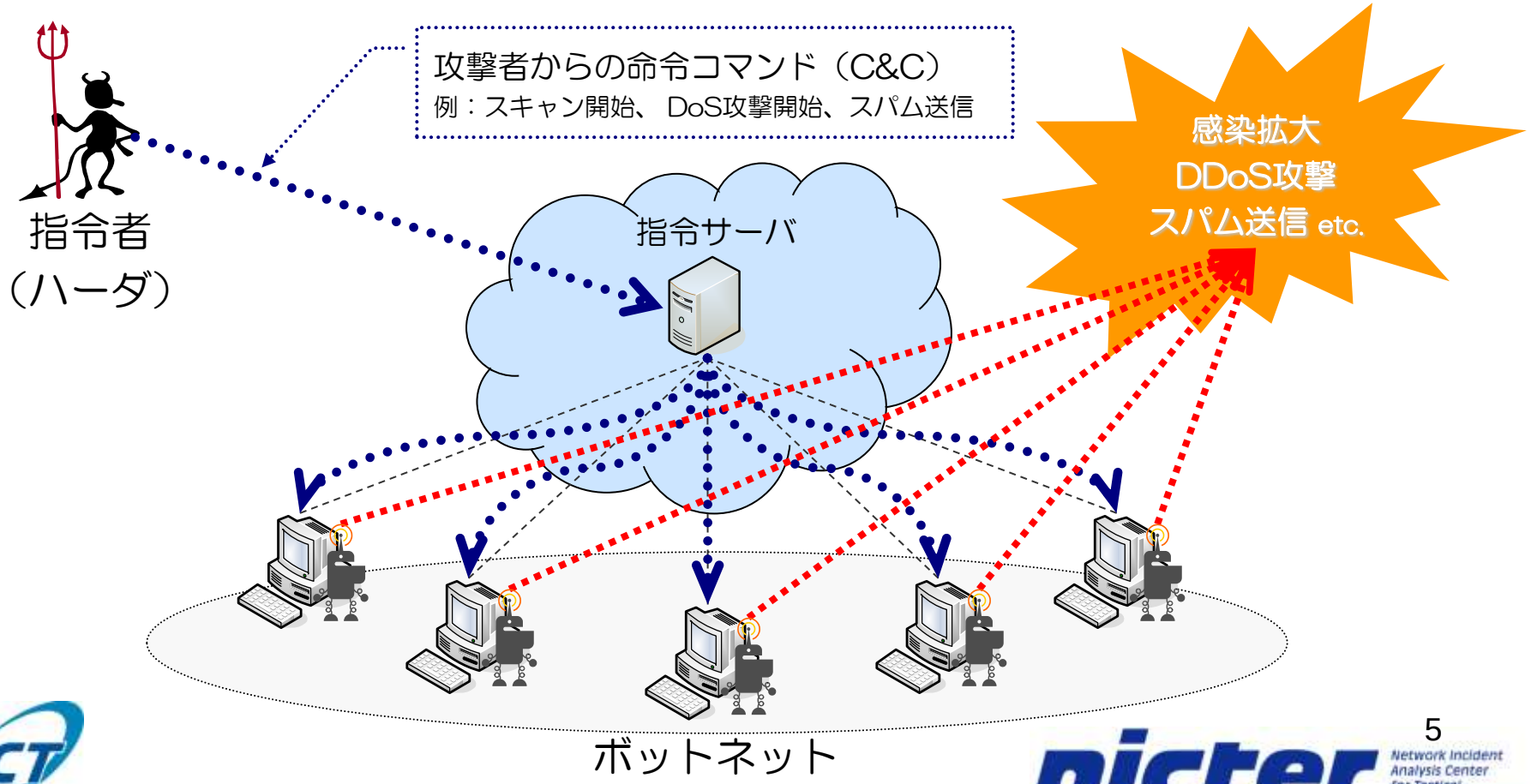
- **トロイの木馬**
  - ✓ 有用なプログラムやファイルに偽装
  - ✓ ユーザ自身によるシステムへのインストールや起動を誘う
  - ✓ 感染機能を持たないものが多い

マルウェア関連用語
～ マルウェアの目的に着目した分類～

- **スパイウェア**
  - ✓ 個人情報や行動履歴を収集し，特定のサーバなどに送信する
  - ✓ ユーザのキーボード操作を記録・収集するキーロガーもスパイウェアの一種
- **アドウェア**
  - ✓ ユーザに企業広告などを提示することを目的にしたプログラム
  - ✓ ユーザの同意なしに広告を頻繁にポップアップ／Webサイトに強制誘導
- **ランサムウェア**
  - ✓ ユーザのPC上のデータを強制的に暗号化／パスワード付きZIP圧縮
  - ✓ データの復号や解凍の見返りとしてユーザから身代金（ransom）を搾取
- **スケアウェア**
  - ✓ ユーザに虚偽の情報（マルウェア感染等）を提示
  - ✓ 不安（scare）を煽り無意味なソフトウェアを販売

マルウェア関連用語
～ その他の分類 ～

- **ボット**
  - ✓ 指令者からの遠隔操作により多岐に渡る活動を行うマルウェア
  - ✓ ボットネットと呼ばれるオーバレイネットワークを形成（数百～一千万台規模）



マルウェア年表（1970年～2010年）

Year	Malware
1970	
1971	Creeper (1st worm)
1972	# The term “virus” first appeared in a SF novel “When HARLIE Was O
1973	
1974	
1975	# The term “worm” first appeared in a SF novel“The Shockwave Rider”
1976	
1977	
1978	
1979	
1980	Xerox PARC Worm
1981	
1982	Elk Cloner (1st virus)
1983	
1984	# Cohen defined virus in his paper “Computer Viruses - Theory and Exp
1985	
1986	Brain (1st IBMPC virus), PC-Write (1st Trojan horse), Virdem
1987	Cascade, Jerusalem, Lehigh, Christmas Tree, MacMag
1988	Byte Bandit, Stoned, Scores, Morris Worm
1989	AIDS (1st ransomware), Yankee Doodle, WANK

発見の時代

Year	Malware
1990	1260 (1st polymorphic virus), Form, Whale
1991	Tequila, Michelangelo, Anti-Telefonica, Eliza
1992	Peach (1st anti-antivirus programs), Win.Vir_1_4 (1st Windows virus)
1993	PMBS
1994	Good Times (1st hoax)
1995	Concept (1st macro virus)
1996	Laroux, Staog (1st Linux m.w.)
1997	ShareFun, Homer, Esperanto
1998	Accessiv, StrangeBrew (1st Java m.w.), Chernobyl
1999	Happy99, Tristate, Melissa, ExploreZip, BubbleBoy, Babylonia
2000	Loveletter, Resume, MTX, Hybris
2001	Anna Kournikova, BadTrans, CodeRed I, Sircam, CodeRed II, Nimda,
2002	LFM-926 (1st Flash m.w.), Chick, Fbound, Shakira, Bugbear
2003	Sobig, SQLSlammer, Deloder, Sdbot, Mimail, Antinny, MSBlaster, Wel Agobot, Swen, Sober
2004	Bagle, MyDoom, Doomjuice, Netsky, WildJP, Witty, Sasser, Wallon, Bo Cabir (1st Symbian m.w.), Amus, Upchan , Revcuss, Lunii, Minuka, Vun
2005	Bropia, Locknut, BankAsh, Banbra, Anicmoo, Commwarrior, Pgpcoder Gargafx, Peerload, Cardblock, PSPBrick (1st PSP m.w), DSBrick (1st Ni m.w.), Dasher
2006	Kaiten, Leap (1st Mac OS X m.w.), Redbrowser, Cxover, Exponny, Mdr Flexispy, Spaceflash, Stration, Mocbot, Fujacks, Allaple
2007	Storm Worm, Pirlames, Zlob, Srizbi (1st full-kernel m.w.), Silly, Pidief
2008	Mebroot, Infomeiti, Conficker
2009	Virux, Yxes,Gumbler, Induc, Ikee (1st iPhone m.w.)
2010	Zimuse, Trojan-SMS. AndroidOS.FakePlayer (1st Android m.w.), Stuxnet

実験的試行の時代

悪用の時代

6

インシデント分析センタ nicter 概要

nicter = **N**etwork **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse

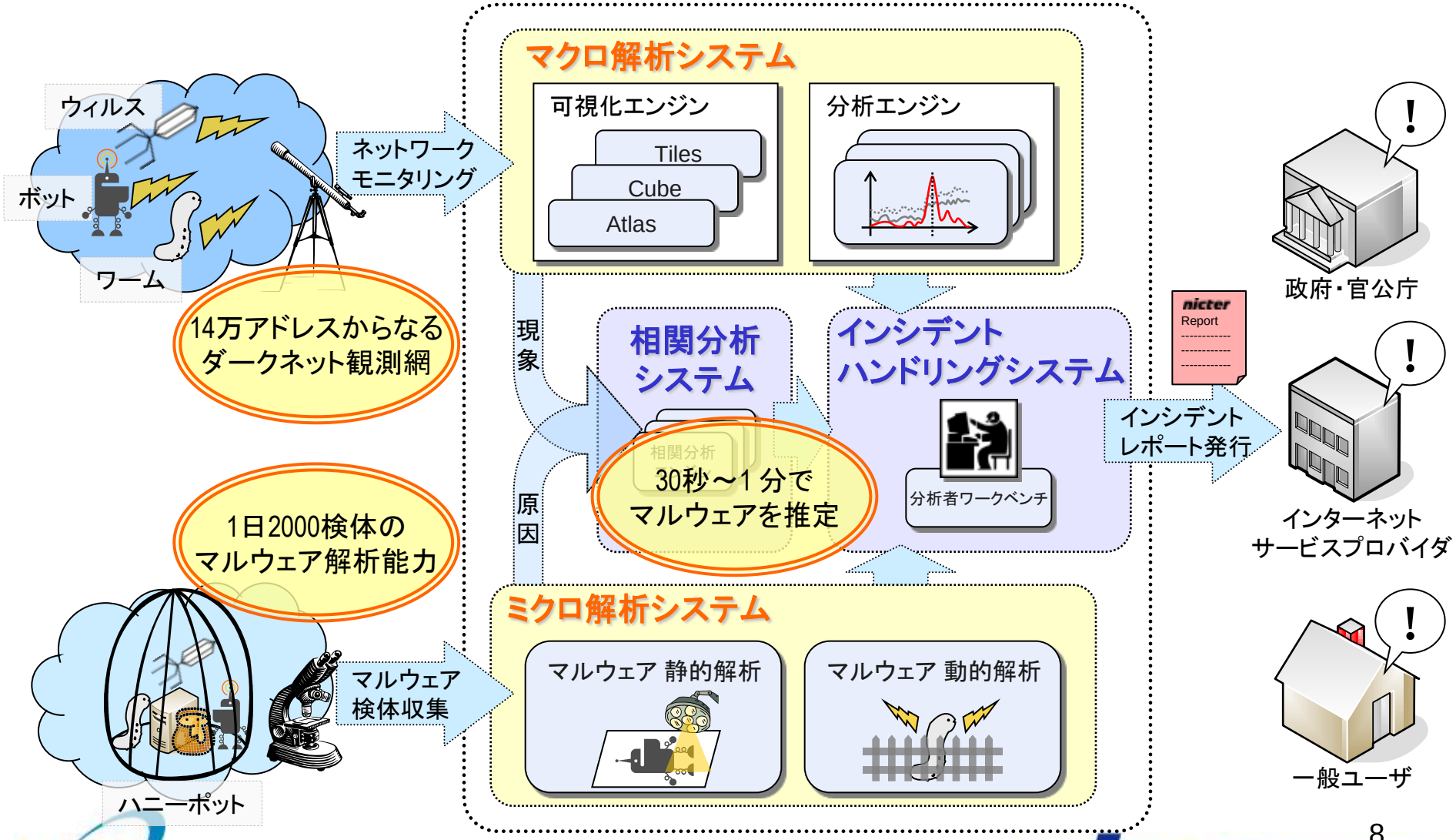
目的:

広域ネットワークにおけるセキュリティインシデント（セキュリティ事故）の迅速な状況把握・原因究明・対策導出。

主要コンポーネント

- マクロ解析システム　（ネットワークモニタリング）
- ミクロ解析システム　（マルウェア解析）
- マクロ-ミクロ相関分析システム　（マクロとミクロの融合）

nicterの全体像

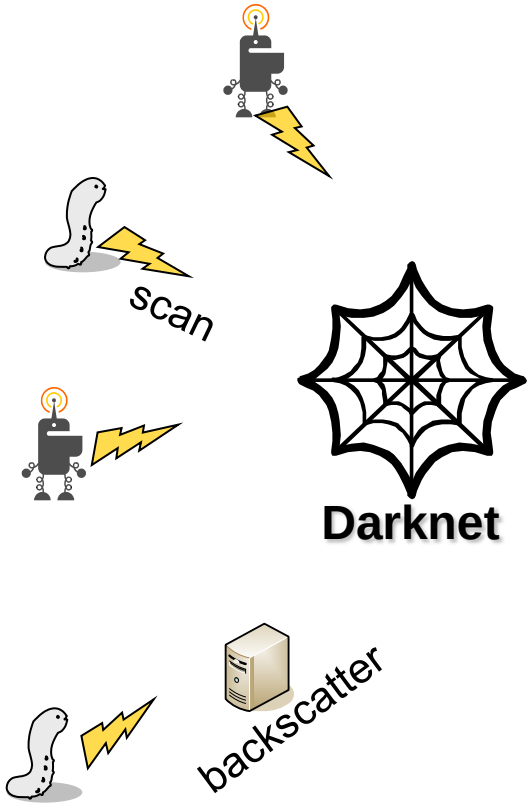

マクロ解析システム
可視化エンジン
Tiles
Cube
Atlas
分析エンジン
ウィルス
ボット
ワーム
ネットワーク
モニタリング
14万アドレスからなる
ダークネット観測網
現象
原因
相関分析
システム
相関分析
30秒～1分で
マルウェアを推定
インシデント
ハンドリングシステム
分析者ワークベンチ
nicter
Report
インシデント
レポート発行
政府・官公庁
インターネット
サービスプロバイダ
一般ユーザ
1日2000検体の
マルウェア解析能力
ハニーポット
マルウェア
検体収集
ミクロ解析システム
マルウェア 静的解析
マルウェア 動的解析

ダークネットとは？

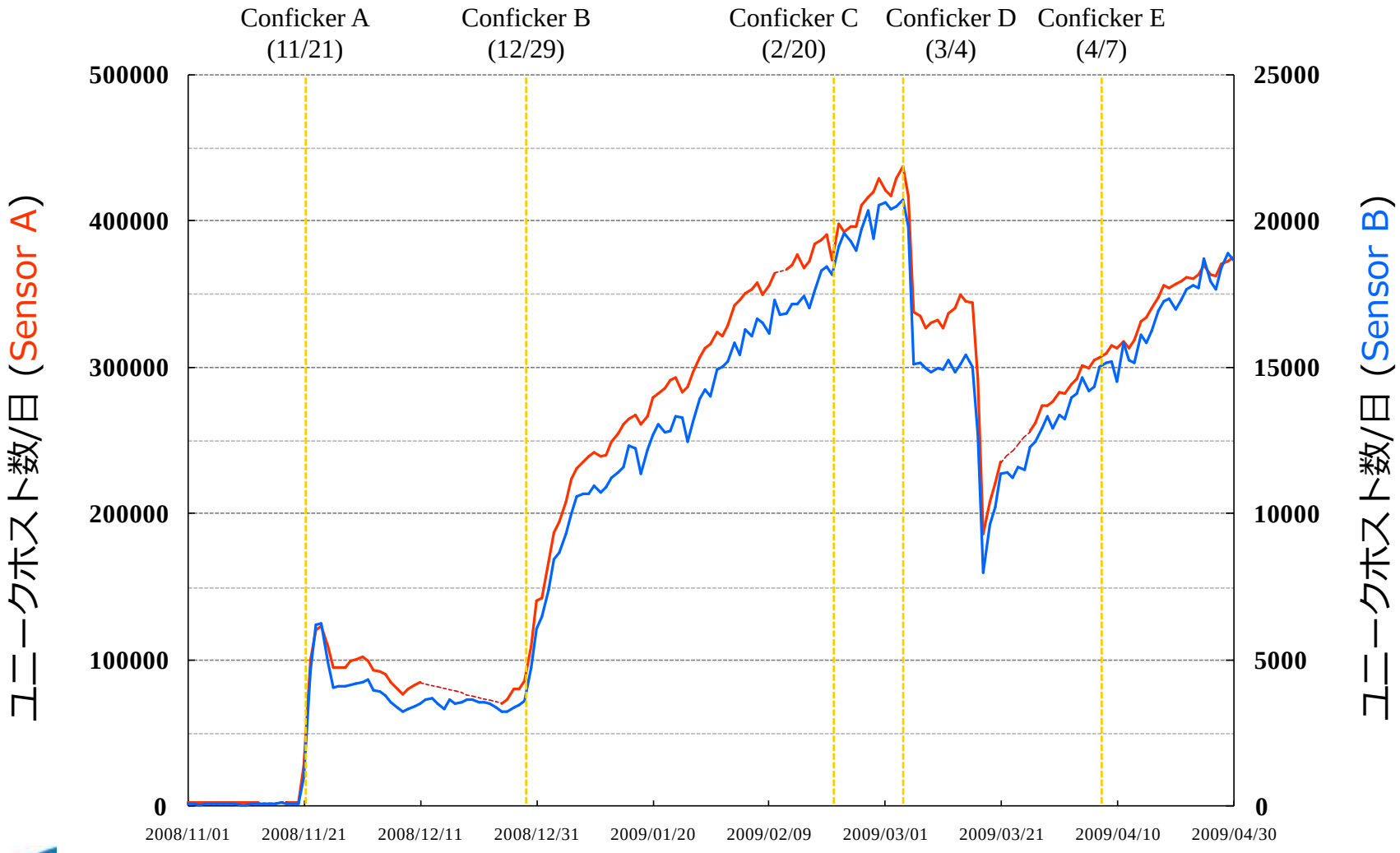
- ユーザマシンやサーバが接続されていない
  未使用アドレスブロック

- ダークネットトラフィックはなぜ発生？
  - ✓ マルウェアによるスキャンや攻撃
  - ✓ DDoS攻撃の跳ね返り（Backscatter）
  - ✓ 設定ミス

- ダークネット観測のメリット
  1. プライバシ問題が回避可能
     → ネットワークの端点で自分宛の通信のみ観測。
  2. 観測データに正・不正の区別が不要
     → 飛んで来たものは全て不正な通信。
  3. パッシブモニタリング
     → 待っているだけで定常的に通信が到来。

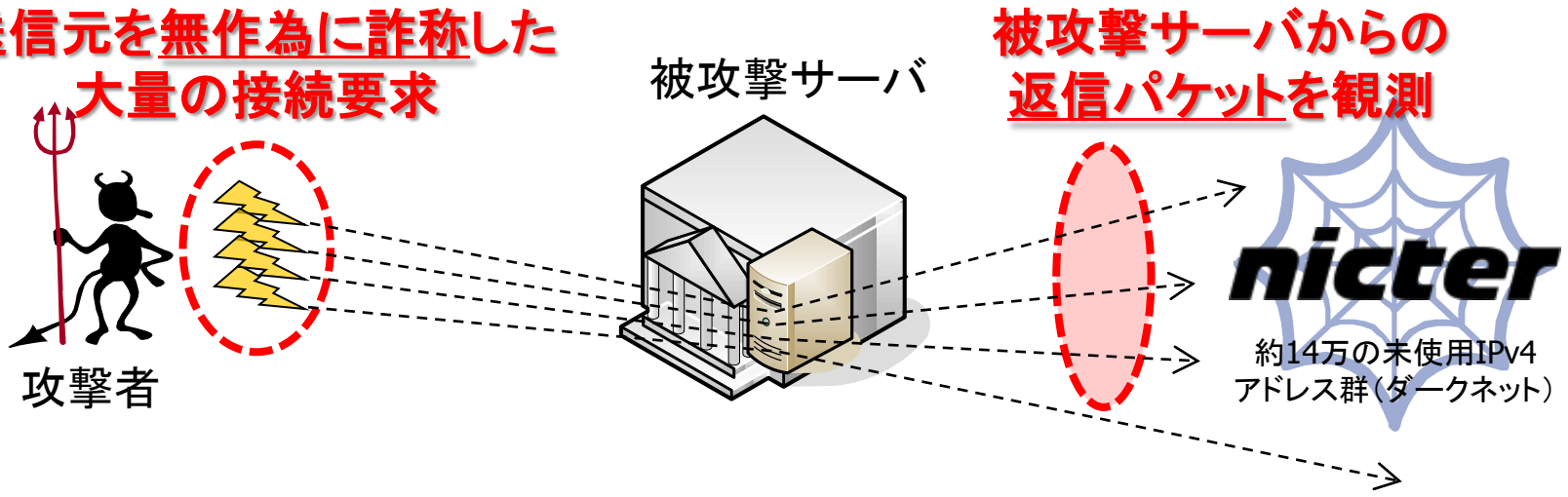


Conficker感染爆発時の ダークネット観測結果（ユニークホスト数 on 445/tcp）

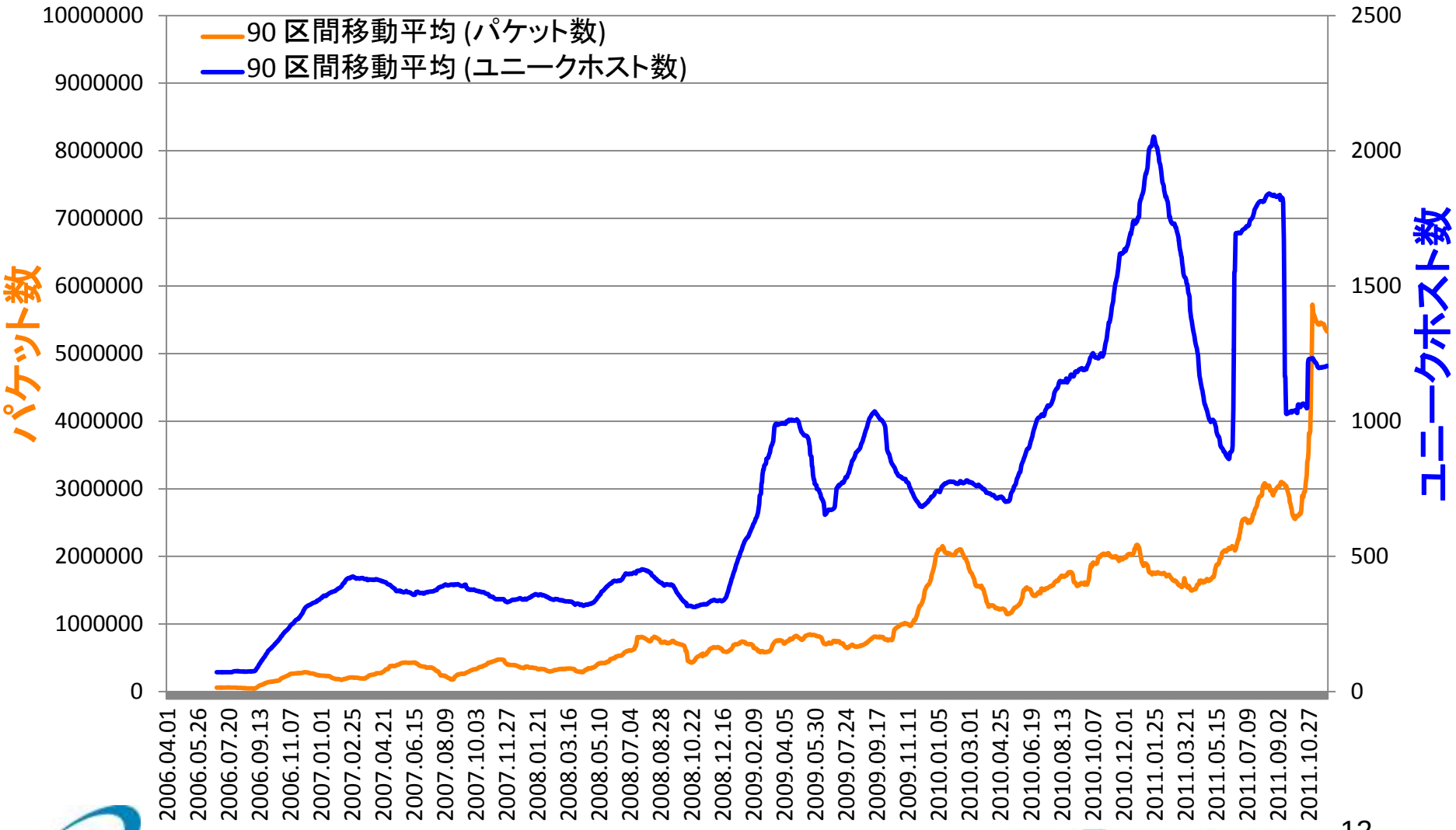


バックスキャッタ観測の仕組み

- **バックスキャッタ：**
  送信元IPアドレスが詐称されたDDoS攻撃の跳ね返り



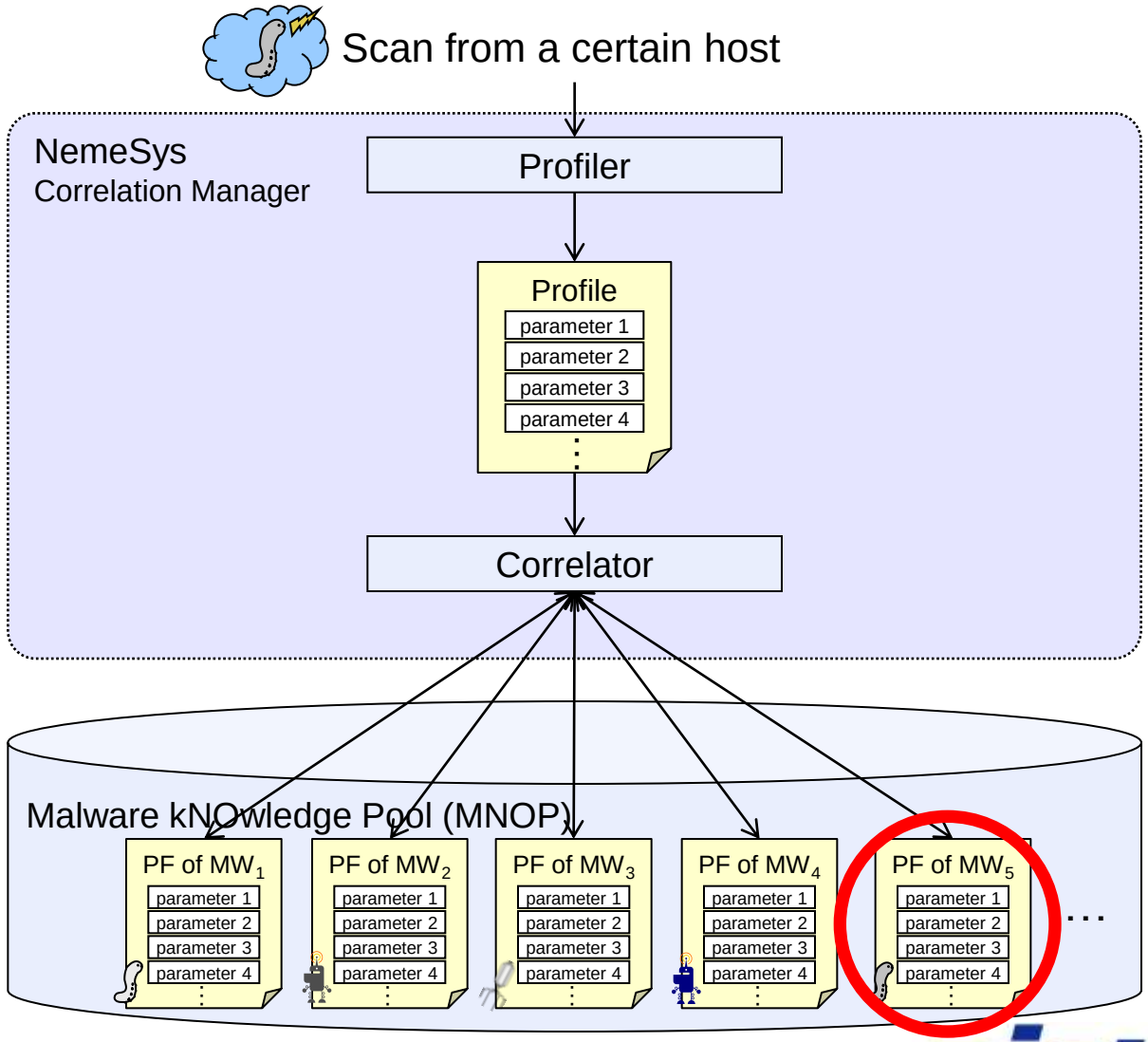
バックスキャッタの長期観測結果



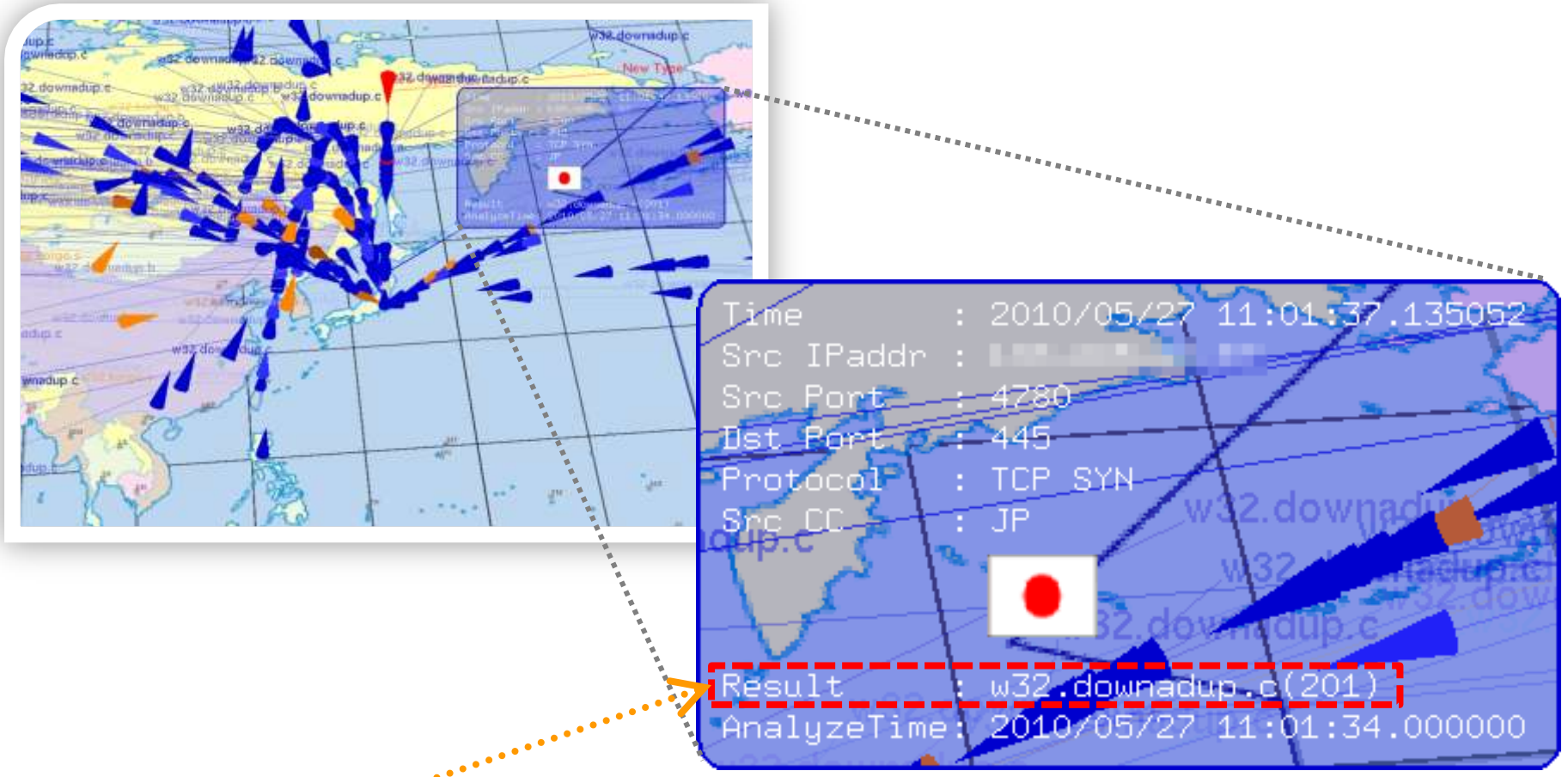
NICT

nicter Network Incident Analysis Center for Tactical Emergency Response

マクローミクロ相関分析システム



相関分析結果のリアルタイム可視化



ダークネットへの攻撃を行ったホストに
感染している**マルウェアをリアルタイムで特定**

NICT

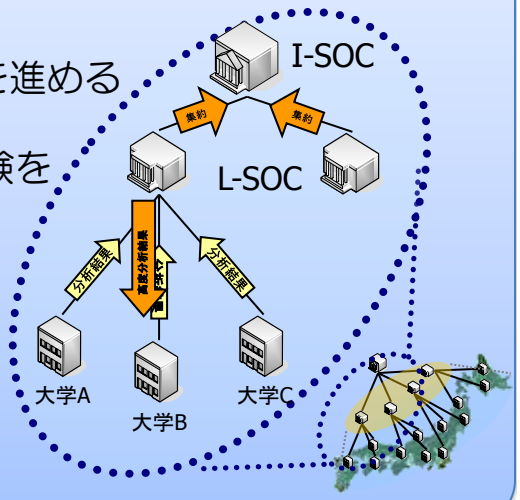
nicter Network Incident Analysis Center for Tactical Emergency Response

nicter 外部展開の取り組み

大学系：全国規模の観測・分析網構築

- 日本全国の大学にnicterのセンサ設置を進める
- 2010年度に実証実験を開始し、分析結果を各大学に提供

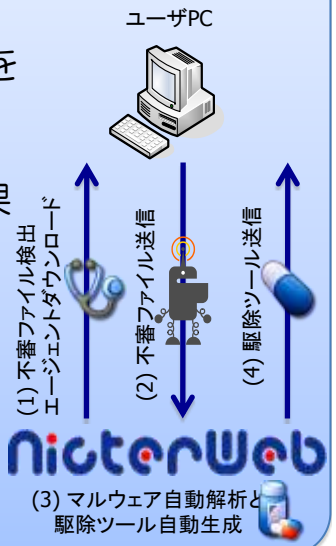
※平成20年度委託研究
「インシデント分析の広域化・高速化技術に関する研究開発」との連携



ユーザ系：マルウェア対策ユーザサポート

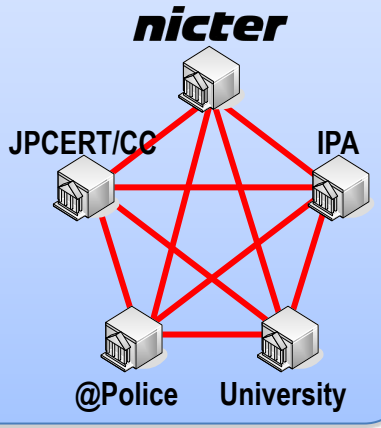
- 不審ファイル検出エージェントをユーザに配布
- nicterのマルウェア自動解析結果から駆除ツール自動生成を行い、ユーザに駆除ツールを送信
- 2011年度に実証実験を実施

※平成21年度委託研究
「マルウェア対策ユーザサポートシステムの研究開発」との連携



セキュリティ関連組織系：定点観測友の会

- 国内のセキュリティ関連組織の情報共有ネットワーク（定点観測友の会）にnicterの観測結果を提供
- JPCERT/CC、IPA、@Police等への情報提供を通して、社会への注意喚起に寄与



企業系：NIRVANA（nicter real-network visual analyzer）

- 国内大手企業からの要請により、nicterの可視化技術を応用した、実トラフィックリアルタイム可視化システムを開発
- 2009年度末から定常運用開始
- 国内SIerから一般販売中

新たな脅威たち・・・

- ドライブ･バイ･ダウンロード攻撃
- 標的型攻撃
  (Advanced Persistent Threat)
- SNSマルウェア
- IPv6ネットワーク上の脅威

etc…

ドライブ・バイ・ダウンロード攻撃とは？

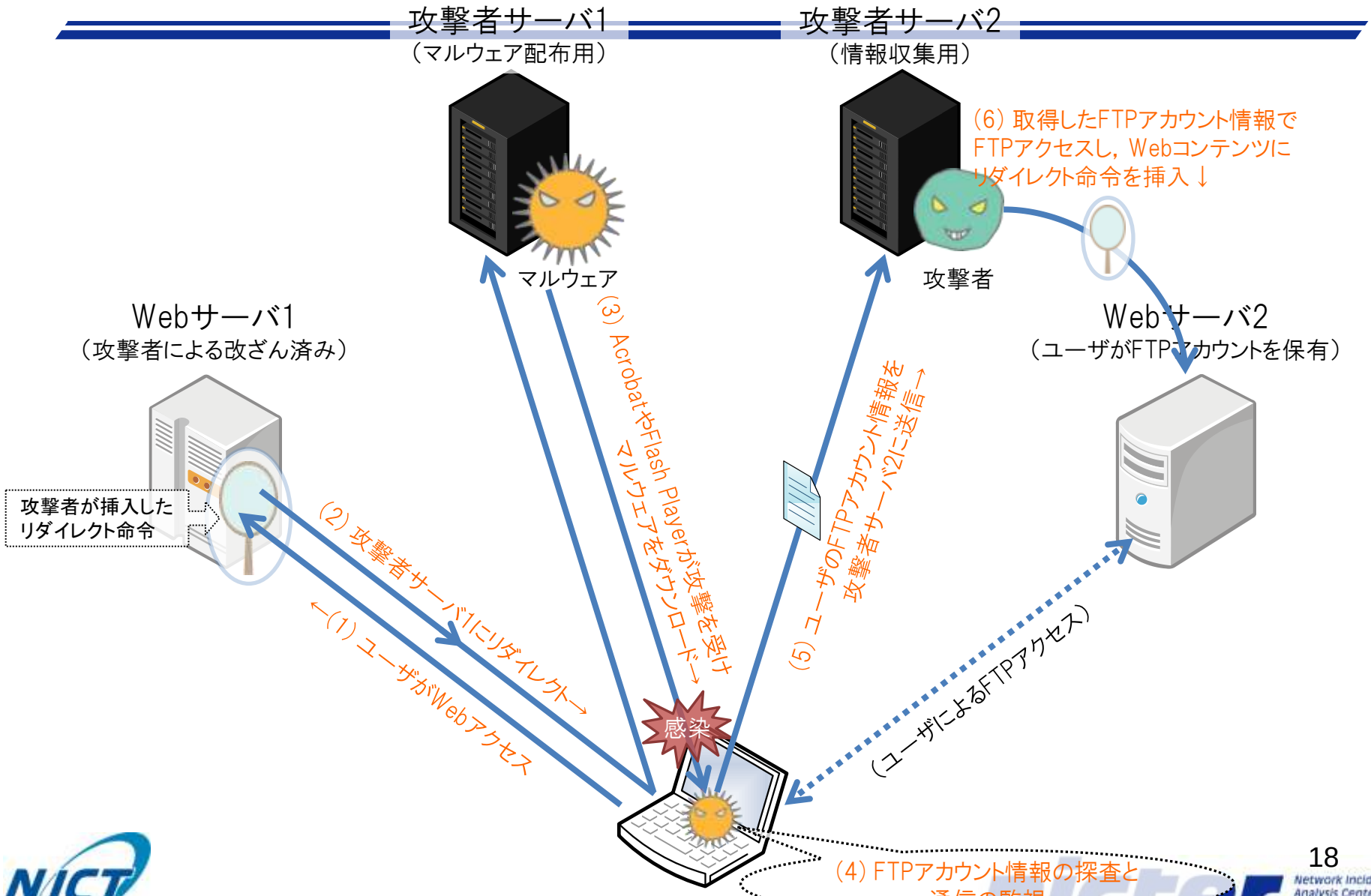
- Webサイトにアクセスしただけでマルウェアに感染する新種の攻撃。

- ユーザのWebブラウザに不正コードをダウンロードさせ、マルウェア感染を引き起こす。

- 2009年初頭からインターネットにおける最大の脅威
  - ✓ Niels Provos, et al. (Google), “The Ghost In The Browser,”
    ～ 攻撃はブラウザの中で起こっている ～

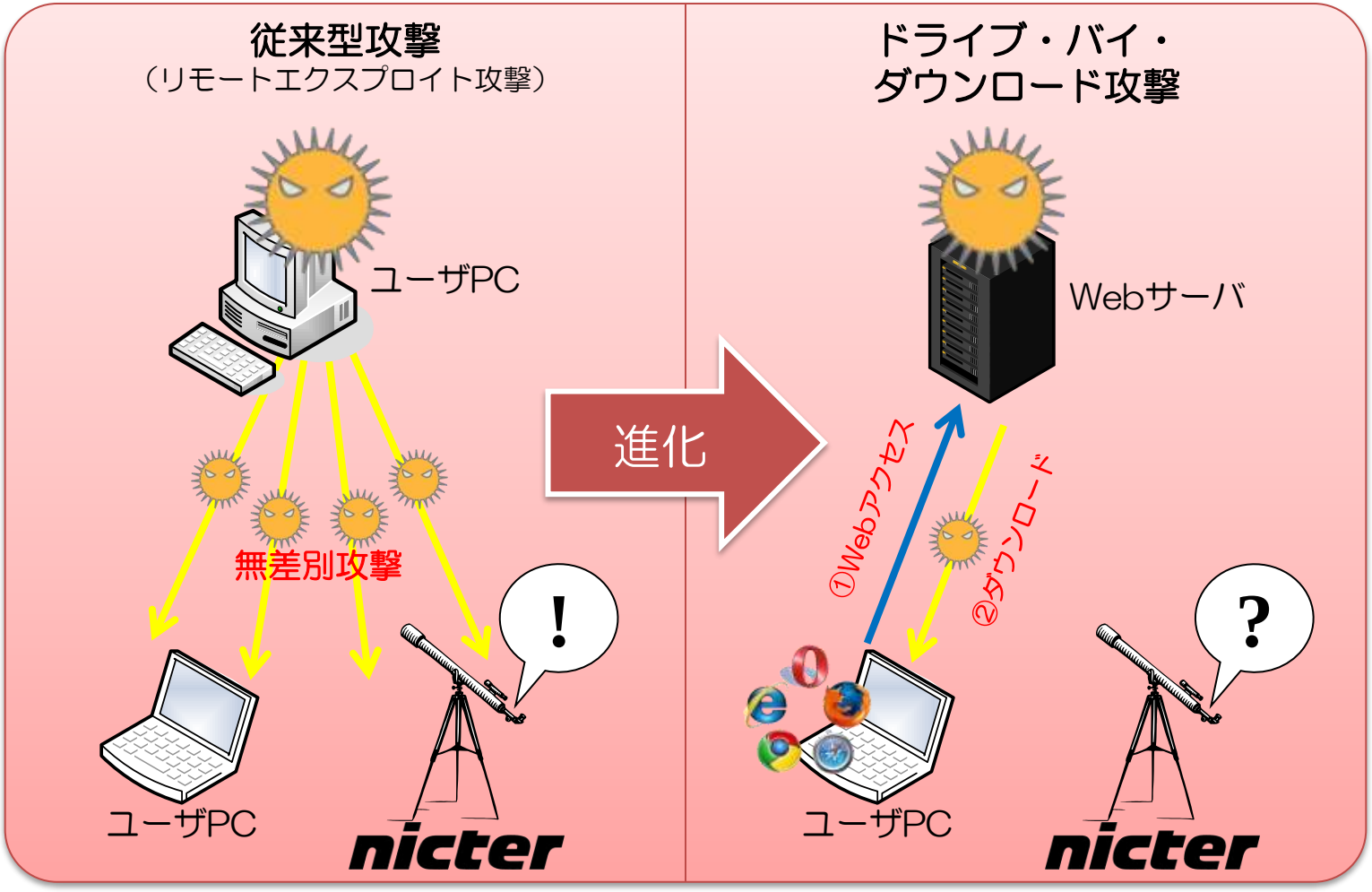
- 最初の発見：2009年4月 Gumbler攻撃

Gumblar攻撃の流れ



18

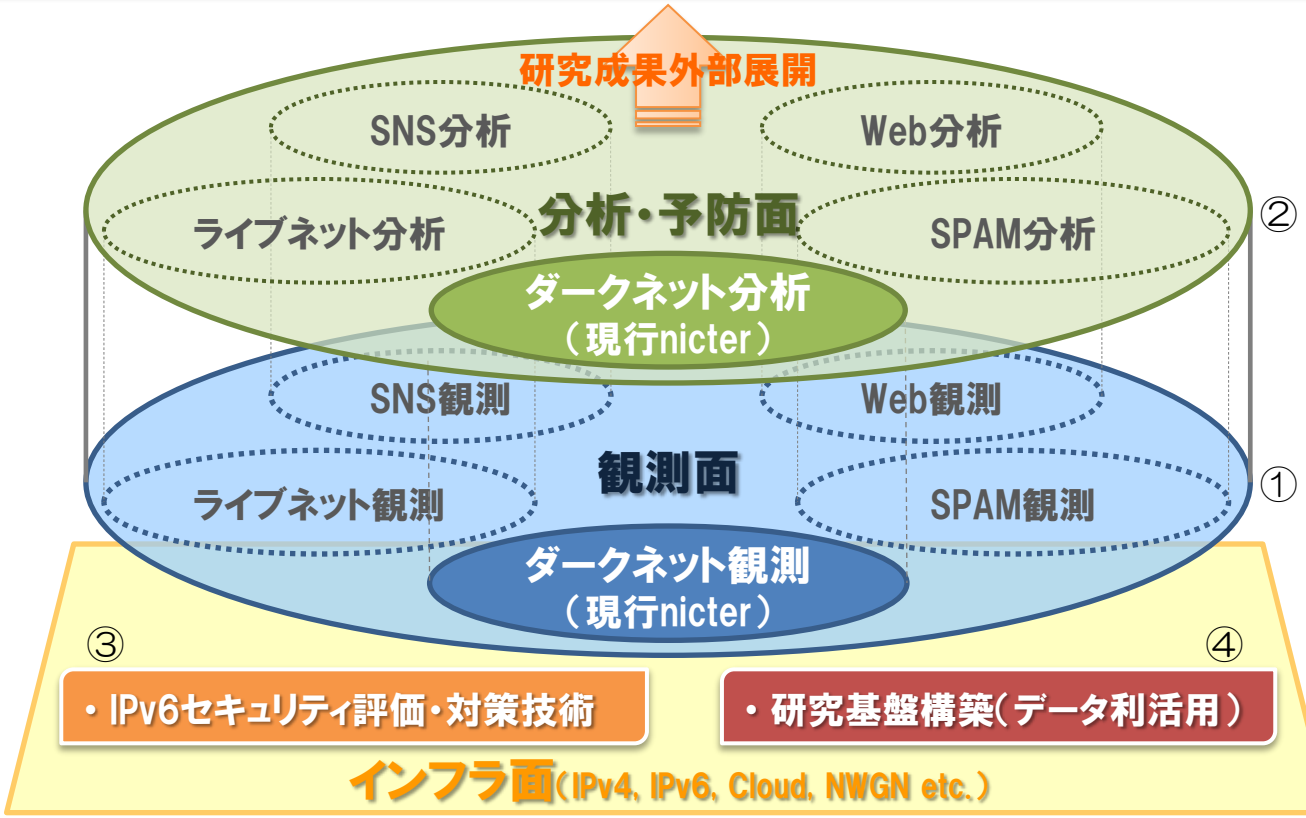
従来型攻撃との本質的な違い



NICT サイバーセキュリティ研究室の研究概要 (1/3)

実践的サイバーセキュリティ技術の確立
～ 守りのセキュリティから攻めのセキュリティへ ～

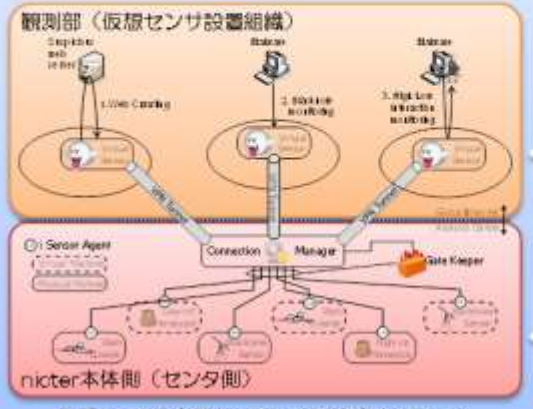
① 広域性・詳細性・能動性を兼ね備えた世界最大規模の能動的サイバー攻撃観測網を構築
② 進化を続けるサイバー攻撃に追随/先行するサイバー攻撃分析・予防基盤技術の開発
③ 新たな情報通信インフラの安全性を確保するIPv6セキュアネットワーク構築技術の確立
④ nicter収集情報の安全な利活用を促進する研究基盤構築と即効性のある成果展開



NICT サイバーセキュリティ研究室の研究概要 (2/3)

★ 能動的サイバー攻撃観測網

- センタ側での異種センサ動的スイッチング



センサは簡潔に

センタは柔軟に

異種センサ統合型ネットワーク観測プラットフォーム

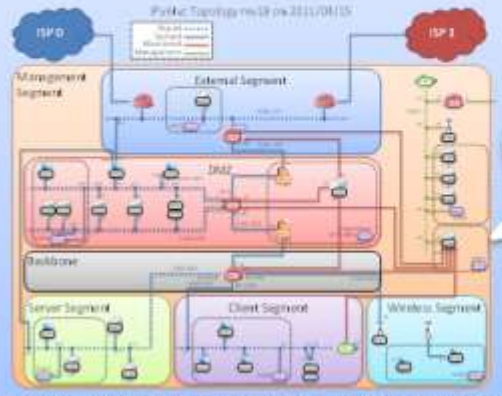
★ サイバー攻撃分析・予防基盤技術

- Web媒介型マルウェアの分析・予防フレームワーク

ドライブ・バイ・ダウンロード攻撃対策フレームワーク

★ IPv6セキュアネットワーク技術

- IPv6大規模テストベッド上での攻撃実証と対策検討

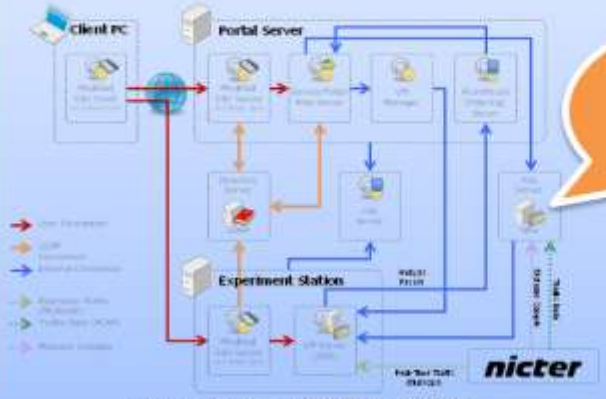


IPv6技術検証協議会で産学官の力を結集

IPv6セキュリティ検証環境@マイクロソフト大手町テクノロジーセンター

★ サイバーセキュリティ研究基盤

- nicter収集情報を蓄積する安全な遠隔分析環境



nicter収集情報の利活用促進

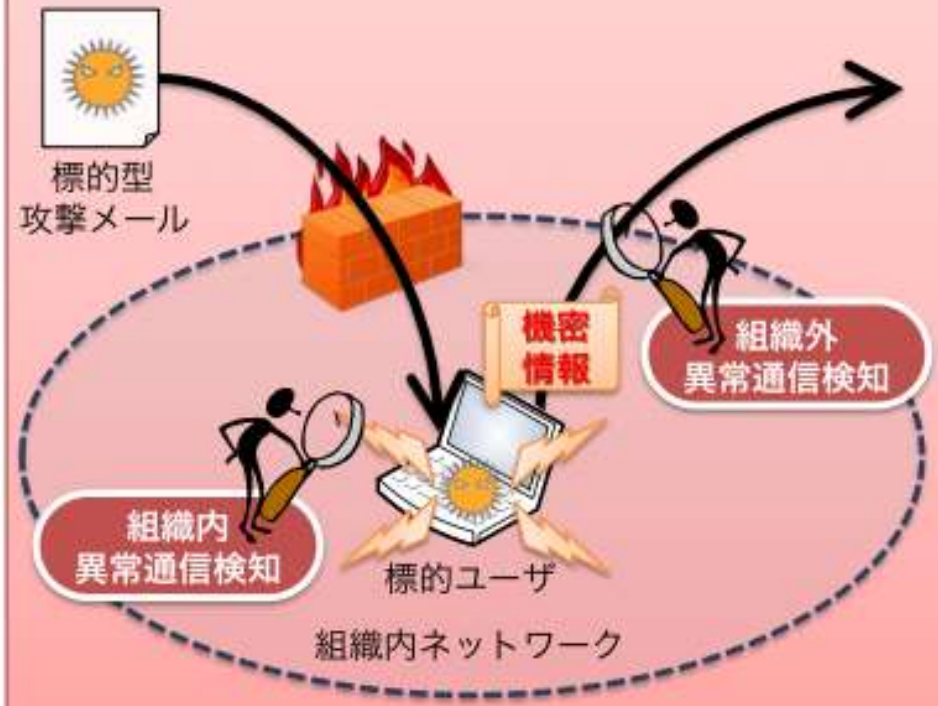
サイバーセキュリティ研究基盤NONSTOP

NICT サイバーセキュリティ研究室の研究概要 (3/3)

★標的型攻撃対策技術

システムではなく人間を狙った攻撃であるため
マルウェア感染を100%防止することは困難

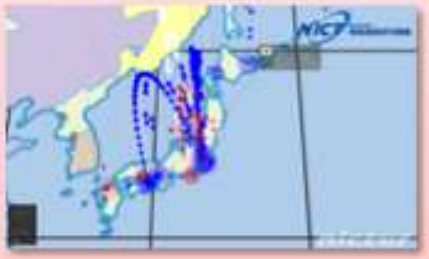
→ 感染後のマルウェアの活動を迅速に検知

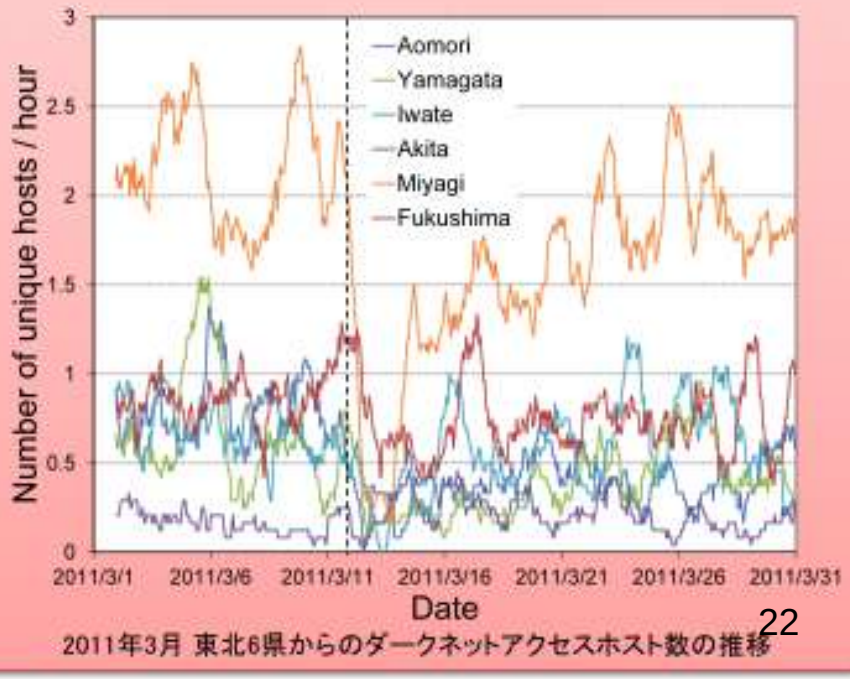


★ダークネット観測網災害応用技術

平常時：ダークネットにアクセス×（感染）
災害時：ダークネットにアクセス◎（疎通）

→ 被災地のネットワーク
死活状況を推定





2011年3月 東北6県からのダークネットアクセスホスト数の推移

まとめ

- サイバー攻撃の高度化
  - ✓ 絨毯爆撃型 → ピンポイント型
- サイバーセキュリティR&D
  - ✓ 新たな観測・分析の仕組みが必要
- All Japan体制の産学官連携が必須