資料１－６

最近の目に見えない脅威と情報セキュリティ対策について

（「次世代の情報セキュリティ政策に関する研究会」のために）

KDDI株式会社　情報セキュリティフェロー
NICT　インシデント対策G　リーダー

中尾　康二

近年のインターネットにおける脅威
（別スライドを用いて説明）

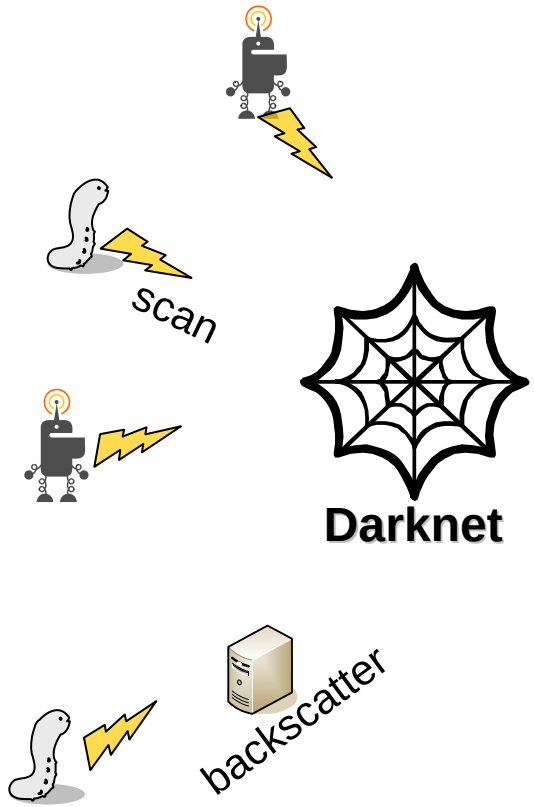
ダークネットでモニターを

- ダークネットとは、実ホストが存在しない
  未使用アドレス（ブロック）

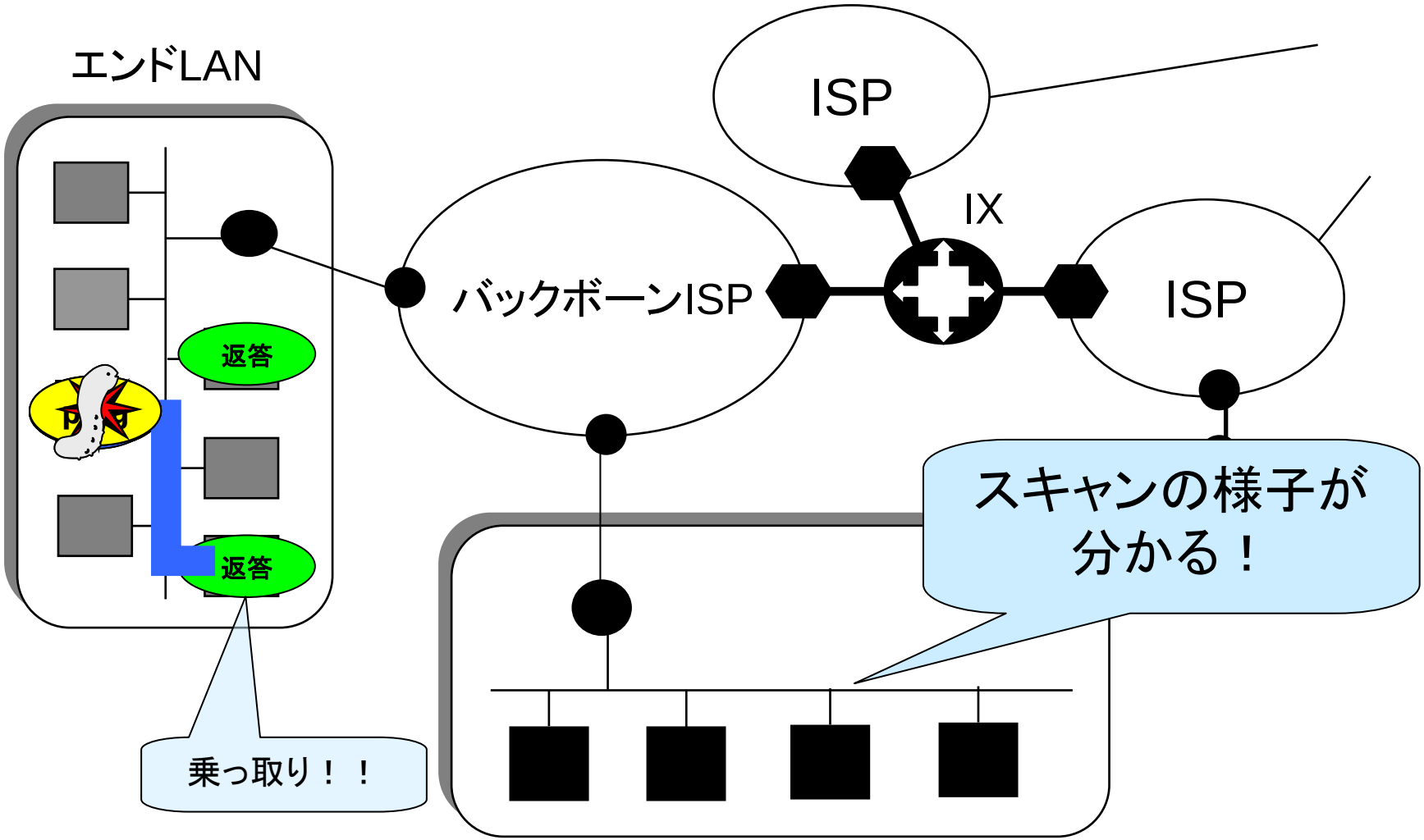
- ダークネットに届くパケットは
  - マルウェアによるスキャン
  - マルウェア本体の感染行為（主にUDP）
  - DDoS攻撃のBackscatter
  - 設定ミス

  などが原因。

- インターネット上で広範囲に影響を与える攻撃の把握に役立つ。

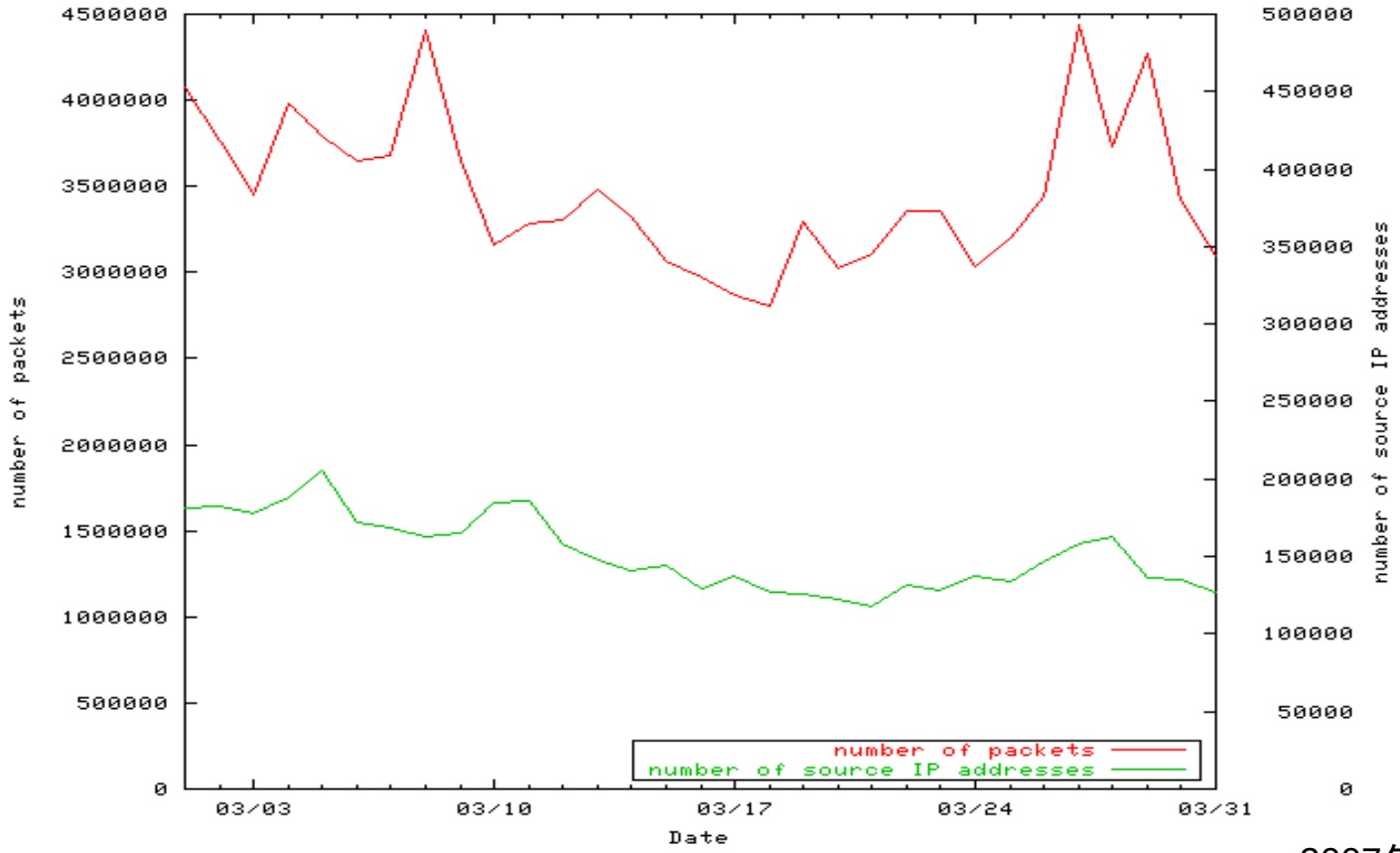


マルウェアの感染の様子とダークネットによる監視



ダークネットにパケットなんて届くの？

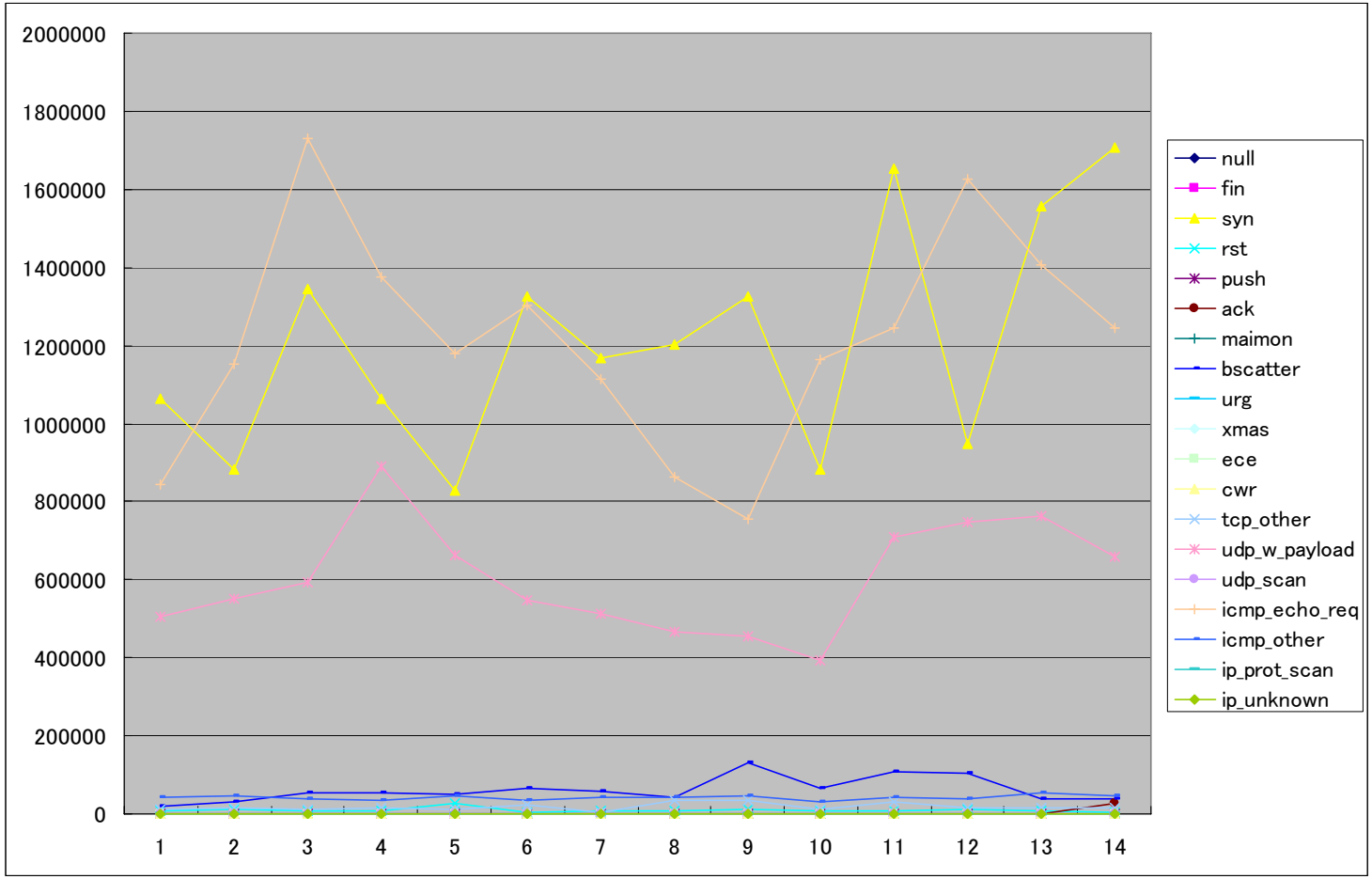
こんなに届くんです！（nicter /16 アドレスブロックの例）



2007年3月1～31日

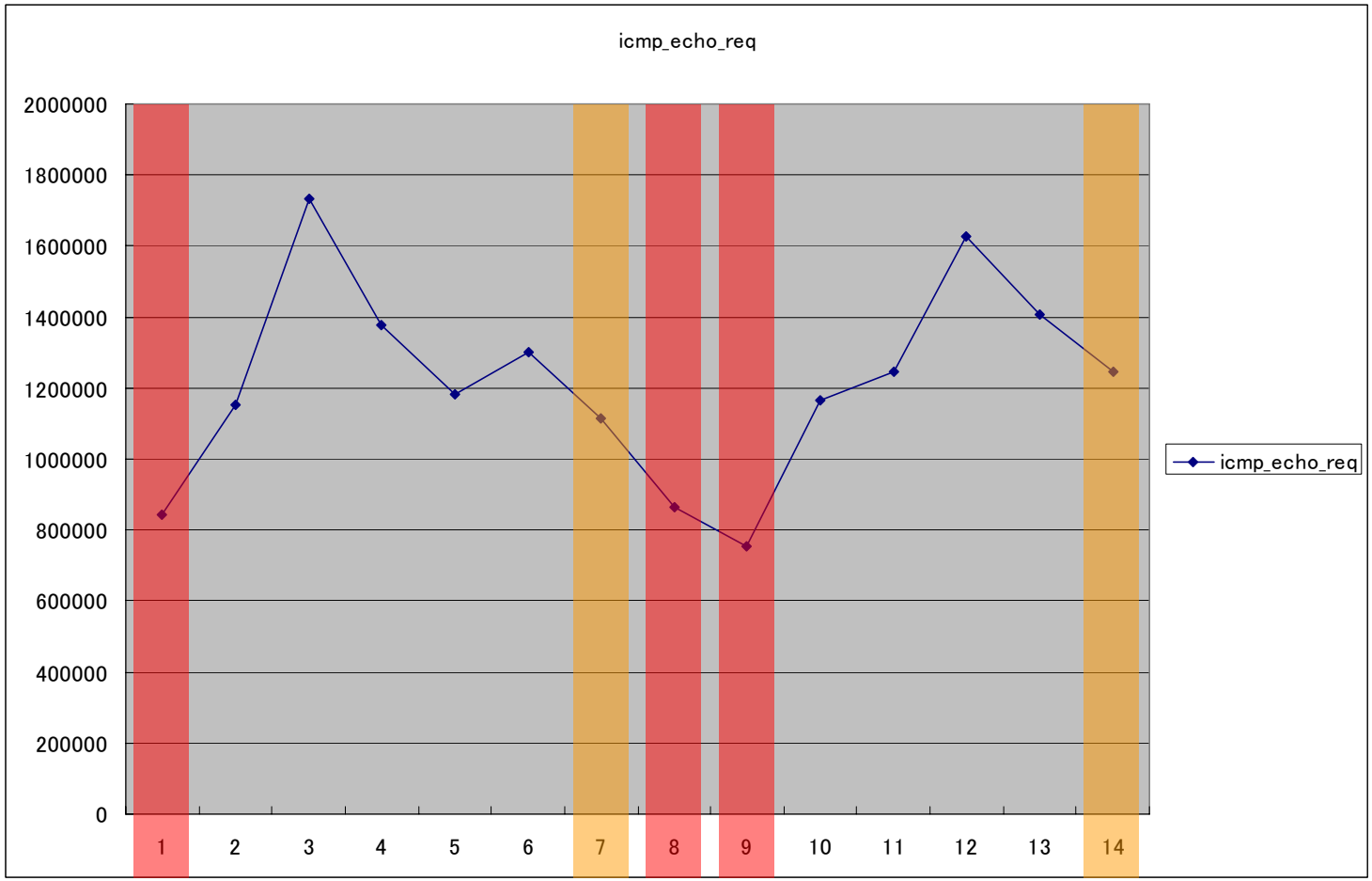
1日あたり 約350万パケット / 約15万ホス

2006年10月1日～14日の傾向（nicterセンサ）

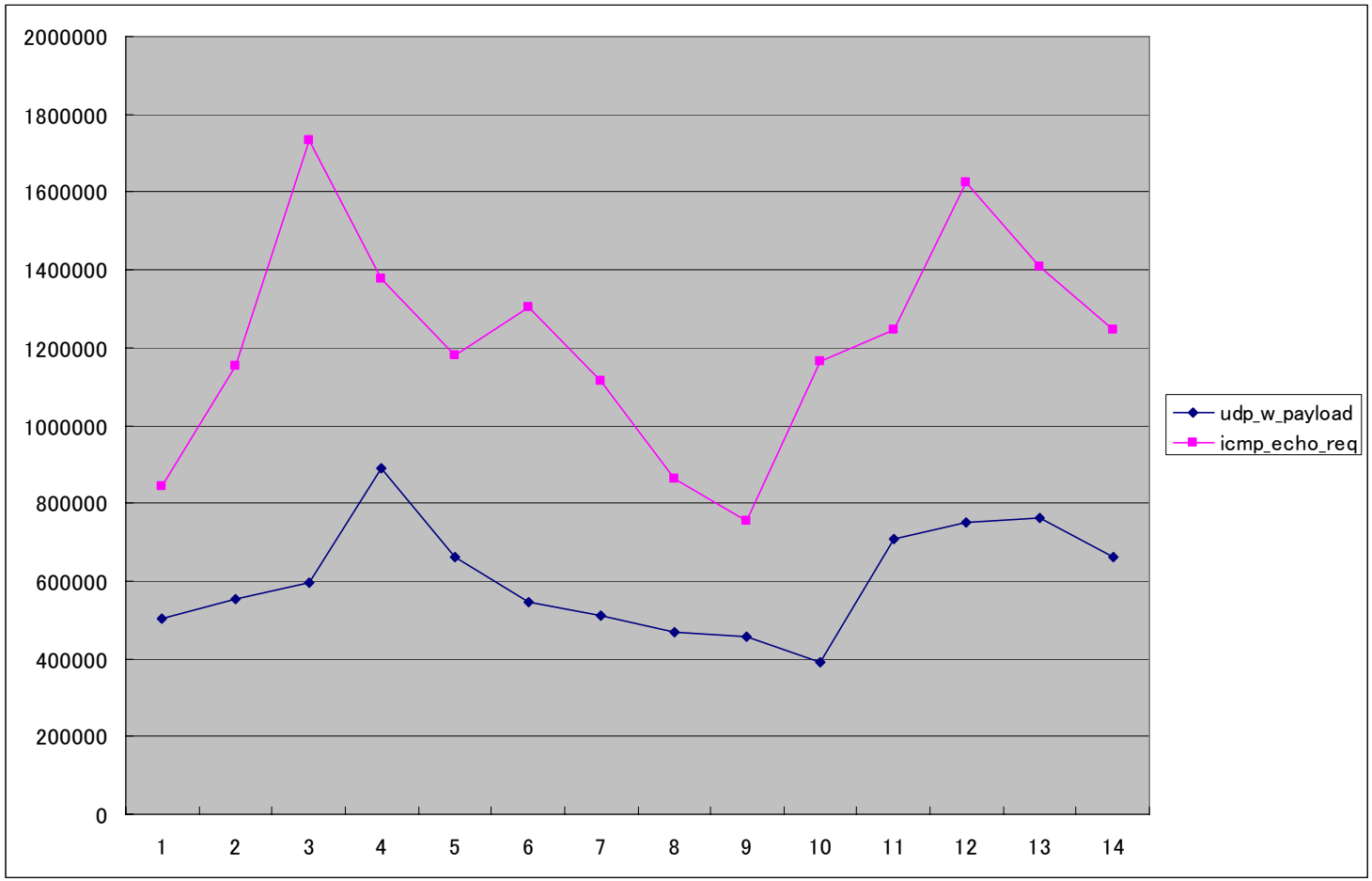


1位 ICMP Echo Request
2位 TCP SYN
3位 UDP with Payload

ICMP Echo Request



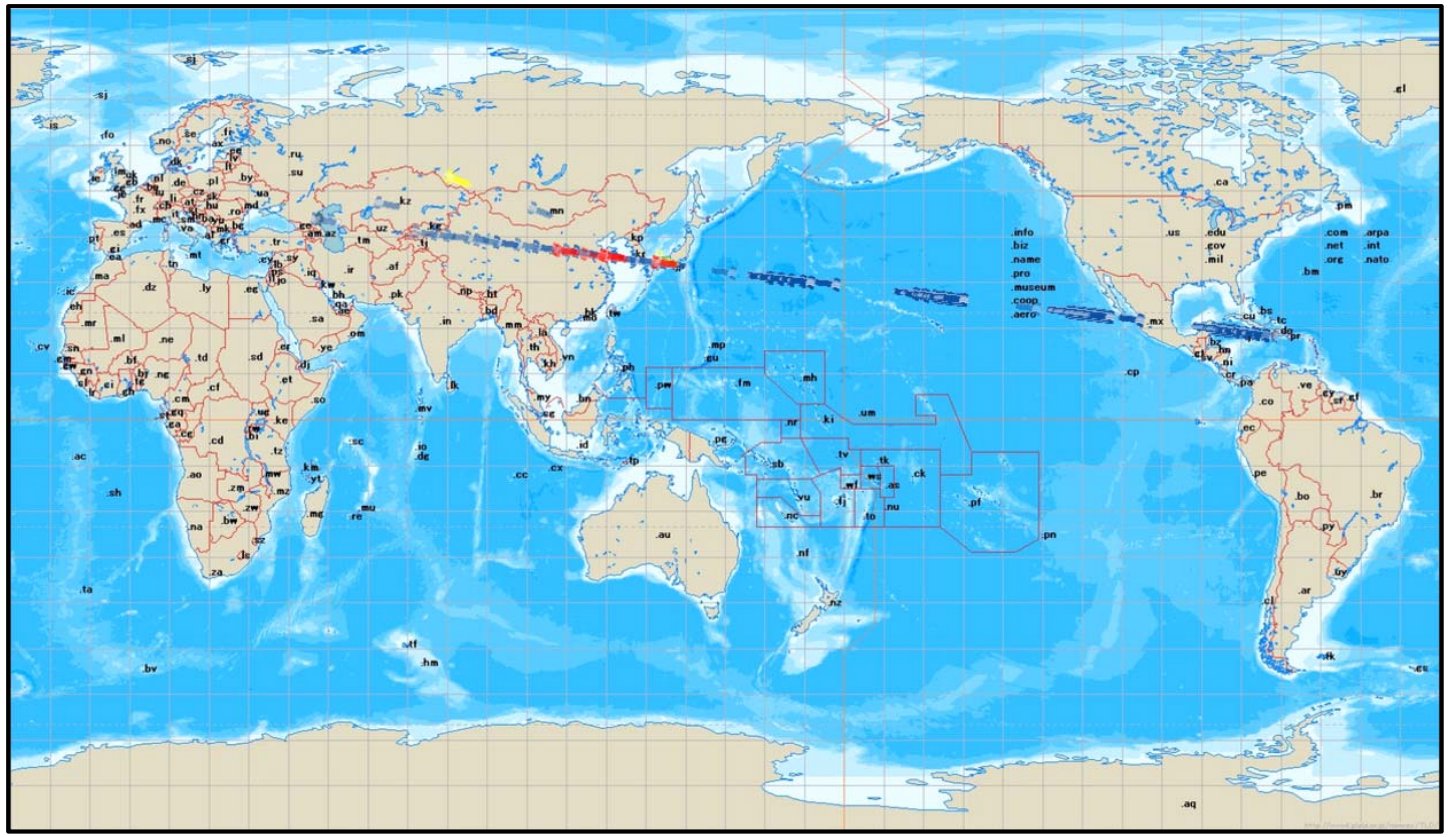
UDP（ペイロードあり）とICMP Echo Request



傾向が極端に類似。

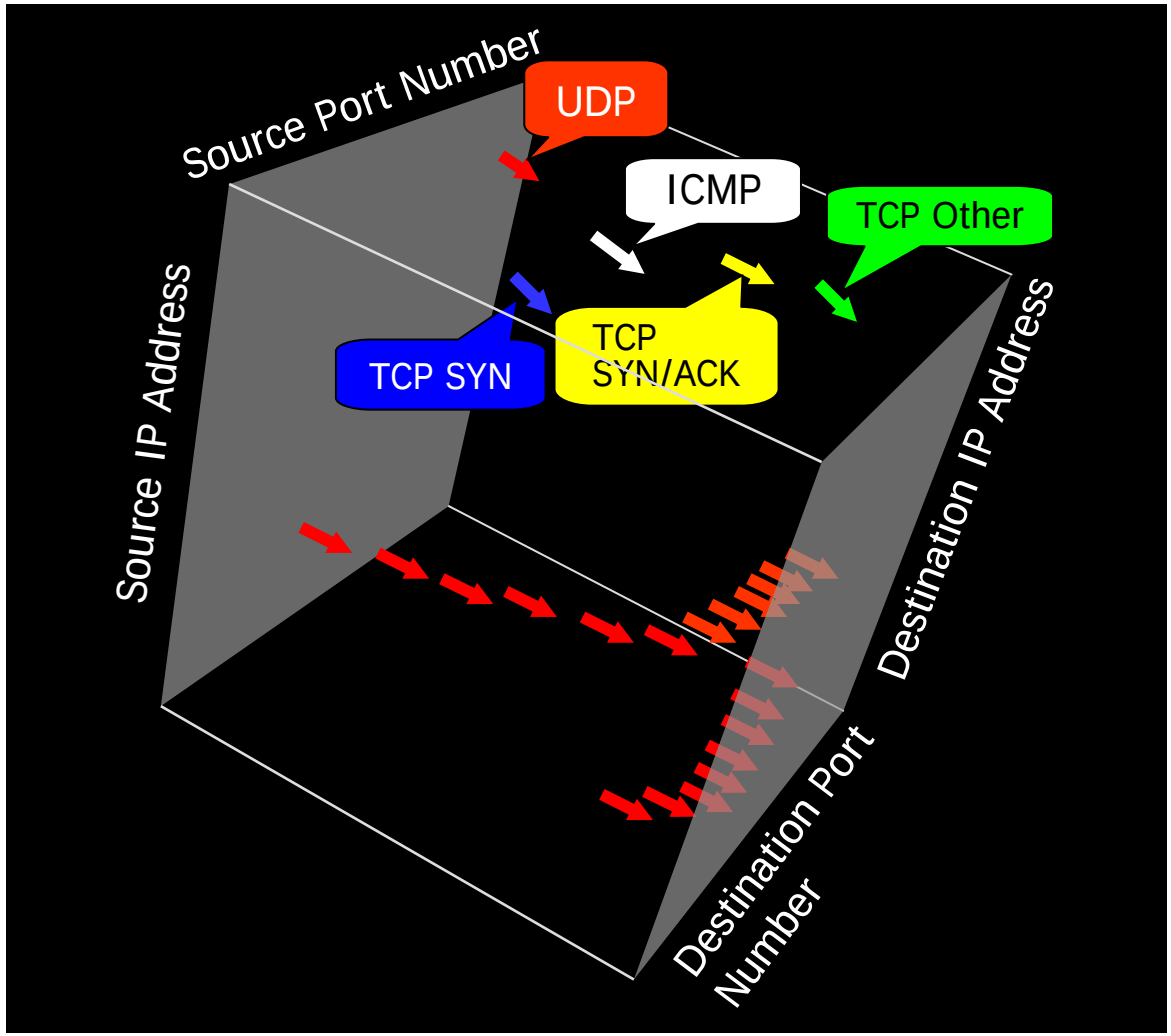
ダークネット・トラヒックの世界地図上での可視化

- ダークネットに飛来する各種攻撃パケットの発信元アドレスをもとに、世界地図上でリアルタイムに可視化。



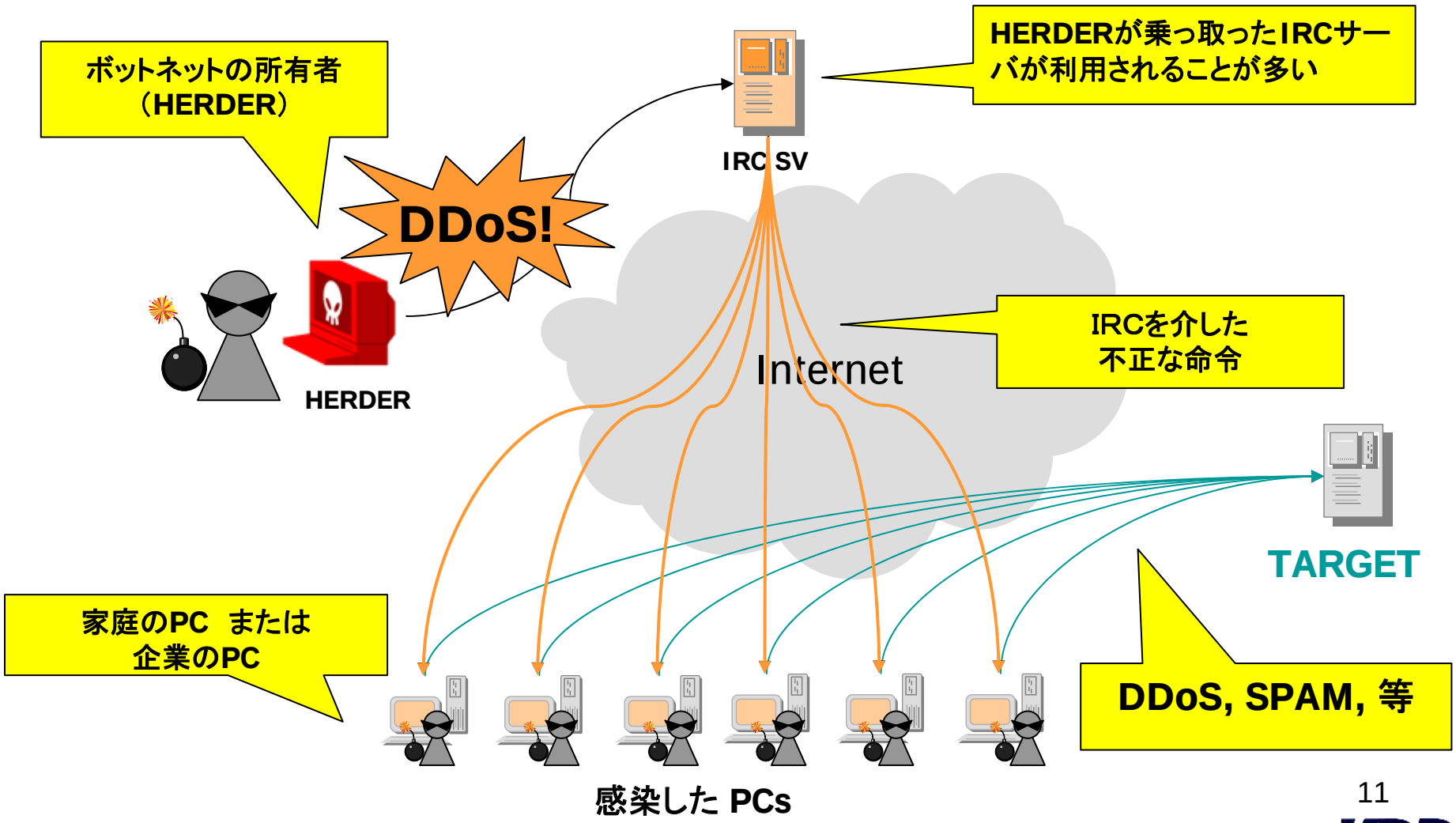
ダークネット・トラヒックの3次元空間上での可視化

- 3次元空間上でダークネット・トラヒックを可視化
- 左平面が攻撃元右平面が観測ネットワーク
- IPアドレスとポート番号を軸にとり3Dにマッピング

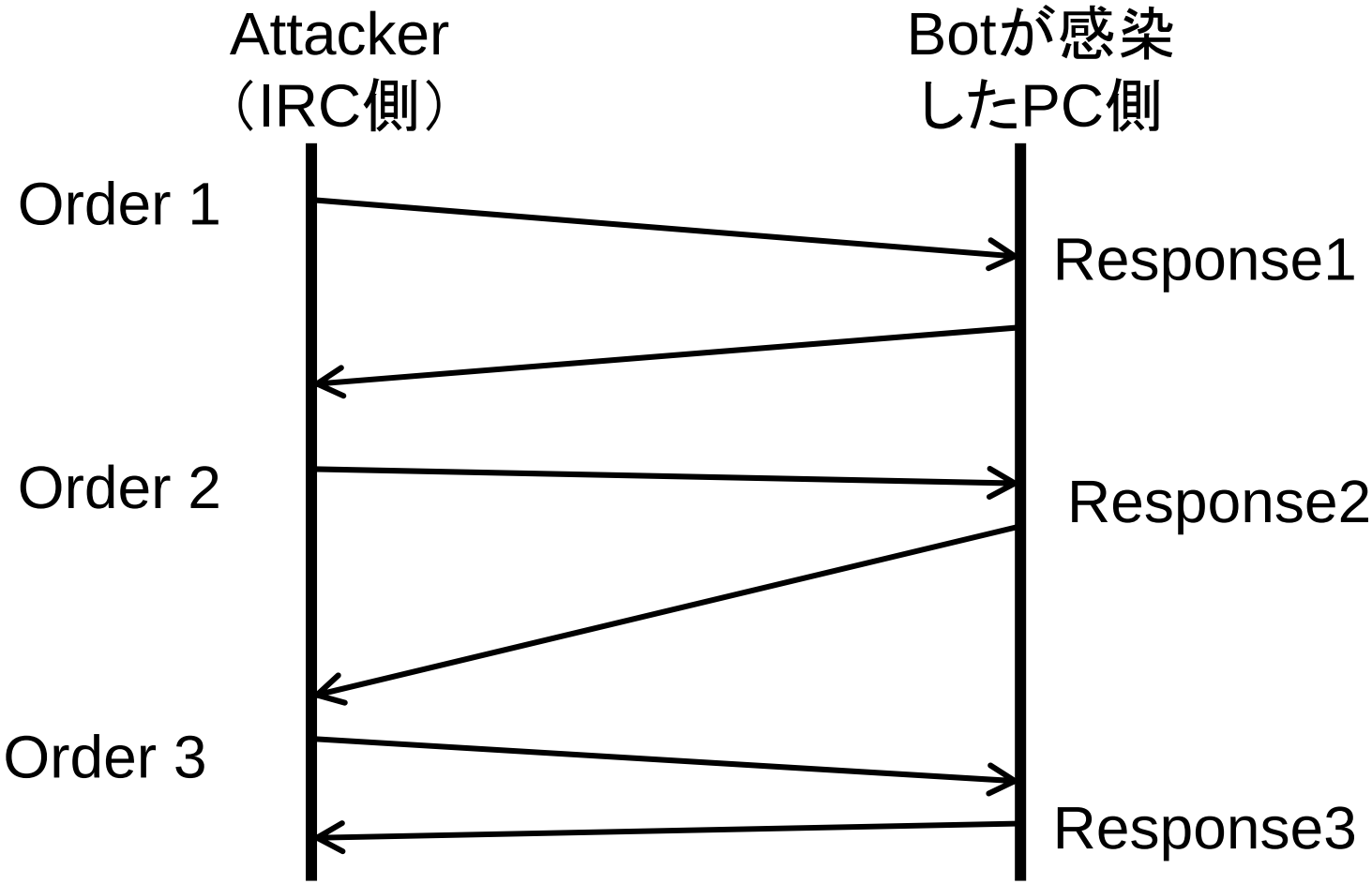


見えない脅威：ボットネット（Botnets）

According to analysis of Agobot source code.



IRCを介したHerder and Botの通信



IRC Protocol
（通常IRCプロトコルで利用されるコマンド）

NICK	**Inform Nickname to the Server (Nickname is an identifier)** Syntax: nick <nickname> Example: nick mikey
USER	**Inform Username to the Server** Syntax: user <username> <mode> <unused> :<real-name> Example: user ms-hattori 0 * :Masakazu Hattori
QUIT	**Termination of the connection** Syntax: quit [:<comment>] Example: quit :bye
JOIN	**Join the channel** Syntax: join <channel-names> [<keywords>] Example: join #TestChannel
PART	**Leave from the channel** Syntax: part <channel-names> [:<comment>] Example: part #TestChannel
PRIVMSG	**Send messages** Syntax: privmsg <nicknames or channel-names> :<message> Example: privmsg #TestChannel :Hi, guys!

SDBot.Bの場合のチャットやりとり

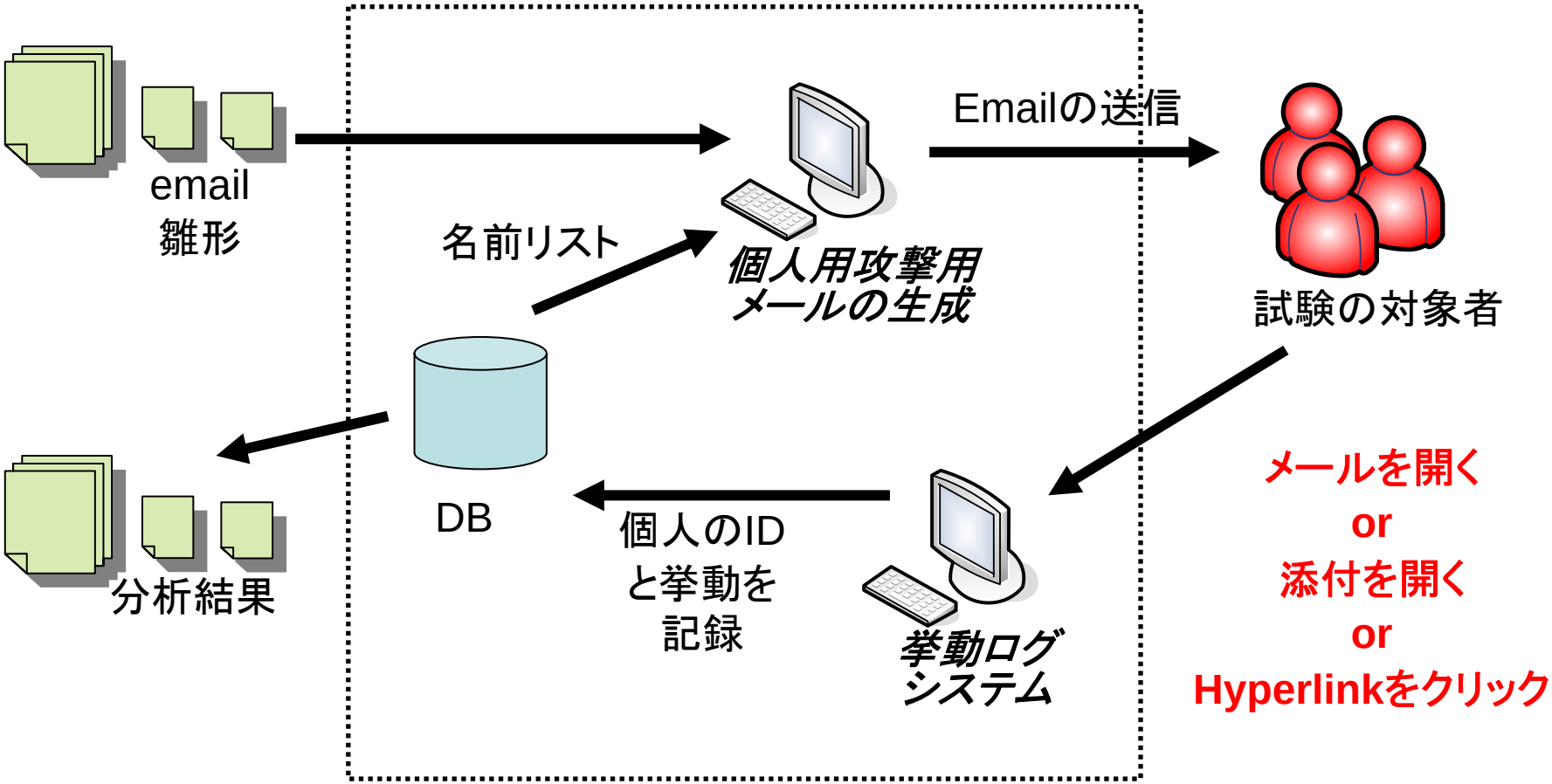
Sender	Content
Attacker	PRIVMSG #d3l3t3 :.login gr34t
Bot（PC側）	PRIVMSG #d3l3t3 :password accepted.
Attacker	PRIVMSG #d3l3t3 :.about
Bot（PC側）	PRIVMSG #d3l3t3 :mIRC v6.03 Khaled Mardam-Bey by [sd]
Attacker	PRIVMSG #d3l3t3 :.sysinfo
Bot（PC側）	PRIVMSG #d3l3t3 :cpu: 1300MHz. ram: 255MB total, 102MB free. os: Windows XP (5.1, build 2600). uptime: 0d 2h 27m. Current user: nakao
Attacker	**PRIVMSG #d3l3t3 :.syn 192.168.17.140 80 60**
Bot（PC側）	**PRIVMSG #d3l3t3 :SYN flooding [192.168.17.140:80] for 60 seconds**

Botの動画

見えない脅威：スピア型攻撃

「IPA　情報セキュリティ白書　2007」より抜粋

ソーシャルエンジニアリング試験



RAISS会議　中国の報告から

ソーシャルエンジニアリング試験の結果

- 6つのタイプの51，300の試験メールを8550人を対象に2006年12月の間に試験送信を実施
- *43．0%*の対象者がテストメールを開封
- *23．9%*の対象者がテストメールの添付、またはハイパーリングをクリック

見えない脅威：フィッシング

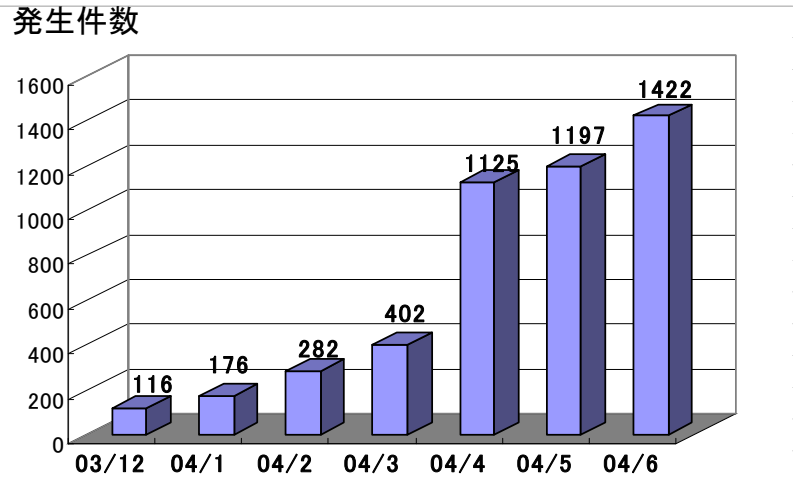
フィッシングとは、本物の金融機関などのHPをそっくりまねて作成された偽サイトを用意し、本物サイトに見せかけて信用させ、個人の口座番号やクレジットカード情報などを盗み取る手法である。
多くのフィッシングサイトは電子メール等で偽のお知らせを送り、同メールに記されているURLをクリックさせて偽サイトに誘導している。

◆これまでは、本物そっくりのHPを作成しても、URL(http://で始まるサイト名）は異なるため、このWebブラウザのURL表示部分（アドレスバー）を隠して表示させていたが、Internet Explorerのアドレスバーに偽URL情報を表示することが出来る不具合が発見されたため、今後はこれを利用してURLも本当のサイト名に偽った情報を表示させて信用させ、個人情報を入力させるような手法が広まることが懸念されている。

被害状況

米国：・発生件数　；176件（2004年1月）→1422件（6月）
・**被害総額　；24億ドル**（2004年4月まで）
・被害者数　；198万件（2003年中）

日本：まだ大々的な被害は報告されていないが、
①ある通信事業者や一部クレジット会社が会員向に注意案内を出している。
（日本語のフィッシングサイトが構築されている模様）
②ある通信事業者では、Iユーザの HPが改竄され、フィッシングサイトとして利用された
（2004・10～05・07　45件）



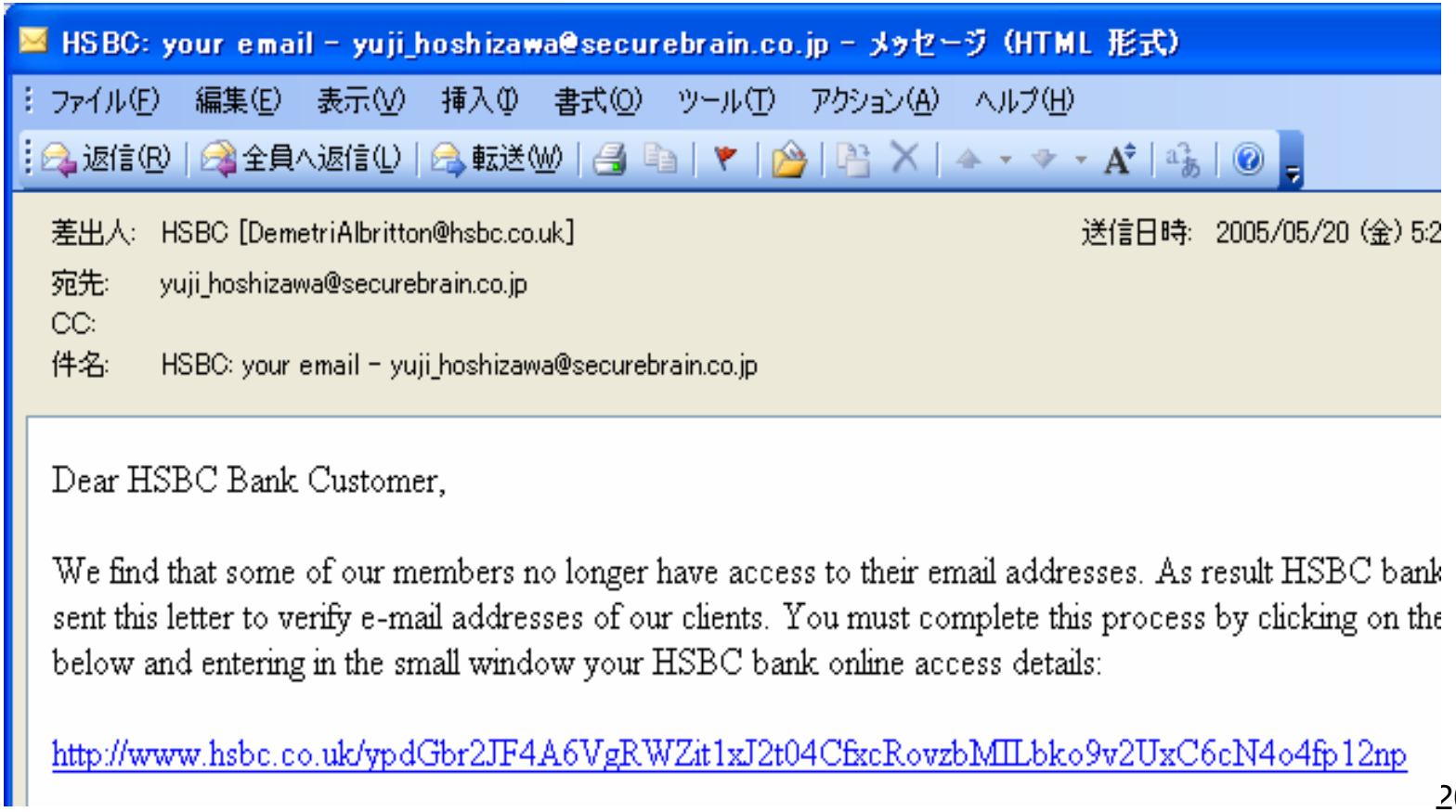
米国でのフィッシング件数は急増、被害は莫大！

・Fish（動詞）：（それとなく）[…を]手に入れようとする
・so**ph**isticated されたメールを悪用する

フィッシングメール事例1

SecureBrain

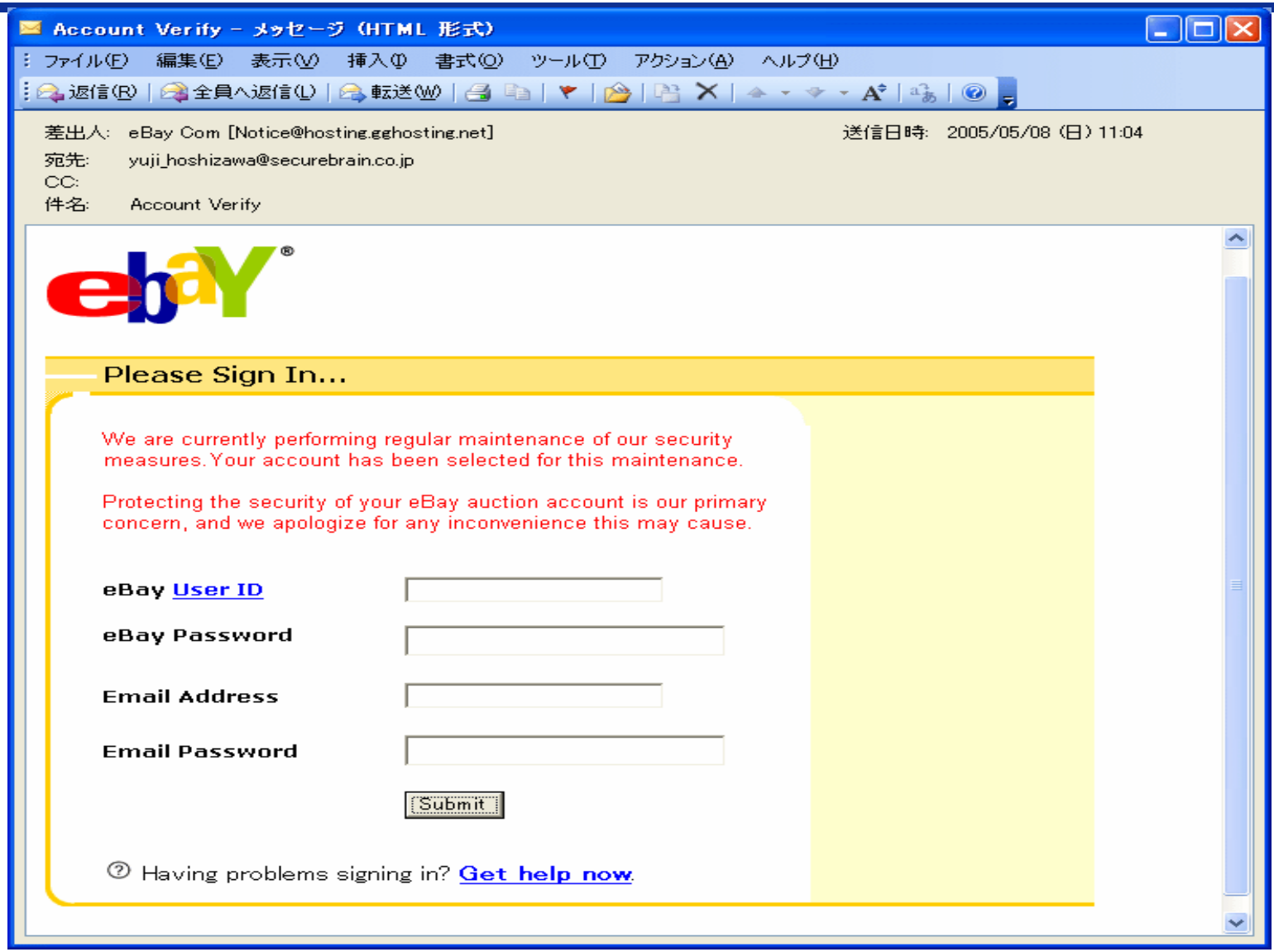
- 差出人を詐称し、件名に受信者のメールアドレスを挿入している。本文は一見テキストメールのように見えるがHTMLメール



KDDI

フィッシングメール事例2

SecureBrain

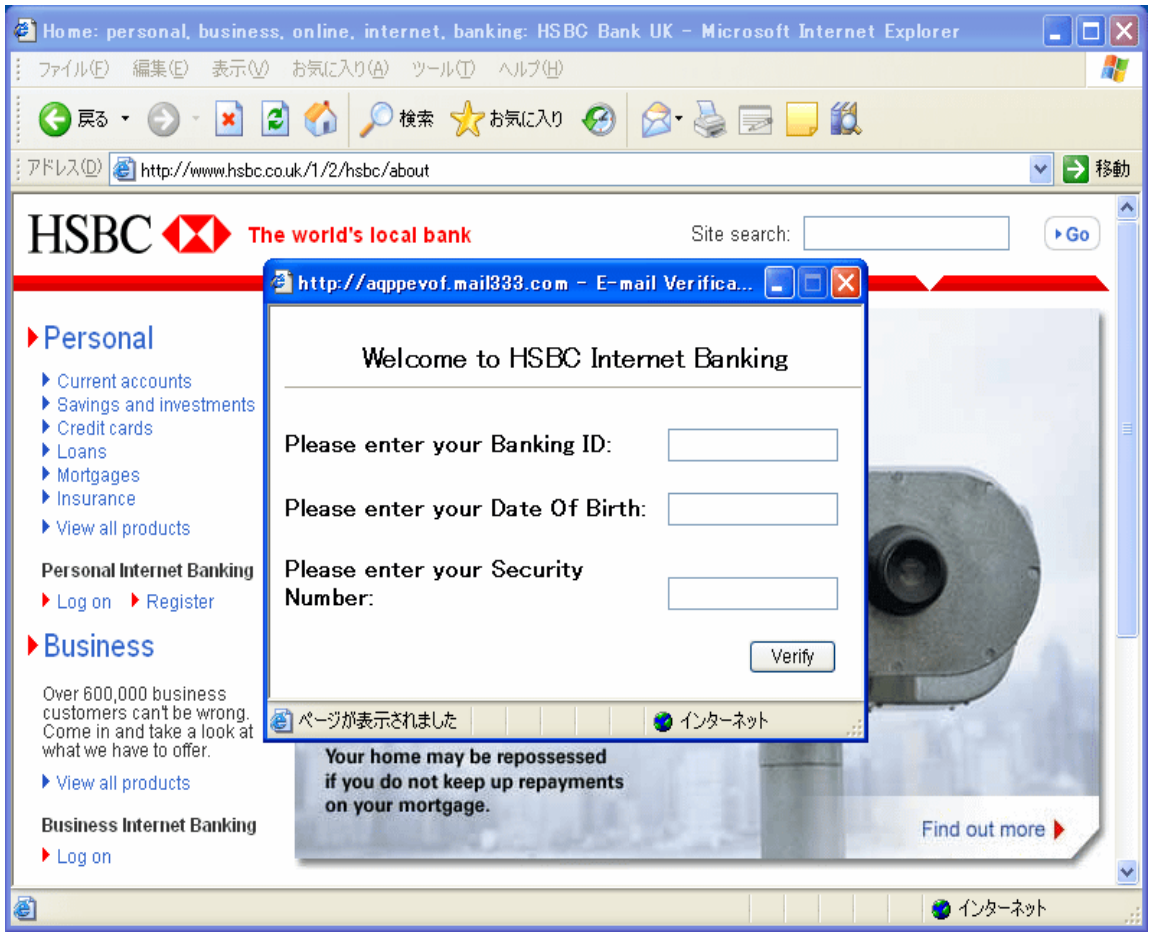


KDDI

ポップアップウィンドウ事例3

SecureBrain

- 偽の入力画面を本物らしく見せるため、バックグラウンドに本物のサイトを表示する。

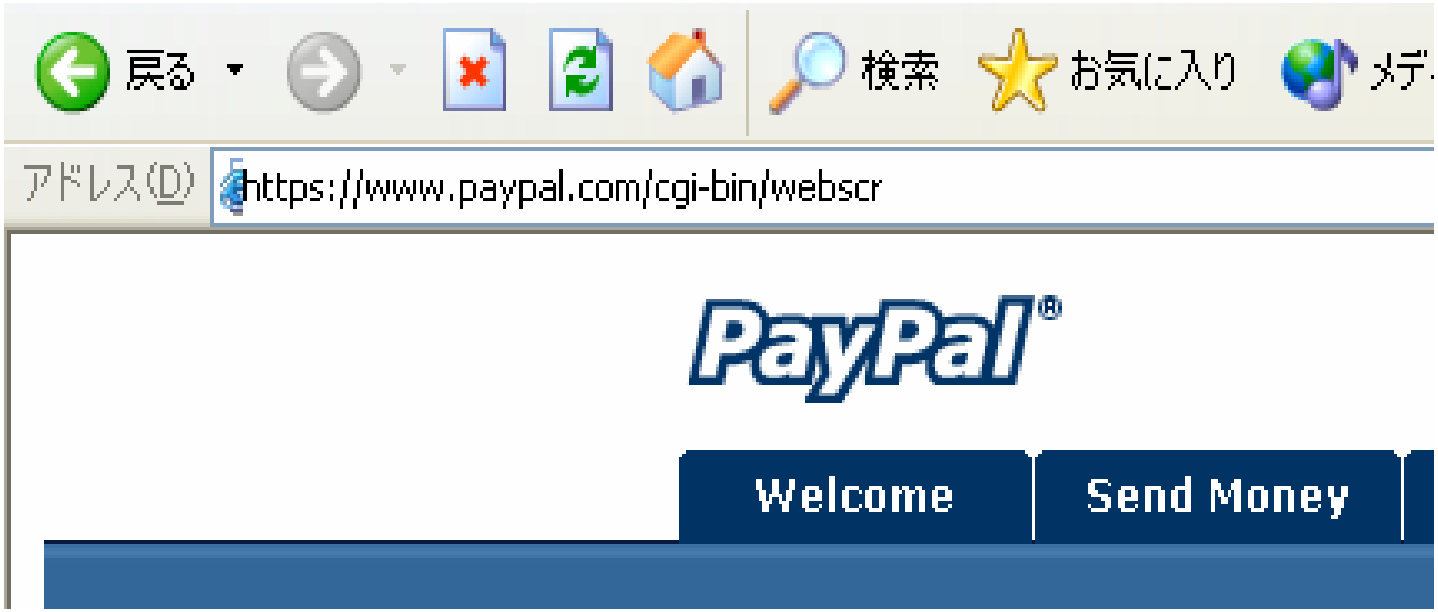


KDDI

アドレスバー偽装　事例4

SecureBrain

- ポップアップウィンドウでアドレスバーを偽装する手口。アドレスバー上にそれらしい文字列を配したポップアップウィンドウを表示し、実際にアクセスしているURLを隠している

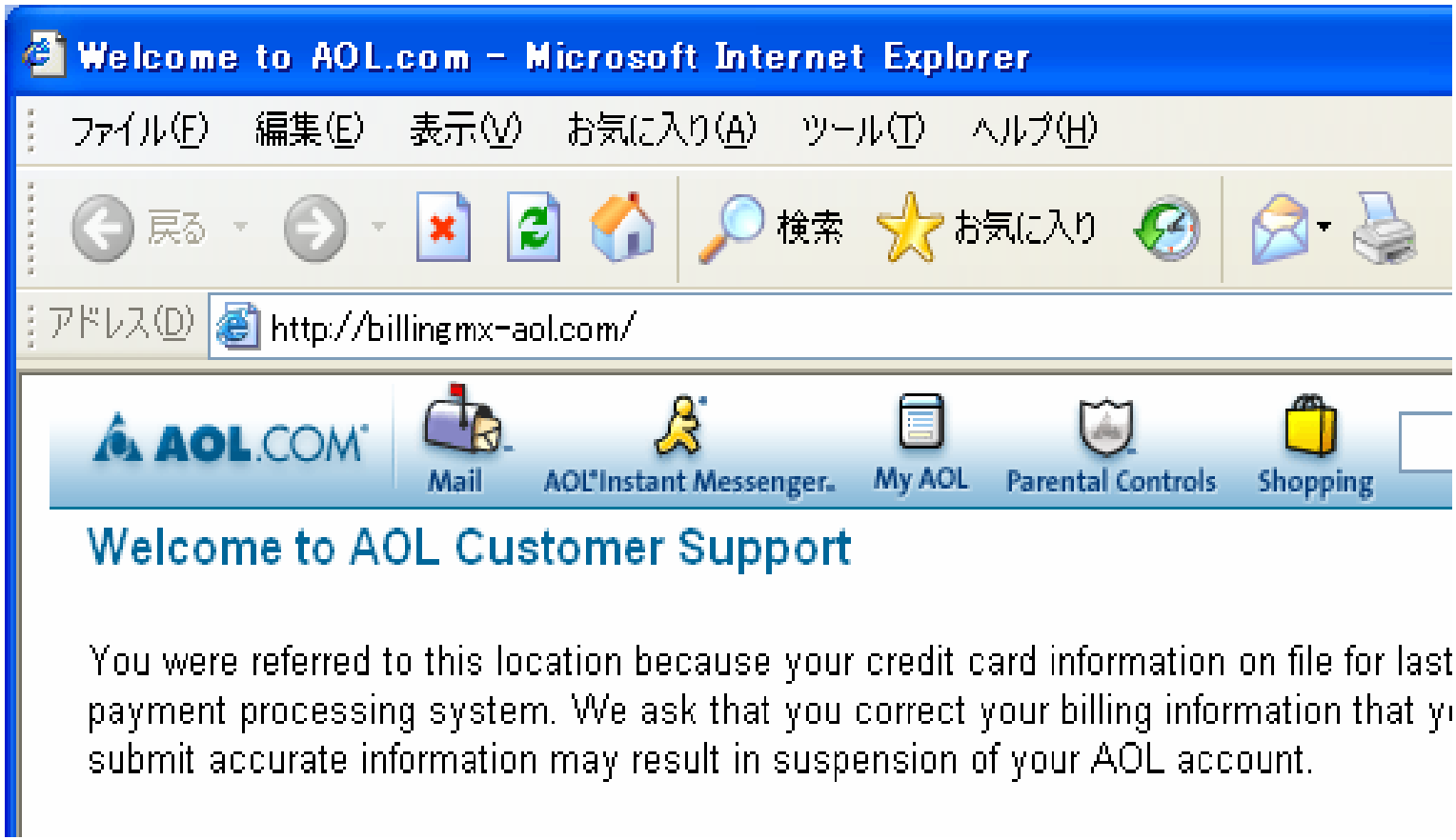


KDDI

紛らわしいURL　事例5 (1/3)

SecureBrain

- 会社名の一部などを使った紛らわしいURLで騙す



KDDI

紛らわしいURL　事例5 (2/3)

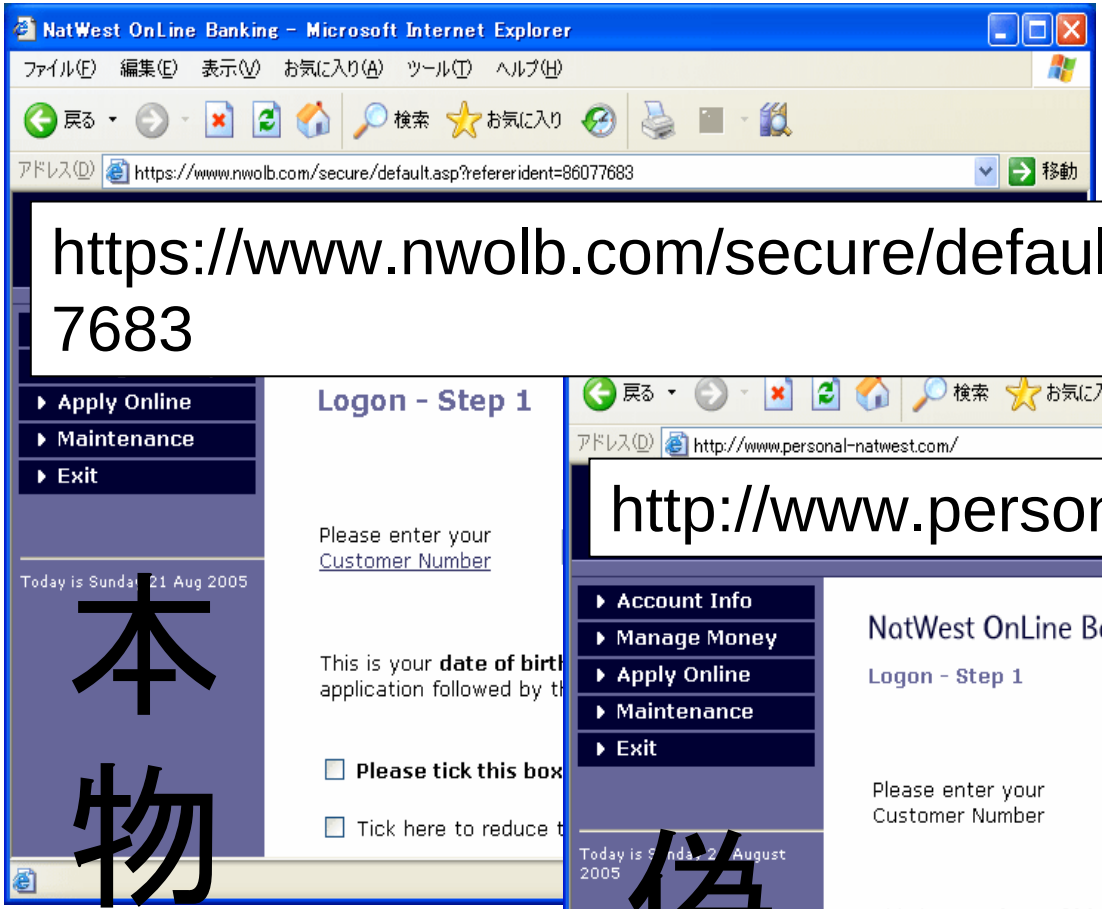
SecureBrain

- msnbillingupdate.com
- userpage-charterone.com
- ebay.member-security.com/.eBay/
- ebay-loginpage.com
- paypal-com-us.com
- www.paypal.com.international-transaction.info
- protect-paypal.com
- online-hsbc.com
- www.paypal.com-cgi-bin.biz
- nicos.concourse.jp
- regionsbank.com.dish2.net.ibizdns.com
- www.fraud-control.net/paypal/
- staff.earthlink-box.net

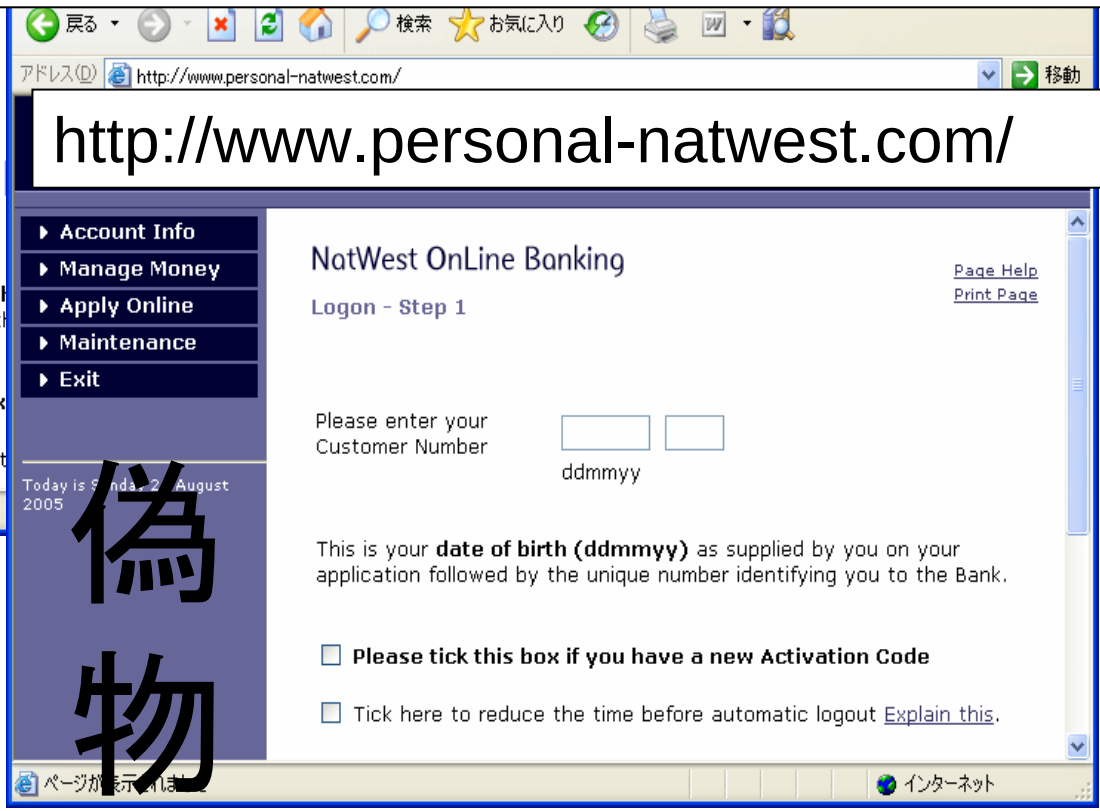
KDDI

紛らわしいURL　事例5 (3/3)

SecureBrain



https://www.nwolb.com/secure/default.asp?refererident=86077683



http://www.personal-natwest.com/

KDDI

フィッシング対策 (1/2)

SecureBrain

- 利用者の自衛手段
  - メール中のリンクは安易にクリックしない
  - 個人情報をメールで送信しない
  - ブラウザには最新のパッチを当てる
  - 個人情報を送信する前に鍵マークを確認する
  - サーバ証明書で本物のサイトかどうかチェックする
  - 目的のサイトにはブラウザのブックマークからアクセスするか、直接アドレスを入力してアクセスする
  - アドレスバーのURLを確認する
  - アンチウイルスを正しく使う

KDDI

フィッシング対策 (2/2)

SecureBrain

- メールにおける対策
  - アンチスパム技術でフィッシングメールを検出する
  - 送信ドメイン認証技術でメールの送信元が信頼できるものかどうか確認する
- Webにおける対策
  - URLフィルタリングで偽サイトを訪問させない
  - サーバ証明書を認証する事により、通信相手が本物に間違いない事を確認する

KDDI

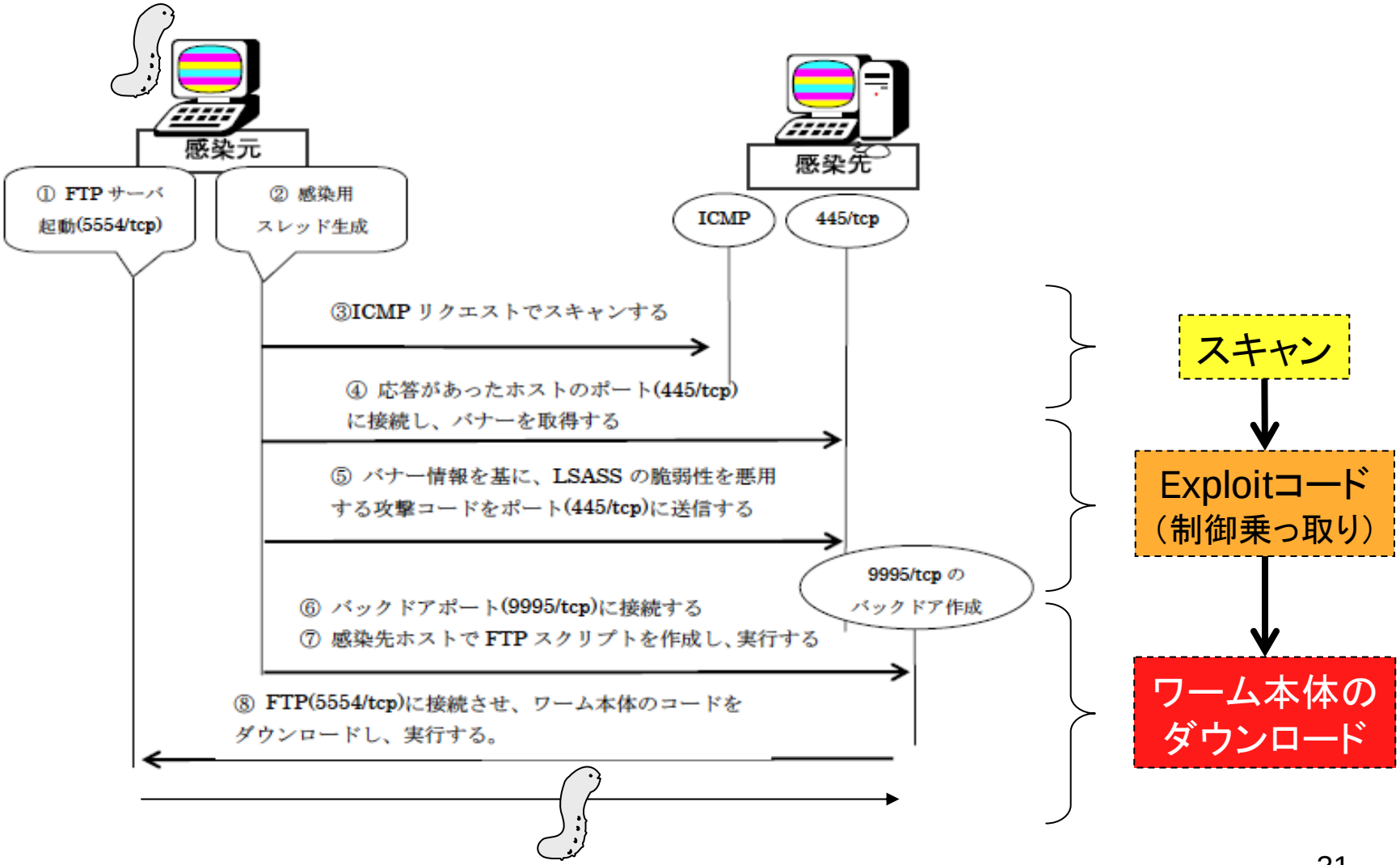
ウイルス/ワークに関連する最新技術

- 攻撃シナリオ
- 国内外の動向概要
- NICTの研究開発の紹介

マルウェア（ウイルス・ワーム・ボット）の主な感染経路

- **ファイル媒介型**
  - 実行ファイル (.exe, .bat など) や一般のファイル (.doc, .xls など) に自分自身，あるいは不正なマクロを組み込み，他のコンピュータに持ち込まれるのを待つ
- **電子メール媒介型 (マスメーラ型)**
  - 電子メールの添付ファイルとして拡散する．誤って実行すると．使用者のアドレス帳に登録された宛先に自分自身を添付して再送信する
- **Web 媒介型**
  - 通常の Web ページを装いながら，内部に Web ブラウザの脆弱性を攻撃するスクリプトを含み，その Web ページを参照したユーザのホストに感染する
- **リモート侵入（脆弱性攻撃）型 (ワーム)**
  - ネットワーク越しに，ホストのセキュリティホールを攻撃し，対象の制御を奪う．侵入に成功したホストを踏み台にしてさらに感染を広げるものが多い．感染．流行の速度が非常に速い．

ワームの感染例(Sasser.Dの例)（警察庁 *@Police* より）



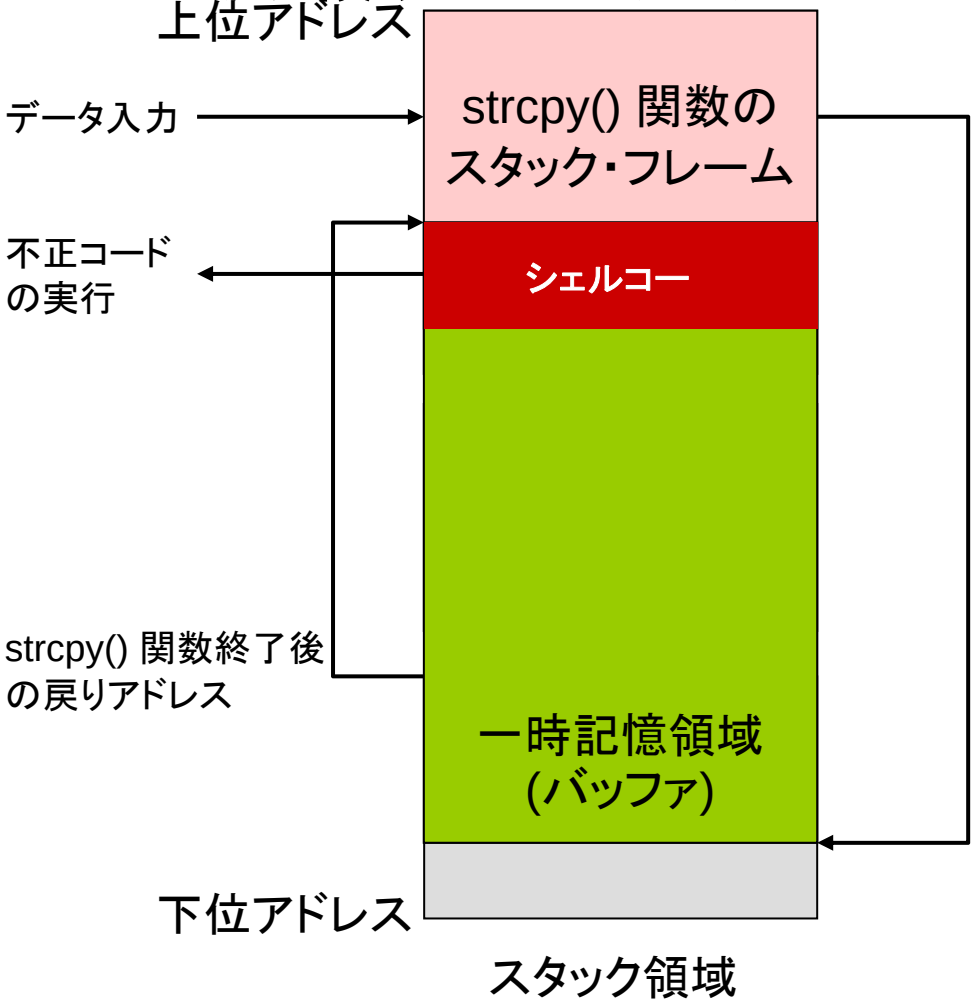
Exploitコード

- ネットワーク越しに攻撃対象ホストへ特定のデータ列を送り込み，任意のコマンドを実行させる
  - サービスアプリケーションが持つバッファオーバーフロー等の脆弱性を悪用した攻撃
  - 実行される任意のコマンドは，ユーザアカウントの作成や管理者パスワードの変更，悪意のプログラムのダウンロードなどを行う

- サービスアプリケーションの開発時に，入力データ長のチェックを行っていないことが原因
  - 想定したデータ長を大きく上回るデータが入力され，メモリ空間(バッファ) に書き込まれることで，任意のコマンドが実行される

バッファオーバーフロー攻撃

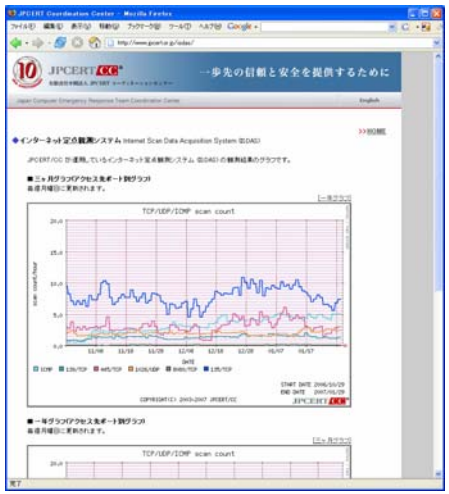
- スタック領域でのバッファオーバーフロー攻撃



スタック領域:
主にデータの一時的な保存のために確保されたメモリ領域
strcpy() 関数:
文字列のコピーを行う標準関数
一時記憶領域 (バッファ):
コピーのために一時的にデータを保存する場所

日本国内の広域ネットワーク観測技術

- インターネット定点観測システム (日本)
  - 広範囲に配置されたセンサからトラフィック情報を収集し，宛先ポート，プロトコル別の傾向や，発信元の国家/地域別の統計情報などを公開
    - ISDAS – JPCERT/CC
    - @police – 警察庁
    - TALOT2 – IPA
    - WCLSCAN – 鈴木裕信氏ほか
    - TINY – Telecom-ISAC



[ISDAS]

[@police]

[WCLSCAN]

海外での取り組み

- ミシガン大学 (アメリカ)
  - Internet Motion Sensor (IMS)
  - 広範囲にわたる未使用アドレスブロックの観測プロジェクト．一部のパケットに応答を返し TCP コネクションを結ぶことで，より詳細な情報の取得を目指す．

[IMS]

- EureCOM (フランス)
  - Leurrecom と呼ばれる世界中に分散するハニーポットによる情報収集プロジェクト (40 組織，25 カ国 / 地域)

[Leurrecom]

- REN-ISAC (アメリカ)
  - Internet2 (“Abilene” backbone network) で観測されるトラフィックを分析し，“Daily Weather Reports” としてネットワーク上の攻撃状況のレポートを行う．

[REN-ISAC]

- Korea Internet Security Center (KISC) (韓国)
  - National Cyber Security Center (NCSC)，および Defense Security Command (国軍機務司令部) の共同プロジェクト
  - ハニーポットや隔離された環境でのボットの実行・解析を行い，ボットネットの検出と機能停止に取り組む．

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

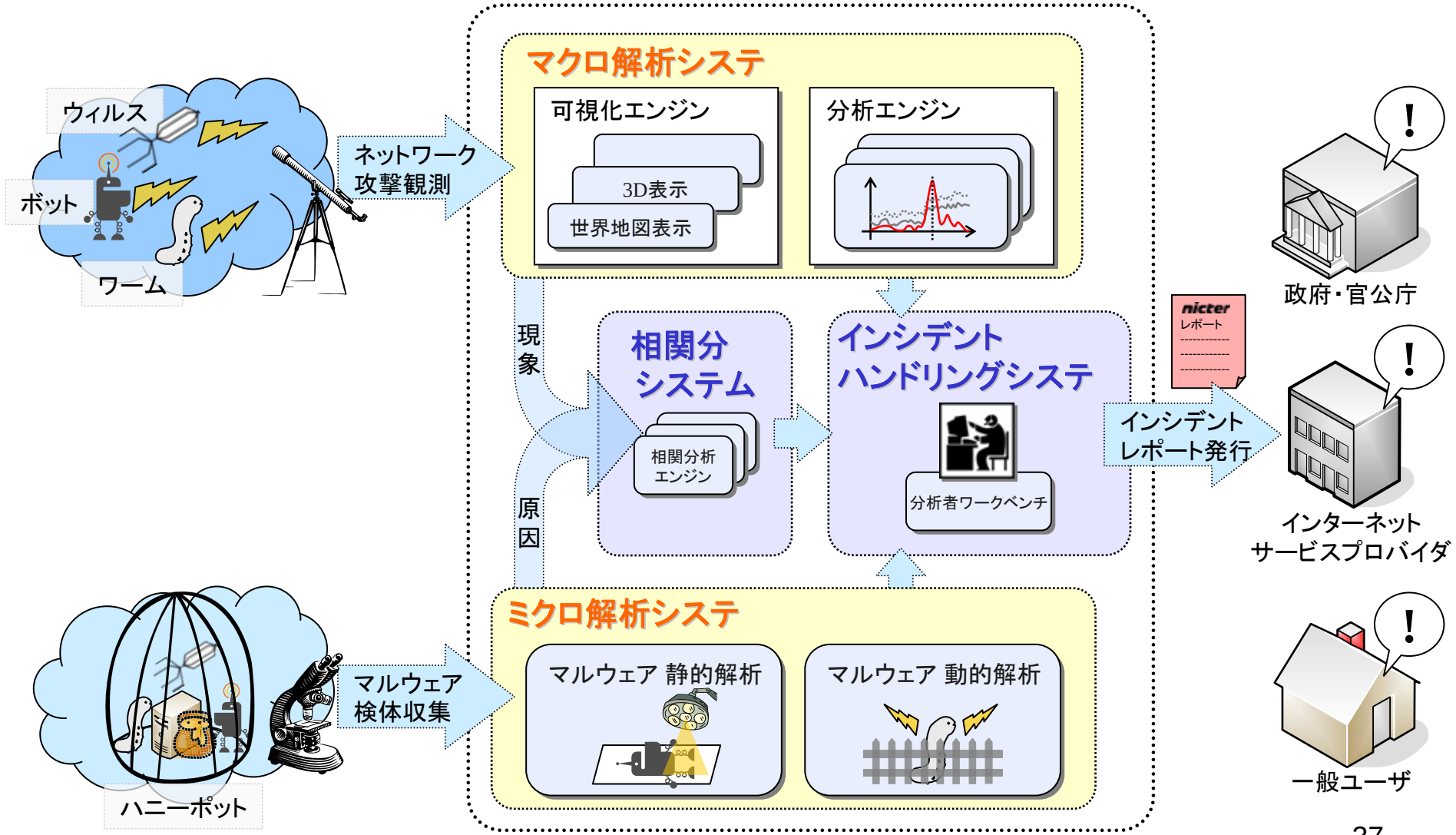
目的:

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）の統合的分析とその対策。

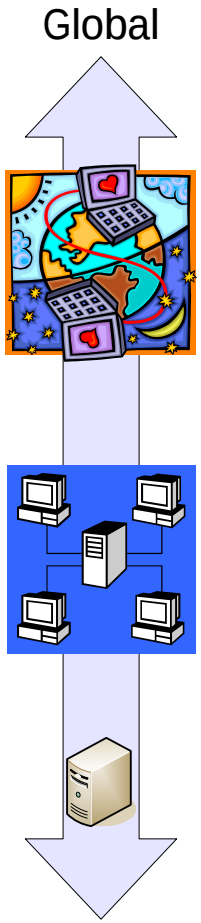
主要コンポーネント

- 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



nicterの情報源



- **ISPからの実トラヒック**
  - ペイロード等のプライバシ情報の匿名化が課題
- **ダークネット**による観測トラヒック（400-600MB/day）
  - 実ホストの存在しない未使用アドレス(群)-10万以上のIPアドレスを観測
  - Incomingパケットは攻撃の可能性が非常に高い
- **国内大学NWに設置されたIDSのログ (100MB/day)**
- **ハニーポット・ダミーメールアカウント・Webクローラ**
  - 脆弱なホストに見せかけ、攻撃コード、マルウェア検体を取得
  - メール添付型ウイルスを収集するために多数のダミーアカウントを用意
  - Webクローラでメールアーカイブを取得し、メール添付型ウイルスを収集

マクロ解析システム
（MacS: Macro analysis System）

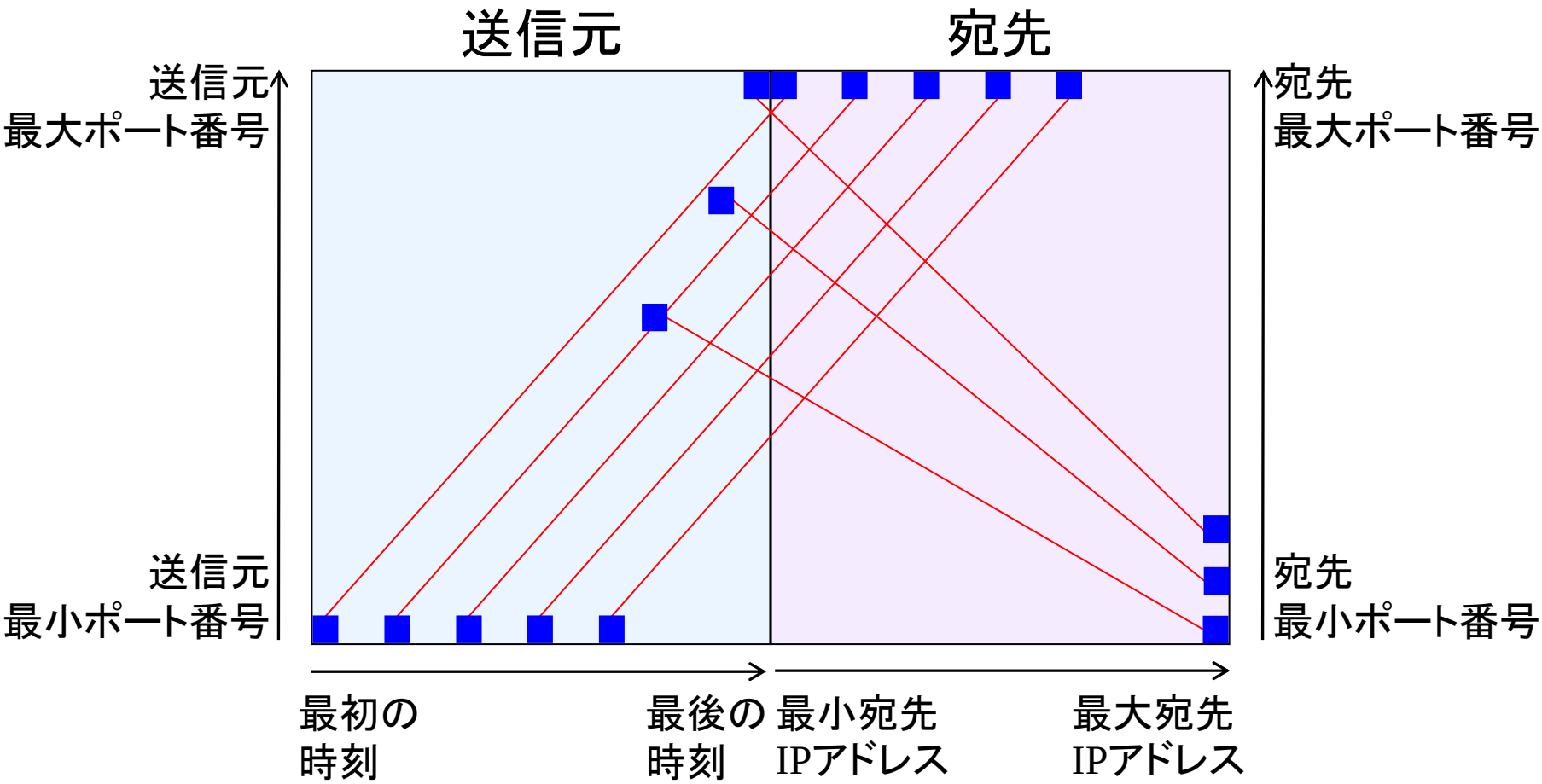
振舞分析と変化点検出

- **振舞分析**：TAP（Traffic Analysis & Profiling）
  - 攻撃ホスト（送信元IPアドレス）ごとに短時間（30秒）の挙動を分析
  - スキャンの振舞を以下のパラメータによって自動分類しDB化
    - 送信元ポート番号
    - 宛先IPアドレス/ポート番号
    - プロトコル種別
    - シーケンシャル/ランダムスキャン
  - **新規の攻撃パターン**を自動検出

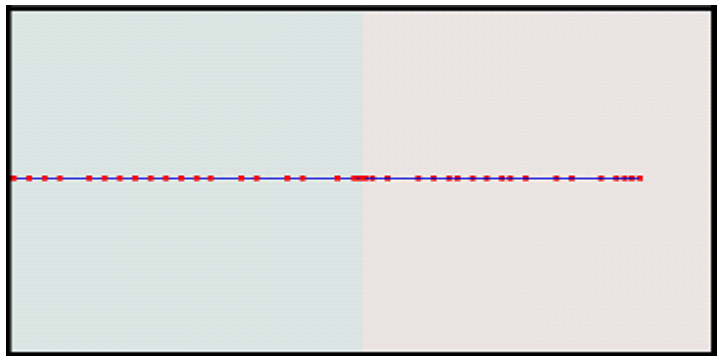
- **変化点検出**: CPD（Change Point Detector）
  - 観測トラヒックの**急激な変化**を自動検出

振舞分析(TAP)の可視化

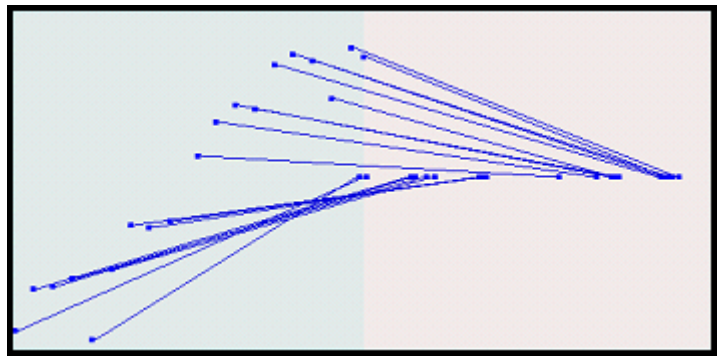
- 攻撃ホストごとに、その挙動を描画。



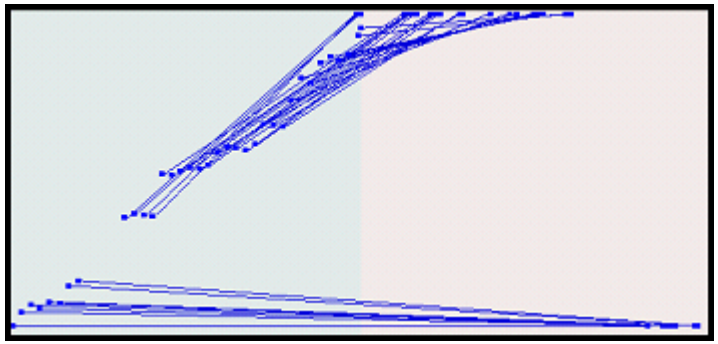
振舞分析(TAP)の可視化の例



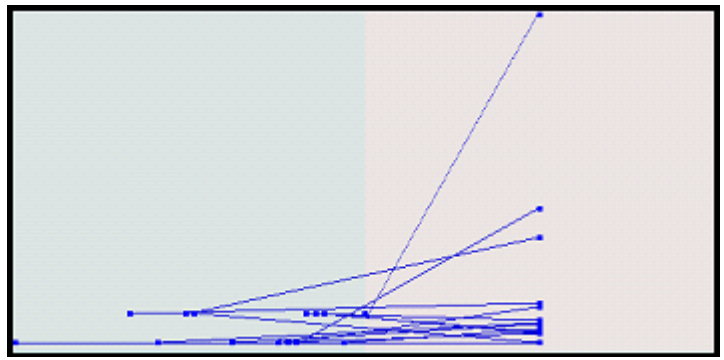
UDP scanning for many IP addresses



Network scanning to many IP addresses



Two types of simultaneous scannings
(network scan (up) + port scan (down))



Port scan for a single IP address

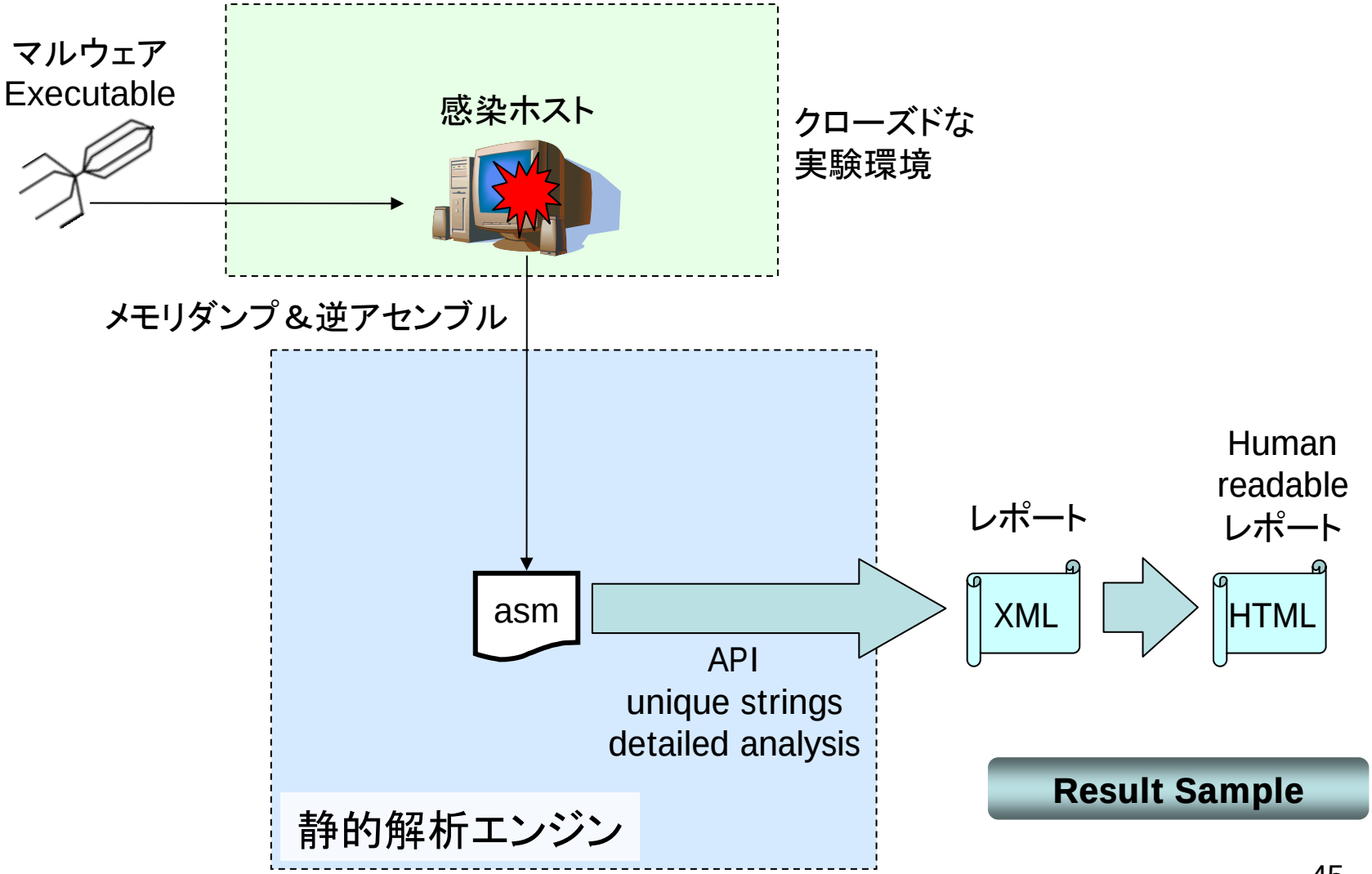
ミクロ解析システム
（MicS: Micro analysis System）

マルウェア 静的解析/動的解析

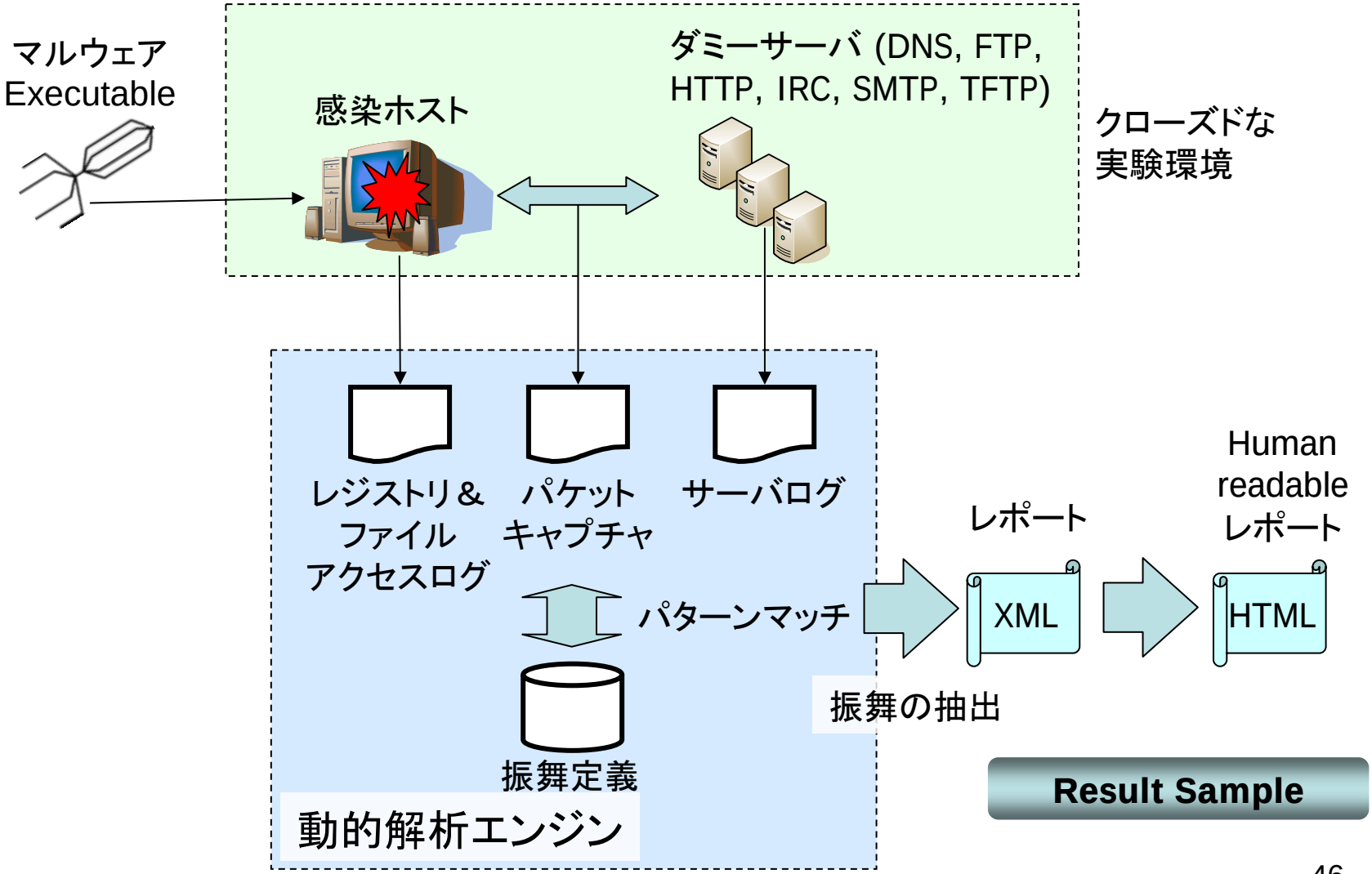
- **静的解析（Malware Code Analyzer）**
  - ホワイトボックスアプローチ
  - 難読化されたマルウェアのコードを解析するため、メモリ上に展開された，マルウェアをダンプし解析

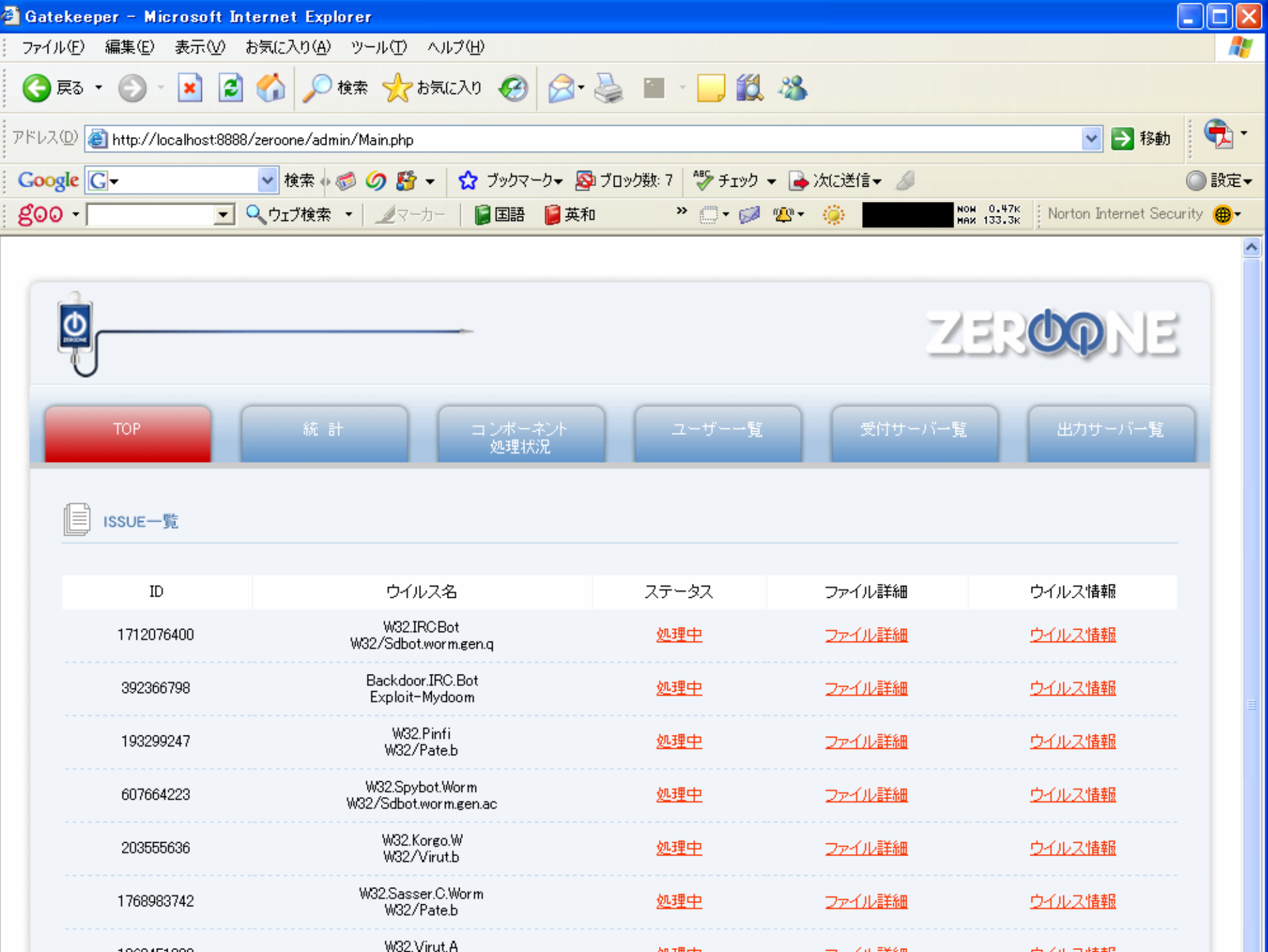
- **動的解析（Malware Behavior Analyzer）**
  - ブラックボックスアプローチ
  - 仮想的なインターネット環境（箱庭環境）の中でマルウェアを動作させ、その挙動を抽出

マルウェア 静的解析（Code Analysis）



マルウェア 動的解析（Behavior Analysis）

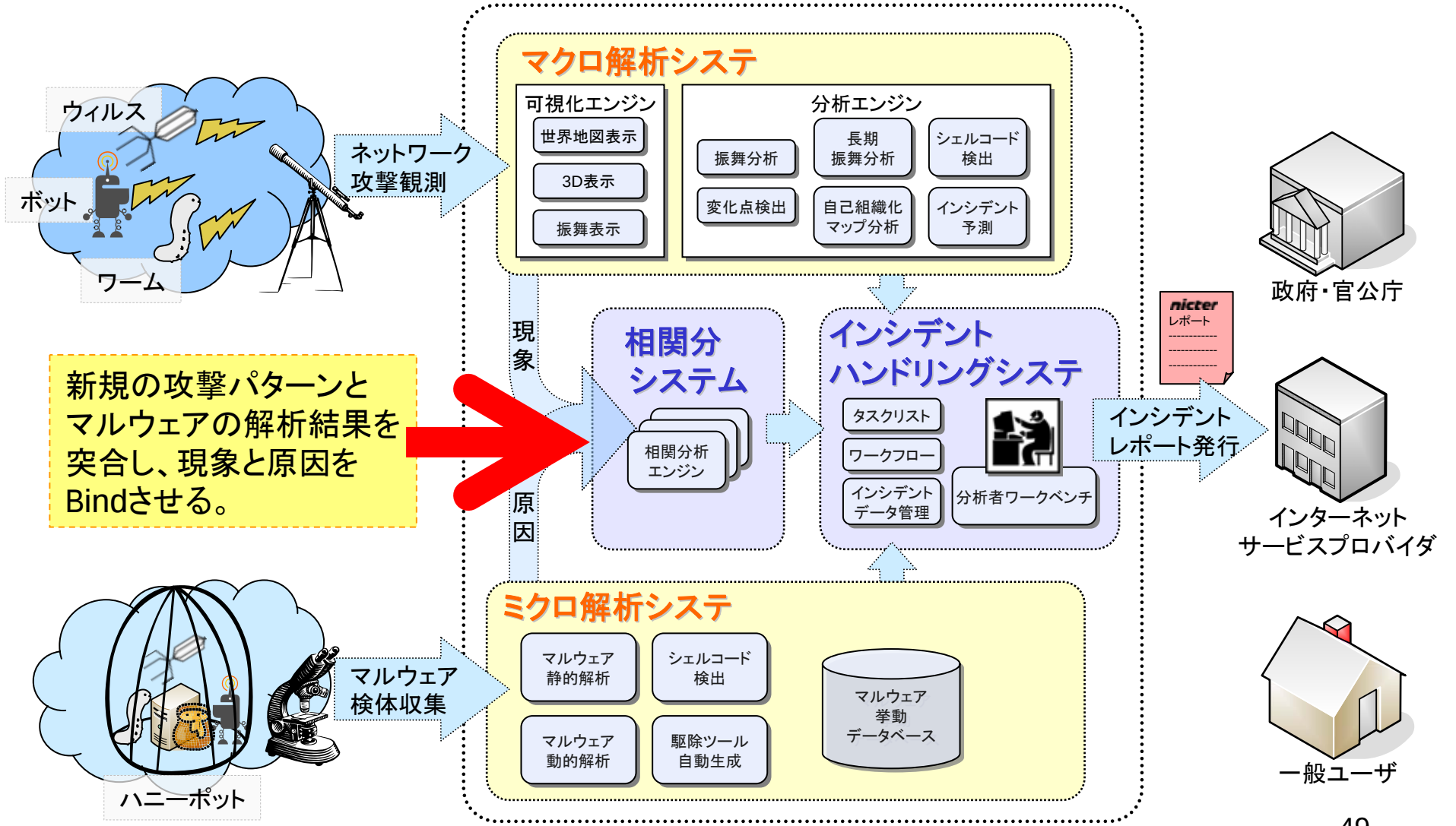



Gatekeeper - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り
アドレス(D) http://localhost:8888/zeroone/admin/Main.php
移動
Google 検索 ブックマーク ブロック数: 7 チェック 次に送信 設定
goo ウェブ検索 マーカー 国語 英和
Norton Internet Security
ZERO ONE
TOP
統 計
コンポーネント処理状況
ユーザー一覧
受付サーバー一覧
出力サーバー一覧
ISSUE一覧
ID
ウイルス名
ステータス
ファイル詳細
ウイルス情報
1712076400
W32.IRCBot
W32/Sdbot.worm.gen.q
処理中
ファイル詳細
ウイルス情報
392366798
Backdoor.IRC.Bot
Exploit-Mydoom
処理中
ファイル詳細
ウイルス情報
193299247
W32.Pinfi
W32/Pate.b
処理中
ファイル詳細
ウイルス情報
607664223
W32.Spybot.Worm
W32/Sdbot.worm.gen.ac
処理中
ファイル詳細
ウイルス情報
203555636
W32.Korgo.W
W32/Virut.b
処理中
ファイル詳細
ウイルス情報
1768983742
W32.Sasser.C.Worm
W32/Pate.b
処理中
ファイル詳細
ウイルス情報
W32.Virut.A

マクロ-ミクロ相関分析システム

（NemeSys: Network and malware enchaining System）

マクロ-ミクロ相関分析システム



マクロ-ミクロ相関分析システム概要

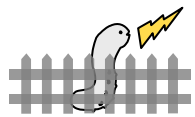
目的:

マクロ解析において検出された新規の攻撃と、ミクロ解析において分析されたマルウェアの相関を調べることで、ネットワーク上の**現象**と**原因**を関連付ける。

基本アイデア(スキャンに基づく相関分析)

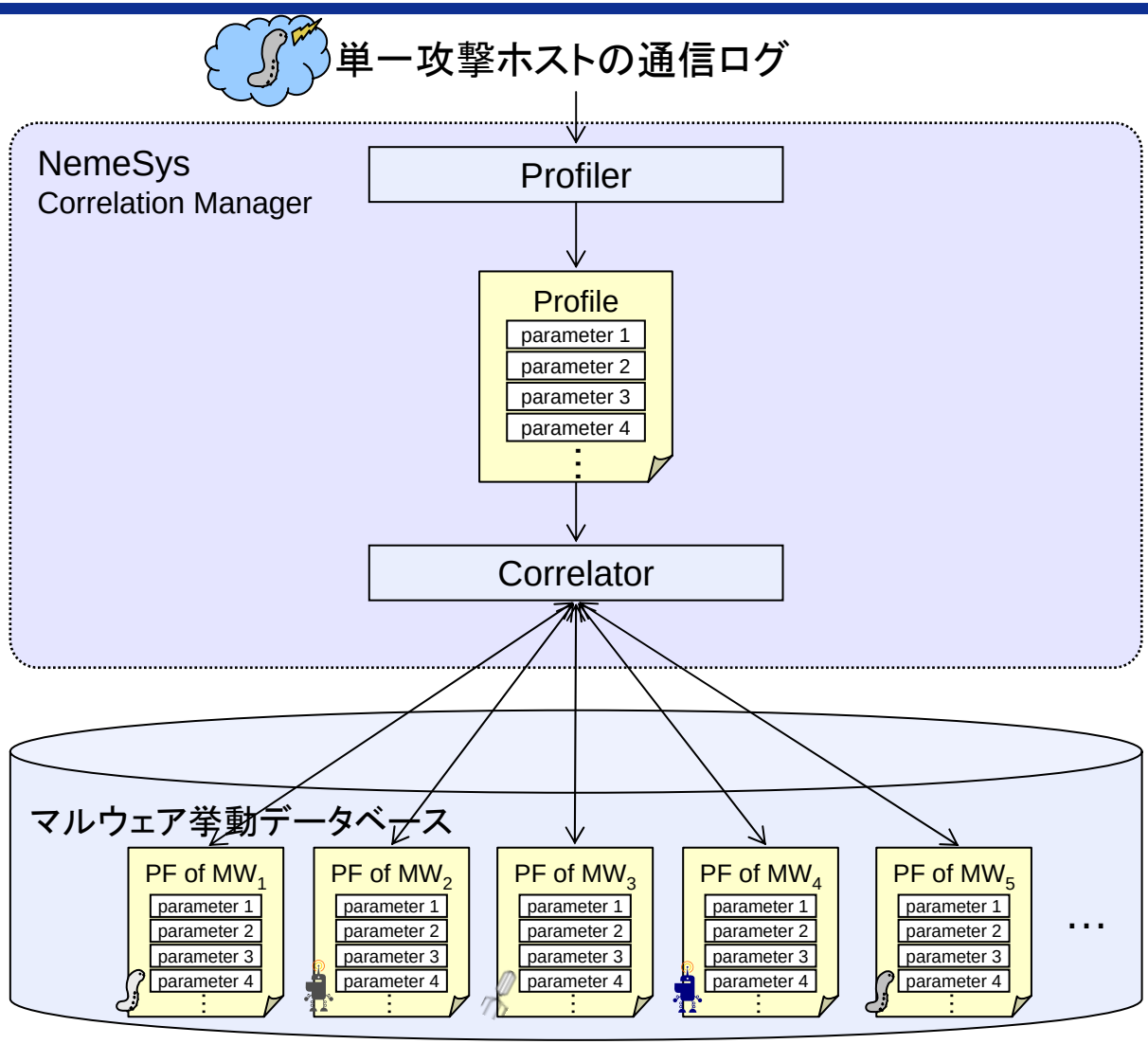
- 特定ホストからダークネットへのスキャンをプロファイル化

- マルウェア動的解析で得られるスキャンをプロファイル化



- プロファイル間の相関を計算し、該当ホストが感染している可能性の高い**マルウェアの候補リスト**を出力

マクローミクロ相関分析のイメージ



Similarity Ranking for ICID 20051218_129.44.179.182 - Opera

ファイル(F) 編集(E) 表示(V) ブックマーク(B) ウィジェット(G) ツール(T) ヘルプ(H)

新しいタブ | Similarity Ranking for IC...

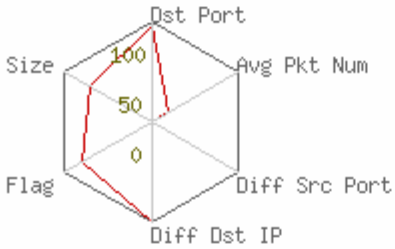
//localhost:8080/correlation/20051218_129.44.179.182/20051218_129.44.179.182.html 画像: 44/96

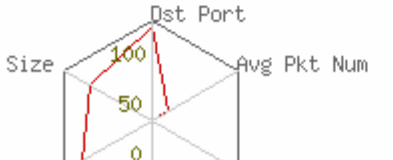
Google で検索

NemeSys
network and malware enchaining system

nicter

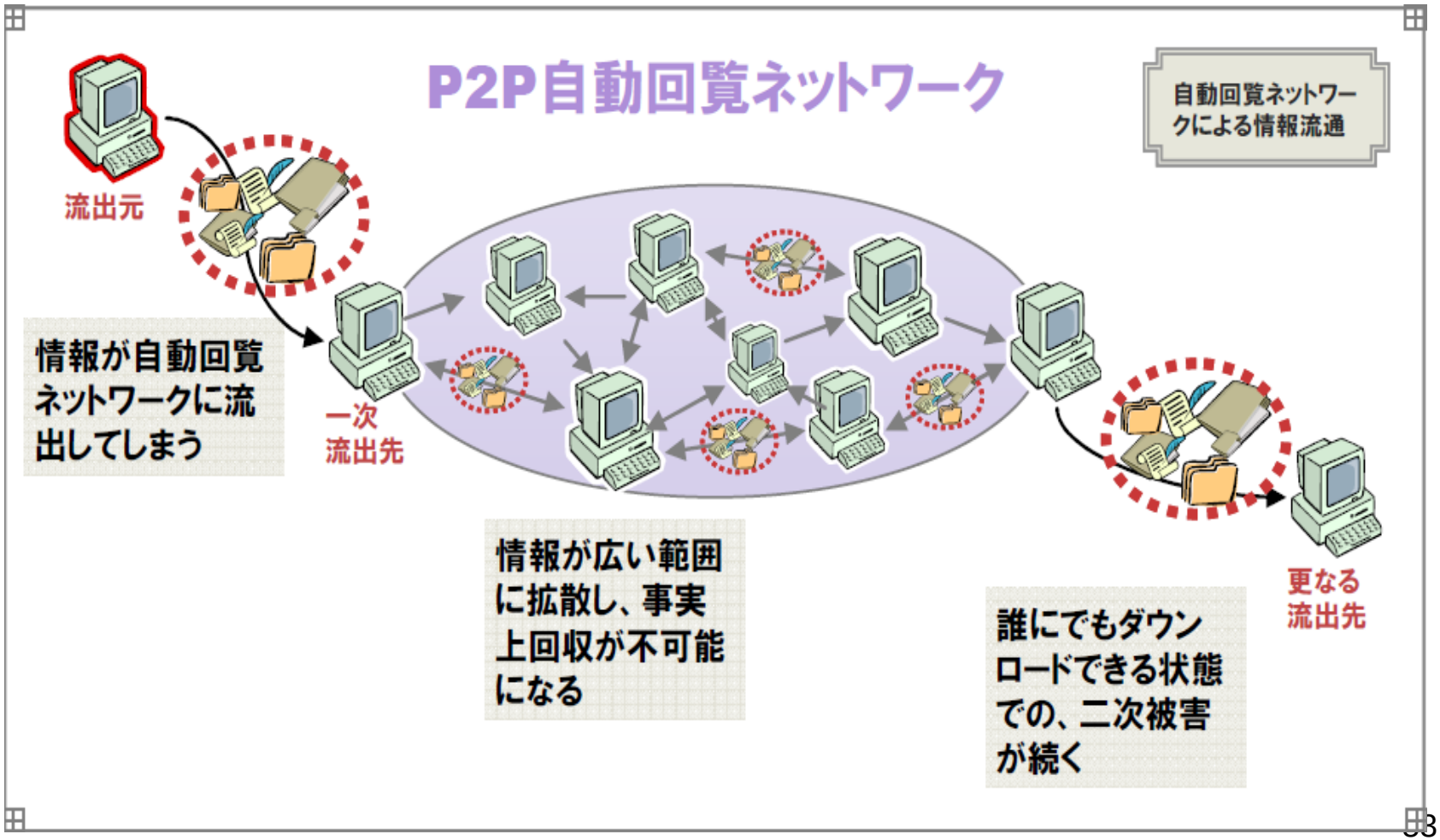
Similarity Ranking for the Incident Candidate (ICID 20051218_129.44.179.182) [Packet Dump] [NemeSys Index] [Pcat Index]

Similarity: 0.78 0.96 0.00 0.01 1.00 1.00	Malware Name: W32.Gobot.A **Candidate #1**
 Similarity Chart Behavior Graph	Captured Date: 2006/11/01 21:10:15 Packet Category: TCP_SYN_Scan Port Set: TCP/139 TCP/3127 TCP/445 TCP/6667 [Code Analysis] [Behavior Analysis] [Micro Analysis Dump] [NemeSys Index] [3D Visualization]

Similarity: 0.77 0.94 0.00 0.02 1.00 1.00	Malware Name: W32.Gobot.A **Candidate #2**
	Captured Date: 2006/11/01 21:10:15 Packet Category: TCP_SYN_Scan Port Set: TCP/139 TCP/3127 TCP/445 TCP/6659 [Code Analysis] [Behavior Analysis] [Micro Analysis Dump] [NemeSys Index]

さらなる脅威：情報漏えい（1）

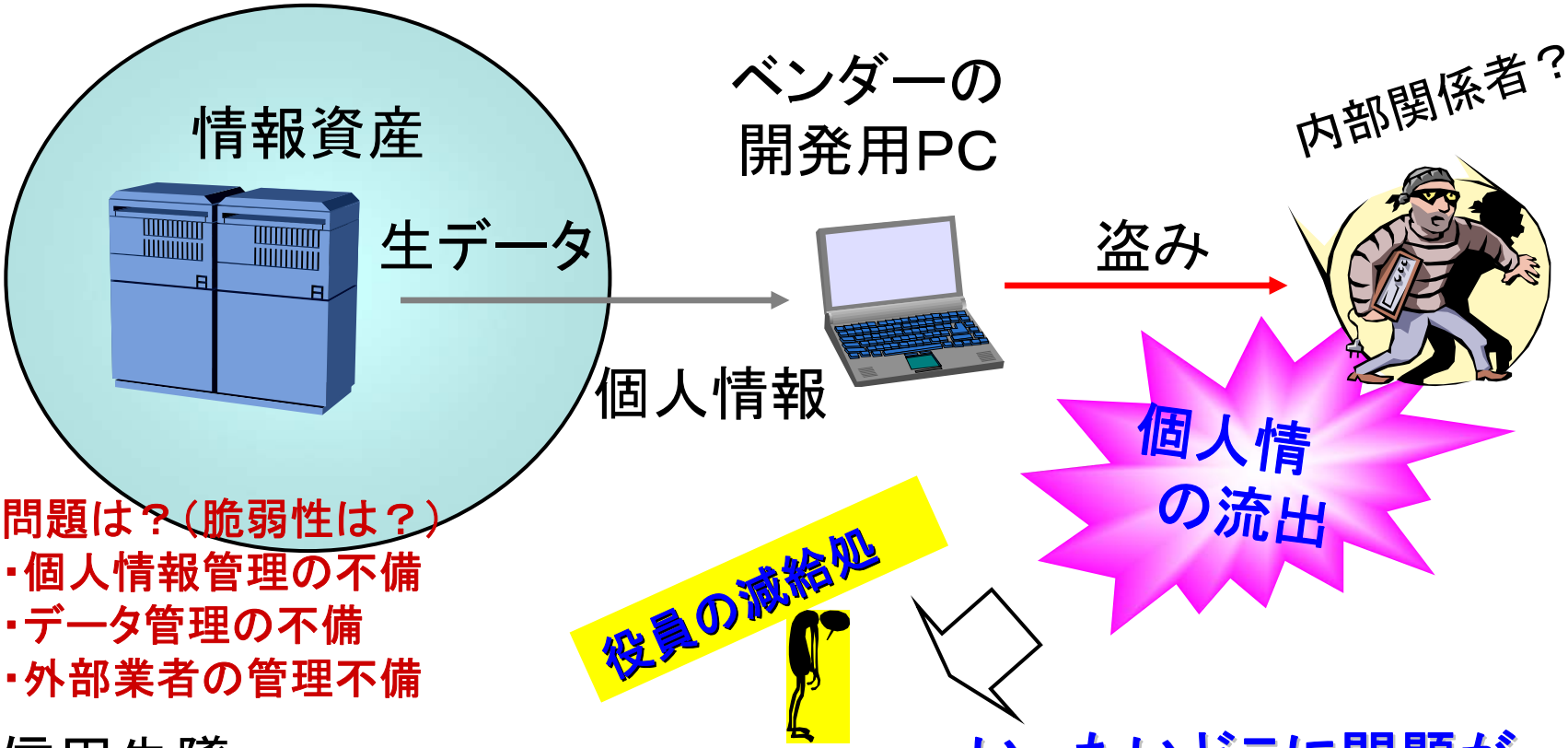
1）WinnyなどのP2Pソフト利用の脅威



「IPA　情報セキュリティ白書　2007」より抜粋

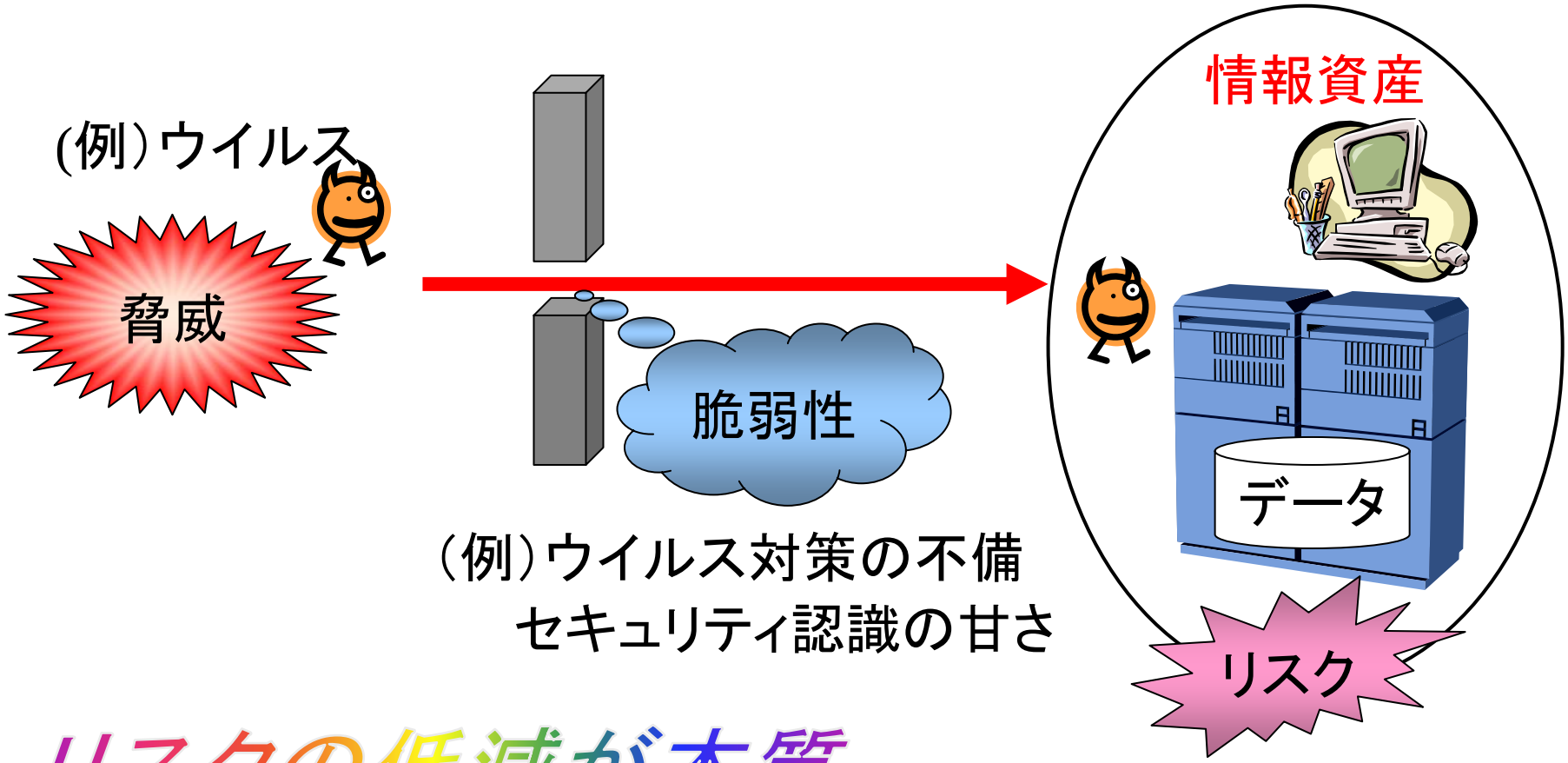
さらなる脅威：情報漏えい　事例（2）

B社の顧客情報56万人分の会員カード情報流出が発覚。
（2003年6月）



- 信用失墜
- 顧客への詫び状、商品券送付（500円×全会員115万人⇒5億7500万円！）

脅威、脆弱性、および資産に対するリス



(例)ウイルス対策の不備
セキュリティ認識の甘さ

サービス停止
データ破壊

リスクの低減が本質

・情報資産の重要度×脅威×脆弱性
・情報セキュリティ対策の必要性

情報セキュリティマネジメントの確保が重要

ISO/IEC 27002

- Security policy
- Organising information security
- Asset management
- Human resources security
- Physical & environmental security
- Communications & operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

ISMS構築運用

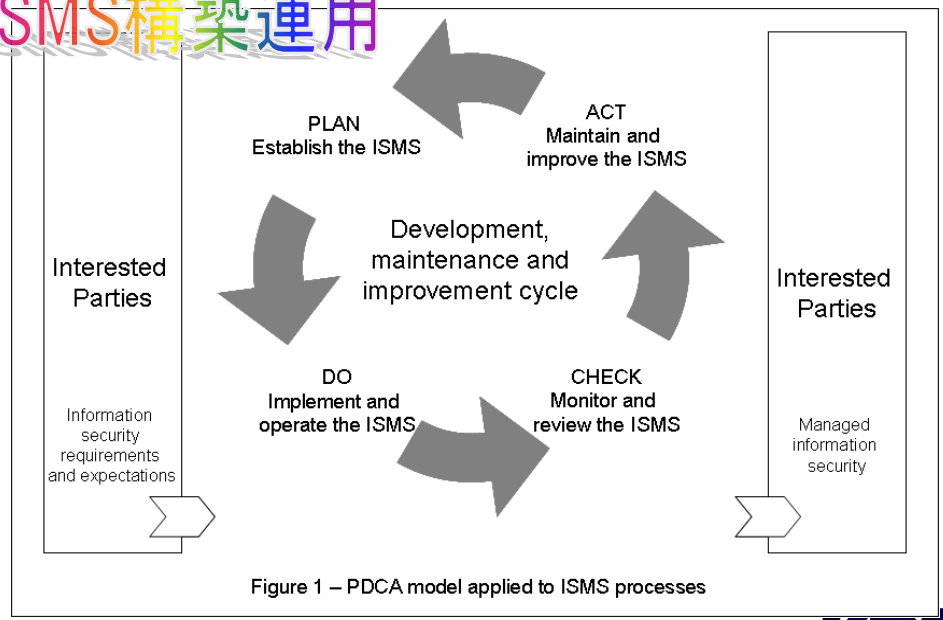


Figure 1 – PDCA model applied to ISMS processes

情報セキュリティ対策とは（具体例）

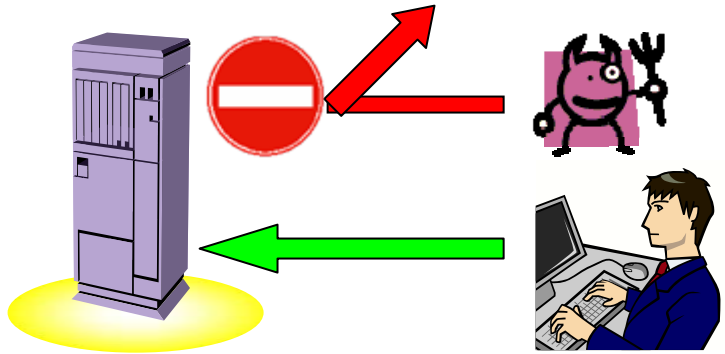
①物理的対策

不正侵入等から保護

②人的対策

情報セキュリティの
重要性の周知徹底

③技術的対策



情報資産へのアクセス制御

④運用等における対策

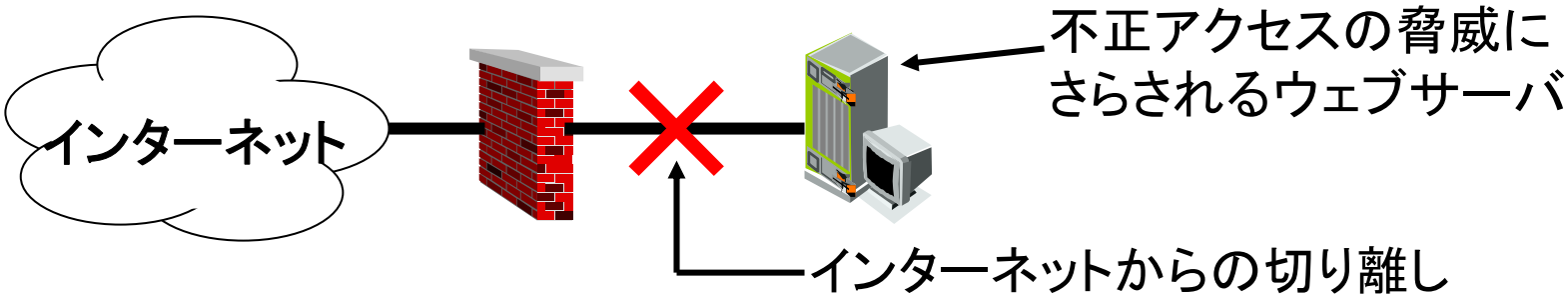
情報セキュリティ対策の
遵守状況の確認

⑤緊急時における対策

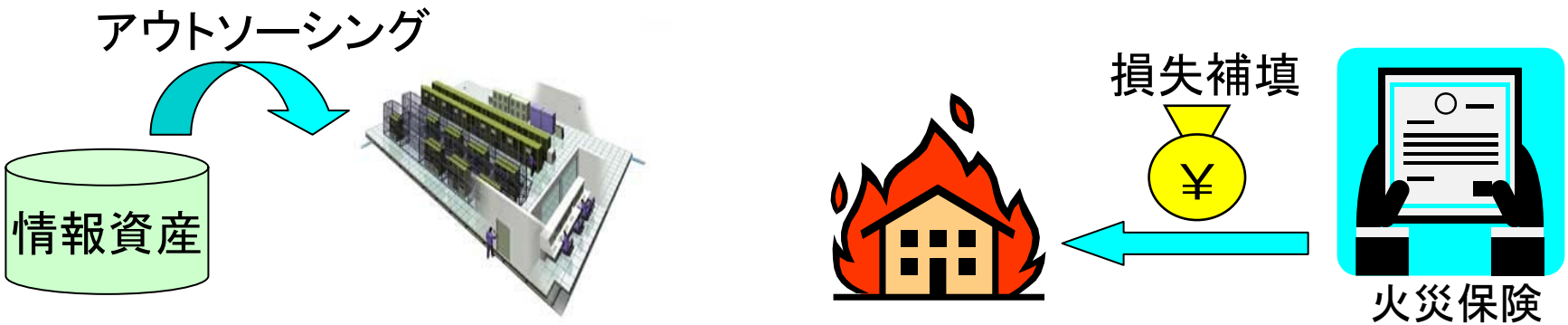
危機管理面の整備

リスク回避及び移転

①リスクの回避：業務の廃止、情報資産の破棄により、リスクが発生しないようにすること



②リスクの移転：リスクを、契約等により他者に移転すること



日本ISMSユーザグループの活動

日本ISMS ユーザグループ（J-ISMS UG）

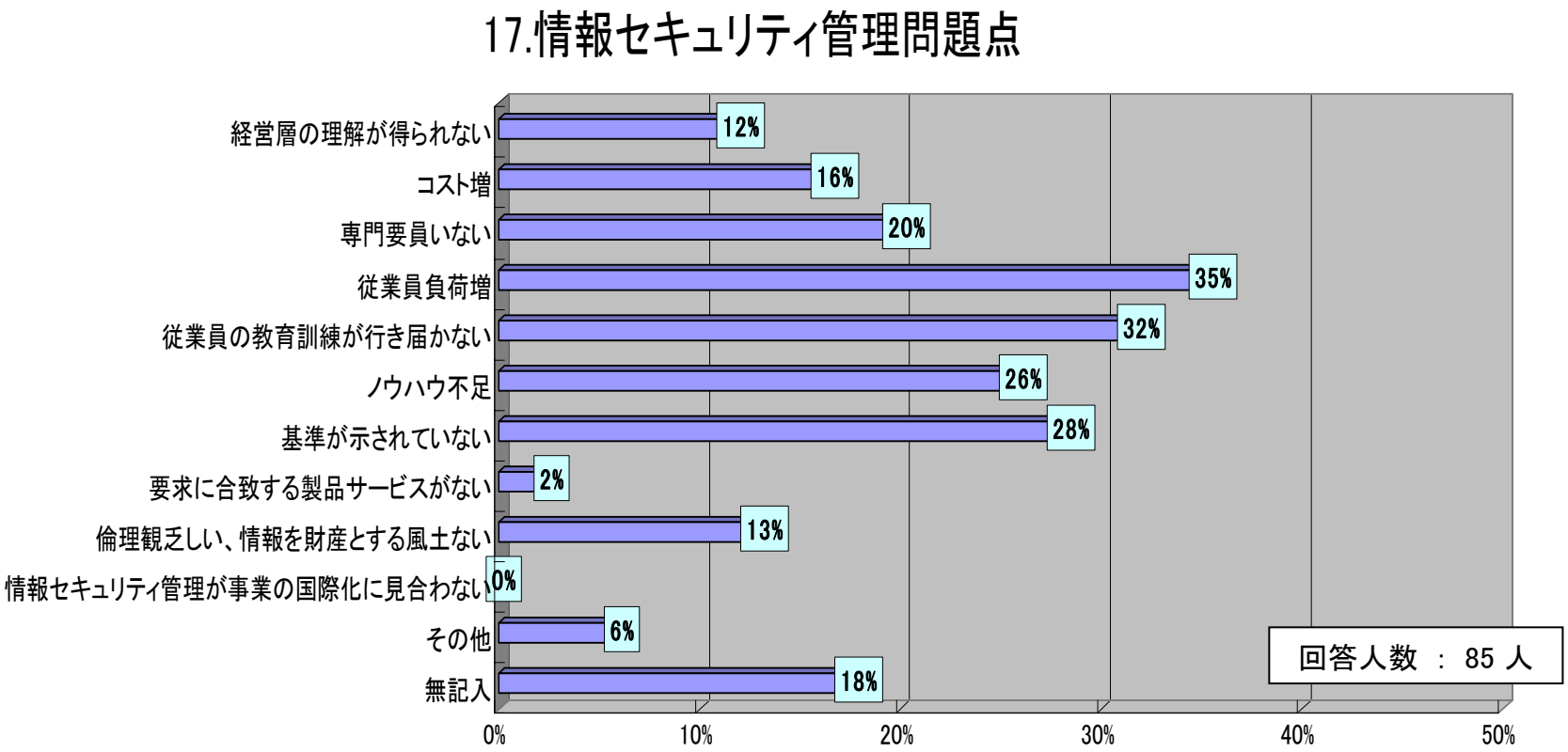
- 日本ISMSユーザグループは、ISMSの構築・運用など広範囲に渡るISMS 関連技術を共有し、お互いの経験に基づく意見交換・議論を進め、日本における健全かつ効果的なISMS 普及・促進に貢献することを目的として下記発起人メンバーにより2004年7月29日に設立されました。
  URL: http://www.j-isms.jp/

- **発起メンバー（五十音順）**
  - **IBM ビジネスコンサルティングサービス株式会社**
  - **株式会社アズジェント**
  - **NTTコミュニケーションズ株式会社**
  - **株式会社NTTデータインフォプリオ・セキュリティコンサルティング**
  - **グローバルセキュリティエキスパート株式会社**
  - **KDDI**株式会社
  - **日本電気株式会社**
  - 株式会社日立製作所
  - 松下電器産業株式会社　　**以上9社**
- **オブザーバ**
  - **経済産業省　商務情報政策局　情報セキュリティ政策室**
  - 財団法人 日本情報処理開発協会（**JIPDEC**）
  - **インターナショナルISMS-UG**

日本ISMSユーザグループの活動目的

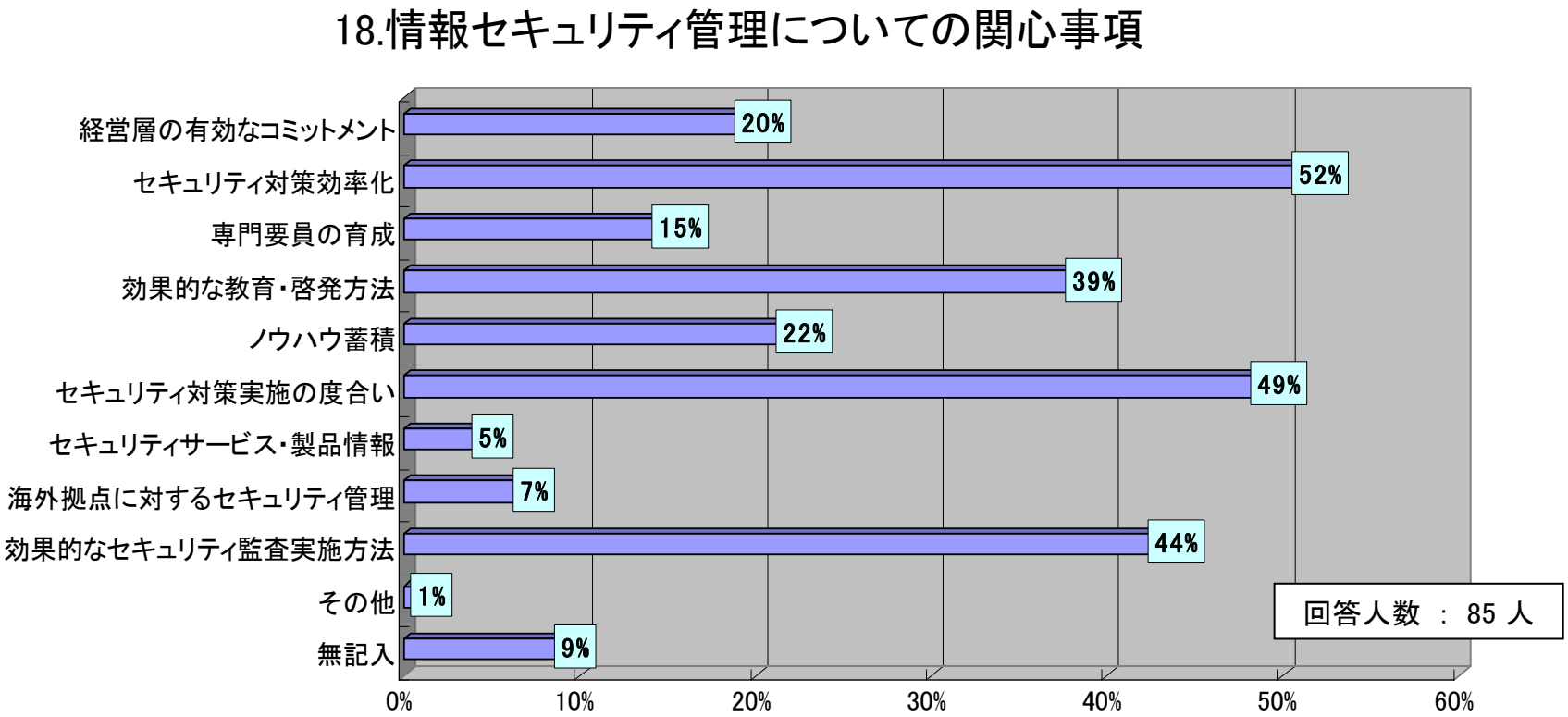
- わが国におけるISMSの普及・高度化
  - ISMS構築・運用の実践的な事例を幅広い業種から募る
  - ISMSの幅広い普及を促進する
    - 情報セキュリティ管理に関わる情報の共有
    - ISMS構築、認証、運営等に関わる問題点の議論
      - 事業目的に合った情報セキュリティ管理プロセスの構築
      - 業務プロセスとISMSの円滑かつ密接な連携
      - その他

アンケート集計結果
セキュリティへの取組（17,管理問題点）



- 管理問題点は、「従業員の負荷増」、「教育訓練の不備」、「基準がない」、「ノウハウ不足」等が高い割合で挙げられており、人的・制度的な項目が問題点となっている。

アンケート集計結果
セキュリティへの取組（18,関心事項）



- 関心事項については、「セキュリティ対策効率化」、「セキュリティ対策実施の度合い」、「効果的な教育・啓発方法」、「効果的なセキュリティ監査実施方法」等に関心が高くなっている。

Telecom-ISAC　Japanの活動（概要）

活動の概要

(1) Portal Site

General information
about T-ISAC-J
News
Conference Info.

(2) Public Relations

Public

(3) Operation

(6) Relationship

Malware handling
Advisory
Removal tools
Reports

Malware center

JPCERT/CC

Malware data/information

Wide area monitoring
Advisory
Reports
Advisory for protection

Monitoring center

NiCT

ISP Network

Monitoring data/information

Routing operation
BGP information
Analysis tools
Trouble information

Routing Operation center

JPNIC

Routing data

Members

Emergency operation

Operation center

JPCERT/CC

Member

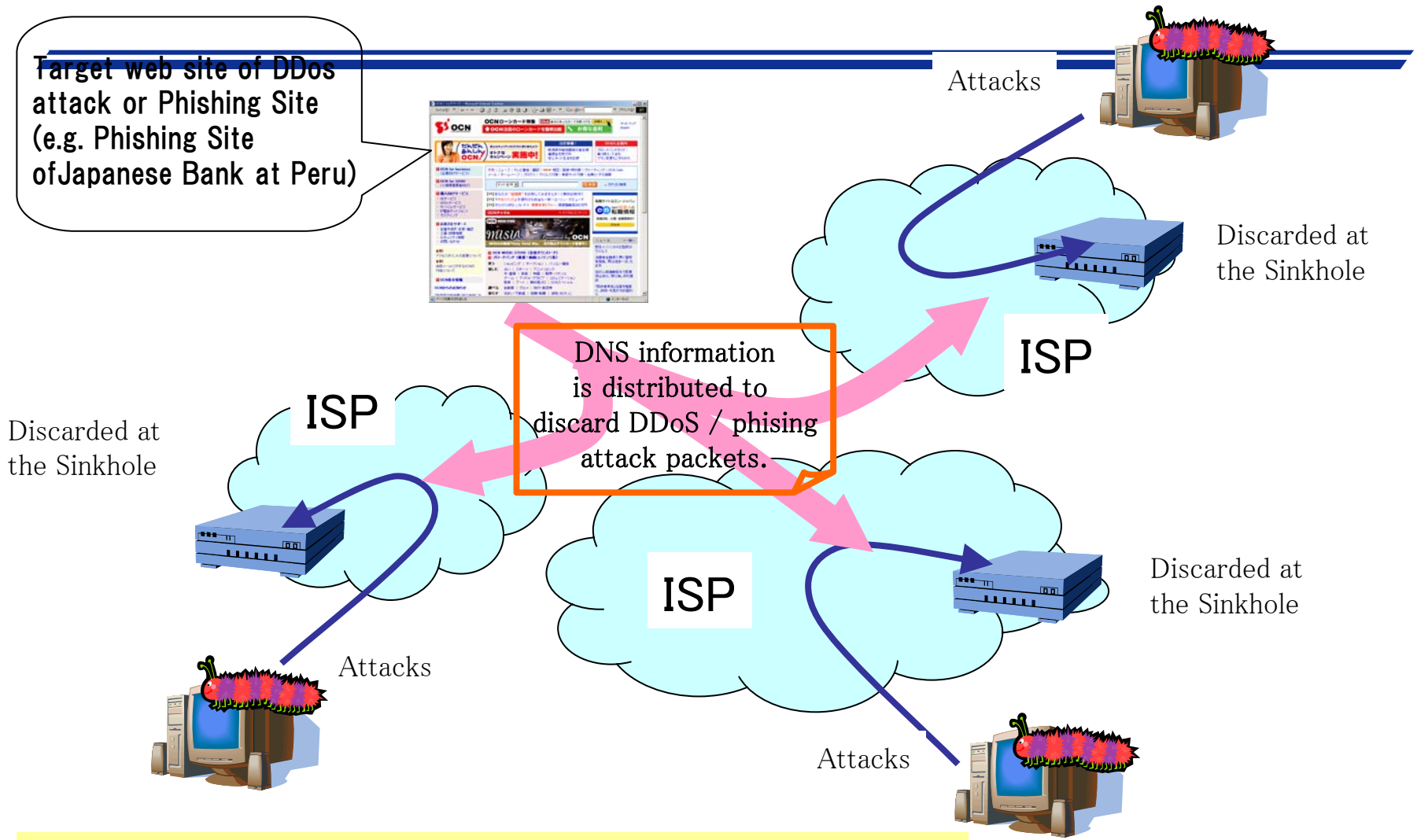
Incident information

(4) Data/Information

Member information
Activity reports
reports from WGs

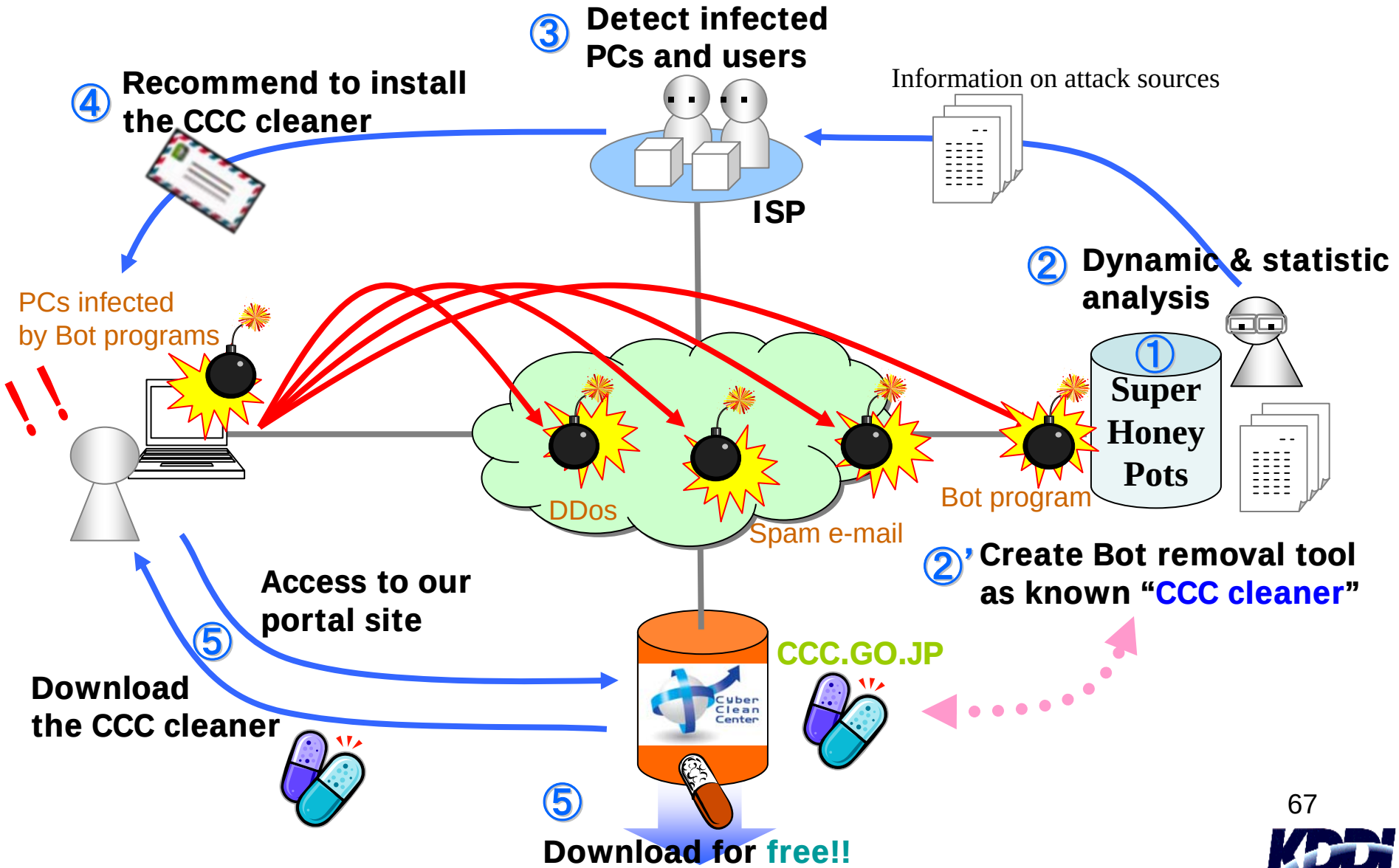
(5) Services

活動 (1) Sinkhole operation scheme



1. Telecom-ISAC requests ISPs to handle the worm!
2. Each ISP member of T-ISAC-J cooperates to drop harmful packets while Telecom-ISAC Japan leads the way.

活動(2) Cyber Clean Center（CCC)



まとめ

- 攻撃側は、防御・対策側の技術を理解しながら、多様、かつ複雑な手を打ってくる。
- 攻撃手法として、極力、「見えない（感知させない）」攻撃が増えてきている。
- 技術的な防御策としての研究開発は世界的に進歩しており、国際的な連携も強くなってきている。
  （ハッカーもそこに絡んでいると思われる）
- 技術のセキュリティには限界があり、総合的なセキュリティを確保するために、「情報セキュリティマネジメントの確保」は必達の課題となる。
  →「セキュリティマネジメント」と「内部統制」は車輪の両軸
- 今後の大きな課題として、ソーシャルエンジニアリング系の脅威に対抗するための教育、啓蒙が重要

今後の検討課題

今後重要と想定されるセキュリティ技術

- **NW系**
  -Internet　IPv4（監視、マルウェア解析、イベント分析等）
  -NGNにおけるセキュリティ技術（脅威分析から）
  -IPv6におけるセキュリティ技術（脅威分析から）
  -Mobile通信におけるセキュリティ技術
- **セキュリティ応用系**
  -ホームネットワークにおけるセキュリティ技術
  -ITSにおけるセキュリティ技術
  -その他
- **セキュリティ基盤系**
  -IdM技術、バイオメトリクス技術、暗号プロトコル

等

IPv6 security issues

- Routing-header 0 problem
- routing vulnerability is the same as the IPv4 network; no major change
- ambiguity of addresses
  - 6to4, mapped-v4 address, etc.
- IPv4 and IPv6 are two different networks; but the application designer does not care much about that
- Too many optional headers that can be embedded in an IPv6 packet

携帯電話における脅威への対策例

盗聴	通信内容の暗号化
迷惑メール、ワンギリ	メールフィルタ等の防御機能 サービス機能の制限
有害サイト	URLフィルタサービスの提供 年齢認証によるwebアクセス制限
ウイルス、DoS攻撃	ネットワークへのIDS設置、Fire Wall強化 ネットワーク、端末へのウイルススキャン導入
なりすまし	PKI認証、バイオメトリクス認証
盗難、紛失	移動機遠隔ロックや遠隔データ消去 非活性化デバイス（SPCなど）

Thank you for listening Q&A