<Internet Week 2013　S6>
サイバー犯罪の動向と対策、
インターネットのセキュリティと通信の秘密

ACTIVE
（Advanced Cyber Threats response InitiatiVE）
プロジェクトの取り組み

2013年11月28日

Telecom-ISAC Japan　ステアリングコミッティ運営委員
Telecom-ISAC Japan　ACTIVE業務推進WG　主査
NTTコミュニケーションズ株式会社　先端IPアーキテクチャセンタ
湯口 高司

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

1. ACTIVEプロジェクトの背景

多種多様なマルウェア感染経路が存在

- ネットワーク感染(ボット型)
- Web経由の感染
- メール経由の感染
- USB経由の感染　　など

マルウェア感染時にはさまざまな脅威が存在

- 不正アクセスインシデント
- 他人のPCを踏み台にしたサイバー攻撃
- フィッシング、SPAMメール
- PCの破壊活動　　など

- 昨今、マルウェア感染による国家機密の情報窃取等、サイバー攻撃の脅威が増大
- 悪性サイトの閲覧によりマルウェア感染するなど、その感染手法が巧妙化し、利用者が自力で検知することが困難

ISP等 = お客さま対応、インシデント対応の観点からマルウェアの感染率の低下を実施する必要性がある

行政 = 安心・安全なインターネットの利用環境の向上、維持の観点からマルウェアの感染率の低下が望まれる

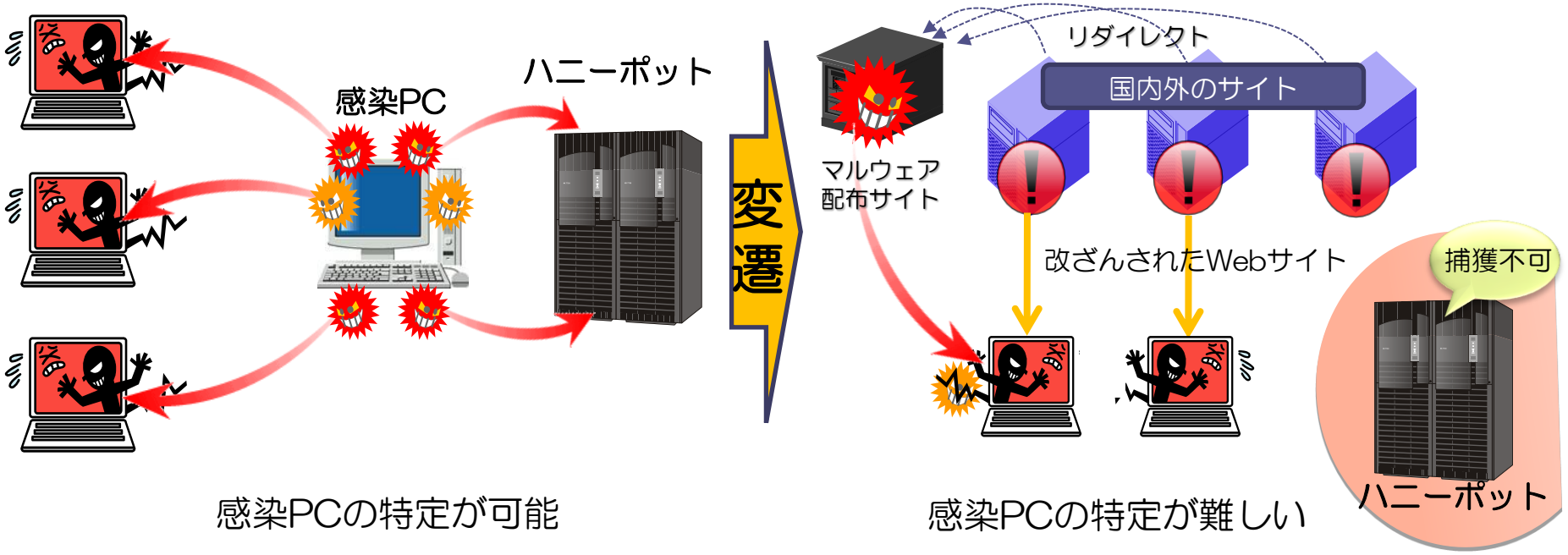
2. マルウェア感染経路の変遷

ネットワーク感染型マルウェア

- ネットワーク経由で感染するマルウェア
- OSの脆弱性を攻撃して感染
- ハニーポットにて捕獲可能であり、Cyber Clean Centerの取り組み（2006~2010年度）の駆除対象

Web感染型マルウェア

- Webサイトの閲覧により感染するマルウェア
- ブラウザまたはブラウザのプラグインの脆弱性を攻撃して感染
- ACTIVEではネットワーク感染型の他、この対応も注力していく必要あり

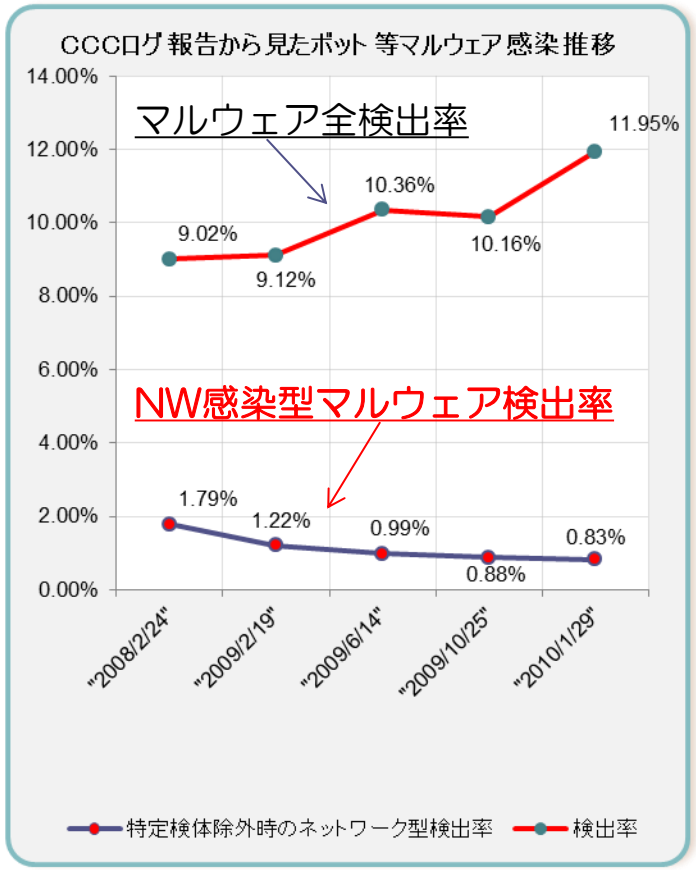


感染PCの特定が可能

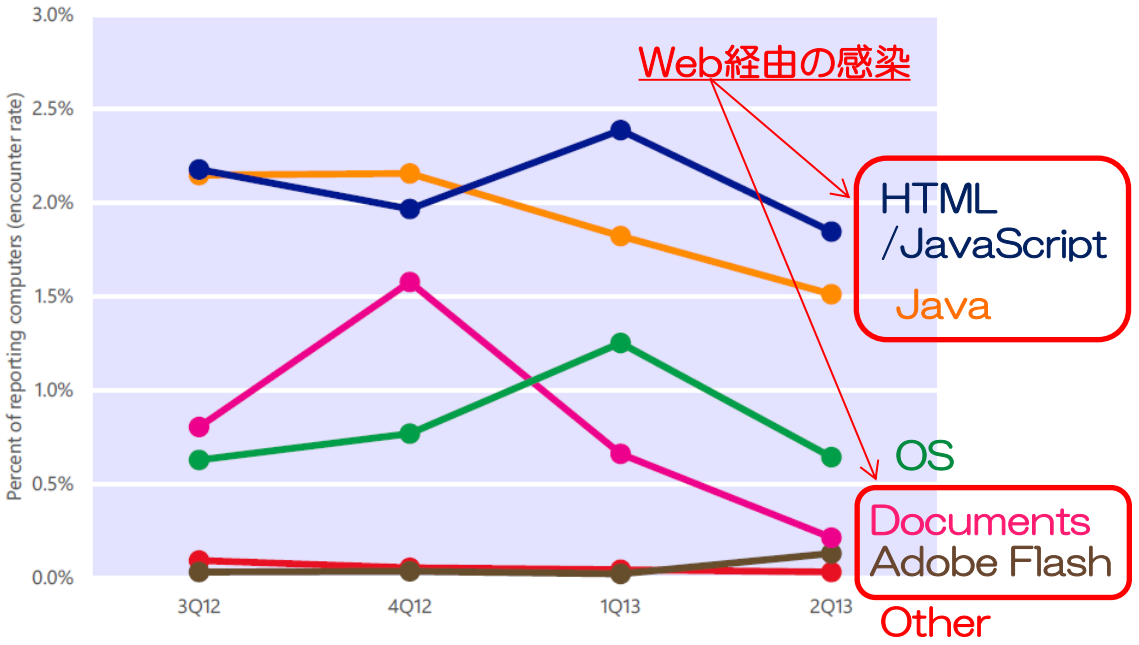
感染PCの特定が難しい

2. マルウェア感染経路の変遷

■ マルウェア感染率推移
（出典：Cyber Clean Center実績）



■ 主な感染経路の移り変わり
（出典：Microsoft Security Intelligence Report 15）



（3Q12 から 2Q13 までの四半期ごとに Microsoft マルウェア対策製品が検出したさまざまな種類のエクスプロイトの流行を、影響を受けたコンピューターの台数の割合で示したグラフ）

- マルウェア全検出率（赤線）は増加しているものの、ネットワーク感染型マルウェアの検出率（紫線）は減少

- NW経由の感染（OSの脆弱性を狙った攻撃）と比較すると、Web経由の感染（HTML/JavaScriptやJavaの脆弱性を狙った攻撃）が上位を占める

3. ACTIVEプロジェクトの概要

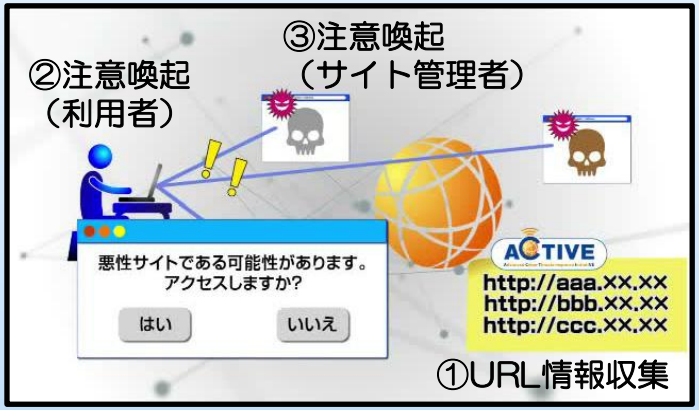
■ ACTIVE（Advanced Cyber Threats response InitiatiVE）

➢ 総務省主管の国民のマルウェア対策支援プロジェクト

http://www.active.go.jp/

- 2013年11月1日開始
- 目的：マルウェア感染の削減等により、安心・安全なインターネットの実現を目指す
- マルウェア感染防止から駆除まで一貫して取り組む総合的なマルウェア感染対策であり、官民連携により行う同様のプロジェクトは世界初の試み

マルウェア感染防止の取り組み



① マルウェア配布サイト等のURL情報をリスト化
② マルウェア配布サイト等にアクセスしようとする利用者に注意喚起
③ マルウェア配布サイト等の管理者に対しても適切な対策を取るように注意喚起

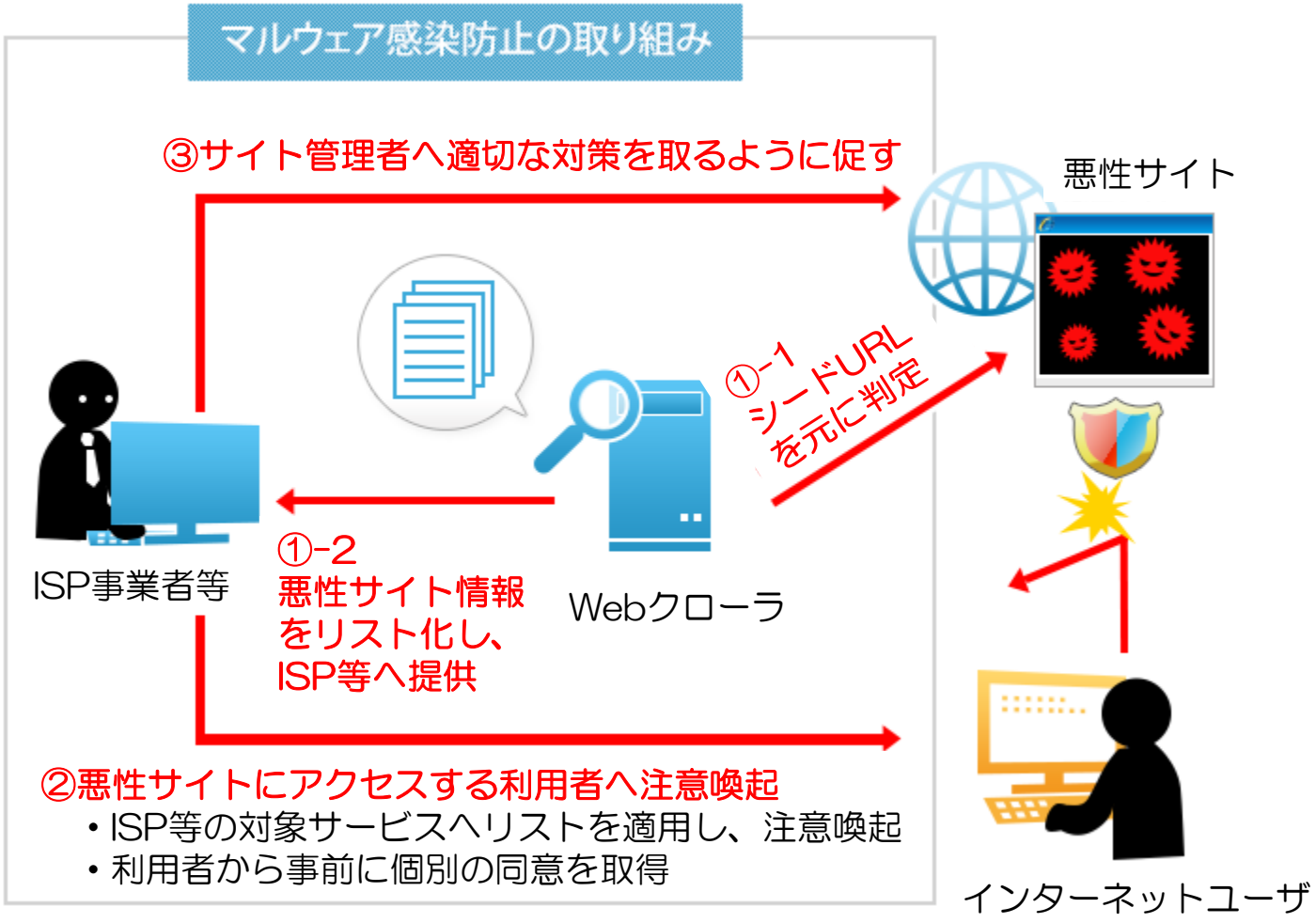
マルウェア駆除の取り組み

① マルウェアに感染した利用者のPCを特定
② 利用者に適切な対策を取るように注意喚起
③ 利用者は、注意喚起の内容に従いPCからマルウェアを駆除

3. ACTIVEプロジェクトの概要

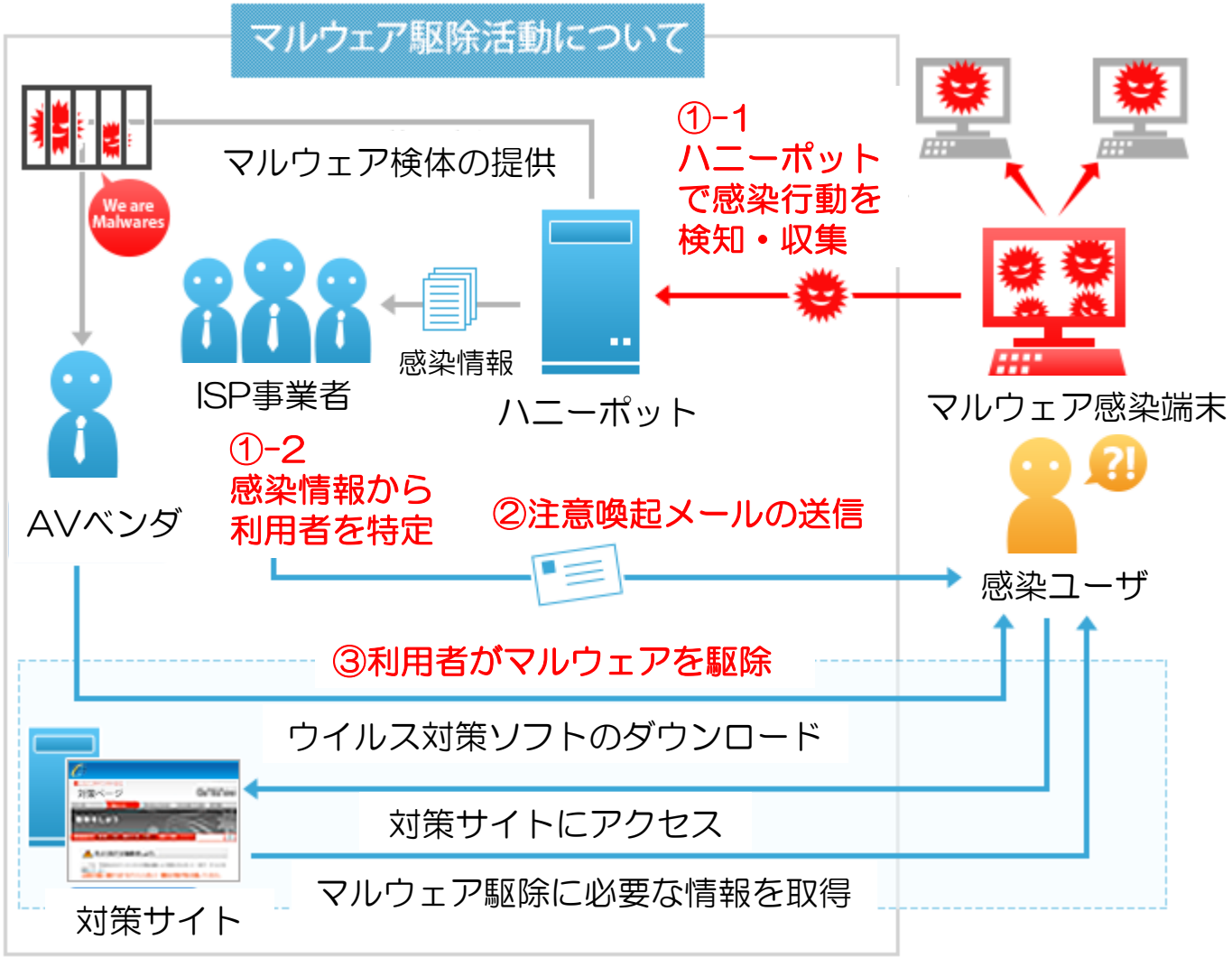
■ マルウェア感染防止の取り組み

✓ 各社の対象サービスに対して、利用者から事前に個別の同意を取得



3. ACTIVEプロジェクトの概要

■ マルウェア駆除の取り組み



4. ACTIVEプロジェクト体制（2013年11月現在）

■ ISP等の通信事業者やセキュリティベンダなどが参画

総務省

財政支援、全体支援

Telecom-ISAC Japan

主査　：エヌ・ティ・ティ・コミュニケーションズ株式会社
副主査：ニフティ株式会社、T-ISAC-J企画調整部

参画事業者間の調整

NECビッグローブ株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社
エヌ・ティ・ティレゾナント株式会社
株式会社NTTぷらら
株式会社インターネットイニシアティブ
株式会社エヌ・ティ・ティピー・シーコミュニケーションズ
株式会社ハイホー
KDDI株式会社
ソネット株式会社
ソフトバンクBB株式会社
ソフトバンクテレコム株式会社
ニフティ株式会社

インターネットサービスプロバイダー など

NTTコムテクノロジー株式会社
NRIセキュアテクノロジーズ株式会社
エヌ・ティ・ティ・コムチェオ株式会社
エヌ・ティ・ティ・ソフトウェア株式会社
エヌ・ティ・ティラーニングシステムズ株式会社
株式会社FFRI
株式会社カスペルスキー
株式会社日立製作所
トレンドマイクロ株式会社
日本電信電話株式会社
日本マイクロソフト株式会社
マカフィー株式会社

マルウェア収集・駆除のための技術支援

5. ACTIVEにおける「通信の秘密」との関係

■ ACTIVEプロジェクトにおける攻撃収集手法と「通信の秘密」との関係

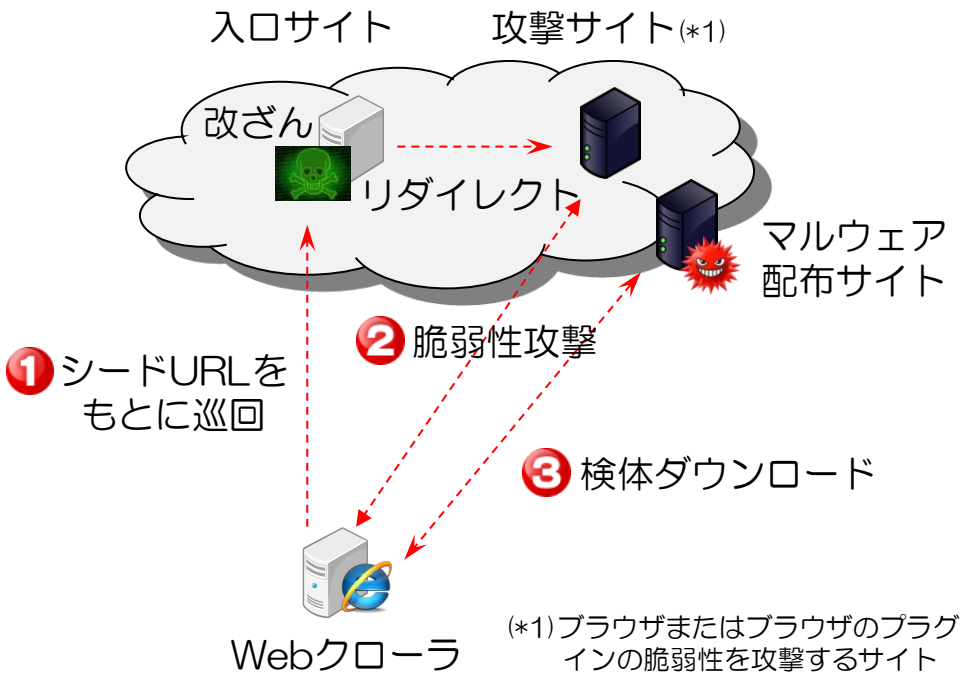
マルウェア感染防止の取り組み

- Webクローラを用いてシードURLを元に当該サイトURLの悪性判定を実施
- 利用者から事前に個別の同意を取得する

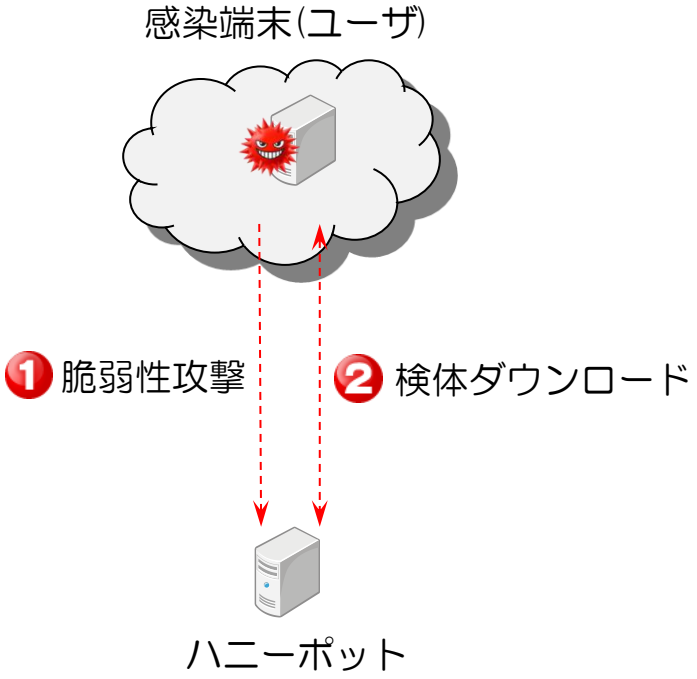
マルウェア駆除の取り組み

- 通信当事者として、ハニーポットを用いて攻撃情報を収集する
- 攻撃の発信元(感染ユーザ)を特定し、注意喚起を行う

【Web感染型マルウェアの攻撃情報を収集】



【NW感染型マルウェアの攻撃情報を収集】



5. ACTIVEにおける「通信の秘密」との関係

■ ACTIVEプロジェクトにおける「通信の秘密」との関係

総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」の公開資料抜粋
http://www.soumu.go.jp/main_content/000264105.pdf

（1）マルウェア感染防止の取組

① マルウェア配布サイトのURL情報をリスト化。
② マルウェア配布サイトにアクセスしようとする利用者に注意喚起。
③ マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

通信の秘密との関係

ISP等が、利用者がアクセスしようとするサイトのURLの情報を知得し、注意喚起を行うことについては、利用者の同意に基づいて行われており、通信の秘密の侵害にあたらない。

（2）マルウェア駆除の取組

① マルウェアに感染した利用者のPCを特定。
② 利用者に適切な対策を取るよう注意喚起。
③ 注意喚起の内容に従いPCからマルウェアを駆除。

通信の秘密との関係

① ACTIVE事務局が、マルウェア感染パソコンからハニーポットに来た通信における送信元IPアドレスを、当該IPアドレスの割当てを行っているISPに提供することは、ACTIVE事務局は当該通信を受信する一方当事者であり、通信の秘密の侵害にあたらないと考えられる。

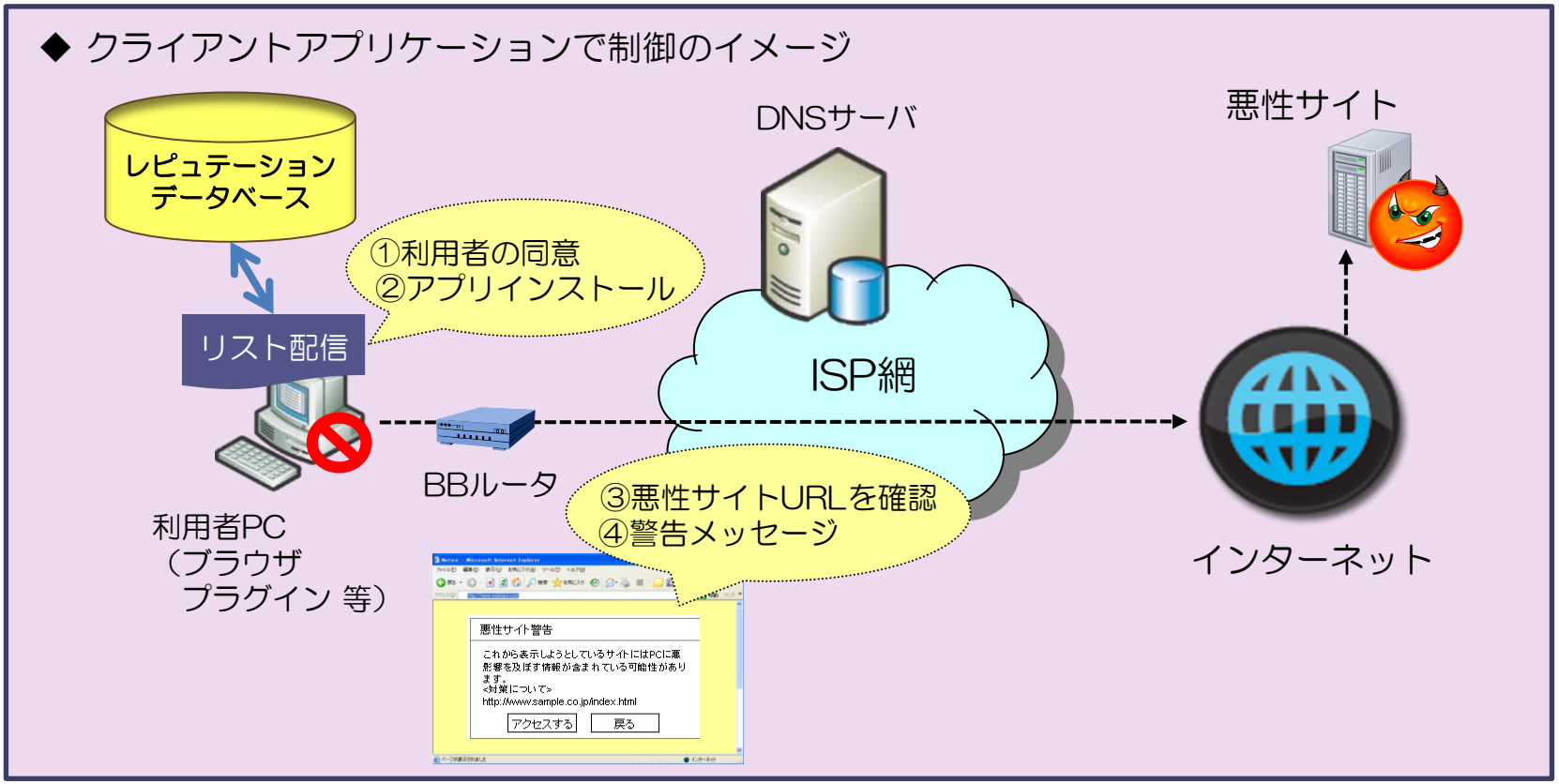
② 上記ISPが、当該IPアドレスをどの契約者に割り当てたか顧客情報と突合し、該当契約者を割り出す行為は、マルウェア感染パソコンに対する現在の危難を避けるための緊急避難として、通信の秘密の侵害に係る違法性は阻却されると考えられる。

6. マルウェア感染防止の取り組み

■ 悪性サイトへアクセス時の利用者への注意喚起方式

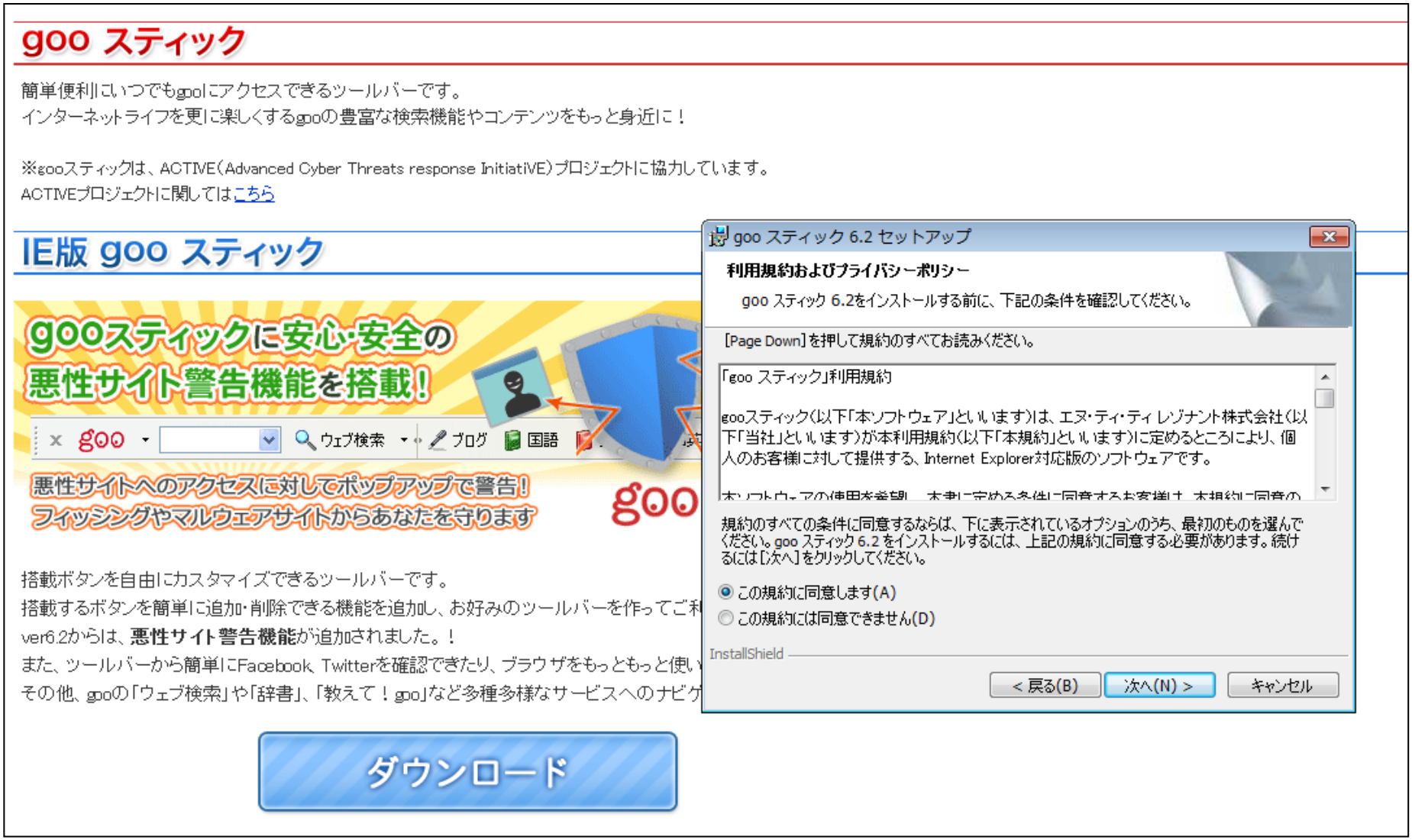
- 各社の対象サービスに依存
  - ✓ クライアントアプリケーションで制御
  - ✓ ISPネットワーク内で制御
    - ※ DNSで制御する方式は、オーバーブロッキングを考慮して適用外
- 対象サービスに対して、利用者から事前に個別の同意を取得することが前提

◆ クライアントアプリケーションで制御のイメージ



6. マルウェア感染防止の取り組み

■ 申し込み時のユーザ同意の取得（例：gooスティック）



6. マルウェア感染防止の取り組み

■ 悪性サイトにアクセス時の注意喚起（例：gooスティック）

ご清聴ありがとうございました