

インターネットにおける ボットネットの現状と対策について

警察庁情報通信局
情報技術解析課

目次

1. ボットネットとは
2. ボットネットの現状
 1. 犯罪情勢
 2. 観測状況
3. ボットネットへの対策

1 . ボットネットとは

ボットネットとは？

- ボット

ロボットに由来した、ボットと呼ばれるプログラムに感染したコンピュータ

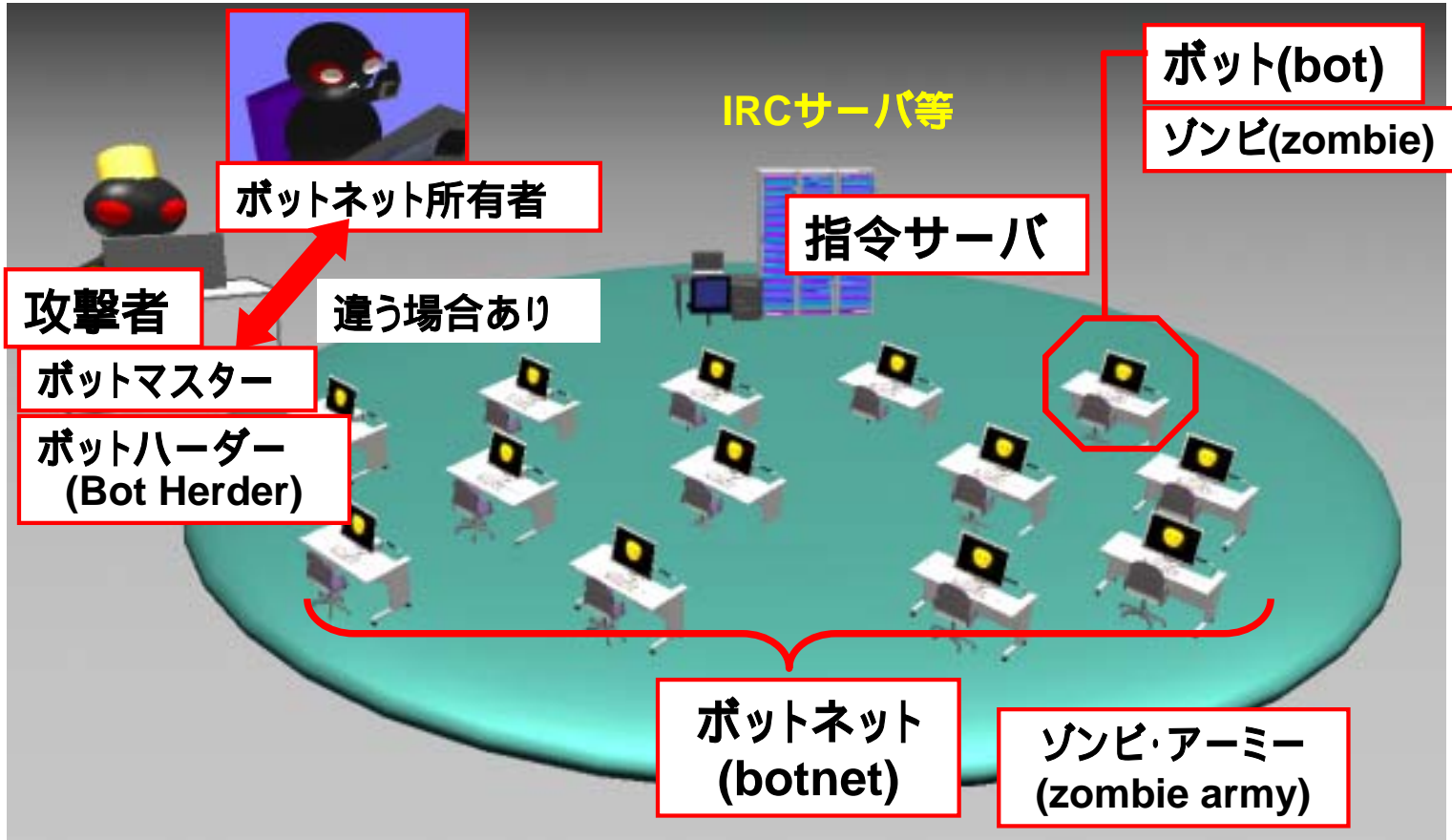
- ボットネット

「攻撃者」・「指令サーバ」・

「ボットに感染したコンピュータ」

から構成されるネットワーク

ボットネットの構成



ボットネットの特徴

● 指令サーバ

- 主にIRC（インターネットリレーチャット）サーバを使用
- 指令サーバの大半は不正アクセスして乗っ取ったコンピュータ

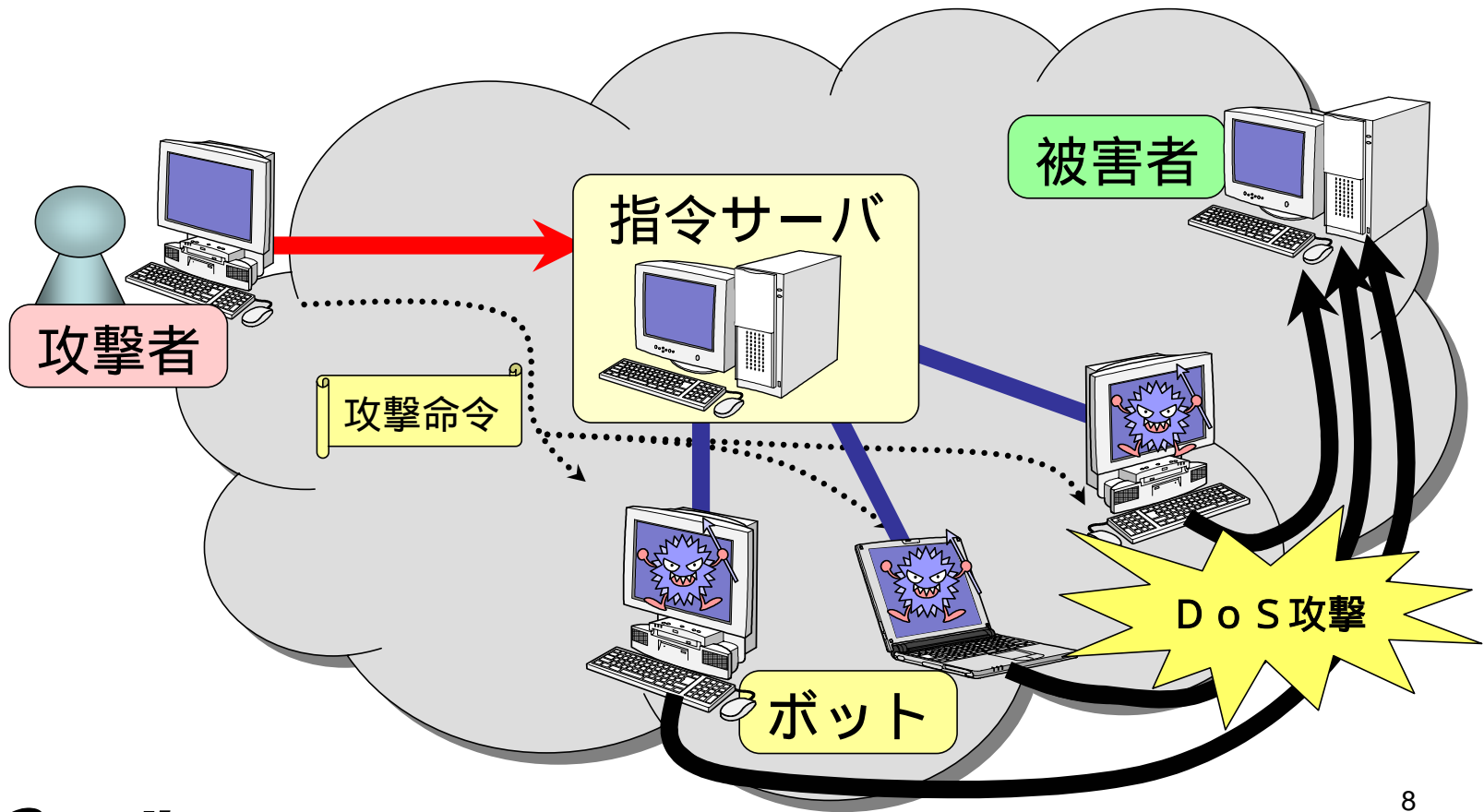
● 攻撃者

- 指令サーバへ管理者として接続、命令送信
- 金銭目的であることが多い

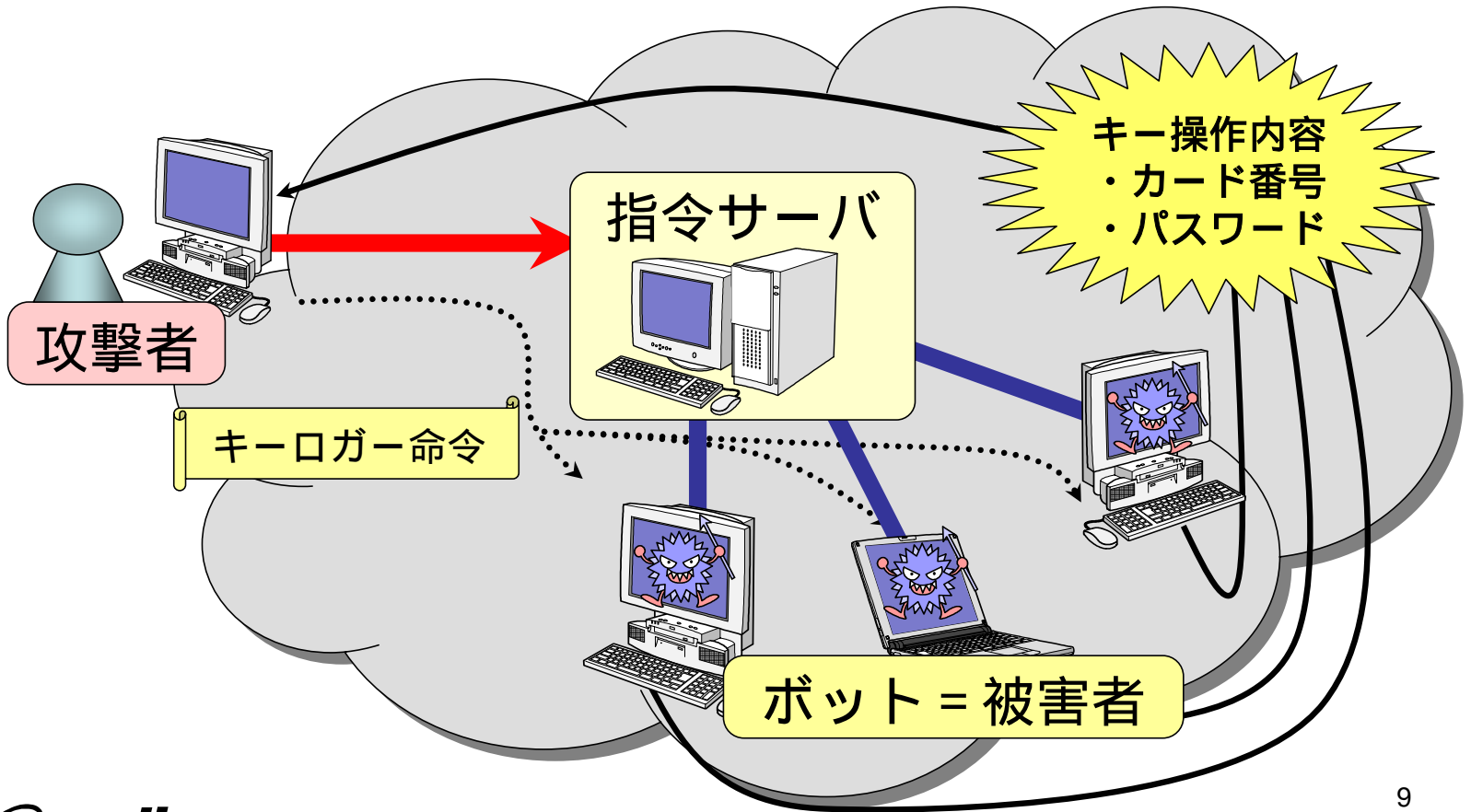
ボットネットの危険性

- コンピュータウイルス
 - 勝手に破壊活動などをするプログラム
- ワーム
 - 自己増殖するコンピュータウイルス
- ボット
 - 攻撃や感染拡大、情報窃盗など多機能
 - 見つからないように動作、遠隔操作可能
 - ソースコード公開～機能追加変更が可能

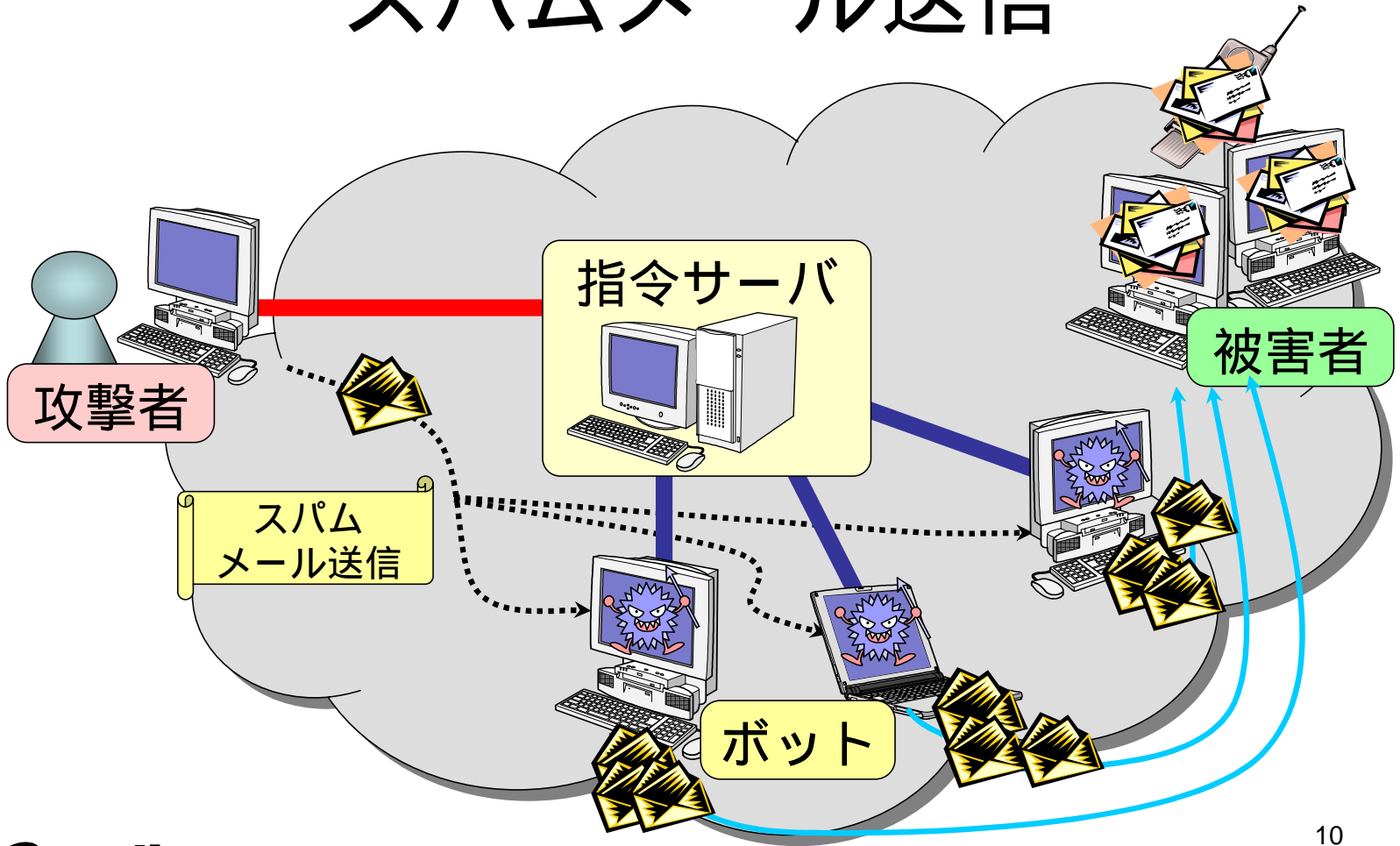
D o S 攻撃



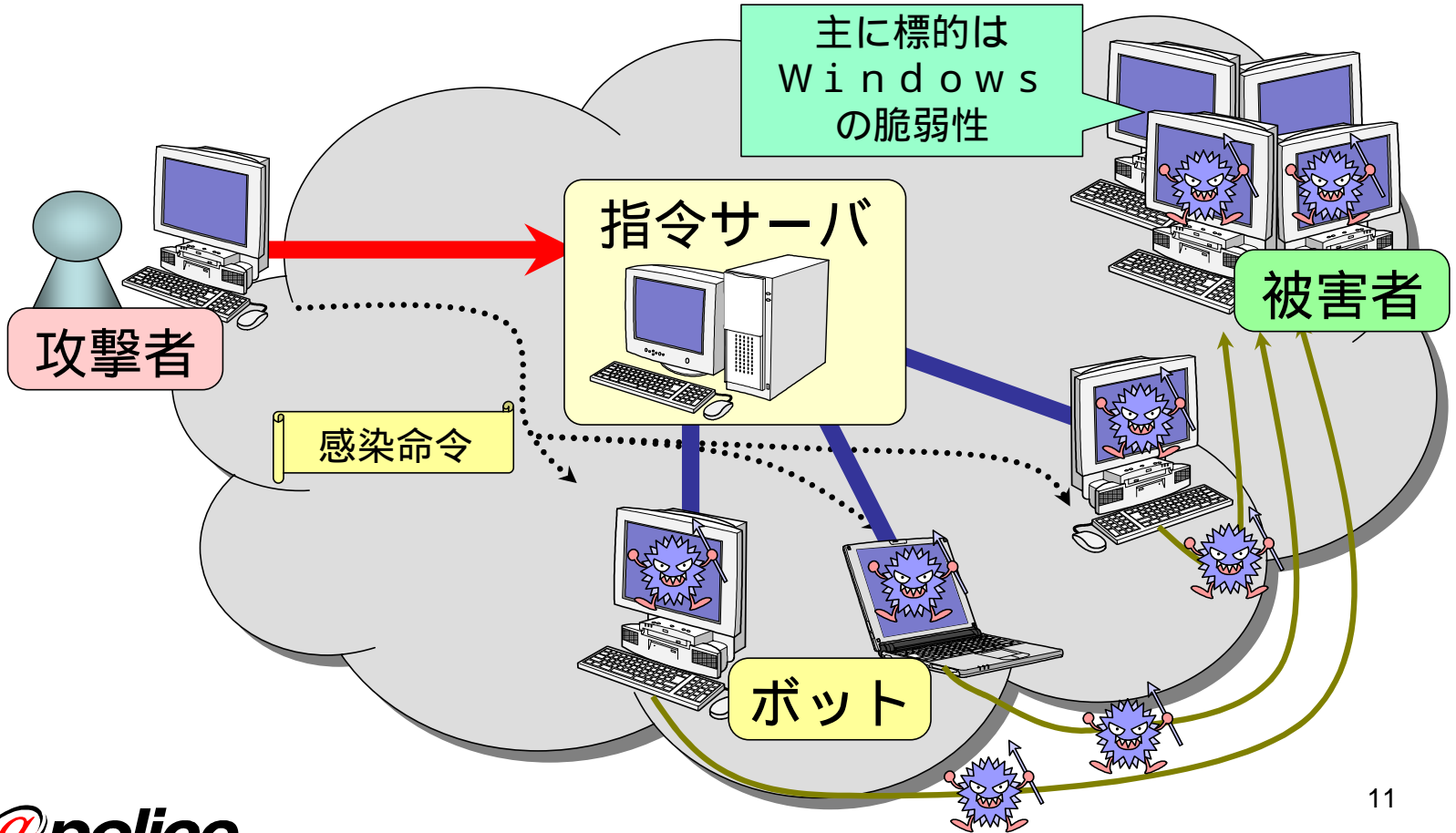
キーロガー



スパムメール送信



感染活動



2 . ボットネットの現状

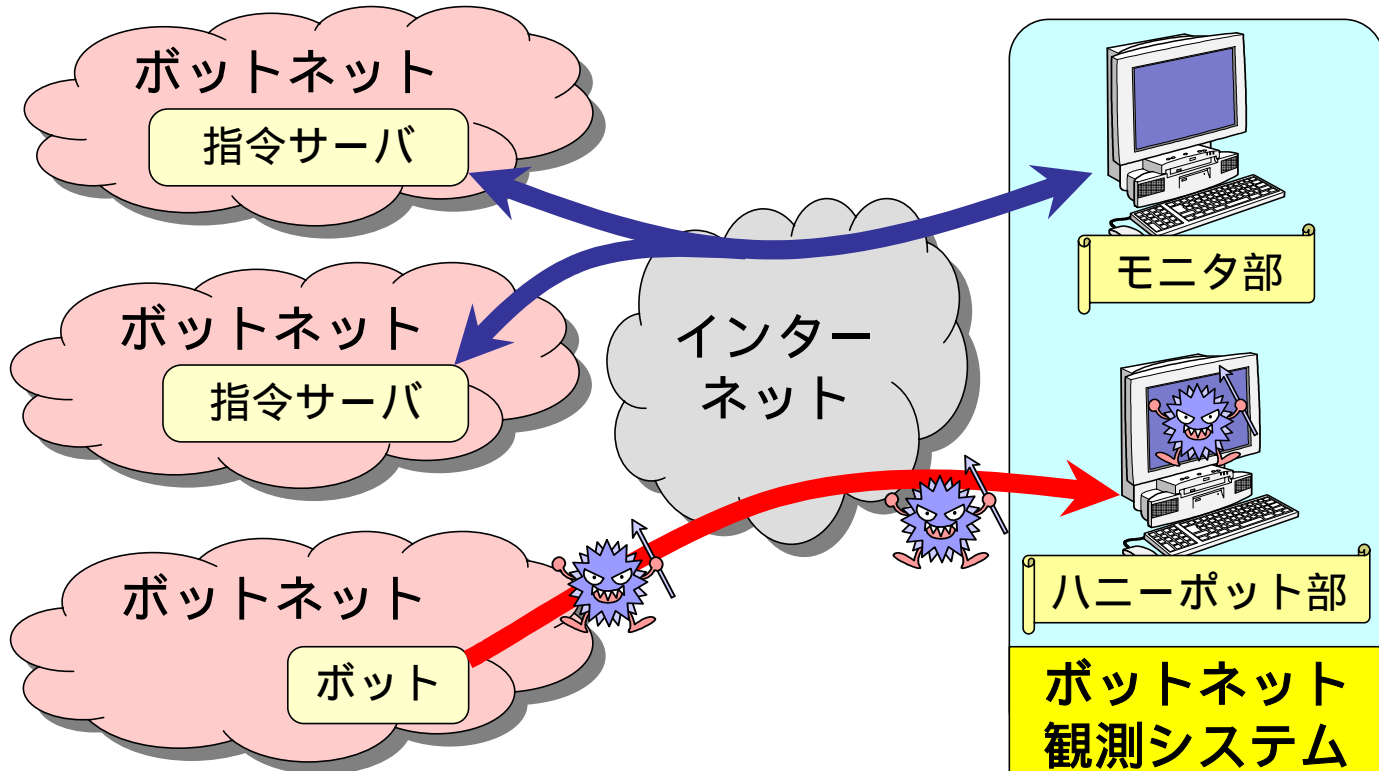
ボットネットの犯罪報道

- 2004年 6月 発生
 - DNSサーバへの大規模なDoS攻撃
- 2005年10月 オランダで逮捕
 - DoS攻撃で企業恐喝
- 2005年11月 アメリカで逮捕
 - ボットネット自体の販売・レンタル
- 2006年 5月 韓国で逮捕
 - 1万6千台のボットでスパムメール送信

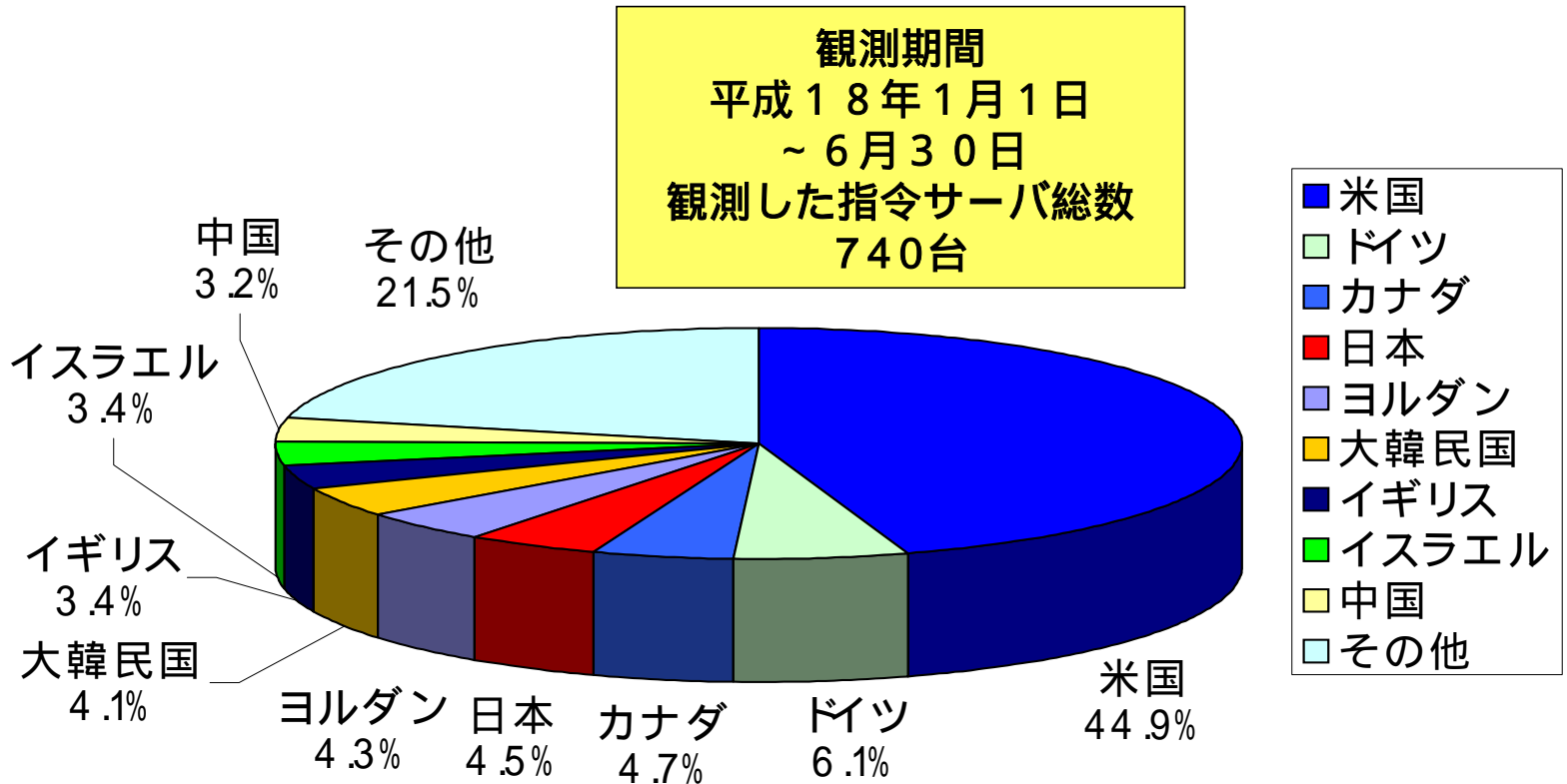
ボットネット観測システム

- H 1 7 年 1 月 から 運用 開始
- システム 構成
 - 命令 を 記録 する 「 モニタ部 」
 - 実際 に 感染 させる 「 ハニーポット部 」

観測システム～概要図



指令サーバの分布状況



3 . 对策等

今後の動勢

- ボットネットの多様化
 - ネットワーク（OS等の脆弱性）
 - Windowsの脆弱性を狙った感染以外にもLinuxを対象とした感染も出現
 - 新たな脆弱性を狙う感染手法を実装
 - 電子メール
 - Webサイト
 - P2P・インスタントメッセンジャー等

対策（１）

- ボットネットを撲滅するには
 - ボットの数減らすことが第一
 - OSの定期的なアップデート
 - ウイルス対策ソフトの導入
 - パーソナルファイアウォールの導入
- 等の基本的な対策

対策（２）

- ボットネットを撲滅するには
 - ボットの数減らすことが第一
 - ユーザのセキュリティ意識の向上、
 - そのためにセキュリティ啓発活動が重要

今後の動勢

- ボットネットの多様化
 - ネットワーク（OS等の脆弱性）
 - Windowsの脆弱性を狙った感染以外にもLinuxを対象とした感染も出現
 - 新たな脆弱性を狙う感染手法を実装
 - 電子メール
 - Webサイト
 - P2P・インスタントメッセージー等

インターネットにおける
ボットネットの現状と対策について

警察庁セキュリティポータルサイト@police
<http://www.cyberpolice.go.jp/>

警察庁情報通信局
情報技術解析課