HITACHI
Inspire the Next

遠隔操作ツール RATの紹介

～Poison Ivy～

2012/05/25
Hitachi Incident Response Team
寺田　真敏

RAT: Remote Access Trojan / Remote Administration Tool

遠隔操作ツール（RAT）

⇒ APT攻撃につながる機能改良

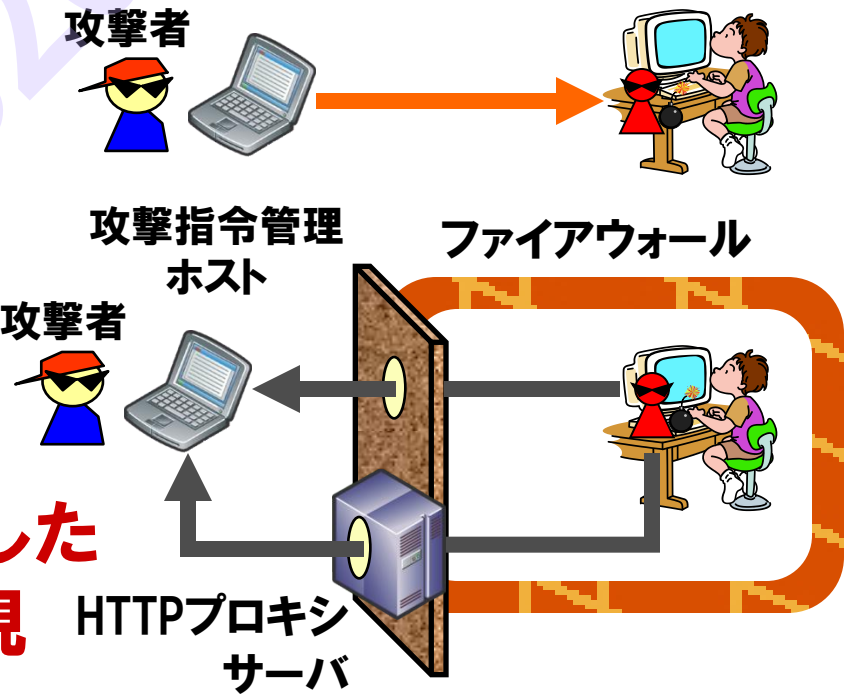
- 遠隔操作ツール（RAT）の進化
  侵入したシステムを遠隔から操作するためのプログラム
  潜伏活動や窃取活動で利用されている

攻撃側発呼型から

- 2000年前後 BackOrifice、SubSeven など

攻撃側着呼型へ

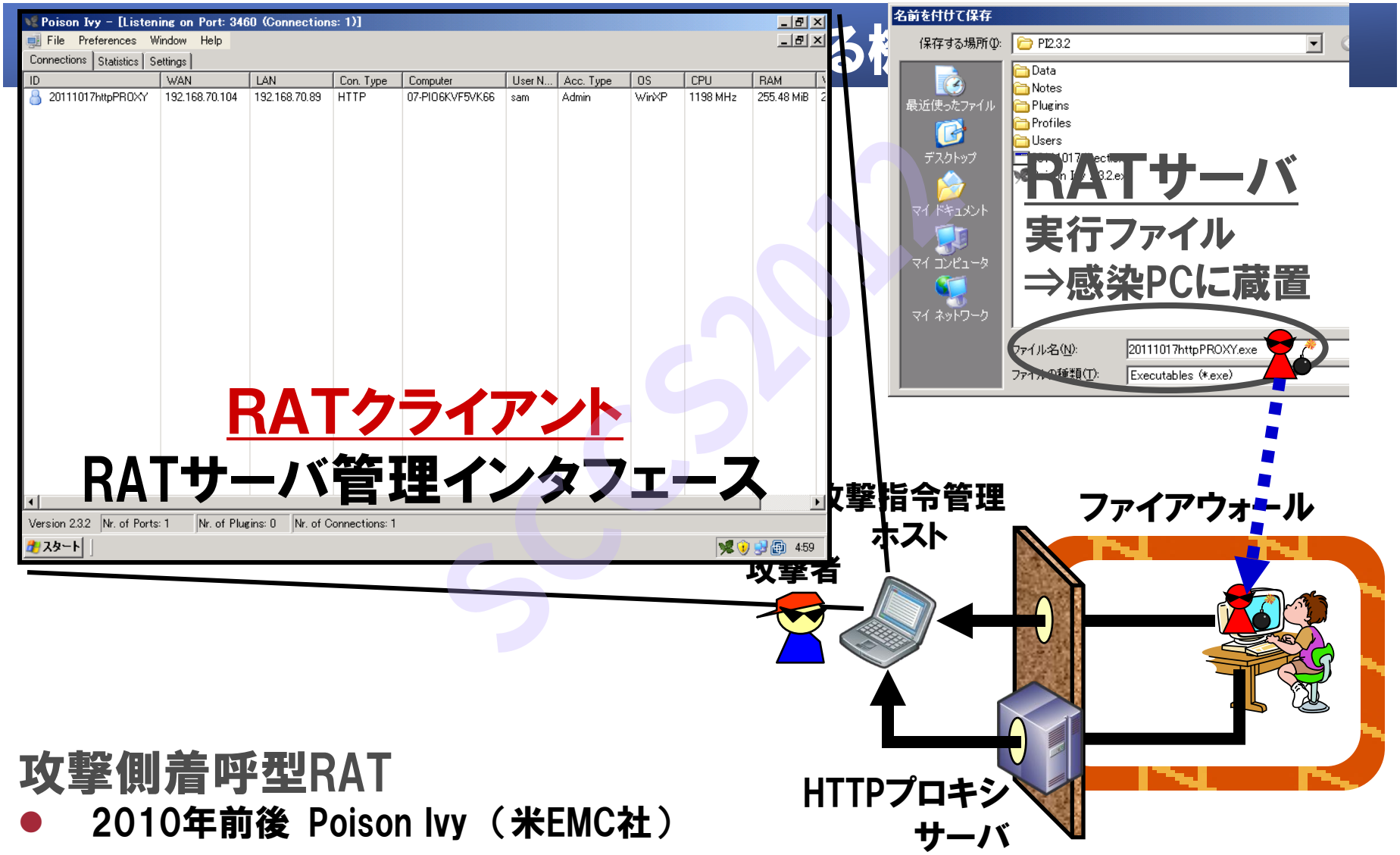
- 2010年前後 Poison Ivy（米EMC社）
  MFC Hunter（三菱重工業）



⇒潜伏中、ファイアウォールを介した
外部接続可能な通信環境を実現

RAT: Remote Access Trojan / Remote Administration Tool

1 遠隔操作ツール（RAT）



攻撃側着呼型RAT

- 2010年前後 Poison Ivy（米EMC社）

RAT: Remote Access Trojan / Remote Administration Tool

RATサーバ（＝窃取活動用ウイルス）

HIRT Hitachi Incident Response Team

①攻撃指令管理ホスト、中継の設定

←攻撃指令管理ホスト
←HTTPプロキシサーバ

RATサーバの作成
GUIで2ステップ
ほどの操作

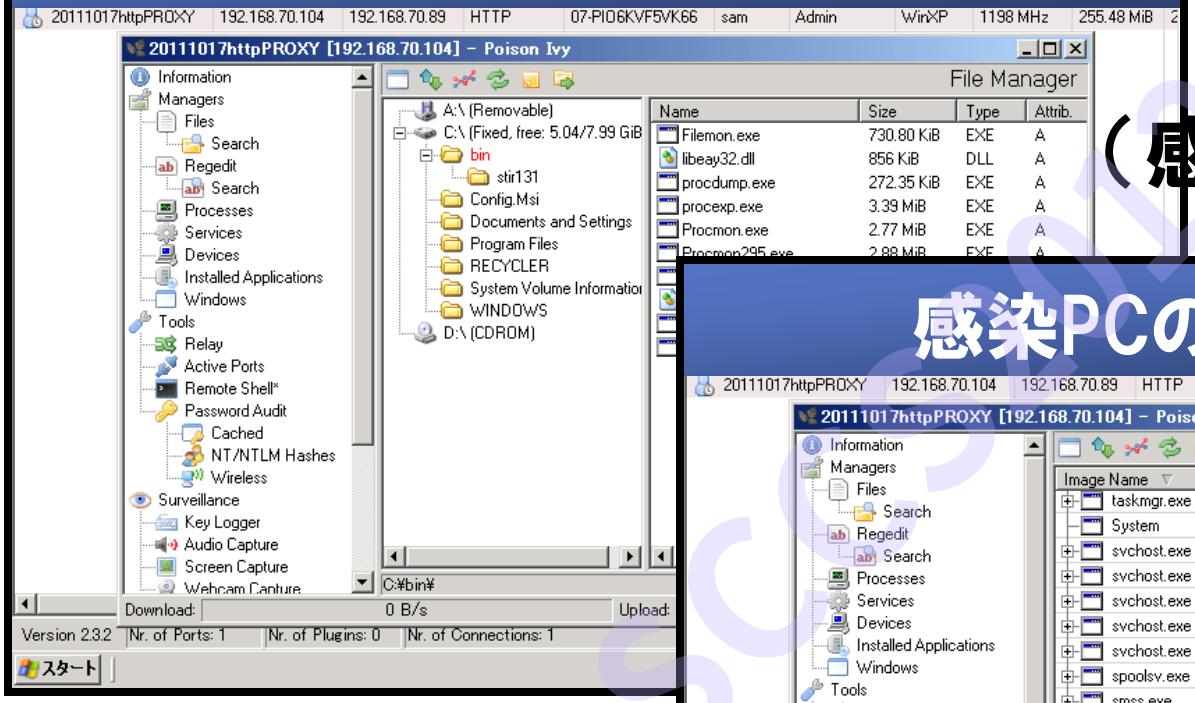
②実行ファイルの生成

RATサーバ
実行ファイル
⇒感染PCに蔵置

2 RATサーバ（＝窃取活動用ウイルス）

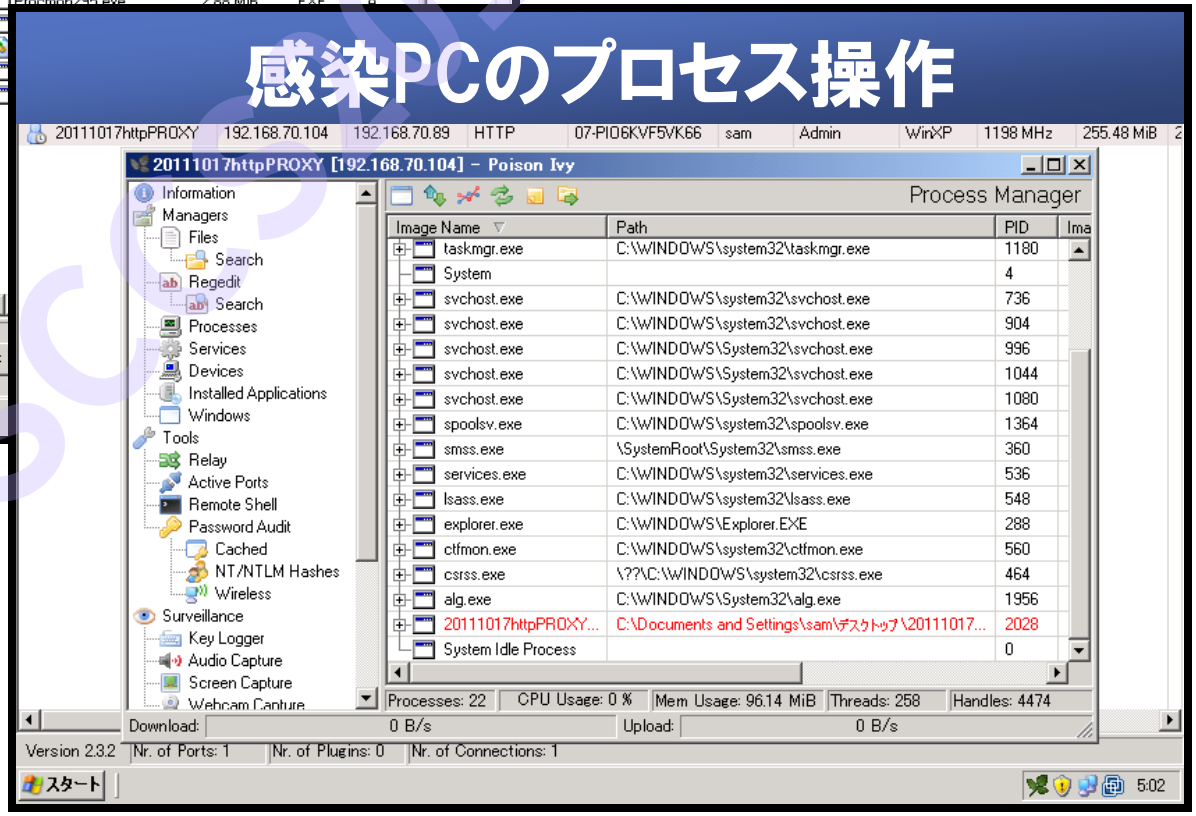
Hitachi Incident Response Team

感染PCのファイル／フォルダ操作



RATサーバの遠隔操作（感染PCの遠隔操作）

感染PCのプロセス操作

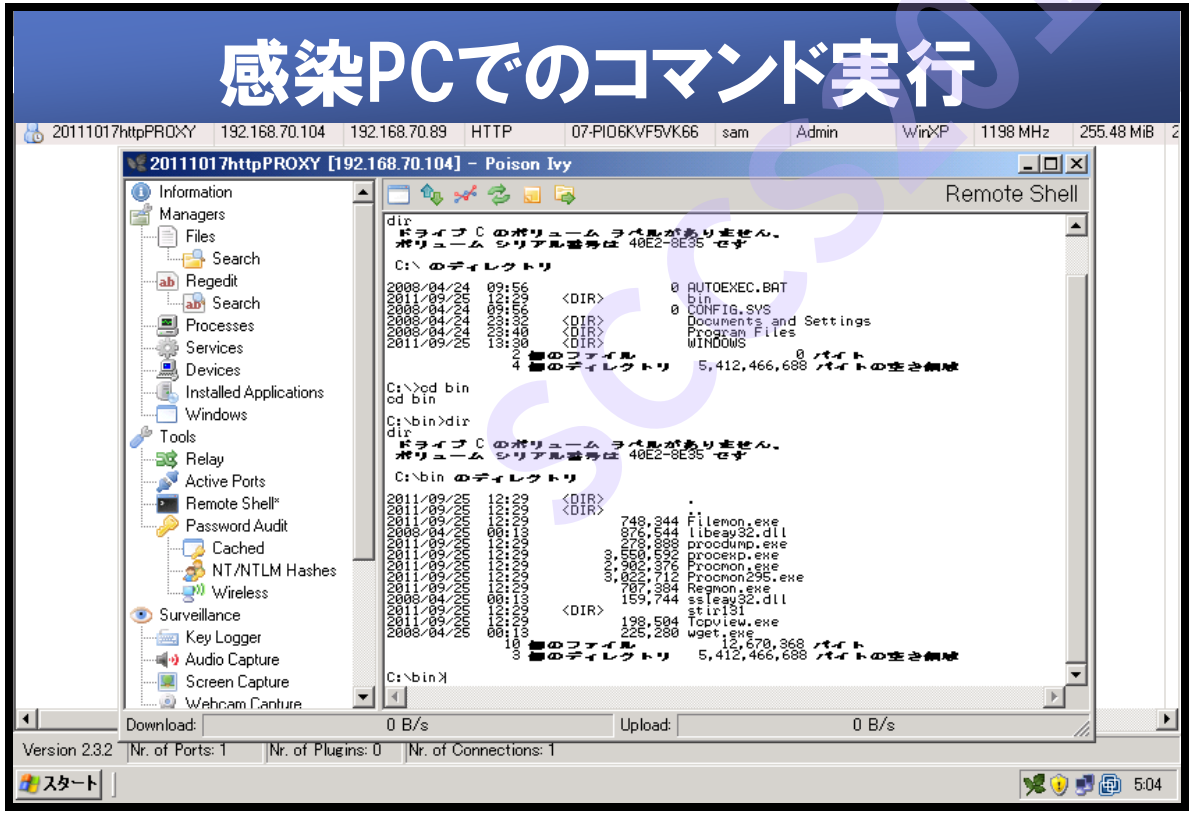


PCを直接操作している状態と等価

3 遠隔操作ツール(RAT)による情報窃取

Hitachi Incident Response Team

RATサーバの遠隔操作（感染PCの遠隔操作）

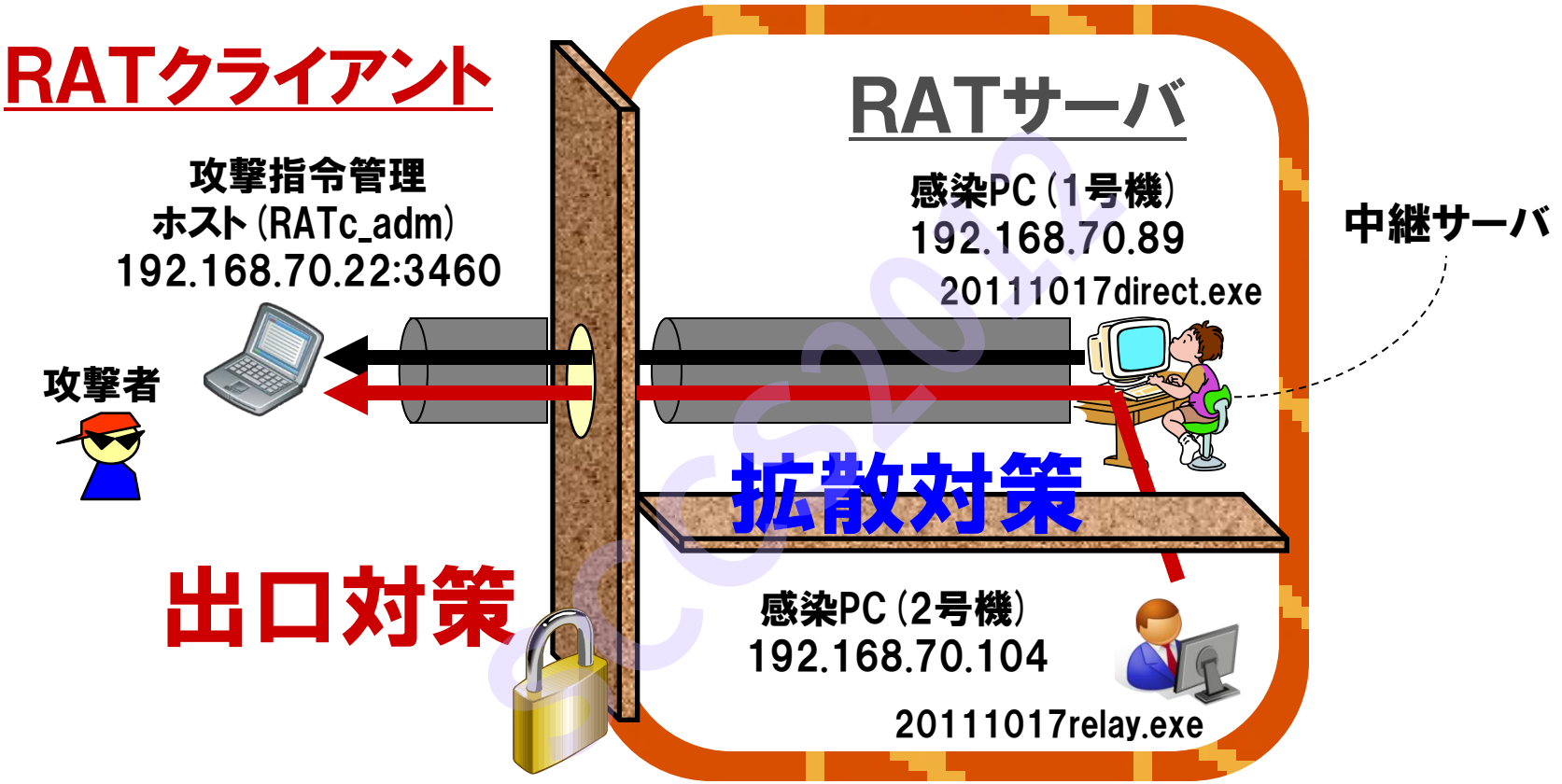


3 遠隔操作ツール（RAT）による情報窃取

感染PCの画面キャプチャ

RATサーバの遠隔操作（感染PCの遠隔操作）

4 対策



感染PC(2号機)が直接外部と通信できない環境に設置されていても、
攻撃指令管理ホストは、中継機能を使うことによって、
攻撃指令管理ホストと感染PC(1号機)の通信路(土管)を介して、
感染PC(2号機)を遠隔操作できる。

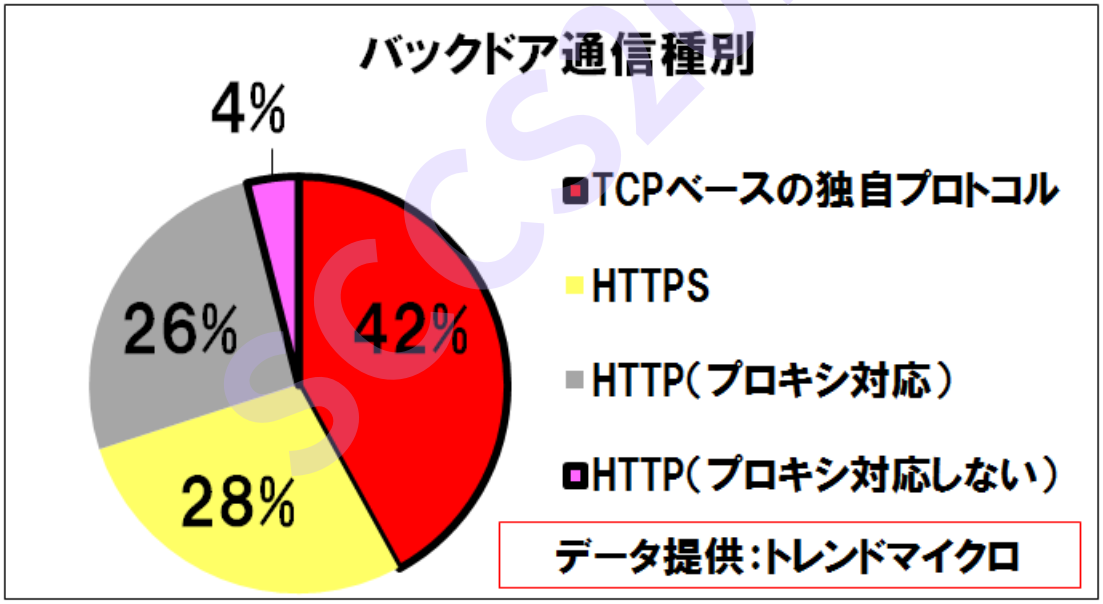
Hitachi Incident Response Team

出口対策例（設計での対策）
① サービス通信経路設計の効果

出口対策

IPA

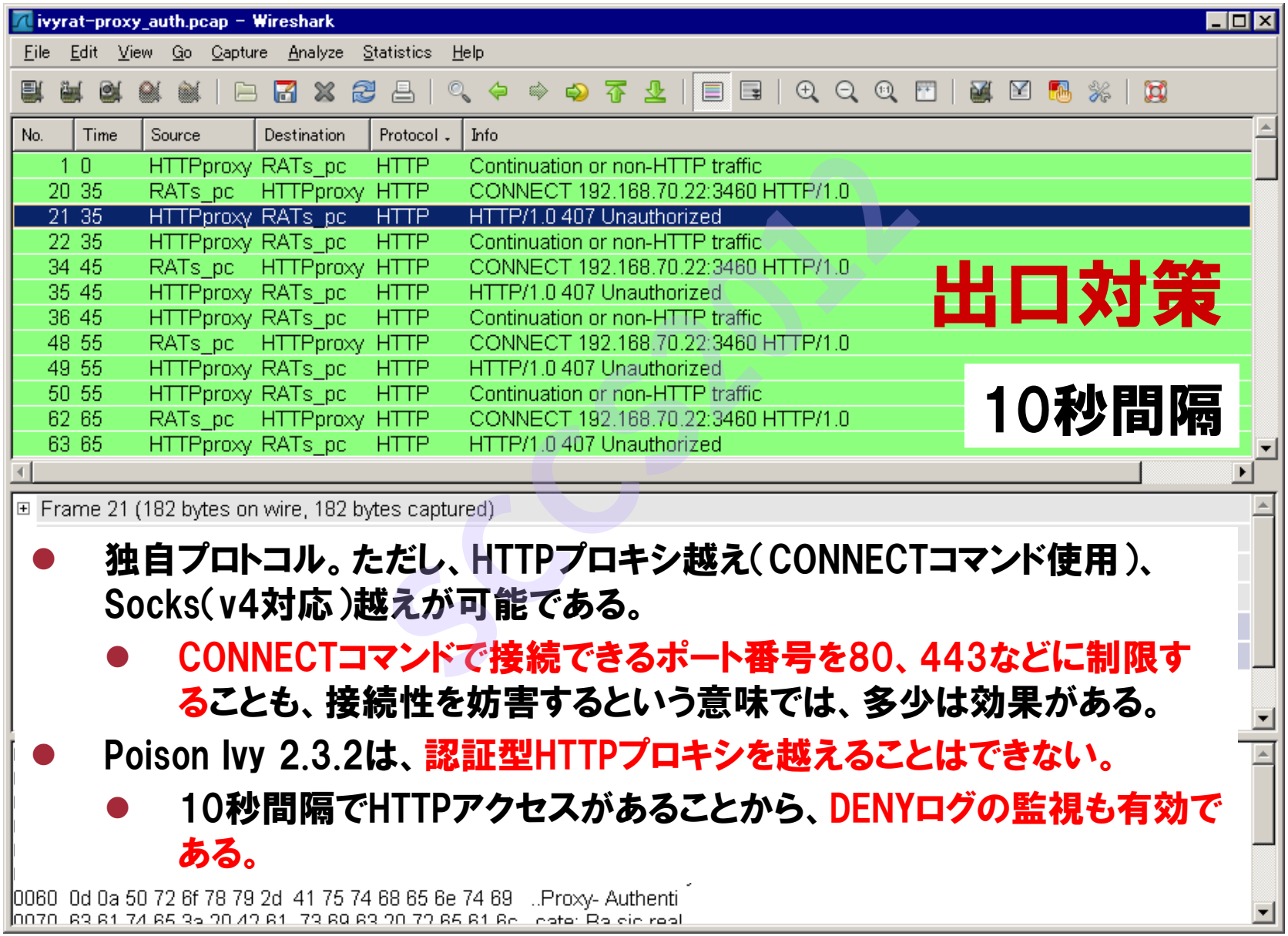
- FWでプロキシ経由以外の通信を遮断することで・・・
  - TCPベースの独自プロトコルとHTTP（プロキシ対応しない）通信の46％のバックドア通信を遮断可能。



※2011年4月～10月国内で収集
標的型攻撃メールに添付されていたと思われるウイルス50個のバックドア通信サンプル

9

4 対策



- 独自プロトコル。ただし、HTTPプロキシ越え(CONNECTコマンド使用)、Socks(v4対応)越えが可能である。
  - CONNECTコマンドで接続できるポート番号を80、443などに制限することも、接続性を妨害するという意味では、多少は効果がある。
- Poison Ivy 2.3.2は、認証型HTTPプロキシを越えることはできない。
  - 10秒間隔でHTTPアクセスがあることから、DENYログの監視も有効である。