2008年のネットワーク運用における セキュリティ動向

NTT communications
先端 IPアーキテクチャセンタ

NSP-Security-Japan Moderator

水口 孝則

2002 – *実際にあった*セキュリティ問題

The *Real* Security Problem

- 2002年9月頃、ISP/SP *セキュリティ運用*技術者は以下のことができなかった:
  September 2002 ISP/SP Operations Security Engineers could not:
  - 直接接続されているピア相手の知り合いの *セキュリティ*技術担当者を見つけられなかった
    Find their *security* colleagues in their directly attached peers.
  - 2 Hop 離れているプロバイダだとセキュリティ技術者自体が見つけられなかった
    Find security engineers in providers two hops away.
  - アジア地域だとまったくもってセキュリティ技術者を見つけられなかった
    Find ANY security engineers in the Asian providers.
- 大きなセキュリティ攻撃があった場合、まずそもそも共同に攻撃に対して効果的にアクションをとる以前の問題である、誰と一緒に作業をすればいいのかすらわからなかった
  When big attacks happened, there was no way for the people who needed to work with each other to find/contact one another … let alone work collectively to mitigate the attack.

JANOG14 から

NSP-Security立ち上げ

2003 – 変化が起こった年

A Year of Difference

2003年9月　ISP/SPセキュリティ運用者は以下が可能になった
September 2003 ISP/SP Operations Security Engineers Can:

- 直接接続されているピアやグローバルISPだと知っているセキュリティ技術担当者を見つけることができる
  Find their *security* colleagues in their direct peers and a huge range of global ISP/SPs
- メール、チャット、iNOC電話、電話などを用いてインターネット上の攻撃等に共同で対応できるようになった
  Work with each other via email, chat, iNOC Phone, and POTs to collectively mitigate attacks and incidents on the Internet
- プロバイダ間でTracebackや対応をできる
  Execute inter-provider traceback and mitigation
- 起こることが予測されている攻撃(Blaster等)に対して事前対応できた
  Apply proactive measures to prepare for projected attacks (e.g., Blaster)

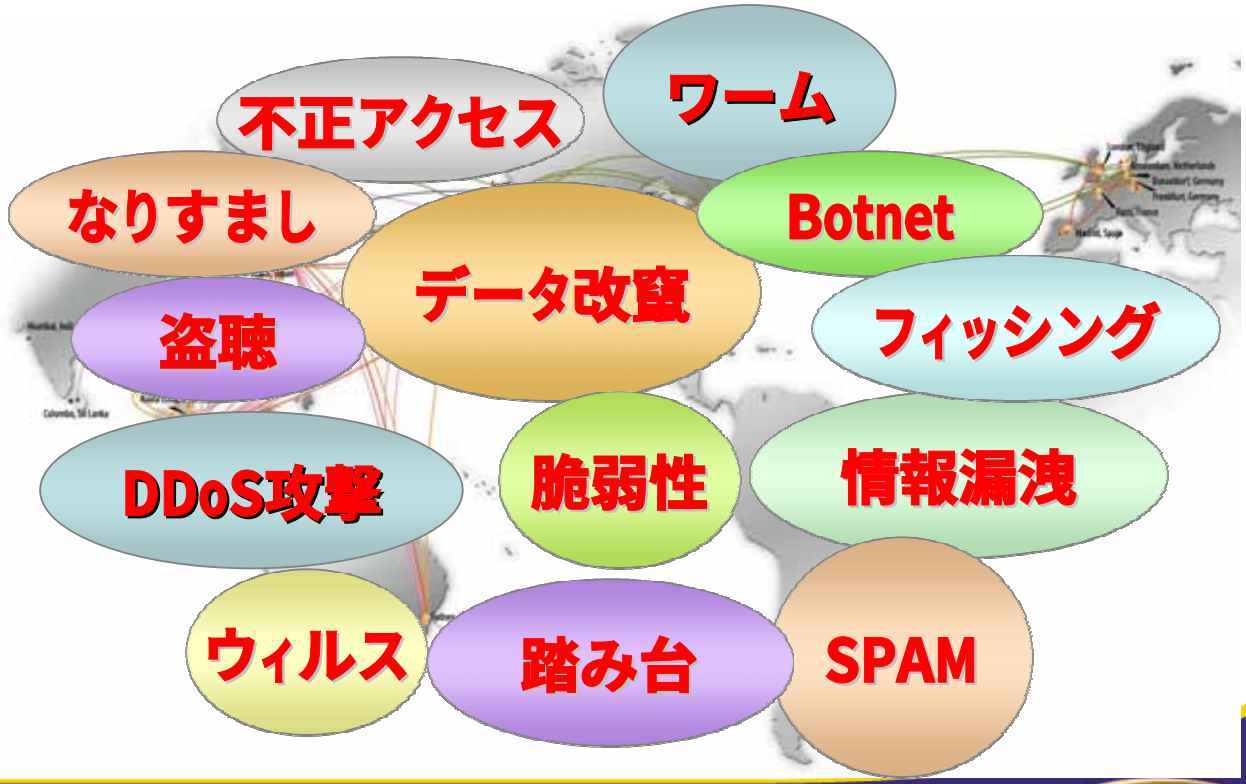
What changed?

JANOG14　から

■NSP-Security/NSP-Security-Japanとは…
・世界中のISP/SPが連携してセキュリティ対応を行うコミュニティ

NTT Communications

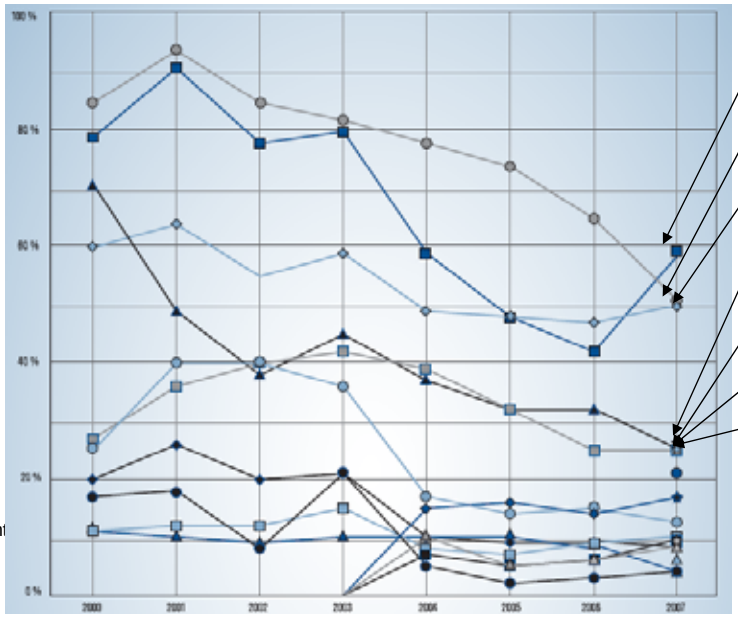
ネットワークに起因する様々なセキュリティ問題



NTT Communications

過去12カ月のアタックタイプと不正トラフィック検知状況

-CSI/FBI 2007 Computer Crime & Security Survey

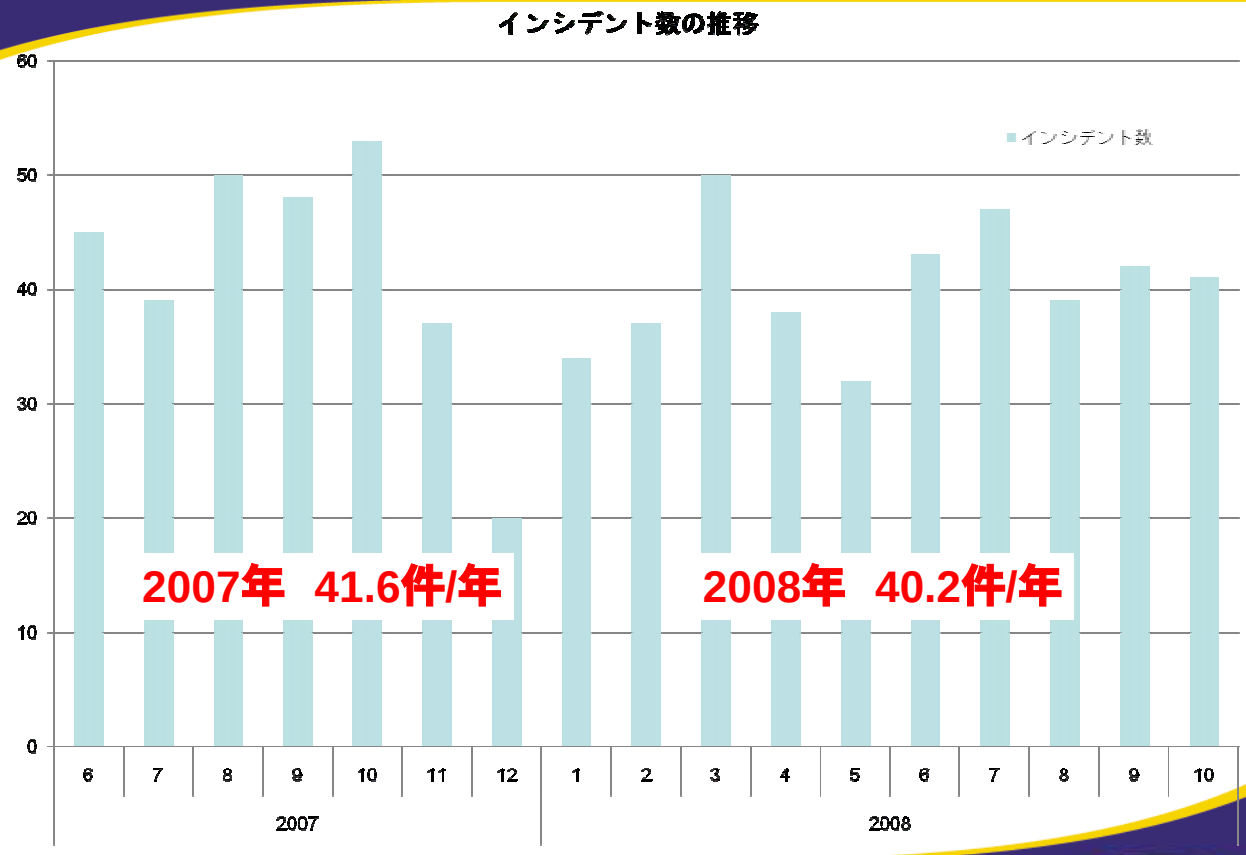


- 内部からの不正利用
- ウィルス
- PC盗難
- フィッシング
- DoS (Denial of Service)
- 情報への不正アクセス
- Instant messenger Abuse

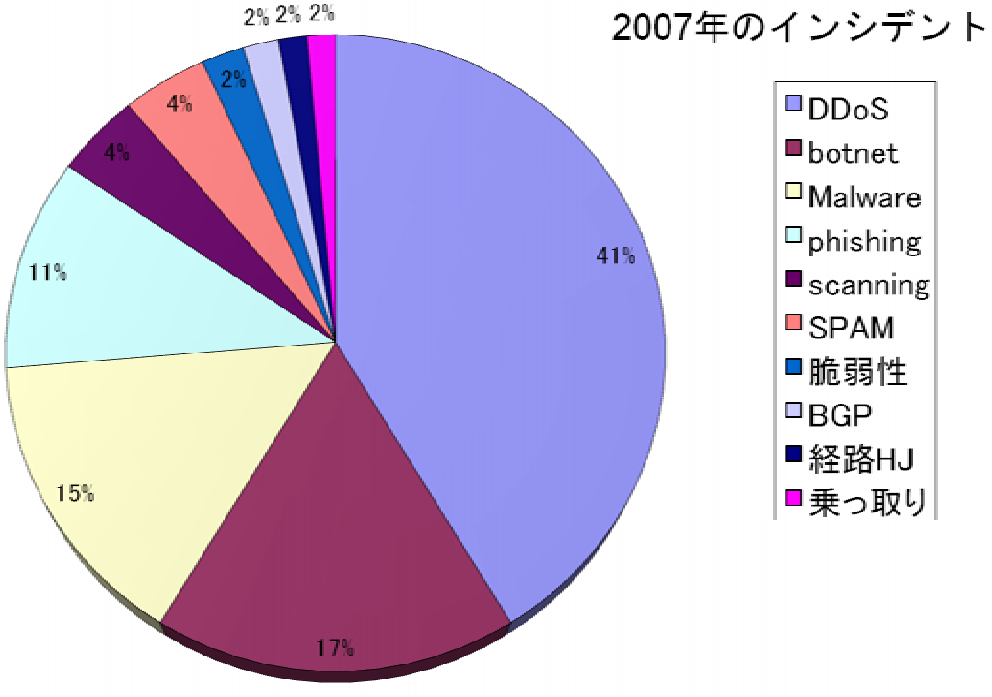
•ウイルス検知は年々減少の傾向にある
•2007年にフィッシングやメッセンジャーSPAM (Vishing) などが登場

NSP-Securityに見るSecurityの動向

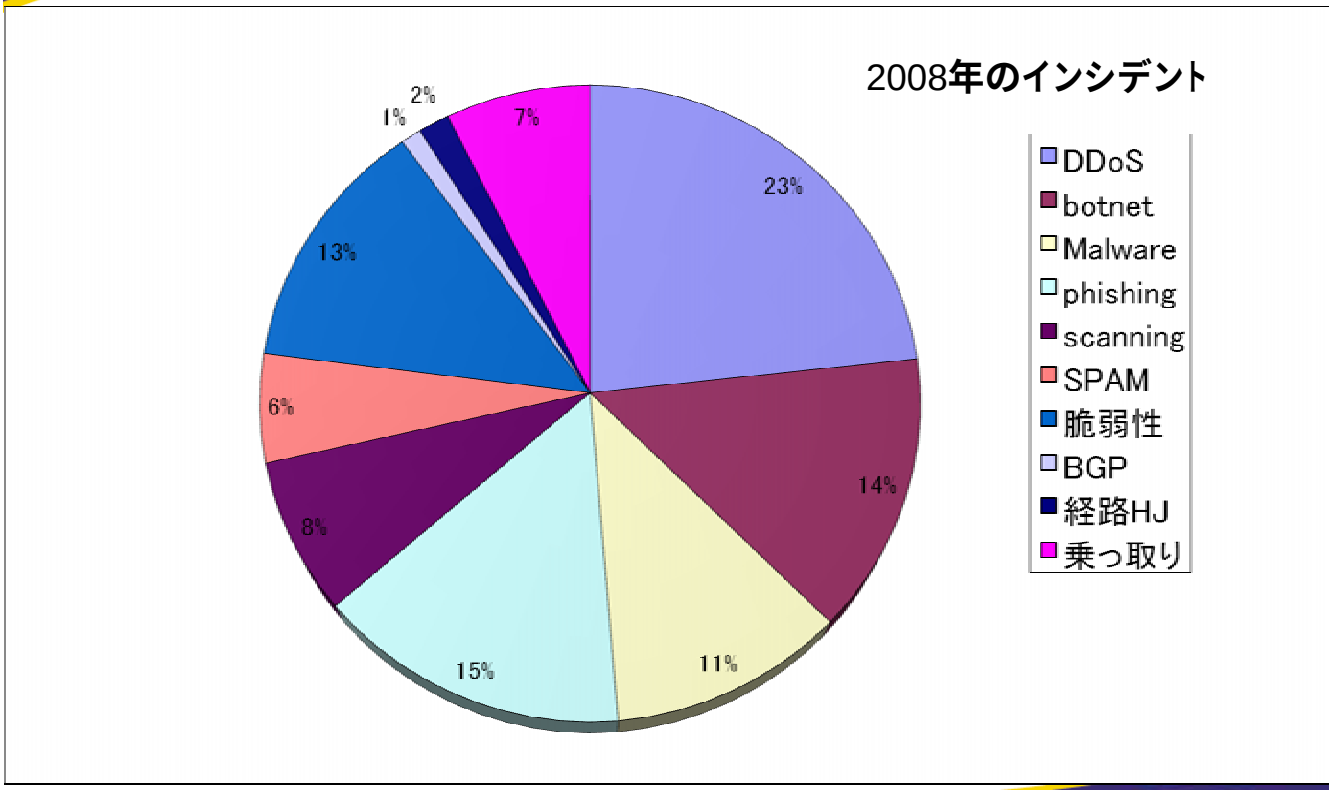
対応インシデント数



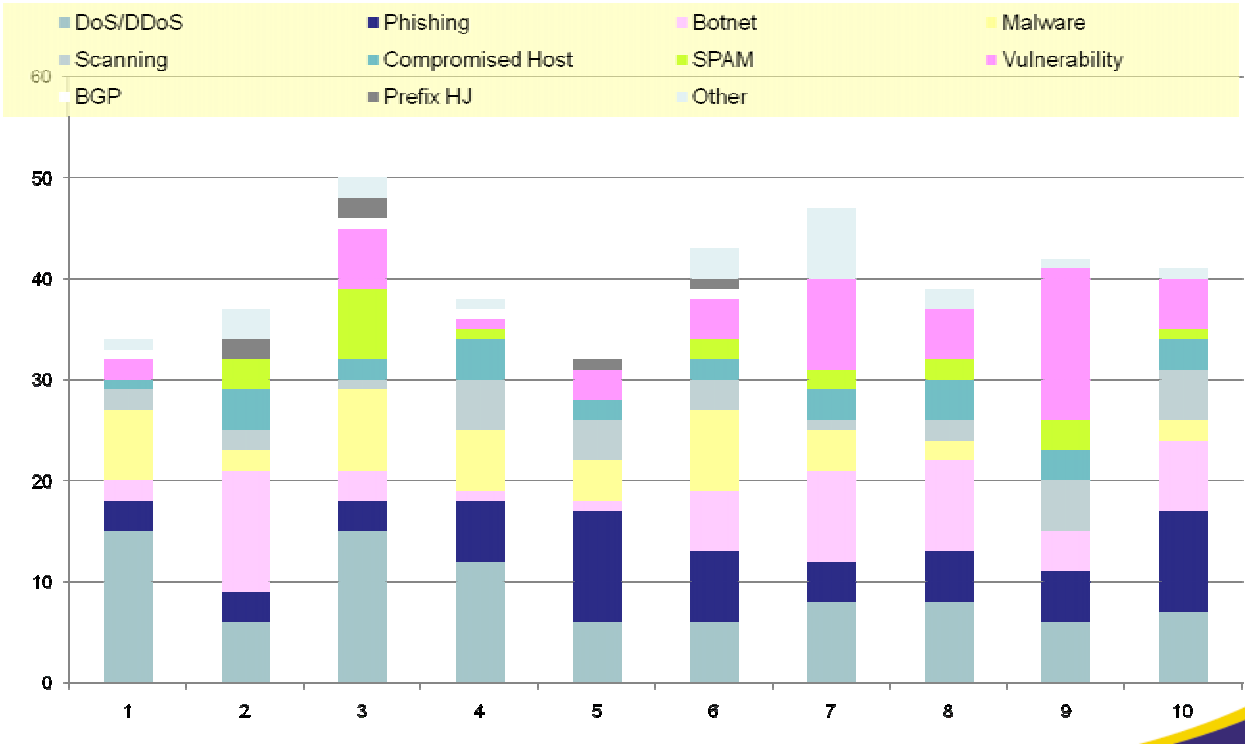
インシデント種別（2007年6月～12月）



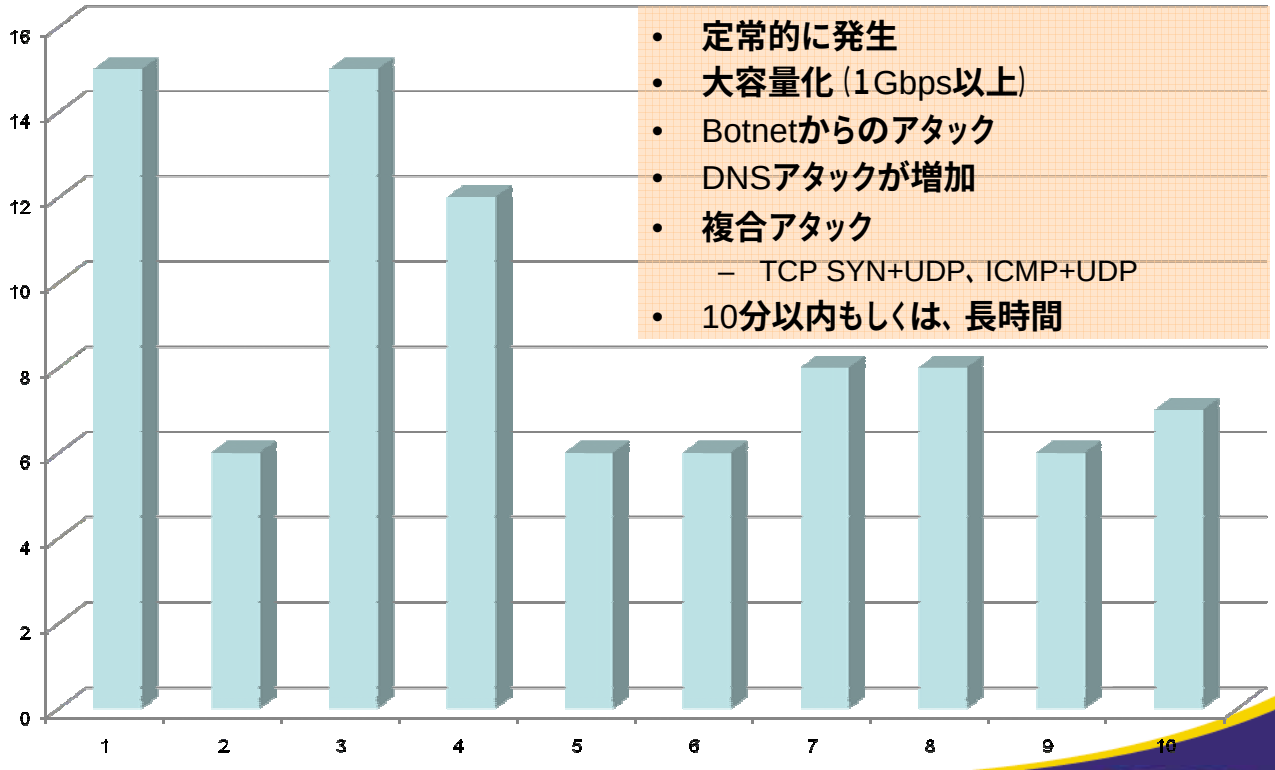
インシデント種別 (2008年1月～9月)



インシデント種別

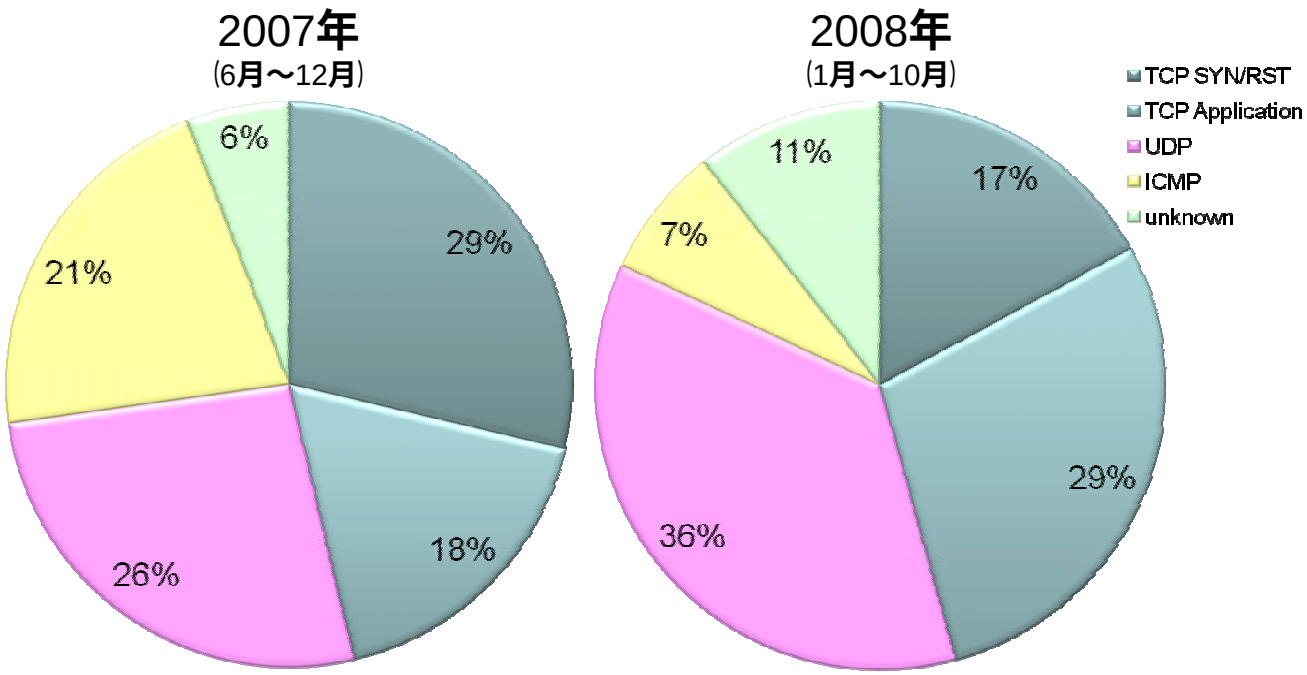


DDoSの特徴

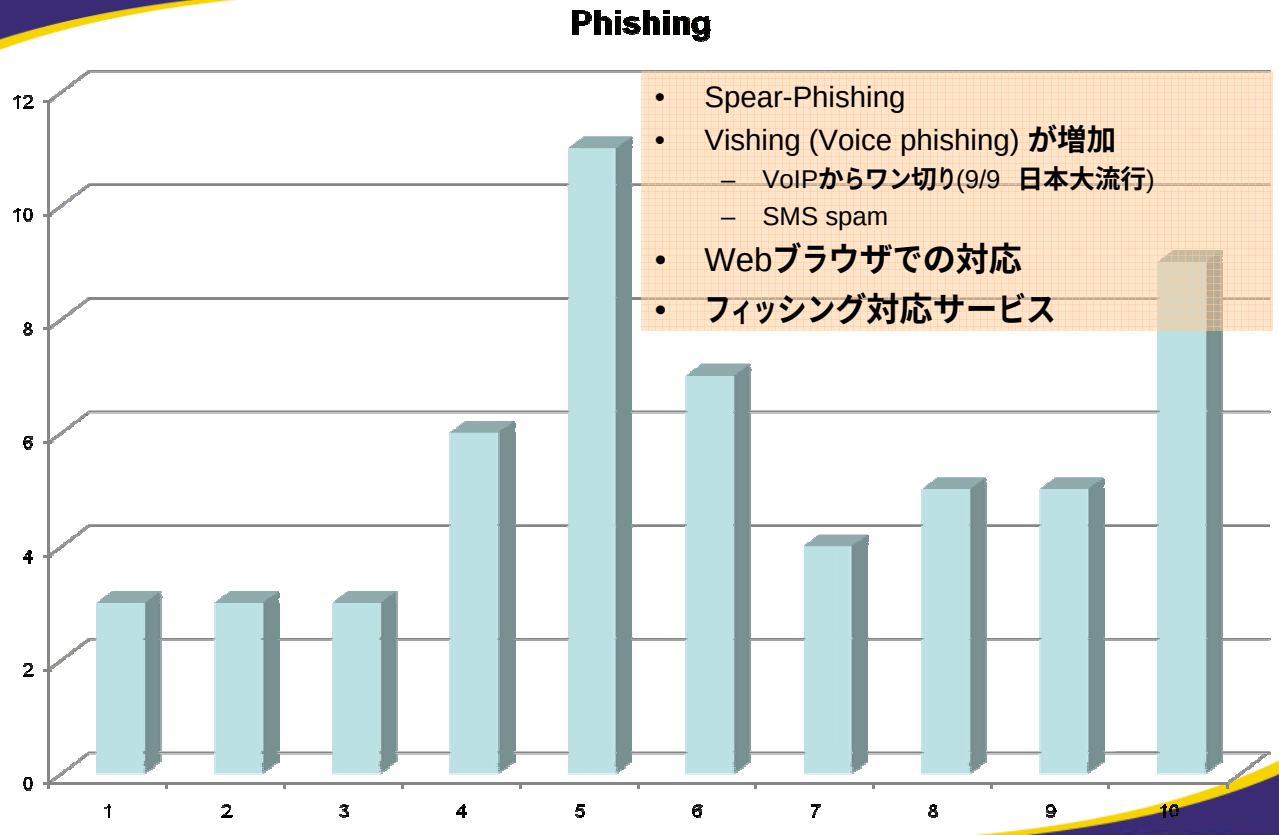


- 定常的に発生
- 大容量化（1Gbps以上）
- Botnetからのアタック
- DNSアタックが増加
- 複合アタック
  - TCP SYN+UDP、ICMP+UDP
- 10分以内もしくは、長時間

DoS/DDoS アタック種別

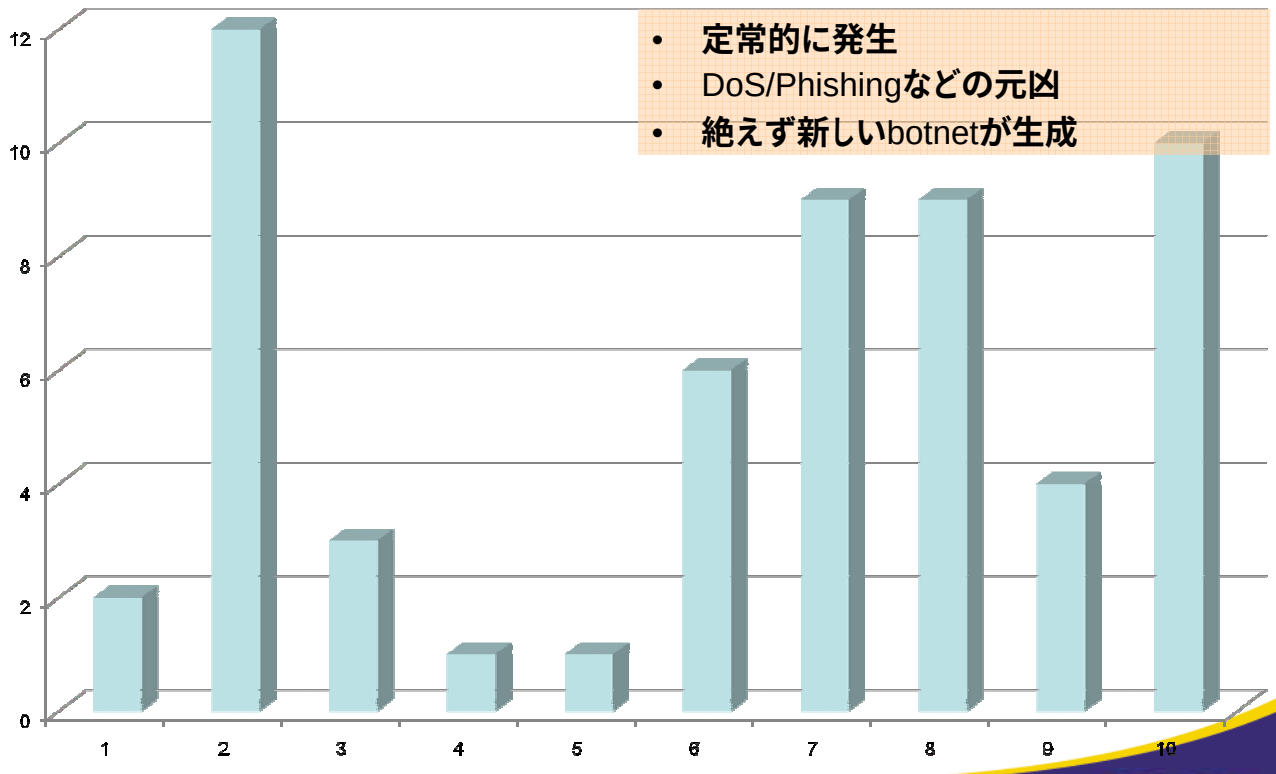


Phishingの特徴



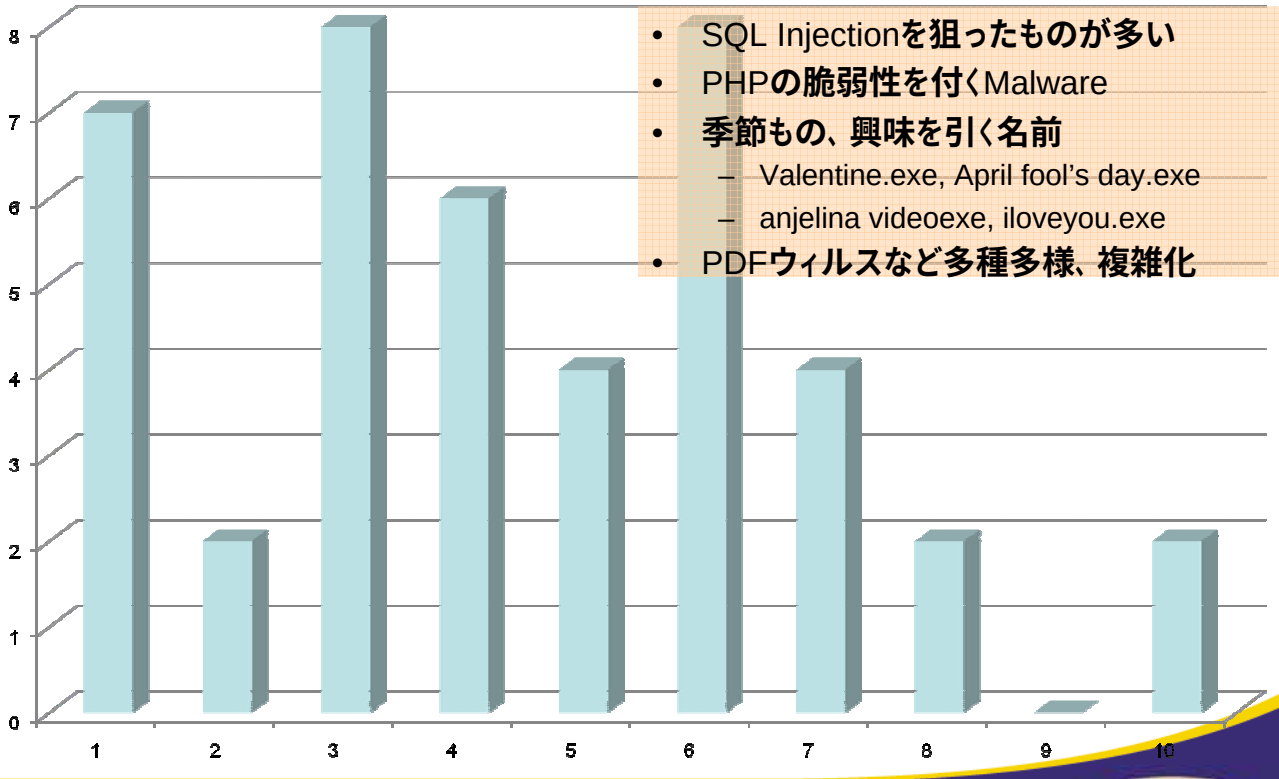
- Spear-Phishing
- Vishing (Voice phishing) **が増加**
  - VoIP**からワン切り**(9/9 **日本大流行**)
  - SMS spam
- **Webブラウザでの対応**
- **フィッシング対応サービス**

Botnetの特徴



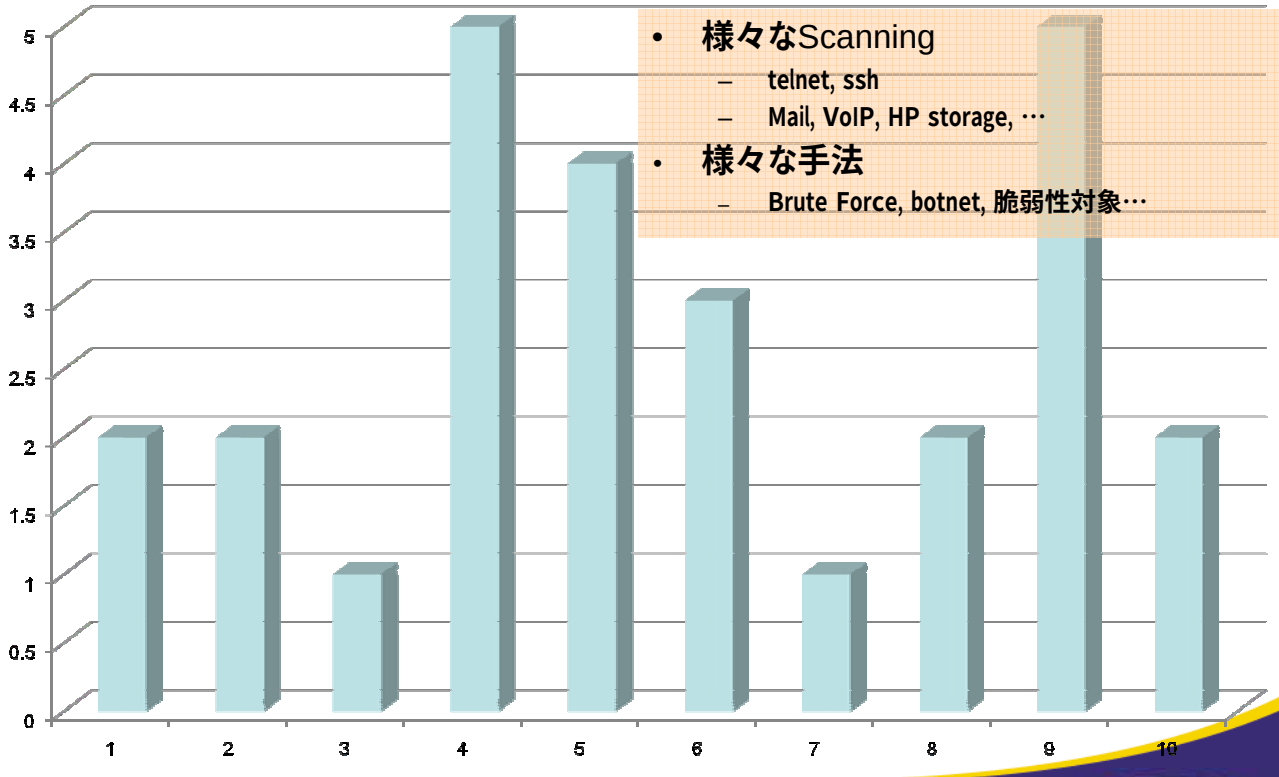
- **定常的に発生**
- DoS/Phishing**などの元凶**
- **絶えず新しい**botnet**が生成**

Malwareの特徴



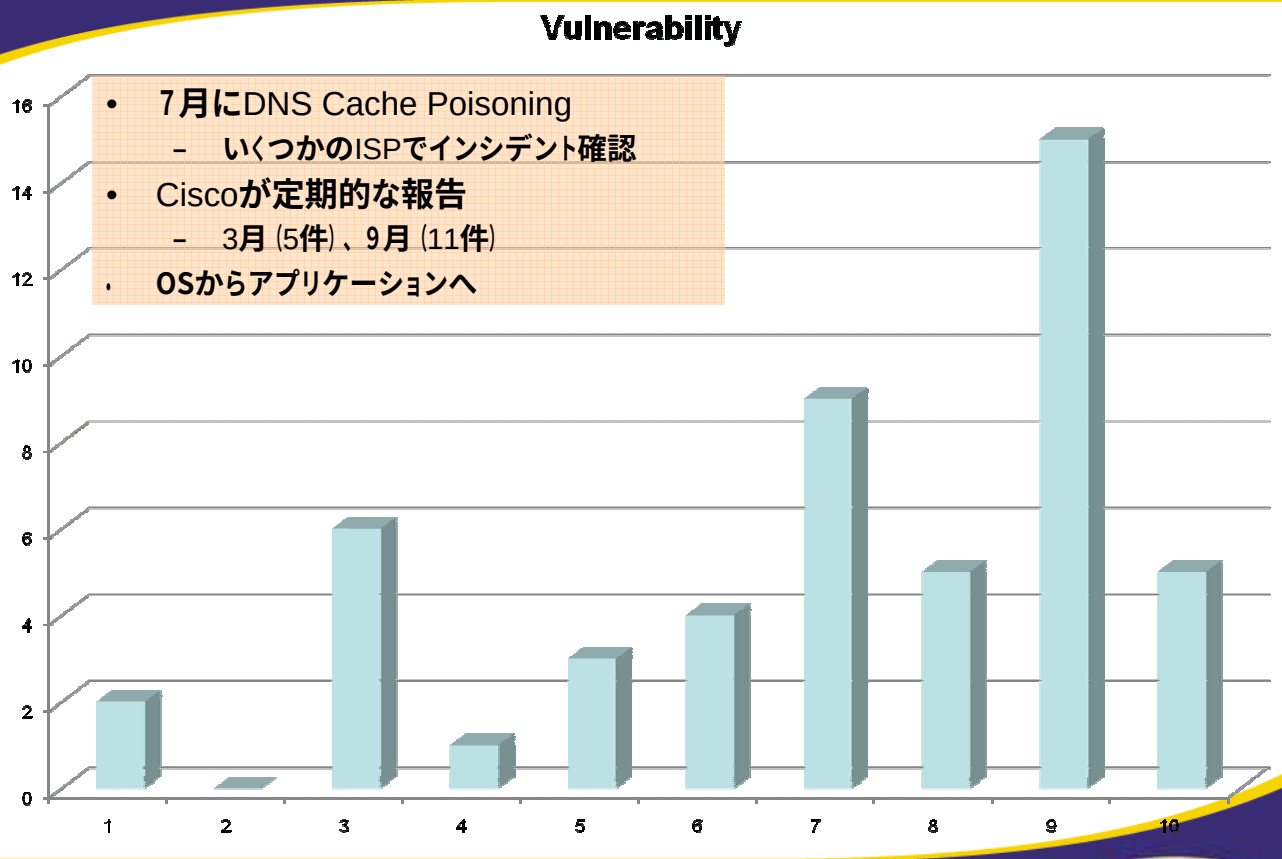
- SQL Injectionを狙ったものが多い
- PHPの脆弱性を付くMalware
- 季節もの、興味を引く名前
  - Valentine.exe, April fool's day.exe
  - anjelina videoexe, iloveyou.exe
- PDFウィルスなど多種多様、複雑化

Scanningの特徴



- 様々なScanning
  - telnet, ssh
  - Mail, VoIP, HP storage, …
- 様々な手法
  - Brute Force, botnet, 脆弱性対象…

脆弱性 (Vulnerability)



2008年イベントに関連インシデント

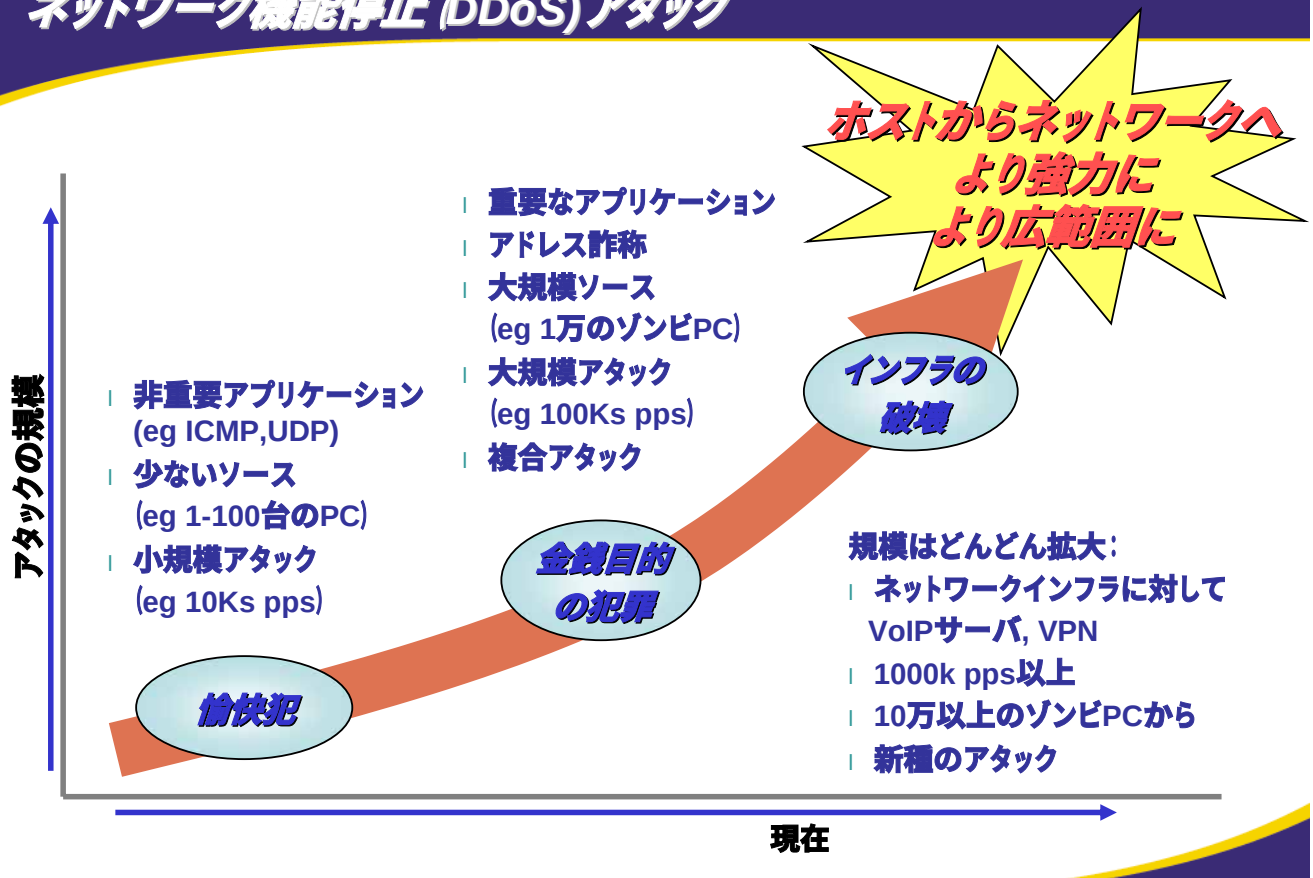
- 北京オリンピック
  - アタックは見受けられず
- 洞爺湖サミット
  - アタックは見受けられず
- ロシアのグルジア侵攻
  - 両政府のWebに*Cyber Attack*
- その他
  - イベント系Worm/Virus
    - Valentine.exe, April fool's day.exe
  - 大規模トラブル
    - YouTube経路ハイジャック
  - 2chへのアタック
    - 韓国の5000ホストのbotnetから

事例1：

- フリーDNSサービスを提供している業者がおりました
  - xxx.mizuguchi-dns.jp　　xxxという名前をフリー提供
- 誰かが、アカウント登録し、cookingというアドレスを登録
  - Cooking.mizuguchi-dns.jp　　10.0.0.1
- ある日、ユーザから苦情が寄せられたので見てみる
  - cooking.mizuguchi-dns.jpは、実は、phisingサイトだった
- フリーDNSの管理者が不正利用を確認し、以下の対処を実施
  - AccountをDisable
  - cooking.mizuguchi-dns.jp　　0.0.0.0
- 登録者（phising業者）から苦情が来た
  - 「24時間でサイトを落とすから、待って欲しい」と言ってきた
- 言うことを聞かないとPacketを送りつけるぞと脅迫
  - SkypeやVoIPプロバイダを使って、whoisに登録されている電話番号にPacket Floodingを掛けてきた

2008.1.17

ネットワーク機能停止（DDoS）アタック



Thank You!!

コンタクト：
nsp-security-jp-owner@puck.nether.net