JPCERT CC®

海外におけるインターネットセキュリティインシデント概観
～2009年7月の韓国大規模DDoSインシデントのその後

一般社団法人　JPCERTコーディネーションセンター
国際部　部長代理　鎌田敬介/ Keisuke Kamata

@Internet Week 2009
2009年11月24日

韓国大規模DDoSインシデント: おさらい

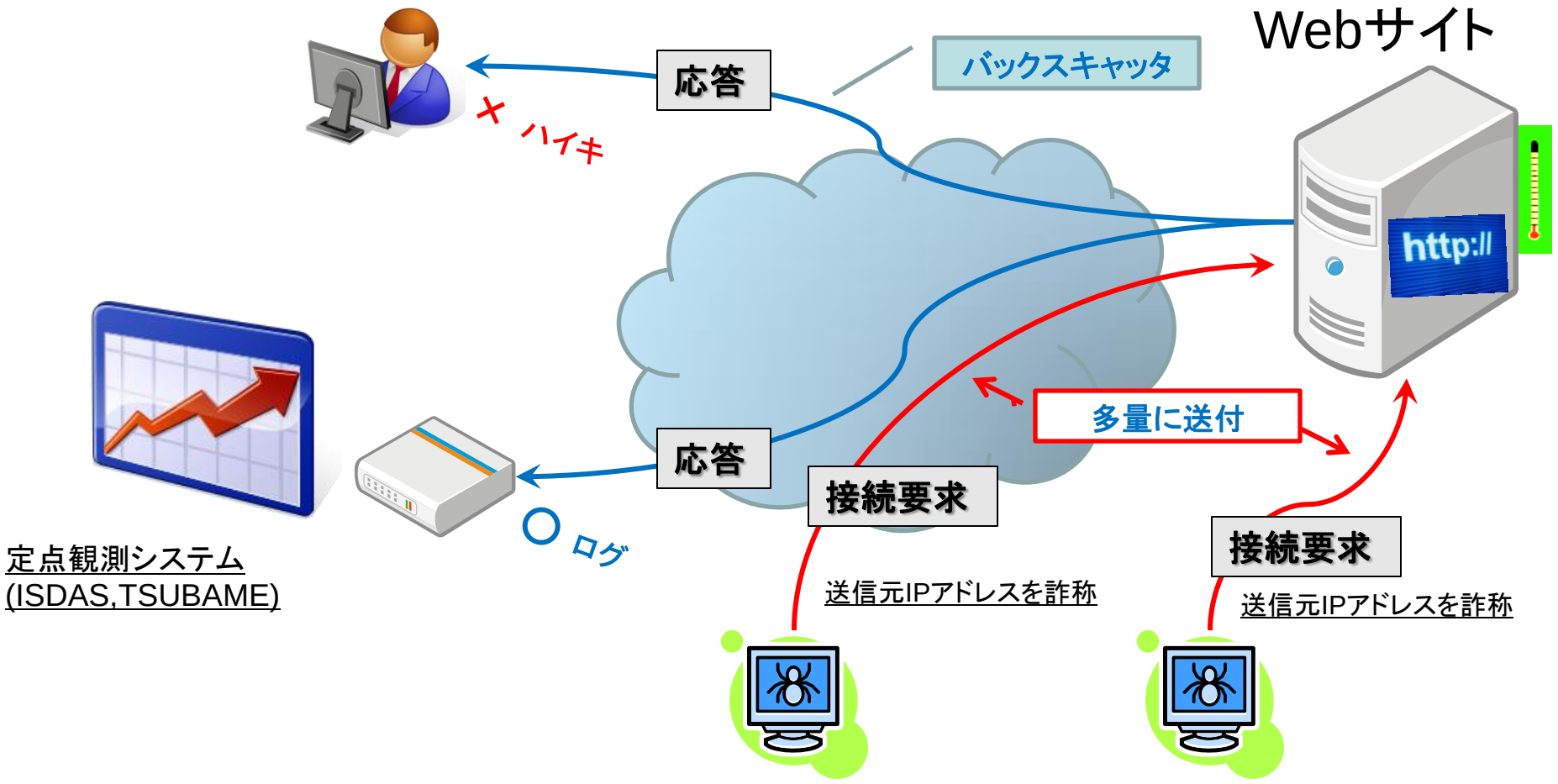
- 2009年7月7日頃～数日間にわたって発生
- 韓国の政府系組織を主な対象とした大規模、長期間のDDoS攻撃が発生
- 主な原因は公開ソフトがマルウエアに置き換えられたことによってBotが構築されたこと **など**
  - 非常に巧妙で複雑だった

未だに全容は明らかになっていない

全体概要
（http://www.issuemakerslab.com/より引用）

http://www.issuemakerslab.com/77ddos_botnet_issuemakerslab.jpg

JPCERT/CCの定点観測システムISDASにて DDoS（Syn-Flood）攻撃のバックスキャッタを観測



JPCERT/CC の関与

- 韓国 KrCERT/CC などがインシデント対応

- JPCERT/CC の協力
  - 韓国KrCERT/CCへ情報提供
  - 7月上旬KrCERT/CCより日本国内367のボット等のIPアドレスを受理
    - 国内への通知連絡を実施

- JPCERT/CC と KrCERT/CC の関係
  - 2国間のインシデント対応で協力
  - APCERT(アジア太平洋地域のCERTの集まり)などの枠組みで連携

DDoS: その後のストーリー

- 韓国KrCERT/CCをはじめとして政府系組織を中心に未だに情報収集・分析を続けている
- マルウエア配布経路は1つではなかった
- 今月に入っても新たな事実が発覚している
  - DDoS攻撃のパターンなど
  - それだけ巧妙・複雑だった
- 今回のようなケースを踏まえた様々な対策を検討中
  - 韓国側は目下情報収集を継続

技術面における対策 （検討中、一部）

JPCERT CC®

- DDoS 対策装置の購入
  - メディアに公開された情報では200億韓国ウォンが投入されるらしい（約15億円相当）
  - 主に政府系組織のサイトなど重要拠点へのDDoS対策が目的
  - 中小企業向けのDDoS対策サービスを検討
- 韓国のウェブサイトのマルウェア配布状況を監視
  - 将来的にはすべてのウェブサイトを対象としたい
  - まずは2010年に100万サイトの監視
- 既存のセキュリティ対策事業の全般的な強化
  - 監視、観測など

体制面での対策（検討中）

- 韓国KrCERT/CCの能力強化
  - 現状50人程度から倍増させる計画
  - マルウエア分析体制
    - など技術的な対応体制の強化

- DDoS攻撃に参加させられているIPアドレスユーザへの通知連絡体制の整備
  - 駆除ツールの作成と配布も検討

今回のインシデント対応の問題点

- 普段対応していたDDoS攻撃の10倍以上の規模を想定する
  - そのような場合への対処方法が考慮されているか？

- リアルタイムのコミュニケーション方法
  - ISPとウェブサイト管理者
  - KrCERT/CCとISP
  - など関係者間

まとめ

- 複雑かつ巧妙なインシデントであり全容把握が困難
  - 多くの関係者の協力が必要
  - 長期的な情報収集が必要となっている
- どの程度のDDoSを考慮して対策するか？
  - 1Gbps？10Gbps？100Gbps？それ以上??
- 緊急時の連絡・協力体制の整備

お問い合わせ先

- 一般社団法人
  JPCERTコーディネーションセンター
  - Email：office@jpcert.or.jp
  - Tel：03-3518-4600
  - http://www.jpcert.or.jp
- インシデント報告の届出
  - 報告様式
    http://www.jpcert.or.jp/form/
  - Email：info@jpcert.or.jp
    PGP Fingerprint ： FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048