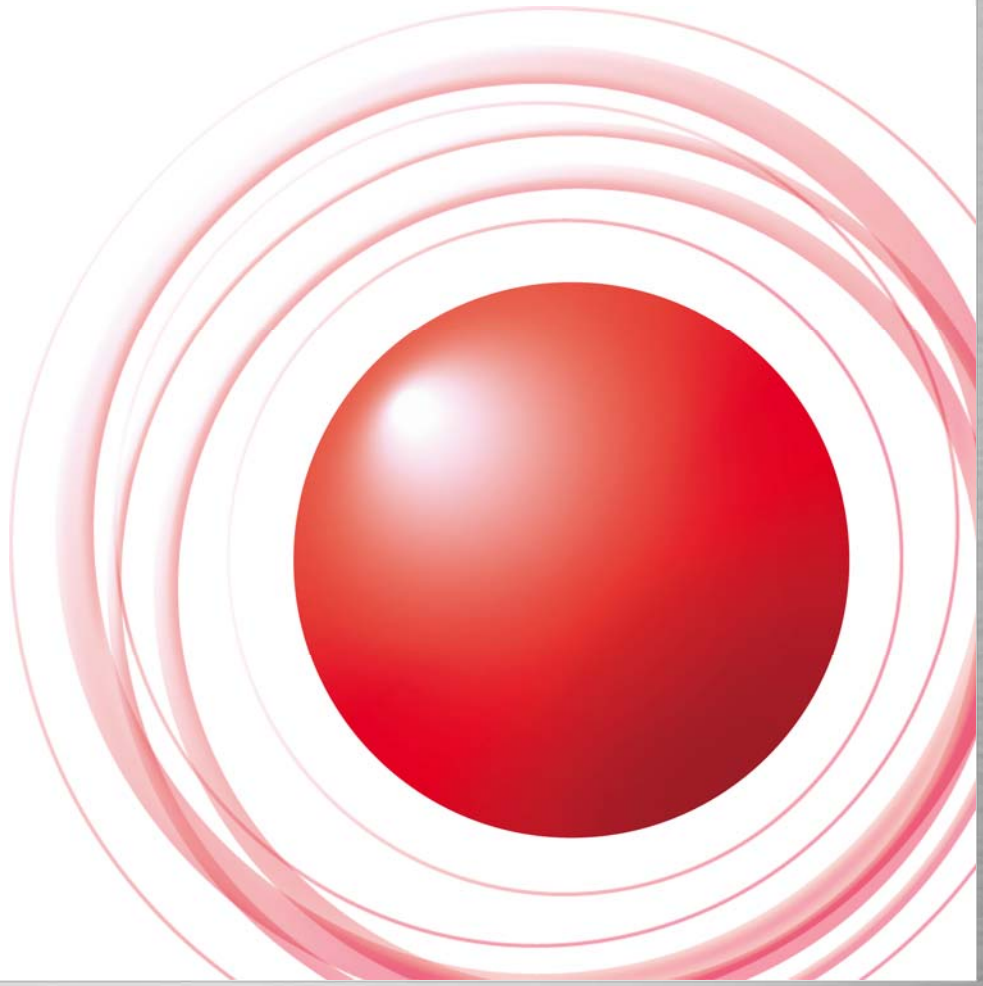
IIJ Technical WEEK 2010
セキュリティ動向 2010(1)

IIJ Internet Initiative Japan



2010/11/19

株式会社インターネットイニシアティブ
サービス本部 セキュリティ情報統括室
齋藤 衛

Ongoing Innovation

自己紹介

齋藤　衛（さいとう　まもる）

株式会社インターネットイニシアティブ サービス本部 セキュリティ情報統括室 室長
1967年生まれ。1993年中央大学大学院 理工学研究科 管理工学専攻修了。

1995年株式会社インターネットイニシアティブに入社。法人向けファイアウォールサービスに従事の後、法人向けセキュリティサービスの 開発(マネージドセキュリティサービス、IDSサービス、DDoS対策サービスなど)、セキュリティサービス担当プロダクトマネージャを経て、現職。

2001年よりIIJグループの緊急対応チーム IIJ-SECTの活動を行う(IIJ-SECTは2002年にFIRSTに加盟)。Telecom-ISAC Japan 、日本シーサート協議会、日本セキュリティオペレーション事業者協議会、Web感染型マルウェア対策コミュニティなどの複数の団体の運営委員。総務省「次世代の情報セキュリティ政策に関する研究会」構成員、安心・安全インターネット協議会P2P研究会、永遠のビギナー対策研究会、安心ネットづくり促進協議会 児童ポルノ対策作業部会 技術者SWG、IPAサービス妨害攻撃対策検討会、インターネットの安定的な運用に関する協議会など複数の団体で活動を行う。共訳書として「ファイアウォール構築 第二版」(オライリー・ジャパン) 。IIJ-SECTの活動は平成21年度「経済産業省商務情報政策局長表彰（情報セキュリティ促進部門）」を受賞。

2010年を振り返って

9月に発生した中国からの DDoS攻撃について

2010年を振り返って

2010年のインシデント(IIRで言及したもの)

2009年
- オバマ大統領来日
- 習近平中国国家副主席来日
- iPhoneウイルス
- Twitter DNS不正操作
- SEOポイズニングでスケアウェア感染
- Gumblar.X改ざん流行

2010年
- .ru.8080改ざん流行
- バンクーバーオリンピック
- 百度DNS不正操作
- ハイチ地震、チリ地震関連SEOポイズニング
- 標的型攻撃Operation Aurora
- 著作権団体を装い金銭を要求するマルウェア
- ボットネットpushdoによる目的不明SSL通信
- ボットネットmiraposaのテイクダウン
- ボットネットWaledacのテイクダウン
- 韓国から2ちゃんねるに対するDDoS攻撃
- BlackBerryやiPhoneに対する攻撃手法の公開
- マルウェアStuxnetの拡散
- サッカーワールドカップ
- ベトナムのユーザに対する標的型攻撃
- インドの政府機関、企業に対するスパイネット
- WordPress脆弱性を悪用したブログサイトの一斉改ざん
- 日本国内で一般企業に対する標的型攻撃
- VoIIP(SIP)不正利用による金銭被害
- Twitterにクロスサイトスクリプティング脆弱性
- 中国からの一斉DDoS攻撃
- MOAUB（毎日脆弱性を公開する試み）

2010年を振り返って

2010年注目トピック

- クラウドコンピューティング利用の一般化
- スマートフォンなど携帯電話のビジネス利用
- 標的型攻撃
- Webで感染するマルウェア
- 児童ポルノ対策
- 暗号アルゴリズムの2010年問題
- 国際間DDoS攻撃

2010年を振り返って

クラウドコンピューティング利用の一般化

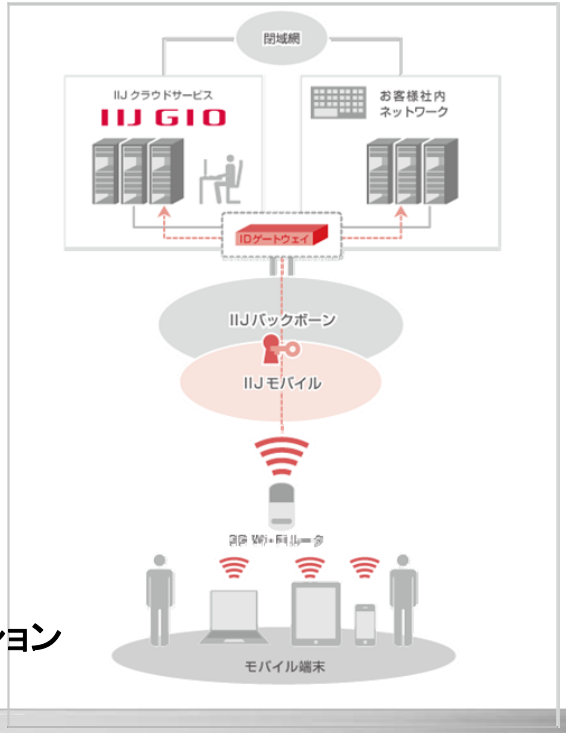
- インシデント/問題点
  - クラウドコンピューティングの利用が一般化してきたため、実際にインシデントがクラウド環境で発生している。
  - そのほとんどがパスワード管理の問題
    （事業者側の情報提供不足の問題、もしくは利用者側意識の問題）
  - インシデント発生時のフォレンジック調査への準備
- Cloud Security Alliance
  “Top Threats to Cloud Computing V1.0”(初版 2010/03/01)
  - ユーザのリスクマネジメント判断の根拠作成を補助するためのもの。
  - “Security Guidance for Critical Area in Cloud Computing”とともに使用する。
  - 今後も随時更新される。
  - 脅威、(実際に発生した事件については)事例、対処法
  - 初版では7つの脅威
    - クラウドコンピューティングの不正乱用
    - 安全でないインタフェースやAPI
    - 内部犯行
    - 共有化の技術の問題
    - 情報の消失や漏えい
    - 使用権やサービスの乗っ取り
    - リスク特性の隠ぺい

http://www.cloudsecurityalliance.org/topthreats.html

2010年を振り返って

スマートフォンなど携帯電話のビジネス利用

- インシデント/問題点
  - iPhone ,Android ウイルス
  - 実装が不安定（頻繁なファームウェアのアップデート、新機能追加）
  - 携帯電話としての機能向上による情報セキュリティポリシーとの不整合（無線LAN機能、VPN機能、リモートデスクトップ機能など）
  - 簡便なユーザインタフェースと未成熟な利用方法（写真、位置情報の公開など、SNSとの連携）
  - 公的利用と私的利用の境界が不明瞭に（利用者の意識に強く依存）

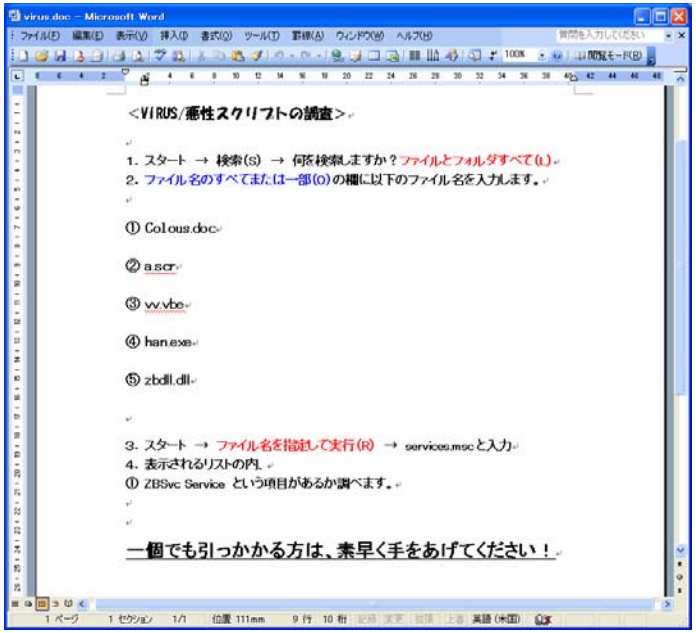


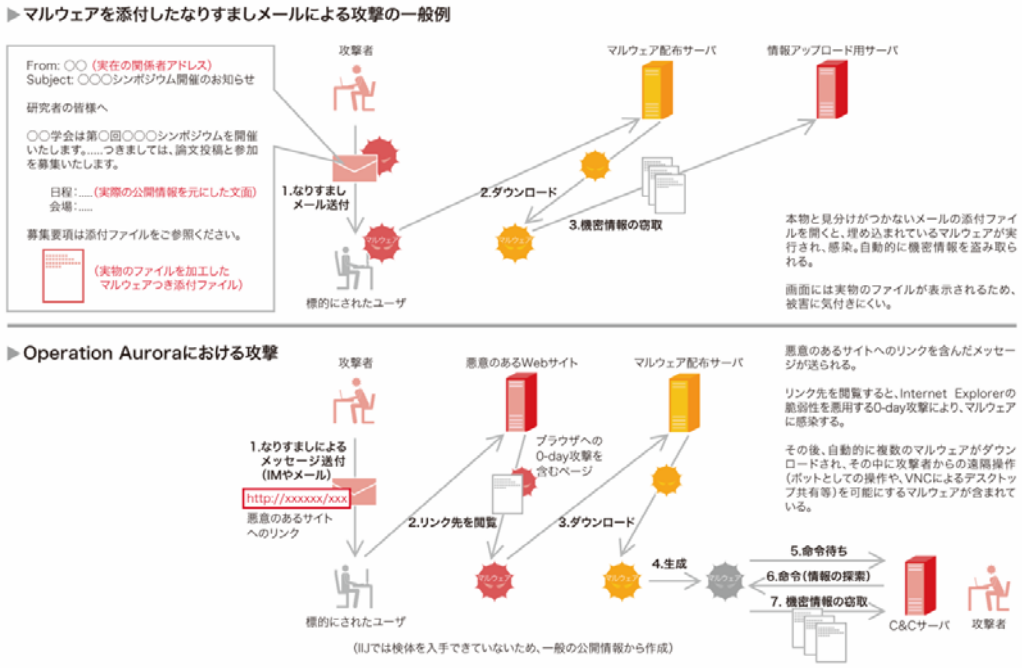
IIJ GIOスマートモバイルソリューション

2010年を振り返って

標的型攻撃

- インシデント/問題点
  - Operation Aurora
    - 2009/12-2010/01 USの複数の企業が対象(報道では60社)
    - IMやメールなどでURLを送付し、Webでのアクセスを誘う
    - IEの0-day攻撃によりマルウェア感染、企業秘密等が漏えい
  - 国内における標的型攻撃

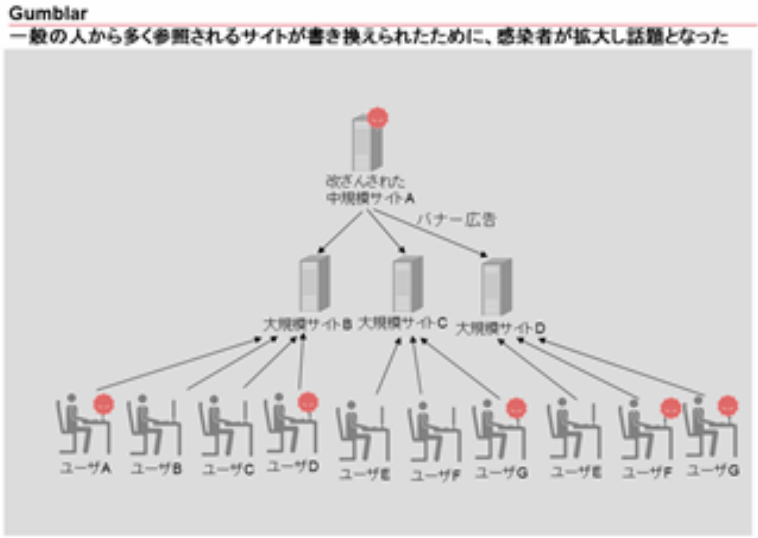




2010年を振り返って

Webで感染するマルウェア

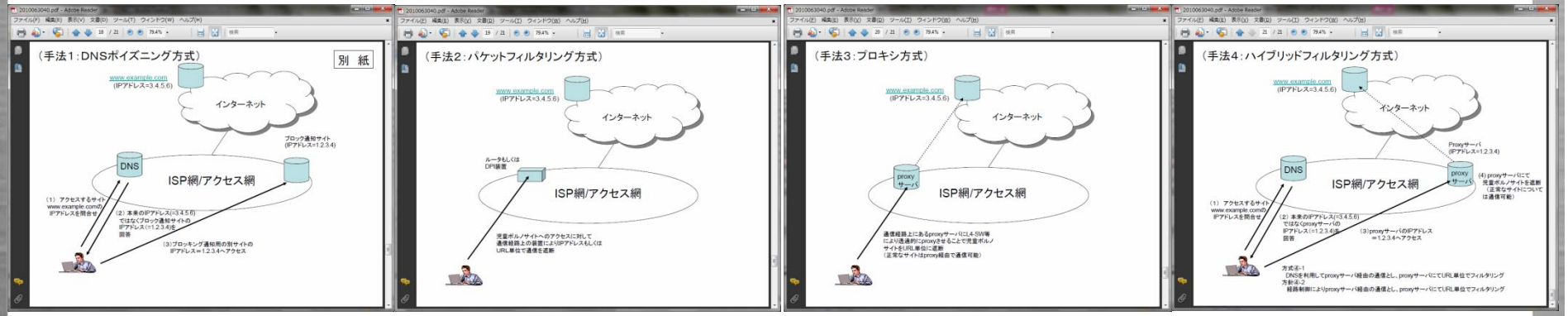
- インシデント/問題点
  - Gumblar(バナー広告)、Microad(Web広告)、mstmp(アクセス解析サービス)
  - SNSワーム(Facebook, Twitterなど)
  - 「正当な」Webコンテンツの一部から、マルウェア感染に誘導される。
    - ブラックリスト、RDBなどでは防げない
  - ブラウザの脆弱性
  - ブラウザのプラグインの脆弱性(pdf, flash, quicktime, Java)



2010年を振り返って

児童ポルノ対策

- インシデント/問題点
  - 児童ポルノ対策自体に反論することはできない。特に海外においては人の命にかかわる意味が強い。
  - 対策手法については、日本のインターネット利用者にとって他人事ではなく、慎重に検討すべきことである。
  - DNSポイズニング方式にはオーバーブロッキングの問題がある。
  - URLフィルタ方式はURLをISPが検証するということであり、電気通信事業法上の通信の秘密と衝突している。



導入が検討された4方式：安心ネットづくり促進協議会 ISP技術者SWG報告書より
http://good-net.jp/modules/news/uploadFile/2010063041.pdf

暗号アルゴリズムの2010年問題

- インシデント/問題点
  - 新しい暗号アルゴリズムの採用
    - ソフトウェア、ファームウェアでの対応
    - ハードウェアでの対応
  - 古い暗号アルゴリズムの利用停止
    - 古い携帯端末等、新しい暗号アルゴリズムを利用できない実装への対処
    - 多くのSSLサーバで56bitDESを受け入れるとしている(2010年IIJ調べ)

2010年を振り返って

9月に発生した中国からの DDoS攻撃について

DDoS攻撃の事例

報道等に見るDDoS攻撃

2000年前後：DDoS攻撃は海外、特にU.S.で発生するもの。
　例：2000年2月Yahoo.com,Amazon.com,eBay.comへの一斉攻撃

2003年 5月　国内の製薬会社等への抗議メール一斉送信
　（英国の研究施設における動物実験に対する動物愛護団体による抗議活動）
2004年1月　韓国から2ちゃんねる掲示板に対する攻撃（韓国竹島切手発売に端を発する）
2004年4月～ Antinnyウイルスによるコンピュータ著作権協会(ACCS)への一斉通信
2004年8月　日本サッカー協会、スポンサー企業、官公庁、報道機関などに対する攻撃
　（サッカー試合：AsiaCup2004）
2004年12月 韓国ヨン様サイトに対する日本からの攻撃
2005年1月　靖国神社等に対する攻撃
2005年2月から9月 中国から日本の官公庁に対する同時多発攻撃（尖閣諸島灯台接収）
2005年4月　スクエアエニックス、ファイナルファンタジーXI
　ガンホーオンラインエンターテイメント、ラグナロクオンライン（RMT排除）
2005年8月　日本から韓国 VANK(**Voluntary Agency Network of Korea**) サイトを攻撃

DDoS攻撃の事例

報道等に見るDDoS攻撃(2)

2006年2月　韓国から島根県Webサーバに対する攻撃（竹島の日）
2006年3月　DNSの再帰的問い合わせを悪用した攻撃の発生
2006年4月　英国の企業に攻撃を行い恐喝(10月に犯人としてロシア人逮捕)
2006年6月　韓国から2ちゃんねるに対する攻撃
　　韓国から島根県Webサーバに対する攻撃
2007年2月　DNSルートサーバへの攻撃
　　ニコニコ動画約3000台からのsyn flood攻撃を受けサービス停止
2007年4月　ミクシィIT系求人サイト「Find Job！」に攻撃
2007年5月　エストニアに対する攻撃
　　日本国内企業に対する攻撃恐喝事件
2008年1月　米国のハッカー集団によるサイエントロジー教会に対する攻撃
2008年4月　韓国から2ちゃんねるに対する攻撃
2008年5月　日本国内企業に対するDDoS攻撃恐喝事件
2008年8月　グルジア紛争にともなう攻撃
　　北京オリンピック関連サイトへの攻撃
2008年9月　オンラインゲームリネージュII公式サイトに対する攻撃
2008年12月 韓国から2ちゃんねるに対する攻撃

DDoS攻撃の事例

報道等に見るDDoS攻撃(3)

2009年2月　DNS replyパケットを悪用した DNSリゾルバへの攻撃
　　韓国から島根県Webサーバに対する攻撃
2009年5月　中国国内でDNSリゾルバに対する攻撃(519暴風影音事件)
2009年6月　イラン大統領選挙に関連した攻撃
2009年7月　マルウェアを利用した米国および韓国に対する攻撃
2009年8月　twitter,facebook等に対する攻撃(グルジア人活動家のコンテンツ目標)
2009年10月 Amazon EC2利用Webサイトに対する攻撃
2010年3月　韓国から2ちゃんねるに対する攻撃
2010年6月　中国から韓国に対する攻撃(上海万博のアイドルグループ公演キャンセル)
2010年9月　中国から日本政府官公庁関係サイト、企業に対する攻撃(尖閣諸島船舶衝突)
2010年10月　中国からフィリピン、マレーシアに対する攻撃(南沙諸島領土問題)
2010年11月　ミャンマーDDoS攻撃でインターネットがダウン(総選挙関連)

DDoS攻撃の起こる理由

- 個人や集団の喧嘩
  - 掲示板などでの喧嘩の報復
  - いいがかりや逆恨みによるいやがらせ
- 集団同士による争い
  - スポーツ
  - 国家間の関係・国民感情
  - 宗教
- 犯罪
  - DDoS攻撃恐喝事件
- サイバー戦争
  - まだ事例はない（グルジア？）
  - サイバー戦争準備中の国家
- その他（原因不明の攻撃）

今回の事件について

原因と攻撃予告

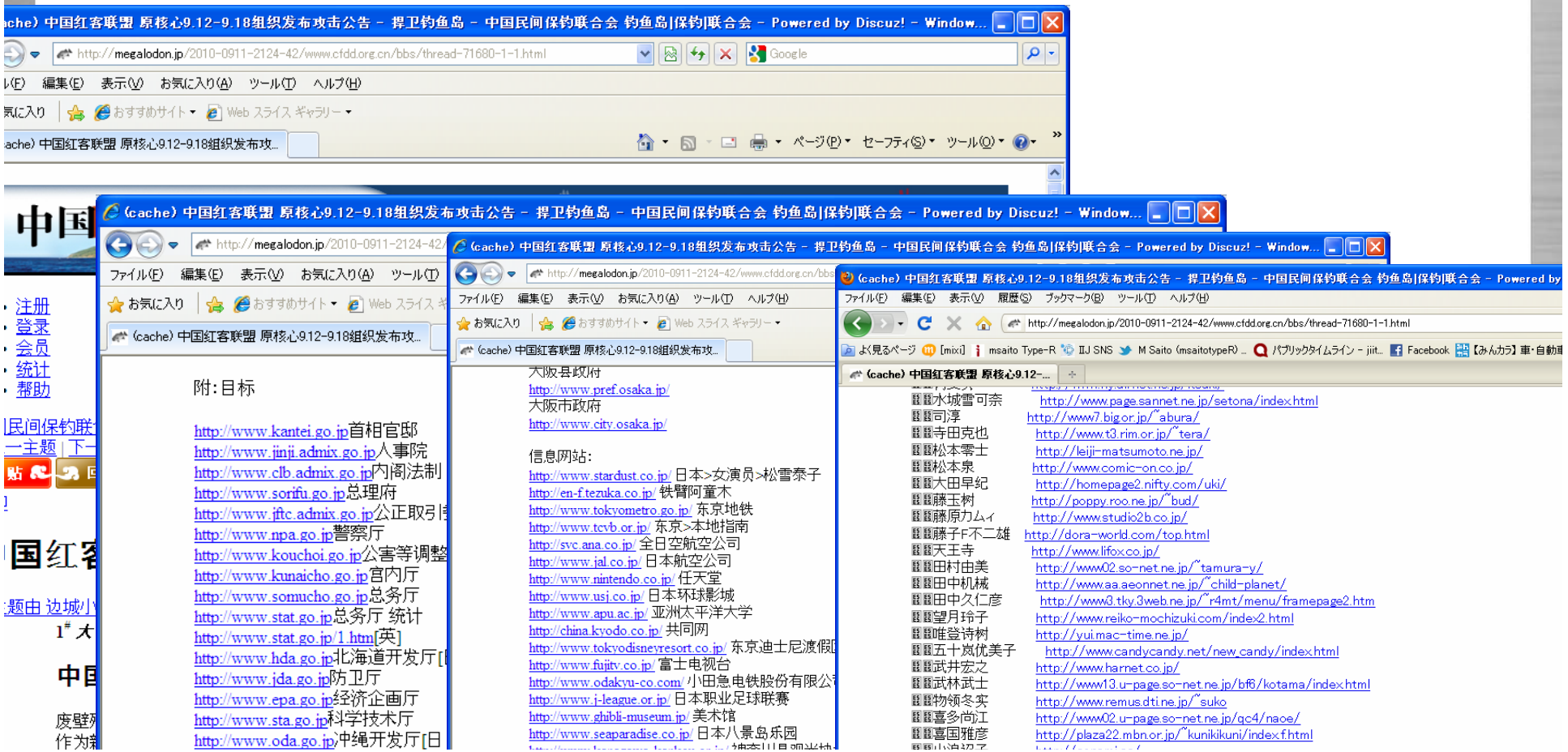
- 原因：尖閣諸島における海上保安庁巡視船と中国船の衝突
  - 最近では2003年6月の上海活動家上陸以来
  - 2005年発生の日本の官公庁に対するDDoS攻撃は、尖閣諸島灯台の接収に端を発する
- 9月18日に攻撃予告（満州事変の日）
  - 10月も継続（10月1日は独立記念日）

海上保安庁のホームページより
http://www.kaiho.mlit.go.jp/info/books/report2005/tokushu/p018.html

今回の事件について

攻撃者側の情報

- 掲示板、IMなどで仲間を募集。目標や攻撃方法を伝授。
- 偏った日本の知識 --- 若者世代



今回の事件について

攻撃者側の情報(2)

DDoS攻撃手法専用ツールの共有と練習

毎日定時にオンライン上に集結し、攻撃手法の伝授といくつかの目標に対する練習を行う。

DDoS攻撃ツール

検索エンジンなどで簡単に見つけることができる。攻撃対象や攻撃手法が固定された専用ツールから、選択可能なツールまで、機能や攻撃目標は多岐にわたる。

注意:

安易に利用しないこと。
言語環境依存性が高い場合が多い。
マルウェアに感染させられることが多い。

DDoS攻撃ツールの例

今回の事件について

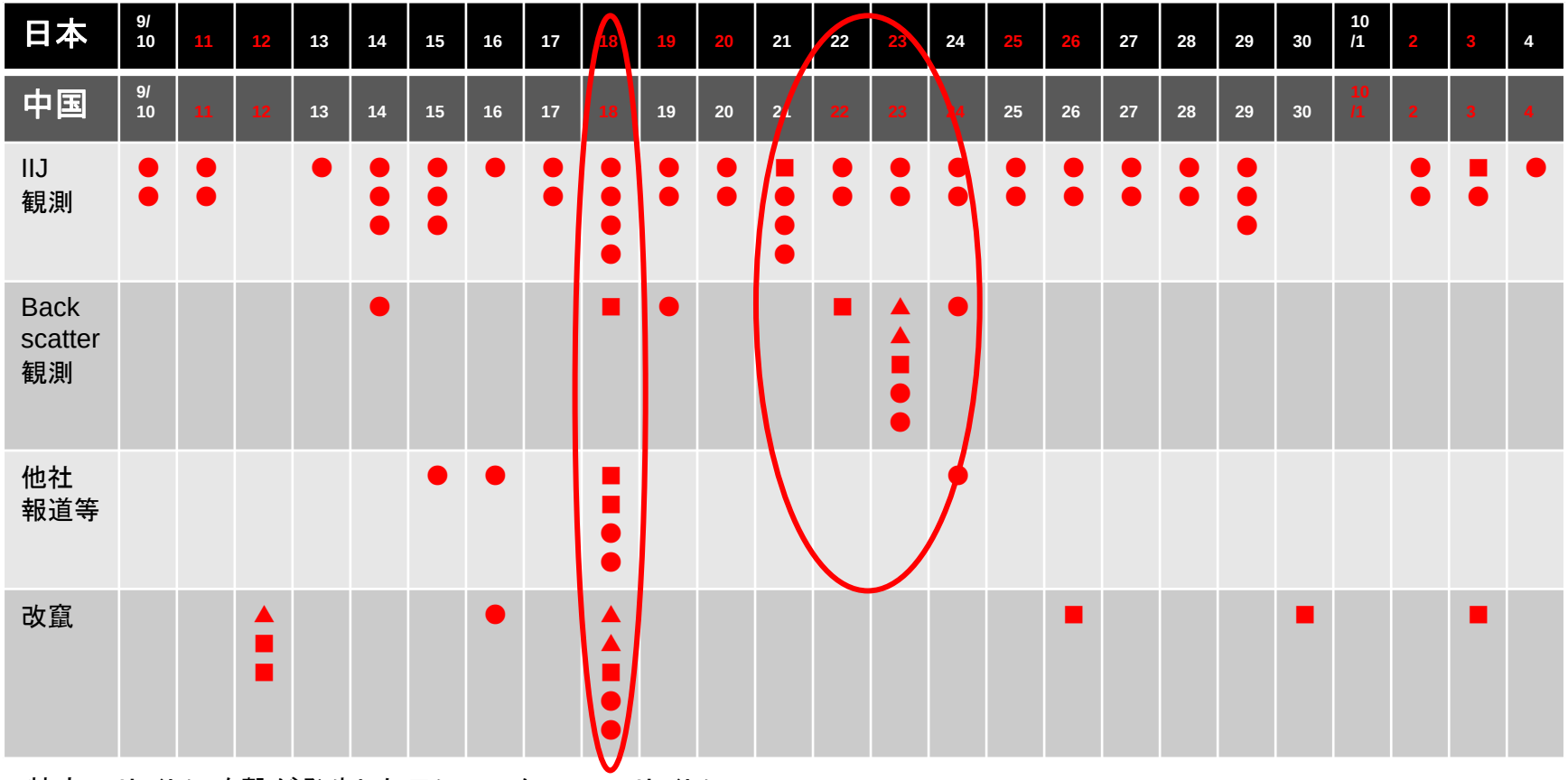
攻撃の様子

- DDoS攻撃の様子
  - SYN flood 16万pps
  - Connection flood 数万cps
  - HTTP GET flood数万cps
  - UDP flood, ICMP flood 1.4Gbps
  - DNS flood 数万pps
- 標的型攻撃メール
- FTPブルートフォース
- SQLインジェクションの脆弱性を持つサイト捜索
- 他国proxyサイト(or Botnet)利用DDoS攻撃
- 最長291時間（12日間）

- 攻撃対象
  - 政府官公庁関係サイト (地方公共団体含む)
  - 大学等教育関係機関
  - 一般企業など 航空会社、電子マネー、音楽関係企業、出版社(マンガ)、漁業団体
- 加えて
  - 上記にリンクのあるサイト
  - 近隣のIPアドレス

今回の事件について

攻撃の全体像(2)発生状況



特定のサイトに攻撃が発生した日にマーク。1つのサイトに1日で複数攻撃が発生していてもマークは一つ。IIJ観測はIIJの顧客に対する攻撃。Backscatter 観測はIPアドレスを詐称された他者に対する攻撃(IIR Vol.8参照)。他社報道等及び改竄は外部情報によるもの。IIJの守備範囲では改竄の試みは多数検出されたが、改竄は発生していない。

▲ 教育関係サイト
■ 一般企業や団体等
● 官公庁関係サイト(地方公共団体含む)

今回の事件について

DDoS攻撃以外の影響

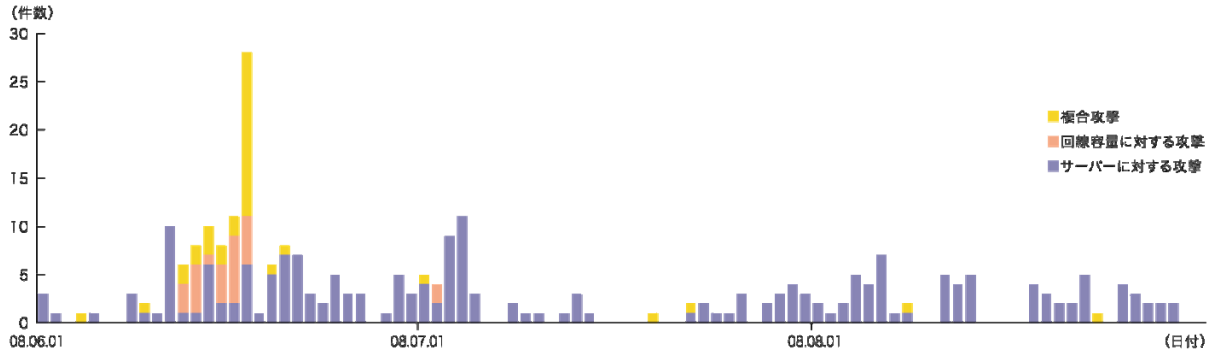
- 改ざん、標的型攻撃メールなど

IBM ISS TokyoSOC Report
https://www-950.ibm.com/blogs/tokyo-soc/entry/adobe_0day_20100922?lang=ja

今回の事件について

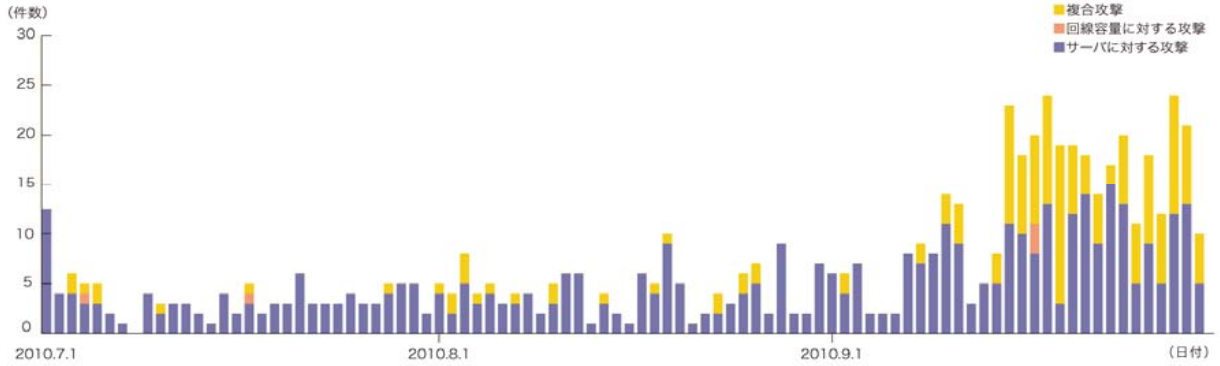
DDoS攻撃と判断された異常の増加

- 3件/日



IIJ Internet Infrastructure Review(定期発行技術レポート) Vol. 1　より
http://www.iij.ad.jp/development/iir/

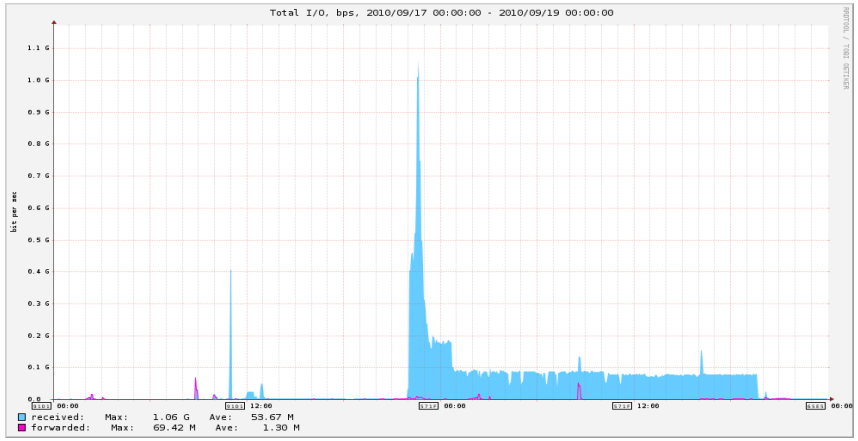
- 6.76件/日



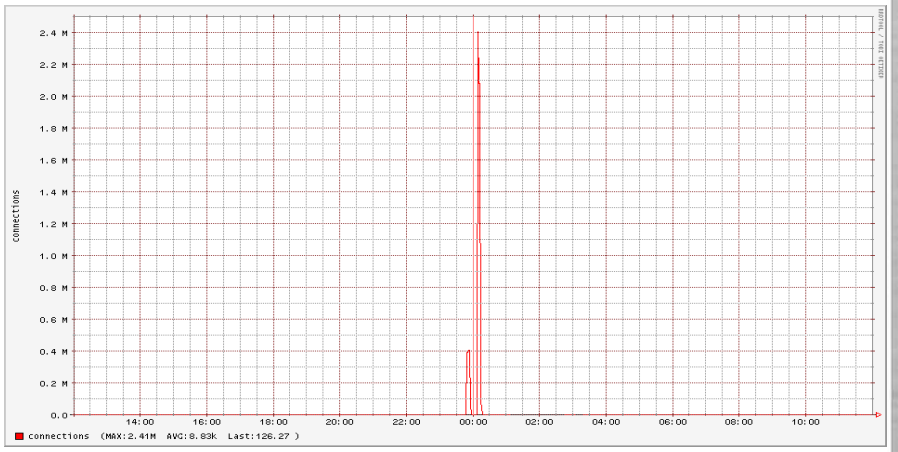
IIJ Internet Infrastructure Review Vol. 9　より

今回の事件について

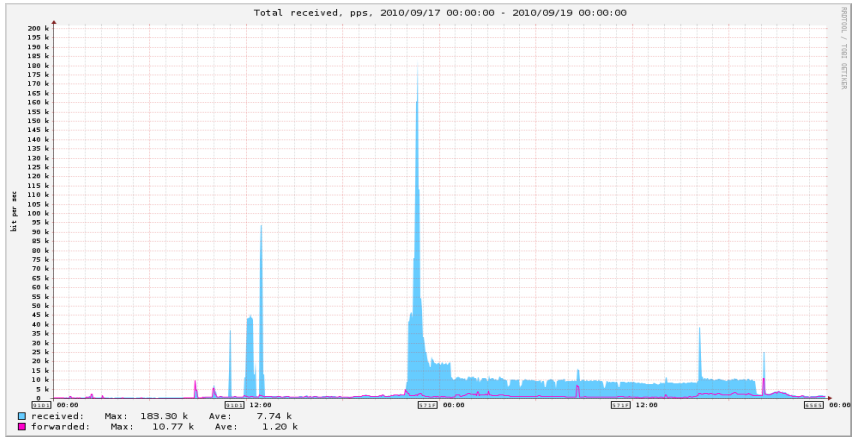
DDoS攻撃のさまざまなview



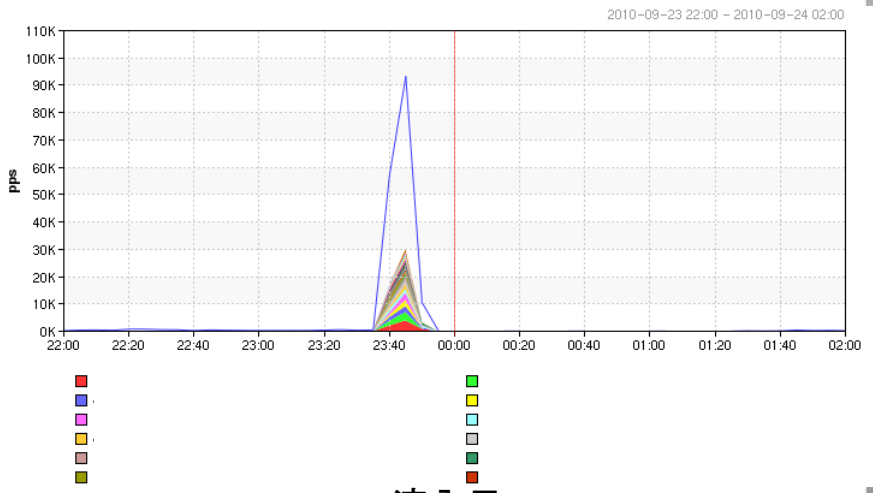
通信量



接続数



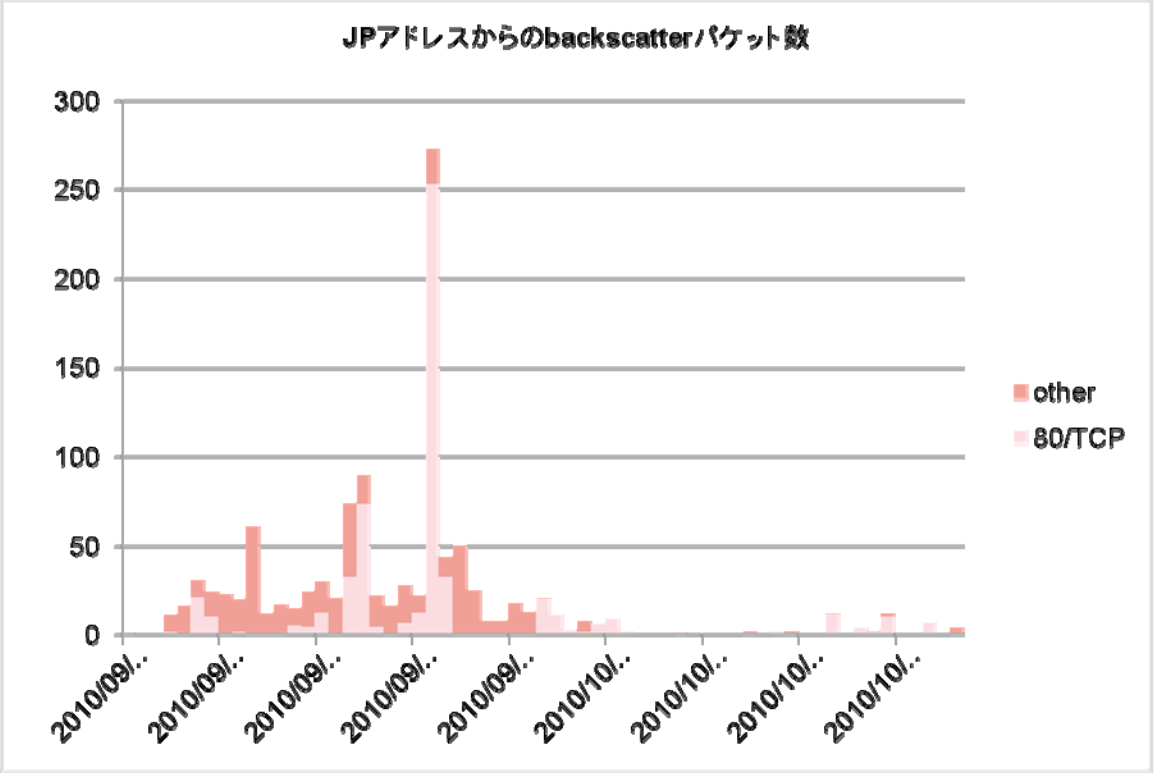
パケット数



流入元

今回の事件について

DDoS攻撃によるbackscatterの観測



- いくつかの攻撃ではIPアドレスの詐称は行われていた

Backscatter:

元となる攻撃パケットが発信元IPアドレスをランダムに詐称（IPスプーフィング）していると、攻撃先からの応答パケットは本来の発信元ではなく、詐称されたIPアドレスに向けて送り返される。このパケットをDDoS攻撃によるbacscatterと呼ぶ。

今回の事件について

今回の攻撃の特徴:リンク先への攻撃

- 事前の「練習」によって top page が”固い”ことがわかったため、攻撃先のコンテンツからリンクが張られている先のサーバに攻撃先を変更。
- 例:
  サイト検索: http://search.example.co.jp/
  ご意見募集cgi: http://www.example.co.jp/goiken.cgi
  関連会合サイト: http://www.kokusai-kaigi2010.org/

- このようなリンクは、tope page Webサーバとは別のサーバの機能であったり、他の団体の運営するWebサーバであったりする。これらのサーバからすると突然攻撃が発生したように見え、因果関係が把握しにくい。
- また、特に国際会合の期間限定Webサイトなどは、小規模なサイトであることが多く、安価なレンタルサーバ等で構築されていたり、コンテンツのアップロードのみに注力し、適切な運用を行っていなかったりした。このため、対応に苦慮することになる。

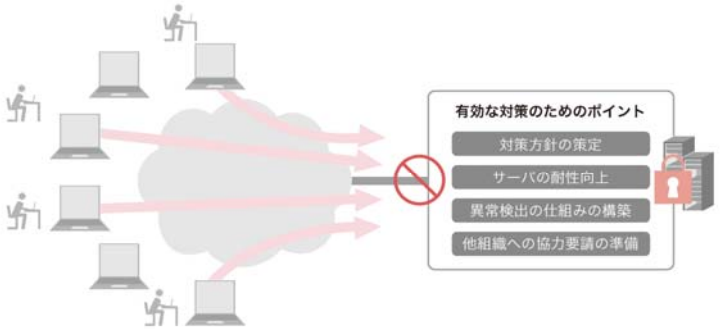
今回の事件について

小規模サイトでのDDoS攻撃への備え(IIR Vol.9より)

- 今回の事件のように、もともとの攻撃対象であったサイトからリンクされていたという外的な要因で攻撃が発生することもありうる。

[DDoS攻撃への4つの備え]

- DDoS攻撃を受けた時の対策方針の策定
  - 継続する必要があるのか、サービスを提供する範囲や内容を制限してよいか
- サーバの耐性向上
  - 適切な資源の確保、処理上限の設定、アプリケーションやOSの対策機能の導入
- 異常検出の仕組みの構築
  - ログの取得、ログサーバの準備、異常検出・解析スクリプトなどの準備
- 他組織への協力要請の準備
  - 通信の取り扱い、提供する情報の範囲、さらに他の組織に対する情報開示



その他の参考情報

- 独立行政法人情報処理推進機構：サービス妨害攻撃対策検討会 報告書
  （近日公開）
- SANS：Help Defeat Distributed Denial of Service Attacks: Step-by-Step
  http://www.sans.org/dosstep/
- VeriSign：DDoS Mitigation – Best Practices for a Rapidly Changing Threat Landscape Whitepaper(要ユーザ登録)
  http://www.verisign.com/forms/ddosbestpracticeswp.html?toc=MYUM9-0000-02-00
- Lenny Zeltser:Network DDoS Incident Response Cheat Sheet
  http://zeltser.com/network-os-security/ddos-incident-cheat-sheet.html

IIJ Internet Initiative Japan

ご清聴ありがとうございました

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466（9：30～17：30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation