DNSセキュリティイシューへの対応
～セキュリティ事業者の視点～

2014年11月20日

JSOC JAPAN SECURITY OPERATION CENTER

株式会社ラック
セキュリティプロフェッショナル本部
JSOC統括部 JSOC アナリシスグループ
阿部 正道

JSOC : Japan Security Operation Center

LACが誇るセキュリティ監視センター「JSOC」。防衛基地のようなこの施設では、ネットワークセキュリティに関するプロフェッショナルであるアナリストとエンジニアが24時間365日の体制で、日々発生するセキュリティの脅威からお客様を守っています。

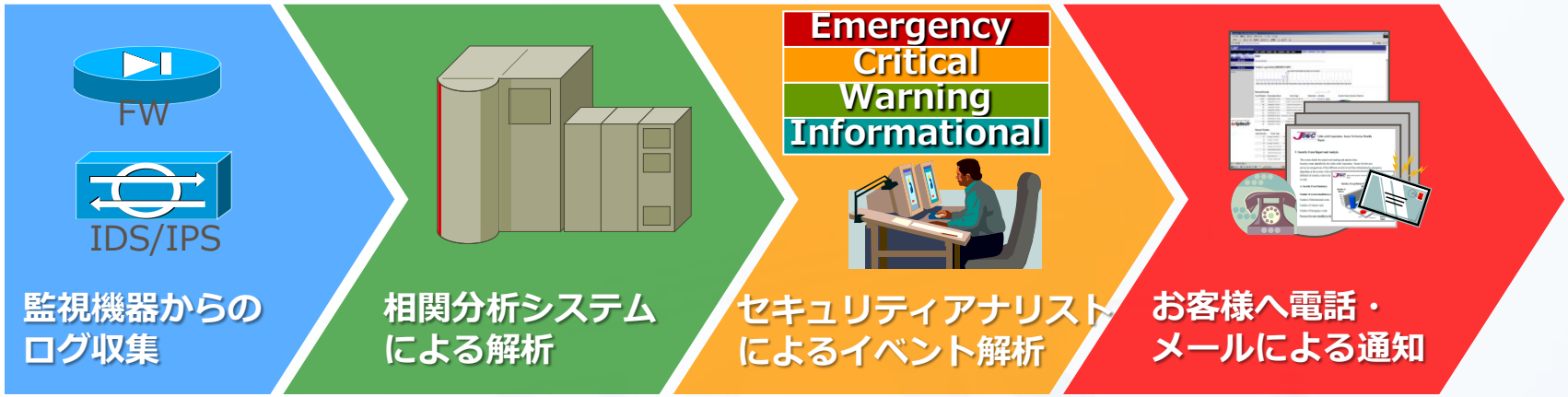




- 足掛け13年にわたる、セキュリティ監視サービスの継続実績
- 24時間365日、年中無休の監視・運用サービス
- 専門のセキュリティアナリストによる高度な情報分析
- アナリスト・エンジニア総勢90名以上での運用体制
- 監視センサー数は約1400、1日の処理ログ量は5億件以上
- 契約顧客は約850社（2014年9月時点、契約中）
- 主要ベンダーのセキュリティ監視デバイスにマルチ対応

ログ収集からお客様へ通知まで

JSOC



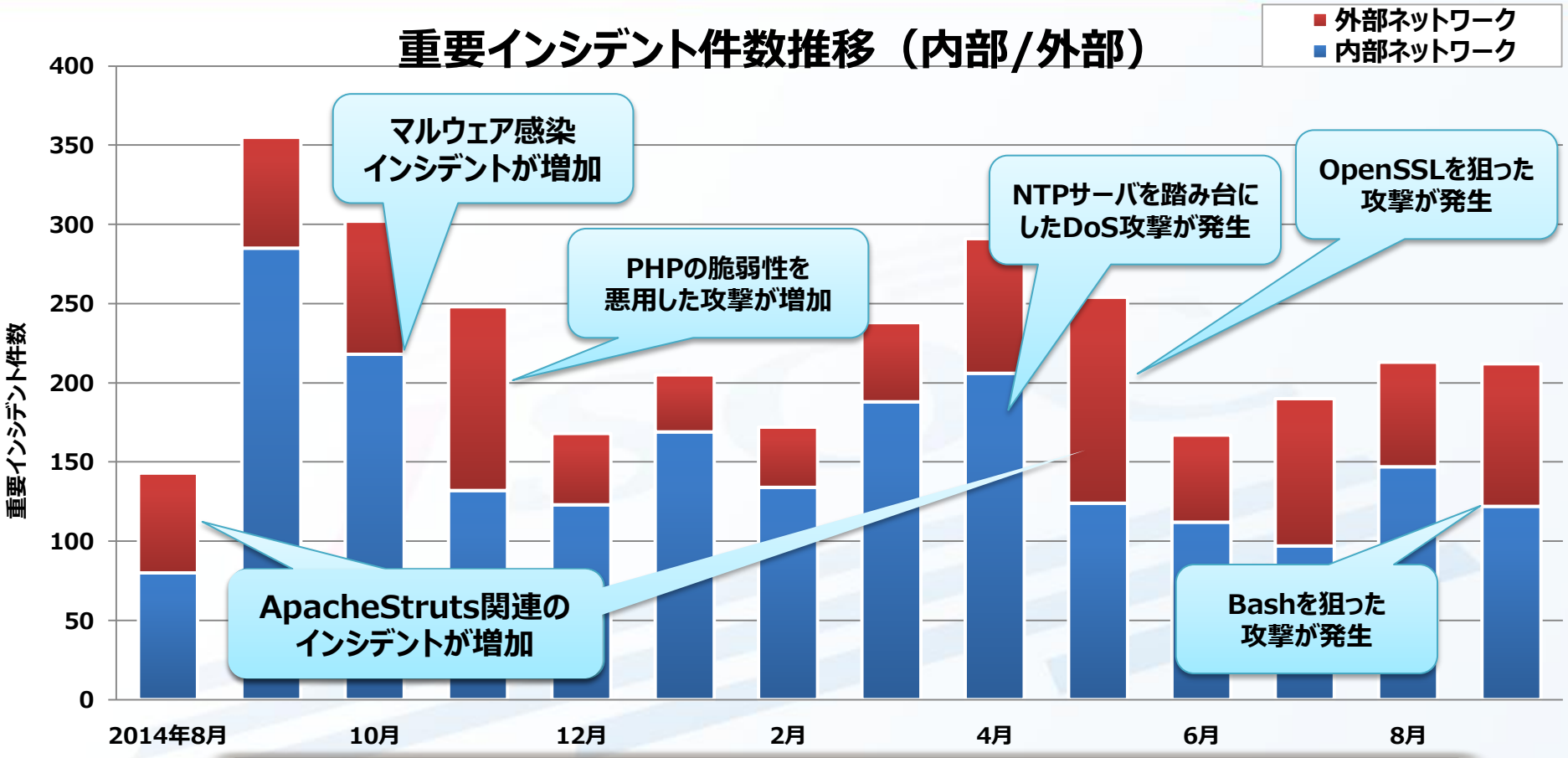
High

重要度

Low

Emergency	攻撃が成功したと判断された場合	即時連絡	15分以内、電話・メール
Critical	攻撃の失敗を確認できない場合。または成功している可能性が高いと判断された場合		
Warning	実害を狙った攻撃だが、失敗を確認している場合	安全宣言	専用WEBポータル
Informational	偵察活動のような、実害のない攻撃活動を検出した場合		
誤検知	通常通信もしくは誤検知と判断された場合		

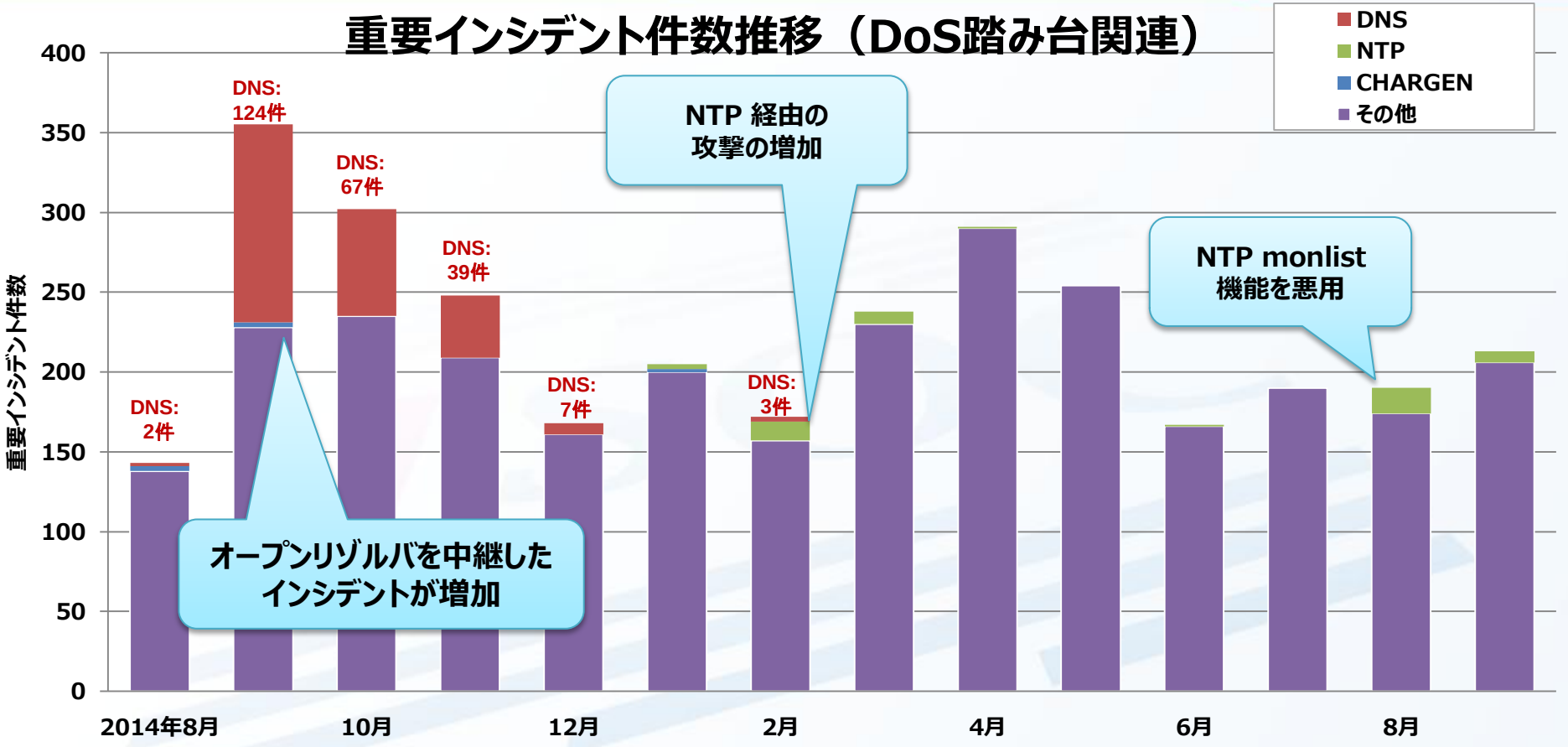
インシデントの内訳（内部/外部）



外部からの攻撃は脆弱性公表から悪用までが短く被害拡大に繋がり易い

マルウェア感染は特に「情報や金銭」の窃取が主たる目的のものが多い

インシデントの内訳（DoS踏み台関連）

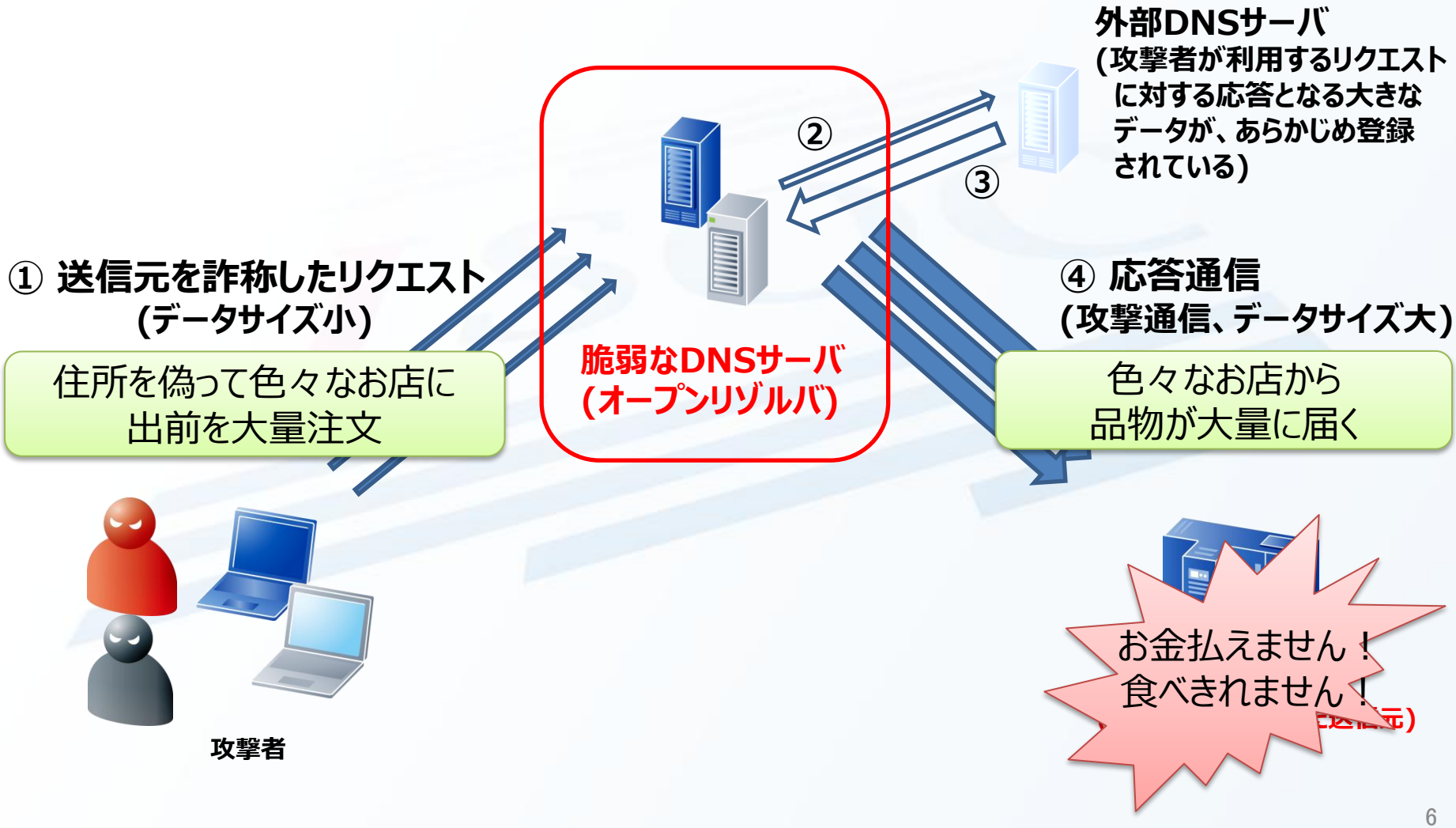


突発的に増加するものが多いが、発生後に対策を進めることで収束

管理者、利用者が知らない間に動いていたケースも

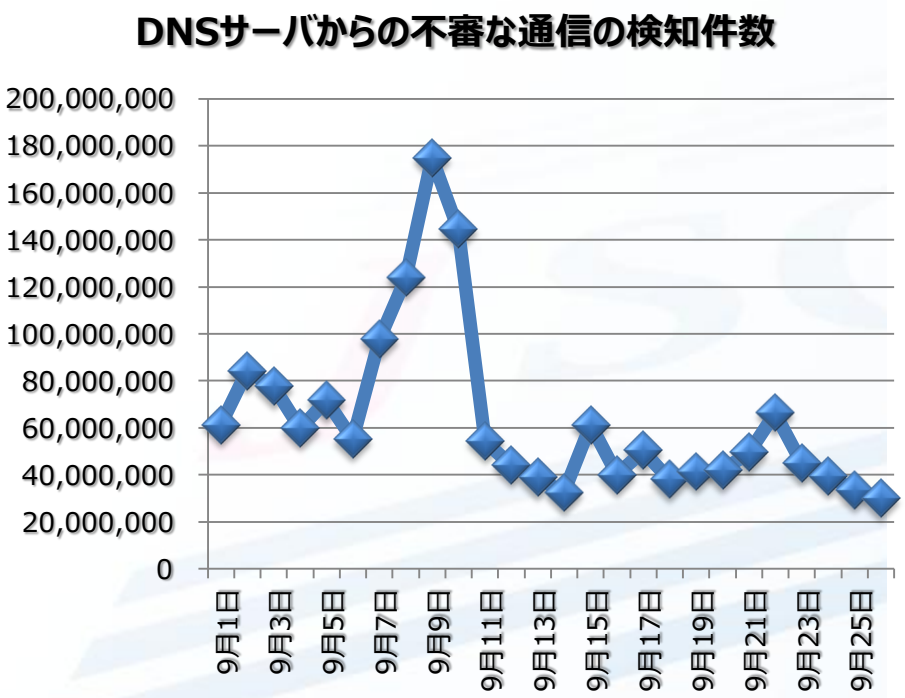
DNSリフレクター（アンプ）攻撃（2013年9月）

- 攻撃者、被害者とは**無関係な DNS サーバが悪用**される

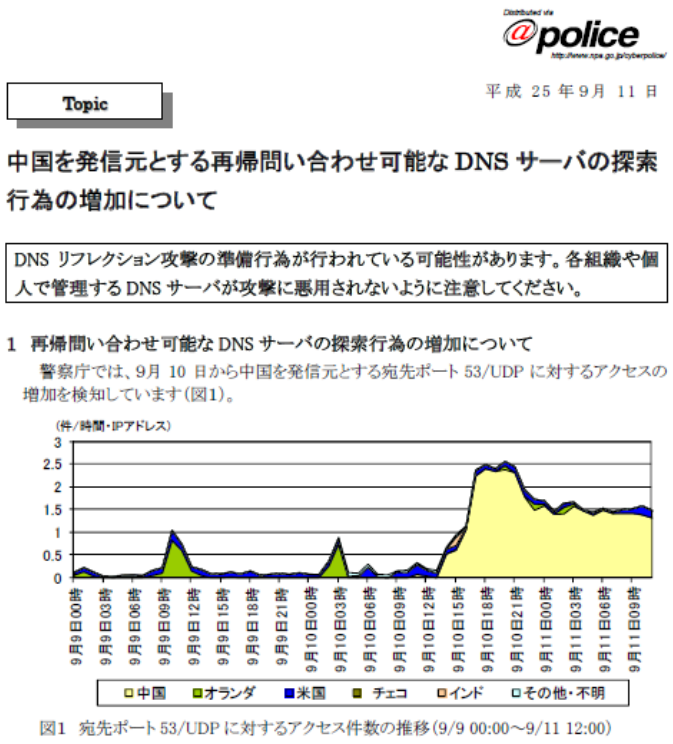


DNSリフレクター（アンプ）攻撃（2013年9月）（2）

その時、JSOCは・・・？



JSOCでは実際の攻撃を検知



Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 25 年 9 月 11 日

Topic

中国を発信元とする再帰問い合わせ可能な DNS サーバの探索行為の増加について

DNS リフレクション攻撃の準備行為が行われている可能性があります。各組織や個人で管理する DNS サーバが攻撃に悪用されないように注意してください。

1 再帰問い合わせ可能な DNS サーバの探索行為の増加について

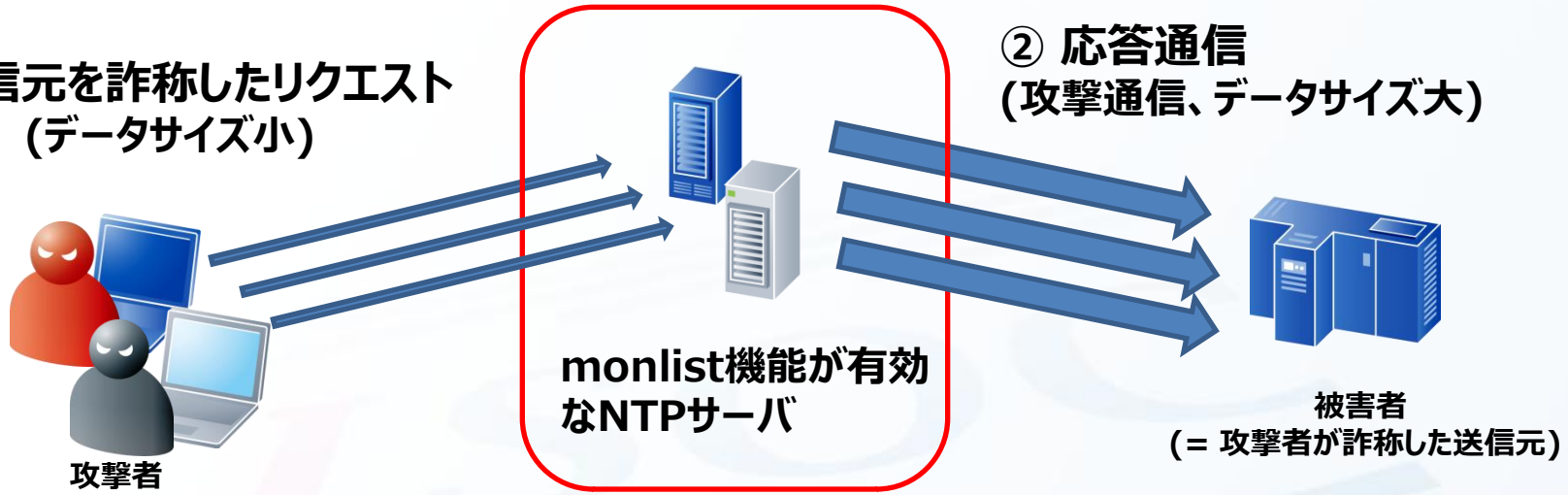
警察庁では、9月 10 日から中国を発信元とする宛先ポート 53/UDP に対するアクセスの増加を検知しています(図1)。

図1 宛先ポート 53/UDP に対するアクセス件数の推移(9/9 00:00～9/11 12:00)

警察庁はスキャンの増加を警告

出典：http://www.npa.go.jp/cyberpolice/detect/pdf/20130911.pdf

NTPサービスを悪用したDoS攻撃の増加(2014年2月)



- 2月10日にCDNサービスのクラウドフレアにて、NTPサーバを踏み台にした、400GbpsのDDoS攻撃を観測。
- スパム対策組織のSpamhausで起こった300GbpsのDDoS攻撃は30,956台のDNSオープンリゾルバを利用したのに対して、今回の400GbpsのDDoS攻撃はわずか4,592台のNTPサーバを利用のみで達成している。

参考：Technical Details Behind a 400Gbps NTP Amplification DDoS Attack
http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

事例：発生要因について

サーバを誰も管理していなかった

一時的に立てたサーバがそのままになっていた。

DNSサービスが起動していたが、誰も管理していなかった。

ファイアウォールの設定が誤っていた

意図せず外部から参照できるような設定になっていた

外部には公開していないはずだったが、公開されてしまっていた。

組み込み系の製品で、知らずに動作していた

DNS に限らず、IPカメラやプリンタなどで標準で公開されており、

単体ではログも記録されないため、発見および対応が遅れた。

被害が止められない理由

管理していない、できていない

頻繁に変更するものではないため、詳細な設定は把握していない場合が多い。

動作させて稼働していればよいという認識が強い。

設定値の見直しがされにくい

上記同様、設定変更することが少ないので、見直しを行う機会もなかった。

製品の標準設定などである場合、その設定に気付かないことも。

エンドユーザ様の反応が鈍い

ホスティング事業者様などで、エンドユーザ様の対応が進まないため

通信を勝手に止めることができない。

参考URL

各所から公開されている注意喚起などをもとに、ぜひ設定の見直しを！

DNS の再帰的な問合せを使った DDoS 攻撃の対策について
http://jprs.jp/tech/notice/2006-03-29-dns-cache-server.html
技術解説：「DNS Reflector Attacks（DNSリフレクター攻撃）」について
http://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html

情報処理推進機構：情報セキュリティ：DNSキャッシュポイズニング対策
http://www.ipa.go.jp/security/vuln/DNS_security.html

DNS の再帰的な問合せを使った DDoS 攻撃に関する注意喚起
http://www.jpcert.or.jp/at/2006/at060004.txt
DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起
http://www.jpcert.or.jp/at/2013/at130022.html

DNSの再帰的な問い合わせを悪用したDDoS攻撃手法の検証について
http://www.cyberpolice.go.jp/server/rd_env/pdf/20060711_DNS-DDoS.pdf

JSOCの最新傾向は？ ⇒ JSOC INSIGHT

- JSOC INSIGHTとは？
  - ・JSOCで観測した脅威傾向をまとめたレポート
  - ・四半期ごとにリリース
  - ・最新版（Vol.5）を11月12日に公開

Vol.5 のトピック

- ・世界中で広く利用されている暗号ライブラリ(OpenSSL)の脆弱性を悪用する攻撃について
- ・ボットネットからの大規模な攻撃とその影響について
- ・日本を標的とした攻撃が続いていることについて

その他のレポートも公開しておりますので、
是非弊社ホームページへお越しください。

⇒http://www.lac.co.jp/

LAC
安心とともに

Thank you. Any Questions ?

※ 本資料は2014年11月現在の情報に基づいて作成しており、記載内容は予告なく変更される場合があります。
※ 本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。
※ その他記載されている会社名、製品名は一般に各社の商標または登録商標です。

LAC 安心とともに
株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1
平河町森タワー
Tel 03-6757-0113 Fax 03-6757-0193
sales@lac.co.jp
www.lac.co.jp