D1-1 サイバー攻撃最前線2017
JSOCが見た、意外とよくあるインシデント
～JC3の知見を添えて～

JSOC JAPAN SECURITY OPERATION CENTER

2017年11月28日

株式会社ラック
サイバーセキュリティ事業部
JSOC
阿部 正道

アジェンダ

- 自己紹介＆JSOC紹介
- 最近のセキュリティトピックについて
- いまだによくあるインシデント
  - 今なお残る、設定不備による脅威
  - 気付いてますか？脆弱ですよ！
- 改ざん被害にあった場合の事例
  ～JC3 における Web改ざんサイト無害化について～
- まとめ

自己紹介

阿部 正道

株式会社ラック　サイバーセキュリティ事業部 JSOC

2002年 ラック入社、JSOC へ配属

入社より一貫して JSOC に勤務する。
セキュリティアナリストとして、100ヶ月間分析業務に従事。
その後サービス企画を経て、セキュリティ監視・運用支援システム
「LAC Falcon」の分析面の開発に関与。

2014年 アナリストグループ リーダーへ

2016年 JSOC アナリシスグループマネージャーへ

現在は JSOC での新サービス検討や管理を実施する。

外部活動としては ISOG-J および JC3 に参加している。

Japan Security Operation Center（JSOC）とは

JSOCは
ラックが誇る
国内最大規模の
セキュリティ監視センター

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お守りします

JSOCの特徴

- 17年以上にわたる監視サービス継続実績
- 200名以上のセキュリティ技術者による運用体制
- 自社開発の監視システム「LAC Falcon®」
- セキュリティアナリストによる高度な分析
- 監視センサー数は2,000台以上
- 1日の処理ログ量は14億件以上
- 契約顧客は900社以上
- 主要セキュリティ監視デバイスにマルチ対応

提供サービス

- マネージド・セキュリティ・サービス
  - IDS/IPS 監視・運用サービス
  - マルウェア対策製品 監視・運用サービス
  - WAF運用管理サービス
  - NEW クラウドWAF監視・運用サービス
- JSOC 24+シリーズ

4

JSOCにおけるセキュリティインシデントの重要度

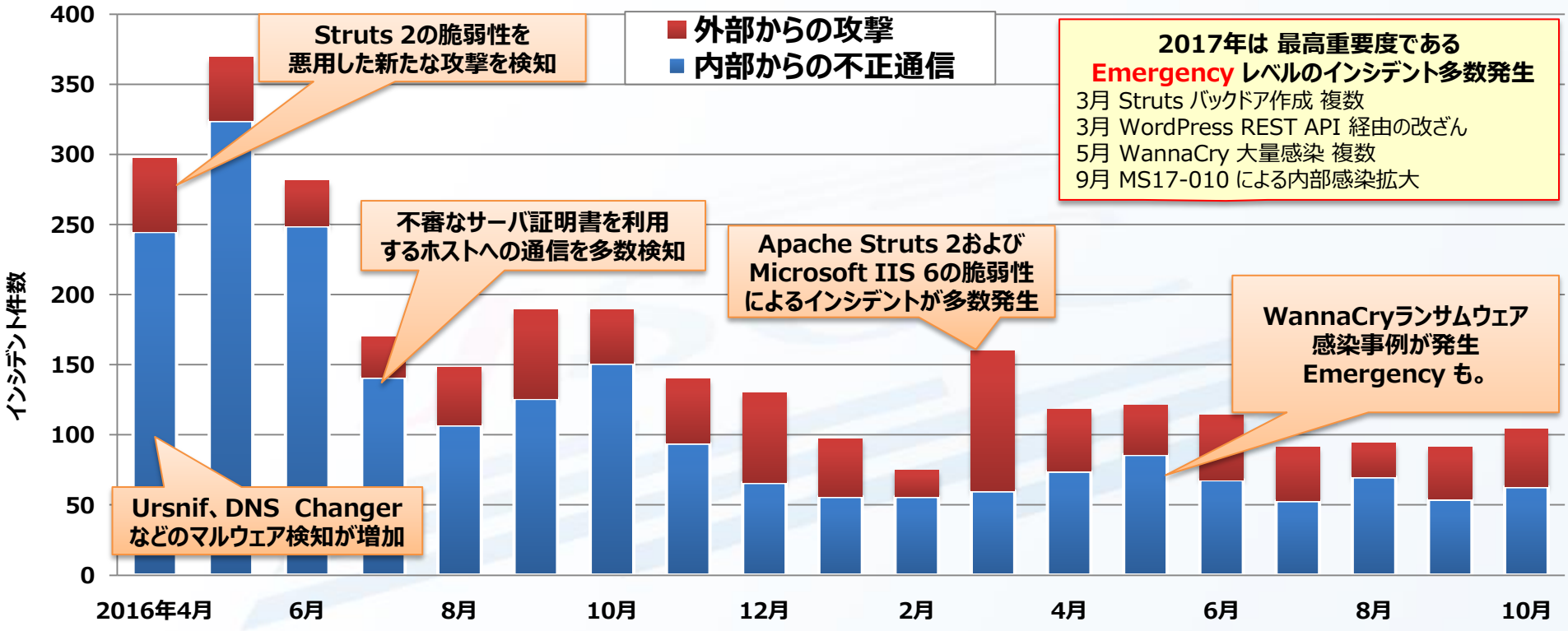
JSOCアナリストによる 高精度なインシデント通知

重要度	JSOCのインシデント判断
Emergency（緊急）	**攻撃が成功し、緊急事態と判断**したインシデント
Critical（重要）	**攻撃が成功した可能性が高いと判断**したインシデント
Warning（警告）	**経過観察が必要と判断**したインシデント
Informational（情報）	**攻撃ではないと判断**したインシデント

電話による
緊急連絡を実施
↓
要対応・確認

ポータルへの
情報掲載
↓
レポート等で状況確認

JSOC全体の状況:重要インシデントの発生状況

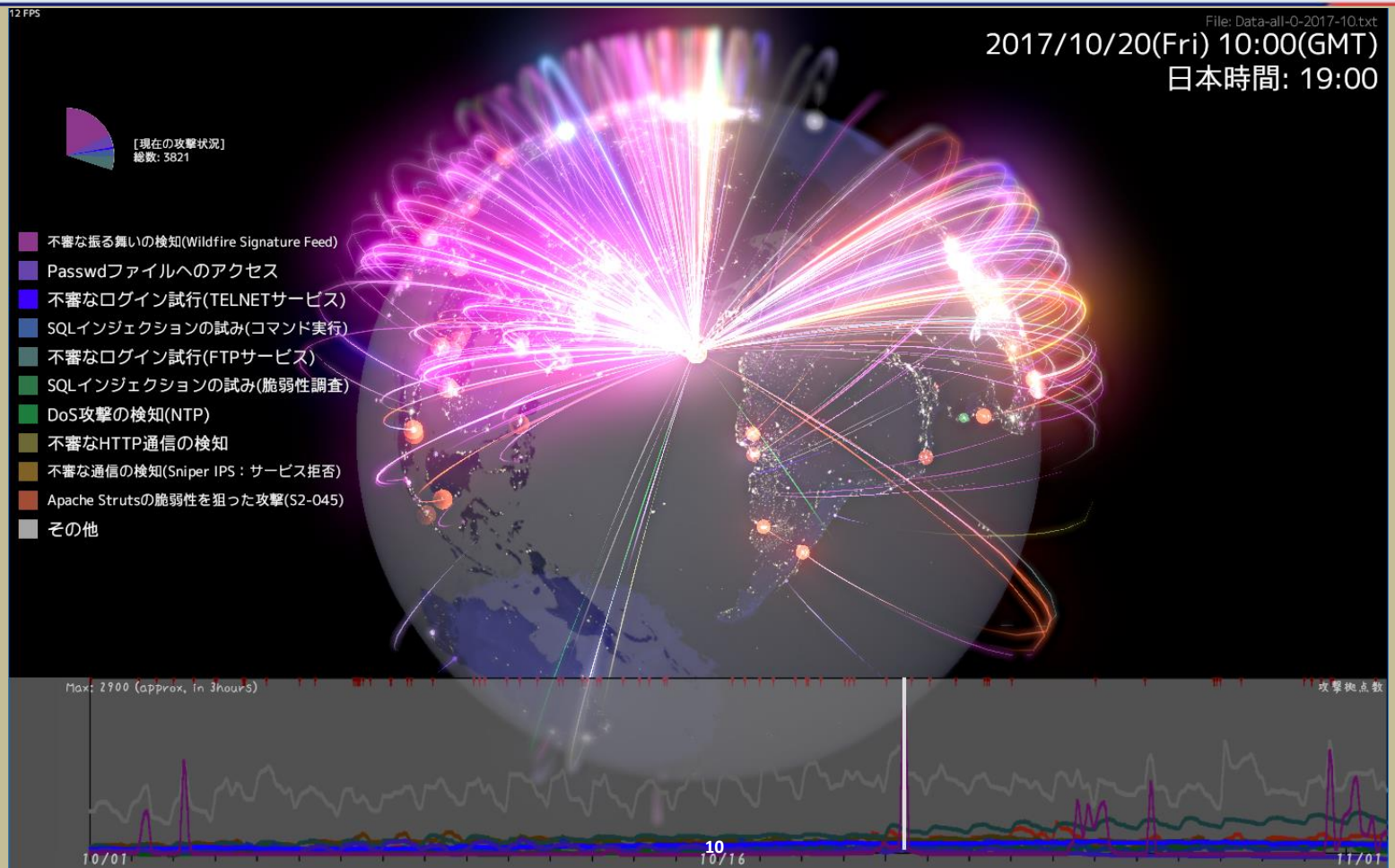


毎月のように多様なインシデント傾向が継続して発生中

2016年度より危険性が高いものが多く、相次いで注意喚起

件名	発出日
【注意喚起】PAN-OSにおけるコマンド実行の脆弱性について	2016/4/6
【注意喚起】ケータイキット for Movable Typeの脆弱性について	2016/4/25
【注意喚起】Apache Struts における脆弱性 (S2-032、CVE-2016-3081)について	2016/4/27
【注意喚起】Apache Struts 2 における脆弱性(S2-037、CVE-2016-4438)について	2016/6/20
【注意喚起】Cisco ASAのSNMP機能におけるバッファオーバーフローの脆弱性について	2016/8/22
【注意喚起】ISC BIND 9 におけるサービス不能の脆弱性(CVE-2016-2776)について	2016/10/03
【注意喚起】WordPress における脆弱性について	2017/2/6
【注意喚起】Apache Struts における脆弱性 (S2-045、CVE-2017-5638) について	2017/3/8
【注意喚起】Microsoft IIS 6.0 の WebDAV 機能におけるバッファオーバフローの脆弱性 (CVE-2017-7269)について	2017/3/30
【注意喚起】特定種別のランサムウェアによる被害拡大について	2017/5/15
【注意喚起】Apache Struts における脆弱性 (S2-052、CVE-2017-9805) について	2017/9/6

なくなることはない、世界中からの攻撃(2017年10月)



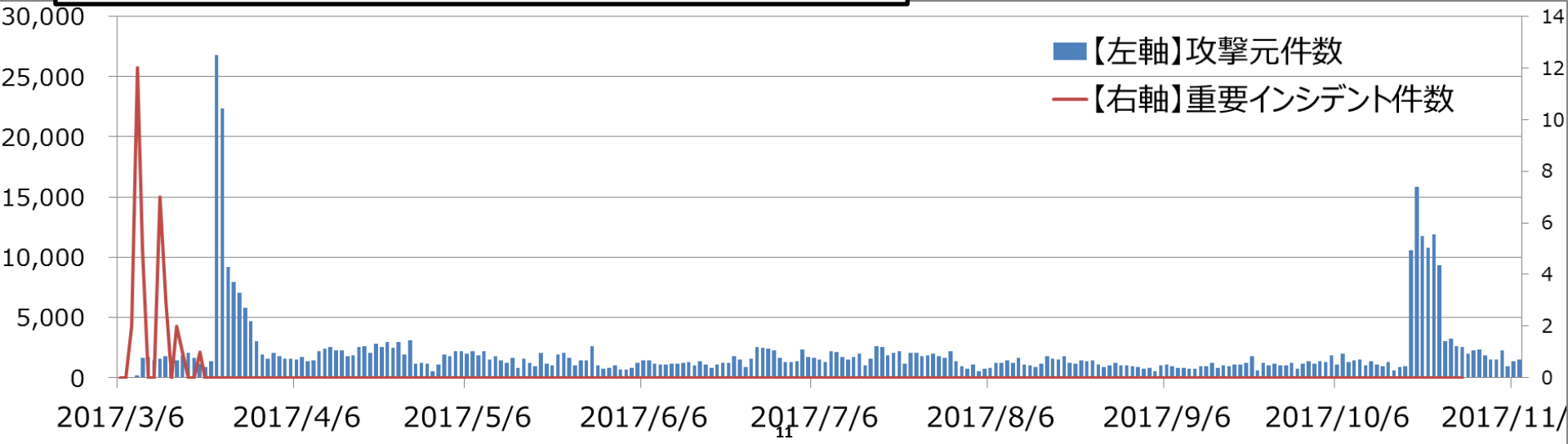
Apache Struts 2 の脆弱性(S2-045)

CVE-2017-5638（S2-045）の脆弱性

3月7日、Web アプリケーションを構築するフレームワークApache Struts 2 に任意のコードが実行される脆弱性(CVE-2017-5638、S2-045) が公開された。この脆弱性を悪用した攻撃を多数検知し、複数のお客様で実害が発生した。

JSOC にて確認している攻撃手法

- cat コマンドでファイル参照
- /etc/passwd ファイルの参照
- iptables stop による通信制御無効化
- wget によるバックドアファイルの取得、作成
- cmd.exe を起動し、whoami コマンドの実行



いまだによくあるインシデント事例紹介

不正なファイルのアップロード

JSOC

事象

- **違法コピーの不正なファイル置き場にされていた**

認知度
高

原因

・FTP を書き込み権限ありの anonymous 許可設定で運用していた
・HTTP の書き込み権限が有効で、PUT でファイルをアップロードされた
・メンテナンス期間のみの暫定サーバが稼動したままになっていた

リスク

・ディスクや帯域の圧迫、システム障害
・著作権侵害による訴訟

対策

・稼動するサーバの適切な管理
・サーバ、アカウント情報のたな卸し

スパムメール配信の踏み台にされた

JSOC

事象

- **スパムメールを配信していると外部から指摘があった**

認知度
高

原因

・メールリレーの設定が不適切であった
・Proxy(HTTP) の設定が不適切で、踏み台にされた

リスク

・外部への迷惑メール送信
・ブラックリスト掲載によるメール送信不可

対策

・設定内容の見直し
・送信元IPによるアクセス制御

アカウントの不適切な管理

JSOC

事象

- **外部から不正にログインされた**

認知度
高

原因

・デフォルトの ID、パスワードで運用していた
・脆弱なパスワードが設定されており、admin/adminなどで侵入された

リスク

・WEB ページの改ざん
・情報漏えい

対策

・設定内容の見直し
・送信元IPによるアクセス制御

アクセス制御の未実施・考慮不足

事象

- **内部向けの機器に外部からアクセスできてしまった**

認知度
中

原因

・ネットワークカメラが公開されており、室内が覗き見できる状況であった
・プリンタが公開されており、外部から大量の印刷が行われた
・DNS や NTP の設定が不適切で、DDoS 攻撃の踏み台にされた

リスク

・情報漏えい
・外部への攻撃への加担

対策

・設定内容の見直し
・送信元IPによるアクセス制御

NTPサービスを悪用したDoS攻撃(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

17

セキュリティ監視ができていなかった

JSOC

事象

- **IPS で攻撃を遮断しているつもりができていなかった**

認知度
中

原因

・(そもそも)設定ミス、設定不足
・WAF を入れていたが、検知のみの設定になっていた
・SSL(HTTPS)による暗号化通信で攻撃され、遮断できなかった

リスク

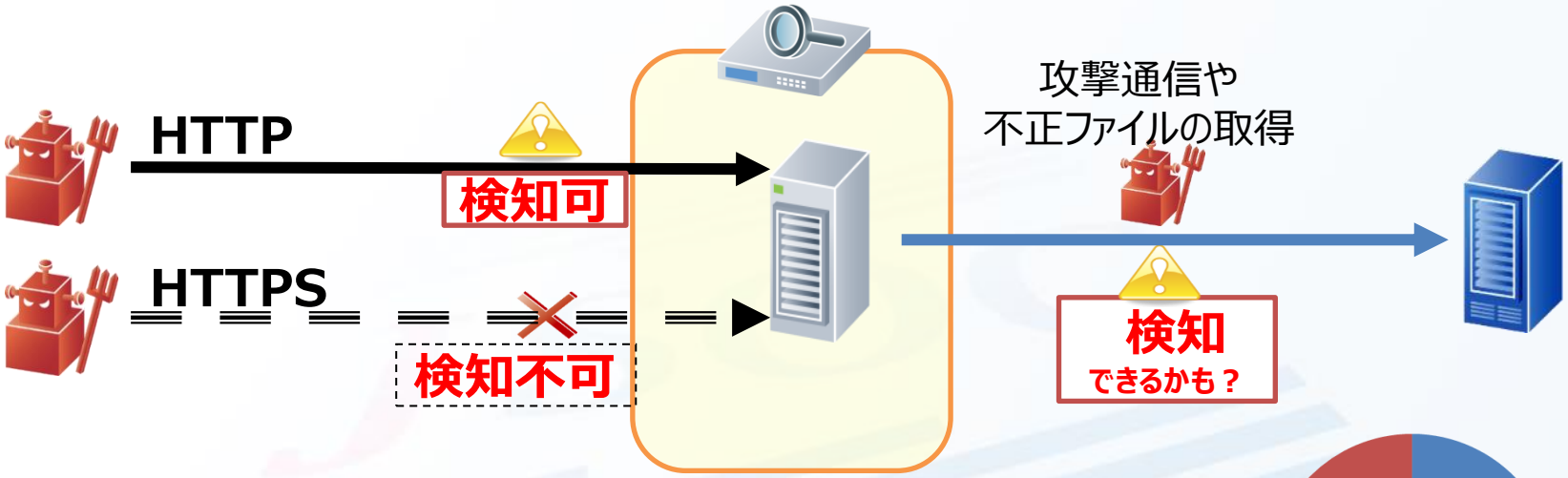
・WEB 改ざん
・情報漏えい

対策

・設定内容の見直し
・SSL 復号製品の導入

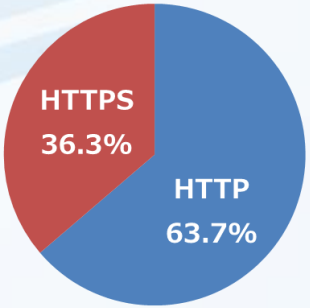
HTTPS(SSL)による暗号化通信での被害事例

※あくまで代表例で、SSL証明書のインストールなどで検知できる場合もあります



暗号化通信での被害事例が発生

HTTPS 経由にて、攻撃を検知できない事例が複数発生。
突然バックドアファイルを取得に行く通信を検知し、調査の結果
HTTPS 経由で Apache Struts2の脆弱性をついた攻撃が
成功していたことが判明した。



■HTTPの割合 ■HTTPSの割合

※2017年7月 JSOC顧客における平均値

脆弱性対策ができていなかった(1)

JSOC

事象

- **頑張ってアップデートしてたのに有効ではなかった**

認知度 **低**

原因

・アップデートしたプログラム、ライブラリが利用中のものと違った
・本体ではなくプラグインの脆弱性だった
・更新後、再起動していなかった

リスク

・WEB 改ざん
・情報漏えい

対策

・稼働中のプログラムの更新
・不要なものは削除する

脆弱性対策ができていなかった(2)

事象

- **アップデートが必要だと認識していなかった**

認知度 **低**

原因

・アプライアンス製品も OpenSSL を使ってた
・Firewall で通信遮断したから、脆弱性あるけど大丈夫
・NTP の標準設定を知らなかった

リスク

・情報漏えい
・内部への侵入

対策

・何が公開されているか、外からの調査
・アクセス制御できているか、再確認

インシデント対応体制ができていなかった

事象

➢ **インシデント検知はできたが、対応に着手できなかった**

認知度
中

原因

・緊急時の連絡フローは作成したが、最後のGoサインを出せる人が明確ではなかった
・技術面での手順書などに注意が行き、本番当日の想定が希薄だった

リスク

・インシデント発生時の対応の遅れによる被害拡大

対策

・インシデント対応訓練の実施と権限範囲の明確化

番外編：外部からのマルウェア感染、不正侵入(1)

事象

➢ **何もしていないのに持ち出しPCがウイルス感染した！**

認知度 **低**

原因

・USBスティック型モデムやSIM内蔵型端末で、グローバルIPが割り振られていた
・社内用のつもりで、ネットワーク接続では「ホーム ネットワーク」を選択していた

リスク

・情報漏えい
・内部への侵入

対策

・外部から接続できてしまわないか、
IP アドレスを確認する

番外編：外部からのマルウェア感染、不正侵入(2)

press release in English ▶

JC3 日本サイバー犯罪対策センター
JC3 : Japan Cybercrime Control Center

HOME | 活動概要 | 情報提供 | イベント情報 | 会員ページ | 関連リンク | JC3について

HOME > 情報提供 > 注意喚起情報 > 脆（ぜい）弱性

グローバルIPアドレスを直接割り当てられたPCのセキュリティ対策について

2017年 6月28日

最近、グローバルIPアドレスが直接割り当てられたコンピュータにおいて、不正侵入やマルウェア感染を引き起こす事例が相次いで発生しています。セキュリティ対策が不十分なPCやタブレット等に対して、データ通信カード、USBスティック型モデム等によってグローバルIPアドレスが直接割り当てられているにもかかわらず、これに気付かずに使用していることが想定されます。

利用者、管理者の方におかれましては、以下の①～③のウェブサイトも参考にして、社外持ち出し用のPCやタブレット等のセキュリティ設定（セキュリティパッチやパーソナルFWの設定等）をご確認いただくとともに、利用している機器にグローバルIPアドレスが割り当てられている場合には、脆弱性が悪用される可能性の有無についてもご確認されることを推奨いたします。

① ソフトウェアのぜい弱性に関する注意喚起について（JC3）
https://www.jc3.or.jp/topics/vul20161222.html

② ランサムウエア "WannaCrypt" に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2017/at170020.html

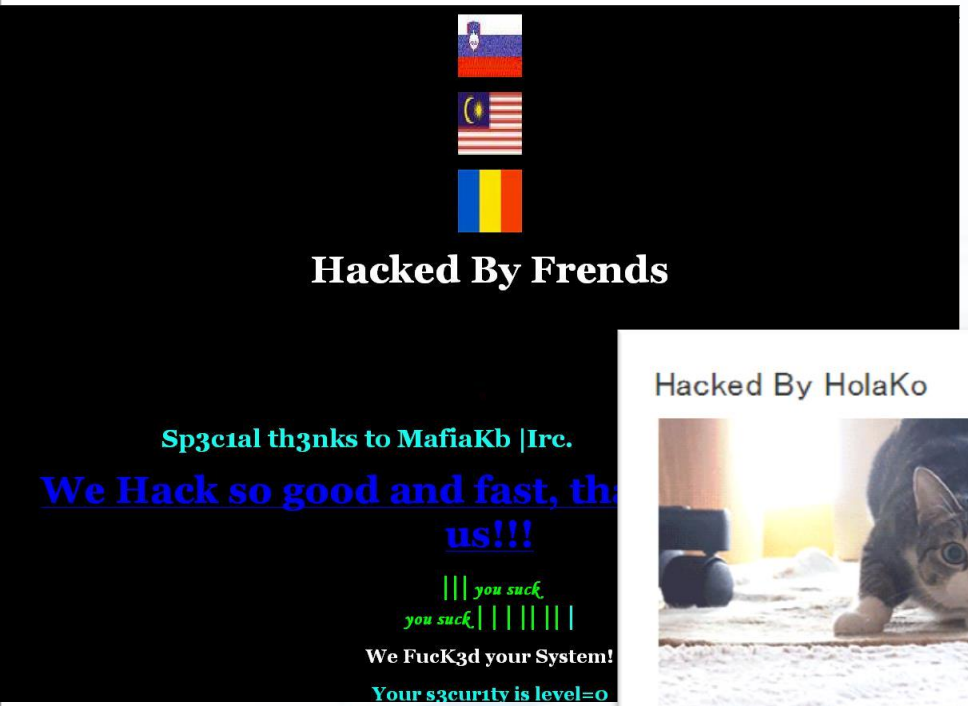
③ IPAに寄せられているランサムウェアの相談について～Wanna Cryptorの感染防止のために今すぐWindows Updateを～（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20170515.html

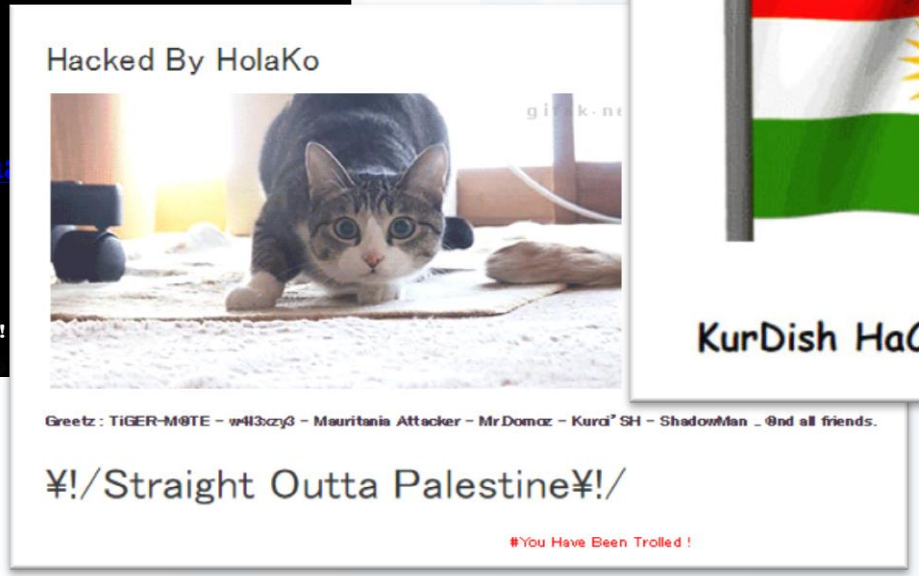
グローバルIPアドレスを直接割り当てられたPCのセキュリティ対策について
https://www.jc3.or.jp/topics/gip_sec.html

改ざん被害にあった場合の事例

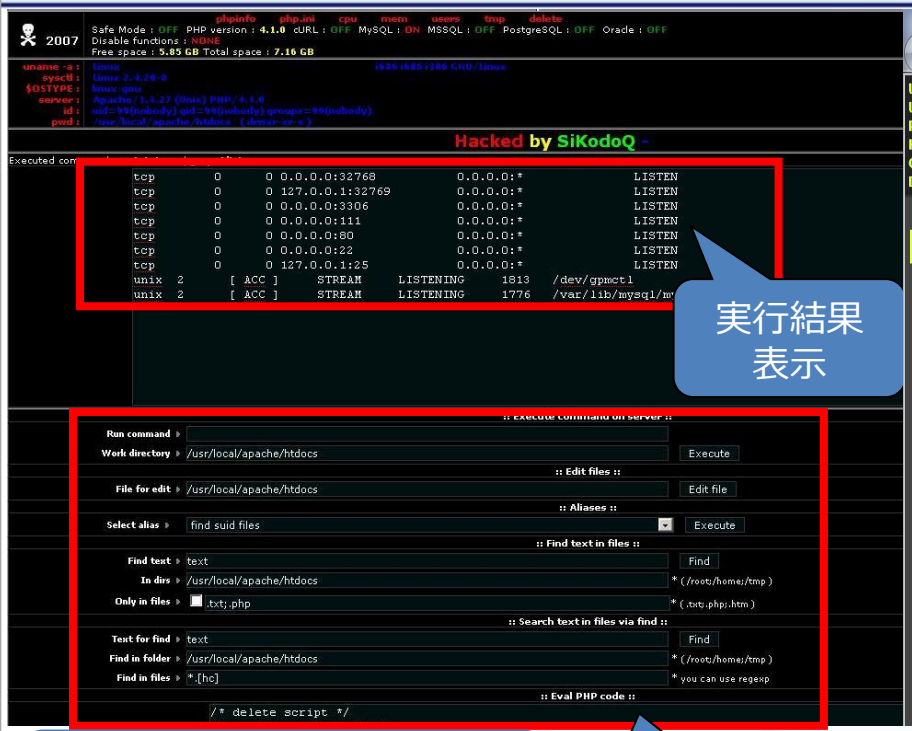
- Web ページの改ざん
- バックドア設置
- 外部サイトへ転送

Web ページの改ざん





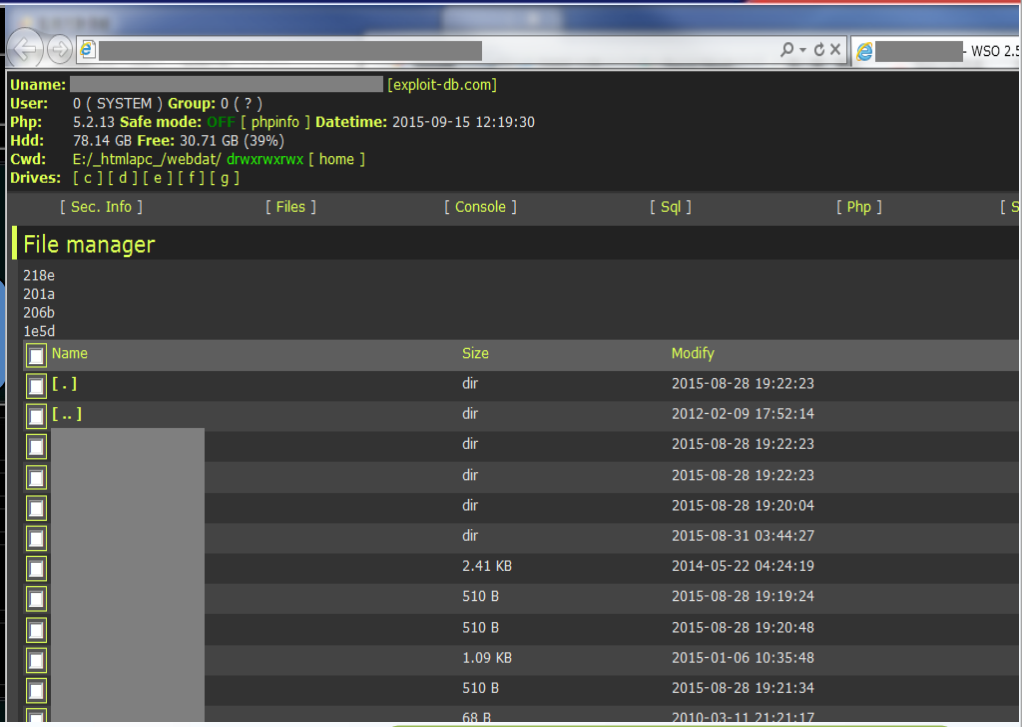
バックドア設置



実行結果表示

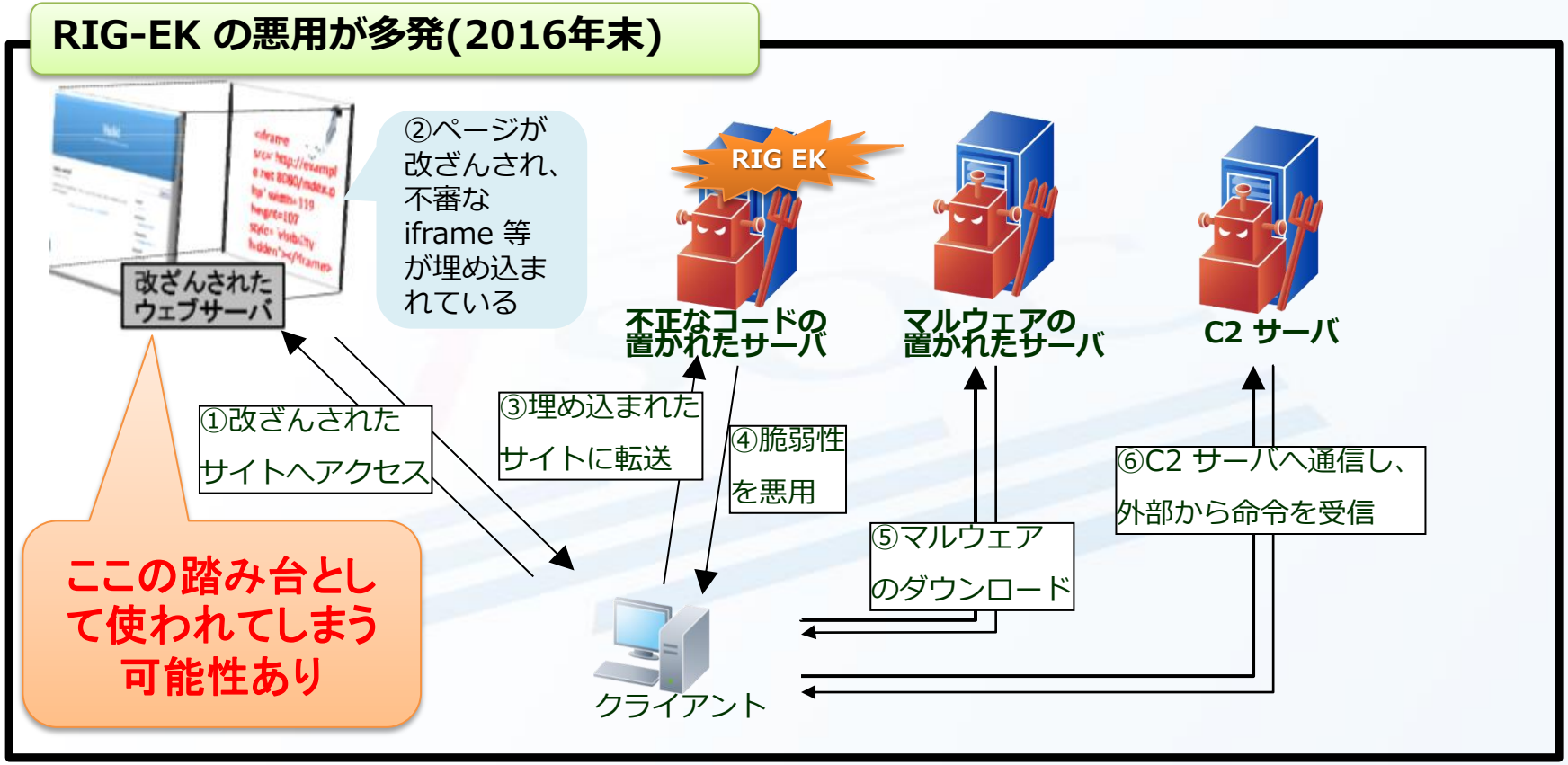
R57shell や c99shell および名のないWebShell

任意のコマンドを実行出来る



Web Shell by orb(WSO)と呼ばれる高機能WebShell

外部サイトへの転送



相次ぐ不正送金の被害

1　平成28年上半期の発生状況

発生件数及び被害額　　857件　約８億9800万円

期間	件数	被害額	実被害額
平成28年上	857件	約８億9800万円	約７億7200万円
平成27年下	740件	約15億3000万円	約12億6400万円
平成27年上	755件	約15億4300万円	約13億8300万円

※　被害額　・・・犯人が送金処理を行った全ての額

※　実被害額・・・「被害額」から金融機関が不正送金を阻止した額を差し引いた実質的な被害額

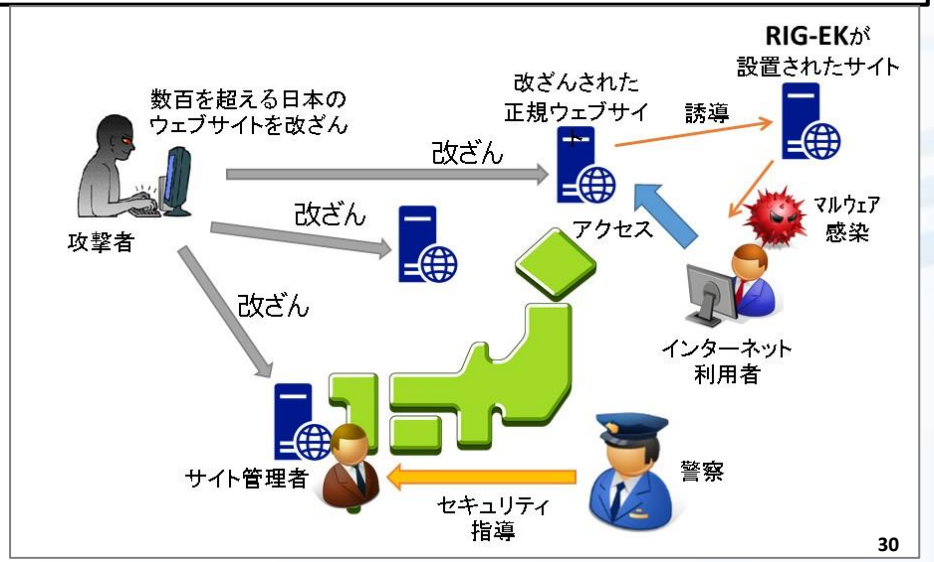
平成28年上半期におけるインターネットバンキングに係る不正送金事犯の発生状況等について
http://www.npa.go.jp/cyber/pdf/H280908_banking.pdf

不正改ざんサイトの無害化について

日本のサイトが踏み台に

オンラインバンキングなどの金融関連情報や、キー入力情報などを窃取する Ursnif の感染が複数の企業等で増加。感染源の一部となっていたRIG-EKについて、日本のサイトが多数改ざんされていた。

JC3経由で県警様を通じ、全国 38 都道府県、 298 サイトへのセキュリティ指導を実施した。



まとめ

○外部からネットワーク越しにどう見えるか、
　しっかり確認する

○モバイル端末にも注意

○通信元もアクセス権も「必要最低限」に

Thank you. Any Questions ?

※ 本資料は2017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。
※ 本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。
※ 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。

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