入れて安心していたセキュリティ対策機器が攻撃されたあの日

2016年11月29日

株式会社ラック
サイバーセキュリティ事業部 JSOC
賀川　亮

アジェンダ

- 自己紹介＆JSOC紹介
- セキュリティ製品に対する脅威について
- 非常に簡単に行えてしまう、セキュリティ製品の攻略例
- セキュリティレベルを高く保つために必要な当たり前のこと
- 今なお残る、設定不備による脅威
- まとめ

自己紹介

株式会社ラック　サイバーセキュリティ事業部
JSOC グループリーダー　賀川 亮 , CISSP

カガワ リョウ
賀川　亮

◆プロフィール
生まれは福島、育ちは神奈川

入社：2003年（14年目）
現在に至るまでラック一筋

入社後JSOC配属となりセキュリティデバイスの運用に2年ほど携わる。

その後、4年ほどセキュリティアナリストとしてあらゆるログにまみれる生活を送り、
ログにまみれ疲れた頃に、某外部秘密組織にセキュリティアナリストとして、6年ほど
家族にも言えない（情報機密的な意味で）お仕事に携わる。

2014年7月～ JSOCに舞い戻り、JSOCでアナリストグループリーダーとして
24h365d インシデント対応業務を遂行している。

JSOC (Japan Security Operation Center)

LAC

自社独自の監視・分析システム「LAC Falcon(TM)」

100名以上のプロフェッショナル

15年以上のSOC経験と実績

1995 ネットワークセキュリティ事業を開始

2000 セキュリティ監視センター設置、「九州・沖縄サミット」の不正アクセス監視を支援

2001 JSOCの運用がスタート

ワームが大流行（Nimda, Codered, Slammer など）

2005 監視対象セキュリティ機器の台数が500台を突破

SendmailやCiscoIOS等攻撃が流行

2011 JSOCのスタートから10年。監視対象セキュリティ機器の台数が900台を突破

SQLインジェクション大流行

USBメモリの使用や、WEBサイトの閲覧で感染するウイルスの流行（Conficker など）

2012 次世代型Firewall（PaloAlto）への監視サービス提供を開始

個人情報の搾取に特化したウイルスの登場

2014 マルウエア対策製品（FireEye）への監視サービス提供を開始

2012年以降 APT(標的型攻撃)による情報漏えい事故が多発

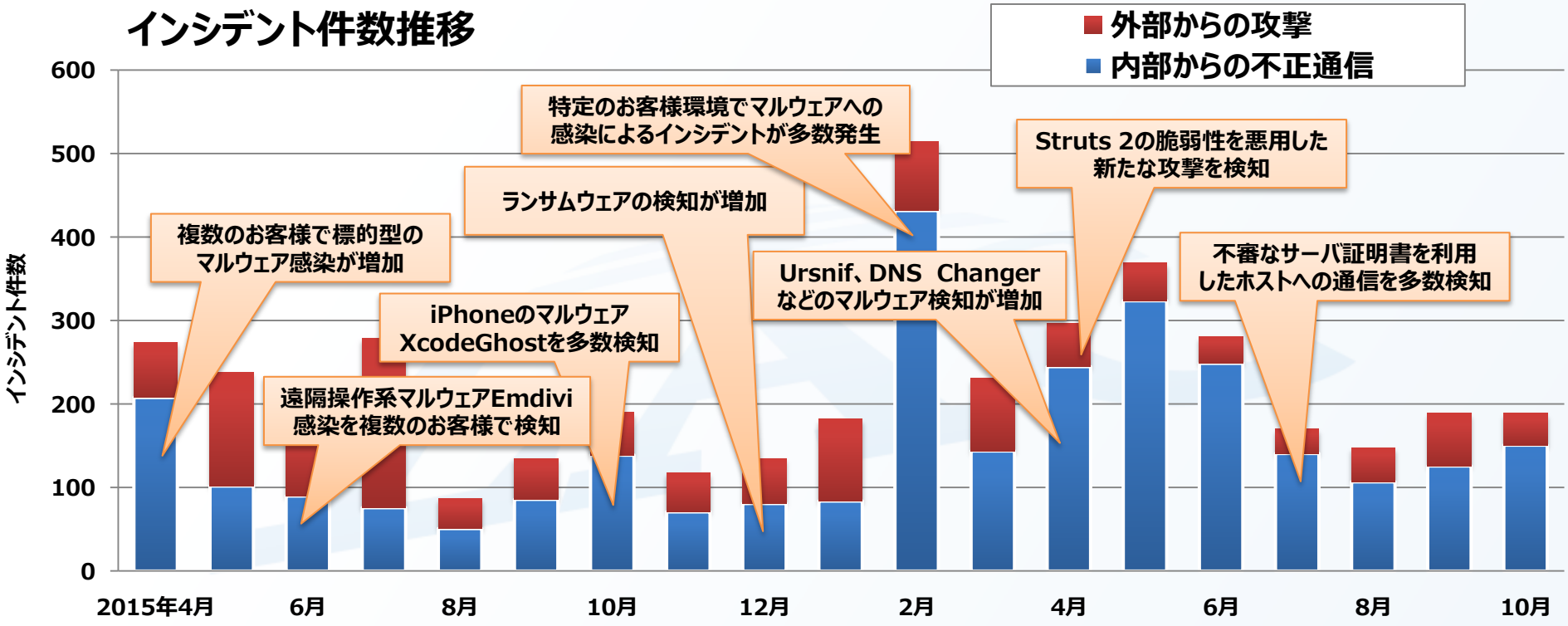
2016

金銭搾取目的のマルウェア流行
大規模個人情報漏洩
セキュリティデバイスを狙った攻撃が複数登場

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見て取れる状況が継続

相次ぐセキュリティ製品に対する脅威

Juniper社　ScreenOS

SSHの管理コンソールに第三者が
容易にログイン可能な脆弱性が発覚

FORTINET社　FortiOS

Cisco社 CiscoASAシリーズ

複数の任意のコマンドを実行可能な
脆弱性が発覚

FireEye社 FireEyeシリーズ

任意のコードが実行可能な
脆弱性が発覚

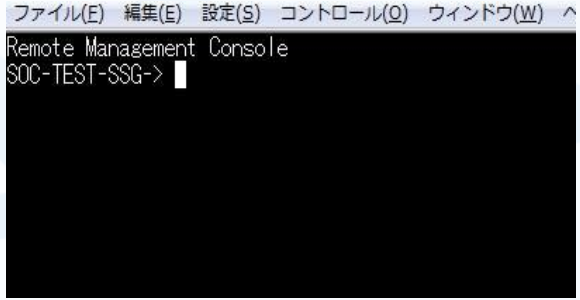
Palo Alto Networks社 PANOS

WebAPI経由で任意のOSコマンドが
実行可能な脆弱性などが発覚

ScreenOSに認証回避の脆弱性(1)

脆弱性の概要

脆弱性番号	CVE-2015-7755
影響バージョン	ScreenOS 6.3.0r17～6.3.0r20
対象経路	TELNET、SSH(SCP含む)、シリアルコンソール
ユーザID	任意の文字列(存在していないユーザでも可能)
パスワード	<<< %s(un='%s') = %u



認証を回避するパスフレーズを入力することで、特に**特殊な操作をすることなく**ログイン可能

ScreenOSに認証回避の脆弱性(2)

攻撃の確認方法および対策

ログイン成功時のログ(SSHにaaaaというユーザでログインを試みた場合)

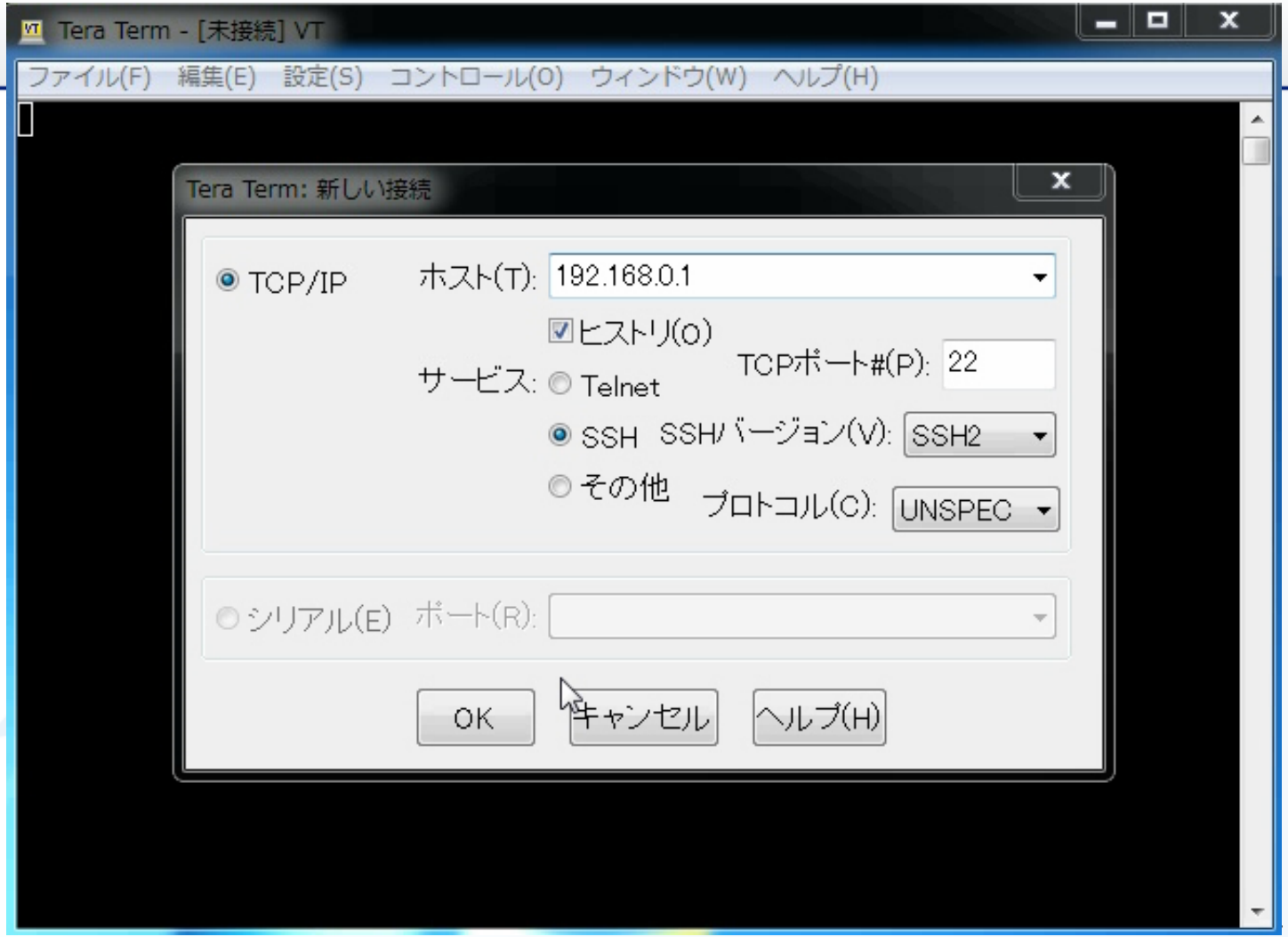
2016-11-16 19:07:23 system warn 00515 Admin user **system** has logged on via SSH from 192.168.0.2:57411
2016-11-16 19:07:23 system warn 00528 SSH: Password authentication successful for admin user 'aaaa' at host 192.168.0.2.

ログインを試みたユーザ名に関わらず、system というアカウント名で
ログインしているように記録される

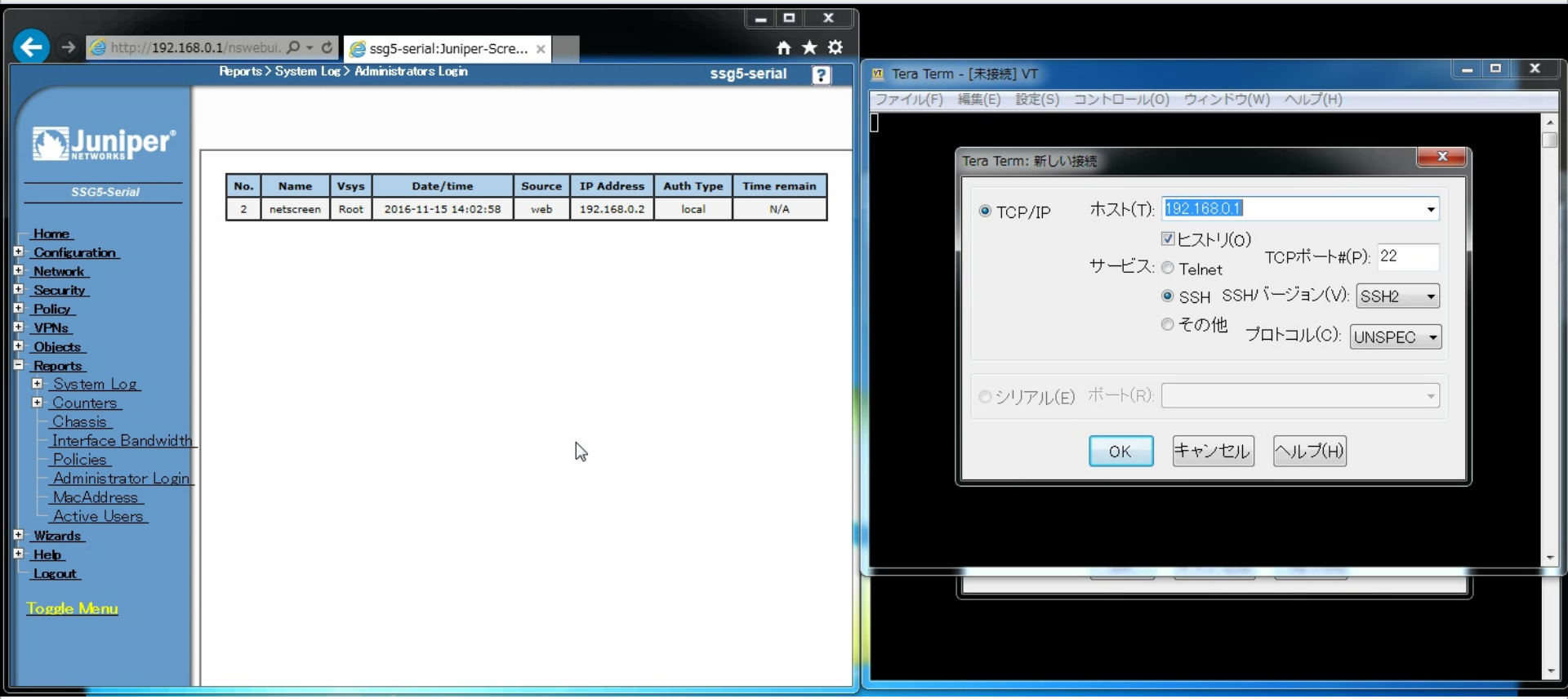
対策方法

- Juniper社から提供されている対策バージョンへの更新
- 対象機器に対するTELNETやSSHを用いた管理ログインについて、IPアドレスを制限
- シリアルコンソールでもログインが可能であるため、物理アクセス制御

デモ１



デモ２

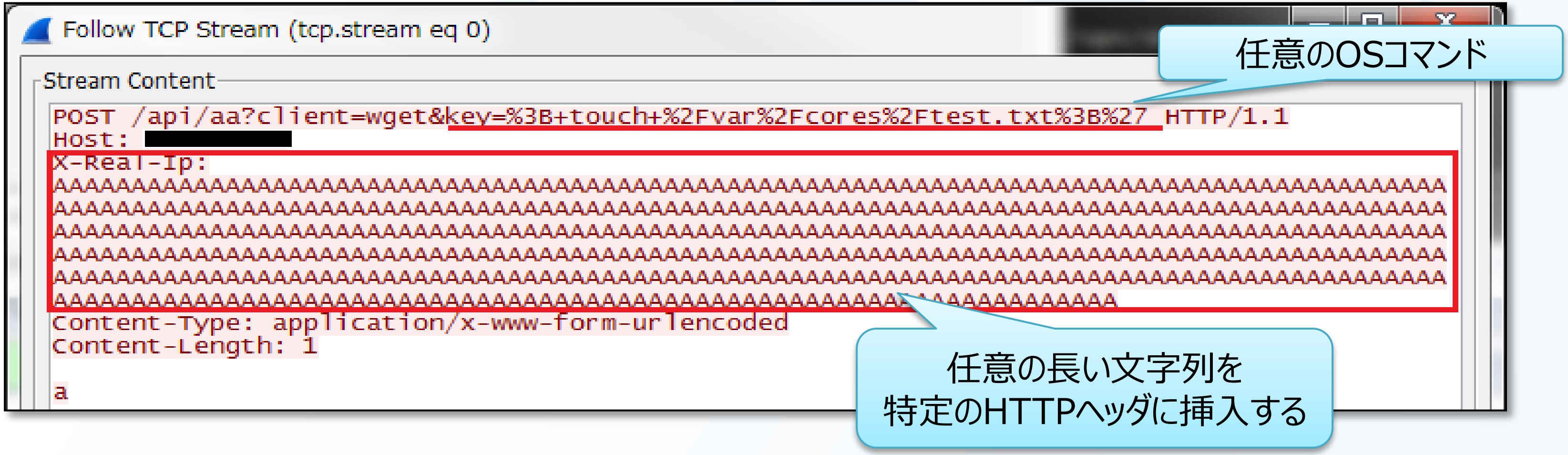


PAN-OS のリモートコード実行の脆弱性

脆弱性概要

2月23日～25日、 Palo Alto Networks社のNGFW向けOS「PAN-OS」のアップデートが公開、5件の脆弱性を修正した。3月16日、当該脆弱性の修正を待って、ドイツのカンファレンスにて脆弱性の検証方法が公開された。

修正された脆弱性の中で、 Web ベースの API を経由して事前認証なく任意の OS コマンドが実行可能な脆弱性(CVE-2016-3655)は、公開された手法を用いて実際に一部の OS コマンドが実行可能なことを確認した。JSOCで被害を確認した事例は無し。



Shadow BrokersによるNSAの機密情報公開？(1)

公開されたファイルに攻撃ツール

Shadow Brokersと呼ばれると呼ばれるグループが、NSA（米国家安全保障局）内部の人員で構成されているとされる「Equation Group」から入手した情報として、2つのファイルを公開。

いずれもPGPで暗号化されていたが、一つは復号キーを含め内容が公開され、ファイル群には主にFirewall製品に対する攻撃ツール等が含まれていた。

Exploits
(攻撃ツール群)

Implants
(Firewall製品の不正ファームウェア群)

Tools
（その他の補助ツール群）

Exploits	
EGREGIOUSBLUNDER（FortiGate社製品用）	**ELIGIBLEBACHELOR**（TOPSEC社製品用）
ELIGIBLEBOMBSHELL（TOPSEC社製品用）	**ELIGIBLECANDIDATE**（TOPSEC社製品用）
ELIGIBLECONTESTANT（TOPSEC社製品用）	**ESCALATEPLOWMAN**（WatchGuard社製品用）
EXTRABACON（Cisco社製品用）	**EPICBANANA**（Cisco社製品用）

0day

Shadow BrokersによるNSAの機密情報公開？(2)

EXTRABACON

Cisco社のFirewall製品であるCisco ASA(FirePOWER含む)に、不正なSNMPパケットが送りつけられることで任意のコードが実行される恐れのある脆弱性(CVE-2016-6366)が公開された。

公開されたツールを脆弱な環境に対して実行すると、**Cisco ASAがクラッシュして再起動**するケースと、**管理アクセスの認証が無効化される**ケースのいずれかが発生することを確認した。

```
login as:
@            password:
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa# configure terminal
ciscoasa(config)#
```

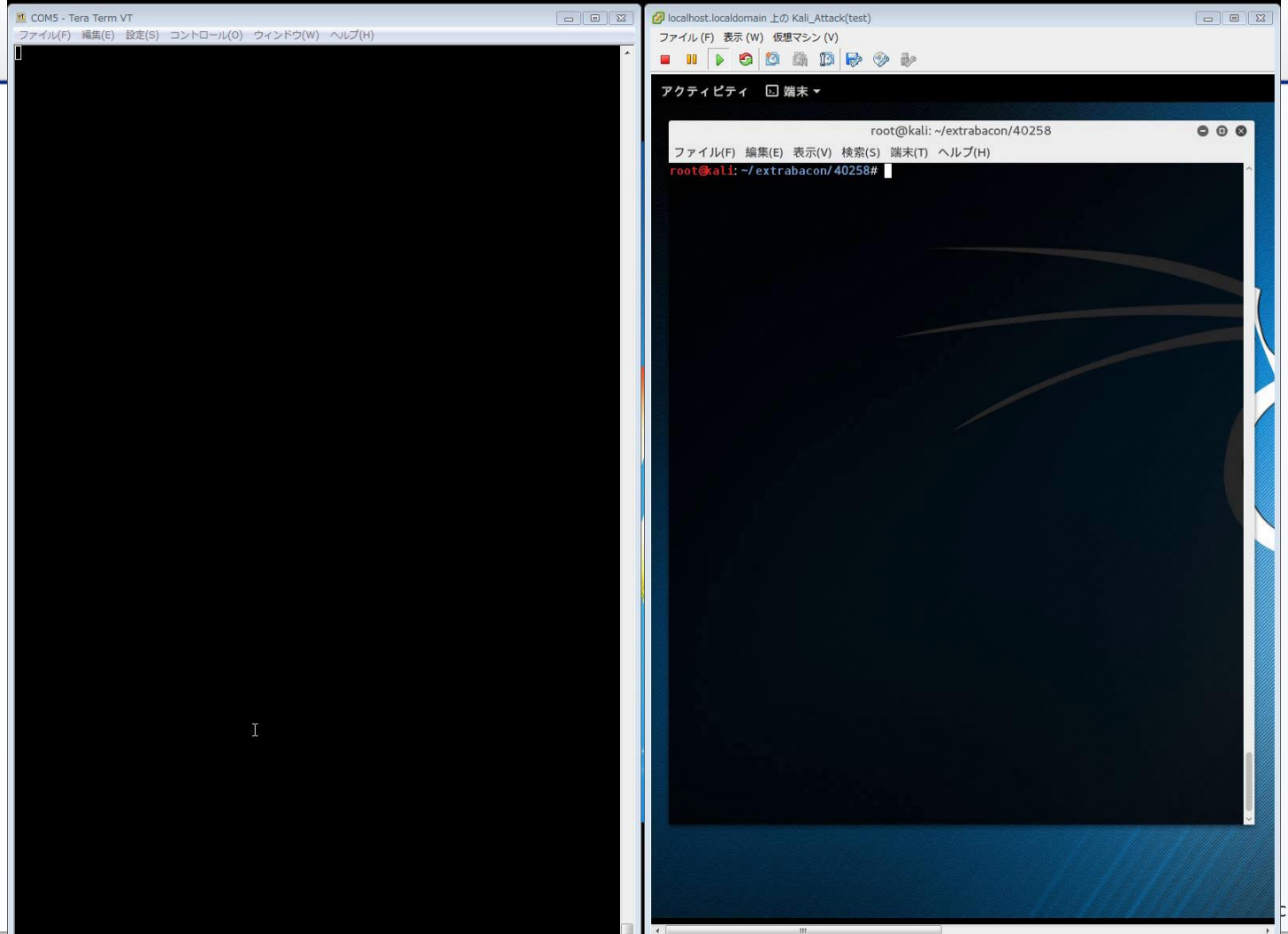
攻撃が成功すると、ログイン時にユーザ名とパスワードに何を入力してもログイン可能な状態になることを確認。

※この例では何も入力しない（ユーザ名やパスワード入力時にEnterのみ入力）で特権モードになっている。

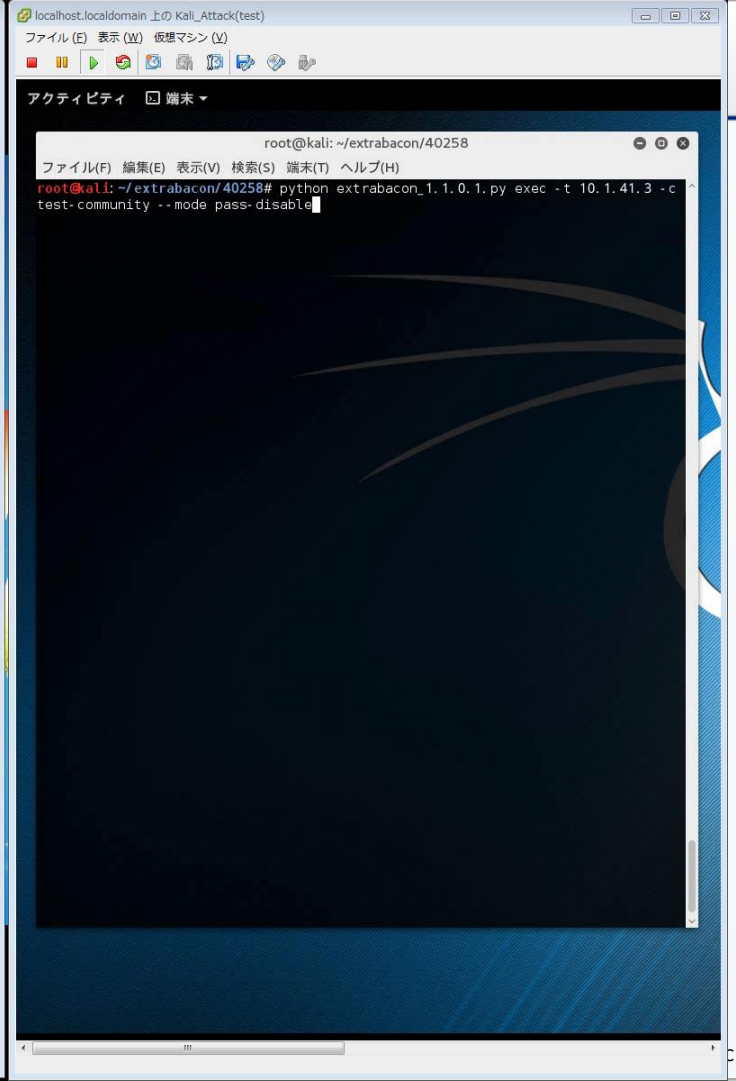
攻撃の主な成立条件
SNMPサービスにアクセス可能であること
SNMPのコミュニティ名やアカウント名などを攻撃者が知っていること ※「public」など容易に類推できるコミュニティ名は注意

昨年からNetScreen、PaloAlto、FortiGateなど管理権限を奪取可能な脆弱性の公表が続いているが、管理アクセスの厳格化（送信元の制限など）で防げることも多いため、設定状況の見直しが望ましい

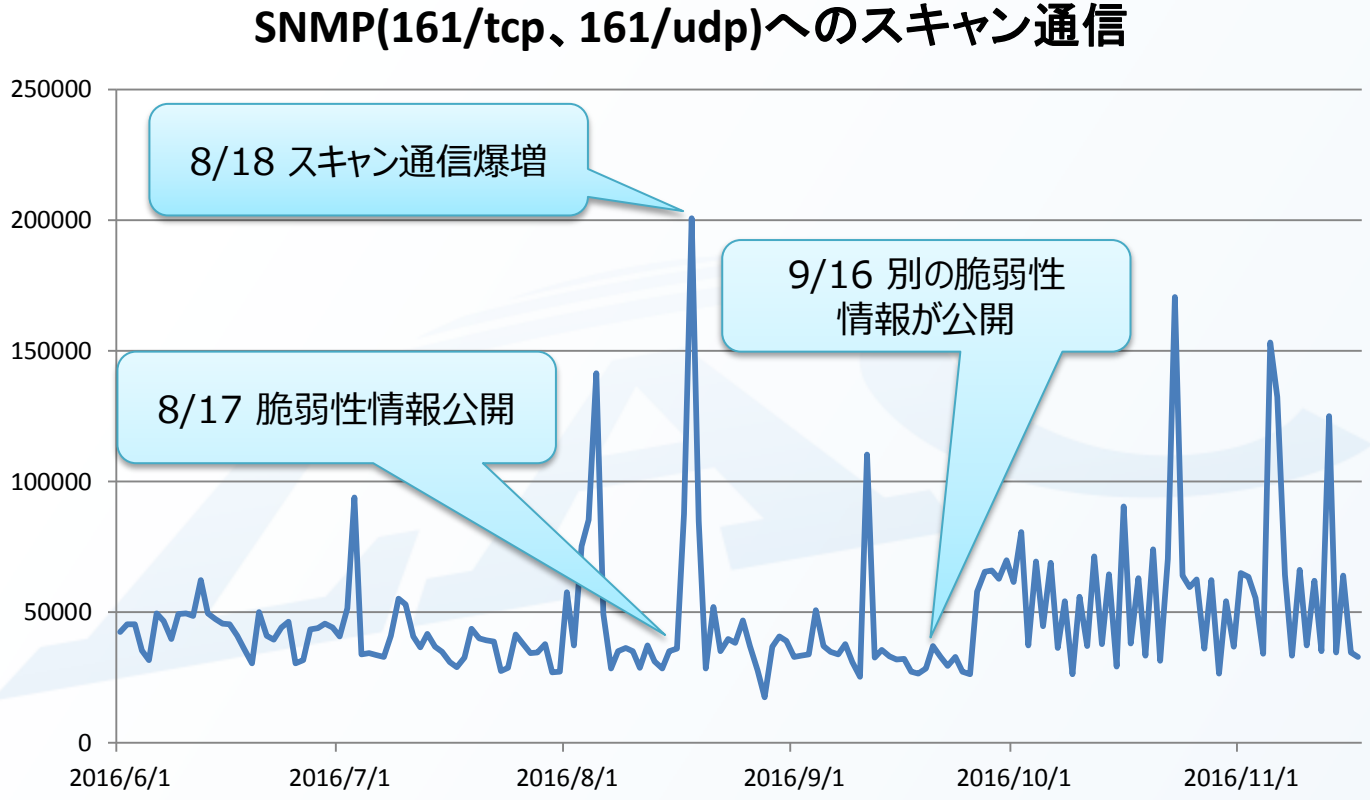
デモ１



デモ２



オープンな環境は意外と多く、調査行為はさらに多い



大事なのは、適切なアクセス制御と情報収集・維持管理

身勝手な思い込みが、習慣となる危険性

「多分、大丈夫だろう」と自分に都合よく考えて、一方的に安全だと思い込み運転することを、一般に「だろう運転」と呼んでいます。その結果、「まさか、そうなるとは思わなかった」というような、思わぬ出来事が起きることがあります。

状況確認をおろそかにせず、危険を察知しましょう

自分に都合よく考える「だろう運転」は、繰り返すうちに「危険な運転である」という意識が薄くなり、やがて「大丈夫だろう」と身勝手な思い込みが習慣になり、結果として事故を起こすリスクが高まります。

「～だろう」から、「～かもしれない」に

当たり前のことを当たり前に継続実施し続けることが肝要

設定不備によるインシデント事例

設定不備によるインシデントも依然、発生中

JSOCで確認しているインシデントは、オーバーフロー系の攻撃やSQLインジェクションなど脆弱性を狙った攻撃が数多くありますが、中には**サーバや機器の設定不備**に起因するインシデントも一定数発生しています。

事例紹介

- FTP サーバを書込み権限ありの anonymous 許可設定で運用していた
- ネットワークカメラが意図せず公開されていた
- デフォルトの ID 、パスワードで運用していた
- SIP サーバが外部から悪用され、数十万の料金を請求された
- squid が SPAM メールの踏み台にされた
- 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
- DNS や NTP の設定が不適切で、DDoS 攻撃の踏み台にされた
- SSHサーバに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

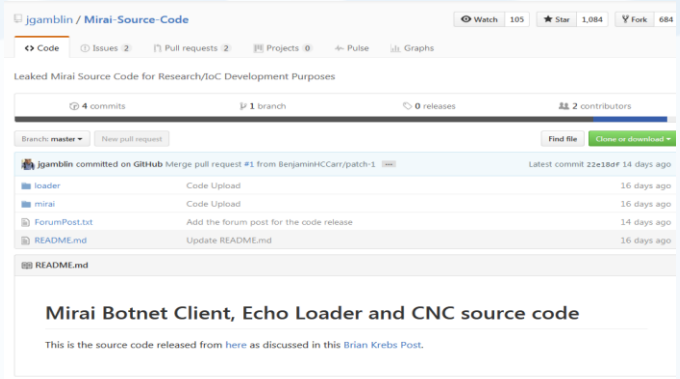
アップデートで回避できないインシデントは少なくない

IoT機器用マルウェア「Mirai」(1)

「Mirai」のソースコードが公開

9月下旬にKrebsOnSecurityに対して行われた最大級のDDoS攻撃(620Gbps)は「Anna-senpai」を名乗るユーザが作成した「**Mirai**」というマルウェアが50万台のCCTV等のIoTデバイスに感染してボットネットを形成し行われたものであると報じられました。

2016年10月1日にHack Forumsにて「Anna-senpai」は「Mirai」のコードのリンクとその内容について書き込みを行い、リンク上のファイルは2週間後に削除する旨が書かれていたが、その後GitHubにて公開された。



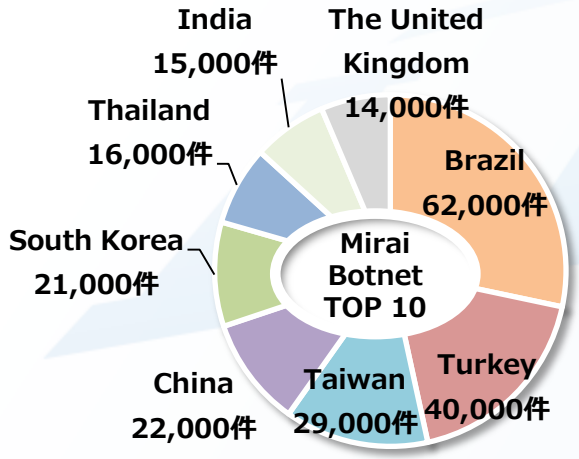
https://github.com/jgamblin/Mirai-Source-Code
http://moshbox.jp/?p=18727

IoT機器用マルウェア「Mirai」(2)

「Mirai」の被害状況

「Mirai」のボットネットを形成したデバイスにはXiongMai(雄邁)という中国のメーカーのソフトウェア、およびハードウェアが多く含まれていました。

ボットネットを形成するデバイスはベトナム、ブラジル、トルコに多くみられ、ありがちなユーザ名とパスワードの組み合わせ62種類を利用して感染活動を広げた模様。



ユーザー名	パスワード
666666	666666
888888	888888
admin	(なし)
admin	1111
admin	1111111
admin	1234
admin	12345
admin	123456
…	…
…	…
admin	admin

http://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet

まとめ

セキュリティ製品であっても、簡単に攻略できてしまう脆弱性は普通に存在。

大半は適切なアクセス制御と設定・維持管理で防げるものが多い。
中には致命的なものもある（例：2014年のGNU Bashの脆弱性など）ので
「すぐに動ける」「定期的に見直しが行える」体制作りをインシデントレスポンスの体制と
同様に備えておくべき。

サポートが切れた製品、簡易組み込み設計で未サポートなものなど、危険が含まれたままの
可能性が危惧されるため、地道だけれど当たり前の運用を当たり前にやる（できる状況で
あることを確認する）ことが一番効果的。

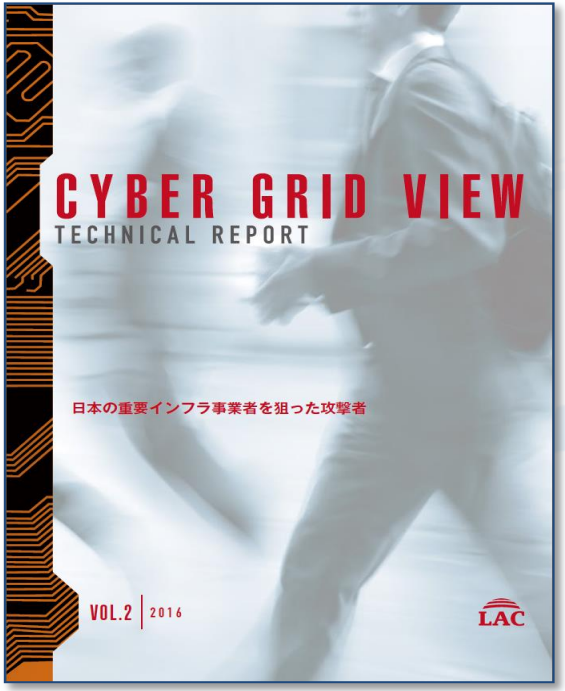
ただし、その当たり前の運用を実施するのは「人」であるため、製品の機能も以上に
やっぱり**セキュリティは「人」が担うもの**だとあらためて実感している。

「人」の教育と、「～かもしれない」という気付き、適切な管理の「仕組み」を満たすこと。
機器やサービスへの投資も必要だけれど、人への投資も忘れずに。**必要ならばご協力します。**

Cyber Grid View Vol.2の公開（LAC）

サイバー救急センターで対応した
実際のインシデントレポート第2弾

- 日本の重要インフラ事業者を狙った攻撃に使われた「Daserf」



Point

- DaserfのC2サーバのIPアドレスは、韓国のインターネットサービスプロバイダを利用するケースが多いことを確認
- Daserfを利用する攻撃者は日本の重要インフラを標的とし、長期間に渡って標的組織に潜伏しつつ活動していることを確認
- 調査・分析より得られた断片的な状況証拠から、Daserfを利用する攻撃者像を推察

http://www.lac.co.jp/security/report/2016/08/02_cgview_01.html

JSOC INSIGHTの概要

「JSOC INSIGHT」とは？

四半期毎にJSOCで検知した特徴的なインシデントを取りまとめた定期レポート

Vol.13の概要

■ **検知傾向ピックアップ**
- 感染端末のDNSサーバの設定を書き換えるDNS Changer
- 大量に検知したインターネットからの攻撃通信例

■ **トピックス**
- 相次ぐApache Struts 2の脆弱性公開
- Ursnifの感染事例の急増
- ランサムウェア感染を誘導する不審メールの増加

http://www.lac.co.jp/security/report/pdf/20161031_jsoc_o001m.pdf

JSOC INSIGHT Vol.14 も準備中！

LAC
ともに、イキル

Thank you. Any Questions ?

※ 本資料は2016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