

# 続・セキュリティのおはなし [Enog52]

2018/8/31

NS・コンピュータサービス

小野澤 進

# 今日のおはなし

- 最近の情報セキュリティ脅威
- ツールあれこれ
- まとめ

# 最近の情報セキュリティ脅威

...



# 情報セキュリティ脅威の変化

◆組織向け情報セキュリティ10大脅威（赤枠は前年度ランク外）

順位	2018年	2017年
1	標的型攻撃による被害	標的型攻撃による情報流出
2	ランサムウェアによる被害	ランサムウェアによる被害
3	ビジネスメール詐欺による被害	ウェブサービスからの個人情報窃取
4	脆弱性情報の公開に伴う悪用増加	サービス妨害攻撃による被害
5	セキュリティ人材の不足	内部不正による情報漏えいと業務停止
6	ウェブサービスからの個人情報窃取	ウェブサイト改ざん
7	IoT機器の脆弱性の顕在化	ウェブサービスへの不正ログイン
8	内部不正による情報漏えい	IoT機器の脆弱性の顕在化
9	サービス妨害攻撃による被害	攻撃のビジネス化
10	犯罪のビジネス化	インターネットバンキング、クレジットカード情報の不正利用

# 情報セキュリティ脅威の変化

## ◆ちなみに2014年との比較

順位	2018年	2014年
1	標的型攻撃による被害	標的型メールを用いた諜報活動
2	ランサムウェアによる被害	不正ログイン・不正利用
3	ビジネスメール詐欺による被害	ウェブサイト改ざん
4	脆弱性情報の公開に伴う悪用増加	ウェブサービスからの個人情報漏えい
5	セキュリティ人材の不足	オンラインバンキングからの不正送金
6	ウェブサービスからの個人情報窃取	悪意あるスマートフォンアプリ
7	IoT機器の脆弱性の顕在化	SNSへの軽率な情報公開
8	内部不正による情報漏えい	紛失や設定不備による情報漏えい
9	サービス妨害攻撃による被害	ウィルスを使った詐欺恐喝
10	犯罪のビジネス化	サービス妨害攻撃による被害

## 新たにランクインした脅威について調べてみる

### ◆ビジネスメール詐欺（BEC）

- 経営者や取引先になりすまし、不正な送金を指示し金銭をだまし取る
- 2016年以降、国内企業にも被害
  - 2017年12月 日本航空がビジネスメール詐欺によって約3億8000万円の被害
  - 国内企業、自治体においても約4割が受信経験あり（トレンドマイクロ社調査）

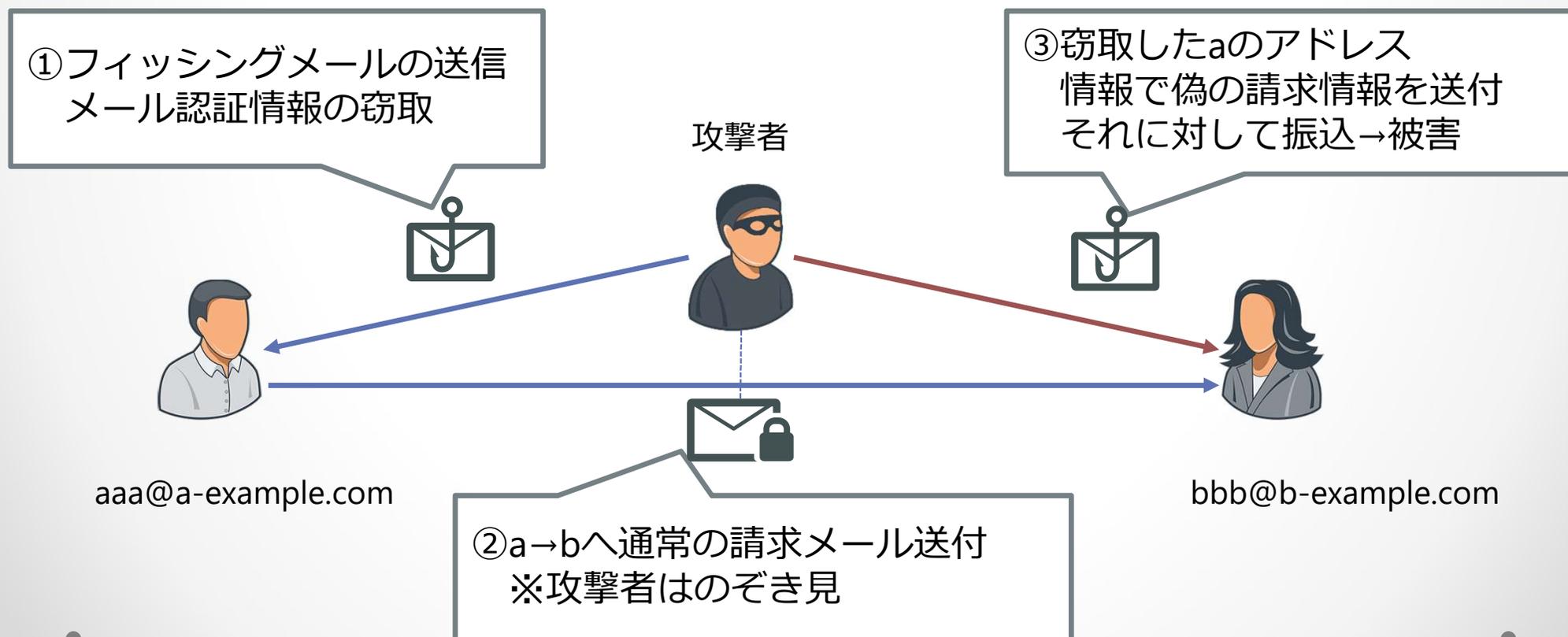
### ◆ビジネスメール詐欺の手法

1. 請求書の偽装
2. 経営者なりすまし
3. 従業員メールアカウントの窃取
4. 権威ある第三者へのなりすまし
5. 詐欺の準備としての情報窃取

# ビジネスメール詐欺の手法

## ◆ メールアカウントの乗っ取り

- キーロガー、RATマルウェアの送付
- フィッシングメール (HTMLメール・PDF→フィッシングサイトへ)



# ビジネスメール詐欺の手法

## ◆ソーシャルエンジニアリング

- メール返信先、差出人の偽装
- 詐欺メール送信時間の調整
- 判断力を鈍らせる（件名に「至急対応」「機密事項」など）

### ◆実際の返信先は正しいの？

Return-Path: **attacker@example.net**

...

From: "aaa@a-example.com" <aaa@a-example.com>

↑ 一般的なメールソフトは差出人にFrom:の値を表示する

### ◆パッと見正しい送信元に見えても...

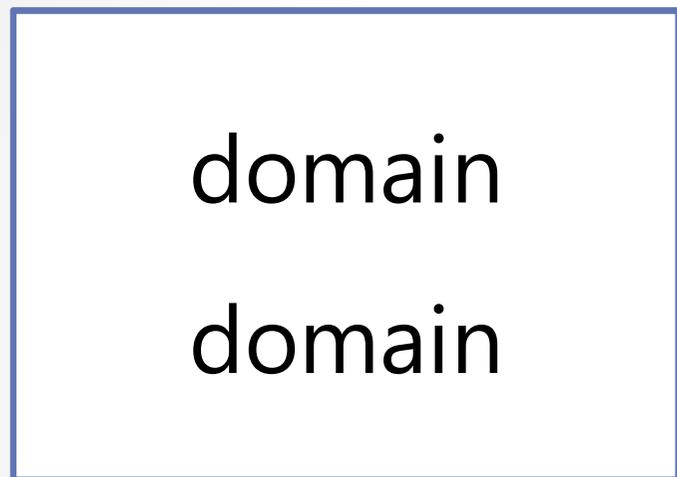
From: "aaa@a-example.com" <aaa@a-example.com>

≠

From: "aaa@a-exampie.com" <aaa@a-exampie.com>

## でも本当に見間違える？

ホモグラフ攻撃という手法もあります。



上下の違いがわかりますか？

上の文字はピュニコード変換すると以下のように変換されます。

上段：xn--domain-

下段：xn--dmain-jye ※oをギリシャ文字で似た形のoに変えています

このように、国際化ドメインを悪用した見せ方も存在しています。

## でも本当に見間違える？

「こんちにはみさなん おんげき ですか？」

タイポグリセミア (Typoglycemia) 現象

単語のはじめと終わりが合っていれば、単語の意味を脳内で補完してしまう現象

みまなさに だじいな おらしせ。  
こたのび なかお せいげどつう が  
ぜたついに ばれない ように  
どやらきの リニューアルを  
おなこいました。

ちみなにこのぶんしょうのじんゆばんも  
ばなれいようにいかれえています。

中尾清月堂ホームページより

<http://nakaoseigetsudou.jp/nakao/blog/いよいよ始まりました！どら焼きキャンペーン！>

## それっぽいメールは届いているか

閉じる 返信 全員に返信 転送 削除 迷惑メール 操作 ▼

**ご請求額の通知** 2018年08月08日 午後 5:24

差出人: ai ado

宛先: ( )

? 文書\_04015.iqy (238 B) [ダウンロード](#) | [ブリーフケース](#) | [削除](#)

メッセージにはテキストの内容がありません。

間違いがあれば連絡をお願いします。  
写真を送信致します。

それっぽい件名でしたが詐欺メールではなく、新たな添付ファイル(.iqy)によるオンライン銀行詐欺メールのようでした。（「URSNIF（アースニフ）」に感染）

# 対策は？

## ◆ビジネスメール詐欺（BEC）

- 技術的な対策
  - ✓ ウィルス対策ソフトによる認証情報窃取ツールの排除
  - ✓ Webフィルタによる不正URLに対する接続遮断
  - ✓ メールゲートウェイでのセキュリティ対策  
(なりすまし検出、不正URL、サンドボックス)
- 人の対策
  - ✓ 情報セキュリティに関するトレーニング  
(新たな脅威の認識、送信元詐称を行う手法の認識)
  - ✓ 依頼元本人への確認、第三者の確認プロセス

## (戻って)新たにランクインした脅威について調べてみる

### ◆脆弱性情報の公開に伴う悪用増加

- 2017年に悪用された脆弱性Top10のうち7つがMicrosoft製品  
3つがAdobe Flash Playerに関するもの
- サーバで利用されるOSS製品の脆弱性も多い  
Webアプリケーションサーバ、CMSソフトウェア

公開日	CVE	概要
2018-03-29	CVE-2018-7600	CMS Drupal リモートから任意のコードが実行可能
2018-04-26	CVE-2018-7602	CMS Drupal リモートから任意のコードが実行可能
2017-03-10	CVE-2017-5638	Apache Struts2 リモートで任意のコードが実行可能
2017-01-26?	-	WordPress 4.7.1 REST API 脆弱性による改ざんが可能
2018-08-22	CVE-2018-11776	Apache Struts2 リモートで任意のコードが実行可能

# 話題になった脆弱性

## ◆ハードウェアに関する脆弱性

- CPUの分岐予測・投機的実行の実装に脆弱性が判明
- 1995年以降のプロセッサ全て(一部除く)が影響

公開日	CVE	呼称	
2018-01-03	CVE-2017-5753	Spectre (Variant 1)	境界チェックのバイパス
2018-01-03	CVE-2017-5754	Meltdown (Variant 2)	分岐ターゲットのインジェクション
2018-01-03	CVE-2017-5715	Spectre (Variant 3)	不正なデータのキャッシュ読み込み
2017-03-10	CVE-2018-9056	BranchScope	セキュリティ保護機能(SGX)も回避
2018-05-22	CVE-2018-3639	Spectre (Variant 3a)	Spectreの亜種
2018-05-22	CVE-2018-3640	SpectreNG (Variant 4)	Spectreの亜種
2018-07-10	CVE-2018-3693	Spectre1.1	Spectre Variant 1の亜種
2018-08-14	CVE-2018-3615	L1TF (Foreshadow)	Intel SGX保護内容が読取の可能性
2018-08-14	CVE-2018-3646	L1TF (Foreshadow)	ゲストOS間でメモリ情報読取の可能性
2018-08-14	CVE-2018-3620	L1TF (Foreshadow)	OS内にて情報読取の可能性

## 話題になった脆弱性

### ◆ Spectre/Meltdown対策としてはやはりパッチの適用？

- 修正により様々な不具合も
  - ✓ OSのパフォーマンス低下 大きいもので20%程度低下 (Intel)
  - ✓ WindowsOSのBSOD、起動不可
  - ✓ マイクロコードパッチ適用のシステムで再起動発生 など

### ◆ すぐに対応した方がよいとは分かっているけど…

- 対応できる人が少ない (パッチ適用後の不具合含め)
- 自社への影響度や範囲の把握

# 脆弱性評価としてのCVSSの活用

## ◆ CVSS (Common Vulnerability Scoring System)

- 情報システムの脆弱性に対するオープンで汎用的な評価手法
- 脆弱性の深刻度を同一の基準の下で定量的に比較できる
- 現在はCVSS v2 / v3の値を併記

## ◆ CVSS v3の深刻度

深刻度	スコア
緊急	9.0 ~ 10.0
重要	7.0 ~ 8.9
警告	4.0 ~ 6.9
注意	0.1 ~ 3.9
なし	0

単純に赤色だったらヤバい

くらいの読み方しかしていませんでした…

# 脆弱性評価としてのCVSSの活用

- ◆ CVSS(v3) の仕組みをしらべる  
次の3つの基準で脆弱性を評価

## 基本評価値

脆弱性そのものの特性を評価する基準  
ベンダーや脆弱性を公表する組織が算出  
(攻撃の難易度、権限、ユーザ関与度、影響の評価...)

## 現状評価 基準

現在の深刻度を評価する基準  
脆弱性への対応状況に応じて変化  
(攻撃コードの存在、脆弱性対策可否...)

## 環境評価 基準

ユーザが脆弱性への対応を決めるために評価する基準  
ユーザ環境を含め最終的な深刻度を評価  
(基本評価値をユーザ環境に合わせて再評価)

## 脆弱性評価としてのCVSSの活用

◆例えば、CPUの脆弱性はどの程度のスコアだったのか(現時点の値)

公開日	CVE	呼称	CVSS v3 (NVD)
2018-01-03	CVE-2017-5753	Spectre (Variant 1)	5.6 (MEDIUM)
2018-01-03	CVE-2017-5754	Meltdown (Variant 2)	5.6 (MEDIUM)
2018-01-03	CVE-2017-5715	Spectre (Variant 3)	5.6 (MEDIUM)
2017-03-10	CVE-2018-9056	BranchScope	5.6 (MEDIUM)
2018-05-22	CVE-2018-3639	Spectre (Variant 3a)	5.5 (MEDIUM)
2018-05-22	CVE-2018-3640	SpectreNG (Variant 4)	5.6 (MEDIUM)
2018-07-10	CVE-2018-3693	Spectre1.1	5.6 (MEDIUM)
2018-08-14	CVE-2018-3615	L1TF (Foreshadow)	6.4 (MEDIUM)
2018-08-14	CVE-2018-3646	L1TF (Foreshadow)	5.6 (MEDIUM)
2018-08-14	CVE-2018-3620	L1TF (Foreshadow)	5.6 (MEDIUM)

# 脆弱性評価としてのCVSSの活用

◆ 深刻度の高い脆弱性に環境評価基準を適用してみる

CVE	概要	CVSS v3
CVE-2018-7600	Drupal リモートから任意のコードが実行可能	9.8(CRITICAL)

**9.8**  
(Critical)

基本評価基準

<b>攻撃元区分: Attack Vector (AV)</b> ネットワーク (N) 隣接ネットワーク (A) ローカル (L) 物理 (P)	<b>影響の想定範囲: Scope (S)</b> 変更なし (U) 変更あり (C)
<b>攻撃条件の複雑さ: Attack Complexity (AC)</b> 低 (L) 高 (H)	<b>機密性への影響: Confidentiality (C)</b> なし (N) 低 (L) 高 (H)
<b>攻撃に必要な特権レベル: Privileges Required (PR)</b> 不要 (N) 低 (L) 高 (H)	<b>完全性への影響: Integrity (I)</b> なし (N) 低 (L) 高 (H)
<b>利用者の関与: User Interaction (UI)</b> 不要 (N) 要 (R)	<b>可用性への影響: Availability (A)</b> なし (N) 低 (L) 高 (H)

# 脆弱性評価としてのCVSSの活用

- ◆環境評価基準を適用すると以下のように変化する
  - ・インターネットには公開しておらず、利用業務も限定的と仮定

環境評価基準 6.9 (Medium)

機密性の要求度: Confidentiality Requirement (CR)  
未評価 (X) **低 (L)** 中 (M) 高 (H)

完全性の要求度: Integrity Requirement (IR)  
未評価 (X) **低 (L)** 中 (M) 高 (H)

可用性の要求度: Availability Requirement (AR)  
未評価 (X) **低 (L)** 中 (M) 高 (H)

緩和策後の攻撃元区分: Modified AV (MAV)  
未評価 (X) ネットワーク **隣接ネットワーク** ローカル 物理

緩和策後の攻撃条件の複雑さ: Modified AC (MAC)  
未評価 (X) 低 高

緩和策後の攻撃に必要な特権レベル: Modified PR (MPR)  
未評価 (X) 不要 低 高

緩和策後の利用者の関与: Modified UI (MUI)  
未評価 (X) 不要 要

自組織にあわせて影響度を再評価することで、優先度をつけて対応できる

## 運用段階における脆弱性管理

◆ 突然発表される脆弱性に対してどうしても動きが遅くなりがち…

1. 組織が利用しているソフトウェア構成を把握しておく
2. 最新の脆弱性情報を入手し評価する
  - Japan Vulnerability Notes (<http://jvn.jp/>)
  - 各ソフトウェアベンダページ
  - セキュリティベンダブログページ
3. 定期的な脆弱性診断を行う
  - 脆弱性検出と対処が完了したことの確認

ツールあれこれ

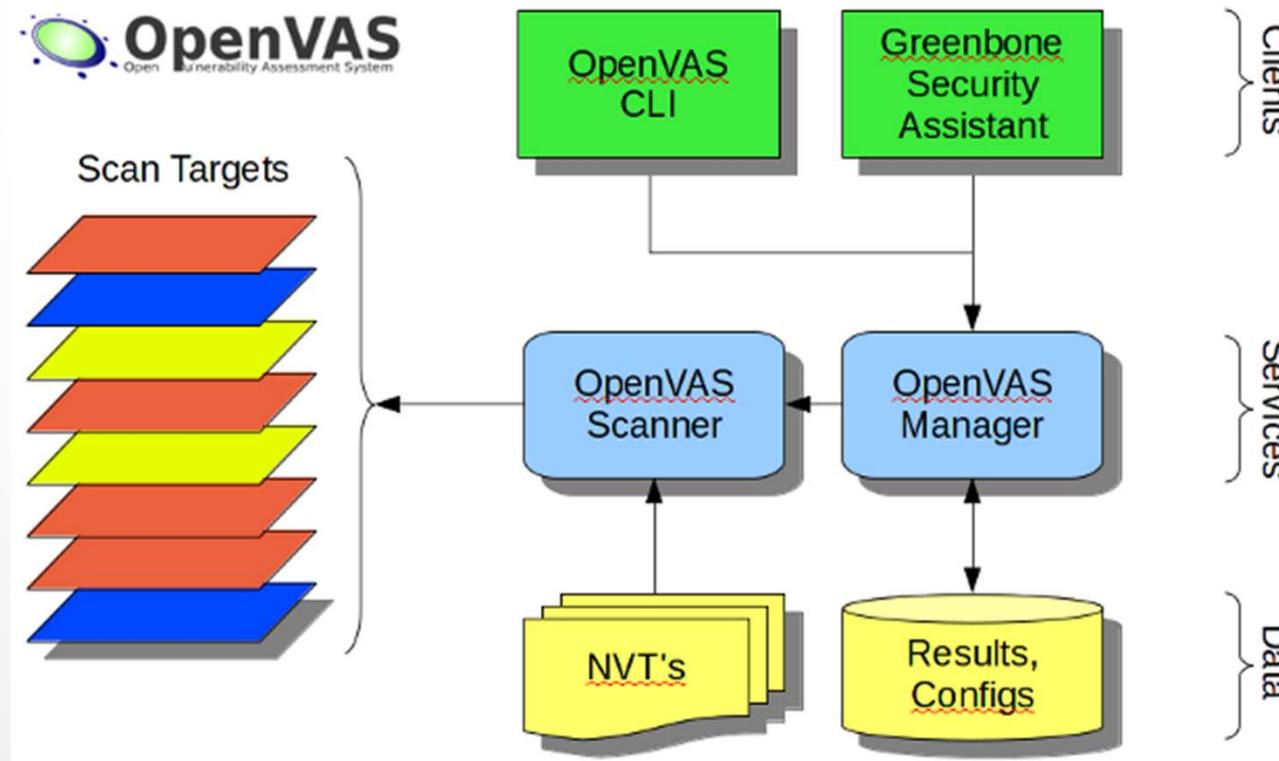
...

定番～試してみたかったもの

# 脆弱性調査におけるツール

## ◆オープンソースな脆弱性検出

- OpenVAS
  - Linux/Windows/ESXi/CiscoOSを対象とした脆弱性スキャナ
  - SSH/SMBを利用したエージェントレススキャン対応
  - 定期実行しEmailの通知が可能





# 脆弱性調査におけるツール

## ◆OpenVAS スキャン結果一覧

 **Dashboard**   Scans   Assets   SecInfo   Configuration   Extras   Administration   Help

 **Report: Results (148 of 727)**

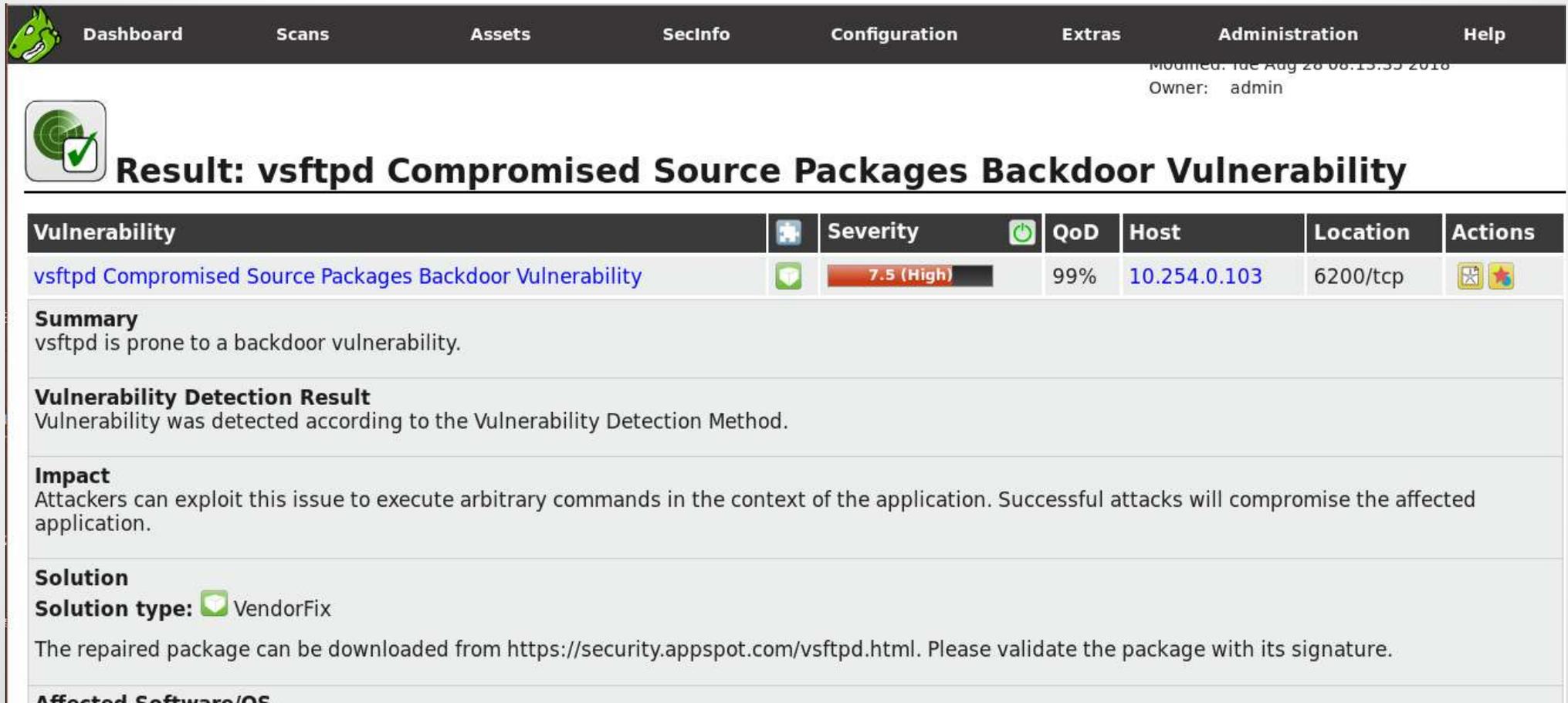
ID: 4a8ece83-43ad-4c17-9386-4151aa0588aa  
Modified: Tue Aug 28 08:17:18 2018  
Created: Mon Aug 27 09:23:43 2018  
Owner: admin

1 - 100 of 148

Vulnerability	Severity	QoD	Host	Location	Actions
Check for rexecd Service	10.0 (High)	80%	10.254.0.103	512/tcp	 
Pidgin MSN SLP Packets Denial Of Service Vulnerability (Linux)	10.0 (High)	80%	10.254.0.103	general/tcp	 
Ubuntu Update for samba USN-1423-1	10.0 (High)	97%	10.254.0.103	general/tcp	 
OS End Of Life Detection	10.0 (High)	80%	10.254.0.103	general/tcp	 
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	10.254.0.103	80/tcp	 
Ubuntu Update for apt USN-1215-1	10.0 (High)	97%	10.254.0.103	general/tcp	 
Ubuntu Update for freetype USN-1403-1	10.0 (High)	97%	10.254.0.103	general/tcp	 
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC)	10.0 (High)	100%	10.254.0.103	general/tcp	 
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03	10.0 (High)	100%	10.254.0.103	general/tcp	 
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 04	10.0 (High)	100%	10.254.0.103	general/tcp	 

# 脆弱性調査におけるツール

## ◆OpenVAS 検出脆弱性詳細



The image shows the OpenVAS web interface. At the top, there is a navigation bar with links for Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. Below the navigation bar, the main content area displays a vulnerability report. The report title is "Result: vsftpd Compromised Source Packages Backdoor Vulnerability". The report is presented in a table format with columns for Vulnerability, Severity, QoD, Host, Location, and Actions. The vulnerability details include a summary, detection result, impact, and solution.

Vulnerability	Severity	QoD	Host	Location	Actions
<a href="#">vsftpd Compromised Source Packages Backdoor Vulnerability</a>	7.5 (High)	99%	10.254.0.103	6200/tcp	

**Summary**  
vsftpd is prone to a backdoor vulnerability.

**Vulnerability Detection Result**  
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**  
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

**Solution**  
**Solution type:** VendorFix  
The repaired package can be downloaded from <https://security.appspot.com/vsftpd.html>. Please validate the package with its signature.

**Affected Software/OS**

# 脆弱性調査におけるツール

## ◆侵入テストツール

- Metasploit
  - ✓ 侵入テスト、脆弱性スキャンに利用されるソフトウェア
  - ✓ 脆弱性スキャナで検出された脆弱性の検証等に利用
  - ✓ Kali LinuxにCommunityエディションが同梱
  - ✓ あくまで侵入テスト用のツール

※Kali Linux… 侵入テストを目的としたLinuxディストリビューション

## その他の公開ツール

### ◆情報収集の手法として

- OSINT(オシント)という言葉
  - ✓ オープン・ソース・インテリジェンス ( Open Source INTelligence )
  - ✓ 一般公開されている情報を情報源とした、情報収集
    - 報道、インターネット、書籍等を対象として収集
    - 最近ではセキュリティ分野でも利用される

# その他の公開ツール

## ◆情報収集サイト

- Shodan

<https://www.shodan.io/>

インターネット接続機器の情報データベース

自社の公開サーバがインターネットからどのように見られているかを確認できる。不適切な公開サーバへの早期対応に利用できる。

同じようなサービスとしてCensysがある

The screenshot displays the Shodan search engine interface. At the top, there is a navigation bar with the Shodan logo and a search bar. Below the search bar, there are several tabs: Exploits, Maps, Share Search, Download Results, and Create Report. The main content area shows search results for a specific IP address. On the left, there is a section for 'TOTAL RESULTS' showing 37,559 results, and a 'TOP COUNTRIES' section with a world map highlighting the United States. In the center, there is a section for 'Added on 2018-08-29 05:37:38 GMT' with a flag for the United States, Seattle, and a list of technologies including php. On the right, there is a section for 'SSL Certificate' with details such as Issued By, Issued To, and Expires. Below the SSL Certificate section, there is a section for 'Supported SSL Versions' showing TLSv1.2. The interface is dark-themed with white text.

## その他の公開ツール

### ◆情報収集サイト

- Virustotal

<https://www.virustotal.com/>

疑わしいファイルやURLを検査してくれるオンラインサービス

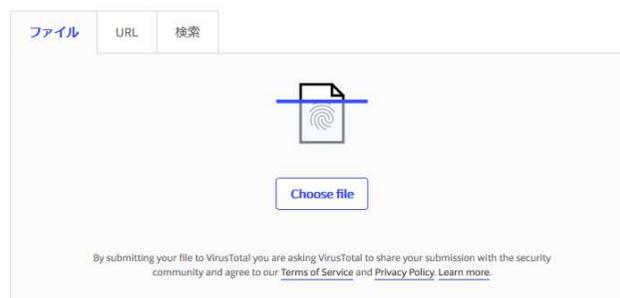
複数のウィルスチェックエンジンでファイルチェックを行う

同じようなサービスとしてHybrid Analysisというサービスもある

(オンラインサンドボックス)



Analyze suspicious files and URLs to detect types of malware,  
automatically share them with the security community.



# その他の公開ツール

## ◆OSINTツール

- Maltego

- ✓ インターネット上の情報を収集しそれらの関連性を分析できるツール
- ✓ ドメイン、IP、組織、人、E-mailなど
- ✓ 各種サービスのAPIを利用して連携が可能（Shodan/Virustotal）



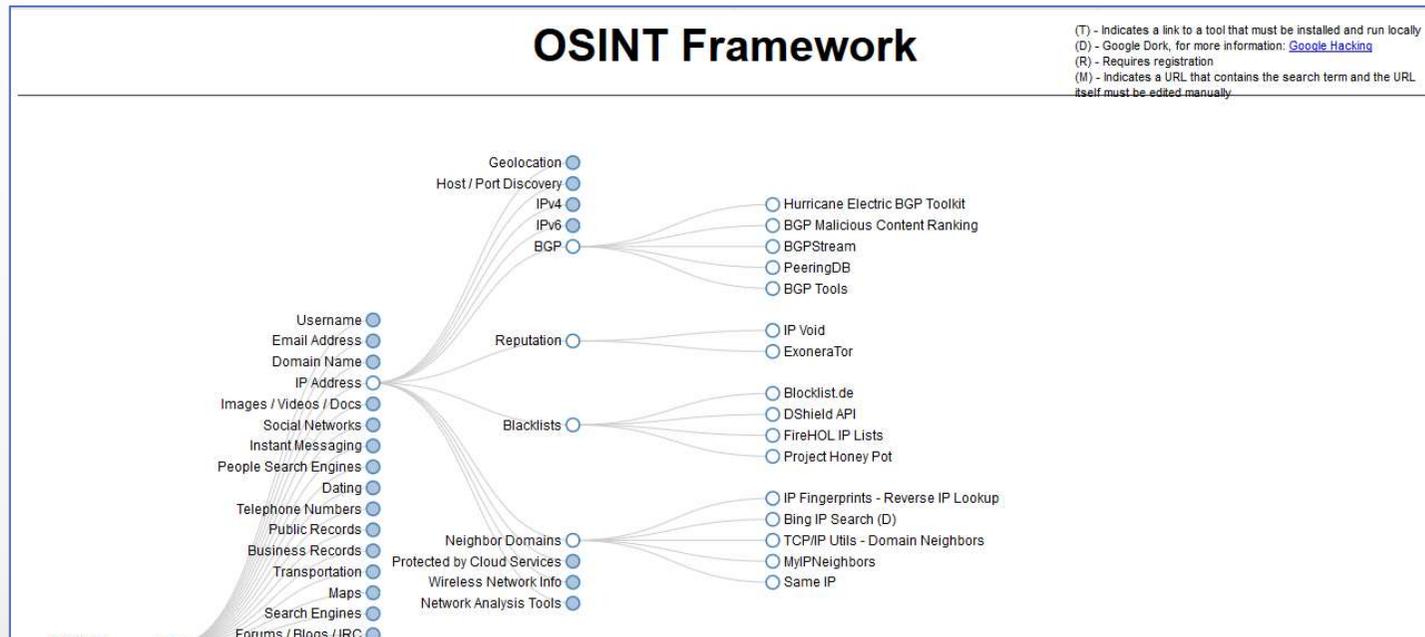
# その他の公開ツール

## ◆ OSINT ツール

- OSINT Framework

- <http://osintframework.com/>
- 情報収集のリンク集
- カテゴリ毎に分類されている

IP address → Blacklist → 情報収集サイトリスト



# まとめ

- ◆ 攻撃(マルウェア・フィッシング)の手法は日々変化
- ◆ でも悪用されるツールはあまり変わっていない
  - メール、脆弱性
- ◆ 脆弱性管理もツール(CVSS/スキャナ)を活用して効率的に
- ◆ 不適切な情報が公開されていないかOSINTしてみる
  - 自分が収集できる情報→他人も同じように情報収集できる
- ◆ 各人のセキュリティ意識（新しい脅威の認識）も大切

# おわり



ありがとうございました。