脆弱性スキャナによる対策支援の課題

フューチャーアーキテクト株式会社
Technology Innovation Group
神戸　康多

自己紹介

- 神戸康多（かんべこうた）
- フューチャーアーキテクト株式会社所属
- サウナが趣味（週2）
- Linux/FreeBSD向け脆弱性スキャナVuls作者 GitHub

本日のテーマ

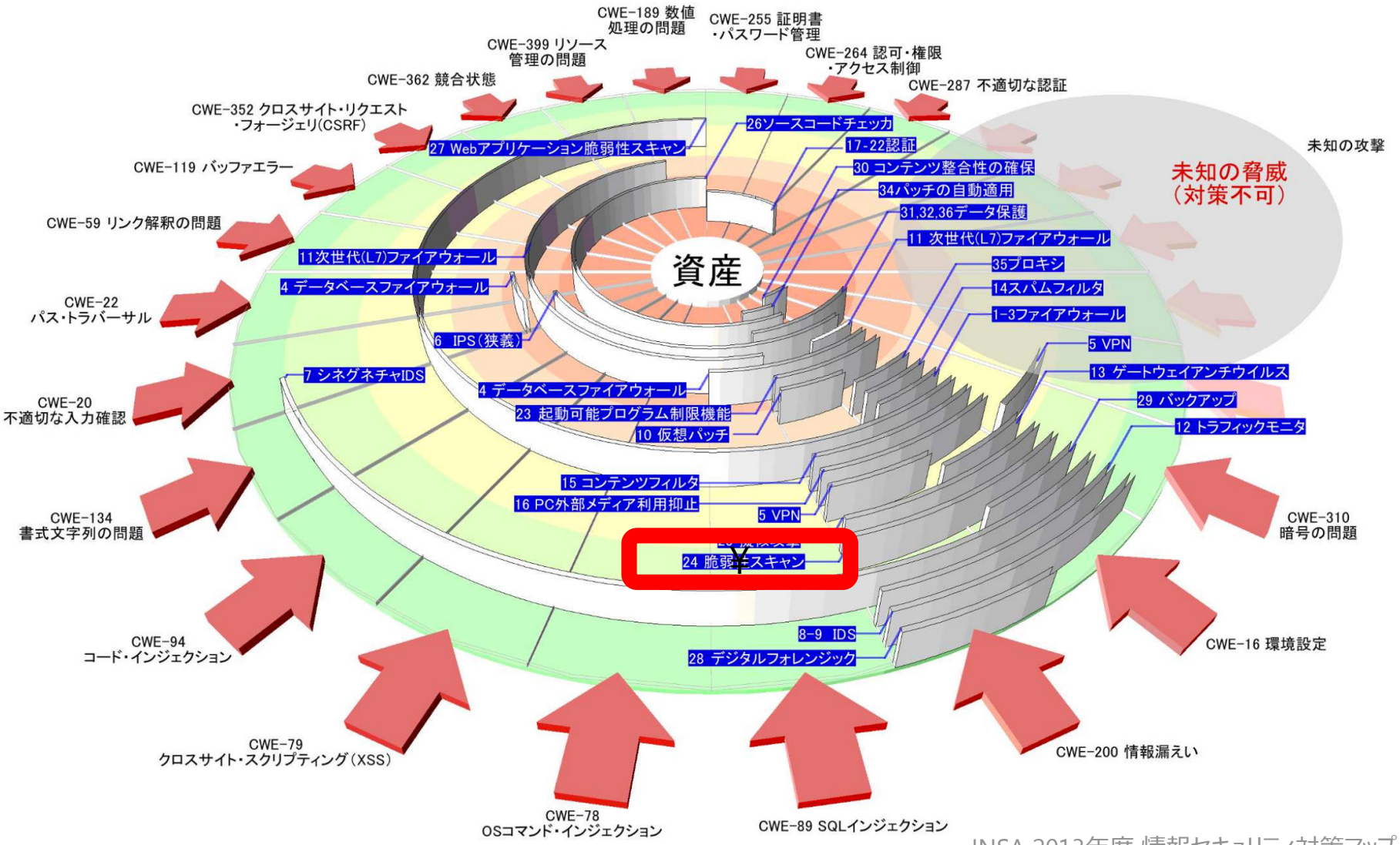
I. IPS/IDS/Antivirusではカバーできない脆弱性を紹介。
Linuxサーバでのパッケージ、ライブラリなどのアップデートの重要性を知る。

II. 人力での脆弱性対策の大変さを知る。

III. OSSの脆弱性スキャナVulsを用いて、**楽に、漏れなく、無料で**出来る脆弱性対策の一例を紹介する。

本日の対象範囲

- Linuxシステムの、24. 脆弱性スキャンが対象



JNSA 2013年度 情報セキュリティ対策マップより

IDS/IPS, Antivirusでは防げない脆弱性も存在する

- Dirty Cow (CVE-2016-5195)
- SSH接続可能な一般ユーザがRootへ権限昇格可能な脆弱性

- 内部犯行可能
  - ✓運用ルールで一般ユーザ、Rootユーザを分けていても、数秒で一般ユーザがRootユーザに権限昇格可能

- SSHで接続可能なユーザであれば誰でも簡単に実行可能
  - ✓PoCが沢山公開されている
  - ✓https://dirtycow.ninja/
- PoCをカスタマイズすればIDS/IPS, Antivirusでの検知は難しい

Linuxサーバもソフトウェアアップデートは必要

OSパッケージ、ライブラリアップデート方法は2種類

- プロダクション環境は**手動アップデート**を採用するケースが多い

自動アップデート

メリット

- **手間なし**
- **漏れなし**

デメリット

- **サービスダウン**の可能性
  - ✓ミドルウェア、ライブラリのAPIが変更される可能性

手動アップデート

メリット

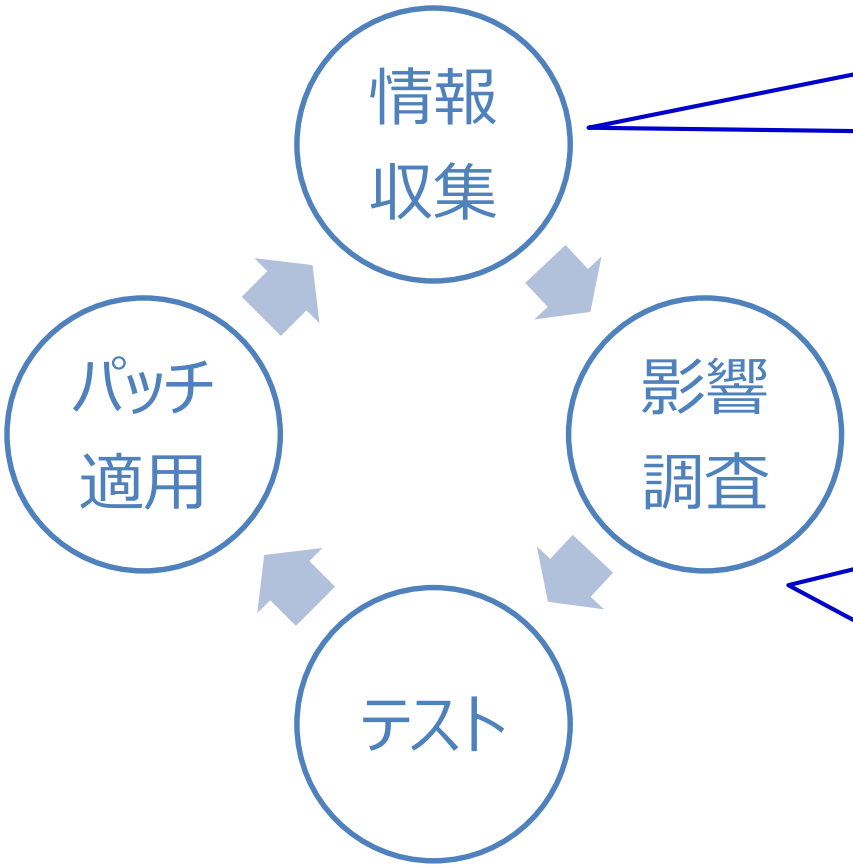
- 事前に**テスト可能**

デメリット

- 脆弱性情収集、影響調査の**コスト大**
- **漏れる**可能性あり

手動アップデート運用での脆弱性対策は大変

- 日々公開される脆弱性情報を追い続ける必要がある
- システム運用者は以下のサイクルを日々回している



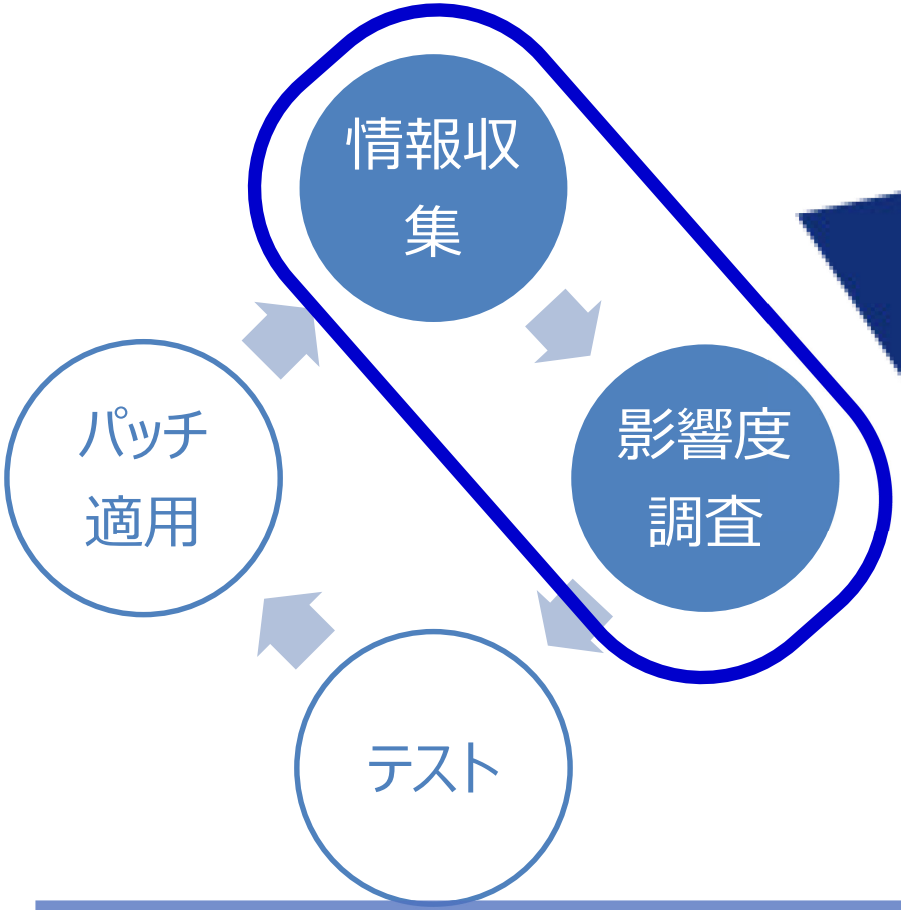
- 約7千件/年の脆弱性
- 全部チェックするのは大変
- 漏れたら放置されてしまう

- 大規模、カオスな環境は大変
- パッケージ、ライブラリ、N/W機器
- 漏れはないか？

毎日の大変な作業は自動化すべき

Vulsは脆弱性情報の収集、影響度調査を自動化する

- 日々の情報収集、影響度調査を自動化
- パッチ適用漏れによる脆弱性の放置を防ぐ



Vuls

私が作りました

Vulsを作った経緯

100台規模のLinux環境を運用した経験より…

- Ubuntu, CentOS, Debianなどディストリビューション、バージョンもバラバラ。Ruby, Javaなど複数の言語

人力での脆弱性対策が大変だった

- 日々公開される脆弱性情報を全てチェック
- 影響調査
- 見逃してないか？調査結果は正しいか？
- またOpenSSLか…

Vulsは怒りと憎しみから生まれた

Vuls概要

- 潜在する脆弱性と該当サーバを可視化
- 定期実行で対策漏れがなくなる

Vulsの特徴

- 世界で注目のOSS
- エージェントレス
- 日本語レポート
- OSパッケージ、言語ライブラリ、N/W機器に対応
- 対象OSが幅広い
- プラットフォーム非依存
- WebUI

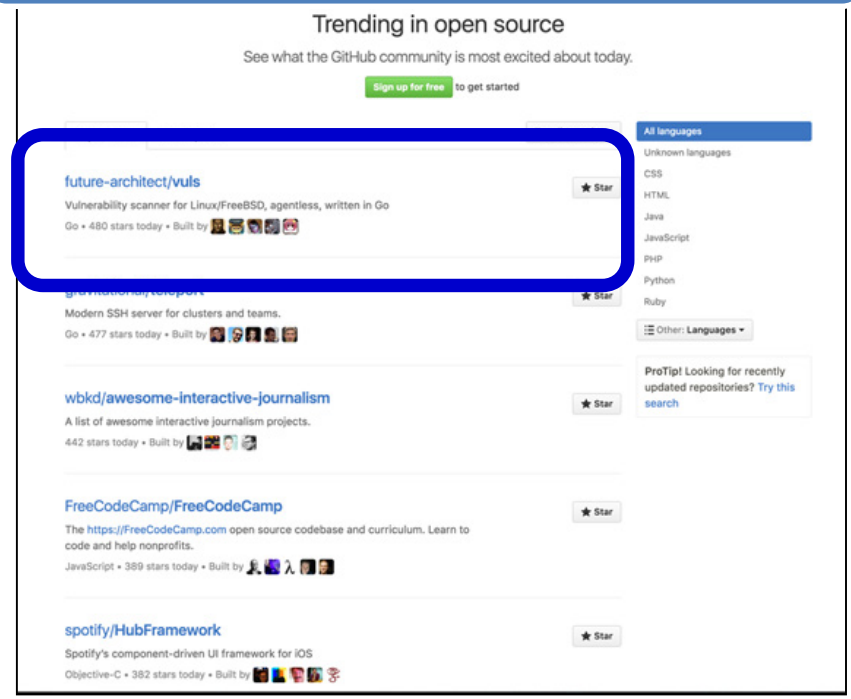
Vulsの特徴　世界で注目のOSS

- **世界で注目のOSS**
- エージェントレス
- 日本語レポート
- OSパッケージ、言語ライブラリ、N/W機器に対応
- 対象OSが幅広い
- プラットフォーム非依存
- WebUI

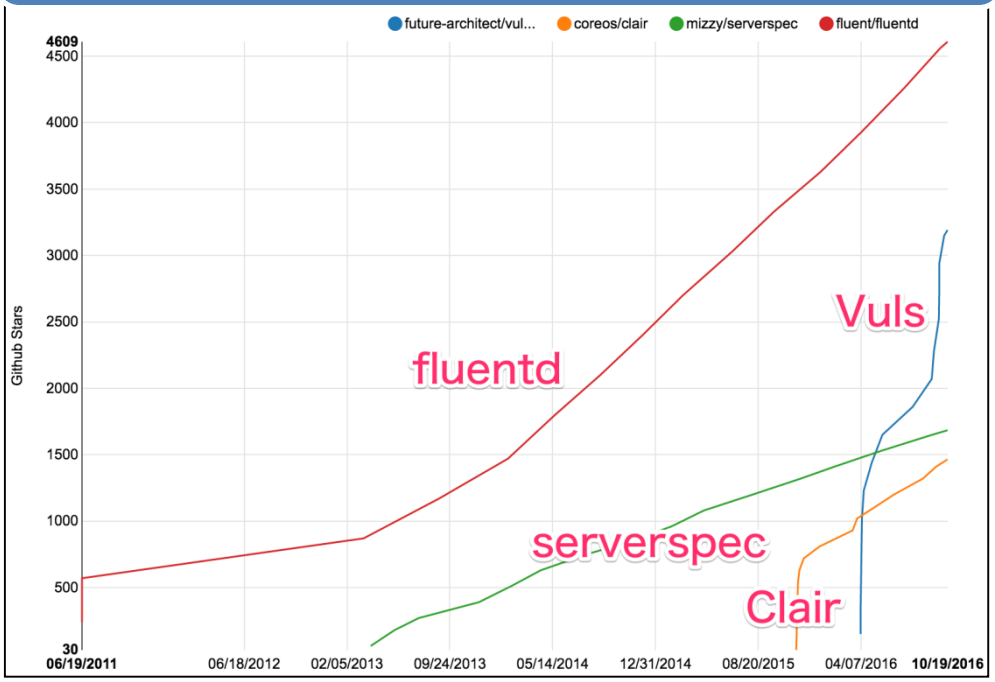
Vulsの特徴　世界で注目のOSS

- 2016/4/1 GitHub公開
  - ✓ https://github.com/future-architect/vuls
- 公開直後から世界中で話題になり、2016/10/1にGitHubスター獲得ランキング全言語1位に

世界1位



スター数は順調に増加



Vulsの特徴　エージェントレス

- 世界で注目のOSS
- **エージェントレス**
- 日本語レポート
- OSパッケージ、言語ライブラリ、N/W機器に対応
- 対象OSが幅広い
- プラットフォーム非依存
- WebUI

Vulsの特徴　エージェントレス

セットアップが簡単

- 1台のみでよい

既に動いている本番環境に導入しやすい

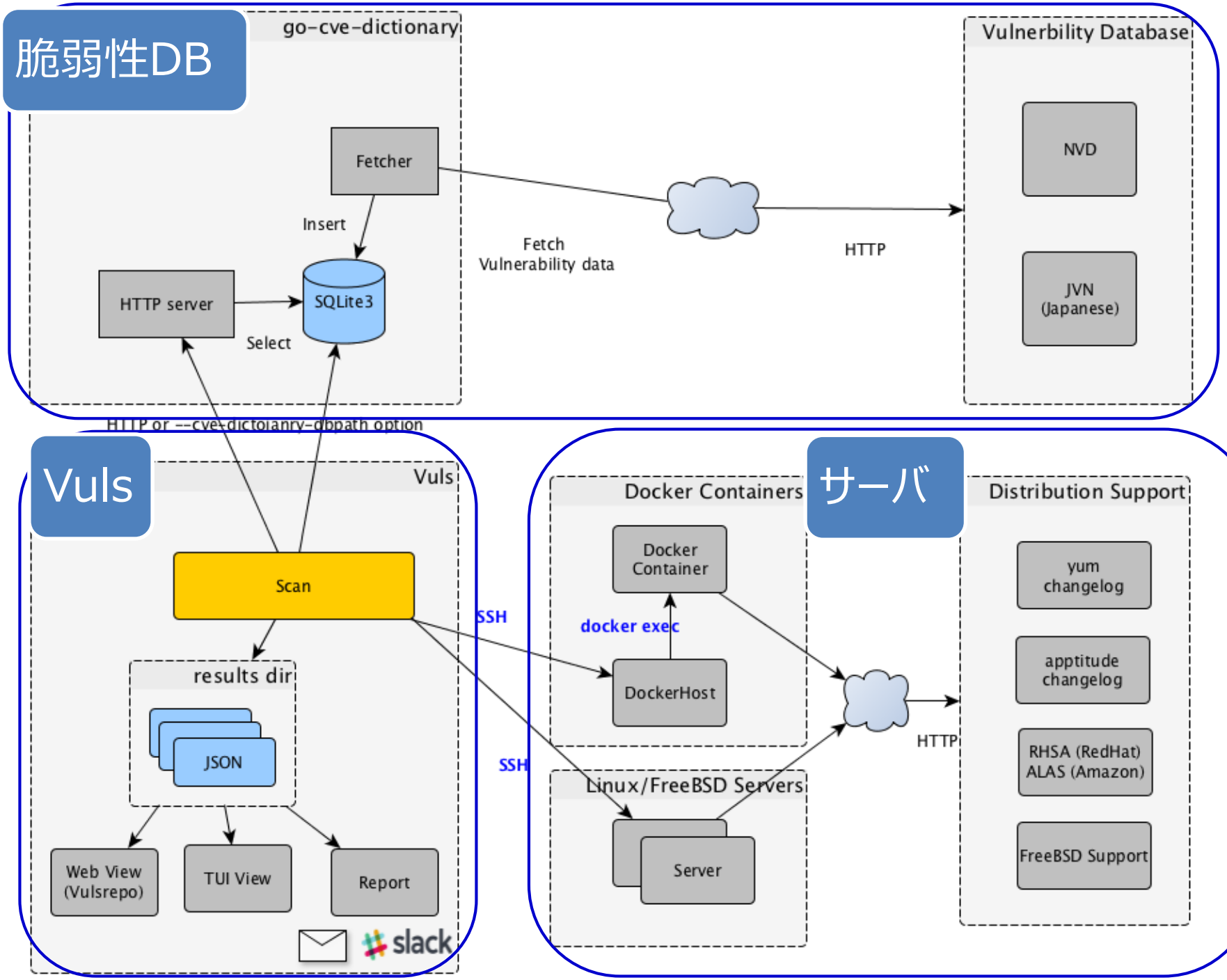
- 既存本番環境にエージェントを入れたくない/入れられないケースでも導入可能

大規模環境向き

- Vuls本体のデプロイ、アップデートが簡単

Vulsサーバから対象サーバにはSSHで接続

- 対象サーバ上でコマンドを発行（ホワイトボックス）
- 非破壊テスト型スキャナ

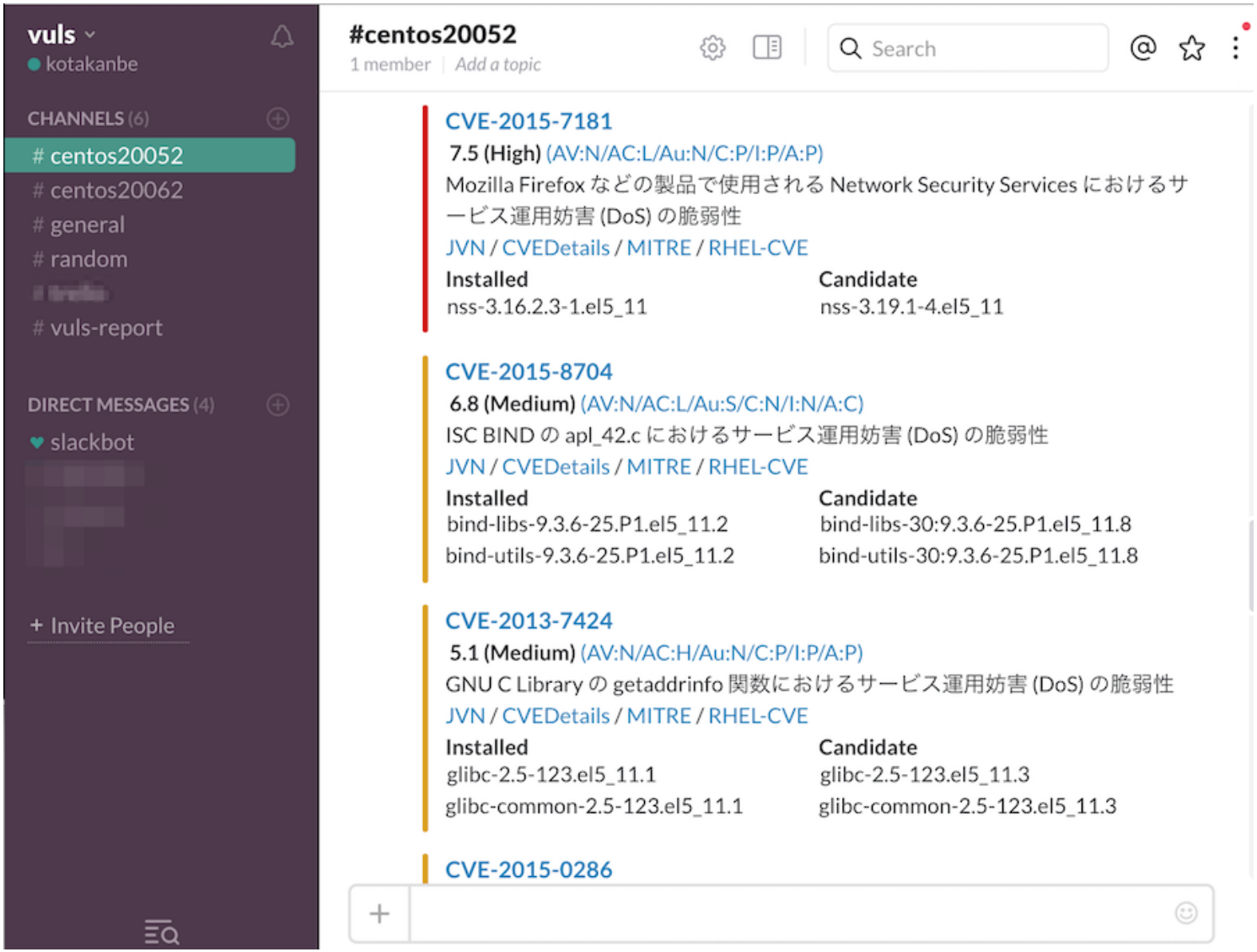

脆弱性DB
go-cve-dictionary
Fetcher
Insert
HTTP server
SQLite3
Select
Fetch
Vulnerability data
HTTP
Vulnerbility Database
NVD
JVN
(Japanese)
HTTP or --cve-dictionary-dbpath option
Vuls
Vuls
Scan
results dir
JSON
Web View
(Vulsrepo)
TUI View
Report
slack
SSH
SSH
サーバ
Docker Containers
Docker
Container
docker exec
DockerHost
Linux/FreeBSD Servers
Server
HTTP
Distribution Support
yum
changelog
apptitude
changelog
RHSA (RedHat)
ALAS (Amazon)
FreeBSD Support

Vulsの特徴　日本語レポート

- 世界で注目のOSS
- エージェントレス
- **日本語レポート**
- OSパッケージ、言語ライブラリ、N/W機器に対応
- 対象OSが幅広い
- プラットフォーム非依存
- WebUI

Vulsの特徴　日本語レポート

- Slack, E-mail通知に対応（2016/11時点）



Vulsの特徴　OSパッケージ、言語ライブラリ、N/W機器に対応

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

プラットフォーム非依存

WebUI

Vulsの特徴　OSパッケージ、言語ライブラリ、N/W機器に対応

- CPE登録済みのものであれば脆弱性の検知が可能
- 参考: IPA共通プラットフォーム一覧CPE概説
  - ✓ https://www.ipa.go.jp/security/vuln/CPE.html

Vulsの設定ファイル　RoR4.2.1を定義した例

```
[servers]

[servers.172-31-4-82]
host         = "172.31.4.82"
user         = "ec2-user“
keyPath      = “/home/username/.ssh/id_rsa"
cpeNames = [
    "cpe:/a:rubyonrails:ruby_on_rails:4.2.1",
]
```

Vulsの特徴　OSパッケージ、言語ライブラリ、N/W機器に対応

CPEの調べ方その１

- NVDで検索する
- https://web.nvd.nist.gov/view/cpe/search

CPEの調べ方その2

- NVDでの検索は面倒という方のためのツール
- ターミナルでインクリメンタル検索可能
- https://github.com/kotakanbe/go-cpe-dictionary

それでも面倒という方は…

Vulsの特徴　OSパッケージ、ライブラリ、N/W機器にも対応

- プログラミング言語ライブラリ用脆弱性スキャナ OWASP Dependency-Checkと連携する方法
- 利点
  - ✓Vulsの設定ファイルにライブラリのCPEを定義しなくてよい
  - ✓バージョンアップ時にVuls設定ファイルの変更不要
  - ✓Vulsと連携すると日本語でのレポートが可能

Vulsの設定ファイル

```
[servers]
[servers.172-31-4-82]
host         = "172.31.4.82"
user         = "ec2-user"
keyPath      = “/home/username/.ssh/id_rsa"
dependencyCheckXMLPath = "/tmp/report.xml“
```

Vulsの特徴　対象OSが幅広い

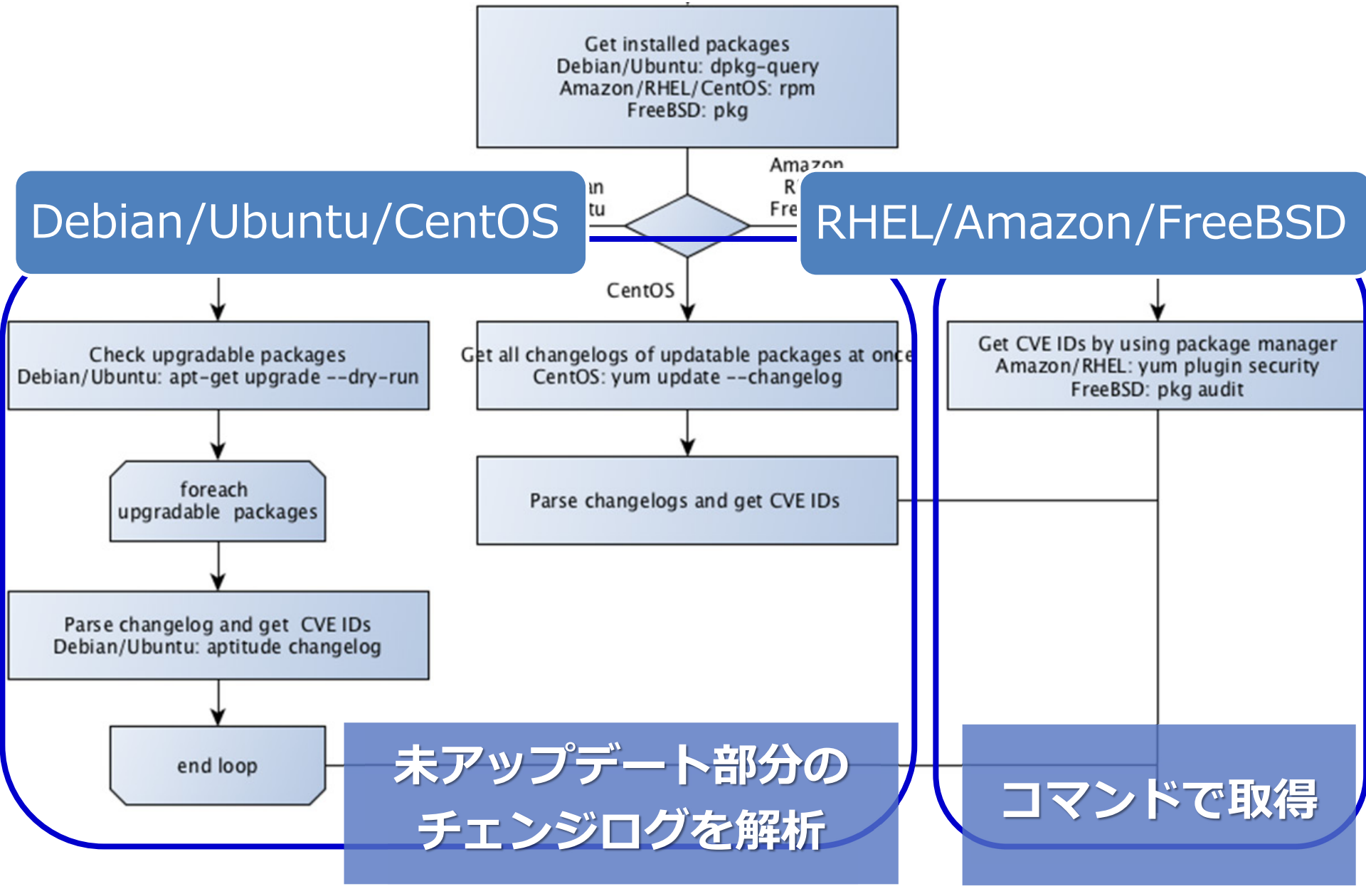
- 世界で注目のOSS
- エージェントレス
- 日本語レポート
- OSパッケージ、言語ライブラリ、N/W機器に対応
- **対象OSが幅広い**
- プラットフォーム非依存
- WebUI

Vulsの特徴　対象OSが幅広い

- Linux系OS, FreeBSDの脆弱性をスキャン可能
- サポート期間中のものが対象

Redhat系	RHEL	(5), 6, 7　※ RHEL5は対応予定
	CentOS	5, 6, 7
	Amazon Linux	全バージョン
Debian系	Debian	7, 8
	Ubuntu	12, 14, 16
BSD	FreeBSD	10, 11

OSごとのスキャンフロー



Vulsの特徴　対象OSが幅広い - チェンジログ解析の理由

- 脆弱性情報には該当するパッケージ、バージョン情報が含まれる。実装前はバージョンの比較で実現できるだろうと思っていたが、以下の通りバージョン比較での実現は不可能であることを悟る

Ubuntuパッケージ、バージョンの例	
locales	2.13+git20120306-21
login	1:4.1.5.1-1.1ubuntu7
lsb-base	9.20160110
make	4.1-6
mawk	1.3.3-17ubuntu2
mime-support	3.59ubuntu1
multiarch-support	2.21-0ubuntu5

試行錯誤の末、チェンジログの解析を思いつく

Vulsの特徴　プラットフォーム非依存

- 世界で注目のOSS
- エージェントレス
- 日本語レポート
- OSパッケージ、言語ライブラリ、N/W機器に対応
- 対象OSが幅広い
- **プラットフォーム非依存**
- WebUI

Vulsの特徴　プラットフォーム非依存

オンプレ、クラウドどこでも動作

- SSH接続できればスキャン可能
- Vuls本体はGo言語製のプログラム

Dockerコンテナの脆弱性もスキャン可能

- DockerホストにSSH接続
  コンテナへはdocker execでコマンド発行
- Dockerコンテナには SSHデーモンを起動しなくてもよい

Vulsの特徴　WebUI

- 世界で注目のOSS
- エージェントレス
- 日本語レポート
- OSパッケージ、言語ライブラリ、N/W機器に対応
- 対象OSが幅広い
- プラットフォーム非依存
- **WebUI**

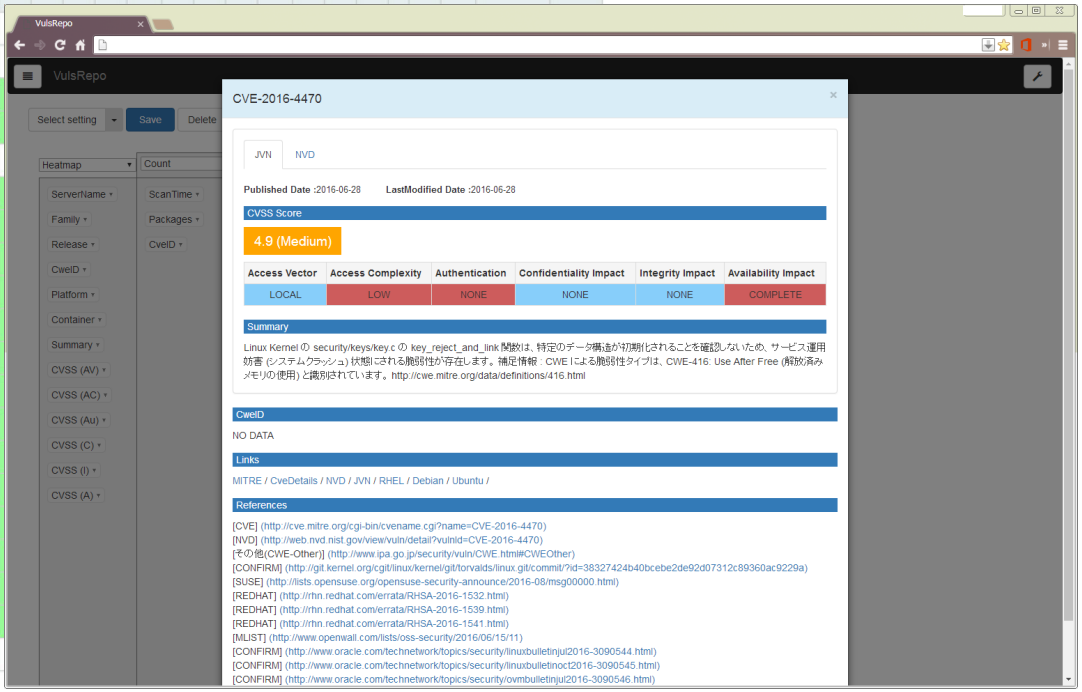
Vulsの特徴　WebUI

VulsRepo

- Exelのピボットテーブルのようにスキャン結果の分析が可能
- https://github.com/usiusi360/vulsrepo

CVSS Severity ▾ CVSS Score ▾

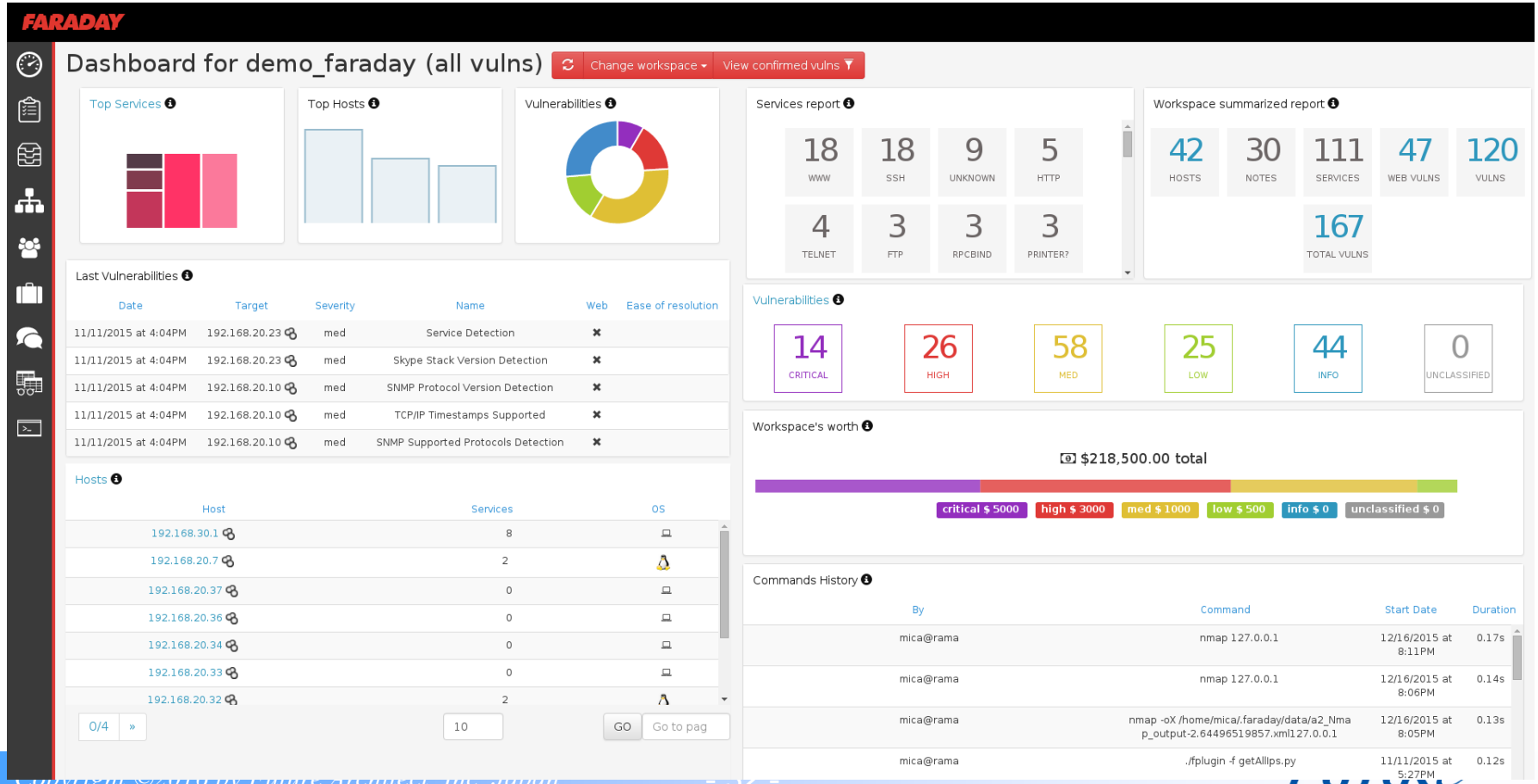
		CVSS Severity	Low								Medium														High									Unknown	Totals
		CVSS Score	1.7	1.9	2.1	2.6	2.8	3.3	3.5	3.6	4	4.3	4.4	4.6	4.7	5	5.1	5.5	5.8	6.1	6.2	6.4	6.5	6.8	6.9	7.1	7.2	7.5	7.6	7.8	8.5	9	9.3	10	Unknown	
ServerName	Container																																			
	centos_5.1			2	6	13		8		4	2	82		8	2	129	20		30																	
	centos_5.2			3	10	16		8		6	4	82	2	12	2	159	15		24																	
	centos_5.4			1		4		4			2	22		2	1	39	7		4																	
	centos_5.6			2		4		3			1	19		1		31	4		2																	
	centos_5.7			4		6		1			4	35		1		56	5		6																	
	centos_5.8			2		4					4	29				39	3		6																	
	centos_5.9			1		2					1	14				14	3		2																	
	centos_5.10											13				13	3																			
	centos_5.11											12				16	2																			
localhost	centos_6.0			11	2	30					10	216		1		354			17																	
	centos_6.1			7	2	18					6	132		1		210			13																	
	centos_6.2			7	2	18					6	117		1		173			13																	
	centos_6.3			7	2	18					6	118		1		173			13																	
	centos_6.4			4	2	4					4	81				122			9																	
	centos_6.5			1	2	1						25				53			5																	
	centos_6.6			1	2	1						23				44			3																	
	centos_6.7			1	1	1						11				23			3																	
	centos_6.8					2										10			2																	
	None		2	2	4	3	1		6		13	11		2		27		3	2																	
	Totals		2	56	35	145	1	24	6	10	63	1,042	2	30	5	1,685	62	3	154																	



Vulsの特徴　WebUI

Faraday

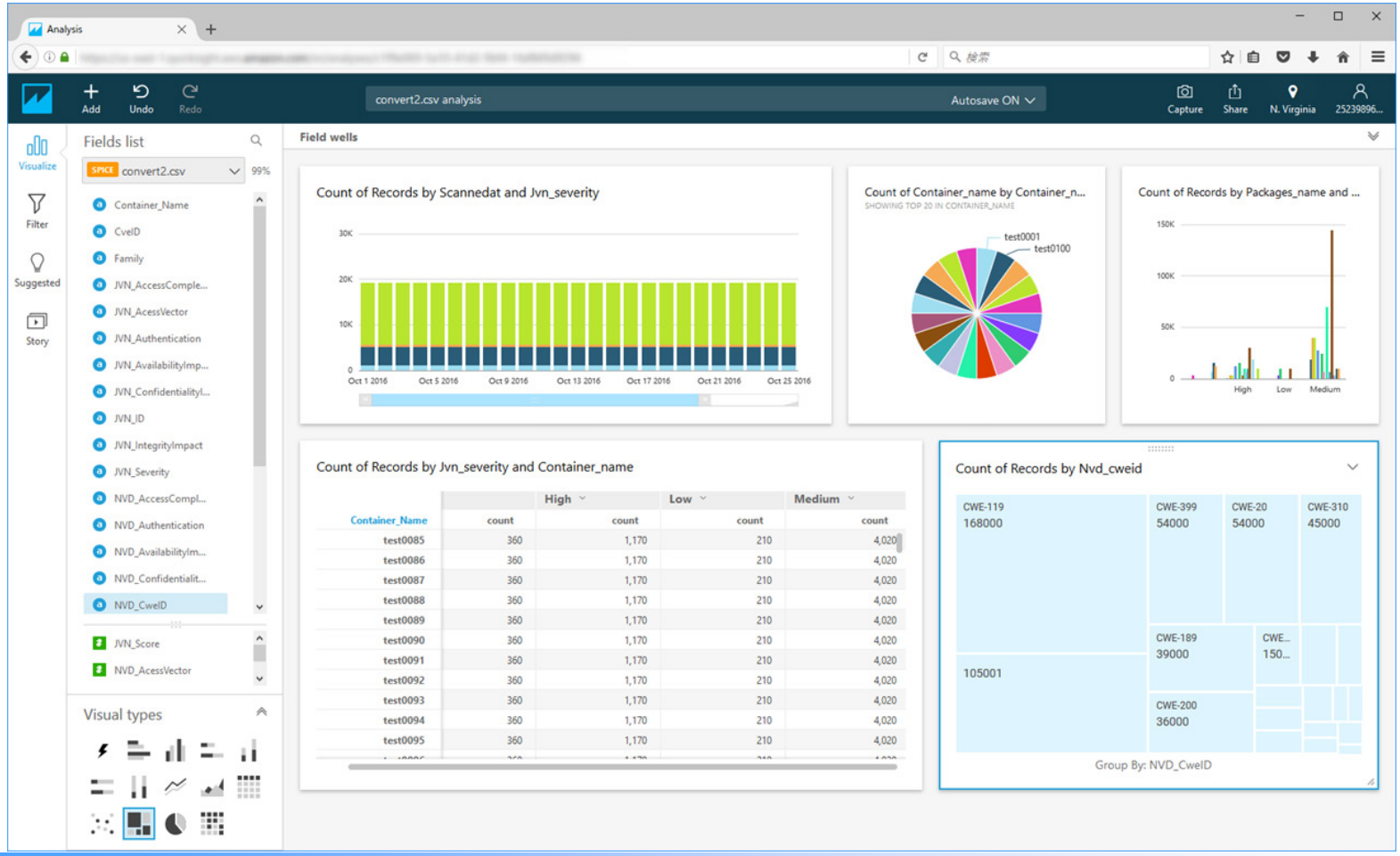
- 現在、Vulsプラギン作成中
- https://github.com/infobyte/faraday



Vulsの特徴　WebUI

AWS Quicksight

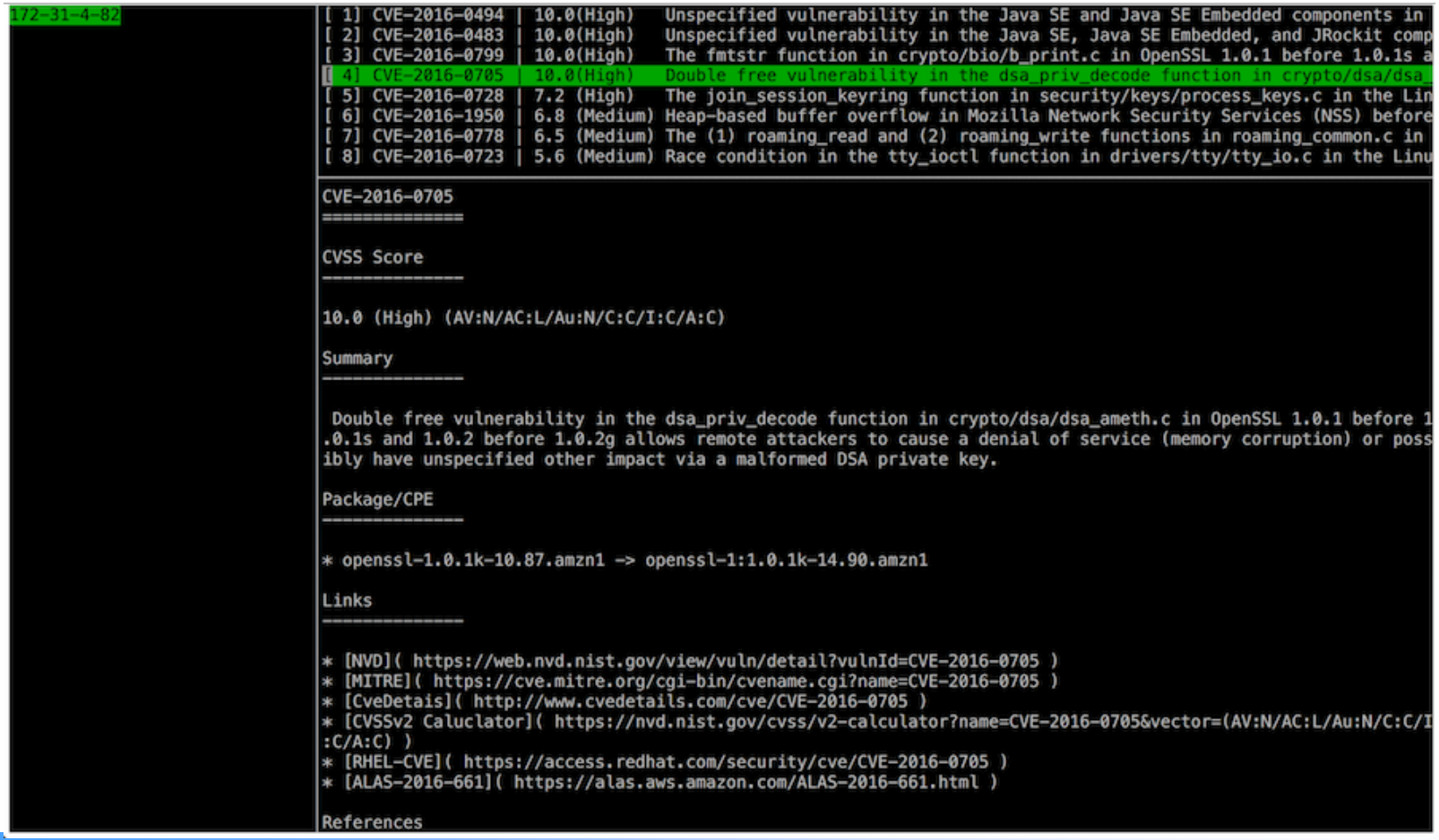
- AWSのBIツールを使ってダッシュボードを作った例



Vulsの特徴　TUI

Vuls TUI

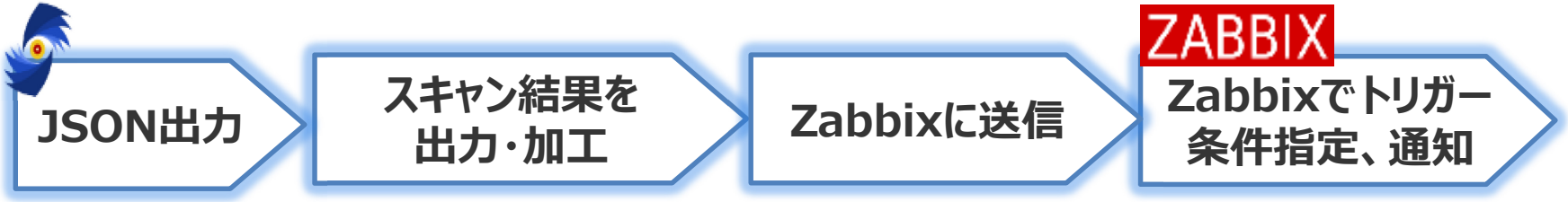
- ターミナルUIがVuls本体に付属している



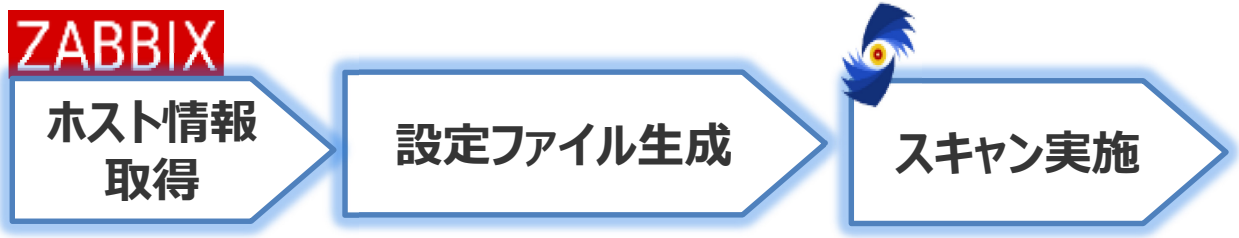
他ツールとの連携

Zabbixとの連携

Qiita:脆弱性スキャナVulsのスキャン結果をZabbixへ連携しアラート通知する



Qiita:Zabbixに登録されたホスト情報を脆弱性スキャナVulsへ自動連携する



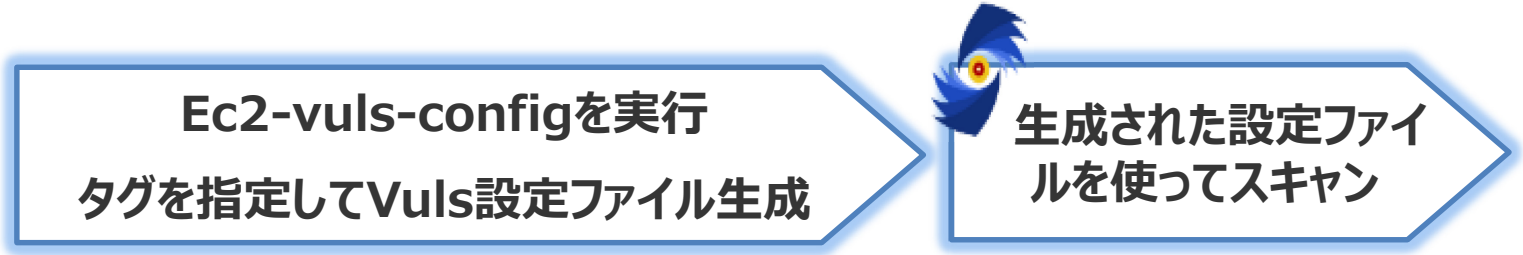
他ツールとの連携

AWSとの連携

Qiita:脆弱性スキャナVulsでEC2をスキャンし脆弱性深刻度をタグ付け

Name	vuls	インスタンスタ	アベイラビリティ	インスタンスの	ステータスチェ	アラームのステ
amazon1	High	t2.nano	ap-northeast-1b	running	2/2 のチェッ..	なし

EC2のVulsスキャンをほんの少し便利にするツール「ec2-vuls-config」

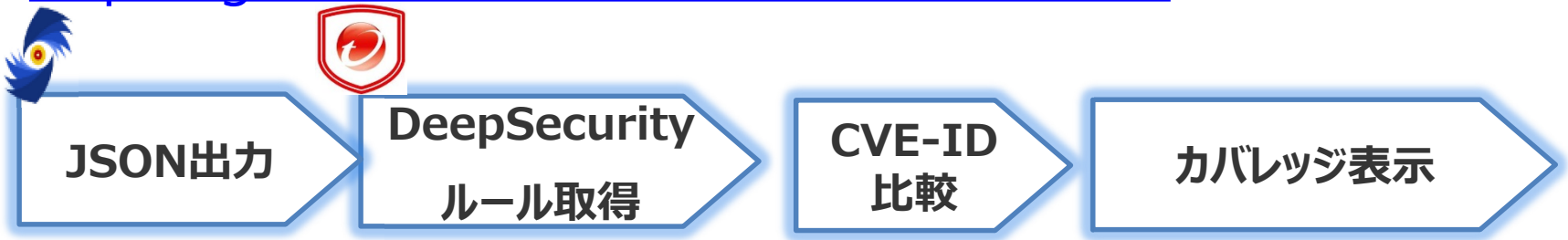


他ツールとの連携

Redmineと連携した脆弱性対策のワークフロー

Trend Micro Deep Security ルールのカバレッジ表示

https://github.com/kn0630/vulssimulator_ds



活発な開発

- 半年間で 182 個の機能拡張、バグフィックス(2016/11/15)
  - ✓ FreeBSD Support by justyntemme #90
  - ✓ High Speed Scaning on CentOS by ti-ga #138
  - ✓ High speed data fetch from JVN by kotakanbe #21
  - ✓ High speed scanning on Ubuntu(20x Faster on Ubuntu, 4x Faster on Debian) by kotakanbe #172
  - ✓ Setup Vuls using DockerHub by matsuno #223
  - ✓ Add support for reading CVE data from MySQL. by oswell #225
  - ✓ Integrate OWASP Dependency Check #232
  - ✓ …

Vuls vs OpenVAS vs AWS Inspector

Qiita: Vuls・OpenVAS・Amazon Inspectorを徹底比較

今後の課題

スキャンの検知精度の向上

- 現状Ubuntu/Debian/CentOSはチェンジログを解析
  チェンジログの記述次第で検知漏れの可能性があるため、
  バージョン比較での検知ロジックを併用し精度を向上させる

大規模環境対応

- 数千台、数万台規模を想定したチューニング

他の脆弱性スキャナとの連携

- 設定、状態までを考慮した賢いスキャン
- サーバ設定Audit系
- WordPressプラギン用脆弱性スキャナなど

Vulsの参考情報

- GitHub VulsのREADMEが充実
  - ✓ 日本語のREADME
- Qiita: 脆弱性スキャナVuls 関連リンク集
- Vuls祭り #1 2016/9/26 開催　100名ほど参加
  - ✓ Slides@connpass
- Qiita: Vuls Advent Calendar 2016
- Join Slack Team 参加者263名（日本語チャネルは138名）
  - ✓ http://bit.ly/2ft8H5c

まとめ

サーバのソフトウェアアップデートは必要です

- IPS/IDS, Antivirusでは防げない脆弱性が存在します
- ツールを使ってシステムに潜在する脆弱性を見える化しましょう

Vulsは**継続的な脆弱性対策**を可能にします

- 新規に脆弱性やアープデートが公開されたタイミングで、脆弱性の詳細情報と該当するサーバをVulsが教えてくれます

OSSなので明日から**無料**で使えます！

有償サポートやカスタマイズはご相談ください

- フューチャーアーキテクト株式会社　担当：神戸（かんべ）まで
- mailto: gr-tig-ta-security@future.co.jp