セキュリティの現状とOSSの応用

フューチャーアーキテクト株式会社
スペシャリスト
林　優二郎

自己紹介

はやし　ゆうじろう

林　優二郎

フューチャーアーキテクト新卒入社
技術部門に所属、セキュリティリーダー

社内のコンポーネント開発担当後、
セキュリティチーム立ち上げ担当

最近のトピック

「中小企業の情報セキュリティ対策ガイドライン」、7年ぶりに改訂 - 経営への影響なども解説

情報処理推進機構（IPA）は、中小企業を対象とした「中小企業の情報セキュリティ対策ガイドライン 第2版」を公開した。

同資料は、中小企業において重要な情報の漏洩や滅失などを防ぐことを目的に、セキュリティ対策の考え方や実践方法を説明したガイドライン。同機構のウェブサイトよりダウンロードすることができる。

昨今の脅威動向を踏まえ、同機構が開催した有識者による検討ワーキンググループが改定案を策定。8月から9月に実施したパブリックコメントを経て、今回7年ぶりに改訂した。

インシデントなどが事業へ及ぼす影響も高まっているとして、あらたに経営者の視点を踏まえた内容を追加。経営者向けの「経営者編」と、システム管理者向けの「管理実践編」で構成されている。

7年ぶりの改訂となった中小企業の情報セキュリティ対策ガイドライン 第2版

<http://www.security-next.com/075778>

今年は国が本気出してセキュリティ対策し始めた年

経産省

2016/02/08 秘密情報の保護ハンドブック～企業価値向上に向けて～
2016/03/01 情報セキュリティ管理基準（平成28年改正版）
2016/03/24 不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況

総務省

2016/03/19 不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況

NISC

2016/01/25 我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針
2016/02/02 ネットワークビギナーのための情報セキュリティハンドブック

警察庁

2016/03/17 情報技術解析平成 27 年報
2016/04/14 平成27年における出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について

IPA

2016/03/03 内部不正による情報セキュリティインシデント実態調査報告書
2016/03/04 営業秘密管理・保護システムに関するセキュリティ要件調査報告書
2016/03/08 2015年度 中小企業における情報セキュリティ対策に関する実態調査報告書
2016/03/16 つながる世界の開発指針
2016/03/31 公衆無線 LAN 利用に係る脅威と対策
2016/03/31 情報セキュリティ10大脅威 2016
2016/05/10 企業のCISOやCSIRTに関する実態調査2016
2016/05/12 IoT開発におけるセキュリティ設計の手引き
2016/05/31 増加するインターネット接続機器の不適切な情報公開とその対策
2016/06/09 企業における情報システムのログ管理に関する実態調査
2016/06/29 特定業界を執拗に狙う標的型サイバー攻撃の分析レポート

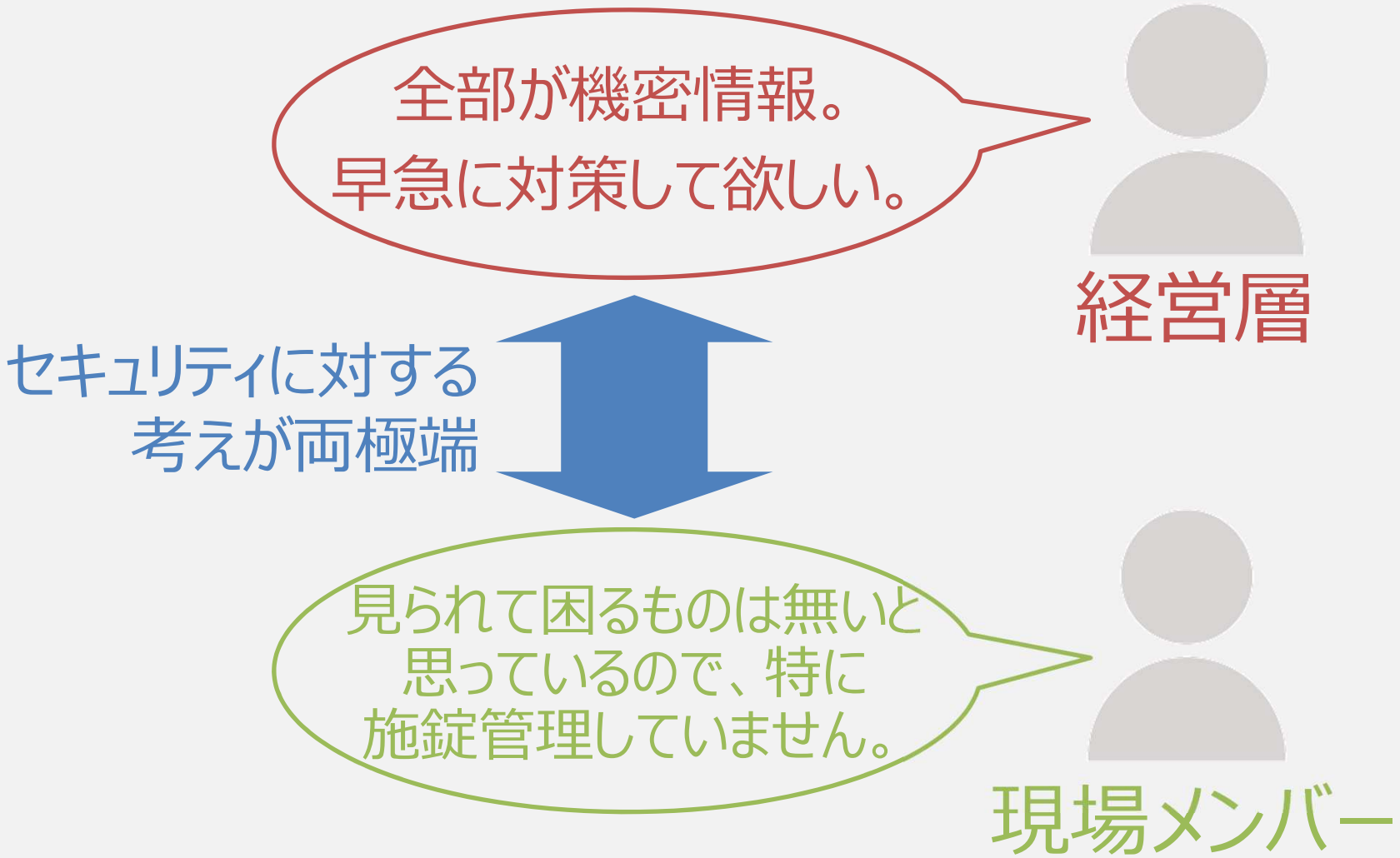
・
・

ガイドラインは整備されたが、
具体的に何をしていいか分からない、
という声も・・・

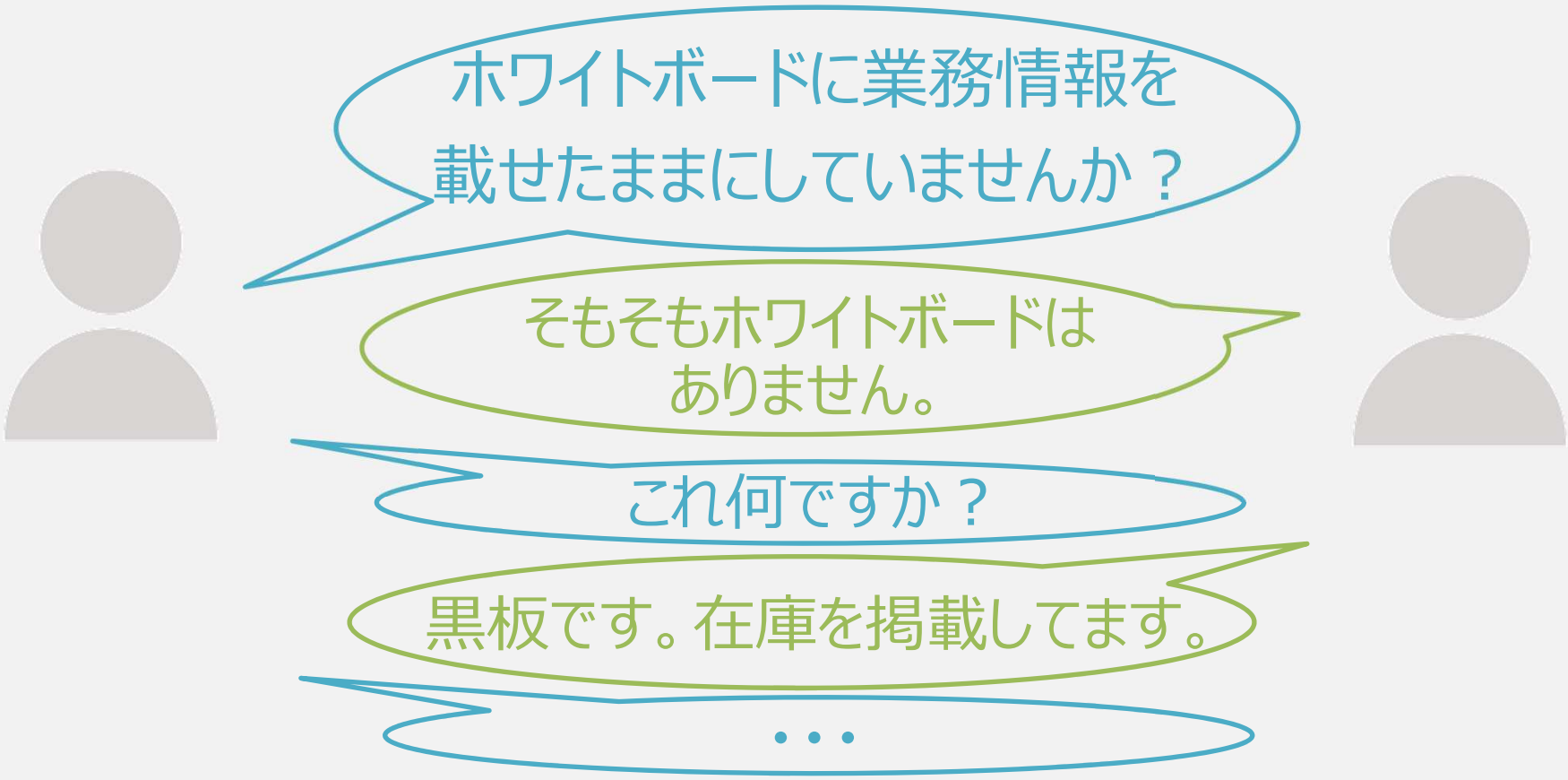
- ✓ 自社のセキュリティレベルが把握できてない
- ✓ どこまで対策すべきか分からない
- ✓ どこから対策打てばいいのか分からない
- ✓ どの程度投資すべきか分からない

・・・

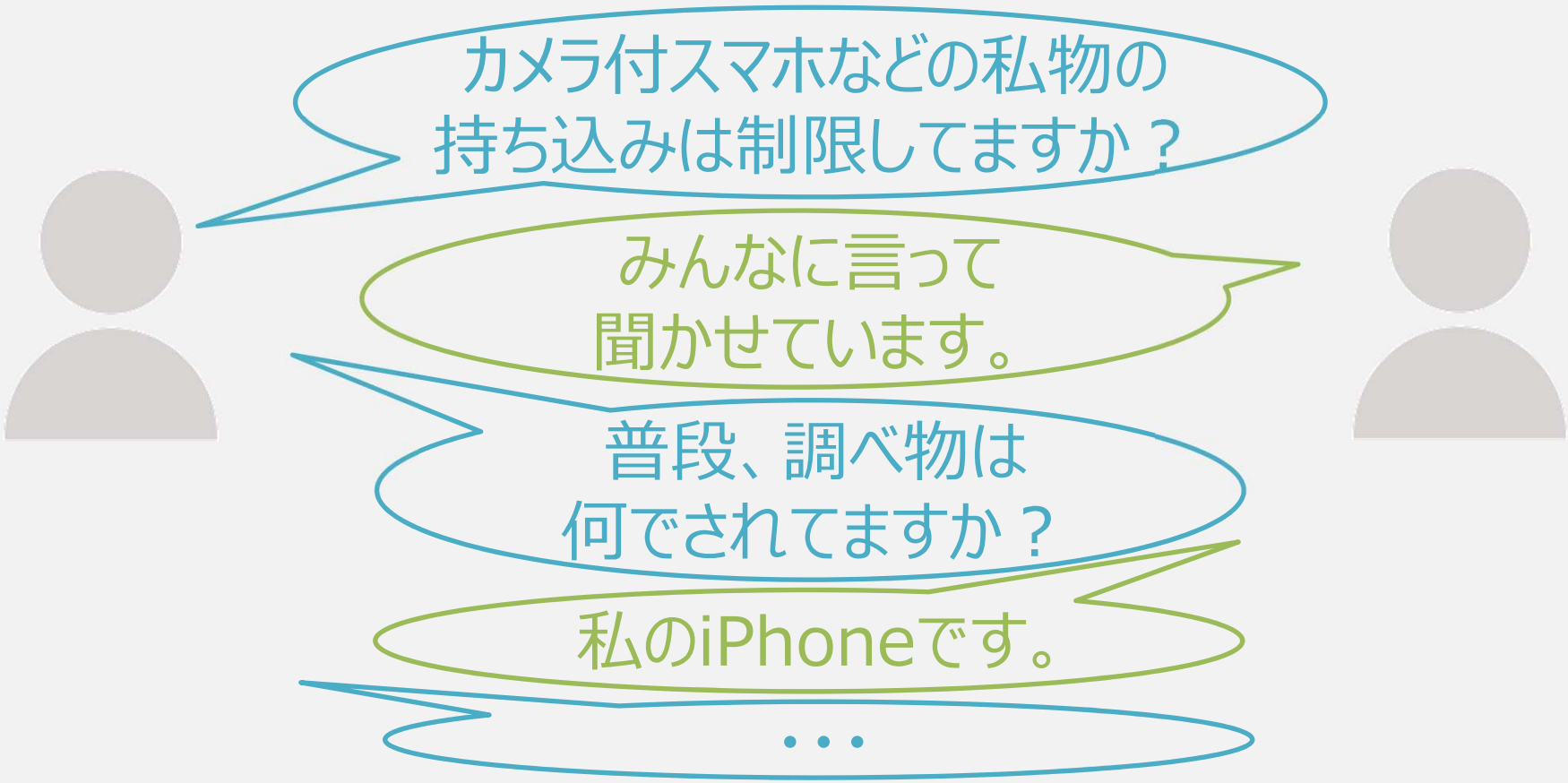
現場と経営者で両極端


全部が機密情報。
早急に対策して欲しい。
経営層
セキュリティに対する
考えが両極端
見られて困るものは無いと
思っているので、特に
施錠管理していません。
現場メンバー

何が守るべき情報か意識してない

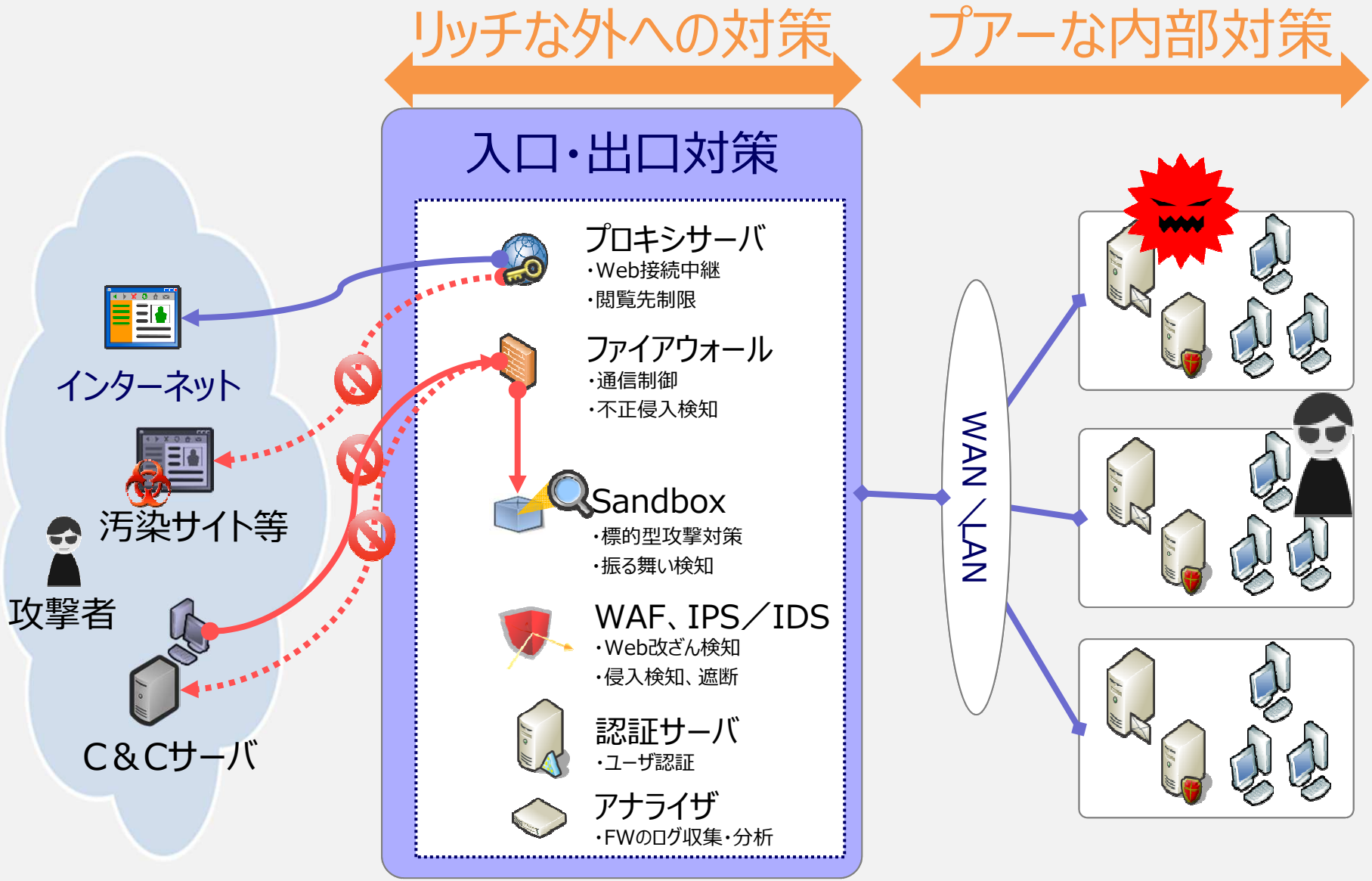


そもそも無意識なことも・・・



技術的対策として
セキュリティ対策機器導入を
検討している企業も多いが・・・

外だけ対策して中は不十分な場合も・・・



ベネッセの個人情報漏えい事件

委託先社員から
情報が漏えい

各　位

会 社 名： 株式会社ベネッセホールディングス
代表者名：代表取締役会長兼社長　原田　泳幸
（コード番号：9783　東証第一部）
問合せ先：ブランド・広報部長　　小沼　和幸

個人情報漏えい事故調査委員会発足に関するお知らせ

2014 年7月9日付の「お客様情報
とおり、子会社ベネッセコーポレー
客様をはじめ、ステークホルダーの
くお詫び申し上げます。
すでに緊急の対応として、全
ます。事実関係の調査分析を行
原田代表取締役会長兼社長の諮
情報漏えい事故調査委員会を下

1．　個人情報漏えい事故調査
委員長　　小林英明弁護士
※その他の委員は人選中で

2．　委員会設置日
2014年７月15日

各　位

会 社 名：　株式会社ベネッセホールディングス
代表者名：　代表取締役会長兼社長　原田　泳幸
（コード番号：9783　東証第一部）
会 社 名：　株式会社ベネッセコーポレーション
代表者名：　代表取締役社長　小林　仁

問合せ先：　株式会社ベネッセホールディングス
ブランド・広報部長　　小沼　和幸

＜お客様情報の漏えい＞
弊社グループ会社の業務委託先の元社員の逮捕について

本日、株式会社ベネッセコーポレーション（以下「弊社」といいます）のシステム開発・運用を行っているグループ会社・株式会社シンフォーム（本社：岡山市北区、代表取締役社長：田中隆章）の業務委託先の元社員（39 歳、男性）が、弊社お客様情報を社外に漏えいさせたとして、不正競争防止法違反の容疑で警視庁に逮捕されました。

このような事態を招きましたことを深く反省いたしますとともに、お客様をはじめとする皆様に、多大なご心配・ご迷惑をおかけいたしますことを、深くお詫び申し上げます。

本件は、本年７月９日に公表いたしましたとおり、お客様からのお問合せをきっかけとしてお客様情報漏えいの事実が確認され、警察による捜査が開始されておりました。弊社は７月 15 日に警視庁に刑事告訴しております。

捜査協力の観点から公表を差し控えてまいりましたが、当該元社員の逮捕を受け、当該事案の概要をご報告いたします。

弊社では、本件を厳粛に受け止め、お客様情報の管理を一層強化し、再発防止を図っておりますが、引き続き全社一丸となって内部管理態勢の一層の強化に取り組み、お客様からの信頼回復に努めてまいります。

Stuxnet

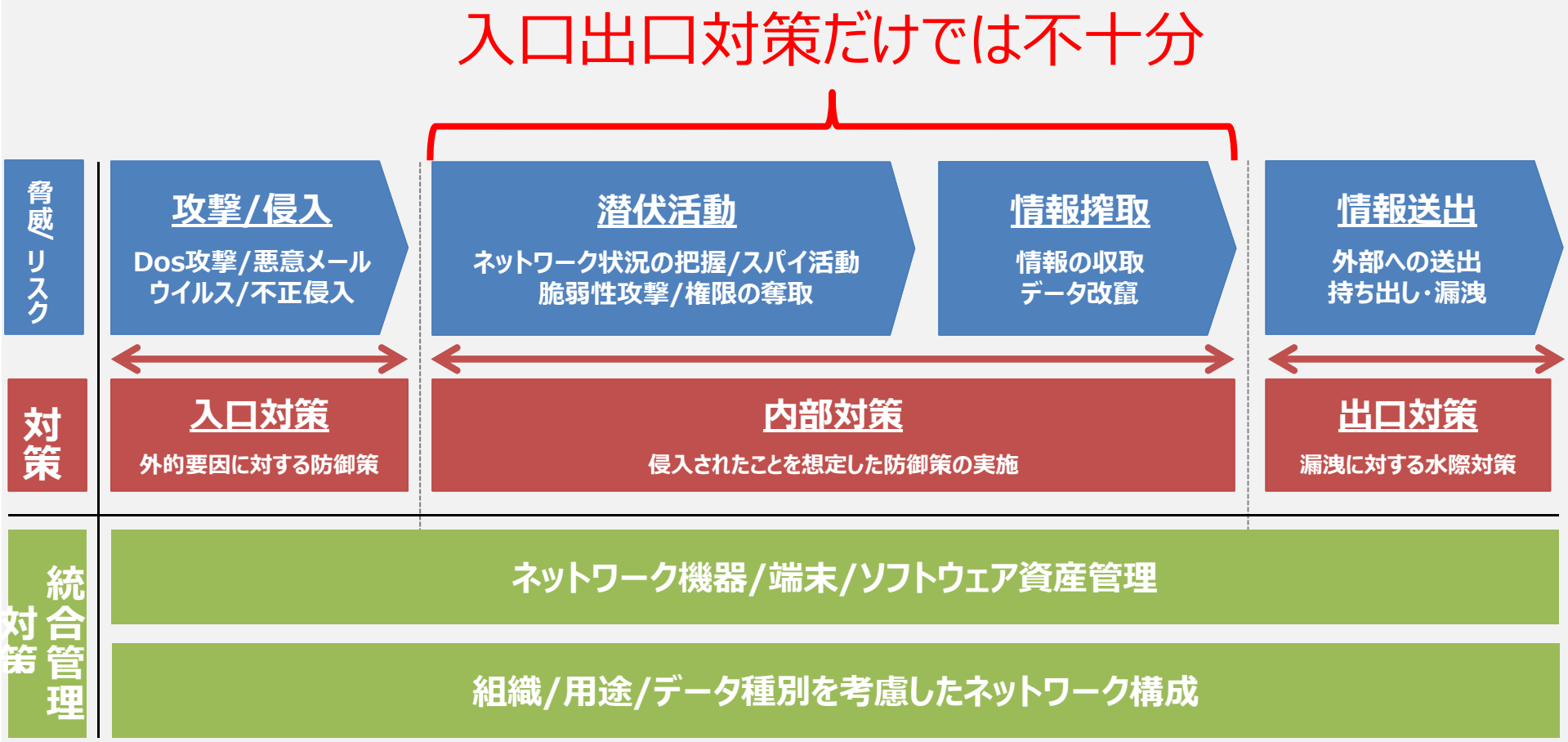
ATP型のコンピューター・ワーム。 

イランの国家政策である核開発を妨害し遅延させる目的で使用され、実際に、2009年から2010年にかけて、イラン国内の核燃料施設でウラン濃縮用遠心分離機を破壊する、という物理的実害を引き起こした。

スタクスネットはまた、それまで比較的安全だと信じられていた、インターネットに接続していない産業用制御システムにもUSBメモリーを介して感染・発症することから、産業用システムのセキュリティ管理のあり方を根本から考え直させた、という点でも衝撃的であった。

参照URL: <https://eset-info.canon-its.jp/malware_info/trend/detail/160308.html>

多層防御が常識


入口出口対策だけでは不十分
脅威/リスク
攻撃/侵入
Dos攻撃/悪意メール
ウイルス/不正侵入
潜伏活動
ネットワーク状況の把握/スパイ活動
脆弱性攻撃/権限の奪取
情報搾取
情報の収取
データ改竄
情報送出
外部への送出
持ち出し・漏洩
対策
入口対策
外的要因に対する防御策
内部対策
侵入されたことを想定した防御策の実施
出口対策
漏洩に対する水際対策
統合管理対策
ネットワーク機器/端末/ソフトウェア資産管理
組織/用途/データ種別を考慮したネットワーク構成

とはいえ、お金も対応する人も限られている

さらに・・・

経産省のガイドラインに記載の通り
リターンを求めない投資が必要

2．経営者が認識する必要がある「3原則」

(1) セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。このため、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。

(2) 子会社で発生した問題はもちろんのこと、自社から生産の委託先などの外部に提供した情報がサイバー攻撃により流出してしまうことも大きなリスク要因となる。このため、自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要である。

(3) ステークホルダー（顧客や株主等）の信頼感を高めるとともに、サイバー攻撃を受けた場合の不信感を抑えるため、平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要である。

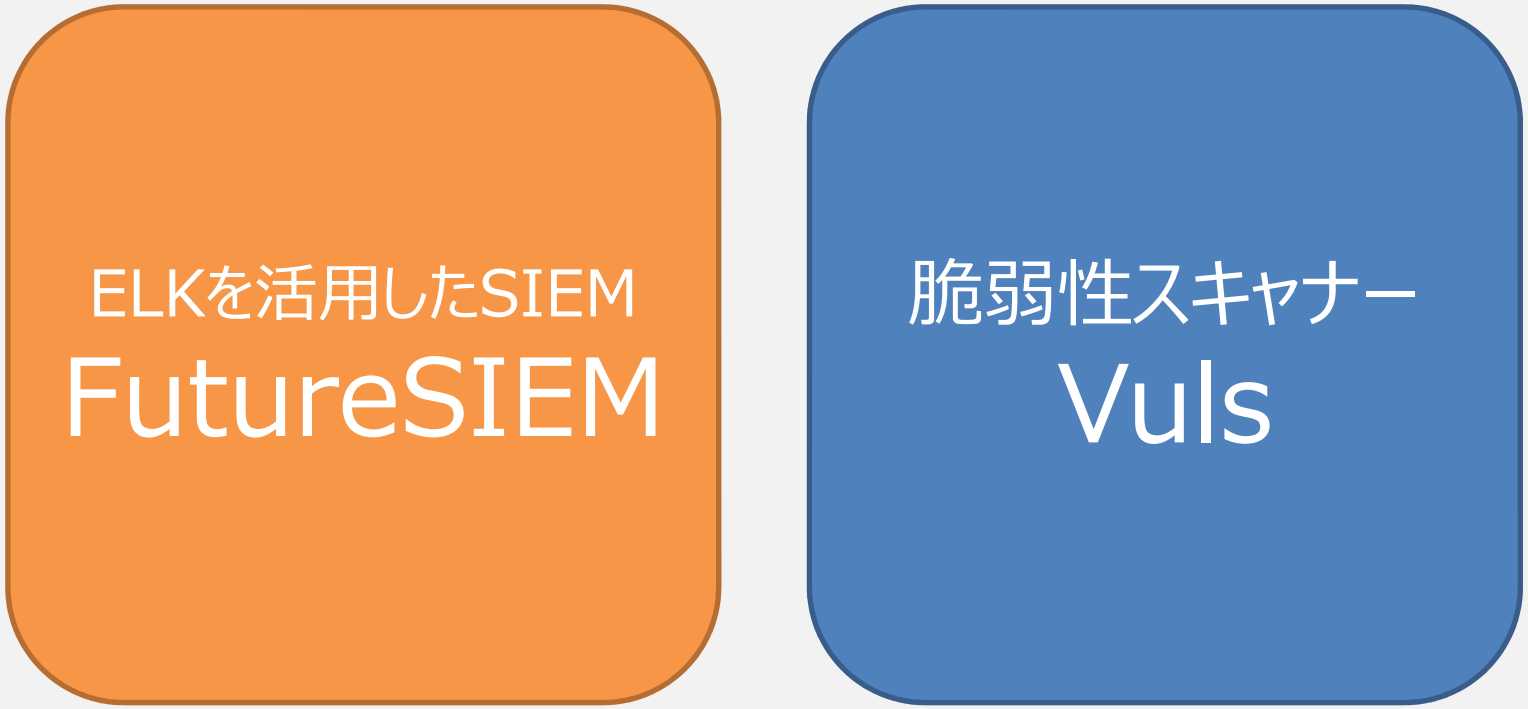
参照URL: <http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf>

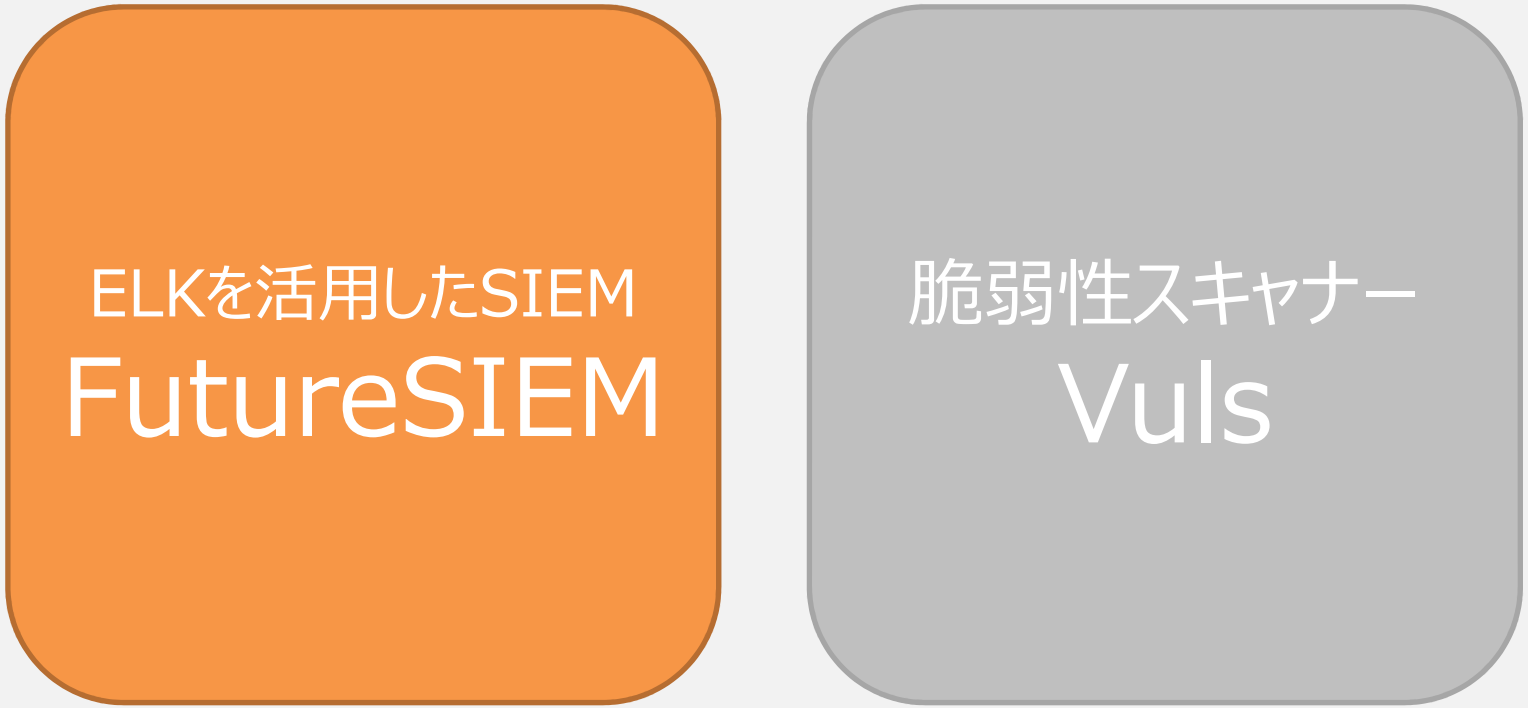
現場の負荷も増える

- ✓ 新規セキュリティ機器のキャッチアップ
- ✓ セキュリティ機器のチューニング
  （ルール、フィルタリング、ログレベル、・・・）
- ✓ 取得した膨大な量の情報をチェック
- ✓ 現行業務をやりつつ対応

  ・・・

内部対策（にかぎらず）は出来る限り
OSSを活用して、費用を抑えて対策したい


ELKを活用したSIEM
FutureSIEM
脆弱性スキャナー
Vuls


ELKを活用したSIEM
FutureSIEM
脆弱性スキャナー
Vuls

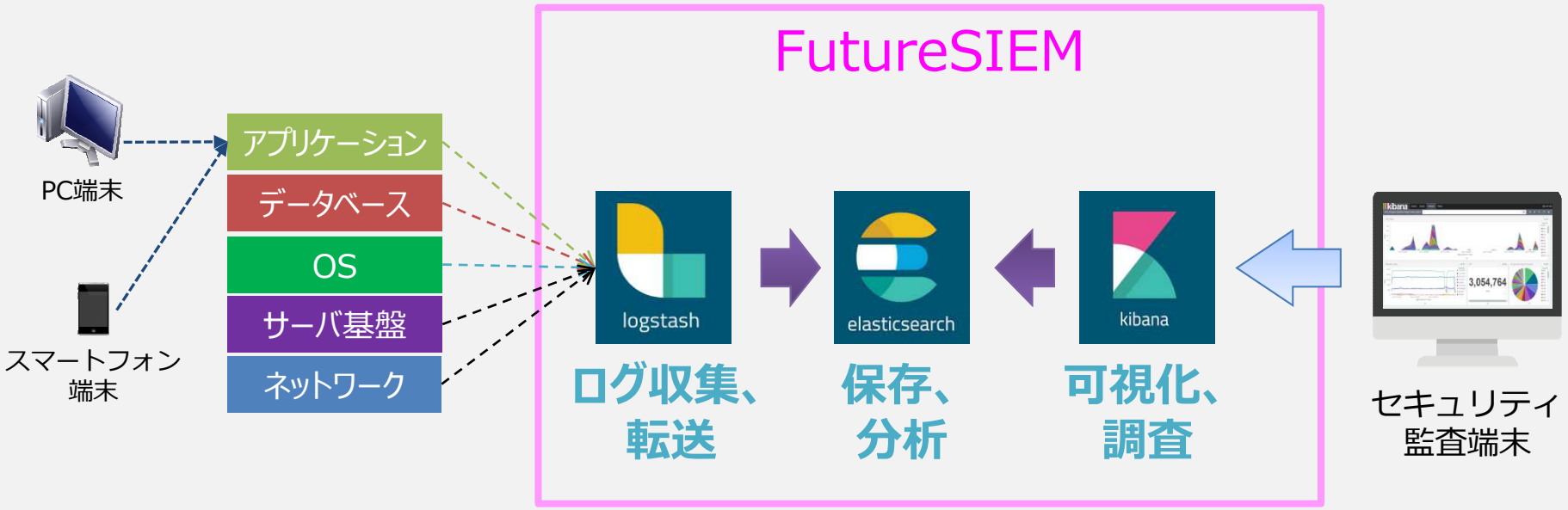
内部対策は、

- ✓ 入口出口対策をすり抜けたウィルス等
- ✓ 悪意を持った人

であることが多いので、基本的に１つのログやセンサーでは検知できない

横断的な分析が必要

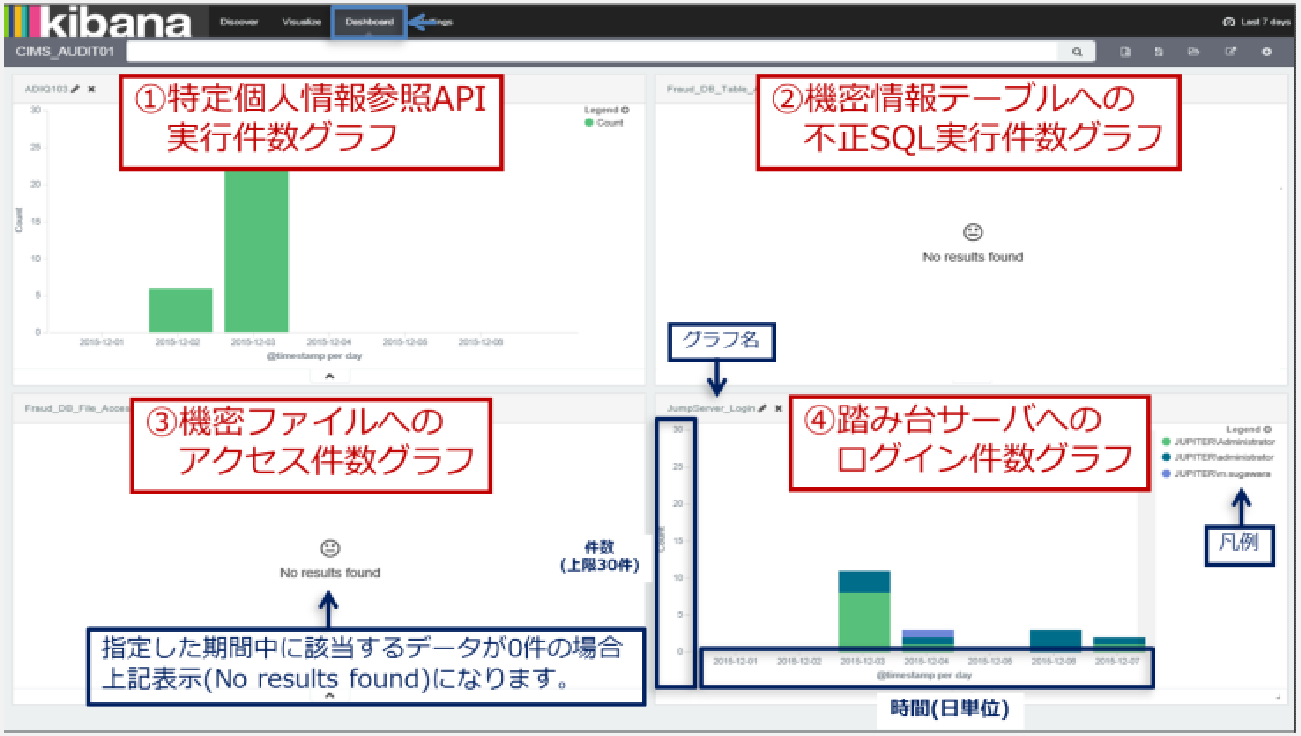
FutureSIEM



OSSを組み合わせて
アプリやDB、OS、NWなど
各種ログを横断的に収集し、分析

FutureSIEMの特徴

- ✓ シンプルな画面で誰でも直感的に異常が分かる（属人化の廃止）
- ✓ 多種多様なログの種類に対応
- ✓ OSSを使っているため、基本的には無料で利用可能
  （SIEM製品を購入すると高額な場合が多い）
- ✓ 大手証券会社にて導入され、セキュリティレベル向上と運用負荷低減



考えられる活用パターン

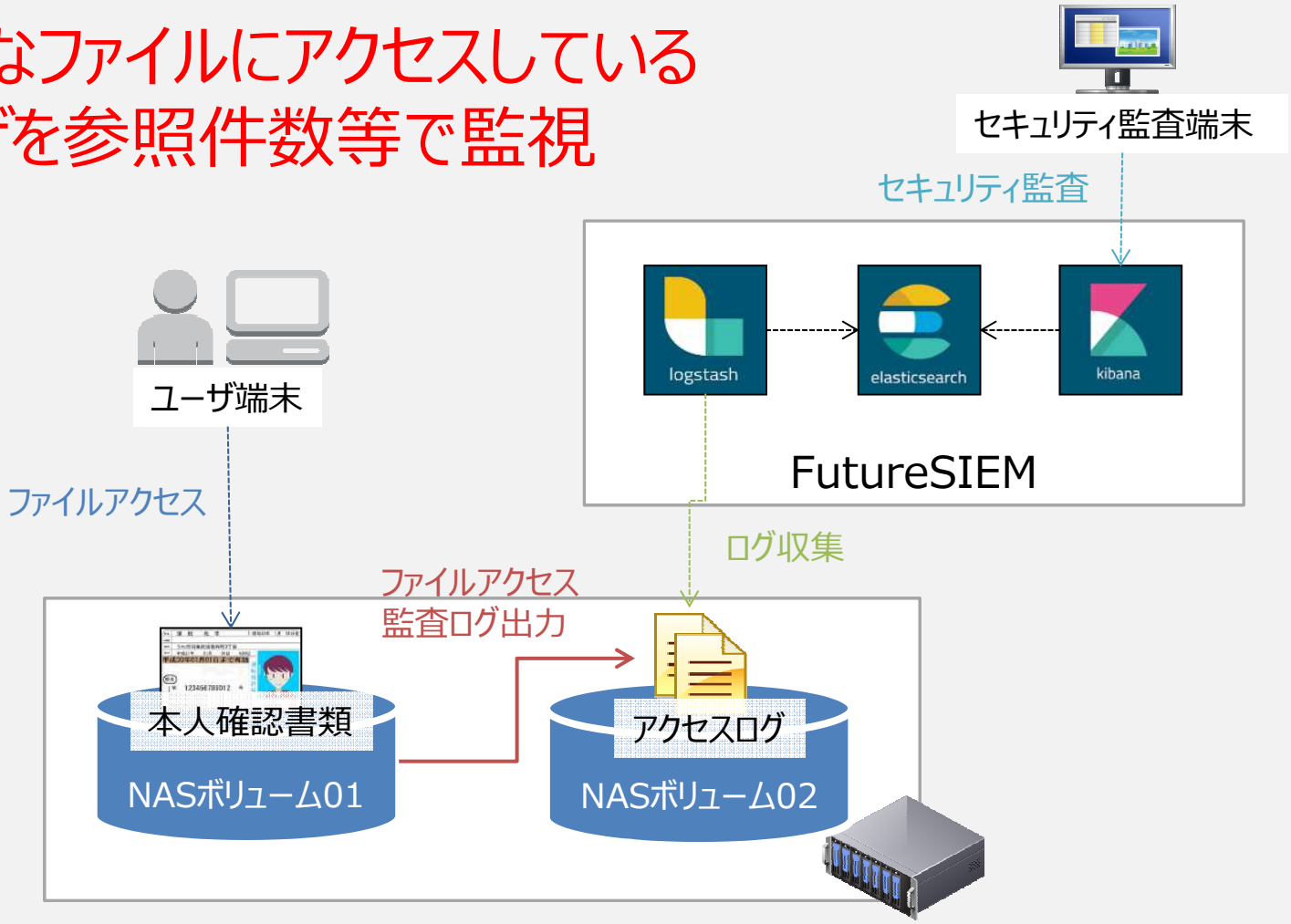
【ケース①】
・ITシステム運用
・アプリケーション運用
・セキュリティ分析

【ケース②】
・マーケティング洞察
・ビジネス配備
・顧客センチメンタル分析

【ケース③】
・Webサイト検索
・内部/イントラ検索
・URL検索

ユースケース①：
本人確認書類の画像データのファイルアクセス監査

重要なファイルにアクセスしている
ユーザを参照件数等で監視



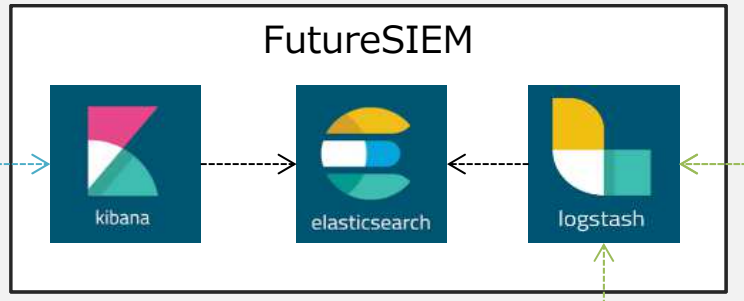
ユースケース②：
インターネットからの不正Webアクセス監査

グラフイメージ図

アクセス元のグローバルIPアドレスから
どこからアクセスされているかの監視

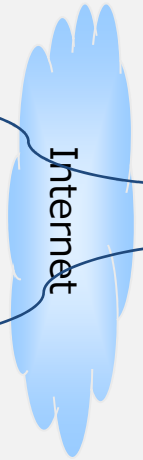
監査端末

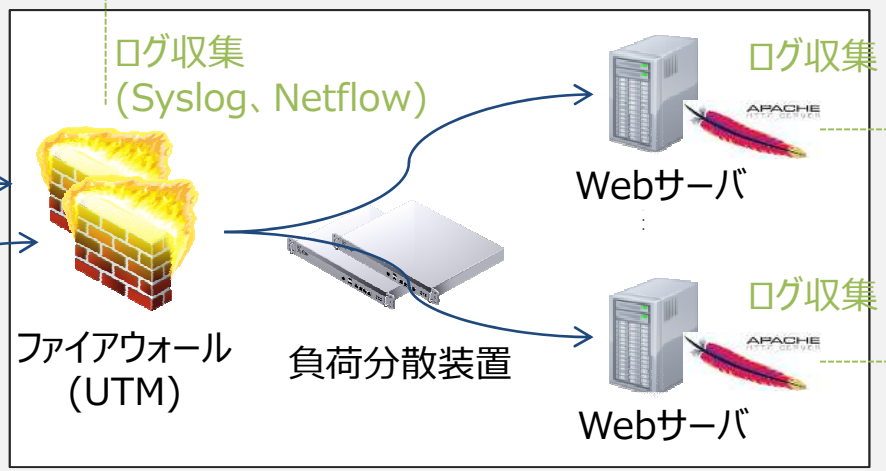
ログ分析

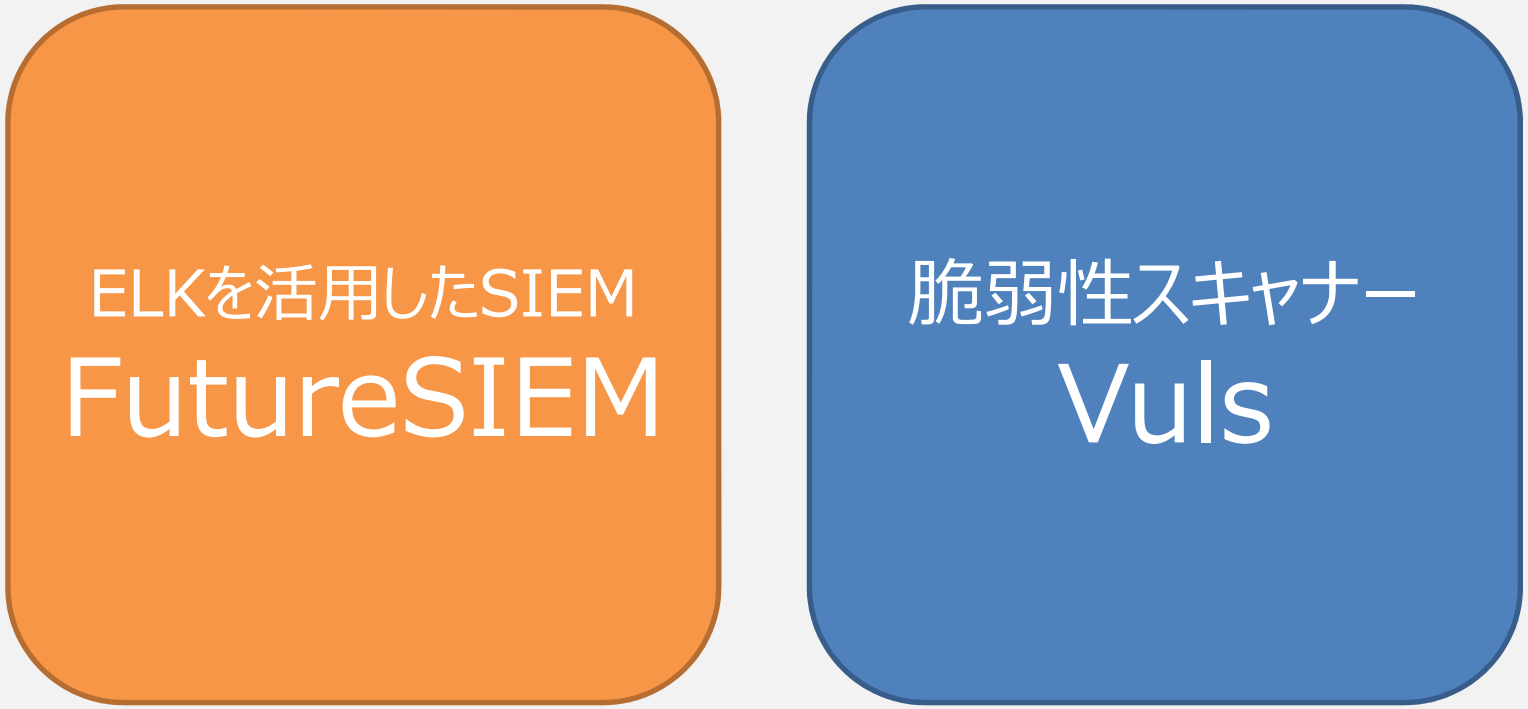


パソコン端末

スマートデバイス





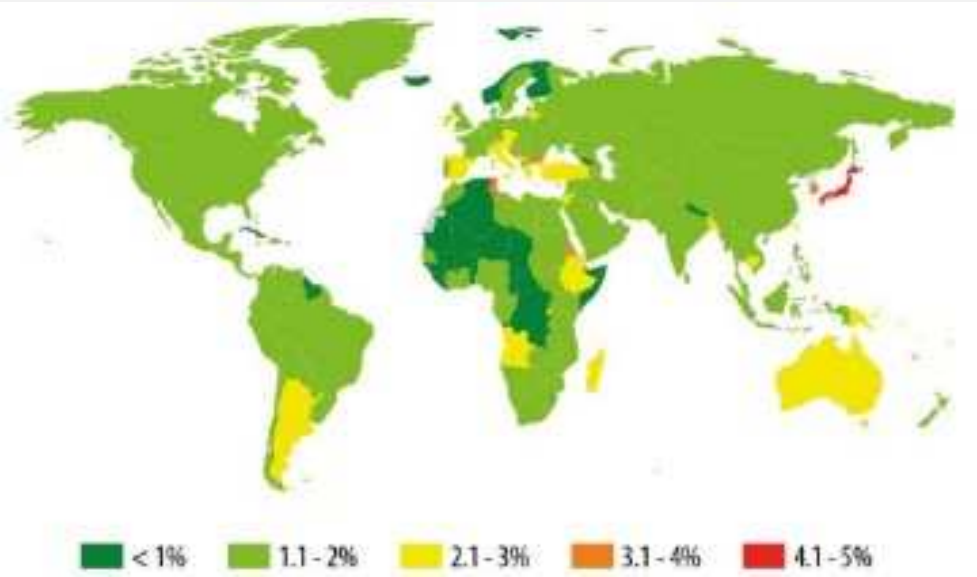

ELKを活用したSIEM
FutureSIEM
脆弱性スキャナー
Vuls

ELKを活用したSIEM
FutureSIEM

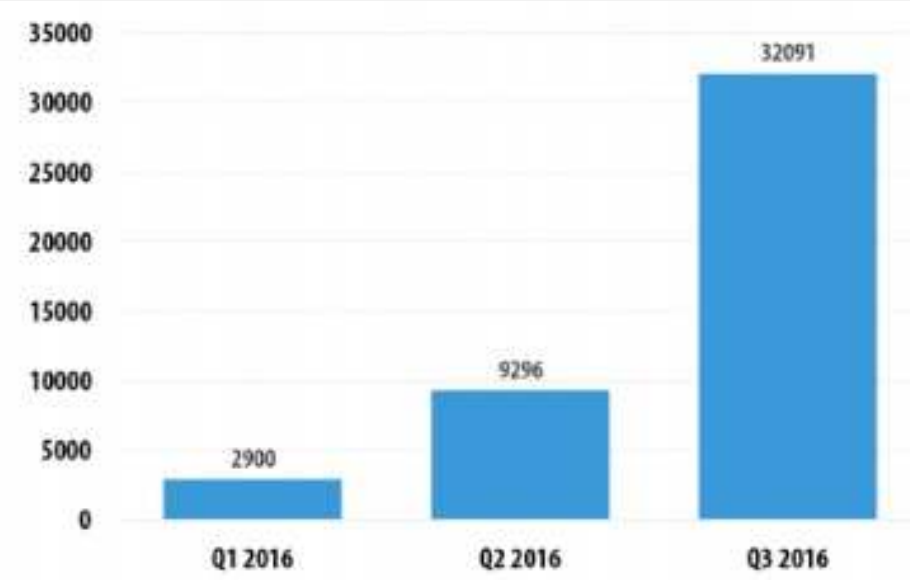
脆弱性スキャナー
Vuls

最近のトピック②

ランサムウェアの遭遇率は
日本が１位（２位クロアチア、３位韓国）



ランサムウェア亜種の件数は
激増



参考URL: <http://www.security-next.com/075858>

Googleのアンケート結果

参照URL: <https://japan.googleblog.com/2016/02/blog-post.html>

ソフトウェア・アップデートも大変

- ✓ システムで利用している技術要素を把握し、常にアップデートしなければならない
- ✓ JVNやNVDなどの脆弱性情報チェックは運用負荷が高い
- ✓ ほとんど自分に関係ない情報なのでツライ
- ✓ 情報を見逃したら脆弱性が放置されたまま残ってしまう
- ✓ 利用中のJavaライブラリの脆弱性まで追い切れない
- ✓ シグニチャベースのアンチウィルスだけでは不十分

そこでOSSで自動化

VULnarability Scanner

脆弱性　スキャナー

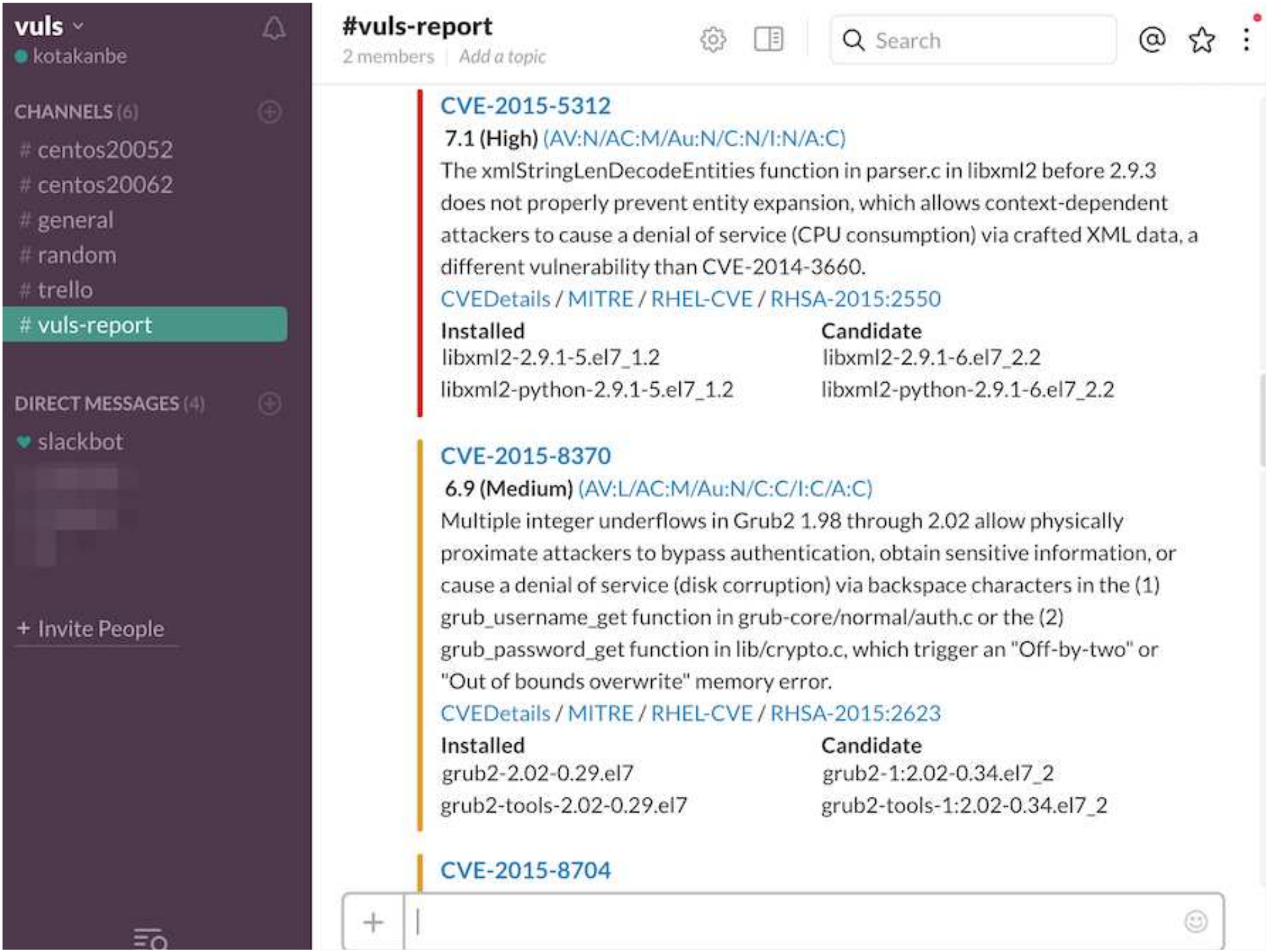
2016年4月1日、
GitHubにOSSとして公開！！

概要

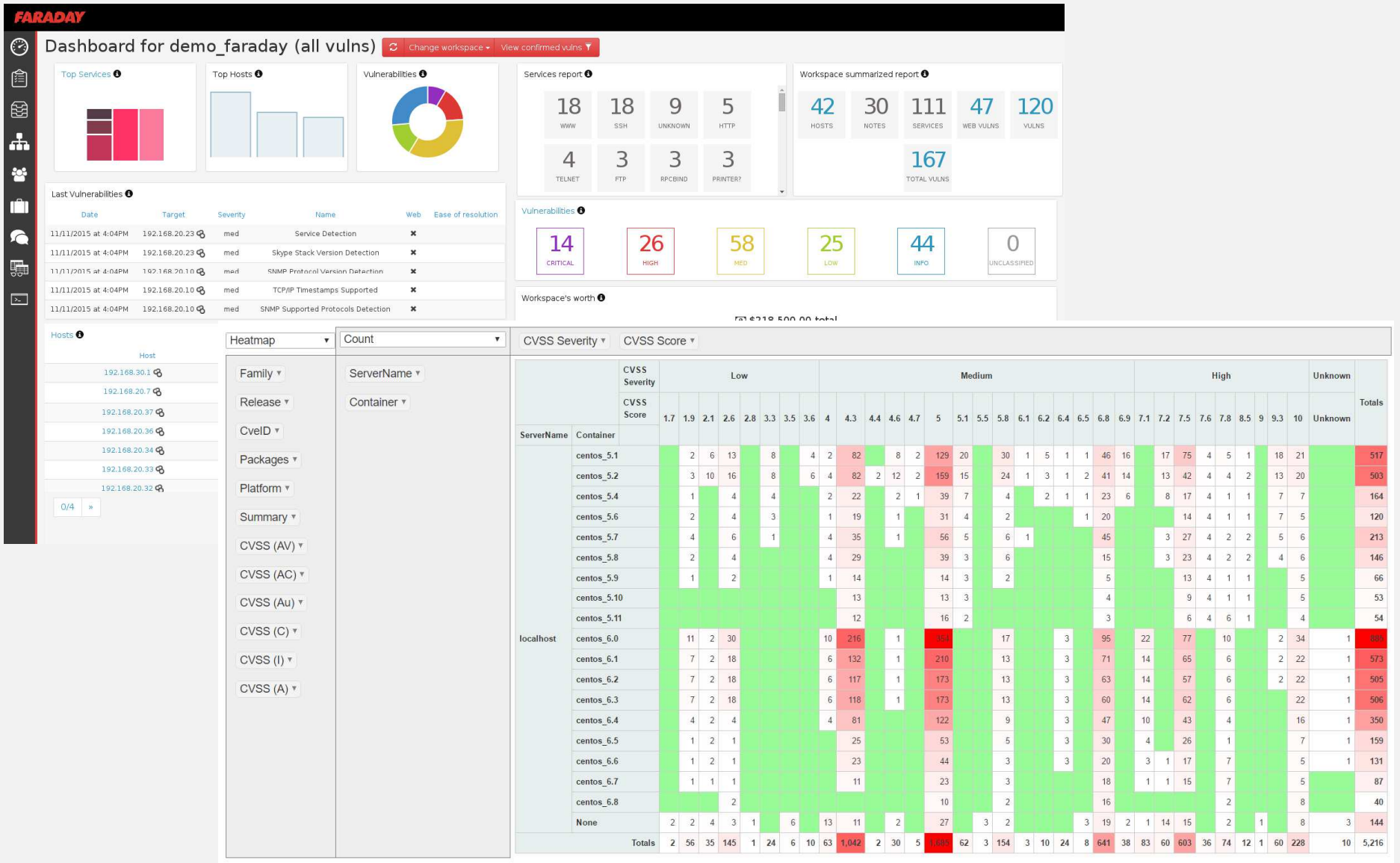

管理下のシステム
ソフトウェア情報
ubuntu
redhat.
FreeBSD
突合
脆弱性情報
JVN
(日本の脆弱性データベース)
NVD
(米国の脆弱性データベース)
e-mail、slack等で
脆弱性を通知
CSIRT、
システム管理者

特徴

- ✓ エージェントレス
  (モジュール配布も不要で現行環境への影響が少ない)
- ✓ セットアップ、初期設定が簡単
  (バイナリコピーのみ。サーバ手動登録不要)
- ✓ パッケージ以外のソフトウェアの脆弱性も検知可能
- ✓ オンプレ、クラウドの両方に対応
- ✓ Linuxの主要ディストリビューションに対応
  (AmazonLinux、CentOS、Ubuntu、RHEL、FreeBSD、・・・)
- ✓ オープンソースなので、ブラックボックスな仕組み、挙動がない
- ✓ 豊富なレポート手段（Slack, e-mail, TUI …）


vuls
kotakanbe
CHANNELS (6)
centos20052
centos20062
general
random
trello
vuls-report
DIRECT MESSAGES (4)
slackbot
+ Invite People
#vuls-report
2 members | Add a topic
Search
CVE-2015-5312
7.1 (High) (AV:N/AC:M/Au:N/C:N/I:N/A:C)
The xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.3 does not properly prevent entity expansion, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data, a different vulnerability than CVE-2014-3660.
CVEDetails / MITRE / RHEL-CVE / RHSA-2015:2550
Installed
libxml2-2.9.1-5.el7_1.2
libxml2-python-2.9.1-5.el7_1.2
Candidate
libxml2-2.9.1-6.el7_2.2
libxml2-python-2.9.1-6.el7_2.2
CVE-2015-8370
6.9 (Medium) (AV:L/AC:M/Au:N/C:C/I:C/A:C)
Multiple integer underflows in Grub2 1.98 through 2.02 allow physically proximate attackers to bypass authentication, obtain sensitive information, or cause a denial of service (disk corruption) via backspace characters in the (1) grub_username_get function in grub-core/normal/auth.c or the (2) grub_password_get function in lib/crypto.c, which trigger an "Off-by-two" or "Out of bounds overwrite" memory error.
CVEDetails / MITRE / RHEL-CVE / RHSA-2015:2623
Installed
grub2-2.02-0.29.el7
grub2-tools-2.02-0.29.el7
Candidate
grub2-1:2.02-0.34.el7_2
grub2-tools-1:2.02-0.34.el7_2
CVE-2015-8704

ダッシュボード表示や集計も可能



		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	1	5	1	1	46	16		17	75	4	5	1		18	21		517
	centos_5.2			3	10	16		8		6	4	82	2	12	2	159	15		24	1	3	1	2	41	14		13	42	4	4	2		13	20		503
	centos_5.4			1		4		4			2	22		2	1	39	7		4		2	1	1	23	6		8	17	4	1	1		7	7		164
	centos_5.6			2		4		3			1	19		1		31	4		2				1	20				14	4	1	1		7	5		120
	centos_5.7			4		6		1			4	35		1		56	5		6	1				45			3	27	4	2	2		5	6		213
	centos_5.8			2		4					4	29				39	3		6					15			3	23	4	2	2		4	6		146
	centos_5.9			1		2					1	14				14	3		2					5				13	4	1	1			5		66
	centos_5.10											13				13	3							4				9	4	1	1			5		53
	centos_5.11											12				16	2							3				6	4	6	1			4		54
localhost	centos_6.0			11	2	30					10	216		1		354			17			3		95		22		77		10			2	34	1	886
	centos_6.1			7	2	18					6	132		1		210			13			3		71		14		65		6			2	22	1	573
	centos_6.2			7	2	18					6	117		1		173			13			3		63		14		57		6			2	22	1	505
	centos_6.3			7	2	18					6	118		1		173			13			3		60		14		62		6				22	1	506
	centos_6.4			4	2	4					4	81				122			9			3		47		10		43		4				16	1	350
	centos_6.5			1	2	1						25				53			5			3		30		4		26		1				7	1	159
	centos_6.6			1	2	1						23				44			3			3		20		3	1	17		7				5	1	131
	centos_6.7			1	1	1						11				23			3					18		1	1	15		7				5		87
	centos_6.8					2										10			2					16						2				8		40
	None		2	2	4	3	1		6		13	11		2		27		3	2				3	19	2	1	14	15		2		1		8	3	144
	Totals		2	56	35	145	1	24	6	10	63	1,042	2	30	5	1,605	62	3	154	3	10	24	8	641	38	83	60	603	36	74	12	1	60	228	10	5,216

高い検知率

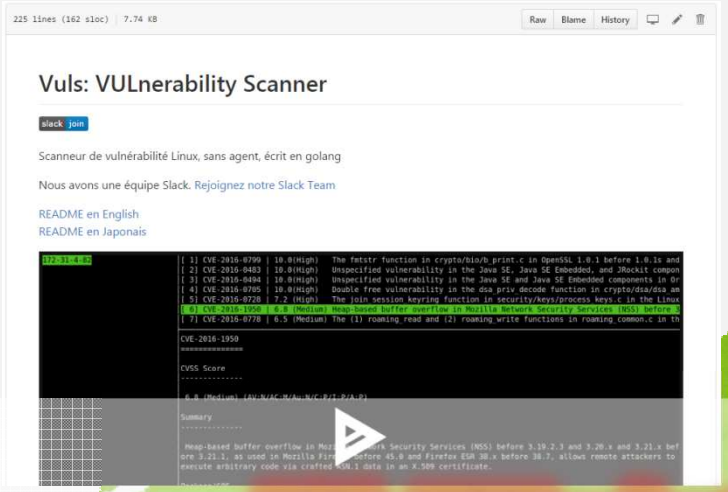
CVE検知数比較（スキャン対象：RHEL7.2）

	Vuls	OpenVAS	Inspector
検知数	203	141	190
未検知の疑い	0	0	0
誤検知の疑い	0	1	0
正常検知数	203	140	190

1	CVE-2013-4312		CVE-2013-4312
2	CVE-2015-3217	CVE-2015-3217	
3	CVE-2015-5073	CVE-2015-5073	
4	CVE-2015-8325		CVE-2015-8325
5	CVE-2015-8374		CVE-2015-8374
6	CVE-2015-8543		CVE-2015-8543
7	CVE-2015-8710		CVE-2015-8710
8	CVE-2015-8746		CVE-2015-8746
9	CVE-2015-8803		CVE-2015-8803
10	CVE-2015-8804		CVE-2015-8804
11	CVE-2015-8805		CVE-2015-8805
12	CVE-2015-8812		CVE-2015-8812
13	CVE-2015-8844		CVE-2015-8844
14	CVE-2015-8845		CVE-2015-8845
15	CVE-2015-8956		CVE-2015-8956
16	CVE-2016-0643		CVE-2016-0643

同様に困っている人が世界中にいたようで、
大きな反響があり・・・

フランス語

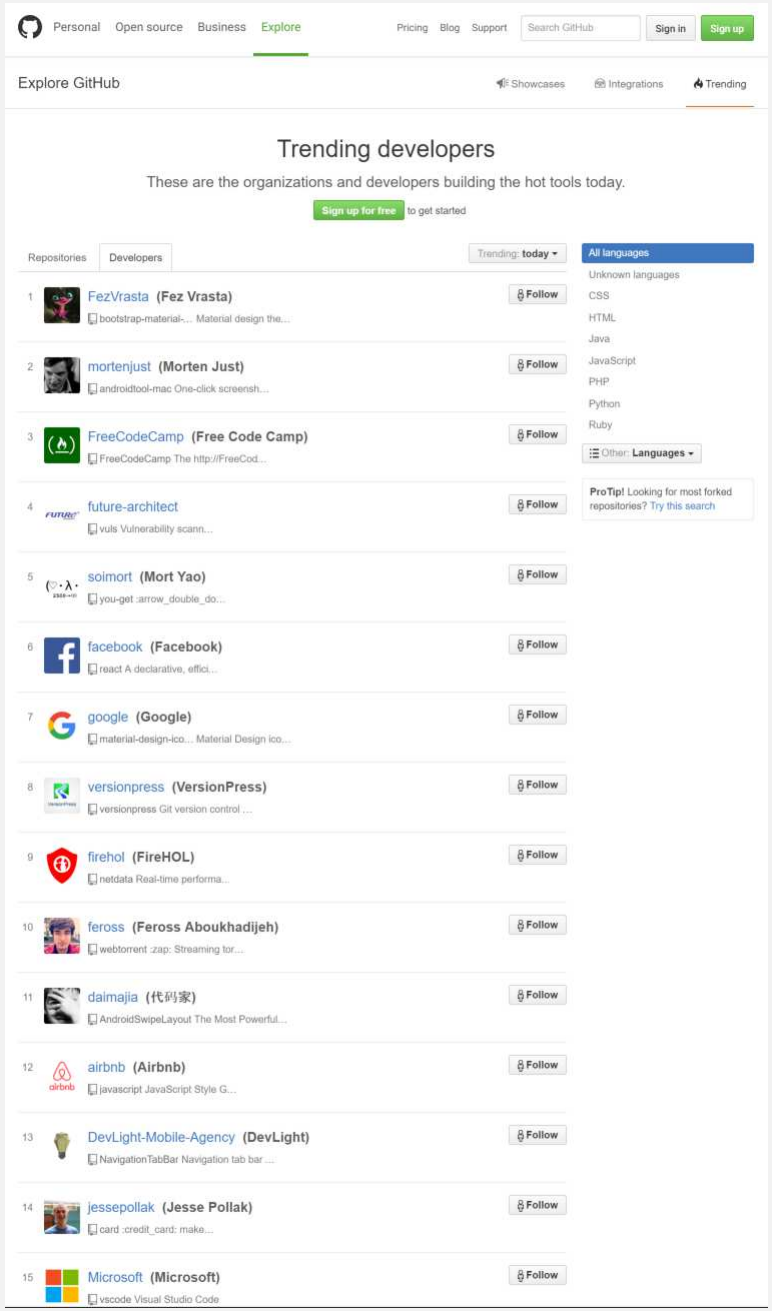


中国語

世界中で大反響！

※2016年4月時点

一時的に 4 位（企業ランキング１位）



FUTURE Architect　future-architect

世界6位　facebook

世界7位　Google

世界12位　airbnb

世界15位　Microsoft

順風満帆なことばかりではなく・・・

kenshaw 12:48 PM

kotakanbe: security in this thing is completely broken -- it needs to be 'root' to scan for packages on Debian derived systems -- I killed the thing when it got to scanning for packages to upgrade

Is all this do is check installed package versions against the CVE database?

Because that's pretty much worthless

that's not "detecting a vulnerability" -- that's just checking package version

my assumption when it said "vulnerability detection" in the readme was that you were building something akin to nessus/openvas -- but this as far as i can tell does none of the above, and completely breaks all security by have a nice central repository of all SSH keys

kotakanbe 12:55 PM

Many DevOps tools need root privilege something like Chef, Serverspec...

In the case of Debian like Linux, the scan procedure is below...
1. apt-get upgrade --dry-run (to search upgradable packages)
2. apt-get changelog (from installed version to candidate version)
3. parse changelog to get CVE IDs.

すごい怒ってる

kenshaw 12:55 PM

the fuck? you know nothing about these systems then

you don't need to do apt-get upgrade --dry-run

you shouldn't be within 200 yards of a linux server

kotakanbe: word of advice, look into the 'dpkg' command

also, you shouldn't be doing anything involved with 'security scanning' that requires root access of any kind

you're making the world worse off than it already is -- you should be ashamed of what you wrote and released to the public

kenshaw 1:04 PM

btw -- the reason you should be ashamed is that the two package managers you're "scanning", rpm + deb, both have supported for YEARS to report when packages are out of date -- if a vulnerability has a public CVE, then debian/redhat systems will have already gotten a security package released at least 48+ hours

kenshaw 1:11 PM
calling 'vuls' a 'vulnerability scanner' is like calling ssh a Windows UI

kotakanbe 1:25 PM
Thanks for you kindness.

意見に対して感謝言ったら、
火に油を注いでしまった様子

kenshaw 1:26 PM
definitely not being kind -- the problem in the software world is too many people push out crap and cause other people to use it -- this is one of those things

the only reason i can assume they continue to do that is because they never had anyone to tell them 'no' or 'this sucks' -- well, let me be the first to tell you -- this sucks, horribly

コミュニティメンバーのフォロー

seirios 11:58 PM

Vuls has just been released ,and the application is still under development.
Such like this software has some sort of problem, usually.

No one command you to use this application, and so you may not have to use it, if you do not like this.

Only to blame for the software which slide into growth is desired , is not make a constructive discussion .

aomoriringo 1:03 PM

少なくとも人格攻撃のとこは外して読みましょ

> also, you shouldn't be doing anything involved with 'security scanning' that requires root access of any kind

つまりこの人、セキュリティのためのソフトウェアなのにrootを要求するなといってるわけだけど

rootなしを前提にしたときって現実的にはたぶん同じような機能をもたせられないよね。

「ネットワーク経由でスキャンする機能を持ったらssh keyを全部持ったcenteral serverができてセキュリティ的に完全に死んじゃうじゃん」っていう話はまあわからなくもない

が、それはvulsの機能とはまた別の話だと思うわけで、「世界をより悪くしてる」なんて言えるわけない (edited)

そして、彼はOpenVASを
紹介して去っていった・・・

国内コミュニティも盛り上がり、
いろいろなメディア等でも取り上げて頂いた

ThinkIT

インタビュー

連載: OSSルーキーズ

脆弱性検知ツール「Vuls」の開発者に聞いた OSSをバズらせる極意

鈴木 教之（Think IT編集部）　2016年8月10日(水)

ツイート　いいね！ 381　シェア　G+1　3　B! ブックマーク　48

バルスというツールをご存知だろうか？ 日本ではとあるアニメの崩壊の呪文として扱われることの多いこのフレーズがいま、サーバー管理者のシステム崩壊を防ぐためのツールとして注目されている。OSSの脆弱性検知ツールであるVuls（バルス）について、開発元であるフューチャーアーキテクトの神戸 康多氏と林 優二郎氏に詳しく話を聞いた。

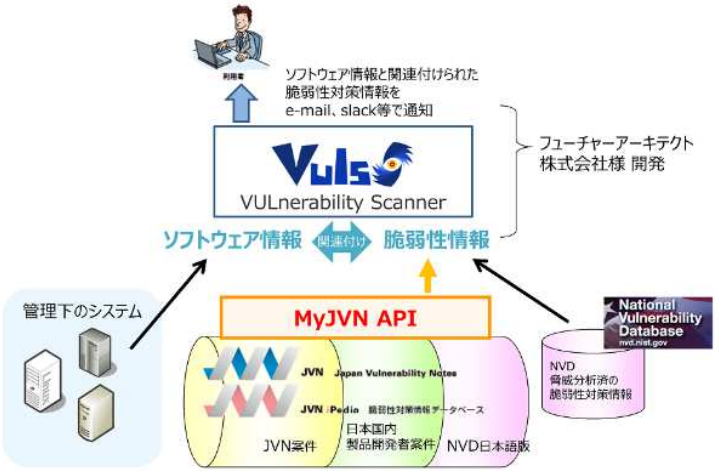
参照URL: <https://thinkit.co.jp/article/10092>

IPAのWeb記事 （ MyJVN事例紹介）

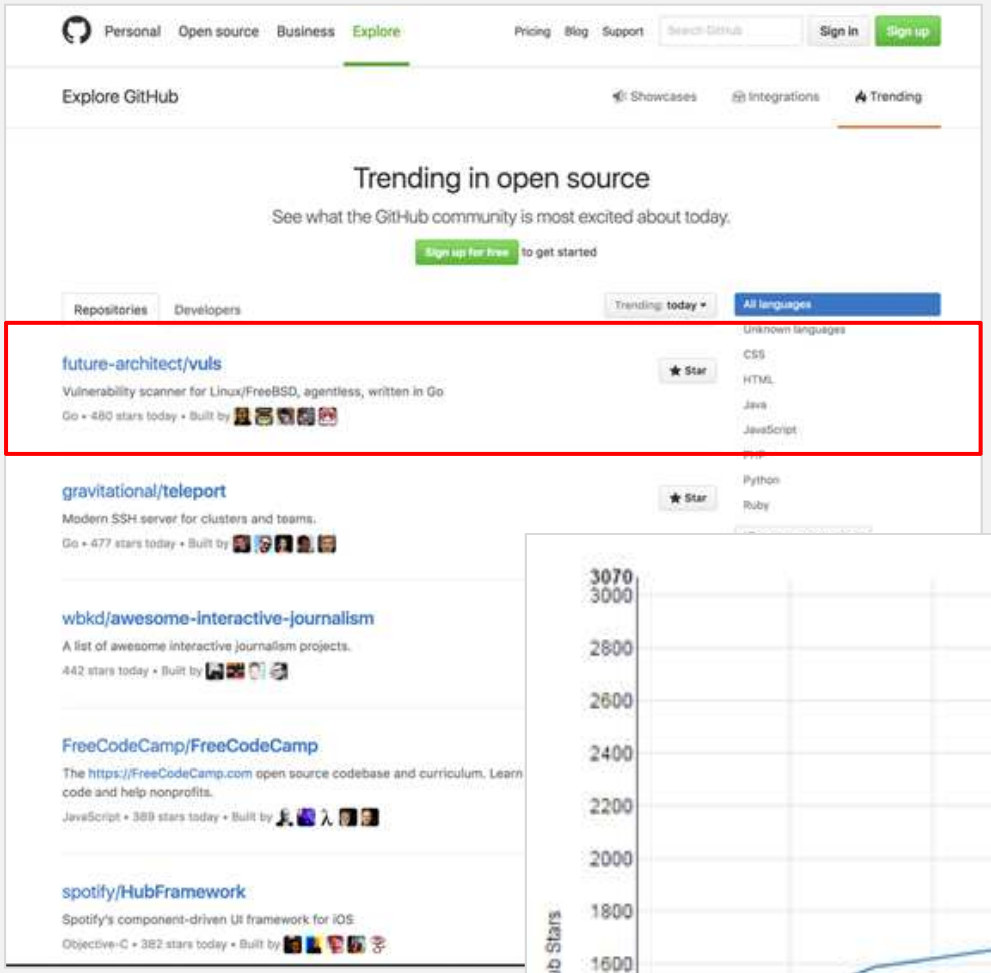
[活用事例] その5

フューチャーアーキテクト株式会社様では、脆弱性情報の収集と検知を自動化する脆弱性スキャン
しています(2016年4月1日から無償提供)。
Vulsでは、情報源のひとつとして、MyJVN APIを利用して「脆弱性対策情報データベース JVN iPed
より、脆弱性がどのサーバに該当するかを特定しています。利用者は、Vulsから提供される日本語

- Vuls(VULnerability Scanner)
- 脆弱性スキャンツール「Vuls」を無償で公開



参照URL: <http://jvndb.jvn.jp/apis/>


Personal
Open source
Business
Explore
Pricing
Blog
Support
Sign in
Sign up
Explore GitHub
Showcases
Integrations
Trending
Trending in open source
See what the GitHub community is most excited about today.
Sign up for free to get started
Repositories
Developers
Trending: today
All languages
Unknown languages
CSS
HTML
Java
JavaScript
PHP
Python
Ruby
future-architect/vuls
Vulnerability scanner for Linux/FreeBSD, agentless, written in Go
Go • 480 stars today • Built by
Star
gravitational/teleport
Modern SSH server for clusters and teams.
Go • 477 stars today • Built by
Star
wbkd/awesome-interactive-journalism
A list of awesome interactive journalism projects.
442 stars today • Built by
FreeCodeCamp/FreeCodeCamp
The https://FreeCodeCamp.com open source codebase and curriculum. Learn code and help nonprofits.
JavaScript • 389 stars today • Built by
spotify/HubFramework
Spotify's component-driven UI framework for iOS
Objective-C • 382 stars today • Built by

1 位（/約1,000万）に！


future-architect/vul...
Github Stars
3070
3000
2800
2600
2400
2200
2000
1800
1600
1400
1200
1000
800
600
400
150
04/06/2016
04/30/2016
05/23/2016
06/15/2016
07/09/2016
08/01/2016
08/24/2016
10/03/2016
GitHub Trendingで世界1位
ThinkIT掲載
JANOG38講演
July Tech Festa講演
GitHub Trendingで世界4位
4/1公開

既存環境にも導入しやすい

- ✓ エージェントレスのため、既存環境への影響が最小限
- ✓ Zabbixへの連携も可能

脆弱性検知結果を出力・加工

ZABBIX スキャンスクリプトをcronに登録し、Zabbixに送信

ZABBIX Zabbixで条件指定、新規脆弱性検知

様々な出力形式に対応

```
$ vuls scan -report-json
$ vuls scan -report-mail
$ vuls scan -report-s3
$ vuls scan -report-slack
$ vuls scan -report-text
```

```
# 脆弱性の数
$ cat vuls/results/current/target1.json |
jq '[.KnownCves[]?, .UnknownCves[]?
| .CveDetail.CveID] | length'
```

79 ← 脆弱性の数を取得

```
# Cvss Scoreの最大値
$ cat vuls/results/current/target1.json |
jq '[.KnownCves[]?, .UnknownCves[]?
| .CveDetail.Nvd.Score] | max'
```

10 ← CVSSスコアを取得

```
#!/bin/bash
VULS_ROOT="/root/vuls"
VULS_RESULT_DIR="$VULS_ROOT/results"

vuls scan -cve-dictionary-
dbpath=$VULS_ROOT/cve.sqlite3 -report-json
files="$VULS_RESULT_DIR/current/*"
for filepath in $files; do
    TARGET_NAME=`basename $filepath .json`
    zabbix_sender -z localhost -s $TARGET_NAME -
k nvd_count -o `cat $filepath | jq
'[.KnownCves[]?, .UnknownCves[]?
| .CveDetail.CveID] | length'`
    zabbix_sender -z localhost -s $TARGET_NAME -
k nvd_max -o `cat $filepath | jq
'[.KnownCves[]?, .UnknownCves[]?
| .CveDetail.Nvd.Score] | max'`
done
```

zabbix senderを使って脆弱性情報を送信するスクリプトを定期実行

ZABBIX

Monitoring | Inventory | Reports | Configuration | Administration

Dashboard | Overview | Web | Latest data | Triggers | Event

History: History » Latest data » History » Latest data » History

target1: number of vulnerabilities

Timestamp	Value
2016-07-12 14:20:34	32
2016-07-12 14:06:03	32
2016-07-12 13:37:38	38
2016-07-12 12:05:00	43
2016-07-11 15:11:14	80

条件指定、新規脆弱性検知、などをZabbixで組み込む

今後、利用が予想される場面

PCIデータ･セキュリティ基準（抜粋）

要件 11:　　セキュリティシステムおよびプロセスを定期的にテストする。

脆弱性は、悪意のある個人や研究者によって絶えず検出されており、新しいソフトウェアによって広められています。システムコンポーネント、プロセス、およびカスタムソフトウェアを頻繁にテストして、セキュリティ管理が変化する環境に継続的に対応できるようにする必要があります。

PCI DSS 要件	テスト手順	ガイダンス
11.1 四半期ごとにワイヤレスアクセスポイントの存在をテストし（802.11）、すべての承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントを検出し識別するプロセスを実施する ***注:*** *プロセスで使用される方法には、ワイヤレスネットワークのスキャン、システムコンポーネントおよびインフラストラクチャの論理的/物理的な検査、ネットワークアクセス制御（NAC）、無線 IDS/IPS が含まれるがこれらに限定されるわけではない。* *いずれの方法を使用する場合も、承認されているデバイスと承認されていないデバイスを両方検出および識別できる機能を十分に備えている必要がある。*	**11.1.a** ポリシーと手順を調べ、四半期ごとに承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントを両方検出し識別するプロセスが定義されていることを確認する。	ネットワーク内でのワイヤレステクノロジの実装と利用は、悪意のある者がネットワークとカード会員データにアクセスするために使用する最も一般的な経路の 1 つです。ワイヤレスデバイスまたはネットワークが企業の知らない間にインストールされた場合、攻撃者はネットワークに容易に、かつ「認識されずに」侵入できます。不正なワイヤレスデバイスはコンピュータまたは他のシステムコンポーネント内に隠れているか、接続している可能性があります。または、ネットワークポートや、スイッチやルーターなどのネットワークデバイスに直接接続している可能性もあります。このような不正デバイスは環境内への不正なアクセスポイントになる可能性があります。 どのワイヤレスデバイスが承認されているかがわかっていると、管理者は承認されていないワイヤレスデバイスを素早く特定でき、承認されていないワイヤレスアクセスポイントの ID に対応することで、悪意のある者への CDE のそれ以上の開示を予防することで被害を最小限にとどめることができます。 ワイヤレスアクセスポイントをネットワークに簡単に接続できること、その存在を検出するのが困難なこと、および権限のないワイヤレスデバイスがもたらすリスクの増加により、ワイヤレステクノロジの使用を禁止するポリシーが存在する場合でも、これらのプロセスを実行する必要があります。 環境内に不正なワイヤレスアクセスポイントがインストールされていないことを確実にするた
	11.1.b 方法が、少なくとも以下を含むすべての不正なワイヤレスアクセスポイントを検出して識別するのに十分であることを確認する。 ▪ システムコンポーネントに挿入された WLAN カード ▪ ワイヤレスアクセスポイントを作成するためにシステムコンポーネントに（USB などで）接続したポータブルやモバイルデバイス ▪ ネットワークポートまたはネットワークデバイスに接続されたワイヤレスデバイス	
	11.1.c 最近のワイヤレススキャンの出力を調べて、以下を**確認**する。 • 承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントが識別される • すべてのシステムコンポーネントおよび施設に対し、このスキャンが少なくとも四半期ごとに実施されている	
	11.1.d 自動監視（ワイヤレス IDS/IPS や NAC など）が使用されている場合は、担当者に通知するための警告が生成されるように構成されていることを確認する。	
11.1.1 文書化されている業務上の理由を含め、承認されているワイヤレスアクセスポイントのインベントリを維持する。	**11.1.1** 文書化されている記録を調べて、承認されているワイヤレスアクセスポイントのインベントリが維持されており、すべての承認されているワイヤレスアクセスポイントに対して業務上の理由が文書化されていることを確認する。	

参照URL: <https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/PCI_DSS_v3.pdf>