CODEBLUE 2024

神戸康多
フューチャー株式会社

自己紹介

神戸康多（かんべこうた）

フューチャー株式会社

OSS脆弱性スキャナ「Vuls」作者

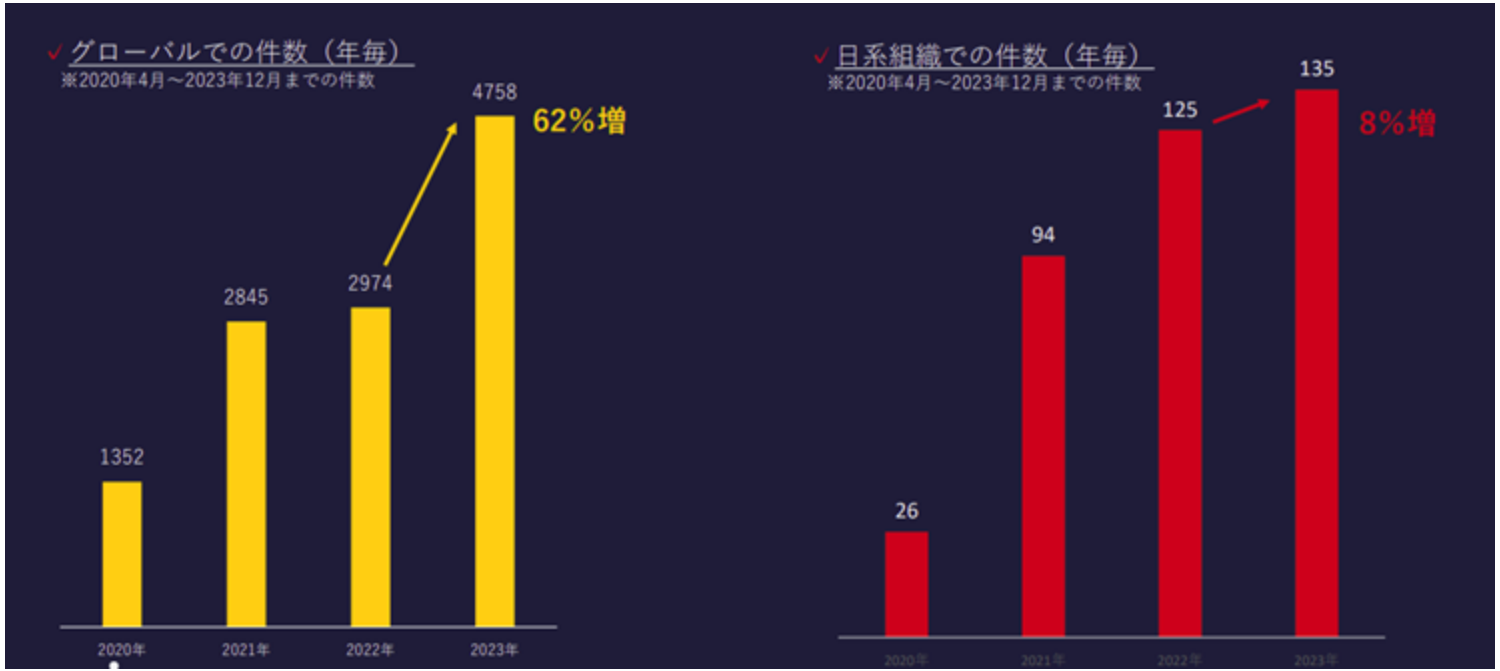
脆弱性管理クラウド「FutureVuls」の運営

実績

- 情報処理学会ソフトウェアジャパン2020 アワード
- BlackHat Asia Arsenal, HITCONなど海外カンファレンス講演
- Google OSS Peer Bonus Winners of 2022

ランサムウェア発生件数

ランサムウェアの被害件数はグローバル・国内ともに年々増加傾向である。
技術の進展に伴い脆弱な機器がネットワーク接続されるケースの増加といった理由で、**最近は情報の価値密度が高いサーバ環境が狙われている**。



出所：株式会社マクニカ セキュリティ研究センター 公開情報から読み解く日系企業のランサム被害傾向

ランサムウェアの侵入経路（国外・国内）

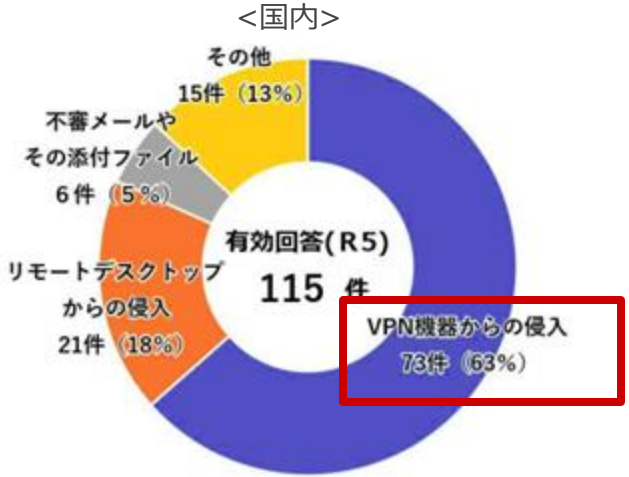
侵入経路は、脆弱性の悪用が一番多い

- グローバルでは、脆弱性の悪用が「36%」
- 国内は「63%」がVPN機器からの侵入（脆弱性の悪用＋弱い認証）

<グローバル>

出所：SOPHOS ランサムウェアの現状2023 年版

<国内>

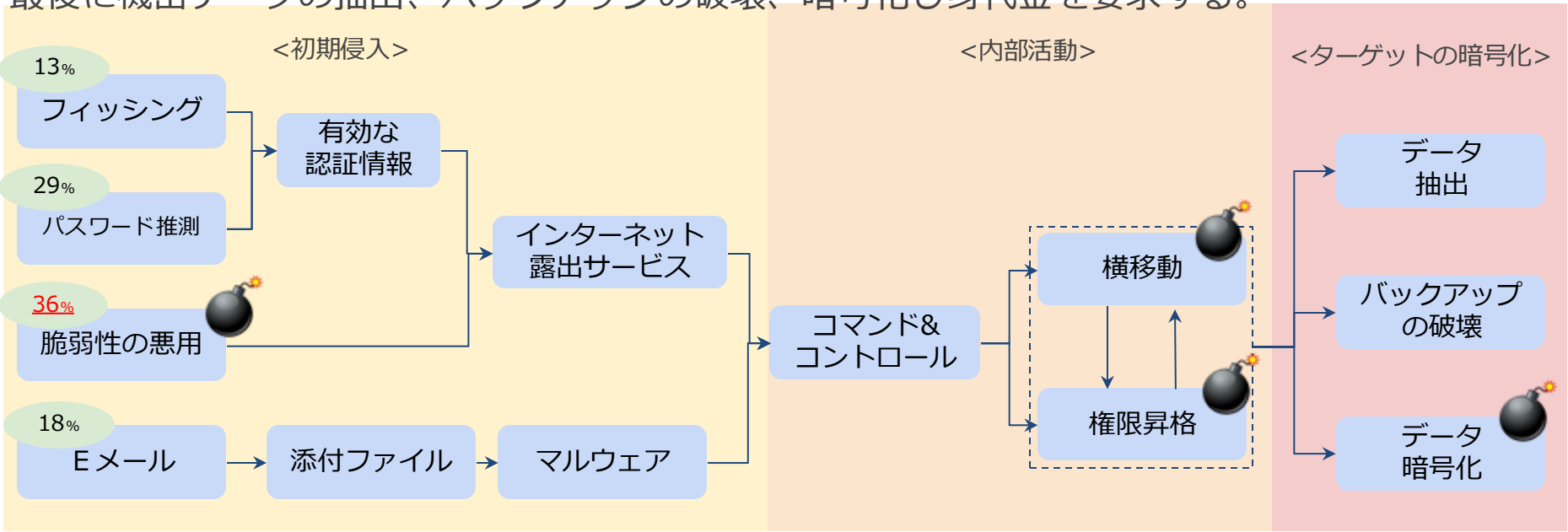


出所：警察庁令和5 年における　サイバー空間をめぐる脅威の情勢等について

ランサムウェア攻撃の各段階と脆弱性の悪用

フィッシング、パスワード推測、脆弱性の悪用、Eメール等で侵入する。
その後、C2への接続、管理者権限への昇格や横方向への移動を行う。
最後に機密データの抽出、バックアップの破壊、暗号化し身代金を要求する。

凡例
侵入の割合

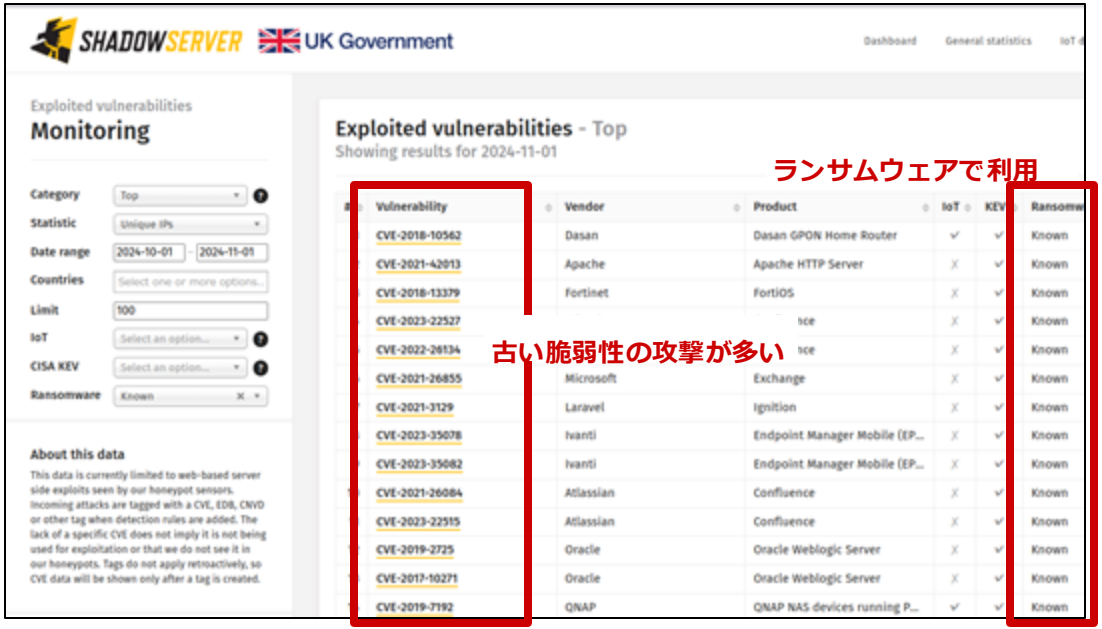


初期侵入だけでなく、横移動・権限昇格などでも脆弱性は悪用される

ランサムウェアグループが悪用する脆弱性とは

ランサムウェアグループはゼロデイ攻撃をド派手にしかけてくる印象があるが、既知の古い脆弱性が狙われるケースも多い。**ランサムウェアキャンペーンで悪用されている脆弱性の全66件のうち「48.5%」が2022年以前のCVEとなっている**（2024/11/11時点）

2023年には、ゼロデイ攻撃が大幅に減少し、攻撃者はより古い脆弱性や既存の認証情報を悪用する傾向が強まっている。



リスクには有効期限が無く、古い脆弱性をそのままにしている場合は餌食となる。

出所: IBM X-Force脅威インテリジェンス・インデックス2024　　ShadowServer: Top100をRansomeware=knownでフィルタ

ランサムグループが利用する既知の脆弱性

CISAのサイトを「#stopransomware」で検索し、ランサムグループの詳細情報を見ると古くてインパクトが大きい脆弱性が継続的に使われていることがわかる。

CISA-KEVの「**1,207件中239件（19.8%）**」がランサムキャンペーンで悪用されている。

古い脆弱性も使われている

グループ名	段階	CVE-ID	概要
LockBit	初期侵入	CVE-2021-44228	Log4Shell
		CVE-2021-26855	ProxyLogon
Black Basta	初期侵入	CVE-2024-1709	Citrix
	横移動・権限昇格	CVE-2020-1472	ZeroLogon
		CVE-2021-34527	PrintNightmare

出所：CISAのサイトを「#stopransomware」で検索

ランサムウェア対策において脆弱性管理は必須である

CISA#Stopransomwareのランサムグループ詳細ページには「脆弱性管理とパッチ適用をせよ」と書かれている。脆弱性管理は基本中の基本であり、当然やらないといけない。

また、CISAの2023年に悪用された脆弱性TOP15には、「悪意のあるサイバー攻撃者は、脆弱性が**公開されてから 2 年以内に脆弱性を悪用**することに最も成功し続けています」

出所：CISAのサイトを「#stopransomware」で検索

CISA 2023 Top Routinely Exploited Vulnerabilities

「家に最先端の防犯システムがあっても、窓が割れたまま放置してたら侵入し放題になる」

脆弱性管理の進化（手動 → 自動）

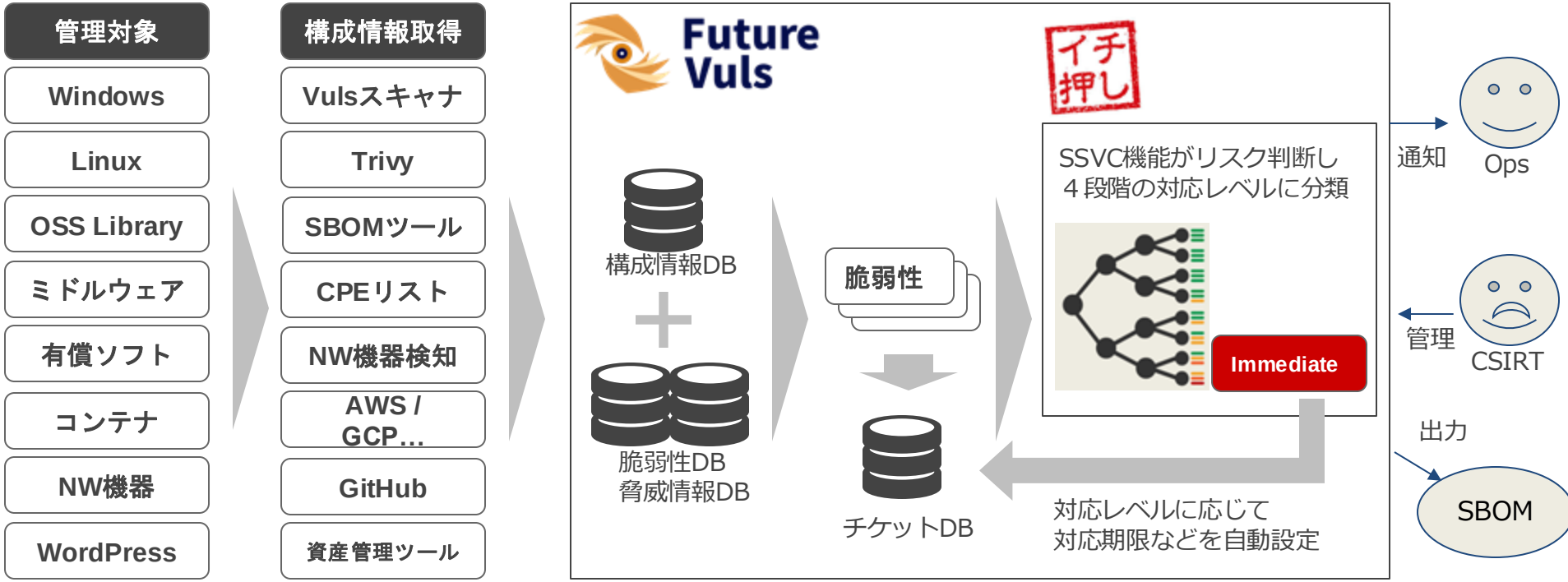
これまで主流だったCVSSスコアでの判断では絞り込みができず実運用が回らない。脅威情報を元に実際に悪用されている「5%」を特定し、優先的に対応するのがトレンドである。

	これまで（手動）	現在（自動）
資産と脆弱性の特定	● 手動の資産管理 ● 手動の脆弱性情報収集 ● 手動の影響調査	● スキャナやSBOMで資産登録 ● 自動でNW機器を特定 ● 自動で脆弱性検知
リスク判断	● CVSS≧7.0は全て対応 ● 手動で脅威情報の収集 ● 手動で判断し社内メール送付	● 実際に悪用される5%を特定 ● リスクを自動判断（SSVC） ● 自動で対応指示
対応	● 手動でパッチ、仮想パッチ適用 ● 手動での対応状況管理（Excel） ● 手動でメールで対応を催促	● 自動でパッチ、仮想パッチ適用 ● 自動で対応状況を管理 ● 自動で対応催促

次ページよりランサムウェア対策の観点からFutureVulsの機能を紹介

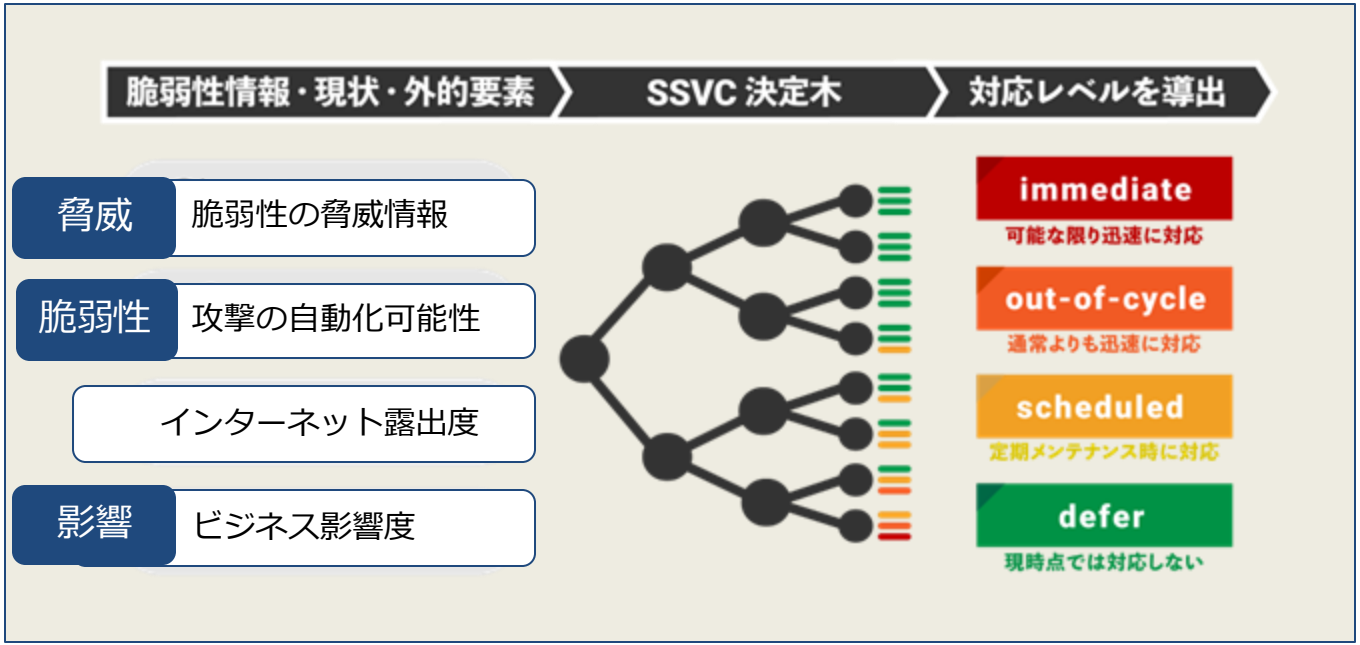
FutureVulsの脆弱性管理の全体像

FutureVulsは全社の資産と脆弱性を一元管理。検知した脆弱性のリスクを自動判断し、運用者に対応を自動指示。セキュリティ管理者は画面上で対応状況を追跡し催促も可能。



SSVC - 米国政府推奨のCVSSの課題を解決するトリアージ手法

FutureVulsのSSVC機能は**『リスク = 脆弱性 x 脅威 x 影響』**を考慮して対応優先度を４段階に自動で決定する。「インターネット公開の重要システム」を想定して分類したところ、**immediate**と**out-of-cycle**を全体の**1.5%**まで絞り込めた。



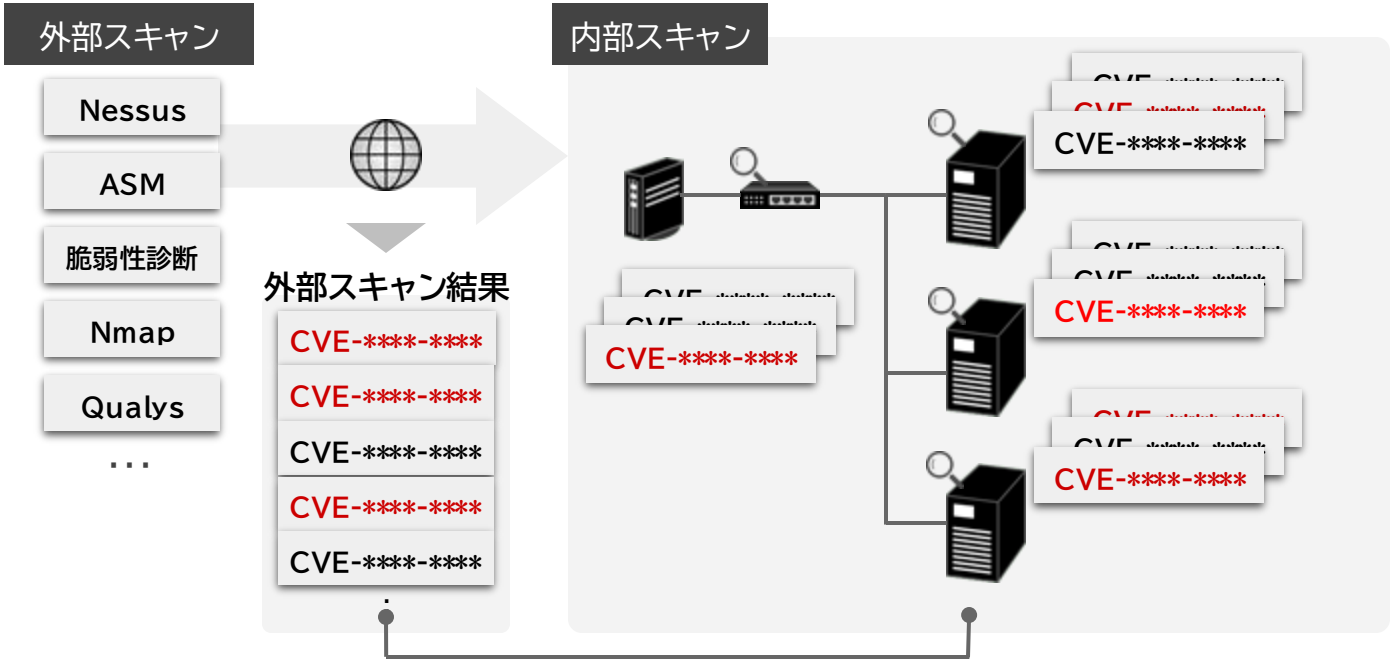
FutureVulsのランサム対策機能：ランサムウェア悪用フィルタ

ランサムウェアキャンペーンで悪用されている脆弱性を全社横断でチェックできる。
CISA KEVとVulnCheck KEVに定義されている、ランサムウェアキャンペーン悪用情報を用いて、検知された脆弱性をフィルタし、対応状況を確認可能。一括操作で対応を指示。

初期侵入はもちろん、横移動、権限昇格に使われる脆弱性も可視化できる

FutureVulsのランサム対策機能：外部スキャンインポート

外部スキャン結果をインポート可能。内部で検知された脆弱性のうち、ランサムウェアの初期侵入に使われる「インターネットに露出している脆弱性」を画面上で特定できる。



FutureVuls で内部・外部の脆弱性を関連付けて統合管理

FutureVulsのランサム対策機能：外部スキャンインポート

「外部スキャン列」がチェックされた脆弱性はインターネットに露出中の脆弱性である。
さらに「ランサムで利用」マークがついているものは緊急対応が必要と判断できる。

さらに該当する「システム > サーバ > ライブラリ」をドリルダウンで特定できる

FutureVulsのランサム対策機能：EPSSでのソートと対応催促

検知された脆弱性を、EPSS（今後30日以内に悪用される可能性）でソート可能。
高リスクな脆弱性を放置している担当者に一括で対応を指示できる。

警戒情報	Immediate...	Out of Cyc...	SSVC最高...	Exploit信...	サマリ	EPSS Score	EPSS Percentile
⚠	0	1	out_of_cy...		Apache Tomcat における入力確認に関す...	97.50%	99%
-	0	0	scheduled		Action View における脆弱性	97.45%	99%
⚠	0	1	out_of_cy...		複数のフォーティネット製品における認...	97.37%	99%
⚠	1	0	immediate		Apache Tomcat の複数の脆弱性に対する...	97.37%	99%
-	0	0	scheduled		OpenSSL の AES-NI の実装における重要...	96.90%	99%
-	0	0	scheduled		Rails におけるコードインジェクションの...	96.50%	99%
⚠	0	1	out_of_cy...		sudo にヒープベースのバッファオーバー...	96.33%	99%
-	0	0	scheduled		OpenBSD の OpenSSH 等複数ベンダの...	96.25%	99%
⚠	0	1	out_of_cy...		Google Chrome におけるバッファエラー...	94.84%	99%
-	0	0	scheduled		Apache Tomcat に安全でないデシリアラ...	91.41%	99%
-	0	0	scheduled		Apache Tomcat における複数のサービス...	91.22%	98%
-	0	0	-		Git におけるリンク解釈に関する脆弱性	84.99%	98%
-	0	0	scheduled		OpenSSL の ASN.1 BIO の実装の crypto/...	84.35%	98%
⚠	4	1	immediate		インターネット技術タスクフォース (IET...	83.78%	98%
-	0	0	scheduled		Apache Tomcat におけるオープンリダイ...	78.91%	98%
-	0	0	scheduled		Apache Tomcat におけるリソースの枯渇...	72.67%	98%

EPSSを用いれば、近い将来悪用されそうな脆弱性を補完できる

FutureVulsのランサム対策機能：ソフトウェア横断検索

ゼロデイ脆弱性や大きな話題となっている脆弱性のニュースが公開された際に、対象ソフトウェアを全社横断で検索可能。

表示されたシステム、サーバ、バージョン番号をもとに影響を判断して注意喚起できる。

グループID	グループ名	サーバ名	ソフトウェア	CPE	バージョン
2320	Webアプリ A	NW機器	fortigate-1000d	cpe:2.3:h:fortinet:fortigate-1000d:*:*:*:*:*:*:*:*	ANY
2320	Webアプリ A	NW機器	fortios	cpe:2.3:o:fortinet:fortios:7.2.0:*:*:*:*:*:*:*	7.2.0
2336	sudoadmin	forti	fortios	cpe:2.3:o:fortinet:fortios:5.4.0:aaaa:*:*:*:*:aaa:*	5.4.0
2320	Webアプリ A	NW機器	fortigate	cpe:2.3:h:fortinet:fortigate:*:*:*:*:*:*:*:*	ANY

まとめ

ランサムウェア対策の基本は脆弱性管理

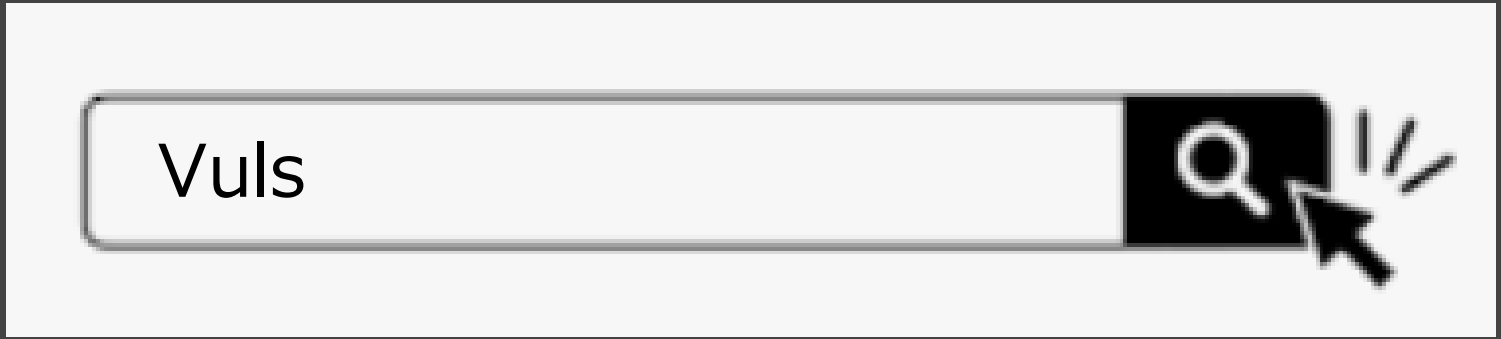
ゼロデイ攻撃が騒がれ目立つが、古くてインパクトの大きい脆弱性も継続的に使われている

リスクベースでの脆弱性管理が主流

FutureVulsでは、無償公開の脅威情報で実際に悪用されている「5%」の脆弱性を特定し、さらにSSVCで『リスク = 脆弱性 x 脅威 x 影響』を判断できる

FutureVulsは徹底的に自動化可能

FutureVulsは脆弱性管理のプロセスを**徹底的に自動化**。少人数でも運用がまわる



FutureVuls Blogでスライドと全文ログを公開予定です
展示ブースでお待ちしてます