AIによるソフトウェア脆弱性対応ソリューション

VR/manager

Rakusol
株式会社 ラクソル

脆弱性対策のために公開された脆弱性情報を攻撃者が悪用

脆弱性情報の公開後、攻撃コードが流通して
攻撃が本格化するまでの時間が近年は短くなっている傾向

順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	NEW

ソフトウェアの脆弱性対策で
対応が可能な脅威

※引用：IPA「情報セキュリティ10大脅威2022」
https://www.ipa.go.jp/security/vuln/10threats2022.html

01 - ネットワーク機器のソフトウェア脆弱性対策の必要性

VPN装置の脆弱性によりトヨタグループの国内全工場が終日停止

（出典）https://xtech.nikkei.com/atcl/nxt/mag/nc/18/092400133/030900072/

ネットワークセキュリティー装置を手掛ける米ソニックウォールが2021年12月から2022年2月にかけて公表した、
VPN（仮想私設網）装置「Secure Mobile Access（SMA）100」シリーズの複数の脆弱性である。
脆弱性を悪用されると、認証情報が盗まれるなどの被害に遭う恐れがある。日本ではセキュリティーの民間団体であるJPCERTコーディネーションセンター（JPCERT/CC）が2022年1月と2月に、同脆弱性を狙ったサイバー攻撃に関する注意喚起を出している。ただSMA100シリーズの脆弱性と、今回の小島プレスやGMBへのサイバー攻撃との関連は現時点で不明だ。

VPN装置の脆弱性を悪用するランサムウエア攻撃は以前から目立つ。新型コロナウイルス禍でテレワークが増え、VPNに注目が集まるなか、
多くの企業や組織は脆弱性を放置する危険性を認識しているはずだ。
だが、「従業員向けのVPN装置と別に設置する、保守用のVPN装置が盲点となりやすい」とS&Jの三輪社長は指摘する。

存在を認識していなければ、当然ながら脆弱性は放置される。犯罪者集団から見れば、不正侵入に格好の入り口となるわけだ。加えて、多くの企業が使う米マイクロソフトのID管理システム「Active Directory（AD）」にも注意が必要だ。ランサムウエア攻撃の犯罪者の多くはADを乗っ取り、配下の端末に暗号化モジュールをばらまくからだ。

（出典）https://www.yomiuri.co.jp/national/20220614-OYT1T50054/amp/

ウイルスの侵入口は、小島プレスの子会社の通信用機器だったことが判明。機器には、攻撃を受けやすい 脆弱性があった。

解 説

複数の報道によると、2022年3月1日に公表された小島プレス工業のマルウェア感染被害によりトヨタグループ14工場28ライン（日野自動車、ダイハツ工業の一部を含む）が操業停止となりました。
このマルウェアの侵入経路は、小島プレス工業の子会社が使用していたVPN装置「Secure Mobile Access（SMA）100」（米国・ソニックウォール社製）の脆弱性であるとされています。
ソニックウォール社の製品については、2020年以降に3件の深刻度「緊急（CVSS v3）」の脆弱性が報告されており、これらの脆弱性を突いたサイバー攻撃により今回の被害が発生した模様です。
脆弱性の報告からサイバー攻撃までの間には、脆弱性対策を行うための十分な時間があったことから、日々自社のIT資産に関する脆弱性の情報を入手し対策を講じていれば被害を未然に防ぐことができたと思われます。

大阪の某総合医療センターにサイバー攻撃、取引先の脆弱性突く

（出典）https://www.security-next.com/141214/2

某給食会社のリモートメンテナンス用のVPN装置として設置されていたVPN製品への攻撃が発端。栄養給食管理システムのサーバからは、攻撃者が用いたランサムウェアやツールのフォルダが発見されており、攻撃対象とされたIPアドレスやパスワードなどの情報も含まれていた。
「Active Directoryサーバ」には、各サーバに対するログオンが失敗した大量のログが残存。特定のIDや複数のパスワードを組み合わせ、ログオンを試行する「総当たり攻撃」が行われたものと見られる。またセキュリティ機能が無効化された形跡なども見つかった。

（出典）https://www.asahi.com/articles/ASQC75HZ5QC7ULZU00N.html
攻撃に用いられたランサムウエアはPhobosの亜種「Elbie」と思われる。

（出典）https://www.fortinet.com/jp/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials
クラッカーにより、2019年8月より複数回にわたり87,000台のFortiGate SSL-VPNデバイスへのSSL-VPNアクセス情報を公開された。

解 説

大阪の某総合医療センターに対して2022年10月31日にサイバー攻撃があり、電子カルテやオーダーを含めた基幹システムが停止しました。
この影響でほぼ全ての科が診療停止し、手書きのカルテに切り替えて診療するなどの対応をしながら、順次システムの復旧を行いました。
年を越した2023年1月11日にシステムが完全復旧し通常業務に復帰しました。

システム停止に至った発端は、医療センターを中心とした医療サービスのサプライチェーンを構成する給食会社へのサイバー攻撃でした。
医療センターの給食業務を担っていた給食会社のデータセンターに、システムのリモートメンテナンス用として「Fortinet製　FortiGate 60E」というVPN製品が設置されていました。

このVPN製品には2018年7月に公開されたパストラバーサル（公開していないフォルダが参照可能となる）の脆弱性があり、給食会社の機器は、この脆弱性に対応したソフトウェアのバージョンにアップグレードされていませんでした。某調理センターのVPN製品を踏み台に、栄養給食管理システムがクラックされ、さらにそこからサプライチェーンで接続されている医療センターのActive Directoryサーバがブルートフォースにより攻撃され基幹システムの停止に至りました。

4 ソフトウェア脆弱性の基本対策事項

「政府統一基準」で求められるソフトウェアの脆弱性対策

「政府統一基準」は、国内の政府機関が実施すべき対策の指針を示したもので、
具体策として「政府機関等の対策基準策定のためのガイドライン」が示されています。
ソフトウェアの脆弱性対策については、「政府統一基準」P42 6.2.1項 ソフトウェアに関する脆弱性対策、
並びに、「ガイドライン」P198 6.2.1項 ソフトウェアに関する脆弱性対策にて示されています。

基本対策事項

- 01 脆弱性情報の入手
- 02 サポート終了製品の利用禁止
- 03 脆弱性の存在確認
- 04 定期的な脆弱性の確認
- 05 脆弱性対策計画策定
- 06 脆弱性対策実施状況の確認
- 07 脆弱性対策実施状況の記録
- 08 信用できる方法での対策ファイルの入手

5 VRmanagerによる各対策事項の実現方法

政府統一基準対策事項	VR/manager 機能
01 脆弱性情報の入手	**脆弱性情報の収集機能**（JVN-APIによる自動収集） P-09へ
02 サポート終了製品の利用禁止	**脆弱性辞書によるフラグ管理機能** P-09へ
03 脆弱性の存在確認	**脆弱性リスクを有する資産特定機能** （インベントリ収集システムと自動連係） P10,P11へ
04 定期的な脆弱性の確認	**脆弱性情報の収集機能**（JVN-APIによる自動収集） P-09へ
05 脆弱性対策計画策定	**脆弱性リスク評価機能** P12,P13へ （CVSS情報等を元に組織としての当該脆弱性対応要否を設定）
06 脆弱性対策実施状況の確認	**脆弱性対策機能** P-14へ （当該資産の管理者にアラート通知され脆弱性対応ワークフローが自動起票）
07 脆弱性対策実施状況の記録	**脆弱性対応状況管理機能** P-15へ （脆弱性対応ワークフローのステータス管理）
08 信用できる方法での対策ファイルの入手	**脆弱性対策機能** P-14へ （対策依頼にセキュリティパッチファイルを添付可能）

6 VRmanagerの仕組み

JVN Japan Vulnerability Notes

JVN
日本の脆弱性データベース

脆弱性情報を公開

MYJVN APIを利用して自動連携

VR/manager

01
AI
JVNの脆弱性情報を**AIモデル が自動で辞書登録**

脆弱性情報辞書

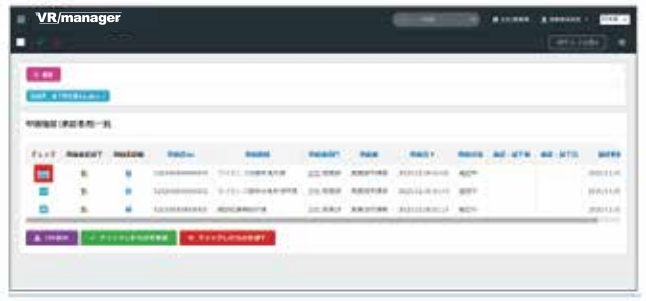
02
組織内に存在する**脆弱性を管理者に通知**

03
脆弱性の内容を**確認し対応方法を管理者が入力**

ワークフロー
- 脆弱性情報
- 脆弱性対策方法
- セキュリティパッチ

04
ユーザが脆弱性対応を実施しワークフローで**管理者に報告**

VRmanager ユーザー管理画面



Rakusol 株式会社 ラクソル

JVN の脆弱性情報を自動収集

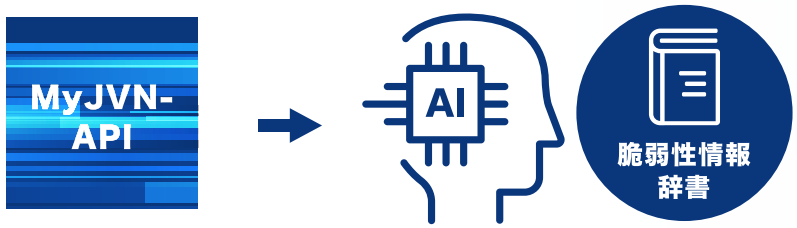
APIを利用して脆弱性対策情報を取得し、取得した情報をAIを用いて脆弱性辞書に分類します

☑ 脆弱性情報はJVNの情報を利用します

JVN は「Japan Vulnerability Notes」の略で日本で使用されているソフトウェアの脆弱性関連情報と対策情報が提供されます。IPA と JPCERT により運営されています。

☑ MyJVN-APIによる自動収集

My JVN API は、JVNの情報をWebを通じて利用するためのWEBインターフェースです。My JVNが提供するAPI を利用して脆弱性対策情報を取得し、取得した情報をAIを用いて脆弱性辞書に分類します。



脆弱性対策情報取得

取得した情報を
AIが脆弱性情報辞書に分類

脆弱性対策情報例

JVN iPedia 脆弱性対策情報データベース

JVNDB-2021-002977
Adobe Reader および Acrobat における解放済みメモリの使用に関する脆弱性

概要

Adobe Reader および Acrobat には、解放済みメモリの使用に関する脆弱性が存在します。

想定される影響

CVSS v3 による深刻度　基本値: 8.8 (重要)

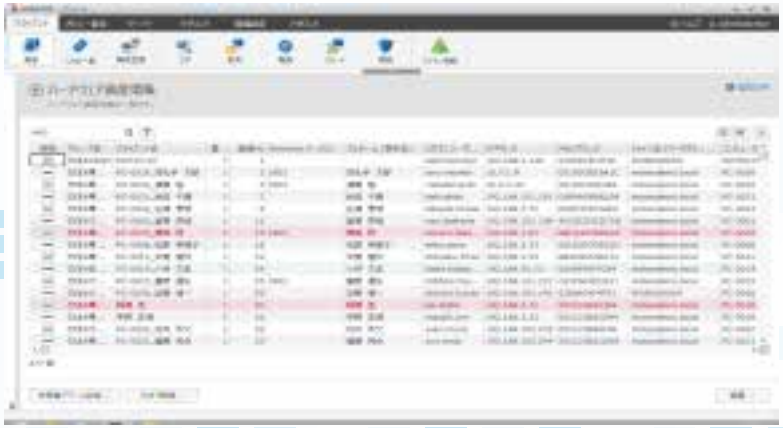
対策

Adobe Acrobat Reader DC 2017 (Classic 2017) 2017.011.30190 未満
Adobe Acrobat 2020 (Classic 2020) 2020.001.30020 未満
Adobe Acrobat 2017 (Classic 2017) 2017.011.30190 未満
Adobe Acrobat DC (連続トラック) 2021.001.20135 未満

7 02- 脆弱性リスクを有する資産特定機能

☑ インベントリツールで取得したPC/サーバのインベントリ情報を定期取り込み、
リスクを有する資産を特定

インベントリ収集ツール



インベントリ情報を
VRmanagerへ
定期取込

VR/manager

【インベントリ情報収集】

ハードウェア・ソフトウェア情報（インベントリ情報）を自動収集。
VRmanager は、主要なインベントリツールの
出力レイアウトに対応が可能です。
※インベントリ情報と組織・ユーザ情報の連携キーとして
機器管理番号が必要です。

【脆弱性リスクを有する資産の特定】

インベントリ収集システムからインベントリ情報を
定期的に取り込み、台帳を自動作成します。
各ハードウェアにインストールされているソフトウェアの情報も
定期的に取り込み、データベースに格納し、JVNの脆弱性情報を
元にリスクのある資産を特定します。

7 03- 脆弱性リスクを有する資産特定機能

☑ **SNMPマネージャで取得したネットワーク機器のMIB情報を定期取り込み、リスクを有する資産を特定**（標準でZABBIXで取得したMIB情報を取り込むことが可能です）

ZABBIX

MIB情報を
VRmanager
へ定期取込

VR/manager

【ネットワーク機器のMIB情報収集】

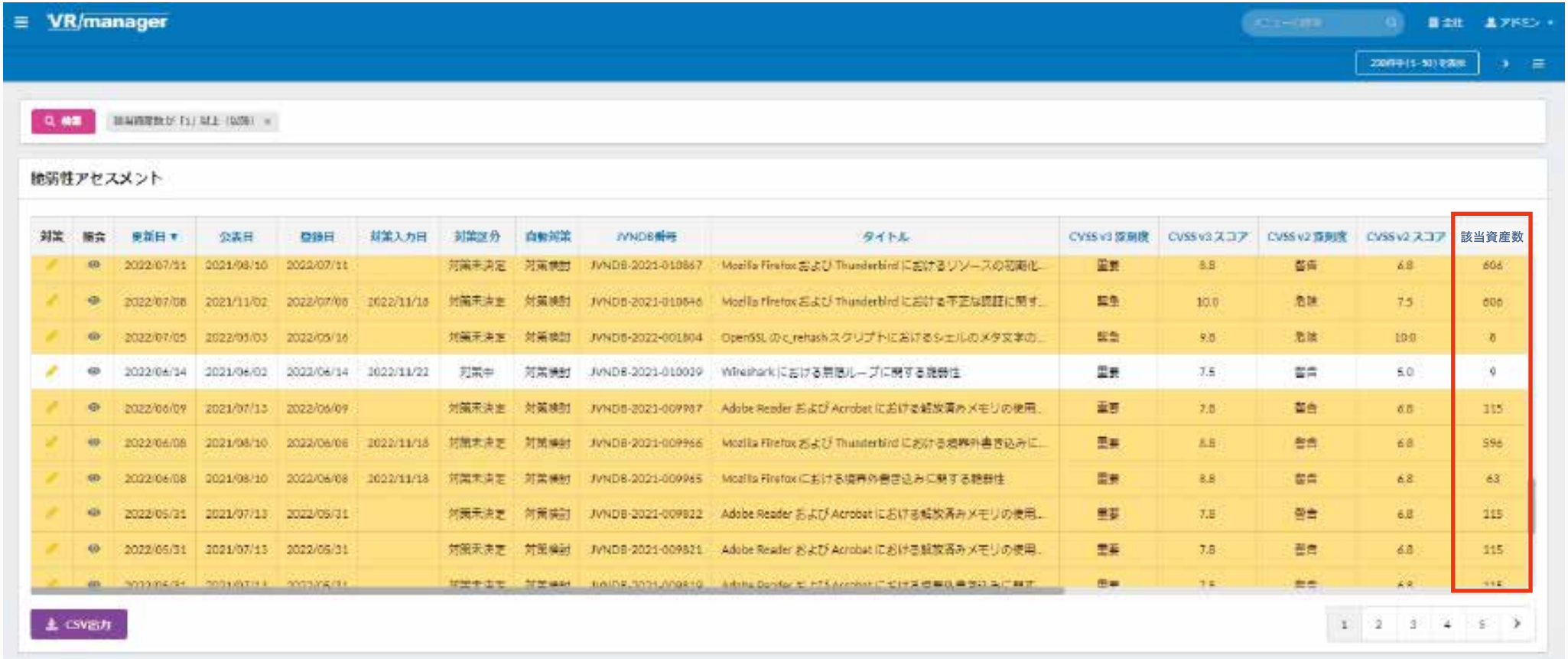
ZABBIXが収集したネットワーク機器等のMIB情報
（sysDescr:システムの詳細情報）をファイルで出力します。
VRmanager は、標準でZABBIXのMIBファイルに対応しています。
※MIB情報と組織・ユーザ情報の連携キーとして
ホスト名のハードウェア台帳への事前登録が必要です。

【脆弱性リスクを有する資産の特定】

ZABBIXが収集したネットワーク機器等のMIB情報を定期的に
取り込み、台帳を自動作成します。
取り込んだMIB情報をデータベースに格納し、JVNの
脆弱性情報を元にリスクのあるネットワーク機器等を特定します。

7 04- 脆弱性対策計画策定

- 組織内に該当するIT資産がある脆弱性を一覧表示
- インベントリ情報と脆弱性辞書の内容を突合し、組織内に存在する脆弱性毎に脆弱性の情報と該当資産数等を表示します。



7 05- 脆弱性対策計画策定

☑ 脆弱性の内容を確認しリスクアセスメントを実施

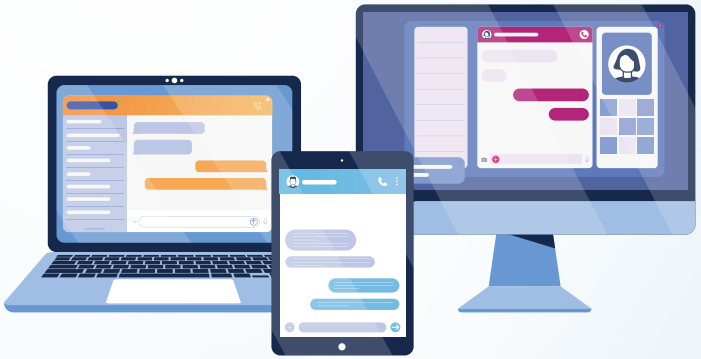
脆弱性の詳細画面では主に以下の内容が確認できます。

1. 公表日・登録日
2. タイトル
3. 概要
4. 影響を受けるシステム
5. 想定される影響
6. 対策方法
7. ベンダ情報
8. 深刻度のスコア（CVSS）

これらの情報や組織内の脆弱性対象資産数を基にリスクアセスメントを行います。

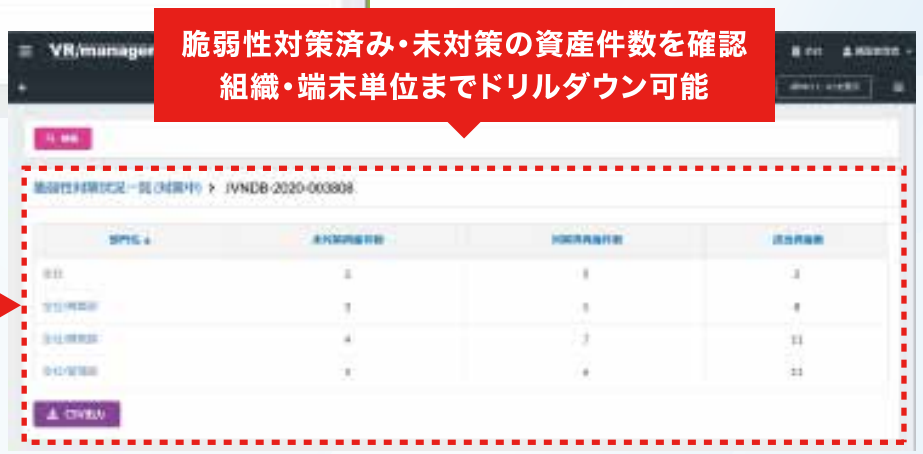
7 06- 脆弱性対策

- 脆弱性対応ワークフローの進捗状況を確認
- 対応中の脆弱性一覧、JVNDB 番号、タイトル、開始日時、脆弱性詳細、対応状況毎の対象資産数を確認できます



07- 脆弱性の対応状況管理

- 脆弱性対応ワークフローの進捗状況を確認
- 対応中の脆弱性一覧、JVNDB 番号、タイトル、開始日時、脆弱性詳細、対応状況毎の対象資産数を確認できます。



8 VRmanager 価格について

初期導入 価格表		ver. 7.3
品名	参考定価	備考
クラウドサーバ設定	¥154,000	VPC設定、セキュリティグループ設定、インスタンス設定、監視設定等
インベントリ連携設定	¥385,000	定期的に資産管理ツールからのインベントリファイルを サーバ連携し取り込みます。
組織・ユーザマスタ設定	都度お見積り	組織及びユーザマスタを設定します。
シングルサインオン設定	都度お見積り	認証基盤に合わせてシングルサインオン設定します。
リモートサポート（人日）	¥69,000	リモートからお客様クラウドサーバに対して導入サポートを行います。

年間システム利用料 価格表	
年間システム基本利用料（参考定価）	
端末1台※	¥3,600

※最小契約台数は**100台以上**、1台単位