これは助かる！ありそうでなかった運用フレームワーク

～脆弱性管理の手引き～

日本シーサート協議会
脆弱性管理WG

目次

はじめに

- 日本シーサート協議会の脆弱性管理WGより、
  ユーザ（システム管理者）の立場での脆弱性管理についてまとめた
  手引書を一般公開いたしました。

https://www.nca.gr.jp/activity/pub_doc/_10.html

- 現在上記の手引書をもとにトレーニングコンテンツを作成中です

- 本日はトレーニングコンテンツとして再構成中の資料をもとに、
  ユーザ（システム管理者）としての脆弱性管理ではどのようなことを
  実施する必要があるのかを解説いたします。

はじめに（日本シーサート協議会　組織概要）

● 設立
2007年3月（2020年4月より一般社団法人として活動開始）

● 名称
正式名称：一般社団法人 日本シーサート協議会
略称：日本シーサート協議会
英語名：NIPPON CSIRT ASSOCIATION
ウェブ： https://www.nca.gr.jp/

CSIRT
日本シーサート協議会

● 使命
本協議会の全会員による緊密な連携体制等の実現を追及することにより、
会員間に共通する課題の解決を目指す
社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る

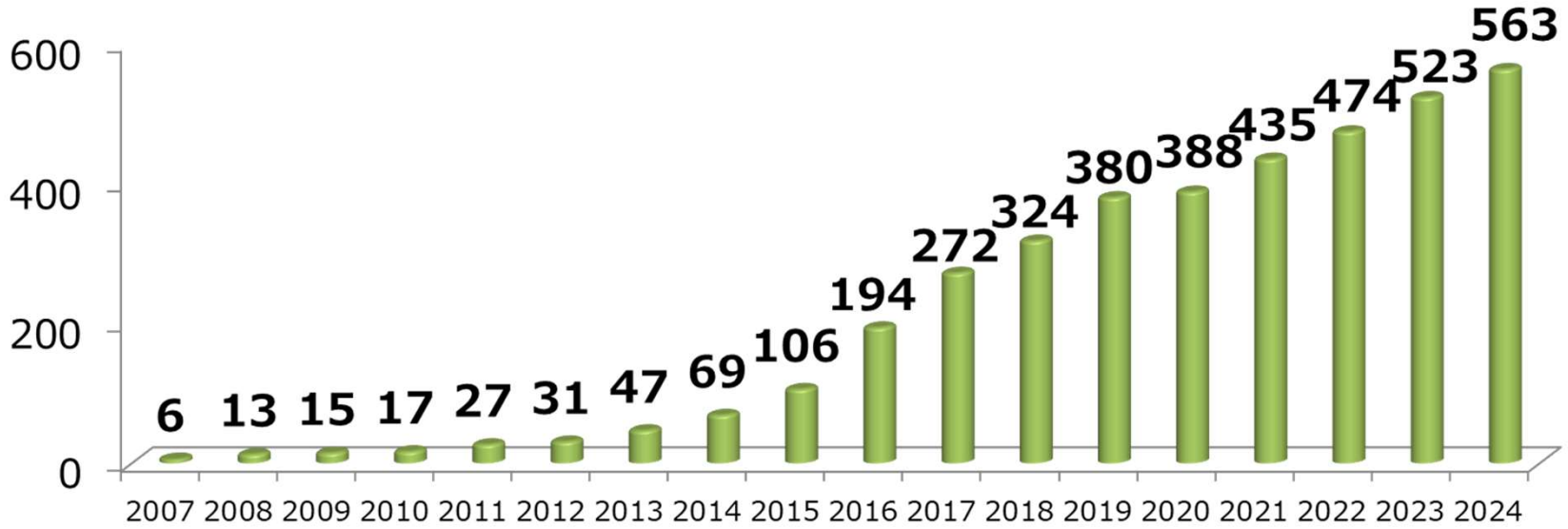
はじめに（日本シーサート協議会　活動概要）

- さまざまな場の提供
  -シーサート間の交流の場
  -シーサート間の連携のあり方に関する検討の場
  共有方法検討等
- シーサート構築支援
- シーサート活動支援
  -セキュリティインシデントへの対応支援
  -事例情報提供、対策情報提供等

CSIRT
日本シーサート協議会

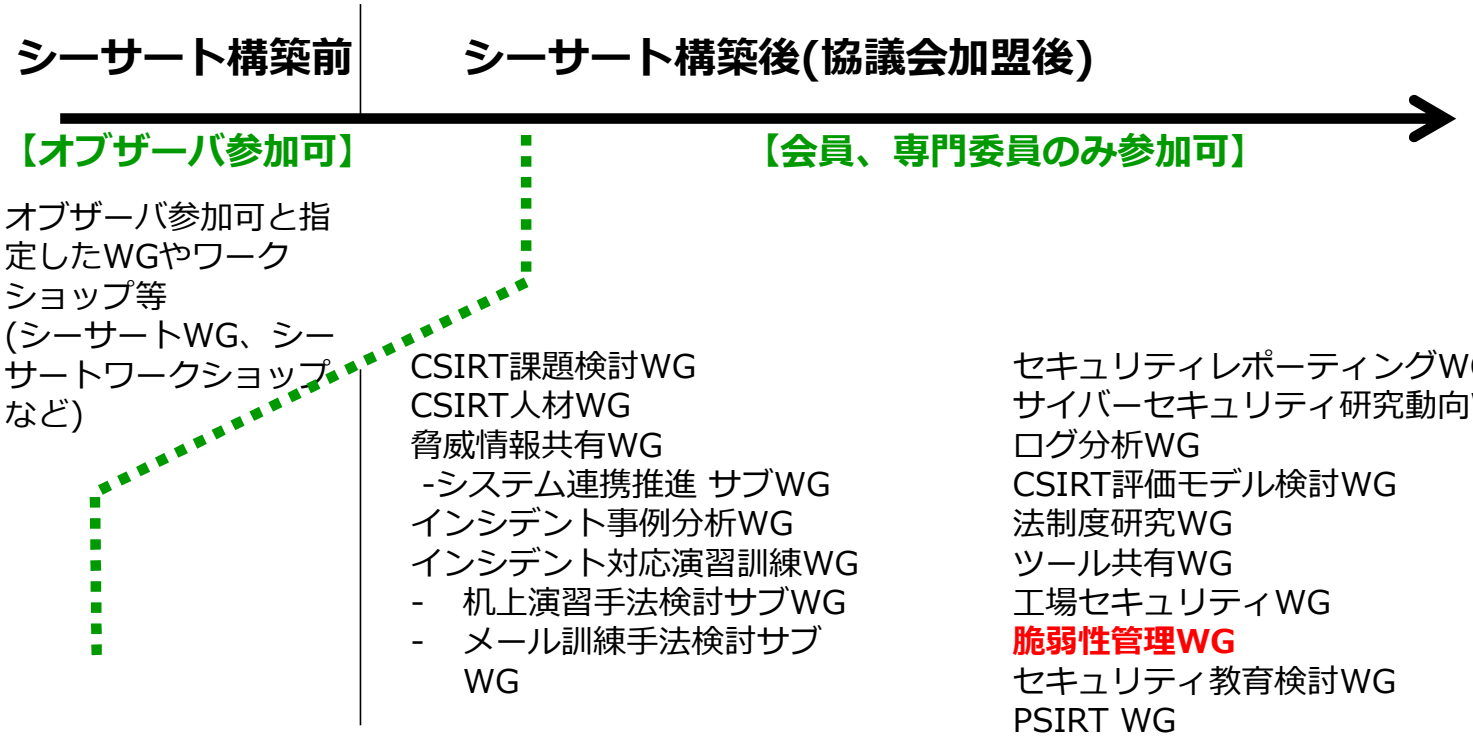
はじめに（日本シーサート協議会加盟数(累積)の推移）

日本シーサート協議会の加盟チーム数も順調に伸び、
累積で563チームとなりました(2024年10月現在)



はじめに（日本シーサート協議会ワーキンググループ）

問題提起と解決のための活動としてワーキンググループを立ち上げ、
会員ならびに協議会外部の協力者と共に、問題解決を図っていきます。
https://www.nca.gr.jp/activity/index.html



はじめに（脆弱性管理WG）

・目的
脆弱性管理WGでは脆弱性管理のあるべき姿
（を踏まえて理想と現実の折り合いをどのようにつけるか）について、
多様な業種の皆様と議論し、知見を蓄積すること

・運営体制

主査	：石田悠	NTT WEST-CIRT
副主査	：柴田はるな	NTT WEST-CIRT
	大石眞央	NTTDATA-CERT

自己紹介(いしだ)

- 石田 悠(イシダ ユウ)
  - NTT西日本　セキュリティ＆トラスト部
  - 　NTT WEST-CIRT
  - 　CISSP、CCSP、 Certified SIM3 Auditor

- 経歴
  - 2010年　：NTT西日本入社
  - ～2018年：ひかり電話の方式検討・運用・監視
  - ～現在　　：脆弱性管理業務

- 日本シーサート協議会での活動
  - 2018年～：関西地区活動委員
  - 2022年～：脆弱性管理WG主査として活動

自己紹介(オーイシ)

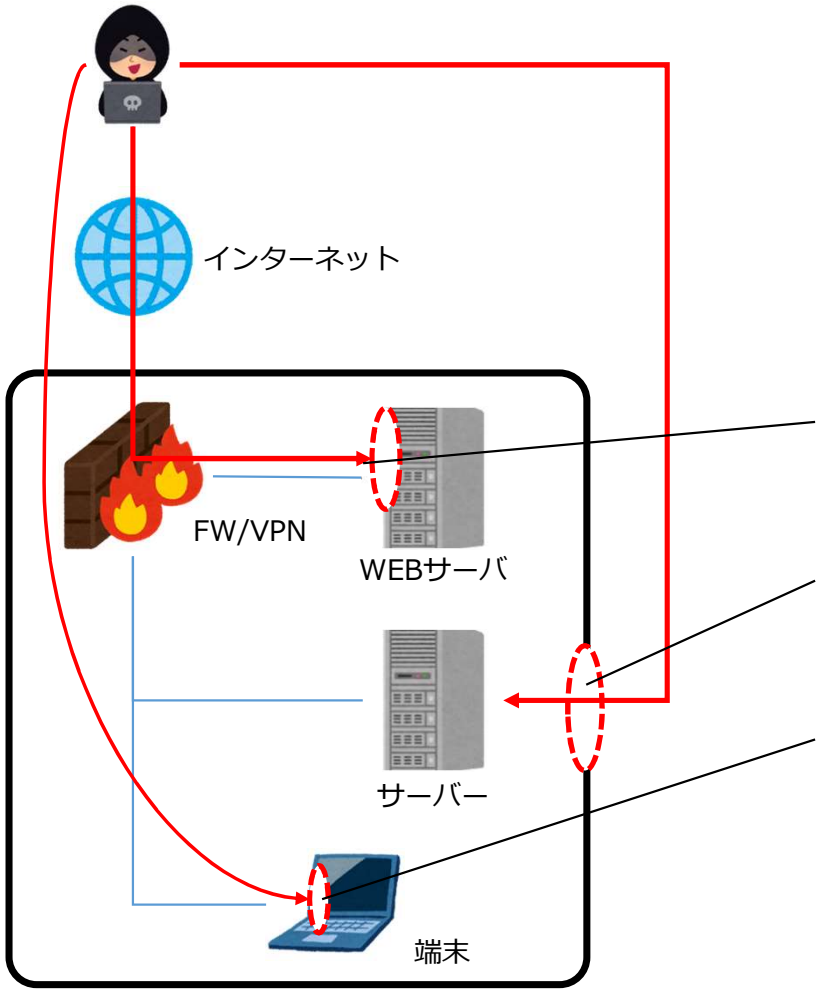
- 大石眞央(オーイシマサオ)
  - 株式会社NTTデータグループ
    - 情報セキュリティ推進室 NTTDATA-CERT
  - CISSP, GCIH, GCTI, GSTRT, RISS Certified SIM3 Auditor
- 経歴
  - 某通信会社
    - 霞ヶ関の客先でセキュリティ業務
    - 主にSOCアナリスト+顧客対応
  - 某ベンチャー企業
    - セキュリティ部署の立ち上げ
    - 脆弱性管理SaaS開発協力 etc.
  - 2019.03より現職
    - 脆弱性対応とインシデント分析Tのリーダー
    - IPA 10大脅威選考会メンバー (2020 --)
    - NCA 脆弱性管理WG副主査
    - グローバル動向四半期レポート メインライター (2019.04 – 2020.03)

自己紹介(しばた)

- 柴田　はるな（シバタ　ハルナ）
  - NTT西日本　セキュリティ＆トラスト部
  - CISSP, CCSP, 個人情報保護士
    Certified SIM3 Auditor
- 業務経験
  - 2016年入社
  - ログ分析・セキュリティ機器運用（～2019年）
  - 脆弱性管理（～現在）
- 日本シーサート協議会での活動
  - NCA 脆弱性管理WG副主査
  - TRANSITS講師
  - 関西地区活動委員

脆弱性と脆弱性管理

脆弱性とは



- プログラムや設定上の問題に起因する「弱点」
- 悪用できるバグ
- 守るべき情報資産・機能に対する意図しない経路

例：WEBサーバの設定上の問題

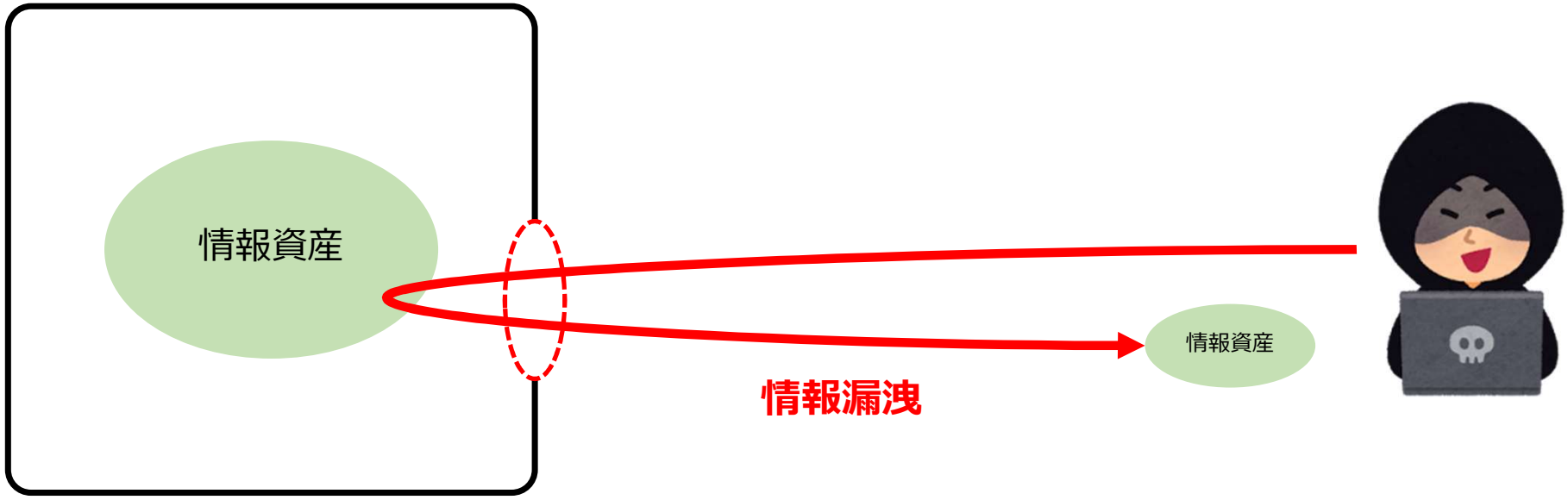
例：リモート保守のために勝手に開けられた経路

例：利用しているアプリケーションの不具合

脆弱性を放置すると何が起こるか①

■情報漏えい

・機密情報や個人情報などの内部に留めておくべき情報が外部に漏れてしまうこと
・損害賠償や対応コストなどの経済的損失や組織の信頼性低下等の損害が発生

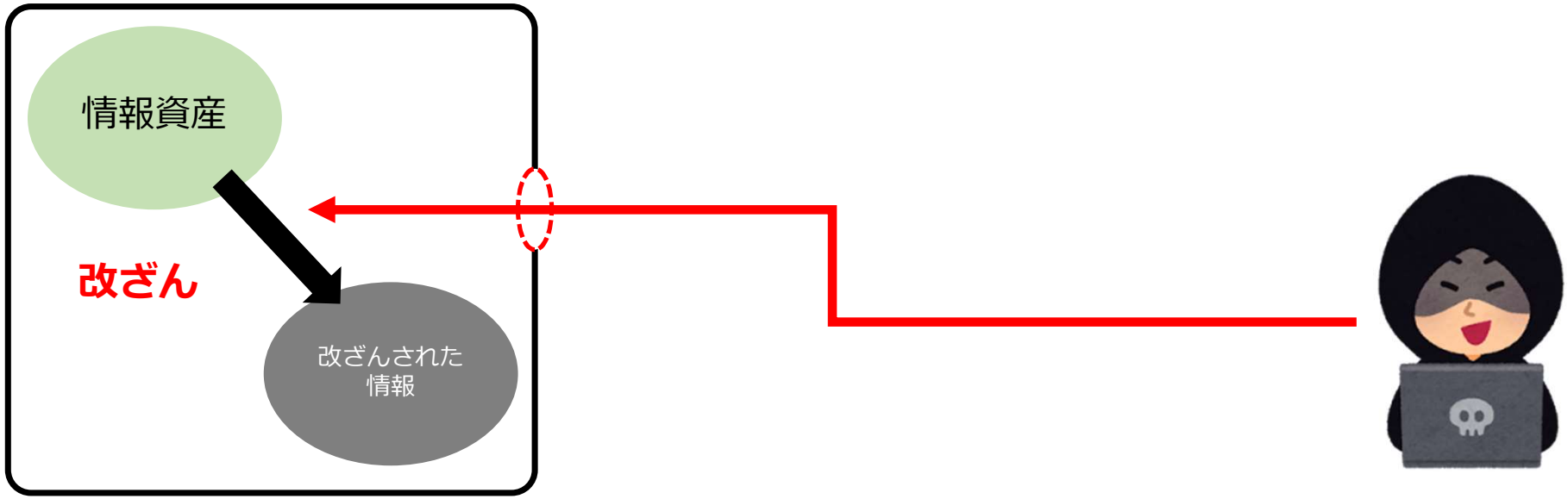


脆弱性を放置すると何が起こるか②

■データ改ざん

・管理者や正規のユーザが意図しない値・形式にデータを書き換えること

・業務の中断やデータの復旧対応、組織の信頼性低下等の損害が発生

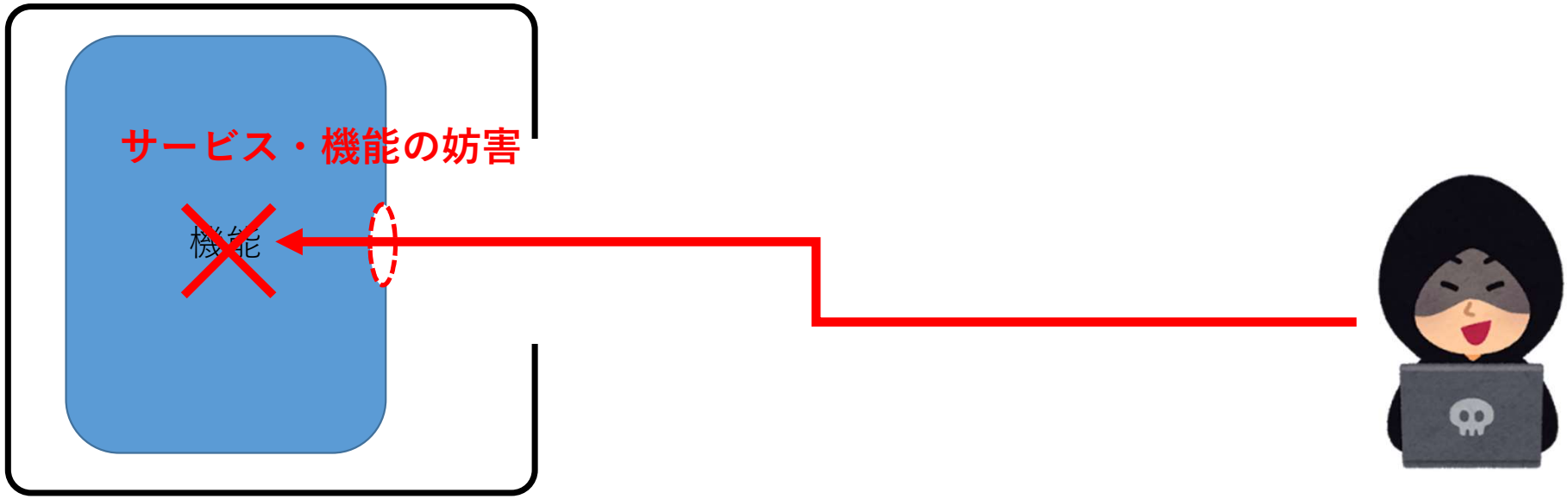


脆弱性を放置すると何が起こるか③

■サービス・機能の妨害（DoS）

・大量のデータや不正な形式のデータを送り込みシステムの正常な稼働を阻害すること

・サービス停止による売り上げの損失、復旧対応コスト、組織の信頼性低下等の損害が発生

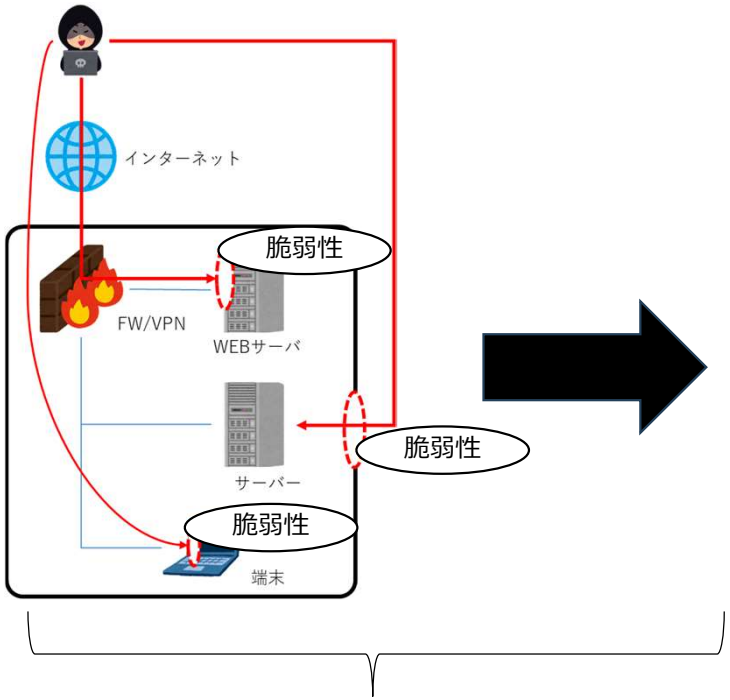


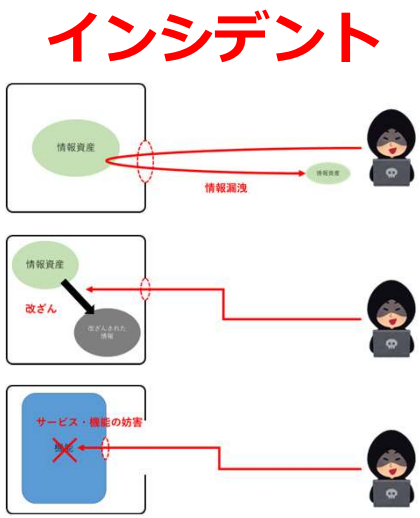
脆弱性管理の必要性

脆弱性があるから管理する：×

↓

インシデントの発生による損害を予防する：○





損害

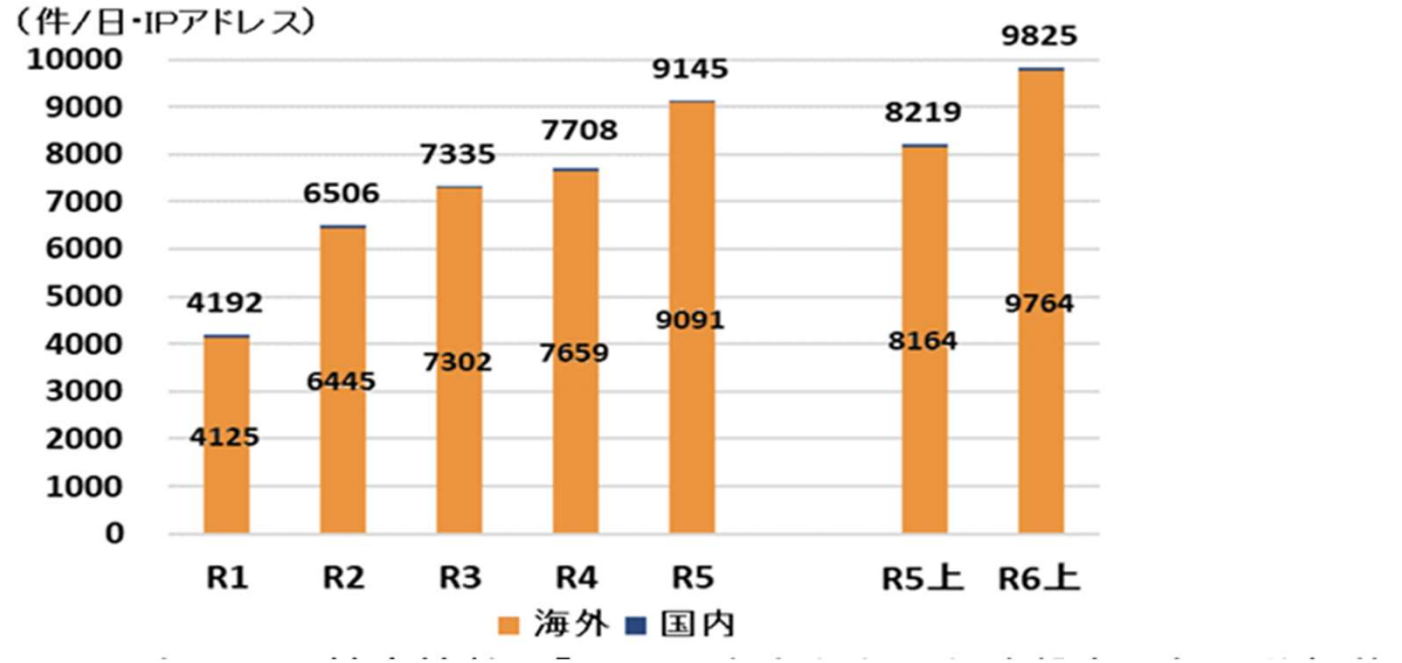
- **経済的損失**
- **信頼性の低下**
- **法的リスク**

脆弱性管理によってインシデントの発生を予防

脆弱性を悪用した攻撃の増加

警察庁が設置したセンサーにおいて検知した脆弱性探索行為等の不審なアクセス件数

【図表１：検知したアクセスの送信元で比較した１日・１IP アドレス当たりの件数の推移】



出典：警察庁（令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について）

脆弱性を悪用されて攻撃された事例

徳島県つるぎ町立半田病院
コンピュータウイルス感染事案有識者会議調査報告書について

令和3年10月31日の未明、つるぎ町立半田病院がサイバー攻撃を受け、電子カルテをはじめとする院内システムがランサムウェアと呼ばれる身代金要求型コンピュータウイルスに感染し、カルテが閲覧できなくなるなどの大きな被害が生じました。令和4年1月4日の通常診療再開までの間、患者さんをはじめ関係者の皆さまには多大なご迷惑とご心配をおかけいたしましたこと、改めて深くお詫び申し上げます。

事件発生後、当院の職員は一丸となって早期復旧を目指しました。全容解明や情報漏えい有無の特定よりも、まずは病院としての機能を一日も早く取り戻すために、患者さんのデータをいかに復元させるか、端末を利用できる状況にどのように戻すかに焦点を当てインシデント対応を行っていきました。幸いにして、調査復旧を請け負った事業者の作業、電子カルテ業者の仮システムの構築、そして、電子カルテより必要に応じて抽出していたデータなどを利用し、令和4年1月4日に通常診療を再開することが出来ました。

事件発生後、全国の病院や事業所が当院のようなサイバー攻撃を受けないためにも、詳細な状況を公表することが責任であると考え、できうる限りの情報を公開してきました。その結果、あらゆるマスコミや業界誌等からの取材依頼があり、逆に様々な情報提供もありました。この状況は今現在も続いており、今後も積極的な情報開示に努めてまいります。

4.4.2　閉域網ではないにもかかわらずインターネット上の脅威を評価していなかった

VPN 装置 によってインターネットからの外部接続が可能なネットワークであったにもかかわらず、VPN 装置の脅威を評価しなかった。

- ■ VPN 装置の脆弱性の是正を行っていない
  VPN 装置の脅威をまったく評価せず、結果として、VPN 装置の脆弱性の是正、パスワードの変更を行っていなかった。
- ■ VPN 装置への接続元 IP アドレスの限定を行っていない
  保守のための接続であれば、接続元 IP アドレスを限定すべきであった。

4.5.2　コンピュータへのログイン

VPN に接続しただけでは単にネットワークにつながっているだけであり、病院内ネットワークに接続されたコンピュータにログインする必要がある。ログインについては、以下の方法を使用したと考えられる。

- ✓ 総当たり攻撃
  - ➢ パスワードは 5 桁であった
  - ➢ ロックアウトの設定はなかった
  - ➢ Administrator の ID は変更されていなかった
- ✓ 既知の脆弱性を利用した侵入
  - ➢ すべての既知の脆弱性が存在しており、リモートコードの実行が可能だった
  - ➢ ウイルス対策ソフトは停止していた

出典：半田病院（コンピュータウイルス感染事案有識者会議報告書）

サイバー攻撃による経済的損失

10. サイバーセキュリティに関する問題が引き起こす経済的損失 | 白書掲載番号（Ⅱ-1-10-5）

調査・分析の実施主体	対象地域	対象期間	経済的損失の概要	損失額
トレンドマイクロ	日本	2023年【調査時期】	過去3年間でのサイバー攻撃の被害を経験した法人組織の累計被害額の平均	1億2,528万円
警察庁	日本	2023年上半期	ランサムウェア被害に関連して要した調査・復旧費用の総額	26%が100万円未満 19%が100万～500万円未満 25%が500万～1,000万円未満 23%が1,000万～5,000万円未満 8%が5,000万円以上
FBI	米国	2022年	サイバー犯罪事件による被害報告総額	102億ドル
NFIB	英国	2023年	サイバー犯罪による被害報告総額	560万ポンド
Sophos	世界14か国	2023年	直近のランサムウェア攻撃の修復に要した1組織あたりの年間平均コスト	182万ドル
IBM	世界16か国	2023年	組織における1回のデータ侵害にかかる世界平均コスト	445万ドル
Cybersecurity Ventures	世界	2025年【予測】	サイバー犯罪によるコスト	10兆5,000億ドル
Fastl	北米、欧州、アジア、太平洋地域	2023年	サイバー攻撃を受けた企業の損失	過去12ヶ月間収益の9%

大きい画像はこちら

（出典）各種公開資料を基に作成

出典：総務省　情報通信白書　令和5年版

脆弱性管理を行う立場の分類

「脆弱性管理」の中でどのようなことをする必要があるのかはその立場によって異なる。今回は**ユーザ（システム管理者）の立場**にフォーカスして説明する。

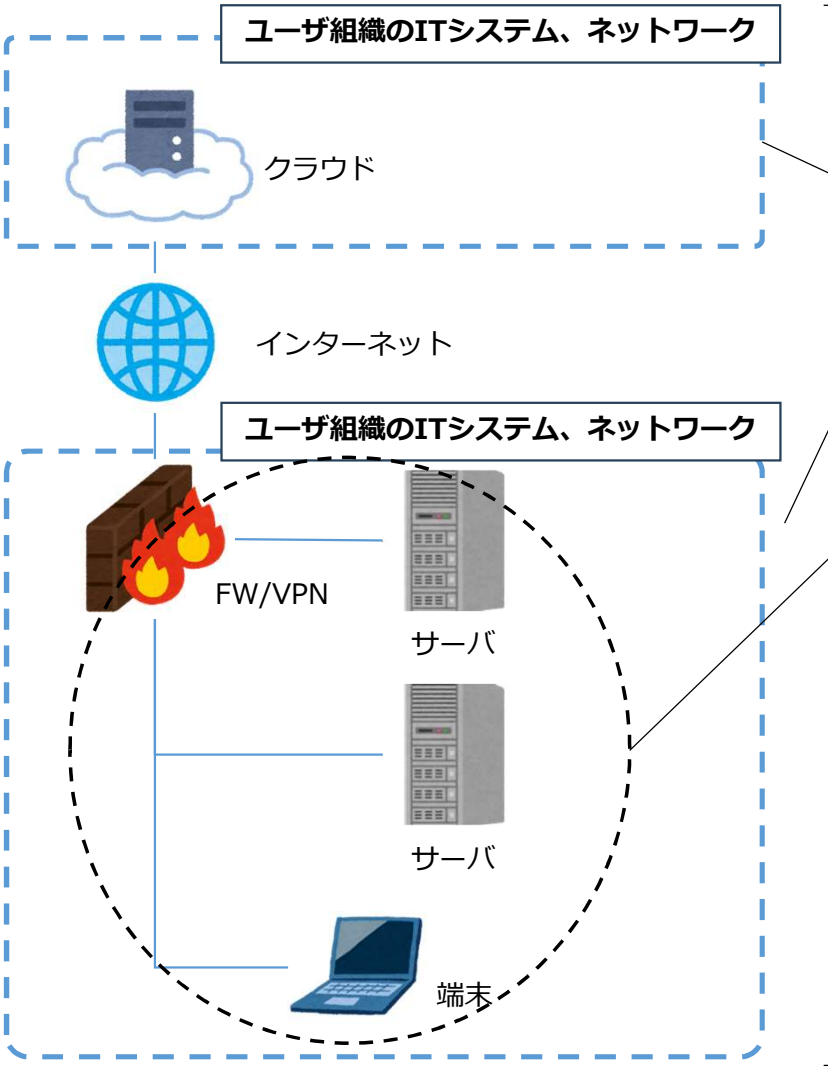
■ユーザ（システム管理者）

・ITサービス/製品の提供を受ける組織において、当該ITサービス/製品の脆弱性管理を行う立場
・自組織の損害を予防するため脆弱性管理を行う

■ITサービス/製品の提供者
・ITサービス/製品を直接または間接（サプライチェーン）的にユーザに提供する立場
・自組織が開発したITサービス/製品の脆弱性管理を行う

■システムインテグレータ（SIer）
・ユーザの要望に従ってシステムを構築する立場
・契約不適合にならないように脆弱性管理を行う

ユーザ（システム管理者）の観点



- **脆弱性管理の対象**は何か
- **自組織のITシステム、ネットワークの設計や設定**の不備はないか
- **利用しているサービス、ソフトウェアや製品に脆弱性**はないか
- **脆弱性があった場合、どれくらいのリスクか**
- **どのように対処・対策するか**

※システムの導入の段階から想定リスクを洗い出し、対処すること（セキュリティバイデザイン）は重要だが、本ドキュメントでは主に導入後の脆弱性管理について記載する。

ユーザ観点での脆弱性管理の流れ

ユーザ観点での脆弱性管理は下記の流れで実施する。

脆弱性管理対象の識別

脆弱性管理対象の識別

脆弱性管理対象の識別の際には下記の事項を把握する必要がある。

把握ポイント、目的と収集情報の例

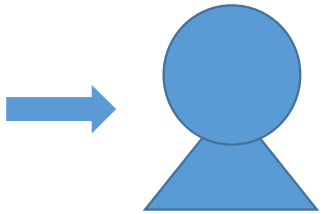
把握事項	目的	例
ソフトウェア名/製品名	・脆弱性情報収集のキーワード	○○ソフトウェア
バージョン情報	・脆弱性に該当するかの確認	1.2.3
機能カテゴリ/保持情報	・リスク評価の判断材料	VPN接続用
構成	・リスク評価の判断材料	社内NWへの接続
外部アクセス可否・ポート情報	・リスク評価の判断材料	インターネットからの アクセス可
設置場所	・リスク評価の判断材料	××ビル
管理者/責任範囲	・対処を行う主体の判断	○○部門

脆弱性管理対象の識別の必要性

脆弱性管理対象の識別を行わない場合

脆弱性情報

xxxに脆弱性があります。
対象のバージョンは○○です。
□□の構成の場合に影響があります。
使用している場合は対応してください。

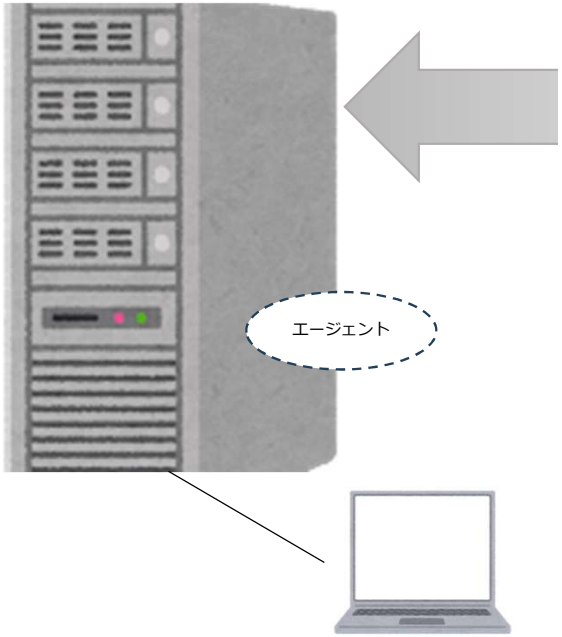


- 自組織にあるITサービス/製品が脆弱性の影響を受けるかわからない
- 脆弱性情報が公開されたときの組織のリスクがわからない
- 脆弱性対策として適切な対応がわからない

脆弱性管理対象の識別を実施することで、
後工程で自組織にあるITサービス/製品に応じた適切な対応を実施することができる。

脆弱性管理対象の識別の補助・効率化

ソフトウェア情報の確認には仕様書、設計書等の確認、担当者へのヒアリングが必要だが、下記のような手段による補助・効率化も考えられる



■外部スキャンによる管理対象の情報収集
メリット　：自動で定期的に情報収集可能
デメリット：外部からのアクセス経路が必要/構成により導入可否の確認が必要

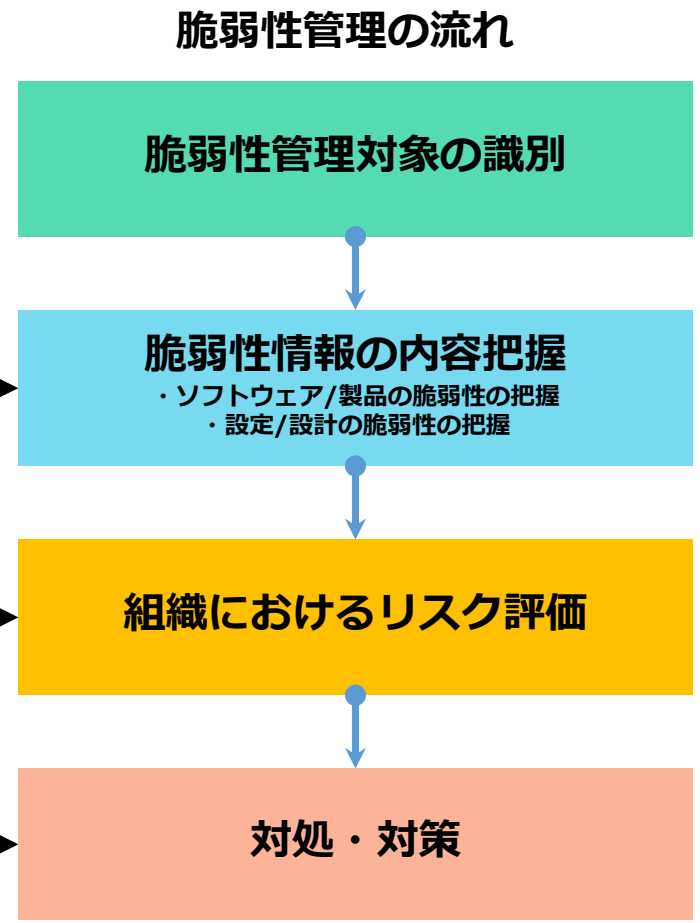
■エージェントによる管理対象の情報収集
メリット　：自動で定期的に情報収集可能
デメリット：管理対象のパフォーマンスへの影響/構成により導入可否の確認が必要

■GUI/CLI操作（手動）による管理対象の情報収集
メリット　：特別な準備は不要
デメリット：手動のため管理対象が多いと負担が大きい

- 複雑なシステムやドキュメントが存在しないなど管理が不十分な場合、上記手段を組み合わせた情報収集が必要となる。

把握した事項と後工程の関連性

把握事項	目的	例
ソフトウェア名/製品名	・脆弱性情報収集のキーワード	○○ソフトウェア
バージョン情報	・脆弱性に該当するかの確認	1.2.3
機能カテゴリ/保持情報	・リスク評価の判断材料	VPN接続用
構成	・リスク評価の判断材料	社内NWへの接続
外部アクセス可否・ポート情報	・リスク評価の判断材料	インターネットからのアクセス可
設置場所	・リスク評価の判断材料	××ビル
管理者/責任範囲	・対処を行う主体の判断	○○部門



脆弱性情報の内容把握

前工程との関連性

脆弱性管理の流れ

脆弱性管理対象の識別

↓

脆弱性情報の内容把握
・ソフトウェア/製品の脆弱性の把握
・設定/設計の脆弱性の把握

↓

組織におけるリスク評価

↓

対処・対策

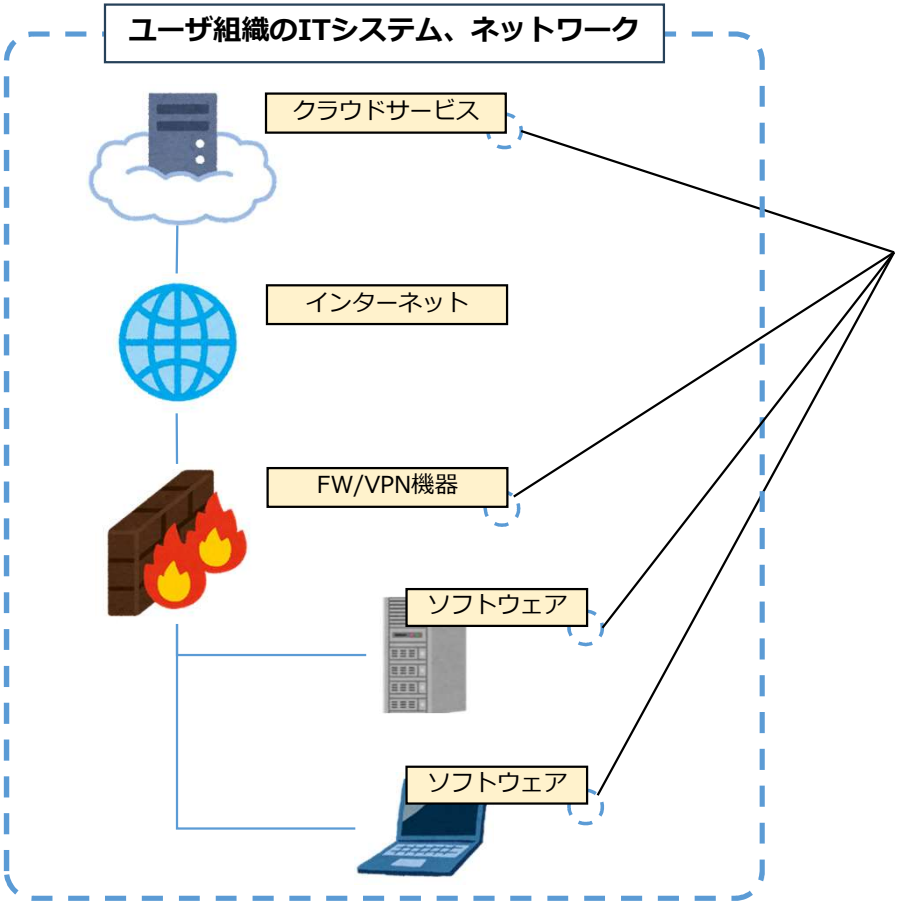
把握事項	目的	例
ソフトウェア名/製品名	・脆弱性情報収集のキーワード	○○ソフトウェア
バージョン情報	・脆弱性に該当するかの確認	1.2.3
機能カテゴリ/保持情報	・リスク評価の判断材料	VPN接続用
構成	・リスク評価の判断材料	社内NWへの接続
外部アクセス可否・ポート情報	・リスク評価の判断材料	インターネットからのアクセス可
設置場所	・リスク評価の判断材料	××ビル
管理者/責任範囲	・対処を行う主体の判断	○○部門

把握事項	例
CVE-ID・脆弱性の名称	CVE-2024-xxxxx
対象ソフトウェア・製品	○○ソフトウェア
対象バージョン	ver 2.x.x～ver 3.y.y
脆弱性発露の条件	ローカルNWへの接続
影響	アクセス制御の不備による特権昇格
CVSS	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
EPSS	0.12455
KEVC	記載あり
対応策・対応手順	パッチの適用
緩和策・回避策	設定変更・××機能の停止

「**脆弱性管理対象の識別**」で集めた情報に合致する脆弱性情報を収集し、影響を受ける「**脆弱性情報の内容把握**」を行う

脆弱性情報の内容把握

把握すべき脆弱性情報は「**ソフトウェア/製品の脆弱性**」、「**設定/設計の脆弱性**」に大別でき、それぞれ脆弱性情報の内容把握をするための手段が異なる

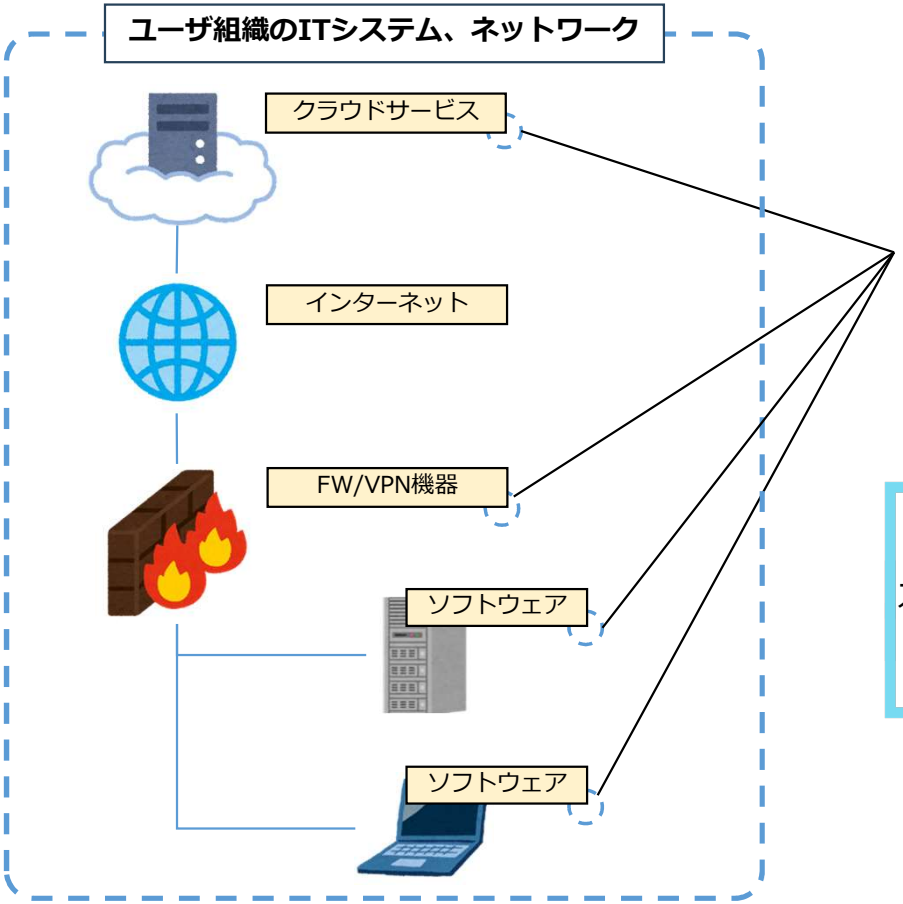


ソフトウェア/製品の脆弱性
ソフトウェア/製品の開発の過程で発生するさまざまな要因によるものである。ユーザは、ソフトウェア/製品の提供者をはじめとした外部組織からの情報収集が必要

設定/設計の脆弱性
ユーザによる設定/設計ミスを起因とするため、ユーザ自身での確認が必要

脆弱性情報の内容把握

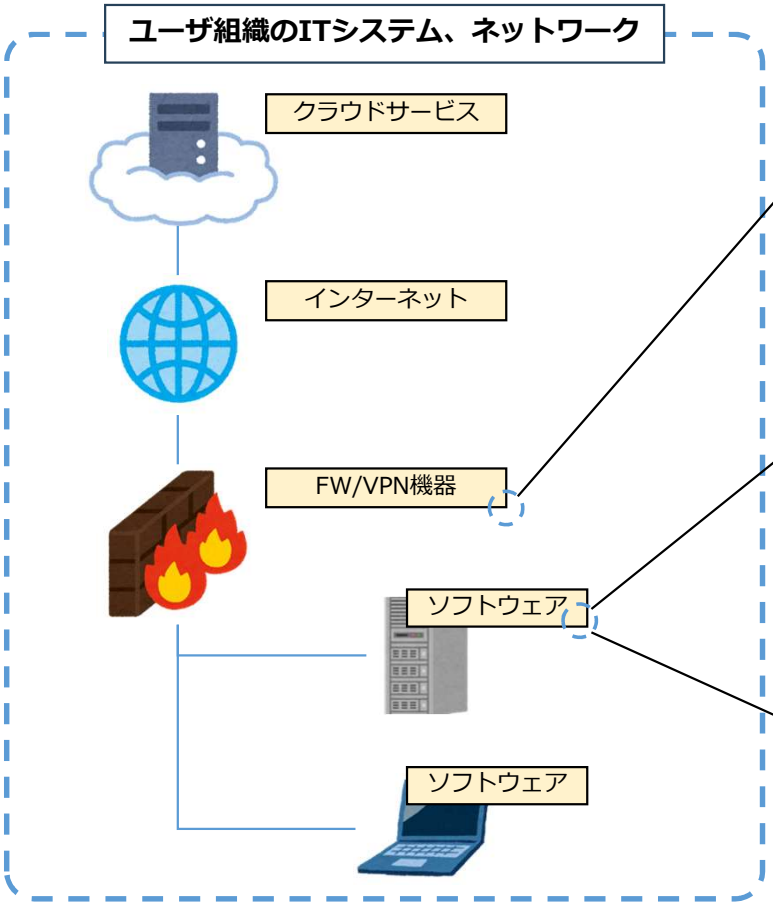
把握すべき脆弱性情報は「**ソフトウェア/製品の脆弱性**」、「**設定/設計の脆弱性**」に大別でき、それぞれ脆弱性情報の内容把握をするための手段が異なる



ソフトウェア/製品の脆弱性
ソフトウェア/製品の開発の過程で発生するさまざまな要因によるものである。ユーザは、ソフトウェア/製品の提供者をはじめとした外部組織からの情報収集が必要

本講演では**ソフトウェア/製品の脆弱性**に焦点を当てています。

ソフトウェア/製品の脆弱性の例

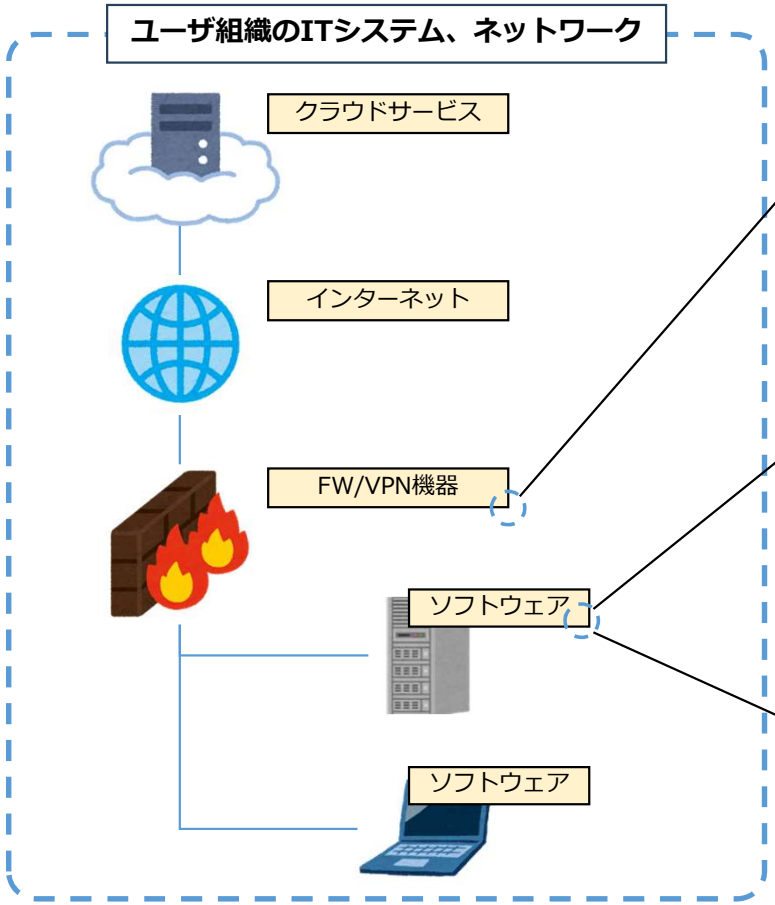


CVE-2020-5902: F5 Networks BIG-IPの脆弱性
脆弱性が悪用されると、認証されていない遠隔の第三者が、影響を受ける製品のTraffic Management User Interface (TMUI) 経由で、任意のコードを実行するなどの可能性があります。
https://www.jpcert.or.jp/at/2020/at200028.html

CVE-2021-41773: Apache HTTP Serverの脆弱性
Apache HTTP Serverのバージョン2.4.49には、パストラバーサルの脆弱性があります。結果として、遠隔の第三者が、細工したリクエストを送信し、Apache HTTP Serverが稼働するサーバーでアクセスが適切に制限されていないドキュメントルート外のファイルを読み取るなどの可能性があります。
https://www.jpcert.or.jp/at/2021/at210043.html

CVE-2017-1001000: Wordpressの脆弱性
ブログ投稿を編集または削除するときにユーザー指定の入力が「id」パラメーターに適切にサニタイズされないため、REST APIに権限昇格の脆弱性があります。認証されていないリモートの攻撃者がこの問題を悪用し、任意のPHPコードの実行、ブログ投稿へのコンテンツの挿入、ブログ投稿属性の変更、またはブログ投稿の削除を行う可能性があります。
https://jp.tenable.com/plugins/was/98261

ソフトウェア/製品の脆弱性の例



CVE-2020-5902: F5 Networks BIG-IPの脆弱性

バックドアを作成され、内部に侵入される可能性がある

CVE-2021-41773: Apache HTTP Serverの脆弱性

情報漏えいする可能性がある

CVE-2017-1001000: Wordpressの脆弱性

情報を改竄される可能性がある

ソフトウェア/製品の脆弱性情報の把握

ソフトウェア/製品の脆弱性の把握には下記の事項を押さえた情報収集が必要

把握事項	例
CVE-ID・脆弱性の名称	CVE-2024-xxxxx
対象ソフトウェア・製品	○○ソフトウェア
対象バージョン	ver 2.x.x～ver 3.y.y
脆弱性発露の条件	ローカルNWへの接続
影響	アクセス制御の不備による特権昇格
CVSS	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
EPSS	0.12455
KEVC	記載あり
対応策・対応手順	パッチの適用
緩和策・回避策	設定変更・××機能の停止

ソフトウェア/製品の脆弱性情報の把握

ソフトウェア/製品の脆弱性の把握には下記の事項を押さえた情報収集が必要

把握事項	例
CVE-ID・脆弱性の名称	CVE-2024-xxxxx
急ソフトウェア・製品	○○ソフトウェア
	.x.x～ver 3.y.y
	カルNWへの接続
影響	アクセス制御の不備による特権昇格
CVSS	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
EPSS	0.12455
KEVC	記載あり
対応策・対応手順	パッチの適用
緩和策・回避策	設定変更・××機能の停止

CVE-ID
ソフトウェア/製品の脆弱性に一意に付与される識別番号
各種情報は、CVE-IDに紐づいて公開されることが多い
危険度の高い脆弱性には固有の名称が付けられることがある

組織におけるリスク評価のパートで説明します

脆弱性情報の情報源

ソフトウェア/製品の脆弱性情報の把握には下記のような手段がある

■セキュリティ関連の団体/組織からの情報収集
JPCERT/CC : https://www.jpcert.or.jp/menu_alertsandadvisories.html
IPA : https://www.ipa.go.jp/security/vuln/index.html
IPA/ JPCERT/CC （JVN） : https://jvn.jp/
CISA（KEVC） : https://www.cisa.gov/known-exploited-vulnerabilities-catalog
NIST（NVD） : https://nvd.nist.gov/search

■ソフトウェア/製品の開発ベンダからの情報収集
Microsoft : https://msrc.microsoft.com/update-guide/
Red Hat : https://access.redhat.com/security/ 等

■セキュリティベンダが運営するサイトからの情報収集
SIOS : https://security.sios.jp 等

■脆弱性情報配信サービスによる情報収集
vuldb : https://vuldb.com 等

セキュリティ関連の団体/組織サイトの例

Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起

最終更新: 2024-04-25

X ポスト　メール

JPCERT-AT-2024-0009
JPCERT/CC
2024-04-13（公開）
2024-04-25（更新）

I. 概要

2024年4月12日（現地時間）、Palo Alto Networksは、PAN-OSのGlobalProtect機能におけるOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関するアドバイザリを公開しました。GlobalProtectはリモートアクセス（VPN）などを提供する機能です。本脆弱性の悪用により、認証されていない遠隔の第三者が、ルート権限で任意のコードを実行する可能性があります。

アドバイザリの公開当時、Palo Alto Networksは、本脆弱性を悪用する攻撃を限定的に確認しているとのことでしたが、2024年4月17日（現地日付）、本脆弱性を実証するコード（Proof-of-Concept）が公開され、脆弱性を悪用する攻撃の増加を確認していると明らかにしました。JPCERT/CCは日本国内から本脆弱性を悪用する攻撃の被害に関する報告をいただいています。Palo Alto Networksなどが公開する最新の情報をご確認の上、速やかに対策や回避策の適用をご検討いただき、脆弱性を悪用する攻撃の被害を受けていないかをご確認いただくことを推奨します。

Palo Alto Networks
CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway
https://security.paloaltonetworks.com/CVE-2024-3400

更新: 2024年4月25日追記

「V. 侵害調査方法」の情報を更新し、本脆弱性を悪用する攻撃を受けた場合の対処方法や手順に関するPalo Alto Networksのリンクを追記しました。

II. 対象

対象となるシステムおよびバージョンは次のとおりです。詳細や最新の情報はPalo Alto Networksが提供する情報をご参照ください。

- PAN-OS 11.1：11.1.2-h3より前のバージョン
- PAN-OS 11.1：11.1.1-h1より前のバージョン
- PAN-OS 11.1：11.1.0-h3より前のバージョン

JPCERT/CC 注意喚起
https://www.jpcert.or.jp/at/2024/at240009.html

CVE-2024-3400 Detail

Description

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Palo Alto Networks, Inc.　**Base Score:** 10.0 CRITICAL　**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://security.paloaltonetworks.com/CVE-2024-3400	Vendor Advisory
https://unit42.paloaltonetworks.com/cve-2024-3400/	Exploit, Vendor Advisory
https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	Technical Description, Vendor Advisory
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/	Exploit, Third Party Advisory

This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Palo Alto Networks PAN-OS Command Injection Vulnerability	04/12/2024	04/19/2024	Apply mitigations per vendor instructions as they become available. Otherwise, users with vulnerable versions of affected devices should enable Threat Prevention IDs available from the vendor. See the vendor bulletin for more details and a patch release schedule.

NVD
https://nvd.nist.gov/vuln/detail/CVE-2024-3400

セキュリティ関連の団体/組織サイトの例

Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起

最終更新: 2024-04-25

X ポスト　メール

JPCERT-AT-2024-0009
JPCERT/CC
2024-04-13（公開）
2024-04-25（更新）

I. 概要

2024年4月12日（現地日付）、Palo Alto Networksは、PAN-OSのGlobalProtect機能におけるOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関するアドバイザリを公開しました。GlobalProtectはリモートアクセス（VPN）などを提供する機能です。本脆弱性の悪用により、認証されていない遠隔の第三者が、ルート権限で任意のコードを実行する可能性があります。

アドバイザリの公開当時、Palo Alto Networksは、本脆弱性を悪用する攻撃を限定的に確認しているとのことでしたが、2024年4月17日（現地日付）、本脆弱性を実証するコード（Proof-of-Concept）が公開され、脆弱性を悪用する攻撃の増加を確認していると明らかにしました。JPCERT/CCは日本国内から本脆弱性を悪用する攻撃の被害に関する報告をいただいています。Palo Alto Networksなどが公開する最新の情報をご確認の上、速やかに対策や回避策の適用をご検討いただき、脆弱性を悪用する攻撃の被害を受けていないかをご確認いただくことを推奨します。

Palo Alto Networks
CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway
https://security.paloaltonetworks.com/CVE-2024-3400

更新: 2024年4月25日追記

「V. 侵害調査方法」の情報を更新し、本脆弱性を悪用する攻撃を受けた場合の対処方法や手順に関するPalo Alto Networksのリンクを追記しました。

II. 対象

対象となるシステムおよびバージョンは次のとおりです。詳細や最新の情報はPalo Alto Networksが提供する情報をご参照ください。

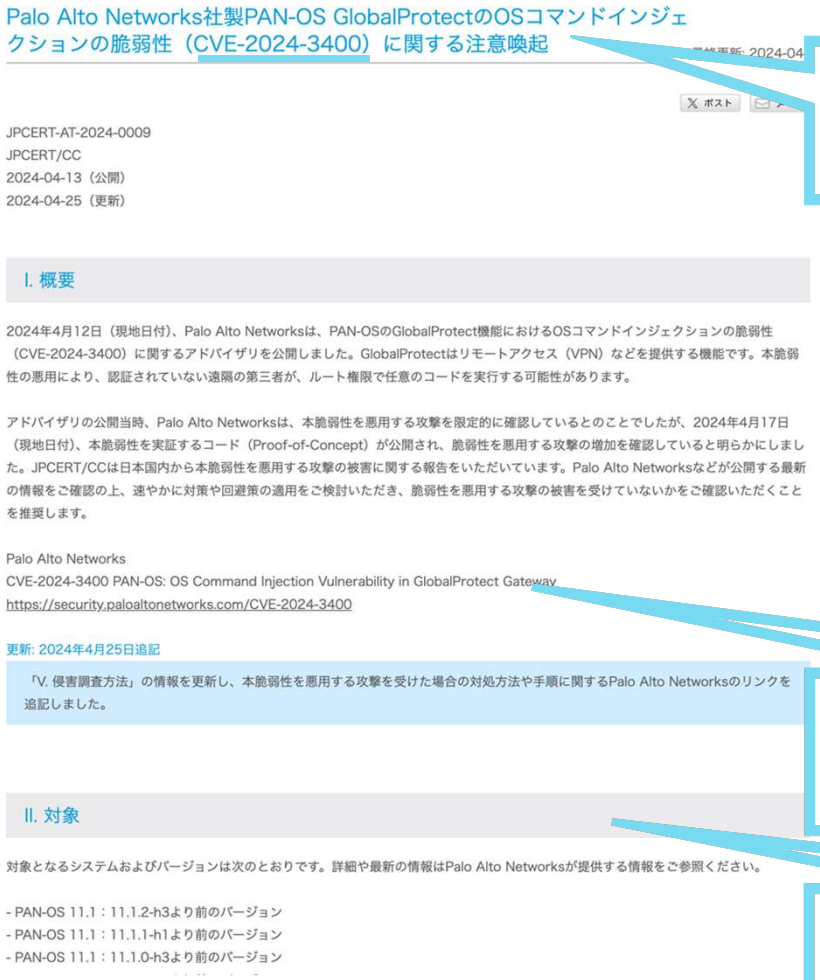
- PAN-OS 11.1：11.1.2-h3より前のバージョン
- PAN-OS 11.1：11.1.1-h1より前のバージョン
- PAN-OS 11.1：11.1.0-h3より前のバージョン

JPCERT/CC 注意喚起
https://www.jpcert.or.jp/at/2024/at240009.html

日本国内での利用が多い製品において、下記のような状況の際に、インシデントを未然に防ぐ/インシデント発生時の影響を小さくする事を目的に情報展開される

- 悪用された場合に、影響が深刻である可能性がある
- すでに悪用や侵害が報告されている

セキュリティ関連の団体/組織サイトの例



Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起

JPCERT-AT-2024-0009
JPCERT/CC
2024-04-13（公開）
2024-04-25（更新）

I. 概要

2024年4月12日（現地日付）、Palo Alto Networksは、PAN-OSのGlobalProtect機能におけるOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関するアドバイザリを公開しました。GlobalProtectはリモートアクセス（VPN）などを提供する機能です。本脆弱性の悪用により、認証されていない遠隔の第三者が、ルート権限で任意のコードを実行する可能性があります。

アドバイザリの公開当時、Palo Alto Networksは、本脆弱性を悪用する攻撃を限定的に確認しているとのことでしたが、2024年4月17日（現地日付）、本脆弱性を実証するコード（Proof-of-Concept）が公開され、脆弱性を悪用する攻撃の増加を確認していると明らかにしました。JPCERT/CCは日本国内から本脆弱性を悪用する攻撃の被害に関する報告をいただいています。Palo Alto Networksなどが公開する最新の情報をご確認の上、速やかに対策や回避策の適用をご検討いただき、脆弱性を悪用する攻撃の被害を受けていないかをご確認いただくことを推奨します。

Palo Alto Networks
CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway
https://security.paloaltonetworks.com/CVE-2024-3400

更新: 2024年4月25日追記
「V. 侵害調査方法」の情報を更新し、本脆弱性を悪用する攻撃を受けた場合の対処方法や手順に関するPalo Alto Networksのリンクを追記しました。

II. 対象

対象となるシステムおよびバージョンは次のとおりです。詳細や最新の情報はPalo Alto Networksが提供する情報をご参照ください。

- PAN-OS 11.1：11.1.2-h3より前のバージョン
- PAN-OS 11.1：11.1.1-h1より前のバージョン
- PAN-OS 11.1：11.1.0-h3より前のバージョン

JPCERT/CC 注意喚起
https://www.jpcert.or.jp/at/2024/at240009.html

CVE-IDや脆弱性名の名称

日本国内での利用が多い製品において、下記のような状況の際に、インシデントを未然に防ぐ/インシデント発生時の影響を小さくする事を目的に情報展開される

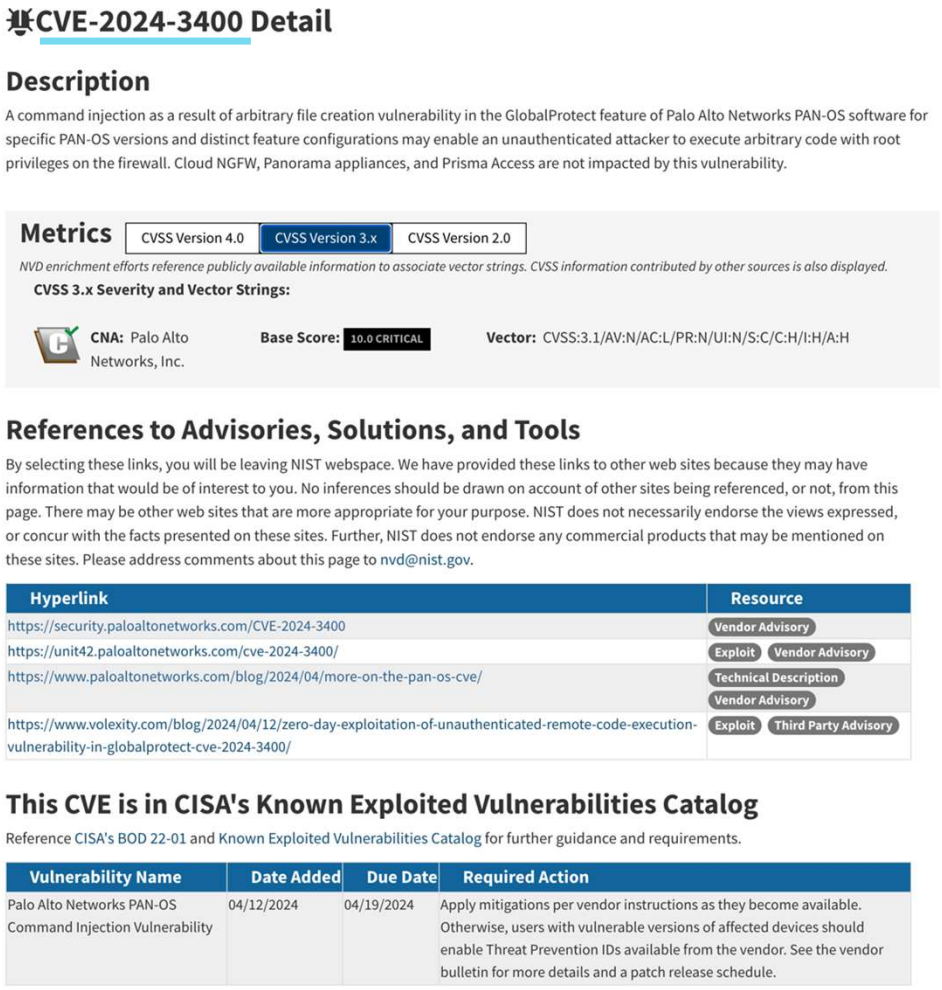
- 悪用された場合に、影響が深刻である可能性がある
- すでに悪用や侵害が報告されている

開発ベンダサイトへのリンク

対象ソフトウェアや対象バージョン

セキュリティ関連の団体/組織サイトの例

報告されたすべての脆弱性について、一定のフォーマットで情報を提供する



CVE-2024-3400 Detail

Description

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Palo Alto Networks, Inc. **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://security.paloaltonetworks.com/CVE-2024-3400	Vendor Advisory
https://unit42.paloaltonetworks.com/cve-2024-3400/	Exploit, Vendor Advisory
https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	Technical Description, Vendor Advisory
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/	Exploit, Third Party Advisory

This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Palo Alto Networks PAN-OS Command Injection Vulnerability	04/12/2024	04/19/2024	Apply mitigations per vendor instructions as they become available. Otherwise, users with vulnerable versions of affected devices should enable Threat Prevention IDs available from the vendor. See the vendor bulletin for more details and a patch release schedule.

NVD
https://nvd.nist.gov/vuln/detail/CVE-2024-3400

セキュリティ関連の団体/組織サイトの例

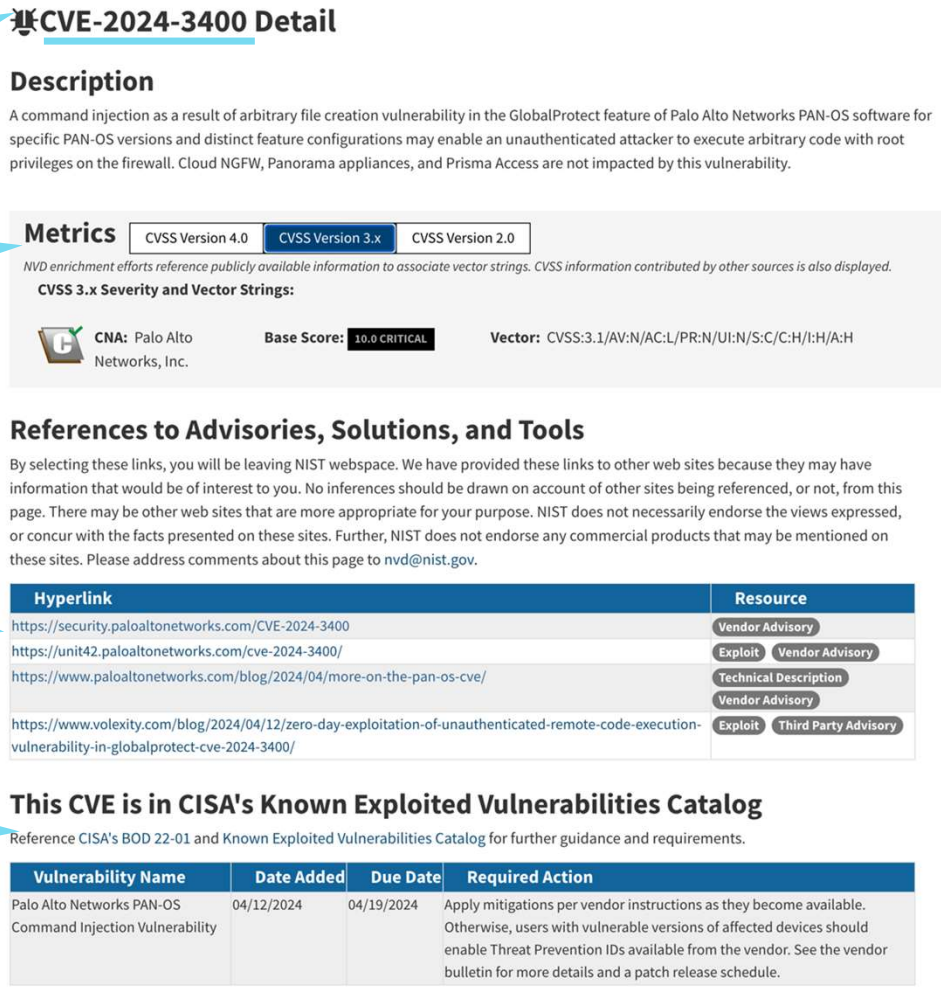
CVE-ID

CVSS

報告されたすべての脆弱性について、一定のフォーマットで情報を提供する

開発ベンダサイトへのリンク

KEVCの記載状況



CVE-2024-3400 Detail

Description

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Palo Alto Networks, Inc. **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://security.paloaltonetworks.com/CVE-2024-3400	Vendor Advisory
https://unit42.paloaltonetworks.com/cve-2024-3400/	Exploit, Vendor Advisory
https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	Technical Description, Vendor Advisory
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/	Exploit, Third Party Advisory

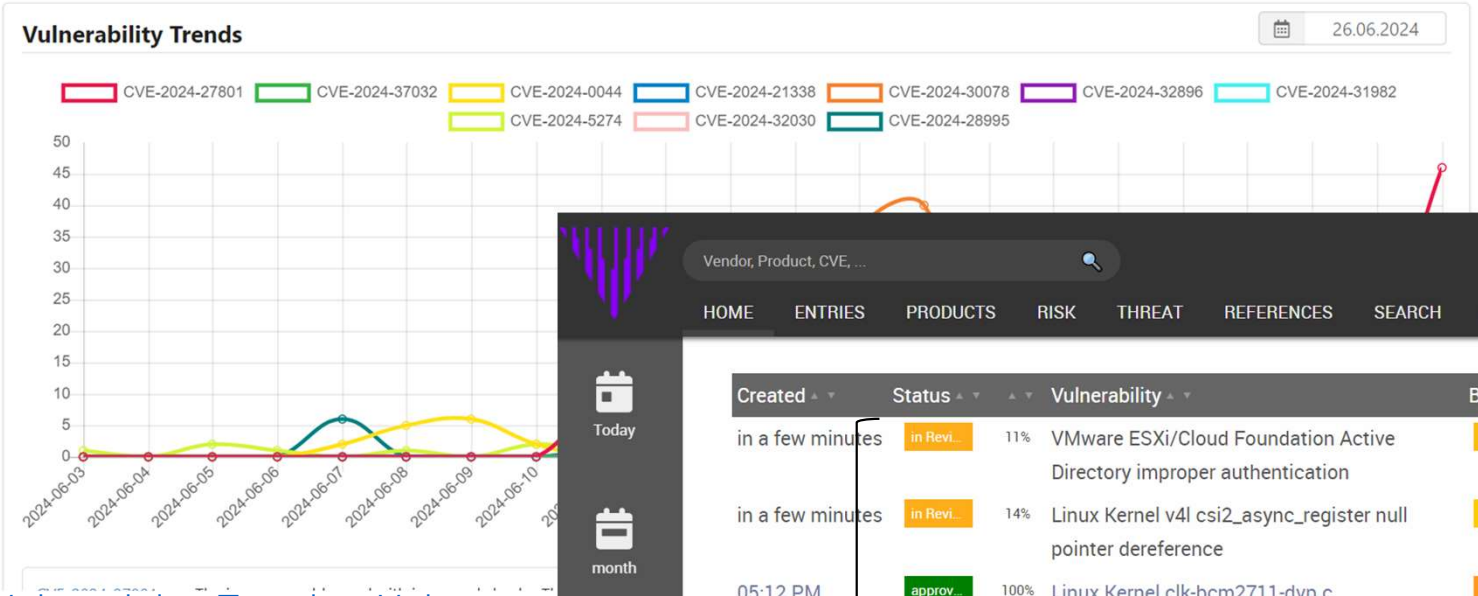
This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

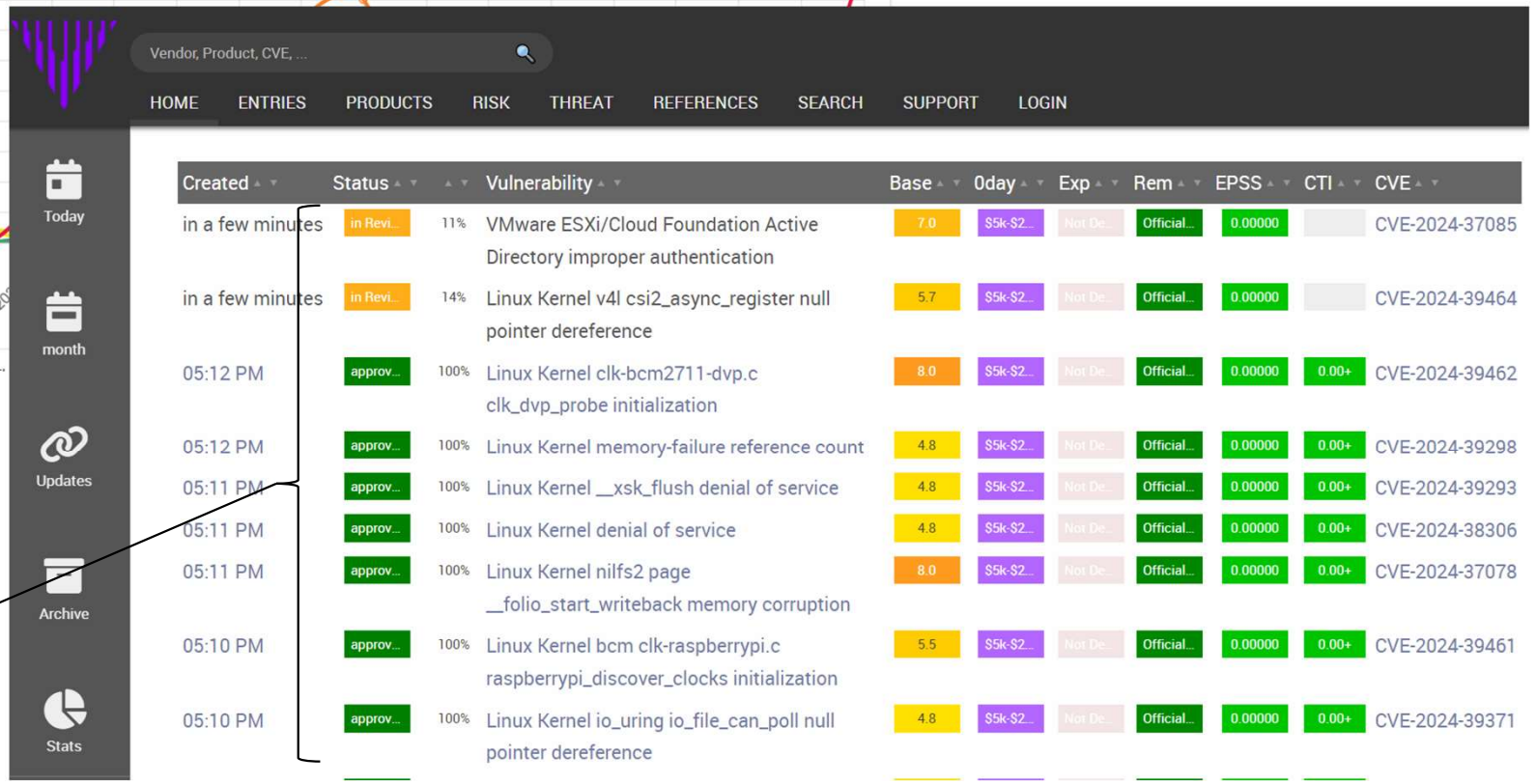
Vulnerability Name	Date Added	Due Date	Required Action
Palo Alto Networks PAN-OS Command Injection Vulnerability	04/12/2024	04/19/2024	Apply mitigations per vendor instructions as they become available. Otherwise, users with vulnerable versions of affected devices should enable Threat Prevention IDs available from the vendor. See the vendor bulletin for more details and a patch release schedule.

NVD
https://nvd.nist.gov/vuln/detail/CVE-2024-3400

情報配信サービスの例



[Vulnerability Trends – Vulmon]



あらゆる製品の
脆弱性情報を一つ
のサイトで一覧化
されている

[Vulnerability Database 🛡 (vuldb.com)]

脆弱性情報収集アプローチ

■注意喚起情報から始める

2023

公開日	注意喚起内容	テキスト (PGP署名付き)
2023-10-23	Cisco IOS XEのWeb UIの脆弱性(CVE-2023-20198)に関する注意喚起 (更新)	6.37KB
2023-10-20	Citrix ADCおよびCitrix Gatewayの脆弱性 (CVE-2023-4966) に関する注意喚起 (公開)	5.50KB
2023-10-18	Cisco IOS XEのWeb UIにおける権限昇格の脆弱性 (CVE-2023-20198) に関する注意喚起 (公開)	
2023-10-18	2023年10月Oracle製品のクリティカルパッチアップデートに関する注意喚起 (公開)	3.36KB
2023-10-18	ProselfのXML外部実体参照 (XXE) に関する脆弱性を悪用する攻撃の注意喚起 (更新)	5.88KB
2023-10-11	2023年10月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	3.91KB
2023-10-11	Citrix ADCおよびCitrix Gatewayの脆弱性 (CVE-2023-3519) に関する注意喚起 (更新)	7.27KB
2023-10-10	ProselfのXML外部実体参照 (XXE) に関する脆弱性を悪用する攻撃の注意喚起 (公開)	
2023-09-22	Array Networks Array AGシリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起 (更新)	7.81KB
2023-09-19	複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品における任意のコード実行の脆弱性に関する注意喚起 (公開)	4.42KB

引用：JPCERT/CC
https://www.jpcert.or.jp/at/2023.html

■利用製品の情報から始める

引用：IPA　https://jvndb.jvn.jp/en/

- CVE-ID・脆弱性の名称
- 対象ソフトウェア・製品
- 概要

開発ベンダやセキュリティベンダの
サイトから詳細情報収集

項目	内容
対象バージョン	○○
脆弱性発露の条件	○○
影響	○○
CVSS	○○
EPSS	○○
KEVC	○○
対応策・対応手順	○○
緩和策・回避策	○○

脆弱性情報収集アプローチ

■注意喚起情報から始める

網羅性や速報性はないが、影響が深刻な脆弱性の情報のみが公開される

引用：JPCERT/CC
https://www.jpcert.or.jp/at/2023.html

■利用製品の情報から始める

網羅性や速報性はあるが、影響が深刻ではない脆弱性の情報も多く公開される

引用：IPA　https://jvndb.jvn.jp/en/

- CVE-ID・脆弱性の名称
- 対象ソフトウェア・製品
- 概要

開発ベンダやセキュリティベンダのサイトから詳細情報収集

項目	内容
対象バージョン	〇〇
脆弱性発露の条件	〇〇
影響	〇〇
CVSS	〇〇
EPSS	〇〇
KEVC	〇〇
対応策・対応手順	〇〇
緩和策・回避策	〇〇

脆弱性情報収集アプローチの例

■注意喚起情報から始める

2023

公開日	注意喚起内容	テキスト (PGP署名付き)
2023-10-23	Cisco IOS XEのWeb UIの脆弱性(CVE-2023-20198)に関する注意喚起 (更新)	6.37KB
2023-10-20	Citrix ADCおよびCitrix Gatewayの脆弱性 (CVE-2023-4966) に関する注意喚起 (公開)	5.50KB
2023-10-18	Cisco IOS XEのWeb UIにおける権限昇格の脆弱性 (CVE-2023-20198) に関する注意喚起 (公開)	
2023-10-18	2023年10月Oracle製品のクリティカルパッチアップデートに関する注意喚起 (公開)	3.36KB
2023-10-18	ProselfのXML外部実体参照 (XXE) に関する脆弱性を悪用する攻撃の注意喚起 (更新)	5.88KB
2023-10-11	2023年10月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	3.91KB
2023-10-11	Citrix ADCおよびCitrix Gatewayの脆弱性 (CVE-2023-3519) に関する注意喚起 (更新)	7.27KB
2023-10-10	ProselfのXML外部実体参照 (XXE) に関する脆弱性を悪用する攻撃の注意喚起 (公開)	
2023-09-22	Array Networks Array AGシリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起 (更新)	7.81KB
2023-09-19	複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品における任意のコード実行の脆弱性に関する注意喚起 (公開)	4.42KB

引用：JPCERT/CC
https://www.jpcert.or.jp/at/2023.html

■利用製品の情報から始める

引用：IPA　https://jvndb.jvn.jp/en/

- CVE-ID： CVE-2020-5902
- 対象ソフトウェア: F5 Networks BIG-IP
- 概要：略

開発ベンダやセキュリティベンダの
サイトから詳細情報収集

項目	内容
対象バージョン	15系のバージョン 15.0.0 から 15.1.0 まで
脆弱性発露の条件	TMUI(管理画面)が外部からアクセス可能なこと
影響	リモートからの任意コード実行。実際の攻撃観測済み。
CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
EPSS	0.9754
KEVC	記載なし(KEVCが公開される前であるため)
対応策・対応手順	なし(いわゆるゼロデイ脆弱性)
緩和策・回避策	TMUIへのアクセス制限。当該機器へのアクセス制限。

組織におけるリスク評価

前工程との関連性

脆弱性管理の流れ

脆弱性管理対象の識別

脆弱性情報の内容把握
・ソフトウェア/製品の脆弱性の把握
・設定/設計の脆弱性の把握

組織におけるリスク評価

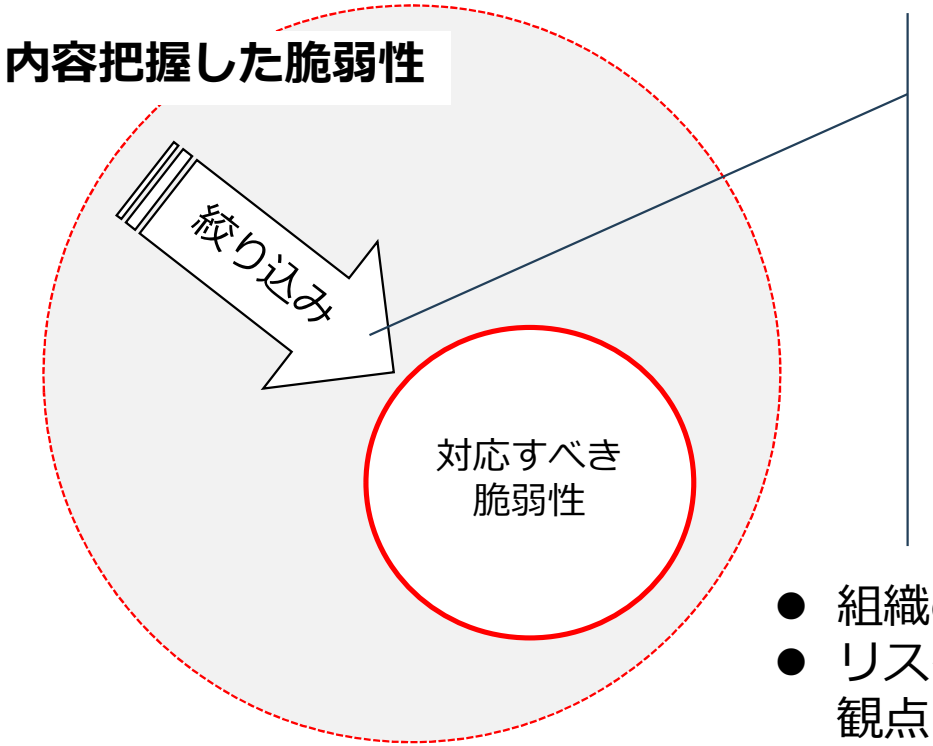
対処・対策

把握事項	目的	例
ソフトウェア名/製品名	・脆弱性情報収集のキーワード	○○ソフトウェア
バージョン情報	・脆弱性に該当するかの確認	1.2.3
機能カテゴリ/保持情報	・リスク評価の判断材料	VPN接続用
構成	・リスク評価の判断材料	社内NWへの接続
外部アクセス可否・ポート情報	・リスク評価の判断材料	インターネットからのアクセス可
設置場所	・リスク評価の判断材料	××ビル
管理者/責任範囲	・対処を行う主体の判断	○○部門

「**脆弱性管理対象の識別**」と「**脆弱性情報の内容把握**」で集めた情報をもとに「**組織におけるリスク評価**」を行う

対応する脆弱性の絞り込み

大量の脆弱性のすべてに対応するのは非現実的であり、
各組織においてどのような脆弱性に対応するかの判断基準が必要となる



【絞り込みの基準例】

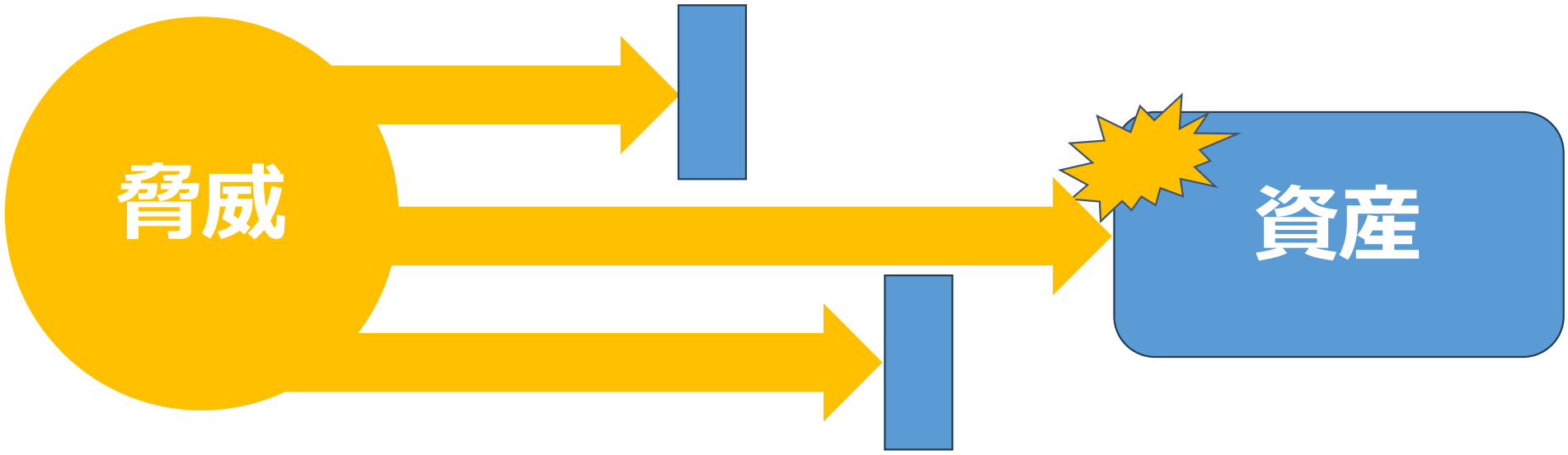
■共通の指標による絞り込み
- 脆弱性の深刻度
- 脆弱性が悪用されている状況　等

■脆弱性スキャナ/脆弱性DBサービスによる絞り込み
- 各製品/サービスのリスクの数値化（スコア）による絞り込み
- 脆弱性の解説/レポート内容による絞り込み

- 組織の事業特性やリソースを考慮した判断基準が必要となる。
- リスクの発生可能性は変動するため、継続的なモニタリングの観点も考慮することが望ましい。

リスク評価

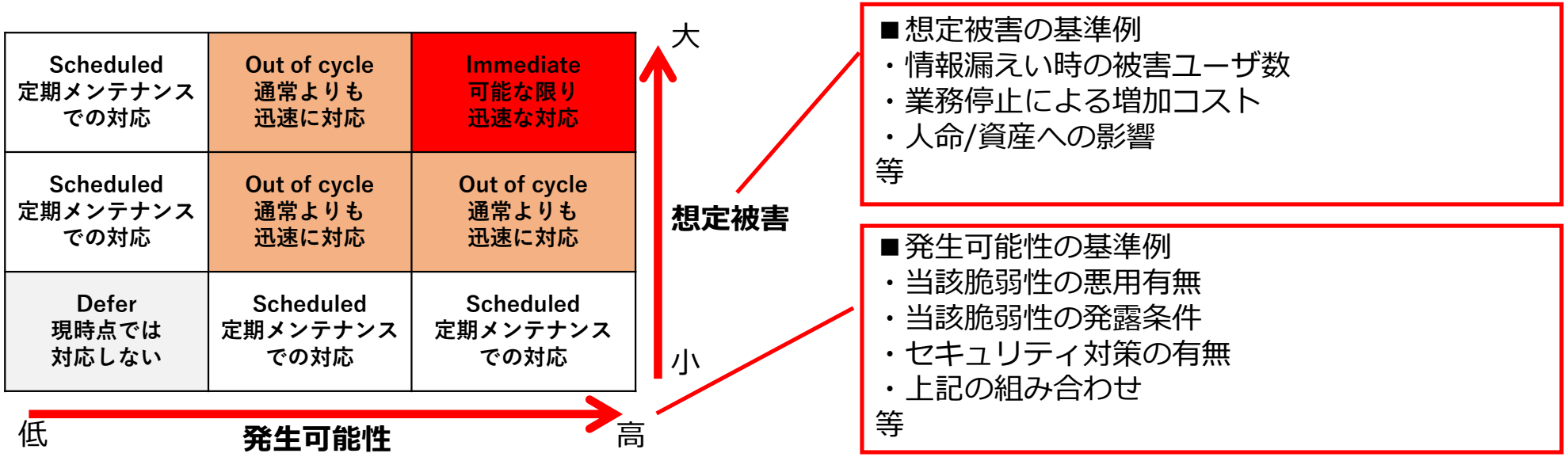
リスク：
脆弱性によってもたらされる、組織に対して損害や影響を発生させる**可能性**



脆弱性が資産に与える影響の大きさのみをリスク評価の物差しに使うのではなく、脆弱性が悪用される可能性（≒脅威度あい）をリスク評価に組み込むことで、効果的な判断に繋げることができる。

組織におけるリスク評価基準

リスク評価基準は各組織のリスク選好性・業務特性によって異なるが、
以下のような例が考えられる



- 前段の絞り込みに用いる指標（CVSS、EPSS等）を活用したリスク評価基準も考えられる。
- リスク評価基準については事前に経営層との合意を取ることが望ましい。
- リスク評価結果については具体的なアクションに結び付いた表現が必要。

リスク評価する際に参考にできる指標、情報

ソフトウェア/製品の脆弱性ごとに付与される下記の指標や情報を参考にリスク評価を行うことができる。

- CVSS（ Common Vulnerability Scoring System ）
- EPSS（Exploit Prediction Scoring System）
- KEVC（Known Exploited Vulnerabilities Catalog）

※設計/設定の脆弱性の場合は別の考え方が必要となるが、
本講演ではソフトウェア/製品の脆弱性に焦点を当てて解説する

CVSS - Common Vulnerability Scoring System

- 脆弱性の深刻度を測定するオープンで標準的な評価手法
- 最新版は v4.0 (2023/10 リリース)
- 各CVEにCVSSスコアが付与され、攻撃の難易度と攻撃による影響の2軸で脆弱性の深刻度を数値化（ 0.0～10.0 ）

攻撃の難易度

攻撃者がシステムを容易に攻撃できるか

攻撃による影響

情報の CIA をどの程度侵害するか

※スコアをもとに利用者が脆弱性対応の要否・緊急性を判断する必要がある。

CVSS v4.0　メトリクスの例

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

【攻撃の難易度】

AV（攻撃ベクトル）:N（Network）　→　攻撃者がネットワークを介して脆弱性を悪用できる
AC（攻撃の複雑さ）:L（Low）　→　攻撃を成功させるために特別な条件や複雑な手順が不要
AT（攻撃の要件）:N（None）　→　攻撃を成功させるために特別な前提条件が不要
PR（特権の必要性）:N（None）　→　攻撃を成功させるために特権が不要
UI（ユーザ関与）:N（None）　→　攻撃を成功させるためにユーザーの関与が不要

【攻撃による影響】

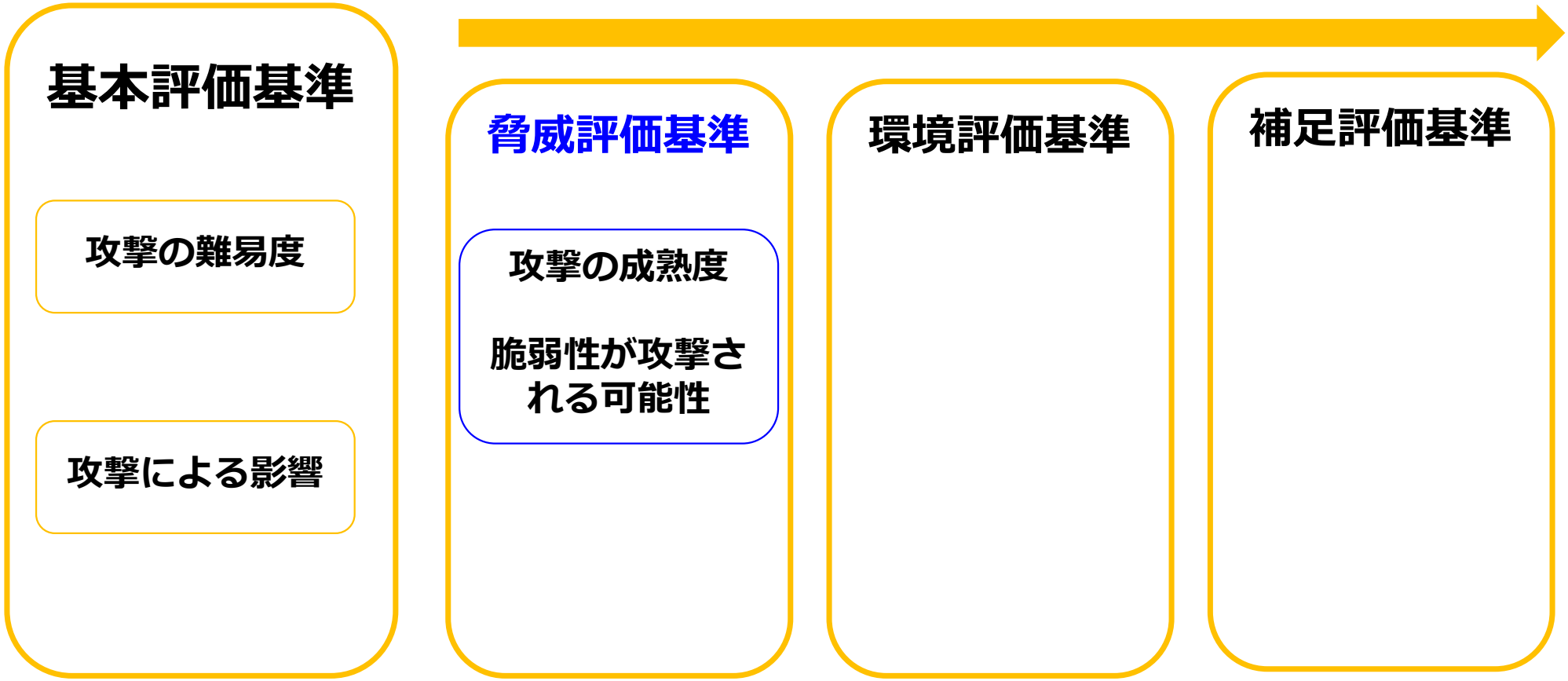
VC（機密性への影響）:H（High）/VI（完全性への影響）:H （High） /VA（可用性への影響）:H （High）
→　攻撃が成功すると機密性、完全性、可用性に重大な影響
SC :N（None）/SI:N（None）/SA:N （None）（後続システム※の機密性、完全性、可用性への影響）
→攻撃が成功しても、後続システムの機密性、完全性、可用性に影響を与えない

※脆弱性が存在するシステム（Vulnerable System）に依存している、またはその影響を受けるシステム

CVSS v4.0 Specification Document

補足：CVSS v4.0

基本評価基準をもとに、利用者が脆弱性対応の要否・緊急性を判断するメトリクスが実装されている

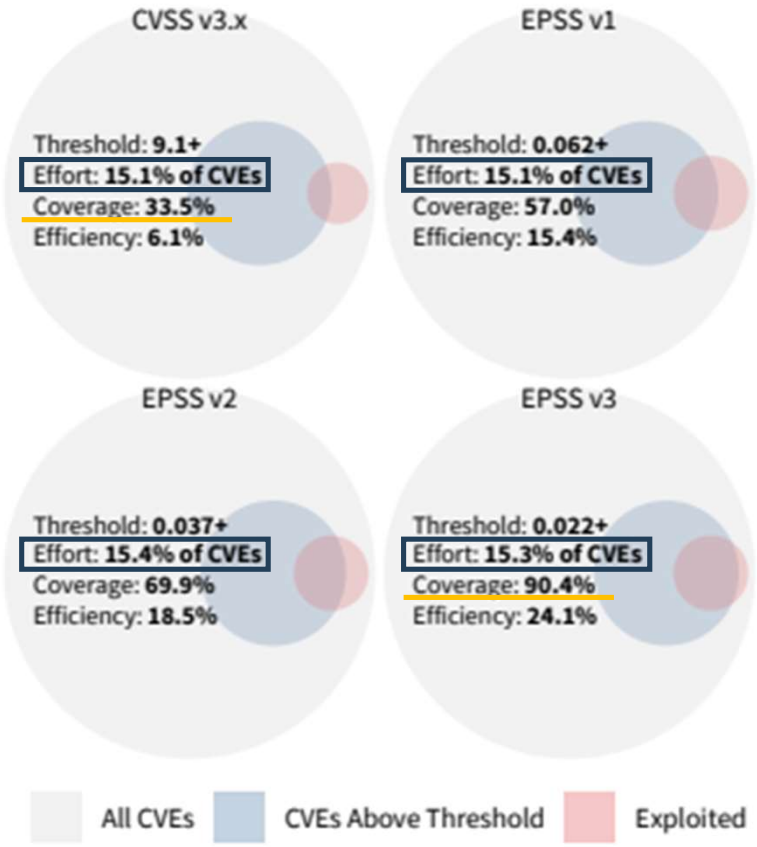


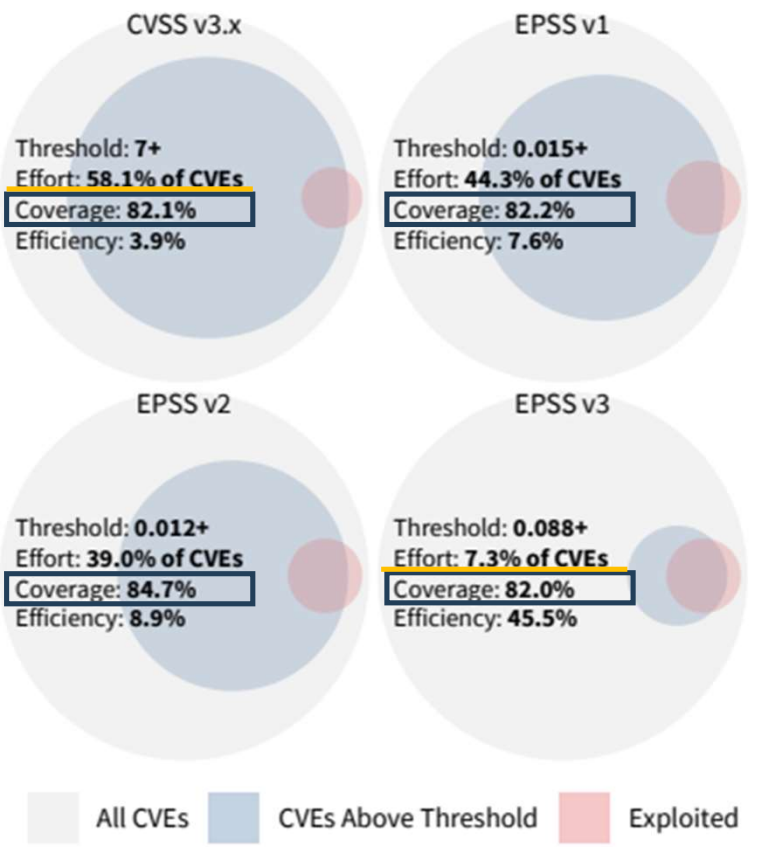
EPSS - Exploit Prediction Scoring System

- ソフトウェアの脆弱性が悪用される可能性（確率）を推定するためのデータ駆動型の取り組み
- スコアは0.0から1.0の範囲で、数値が高いほど悪用される可能性が高い

Exploit Prediction Scoring System (EPSS) (first.org)

EPSSを用いる効果





[Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights (arxiv.org)]

KEVC - Known Exploited Vulnerabilities Catalog

CISA によって管理される実際に悪用された脆弱性情報

- すべての連邦民間行政府（FCEB）機関は、拘束的業務指令（BOD）22-01「既知の悪用される脆弱性の重大なリスクの低減」に基づき、所定の期限内にKEVカタログの脆弱性を是正することが義務付けられている。
- このリストに含まれている脆弱性は既に攻撃に利用されていることが確認されているため、優先的な対応が求められる。

CVE が採番されているか

攻撃が観測されているか

明確な改修ガイダンスがあるか

期間	KEV 新規掲載件数
2023年 07月 ～ 09月	43 件
2023年 10月 ～ 12月	48 件
2024年 01月 ～ 03月	41 件
2024年 04月 ～ 06月	34 件

Reducing the Significant Risk of Known Exploited Vulnerabilities | CISA

リスク評価に使う情報のまとめ

脆弱性管理対象の識別で得た情報と脆弱性情報の内容把握で得た情報（CVSS、EPSS、KEVC記載　等）を元にリスク評価に使う情報をまとめる

脆弱性管理対象の識別で得た情報

把握事項	目的	例
ソフトウェア名/製品名	・脆弱性情報収集のキーワード	○○ソフトウェア
バージョン情報	・脆弱性に該当するかの確認	1.2.3
機能カテゴリ/保持情報	・リスク評価の判断	
構成	・リスク評価の判断	
外部アクセス可否・ポート情報	・リスク評価の判断	
設置場所	・リスク評価の判断	
管理者/責任範囲	・対処を行う主体の	

脆弱性情報の内容把握で得た情報

把握事項	例
CVE-ID・脆弱性の名称	CVE-2024-xxxxx
対象ソフトウェア・製品	○○ソフトウェア
対象バージョン	ver 2.x.x～ver 3.y.y
脆弱性発露の条件	ローカルNWへの接続
影響	アクセス制御の不備による特権昇格
CVSS	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
EPSS	0.12455
KEVC	記載あり
対応策・対応手順	パッチの適用
緩和策・回避策	設定変更・××機能の停止

リスク評価に使う情報

把握事項	例
該当するシステム	××システム
想定される被害	情報漏えい/改ざん/機能停止
機能・サービス	○○業務・×××サービス
保持情報	個人情報（ｘｘｘ万件）
被害発生可能性	高

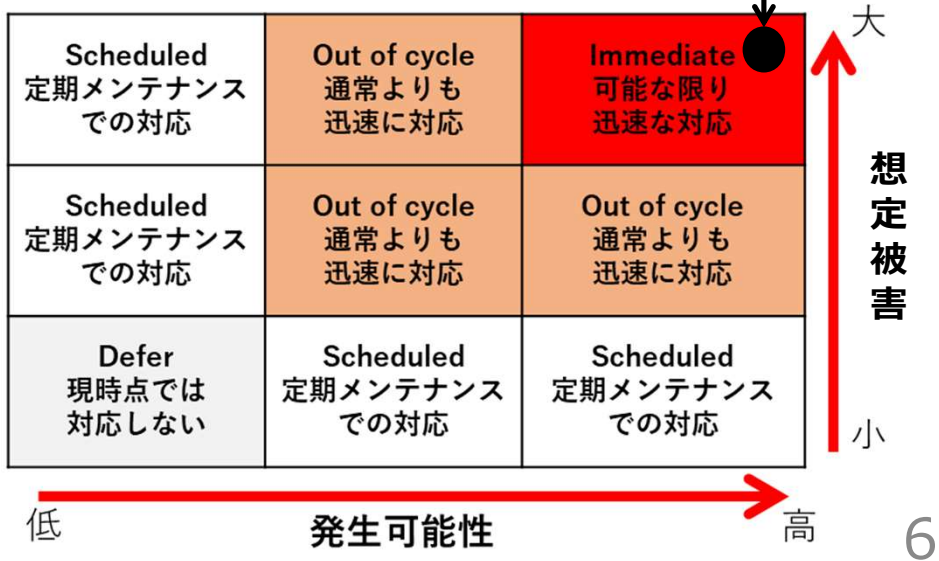
組織におけるリスク評価

リスク評価に使う情報と事前に定めた判断基準を照らしあわせ、
リスク評価を実施する

リスク評価に使う情報

把握事項	例
該当するシステム	××システム
想定される被害	情報漏えい/改ざん/機能停止
機能・サービス	○○業務・×××サービス
保持情報	個人情報（ｘｘｘ万件）
被害発生可能性	高

判断基準へのマッピング



関係部署との合意

- 一貫した判断の根拠を持つこと
  - 社内・社外で共通の基準を合意することが望ましい

- 情報を共有する相手が受け取りやすい工夫

誰に連絡すれば
よいかを把握

連絡先の統一
(PoC)

連絡方法の
統一

手順の標準化

脆弱性専用の
不具合管理

SSVC

リスク評価、意思決定、対処・対策を行う上でSSVCのようなフレームワークの活用も考えられる

SSVC（Stakeholder-Specific Vulnerability Categorization）

- 組織ごとの環境特性を考慮した判断プロセスを事前に整理することで迅速な判断が可能
- 判断プロセスが明確になるためCSIRT（セキュリティ担当）以外の関係者との合意形成に有用
- 参考：https://www.cisa.gov/ssvc-calculator

脆弱性への対処・対策

前工程との関連性

脆弱性管理の流れ

脆弱性管理対象の識別

脆弱性情報の内容把握
・ソフトウェア/製品の脆弱性の把握
・設定/設計の脆弱性の把握

組織におけるリスク評価

対処・対策

リスク評価に使う情報

把握事項	例
該当するシステム	××システム
想定される被害	情報漏えい/改ざん/機能停止
機能・サービス	○○業務・×××サービス
保持情報	個人情報（ｘｘｘ万件）
被害発生可能性	高

判断基準へのマッピング

判断基準（例）

Scheduled 定期メンテナンス での対応	Out of cycle 通常よりも 迅速に対応	Immediate 可能な限り 迅速な対応
Scheduled 定期メンテナンス での対応	Out of cycle 通常よりも 迅速に対応	Out of cycle 通常よりも 迅速に対応
Defer 現時点では 対応しない	Scheduled 定期メンテナンス での対応	Scheduled 定期メンテナンス での対応

大
想定被害
小
低
発生可能性
高

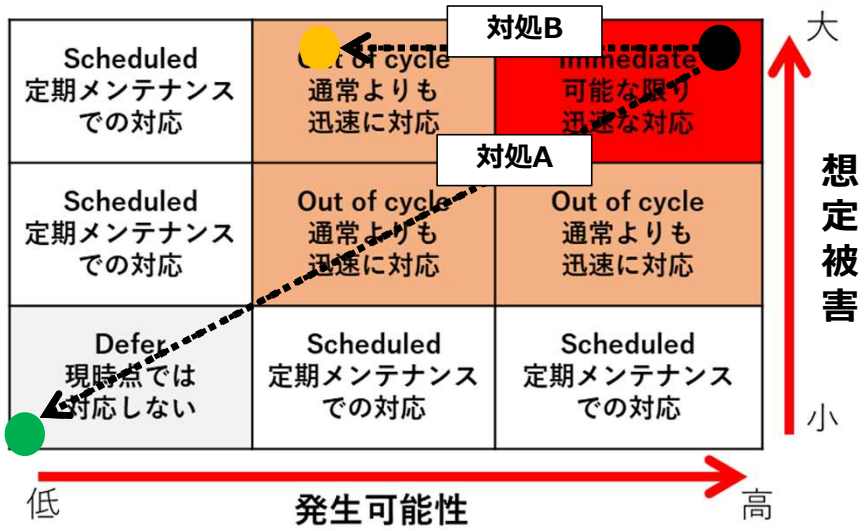
「**組織におけるリスク評価**」で実施したリスク評価をもとに
「**対処・対策**」を行う

対処・対策①

取りうる対処・対策について下記の把握事項を押さえ、リスク評価がどう変わるのかを確認する

対処・対策案	**把握事項**	例
対処A	実施内容	パッチの適用
	効果	脆弱性の解消
	対処案実施の影響	不明のため要検証
	実施可能スケジュール	○月×日（検証後）
対処B	実施内容	・機能の一部停止 ・接続元IPアドレス制限 ・接続可能時間の制限　等
	効果	発生可能性の低減
	対処案実施の影響	無し
	実施可能スケジュール	△月×日

対処A、対処Bそれぞれのリスク評価遷移イメージ



- 対処を実施した場合、リスク評価がどのように変わるかを確認し、追加対策の必要性を検討する。

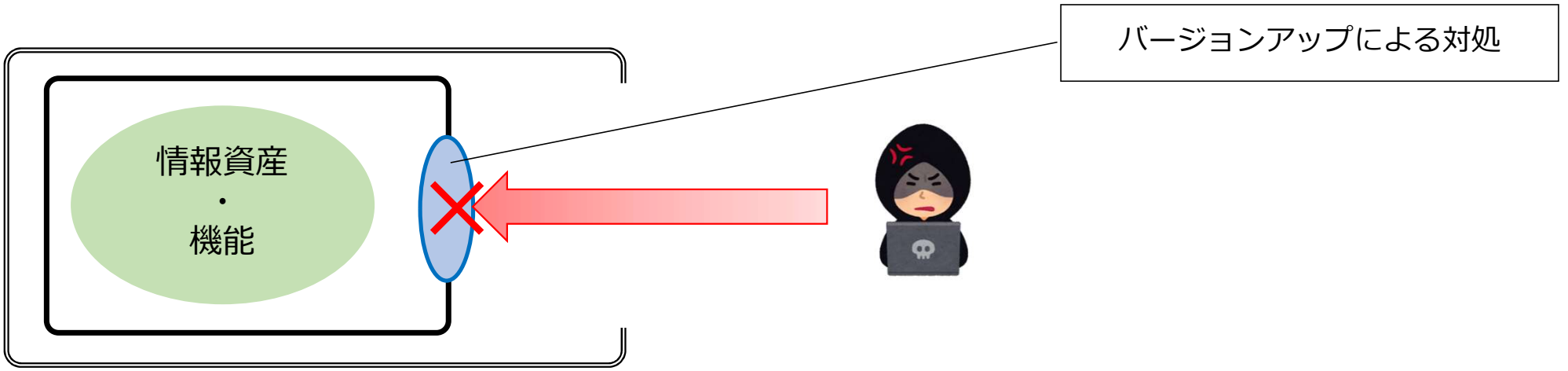
対処・対策②

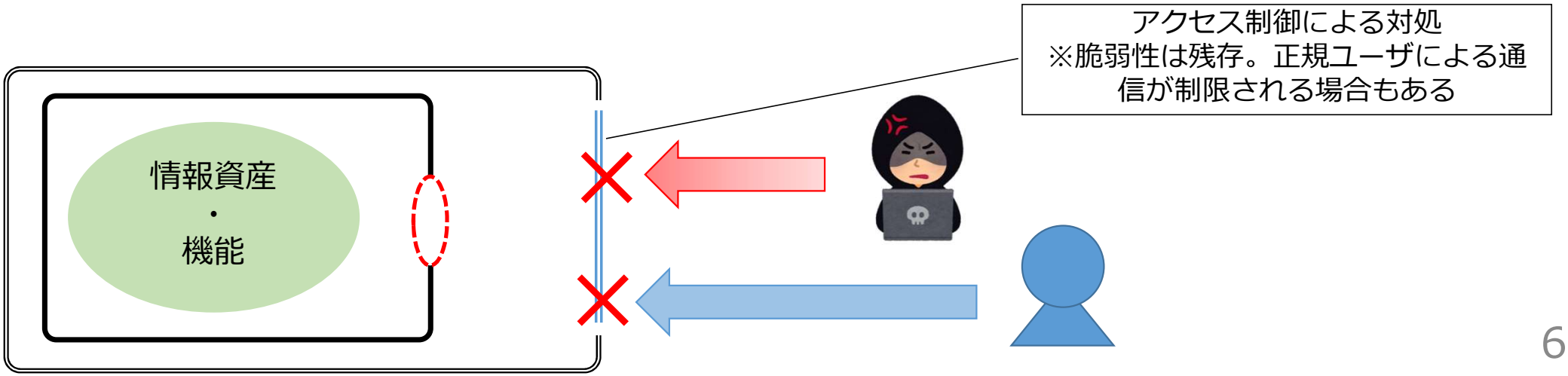
対処・対策には脆弱性の根本原因を解消するものと、暫定的なものがある

【原因の解消】
・パッチの適用、脆弱性が修正されたバージョンへのアップデート（ソフトウェア/製品の脆弱性）
・設計の変更と実装への反映、設定の修正（設計/設定の脆弱性）

【暫定的な対処・対策】
・ネットワーク機器での制限　（※通常の制限に加えた追加制限。通常通信の一部制限を含む）
　・ファイヤーウォールでのポート、IPアドレス制限　等
・セキュリティ機器での対処
　・WAF/IPSによる攻撃検知・遮断　等
・設定変更（※通常の設定に加えた追加設定。機能の一部制限を含む）
　・該当ソフトウェアの設定変更、関連ソフトウェアの設定変更

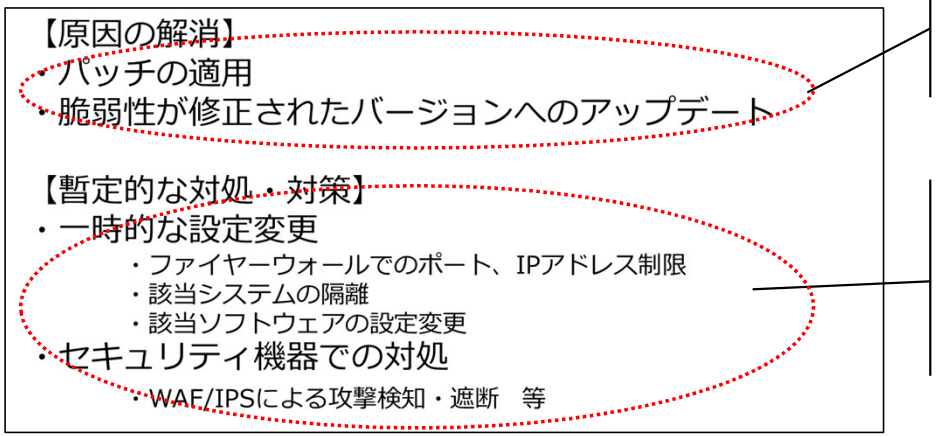
対処・対策のイメージ


バージョンアップによる対処
情報資産
・
機能


アクセス制御による対処
※脆弱性は残存。正規ユーザによる通信が制限される場合もある
情報資産
・
機能

対処・対策の影響

それぞれの対処・対策がシステムにどのような影響を与えるのか考慮する必要がある。



・アップデートによってシステムが提供する機能に影響が出ないか？
例　・アップデート作業による一時的な機能停止
・他のソフトウェア/製品の機能への影響

・発生可能性、想定被害をどこまで緩和できるか？
・システムが提供する機能に影響が出ないか？
例　・WAFへのシグネチャ設定
（適用時点でのエクスプロイト遮断、正常通信の一部遮断等）

対処・対策のための事前合意・契約

- 一般的に取りうる対処・対策の作業を誰がどのような速度で実施するのかについては、事前に関係者との意識合わせをしておくことが望ましい。

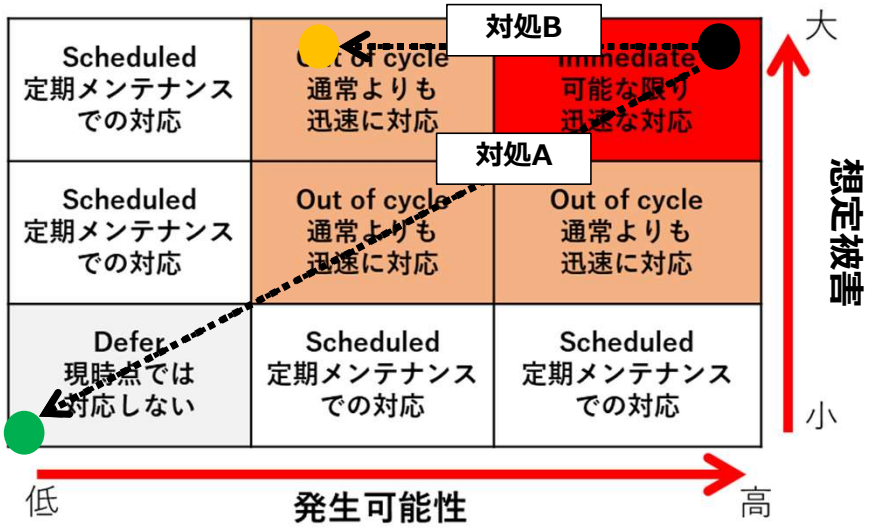
- 実作業についてはソフトウェア/製品の開発ベンダ、保守ベンダ、セキュリティ対策サービスの提供ベンダが行うことも多いため、事前の契約、合意※が必要となる。

●業務委託契約の場合、脆弱性への対処依頼が偽装請負とみなされる行為にならないかに留意し、事前に依頼のフローを定める必要がある。

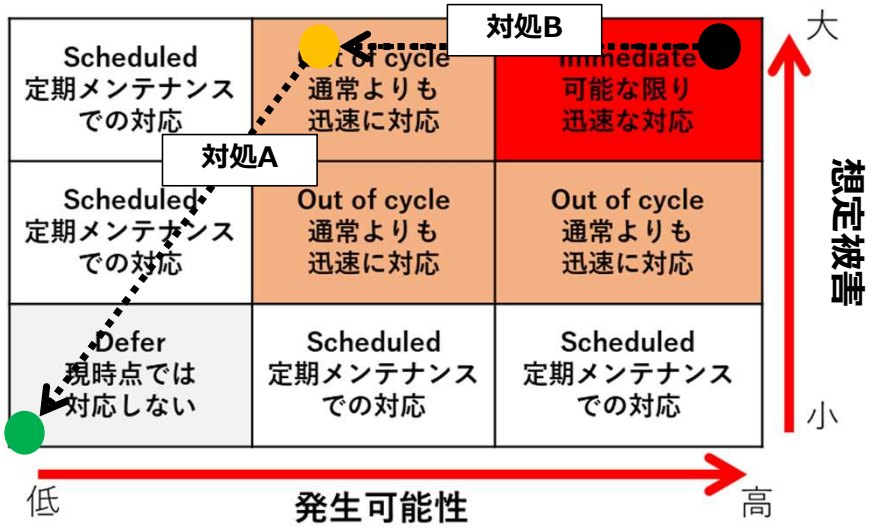
対処・対策の計画

脆弱性を根本的に解消する対処Aがシステムに影響を与える可能性がある場合、
「発生可能性を低減する対処B」→「対処Aの検証による影響確認」
→「対処Aの実施」といった対処計画が考えられる。

対処A、対処Bそれぞれのリスク評価遷移イメージ

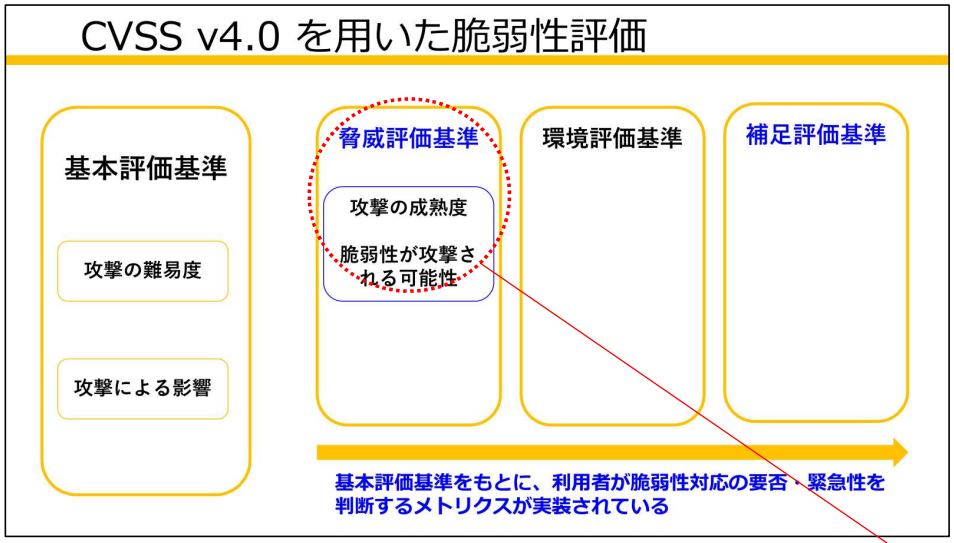


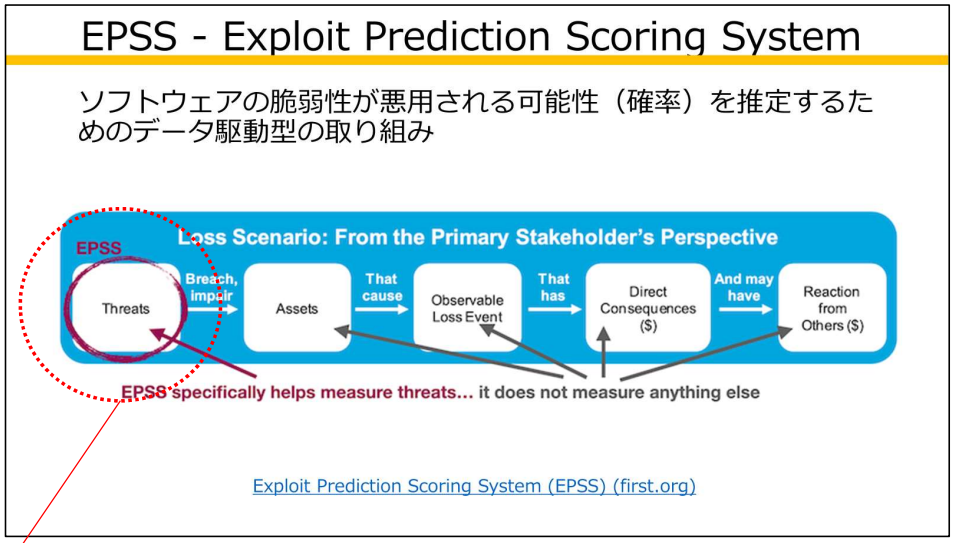
対処Aの検証前に対処Bでリスク緩和を行う際の
リスク評価遷移イメージ



対処・対策の優先順位の変動

リスク評価に用いた指標が変動することにより対処・対策の優先順位も変動する可能性がある。
どのような場合に緊急度が高まるのかについて、関係者と事前に意識合わせをしておくことが望ましい。





脅威が変わることによりリスク評価の変化

対処・対策状況の管理①

対処・対策は中長期に及ぶこともあるため、各脆弱性の対処状況についても定期的なモニタリングが必要となる。

脆弱性	対象システム	対処スケジュール
		1月 / 2月 / 3月 / 4月
CVE-2024-xxx1	システム①	▲対処済み
	システム②	▲対処予定
	システム③	▲対処予定
CVE-2024-xxx2	システム①	▲対処済み
	システム③	▲対処予定

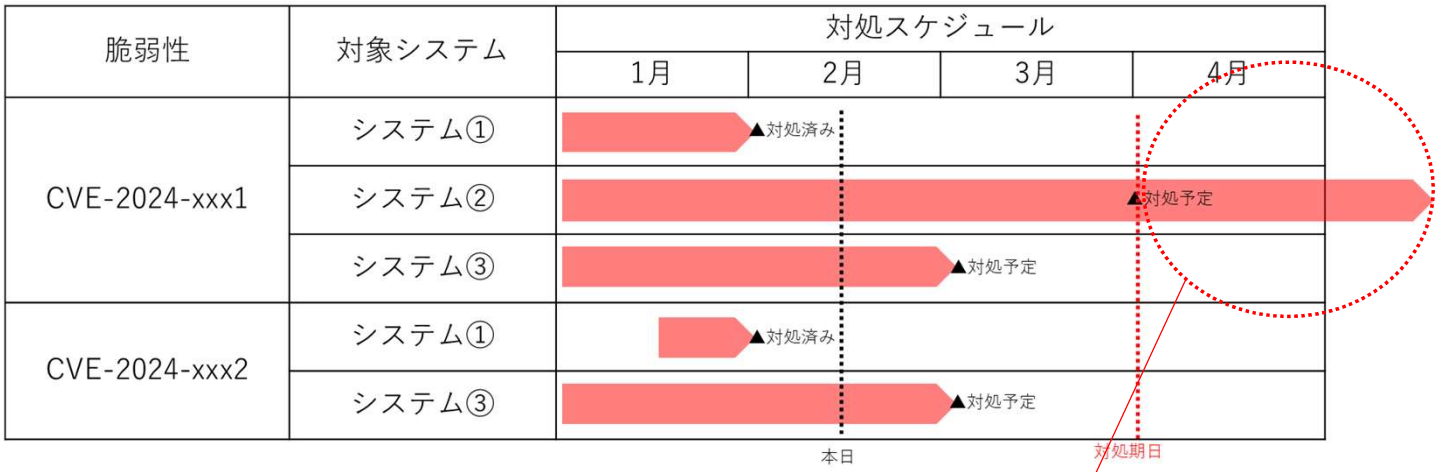
本日　　対処期日

予定通りに対処が実施されているか

・対処予定に変更はないか
・前提となるリスク評価に変化はないか

対処・対策状況の管理②

- 事前に定めた対処期日を超過しても対処・対策が出来ない場合は、リスク受容（リスク保有）の判断をする必要がある。
- リスク受容（リスク保有）の判断は経営層（または権限移譲された者）との合意に基づき行うことが望ましい。



脆弱性によるリスク評価と対処による影響を比較したうえで、リスク受容（リスク保有）を実施

対処・対策のための態勢

影響が広範囲・深刻な脆弱性の対応においては、通常時とは異なる対応態勢が必要となる場合がある。

【態勢の例】

・即時対応が必要なシステムが複数かつ想定被害が非常に大きい
　→　CISOをトップとした態勢

・即時対応が必要なシステムが複数
　→　セキュリティ部門の長をトップとした態勢

・臨時メンテナンスで対応
　→　システム担当チームとセキュリティ担当者で対応

- 影響範囲・深刻度に応じてどのような対応態勢をとるかは事前に経営層と合意を取る必要がある。

補足：対処・対策

- 前述の対応態勢についてはインシデント対応への移行も踏まえて通常時・非常時の態勢を事前整理しておくことが望ましい。

- 対応態勢について事前整理する際には、対応状況の持続的なモニタリング/レポーティングの範囲・方法も踏まえて検討が必要となる。

継続的な脆弱性管理のために

継続的な脆弱性管理のために

脆弱性管理の流れを継続的に実施するために、業務を文書化が必要。

脆弱性管理対象の識別

↓

脆弱性情報の内容把握

・ソフトウェア/製品の脆弱性の把握
・設定/設計の脆弱性の把握

↓

組織におけるリスク評価

↓

対処・対策

継続的な実施
実効性の維持・改善

業務を文書化

「脆弱性管理対象の識別」の文書化内容

脆弱性管理対象の識別

脆弱性情報の内容把握
・ソフトウェア/製品の脆弱性の把握
・設定/設計の脆弱性の把握

組織におけるリスク評価

対処・対策

・脆弱性管理対象の
組織・システム・サービス
どこまでをみるのか
・対象を識別するための
手順・ツール
・管理区分
（例：システム単位で管理）

「脆弱性情報の内容把握」の文書化内容

脆弱性管理対象の識別

↓

脆弱性情報の内容把握

・ソフトウェア/製品の脆弱性の把握
・設定/設計の脆弱性の把握

↓

組織におけるリスク評価

↓

対処・対策

・脆弱性情報把握の
手順・ツール
-情報収集先（URL等）

「組織におけるリスク評価」の文書化内容

脆弱性管理対象の識別

脆弱性情報の内容把握
- ソフトウェア/製品の脆弱性の把握
- 設定/設計の脆弱性の把握

組織におけるリスク評価

対処・対策

- どのような脆弱性に対応するかの判断基準
- 判断基準に利用する脆弱性の評価指標
- 脆弱性が悪用される可能性の継続的なモニタリングの手順・ツール
- 関係部署との合意事項

「対処・対策」の文書化内容

脆弱性管理対象の識別

脆弱性情報の内容把握
- ソフトウェア/製品の脆弱性の把握
- 設定/設計の脆弱性の把握

組織におけるリスク評価

対処・対策

- 通常時・非常時の態勢
- 持続的なモニタリング/レポーティングの範囲・方法

簡易チェックリスト

チェックリスト①

脆弱性管理対象の識別

確認ポイント	✓
ソフトウェア名/製品名	
バージョン情報	
構成情報	
管理している担当	
識別する手順・ツール	

チェックリスト②

脆弱性情報の内容把握

・ソフトウェア/製品の脆弱性の把握
・設定/設計の脆弱性の把握

確認ポイント	✓
脆弱性情報の集める情報源	
脆弱性に該当するソフトウェア・バージョンの把握する際のポイント	
脆弱性の発露条件・影響の把握する際のポイント	
対応策・対策手順の把握する際のポイント	
緩和策・回避策の把握する際のポイント	

チェックリスト③

組織におけるリスク評価

確認ポイント	✓
リスク評価基準の準備（事前に経営層と合意済みであればなおよい）	
絞り込みに用いる指標（CVSS等）の選択	
絞り込みの手順・ツール（スキャナやDBサービス等）	
変動するリスクの継続的なモニタリング	
関係部署の把握（誰とどう連絡を取るのか）	

チェックリスト④

対処・対策

確認ポイント	✓
対処・対策状況の管理方法	
対処・対策の作業は誰がどのような速度で実施するか事前の意識合わせ	
関係するベンダとの事前契約・合意	
通常時・緊急時の体勢について事前の合意	
リスク評価が変動した際の方針について関係者と事前の意識合わせ	
リスク受容（リスク保有）の判断する方法	

まとめ

- 脆弱性管理の難しさとして、大量かつ様々な脆弱性によるまだ起きていない（そして起こらないかもしれない）事柄に対して対処・対策をしなければならない、という点があります。

- 効果的な脆弱性管理を行うためには
  - 脆弱性管理対象の識別
  - 脆弱性情報の内容把握
  - 組織におけるリスク評価
  - 対処・対策

  の各工程のつながりを理解したうえで、
  リソース/手順の整備や関係者との事前合意をする必要があります。

- リスク評価に用いた指標・情報は変動し、また対処・対策は中長期に及ぶ可能性があるため、継続的なモニタリングを行いながら脆弱性管理をする必要があります。

さいごに

- 本講演のもととなった脆弱性管理の手引書は下記にて公開しています

https://www.nca.gr.jp/activity/pub_doc/_10.html

- 今回触れていない部分についてのコラムもあるので、興味がございましたら是非読んでみてください