TLP:CLEAR

脆弱性管理の手引書
（Ver.1.0）公開版
■システム管理者 編

脆弱性管理WG

TLP:CLEAR

改版履歴

- 2024.07.31 1.0版 初版作成
- 2024.10.17　1.0版（公開版）　更新

TLP:CLEAR

はじめに

本資料の目的・ターゲット

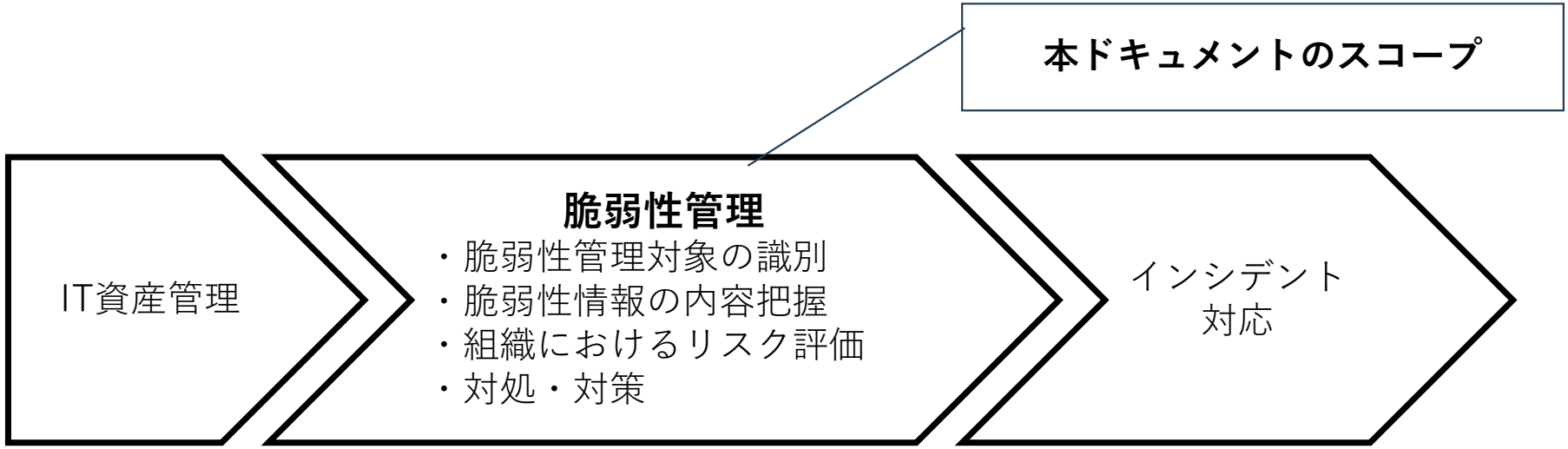
セキュリティを考える際の脆弱性管理の重要性は多くの人が認識するところであるが、
どのような事項が脆弱性管理に必要かはその立場によって異なる。
本ドキュメントでは日本シーサート協議会　脆弱性管理WGにおける議論で得た知見を整理し、
脆弱性管理に必要な事項を立場ごとに分けて記載することで、
セキュリティ担当者（CSIRTメンバ）がユーザ（システム管理者）、ITサービス/製品の提供者、
システムインテグレータ（Sier）が各々実施すべき脆弱性管理の要点を把握する一助となること
を目指す。
初版はユーザ（システム管理者）の立場での脆弱性管理について記載を行う。

TLP:CLEAR

本ドキュメントのスコープ

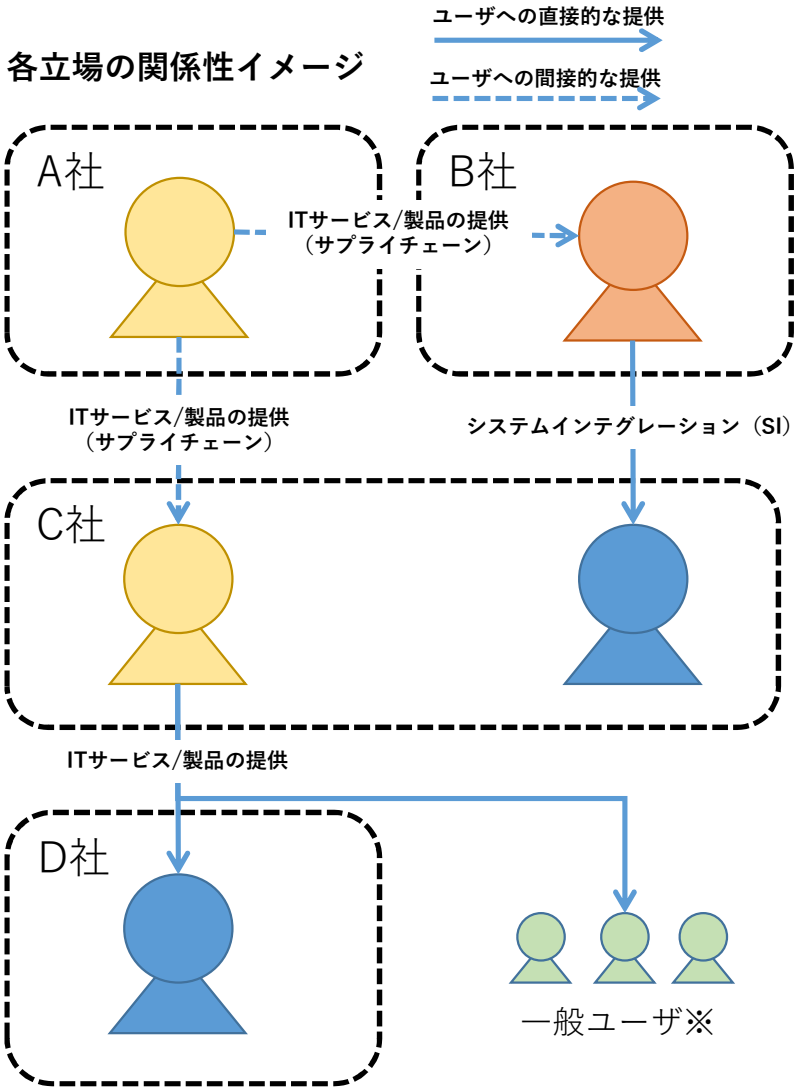
・IT資産そのものの識別に関しても様々な問題/課題は存在するが、
本ドキュメントでは脆弱性管理にフォーカスするため、ある程度のIT資産の識別（IT資産管理）がされている前提で脆弱性管理に必要なポイントを記載する。

・インシデント対応の際においても脆弱性管理で得た情報は活用されるが、
（現時点では）本ドキュメントのスコープ外とする。



TLP:CLEAR

脆弱性管理を行う立場の分類



本ドキュメントでは下記のように立場を分け、主にユーザ（システム管理者）の立場での脆弱性管理のポイントを記載する。

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

ITサービス/製品の提供者

・ITサービス/製品を直接的または間接（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）

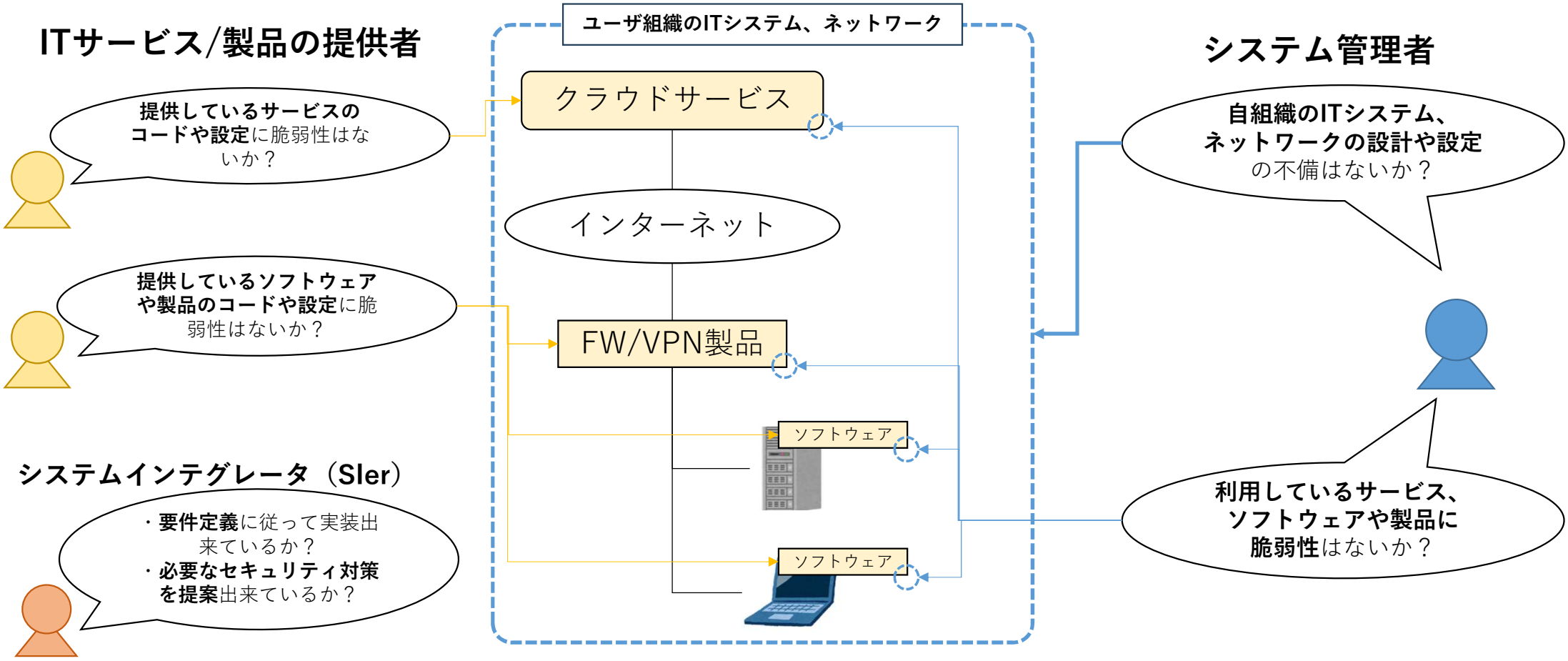
・ユーザの要望に従ってシステムを構築する立場
・契約不適合にならないように脆弱性管理を行う

※一般ユーザの立場での脆弱性管理については本ドキュメントでは言及しない

TLP:CLEAR

立場毎の脆弱性管理の観点

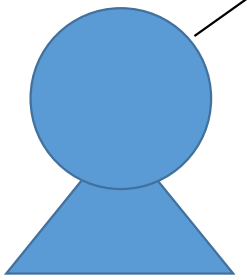
同じ「脆弱性管理」であってもその立場によって観点は異なる



TLP:CLEAR

システム管理者の観点

システム管理者の立場から考えた場合、下記のような観点での確認が必要となる



システム管理者

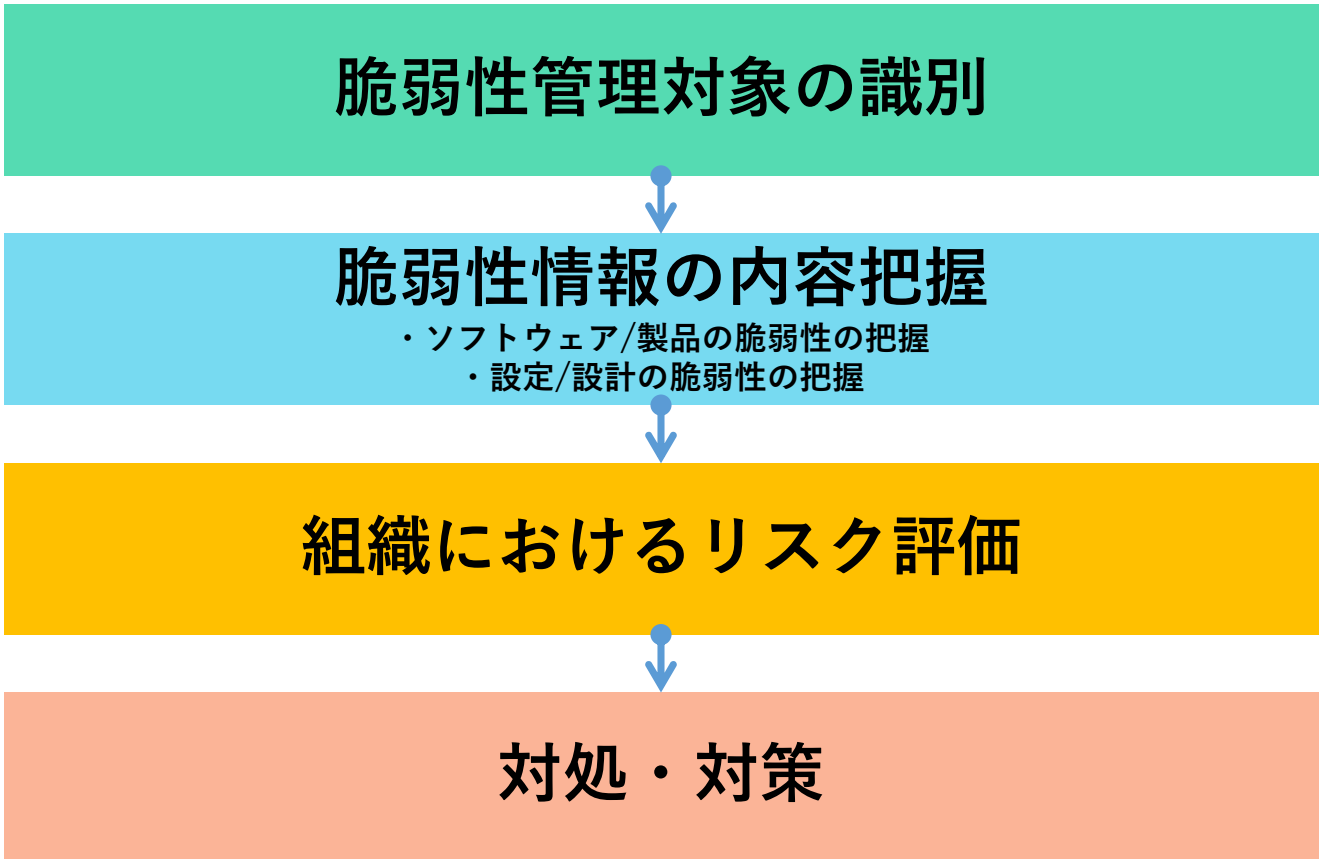
・脆弱性管理の対象は何か？
・利用しているソフトウェア・製品の脆弱性に
どのように対応するか？
・自組織のITシステム・ネットワークの設定/設計は適切か？

※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。

TLP:CLEAR

システム管理者観点での脆弱性管理の流れ

システム管理者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①

TLP:CLEAR

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②

TLP:CLEAR

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。

脆弱性管理対象の識別（管理区分の例）

TLP:CLEAR

■サービス・機能を起点

サービス・機能Ⅰ	関連システム・サーバ	システムA
		システムB
	管理組織・責任者	○○部△△
サービス・機能Ⅱ	関連システム・サーバ	システムA
		システムC
	管理組織・責任者	○○部□□

■ソフトウェアを起点

ソフトウェア①	利用システム・サーバ	システムA
		システムB
ソフトウェア②	利用システム・サーバ	システムA

■システム・サーバを起点

システムA	利用ソフトウェア	ソフトウェア①
		ソフトウェア②
	設置場所	○○ビル
	サービス・機能	××機能
システムB	利用ソフトウェア	ソフトウェア①
	設置場所	△△データセンタ
	サービス・機能	□□サービス

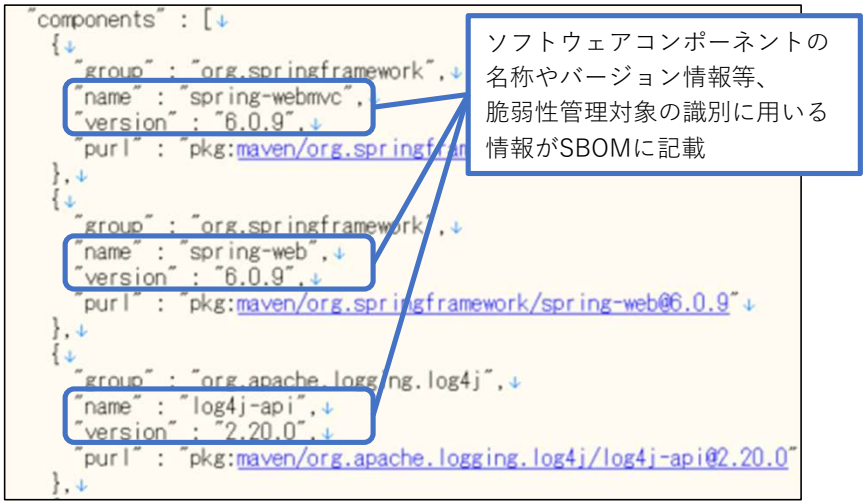
■その他
・設置場所（オンプレ/クラウド等）
・システム区分（閉域/外部公開等）
・組織/会社における価値、重要性

- どのような管理区分を起点とするかは各組織の既存のIT資産管理方法、責任分担、管理対象の規模/種類を考慮して検討する必要がある。

TLP:CLEAR

Column：脆弱性管理対象の識別

脆弱性管理対象の識別において、SBOM (Software Bill of Materials)を活用することも考えられます。
SBOMとは「ソフトウェアコンポーネントを構成する要素のリスト」※1であり、
脆弱性管理対象の識別における情報源として用いることで、特にソフトウェアサプライチェーンにおける『透明性』と『追跡可能性』が期待されます。



SBOMのイメージ(抜粋)
ソフトウェアの部品(ライブラリ, パッケージ)情報を保持する

SBOMには、ソフトウェアに含まれるコンポーネントの名称やバージョン情報等の情報が記載される。

■メリット※2
・使用コンポーネントの一覧化による脆弱性残留リスクの低減
・脆弱性管理のコスト低減

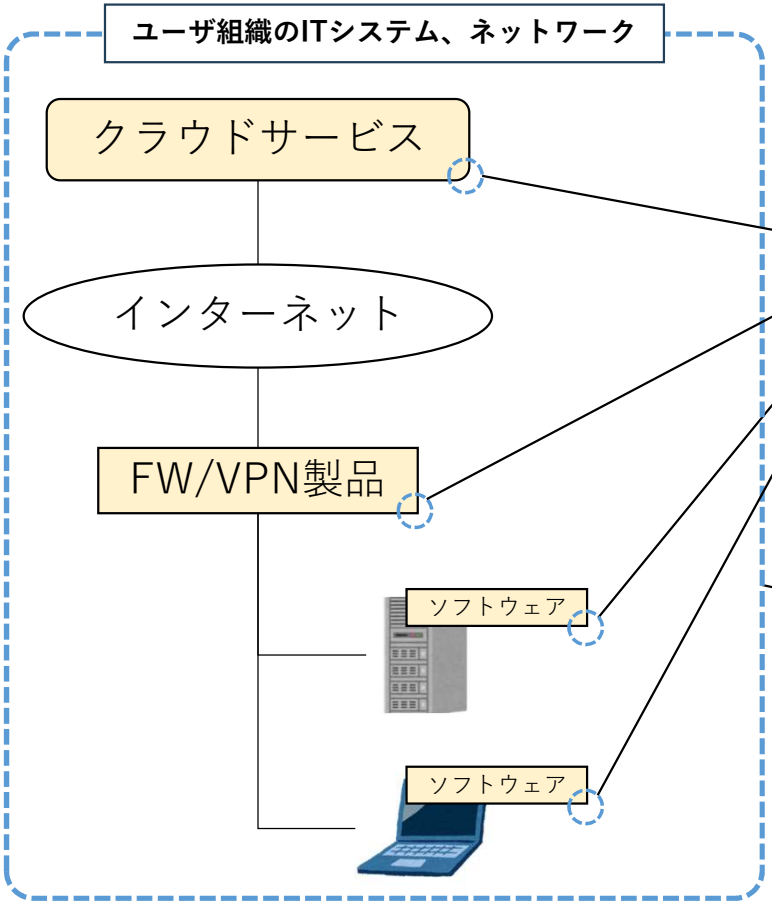
■SBOMを脆弱性管理に活用する際の課題※3
『導入に係るコスト』や『SBOMを作成するツールの出力内容のバラつき』が挙げられる。

※1：米国 CISA, NSA, ODNI, “Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption”, https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF
※2：経済産業省, “サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性”,p10, https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/011_03_00.pdf
※3：STコンソーシアム, “セキュリティ・トランスペアレンシー・コンソーシアム活動ビジョン「セキュリティ透明性の向上と活用に向けて」”, https://www.st-consortium.org/?page_id=1066

脆弱性情報の内容把握

TLP:CLEAR

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

■ソフトウェア/製品の脆弱性の把握①

TLP:CLEAR

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である

把握事項	例
CVE・脆弱性の名称	CVE-2023-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
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/製品の脆弱性の把握②

TLP:CLEAR

ソフトウェア/製品の脆弱性情報把握には下記のような手段が考えられる

■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://jvndb.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

※特定のサービス紹介は本ドキュメント内では割愛

■脆弱性情報配信サービスによる情報収集

※特定のサービス紹介は本ドキュメント内では割愛

■ソフトウェア/製品の脆弱性の把握③

TLP:CLEAR

情報収集の例

■深刻な脆弱性の確認

公開日	注意喚起内容	テキスト (PGP署名付き
023-10-23	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
023-10-20	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
023-10-18	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)	
023-10-18	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
023-10-18	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
023-10-11	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
023-10-11	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
023-10-10	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)	
023-09-22	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
023-09-19	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	4.42KB

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

■特定条件での検索

引用：JVN　https://jvndb.jvn.jp/en/

- **CVE・脆弱性の名称**
- **対象ソフトウェア・製品**

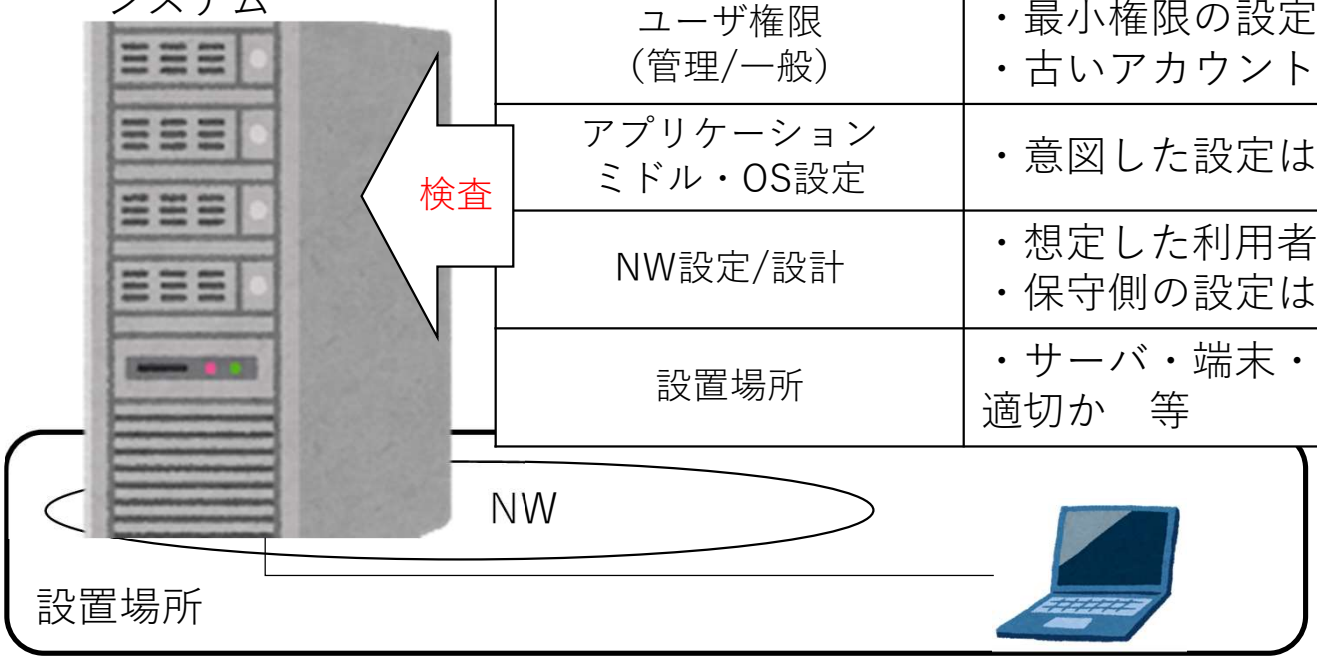
開発ベンダやセキュリティベンダの
サイトから詳細情報収集

- 対象バージョン
- 脆弱性発露の条件
- 影響
- 対応策・対応手順
- 緩和策・回避策

■設定/設計の脆弱性の把握①

TLP:CLEAR

設定/設計の脆弱性の把握には下記の事項を押さえた検査が必要である



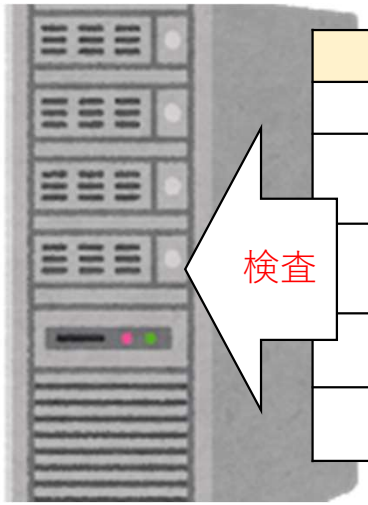
把握事項	確認ポイント※
保持/流通情報	・意図した情報のみが保存/流通しているか　等
ユーザ権限 （管理/一般）	・最小権限の設定はされているか ・古いアカウントが残存していないか　等
アプリケーション ミドル・OS設定	・意図した設定は保たれているか　等
NW設定/設計	・想定した利用者（IPアドレス）に制限できているか ・保守側の設定は適切か　等
設置場所	・サーバ・端末・IoT機器等への物理的なアクセス制限は適切か　等

※各組織の規程に準拠した確認が必要

■設定/設計の脆弱性の把握②

TLP:CLEAR

検査での確認ポイントは各組織の規程類やインシデント・誤設定事例を考慮し、必要な事項を反映する必要がある



検査

把握事項	確認ポイント※
保持/流通情報	・意図した情報のみが保存/流通しているか　等
ユーザ権限 （管理/一般）	・最小権限の設定はされているか ・古いアカウントが残存していないか　等
アプリケーション ミドル・OS設定	・意図した設定は保たれているか　等
NW設定/設計	・想定した利用者（IPアドレス）に制限できているか ・保守側の設定は適切か　等
設置場所	・サーバ・端末・IoT機器等への物理的なアクセス制限は適切か　等

規程類との
比較・反映

各組織の規程類

- セキュリティポリシ
- スタンダード
- マニュアル
- 設計書
- 業務指示文書

インシデント・
誤設定事例
との比較・反映

■セキュリティニュースサイト、ブログ
■製品ベンダからの情報
■利用クラウドサービスからの通知　等

脆弱性情報の内容把握（全体イメージ）

TLP:CLEAR

脆弱性管理対象の識別

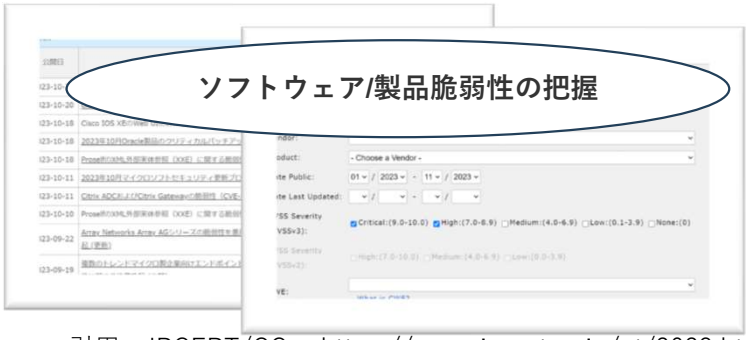
システムA	利用ソフトウェア	ソフトウェア①
		ソフトウェア②
	設置場所	○○ビル
	機能	××機能

システムB	利用ソフトウェア	ソフトウェア①
		ソフトウェア③
	設置場所	○○ビル
	機能	△△機能

情報収集
該非確認

検査

脆弱性の公開等を契機とした脆弱性の把握



引用：JPCERT/CC　https://www.jpcert.or.jp/at/2023.html
JVN　https://jvndb.jvn.jp/en/

定期検査や規定見直し等を契機とした脆弱性の把握

把握事項	確認ポイント※
保持/流通情報	
（管理）	
アプリケーション ミドル・OS設定	・意図した設定は保たれているか　等
NW設定/設計	・想定した利用者（IPアドレス）に制限できているか ・保守側の設定は適切か　等
設置場所	・サーバ・端末・IoT機器等への物理的なアクセス制限は適切か　等

設定/設計の脆弱性の把握

- 「脆弱性管理対象の識別」と「脆弱性情報の内容把握」によって脆弱性を持つIT資産と脆弱性の発露条件/影響を把握できる。

TLP:CLEAR

Column：外部ツールを使った脆弱性の内容把握

これまで解説した通り、設計やメンテナンス時点の設定情報を把握しておくことはシステムの脆弱性管理において重要です。しかし、設定変更時の情報更新漏れやそもそも設計時の考慮漏れなど、複数のシステムを管理しているほど、完全に把握することが難しいです。そこで、ペンテストツールやAttack Surface Management(ASM)、Cloud Security Posture Management(CSPM)などの外部ツールやサービスを活用することによって、現時点での設定や脆弱性の把握を補完されることが期待できます。

- ペンテストツール

ペンテストツールは脆弱性診断(ペンテスト)業務に利用されるツールです。無償であったり、シンプルなものであったりと、脆弱性診断士ではなくとも簡易的に利用可能なものがあります。ツールの一種であるNWスキャナーでは、ポートの開閉状況や(対象システムにおける)サービス起動状況などを探査し、攻撃者の視点からユーザが意図していない設定を発見することができます。ツールによってはWeb管理画面や認証なしに書き込み可能なDB、期限切れSSL証明書など望ましくない設定を発見するものもあります。
注意点として、これらのツールは攻撃者も悪用するものであり、許可なく自らの管理外NWや機器などに使用することはセキュリティ攻撃と見做される可能性があります。

- Attack Surface Management(ASM)

ASMは外部(インターネット)からアクセス可能なIT資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスです※1。
ベンダーが提供するASMサービスはその性質上、NWスキャナー機能を有していることが多いです。そのため、自らがスキャナーを実行せずとも、ASMサービスが定期的に実行しているため、結果のみを得ることができます。

- Cloud Security Posture Management(CSPM)

CSMPはIaaSやPaaSなどのクラウドインフラストラクチャーの設定や状態を検査することで脆弱な設定や望ましくない設定、アカウントや権限の使い回し、書き込み制限されていないオブジェクトストレージなどリスクの高い状態を発見するツールやサービスです。クラウドサービスプロバイダー(CSP)自体が提供していたり、サードパーティーベンダーが提供していたりします。サードパーティーのサービスは複数のクラウドサービスに対応することで一元管理機能を提供するものが多いです。

※1ASM（Attack Surface Management） 導入ガイダンス, 経済産業省
https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

TLP:CLEAR

Column：デフォルト設定と推奨設定

NW機器などのアプライアンス製品やOS、WordPressなどの一部のサーバーアプリケーション、多くのクラウドサービスでは初期セットアップを容易にするためにデフォルト設定(工場出荷時設定)として、管理機能や外部からコントロール可能なセットアップサービスが起動していたり、それらが全てのNWレンジからアクセス可能だったりします。これらの設定はそれ自体が脆弱な設定であったり、設定値がマニュアル等で公開されていたりするので、攻撃者によく狙われます。そのため、各サービスベンダーやセキュリティ専門家はシステムの設計に合わせてデフォルト設定からの変更を推奨しています。概ねのシステムや環境において堅牢になる望ましい設定を推奨設定と呼んだりします。
推奨設定に変更することで機器自体に脆弱性があった場合にもその発動条件を満たさない、もしくは被害拡大を防ぐ、そもそも攻撃が到達しないなど、セキュリティリスクの低減が期待できます。

- 推奨設定の例
  - 認証が必要な機器やシステムは可能な限り、デフォルトパスワードから変更し二要素以上の認証を設定
  - 利用しないサービスは停止する
  - RDPやWeb管理画面等の管理機能はインターネット側から直接アクセスできないようにする
  - 利用用途に応じて、アカウント(権限)を分ける
  - ログを長期間保存する設定にする

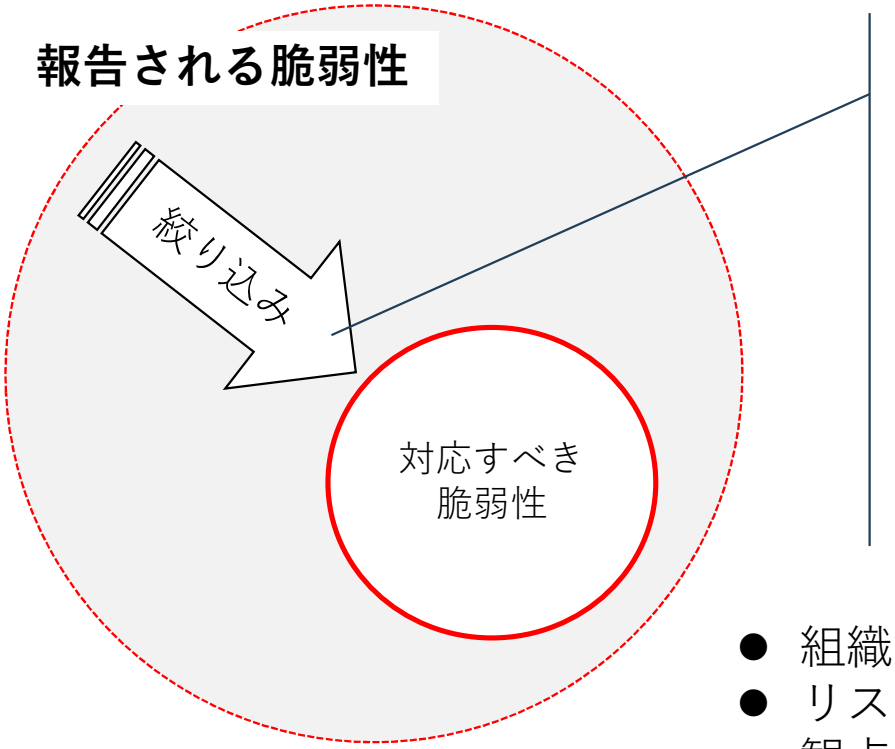
- 脆弱な設定が攻撃に悪用された例
  - Microsoft Windows (WannaCry)
    - インターネット側にファイル共有機能(SMBv1)を公開設定していたサーバーは、ランサムウェアに感染およびファイルを暗号化されてしまった※1
  - Amazon Web Services
    - S3 bucketの書き込み権限設定が制限されていなかったため、攻撃者により決済情報を盗み取る不正な改ざんをされた※2
  - TP-Link (Mirai)
    - Web管理画面の公開設定にて、インターネット側からのアクセスを許可していたWiFiルーターがボットネットに感染してしまった※3

※1ランサムウエア "WannaCrypt" に関する注意喚起, JPCERT/CC
https://www.jpcert.or.jp/at/2017/at170020.html
※2 Incident Report: TaskRouter JS SDK Security Incident - July 19, 2020, twilio
https://web.archive.org/web/20210813010417/https://www.twilio.com/blog/incident-report-taskrouter-js-sdk-july-2020
※3 NICTER 解析チーム
https://twitter.com/nicter_jp/status/1788753973257933189

組織におけるリスク評価①

TLP:CLEAR

大量に報告される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

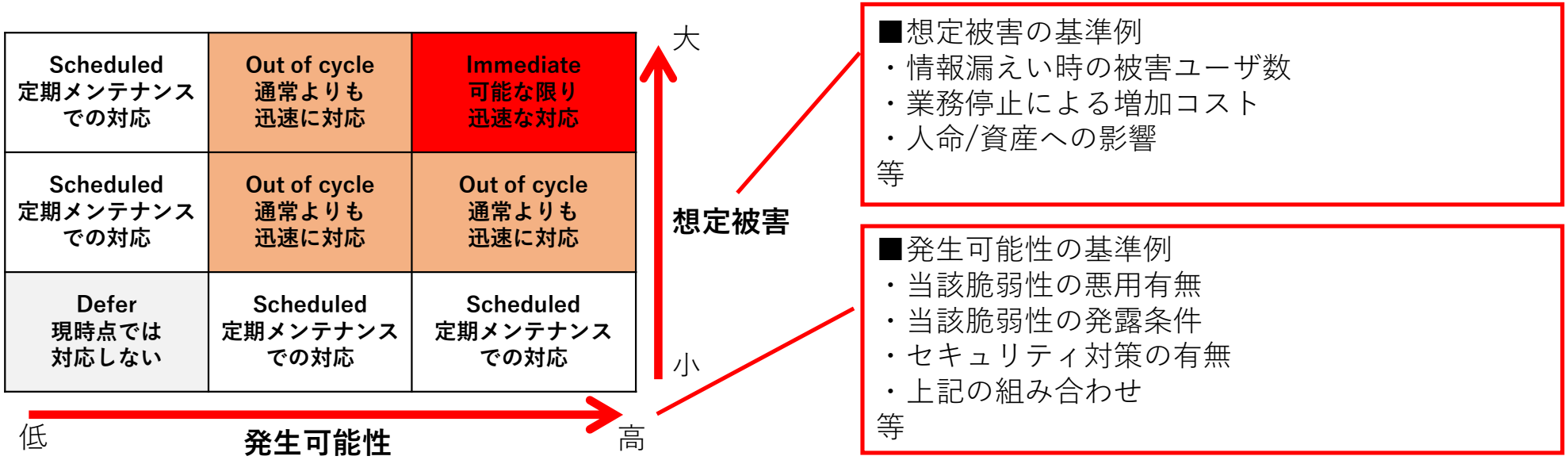
■脆弱性スキャナ/脆弱性DBサービスによる絞り込み
- 各製品/サービスのリスクの数値化（スコア）による絞り込み
- 脆弱性の解説/レポート内容による絞り込み

- 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。

組織におけるリスク評価②

TLP:CLEAR

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。
- リスク評価の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。

組織におけるリスク評価③

TLP:CLEAR

ここまでで把握した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

確認した情報

把握事項	例
該当するシステム	C部門××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

Column：組織におけるリスク評価

TLP:CLEAR

脆弱性の深刻度や影響を評価するための手法は定期的に見直されます。脆弱性の深刻度を表す基準としてよく用いられる CVSS は 2023 年 10 月に v4 がリリースされました。
Common Vulnerability Scoring System (first.org)

また対処するべき脆弱性の対象を絞り込むための手法として、脆弱性が悪用されているかどうかを判断軸として組み込むことが推奨されています。脆弱性が資産に与える深刻度のみをリスク評価の物差しに使うのではなく、脆弱性の脅威度合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ます。代表的な指標として、悪用される可能性を定量化した EPSS や、実際に悪用された脆弱性のリストである KEV などを参照することができます。これらの指標は CVSS を置き換えるものではないことに注意してください。脆弱性が組織に与えるリスクを評価する際には、発生可能性および、対象となる資産に与える想定被害を考慮する必要があり、 脆弱性の深刻度、脅威度合いは、発生可能性の評価をより効果的に行うために活用できます。
Exploit Prediction Scoring System (EPSS) (first.org)
Known Exploited Vulnerabilities Catalog | CISA

これらの判断指標を新規に採用したり更新する際には、関係部門と評価方法の変更点を十分に議論し合意しましょう。リスク評価の結果を具体的なアクションに結び付いた表現とすることは、評価方法の変更時に説明コストを下げる効果が期待されます

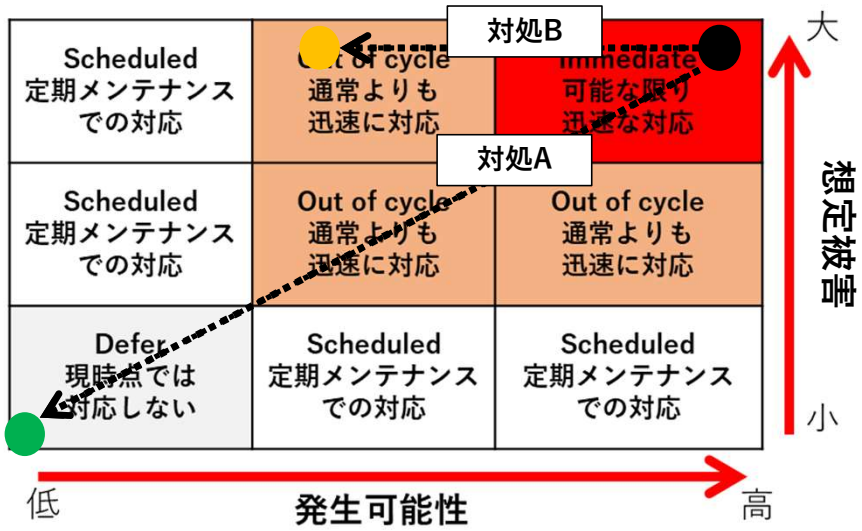
対処・対策①

TLP:CLEAR

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。

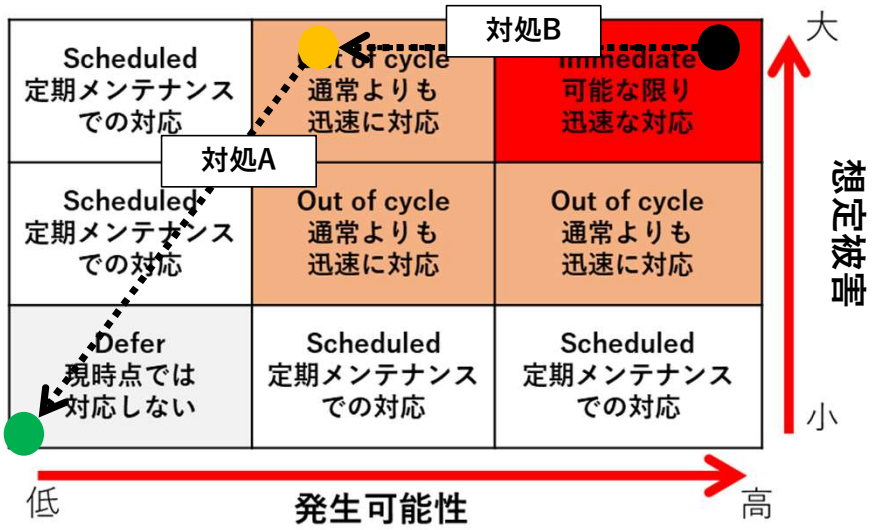
対処・対策②

TLP:CLEAR

実施する対処計画の決定に関しては、関係者とのコミュニケーションを通して
実施の影響、実施可能スケジュールを検討する必要がある

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



- 業務への影響等を考慮するとリスクを解消する対処がすぐには実施できないことも考えられる。
- リスクを緩和する暫定対処策も含めて対処計画を検討する必要がある。

対処・対策③

TLP:CLEAR

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

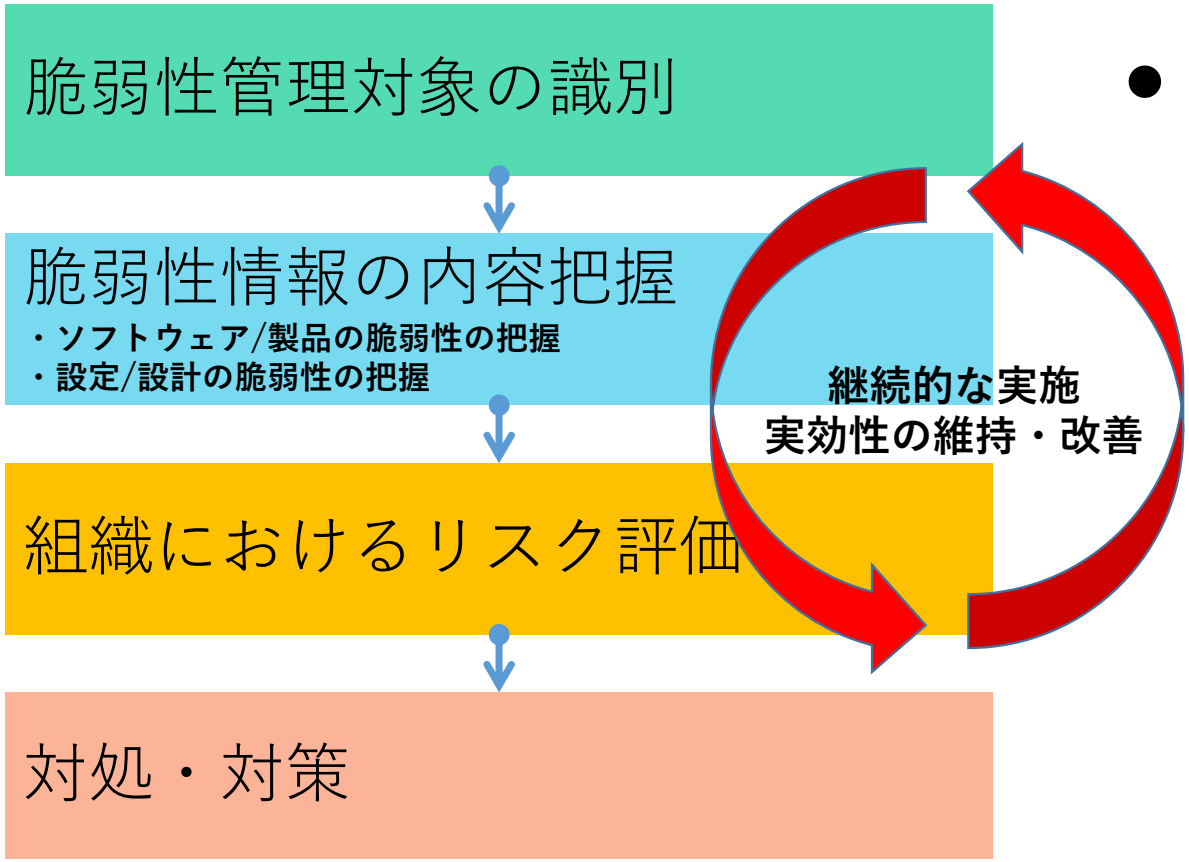
・臨時メンテナンスで対応
　→　システム担当チームとセキュリティ担当者で対応

- 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。

TLP:CLEAR

脆弱性管理とガバナンス

脆弱性管理の流れを継続的に実施するには組織的なガバナンスが必要となる



- **下記事項について文書化し、定期的に見直しを図ることが望ましい。**
  - 組織における脆弱性管理の位置づけ、判断基準、緊急時の態勢に関する経営層の合意
  - 必要なスキルセットの整理と人材の育成
  - 脆弱性管理に必要な手順の整理
  - 脆弱性管理に必要なツール（連絡手段、管理・効率化ツール）の整備

TLP:CLEAR

Column：対処・対策の方針と継続的なモニタリング

脆弱性に起因するすべてのリスクを即座に解消するのは困難です。
どういった優先順位や対応期限を設けるかを事前に考えておく必要があります。
事前に考えておくことにより「攻撃による想定被害、影響度合いを考慮した対応」、「重大な脆弱性への迅速な対応」が可能になります。

考え方の一例としてSSVC（Stakeholder-Specific Vulnerability Categorization）というものがあります。 SSVCは脆弱性の分類と組織の対応方針を決定する手段であり、対応者の立場や環境要因を加味して対処の優先順位付けを行うことができます。
（参考：SSVCツール　https://www.cisa.gov/ssvc-calculator）

優先順位や対応期限の考え方については、経営層や実際に対応する関係者と合意をとりましょう。
考え方について合意できていれば、スムーズな対応が期待できます。
　またリスク対処・対策を実際に実行できているかモニタリングをすることも大切です。 対応完了までに状況（脅威の発生可能性・想定被害 等）が変動することもあるため、定期的に確認しリスクの再評価をする必要があります。
脆弱性管理においては多くのリスクをモニタリングすることになるので、ダッシュボード等を活用した効率的な管理の検討も必要です。

TLP:CLEAR

執筆	日本シーサート協議会 脆弱性管理WG
編集責任	石田 悠（NTT WEST-CIRT　西日本電信電話株式会社）
コラム執筆	脆弱性管理対象の識別：井上 陽水(株式会社NTTデータグループ) 外部ツールを使った脆弱性の内容把握：大石 眞央(NTTDATA-CERT　株式会社NTTデータグループ) デフォルト設定と推奨設定：大石 眞央(NTTDATA-CERT　株式会社NTTデータグループ) 組織におけるリスク評価：伊藤 彰嗣(RM-CSIRT　楽天モバイル株式会社) 対処・対策の方針と継続的なモニタリング：柴田 はるな（NTT WEST-CIRT　西日本電信電話株式会社）
執筆協力	脆弱性管理WGメンバ、寺田 真敏（東京電機大学）

※CSIRT名、会社名は執筆時点のもの