3．CVSSv3を利用した影響分析

共通脆弱性評価システムCVSS
～ CVSS とは何か ～

- CVSS とは…

Common Vulnerability Scoring System
（共通脆弱性評価システム）

- 脆弱性に対する汎用的な評価指標
- 脆弱性の深刻度を 0.0 ～ 10.0 で数値化
- 3 つの基準で脆弱性の深刻度を評価

共通脆弱性評価システムCVSS
～ CVSS の特徴 ～

■ 標準化された評価基準である

ソフトウェアやハードウェアのベンダに依存しない評価基準
のため、異なった製品間の脆弱性を比較する物差しになる

■ オープンである

脆弱性を評価する方法（計算式）が公開されており、誰でも
CVSS スコアを採点することが可能

■ 多数の組織が支持している

多くの組織が CVSS を採用しており、同じ視点で評価作業を
進めることが容易

共通脆弱性評価システムCVSS
～ CVSS の利用目的 ～

■ 脆弱性の深刻度を評価する

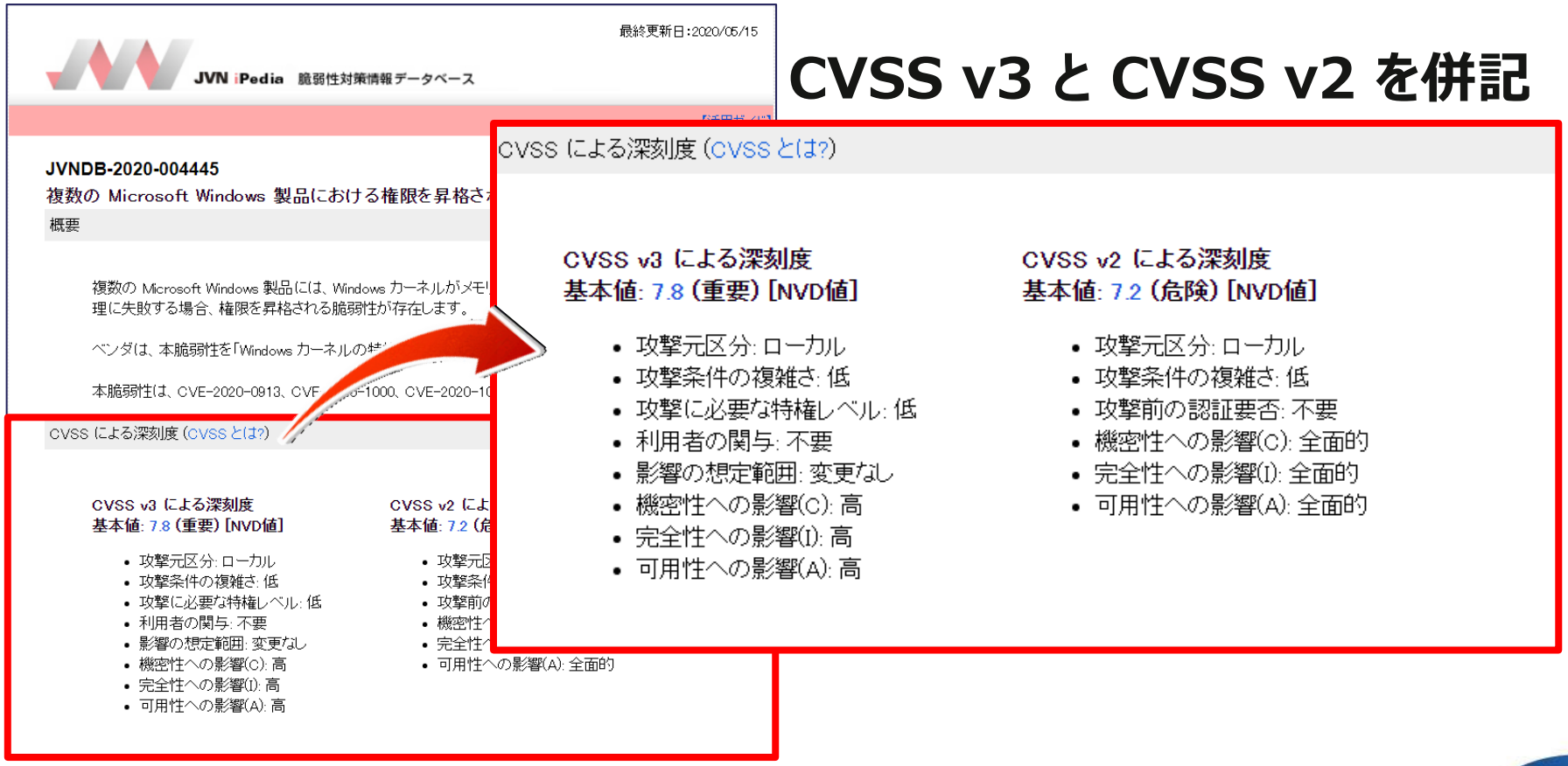
ある脆弱性の深刻度について、非常に深刻なものなのか、
さほど深刻でないものなのかを数値で確認することができる。

■ 脆弱性対策の優先順位をつける

複数の脆弱性がある時、どの脆弱性がより深刻なのかを比較し、
対策に優先順位をつけることができる。

共通脆弱性評価システムCVSS
～ CVSS の確認 ～

IPAが提供する JVN iPedia で CVSS を公開



CVSS v3 と CVSS v2 を併記

https://jvndb.jvn.jp/ja/contents/2020/JVNDB-2020-004445.html

共通脆弱性評価システムCVSS
～ CVSS v2.0 と CVSS v3.0 の違いについて ～

IPA

■CVSS v2.0 から CVSS v3.0 への変更点

■ CVSS v2.0

- 2007年6月に仕様公開
- 多くは v3.0 と併記する形で残存

CVSS v2	
攻撃の難易度	どこから攻撃可能であるか 攻撃元区分(AV:Access Vector)
	攻撃する際に必要な条件の複雑さ 攻撃条件の複雑さ(AC:Access Complexity)
	攻撃するために認証が必要であるか 攻撃前認証要否(Au:Authenticaiton)

■ CVSS v3.0

- 2015年6月に仕様公開
- 仮想化等、技術環境の変化を取込み
- 2019年6月に v3.1 を仕様公開

CVSS v3	
攻撃の難易度	どこから攻撃可能であるか 攻撃元区分(AV:Attack Vector)
	攻撃する際に必要な条件の複雑さ 攻撃条件の複雑さ(AC:Attack Complexity)
	攻撃する際に必要な特権レベル 必要な特権レベル(PR:Privileges Required)
	攻撃する際に必要なユーザ関与レベル ユーザ関与レベル(UI:User Interaction)

詳細は下記ページを参照

https://www.ipa.go.jp/security/vuln/scap/cvss.html
https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

CVSS v3.0 から CVSS v3.1 への変更点

スコアリング指針の明確化

- 攻撃元区分(AV: Attack Vector)の隣接ネットワークに、MPLS、VPNなどを使って接続された管理ネットワークを含めた。
- ソーシャルエンジニアリング攻撃などで、ダウンロードした不正なファイルを開いた場合の攻撃は、攻撃元区分(AV: Attack Vector)をローカルとする。など

v3.0 計算式の不具合の修正

ただし、計算式の不具合の修正による数値上の変動は、最大0.1の増減に留まる。

- 言語によって小数計算に誤差が生じる問題
- 環境評価の再評価において、評価が逆転してしまう問題

CVSS 拡張

- 独自の評価基準を追加できるようにした。

共通脆弱性評価システムCVSS
～ 直近のCVSSの状況 ～

IPA

2023年11月にCVSS v4.0 が公開された

「基本評価基準」の精密化

- 「攻撃の実行条件」を追加
- 「スコープ」の代わりに「後続システムへの影響」（機密性や完全性や可用性）を追加
- 「ユーザ関与レベル」について、従来の要/不要の2択から、アクティブ/パッシブ/なしの3択になり、詳細な評価が可能になった

「現状評価基準」や「環境評価基準」に関する変更

- 「現状評価基準」は「脅威評価基準」に名称を改め、評価項目は「利用可能な対策のレベル」と「脆弱性情報の信頼性」が削除され、「攻撃される可能性」のみに変更
- OT関連システムに関する評価として、環境評価基準では人身への被害を考慮し、「後続システムの完全性への影響」、「後続システムの可用性への影響」に関する評価値として「安全性」を追加

「補助評価基準」を追加

- CVSSのスコアには関係しないが、脆弱性対策を行う上での組織内での評価に有効な「回復可能性」や「対応の困難度」等の評価項目を追加

共通脆弱性評価システムCVSS
～ 直近のCVSSの状況 ～

IPA

■ 2023年11月にCVSS v4.0 が公開された

■ CVSSスコアの命名規則に関する変更

- 従来は評価結果を評価の段階に応じて「基本値」「現状値」「環境値」と呼称していたのを、使用した評価基準に応じて名称が決まる形式に変更された

例：CVSS-BE(基本評価基準（Base Metrics）と環境評価基準（Environmental Metrics）で評価)
CVSS-BT(基本評価基準（Base Metrics）と脅威評価基準（Threat Metrics）で評価)

・NVDで提供されるCVSSはv3のみとなっている（2024年3月時点）

・古い脆弱性対策情報ではCVSS v2,v3両方が提供されている

・CVSS v4の情報は提供が始まっていない

■ 詳細はCVSSを管理しているFIRST(Forum of Incident Response and Security Teams)のWebサイトをご確認下さい
https://www.first.org/cvss/v4-0/

収集した脆弱性の評価
～自組織への影響を分析するために～

IPA

Ｓｔｅｐ１

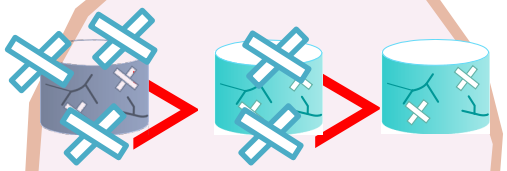
情報の絞込み

全ての情報 → 必要

自組織に関連する情報を抽出

Ｓｔｅｐ２

脆弱性の深刻度を確認



脆弱性の特性や攻撃状況を確認

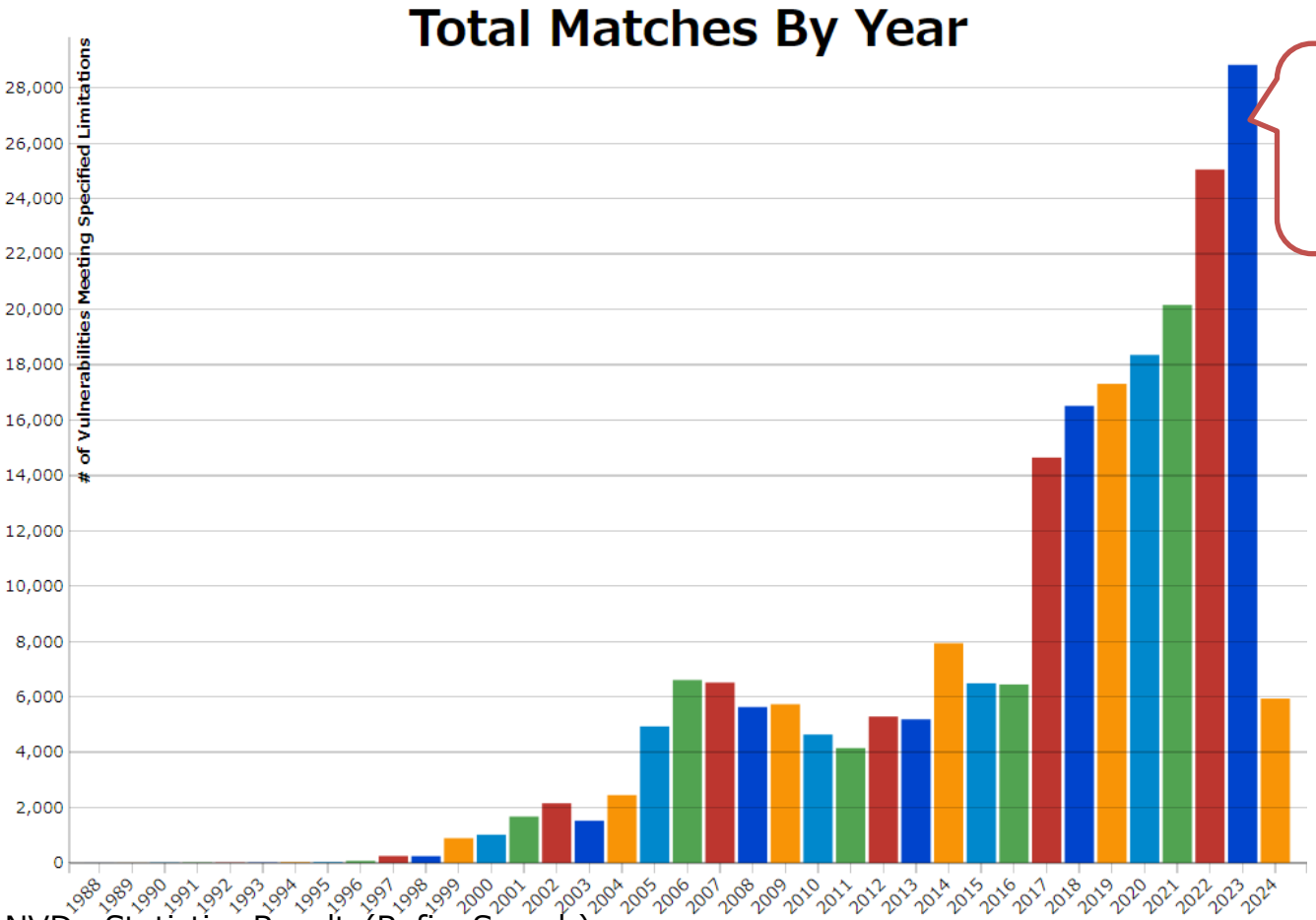
Ｓｔｅｐ３

自組織への影響を分析

自組織の環境を考慮した対策を実施

Step1 情報の絞込み
～自組織に関連する情報を抽出～

■ 日々公表される膨大な数の脆弱性



2023年に登録された
脆弱性の件数だけでも
約29,000件

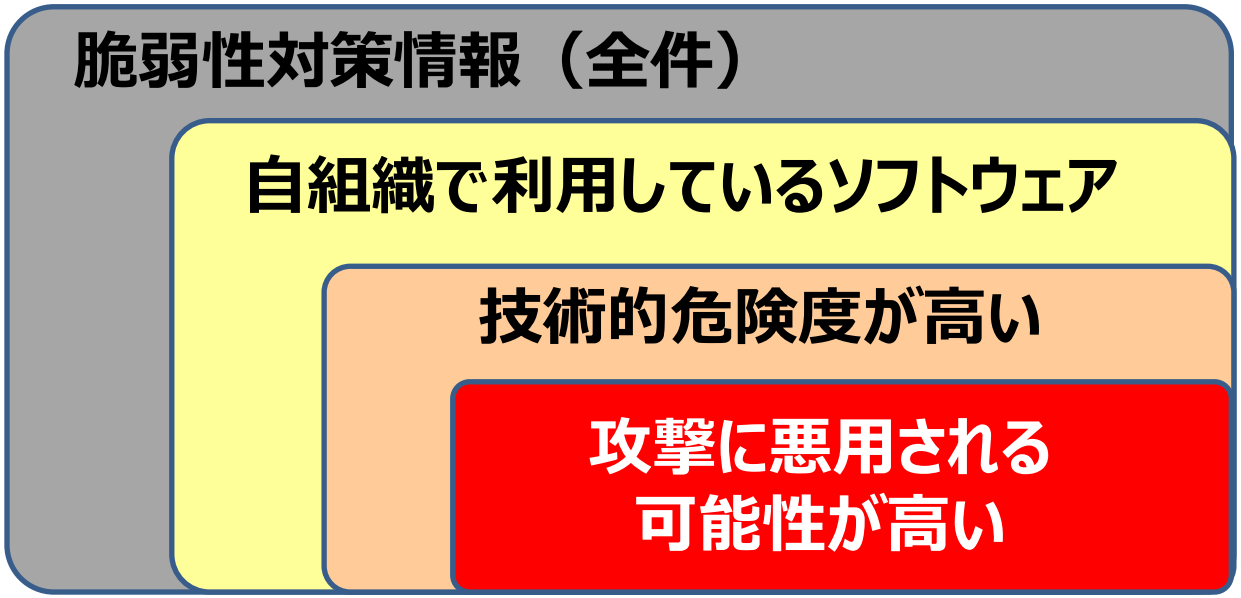
脆弱性情報を全て
確認するのは無理。
どうすれば…

NVD：Statistics Results(RefineSearch)
https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

Step1 情報の絞込み
～自組織に関連する情報を抽出～

■ 自組織に必要な情報だけを抽出することが重要

- 自組織で利用している（関係する）ソフトウェアの情報を収集。
- 収集した情報の中で、「技術的危険度が高いもの」を確認。
- 収集した情報の中で、「攻撃に悪用される可能性が高いもの」を確認。



Step2 脆弱性の深刻度を確認
～脆弱性の特性や攻撃状況を確認～

Ｓｔｅｐ１

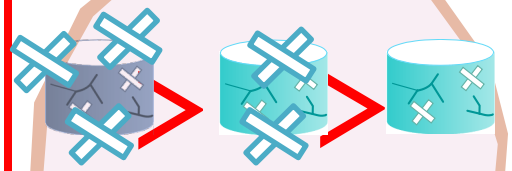
情報の絞込み

全ての情報 → 必要

自組織に関連する情報を抽出

Ｓｔｅｐ２

脆弱性の深刻度を確認



脆弱性の特性や攻撃状況を確認

Ｓｔｅｐ３

自組織への影響を分析

自組織の環境を考慮した対策を実施

Step2 脆弱性の深刻度を確認
～脆弱性の深刻度を確認する際のポイント～

脆弱性に対する評価指標 → CVSS

ポイント

1．脆弱性固有の深刻度はどの程度か？

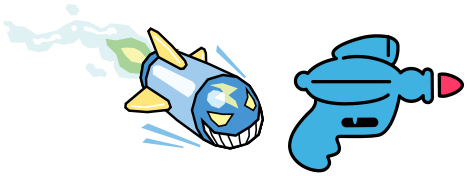
2．いつ被害を受けてもおかしくない状況か？

3．自組織のシステムは危険なのか？

Step2 脆弱性の深刻度を確認
～攻撃状況やシステムの影響度を加味した評価～

■ 脆弱性の深刻度を表す評価

「脆弱性の特性」×「攻撃状況」×「システムへの影響度」



どういう攻撃可能か？
何が侵害されるか？

既に攻撃事例があるか？
対策パッチは出ているか？

システムが機密情報を保持しているか？
システムへの攻撃のしやすさは？
システムが攻撃を受けた場合の影響は？

「SQLインジェクション」×「攻撃観測あり」×「対外システム」
＝**深刻度　高**

「SQLインジェクション」×「攻撃観測なし」×「作業用PC」
＝**深刻度　低**

CVSSとは
～評価基準一覧～

- **評価方法は公開されており、だれでもＣＶＳＳスコアを採点することができます**

Ｓｔｅｐ２

基本評価基準 (0.0 ～ 10.0)	脆弱性の技術的な特性を評価 例：ネットワークから攻撃可能なら危険大 例：攻撃方法が難しければ危険小
現状評価基準 (0.0 ～ 10.0)	ある時点における脆弱性を取り巻く状況を評価 例：ゼロデイ攻撃があれば危険大 例：攻撃コードが利用不可であれば危険小
環境評価基準 (0.0 ～ 10.0)	そのシステムにおける問題の大きさを評価 例：社内の基幹システムで影響大なら危険大 例：被害予想が少なければ危険小

※現状評価基準および環境評価基準は、基本評価基準を元に算出されます
※現状評価を最大と仮定して環境評価を行うことも可能です

CVSSv3 基本評価基準
～脆弱性そのものの特性を評価～

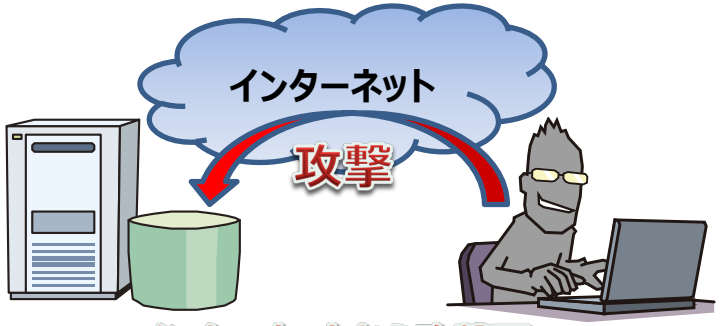
IPA

■基本評価基準とは？

✓ 攻撃の難易度

ローカル攻撃のみ可

OR



インターネットから攻撃可

✓ 攻撃による影響

CVSSv3 基本評価
～脆弱性そのものの特性を評価～

危険小 ⟷ 危険大

	評価項目	選択肢・ポイント			
攻撃の難易度	どこから攻撃可能であるか 攻撃元区分 (AV:Attack Vector)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
	攻撃する際に必要な条件の複雑さ 攻撃条件の複雑さ (AC:Attack Complexity)	高 (H)		低 (L)	
	攻撃する際に必要な特権のレベル 必要な特権レベル (PR:Privileges Required)	高 (H)	低 (L)		不要 (N)
	攻撃する際に必要なユーザ関与レベル ユーザ関与レベル (UI:User Interaction)	要 (R)		不要 (N)	
攻撃による影響	攻撃による影響の想定範囲 スコープ (S:Scope)	変更なし (U)		変更あり (C)	
	機密情報が漏えいする可能性 機密性への影響 (C:Confidentiality Impact)	なし (N)	低 (L)		高 (H)
	情報が改ざんされる可能性 完全性への影響 (I:Integrity Impact)	なし (N)	低 (L)		高 (H)
	業務が遅延・停止する可能性 可用性への影響 (A:Availability Impact)	なし (N)	低 (L)		高 (H)

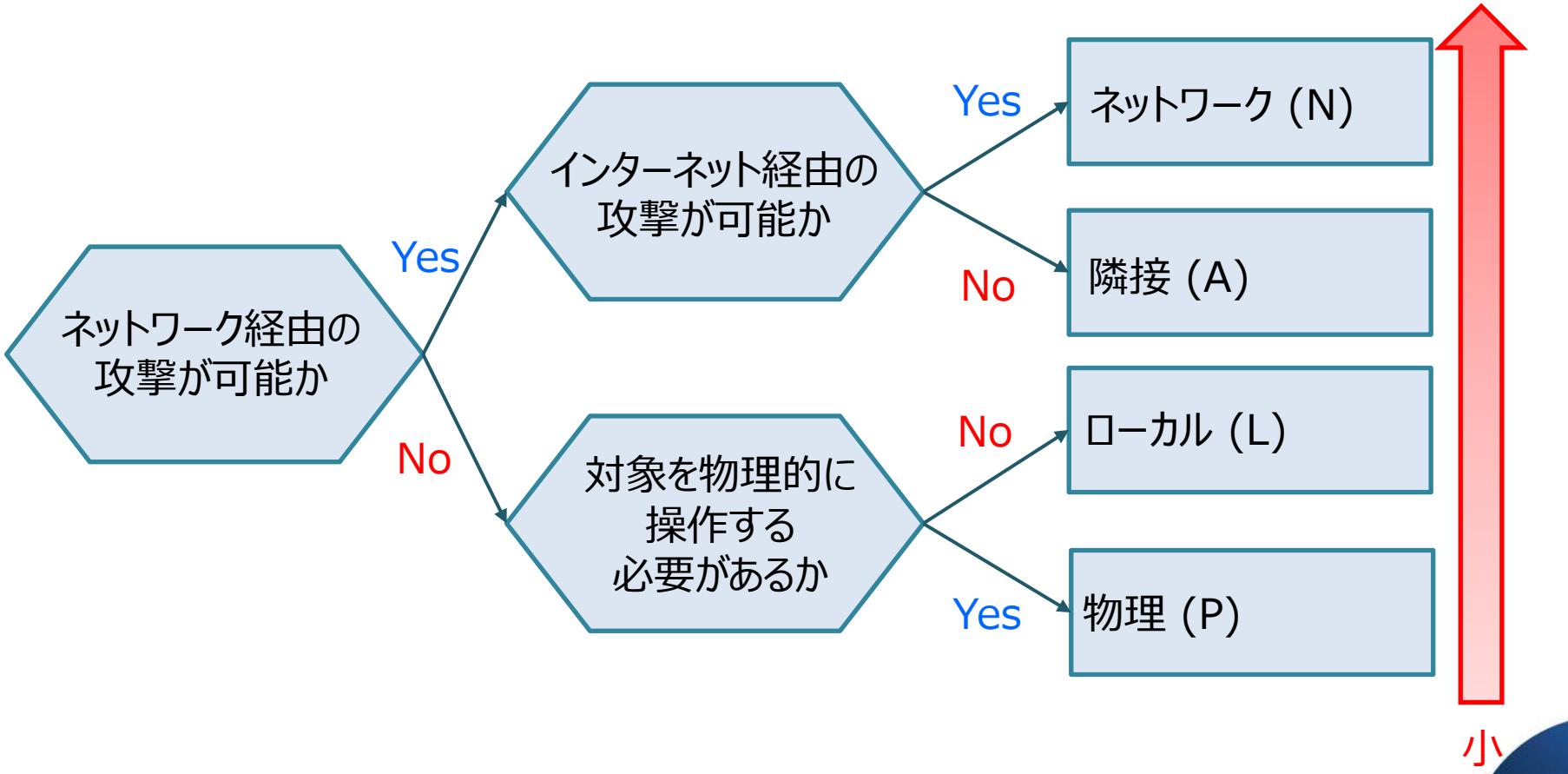
✓ ベンダやセキュリティ関連企業が評価をしている

✓ 時間や環境が変化しても評価結果は変わらない

攻撃元区分（Attack Vector）

■どこから攻撃可能であるか

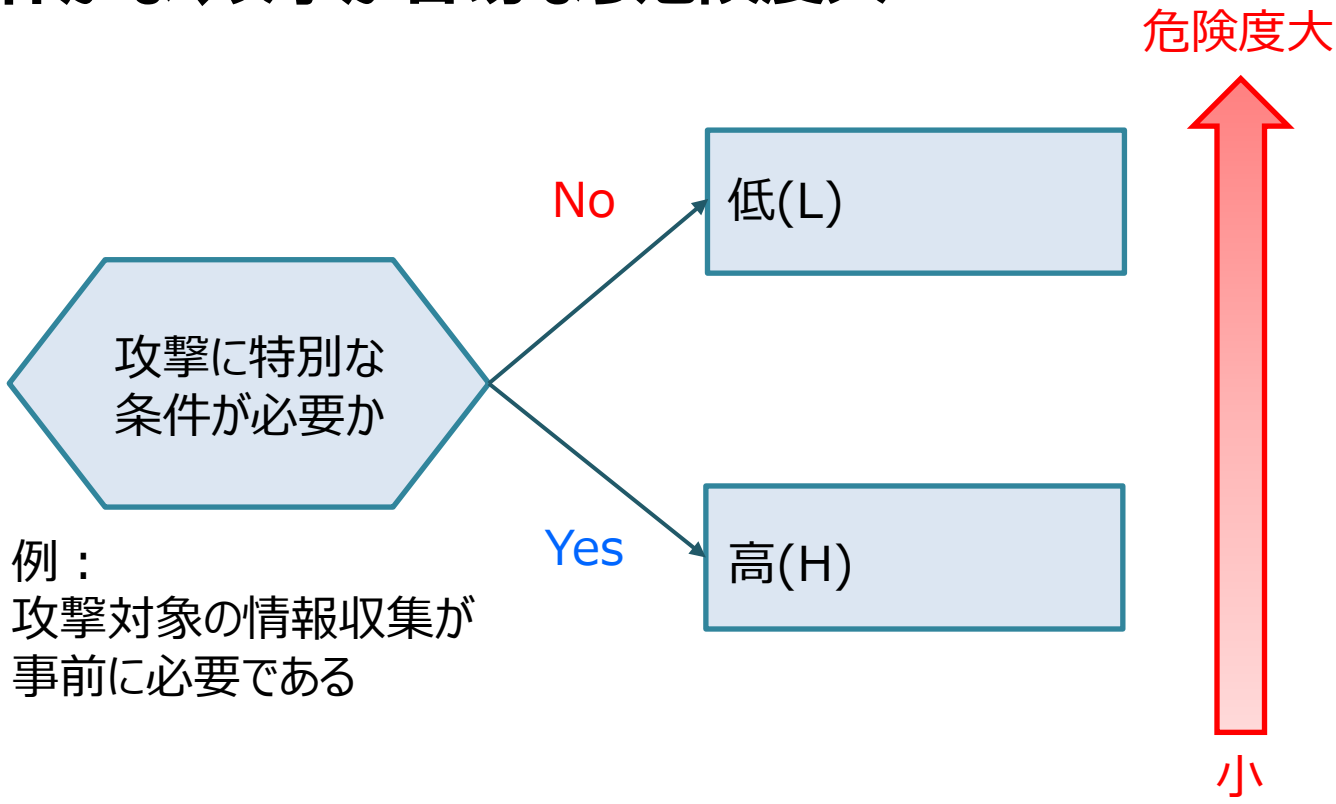
より遠いところから攻撃されるほど危険度大



攻撃条件の複雑さ（Attack Complexity）

■攻撃する際に必要な条件の複雑さ

攻撃条件がなく攻撃が容易なら危険度大

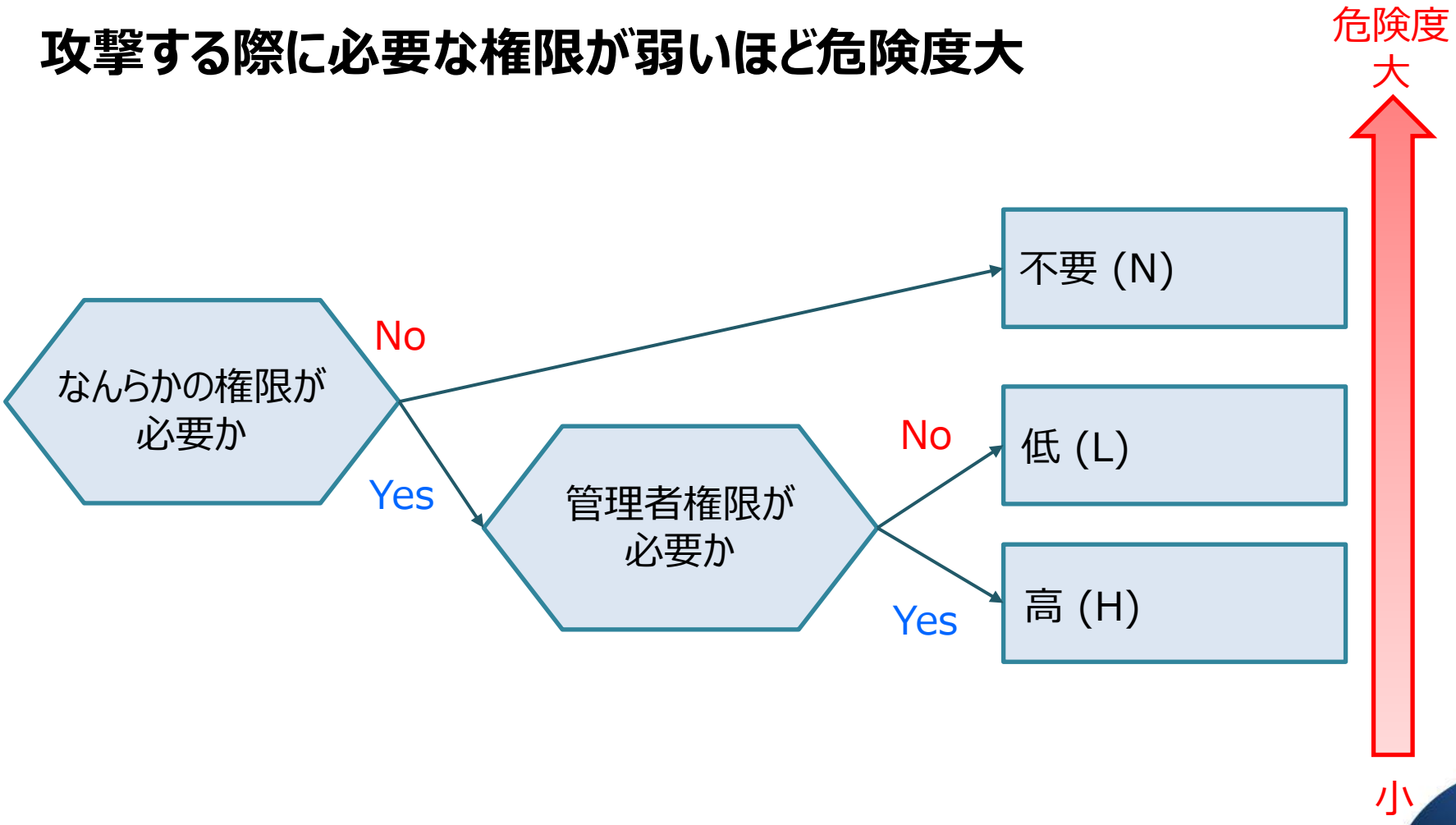


例：
攻撃対象の情報収集が
事前に必要である

必要な特権レベル(Privileges Required)

■ 攻撃する際に必要な特権のレベル

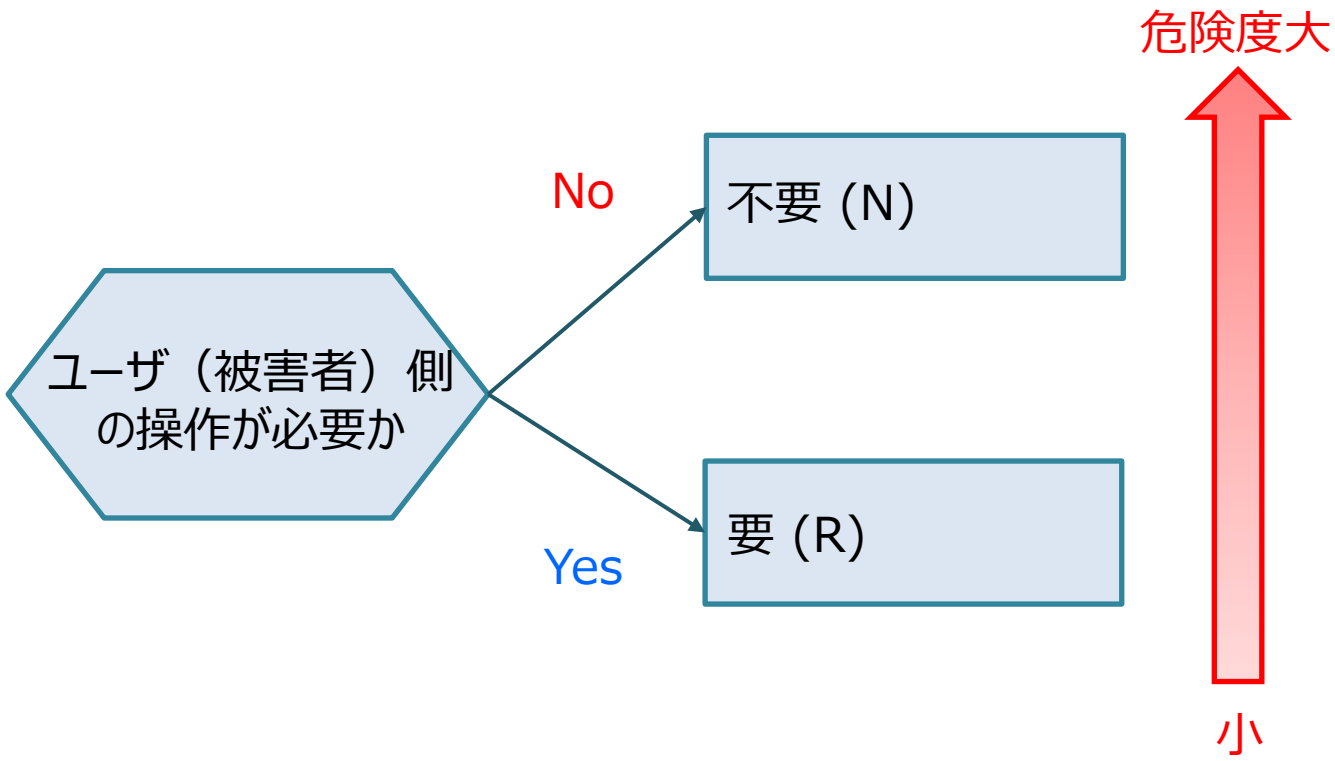
攻撃する際に必要な権限が弱いほど危険度大



ユーザ関与レベル(User Interaction)

■ 攻撃する際に必要なユーザ関与レベル

ユーザ側の操作が不要で攻撃が容易であれば危険度大



CVSSv3 基本評価
～脆弱性そのものの特性を評価～

危険小 ⟷ 危険大

	評価項目	選択肢・ポイント			
攻撃の難易度	どこから攻撃可能であるか 攻撃元区分 (AV:Attack Vector)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
	攻撃する際に必要な条件の複雑さ 攻撃条件の複雑さ (AC:Attack Complexity)	高 (H)		低 (L)	
	攻撃する際に必要な特権のレベル 必要な特権レベル (PR:Privileges Required)	高 (H)	低 (L)		不要 (N)
	攻撃する際に必要なユーザ関与レベル ユーザ関与レベル (UI:User Interaction)	要 (R)		不要 (N)	
攻撃による影響	攻撃による影響の想定範囲 スコープ (S:Scope)	変更なし (U)		変更あり (C)	
	機密情報が漏えいする可能性 機密性への影響 (C:Confidentiality Impact)	なし (N)	低 (L)		高 (H)
	情報が改ざんされる可能性 完全性への影響 (I:Integrity Impact)	なし (N)	低 (L)		高 (H)
	業務が遅延・停止する可能性 可用性への影響 (A:Availability Impact)	なし (N)	低 (L)		高 (H)

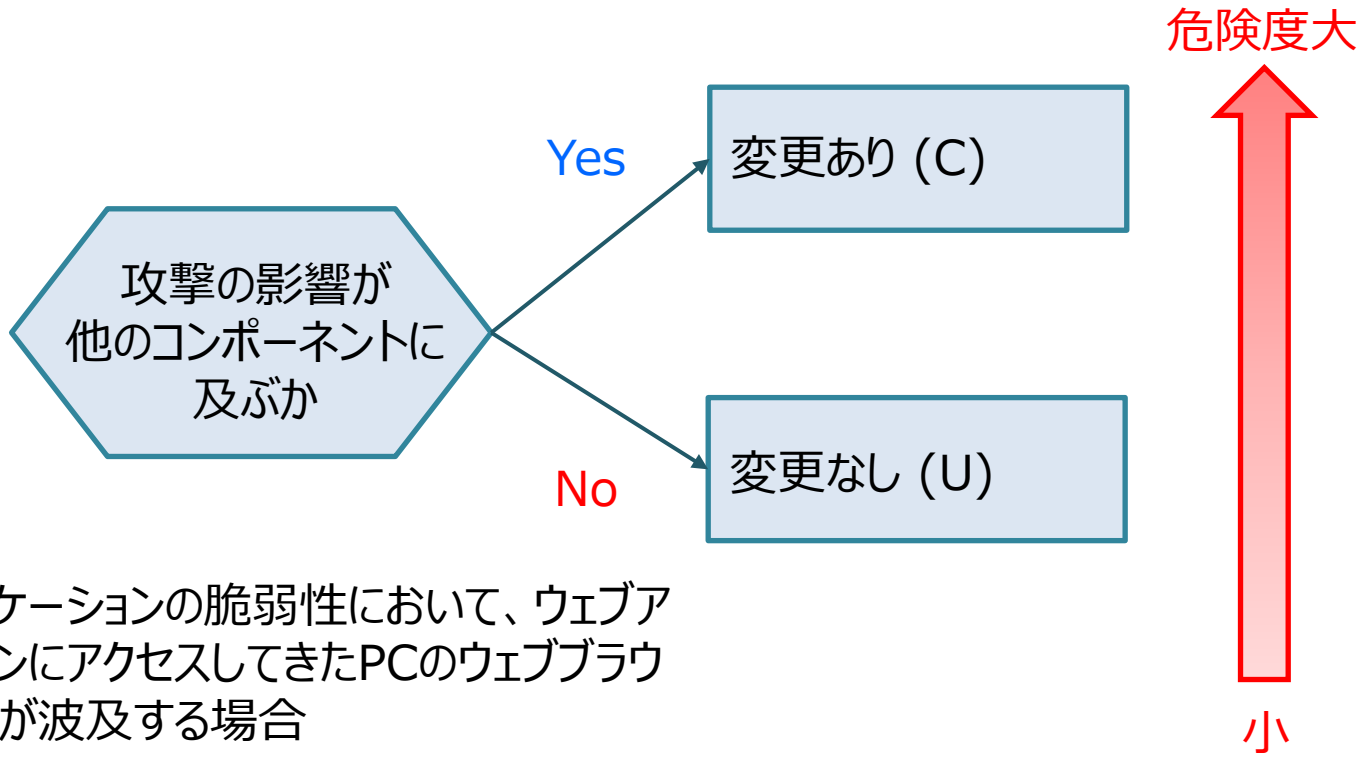
✓ ベンダやセキュリティ関連企業が評価をしている

✓ 時間や環境が変化しても評価結果は変わらない

スコープ(Scope)

■ 攻撃による影響の想定範囲

影響の範囲が脆弱性の影響想定範囲を超えて広がれば危険度大

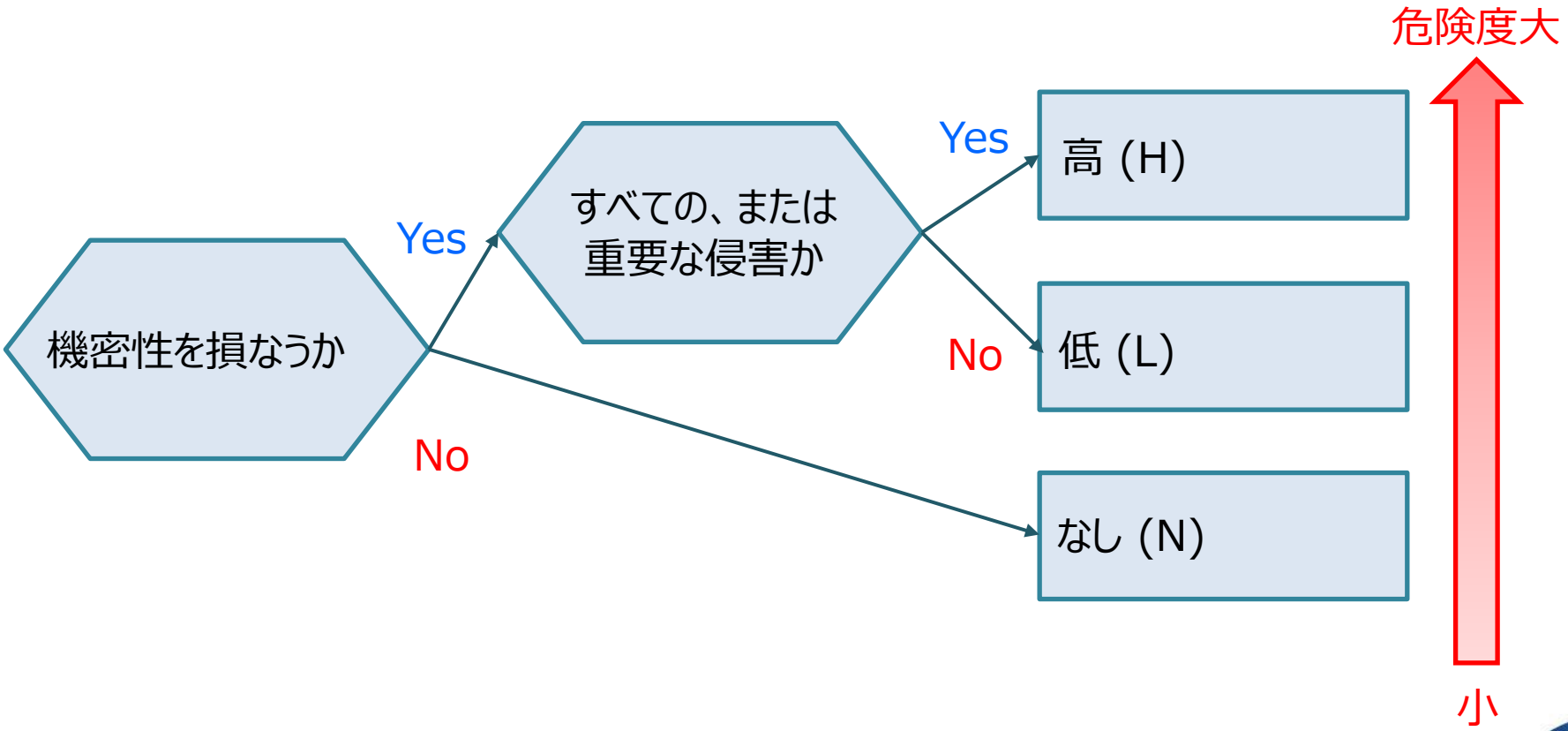


例：
ウェブアプリケーションの脆弱性において、ウェブアプリケーションにアクセスしてきたPCのウェブブラウザにも影響が波及する場合

機密性への影響(Confidentiality Impact)

■機密情報が漏えいする可能性

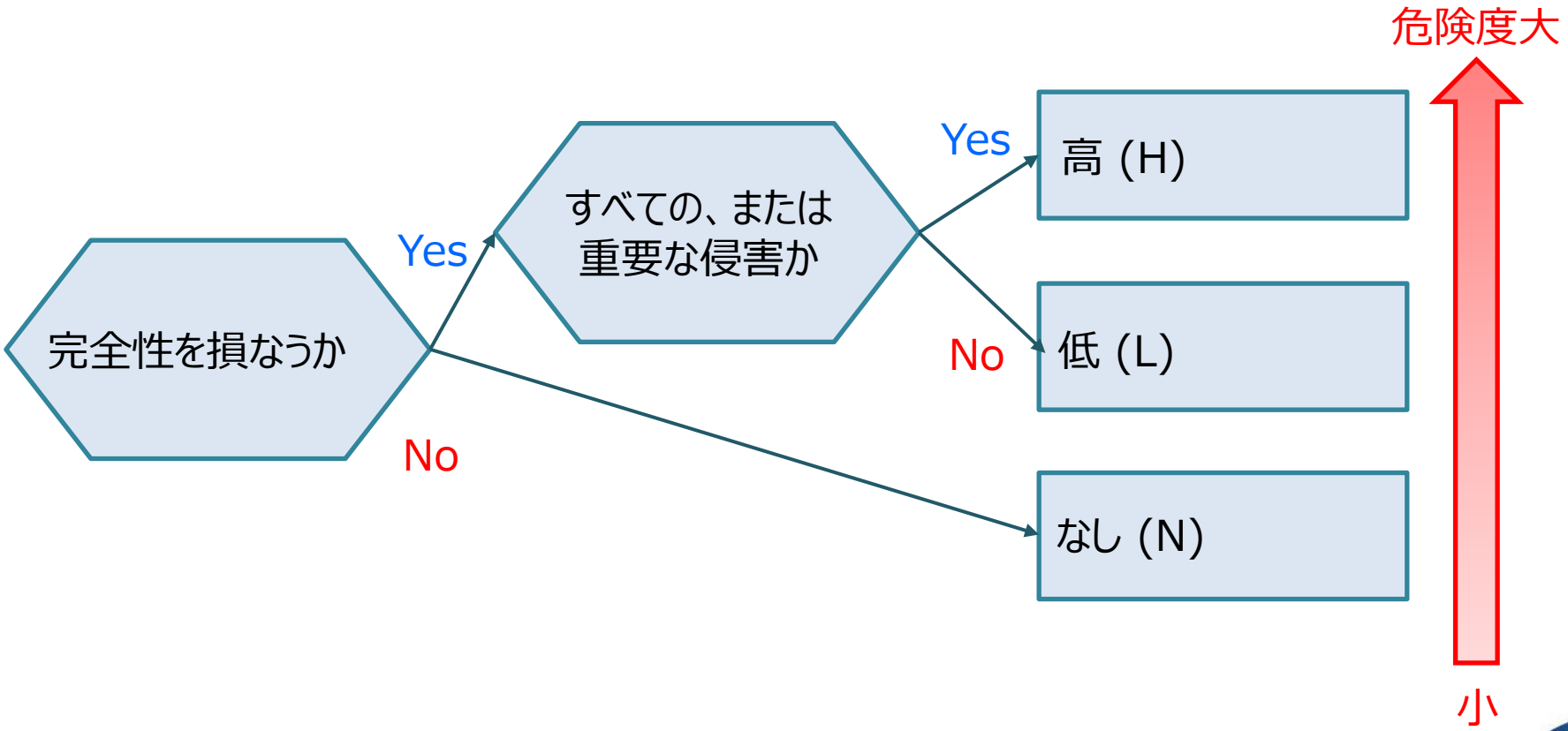
すべての情報または重要な情報が漏えいされると危険度大



完全性への影響(Integrity Impact)

■情報が改ざんされる可能性

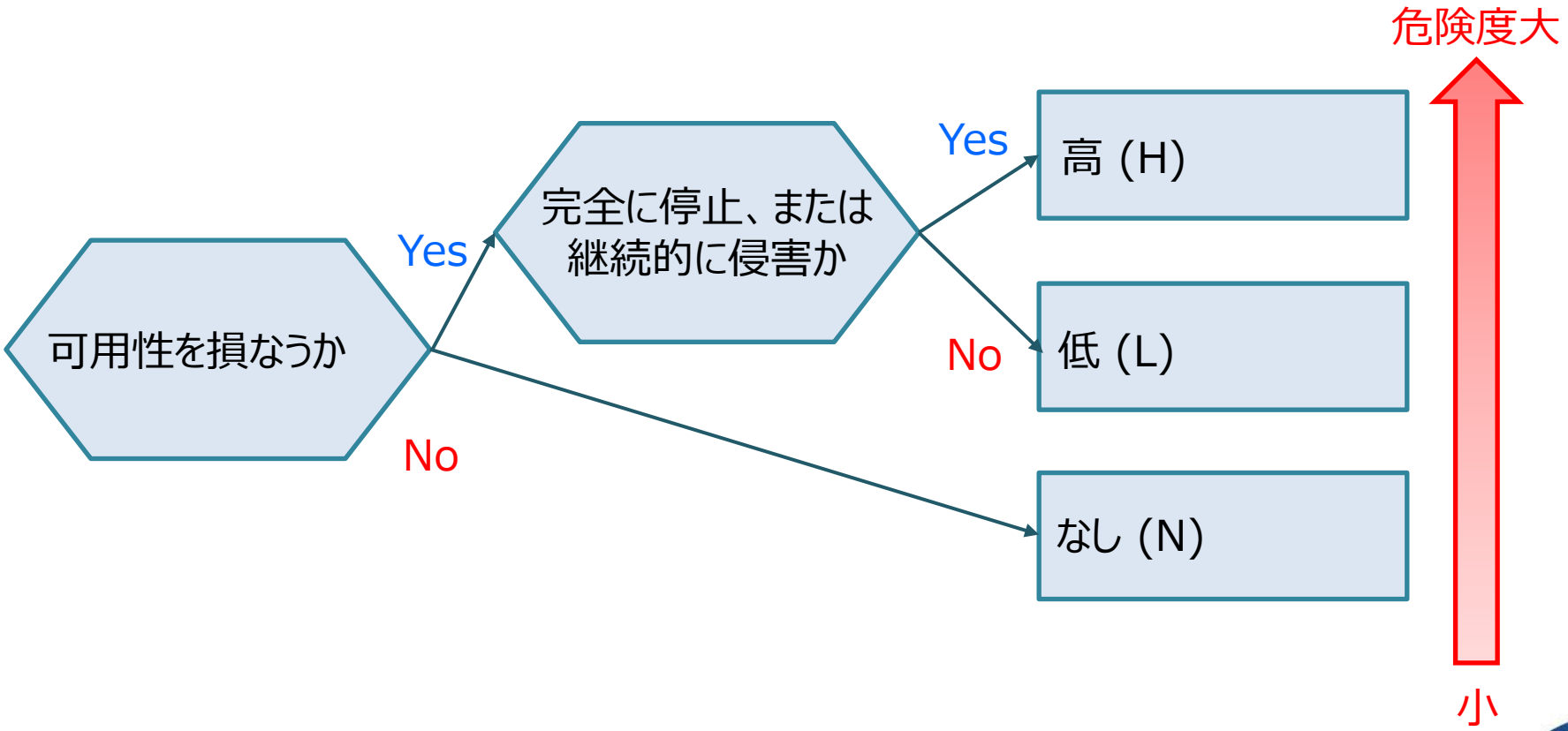
すべての情報または重要な情報が改ざんされると危険度大



可用性への影響(Availability Impact)

■ 業務が遅延・停止する可能性

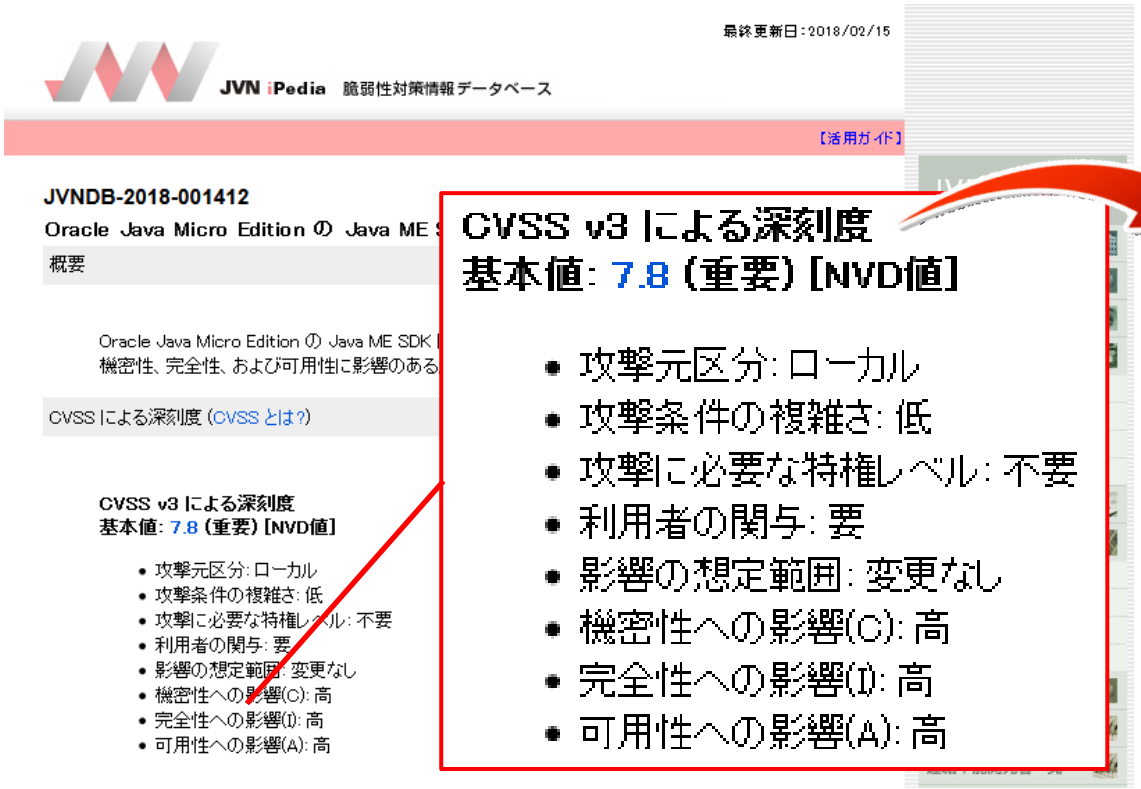
対象が完全に停止するまたは継続的に影響があると危険度大



CVSSv3 基本評価
～脆弱性そのものの特性を評価～

IPA

■JVN iPediaでもCVSSv3基本値を公開中



CVSS v3 による深刻度
基本値: 7.8 (重要) [NVD値]

- 攻撃元区分: ローカル
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 不要
- 利用者の関与: 要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 高
- 完全性への影響(I): 高
- 可用性への影響(A): 高

深刻度	基本値
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0.0

https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-001412.html

✓ CVSSパラメータの選択肢が日本語で確認可能

CVSSv3 基本評価
～脆弱性そのものの特性を評価～

CVSS v3 による深刻度
基本値: 7.8 (重要) [NVD値]

- 攻撃元区分: ローカル
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 不要
- 利用者の関与: 要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 高
- 完全性への影響(I): 高
- 可用性への影響(A): 高

■ 例：脆弱性固有の特性を見てみる

	評価項目	選択肢・ホ			
攻撃の難易度	どこから攻撃可能であるか 攻撃元区分 (AV:Attack Vector)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
	攻撃する際に必要な条件の複雑さ 攻撃条件の複雑さ (AC:Attack Complexity)	高 (H)		低 (L)	
	攻撃する際に必要な特権のレベル 必要な特権レベル (PR:Privileges Required)	高 (H)	低 (L)		不要 (N)
	攻撃する際に必要なユーザ関与レベル ユーザ関与レベル (UI:User Interaction)	要 (R)		不要 (N)	
攻撃による影響	攻撃による影響の想定範囲 スコープ (S:Scope)	変更なし (U)		変更あり (C)	
	機密情報が漏えいする可能性 機密性への影響 (C:Confidentiality Impact)	なし (N)	低 (L)		高 (H)
	情報が改ざんされる可能性 完全性への影響 (I:Integrity Impact)	なし (N)	低 (L)		高 (H)
	業務が遅延・停止する可能性 可用性への影響 (A:Availability Impact)	なし (N)	低 (L)		高 (H)

CVSSとは
～評価基準一覧～

- **評価方法は公開されており、だれでもＣＶＳＳスコアを採点することができます**

基本評価基準 (0.0 ～ 10.0)	脆弱性の技術的な特性を評価 例：ネットワークから攻撃可能なら危険大 例：攻撃方法が難しければ危険小
現状評価基準 (0.0 ～ 10.0)	ある時点における脆弱性を取り巻く状況を評価 例：ゼロデイ攻撃があれば危険大 例：攻撃コードが利用不可であれば危険小
環境評価基準 (0.0 ～ 10.0)	そのシステムにおける問題の大きさを評価 例：社内の基幹システムで影響大なら危険大 例：被害予想が少なければ危険小

※現状評価基準および環境評価基準は、基本評価基準を元に算出されます
※現状評価を最大と仮定して環境評価を行うことも可能です

CVSSv3 現状評価基準
～脆弱性の現在の深刻度を評価～

IPA

■現状評価基準とは？

- ✓ 実際に攻撃が行われている
- ✓ 攻撃コードが一般に公開（攻撃の予兆）

CVSSv3 現状評価
～脆弱性の現在の深刻度を評価～

危険小 → 危険大

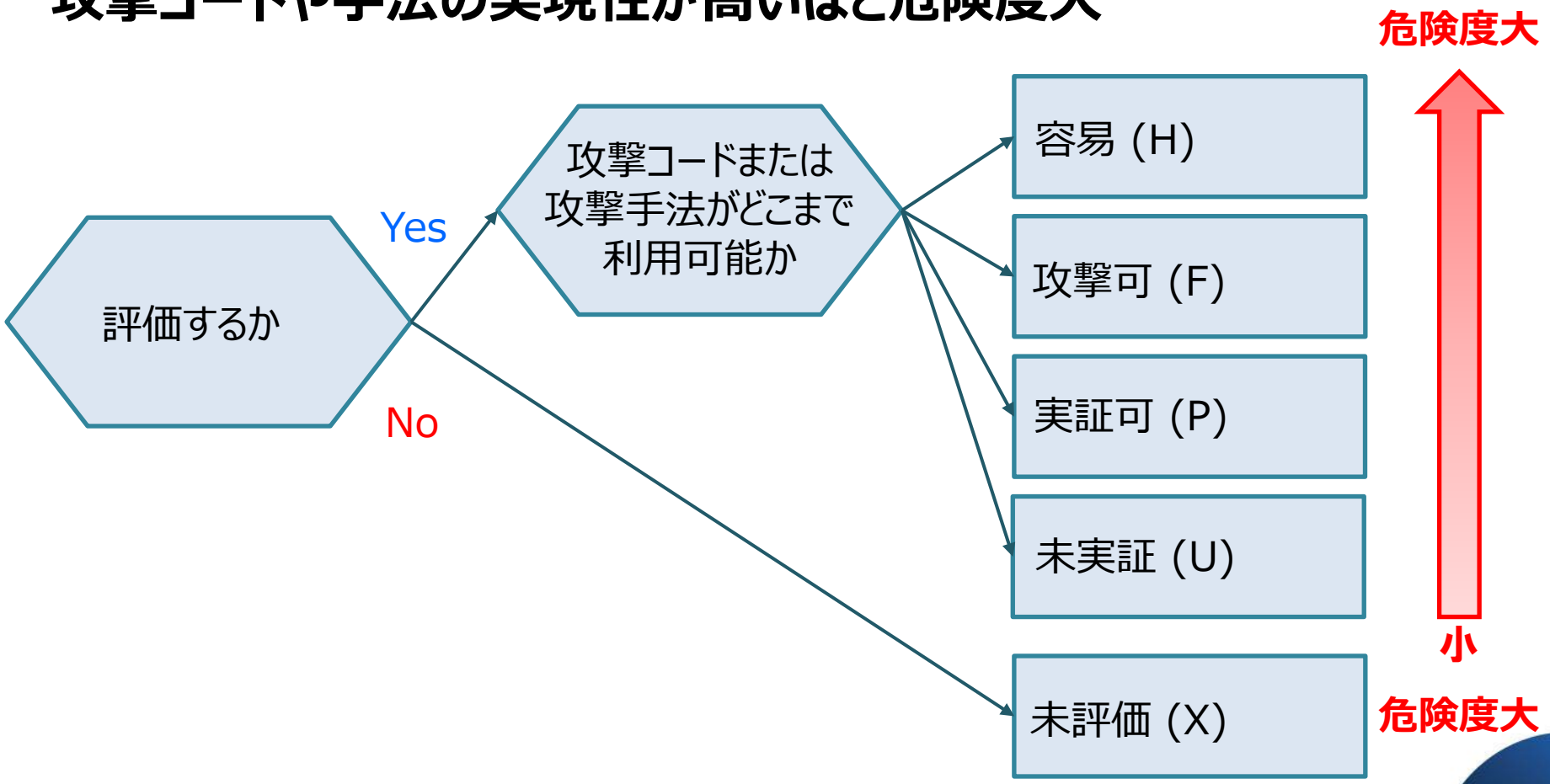
評価項目	選択肢・ポイント				
攻撃コード・攻撃手法が実際に利用可能であるか 攻撃される可能性 （E:Exploit Code Maturity）	未評価 (X)	未実証 (U)	実証可 (P)	攻撃可 (F)	容易 (H)
対策がどの程度利用可能であるか 利用可能な対策のレベル （RL:Remediation Level）	未評価 (X)	正式 (O)	暫定 (T)	非公式 (W)	なし (U)
情報の信頼性はどの程度か 脆弱性情報の信頼性 （RC:Report Confidence）	未評価 (X)	_	未確認 (U)	未確証 (R)	確認済 (C)

- ✓ 時間の変化に応じて評価も変化する
- ✓ 未評価を選択すると最も危険度が高い選択をした場合（容易、なし、確認済）と同じ扱いになります

攻撃される可能性（Exploit Code Maturity）

■攻撃コード・攻撃手法が実際に利用可能であるか

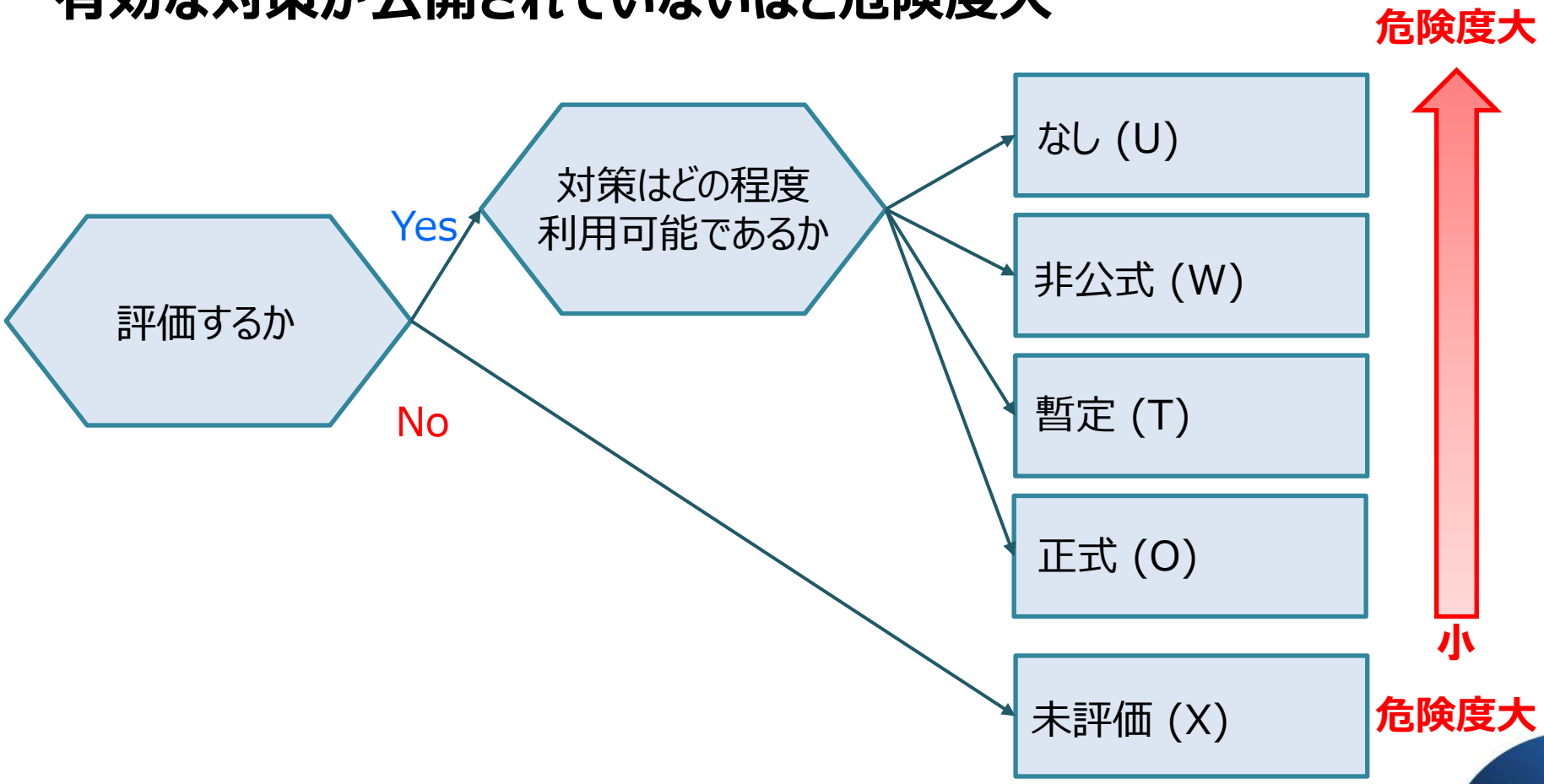
攻撃コードや手法の実現性が高いほど危険度大



利用可能な対策レベル（Remediation Level）

■ 対策がどの程度利用可能であるか

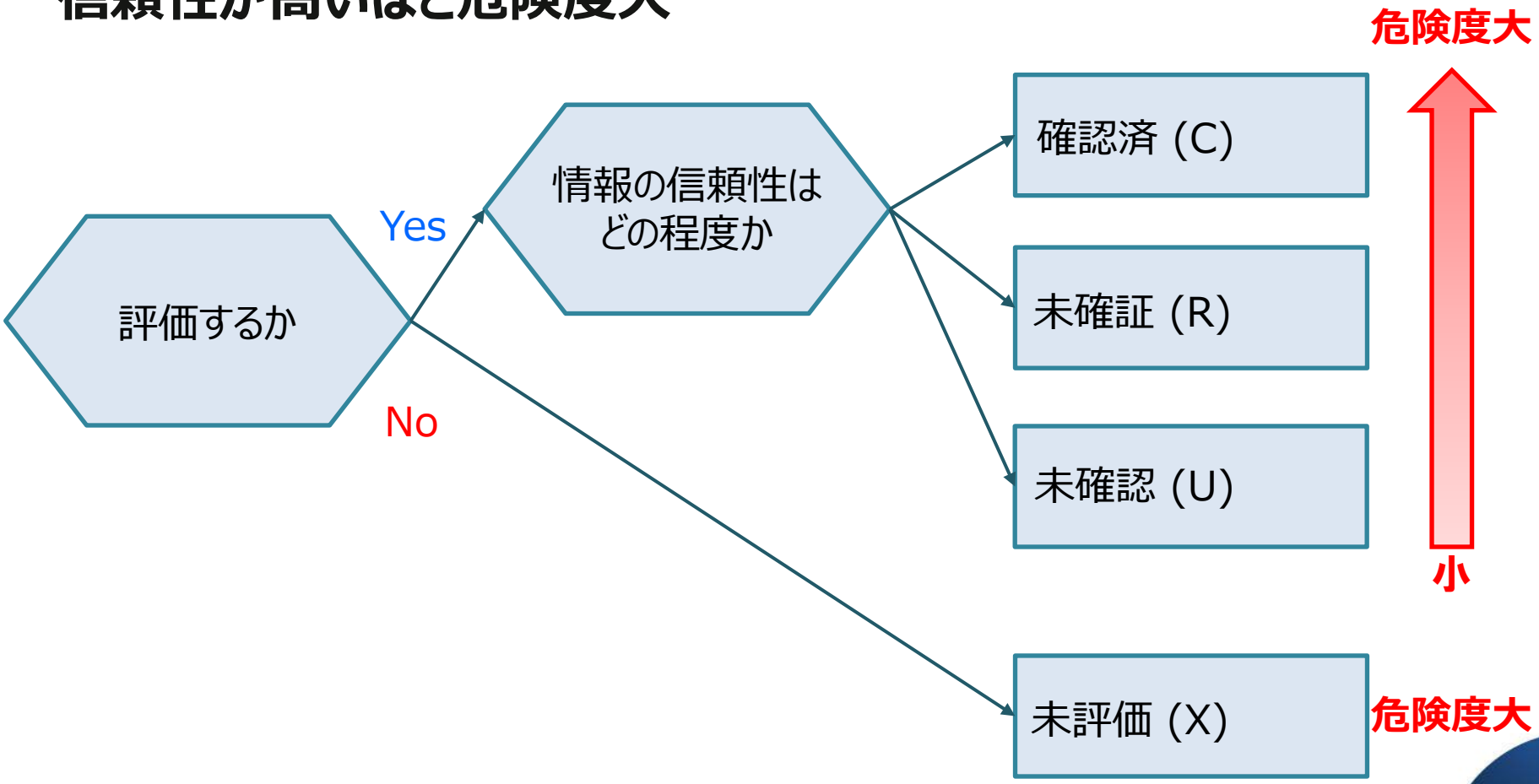
有効な対策が公開されていないほど危険度大



脆弱性情報の信頼性（Report Confidence）

■情報の信頼性はどの程度か

信頼性が高いほど危険度大



Step3 自組織への影響を分析する
～自組織への影響を分析するにはどうすれば良いのか？～

Ｓｔｅｐ１

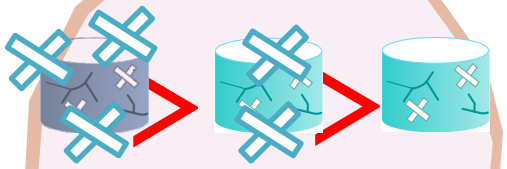
情報の絞込み

全ての情報 → 必要

自組織に関連する情報を抽出

Ｓｔｅｐ２

脆弱性の深刻度を確認



脆弱性の特性や攻撃状況を確認

Ｓｔｅｐ３

自組織への影響を分析

自組織の環境を考慮した対策を実施

CVSSとは
～評価基準一覧～

- **評価方法は公開されており、だれでもＣＶＳＳスコアを採点することができます**

基本評価基準
(0.0 ～ 10.0)

脆弱性の技術的な特性を評価
例：ネットワークから攻撃可能なら危険大
例：攻撃方法が難しければ危険小

現状評価基準
(0.0 ～ 10.0)

ある時点における脆弱性を取り巻く状況を評価
例：ゼロデイ攻撃があれば危険大
例：攻撃コードが利用不可であれば危険小

Ｓｔｅｐ３

環境評価基準
(0.0 ～ 10.0)

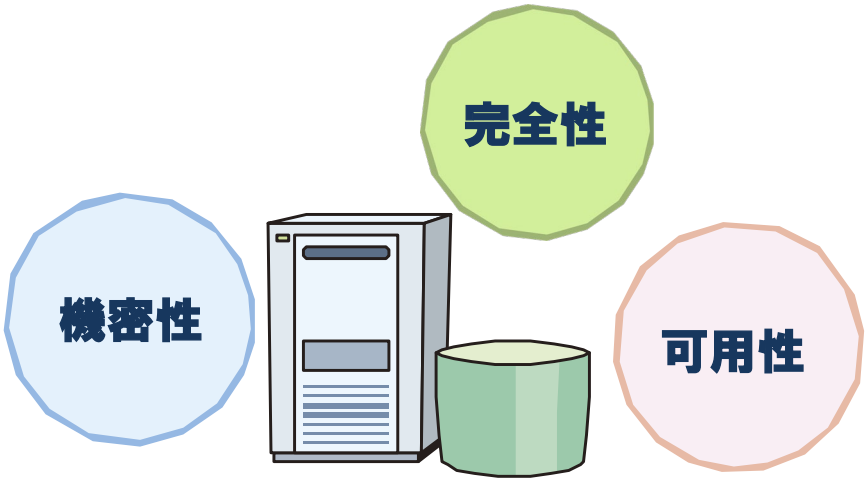
そのシステムにおける問題の大きさを評価
例：社内の基幹システムで影響大なら危険大
例：被害予想が少なければ危険小

※現状評価基準および環境評価基準は、基本評価基準を元に算出されます
※現状評価を最大と仮定して環境評価を行うことも可能です

CVSSv3 環境評価基準
～ユーザの利用環境も含め、最終的な脆弱性の深刻度を評価～

■環境評価基準とは？

- ✓ 対象システムのセキュリティ要求度を評価（機密性、完全性、可用性を評価）
- ✓ 環境条件を加味した基本評価の再評価



CVSSv3 環境評価

～ユーザの利用環境も含め、最終的な脆弱性の深刻度を評価～

危険小 ⟷ 危険大

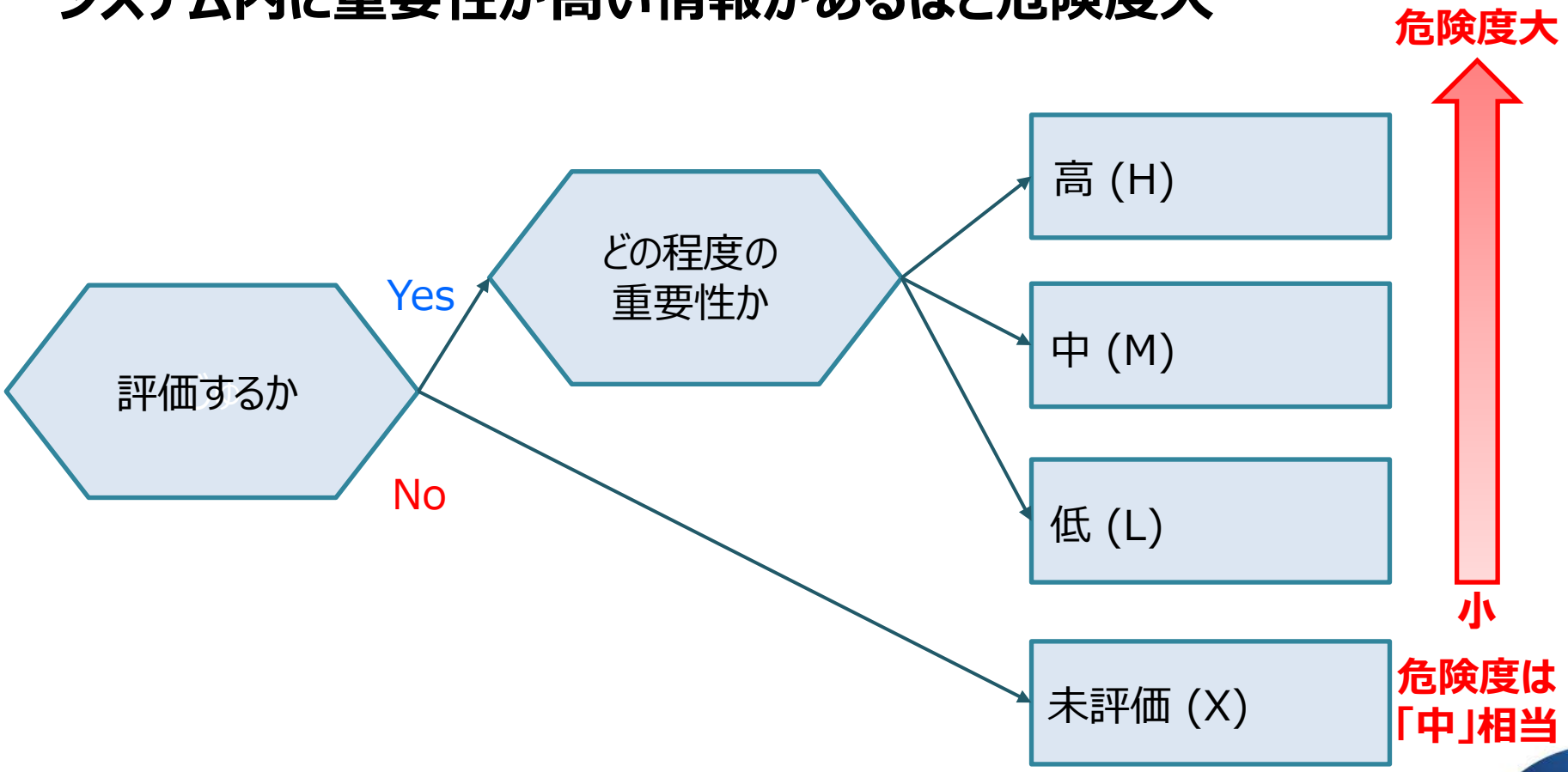
	評価項目	選択肢			
要求度	システムにおける**機密性**の重要度 (CR:Confidentiality Requirement)	未評価 (X)	低 (L)	中 (M)	高 (H)
	システムにおける**完全性**の重要度 (IR:Integrity Requirement)	未評価 (X)	低 (L)	中 (M)	高 (H)
	システムにおける**可用性**の重要度 (AR:Availability Requirement)	未評価 (X)	低 (L)	中 (M)	高 (H)

- ✓ 対象システムのセキュリティ重要度を自組織で評価
- ✓ 未評価を選択した場合「中」と同じ扱いになります

機密性の要求度(Confidentiality Requirement)

■システムにおける機密性の重要度

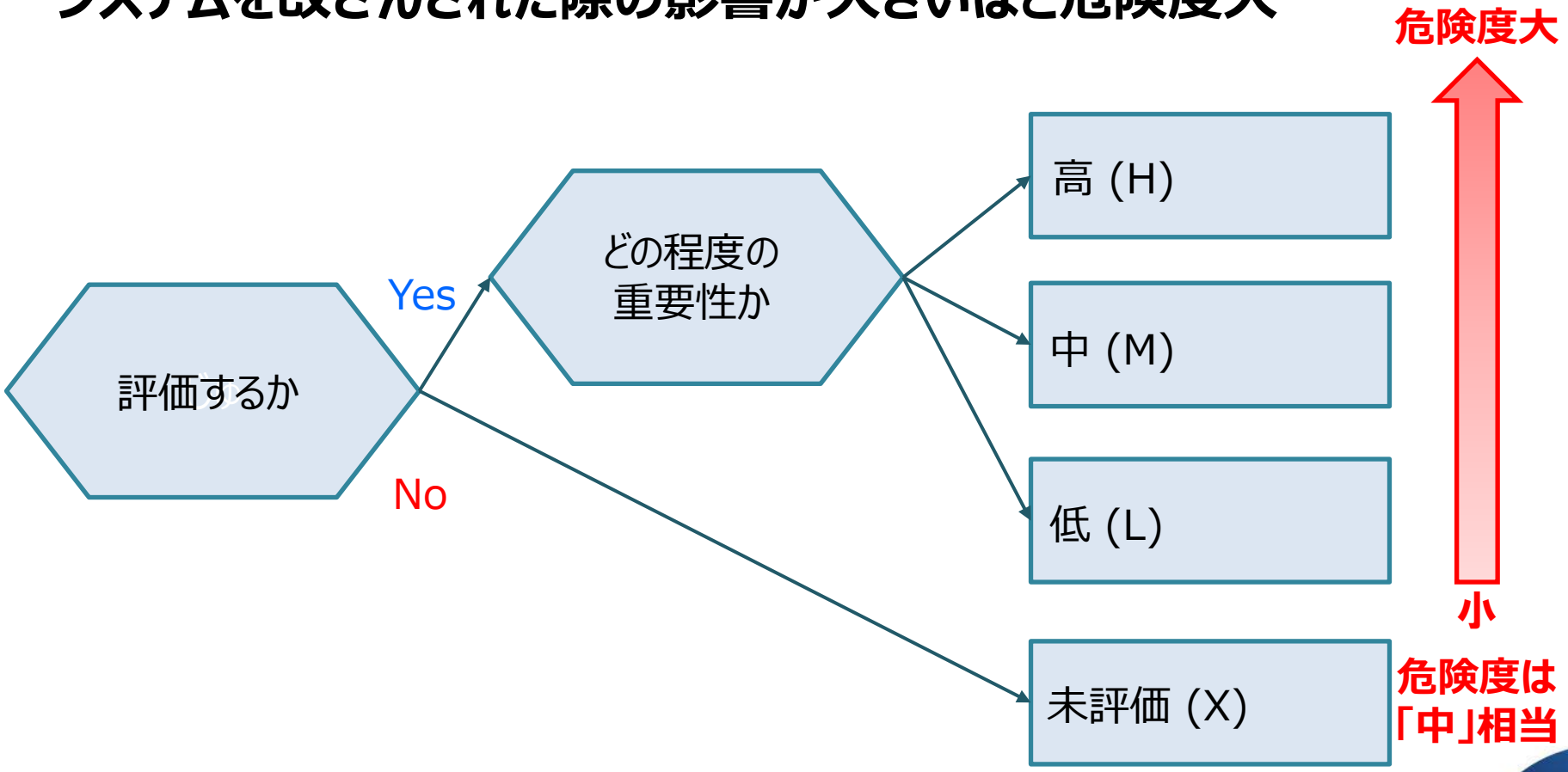
システム内に重要性が高い情報があるほど危険度大



完全性の要求度(Integrity Requirement)

■システムにおける完全性の重要度

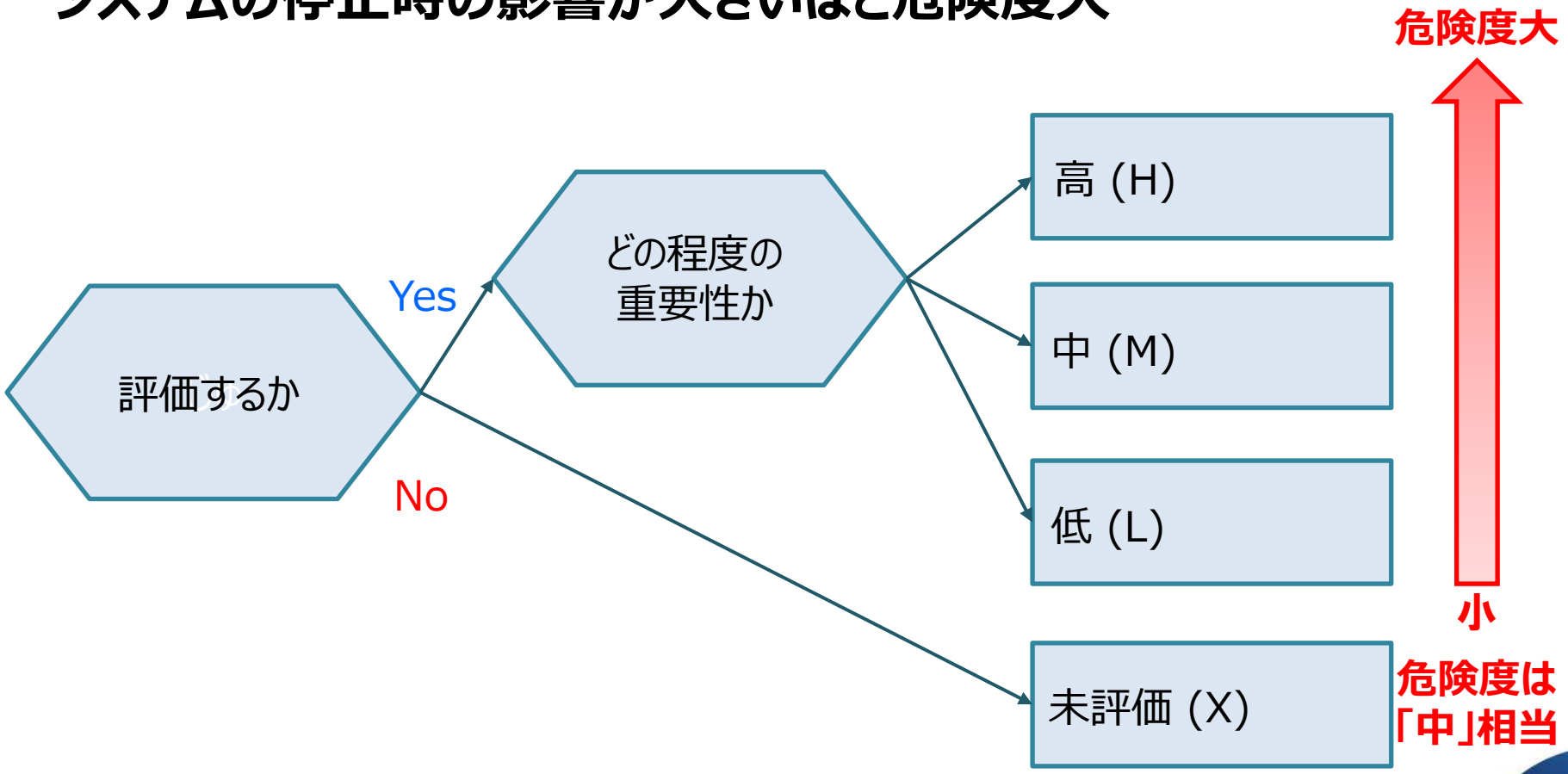
システムを改ざんされた際の影響が大きいほど危険度大



可用性の要求度(Availability Requirement)

■システムにおける可用性の重要度

システムの停止時の影響が大きいほど危険度大



再評価例

- 基本評価基準の攻撃区分は「ネットワーク」だが脆弱性が存在するシステムはインターネット環境からアクセスできない箇所（「隣接」相当）に設置されている。
- 基本評価基準の必要な特権レベルは「高」だが当該システムはデフォルトの認証機能を無効化（「なし」相当）している。
- それ以外は変更なし。

CVSSv3 環境評価

～ユーザの利用環境も含め、最終的な脆弱性の深刻度を評価～

IPA

✓環境条件を加味した基本評価の再評価

危険小 ⇔ 危険大

	評価項目	選択肢・ポイント				
環境条件を加味した再評価	どこから攻撃可能であるかの再評価 緩和策後の攻撃元区分 (MAV:Modified Attack Vector)	未評価 (X)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
	必要な条件の複雑さの再評価 緩和策後の攻撃条件の複雑さ (MAC:Modified Attack Complexity)	未評価 (X)	高 (H)		低 (L)	
	必要な特権のレベルの再評価 緩和策後の必要な特権レベル (MPR:Modified Privileges Required)	未評価 (X)	高 (H)	低 (L)		不要 (N)
	必要なユーザ関与レベルの再評価 緩和策後のユーザ関与レベル (MUI:Modified User Interaction)	未評価 (X)	要 (R)		不要 (N)	
	攻撃による影響範囲の再評価 緩和策後のスコープ (MS:Modified Scope)	未評価 (X)	変更なし (U)		変更あり (C)	
	機密情報が漏えいする可能性の再評価 緩和策後の機密性への影響 (MC:Modified Confidentiality Impact)	未評価 (X)	なし (N)	低 (L)		高 (H)
	情報が改ざんされる可能性の再評価 緩和策後の完全性への影響 (MI:Modified Integrity Impact)	未評価 (X)	なし (N)	低 (L)		高 (H)
	業務が遅延・停止する可能性の再評価 緩和策後の可用性への影響 (MA:Modified Availability Impact)	未評価 (X)	なし (N)	低 (L)		高 (H)

※未評価の場合、基本評価基準と同じ扱いになります

CVSSスコアの算出方法について
～評価をするためにはCVSSスコアの算出が必要～

IPA

CVSSv3 スコアの算出方法について

(1)影響度

調整前影響度 = 1 - (1 - C)×(1 - I)×(1 - A)　…式(1)

影響度(スコープ変更なし)= 6.42×調整前影響度　…式(2)

影響度(スコープ変更あり)= 7.52×(調整前影響度 - 0.029) - 3.25×(調整前影響度 - 0.02)^{15}　…式(3)

(2)攻撃容易性

攻撃容易性 = 8.22×AV×AC×PR×UI　…式(4)

(3)基本値

影響度がゼロ以下の場合

基本値 = 0　…式(5)

影響度がゼロよりも大きい場合

スコープ変更なし

基本値 = RoundUp1(min [(影響度＋攻撃容易性), 10])　…式(6)

(小数点第1位切り上げ)

スコープ変更あり

基本値 = RoundUp1(min [(1.08×(影響度＋攻撃容易性)), 10])　…式(7)

(小数点第1位切り上げ)

https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

CVSSスコアの算出方法について
～CVSS計算ツールを使ってみる～

IPA

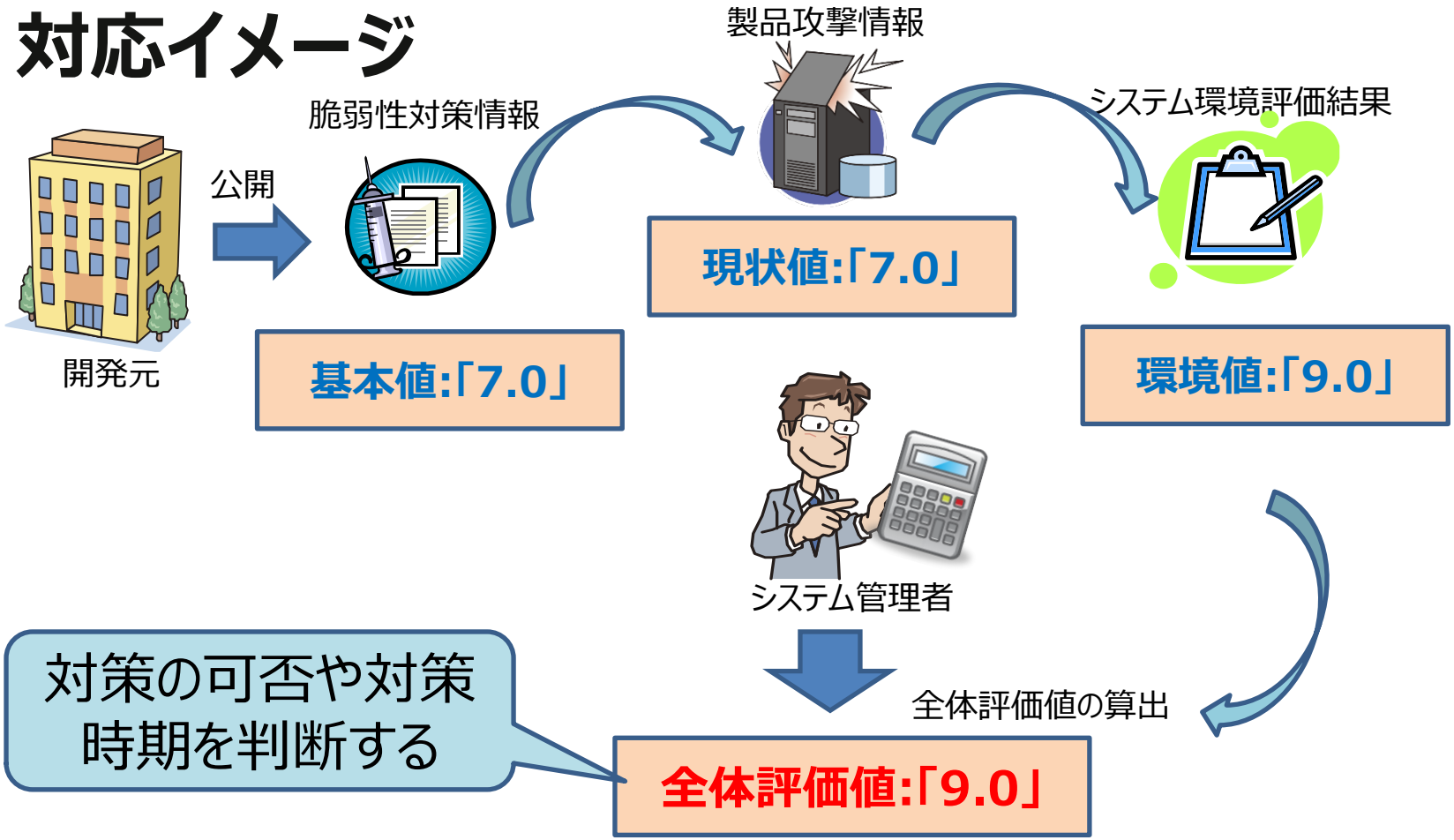
■ 評価結果からスコアの自動計算が可能

https://jvndb.jvn.jp/cvss/ja/v31.html

CVSS全体評価の実施フロー
～脆弱性情報を基に自システムの環境に当てはめて評価～

IPA

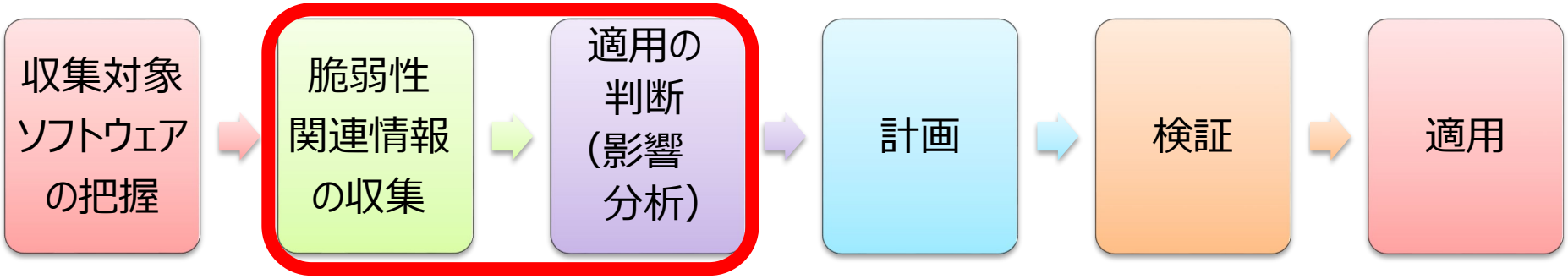
■ 対応イメージ



✓ 公開された脆弱性の基本値と、評価した現状値と環境値（未評価も可）により、全体評価値を求める

脆弱性対策の進め方のフロー

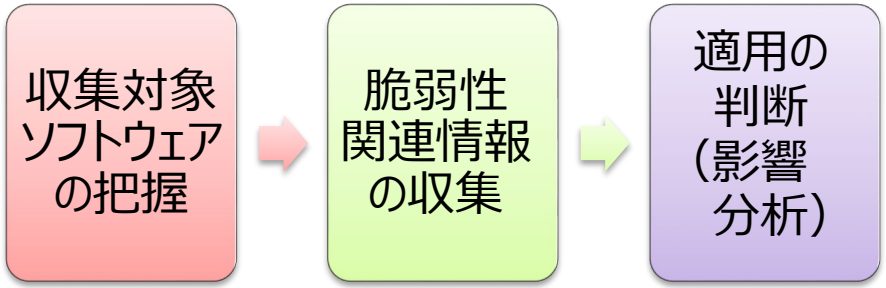
■ 本セミナーで説明する内容



ステップ	概要
【ステップ１】 収集対象ソフトウェアの把握	管理すべきソフトウェアに関する情報を把握 ソフトウェア名・バージョン・パッチ提供元　等
【ステップ２】 脆弱性関連情報の収集	管理すべきソフトウェアに関連する脆弱性情報を収集
【ステップ３】 適用の判断（影響分析）	適用すべき緊急度や優先度を分析

脆弱性対策の進め方のフロー

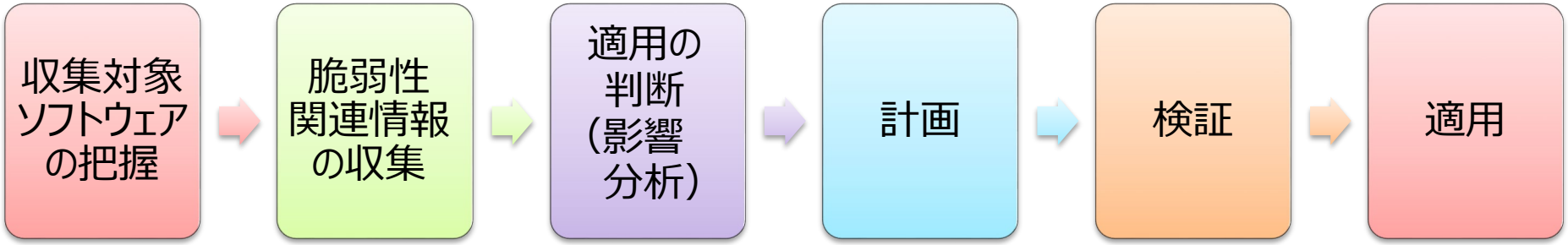
■ 脆弱性対策は6つのステップで実施



ステップ	概要
【ステップ１】 収集対象ソフトウェアの把握	管理すべきソフトウェアに関する情報を把握 ソフトウェア名・バージョン・パッチ提供元　等
【ステップ２】 脆弱性関連情報の収集	管理すべきソフトウェアに関連する脆弱性情報を収集
【ステップ３】 適用の判断（影響分析）	適用すべき脆弱性対策の緊急度や優先度を分析

脆弱性対策の進め方のフロー

■ 脆弱性対策は6つのステップで実施



ステップ	概要
【ステップ４】 計画	影響分析結果に基づき脆弱性対策実施までのスケジュールや方針を計画
【ステップ５】 検証	脆弱性対策を実施することでソフトウェアに影響を与えないかを検証
【ステップ６】 適用	脆弱性対策の適用

まとめ（第３章）

- **CVSSとは何か**

  →脆弱性の深刻度を表す評価手法

- **CVSSv3が脆弱性をどのように評価しているか**

  →下記、3つの基準で評価を行っている

  - 基本評価基準
  - 現状評価基準
  - 環境評価基準

- **CVSSv3をどのように使えばよいか**

  →CVSSv3 計算ツールを活用することで
  評価値を容易に算出可能