本資料は、JPCERT/CCが主催したセミナーにてワークショップ形式で利用したものを、自習形式でも使っていただけるように編集し直したものです。
ワークショップ等の表現はそのまま利用しております。

CVSS勉強会

JPCERTコーディネーションセンター
早期警戒グループ

CVSS とは？

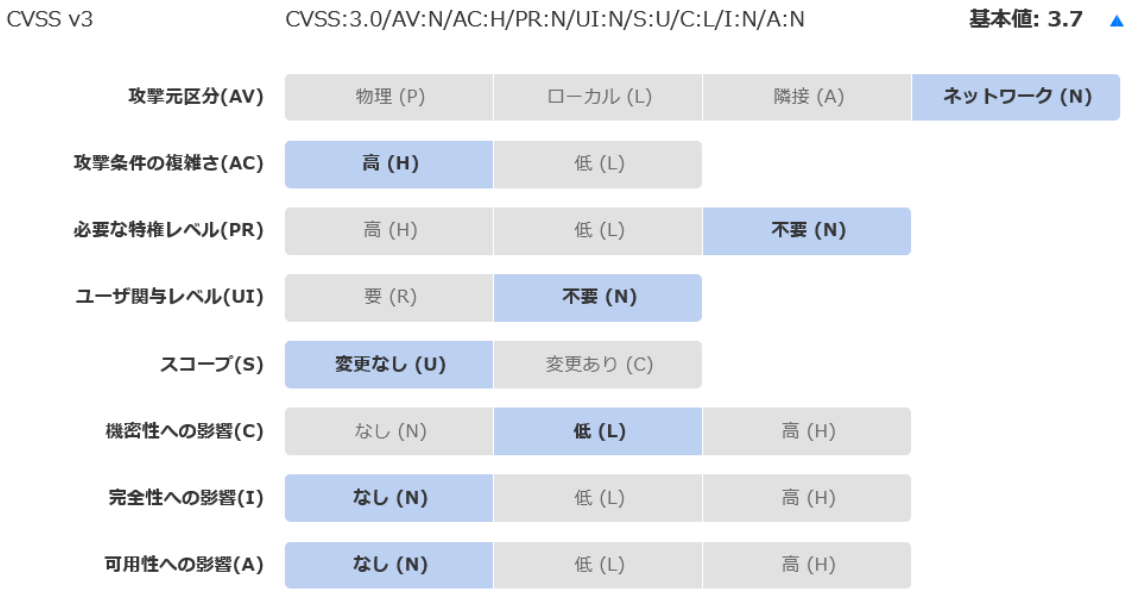
Common **V**ulnerability **S**coring **S**ystem
(共通脆弱性評価システム)

- 情報システムの脆弱性に対する
  オープンで汎用的な評価手法

- どのような攻撃が可能で、どのような
  影響を及ぼすものであるかを
  評価・確認できる

- CVSS は、評価するベンダや国に
  依らず共通

- 基本、現状、環境の評価基準がある



JVN iPedia でも、JVN でも基本評価基準を掲載

http://jvndb.jvn.jp/jvndb/JVNDB-2015-000199

CVSS による深刻度 (CVSS とは?)

CVSS v3 による深刻度
基本値: 7.8 (重要) [IPA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

https://jvn.jp/jp/JVN64636058/

JPCERT/CCによる脆弱性分析結果

CVSS v3　CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H　**基本値: 7.8** ▲

攻撃元区分(AV)	物理 (P)	**ローカル (L)**	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	**低 (L)**		
必要な特権レベル(PR)	高 (H)	低 (L)	**不要 (N)**	
ユーザ関与レベル(UI)	**要 (R)**	不要 (N)		
スコープ(S)	**変更なし (U)**	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	**高 (H)**	
完全性への影響(I)	なし (N)	低 (L)	**高 (H)**	
可用性への影響(A)	なし (N)	低 (L)	**高 (H)**	

世界でも、国内でも活用されている

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9444

CVSS v3.0 Severity and Metrics:
Base Score: 7.5 HIGH
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Impact Score: 3.6
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): None
Integrity (I): None
Availability (A): High

https://tools.cisco.com/security/center/cvssCalculator.x

Cisco Security
Common Vulnerability Scoring System

Choose the version of CVSS calculator: Version 3.1

Common Vulnerability Scoring System (CVSS) Online Calculator, version 3.1

Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:L/E:F/RL:O/RC:U/CR:L/IR:X/AR:L/MAV:L/MAC:L/MPR:N/MUI:R/MS:U/MC:N/MI:N/MA:N

This tool is used to calculate a specific th
CVSS score will be displayed. Use of this

https://access.redhat.com/security/cve/cve-2017-5897

CVSS v3 Score Breakdown	Red Hat	NVD
CVSS v3 Base Score	3.7	9.8
Attack Vector	Network	Network
Attack Complexity	High	Low
Privileges Required	None	None
User Interaction	None	None
Scope	Unchanged	Unchanged
Confidentiality Impact	None	High
Integrity Impact	Low	High
Availability Impact	None	High

CVSS v3 Vector

Red Hat: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

NVD: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

MELSEC シリーズ CPU ユニットにおけるサービス拒否(DoS)及び悪意のあるコードが実行される脆弱性

公開日 2023 年 5 月 23 日
最終更新日 2023 年 9 月 12 日
三菱電機株式会社

■概要

MELSEC シリーズの CPU ユニットには、サービス拒否(DoS)及び悪意のあるコードが実行される脆弱性が存在します。攻撃者は、該当製品に対して不正なパケットを送信することにより、当該製品をサービス停止(DoS)状態に陥らせたり、悪意のあるコードを実行させたりすることができる可能性があります。ただし、悪意のあるコードを実行するためには、攻撃者は、製品の内部構造を知る必要があるため、悪意のあるコードを実行することは、容易ではありません。(CVE-2023-1424)

■CVSS スコア [1]

CVE-2023-1424 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H 基本値 10.0

https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2023-003.pdf

CVSSのバージョン管理

- 米国政府組織(NIAC)が原案を策定, FIRSTが管理
  - 2005年6月にv1が、翌年v2が公開される
  - 現時点での最新は、2019年6月に公開されたv3.1
  - 改訂版v4.0に向けて検討が進んでいる

- JPCERT/CCとして、v3.1の利用を推奨
  - v2は、攻撃対象＝影響範囲＝ホストやシステム
  - v3は、攻撃対象＝攻撃可能なコンポーネント
    - 仮想化やサンドボックス化といったソフトウェアを独立実行する技術に対応
    - 現在のソフトウェア利用環境に対応した評価が可能

以降は、CVSSv3の記述でv3.1に関する説明をする。

CVSSv3 評価基準

以下の3つの基準がある

- Base Metrics（基本評価基準）
- Temporal（現状評価基準）
- Environment（環境評価基準）

次のスライドから、それぞれの基準を説明する。

CVSSv3 基本評価基準 (Base Metrics)

脆弱性そのものの技術的な特性を評価する基準。想定する攻撃シナリオや評価者の違いによる相違はあるが、新たな攻撃手法が検出されるなど大きな変化がない限り、時間の経過による評価の変更がないため、JVNなど多くの脆弱性情報に、この基準が掲載されている。

- 攻撃元区分 (AV: Attack Vector)
- 攻撃条件の複雑さ (AC: Attack Complexity)
- 必要な特権レベル (PR: Privileges Required)
- ユーザ関与レベル (UI: User Interaction)
- スコープ (S: Scope)
- 機密性への影響 (C: Confidentiality Impact)
- 完全性への影響 (I: Integrity Impact)
- 可用性への影響 (A: Availability Impact)

それぞれの項目は、後ろのスライドで説明する。

CVSSv3 現状評価基準 (Temporal Metrics)

攻撃コードが世の中に出回っているか、公式の対策パッチがリリース済みか、といった現状を評価する基準。脆弱性の対象製品のベンダーが本基準を掲載し、対応状況に応じて更新するようなケースで利用される。

- **攻撃される可能性 (E: Exploit Code Maturity)**
  攻撃コードや手法が実際に使用可能であるかを評価
  （容易に攻撃／攻撃可能／実証コードあり／未実装）

- **利用可能な対策のレベル (RL: Remediation Level)**
  脆弱性の対策がどの程度使用可能であるかを評価
  （対策なし／非開発者の対策／暫定対策／公式対策）

- **脆弱性情報の信頼性 (RC: Report Confidence)**
  脆弱性関連情報の信憑性を評価
  （開発者確認済／非開発者情報／未確認情報のみ）

CVSSv3 環境評価基準 (Environmental Metrics)

具体的なユーザ環境固有において、機密性・完全性・可用性それぞれ重要度評価（対象システムのセキュリティ要求度）および実環境に即した基本評価基準の再評価を行う基準。

対象システムのセキュリティ要求度
(Security Requirements)
それぞれの評価項目が失われた場合の影響を選択

- 評価項目
  - 機密性の要求度
    (CR: Confidentiality Requirement)
  - 完全性の要求度
    (IR: Integrity Requirement)
  - 可用性の要求度
    (AR: Availability Requirement)
- 選択肢
  - 高：壊滅的な影響
  - 中：深刻な影響
  - 低：一部の影響

環境条件を加味した基本評価の再評価
(Modified Base Metrics)

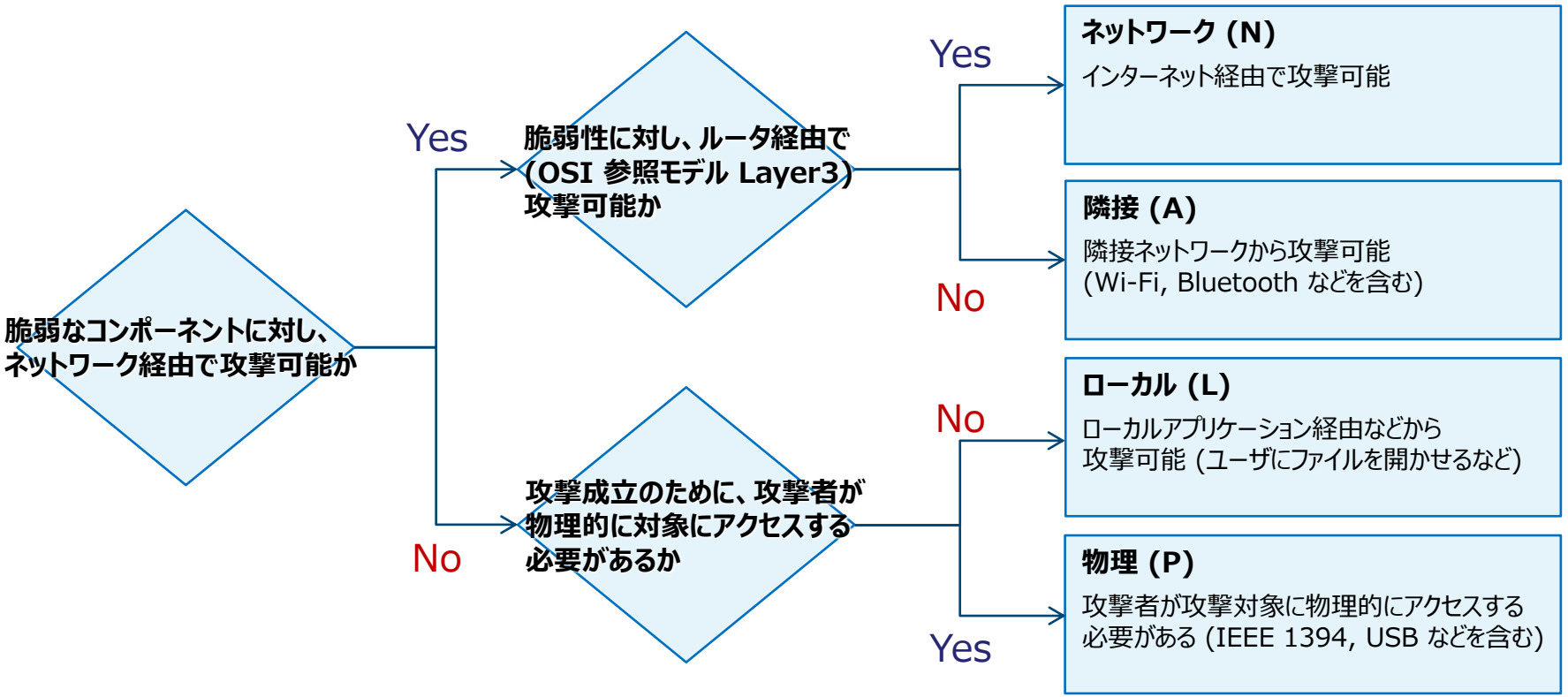
- 緩和策後の攻撃元区分 (MAV)
- 緩和策後の攻撃条件の複雑さ (MAC)
- 緩和策後の必要な特権レベル (MPR)
- 緩和策後のユーザ関与レベル (MUI)
- 緩和策後のスコープ (MS)
- 緩和策後の機密性への影響 (MC)
- 緩和策後の完全性への影響 (MI)
- 緩和策後の可用性への影響 (MA)

CVSSv3 基本評価基準

攻撃元区分 (Attack Vector)

Attack Vector (AV) … 攻撃元区分

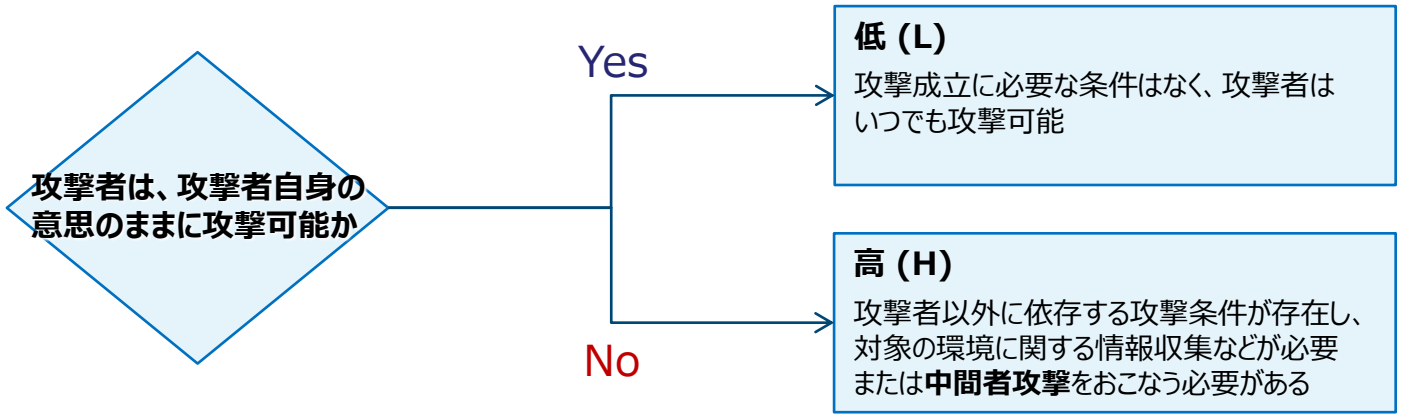
- システムを、どこから攻撃可能であるかを評価



攻撃条件の複雑さ (Attack Complexity)

Attack Complexity (AC) … 攻撃条件の複雑さ

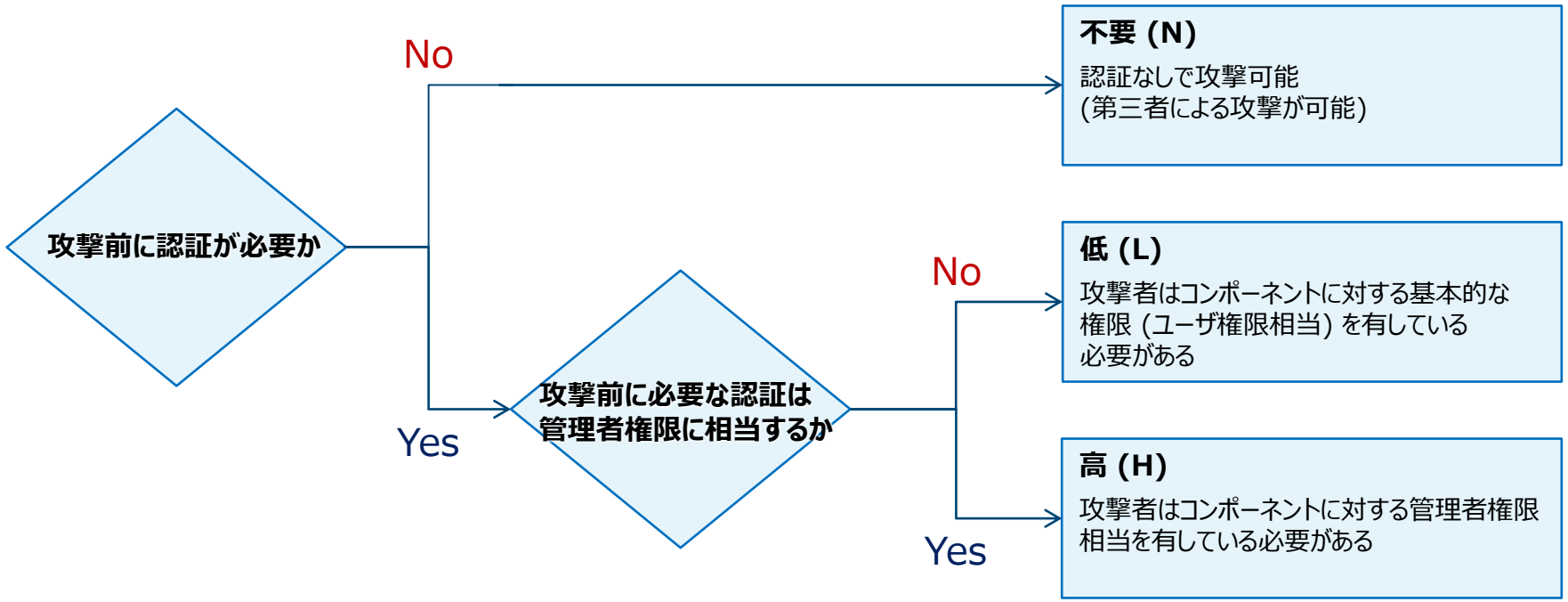
- 攻撃に必要な条件がどのようなものであるのかを評価



必要な特権レベル (Privileges Required)

Privileges Required (PR) … 必要な特権レベル

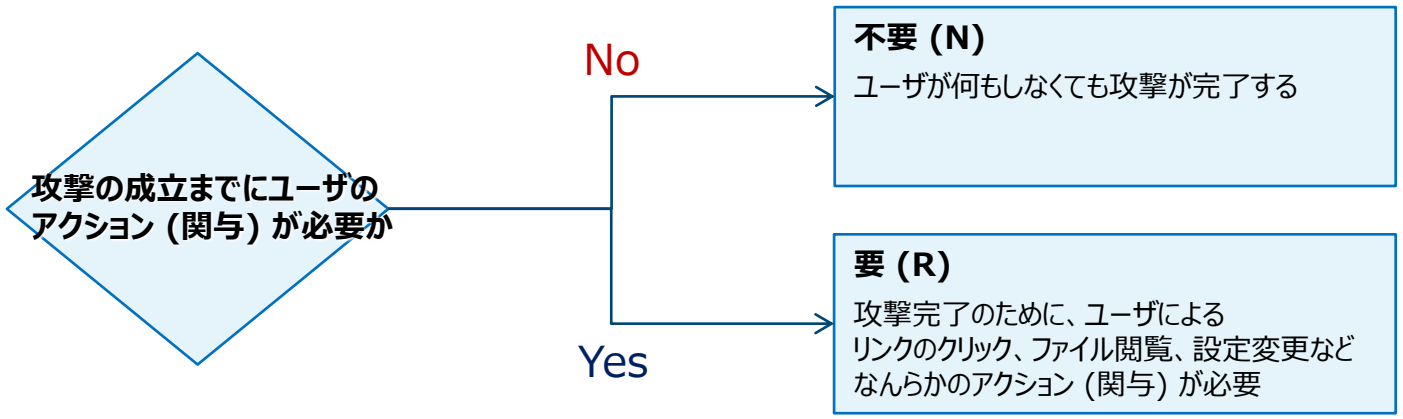
- 攻撃に必要な認証レベルを評価



ユーザ関与レベル (User Interaction)

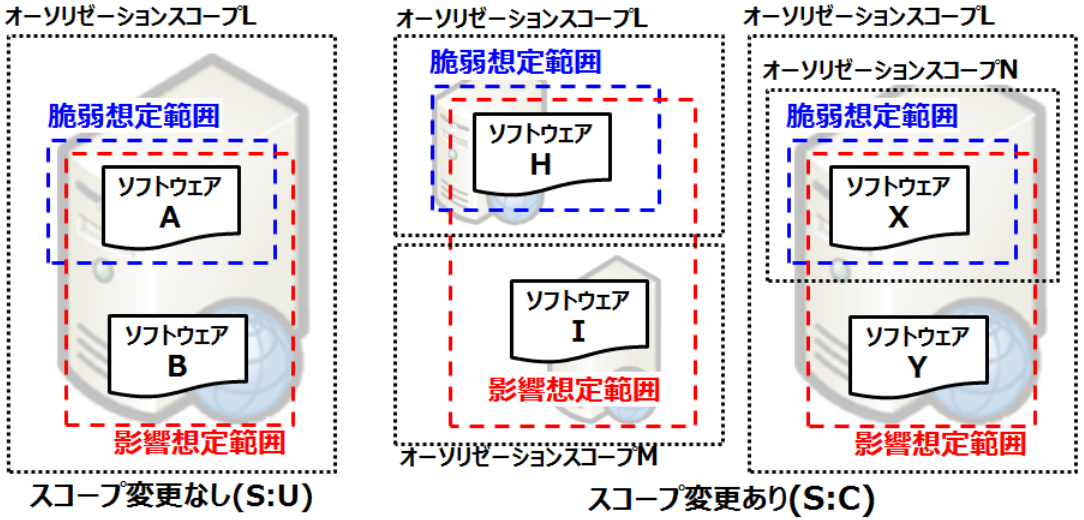
User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価



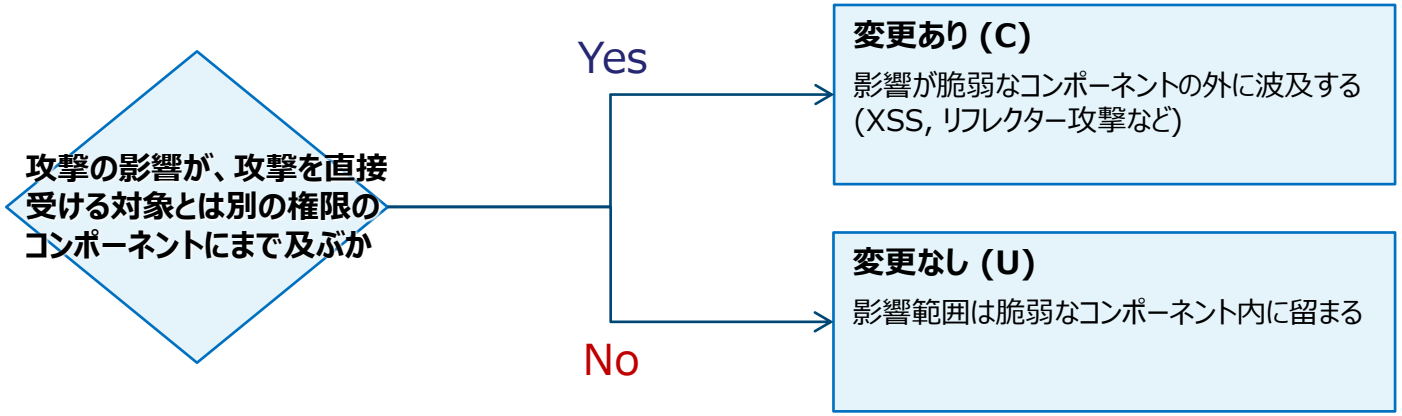
スコープ (Scope)

Scope (S) … スコープ - 被害の影響範囲を評価



情報処理推進機構 (IPA)
共通脆弱性評価システムCVSS v3概説
https://www.ipa.go.jp/security/vuln/CVSSv3.html

オーソリゼーションスコープ（Authorization Scope）
計算機資源に対する管理権限の範囲のこと。
直接攻撃を受ける（脆弱性が存在する）コンポーネント（ソフトウェア）と、この攻撃によって影響を受けるコンポーネントが同じ管理権限でのアクセスを想定していれば、スコープ変更なしとなる。



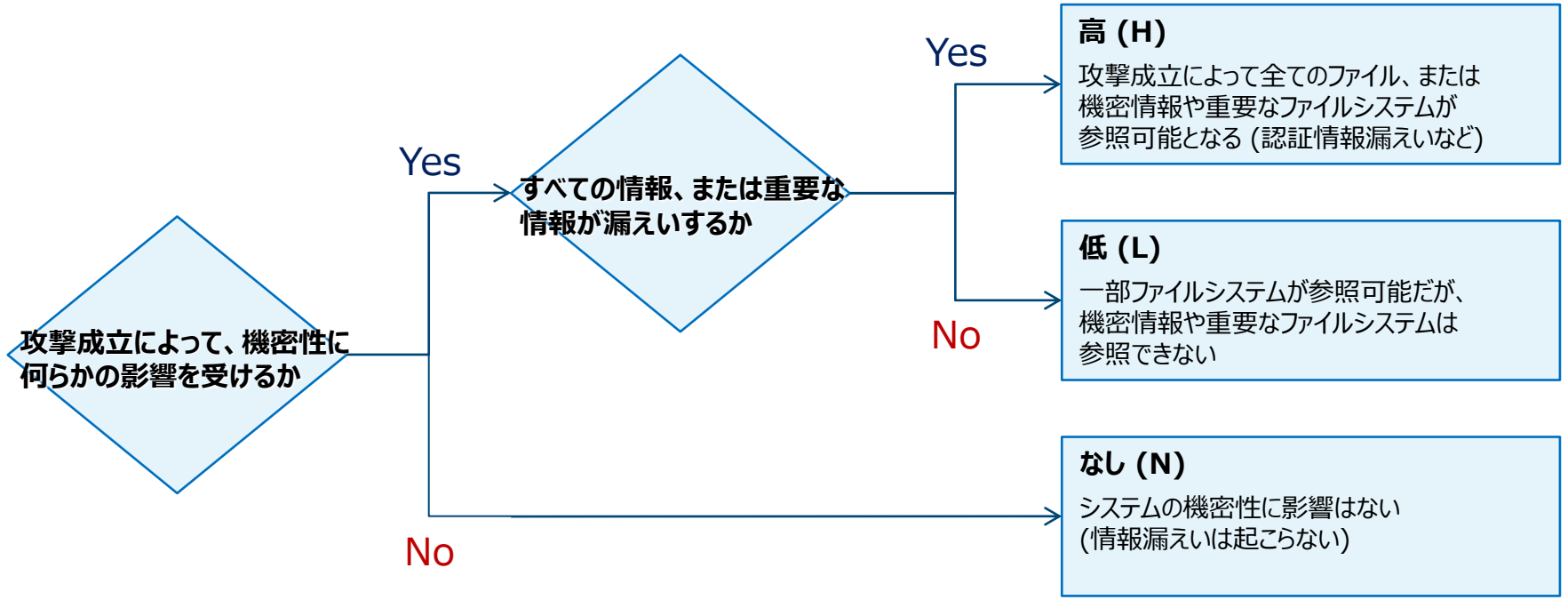
例えば、
XSS（クロスサイトスクリプティング）の脆弱性の場合
- XSSの脆弱性が存在するコンポーネント
  ⇒ Webサーバで稼働するアプリ
  　サーバ管理者がアクセス可能
- 影響を受ける（スクリプトが実行される）コンポーネント
  ⇒ Webアプリ利用者のブラウザ
  　サーバ管理者権限でのアクセスは想定されていない

∴XSSの脆弱性は「Scope 変更あり」となります。

機密性への影響 (Confidentiality Impact)

Confidentiality Impact (C) … 機密性への影響

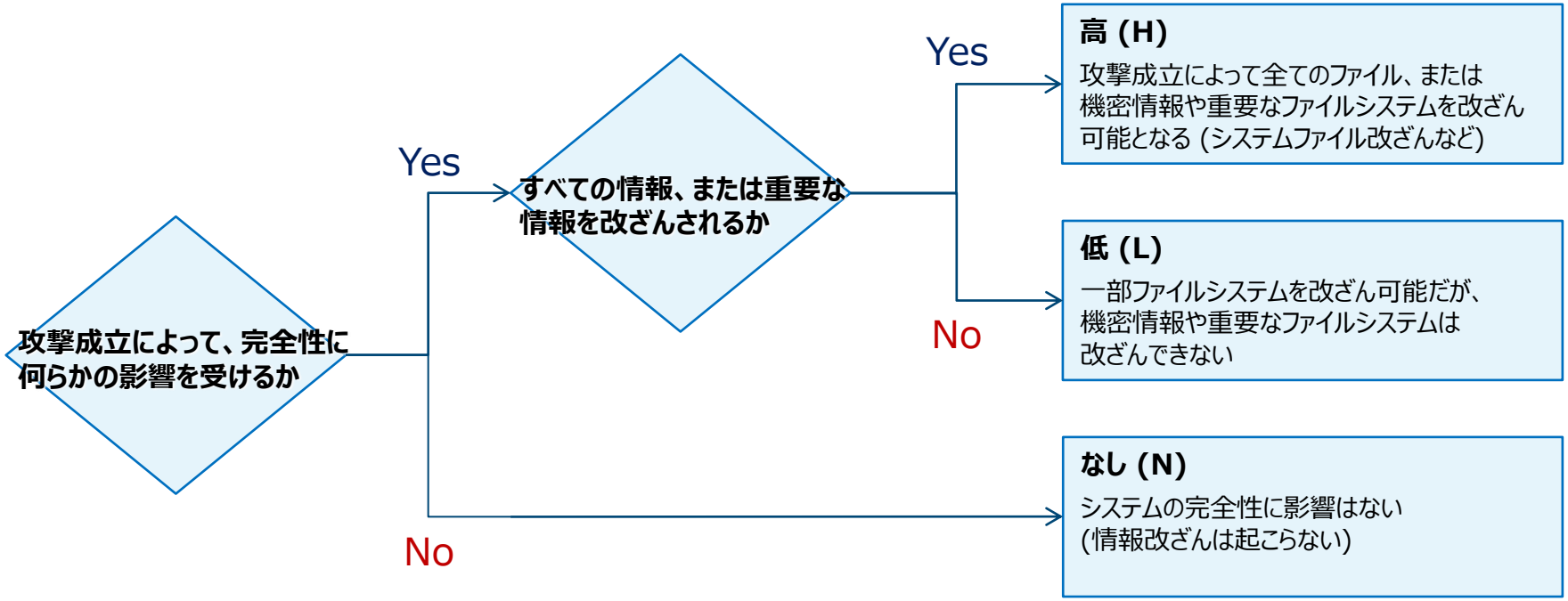
- 攻撃された際に機密性に影響があるかを評価



完全性への影響 (Integrity Impact)

Integrity Impact (I) … 完全性への影響

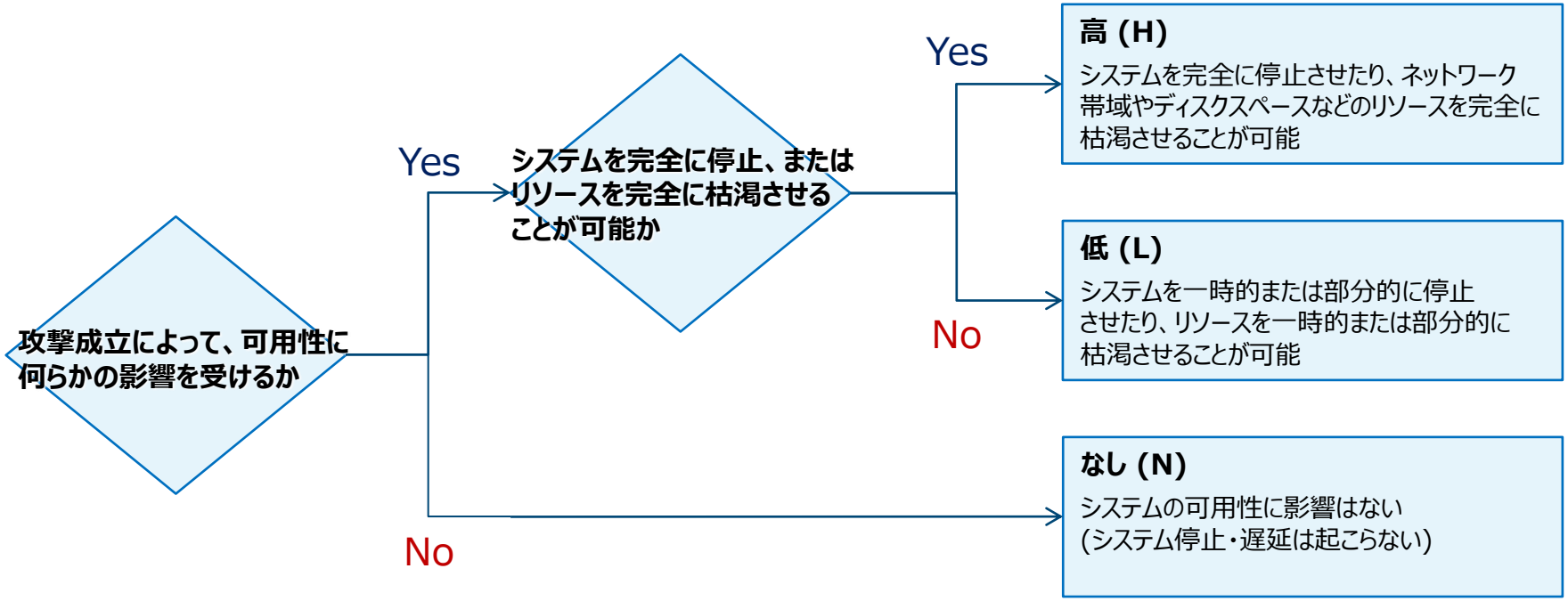
- 攻撃された際に完全性に影響があるかを評価



可用性への影響 (Availability Impact)

Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



CVSSv3 ワークショップの内容と目的

■内容

- JVN で公表した案件のいくつかに CVSSv3 の基本評価基準を適用してみる

■目的

- 脆弱性関連情報 (アドバイザリや届出情報等) を見たときに、攻撃シナリオや脅威について**大まかに**把握できるようになる
- どういった状況で何をされると深刻な脆弱性であると評価されるのかが**なんとなく**わかるようになる
- 頭の体操になる

では始めましょう

- 1案件ごとに基本評価基準を検討
  - 各案件の概要と、まとめのスライドを見ながら、回答シートの各評価基準の選択条件と選択肢から適切なものを選ぶ
    - CVSS Calculatorを使ってもOK
    - ここまでのスライドを復習しながら、1項目ずつ選ぶ
    - 悩んでも投げ出さず、自分なりの理由を考え、選ぶ
- その後、答え合わせ
  - JVN掲載評価と、解説のスライドを自分の回答と比較してみる
    - 評価が一致し、解説も納得できたらOK
    - 評価は異なったが、解説によって納得できたらOK
    - 疑問が残る、自分はこう考えた、などは、気軽に本GitHubのIssueへ

概要：案件1）F-RevoCRM におけるクロスサイトスクリプティングの脆弱性

公開日：2020/01/08　最終更新日：2020/01/08

JVN#97325754
F-RevoCRM におけるクロスサイトスクリプティングの脆弱性

概要
F-RevoCRM には、クロスサイトスクリプティングの脆弱性が存在します。

影響を受けるシステム

- F-RevoCRM 6.0 から F-RevoCRM 6.5 patch6 まで (バージョン 6系)

詳細情報
シンキングリード株式会社が提供する F-RevoCRM には、クロスサイトスクリプティング (CWE-79) の脆弱性が存在します。

想定される影響
当該製品を使用しているユーザのウェブブラウザ上で、任意のスクリプトを実行される可能性があります。

対策方法
パッチを適用する
開発者が提供する情報をもとに、パッチを適用してください。

ワークアラウンドを実施する
次のワークアラウンドを実施することで、本脆弱性の影響を軽減することが可能です。

- 信頼性が低い外部サイト参照の際は、F-RevoCRM からログアウトした状態にしておくか、F-RevoCRM を開いているブラウザと異なるブラウザを使用する
- Proxy サーバなどで不適切なサイトへのアクセスを制限する

https://jvn.jp/jp/JVN97325754/

まとめ：案件1）F-RevoCRM におけるクロスサイトスクリプティングの脆弱性

- **脆弱性の種類**
  クロスサイトスクリプティング (XSS)
- **攻撃のシナリオ**
  ログイン中のユーザが罠リンク (URL) にアクセスすることで、ユーザのウェブブラウザ上で任意のスクリプトを実行される
- **想定される影響**
  結果として、表示情報を**改ざん**されたり、ウェブブラウザの持つ情報を攻撃者に**取得**されたりする。**脆弱なのはウェブサイト**だが、**影響を受けるのはユーザ**
- **補足情報**
  ログインが不要なウェブサイトの一般閲覧者ではなく、ログイン済みユーザを誘導した場合のみ攻撃が成立する。が、攻撃の難易度はCVSS v3 の評価に影響しない

回答シート：案件1）F-RevoCRM におけるクロスサイトスクリプティングの脆弱性

CVSS v3　CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?　基本値: ?.? ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

JVN掲載評価：案件1）F-RevoCRM におけるクロスサイトスクリプティングの脆弱性

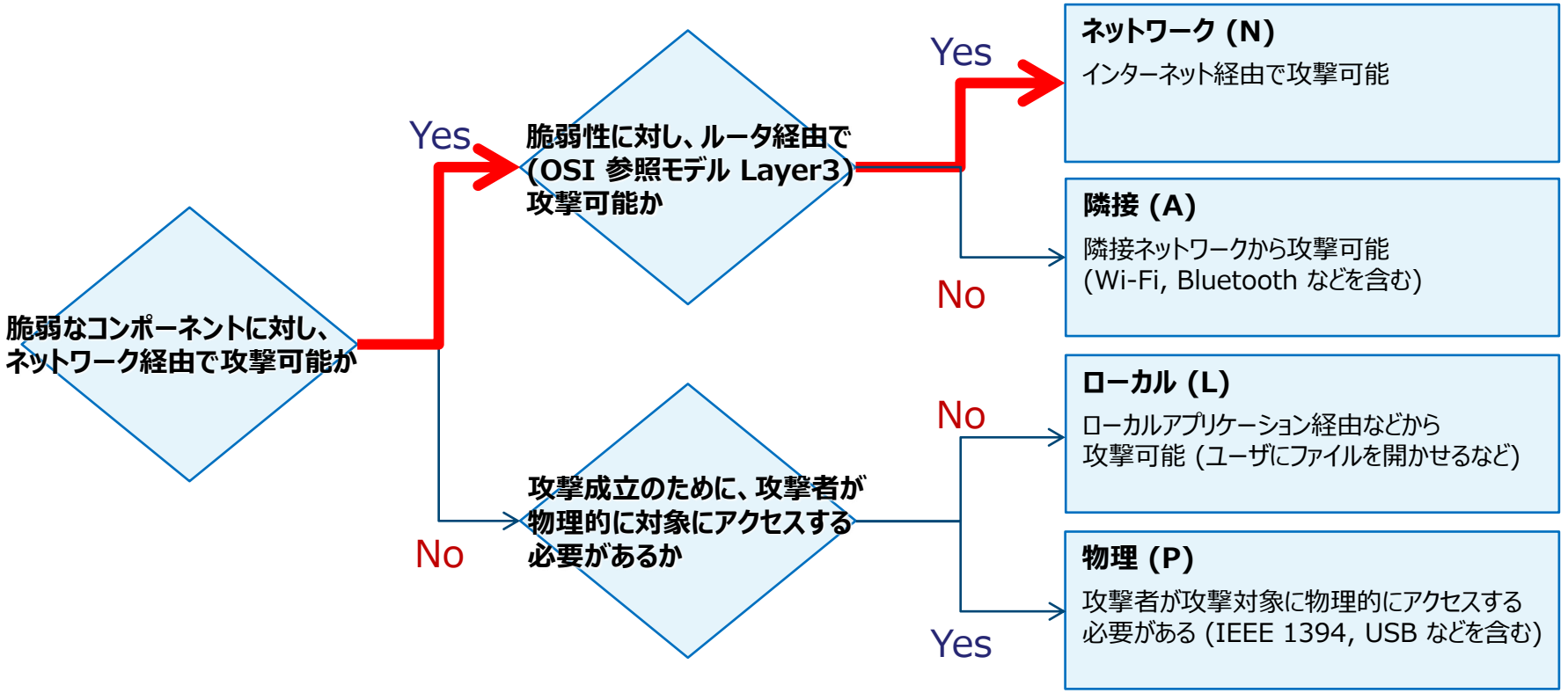
CVSS v3　CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N　**基本値: 6.1** ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	**ネットワーク (N)**
攻撃条件の複雑さ(AC)	高 (H)	**低 (L)**		
必要な特権レベル(PR)	高 (H)	低 (L)	**不要 (N)**	
ユーザ関与レベル(UI)	**要 (R)**	不要 (N)		
スコープ(S)	変更なし (U)	**変更あり (C)**		
機密性への影響(C)	なし (N)	**低 (L)**	高 (H)	
完全性への影響(I)	なし (N)	**低 (L)**	高 (H)	
可用性への影響(A)	**なし (N)**	低 (L)	高 (H)	

Attack Vector (AV) … 攻撃元区分

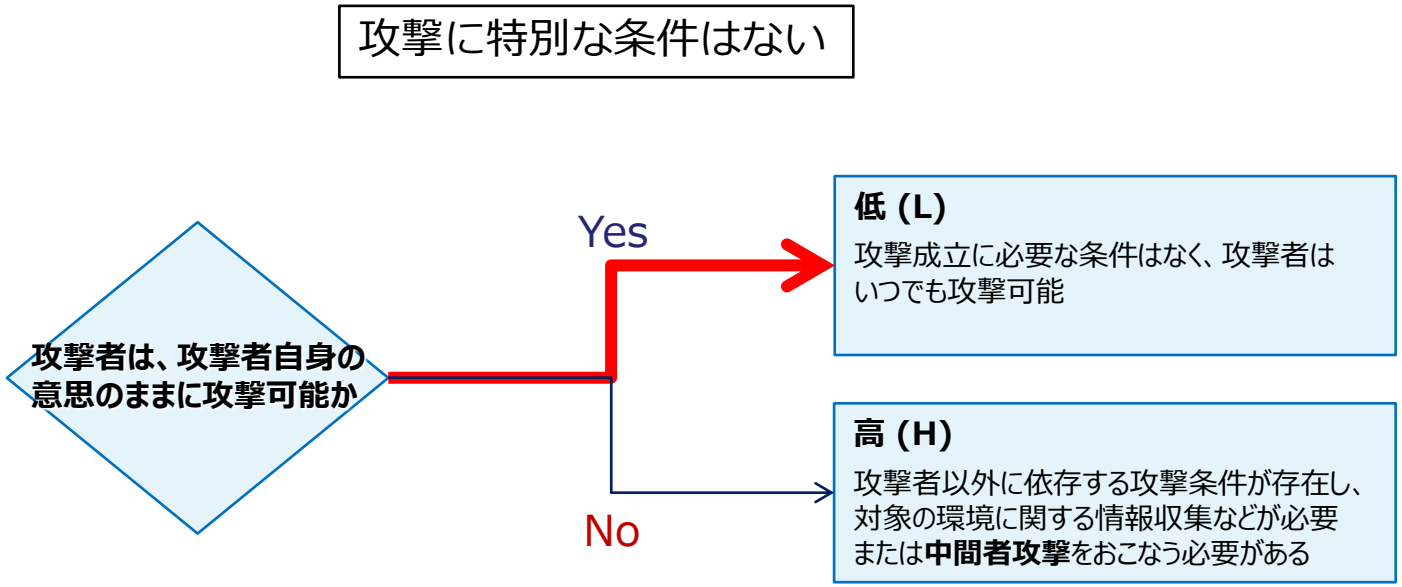
- システムを、どこから攻撃可能であるかを評価

ウェブアプリケーションの脆弱性であり、
ネットワーク経由で攻撃を受ける



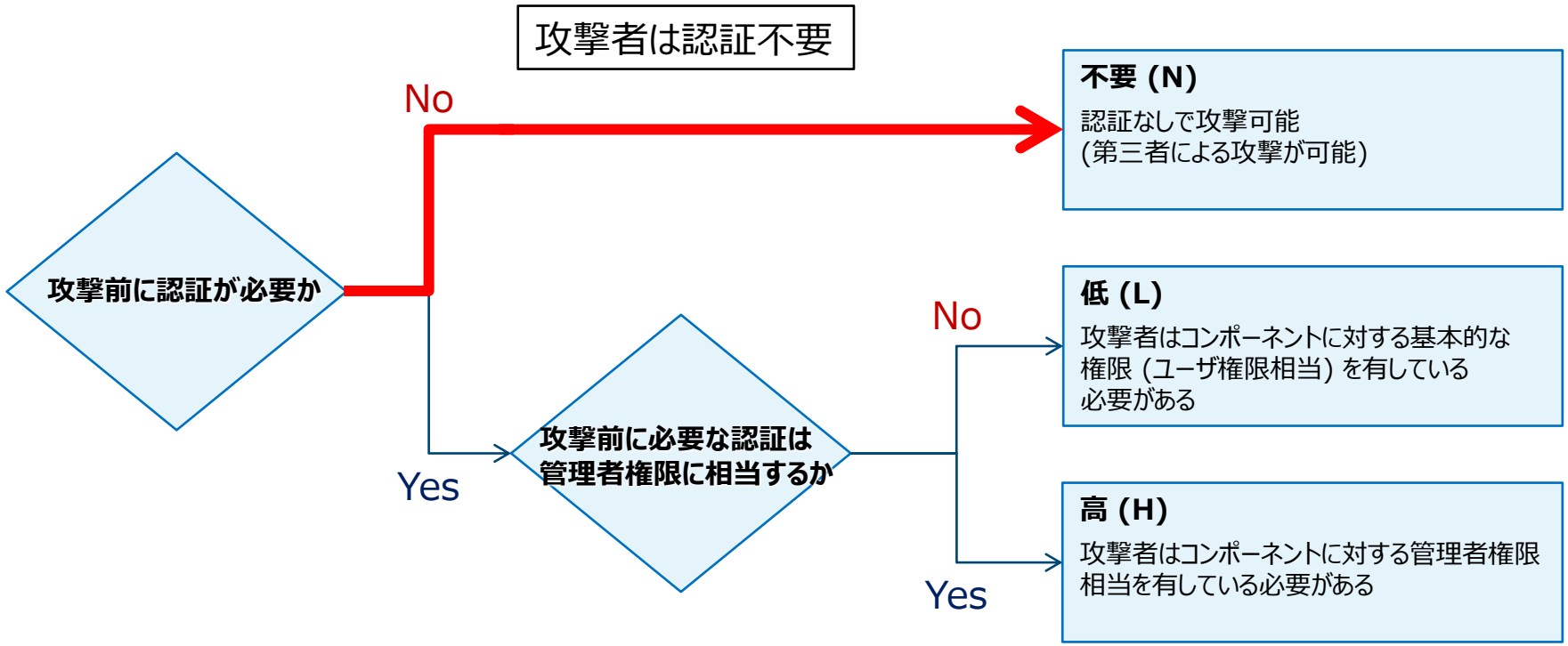
Attack Complexity (AC) … 攻撃条件の複雑さ

- 攻撃に必要な条件がどのようなものであるのかを評価



Privileges Required (PR) … 必要な特権レベル

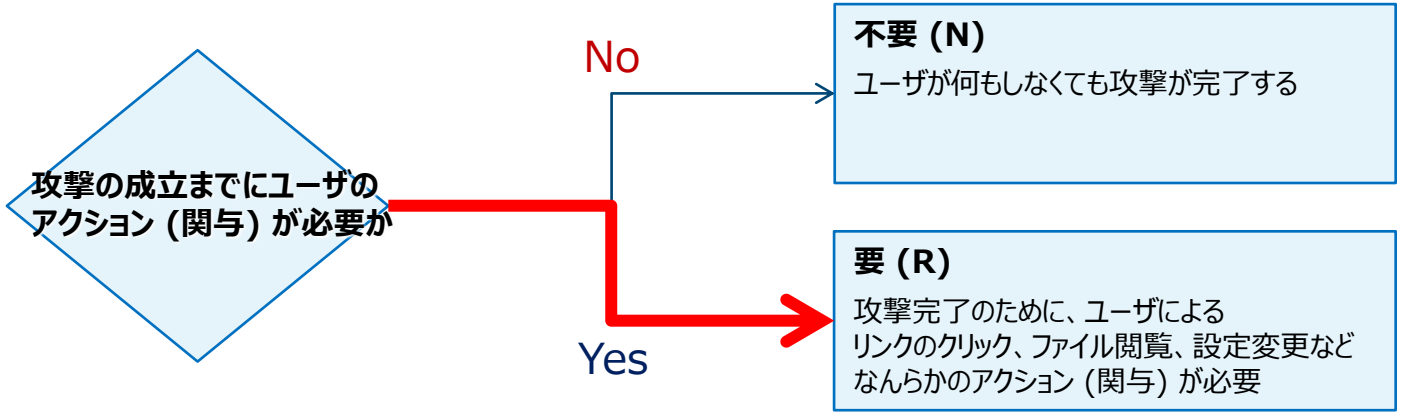
- 攻撃に必要な認証レベルを評価



User Interaction (UI) … ユーザ関与レベル

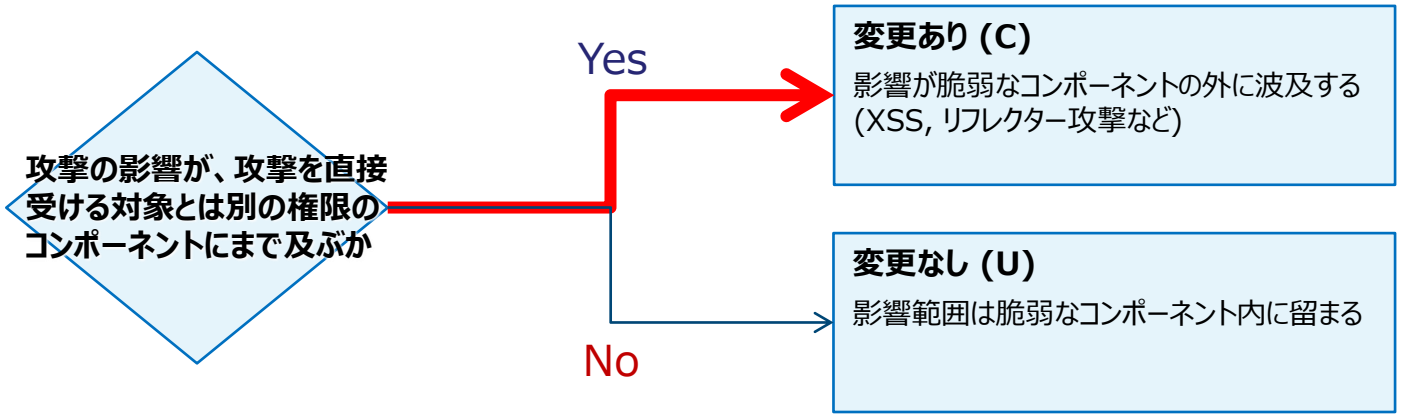
- 攻撃のためにユーザ (被害者) の関与が必要かを評価

当該製品にログイン中のユーザを罠 URL にアクセスさせる必要がある



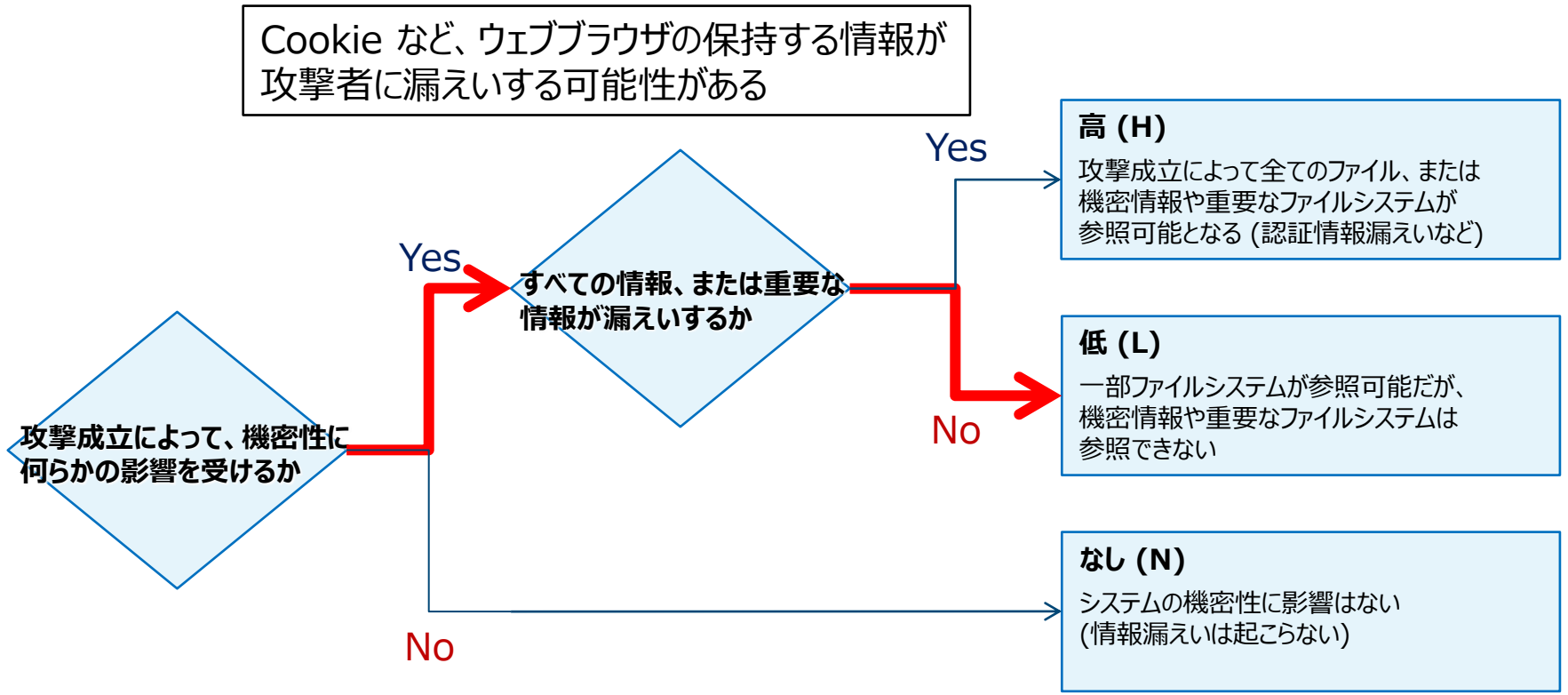
Scope (S) … スコープ - 被害の影響範囲を評価

製品 (F-RevoCRM) 自体は影響を受けず、閲覧者のWebブラウザ上でスクリプトが実行され、製品とはオーソリゼーションスコープが異なる閲覧者の環境が影響を受けるため、「変更あり(C)」となる



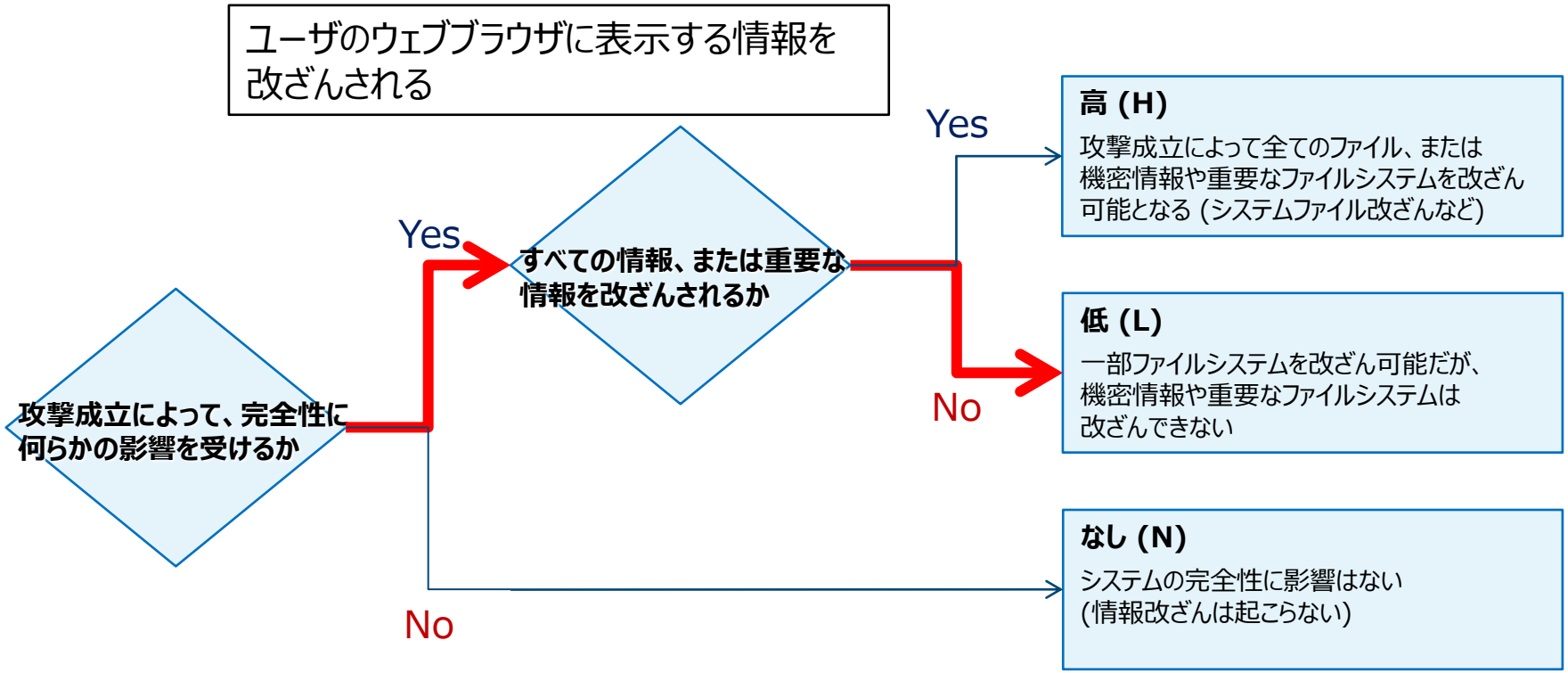
Confidentiality Impact (C) … 機密性への影響

- 攻撃された際に機密性に影響があるかを評価



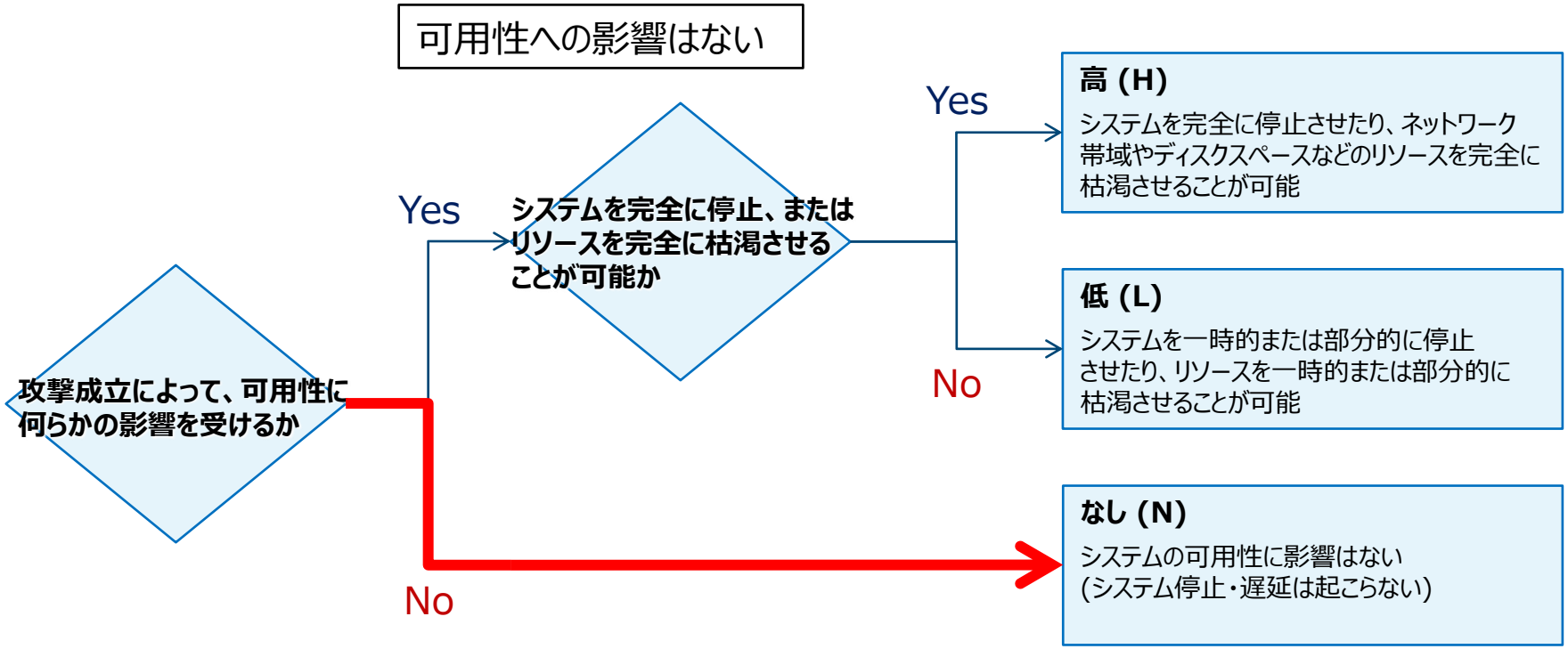
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



解説：案件1）F-RevoCRM におけるクロスサイトスクリプティングの脆弱性

評価項目	評価値	説明
攻撃元区分 (AV)	ネットワーク (N)	ウェブアプリケーションの脆弱性であり、ネットワーク経由で攻撃を受ける
攻撃条件の複雑さ (AC)	低 (L)	攻撃に特別な条件はない
必要な特権レベル (PR)	不要 (N)	攻撃者による認証は不要
ユーザ関与レベル (UI)	要 (R)	当該製品にログイン中のユーザを罠 URL にアクセスさせる必要がある
スコープ (S)	変更あり (C)	脆弱な製品 (F-RevoCRM) とは製品とはオーソリゼーションスコープが異なる閲覧者のウェブブラウザが影響を受ける
機密性への影響 (C)	低 (L)	Cookie など、ウェブブラウザの保持する情報が攻撃者に漏えいする可能性がある
完全性への影響 (I)	低 (L)	ユーザのウェブブラウザに表示する情報を改ざんされる
可用性への影響 (A)	なし (N)	可用性への影響はない

概要：案件2）トレンドマイクロ株式会社製ウイルスバスター クラウドにおける任意のファイルが削除可能な脆弱性

公開日：2020/11/18　最終更新日：2020/11/18

JVNVU#96249940
トレンドマイクロ株式会社製ウイルスバスター クラウドにおける任意のファイルが削除可能な脆弱性

概要
トレンドマイクロ株式会社製ウイルスバスター クラウドには、任意のファイルが削除可能な脆弱性が存在します。

影響を受けるシステム

- ウイルスバスター クラウド バージョン 16.0

詳細情報
トレンドマイクロ株式会社が提供するウイルスバスター クラウドには、権限の低いユーザが製品の「データ消去ツール」機能を利用し、より高い権限が設定されたファイルを削除可能となる脆弱性が存在します。

想定される影響
当該製品にアクセス可能な第三者によって、任意のファイルやフォルダを消去される可能性があります。

対策方法
パッチを適用する
開発者が提供する情報をもとにパッチを適用してください。
パッチは自動的に配信・適用されるとのことです。バージョン 16.0.1409 以降は、本脆弱性に対応したパッチが適用されています。

https://jvn.jp/vu/JVNVU96249940/

まとめ：案件2）トレンドマイクロ株式会社製ウイルスバスター クラウドにおける任意のファイルが削除可能な脆弱性

- **脆弱性の種類**
  任意のファイルを削除される問題
- **攻撃のシナリオ**
  権限のないユーザーが製品の「データ消去ツール」を利用して、**より高い権限が設定されたファイルを削除**できる
- **想定される影響**
  結果として、**当該製品にアクセス可能な第三者**が製品の「データ消去ツール」を使って任意のファイル・フォルダを削除
- **補足情報**
  脆弱性を持つのは**クライアント側アプリケーション**
  削除以外のことはできない。

回答シート：案件2）トレンドマイクロ株式会社製ウイルスバスター クラウドにおける任意のファイルが削除可能な脆弱性

CVSS v3　CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?　**基本値: ?.?** ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

JVN掲載評価：案件2）トレンドマイクロ株式会社製ウイルスバスター クラウドにおける任意のファイルが削除可能な脆弱性

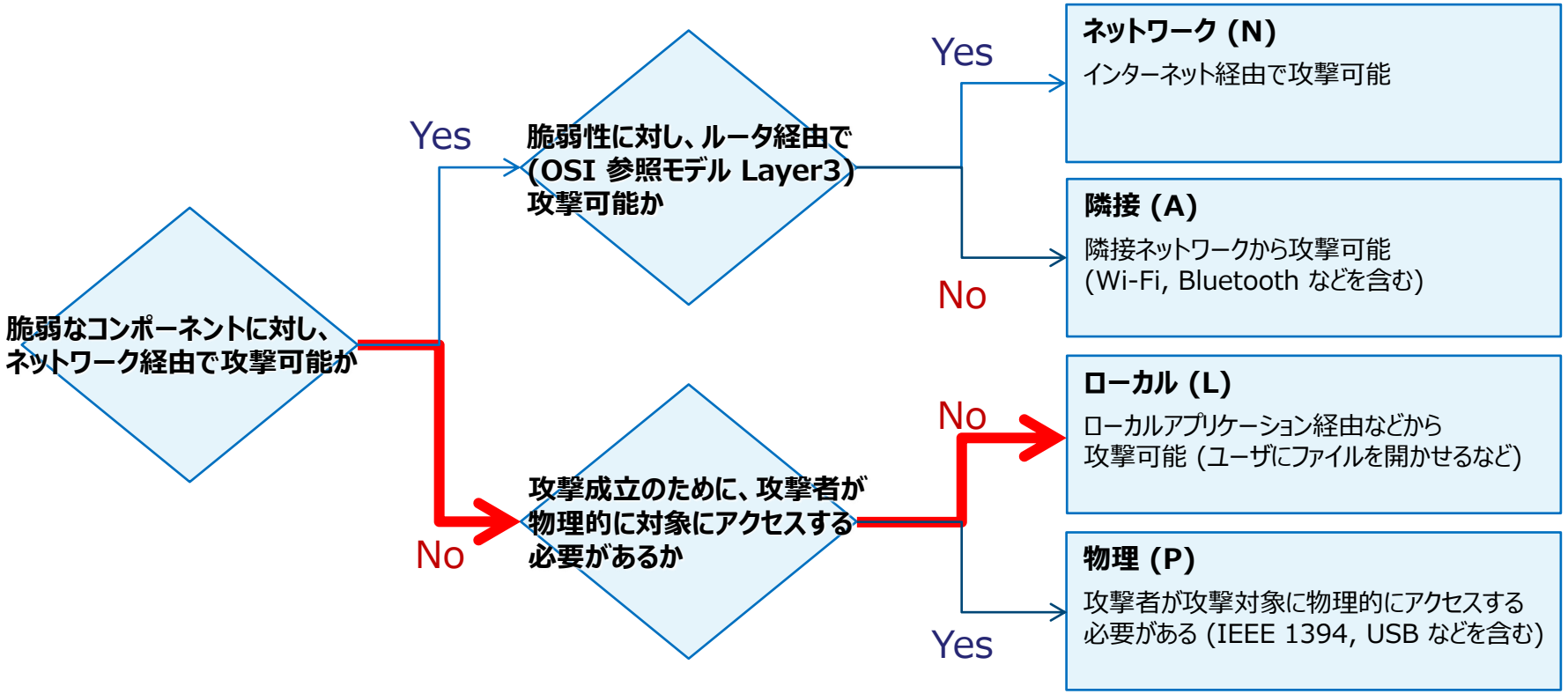
CVSS v3　CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H　**基本値: 5.3** ▲

攻撃元区分(AV)	物理 (P)	**ローカル (L)**	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	**高 (H)**	低 (L)		
必要な特権レベル(PR)	高 (H)	**低 (L)**	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	**不要 (N)**		
スコープ(S)	**変更なし (U)**	変更あり (C)		
機密性への影響(C)	**なし (N)**	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	**低 (L)**	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	**高 (H)**	

Attack Vector (AV) … 攻撃元区分

- システムを、どこから攻撃可能であるかを評価

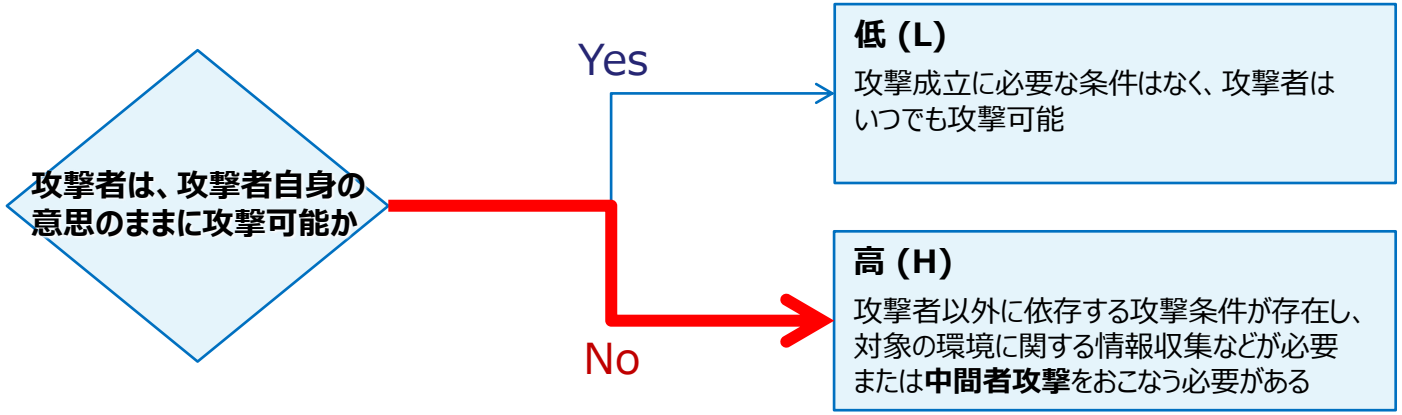
クライアント側アプリケーションのため、動作しているシステムにログインしてアクセスする必要がある



Attack Complexity (AC) … 攻撃条件の複雑さ

- 攻撃に必要な条件がどのようなものであるのかを評価

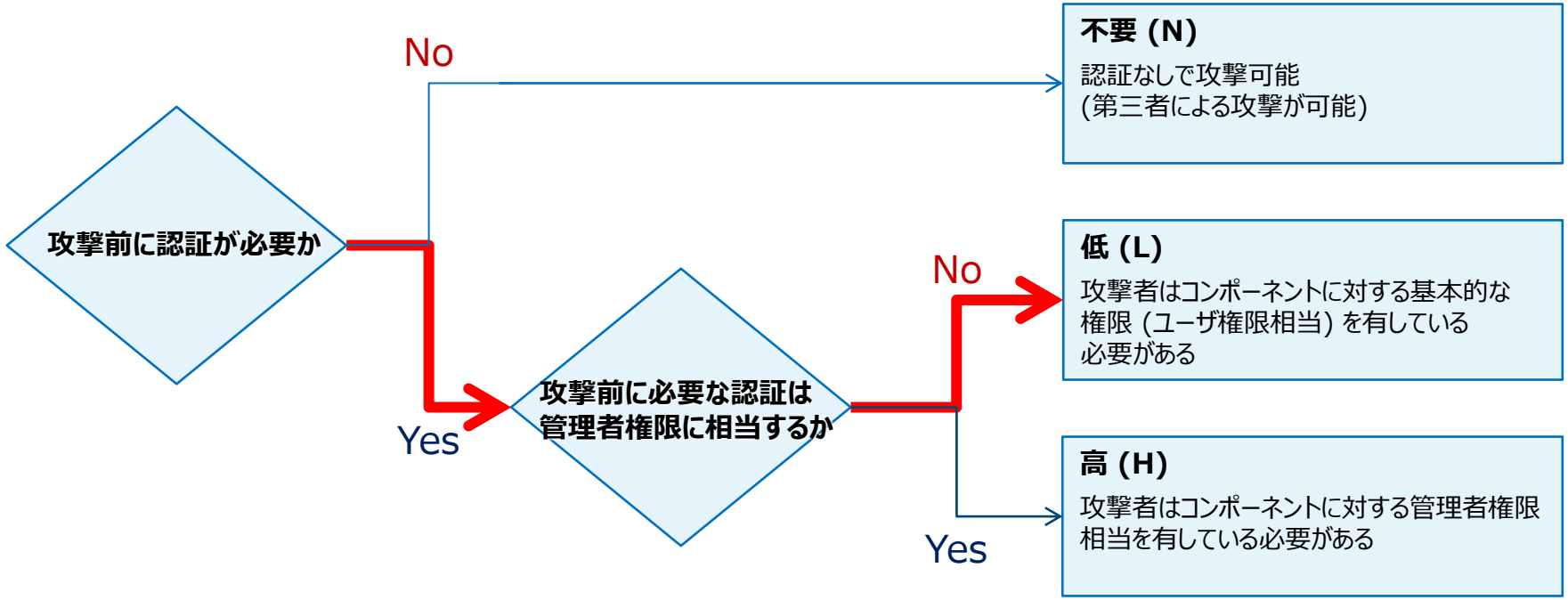
製品が動作しているシステムにログインが必要である



Privileges Required (PR) … 必要な特権レベル

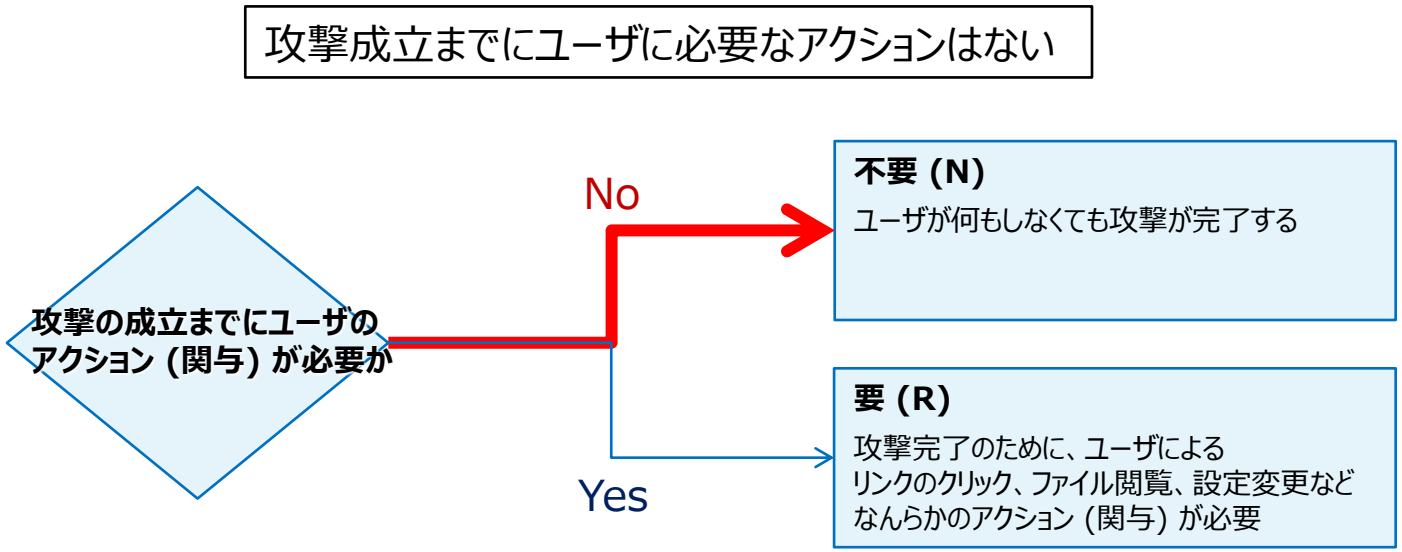
- 攻撃に必要な認証レベルを評価

製品が動作しているシステムにログインできる
ユーザアカウントが必要である



User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価



Scope (S) … スコープ - 被害の影響範囲を評価

製品が動作しているシステム以外には影響はない

攻撃の影響が、攻撃を直接受ける対象とは別の権限のコンポーネントにまで及ぶか

Yes

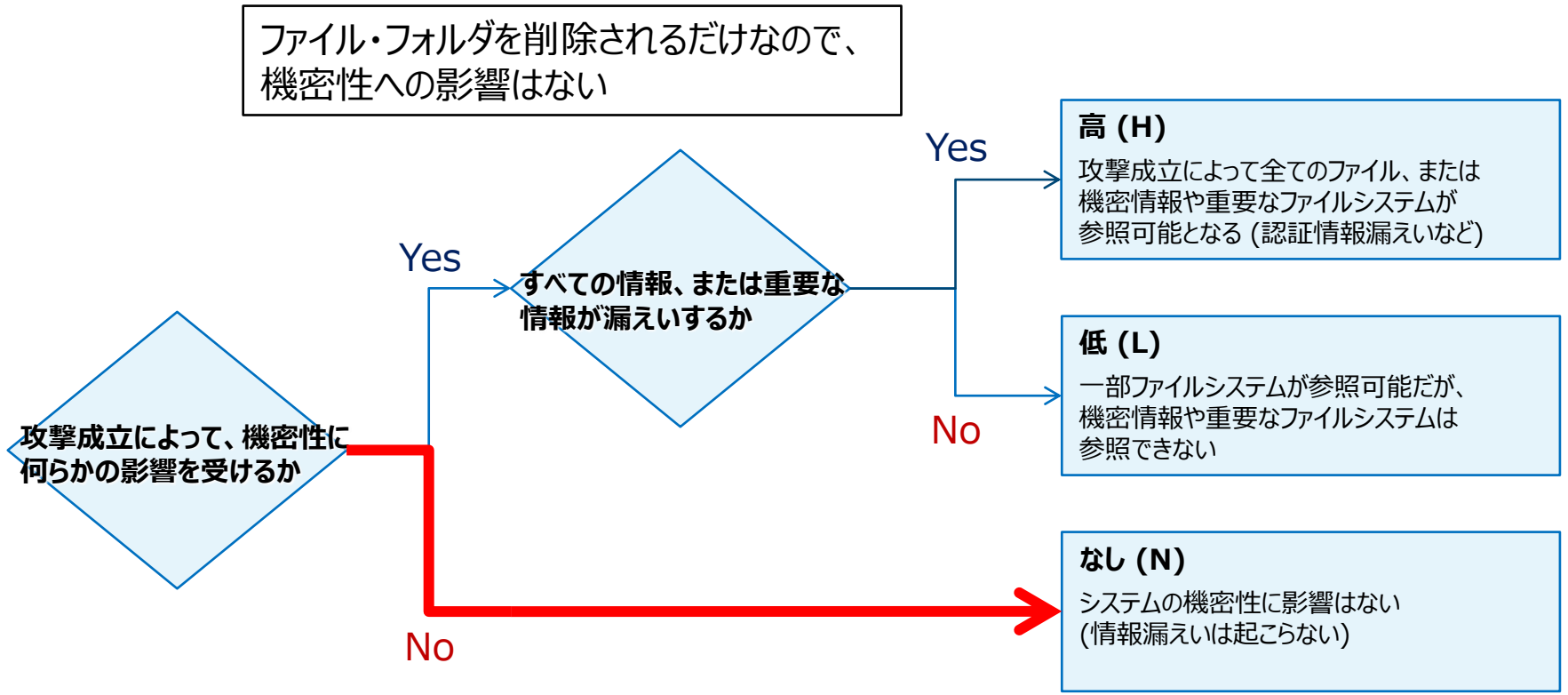
変更あり (C)
影響が脆弱なコンポーネントの外に波及する
(XSS, リフレクター攻撃など)

No

変更なし (U)
影響範囲は脆弱なコンポーネント内に留まる

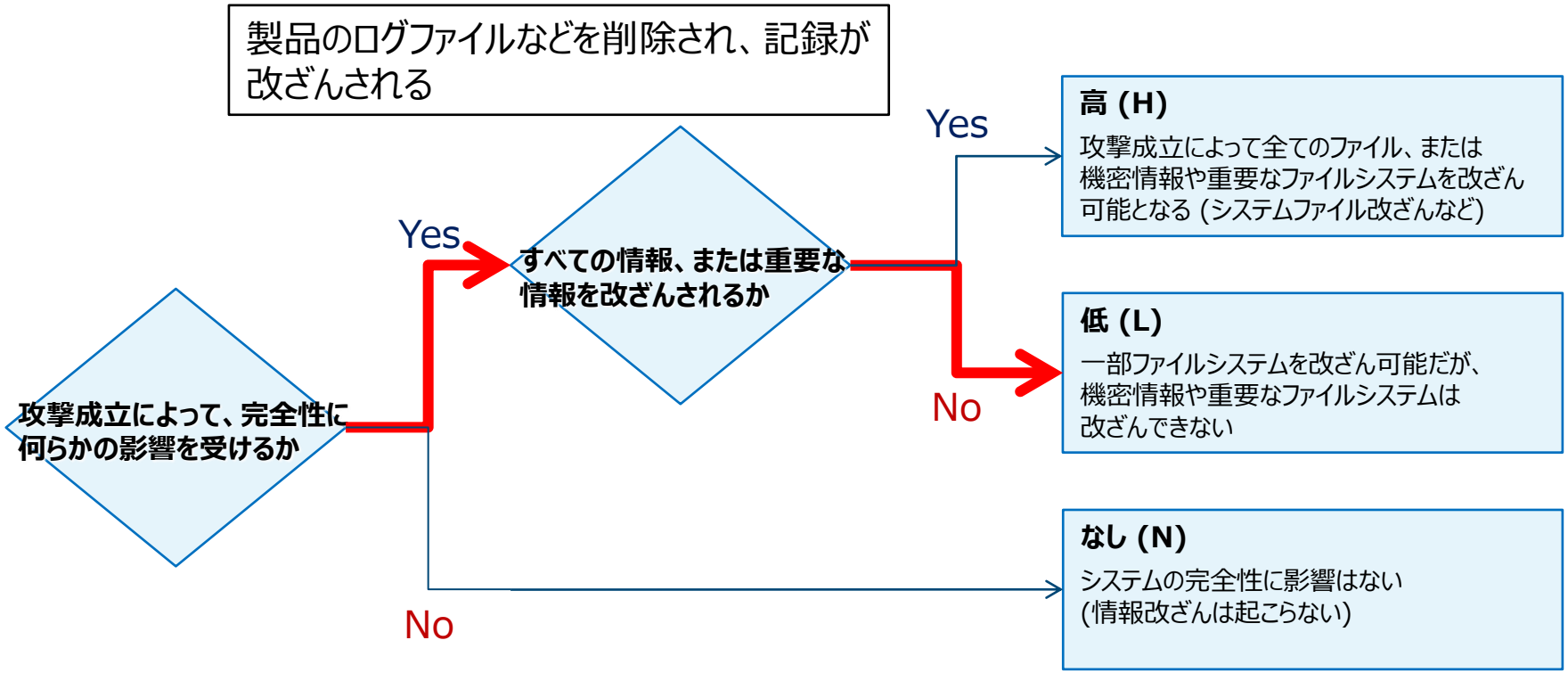
Confidentiality Impact (C) … 機密性への影響

- 攻撃された際に機密性に影響があるかを評価



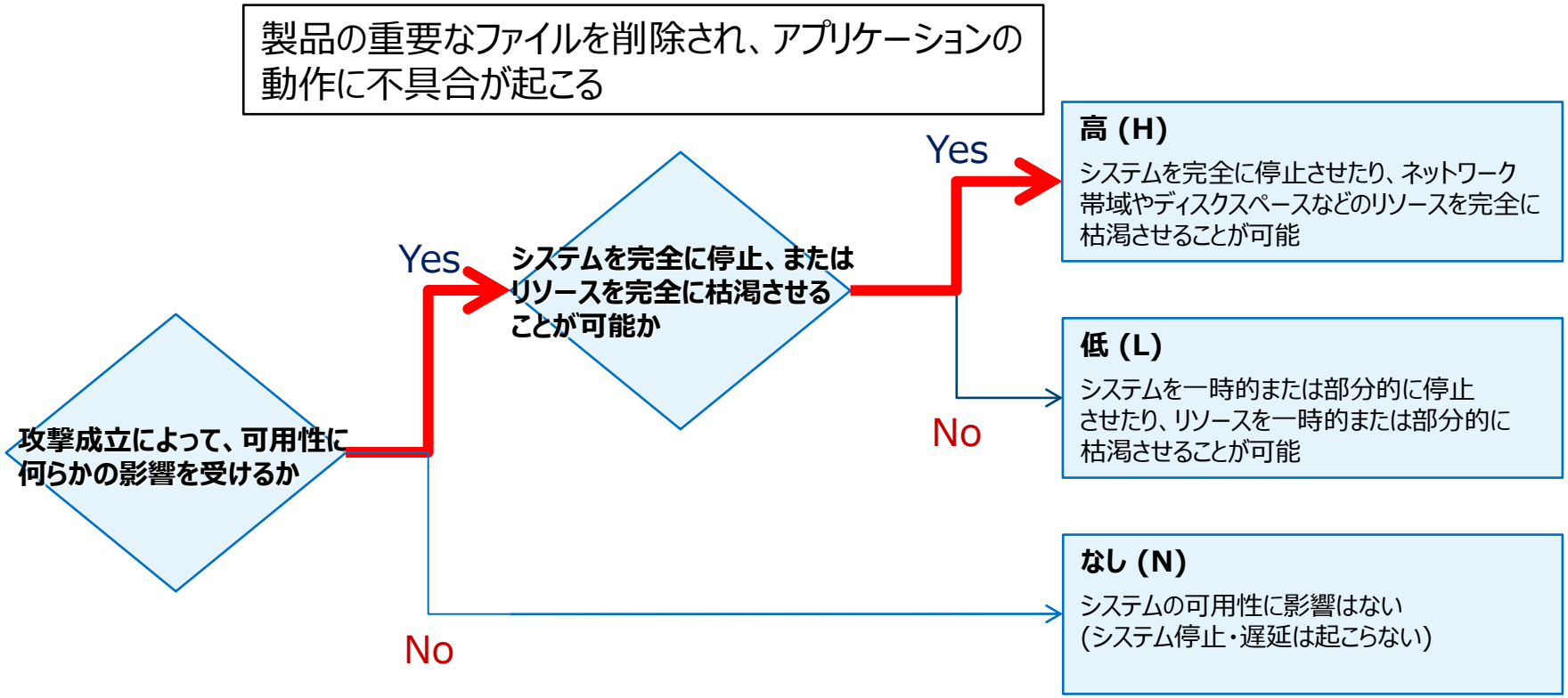
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

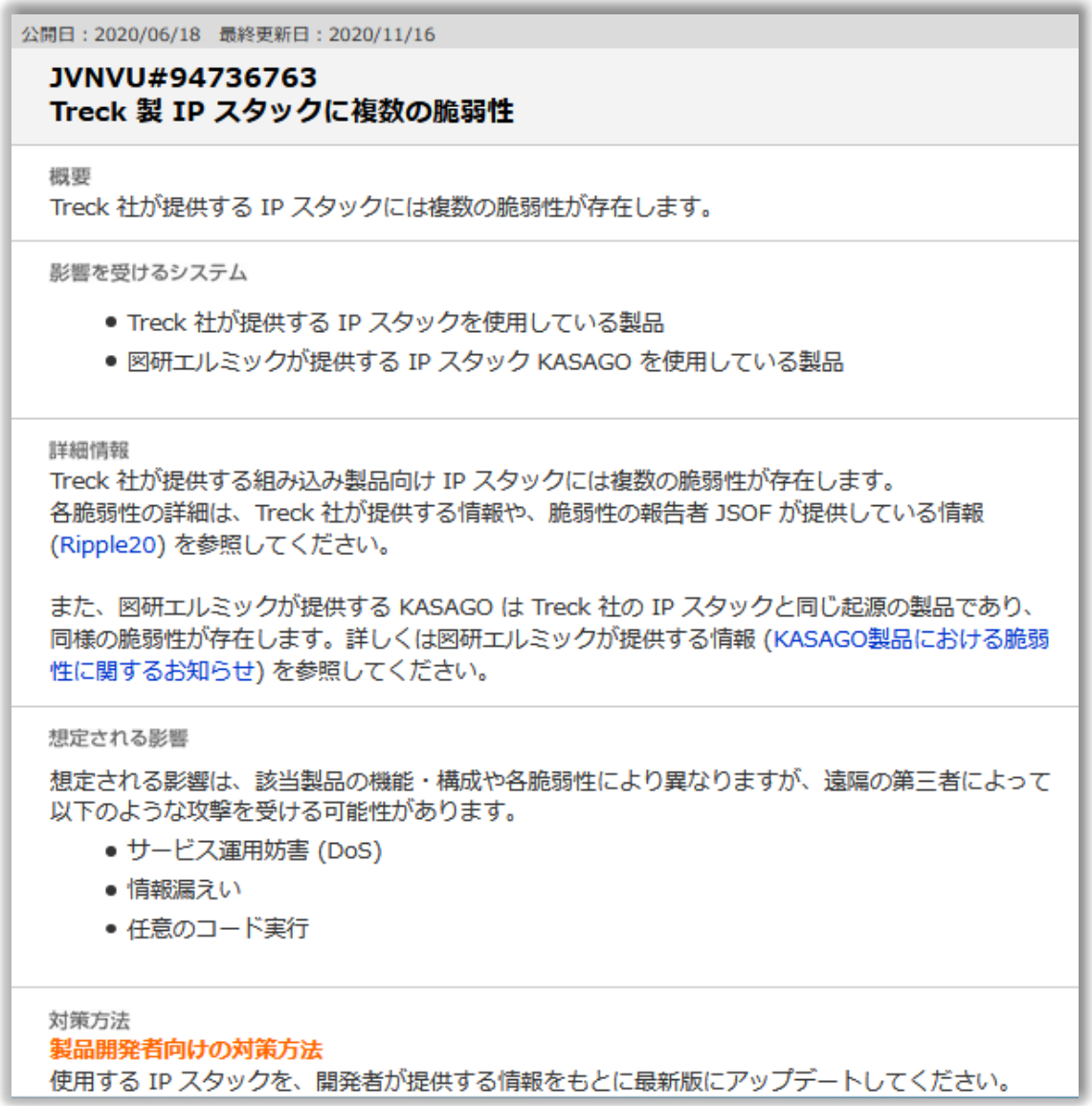
- 攻撃された際に可用性に影響があるかを評価



解説：案件2）トレンドマイクロ株式会社製ウイルスバスター クラウドにおける任意のファイルが削除可能な脆弱性

評価項目	評価値	説明
攻撃元区分 (AV)	ローカル (L)	脆弱な製品はクライアント側アプリケーションのため、動作しているシステムにログインしてアクセスする必要がある
攻撃条件の複雑さ (AC)	高 (H)	脆弱な製品が動作しているシステムにログインする必要がある
必要な特権レベル (PR)	低 (L)	脆弱な製品が動作しているシステムにログインできるユーザアカウントが必要
ユーザ関与レベル (UI)	不要 (N)	攻撃成立までにユーザに必要なアクションはない
スコープ (S)	変更なし (U)	脆弱な製品が動作しているシステム以外には影響はない
機密性への影響 (C)	なし (N)	ファイル・フォルダを削除されるだけなので、機密性への影響はない
完全性への影響 (I)	低 (L)	脆弱な製品のログファイルなどを削除され、記録が改ざんされる
可用性への影響 (A)	高 (H)	製品の重要なファイルを削除され、アプリケーションの動作に不具合が起こる

概要：案件3）Treck 製 IP スタックに複数の脆弱性



公開日：2020/06/18　最終更新日：2020/11/16

JVNVU#94736763
Treck 製 IP スタックに複数の脆弱性

概要
Treck 社が提供する IP スタックには複数の脆弱性が存在します。

影響を受けるシステム

- Treck 社が提供する IP スタックを使用している製品
- 図研エルミックが提供する IP スタック KASAGO を使用している製品

詳細情報
Treck 社が提供する組み込み製品向け IP スタックには複数の脆弱性が存在します。
各脆弱性の詳細は、Treck 社が提供する情報や、脆弱性の報告者 JSOF が提供している情報 (Ripple20) を参照してください。

また、図研エルミックが提供する KASAGO は Treck 社の IP スタックと同じ起源の製品であり、同様の脆弱性が存在します。詳しくは図研エルミックが提供する情報 (KASAGO製品における脆弱性に関するお知らせ) を参照してください。

想定される影響

想定される影響は、該当製品の機能・構成や各脆弱性により異なりますが、遠隔の第三者によって以下のような攻撃を受ける可能性があります。

- サービス運用妨害 (DoS)
- 情報漏えい
- 任意のコード実行

対策方法
製品開発者向けの対策方法
使用する IP スタックを、開発者が提供する情報をもとに最新版にアップデートしてください。

https://jvn.jp/vu/JVNVU94736763/

まとめ：案件3）Treck 製 IP スタックに複数の脆弱性

- **CVE番号**
  CVE-2020-11896
- **脆弱性の種類**
  受信した細工されたパケットに対する処理の問題
- **攻撃のシナリオ**
  遠隔の**第三者**が細工したパケットを送付することで管理者権限で任意のコードを実行可能
- **想定される影響**
  結果として、当該製品に対して**復旧にハードリセットが必要**なDoS 攻撃がおこなわれる可能性がある。
  今回は**停止または遅延**を影響として評価する
- **補足情報**
  攻撃者がパケットを送り付けるだけでいいので、**被害ユーザのアクションはない。**
  IPv4 tunneling を有効にしていることが必要だが、攻撃の難易度は CVSS v3 の評価に影響しない

回答シート：案件3）Treck 製 IP スタックに複数の脆弱性

CVSS v3　CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?　**基本値: ?.?** ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

案件3）Treck 製 IP スタックに複数の脆弱性

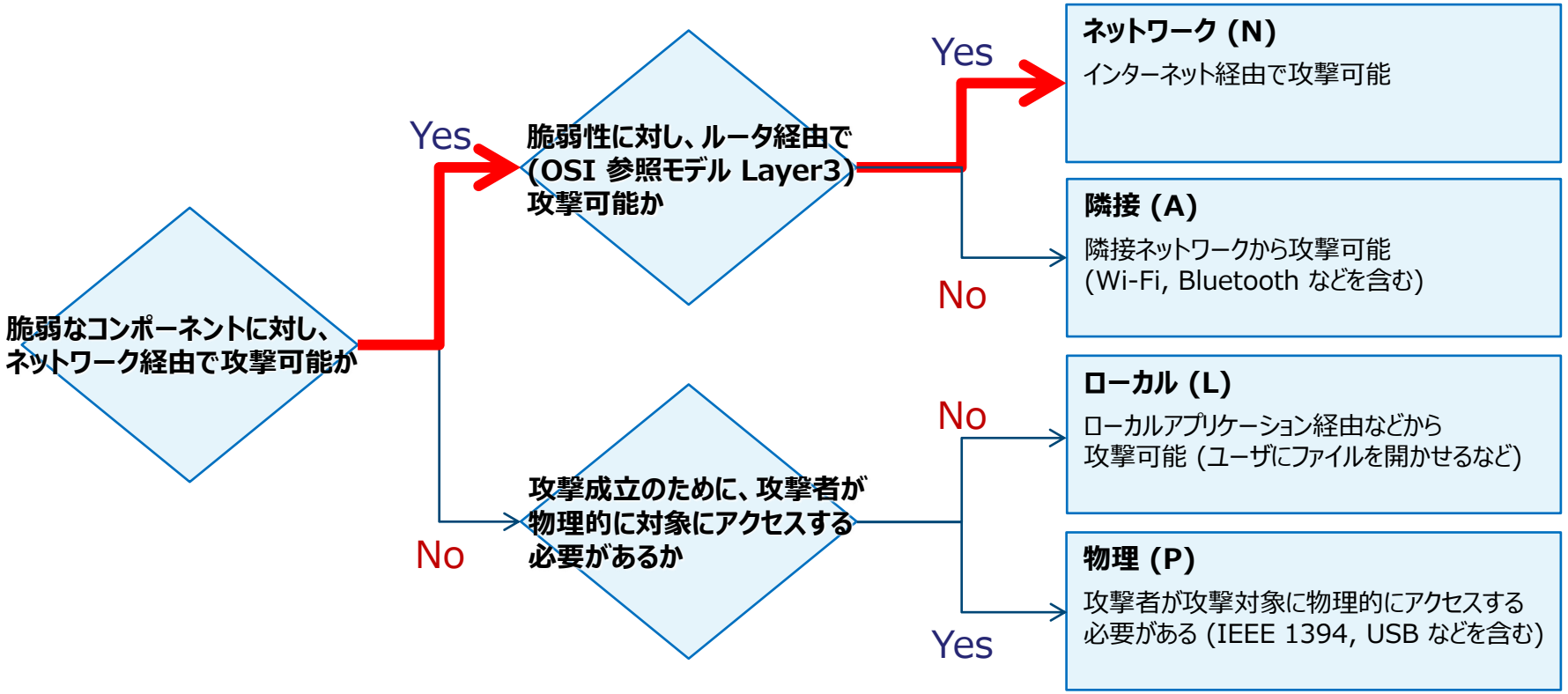
CVSS v3　CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H　**基本値: 10.0** ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	**ネットワーク (N)**
攻撃条件の複雑さ(AC)	高 (H)	**低 (L)**		
必要な特権レベル(PR)	高 (H)	低 (L)	**不要 (N)**	
ユーザ関与レベル(UI)	要 (R)	**不要 (N)**		
スコープ(S)	変更なし (U)	**変更あり (C)**		
機密性への影響(C)	なし (N)	低 (L)	**高 (H)**	
完全性への影響(I)	なし (N)	低 (L)	**高 (H)**	
可用性への影響(A)	なし (N)	低 (L)	**高 (H)**	

Attack Vector (AV) … 攻撃元区分

- システムを、どこから攻撃可能であるかを評価

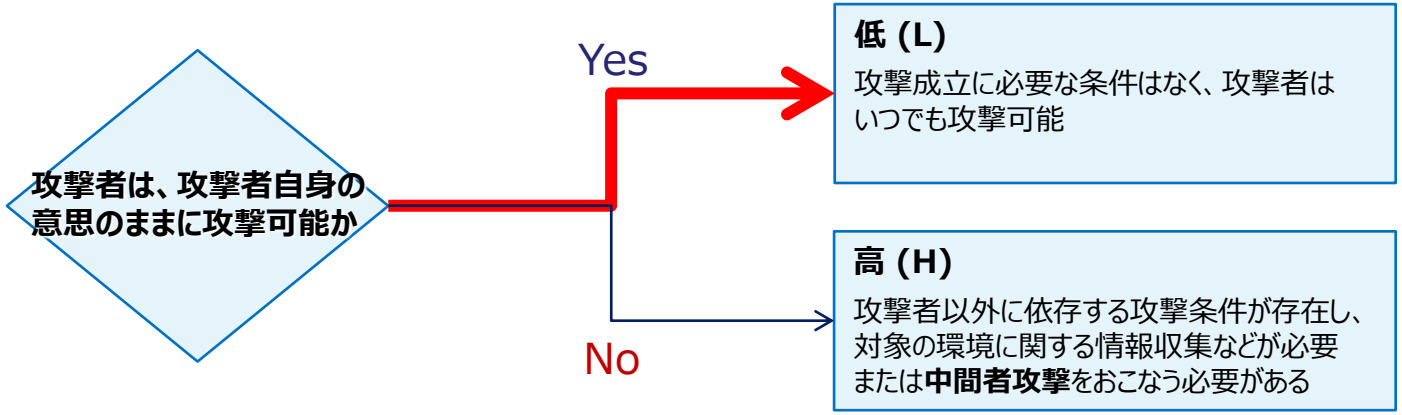
TCP/IP スタックの脆弱性であり、
ネットワーク経由で攻撃を受ける



Attack Complexity (AC) … 攻撃条件の複雑さ

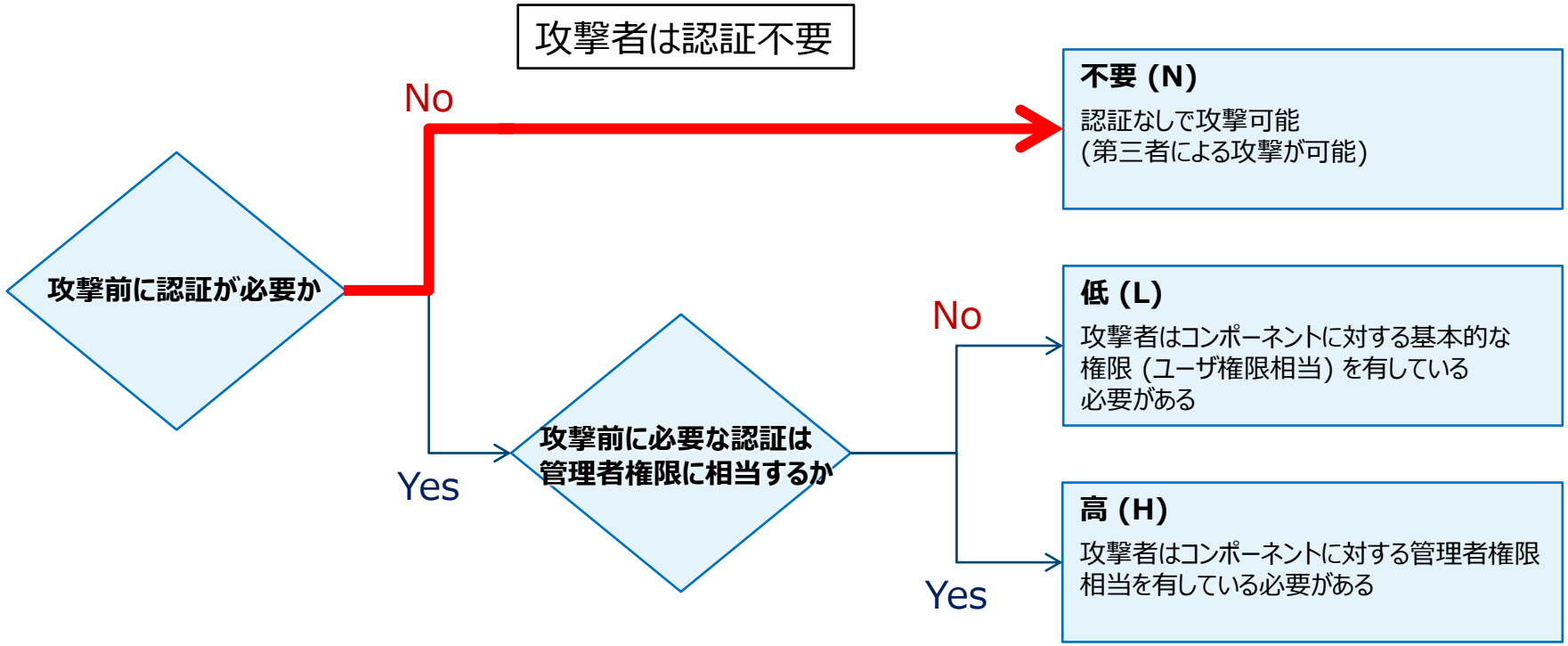
- 攻撃に必要な条件がどのようなものであるのかを評価

IPv4 tunneling を有効にしている必要があるが、
攻撃に特別な条件はない



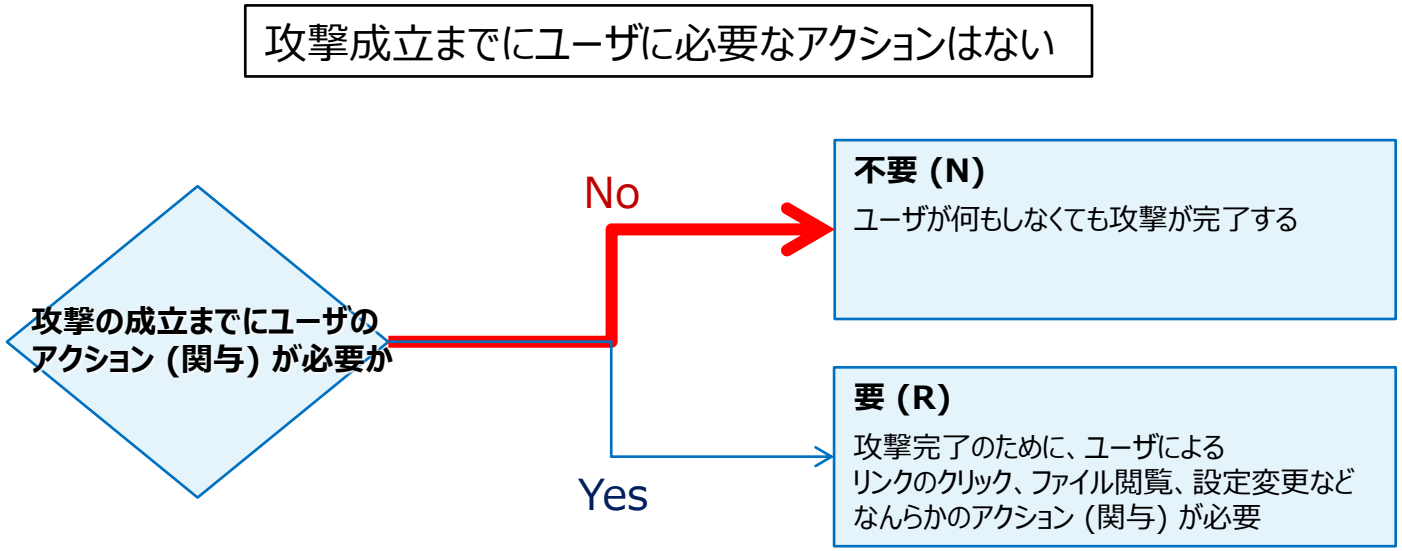
Privileges Required (PR) … 必要な特権レベル

- 攻撃に必要な認証レベルを評価



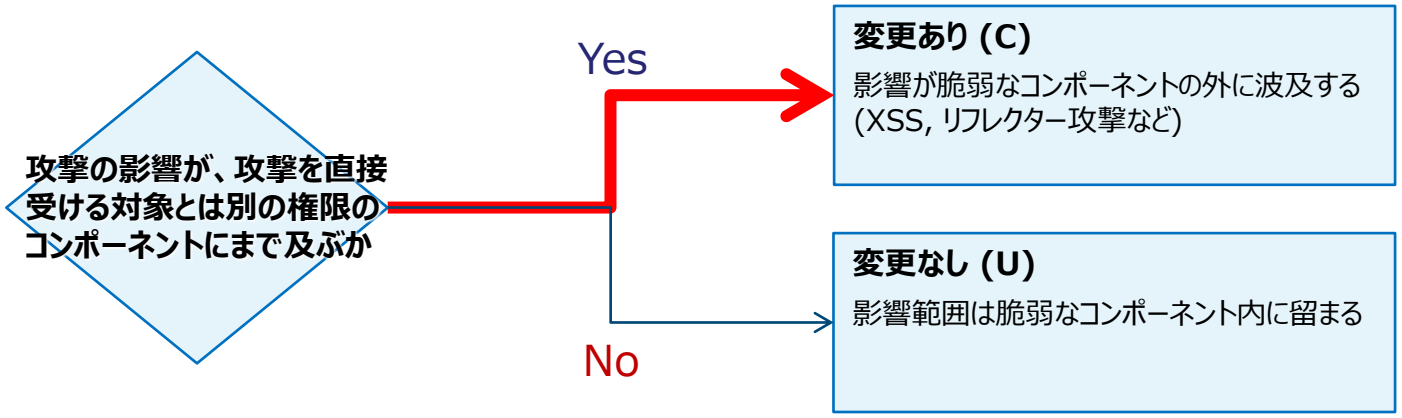
User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価



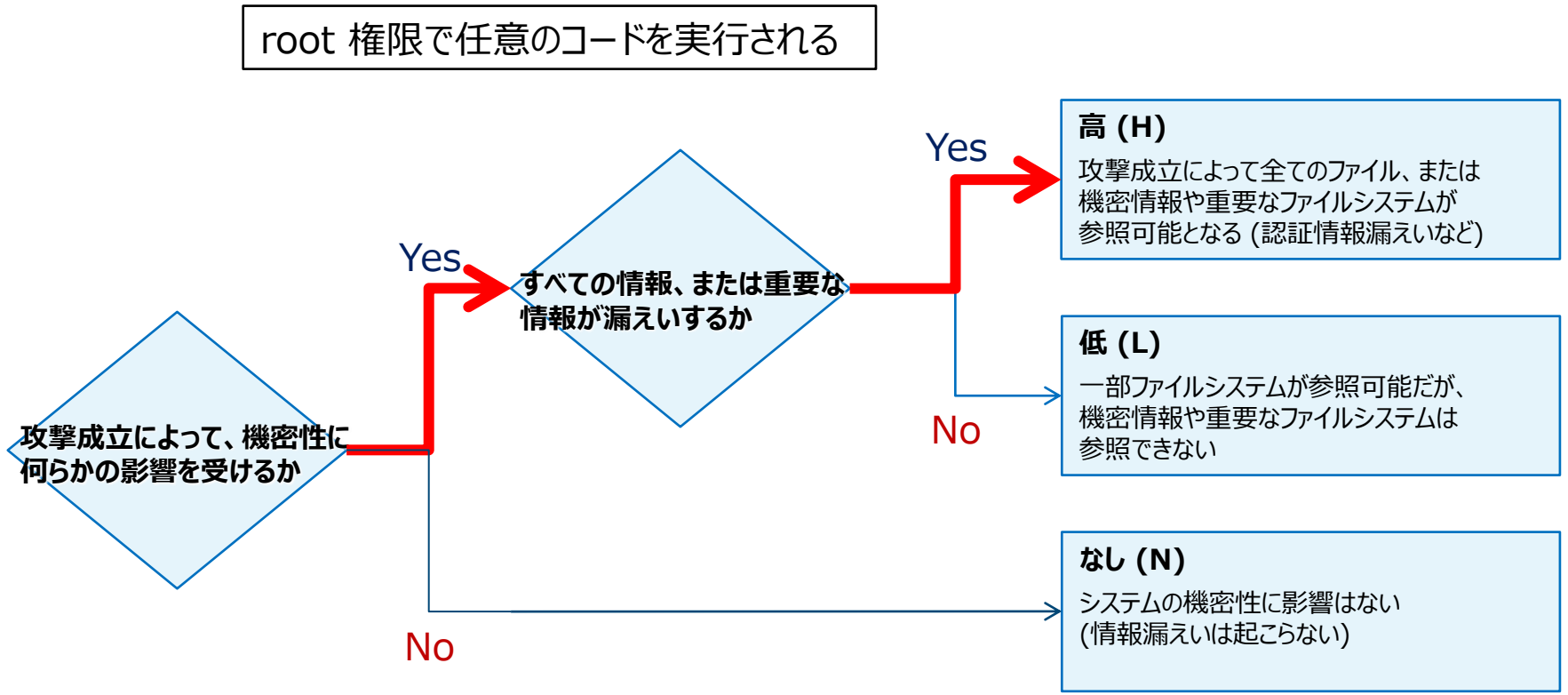
Scope (S) … スコープ - 被害の影響範囲を評価

脆弱な製品 (Treck 製 IP スタック) だけでなく
組み込んでいる製品も影響を受ける



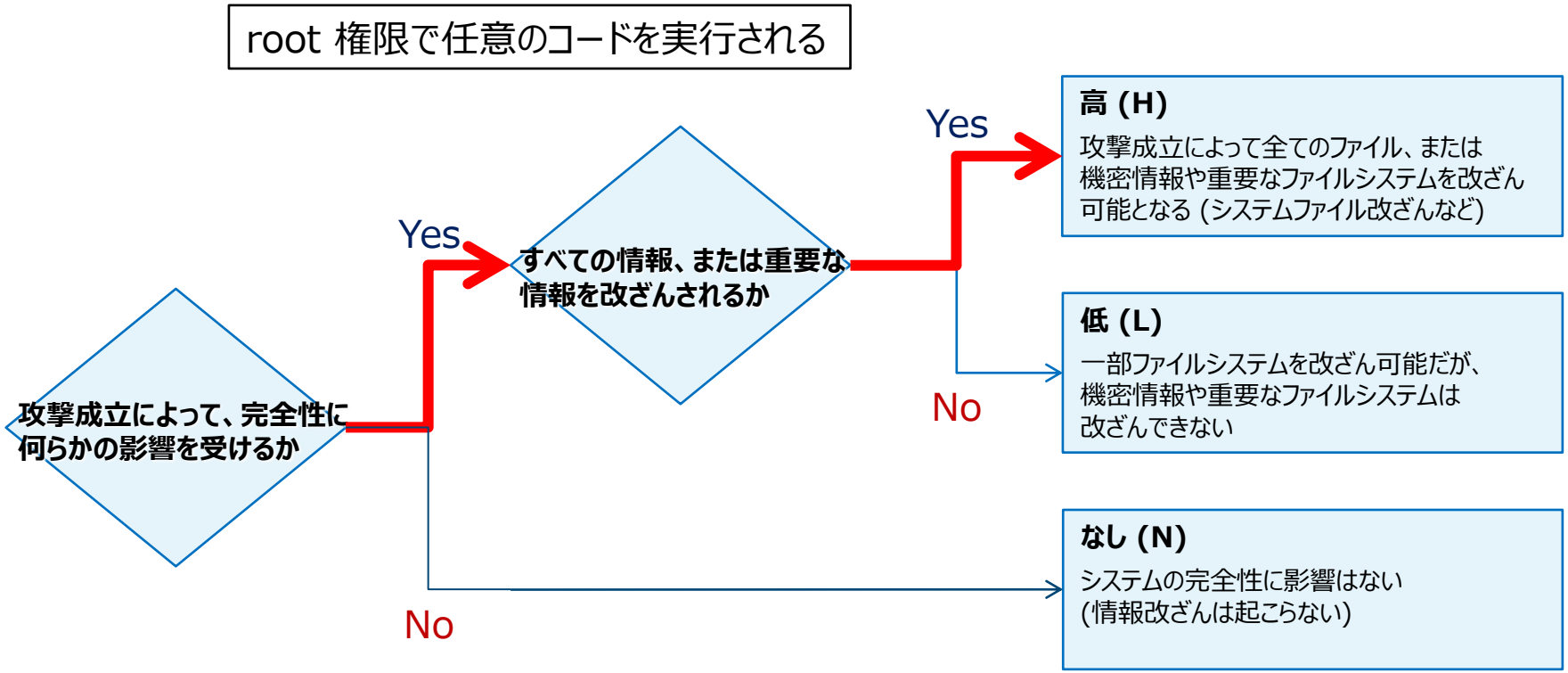
Confidentiality Impact (C) … 機密性への影響

- 攻撃された際に機密性に影響があるかを評価



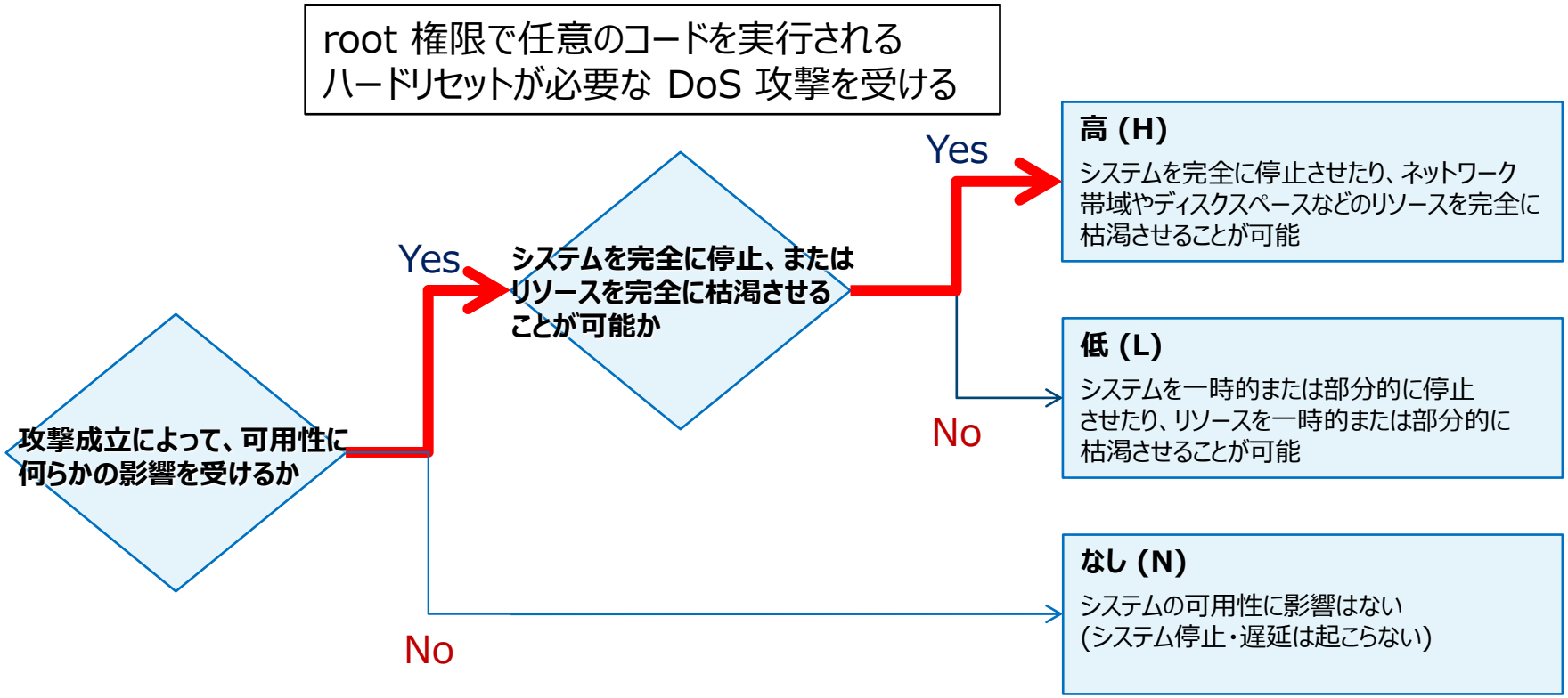
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



解説：案件3）Treck 製 IP スタックに複数の脆弱性

評価項目	評価値	説明
攻撃元区分 (AV)	ネットワーク (N)	TCP/IP スタックの脆弱性であり、ネットワーク経由で攻撃を受ける
攻撃条件の複雑さ (AC)	低 (L)	IPv4 tunneling を有効にしている必要があるが、攻撃に特別な条件はない
必要な特権レベル (PR)	不要 (N)	攻撃者による認証は不要
ユーザ関与レベル (UI)	不要 (N)	攻撃成立までにユーザに必要なアクションはない
スコープ (S)	変更あり (C)	脆弱な製品 (Treck 製 IP スタック) だけでなく組み込んでいる製品も影響を受ける
機密性への影響 (C)	高 (H)	root 権限で任意のコードを実行される
完全性への影響 (I)	高 (H)	root 権限で任意のコードを実行される
可用性への影響 (A)	高 (H)	root 権限で任意のコードを実行される。ハードリセットが必要な DoS 攻撃を受ける

概要：案件4）H2O に開放済みメモリ使用 (use-after-free)

公開日：2016/05/27　最終更新日：2016/05/27

JVN#87859762
H2O における解放済みメモリ使用 (use-after-free) の脆弱性

概要
H2O には、解放済みメモリ使用 (use-after-free) の脆弱性が存在します。

影響を受けるシステム

- H2O バージョン 1.7.2 およびそれ以前

詳細情報
H2O は、オープンソースのウェブサーバソフトウェアです。H2O には、解放済みメモリ使用 (use-after-free) の脆弱性が存在します。

想定される影響
細工されたパケットを受信することで、サービス運用妨害 (DoS) 攻撃を受ける可能性があります。

対策方法
アップデートする
開発者が提供する情報をもとに最新版にアップデートしてください。

ベンダ情報

ベンダ	リンク
奥 一穂	fix use after free on premature connection close (CVE-2016-4817) #920

https://jvn.jp/jp/JVN87859762/

まとめ：案件4）H2O に開放済みメモリ使用 (use-after-free)

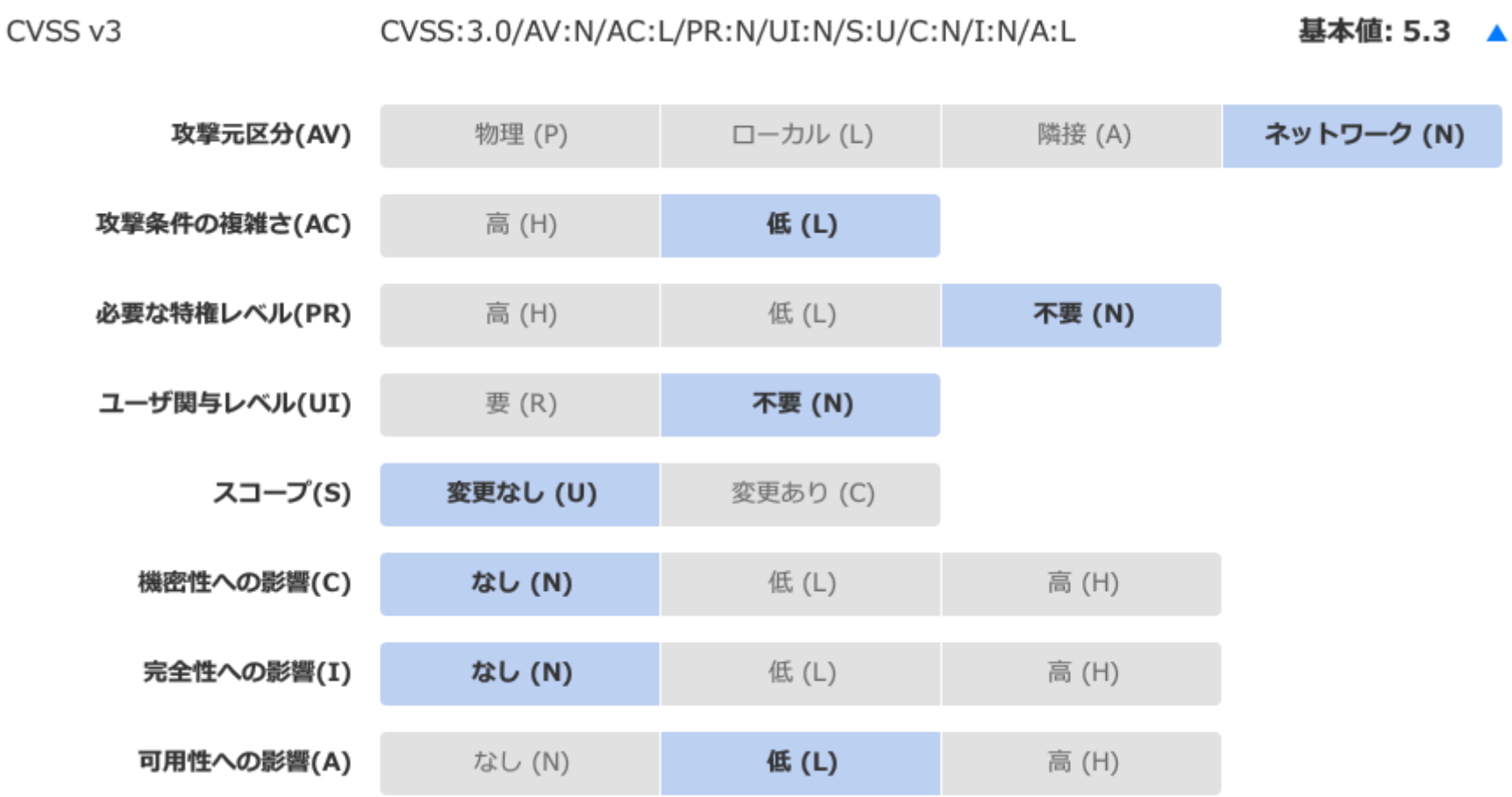
- **脆弱性の種類**
  開放済みメモリ使用 (use-after-free)
- **攻撃のシナリオ**
  遠隔の**第三者**が細工したパケットを送付することでサーバアプリ (H2O) に対するサービス運用妨害攻撃が可能
- **想定される影響**
  結果として、当該製品に対して DoS 攻撃がおこなわれる可能性がある。
  今回は**一時的な停止または遅延**を影響として評価する
- **補足情報**
  攻撃者がパケットを送り付けるだけでいいので、**被害ユーザのアクションはない**

回答シート：案件4）H2O に開放済みメモリ使用 (use-after-free)

CVSS v3　CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?　基本値: ?.? ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

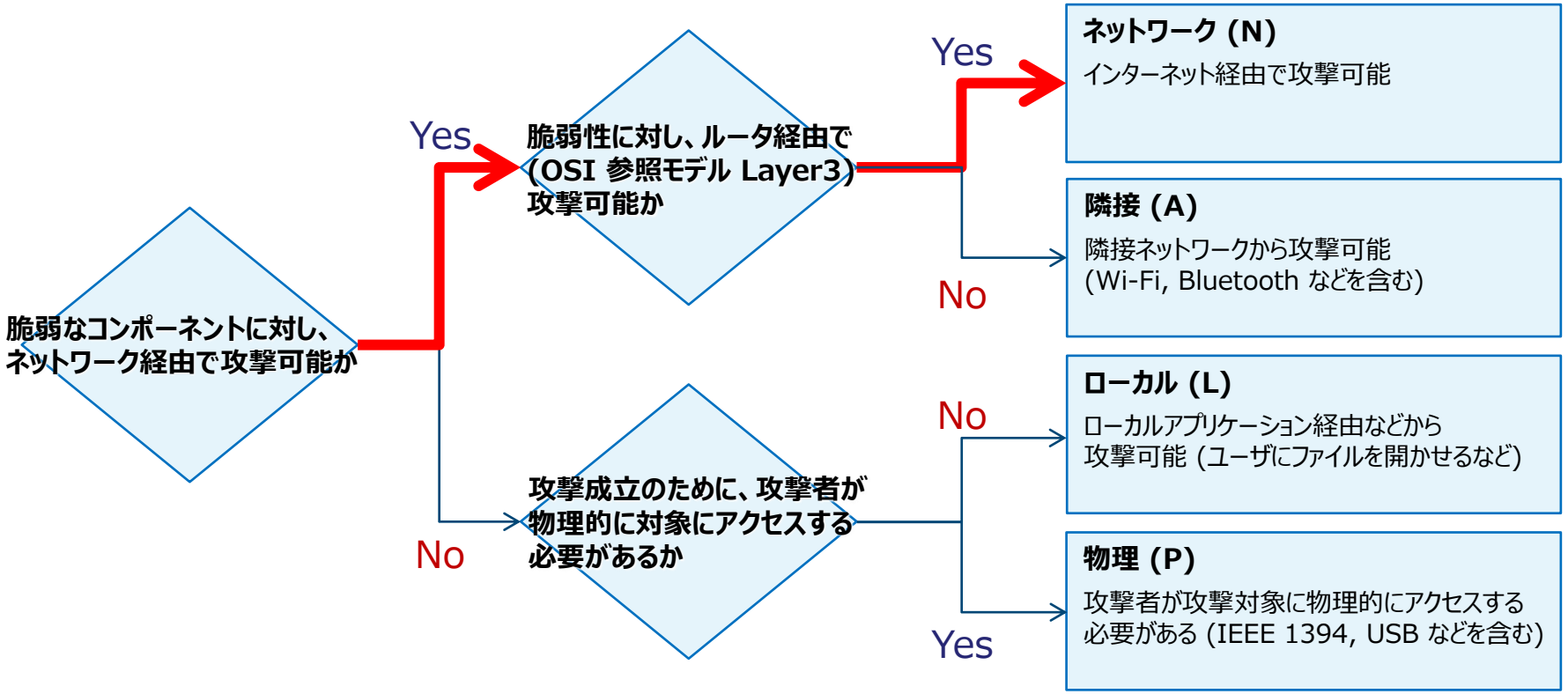
JVN掲載評価：案件4）H2O に開放済みメモリ使用 (use-after-free)



Attack Vector (AV) … 攻撃元区分

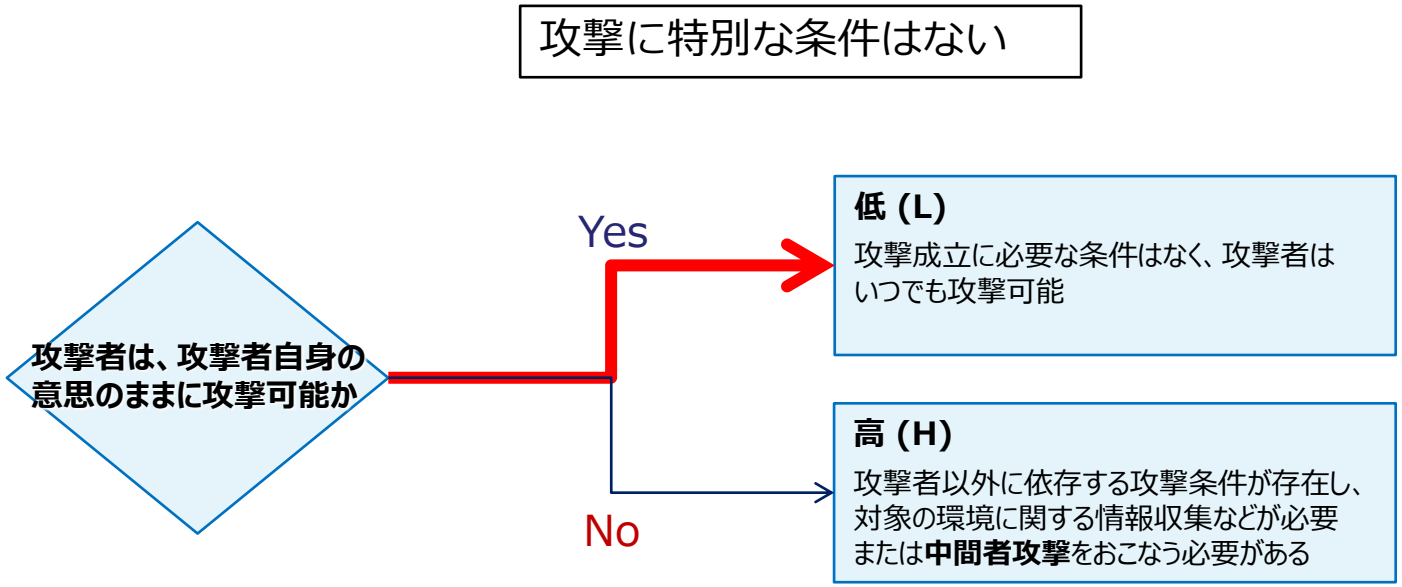
- システムを、どこから攻撃可能であるかを評価

ウェブアプリケーションの脆弱性であり、
ネットワーク経由で攻撃を受ける



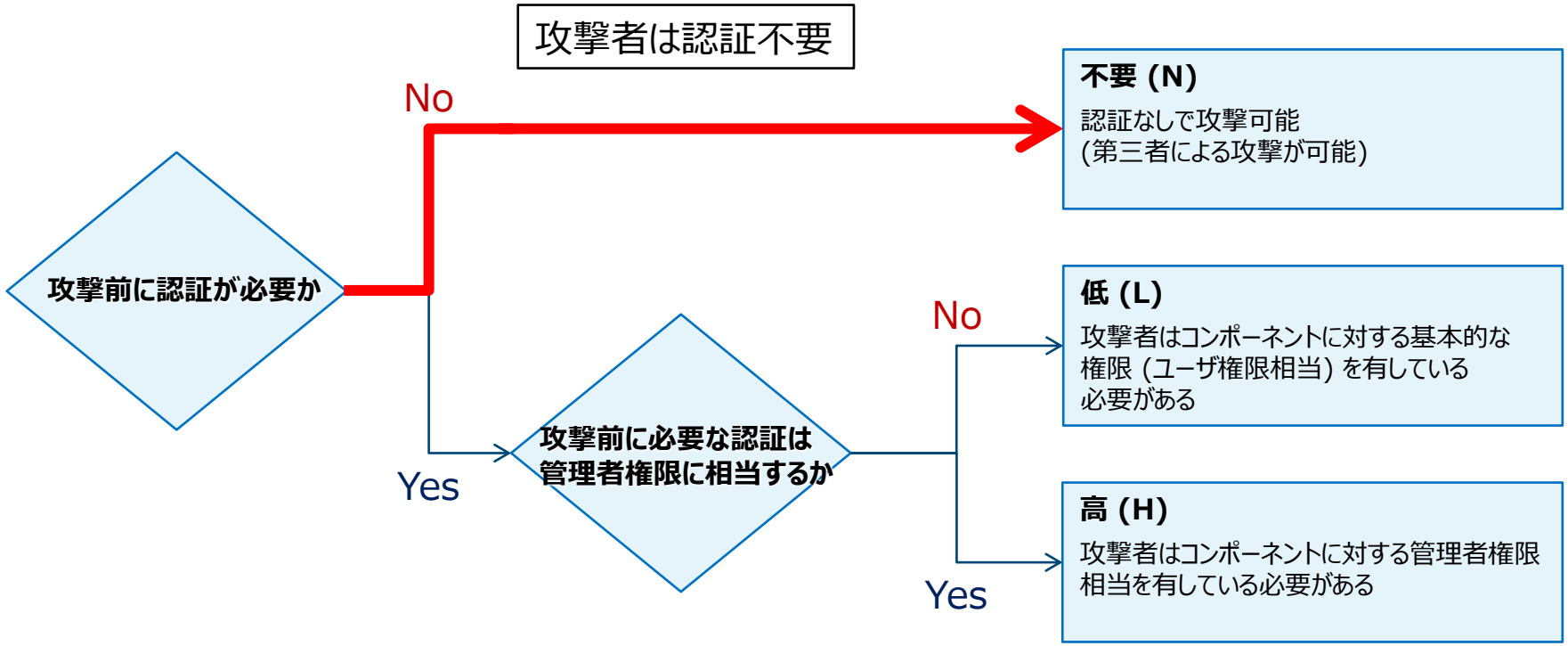
Attack Complexity (AC) … 攻撃条件の複雑さ

- 攻撃に必要な条件がどのようなものであるのかを評価



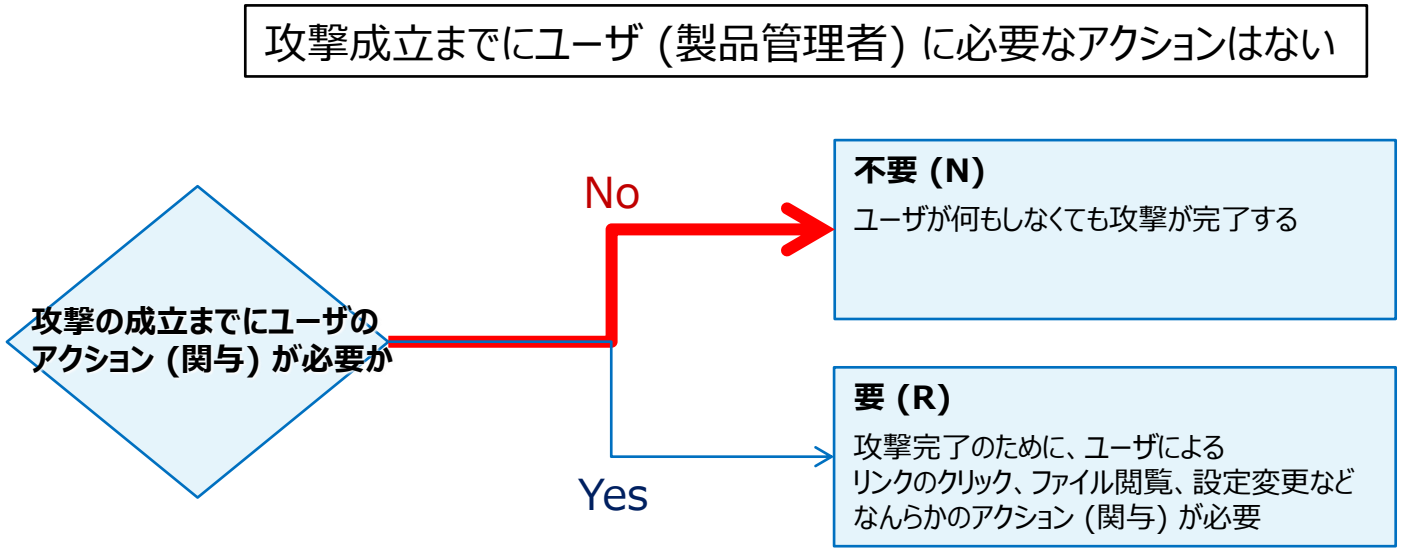
Privileges Required (PR) … 必要な特権レベル

- 攻撃に必要な認証レベルを評価

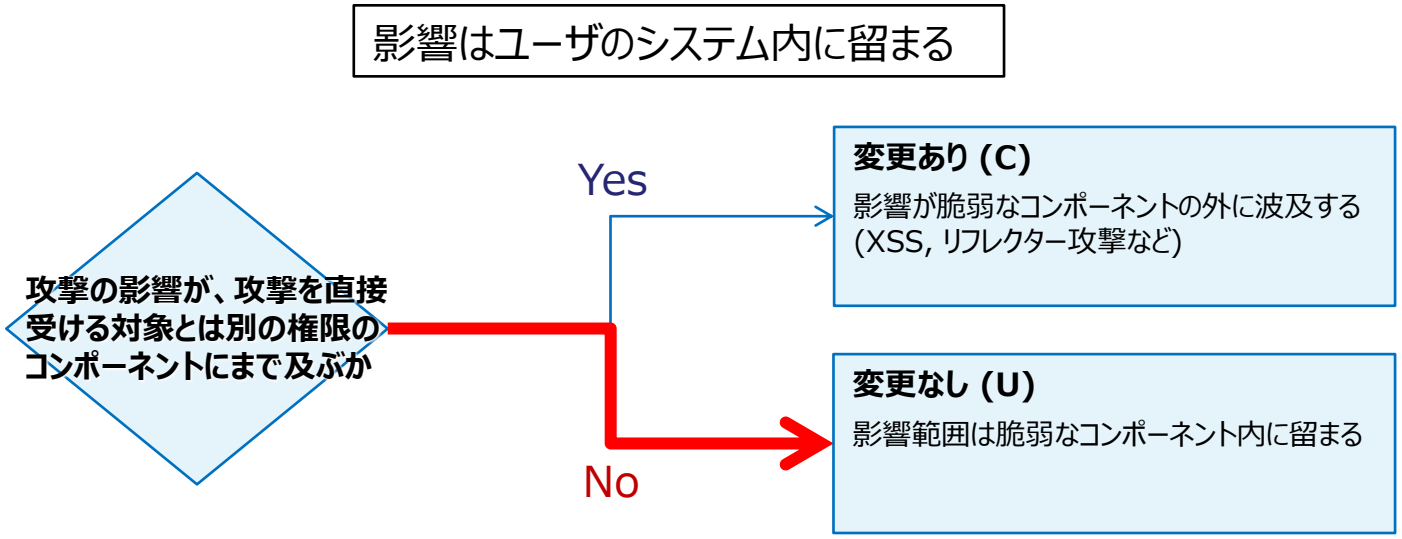


User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価

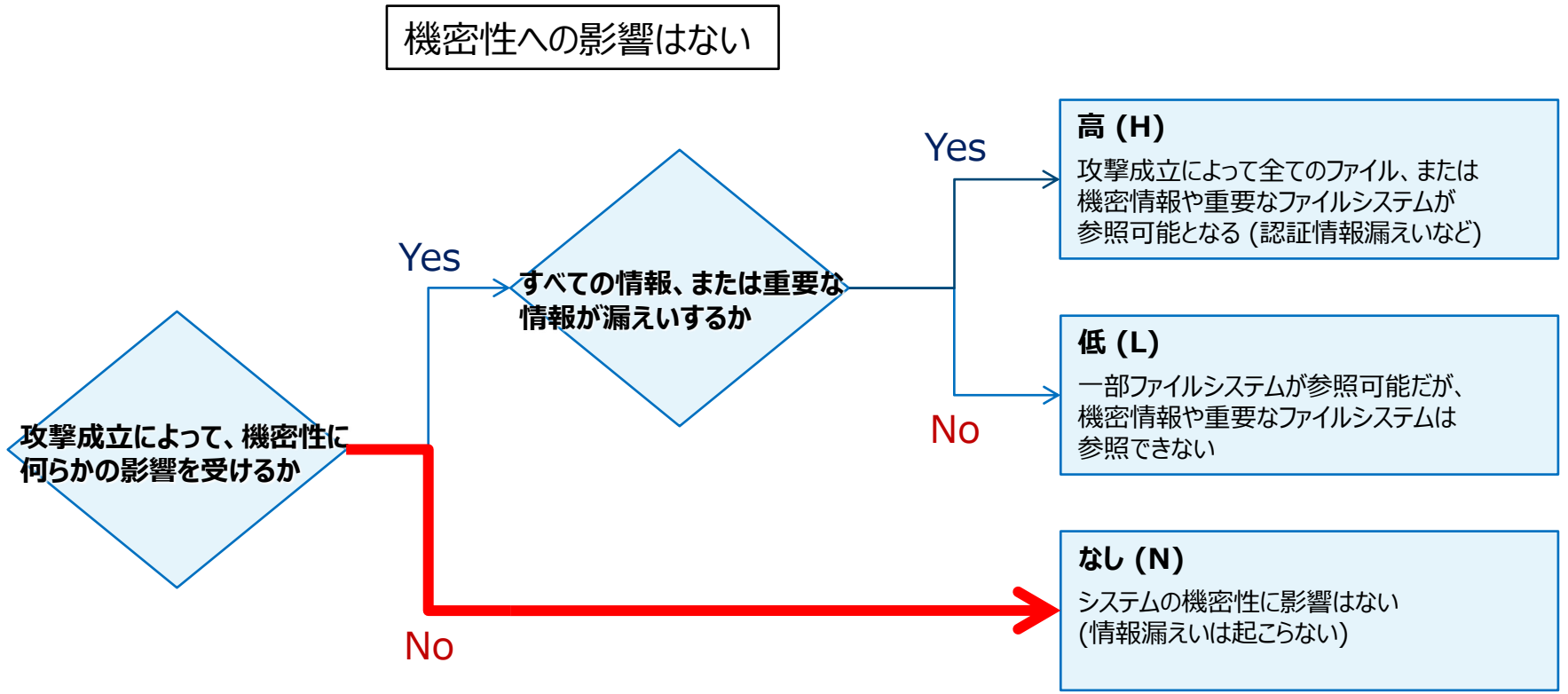


Scope (S) … スコープ - 被害の影響範囲を評価



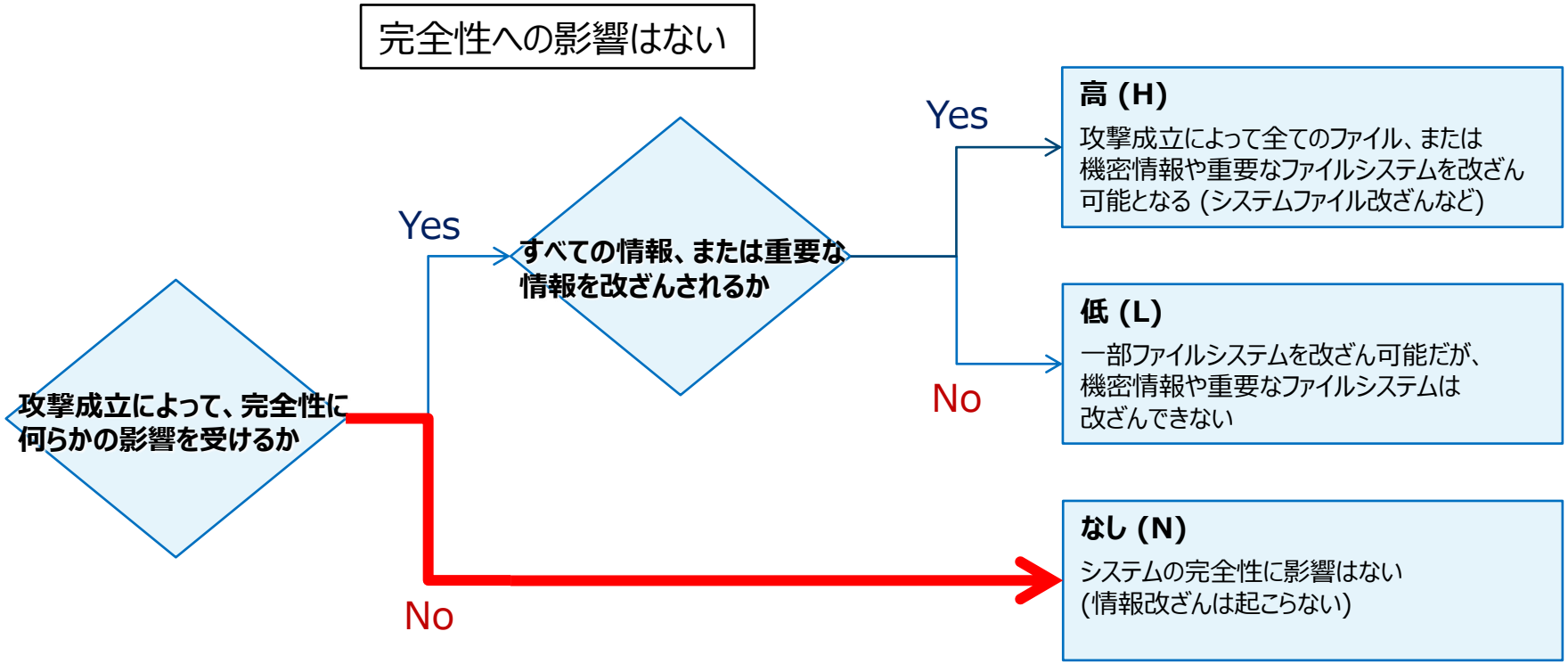
Confidentiality Impact (C) … 機密性への影響

- 攻撃された際に機密性に影響があるかを評価



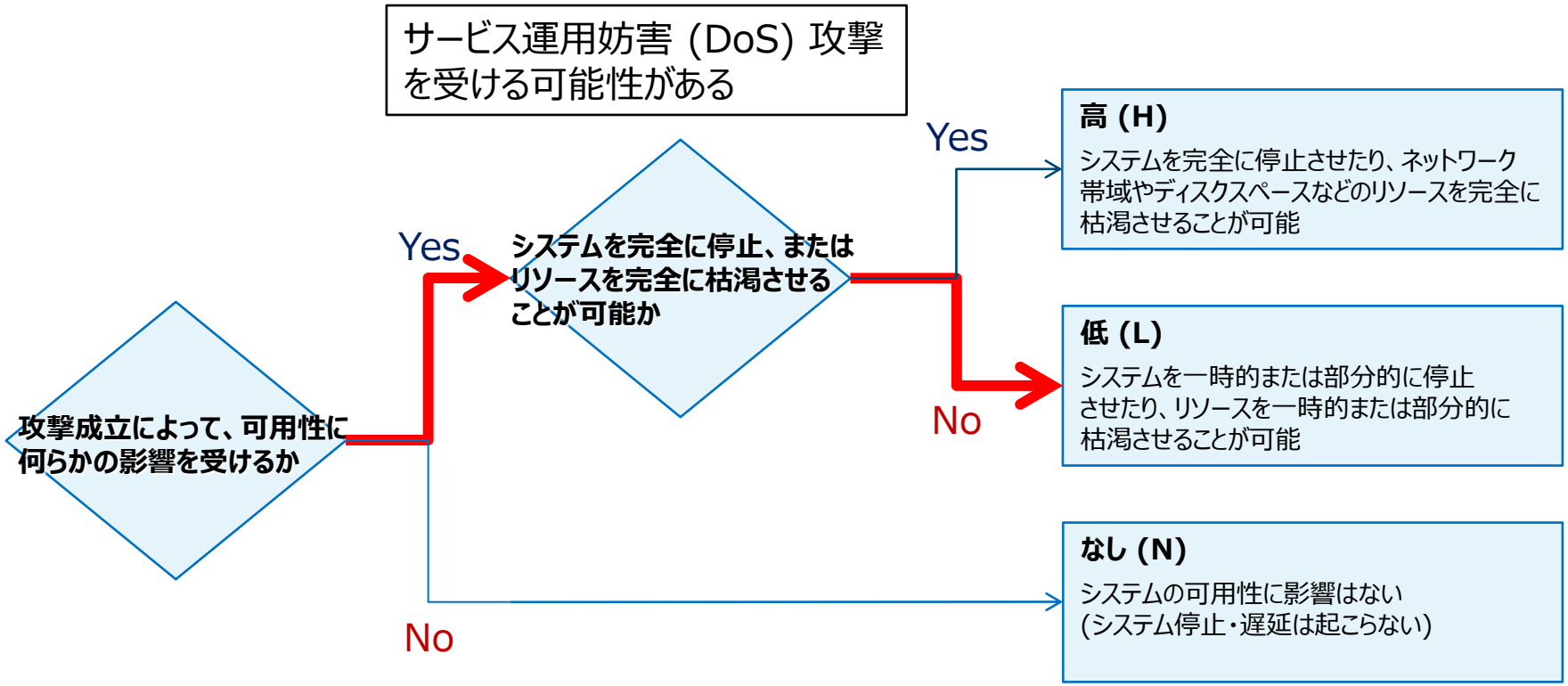
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



解説：案件4）H2O に開放済みメモリ使用 (use-after-free)

評価項目	評価値	説明
攻撃元区分 (AV)	ネットワーク (N)	ウェブアプリケーションの脆弱性であり、ネットワーク経由で攻撃を受ける
攻撃条件の複雑さ (AC)	低 (L)	攻撃に特別な条件はない
必要な特権レベル (PR)	不要 (N)	攻撃者による認証は不要
ユーザ関与レベル (UI)	不要 (N)	攻撃成立までにユーザ (製品管理者) に必要なアクションはない
スコープ (S)	変更なし (U)	影響はユーザのシステム内に留まる
機密性への影響 (C)	なし (N)	機密性への影響はない
完全性への影響 (I)	なし (N)	完全性への影響はない
可用性への影響 (A)	低 (L)	サービス運用妨害 (DoS) 攻撃を受ける可能性がある

概要：案件5）CG-WLR300GNV シリーズの PIN 認証試行回数が制限されていない問題

公開日：2016/06/22　最終更新日：2016/06/22

JVN#75028871
CG-WLR300GNV シリーズにおいて認証試行回数が制限されていない脆弱性

概要
CG-WLR300GNV シリーズには、認証試行回数が制限されていない脆弱性が存在します。

影響を受けるシステム

- CG-WLR300GNV
- CG-WLR300GNV-W

詳細情報
株式会社コレガが提供する CG-WLR300GNV および CG-WLR300GNV-W は、無線 LAN ルータです。CG-WLR300GNV および CG-WLR300GNV-W の WPS 機能では、PIN 認証の試行回数が制限されていないため、ブルートフォース攻撃を受ける可能性があります。

想定される影響
該当機器の無線 LAN 到達範囲にいる第三者によって、PIN 認証に対するブルートフォース攻撃を実行される可能性があります。結果として、PIN が解読され、当該機器が提供するネットワークにアクセスされる可能性があります。

対策方法
ワークアラウンドを実施する
本脆弱性の影響を回避するため、次のワークアラウンドを実施してください。

- WPS 機能を無効にする

https://jvn.jp/jp/JVN75028871/

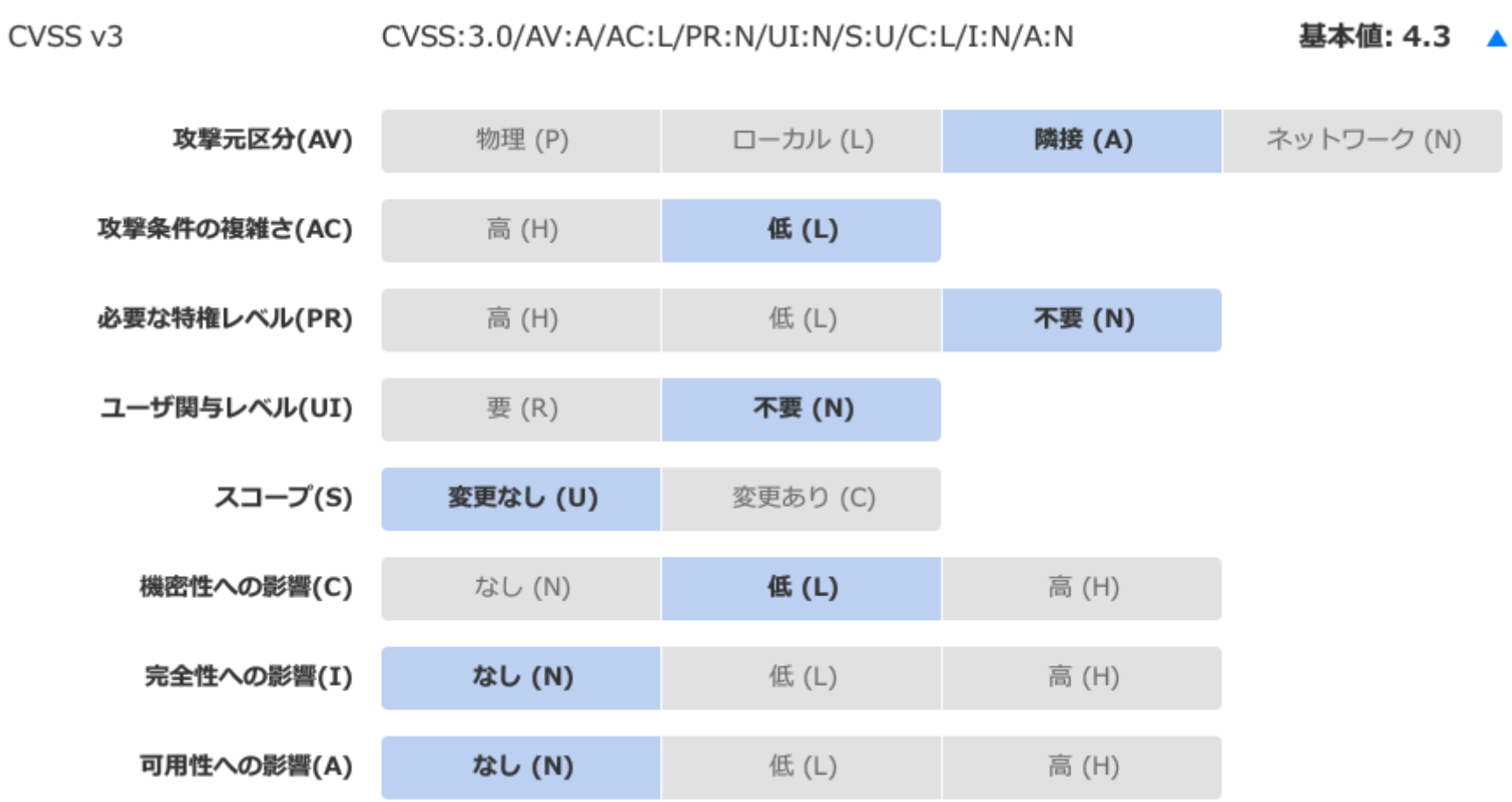
まとめ：案件5）CG-WLR300GNV シリーズの PIN 認証試行回数が制限されていない問題

- **脆弱性の種類**
  WPS 機能の PIN 認証試行回数が無制限
- **攻撃のシナリオ**
  PIN を知らない**第三者**が当該**ルータの無線到達範囲内**から当該ルータの WPS 機能の PIN (暗証番号) を総当たりし、ルータの持つネットワーク内にアクセスされる
- **想定される影響**
  PIN を解読された結果として、当該ルータの LAN 内のサービスを使用されたり、当該製品を経由してネットワークを使用されたりする可能性がある。
- **補足情報**
  影響の評価は一次被害のみを考慮するので、ここでは**PIN が解読される**点のみを問題として評価する

回答シート：案件5）CG-WLR300GNV シリーズの PIN 認証試行回数が制限されていない問題

CVSS v3	CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?			基本値: ?.? ▲
攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

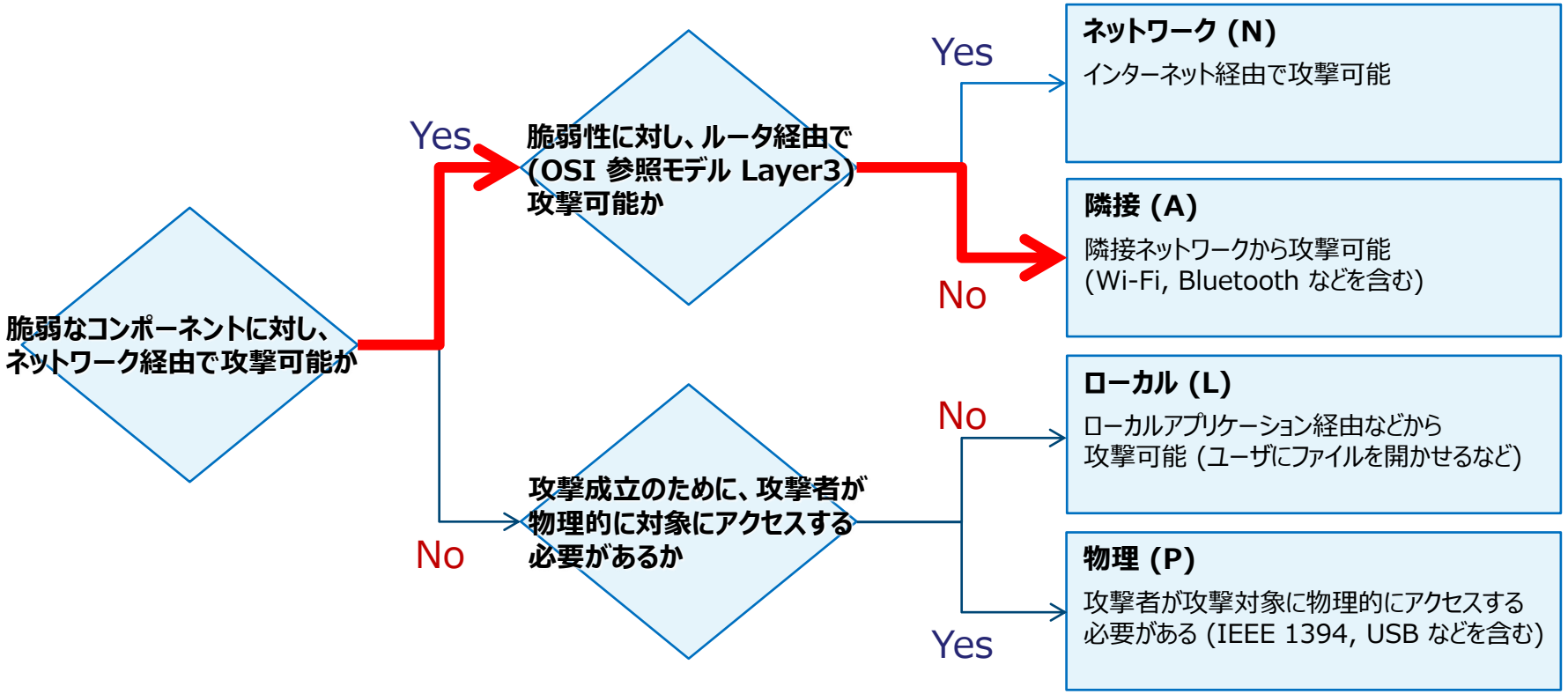
JVN掲載評価：案件5）CG-WLR300GNV シリーズの PIN 認証試行回数が制限されていない問題



Attack Vector (AV) … 攻撃元区分

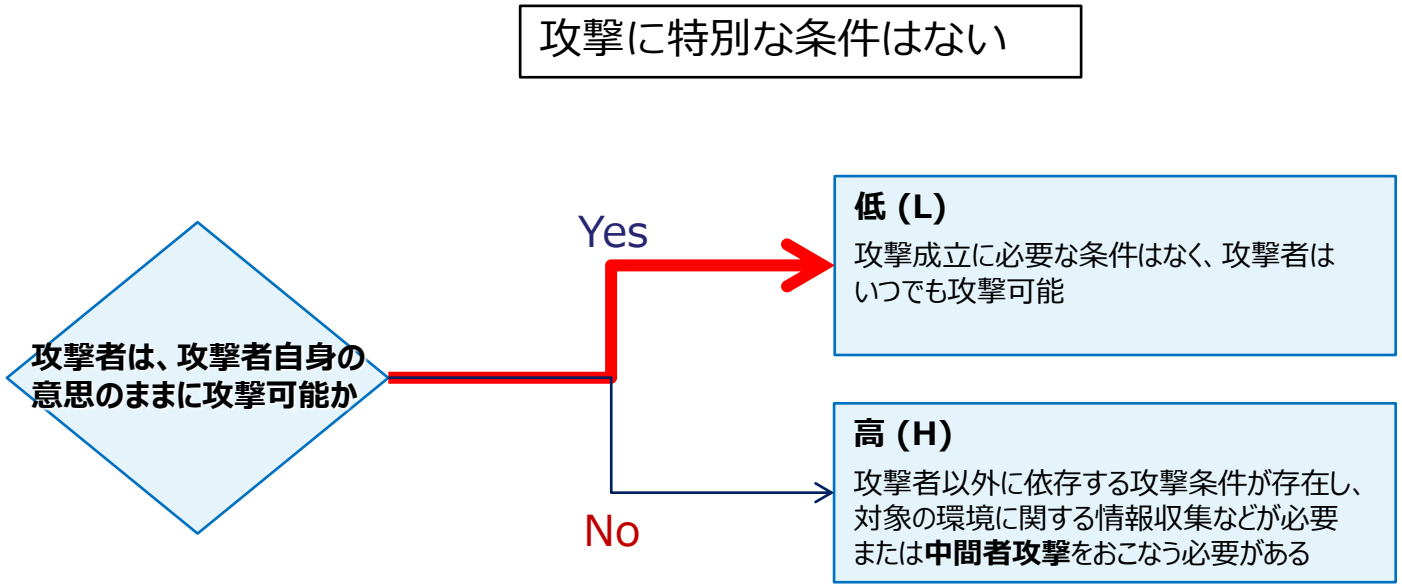
- システムを、どこから攻撃可能であるかを評価

ルータの WPS 範囲内 (無線範囲内) から
攻撃する必要がある



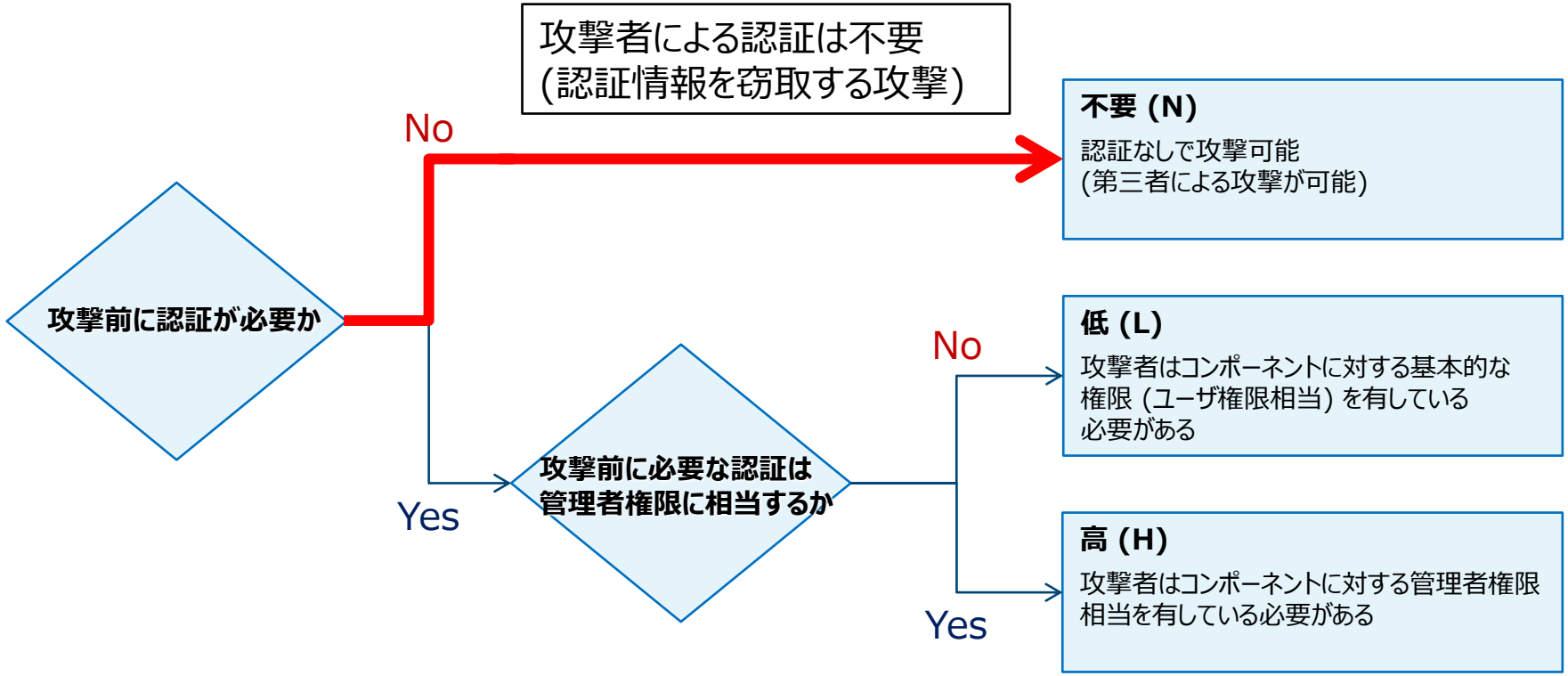
Attack Complexity (AC) … 攻撃条件の複雑さ

- 攻撃に必要な条件がどのようなものであるのかを評価



Privileges Required (PR) … 必要な特権レベル

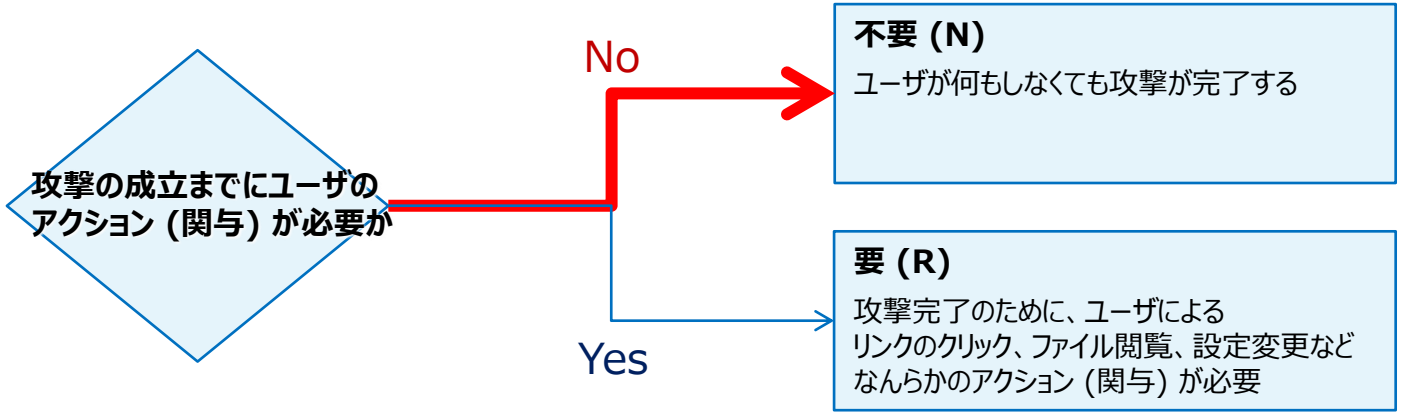
- 攻撃に必要な認証レベルを評価



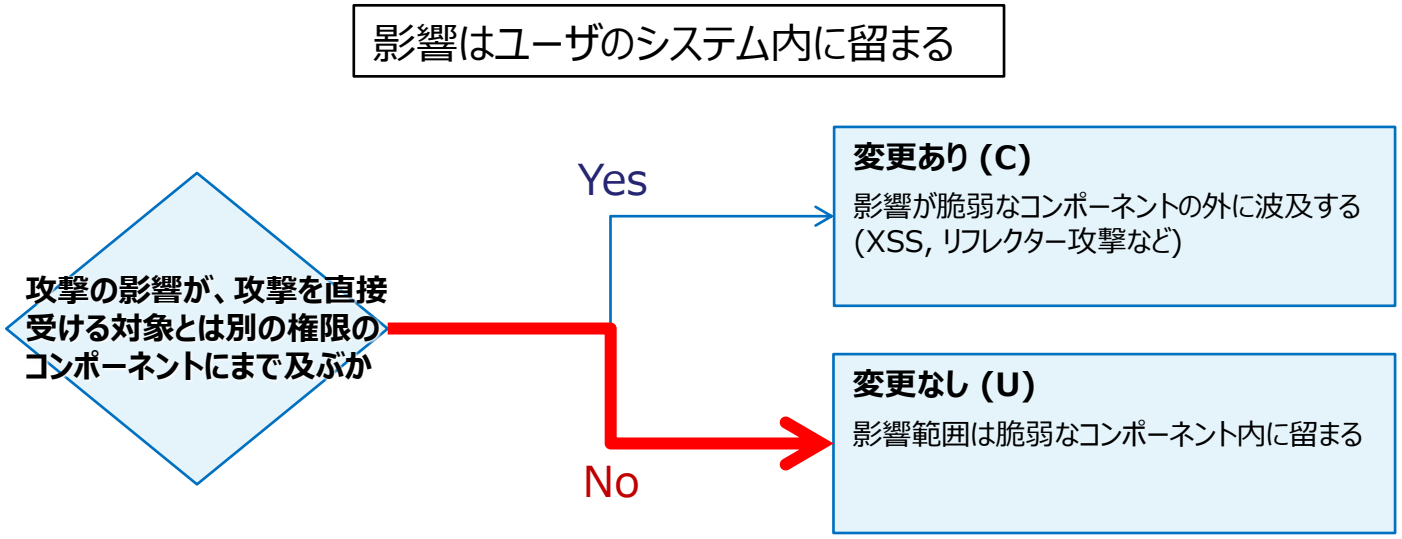
User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価

攻撃成立までにユーザ (製品管理者) に必要なアクションはない



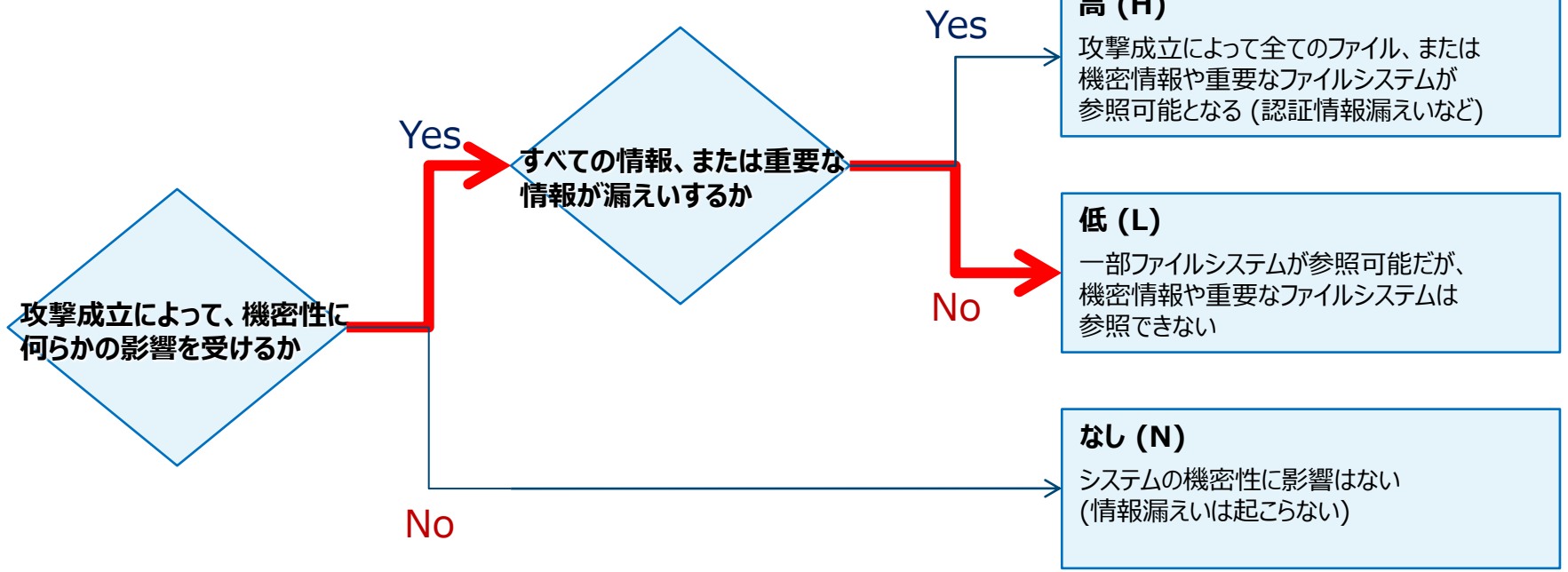
Scope (S) … スコープ - 被害の影響範囲を評価



Confidentiality Impact (C) … 機密性への影響

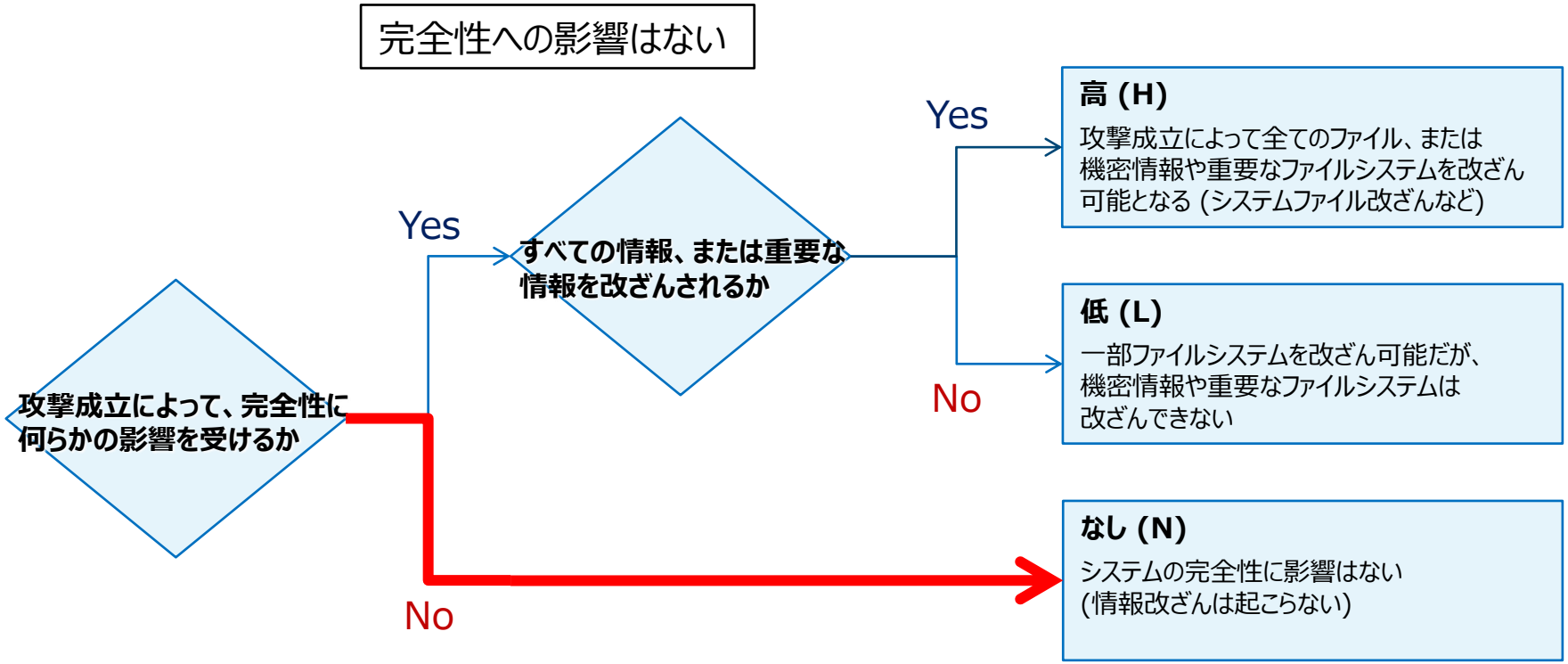
- 攻撃された際に機密性に影響があるかを評価

LAN にアクセスするための PIN (暗証番号) を解読される。
機密情報や重要なファイルシステムの漏えいはない



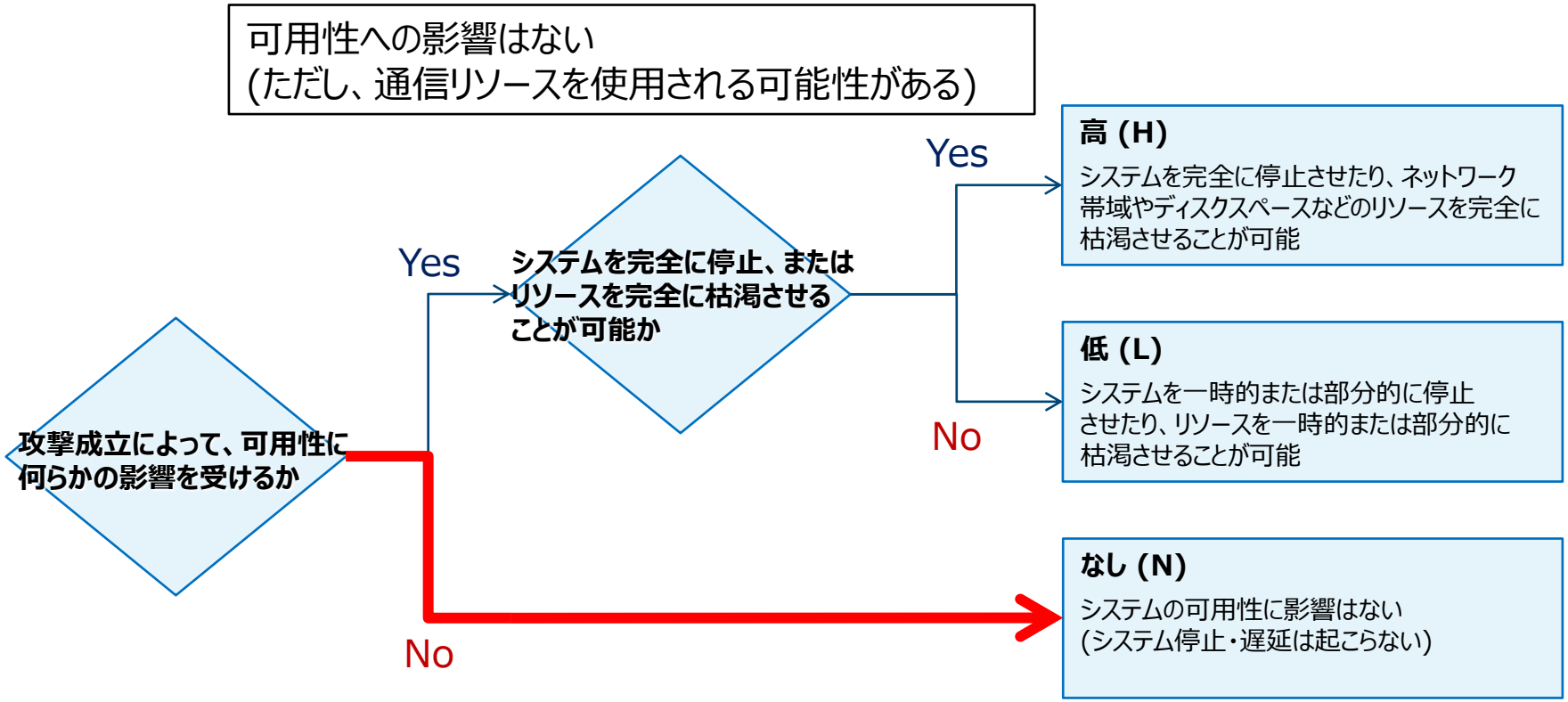
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



解説：案件5）CG-WLR300GNV シリーズの PIN 認証試行回数が制限されていない問題

評価項目	評価値	説明
攻撃元区分 (AV)	隣接 (A)	ルータの WPS 範囲内 (無線範囲内) から攻撃する必要がある
攻撃条件の複雑さ (AC)	低 (L)	攻撃に特別な条件はない
必要な特権レベル (PR)	不要 (N)	攻撃者による認証は不要 (認証情報を窃取する攻撃)
ユーザ関与レベル (UI)	不要 (N)	攻撃成立までにユーザ (製品管理者) に必要なアクションはない
スコープ (S)	変更なし (U)	影響はユーザのシステム内に留まる
機密性への影響 (C)	低 (L)	LAN にアクセスするための PIN (暗証番号) を解読される。 機密情報や重要なファイルシステムの漏えいはない
完全性への影響 (I)	なし (N)	完全性への影響はない
可用性への影響 (A)	なし (N)	可用性への影響はない (ただし、通信リソースを使用される可能性がある)

概要：案件6）Allround Automations PL/SQL Developer が HTTP 経由でアップデートする問題

公開日：2016/04/26　最終更新日：2016/04/26

JVNVU#95625579
Allround Automations PL/SQL Developer が HTTP 経由でアップデートする問題

概要
Allround Automations PL/SQL Developer は、アップデートの確認を HTTP 経由で行っており、また、コマンド実行前にアップデートの内容を検証しません。そのため、攻撃者が任意のコードを実行する可能性があります。

影響を受けるシステム

- PL/SQL Developer version 11

詳細情報
データの信頼性の不十分な検証 (CWE-345) - CVE-2016-2346
報告者によると、Allround Automations PL/SQL Developer は、定期的に HTTP 経由でアップデートを確認します。アップデートが存在した場合、PL/SQL Developer はアップデートファイルをダウンロードし、ファイルの正当性やそのほかの確認を行わぬまま、アップデートを実行します。

中間者 (man-in-the-middle) 攻撃により、この通信に入りこんで必要なフィールドを変更することで、脆弱な機器に任意のデータを書き込み、PL/SQL Developer を実行しているユーザの権限で任意のコードを実行することが可能です。

想定される影響
中間者 (man-in-the-middle) 攻撃により、PL/SQL Developer を実行しているユーザの権限で任意のコードを実行される可能性があります。

対策方法
アップデートする
本脆弱性を修正した PL/SQL Developer version 11.0.6 がリリースされています。この更新により、アップデートの確認は HTTPS で行われ、アップデートのダウンロードは allroundautomations.com

https://jvn.jp/vu/JVNVU95625579/

まとめ：案件6）Allround Automations PL/SQL Developer が HTTP 経由でアップデートする問題

- **脆弱性の種類**
  ソフトウェアのアップデートの正当性を検査しない問題
- **攻撃のシナリオ**
  HTTP 経由で定期的におこなわれるアップデートチェックで
  検出されたアップデートの内容を検証せずに適用するため、
  中間者攻撃などで不正なプログラムを渡されると、
  ソフトウェアが悪意ある挙動をするように書き換えられる
- **想定される影響**
  結果として、**ソフトウェアの権限**で**任意の操作**を実行される
- **補足情報**
  任意の操作が実行可能なので、機密性・完全性・可用性
  すべてに影響を受けることになる

回答シート：案件6）Allround Automations PL/SQL Developer が HTTP 経由でアップデートする問題

CVSS v3　CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?　基本値: ?.? ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

JVN掲載評価：案件6）Allround Automations PL/SQL Developer が HTTP 経由でアップデートする問題

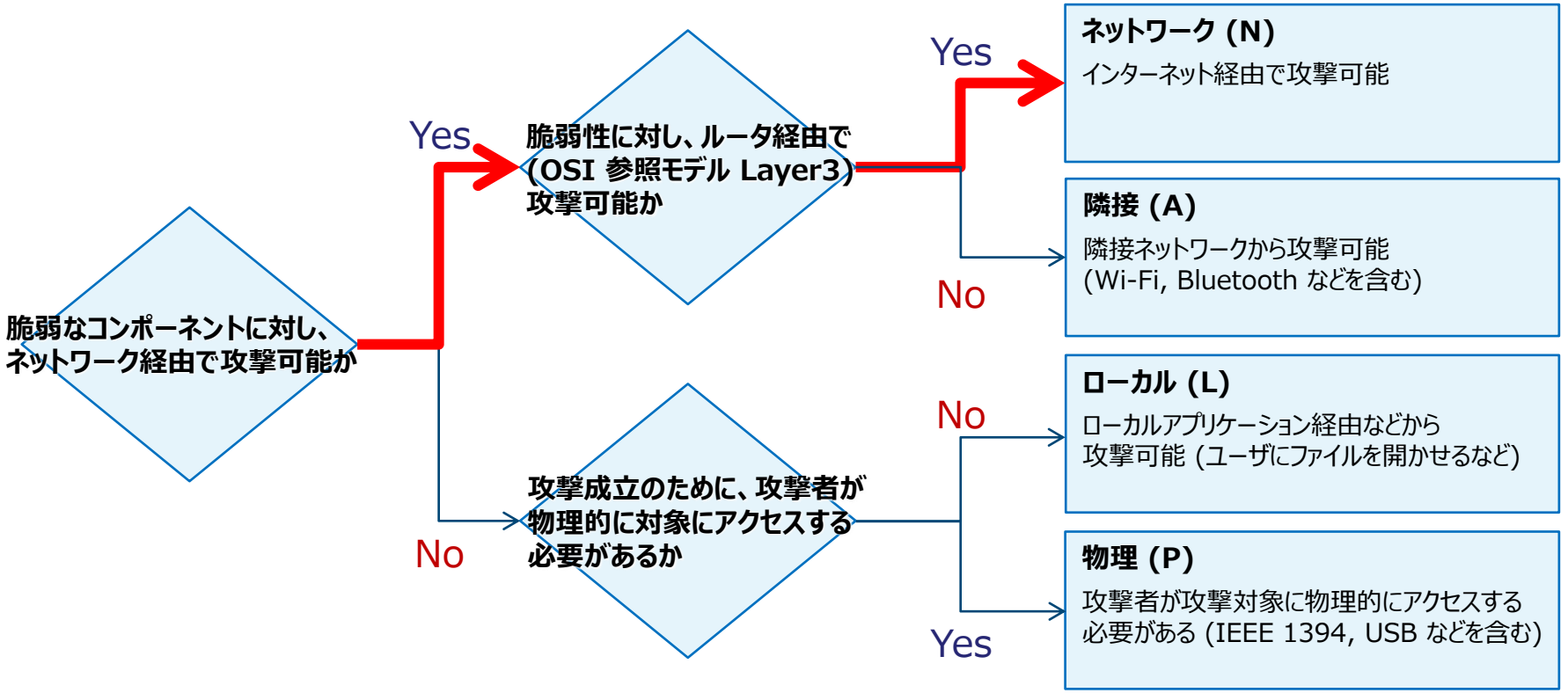
CVSS v3　CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L　**基本値: 5.6** ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	**ネットワーク (N)**
攻撃条件の複雑さ(AC)	**高 (H)**	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	**不要 (N)**	
ユーザ関与レベル(UI)	要 (R)	**不要 (N)**		
スコープ(S)	**変更なし (U)**	変更あり (C)		
機密性への影響(C)	なし (N)	**低 (L)**	高 (H)	
完全性への影響(I)	なし (N)	**低 (L)**	高 (H)	
可用性への影響(A)	なし (N)	**低 (L)**	高 (H)	

Attack Vector (AV) … 攻撃元区分

- システムを、どこから攻撃可能であるかを評価

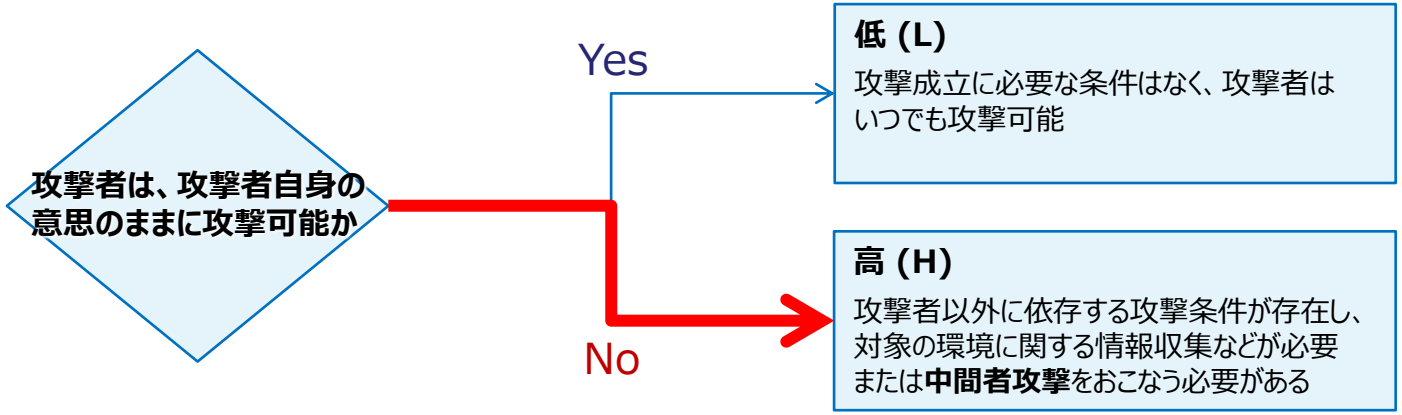
細工されたプログラムは HTTP 経由で渡される



Attack Complexity (AC) … 攻撃条件の複雑さ

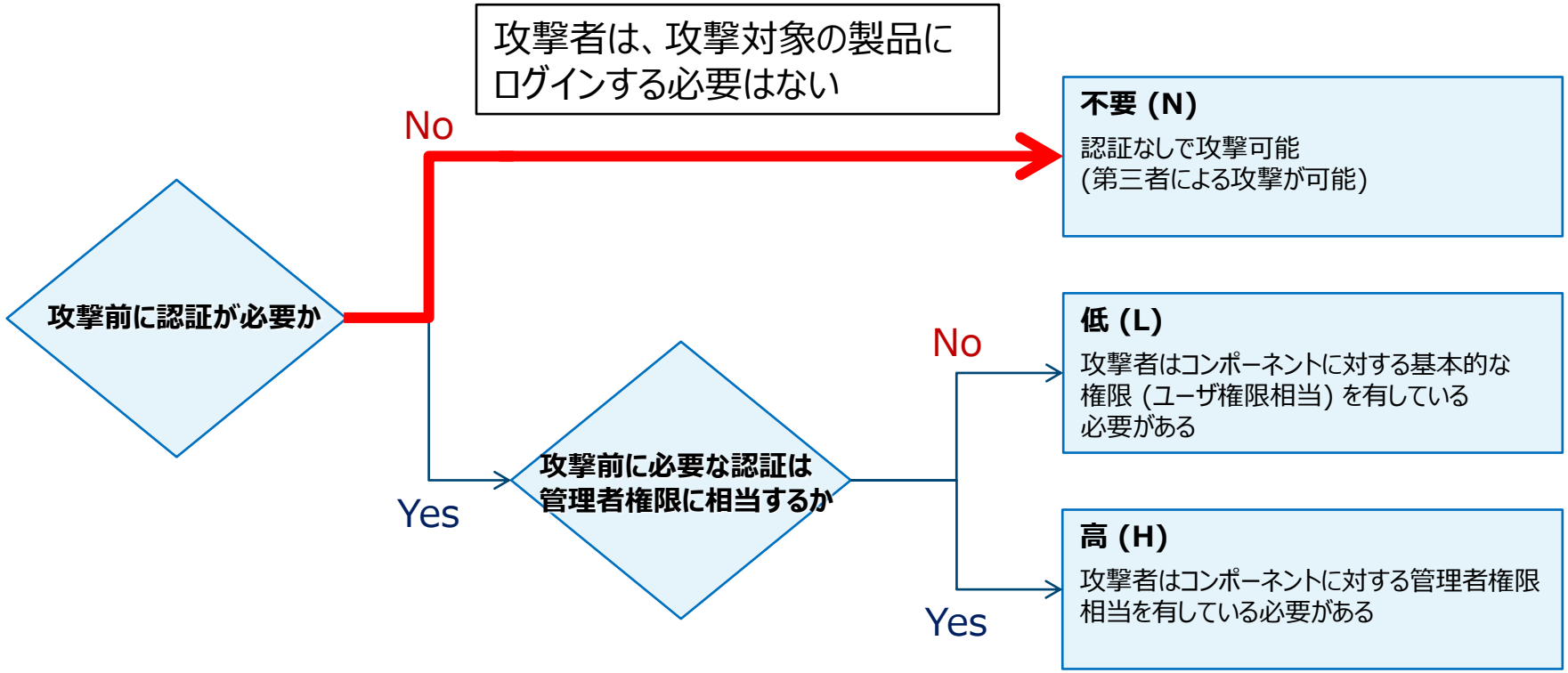
- 攻撃に必要な条件がどのようなものであるのかを評価

中間者攻撃を前提としている



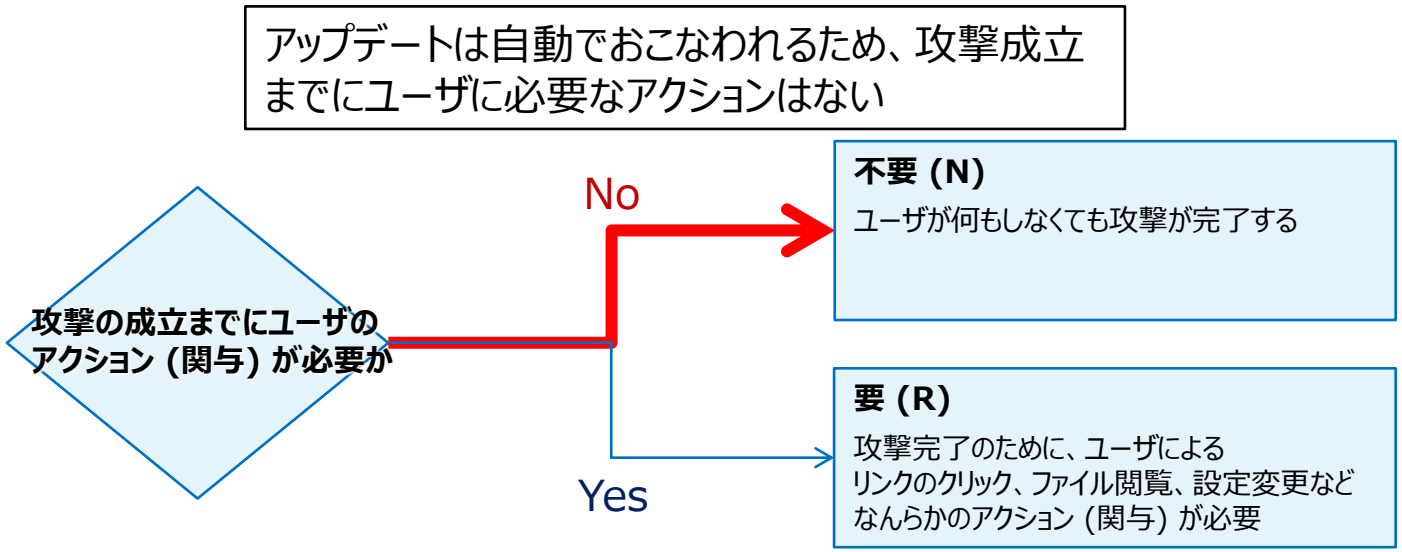
Privileges Required (PR) … 必要な特権レベル

- 攻撃に必要な認証レベルを評価

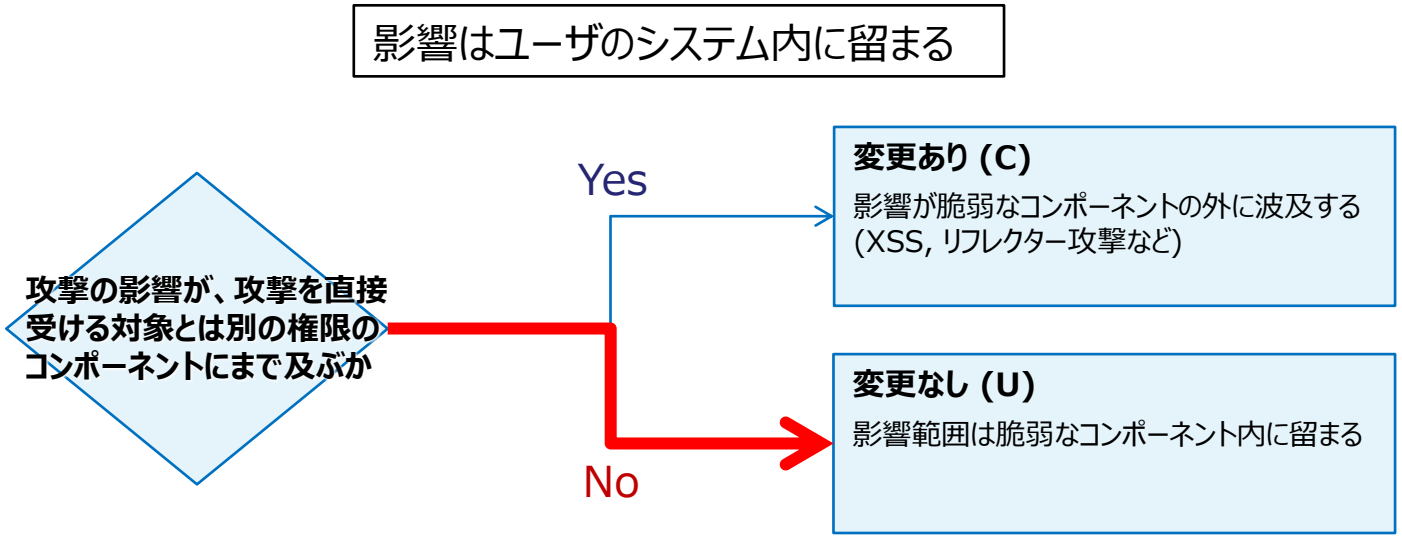


User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価

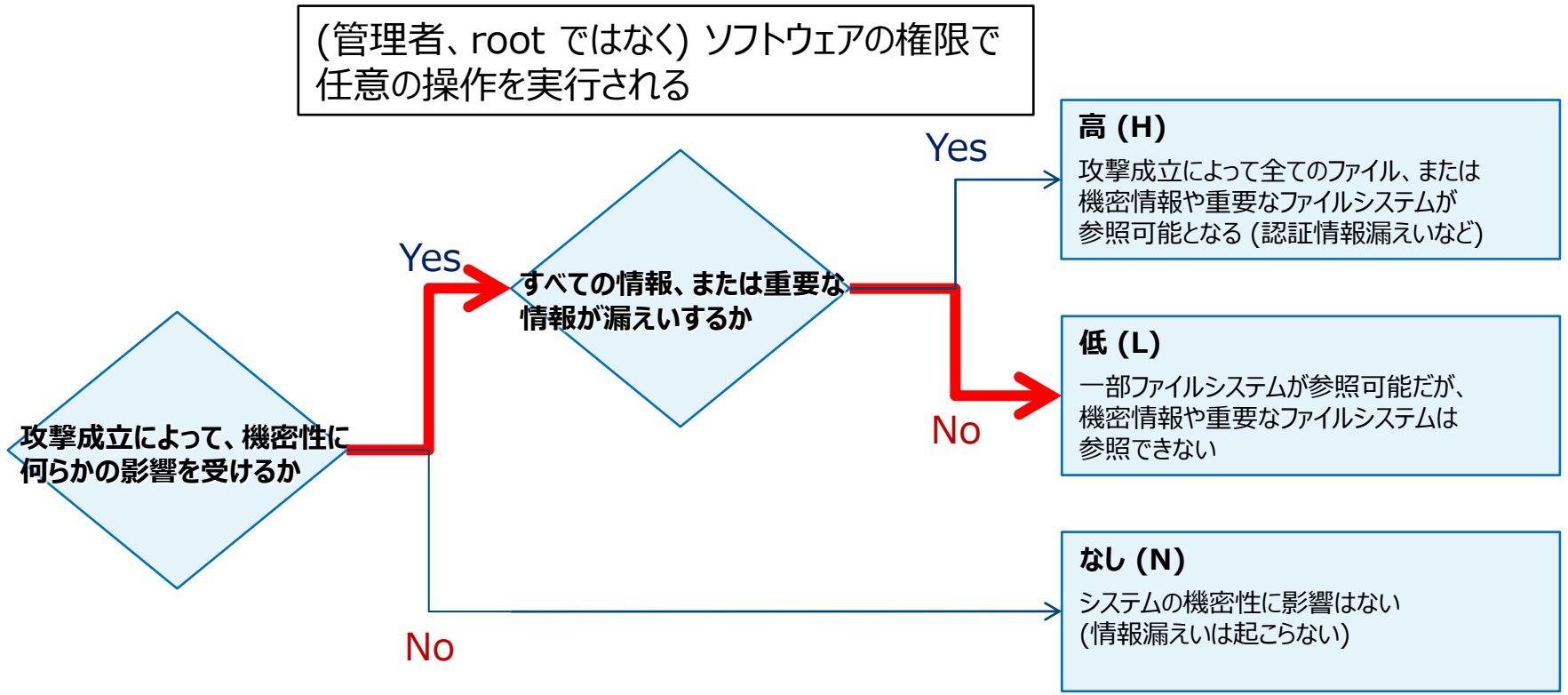


Scope (S) … スコープ - 被害の影響範囲を評価



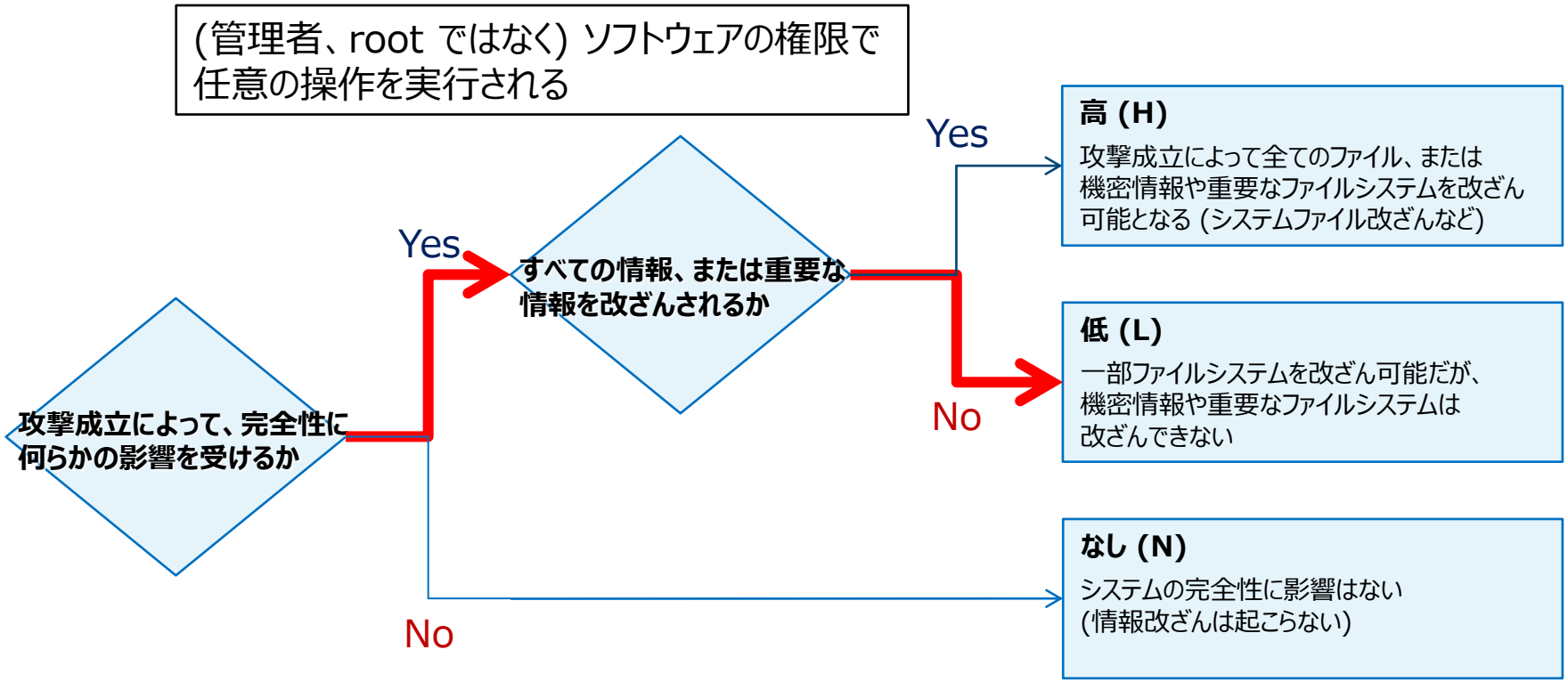
Confidentiality Impact (C) … 機密性への影響

- 攻撃された際に機密性に影響があるかを評価



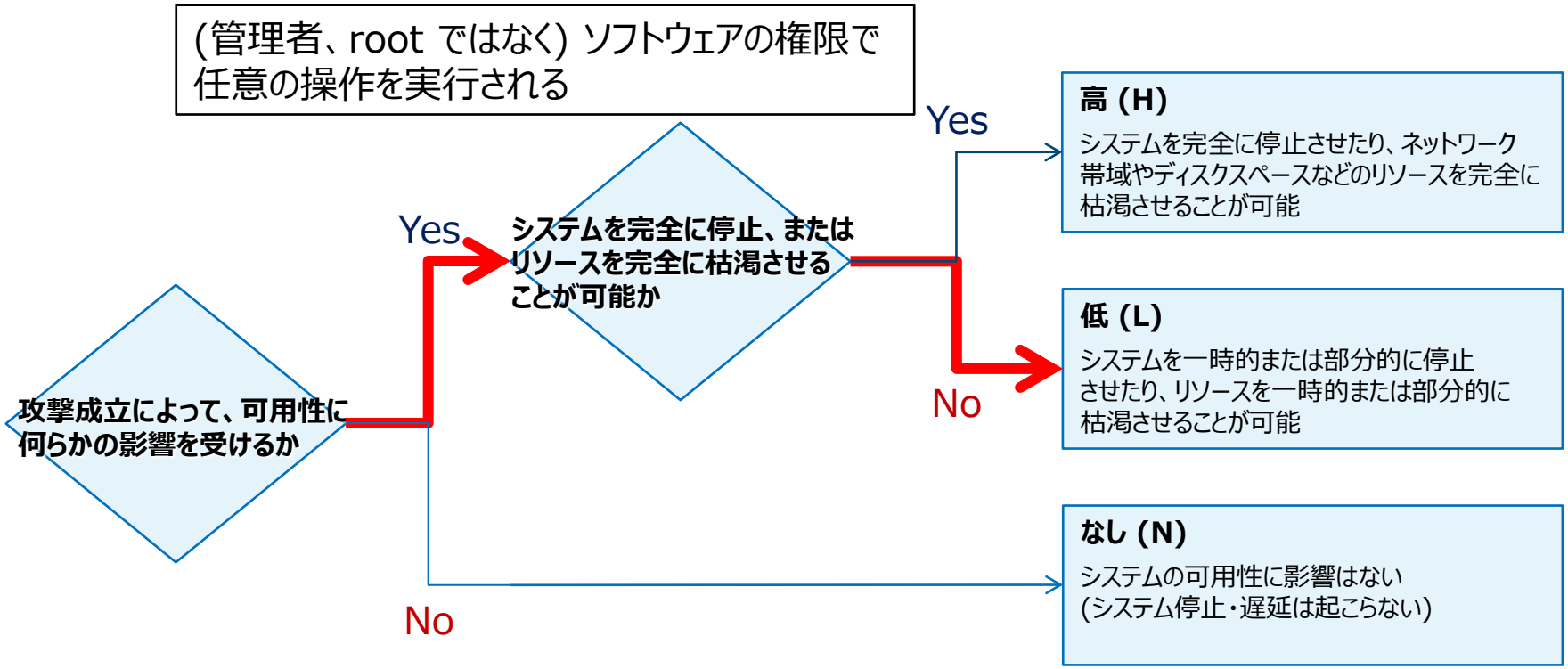
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



解説：案件6）Allround Automations PL/SQL Developer が HTTP 経由でアップデートする問題

評価項目	評価値	説明
攻撃元区分 (AV)	ネットワーク (N)	細工されたプログラムは HTTP 経由で渡される
攻撃条件の複雑さ (AC)	高 (H)	中間者攻撃を前提としている
必要な特権レベル (PR)	不要 (N)	攻撃者は、攻撃対象の製品にログインする必要はない
ユーザ関与レベル (UI)	不要 (N)	アップデートは自動でおこなわれるため、攻撃成立までにユーザに必要なアクションはない
スコープ (S)	変更なし (U)	影響はユーザのシステム内に留まる
機密性への影響 (C)	低 (L)	(管理者、root ではなく) ソフトウェアの権限で任意の操作を実行される
完全性への影響 (I)	低 (L)	(管理者、root ではなく) ソフトウェアの権限で任意の操作を実行される
可用性への影響 (A)	低 (L)	(管理者、root ではなく) ソフトウェアの権限で任意の操作を実行される

概要：案件7）DEXIS Imaging Suite 10 に認証情報がハードコードされている問題

公開日：2016/09/08　最終更新日：2016/09/08

JVNVU#91018225
DEXIS Imaging Suite 10 に認証情報がハードコードされている問題

概要

DEXIS が提供する DEXIS Imaging Suite 10 は、歯科向けの X 線画像処理ソフトウェアです。DEXIS Imaging Suite 10 には複数の認証情報がハードコードされているため、管理者または root 権限で患者情報データベースにアクセスされる可能性があります。

影響を受けるシステム

- DEXIS Imaging Suite 10

DEXIS Imaging Suite 10 以外のバージョンでも本脆弱性の影響を受ける可能性があります。

詳細情報

認証情報がハードコードされている問題 (CWE-798) - CVE-2016-6532
DEXIS Imaging Suite 10 にはデータベースの複数の認証情報がハードコードされているため、管理者または root 権限で患者情報データベースにアクセスされる可能性があります。

想定される影響

遠隔の攻撃者によって、管理者権限で当該製品の患者情報データベースにアクセスされる可能性があります。

対策方法

データベースの認証情報を更新する
開発者はデータベースの認証情報を変更するよう推奨しており、変更方法について次のように述べています。より詳しい情報は DEXIS Customer Support へお問い合わせください。

Changing the DEXIS database password

This procedure targets installations of DEXIS Imaging Suite (version 10). It will not

https://jvn.jp/vu/JVNVU91018225/

まとめ：案件7）DEXIS Imaging Suite 10 に認証情報がハードコードされている問題

- **脆弱性の種類**
  既知の認証情報を使用して管理者権限でログインできる問題
- **攻撃のシナリオ**
  既知の認証情報でログインするのみ
- **想定される影響**
  管理者または root 権限で**任意の操作**を実行される
- **補足情報**
  root 権限で任意の操作が実行可能なので、機密性・完全性・可用性すべてに**深刻な影響**を受けることになる

回答シート：案件7）DEXIS Imaging Suite 10 に認証情報がハードコードされている問題

CVSS v3	CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?			基本値: ?.? ▲
攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

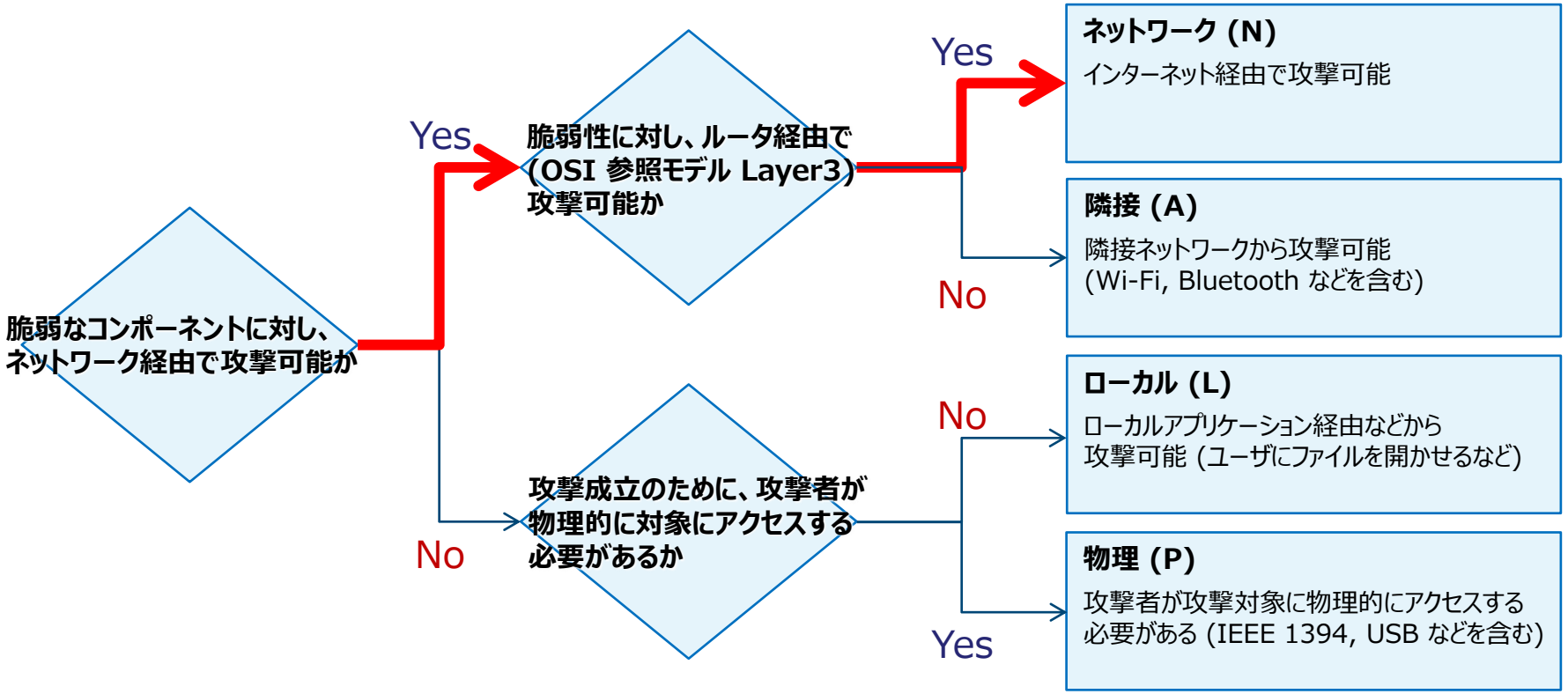
JVN掲載評価：案件7）DEXIS Imaging Suite 10 に認証情報がハードコードされている問題

CVSS v3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H			基本値: 9.8 ▲
攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	**ネットワーク (N)**
攻撃条件の複雑さ(AC)	高 (H)	**低 (L)**		
必要な特権レベル(PR)	高 (H)	低 (L)	**不要 (N)**	
ユーザ関与レベル(UI)	要 (R)	**不要 (N)**		
スコープ(S)	**変更なし (U)**	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	**高 (H)**	
完全性への影響(I)	なし (N)	低 (L)	**高 (H)**	
可用性への影響(A)	なし (N)	低 (L)	**高 (H)**	

Attack Vector (AV) … 攻撃元区分

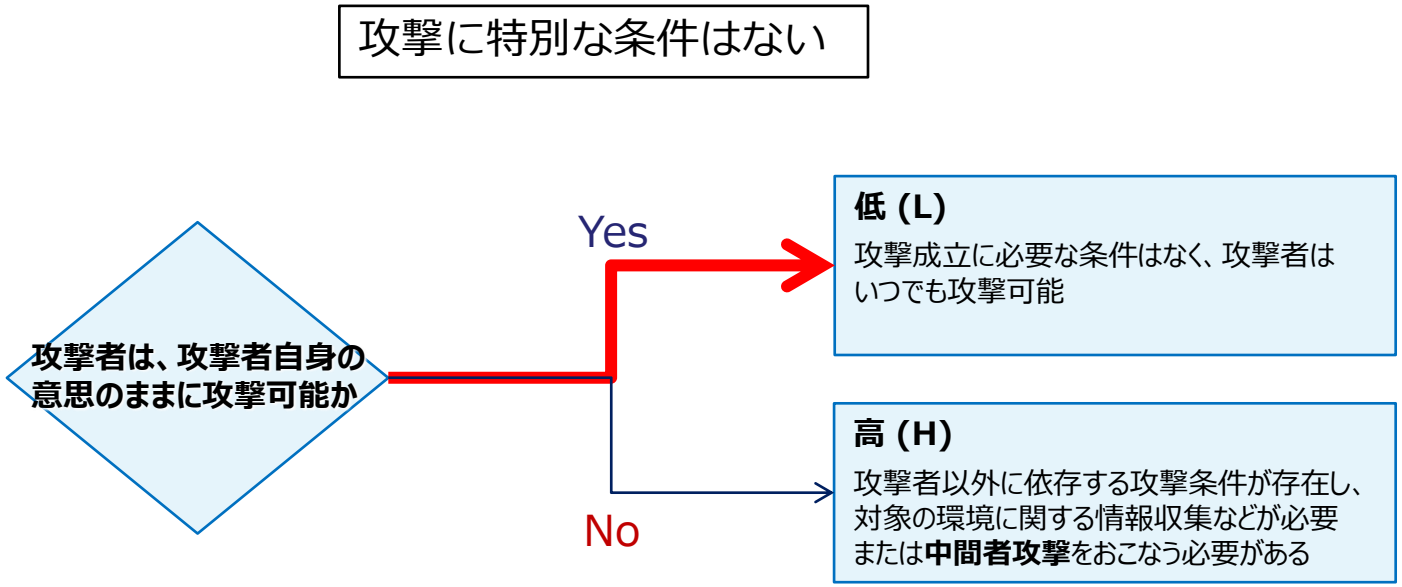
- システムを、どこから攻撃可能であるかを評価

ネットワーク経由でログインする必要がある



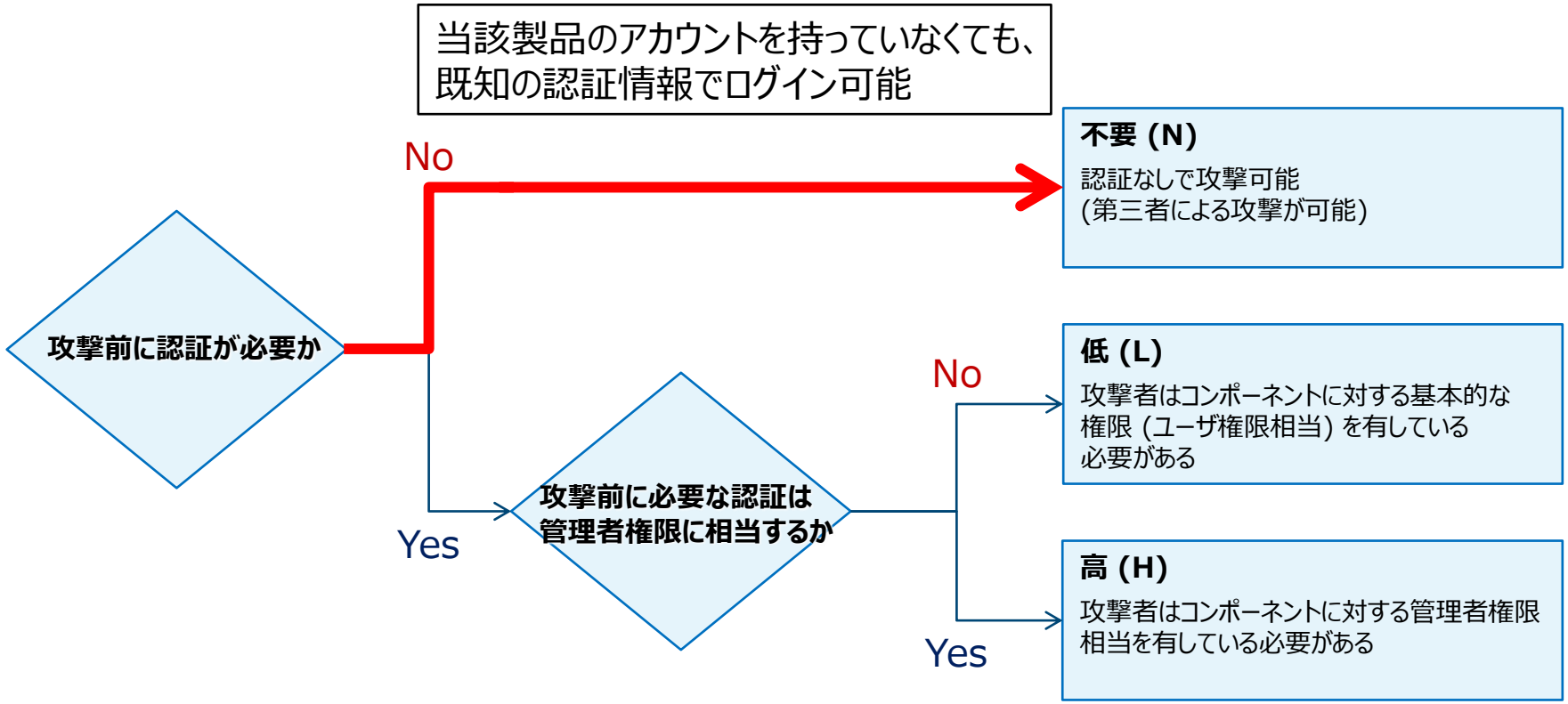
Attack Complexity (AC) … 攻撃条件の複雑さ

- 攻撃に必要な条件がどのようなものであるのかを評価



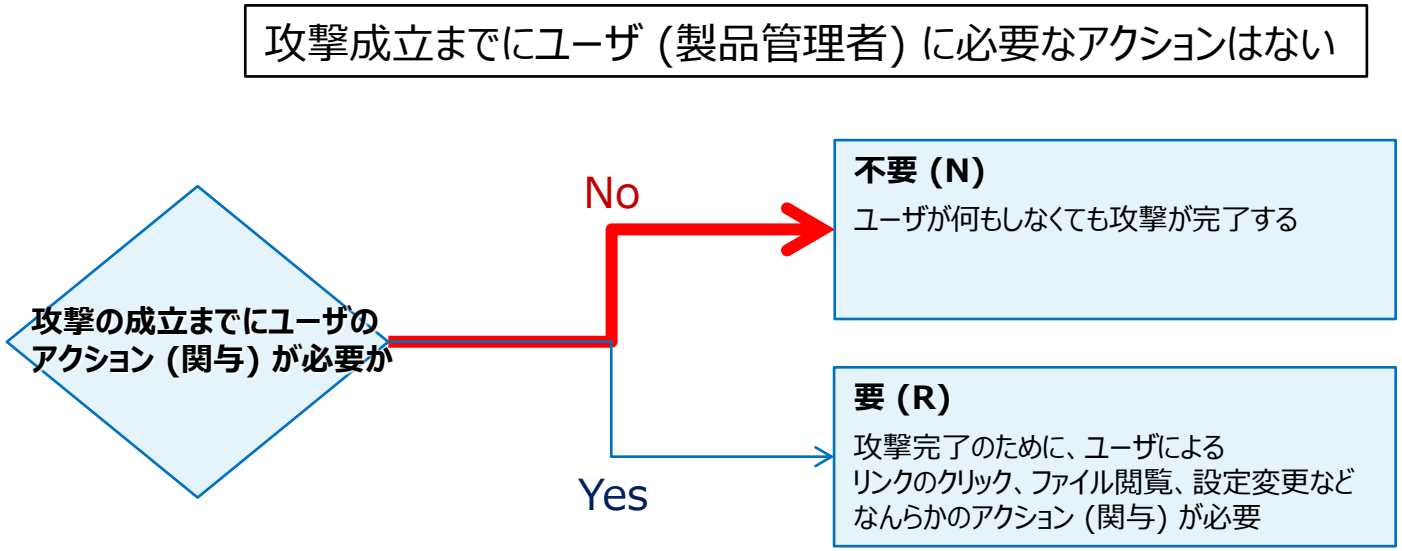
Privileges Required (PR) … 必要な特権レベル

- 攻撃に必要な認証レベルを評価

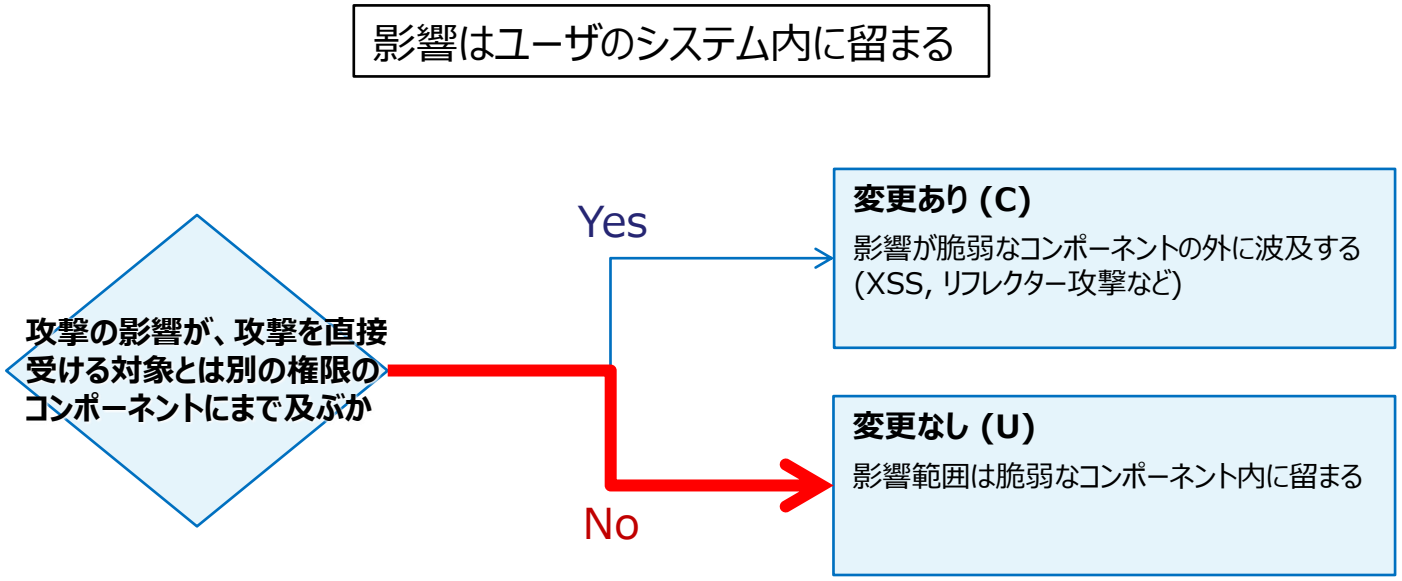


User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価

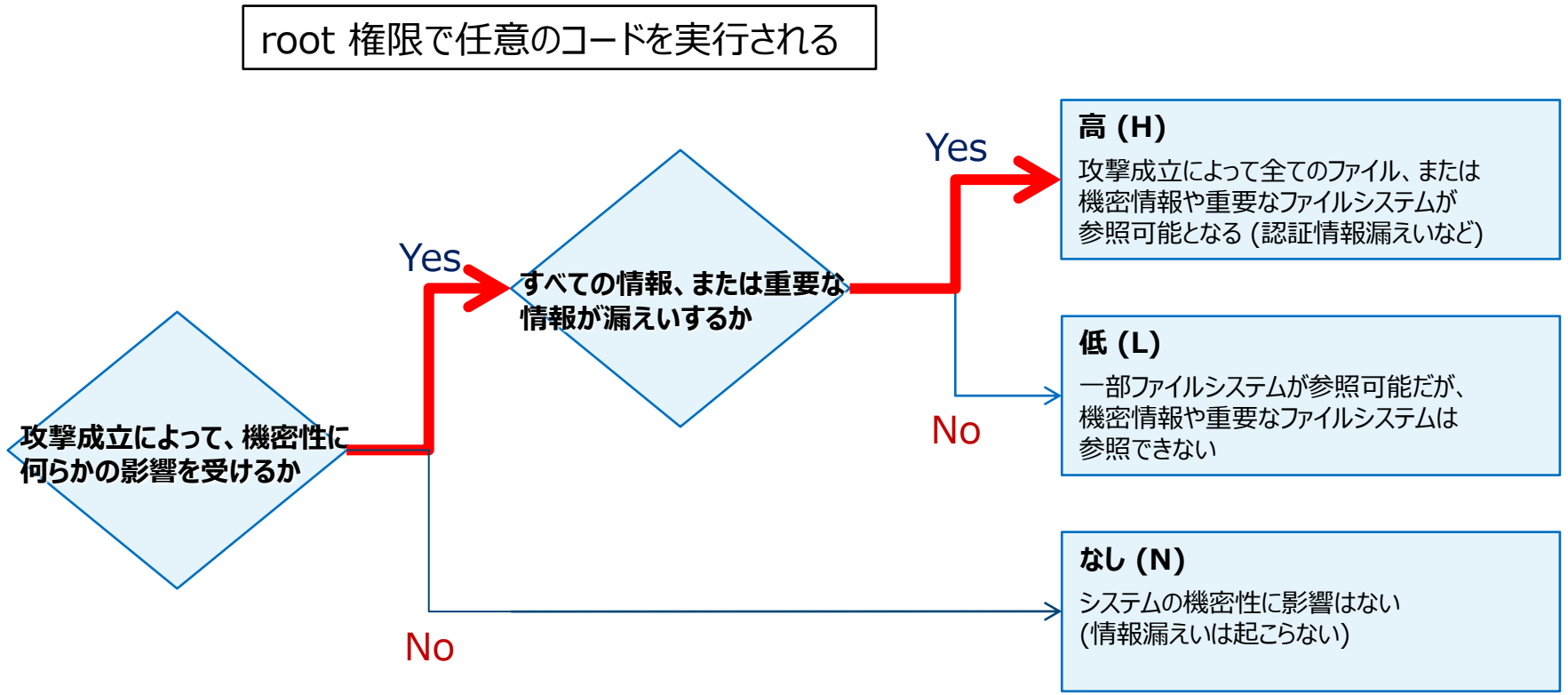


Scope (S) … スコープ - 被害の影響範囲を評価



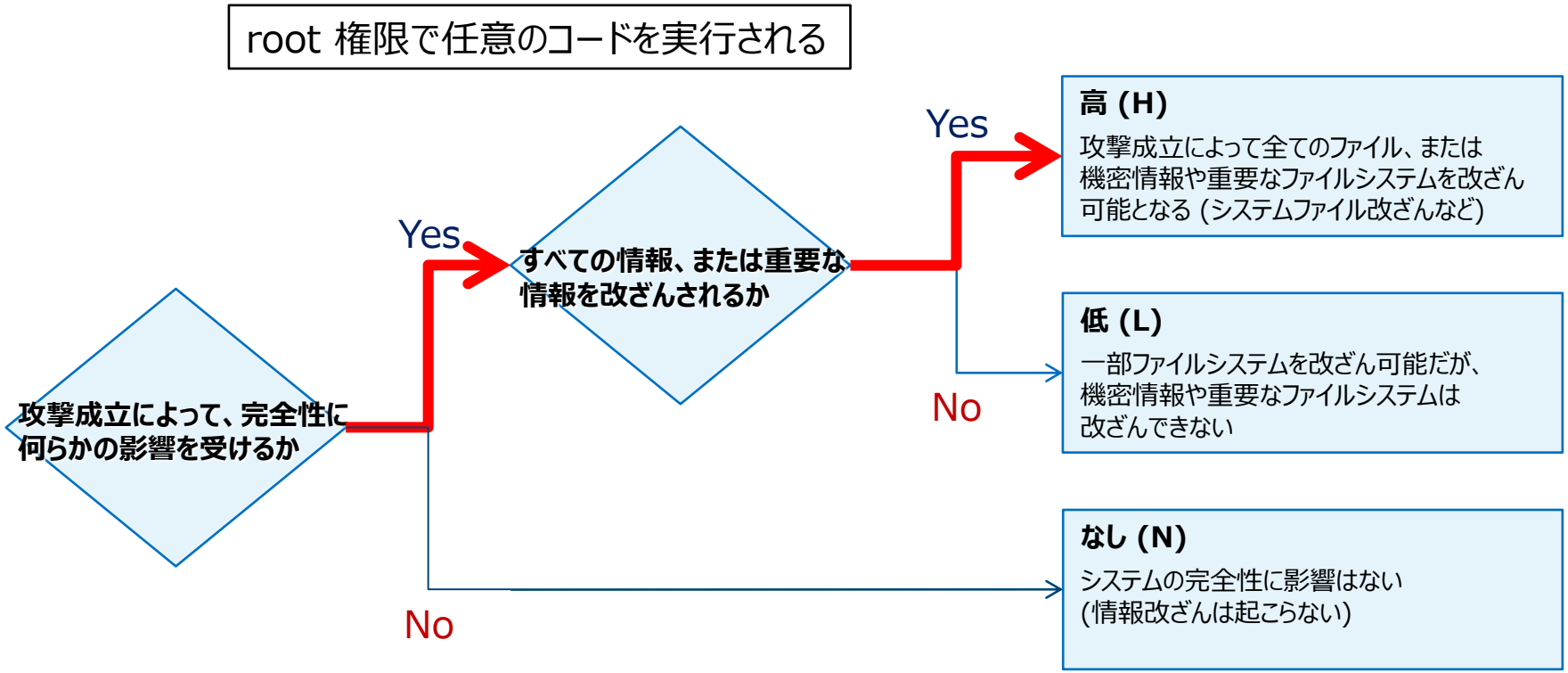
Confidentiality Impact (C) … 機密性への影響

- 攻撃された際に機密性に影響があるかを評価



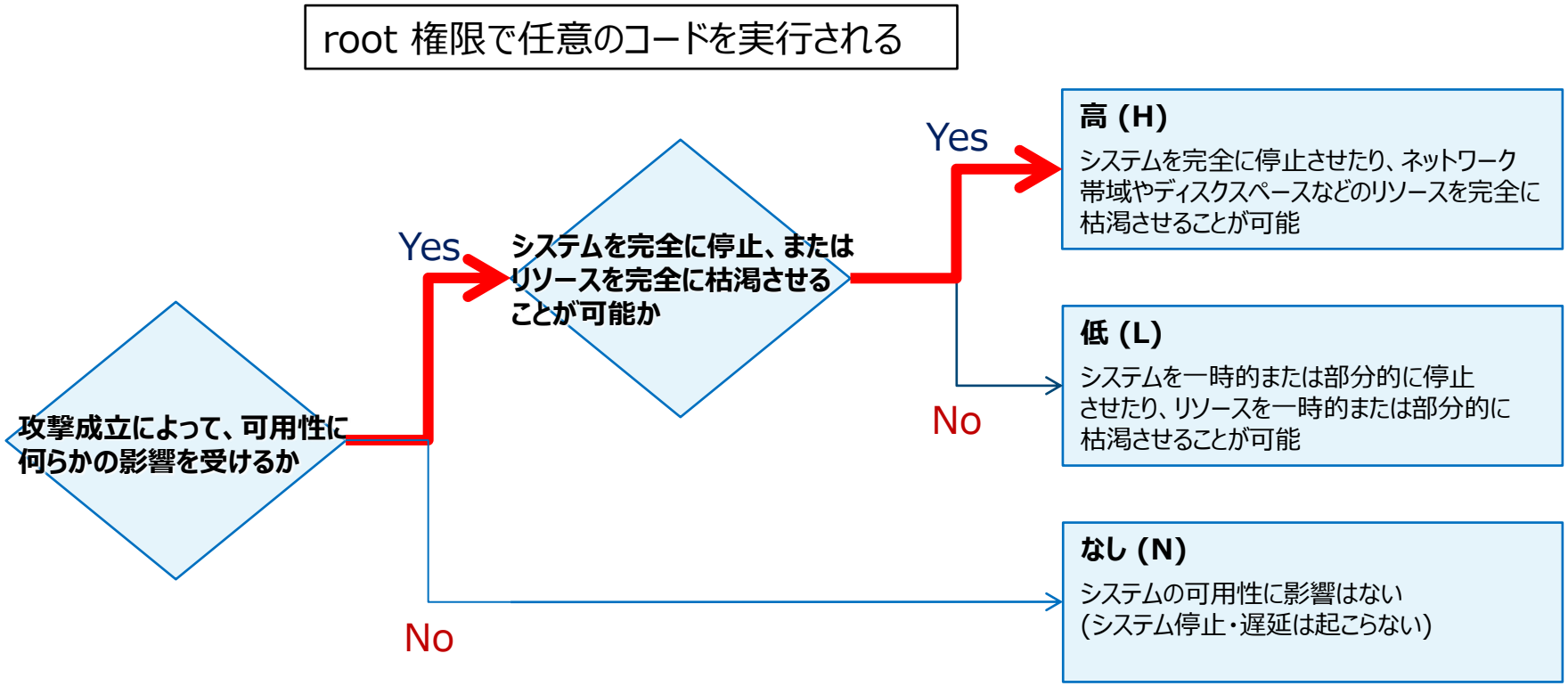
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



解説：案件7）DEXIS Imaging Suite 10 に認証情報がハードコードされている問題

評価項目	評価値	説明
攻撃元区分 (AV)	ネットワーク (N)	ネットワーク経由でログインする必要がある
攻撃条件の複雑さ (AC)	低 (L)	攻撃に特別な条件はない
必要な特権レベル (PR)	不要 (N)	当該製品のアカウントを持っていなくても、既知の認証情報でログイン可能
ユーザ関与レベル (UI)	不要 (N)	攻撃成立までにユーザ (製品管理者) に必要なアクションはない
スコープ (S)	変更なし (U)	影響はユーザのシステム内に留まる
機密性への影響 (C)	高 (H)	root 権限で任意の操作を実行される
完全性への影響 (I)	高 (H)	root 権限で任意の操作を実行される
可用性への影響 (A)	高 (H)	root 権限で任意の操作を実行される

概要：案件8）ImageMagick に入力値検証不備

公開日：2016/05/06　最終更新日：2016/09/23

JVNVU#92998929
ImageMagick に入力値検証不備の脆弱性
緊急

概要
ImageMagick は、delegate の仕組みを使って入力データの処理を行う前の検証が適切に実行されていないため、結果として任意のコードを実行される可能性があります。この問題は "ImageTragick" としても知られています。

影響を受けるシステム

- ImageMagick 6.9.3-10 より前のバージョン
- ImageMagick 7.0.1-1 より前のバージョン

詳細情報
不適切な入力検査 (CWE-20) - CVE-2016-3714
研究者は、メーリングリストに次のように投稿しています:

> *Insufficient filtering for filename passed to delegate's command allows remote code execution during conversion of several file formats.*
>
> *ImageMagick allows to process files with external libraries. This feature is called 'delegate'. It is implemented as a system() with command string ('command') from the config file delegates.xml with actual value for different params (input/output filenames etc). Due to insufficient %M param filtering it is possible to conduct shell command injection.*
>
> *delegate* 先のコマンドに渡す前のファイル名のフィルタリングが不十分なため、ファイル形式の変換中に任意のコードを実行される可能性がある。

https://jvn.jp/vu/JVNVU92998929/

まとめ：案件8）ImageMagick に入力値検証不備

- **脆弱性の種類**
  画像ファイルの処理に任意コード実行の脆弱性
- **攻撃のシナリオ**
  細工された画像ファイルが**ネットワーク経由**で読み込まれ、ImageMagick を呼び出したユーザの権限で任意のコードを実行される。CVSSv2 のスコアから、root 権限を持つユーザが ImageMagick を呼び出すことを想定していると考えられる。**外部の第三者**が製品を**直接**攻撃可能。
- **想定される影響**
  root 権限で**任意のコード**を実行される
- **補足情報**
  製品における ImageMagick の**実装により攻撃成否が変わる**

回答シート：案件8）ImageMagick に入力値検証不備

CVSS v3　CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?　基本値: ?.? ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

JVN掲載評価：案件8）ImageMagick に入力値検証不備

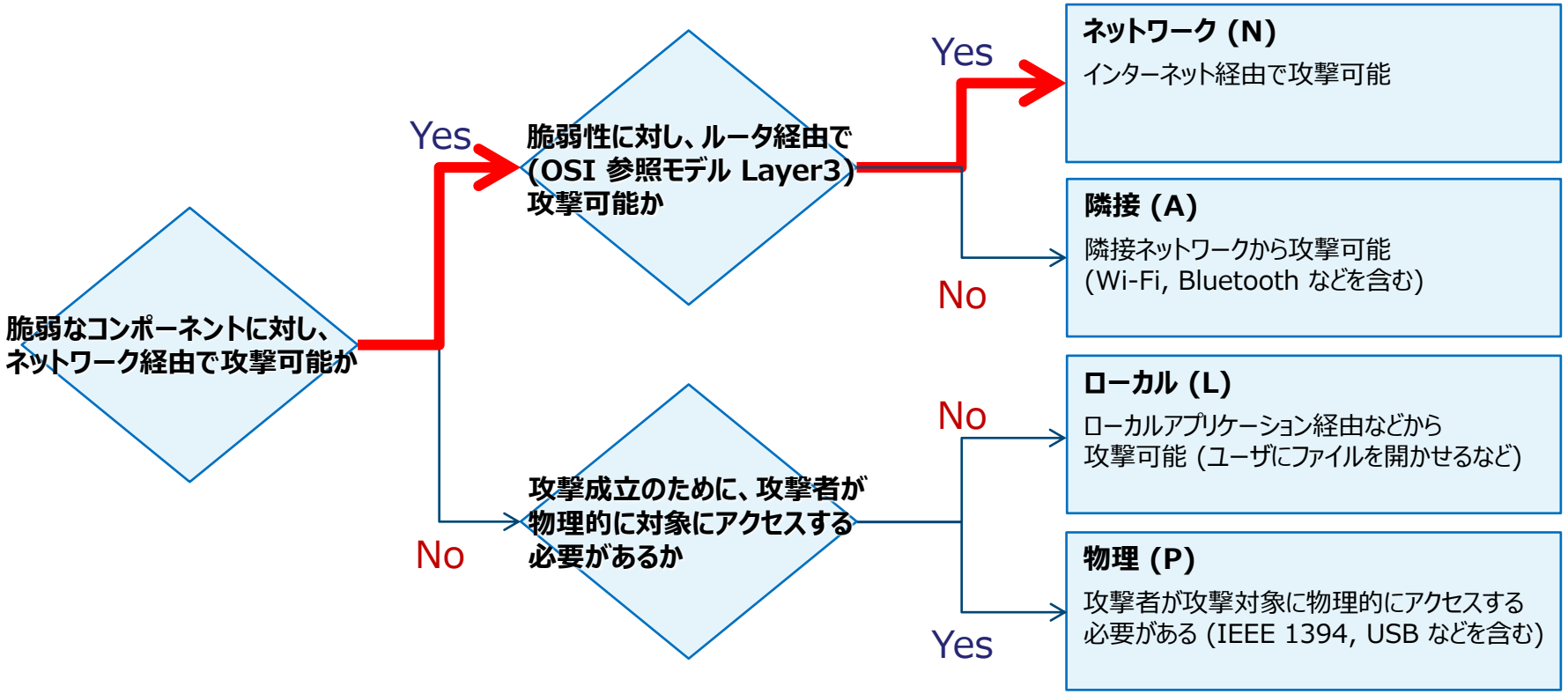
CVSS v3　CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H　**基本値: 8.1** ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	**ネットワーク (N)**
攻撃条件の複雑さ(AC)	**高 (H)**	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	**不要 (N)**	
ユーザ関与レベル(UI)	要 (R)	**不要 (N)**		
スコープ(S)	**変更なし (U)**	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	**高 (H)**	
完全性への影響(I)	なし (N)	低 (L)	**高 (H)**	
可用性への影響(A)	なし (N)	低 (L)	**高 (H)**	

Attack Vector (AV) … 攻撃元区分

- システムを、どこから攻撃可能であるかを評価

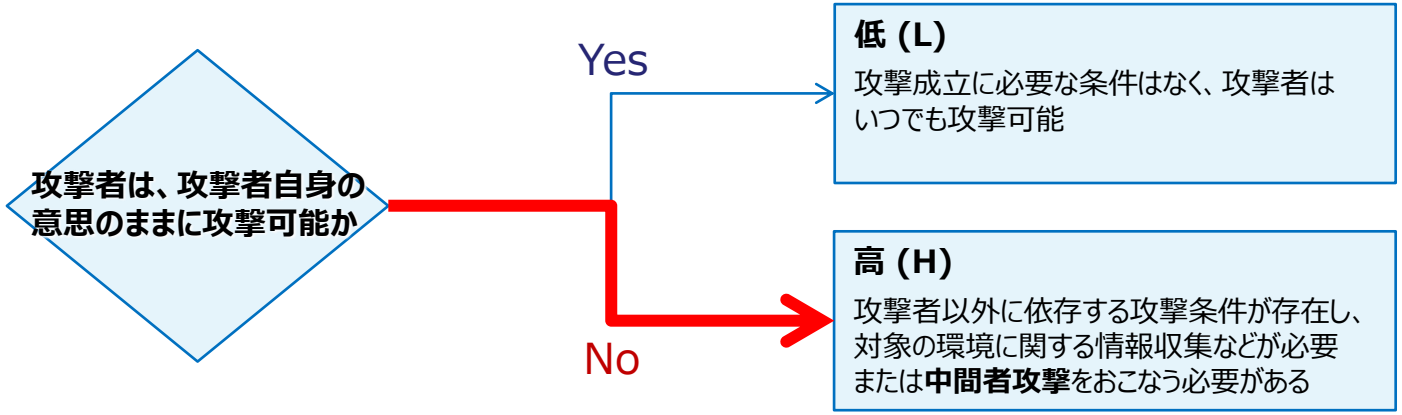
画像ファイルをネットワーク経由で送付する



Attack Complexity (AC) … 攻撃条件の複雑さ

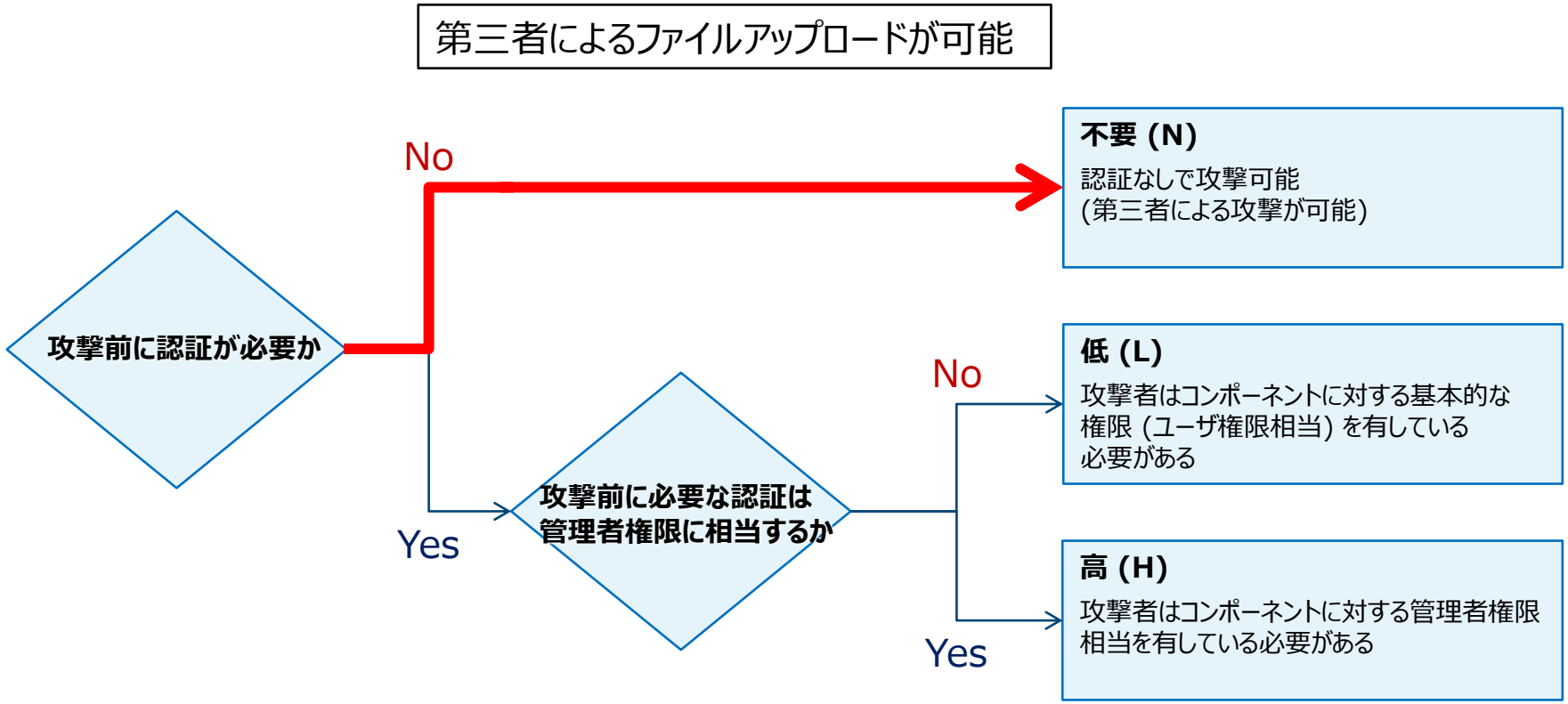
- 攻撃に必要な条件がどのようなものであるのかを評価

実装により攻撃成否に影響がある



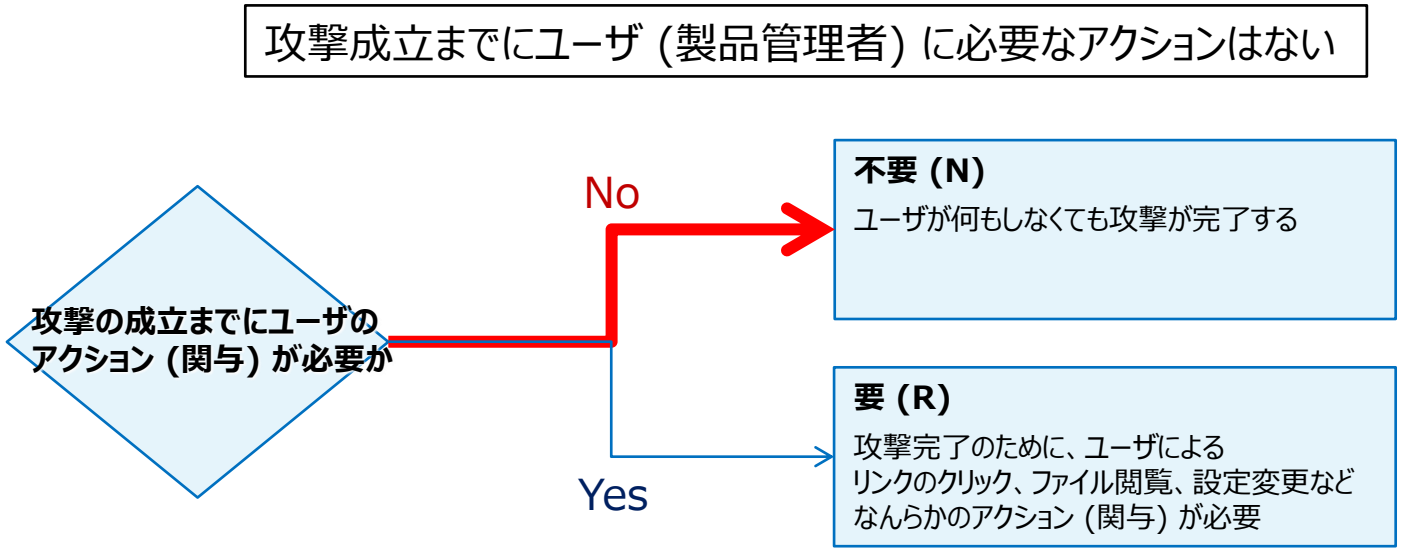
Privileges Required (PR) … 必要な特権レベル

- 攻撃に必要な認証レベルを評価



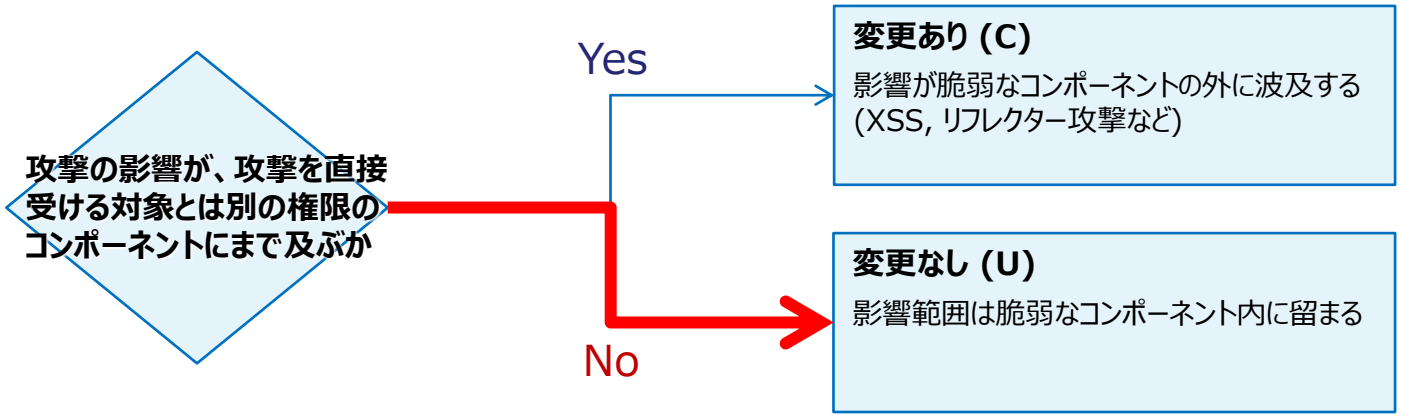
User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価



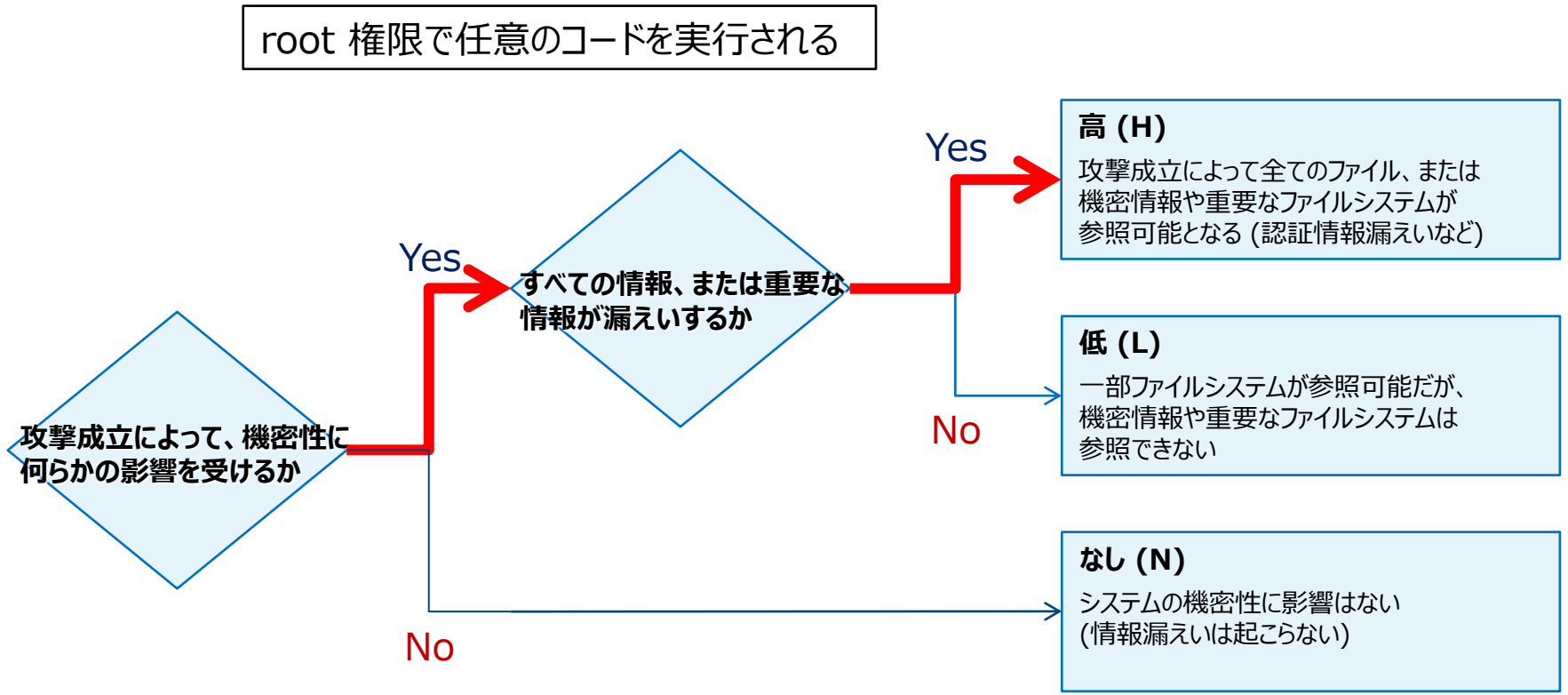
Scope (S) … スコープ - 被害の影響範囲を評価

影響はユーザのシステム内に留まる



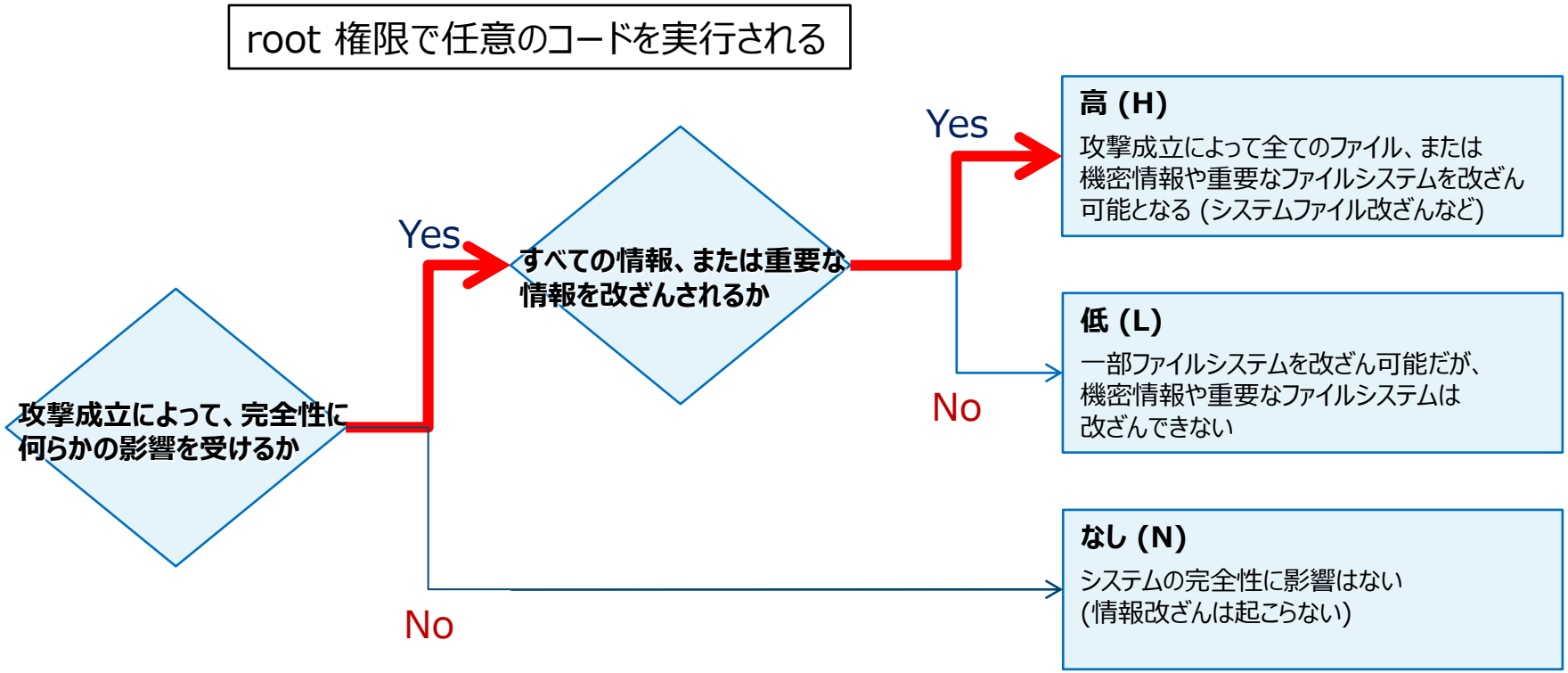
Confidentiality Impact (C) … 機密性への影響

- 攻撃された際に機密性に影響があるかを評価



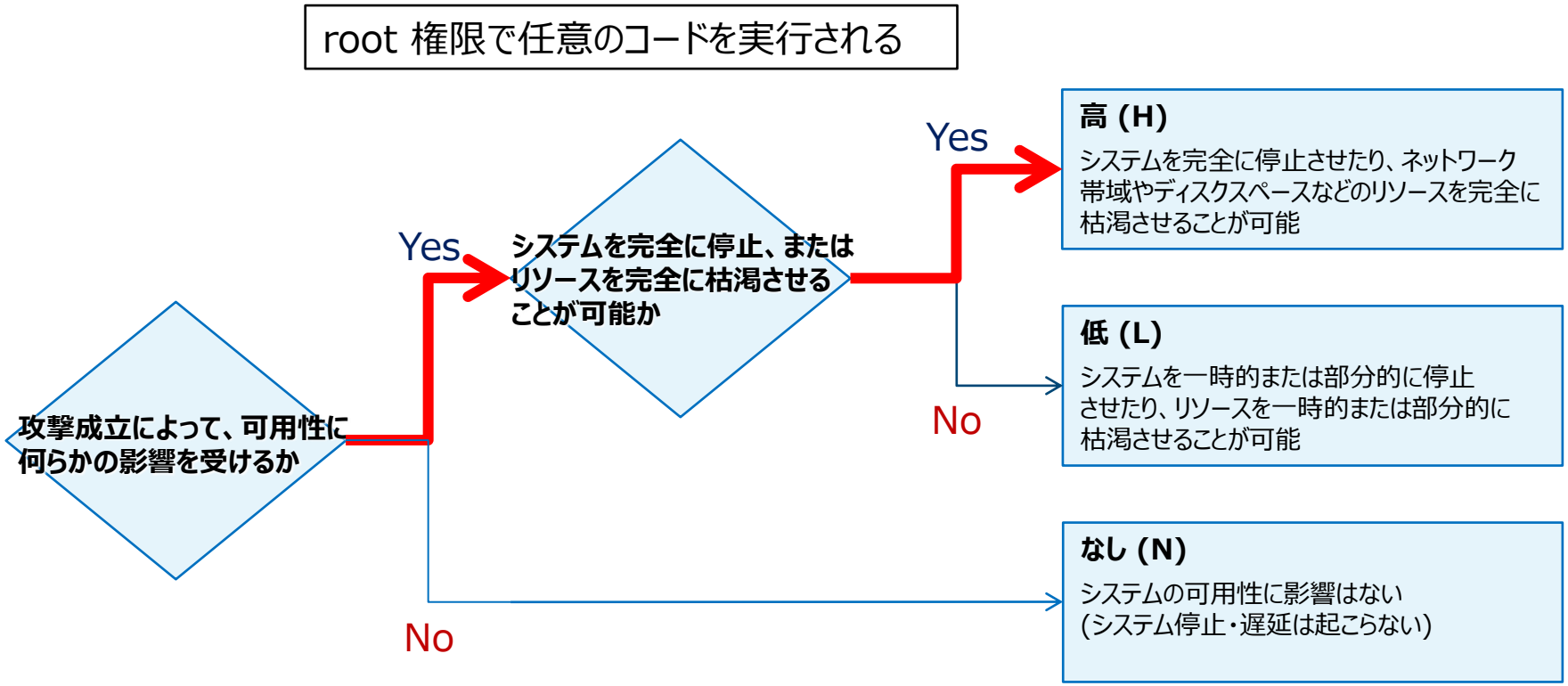
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



解説：案件8）ImageMagick に入力値検証不備

評価項目	評価値	説明
攻撃元区分 (AV)	ネットワーク (N)	画像ファイルをネットワーク経由で送付する
攻撃条件の複雑さ (AC)	高 (H)	実装により攻撃成否に影響がある
必要な特権レベル (PR)	不要 (N)	第三者によるファイルアップロードが可能
ユーザ関与レベル (UI)	不要 (N)	攻撃成立までにユーザ (製品管理者) に必要なアクションはない
スコープ (S)	変更なし (U)	影響はユーザのシステム内に留まる
機密性への影響 (C)	高 (H)	root 権限で任意の操作を実行される
完全性への影響 (I)	高 (H)	root 権限で任意の操作を実行される
可用性への影響 (A)	高 (H)	root 権限で任意の操作を実行される

概要：案件9）PhishWall クライアント Internet Explorer版のインストーラに DLL 読込みの脆弱性

公開日：2016/08/17　最終更新日：2016/08/17

JVN#45583702
PhishWall クライアント Internet Explorer版のインストーラにおける DLL 読み込みに関する脆弱性

概要
PhishWall クライアント Internet Explorer版のインストーラには、DLL 読み込みに関する脆弱性が存在します。

影響を受けるシステム

- PhishWall クライアント Internet Explorer版 Ver. 3.7.8.1 およびそれ以前のインストーラ

詳細情報
株式会社セキュアブレインが提供する PhishWall クライアント Internet Explorer版は、不正送金やフィッシング対策用のソフトウェアです。PhishWall クライアント Internet Explorer版のインストーラには、DLL を読み込む際の検索パスに問題があり、意図しない DLL を読み込んでしまう脆弱性が存在します。

当該製品のインストーラは Install Shield の旧バージョンで作成されていますが、最新の Install Shield では、DLL 読み込みの問題に対して対策を行っています。詳細については「Best Practices to Avoid Windows Setup Launcher Executable Issues」を参照してください。

想定される影響
インストーラを実行している管理者の権限で、任意のコードを実行される可能性があります。

対策方法
最新のインストーラを使用する
開発者が提供する情報をもとに、最新のインストーラを使用してください。
なお、本脆弱性の影響を受けるのはインストーラの起動時のみのため、既存のユーザは PhishWall クライアント Internet Explorer版をアップデートする必要はありません。

https://jvn.jp/jp/JVN45583702/

まとめ：案件9）PhishWall クライアント Internet Explorer版のインストーラに DLL 読込みの脆弱性

- **脆弱性の種類**
  インストール時に意図しない DLL ファイルを呼び出す問題
- **攻撃のシナリオ**
  当該製品のインストール時に、特定の名称の DLL ファイルが特定のディレクトリに存在する場合、**第三者**が用意した DLL ファイルを意図せず呼び出してしまう
- **想定される影響**
  第三者が細工した DLL ファイルを設置された状態で**ユーザが**インストーラを実行した場合、**管理者権限**で**任意のコード**を実行される可能性がある
- **補足情報**
  攻撃者は遠隔地にいてもいいが、インストーラはユーザの**ローカルシステム**上で実行される

回答シート：案件9）PhishWall クライアント Internet Explorer版のインストーラに DLL 読込みの脆弱性

CVSS v3	CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:?			基本値: ?.? ▲
攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

JVN掲載評価：案件9）PhishWall クライアント Internet Explorer版のインストーラに DLL 読込みの脆弱性

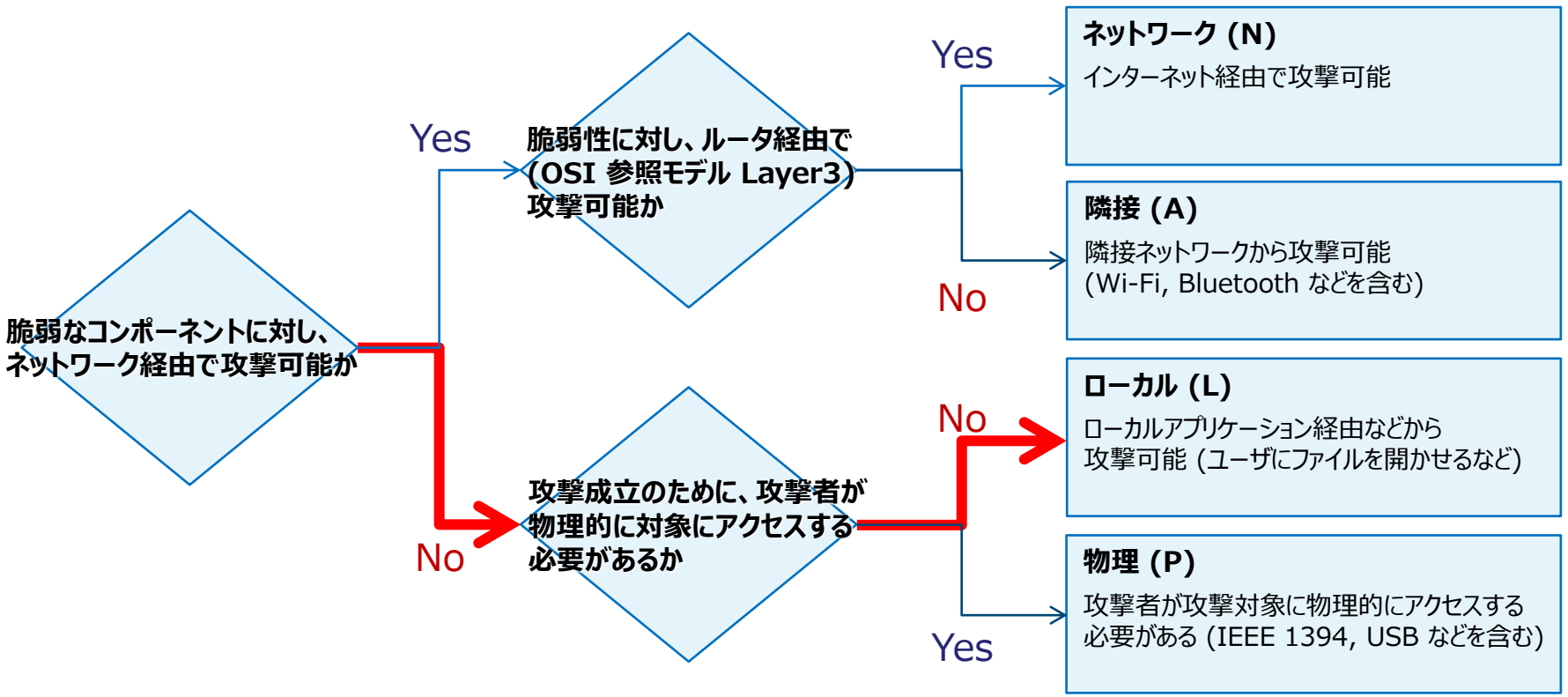
CVSS v3　CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H　**基本値: 7.8** ▲

攻撃元区分(AV)	物理 (P)	**ローカル (L)**	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	**低 (L)**		
必要な特権レベル(PR)	高 (H)	低 (L)	**不要 (N)**	
ユーザ関与レベル(UI)	**要 (R)**	不要 (N)		
スコープ(S)	**変更なし (U)**	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	**高 (H)**	
完全性への影響(I)	なし (N)	低 (L)	**高 (H)**	
可用性への影響(A)	なし (N)	低 (L)	**高 (H)**	

Attack Vector (AV) … 攻撃元区分

- システムを、どこから攻撃可能であるかを評価

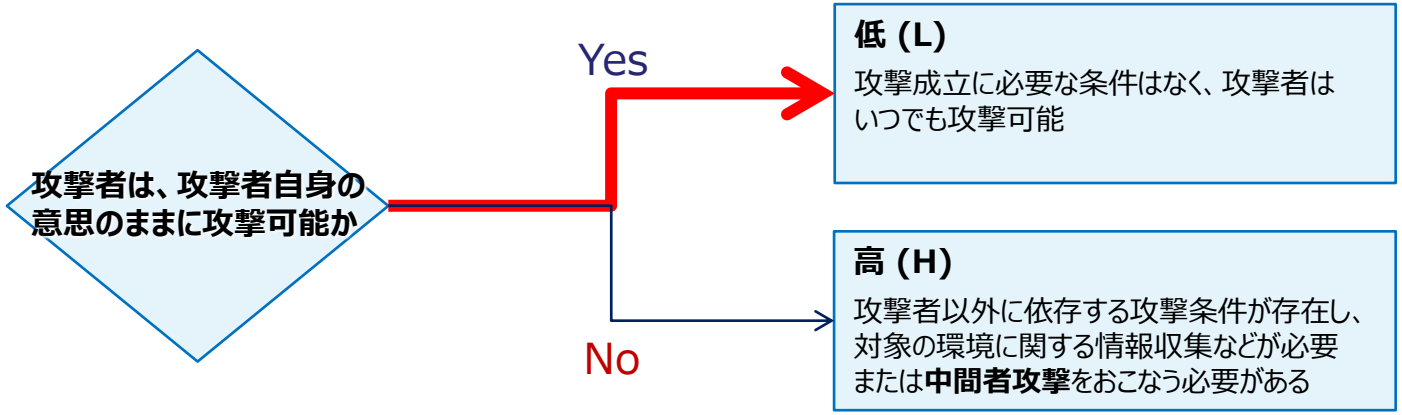
ユーザのローカル環境で実行することで発現する



Attack Complexity (AC) … 攻撃条件の複雑さ

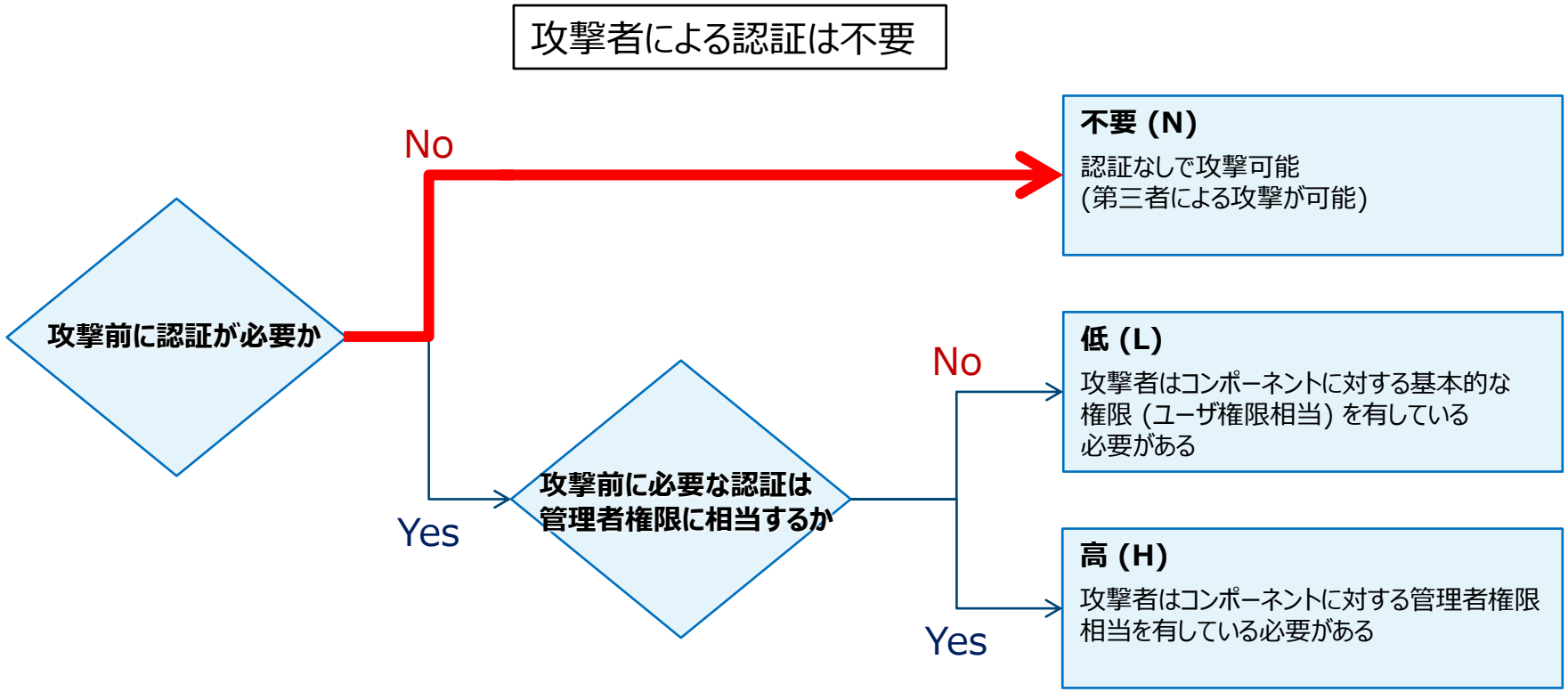
- 攻撃に必要な条件がどのようなものであるのかを評価

攻撃に特別な条件はない



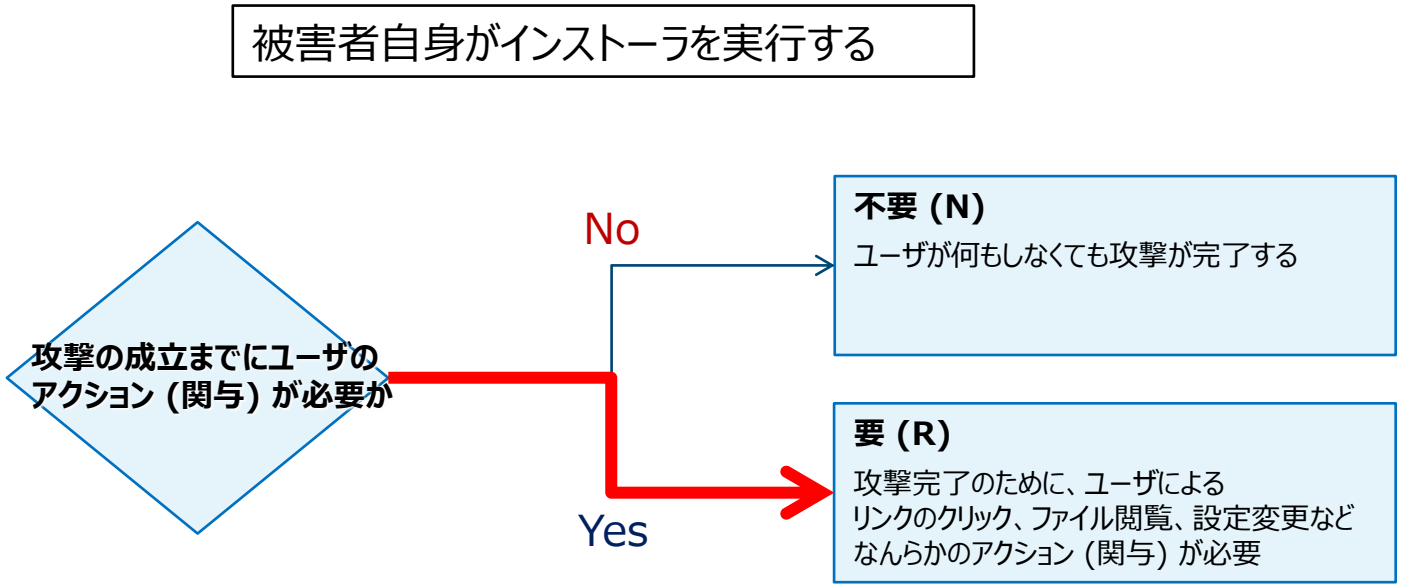
Privileges Required (PR) … 必要な特権レベル

- 攻撃に必要な認証レベルを評価



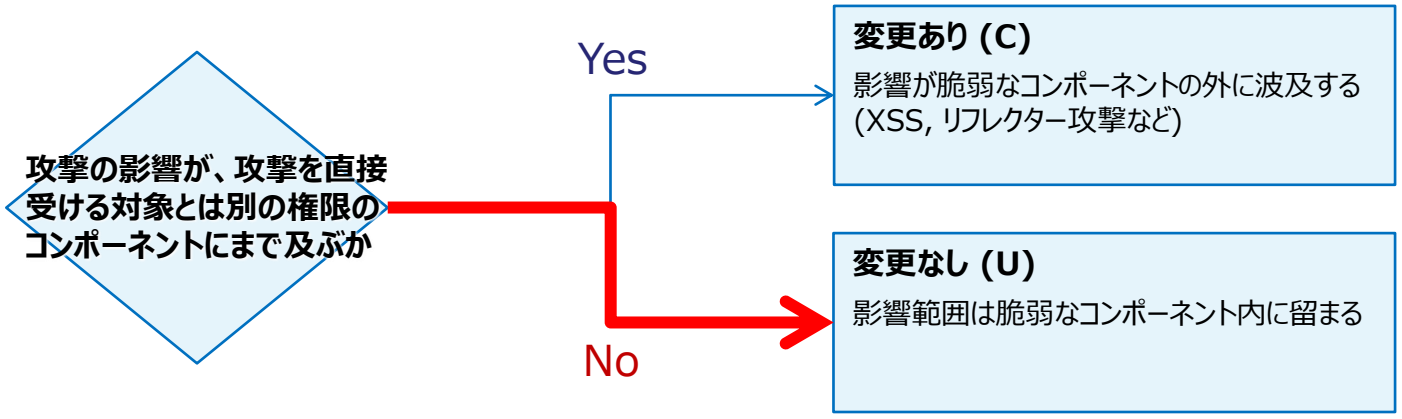
User Interaction (UI) … ユーザ関与レベル

- 攻撃のためにユーザ (被害者) の関与が必要かを評価



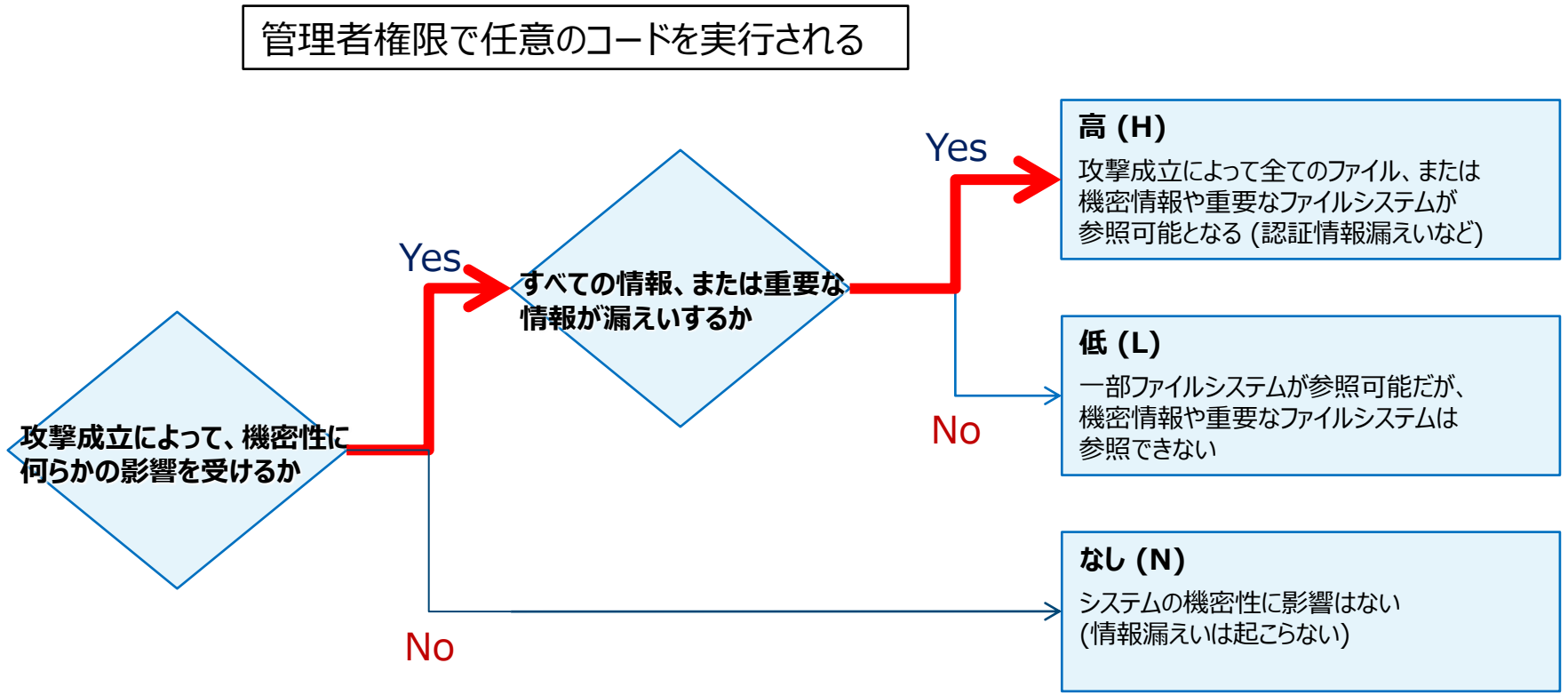
Scope (S) … スコープ - 被害の影響範囲を評価

影響はユーザのシステム内に留まる



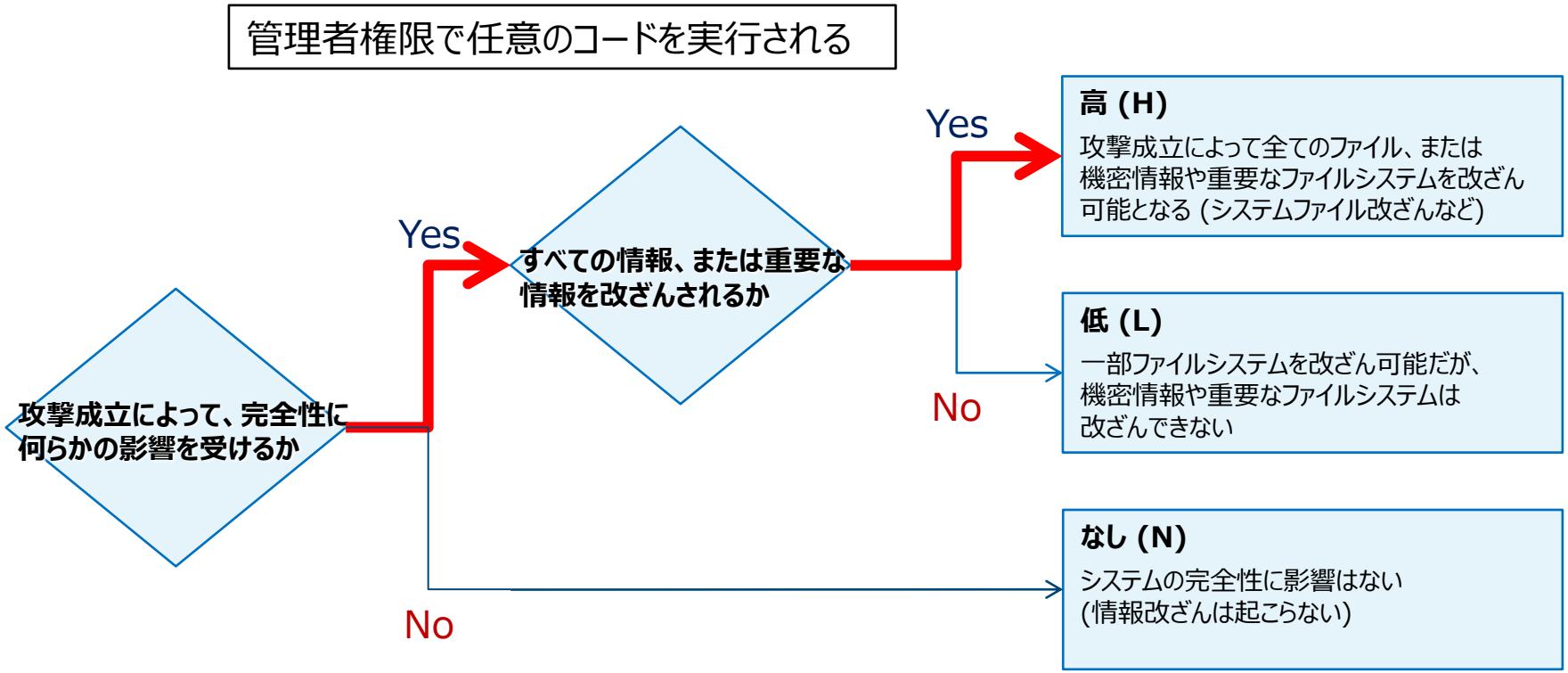
Confidentiality Impact (C) … 機密性への影響

- 攻撃された際に機密性に影響があるかを評価



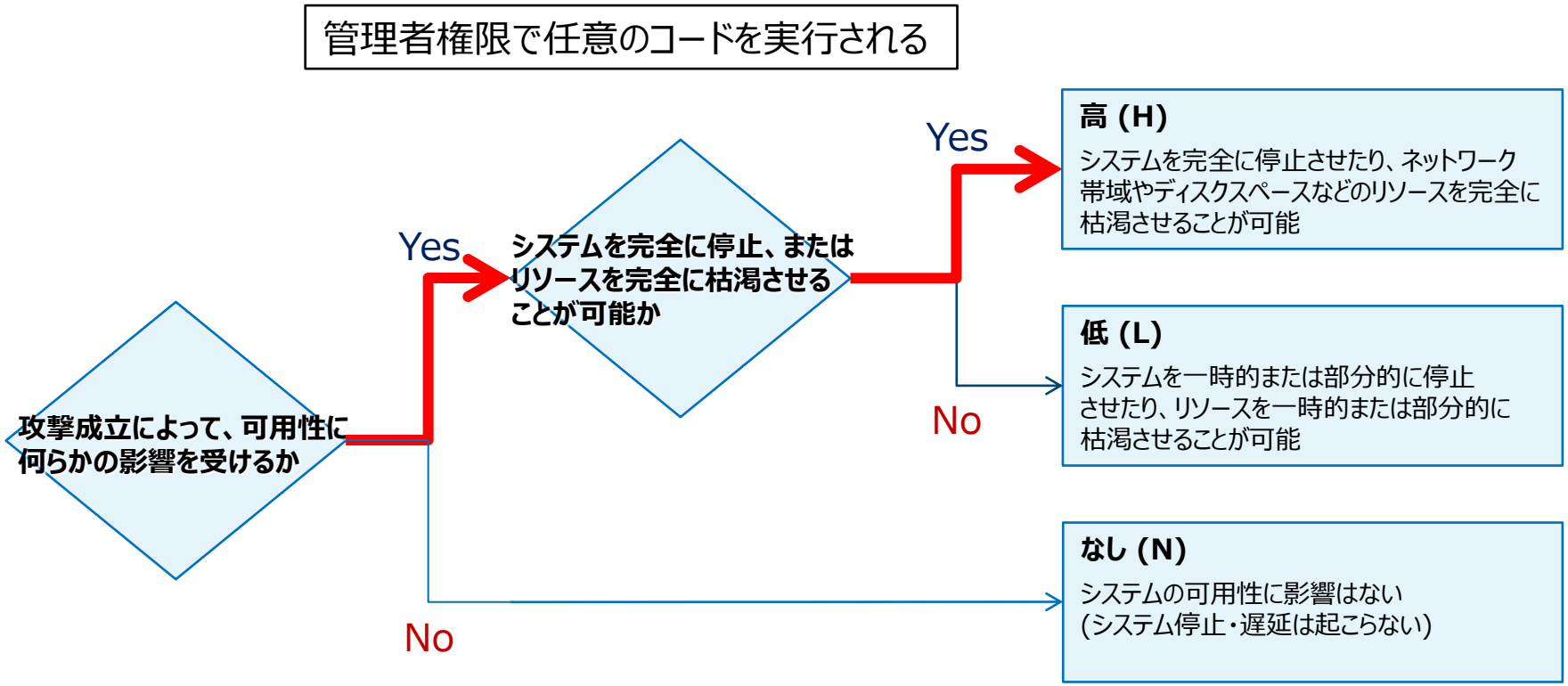
Integrity Impact (I) … 完全性への影響

- 攻撃された際に完全性に影響があるかを評価



Availability Impact (A) … 可用性への影響

- 攻撃された際に可用性に影響があるかを評価



解説：案件9）PhishWall クライアント Internet Explorer版のインストーラに DLL 読込みの脆弱性

評価項目	評価値	説明
攻撃元区分 (AV)	ローカル (L)	ユーザのローカル環境で実行することで発現する
攻撃条件の複雑さ (AC)	低 (L)	攻撃に特別な条件はない
必要な特権レベル (PR)	不要 (N)	攻撃者による認証は不要
ユーザ関与レベル (UI)	要 (R)	被害者自身がインストーラを実行する
スコープ (S)	変更なし (U)	影響はユーザのシステム内に留まる
機密性への影響 (C)	高 (H)	管理者権限で任意のコードを実行される
完全性への影響 (I)	高 (H)	管理者権限で任意のコードを実行される
可用性への影響 (A)	高 (H)	管理者権限で任意のコードを実行される

参考文献

FIRST

Common Vulnerability Scoring System v3.1: Specification Document
https://www.first.org/cvss/v3.1/specification-document

Common Vulnerability Scoring System v3.1: Examples
https://www.first.org/cvss/v3.1/examples

情報処理推進機構 (IPA)

共通脆弱性評価システムCVSS v3概説
https://www.ipa.go.jp/security/vuln/CVSSv3.html

JVN iPedia 脆弱性対策情報データベース
http://jvndb.jvn.jp/

JVN

Japan Vulnerability Notes
https://jvn.jp/

不明点は JVN ベンダポータルサイトの問い合わせフォーム
または jvn@jvn.jp までお問い合わせください。

ありがとうございました