IPA Better Life with IT

情報セキュリティEXPO

増加する脆弱性を評価するシステム（CVSS）の活用
～脆弱性対策の適切な運用のために～

2018年5月11日

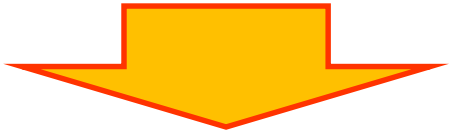
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
小林 桂

本日の内容

- はじめに
- CVSSとは
- 基本評価基準(Base Metrics)
- 現状評価基準(Temporal Metrics)
- 環境評価基準(Environmental Metrics)
- まとめ

はじめに

- 日々公開される脆弱性(ソフトウェアや情報システムに存在するセキュリティ上の弱点)の情報、正しい理解と判断が求められる。
  - その脆弱性の特長は？深刻度は？
  - 自組織ではその脆弱性の影響を受けるか
  - 脆弱性対応の優先順位は？



これらを評価できる脆弱性評価基準が必要に

CVSSとは
～CVSSの評価基準～

- 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手法
  - CVSSv2 と CVSSv3 がある。
  - 脆弱性の深刻度を 0.0 ～ 10.0 のスコアで評価
  - CVSSでは次の 3 つの基準で脆弱性を評価します
    I. 基本評価基準(Base Metrics)
    II. 現状評価基準(Temporal Metrics)
    III. 環境評価基準(Environmental Metrics)

CVSSとは
～CVSSの評価基準～

IPA

I. 基本評価基準 (Base Metrics)

II. 現状評価基準 (Temporal Metrics)

III. 環境評価基準 (Environmental Metrics)

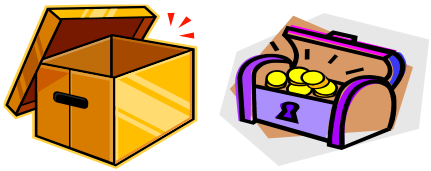
「脆弱性の特性」

攻撃の難易度は？
攻撃された場合の影響は？

「攻撃状況」

既に攻撃されている？
対策パッチは出ている？

「システムの重要度」



想定環境は？
システムの重要度は？

例えば
「SQLインジェクション」×「攻撃観測なし」×「内部システムで利用」
＝**深刻度 低**

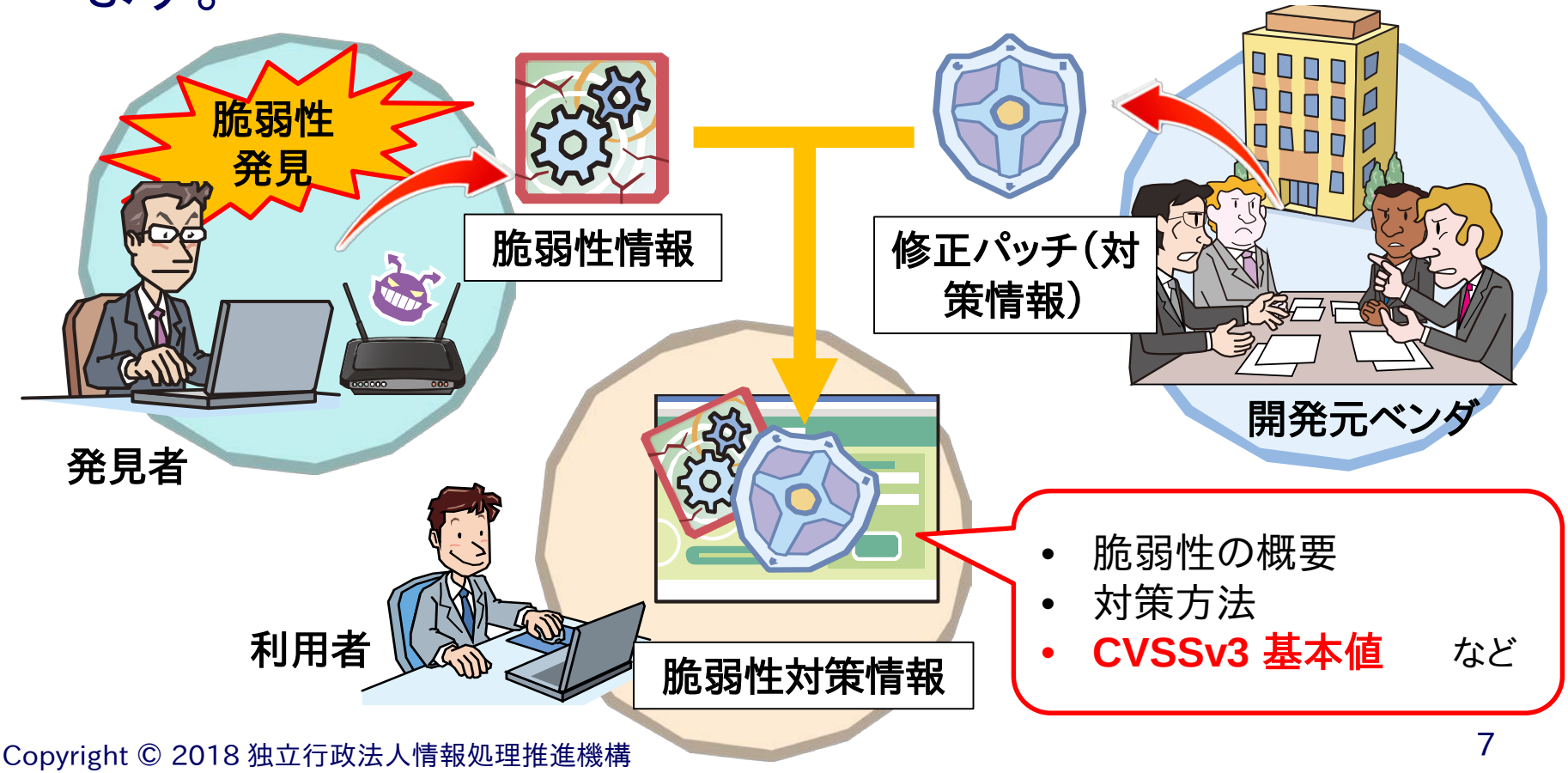
「サービス妨害（DoS）」×「攻撃観測あり」×「対外システムで利用」
＝**深刻度 高**

本日の内容

- はじめに
- CVSSとは
- 基本評価基準(Base Metrics)
- 現状評価基準(Temporal Metrics)
- 環境評価基準(Environmental Metrics)
- まとめ

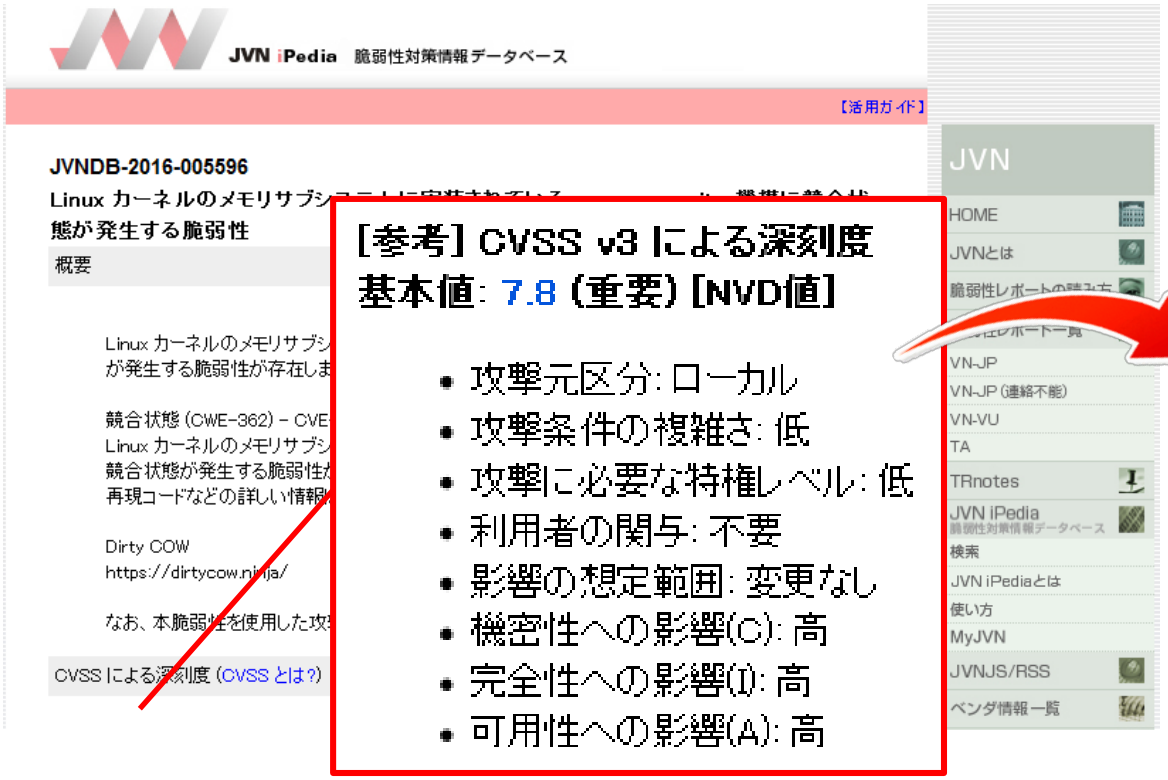
基本評価基準(Base Metrics)

- 一般的に、脆弱性が発見されると、その脆弱性の修正を行い利用者に向けて脆弱性対策情報の公開を行います。



基本評価基準(Base Metrics)

- JVN iPedia 脆弱性対策情報データベースでも CVSSv3 基本値を公開



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

基本評価基準(Base Metrics)

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)
	攻撃にユーザの関与が必要か否か ユーザ関与レベル(UI:User Interaction)	要(R)		不要(N)	
	別のコンポーネントへの攻撃による影響範囲 スコープ(S:Scope)	変更なし(U)		変更あり(C)	
攻撃による影響	機密情報の漏えい被害 機密性への影響　(C:Confidentiality Impact)	なし(N)	低(L)		高(H)
	情報の改ざん被害 完全性への影響　(I:Integrity Impact)	なし(N)	低(L)		高(H)
	業務が遅延・停止する被害 可用性への影響 (A:Availability Impact)	なし(N)	低(L)		高(H)

本日の内容

- はじめに
- CVSSとは
- 基本評価基準(Base Metrics)
- 現状評価基準(Temporal Metrics)
- 環境評価基準(Environmental Metrics)
- まとめ

現状評価基準(Temporal Metrics)

- 脆弱性の脅威は、時間経過や状況変化により変化する場合がある

例えば…

脆弱性情報が公開されると、攻撃者も攻撃に悪用する準備をする。

攻撃が流行すれば危険性が増加し、対策の緊急性も高くなる。

現状評価基準(Temporal Metrics)

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 攻撃可能性　(E:Exploitability)	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 対策のレベル　(RL:Remediation Level)	正式 (O)	暫定 (T)	非公式 (W)	なし (U)
情報の信頼性 情報信頼性　(RC:Report Confidence)	_	未確認 (U)	未確証 (R)	確認済 (C)

※すべての項目で未評価 (X:この項目を評価しない) という選択肢があります。

本日の内容

- はじめに
- CVSSとは
- 基本評価基準(Base Metrics)
- 現状評価基準(Temporal Metrics)
- 環境評価基準(Environmental Metrics)
- まとめ

環境評価基準(Environmental Metrics)

- 対象システムのセキュリティ要求度(CR、IR、AR)
  - 対象システムのセキュリティ要求度に応じた評価の重みづけ
- 緩和策後影響度
  - 環境条件を加味した基本評価の再評価

環境評価基準(Environmental Metrics)

- 対象システムのセキュリティ要求度(CR、IR、AR)
  - 脆弱性の脅威度は組織の特性や守るべき情報資産によっても異なる

例えば

ウェブサイトを停止させられる脆弱性

環境評価基準(Environmental Metrics)

- 対象システムのセキュリティ要求度(CR、IR、AR)
  - 対象システムのセキュリティ要求度に応じた評価の重みづけ

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要求度 機密性の要求度(CR:Confidentiality Requirement)	低 (L)	中 (M)	高 (H)
	システムにおける完全性の要求度 完全性の要求度(IR:Integrity Requirement)	低 (L)	中 (M)	高 (H)
	システムにおける可用性の要求度 可用性の要求度(AR:Availability requirement)	低 (L)	中 (M)	高 (H)

環境評価基準(Environmental Metrics)

- 自組織にとっての影響を評価
  - 組織の環境や利用方法によっては、脆弱性の影響が緩和される場合がある。

例えば

自組織の環境では、

- 脆弱性のある製品は、内部ネットワークからのみ利用できる
- 脆弱性のある製品を、別の製品によりバックアップして利用している

環境評価基準(Environmental Metrics)

- 緩和策後影響度
  - 環境条件を加味した基本評価の再評価

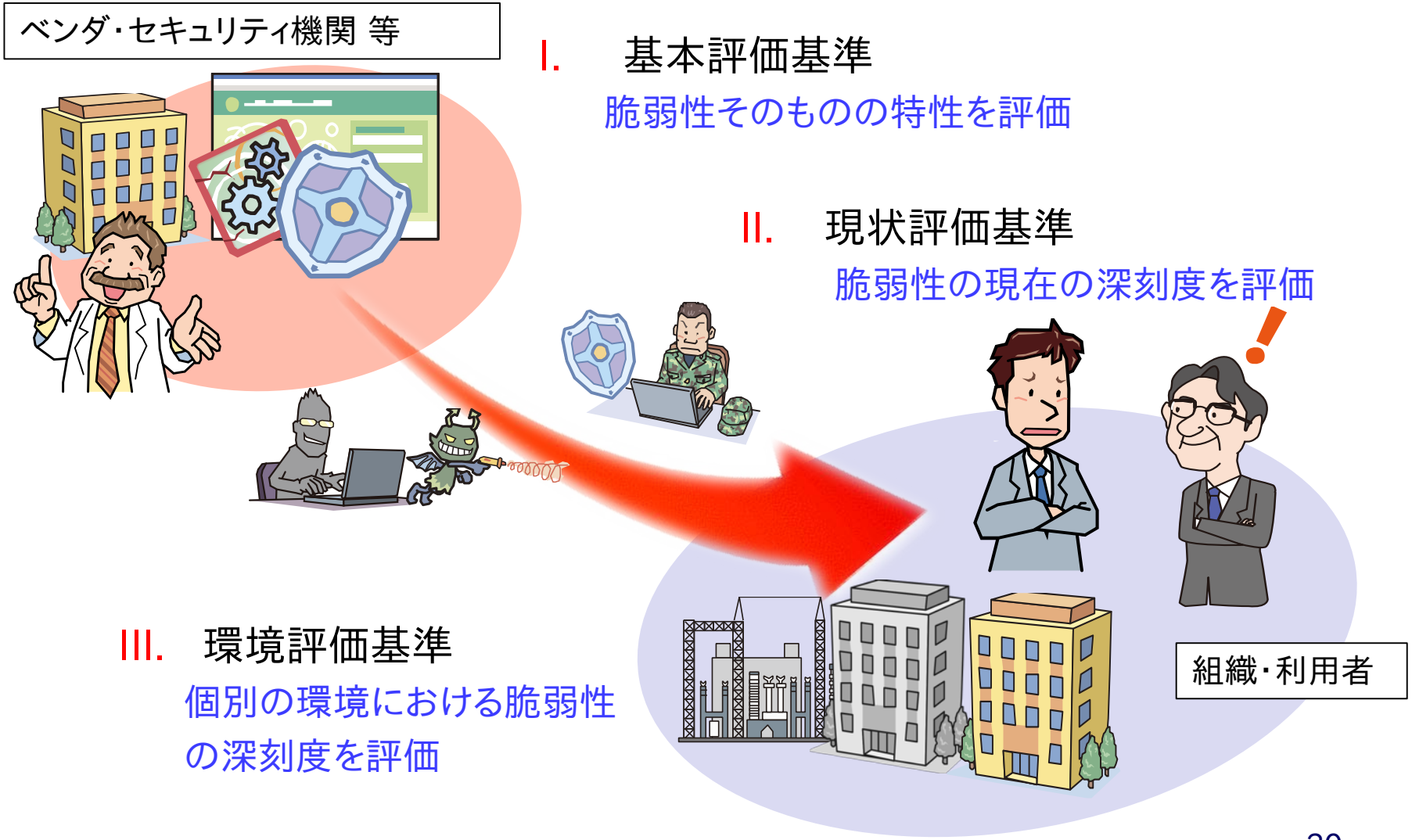
危険小 ← → 危険大

	評価項目	選択肢			
攻撃の難易度	どこから攻撃可能であるか 緩和策後の攻撃元区分(MAV:Modified Attack Vector)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
	緩和策後の攻撃条件の複雑さ 攻撃する際に必要な条件の複雑さ(MAC:Modified Attack Complexity)	高 (H)		低 (L)	
	攻撃する際に必要な特権のレベル 緩和策後の必要な特権レベル(MPR:Modified Privileges Required)	不要 (N)		低 (L)	高 (H)
	攻撃する際に必要なユーザ関与レベル 緩和策後のユーザ関与レベル(MUI:Modified User Interaction)	不要 (N)		要 (R)	
	攻撃による影響範囲 緩和策後のスコープ(MS:Modified Scope)	なし (N)		低 (L)	高 (H)
攻撃による影響	対象とする影響想定範囲の情報が漏えいする可能性 緩和策後の機密性への影響(MC:Modified Confidentiality Impact)	なし (N)		低 (L)	高 (H)
	対象とする影響想定範囲の情報が改ざんされる可能性 緩和策後の完全性への影響(MI:Modified Integrity Impact)	なし (N)		低 (L)	高 (H)
	影響想定範囲の業務が遅延・停止する可能性 緩和策後の可用性への影響(MA:Modified Availability Impact)	なし (N)		低 (L)	高 (H)

本日の内容

- はじめに
- CVSSとは
- 基本評価基準(Base Metrics)
- 現状評価基準(Temporal Metrics)
- 環境評価基準(Environmental Metrics)
- まとめ

まとめ
～各評価基準の活用イメージ～



最後に

- CVSSについてもっと知りたい方は

  共通脆弱性評価システムCVSS v3概説

  https://www.ipa.go.jp/security/vuln/CVSSv3.html

IPA　CVSS　[検索]

脆弱性対策は日々の情報収集と
タイムリーな対策が重要です。
危険な脆弱性を放置しないよう、
適切な対応を行いましょう。