IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

「CVSS」を使いこなすための勘所
～ウェブサイト運営者になって～
＜参考資料＞

独立行政法人 情報処理推進機構（IPA）
セキュリティセンター
情報セキュリティ技術ラボラトリー

2010年12月6日公開

評価の解説　＜基本評価値＞

基本評価値

基本評価値の項目と選択肢

項目	選択肢・ポイント		
攻撃元区分 （AV Access Vector） どこから攻撃可能であるか	ローカル 0.395	隣接N/W 0.646	ネットワーク 1.0
攻撃条件複雑さ （AC Access Complexity） 攻撃する際に必要な条件の複雑さ	高 0.35	中 0.61	低 0.71
攻撃前認証要否 （Au Authentication） 攻撃するために認証が必要であるか	複数 0.45	単一 0.56	不要 0.704
機密性への影響 （C Confidentiality Impact） 機密情報が漏えいする可能性	なし 0.0	部分的 0.275	全面的 0.660
完全性への影響 （I Integrity Impact） 情報が改ざんされる可能性	なし 0.0	部分的 0.275	全面的 0.660
可用性への影響 （A Availability Impact） 業務が遅延・停止する可能性	なし 0.0	部分的 0.275	全面的 0.660

4つの式で算出

式1　影響度 = 10.41×(1 − (1 − C) × (1 − I) × (1 − A))

式2　攻撃容易性 = 20×AV×AC×Au

式3　f(影響度) = 0 (影響度が0の場合), 1.176 (影響度が0以外の場合)

式4　基本値 = ((0.6×影響度) + (0.4×攻撃容易性) −1.5) ×f(影響度)　（小数点第 2 位四捨五入）

攻撃元区分(AV)

《概要》

脆弱性のあるシステムをどこから攻撃可能であるかを評価

《選択肢》

- 【ネットワーク】

  対象システムをネットワーク経由でリモートから攻撃可能である場合に評価
  メールの添付やウェブを経由するものも対象

- 【隣接ネットワーク】

  対象システムをローカル IP サブネット、ブルートゥース、 IEEE 802.11などから攻撃する必要がある場合に評価

- 【ローカル】

  対象システムを物理アクセスやIEEE 1394、USB 経由、ローカルアクセス権限から攻撃する必要がある場合に評価

攻撃条件の複雑さ(AC)

《概要》

脆弱性のあるシステムを攻撃する際に必要な条件の複雑さを評価

《選択肢》

- 【低】

  特別な攻撃条件を必要とせず、対象システムを常に攻撃可能である

- 【中】

  特定のグループのシステムやユーザに対してのみ攻撃可能である
  攻撃前にいくつかの情報収集が必要である
  攻撃するには、標準以外の設定になっている必要がある
  誘導させて行う攻撃は中以上になる

- 【高】

  攻撃前に権限昇格や偽装、疑われやすい方法での情報収集が必要である
  対象システムが特定の設定の場合のみ攻撃可能である

重要:攻撃コードの作成の技術的な難しさは考慮しない

攻撃前の認証要否（Au）

《概要》

脆弱性を攻撃するために対象システムの認証が必要であるかどうかを評価

《選択肢》

- 【なし】

  攻撃前に認証（ログイン等）が不要である

- 【単一】

  攻撃前に認証（ログイン等）が必要である

- 【複数】

  攻撃する場合、2つ以上の認証（ログイン等）が必要である

機密性への影響(C)

《概要》

脆弱性を攻撃された際に、対象システム内の機密情報が漏えいする可能性を評価

《選択肢》

- 【全面的】
  - メモリやファイルにある機密情報が全て参照可能である
  - 重要なシステムファイルが全て参照可能である
- 【部分的】
  - 一部の機密情報が参照可能である
  - 一部の重要なシステムファイルが参照可能である
- 【なし】
  - システムの機密性に影響はない

完全性への影響(I)

《概要》

脆弱性を攻撃された際に、対象システム内の情報が改ざんされる可能性を評価

《選択肢》

- 【全面的】
  - システム全体の情報が改ざん可能である
  - システム保護機能を全て回避し、情報が改ざん可能である
- 【部分的】
  - 一部の情報が改ざん可能である
  - 一部のシステムファイルが改ざん可能である
- 【なし】
  - システムの完全性に影響はない

可用性への影響(A)

《概要》

脆弱性を攻撃された際に、対象システム内の業務が遅延・停止する可能性を評価

《選択肢》

- 【全面的】

  リソース(ネットワーク帯域、プロセッサ処理、ディスクスペースなど)を完全に枯渇させることが可能である

  システムを完全に停止させることが可能である

- 【部分的】

  リソースを一部枯渇させることが可能である

  業務の遅延や一時中断が可能である

- 【なし】

  システムの可用性に影響はない

評価の解説　＜現状評価値＞

現状評価値

現状評価値の項目と選択肢

項目	選択肢・ポイント			
攻撃可能性　(E Exploitability) どこから攻撃可能であるか	未実証 0.85	実証可 0.90	攻撃可 0.95	容易 1.00
対策のレベル　(RL Remediation Level) 対策がどの程度利用可能であるか	正式 0.87	暫定 0.90	非公式 0.95	なし 1.00
情報信頼性　(RC Report Confidence) 情報の信頼性	-	未確認 0.90	未確証 0.95	確認済 1.00

※現状値は全ての値で未評価<1.00>(この項目を評価しない)という項目がある

1つの式で算出
式5　現状値 = 基本値 ×E×RL×RC
（小数点第 2 位四捨五入）

攻撃される可能性(E)

《概要》

攻撃コード・攻撃手法が実際に利用可能であるかを評価

《選択肢》

- 【容易に攻撃可能】
  攻撃コードがいかなる状況でも利用可能である
  攻撃コードを必要とせず、攻撃可能である

- 【攻撃可能】
  攻撃コードが存在し、ほとんどの状況で使用可能である

- 【実証可能】
  実証コードが存在している
  完成度の低い攻撃コードが存在している

- 【未実証】
  実証コードや攻撃コードが利用可能でない
  攻撃手法が理論上のみで存在している

利用可能な対策のレベル(RL)

《概要》

脆弱性の対策がどの程度利用可能であるかを評価

《選択肢》

- 【なし】
  利用可能な対策がない
  対策を適用できない

- 【非公式】
  製品開発者以外からの非公式な対策が利用可能である

- 【暫定】
  製品開発者からの暫定対策が利用可能である

- 【正式】
  製品開発者からの正式対策が利用可能である

脆弱性情報の信頼性（RC）

《概要》

脆弱性の対策がどの程度利用可能であるかを評価

《選択肢》

－【確認済】

製品開発者が脆弱性情報を確認している
脆弱性情報が実証コードや攻撃コードなどにより広範囲に確認されている

－【未確証】

セキュリティベンダーや調査団体から、複数の非公式情報が存在している

－【未確認】

未確認の情報が１件のみ存在している
いくつかの相反する情報が存在している

評価の解説　＜環境評価値＞

環境評価値

環境評価値の項目と選択肢

項目	選択肢・ポイント				
二次的被害（CDP Collateral Damage Potential） システムからの二次的被害の可能性	なし 0.0	軽微 0.1	中程度 0.3	重大 0.4	壊滅的 0.5
システム範囲（TD Target Distribution） システムの影響範囲	-	なし 0.00	小規模 0.25	中規模 0.75	大規模 1.00
機密性の要求度（CR Confidentiality Requirement） システムにおける機密性の重要度	-	-	低 0.5	中 1.0	高 1.51
完全性の要求度（IR Integrity Requirement） システムにおける完全性の重要度	-	-	低 0.5	中 1.0	高 1.51
可用性の要求度（AR Availability Impact） システムにおける可用性の重要度	-	-	低 0.5	中 1.0	高 1.51

※環境値は全ての値で未評価<CDP：0.0，その他：1.00>（この項目を評価しない）という項目がある

3つの式で算出

式6　調整後影響度 = min（10.0,10.41×（1-（1-C×CR）×（1-I×IR）×（1-A×AR））

式7　調整後現状値 = 式3　式4　の影響度に、式6の調整後影響度の計算結果を代入し、基本値を再計算する。その基本値で式5の現状値を再計算する。

式8　環境値 =（ 調整後現状値 +（10- 調整後現状値 ）×CDP）×TD　（小数点第 2 位四捨五入）

二次的被害の可能性（CDP）

《概要》

対象システムが脆弱性を攻撃された場合の物理的な機器への被害や、生活基盤、身体などへ及ぼす二次的な被害の可能性を評価

《選択肢》

- 【壊滅的】
  攻撃が成功すると壊滅的な被害が発生する可能性がある
- 【重大】
  攻撃が成功すると重大な被害が発生する可能性がある
- 【中程度】
  攻撃が成功すると中程度の被害が発生する可能性がある
- 【軽微】
  攻撃が成功すると軽微な被害が発生する可能性がある
- 【なし】
  攻撃されても二次的な被害が発生しない

影響を受ける対象システムの範囲（TD）

《概要》

利用環境の中で、脆弱性を攻撃される可能性のある対象システムを利用している範囲を評価

《選択肢》

- 【大規模】

  対象システムが広範囲に存在し、利用環境の76～100%にリスクがある

- 【中規模】

  対象システムが存在するが、中程度の範囲で、利用環境の26～75%にリスクがある

- 【小規模】

  対象システムが存在するが、小程度の範囲で、利用環境の1～25%にリスクがある

- 【なし】

  対象システムが全く存在しない

  対象システムが物理的に隔離されていて、利用環境へのリスクがない

対象システムのセキュリティ要求度（CR, IR, AR）

《概要》

- 対象システムが要求されるセキュリティ特性に関して、その該当項目(「機密性(C)」、「完全性(I)」、「可用性(A)」)を重視する場合、その該当項目を高く評価
- 「機密性の要求度 (Confidentiality Requirement, CR) 」、「完全性の要求度 (Integrity Requirement, IR) 」、「可用性の要求度 (Availability Requirement, AR) 」を評価

《選択肢》

- 【高】
  対象システムの該当項目を失われると、壊滅的な影響がある
- 【中】
  対象システムの該当項目を失われると、深刻な影響がある
- 【低】
  対象システムの該当項目を失われても、一部の影響にとどまる