

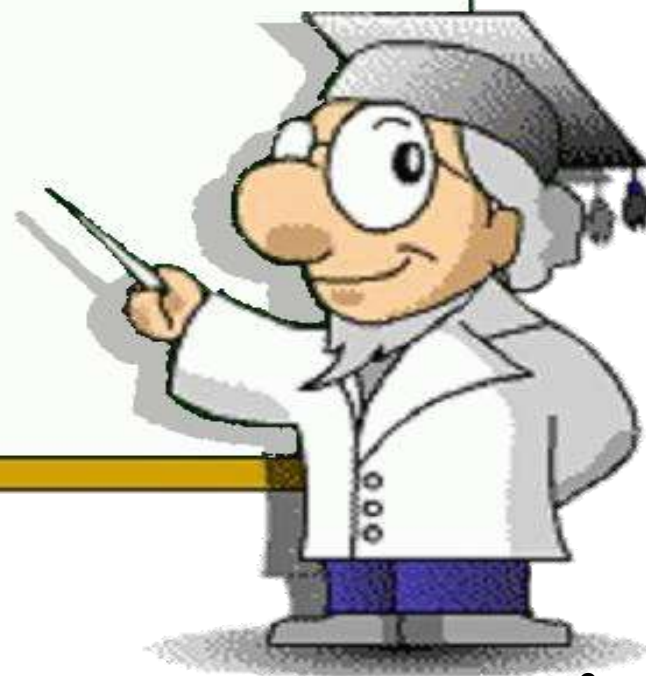
「CVSS」を使いこなすための勘所 ～ウェブサイト運営者になって～

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

アジェンダ

1. はじめに
2. CVSSの基本
3. 評価項目と評価値
4. 評価してみよう（実践編）
5. 評価してみよう（解答編）



1. はじめに

本セッションでは、CVSSの評価を実際に体験していただきます。

CVSSの評価をハンズオンで実施していただき、CVSSの理解を深めましょう！



2. CVSSの基本

CVSSの目的

- 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、とても深刻なものか、さほど深刻ではないものなのか、評価することができる。

- 脆弱性対策に優先順位をつける

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

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**評価基準なので、異なった製品間の脆弱性を比較する物差しになる。
- **多数の組織が支持している**
国内外**30組織以上**が採用を支持しているため、同じ視点で評価作業を進めることが容易。
- **オープンである**
評価方法は公開されており、**誰でもCVSSスコアを採点**することができる。

3. 評価項目と評価値

3種類の評価値

項目毎の選択肢から度合いを決定し算出

基本値
0.0 ~ 10.0

脆弱性の技術的な特性を評価
例: システムの乗っ取りが可能なら高評価

現状値
0.0 ~ 10.0

ある時点における脆弱性を取巻く状況を評価
例: ゼロデイ攻撃があれば高評価

環境値
0.0 ~ 10.0

その利用者における問題の大きさを評価
例: 社内の基幹システムで利用なら高評価

基本評価

基本評価の項目と選択肢

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つの式で基本値を算出

式1 影響度 = $10.41 \times (1 - (1 - C) \times (1 - I) \times (1 - A))$

式2 攻撃容易性 = $20 \times AV \times AC \times Au$

式3 $f(\text{影響度}) = 0$ (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 = $((0.6 \times \text{影響度}) + (0.4 \times \text{攻撃容易性}) - 1.5) \times f(\text{影響度})$ (小数点第2位四捨五入)

現状評価

現状評価の項目と選択肢

項目	選択肢・ポイント			
攻撃可能性 (E Exploitability) <small>どこから攻撃可能であるか</small>	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) <small>対策がどの程度利用可能であるか</small>	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) <small>情報の信頼性</small>	-	未確認 0.90	未確認 0.95	確認済 1.00

※ 現状評価は全ての項目で未評価<1.00> (この項目を評価しない) という選択肢がある

1つの式で現状値を算出

式5 現状値 = 基本値 × E × RL × RC
 (小数点第 2 位四捨五入)

環境評価

環境評価の項目と選択肢

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

※ 環境評価は全ての項目で未評価<CDP:0.0, その他:1.00> (この項目を評価しない) という選択肢がある

3つの式で環境値算出

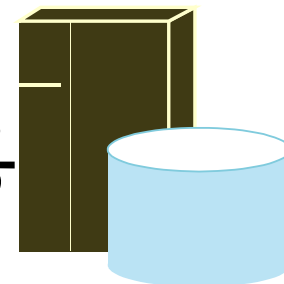
式6 調整後影響度 = $\min(10.0, 10.41 \times (1 - (1 - C \times CR) \times (1 - I \times IR) \times (1 - A \times AR)))$

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)₁₁

例題 想定するウェブサイト

あなたはウェブサイト「脆弱性対策情報DB」の運用者です。
「脆弱性対策情報DB」は日々脆弱性対策情報を蓄積しています。
「IPA Vuln Web DB」というウェブアプリケーションを使用しています



利用者は、ウェブブラウザから「脆弱性対策情報DB」へアクセスし、内容を閲覧・検索することができます。
ユーザ登録により各脆弱性対策情報にコメントをすることができます。
内容の閲覧・検索は「IPA Vuln Web DB」の機能です。



運用者は、「IPA Vuln Web DB」を通して、日々収集している脆弱性対策情報を蓄積していきます。



IPA Vuln Web DBは、架空の製品です。

例題 基本評価値

「IPA Vuln Web DB」の脆弱性が発見されました！
基本評価値を付けてみましょう。

IPA Vuln Web DBにおけるSQLインジェクションの脆弱性

<概要>

IPA Vuln Web DBにはSQLインジェクションの脆弱性があります。

<想定される影響>

遠隔の第三者が、細工したHTTPリクエストを送信することで、
認証なしにそのサイトで使用しているDBを操作（内容の取得・
編集・削除）できてしまいます。

例題 基本評価値

選択してみよう！

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	隣接N/W	ネットワーク
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	中	低
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	単一	不要
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	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

例題 基本評価値 解答

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	隣接N/W	ネットワーク
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	中	低
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	単一	不要
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	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

例題 基本評価値 解説

IPA Vuln Web DBにおける SQL インジェクションの脆弱性		
評価項目	選択肢	理由
攻撃元区分 (AV)	ネットワーク	遠隔の第三者からの攻撃である
攻撃条件の複雑さ (AC)	低	細工したURLを用意し、そのURLへアクセスするだけ
攻撃前の認証要否 (Au)	なし	認証なしにDBを操作
機密性への影響 (C)	部分的	DBを操作 (内容の取得・編集・削除) DBの情報が漏えいする可能性がある
完全性への影響 (I)	部分的	DBを操作 (内容の取得・編集・削除) DBの情報を編集される可能性がある
可用性への影響 (A)	部分的	DBを操作 (内容の取得・編集・削除) DBの情報を削除されウェブサイトが機能しなくなる可能性がある

結果
7.5

例題 現状評価値

「IPA Vuln Web DB」の公開されている状況は次のとおりです。
現状評価値を付けてみましょう。

IPA Vuln Web DBにおけるSQLインジェクションの脆弱性

＜製品開発者による情報発信＞

IPA Vuln Web DBの開発者が公式サイト上で脆弱性の存在を確認したことを発表。

同サイトで、検索機能のオフを行うことによる暫定的な対策を発表。

＜第三者による情報発信＞

脆弱性を実証するためのコードが第三者のブログで公表されている。

例題 現状評価値

選択してみよう！

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

例題 現状評価値 解答

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	実証可	攻撃可	容易
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	暫定	非公式	なし
情報信頼性 (RC Report Confidence) 情報の信頼性	-	未確認	未確認	確認済

例題 現状評価値 解説

IPA Vuln Web DBにおける SQL インジェクションの脆弱性		
評価項目	選択肢	理由
攻撃可能性 (E)	実証可能	実証コードがブログで公開される
対策レベル (RL)	暫定	検索機能のオフを行うことによる暫定的な対策
情報の信頼性 (RC)	確認済	IPA Vuln Web DBの開発者が脆弱性の存在を確認したことを発表。

結果

6.1

例題 環境評価値

「IPA Vuln Web DB」を使用している環境は次の通りです。
所属チームとしての環境評価値を付けてみましょう。

<前提>

運用チームは「脆弱性対策DB」のサイト運用をメイン業務としている。
運用チームでは環境値評価に当たって、システムへの影響を評価する。

<二次的被害>

「脆弱性対策DB」は独立したシステムで、会社内の他のシステムとの連携はない。

<システムの範囲>

会社が運用するサイトは「脆弱性対策DB」以外にも多数あるが、運用チームが考える対象は「脆弱性対策DB」サイトのみである。

<機密性・完全性・可用性の要求度>

個人情報など機微な情報は取り扱っていない。作成中の原稿は漏えいしたくない。
掲載内容の改ざんや、サイトにウイルスを埋め込みをされてはならない。
数日止まるのは困るが、
常に稼働していなければならないという程のシステムではない。

例題 環境評価値

選択してみよう！

項目	選択肢				
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	軽微	中程度	重大	壊滅的
システム範囲 (TD Target Distribution) システムの影響範囲	-	なし	小規模	中規模	大規模
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	中	高
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	中	高
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	中	高

例題 環境評価値 解答

項目	選択肢				
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	軽微	中程度	重大	壊滅的
システム範囲 (TD Target Distribution) システムの影響範囲	-	なし	小規模	中規模	大規模
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	中	高
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	中	高
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	中	高

例題 環境評価値 解説

IPA Vuln Web DB		
評価項目	選択肢	理由
二次的被害 (CDB)	なし	他のシステムとの連携はない
システム範囲 (TD)	大規模	チームとしての業務では、大きな範囲の影響を被ると判断
機密性の要求度 (CR)	低	個人情報など機微な情報は取り扱っていない
完全性の要求度 (IR)	高	掲載内容の改ざんや、サイトにウイルスを埋め込みをされてはならない。
可用性の要求度 (AR)	中	数日止まるのは困るが、常に稼働していなければならないという程のシステムではない。

結果

6.2

4. 評価してみよう（実践編）

～ 5つの脆弱性の基本値の評価（ハンズオン）～

評価を試してみよう（1）

IPA Server OS*2におけるサービス運用妨害（DoS）の脆弱性

<概要>

IPA Server OSにはICMPパケットの処理に不備があり、サービス運用妨害（DoS）状態となる脆弱性があります。

<想定される影響>

遠隔の第三者が、細工したICMPパケットを送付することで、認証なしにIPA Server OSをシャットダウンさせることができます。

*2:IPA Server OSは、架空の製品です。

評価を試してみよう (2)

IPA Vuln Web DBにおけるSQLインジェクションの脆弱性

<概要>

IPA Vuln Web DBには、SQLインジェクションの脆弱性が存在します。

<想定される影響>

IPA Vuln Web DBにログイン可能な利用者が、細工したコメントを送付することによってそのサイトで使用しているDBを操作(内容の取得・編集・削除)できてしまいます。

評価をしてみよう（3）

IPA Vuln Web DBにおけるクロスサイト・スクリプティングの脆弱性

<概要>

IPA Vuln Web DB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。

<想定される影響>

利用者がIPA Vuln Web DBの検索ページに関する細工を施されたURLにアクセスしてしまうことで任意のスクリプトを実行されてしまいます。

評価を試してみよう（４）

IPA Server OSにおけるバッファオーバーフローの脆弱性

<概要>

IPA Server OSにはICMPパケットの処理に不備があり、バッファオーバーフローの脆弱性があります。

<想定される影響>

遠隔の第三者が、細工したICMPパケットを送付することで、認証なしに、IPA Server OSを完全に制御することができてしまいます。

評価を試してみよう（5）

解凍ソフトAにおけるバッファオーバーフローの脆弱性

<概要>

解凍ソフトAには、ZIPファイルの取り扱いに不備があり、バッファオーバーフローの脆弱性が存在します。

<想定される影響>

細工されたZIPファイルを解凍ソフトAを通して開くことで、解凍ソフトAの動作権限で任意のコードを実行されてしまいます。

解答編

評価を試してみよう（1）

IPA Server OS*2におけるサービス運用妨害（DoS）の脆弱性

<概要>

IPA Server OSにはICMPパケットの処理に不備があり、サービス運用妨害（DoS）状態となる脆弱性があります。

<想定される影響>

遠隔の第三者が、細工したICMPパケットを送付することで、認証なしにIPA Server OSをシャットダウンさせることができます。

解答 (1)

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	隣接N/W	ネットワーク
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	中	低
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	単一	不要
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	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

解答（1）解説

評価項目	選択肢	理由
攻撃元区分 (AV)	ネットワーク	遠隔の第三者からの攻撃である
攻撃条件の複雑さ (AC)	低	細工したICMPパケットを送付するだけ (ICMPパケットの細工の難易度は考慮しない)
攻撃前の認証要否 (Au)	なし	認証なしにシャットダウンさせる
機密性への影響 (C)	なし	情報漏えい等の記載なし
完全性への影響 (I)	なし	システムの改ざん等の記載なし
可用性への影響 (A)	全面的	IPA Server OSをシャットダウンさせる

結果

7.8

評価を試してみよう (2)

IPA Vuln Web DBにおけるSQLインジェクションの脆弱性

<概要>

IPA Vuln Web DBには、SQLインジェクションの脆弱性が存在します。

<想定される影響>

IPA Vuln Web DBにログイン可能な利用者が、細工したコメントを送付することによってそのサイトで使用しているDBを操作(内容の取得・編集・削除)できてしまいます。

解答 (2)

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	隣接N/W	ネットワーク
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	中	低
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	単一	不要
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	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

解答 (2) 解説

評価項目	選択肢	理由
攻撃元区分 (AV)	ネットワーク	遠隔の第三者からの攻撃である
攻撃条件の複雑さ (AC)	低	細工したコメントを送付するだけ
攻撃前の認証要否 (Au)	単一	IPA Vuln Web DBにログイン可能な利用者
機密性への影響 (C)	部分的	DBを操作 (内容の取得・編集・削除) DBの情報が漏えいする可能性がある
完全性への影響 (I)	部分的	DBを操作 (内容の取得・編集・削除) DBの情報を編集される可能性がある
可用性への影響 (A)	部分的	DBを操作 (内容の取得・編集・削除) DBの情報を削除されウェブサイトが機能しなくなる可能性がある

結果

6.5

評価を試してみよう (3)

IPA Vuln Web DBにおけるクロスサイト・スクリプティングの脆弱性

<概要>

IPA Vuln Web DB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。

<想定される影響>

利用者がIPA Vuln Web DBの検索ページに関する細工を施されたURLにアクセスしてしまうことで任意のスクリプトを実行されてしまいます。

解答 (3)

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	隣接N/W	ネットワーク
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	中	低
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	単一	不要
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	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

解答 (3) 解説

評価項目	選択肢	理由
攻撃元区分 (AV)	ネットワーク	遠隔の第三者からの攻撃である
攻撃条件の複雑さ (AC)	中	利用者を細工を施したURLにアクセスさせる必要
攻撃前の認証要否 (Au)	なし	攻撃の際、該当システムへの認証はない
機密性への影響 (C)	なし	IPA Vuln Web DBの情報が漏えいするわけではない
完全性への影響 (I)	部分的	利用者が表示した際に意図しないスクリプトが実行される *スクリプトの内容は考慮しない
可用性への影響 (A)	なし	IPA Vuln Web DBが停止するわけではない。

結果

4.3

評価を試してみよう（４）

IPA Server OSにおけるバッファオーバーフローの脆弱性

<概要>

IPA Server OSにはICMPパケットの処理に不備があり、バッファオーバーフローの脆弱性があります。

<想定される影響>

遠隔の第三者が、細工したICMPパケットを送付することで、認証なしに、IPA Server OSを完全に制御することができてしまいます。

解答 (4)

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	隣接N/W	ネットワーク
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	中	低
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	単一	不要
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	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

解答（４）解説

評価項目	選択肢	理由
攻撃元区分 (AV)	ネットワーク	遠隔の第三者からの攻撃である
攻撃条件の複雑さ (AC)	低	細工したICMPパケットを送付するだけ (ICMPパケットの細工の難易度は考慮しない)
攻撃前の認証要否 (Au)	なし	認証なしに完全に制御
機密性への影響 (C)	全面的	完全に制御されるので、情報を取得することも可能
完全性への影響 (I)	全面的	完全に制御されるので、全て改ざんすることも可能
可用性への影響 (A)	全面的	完全に制御されるので、システム上の全てのファイルを消去することも可能

結果

10.0

評価を試してみよう（5）

解凍ソフトAにおけるバッファオーバーフローの脆弱性

<概要>

解凍ソフトAには、ZIPファイルの取り扱いに不備があり、バッファオーバーフローの脆弱性が存在します。

<想定される影響>

細工されたZIPファイルを解凍ソフトAを通して開くことで、解凍ソフトAの動作権限で任意のコードを実行されてしまいます。

解答 (5)

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	隣接N/W	ネットワーク
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	中	低
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	単一	不要
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	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

解答 (5) 解説

評価項目	選択肢	理由
攻撃元区分 (AV)	ネットワーク	攻撃のシナリオとしては、メール等で送付することを想定する。
攻撃条件の複雑さ (AC)	中	メール等で送付した後、ファイルを開かせるという利用者のアクションが必要になる。
攻撃前の認証要否 (Au)	なし	メールを送付する場合、認証は特に必要ない。
機密性への影響 (C)	部分的	任意のコードの実行の結果、情報が漏えいする可能性あり。 プログラムの実行権限は一般ユーザを想定する。
完全性への影響 (I)	部分的	任意のコードの実行の結果、ファイル等を改ざんする可能性あり。
可用性への影響 (A)	部分的	任意のコードの実行の結果、重要ファイルの消去される可能性あり。

結果

6.8

まとめ

まとめ

- CVSS値の評価をできることで、自社製品の脆弱性対策情報に活用できます。
- 評価結果は数値化されるため、対策の優先度の指標とすることができます。
- CVSS値の計算には、JVN iPediaのCVSS計算機が便利です。

JVN iPediaとCVSS計算機

<http://jvndb.jvn.jp/cvss/>



JVN iPedia Vulnerability Countermeasure Information Database

JVN iPediaにはCVSS計算機があります。

- 脆弱性対策情報に現状値・環境値の代入ができる。
- 自分でCVSS値を計算する際に利用できる。



CVSS による深刻度 (CVSS とは?)

基本値 4.0 (警告) [IPA値]

- ・ 攻撃元区分: ネットワーク
- ・ 攻撃条件の複雑さ: 低
- ・ 攻撃前の認証要否: 単一
- ・ 機密性への影響(C): なし
- ・ 完全性への影響(I): なし
- ・ 可用性への影響(A): 部分的

各脆弱性対策情報内
「CVSSによる深刻度」

リンクをクリック

JVNDB-2010-002129

基本値は 4.0

現状値は N/A

環境値は N/A

全1部制訂値は 4.0

基本値

攻撃の可能性について

攻撃元区分 (AV: Access Vector) ネットワークから攻撃可能 (Network)

攻撃条件の複雑さ (AC: Access Complexity) 低 (Low)

攻撃前の認証要否 (Au: Authentication) 単一認証操作が必要 (Single Instance)

影響について

機密性への影響 (情報漏洩の可能性がある。Confidentiality Impact) 影響なし (None)

完全性への影響 (情報改ざんの可能性。Integrity Impact) 影響なし (None)

可用性への影響 (業務停止の可能性。Availability Impact) 部分的な影響に留まる (Partial)

現状値

CVSS 2.0 JVN iPedia

脆弱化される可能性 (E: Exploitability) 未評価 (Undefined)

利用可能な対策のレベル (RL: Remediation Level) 未評価 (Undefined)

脆弱性情報の信頼性 (RC: Report Confidence) 未評価 (Undefined)

環境値

影響の程度について

二次的被害の可能性 (CDP: Collateral Damage Potential) 未評価 (Undefined)

影響を受ける対象システムの範囲 (TD: Target Distribution) 未評価 (Undefined)

要求の程度について

機密性の要求度 (CR: Confidentiality Requirement) 未評価 (Undefined)

完全性の要求度 (IR: Integrity Requirement) 未評価 (Undefined)

可用性の要求度 (AR: Availability Requirement) 未評価 (Undefined)