４．脆弱性の評価事例

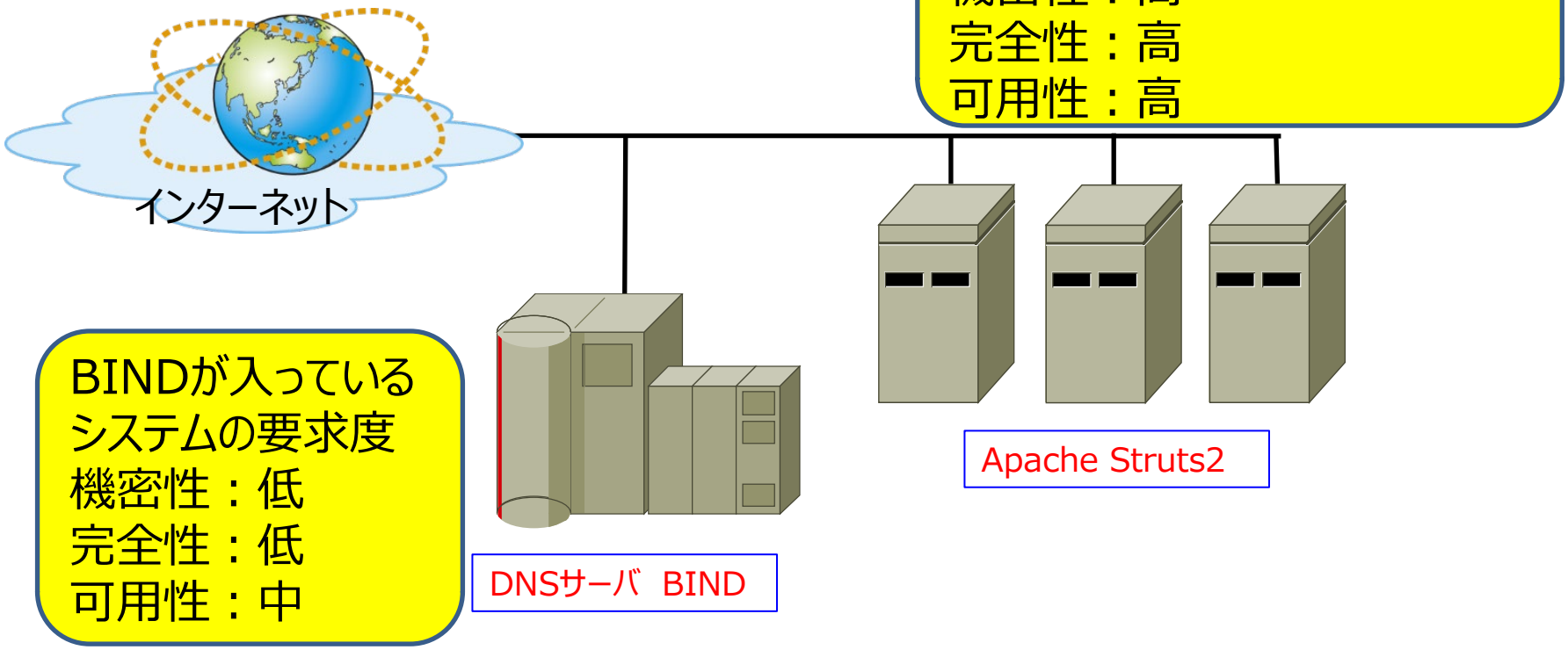
実際のケースによる理解
～情報収集や分析を行ってみましょう～

- １．DNSサーバBINDの脆弱性を確認したケース
- ２．Apache Struts2の脆弱性を確認したケース

✓ 実際に脆弱性を確認した際に、どういった情報を入手すべきなのか、分析結果はどうなるのかを見ていきしょう。

システムの運用環境

■運用環境



✓ 予め、各製品に要求される要求度を設定

組織の対応方針

CVSSの分析結果で組織の対応方針を策定

例）

CVSS環境値	選択肢
7.0-10.0	即時に脆弱性対策を実施する
4.0-6.9	1ヶ月以内に対策を実施する
0.1-3.9	3ヶ月以内に対策を実施する
0.0	対策の必要なし

※上記対応方針はあくまで一例となります

■ケース1
BINDの脆弱性を確認したケースを見てみましょう

BINDの脆弱性を確認したケース
～対応方針決定までの流れについて～

- **BINDの脆弱性を確認したケースは以下の流れで進めます。**

① ニュースサイトなどから脆弱性の情報を入手する
② 関連情報をベンダサイトやセキュリティ関連のサイトから収集する
③ 収集した情報を分析・評価し、対応策を決定する

BINDの脆弱性を確認したケース
～① ニュースサイトなどから情報を入手する～

「BIND 9」に複数の脆弱性 - DoS攻撃受けるおそれ

DNSサーバ「BIND 9」に複数の脆弱性が含まれていることがわかった。開発元や関連機関では注意を呼びかけている。

EDNSオプションにおける特定の組み合わせを処理した場合にメモリリークが生じて「BIND」や設定によってはシステムのメモリが枯渇し、サービス拒否に陥るおそれがある「CVE-2018-5744」が明らかとなったもの。

リモートより攻撃することが可能で「権威DNSサーバ」「キャッシュDNSサーバ」の双方に影響がある。悪用は確認されていない。重要度は4段階中2番目にあたる「高（High）」とレーティングされている。

また外部データベースを利用してゾーンデータを扱う「DLZ（Dynamically Loadable Zones）」を利用した場合に、転送許可されていない場合でもゾーン転送が行われ、ゾーンデータが流出するおそれがある「CVE-2019-6465」が判明。

さらに攻撃者が用意したキーを読み込ませる必要があるため、悪用は難しいと見られるが、DNSSECにおけるトラストアンカーの管理に用いる「managed-keys」の処理でクラッシュし、サービス拒否が生じるおそれがある脆弱性「CVE-2018-5745」が明らかとなった。

「CVE-2019-6465」「CVE-2018-5745」の重要度は、1段階低く、上から3番目にあたる「中（Medium）」とレーティングされている。悪用は確認されていない。

Internet Systems Consortium（ISC）は、これら脆弱性に対処した「同9.12.3-P4」「同9.11.5-P4」をリリース。日本レジストリサービス（JPRS）をはじめ、関係機関では注意喚起を行っている。

（Security NEXT - 2019/02/22 ） ツイート

◆ニュースサイト

ニュースサイトから判明したこと

- 脆弱性の存在有無
- CVE番号
- 重要度
- 修正版のバージョン

出典：Security NEXT
http://www.security-next.com/102783

BINDの脆弱性が確認されたケース
～② 関連情報を収集する～

◆開発ベンダのサイト

CVE-2018-5744: A specially crafted packet can cause named to leak memory

Updated on 21 Feb 2019　2 minutes to read | Contributors Michael McNally

CVE: CVE-2018-5744

Document version: 2.0

Posting date: 21 February 2019

Program impacted: BIND

Versions affected: BIND 9.10.7 -> 9.10.8-P1, 9.11.3 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions
Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected.

Severity: High

Solution:

Upgrade to a version of BIND containing a fix for the memory leak.

- BIND 9.11.5-P4
- BIND 9.12.3-P4

BIND Supported Preview Edition is a special feature preview branch of BIND provided to eligible ISC support customers.

- BIND 9.11.5-S5

Acknowledgements: ISC would like to thank Toshifumi Sakaguchi for reporting this issue to us.

ベンダ情報から判明したこと

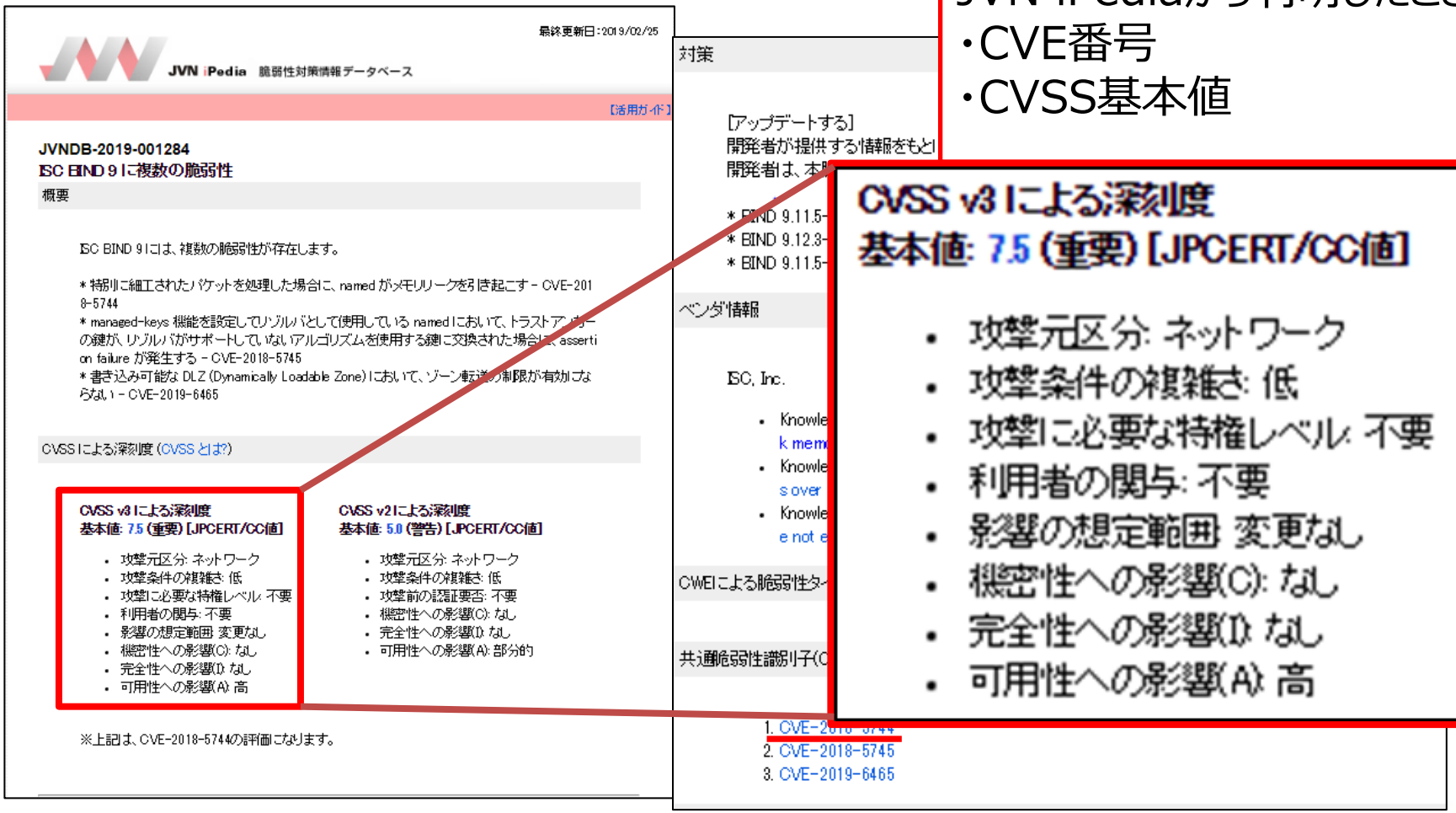
- CVE番号
- 危険度
- 影響を受けるバージョン
- 解決策

出典：ISC
https://kb.isc.org/docs/cve-2018-5744

BINDの脆弱性が確認されたケース
～② 関連情報を収集する～

◆脆弱性データベースの情報(JVN iPedia)

JVN iPediaから判明したこと
・CVE番号
・CVSS基本値



最終更新日：2019/02/25

JVN iPedia 脆弱性対策情報データベース

【活用ガイド】

JVNDB-2019-001284
ISC BIND 9 に複数の脆弱性

概要

ISC BIND 9 には、複数の脆弱性が存在します。

* 特別に細工されたパケットを処理した場合に、named がメモリリークを引き起こす - CVE-2018-5744
* managed-keys 機能を設定してリゾルバとして使用している named において、トラストアンカーの鍵が、リゾルバがサポートしていないアルゴリズムを使用する鍵に交換された場合に、assertion failure が発生する - CVE-2018-5745
* 書き込み可能な DLZ (Dynamically Loadable Zone) において、ゾーン転送の制限が有効にならない - CVE-2019-6465

CVSS による深刻度 (CVSS とは?)

CVSS v3 による深刻度
基本値: 7.5 (重要) [JPCERT/CC値]

- 攻撃元区分: ネットワーク
- 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: 不要
- 影響の想定範囲: 変更なし
- 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): 高

CVSS v2 による深刻度
基本値: 5.0 (警告) [JPCERT/CC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: 不要
- 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

※上記は、CVE-2018-5744の評価になります。

対策

[アップデートする]
開発者が提供する情報をもと
開発者は、本

* BIND 9.11.5-
* BIND 9.12.3-
* BIND 9.11.5-

ベンダ情報

ISC, Inc.

- Knowle
  k mem
- Knowle
  s over
- Knowle
  e not e

CWEによる脆弱性タ

共通脆弱性識別子(C

1. CVE-2018-5744
2. CVE-2018-5745
3. CVE-2019-6465

CVSS v3 による深刻度
基本値: 7.5 (重要) [JPCERT/CC値]

- 攻撃元区分: ネットワーク
- 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: 不要
- 影響の想定範囲: 変更なし
- 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): 高

https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-001284.html

BINDの脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

CVSS v3 による深刻度
基本値: 7.5 (重要) [JPCERT/CC値]

- 攻撃元区分: ネットワーク
- 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: 不要
- 影響の想定範囲: 変更なし
- 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): 高

◆CVSS基本評価は？

	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)

BINDの脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

IPA

◆CVSS現状評価は？

参考情報
・攻撃コード等は確認されていない
・対策がベンダから公開されている
・情報がベンダから公開されている

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)

BINDの脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

IPA

◆CVSS環境評価は？

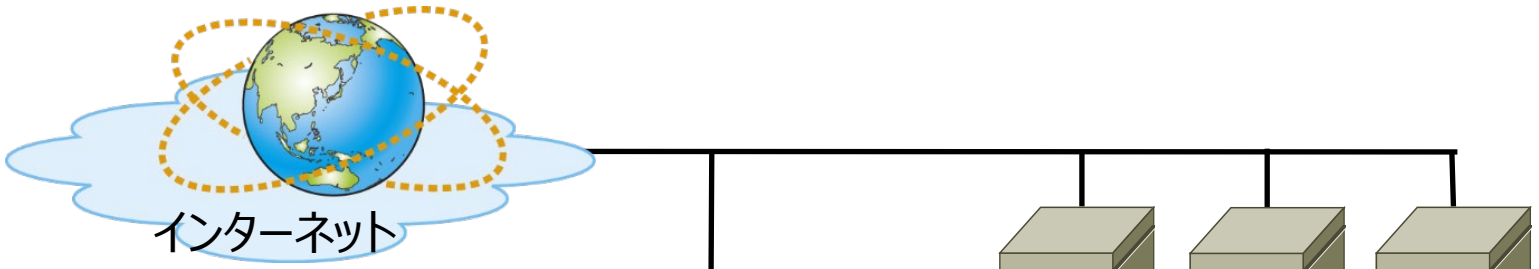
対象システムのセキュリティ要求度

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)

システムの運用環境

■運用環境



BINDへの要求度
機密性：低
完全性：低
可用性：中

システムのネットワークの
環境を考慮して再評価

✓運用状態に合わせて再評価を行う。

BINDの脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

IPA

◆CVSS環境評価は？

対象システムのセキュリティ要求度

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)

BINDの脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

IPA

◆CVSS環境評価は？

評価例）

	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)

スコア算出例（CVSS基本値）

基本評価基準

7.5
(High)

攻撃元区分: Attack Vector (AV)

ネットワーク (N) | 隣接ネットワーク (A) | ローカル (L) | 物理 (P)

攻撃条件の複雑さ: Attack Complexity (AC)

低 (L) | 高 (H)

攻撃に必要な特権レベル: Privileges Required (PR)

不要 (N) | 低 (L) | 高 (H)

利用者の関与: User Interaction (UI)

不要 (N) | 要 (R)

影響の想定範囲: Scope (S)

変更なし (U) | 変更あり (C)

機密性への影響: Confidentiality (C)

なし (N) | 低 (L) | 高 (H)

完全性への影響: Integrity (I)

なし (N) | 低 (L) | 高 (H)

可用性への影響: Availability (A)

なし (N) | 低 (L) | 高 (H)

■スコア算出例（CVSS現状値）

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～

スコア算出例（CVSS環境値）

BINDの脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

例）

CVSS環境値	選択肢
7.0-10.0	即時に脆弱性対策を実施する
4.0-6.9	1ヶ月以内に対策を実施する
0.1-3.9	3ヶ月以内に対策を実施する
0.0	対策の必要なし

評価値は6.5。
システムの脆弱性対応を
1ヶ月以内に実施する。

※上記対応方針はあくまで一例となります

■ケース2
Apache struts2の脆弱性が確認されたケースを見てみましょう

Apache struts2に脆弱性が確認されたケース
～対応方針決定までの流れについて～

- **Apache Struts2の脆弱性を確認したケースは以下の流れで進めます。**

① ニュースサイトなどから脆弱性の情報を入手する
② 関連情報をベンダサイトやセキュリティ関連のサイトから収集する
③ 収集した情報を分析・評価し、対応策を決定する

Apache struts2に脆弱性が確認されたケース
～① ニュースサイトなどから情報を入手する～

IPA

◆ニュースサイト

「Apache Struts 2」に危険度の高いRCE脆弱性、修正バージョンの適用を推奨

岩崎 宰守　2017年9月6日 13:03

Tweet　リスト　B! 11　Pocket 27

Apache Software Foundationは5日、「Apache Struts 2」について、危険度の最も高い"Critical"1件を含む脆弱性3件に関するアドバイザリを公開し、脆弱性を修正した最新バージョン「2.5.13」の提供を開始した。

Criticalと評価されているのは、リモートから任意のコードを実行できる（RCE：Remote Code Execution）脆弱性「S2-052」（CVE-2017-9805）。XStreamのハンドラにおけるXMLペイロード処理の問題によるもので、攻撃者がリモートから特別に細工を施したXMLリクエストを送信することで任意のコードを実行できるもの。RESTプラグインを使用しているバージョン「2.5」～「2.5.12」の環境で影響を受ける。

Apache Software Foundationでは回避策として、RESTプラグ
たはXMLリクエストを受け付けないように制限することを挙げてい

このほかの脆弱性2件は、いずれもDoS攻撃が可能になるもの。
（CVE-2017-9804）は、S2-047の修正が不完全だったもので、
れたURLの検証不備によりDoS攻撃が可能になる。危険度は"Low"

一方の「S2-051」（CVE-2017-9793）は、RESTプラグインに
ライブラリを使用しているときに、攻撃者がリモートから特別に細工を施したXML
リクエストを送信することで、DoS攻撃を実行できてしまうもの。危険度は
"Medium"。

ニュースサイトから判明したこと

- 脆弱性の有無
- CVE番号
- 影響を受けるバージョン
- 修正版のバージョン
- 攻撃コードの有無

【追記 13:43】

独立行政法人情報処理推進機構（IPA）によれば、S2-052の脆弱性を悪用する攻撃コードが公開されており、これが動作することを確認したという。このため、対策済みのバージョンへのアップデートまたは回避策の適用を、至急実施することを推奨している。また、NTTセキュリティ・ジャパンでも、S2-052の脆弱性に対する攻撃が成功することを確認したという。

出典：INTERNET Watch
https://internet.watch.impress.co.jp/docs/news/1079383.html

Apache struts2に脆弱性が確認されたケース
～② 関連情報をベンダサイトやセキュリティ関連のサイトから収集する～

IPA

◆開発ベンダのサイト

ページ / Home / Security Bulletins

S2-052

作成者 Lukasz Lenart、最終変更日9 07, 2017

Summary

Possible Remote Code Execution attack when using the Struts REST plugin with XStream handler to handle XML payloads

Who should read this	All Struts 2 developers and users
Impact of vulnerability	A RCE attack is possible when using the Struts REST plugin with XStream handler to deserialise XML requests
Maximum security rating	Critical
Recommendation	Upgrade to Struts 2.5.13 or Struts 2.3.34
Affected Software	Struts 2.1.2 - Struts 2.3.33, Struts 2.5 - Struts 2.5.12
Reporter	Man Yue Mo <mmo at semmle dot com> (lgtm.com / Semmle). M
CVE Identifier	CVE-2017-9805

Problem

The REST Plugin is using a `XStreamHandler` with an instance of XStream for deserialization witho
Execution when deserializing XML payloads.

Solution

Upgrade to Apache Struts version 2.5.13 or 2.3.34.

ベンダ情報から判明したこと

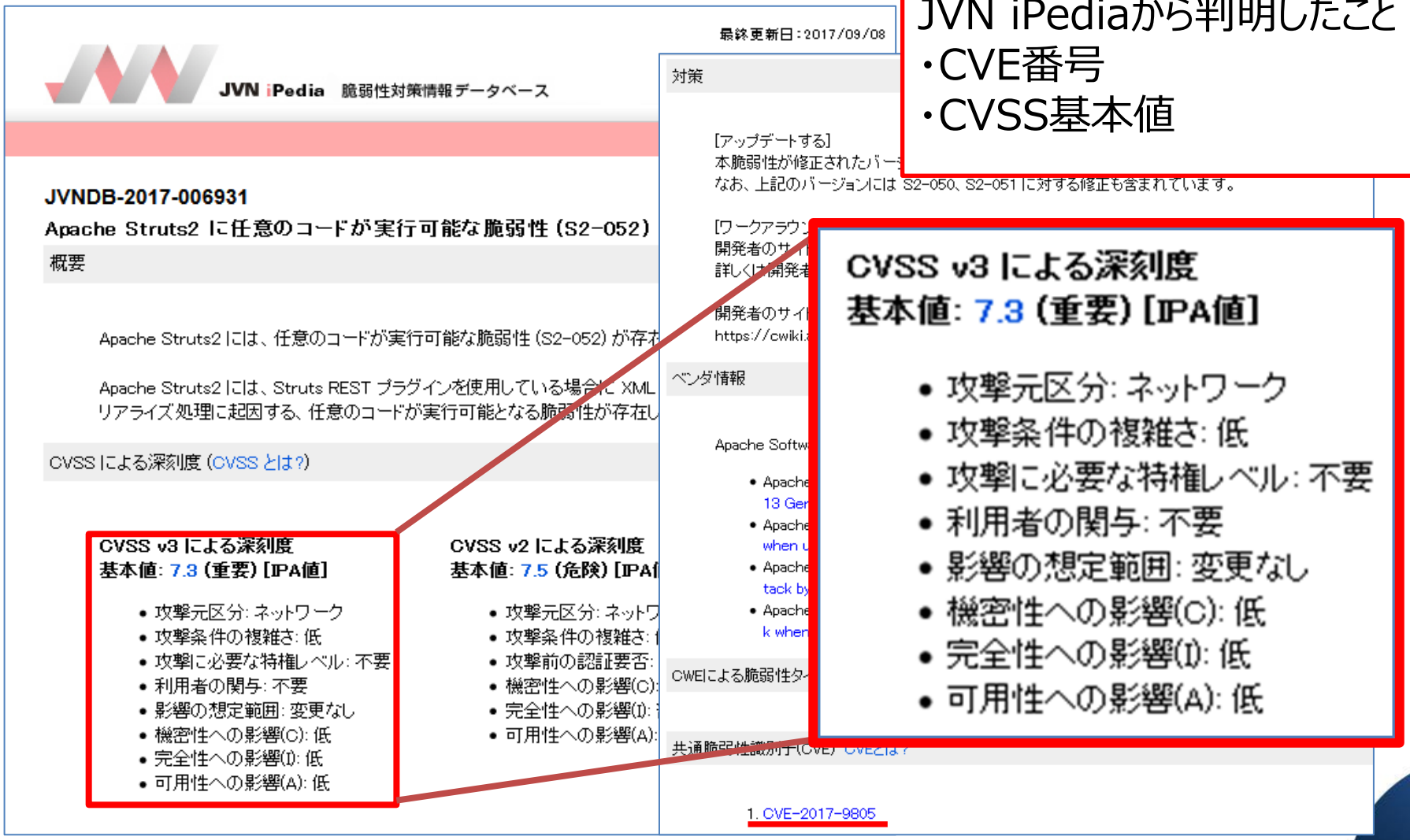
- 危険度
- 修正版のバージョン
- 影響を受けるバージョン
- CVE番号

出典：Apache Software Foundation
https://cwiki.apache.org/confluence/display/WW/S2-052

Apache struts2に脆弱性が確認されたケース
～② 関連情報をベンダサイトやセキュリティ関連のサイトから収集する～

◆脆弱性データベースの情報(JVN iPedia)

JVN iPediaから判明したこと
・CVE番号
・CVSS基本値



Apache struts2に脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

CVSS v3 による深刻度
基本値: 7.3 (重要) [IPA値]

- 攻撃元区分: ネットワーク
- 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: 不要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 低
- 完全性への影響(I): 低
- 可用性への影響(A): 低

◆CVSS基本評価は？

	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)

Apache struts2に脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

IPA

◆CVSS現状評価は？

参考情報
・攻撃コードが確認されている
・対策がベンダから公開されている
・情報がベンダから公開されている

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)**

Apache struts2に脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

IPA

◆CVSS環境評価は？

対象システムのセキュリティ要求度

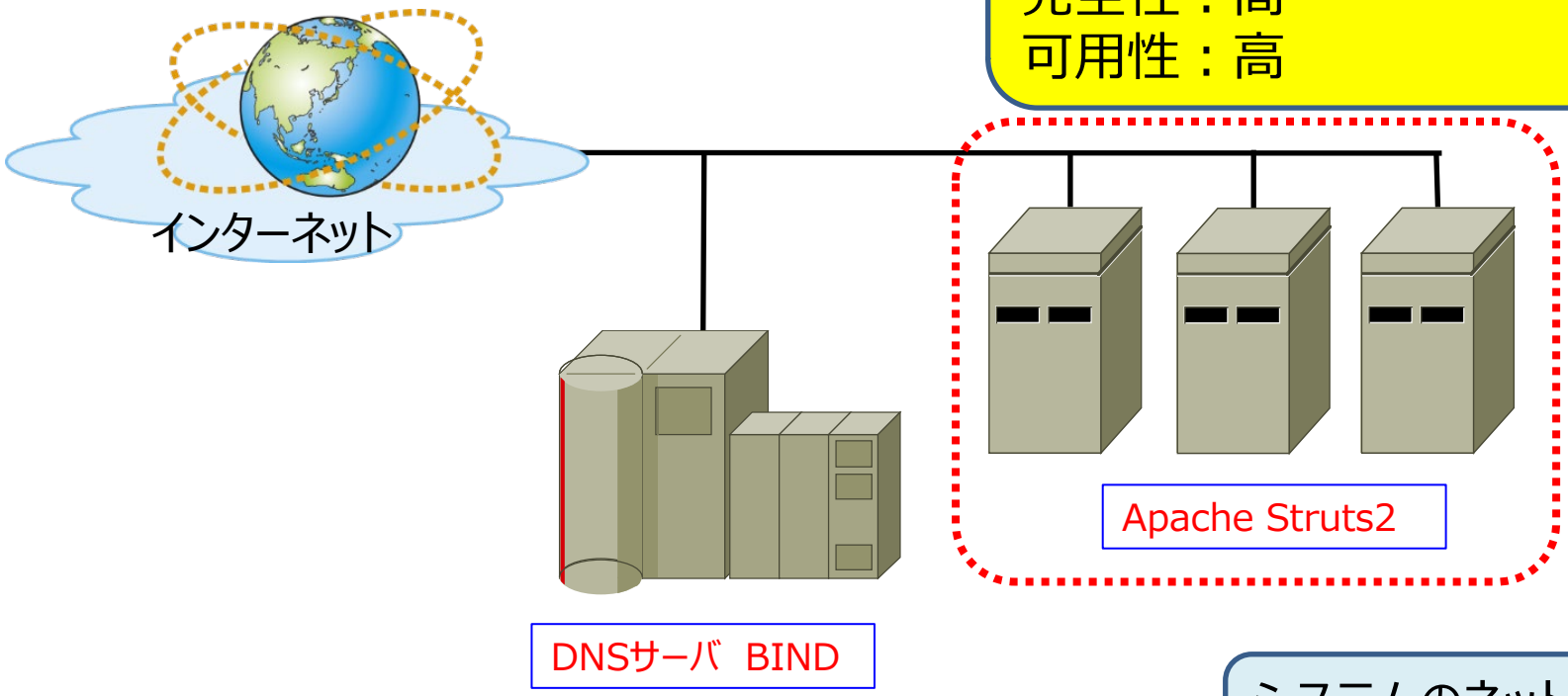
危険小 ⟷ 危険大

	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)

実システムの運用環境

■運用環境

Apache Struts2への要求度
機密性：高
完全性：高
可用性：高



システムのネットワークの
環境を考慮して再評価

✓運用状態に合わせて再評価を行う。

Apache struts2に脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

IPA

◆CVSS環境評価は？

対象システムのセキュリティ要求度

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)

Apache struts2に脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

IPA

◆CVSS環境評価は？

評価例）

	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)

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

■スコア算出例（CVSS基本値）

基本評価基準

7.3
(High)

攻撃元区分: Attack Vector (AV)

ネットワーク (N) | 隣接ネットワーク (A) | ローカル (L) | 物理 (P)

攻撃条件の複雑さ: Attack Complexity (AC)

低 (L) | 高 (H)

攻撃に必要な特権レベル: Privileges Required (PR)

不要 (N) | 低 (L) | 高 (H)

利用者の関与: User Interaction (UI)

不要 (N) | 要 (R)

影響の想定範囲: Scope (S)

変更なし (U) | 変更あり (C)

機密性への影響: Confidentiality (C)

なし (N) | 低 (L) | 高 (H)

完全性への影響: Integrity (I)

なし (N) | 低 (L) | 高 (H)

可用性への影響: Availability (A)

なし (N) | 低 (L) | 高 (H)

■スコア算出例（CVSS現状値）

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～

スコア算出例（CVSS環境値）

Apache struts2に脆弱性が確認されたケース
～③ 収集した情報を分析して評価する～

例）

CVSS環境値	選択肢
7.0-10.0	即時に脆弱性対策を実施する
4.0-6.9	1ヶ月以内に対策を実施する
0.1-3.9	3ヶ月以内に対策を実
0.0	対策の必要なし

評価値は7.8。
運用サーバの脆弱性対応を
即時に実施する。

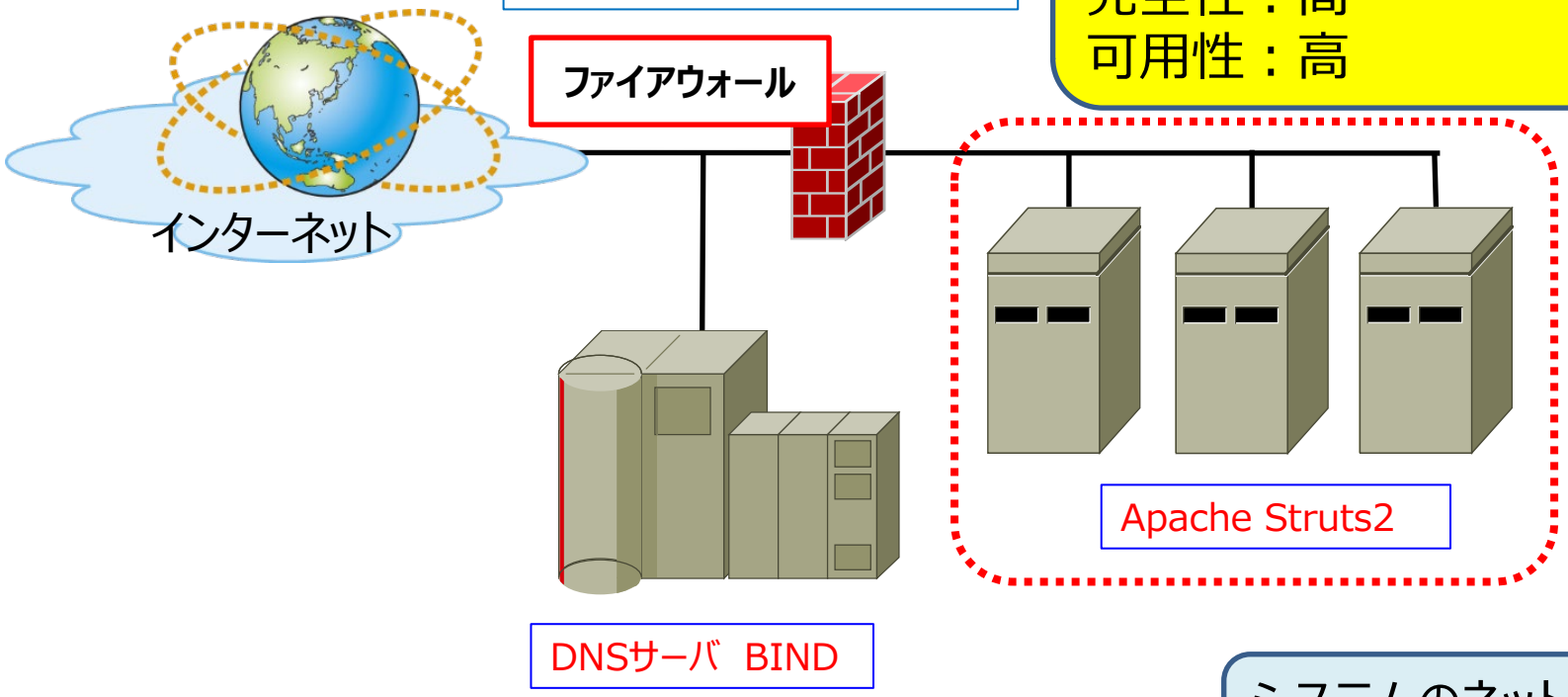
※上記対応方針はあくまで一例となります

環境による再評価でスコアが変わるケース

■運用環境

ファイアウォールによってウェブサーバへのアクセスが制限されている

Apache Struts2への要求度
機密性：高
完全性：高
可用性：高



システムのネットワークの環境を考慮して再評価

✓運用状態に合わせて再評価を行う。

環境による再評価でスコアが変わるケース

◆CVSS環境評価は？

評価例）

	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)

参考：環境による再評価でスコアが変わるケース

スコア算出例（CVSS環境値）

CVSSを使う上での注意事項

・CVSSはあくまで「基準」であり、それのみに従っていればよいわけではない。

・CVSSが低くても攻撃が行われているのであれば、対策を優先的に行わなければいけないケースもある。

参考：
2014年に話題になったSSLの脆弱性である「heartbleed」は、CVSSの基本値5.0と極端に高い数値ではなかったが、2018年においても脆弱性を悪用した被害が発生しており、対策の必要性が高いものであった。

まとめ（第4章）

1.自組織で利用しているソフトウェアを把握し、
　脆弱性情報を日々収集する運用方法を策定する。

2.発見した脆弱性情報から、基本値、現状値、環境値を
　算出。自組織の方針を決定する。

3.自組織のリソースで対応できる方針を作成する。

例）

CVSS環境値	選択肢
7.0-10.0	即時に脆弱性対策を実施する
4.0-6.9	1ヶ月以内に対策を実施する
0.1-3.9	3ヶ月以内に対策を実施する
0.0	対策の必要なし