6X-07

# 開発者・運用者・利用者の視点で分類したSSL/TLSの脆弱性に関するランキングの作成

川村優花† 大丸雅人‡ 小川梨恵‡ 桐生直輝‡ 西倉裕太‡ 齋藤孝道†
明治大学† 明治大学大学院‡

## 1. はじめに

インターネットの通信での改ざん，なりすまし，及び盗聴などの脅威への対策として，SSL/TLS（Secure Sockets Layer / Transport Layer Security）というセキュリティプロトコルが広く利用されている．その一方で，SSL/TLSの仕様及び実装の脆弱性が，現在もなお，脆弱性情報データベースにおいて，多数報告されている．しかし，脆弱性情報データベースは全ての立場の人を対象に作成されているので，数多くの脆弱性の中から自分が注意するべき情報を探す事が容易であるとは言えないと推測する．そこで，本論文では開発者，運用者，及び利用者の 3 つの視点で脆弱性を分類し，各視点の人が注目するべき指標となるよう，深刻度のランキングを作成することを試みた．

## 2. 基礎知識

### 2.1 CVSS

CVSS（Common Vulnerability Scoring System）[1]とは，脆弱性の深刻度を同一の基準の下で定量的に比較可能にすることを目的とした，脆弱性の評価である．CVSS は，FIRST（Forum of Incident Response and Security Teams）が管理している．CVSS で定義されている評価基準の 1 つである基本評価基準を使うと，CVSS 基本値を計算できる．CVSS 基本値とは，脆弱性の影響度及び攻撃容易性をもとに，脆弱性の深刻度を 10 点満点で表した値である．

### 2.2 JVN iPedia

JVN iPedia[2]とは，日本国内外問わず脆弱性対策情報の収集，蓄積を目的とした脆弱性情報データベースである．JVN iPedia は JPCERT/CC と情報処理推進機構（IPA）が共同で管理している．JVN iPedia では， CVSS 基本値や，ベンダの対策状況といった情報を掲載している．JVN iPedia に掲載される情報は，JVN（Japan Vulnerability Notes）に掲載される情報，NVD（National Vulnerability Database）[3]，及び国内ベンダから収集している．

Ranking of SSL/TLS Vulnerabilities from the Viewpoints of Developers, Operators, and Users
†Yuka KAWAMURA ‡Masato OMARU
‡Rie OGAWA ‡Naoki KIRYU ‡Yuta NISHIKURA
†Takamichi SAITO
†Meiji University
‡Graduate School of Meiji University

## 3. 視点別の脆弱性の分類と評価

### 3.1 概要

ランキングを作成するにあたって，開発者，運用者，及び利用者を以下のように定める．

- 開発者
  OpenSSL といった，SSL/TLS ライブラリの開発者
- 運用者
  サーバサイドで SSL/TLS 関連のアプリケーションを使っている人
- 利用者
  クライアントサイドで SSL/TLS 関連のアプリケーションを使っている人

以降，下記 1～3 の手順で開発者，運用者，及び利用者の 3 つの視点でランキングを作成する．

1. JVN iPedia から収集した SSL/TLS に関する脆弱性を，以下の基準で開発者，運用者，及び利用者向けに分類する
   - 開発者向け脆弱性
     SSL/TLS ライブラリに関する脆弱性
   - 運用者向け脆弱性
     サーバサイドの（SSL/TLS 関連）アプリケーションに関する脆弱性
   - 利用者向け脆弱性
     クライアントサイドの（SSL/TLS 関連）アプリケーションに関する脆弱性
2. 脆弱性の発生する原因が共通する脆弱性を集約して，抽象化する
3. 3.2 に示す評価基準を用いて評価を行い，開発者，運用者，及び利用者のそれぞれの視点で，脆弱性の深刻度のランキングを作成する

### 3.2 評価基準

ランキングの作成に用いる評価値 $E$ の算出に以下（1）の計算式を用いた．ただし，全ての計算において少数第二位を四捨五入する．評価値 $E$ 価の最大値は 140 となる．

$$E = A \times 7 + B \times 5 + C + D \quad \cdots (1)$$

ここで，$A$～$D$は以下のとおり定める：

$A$：原因をもとにした分類における脆弱性の CVSS の平均値．

$B$：原因をもとにした分類における脆弱性の数．
$B$ = *原因をもとにした分類における脆弱性の数* × 10 ÷ *原因をもとにした分類における脆弱性の数の最大値*

$C$：原因をもとにした分類における脆弱性において，以下に定める対策の評価値の平均値． JVN iPedia では対策状況が 3 つに分類されるので，以下のとおりに評価値を定める．

1）主要なベンダの正式な対策情報などが公開されている場合：10

2）該当製品のベンダページは存在しているが，対象の脆弱性情報についてベンダページ上で情報が存在しない場合：5

3）該当製品の脆弱性についてのベンダ情報やベンダページが存在しない場合：0

$D$：原因をもとにした分類における公表日の評価値の平均値．
$D$ =（（*公表年* − 2000）× 12 + *公表月* − 補正値）× 10 ÷169

補正値には，最も古いデータの月の値を入れる．

### 3.3 評価結果

#### 3.3.1 開発者視点のランキング

表 1 より，開発者が，SSL/TLS 関連のプログラムの設計及び実装時に注意すべき最も大きな問題として，証明書検証時の問題があることがわかる．また，プログラムの作成後，テストをする際などにも，表 1 に列挙されている脆弱性に注意することが重要であると言える．

表 1　開発者視点のランキング

| 順位 | 脆弱性 | 評価値 |
|---|---|---|
| 1 位 | x.509 証明書検証時の問題 | 105.6 |
| 2 位 | TLS 1.0 の Client Hello メッセージ内の Server Names の処理に関する問題 | 86.4 |
| 3 位 | TLS サーバ名の拡張子や楕円曲線暗号の処理に不備がある問題 | 71.4 |
| 4 位 | 整合性チェック (integrity-check) の失敗を誘発される問題 | 70.6 |
| 5 位 | SSL レコードに含まれるメモリの扱いに関連する問題 | 70.3 |

#### 3.3.2 運用者視点のランキング

運用者のランキング 1 位も，開発者のランキングの 1 位と同様に，証明書検証時の問題となった．たとえば，アプリケーションにパッチを当てる際の優先順位の判断基準として活用するのであれば，その脆弱性に関するパッチ適用は優先すべきことであると言える．また，SSL/TLS を利用する場合，通信自体とは別に，認証が回避される脆弱性が多いことが分かる．

表 2 運用者視点のランキング

| 順位 | 脆弱性 | 評価値 |
|---|---|---|
| 1 位 | x.509 証明書検証時の問題 | 107.5 |
| 2 位 | 認証を回避される問題 | 90.2 |
| 3 位 | SSL セッションを通じてクエリのインターフェースへ接続される問題 | 88.7 |
| 4 位 | Cisco Unified Wireless Network (UWN) Solution が TLS および SSL を適切に実装しない問題 | 88.5 |
| 5 位 | 権限をもっていないクライアントでも，SSL と HTTPS クライアントのハンドシェイク処理を完了させてしまう問題 | 87.9 |

#### 3.3.3 利用者視点のランキング

表 3 の脆弱性が多く報告されるアプリケーションについて，利用をやめる際の判断基準となる．

表 3 利用者視点のランキング

| 順位 | 脆弱性 | 評価値 |
|---|---|---|
| 1 位 | x.509 証明書検証時の問題 | 103.7 |
| 2 位 | SSL ソケットを適切に処理しない問題 | 89.5 |
| 3 位 | Web Socket 実装が SSL を適切に処理しない問題 | 88.7 |
| 4 位 | 任意のコードを実行される問題 | 85.6 |
| 5 位 | SSL セッションのスレッドの安全性を保証しない問題 | 84.3 |

## 4. まとめ

本論文では，開発者，運用者，及び利用者の 3 つの視点で，SSL/TLS の仕様及び実装における脆弱性を分類し，深刻度のランキングを作成した．これらにより，開発者，運用者，及び利用者は，SSL/TLS の仕様及び実装における脆弱性について，どのような脆弱性を特に重視すべきかの示唆を得ることができると期待できる．

## 5. 参考文献

[1] https://www.ipa.go.jp/security/vuln/CVSS.html
[2] http://jvndb.jvn.jp/nav/jvndb.html
[3] https://nvd.nist.gov/