2021 年 12 月 13 日
内閣官房内閣サイバーセキュリティセンター

# ApacheLog4j の脆弱性(CVE-2021-44228)に関する注意喚起

ApacheLog4j の脆弱性に関する情報に対応するため、速やかに措置を講じる等により、サイバーセキュリティの確保に努めてください。

2021 年 12 月 10 日及び 13 日、内閣サイバーセキュリティセンターは、政府機関等及び重要インフラ事業者等に向けて、ApacheLog4j の脆弱性(CVE-2021-44228)に係る注意喚起を行いました。

本件については、多くのユーザに影響があると考えられることから、重要インフラ事業者等に対する注意喚起（別紙）について、広く一般にも活用していただけるよう公開するものです。

既に本脆弱性を悪用する実証コードが公開されており、悪用を試みる通信が発生しているとの情報もあるところです。独立行政法人情報処理推進機構(IPA)や一般社団法人 JPCERT コーディネーションセンターからも注意喚起及び対策手法を公開していますので、これらを参考に、システムに対する影響を検討のうえ、速やかに措置を講じるようお願い致します。

(参考)

「Apache Log4j の脆弱性対策について(CVE-2021-44228)」(IPA)
https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html

「Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起」(JPCERT/CC)
https://www.jpcert.or.jp/at/2021/at210050.html

本件に対する問い合わせ先
内閣サイバーセキュリティセンター(NISC)
電話：03-5253-2111（代表）
基本戦略総括グループ
情報統括グループ
重要インフラ第２グループ

別紙

2021 年 12 月 10 日

内閣サイバーセキュリティセンター
重要インフラグループ

# Apache Log4j の脆弱性(CVE-2021-44228)に関する注意喚起

## 1. 対象ソフトウエア

・Apache Log4j 2.0 から 2.14.1

上記ライブラリには、外部の第三者の意図による任意のコード実行（プログラムの異常終了、プログラムの実行、当該サーバーに保存されているデータの改ざん・削除・漏えい等）の脆弱性が存在します。本脆弱性の実証コード(PoC コード)の存在を確認されており、本脆弱性の影響を受けるサーバーがインターネット上に存在するか偵察活動が行われています。

## 対応

対象ソフトウエアを最新のバージョンに更新。

更新方法等については、参考 URL 参照。バージョンアップができない場合は、緩和策や監視等を検討ください。

参考 URL

・Apache Log4j 2 (Apache Software Foundation)
https://logging.apache.org/log4j/2.x/

・RCE 0-day exploit found in log4j, a popular Java logging package (LunaSec)
https://www.lunasec.io/docs/blog/log4j-zero-day/