第126回スクエアfreeセミナー

# Log4jの脆弱性対策はお済ですか？

## オープンソースソフトウェアの脆弱性対策をご紹介します

株式会社*OPEN*スクエア
田中　昭造

# まだ、終わってLog4j脆弱性を狙った攻撃

Log4j脆弱性はCVSSスコア：10.0に分類された深刻度が"緊急"の脆弱性です
- ・任意のコマンドが実行できる
- ・著名なソフトウェアベンダーでも多数採用している

脆弱性を狙った攻撃数は少なくなりましたが、終息した訳ではありません。Log4j脆弱性がゼロディ脆弱性で無くなっただけです、、、、

## 米国では「Log4j」脆弱性の放置に法的措置も攻撃に引き続き警戒を呼び掛け

米連邦取引委員会（FTC）は、この脆弱性を悪用する集団が増えている実態を受け、対策を怠った企業の責任(法的措置）を追及すると表明しました。(2022/1/4)

# Log4jの脆弱性検知ツール

**対策はしたいが、そもそも、Log4jを使っているのか、何処で使っているのか分からない？**

そこで、
Linuxコマンド
＃　find / -name kig4j-*.jar　等

米国土安全保障省（DHS）
https://github.com/cisago

セキュリティ会社からも
https://www.crowdstri -search-tool/

OSSの脆弱性対策ソリューション提供もWhiteSource社からも
https://github.com/whitesource/log4j-detect-distribution

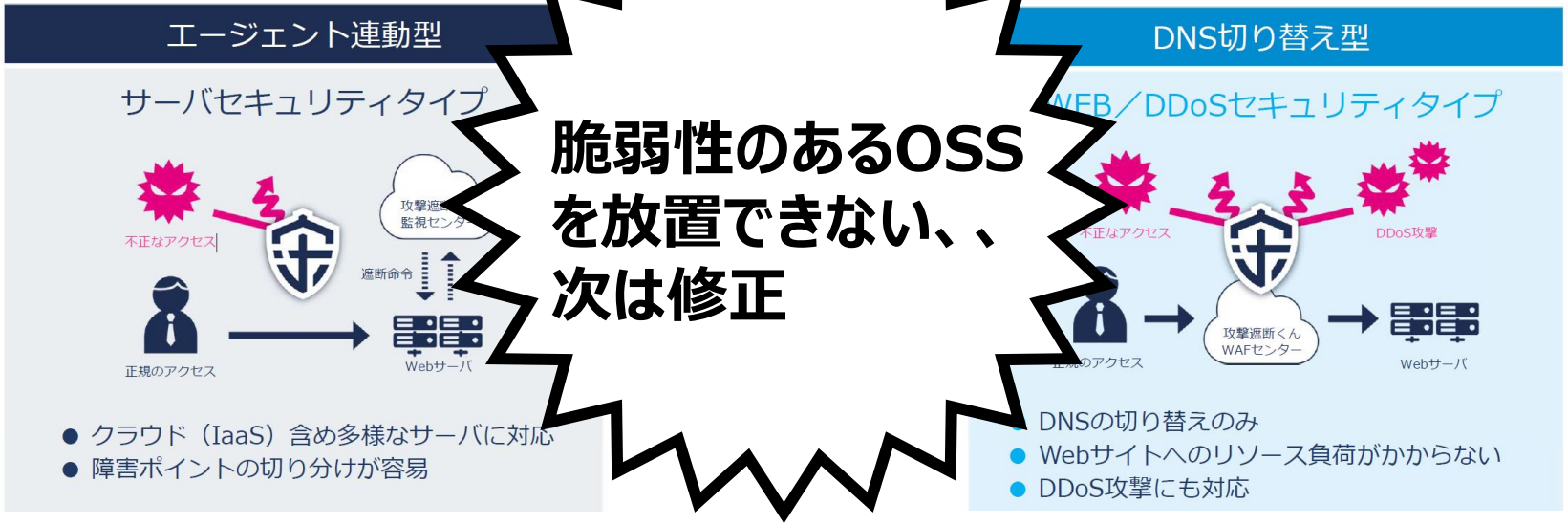
**ただ、
完全に検知できないとの指摘も**

# WAFの導入検討

## 自社のシステムを変更することなく、直ぐにLog4j脆弱性を狙った攻撃を防御

保守・運用に手間を掛ける事なく、24時間365日
Webシステムを守るクラウド型WAFがお勧めです

攻撃遮断くん




**脆弱性のあるOSSを放置できない、、次は修正**

# OSSセキュリティ&コンプライアンス管理ソリューションの導入

**Log4jは何処で使っているのかな？**
**どうやって修正するのかな？**


WhiteSource が解決します

**OSSの脆弱性チェック**
**＆ リアルタイムに通知**
**修正方法の提示**

## Log4j脆弱性が修正されたバージョンを提案

# ご清聴ありがとうございました。

**OSSの脆弱性対策にはWhiteSource,攻撃遮断くんが有益です。**
**WhiteSource,攻撃遮断くんに関するお問い合わせは当社までお願い致します。**

＜お問い合せ先＞

株式会社OPENスクエア

営業担当

E-Mail : sales_os@opensquare.co.jp
TEL : 03-6413-1840

END