OSS脆弱性管理サービス

目次

FUJITSU

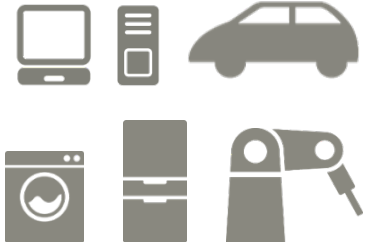
ソフトウェアを取り巻く環境の変遷

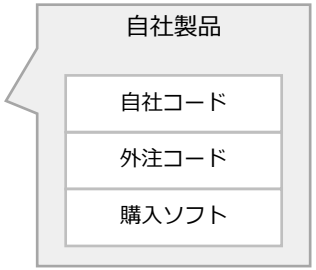
FUJITSU

過去

- スタンドアローン
- クローズドネットワーク

- 小規模
- ウォーターフォール開発





現在

- **クラウド、IoT**
- **インターネット接続**

- 大規模
- アジャイル開発
- **OSS (Open Source Software) の活用**

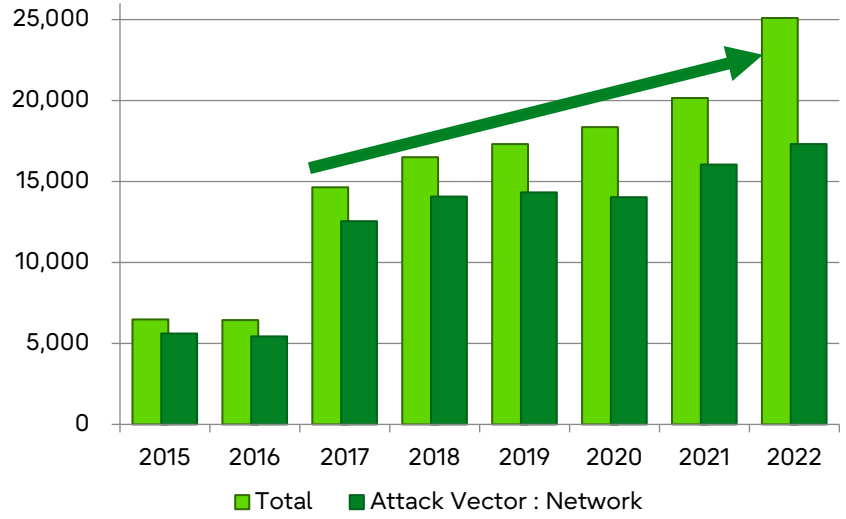
脆弱性悪用、サイバー攻撃、国家間サイバー戦争、訴訟など、
時代の変化とともに**セキュリティ脅威の増加、利用者責任が拡大**しており、
脆弱性などの情報を監視・管理し、セキュリティ リスクの軽減が重要

セキュリティ脅威の増加

○ 脆弱性の発生件数

CVE（脆弱性）発生件数 と うち攻撃区分「Network」の件数

約70%が攻撃区分「Network」の脆弱性



Source ：https://nvd.nist.gov/vuln/search

参考

2017年に脆弱性数が急増していますが、これはCVEの採番機関CAN (CVE Numbering Authority) になるための認定基準が緩和され、CVE採番機関の数が増加したことが一因だと言われています。

○ 主要OSSの脆弱性の状況について

✓ linux_kernel
- 2022年570件の脆弱性が発生
  営業日換算では2.3件/日の脆弱性が発生
- 組込みシステムでカスタマイズして利用する際は、専任の担当をあて脆弱性の管理が必要

✓ OpenSSL
- 2022年13件の脆弱性が発生
- 13件中12件がリモートネットワークから容易に攻撃可能な脆弱性であり、早急に脆弱性対応が必要

✓ Java
- 某システムでは mavenでダウンロードしたLog4jなど169ライブラリをSEがメンテナンスし、脆弱性を管理

セキュリティに対する法整備が急速に進んでおり、
セキュリティ対策ノウハウが求められる時代になっている

セキュリティに関連する世の中の動向

FUJITSU

- リスクの増加によりサイバーセキュリティの向上が急務
  - → 製品にSBOM適用することが対抗手段となる　※SBOM : Software Bill Of Materials（ソフトウェア部品表）
- 米国大統領令をきっかけにSBOMに関連する活動が活発化

  - 米国では政府関連の調達でSBOM適用が入札要件になっている
  - 日本、EUも米国に追従してSBOM適用を推進する流れ
  - SBOM適用できない製品が市場から締め出される

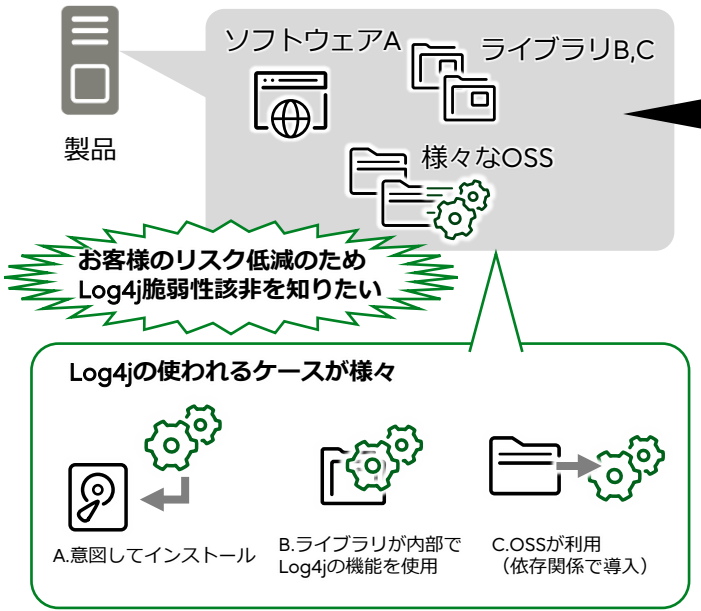
Open Source Security Summit Japanの様子

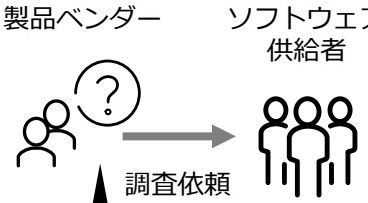
2021-05	**米国**	**政府による「国家サイバーセキュリティ改善に関する大統領令」**
2022-01,05	米国	政府が White Houseで Open Source Security Summit I / II を開催
2022-08	日本	経済産業省の後援で Open Source Security Summit Japan を開催
2022-09	**EU**	**サイバーセキュリティに関して「Cyber Resilience Act」を発表**
2023-01	日本	経済産業省と米国国土安全保障省がサイバーセキュリティに関する協力覚書（MoC：Memorandum of Cooperation）に署名

https://openssf.org/blog/2022/08/24/outcomes-from-open-source-software-security-summit-in-japan/

Apache Log4jの脆弱性：Log4Shell

- **脆弱性の深刻度（CVSS）：最高値10.0**（攻撃が比較的容易）
- Log4jはWebサーバで広く使用される**Java言語の利用頻度の高い汎用ライブラリ**（ソフトウェア部品）
- Log4jが動作するアプリケーションに対して**外部から任意のコードを実行し情報漏えい等の被害の恐れ**
- その後も相次いで**情報漏えい**や**任意コード実行に関する脆弱性**、**DoS攻撃**に関する脆弱性が公表された





- 担当箇所以外の**該非が分からない**
- 担当に調査依頼が必要なため**情報が揃うまでに時間がかかる**

該非調査やその後の修正対応に時間がかかることでお客様がセキュリティリスクに晒されてしまう

- お客様の業務やサービスの停止による機会損失
- 情報漏洩/盗難による信用の失墜、損害賠償

ⓘ ソフトウェアの利用状況を把握し、日々、脆弱性を管理していれば問題ない

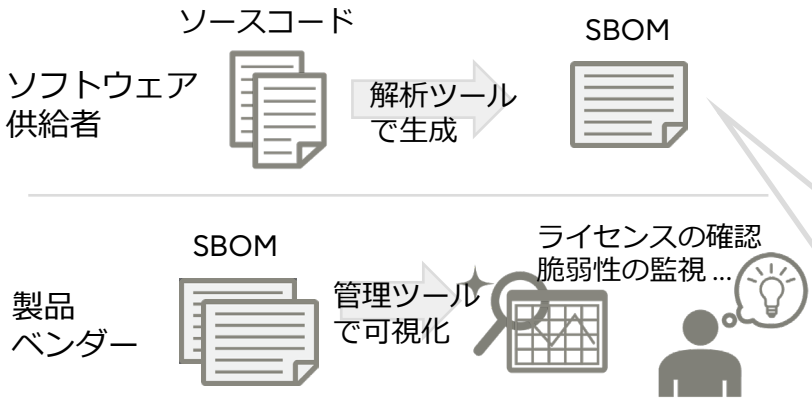
※ この事例以降で世の中が法令の整備に取組むようになった

「SBOM」がリスクを軽減

FUJITSU

SBOM : Software Bill Of Materials（ソフトウェア部品表）とは

製品に含まれるすべてのソフトウェアをまとめて管理するために、その名前やライセンス、依存関係などを機械処理しやすい形で一覧化したもの



SBOMで実現したいこと

ソフトウェア情報をデータ化することで
- **ライセンス コンプライアンス**
- **脆弱性などのセキュリティ リスク軽減**

SBOMの例 (抜粋)

```
…
PackageName: main-src  コンポーネント名
SPDXID: SPDXRef-Package-main-src
PackageDownloadLocation: git+https://github.com/swinslow/spdx-examples.git …
FilesAnalyzed: true
PackageVerificationCode: 7f560718ca985c9334efbb56291e494df22ed97c
PackageLicenseConcluded: GPL-3.0-or-later AND BSD-3-Clause
PackageLicenseInfoFromFiles: BSD-3-Clause
PackageLicenseInfoFromFiles: GPL-3.0-or-later
PackageLicenseDeclared: GPL-3.0-or-later
PackageCopyrightText: NOASSERTION

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-main-src
…  依存関係
```

ライセンス情報

https://github.com/spdx/spdx-examples

脆弱性管理の流れ

FUJITSU

○ ソフトウェアの利用状況を正確に把握し、最終的な脆弱性への対応の判断を迅速に行う必要がある

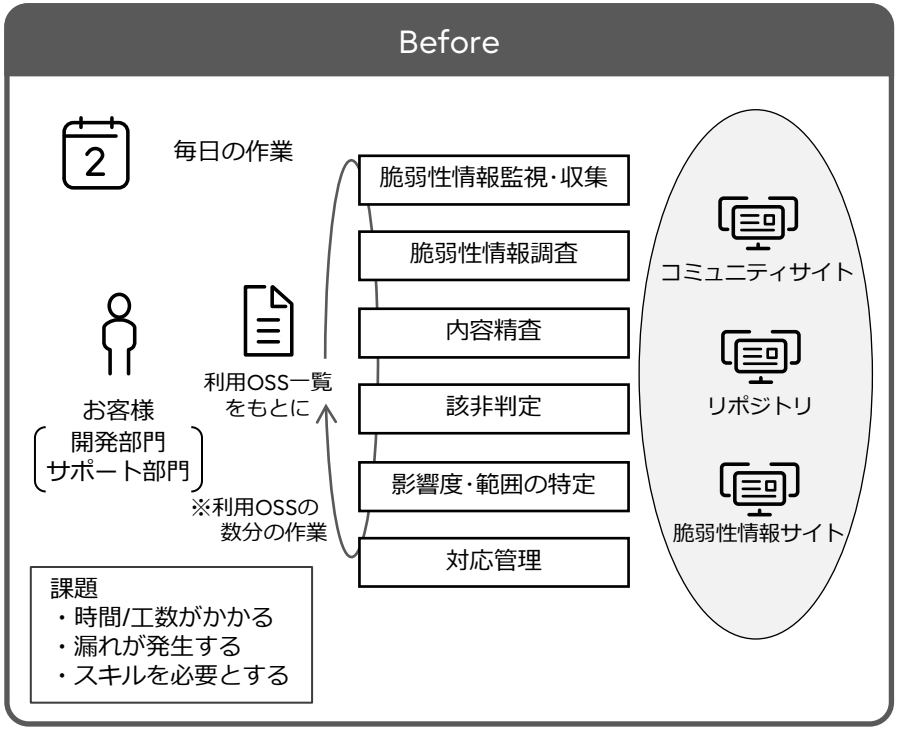
脆弱性情報監視･収集	・利用しているソフトウェアに関する脆弱性情報を、**脆弱性情報サイトを監視**し、脆弱性情報を収集
↓	
脆弱性情報調査	・利用しているソフトウェアに関する脆弱性情報がどのようなものかを調査（**脆弱性情報の正確な把握**）
↓	
内容精査	・脆弱性情報が正確なものかをコミュニティサイトなども調査（**脆弱性情報の正確な把握**）
↓	
該非判定	・脆弱性情報が利用しているソフトウェアに**該当するかを判断** ・該当する場合、**パッチ情報･アップデート情報を収集**
↓	
影響度･範囲の特定	・脆弱性対応（アップデート情報）によって**影響を受ける機能の影響･範囲を調査**
↓	
対応管理	・機能影響･範囲よりアップデートの優先順位･時期の検討など、**対応の判断と最終的な対応状況を管理**

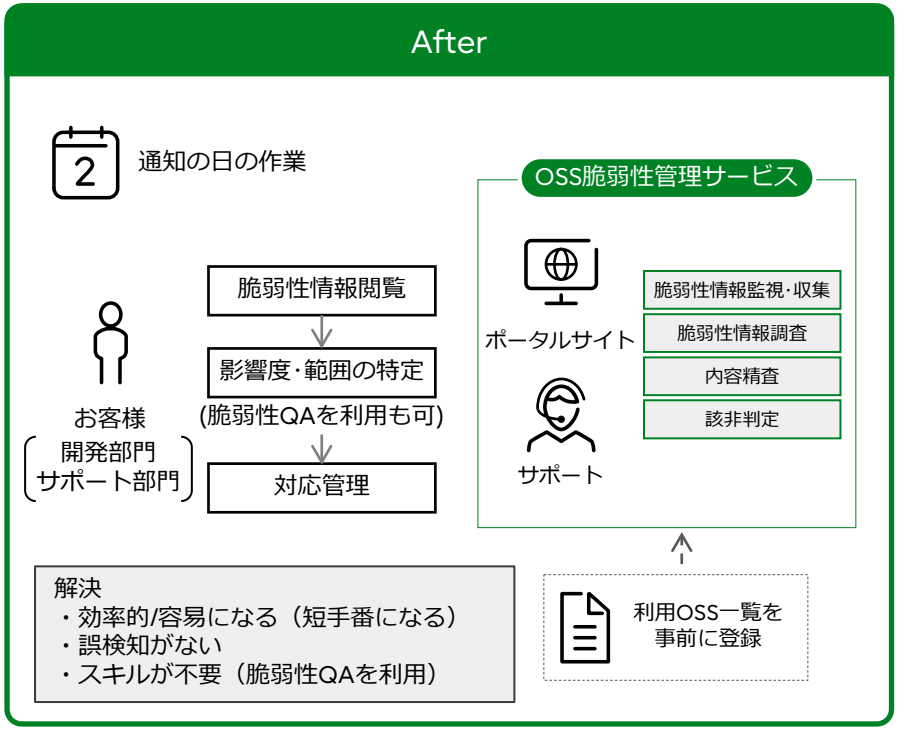
手作業では時間がかかる、OSSに関するスキルが求められる、確認漏れが発生する

OSS脆弱性管理サービス 利用イメージ

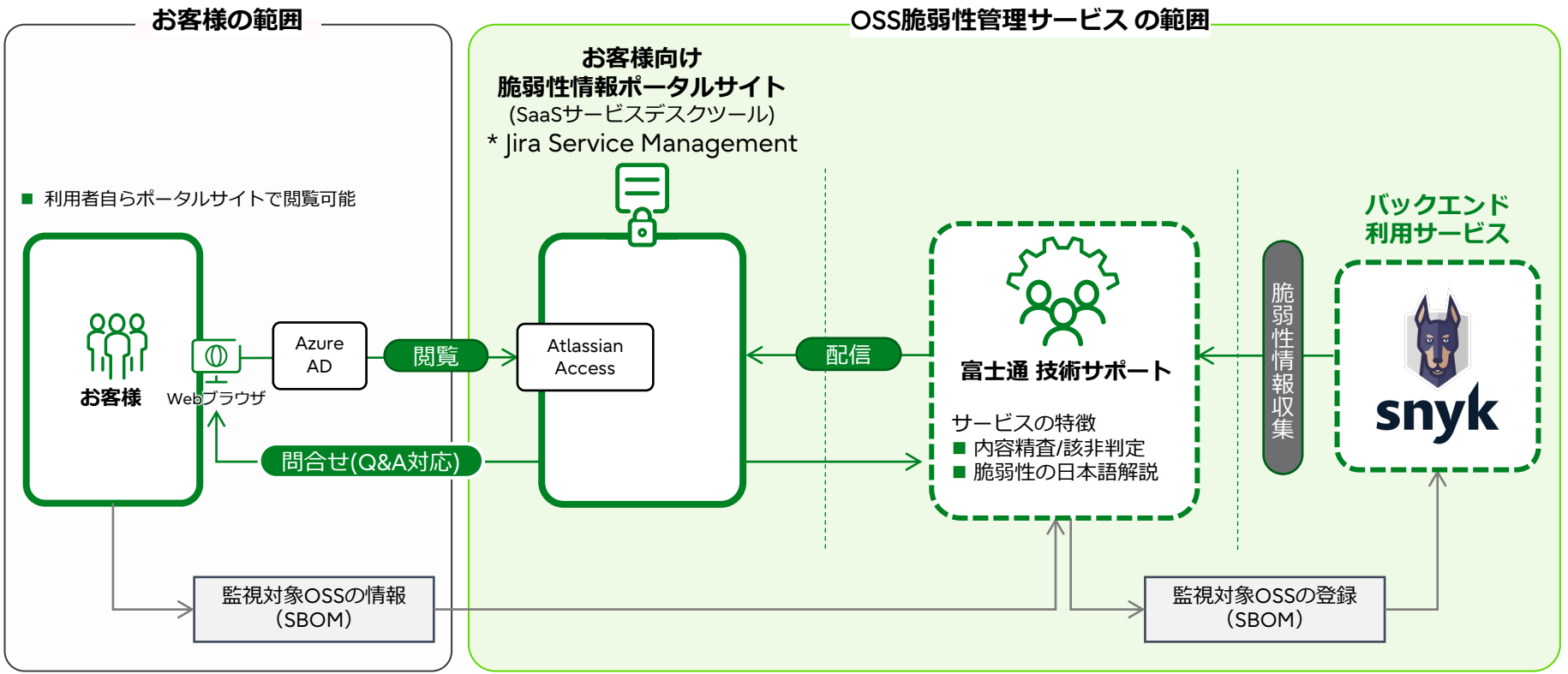
FUJITSU

スキルを必要とせず、工数削減や対応漏れを無くすことが可能





OSS脆弱性管理サービス の構成



お客様向け脆弱性情報ポータルサイト 画面イメージ

FUJITSU

ポータル画面 (ログイン後)

右上のリクエストのリンク > ご自身が所属するプロジェクト名 、もしくは、画面中央の「脆弱性一覧」のリンクをクリックすると、プロジェクトのバージョン毎の登録OSSに対し、発生した脆弱性情報が一覧で表示されます。

脆弱性一覧画面

要約の列に表示されたCVE番号をクリックすると、脆弱性の詳細が表示されます。

初期表示では、監視対象OSSに発生した脆弱性が、発生した日付順に表示されています。
「作成日」「更新日」「優先度（CVSSスコア）」のタイトルをクリックすると、並べ替えができます。

脆弱性詳細画面

OSS名、OSSバージョン、日本語訳、対象バージョン、修正バージョン、種別、NVD URL、優先度(脆弱性の深刻度)、CVSSスコアなど、脆弱性の詳細が表示されます。

ステータスで「オープン」「対応済み」など脆弱性を管理することができます。

OSS脆弱性管理サービス サービスメニュー

FUJITSU

サービスメニュー		サービス概要
脆弱性管理	30ソフトウェア／月	ひと月あたり30ソフトウェア･バージョンまでを対象に脆弱性情報を収集･分析し、配信します
	40ソフトウェア／月	ひと月あたり40ソフトウェア･バージョンまでを対象に脆弱性情報を収集･分析し、配信します
	50ソフトウェア／月	ひと月あたり50ソフトウェア･バージョンまでを対象に脆弱性情報を収集･分析し、配信します
	60ソフトウェア／月	ひと月あたり60ソフトウェア･バージョンまでを対象に脆弱性情報を収集･分析し、配信します
	70ソフトウェア／月	ひと月あたり70ソフトウェア･バージョンまでを対象に脆弱性情報を収集･分析し、配信します
	1プロジェクト／月	1プロジェクトの脆弱性情報を収集･分析し、配信します
脆弱性Q＆A	基本10チケット	脆弱性情報に関するお問い合わせに応じます（10チケット分）
	追加1チケット	脆弱性情報に関するお問い合わせに応じます（基本チケットに加えて1チケット単位で追加可）

（注）・OSS脆弱性管理サービス は、SaaSセキュリティツールで管理可能なソフトウェアを対象に収集した脆弱性情報をお客様向け脆弱性情報ポータルサイトにて提供します。
脆弱性情報が発行されないソフトウェアに関しては、お客様向け脆弱性情報ポータルサイトにて提供されない場合があります。
・OSS脆弱性管理サービス で提供する脆弱性に関して、お客様の製品への影響範囲の特定などは行いません。
製品等への影響の有無の特定などは必要に応じてお客様の責任の下に実施ください。
・OSS脆弱性管理サービス で提供する脆弱性情報は、正確性などを完全に保証するものではありません。
製品等への修正対応などは必要に応じてお客様の責任の下に実施ください。
・お客様からの脆弱性の質問に対して、事例・ノウハウを基とし、調査を加えたベストエフォートで回答いたします。
・脆弱性の質問に対する回答内容は、お客様の実環境や実利用形態にて検証をするものではなく、解決･動作を完全に保証するものではありません。

お問合せ

FUJITSU

- OSS脆弱性管理サービス についてのお問い合わせは、
  下記お問合せページよりご依頼ください。

  - Linux情報へのお問合せ
    https://www.fujitsu.com/jp/products/software/os/linux/contact/

商標

- Linux® は、米国およびその他の国における Linus Torvalds の登録商標です。
- OpenSSL は、OpenSSL Software Foundation, Inc.の米国およびその他の国における商標または登録商標です。
- Java は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。
- Apache Log4j、Log4j、Apache は、The Apache Software Foundation の米国およびその他の国における商標または登録商標です。
- SPDX® は、The Linux Foundation の米国およびその他各国における登録商標です。
- Microsoft、Windows、Microsoft Azure またはその他のマイクロソフト製品の名称およびロゴは、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Atlassian、Jira Software、Jira Service Management、Atlassian Access またはその他のアトラシアン製品の名称およびロゴは、Atlassian Pty Ltd. の豪州、米国およびその他の国における商標または登録商標です。
- 本資料中の社名、製品名、サービス名などの名称およびロゴは、すべて各社および商標権者の商標または登録商標です。
- 本資料に掲載されているシステム名、製品名などには、必ずしも商標記号（™、℠または®）を付記しておりません。

Thank you