OpenSSF 活動紹介
～ CSS/OWS2024 ～

サイバートラスト株式会社
OSS事業本部
池田 宗広
（LF Japan Evangelist）

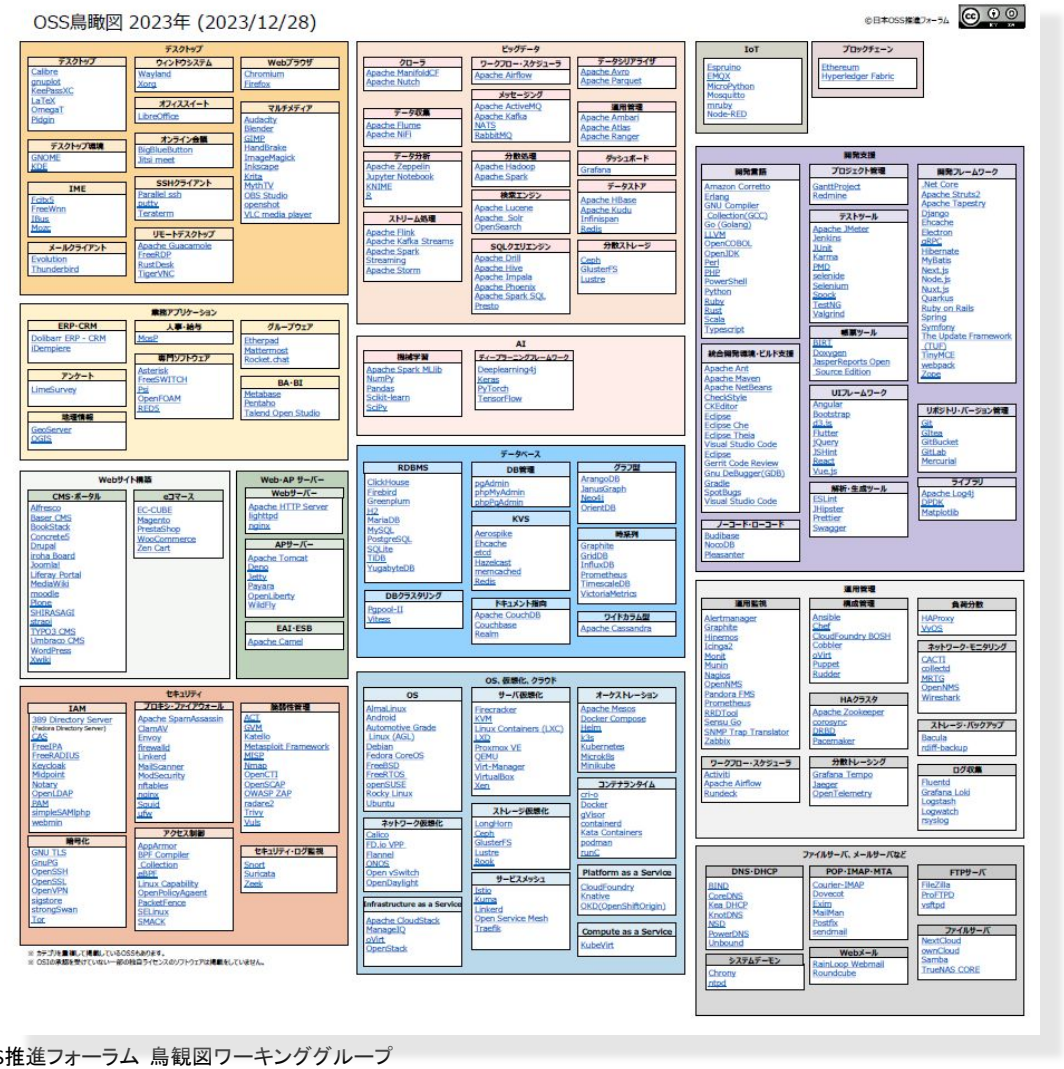
目次

- OSS・ソフトウェアサプライチェーンセキュリティ関連動向
- ソフトウェアサプライチェーンセキュリティの全体像
- OpenSSF (Open Source Security Foundation)
- 主要な OSS アクティビティ紹介
- まとめ

OSS・ソフトウェアサプライチェーンセキュリティ関連動向

オープンソースソフトウェアの利活用領域は広範・拡大中

OSSの利活用範囲は非常に幅広い



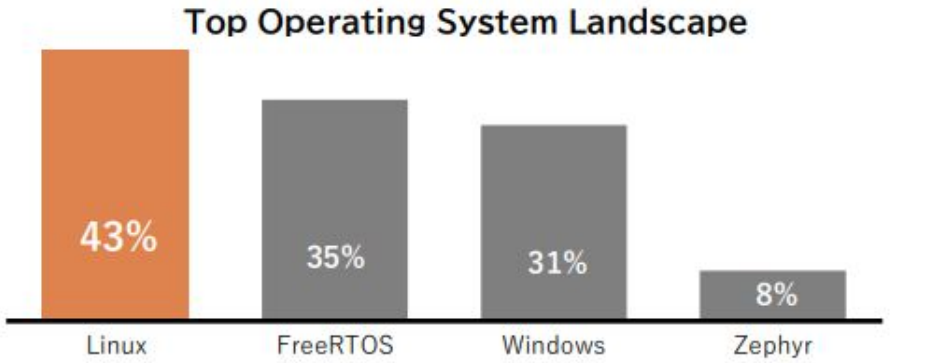
出典：日本OSS推進フォーラム 鳥観図ワーキンググループ
（https://ossforum.jp/index.php/choukanzu-wg/）

IoT機器におけるLinux採用拡大

スマートデバイスやIoT機器の普及に伴い、より高度な処理やセキュリティ対策が可能なLinux OSのニーズが増加

IoT機器で採用されるOSの採用傾向は

Linuxが43%でトップ



出典：Eclipse Foundation『IoT Developer Survey 2020』

「情報セキュリティ10大脅威 2024」
独立行政法人情報処理推進機構(IPA)発表

cybertrust

2023年（組織）	順位	2024年（組織）	U/D
ランサムウェアによる被害	1位	ランサムウェアによる被害	→
サプライチェーンの弱点を悪用した攻撃	2位	**サプライチェーンの弱点を悪用した攻撃**	→
標的型攻撃による機密情報の窃取	3位	内部不正による情報漏えい	↑
内部不正による情報漏えい	4位	標的型攻撃による機密情報の窃取	↓
テレワーク等のニューノーマルな働き方を狙った攻撃	5位	**修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）**	↑
修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6位	不注意による情報漏えい等の被害	↑
ビジネスメール詐欺による金銭被害	7位	**脆弱性対策情報の公開に伴う悪用増加**	↑
脆弱性対策情報の公開に伴う悪用増加	8位	ビジネスメール詐欺による金銭被害	↓
不注意による情報漏えい等の被害	9位	テレワーク等のニューノーマルな働き方を狙った攻撃	↓
犯罪のビジネス化（アンダーグラウンドサービス）NEW	10位	犯罪のビジネス化（アンダーグラウンドサービス）	→

「サプライチェーン攻撃」が上位に定着

脆弱性に対し、修正公開前情報、公開対策情報を悪用する攻撃の脅威が増加
(ゼロデイ/Nデイ攻撃)

出典：
https://www.ipa.go.jp/security/10threats/10threats2024.html

欧米英における主なセキュリティ法規制 （2024年10月時点）

cybertrust

主要各国にてサイバーセキュリティ法規制が策定され、相互承認する方向（各国共通規定）

国、地域	法規制	主な対象製品	規制開始	(整合)規格
イギリス 	**PSTI**	消費者向け、且つ インターネット接続可能な （有線/無線)製品	**2024年4月29日**	ETSI EN 303 645
EU 	**無線機器指令 (RED)**	無線機器、且つ インターネット接続できる機器	**2024年8月→ 2025年8月に延伸**	2024年6月 (リリース予定)
	サイバーレジリエンス法 （CRA）	デジタル要素を含む ソフトウェア、ハードウェア製品	**(2024/10/10 EU Concil 採択)**	ETSI EN303 645 IEC62443
	NIS2指令 (NIS2 Directive)	重要インフラ（セクター） 事業者及び そこに導入されるIoT機器	**2024 各国内法へ移行**	調整中
米国 	**2020年 IoT サイバーセキュリティ改善法**	トランスディーサ x 1 ネットワーク x 1以上	**（政府調達品） 2022年12月**	NIST IR 8259/ NIST IR 8425
日本 	**セキュリティ要件適合評価及びラベリング制度（ JC-STAR） (旧称: IoTセキュリティ適合性評価制度)**	最低限の要件☆1から 重要インフラ☆4まで 4段階に分けて制度設計	**2025年3月～☆1申請受付開始 ☆2以上の日程は未定**	**米英欧と相互承認前提** ETSI303 645/IEC62443参照し策定 （☆1のみ日本独自）

TÜV SÜD Japan_Cybersecurity_ET+2023 を基に最新情報を加筆し修正

重要なイベントと OSS コミュニティの動き

cybertrust

CII/OSSC

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2021/05/12
米国 大統領令「国家のサイバーセキュリティ強化について」

2022/05/11
日本国 経済安全保障推進法　成立

2022/05/12
OSS Security Summit II @ Whitehouse

OSS Mobilization Plan

2022/08/23
OSS Security Summit Japan

2022/09/15
EU Cyber Resilience Act 法案公開

2024/10/10EU Council **採択**

LF EU

SPDX 3.0

2023/09/13
Secure OSS Summit@DC

2025/3～
セキュリティラベリング制度（JC-STAR）

SolarWinds

log4shell

xz-utils

2020 | 2021 | 2022 | 2023 | 2024 | 2025

Java 用ログライブラリ log4j の深刻な脆弱性
攻撃が多数発生

広範に利用されている圧縮展開ツール　xz に仕込まれたバックドア
広く流通はしなかったが、OSS メンテナへの「信頼」を利用した重大な事件

SolarWInds 社のネットワーク監視ツール　Orion にマルウェア SUNBURST が混入
米国政府機関を含む約 100の組織がバックドアからの侵入を許したと見られる

ソフトウェアサプライチェーンセキュリティの全体像

「サプライチェーンセキュリティ」とはなにか

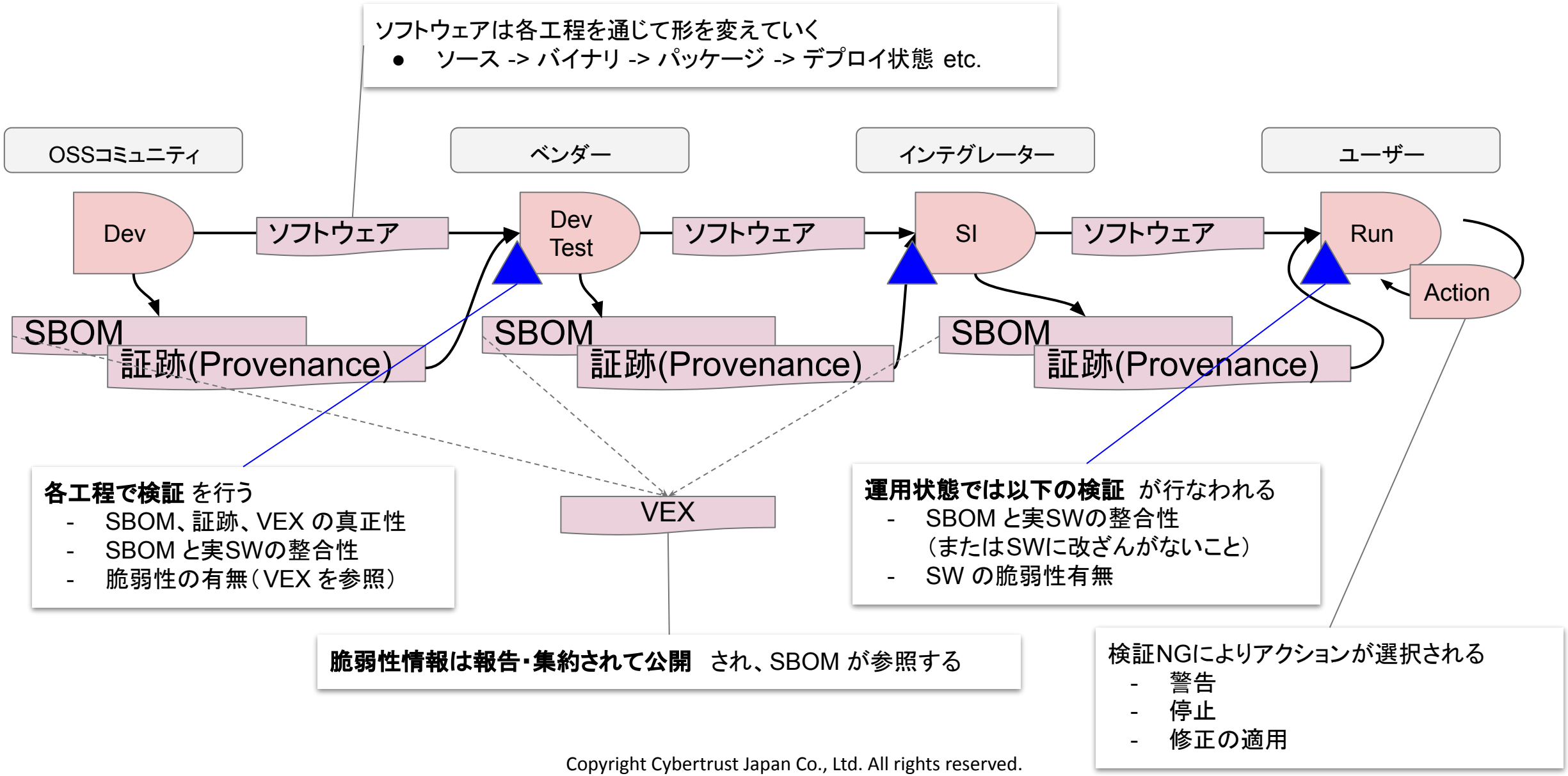
ソフトウェアサプライチェーン

- 設計、開発、実装、テスト、パッケージ、流通、インストール、実行に至る、ソフトウェアが作られてから使われるまでの全ての工程とその関係・流れのこと

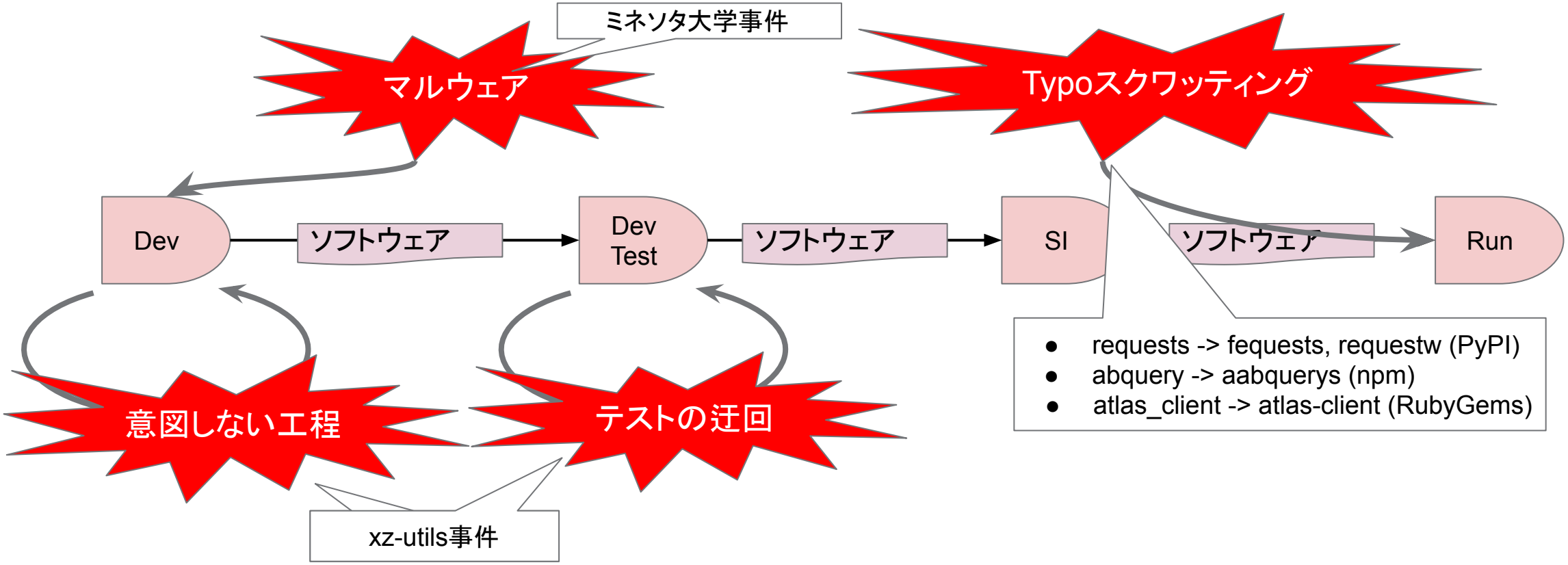
ソフトウェアサプライチェーンセキュリティ

- あるソフトウェアが、
  ✔ 期待する主体によって行われ、
  ✔ 期待する工程を経て、
  ✔ 期待する経路を通り、
  ✔ 期待する構成で、
  ✔ 期待する機能をもって
  実行場所に届くこと、それらが検証できること

サプライチェーンセキュリティの全体的理想像



サプライチェーンセキュリティ侵害の例



xz-utils 事件

CVE-2024-3094

- 広く使われている圧縮・展開ツール xz に、バックドアが混入
- バックドア経由で root 権限の奪取、リモートコードの実行が可能
- 配布はベータ版ディストリビューションまでで、広い実害はなかった
- 攻撃者は数年の活動で信頼を獲得し、健康上の理由で活動を制限していた旧メンテナからメンテナ権限を正規に取得した上で攻撃コードを混入させた

課題・教訓

- 重要な OSS でもメンテナが１人で奮闘しているケースは多い
  → OSS を「公共財」として維持する活動が必要
  → OSS PJ の健全性を検証する仕組みが必要
- ソフトウェアが経た工程を検証する術が必要
  → ソフトウェアサプライチェーンセキュリティの強化が必要
- メンテナの「信頼」をどう担保するか
  → ？？？

OpenSSF
(Open Source Security Foundation)

OpenSSF

cybertrust

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

- https://openssf.org/
- OSS のセキュリティ強化・向上を目的とした、The Linux Foundation 傘下のプロジェクト
- 業界横断的なコミュニティとして目的の達成を目指す
- 参加企業・団体
  - プレミアメンバー (18)
    - AWS, Apple, Cisco, GitHub, Google, Intel, IBM, Microsoft, Red Hat, etc.
  - 一般メンバー (84)
    - Akamai, Blooomberg, Boeing, Comcast, docker, f5, GitLab, Goldman Sachs, SAP, SUSE, AMD, etc.
  - アソシエイトメンバー (21)
    - CMU, Eclipse Found., ISCAS, MITRE, OWASP, PSF, Rust Foun., TODO grp, etc.
- 日本からのメンバー：5社
  - サイバートラスト、サイボウズ、ルネサスエレクトロニクス、日立製作所、スズキ

OpenSSF の構成

Arun Gupta
OpenSSF Board Chair
VP and GM,Open Ecosystem Initiatives,
Intel Corporation

Governing Board (GB)

Technical Advisory Board (TAC)

Committees

- Marketing
- Governance
- Public Policy
- Technical Response
- Budget & Finance

Working Groups

- End Users WG
- AI/ML Security WG
- Best Practices WG
- Security Tooling WG
- Supply Chain Integrity WG
- Vulnerability Disclosures WG
- Securing Critical Projects WG
- Metrics & Metadata WG
- Securing Software Repositories WG
- Diversity, Equality, &Inclusion WG

Projects

- Alpha-Omega
- sigstore

Ref :
OpenSSF 2023 Annual Report
OpenSSF Town-Hall Mtg, 2024-06-06
(2023/3 以降正式な組織図がないので誤りあるかも)

OpenSSF Mission

The Open Source Security Foundation (OpenSSF) seeks to make it easier to sustainably secure the development, maintenance, and consumption of the open source software (OSS) we all depend on. This includes fostering collaboration, establishing best practices, and developing innovative solutions.

OpenSSF は我々全員が依拠する Open Source Software (OSS) の安全な開発・メンテナンス・利用が、継続的かつ容易に行えることを目指す。これには協働の促進、ベストプラクティスの確立、革新的な解法の開発を含む。

https://openssf.org/about/

OpenSSF Vision

OSS is a digital public good and as an industry, we have an obligation to address the security concerns with the community. We envision a future where OSS is universally trusted, secure, and reliable. This collaborative vision enables individuals and organizations in a global ecosystem to confidently leverage the benefits and meaningfully contribute back to the OSS community.

OSS は「デジタル公共財」であり、コミュニティと共にセキュリティへの懸念に対処する責任が我々にはある。我々は、OSS は誰もが信頼でき、安全で、頼ることのできるものである未来を思い描く。この協働のビジョンは、世界中の個人と組織が世界的なエコシステムのなかで、確信をもって OSS の恩恵を活用し、また OSS コミュニティへ価値ある貢献を行うことにを可能にする。

https://openssf.org/about/

OpenSSF に参加する意義とはなにか

OSS is a digital public good

OSS は「デジタル公共財」

OpenSSF ＝「共有地の悲劇」を起こさないための仕組み

- リソースを集約：資金、スキル、時間
- 取り組みを定義：Projects
- 枠組みを定義：GB, TAC, Committees, Working Groups

ただし、参加しているかどうかに関わらず情報は全てオープン
→ 参加することは共有財産を守るという意思表示

OpenSSF 主催の Global Events

cybertrust

Secure OSS Community Day

- 北米（NA）、欧州（EU）、日本（Japan）の三極で毎年開催される Open Source Summit で毎回併催
  - 昨年までは「OpenSSF Day」という名前だった
- 2024年の Japan は 10/30＠虎ノ門ヒルズ にて開催
  - https://events.linuxfoundation.org/soss-community-day-japan/

Secure OSS Fusion

- 2024年から開始された OSS セキュリティのトップイベント（？）
- 2024年は 10/22-23＠Atlanta
  - https://events.linuxfoundation.org/soss-fusion/

OpenSSF Japan Chapter

cybertrust

不定期（2～3ヶ月に一度）Meetup 開催中

- 10/3：OSSEU レポート、SLSA 概要紹介（豊洲 ルネサス本社）
- 11/1：SLSA Workshop 日本語版（六本木 国際文化会館）
  - 今後も OpenSSF 日本メンバーで企画・開催していきます
    （池田もメンバーかつ LF Japan Evangelist として積極的に参画します！）
- 今後のネタ：SOSS Fusion / OSSJ ラップアップ、CRA概要、etc.

参考：2024年内の主要イベント

- 10/28, 29：Open Source Summit Japan（虎ノ門ヒルズフォーラム）
- 10/30：Secure OSS Community Day（虎ノ門ヒルズフォーラム）
- 11/1：Japan SBOM Summit（六本木 国際文化会館）

OpenSSF への参画

様々な方法で情報を共有しています。

まずは情報収集と議論への参加を通じて、参画すべき WG/PJ/SIG を決めるのがよいと思います。

- https://github.com/ossf
  - Technical Working Group その他の Github レポジトリー覧
- https://lists.openssf.org/g/main
  - Mailing list
  - main は「親」のダミー ML なので、実際の ML は Subgroups を参照
- https://bit.ly/ossf-calendar
  - ミーティングカレンダー
- https://slack.openssf.org
  - Slack
- https://www.youtube.com/c/OpenSSF
  - Youtube チャンネル
- https://www.linkedin.com/company/openssf/
  - LinkedIn
- https://twitter.com/theopenssf
  - Twitter

※ OpenSSF Get Involved ページにリンクリストがあります

- https://openssf.org/getinvolved/

主要な OSS アクティビティ紹介

OSS アクティビティ: OSS PJ の評価・プロセス強化

OpenSSF Best Practice Badge

- OSS PJ の開発プロセスに関するベストプラクティスを基準として提供
  - ライセンス、ドキュメント、バージョン管理、テスト、バグ・脆弱性報告プロセス
- 自己検証し基準に合致している場合「バッジ」がもらえる

Scorecard

- 自動スキャンにより OSS PJ のセキュア度をスコア付けするツール
- GitHub Action またはローカルで実行

OSSアクティビティ: サプライチェーンセキュリティ

cybertrust

SLSA (Supply-chain Levels for Software Artifacts)

- 開発プロセスを対象としたサプライチェーンセキュリティフレームワーク
  - 要件・チェックリスト的な位置付け
  - ← → S2C2F はユーザーを対象としたフレームワーク
- 2024/10時点の最新版: v1.0 (2023/04/19)
  - トラックは「ビルド」のみ
    - トラック: セキュリティ強化対象のカテゴリ
    - 今後のバージョンでコーディング、ビルドPFオペレーションなどのトラックへ拡張
- セキュリティの実現度合いをレベルで表現
  - SLSA v1.0では Build Level 0~3 を定義
- 工程証跡(provenance)の生成、証跡への署名、ビルドプラットフォームのユーザーからの分離などを要求(要求事項はレベルによる)
- GitHub Actions がレベル3に対応
  - ビルドプラットフォームへの要求はクラウド指向が強い

in-toto

- サプライチェーンセキュリティのためのフレームワーク
- in-toto Attestation Framework が工程証跡(provenance)のスキーマとして SLSA から参照されている
- 真正・完全な工程メタデータと SBOM を統合するための仕組みである SBOMit も in-toto Attestation を参照している
  - CNCF (Cloud Native Computing Foundation) 傘下の PJ(OpenSSF 傘下ではない)

OSSアクティビティ: サプライチェーンセキュリティ

S2C2F (Secure Supply Chain Consumption Framework)

- OSS 利用者を対象としたサプライチェーン セキュリティフレームワーク
  - ← → SLSA は開発プロセスを対象としたフレームワーク
- 2024/10時点の最新版: v1.1 (2022/10/19)
- Level 1 : 最低限の OSS 管理
  - 利用する OSS の棚卸、脆弱性スキャン、ライセンススキャン、手動アップデート
- Level 2 : 安全な OSS 活用と MTTR(平均修復時間)の改善
  - インシデント対応計画、自動アップデート、SW の完全性検証
- Level 3 : ゼロデイ攻撃からの防御
  - ソースコードの把握、マルウェアスキャン、provenance 生成・検証、取得元の制限
- Level 4 : より先進的な防御
  - 信頼できるPFでのリビルド、バイナリへの署名付与、SBOM の生成と署名付与
  - 参考: https://github.com/ossf/s2c2f/blob/main/specification/framework.md

OSS アクティビティ: サプライチェーンセキュリティ

SPDX (Software Package Data eXchange)

- 標準 SBOM フォーマットの一角
- The Linux Foundation 主導
- 2024/10 時点の最新版: v3.0
- 発祥はライセンス管理から、v3.0 で脆弱性情報のための
  フィールドも拡張

CycloneDX

- 標準 SBOM フォーマットのもう一つの一角
- OWASP (Open Web Application Security Project) 主導
- 発祥がセキュリティからであり脆弱性情報の記述に強い
  - CycloneDX は直接 OpenSSF 傘下の PJ ではないが、OWASP は OpenSSF の Associate メンバーであり、かつ重要な PJ なのでここに記した

OpenVEX (Open Vulnerability EXchange)

- 脆弱性情報フォーマットを標準化する試み

OSS アクティビティ: サプライチェーンセキュリティ

cybertrust

GUAC

- SBOM、依存性情報、脆弱性情報のグラフによる可視化

Protobom

- 統一的な SBOM データ構造を表現するためのプロトコルバッファ
- デファクトが SPDX, CycloneDX と二分している状況に対して、SBOM を扱うソフトウェアには有用

OSS アクティビティ: サプライチェーンセキュリティ

cybertrust

[sigstore]

- 署名と署名検証のためのツールおよびインフラ
  - K8S のコンテナ検証、LLVM のリリース署名で採用済み
  - 仕組み自体は特に対象を限定せず汎用
    （コード、コンテナ、パッケージ、SBOM 等に適用可能）
- OSS 開発者が手軽に使えるよう、カギの管理や複雑な手順を排除することが最大の特長

OSS アクティビティ: セキュアな開発

cybertrust

LF Training

- 「セキュアソフトウェア開発 (LFD121-JP)」
- Developing Secure Software (LFD121)

OpenSSF ガイド（日本語訳）

- C および C++ のコンパイラ・オプション強化ガイド
- ソースコード管理プラットフォーム設定のベストプラクティス
- より安全なソフトウェア開発のための簡潔なガイド
- オープンソースソフトウェアを評価するための簡潔なガイド
- セキュリティ研究者のためのオープンソース ソフトウェア プロジェクトと脆弱性の公表を調整するためのガイダンス
- npm ベストプラクティス ガイド
- オープンソース プロジェクト向けに協調的脆弱性開示プロセスを実装するためのガイド

参考：OpenSSF 以外

ソフトウェア管理に向けた SBOM の導入に関する手引 Ver.2.0

- 2023/07/28 の Ver.1 に続き、2024/08/29 に経済産業省 サイバーセキュリティ課が Ver.2 を公表
- SBOM の導入・活用に向け、どこから手を付けるべきかがまとめられている
- Ver.2 では 第7章「脆弱性管理プロセスの具体化」、付録「SBOM対応モデル」、「SBOM取引モデル」が加筆
- 特に脆弱性管理を SBOM の重要なユースケースとして位置づけたことが注目される

セキュリティ透明性確保に向けた可視化データ活用～脆弱性管理編～

- セキュリティ・トランスペアレンシー・コンソーシアムが 2024/10/21 に公表
- SBOM を脆弱性管理に活用するための知見集

まとめ

まとめ

- ソフトウェア、なかでも OSS のセキュリティとサプライチェーンセキュリティの強化・改善は社会を維持するための課題
- OpenSSF は、OSS のセキュリティ・サプライチェーンセキュリティ強化の中心的役割を果たすための The Linux Foundation 傘下の PJ
- OpenSSF は Digital public good = デジタル公共財 である OSS に対して「共有地の悲劇」を起こさないための仕組み
- OSS へ参画・貢献する方法は色々ある
  - 開発への参画
  - イベントへの参加・議論
  - スポンサー

まとめ：サイバートラストの場合

サイバートラストは様々な OSS のユーザかつコントリビュータとして
OpenSSF への積極的な参画を始めとするコミュニティへの貢献をコミットし
セキュアなソフトウェアおよびサプライチェーンを実現します

- SBOM 管理
- 脆弱性管理

- ビルドツリースキャン
- 脆弱性管理

- エンタープライズ向け Linuxディストリビューション
- RHEL 互換
- 長期サポート

- IoT・組込み向け Linuxディストリビューション
- 超長期脆弱性サポート
- IEC62443-4-2 認証取得支援

参考：サプライチェーンセキュリティ アクティビティマップ

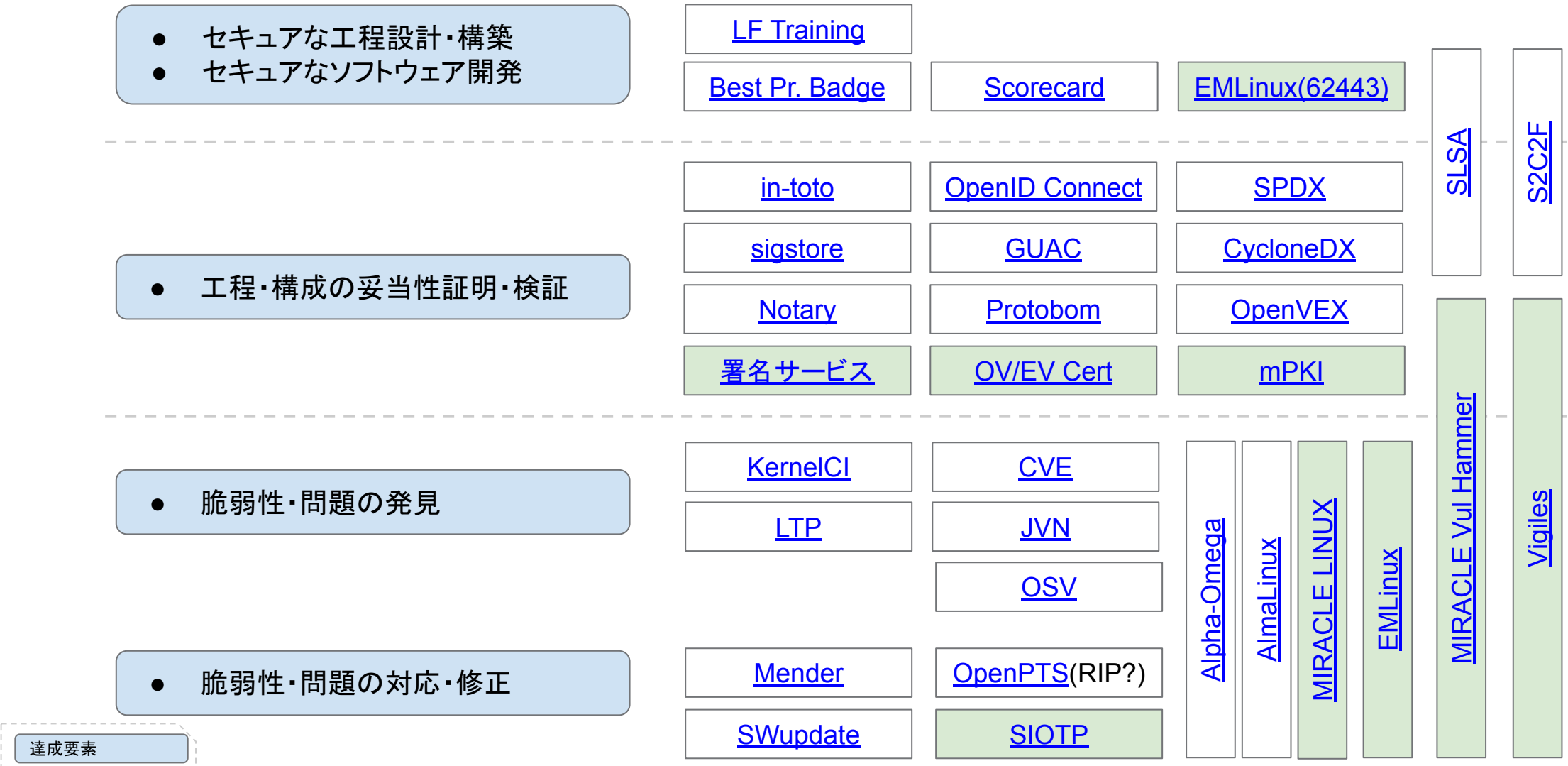
cybertrust

- セキュアな工程設計・構築
- セキュアなソフトウェア開発

- 工程・構成の妥当性証明・検証

- 脆弱性・問題の発見

- 脆弱性・問題の対応・修正



達成要素
OSS
CTJ 商材

cybertrust

すべてのヒト、モノ、コトに 信頼を

留意事項

本資料に記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。
その他本資料に記載されているイラスト・ロゴ・写真・動画・ソフトウェア等は、当社または第三者が有する知的財産権やその他の権利により守られております。
お客様は、当社が著作権を有するコンテンツについて、特に定めた場合を除き、複製、改変、頒布などをすることはできません。
本資料に記載されている情報は予告なしに変更されることがあります。また、時間の経過などにより記載内容が不正確となる場合がありますが、当社は、当該情報を更新する義務を負うものではありません。