オープンソースソフトウェアをより安全にするための取組み
- オープンソースソフトウェアの産業適用状況
- オープンソースソフトウェアとしての脆弱性対策
- The Linux Foundationの役割

Yoshiya ETO
Fellow, The Linux Foundation
Oct. 2023

THE LINUX FOUNDATION

自己紹介

Linux Foundation Leadership Teams

LEADERSHIP | BOARD OF DIRECTORS | FELLOWS | ADVISORY BOARD

GREG KROAH-HARTMAN
Fellow

JANINA SAJKA
Fellow

LINUS TORVALDS
Fellow

RICHARD PURDIE
Fellow

SHUAH KHAN
Fellow

THOMAS GLEIXNER
Fellow

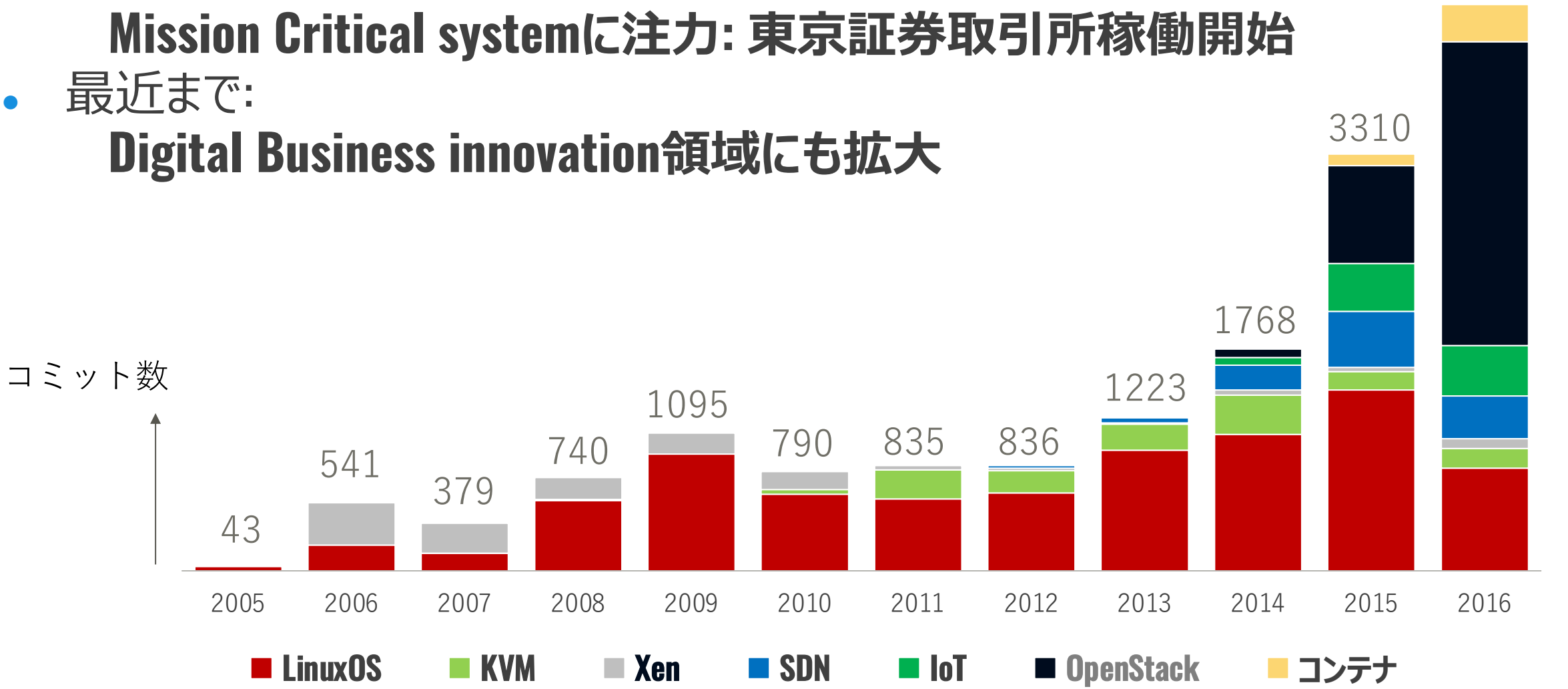
TILL KAMPPETER
Fellow

YOSHIYA ETO
Fellow

THE LINUX FOUNDATION

前職でのオープンソース開発実績

- 2010年頃まで:
  Mission Critical systemに注力: 東京証券取引所稼働開始
- 最近まで:
  Digital Business innovation領域にも拡大



The Linux Foundationご紹介

- 2007年設立時のメンバー/活動領域
  - 主要メンバー: Fujitsu, Hitachi, HP, IBM, Intel, NEC, Oracle
  - 活動領域: promote, protect, and advance Linux
- 2023年の状況

2,300+
メンバー企業
（41か国から）

100%
Fortune 100
Tech&Telecomから

740,000+
コードを貢献する
開発者

950+
オープンソース
プロジェクト

$100B
共有技術の
資産価値

対象プロジェクト: さまざまな技術分野・業種

THE LINUX FOUNDATION

技術分野

セキュリティ	Let's Encrypt, CII Core Infrastructure Initiative, OpenSSF, Falco, ./rtp, Confidential Computing Consortium, seL4, Open Security Controller
ネットワーク	LF Networking, OpenDaylight, fd.io, Clusterduck Protocol, DENT, DANOS, AKRAINO
クラウド	Cloud Native Computing Foundation, kubernetes, argo, envoy, KUDO, Crossplane, soda foundation, Cloud Foundry, Istio
ブロックチェーン	Hyperledger, Hyperledger Fabric, Accord Project, ERGO, DIF
エッジ/IoT	LF Edge, yocto project, Zephyr, ACRN, Dronecode, FLEDGE, Sound Open Firmware, OpenEEW
Web	node.js, OpenJS Foundation, GraphQL, appium, jQuery, Reactive Foundation, DOJO, ESLint
AI	LF AI, ONNX, Horovod, Delta Lake, ForestFlow, JanusGraph, kepler.gl, Ludwig, PyTorch
CI/CD	CD Foundation, Jenkins, Spinnaker, TEKTON, TERN, StackStorm, Vitess, etcd, SPIRE
ハードウェア	RISC-V, OpenPOWER, CHIPS Alliance, UNIMATRIX, 3MF Consortium
標準	Alliance for Open Media, OpenChain, Community Data License Agreement, Joint Development Foundation, SPDX, Open Manufacturing Platform, Open Container Initiative

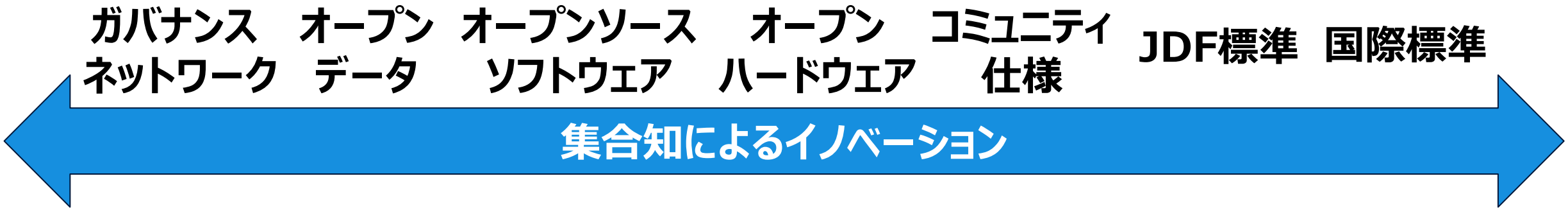
業種

自動車	Automotive Grade Linux, ELISA, KernelCI
エネルギー	LF Energy, RIAPS, EM2, POWSYBL, GXF, CoMPAS, OpenEEmeter, OperatorFabric
フィルム/映画	ASWF, OpenColorIO, OpenVDB, OpenEXR, OpenTimelineIO, OpenEXR, OSL Open Shading Language
金融/財務	FINOS, EGEND, FDC³, Cloud Service Certification, FATE, Perspective, openMAMA, morphir
通信	ONAP, Anuket

The Linux Foundationのプロジェクトで行われていること

- プラットフォームソフト・データをオープンソース化: 重要だが競争領域でない
  - 共通技術で製品差異化/ベンダーソリューションを極小化
    ⇔自社でオープンソースエンジニアを抱えて最大限の価値教授
- 他社と共同開発/投資を共有: ダーウィンの進化論的開発モデル
  - 複数のアイデアを混ぜ合わせて独自な進化/自由に作れない
    他社アイデアでエコシスム拡大する場合もある: K8sのgoogle内議論

オープンコラボレーションに幅広い役割



参画に必要な経験知:

法的な調整や構造
業界別の経験
技術分野毎の経験
成功の実績

拡大していくために必要な経験知:

セルフサービスオプション
アンブレラと柔軟なプロジェクト構造
メンバーシップモデルとネットワーキング効果
システムとプロセスの注力ポイント
厳格なIP管理とセキュリティの注力ポイント

オープンソースソフトウェア利用状況

THE LINUX FOUNDATION

Auditしたソフトウェアの99%にオープンソースが取り込まれている

Auditしたソースコードのうち78%はオープンソースのコード

Source: 2022 Backduck OSSRA

https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2022-ossra-report.pdf

オープンソースソフトウェアの定義

1. Free Redistribution: 再配布の自由
2. Source Code: ソースコード公開の自由
3. Derived Works: 派生ソフトウェアの作成と配布の自由
4. Integrity of The Author's Source Code: 作者のソースコードの完全性
5. No Discrimination Against Persons or Groups: 個人やグループに対する差別の禁止
6. No Discrimination Against Fields of Endeavor: 利用する分野に対する差別の禁止
7. Distribution of License: 再配布時の追加ライセンス不要
8. License Must Not Be Specific to a Product: 特定製品でのみ有効なライセンスの禁止
9. License Must Not Restrict Other Software: 他のソフトウェアを制限するライセンスの禁止
10. License Must Be Technology-Neutral: ライセンスは技術中立的でなければならない

https://opensource.org/osd/
https://opensource.jp/osd/osd19/

一部定義の詳細

1. 再頒布の自由

「オープンソース」であるライセンスは、出自の様々なプログラムを集めたソフトウェアディストリビューションの一部として、ソフトウェアを販売あるいは無料で頒布することを制限してはなりません
ライセンスは、このような販売に関して印税その他の報酬を要求してはなりません

6. 利用する分野に対する差別の禁止

ライセンスはある特定の分野でプログラムを使うことを制限してはなりません

例えば、プログラムの企業での使用や、遺伝子研究の分野での使用を制限してはなりません

BUSL/BSL, Business Source License, はオープンソースソフトウェアではない

https://opensource.jp/osd/osd19/

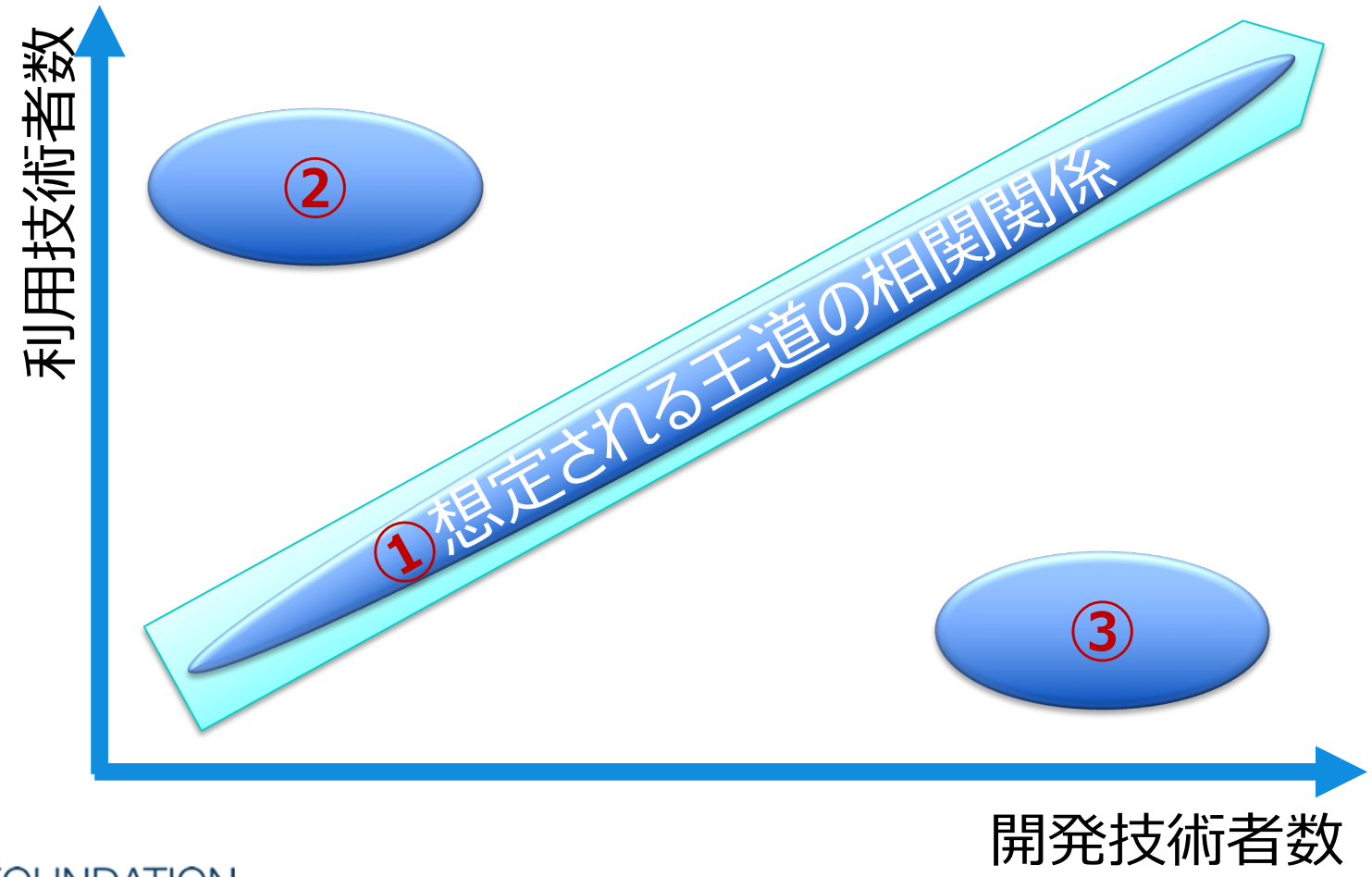
ライセンス変更の事例

Company	Project	元License	変更後License	変更日
HashiCorp	Terraform	MPL-2.0	BUSL	2023
Elastic	ElasticSearch and Kibana	Apache-2.0	Elastic License & SSPL	2021
MongoDB	MongoDB	AGPL-3.0	SSPL	2018
Confluent	Confluent	Apache-2.0	Confluent Community License	2018
Redis Labs	Redis Stack	AGPL-3.0	SSPL and Redis Source Available License	2018 2021
Timescale	TimescaleDB	Apache-2.0	Timescale License	2018
Cockroach Labs	CockroachDB	Apache-2.0	BUSL	2019
Airbyte	Airbyte	MIT	Elastic License	2021

なぜオープンソースソフトウェアライセンスが変更される?

1. VCによる早期のマネタイズ要求
2. 特定企業のみによる開発/ソースコード公開
   - オープンソースコミュニティの健全性の検証
     scorecardによる数値化
     https://securityscorecards.dev/

オープンソースプロジェクトの種類・何処をめざすか?



オープンソースソフトウェア利用状況

THE LINUX FOUNDATION

Auditしたソフトウェアの99%にオープンソースが取り込まれている

Auditしたソースコードのうち78%はオープンソースのコード

Source: 2022 Backduck OSSRA
https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2022-ossra-report.pdf

現在のソフトウェア開発手法/潮流= 事業のため源流開発

GAFAM等BigTechが作る世界的な潮流

① オープンソースプロジェクトで技術開発
② 開発技術・既存技術で製品・サービス開発
③ 製品・サービスからのフィードバック投資

④ 利用技術者などのエコシステム形成

オープンソースプロジェクト活用

- 再発明を避け機能開発速度を上げる
- 開発に参加する複数の企業が
  自身の事業最適化にしのぎを削る

オープンソースの脆弱性と影響

- OpenSSL: Heart Bleed: 2013年12月 CVE-2014-0160 record created
- Apache Stratus2: 2017年1月29日 CVE-2017-5638 record created..
- Log4Shell: 2021年11月26日 CVE-2021-44228 record created

防衛・経済活動で幅広く使われていて影響が甚大

品質が悪いわけではない

オープンソースの脆弱性と経済影響

- Heartbleed=OpenSSLの脆弱性, 2014年4月発覚
  - 三菱UFJニコスのWebから894人分の個人情報流出: 2014/4/18
    source: https://xtech.nikkei.com/it/article/NEWS/20140421/551884/
  - メニコンのWebからクレジットカードなどの個人情報漏洩: 2018/5/17
    source: https://xtech.nikkei.com/atcl/nxt/column/18/00001/00561/
- Apache Struts2: source: https://saas.gmocloud.com/service/websecurity/threat/struts2.html
  - 国土交通省で約20万件の顧客情報が流出: 2017/6/6
  - 総務省で2.3万人の個人情報が流出: 2017/4/13
  - GMOペイメントゲートウェイが運営しているサイトから個人情報72万件が流出: 2017/4/5
  - ぴあが運営するサイトからクレジットカード情報3.2万件が流出の可能性: 2017/3/7
- Log4Shell = Log4jの脆弱性: 進行中
  - 栃木県警察*も注意喚起: https://www.pref.tochigi.lg.jp/keisatu/n33/ccat/log4shell.html

*: 同様の情報: 滋賀県警、広島県警、長崎県警、流山商工会議所、彦根商工会議所

オープンソース利活用上の脆弱性対策 –第Zero期

- OSS: 誰かが、基本自分のシステムのために開発
  - 開発者想定のワークロードには良い品質

- 製品開発向けに自社内で十分品質確保
  - 検出障害は製品ごとに管理・維持
  - オープンソースのバージョンアップ毎に再Fix・テスト…

- **品質確保段階で前述の脆弱性を検出・修正できなかった**

オープンソースコミュニティとしての脆弱性対策 –第一期

- **Core Infrastructure Initiative, CII: Heartbleed及び類似事例対策**

  Source: https://internet.watch.impress.co.jp/docs/news/646136.html

  初期メンバー: **Amazon Web Services、Cisco、Dell、Facebook、Fujitsu、Google、IBM、Intel、Microsoft、NetApp、Rackspace、VMware**

  1. 重要な開発者がフルタイムでオープンソースプロジェクトに取り組むためのフェローシップ、セキュリティ監査、コンピューティングおよびテストインフラ、旅行、対面会議**予算**
     - OpenSSL: $550K, NTPsec: $150K, ntpd: $180K, OpenSSH: $50K, 他

       https://en.wikipedia.org/wiki/Core_Infrastructure_Initiative
  2. **Best Practices Security Badge Program**
     後の**scorecard by OpenSSF**の一部として取り込まれている

オープンソースソフトウェア利用者の脆弱性対策 –第二期

- 大統領令により政府調達要件にSBOM必須化: 2021年5月12日に署名

President Biden‘s Cybersecurity Executive Order 14028 any company that sells software to the federal government will be mandated to provide a complete Software Bill of Materials (SBOM)

- White HouseがOpen Source Security Summit主催
  - 源流に遡って対策を打たないと

Open Source Security Summit要約: ホワイトハウス主催

https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

- 本日ホワイトハウスは、政府と民間企業の関係者を招集し、オープンソースソフトウェアのセキュリティを向上させるための取り組みと、新たなコラボレーションによって改善を迅速に進める方法について議論いたしました
- 国家安全保障分野で使用されているソフトウェア含め、主要なソフトウェアパッケージのほとんどはオープンソースソフトウェアを取り込んでいます
  ソフトウェアは、経済の全セクターであらゆる場所に存在し、米国人が毎日使用する製品やサービスの基盤となっています
- オープンソース・ソフトウェアは、独自の価値をもたらすと同時に、その使用範囲の広さと継続的なセキュリティ・メンテナンスに責任を負うボランティアの数から、独自のセキュリティ上の課題も抱えています

Open Source Security Summit要約: ホワイトハウス主催

https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

- 会議には、Anne Neuberger: 国家安全保障副顧問（サイバーおよび新技術担当）、Chris Inglis: 国家サイバー長官、科学技術政策局、国防総省、商務省、エネルギー省、国土安全保障省、サイバーセキュリティおよびインフラセキュリティ局(CISA)、米国標準技術研究所、米国科学財団の職員が参加いたしました
- 民間企業では、Akamai、Amazon、Apache Software Foundation、Apple、Cloudflare、Facebook/Meta、GitHub、Google、IBM、The Linux Foundation、Open Source Security Foundation、Microsoft、Oracle、RedHat、VMWareが参加しています
- バイデン大統領は、ソフトウェアセキュリティを国家的な優先事項としています
  彼のサイバーセキュリティに関する大統領令は、安全なソフトウェア開発ライフサイクル手法を使用し、特定の連邦セキュリティガイダンスを満たした企業のみが連邦政府に販売できるようにすることを要求しています

Open Source Security SummitII要約: 米国行政機関主導

https://www.linuxfoundation.org/press-release/linux-foundation-openssf-gather-industry-government-leaders-open-source-software-security-summit/

- 本会合は米国行政機関主導のもと、**The Linux Foundationが主催**しました
  米国政府機関(NSC, ONCD, CISA, NIST, DOE, OMB)及び主要企業37社90名が参加
- LFとOpen Source Security Foundationは様々な経済セクターから情報提供を受け、OSSとソフトウェアのサプライチェーンセキュリティに幅広く対応する初の実践計画を発表
- この計画では3つの目標に対する10の主要な問題が明らかにされ、解決策実践には、2年間で約1億5千万ドルの資金が必要
  I. セキュアな OSS の開発・提供
  II. 脆弱性検出と修復方法の強化
  III. エコシステムにおけるパッチ適用までの時間短縮
- 実践に向けAmazon,Ericsson,Google,Intel,Microsoft,VMWareが3,000万ドル以上の資金提供
- OpenSSF参画企業が 1億1000万ドル以上かけ実践中のOSSセキュリティ対策活動で当面補う

Open Source Security SummitII要約: 米国行政機関主導

https://www.linuxfoundation.org/press-release/linux-foundation-openssf-gather-industry-government-leaders-open-source-software-security-summit/

- 本会合は米国行政機関主導のもと、The Linux Foundationが主催しました
  米国政府機関(NSC, ONCD, CISA, NIST, DOE, OMB)及び主要企業37社90名が参加
- LFと**Open Source Security Foundation**は様々な経済セクターから情報提供を受け、オープンソース開発とソフトウェアのサプライチェーンセキュリティに幅広く対応する初の実践計画を立案
- この計画では**3つの目標に対する10の主要な問題**を明らかにした
  解決策実践には、**2年間で約1億5千万ドルの資金**が必要
  I. **OSS**開発をセキュアにする
  II. 脆弱性の検出と修復の強化
  III. エコシステムのパッチ応答時間を短縮
- 実践に向けAmazon,Ericsson,Google,Intel,Microsoft,VMWareが3,000万ドル以上の資金提供
- OpenSSF: Premier member=21社、General member=70社(うち日本から5社)

Open Source Security Summit Japan: 2022/8/23

- 経済産業省サイバーセキュリティ・情報課　上村審議官
- 米国ホワイトハウスの国家サイバー長官　**Chris Inglis**
- **The Linux Foundation: Jim Zemlin, OpenSSF: Brian Behlendorf**
- 参加企業: **20**社以上の企業・団体が出席
  - 日立製作所、富士通、**NEC**、**NTT**データ、トヨタ、**LINE**、産総研、**IPA**他

3つの目標

1. **OSS開発をセキュアにする**
   - コードとオープンソースパッケージのセキュリティ上の欠陥や脆弱性の防止に注力
2. 脆弱性の検出と修復の強化
   - 欠陥の検出、それらを修正するプロセスの強化
3. エコシステムのパッチ応答時間を短縮
   - 修正の配布、実装のための応答時間を短縮

OSS開発をセキュアにする

THE LINUX FOUNDATION

ストリーム 1：基本基準を満たすセキュアなソフトウェア開発の教育と認定 をすべての人に提供

- **Developing Secure Software (LFD121)**
- **Secure Software Development: Requirements, Design, and Reuse (LFD104x)**
- **Secure Software Development: Implementation (LFD105x)**
- **Secure Software Development: Verification and More Specialized Topics (LFD106x)**

ストリーム 2：10,000以上のOSS コンポーネント対象にリスク評価パブリックダッシュボード開設

- ベンダー中立な指標に基づくリスク評価パブリックダッ シュボード: **LFX.io**

ストリーム 3：ソフトウェアリリースでのデジタル署名の採用を加速

- **Free sigstore Signing Service to Confirm Origin and Authenticity of Software**

ストリーム 4：メモリセーフでない言語を置き換えることで、多くの脆弱性の根本原因を排除

脆弱性の検出と修復の強化

THE LINUX FOUNDATION

ストリーム 5： OpenSSF内にOpen Source Security Incident Response Team設立

- クリティカルな脆弱性対応時、セキュリティの専門家がオープンソースプロジェクトを支援

ストリーム 6：メンテナーと専門家による新しい脆弱性の検出加速

- 高度なセキュリティツールと専門家のガイダンスをメンテナーに提供

ストリーム 7：1 年に1 度/最大200のクリティカルOSSコンポー ネントをサードパーティコードレビュー

ストリーム 8：クリティカルなOSS コンポーネント決定調査の改善のため、業界全体でデータ共有

エコシステムのパッチ応答時間を短縮

ストリーム 9：あらゆるところにSBOMを

- SBOMツールとトレーニングを 改善し採用を促進: SPDX, OpenChain認証

ストリーム 10：最もクリティカルな10のOSS ビルド システム、パッケージマネージャー、およびディストリビューションシステムを強化

オープンソースソフトウェア業界のSBOMの意味

- オープンソースソフトウェアのライセンス間の矛盾
  - 有名な事例: **GPL v.s.** 昔の**BSD**ライセンス
    - ✓ **GNU GPL**の第**6**項抜粋
      You may not impose any further restrictions on the recipients' exercise of the rights granted herein.
    - ✓ 昔の**BSD**ライセンス
      All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
  - **Apache Software Foundation Web**サイト: **GPLv2**と**Apache License ver2.0**は両立しない
- **Copyleft**
  - インストール条項のあるライセンス: **GPL v.3**
- 商用に使えないライセンス

古からオープンソースを商用利用するには、ライセンス管理する必要があった

システムを安全に保つ

THE LINUX FOUNDATION

- OpenSSF活動を活用してオープンソースを評価/安全なコードを書く/流通させる
  - 開発者をトレーニングする: LFD104-JPx, LFD105-JPx, LFD106-JPx, LFD121-JP
  - **Scorecard: 複数の視点でオープンソースプロジェクトの健全性を可視化**
  - Sigstore: 無償の署名ツール
- 内部システム/製品/サービスの**SBOM**を作って脆弱性検出に備える
  - GitのbuildにSBOM生成ツールが既に統合されています: **sbom-tools**
  - SBOMの標準仕様はISOで既に規定され、かつ更新されています: **SPDX 3.0**
- 脆弱性報告に速やかに修正適用ができるシステム構成/運用にしておく
  - テスト自動化追求
  - 定期的な修正適用・バージョンアップを計画
  - **ステートレス**なマイクロサービス/コンテナアプリケーションでシステム構築

Linux Foundationとは　–最後にもう一度、個人的な思い-

- 501(c) (6)で規定される米国非課税団体
  - カリフォルニア州で登記
  - Form 990で内国歳入庁に毎年申告
- 社会基盤サービスとしてのオープンソースソフトウェアを維持する財団

  米国・欧州・日本での
  - 文化的な社会基盤サービスへの認識の違い
  - 政府のオープンソースソフトウェアの重要性の認識の違い
- 先進技術のファンダメンタルに関する議論が活発
  - Generative AI生成ソースコードのSBOM生成などが検討されている

現在のソフトウェア開発手法/潮流= 事業のため源流開発

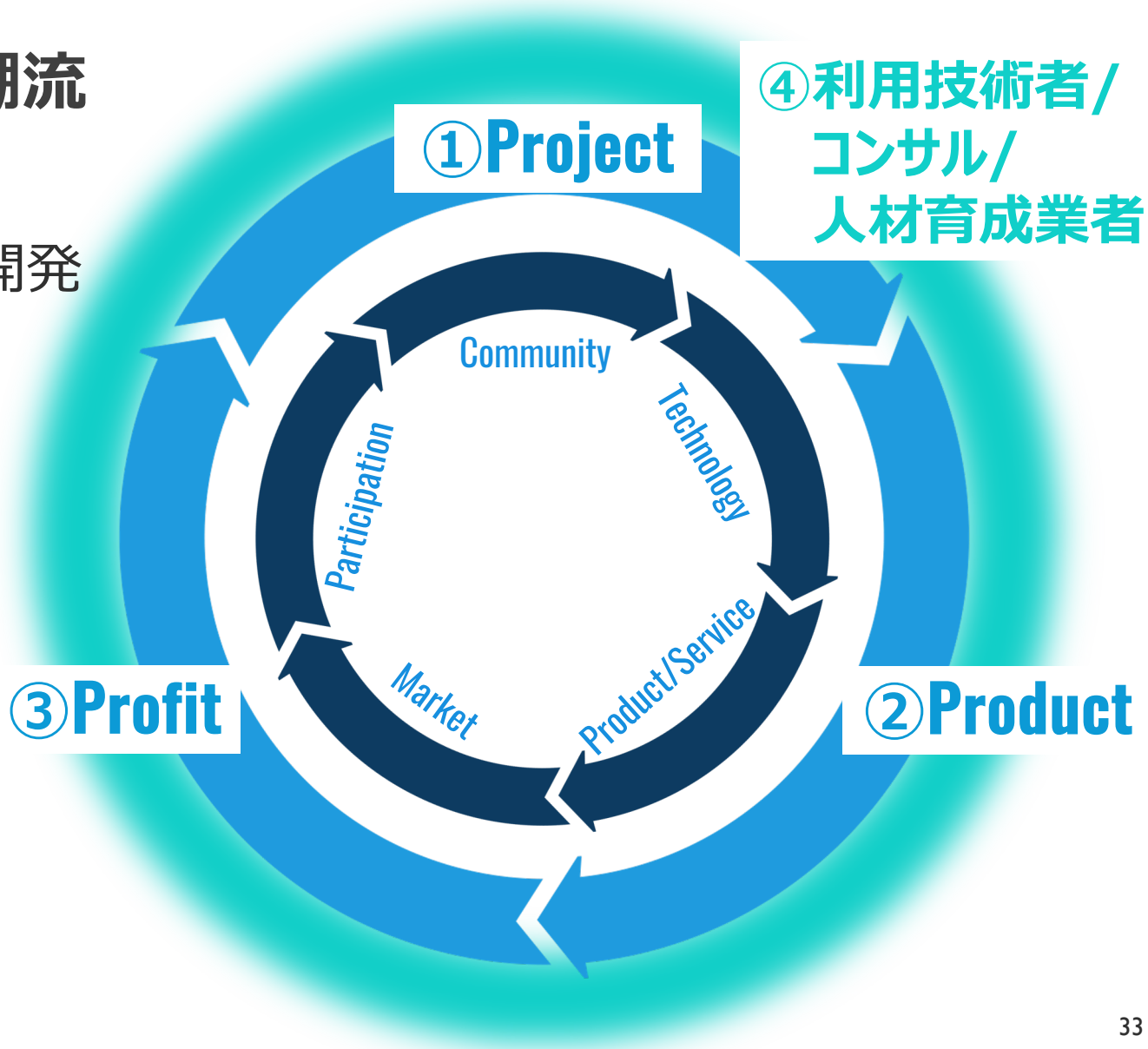
GAFAM等BigTechが作る世界的な潮流

① オープンソースプロジェクトで技術開発
② 開発技術・既存技術で製品・サービス開発
③ 製品・サービスからのフィードバック投資

④ 利用技術者などのエコシステム形成

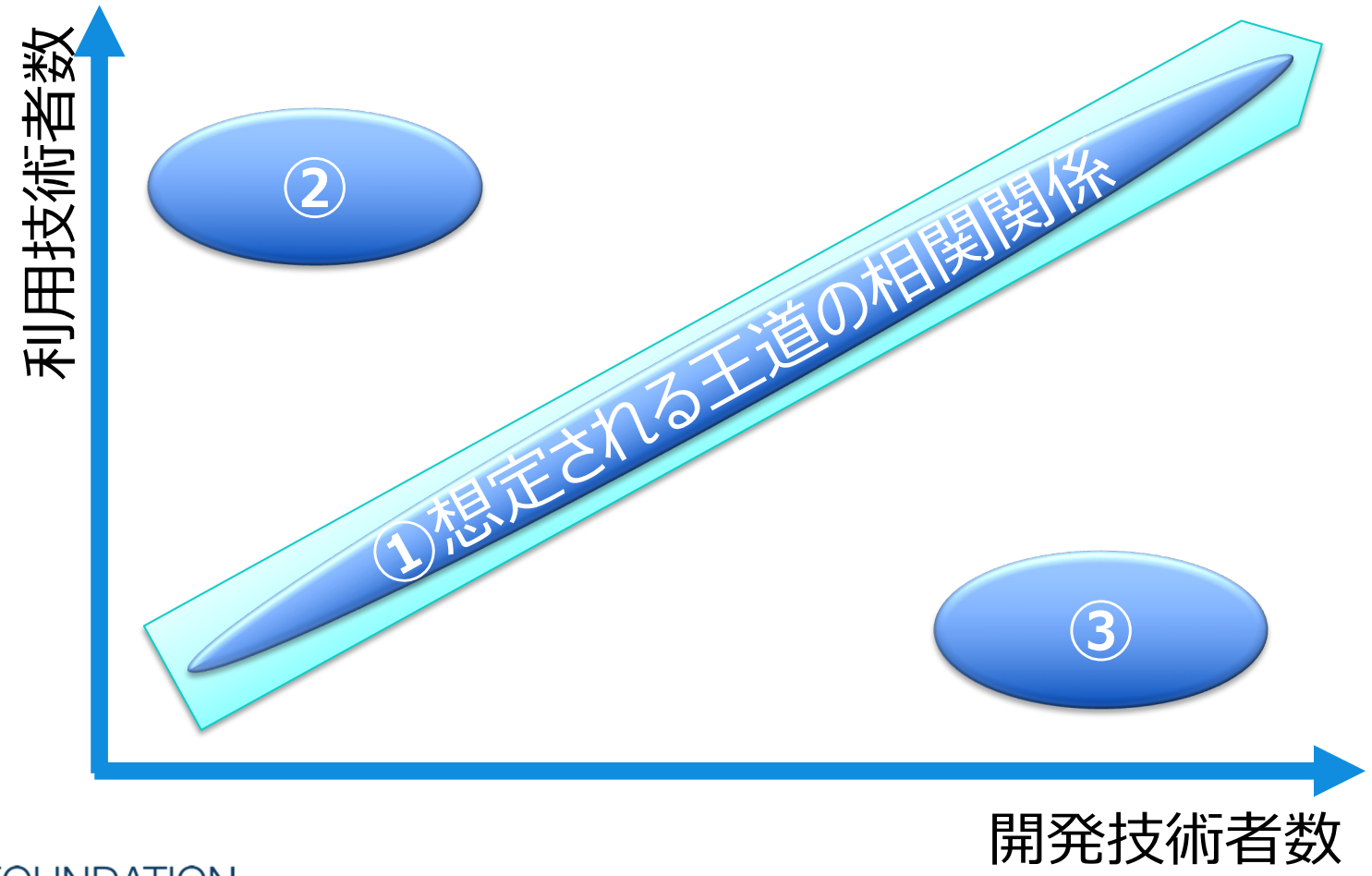
オープンソースプロジェクト活用

- 再発明を避け機能開発速度を上げる
- 開発に参加する複数の企業が
  自身の事業最適化にしのぎを削る



THE LINUX FOUNDATION

オープンソースプロジェクトの種類・何処をめざすか?



ありがとうございました

THE LINUX FOUNDATION