Orchestrating a brighter world NEC

【MTG】 OSSのセキュリティ・ライセンスリスクを回避してOSSを有効活用するには

2021年3月5日(金) 12:00~12:45

NEC 先端SI技術開発本部 OSS推進センター
米嶋 大志

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

0. はじめに

自己紹介

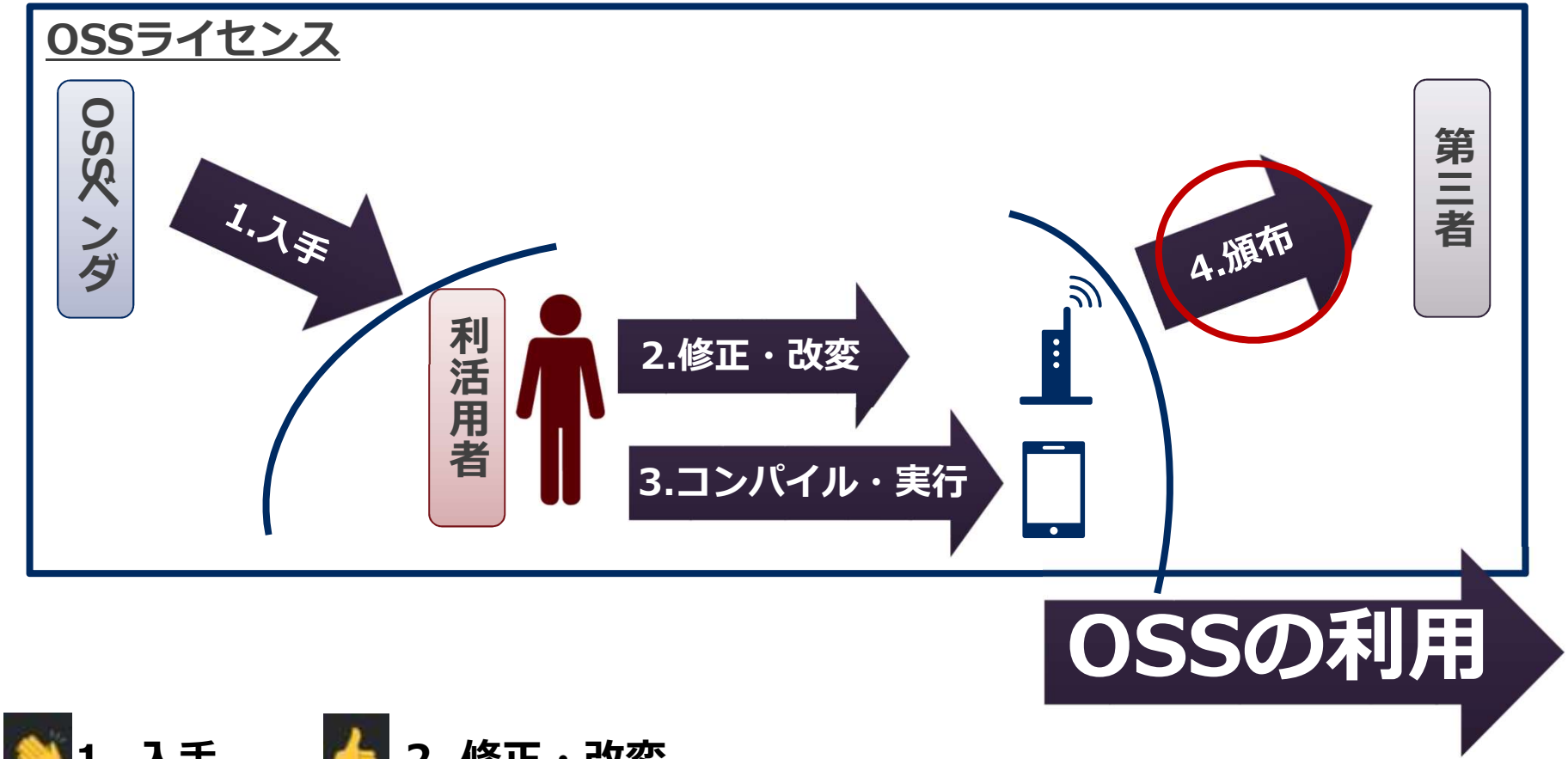
名前
：米嶋 大志

会社
：NEC（新卒、6年目）

部署
：OSS推進センター

担当業務
：社内へのOSS活用促進
：BlackDuckの製品担当

Q.1)OSSライセンスが許諾しているのはどの場面か？



1. 入手
2. 修正・改変
3. 実行
4. 頒布
5. その他

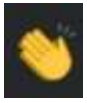
ライセンス条件に従って、
第三者へ提供

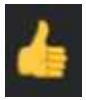
A. 4

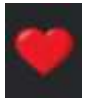
Q.2)OSSを選定するにあたって、適切なパッケージ選択は？

前提

- OSはRHEL 8
- 顧客環境に構築するWebアプリケーション(3年予定)、選定を頼まれている
- コミュニティが提供しているVer.は10.0(α版)系、9.0系、8.5系、7.0系(6.5未満は既にEoL)
- RHELのBaseリポジトリには、コアパッケージに含まれる7.0系が提供


1. コミュニティ版10.0(α版)系の最新Ver.


2. コミュニティ版9.0系の最新Ver.


3. コミュニティ版9.0系、8.5系、7.0系の各最新版ならどれでも良い


4. 最新版ではないがRHELリポジトリに含まれるパッケージ


5. その他

A. 4＞2＞3、1

今日のゴール

1. 不用意なOSSの利用にはリスクがあることの理解

2. そのリスクをコントロールして、

**　　社内で活用を促進できるよう体制を考える**

+@. NECのソリューションを理解していただく

目次

0. はじめに（←いま）

1. 一般的なOSSのリスクとは

2. NEC社内で実施しているOSS管理体制について

3. NECがご支援できるソリューション紹介
　　＋BlackDuckのデモ

プロファイル

社名	NEC（商号：日本電気株式会社 英文： NEC Corporation)
本社	東京都港区芝五丁目7番1号　地図 Tel: 03-3454-1111
創立	1899年(明治32年)7月17日
代表取締役	執行役員社長 兼 CEO 新野 隆 執行役員副社長兼 CFO 森田 隆之
資本金	3,972億円 (2020年3月末現在)
売上収益	2019年度実績 単独 1兆7,897億円 連結 3兆952億円
グループ主要事業	社会公共、社会基盤、エンタープライズ、ネットワークサービス、 システムプラットフォーム、グローバル
従業員数	単独 20,125名(2020年3月末現在) 連結 112,638名(2020年3月末現在)
会社数	連結子会社 300社(2020年3月末現在)

OSS推進センター 社内での役割

- 社長
- 取締役会
  - クロスインダストリーユニット
  - グローバルビジネスユニット
    - RHQ（地域統括会社）
  - 社会公共ビジネスユニット
    - 支社・支店
  - 社会基盤ビジネスユニット
  - エンタープライズビジネスユニット
  - ネットワークサービスビジネスユニット
  - デジタルビジネスプラットフォームユニット
  - システムプラットフォームビジネスユニット
  - ビジネスイノベーションユニット
  - 研究開発ユニット
  - コーポレート

(2020年4月1日現在)

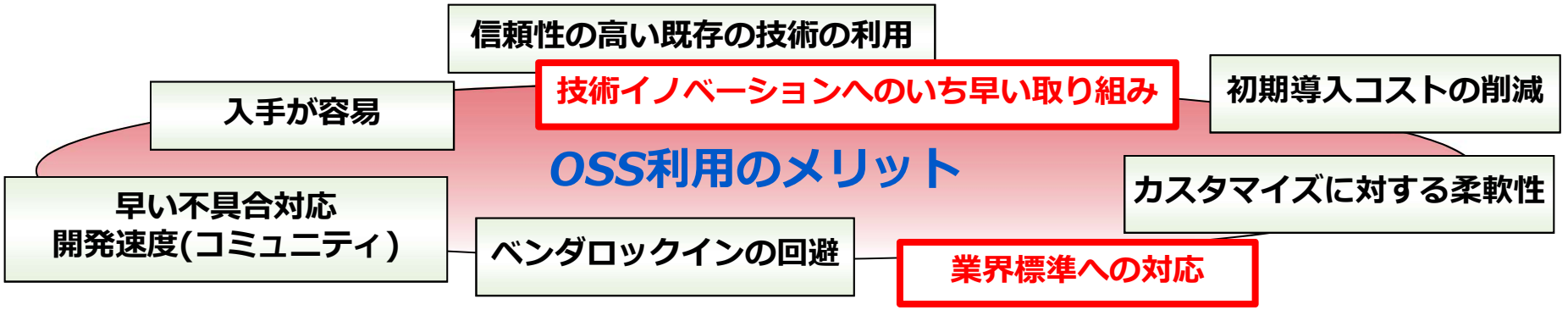
OSS推進センター活動内容

OSS全社 啓発 普及	ＯＳＳを安全に活用するための 社内ルール・基盤・情報を整備 ＳＩ・製品事業におけるＯＳＳ活用を支援
コミュニティ活動	ＯＳＳコミュニティの 活性化・健全化への貢献
OSSサポート事業	サポートサービス提供で 安心なＯＳＳ環境 をお客様に提供 先進ＯＳＳ技術のＳＩ適用加速
Linux事業	安全・安心な Linux環境とサポートサービス の提供 DX、ICTモダナイゼーションを支える

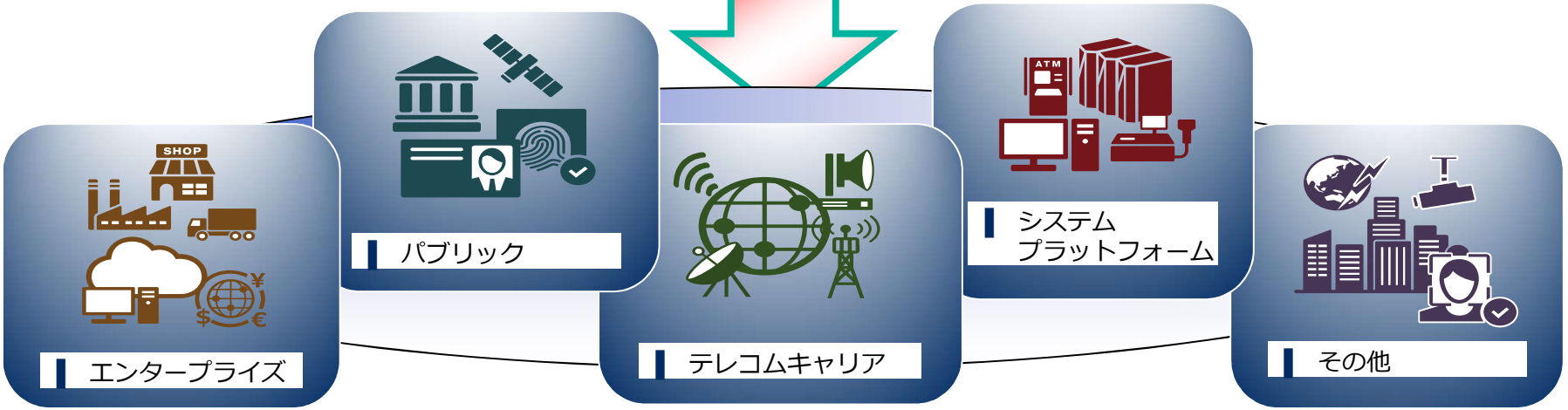
1. 一般的なOSSのリスクとは

多様な製品・サービスで活用されるOSS

- 多くのメリットがあり、多様な事業セグメントでOSSの活用が拡大
- 今や利用しないことが競争力欠如につながる状況



NECもすべての事業セグメントで活用



OSSにおけるリスクとは

広がるOSS利用と課題

- 利用が広がる一方で、課題も顕在化。
  対応しきれていないケースが多数存在。
  - ✓ OSS利用に精通した人材不足
  - ✓ 現場判断で不用意に利用され、把握・管理不足

主に問題となりうる要素

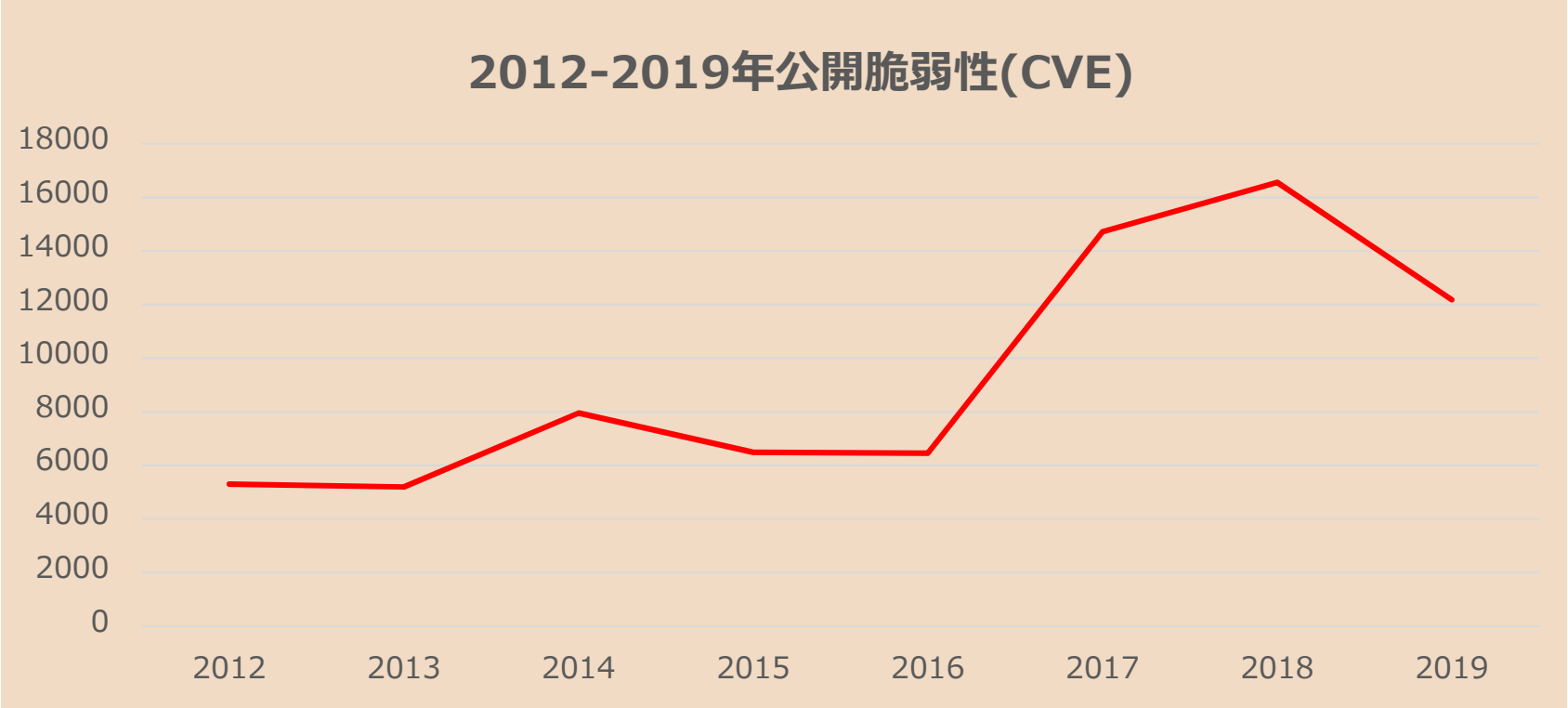
① OSSライセンス違反
GPLなどOSSライセンスに違反した状態で利用。
（著作権侵害＝コンプライアンス問題）

② セキュリティ脆弱性
脆弱性の存在、新規発覚を把握できず、対策遅れ。
（情報セキュリティ事故、情報漏洩）

③ メンテナンス不備
開発が終了したバージョンや活発でないOSSを採用。
（バグ放置、障害の原因）

CVEレコードの推移

CVE (Common Vulnerabilities and Exposures)：共通脆弱性識別子



※統計情報 CVE Details　https://www.cvedetails.com/browse-by-date.php

JVN iPediaの登録状況推移

1-1. 脆弱性対策情報の登録状況

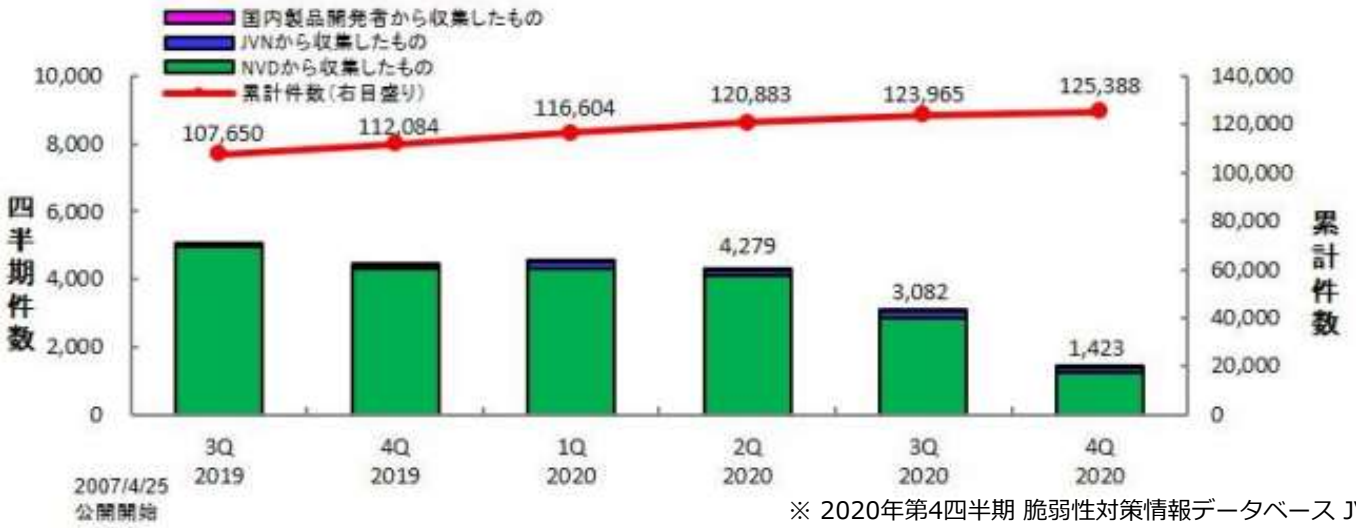
～脆弱性対策情報の登録件数の累計は 125,388 件～

2020 年第 4 四半期（2020 年 10 月 1 日から 12 月 31 日まで）に JVN iPedia 日本語版へ登録した脆弱性対策情報は右表の通りとなり、2007 年 4 月 25 日に JVN iPedia の公開を開始してから本四半期までの、**脆弱性対策情報の登録件数の累計は 125,388 件になりました**（表 1-1、図 1-1）。

また、JVN iPedia 英語版へ登録した脆弱性対策情報は右表の通り、累計で 2,217 件になりました。

表 1-1. 2020 年第 4 四半期の登録件数

	情報の収集元	登録件数	累計件数
日本語版	国内製品開発者	3 件	246 件
	JVN	179 件	9,705 件
	NVD	1,241 件	115,437 件
	計	1,423 件	125,388 件
英語版	国内製品開発者	3 件	244 件
	JVN	26 件	1,973 件
	計	29 件	2,217 件



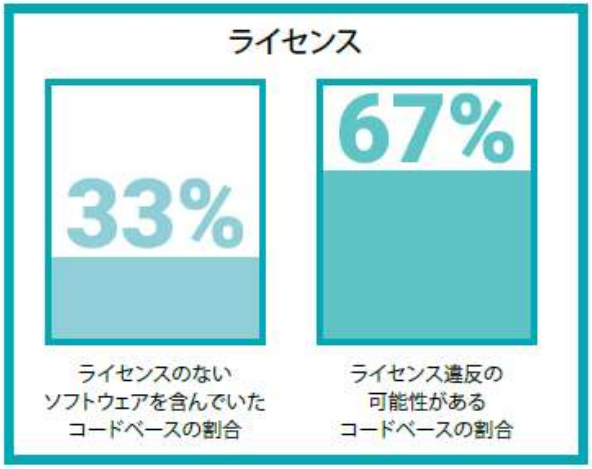
※ 2020年第4四半期 脆弱性対策情報データベース JVN iPediaの登録状況
https://www.ipa.go.jp/security/vuln/report/JVNiPedia2020q4.html

2019年実績：OSSライセンス、脆弱性の状況

2019年
監査データ分析

99%
監査したコードベースにOSSコンポーネントが含まれている

70%
監査したコードベース全体のオープンソースが占めていた割合



出典： 2020 Open Source Security and Risk Analysis (OSSRA) Report（2020年5月公開）
https://www.synopsys.com/software-integrity/resources/analyst-reports/2020-open-source-security-risk-analysis.html

OSSコンプライアンスへの関心の高まり

Linux Foundation
https://www.linuxfoundation.jp/resources/open-source-guides/

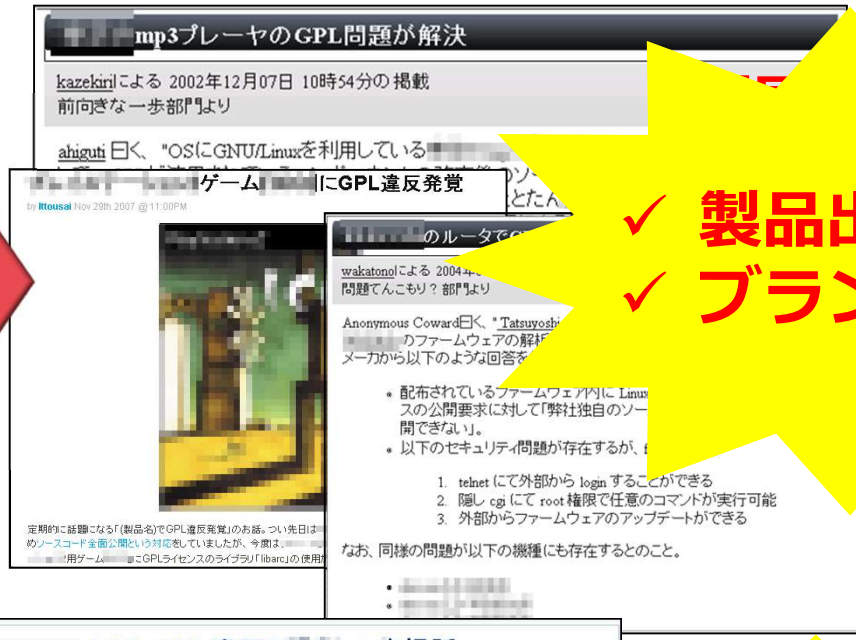
OpenChain
https://www.openchainproject.org/ja/

OSSライセンス違反(疑い)事例

①掲示板等で指摘

携帯音楽プレーヤー
ルータ
ゲームソフト
…

出展：Srad.jp
Engadget 日本版 より抜粋



②GPL違反訴訟

無線ルータ
無線ルータ
HDテレビ、ルータ等
…

出展：ITmedia エンタープライズ
OSDN magazine
Software Freedom Conservancy より抜粋

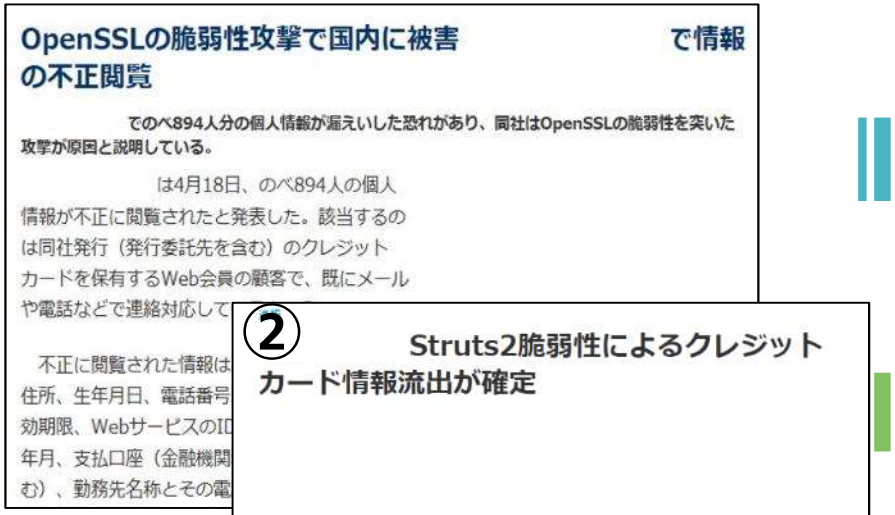
損害

- ✓ 製品出荷停止
- ✓ ブランド低下
- ✓ 賠償・訴訟費用
  (W社例：14万ドル)
- ✓ 販売停止
- ✓ 自社コード開示
- ✓ ブランド低下

OSS脆弱性に起因する情報漏洩事例

① 2014/04　M社：OpenSSLの脆弱性を突かれ不正アクセス
② 2017/03　G社等：Apache Strutsの脆弱性を突かれ不正アクセス

①


OpenSSLの脆弱性攻撃で国内に被害　で情報の不正閲覧

でのべ894人分の個人情報が漏えいした恐れがあり、同社はOpenSSLの脆弱性を突いた攻撃が原因と説明している。

は4月18日、のべ894人の個人情報が不正に閲覧されたと発表した。該当するのは同社発行（発行委託先を含む）のクレジットカードを保有するWeb会員の顧客で、既にメールや電話などで連絡対応して

不正に閲覧された情報は
住所、生年月日、電話番号
効期限、WebサービスのID
年月、支払口座（金融機関
む）、勤務先名称とその電

②

Struts2脆弱性によるクレジットカード情報流出が確定

は2017年4月5日、3月10日にApache Struts2の脆弱性を悪用され「情報漏洩の可能性がある」（　のWebページ）としていた個人情報について、「不正に取得されたことが判明した」（同社）と続報を公開した。

いずれも脆弱性対応の
遅れ・漏れが原因

日本で初「Heartbleed」の悪用
顧客情報の漏えい

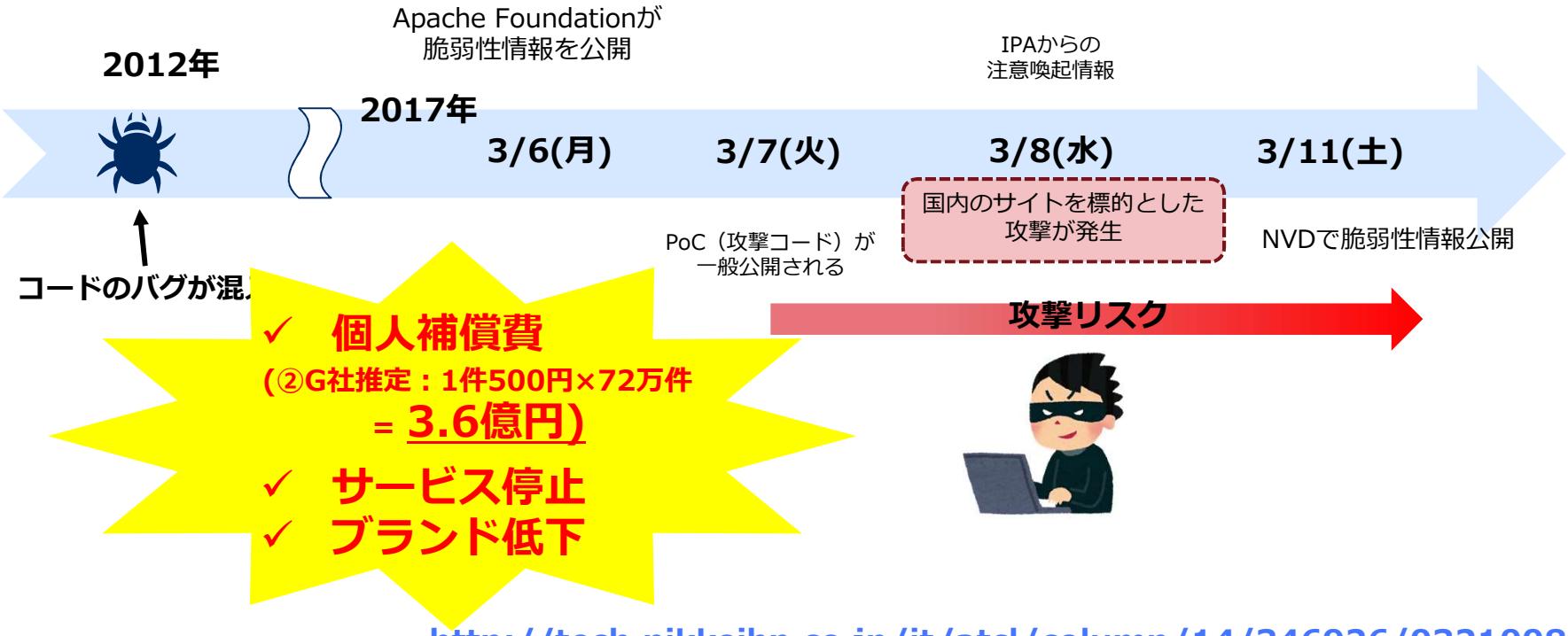
都税クレジットカードお支払サイト、
住宅金融支援機構、
日本貿易振興機構（JETRO）、
日本郵便、ニッポン放送など、
脆弱性発覚後10日程度で
7組織、計約72万件以上
の個人情報が流出

出展：Itmediaエンタープライズ
　　日経Itpro　より抜粋

Apache Sturuts2の実例でみるタイムライン

2017年3月に公開されたApache Struts2の脆弱性（CVE-2017-5638）

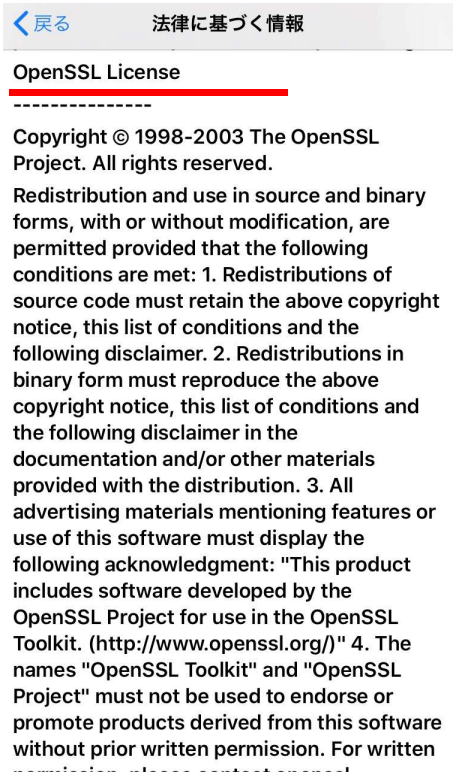
- 都税クレジットカードお支払サイト,住宅金融支援機構（GMOペイメントゲートウェイ運営）,日本貿易振興機構（JETRO）, 日本郵便, ニッポン放送など3/17までに7組織、計約72万件の個人情報が流出。



http://tech.nikkeibp.co.jp/it/atcl/column/14/346926/032100893/

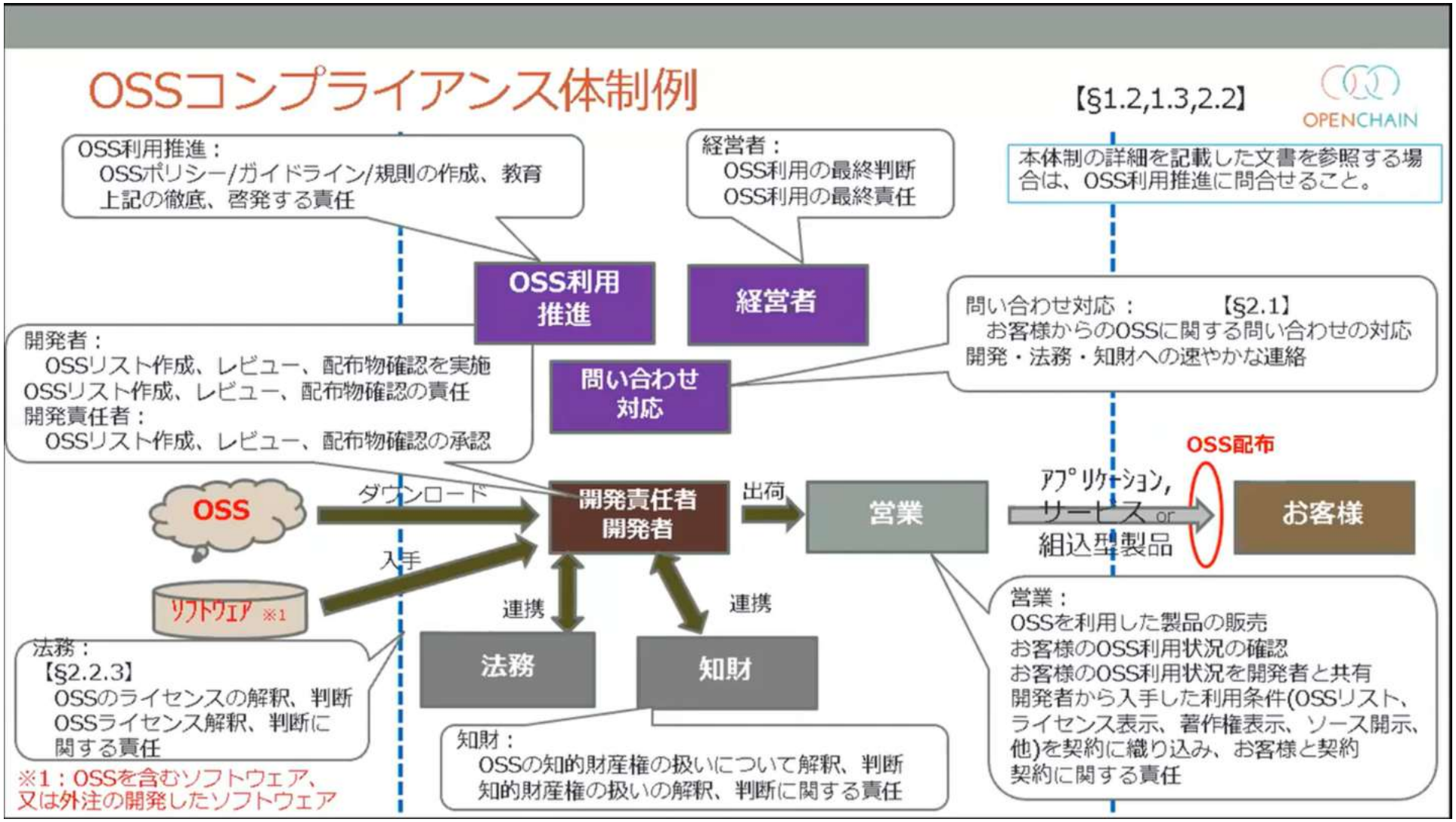
(参考)iPhoneでOSSライセンスを確認してみる

お使いのiPhoneからも、OSSに関する情報を確認できます。
「設定」→「一般」→
「法律に基づく情報および認証」→「法律に基づく情報」



2. NEC社内で実施しているOSS管理体制について

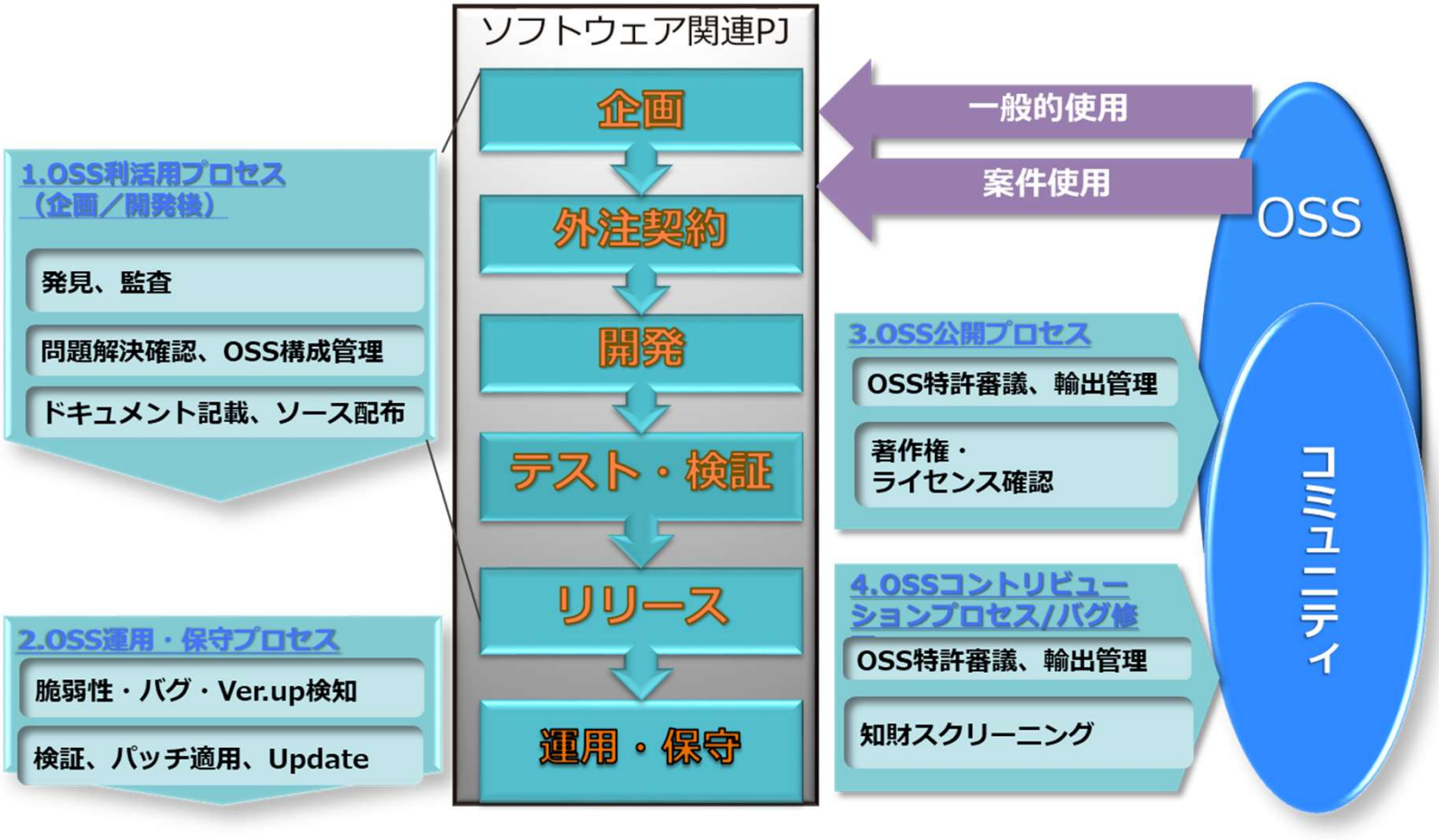
OpenChainのベストプラクティスを紹介



OpenChainJWG 2020年12月会合発表資料 EducationWGの教育資料(コンプライアンスプログラム・バージョン)より引用

【NEC社内のOSSプログラム】①OSS利活用プロセス

OSS利活用プロセスはプロジェクトがソフトウェア開発でOSSを利用する際に、開発の各工程において、またOSSの公開やコミュニティへ貢献する際の実施すべきタスクを4種類のプロセスで定めたものです。



【NEC社内のOSSプログラム】②推奨OSS・ハイリスクOSS

推奨・要確認・ハイリスクOSS

推奨OSS　　：プロジェクトで複数件の活用実績がある、
有識者が活用のリスクの少ないと判断したOSS（ホワイトリスト）

ハイリスクOSS：公式に発表されているEoLを迎えている、あるいは脆弱性が
著しく多いOSSなど、NECグループでの利用を見合わせるべき
OSS（ブラックリスト）

要確認OSS　　：推奨OSS、ハイリスクOSS以外のOSS（リストはない）

OSS選定時のルール

①可能な限り推奨OSSから選択する。
②ハイリスクOSSの新規採用は禁止。
③OSSを利用する際にリスクを十分に判断できない場合は必ず「OSS利活用プロセス」に則りOSSのリスク調査を窓口に調査依頼する。

@. NECのソリューションを理解していただく

Black Duckが提供する主な機能

BLACKDUCK BY SYNOPSYS®

1. **OSSスキャン&リスト化**
   膨大なKBを基OSSコンポーネントを認識
2. **リスク情報の紐付け**
   ライセンス・セキュリティ・運用のリスクを可視化
3. **対応・修正状況の管理**
   ポリシーを管理し、違反への早期対応が可能
4. **モニタ・アラート機能**
   最新の脆弱性をウォッチし、アラートを発信！

顧客課題を解決する要素とNECの強み

ツール機能

- **OSSスキャン&リスト化**
- **リスク情報の紐付け**
- **対応・修正状況の管理**
- **モニタ・アラート機能**

NEC強み

トータルソリューション提案力

- HW・OS・AP一気通貫サポートのトータルソリューション

シェア国内トップクラス

活用ノウハウ

- 自社でのBlack Duck活用実績(10年以上)
- 高品質のサポート＋導入支援、解析支援

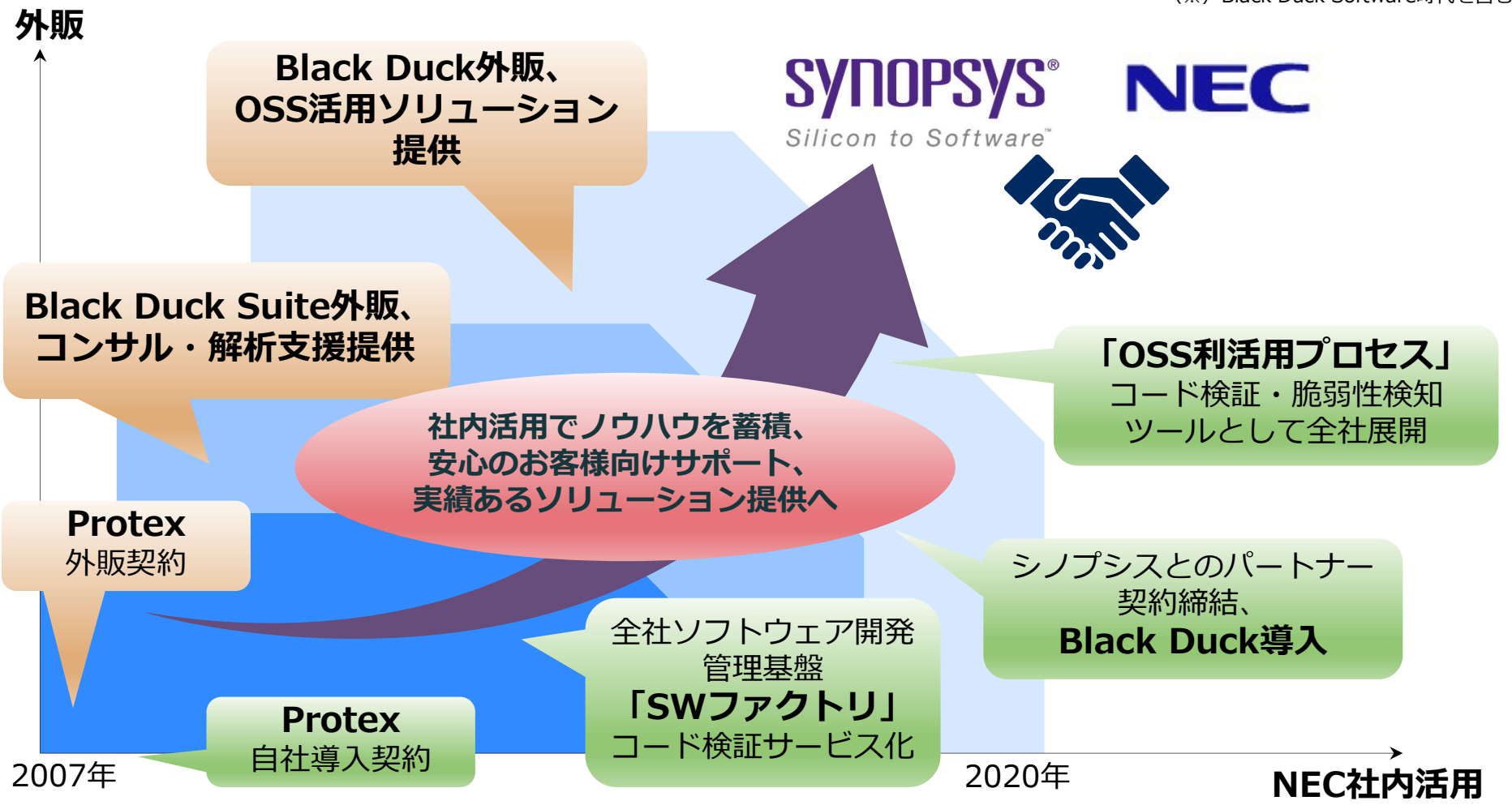
OSSライセンスコンサル

- ネットに散在する都市伝説に惑わされないOSSライセンスの正しい理解、正しい判断ができる組織育成を支援。

NECとシノプシスのパートナーシップ

- NEC社内活用と外販の両輪で10年以上に渡る協業(※)
- DXを支えるOSS活用ソリューションの提供で引き続き連携

（※）Black Duck Software時代を含む



お問い合わせ

NEC　OSS推進センター

- Black Duck担当
  - E-Mail　：　blackduck-info@osspf.jp.nec.com


Orchestrating a brighter world
NEC