第23回情報セキュリティ・シンポジウム
オープン・ソース・ソフトウェアのセキュリティ

OSSの世界観とセキュリティ

2023年3月3日（14:05-14:45）

JPCERTコーディネーションセンター
真鍋 敬士

はじめまして

https://www.jpcert.or.jp/recruit/

- 1998年　財団法人日本情報処理開発協会（現 日本情報経済社会推進協会）の研究員としてJPCERT/CCの業務に従事
- 2000年　JPCERT/CC運営委員（2002年から理事）
- 2016年　金融ISAC理事

- 1991年頃～
  - 配属された研究室でUNIXワークステーションの管理作業を担当させられる（ほとんどはフリーソフトウェアのインストール作業）
  - 浮動小数点コプロセッサを搭載していないPCで動作する386BSDを探していてLinuxを見つける
  - Linuxコンソールで日本語を表示するプログラムを開発してユーザーやプログラマに配布
  - フリーソフトウェアのLinuxへの移植作業等に携わっていた面々を中心とした連絡をしていく中で国内向けのLinuxのメーリングリスト（ML）を立ち上げ
  - Linuxディストリビューション向けの日本語拡張キットの作成と配布
- 1995年頃～
  - ダイアルアップ通信用ソフトウェアの開発と配布
  - トンネリングソフトウェアの開発と配布
- 2000年頃～
  - いくつかの民間営利企業でOSSを取り扱う業務に就く

JPCERT/CCとは

■ 一般社団法人JPCERTコーディネーションセンター

Japan Computer Emergency Response Team / Coordination Center

- コンピューターセキュリティインシデントへの対応、国内外にセンサーをおいたインターネット定点観測、ソフトウェアや情報システム・制御システム機器などの脆弱性への対応など国内の「セキュリティ向上を推進する活動」を実施
- サービス対象: 国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等のセキュリティに関わる担当者
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する**日本の窓口となる「CSIRT」**

※各国に同様の窓口CSIRTが存在する（米国のCISA（US-CERT）、CERT/CC、中国のCNCERT/CC、韓国のKrCERT/CC等）

- 経済産業省からの委託事業としてサイバー攻撃等国際連携対応調整事業を実施
- サイバーセキュリティ基本法上の「サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関」
- サイバーセキュリティ協議会（2019年発足）の事務局をNISCとともに実施
（事案対応の相談や情報共有活用の運用面を担当）

お品書き

一般教養としてのOSS

背景にある考え方

現実社会における悩み

OSS（オープン・ソース・ソフトウェア）とは

- OSI（Open Source Initiative）による定義（1998年～）

	公式（https://opensource.org/definition/）	日本語訳（https://opensource.jp/osd/osd19/）
1	Free Redistribution	再頒布の自由
2	Source Code	ソースコード
3	Derived Works	派生ソフトウェア
4	Integrity of The Author’s Source Code	作者のソースコードの完全性（integrity）
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（fields of endeavor）に対する差別の禁止
7	Distribution of License	ライセンスの分配（distribution）
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

- OSIによる定義のルーツはDebian社会契約（https://www.debian.org/social_contract）

OSSに対する姿勢（日本）

- 特許庁（2019年）
  - デジタル化、IoT 化時代におけるオープンソースソフトウェアに係る知財リスク等に関する調査研究報告書
    https://www.jpo.go.jp/resources/report/takoku/document/zaisanken_kouhyou/2019_06_1.pdf
  - Opensource for ALL
    https://www.jpo.go.jp/resources/report/takoku/document/zaisanken_kouhyou/2019_06_2.pdf
- 経済産業省（2022年）
  - オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を拡充しました
    https://www.meti.go.jp/press/2022/05/20220510001/20220510001.html
  - OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集
    https://www.meti.go.jp/press/2022/05/20220510001/20220510001-1-2.pdf

OSSに対する姿勢（米国）

- America’s Home for Open Source Projects from the Federal Government
  - https://code.gov/
- U.S. Department of Commerce
  - https://www.commerce.gov/about/policies/source-code

【余談】2016年の“Federal Source Code Policy”が根拠

■ 発表当時のURL（リンク切れ）

https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

■ アーカイブサイトのURL

https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

■ ホワイトハウスサイト内のURL

https://www.whitehouse.gov/**wp-content**/uploads/legacy_**drupal**_files/omb/memoranda/2016/m_16_21.pdf

https://wordpress.org/　https://www.drupal.org/

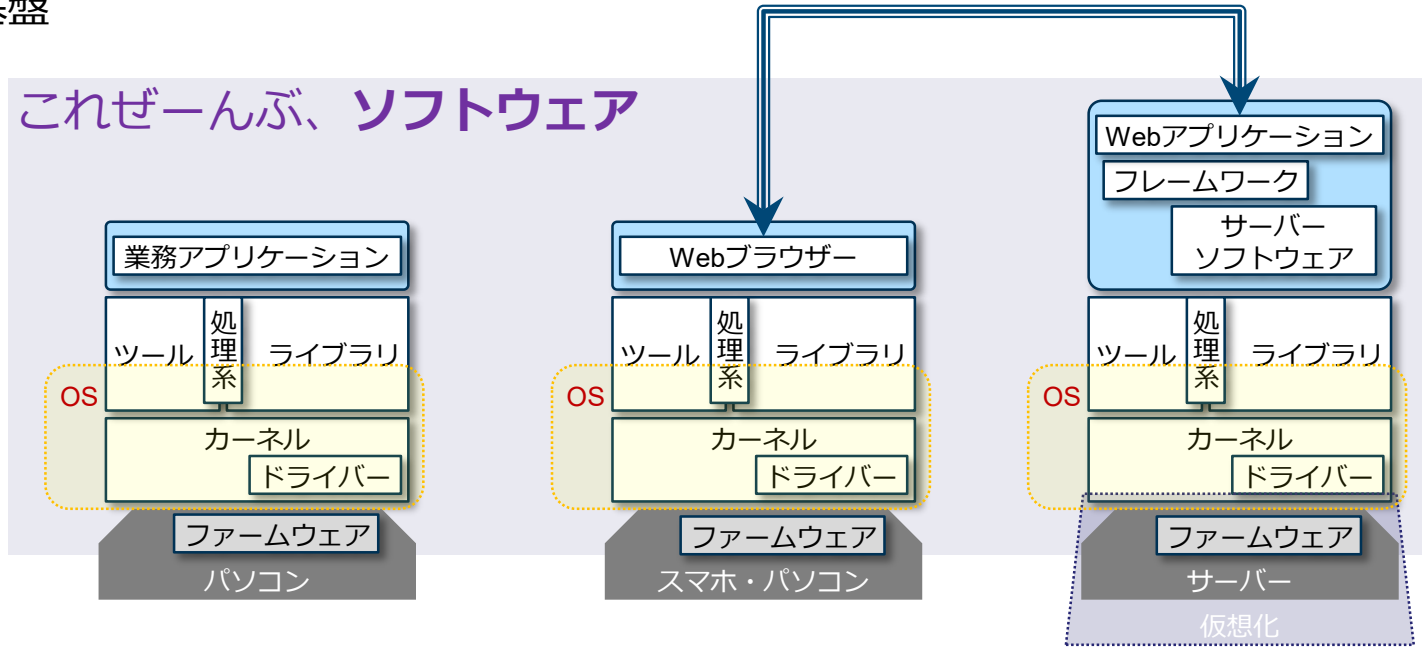
オープンソースのコンテンツマネージメントシステム

OSS活用に関する実態調査

- シノプシス社「オープンソース・セキュリティ&リスク分析レポート」
  https://www.synopsys.com/ja-jp/japan/press-releases/2022-05-19.html
  - 調査は毎年行われており、レポートでは経年変化にも触れられている
  - 2,400を超す商用ならびに内製のコードベースを調査
    - コードベースの**97%**にOSSが含まれていた
    - 全コードベースに占めるOSSコードの割合は**78%**
    - コードベースの**30%**にライセンスがないまたはカスタム・ライセンスを使用したOSSが含まれていた
  - 2,097のコードベースに対してセキュリティ・リスク診断
    - コードベースの**85%**に過去4年間以上開発活動実績のなかったOSSが含まれていた
    - **88%**は、最新バージョンではないOSSコンポーネントを使用していた
    - コードベースの**48%**から1つ以上の高リスクな脆弱性が検出された
    - **81%**のコードベースからは1つ以上の既知のOSS脆弱性が検出された
  - レポートではOSSプロジェクトにおける開発者の人数にも言及

ソフトウェア超雑概説

- ひとことで**ソフトウェア**と言っても...
  - システムソフトウェアとアプリケーションソフトウェア
  - プログラミング言語処理系（開発環境と実行環境）
  - 仮想化基盤
  - ...



お品書き

一般教養としてのOSS

背景にある考え方

現実社会における悩み

A long time ago,

この動作を
変えられないの？

これもできるように
ならないの？

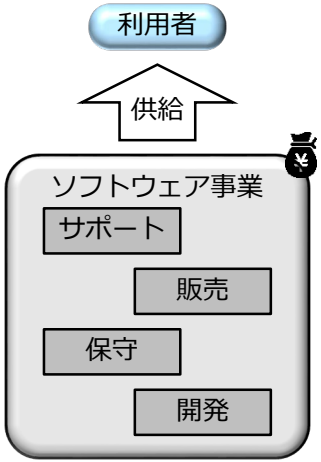
UTSL

(Use The Source, Luke)

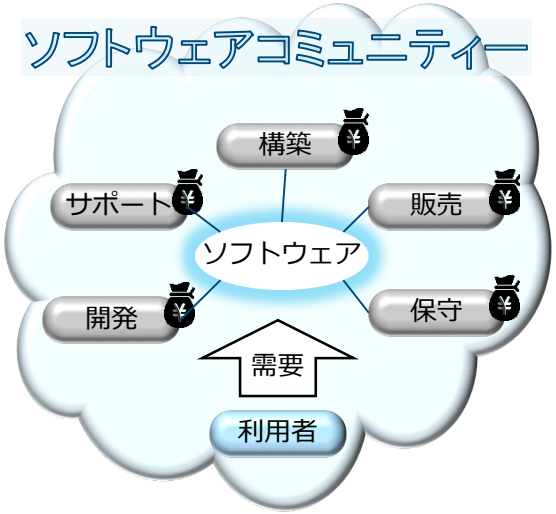
この動作は
おかしいよね？

どうやって使うの？

20世紀：資源としてのソフトウェア

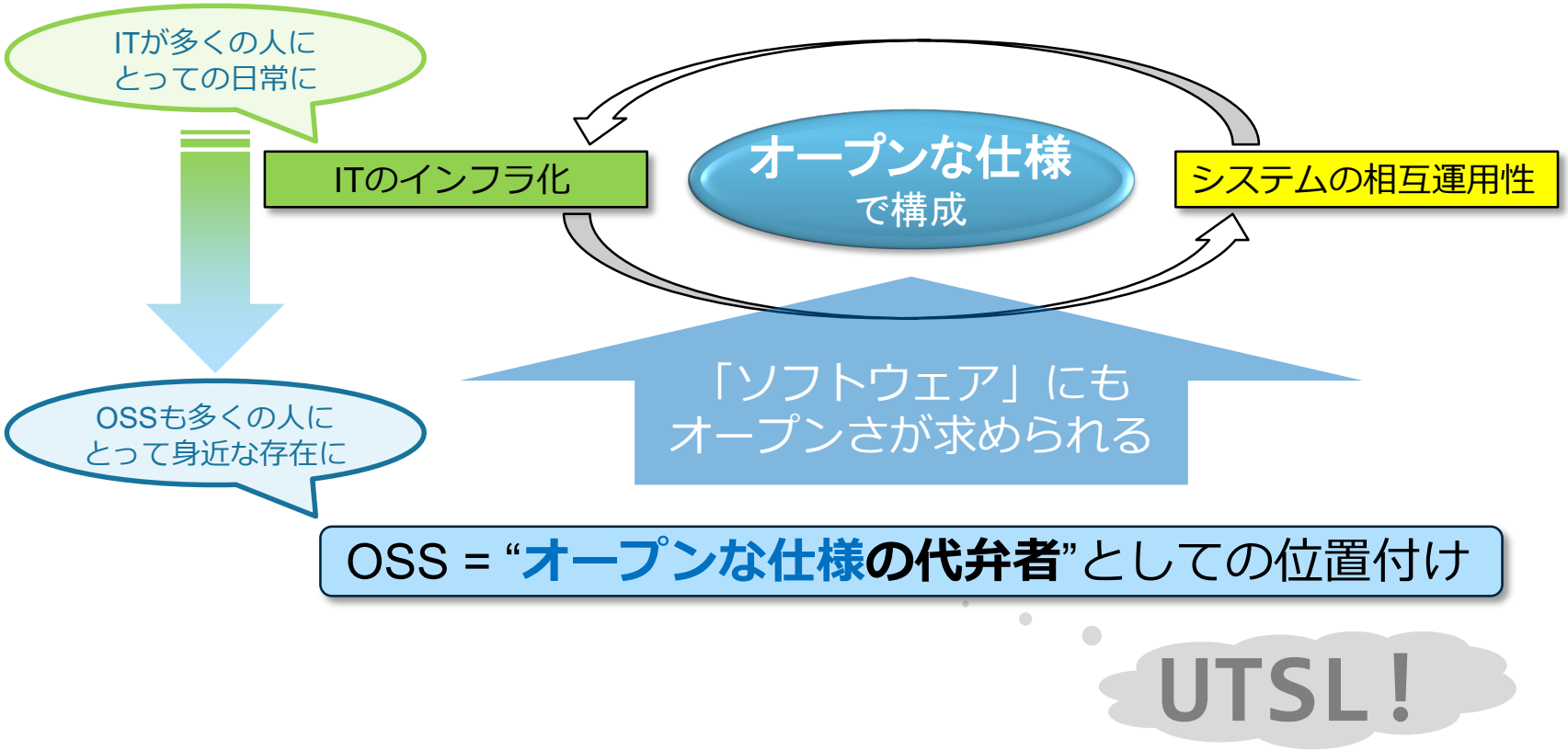


VS



認めない	財の非排除性	認める
私企業に委ねる	持続性	コミュニティーに委ねる
秘匿性で確保	安全性	透明性で確保

21世紀：担い手としてのソフトウェア



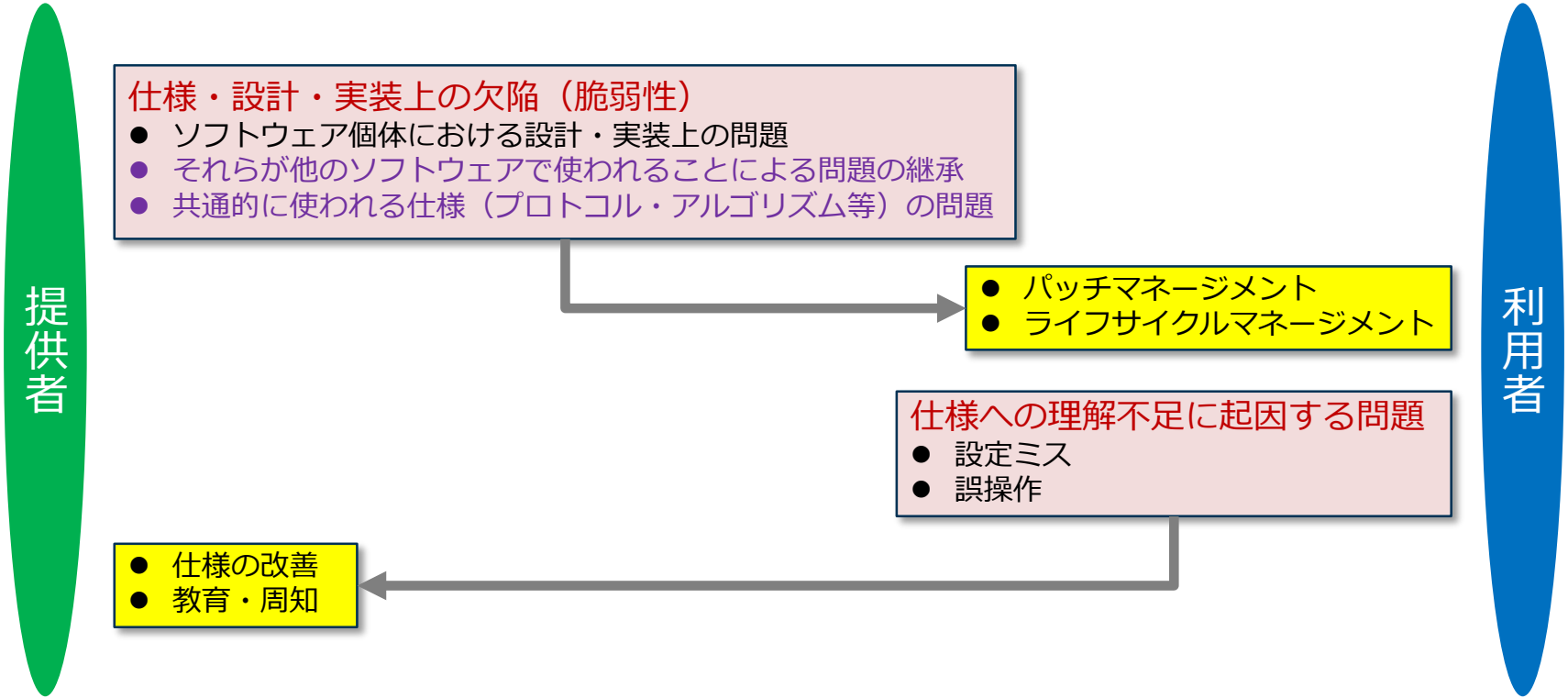
お品書き

一般教養としてのOSS

背景にある考え方

現実社会における悩み

ソフトウェアのセキュリティ

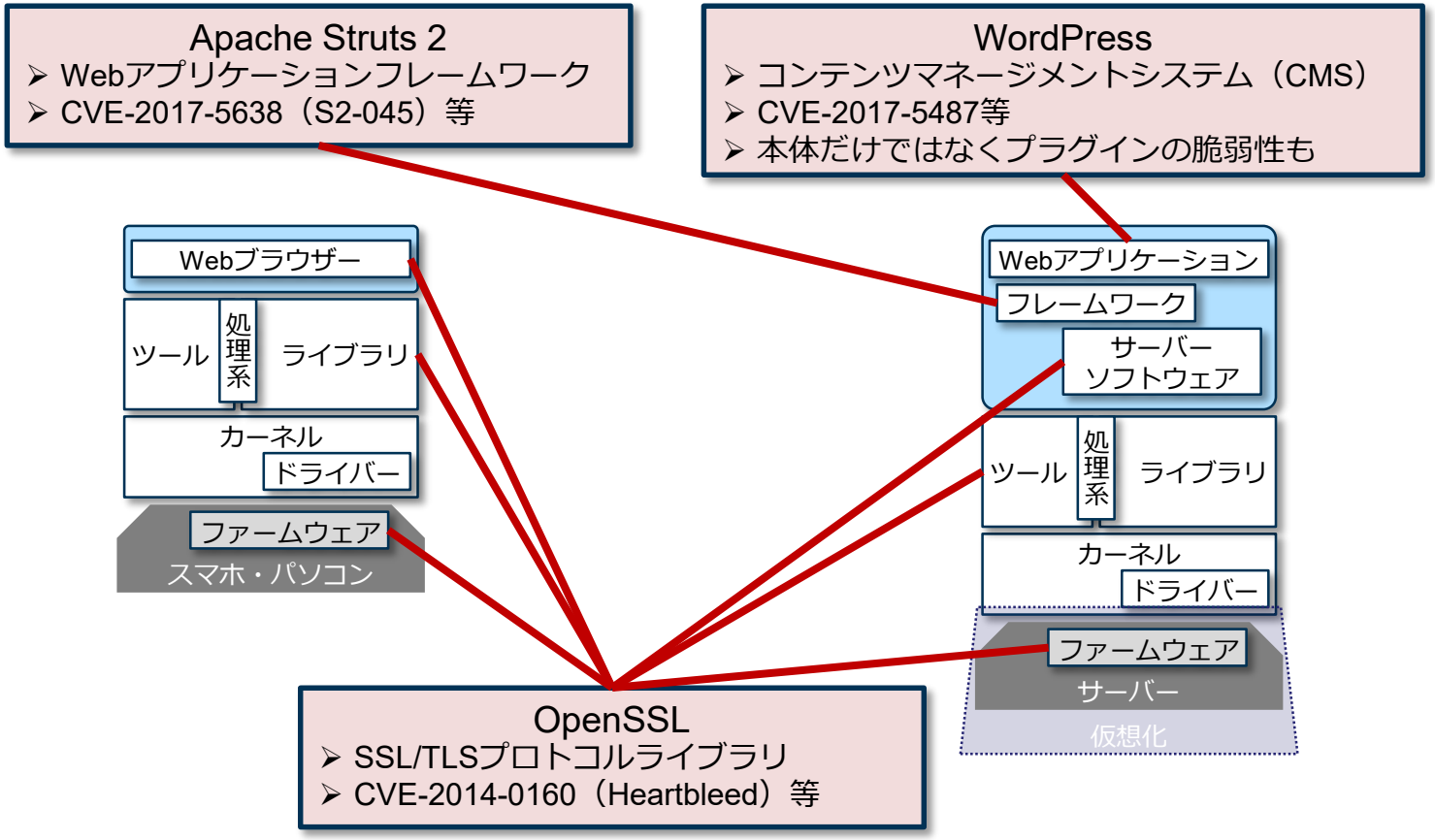


“Software Bill of Materials”

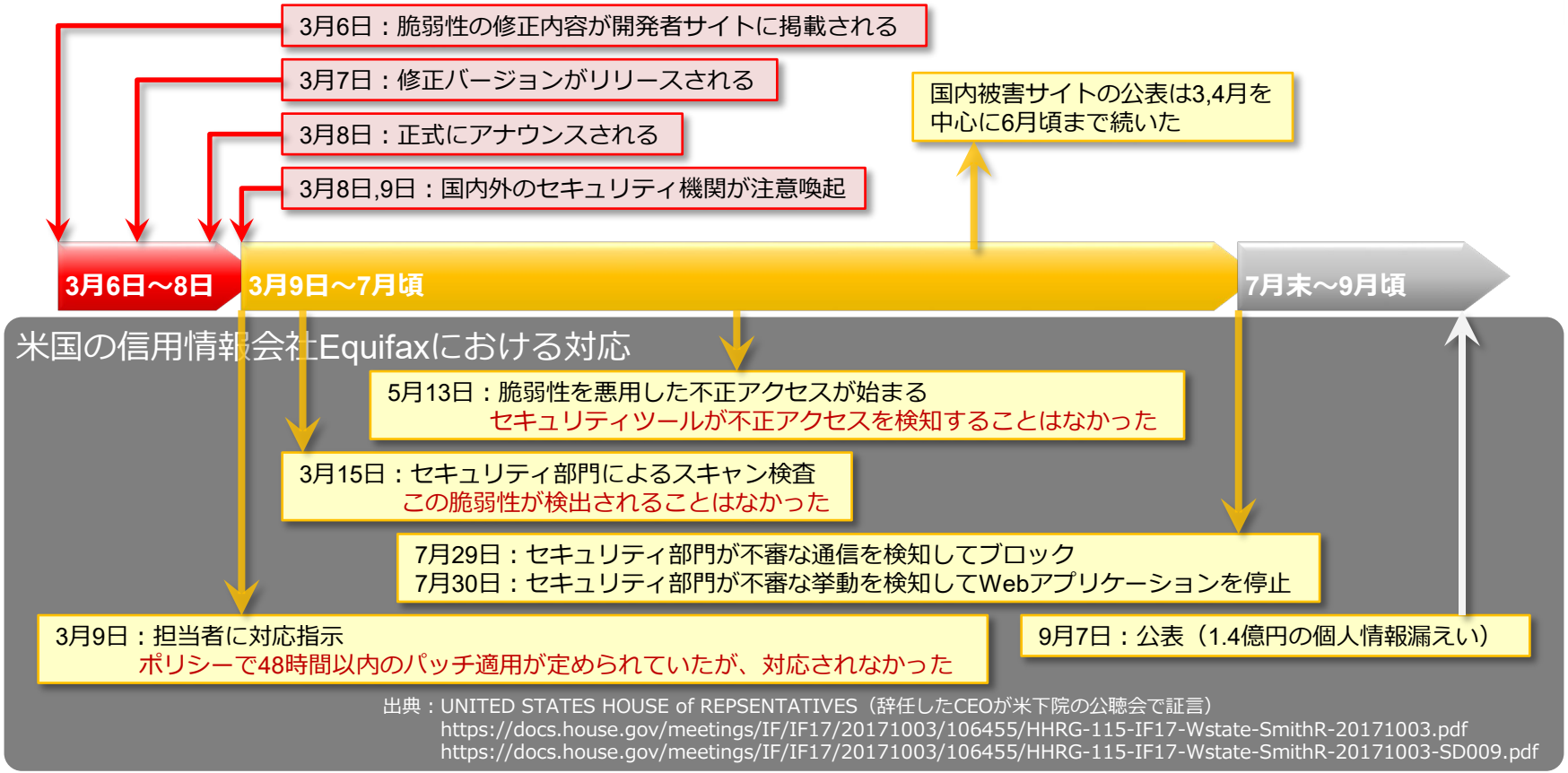
- 2018年、NTIA（米国商務省電気通信情報局）のAllan Friedman博士が発表
  NTIA「SOFTWARE BILL OF MATERIALS」
  https://www.ntia.gov/SBOM
  - 従来から提唱されていたソフトウェア構成管理の考え方
  - セキュリティ、ライセンス、資産管理といった課題
  - ソフトウェアコンポーネント透明性への取り組みとして協議

- 2021年、大統領令でソフトウェアサプライチェーンのセキュリティ確保
  The White House「Executive Order on Improving the Nation’s Cybersecurity」
  https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
  - NIST（米国国立標準技術研究所）がガイダンスを策定する
  - ガイダンスでは製品購入者へのSBOM提供について記載する
    - 2021年7月にNTIAがSBOMの最小要素を発表

影響範囲の広いOSSの脆弱性例

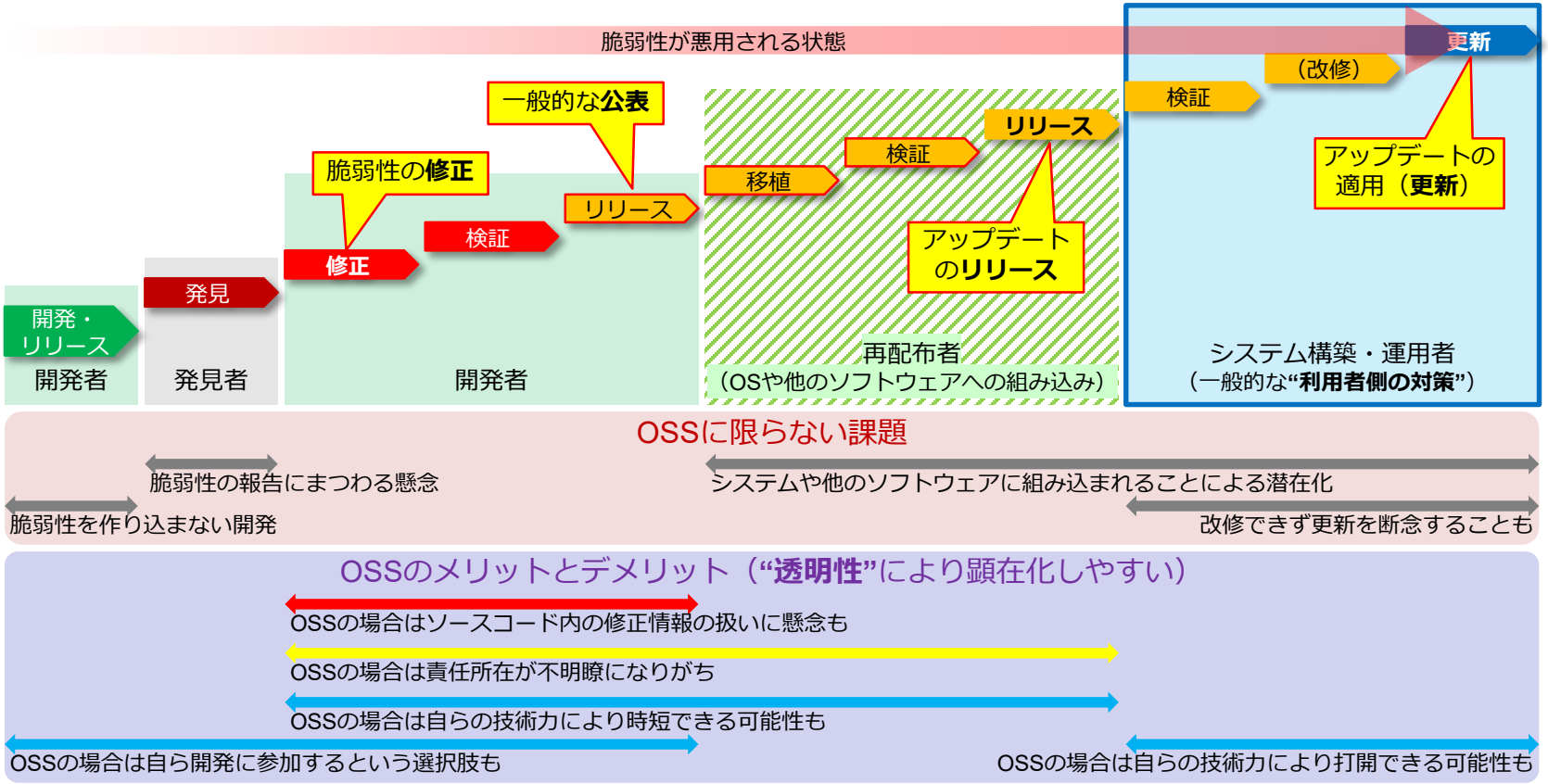


S2-045を悪用する攻撃への対応



出典：UNITED STATES HOUSE of REPSENTATIVES（辞任したCEOが米下院の公聴会で証言）
https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf
https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003-SD009.pdf

脆弱性対応には多くのステップがある



お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/reference.html

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/