資料 4

SYNOPSYS®
Silicon to Software™

OSSの脆弱性・継続性の実態とその管理

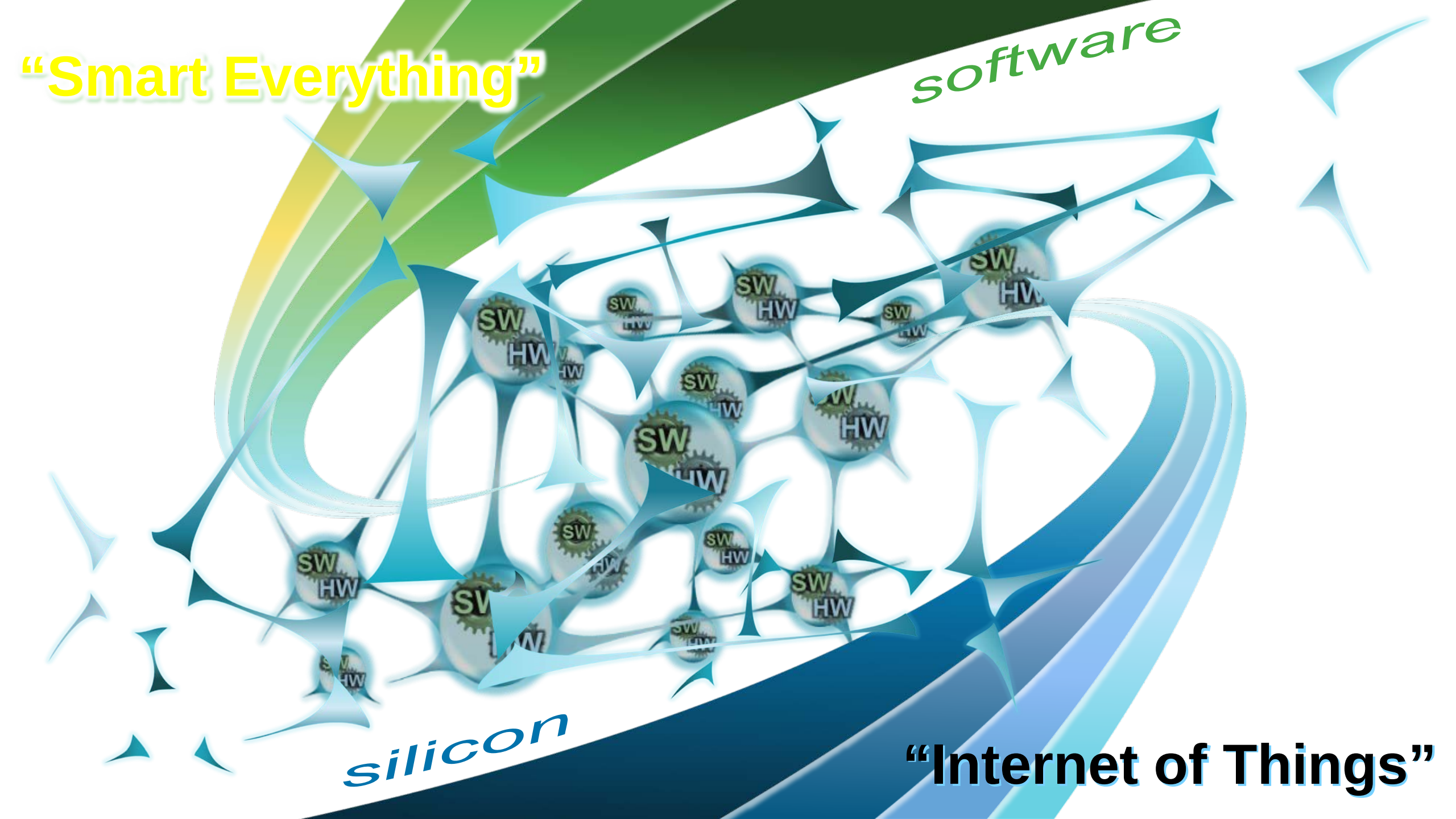
ソフトウェアのセキュア調達・セキュア開発

C-SCRM: Cyber-Supply Chain Risk Management

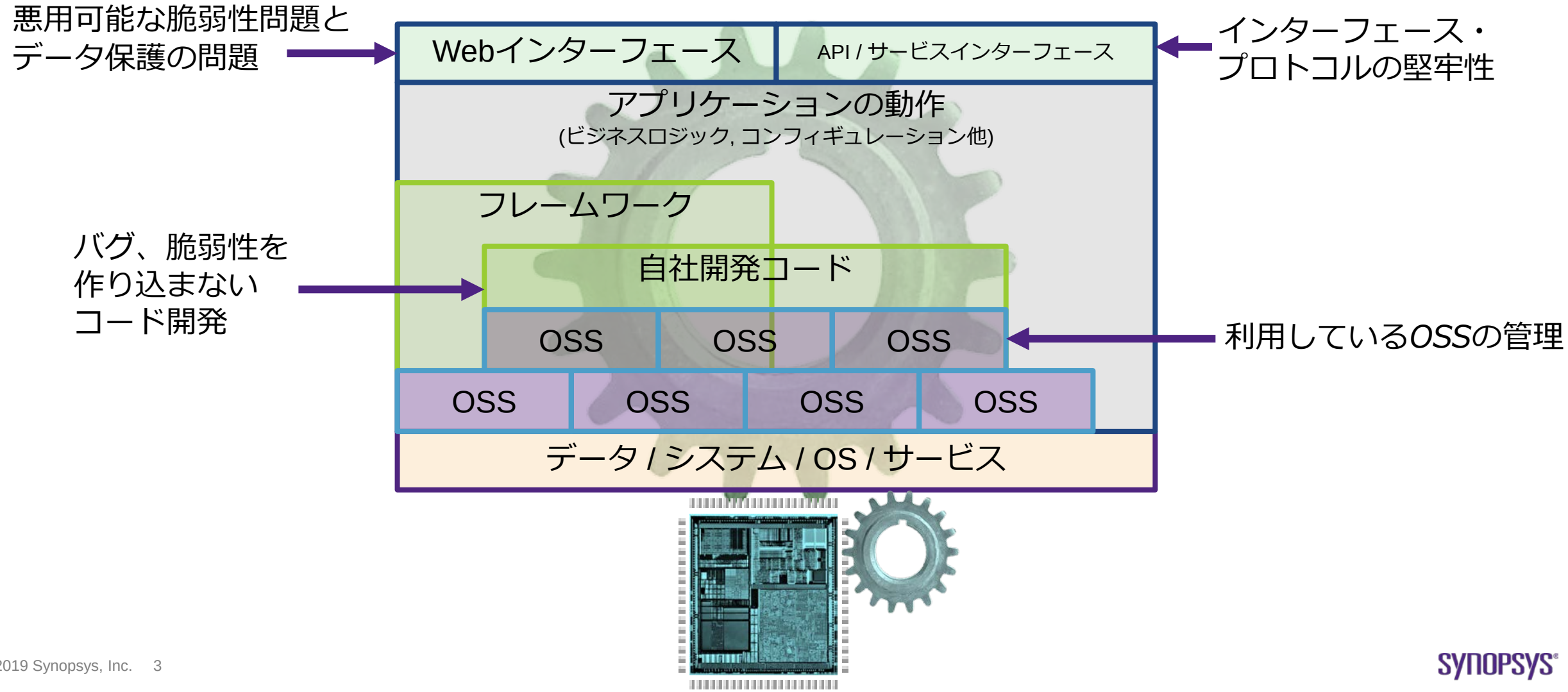
日本シノプシス合同会社
ソフトウェア・インテグリティ・グループ

明石 貴昭

2019/11/06


“Smart Everything”
software
silicon
“Internet of Things”

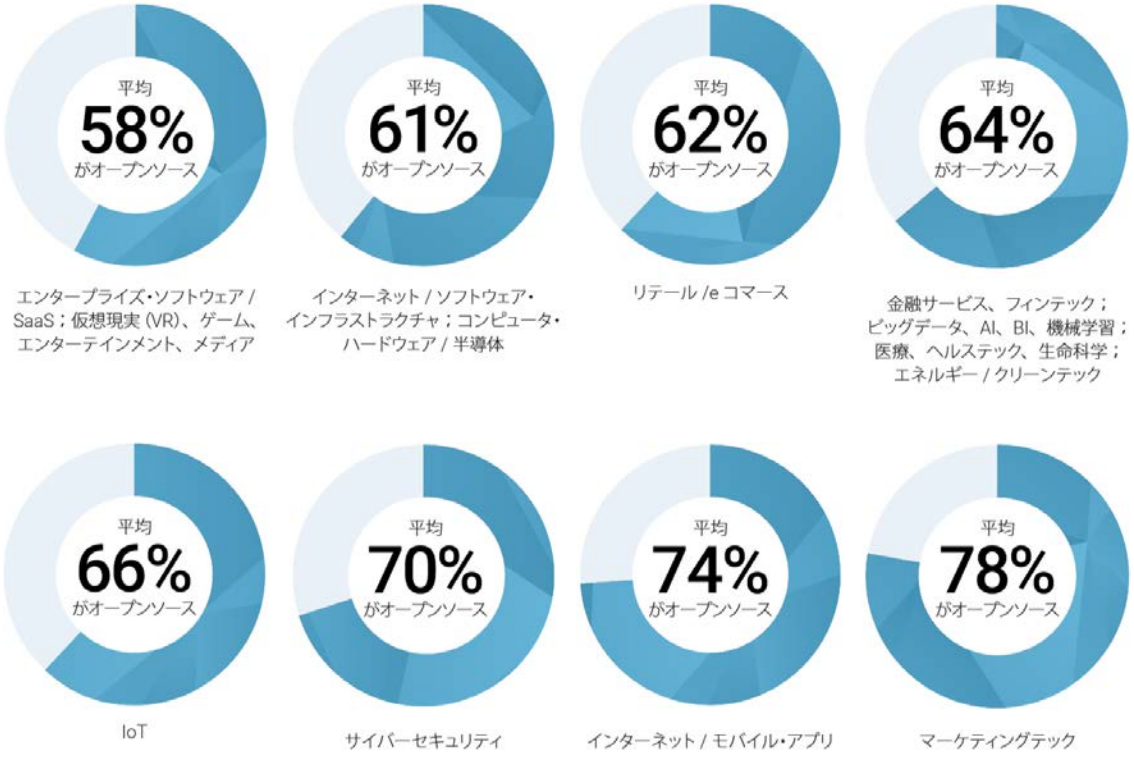
多くの脆弱性はソフトウェアに潜む



SYNOPSYS®

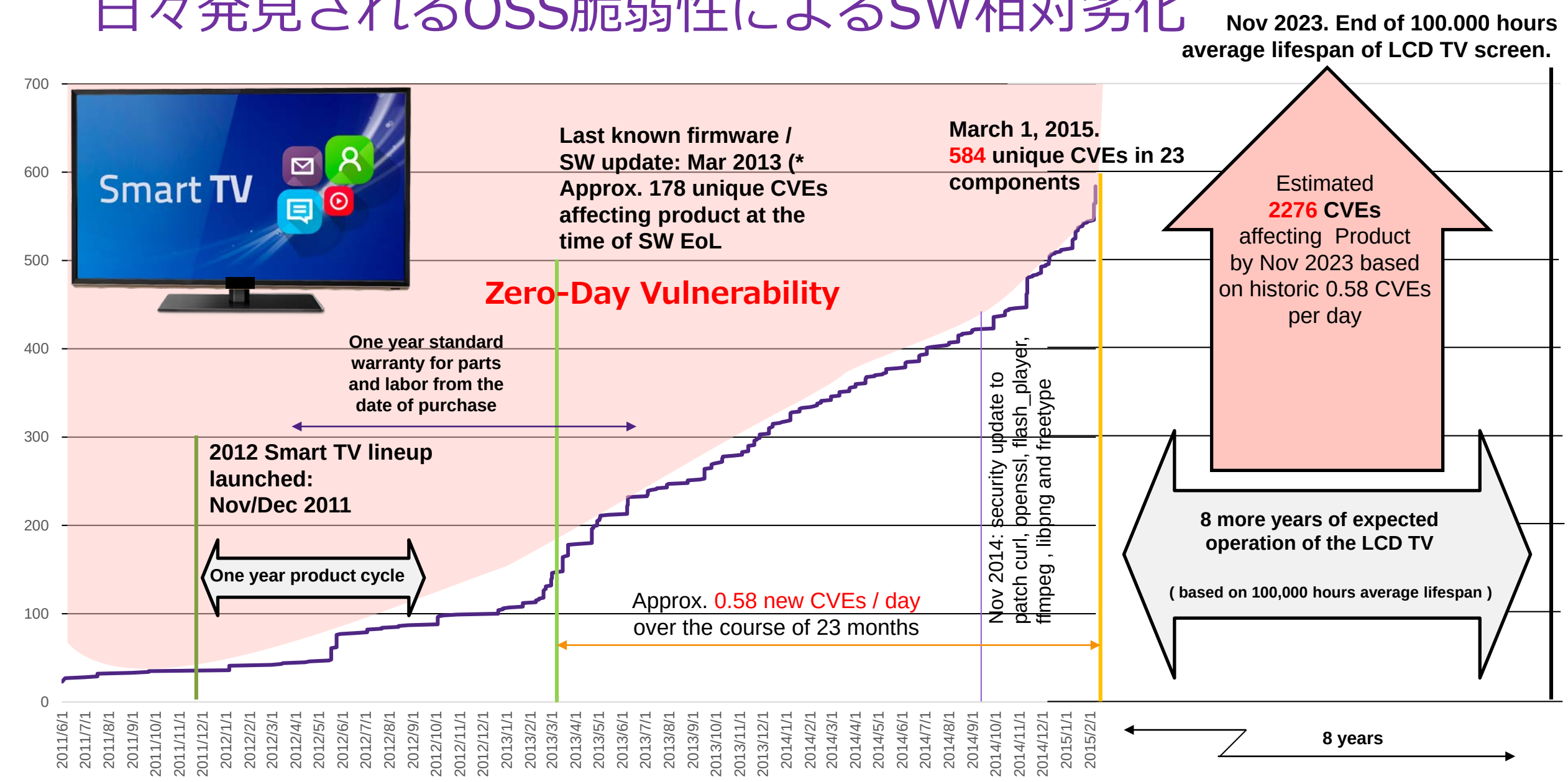
2019年オープンソース・セキュリティ＆リスク分析（OSSRA）レポート

https://www.synopsys.com/ja-jp/software-integrity/resources/reports/2019-open-source-security-risk-analysis.html



SYNOPSYS®

日々発見されるOSS脆弱性によるSW相対劣化

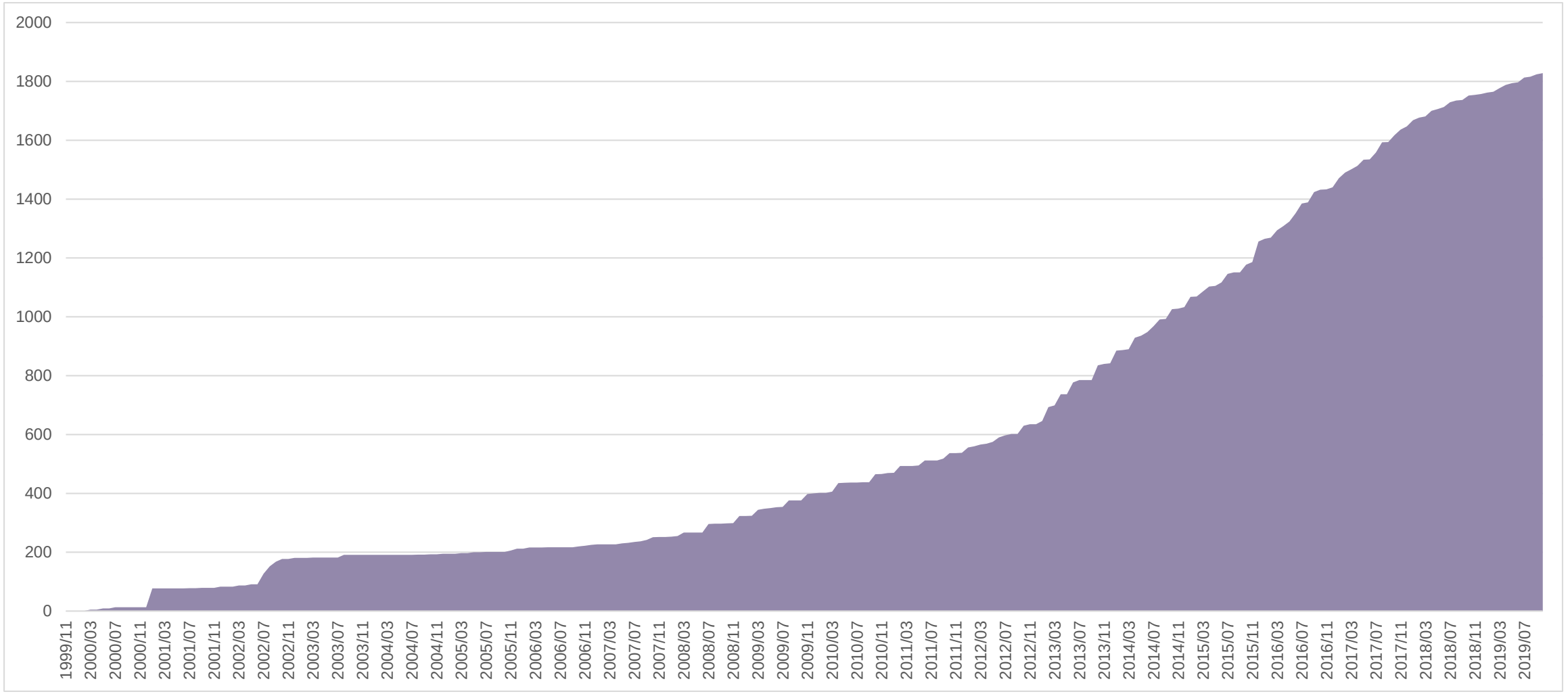


(* date may not be fully accurate, as e.g. partial OTA updates may have been delivered after this date as well (see sec. update on Nov 2014)

SYNOPSYS®

模擬 水プラント脆弱性積算数 – Applicationのみ

名工大 橋本研究室 提供データ



SYNOPSYS®

メーカーサポート終了後も1400以上の既知の脆弱性を含んだまま利用され続けている医療機器

- ICS-CERT アドバイザリ: ICSMA-16-089-01
  - CareFusion社Pyxis Supply Station薬剤管理システムの脆弱性
- ソフトウェアコンポジション解析により1418個既知の脆弱性を検出
  - Critical: 179個
  - Major: 606個
  - Minor: 97個
- 検出されたコンポーネントの一例
  - Microsoft Windows XP, Sybase SQL Anywhere 9, BMC Appsight 5.7, など

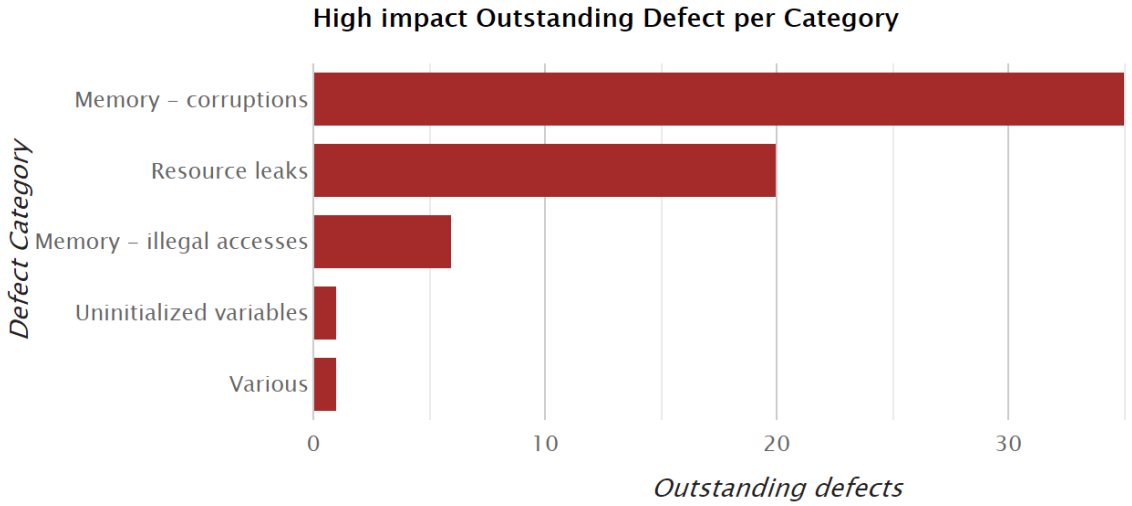
ソフトウェアで利用されるコンポーネントと既知の脆弱性の把握が重要

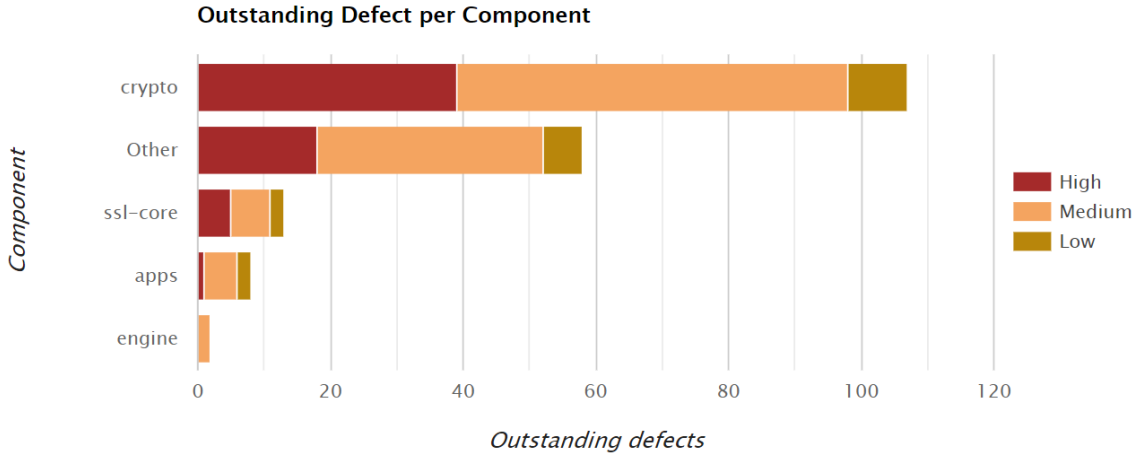
SYNOPSYS®

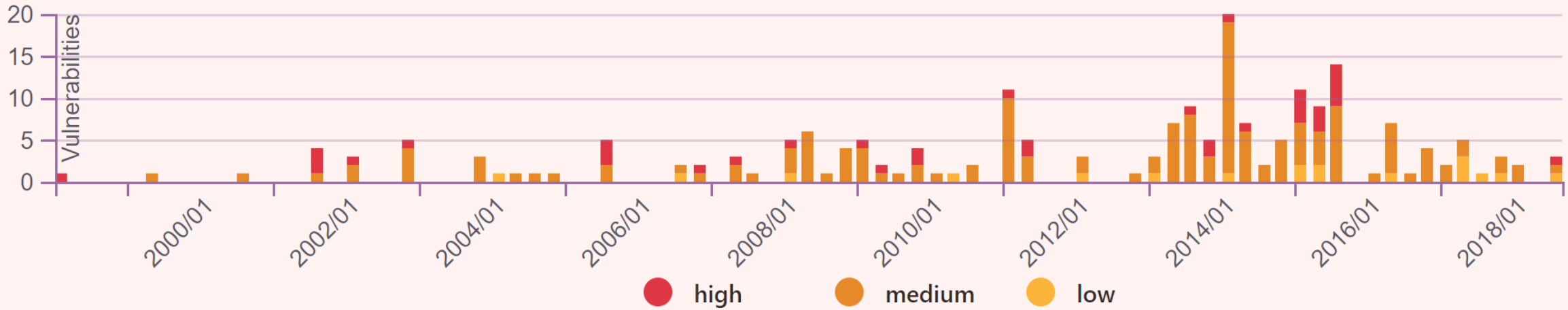
CWEとCVEの傾向: OpenSSL プロジェクトの例

https://scan.coverity.com/projects/openssl

2006以降 開発中に修正/ツール検出されたバグ、CWE (Common Weakness Enumeration) 821/1075個







リリース後に発見されたCVE (Common Vulnerability Enumeration) 183個 ※2019/9現在

ソフトウェア開発時のバグ！（CWE他）

クロスサイトスクリプト
(XSS)
SQLインジェクション

バッファ
オーバーフロー

NULLポインタの間接参照
未初期化の値の使用
解放済みリソースの使用
ゼロの除算

スレッドのデッドロック
2重ロックまたはアンロックの欠如
データ競合状態
無限ループ

リソース
リーク

実行時のエラーを引き起こす！

安全でない
データハンドリング

メモリ
不正アクセス

メモリ破損

プログラムの
クラッシュ

プログラムの
ハングアップ

不正アクセス

任意コードの実行

サービス拒否

リリース/運用後に発見されると**「脆弱性」**

（CVEとして登録され既知の脆弱性として知れ渡り攻撃コードが作られるとハッカーの攻撃対象となる）

SYNOPSYS®

OSSや3rd Party SWを使用する場合のリスク

ライセンス汚染

- 意図せずコピーレフトOSS等の混入が発生していないか

日々発見されていく脆弱性

- 早期発見、対策の必要性

OSS開発プロジェクトの活動状況

- 採用以降、パッチ提供が滞らない、活発なOSSプロジェクトであるか

システム, ソフトウェアの調達時テストゲートの必要性

日々増加する脆弱性に対して、動的管理できる*SBoM*が望ましい

供給側でSBoM提供

又は

調達側で、SW構造解析ツール
による自主確認

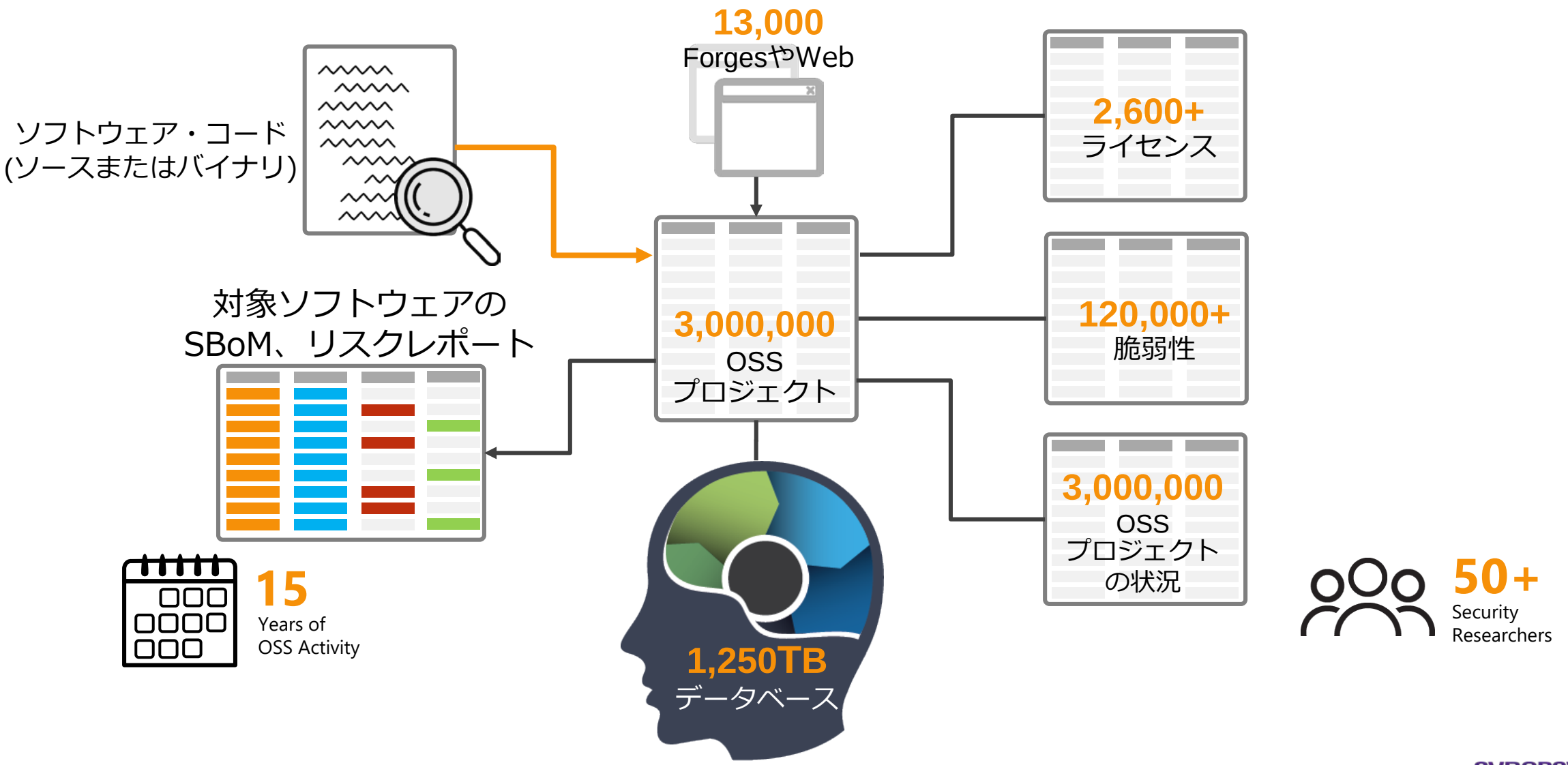
共通の確認基盤
がある事が望ましい

- **社内運用機器(内包されるSW)調達**
  - 完成品(パッケージ等)の購入
  - 外部開発委託品
    - ソースコード納品
    - バイナリ納品
  - オープンソース・ソフトウェア利用
    - LinuxやWebサーバー等

- **商品化されるソフトウェア、サービス**
  - 部品として完成品(パッケージ等)の購入、OEM等
  - 外部開発委託
    - ソースコード納品
    - バイナリ納品
  - 部品としてオープンソース・ソフトウェア利用

SYNOPSYS®

シノプシス OSS データベース



SYNOPSYS®

Cyber-Supply Chain Risk を低減するために

信頼できるSWのSBoM管理に基づく調達スキームの実現

- 調達側がSW(HWに同梱される場合含)の素性を確認の上、調達できる仕組み
- SBoMならびに元となるデータベースの真正性が重要
- 調達側の教育が必要（SW調達をBlack-boxで行ってはならない）

日々増え続ける脆弱性対策

- SBoMの動的管理による早期発見、対策
- 重要システムにおいては、メーカーへ長期脆弱性対策の義務付け、もしくは期限付きサブスクリプション・モデルでの販売を検討いただく

セキュリティ・バイ・デザインによるシフトレフト

- 機能的品質だけでなく、セキュリティの観点で堅牢なソフトウェア開発の推進
- 増大一途のSWに、人的コードレビューの限界. ツールによるSDLC初期からのセキュリティ診断の自動化.
- 根本的には、バグ FREE 開発へ向かうべき. バグ FREE＋セキュア・コーディング教育が必要.

SYNOPSYS®

サイバーアシュアランスのための調達基準

SYNOPSYS

サプライチェーンにおける
サイバー アシュアランスのための調達基準

はじめに

-ISO 27001

-NIST SP 800-53

-NIST SP 800-82

-ISA 62SA

-FIPS 140-2

-UL 2900

サプライヤーは、潜在的なセキュリティ インシデント、不正アクセスに対する製品の脆弱性、機能の喪失、マルウェアの侵入、あるいは、機密性、完全性または可用性のあらゆる侵害に対応するために設計されたセキュリティスタンダードおよびプロセスをすでに策定済みであり、機器および製品の開発期間すべてを通じて、当該スタンダードおよびプロセスを履行することを表明し保証すること。

Verizon社では、装置を提供するベンダに対し、Defensicsで各プロトコルのファズテストを実施することを義務付けています。

2.1.4 Security

M-14 — The vendor shall perform protocol robustness testing using ***Synopsys (ex-Codenomicon) Defensics*** or a Verizon-approved equivalent solution for all active protocols implemented in the product, and provide results of the testing for Lab Entry. These protocols and formats include, but are not limited to:

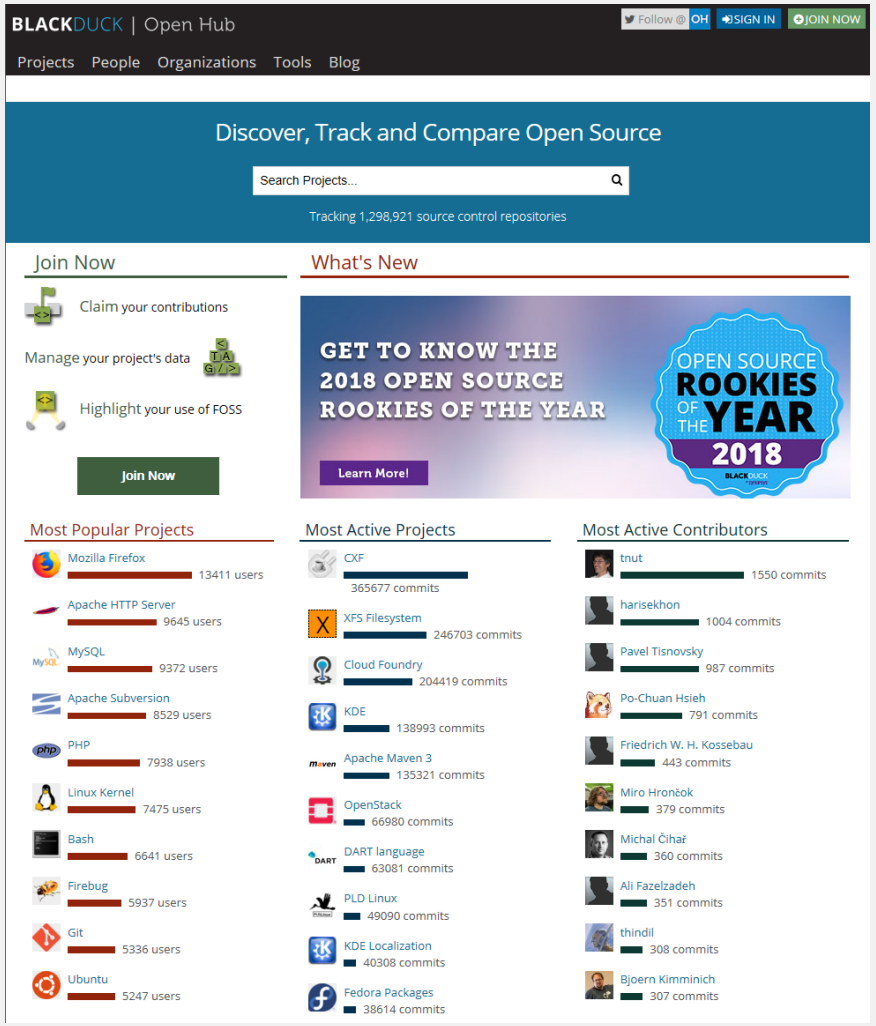
..... BGP, Diameter, DNS, DVRMP, EAP, FTP, GRE, GTP, H.225, H.248, H.323, HTTP, ICMP, IMAP, IPSec, IPv4, IPv6, IS-IS, ISAKMP/IKE, LDAP, MGCP, MPLS/LDP, NTP, OSPF, PIM, POP3, RADIUS, RIP, RSVP, RTP, RTSP, SIGCOMP, SIP, SNMP, SMTP, SSH, SSL/TLS, TACACS, TR-069, XML/SOAP, WAP.

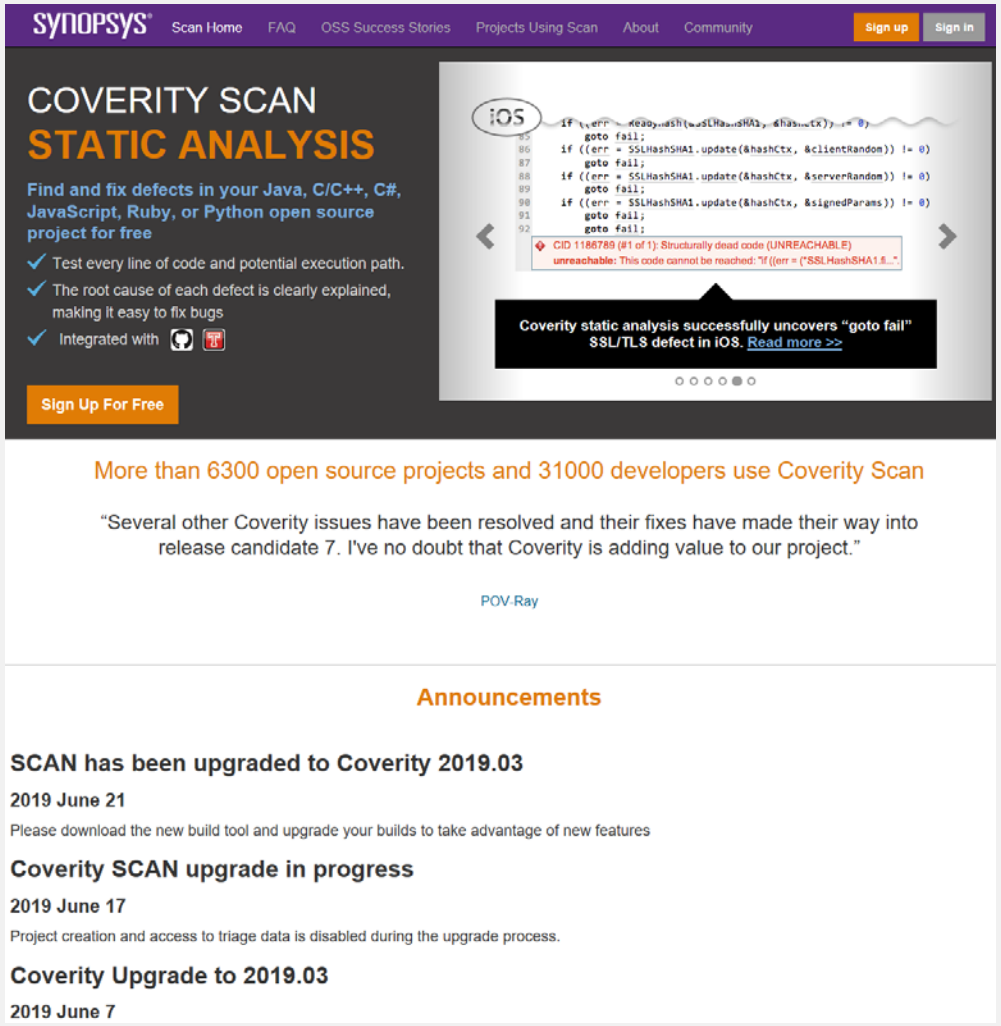
（抜粋）

SYNOPSYS

Open Hub (OSS情報提供) と Coverity Scan (OSS静的解析)

※いずれも無償提供





SYNOPSYS®

SYNOPSYS®
Silicon to Software™

Thank You