経済産業省

資料4

サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性

令和元年９月５日

経済産業省　商務情報政策局

サイバーセキュリティ課

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

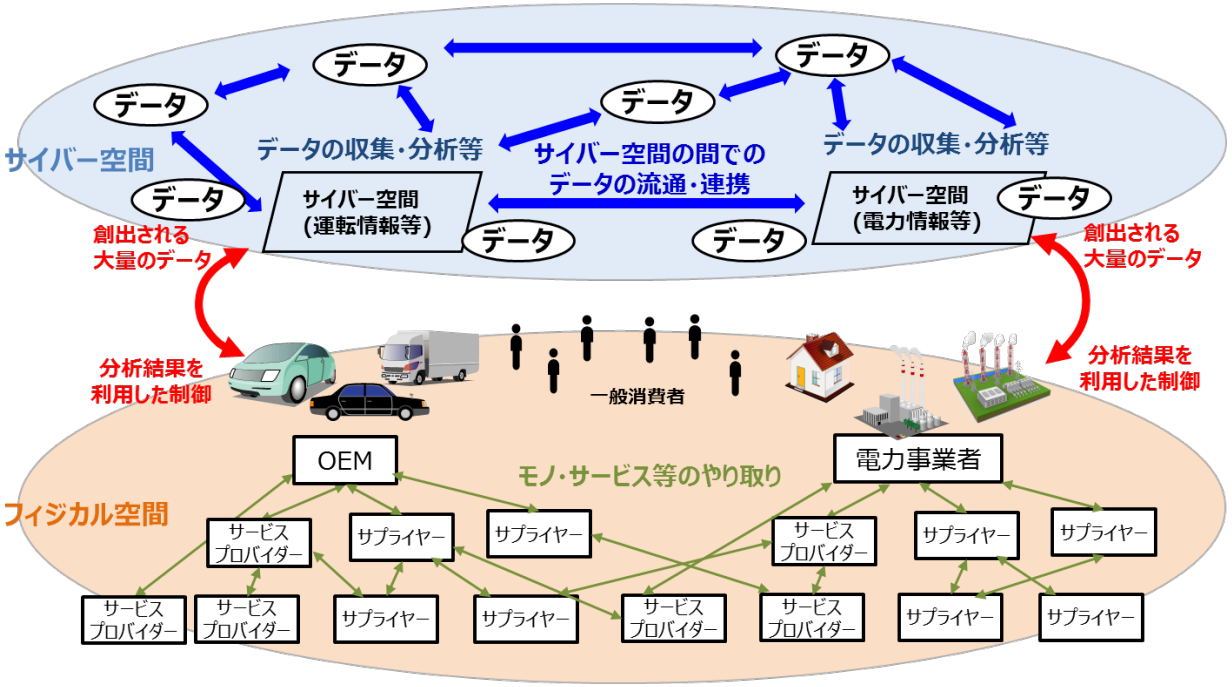
２．ソフトウェアに起因したインシデント事例

３．ソフトウェアの信頼性確保に関係する取組
（１）海外の取組事例
（２）国内の取組事例

４．本タスクフォースの検討事項

＜サプライチェーン構造の変化＞
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の策定

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**。
- 経済産業省では、「Society5.0」における**セキュリティ対策の全体像を整理**し、産業界が自らの対策に活用できる**セキュリティ対策例をまとめた、『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）』を平成31年4月に策定。**



Society5.0の社会におけるモノ・データ等のつながりのイメージ

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

＜三層構造と６つの構成要素＞
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造と６つの構成要素**）を提示。

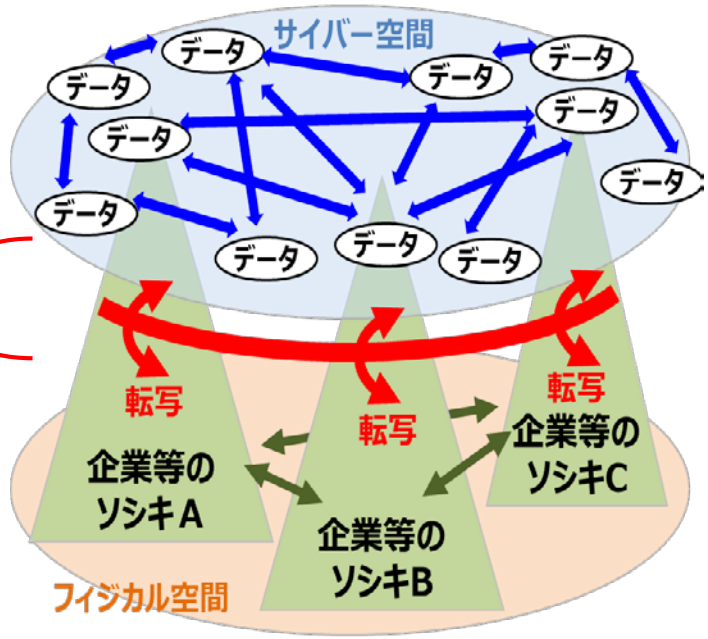
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



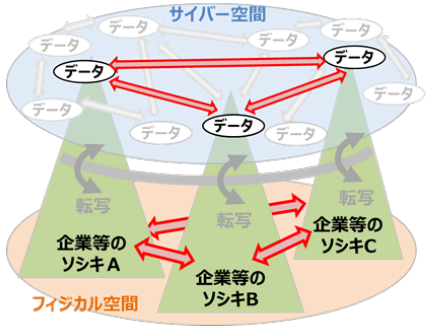
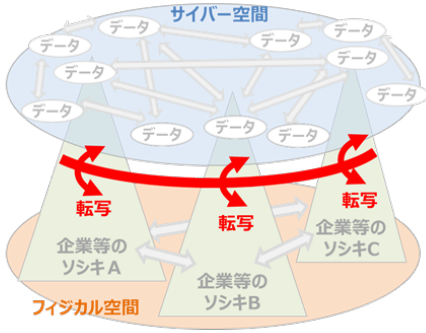
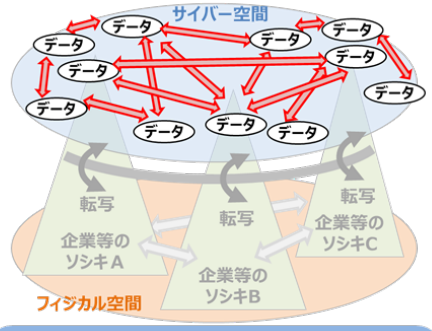
6つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を6つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	• ハードウェア、ソフトウェア及びそれらの部品 操作する機器を含む
データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	• 定義された目的を達成するための一連の活動の手続き
システム	• 目的を実現するためにモノで構成される仕組み・インフラ

＜CPSFの全体概要＞
三層構造モデルに基づきリスク源、対応方針等を提示

- サプライチェーンの信頼性を確保する観点から、産業社会を３つの層から捉え、それぞれにおいて**守るべきもの、直面するリスク源、対応方針**等を整理。

	企業間のつながり【第１層】	**フィジカル空間とサイバー空間のつながり【第２層】**	**サイバー空間におけるつながり【第３層】**
新たなサプライチェーン構造の整理			
機能（守るべきもの）	• 平時及び緊急時のリスク管理・対応体制の構築と運用 • 企業内及び企業間のリスク管理・対応体制の構築と運用	• フィジカル空間とサイバー空間の境界における情報の正確な転写及び正確な転写の証明	• データの加工・分析 • データの保管 • データの送受信
セキュリティインシデント	• 保護すべき資産の棄損 • 他組織のセキュリティ事象発生に起因する事業停止	• 不正確なデータの送信 • 安全に支障をきたす動作	• 保護すべきデータの漏えい • なりすまし等による不正な組織からのデータ受信
リスク源（構成要素ごとに整理）	• セキュリティリスクに対するガバナンスの欠如 • 他組織との連携状況の未把握	• 不正なIoT機器との接続 • 許容範囲外の入力データ	• 通信経路が保護されていない • 通信相手を識別していない
対策要件	■ マネジメントルールの徹底 ■ 関係者との役割分担	■ 接続相手の認証 ■ 安全なIoT機器の導入	■ 暗号化によるデータ保護 ■ データの提供者の信頼性確認

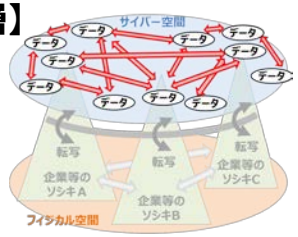
CPSFに基づく具体化・実装の推進

- 平成31年4月、**サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）**を策定。
- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**TFを新たに設置。**

実際の産業活動の内容

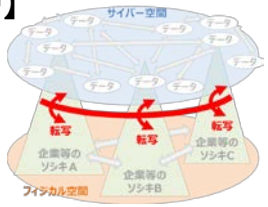
具体的な対策手法やルールの明確化

【第3層】



サイバー空間におけるつながり

【第2層】



フィジカル空間とサイバー空間のつながり

データを介した連携を行う産業活動
（分野間の連携 等）

分野別の産業活動
- ビル
- 電力
- 防衛
- 自動車
- スマートホーム 等

規模別の産業活動
- 大企業
- 中小企業 等

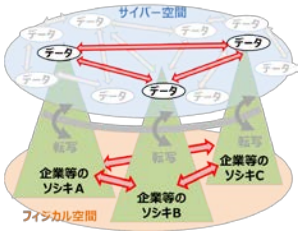
データの信頼性
（データの完全性、真正性等の確認　等）

転写機能を持つ機器の信頼性の確認手法
- 機器・システムのセキュリティ 等

ソフトウェアの取扱に関するルール・管理手法
- Software component transparency 等

【第1層】

企業間のつながり



産業サイバーセキュリティ研究会WG 1

標準モデル（CPSF）

- **ビルSWG**
- **電力SWG**
- **防衛産業SWG**
- **自動車産業SWG**
- **スマートホームSWG**
- **・・・**

分野横断SWG

『第3層』TF (⇒ データ区分に応じて適切なセキュリティ対策要件 等)

ソフトウェア TF （⇒ OSSを含むソフトウェア管理手法 等)

『第2層』TF (⇒ 機器のラベリングの仕組、認証制度の在り方 等)

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

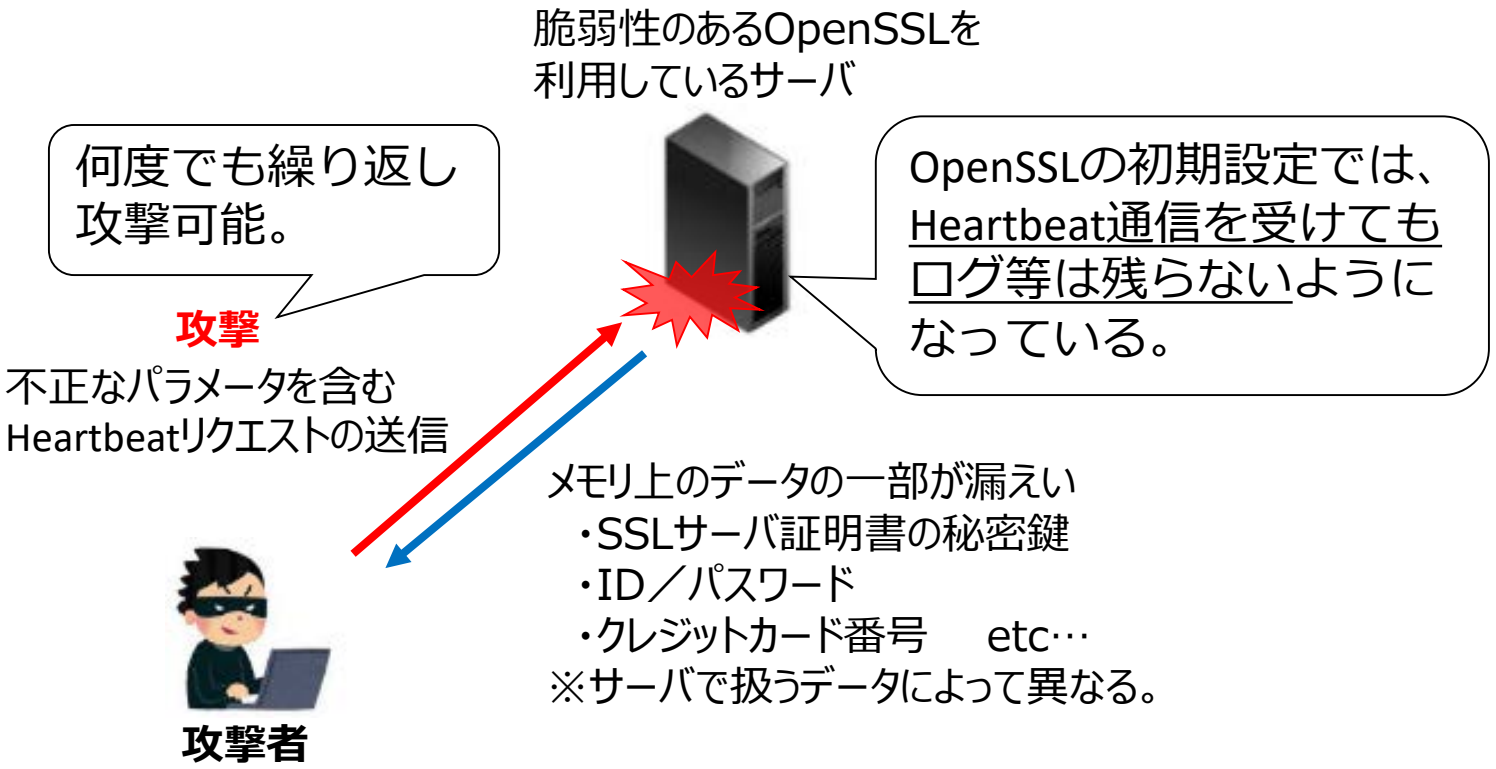
２．ソフトウェアに起因したインシデント事例

３．ソフトウェアの信頼性確保に関係する取組
（１）海外の取組事例
（２）国内の取組事例

４．本タスクフォースの検討事項

OSSライブラリの脆弱性：”Heartbleed”

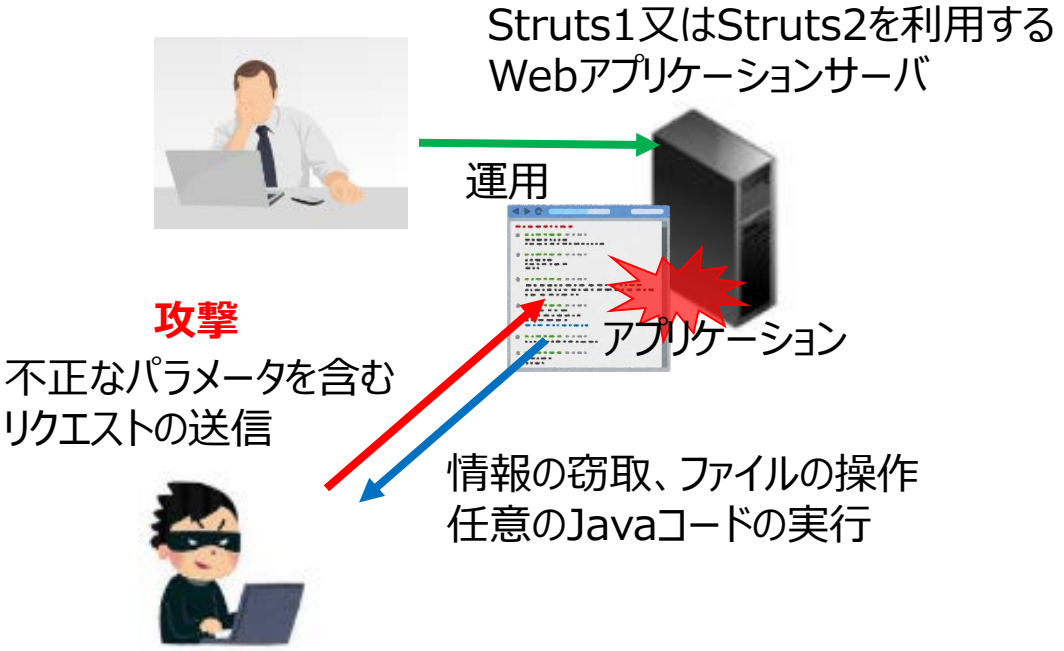
- OpenSSL（SSL/TLSプロトコルのオープンソースのライブラリ）において、Heartbeat※機能で見つかった脆弱性（2014年4月公表）。
  ※機器間で通信が行われていない間もTLSセッションの接続を維持し、通信相手が存在しているかを確認する機能。
- 脆弱性を含んだバージョンのOpenSSLサーバ宛に、細工をしたHeartbeatのリクエストを送ると、その返答にサーバのメモリ上のデータが含まれてしまうもの。メモリ上の**ID/PWやSSLサーバ証明書の秘密鍵が漏えいする可能性があった。**



サポートの終了したOSSで見つかった脆弱性：“Apache Struts1”

- 2014年4月17日、Apache Struts2において任意のJavaコードが実行されてしまう脆弱性（CVE-2014-0094）が公表された。
- セキュリティベンダー等の検証の結果、同様の脆弱性は**2013年4月5日に開発元のサポートが終了したApache Struts1にも存在することが判明**したが、開発元からの修正パッチの提供※はなく、またStruts2へのバージョンアップも容易でないことから、**サービスを停止するシステムが出た。**

※開発元（Apacheソフトウェア財団）のサポート終了後も、公表されているソースコードを基に、独自の修正パッチを開発・提供している企業・団体等は存在している。



Struts1を利用しており、停止した公共サービス例

政府機関等	製品・サービス
国税庁	確定申告書等作成コーナー等
IPA	ITパスポート受付システム
島根県警	遺失物公開システム
みやま市図書館	ＷＥＢ蔵書検索サービス
	etc…

OSSライブラリに悪意のあるコードが仕込まれる：Copay

- 仮想通貨（暗号資産）のウォレットアプリ「Copay」にユーザーの仮想通貨を盗み出すバックドアが仕掛けられて公開されていた。
- 攻撃者はCopay本体ではなく、Copayが利用する外部ライブラリの一つ（event-stream）を正規の権限で編集し、悪意のあるコードが仕込まれた外部ライブラリ（flatmap-stream）に関連させることでバックドアを仕掛けた。
- 悪意あるコードを追加する工程を複雑にし、かつ隠蔽を行うことで発覚を遅らせようとした。

2017.10 ・開発者によるevent-streamの最終更新

⋮

2018.8末 ・攻撃者がevent-streamの開発者に**「メンテナンスを引き継ぎたい」と持ちかけメンテナンス権限を取得**

2018.9.9 ・攻撃者がevent-streamを更新 → event-streamがflatmap-streamと関連

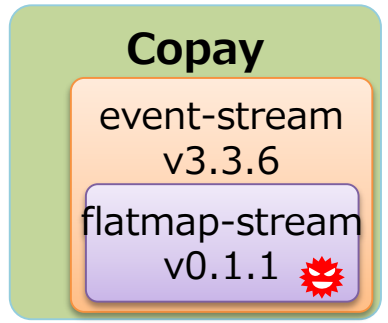
2018.10.5 ・攻撃者がflatmap-streamに**悪意のあるコードを追加**

2018.10.26 ・Copayが更新

→ Copayが悪意のあるコードが仕込まれたflatmap-stream に関連するようになり、攻撃者がバックドアを利用できるように

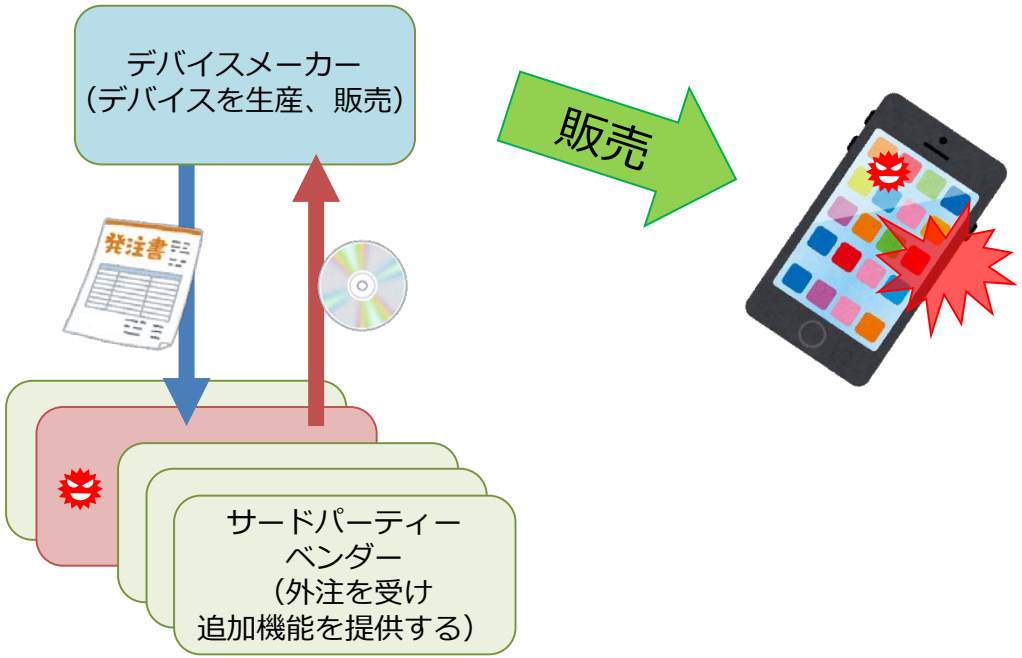
⋮

2018.11.26 ・ニュースになり、 flatmap-streamは削除された



サードパーティベンダーが悪意のあるコードを仕込む：Triada

- Triadaは感染したAndroidデバイスに悪意のあるアプリをインストールしたり、スパム広告を表示させたりするマルウェア。
- 2016年に発見された初期のTriadaは、ユーザがTriadaの組み込まれたアプリをインストールすることで感染するタイプであったが、**2017年7月に発見された新種は出荷前のAndroidデバイスにプレインストールされ、ファームウェアのバックドアになっていた**。
- Androidデバイスメーカーから外注を受けた**ソフトウェアベンダーが、ソースコードにTriadaのコードを紛れ込ませていた**と見られている。



IoT機器のサプライチェーンリスク：ASUS社端末におけるアップデート機能を悪用した攻撃

- 台湾のIT機器大手ASUS社※1において、正規のアップデートサーバが攻撃を受け、当該サーバから**端末向けに配布されたアップデートファイルを介し、数十万の同社端末がマルウェアに感染**する事案が発生。

（出典：MOTHERBOARD誌にてKim Zetter氏執筆。さらにKaspersky社が本件の簡易レポート発出。）

- 正規のダウンロード経路を悪用した同様の攻撃は、2017年に「CCleaner※2」においても発生しており、**マルウェア感染経路の一つ**として警戒を要する。

※1 ASUS社：台北市に本社を置く大手PC、スマートフォン、周辺機器製造メーカー。ソニー、アップル、HP、EPSON等への部品供給も行う。
※2 CCleaner：ハードディスク内部の不要なファイルやレジストリを削除するためのツール。イギリスの Piriform Ltd. が開発。

本事案の詳細（原因・影響等）

- 本攻撃は**2018年6月から11月**にかけて発生。「Shadow Hammer」と呼ばれる。
- 「ASUS Live Update Utility（アップデートサーバ）」による**ソフトウェアアップデートを経由**し、**マルウェア（バックドアファイル）**が**数十万台のASUS端末**に感染。

※ Kaspersky社は数百万台に上る可能性も指摘

- 本攻撃の大きな特徴として、**マルウェアは標的とする端末のMACアドレスをあらかじめ保有**しており、**感染端末のMACアドレスを参照し、それが標的端末であるかを識別**していた。

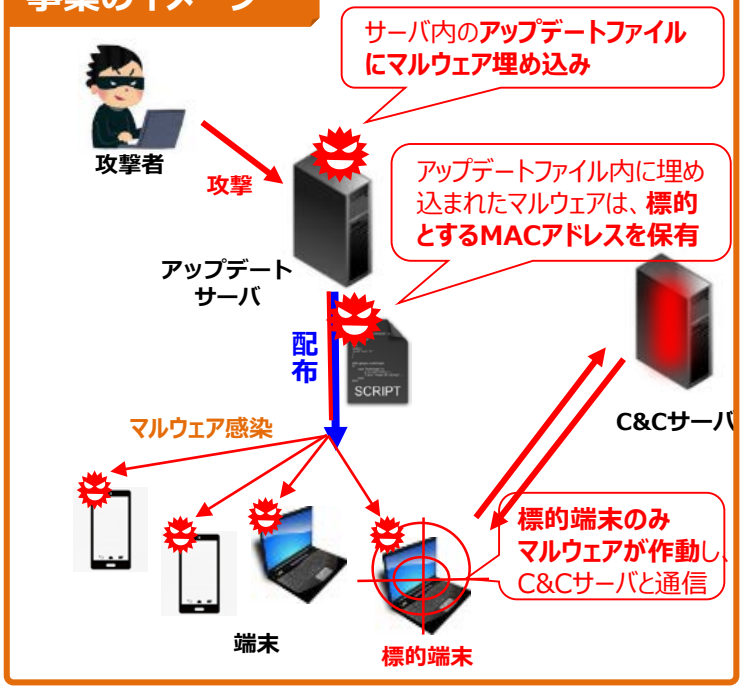
※ Kaspersky社は、200の検体サンプルから600の標的MACアドレスを確認している由

- 識別の結果、**マルウェア感染端末が標的端末であった場合、C&Cサーバと通信を開始する攻撃手法**。実際に標的端末が感染。

✓ 標的端末以外ではマルウェアを作動させないことで、事案の発覚を遅らせる狙いがあるとみられる。

✓ 攻撃者はMACアドレスにより、生産ロット等から標的とする特定の出荷先を絞り込んだものと推測される。

事案のイメージ



OSSのライセンスが問題になった事例

- OSSの利用に際しては、脆弱性対策だけでなく、使用許諾条件等を確認してライセンス違反を回避することも重要。
- ライセンス違反による訴訟により、販売の差し止めや損害賠償請求が行われたり、違反が公になるとブランドの毀損やネガティブキャンペーンにつながったりすることもある。

EPSON KOWAの例

・2002年、エプソンコーワは、リリースしたLinux用高品質プリンタドライバ及びスキャナドライバについて、第三者からGPLの条件と異なっているとの指摘を受け、対応を行った。（訴訟は無し。）
・同社は、GPLと非GPLのソースコード及び非公開のバイナリについて、個々のライセンスを明確にせずに二次配布を行った（GPL違反）。また、ドライバがリンクしていたLGPLのライブラリについても使用許諾がLPGLに準拠するものではなかった。
・同社は、指摘に基づき、ライセンスを明確化するとともに、GPL準拠のライブラリをLPGL準拠のものに差し替えた上で、LGPL第6条に基づき非公開コンポーネントのリバースエンジニアリングを許可するよう使用許諾を修正した。

Panasonic Avionics（パナソニックの関連会社）の例

・2017年3月、Panasonic Avionicsが開発した航空機内エンターテイメント（IFE）ソフトウェアについて、米国のCoKinetic SystemsからGPL違反を訴えられたもの。
・CoKinetic Systemsは、本件は過失によるGPL違反ではなく、競合企業が類似のソフトウェアを開発するのを妨害する目的で故意にソースコードの開示を拒否したとして、１億ドルの賠償を求める訴訟をニューヨーク連邦裁判所で起こした。2018年1月に両社は和解したが、賠償額は明かされていない。

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

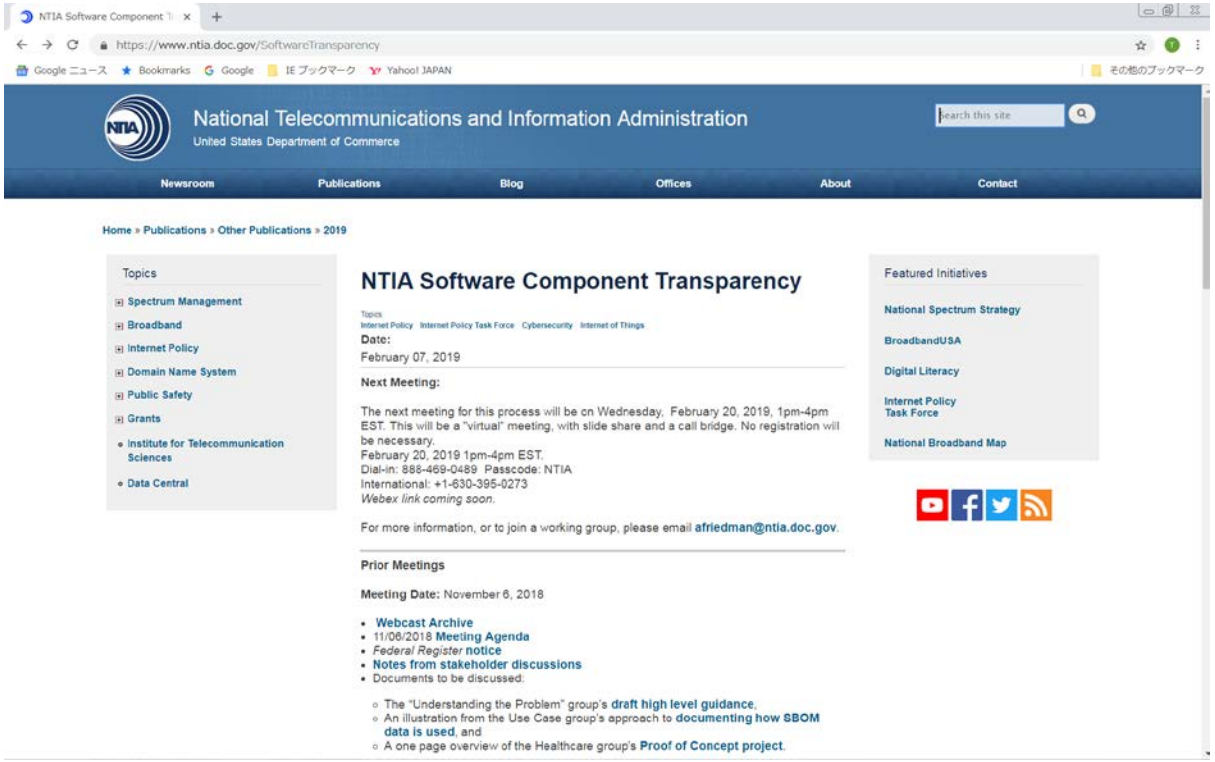
２．ソフトウェアに起因したインシデント事例

３．ソフトウェアの信頼性確保に関係する取組
（１）海外の取組事例
（２）国内の取組事例

４．本タスクフォースの検討事項

NTIA Software Component Transparencyに関する会合の設置

- 昨年、米国NTIA（電気通信情報局）において、「Software Component Transparency」に関するMultistakeholder Meetingが設置された。
- ここでは、ソフトウェアの脆弱性情報の理解と処理、成長するIoTマーケットへの対処、安全なソフトウェア開発ライフサイクルの促進の3つを柱に、既に5回会合が開催された。



官民関係者によるオープンかつ透明なかたちでの議論を目的としていることもあり、最終成果物及び活動期間（終了時期）は明記されていない
（「標準化に関与することを目指してはいない」ともある）

ねらい

ソフトウェアの脆弱性情報
理解と処理

成長するIoTマーケットへの対処

安全なソフトウェア開発
ライフサイクルの促進

過去の開催

2018年　7月19日（第1回）
11月 6日（第2回）
2019年　2月20日（第3回）
4月11日（第4回）
6月27日（第5回）
9月 5日（予定）

NTIA会合の概要（ワーキンググループ、参加者等）

- 参加メンバーは、ソフトウェアベンダー、通信プロバイダ、金融サービス事業者等幅広い参加を募る形となっている。また、４つの作業WGが設置され、各WGの発表と全体討議の形で進められている。

積極的な参加者の所属組織

エントリーがオープンな形で進められ、遠隔でも参加（傍聴）が可能なため参加者の全体像は明らかでないが、以下は資料等から判明した、積極的な参加者組織

（セキュリティ機関）
CERT/CC、 Nova Leah、NYUサイバーセキュリティセンター
（OSS）
Linux Foundation
（セキュリティ事業者）
マカフィー、 s-Fractal Consulting LLC
Turnaround Security
CA Veracode、Cyber Services Eventable
（その他IT事業者）
マイクロソフト、PSIRT（CISCO）、シーメンス、Oracle、PTC
（医療ヘルスケア）
New York Presbyterian、Ion Channel
（行政）
NTIA、NIST
（その他）
Consumer Technology Association、SAFECode.or

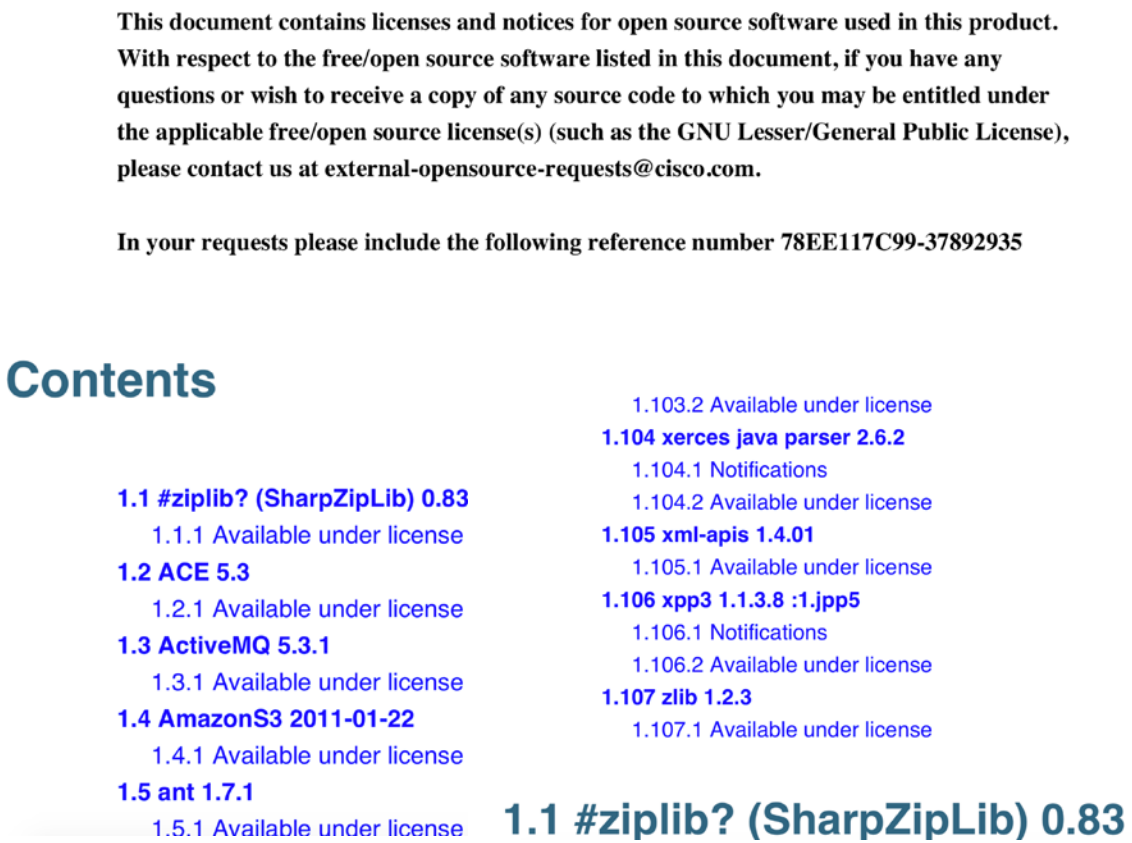
設置されたワーキンググループ

Understanding the Problem	SBoMの共有を含めて、「ソフトウェア透明性」の概念と課題の洗い出し。用語、課題の明確化、実装ガイドといった成果が想定されている。
Use Cases and State of Practice	SBoM活用に関する現在と将来のユースケース特定。現状での成功要因と課題を目指す
Standards and Formats	ソフト開発に当たり利用される、外部のソフトウェア部品、共有ライブラリー、商用ソフトウェア、オープンソースについての現在の標準とイニシアチブの調査
Healthcare Proof of Concept	SBoMフォーマット・プロトタイプ作成及びSBoM作成・活用ユースケース開発、利用方法確立等を、医療組織と医療デバイス製造業者で進める。

（参考）SBoMについて

- SBoM (Software Bill of Material）はソフト部品構成表ともいえるもの。様々なソフトウェア部品の一覧とそのライセンス等でまとめられている。
- NTIAは、2019年8月に開催されたBlackhatでもSBoMに係る取り組みを発表。

SBoMのイメージ



This document contains licenses and notices for open source software used in this product. With respect to the free/open source software listed in this document, if you have any questions or wish to receive a copy of any source code to which you may be entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please contact us at external-opensource-requests@cisco.com.

In your requests please include the following reference number 78EE117C99-37892935

Contents

1.1 #ziplib? (SharpZipLib) 0.83

補足

一義的なSBoMの定義があるわけではなく、ばらばらな取組が個別に進んだ

標準化が進んだリーダー格は、ISO/IEC 19770-2のSWIDとLinux FoundationのSPDX

食品医薬品局（FDA）（CBoM）や金融機関がSBoMの活用で先行しているとされる

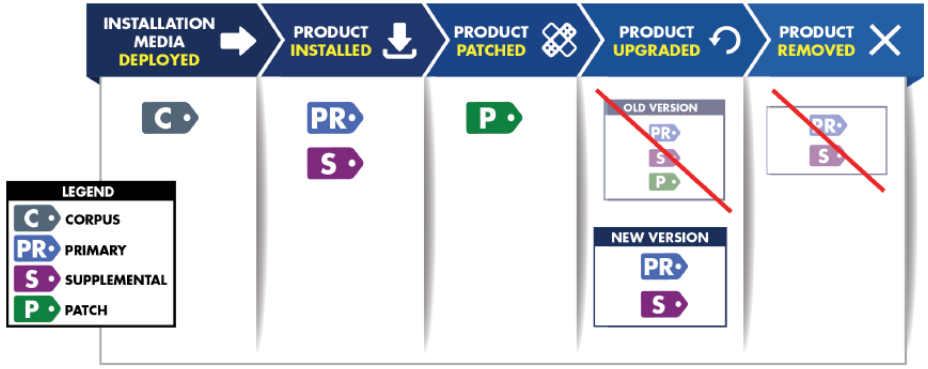
ただし、（OSSを中心とする）ソフトウェアの脆弱性対策としてはまだこれから

https://www.ntia.doc.gov/files/ntia/publications/corman_swct_kickoff_perspective.pdf

（参考）ソフトウェアIDタグ（SWID）

- SWIDは、ISOとIECによるソフトウェアの特定に関する国際規格（ISO/IEC 19770-2）（2009年11月）。ソフトウェアのライフサイクルに応じて4つのタグの種類があり、構成要素についても整理されている。
  （国際標準化を受け、NISTがSWID作成ガイドラインを公表）

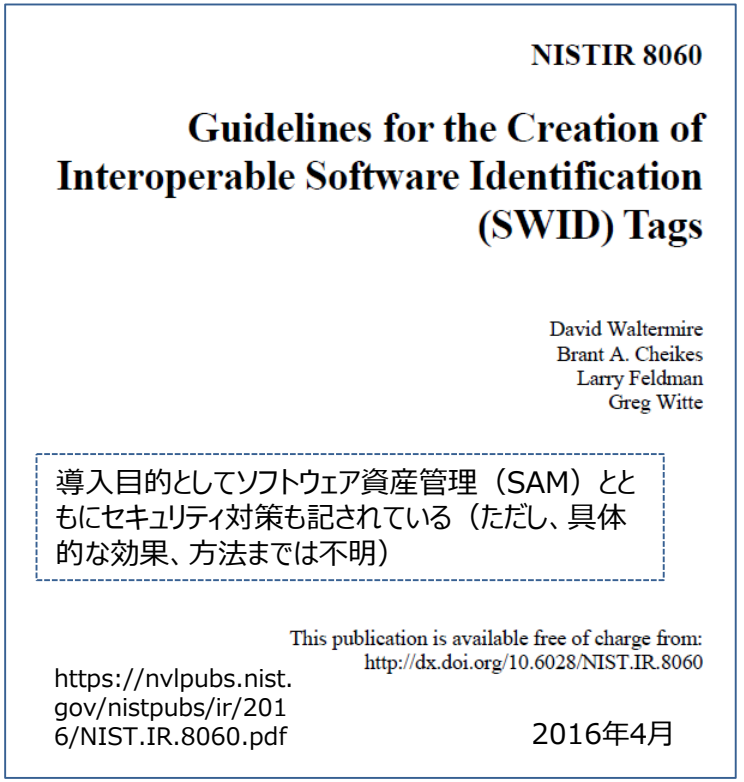
- XMLフォーマット
- 必須属性と任意属性を持っており拡張可能
- 2015年改訂版では、パッチ対応属性やハッシュ値属性のサポートなど脆弱性対策に関連する項目が盛り込まれた



SWIDタグとソフトウェアライフサイクル

組織名_プロダクト名.swidtag

要素			説明
ルート属性(SoftwareIdentity)			ソフトウェア識別についてのルート属性を記述する。
子要素	組織情報(Entity)	タグを生成した組織は必須，他は選択	このSWIDタグに対して責任のある組織の情報を記述する。
	リンク情報(Link)	選択	他のファイルの参照関係を記述する。関係するファイルやダウンロード元，脆弱性データベース，使用権なども定義できる。
	メタ情報(Meta)	選択	このSWIDに関する任意の情報を記述する。
	ソフトウェアの本来情報(Payload)	選択	インストールされるファイルについて本来の情報を記述する。
	ソフトウェアの実際情報(Evidence)	選択	SWIDタグが見つからないソフトウェアのシステム検査結果を記述する。
	署名情報(Signature)	選択	このSWIDタグに対して責任のある組織の署名情報を記述する。



NISTIR 8060

Guidelines for the Creation of Interoperable Software Identification (SWID) Tags

David Waltermire
Brant A. Cheikes
Larry Feldman
Greg Witte

導入目的としてソフトウェア資産管理（SAM）とともにセキュリティ対策も記されている（ただし、具体的な効果、方法までは不明）

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8060

https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf

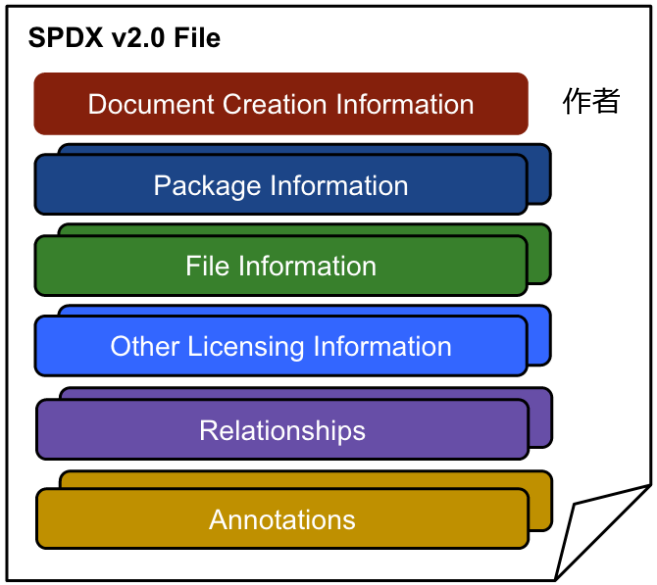
2016年4月

（図左上）Guidelines for the Creation of Interoperable Software Identification (SWID) Tags（2016年4月NIST）https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf
（図左下）IT資産管理関連タグの国際標準化動向（2016年6月ソフトウェア資産管理評価認定協会代表理事 高橋快昇氏）http://www.samac.or.jp/img/2016_seminar/pdf/file10.pdf

（参考）ソフトウェアパッケージデータ交換（SPDX）

- SPDXはライセンス、著作権、セキュリティ等のソフトウェアの構成要素（bill of material）についてのオープンな標準で、Linux Foundationが支援するSPDX Working Groupが策定した。
- ライセンスの登録、管理が中心となっている。

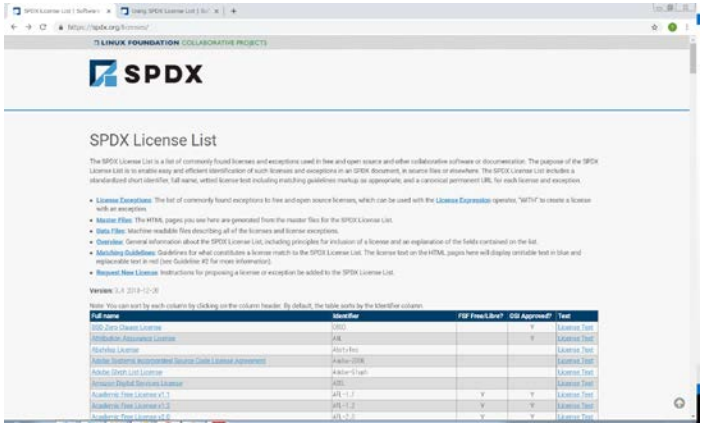
SPDXファイルの構成要素



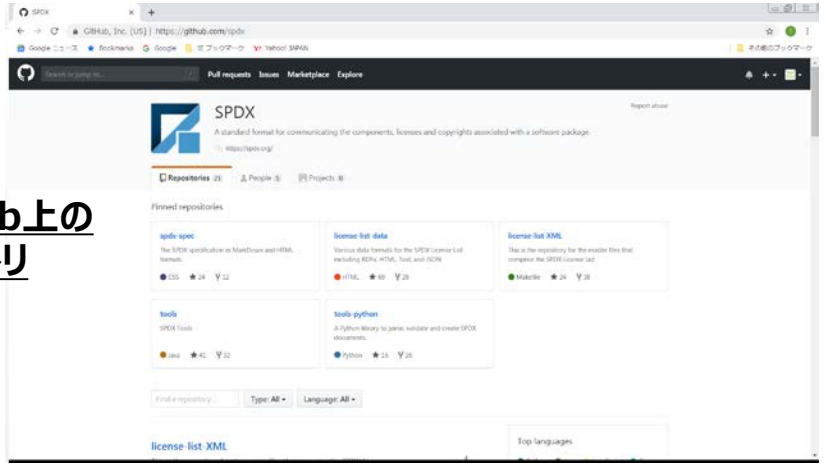
注記

- ソースファイル
- データベース情報：パッケージの正式名、バージョン、ファイル名、ダウンロード場所ライセンス情報、著作権情報、脆弱性情報等等
（参考：IPA「ソフトウェア識別管理に向けた分析事業」の報告書」）

ライセンスリスト



GitHub上のリポジトリ



BSA - Framework for Secure Software

- 米国のBSA（Business Software Alliance）は、ソフトウェアライフサイクルにおいてリスクベース等の観点からセキュリティを評価するためのフレームワーク（BSA - Framework for Secure Software）を2019年4月30日に策定。ソフトウェア開発組織におけるプロセスと製品機能のベストプラクティスを整理。
- このフレームワークでは、３つの機能（Functions）とその配下のカテゴリー/サブカテゴリー毎に、診断ステートメント及びその留意点、参照文書を体系化。

【 BSA - Framework for Secure Softwareにおける取りまとめ概要】

機能（英語名）	カテゴリー/サブカテゴリー	カテゴリー/サブカテゴリーの一例	診断ステートメント	留意点	参照文書
セキュアな開発(SECURE DEVELOPMENT)	• 各機能に関連する複数の考慮事項を提示 • カテゴリーにおいて領域的な分類をした上で、サブカテゴリーにおいて詳細な考慮事項が体系化されている	• セキュアコーディング/ソフトウェアデザイン時の脅威モデリングとリスク分析 • テストと検証/ソフトウェアの攻撃対象領域の分析と検証	• 各カテゴリー/サブカテゴリーで示された考慮事項の達成をサポートする一連(複数パターン)の結果(ベストプラクティス)を提示 • 各結果が現状と合致するかによって評価の実施可能	• 診断ステートメントを用いて評価を行う際の留意点、補足情報等	• 診断ステートメントにおいて示された結果に関する詳細情報(達成手法等)の参照先 • 参照先は、ISO/IEC、SAFECode、等
セキュアな機能(SECURE CAPABILITIES)		• ID管理と認証のサポート/認証失敗のリスクを招くアーキテクチャ上の弱点対策 • パッチ適用性/安全な更新プログラムとセキュリティパッチの受け取り			
セキュアなライフサイクル(SECURE LIFECYCLE)		• 脆弱性管理/ベンダーによる最新の脆弱性管理計画の維持 • 構成/安全なインストールとオペレーションを容易にする構成、構成ガイダンス			

NIST - Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

- NISTにより、セキュリティに配慮したソフトウェア開発手法を既存の標準やガイドライン等を参照する形でSecure Software Development Framework (SSDF)として整理（2019年6月にドラフト版を公表）。
- SSDFでは、各手法を「組織構築」「ソフトウェア保護」「セキュアなソフトウェア」「脆弱性レポート対応」の4つに分類の上、何をすべきか（Practice-Taskの2階層）、事例、参照文書について体系化。

【 SSDFにおける各手法の分類】

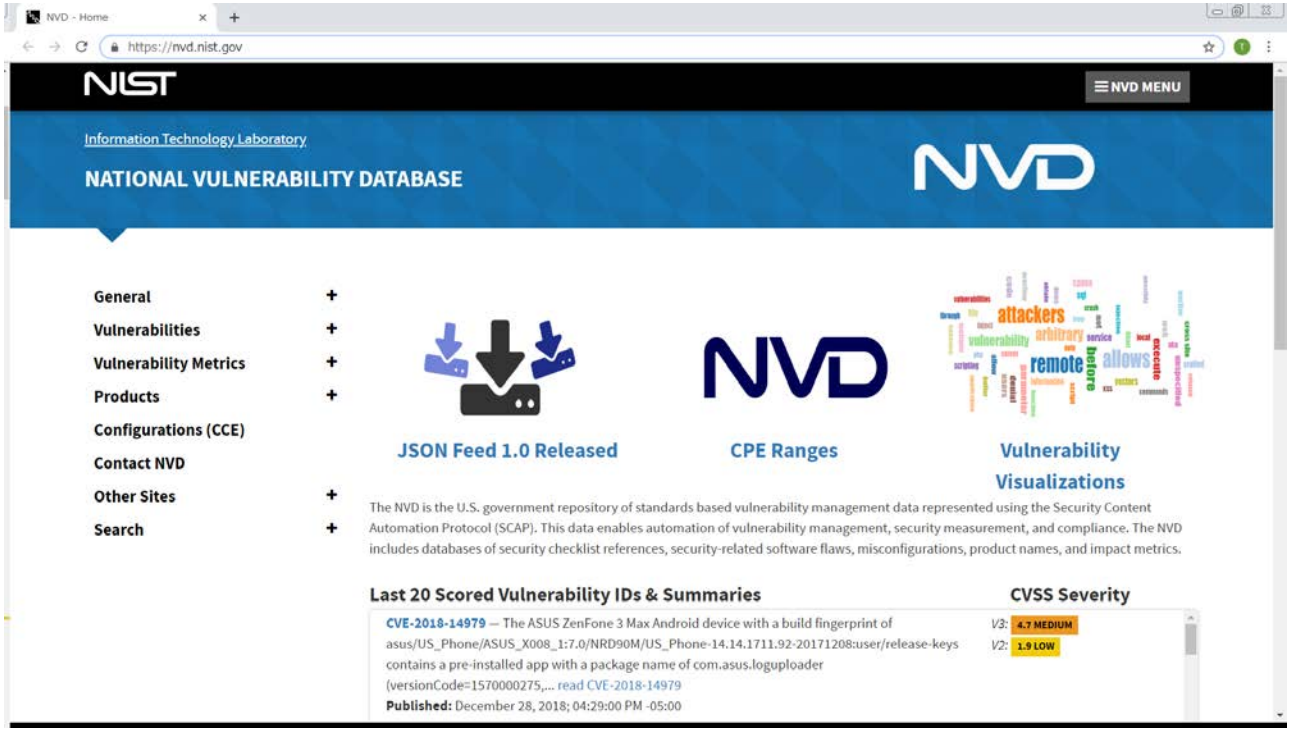
分類	分類（英語名）	概要	手法例	備考
組織構築	Prepare the Organization（PO）	人材、処理能力、技術等のソフトウェア開発リソース確保	• ソフトウェア開発におけるセキュリティ要件を定義 • 各役割と責任の実装	• PSの中でSBOMの作成と維持について言及あり • 参照文書（Reference）は、ISO、BSA、NIST CSF 等
ソフトウェア保護	Protect the Software（PS）	ソフトウェアの全てのコンポーネントを改ざんや不正アクセスから保護	• 全ての形式のコードを改ざんや不正アクセスから保護	
セキュアなソフトウェア	Produce Well-Secured Software（PW）	ソフトウェアリリース時のセキュリティに関する脆弱性を最小化	• ソフトウェアデザインにおいてリスク情報・セキュリティ要件を考慮	
脆弱性レポート対応	Respond to Vulnerability Reports （RV）	ソフトウェアセキュリティの脆弱性の認識、適切な対応、将来にわたる予防策	• 継続的な脆弱性の特定・確認 • 改善策の評価・優先付け	

ソフトウェア脆弱性情報　（NVD、CVE）

- NVD（National Vulnerabilitiy Database）は、NISTが運営する脆弱性データベースで、SCAP（Security Content Automation Protocol）を用いることで脆弱性管理の自動化を支えている。

NVD

セキュリティチェックリストへの参照、セキュリティに資するソフトウェアの欠陥、製品名、影響等がデータベースに盛り込まれている



https://nvd.nist.gov/

(以下はIPAのHPより)

SCAP：
米国政府が推進している情報セキュリティにかかわる技術面での自動化と標準化を実現する技術仕様

CVE(Common Vulnerabilities and Exposures)：個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番している識別子。SCAPの構成要素のひとつとなっている。

https://www.ipa.go.jp/security/vuln/CVE.html

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

２．ソフトウェアに起因したインシデント事例

３．ソフトウェアの信頼性確保に関係する取組

（１）海外の取組事例

（２）国内の取組事例

４．本タスクフォースの検討事項

ソフトウェア脆弱性情報　（JVN）

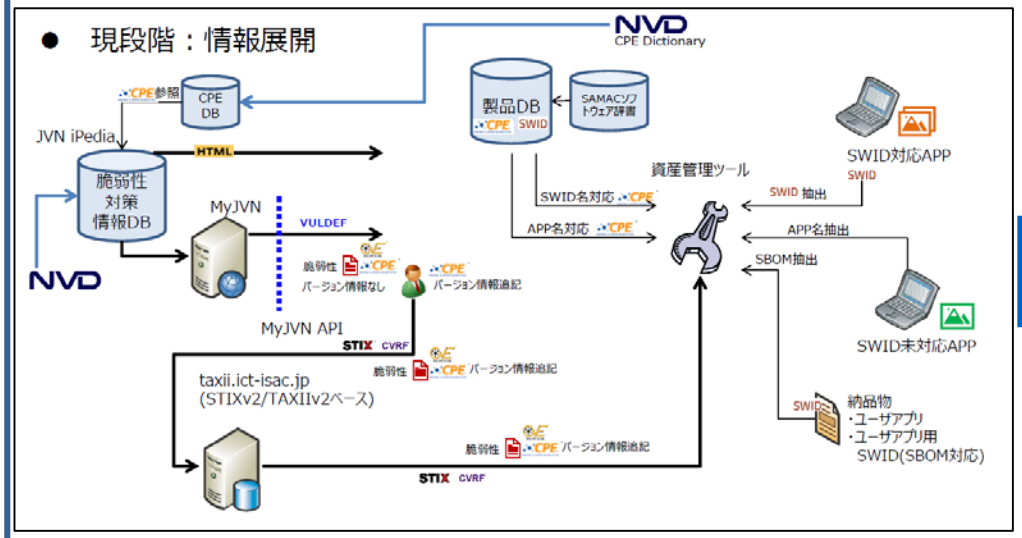
- Japan Vulnerability Notes（JVN）は、IPAとJPCERT/CCが共同運営する脆弱性対策情報ポータルサイト。
- 「情報セキュリティ早期警戒パートナーシップ」制度に基づいて報告され調整された脆弱性情報や、CERT/CC など海外の調整機関と連携した脆弱性情報が公表されている。

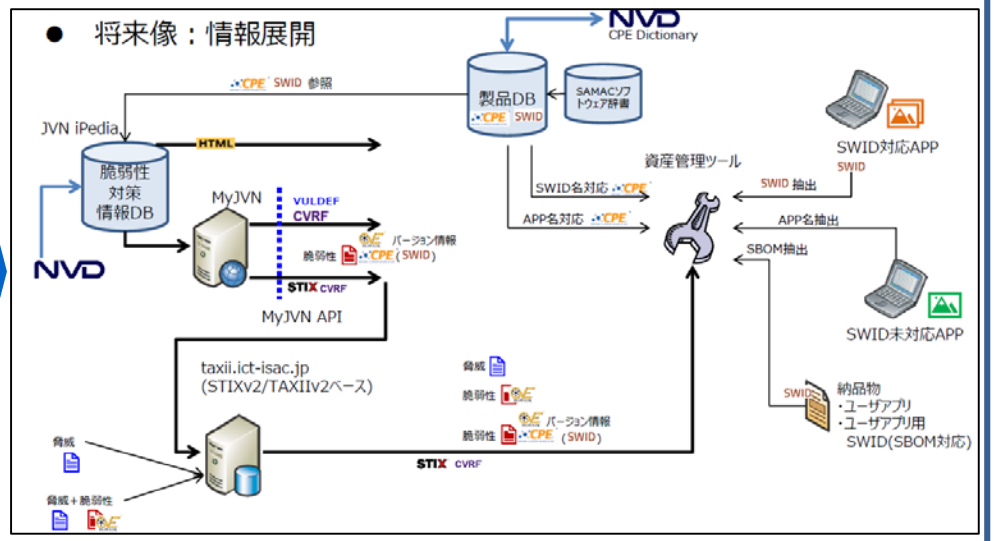
脅威情報や脆弱性情報の一元管理・共有への取組

- 脅威情報や脆弱性情報を一元管理・共有することで、各社の情報システムやサービスに対する迅速かつ効率的なセキュリティ対策・対応が進むことが期待される。
- 民間団体（ICT-ISAC、金融ISAC、Software ISAC等）を中心に、上記取組が進められている。

（取組の一例）ICT-ISAC

ICT-ISACでは、総務省の実証事業において脅威情報と脆弱性情報の共有を機械化し、迅速に処理することによりサイバー攻撃から防御する取組を行っている。





サイバー攻撃に関するJVN iPedia情報をSTIX/TAXII形式で交換する情報共有基盤を構築

（参考）OSSコミュニティ

- 国内外にあるOSS推進組織やコミュニティ等のうち、主なものは以下のとおり。

名称	概要	URL
Linux Foundation	世界のトップ百万ドメインの95%以上が利用しているOSであるLinuxに関するコミュニティにインフラ、サービス、イベント、トレーニングなどを通じた支援を実施	https://www.linuxfoundation.jp/about/
Apache Software Foundation	WebサーバソフトウェアであるApache HTTP Server開発のために発足したが、現在はそれ以外も数多いOSSプロジェクトをサポートするコミュニティ	https://www.apache.org/
Open Chain	オープンソースのライセンスコンプライアンスをシンプルで一貫性のあるものにすることでオープンソースの信頼を高めようとするプロジェクト。富士通、日立、マイクロソフト、NEC（いずれもプラチナ）等多数のグローバル企業が参画	https://www.openchainproject.org/ja/
Automotive linux	自動車メーカ、サプライヤ等が自動車のアプリ向けのLinuxベースのプラットフォームを構築しデファクト標準を目指すプロジェクト。トヨタ自動車、パナソニック（プラチナ）等が参画	https://www.automotivelinux.org/
SPDX	SBOMの策定、更新及びOSS上のライセンス管理支援（リスト提供等）を支援するプロジェクト。Linux Foundationの支援を受け、コミュニティへの参加もオープンである	https://spdx.org/participate（コミュニティ）
OSDN	オープンソースソフトウェア開発者に向け無料で利用できる世界規模でのソフトウェア/ファイル配信ネットワークを提供。個人、企業によるオープンソース活動の拠点としても利用	https://ja.osdn.net/
Open Source Initiative	「オープンソース」の利益を啓発、支持し、オープンソースコミュニティの様々な人達との橋渡しを目的に、国内外の数多くのOSSコミュニティの支援機能も果たす	https://opensource.org/community
日本OSS推進フォーラム	日本における情報システムのユーザー、ベンダー、学識経験者の有識者が参集し、OSSの活用上の課題について、自由な立場で議論し、課題解決に向けての取組みを行う	http://ossforum.jp/

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

２．ソフトウェアに起因したインシデント事例

３．ソフトウェアの信頼性確保に関係する取組
（１）海外の取組事例
（２）国内の取組事例

４．本タスクフォースの検討事項

【本TFにおける検討の背景】
企業・団体が抱えるソフトウェアのセキュリティ確保に関する課題

- 平成30年度の委託事業において、民間企業・団体等にソフトウェアのセキュリティ確保に関する課題についてヒアリングを行ったところ、ソフトウェアの管理手法や、脆弱性対応やビジネス利用等のOSSの利活用に関するものが多く挙げられた。

- ソフトウェア管理の統一フォーマットへのニーズ【大手製造業】
- SBoM の活用により新たに生じる懸念点【業界団体】
- SPDX、SWID の共通化議論が進んでいない【大手製造業】

ソフトウェアの管理手法に関する課題

- OSSの脆弱性対応コストの増加【大手製造業】
- 安全なOSSの選定（OSSの目利き）が困難【研究機関等】
- 脆弱性への対応可否判断が困難【大手製造業】
- ライセンスによる制約【大手SIer等】
- OSSを前提としない商取引慣行【業界団体】
- 海外OSSコミュニティでの発言力向上【大手製造業】
- 国内OSSコミュニティの活性化【大手製造業】

脆弱性対応やビジネス利用等、OSSの利活用に関する課題

- SBoMなどのソフトウェア管理手法について、その必要性は認識されているものの、課題を含めて検討する枠組みが存在しない。国際的な議論を注視しながら検討を進めていく必要がある。

- OSSを安全に利活用するための取組は、各企業・組織の活動に強く依存。脆弱性管理に関しては IPA, JPCERT/CCによる枠組みが構築されているが、協調領域として取り組むべき領域があるのではないか。

【現状】CPSFにおけるソフトウェア関連の記載の例

- CPSFでは、**機器の正規品確認を目的としたソフトウェアの真正性の確認や、脆弱性の確認を実施することを要求**。
- 一方、ソフトウェアの複雑化、OSSの利用拡大などに伴い、ソフトウェアそのもののセキュリティをどのように維持し続けるのか、それをどのように確認するかについては明確化されていない。

対策要件に応じたセキュリティ対策例集　（サイバー・フィジカル・セキュリティ対策フレームワーク　添付Ｃ）

対策要件ID	対策要件	対策例
CPS.SC-4	外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	<Basic> • ・・・ • 組織は、IoT機器や**ソフトウェア**に含まれるIDや秘密鍵、電子証明書等を用いて調達した**機器が正規品であることを確認**する。
CPS.CM-7	自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が**必要な脆弱性の有無**を確認する。	• ・・・

ソフトウェア管理手法のあり方　～利用者が留意するべき事項～

	開発中	運用中 （脆弱性情報の収集）	運用中 （脆弱性対応）
P.7 HeartBleedの脆弱性	✓使用中のOSSバージョン把握 ✓脆弱性情報の確認 ✓保守・サポート期間の確認		✓OSSのアップデート ✓WAF等による暫定対処 ✓サービスの一時停止
P.8 Strutsの脆弱性			
P.9 Copayの脆弱性	✓開発プロセスの確認	✓使用中のソフトウェアのバージョン把握 ✓脆弱性情報の確認 ✓コードサイニング証明書の確認	✓ソフトウェアのアップデート ✓FW等による暫定対処 ✓ソフトウェアの利用停止
P.10 Triadaの脆弱性			
P.11 ASUSの脆弱性	✓ パッチ配信サーバの安全性確認	✓脆弱性情報の確認	✓マルウェアの削除
P.12 OSSのライセンス問題	✓ライセンス内容の確認		✓ライセンス違反の是正

JVN等の活用により効率化

SBoM等の活用により効率化

STIX/TAXIIの活用により効率化・自動化

ソフトウェア管理手法のあり方　～利用者が留意するべき事項～

	開発中	運用中 （脆弱性情報の収集）	運用中 （脆弱性対応）
P.7 HeartBleedの脆弱性	ソフトウェア管理手法 （第1回TFで特にご議論 頂きたい内容）		脆弱性対応 （次回以降）
P.8 Strutsの脆弱性			
P.9 Copayの脆弱性			
P.10 Triadaの脆弱性			
P.11 ASUSの脆弱性			
P.12 OSSのライセンス問題	OSS利活用（次回以降）		

JVN等の活用により効率化

SBoM等の活用により効率化

STIX/TAXIIの活用により効率化・自動化

本TFにおける検討の方向性

- **ソフトウェア管理手法、脆弱性対応、OSSの利活用等**に関する検討を行う。

ソフトウェア管理手法の検討

- ソフトウェアの開発から、運用中の脆弱性発見まで
- 構成管理・脆弱性管理に求められるソフトウェア管理手法のあり方
- SBoM等ソフトウェア管理スキームの活用に求められる技術面・制度面の課題

脆弱性対応手法の検討

- 脆弱性が発見された場合のソフトウェアへの対応
- 脆弱性発覚時に必要な脆弱性への対応手法・体制のあり方
- 運用中システムへの脆弱性対応に求められる技術面・制度面の課題

OSSを利活用する際のビジネス的な側面の検討

・OSS利用に関連するライセンスや契約
・OSS活用のベストプラクティス／OSSコミュニティへの発信

第1回
検討事項

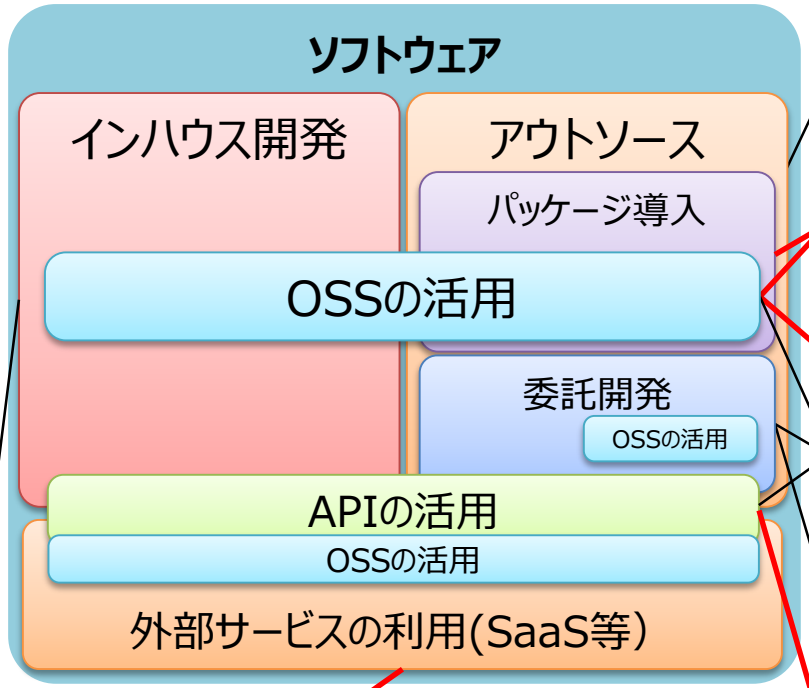
次回以降
検討予定事項

実効的なソフトウェア管理手法の検討

- 安全なソフトウェアを選定する上でも、開発したソフトウェアを流通させる上でも、ソフトウェアの構成情報の可視化は重要。国際的な動きとも連携しつつ、産業横断的に活用できるソフトウェア管理のあり方について検討。
- 国際的な動きとも連携しつつ、産業横断的に活用できるソフトウェア管理のあり方について検討を開始する。

検討事項（案）

- **構成管理・脆弱性管理に求められるソフトウェア管理手法のあり方**
- **SBoM等ソフトウェア管理スキームの活用に求められる技術面・制度面の課題**
- **NTIA等、諸外国機関との連携**



- 利用ソフトウェア・APIの脆弱性管理
- **保守・サポート期間の終了**
- **安全なOSSの選定、評価**
- ライセンスによる制約
- 再委託、再々委託先等の管理
  - 開発環境の管理
  - コーディング規約
- 責任分界

SBOMの活用

- セキュリティの要件定義の能力
- セキュアコーディング
- 脆弱性ハンドリング

- **安全な接続先の選定、評価**
- **SLAの担保**

- **安全なAPIの選定、評価**

（参考：次回以降）脆弱性対応手法及びOSSを利活用する際のビジネス的な留意事項等についての検討

- 脆弱性が発覚した際の効果的な対応手法及び既知の脆弱性の管理手法等について検討。
- OSSコミュニティの有効活用も含め、OSS活用のベストプラクティスや、OSS利用時に問題となり得る安全性のリスクやOSSのサポート期間、ライセンスの問題などを整理。

検討事項（案）

- **脆弱性発覚時に必要な脆弱性への対応手法・体制のあり方**
- **運用中システムへの脆弱性対応に求められる技術面・制度面の課題**
- **利用するOSSの安全性を評価するために必要な要件・体制**
- **ビジネスリスクマネジメント／OSS利用に関連するライセンスや契約**
- **OSS活用のベストプラクティス／OSSコミュニティへの発信**