経済産業省

資料3

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3年1月13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. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

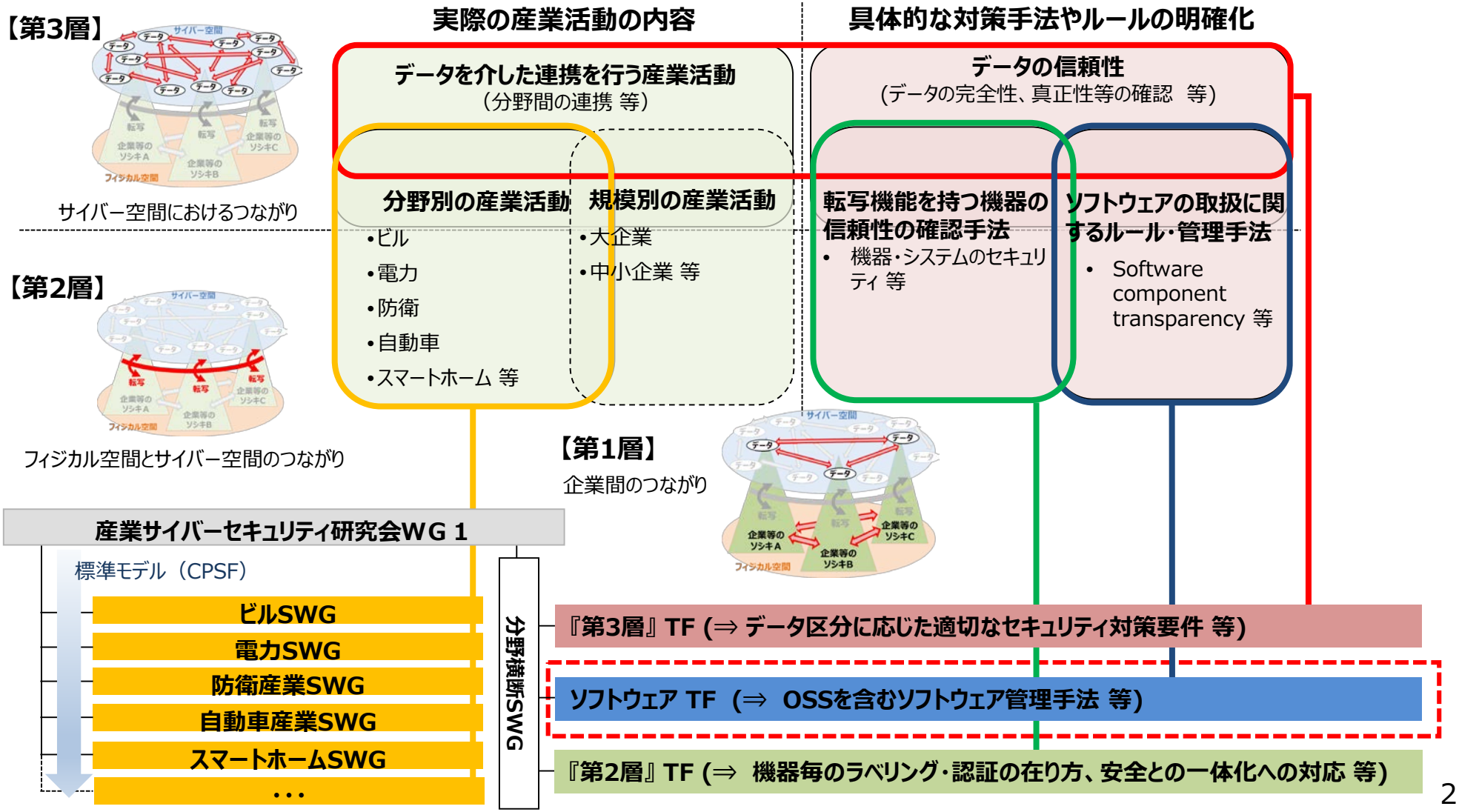
4. 本タスクフォースにおける検討事項

（１）OSS管理手法に関する事例集の作成

（２）国内でのSBOM活用促進に向けて

CPSFに基づくセキュリティ対策の具体化・実装の推進

- 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**タスクフォース（TF）にて議論。**



テーマ別TFの検討状況

- 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**タスクフォース（TF）にて議論。**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
（分野ごとに検討するためのSWGを設置）

- **ビルSWG**
  - ガイドライン第1版の策定
- **電力SWG**
  - 既存ガイドラインの強化
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表
- **スマートホームSWG**
  - ガイドライン案パブコメを実施
- ・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データマネジメントを俯瞰するモデルを提案し、データの信頼性確保に求められる要件を検討

ソフトウェアTF：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

検討事項：
OSSの管理手法に関するプラクティス集の策定等

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。

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. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

（１）OSS管理手法に関する事例集の作成

（２）国内でのSBOM活用促進に向けて

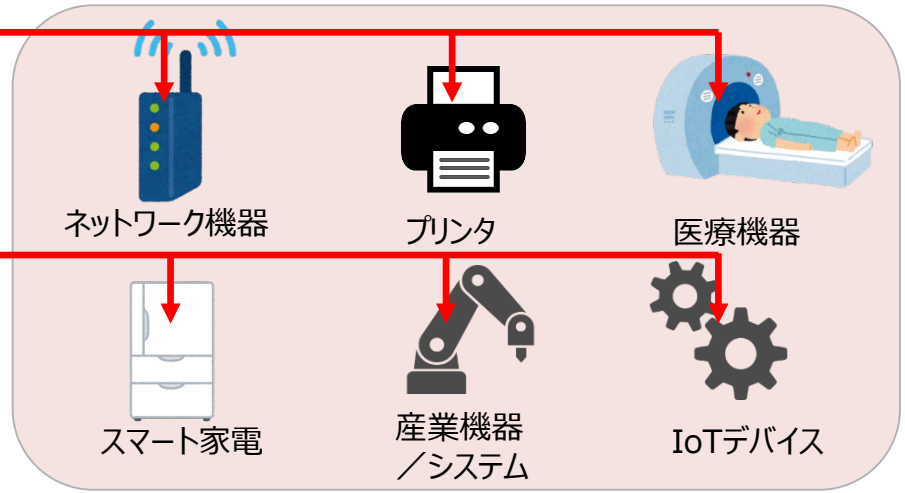
プロトコルスタックの脆弱性：“Ripple20”

- 2020年6月、JSOF社は、**Treck社※1が開発したTCP/IPプロトコルスタック※2「Treck TCP/IP Stack」に複数の脆弱性**があることを発表（発表年や当スタックが20年以上前から存在していること等に由来し、19の脆弱性の総称をRipple20と命名）。遠隔の第三者によって、**任意のコード実行、情報の窃取、サービス運用妨害（DoS）等の攻撃を受ける可能性**があり、最新バージョンへの更新やパッチの適用、 IPパケットのフィルタリング等の対策を呼び掛けている。
- Treck TCP/IP Stackは多数の企業が製品に採用しており、数億台かそれ以上の機器が影響を受けるとされ、家庭向けデバイス、ネットワーク機器、医療機器、産業制御機器／システム、重要インフラ分野などの幅広い領域への影響が懸念される。

◆攻撃イメージ／影響範囲の例

想定被害：任意のコード実行、情報漏えい、DoS

Treck TCP/IP Stackの採用製品は、下図以外にも多岐に渡る



- ✓ Treck TCP/IP StackはHP社、Schneider Electric社、Intel社、Rockwell Automation社、Caterpillar社、Baxter社等の製品が採用。
- ✓ 同様の脆弱性が、関連する他のTCP/IPスタックにも存在することが報告されている。

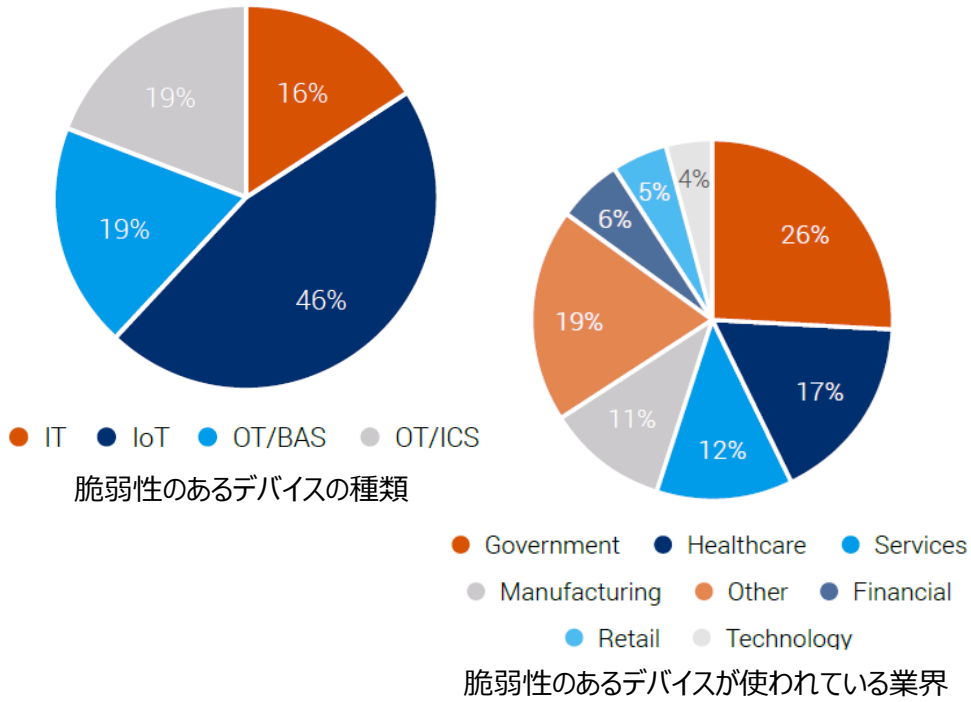
https://www.jsof-tech.com/ripple20/

※1　組み込み機器向けのインターネットプロトコルスタックを設計・開発する米国の企業
※2　階層構造で構成されるインターネットプロトコル群

プロトコルスタックの脆弱性：“AMNESIA:33”

- 2020年12月、Forescout社は、**<u>複数のオープンソースTCP/IPスタックに33の脆弱性</u>**があることを発表。150以上のベンダーの数百万台のIoT、OT、ITデバイスに影響し、メモリ破壊により、**<u>リモートコード実行、DoS、情報漏洩、DNSキャッシュポイズニング等に利用されるおそれ。</u>**
- 複数のオープンソースTCP/IPスタックが影響を受け、脆弱性のある全てのデバイスを特定しパッチを適用することには多大な労力がかかるとし、**<u>リスク軽減のベストプラクティスを提示</u>**している。

潜在的に影響を受ける可能性があるデバイスの種類と、
デバイスが用いられている業界
（Forescout社が自社データベース等の情報から算出）



影響範囲

以下のTCP/IPスタックを使用しているデバイス
- uIP、Contiki OS、Contiki-NG
- Nut/Net
- FNET
- picoTCP、picoTCP-NG

リスク軽減のベストプラクティス

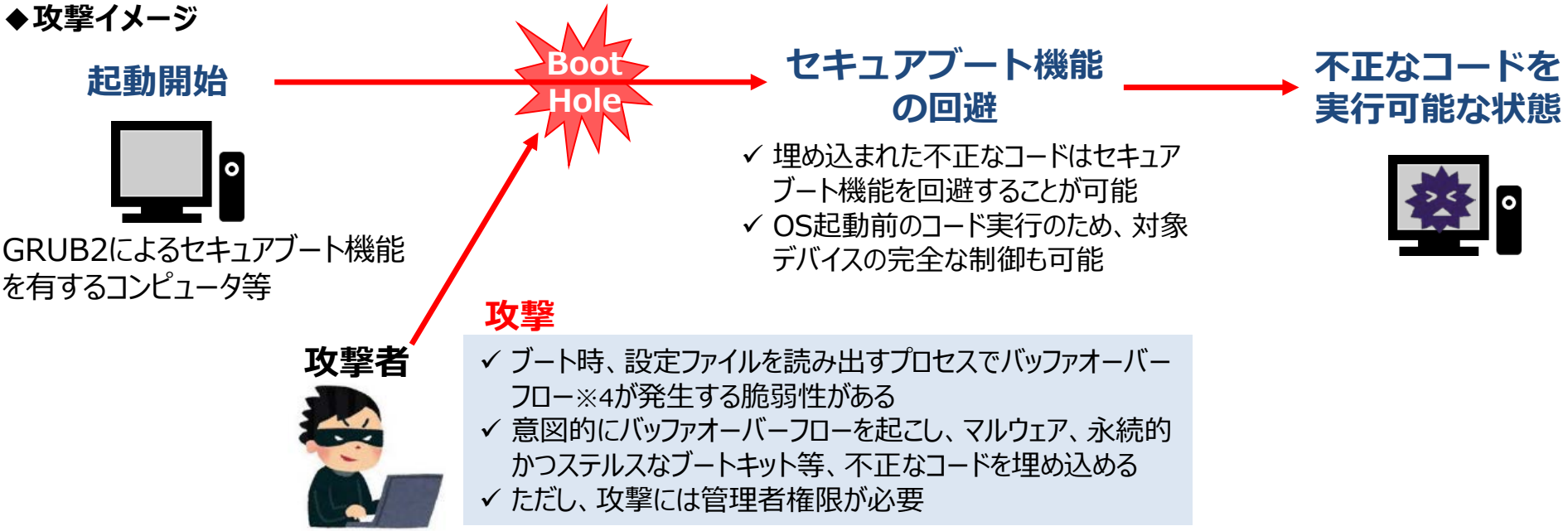
- リスクとexposure（露出）の洗い出し
- 内部DNSサーバへの依存
- IPv6トラフィックの無効化かブロック
- ネットワークのセグメンテーション
- 可能な場合はパッチ適用
- 不正なパケットの監視

https://www.forescout.com/research-labs/amnesia33/

GRUB2ブートローダーの脆弱性：“BootHole“

- 2020年7月、Eclypsium社※1は、Linux等で用いられるブートローダー※2**「GRUB2」の脆弱性**（BootHoleと命名）を報告した。OSが起動する前段階において不正なプログラム実行を防ぐ**「セキュアブート機能」※3を回避**できることが確認されている。この脆弱性の悪用により、対象のデバイスが**完全に制御される可能性**がある。
- Red Hatなどの主要Linuxディストリビュータ等は、この問題に関するセキュリティ情報を公開し、対応を表明している。

◆攻撃イメージ



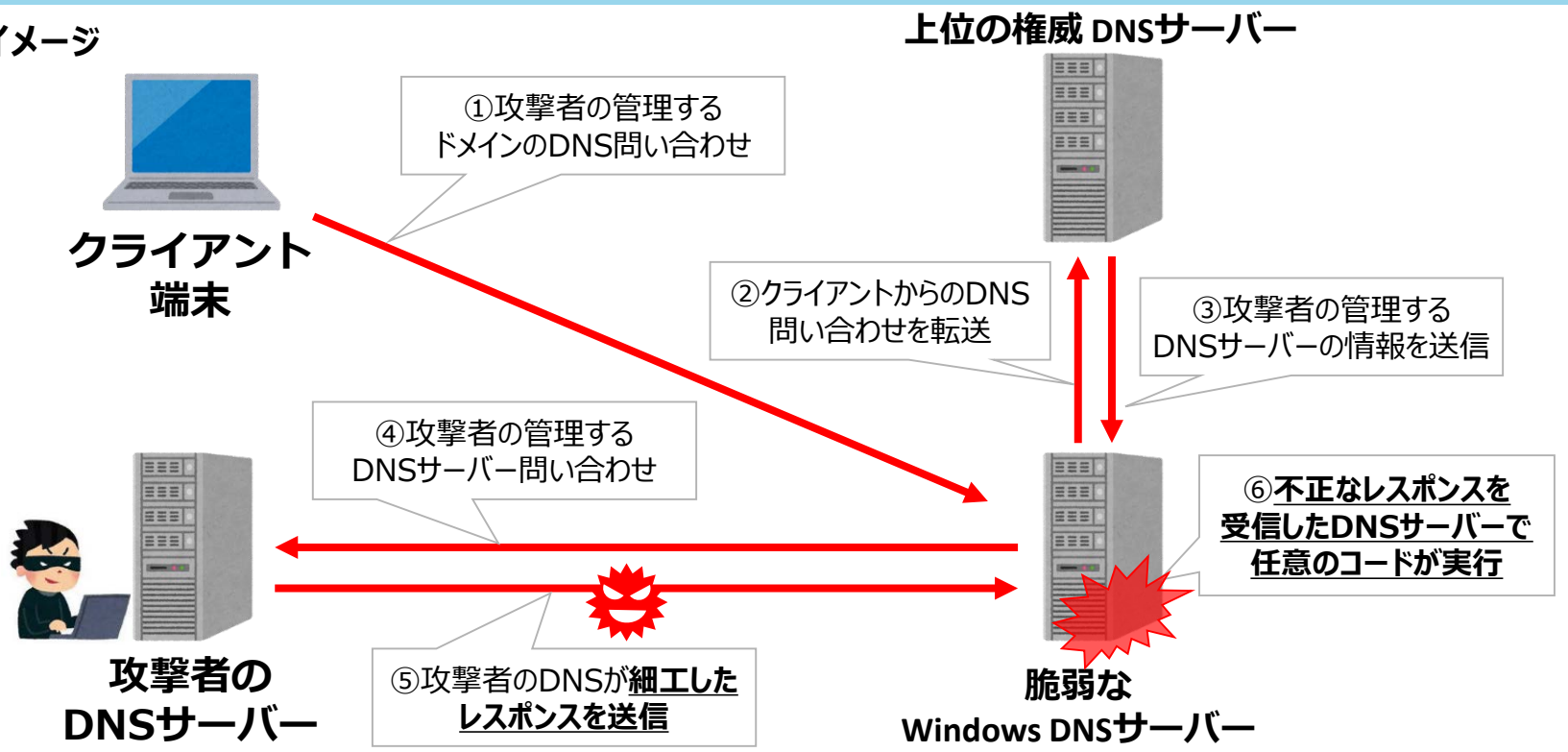
※1 企業向けファームウェア/ハードウェア分野における米国のセキュリティ企業
※2 コンピュータの起動直後に自動的に実行されるコンピュータプログラム
※3 OS起動前に実行されるプログラムの署名を確認することでデバイスを保護する機能
※4 データの一時記憶領域に想定以上の長さのデータが入力されてしまう現象

https://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/

Windows DNSサーバーの脆弱性：“SIGRed”

- 2020年7月、イスラエルのセキュリティ企業によって、**Windows DNS Serverの脆弱性「SIGRed」が発表**された。攻撃者が不正なDNSレスポンスを送信することで、DNSサーバー上で**任意のコードが実行される**可能性があり、Microsoft社は早急にパッチを適用するよう推奨している。
- 本脆弱性は17年前から存在するとされ、Windows Server 2003等、サポート終了済製品にも影響する可能性がある。

◆攻撃イメージ



https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/
https://www.secure-sketch.com/blog/cve-2020-1350-sigred

Netlogonの特権昇格の脆弱性：“Zerologon”

- 2020年9月、オランダのセキュリティ企業によって、**Netlogon※の特権昇格の脆弱性「Zerologon」**の詳細が発表された。この脆弱性を悪用して**ドメインコントローラーを攻撃された場合、ドメイン管理者の権限が奪取され、ドメインに参加する全ての端末が制御下に置かれるおそれ**がある。
- 悪用のためのコードも公開されており、米政府やMicrosoft社では、**本脆弱性を悪用した攻撃が実際に行われていることを確認、パッチの適用を呼び掛け**ている。

※ WindowsのActive Directoryのユーザ認証に使われるプロトコル

◆攻撃イメージ

攻撃者

ドメインコントローラへTCP接続が可能な環境であれば、認証情報がなくとも攻撃可能
（内部ネットワークに侵入した攻撃者、悪意のある内部関係者、オンプレミスのネットワークポートにデバイスを接続した人等）

Client Challenge
=000…00

Client Credential
=000…00

…

NetrServerPasswordSet2
enc.password = 0000…00

ドメインコントローラー

ChallengeとCredentialの
復号結果が一致するまで繰り返し

パスワードの長さをゼロバイトとし、
空のパスワードを設定可能

Windowsに限らず、Netlogonプロトコルを実装するSambaをドメインコントローラーとして使用している場合等にも影響

Netlogonの認証プロセスにおける暗号化アルゴリズムの不具合（初期化ベクトルが**すべて「0」**）により、1/256の確率でChallengeとCredentialの復号結果がすべて「0」で一致。
コンピューターアカウントは認証回数に制限がないため、試行を繰り返すことで**3秒程度で認証に成功**。

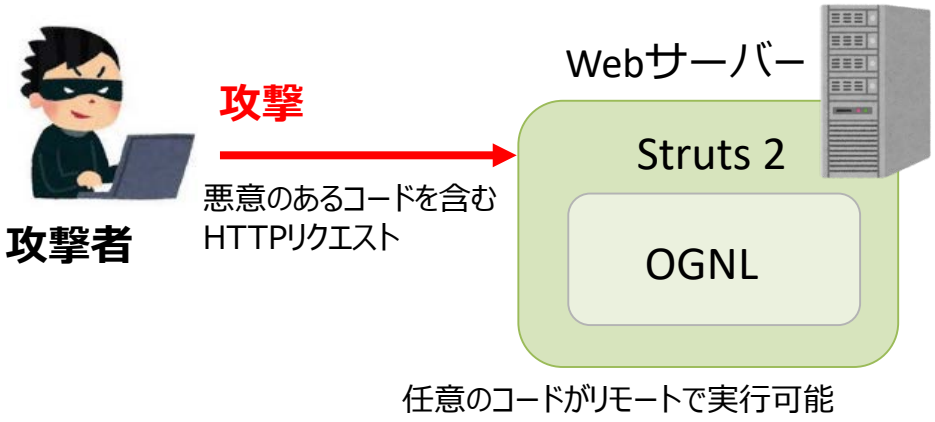
https://www.secura.com/blog/zero-logon

Apache Struts 2の脆弱性

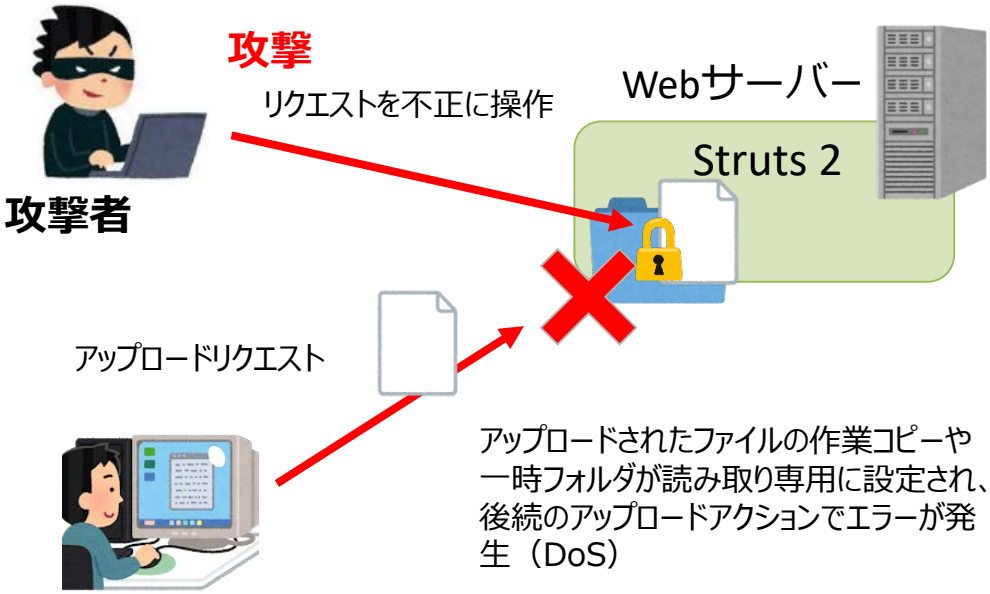
- Apache Software Foundation は、**2020年8月にWebアプリケーションフレームワーク Apache Struts 2 の2件の脆弱性に関する情報を公開**した。また、**12月にも類似の脆弱性を公開**し、修正済みバージョンへのアップデートを強く推奨している。
- 本脆弱性が悪用されると、Apache Struts 2 が動作するサーバーにおいて、**遠隔の第三者により任意のコードが実行**されたり、**サービス運用妨害(DoS)** の可能性がある。
- これまでも同様のOGNL※関連の脆弱性が度々見つかっており、多くのサイトで情報漏洩の被害が発生。

※Object Graph Navigation Language：Javaに似たコードをコンパイルなしで実行するライブラリ。Struts 2において多用されている。

◆攻撃イメージ（CVE-2019-0230、CVE-2020-17530）



◆攻撃イメージ（CVE-2019-0233）

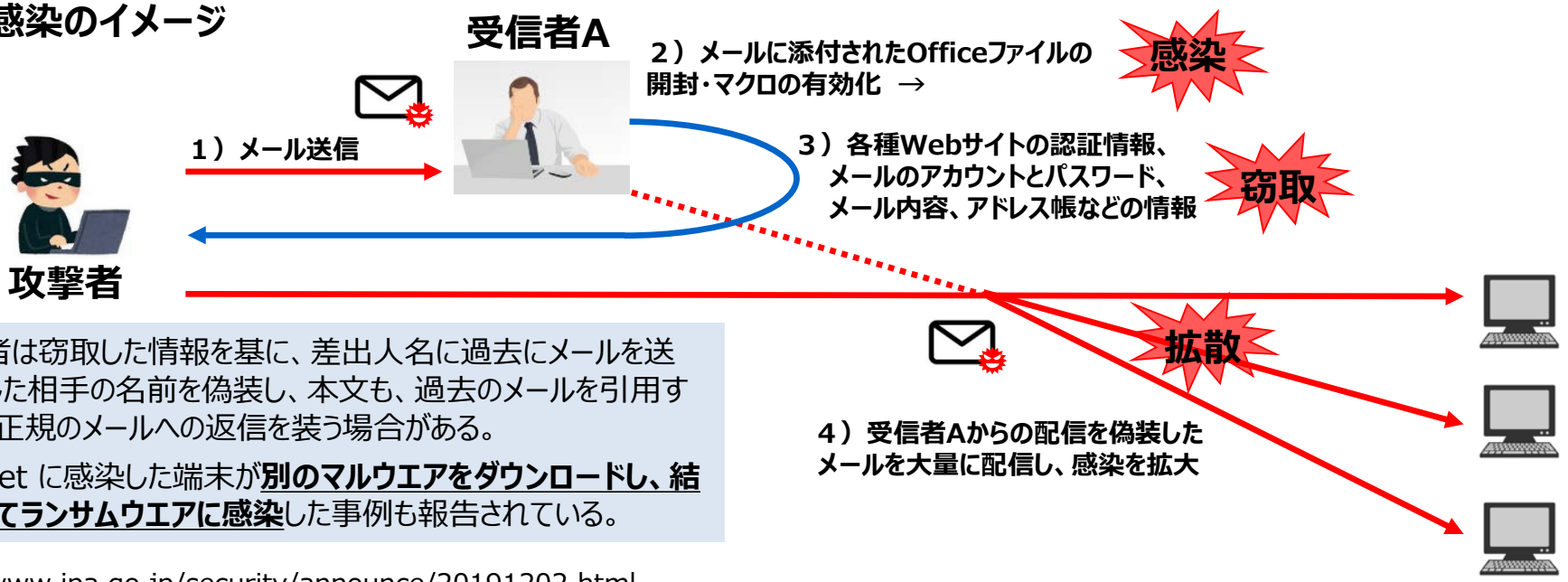


https://struts.apache.org/announce#a20200813

ウイルスへの感染を狙う攻撃メール：“Emotet”

- Emotetは、情報の窃取や、他のマルウェアへの感染のため悪用されるマルウェアであり、国内でも2019年10月に複数企業が感染を公表するなど事例が相次いでいた。2020年2月以降、Emotetへの感染を狙った攻撃メールは観測されていなかったが、**7月頃から攻撃活動再開が確認され、IPAやJPCERT/CCが注意喚起を行っている**。
- また、新たな攻撃手法として、**Emotetが正規のメールから添付ファイルを窃取してEmotetへの感染を引き起こすOfficeファイルとともに送付する事例**や、メール配信経路のセキュリティ製品による検知や検疫からのすり抜けを狙って**パスワード付きZIPファイルが添付される事例**が確認されている。

攻撃・感染のイメージ



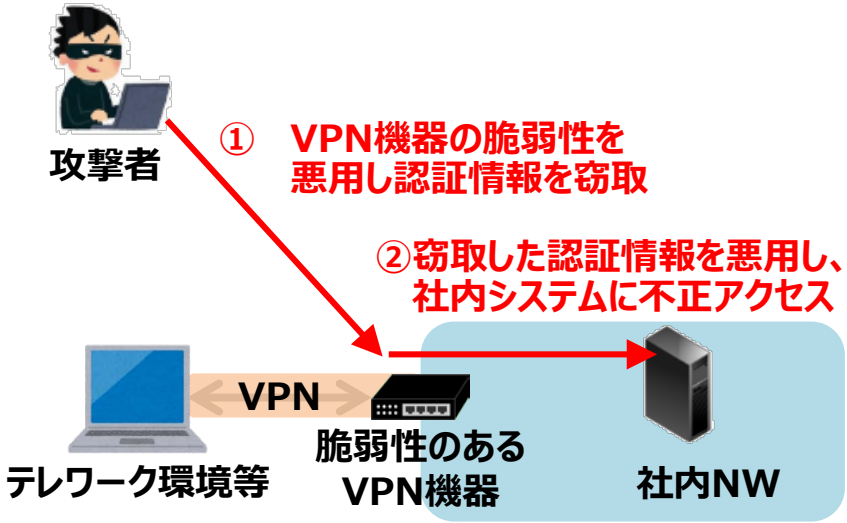
- ✓ 攻撃者は窃取した情報を基に、差出人名に過去にメールを送受信した相手の名前を偽装し、本文も、過去のメールを引用する等、正規のメールへの返信を装う場合がある。
- ✓ Emotet に感染した端末が**別のマルウエアをダウンロードし、結果としてランサムウエアに感染**した事例も報告されている。

https://www.ipa.go.jp/security/announce/20191202.html
https://www.jpcert.or.jp/newsflash/2020072001.html

VPN機器の認証情報流出

- **VPN機器の脆弱性**が相次いで報告され、そうした脆弱性を**悪用するコードが公開**されるなど深刻な状況が発生。**攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入**し、攻撃を展開。
- 2020年8月、Pulse Secure製VPN機器の脆弱性が悪用され、**国内外900以上の事業者からVPNの認証情報が流出**。2020年11月、Fortinet製品の**VPN機能の脆弱性の影響を受ける約5万台の機器に関する情報が公開**。**認証情報等が悪用されることで容易に侵入されるおそれ**。
- **どちらのケースも既に悪用されている可能性**があるため、**機器のアップデートや多要素認証の導入といった事前対策**に加え、事後的措置として**侵害有無の確認や、パスワード変更等の対応**が必要。

VPN機器に対する不正アクセス



Pulse Secure製VPN機器の脆弱性

2019年4月	脆弱性情報公開
2019年8月	脆弱性の悪用を狙ったとみられるスキャンを確認
2019年9月	脆弱性を悪用したとみられる攻撃を確認
2020年8月	国内外900社（国内は38社）の認証情報が公開

Fortinet製FortiOSの脆弱性

2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等

https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.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. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

（１）OSS管理手法に関する事例集の作成

（２）国内でのSBOM活用促進に向けて

【米国】NTIA Software Component Transparency

- 2018年7月、米国NTIA（電気通信情報局）は「Software Component Transparency」に関するMultistakeholder Meetingを設置。4つのグループを中心に、SBOM（Software Bill of Materials）の活用に関して議論を重ねている。
- SBOMの活用における様々な課題に関するドラフト文書を作成中。

NTIA Software Component Transparency における4つのグループと最新のドラフト文書

■ **Framing Working Group**
SBOM仕様の定義と改善に関する未解決の課題に重点を置く

■ **Awareness and Adoption Group**
認知と導入、さらには導入を促進するSBOMのビジネスプロセスに重点を置く

■ **Formats & Tooling Group**
SBOM作成と利用の自動化に重点を置き、表記形式間のトランスレータ開発や、ギャップ分析を目指す

■ **Healthcare Proof of Concept (PoC) Group**
医療機器分野でのPoCを継続し、コミュニティを支援するデモとPoCのためのアドバイザーとして機能する

→

Sharing and Exchanging SBOMs v0.2
SBOMの提供者と利用者の負担を最小化するためのSBOMデータの共有方法に関するいくつかのオプションを提示

Software Identification Challenge and Guidance v0.2
ソフトウェアコンポーネントを国際的に一意に識別するための課題（名前の問題）への対処方法を検討

Requirements for Sharing of Vulnerability Status Information ("VEX") v0.1
SBOMにより存在が明らかになる脆弱性について、そのexploitabilityを評価する仕組みの検討

Playbook for SBOM Consumers
ソフトウェア利用者がSBOMを取得、管理、活用するためのワークフローについて解説

Healthcare Delivery Organization (HDO) SBOM PoC 2.0 Quick Start Guide v1.2
SBOM PoCに関する情報、経験、ベストプラクティスを業種を問わず関心のある関係者に提供

https://www.ntia.doc.gov/SoftwareTransparency

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

- NISTは、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（2020年4月に最終版を公開）。
- 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けるセキュリティ要件への合致とリスク低減	
脆弱性対応	Respond to Vulnerabilities（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 • 脆弱性の評価・優先付け・修正	

【米国】NIST SP 800-53 Rev. 5/SP 800-53B

- 2020年9月、NISTは、情報システム・組織向けのセキュリティ・プライバシー管理策カタログであるSP 800-53の第5版を公開。2020年10月には、同文書の関連文書として、管理策を参照しセキュリティ影響度別にベースラインを提示するSP 800-53Bを公開している。
- 第4版からは、サプライチェーンリスク管理(SCRM)に関する管理策ファミリの新設、最新のセキュリティ関連動向を反映した管理策等の追加等の改定が行われている。

SP 800-53 Rev. 5 及び関連文書の策定状況

SP 800-53 Rev. 5 2020年9月公開
情報システム・組織に対するセキュリティ・プライバシー管理策

- 脅威とリスクから組織のオペレーションや資産、個人、関係組織等を保護するために情報システム・組織が実装すべきセキュリティ・プライバシー管理策のカタログを提供する。

SP 800-53A 2014年11月公開
連邦政府情報システム・組織におけるセキュリティ・プライバシー管理策の評価

- 連邦政府のシステム・組織内で採用されるセキュリティ/プライバシー管理策の評価を実施する一連の手順を示す

SP 800-53B 2020年10月公開
情報システム・組織に対するベースライン管理策

- 連邦政府機関向けにセキュリティ管理策(影響度低/中/高の3段階に分けて実施)とプライバシー管理策(Personally Identifiable Information (PII)を処理する場合、影響度にかかわらず実施)のベースラインを提示する

SP 800-53 Rev. 5 における主な改訂ポイント

1	成果ベースの管理策策定	管理策を実装するエンティティ(組織、システム)に関する記述を削除
2	管理策カタログの統合	セキュリティ管理策とプライバシー管理策を統合された管理カタログに統合
3	SCRMの統合	サプライチェーンリスク管理(SCRM)の管理策ファミリを新設
4	管理策選択プロセスを管理策から分離	管理策のベースラインや選択プロセスに関する記述を削除して全体をスリム化し、新たな文書としてSP 800-53Bを策定。今後、SP 800-37(リスク管理フレームワーク)等の関連文書も合わせてメンテナンスされる予定。
5	管理策ベースラインを別文書に移転	
6	最新の管理策を追加	最新の脅威インテリジェンスや攻撃データに基づき管理策を新設 (例：サイバーレジリエンス、セキュアなシステム設計、セキュリティ・プライバシーガバナンス、説明責任をサポートする管理策)

アプリケーションに最も利用されているFOSSコンポーネントに関する調査

- Linux Foundation のCore Infrastructure Initiative (CII) と、ハーバード大学イノベーションサイエンス研究所は、 Census II プロジェクトとして、現代のソフトウェアの8~9割を占めるとされるFOSS (Free and Open Source Software) について調査。
- 2020年2月、製品アプリケーションに最も一般的に利用されているFOSS コンポーネントを特定し、その潜在的な脆弱性について検討した予備的レポートを公表。

調査概要

- 依存関係の分析から、最も利用されているコンポーネントを調査。JavaScriptが圧倒的に多かったため、JavaScriptと、非JavaScriptのそれぞれについて、最も使用頻度の高い10のパッケージを抽出。
- FOSSの開発者について、個人事業主と特定されたのは15%程度であり、雇用者の率が高い。大手ベンダーの従業者であるケースも見られた。

調査によって得られた課題

1．ソフトウェアコンポーネントに標準化された命名規則の欠如
　　NISTの脆弱性管理や、NTIAのSBOMと同様の問題が、データセットを分析する際に顕在化。

2．個人の開発アカウントのセキュリティの重要性の増大
　　多くのプログラムが開発者の個人アカウントに存在。Copayの事例では、悪意ある者が正当な管理権限を委譲されてバックドアを仕掛けたが、アカウントへの侵入や乗っ取りの危険性もある。Left-padの事例では、パッケージの名前争いを発端として開発者がコードをレポジトリから削除したことにより、当該コードに依存していた多くのパッケージが機能しなくなった。

3．OSSにおけるレガシーソフトウェアの永続性
　　基本的に同じ機能を有する新しいパッケージが存在するにもかかわらず、古いパッケージの方が利用率が高いケースがある。互換性のバグへの懸念や、改修にかかる時間やコストの制約から、新しいソフトウェアへの切り替えが進みにくいことが原因。古いパッケージの開発者は時間と共に減少するため、FOSSのレガシー問題についても認識する必要がある。

https://www.coreinfrastructure.org/programs/census-program-ii/

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. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

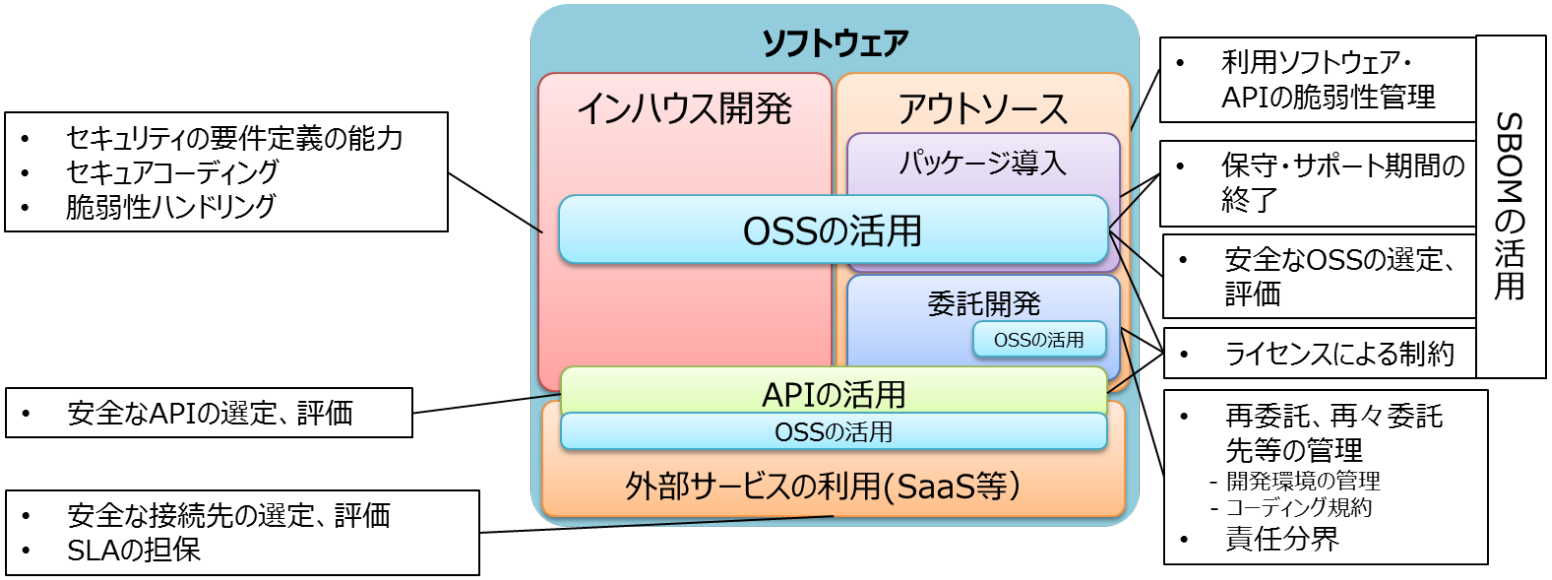
（１）OSS管理手法に関する事例集の作成

（２）国内でのSBOM活用促進に向けて

本タスクフォースの検討の方向性

- 仮想化技術の進展などにより、**OSSを含むソフトウェア技術への依存が高まる中**で、**ソフトウェアの管理手法、脆弱性対応やライセンス対応等の重要性が増している**。
- 2018年、**米国NTIA（電気通信情報局）は、「Software Component Transparency」を設立**し、ソフト部品構成表である**SBOM (Software Bill of Material）の活用に関する議論**を推進。
- 本タスクフォースでは、**適切なソフトウェア（特にOSS）の管理手法、脆弱性対応やライセンス対応等を検討**。

ソフトウェアを利用する際に考慮すべき観点



本タスクフォースの検討の方向性

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

第1回　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

第2回　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

第3回　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

OSS管理手法に関する事例集の作成

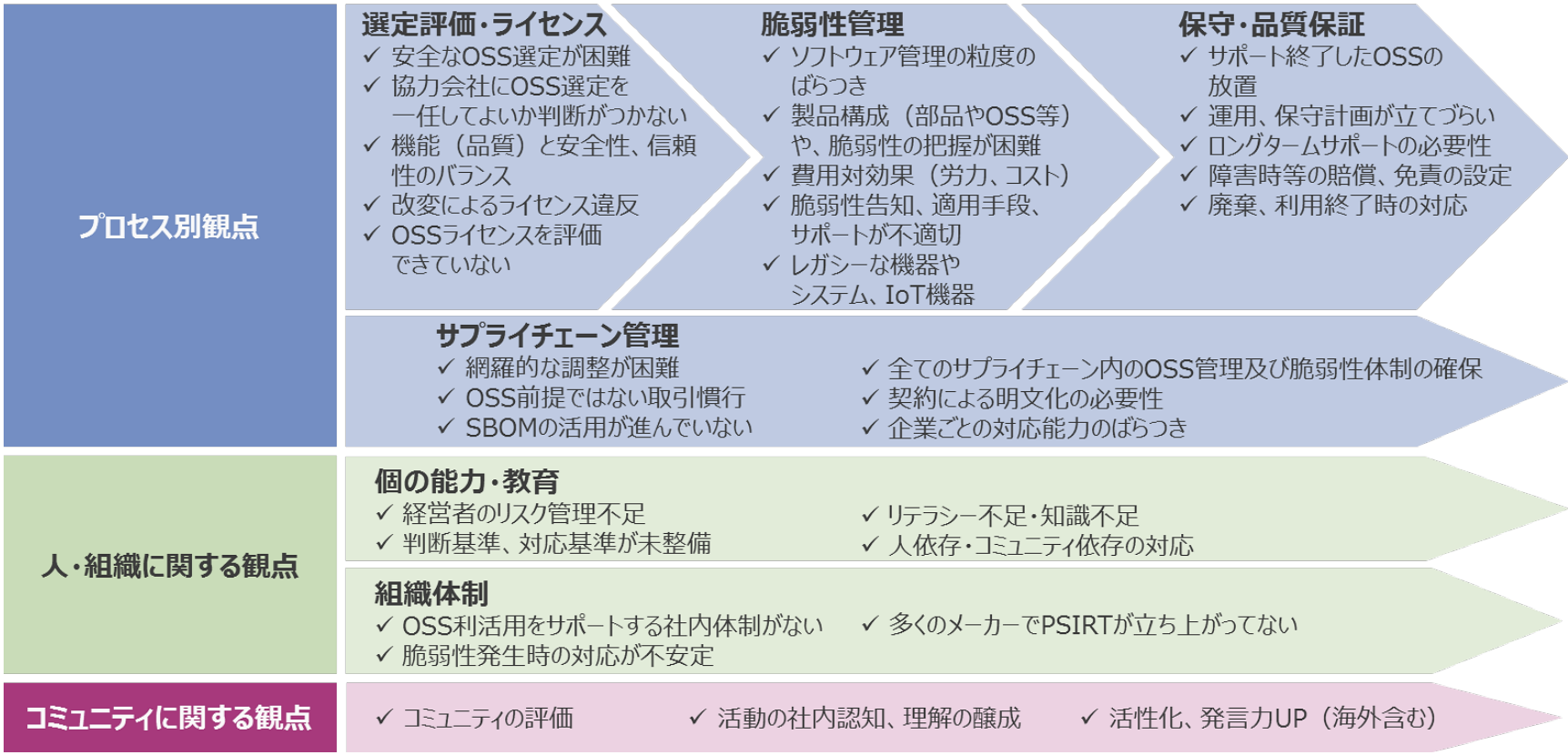
- 3回のタスクフォースでの議論を経て**「OSSの利活用及びセキュリティ確保に向けた管理手法」の事例集作成に着手。参考となる事例を共有し、企業における適切なOSS利用を促進**する。
- 担当者が自社のOSS管理等を検討する際の参考資料や、経営層への説明時の補足資料等として活用されることを想定。

章	タイトル	作成方針（案）
1	目的	• 本書を作成する目的を、これまでのTFにおける資料・議論を基に取りまとめる。 ✓ OSS利活用に関する課題の観点を整理し、その観点ごとに各種事例をとりまとめて公開することにより、「OSS利活用及びセキュリティ確保に向けた管理手法」の参考情報を提供する。 ✓ 事例を自社の取組みの参考にしてもらうことで、**OSSの留意点（ライセンス遵守、脆弱性対応等）を考慮した適切なOSS利用を促進**する。 ✓ また、**企業のOSS利用の障壁を取り除くことで更なるOSS利用を促し、OSSのメリットを享受し競争力向上につながることを期待**。 • 事例集が、OSS管理等検討時の参考資料、経営層への説明の補足資料等として活用されることを想定。
2	OSSの概要	• 読者の理解を助けるために、OSSの基礎的な情報を取りまとめる。 ✓ 「OSSとは何か」「OSS利活用の長所・短所（リスク）」「OSSライセンスの概要」「OSSコミュニティ活動の利点」「OSSに関する課題」「インシデント事例」等。 • 併せて政府・関係機関のこれまでの取り組みも紹介する。
3	整理方法	• 事例を紹介するにあたり、読者の理解を助けるために、本書で取り上げる事例の分類・整理を示す。 • 各事例の種類を一覧で示す。
4	事例	• 各社の事例を順次記載する。

事例集の作成状況

- 昨年度から今年度にかけ、本TF委員からの推薦や公開情報の調査等を踏まえ、**OSSの管理手法等で参考になる取組を実施している企業に対しヒアリングを実施**。
- **ITベンダ／サービス、金融、自動車／電機メーカー等の業種から10社以上にヒアリング**。

OSS利活用における留意事項の観点



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. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

（１）OSS管理手法に関する事例集の作成

（２）国内でのSBOM活用促進に向けて

国内でのSBOMの活用促進に向けて（実証事業（PoC）の実施）

- 米国NTIAが主導するSoftware Component Transparencyでは、ヘルスケア分野におけるPoC等を通じて、ベストプラクティス等を記した成果物が作成・公表されつつある。
- 他方、ソフトウェア分野における業界構造や商習慣が異なる日本においては、総論としてSBOMの有用性は理解されているものの、実際の活用促進に向けては、導入コストをはじめとして様々なハードルがある。
- 適切なSBOMの活用を推進するために、実証事業を実施してはどうか。また、その際どのような事項を検証する必要があるかご意見をいただきたい。

NTIAが公開したドラフト文書の概要（10月22日時点）

Requirements for Sharing of Vulnerability Status Information ("VEX") v0.1

SBOMによって明らかになる脆弱性が必ずしも悪用可能であるわけではないため、そのexploitabilityを評価する仕組みの検討等を示唆

Playbook for SBOM Consumers

SBOMを受領したソフトウェア利用者がそのSBOMをセキュアに管理するための観点（契約や知的財産等）、ソースコード納品の場合/バイナリ納品の場合それぞれのSBOMの完全性の検証、特にコンパイルやコンテナ実行時などに追加の依存関係が生じることへの注意など、実践的な内容を多く含む

HDO SBOM PoC 2.0 Quick Start Guide v1.2

ヘルスケア部門におけるPoCにおいて、活用した技術、SBOMに含まれる項目、SBOMの取込から脆弱性/リスク管理等、ユースケースに基づく情報を紹介

SBOMのPoCで示したい内容

（SBOMの導入にかかるコスト）＜（SBOM導入により削減できる脆弱性対応・ライセンス管理のコスト）

SBOMの活用促進に向けて検証すべき事項（仮説）

●適切なSBOMの活用レベル

・自社におけるSBOMの活用
・サプライチェーンにおけるSBOMの共有
・共有したSBOMの活用　etc.

低 → 高
・導入コスト
・コスト削減効果

●適切なSBOMの活用・共有の範囲

業界、サプライチェーン、個社　etc.

●SBOMの導入に適した分野

業界構造・商慣習等を踏まえる必要がある　etc.

●SBOM導入に向けた技術的検討が必要な観点

SBOM生成・共有・検証・管理手法
各コンポーネントの名称等、フォーマットの統一方法　etc.

●その他

実効性の担保方法（契約への盛り込み、ガイドライン等）