経済産業省

資料４

サイバーセキュリティに関連する海外の動き

令和３年３月

経済産業省　商務情報政策局

サイバーセキュリティ課

１．最近のインシデント事例

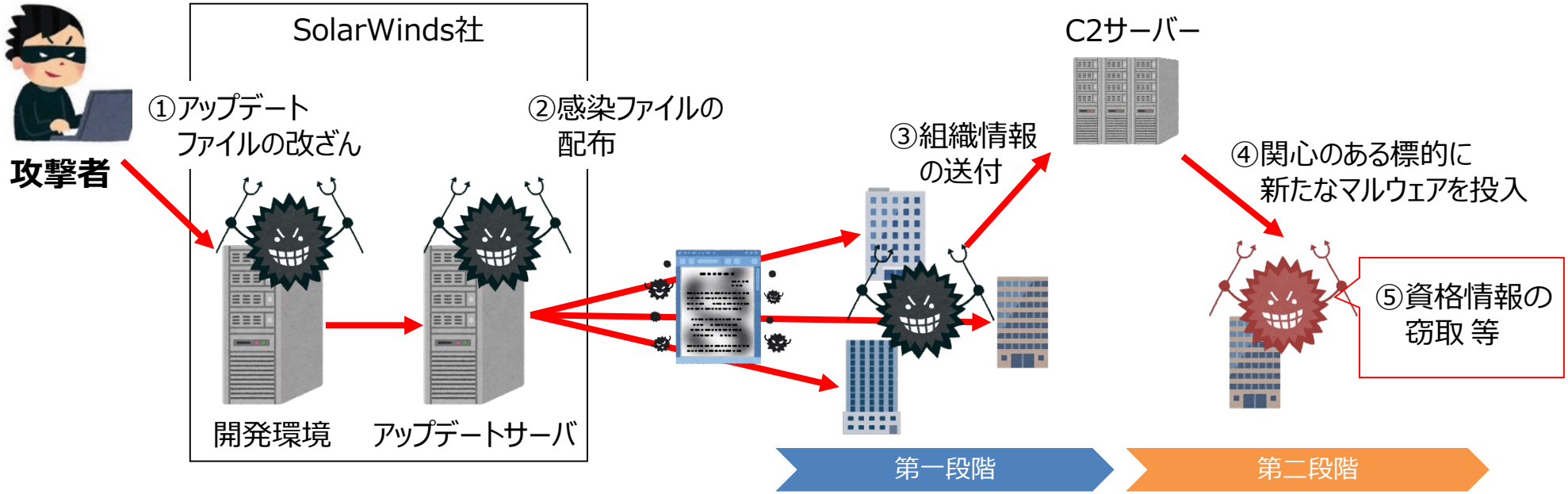
２．米国のサイバーセキュリティに関する取組

３．欧州のサイバーセキュリティに関する取組

SolarWinds Orion Platformのアップデートを悪用した攻撃

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、**正規のアップデートを通じてマルウェアが仕込まれた**ことを公表。
- 攻撃は2019年9月には始まっていたとみられ、2020年3月～6月のアップデートファイルが侵害されたことで、米政府機関等を含む**最大約18,000組織が影響**を受けたとされる。
- 初期段階のマルウェアは、セキュリティサービスの検知を回避しつつ被害組織の情報をC2サーバーへ送信。**攻撃者が関心のある標的に対しては第２段階のマルウェアが投入**され、資格情報を窃取した上で、**米国政府内、政府間のやり取りを傍受していた可能性が指摘されている。**

◆攻撃イメージ



（出典）各種公開情報に基づき経済産業省作成

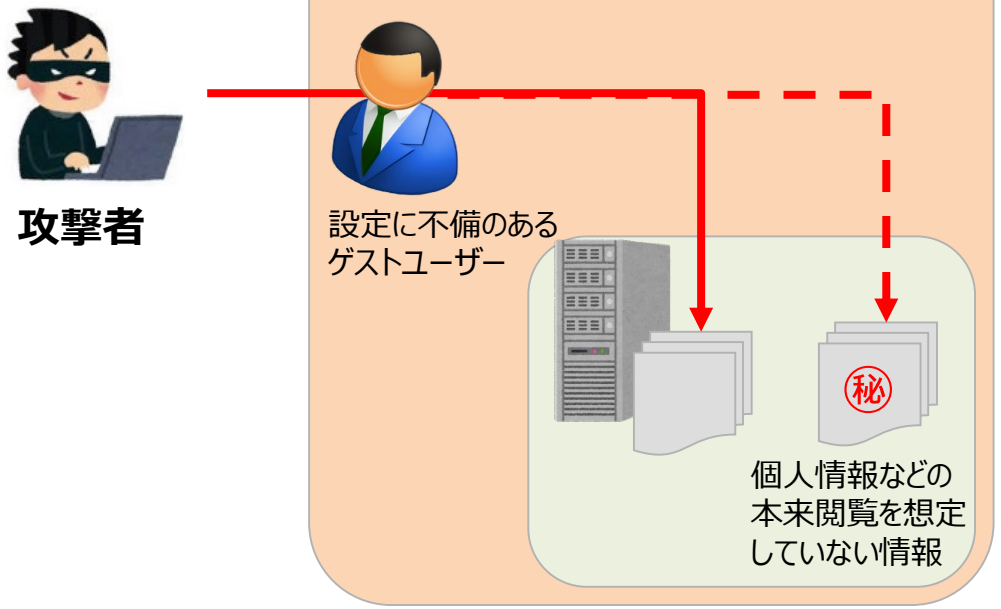
クラウドサービスの設定不備を原因とする不正アクセス

- 2020年12月25日、セールスフォース・ドットコムは、同社が提供するサービスにおける**ゲストユーザーに対する情報共有に関する設定が適切に行われていない場合、一部情報が第三者より閲覧できる**事象の発生を公表。また、**複数の国内事業者が本事象による不正アクセス及び個人情報漏えいの発生**を公表。
- 本サービスを組み込んだシステムがパッケージとして複数の顧客に提供され、同時に被害が発生したケースも。
- クラウドサービスを活用する際には、サービスの利用状況や各種設定の確認・見直しを行うなど、適切なセキュリティ対策を講ずることが重要。

◆不正アクセスがあったと公表した事業者等

- キャッシュレス決済サービス事業者
- サービス事業者
- クレジットカード事業者
- 小売事業者
- 玩具メーカー
- ガス事業者
- 地方自治体
- 独立行政法人　　他

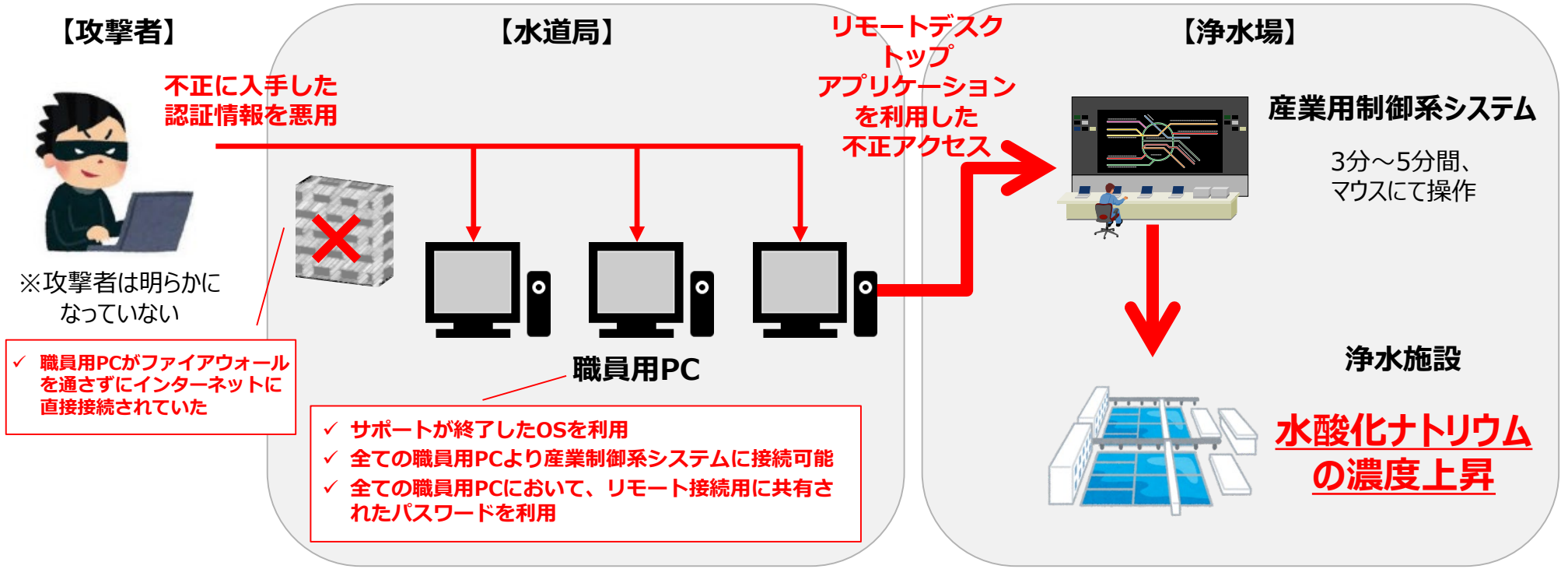
◆攻撃イメージ



（出典）各種公開情報に基づき経済産業省作成

水道システムへの不正アクセス事例

- 2021年2月、アメリカフロリダ州オールズマー市水道局は、**水道における産業用制御系システムを対象とした不正アクセス**によって、飲用水に含まれる水酸化ナトリウムの量が一時的に通常の約100倍に上昇したと発表した。なお、オペレーターが異常に気付き、即座に設定を戻したため、実際の被害はなかったとされる。
- 報道によると、**職員用PCよりリモートデスクトップアプリケーションを利用して、**産業用制御系システムへの不正アクセスが行われたとされている。

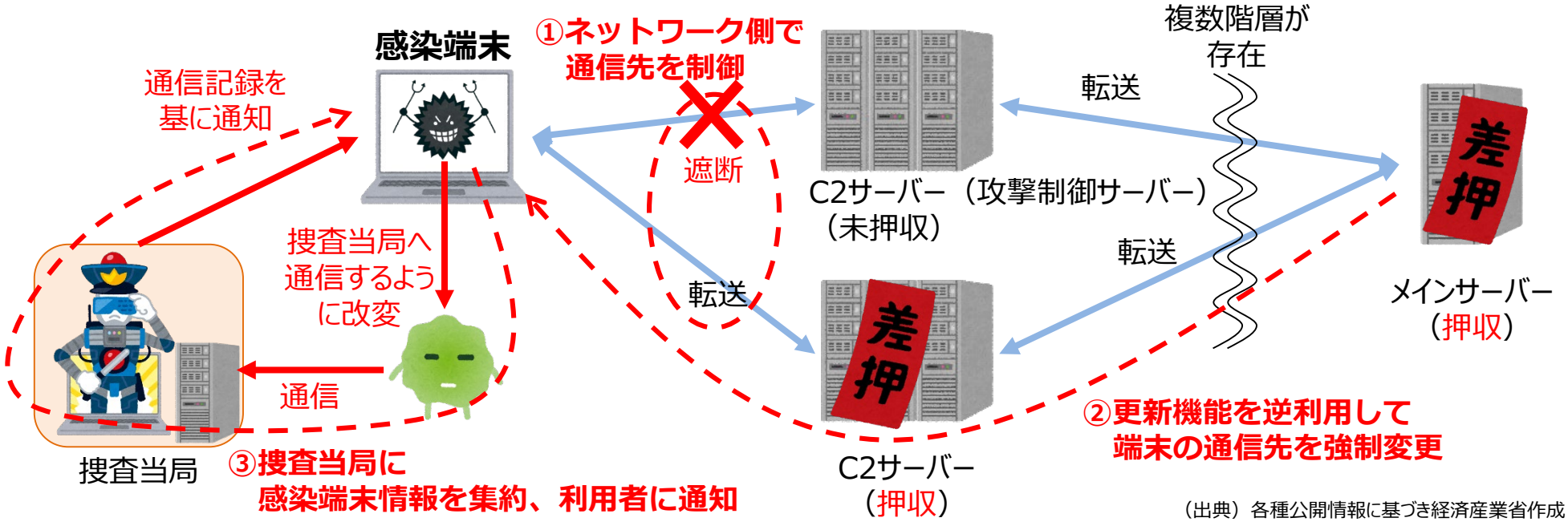


（出典）各種公開情報に基づき経済産業省作成

Emotet テイクダウン作戦（Operation Ladybird）

- 2021年1月27日、Europol（欧州刑事警察機構）は、世界的に猛威を奮ったマルウェア**「Emotet」の国際的なテイクダウン作戦**（サーバー等攻撃インフラの接収）が成功裏に実施されたと公表。
- 日本でも、海外の捜査当局からの情報提供に基づき、**インターネットサービスプロバイダからEmotetに感染している機器の利用者に対する注意喚起**を行うことを、総務省、警察庁、（一社）ICT-ISACの連名により2月19日に公表。
- 感染端末では、Emotet感染を原因とする認証情報の窃取・別のマルウェアへの二次感染が疑われるため、調査と対処が必要。

◆Emotet攻撃インフラとテイクダウン（赤字）のイメージ



（出典）各種公開情報に基づき経済産業省作成

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。

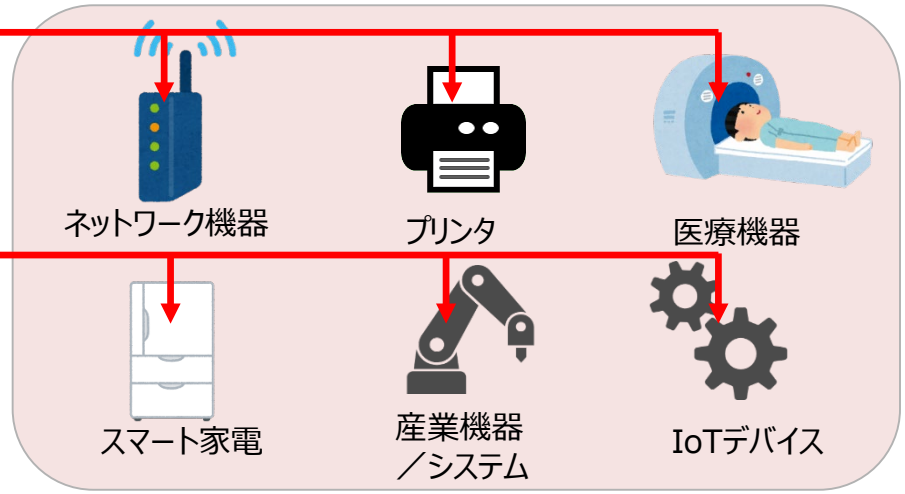
◆攻撃イメージ／影響範囲の例

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/

Treck TCP/IP Stackの採用製品は、下図以外にも多岐に渡る

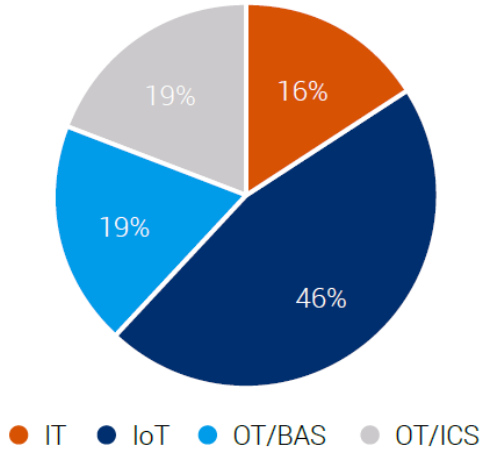


※1　組み込み機器向けのインターネットプロトコルスタックを設計・開発する米国の企業
※2　階層構造で構成されるインターネットプロトコル群

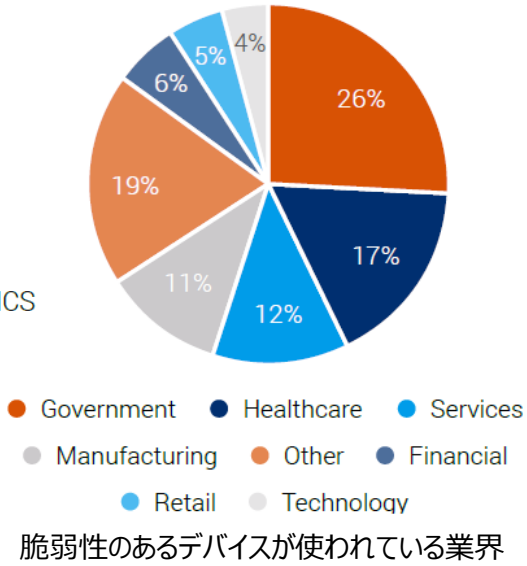
プロトコルスタックの脆弱性：“AMNESIA:33”

- 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）



脆弱性のあるデバイスの種類



脆弱性のあるデバイスが使われている業界

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

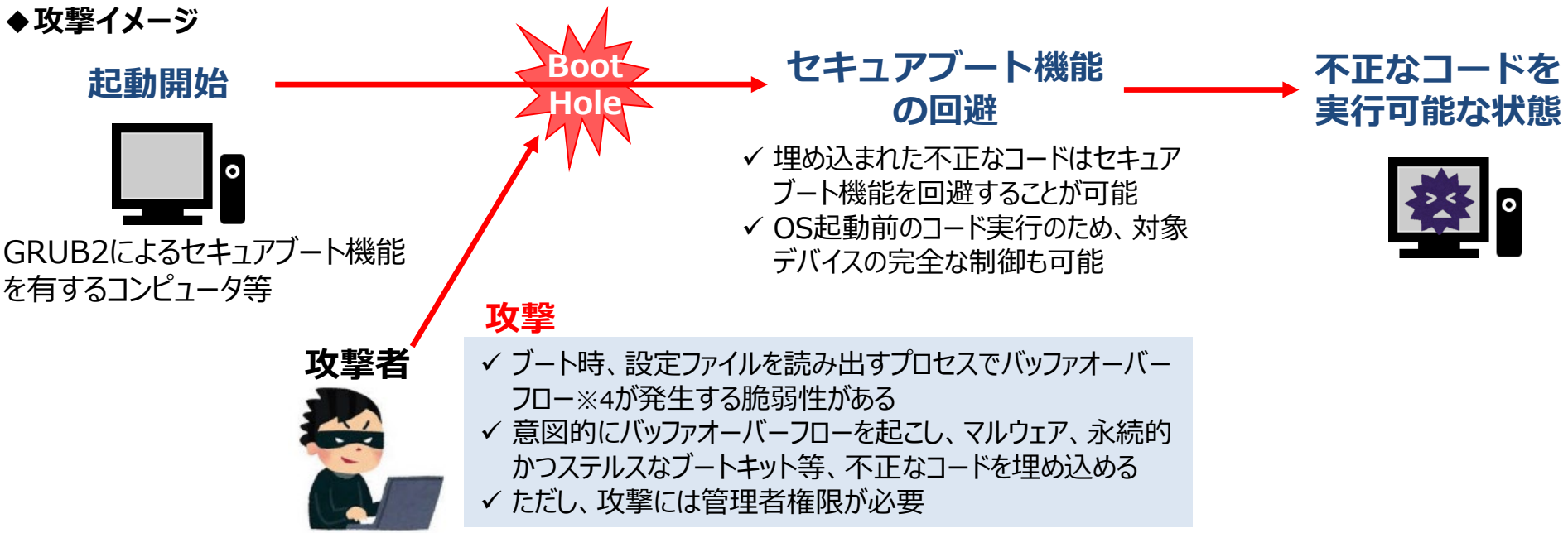
- リスクとexposure（露出）の洗い出し
- 内部DNSサーバへの依存
- IPv6トラフィックの無効化かブロック
- ネットワークのセグメンテーション
- 可能な場合はパッチ適用
- 不正なパケットの監視

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



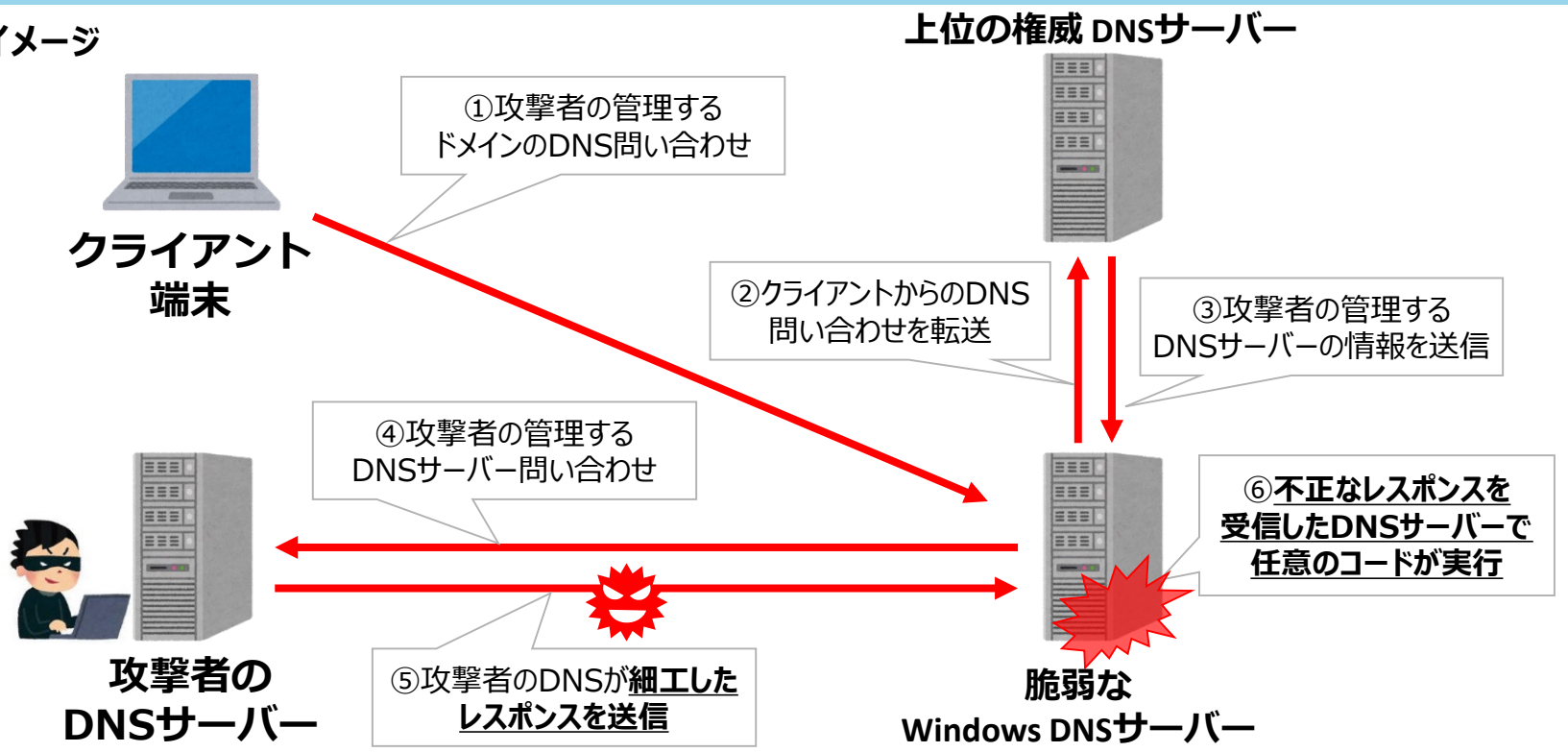
※1 企業向けファームウェア/ハードウェア分野における米国のセキュリティ企業
※2 コンピュータの起動直後に自動的に実行されるコンピュータプログラム
※3 OS起動前に実行されるプログラムの署名を確認することでデバイスを保護する機能
※4 データの一時記憶領域に想定以上の長さのデータが入力されてしまう現象

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



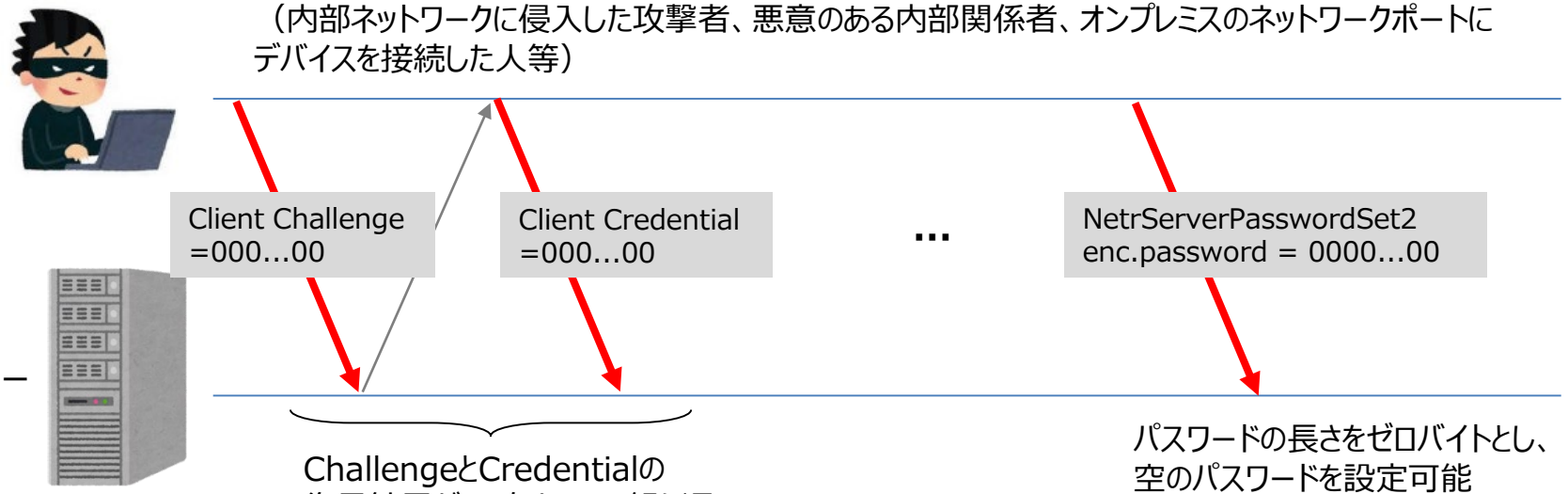
https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/
https://www.secure-sketch.com/blog/cve-2020-1350-sigred

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



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**。

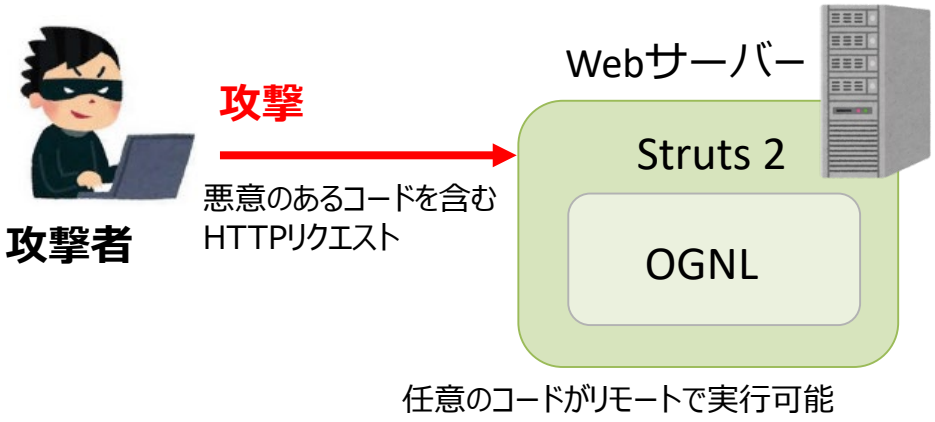
https://www.secura.com/blog/zero-logon

Apache Struts 2の脆弱性

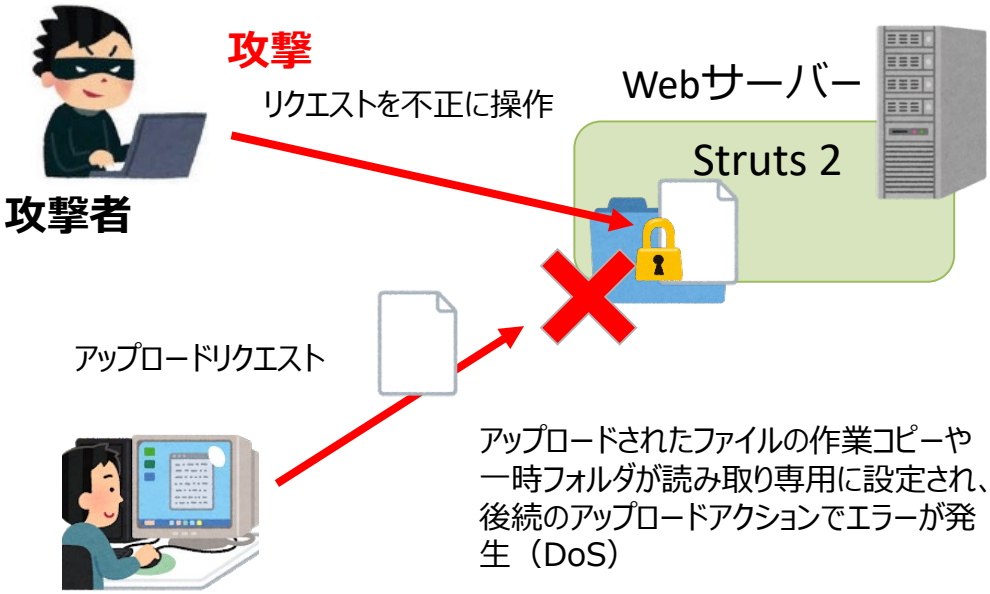
- Apache Software Foundation は、**2020年8月にWebアプリケーションフレームワーク Apache Struts 2 の2件の脆弱性に関する情報を公開**した。また、**12月にも類似の脆弱性を公開**し、修正済みバージョンへのアップデートを強く推奨している。
- 本脆弱性が悪用されると、Apache Struts 2 が動作するサーバーにおいて、**遠隔の第三者により任意のコードが実行**されたり、**サービス運用妨害(DoS)** の可能性がある。
- これまでも同様のOGNL※関連の脆弱性が度々見つかっており、多くのサイトで情報漏洩の被害が発生。

※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）

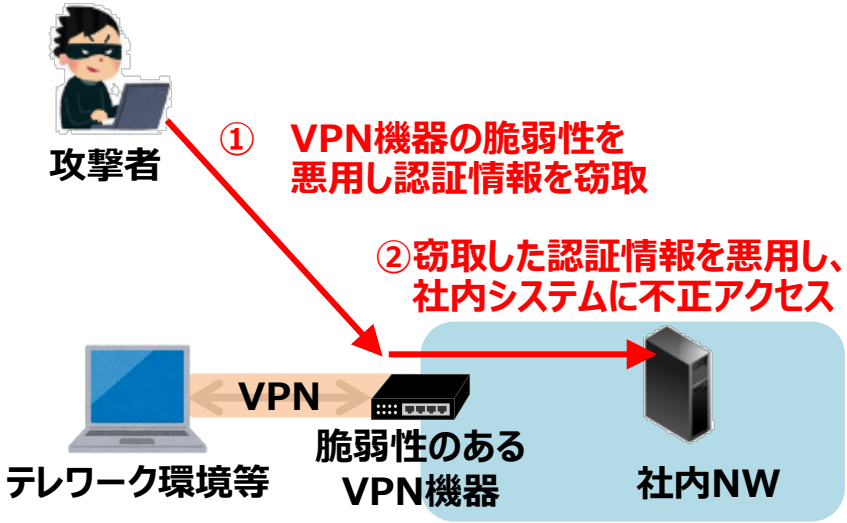


https://struts.apache.org/announce#a20200813

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

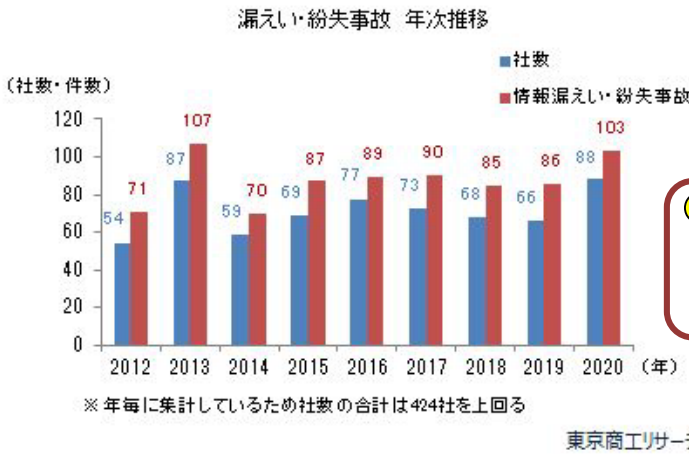
Fortinet製FortiOSの脆弱性

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

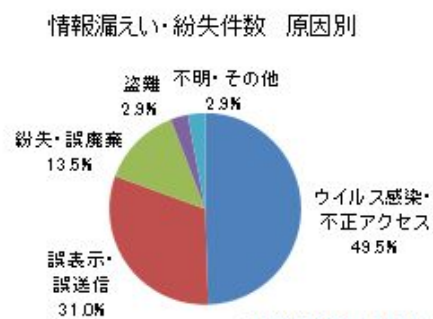
https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

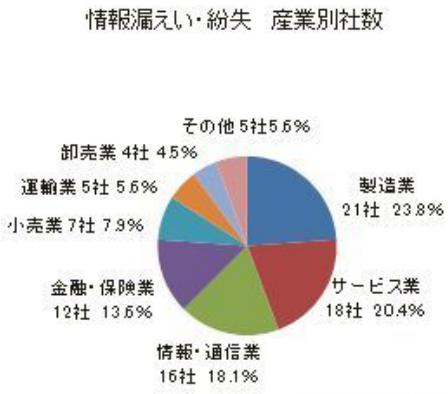
個人情報の流出事案

- 2020年の個人情報の流出事案は、公表社数、件数ともに増加傾向。2013年の107件に次いで2番目に多い水準で、7年ぶりに100件を上回った。
- 原因の約5割が、ウイルス感染・不正アクセスで、次いで誤表示・誤送信で約3割を占める。



2020年は88社103件、漏えいした個人情報は2,515万47人分





米国ホテルチェーンの事例（2020年4月）

攻撃者

不正アクセス

①フランチャイズホテルの従業員
ログイン情報を取得(※1)
②ホテルチェーンのシステムにアクセス

米国ホテルチェーン

・推定520万人の個人情報が流出。
・同ホテルチェーンは2018年にも3億8300万人分の個人情報流出により、欧州当局から約132億円の罰金が科された。
＜流出した情報＞
氏名、住所、メールアドレス、電話番号、ロイヤリティプログラムのアカウント詳細、部屋の好み等

※1:ログイン情報の取得経路は明らかになっていない。

国内スマホ決済サービスの事例（2020年12月）

攻撃者

不正アクセス

アクセス権限の設定不備を
突いて社員しか閲覧できないはずの
情報を閲覧

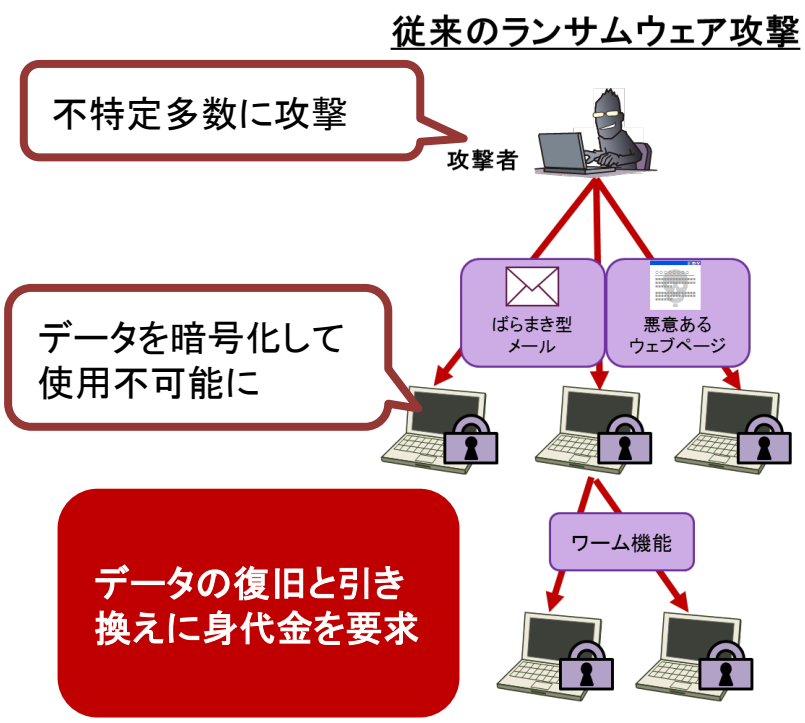
加盟店データベース管理サーバ

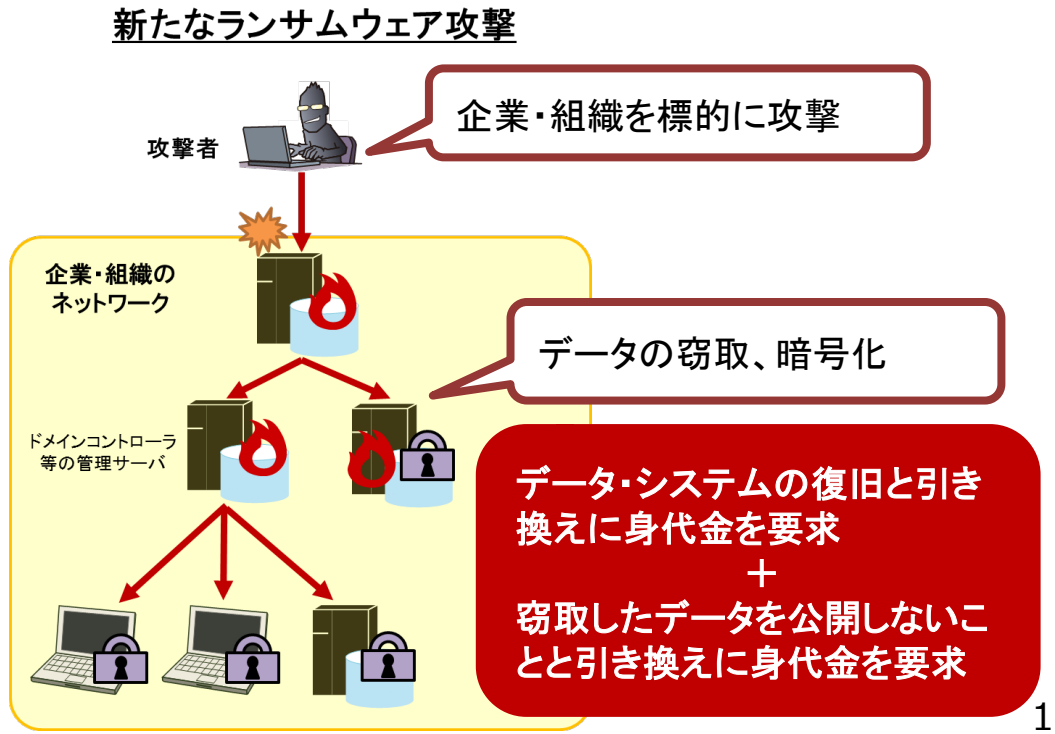
・260万店舗の加盟店などの営業情報が最大2007万件流出。
・発表時点でデータの不正利用は確認されていない。
＜流出した情報＞
加盟店の店名、住所、電話番号、代表者名、代表者生年月日、契約日、売り上げ振込先、営業対応履歴、加盟店営業先の店名、所属、役職、連絡先 等

https://www.tsr-net.co.jp/news/analysis/20210115_01.html
https://pc.watch.impress.co.jp/docs/news/1293581.html
https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident

ランサムウェアとその手口の変化（二重の脅迫）

- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可能にし、その**解除と引き換えに金銭を要求**する。
- **新たな（標的型）ランサムウェア攻撃（二重の脅迫）とは**
  - ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを窃取した後に一斉に暗号化してシステムを使用不可能にし、脅迫をするサイバー攻撃。
  - システムの**復旧に対する金銭要求**に加えて、窃取した**データを公開しない見返りの金銭要求**も行うので、**二重の脅迫**と恐れられる。窃取された情報に顧客の情報や機微情報を含む可能性がある場合には、被害組織はより困難な判断を迫られることになる。





１．最近のインシデント事例

２．米国のサイバーセキュリティに関する取組

３．欧州のサイバーセキュリティに関する取組

NISTIR 8259シリーズ

- IoT機器を管理する組織向けの推奨事項をまとめたNISTIR 8228に対し、**NISTIR 8259として、IoT機器の製造者に推奨される6つのサイバーセキュリティに関連する活動を整理**(2020年5月公開)。同時に公開された6つのコアサイバーセキュリティ機能を示したNISTIR 8259Aに続き、2020年12月にはNISTIR 8259B、8259C、8259Dのドラフト版が公開。

NIST IR 8259 (2020年5月公開)
(Foundational Cybersecurity Activities for IoT Device Manufacturers)

IoT機器の製造者に推奨される**6つのサイバーセキュリティに関連する活動**を定義。

NIST IR 8259A (2020年5月公開)
IoT Device Cybersecurity Capability Core Baseline

IoT機器が備えるべき**6つのコアサイバーセキュリティ機能**を定義。

NIST IR 8259B (Draft) (2020年12月ドラフト公開)
IoT Non-Technical Supporting Capability Core Baseline

製造業者が製造するIoT機器をサポートするために導入を検討すべき、**4つの非技術的サポート機能（※）**を定義。
※①ドキュメンテーション（情報収集）、②情報提供及び問合わせの受付、③情報発信、④教育及び意識醸成

NIST IR 8259C (Draft) (2020年12月ドラフト公開)
Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline

8259A及び8259Bを拡張し、**カスタマイズされたプロファイルを作成するためのプロセス**を提供。

NIST IR 8259D (Draft) (2020年12月ドラフト公開)
Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

8259Cに記載されているプロセスを用いて作成した**連邦政府向けプロファイル**を提供。

（参考）NISTIR 8259、8259A、8259B

- IoT機器の製造者に推奨される6つのサイバーセキュリティに関連する活動(NISTIR 8259)、6つのコアサイバーセキュリティ機能(8259A)、4つの非技術的サポート機能(8259B)を定義。

NISTIR 8259	販売前に影響する活動	活動1：想定顧客の特定、想定ユースケースの定義 活動2：顧客が有するサイバーセキュリティのニーズ及び目的の調査 活動3：顧客のニーズ及び目的への対処方法の決定（NISTIR 8259Aにてベースラインとなるコアサイバーセキュリティ機能を定義） 活動4：顧客のニーズ及び目的の適切なサポートに向けた計画（ハードウェア、ソフトウェアの適切なプロビジョニング、ビジネスリソースの考慮）
	販売後に影響する活動	活動5：顧客とのコミュニケーション手段の定義 活動6：顧客に伝える内容と伝達方法の決定（製造業者の設計・開発時のリスク関連の仮説、サポートと寿命、デバイス構成・機能、ソフトウェアの更新、デバイスの廃止オプション、技術的及び非技術的手段）

8259A	（１）**機器の識別**： IoT機器を論理的・物理的に一意に識別できる。	（４）**インターフェイスへの論理アクセス**： IoT機器のインターフェースへの論理アクセス、及びインターフェイスで利用されるプロトコルとサービスを正規のエンティティのみに制限できる。
	（２）**デバイスの構成**： IoT機器のソフトウェアの構成変更を、正規のエンティティのみが行うことができる。	（５）**ソフトウェアの更新**： IoT機器のソフトウェアは、安全かつ設定可能なメカニズムを用いる正規のエンティティにみによってのみ更新できる。
	（３）**データ保護**： IoT機器が保存・伝送するデータを不正アクセス及び改ざんから保護することができる。	（６）**サイバーセキュリティ状態認識**： IoT機器は自身のセキュリティに関する状態を報告し、その情報に対するアクセスを正規のエンティティのみに制限する。

8259B	（１）**ドキュメンテーション**： IoT機器の開発及びライフサイクル全体を通じて、IoT機器のサイバーセキュリティに関連する情報を作成、収集、保存する能力	（３）**情報発信**： IoT機器のサイバーセキュリティに関連する情報を発信する能力
	（２）**情報及び問合せの受付**： 顧客からのIoT機器のサイバーセキュリティに関連する情報や問合せを受け付ける能力	（４）**教育及び意識**： IoT機器のサイバーセキュリティに関連する情報や状況、機能等について、顧客の意識を創出し教育する能力

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	

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)

NTIA Software Component Transparency

- 米国NTIAが2018年から主導するSoftware Component Transparencyでは、実証事業（PoC）等を通じて、SBOMに関する成果物が作成・公表されつつある。
- **PoCについても**、ヘルスケア分野に続き、**自動車、電力分野での議論が開始**。

NTIA で作成中のドラフト文書例

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

NTIAにおけるSBOMのPoC

Healthcare SBOM Proof of Concept

病院、医療機器メーカー、ベンダーが参加。2回のPoCを経てSBOM活用の手法、課題等を公開。

Automotive Industry SBOM Project

Auto-ISACを中心としたサプライヤ中心のプロジェクト。12ヶ月ほどかけてサプライヤの推奨事項をとりまとめる予定。

Energy and Bulk Power community

1/26キックオフ。米国エネルギー省からもプレゼンターとして参加。

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

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/

カルフォルニア州消費者プライバシー法施行に関する動向（概要）

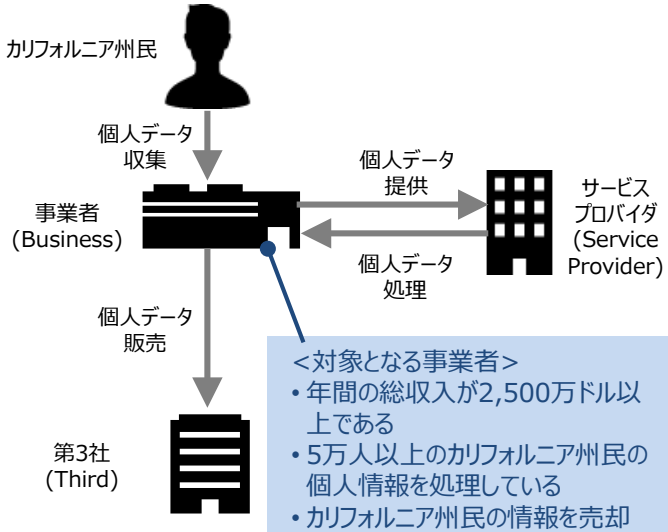
- 個人データに関する問題をきっかけに、米国カリフォルニア州にて2020年1月1日に「カリフォルニア州消費者プライバシー法」が施行された。
- 消費者データのプライバシー規制については、バーモント州（2018年12月施行）、ネバダ州（2019年10月施行）、メイン州（2020年7月施行）等でも制定されている。

背景

- **カリフォルニア州で通称「Shine the Light」法施行（2005年）**「Shine the Light」法とは、企業がマーケティングを目的として第三者と共有する個人情報の内容を請求する権利を、年1回に限りカリフォルニア州の居住者に付与するものである。
- **ケンブリッジ・アナリティカ問題（2018年）**2018年3月、Facebookから大量の個人データが流出したことが発覚した際、コンサルティング会社であるケンブリッジ・アナリティカ社がそれらを集め、2016年米大統領選などに使っていたことが明らかとなった。

動向の概要

- 2020年1月1日に、カルフォルニア州はプライバシー権及び消費者保護の強化を目的として、カリフォルニア州消費者プライバシー法を施行した。
- カリフォルニア州消費者プライバシー法では、一定の条件を満たしたカリフォルニア州民の個人情報を収集する事業者を対象としており、消費者に対して以下に示す5つの権利を認めた。



＜対象となる事業者＞
- 年間の総収入が2,500万ドル以上である
- 5万人以上のカリフォルニア州民の個人情報を処理している
- カリフォルニア州民の情報を売却することで年間の収入の50%を得ている

消費者の5つの権利

No	内容
1	企業が収集した個人情報のカテゴリー、情報源、情報の用途および収集した情報の開示先など、**企業のデータ収集の運用について開示請求する権利**
2	消費者による請求から過去12カ月の間にその消費者について収集した具体的な**個人情報のコピーを受け取る権利**
3	**本人の個人情報を削除してもらう権利**（ただし、例外有）
4	企業のデータ売却の運用について知り、その消費者の**個人情報を第三者に売却しないよう求める権利**（いわゆるオプトアウト）
5	消費者らがカリフォルニア州プライバシー法により付与された新たな権利を行使したことに基づいて**差別されない権利**

(出所) JETRO"施行が迫る「カリフォルニア州消費者プライバシー法」（米国）"（2019/6/6）等を参考に作成

カルフォルニア州消費者プライバシー法施行に関する動向（影響）

- カルフォルニア州消費者プライバシー法施行により、企業は個人情報取扱いに関する義務を負った。またこれらの義務を遵守できなかった場合のペナルティも定められており、企業は対応が必要となる。

事業者に課せられる義務

セキュリティ対策の実施
(第1798.150条)

- 個人情報を保護するための合理的なセキュリティ手順と慣行を実装する義務が事業者に課された。この義務について、事業者は身元の偽装や、個人情報への不正なアクセスまたは削除を防ぐ合理的なセキュリティ措置を実行しなければならないとされている。

開示請求等への対応
(第 1798.100 条,規則第 999.313 条)

- 企業として法令を順守するため主に以下の内容に対応する必要があるとされた。
  - ◆ 請求している消費者の本人確認をする手順を実施すること
  - ◆ 45日以内に情報開示するために社内で個人情報を特定・発見することができるようにすること
  - ◆ 特定の情報開示を電子的に行う方法を開発すること 等

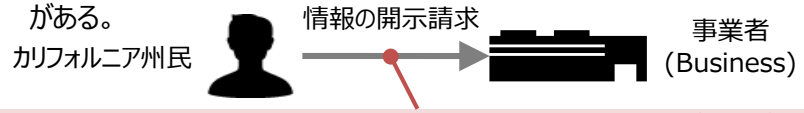
義務に違反した事業者へのペナルティ等

消費者により提起される民事訴訟
(第1798.150条)

- 暗号化されておらず、かつ修正されていない個人情報が、不正アクセス、流出、窃取又は開示の対象となった場合、当該消費者は、以下のいずれかについて民事訴訟を提起することができるとされた。
  - ◆ 違反1件について消費者一人当たりで100ドル以上750ドル以下の、又は実損害の、いずれか大きい額の損害を回収するため
  - ◆ 差止命令による救済又は宣言的救済
  - ◆ 裁判所が適切と判断するその他の救済

開示請求への対応不足による罰金
(第1798.155条)

- 消費者からの情報開示請求に対して1件あたり最大2,500ドルの罰金（故意だと認定される場合には最大7,500ドル）を科せられる可能性がある。



請求に対して45日以内に事業者は情報を開示する必要があるが、不遵守を通知されてから30日以内に対応がされていないと判断された場合、罰金が科される可能性がある。

＜日本企業への影響＞
今後、日本企業・組織が米国国内においてビジネスを行っていく上では、説明責任の一環として、例えば「**カルフォルニア州消費者プライバシー法の適用を受けるか否か**」、（受ける場合）「**どのようにカルフォルニア州消費者プライバシー法を遵守しているか**」、（受けない場合）「**なぜカルフォルニア州消費者プライバシー法の適用を受けないと判断をしたか**」について、説明できるように準備する必要がある。

(出所) JETRO "施行が迫る「カリフォルニア州消費者プライバシー法」（米国）"(2019/6/6)、"カリフォルニア州消費者プライバシー法(CCPA)実務ハンドブック"（2019/12/25）等を参考に作成

１．最近のインシデント事例

２．米国のサイバーセキュリティに関する取組

３．欧州のサイバーセキュリティに関する取組

欧州サイバーセキュリティ認証フレームワーク

- 「Cybersecurity Certification Framework」の創設を含む「Cybersecurity Act」は、2019年4月9日に欧州理事会で採択され、6月27日に発効。
- 「Cybersecurity Act」に基づき、ENISAが具体的な産業分野毎に「候補スキーム(Candidate Scheme)」を欧州委員会に提案し、順次、認証フレームワークが策定される予定。

欧州委員会、ENISAの動向

※更新部分に下線

- 2019年4月、規則（Regulation）として、「Cybersecurity Act」が欧州理事会で採択、6月27日に発効。
- 2020年2月、ENISAがIoT、クラウドインフラ及びクラウドサービス、電子医療記録、トラストサービス等の4分野について、欧州サイバーセキュリティ認証フレームワークの「候補スキーム(Candidate Scheme)」を提案するホワイトペーパーを公開。
- 2020年7月、ENISAが最初の候補スキームでありCommon Criteriaに基づく「EUCC Candidate Scheme」のドラフト版を公開。
- 2020年12月、ENISAがクラウドサービスに関する候補スキーム「EUCS – CLOUD SERVICE SCHEME」のドラフト版を公開。
- 2021年2月、欧州委員会がENISAに5Gネットワークのための認証スキームの立案を指示。

Cybersecurity Actの概要

- 欧州委員会は、欧州サイバーセキュリティ認証スキームの対象となるICT製品、サービス、プロセス、カテゴリのリストを含む「Union rolling work programme」を発行。最初の「Union rolling work programme」は2020年6月28日までに発行される（Article 47）。
- 本スキームでは、ICT製品等について、インシデントの可能性と影響の観点を考慮し、「basic」、「substantial」または「high」のいずれかの保証レベルを1つ以上特定する（Article 52）。
- ICT製品等の製造者又は提供者は、保証レベル「basic」に対応する低リスクを示すICT製品等について、本スキームに示されている要件の充足が実証されていることを示すEU適合宣言をボランタリーに発行することができる（Article 53）。
- 本スキームには、評価に適用される国際規格、欧州規格又は国内規格への参照及び第三国との認証制度の相互承認のための条件等が含まれる（Article 54）。
- 欧州委員会は、サイバーセキュリティ認証スキームが義務づけられることによって、ICT製品等の適切なレベルのサイバーセキュリティを確保し、国内市場の機能を改善することに効果があるか定期的にアセスメントを行う。最初のアセスメントは2023年末までに行われ、その後は少なくとも2年ごとに行われる（Article 56）

（参考）ENISA：Cybersecurity Certification - EUCC Candidate Scheme

- EUCC Candidate Schemeは、ICT製品を対象とするCommon Criteria（CC：ISO/IEC15408）と、関連する共通評価方法（ISO/IEC 18045）に基づく**欧州サイバーセキュリティ認証フレームワークにおける最初の候補スキーム**（2020年7月ドラフト版発行）。欧州においてSOG-IS※1の下で運用されていた**既存のCCのスキームの後継**として機能させることが目的。
- 本文書では、評価はCCに基づくものであること（3章）、保証レベルは「substantial」か「high」の2段階であること（4章）、自己適合性評価は認められないこと（5章）、認証証明書の有効期間は最長5年間であること（20章）等、**Cybersecurity Actにより候補スキームに必要とされる要件**（認証取得の際に実装すべき要求事項やその評価プロセス、認証制度の運用等に関する事項等）**を網羅的に規定**。

※1欧州におけるCC加盟国の認証機関間の調整を行う組織

本文書の目次と、関連するCybersecurity Act 54条1項の項目 a – v の対応*

章	目次	*
1	主題とスコープ	a
2	本スキームの目的	b
3	評価標準	c
4	保証レベル	d
5	自己適合性評価	e
6	認証機関向けの具体的な要求事項	f
7	認証機関の通知と認可	f
8	具体的な評価基準及び評価手法	g
9	認証に必要な情報	h

章	目次	*
10	マークとラベル	i
11	コンプライアンスを監視するための規則	j
12	認証証明書の発行、維持、継続および更新の条件	k
13	違反に関する規則	l
14	脆弱性管理に関する規則	m
15	パッチ管理	m
16	認証機関による記録の保持	n
17	国家的または国際的なスキーム	o
18	認証証明書の内容とフォーマット	p

章	目次	*
19	情報の可用性	q
20	認証証明書の有効期間	r
21	認証証明書の開示ポリシー	s
22	第三国との相互認証	t
23	ピア評価	u
24	補足的なサイバーセキュリティ情報—第55条	v
25	スキームの追加要素	a
26	アドホックWGからの推奨事項	-
27	参考	-

(参考) ENISA : EUCS - Cloud Services Scheme

- EUCS–Cloud Services Schemeは、 欧州クラウドサービスを対象にEUサイバーセキュリティ認証制度を構築することを目的として作成された認証スキームである(2020年12月ドラフト版発行)。
- 本文書にはクラウドサービスプロバイダーが認証取得するために満たすべき技術的要件及び目的等が定められており、個別の技術的要件ごとに、「Cybersecurity Act」によって定義された「high」、「substantial」、「basic」の3つの保証レベルが定められている。なお、本スキームはvoluntaryであるとしている。

認証取得するために満たすべき技術的要件(大項目)

No.	項目	No.	項目
1	情報セキュリティのための組織	11	ポータビリティ及び相互運用性
2	情報セキュリティポリシー	12	変更管理及び構成管理
3	リスクマネジメント	13	情報システムの開発
4	人的資源	14	調達管理
5	資産の管理	15	インシデント管理
6	物理的セキュリティ	16	事業継続
7	運用のセキュリティ	17	順守
8	ID、認証及びアクセス管理	18	ユーザードキュメント
9	暗号化及び鍵管理	19	政府機関からの調査依頼への対応
10	通信のセキュリティ	20	製品のセーフティ及びセキュリティ

３つの保証レベル

保証レベル	説明
high	**<対象> mission-criticalなデータ、システムを扱うサービス** <攻撃者プロファイル> 高度なスキルを持ったチーム <評価> substancialに加え、管理策の自動監視及び適切な要員によって実施される**複数年に渡り計画されるペンテストや技術的レビュー**
substantial	**<対象> business-criticalなデータ、システムを扱うサービス** <攻撃者プロファイル> 様々な既知のハッキング手法にアクセスできるが、リソースが限られている小さなチーム <評価> basicに加え、インタビューやサンプル検査、**設計どおり実装されているかの検証**を含むオンサイト監査、**既知の攻撃手法を使ったペンテスト**
basic	**<対象> 重要でないデータ、システムを扱うサービス** <攻撃者プロファイル> 限られたスキルのみを有し、限られたリソースにより既知の攻撃を繰り返す一人の人物 <評価> 事前定義された監査計画に沿った、技術的・組織的な措置(CSP自身による**自動化された既知の脆弱性やコンプライアンスに係る検査**を含む)の履行を確認するための**書類確認**

欧州NIS指令の改正

- 2020年12月、欧州委員会は、域内の重要インフラ事業者等のサイバーセキュリティ対策について規定するNIS指令(Directive (EU) 2016/1148)の改訂案を公表。
- 現行指令から、適用業種が大きく拡大しており、事業者に課すセキュリティ要件や罰則等においても規定が強化されている。

変更項目	現行NIS(2016年制定)の規定	主な改正事項
適用範囲	● **基幹サービス運営者** ①エネルギー(電力、石油、ガス)、②輸送、③銀行、④金融市場インフラ、⑤医療、⑥上水道、⑦デジタルインフラ ● **デジタルサービス提供者** ①オンラインマーケット、②オンライン検索エンジン、③クラウドコンピューティングサービス	● 基幹サービス運営者・デジタルサービス提供者という分類を、重大エンティティ(essential entity)と重要エンティティ(important entity)に変更。 ● 重大エンティティは、基幹サービス運営者７分野に**「下水道」、「行政」、「宇宙」の３分野を追加**した10分野 ● 重要エンティティには、デジタルサービス提供者以外に、「郵便・配送」、「廃棄物処理」、「化学品」、「食品」、**「製造(医療機器、コンピューター及び電気電子製品、電気設備、機械設備、自動車、その他の輸送機器)」が追加**
適用範囲の事業者に関連する規律	● 適用範囲の事業者が適切かつ均衡の取れた技術的及び組織的措置を講じる。 ● サービスの継続性に重大な影響を及ぼすインシデントの、管轄官庁又はCSIRTへの届出。	● 重点的な対策（サイバーセキュリティテスト、暗号化の利用等）をリストアップし、**セキュリティ要件を強化** ● **ICTサプライチェーンにおけるセキュリティへの対応を明記** ● インシデント報告に関して、**プロセス、内容、およびタイムラインに関するより正確な規定を設定**
罰則	● 罰則を設けることのみ規定	● **罰則の程度を指定**（1000万ユーロまたは全世界の年間売上高の2%を上限とする罰金）

EN 303 645 – Cyber Security for Consumer Internet of Things: Baseline Requirements(ETSI)

- 2018年10月に、英国で策定された「消費者向けIoT製品のセキュリティに関する行動規範」に基づく欧州標準。本文書は**消費者向けIoT製品のセキュリティベースラインを確立**し、**今後のIoT認証スキームの基礎を提供する**としている。（2020年6月に最終版を公開）
- 消費者向けIoT製品のセキュリティを確保するための開発・製造者向けガイダンスであり、消費者IoTのためのサイバーセキュリティ規定（1-13）及びデータ保護規定（14）を記載している。
- 現時点では推奨事項であるが、将来の改訂において義務化される可能性も言及されている。また、別添で各規定は必須要件(M)と推奨要件(R)、条件付き必須要件(MC)等に細分化されている。

消費者IoTのためのサイバーセキュリティ規定及びデータ保護規定

No	規定内容	No	規定内容
1	単一のデフォルトパスワードを使用しない	8	パーソナルデータの安全性を確保する
2	脆弱性の報告管理手段を実装する	9	ネットワークの停止・停電等に対するシステムのレジリエンスを確保する
3	ソフトウェアを定期的に更新する	10	システムの遠隔データを調査する
4	機密性の高いセキュリティパラメータを安全に保存する	11	ユーザーが自身のデータを容易に削除できるようにする
5	安全に通信する	12	機器の設置とメンテナンスを容易にできるようにする
6	攻撃対象になる場所を最小限に抑える	13	入力データを検証する
7	ソフトウェアの完全性を確保する	14	個人データを保護するための機能を提供する

規定内容の例

「ソフトウェアを定期的に更新する」の例

必須要件(M)
ネットワークインタフェース上でアップデートが配信される場合、機器は信頼関係（トラストリレーションシップ）を通じて真正性と完全性を検証しなければならない。

推奨要件(R)
消費者IoT機器における全てのソフトウェアコンポーネントが、安全にアップデートできるようにすべきである。

条件付き必須要件(MC)
制約を受けた機器ではない場合、機器は安全にアップデートをインストールするための仕組みを有しなければならない。

条件付き推奨要件(RC)
ソフトウェアのアップデートに、自動的なアップデートの仕組みが用いられるべきである。

プライバシー・シールド無効化に関する動向（概要）

- 米国が2016年にEUと締結していたプライバシーシールドに対して、2020年7月にEU司法裁判所は無効とする判決を下した。

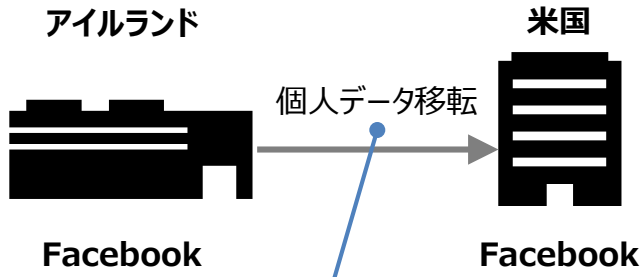
背景

- **米国はEUに対してプライバシーシールドを締結（2016年）**プライバシーシールドとは、EUのプライバシー原則を遵守することを個別企業が米国商務省に登録した場合に、個人データをEU域外へ持ち出せるとしたもの
- **EUにてGDPRが施行（2018年）**GDPRでは原則EU域内から個人データを移転させることは違法とした。
- **個人データ移転についてEU司法裁判所に申し立て**本申し立てはEU在住ユーザがFacebookに対して行ったものである。

動向の概要

- 2020年7月16日に、EU司法裁判所はEU市民の情報が十分に保護されないとの理由から、EUから米国への個人データの移転を認めるプライバシー・シールド決定を無効とする判決を出した。
- プライバシーシールドとは、米国が2016年にEUと締結したものであり、企業はEUのプライバシー原則を遵守すると米国商務省に登録した場合、EU域内から個人情報を移転できるとしたものである。
- 一方で、EU司法裁判所は標準的契約条項（Standard contractual clauses：SCC）と呼ばれるデータ移転契約のひな形を利用することにより、個人データ移転は可能とした。

プライバシーシールドの例（例：Facebook）



プライバシーシールドにおいては米国商務省に事前登録した場合、個人データ移転を認めるとしていた。

標準的契約条項
(Standard contractual clauses：SCC)

欧州委員会が決定したデータ移転契約のひな型で、個人データの移転をGDPR上適法化するためのもの。なお、以下の3つのひな型が用意されている。

- 域内管理者・第三国管理者間のモデル条項 (Decision 2001/497/EC)
- 域内管理者・第三国管理者間のモデル条項 (Decision 2004/915/EC)
- 域内管理者・第三国処理者間のモデル条項 (Decision 2010/87/EU)

(出所)　JETRO" EU司法裁、米国との個人データ移転に関する「プライバシー・シールド」を無効と判断"(2020/7/17)、"標準的契約条項（Standard contractual clauses：SCC）（欧州委員会資料の仮訳）"（2018/3/28）等を参考に作成

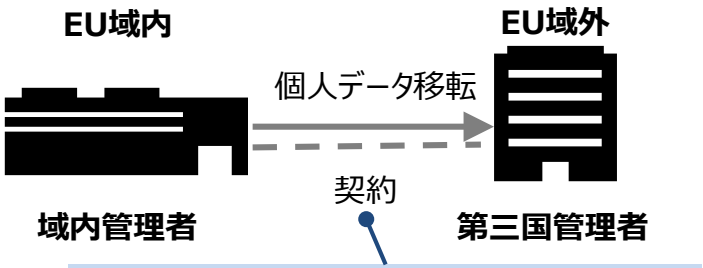
プライバシー・シールド無効化に関する動向（企業への影響）

- 個人データをEU域内から移転する企業は契約の再締結が必要となる他、場合によってはデータ移転を中止する必要が発生する可能性がある。また、日本企業への影響は限定的であるが対応が必要となる場合がある。

契約の締結

- EU司法裁判所は個人データの移転をGDPRの内容に沿った形で実施するためのルールである標準的契約条項のひな形を使用することは認めたため、企業はデータ移転契約を締結する必要が生じた。

<域内管理者・第三国管理者間の場合>

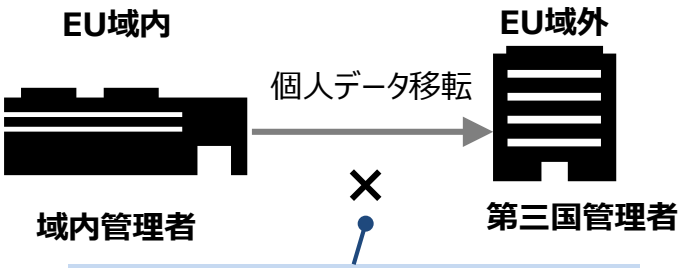


データ移転契約を結ぶ必要がある。

データ移転の中止

- 個人データをEU域内から移転する企業はデータ輸入者が標準的契約条項を守れないと判断した場合には、個人データ移転を中止する必要が発生する。

<域内管理者・第三国管理者間の場合>



データ移転を中止する場合がある。

＜日本企業への影響＞

- 日本とEUは2019年1月に相互に十分性認定をしていることから、**影響は限定的**と見られる。
- ただし、日本に対する十分性認定も欧州委員会による見直しにおいて厳しく審査される可能性があるため、従来、日本への移転を十分性認定のみに基づき行っていた場合は**標準的契約条項を併用することがより安全**と思われる。

(出所) JETRO" EU司法裁、米国との個人データ移転に関する「プライバシー・シールド」を無効と判断"(2020/7/17)等を参考に作成