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２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

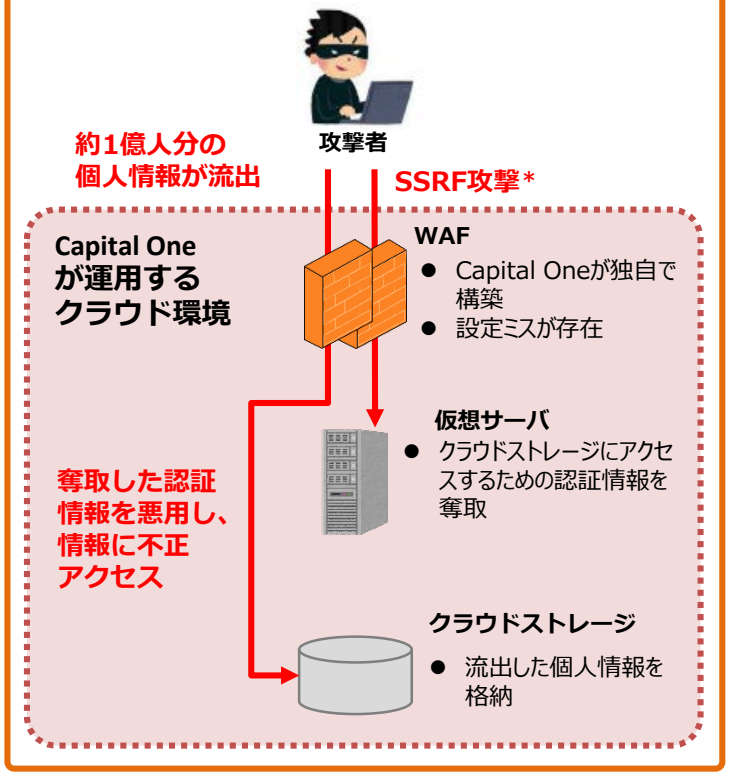
Capital One社における個人情報漏えい事例

- 2019年7月29日、**米国の金融大手Capital One は、不正アクセスにより1億人を超える個人情報**(クレジットカードへの申し込みをした消費者や中小企業の氏名/名称、住所、郵便番号、電話番号、メールアドレス等)**が流出したと発表**した。
- 原因の一つは、 Capital Oneがクラウド環境に独自で構築した**ウェブ・アプリケーション・ファイアウォール(WAF)の設定ミス**とされる。

本事例の詳細（原因・影響等）

- 2019年7月29日、米国の金融大手Capital One は、不正アクセスにより1億人を超える個人情報が流出したと発表した。
- 流出した情報は、クレジットカードへの申込みを行った消費者及び中小企業の氏名/名称、住所、郵便番号、電話番号、メールアドレス等で、クレジットカード番号、ログイン情報は含まれないとされる。
- Capital Oneがクラウド環境に独自で構築したウェブ・アプリケーション・ファイアウォール(WAF)の設定ミスにより、仮想サーバに割り当てられたクラウドストレージにアクセスするための認証情報を奪取されたことがインシデント発生の原因の一つとされる。
- 攻撃者は、奪取した認証情報を悪用し、個人情報を格納したクラウドストレージへアクセスした。そこから、外部アクセス可能なクラウドストレージにデータをコピーすることにより、結果的に約1億人分の個人情報を流出させた。
- 本件に関して、Capital Oneに加えて、漏えいしたデータがサイト上で公開されたGitHubも被告とした複数の集団代表訴訟(クラスアクション)が提起されている。

事例のイメージ



＊：Server Side Request Forgeryの略。公開サーバから内部のサーバにリクエストを送信することにより、内部のサーバを攻撃する手法。

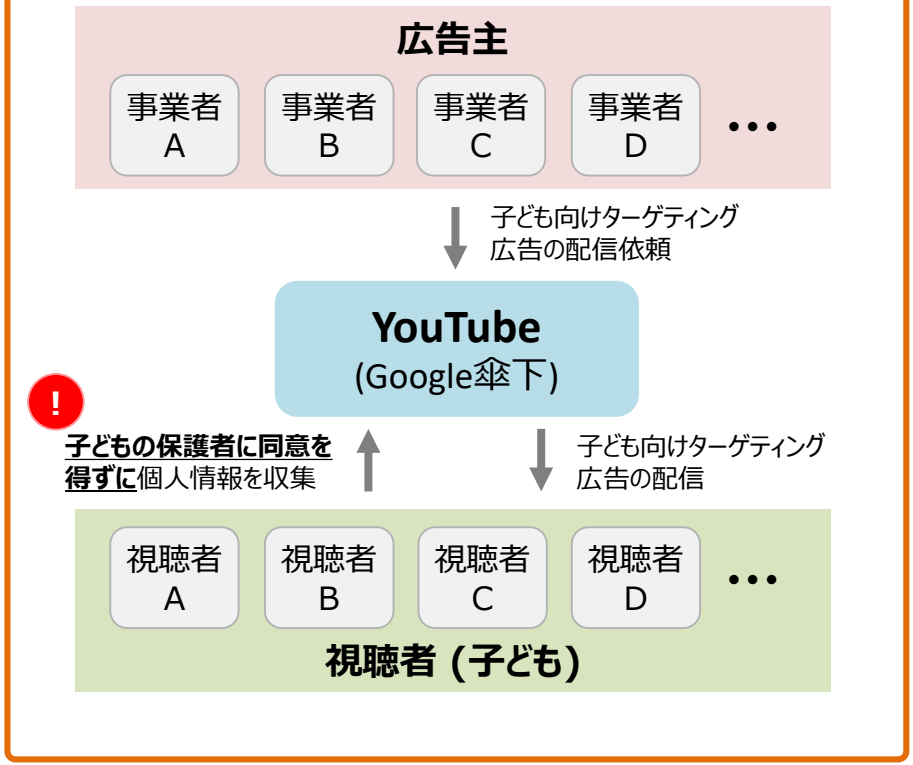
米国児童オンラインプライバシー保護法違反事例 (YouTube)

- 2019年9月4日に、**米国連邦取引委員会(FTC)は、Googleと傘下のYouTubeに、児童オンラインプライバシー保護法(COPPA)違反に対する和解金として1億7000万ドル(約180億円)を課すと発表**した。
- YouTube上の子ども向けチャンネルの視聴者(子ども)に対して、その**保護者に同意を得ずにクッキーを使い個人情報を収集していたことがCOPPA違反**とされた。

本事例の詳細（原因・影響等）

- YouTubeで配信されるチャンネルの内、COPPAの対象となる13歳未満の子どもが視聴する可能性が高いものについて、保護者に無断で子どもの個人情報を収集しマーケティングに利用している疑いが生じていた。
- 2018年4月に、子どもの人権やプライバシーの擁護に取り組む団体や消費者団体など20の団体がFTCに対し、YouTubeをCOPPA違反の疑いで捜査するよう求める請願書を共同で提出した。
- 上記を受けて、FTCとニューヨーク司法長官は、Googleと傘下のYouTubeが、子ども向けチャンネル視聴者に対して、保護者に同意を得ずにクッキーを使い個人情報を収集していたことをCOPPA違反と申し立てた。
- 2019年9月4日にFTCが発表した和解条件は、和解金1億7000万ドル(約180億円)の支払いと、子ども向けコンテンツ関係者向けのCOPPA順守トレーニング及び、COPPA対応に向けたシステム改善の実施である。

事例のイメージ



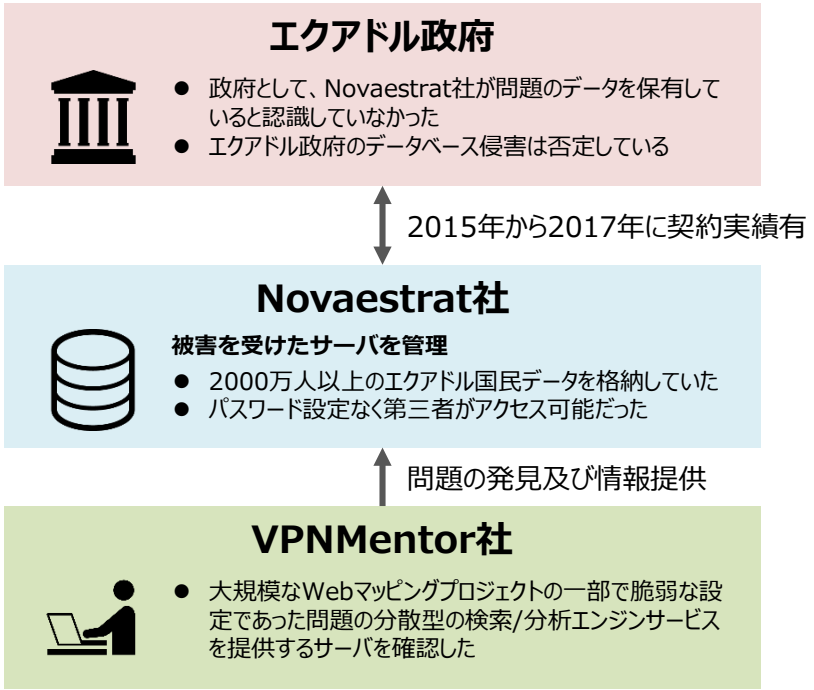
エクアドル全国民情報流出の可能性

- 2019年9月16日、VPNサービスのレビュー等を行うvpnMentorは、**エクアドル全国民分に相当する大量のデータがインターネット上で漏洩している疑いがあることを発表**した。
- 同国のコンサルティング企業が、検索/分析エンジンサービスを提供するサーバを、**パスワードなしで誰でもデータにアクセスできる状態にしていたことが原因**とされる。

本事例の詳細（原因・影響等）

- 2019年9月16日、エクアドル政府は、同国民2000万人超(故人を含む)の情報が流出した疑いがあることを明らかにした。
- サーバに保存されていたデータには、エクアドル国民2000万人超の個人情報のほか、750万件の金融関連の情報や250万件の自動車の所有者情報が含まれていた。
- Novaestrat社と呼ばれる同国のコンサルティング企業が、分散型の検索/分析エンジンサービスを提供するサーバを、パスワードなしで誰でもデータにアクセスできる状態にしていたことが原因とされている。
- 2015年から2017年にかけて、エクアドル政府は、複数の契約を同社との間で結んでいたが、同社が流出の疑われる当該データを保有する契約ではなかった。

事例のイメージ



航空機の脆弱性に関するBlack Hat USA 2019での報告

- 2018年9月、大手航空機メーカーのサーバにおいて、航空機の**システム構成に関する情報がインターネット上に公開**されていることが発覚。IOActive社(I社)は、特定の脆弱性を用い、機内エンターテイメントシステム等から、**機器の操作に関わるネットワークに到達できることを発見**し、メーカーに報告。メーカーはI社に対して、報告されたのは**悪用可能な脆弱性ではなく、緩和策も実施済と回答するも、詳細は不開示**。
- これに失望したI社は2019年8月の**Black Hatで脆弱性の詳細を公開**。
- これを受けメーカーは、I社は航空機ネットワークの一部を評価しただけで、I社のシナリオでは**重要な航空機システムに影響を与えることはできず、発表は無責任だと失望を表明**。

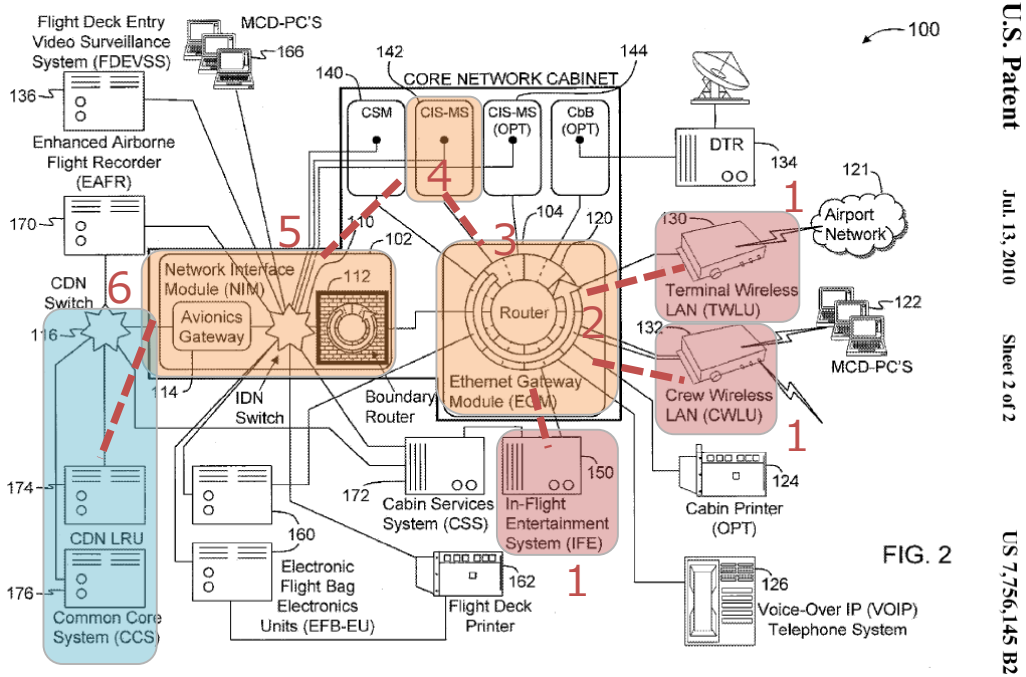


FIG. 2

U.S. Patent Jul. 13, 2010 Sheet 2 of 2 US 7,756,145 B2

●基本的な攻撃対象の解説図

1の機内エンターテイメントシステムや外部ネットワークから、6の機体の操作やナビゲーションに関連するとされるネットワークに到達できると解説されている。

https://ioactive.com/arm-ida-and-cross-check-reversing-the-787s-core-network/
https://www.wired.com/story/boeing-787-code-leak-security-flaws/

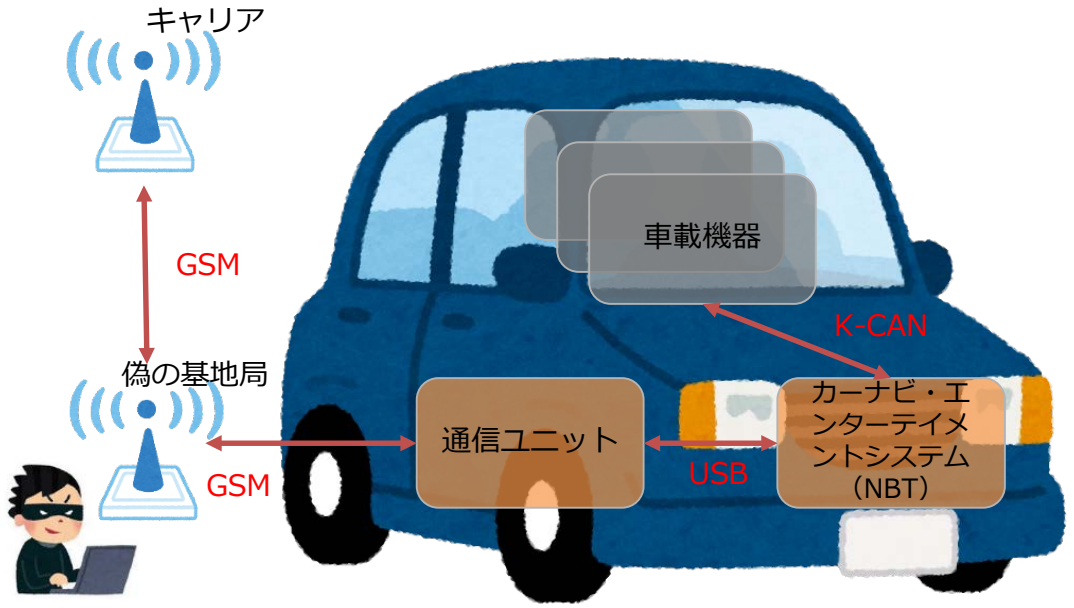
自動車の脆弱性に関するBlack Hat USA 2019での報告

- 2018年2月、中国Tencent社のKeen Security labは、大手自動車メーカーの自動車の脆弱性を検証してメーカーに通知。これを受け、メーカーは緩和策を実施。また、Keen labは、責任ある開示（Responsible Disclosure)方針に従い、2019年8月のBlack Hatにおいて、分析結果、検証内容及び対応策の詳細をメーカーと**共同発表**した。
- 報告では、カーナビやエンターテイメントシステムを提供する車載機器の脆弱性を用いて、偽の携帯電話ネットワークからSMSを送付する等の操作により、ドアの開錠や任意コード実行等の操作が行えたとしている。

＜開示プロセス＞

2017年2月～2018年2月	Keen labが自動車の脆弱性及び攻撃チェーンを検証し、メーカーに通知
2018年3月	メーカーは通知された脆弱性を確認し、緩和策を計画
2018年4月	脆弱性に関するCVE番号が予約
2018年5月	Keen labが概要レポートを一般公開
2018年夏	メーカーが必要な対策と緩和策を実施
2019年8月	Black Hatにおいて共同発表、詳細レポートを公開

＜偽GSM基地局を用いた遠隔攻撃イメージ＞

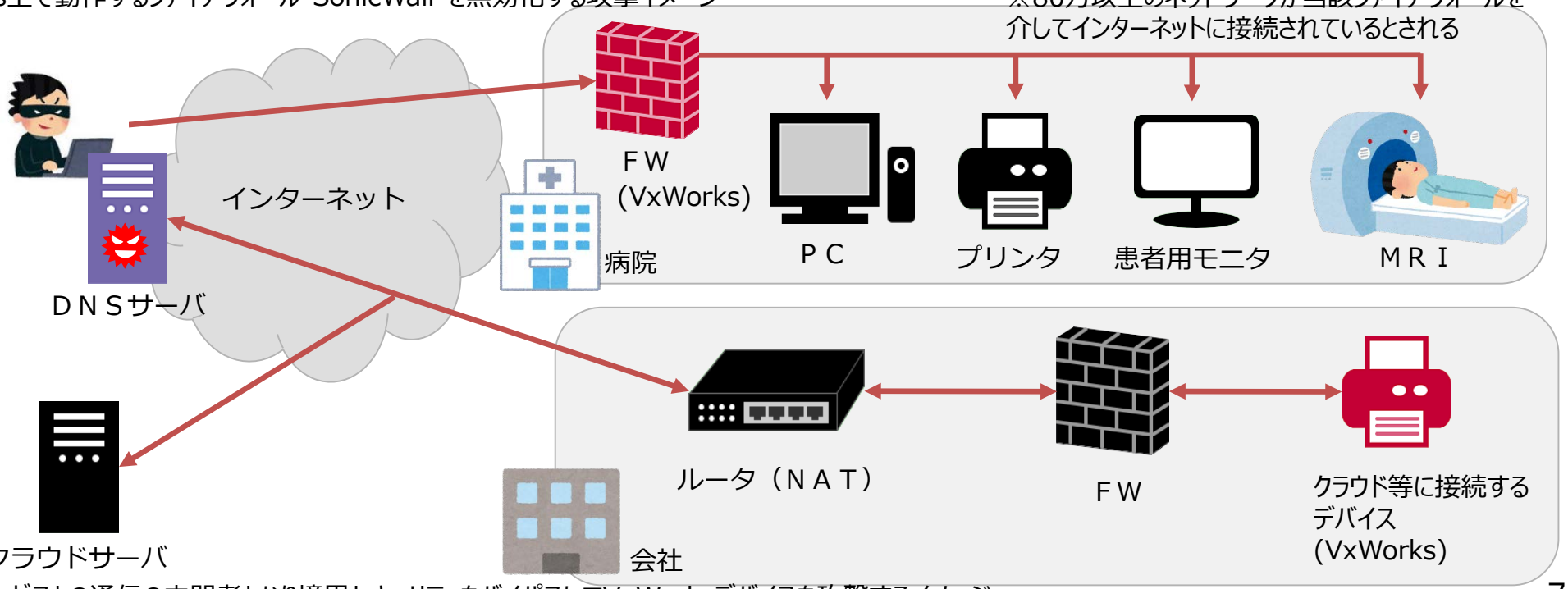


https://www.blackhat.com/us-19/briefings/schedule/#-days--mitigations-roadways-to-exploit-and-secure-connected-bmw-cars-15313

リアルタイムOS　VxWorks等における脆弱性（URGENT/11）

- 2019年7月、Armis Labは、**医療、自動車、航空機、防衛など幅広い産業において20億個以上のデバイスで採用されるWindRiver社のVxWorksに11個の脆弱性**があることを発表。本脆弱性はVxWorksが採用するTCP/IPスタックに存在し、これを利用することでファイアウォール等の境界セキュリティを制御したりバイパスすることが可能となり、ネットワーク内外でマルウェアを伝搬させることができるようになるとされる。
- 同10月、VxWorksと同じ旧Interpeak社製のTCP/IPスタックをサポートしていた**別のリアルタイムOSにも同様の脆弱性**があることが発覚。影響の拡大が懸念される。

VxWorks上で動作するファイアウォール“SonicWall”を無効化する攻撃イメージ



クラウドサービスとの通信の中間者となり境界セキュリティをバイパスしてVxWorksデバイスを攻撃するイメージ

https://www.armis.com/urgent11/

スマートスピーカーを悪用したフィッシング攻撃

- 2019年10月、ドイツのセキュリティ研究機関 SRLabs（Security Research Labs）が、スマートスピーカーの機能を悪用し、ユーザのパスワードの窃取や会話の盗聴が可能であることを公表。
- スマートスピーカーは、特定のフレーズを認識することでそれに対応した機能を実行するが、特定のフレーズに続く内容をテキスト化してサーバに送信する機能がある。
- スマートスピーカーのアプリストアに相当するAlexa SkillやGoogle Assistantの審査を、無害なアプリを装って通過した後に、メッセージを改変する手法によるフィッシングなど（※）、当該機能を利用してユーザの個人情報等を窃取するスマートスピーカーを通じた攻撃手法が実証された。

※攻撃プロセスの概要

●偽のメッセージでフィッシング

1．特定のフレーズ（e.g.「Start」）に続く内容をサーバに送信する、一見して無害なアプリを作成。
2．審査通過後、最初のメッセージをエラーメッセージのように改変（e.g.「現在この機能は利用できません。」）。
3．スピーカーにフィッシングメッセージを発声させる（e.g.「重要なアップデートがあります。Start updateに続いてパスワードを発声してください。」）　。
4．「Start」の後にユーザが発声したパスワードがサーバに送信される。

●アプリの終了を誤認させて盗聴

1．一見して無害なアプリを作成。
2．審査通過後、アプリの終了時等に「Good Bye」と発声させた後、スピーカーが音声化できない文字列（e.g.“ . “）を繰り返すことで、アプリの動作を継続させるようアプリを改変。
3．２．の終了音やメッセージを聞いたユーザは、アプリが停止したと錯覚。
4．アプリが動作している間にユーザが特定のキーワードを発声した場合、それがサーバへ送信される。

https://srlabs.de/bites/smart-spies/

Medtronic社の電気手術器に複数の脆弱性

- 2019年11月、US-CERTは、Medtronic社製の電気手術器に複数の脆弱性（CVE-2019-13543、CVE-2019-13539、CVE-2019-3464）が存在するとして、注意喚起を行った。これらの脆弱性により、攻撃者はリモートから特定の攻撃コードを送信することで、ファイルの上書きや不正コードの実行等を行うことが可能とされる。
- 該当するデバイスのネットワーク接続はデフォルトでは無効であり、再起動時にもイーサネットポートが無効になる構成となってはいるが、多くの場合、ネットワークに接続して利用されているため、Medtronic社はパッチを適用するまで、当該デバイスをネットワークに接続しないことを推奨している。

電気手術器の3つの脆弱性

ハードコードされた資格情報の使用	デバイスにハードコードされた資格情報が発見された場合、それらを使用して機器のファイルを読み取られる可能性がある。
脆弱なハッシュアルゴリズムを使用している問題	OSパスワードに脆弱なハッシュアルゴリズムを利用しており、開示されている他の脆弱性と組み合わせて、これらのハッシュを取得される可能性がある。
適切でない入力確認	脆弱なバージョンのrsshユーティリティを使用してファイルのアップロードが可能であることから、ファイルにアクセスされたり、任意のコードを実行されたりする可能性がある。

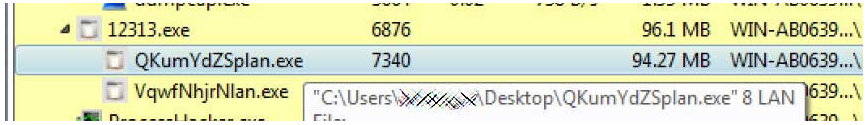
https://www.us-cert.gov/ics/advisories/icsma-19-311-02

ランサムウェア「Ryuk」がWake-On-Lanを利用して電源オフのデバイスを暗号化

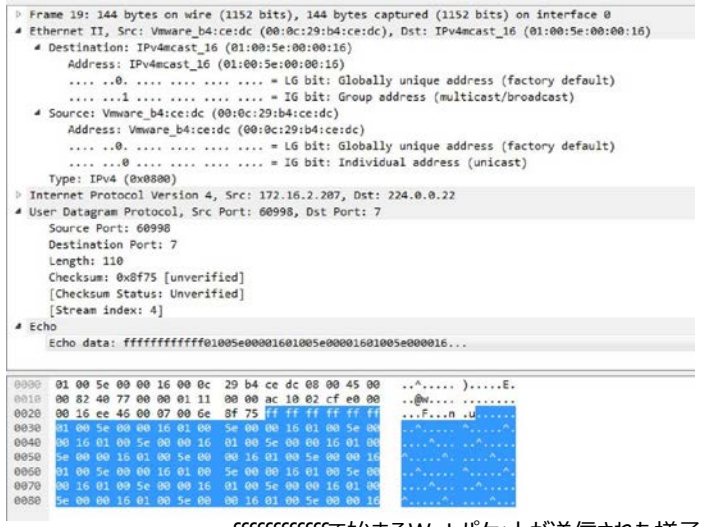
- 2018年夏頃から存在が確認されている標的型ランサムウェア「Ryuk」は、これまでも海外の多くの企業・行政機関に被害を与えているが、少しずつ新しい機能が追加されている。
- 2019年10月頃に出現したRyukの新しい機能は、ネットワーク上の電源がオフになっているデバイスを起動できるWake-On-Lan(WOL)機能を利用し、電源がオフになっている端末ですら暗号化できるため、企業内ネットワーク等において感染が広がる恐れがある。

攻撃プロセスの概要

①サブプロセスの作成	・マルウェアが実行されると、自身のコピーであるサブプロセスを、特別なモードで実行。
②ネットワークの確認	・特別なモードで実行された場合、デバイスのARPテーブルをスキャンし、プライベートネットワークを確認。
③WoLパケットを送信、デバイスを起動	・デバイスのMACアドレスにWake-on-Lan（WoL）パケットを送信して起動を試みる。
④ドライブをマウントし、暗号化	・起動に成功した場合、そのデバイスのドライブの暗号化を試みる。



特別なモード（実行引数「8 LAN」）でサブプロセスが実行された様子



ffffffffffffで始まるWoLパケットが送信された様子

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/

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

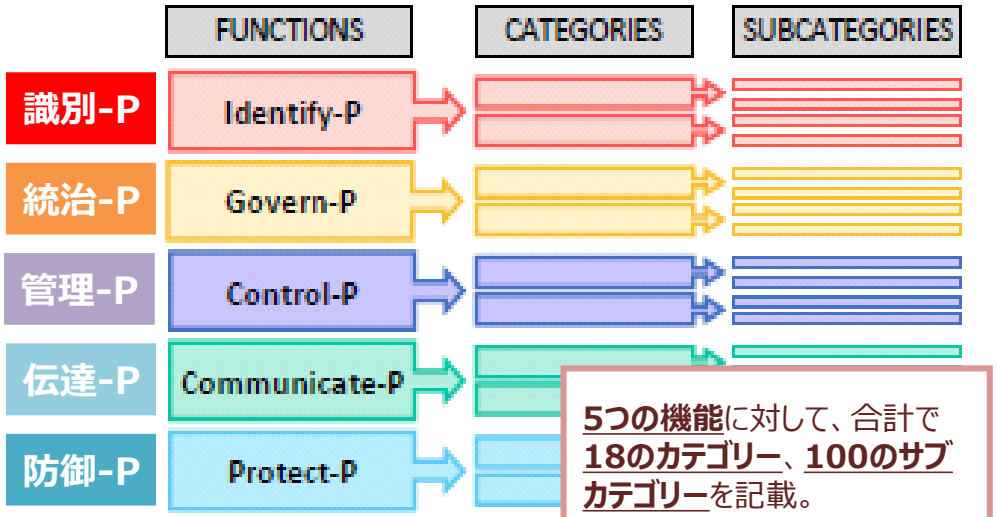
NISTプライバシーフレームワーク Version 1.0

- NISTは、2020年1月、**NISTプライバシーフレームワーク Version 1.0を公開**した。
- 同フレームワークの活用を通じて、企業には、顧客との信頼関係を確立し、規制対応をより確実なものとしつつ、個人、ビジネスパートナーとのプライバシーに関わるコミュニケーションを促進することが期待されている。
- 機能や、カテゴリー、サブカテゴリー、インプリメンテーション・ティア等、NISTサイバーセキュリティフレームワーク(CSF)と同様の構造を採用しており、**CSFとの併用を促進するような構成**となっている。

プライバシーフレームワークの構造

NIST Cybersecurity Frameworkと同様の構造を採用。

- 「識別-P」、「統治-P」、「管理-P」、「伝達-P」、「防御-P」という5つの機能に対して、18のカテゴリーと100のサブカテゴリーが示されている。
- 基本構造は9月の準備ドラフト(preliminary draft)から変更なし。

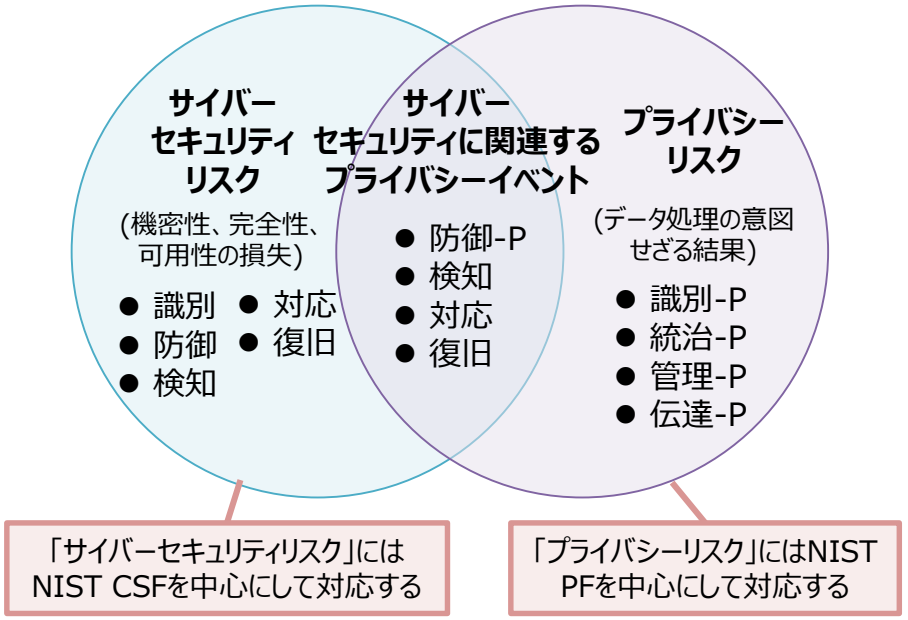


-P：CSFの5分類と区別するため追記されている

サイバーセキュリティフレームワーク(CSF)との関係

CSFとの併用を促進する構成を採用。

- サイバーセキュリティリスクとプライバシーリスクの関係を整理し、網羅的なリスク対応が可能となるようにCSFとプライバシーフレームワーク(PF)の機能をマッピングしている。



出典：NIST PRIVACY FRAMEWORK Version 1.0

NIST SP800-171 のアップデート及びSP 800-171Bの策定

- 2020年2月、**SP 800-171の第2版が公開**された。**110項目のセキュリティ要件には変更がなく**、付録Fに記載されていたディスカッションセクションを、セキュリティ要件に併記するという小規模な改定を実施している。
- 重要性の高いプログラムや価値の高い資産で扱われるCUIを高度な標的型攻撃から保護する追加の対策を示すSP 800-171Bは同じタイミングで公開されず、ドラフトのままとなっている。

SP 800-171及び関連文書の策定状況

SP 800-171 Rev. 2 — 2020年2月 公開
連邦政府外のシステムと組織における管理された非格付け情報(CUI)の保護

- 対策要件は変更されていないが、付録Fに記載されていたディスカッションがセキュリティ要件に併記される形となった。

SP 800-171A — 2018年6月 公開
管理された非格付け情報向けセキュリティ要件の評価

- SP 800-171で提示されているセキュリティ要件への準拠を評価するための評価手順及び方法論を提供する。

SP 800-171B — 2019年6月 ドラフト公開
CUIを処理する重要性の高いプログラム及び価値の高い資産向けの高度なセキュリティ要件

- 重要性の高いプログラムや価値の高い資産で扱われるCUIの機密性保護のために推奨される高度なセキュリティ要件を提供する。

SP 800-171とSP 800-171Bとの関係

- SP 800-171Bは、高度な標的型攻撃(APT攻撃)からCUIを保護するため、SP 800-171が提示する要件を補完する。
- SP 800-171Bが提示する要件は、「損害を制限する運用」、「侵入耐性アーキテクチャ」、「サイバーレジリエンス＆サバイバビリティ」の3点をサポートし、価値の高い資産の保護を実現する。

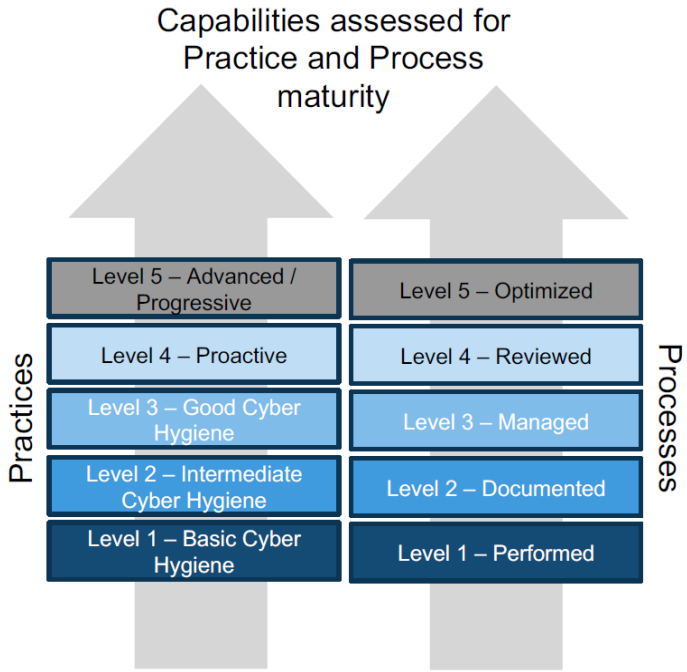
出典：Draft NIST Special Publication 800-171B

Cybersecurity Maturity Model Certification (CMMC)の策定

- 米国国防省（DoD）は、NIST SP800-171について、自己宣言でありTier2以下では対応が十分でなく、特に中小企業には対応困難、との認識の下、５段階の成熟度モデルを用いた新たなフレームワークであるCMMCを、カーネギーメロン大学、ジョンズホプキンス大学と共に開発、2020年1月に第1版を策定。
- CMMCは、最終的にはDoDの調達に関わるすべての企業（約30万社）に対して第三者認証を求めることを検討中。
- どのTierの契約にどのレベルの認証が求められるのか、政府が決定するとしている。

【プロセスとプラクティスの成熟度の考え方】

- CMMCでは、各ドメイン（例：資産管理ドメイン）について、プロセスの成熟度、プラクティスの成熟度を５段階で評価。
- 例えばあるドメインのプロセス成熟度が３、プラクティス成熟度が２の場合、レベル２と評価される。



NISTIR 8228 – Consideration for Managing IoT Cybersecurity and Privacy Risks

- IoT機器の導入に伴い生じる、**サイバーセキュリティとプライバシーのリスクを軽減するための推奨事項**を整理。（2019年6月発行）
- IoT機器の機能の多様性を踏まえ、機器のセキュリティ、データのセキュリティ、個人のプライバシー情報という３つの観点からIoTデバイスにおいて生じうる懸念を列記し、NIST Cybersecurity Framework、SP 800-53 Rev.5（Draft）との対応関係を整理。

IT機器と比較して、IoT機器がサイバーセキュリティリスク、プライバシーリスクに影響を与えうる３つの懸念

物理世界とデバイスとの相互作用	IoT機器の多くは、従来のIT機器では通常行わない方法で物理世界とのやりとりを行う。
デバイスアクセス、管理、モニタリング機能	IoT機器の多くは、従来のIT機器と同じ方法でアクセス、管理、監視することができない。
サイバーセキュリティ機能、プライバシー機能の可用性、効率、有効性	IoT機器のためのサイバーセキュリティ機能、プライバイシー機能の可用性、効率、有効性は、従来のIT機器とは異なる。

IoT機器のサイバーセキュリティリスク、プライバシーリスクを軽減する対処領域

機器のセキュリティを守る	• アセットの管理、脆弱性管理、アクセス管理、機器のセキュリティインシデント検知
データのセキュリティを守る	• データ保護、データのセキュリティインシデント検知
個人のプライバシー情報を守る	• 情報フローの管理、特定個人情報の処理権限の管理、特定個人情報の提供に際する意思決定、データ管理との分離、プライバシー違反の検知

NISTIR 8259 2nd draft - Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufactures

- 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、**IoT機器の製造者に任意だが推奨される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1月ドラフト第2版公開)。**6つのコアサイバーセキュリティ機能をベースラインと定義**し、当該機能を達成するために実装すべき重要要素や、既存のIoTセキュリティガイダンスへの参照がまとめられている。
- ベースラインを元に、産業分野により異なるセキュリティ要求を踏まえた機能の特定が必要としている。

製造者に推奨されるサイバーセキュリティ関連活動

販売前に影響する活動	活動1：予想される顧客特定、ユースケース定義 活動2：顧客のサイバーセキュリティの目標調査 活動3：顧客目標に対処する方法決定（6つのコアサイバーセキュリティ機能） 活動4：顧客目標の適切なサポート計画（ハード、ソフト、ファームウェア、ビジネスリソースの適切なプロビジョニング）
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アプローチ定義 活動6：顧客に伝える内容と伝達方法決定（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、提供するデバイスセキュリティ機能、デバイス構成・機能、ソフトウェア及びファームウェアの更新、デバイスの廃止オプション）

6つのコアサイバーセキュリティ機能

（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、及びこれら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認可エンティティのみに制限可。
（２）デバイスの構成：IoT機器のソフトウェア・ファームウェアの構成変更が可能。変更は、認可エンティティのみが行うことができる。	（５）ソフトウェア等の更新：IoT機器のソフトウェア・ファームウェア更新は、認可エンティティによって安全かつ構成可能なメカニズムを用いてのみ実行できる。
（３）データ保護：IoT機器が保存・送信するデータを不正なアクセス及び変更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機器はセキュリティ状態を報告し、認可エンティティのみにアクセスを許可。

NISTIR 8267 draft - Security Review of Consumer Home Internet of Things (IoT) Products

- NISTIR 8267では、スマートホームで用いられる7カテゴリ※1の家庭用IoTデバイスについて、サンプル調査※2を通じてセキュリティ機能をレビューした上で、NISTIR 8259 draftも参照しつつ、家庭用IoTデバイスのメーカーが開発時に考慮すべき事項をまとめている（2019年10月ドラフト版公開）。

※１　スマート電球・照明・カメラ・ドアベル・プラグ・サーモスタット・TV
※２　公開情報調査やネットワークキャプチャ等の実機調査を実施。分解等を含むより詳細な調査は行っていない。

家庭用IoTデバイスメーカーが考慮すべき事項

- ユーザーによるデバイスの初期設定時に、NIST SP 800-63が示したベストプラクティスと同等な強度のパスワードを設定するよう要求すること
- 中間者攻撃を防ぐため、認証書や公開鍵をホスト名と関連付ける”Certificate Pinning”を用いること
- デバイスのソフトウェア/ファームウェアの更新やデバイスを通じてやりとりされる機密データを保護するために、 NIST SP 800-52 Rev-2で推奨されるTLS暗号化スイートを使用すること
- USBを含む使用されない物理的又は論理的アクセスポートを閉じるか、アクセスを防ぐこと
- 家の外に設置されるセキュリティに関連するIoTデバイスに物理的リセットボタンを実装しないこと
- デバイスのソフトウェア/ファームウェアの更新ができ、かつ、そのことがタイムリーにユーザーへ通知されるようなプロセスを、ベストプラクティスに沿って開発・実装すること
- UPnP通信はデフォルトでは認証を利用しないため、UPnP通信を保護するために追加の端末保護機能を実装すること
- サイバーセキュリティ機能は、技術に詳しくないユーザーにも分かりやすいものにするなど、適用可能性や実行性の高いものにすること

NISTIR 8276 draft - Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

- NISTが2015年と2019年に実施したサイバーサプライチェーンリスク管理(C-SCRM)に関するケーススタディをベースに、8つのキープラクティスを提示（2020年2月ドラフト公開 ）。
- 「2 Problem Definition」の項には、デジタル化の進展に伴い、昨今では**サイバーセキュリティイベントの影響が、データの損失だけでなく、重大な経済的損失、安全性の侵害や人命の損失にまで繋がり得る**との、第2層TFにおける議論と類似する記載がある。

米国におけるサイバーサプライチェーンリスク管理(C-SCRM)に係るこれまでの検討プロセス

2008年1月
包括的サイバーセキュリティイニシアチブ(CNCI) #11「グローバルサプライチェーンのリスク管理のための多方向からのアプローチの開発」

2012年10月
NIST IR 7622「連邦情報システムのための国家サプライチェーンリスク管理プラクティス」公開

2015年4月
NIST SP 800-161「連邦情報システム/組織向けサプライチェーンリスク管理プラクティス」公開

2015年9月
サイバーサプライチェーンリスク管理に関する民間事業者の対応におけるケーススタディ(18件)を公開

2018年4月
NIST Cybersecurity Framework Ver.1.1 公開 (サプライチェーンリスク管理に関する対策カテゴリーを新たに追加)

2020年2月
Draft NIST IR 8276「サイバーサプライチェーンリスク管理におけるキープラクティス」公開

C-SCRMにおける8つのキープラクティス

1. 組織をまたいだサイバーサプライチェーンを統合する
2. C-SCRMに関する公式のプログラムを設置する
3. 自組織の重要なサプライヤーを認識し、管理する
4. 自組織のサプライチェーンを理解する
5. 重要なサプライヤーと密接に協力する
6. 重要なサプライヤーを自組織のレジリエンス、改善活動に含める
7. サプライヤーとの関係全体を通じて評価と監視を行う
8. 事業継続を保証するためのライフサイクル全体に対する計画を立てる

NTIA Software Component Transparencyに関する議論

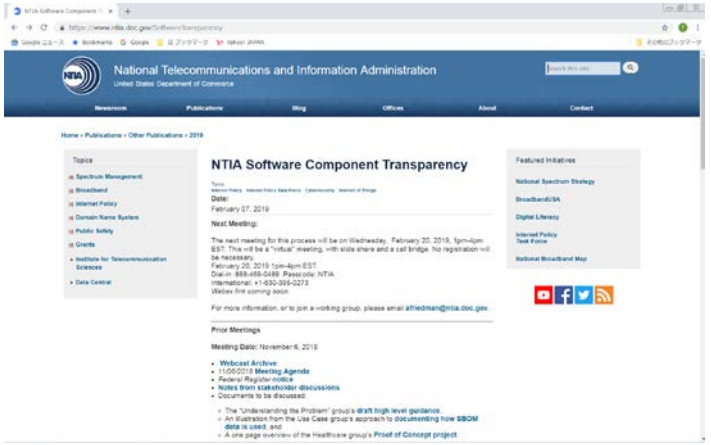
- 2018年、米国NTIA（電気通信情報局）において、「Software Component Transparency」に関するMultistakeholder Meetingが設置された。
- 2019年11月初旬までにNTIA Software Component Transparencyの最初の成果物として、SBOMに関するレポート集が公表された。

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（第6回）
11月18日（第7回）
2020年　2月13日（第8回）

SBOMに関するレポート集（https://www.ntia.gov/SBOM）

1. **Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)**（ソフトウェアコンポーネントトランスパレンシーの構築：共通ソフトウェア部品表（SBOM）の確立）
2. **Roles and Benefits for SBOM Across the Supply Chain**（サプライチェーン全体でのSBOMの役割と利点）
3. **Survey of Existing SBOM Formats and Standards**（既存のSBOM形式と標準の調査）
4. **Healthcare Proof of Concept Report**（ヘルスケアPOCレポート）

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（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	

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			

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

- 2019年4月、Cybersecurity Act が欧州理事会で採択、6月27日に発効。
- **2019年9月、ENISAがサイバーセキュリティ認証スキームの候補を準備するためのアドホックワーキンググループの設立を呼びかけ。候補スキームとしてCommon Criteria(ISO/IEC 15408)も考えられるとの記載もある。**

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）

消費者向けIoT製品のセキュリティに関する行動規範（英国）

- 英国デジタル・文化・メディア・スポーツ省（DCMS）が、消費者向けIoT製品の開発、製造及び販売の段階で安全が確保されるよう、**製造メーカー等が実践すべき対策を13項目のガイドライン**にまとめ、2018年10月に公表。
- 一部の項目の義務化法案について2019年5月～6月にかけてパブリックコメントを実施。コメントを踏まえた**ドラフト法案を2020年1月に公開。**

ベストプラクティス一覧（13項目）

1. デフォルトパスワードを使用しない
2. 脆弱性の情報公開ポリシを策定する
3. ソフトウェアを定期的に更新する
4. 認証情報とセキュリティ上重要な情報を安全に保存する
5. 安全に通信する
6. 攻撃対象になる場所を最小限に抑える
7. ソフトウェアの整合性を確認する
8. 個人データの保護を徹底する
9. 機能停止時の復旧性を確保する
10. システムの遠隔データを監視する
11. 消費者が個人データを容易に削除できるように配慮する
12. デバイスの設置とメンテナンスを容易にできるように配慮する
13. 入力データを検証する

義務化項目の案（3項目）

① IoTデバイスのパスワードはユニークにする、かつ工場出荷時の共通設定にリセットできないようにする

② IoT製品メーカーは脆弱性開示ポリシーの一部として連絡先を提供する

③ IoT製品メーカーはデバイスに対するセキュリティアップデートを提供する最低期間を明示する

ePrivacy規則の策定

- **ePrivacy規則は、**現行のePrivacy「指令」を「規則」とし、執行及び制裁を大幅に強化するものである。
- **2019年11月、欧州理事会常任委員会（COREPER）が同ドラフトを否決**した後、**2020年2月**に欧州理事会議長が、同規則の**修正版ドラフトを再度発表**している。
- 修正版ドラフトでは、電子通信ネットワークプロバイダ等がエンドユーザの利益や基本的権利等を侵害しない限りにおいて、「正当な利益」(legitimate interests)がメタデータの処理及びクッキーの取得に対する法的根拠となり得ることが示されている。

ePrivacy規則 策定に係るこれまでのプロセス

- **2017年1月**：欧州委員会がePrivacy規則ドラフトを発表
- **2017年10月**：欧州議会LIBE(市民的自由・司法・内務委員会)で修正採択
- **2018年5月**：欧州一般データ保護規則(GDPR)施行
- (この間、業界団体等による意見提出や閣僚理事会による複数回のドラフト公表を実施)
- **2019年9月**：欧州理事会議長が、ePrivacy規則の修正版ドラフトを発表
- **2019年11月**：欧州理事会常任委員会（COREPER）が同ドラフトを否決
- **2020年2月**：欧州理事会議長が、ePrivacy規則の修正版ドラフトを発表

ePrivacy規則ドラフトの主なポイント

規制対象	● 電子通信サービスに関連して実行される電子通信コンテンツ及び電子通信メタデータの処理 ● エンドユーザーの端末機器情報(例：クッキー) ● 電子通信サービスのユーザーの公開ディレクトリ提供 ● エンドユーザーへのダイレクトマーケティング
地理的な適用範囲	● 域外適用あり (処理の場所や事業者の所在地を問わない)
通信データの保護	● 「電気通信コンテンツ」(通信されるデータそのもの)と「電気通信メタデータ」(コンテンツの通信のために処理される日時・種類等のデータ)の秘密性を規定
クッキーの取扱い	● 同意を得ている場合や、サービスプロバイダに「正当な利益」がある場合等を除いて原則として禁止
ダイレクトマーケティングの実施	● 原則としてエンドユーザーの同意を得る必要がある。
執行と制裁	● 違反した条項に応じて、下記いずれかが適用される。 - 1000万ユーロ以下、又は前会計年度の全世界年間売上高の2%以下のいずれか高いほう - 2000万ユーロ以下、又は前会計年度の全世界年間売上高の4%以下のいずれか高いほう

欧州におけるクラウドインフラ構築の動き：Gaia-X プロジェクト

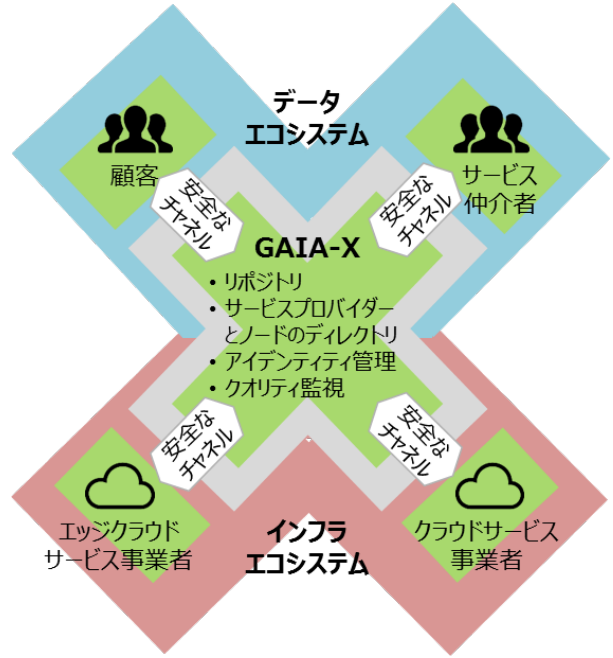
- 2019年10月29日、**<u>ドイツ政府とフランス政府は、EU規模でのデータの共有や利活用を支援するため、クラウドサービスのインフラを構築する構想(GAIA-X プロジェクト)を発表</u>**した。
- 現在、ドイツとフランスで構想が主導されており、2020年春までにソリューションの開発とルールの形成を担当する法的効力のある組織を設立し、2020年末までに概念実証(PoC)を行う予定とされている。
  - FAQs on the GAIA-X project (https://www.bmwi.de/Redaktion/EN/FAQ/Data-Infrastructure/faq-projekt-gaia-x.html)

取組の背景と目的

背景	● IoTが進展する中、様々なIoT機器等から収集したデータを、組織横断で活用することが重要になると見られている。 ● 既存のクラウドサービス市場は欧州外のプレイヤーに席巻されている。
目標	● データの主権確立 (data sovereignty：データに対する完全なコントロール及びデータへのアクセス権限に関する自由な決定) ● 特定サービスへの依存の減少 (reduce dependencies) ● より幅広い層に対するクラウドサービスの魅力増進 (make cloud services attractive on a broad basis) ● イノベーションのためのエコシステムの創出 (creating an ecosystem for innovation)
取組	ドイツ、EU規模での安全かつ連携したデータ・インフラの創出 (creating a secure and federated data infrastructure in Germany and in Europe more broadly)

取組の全体像

- Gaia-Xは、複数の異なるクラウドサービス間のリンクとして機能することで、組織を跨いだ安全なデータの共有や各種サービスの利用を可能にする。



出典： ”Project GAIA-X：A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem”

EU-FOSSA project

- EU-FOSSA (Free and Open Source Software Auditing) プロジェクトは、OpenSSLのHeartBleed発覚後に欧州議会の意向を受け欧州委員会によって開始。
- 2017年からのFOSSA2においては、2019年1月より、15のフリーソフトプロジェクト（7-ZIP、Apache Tomcat等）に対する**バグ発見報酬プログラム**を開始。**報酬の合計は851万ユーロ**に上る。他に、ハッカソンの開催や開発者コミュニティとの関係構築を推進。

取組１： 脆弱性発見者への報奨金プログラム	HackerOne、Intigritiなどの脆弱性調整及びバグ報奨金プラットフォームを利用し、EUの機関が使う15のフリーソフトウェアプロジェクトを対象に、バグの発見者に報酬を支払う。
	報酬金はプロジェクトにより異なる。報酬金の合計額が最も高いのはPuTTY（リモートログオンクライアント）の9万ユーロ。金額は重要性などに応じて各プロジェクトが決定する。15プロジェクトの合計は851万ユーロ。バグ発見（バグハント）に加え、バグが修正されると20%のボーナス。
取組２： ハッカソンの開催	2019年4月開催の第1回では、ヨーロッパだけでなくキューバ、モロッコ、ロシア等からも参加。230以上の課題解決につながった。5月の第2回では、Apacheプロジェクトから30人以上が参加すると共に、米国やロシア、クロアチア等、世界中から参加者が集まっている。
取組３： 開発者コミュニティとの関係構築	重要なOSSの開発者コミュニティが抱える問題を把握して支援を行うために、コミュニティとの永続的な関係を構築することが重要であるとし、いくつかのオープンソースプロジェクトやコミュニティに対し、定期的な対話の機会を作るためのアプローチを行っている。また、OSS開発者の支援、コミュニティとの関係構築、及びOSSのセキュリティと整合性の向上を目的とした調査事業が実施されている。

https://ec.europa.eu/info/departments/informatics/eu-fossa-2_en