産業サイバーセキュリティ対策説明会の開催概要

- １１月２８日に行われた説明会には、素材産業や生活製品産業の関係者など約１５０名もの方々に参加いただきました。会場では、サイバー事故が起きたときの対処方法、セキュリティ対策投資を経営層に通すための説明方法など、参加者から活発な質問がありました。
- 今回、ご参加いただけなかった方もおられますので、ご検討の参考になればと思い、説明資料をお送りさせていただきます。貴団体会員の皆様へ共有いただければ幸いです。

産業サイバーセキュリティ対策説明会
日時：１１月２８日（木）１０～１１時
場所：経済産業省　本館地下２階講堂
タイトル：産業サイバーセキュリティ対策強化へ向けて
講師：経済産業省商務情報政策局サイバーセキュリティ課
　　鴨田浩明　企画官

＜ご参考＞
サイバーセキュリティ経営ガイドライン
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

IPA（情報処理推進機構）産業サイバーセキュリティセンター
https://www.ipa.go.jp/icscoe/

経済産業省

産業サイバーセキュリティ対策強化へ向けて

経済産業省　商務情報政策局

サイバーセキュリティ課

業界横断的に対応が求められるサイバー脅威（脆弱性）

- 当省実施の委託調査により、当省所管業界の情報システムにおいて、**業界横断的に特に対応が求められる脅威**が判明。
- **どの脅威も基本的な対策により回避できるもの**であり、**各業界に本脅威情報と対策を周知することで、業界横断的なサイバーセキュリティ対策の底上げが期待**される。

要対応項目:「Patching Cadence」「Network Security」「DNS Health」「Application Security」

「Patching Cadence」
- ソフトウェアプログラムを更新し、修正や機能変更を行うための修正プログラムを適用すること。

「Network Security」
- ネットワーク外部からの不正アクセスを防止し、データの改ざんや情報漏えい、サービスの停止といったセキュリティ事案から情報資源を保護すること。

「DNS Health」
- 「IPアドレス」と「ドメイン名」を組み合わせて管理するシステム（DNS）について、なりすましや不適切な応答を行わないようにセキュリティを確保すること。

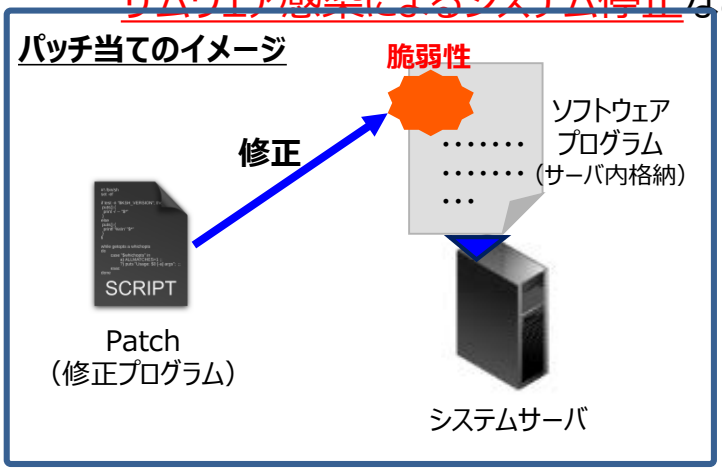
「Application Security」
- アプリケーションに対する脅威からシステムを保護するため、アプリケーション内のセキュリティを確保すること。

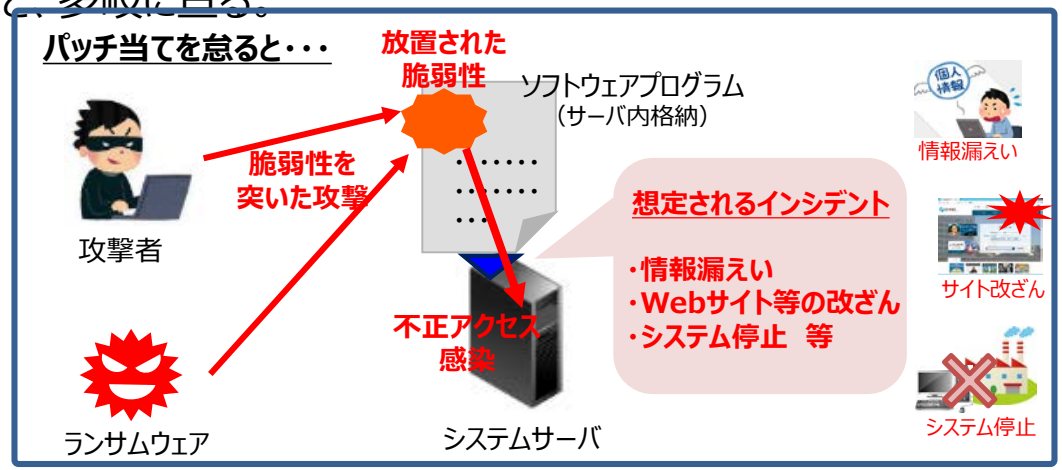
詳細な説明と対策方法例は次ページから。

要対応項目１：Patching Cadence（パッチ当て処理）１

- **Patching（パッチ当て）とは？**　～不具合のあるソフトウェアの応急措置～
  - ソフトウェアプログラムを更新し、修正や機能変更を行うための修正プログラムを適用すること。「パッチを当てる」と表現する。
  - ソフトウェアに脆弱性や問題点が発見された際などに、これらの不具合を解消するための手段として用いられる。

- **Patching（パッチ当て）を怠ると？**
  - つまりはソフトウェアの脆弱性を放置していることに等しいので、あらゆるサイバー攻撃の温床となる。
  - 想定されるサイバー攻撃被害は、不正アクセスによる情報漏えいやWebサイト等の改ざん、ランサムウェア感染によるシステム停止など、多岐に亘る。





要対応項目１：Patching Cadence（パッチ当て処理）２

● Patching（パッチ当て）はなぜ必要か？

– 近年のソフトウェアは、そのプログラムの複雑性から、脆弱性や問題点等の欠陥が存在することは避けられず、それは運用段階になってからも次々と発見される。

– 適時に適正なパッチ当てをすることで、システムの脆弱性の数を減らすことは、サイバーセキュリティ対策の基本。

● Patching（パッチ当て）の主な対策方法は？

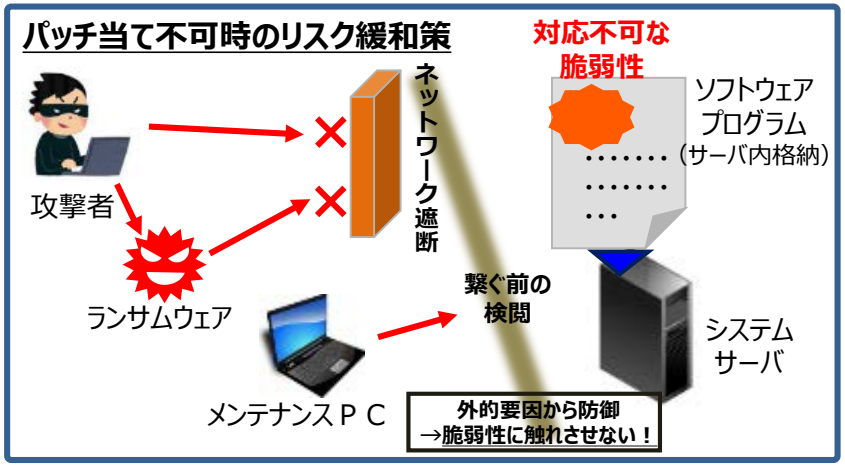
– 最新の脆弱性情報を常に確認し、それに対応する最新のパッチを入手する手段を確立しておく。

– 普段から資産（ソフトウェア等）を把握し、パッチ当ての対象、時期、種類、バージョンを管理しておく。

– 適切なパッチ管理のために、関連作業の手順化、スケジュール化などで業務の効率化を図る。

✓ システム（特に制御系）によっては、カスタマイズや独自で開発したソフトウェアの導入のため、パッチ当てがシステム全体に対して悪影響を及ぼすこともある。

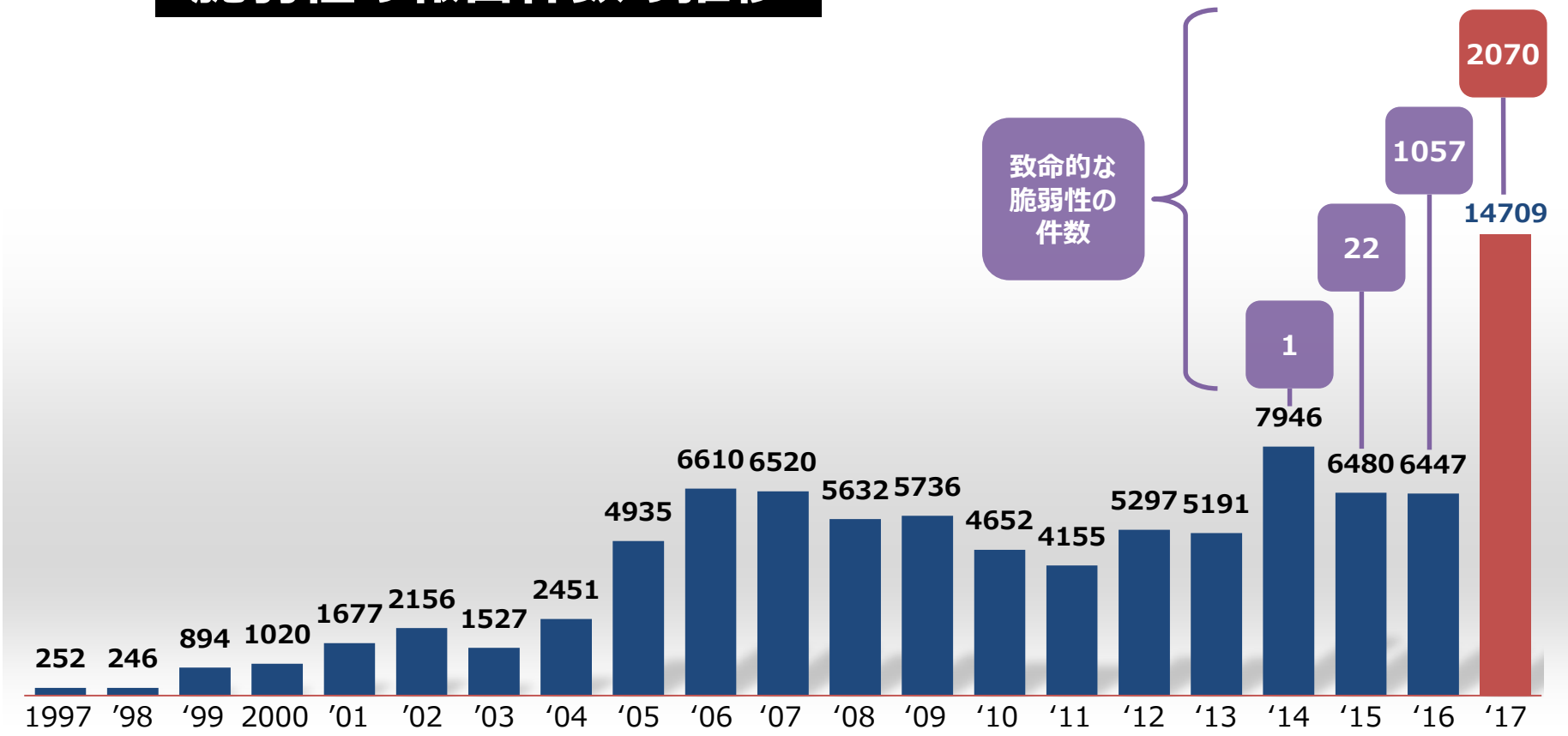
✓ その場合、脆弱性放置によるリスクは許容せざるを得ないが、ネットワークからの遮断やメンテナンスPCの接続制限等、**リスク緩和策**を講じることが重要。



（参考）発見される脆弱性の数は年々増加傾向

- 致命的な脆弱性だけでも、1日あたり 5～6件 が新規に見つかっている

脆弱性の報告件数の推移



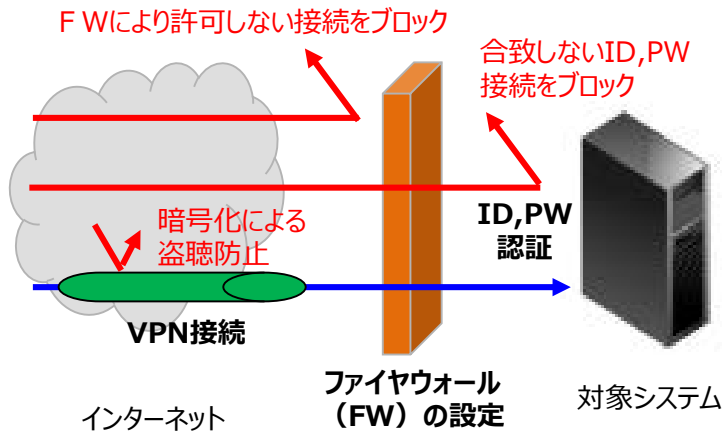
<出典：ESET「Vulnerabilities in 2017 hit an historic peak, smashing previous records」>

要対応項目２：Network Security（ネットワークセキュリティ）１

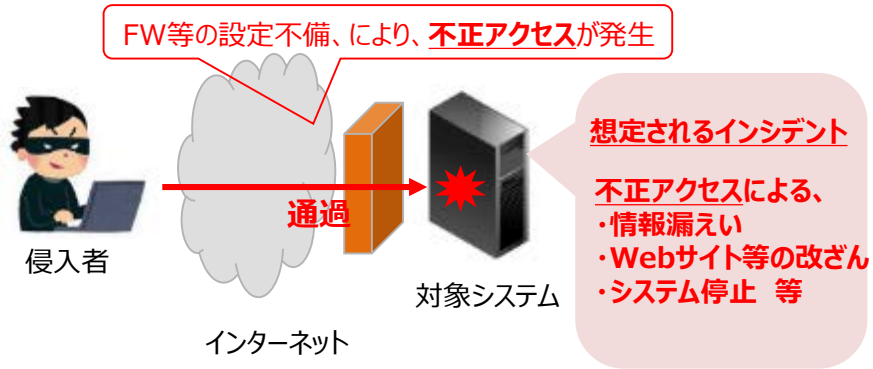
- **Network Securityとは？**　～不正アクセスの防止～
  - 所有する情報資源（システム）をネットワークに接続して様々なサービスを利用する際、ネットワーク外部からの不正アクセスを防止し、データの改ざんや情報漏えい、サービスの停止といったセキュリティ事案から情報資源を保護すること。

- **Network Securityを怠ると？**
  - システム利用の利便性向上にはネットワークへの接続は不可欠である一方、ネットワークセキュリティの不備による情報の漏えい等のセキュリティ事案が後を絶たない状況。
  - 想定されるサイバー攻撃被害は、不正アクセスによる情報漏えいやWebサイト等の改ざんなど。

ネットワークセキュリティのイメージ



ネットワークセキュリティを怠ると・・・



要対応項目２：Network Security（ネットワークセキュリティ）２

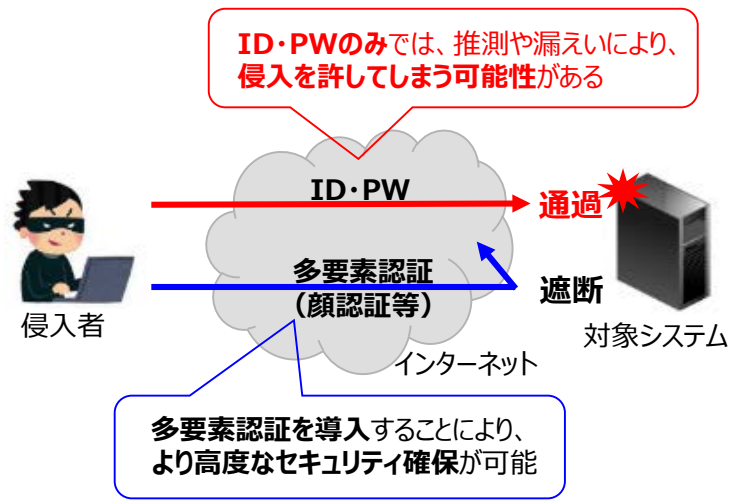
- **Network Securityの主な対策方法は？**

  - アクセスコントロール：IPアドレスによる許可端末の確認や「ID」及び「パスワード」による認証などにより、適切な端末や利用者からの接続かどうかを判断し、不適切な接続をブロックし、制限する。
  - ファイヤウォール：ネットワークの外部と内部の境界に強固な壁を構築して、設定したルールに該当しない接続を防御する。
  - VPN(Virtual Private Network)：端末とネットワーク間を暗号化して接続する。通信が暗号化されているため、仮に途中でインターセプト（盗聴）されても安全である。

✓ 近年、特にクラウドサービスの利用において、「ID」及び「パスワード」のみによる認証では、容易に推測できるパスワードを設定してしまうことや、使い回しされたパスワードの漏えい等により、不正アクセスを許してしまう事案が発生している。

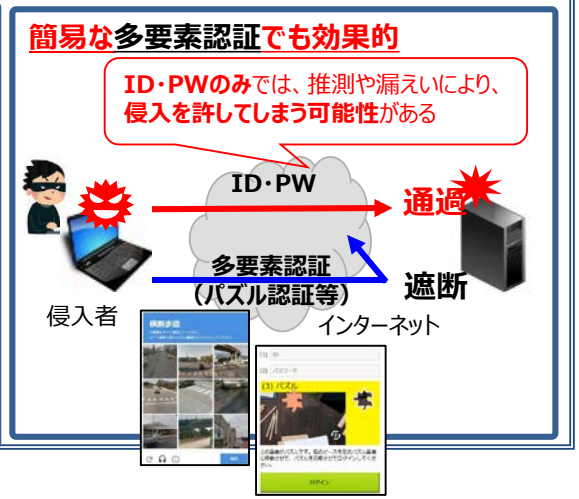
✓ そのため、ワンタイムパスワードや顔認証等も加えた複数の認証（**多要素認証**）を導入することで、より高度なセキュリティを確保することが求められる。

多要素認証の利点



要対応項目２：Network Security（ネットワークセキュリティ）３

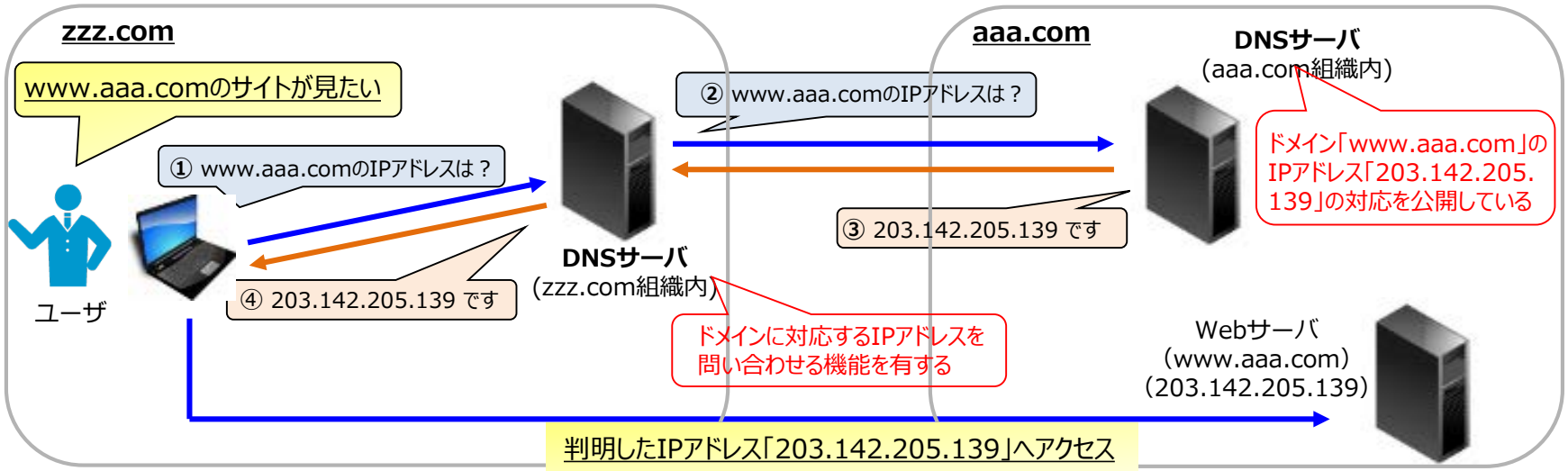
- **最近特に増加しているリスト型攻撃とその対処法は？**
  - 最近特に一般ユーザ向けのWebサイト（会員サービスサイトやショッピングサイト等）において、「ID」及び「パスワード」のみによる認証しか行っていない場合に、不正アクセスを許してしまう事案が多発している。
  - これまでは「ブルートフォース攻撃/辞書攻撃」と呼ばれる、IDとパスワードを総当たりで試す攻撃が多かったため、１つのIDに対して大量のログイン試行と失敗が発生することから検知可能であった。
  - しかし最近は、ユーザが複数のサービスで同じIDとパスワードなどを使いまわす習慣を狙い、他の事案で流出したIDとパスワードがセットとなったアカウント情報リストを利用した「リスト型攻撃」が増えてきている。リスト型攻撃は不正アクセスを許してしまう確率が高く、また１つのIDに対するログイン試行回数が少ないため、攻撃に気付きにくい。
  - 攻撃はロボットプログラムで自動実行されることが多いので、手動動作を必要とするパズル認証を追加するなど簡易な多要素認証を導入することでも、より高度なセキュリティを確保が可能である。



要対応項目３：DNS Health（DNSヘルスチェック）１

- **DNS（Domain Name System）とは？**　～「IPアドレス」と「ドメイン名」の管理～
  - インターネット上で使用する「IPアドレス」と「ドメイン名」を組み合わせて管理するシステムのこと。
    - ✓ 「IPアドレス」は、インターネット上におけるコンピュータ独自の住所。「203.142.205.139」などと表記。
    - ✓ 「ドメイン名」は、IPアドレスが人間に判別できるように付した英数字の記号。「meti.go.jp」などと表記。
  - つまり、コンピュータがインターネット上で扱う「IPアドレス」と、人間の理解できる標記である「ドメイン名」のつなぎ役。インターネット通信において重要な役割を担っている。
  - 特に、メール送信元のドメイン名が詐称されていないかを検査するための仕組みであるSPFは、DNSのこの機能を利用している（詳細は次ページ）。

DNSの仕組み：インターネット通信における名前解決

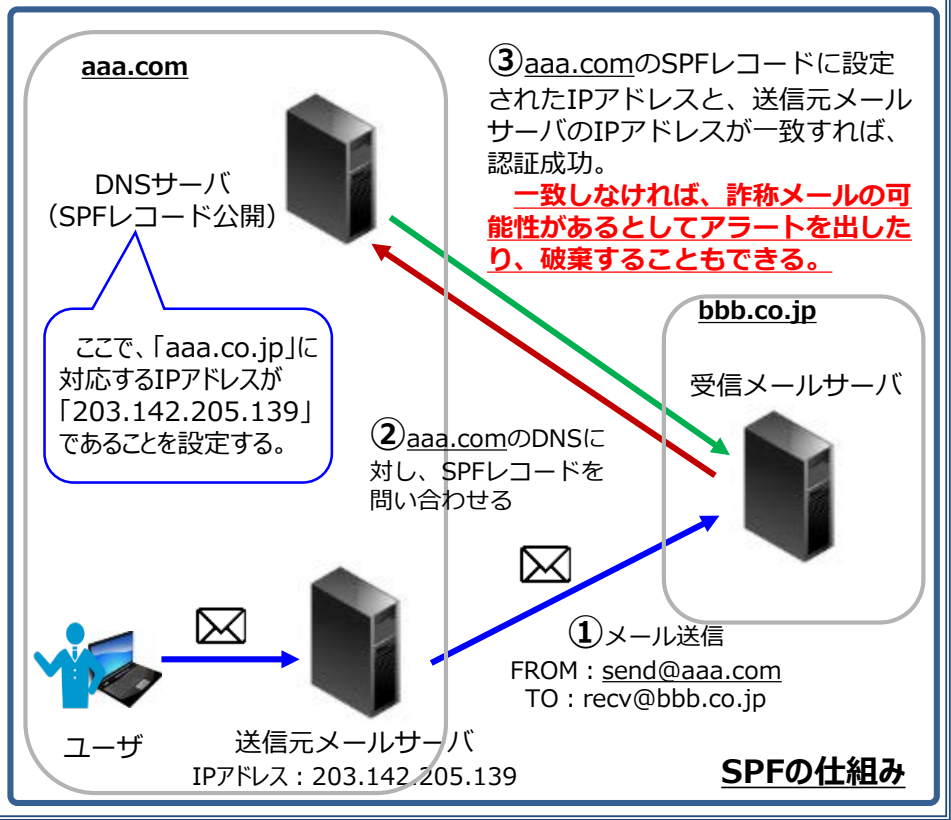


要対応項目３：DNS Health（DNSヘルスチェック）２

- **SPF（Sender Policy Framework）とは？**　～なりすましメールの防止～
  - メールのなりすまし防止やスパムメール対策の一つであり、送られてきたメールが、正規のメールサーバから送信されているかを判断するためのもの。
  - 管理者は、**DNSサーバ（において公開しているSPFレコード）に、メールサーバの「ドメイン名」に対応する「IPアドレス」を記載しておくことで、メール受信者は、正規のメールサーバから送信されたメールかどうか確認できる。**

- **SPFを確認しないと？**
  - 攻撃者は、送信元のメールアドレスを詐称し、送信元になりすましてメールを送付しても、受信者に気づかれにくい。
  - 送信元を詐称された「偽メール」の受信者は、当該メールが信頼できる送信元からのメールであると信じてしまい、悪意のある添付ファイルやURLリンクを疑うことなく開いてしまう可能性がある。

➡ **標的型攻撃の温床となる**

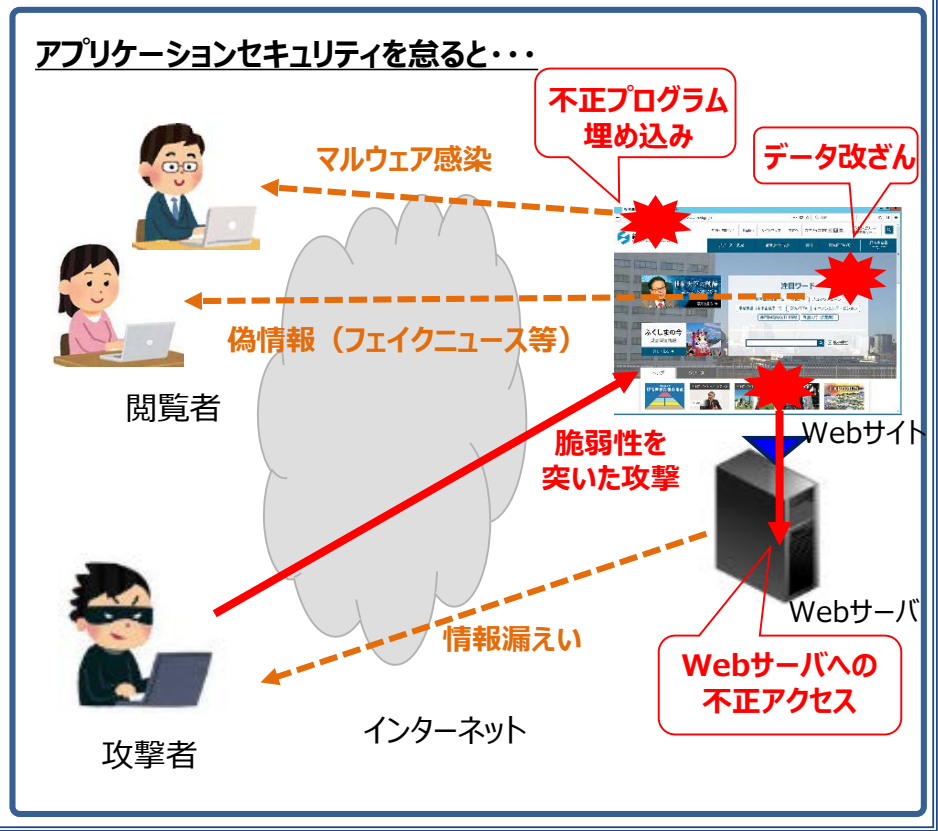


要対応項目４：Application Security（アプリケーションセキュリティ） 1

- **Application Securityとは？**　～アプリケーションの保護～
  - アプリケーション（ソフトウェアの一種で、使用者の業務に応じて作成したプログラム）に対する脅威からシステムを保護するため、アプリケーション内のセキュリティを確保すること。
  - アプリケーションに対する脅威には、DoS攻撃や不正アクセスによる情報漏えいやデータ改ざん等がある。

- **Application Securityを怠ると？**
  - 最近のアプリケーションはネットワーク上で利用可能なものが多く、ネットワーク経由の脅威に晒されている状況。
  - 特に、**Webアプリケーション**（Webサイト等）については、インターネット上での利用が前提であるため、攻撃者の標的になりやすく、セキュリティ事案も日常的に発生している状況。

✓ 2019年以降、日本において国際会議・世界大会が続く。
✓ 日本のWebサイトは大小問わずハクティビストや愉快犯の主張や攻撃力を誇示する場となりやすく、特に警戒が必要。



要対応項目４：Application Security（アプリケーションセキュリティ）２

- **Webアプリケーションにおける主な対策方法は？**
  - Webアプリケーション開発の設計段階から、「脆弱性を作り込まない実装」を実現することが理想。
    - ✓ 具体的には、それぞれの脆弱性の原因そのものをなくす根本的な解決策を講じることで、その脆弱性を狙った攻撃を無効化する。
  - Webアプリケーションを格納するWebサーバのセキュリティ対策も考慮する必要がある。
    - ✓ 具体的には、OSやソフトウェアの脆弱性対応、リモート操作する際の認証機能強化など。
  - 運用段階では、脆弱性診断テスト（Webアプリケーションに内在する脆弱性を、ツールや手動診断により検出する）が有効。疑似攻撃（ペネトレーションテスト）を行うこともある。

✓ Webアプリケーションの脆弱性を利用した攻撃には、
- SQLインジェクション

  →DB不正操作による情報漏えい、データ改ざん
- クロスサイト・スクリプティング

  →不正サイト誘導によるマルウェア感染

などがある。

✓ いずれもよく知られた脅威であり、**基本的な対策で回避できる**ため、対策は必須。

【参考】安全なウェブサイトの作り方（IPA）

「安全なウェブサイトの作り方」は、IPAが届出を受けた脆弱性関連情報を基に作成した、ウェブサイト開発者や運営者が適切なセキュリティを考慮したウェブサイトを作成するための資料。

目次

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

お願いのポイント

■ オリンピック等世界的な注目を集めるイベントに当たっては、**サイバー攻撃が増加**する傾向にある。

■ いわゆる制御系を打ち抜くといった攻撃に加え、**Webの改ざんなど**、提供するサービスに直接影響は与えないが、**社会的な混乱を招くような攻撃を行う愉快犯**が発生する恐れあり。

■ 今回紹介する対策はいずれも基本的なものであるが、調査結果によれば、**日本企業では十分に対策が出来ていない**傾向。

■ このため、各業界においては、前述の問題意識を御理解頂き、**経営層が中心になって対策を実施**していただきたい。

サイバー攻撃の動向

情報セキュリティ10大脅威 2019

昨年順位	個人の脅威	順位	組織の脅威	昨年順位
1位 (*)	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位 (*)	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者の被害	3位	ランサムウェアによる被害	2位
NEW	メール等を使った脅迫・詐欺の手口による金銭要求	4位	**サプライチェーンの弱点を悪用した攻撃の高まり**	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位 (*)	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT機器の不適切な管理	10位	不注意による情報漏えい	12位

(※)クレジットカード被害の増加とフィッシング手口の多様化に鑑み、2018年個人1位の「インターネットバンキングやクレジットカード情報等の不正利用」を本年から、
①インターネットバンキングの不正利用、②クレジットカード情報の不正利用、③仮想通貨交換所を狙った攻撃、④仮想通貨採掘に加担させる手口、⑤フィッシングによる個人情報等の詐取に分割

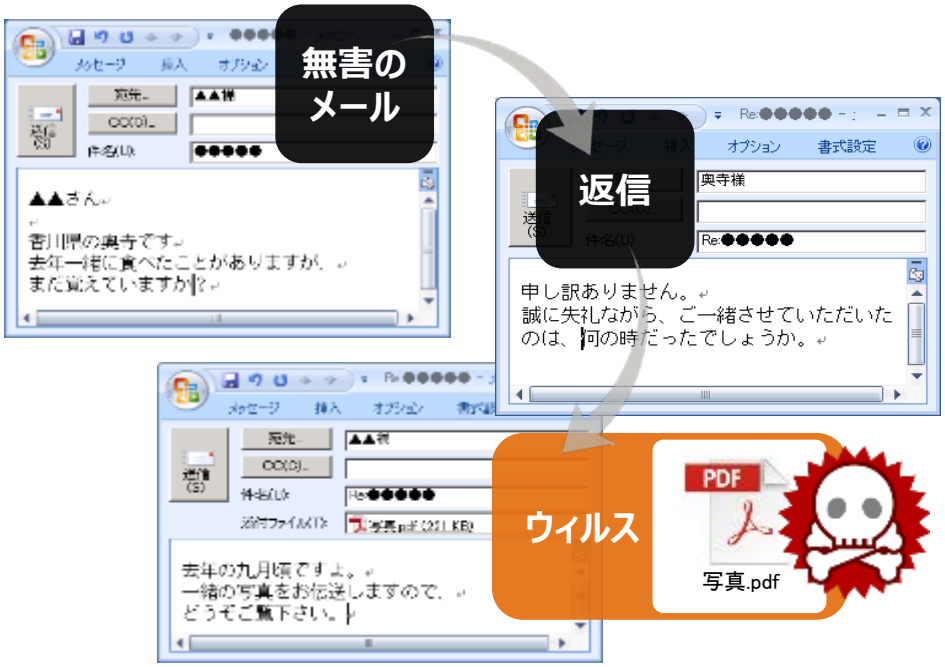
<出典：（独）情報処理推進機構 https://www.ipa.go.jp/security/vuln/10threats2019.html>

標的型メール攻撃による被害

- 添付ファイルやメール本文のリンク先にマルウェアを仕込み、開かせることでコンピュータをマルウェアに感染させる

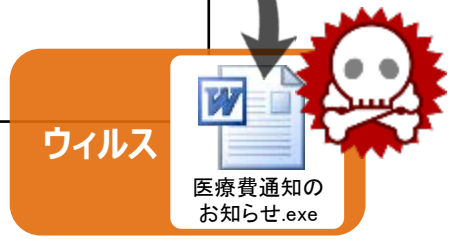
どんなに訓練をしても、メールによる感染を“ゼロ”にはできない

やりとり型



医療費通知を装うメール

差出人	“健康保険組合”
宛先	●●●●様
件名	医療費通知のお知らせ
添付	医療費通知のお知らせ.zip
本メールは、保険を利用して診察や診療を受けられた方に、医療費のご負担等をお知らせしています。	

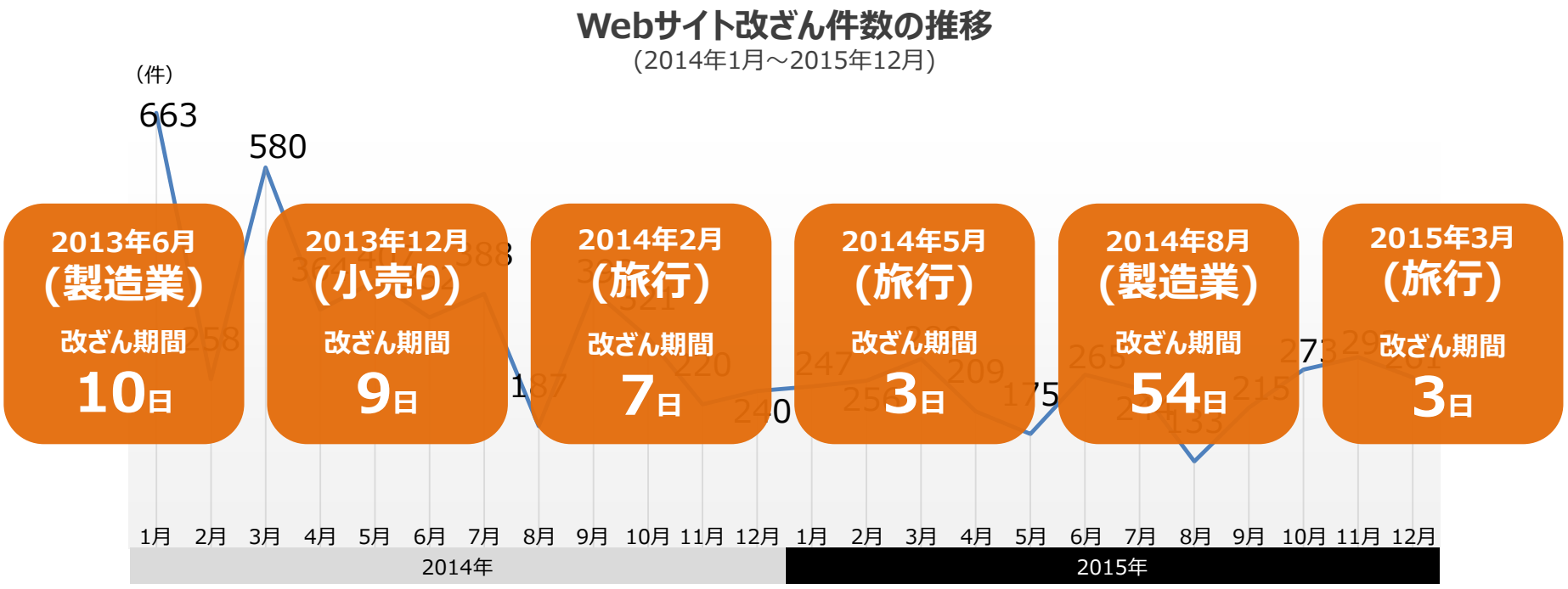


<出典：NHK クローズアップ現代「国家の“サイバー戦争”～情報流出の真相～」2013/6/6放送>

マルウェアの感染経路はメールだけではない

- Webページを閲覧した、ただそれだけで、あなたのパソコンはマルウェアに感染しています

あなたが仕事中に見ているそのWebサイト、本当に安全ですか？



<出典：JPCERT/CC「インシデント報告対応レポート」https://www.jpcert.or.jp/ir/report.html>

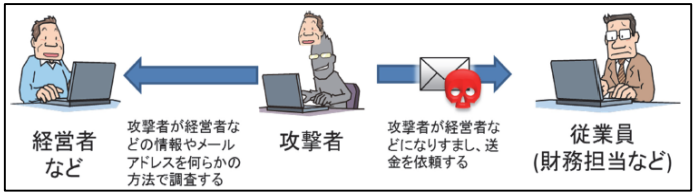
ビジネスメール詐欺

- ビジネスメール詐欺とは、偽の電子メールを組織・企業に送りつけ、従業員を騙して送金取引にかかる資金を詐取するといった、金銭的な被害をもたらすサイバー攻撃。
- 詐取行為の準備として、企業内の従業員などの情報が狙われたり、情報を窃取するウィルスが悪用されることもある。

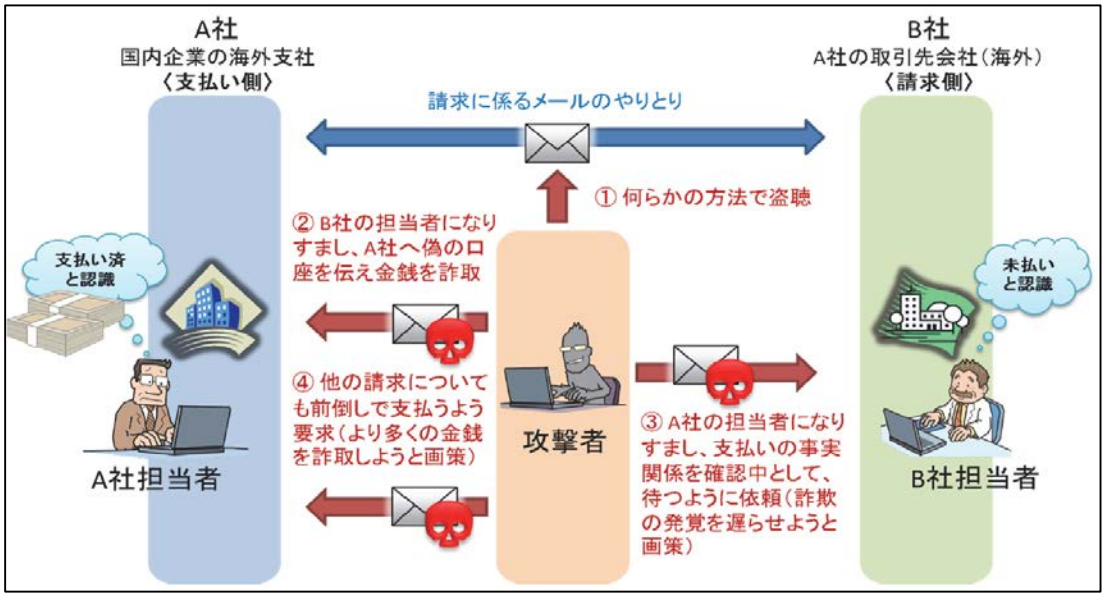
だまされない自信はありますか？

BECの５つのタイプ

タイプ1：取引先との請求書の偽装
タイプ2：経営者等へのなりすまし
タイプ3：窃取メールアカウントの悪用
タイプ4：社外の権威ある第三者へのなりすまし
タイプ5：詐欺の準備行為と思われる情報の詐取



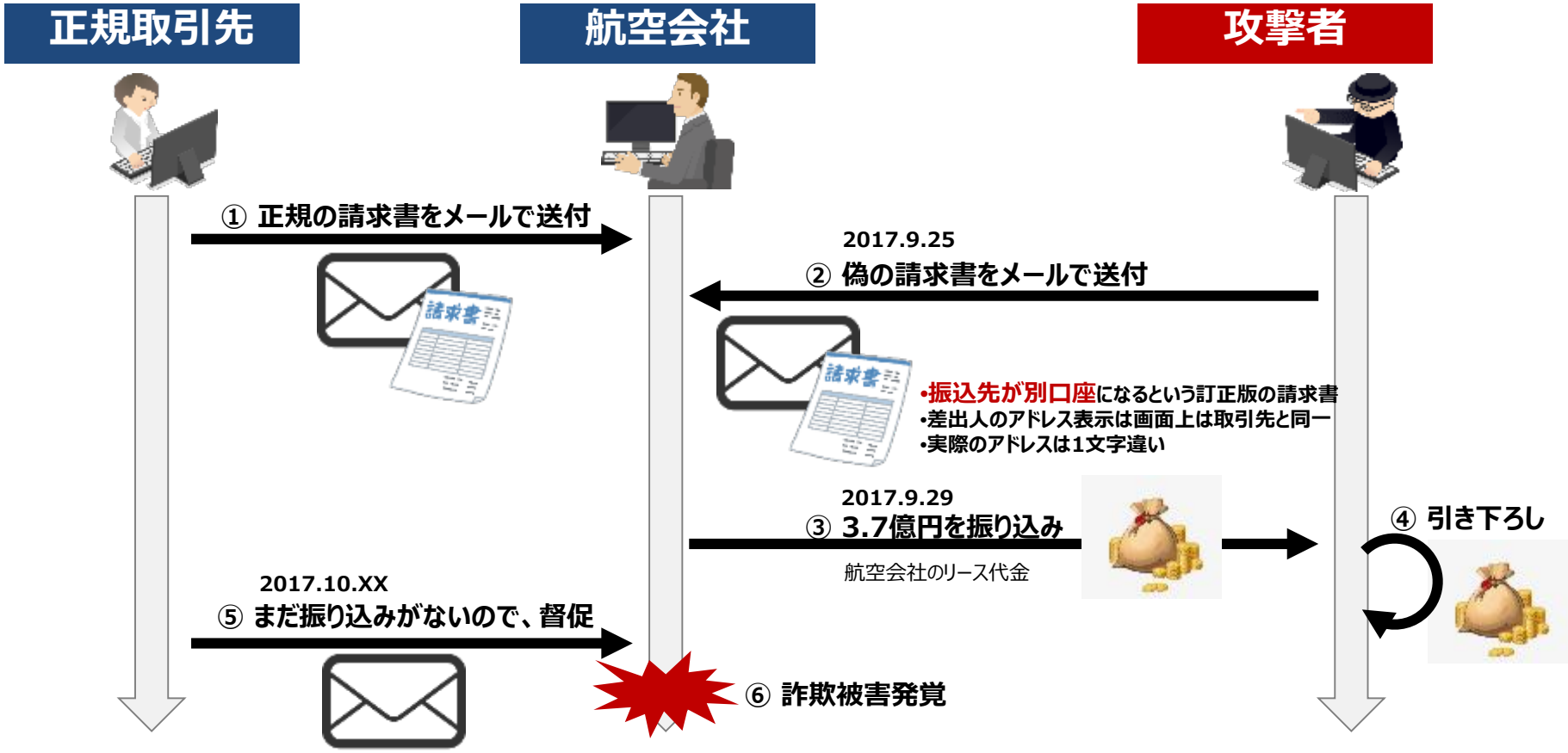
＜事例：海外取引を狙った攻撃＞



＜出典：（独）情報処理推進機構、【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報）＞

ビジネスメール詐欺：航空会社の事例

- 2017年9月 航空会社のビジネスメール詐欺事例



- 上記取引の過程でマルウェアは使用されていない
- 攻撃者が偽の請求メールを送付できるということは、「正規取引先」「日本航空」いずれかのコンピュータが**マルウェアに感染するなどして、メールが盗み取られていた**可能性

ランサムウェアによる被害

- 業務を遂行する上で必要な情報を暗号化された場合、事業継続にも支障がでるおそれのある攻撃。

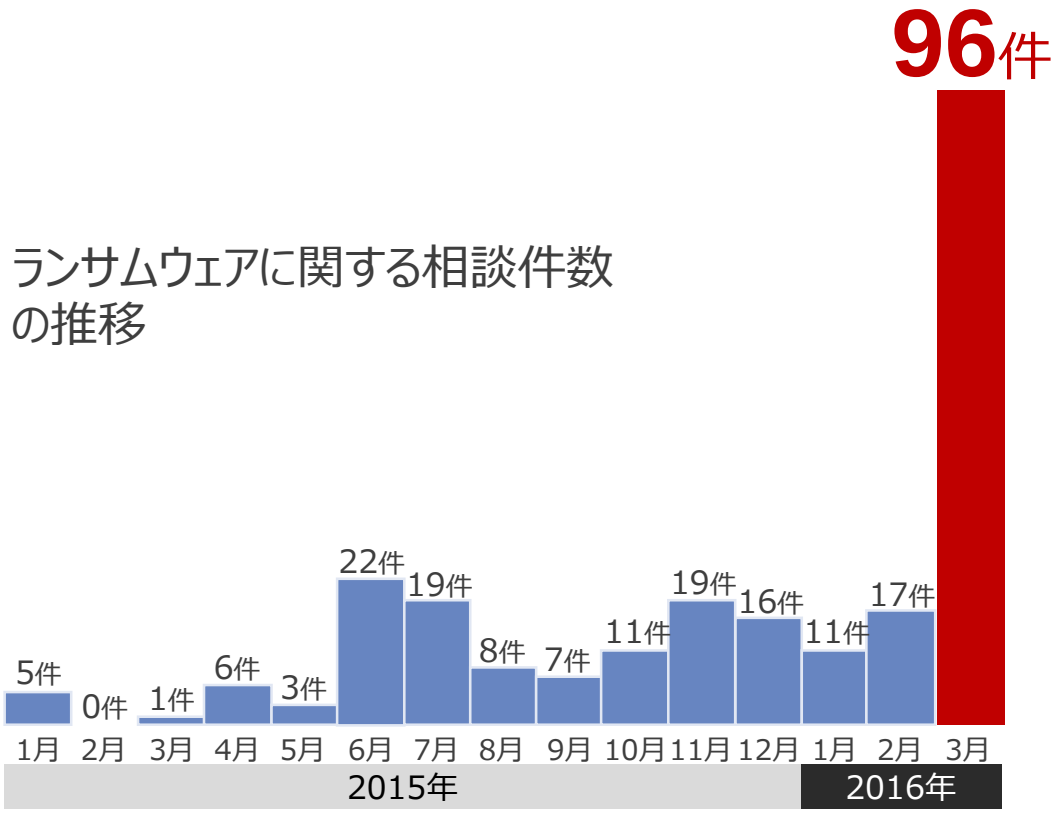
大切なデータを返して欲しければ、金を払え！

ランサムウェアとは、
身代金要求型のマルウェア

ランサムウェアに感染すると、
ファイルが勝手に暗号化され、
開くことができなくなる

攻撃者は、暗号を解くために、
被害者に金銭を要求

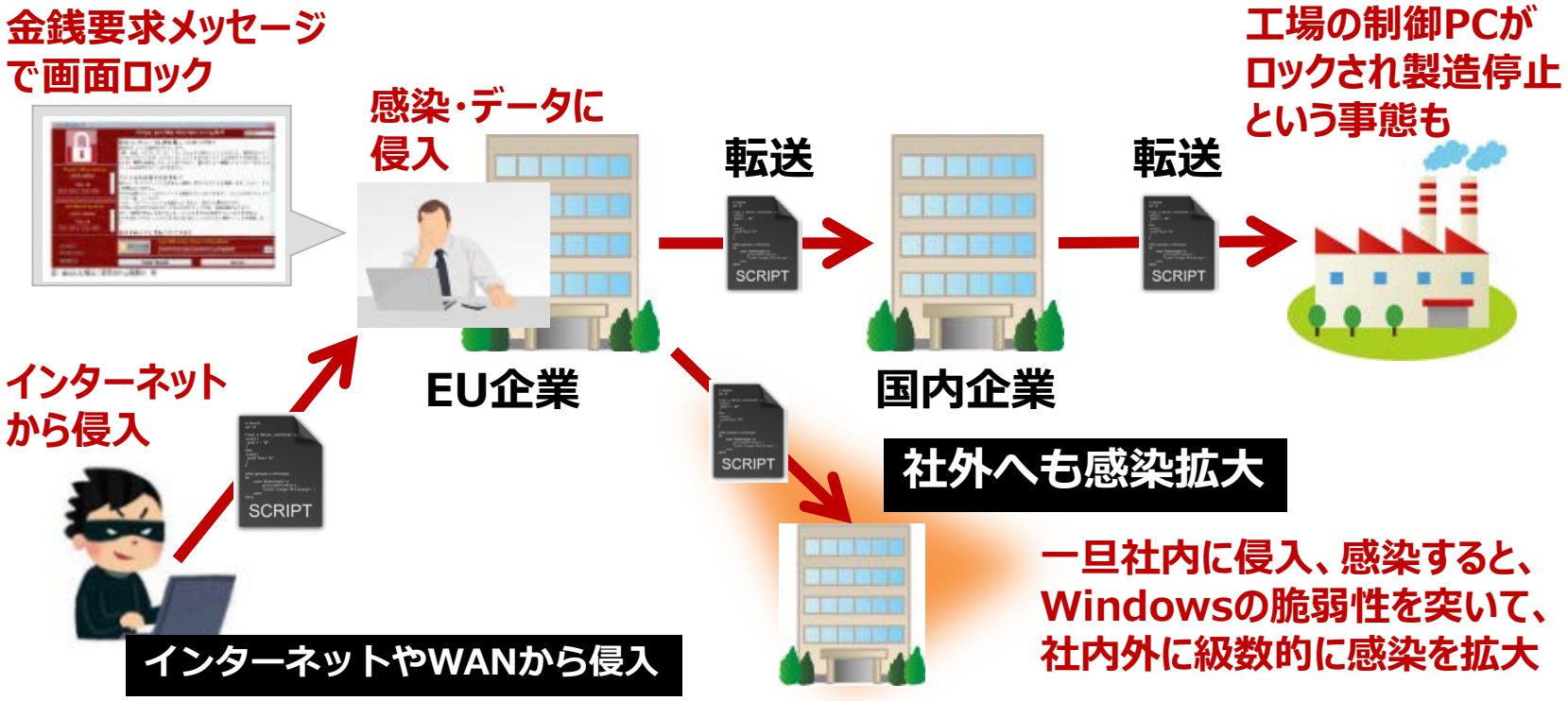
ランサムウェアに関する相談件数の推移



<出典：（独）情報処理推進機構>

サプライチェーンの弱点を悪用した攻撃の高まり

- 平成29年５月、世界の少なくとも約150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
- 感染した欧州企業から、サプライチェーン経由で国内企業も感染。



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。

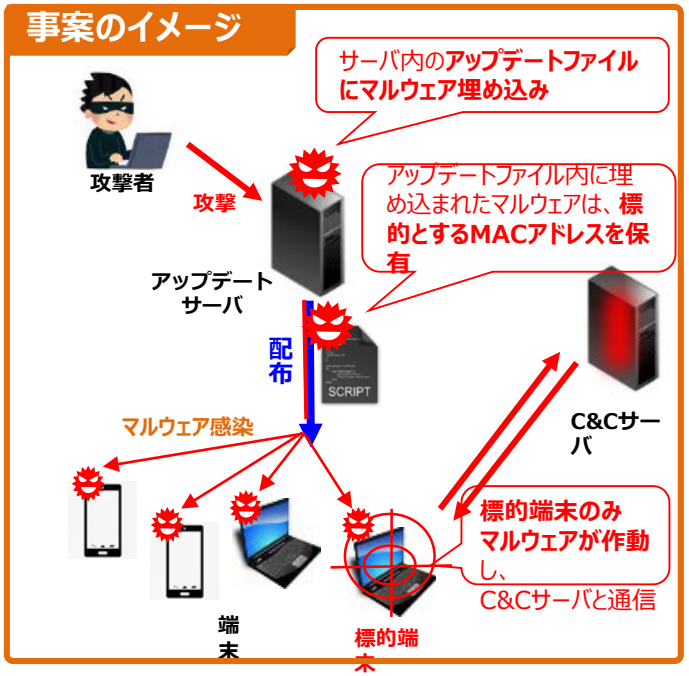
※ Kaspersky社は、200の検体サンプルから600の標的MACアドレスを確認している由

- 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。

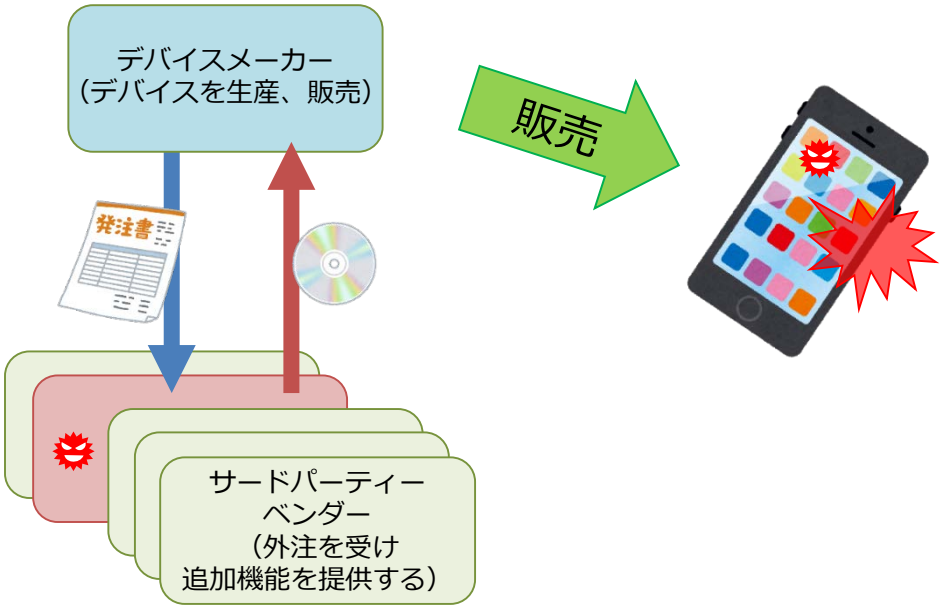
✓ 攻撃者はMACアドレスにより、生産ロット等から標的とする特定の出荷先を絞り込んだものと推測される。

事案のイメージ



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

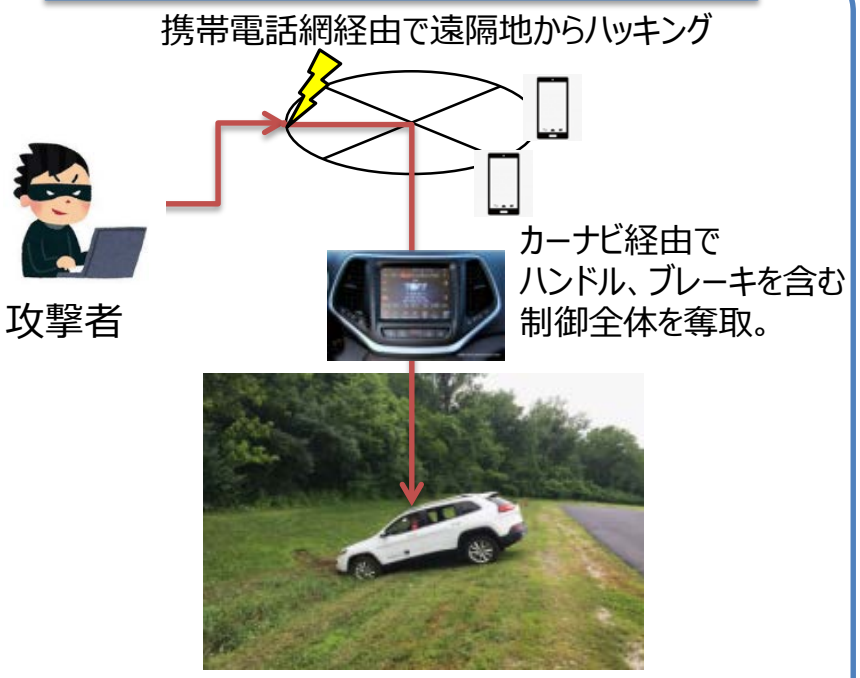
- Triadaは感染したAndroidデバイスに悪意のあるアプリをインストールしたり、スパム広告を表示させたりするマルウェア。
- 2016年に発見された初期のTriadaは、ユーザがTriadaの組み込まれたアプリをインストールすることで感染するタイプであったが、**2017年7月に発見された新種は出荷前のAndroidデバイスにプレインストールされ、ファームウェアのバックドアになっていた**。
- Androidデバイスメーカーから外注を受けた**ソフトウェアベンダーが、ソースコードにTriadaのコードを紛れ込ませていた**と見られている。



IoTの進展に伴う新たなセキュリティ上の脅威：新たにつながるデバイス

- これまでネットワークに接続されていなかった自動車やカメラなどの機器が、WiFiや携帯電話網などを介してインターネットに接続されることにより、新たな脅威が発生し、それに対するセキュリティ対策が必要となった。

自動車へのハッキングよる遠隔操作



人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

監視カメラの映像がインターネット上に公開

セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。

IoTの進展に伴う新たなセキュリティ上の脅威：ドローン・航空機の脅威

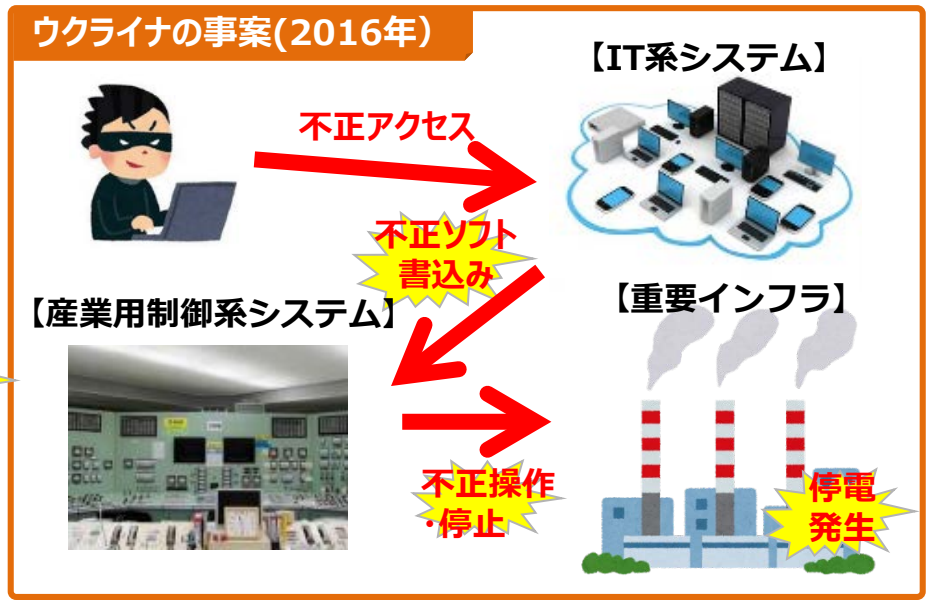
- 2012年、テキサス大学オースティン校の研究グループが**GPS信号を用いてドローンのハッキング**に成功。また、2018年に横浜国立大学の研究グループは、**超音波によりドローンの超音波距離計を攪乱**させ、制御を喪失させることを実証。
- 米国国土安全保証省（DHS）でも、2016年に民間航空機のサイバーセキュリティ脆弱性評価において、遠隔からのボーイング757のハッキングに成功し、民間航空機のサイバー攻撃に対する脆弱性を認識。

テキサス大学の実験

横浜国立大学の実験

制御系にも影響が波及：制御系システムへのサイバー攻撃

- 米国ICS-CERTは、**米国の重要インフラへのサイバー攻撃のうち一割は、制御系まで到達**していると報告。
- ドイツ情報セキュリティ庁（BSI）は、2014年にドイツの製鉄所において、外部からの制御システムの**不正操作により溶鉱炉が制御不能**となり、生産設備に甚大な損傷が発生したと報告。
- ウクライナでは、2015年と2016年にサイバー攻撃による停電が発生。検体検査の結果から、**2016年の攻撃(CrashOverRide)** は、**サイバー攻撃のみで停電が起こされた可能性があると報告されている。**



（出典）IT Security Situation in Germany 2014 （BSI）に基づき経済産業省作成
（図は参考）https://www.jiji.com/jc/v2?id=20110311earthquake_25photo，https://upload.wikimedia.org/wikipedia/commons/1/1f/Alto_horno_antiguo_Sestao.jpg

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**。

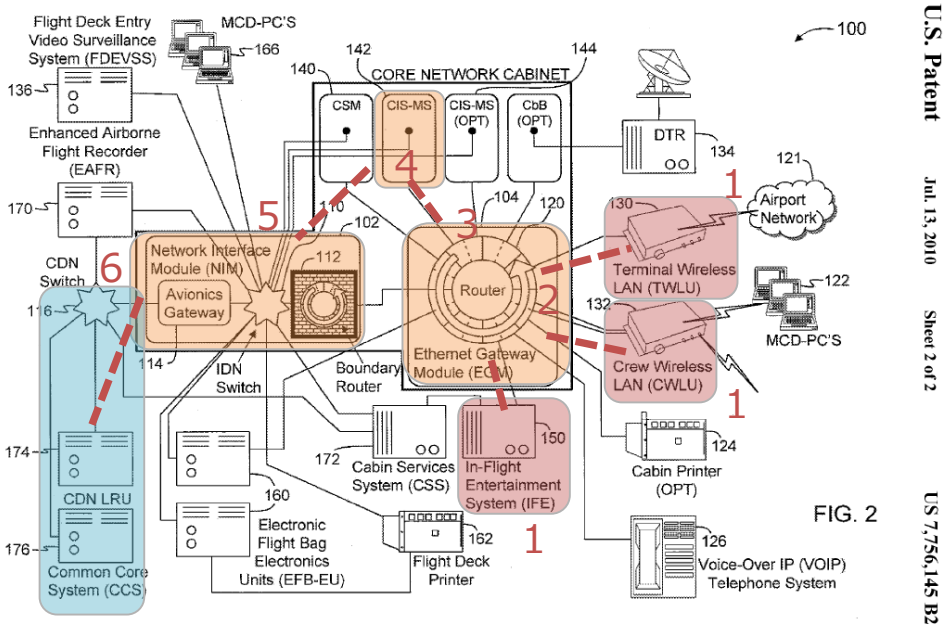


FIG. 2

●基本的な攻撃対象の解説図

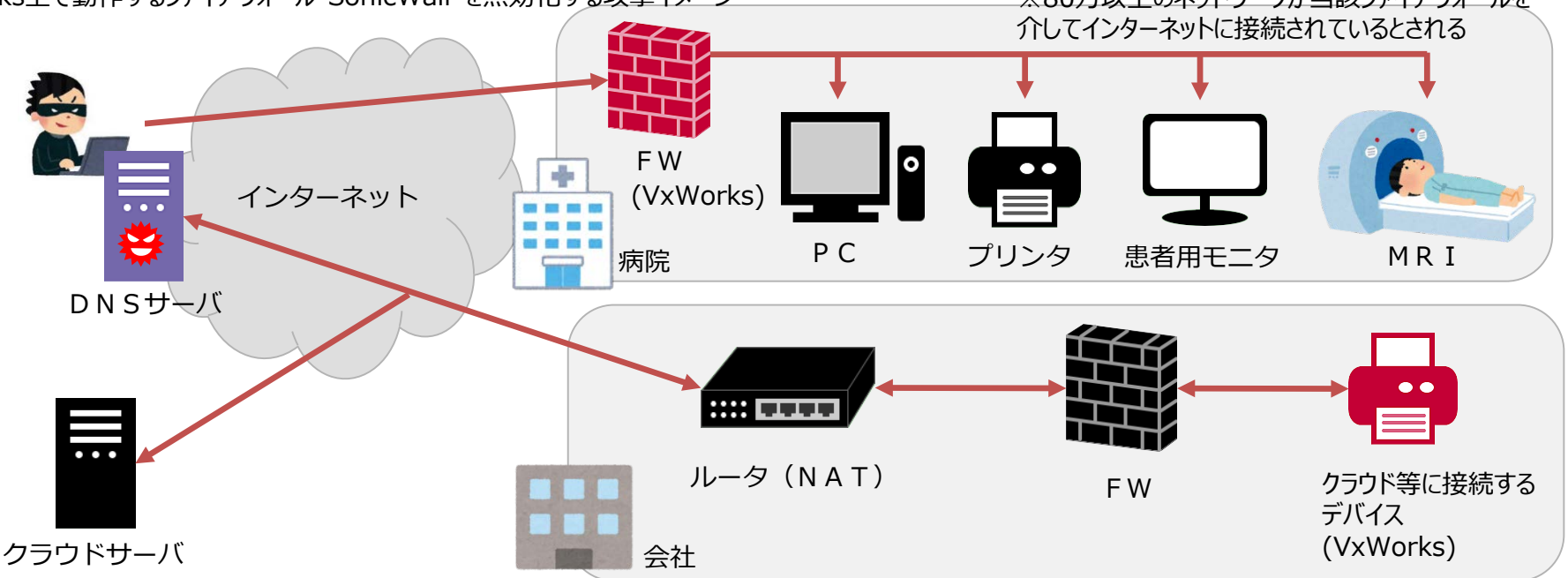
1の機内エンターテイメントシステムや外部ネットワークから、6の機体の操作やナビゲーションに関連するとされるネットワークに到達できると解説されている。

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

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



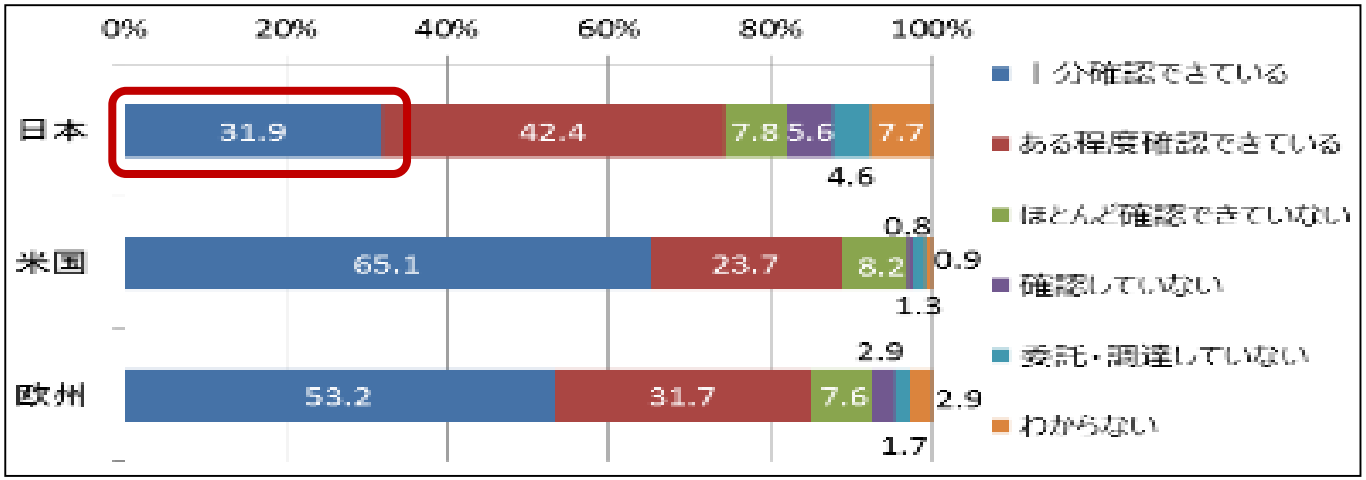
クラウドサービスとの通信の中間者となり境界セキュリティをバイパスしてVxWorksデバイスを攻撃するイメージ

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

取引先へのサイバーセキュリティ対策の遅れ

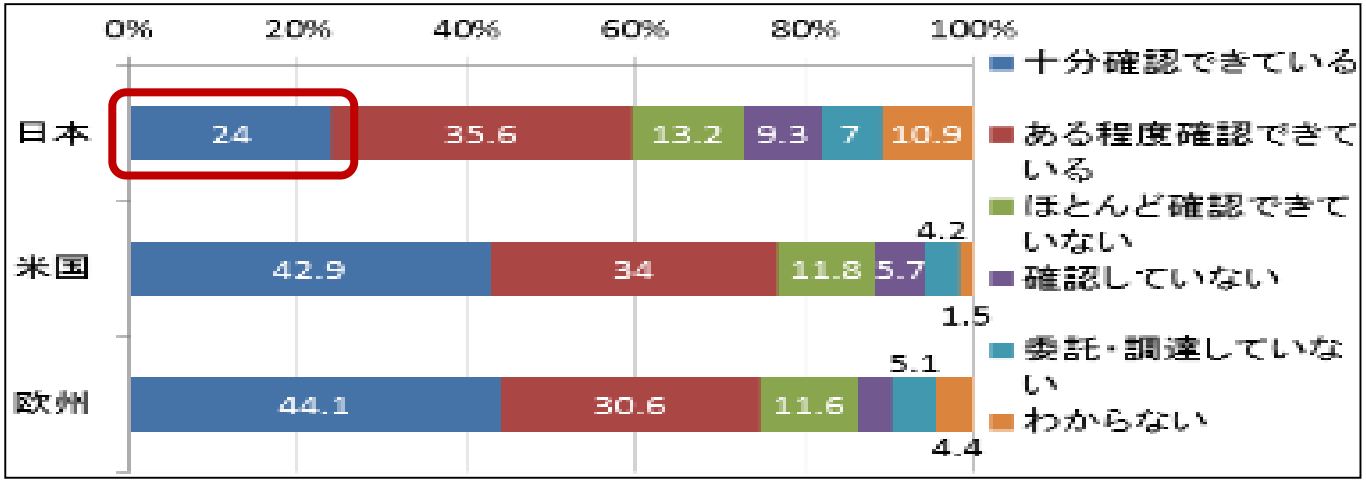
- 日本企業では、委託先等の取引先への対応が大幅に遅れている

■委託先のセキュリティ対策状況把握（業務委託先）



状況把握は
- **米国の半分以下**
- **欧州の2/3**

■委託先のセキュリティ対策状況把握（物品調達先）



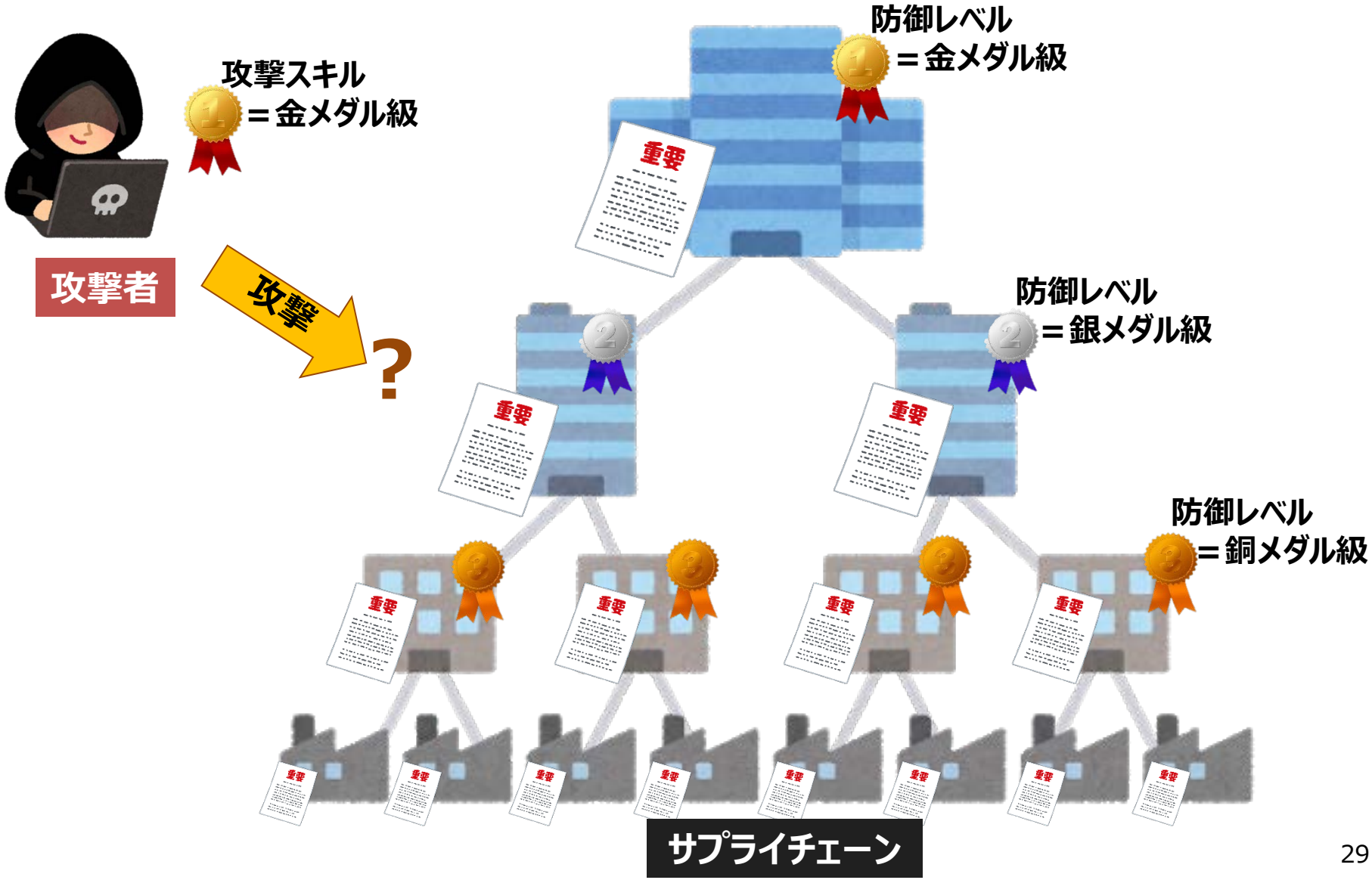
状況把握は
- **欧米の6割以下**

出典：独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017-調査報告書-」（2017年4月13日）

＊日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）。 回収は日本755件、米国527件、欧州526件。

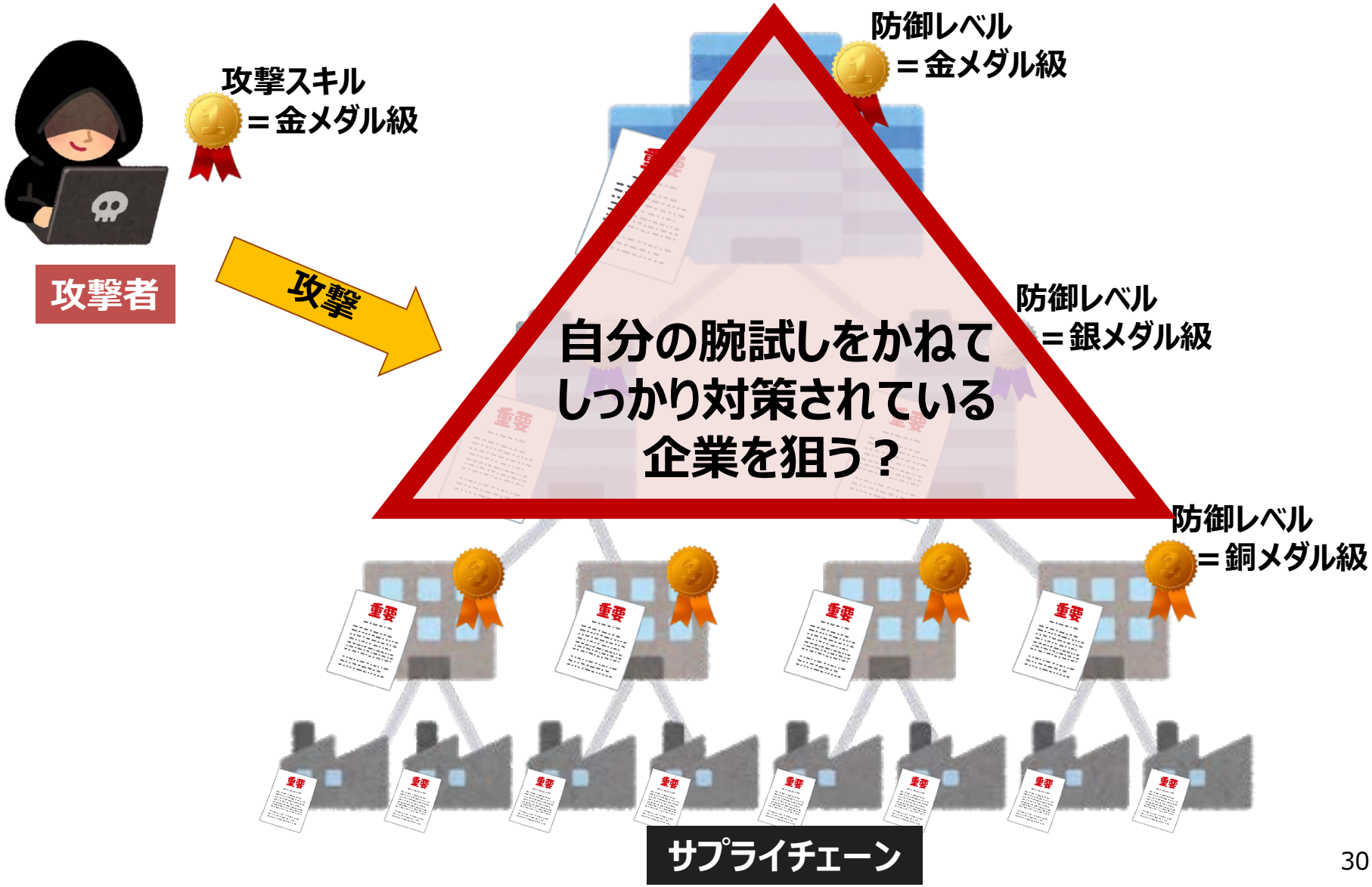
攻撃者はサプライチェーンのどこを狙うか

- 企業の対策レベルはバラバラだが、「金（カネ）」になる重要情報は至る所に存在する。



攻撃者はサプライチェーンのどこを狙うか

- 企業の対策レベルはバラバラだが、「金（カネ）」になる重要情報は至る所に存在する。

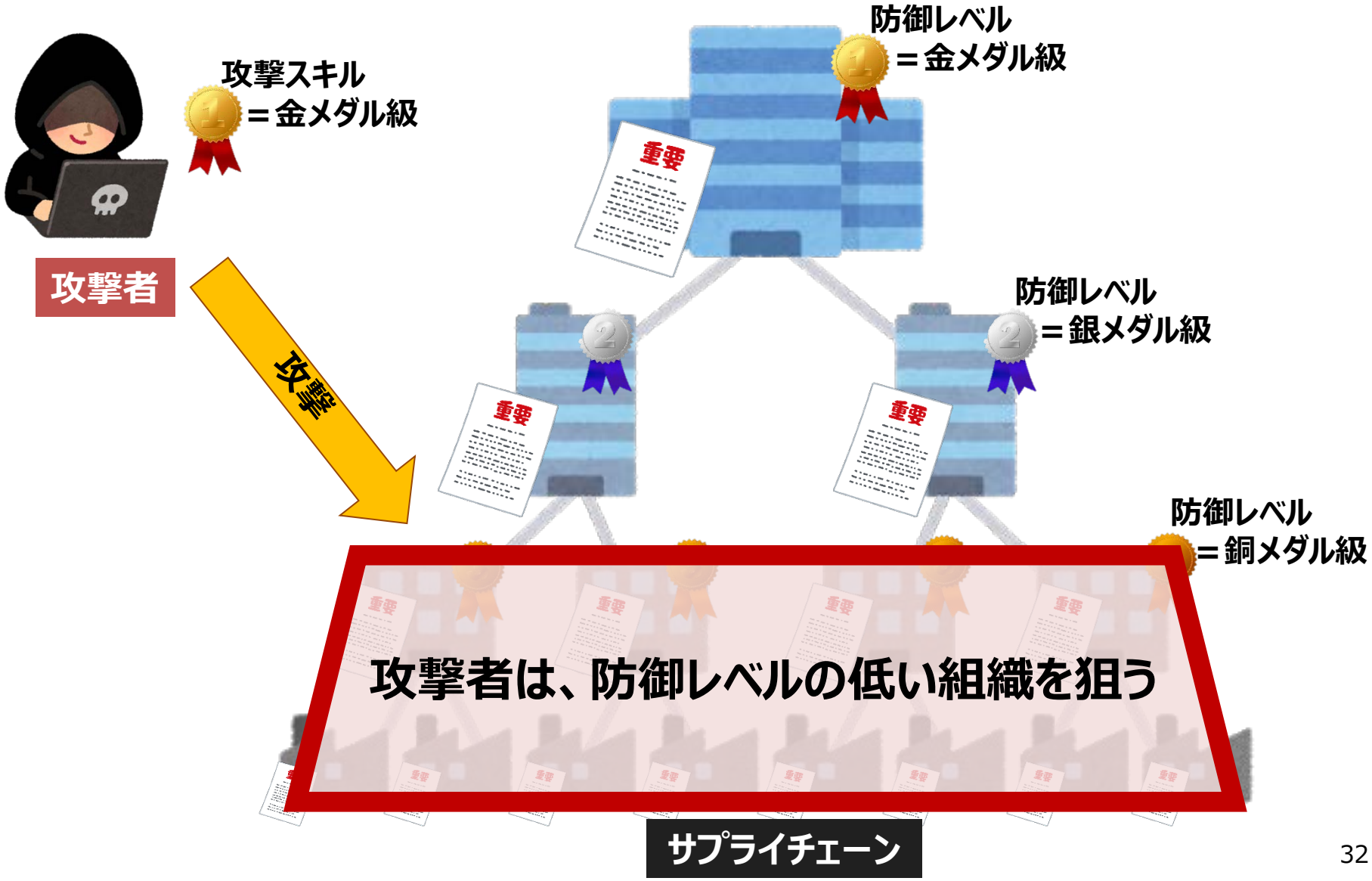


答：いいえ

- 防御レベルの高いシステムの攻撃に失敗すると、**攻撃の痕跡**が残ります
- 攻撃者は、**痕跡を残すことを嫌います**
- 攻撃者にとってリスクの低い**防御レベルの低い企業が標的**になります

攻撃者はサプライチェーンのどこを狙うか

- 企業の対策レベルはバラバラだが、「金（カネ）」になる重要情報は至る所に存在する。



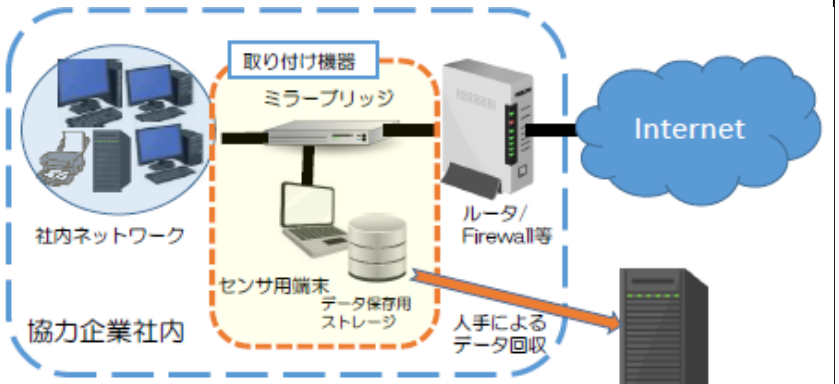
中小企業に対するサイバー攻撃の調査･分析結果（大阪商工会議所）

● 地域の中小企業も、例外なくサイバー攻撃の脅威にさらされている

中小企業被害実態に関する調査

■調査内容

実証期間：平成30年9月～平成31年1月
実証内容：中小企業30社を対象に、ネットワーク上の通信データ等を一定期間収集。



解析システムネットワークのイメージ

■ 調査結果（中間報告）

- 調査した**30社全てでサイバー攻撃**を受けていたことを示す不審な通信が記録されていた。
- 少なくとも5社ではコンピューターウイルスに感染するなどして、**情報が外部に流出したおそれ**があることが分かった。

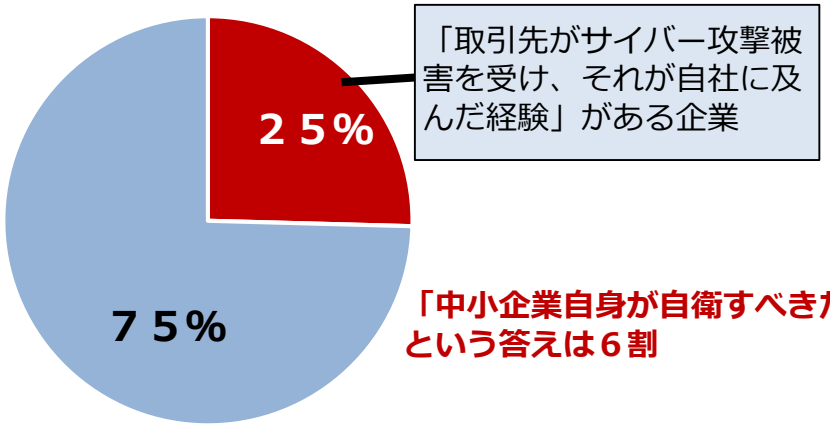
取引先経由の被害に関する調査

■調査内容

調査期間：平成31年2月～3月
調査内容：全国の従業員100人以上の企業を対象に、郵送、FAX、メール、Web、対面による依頼･回答

■調査結果（中間報告）

- 大企業･中堅企業118社に調査したところ、取引先がサイバー攻撃被害を受け、**影響が自社に及んだ経験**がある企業が30社あった（**25%**）



「中小企業自身が自衛すべきだ」という答えは６割

出典：大阪商工会議所「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」（2019年5月）

<出典：大阪商工会議所「平成30年度中小企業に対するサイバー攻撃実情調査（報告）」共同研究実施者：神戸大学、東京海上日動火災保険（株）(2019年7月）>

中小企業の被害事例

● 重要インフラや大企業だけでなく、中小企業においてもサイバー攻撃の被害は発生。

	事例	業種	所在地	従業員規模
ウィルス感染	従業員が**メールに添付されていたファイルを不用意に開き**、当社の基幹システムの設定が書き換わる障害が発生した。 システムベンダの協力を得て障害の調査を行い、復旧するまでの**1週間ほど、基幹システムの一部が使用できなくなった**。	製造業	静岡県	５１～１００名
	役員のパソコンが**ウイルスに感染**し、保存されていた過去の電子メールが、これまでの送受信先などに大量に送信され、自社および取引先の**重要な情報が漏洩**してしまった。取引先からはクレームが上がり、謝罪をしたものの**信頼を失墜**することとなった。	製造業	栃木県	５１～１００名
	ウイルス対策ソフトの契約更新を失念し、数日間サポートが切れた。そのわずかの間に、インターネットに繋がっていたPCが**「トロイの木馬」に感染**した。 急ぎアプリケーションを停止し、自社でリカバリーしたが、**復旧までに約2か月**を要し、その間、仕事にも支障をきたした。	卸売業	福岡県	２１～５０名
ランサムウェア	ある日届いた経営者宛の**メールに添付されているファイルを開いて**しまった結果、「ファイルをロックしたので、解除して欲しければ連絡をするように」と電話番号を含む**警告画面がパソコンのスクリーン上に表示され消えなくなった**。 社内の重要データは共有サーバで管理されており、**バックアップ等を行っていた**ため会社としての被害はなかったが、個人の写真などのデータは参照できなくなっていた。	製造業	神奈川県	６～２０名

<出典：IPA 2016年度中小企業における情報セキュリティ対策の実態調査>

サプライチェーン経由で発生する事故

- 取引先も含めてセキュリティを確保することが重要。
- 自社が対策をしていないことで**委託元に迷惑**をかけてしまう可能性もある。

公表年	委託元業種	被害内容	原因
2013	卸売業、小売業	会員の個人情報が改ざん。**約２ヶ月間サービス停止**。	**委託先が管理**するWebサイトが不正アクセスを受けた。
2014	情報通信業	Webサイト内のファイルが改ざん。オンラインバンキングで不正送金を行うマルウェアが設置され、当該**マルウェアが委託元製品の顧客に数千件ダウンロードされた**。サービスの再開にあたってWebサイトの委託先を別企業に変更した。	ダウンロードサービスを委託している**委託先のWebサイト**が不正アクセスを受けた。
2015	卸売業、小売業	ECサイトの会員の個人情報が漏洩。事故の発表後、委託元企業の**株価が３日間下落し、年初来安値を更新**。	**再々委託先が管理**するサーバが不正アクセスを受けた。
2016	その他サービス業	顧客の個人情報が漏洩。事故の影響もあり、**販売数が前年比1割減**となった。	**委託先の端末**がマルウェアに感染し、攻撃者が個人情報のあるサーバに侵入した。
2017	国家公務、地方公務	救急医療機関等の情報を掲載しているWebサイトの内容が改ざん。再発防止策実施までの間、**Webサイトの公開を停止**した。	**委託先が類推可能なIDとパスワードを利用**していた。

サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
平成28年12月8日改訂（Ver.1.1）
平成29年11月16日改訂（Ver2.0）

● セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドラインを公表

概要

経営者が適切なセキュリティ投資を行わないと…

- 社会からリスク対応の是非が問われる
- 経営責任や法的責任が問われる
- 国際的なビジネスに影響をもたらす

セキュリティ対策の実施を
「コスト」と捉えるのではなく「投資」と捉える

経営戦略としての**セキュリティ投資は必要不可欠**
かつ**経営者としての責務**

経営者が認識する必要がある 三原則

経営者は
サイバーセキュリティリスクを
認識し
リーダーシップによって
対策を進める
ことが必要

自社は勿論のこと
ビジネスパートナーや
委託先も含めた
サプライチェーンに対する
セキュリティ対策
が必要

平時および
緊急時のいずれにおいても
サイバーセキュリティリスクや
対策に係る情報開示など
関係者との
適切なコミュニケーション
が必要

サイバーセキュリティ経営ガイドライン

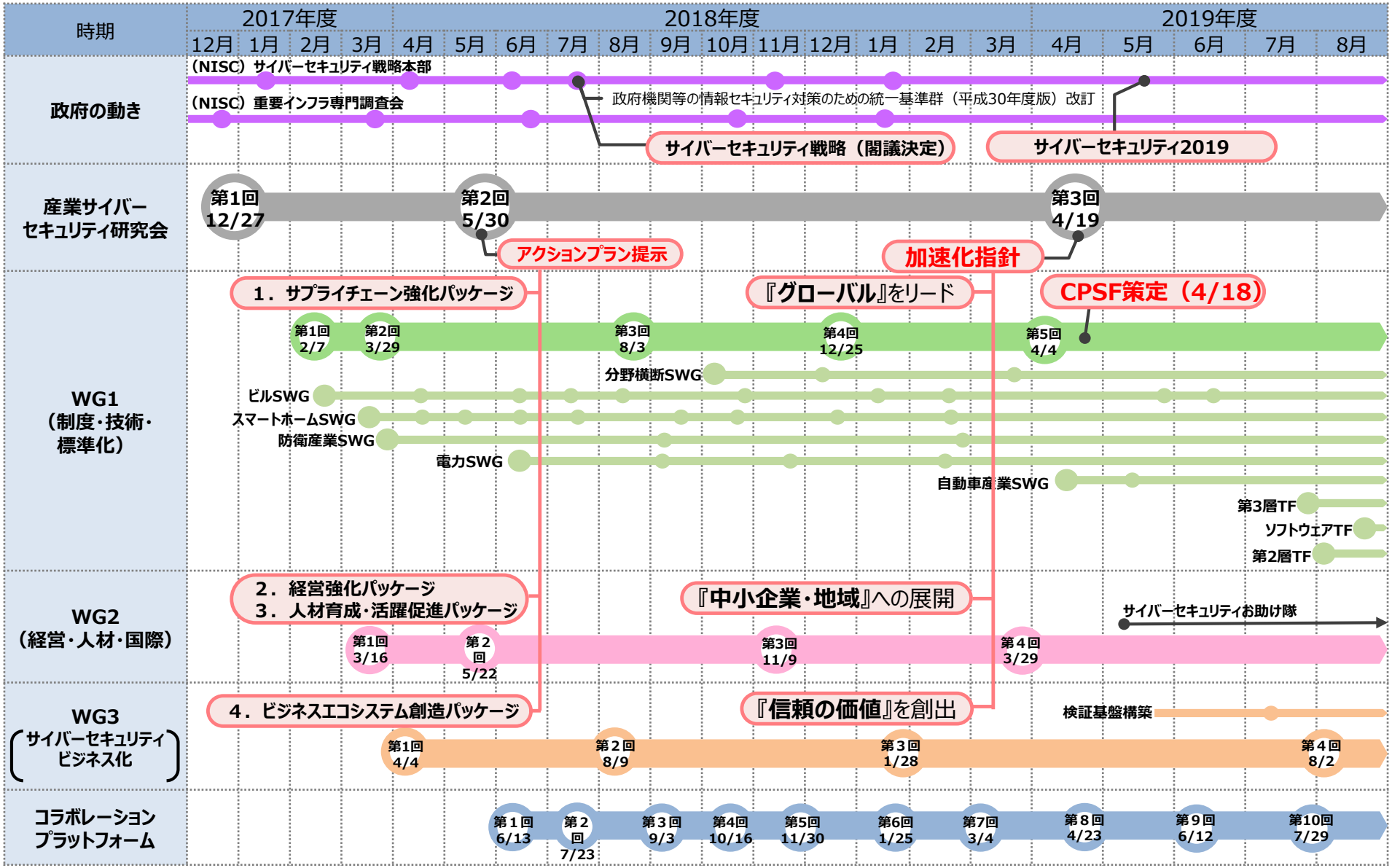
平成27年12月28日策定
平成28年12月8日改訂（Ver.1.1）
平成29年11月16日改訂（Ver2.0）

- 経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき**重要10項目**

指示 1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示 2	サイバーセキュリティリスク管理体制の構築
指示 3	サイバーセキュリティ対策のための資源（予算、人材等）確保
指示 4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示 5	サイバーセキュリティリスクに対応するための仕組みの構築
指示 6	サイバーセキュリティ対策におけるPDCAサイクルの実施
指示 7	インシデント発生時の緊急対応体制の整備
指示 8	インシデントによる被害に備えた復旧体制の整備
指示 9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策および状況
指示 10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用および提供

（参考①）
産業分野毎の産業サイバーセキュリティ対策の強化へ向けた取組について

産業サイバーセキュリティ研究会関連の動き



産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
アクションプランを加速化する３つの指針を提示

構成員

※2019年4月開催時点

石原　邦夫	日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、東京海上日動火災保険株式会社相談役
泉澤　清次	三菱重工業株式会社取締役社長
遠藤　信博	日本経済団体連合会情報通信委員長、日本電気株式会社会長、サイバーセキュリティ戦略本部員
小林　喜光	経済同友会代表幹事、株式会社三菱ケミカルホールディングス取締役会長
篠原　弘道	日本電信電話株式会社取締役会長
中西　宏明	株式会社日立製作所会長
船橋　洋一	アジア・パシフィック・イニシアティブ理事長
村井　純(座長)	慶應義塾大学教授、サイバーセキュリティ戦略本部員
渡辺　佳英	日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

オブザーバー

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

WG１（制度･技術･標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日

１．サプライチェーン強化パッケージ

WG２（経営･人材･国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日

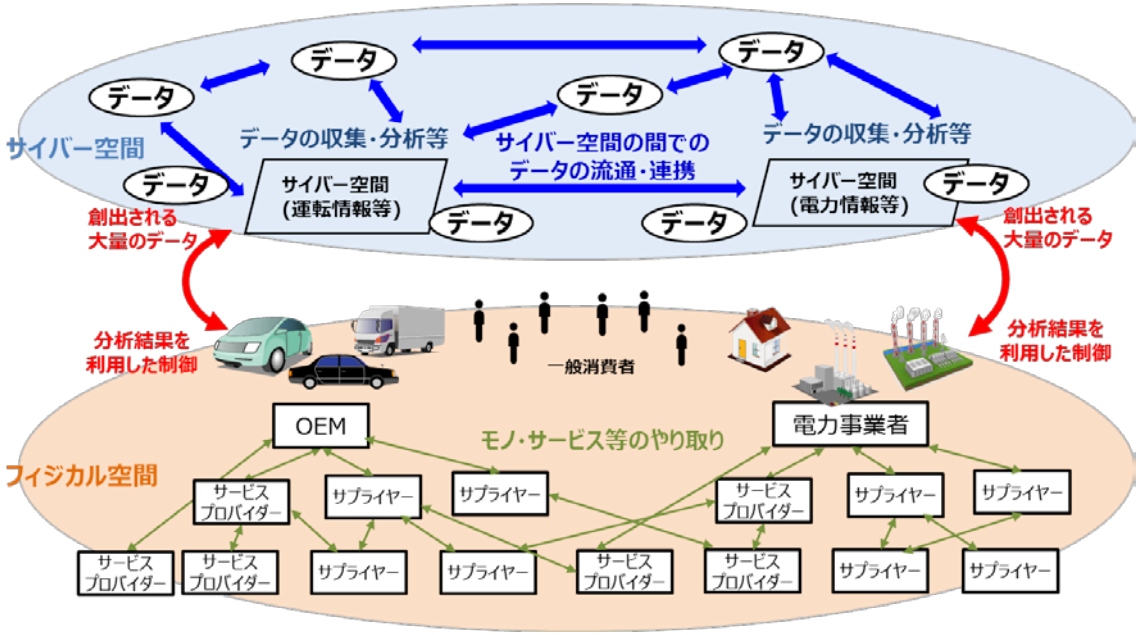
４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

＜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。

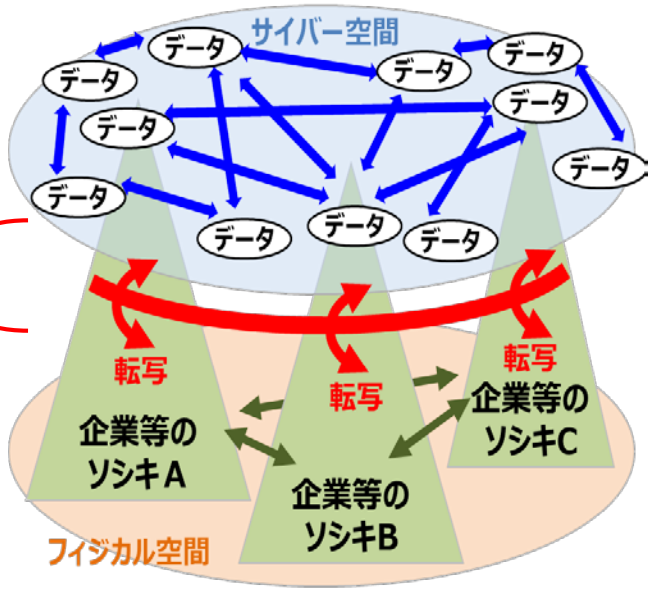
三層構造

「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



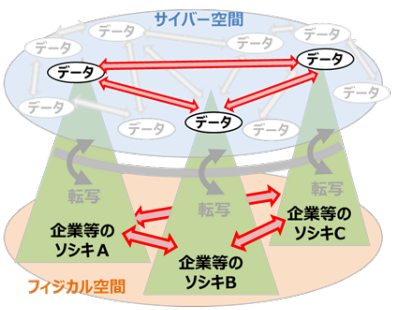
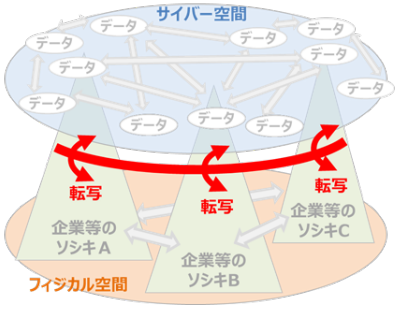
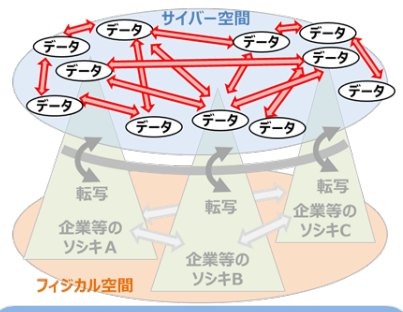
6つの構成要素

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

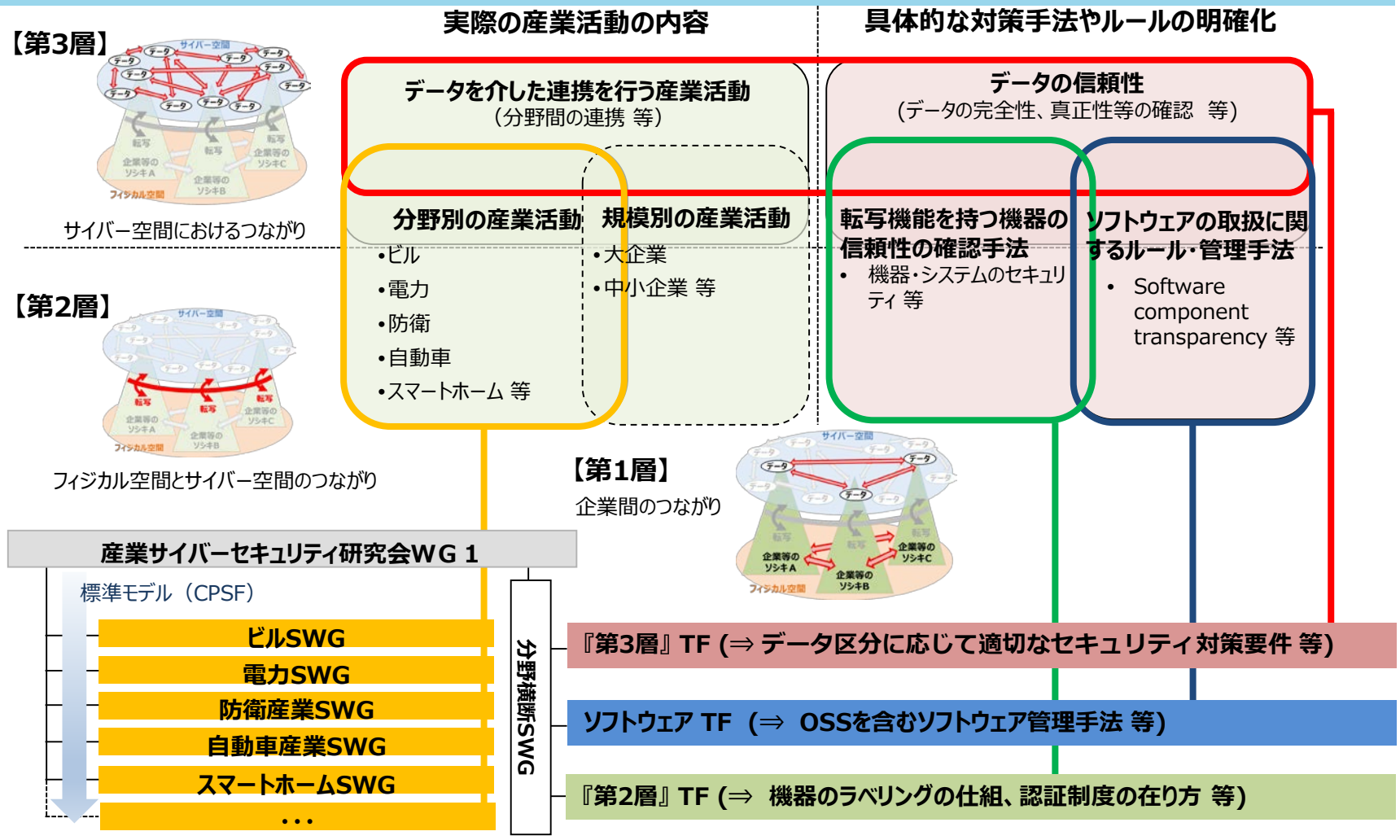
＜CPSFの全体概要＞
三層構造モデルに基づきリスク源、対応方針等を提示

- 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**。



（参考②）
中小企業のサイバーセキュリティ対策強化へ向けた取組
～サイバーセキュリティお助け隊の創設～

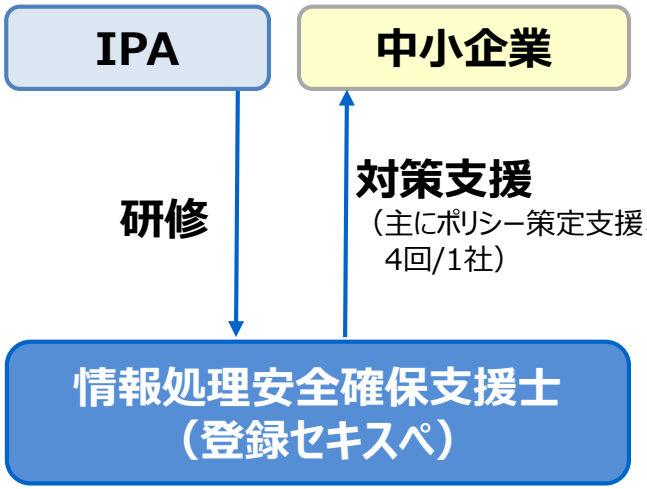
中小企業における現場対応の徹底支援
～事前の備えから、インシデントが発生してしまった後の対応・復旧支援まで

- セキュリティ対策を始めるに当たって何をやればいいのかわからない、そういった悩みをもつ中小企業に対し、**専門家を派遣し、セキュリティポリシーの策定を支援。**
- インシデントが発生してしまったが対処方法がわからない、そんな中小企業の事後対応を支援する簡易保険の実現を目指し、**サイバーセキュリティお助け隊による支援体制を構築。**

特定 → 防御 → 検知 → 対応 → 復旧

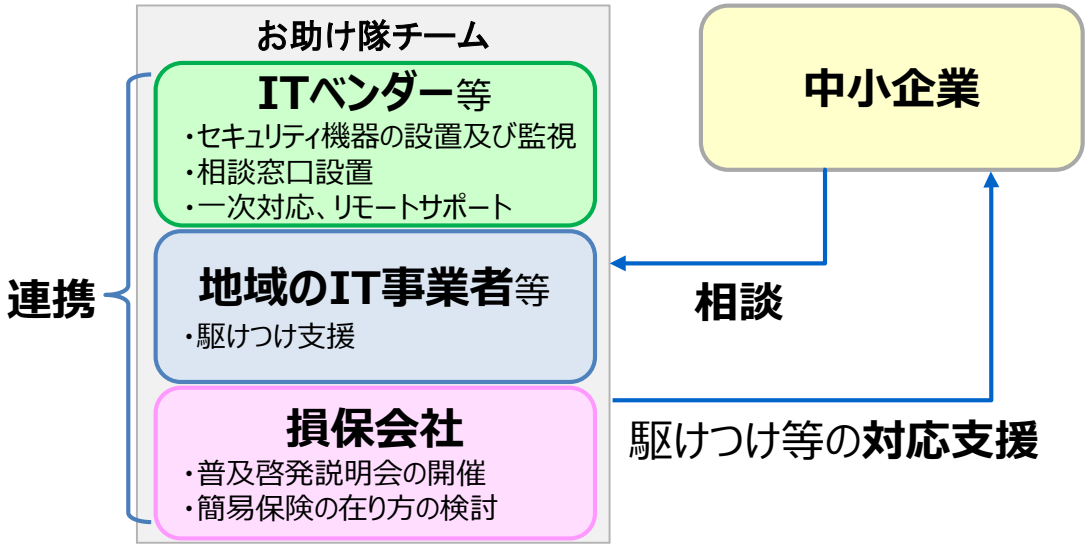
主に事前支援（セキュリティマネジメント指導）

・中小企業に専門家を派遣し、実践的なセキュリティ対策の定着につなげる。



主に事後支援（サイバーセキュリティお助け隊）

・中小企業がサイバー攻撃等で困った時の**相談窓口、駆けつけ支援体制**を構築。
・**将来的な民間サービスとしての自走を目指し、今年度は８地域で実証。**
・今年度の結果を踏まえ、来年度以降、**全国展開を目指すための方策を実施。**



（参考③）
産業分野を超えた情報共有の仕組の構築について

サイバーセキュリティ協議会の概要

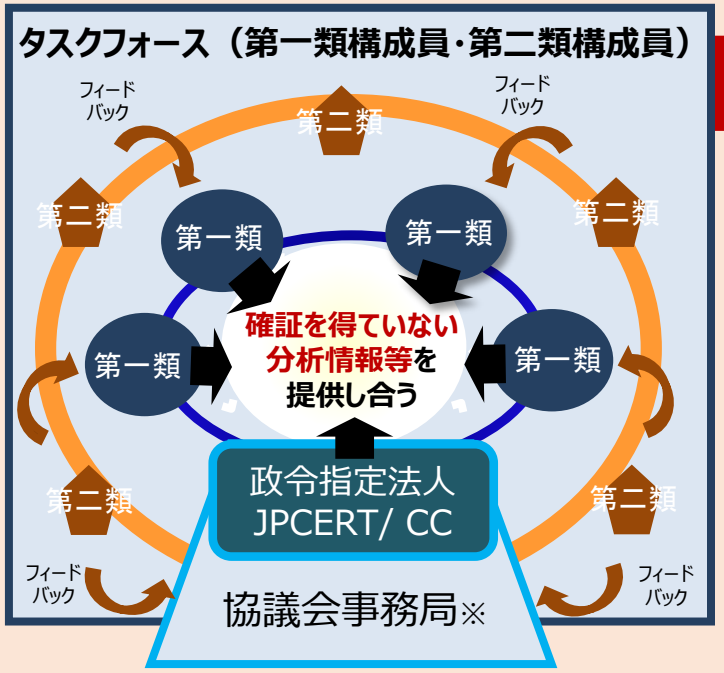
NISC HPから引用

目的

我が国のサイバーセキュリティに対する脅威に積極的に対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行う

主として、**脅威情報等の共有・分析、対策情報等の作出・共有等**を**迅速に**行う（原則システムを活用）

サイバーセキュリティ協議会（CS戦略本部長等により組織）



作出した対策情報等の共有

一般の構成員

総会

全構成員により構成（各構成員に１の議決権）

・総会は毎年開催（電子的手段の開催も可）
・規約の改正　等を実施

運営委員会

運営委員は、CS戦略本部長等

・構成員の入会の承認、除名
・**情報提供等協力の求め**
等に関することを担当

※事務局の庶務はNISC基本戦略２Gが担当

協議会の特徴

①官民、業界といった従来の枠を越えた**オールジャパンによる**情報共有体制

②システムを用いて情報共有等を行う「**バーチャル協議会**」

③直感的な違和感といった**早期の段階からの情報提供、相談等を促進**
構成員には、法律に基づく守秘義務※、情報提供義務が適用　※罰則付き

④**ギブアンドテイクルールを徹底し、積極的な情報提供者へのメリットを増加**　※積極的な情報提供に意欲と能力のある構成員を「**タスクフォース**」としてグループ化

我が国のサイバーセキュリティを確保する観点から、
構成員になるためには、右の要件を満たし、
運営委員会の承認を得なければならない
（加入は任意）

申込みを行うことのできる者

◆国の関係行政機関　◆地方公共団体　◆重要インフラ事業者
◆サイバー関連事業者（主にセキュリティ関連事業者を想定）
◆大学・教育研究機関　等であり、協議会の活動に賛同する者
（事業者等の団体や個人も含む）

詳しくはNISC　HPを参照　⇒　https://www.nisc.go.jp/conference/cs/kyogikai/

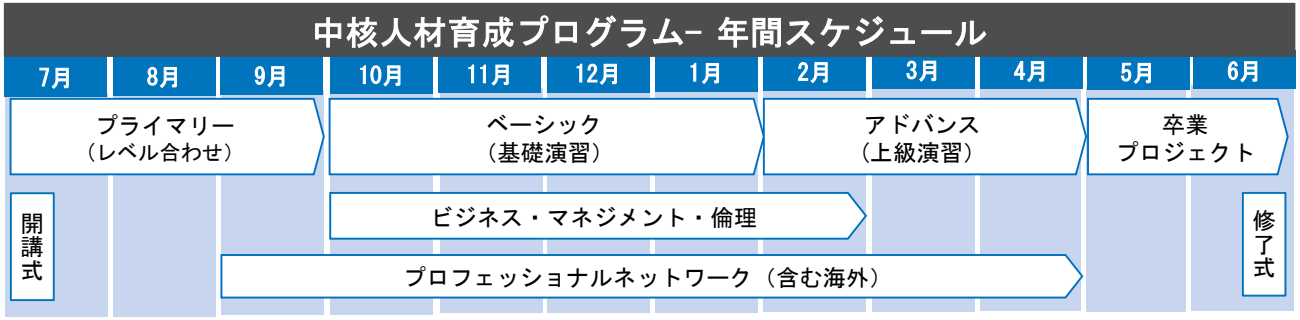
狙い等について質問がある場合は、経産省サイバーセキュリティ課　尾崎、津國、飯山へ（03-3501-1253）

（参考④）
IT系・制御系に精通したサイバーセキュリティ専門人材の育成について

産業サイバーセキュリティセンター（ICSCoE）

- 2017年4月、IPAに産業サイバーセキュリティセンターを設置し、IT系・制御系に精通した専門人材の育成を開始。
- 世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年程度のトレーニングを実施。

1年を通じた集中トレーニング

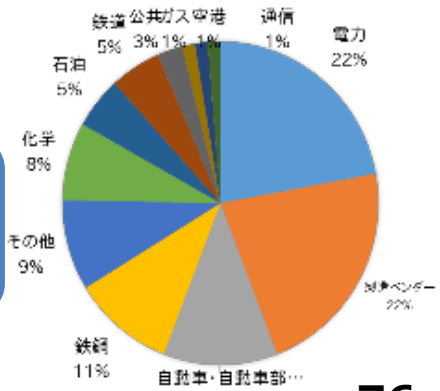


◀模擬プラント全景

- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

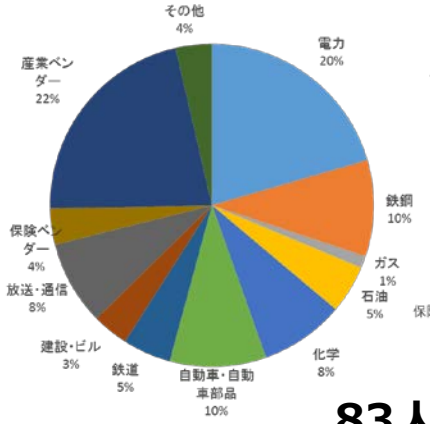
現場を指揮・指導するリーダーを育成

第１期受講生（平成29年7月～平成30年6月）業界別構成



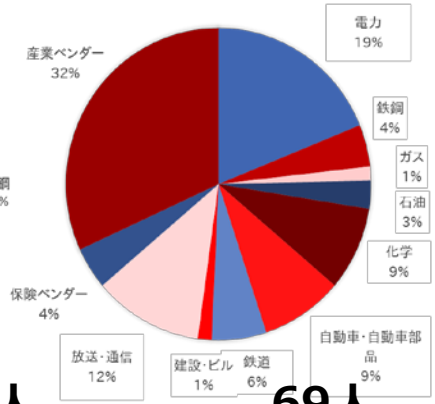
76人

第２期受講生（平成30年7月～令和元年6月）業界別構成



83人

第３期受講生（令和元年7月～令和2年6月）業界別構成



69人

模擬プラントを含めた実践的施設（千石、秋葉原）

- 座学や基礎演習を行う千石と、各業界を想定した実機を使った模擬プラントを実際に攻撃して脆弱性を洗い出すなどの実践的なプログラムを行う秋葉原で活動を展開。

千石ー研修・演習施設

＜座学＞

＜基礎演習＞

秋葉原ー模擬プラント

＜実践的プログラム＞

攻撃

模擬プラントを攻撃

①発電模擬プラント

②機械製造模擬プラント

対策を検討

受講生

脆弱性を発見

模擬プラント全景

③鉄鋼圧延模擬プラント
④鉄道運行管理模擬プラント
⑤スマートグリッド模擬プラント
⑥施設管理模擬プラント

模擬プラント