サイバーセキュリティ政策の動向

2025年２月26日

総務省 サイバーセキュリティ統括官室
企画官

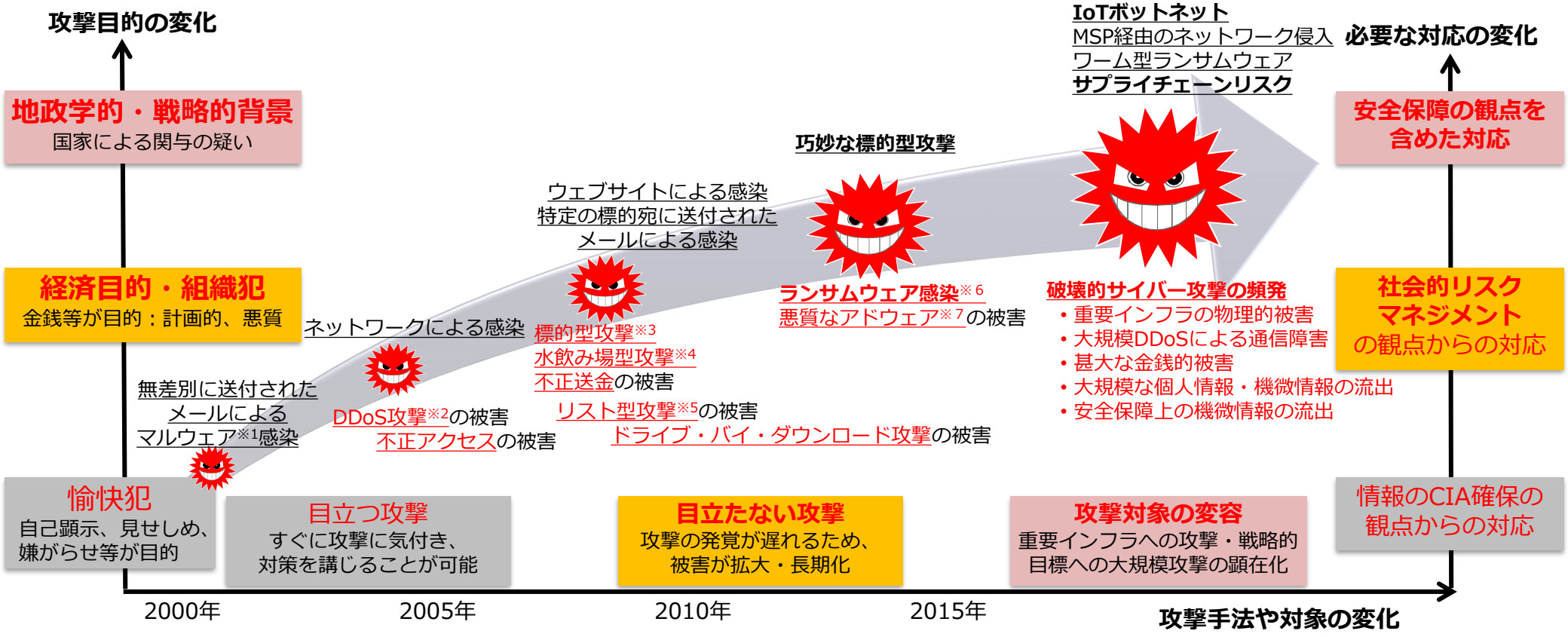
西村　卓

目次

1　サイバーセキュリティを取巻く動向

サイバーセキュリティ上の脅威の増大

インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、サイバーセキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。



※1 マルウェア(Malware)　Malicious softwareの短縮語。コンピュータウイルスのような有害なソフトウェアの総称。

※2 DDoS攻撃　分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数の端末から一斉に大量のデータを特定宛先に送りつけ、宛先のサーバ等を動作不能にする攻撃。

※3 標的型攻撃　機密情報等の窃取を目的として、特定の個人や組織を標的として行われる攻撃。

※4 水飲み場型攻撃　標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

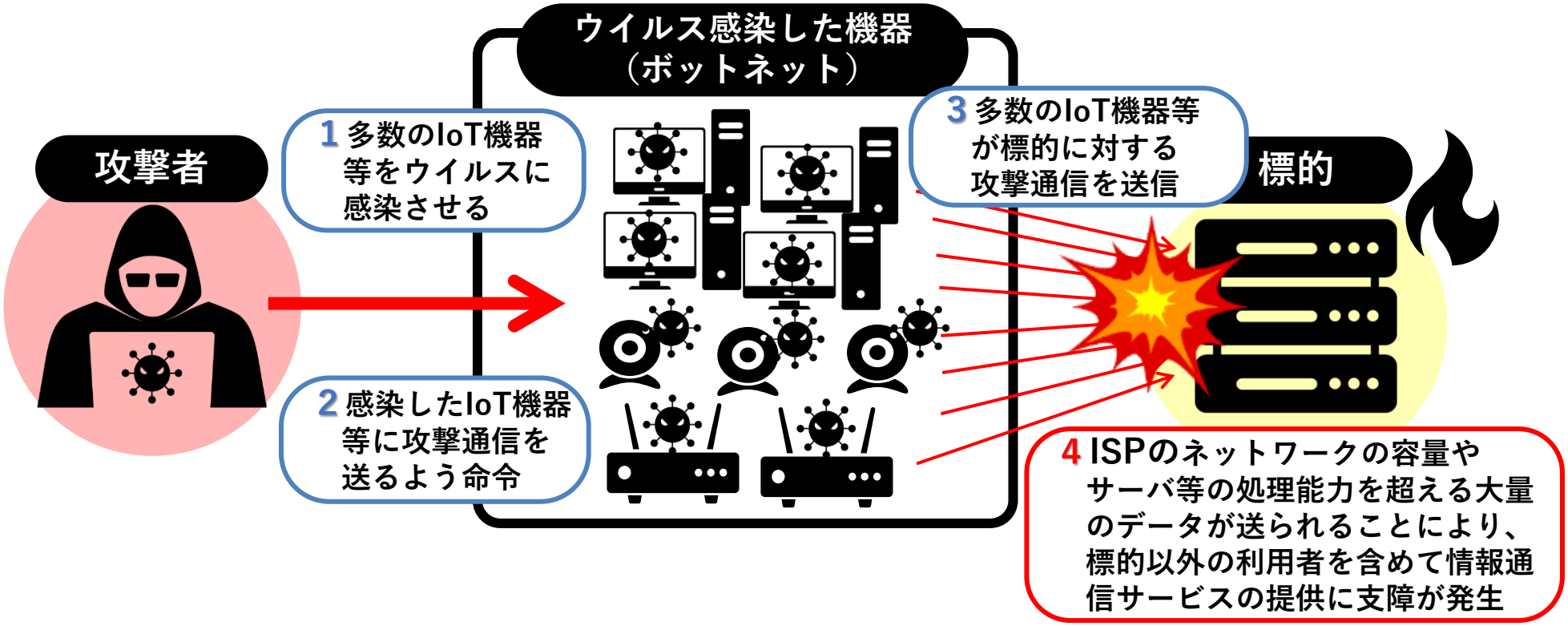
※5 リスト型攻撃　不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃。

※6 ランサムウェア(Ransomware)　身代金要求型ウイルスのこと。感染端末上にある文書などのファイルが暗号化され、暗号解除のためには金銭を要求される。

※7 アドウェア(Adware)　広告表示によって収入を得るソフトウエアの総称。狭義には、フリーウエアと共にインストールされ、ブラウザー利用時に広告を自動的に付加するソフト

サイバー攻撃の動向　①DDoS攻撃

【DDoS攻撃※のイメージ】※DDoS攻撃（分散型サービス不能攻撃：Distributed Denial of Service attack）



【最近の事例】

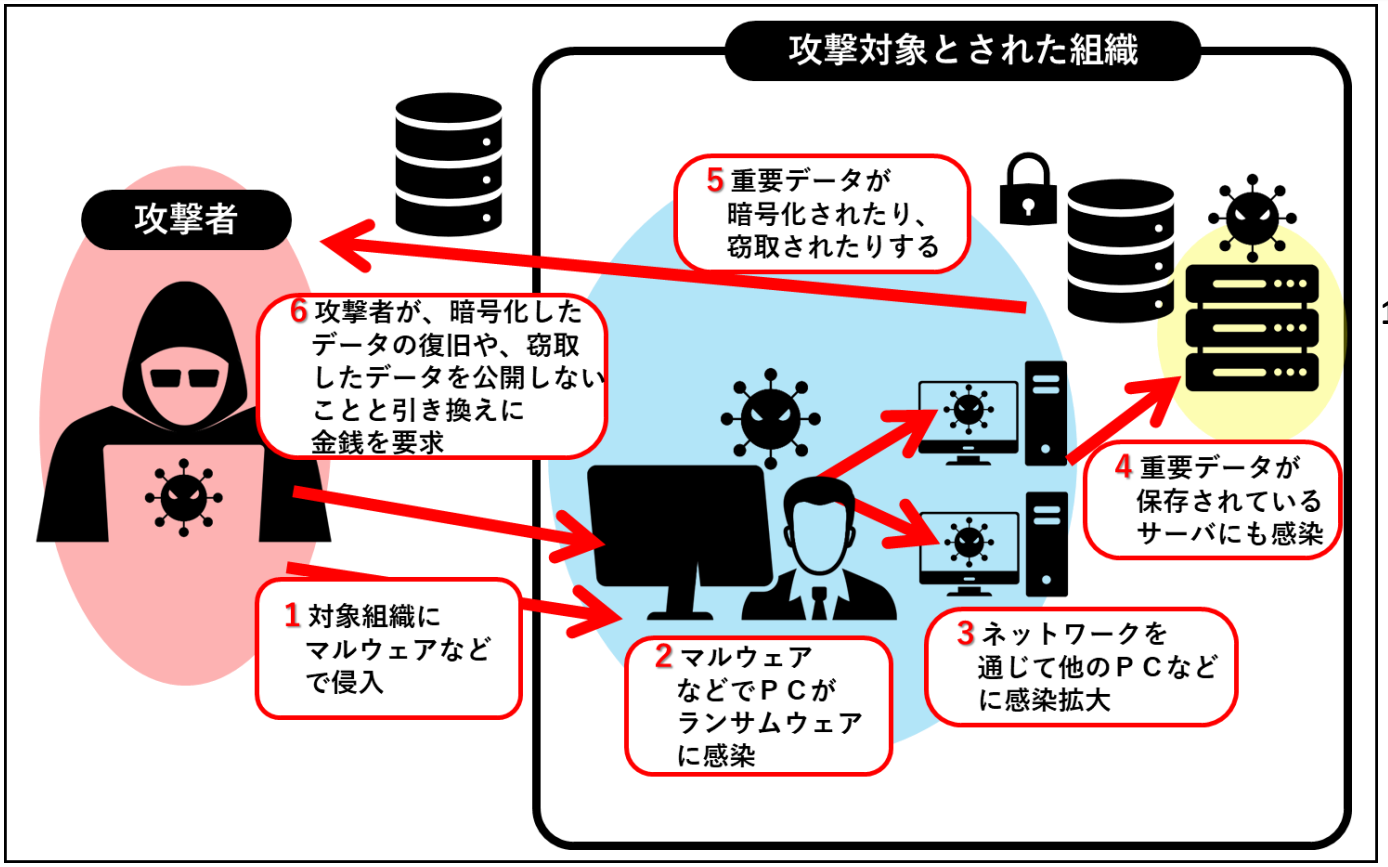
（IoT機器が不正アクセスされた事例）

- 2023年1月、国土交通省近畿地方整備局が管理する河川監視用のカメラ 199台において、大量の通信を確認。
- その後中国地方整備局、四国地方整備局が管理するカメラも合わせ、不正アクセスの疑いのある337台のカメラの運用を休止。

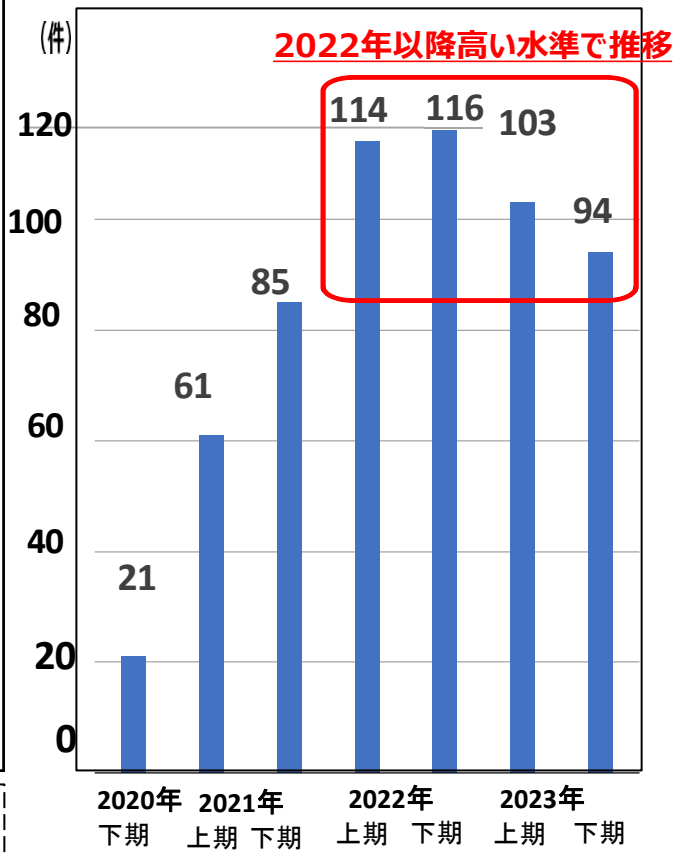
（ウェブサイト等への障害が発生した事例）

- 2023年3月から6月にかけて、国内外のDNSサーバが散発的にDDoS攻撃を受け、Webサイトの閲覧やメールの送信の障害が断続的に発生。
- 2023年11月、米OpenAIのサービスChartGPTがDDoS攻撃を受け、一時利用不可となった。
- 2024年12月、JALや三菱UFJ銀行のシステムがDDoS攻撃を受け、航空券販売やインターネットバンキングで障害が発生。

サイバー攻撃の動向　②ランサムウェア攻撃



企業・団体等における
ランサムウェア被害の報告件数



出典：「令和5年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）より総務省作成

【最近の事例】

（ランサムウェアに感染したとされる事例）

- 2024年5月、岡山県精神科医療センターのシステムがランサムウェアに感染し、電子カルテから紙カルテに切り替えたほか、患者情報が漏えいした疑い。
- 2024年5月、印刷業務等を請け負うイセトー社がランサムウェアの被害に遭い、個人情報が漏えいした疑い。
- 2024年6月、KADOKAWA社がランサムウェアの被害に遭い、一部サービスが停止・縮小となったほか、従業員情報や社外秘の情報が漏えいした疑い。

（参考）サイバー攻撃に起因する重要インフラ等の業務停止

病院に対するサイバー攻撃の事例

2024年3月、鹿児島県霧島市の**国分生協病院**が、**「ランサムウエア」**と呼ばれる身代金要求型のコンピューターウイルスによる**サイバー攻撃を受け**、**救急・一般外来患者の受入れを制限。**

国分生協病院が「ランサムウエア」サイバー攻撃受ける　一部診療を制限

2024/03/04 20:55

医療・福祉　霧島市　コンピューターウイルス　ランサムウエア

鹿児島県霧島市の国分生協病院は４日、身代金要求型コンピューターウイルス「ランサムウエア」によるサイバー攻撃を受けたと発表した。現在、救急や一般外来の受け入れを制限している。

拡大

厚生労働省によると、県内医療機関へのランサムウエア攻撃は、確認できた２０２１年度以降初めて。

同院によると、画像管理サーバーの一部データが暗号化された。個人情報の流出は、現時点で確認されていない。紙カルテを運用し、予約外来や入院患者は対応している。

２月２７日午後９時半ごろに攻撃を確認。２８日午前８時半に外来、救急の受付停止を決定し、紙カルテを運用。厚労省に初動対応チームの派遣を要請した。

院内全体のインターネット接続を停止しており、再侵入などの兆候はない。攻撃者から身代金の要求はされておらず、支払いや交渉には応じない構え。

（2024年3月4日 南日本新聞
https://373news.com/_news/storyid/191272/）

ガス事業に対するサイバー攻撃の事例

2023年6月、住宅設備製造事業者の**パーパス社**がエネルギー事業者向けに提供するクラウドサービスがサイバー攻撃を受け**サービス停止**。このサービスを利用する全国約1,000のLPガス会社において、**検針業務が遅延する等の影響が発生。**

パーパスのマルウエア被害で顧客サービスに影響、エネルギー系企業が相次ぎ発表

森岡 麗　日経クロステック／日経コンピュータ

2023.06.15

ホクトや日本エネルギーといったガスや電気などエネルギー業界の企業が6月8～15日に相次いで、利用している外部サービスでシステム障害が発生していると発表した。この障害により各社では、ガス料金などの情報閲覧、集金や請求書の発行、引っ越し時の利用料金精算や請求金額の説明、料金に関する問い合わせ対応、ウェブ会員サービスへのアクセスなどができないといった事象が生じているもようだ。

このシステム障害は、住宅設備関連機器やITサービスなどを手掛けるパーパスのエネルギー事業者向け管理サービス「クラウドAZタワー」シリーズのサーバーがマルウエア攻撃を受け、2023年6月8日午前10時半ごろから同サービスの提供を停止していることを指す。パーパスによれば、同サービスを利用中のエネルギー事業者は約1100社に上る。

（2023年6月15日 日経クロステック
https://xtech.nikkei.com/atcl/nxt/news/18/15416/）

港湾に対するサイバー攻撃の事例

2023年７月、愛知県名古屋市の**名古屋港**で、**港内のコンテナターミナルの管理システムに対するサイバー攻撃が発生**。7月4日午前から7月6日午後までの約2日半にわたり、**名古屋港でのコンテナの搬出入が完全に停止。**

名古屋港にサイバー攻撃か　システム障害、搬出入中止

サイバー防衛　＋フォローする

2023年7月5日 13:16 (2023年7月5日 18:53更新)

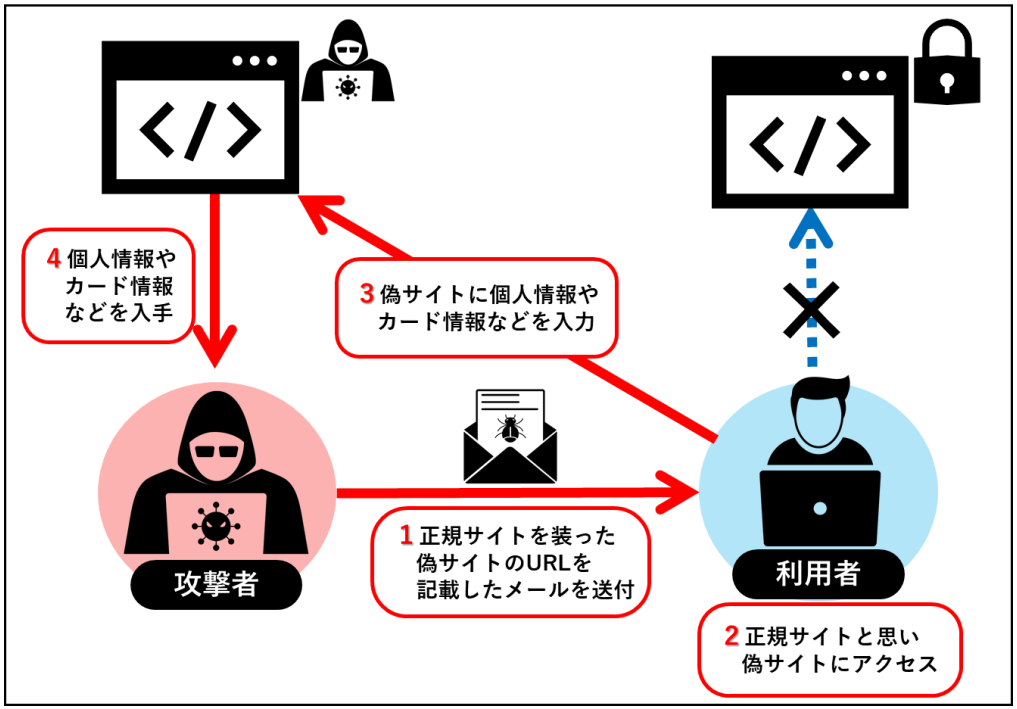
保存

トレーラーの出入りもなくなった名古屋港のコンテナ埠頭（5日午後、愛知県飛島村）

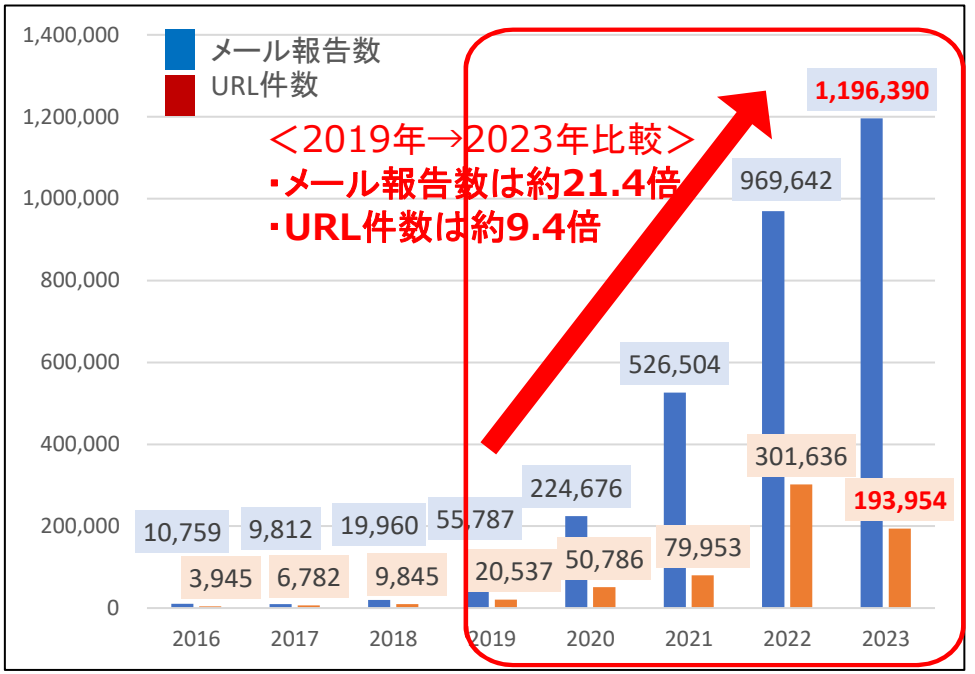
名古屋港運協会（名古屋市）は5日、名古屋港内のコンテナターミナルを管理するシステムで障害が発生したと発表した。トレーラーによるコンテナの搬出入作業を終日中止した。同協会はシステムの復旧を進め、6日午前8時半からの作業再開を目指している。

（2023年7月5日 日本経済新聞
https://www.nikkei.com/article/DGXZQOFD053RH0V00C23A7000000/）

サイバー攻撃の動向　③フィッシング



フィッシング報告件数及びフィッシングサイトのURL数



出典：「フィッシング報告状況」（フィッシング対策協議会）より総務省作成

【最近の動向】＜2024/3 フィッシング報告状況（フィッシング対策協議会）＞

- **Amazon 及び東京電力をかたるフィッシング**の報告が急増し、それぞれ報告数全体の約 15.9% を占めた。次いで報告が多かった**イオンカード、三井住友カード、メルカリ、ETC利用照会カードをかたるフィッシング**の報告をあわせると、全体の約 66.7 % を占めました。1,000 件以上の大量の報告を受領したブランドは 15 ブランドあり、これらで全体の約 90.5 % を占めました。
- 分野別では、**クレジット・信販系 約 34.7 %、電力系約15.9%、オンラインサービス系約7.8%、行政サービス　系約3.4%、金融系 約3.1 %** となり、EC系と電力系ブランドの割合が急増、クレジット・信販系も報告数も増加。
- SMSから誘導されるスミッシングについては、**宅配便関連の不在通知を装う**文面、**Appleをかたる**フィッシングサイトへ誘導するタイプの報告などが見られます。

【最近の事例】

2023年、宿泊予約を提供するBooking.comが不正アクセスを受け、攻撃者がユーザに正規のメッセージを用いてフィッシングサイトへアクセスさせる事案が発生。

新たなサイバー安全保障体制の検討（能動的サイバー防御）

- ✓ **国家安全保障戦略**（令和４年12月16日閣議決定）に**「能動的サイバー防御」の体制整備**が盛り込まれた。
- ✓ 令和６年6月、内閣官房に**有識者会議**を立上げ、**検討事項（ア）～（ウ）**につき、有識者会合の下の分科会にて詳細を検討。
- ✓ 令和６年10月４日 **石破内閣総理大臣所信表明演説**（抜粋）『能動的サイバー防御の導入に向けた**検討を更に加速させる**など、サイバーセキュリティの強化に取り組みます』

○国家安全保障戦略　抜粋（令和４年12月16日閣議決定）

Ⅵ　我が国が優先する戦略的なアプローチ　／２ 戦略的なアプローチとそれを構成する主な方策

⑷ 我が国を全方位でシームレスに守るための取組の強化

ア サイバー安全保障分野での対応能力の向上

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる。

具体的には、まずは、最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する。（略）

その上で、武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

(ｱ) 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。

(ｲ) 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

(ｳ) 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。これらの取組は総合的な防衛体制の強化に資するものとなる。

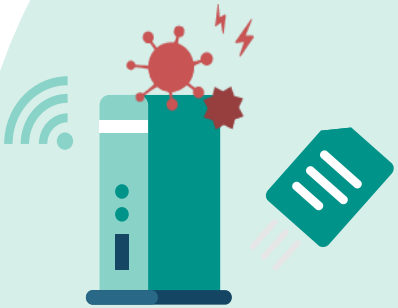
２　総務省における取組み

（1）情報通信ネットワークの安全性・信頼性の確保

IoT機器の乗っ取りによる被害例

ルーターが乗っ取られ、サイバー攻撃の踏み台にされてしまう

2021年8月から9月にかけて、過去最大級のサイバー攻撃が世界各地で相次いで発生した。新種のボットネット「Meris」によるもので、標的に大量のデータトラフィックを送り付けてサービス不能状態に陥れるDDoS攻撃が25万台のルーターから仕掛けられていた。



ルーターが攻撃され、個人情報などが盗まれる

X氏は、知らないうちに 数万円が銀行口座から不正送金されていた。原因は家庭用ルータのDNS設定が改変されていたこと。DNS設定を変更することでサイバー犯罪者は、X氏の通信をすべて傍受し、銀行口座の認証情報を含むさまざまな情報を入手していたとみられる。

ネットワークカメラの映像が第三者に覗かれる

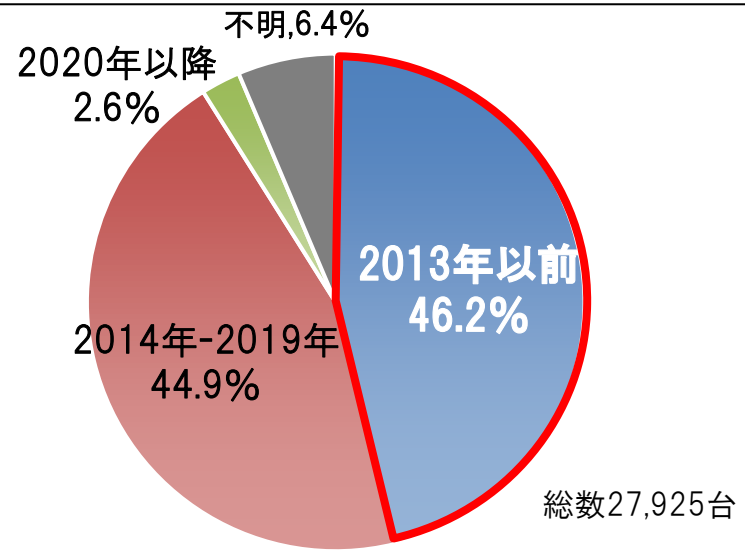
学校防犯システムと保育所見守りカメラにおいて、マルウェア感染の特徴のある通信を国立研究開発法人情報通信研究機構（NICT）が観測した。十分なセキュリティ対策が行われていないことにより、マルウェアに感染し、どちらも第三者から映像が閲覧できる状態になっていた。また、保育所ではインターネットが使えない状態となっていた。

明らかになった主な課題

脆弱性等があるIoT機器やサイバー攻撃の脅威に関する課題

■ **ID・パスワードに脆弱性があるIoT機器**は、10年以上前の機種が４割強も存在するなど**古い機器を中心に残存。**

ID・パスワードに脆弱性がある機器の発売年別内訳
（2022年11月～2023年４月）



■ **サイバー攻撃の脅威は変化**しており、
①**新たなネットワーク経路**（通信プロトコル、ポート）を狙った攻撃
②**ID・パスワード以外の脆弱性**（ファームウェア等）を狙った攻撃
も発生。

■ **マルウェアの活動状況は依然として活発**であり、**サイバー攻撃関連の通信数**は、**５年前と比較して約3倍に増加。**

利用者の意識に関する課題

■ IoT機器のセキュリティ対策に対する**利用者の意識が十分ではなく、対策方法も利用者にとって難しい**ものとなっている。

Wi-Fiルータ利用者向けのアンケート結果によれば、
- **57.8%**の利用者がWi-Fiルータのセキュリティを意識したことがない
- **81.7%**の利用者が自宅のWi-Fiルータがサイバー攻撃されると考えたことがない
- 購入時のパスワードをそのまま利用している利用者が**42.7%**

（出典）デジタルライフ推進協会（DLPA）Wi-Fiルーターセキュリティ対策ポイントを基に作成

■ **法人利用者**については、管理責任の所在が曖昧など**適切な管理体制がない**ケースもある。

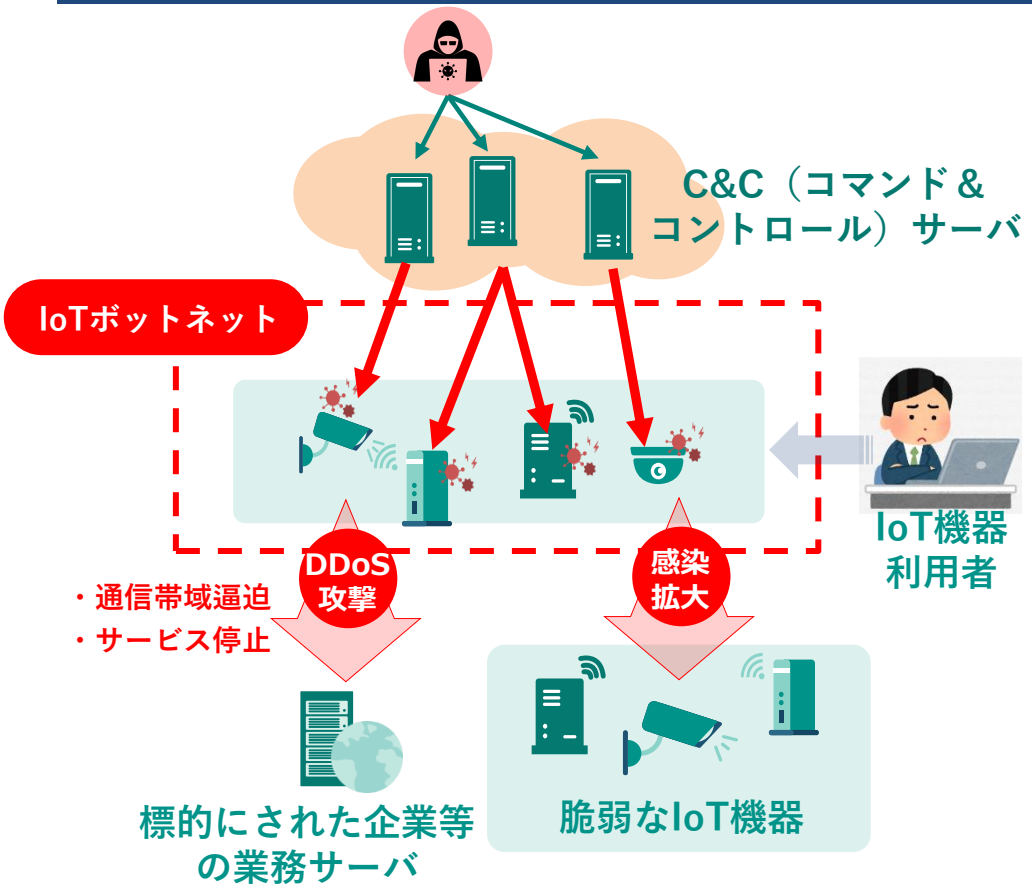
	所有者	設置者	管理者	使用者
一般利用者	購入者			（＋家族）
法人利用者	企業	設置委託業者	管理委託業者	社員、客

（出典）第３回情報通信ネットワークにおけるサイバーセキュリティ対策分科会 ヤマハ発表資料を基に作成

IoT機器を悪用したサイバー攻撃（DDoS攻撃等）対策（全体像）

➢ IoT機器を悪用したサイバー攻撃（DDoS攻撃等）への対策として、①指令通信を出すC&C（コマンド＆コントロール）サーバの検知と対処、②ウィルスに感染した、又は感染する危険性が高い脆弱なIoT機器の検出と対処、の両面から　**<u>総合的なIoTボットネット対策を講じる必要。</u>**

IoT機器を悪用したサイバー攻撃（DDoS攻撃等）のイメージと必要な対策



対策①
IoTボットネットに対して指令通信を出す
C&C（コマンド＆コントロール）サーバへの対処

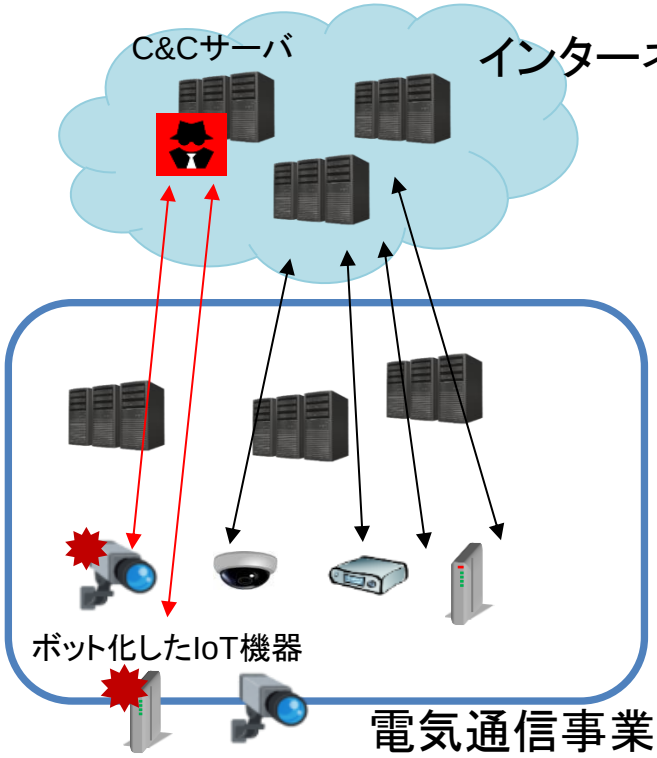
対策②
ウイルスに感染した、又は感染する危険性が
高い脆弱なIoT機器への対処

IoT機器を悪用したサイバー攻撃（DDoS攻撃等）には、
C&CサーバとIoT機器の両面から対策を行うことが効果的

対策①指令通信を出すC&Cサーバへの対処

・電気通信事業者※1は通信を安定的に流すため、普段から自社のネットワーク上を流れるフロー情報※2を観測している。
・このフロー情報を分析すると、IoTボットネットと通信するC＆Cサーバ※3を事前に検知できることがある。
・攻撃の標的となる企業等の側からは根本的な対策が難しいDDoS攻撃に対し、
電気通信事業者がフロー情報を分析することで、攻撃の指示を行う可能性のあるC＆Cサーバを事前に検知し、
対策に活用するための実証事業を実施している。

※1 電気通信事業者　本事業においては、インターネットサービスプロバイダーを指す。
※2 フロー情報　通信経路を流れるデータのうち、ヘッダ情報等（IPアドレスなど）。
具体的な通信の内容（例えば、個々人のメールアドレスやメールの内容など）は含まない。
※3 C&Cサーバ　ウイルスに感染した端末に情報漏洩やデータ破壊に係る指示を送るサーバ。



①フロー情報を収集・分析し、
C&Cサーバを洗い出し

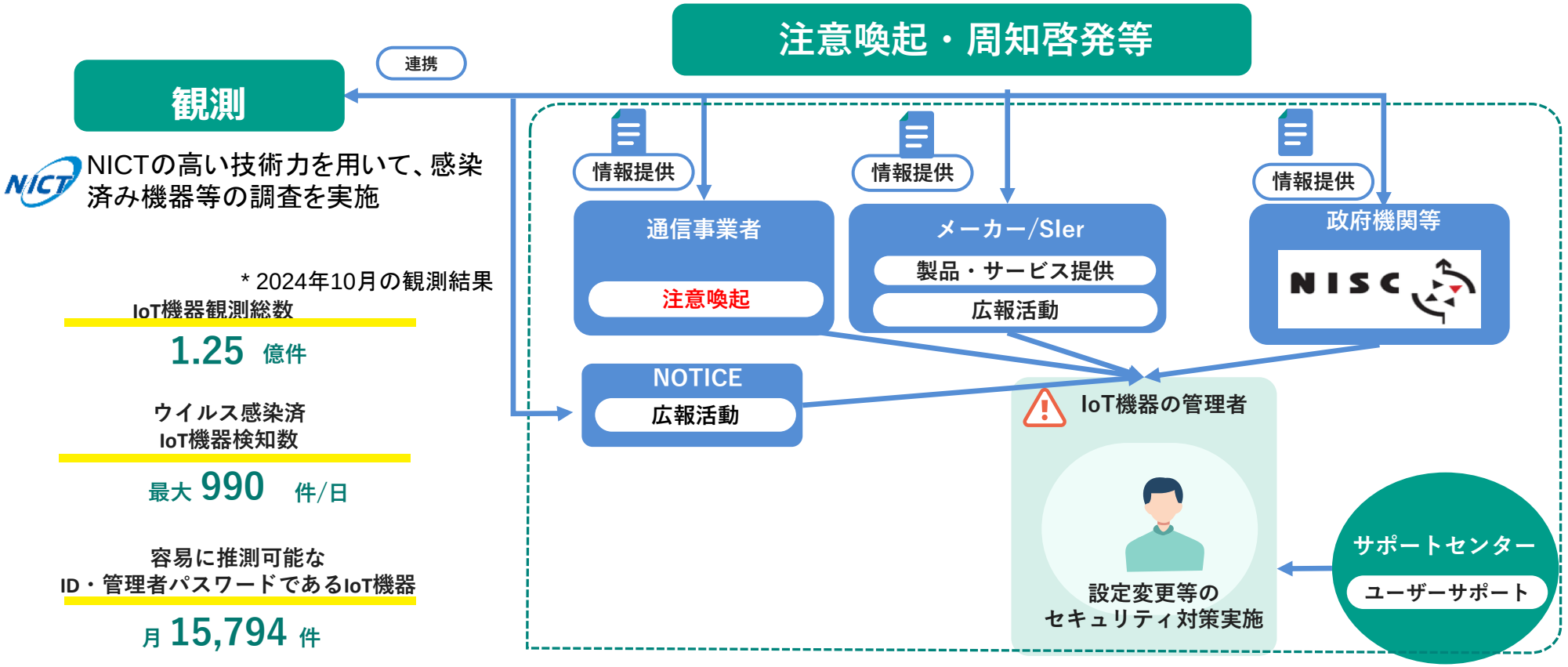
専門家による分析や
疑わしいC&Cサーバへの
接続テスト等を行い、
C&Cサーバリストの精度を向上

②電気通信事業者間で
C&Cサーバ情報を
共有し、対策に活用

本事業と通信の秘密との関係については、総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ」（2021年11月）において整理。

対策②ウイルスに感染したIoT機器への対処

✓　ウイルスに感染したIoT機器は新たな機器に感染を広げ規模を拡大するため感染拡大通信を行う。この感染拡大通信等をNICTが観測・調査し、**既に感染しているIoT機器や、今後感染する危険性が高い脆弱なIoT機器を発見**する。**それらのIoT機器を使用している管理者**に対し、電気通信事業者と連携して**注意喚起・周知啓発等**を行うことで、IoTボットネットによる**サイバー攻撃（DDoS攻撃）の発生と被害を軽減**する。（NOTICE事業）



* 2024年10月の観測結果

IoT機器観測総数
1.25 億件

ウイルス感染済
IoT機器検知数
最大 990 件/日

容易に推測可能な
ID・管理者パスワードであるIoT機器
月 15,794 件

ファームウェアに
高リスク脆弱性を有するIoT機器
月 4,891 件

※利用者からのサイバー攻撃の被害の申告を待つことなくプッシュ型による支援を実施

NICTにおけるサイバー攻撃観測技術の全体像

- **急増するサイバー攻撃**から社会システム等を守る**サイバーセキュリティ分野の技術の高度化が不可欠**となっていることを踏まえ、 NICTにおいてサイバー攻撃観測技術の研究開発を推進。
- サイバー攻撃を**受動的/積極的**、および**広域的/局所的**に観測して各所対策に活用するなど、様々な技術を活用して研究開発に取り組んでいる。
- 更なる高度化を図るため、各研究分野において**AIを積極的に活用。**

インシデント分析センター（ニクター）

NICTER

対サイバー攻撃アラートシステム（ダイダロス）

DAEDALUS

Passive

サイバー攻撃統合分析プラットフォーム
（ニルヴァーナ・カイ）

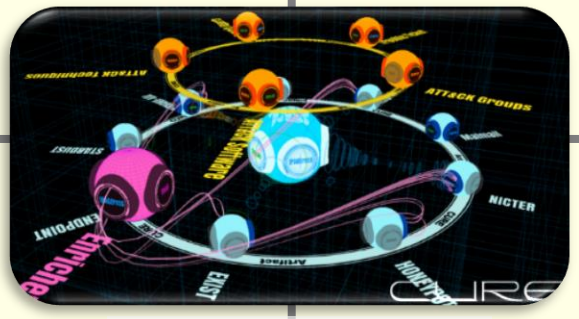
NIRVANA改

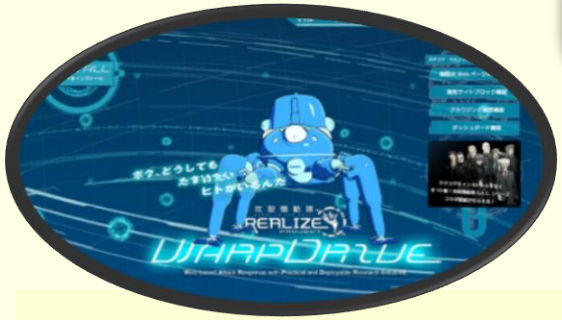
脆弱性管理プラットフォーム
（ニルヴァーナ・カイ・ニ）

NIRVANA改弐

Global

Local





サイバーセキュリティ
ユニバーサル・リポジトリ

CURE

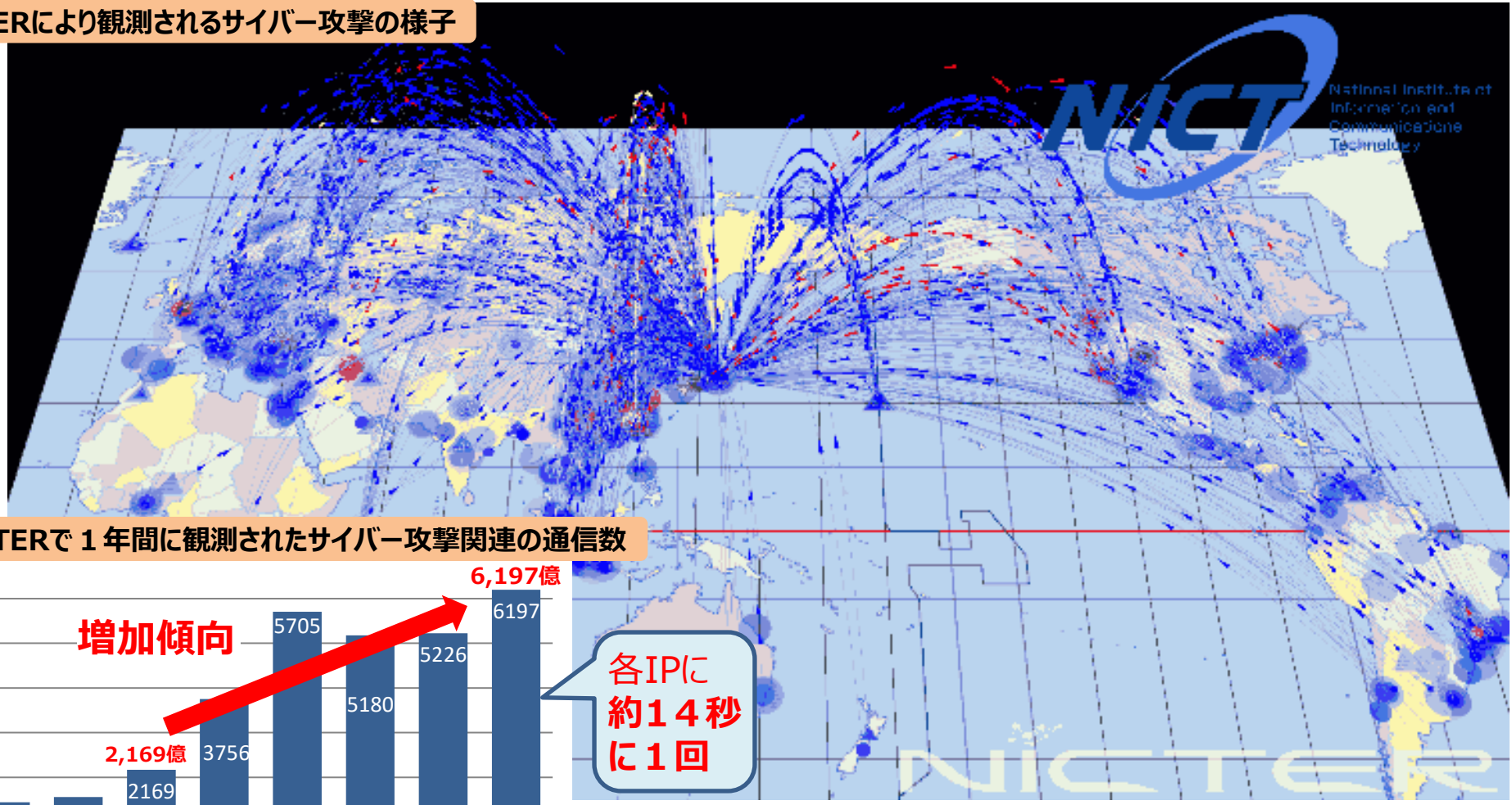
Active

AIを活用したサイバーセキュリティの高度化

サイバー攻撃の観測の可視化（NICTERによる観測）

➢ 国立研究開発法人情報通信研究機構（**NICT**）では、大規模サイバー攻撃観測網である**NICTERにおいて、未使用のIPアドレス30万個（ダークネット）を活用**し、グローバルに**サイバー攻撃の状況を観測。**

NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測されたサイバー攻撃関連の通信数

※1IPアドレス当たり
年間226万パケット

※2020年は特異的な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されたため、例外的にパケット数が多かったものと推測

２　総務省における取組み
（２）サイバー攻撃への自律的な対処能力の向上

CYNEXの背景

我が国では、利用されている**セキュリティ機器・サービスが海外企業に大きく依存**しており、開発に必要なデータの蓄積が困難。また、人材育成に必要なデータ・仕組みが不十分であり、**セキュリティ人材も大きく不足**。

セキュリティ機器・サービス開発の課題

- **情報が集まらない**ので、実データによる研究開発を行えず、国産技術を作れない。そのため情報が集まらない。
- 海外で分析され**結果の根拠が不明**。
- **日本特有の攻撃**に対応できない。

経済安全保障上も大きなリスク

セキュリティ人材育成の課題

- 演習の実施には、**高度な技術力**と**計算機環境**が必要
- **海外教材に依存**し、国内組織特有のネットワーク構成の脆弱性を突いた攻撃などを反映できない

- **国内業界はデータ負けのスパイラル**
  1. 国産の**セキュリティ技術が普及しない**
  2. サイバー攻撃の**実データが集まらない**
  3. 実データを使った**研究開発ができない**
  4. 良い国産セキュリティ**技術を作れない**

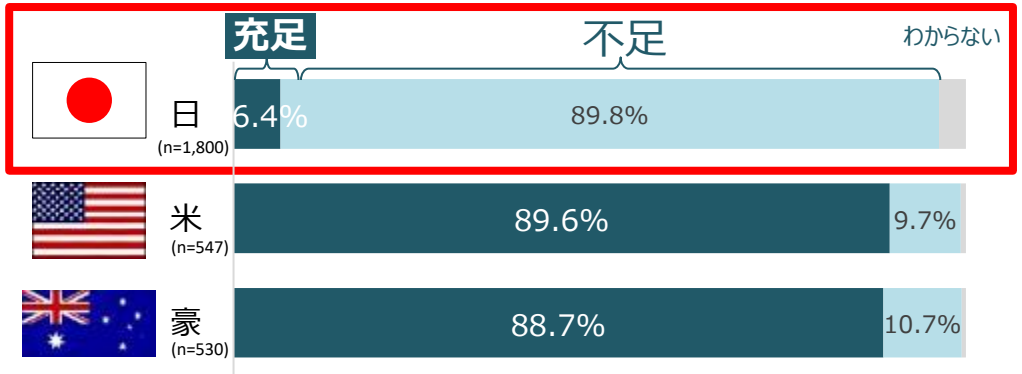
- **高騰するサイバーセキュリティ情報**
  - ✓ 国内のデータが海外に流れ、海外で分析
  - ✓ 海外で生成された脅威情報を高額で購入
- **セキュリティ人材育成も困難**
  - ✓ データ不足から海外製の教材に依存せざるを得ない

国内でサイバーセキュリティ情報を生成・蓄積・提供し、また人材育成にも活かす環境が必要

（参考）我が国におけるサイバーセキュリティ人材の不足

- 日本では人材の不足感が高く、**セキュリティ人材が充足していると感じている企業は１割未満。**
- **ＩＴ企業に**おいても、セキュリティ人材を「確保できている」との回答は**１割未満に留まる。**
- 各企業のセキュリティ対策としても**人材育成は喫緊の課題。**

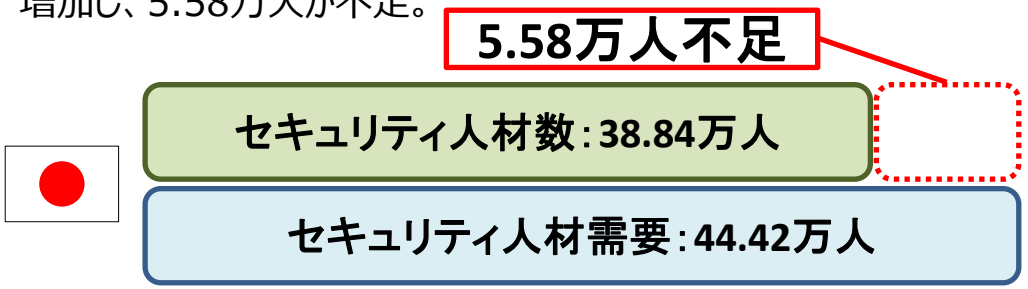
セキュリティ対策に従事する人材の充足状況



出典：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2022」より作成

サイバーセキュリティ人材需要

2022年、日本におけるセキュリティ人材需要は2021年から40.1%増加し、5.58万人が不足。



出典：（ISC)² 「(ISC)² Cybersecurity Workforce Study（2022年版）」より作成

今後の投資を要するセキュリティ対策領域

➢今後、より積極的に取り組みたいと考えている領域

(複数選択５つまで可／n=285)

高度なエンドポイントセキュリティ対策	35.4%
クラウドセキュリティ対策	35.1%
サイバーセキュリティ人材の育成	**30.2%**
ネットワークセキュリティ対策	24.9%
資産管理	21.4%
メールセキュリティ対策	19.6%
内部不正対策	18.9%
インシデント対応体制（CSIRT）の強化	18.2%
セキュリティ監視体制（SOC）の強化	16.5%

➢サイバーセキュリティ対策に取り組む上での課題

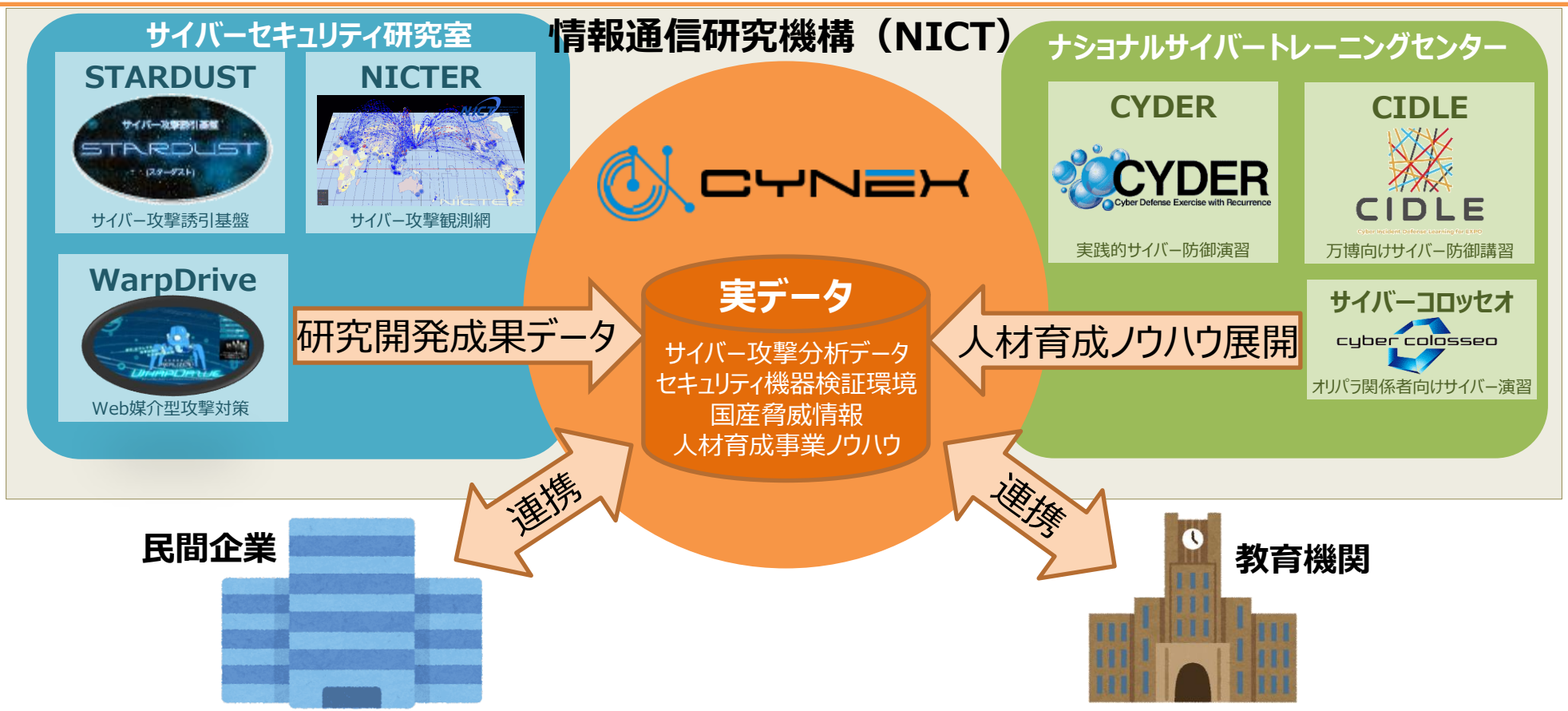
(複数選択可／n=285)

知見のある実務担当者が足りない	**72.6%**
従業員の意識が低い	49.1%
投資対効果が分からない	44.9%
どれだけ投資すべきか分からない	38.2%
サイバー攻撃の進化に追いつけない	34.0%
対策のための予算を確保できない	28.4%
経営層の理解が乏しい	28.4%

出典：KPMGコンサルティング「サイバーセキュリティサーベイ2022」より抜粋

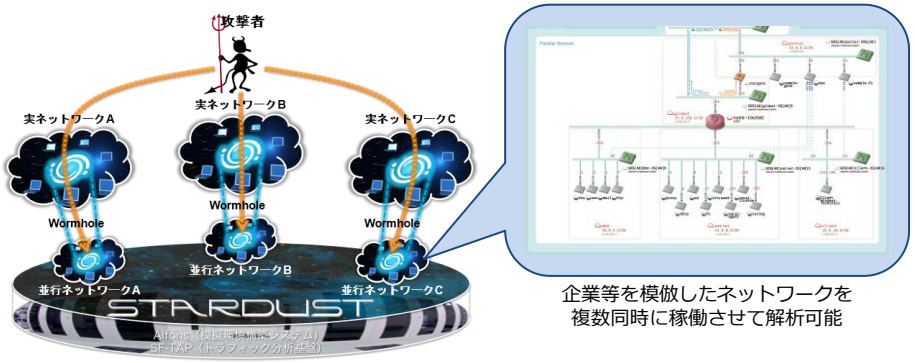
研究開発・人材育成の産学官連携拠点『CYNEX』（サイネックス）

- データ負けのスパイラルにより、国産セキュリティ技術の開発が低迷。
- サイバー攻撃に関する実データを国内で大規模に収集・蓄積し、活用する仕組み作りが必要。
- 情報通信研究機構（NICT）では、これまで次のような取組を実施
  - ・最先端のサイバーセキュリティ関連技術の研究開発（サイバーセキュリティ研究室）
  - ・実践的サイバー防御演習等による人材育成（ナショナルサイバートレーニングセンター）
- これらのデータ・知見を活用し、サイバーセキュリティに関する産学官の結節点となる先端的基盤として
  ＣＹＮＥＸ（CYbersecurity NEXus：サイネックス） を構築



CYNEXの具体的な活動の推進（４つのCo-Nexus）

■ サイバー攻撃の共同解析と解析者コミュニティ形成



サイバー攻撃誘引基盤STARDUST

企業等を模倣したネットワークを複数同時に稼働させて解析可能

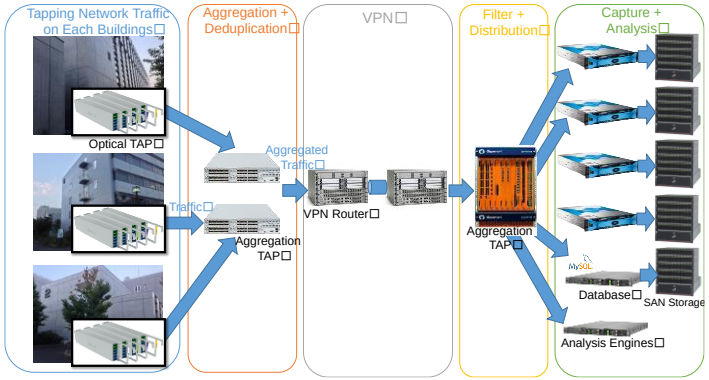
■ 高度な解析者の育成とCYNEX独自の脅威情報の生成･発信

自主学習型オンラインSOC研修

OJTでのSOC業務従事

国産脅威情報発信/提供

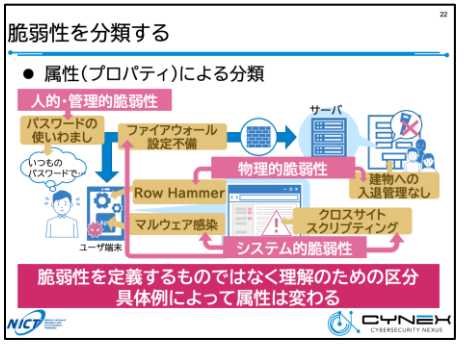
■ 国産セキュリティ製品のテスト環境提供による実用化支援



国産セキュリティ製品テスト環境（機構内部ネットワーク観測システム）

■ 演習基盤開放による国内セキュリティ人材育成事業の活性化(CYROP)

サイバーセキュリティ演習基盤CYROP



CYNEXオリジナル演習教材

政府端末情報を活用した脅威情報の収集・分析『CYXROSS』（サイクロス）

- 我が国におけるサイバーセキュリティ対策は海外由来の製品に依存しているため、サイバー安全保障の観点から、国内でセキュリティ製品の創出を行い、国内の製品でサイバー攻撃に対応できる体制を整備する必要がある。
- **安全性や透明性の検証が可能なセンサーを政府端末に導入してサイバーセキュリティ情報を収集し、国立研究開発法人情報通信研究機構（NICT）の能力を活用して分析**する実証事業を実施。
- NICTが開発した様々な技術や観測等で蓄積したデータも活用し、我が国独自のサイバーセキュリティに関する情報を生成。

安全性・透明性を検証可能なセンサー(ソフトウェア)を開発し政府端末に導入

サイバー脅威

サイバー脅威

サイバー脅威

収集した情報をNICTに集約

・検体情報
・アラート情報
・端末情報　等

分析結果を各省庁等に提供

・検体分析結果
・攻撃傾向の統計情報
・サイバー脅威情報(IoC) 等

我が国独自のサイバー情勢分析能力を強化
政府システムのセキュリティ対策を強化

NICTの能力強化

NICT
情報通信研究機構

情報分析

NICTが開発したサイバーセキュリティ技術及び蓄積してきたデータ等を活用

NICTER
サイバー攻撃観測技術

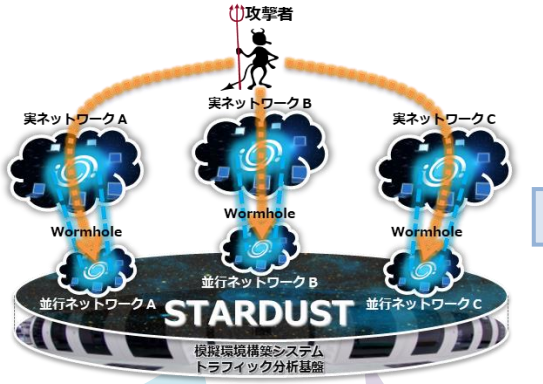
STARDUST
標的型攻撃観測・分析技術

NIRVANA改
サイバー攻撃情報統合分析技術

実践的なサイバーセキュリティ人材の育成『CYDER』（サイダー）

- サイバー攻撃が巧妙化・複雑化し、サイバーセキュリティ人材の需要は増える一方、育成が追い付かず人材不足が拡大。
- 特に、実践的な対処能力を有するサイバーセキュリティ人材を育成するためには、実際にサイバー攻撃を受けた場合を想定して、実機の操作を伴う演習を模擬環境を用いて行う必要（しかしそのような模擬環境の構築にはかなり高度な技術が必要）。
- 情報通信研究機構（NICT）においては、STARDUST等の研究開発を通じて高度な模擬環境の構築技術等を有していることから、これを用いて**実戦さながらの演習の環境・教材を構築**。
- この演習環境・教材を活用し、**実践的サイバー防御演習「CYDER」**を実施、人材育成を推進。

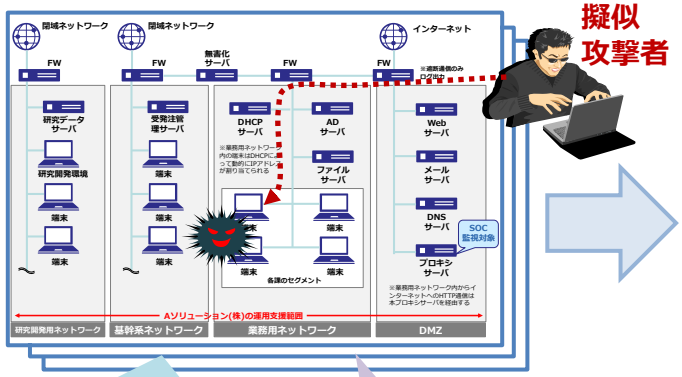
NICTの研究で得られた知見・ノウハウ



攻撃者をだますほどのリアルな模擬環境の構築技術

最新のサイバー攻撃の観測・分析結果

実戦さながらの演習環境・教材の構築



企業・地方公共団体の**社内LANや端末を再現**した環境を構築

最新のサイバー攻撃動向を踏まえた**演習シナリオ**を作成

実践的サイバー防御演習「CYDER」の実施

専門指導員による補助

本番同様のデータを使用した演習

実機の操作を伴う**実戦さながらの模擬演習**

国機関、地方公共団体、重要インフラ事業者等を中心に**年間3,000人以上を育成**
また、ASEAN地域や大洋州島しょ国に対する能力構築支援など、**外交・海外展開の場でも活用**

産業界への期待

１．ネットワーク上の脆弱性への対応

セキュリティ対策においては、ネットワークで発見された脆弱性に対して速やかに対処し、セキュリティ上のリスクを低減させる取り組みが重要

⇒ ネットワークやICTシステムに**知見を有する企業**が積極的に**脆弱性情報を収集**し、情報共有や**顧客の対処支援**を行うことで、社会全体のセキュリティリスクが低減

２．サイバーセキュリティ人材育成

サイバーセキュリティ事案への対処や脆弱性対応の重要性が増大し、対応できる人材の育成が急務

⇒ 産業界としてこれらに速やかに対応できる**人材育成が質、量の両面から必要**