総務省のサイバーセキュリティ政策の動向

２０２５年２月

総務省　サイバーセキュリティ統括官室
総括補佐　梅城 崇師

自己紹介

梅城　崇師　（うめき　たかのり）

2007年　**総務省 入省**

2013年
３年間

内閣サイバーセキュリティセンター(NISC)　出向

- ✓ 重要インフラ事業者等のサイバーセキュリティ対策
- ✓ サイバーセキュリティ基本法（2014.11成立）
- ✓ 日本年金機構における不正アクセスによる情報流出事案（2015.6）

2019年
２年間

総務省 サイバーセキュリティ統括官室

- ✓ 人材育成、IoT機器対策等
- ✓ 新型コロナ対応（2019.12）
- ✓ テレワークセキュリティ対策

2022年
２年間

デジタル庁 出向

- ✓ デジタル大臣秘書官（サイバーセキュリティ担当大臣も兼務）
- ✓ マイナンバー、自治体システム標準化を始め諸々
- ✓ 能動的サイバー防御の制度検討

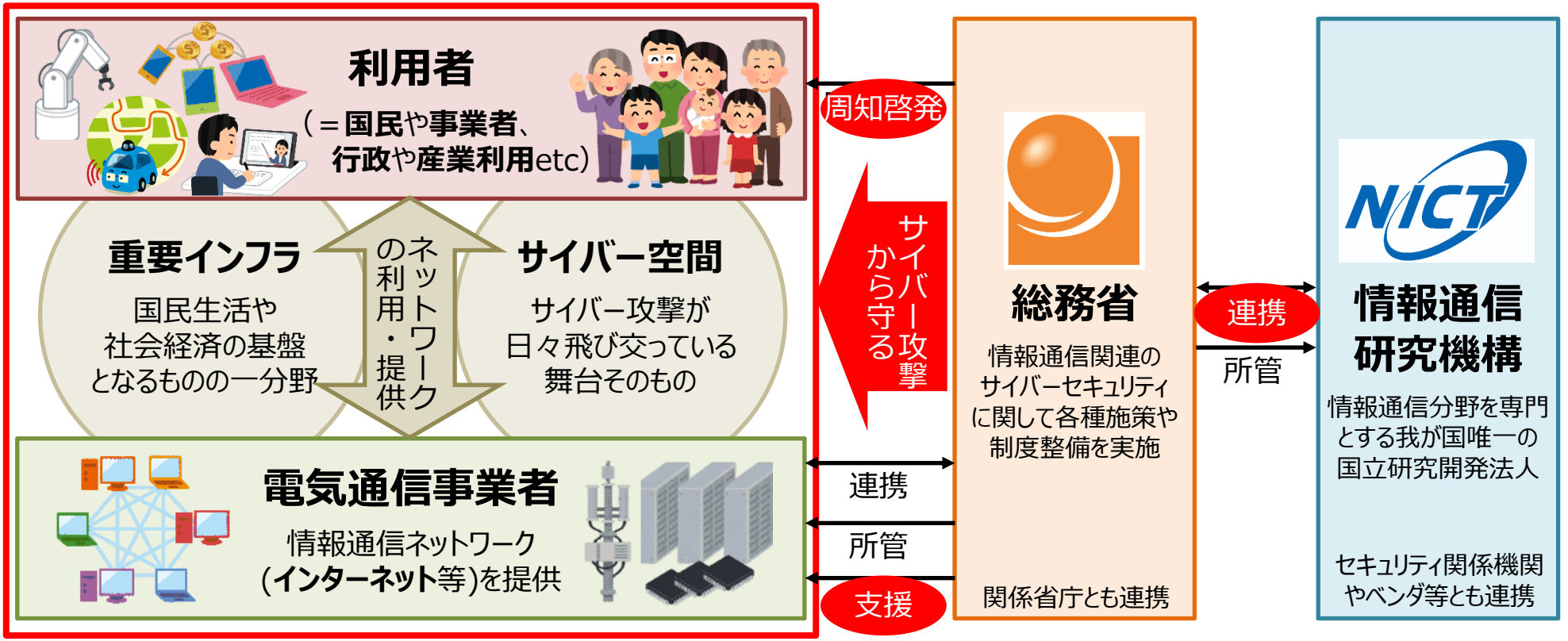
2024年

総務省 サイバーセキュリティ統括官室（再び）

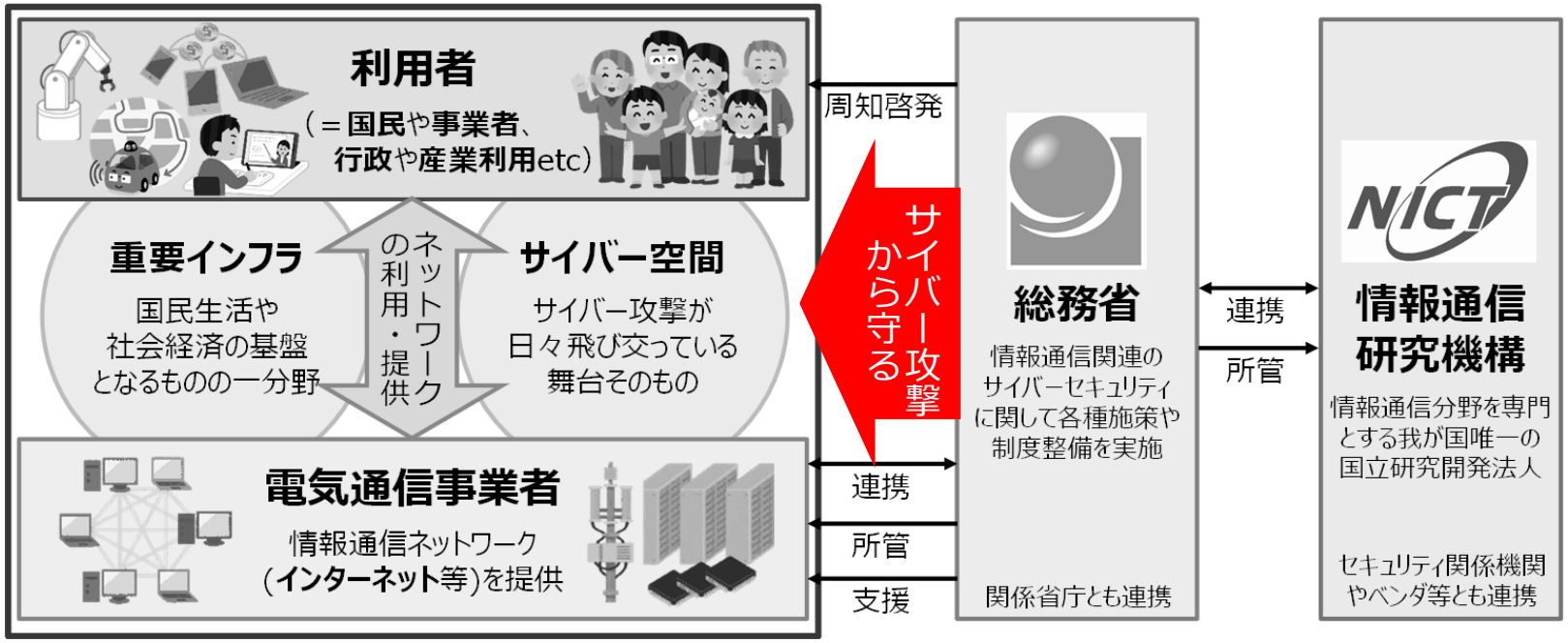
- ✓ 統括補佐（室内全体のとりまとめ）

サイバーセキュリティにおける総務省の役割

- 総務省所管である**電気通信事業者～情報通信ネットワーク～インターネット**は２つの側面
  - 機能停止すれば国民生活や経済社会に甚大な影響が発生する**重要インフラ**（国の基盤となる15分野の一つ）
  - サイバー攻撃が飛び交う**サイバー空間そのもの**（サイバーセキュリティ確保のための重要な役割）
- **情報通信研究機構(NICT)**は、**サイバー攻撃**に関する**観測・分析**を長年行い、**高度な技術・人材**を保有
- **総務省**はNICTや電気通信事業者等と連携し、**ネットワークや利用者**を**サイバー攻撃から守る**取組を実施
  （加えて、脅威情報・技術の国産化プロジェクトを推進し、我が国自らの力で脅威を検知し対抗できる基盤を構築）

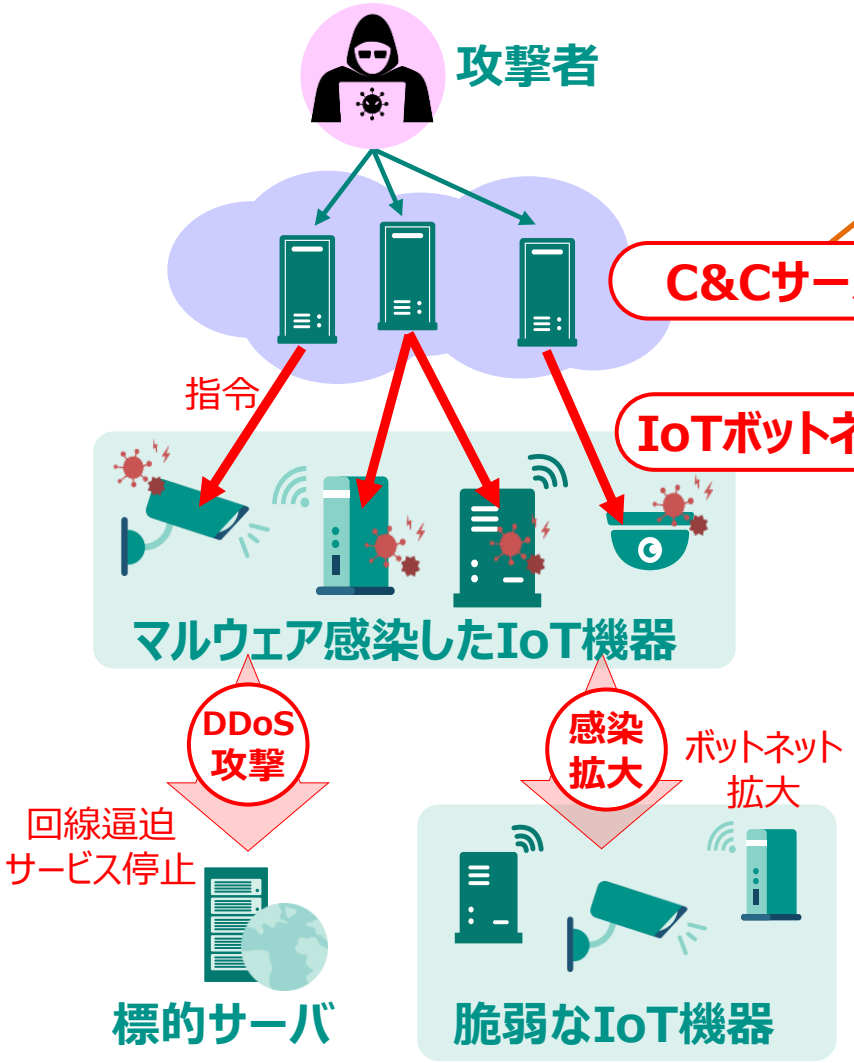


①ネットワークをサイバー攻撃から守る



IoT機器を悪用したサイバー攻撃(DDoS攻撃等)への対策

- IoT機器の急増に伴い、**IoT機器を悪用**した大規模なサイバー攻撃（**DDoS攻撃**等）が発生
- DDoS攻撃は**ネットワーク全体の速度低下**を引き起こしかねないほか、**標的側での対応が難しい**
- 総務省・ISP等が協力して、攻撃指令を行う**C&Cサーバ**と、攻撃役となる**脆弱なIoT機器**の両面から対策



IoTボットネットに対して指令通信を出す C&Cサーバへの対処

電気通信事業者がネットワークの管理のために利用する「**フロー情報**※」を**分析**することで、**C&Cサーバを検知**
→ 対策に活用するための**実証事業を実施中**

※IPアドレス、ポート番号、プロトコル、パケット数などに関する情報
ヘッダー情報のみでペイロード（データの本体部分）は含まない

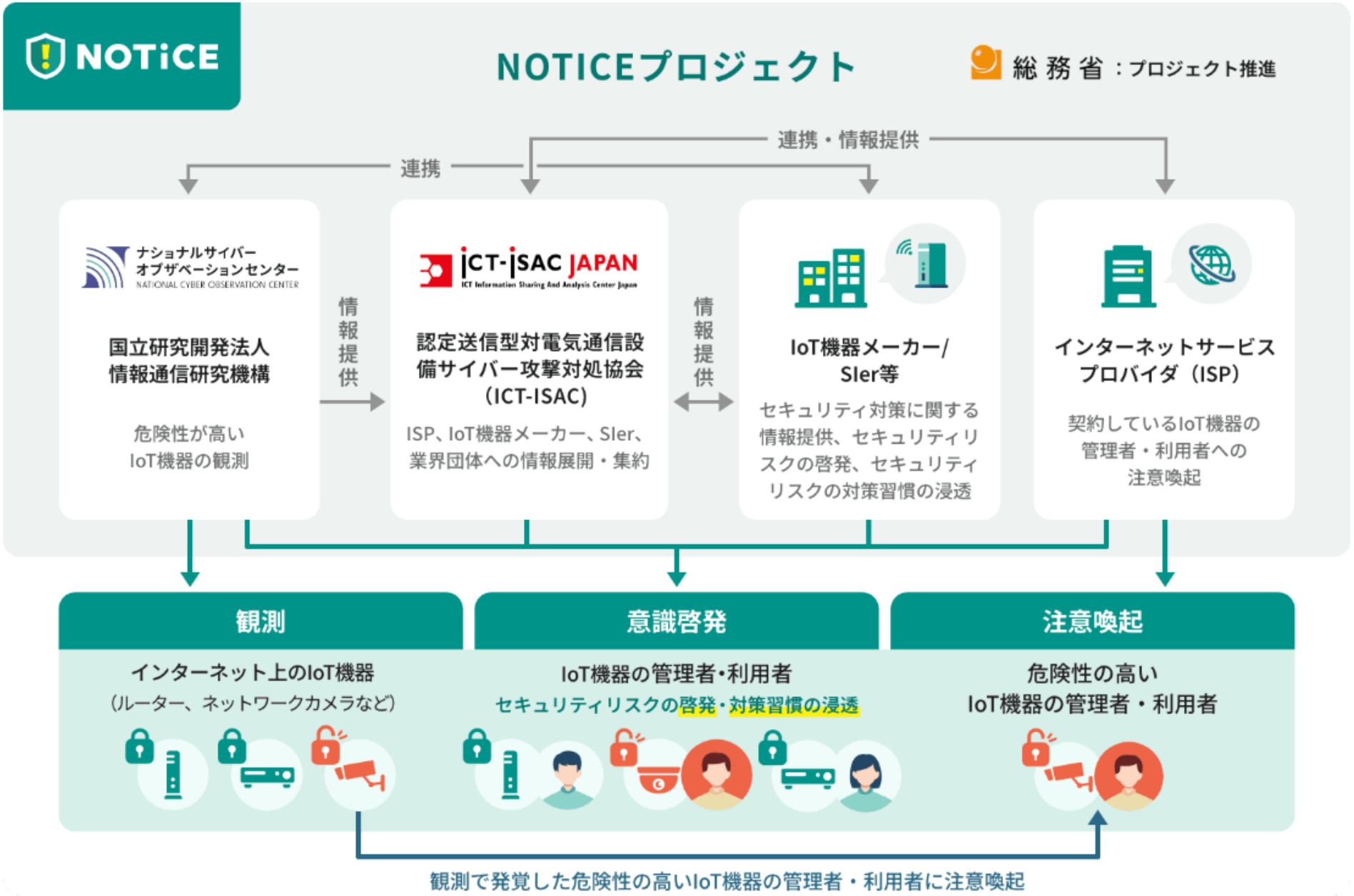
マルウェアに感染した/感染する危険性が高い 脆弱なIoT機器への対処

サイバー攻撃に悪用されるおそれのある**IoT機器を調査**し、
（サイバーセキュリティに知見のあるNICTにおいて調査を実施）
電気通信事業者を通じ、**IoT機器の利用者に注意喚起**

＜調査＆注意喚起の対象＞
① 既にマルウェアに感染している機器
② ファームウェアの脆弱性等がある機器
③ ID・パスワードの設定に脆弱性がある機器

→「**NOTICE**」プロジェクト NOTiCE

NOTICEプロジェクト概要



2024年12月のNOTICE実施状況

IoT機器観測総数

月1.25億件

参加インターネットサービスプロバイダ（ISP）のIPアドレスに対して観測している総数

容易に推測可能なID・パスワードであるIoT機器

月14,665件

容易に推測可能なIDやパスワードを使用しているため、攻撃者によって管理権限を乗っ取られたり、サイバー攻撃に加担させられる危険性がある機器

ファームウェアに高リスク脆弱性を有するIoT機器

月4,399件

第三者に不正利用される危険性があるファームウェア脆弱性を有するIoT機器

マルウェア感染IoT機器検知数

最大1,929件/日

Miraiに既に感染していると推定されるIoT機器。サイバー攻撃に加担させられている可能性がある。

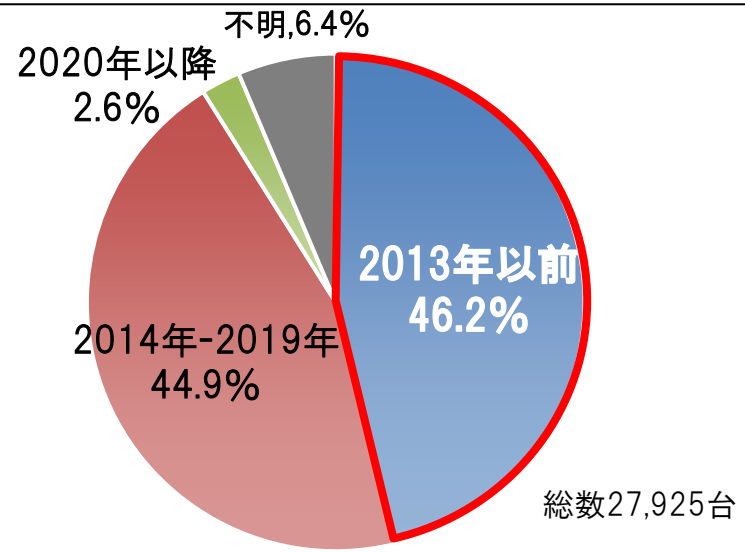
※IPアドレスが変動している場合は、重複して計上している場合があります
※当月1日あたりの最大値を掲載しています

IoT機器に関して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機器のセキュリティ対策

➢ IoT機器のセキュリティ対策は、**管理者**を置いて**継続的**に管理することが重要。振り返りを。

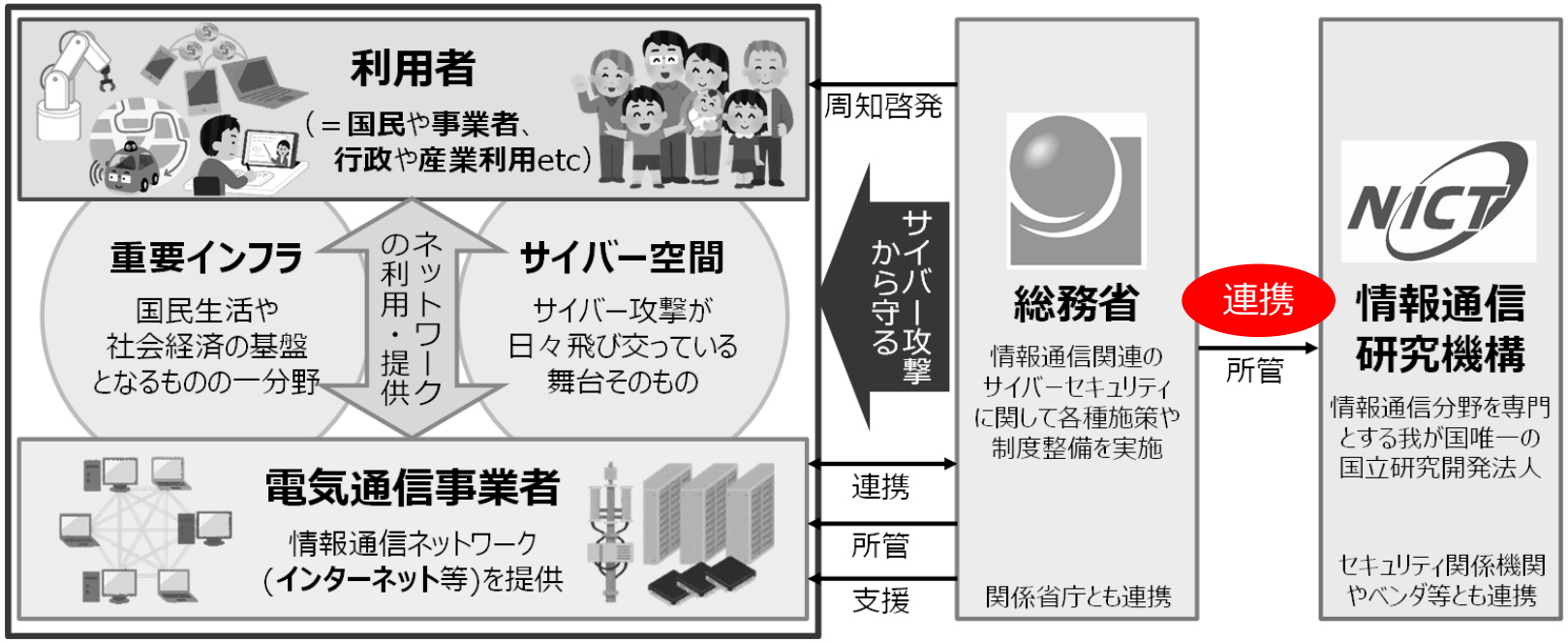
設置時のチェック項目

- ✓ ファームウェアが最新版でない場合はアップデート
- ✓ 推測されにくい複雑なパスワードに変更
- ✓ 使用しない機能や設定は無効

利用中の定期的なチェック項目

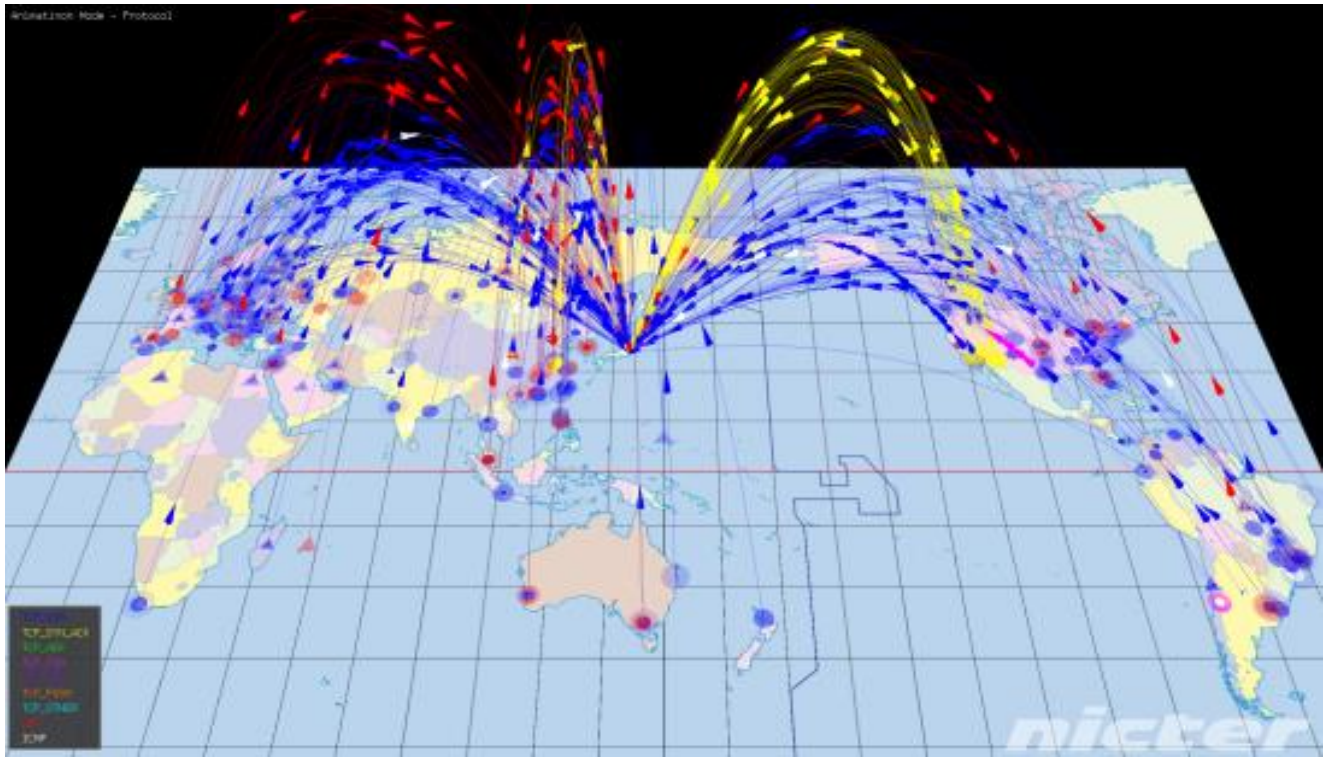
- ✓ ファームウェアが最新版でない場合はアップデート
- ✓ サポートが終了したルーターやネットワークカメラは買い替え

②研究機関であるNICTとの連携



NICTER （ニクター）・DAEDALUS（ダイダロス）

- ダークネット（未使用ＩＰアドレス）への通信をセンサーで観測することで、**サイバー攻撃の地理的情報や攻撃量、攻撃手法等をリアルタイムに可視化**し、**24時間365日観測中**。
- 本技術を応用して、地方公共団体情報システム機構（J-LIS）との協力により、2013年から**ウイルスに感染した自治体へDAEDALUS（ダイダロス）によるアラートを提供**。
- DAEDALUSは、2024年3月時点で、**772の自治体等**に導入済み。

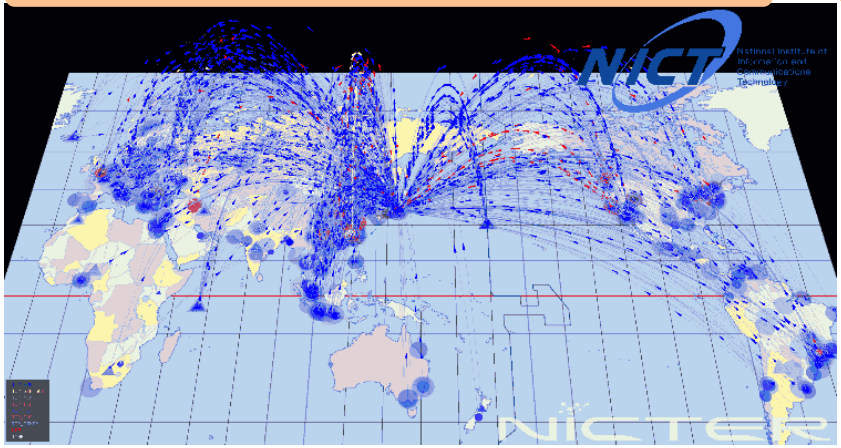


※NICTER（**N**etwork **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse）※DAEDALUS (**D**irect **A**lert **E**nvironment for **D**arknet **A**nd **L**ivenet **U**nified **S**ecurity)

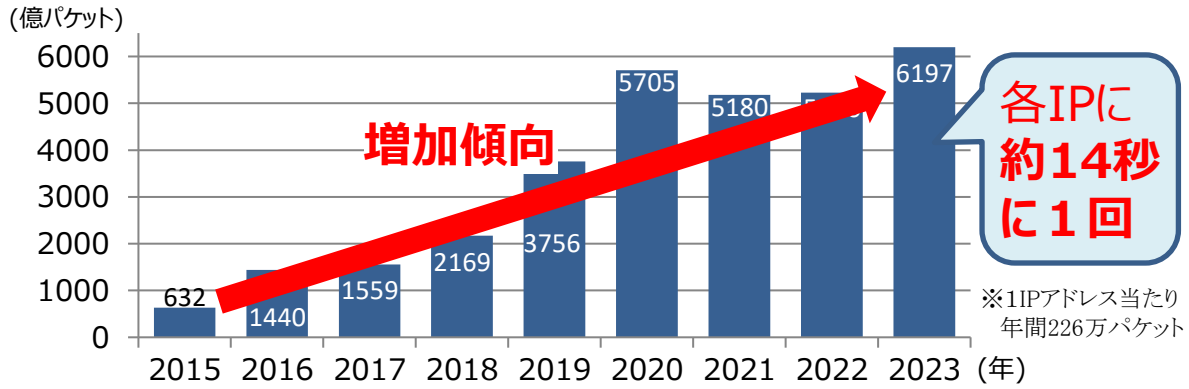
NICTERによる観測結果（セキュリティ脅威の増大）

- ✓ サイバー攻撃は量的にも増大。**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「NICTER」にて**グローバルにサイバー攻撃の状況を観測**しているが、**サイバー攻撃関連の通信は年々増加**。
- ✓ 攻撃通信のターゲットとしては、ルータやWebカメラ等の**IoT機器を狙ったものが最多**。

NICTERにより観測されるサイバー攻撃の様子



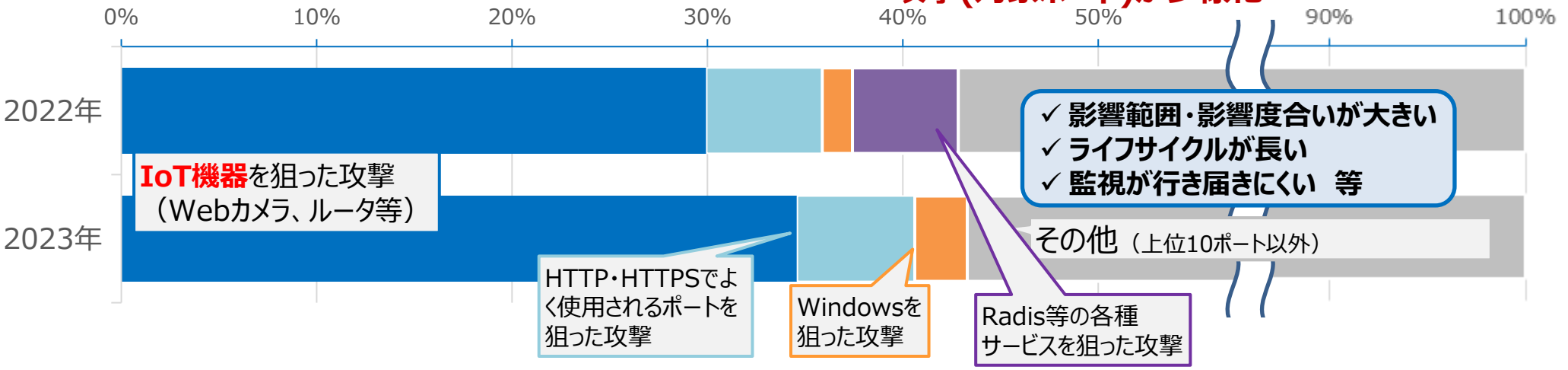
NICTERで１年間に観測されたサイバー攻撃関連の通信数



（出典）国立研究開発法人情報通信研究機構「NICTER観測レポート2023」を基に作成

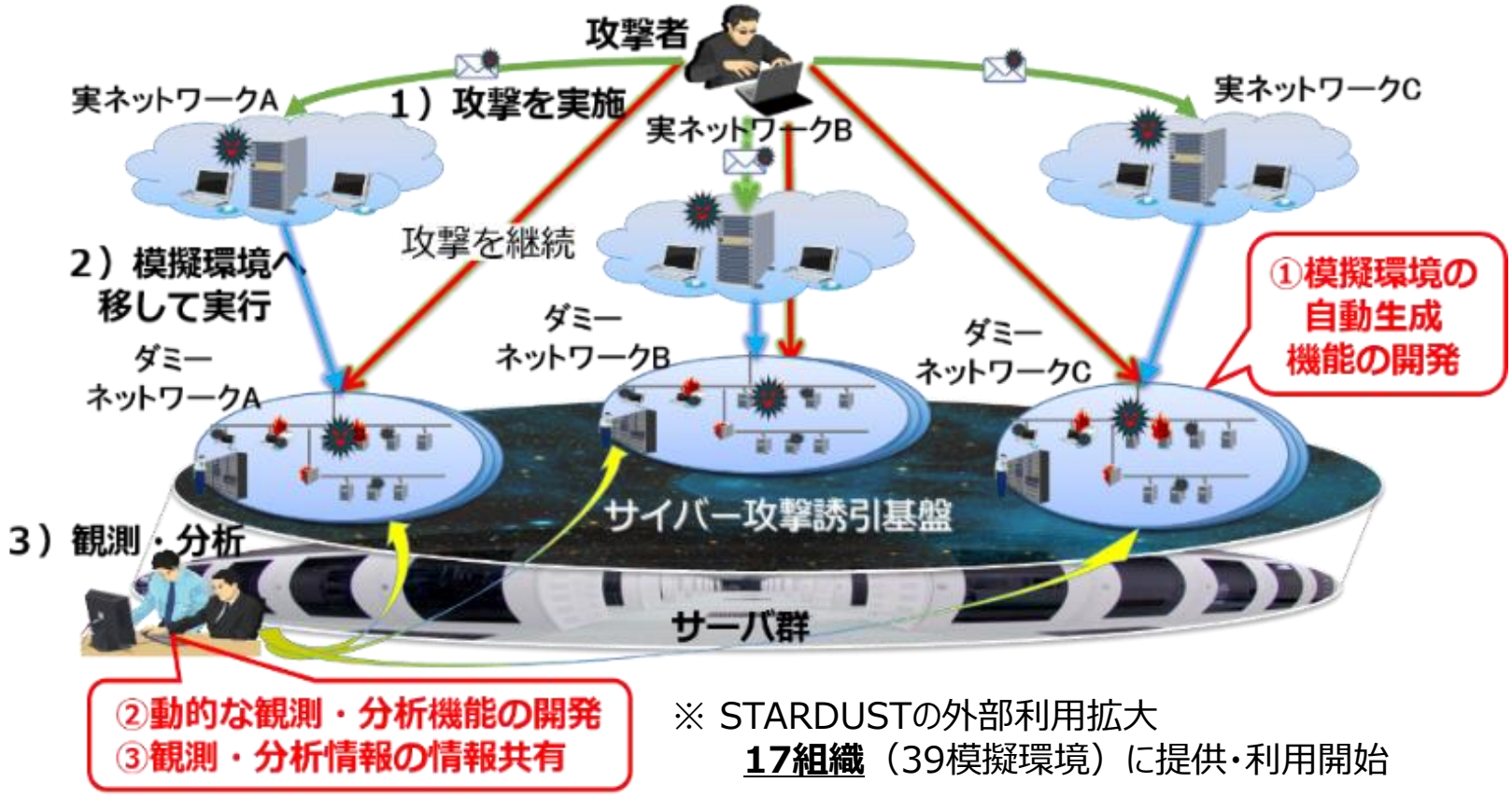
NICTERにより観測された通信の内容（上位10ポートの分析）

- ✓ **IoT機器を狙った攻撃が依然としてトップ**
- ✓ **攻撃(対象ポート)が多様化**



STARDUST （スターダスト）

- 高度かつ複雑なサイバー攻撃に対処するため、**政府や企業等の組織を精巧に模擬したネットワークに攻撃者を誘い込み**、**攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握する**ことが可能な、高度で効率的な**サイバー攻撃誘引基盤**（STARDUST）を構築。
- STARDUSTを用いて攻撃誘引を行うことで、標的型攻撃の実データを作り出し、**攻撃者をだますほどリアルな模擬ネットワーク構築及び対策技術のノウハウを蓄積**することができる。

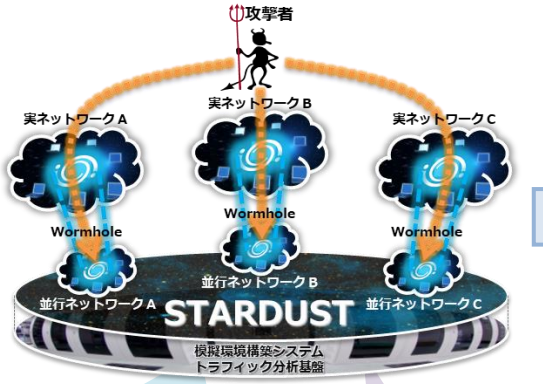


※ STARDUSTの外部利用拡大
17組織（39模擬環境）に提供・利用開始

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。

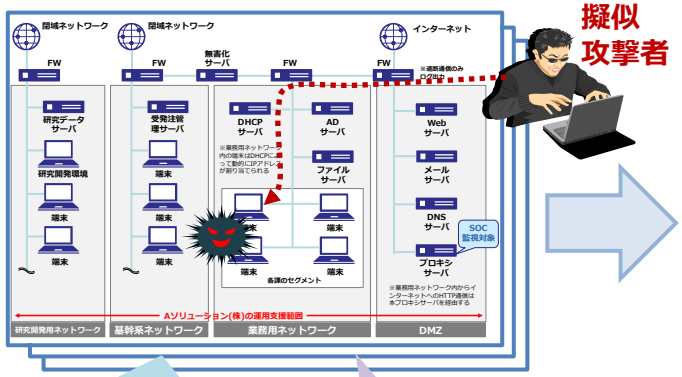
NICTの研究で得られた知見・ノウハウ



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**

ナショナルサイバートレーニングセンターによる人材育成

- 2017年4月より、情報通信研究機構（NICT）に**「ナショナルサイバートレーニングセンター」**を設置。
- NICTの研究成果等を活用して、実践的サイバー防御演習「CYDER」のほか、万博向けサイバー防御演習「CIDLE」、若手人材を対象とした育成プログラム「SecHack365」を実施。

CYDER（サイダー）

国機関・地方公共団体・独立行政法人等を対象とした「実践的サイバー防御演習」

全国の会場で**年間計100回**、**計3,000名規模**で実施
2017年度以降、延べ**20,000名超**が受講

CIDLE（シードル）

2025年大阪・関西万博関連組織を対象とした「万博向けサイバー防御講習」

2023年度から、**万博関連組織を対象**として、**オリパラ2020東京大会のレガシーも活用**し、
NICTの豊富な知見に基づく**講義・演習プログラム**を実施

SecHack365（セックハック サンロクゴ）

25歳以下の若手人材を対象とした「セキュリティイノベーター育成プログラム」

年間40名程度の受講者を選抜し、**1年間のトレーニング**コースを実施
2017年度以降、計**289名が修了**

実践的サイバー防御演習
CYDER

万博向けサイバー防御講習
CIDLE

セキュリティイノベーター育成プログラム
SecHack365

データ負けのスパイラル

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

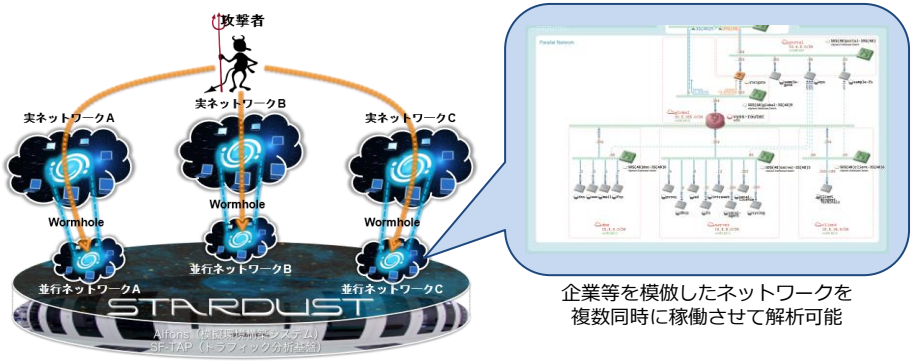
国内でサイバーセキュリティ情報を生成・蓄積・提供し、また人材育成にも活かす環境が必要

研究開発・人材育成の産学官連携拠点『CYNEX』

- 国内で**サイバーセキュリティ情報を生成・蓄積・提供**し、これを**分析し対処できる人材の育成**が重要
- 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
  サイバーセキュリティ研究室・・・サイバーセキュリティ関連の**最先端技術の研究開発**
  ナショナルサイバートレーニングセンター・・・実践的サイバー防御**演習等による人材育成**
- これらのデータ・知見を活用し、**産学官の結節点(ネクサス)**となる先端的基盤の構築のため
  ＣＹＮＥＸ（CYbersecurity NEXus：**サイネックス**） を2021年４月に組織

CYNEXの具体的な活動

■ 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

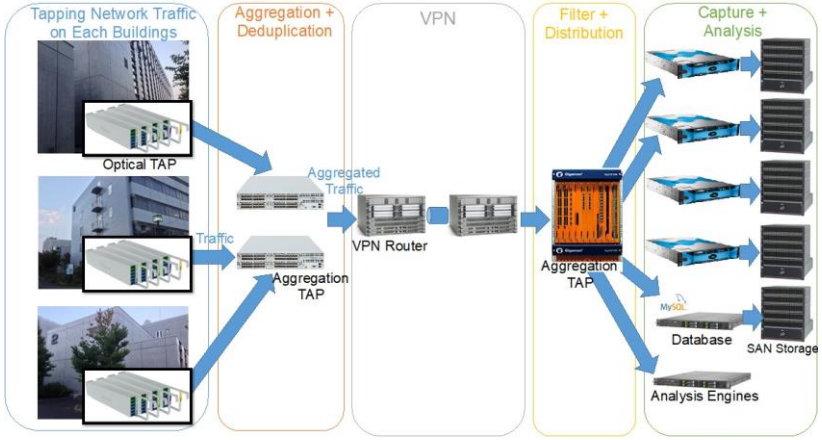
■ 高度な解析者の育成とCYNEX独自の脅威情報の生成・発信

自主学習型オンラインSOC研修

OJTでのSOC業務従事

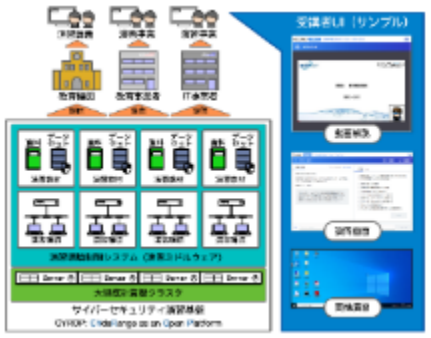
国産脅威情報発信/提供

■ 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

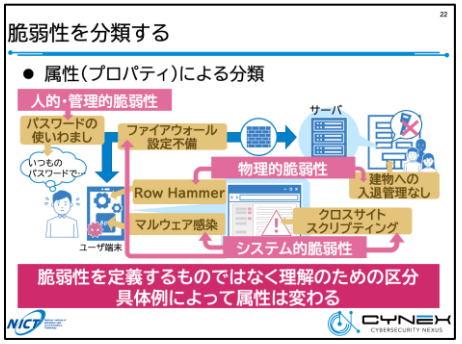


国産セキュリティ製品テスト環境（機構内部ネットワーク観測システム）

■ 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

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

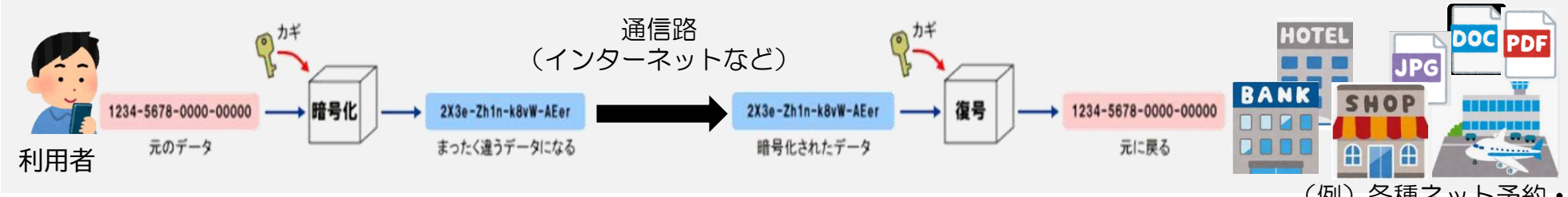
分析結果を各省庁等に提供

・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

NICTにおける暗号技術の研究開発

サイバーセキュリティにおける暗号技術の重要性

- 「**暗号化**」とは、送信者と受信者の間の**通信の内容を秘匿**し、**第三者（他人）による解読を困難にする**こと。
  例えば、ネットサービスでは、個人情報、パスワード、クレジットカード情報等の暗号化により、利用者は安心してサービスを利用可能。



（例）各種ネット予約・クラウドサービス等

- 暗号は、通信相手の**本人性確認**や通信内容の**非改ざん性確認**にも応用されている。
- デジタル経済におけるセキュリティの確保のためには、常に**高い安全性**が保証された**暗号技術の利用**が不可欠。

暗号技術に係る現状とNICTの取組

- **暗号技術の安全性は、**一般に**解読時の計算量に依拠**。
- 近年、**スパコンの処理能力の向上**により、**現行の暗号が解読**され、安全・安心な通信が脅かされる**リスク（＝危殆化）**。
- さらに、**将来の量子コンピュータの実用化や、未知の解読手法の発見により、現行の暗号が急激に危殆化するリスクも**。
  量子コンピュータの実用化時期は未定だが、現在でも**ハーベスト攻撃**※の脅威が指摘。

  Googleが開発中の量子コンピュータは、スパコンで47年間かかる計算を一瞬で完了させた。（2023年）

（※）ハーベスト攻撃とは、量子コンピュータが実用化されるまでの間に暗号処理されたデータを盗聴などにより大量に収集しておき、量子コンピュータが実現したタイミングで一気にデータの解読を行うという攻撃手法。

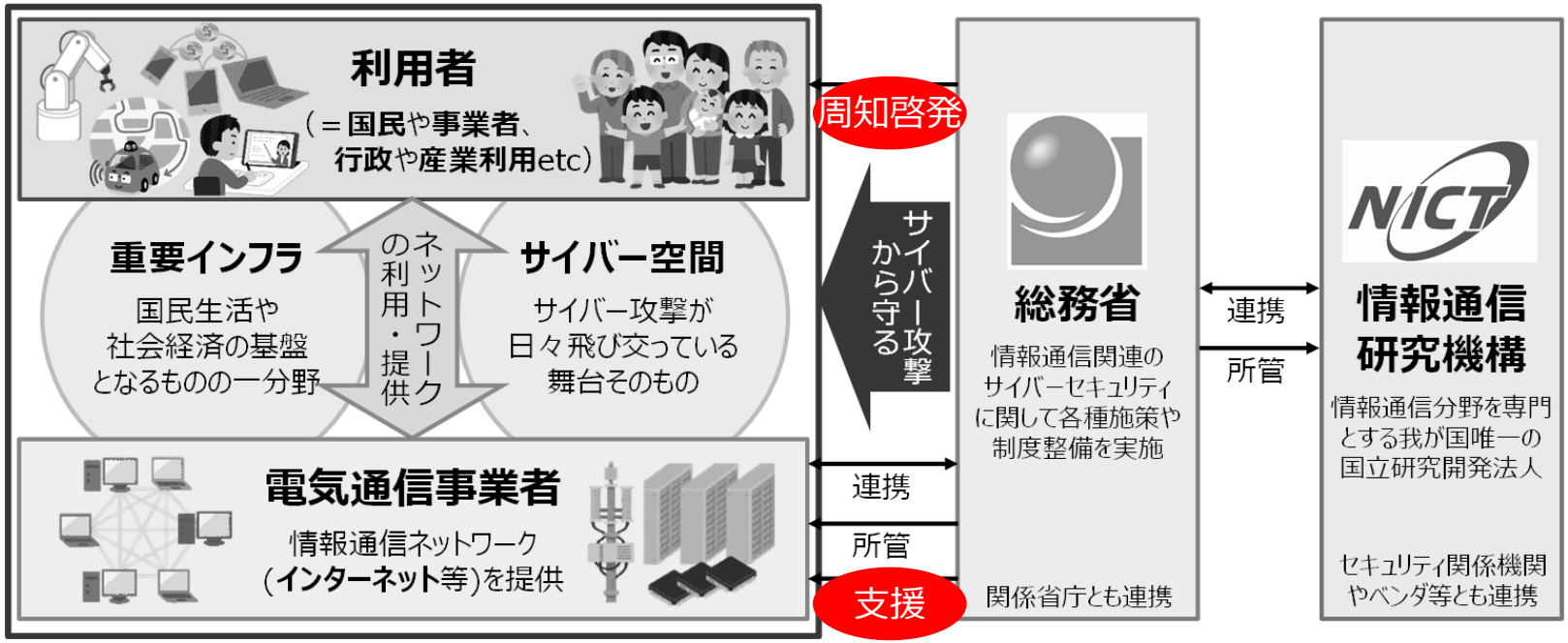
- 解読技術の向上に対抗するには、**現行の暗号の評価・監視**、**新たな暗号への移行**が定期的に必要

⇒ **CRYPTREC**（クリプトレック）プロジェクトにおける評価・監視プロセスにより**電子政府推奨暗号リストを随時更新**

- 暗号技術は、機密保持・安全保障にも関わりうることから、他国に委ねず、**自国において暗号技術の研究や評価に必要な人材を育成・確保**する必要性

⇒ NICTは、格子暗号と多変数公開鍵暗号の**解読コンテスト**において**世界記録を達成**

③事業者への支援＆利用者への周知啓発



ISP等に対するネットワークセキュリティの確保

- インターネットは歴史的に、接続性と可用性を重視し、信頼できる限られた環境での使用が想定
  →仕様に脆弱な部分があり、**通信経路(BGP)**や**DNSのハイジャック**、**なりすましメール**などが発生・懸念
- **セキュリティ向上策（電子認証技術を活用したRPKI／DNSSEC／DMARC）**が国際標準化
- 費用や導入インセンティブの面から、国内での普及が進まないため、**ガイドライン策定**により導入を後押し

BGPハイジャック

Border Gateway Protocol
＝ネットワーク間で経路情報を交換するためのプロトコル

RPKI (Resource Public-Key Infrastructure)

IPアドレスとAS(ネットワークの集まり)番号の正当な所有者が、デジタル署名付きの情報を登録
受け取った経路情報が登録情報と一致するか確認することで、経路情報が正当かを確認
※登録情報をROA(Route Origin Authorization)、確認検証プロセスをROV(Route Origin Validation)という

→IPアドレスの分配を受けた者と、AS運用者の対策をガイドライン化
→JPNICから公開(2024.11) https://www.nic.ad.jp/ja/rpki/guideline/

DNSハイジャック

Domaine Name System
＝ドメイン名をIPアドレス等に紐付けるための技術

DNSSEC (Domain Name System SECurity Extensions)

ドメインに関する正当な情報を保持するDNSサーバ(権威DNSサーバ)で、登録情報にデジタル署名を付与
DNS情報を読み取る側(フルリゾルバ)がデジタル署名を確認することで、DNS情報が正当かを確認

→ドメイン名登録者、権威DNSサーバ運用者、フルリゾルバ運用者の対策をガイドライン化
→ガイドライン公開に向け検討・調整中

なりすましメール

DMARC (Domain-based Message Authentication, Reporting and Conformance)

ドメインの正当な所有者(メール送信側)が、処理方針をDNS上で宣言
受信側は、SPFやDKIMの検証を実施し、検証失敗時に送信側の処理方針に従って処理
※SPF：送信元IPアドレスを確認し、正当なドメインからのメールかを確認する仕組み
※DKIM：メールにデジタル署名を追加し、内容の改ざんを防ぐ仕組み
※処理方針：認証失敗時の処理方針として、何もしない(none)/隔離(quarantine)/拒絶(reject)を記載

→メール送信側、メール配信・再配信事業者、メール受信側の対策をガイドライン化
→迷惑メール対策推進協議会から公開(2024.6) https://www.dekyo.or.jp/soudan/aspc/report.html

地域に根付いたセキュリティコミュニティの形成促進

■ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ（**地域SECUNITY（セキュニティ）**）の形成を促進。

- 全国規模で事業展開する企業に比べ、地域の企業や地方公共団体などについては、有効なサイバーセキュリティ対策をとるための人材育成・普及啓発の機会や情報共有の枠組みなどが不足。

➡

- 地域の企業や地方公共団体については、各者とも単独で有効なサイバーセキュリティ対策をとることは困難であり、地域レベルでのコミュニティを形成して情報共有等を強化する必要。

地域に根付いたセキュリティコミュニティ

セキュリティコミュニティの形成の促進

●①当該地域における大手事業者、②業界団体（地方支部など）、③都道府県警、④サイバーセキュリティ関係事業者・機関、⑤地方公共団体、⑥有識者などによる地域のサイバーセキュリティ向上のための推進体制を構築する。なお、情報共有体制がすでに存在している地域においては、既存の体制を活用。

セキュリティ関連の情報共有

定期的なセミナーや演習等の実施

●地域の企業等向けに①定期的なセミナーやインシデント演習の実施、②セキュリティ関連の情報共有の枠組みなどを構築。

無線LANのセキュリティ対策

- 総務省では、**無線LAN(Wi-Fi)のセキュリティ対策**のため、2004年からガイドラインを作成
  ※2004年5月「安心して無線LANを利用するために」
- 新技術や最新のセキュリティ動向に対応するため、**2024年３月に最新の改定版を公表**

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/ →

自宅 Wi-Fi利用者 向け 簡易マニュアル

✓ 自宅にWi-Fiを設置・利用する方に向け、次のポイントをわかりやすく解説

① セキュリティ方式は **WPA2 または WPA3** に（WEPやTKIPは避ける）

② **パスワードは第三者に推測されにくい**ものに（管理用パスワードも要注意）

③ **ファームウェアを最新**に（自動更新設定を推奨）

公衆 Wi-Fi利用者 向け 簡易マニュアル

✓ 外出時に公衆Wi-Fiを利用する方に向け、次のポイントをわかりやすく解説

① 接続する**アクセスポイントをよく確認**（提供者やSSID名を確認；不審なものは使わない）

② **正しいURLでHTTPS通信**しているか確認（URL欄にエラーがない＆ドメインを確認）

公衆 Wi-Fi提供者 向け セキュリティ対策の手引き

✓ 公衆Wi-Fiを提供する方に向け、次のような点を確認するためのガイドを提示

・「公衆Wi-Fi」提供には**どのようなリスク**があるのか

・具体的に**どのような対策**をすればいいのか

テレワークのセキュリティ対策

- 総務省では、**テレワーク**の**セキュリティ対策**のため、2004年からガイドラインを作成
- **コロナ禍**による**業務環境やセキュリティ動向の変化**に対応するため**2021年に全面改定**
- ガイドラインを補完するものとして、セキュリティ専任担当がいないような中小企業等でも、**最低限のセキュリティを確実に確保**してもらうための**チェックリスト**や**設定解説**等を策定

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/ →

テレワークセキュリティガイドライン

（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４版

- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、理解や検討が難しい場合

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)

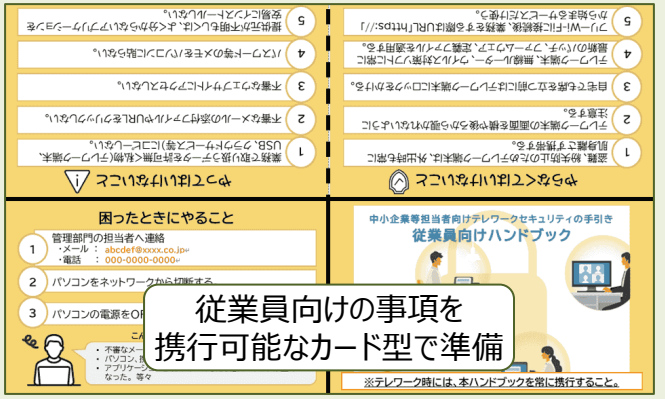
（2022年５月　第３版）

2020年９月初版
2021年５月第２版

中小企業等に向け**最低限のセキュリティを確実に確保**してもらうためのものに限定

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能



従業員向けの事項を携行可能なカード型で準備

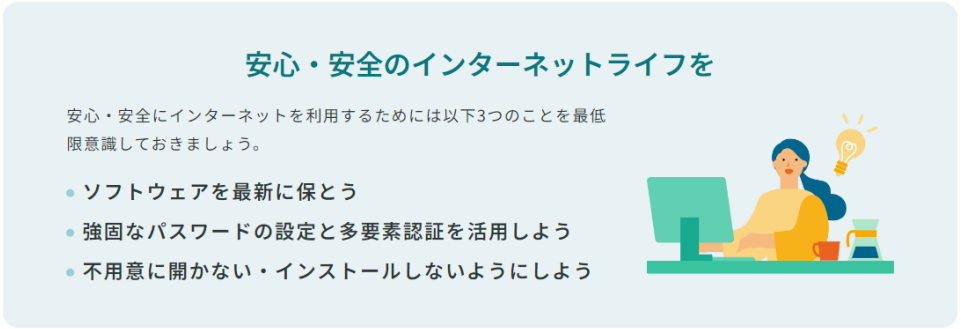
Android／Chatwork／Chromeリモートデスクトップ／Cisco ASA／Cisco Webex Meetings／Dropbox／Exchange Online／Gmail／Google Meet／Googleドライブ／iOS／LANSCOPE エンドポイントマネージャー クラウド版／LINE／macOS／Microsoft Defender／Microsoft OneDrive／Microsoft Teams chat／Microsoft Teams Meeting／Windows／Windows リモートデスクトップ／YAMAHA VPNルーター／Zoom／ウイルスバスター ビジネスセキュリティサービス／たよれーるDMS

よく利用される製品・サービスの**具体的設定**の**解説資料**も準備

適宜改定

総務省「国民のためのサイバーセキュリティサイト」

➢ 総務省は、サイバーセキュリティに関する周知啓発を一層強化するため、
2024年５月、「国民のためのサイバーセキュリティサイト」を全面的にリニューアルし、内容等を更新。



主な内容

●サイバーセキュリティ初心者のための三原則
- ・サイバーセキュリティって何？
- ・サイバーセキュリティの三原則
  - その１　ソフトウェアを最新に保とう
  - その２　強固なパスワードの設定と多要素認証を活用しよう
  - その３　不用意に開かない・インストールしない

●家庭での対策
（最低限意識してほしいこと、その他意識してほしいこと）

●職場での対策
（システムを“利用”利用する人向けの対策、
システムを“管理”する人向けの対策、
経営者向けの対策）

●事故・被害事例及び対処
（家庭での被害事例及び対処、職場での被害事例及び対処）

●システム、サービス別のセキュリティ対策
●サイバーセキュリティの基礎知識
●用語集・その他リンク

こちらのQRコードからもアクセスできます。

URL）https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

その他

AIとサイバーセキュリティ

- あらゆる分野において生成AIの実装が急速に進んでいる一方で、生成AIを巡るリスクとして、偽誤情報の拡散、プライバシーの侵害、知的財産権の侵害等に加えて、サイバー攻撃への悪用等によるサイバーセキュリティのリスクが新たに指摘されている。
- 他方、サイバー攻撃の大規模化・複雑化・巧妙化に伴い、サイバーセキュリティ対策の業務負荷が課題となっている中、サイバー攻撃対策への生成AI等の利活用が期待されている。
- こうした背景を踏まえ、生成AI等のAI技術を巡る最新動向を把握しつつ、AIに起因するセキュリティリスクを可能な限り回避・低減するための「Security for AI」に取り組むとともに、AIをセキュリティ対策に効果的に活用するための「AI for Security」に取り組むことが必要。

生成AIの負の影響

サイバー攻撃に悪用される可能性

（例）
- 生成AI利用によるフィッシングメールの巧妙化
- マルウェアの生成、亜種の大量生産

生成AIへのサイバー攻撃・脆弱性内包

（例）
- リスクにつながる悪意のある入力
- LLMの学習データの汚染
- 事業者設定ミスによる安全ではない出力処理

Security for AI
安心安全な利用の促進

① 生成AIの進展によるサイバーセキュリティへの影響に係る調査・検証
- 生成AI等がサイバーセキュリティに与える負の影響の検証・評価
- AIの安心・安全な開発・提供に向けたセキュリティのガイドラインの策定

＜実例検証＞

② 米国専門機関とのAI安全性に関する共同研究事業
- AIの安全性に係る分野の研究開発を推進するため、北米にNICTの研究拠点を構築し、米国等の様々な専門機関との共同研究事業を実施

＜理論研究＞

生成AIの正の影響

サイバー攻撃対策への活用の可能性

（例）
- サイバー防御の自動化
- セキュリティレポート作成の自動化
- 脅威インテリジェンスの精度向上
- 脆弱性のない安全なコード開発の支援
- サイバー攻撃の予見
- インシデント対応の支援

AI for Security
サイバーセキュリティ対策への活用

③ AIを用いたサイバー脅威情報収集・分析の高度化
- 世界中の様々な機関等から発信されるサイバー脅威情報をAIを活用して収集・分析するための技術を開発及び展開

＜平時の分析活動＞

④ 生成AI等を活用した重要インフラ分野におけるサイバーセキュリティ対策強化
- 生成AI等を活用した攻撃インフラ分析の精緻化・迅速化の検証
- 当該情報等を用いた対処オペレーション業務の効率化・迅速化の検証とノウハウの展開

＜攻撃インフラ特定＞

能動的サイバー防御（Active Cyber Defense）

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。