くらしの中に
総務省
MIC Ministry of Internal Affairs and Communications

サイバーセキュリティ政策の現状と課題について

2026年2月27日

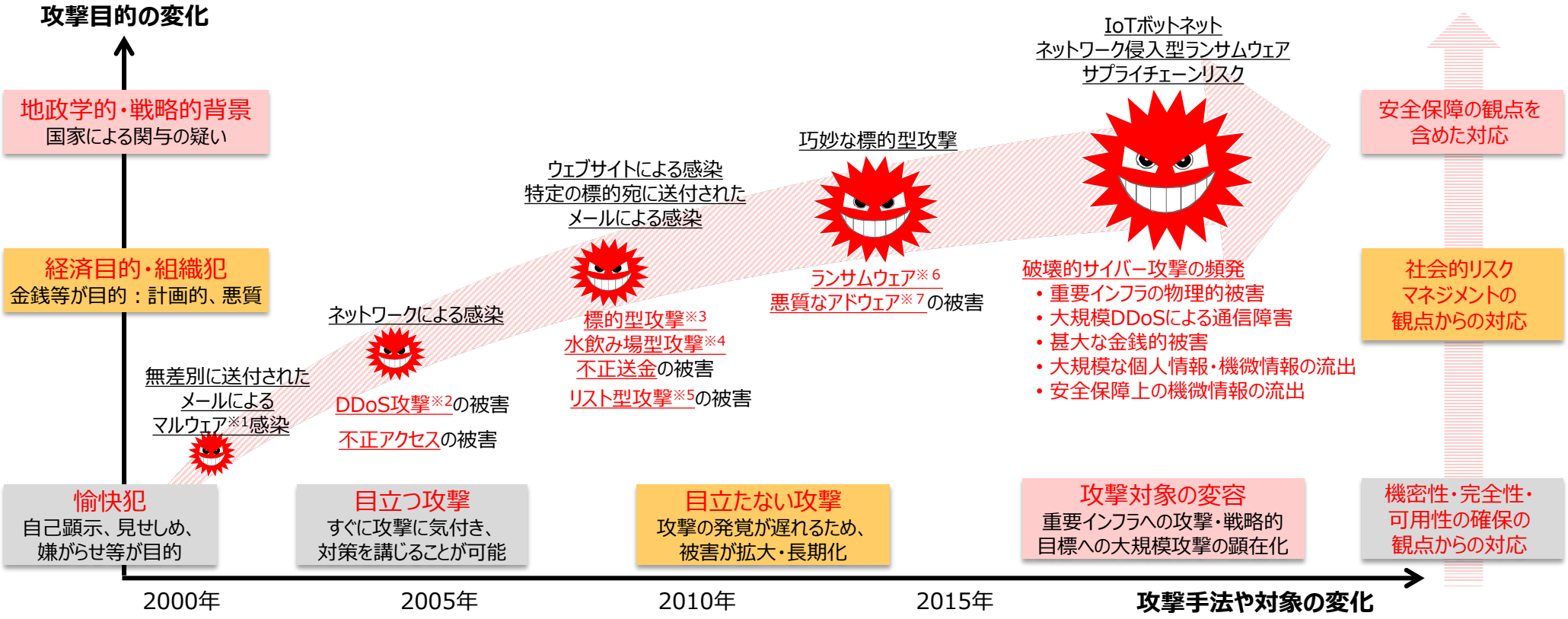
総務省 サイバーセキュリティ統括官

三田　一博

目　次

サイバー攻撃の巧妙化・高度化

- サイバー空間が国民生活や社会・経済活動の基盤となる一方、**サイバーセキュリティ上の脅威は増大の一途**
- サイバー攻撃の主体や目的の変化（愉快犯→金銭目的→地政学的・戦略的背景）、攻撃手法・対象の拡大等により、サイバー攻撃は**巧妙化・高度化し、その被害は深刻化**



※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

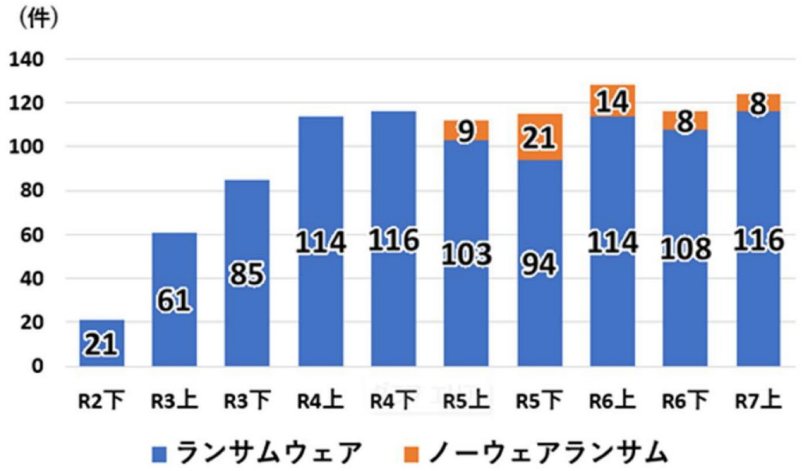
※5 リスト型攻撃　不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃

※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。

※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ウェア

サイバー攻撃（ランサムウェア）による被害

ランサムウェア被害報告件数

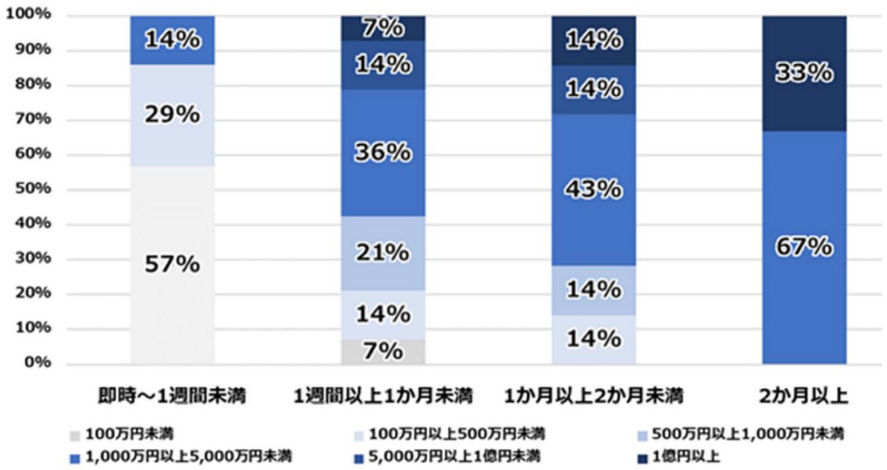


※ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。

令和７年上半期におけるランサムウェアの被害報告件数は116件であり、半期の件数として令和４年下半期と並び最多となった。組織規模別のランサムウェア被害件数は、前年と同様に**中小企業が狙われる状況が継続**しており、77件で約３分の２を占めて件数・割合ともに過去最多となった。RaaSによる**攻撃実行者の裾野の広がりが、対策が比較的手薄な中小企業の被害増加につながっている**と考えられる。

出典：令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和７年９月 サイバー警察局）

ランサムウェア被害からの復旧期間と費用の関係性



ランサムウェアによる被害に遭った企業・団体等に実施したアンケートの結果によると、令和６年と比較して、**ランサムウェアの被害による調査・復旧費用が高額化**しており、1,000万円以上を要した組織の割合は、50%から59%に増加した。中小企業の被害が増える中で費用負担が増加しており、**被害組織の経営に与える影響は決して小さくない**と考えられる。

出典：令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和７年９月 サイバー警察局）

国家を背景とした攻撃キャンペーンによる被害の深刻化

■ サイバー攻撃の巧妙化・高度化や国家を背景とした攻撃キャンペーン等により、政府機関・重要インフラ等を標的に、重要インフラサービスの停止や機微情報の流出等、**国民生活・経済活動及び安全保障に深刻かつ致命的な被害を及ぼす恐れが顕在化。**

■ 被害が生じる前に脅威を未然に排除することを含め、強固な官民連携・国際連携の下、民間事業者への情報提供、アトリビューション、アクセス無害化等、多様な手段の組み合わせによる**実効的な防止・抑止の実現が急務。**

有事を想定した重要インフラ等への事前侵入

- 2023年5月、米国は、中国を背景とするグループ「Volt Typhoon」が、事前のアクセス確保を通じた有事における米国内の重要インフラの機能不全を狙い、システム内寄生攻撃等を実施と公表。

国家背景アクターによる機微技術情報、金銭等資産等の窃取

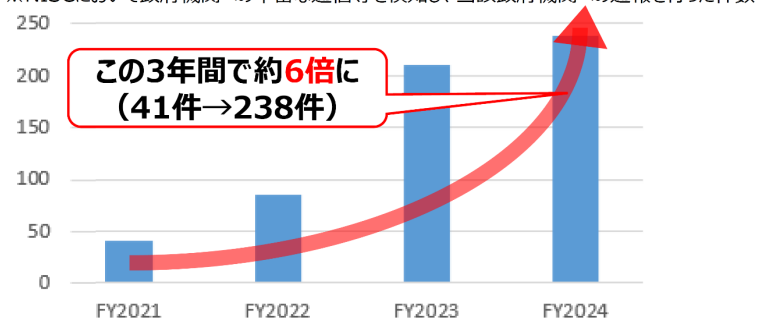
- 2019年以降、中国の関与が疑われるグループ「MirrorFace」が、日本の安全保障や先端技術に係る情報窃取を狙う攻撃キャンペーンを実行。
- 2024年5月、北朝鮮を背景とする攻撃グループ「TraderTraitor」が、暗号資産関連事業者から約482億円相当の暗号資産を窃取。

重要インフラの機能停止

- 2023年7月、名古屋港でランサムウェア攻撃によるシステム障害の発生により、業務が約3日間停止し、物流に大きな影響。
- 2024年から2025年の年末年始にかけて、航空事業者、金融機関、通信事業者等が相次いでDDoS攻撃を受け、サービス一時停止等の被害。

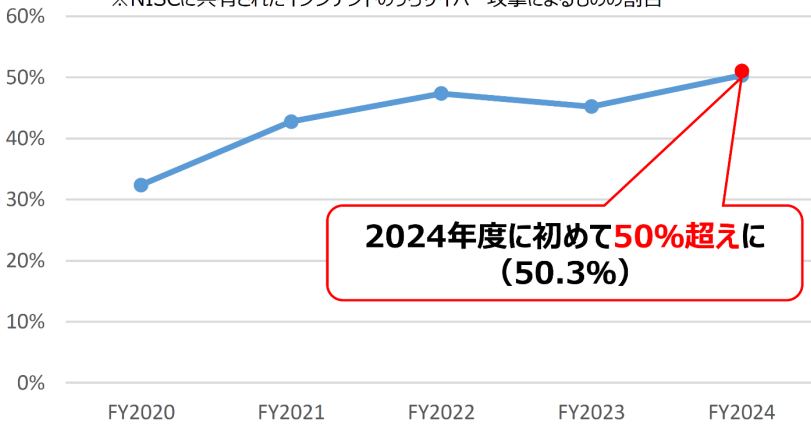
政府機関へのサイバー攻撃疑いの件数※

※NISCにおいて政府機関への不審な通信等を検知し、当該政府機関への通報を行った件数



重要インフラで発生したインシデントのうちサイバー攻撃の割合※

※NISCに共有されたインシデントのうちサイバー攻撃によるものの割合



出典：内閣官房資料

DXの浸透によるサイバー攻撃の標的・影響の多様化・複雑化

■ DXの浸透により、個人・中小企業を含め、あらゆる主体がサイバー攻撃の標的となり、直接的な被害に止まらず、サプライチェーンの停止、漏えい情報の拡散、IoT機器の乗っ取り等により、更に深刻な攻撃に発展するおそれ。

■ 政府機関・地方公共団体・重要インフラ事業者のみならず、製品ベンダー・中小企業・個人等まで、様々な主体に対し、**リスクや能力を踏まえ、適切な対策を求めていく**ことで、**社会全体のサイバーセキュリティ向上**を図る必要。

事業活動の停止・漏えい情報の拡散

2024年6月、出版事業等を行う大手企業がランサムウェアを含む大規模サイバー攻撃を受け、Webサービス等が停止したほか、個人情報や企業情報が漏えいし、SNS等を通じて拡散される二次被害も発生。

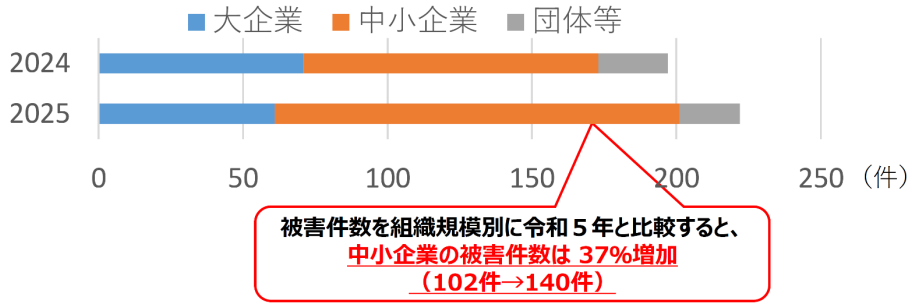
委託先・サプライチェーンへの攻撃と業務停止

- 2022年3月に大手自動車メーカーの取引先がサイバー攻撃（ランサムウェア）を受け、一部のサーバーとコンピュータ端末のデータが暗号化され、同メーカーの国内全工場が一時停止。
- 2022年10月、病院の委託先の給食事業者を経由したサイバー攻撃を受け、通常診療を一時停止。

大規模なDDoS攻撃によるサービスの一時停止

2024年から2025年の年末年始にかけて、航空事業者、金融機関、通信事業者等が相次いでDDoS攻撃を受け、サービス一時停止等の被害。（再掲）

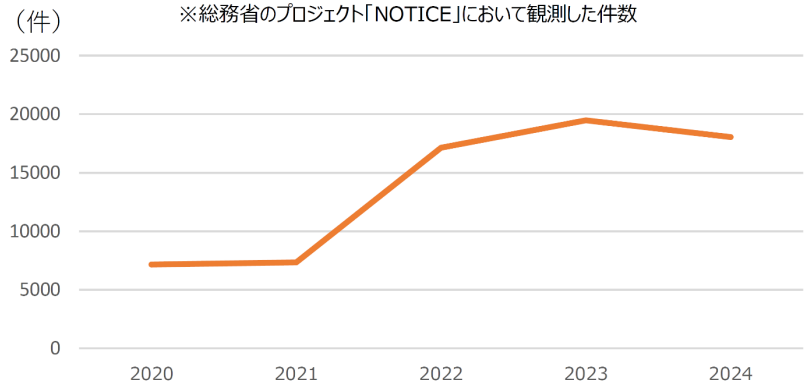
企業・団体等におけるランサムウェア被害の報告件数



出典：警察庁サイバー警察局「令和６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（令和７年３月）」「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（令和６年３月）」を基に作成

マルウェアに感染したIoT機器の検知件数※

※総務省のプロジェクト「NOTICE」において観測した件数



出典：NOTICEサポートセンター 「2025年3月時点のIoT機器観測状況」を基に作成

出典：内閣官房資料

目　次

サイバーセキュリティ政策の歩み

2000年02月

内閣官房 情報セキュリティ対策推進室 設置

- **中央省庁のウェブサイトが相次いで改ざん**される被害が発生（2000.1）
- **政府機関**向け「情報セキュリティポリシーに関するガイドライン」策定（2000.7）
- 「**重要インフラ**のサイバーテロ対策に係る特別行動計画」策定（2000.12）

2006年02月

第１次情報セキュリティ基本計画 策定

- 内閣官房 **情報セキュリティセンター**（NISC）設置（2005.4）
- **情報セキュリティ政策会議**設置（2005.5）
- 「**政府機関**の情報セキュリティ対策のための統一基準」（2005.12）
- 「**重要インフラ**の情報セキュリティ対策に係る行動計画」策定（2005.12）

2014年11月

サイバーセキュリティ基本法 公布

- 法令で初めて「**サイバーセキュリティ**」という用語が使用
- 法律に基づき、「**サイバーセキュリティ戦略本部**」が設置（2015.1）
- 法律に基づき、「**内閣サイバーセキュリティセンター**」（NISC）が発足（2015.1）
- 法律に基づき、「**サイバーセキュリティ戦略**」が閣議決定（2015.9）

2025年05月

サイバー対処能力強化法 公布

- 「**能動的サイバー防御**」の具体化
- 「内閣サイバーセキュリティセンター」が**「国家サイバー統括室」**（NCO）**に改組**（2025.7）
- 事故報告の義務化、通信情報の利用、攻撃サーバの無害化等（順次施行）

サイバー対処能力強化法等の整備

- **サイバー対処能力強化法**（正式名称は「重要電子計算機に対する不正な行為による被害の防止に関する法律」）**及び同整備法**が令和７年５月23日に公布
- サイバー対処能力強化法に基づく各般の施策を適切に機能させるための基本的な事項をあらかじめ示すとともに、これらの施策に係る事務の適正な実施を確保するための基本的な事項を示すため、**基本方針を策定**（令和７年12月閣議決定）

サイバー対処能力強化法

官民連携

- ✓ 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告
- ✓ 情報共有・対策のための協議会の設置
- ✓ 脆弱性対応の強化

通信情報の利用

- ✓ 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得
- ✓ （同意によらない）通信情報の取得
- ✓ 自動的な方法による機械的情報の選別の実施
- ✓ 関係行政機関の分析への協力
- ✓ 取得した通信情報の取扱制限
- ✓ 独立機関による事前審査・継続的検査　等

✓ 分析情報・脆弱性情報の提供等

サイバー対処能力強化法整備法

アクセス・無害化

- ✓ 重大な危害を防止するための警察による無害化措置
- ✓ 独立機関の事前承認・警察庁長官等の指揮 等
  （警察官職務執行法改正）
- ✓ 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- ✓ 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等
  （自衛隊法改正）

組織・体制整備等

- ✓ サイバーセキュリティ戦略本部の改組、機能強化
  （サイバーセキュリティ基本法改正）
- ✓ 内閣サイバー官の新設（内閣法改正）　等

施行期日
（主なもの）
【組織・体制整備等】 令和７年７月１日施行
【官民連携】【アクセス・無害化】 令和８年10月１日施行予定
【通信情報の利用】 公布の日（令和７年５月23日）から起算して２年６月を超えない範囲内において政令で定める日

（参考）サイバー対処能力強化法等 － 官民連携の強化

- 基幹インフラ事業者が**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情報共有、対処支援等の取組を強化**

基幹インフラ事業者によるインシデント報告等

- 基幹インフラ事業者は、特定重要電子計算機を導入したときは、その製品名等を事業所管大臣に届出（当該事業所管大臣は当該届出に係る事項を内閣総理大臣に通知）
- 基幹インフラ事業者は、特定重要電子計算機のインシデント情報やその原因となり得る事象を認知したときは、事業所管大臣及び内閣総理大臣に報告

情報共有・対策のための協議会の設置

- 内閣総理大臣は、サイバー攻撃による被害の防止のため、関係行政機関の長により構成される「情報共有及び対策に関する協議会」を設置
- 協議会には、基幹インフラ事業者、電子計算機等のベンダー等をその同意を得て構成員として加える
- 構成員に対しては、守秘義務を伴う被害防止に関する情報を共有するとともに、必要な情報共有を求めることが可能

脆弱性対応の強化

- 内閣総理大臣・事業所管大臣※が重要電子計算機に用いられる電子計算機等の脆弱性を認知
  → 電子計算機等のベンダー等に対して情報提供、対応方法の公表・周知
- 基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機等に関連する脆弱性の場合
  → 事業所管大臣※は、その電子計算機等のベンダー等に対し、必要な措置を講ずるよう要請　　等

（※）電子計算機やそれに組み込まれるプログラムの供給を行う事業を所管する大臣

（参考）サイバー対処能力強化法等 － 通信情報の利用

- 我が国に対する**サイバー攻撃の実態を把握するため、通信情報を利用し、分析**。これらについては、独立機関がチェック。制度設計に当たっては、**「通信の秘密」に十分配慮**

基幹インフラ事業者等との協定（同意）に基づく通信情報の取得

- 内閣総理大臣は、基幹インフラ事業者等との協定に基づき、通信情報を取得（このうち、外内通信に係る通信情報を用いて分析を実施、当該事業者に必要な分析結果を提供）

（同意によらない）通信情報の取得

- 【外外通信の分析】
  内閣総理大臣は、国外の攻撃インフラ等の実態把握のため必要があると認める場合には、独立機関の承認を受け、通信情報を取得
- 【外内通信又は内外通信の分析】
  内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、独立機関の承認を受け、通信情報を取得

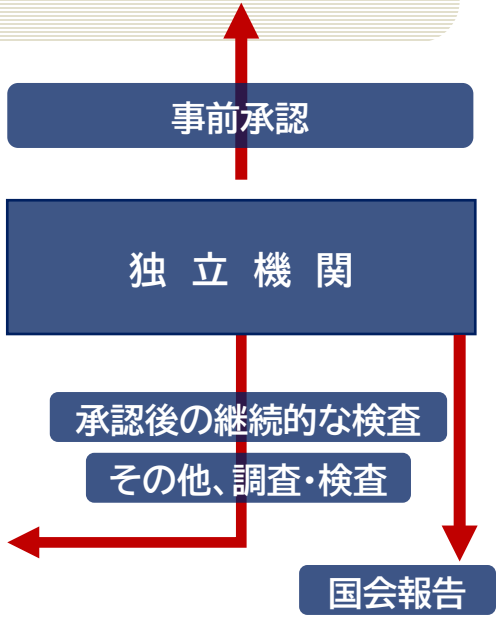
（※）外外通信：国内を経由し伝送される国外から国外への通信
外内通信：国外から国内への通信
内外通信：国内から国外への通信

自動的な方法による機械的情報の選別の実施

- 内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、調査すべきサイバー攻撃に関係があると認めるに足りる機械的情報を選別
  （それ以外のものを直ちに消去）

※ 機械的情報とは、アイ・ピー・アドレス、指令情報等の意思疎通の本質的な内容ではない情報

※ その他、関係行政機関の分析への協力、取得した通信情報の取扱制限 等を規定



（参考）サイバー対処能力強化法等 － 分析情報・脆弱性情報の提供等

基幹インフラ事業者から
届出された**電子計算機の情報**

基幹インフラ事業者から
報告された**インシデント情報**

選別した後の**通信情報**※

協議会を通じて得た情報

その他の情報
（外国政府から提供された情報等）

情報の整理・分析

通信情報や秘密を含み得る

総合整理分析情報

国の行政機関 等

通信情報は含まないが秘密は含み得る

提供用総合整理分析情報

協議会の構成員 等※

通信情報や秘密は含まず

周知等用総合整理分析情報

基幹インフラ事業者
電子計算機等の供給者
公表・周知 等

※外国政府等に対しても、必要に応じ提供可能

（参考）サイバー対処能力強化法等 － アクセス・無害化

- **サイバー攻撃による重大な危害を防止**するための**警察・自衛隊による措置**等を可能とし、その際の**適正性を確保するための手続を新設**

警察

- 措置の主体は、警察庁長官が指名した警察官に限定
- 措置を実施する場面は、
  - ① サイバー攻撃に用いられる電気通信等を認めた場合で
  - ② そのまま放置すれば重大な危害が発生するおそれがあるため緊急の必要があるとき
- 措置の内容は、
  - ① 攻撃関係サーバ等の管理者等への措置の命令
  - ② 攻撃関係サーバ等への措置※１を自ら実施

（※１）インストールされている攻撃のためのプログラムの停止・削除など

- 国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議
- 措置に際しての手続は、独立機関の承認、警察庁長官等の指揮

（承認を得るいとまがないと認める特段の事由がある場合：事後通知）

内閣官房※３の調整の下で緊密に連携

防衛省・自衛隊

（警察と共同対処）

- 内閣総理大臣が次の場合に通信防護措置を命じた上で、自衛隊の部隊等が措置を実施（新たな行動類型）
  - ① 一定の重要な電子計算機に対するサイバー攻撃であり
  - ② 外国政府を背景とする主体による高度な攻撃と認められるものが行われ
  - ③ 自衛隊が対処する特別の必要※２があるとき

（※２）自衛隊が有する特別な技術又は情報が必要不可欠であるなど

- 自衛隊及び日本に所在する米軍が使用する電子計算機をサイバー攻撃から職務上警護する自衛官が、緊急の必要があるときに無害化措置を実施
- 措置を実施する場面・措置の内容は、警察と同様
- 国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議
- 措置に際しての手続は、独立機関の承認、防衛大臣の指揮

（承認を得るいとまがないと認める特段の事由がある場合：事後通知）

申請 ⇩ ⇧ 承認　　申請 ⇩ ⇧ 承認

独 立 機 関

※３ アクセス・無害化については、その実施主体が警察及び自衛隊になるが、こうした措置は国家安全保障の観点から整合性のとれた形で行われる必要があり、内閣官房（新組織）が、国家安全保障局（NSS）とも連携しつつ、その司令塔機能を発揮

（参考）サイバー対処能力強化法等 － 組織・体制整備等

● 能動的サイバー防御を含む各種取組を実現・促進するため、司令塔たる**内閣官房新組織の設置**等、**政府を挙げた取組を推進するための体制を整備**（内閣官房（司令塔・総合調整）と内閣府（実施部門）が一体となって機能）

サイバーセキュリティ戦略本部の強化

□ サイバーセキュリティ戦略本部を
- 本部長：内閣総理大臣
- 本部員：全ての国務大臣

とする組織に改組

※ 有識者から構成される「サイバーセキュリティ推進専門家会議」を設置

□ サイバーセキュリティ戦略本部の所掌事務に
- 重要インフラ事業者等のサイバーセキュリティの確保に関する国の施策の基準の作成
- 国の行政機関等におけるサイバーセキュリティの確保の状況の評価

を追加

内閣サイバー官の設置

□ サイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官を内閣官房に新設

※１ 内閣サイバー官は、国家安全保障局次長を兼務

※２ 内閣サイバーセキュリティセンター（NISC）の改組は政令で実施

内閣府特命担当大臣の設置等

□ 官民連携や通信情報の利用に関する事務を内閣府の所掌事務に追加

□ これら事務を掌理する内閣府特命担当大臣の設置が可能

（参考）欧米主要国の取組

官民連携関係

■ 主要国は、2010年代後半から最近にかけ、**政府からの情報提供、重要インフラ事業者による報告の義務化を制度化**

- 国家ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年)
  重要ｲﾝﾌﾗｻｲﾊﾞｰｲﾝｼﾃﾞﾝﾄ報告法(2022年)
- 豪州ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年)
  重要ｲﾝﾌﾗ保安法(2018年)
- 国家ｻｲﾊﾞｰ戦略(2022年)
  ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ規則(2018年)
- ｻｲﾊﾞｰﾚｼﾞﾘｴﾝｽ法(2024年)
  ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ指令(2016年)

通信情報の利用関係

■ 主要国は、**以前より、国家安全保障等の目的のために外国関係の通信情報を利用**

■ 政府における通信情報の利用について **専門の独立機関が監督**

- 英国：調査権限法
  (2016年制定)
- 米国：外国情報監視法
  (2008年改正)
- ドイツ：連邦情報局法
  (2016年改正)
- 豪州：通信情報傍受及び
  アクセス法(2021年改正)

アクセス・無害化関係

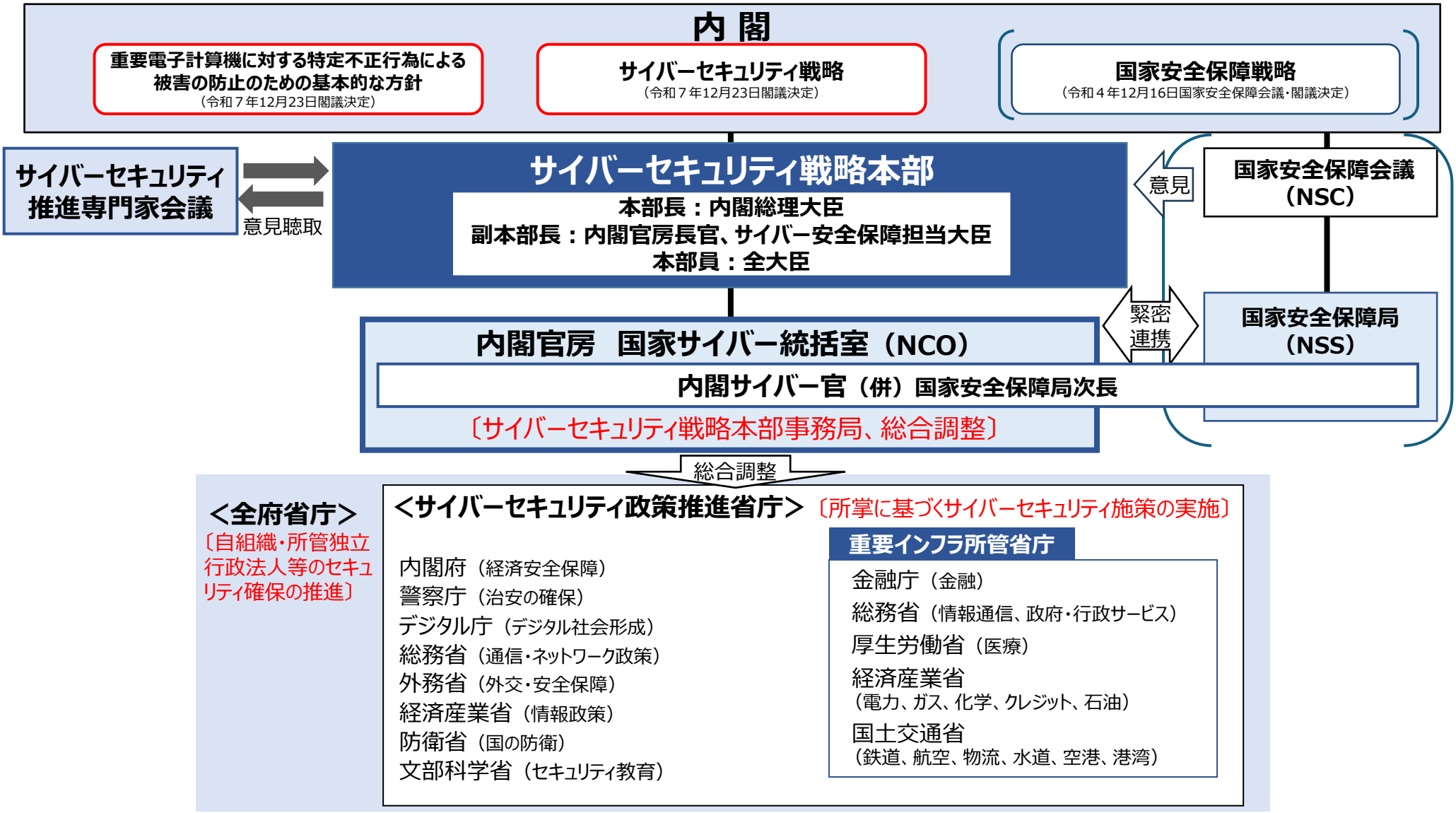
- 米国：Volt Typhoonによるボットネットワーク（感染ルータ群）に対する**無害化措置**（2024年）
- カナダ：政府ネットワークからの情報窃取防止目的で、攻撃者の海外サーバに対する**無害化措置**（2019年以降）
- 英国、豪州も同様の取組を推進。

＊ 各国の法制及び実態の全てを網羅するものではない。

出典：内閣官房資料

サイバーセキュリティ政策の推進体制

- 内閣総理大臣を本部長とするサイバーセキュリティ戦略本部の下、**全府省庁が連携してサイバーセキュリティ政策を推進**
- 総務省は通信・ネットワーク政策を所掌し、重要インフラ分野のうち情報通信分野及び地方行政分野を所管



新たな「サイバーセキュリティ戦略」（令和７年12月23日 閣議決定）

○ **「国家安全保障戦略」**及び**サイバー対処能力強化法等**に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に、**実施すべき諸施策の目標や実施方針を内外に示す。

基本的な考え方

○ サイバー空間は、経済社会の持続的な発展、自由主義、民主主義、文化発展を支える基盤。

○ 法の支配、基本的人権の尊重といった普遍的価値に基づく国際秩序が深刻な危機にさらされ、サイバー脅威による国民生活・経済活動、ひいては国家安全保障上の懸念が高まっている。

「５つの原則」※を、引き続き「基本原則」として堅持した上で、国がこれまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することを明確化

（※施策の立案・実施原則となる「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」）

情勢認識

厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大	社会全体のデジタル化の進展とサイバー脅威の増大	AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

施策の方向性

1 深刻化するサイバー脅威に対する防御・抑止

- 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来の施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

2 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- 様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施（政府機関等が範となり対策）
- デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要インフラ事業者・地方公共団体等の対策強化

サプライチェーン全体のレジリエンス確保（中小企業・ベンダー等）

全員参加によるサイバーセキュリティ向上

サイバー犯罪対策を通じた安全・安心の確保

3 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

- 産学官を通じたサイバー人材の確保・育成
- 国産を核とした、新技術・サービスの創出

効率的・効果的な人材の育成・確保

新たな技術・サービスのエコシステム形成

先端技術（AI、量子技術等）への対応・取組

官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指す。

出典：サイバーセキュリティ戦略

（参考）新たなサイバーセキュリティ戦略の構成［1/2］

Ⅰ. 策定の趣旨・背景

- サイバー空間を巡る脅威に対応するために行う様々な取組を一体的に推進するため、**今後５年の期間を念頭にとるべき諸施策の目標や実施方針を提示**

Ⅱ. 本戦略における基本的な考え方

1 確保すべきサイバー空間の在り方及び基本原則

自由、民主主義、基本的人権の尊重、法の支配といった普遍的価値に基づく国際秩序が深刻な危機にさらされている中で、**サイバー空間が「自由、公正かつ安全な空間」であること**や、**「５つの原則」（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）を施策の立案・実施の基本原則とすることの重要性を確認**

2 サイバー空間を取り巻く情勢認識及び今後の見通し

（１）厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大

- 地政学的緊張を反映し、サイバー空間の状況も緊迫。サイバー攻撃関連通信数は増加傾向にあり、外国国家の関与が疑われる組織化・洗練化されたサイバー攻撃が顕在化するなど、**質・量の両面でサイバー攻撃の脅威は増大し、国民生活や経済活動の基盤、国家及び国民の安全に深刻・致命的な被害を生じさせるおそれが現実化**

（２）社会全体のデジタル化の進展とサイバー脅威の増大

- 国民生活・経済活動のデジタルサービスへの依存が高まる中、経済的な目的を含め、**様々な動機に基づくサイバー攻撃が国民生活や企業活動、社会経済に与える影響が深刻化**。また、サイバー犯罪の巧妙化等の新たな脅威にも直面しており、**サイバー空間における脅威は質・量両面で増大**

（３）AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

- 生成AIをはじめとするAIの急速な発展は産業や国民生活の利便性や効率性を大きく向上させる潜在力を持つ一方、**AIに対する攻撃やAIを利用した攻撃が、新たなサイバーセキュリティ上のリスクとして深刻さを増すことが想定**
- 量子コンピュータや量子通信の実用化が現実的なものとなりつつある中、現在広く使われている**公開鍵暗号の安全性の低下・危殆化が懸念**

3 サイバー空間を取り巻く課題認識及び施策の方向性

（１）深刻化するサイバー脅威に対する防御・抑止

- 政府機関等が緊密に連携し、通信情報の利用を含む情報収集等を行うとともに、官民連携・国際連携の下、事案発生後の的確な対処を含め、**能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、我が国に対するサイバー脅威を能動的に防御・抑止**

（２）幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- **政府機関等が範となり**、強固な対策を実践していくとともに、重要インフラ事業者・地方公共団体はもちろんのこと、サイバーセキュリティ確保に大きな影響・役割を持つサイバー関連事業者や製品ベンダー、そして中小企業・個人等といった**様々な主体に求められる対策と実効性確保に向けた方策を明確化し、迅速に実施**

（３）我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

- 産官学を通じて、**サイバーセキュリティ人材の確保・育成・裾野拡大にこれまで以上に注力**。また、研究・開発から実装・運用まで、産官学の垣根を越えた協働による**国産技術・サービスを核とした新たな技術・サービスを生み出すエコシステムを形成**するとともに、**AIや量子技術等の新たな技術革新がもたらす変革に対応**

（参考）新たなサイバーセキュリティ戦略の構成［2/2］

Ⅲ．目的達成のための施策　※赤字は総務省の取組

1 深刻化するサイバー脅威に対する防御・抑止

（１） 国が要となる防御・抑止

① インシデント対処の高度化による被害の拡大・深刻化の防止

② 通信情報を含むサイバーセキュリティ関連情報の集約、効果的な分析と活用
サイバー空間の観測（NICTER等）を通じて得られた情報等、分析に有用なあらゆる情報をNCOに集約

③ アクセス・無害化措置をはじめとする多様な手段を組み合わせた能動的な防御・抑止

④ 体制・基盤・人材等の総合的な整備・運用
官民が連携（NICT等を含む）し、高度な情報収集・分析能力を担う体制・基盤・人材等を総合的に整備

（２）官民連携エコシステムの形成及び横断的な対策の強化

① 官民間の双方向・能動的な情報共有と対策強化のサイクルの確立

② 官民における脅威ハンティングの実施拡大

③ 演習の体系的な実施
実践的サイバー防御演習「CYDER」、分野別演習開発プラットフォーム「CYROP」、若手セキュリティ人材育成事業「SecHack365」、高度なサイバー攻撃への対処能力構築のための高度演習基盤構築等

（３）国際連携の推進・強化

① 同盟国・同志国等との情報・運用面での協力の強化

② インド太平洋地域におけるサイバー安全保障分野の対応能力向上の支援・推進
日ASEANサイバーセキュリティ能力構築センター（AJCCBC）等の活用

③ 国際的なルール形成の推進

2 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

（１）政府機関等におけるサイバーセキュリティ対策の強化

① 対策水準の向上と継続的な見直し

② 政府機関等の監視体制・インシデント対応力の更なる強化・高度化
政府横断的な不正な通信の監視等の取組を公的関係機関（NICT及びIPA）と連携し、強化・高度化
CYXROSSセンサーを順次、全府省庁を含む政府機関等の端末に導入して監視及び分析

③ 強靭な政府情報システムの構築と運用

④ 政府機関等におけるサイバーセキュリティ人材の育成・確保と体制の強化
現実に即した大規模な演習環境を新たに構築し、政府機関等の中核的な対処人材の育成を推進

（２）重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化

① 重要インフラ事業者等におけるサイバーセキュリティ対策の強化、地方公共団体におけるサイバーセキュリティ対策の強化
重要インフラ防護範囲の在り方の見直しを検討

② 大学・教育研究機関におけるサイバーセキュリティ対策の強化
人員体制構築に必要な実践的サイバー防御演習（CYDER）等の研修プログラムの活用推進

（３）ベンダー、中小企業等を含めたサプライチェーン全体のレジリエンスの確保

① セキュアバイデザイン原則等に基づくベンダー等における責任あるサイバーセキュリティ対策の取組みの推進

② サプライチェーンを通じたレジリエンスの確保
国際海底ケーブル等の安全性、信頼性及び冗長性の確保、防護、自律的な生産・敷設・保守の体制の確保

③ 中小企業を始めとした個々の民間企業等における対策の強化

（４）全員参加によるサイバーセキュリティの向上

NOTICE等によるIoTの設定不備や脆弱性に関する注意喚起や助言、情報提供等

（５）サイバー犯罪への対策

3 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

（１） 効率的・効果的な人材の育成・確保

① 人材フレームワークの整備と効果的な運用

② サイバーセキュリティ人材の育成に資する教育や演習・訓練の更なる充実
CYDER、CYROP等の実践的な演習や演習基盤の提供等、多様な学びの場を体系的に整備・拡充

（２）新たな技術・サービスを生み出すためのエコシステムの形成

研究開発・開発支援・実証の実施・拡充及びそれらを通じた技術情報（マルウェア情報、脆弱性情報等の一次データ）等の提供

（３）先端技術に対する対応・取組

① AIに係る安全性確保、AIを活用したサイバーセキュリティの強化
AIの開発・運用等に係るガイドラインの策定・改定や周知・浸透の推進
AIを活用したサイバー攻撃インフラの検知やサイバーセキュリティ関連情報の分析の精緻化・迅速化等の推進

② 量子技術の進展に伴う耐量子計算機暗号（PQC）への円滑な移行の推進
2035年までに政府機関等におけるPQCへの移行を目指し、2026年度に工程表（ロードマップ）を策定
2030年頃の量子暗号通信（QKD）の社会実装に向け、テストベッドの広域化・高度化、ユースケースやビジネスモデルの創出・実証等を推進

Ⅳ．本戦略の推進体制

- NCOは、重要インフラ、基幹インフラ所管省庁及びアクセス・無害化措置実施省庁との間で総合調整、関係省庁との間で相互協力を実施

重要インフラのサイバーセキュリティの確保

重要インフラ

国家サイバー統括室 National Cybersecurity Office

共通ルール
- ●分野共通ルールの設定
  - ・重要インフラ行動計画
  - ・安全基準等策定指針

体制強化支援
- ●障害対応体制・情報共有体制強化支援
  - ・情報共有体制（セプター：CEPTOAR）の活動支援（分野別/分野横断）
  - ・適時適切な情報提供

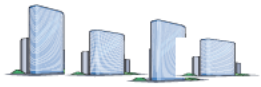
演習
- ●防護基盤の強化
  - ・分野横断的演習の実施

安全基準等の継続的改善の推進 ／ 情報共有体制の強化 ／ 分野横断的演習

重要インフラ所管省庁

連携

- ●分野別ルールの設定（業界団体と連携）
  - ・所管分野の特性に応じたルール策定



重要インフラ事業者等（全15分野）

- ●社内ルールの設定・体制の整備
  - ・各種業法等に基づく情報セキュリティポリシー策定
  - ・運用ルールの設定
  - ・体制の整備（内部監査、CSIRT等）

- 情報通信
- 政府・行政サービス
- 水道
- 医療
- 電力
- ガス
- 化学
- 石油
- クレジット
- 金融
- 航空
- 空港
- 鉄道
- 物流
- 港湾

組織内CSIRT等

- ●組織内における対処
  - ・情報システム等の監視
  - ・インシデント情報の集約・分析
  - ・対処方針決定・指示
  - ・責任者等への報告・連絡
  - ・要員等への教育・訓練

セプターカウンシル（総会、運営委、WG等）

セプター（情報通信分野）
A社 B社 C社 ・・・

セプター（電力分野）
セプター（金融分野）
セプター（医療分野）
・
・

* CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response

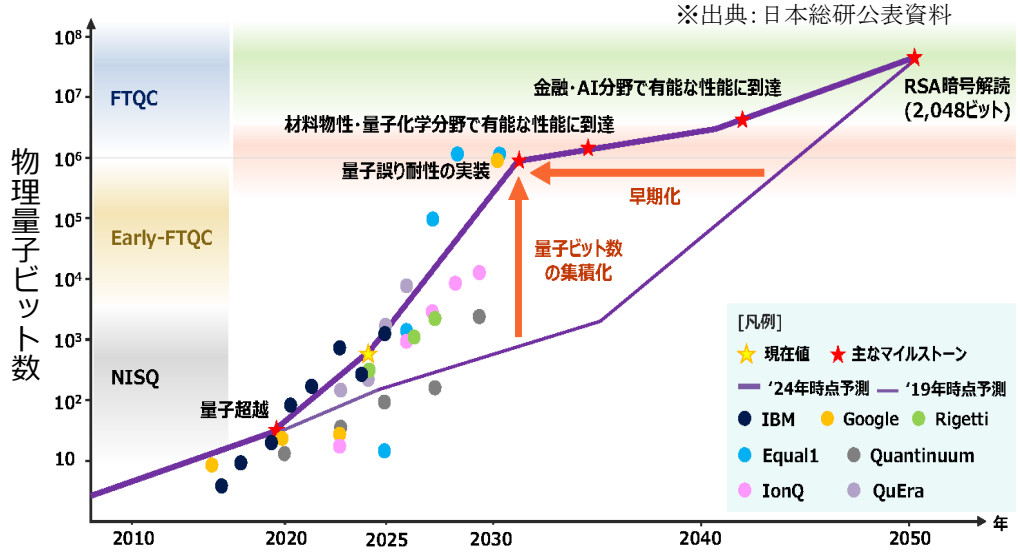
出典：内閣官房資料

量子計算機の実現による暗号の危殆化の懸念

- **量子計算機を利用して現代暗号を効率的に解読する方法が存在**（Shorアルゴリズム;1994年考案）
- 量子計算機の研究が加速しており、**将来的に実用的で大規模な量子コンピュータが実現**
  → 現在広く利用されている公開鍵暗号の安全性が低下（危殆化）するおそれ
  「公開鍵暗号方式」は、事前に暗号鍵を送受信先で設定する必要がないため、通信ネットワークで広く利用
  なお、事前に暗号鍵を共有する「共通鍵暗号方式」については、暗号鍵の長さを増やすことで量子計算機による影響を限定することが可能
- データを保存しておき、量子コンピュータでの暗号解読が可能となった後に解読を行うHNDL※攻撃も懸念
  ※Harvest Now, Decrypt Later
- 政府等の機微な情報を取り扱うシステム等において、**「耐量子計算機暗号(PQC)」への移行検討が重要な課題**

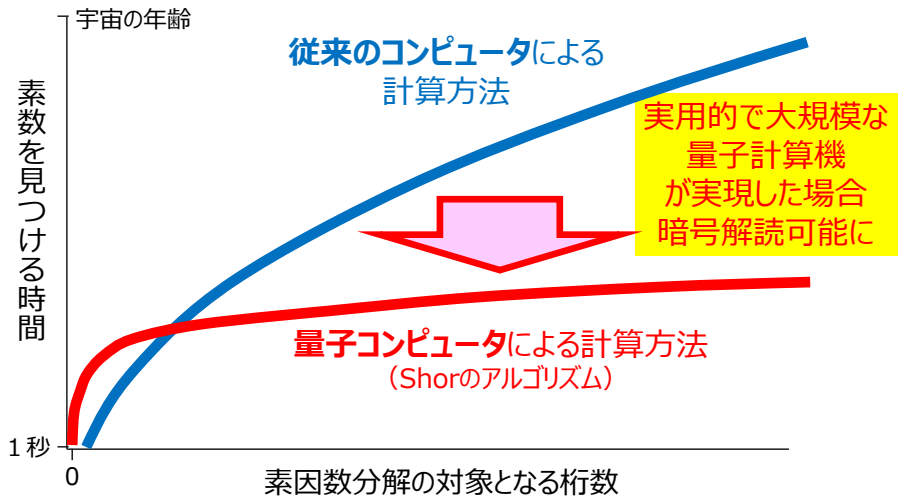
量子計算機の進展予想
例：民間事業者によるロードマップ

※出典：日本総研公表資料



実用的な量子計算機による影響
例：RSA暗号の安全性評価

※出典：Quantum Computing (Stolze and Suter)をもとに総務省作成



（参考）

- ✓ 現在の量子計算機は、15（=3×5）や 21（=3×7）の素因数分解が行える程度だが、**暗号解読には数百桁以上の数の素因数分解**が必要
- ✓ 暗号解読には10^9回規模の演算を要するため、量子計算機の規模(量子ビット数の増加)だけでなく、まだ実用化されていない**誤り訂正技術**も必要

政府機関等における耐量子計算機暗号（PQC）移行

政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）（令和７年11月）

政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議

工程表(ロードマップ)の骨子（概要）

移行対象	• **「政府機関等のサイバーセキュリティ対策のための統一基準」の適用対象**となる情報システム
移行期限	• 原則として、**2035年を目処**に移行。ただし、**情報の重要性や暗号技術の利用状況等を把握**した上で、どのように移行を進めるかを検討し、適切に判断 • **例えば、特に機微な情報や保護期間が非常に長期となることが想定される情報等を扱う場合等**においては、**より早期に移行**を行うことも含め、情報システムごとに適切に検討を行う
移行に向けた取組	• 今後策定する工程表（ロードマップ）において、政府機関等が移行に向けた計画を策定できるよう、**移行に向けた計画に盛り込むべき基本的事項や留意すべき事項**を示す • **政府機関等は、今後策定する工程表（ロードマップ）を踏まえ、移行に向けた計画を策定し、移行期限までにPQCへ移行**を行う

中間とりまとめを踏まえつつ、骨子を基に、**2026年度中に工程表（ロードマップ）を策定する予定**

出典：内閣官房資料

CRYPTRECにおけるPQCの検討

- CRYPTREC（※）では、PQCに関し、2019年度に**タスクフォースを設置して量子計算機時代に向けた暗号の在り方について検討を開始**し、主にPQCの技術的な内容をまとめて、「CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）」を公表（2022年度公表、2024年度改定）
  ※ **CRYPT**ography **R**esearch and **E**valuation **C**ommittees。デジタル庁・総務省・経済産業省・NICT・IPAが共同で開催する暗号技術評価等を実施するプロジェクト
- 2025年３月には、PQCに関する米国等の動向や国内における議論の高まりに応じて、**CRYPTREC暗号リストへの掲載に向け、PQCの安全性評価及び実装性能評価に関する活動を開始**

CRYPTREC

暗号技術検討会（事務局：デジタル庁、総務省、経済産業省）

- CRYPTREC暗号の安全性及び信頼性確保のための調査・検討
- CRYPTREC暗号リストの改定に関する調査・検討
- 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討

暗号技術評価委員会（事務局：NICT、IPA）

- 暗号技術の安全性及び実装に係る監視及び評価
- 新技術等に係る調査及び評価
- 暗号技術の安全な利用方法に関する調査

暗号技術活用委員会（事務局：IPA、NICT）

- 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
- 暗号技術の利用状況に係る調査及び必要な対策の検討
- 暗号政策の中長期的視点からの取組の検討

CRYPTREC暗号リスト

電子政府推奨暗号リスト

安全性及び実装性能が確認された暗号技術で、市場における利用実績が十分であるか今後の普及が見込まれ、利用を推奨するもののリスト

推奨候補暗号リスト

安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト

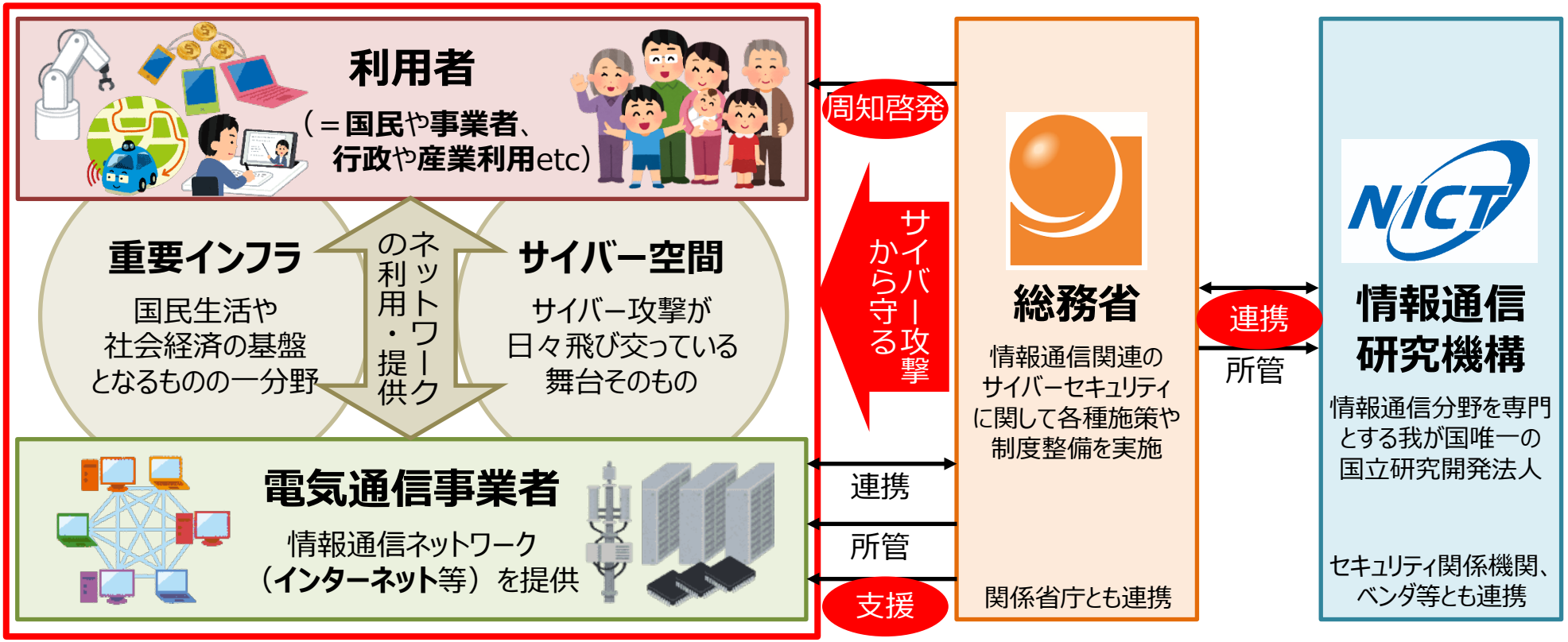
運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったと確認されたが、互換性維持のために継続利用を容認する暗号技術のリスト

目　次

サイバーセキュリティにおける総務省の役割

- 総務省が所管する**電気通信事業／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）
- 国立研究開発法人**情報通信研究機構（NICT）**は、サイバー攻撃に関する**観測・分析**を長年実施し、**高度な技術・人材**を保有
- 総務省は、NICT、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て対抗できる基盤を構築）



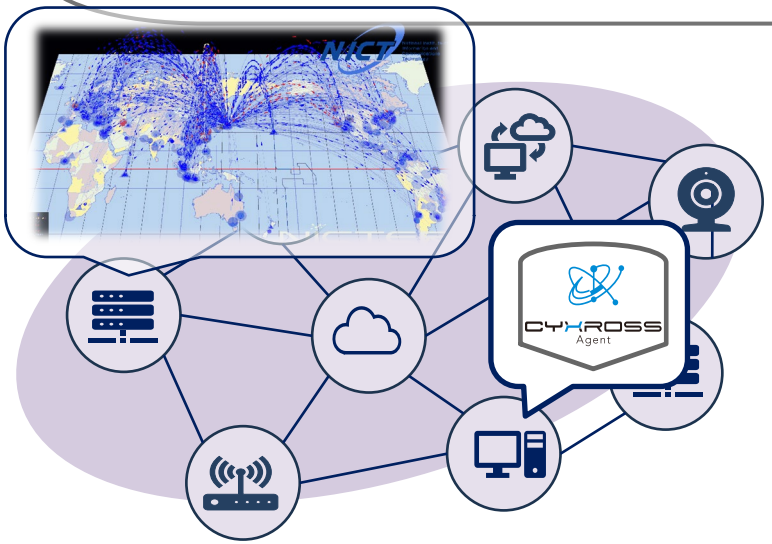
サイバーセキュリティ技術のエコシステムの形成

取組 **NICTの知見やデータの提供による国産技術の研究開発を支援**

- サイバーセキュリティに関して豊富な知見を有する**NICTの下、サイバー攻撃の観測・分析等に関する研究開発・基盤構築を推進**するとともに、**NICTの知見やNICTが収集するデータを民間に広く開放して国産技術の研究開発を支援**

【主なプロジェクト】

インターネット	NICTER ニクター	国内外の未使用IPアドレスから構成される「ダークネット」への通信を観測することで、通常は通信が行われない宛先に届く**不審な通信を検知**し、悪意のあるプログラムに感染した機器によるスキャン活動等、サイバー攻撃に関連する通信として把握することにより、**サイバー攻撃の全体的な傾向や動向を大局的に観測**
LAN	STARDUST スターダスト	**政府、企業等の組織を精巧に模擬したネットワーク（おとりのネットワーク）に攻撃を誘い込み**、攻撃者の組織侵入後の挙動を観測することで、**巧妙化・高度化するサイバー攻撃を詳細に観測**
端末	CYXROSS サイクロス	NICTが開発した**国産検知ソフトウェア（CYXROSSセンサー）を政府機関の端末に導入**し、我が国独自の**一次情報**の収集・分析体制を整備することで、**政府機関等に対するサイバー攻撃の監視を強化**



我が国独自のセンサーによる
サイバー脅威情報の収集・分析

NICT National Institute of Information and Communications Technology

研究開発・基盤構築を
一体的に実施

NICTを核とした
エコシステムの形成

国産セキュリティ技術の
創出の支援

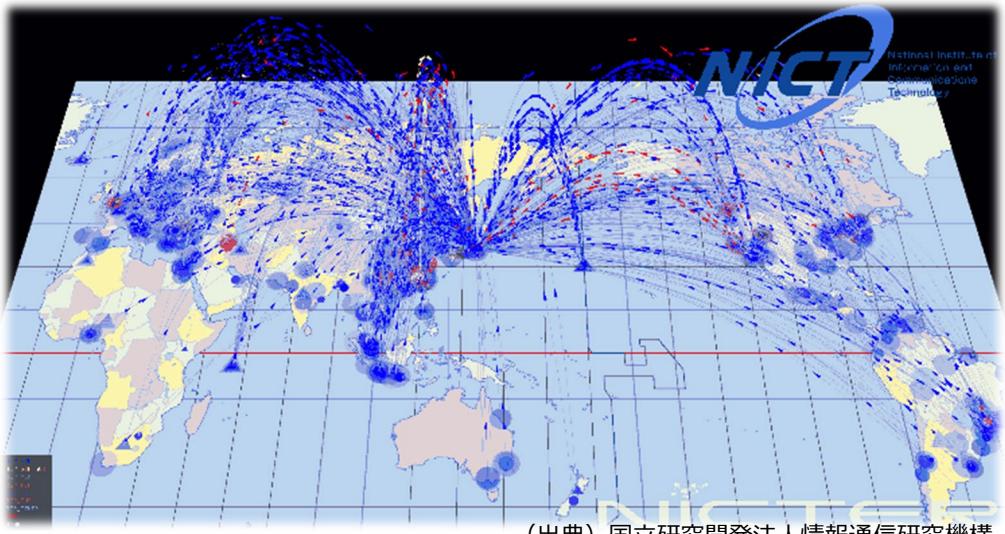
被害の未然防止のための
サイバー脅威情報の生成・共有

サイバー攻撃の大局的観測

サイバー攻撃関連通信の観測［NICTER（ニクター）］

- 国内外の未使用IPアドレスから構成される「ダークネット」への通信を観測することで、通常は通信が行われない宛先に届く**不審な通信を検知**し、悪意のあるプログラムに感染した機器によるスキャン活動等、サイバー攻撃に関連する通信として把握することにより、**サイバー攻撃の全体的な傾向や動向を大局的に観測**

NICTERによるサイバー攻撃関連通信の観測



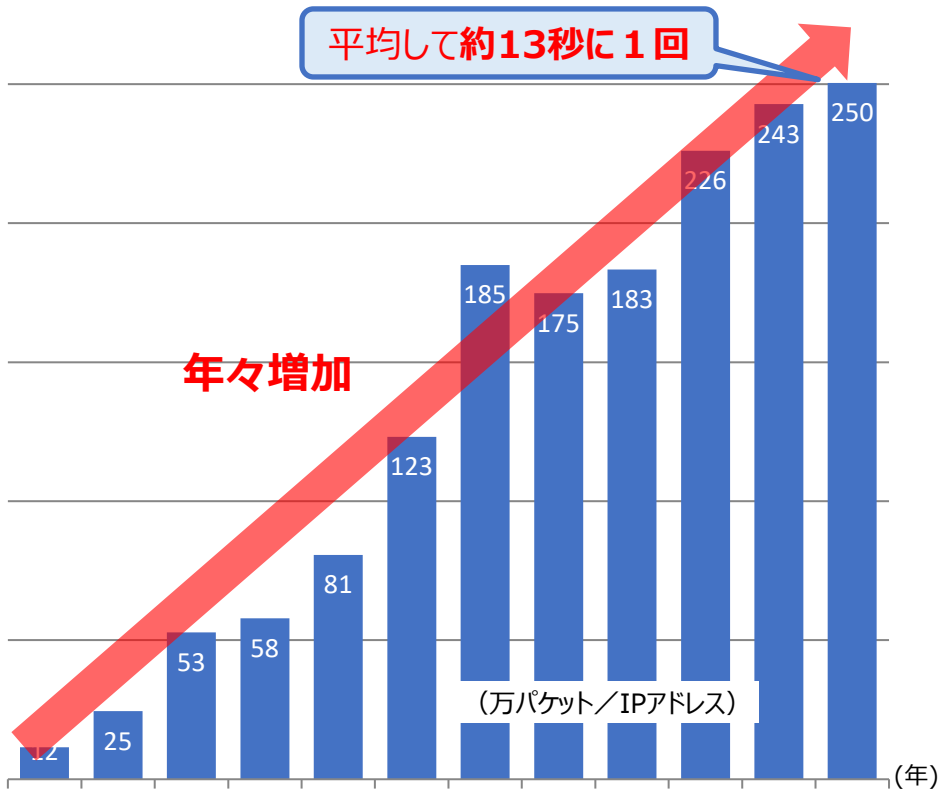
（出典）国立研究開発法人情報通信研究機構

観測結果は様々な取組に活用

① 悪意あるプログラムに感染したネットワーク機器の発見

② 自治体が管理するネットワーク機器が悪意あるプログラムに感染していることを検知した場合は、地方公共団体情報システム機構（J-LIS）の協力の下、当該自治体に警告を発出（2025年5月時点で775の自治体等が導入）

NICTが観測したサイバー攻撃関連通信数の推移（1つのIPアドレスで１年間に観測されるパケット数）

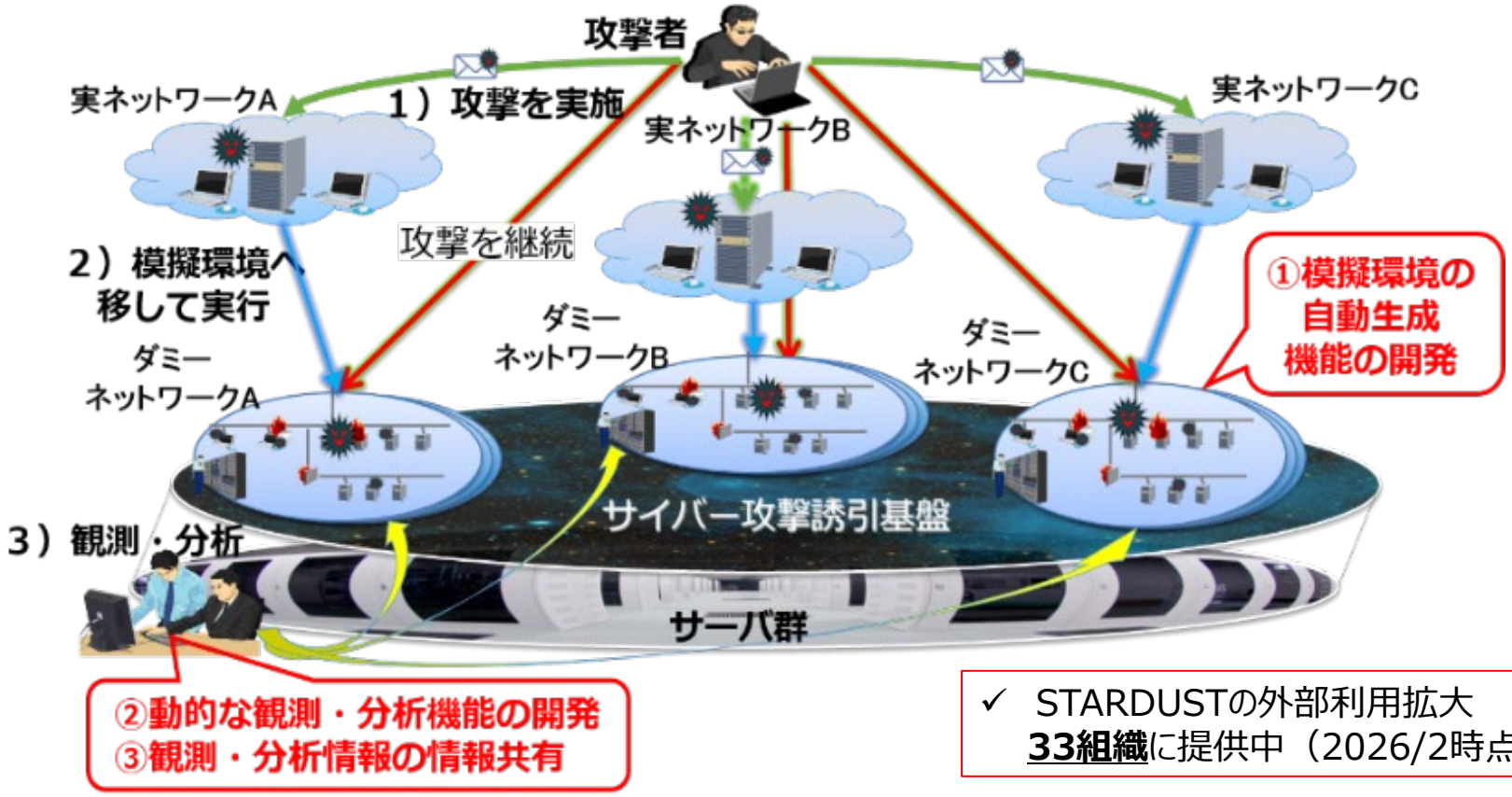


（出典）国立研究開発法人情報通信研究機構「NICTER観測レポート2025」等を基に作成

サイバー攻撃誘引基盤による攻撃手法の分析

サイバー攻撃誘引基盤［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**を構築
- 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でのプログラム観測やRAT解析による対策技術のノウハウを蓄積**



✓ STARDUSTの外部利用拡大
33組織に提供中（2026/2時点）

（出典）国立研究開発法人情報通信研究機構

我が国独自センサーによる政策機関等における対策の強化

政府端末情報を活用した情報収集・分析［CYXROSS（サイクロス）］

- NICTが開発した**国産検知ソフトウェア（CYXROSSセンサー）を政府機関の端末に導入**し、我が国独自の**一次情報**の収集・分析体制を整備することで、**政府機関等に対するサイバー攻撃の監視を強化**（政府機関等の一部に導入済み）
- サイバー攻撃に関する情報（サイバー脅威情報）を**我が国独自に収集し、分析・検知することで、サイバーセキュリティ対策を強化**

CYXROSS Agent

サイバーセキュリティ対策の強化

①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

・悪意あるプログラム本体のファイル
・不審な端末挙動に関する端末ログ
等

②収集した情報をNICTに集約

⑤分析結果を提供

NICT
情報通信研究機構

④監視・分析

④分析・検知能力の強化

サイバー脅威情報を用いた分析・検知能力の強化

③NICTの技術と蓄積データの活用

NICTER
サイバー攻撃観測技術

STARDUST
標的型攻撃観測・分析技術

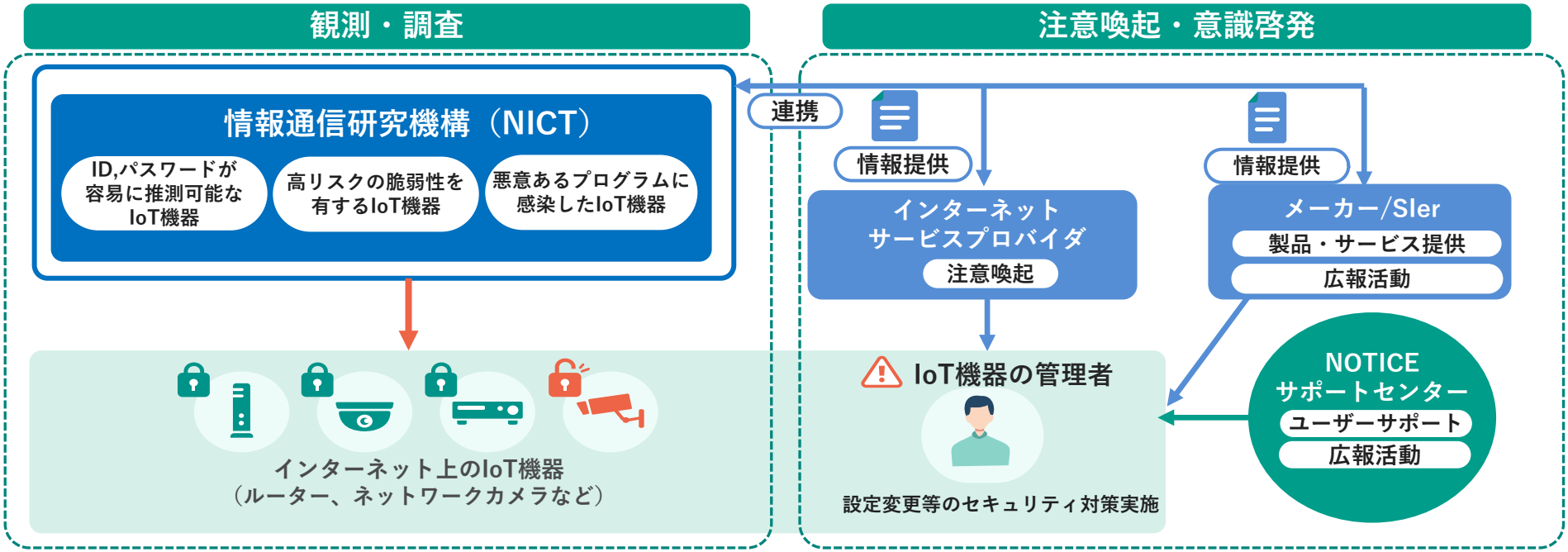
NIRVANA改
サイバー攻撃情報統合分析技術

脆弱性のあるIoT機器の管理者への注意喚起

悪意あるプログラムに感染したネットワーク機器等の発見、管理者への注意喚起［NOTICE（ノーティス）］

- NICTがインターネットを観測・調査し、**悪意あるプログラムに感染したネットワーク機器や、今後感染する危険性が高い脆弱なネットワーク機器を発見**
- 電気通信事業者を通じ、当該機器の**管理者に注意喚起**して対応を促すことで、被害の発生を防止

みんなで守る、IoT。 NOTiCE



2026年1月の結果

IoT機器観測総数	容易に推測可能なID,パスワードであるIoT機器	高リスク脆弱性を有するIoT機器	悪意あるプログラムに感染したIoT機器検知数
月 1.18 億件	月 13,116 件	月 2,415 件	最大 249 件/日

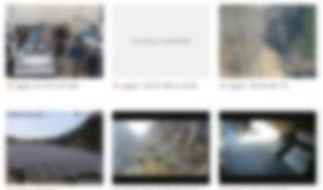
（出典）国立研究開発法人情報通信研究機構

IoT機器についてお願いしたいこと

- 政府でもNOTICEプロジェクトなどの対策を進めているが、IoT機器に関するセキュリティ事案は依然存在。
- **IoT機器**に関する事案の多くは、**初歩的なセキュリティ対策の不足に起因**するもの。
- IoT機器の**利用状況を把握**し、その**管理責任を明確**にした上で、**設定の確認等の対策**をお願いしたい。

例１）ネットワークカメラ

✓**管理者が意図しない形で映像が公開**
（公開情報をまとめたサイトも存在）
→情報漏洩、プライバシー侵害のリスク



（出典）総務省広報誌

✓**悪意のあるプログラムに感染**
→サイバー攻撃を中継する「踏み台」として利用

対策

✓**パスワード認証**の設定、
設定している場合は**十分に長いパスワード**か

✓**ファームウェアのバージョン**が最新であるか、
機器の**製品サポート**は継続しているか

✓**使用しない機能や設定**が有効になっていないか

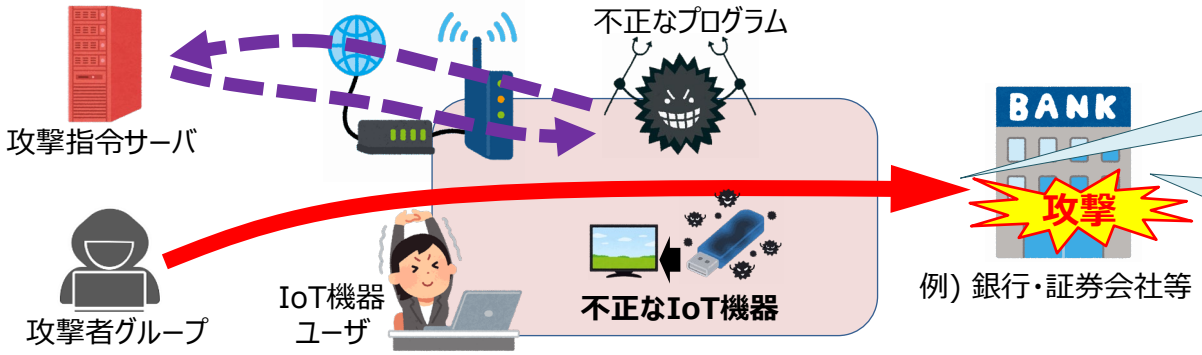
例２）不正なストリーミングデバイス

✓無料で国内外のTV番組が視聴できると謳う「ストリーミングデバイス」等の形で存在し、**購入時点で不正なプログラムが混入しているもの**がある
→ 利用者が気付かず、サイバー攻撃に悪用

対策

✓**機器の製造元を確認**

✓**不審なサービスの利用を控える**

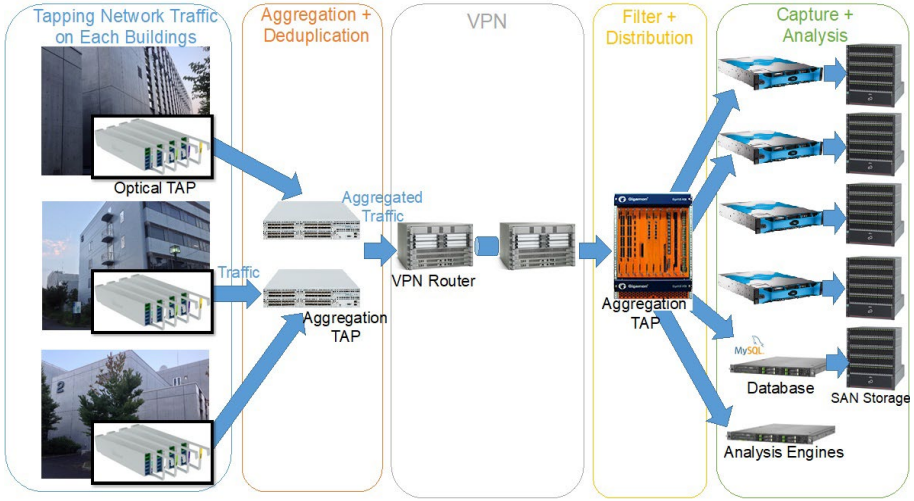


家庭内に設置している機器を経由することで、
サイバー攻撃を一般家庭に偽装
→サイバー攻撃として**検知・防御が困難**

サイバー攻撃や犯罪インフラとしての**悪用が懸念**
（国内に**数千～数万台が存在すると推定**）
→実際にネットバンキングによる不正送金や
オンライン証券取引等での**悪用報告**あり

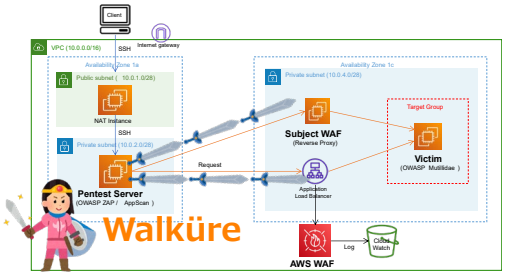
サイバーセキュリティに関する産学官連携

- NICTの有するサイバーセキュリティ関連情報や様々な知見を、約100の参画組織に開放し産官学連携を促進
- テスト環境提供等により、サイバーセキュリティ製品・サービスの開発を支援



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）

実機検証環境



レッドチーム体制

（出典）国立研究開発法人情報通信研究機構

✓ 実用化に至った例

kr:ns

都内のスタートアップ・レインフォレストが同スタートアップのクルウィットと共同開発したIPレピテーションサービス（脅威インテリジェンスサービスの一種）。同社のサイバー攻撃観測により得られた独自の情報を用いてIPアドレスを評価するThreat Intelligenceサービス。

✓ 性能強化に役立った例

Driverware NonCopy 2

機密情報保護を目的として、特定のフォルダ内のファイルを自動的に暗号化し、外部デバイスへの持ち出しや印刷、スクリーンショット取得などを制限することで、情報漏えいを防止するソフトウェア。企業や官公庁などでの実績あり。

サイバーセキュリティ人材の育成

- サイバー攻撃が巧妙化・高度化し、**サイバーセキュリティ人材の需要は増大しているものの、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、実機の操作を伴う演習を模擬環境を用いて行う必要
- NICTでは、サイバー攻撃観測技術等のサイバーセキュリティに関する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、これらを用いて**官民の人材育成を支援**

CYDER Cyber Defense Exercise with Recurrence（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年度の開始以降、2024年度までに、延べ**25,000名超**が受講

SecHack365（セックハック サンロクゴ）

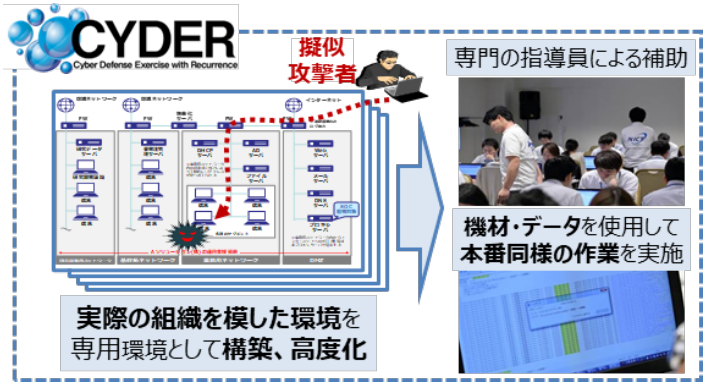
25歳以下の若手人材を対象とした「セキュリティイノベーター育成プログラム」

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年度の開始以降、2024年度までに、**計300名超が修了**

途上国への能力構築支援

演習プログラムの提供を通じた途上国への能力構築支援

演習プログラムの提供を通じて**サイバーセキュリティ能力構築支援**を実施
ASEANや大洋州島しょ国・地域のサイバーセキュリティ能力を底上げ



実践的サイバー防御演習
CYDER

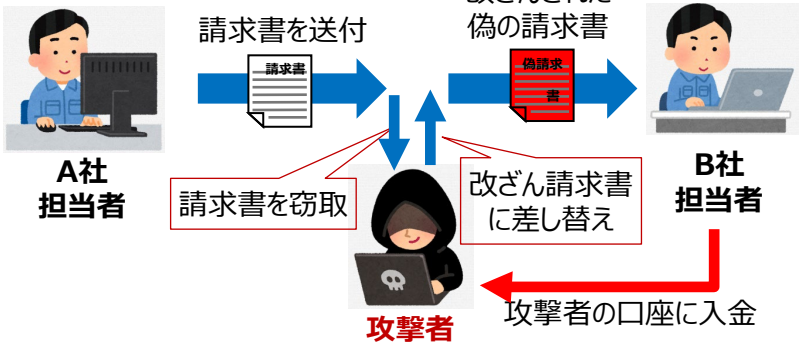
セキュリティイノベーター育成プログラム
SecHack365

途上国への能力構築支援

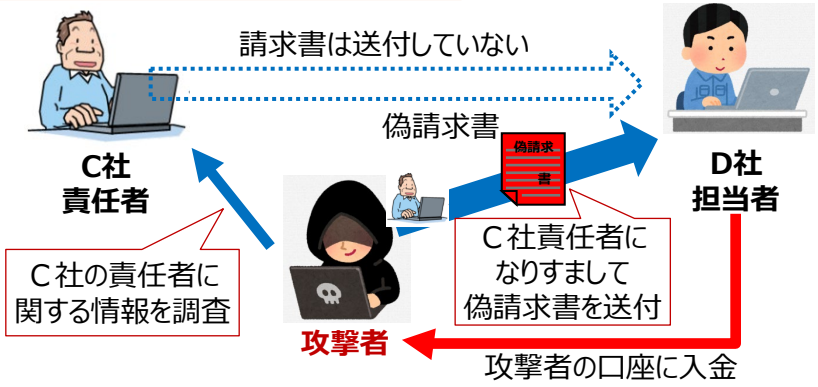
トラストサービスの推進（データの信頼性の確保）

- 個人・企業を問わず電子データのやりとりが急増し、**データ改ざんや送信元なりすましによる被害も発生**
- こうした不正行為に対抗し、流通する電子データの信頼性を確保するためにも、**「電子署名」、「タイムスタンプ」、「ｅシール」等の「トラストサービス」の制度を構築し、その普及を推進**
- 「ｅシール」については、令和７年３月に制度整備を行い、令和８年３月に制度運用を開始予定

例１）データ改ざん



例２）送信元なりすまし



① 電子署名

- ✓ **署名者の意思を確認できる仕組み**
- ✓ **電子署名法**に基づく認定制度あり
  ※2021年9月のデジタル庁設置に伴い、総務省からデジタル庁に業務移管

- 電子契約
- 電子申請・申告　等

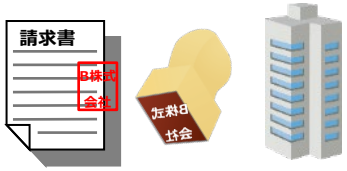
② タイムスタンプ

- ✓ **データの存在証明の仕組み**
- ✓ **総務大臣告示**に基づく認定制度あり
  ※2005年に民間の認定制度が開始、2021年4月に総務大臣認定制度を創設

- 税関係書類のスキャナ保存
- 官報情報　等

③ ｅシール

- ✓ **文書の発行元を確認できる仕組み**
- ✓ **総務大臣告示**に基づく認定制度あり
  ※2019年から総務省で制度検討を開始、2025年3月に総務大臣認定制度を創設



- 作業報告書、請求書
- 組織等の公表資料　等

サイバーセキュリティに関するガイドラインの策定

- 総務省では、インターネットを安心して利用できるよう、**無線LAN（Wi-Fi）、クラウドサービス、テレワーク等に関するセキュリティ対策のガイドラインを策定し、公表**

無線LANのセキュリティ対策に関するガイドライン

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 又は 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

「AIのセキュリティ確保のための技術的対策に係るガイドライン」の策定

背景・目的等

- 生成AIの社会実装が急速に進む中、**AIのセキュリティ確保が重要な課題**となっており、「デジタル社会の実現に向けた重点計画」では、**総務省が令和７年度末までにAIとセキュリティのガイドラインを策定・公表**するとされている。
- これを受け、総務省では、サイバーセキュリティタスクフォースの下に**「AIセキュリティ分科会」を開催**し、**生成AIを不正操作することによって機密情報を漏えいさせたり、AIシステムを停止させるといったAI固有の脅威に対応し、AIのセキュリティを確保するための技術的対策を検討**（令和７年９月～12月）。
- 分科会の取りまとめ(令和７年12月)を踏まえて、総務省は、AIの開発者や、AIを組み込んだシステムを提供する者を対象に、**「AIのセキュリティ確保のための技術的対策に係るガイドライン」を策定予定**（本年度内を予定）。

AIに対する主な攻撃とその対策（概観）

主な対策 / 主な攻撃	AI開発者における対策	AI提供者における対策				
	安全基準等の学習による不正な指示への耐性の向上	システムプロンプトによる不正な指示への耐性の向上	ガードレール等による入出力や外部参照データの検証			オーケストレータやRAG等の権限管理
			入力プロンプトの検証	外部参照データの検証	出力の検証	
直接プロンプトインジェクション攻撃	○	○	○		○	○
間接プロンプトインジェクション攻撃	○	○	○	○	○	○
DoS攻撃（サービス拒否攻撃）	○	○	○			

（参考）「AIのセキュリティ確保のための技術的対策に係るガイドライン」(案)の概要

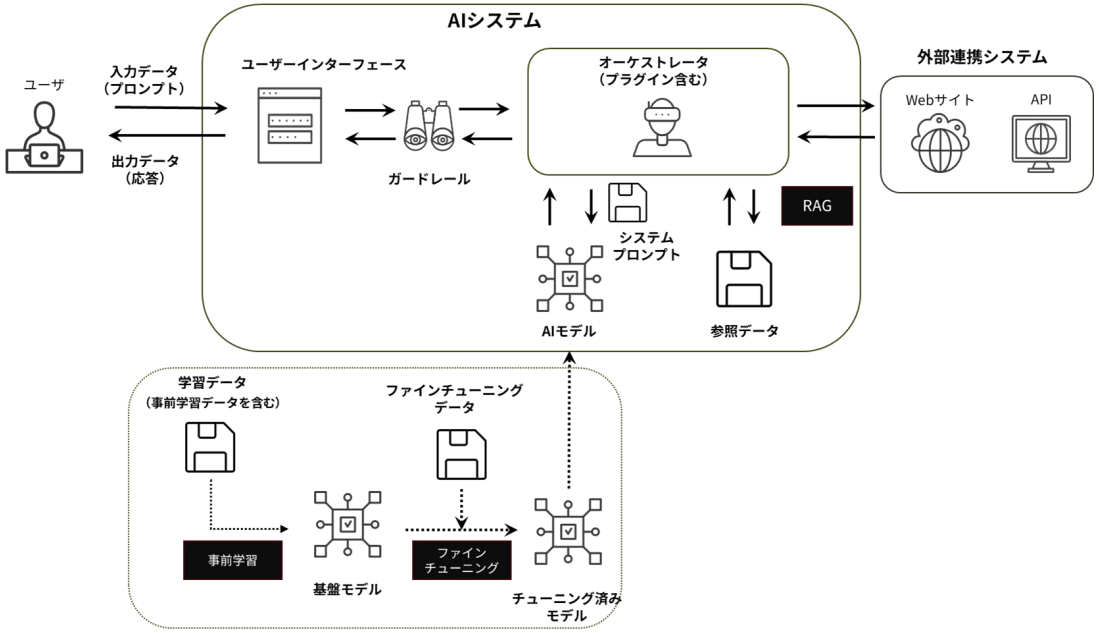
令和７年度内に策定・公表予定

ガイドライン（案）の想定読者

- **AI開発者**
  AIシステムを開発する事業者：AIモデル・アルゴリズムの開発、データ収集（購入を含む。）、前処理、AIモデル学習及び検証を通してAIモデル、AIモデルのシステム基盤、入出力機能等を含むAIシステムを構築する役割を担う。
- **AI提供者**
  AIシステムをアプリケーション、製品、既存のシステム、ビジネスプロセス等に組み込んだサービスとしてのAI利用者（AI Business User）：AIシステム検証、AIシステムの他システムとの連携の実装、AIシステム・サービスの提供、正常稼働のためのAIシステムにおけるAI利用者（AI Business User）側の運用サポート又はAIサービスの運用自体を担う。

ガイドライン（案）で取り扱うAI

ガイドライン（案）では、社会実装が進み、脅威が顕在化し始めている大規模言語モデル（LLM）及びLLMを搭載したシステムを主な対象とした。

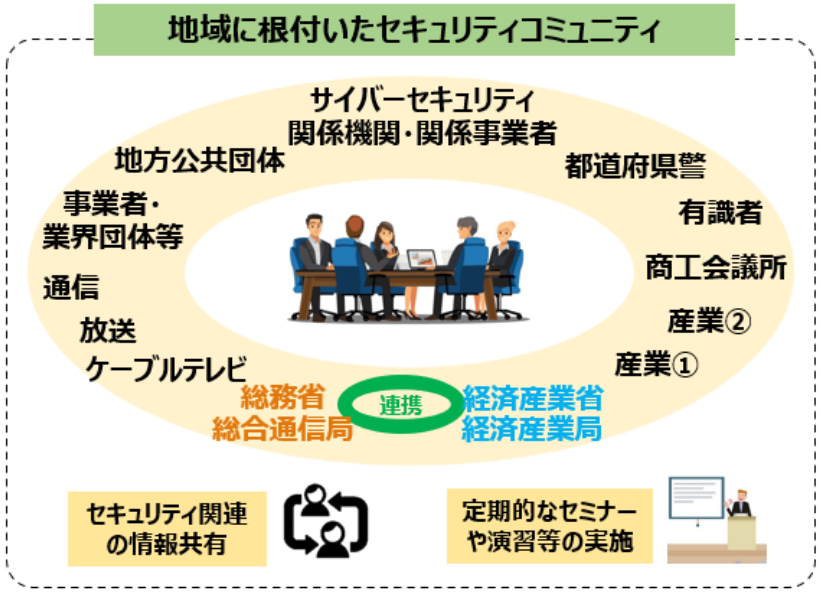


代表的なシステム構成の例

ガイドライン（案）の構成

各地域におけるサイバーセキュリティ啓発活動

- 総務省では、経済産業省と連携し、地域単位のサイバー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**
- 2025年度は、全国各地の総合通信局等の管区において**サイバーセキュリティに関するセミナー等を開催**（セミナーは令和８年１月末時点で計1,435名が参加）



サイバーセキュリティに関するセミナー

- 全国各地の総合通信局等の管区においてサイバーセキュリティに関するセミナーを開催
- ランサムウェア等の最新のサイバー攻撃に関する講演や、学生を含む若年層に向けてのサイバーセキュリティ対策の体験講座等を実施

出典：近畿総合通信局ウェブサイト

【各地域の連絡会】

名称	事務局
北海道地域情報セキュリティ連絡会	北海道総合通信局、北海道経済産業局、北海道警察本部
東北地域サイバーセキュリティ連絡会	東北総合通信局、東北経済産業局
関東サイバーセキュリティ連絡会	関東総合通信局、関東経済産業局
信越サイバーセキュリティ連絡会	信越総合通信局、関東経済産業局
北陸サイバーセキュリティ連絡会	北陸総合通信局
東海サイバーセキュリティ連絡会	東海総合通信局、中部経済産業局

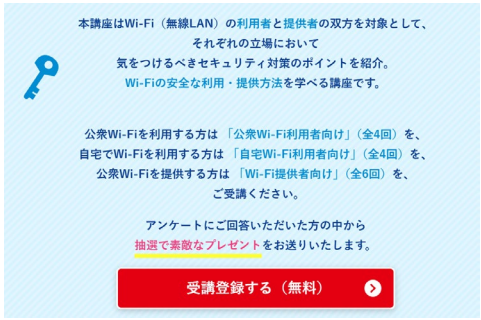
名称	事務局
関西サイバーセキュリティ・ネットワーク	近畿総合通信局、近畿経済産業局、（一財）関西情報センター
中国地域サイバーセキュリティ連絡会	中国総合通信局、中国経済産業局
四国サイバーセキュリティネットワーク	四国総合通信局、四国経済産業局
九州・沖縄地域情報セキュリティ推進連絡会議	九州総合通信局、九州経済産業局
沖縄サイバーセキュリティネットワーク	内閣府沖縄総合事務局、沖縄総合通信事務所、沖縄県警察本部

サイバーセキュリティに関する全国向けの周知・広報活動

政府広報オンライン

出典：政府広報オンライン

無料オンライン講座　今すぐ学ぼう Wi-Fiセキュリティ対策



総務省X

総務省YouTubeチャンネル

公衆Wi-Fi提供者向け第１回　【事例紹介アニメ】その公衆Wi-Fi､悪用されていませんか？【今すぐ学ぼう ...

YouTube · 総務省動画チャンネル

視聴回数: 300 回 · 7 か月前

総務省
Ministry of Internal Affairs and Communications

御清聴ありがとうございました