資料３

※サイバーセキュリティ戦略本部 第１回会合
（令和7年7月1日）資料１に基づき作成

新たなサイバーセキュリティ戦略の方向性

令和7年９月19日

内閣官房 国家サイバー統括室

サイバー攻撃の巧妙化・高度化及び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

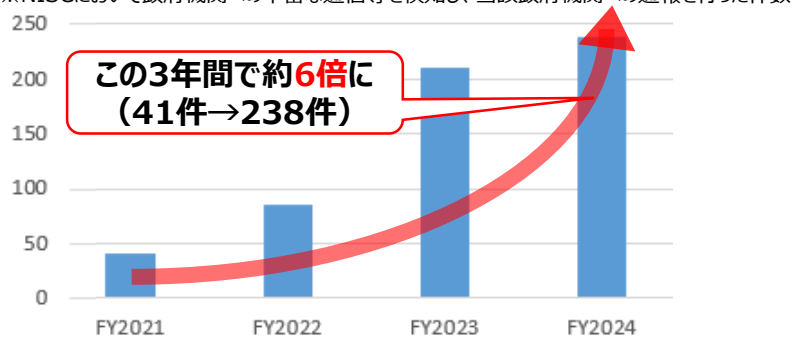
- 2019年以降、中国の関与が疑われるグループ「MirrorFace」が、日本の安全保障や先端技術に係る情報窃取を狙う攻撃キャンペーンを実行。
- 2024年5月、北朝鮮を背景とする攻撃グループ「TraderTraitor」が、暗号資産関連事業者から約482億円相当の暗号資産を窃取。

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。

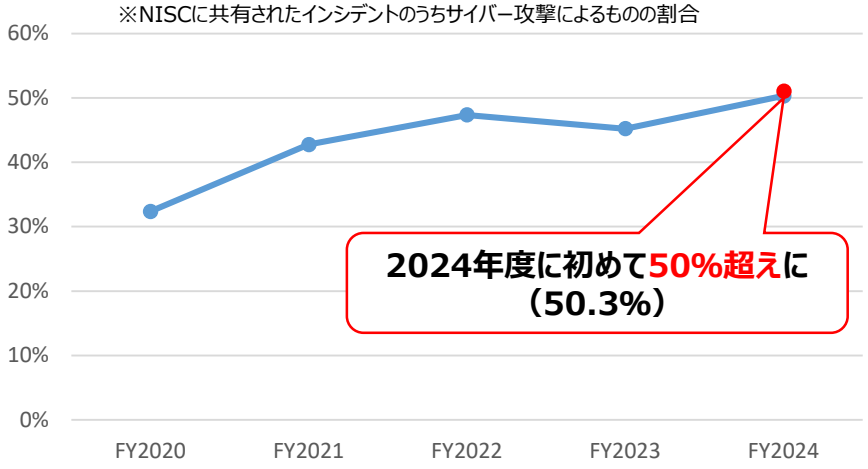
政府機関へのサイバー攻撃疑いの件数※

※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



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。

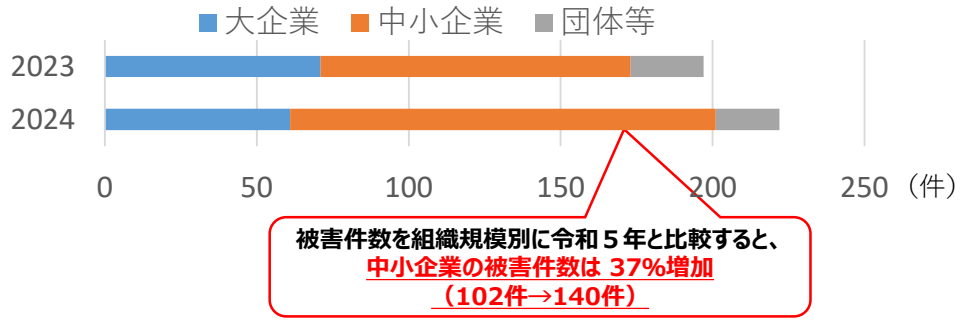
委託先・サプライチェーンへの攻撃と業務停止

- 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）

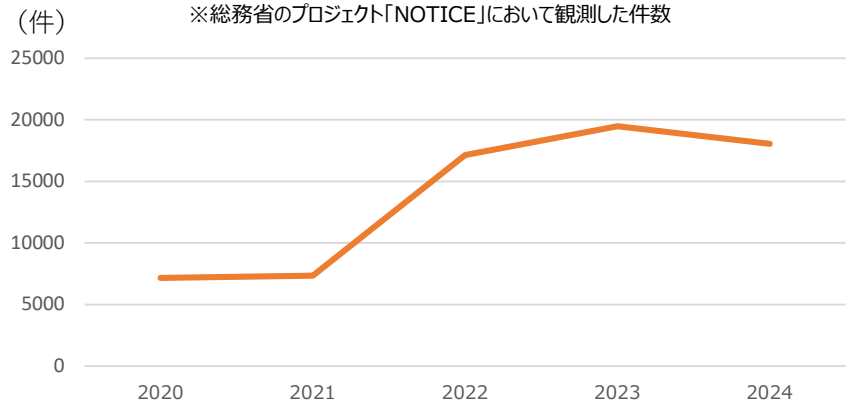
企業・団体等におけるランサムウェア被害の報告件数



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

諸外国のサイバーセキュリティ戦略

■ 欧米諸国では、**脅威の防止・抑止、社会全体のサイバーセキュリティ向上、人的・技術的基盤の確保等**を国家戦略において明記しているところ、国際的な協調を図る必要。

英国 National Cyber Strategy 2022	米国 National Cybersecurity Strategy 2023	豪州 2023-2030 Australian Cyber Security Strategy
＜第１部　戦略＞ ○**戦略の背景**（＝サイバー空間動向等） ○**国家の対応**（＝ビジョン（「2030年までサイバー大国の地位を保持し、国益を保護・増進」）、目標、原則等） **＜第２部　実施＞**(2025年までの実施措置) ○**第１の柱：英国のサイバーエコシステムの強化**（＝Whole-of-Societyアプローチ、人材育成、国際競争力向上） ○**第２の柱：レジリエントで豊かなデジタル国家の構築**（＝リスクへの理解増進、リスク管理、レジリエンス強化） ○**第３の柱：サイバーパワーの確保に不可欠な技術の先導**（＝技術的優位の保持、技術標準化の推進等） ○**第４の柱：より安全で豊かでオープンな国際秩序の実現のためのグローバルなリーダーシップと影響力の発揮**（＝同志国との集団的活動の強化、グローバルなガバナンスの形成等） ○**第５の柱：安全保障の強化のための敵対者の検知・破壊・抑止**（＝脅威の検知・調査、情報共有、脅威の抑止・破壊、脅威に対抗するアクション） ○**目標の実現のために**（＝政府全体の役割と責任、投資、成果の測定等）	○**イントロダクション** ・**戦略をめぐる環境**（＝サイバー空間を巡る動向、悪意あるアクターの活動） ・**アプローチ**（＝責任のリバランス、長期的投資を指向するインセンティブ付け） ・**既存の政策を踏まえた取組** ○**第１の柱：重要インフラ防御**（＝基準強化、官民連携、事案対処プロセスの見直し、連邦機関の防御の現代化等） ○**第２の柱：脅威アクターの破壊**（＝官民連携による対処強化、情報共有と通知(注意喚起)の迅速化、サイバー犯罪への対処等） ○**第３の柱：市場の力の活用**（＝セキュアなIoT、安全でないソフトウェアの責任のシフト等） ○**第４の柱：レジリエントな未来への投資**（＝インターネット技術基盤の確保、人材強化戦略策定等） ○**第５の柱：国際連携の強化**（＝脅威に対抗するための連携、能力構築支等） ○**実施** ・**効果の評価**の実施 ・インシデントから得られる**教訓の統合** ・**投資**を通じたオープン・自由・信頼できる・セキュアなインターネット空間の実現	○**概要：2030年のビジョン** ・2030年までに豪州がサイバーセキュリティで世界のリーダーとなることを目指す。そのため、６つのシールドで国民を保護する。 ○**戦略の背景** ○**Shield１：強固な企業と市民**（＝中小企業支援、脅威アクターの破壊・抑止、ビジネス部門への明確なガイダンスの提供等） ○**Shield２：安全なテクノロジー**（＝デジタル製品・ソフトウェアの信頼確保、新興技術(AI,耐量子計算機暗号)の安全な私用の促進等） ○**Shield３：世界最高レベルの脅威共有と遮断**（＝産業界との戦略レベルの脅威情報共有、対処レベルの情報共有促進） ○**Shield４：重要インフラ防護**（＝義務づけの強化、演習等） ○**Shield５：自立的能力**（＝人材育成、自国のサイバーセキュリティ産業育成） ○**Shield６：強靱な地域とグローバル・リーダーシップ**（＝アジア太平洋の同志国との連携強化、国際ルール・規範・標準の策定・保護） ○**次のステップ：実施と評価** ・リソース配分、産業界との協調、進捗状況評価等を通じて、戦略を着実に実施する。

脅威の防止・抑止
能動的サイバー防御、情報共有、演習　等

社会全体のサイバーセキュリティ向上
基準の強化、セキュアバイデザイン　等

人的・技術的基盤の確保
人材育成、産業育成

サイバー対処能力強化法※1及び同整備法※2について

※1　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（令和７年法律第42号）
※2　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の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）

- 国家安全保障戦略（令和4年12月16日閣議決定）では、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との目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISCの発展的改組・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の設置** 等の実現に向け検討を進めるとされた。
- 令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概　要

総　則
- 目的規定、基本方針等（第１章）

官 民 連 携（強化法）
- 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

  （第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（強化法）
- 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（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

→ 分析情報・脆弱性情報の提供等（第８章）

アクセス・無害化措置（整備法）
- 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（整備法）
- 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　公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項

■ 社会全体へのDXの浸透や、AI・量子技術等の進展により、サイバー空間を巡るリスクが急速に変化する中、**喫緊に取り組むべき施策の方向性**を取りまとめ（2025年5月29日サイバーセキュリティ戦略本部決定）。

■ これらの施策について、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施策と一体的に推進するため、改組後のサイバーセキュリティ戦略本部において、政府全体の推進体制を強化するとともに、**年内を目処に新たなサイバーセキュリティ戦略を策定。**

新たな司令塔機能の確立

- NISCを我が国におけるサイバーセキュリティの司令塔機能を担う新組織へ発展的に改組
- 新組織を中心に、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

巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化

- 新たな官民連携エコシステムの実現
  - 官民連携基盤の整備
  - 政府からの積極的な情報提供
  - 報告等に係る民間の負担軽減　等
- 政府機関等に対する横断的な監視体制の強化、セキュリティ対策水準の向上及び実効性の確保
- 小規模自治体、医療機関等に対する支援の推進
- 官民横断的な対策の強化
  - 演習や能力構築による実践的対応力の強化
  - 脅威ハンティングの実施拡大
  - 重要インフラに係る新たな基準の策定　等
- セキュアバイデザイン原則等に基づく取組みの推進
  （IoT製品等のセキュリティ対策やソフトウェアの透明性確保　等）
- 中小企業を含めたサプライチェーン全体のレジリエンス強化
  （関係法令の適用関係の明確化、対策サービスに係る支援等　等）

サイバーセキュリティを支える人的・技術的基盤の整備

- 関係政府機関等における高度人材の確保
  （民間人材の活用、演習環境の構築　等）
- 官民共通の「人材フレームワーク」策定
- 国産技術を核とした、新たな技術・サービスを生み出すエコシステムの形成
  （研究開発や実証等を通じた技術情報等の提供、政府機関等による積極的な活用　等）
- 先端技術がサイバーセキュリティに及ぼす影響への対応
  - AIに係る安全性の確保
  - PQCへの移行

国際連携を通じた我が国のプレゼンス強化

- 国際的なルール整備に関し、二国間・多国間関係を強化、進展
- ASEAN、太平洋島嶼国に対する能力構築プログラムの提供

新たなサイバーセキュリティ戦略の方向性

- サイバー空間を取り巻く切迫した情勢や社会全体へのDXの浸透等に対応するとともに、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べく、中長期的に政府が取り組むべきサイバーセキュリティ政策の方向性を広く内外に示すため、５年の期間を念頭に、**新たな「サイバーセキュリティ戦略」を年内を目途に策定。**

深刻化するサイバー脅威に対する防止・抑止の実現	幅広い主体による社会全体のサイバーセキュリティ向上	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
• 巧妙化・高度化や、国家背景のキャンペーン等により、サイバー脅威が国民生活・経済活動及び安全保障に深刻かつ致命的な影響を及ぼす恐れ • 被害が生じる前の脅威の未然排除、事案発生後の的確な対処を含め、安全保障の観点も踏まえた実効的な防止・抑止の実現が急務	• DXの浸透により、あらゆる主体がサイバー攻撃の標的となり、直接的な被害にとどまらず、更なる攻撃に悪用される恐れ • 社会全体のサイバーセキュリティ向上に向けて、幅広い主体に対し、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	• 人口減少に伴い、官民を通じて、サイバーセキュリティ人材の不足が深刻化する恐れ • AIや量子技術等、技術革新が進展する一方、サイバーセキュリティに関する技術の多くを海外に依存
施策の方向性		
• 新たな司令塔組織（国家サイバー統括室）を中心に、官民連携・国際連携の下、安全保障の観点も踏まえ、能動的サイバー防御を含む多様な手段を組み合わせた総合的な対応方針・体制の確立・実行	• 政府機関等が範となり、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	• 産官学を通じたサイバーセキュリティ人材の確保・育成・裾野拡大 • 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

目指すべき姿

広く国民・関係者の理解と協力の下、国がサイバー防御の要となり、官民一体で我が国のサイバーセキュリティ対策を推進