資料１－１

サイバーセキュリティ2026
（2025年度年次報告・2026年度年次計画）
（案）の概要

2026年７月31日
国家サイバー統括室

1　サイバー脅威の動向等

- **我が国が戦後最も厳しく複雑な安全保障環境に直面する中、サイバー空間を取り巻く環境は、近年、一層深刻化。**
  質・量の両面で増大するサイバー攻撃の脅威は、国民生活、経済活動に多大な影響、ひいては国家安全保障上の大きな懸念。
- **社会全体のデジタル化が大きく進展する中、サプライチェーン等を通じたサイバー攻撃による被害の社会的影響は依然大きい。**
- AIを悪用してサイバー攻撃の大部分を自動的に実行することで、効率的に大規模攻撃が可能になった旨の報告や、フロンティアAIモデルによるサイバーセキュリティ性能の向上等、AI技術が急速に進展する中、**AI技術の進展・普及に伴うサイバー脅威への対応が必要。**

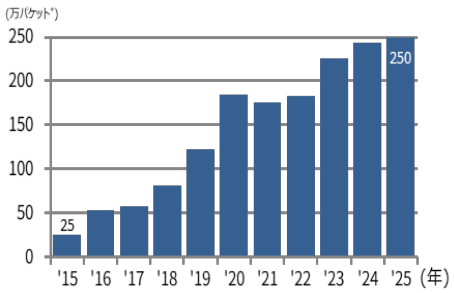
➢ 2025年度における主な国内のサイバー攻撃事案

- 電気通信事業者のメールセキュリティサービスに対し、ゼロデイ脆弱性を利用した不正アクセス（メールアカウント・パスワード等の漏えい）（2025年4月）
- 大手飲料メーカーに対するランサムウェア攻撃（受注・出荷業務等の停止、約11万5千件の個人情報漏えい）（2025年9月）
- 大手通販業者に対するランサムウェア攻撃（受注・出荷業務等の停止、約74万件の個人情報漏えい）（2025年9月）
- 医療機関に対するランサムウェア攻撃（電子カルテ等の閲覧不能、患者等の氏名、住所、病名等の漏えい）（2026年3月）

➢ （参考）政府機関等のサイバーセキュリティの確保の状況評価

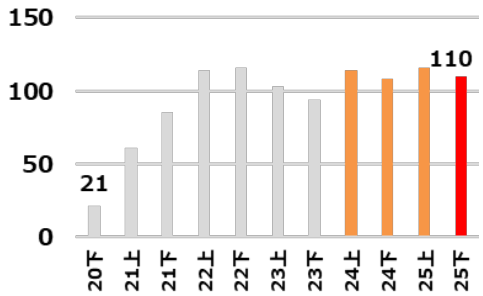
・インシデントに関連してNCOが各府省庁等から受領した報告等の件数（2024年度：447件→2025年度：517件）、GSOCから政府機関等への通報件数、各府省庁等への脆弱性等の情報提供件数のいずれも、前年度比で増加

NICTERが観測したサイバー攻撃関連通信数
※1IPアドレス当たりの年間観測パケット数



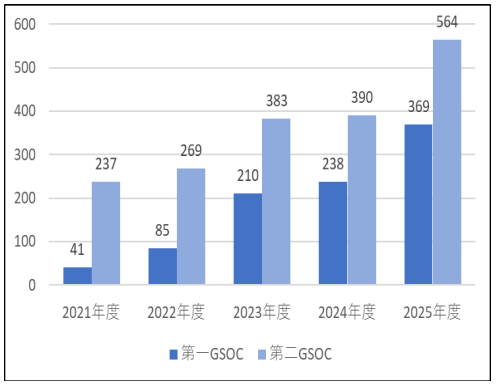
国立研究開発法人情報通信研究機構「NICTER観測レポート2025」（2026年2月5日）を基に作成

ランサムウェア被害報告件数



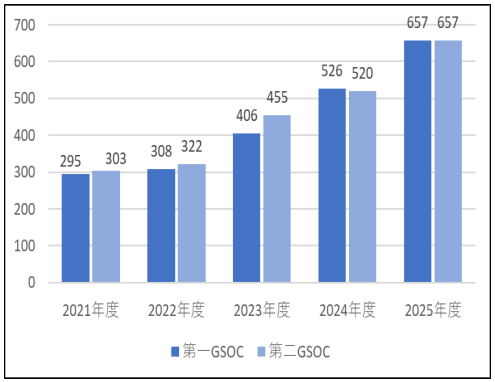
警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について（2026年3月）」を基に作成

GSOCによる政府機関等に対する不正な活動等※の通報件数



※外部から政府機関等に対する不正アクセス、サイバー攻撃やその準備動作に係るもの、標的型攻撃等によりもたらされた不正プログラムが行うもの、これらに該当するとの疑いがあるもの等

GSOCが情報提供したソフトウェアの脆弱性情報等の件数



2　サイバー脅威に対する対応の状況

- 厳しさを増すサイバー空間を巡る情勢を踏まえ、能動的サイバー防御を導入可能とするサイバー対処能力強化法等の整備や新たなサイバーセキュリティ戦略の策定、政府機関・重要インフラ等における対策・レジリエンスの向上、国際連携の強化といった取組を推進
- AI性能の高度化を踏まえ、政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」（2026年5月とりまとめ）に基づき、対応を推進

【サイバー脅威への対応に向けた昨今の主な取組】

法整備・戦略策定等

- サイバー対処能力強化法等の成立（2025年5月）
- 新たなサイバーセキュリティ戦略の策定（2025年12月）
- サイバー対処能力強化法に基づく基本方針の策定（2025年12月）
- アクセス・無害化措置の運用に関する指針の策定（2025年12月）

政府機関等

- 「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群」の一部改訂（2025年9月）
- 監査等の取組を通じて、政府機関等全体としての対策水準の向上を推進
- GSOCに関して、横断的なASMと一体的な運用、PDNSの導入等によるセキュリティレベルの底上げ
- AI性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」を取りまとめ
  （政府機関等の情報システムにおける対応、高性能AI を活用したサイバー対処能力の強化等）（2026年5月）

重要インフラ等

- 重要インフラ統一基準の施行（2026年10月）に向けた取組
- AI性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」を取りまとめ
  （重要インフラ事業者等への注意喚起やインシデント情報の収集等の実施、金融分野等での先行的な取組の実施及び他分野への展開、人材育成支援の推進、ソフトウェア・ベンダへの注意喚起等）（2026年5月）

国際連携

- 同盟国・同志国等との間で閣僚級を含む様々なレベルでの連携強化
  ・日英間の協力関係を「戦略的サイバー・パートナーシップ」に格上げ（2026年1月）
- 国連やG7等における国際的なルール形成への参画
  ・G7サイバーセキュリティWGの成果としてIoTセキュリティ及びSBOM for AIに関する合意文書を発出（2025年6月）
- パブリック・アトリビューションや国際文書等における連携強化
  ・「Salt Typhoon」に関する米国政府主導の国際アドバイザリーへの共同署名（2025年8月）
- インド太平洋地域における対応能力向上のための支援
- 国際的なサイバーセキュリティ分野の会議へのNCO幹部の登壇等を通じた、我が国のビジョンの積極的な対外発信
  ・サイバー・チャンピオンズ・サミット2026に内閣サイバー官が参加、次回は日本開催する旨を発表（2026年3月）

3　2025年度のサイバーセキュリティ関連施策の主な取組実績・評価

- サイバー対処能力強化法等の施行に向けた対応をはじめ、昨年策定した年次計画や新たなサイバーセキュリティ戦略に掲げたサイバーセキュリティ関連施策は、これら計画・戦略に照らして着実に進展。
- 一方、**我が国が戦後最も厳しく複雑な安全保障環境に直面するとともに、AIの技術的進展等も相まって、サイバー空間を取り巻く情勢の厳しさは増大。関係施策の一層の強化、AIを含め状況変化を踏まえた機動的な対応が必要。**

【2025年度の主なサイバーセキュリティ関連施策の進捗状況】

深刻化するサイバー脅威に対する防御・抑止

サイバー対処能力強化法等の施行に向けた対応

- 基幹インフラ事業者等による国へのインシデント報告等のための情報共有基盤の準備
- サイバー脅威情報の集約・分析のための体制・基盤の整備
- アクセス・無害化措置の運用に関する指針の策定
- サイバー対処能力強化法に基づく基本方針の策定、関係政令の公布
- 新協議会の立上げに向けた協議会の運営形態や関連規約の検討

そのほか官民連携

- 脅威ハンティングの普及促進、実施等に関する基本方針の策定に向けた検討

国際連携

- 大臣レベルを含む意見交換等を通じた二国間協力強化や、多国間枠組の連携強化

サイバー対処能力強化法等の実施に向けた準備、我が国のサイバー安全保障確保のための体制・基盤等の総合的な整備や国際連携強化等が必要

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

- 政府統一基準群のガイドラインの改定
- 実践的サイバー防御演習（CYDER）による人材育成

重要インフラ・地方公共団体

- 重要インフラ統一基準の施行に向けた取組
- 地方公共団体が実施するセキュリティ対策経費に係る地方財政措置の拡充や、「地方版ASMシステム」の基盤整備に向けた検討

サプライチェーン

- JC-STARの普及促進、高度基準整備、諸外国制度との相互承認
- SCS評価制度の構築方針の公表
- 同制度に基づく対策を伴走支援する新類型の「サイバーセキュリティお助け隊サービス」の制度検討

政府機関等は、他の主体の範となるべく対策向上等に取り組むとともに、各主体、サプライチェーン全体における対策強化等が必要

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

人材育成・確保

- サイバーセキュリティ人材フレームワークの策定
- SecHack365、セキュリティ・キャンプ、中核人材育成プログラム等を通じたサイバー人材育成推進

技術・サービスのエコシステム形成

- 経済安全保障重要技術育成プログラムやAIPプロジェクト等を通じた、技術・研究開発
- CYXROSSセンサーの政府機関等への導入による情報収集・分析を強化する取組の推進
- IPAにおける有望なスタートアップ製品・サービス等の調達等に向けた取組の推進

AI・量子技術の進展への対応

- AIセキュリティ確保のための技術的対策ガイドラインの策定
- 政府機関等におけるPQC利用に関する関係府省庁連絡会議の立ち上げ、中間とりまとめ

人材育成、我が国の対応能力や自律性向上に向けたエコシステム形成、サイバー分野でのAI技術の進展等への対応の抜本的強化等が必要

4　特に強力に取り組むべき施策（１）日本成長戦略における分野横断的課題としてのサイバーセキュリティ

●2025年11月、内閣に設置された日本成長戦略本部において、８つの分野横断的課題の一つにサイバーセキュリティが挙げられ、サイバーセキュリティ推進専門家会議で議論、検討

●日本成長戦略における分野横断的課題としてのサイバーセキュリティに対する対応を2026年度の「特に強力に取り組むべき施策」に位置づけ

■対応の方向性（概要）

17の戦略分野における成長投資を下支えするため、「サイバーセキュリティ戦略」に基づき、サイバー対処能力強化法等の着実な実施や関連制度の機動的な見直し等により、サイバー脅威への対応を強化する。その際、この対応が成長に必要な投資との認識を共有した上で、官民が協力した持続可能なサイバーセキュリティ確保の在り方を検討する。

■講ずるべき施策パッケージ（概要）

① 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

・SCS評価制度等の整備等による**17の戦略分野を始めとしたサプライチェーン全体の対策の強化**、重要インフラ統一基準の策定等による**重要インフラ分野における対策の強化**、強靭なシステムの構築・運用や高機密ソブリンクラウド(仮)の導入を進めるための早急な検討等による**政府機関等の対策の強化**、地方公共団体・中小企業・医療・大学等の**一層の対策が必要な分野の底上げ**

② 国が要となって推進するサイバー脅威に対する防御・抑止

・防御側に係る施策と攻撃者に対抗する施策を“車の両輪”とし、サイバー対処能力強化法等に基づく取組を含め、平素から継続的に攻撃者側にコストを賦課することにより、**国が要となって、官民全体でサイバー脅威の防御・抑止を推進**

③ 我が国のサイバー対応強化と自律性確保のための人材・技術・産業の育成・確保

・人材フレームワークの活用促進。企業等のセキュリティ担当者のスキル向上・若手技術者の能力向上、大学等におけるセキュリティ教育の強化に向けた教育・訓練機会の提供。

・各製品・技術等の「官民投資ロードマップ」との連携も含め、技術・研究開発プログラム等の推進、先進的・有望セキュリティ製品・サービスの政府機関等における積極的な活用及び評価等による、国内におけるサイバーセキュリティ技術・研究開発、産業育成の推進

④ AI等の技術進展への対応

・**「Project YATA-Shield」に基づく、AIを活用した政府全体の重要システムの脆弱性点検等の必要な対応の速やかな実施。**
サイバーセキュリティ関連情報の集約化や、機密性の高いデータを扱う際のAI活用の考え方等の検討・具体化。AISIの機能の抜本的強化。新協議会の枠組みの下で、IPA ・AISIと連携し情報共有等の取組を強化するなどのAIセキュリティ に関する官民連携の強化

・政府機関等における耐量子計算機暗号（PQC）への移行のための工程表の策定、産業界の移行を後押しするためのガイドラインの整備や、移行作業の支援に向けた実証。量子暗号通信の特徴を踏まえた導入・運用方法のガイドラインの整備や、技術課題の実証

4　特に強力に取り組むべき施策（２）AI性能の高度化を踏まえた対策パッケージ「Project YATA-Shield」

- AI 技術が急速に進展・普及し、サイバー攻撃にAI が悪用されることで、攻撃のスピード・規模が劇的に増加するなど、サイバーセキュリティにおける脅威に直面している状況
- 2026年5月、AI性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」を取りまとめた。同パッケージに基づき、関係省庁・関係機関は、これら施策を迅速かつ的確に実施。
- このことを踏まえ、対策パッケージ「Project YATA-Shield」を、2026年度の「特に強力に取り組むべき施策」に位置づける。

「Project YATA-Shield」の概要

基本的な認識・考え方

重要インフラ事業者等・政府機関等が取るべき対応

- **発見された脆弱性のパッチ適用やリスク緩和措置**を速やかに実施（リスクベース）
- **基本的な対策**、**多層防御の実施**、**インシデント発生時の備え**　等

※英国・米国政府の注意喚起も参考に

脆弱性を発見するAIの進化

- **Anthropic（Project Glasswing）**：Mythosへのアクセスを、**ビッグテックや重要インフラ等**に限定。
- **OpenAI**：GPT-5.5-Cyberへのアクセスを、**一部の認証者**に限定して付与。

実施する施策

重要インフラ事業者等・政府機関等への対応

① 重要インフラ事業者等への注意喚起等
② 金融分野での先行的な取組及び 他分野への展開
③ 人材育成支援
④ 政府機関等の情報システムにおける対応

脆弱性の発見・修正等への対応

① 外国政府機関やビッグテック等との更なる連携
② ソフトウェア・ベンダへの注意喚起
③ AISIによる技術支援等
④ 技術開発の推進
⑤ 高性能AIを活用したサイバー対処能力強化