情報セキュリティ白書2025に見る脅威の動向と対策

2026年3月

独立行政法人情報処理推進機構
セキュリティセンター

IPA Better Life with IT

自己紹介

■小山　明美（こやま　あけみ）

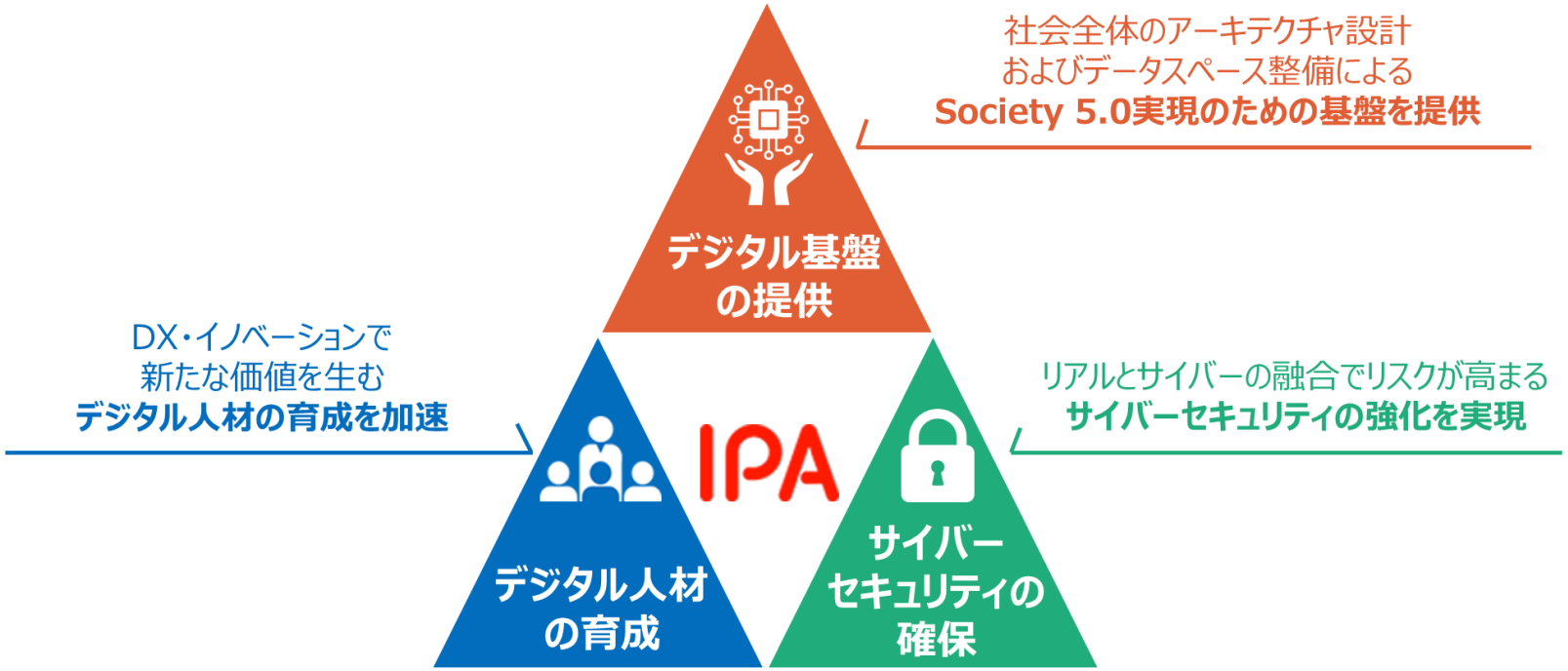
独立行政法人情報処理推進機(IPA)
セキュリティセンター サイバー情勢分析部　調査グループ　グループリーダー
（併任）AIセーフティインスティテュート

- **出版物・発刊物**
  - 情報セキュリティ白書
  - 情報セキュリティ読本
  - 情報セキュリティ10大脅威
- **社会調査事業**
  - 米国におけるAIのセキュリティ脅威・リスクの認知調査レポート
  - AI利用時のセキュリティ脅威・リスク調査報告書
  - 企業の内部不正防止体制に関する実態調査
  - クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査
- **ツール**
  - サイバーセキュリティ経営可視化ツール
- **ガイド**
  - サイバーセキュリティ経営ガイドライン Ver 2.0実践のためのプラクティス集
  - 組織における内部不正防止ガイドライン

独立行政法人情報処理推進機構（IPA）について

日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人。
誰もが安心してITのメリットを実感できる「**頼れるIT社会**」の実現を目指しています。

「**人材**」、「**セキュリティ**」、「**デジタル基盤**」の3つの中核事業



■ **名称: 独立行政法人情報処理推進機構**
(Information-technology Promotion Agency, Japan)
■ **設立: 2004年1月5日**
（前身母体の設立は1970年10月1日）
■ **理事長: 齊藤 裕**

サイバーセキュリティに関する業務概要

平時からインシデント発生時まで、サイバーセキュリティのマネジメントからオペレーションまでトータルな施策・対応を実施。

普及啓発／地域・中小企業支援

- **地域・中小企業支援**
  - セキュリティ自己宣言制度
  - サイバーセキュリティお助け隊
  - セキュリティ相談窓口
- **普及啓蒙コンテンツの発信**
  - セキュリティ10大脅威
  - 情報セキュリティ白書
  - AIセキュリティ調査

相談受付件数12,787件（2024年）

SECURITY ACTION
セキュリティ対策自己宣言

累計宣言数 約39万件
（2024年12月）

サイバーセキュリティ お助け隊

サイバー攻撃の検知分析／対処支援

- **サイバー情勢の地政学分析**
- **標的型サイバー攻撃の対策支援**

J-CRAT
初動対応支援
366件
（2023年）

- **情報共有**（攻撃対策情報、脆弱性情報、マルウェア・不正アクセス届出）
- **不正通信監視**（独法等）
- **サイバー事故原因究明**

JVN iPedia
脆弱性データベース
約22万件登録（2024年12月）

J-CSIP
情報共有枠組
業界数13（組織数279）
（2023年12月現在）

ガイドライン策定／セキュリティ評価・認証

- **セキュリティガイドライン**（中小企業向け、内部不正対策等）
- **情報セキュリティ監査・評価**
  - 情報セキュリティ監査（独法等）、政府システム監査
  - クラウドセキュリティ評価（ISMAP）
  - 制御システムリスクアセスメント支援

JC-STAR

- **評価認証・暗号**
  - IoT製品セキュリティラベリング（JC-STAR）、JISEC
  - 暗号動向調査

CRYPTREC
Cryptography Research and Evaluation Committees

セキュリティ人材育成

- **国家資格「情報処理安全確保支援士」**
  登録者数22,845名（2024年10月1日時点）
- **中核人材育成プログラム**
  累計435名修了（2017年～）
- **若手人材発掘（セキュリティ・キャンプ）**
  累計1,232名受講（2004年度～）
- **情報セキュリティコンクール**
  応募約５万点（2023年度）

情報セキュリティ白書2025

2024年度*のサイバーセキュリティに関する国内外の政策・取り組み、脅威の動向、インシデントの発生状況、被害実態などの定番トピックの他、その年ならではの注目事象などを取り上げています。
（＊政策動向についてはサイバー対処関連法案やトランプ政権の方針変更など2025年5月までの情報を含みます。）

サブタイトル

一変する日常：支える仕組みを共に築こう

印刷書籍版（9月30日発行）

ISBN

ソフトカバー／A4判　232ページ(前年比32ページ減)

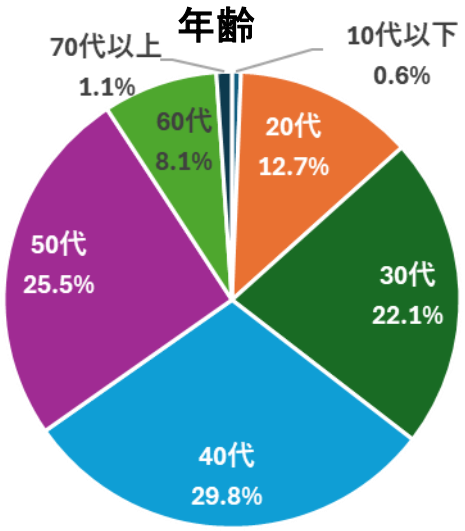
定価：2,200円（本体価格2,000 円＋税10%）

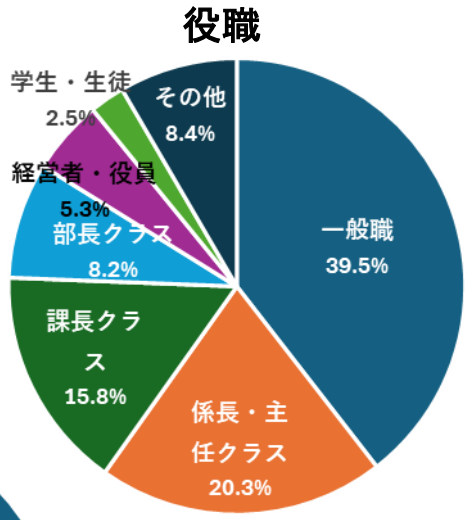
購入方法：Amazon、全国官報販売協働組合、
書店（お取り寄せ）

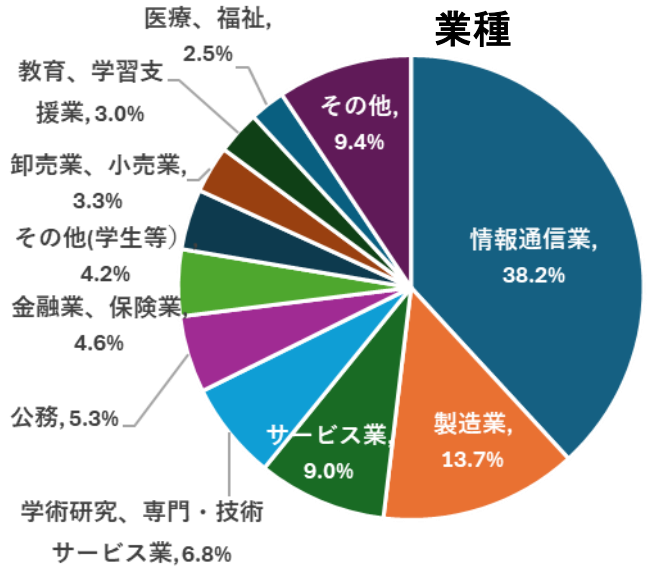
PDF版　（9月30日発行）

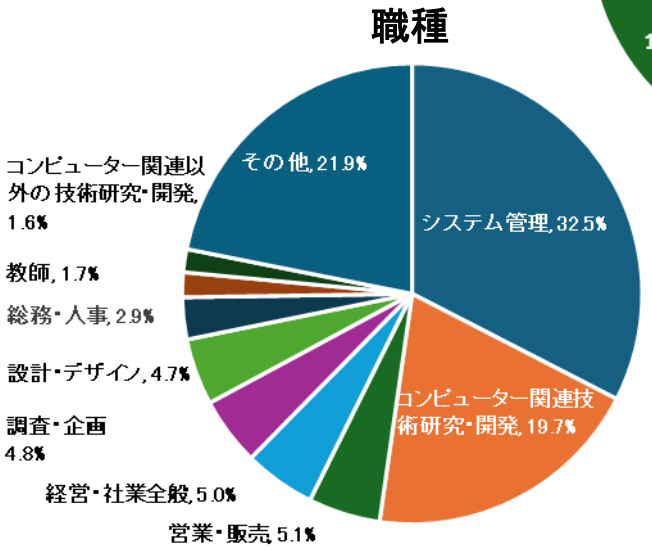
https://www.ipa.go.jp/publish/wp-security/2025.html

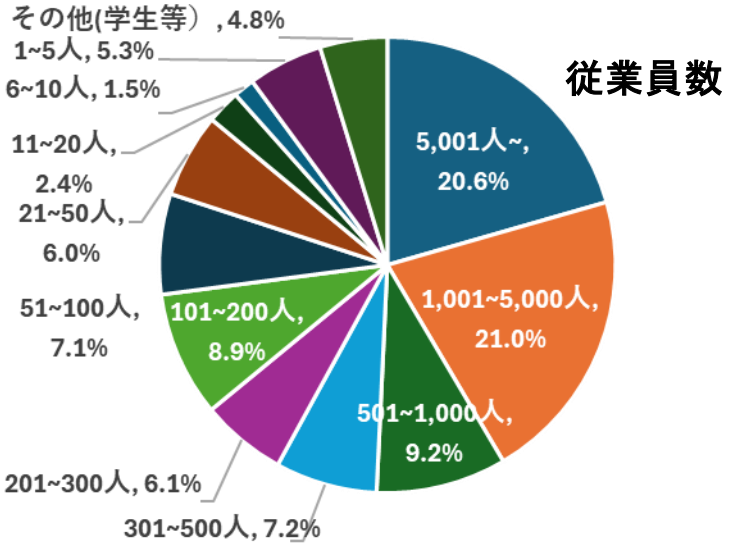
参考　情報セキュリティ白書2025利用者属性







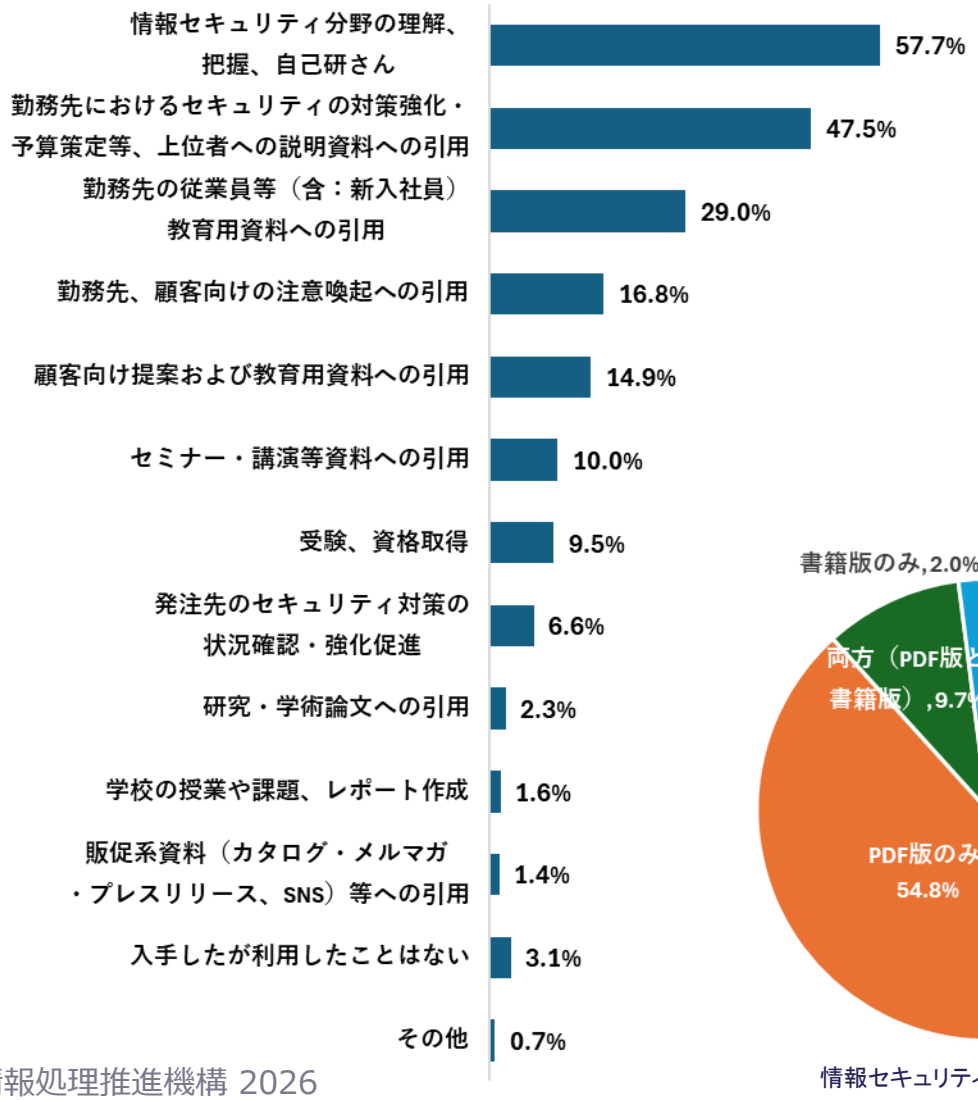




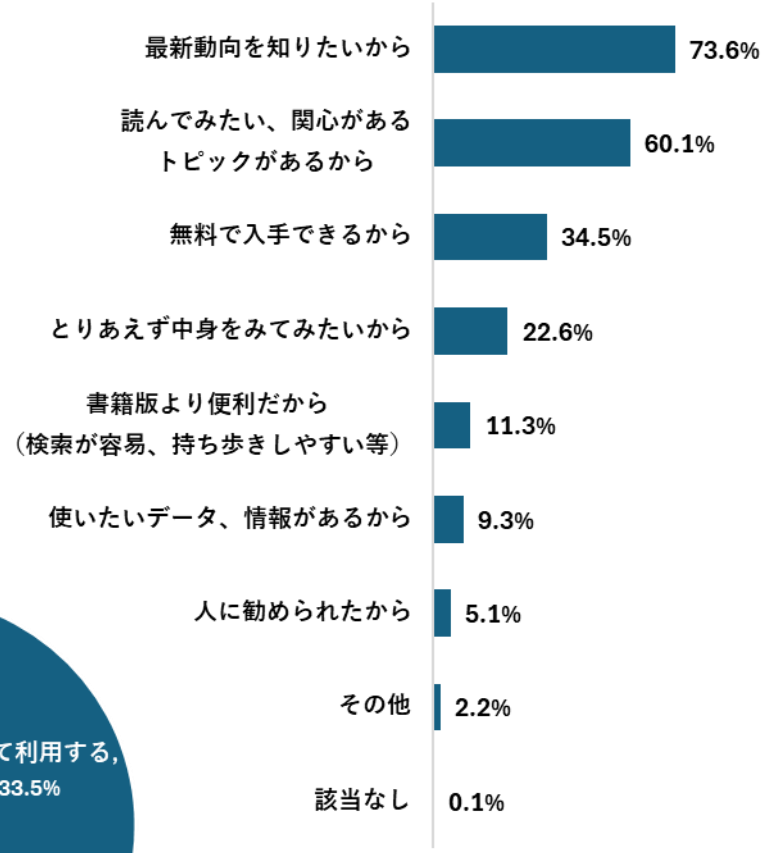
情報セキュリティ白書2025
ダウンロードいただいた方へのアンケートより（n=6,636）

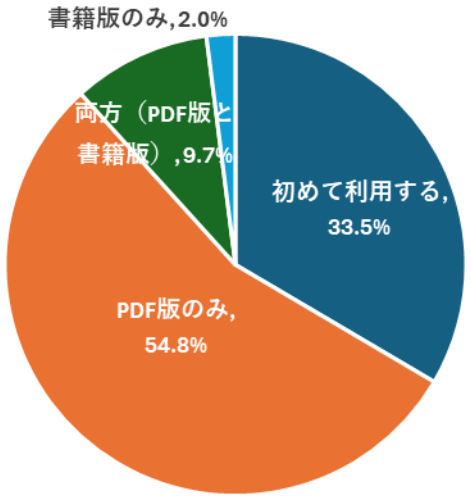
参考　情報セキュリティ白書をダウンロードした方に伺いました。

利用経験者の“利用の仕方”



初めて利用する人の“動機”





情報セキュリティ白書2025をダウンロードいただいた方へのアンケートより（n=6,636）

サブタイトルの変遷に見るセキュリティの動向

- 白書2021(2020年度) 変わる生活、変わらぬ脅威：自らリスクを考え新しい行動を
  - スマホ決済の不正利用、廃棄HDDからの情報流出、コロナ感染拡大
  - サイバーセキュリティお助け隊、ISMAP、GDPR本格運用開始

- 白書2022(2021年度) 進むデジタル、広がるリスク：守りの基本を見直そう
  - ニューノーマル環境への攻撃、ランサムウェア（二重の脅迫）、Emotet
  - Solar Winds、Colonial Pipeline 事案によりで米国対策強化

- 白書2023(2022年度) ゆらぐ常識、強まる脅威：想定外に立ちむかえ
  - 病院や自動車部品会社のランサムウェア被害、サプライチェーン攻撃
  - ロシアのウクライナ侵攻（武力戦と情報戦のハイブリッドな戦い）

- 白書2024(2023年度) 変革の波にひそむ脅威：リスクを見直し対策を
  - 国家関与のサイバー攻撃、ランサム攻撃の更なる活発化(港湾，クラウド)
  - AI技術投入で認知戦・情報戦の激化，AIの安全な利用を目指す制度作り

2024年度の情報セキュリティの概況

白書2025(2024年度）一変する日常：支える仕組みを共に築こう

- **ランサムウェア攻撃、標的型攻撃、DDoS攻撃**などが国内外で多数観測されるとともに、攻撃の手口の巧妙化・洗練化も確認されるなど、**サイバー空間における脅威はますます増大**。
  国際情勢が一層厳しさを増す中で、**地政学リスク**に起因するサイバー攻撃や偽情報の拡散など**認知領域における情報戦**なども観測。
- 生成AIをはじめとするAI関連技術の進展は著しく、**サイバー攻撃・防御の双方でAIの利用**が進展。
  サイバー攻撃によるAIシステムへの攻撃や悪用、認知領域への攻撃が懸念。
- 国内では、**サイバー対処能力強化法及び同整備法**、**国家サイバー統括室**の設置等、「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るための**能動的なサイバー防御**を実施する体制の整備。
- システムの設計段階から脆弱性を除去し、攻撃を未然に防ぐための「**セキュア・バイ・デザイン**」に向けた取組（例えば、JC-STAR（セキュリティ要件適合評価及びラベリング制度）の運用開始や、**サプライチェーンのセキュリティ強化**に向けたセキュリティ対策評価制度など）についても多くの進展が見られました。

2024年度の情報セキュリティの概況（時系列）

2024年度の国内外の主な情報セキュリティインシデント・事件及び情報セキュリティ政策・イベント

	主なセキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2024年4月	●米国のマルチクラウドデータウェアハウスプラットフォームを利用している複数の組織を標的としたデータ侵害が発生（1.1.1） ●米国のセキュリティベンダーが提供するファイアウォール用OSに対するゼロデイ攻撃を確認（1.2.4）	●米国「外国敵対勢力が管理するアプリから米国人を保護する法」成立（4.1.1）
5月	●国家の支援が疑われるサイバー攻撃グループが、国内の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（1.2.2） ●行政機関等から通知書等の印刷と発送を請け負っていた印刷会社でランサムウェア被害（1.2.1）	●「重要経済安保情報保護活用法」成立（3.1.1） ●NISCと警察庁が、米国CISAの作成したサイバー脅威緩和に関する国際ガイダンスに共同署名（4.1.1） ●「AIソウル・サミット」開催（2.1.3）
6月	●総合エンタメ企業が展開する動画共有サービス等がランサムウェア攻撃を受け、サービス停止（1.2.1）	●「G7プーリア・サミット」開催（3.1.1）
7月	●日本・NATOの活動に抗議するDDoS攻撃が発生（1.2.3） ●米国サイバーセキュリティ会社のシステム障害により世界約850万台のWindowsデバイスに影響が発生（1.1.1） ●パリオリンピック関連のスポンサー、パートナーを標的としたDDoS攻撃が発生（1.1.1）	●NISCと警察庁は、オーストラリアのACSCが作成したAPT40に関する国際アドバイザリーに共同署名（4.1.1） ●NISC「サイバーセキュリティ2024」公表（3.1.1） ●NISTは、生成AIのセキュア開発のためのプロファイルである「SP 800-218A」公開（4.1.2）
8月	●不動産仲介業の従業員が同業他社に転職する際、不動産登記簿に基づく社内資料を不正持ち出し（1.2.7） ●米国の国際空港がランサムウェア攻撃を受け、フライト情報表示等の重要な機能に影響が発生（1.2.5）	●EU「AI Act」発効（2.1.1,2.1.3） ●経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 2.0」公表（3.1.3）
9月	●米国司法省は、国家の支援が疑われる攻撃グループに侵害された20万台超の消費者向け機器からなるボットネットを無害化したと発表（1.2.2） ●米国の水処理施設にランサムウェア攻撃（1.2.5）	
10月	●ランサムウェア開発者らを欧州刑事警察機構等による共同捜査により逮捕（4.1.1） ●日米共同統合演習に抗議するDDoS攻撃が発生（1.2.3）	●ACSCは、重要インフラ事業者に向けて策定した「OTサイバーセキュリティの原則」公開（4.1.5）
11月	●米国大統領選挙で、複数の国家が関与すると見られる影響工作を確認（2.2.3） ●米国大統領選挙期間中に大規模なDDoS攻撃が数日にわたり発生（1.1.1） ●国家の支援が疑われる攻撃グループが9社の米国通信事業者、及び世界中の企業数十社を侵害していたことをFBI等が公表（1.1.1、1.2.5）	●IPAとAJCCBCは、オランダのNCSCと協働し、タイで重要情報インフラ保護に関する人材育成プログラムを提供（4.1.1） ●経済産業省とIPAは米国・EU政府と連携し、「インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク」開催（4.1.1）
12月	●米国の地域交通局がランサムウェア攻撃を受け、鉄道の遅延等の一時的な混乱が発生（1.2.5） ●年末から年始にかけて国内の重要インフラ企業等へ大規模なDDoS攻撃が発生（1.2.3）	●EU「サイバーレジリエンス法」発効（4.1.3） ●国連総会にて、サイバー犯罪に関する包括的な国際条約である「国連サイバー犯罪条約」採択（4.1.1） ●EUのサイバーセキュリティ能力を強化する「サイバー連帯法」及び「改正サイバーセキュリティ法（CSA）」が成立（4.1.3）
2025年1月	●警察庁及びNISCは、安全保障や先端技術に係る情報窃取を目的とした攻撃グループによる攻撃キャンペーンについて、国家の関与が疑われる組織的なサイバー攻撃活動であるとして注意喚起（1.2.2）	●「U.S. Cyber Trust Mark」運用開始（4.1.2） ●米国大統領令14144、ソフトウェアサプライチェーンセキュリティ強化策等を指示（4.1.2） ●EU「デジタルオペレーショナルレジリエンス法」全面適用開始（4.1.3） ●米国大統領令14179、Biden政権のAI統制施策を棄却（4.1.2）
2月	●営業秘密にあたる研究データを外国企業に漏えいしたとして国立研究開発法人の元研究員に有罪判決（1.2.7）	●「AIアクションサミット」開催（2.1.3） ●「サイバー対処能力強化法案」及び「同整備法案」が閣議決定（3.1.1） ●米国DHS、CISA等所管機関の活動縮小（4.1.2）
3月	●地方銀行をかたる自動音声を含む電話による大規模なボイスフィッシング被害が発生（1.1.2）	●経済産業省「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）」公開（3.1.3） ●IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」運用開始（3.3.1）

ランサムウェア被害、標的型攻撃、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。

表の（数字）は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。

目次概要

目次	概要
1章　国内外のサイバー脅威の動向 1.1 2024年度に観測されたインシデント状況 1.2 インシデント事例や脆弱性、攻撃の動向と対策	2024年は**世界各地で紛争や対立が発生、再燃し、地政学的な緊張**の高まりが顕著であった。これに伴い、サイバー空間では**国家の関与**が疑われる攻撃、世界的な大規模イベントや各国の**選挙を標的**とした攻撃等が確認され、サイバー空間における脅威の深刻化が実社会に及ぼす影響の大きさを浮き彫りにした。 １本章では、国内外で発生した主なインシデントの概要、手口、対策の動向等を解説する。
2章　最近のサイバー空間を巡る注目事象 2.1 AIの安全性確保の取り組み 2.2 偽・誤情報の脅威と対策の動向	最近のサイバー空間には**AIの普及**により急速な変化がもたらされている一方、そのAIを悪用した**偽情報の拡散**が公共への大きな脅威となっている。 ２章では注目事象として、AIセーフティ実現に向けた取り組みと、偽情報・誤情報の脅威と対策を取り上げる。
3章　国内の政策及び取組みの動向 3.1 国内のサイバーセキュリティ政策の状況 3.2 サイバーセキュリティ人材の現状と育成 3.3 製品・サービスの評価・認証制度・暗号技術の動向 3.4 組織・個人に向けたサイバーセキュリティ対策の普及活動	2024年には、我が国の**サイバー安全保障分野での対応能力向上**を目的とした各種法整備が進み、政府機関等により、これに関連した様々な取り組みが開始された。また、網羅的なセキュリティ対策強化のため、**中小企業**を含む人材育成の取り組みや機会創出、**評価・認証制度**の運営、普及啓発活動も進んでいる。 ３章ではサイバーセキュリティに関する国内の政策、取り組みについて解説する。
4章　国際的な政策及び取り組みの動向 4.1 国際的なサイバーセキュリティ政策の状況 4.2 国際標準化活動	2024年は**欧米各国で国政選挙**が行われたが、そこでは分断や混乱を狙った様々な**サイバー攻撃や影響力工作**が見られた。国際連携により国境を越えた脅威に対抗する我が国の取り組みと、各国・各地域における情報セキュリティ政策について述べる。 また、2024年のセキュリティ分野での国際標準化の動きとしてISO/IEC JTC 1/SC 27（情報セキュリティ）とIEC TC 65/WG 10（制御システムのセキュリティ）の活動を紹介する。
コラム　耐量子計算機暗号（PQC）、セキュリティは「コスト」か「投資」か、データマネジメント、クラウドサービス、WISDOM-DX、10大脅威	昨今のトピックとして、話題になっているテーマやIPAならではの活動を、初学者にもわかりやすく、簡潔に掲載しました。

情報セキュリティ白書2025(1章目次)

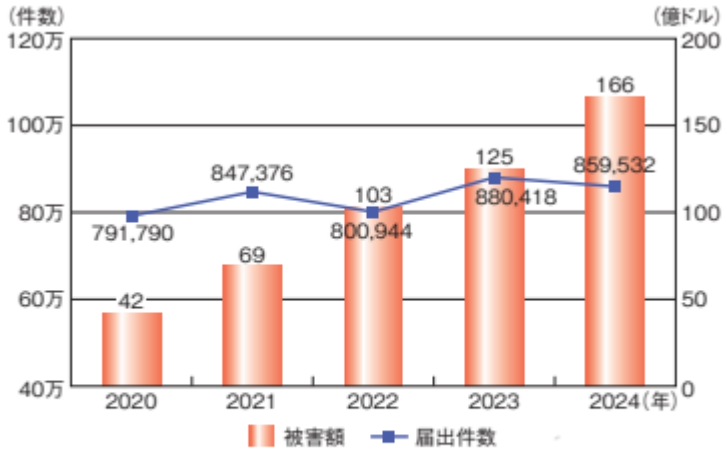
第1章 国内外のサイバー脅威の動向

情報セキュリティ10大脅威2026（2026年1月29日公表）

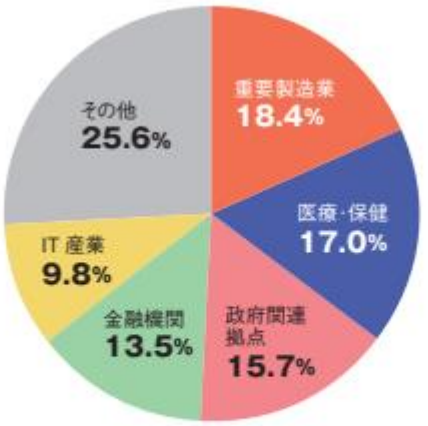
順位	2024	2025	2026
1	ランサムウェアによる被害	ランサム攻撃による被害	ランサム攻撃による被害
2	サプライチェーンの弱点を悪用した攻撃	サプライチェーンや委託先を狙った攻撃	サプライチェーンや委託先を狙った攻撃
3	内部不正による情報漏えい等の被害	システムの脆弱性を突いた攻撃	AIの利用をめぐるサイバーリスク【新規】
4	標的型攻撃による機密情報の窃取	内部不正による情報漏洩等	システムの脆弱性を悪用した攻撃
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	機密情報を狙った標的型攻撃	機密情報を狙った標的型攻撃
6	不注意による情報漏えい等の被害	リモートワーク等の環境や仕組を狙った攻撃	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7	脆弱性対策情報の公開に伴う悪用増加	地政学リスクに起因するサイバー攻撃	内部不正による情報漏えい等
8	ビジネスメール詐欺による金銭被害	分散型サービス妨害攻撃（DDoS攻撃）	リモートワーク等の環境や仕組みを狙った攻撃
9	テレワーク等のニューノーマルな働き方を狙った攻撃	ビジネスメール詐欺	DDoS攻撃（分散型サービス妨害攻撃）
10	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏洩等	ビジネスメール詐欺

1.1.1　世界における情報セキュリティインシデント状況

サイバー攻撃の高度化、激化は依然として続いており、脅威は高まっている



■図 1-1-1　サイバー犯罪の届出件数と被害額の推移(2020～2024年)
(出典)FBI「Internet Crime Report 2024」を基に IPA が作成



■図 1-1-4　ランサムウェア被害を受けた重要インフラの業種別構成比
(2024 年、n=1,403)
(出典)FBI「Internet Crime Report 2024」を基に IPA が作成

上位5業種は2021年以降変わらず引き続き警戒が必要

RaaSがランサムウェアの蔓延と持続化に影響

注目されたインシデント

◆国家関与が疑われる攻撃

Salt Typhoon
- 米国通信事業者9社を含む世界十数社への侵入
- 広域なスパイ活動、情報収集

◆大規模システム障害

CrowdStrike社
- アップデート作業でのミス
- 約850万台のWindowsデバイスに被害

DDoS攻撃の増加

◆パリオリンピック・パラリンピック

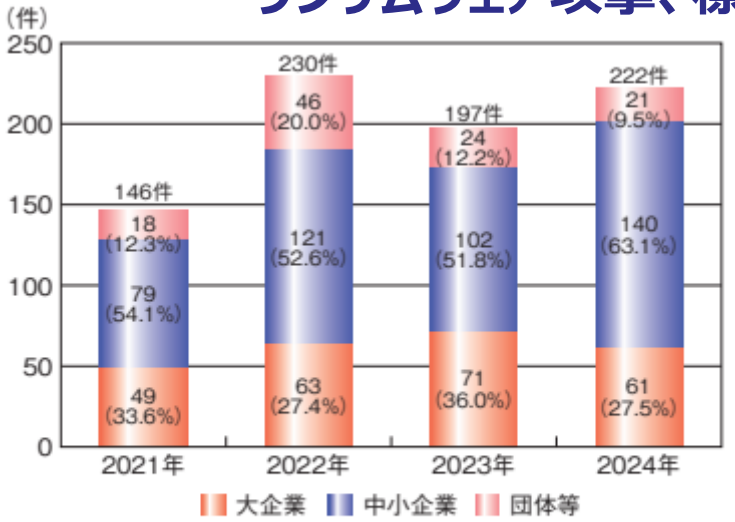
関連会社Webサイトへの攻撃
- 7月　2億件以上、8月　11日間で9000万件以上
- 交通機関のWebサイト最終日1秒当たり50万件以上

◆米国大統領選挙

政党、選挙インフラ等への攻撃
- 11月1日～6日　60億件以上
- ピーク時　1秒当たり70万件以上

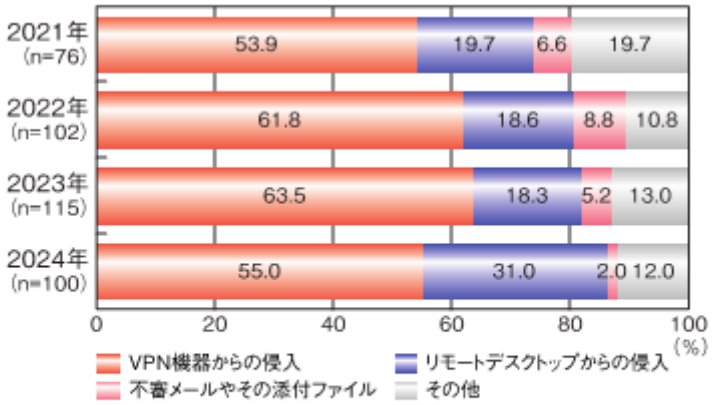
1.1.2 国内における情報セキュリティインシデント状況

ランサムウェア攻撃、標的型攻撃の猛威は続いている。



■図 1-1-11 国内のランサムウェアによる被害件数(2021 ～ 2024 年)
(出典)2021 ～ 2024 年の警察庁資料を基に IPA が作成

中小企業の被害が増加



■図 1-1-12 ランサムウェアの感染経路(2021 ～ 2024 年)
(出典)2021 ～ 2024 年の警察庁資料を基に IPA が作成

テレワークで利用される機器からの侵入が8割

ランサムウェア攻撃事例

◆大規模エンターテインメント企業への攻撃

Webサイト、動画共有サービス、受発注システムが利用停止

25万人を超える個人情報の漏えい

◆印刷企業への攻撃

委託元民間団体32団体、行政機関9団体、
再委託元約60団体に影響
VPN機器への不正アクセスが原因

標的型攻撃事例

◆国家を背景とした攻撃

MirrorFace

国内の学術、シンクタンク、政治家、メディアに関係する個人や組織等と対象とした、標的型攻撃メールを用いた攻撃
2025年1月、警察庁及びNISCが注意喚起

TraderTraitor

暗号資産関連事業者が対象、リクルーターになりすまし従業員に接触
約482億円相当の暗号資産窃取

情報セキュリティ白書2024(2章目次)

第2章　最近のサイバー空間を巡る注目事象

2.1 AIセーフティ実現に向けた取り組み

■AIの急速な発展

1950年～2000年	2000年～2022年	2022年～
AI技術、関連技術の開発	機械学習とディープラーニング	汎用的AIの登場・発展

■AIリスクとは

AIの悪用がもたらすリスク	フェイク画像等がもたらす個人への被害 世論操作（影響工作） AIを悪用したサイバー攻撃 CBRN兵器の開発支援
AIの不適切動作によるリスク	信頼性の問題 バイアス コントロールの喪失
システミックリスク	労働市場リスク 世界的なAI研究開発格差 市場における一部企業への集中と単一障害点 環境へのリスク プライバシーへのリスク 著作権侵害のリスク

■AIセキュリティの現状（2025年3月時点）

AIシステムへのサイバー攻撃　大きな被害はない
AIを悪用したサイバー攻撃　攻撃の参入障壁を下げることが懸念
AIを用いた認知領域への攻撃　広く確認されている

AIセキュリティリスクに関する予測
「2025年とその先に向けて、犯罪市場にAIのもたらす能力はコモディティ化し、サイバー犯罪や国家支援アクターに更なる力添えを間違いなく提供する。」
出典The near-term impact of AI on the cyber threat 2024/01/24 (UK-NCSC)

「サイバーセキュリティ対策が遅れる、あるいは変更がなければ、2027年までに重要なシステムが高度な脅威者に対して脆弱になる現実的な可能性がある。「最先端のAI」の能力に追いつくことが、今後10年間のサイバー耐性にとってほぼ確実に重要となる。」
出典Impact of AI on cyber threat from now to 2027 2025/05/07 (UK-NCSC)

2.1.3 AIセーフティに関する取り組み

2023年5月	2023年12月	2024年2月	2024年5月	2024年7月	2025年3月
日本から「広島AIプロセス」を提唱	「広島AIプロセス包括的政策枠組み」等に各国合意	AIセーフティ・インスティテュート(AISI)設立 （事務局はIPAに設置）	広島AIプロセスフレンズグループを設立 安全・安心で信頼できるAIの実現を目指す、賛同国による自発的な国際枠組み	GPAI東京専門家支援センター設立 GPAIに所属するAIの専門家を支援する組織	広島AIプロセスレポーティングフレームワーク運用開始 2025年5月26日時点19社が参加

役割

政府への支援
・AIセーフティに関する調査、評価手法の検討や基準の作成等

日本におけるAIセーフティのハブ
・産学における関連取組の最新情報の集約
・関係企業・団体間の連携促進
・他国のAIセーフティ関係機関との連携

関連の研究機関との連携実施
・国研等の関係研究機関との連携
・パートナーシップ事業の推進

AIの開発や利用をする者が**AIのリスクを正しく認識**できる仕組みの構築 ＋ ガバナンス確保などの必要となる対策を**ライフサイクル全体で実行**できる仕組みの構築 ⟷ **国内・国際的な関係機関**

イノベーションの促進と**ライフサイクルにわたるリスクの緩和**を**両立**する枠組みを実現

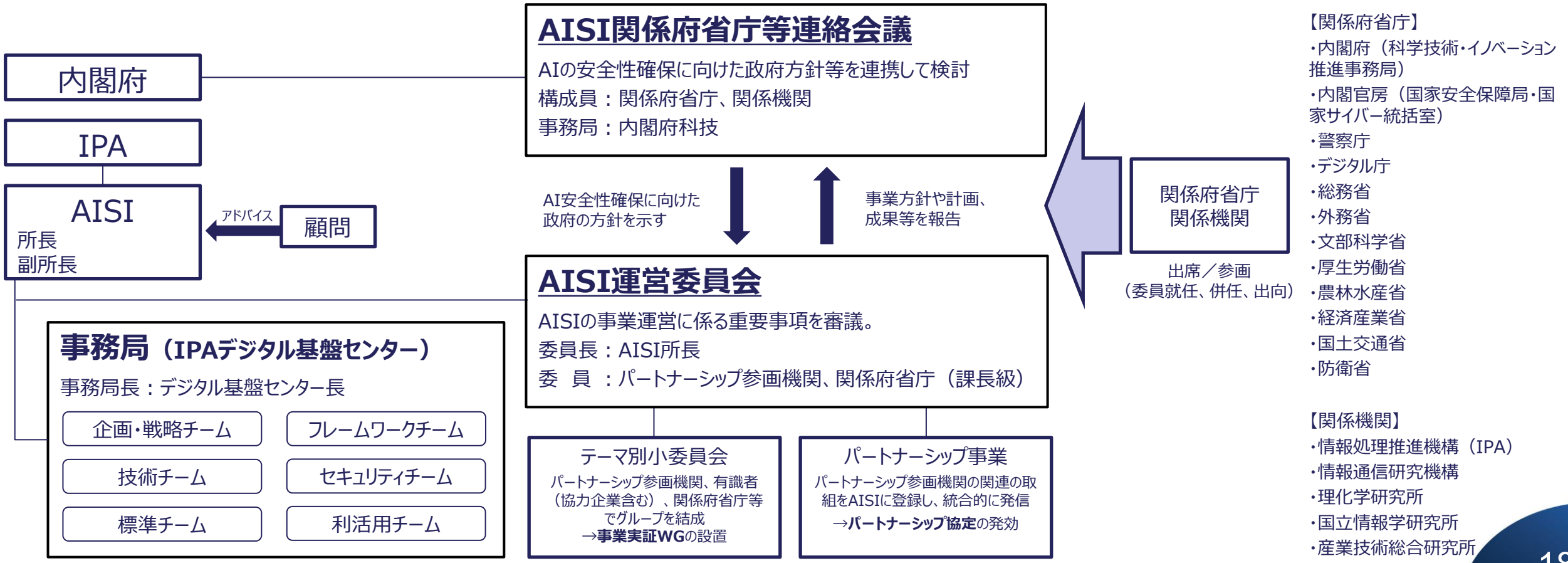
スコープ

- AIによる以下の事象や検討事項の中で、諸外国や国内の動向も見ながら柔軟にスコープを設定し取組を進めていく。

社会への影響 | **ガバナンス** | **AIシステム** | **コンテンツ** | **データ**

AISIの推進体制

- 内閣府を事務局とする「**AISI関係府省庁等連絡会議**」で政府方針等を検討AISI所長を委員長とする「**AISI運営委員会**」で事業方針を検討



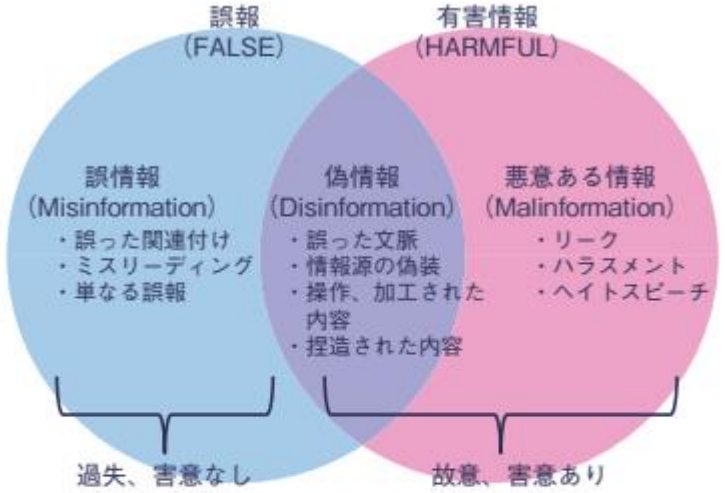
これまでの活動と成果物　https://aisi.go.jp/

	国際	AISI	政府
	イベント	成果物	
2024	AIソウル・サミット, 韓国	• 日米クロスウォーク1の成果公表(4/30)	
	AISI国際ネットワーク会合, 米国	• 米国AI RMF 日本語翻訳版の公表(7/4) • 評価観点ガイドの公表(9/18) • レッドチーミング手法ガイド※の公表(9/25)	• AI事業者ガイドラインの公表(4/19) • 統合イノベーション戦略2024の公表(6/4)
2025 1月	AIアクションサミット, フランス		
2月	AISI国際ネットワーク会合, 仏		• AI制度研究会・中間とりまとめの公表(2/4)
3月		• AIセーフティに関する活動マップの公表(2/7)	
4月		• データ品質マネジメントガイドブック(ドラフト版)の公表(2/7)	• AI事業者ガイドライン1.1版の公表(3/28)
5月		• 年次レポートの公表(2/5)	
6月		• セキュリティ攻撃の俯瞰図の公表(3/26) • AIセーフティの普及に向けた文書の公表(3/26) • 評価観点ガイド1.10版の公表(3/28)	
7月	AISI国際ネットワーク会合, 加	• レッドチーミング手法ガイド1.10版の公表(3/31) • データ品質マネジメントガイドブックの公表(3/31)	• AI法公布(6/4) • 統合イノベーション戦略2025の公表(6/6)
8月		• AISI事業実証ワーキンググループを設置(6/13)	
9月			• AI法施行(9/1)
10月		• セキュリティ攻撃に対するレポート(7/9) • 多言語共同テストレポートの公表(7/18)	• AI戦略本部設置(9/12) • AI戦略専門調査会設置（9/19） • AI基本計画の骨子（たたき台）公表(9/19)
11月			
12月	AISI国際ネットワーク会合, 米	• AIセーフティ評価ツールの公開(9/12) • 米Anthropic社とMOCを締結(10/29)	
2026	Hiroshima Global Forum for Trustworthy AI, 日本	• AIインシデントレスポンス・アプローチブックの公開(1/9)	• AI基本計画を閣議決定(12/23)

マンスリーレポート

2.2 偽・誤情報の脅威の動向

偽情報を中心とした悪意ある情報操作は近年の安全保障上の問題となっている



■図 2-2-1　欧州評議会による情報騒乱(INFORMATION DISORDER)の分類

(出典)Claire Wardle, Hossein Derakhshan「INFORMATION DISORDER : Toward an interdisciplinary framework for research and policy making[※153]」を基に IPA が作成

© Council of Europe, reproduced with permission (from p5 Council of Europe report DGI(2017)09 Information disorder: Towards an interdisciplinary framework for research and policy making)

攻撃類型	攻撃の内容
①情報窃取型	標的型攻撃（マルウェア付きメール、水飲み場攻撃）等により、特定の政府機関、企業、団体、個人のネットワーク、コンピューターに侵入し、機密情報、営業情報、特許、知的財産等を窃取する攻撃。
②機能妨害型	DDoS 攻撃等の手法により、ネットワークの許容量を超える飽和通信要求によって、サーバー、ネットワークを麻痺させる攻撃。
③機能破壊型	標的型攻撃等により、特定の政府機関、企業、団体、個人のネットワークに侵入し、システム破壊・改ざんを行う攻撃。ネットワーク内のデータ消去・改ざんを目的とするものと、制御系システムを標的として物理的破壊を目的とするものがある。
④金銭目的型	標的型攻撃、脆弱性の悪用等により、特定の政府機関、銀行、企業、個人のネットワークに侵入し、不正な送金を行う、またはコンピューター内のデータを暗号化し、解読に身代金を要求する攻撃。
⑤情報操作型	代理主体(Proxy)等を用いて真の発信者を隠匿した上で、SNS 等に偽ニュースを流布させることにより、対象国(主に民主主義国)における世論操作を目的とした攻撃。選挙結果に影響を与えることを企図している攻撃も見られる。
⑥軍事的サイバー攻撃	軍事攻撃と一体的に行われる機能妨害・機能破壊を目的とした攻撃。電子戦の一環として軍隊の指揮統制(C4I)システムを標的とするものと、軍事行動に影響を与える重要インフラを標的としたものがある。
⑦ハイブリッド型	上記①～⑥までの類型を組み合わせた攻撃。近年は①情報窃取型＋⑤情報操作型、②機能妨害型＋⑤情報操作型等の組み合わせが多い。

■**表2-2-1　国家が関与するサイバー攻撃の類型**
(出典)大澤淳「サイバー領域の安全保障政策の方向性」を基にIPAが加筆・編集

■状況のまとめ

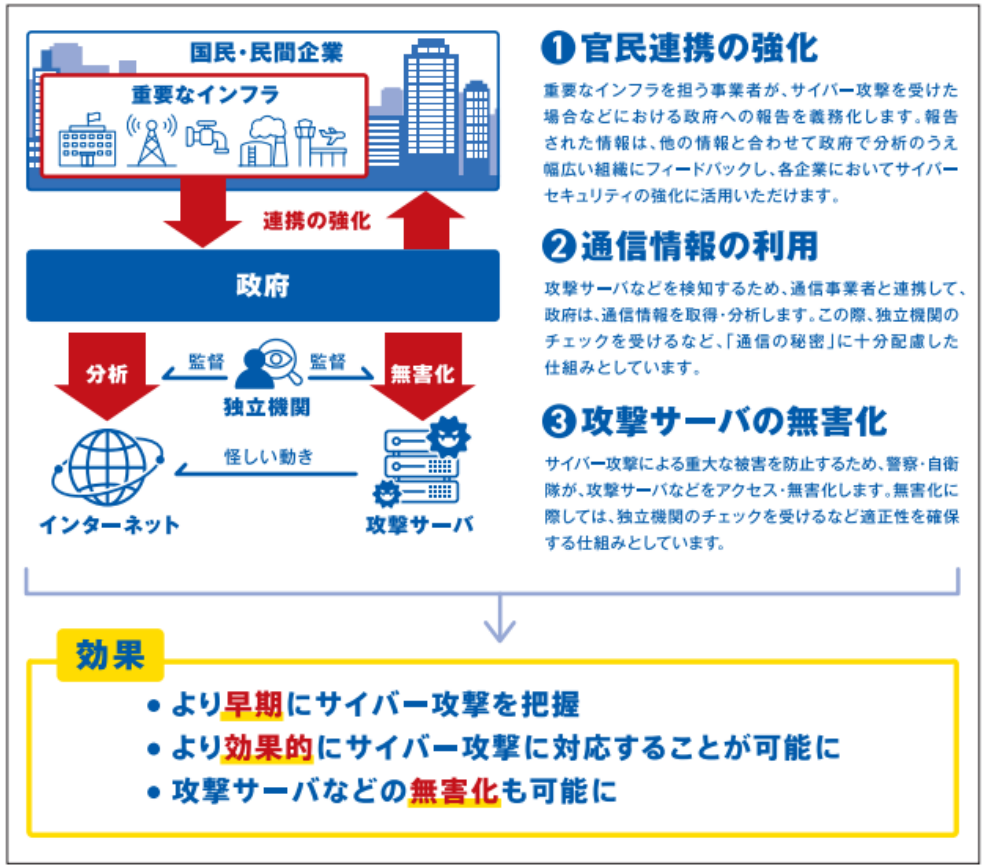
・生成AIが偽・誤情報拡散を加速・巧妙化させている。ユーザが容易に生成AIでフェイク画像・音声・動画を作成できるようになり、ディープフェイクによる混乱が顕在化した。

・旧来のナラティブが延命し続けている。陰謀論や反権威的なナラティブが一度否定されても形を変えて生き残り、別の文脈で再利用されている。安全保障上の懸念国が戦略的なナラティブを拡散することで、自国に有利な認知形成を目指す認知戦の広がりが背景にある。

情報セキュリティ白書2025(3章目次)

第3章　国内の政策及び取り組みの動向

3.1.1政府全体の政策動向



■図 3-1-1　能動的サイバー防御のポイント
（出典）内閣官房「みんなで備えよう。 新・サイバー防御、 はじまる。[※11]」

政府は、サイバー安全保障に関する取り組みとして、**能動的サイバー防御**の実現に向けた検討を進めてきた。

そして2025年5月23日**サイバー対処能力強化法及び整備法が公布**された。

2025年7月には、内閣サイバーセキュリティセンターを改組し、内閣官房に**「国家サイバー統括室（NCO）」が設置**

1年6か月以内に施行される。
（サイバー通信情報監理委員会の設置1年以内
通信情報の利用2年6ヵ月以内）

3.3.1 セキュリティ要件適合評価及びラベリング制度（JC-STAR）

- 本年3月より、IoT製品に対するセキュリティ要件（適合基準）への適合性を自己適合宣言又は客観的評価に基づき可視化するラベリング制度の運用を開始（★１）。
  ※★２～★４については、来年度での運用に向けて、現在検討中。

これからは
「JC-STAR 適合ラベル」で
安心を確かめよう

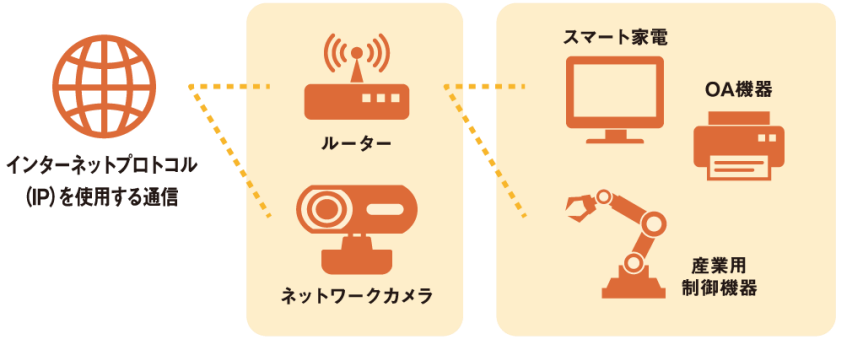
きちんとセキュリティ対策された製品を選びやすく！

適合ラベルの有効期間内は、セキュリティ対策向上のための更新プログラム提供などのサポートが約束され、安心して使い続けることができます。

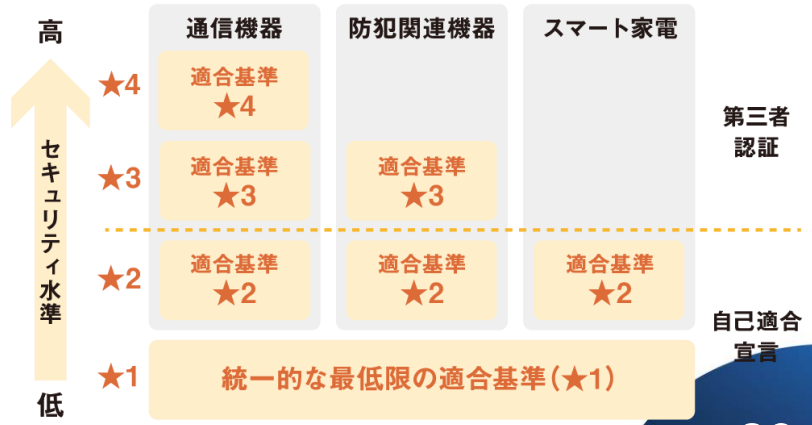
購入者もベンダーも、安全なIoT製品を！

IoT機器を狙ったサイバー攻撃が増加し、多くのIoT機器が乗っ取られて、社会システムを停止させるような被害が現実化している今。IoT製品を使うすべての人・企業・組織は、「被害者」だけでなく、知らないうちに「加害者」になることも！ 利用者や社会全体を守るためには、安全なIoT製品の提供・利用が欠かせないのです。
経済産業省とIPAは、適切なセキュリティ対策を施したIoT製品の普及を目指し、適合ラベルが付与された製品の購入を促進しています。JC-STARのラベル取得は、ベンダー様・販売会社様にとって、IoT製品の購入者から選ばれるための重要な取り組みとなるのです！

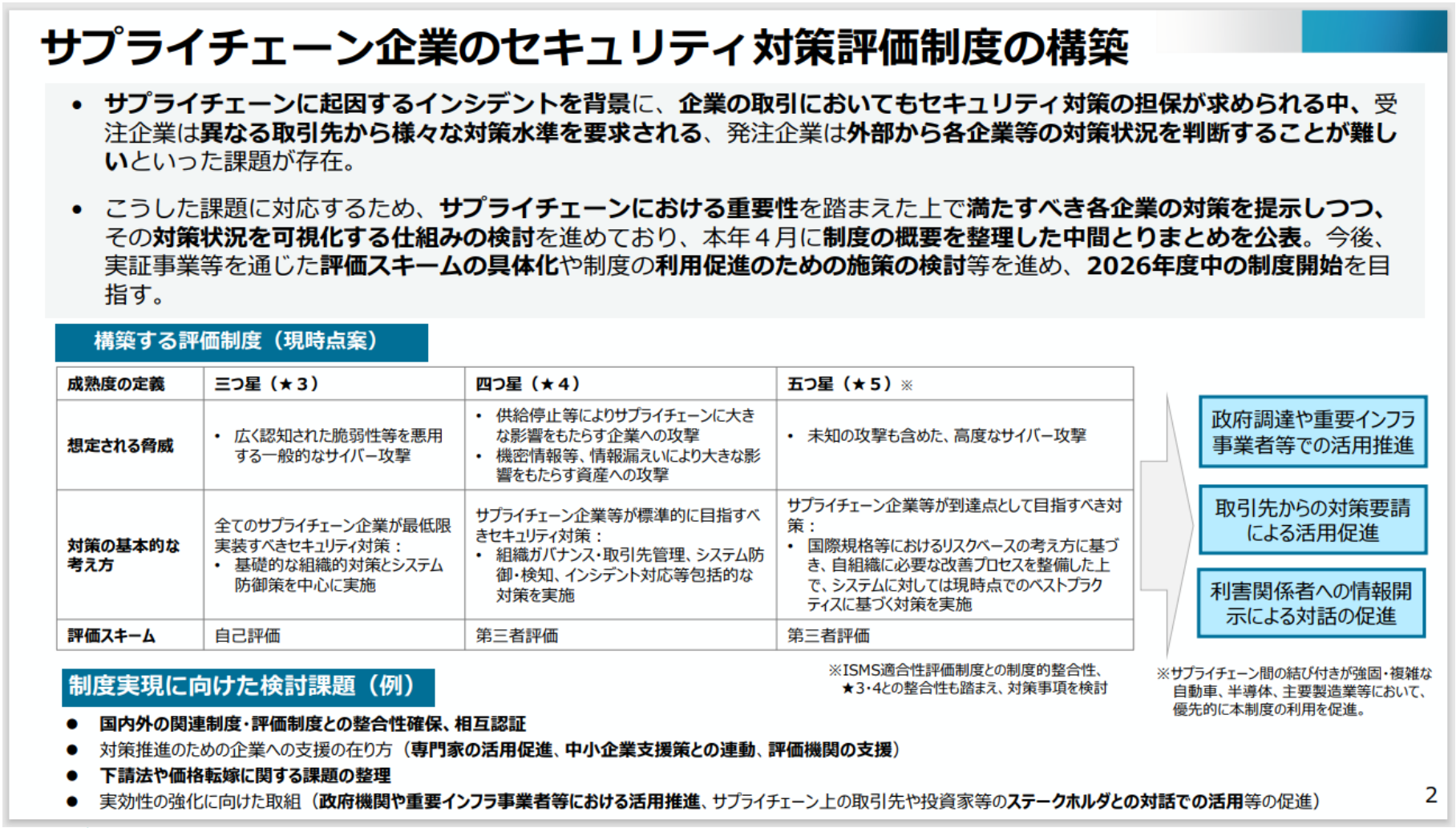
JC-STAR対象製品（例）



製品カテゴリごとの適合基準



3.3.3 サプライチェーン強化に向けた対策評価制度に向けた検討 ～検討中のサプライチェーン企業評価制度～



サプライチェーン企業のセキュリティ対策評価制度の構築

- **サプライチェーンに起因するインシデントを背景**に、**企業の取引においてもセキュリティ対策の担保が求められる中**、受注企業は**異なる取引先から様々な対策水準を要求される**、発注企業は**外部から各企業等の対策状況を判断することが難しい**といった課題が存在。
- こうした課題に対応するため、**サプライチェーンにおける重要性**を踏まえた上で**満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組みの検討**を進めており、本年４月に**制度の概要を整理した中間とりまとめを公表**。今後、実証事業等を通じた**評価スキームの具体化**や制度の**利用促進のための施策の検討**等を進め、**2026年度中の制度開始**を目指す。

構築する評価制度（現時点案）

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★５）※
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が標準的に目指すべきセキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施
評価スキーム	自己評価	第三者評価	第三者評価

※ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

※サプライチェーン間の結び付きが強固・複雑な自動車、半導体、主要製造業等において、優先的に本制度の利用を促進。

制度実現に向けた検討課題（例）

- **国内外の関連制度・評価制度との整合性確保、相互認証**
- 対策推進のための企業への支援の在り方（**専門家の活用促進、中小企業支援策との連動、評価機関の支援**）
- **下請法や価格転嫁に関する課題の整理**
- 実効性の強化に向けた取組（**政府機関や重要インフラ事業者等における活用推進**、サプライチェーン上の取引先や投資家等の**ステークホルダとの対話での活用**等の促進）

2

自己評価の仕組みである「SECURITY ACTION」（一つ星及び二つ星）、「JAMA・JAPIA自工会/部工会サイバーセキュリティガイドライン」や国際標準である「ISMS適合性評価制度」等とは相互補完的な制度として発展することを目指す。

2026年度中
制度開始予定

サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（概要）
https://www.meti.go.jp/press/2025/04/20250414002/20250414002-1.pdf

情報セキュリティ白書2025(4章目次)

第4章　国際的な政策及び取り組みの動向

4.1　国際的なサイバーセキュリティ政策の状況

- 国際社会の概況は、2022年からの**ウクライナ戦争**の長期化に加え、2023年には**イスラエル・パレスチナの紛争**が勃発した。これらの戦いは**武力戦に加え、情報戦、認知戦**などサイバー空間にも及んでおり、当時国間だけでなくで周辺国や支援する国々にも**緊張の高まり**が継続している。
- 2024年は加えて**パリオリンピック・パラリンピック競技大会**という大きなイベントや世界各地で重要な**選挙**が実施された。これらの出来事に関連し、大会の**妨害を意図した攻撃**や、AI等を悪用した偽情報の拡散といった**影響工作**が見られた。

米国の政策

政権交代や国際情勢変化により大きな動きを見せている。バイデン政権下で強化されてきた重要インフラの防御強化や多層防御モデルの促進は継承される一方、組織再編や予算配分の見直しが進められている。トランプ政権では民間企業との連携強化が重視され、サプライチェーンセキュリティやクラウドセキュリティへの注力が継続している。

欧州の政策

欧州各国でも複数の選挙が実施され、一部では政権交代がサイバー政策の展開に影響した。EUレベルでは引き続き法制度の整備が重視され、NIS2指令の施行やCRA・DORAといった新規制の実施が進んだ。欧州全体としては「デジタル主権」や「サイバーレジリエンス」の強化に向けて一貫した方向性を維持している。

参考情報/資料紹介

中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドライン(IPA)
https://www.ipa.go.jp/security/guide/sme/about.html

- 情報セキュリティ対策の必要性、情報を安全に管理する具体的な手順等を分かりやすい言葉で示したガイドライン
- 各種付録も充実

→・情報セキュリティ5か条
・情報セキュリティ基本方針（サンプル）
・5分でできる！情報セキュリティ自社診断
・情報セキュリティハンドブック（ひな形）
・情報セキュリティ関連規程（サンプル）
・中小企業のためのクラウドサービス安全利用の手引き
・リスク分析シート
・中小企業のためのセキュリティインシデント対応手引き

組織における内部不正防止ガイドライン

組織における内部不正防止ガイドライン(IPA)
https://www.ipa.go.jp/security/guide/insider.html (IPA)

- 内部不正防止の重要性や対策の体制、関連する法律などの概要を**易しい文章で説明**
- 「基本方針」「資産管理」「技術的管理」「職場環境」「事後対策」等の10の観点のもと、合計33項目からなる**具体的な対策**
- 自組織の内部不正**対策の状況を把握するためのチェックシート**

IPA サイバーセキュリティ相談窓口（企業組織向け）

◆IPAでは企業組織向けに、セキュリティに関する総合的な相談窓口を設けています。

◆セキュリティインシデント等が発生した際などにご活用ください。

受付可能な相談内容	
各種インシデント発生時の初動対応に関する相談	• 起きている事象をヒアリングして、被害が発生しているか否かを判断します • 被害が発生している場合、有効な応急処置についてご案内します • インシデント対応を行う専門業者一覧の紹介をします • 他に必要な相談・報告先等の紹介をします
標的型サイバー攻撃に関するインシデント相談	• 国家支援型と推定される標的型サイバー攻撃（APT）を受けた場合は、専門的知見をもとに支援を実施します
その他の情報セキュリティに関する一般的な相談	• 中小企業などにおける、情報セキュリティ対策ガイドラインや各種支援ツール・支援施策などをご案内します
脅威情報に関する情報提供	• IPAによる被害拡大防止策の実施や注意喚起のために、標的型サイバー攻撃や、その他の脅威情報に関して情報提供を受付けています。

メール　cs-support@ipa.go.jp

ウェブサイト　https://www.ipa.go.jp/security/support/soudan.html

情報セキュリティ10大脅威

情報セキュリティ10大脅威 2025
https://www.ipa.go.jp/security/10threats/10threats2025.html

☆情報セキュリティ10大脅威 2025
簡易説明資料

組織編

- 解説書［組織編］
- 簡易説明資料［組織編］
- 情報セキュリティ10大脅威の活用法［組織編］

個人編

- 解説書［個人編］
- 個人編ハンドブック
- 情報セキュリティ10大脅威 対策マッピングシート

共通資料

- セキュリティ対策の基本と共通対策
- 知っておきたい用語や仕組み

情報セキュリティ10大脅威 2026
https://www.ipa.go.jp/security/10threats/10threats2026.html

1月29日ランキング発表。解説書、簡易説明資料も現在準備中！！