第389回　NRIメディアフォーラム

セキュリティロードマップ
～2030年に向けたランドスケープ～

NRIセキュアテクノロジーズ株式会社
マネジメントコンサルティング事業本部
リスクマネジメントコンサルティング部

シニアセキュリティコンサルタント	木村　匠
エキスパートセキュリティコンサルタント	入澤　康紀
シニアセキュリティコンサルタント	石井　優斗
アソシエイトセキュリティコンサルタント	市村　海璃
セキュリティコンサルタント	仁尾　紗智乃

2025年3月24日

NRIセキュアテクノロジーズ
NRI SecureTechnologies

Envision the value,
Empower the change

目次

はじめに

「セキュリティロードマップ」とは

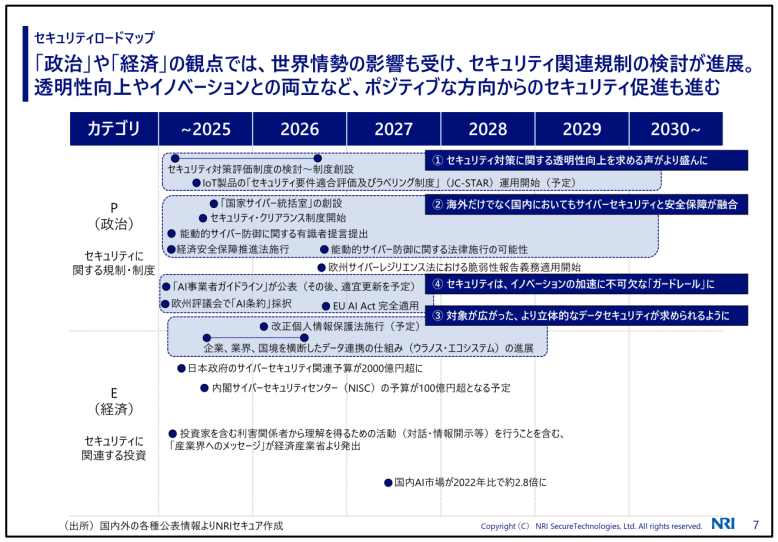
セキュリティに関連する社会環境、デジタル技術に関する2030年までの見通しから導出されるトレンドを捉え、重視すべき課題や打ち手の方針が概観できるもの

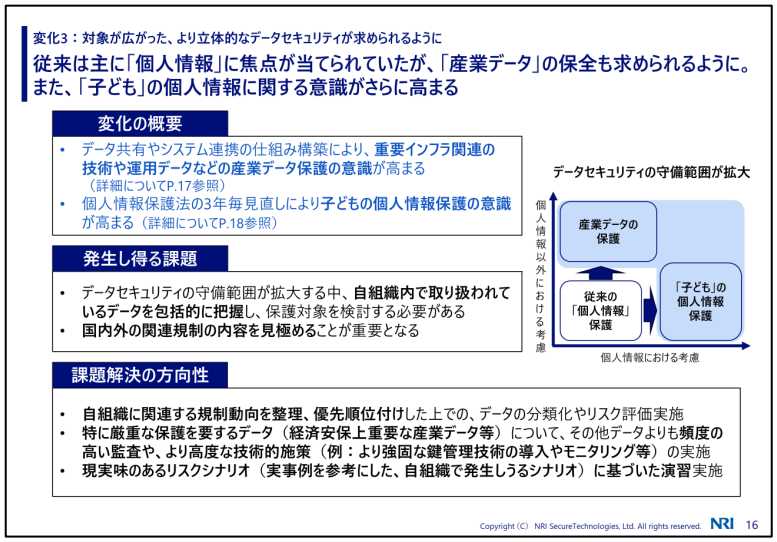
背景・目的

- セキュリティ対策を検討する上で、将来起こりうる脅威への備えは重要である一方、未来のセキュリティトレンドの変化を踏まえた政策や対策を立案するのは容易ではない
- 将来を見越したセキュリティ政策立案や各組織における計画検討のインプットとなるよう、2030年までに発生する可能性のある事象をもとに今後の変化を洞察

ロードマップの内容

- 政策動向や今後発生が見込まれる各種イベントなど、セキュリティに関連する事象を調査し、年表形式で整理
- 整理した各事象を踏まえ、セキュリティを取り巻く動向として、起こりうる変化を考察し、重視すべき課題や打ち手の概要を提示（2025年3月上旬現在の公表情報に基づく）





「セキュリティロードマップ」のサマリ

現在から2030年にかけて現れると予想される、セキュリティに関する動向の変化を洞察

「セキュリティロードマップ」で取り上げる6つの変化

① セキュリティ対策に関する透明性向上を求める声がより盛んに

顧客や社会との信頼を構築しながら守る

② 海外だけでなく国内においてもサイバーセキュリティと安全保障が融合

国際情勢が激化する中、官民連携で守る

③ 対象が広がった、より立体的なデータセキュリティが求められるように

個人から産業まで、あらゆるデータを守る

④ セキュリティは、イノベーションの加速に不可欠な「ガードレール」に

便利で革新的な社会のために守る

⑤ フロンティア領域（宇宙・海洋）へのデジタル技術の積極導入によりサイバー脅威が増加

未知の世界を開拓するために守る

⑥ セキュリティに関する社会技術的（socio-technical）アプローチが普及

技術と社会を総合的に捉えて守る

セキュリティロードマップの全体像

4つのセキュリティ事象カテゴリの説明

セキュリティに関連する事象を、「政治（P）」・「経済（E）」・「社会（S）」・「技術（T）」の4カテゴリで分類

カテゴリ		分類される事象
P：政治	**セキュリティに関する規制・制度**	• セキュリティに関する制度・規制の創出や変更
E：経済	**セキュリティに関連する投資**	• セキュリティ産業全体や個別企業への投資 • 具体的なセキュリティ対策実装のための投資
S：社会	**セキュリティを取り巻く社会の認識やイベント**	• セキュリティ対策に関する意識・認知の醸成 • セキュリティに関連し得る各種イベント
T：技術	**セキュリティを促進する/保護の対象となる技術**	• セキュリティを強化する技術の開発 • セキュリティ対策による保護の対象となる技術の開発

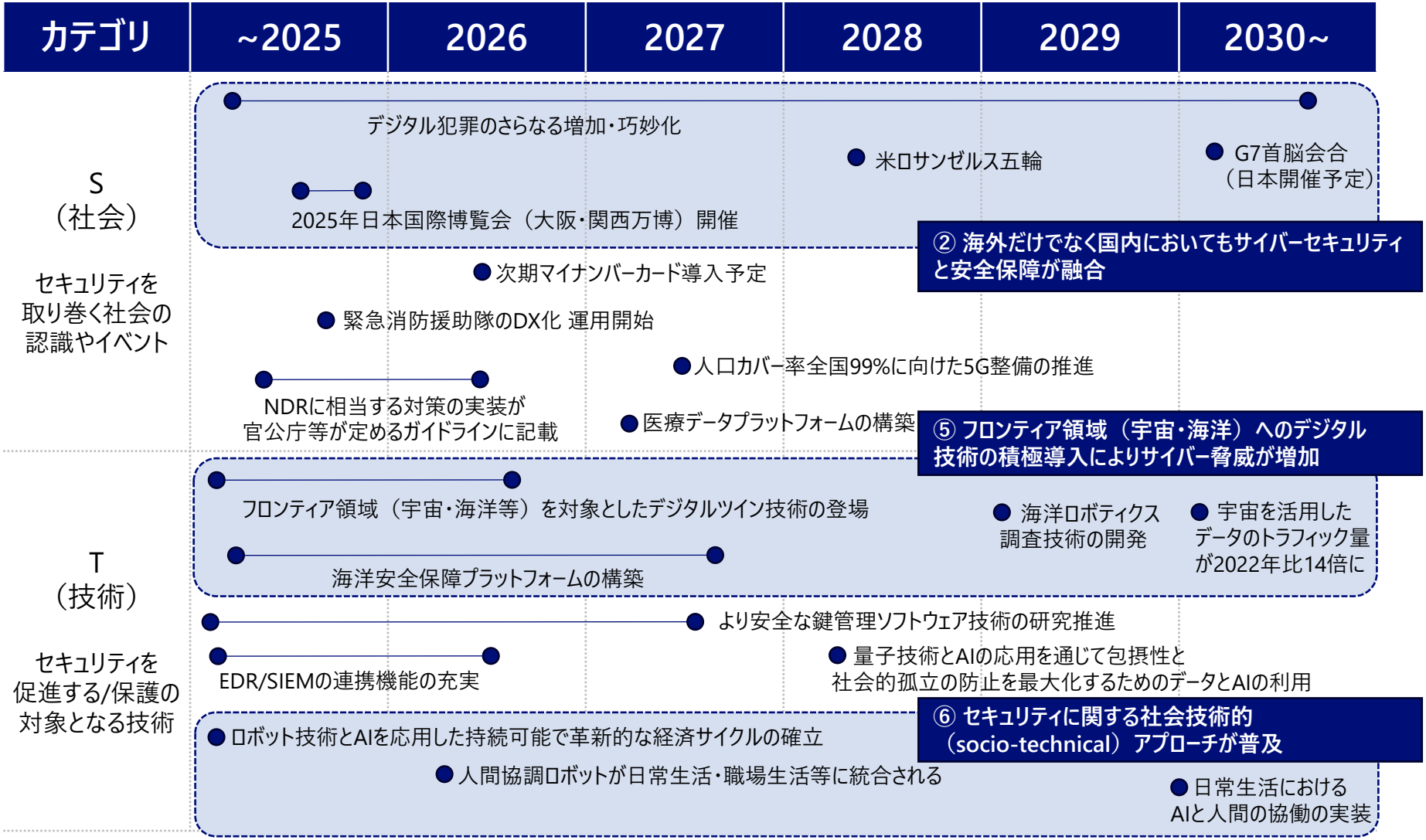
セキュリティロードマップ

「政治」や「経済」の観点では、世界情勢の影響も受け、セキュリティ関連規制の検討が進展。透明性向上やイノベーションとの両立など、ポジティブな方向からのセキュリティ促進も進む

（出所）国内外の各種公表情報よりNRIセキュア作成

セキュリティロードマップ

「社会」や「技術」の観点では、安全保障の観点が意識されつつ、新たな視点でセキュリティを捉えるアプローチの普及も期待される



（出所）国内外の各種公表情報よりNRIセキュア作成

2030年に向けて起こりうる変化

変化1：セキュリティ対策に関する透明性向上を求める声がより盛んに

サプライチェーン強化に向けた組織のセキュリティ対策状況を対外的に開示する流れが加速。国内では関連するセキュリティ対策評価制度が数年以内に運用開始予定

変化の概要

- サプライチェーンでのインシデント増加や、セキュア・バイ・デザインの意識の高まりから、**セキュリティ対策の有効性を社会に示す風潮**が強まる
- **国内ではセキュリティ対策の評価制度が数年以内に運用開始される**見込みで、IoT製品に関しては2025年3月に開始予定
  （詳細についてP.11参照）

発生し得る課題

- 利用環境に則したセキュリティ水準を有する製品の選定が必要
- 自組織から**委託先等への発注の際にも、一定以上のセキュリティ水準を有する組織を選定する責任が生じる可能性**に留意が必要

日本で運用開始が予定されている「セキュリティ対策評価制度」の検討内容

三つ星：★3	四つ星：★4	五つ星：★5
広く認知された脆弱性等を悪用する攻撃	供給停止や情報漏えいで大きな影響をもたらす攻撃	未知の攻撃も含めた高度なサイバー攻撃
全てのサプライチェーン企業が実装すべき組織的対策とシステム防御策が中心	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	リスクベースのアプローチに基づく改善プロセスを整備した上で、リスクに応じて必要な対策
自己評価	**第三者評価**	**第三者評価**

（出所）経済産業省「産業サイバーセキュリティ研究会WG1」2024年12月研究会資料よりNRIセキュア作成
（上段:想定脅威/中段:対策の基本的な考え方/下段:評価スキーム）

課題解決の方向性

- サプライチェーンの範囲が広範な場合、事業リスクを踏まえた優先順位付けを行い、段階的な対応を行う
- 組織的観点の評価については、情報セキュリティベンチマーク（IPA）等の**ツールによる評価も有効**
- 「セキュリティ対策評価制度」の開始に向け、現時点でベンチマークとして想定されている国内外のガイドラインや基準を参考にし、求められる水準を把握することが望ましい

変化1：セキュリティ対策に関する透明性向上を求める声がより盛んに

国内ではこれまでもセキュリティ関連の認証制度等が検討されてきた。直近では、エントリレベルから高度な攻撃への対策を含めた、幅広い対策水準を整備した制度が成立する見込み

■ セキュリティ対策透明性向上に資する国内施策例

年度	制度	動向概要
2013年	CSMS適合性評価制度の創設	IEC624432-1に基づき「CSMS適合性評価制度」として制御システムアセットオーナ等のマネジメントシステムを認証する制度を開始
2013年	EDSA認証制度の創設	同年、IEC62443-4に関連する米ISCI制度との相互承認する形で製品認証制度としてEDSA認証制度(現CSA認証)を開始
2019年以降	記述情報開示に関する原則	企業情報開示に関する原則が発行。有価証券報告書等で開示することが好事例とされた
2025年3月（予定）	セキュリティ要件適合評価及びラベリング制度	2024年8月に公表された「IoT製品に対するセキュリティ適合性評価制度構築方針」に基づき構築された制度。製品種別毎の適合基準に基づき、IoT製品に対する適合性を可視化
2026年以降（見込）	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	取引先等へのサイバー攻撃を起因としたリスクに対するセキュリティ対策の成熟度を評価する制度として検討中。今後具体的なスキーム検討が進む方向

先行する既存制度と相互補完的な関係性を有する制度として創設される見込み。認証のみならず自己適合宣言も含む、**共通の物差しを用いたセキュリティ対策の度合いを対外発信できる評価スキーム**の構築が進行中

（出所）経済産業省「産業サイバーセキュリティ研究会」研究会資料、経営情報学会「ISMS認証制度の課題とその対応」、電子商取引推進協議会「情報セキュリティ対策マネジメント標準」、IPA「制御システムセキュリティへの対応」及びその他各種公表資料よりNRIセキュア作成

変化2：海外だけでなく国内においても、サイバーセキュリティと安全保障が融合

欧米や近隣アジア地域に続き、日本でもサイバーセキュリティと伝統的な「安全保障」が一体として捉えられるように。そのため、政府による官民連携施策がより具体化していく

変化の概要

- 国際情勢の激化も影響し、**海外では既にサイバーセキュリティと安全保障を一体として捉える見方**が主流になりつつある（詳細についてP.13参照）
- 日本でも、**経済安全保障推進法やセキュリティ・クリアランス（SC）制度、能動的サイバー防御の検討**等をきっかけにこのような見方が進展。**NISCも機能を強化**（詳細についてP.14参照）
- **政府が主導する官民連携の取り組みが具体化し、情報共有等への積極的な協力が求められるように**

発生し得る課題

- インシデント発生時、**監督省庁等へのよりスピーディな情報共有**が求められる可能性がある
- 重要インフラや基幹インフラに加え、それ以外の提供サービスについても、**脅威アクターの動機や能力を注視**し脅威に備える必要がある

課題解決の方向性

- 各業界内での情報共有・連携の取り組み推進を図る組織であるISAC等への能動的な参画、外部の専門家との協働等によって、**実用的な脅威インテリジェンス**を自社内に蓄積し、活用する
- **SCを取得して官民連携施策に参画**する（ただし、**SC取得に要するコストと得られるメリットを考慮**する）
- **被害発生時の情報共有のあり方（提供するフォーマット、タイミング、各実施事項の担当組織）**について、経営層を含めて認識を合わせる。政府でも効率的な情報共有の検討が進んでいるため、動向を要注視

変化2：海外だけでなく国内においても、サイバーセキュリティと安全保障が融合

海外では社会活動に大きな影響を及ぼす、安全保障上の脅威となるサイバー攻撃が相次いで発生

- ここでの「安全保障」とは、国家や地域が直面する脅威から、社会の安定やその国/地域で暮らす人々の生活や権利を守ることを指す
- 特に海外では、**安全保障上の脅威となりうるサイバー攻撃の発生**がこれまでに多く報告されている

ウクライナ情勢に関連する脅威

- 2022年2月以降、**ウクライナの衛星通信や高圧変電所等を標的とした攻撃アクターの活動が観測**されていることが報告
- 侵入先の正規ツールを悪用する「現地調達型の攻撃」(living-off-the-land)による脅威が含まれることも報告

通信ネットワークに関する大規模な侵害

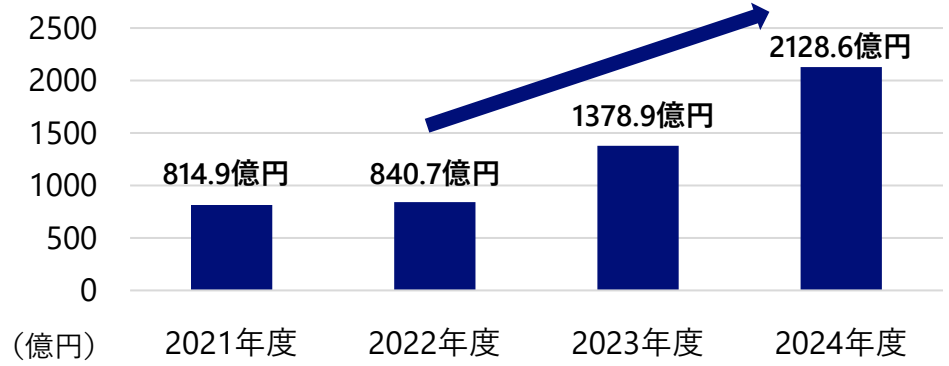
- 米国のサイバーセキュリティ・インフラセキュリティ庁（CISA）等は、**米国内の通信インフラを標的とした攻撃アクターの活動を観測**したと2024年11月に公表
- CISAは、米国のサイバーセキュリティに関する官民連携施策であるJCDC（Joint Cyber Defense Collaborative）も活用し、脅威ハンティングのチームが脅威の軽減に貢献したと公表

（出所）内閣官房「サイバー安全保障分野での対応能力の向上に向けた有識者会議 第1回 資料3」、米国CISA公表資料よりNRIセキュア作成

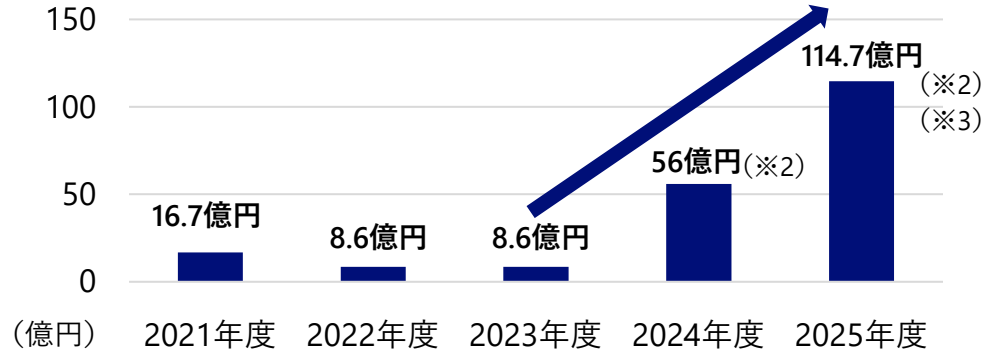
変化2：海外だけでなく国内においても、サイバーセキュリティと安全保障が融合

政府全体のセキュリティ予算やNISCの予算は大幅増加傾向。官民での情報共有体制の強化を始め、各種施策による能動的サイバー防御の実現が図られている

日本政府のサイバーセキュリティ予算（当初予算）（※1）



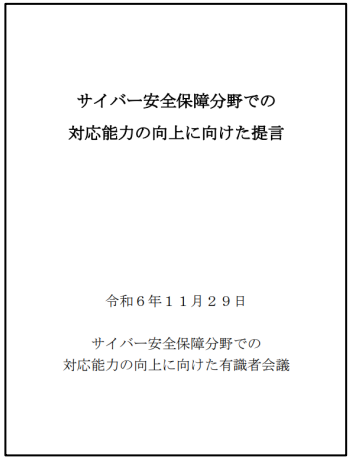
内閣サイバーセキュリティセンター（NISC）予算



（※1）2025年度当初予算要求金額における関連細目が不明のため、2024年度分までを記載。
（※2）2024年度予算及び2025年度予算案については、デジタル庁一括計上分を含む。
（※3）2025年度分については、2024年12月末時点での政府要求額。

（出所）サイバーセキュリティ戦略本部「政府のサイバーセキュリティに関する予算（第41回会合資料）」、内閣官房「予算」（令和3年度～令和7年度）よりNRIセキュア作成

日本政府における「サイバー安全保障」の取り組み


サイバー安全保障分野での
対応能力の向上に向けた提言

令和６年１１月２９日

サイバー安全保障分野での
対応能力の向上に向けた有識者会議

(1) **官民連携の強化**
官民双方向の情報共有の促進等

(2) **通信情報の利用**
一定の条件下での通信情報の利用検討

(3) **アクセス・無害化**
被害防止を目的としたアクセス・無害化を行う権限の検討

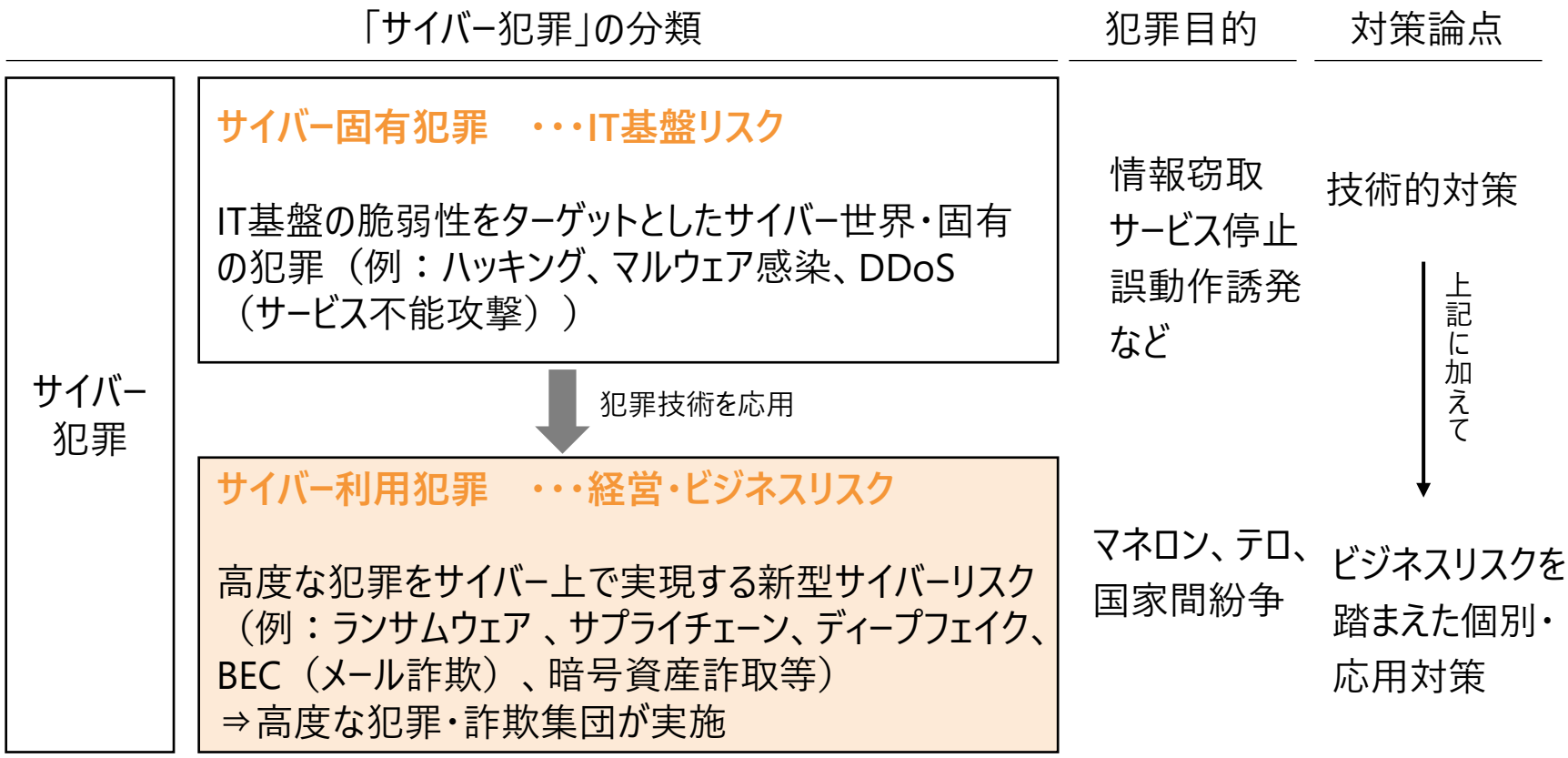
- 2025年通常国会において、いわゆる**「サイバー対処能力強化法案」が提出**されている
- 2025年には**「国家サイバー統括室」を新設**し、さらなる体制整備が図られる

（出所）内閣官房「サイバー安全保障分野での対応能力の向上に向けた有識者会議」、「令和7年度 機構・定員等審査結果（概要）」よりNRIセキュア作成

変化2：海外だけでなく国内においても、サイバーセキュリティと安全保障が融合

【参考】国連では、サイバー犯罪の進化を「サイバー固有犯罪」と「サイバー利用犯罪」の2つに分類。犯罪収益が大きい「サイバー利用犯罪」が近年急増

- 特に「サイバー利用犯罪」は国内の産業構造・商習慣に依存しており、各国/地域での規制強化対象
- これらの**サイバー犯罪の発生には、安全保障上の理由も関係**



（出所）United Nations Information Service Viennaや欧州議会の各種公表資料よりNRIセキュア作成

変化3：対象が広がった、より立体的なデータセキュリティが求められるように

従来は主に「個人情報」に焦点が当てられていたが、「産業データ」の保全も求められるように。また、「子ども」の個人情報に関する意識がさらに高まる

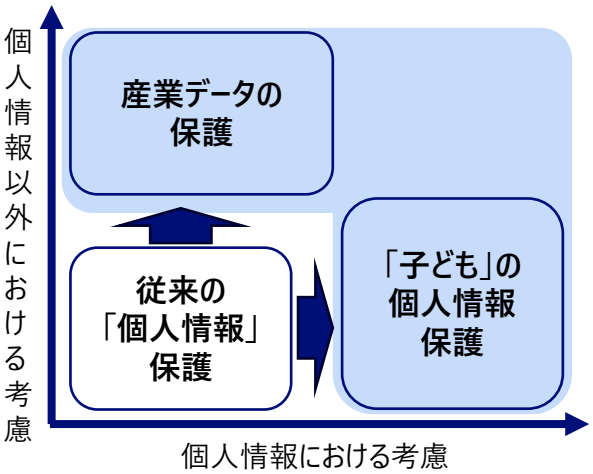
変化の概要

- データ共有やシステム連携の仕組み構築により、**重要インフラ関連の技術や運用データなどの産業データ保護の意識**が高まる（詳細についてP.17参照）
- 個人情報保護法の3年毎見直しにより**子どもの個人情報保護の意識**が高まる（詳細についてP.18参照）

発生し得る課題

- データセキュリティの守備範囲が拡大する中、**自組織内で取り扱われているデータを包括的に把握**し、保護対象を検討する必要がある
- **国内外の関連規制の内容を見極める**ことが重要となる

データセキュリティの守備範囲が拡大



課題解決の方向性

- **自組織に関連する規制動向を整理、優先順位付け**した上での、データの分類化やリスク評価実施
- **特に厳重な保護を要するデータ（経済安保上重要な産業データ等）**について、その他データよりも**頻度の高い監査や、より高度な技術的施策（例：より強固な鍵管理技術の導入やモニタリング等）**の実施
- **現実味のあるリスクシナリオ（実事例を参考にした、自組織で発生しうるシナリオ）に基づいた演習**実施

変化3：対象が広がった、より立体的なデータセキュリティが求められるように

個人情報に限らない「産業データ」の利活用事例が検討されており、活用されるデータの適切なマネジメント（例：意図せぬ知的財産流出の防止）について議論が進んでいる

産業データの種類の例と概要

データの性質		概要
安全保障に関連するデータ	**軍事関連データ**	武器や軍事転用可能な貨物・技術に関するデータ(例: 安全保障貿易管理の対象データ)
	重要インフラデータ	社会基盤を支える重要なインフラに関する技術や運用データ(例: 電力、交通、金融等)
	特定重要物資データ	特定重要物資(半導体や石油等) に関するサプライチェーン等のデータ
企業の競争力に影響するデータ	**営業秘密**	秘密として管理される非公知な情報(例: 設計図、製品作成ノウハウ等)
	限定提供データ	他社との共有を前提に一定条件下で利用可能な情報(例: 自動走行用地図データ等)
	知的財産権で保護されるデータ	創作性が認められるデータ(例: ソースコードやアルゴリズム等の著作物等)
	その他データ	上記のいずれにも該当しないが、企業の競争力に影響するデータ

各分野におけるデータ利活用検討例

（政府のデジタル行財政改革会議より）

分野	利活用の論点	メリット
医療	• 利用できる医療データの充実、電子カルテ等の共通化	• 個人はどの医療機関でも自らの診療情報を参照可 • 創薬の研究開発に活用
金融	• 各種決済データへのAPI連携の検証・検討	• 個人や中小企業が効率的に家計・会計の管理ができる

正の効果の最大化、
負の効果（情報漏洩リスク等）の抑止が必要

（出所）経済産業省「第1回 産業データサブワーキンググループ 資料3」、内閣官房「第8回 デジタル行財政改革会議 資料3」よりNRIセキュア作成

変化3：対象が広がった、より立体的なデータセキュリティが求められるように

「子ども」の個人情報を取り巻く脅威は特に長期的な被害を及ぼすことが指摘されている。国内外で規制の検討が進んでおり、日本でも規律のあり方について議論が続いている

■「子ども」の個人情報を取り巻く脅威は国内外で存在

海外での事例

米連邦取引委員会（FTC）は、**子どもの両親の明確な同意なしに子どもの個人情報を収集**したとして、米国のゲーム会社に**5億2000万ドルの制裁金**を科した。

国内での事例

大量の児童の個人データを保有及び管理しているにもかかわらず、コンプライアンス及びリスク管理に関する部署を設置していなかった等として、個人情報保護委員会が学習塾に指導を行った。

（出所） FTC公表資料、個人情報保護委員会公表資料よりNRIセキュア作成

有識者による指摘

「**子どもは何年も経ってからでないと被害に気づかないことが多い**ため、なりすましによって負う傷は深い。」

（出所）ダニエル・J・ソロブ、ウッドロウ・ハーツォグ著、小向太郎監訳『データセキュリティ法の迷走』勁草書房, 2023年, P.156

■ 様々な国/地域で、「子ども」の個人情報に関する規制検討が進んでいる

国内外における規制の状況

国/地域	規制あるいはその検討例
米国	• 子どものプライバシー設定を高いレベルに設定すること等を求めるカリフォルニア年齢適正デザインコード法が、2024年7月に施行
欧州	• GDPR（一般データ保護規則）前文38項で、子どもは個人データに関して特別の保護を享受すると規定
日本	• 現行の個人情報保護法上、子どもの個人情報の取扱い等に係る明文の規定は基本的にない • **個人情報保護法の3年毎見直しをきっかけに、子どもの個人情報保護に関する規律のあり方に着目**

（出所）カリフォルニア州政府、欧州委員会、個人情報保護委員会の各種公表資料よりNRIセキュア作成

変化4：セキュリティは、イノベーションの加速に不可欠な「ガードレール」に

イノベーションが安全に加速していくために欠かせないものとしてセキュリティが捉えられ、社会全体にとって「ちょうどよい」セキュリティ規制等を創出する機運が高まる

変化の概要

- 近年、AI等によるイノベーションを安心して加速させるための「ガードレール」としてセキュリティを含む各種のルールメイクが進行しつつある
  （詳細についてP.20～21参照）
- 様々な領域で**新技術の普及と調和する自由度の高い対策**を実施しやすくなり、**セキュリティをイノベーションと一体で検討するようになる**

発生し得る課題

- 特に先端的な技術領域に関するセキュリティ規制について、**遵守すべき原則が示された上で、詳細はリスクベースで各事業者が決定するとするルールが幅広い分野で増加する**
- これにより「**原則**」と「**実装**」**のギャップを埋めるための検討**が必要となる

セキュリティに関する規制等はイノベーションの加速と密接な関係に

従来

- チェックリスト的な規制（遵守の仕方に**自由度が少ない**）

これから

- 満たすべき原則が示されるが、詳細な遵守の仕方は**自由度が高く、事業者側での工夫の余地が大きい**
- 例えば、日本の「AI事業者ガイドライン」など

新技術に対して柔軟に対応可能。AIのみならず多様な分野でこのような「リスクベース」の考え方が進展

課題解決の方向性

- 既に従来のチェックリスト型の規制等への対応を整備済みである場合も含め、事業やステークホルダーへの影響を考慮した、**リスクベース型の規制等への対応ロードマップを策定**する
- 脅威分析やリスク分析を実施し、**段階的にリスクベース型の規制対応等へ移行**する

変化4：セキュリティは、イノベーションの加速に不可欠な「ガードレール」に

対応の自由度が低いベースラインアプローチから、対応すべきリスクを明示し必要な対策を事業者が検討するリスクベースアプローチへ、セキュリティ対応のあり方が変化している

	ベースラインアプローチ	リスクベースアプローチ
特徴	• 過去からの蓄積によって、ベストプラクティスが整備されている環境において効率的に不足部分を確認することができる	• 新しい環境、技術、サービスなどにおいて対策が確立されていないケースにおいて、リスクシナリオを想定し、必要な対策を整理することができる
メリット	• 効率的にベストプラクティスとの差分を洗い出せる • 一定の説明責任を果たすことができる • 品質の差異が比較的小さい	• **環境、機能、利用主体、取り扱い情報の質等に則した本質的な対策が選択可能**
デメリット	• **一律の要求を実施するのが不合理**となりうる • **技術や脅威の進化に伴って対策内容が陳腐化しやすい**	• 環境把握/リスク分析などに時間を要する • リスクシナリオ作成など、専門的な知見が必要であり、品質にバラツキがでやすい

医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（総務省・経済産業省）

リスクベースアプローチによるリスクマネジメントプロセスについて規定
「医療情報システム等の特性に応じた必要十分な対策を設計するために、**一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義**する」

（出所）総務省・経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」よりNRIセキュア作成

金融分野におけるサイバーセキュリティに関するガイドライン（金融庁）

金融機関へのサイバーセキュリティ管理態勢について、リスクベースアプローチを採用する旨を記載
「金融庁としては、引き続き、金融機関等の規模・特性に応じ、**リスクベース・アプローチで検査・モニタリングを実施し、その中で個別金融機関等のサイバーセキュリティ管理態勢を検証**していく」

（出所）金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」よりNRIセキュア作成

変化4：セキュリティは、イノベーションの加速に不可欠な「ガードレール」に

AIの領域では、イノベーションの加速という観点からリスクベースの考え方が浸透。今後は他技術領域でも同様の動きが起き得る

例：昨今のAI関連領域におけるリスク対応の考え方

文書	動向
AI戦略会議「AIに関する暫定的な論点整理」	• 生成AIに関する懸念やリスクへの適切な対処を「ガードレール」と表現 「**生成AIの開発・提供・利用を促進するためにも、生成AIに関する懸念やリスクへの適切な対処を行うべき**である。いわば、**「ガードレール」の設置が必要**となる」
AI制度研究会「中間取りまとめ(案)」	• イノベーションの促進とリスクへの対応の両立を要求 「AIの研究開発・実装がしやすい国を実現するため、**AIのイノベーションの促進とリスクへの対応を両立させることが重要**である」 • 各AI事業者へリスクベースによる評価・対応を要求 「AIシステムの安全性の評価について、リスクを理解するAIの開発者、提供者や利用者は、組織内外の専門家チームや評価用のツールなどを使って、**基本的には自らリスク評価を行い、対処していくべき**である」

（出所）内閣府「AIに関する暫定的な論点整理」「AI制度研究会「中間取りまとめ(案)」」よりNRIセキュア作成

■ 2025年2月28日閣議決定の「**人工知能関連技術の研究開発及び活用の推進に関する法律案**」（**AI法案**）においても、概要資料において「**イノベーション促進とリスク対応**」の両立を明記

➡ **イノベーションの後追いでリスクを考えるのではなく、両者を一体で考えることがより一般的に**

（出所）内閣府「人工知能関連技術の研究開発及び活用の推進に関する法律案（AI法案）概要」よりNRIセキュア作成

変化5：フロンティア領域（宇宙・海洋）へのデジタル技術の積極導入によりサイバー脅威が増加

宇宙・海洋等の人類にとってのフロンティア領域に、デジタルツイン技術(※)を始めとした技術導入が進む。一方で、これらの領域を狙うサイバー攻撃等により、甚大な被害発生の恐れも

（※）実在するものと同じ環境を仮想空間に再現し、あらゆる想定をシミュレーションできる技術

変化の概要

- **宇宙・海洋での観測活動等をシミュレーションするデジタルツインや、当該領域を対象にした制御システムの開発が進む可能性**がある
- これらがサイバー攻撃を受けた場合、**シミュレーションデータの改ざん、ミッション失敗、周辺環境への被害発生が見込まれ、多額の経済的損失**が想定される（詳細についてP.23～24参照）

発生し得る課題

- **通信インフラや製品の提供によりサプライチェーンに組み込まれる場合、上記リスクを考慮したセキュリティ対策の検討**が必要となる

課題解決の方向性

- **関連するサービスやシステムの企画段階からサプライチェーン全体を考慮した脅威分析**を行う
- 特に制御システムを狙った攻撃は甚大な経済的・社会的なリスクを招くため、**制御システム向けのセキュア開発プロセスを参考にした開発**を行う。これにより、手戻りが少なく効果的なセキュリティ対策が可能になる
- **宇宙の領域については既にセキュリティガイドライン策定の検討も進みつつあり**、関係するガイドラインの策定動向や脅威動向を注視するのが望ましい

フロンティア領域にも サイバー攻撃等の可能性

	考えられる脅威の例
宇宙	地上で運用される衛星通信システム等を対象にしたサイバー攻撃による、制御システム停止
海洋	海洋での資源生産/掘削に用いるシステムへのサイバー攻撃による、資源/シミュレーション情報の改ざん、漏えい

変化5：フロンティア領域（宇宙・海洋）へのデジタル技術の積極導入によりサイバー脅威が増加

宇宙産業の発展が進むにつれ、攻撃対象領域が拡大し、インシデント発生リスクが増大。その結果、セキュリティの重要性が認識され、今後もルール形成が進むことが予想される

宇宙産業の攻撃対象領域

宇宙産業のインシデント事例

時期	攻撃対象	出来事
2020年	衛星との通信データ	国際会議「Black Hat」において、市販の機材で、静止軌道上の通信衛星18機が暗号化なしで通信していることが明らかになった
2023年	設計書（アメリカ）	攻撃者グループ「LockBit」が、スペースX社の下請業者にランサムウェア攻撃を仕掛け、同社のロケット設計書約3,000点を窃取した
2023年-2024年	内部情報（日本）	宇宙航空研究開発機構（JAXA）は、2023年6月から2024年5月にかけて4回のサイバー攻撃を受け、内部情報が流出した

（出所）経済産業省「民間宇宙システムにおけるサイバーセキュリティ 対策ガイドライン Ver 2.0」、各種報道よりNRIセキュア作成

宇宙産業のセキュリティルール形成動向

時期	組織	出来事
2022年	経済産業省	「民間宇宙システムにおけるサイバーセキュリティ 対策ガイドライン Ver1.0」の公表
2024年	経済産業省	「民間宇宙システムにおけるサイバーセキュリティ 対策ガイドライン Ver2.0」の公表

変化5：フロンティア領域（宇宙・海洋）へのデジタル技術の積極導入によりサイバー脅威が増加

海洋産業のDX化が進むにつれ、攻撃対象領域が拡大し、インシデント発生リスクが増大。その結果、セキュリティの重要性が認識され、今後もルール形成が進むことが予想される

海洋産業の攻撃対象領域

海洋産業のインシデント事例

時期	攻撃対象	出来事
2023年	ターミナルシステム（日本）	名古屋港のコンテナターミナルで使用される統一ターミナルシステムがランサムウェアに感染し、コンテナの搬出入作業が一時停止する事態が発生した
2023年	港湾運営会社（オーストラリア）	オーストラリアの主要な港湾運営会社がハッキング攻撃を受け、運営する各港での操業が停止した
2024年	海底ケーブル（北大西洋）	北大西洋条約機構（NATO）は、欧州で相次ぐ海底ケーブル破損などの破壊工作を受け、対応を協議すると表明した

海洋産業のセキュリティルール形成動向

時期	組織	出来事
2023年	日本海事協会	「船上のシステム及び機器のサイバーレジリエンスに関するガイドライン」の公表
2024年	国土交通省	「港湾分野における情報セキュリティ確保に係る安全ガイドライン」の公表
2024年	日本海事協会	「船舶のサイバーレジリエンスに関するガイドライン」の公表

（出所）各種報道よりNRIセキュア作成

変化6：セキュリティに関する社会技術的（socio-technical）アプローチが普及

AI等の技術が日常生活に溶け込むことにより、セキュリティは単に技術的な問題ではなく社会技術的(※)なものになる。倫理・法・人間の認知/行動を技術と一体的に捉える重要性が増す

（※）社会技術的（socio-technical）とは、技術的要素と社会的要素を一体的に捉える考え方

変化の概要

- 人間に代わって高度なタスクを実行する**AIエージェント等が日常生活に溶け込んでいく**
- 単に技術的リスクだけではなく、**人間の心理の操作や偏見の助長を始めとする社会技術的リスク**についての対策が重要となる
  （詳細についてP.26～28参照）

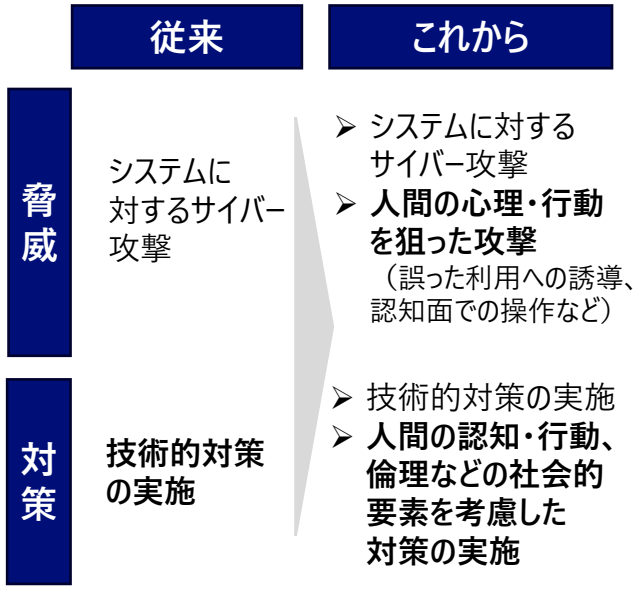
発生し得る課題

- **技術以外の社会的要素も含めた脅威分析**が重要となる
- ただし、**従来の技術的側面での分析を軽視するわけではなく、技術的要素と社会的要素を一体のものとして捉える**ことが重要視される

課題解決の方向性

- 社会的要素の考慮に際しては、**ミクロのレベル（サービスの利用者や悪意のある第三者の心理的背景や行動に着目）**と**マクロのレベル（倫理や社会的規律など社会一般に及ぼし得る影響に着目）**の双方への目配せを意識する
- **セキュリティに関する社会的要素に関連する分野（認知心理学、法学、倫理学、行動経済学等）の知見を有する専門家と協働**してセキュリティ対策を検討することを試みる

従来から脅威の範囲が拡大し、社会的要素も考慮した対応が重要に



変化6：セキュリティに関する社会技術的（socio-technical）アプローチが普及

日常に溶け込みながら発展するテクノロジーの中には、従来の「セキュリティ」の枠に留まらず、より広く技術的要素と社会的要素の双方を横断したリスクをもたらすものが多くある

日常に溶け込むテクノロジー	テクノロジーを取り巻く脅威		
	技術的観点の脅威例		社会的観点の脅威例
例1：SNS等のデジタルプラットフォーム	システムの脆弱性を突いたサイバー攻撃 システムやデバイスに不正アクセスし、**情報資産を盗難、改ざん、破壊等する**	互いに関連	**人間の認知バイアスを悪用した心理的操作** 金銭の支出、個人情報の開示を仕向ける**ダークパターン**（※1）**やフィッシングは、倫理的、法的、社会的課題として対応が求められる** （※1）ユーザーの意思決定や行動を意図的に操るウェブデザイン
例2：生成AIを用いたサービス	AIモデルやAIシステムの脆弱性を突いたサイバー攻撃 プロンプトインジェクション（※2）を用い、**システム制御や情報漏洩、不正操作を実行する** （※2）意図的に誤作動を起こさせるような指令入力を与え、提供側が出力を禁止している情報（開発に関する情報、犯罪に使われうる情報等）を生成させる攻撃手法	互いに関連	**偽・誤情報の流通および拡散** ディープフェイク等により**事実と異なる情報が拡散され、社会を混乱させるリスクが指摘** （例：2022年、ロシアのウクライナ侵攻後、ゼレンスキー大統領がウクライナ軍に降伏を呼びかけるフェイク動画がSNS上で拡散。）

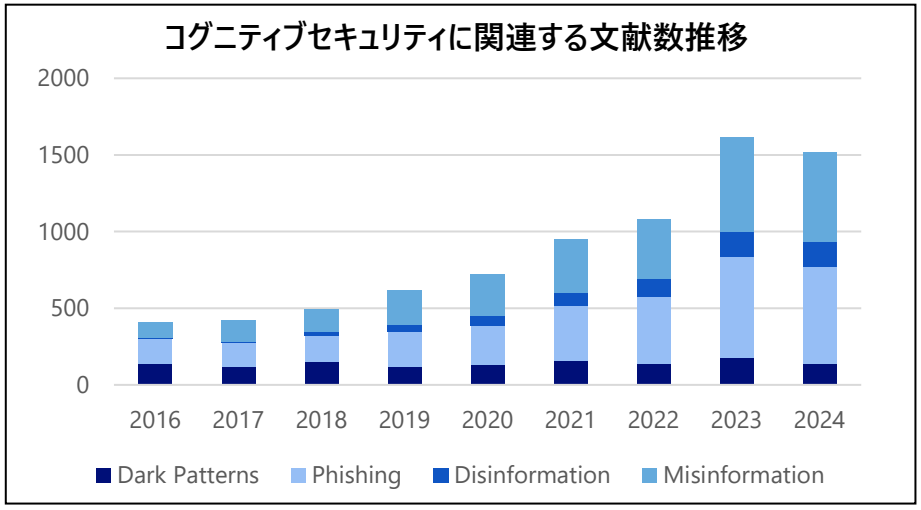
「技術的要素だけ」でもなければ「社会的要素だけ」でもない、双方を視野に入れた「**社会技術的アプローチ**」が求められる

変化6：セキュリティに関する社会技術的（socio-technical）アプローチが普及

人間の認知的な脆弱性を狙った脅威については、アカデミアでの研究が進んでいる。各国では関連する規制が強化されており、日本でも既存規制の見直しの兆しが見られる

コグニティブセキュリティ研究

- コグニティブセキュリティとは「コグニティブ（認知）」と「セキュリティ」を合わせた単語
- **人間の認知的脆弱性を悪用し、操作する情報攻撃から人や社会を守ることを指す**
- **コグニティブセキュリティに関する研究は近年増加傾向**にある



（出所） IEEE Xploreより、ダークパターン、フィッシング、偽・誤情報をキーワードに2016年~2024年までの文献数をNRIセキュアで検索・集計

関連する規制やその検討例

- 欧米を中心に、**各国ではダークパターンの規制が強化されている**
- 日本においても、**個人情報保護法の見直しに関する検討の過程で、ダークパターンに係る規律のあり方について言及**されている

欧米におけるダークパターン関連規制

国/地域	ダークパターンに係る法令	規制内容
EU	DSA（デジタルサービス法）	ダークパターンの設計、構成、運営を禁止とする
	GDPR（一般データ保護規則）	一部原則・義務においては違反となる可能性がある
米国	FTC法（連邦取引委員会法）	商業における不公正・欺瞞的な行為を禁止とする
	CCPA（カリフォルニア州消費者プライバシー法）	ダークパターンを用いて取得した同意を無効とする

（出所）DSA、GDPR、FTC、CCPAの各種公表資料よりNRIセキュア作成

変化6：セキュリティに関する社会技術的（socio-technical）アプローチが普及

特にAIに関する分野では、社会技術システムの一環としてAIシステムを捉えようとする取り組みが始まっている

国際社会における、社会技術的観点への意識

- 英国政府が発行している「International AI Safety Report 2025（国際AIセーフティ報告書2025）」では、**AIに関しての社会技術的な要素が指摘されている**

「国際AIセーフティ報告書2025」

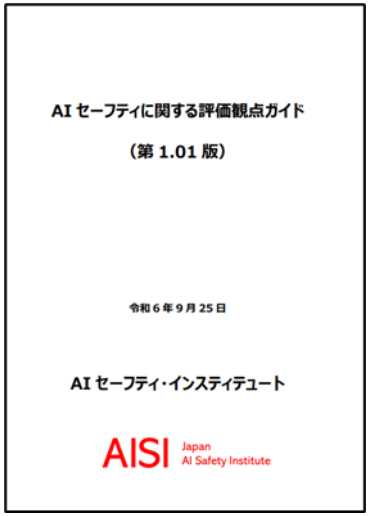
「（中略）システムは真空で運用されるわけではない。**安全性とパフォーマンスを維持するためには、システムを社会技術システムの中に組み込み、継続的にリスクを特定・分析し、防御する仕組みを構築することが重要**」

（出所）Department for Science, Innovation and Technology & UK AISI, “International AI Safety Report 2025”, 2025, P. 205
（翻訳及び太字強調はNRIセキュア）

日本における取り組み

- 2024年2月に設立されたAIセーフティ・インスティテュート（AISI）は、AIの安全性確保に取り組む海外機関と連携
- **2024年9月には、「AIセーフティ」の評価に関するガイドを公表。**今後も継続的に改訂を行っていくとしている

「AIセーフティに関する評価観点ガイド」


AI セーフティに関する評価観点ガイド
（第 1.01 版）
令和 6 年 9 月 25 日
AI セーフティ・インスティテュート
AISI Japan AI Safety Institute

「有害情報の出力制御」、「偽誤情報の出力・誘導の防止」等、社会技術的観点に関連しうる10個の評価観点を提示

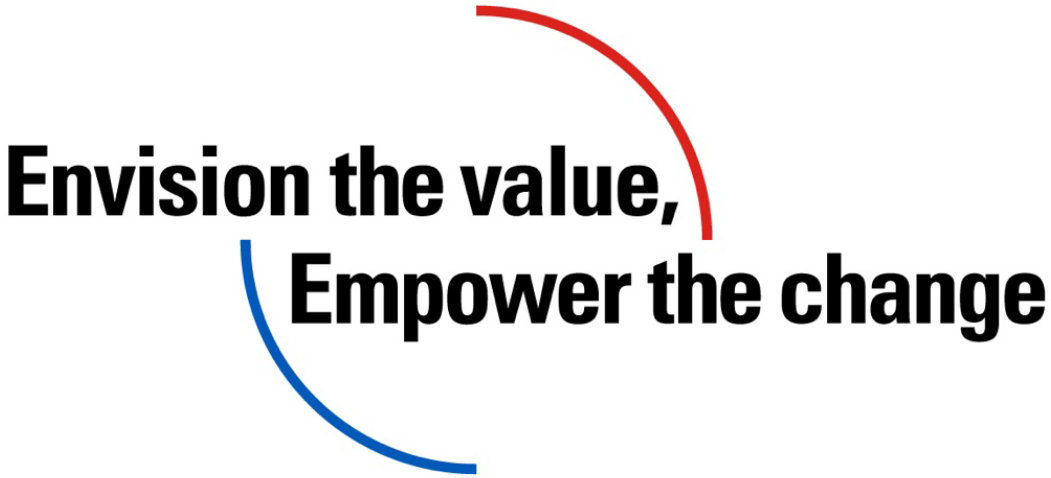
（出所）日本AISI「AIセーフティに関する評価観点ガイド（第1.01版）」よりNRIセキュア作成

セキュリティロードマップのまとめ

セキュリティロードマップのまとめ

本ロードマップで示した6つの変化に対応する上での課題、課題解決の方向性は以下の通り

「セキュリティロードマップ」で取り上げる6つの変化	変化に対応する上での課題例	課題解決の方向性
① セキュリティ対策に関する透明性向上を求める声がより盛んに	• 自組織から委託先等への発注の際にも、適正水準を有する組織を選定する責任が生じる可能性	• セキュリティ対策評価制度開始に向け、ガイドラインや基準を参考にし、求められる水準を把握する
② 海外だけでなく国内においてもサイバーセキュリティと安全保障が融合	• インシデント発生時、監督省庁等へのよりスピーディな情報共有が求められる可能性	• 被害発生時の情報共有のあり方について、経営層を含めて認識を合わせる
③ 対象が広がった、より立体的なデータセキュリティが求められるように	• 自組織内で取り扱われているデータを包括的に把握し、保護対象を検討する必要がある	• 自組織に関連する規制動向を整理、優先順位付けした上での、データの分類化やリスク評価実施
④ セキュリティは、イノベーションの加速に不可欠な「ガードレール」に	• リスクベースでの対応を進める際、「原則」と「実装」のギャップを埋めるための検討が必要となる	• 脅威分析やリスク分析を実施し、段階的にリスクベース型の規制対応等へ移行
⑤ フロンティア領域（宇宙・海洋）へのデジタル技術の積極導入によりサイバー脅威が増加	• サプライチェーンに組み込まれる場合、リスクを考慮したセキュリティ対策の検討が必要となる	• 関連するサービスやシステムの企画段階からサプライチェーン全体を考慮した脅威分析を行う
⑥ セキュリティに関する社会技術的（socio-technical）アプローチが普及	• 技術以外の社会的要素も含めた脅威分析が重要となる	• セキュリティに関する社会的要素に関連する分野の知見を有する専門家と協働して対策を検討


Envision the value,
Empower the change