NISC National center of Incident readiness and Strategy for Cybersecurity

サイバーセキュリティ2024の概要

令和6年7月10日
内閣サイバーセキュリティセンター

「サイバーセキュリティ2024(年次報告・年次計画)」概要（第１部エグゼクティブ・サマリー）

１．サイバー空間を巡る昨今の状況変化と情勢

－ 国家を背景とした攻撃の拡大、未知の脆弱性を悪用したゼロデイ攻撃の増大等、サイバー攻撃の洗練化・巧妙化が一層進展。生成AI等の新技術の普及に伴う新たなリスクも増大。

⇒ 政府機関・重要インフラ事業者、ユーザにサービスを提供するテクノロジー企業などの能力ある主体がより多くの役割・責任を果たすことが重要。サイバー安全保障の観点も含め、平素からの対策強化や対処能力の向上、セキュアバイデザイン・セキュアバイデフォルト原則に基づく措置の具体化、 欧米主要国をはじめとする関係国との協調・連携が必要に。

２．特に強力に取り組む施策（※）

（※）「令和7年度予算重点化方針（案）」でも、これらの施策に重点を置くこととしている。

✓ **欧米主要国並にサイバー安全保障分野での対応能力を向上させるため、能動的サイバー防御の実施に向けた法案を可能な限り早期に取りまとめる**とともに、以下の施策を特に強力に取り組んでいく。

(1) 国民が安心して暮らせるデジタル社会の実現 ～政府機関や重要インフラ等の対応能力の向上～

✓ 政府のサイバーセキュリティ体制の抜本的強化
- アタックサーフェスマネジメントによる脆弱性把握、プロテクティブDNSによる情報収集、CYXROSSの推進

✓ 重要インフラ演習の強化及び個別分野におけるレジリエンス向上
- 〔各分野・分野横断〕官民連携に重点を置いた新演習、〔医療〕病院の外部NWとの接続安全性検証・検査、〔行政〕改正地方自治法に基づく対策

✓ IPAの機能強化及びNICTの取組強化を通じたサイバーセキュリティ対策の底上げ
- 〔IPA〕AISIの創設、サイバー攻撃動向・地政学的情報の分析体制整備、〔NICT〕各分野に特化した新たな演習プログラムの開発

(2) 経済社会の活力の向上及び持続的発展 ～サプライチェーン・リスクへの対応強化とDXを推進・支援する取組の強化～

✓ セキュアバイデザイン・セキュアバイデフォルト原則を踏まえたIoT機器・ソフトウェア製品のサイバーセキュリティ対策強化
- ソフトウェア開発手法のガイドライン作成、SBOM活用推進、「IoT製品に対するセキュリティ適合性評価制度」整備、「NOTICE」調査対象機器拡大

✓ 中小企業のサイバーセキュリティ対策促進
- 「サイバーセキュリティお助け隊サービス」の新サービス類型を含めた普及・展開、中小企業とセキュリティ人材のマッチング及びシェアリングの促進

(3) 国際社会の平和・安定及び我が国の安全保障への寄与 ～欧米主要国をはじめとする関係国との連携の一層の強化～

✓ 海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進
- 多国間枠組み（G7等）又は二国間会談を通じた政策動向等の共有、共同文書等への署名参加、大洋州島しょ国を対象とした能力構築支援

✓ 警察におけるサイバー空間の安全・安心の確保に資する取組の推進
- 外国捜査当局との共同捜査への参加、国内外の多様な主体との連携強化、事案の情報収集・事案横断的な分析

[１] 政府のサイバーセキュリティ体制の抜本的強化

1. 背景及び課題

- サイバー攻撃の侵入起点となり得る**IT資産・サービスの急増**や、Living Off The Land攻撃の台頭等の**サイバー攻撃の手法の劇的な高度化に対応**するため、**政府機関全体におけるサイバーセキュリティ対策は**これまで以上に**戦略的に実行**していくことが強く求められる。
- 各PJMOの運用監視レベルのバラツキ、インシデント等発生時の迅速な情報共有等の課題に対応するため、デジタル庁の**運用監視のレベルを向上**させるとともに、**インシデントの予防・早期発見・早期復旧を実現**するため、デジタル庁システムを横断的に確認する**総合運用監視の枠組みの整備**に取り組む。
- 巧妙化かつ複雑化するサイバー攻撃や未知の脅威が増大する中で、**我が国特有の攻撃事例を十分に収集できていない。**また**国産の製品・サービスの開発に必要なノウハウや知見の蓄積が困難**に。そのため、**我が国独自にサイバーセキュリティに関する情報を収集・分析できる体制の構築**が喫緊の課題。

2. 取組の概要

① 手法

- ✓ **「政府統一基準群」や「IT調達申合せ」をはじめとした基準・ルールの実効性強化**や、**政府サイバーセキュリティ人材の活用・育成強化**、**レッドチームテストといった政府機関の対策・対応について、組織・システム・人的側面を含め多面的に評価するための取組の検討**といった施策を推進。
- ✓ 既存のセキュリティ運用の枠組み（GSOC）の着実な整備・運用や、**脅威を能動的に探し出す「スレットハンティング」の体系的な実施**（この過程で、**アタックサーフェスマネジメントによる脆弱性把握**や**プロテクティブDNSによるTTPの把握**といった新しい施策にも積極的に取り組む）。
- ✓ デジタル庁にて、令和６年度内に**総合運用・監視システムの設計・開発を行い、運用監視を開始する**予定。
- ✓ 安全性や透明性の検証が可能な**国産センサを政府端末に導入**して、得られた情報をNICTの**CYNEX**（※）**に集約し分析**を行う。CYNEXに集約された政府端末情報とNICTが長年収集した情報を横断的に解析することで、**我が国独自にサイバーセキュリティに関する情報の生成**を行う。生成した情報は**政府全体で共有**。

（※）サイバーセキュリティ統合知的・人材育成基盤。

② 取組によって期待される成果・効果

- ✓ **政策・オペレーションの両セグメントにおける自律的な強化**等により、**政府全体での強固なサイバーセキュリティ体制が実現**される。
- ✓ 横断的な運用監視によるITガバナンスの確保及び運用監視レベルの向上により、**インシデントの予防・早期発見・早期復旧**が可能。
- ✓ **我が国独自のサイバーセキュリティ関連情報の生成及び政府全体での分析結果等の共有**によるサイバーセキュリティ対策の一層の強化。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 国自身の体制強化は最重要事項。
- サイバーセキュリティの攻撃技術は日々進化し、高度化・秘匿化が著しく、従来の検知・防御手法では容易に発見・阻止できない。これに対応するためには、攻撃の発見（センシング）とリアルタイムの情報共有、動的な防御が重要で、政府機関にはこれらの導入と運用に全力を注いで頂きたい。
- 省庁間でのサイバー関連情報の共有、適切で効果的な対応を統一的に行う仕組みの構築を強力に進める必要がある。
- 政府情報システムに対する総合運用監視や我が国独自のサイバーセキュリティに関する情報の共有に取り組むことが重要。
- 政府を守る体制だけでなく、重要インフラ・民間企業を含む日本全体の防御体制の抜本的強化が必要。

［２］ 重要インフラ演習の強化及び個別分野におけるレジリエンス向上

1. 背景及び課題

- 重要インフラ事業者等の障害対応体制の有効性検証等を目的に、内閣官房が所管省庁と連携して**「分野横断的演習」を毎年度実施**している。演習を通じた重要インフラの強靭性の確保が図られてきたが、**複数組織での被害発生への対処や官民間での情報共有の実践・確認が課題**となっている。
- **医療機関のセキュリティ対策**は、これまで各医療機関が自主的に取組を進めていたが、サイバー攻撃により長期に診療が停止する事案が発生したことから**自主的な取組だけでは不十分**と考えられる。医療機関におけるサイバーセキュリティ対策を強力に推進することが必要。
- **国・地方公共団体等のネットワークを通じた相互接続が一層進展**する中で、地方公共団体のサイバーセキュリティ対策の実効性を担保することが必要。

2. 取組の概要

① 手法

- ✓ **官民間の連携の実践に重点を置いた新たな官民連携演習**を、現行の分野横断的演習とともに実施する。演習には、内閣官房、所管省庁及び重要インフラ事業者等との間で双方向のやりとりや、シナリオとして重要インフラサービスの途絶や外部の重要インフラサービスの障害発生等の状況を盛り込む。
- ✓ サイバーセキュリティインシデントが発生した**医療機関に対する初動対応支援**や、**医療機関がサイバーセキュリティ対策を講じるにあたっての相談・助言**を行う。また、「医療機関向けセキュリティ教育支援ポータルサイト」において、**職員を対象とした研修にも活用できるコンテンツ等の作成・掲載**を行う。
- ✓ 「医療情報システムの安全管理に関するガイドライン」第6.0版について、医療機関における研修の実施や普及啓発に取り組む。また、「医療機関におけるサイバーセキュリティ対策チェックリスト」において、医療機関における日々のセキュリティ対策を推進するとともに、チェックリストを用いた立入検査を行う。
- ✓ 厚生労働省委託事業において、**病院の外部ネットワークとの接続の安全性の検証・検査**や、**オフライン・バックアップ体制の整備の支援**を実施する。
- ✓ **地方自治法を改正**し、**総務大臣作成の指針を踏まえ、地公体に方針策定を義務付け**、**情報システムの適正利用のための必要な措置**を講じさせる。

② 取組によって期待される成果・効果

- ✓ 重要インフラ事業者等の自組織の障害対応体制の継続的改善を促すとともに、**他の重要インフラ分野において発生した複数組織に影響を与えるインシデントへの対処能力の向上**及び**官民間の情報共有体制の強化**、ひいては重要インフラ分野全体のレジリエンス向上が見込まれる。
- ✓ **医療機関全体のサイバーセキュリティ対策の底上げ**を図り、長期に診療が停止する事案の発生を防ぐことで**地域の診療体制を確保**する。
- ✓ **サイバーセキュリティ基本法所定の「地方公共団体の責務」に係る取組を推進**し、**地公体全体のサイバーセキュリティレベルの底上げを実現**する。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 重要インフラ全体を取りまとめてセキュリティ水準を向上させることは、まさに国が行うべき施策。
- 重要インフラへのサイバー被害の影響は甚大で、演習を通じてその実態を経験することは重要。昨今の国際情勢に鑑みると、より緊密に官民で連携し、「高度なスキル」で「リアリティ」が高い演習を目指して頂きたい。
- 官民連携は具体的な実践に取り組むことなしには達成できない。各省庁が横断的に連携・協力して対処する演習を行う意義は計り知れない。こうした取組を継続し、官民横断的な幅広い参加を募ることが重要。演習を通じて組織的・制度的な対応に不十分な点がないかの検証を行う必要がある。
- 医療機関をはじめとする個別分野特有の演習強化を実施することも重要。
- 分野横断演習においては、演習の目的及び政府の役割の明確化、現実的なシナリオと参加者の選定が必須。ロックド・シールズ等の既存演習の活用等も必要。

[３] IPAの機能強化及びNICTの取組強化を通じたサイバーセキュリティ対策の底上げ

1. 背景及び課題

- **AIの利用機会と可能性が拡大**する一方で、**リスクが多様化・増大**。「**AIセーフティ・インスティテュート**」（AISI）を**IPAに設立**するとともに、AIの安全安心な利用が促進されるよう、**「AI事業者ガイドライン」を公表**。
- IPAは、**各種ガイドライン等の対策基準の整備**や、**サイバーレスキュー隊**を通じたサイバー攻撃に対する**初動対応支援**等の様々な取組を実施。
- **医療機関**等の重要インフラ事業者が**サイバー攻撃により機能停止する事態が相次ぎ**、当該分野の**セキュリティ人材不足も原因の一つ**。行政が支援し、当該分野の実態を踏まえた**早急な人材育成が必要**。

2. 取組の概要

① 手法

- ✓ **AI事業者ガイドラインの履行確保について**、**国際整合性等も踏まえ、検討を推進**するとともに、**AISIを中心として**、国内外のAI専門家の協力を得て、英国や米国をはじめとする、**パートナー国・地域の同等の機関と連携しながら、AIの安全性評価の手法を確立**。
- ✓ IPAにおいて**ガイドラインの作成機能の管理・一元化**等を行うとともに、新たに創設される**「IoT製品に対するセキュリティ適合性評価制度」等と連携**しつつ、実効性を強化。
- ✓ サイバー攻撃動向分析に加え、背景となる**地政学情報等を分析する体制を整備**し、サイバー攻撃への対処能力、**情報収集・分析能力を強化**。
- ✓ NICTが保有する人材育成やサイバーセキュリティ研究の実績・知見を活用し、厚生労働省等と連携しつつ、**各分野に特化した新たな演習プログラムを開発**し、民間企業・団体に提供できる体制を構築する。講師人材の育成も併せて行う。

② 取組によって期待される成果・効果

- ✓ AI事業者ガイドラインにより、**事業者が安全安心なAI活用のための行動につながる指針の確認**ができる。
- ✓ 各企業等の業種・規模などの**サプライチェーンの実態を踏まえた満たすべき対策のメルクマール**や、その**対策状況を可視化**することで活用を活発化させ、サイバーセキュリティ強化の底上げが期待される。それに伴い国家の安全保障・経済安全保障の確保に貢献できる。
- ✓ **医療分野**、**サイバー安全保障分野の対処能力向上**が期待できる。また、**民間人材リソースも活用した実践的サイバー演習の講習機会が拡大**する。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- IPAとNICTの集中強化により、効率的な取組が強化されることを期待。
- 多くの民間人が活躍する公的機関であるIPAやNICTで、官民の信頼関係の醸成、双方向での情報交換等がなされることを期待。特に経済安全保障等の分野では、J-CSIP/J-CRAT等の専門家集団の更なる活躍を期待。
- AIの活用はサイバーセキュリティ対策分野においても重要な位置を占める。その関連でIPAの機能強化を打ち出すことの意義は深い。
- 特に重要インフラ分野での人材確保が喫緊の課題。NICTが知見・実績を有する実践的サイバーセキュリティ人材育成施策を必要な分野に活用することにより、重要インフラ分野におけるサイバーセキュリティ強化等に寄与することが重要。
- 国全体のセキュリティ水準の底上げには横断的・継続的な組織における取組が必要であり、かつ、それを担う人材が不可欠。

1. 背景及び課題

- 欧米諸国を中心に、**ソフトウェアやIoT製品に対するセキュリティ対策強化に向けた議論が加速**。これらの実効性を担保する為には、**SBOM**（Software Bill of Materials（ソフトウェア部品構成表））**の活用促進**や、**IoT機器のセキュリティ要件の適合性を評価する仕組みの構築**が必要。
- IoT機器を乗っ取ることでボットネットを拡大する攻撃が増加し、攻撃のリスクが一層高まる中、**脆弱性のあるIoT機器及び既にマルウェア感染したIoT機器への対処が喫緊の課題**。併せて、フロー情報の分析による**C&Cサーバの検知・共有の取組**も必要。

2. 取組の概要

① 手法

✓ **セキュアバイデザイン・セキュアバイデフォルト原則を踏まえた**下記の取組の推進。

- ソフトウェア開発者の**開発手法に関するガイドラインの作成**や**SBOM活用の推進**、安全な**ソフトウェアの自己適合宣言の仕組み**の検討。
- **「IoT製品に対するセキュリティ適合性評価制度」の整備**、認証製品と政府調達等の連携や諸外国の制度との相互承認に向けた調整、交渉。
- **「NOTICE（※）」の、調査対象機器の拡大**、利用者向け安全管理対策の広報の強化、**IoT機器メーカ等の連携強化**等。
- 実際のIoTボットネットへの対処を見据えた**C&Cサーバの検知・評価・共有・対処の一連の仕組みの改善・検証**に取り組み、フロー情報分析を行うISPの拡充等を通じた**C&Cサーバの観測能力向上**を図る。また、対策時に得られる情報を統合分析し、IoTボットネットの全体像の可視化につなげる。

（※）サイバー攻撃に悪用されるおそれのある IoT 機器を NICTで調査し、当該機器の利用者への注意喚起を行う取組。

② 取組によって期待される成果・効果

✓ SBOMに関する知見の整理やソフトウェアに係る取引モデル等のツールの整備を行うことで、**安心してソフトウェア活用を行うことができる環境が構築**され、その結果、あらゆる産業で**生産性の向上や新たなサービスの創出といった付加価値の増大**が見込まれる。

✓ IoT機器に係る**国際的に調和の取れた適合性評価制度が構築されることで、国内での安全な機器の流通**という効果に加え、企業が海外にIoT機器の販路を広げる際に、**諸外国の制度への対応のために追加対応に割くコストが抑制**されることから、**競争力強化**にもつながる。

✓ 脆弱性のあるIoT機器を削減（増加抑制）するための活動を継続することで、**IoT機器のより安全な利用環境の実現**につながる。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- ソフトウェアやIoT機器のセキュリティ対策に関しては欧米諸国を中心に議論が加速しており、実効性担保の取組は重要。
- 「セキュアバイデザイン」「セキュアバイデフォルト」概念は、近い将来にはICT業界での基本概念として根付いていく。今後は、より具体的な施策に移していく必要がある。
- 中長期的に取り組むべき重要課題。グローバル協調としても重要。
- ソフトウェア・IoTのセキュリティ問題に関しては、開発業者等の連携を更に強化しつつ、継続的な努力が払われるべき。
- IoT機器に関する評価制度を構築することは重要。当該制度では、「諸外国との連携を保つこと」と「過度に敷居（難易度）を高く設定しないこと」に留意。
- NOTICEに関し、今後より多くの情報を双方向でやり取りし、セキュリティ強化に役立てていくことを期待。

［５］ 中小企業のサイバーセキュリティ対策促進

1. 背景及び課題

- サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、**中小企業自身及びその取引先である大企業等への被害が顕在化**。他方で**中小企業においては、リスクを自分事として認識していない**、あるいは、**何をしてよいか分からない状況**。
- **予算や人材が不足している中小企業**が、それぞれの規模や業種、事業上の事情等に照らして**自らに最も効果的なセキュリティ対策の水準を把握**し、それを**実践できる環境を整備**するとともに、中小企業が**使いやすいセキュリティサービスを普及・促進していくことが必要**。

2. 取組の概要

① 手法

- ✓ **サイバーセキュリティお助け隊サービス**について、2023年度に創設した**新たなサービス類型を含め、中小企業等への普及・展開**を図る。
- ✓ **企業規模やIT資産の内容等に応じて**、ガイドラインとも紐付けながら、**費用対効果のある方法等を提示**する。
- ✓ **中小企業等とセキュリティ人材とのマッチング**を促す場を構築し、**セキュリティ人材のシェアリング促進**等、**中小企業における人材探索コストの低減**を図る。

② 取組によって期待される成果・効果

- ✓ **サイバーセキュリティお助け隊サービス**について、中規模以上の中小企業等も含めた**普及啓発を促進**する。
- ✓ 費用対効果のあるセキュリティ対策の方法等の提示を図ることで**産業界のサプライチェーン全体のセキュリティ対策水準の向上**を図る。
- ✓ 中小企業における人材探索コストの低減を図ることで**企業のサイバーセキュリティ対策を行う側の人材を拡充**させる。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- サプライチェーンは中小企業が支えているところも多く、セキュリティ確保は重要。
- 中小企業は犯罪者の格好のターゲットになっている。日本産業界のセキュリティ防御の「要」は中小企業にある。
- 政府主導で中小企業のセキュリティ対策支援を積極的に推進すべき。特に人材と情報共有、補助金支援を中心とした活動に注力すべき。
- レジリエンス確保は中小企業にとって死活的問題。現場の声やニーズに対応して適切な対処方法の提供と普及、それを担う人材の育成等を行う上で「サイバーセキュリティお助け隊サービス」の役割は重要。
- セキュリティ人材のマッチング、シェアリング等の人材確保支援策にも期待。

[６] 海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進

1. 背景及び課題

- 国家安全保障戦略に「**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**」と定めていること等を踏まえ、**同盟国・同志国との協力・連携の強化**がますます重要となっており、外交・安全保障政策との整合性を図りつつ、**技術的な観点も踏まえた国際連携を一層**推進する必要がある。
- 対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保し、サイバー空間全体の安全の確保と直結する**サイバーセキュリティ分野の能力構築支援**についても、「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」に基づき、関係省庁間及び官民による連携を緊密化し、サイバー空間における新たな脅威や各国のニーズを特定した上で、**日本の強みを生かす形で支援を行う必要**がある。

2. 取組の概要

① 手法

- ✓ **同盟国・同志国間での情報交換・政策協調**や、サイバーセキュリティに関する**多国間の枠組み**（G7、IWWN、CRI、日米豪印、FIRST等）**への参画・貢献**、国際シンクタンクやフォーラムにおける我が国政策の発信。
- ✓ 日ASEANサイバーセキュリティ政策会議、インド太平洋地域向け産業制御システムサイバーセキュリティ演習、AJCCBCにおける各種演習・CTFの実施、大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援プロジェクト、世界銀行サイバーセキュリティ・マルチドナー信託基金への拠出等を通じた**インド太平洋地域を含む途上国のサイバー分野にかかる能力構築支援**。

② 取組によって期待される成果・効果

- ✓ 他国との連携を通じて、**サイバーセキュリティ政策の効果的な推進**や**事案発生後の被害の軽減**等を図ることが可能。
- ✓ **ASEANを含むインド太平洋地域**を中心とした政府関係者及び重要インフラ事業者の**サイバーセキュリティに係る能力の底上げ**。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- グローバル視点から必須の取組。
- 海外のサイバーセキュリティ関係機関との協調・連携強化が必要との認識に同意。日本が国際的な枠組みでいかなる貢献ができるかということも、他国の関係機関との信頼関係を構築・醸成・強化する上で不可欠の視点。
- 昨今の地政学的緊張の高まりにより、技術力やスキル等の能力の向上も踏まえた同盟国・同志国との連携・協力強化を図ることが必要。
- 日本と近隣のインド太平洋地域の諸国と強い協力関係を構築することは極めて重要。
- インド太平洋地域は海の草刈り場の様相を呈しており、こうした働き掛けは重要。

[７] 警察庁におけるサイバー空間の安全・安心の確保に資する取組の推進

1. 背景及び課題

- **サイバー空間は**、地域や年齢、性別を問わず、全国民が参加し、**重要な社会経済活動が営まれる公共空間へと変貌を遂げている一方**、ランサムウェア被害の拡大、クレジットカード不正利用被害やフィッシングによるものとみられるインターネットバンキングによる不正送金被害の急増、暗号資産関連業者や学術機関を標的としたサイバー事案の表面化、**重大サイバー事案の発生による社会機能への影響など、サイバー空間を巡る脅威は、極めて深刻な情勢**が続いている。
- こうした状況に対応するため、下記の取組の一層の推進が求められる。
  - ✓ サイバー事案の被害防止対策に関し、**警察への通報・相談の促進、広報啓発、注意喚起**の実施
  - ✓ **事案の横断的・俯瞰的分析の強化**及び**外国捜査機関等との連携**

2. 取組の概要

① 手法

- ✓ 警察庁サイバー警察局において、**国内外の多様な主体と連携しながら**、サイバー空間の脅威情勢を踏まえた国民への注意喚起や関係団体への各種要請等、サイバー事案に係る被害防止対策を効果的に推進する。また、関東管区警察局サイバー特別捜査隊を発展的に改組したサイバー特別捜査部において、情報の収集、整理及び分析を行う体制を強化するとともに、外国捜査機関等との一層ハイレベルな調整を通じて**国際共同捜査に積極的に参画**する。

② 取組によって期待される成果・効果

- ✓ 国内外の多様な主体と手を携え、サイバー空間の脅威情勢を踏まえた適時的確な被害防止対策を行うとともに、外国捜査機関等と連携して、サイバー事案の捜査や実態解明を進めることにより、**サイバー空間の安全・安心の向上**が期待される。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 近年、ランサムウェア攻撃やフィッシング攻撃などの重大サイバー事案が深刻化しており、官民連携・省庁連携の強化や外国捜査機関等との連携強化を一層推進することに期待。
- FBIやEuropolとの協力等、今年度は更に強力な体制での捜査協力に期待。また、TV/SNS等のメディアを通じた犯罪情報の共有を推進して頂きたい。
- 日々高度化し発展するサイバー犯罪に対応するため、警察機関において組織体制の整備や能力上納の施策を図ることは非常に重要。
- 外国機関との連携を期待。

第１部・第２部 サイバーセキュリティに関する情勢

サイバー攻撃の深刻化や巧妙化の進展

－　国家を背景とした攻撃の拡大、 未知の脆弱性を悪用したゼロデイ攻撃の増大等、 サイバー攻撃の洗練化・巧妙化が一層進展。生成AI等の新技術の普及に伴う新たなリスクも増大。

⇒　政府機関・重要インフラ事業者、ユーザにサービスを提供するテクノロジー企業などの能力ある主体がより多くの役割を果たすことが重要。サイバー安全保障の観点も含め、平素からの対策強化や対処能力の向上、セキュアバイデザイン・セキュアバイデフォルト原則に基づく措置の具体化、欧米主要国をはじめとする関係国との協調・連携が必要に。

経済社会の活力の向上及び持続的発展

経済社会における情勢

- 企業活動におけるITの利用促進に伴う脅威の高まり。
- 大企業への直接のサイバー攻撃だけではなく、その取引先の協力会社を攻撃の踏み台にした例も見られる。
- 直接の攻撃を受けた組織のみならずサプライチェーン全体にも被害が及び得る
- ランサムウェア被害の約半数が中小企業。

中小企業・サプライチェーン対策

- 組織向けのサプライチェーン・リスクへの対策は必須であり、特に中小企業を対象とした民間部門に対する対策の支援サービスや機能充実が必要。

IoT製品のセキュリティ確保に向けた取組の推進

- 悪用が懸念されるIoT機器のセキュリティ評価等の対策が必要。

国民が安全で安心して暮らせるデジタル社会の実現

経済社会基盤を支える各主体における情勢

①政府機関等

- インシデント件数は高止まりしている。
  （2021年度207件、2022年度266件、2023年度233件）
- GSOCによる政府機関等への脆弱性情報等の提供も増加。
  （2021年度598件、2022年度630件、2023年度861件）

- 第一、第二GSOCの緊密連携等が必要。
- 脆弱性等の是正を促す仕組み（ASM）や、悪性サイト等のIPアドレスを検知・蓄積するプロテクティブDNSを導入。

②重要インフラ

- 国内外の重要インフラ分野等において、システム障害や情報流出の事例が多数発生。
  （例：港湾施設が、ランサムウェアによるサイバー攻撃を受けて停止）

- 侵入を前提とした多層防御の考え方に基づくシステム設計・運用、サイバー被害を想定した事業継続計画の立案・点検等が必要。

③大学・教育研究機関等

- 大学等の特性を踏まえた上で、主体的なセキュリティ水準の維持・向上を図る必要。

④東京オリンピック・パラリンピック競技大会に向けた取組から得られた知見等の活用

- 大阪・関西万博等への知見の活用が重要。

国際社会の平和・安定及び我が国の安全保障への寄与

国外の動き（諸外国の国際動向）

米国

- 国防総省「サイバー戦略2023」の概要を公表（2023年９月）
- 「セキュアバイデザイン・セキュアバイデフォルト原則」に関する国際ガイダンスの改訂（我が国を含む13の国・組織が共同署名）（2023年10月）

英国

- 「セキュアAIシステム開発ガイドライン」を作成（我が国を含む18の国・組織が共同署名）（2023年11月）

豪州

- 「2023-2030年豪州サイバーセキュリティ戦略」及び「アクションプラン」を公表（2023年11月）
- 「AIシステム使用に関するガイダンス」を作成（我が国を含む11の国・組織が共同署名）（2024年１月）

EU

- 「サイバー強靱化法」を欧州議会が承認、「サイバー連帯法」の政治合意（2024年３月）

ASEAN

- 日本ASEAN友好協力50周年特別首脳会議の開催、「共同ビジョン・ステートメント」及び「実施計画」の公表（2023年12月）

国際協力が不可欠。各国の動向を踏まえ、強化に取り組む。

横断的施策

サイバーセキュリティ分野の研究開発

- 生成AIの普及、量子等の先端的な技術の進展、昨今の国際情勢の複雑化等により安全保障の裾野がサイバー分野に拡大する中、サイバー空間の安全・安心の礎となる研究開発の重要性はますます向上。

- 研究の裾野を広げる観点からの産学官エコシステム構築に向けた体制整備、実践的な研究開発構想の検討を実施。

IT・サイバーセキュリティ人材

- サイバーセキュリティ人材確保の需要の高まりに加え、DXを進めるに当たり、現時点で知識・業務経験を有しない人材のリスキリング等に対する需要が引き続き増大。

- 「デジタル田園都市国家構想総合戦略」において、サイバーセキュリティ人材を含むデジタル推進人材を2026年度末までに230万人の育成を目指す。
- スキルを習得できる環境整備、「プラス・セキュリティ」等の経営層の意識改革、大学・高専等での取組強化が必要。

国民の意識・行動

- デジタル化が着実に進展する一方、フィッシングによる不正送金の被害件数、被害額が過去最多。

- サイバーセキュリティ対策の必要性につき、訴求すべき対象に応じたよりきめ細かな普及啓発活動とともに、各主体が密接に連携・協働することが必要。
- 「サイバーセキュリティ意識・行動強化プログラム」に基づき、引き続き普及啓発活動に取り組む必要。

第３部 戦略に基づく昨年度の取組実績、評価及び今年度の取組（１/４）

１．経済社会の活力の向上及び持続的発展

	経営層の意識改革	地域・中小企業対策	サプライチェーン等の信頼性確保
昨年度の取組例	➢ 経営層の「プラス・セキュリティ」知識補充を目的に、サプライチェーン・リスクへの対応や、セキュリティを意識する企業風土醸成等をテーマにした動画の作成 ➢ 民間企業の情報開示状況の調査・公表等の取組支援 ➢ 「サイバーセキュリティ経営ガイドライン」の周知や可視化ツールの利便性向上	➢ 地域SECUNITYによる、産官学連携の研修やインシデント演習等の実施 ➢ 地域コミュニティでIoTセキュリティ人材を育成するための実証的調査を実施 ➢ 「サイバーセキュリティお助け隊サービス基準」の改定、「SECURITY ACTION」制度の周知、地域におけるセキュリティ指導者の拡大を実施	➢ SBOMの促進や、IoT製品のセキュリティ対策強化に向けた取組を実施 ✓ 「ソフトウェア管理に向けたSBOMの導入に関する手引き」の策定 ✓ IoT製品に対するセキュリティ適合性評価制度の一部運用を開始する方針の決定 ➢ ソフトウェア部品の構成表であるSBOMを通信分野で導入する上での課題等を整理
評価	➢ サプライチェーン・リスクの拡大に伴い、今後の更なる攻撃被害リスクの増大も懸念される中で、コーポレートガバナンスの観点でも、サイバーセキュリティの重要性に対する認識を高めるための更なる取組が必要 ➢ 地域やサプライチェーンを通じた取組の広がりを促すとともに、設定不備等で意図しない情報資産の流出リスクへの対処が必要 ➢ 業界ごとのプラクティスの横展開や産学官の結節点となる基盤の整備、サイバーとフィジカルの双方に対応したフレームワーク等を踏まえた基準・規格づくり等の各種取組を引き続き進展させていくことが必要		
今年度の取組例	➢ 経営層向けの「プラス・セキュリティ」知識を補充するモデルカリキュラム及び普及啓発コンテンツ等の普及 ➢ 「サイバーセキュリティ対策情報開示の手引き」を踏まえた民間における取組支援の継続 ➢ 「サイバーセキュリティ経営ガイドライン」や関連ツール等を通じたサイバーセキュリティ経営の更なる普及啓発	➢ セミナーやインシデント演習等、地域SECUNITYの自発的な運営に向けた取組を支援 ➢ 「クラウドサービスの利用・提供における適切な設定のためのガイドライン」の普及啓発 ➢ 「サイバーセキュリティお助け隊サービス基準」の普及啓発や、「SECURITY ACTION」普及のための周知方法や制度活用について議論	➢ SBOM活用に係る脆弱性管理についての更なる検討や、IoTセキュリティ適合性評価制度の運用開始に向けた対応 ✓ 産業界と連携した普及促進 ✓ 政府調達等を通じた活用 ✓ 国際的な制度調和の促進 ➢ 通信分野におけるSBOM導入後の運用を見据えた課題等の整理

２．国民が安全で安心して暮らせるデジタル社会の実現

	安全・安心な環境構築、デジタル改革との一体的推進	政府機関等の取組	重要インフラの取組
昨年度の取組例	➢「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」、「常時リスク診断対処（CRSA）のエンタープライズアーキテクチャ」等を公開 ➢ セキュリティリスクの小さいSaaS向けの評価の仕組み（ISMAP-LIU）の登録促進や改善 ➢ マイナポータルアプリを刷新し、利便性向上やシステム安定稼働に向けた対応を実施 ➢「NOTICE」の取組の延長・拡充に向けた法改正を実施	➢ 政府対策統一基準群の改定 ➢ サプライチェーン・リスク対策として、規定の見直しやリスク軽減策等を助言 ➢ 適切なリスク対応が必要と考えられる分野等を重点に置き、マネジメント監査を実施 ➢ GSOCで検知したサイバー攻撃の政府機関に対する注意喚起や、次期GSOC構築に向けた検討を実施 ➢ NICT開発センサを政府端末の一部に導入し、端末情報の収集・分析を開始	➢「重要インフラのサイバーセキュリティに係る安全基準等策定指針」を策定 ➢「重要インフラ行動計画」を改定し、港湾を重要インフラに追加 ➢「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」を策定 ➢「分野横断的演習」を実施（過去最多の6,574名（819組織）が参加）
評価	➢ 今後も技術動向を調査しつつ、ガイドライン・技術レポートの策定・改定が必要 ➢ サイバーセキュリティを確保しつつ、利用者にとってより便利なサービスを目指した取組が必要 ➢ 各政府機関等のサイバーセキュリティ対策の現状を適切に把握し、対策を強化するための助言や、一層の促進に向けた取組等を実施することにより、政府機関等全体として、更なるサイバーセキュリティ対策の底上げが図られた ➢ 関係省庁の積極的な取組の継続や一層の推進、情報共有体制の強化に向けた検討の推進、リスクマネジメントの活動全体が継続的かつ有効に機能するような取組の推進、及び人材育成など行動計画の全体を支える共通基盤の強化継続への取組を推進することが必要		
今年度の取組例	➢ ガイドライン・技術レポートの改訂や新規発行、デジタル庁システムへ活用 ➢ ISMAP-LIUの普及・活用を促進するための特別措置 ➢ マイナポータルのサービス拡充やUI・UXの継続的改修、適切な運用管理 ➢「NOTICE」について、ISPやメーカ等との連携体制を構築し、対策を推進	➢ サプライチェーン・リスク対策として、「IT調達申合せ」、「外部サービス申合せ」の取組推進 ➢ 監査において、近年の脅威動向を踏まえたリスク対応等の確認を継続 ➢ 政府機関等とGSOC間の連携、次期GSOCの着実な整備、ASMやプロテクティブDNSといった技術・仕組の導入 ➢ NICT開発センサによる政府端末情報の収集・分析結果をNISC等に共有	➢ 中小規模の重要インフラ事業者でも優先的に最低限遵守すべき分野横断的で一貫した基本的事項（Minimum Requirement）の整理 ➢ 行動計画に基づく、５つの施策群に関する取組の継続 ➢「分野横断的演習」及び官民が連携して参加する演習の実施

３．国際社会の平和・安定及び我が国の安全保障への寄与

昨年度の取組例

「自由・公正かつ安全なサイバー空間」の確保	我が国の防御力・抑止力・状況把握力の強化	国際協力・連携
➢ サイバー協議やその他多国間会合を通じ、サイバー空間における法の支配の推進に積極的に寄与 ➢ 国連オープンエンド作業部会(OEWG)において、2025年以降の国連行動計画(PoA)等に向け、関連の議論に積極的に貢献 ➢ G7、ASEAN及びインターポール(ICPO)の枠組み等における各国機関との情報交換等の国際連携強化	➢ 自衛隊の任務保証に関連する主体との連携を深化させる取組を実施 ➢ リスク管理枠組み（RMF）の実施等による防衛能力強化 ➢ ASEAN地域フォーラムの枠組みにおいて、今後取り組むべき信頼醸成措置について議論 ➢ 外国関係機関との緊密な情報交換、分析、関係省庁と連名での注意喚起	➢ 15以上の国・地域等で行っているサイバー協議を通じ、知見の共有・政策調整 ➢ 日ASEAN友好協力50周年の各種会議・イベントを開催し、今後の方向性等について議論 ➢ 第３回ランサムウェア対策多国間会合への参加、第３回日米豪印上級サイバーグループ対面会合の開催を通じた国際連携の強化

評価

➢ 国連OEWGの会期での議論への貢献等を通じ、国際的なルール及び規範に係る更なる議論の深化を図る必要
➢ 国際協力・連携による知見共有や能力構築支援の取組をサイバー犯罪条約の締約国拡大につなげ、協力を深化させる必要
➢ サイバー空間の脅威の多様化・複雑化を踏まえ、引き続き、我が国の防御力・抑止力・状況把握力の強化が必要
➢ 信頼関係を構築する関係国の幅の拡大、既に信頼関係がある関係国との関係深化を図る必要
➢ 能力構築支援につき、インド太平洋地域を中心に支援対象を拡大し、官民一体で戦略的に対応していく必要

今年度の取組例

➢ 二国間・多国間協議、国連OEWGを通じ、サイバー空間における国際法の適用に関する議論の加速 ➢ 国際会議を通じ、多国間における協力関係構築、外国法執行機関等との連携強化、的確な国際捜査の推進 ➢ 国連におけるサイバー犯罪条約に関し、関係国と連携して議論	➢ 安全保障環境が厳しさを増していることを踏まえ、サイバー攻撃に対する国家の強靱性確保や、防御力・抑止力・状況把握力の向上に向けた取組を引き続き推進	➢ サイバー空間の安定実現に向けて、ASEAN地域等における能力構築支援等の波及効果を狙う施策を実施 ➢ 米欧と協力し、インド太平洋地域の重要インフラ事業者向けの産業制御システムサイバーセキュリティ演習を実施 ➢ 主要同盟国・同志国と重要インフラ防護や脅威情勢認識等に関する協議、連携強化

４．横断的施策

	研究開発の推進	人材の確保、育成、活躍促進	普及啓発、リテラシーの定着・向上
昨年度の取組例	➢ 信頼できるAI等、革新的な人工知能基盤技術の構築等の研究開発を実施 ➢ 産学官連携の基盤となる「CYNEX」を高度化し、セキュリティ情報の収集・分析・提供等の取組を本格化 ➢ 量子暗号通信網構築や、量子インターネットの要素技術の研究開発	➢ 「中核人材育成プログラム」の実施や、ポータルサイト「マナビDX」等を通じた人材育成プログラムの発信 ➢ 受講者ニーズ等を踏まえ、コース再編・内容更新した上で、「CYDER」を実施 ➢ 政府のサイバーセキュリティ関係の研修やスキル認定の見直し	➢ インターネットやSNS等を用いた若年層向け広報活動を実施 ➢ 講座「スマートフォンを安全につかうためのポイント」の内容を更新 ➢ 一般の利用者や指導者などに向けてIPAの教材を提供
評価	➢ 安全保障の観点を含め、イノベーションの源泉となる研究開発と産学官エコシステムの双方の視点を併せ持つ必要 ➢ 研究振興施策が社会において広く活用されるよう取り組む必要 ➢ 量子技術の急速な発展に伴い、引き続き研究開発を推進する必要	➢ 専門人材の必要性は高まっており、人材育成の環境整備等を不断に続けていくとともに、人材の裾野を広げていく取組も必要 ➢ サイバー空間上における脅威が高まっている状況を踏まえ、政府デジタル人材の確保・育成等の取組強化が必要	➢ サイバー空間への参画層の広がり等を踏まえ、高齢者やこども・家庭への対応を含め、取組状況の見直しや強化が必要
今年度の取組例	➢ 基盤技術開発に加え、サイバーセキュリティを含む研究課題に対する支援の継続実施 ➢ 不正機能や当該機能につながり得る未知の脆弱性の技術的検証 ➢ 「CRYPTREC暗号技術ガイドライン」の改定及び耐量子計算機暗号（PQC）等に関する研究開発 ➢ 量子暗号通信の社会実装の推進や量子インターネットの要素技術の研究開発	➢ セキュリティ人材育成に係る手引きなどの普及と利活用の推進、経営者に対する普及啓発を行う ➢ 「CYDER」、「公共職業訓練」、「セキュリティ・キャンプ」等を継続実施し、自立的なセキュリティ人材育成を促進 ➢ 資格試験の活用推進や研修の見直し、スキル認定を更新する仕組みを創設	➢ 関係省庁と連携した普及啓発の取組や、各種コンテンツの利活用促進を実施 ➢ デジタル活用支援推進事業の講習会を引き続き実施 ➢ 情報セキュリティに関する啓発を行う教材やコンテンツの提供、指導者向けセミナーを引き続き実施

第１部エグゼクティブ・サマリー用語集

No.	用　語	解　説
1	セキュアバイデザイン	IT製品（特にソフトウェア）が、設計段階から安全性を確保されていること。前提となるサイバー脅威の特定、リスク評価が不可欠。
2	セキュアバイデフォルト	ユーザ（顧客）が、追加コストや手間をかけることなく、 購入後すぐにIT製品（特にソフトウェア）を安全に利用できること。
3	アタックサーフェスマネジメント	政府機関等の情報システムをインターネット上から組織横断的に常時評価し、脆弱性等の随時是正を促す取組。
4	プロテクティブDNS	ドメインネームシステム（DNS）を活用して悪意あるウェブサイトやマルウェア等の脅威からユーザを保護し、またそれらの脅威の使用するドメイン名やIPアドレスを蓄積する取組。
5	CYXROSS	CYNEX XROSS organ observatory Projectの略称。 政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証作業。
6	IPA	独立行政法人情報処理推進機構。 ソフトウェアの安全性・信頼性向上対策、総合的なIT人材育成事業（スキル標準、情報処理技術者試験等）とともに、情報セキュリティ対策の取組として、コンピュータウイルスや不正アクセスに関する情報の届出受付、国民や企業等への注意喚起や情報提供等を実施している独立行政法人。
7	NICT	国立研究開発法人情報通信研究機構。 情報通信技術分野の研究開発を基礎から応用まで統合的な視点で実施するとともに、産学官で連携し研究成果の社会還元等を行う独立行政法人。
8	AISI	AIセーフティ・インスティテュートの略称。
9	SBOM	Software Bill of Materialsの略称。 ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。
10	NOTICE	National Operation Towards IoT Clean Environmentの略称。 サイバー攻撃に悪用されるおそれのあるIoT機器をNICTで調査し、当該機器の利用者への注意喚起を行う取組。