NISC National center of Incident readiness and Strategy for Cybersecurity

サイバーセキュリティ2022の概要

令和4年6月17日
内閣サイバーセキュリティセンター

１部 エグゼクティブ・サマリー

- サイバーセキュリティ戦略において、各年度ごとに取組状況を年次報告として取りまとめ、次年度の年次計画に反映することとしていることを踏まえて策定するもの。
- 従来の構成の冒頭にエグゼクティブ・サマリーを設け、サイバー空間をめぐる課題と対応の方向性を明らかにし、発信力を強化する観点から、昨今の国際情勢等を踏まえた課題と、戦略本部として特に強力に取り組む施策を明記。

１．サイバー空間を巡る主な情勢の変化と昨今の状況

- 新型コロナ感染症による「ニューノーマル」の拡大
- デジタルトランスフォーメーション（DX）の進展
- 国際情勢の変化によるサイバーリスクの増大

⇒

- 国内でも多様なインシデントが発生
  - ✓ ランサムウェアによる被害拡大
  - ✓ Emotetによる被害拡大

２．情勢の変化に伴い顕在化している政策課題

(1) サイバー空間上における脅威の高まりに対応するための**インシデントの未然防止**
(2) 「公共空間化」によるリスクの広がりに対応するための**地域・中小企業等のセキュリティ強化・支援、サイバー犯罪への対応強化**による安全・安心の確保
(3) 厳しさを増す安全保障環境の中での**国際協力・連携の強化**

３．「自由、公正かつ安全なサイバー空間」の実現のために特に強力に取り組む施策

１）官民連携のオールジャパンの推進体制（ナショナルサート機能の強化）
インシデントの未然防止のための、情報収集・分析力の向上や官民情報共有体制の強化

２）重要インフラ事業者を始めとする民間部門におけるサイバーセキュリティの強化
「重要インフラのサイバーセキュリティに係る行動計画」を踏まえた取組の推進、サイバーインフラの強靭性の確保 等

３）サイバー・フィジカル空間の融合に対応したサイバーセキュリティ対策
ソフトウェアの脆弱性管理等のためのソフトウェア部品表（SBOM※）の普及に向けた取組の推進 等
※SBOM：Software Bill Of Materials

４）地域・中小企業のサイバーセキュリティ対策
経営者の意識改革、地域で共助の取組を推進するセキュリティ・コミュニティ（地域SECUNITY）の活動促進、中小企業に対する「サイバーセキュリティお助け隊」の普及

５）サイバー警察局・サイバー特別捜査隊の新設による官民連携・国際連携の推進
深刻化するサイバー空間の脅威に適切に対処し、安全・安心を確保していくための取組

６）インド太平洋地域における能力構築支援の推進
ASEAN諸国の政府機関に対する演習等を通じたインド太平洋地域における能力構築支援の取組の一層の推進

「サイバーセキュリティ戦略」(令和3年9月28日閣議決定)**に掲げる「自由、公正かつ安全なサイバー空間」の実現**

[１] ナショナルサート機能の強化

1. 背景及び課題

- 深刻なサイバー攻撃に対し、国が主体的に関係機関とも連携しつつ、包括的なサイバー防御を講ずる必要性の増大。
- 情報収集・分析から、調査・評価、注意喚起の実施及び対処等の一連の取組を一体的に推進するための総合的な調整を担う機能としての「ナショナルサート（CSIRT/CERT）」の枠組みを強化する必要。

2. 取組の概要

① 手法

✓ 体制整備：

〔NISC〕情報収集・共有、集約分析、対処調整等の各観点での体制強化。
外交・安全保障等の政策目的との連携・調整。

〔各省庁〕自組織及び関係機関CSIRTとしての機能の整備・強化。
所管業界/分野のサイバー防御のための支援機能の充実。

〔政府全体〕NISCと関係省庁の間の密接な連携体制を構築。

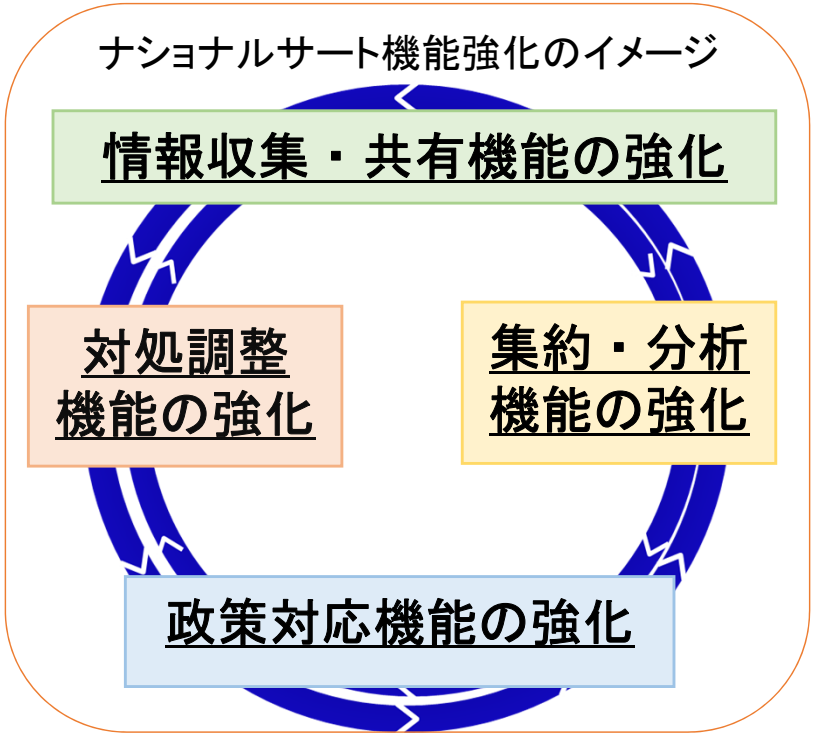
✓ 環境整備：

○ 重要インフラ事業者に限らず、他の民間部門を含めた官民間の情報共有の推進（東京大会のレガシーであるJISPの統合によるサイバーセキュリティ協議会の充実強化等）。

○「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」の開催。

② 取組によって期待される成果・効果

✓ 適宜迅速な情報収集と被害の把握、情報発信の訴求力と網羅性の向上、攻撃特性や深刻度等に応じた細かい対応等。



■ 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

- 包括的なサイバー防御の展開は、我が国のサイバーセキュリティ能力を高める上でも、安全保障の観点からも不可欠。
- 国際連携の強化により、海外関係機関とのリアルタイムの情報交換や緊密な関係構築を図りながら我が国の考え方を内外に発信していくための体制構築も含め、国際連携の強化を期待。
- 国内においても、信頼できる情報の発信源や情報の提供先として活動していくことを期待。
- 政府全体・企業・国民において、情勢変化に即応した柔軟な体制構築を可能とするべき。

[2]重要インフラ事業者を始めとする民間部門におけるサイバーセキュリティの強化

＜「重要インフラのサイバーセキュリティに係る行動計画」（2022（令和４）年６月17日サイバーセキュリティ戦略本部決定）の概要＞

- 安全で安心な社会の実現には、官民の緊密な連携による重要インフラのサイバーセキュリティの確保が必要であり、基本的な枠組みとして、**政府と重要インフラ事業者等との共通の行動計画**※を推進してきた。

※ 「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成29年４月18日サイバーセキュリティ戦略本部決定）

- 重要インフラを取り巻く脅威は年々高度化・巧妙化している中で、昨年のサイバーセキュリティ戦略（令和３年９月28日閣議決定）の策定を踏まえ、**新たな行動計画を策定**する。

◆ **第４次行動計画における有効な取組は継続**

◆ **組織統治の一部としてサイバーセキュリティを組み入れ、組織全体で対応**

◆ 重要インフラを取り巻く脅威の変化に対応するため、**将来の環境変化を先取りし、サプライチェーンを含めてリスクを明確化し対応**

重要インフラ(全14分野)
情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油

	第４次行動計画	新たな行動計画
障害対応体制の強化	○ 経営層に対し、サイバーセキュリティに関する意識を高めるよう働きかけ ○ 事業継続計画の整備とそれを実行するための組織体制の構築	○ **経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組**となるよう、**組織統治の一部としてサイバーセキュリティを組み入れる**。必要な観点として、**経営層の重要インフラサービス障害等に対する責任**等を明記 ○ 重要インフラサービスを提供するために必要な**サプライチェーン等に関わる事業者**が、サイバーセキュリティ基本法に基づき、**サイバーセキュリティの確保に努める責任を有する**旨を明記し、**組織の壁を越えたサプライチェーン全体で障害対応能力を向上**
安全基準等の整備・浸透	○ 分野横断的に必要な対策を共通指針として策定 ○ 事業者の取組についてのアンケート調査・ヒアリング	○ **組織統治、サプライチェーン**等の観点から**共通指針を改定** ○ 事業者における経営層のリーダーシップ、セキュリティ対策等の取組状況を**より正確に把握**し、取組の**継続的な改善を促進**
情報共有体制の強化	○ 多様な連絡形態による情報共有 ○ 共有情報の明確化	○ 重要インフラ事業者等の**自主的な取組の活性化を前提とした共助**の推進 ○ **ナショナルサートの枠組みの強化**の検討との整合性保持
リスクマネジメントの活用	○ リスク評価の推進	○ **経営層による自組織の特性の把握、サプライチェーン・リスクを含めたリスクの明確化**等により**自組織に適した防護対策の実現を促進**
防護基盤の強化	○ 官民が連携して行う演習等の実施	○ **障害対応体制の有効性検証**としての**分野横断的演習の推進** ○ **警察、デジタル庁との連携強化**

[3] サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の社会実装

1. 背景及び課題

➢ サイバー・フィジカル空間の融合で増大するサイバー攻撃の脅威に対応するためのフレームワークの整備・社会実装の推進が必要。

2. 取組の概要

① 手法

✓ CPSFや関連するフレームワーク等の普及啓発のための活動や、国際標準化、関係団体・関係企業との協力等を推進。

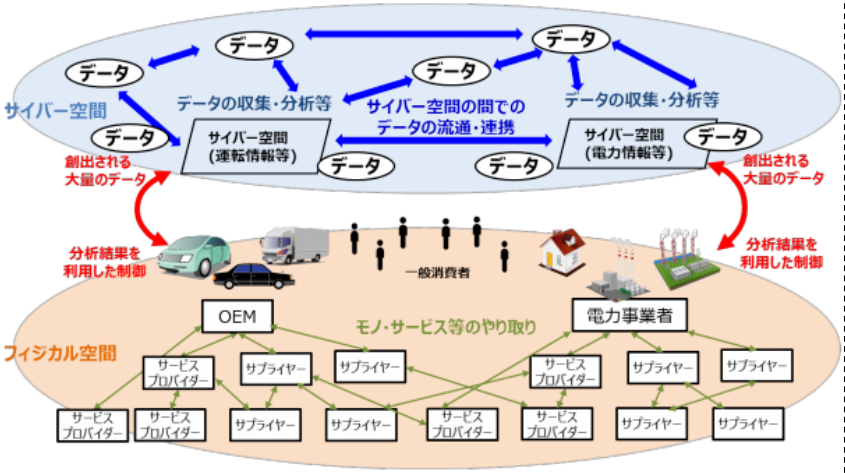
✓ 〔OSS〕OSS事例集の普及促進。
〔SBOM〕脆弱性やライセンス等のソフトウェア管理に必要な情報の整理や、迅速な脆弱性対応を行う上で有用なSBOMの普及に向けた、効果的な活用モデル、SBOM共有に係る取引モデル、ノウハウ等の構築に向けた検討を推進。

② 取組によって期待される成果・効果

[継続施策]

✓ サイバー・フィジカル・システムの理解促進や、これに伴い発生するリスクへの対応力向上。

✓ データにまつわる、ステークホルダーの洗い出し、リスクの見える化、対応策の共有や責任分担の整理が可能となり関係者の役割が整理されることで、データの自由な流通や新たな付加価値の増大に寄与。



■ 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

➢ ひとたびソフトウェアに脆弱性が発覚すると、ほぼ全ての社会に大きな影響を及ぼすことは自明。これらの対応に係る経済的損失を最小限にするべく、CPSFを社会実装し、セキュリティレベルを向上することが必要。

➢ SBOMの導入・普及を検討することは、国際社会の一員として、諸外国（特に米国）に後れを取ることなく推進すべき課題。SBOMが国際標準になることを見越して、我が国における国際標準戦略の一環と位置付け、SBOMに関する知見の整理や取引モデル等のツールの整備を着実に進めていくことが必要。

[4] 地域・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

- サプライチェーンの中でセキュリティが脆弱な部分が狙われ、サプライチェーン全体が影響を受ける事例が新たな脅威として顕在化しており、経済安全保障の観点からも地域・中小企業のセキュリティ対策は急務。
- デジタル田園都市国家構想の実現にあたっても、その両輪として地域・中小企業におけるセキュリティ対策の普及は不可欠。

2. 取組の概要

① 手法

- ✓ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携し、IT導入補助金等の支援策も活用しつつ、中小企業に必要な対策をワンパッケージにまとめた「サイバーセキュリティお助け隊サービス」を普及拡大。
- ✓ 地域で共助の取組を推進するセキュリティ・コミュニティ（地域SECUNITY）の活動促進。

② 取組によって期待される成果・効果

- ✓ 多くの中小企業におけるサイバー攻撃被害の発生・拡大の抑止。
- ✓ 地域企業に必要な情報の伝播や、地域が抱えるセキュリティ人材不足等の課題解決の促進。
- ✓ 産業界主導のSC3と連携して進めることにより、産業界全体のサイバーセキュリティ強化を促進。

サイバーセキュリティ お助け隊

■ 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

- 日本の産業を支える地域・中小企業のセキュリティ向上は喫緊の課題。人員・予算等の不足する地域・中小企業は単独でセキュリティ対策を取ることが困難。経済安全保障の観点からも、明確な目標を立て、政府の強力な支援の下、取組を推進する必要。
- 「デジタル田園都市国家構想」の実現に向けて、各地域におけるデジタル技術を活用した新たな取組が進展しており、これらに対応したセキュリティ対策（セキュリティ・バイ・デザイン等）が必要不可欠。
- 分かりやすい情報発信や対策の導入の加速を支援する政策を実施し、地域・中小企業におけるリテラシーの底上げを図っていくべき。

[5] サイバー警察局・サイバー特別捜査隊の新設による官民連携・国際連携の推進

1. 背景及び課題

➢ サイバー空間の安全・安心を確保するため、警察として、深刻化するサイバー空間の脅威に適切に対処できる態勢の整備に加え、国内外の多様な主体と手を携え、社会全体でサイバーセキュリティ向上のための取組を強力に推進することが必要。

2. 取組の概要

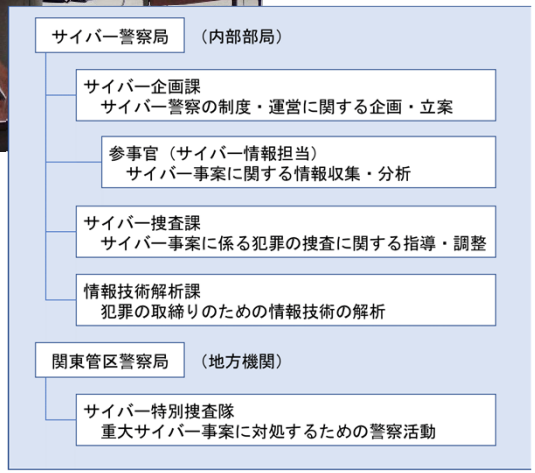
① 手法

✓ 警察庁にサイバー警察局を設置し、警察庁内各局や国内外の多様な主体と連携し、サイバー政策の推進における中心的な役割を担わせる。

✓ 関東管区警察局にサイバー特別捜査隊を設置し、外国捜査機関等との国際共同捜査へ積極的に参画するなど、重大サイバー事案の対処を担わせる。

② 取組によって期待される成果・効果[新規施策]

✓ 本取組により、深刻化するサイバー空間の脅威に適切に対処できる態勢を整備するとともに、国内外の多様な主体と手を携え、社会全体でサイバーセキュリティを向上させるための取組を強力に推進。



■ 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

➢ サイバー攻撃は官民・個人を問わず、あらゆる主体がターゲットになる上、国境がない。サイバー犯罪は従来の犯罪に比べて、「誰でも被害者になり得る」、「どこからでも攻撃が可能」という点において、極めて対応が難しい「高度な犯罪」であり、官民連携と国際連携を強力に推進する必要。

➢ 外国捜査機関との国際共同捜査の円滑な進展が期待でき、我が国のサイバーセキュリティ、特にアトリビューションを高める上で重要。

➢ 多様な人材を積極的に登用して、日本独自の情報源を持つことが国際連携において不可欠。

[6] 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

➢ 世界各国におけるサイバーセキュリティの能力構築を支援することは、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の確保、当該国の健全なサイバー空間の利用の促進、サイバー空間全体の安全確保等に資するため必要。

2. 取組の概要

① 手法

✓ **日ASEANサイバーセキュリティ政策会議の実施**

ASEAN各国・事務局を含めた能力構築支援策の協議、関係組織との調整を実施。

✓ **AJCCBCにおける各種演習等の実施**

タイに構築した「日ASEANサイバーセキュリティ能力構築センター」(AJCCBC)を活用し、各国政府機関・重要インフラ事業者等に対する実践的サイバー防御演習等を実施。

✓ **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の実施**

経済産業省、IPA、米国、EU等が連携して演習を実施。

✓ **JICAと連携した外国捜査機関等に対する支援の実施**

JICAと連携して、ODA対象国を対象とした課題別研修等を実施。

② 取組によって期待される成果・効果

✓ インド太平洋地域の政府関係者及び重要インフラ事業者の能力の底上げ。

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（イメージ）

（令和３年12月　サイバーセキュリティ戦略本部決定）

①世界全体へのセキュリティリスクの低減
②邦人や日本企業の活動の安定の確保
③情報の自由な流通や法の支配を基本原則とする我が国の立場への理解の浸透
④我が国産業等の現地展開を進める基盤の形成
⑤自由で開かれたインド太平洋等への寄与

開発途上国の多様なニーズに応じた効果的な支援を図るため、関係省庁間及び官民による連携を緊密化

■ 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

➢ サプライチェーンの関係諸国のセキュリティ水準向上が不可欠。将来の日本における産業発展の基盤作りのためにも、特に、経済的にますます密接な関係になるインド太平洋地域の国々のCSIRTやセキュリティ技術者と良い関係を築き、同地域におけるセキュリティ能力向上に向けた積極的な支援を実施しつつ、セキュリティ分野のリーダーシップを日本が発揮していくべき。

➢ 同志国との関係強化は、同地域の安全保障に資する重要な国際貢献ともなり、日本国のサイバー防衛に係る取組としても重要。

➢ 日本発のユニークな切り口で、独自の教育プログラムを提供すること等を通じて、緊密に連携できる関係構築に努めていくべき。

2部 サイバーセキュリティに関する情勢

- サイバーセキュリティに関する情勢について、サイバーセキュリティ戦略（以下「戦略」という。）の事項に沿って整理
- 戦略において、サイバーセキュリティに関する経営層の意識改革、安全保障環境の変化、東京大会に向けた取組から得られた知見等の活用及び研究開発・人材育成・リテラシー等について、内容の充実化を図り、また2021年度に発生したサイバーセキュリティインシデントについて総括

経済社会の活力の向上及び持続的発展

コーポレートガバナンスの観点での経営層の認識

・国内企業の経営層のサイバーセキュリティに関する認識には、大きな変化がみられない。
例：「経営会議等で審議される」割合は、2014年以降、3割台で推移

・他国と比較しても、経営層の意識に大きなギャップがある。
例：「経営層のトップダウン指示が対策実施のきっかけ」米55% 日22%

・金銭支払いに係る判断を迫るランサムウェア被害は増加傾向。
例：警察への被害報告は146件（2021年）、下期では前年同時期4倍に増

⇒企業内・企業外（投資家とのコミュニケーション含む）で被害や対策に関する情報が共有されず重大なリスクが見過ごされるおそれ。

中小企業・サプライチェーン対策

・中小企業の対策実施状況にも、大きな変化がみられない。
例：「サイバーセキュリティ対策の必要性を感じたことがない」と回答する企業の割合は約2割（5年前の調査から大きな変化なし）

・背景として、そもそもの意識・リテラシーの問題に加えて、発注元企業や仕入れ先のサイバーセキュリティ対策実施に係る義務づけや要請が進んでいないことも挙げられている。
例：要請時の課題　対策費用の負担57%　下請法等の法令への抵触19%

・国内でも、大企業の下請け企業が被害に遭い、サプライチェーン全体の停止に至るなど、事業運営に影響を与える事例も。

国民が安全で安心して暮らせるデジタル社会の実現

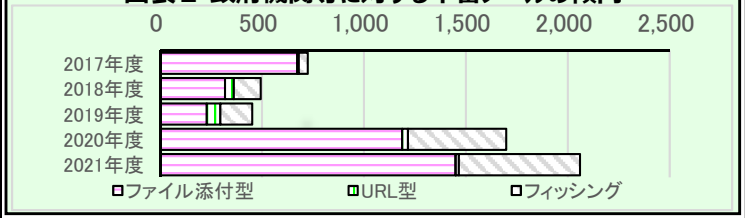
政府機関等に対する攻撃の高度化・巧妙化

政府機関等におけるテレワークの拡大等で利用するソフトウェアの増加に伴い、緊急で対策が必要な脆弱性等の情報提供件数が増加（図表１）。2021年度の不審メールは、マルウェア「Emotet」により、ファイル添付型及びフィッシングが2020年度に続いて活発化（図表２）。

図表１　GSOC※5が情報提供したソフトウェアの脆弱性情報等の件数

年度	2018年度	2019年度	2020年度	2021年度
情報提供件数	290	284	381	598

図表２ 政府機関等に対する不審メールの傾向



サイバーセキュリティインシデント

・ランサムウェアによるコロニアルパイプライン社のシステム停止(2021/5)
・クラウドサービス障害による自治体サービスの一時停止(2021/9)
・金融機関による断続的なシステム障害(～2022/2)
・マルウェア「Emotet」による感染拡大(2022/2以降)
・トンガ諸島の海底火山噴火に伴う海底ケーブル損傷(2022/1) 等

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
バイデン政権はサイバーセキュリティを国家安全保障に関わる最優先事項と位置づけ
・国家のサイバーセキュリティ改善に関する大統領令発出（2021/5）
・官民情報共有の枠組みである、共同サイバー防衛協力（JCDC）を設立(2021/8)
・民間セクターから政府へのサイバー事案の報告義務化に関する法案の可決（2022/3）

英国
・国家サイバー戦略2022の公表（2021/12）
ビジョン：強靭で繁栄するデジタルUKの構築やサイバーパワーに不可欠な技術優位の確保を含む５本柱を提示

EU
・NIS2指令の修正案を採択（2021/12）
※指令対象の全セクターにわたるサイバーセキュリティリスク管理措置報告義務のベースライン等を設定

豪州
・2021年セキュリティ法改正（2021/12, 22/3）
※重要インフラの定義拡大や拡大箇所の重要インフラ資産の登録及び当該資産に対するインシデント報告義務・政府支援措置を定義

中国
・米国政府と民間セクターのネットワークに対し、最も広範かつ活動的で執拗なサイバー諜報脅威と評価
※2022年版の米国インテリジェンスコミュニティの年次脅威評価書による

横断的施策

サイバーセキュリティ分野の研究開発

・トップカンファレンスでの論文発表は、米国・中国・ドイツが上位を占める状況に変化はない。例：日本の研究機関を含む論文は6件

・ただし、暗号研究のカンファレンスでは、日本も一定の存在感。また、NISTの耐量子計算機暗号の標準化に向けた選定作業（現在Round 3）には、国内の研究機関が関与。

・国内で、サイバーセキュリティ分野への活用が期待される研究開発ファンディングの動きが進展。他国も同様。

IT・サイバーセキュリティ人材

・デジタル分野、特にサイバーセキュリティ分野で、人材確保の需要だけではなく、現時点で専門的な知識や業務経験を有しない人材へのリスキリングに対する需要が増大。
例：雇用主が求めるデジタルスキル：サイバーセキュリティ 2位（39%）

・他方、本分野に限らず、我が国ではOJT以外の人材投資が進まない傾向。雇用者・労働者双方の意識に課題。
例：社外学習・自己啓発を行わない個人の割合 46%
労働者：仕事が忙しい55%　費用がかかる29%　家事・育児25%
雇用者：本業に支障をきたす57%　教育内容が実践的でない24%

国民の意識・行動

・サイバー空間に参画する層は、特に高齢者や子どもにも拡大。他方、一部では自覚なくインターネットを利用している可能性。

・こうした動向を踏まえ、脅威の動向も変化。特に高齢者を狙ったフィッシング被害が急増。不安も増している。
例：不在通知偽SMS消費生活相談件数　2019⇒2020（70歳以上割合）
3,800件⇒8,500件（18%⇒28%）

・高齢者や子どもは、家庭の関与や倫理教育の受講経験、視聴するメディアなどが異なるため、方法論は要検討。

１．経済社会の活力の向上及び持続的発展 ～DX with Cybersecurityの推進～

※ リテラシーの定着・向上は4. に纏めて記載。

	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	➢ 「経営可視化ツール」Web版の公開 ➢ 東証「コーポレートガバナンス・コード」附属文書へのサイバーセキュリティ対応の必要性の反映 ➢ 「デジタルガバナンス・コード」への反映、「DX認定制度」「DX銘柄・注目企業」の基準に活用（インセンティブ）	➢ 「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」と連携し、中小企業対策強化、経営層への情報発信、産学官連携の促進、地域SECUNITYの形成促進などを実施。 ➢ 「お助け隊サービス審査登録制度」を開始（12サービス登録）。SC3で利用勧奨。 ➢ 「SECURITY ACTION」を中小企業向け補助金の申請要件等に位置づけ（インセンティブ）	➢ データマネジメント・フレームワーク策定 ➢ IoTに関し日本発の考え方に基づく国際規格の発行
評価	サイバー攻撃被害のリスクが高まりつつある中、上記の取組を更に推進する前提として、コーポレートガバナンスにおける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根本的な取組が必要である。 その上で、サプライチェーンや地域を通じた対策の広がりを更に推進する観点から、現場レベルの取組を進めるに当たって参考となるリソース（先進事例の横展開、ガイドライン等）の整備・活用促進が必要である。		
今年度の新たな取組	➢ 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の策定や「重要インフラにおける安全基準等策定指針」の改訂等、経営層のコミットメントに関連する各種取組の進捗も踏まえつつ、「サイバーセキュリティ経営ガイドライン」の改訂を実施する ➢ 関係省庁が協働し、サイバーセキュリティ経営の位置づけ強化に向けた検討を進める	➢ 物資やサービスの安定供給に支障が生じることのないよう、中小企業等におけるサイバーセキュリティ対策を支援[経済対策] ➢ 取引先への対策の支援（IT導入補助金により、お助け隊サービスの利用を支援） ・要請に係る関係法令の適用関係の整理 [経済対策] ➢ 地域SECUNITYの強化支援及び存在を可視化するマップの公表 ➢ クラウドの適切な設定に関する利用者・提供者に向けたガイドラインの策定	➢ 信頼性のある検証事業者を可視化する制度の創設 ➢ CYNEX：コミュニティの深化・信頼醸成（FY2023～本格稼働）

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	➢「政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針」の策定 ➢ 国民目線にたった利便性向上のため、全地方公共団体によるマイナポータルへの接続実現 ➢ 電気通信事業者を通じて利用者への注意喚起を行う取組「NOTICE」を実施	➢ 近年のサイバーセキュリティ対策の動向等を踏まえた、統一基準群の改定 ➢ 第４期第一GSOCの稼働・運用、効果的かつ効率的な横断的監視及び政府機関等とGSOCの連携推進 ➢ セキュリティ評価制度(ISMAP)に関し、統一的なセキュリティ要求基準に基づいたクラウドサービスに対する追加登録・更新審査の実施	➢ 安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント及び対処態勢の整備、防御基盤の強化等、第４次行動計画に基づく各取組を着実に実施

評価

安全・安心なサイバー空間の利用に向けて、情報発信、技術基盤及び能力向上・周知啓発等のあらゆる観点からの取組を実施し、引き続き<u>サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバーセキュリティ対策を推進</u>。

統一基準群の改定に当たり、クラウドサービスの利用拡大や多様な働き方を踏まえたセキュリティ対策等の強化が図られた。
第４期GSOCシステム構築により、政府機関のクラウド利用の拡大に対応した政府横断的なサイバーセキュリティ強化が図られた。

重要インフラの第４次行動計画に基づく取組については、今後も関係省庁等の積極的な取組を継続し、一層推進するとともに、経済社会活動の相互依存関係の深化が進んでいることを踏まえ、<u>障害対応体制を抜本的に強化する等、同計画の改定に向けた取組を実施することが必要</u>である。

今年度の新たな取組	➢ ナショナルサート機能の強化 ➢「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の策定 ➢ サイバー警察局・特別捜査隊の新設による官民連携・国際連携の推進 ➢ 電気通信ネットワークの安全性・信頼性を確保するための技術実証を実施	➢ 政府情報システムに求められる新たなセキュリティ対策を踏まえた次期統一基準群の骨子策定 ➢ 第５期GSOCシステムの構築に向けた検討 ➢ ISMAPに関し、クラウドサービス利用拡大に向けた新たな仕組みの導入	➢ 第４次行動計画の改定(重要インフラのサイバーセキュリティに係る行動計画) ➢ 改定された計画に基づく、５つの施策群（障害対応体制の強化等）の着実な実施 ➢ サイバーインシデントに係る事故調査の体制整備に向けた実証事業の実施

３．国際社会の平和・安定及び我が国の安全保障への寄与

	「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
昨年度の取組例	➢ DFFT（信頼性のある自由なデータ流通）に関し、2021年G20ローマ・サミットにおいても、その理念のもとに国際的なルール作りを主導することの重要性を発信 ➢ サイバー空間における法の支配を推進するため、国際的なルール及び規範作りに積極的に貢献	➢ 国家の強靱性の確保のため、防衛関連技術の防護等を継続実施 ➢ 抑止力の向上として、サイバー防衛能力の抜本的強化に向けた取組を実施 ➢ 状況把握力の強化に向けて、主要国のサイバー攻撃対処や国家の関与が疑われるようなサイバー攻撃等の情報収集・分析等を実施	➢ 被害が急増するランサムウェア攻撃に対応するための多国間会合に積極的に参加し、多国間で協力してその抑止に効果的に取り組む機運の醸成に寄与するなど、国際協調・協力を推進 ➢ 新たな「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」に基づく取組を実施
評価	外国関係機関との緊密な連携を図り、自由・公正かつ安全なサイバー空間の確保に向けて取り組んでいる一方で、サイバー攻撃の脅威は多様化・複雑化していることから、引き続き同盟国・同志国との緊密な連携を図り、国際ルールや規範の着実な実践を推進するとともに、我が国の防御力・抑止力・状況把握力を強化することが必要である。 また、能力構築支援は基本方針を踏まえ、ASEAN地域における成果・経験をもとに、インド太平洋地域に支援対象を拡大するなど、今後も積極的に取り組む必要がある。		
今年度の新たな取組	➢ 各二国間協議や国連などにおける多国間協議を通じ、関係各国との国際協力へ貢献 ➢ サイバー空間における国際法の適用や国際的なルール・規範づくりに関する議論への積極的な関与 ➢ 我が国の基本理念に沿う新たな国際ルール・規範づくりへの積極的貢献	➢ 我が国の安全保障上の利益を守るため、サイバー攻撃に対する国家の強靱性を確保の推進 ➢ 我が国の防御力、抑止力、状況把握力の継続強化	➢ 知見の共有・政策調整、平時からのサイバー脅威の情報の共有及び能力構築支援の推進 ➢ 開発途上国向けの能力構築支援について、基本方針に基づいた積極的な取組の推進

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	➢ 技術検証体制の構築に向けた検討 ➢ CYNEX：システム基盤を活用した国産セキュリティ製品のテスト環境提供に向けたトライアル ➢ 量子暗号通信の基盤技術（長距離化・中継等）の研究開発	➢ プラス・セキュリティ補充カリキュラム例（部課長級向け）の策定 ➢ CYNEX：システム基盤を活用した演習基盤オープン化に向けたトライアル ➢ 「デジタル人材育成プラットフォーム」：DXリテラシー標準の策定、ポータルサイト「マナビDX」の立上げ	➢ 高等学校「情報Ⅰ」新設に向けた教師・生徒向けコンテンツの充実等 ➢ 「テレワークセキュリティガイドライン」全面改定（中小向けチェックリスト） ➢ サイバーセキュリティ月間：OSや無線LANルータ事業者等と連携
評価	安全保障の観点を含め、実践的な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。 研究振興施策が産学官に広く活用されるよう取り組む必要。	資格制度の活用促進を含め、実践的な対処能力を持つ人材育成に向けて取組を一層強化する必要。 民間事業者によるプログラムの市場形成や教育機関の取組の把握・強化が必要。	従来の普及啓発に留まらず、こどもや高齢者等を対象とする施策の充実が必要。 ↓ 現行のアクションプランを見直し、取組の重点化を図る。
今年度の新たな取組	➢ サイバーセキュリティ分野への活用が期待される研究開発ファンディングについて、産学官での活用を促進 ➢ CYNEX：コミュニティの深化・信頼醸成とシステムの強化（FY2023～本格稼働） ➢ 耐量子計算機暗号等に関するガイドライン策定、CRYPTREC暗号リストの全面改定 ➢ 量子暗号通信ネットワーク・光地上局テストベッドの整備	➢ 「デジタル人材育成プラットフォーム」：スペシャリスト等のスキル標準の策定、企業・大学等の提供講座等の掲載 ➢ 大学・高専等の教育機関における取組の把握・発信、取組促進 ➢ 政府機関人材：既存の研修の整理、スキル認定等に資格試験を活用する仕組みの検討 ➢ 「実践的サイバー防御演習」を受講困難な地方公共団体向けに改良・提供。	➢ 「意識・行動強化プログラム」の見直し ➢ 地域の窓口等に関する一元的可視化、ステークホルダーの連携促進 ➢ 高齢者等向けに講習会を実施する「デジタル活用支援推進事業」について、サイバーセキュリティに関する講座の追加に向けた検討 ➢ 児童・生徒、保護者・教員等向けの出前講座「e-ネットキャラバン」の推進

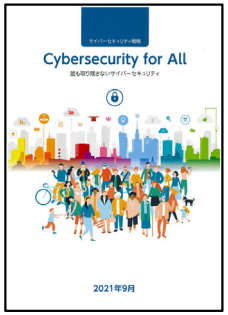
５．推進体制

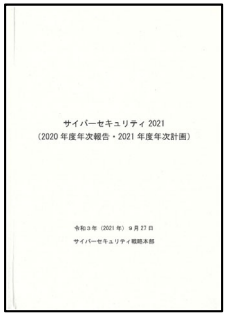
昨年度の実績

- 内閣サイバーセキュリティセンターを中心に、関係機関とのパートナーシップに基づく国内外のインシデント及びサイバー攻撃に関する情報の共有を行うとともに、国際担当者間の会合やIWWNの分析レポートの情報発信により、総合的分析機能の強化を推進。
- 戦略の趣旨を国内外の関係者に向け、効果的に発信し、十分な理解を得ることを目的に、戦略のカラーパンフレット及びサイバーセキュリティ2021の冊子を制作。内閣官房及び関係府省庁において、戦略のカラーパンフレットやサイバーセキュリティ2021の冊子を活用する等して、各種セミナーでの説明等を通じて、我が国のサイバーセキュリティ政策の情報発信を実施。
- 国際協調の重要性の観点から、戦略や開発途上国に対する能力構築支援の基本方針等について、各国サイバーセキュリティ当局及び駐日各国大使館に共有するとともに、NISCのウェブサイトや国連ポータルサイトに掲載する等、我が国のサイバーセキュリティ政策の取組状況を国内外へ積極的に情報発信を実施。

評価

サイバーセキュリティ戦略　サイバーセキュリティ2021





我が国のサイバーセキュリティ政策の国内外の関係者への更なる浸透を図るため、引き続き取り組むことが重要。今後もコロナ禍を通じて定着した「ニューノーマル」とも呼ばれる新しい生活様式に柔軟に対応するため、オンラインを活用したイベントや電子版での配布を行うなど、様々な事業者や個人へ幅広く周知広報活動を実施する。加えて、戦略で掲げた「Cybersecurity for All ～誰も取り残さないサイバーセキュリティ～」のメッセージを含め、我が国のサイバーセキュリティ政策の理解・浸透を広く行うことが必要不可欠であり、関係機関との一層の連携強化を図り、戦略及びサイバーセキュリティ2022の発信等に取り組むことが求められる。

今年度の取組

- 関係機関の一層の能力強化に向けては、既に構築している仕組みの機能向上を図るとともに、連携体制についても逐次見直しを実施する。
- 全ての主体に関する自律的な取組を促進するため、引き続き戦略及びこれに基づく年次計画等の発信を対外に向けて積極的に行い、我が国のサイバーセキュリティ政策が広く理解浸透するよう取り組む。