

# Sec2023-07-01\_【NISC】「サイバーセキュリティ2023の概要」の要約

≡ 分類	専門員調査資料
≡ 文書ID	Sec2023-07-01
📅 出典更新日	@2023年7月10日
🕒 索引更新日	@2023年7月18日 11:07

## ■要約資料概要

### 要約の趣旨

- サイバーセキュリティ2023で示された施策のうち、中小企業のセキュリティ対策に関係の深い記述の部分を要約したものです。
- 中小企業のサイバーセキュリティ対策を検討する際に、国の方向性として、参考にしてください。
- なお、具体的な検討に当たっては、原本を参照してください。

### 原本

[https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023\\_gaiyou.pdf](https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023_gaiyou.pdf)

<https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023.pdf>

### 要約履歴

2023年7月10日 要約初版

## ■サイバーセキュリティ2023の概要

# サイバーセキュリティ2023の概要

令和5年7月4日  
内閣サイバーセキュリティセンター

令和5年7月4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2023(年次報告・年次計画)」の全体構成

**「サイバーセキュリティ2023(年次報告・年次計画)」の全体構成** 1

➤ **「サイバーセキュリティ戦略」**(令和3年9月28日閣議決定)において、戦略に基づく施策を的確に実施するため、サイバーセキュリティ戦略本部で、**各年度の施策の進捗状況を検証し、次年度の計画に反映**することとしていることを踏まえて、**「サイバーセキュリティ2023」**(=今年度の年次報告・年次計画)を策定。

➤ 今年度は、昨年度の構成等に準拠しつつ、**我が国のこれまでの取組実績や今年度特に強力に取り組む施策等の記述を盛り込む**ことを想定。

➤ また、関連施策の実施に必要な予算の効果的・効率的な配分の実現を図るため**「予算重点化方針(案)」**を策定。

**【参考:サイバーセキュリティ2023 構成】**

<p><b>第1部 サイバーセキュリティ2023のポイント(「エグゼクティブ・サマリー」)</b></p> <p>第1 サイバー空間を巡る昨今の状況変化と情勢、及び政策課題</p> <p>第2 今後の取組の方向性 (これまでの取組実績(レガシー)、今年度特に強力に取り組む施策)</p>	<p><b>【参考条文等】</b></p> <p>■ サイバーセキュリティ基本法(平成26年法律第104号)抄 (所掌事務)</p> <p>第26条 本部は、次に掲げる事務をつかさどる。</p> <p>一 サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。(※年次計画・年次報告)</p> <p>二～四 (略)</p> <p>五 前各号に掲げるもののほか、(略)関係行政機関の経費の見積りの方針(※予算重点化方針(略))に関すること。</p>
<p><b>第2部 サイバーセキュリティに関する情勢</b></p> <p>第1章 経済社会の活力の向上及び持続的発展</p> <p>第2章 国民が安全で安心して暮らせるデジタル社会の実現</p> <p>第3章 国際社会の平和・安定及び我が国の安全保障への寄与</p> <p>第4章 横断的施策</p>	<p>■ サイバーセキュリティ戦略(令和3年9月28日閣議決定)抄</p> <p>5 推進体制</p> <p>今後、本部は、本戦略を的確に実施するため、3年間の計画期間内において、各年度の年次計画を作成するとともに、その施策の進捗状況を検証して、年次報告として取りまとめ、次年度の年次計画へ反映する。</p>
<p><b>第3部 戦略に基づく昨年度の実績、評価及び今年度の取組</b> 略(サイバーセキュリティ2022と同じ構成)</p>	

⇒ 年次報告・年次計画の内容を踏まえつつ、併せて今年度の「予算重点化方針(案)」を策定。

- 「サイバーセキュリティ戦略」（令和3年9月28日閣議決定）において、戦略に基づく施策を的確に実施するため、サイバーセキュリティ戦略本部で、各年度の施策の進捗状況を検証し、次年度の計画に反映することとしていることを踏まえて、「サイバーセキュリティ2023」（＝今年度の年次報告・年次計画）を策定。
- 今年度は、昨年度の構成等に準拠しつつ、我が国のこれまでの取組実績や今年度特に強力に取り組む施策等の記述を盛り込むことを想定。
- また、関連施策の実施に必要な予算の効果的・効率的な配分の実現を図るため「予算重点化方針（案）」を策定。

## 【参考：サイバーセキュリティ2023 目次】

### 第1部 サイバーセキュリティ2023のポイント（「エグゼクティブ・サマリー」）

第1 サイバー空間を巡る昨今の状況変化と情勢、及び政策課題第2 今後の取組の方向性

（これまでの取組実績（レガシー）、今年度特に強力に取り組む施策）

### 第2部 サイバーセキュリティに関する情勢

第1章 経済社会の活力の向上及び持続的発展

第2章 国民が安全で安心して暮らせるデジタル社会の実現

第3章 国際社会の平和・安定及び我が国の安全保障への寄与第4章 横断的施策

### 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

略（サイバーセキュリティ2022と同じ構成）

⇒ 年次報告・年次計画の内容を踏まえつつ、併せて今年度の「予算重点化方針（案）」を策定。

## 【参考条文等】

### サイバーセキュリティ基本法（平成26年法律第104号）抄

（所掌事務）

第26条 本部は、次に掲げる事務をつかさどる。

一 サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。（※年次計画・年次報告）

二～四（略）

五 前各号に掲げるもののほか、（略）関係行政機関の経費の見積りの方針（※予算重点化方針）（略）に関すること。

## サイバーセキュリティ戦略（令和3年9月28日閣議決定）抄

### 5 推進体制

今後、本部は、本戦略を的確に実施するため、3年間の計画期間内において、各年度の年次計画を作成するとともに、その施策の進捗状況を検証して、年次報告として取りまとめ、次年度の年次計画へ反映する。

# ■「サイバーセキュリティ2023(年次報告・年次計画)」概要（第1部エグゼクティブ・サマリー）

## 「サイバーセキュリティ2023(年次報告・年次計画)」概要（第1部エグゼクティブ・サマリー）<sup>[2]</sup>

### 1. サイバー空間を巡る昨今の状況変化と情勢、及び政策課題

#### ○ サイバー空間を巡る昨今の状況変化と情勢

- － 様々な分野・組織で情報システムの利用が拡大。サプライチェーンの多様化・複雑化が進展。生成AIなどの新たな技術等も普及。
- － 一方で、これに伴って、サイバー攻撃の侵入口の増加、セキュリティ対策の不備等によるシステム障害・情報漏えいのリスクの高まり。
- － さらに、安全保障環境が厳しさを増す中で、国家を背景としたサイバー攻撃が平素から行われるようになっている。

#### ○ 昨今の状況変化を踏まえた政策課題

- － サイバー安全保障分野における対応能力を欧米主要国と同等以上に向上させることが必要に。
- － ①各主体による対策の強化・対処能力の向上、②政府による支援等の充実・強化、③国際連携・協力の強化が政策課題に。

### 2. 政策課題を踏まえた今年度特に強力に取り組む施策について（※1）

- － 国家安全保障戦略に基づき、我が国を全方位でシームレスに守るため、サイバー空間における必要な取組を進める。
- － サイバーセキュリティ戦略の「3つの方向性<sup>(※2)</sup>」に基づき、施策を推進していく。推進に当たっては、これまでの我が国における取組実績を整理した上で、これを生かしつつ、今後の取組を進めていくことにも留意。以下の施策について、今年度特に強力に取り組んでいく。

#### (1) 経済社会の活力の向上及び持続的発展 ～DXの推進に向けたリスク対策の強化～

- ✓ これまでICTの利活用に必ずしも積極的ではなかった地域・中小企業における対策の促進
- ✓ サプライチェーンリスクの増大を踏まえたソフトウェアセキュリティの高度化に関する取組強化

#### (2) 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のレジリエンスの向上～

- ✓ 政府統一基準群の改定・定着やサイバー空間における脅威動向の把握等を通じた政府情報システムのレジリエンス向上
- ✓ 重要インフラ分野におけるセキュリティ強化のための取組として、安全基準等策定指針の改定等を通じて、各事業者における組織全体での対応の促進を図るとともに、医療分野をはじめとする各分野ごとの取組強化

#### (3) 国際社会の平和・安定及び我が国の安全保障への寄与 ～同盟国・同志国との国際連携・協力の推進～

- ✓ 日ASEAN友好協力50周年記念会議の開催による官民連携の強化等を通じたインド太平洋地域における能力構築支援
- ✓ 日米豪印における協力、ランサムウェア対策を推進するための同志国間の協力枠組みの推進

（※1）「令和6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。

（※2）DXとサイバーセキュリティの同時推進／公共空間化等が進展するサイバー空間全体を俯瞰した安全・安心の確保／安全保障の観点からの取組強化

## 1. サイバー空間を巡る昨今の状況変化と情勢、及び政策課題

### ○ サイバー空間を巡る昨今の状況変化と情勢

- 様々な分野・組織で情報システムの利用が拡大。サプライチェーンの多様化・複雑化が進展。生成AIなどの新たな技術等も普及。
- 一方で、これに伴って、サイバー攻撃の侵入口の増加、セキュリティ対策の不備等によるシステム障害・情報漏えいのリスクの高まり
- さらに、安全保障環境が厳しさを増す中で、国家を背景としたサイバー攻撃が平素から行われるようになっている。

## ○ 昨今の状況変化を踏まえた政策課題

- サイバー安全保障分野における対応能力を欧米主要国と同等以上に向上させることが必要に。
- ①各主体による対策の強化・対処能力の向上、②政府による支援等の充実・強化、③国際連携・協力の強化が政策課題に。

## 2. 政策課題を踏まえた今年度特に強力に取り組む施策について（※1）

- 国家安全保障戦略に基づき、我が国を全方位でシームレスに守るため、サイバー空間における必要な取組を進める。
  - サイバーセキュリティ戦略の「3つの方向性(※2)」に基づき、施策を推進していく。推進に当たっては、これまでの我が国における取組実績を整理した上で、これを生かしつつ、今後の取組を進めていくことにも留意。以下の施策について、今年度特に強力に取り組んでいく。
1. 経済社会の活力の向上及び持続的発展 ～DXの推進に向けたリスク対策の強化～
    - これまでICTの利活用に必ずしも積極的ではなかった地域・中小企業における対策の促進
    - サプライチェーンリスクの増大を踏まえたソフトウェアセキュリティの高度化に関する取組強化
  2. 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のレジリエンスの向上～
    - 政府統一基準群の改定・定着やサイバー空間における脅威動向の把握等を通じた政府情報システムのレジリエンス向上
    - 重要インフラ分野におけるセキュリティ強化のための取組として、安全基準等策定指針の改定等を通じて、各事業者における組織全体での対応の促進を図るとともに、医療分野をはじめとする各分野ごとの取組強化

### 3. 国際社会の平和・安定及び我が国の安全保障への寄与 ～同盟国・同志国との国際連携・協力の推進～

- ・ 日ASEAN友好協力50周年記念会議の開催による官民連携の強化等を通じたインド太平洋地域における能力構築支援
- ・ 日米豪印における協力、ランサムウェア対策を推進するための同志国間の協力枠組みの推進

(※1) 「令和6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。

(※2) DXとサイバーセキュリティの同時推進／公共空間化等が進展するサイバー空間全体を俯瞰した安全・安心の確保／安全保障の観点からの取組強化

## ■[1] 中小企業のサイバーセキュリティ対策促進

[1] 中小企業のサイバーセキュリティ対策促進		3
<b>1. 背景及び課題</b>	<ul style="list-style-type: none"><li>▶ サプライチェーンの中で比較的弱い中小企業へのサイバー攻撃を經由して、発注元の大企業も被害を受けている実態への取組強化が必要である。</li><li>▶ 他方で、そのリスクを自分事として認識していない、あるいは、何をしてもよく分からない状況にある中小企業や、対策費用や人材の確保に課題を感じている中小企業も多数存在する。</li><li>▶ 中小企業の経営者の意識改革や中小企業が使いやすいセキュリティサービスの普及促進・運用改善、大企業が取引先の中小企業に対してセキュリティ対策の支援・要請を行う際の関係法令の適用関係にかかる懸念の払拭を更に進めていくことが必要である。</li></ul>	
<b>2. 取組の概要</b>	<p>① 手法</p> <ul style="list-style-type: none"><li>✓ 「サイバーセキュリティお助け隊サービス」につき、サービス基準の改定による同サービスの拡充等を通じて、中小企業側の様々なニーズに応え、個々の中小企業の要望に応じたサイバーセキュリティ対策の支援を実現する。</li><li>✓ こうした取組を、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)とも連携して実施し、中小企業への対策の浸透を図る。</li></ul> <p>② 取組によって期待される成果・効果</p> <ul style="list-style-type: none"><li>✓ お助け隊サービスの普及を通じて、中小企業のセキュリティが向上するとともに、中小企業におけるサイバー攻撃被害の実態について、サービス提供事業者を通じて把握することが可能になる。あわせて、関係機関への通報や共有が促進されることも期待される。</li><li>✓ 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)との連携により、産業界全体のサイバーセキュリティ強化が期待される。</li></ul>	
<b>■ 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</b>	<ul style="list-style-type: none"><li>▶ 地域・中小企業のサイバーセキュリティ対策は、日本のセキュリティ対策の重要課題であるが、現状はまだ端緒に手が届き始めた段階である。当面は、政府がけん引役を務め、官民一体となって強力に推進することが必要である。</li><li>▶ 中小企業特有の問題(規模・費用・ノウハウの継承ほか)もあり、そうした問題へのきめ細かい具体的対応が求められる。</li><li>▶ 警察庁の2023年3月16日付報道発表資料「令和4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」を見ると、ランサムウェア攻撃被害の53%が中小企業となっており、サプライチェーンで重要な位置を占める中小企業のサイバーセキュリティ対策は、政府だけでなく、自治体からの支援についても議論が必要である。</li></ul>	

### 1. 背景及び課題

- ・ サプライチェーンの中で比較的弱い中小企業へのサイバー攻撃を經由して、発注元の大企業も被害を受けている実態への取組強化が必要である。
- ・ 他方で、そのリスクを自分事として認識していない、あるいは、何をしてもよく分からない状況にある中小企業や、対策費用や人材の確保に課題を感じている中小企業も多数存在する。

- 中小企業の経営者の意識改革や中小企業が使いやすいセキュリティサービスの普及促進・運用改善、大企業が取引先の中小企業に対してセキュリティ対策の支援・要請を行う際の関係法令の適用関係にかかる懸念の払拭を更に進めていくことが必要である。

## 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」につき、サービス基準の改定による同サービスの拡充等を通じて、中小企業側の様々なニーズに応え、個々の中小企業の要望に応じたサイバーセキュリティ対策の支援を実現する。
- こうした取組を、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）とも連携して実施し、中小企業への対策の浸透を図る。

### ② 取組によって期待される成果・効果

- お助け隊サービスの普及を通じて、中小企業のセキュリティが向上するとともに、中小企業におけるサイバー攻撃被害の実態について、サービス提供事業者を通じて把握することが可能になる。あわせて、関係機関への通報や共有が促進されることも期待される。
- 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）との連携により、産業界全体のサイバーセキュリティ強化が期待される。



⇒サプライチェーンで重要な位置を占める中小企業のサイバーセキュリティ対策は、政府だけでなく、自治体からの支援についても議論が必要である。



⇒東京都事業も連携することで一層の効果が期待できる

## ■[2] サプライチェーンリスクを踏まえたソフトウェアセキュリティの高度化に関する取

# 組

[ 2 ] サプライチェーンリスクを踏まえたソフトウェアセキュリティの高度化に関する取組		4
<b>1. 背景及び課題</b>	<ul style="list-style-type: none"><li>サイバー空間とフィジカル空間が密接に関係していく世界において、サイバー攻撃のリスクも増大する中、これに対応するための考え方を整理したフレームワークを整備しているところであり、この社会実装を進めることでセキュリティ対策のレベルを向上させることが必要である。</li><li>特に、ソフトウェアを構成する部品情報を管理し、脆弱性管理等に活用可能なSBOM導入の重要性に対する認識が米国を中心に広まっていることから、こうした動きに対応しつつ、SBOMが有するメリットを生かしていくための仕組み作りや様々な分野への普及が重要である。</li><li>通信システムのソフトウェアでのOSSの普及拡大に伴って多発するサイバー攻撃への対処のため、通信分野におけるSBOM導入が急務である。</li></ul>	
<b>2. 取組の概要</b>	<p>① 手法</p> <ul style="list-style-type: none"><li>脆弱性管理の効率化等を図るため、脆弱性情報とSBOMの紐付けを機械的に行う手法の実証など、2022年度までの取組を深化する。</li><li>代表的な通信システムを対象にSBOMを作成・評価するなど、通信分野でのSBOM導入に向けた取組を進める。</li></ul> <p>② 取組によって期待される成果・効果</p> <ul style="list-style-type: none"><li>SBOMに関する知見の整理、契約モデル等のツールの整備等を通じた、安心してソフトウェア活用を行うことができる環境の構築、ひいては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。</li><li>通信分野でのSBOM導入により、OSS等のソフトウェア部品の脆弱性が確認された際の対応の迅速化等が期待される。</li></ul>	
<b>■ 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</b>	<ul style="list-style-type: none"><li>脆弱性管理等に活用可能なSBOM導入の重要性に対する認識が米国を中心に急速に広まっていることから、脆弱性情報とSBOMの機械的な紐付け実証を経て、早期実用展開に繋げていくことが重要である。</li><li>2021年5月12日付の米大統領令で米国政府は既にSBOM重視の姿勢を打ち出しており、2022年5月には「日米豪印サイバーセキュリティ・パートナーシップ」でSBOMを含めた協力が打ち出されていることから、日本国内だけでなく、同盟国・友好国とも協調した取組が必要である。</li><li>国内外でSBOM導入をはじめとしたソフトウェア・サプライチェーン強化に関する動きが加速されつつあるが、また国内でSBOM管理を実用化している企業は少なく、現状は概念・用語として認知され始めた段階と考えられる。SBOMは、単に脆弱性情報のリスト（部品表）ではなく、バリューチェーン・サプライチェーンに入るための必須要件（国際資格）と考えるべきである。</li></ul>	

## 1. 背景及び課題

- サイバー空間とフィジカル空間が密接に関係していく世界において、サイバー攻撃のリスクも増大する中、これに対応するための考え方を整理したフレームワークを整備しているところであり、この社会実装を進めることでセキュリティ対策のレベルを向上させることが必要である。
- 特に、ソフトウェアを構成する部品情報を管理し、脆弱性管理等に活用可能なSBOM（Software Bill of Materials）導入の重要性に対する認識が米国を中心に広まっていることから、こうした動きに対応しつつ、SBOMが有するメリットを生かしていくための仕組み作りや様々な分野への普及が重要である。
- 通信システムのソフトウェアでのOSS（Open Source Software）の普及拡大に伴って多発するサイバー攻撃への対処のため、通信分野におけるSBOM導入が急務

である。

## 2. 取組の概要

### ① 手法



- 脆弱性管理の効率化等を図るため、脆弱性情報とSBOMの紐付けを機械的に行う手法の実証など、2022年度までの取組を深化する。
- 代表的な通信システムを対象にSBOMを作成・評価するなど、通信分野でのSBOM導入に向けた取組を進める。

## 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、契約モデル等のツールの整備等**を通じた、安心してソフトウェア活用を行うことができる環境の構築、ひいてはあらゆる産業で**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。
- 通信分野でのSBOM導入により、OSS等のソフトウェア部品の脆弱性が確認された際の対応の迅速化等が期待される。



⇒東京都の技術的対策支援として、ゼロトラスト、SASE（Secure Access Service Edge）のフレームワークのネットワーク機能、セキュリティ機能に留まらず、Security by Designの観点から、脆弱性を生まないシステム構築・運用のライフサイクル、及び、ライフサイクルの中でのSBOM等のツールの実証支援も含めることが効果的と思われる

## 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

- 脆弱性管理等に活用可能なSBOM導入の重要性に対する認識が米国を中心に急速に広まっていることから、脆弱性情報とSBOMの機械的な紐付け実証を経て、早期実用展開に繋げていくことが重要である。
- 2021年5月12日付の米大統領令で米国政府は既にSBOM重視の姿勢を打ち出しており、2022年5月には「日米豪印サイバーセキュリティ・パートナーシップ」でSBOMを含めた協力が打ち出されていることから、日本国内だけでなく、同盟国・友好国とも協調した取組が必要である。
- 国内外でSBOM導入をはじめとしたソフトウェア・サプライチェーン強化に関する動きが加速されつつあるが、まだ国内でSBOM管理を実用化している企業は少なく、現状は概念・用語として認知され始めた段階と考えられる。**SBOMは、単に脆弱性情報のリスト（部品表）ではなく、バリューチェーン・サプライチェーンに入るための必須要件（国際資格）と考えるべきである。**

# ■[3] 政府情報システムの防護のための一元的取組

[3] 政府情報システムの防護のための一元的取組		5
<b>1. 背景及び課題</b>	<ul style="list-style-type: none"><li>巧妙化かつ複雑化するサイバー攻撃やICT利活用の進展に伴う未知の脅威が増大する中で、政府情報システムに対するサイバー攻撃リスクが高まっている。これらに迅速に対応するためには、最新の脅威・技術動向を踏まえて政府統一基準を改定し、政府情報システムの情報セキュリティを確保するとともに、サイバー攻撃等に関する情報の収集・分析等を行い、有効な技術や知見を継続的に生み出すことが重要である。一方で、サイバー攻撃等の情報収集・分析に有用なセキュリティ製品・サービスは海外に大きく依存している状態にある。海外事業者のセキュリティ製品に過度に依存することなく、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となっている。</li></ul>	
<b>2. 取組の概要</b>	<ul style="list-style-type: none"><li>① 手法<ul style="list-style-type: none"><li>政府のサイトに対する頻繁なDDoS攻撃やサプライチェーンの脆弱な部分を起点としたサイバー攻撃等のリスクを踏まえ、最新のDDoS攻撃の特徴を踏まえた対策や業務委託先における政府情報の保護に係る対策の強化などを盛り込んだ政府統一基準群の改定を行うとともに、これを踏まえた政府機関等における最新の情報セキュリティ対策の浸透を図る。</li><li>安全性や透明性の検証が可能なセンサーを政府端末に導入して、海外製品に頼らずに端末情報を収集し、得られた情報をNICTのCYNEX（サイバーセキュリティ統合知的・人材育成基盤）に集約・分析を行う。CYNEXに集約された政府端末情報とNICTが長年収集したサイバーセキュリティ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。生成情報は、センサーの導入府省庁のみでなく、政府全体のサイバーセキュリティを統括するNISC、GSOC、デジタル庁等へ共有する。</li></ul></li><li>② 取組によって期待される成果・効果<ul style="list-style-type: none"><li>最新の脅威動向を踏まえた政府統一基準群の反映により、政府機関等におけるインシデントの未然防止及び発生時のレスポンス向上が見込まれる。</li><li>海外製品に過度に依存することなく我が国独自のサイバーセキュリティ関連情報を生成する。</li><li>導入府省庁、NISC、GSOC、デジタル庁等へ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が見込まれる。</li></ul></li></ul>	
<b>■ 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</b>	<ul style="list-style-type: none"><li>広義のCTI（Cyber Threat Intelligence）の自律性の確保は最優先事項と認識している。</li><li>国組織から順次、重要インフラ事業者へと拡大できる仕組みとなることを期待する。</li><li>サイバー攻撃は各国に見られる普遍的現象ではあるが、他方、各国に特有の事情に依存した特徴を有することも考えられる。こうした事態への実効的な対処のため我が国に特化したセキュリティ関連の制度等の構築が喫緊の課題である。</li></ul>	

## 1. 背景及び課題

- 巧妙化かつ複雑化するサイバー攻撃やICT利活用の進展に伴う未知の脅威が増大する中で、政府情報システムに対するサイバー攻撃リスクが高まっている。これらに迅速に対応するためには、**最新の脅威・技術動向を踏まえて政府統一基準を改定し、政府情報システムの情報セキュリティを確保するとともに、サイバー攻撃等に関する情報の収集・分析等を行い、有効な技術や知見を継続的に生み出すことが重要である。**一方で、サイバー攻撃等の情報収集・分析に有用なセキュリティ製品・サービスは海外に大きく依存している状態にある。海外事業者のセキュリティ製品に過度に依存することなく、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となっている。

## 2. 取組の概要

### ① 手法

- 政府のサイトに対する頻繁なDDoS攻撃や**サプライチェーンの脆弱な部分を起点としたサイバー攻撃等のリスクを踏まえ、最新のDDoS攻撃の特徴を踏まえた対策や業務委託先における政府情報の保護に係る対策の強化などを盛り込んだ政**

**府統一基準群の改定を行う**とともに、これを踏まえた政府機関等における最新の情報セキュリティ対策の浸透を図る。

- 安全性や透明性の検証が可能なセンサーを政府端末に導入して、海外製品に頼らずに端末情報を収集し、得られた情報をNICTのCYNEX（サイバーセキュリティ統合知的・人材育成基盤）に集約・分析を行う。CYNEXに集約された政府端末情報とNICTが長年収集したサイバーセキュリティ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。生成情報は、センサーの導入府省庁のみでなく、政府全体のサイバーセキュリティを統括するNISC、GSOC、デジタル庁等へ共有する。



⇒政府機関のサプライチェーンには中小企業も含まれる

## ② 取組によって期待される成果・効果

- 最新の脅威動向を踏まえた政府統一基準群の反映により、政府機関等におけるインシデントの未然防止及び発生時のレジリエンス向上が見込まれる。
- 海外製品に過度に依存することのない我が国独自のサイバーセキュリティ関連情報を生成する。
- 導入府省庁、NISC、GSOC（Govrenment Security Operation Coordination team）、デジタル庁等へ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が見込める。

## ■[4] 医療分野をはじめとする重要インフラ事業者等のサイバーセキュリティ強化

## 1. 背景及び課題

- 重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、官民連携に基づく重要インフラ防護の一層の強化を図る必要がある。
- 特に、医療分野においては、これまで「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきた。しかし、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実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。このため、医療機関における対策強力に推進することが必要である。

## 2. 取組の概要

## ① 手法

- ✓ (重要インフラ分野全般) 行動計画を踏まえつつ、安全基準等策定指針の改定等を通じ、重要インフラ事業者等において、組織統治にサイバーセキュリティを組み入れるための取組が推進され、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応が一層促進されるよう努める。
- ✓ (医療分野) 「医療機関向けセキュリティ教育支援ポータルサイト」を通じたサイバーセキュリティインシデント発生時の相談対応、「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(2023年5月31日改定)に基づく医療機関のシステム・セキュリティ管理者、経営層等の特性に合わせたサイバーセキュリティ対策研修の実施や普及啓発等に取り組む。

## ② 取組によって期待される成果・効果

- ✓ (重要インフラ分野全般) 重要インフラサービスの強靱性を確保し、国民生活や社会経済活動及び安全保障環境に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。
- ✓ (医療分野) 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戦略本部有識者本部員の主な受け止め

- (重要インフラ分野全般) 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律(経済安全保障推進法)及び国家安全保障戦略でも重要インフラ防護の重要性が打ち出されたところであり、これらの法律と戦略に沿った重要インフラのサイバーセキュリティ対策の強化が必要である。
- (医療分野) 医療機関への攻撃が常態化しつつある昨今の状況に鑑みると、国民生活に与える影響が大きい事案となるため、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ることを期待する。

## 1. 背景及び課題

- 重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、官民連携に基づく重要インフラ防護の一層の強化を図る必要がある。
- 特に、医療分野においては、これまで「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきた。しかし、**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実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。このため、医療機関における対策強力に推進することが必要である。**

## 2. 取組の概要

## ① 手法

- (重要インフラ分野全般) 行動計画を踏まえつつ、安全基準等策定指針の改定等を通じ、**重要インフラ事業者等において、組織統治にサイバーセキュリティを組み入れるための取組が推進され、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応が一層促進されるよう努める。**
- (医療分野) 「医療機関向けセキュリティ教育支援ポータルサイト」を通じたサイバーセキュリティインシデント発生時の相談対応、「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(2023年5月31日改定)に基づく医療機関のシステム・セキュリティ管理者、経営層等の特性に合わせたサイバーセキュリティ対策研修の実施や普及啓発等に取り組む。



⇒重要インフラのサプライチェーンには中小企業も含まれ、特に中小企業のサイバーセキュリティ上の脆弱性を低減させることは急務である。経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応が一層促進求められる。

## ② 取組によって期待される成果・効果

- （重要インフラ分野全般）重要インフラサービスの強靱性を確保し、国民生活や社会経済活動及び安全保障環境に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。
- （医療分野）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戦略本部有識者本部員の主な受け止め

- （重要インフラ分野全般）経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）及び国家安全保障戦略でも重要インフラ防御の重要性が打ち出されたところであり、これらの法律と戦略に沿った重要インフラのサイバーセキュリティ対策の強化が必要である。
- （医療分野）医療機関への攻撃が常態化しつつある昨今の状況に鑑みると、国民生活に与える影響が大きい事案となるため、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ることを期待する。

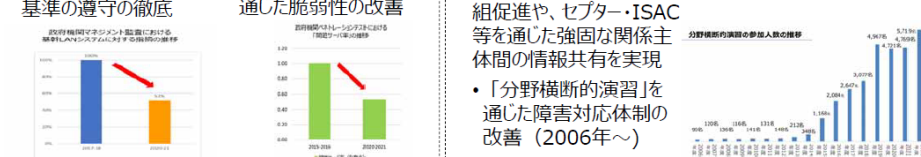
## ■[5] インド太平洋地域における能力構築支援（ASEAN官民連携支援及び島しょ国支援の強化）

<<<<省略>>>>

## ■[6] 日米豪印上級サイバーグループ及びランサムウェア対策多国間会合の枠組みを通じた国際連携<sup>8</sup>

<<<<省略>>>>

## ■第1部（別紙）これまでの取組実績（レガシー）（概要）

第1部（別紙）これまでの取組実績（レガシー）（概要）		9
<p>➢ これまでサイバーセキュリティ分野の幅広い関係者が連携して、制度的な枠組みの策定や官民の協力体制の構築などに取り組んできており、その取組に当たって得られた知見・ノウハウを含め、多様な取組実績が蓄積。</p> <p>➢ セキュリティ施策の検討に当たっては、<u>これまでの取組実績を生かしつつ、取組を進めることが適切。</u></p>		
<b>【これまでの取組実績（レガシー）の具体例】</b>		
○ 制度的な枠組み（サイバーセキュリティ戦略）		
<ul style="list-style-type: none"><li>✓ セキュリティ「コスト」から「投資」への発想転換、「機能保証」、セキュリティ・バイ・デザイン等につき記載(2015年)</li><li>✓ 東京大会の成功とその後の対策を見据えた取組（サイバーセキュリティ対処調整センター）等を記載(2018年)</li><li>✓ “DX with Cybersecurity”、ナショナルサポート機能強化、安全保障面の取組強化等につき記載(2021年)</li></ul>		
○ 政府機関のセキュリティ確保のための取組	○ 重要インフラ分野のセキュリティ確保のための取組	
<ul style="list-style-type: none"><li>✓ 政府統一基準を策定し、<ul style="list-style-type: none"><li>• 適用対象に、独立行政法人等を追加(2016年)</li><li>• CDN・EDR等の強固な対策等を追記(2021年)</li></ul></li><li>✓ セキュリティ対応状況等を詳細に把握する、高度なマネジメント監査やペネトレーションテスト等を実現<ul style="list-style-type: none"><li>• マネジメント監査を通じた基準の遵守の徹底</li><li>• ペネトレーションテストを通じた脆弱性の改善</li></ul></li></ul>	<ul style="list-style-type: none"><li>✓ 重要インフラ行動計画を策定し、<ul style="list-style-type: none"><li>• 化学・クレジット・石油の3分野を追加(2015年)</li><li>• 空港分野を追加(2017年)</li><li>• 任務保証の考えを踏まえた安全かつ持続的提供、官民一体の取組推進を記載(2022年)</li></ul></li><li>✓ 「分野横断的演習」の取組促進や、セクター・ISAC等を通じた強固な関係主体間の情報共有を実現<ul style="list-style-type: none"><li>• 「分野横断的演習」を通じた障害対応体制の改善(2006年～)</li></ul></li></ul>	

- これまでサイバーセキュリティ分野の幅広い関係者が連携して、制度的な枠組みの策定や官民の協力体制の構築などに取り組んできており、その取組に当たって得られた知見・ノウハウを含め、多様な取組実績が蓄積。
- セキュリティ施策の検討に当たっては、これまでの取組実績を生かしつつ、取組を進めることが適切。

### 【これまでの取組実績（レガシー）の具体例】

#### ○ 制度的な枠組み（サイバーセキュリティ戦略）

- セキュリティ「コスト」から「投資」への発想転換、「機能保証」、セキュリティ・バイ・デザイン等につき記載(2015年)

- 東京大会の成功とその後の対策を見据えた取組（サイバーセキュリティ対処調整センター）等を記載(2018年)
- **“DX with Cybersecurity”、ナショナルサート機能強化、安全保障面の取組強化等につき記載(2021年)**

## ○ 政府機関のセキュリティ確保のための取組

- 政府統一基準を策定し、
  - 適用対象に、独立行政法人等を追加 (2016年)
  - CDN・EDR等の強固な対策等を追記 (2021年)
- セキュリティ対応状況等を詳細に把握する、高度なマネジメント監査やペネトレーションテスト等を実現
  - マネジメント監査を通じた基準の順守の徹底
  - ペネトレーションテストを通じた脆弱性の改善

## ○ 重要インフラ分野のセキュリティ確保のための取組

- 重要インフラ行動計画を策定し、
  - 化学・クレジット・石油の3分野を追加(2015年)
  - 空港分野を追加(2017年)
  - 任務保証の考えを踏まえた安全かつ持続的提供、官民一体の取組推進を記載(2022年)
- 「分野横断的演習」の取組促進や、セプター・ISAC等を通じた強固な関係主体間の情報共有を実現
  - 「分野横断的演習」を通じた障害対応体制の改善 (2006年～)

# ■第1部・第2部サイバーセキュリティに関する情勢

第1部・第2部 サイバーセキュリティに関する情勢			10
<b>社会経済活動や国民生活におけるサイバー空間への依存度の高まり</b> システム構築・運用におけるクラウド等の活用の拡大、サプライチェーンの多様化・複雑化、デジタル化による新たな技術・サービスの進展 <b>サイバー攻撃の深刻化・巧妙化</b> ランサムウェアによる被害件数の増加（2021年度146件、2022年度230件）、Emotetの活動再開や新たな手口による感染拡大、国家関与が疑われる攻撃や標的型攻撃の増加			
<b>経済社会の活力の向上及び持続的発展</b> <b>コーポレートガバナンスの観点での経営層の認識</b> ・国内企業の経営層の認識に大きな変化なし。 例「取組を主にIT部門などに任せている」との回答割合が過半数。 ・他国と比べ、経営層とIT部門等との意識にギャップが存在。 例「経営層のトップダウン指示が対策実施のきっかけ」米5割、日2割。 ・海外では、セキュリティリスクを自社で評価する時代から社外・外部からも評価される時代へ。 経営層に対策の必要性に関する意識改革を行うための「気づき」を与えることが重要。 <b>中小企業・サプライチェーン対策</b> ・中小企業の対策実施状況に大きな変化なし。 例「サイバーセキュリティ対策の必要性を感じない」との回答割合が約4割。 ・引き続き増加傾向のランサムウェア被害の約半数が中小企業。 ・対策不足の中小企業がサプライチェーンに存在することがリスク。 ・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。 ・安全なサプライチェーン確保のための技術面からのセキュリティ強化を進める必要。	<b>国民が安全で安心して暮らせるデジタル社会の実現</b> <b>経済社会基盤を支える各主体における情勢</b> ① 政府機関等 ・インシデント件数が年々増加。 (2020年度117件、2021年度207件、2022年度266件) ・GSOCによる政府機関等への脆弱性情報等の提供も増加。 (2020年度381件、2021年度598件、2022年度630件) ・第一、第二GSOCの緊密連携等が必要。 ・政府端末情報を活用したセキュリティ情報の収集・分析等に取組む必要。 ② 重要インフラ ・国内外の重要インフラ分野において、システム障害や情報流出の事例が多数発生 例 医療機関等へのランサムウェア攻撃や、通信障害が発生。 ・サイバー攻撃の被害を想定した事業継続計画の立案が重要。 ・事業継続計画の実効性の点検等が必要。 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・向上の必要。 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 ・G7広島サミット、大阪・関西万博への知見の活用が重要。	<b>国際社会の平和・安定及び我が国の安全保障への寄与</b> <b>国外の動き（諸外国の国際動向）</b> <b>米国</b>  ・バイデン政権初の「国家サイバーセキュリティ戦略」を公表（2023年3月） ・重要インフラ・サイバーインシデント報告法（2022年3月成立）に基づく対応の推進。 <b>英国</b>  「国家サイバー戦略2022」に基づき、国家サイバー諮問委員会(NCAB)を設置し、初会合を実施（2022年11月） <b>EU</b>  当局の権限・監視を強化する「NIS2指令」の発効（2023年1月） 大手通信会社等へのサイバー攻撃で個人情報等が大規模流出（2022年10～11月） <b>豪州</b>  豪州サイバーセキュリティ戦略の見直しを発表（2022年12月） <b>中国</b>  サイバー空間における国際協力に関する白書を公表（2022年11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。	
<b>横断的施策</b>			
<b>サイバーセキュリティ分野の研究開発</b> 生成AIの普及等に加え、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。 例 米国「国家サイバー戦略」では、積極的な女子学生・経歴のための研究開発及び実証を国家が主導・推進する旨を記載。 ・研究の裾野を広げる観点からの産学官工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。 ・量子技術等、中長期的な技術トレンドを視野に入れた対応。	<b>IT・サイバーセキュリティ人材</b> ・人材確保の需要の高まりに加え、企業や組織が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クリソク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」で、サイバーセキュリティ人材を含むデジタル推進人材につき、2026年度末までに230万人の育成を目指すことを提示。 ・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。	<b>国民の意識・行動</b> デジタル化が着実に進展する一方、インターネット利用時に不安を感じる人の比率が増加傾向。 例「サポート詐欺」に係る相談件数が2023年1月に過去最高(IPA) ・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アプローチとともに、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。	

● **社会経済活動や国民生活におけるサイバー空間への依存度の高まり**

- システム構築・運用におけるクラウド等の活用の拡大、サプライチェーンの多様化・複雑化、デジタル化による新たな技術・サービスの進展

● **サイバー攻撃の深刻化・巧妙化**

- ランサムウェアによる被害件数の増加（2021年度146件、2022年度230件）、Emotetの活動再開や新たな手口による感染拡大、国家関与が疑われる攻撃や標的型攻撃の増加

**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認識に大きな変化なし。
  - 例 「取組を主にIT部門などに任せている」との回答割合が過半数。
- 他国と比べ、経営層とIT部門等との意識にギャップが存在。
  - 例 「経営層のトップダウン指示が対策実施のきっかけ」 米5割、日2割。
- 海外では、セキュリティリスクを自社で評価する時代から社外・外部からも評価される時代へ。

● ↓



- **経営層に対策の必要性に関する意識改革を行うための「気づき」を与えることが重要。**
- **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大きな変化なし。
    - 例 「サイバーセキュリティ対策の必要性を感じない」との回答割合が約4割
  - 引き続き増加傾向のランサムウェア被害の約半数が中小企業。
    - 対策不足の中小企業がサプライチェーンに存在することがリスク。
- ↓
  - **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。**
  - **安全なサプライチェーン確保のための技術面からのセキュリティ強化を進める必要。**

## 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**
  - インシデント件数が年々増加。
    - （2020年度117件、2021年度207件、2022年度266件）
  - GSOCによる政府機関等への脆弱性情報等の提供も増加。
    - （2020年度381件、2021年度598件、2022年度630件）
- ↓
  - 第一、第二GSOCの緊密連携等が必要。
  - 政府端末情報を活用したセキュリティ情報の収集・分析等に取り組む必要。
- **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 医療機関等へのランサムウェア攻撃や、通信障害が発生。

- サイバー攻撃の被害を想定した事業継続計画の立案が重要
- 事業継続計画の実効性の点検等が必要。
- 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・向上の必要。
- 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
  - G7広島サミット、大阪・関西万博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と国外の動き (諸外国の国際動向)

### 国外の動き (諸外国の国際動向)

<<<<省略>>>>

## 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の普及等に加え、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。
  - 例 米国「国家サイバー戦略」では、積極的なリスク防止・軽減のための研究開発及び実証を国家が受動・推進する旨を記載
- ↓
- 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。
  - 量子技術等、中長期的な技術トレンドを視野に入れた対応。

### IT・サイバーセキュリティ人材

- **人材確保の需要の高まりに加え、企業や組織が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ク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」で、サイバーセキュリティ人材を含むデジタル推進人材につき、2026年度末までに230万人の育成を目指すことを提示。
- ↓
- **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、インターネット利用時に不安を感じる人の比率が増加傾向。
  - 例「サポート詐欺」に係る相談件数が2023年1月に過去最高（IPA）
- ↓
- **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アプローチとともに、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。



⇒ 【本編p.42より抜粋】

各年代におけるスマートフォン保有率が8割を超え、社会経済におけるデジタル化が着実に進展する一方、インターネット利用時に不安を感じる人の比率が増加傾向にあり、いわゆる「サポート詐欺」に係るIPAへの月間相談件数が2023年1月には過去最高を記録31するなど、安心・安全なサイバー空間の利用には、未だ課題が見られる。

また、一部の年代においてはインターネット利用率がスマートフォン保有率を下回る調査結果が出る等、サイバー空間を利用している自覚のない利用者があることがうかがえるほか、組織についてもランサムウェア被害報告の過半数が中小企業・組織からであること等を踏まえると、サイバーセキュリティ対策の必要性が全ての人・組織に理解されるためには、訴求すべき対象に応じたよりきめ細かなアプローチとともに、各主体が密接に連携し、協働することが必要となってくると考えられる。

このため、重点対象と具体的な取組、各主体の連携強化を企図して改訂された「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がある。

# ■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

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)		
<b>1. 経済社会の活力の向上及び持続的発展</b>		
	<b>経営層の意識改革</b>	<b>地域・中小企業対策</b>
<b>昨年度の取組例</b>	<ul style="list-style-type: none"> <li>▶ サプライチェーン・リスクへの役割・責任の明確化等に関し、「サイバーセキュリティ経営ガイドライン」を改訂</li> <li>▶ 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を公表</li> <li>▶ 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の取りまとめ・公表</li> </ul>	<ul style="list-style-type: none"> <li>▶ 地域SECURITYによる、産官学連携の研修やインシデント演習等を実施</li> <li>▶ 「SECURITY ACTION」制度の周知を図るとともに補助金の拡大を実施</li> <li>▶ 「中小企業の情報セキュリティ対策ガイドライン」の普及を進めるとともに、「サイバーセキュリティお助け隊」サービスの創設等を踏まえて改訂</li> </ul>
		<b>サプライチェーン等の信頼性確保</b>
<b>評価</b>	<ul style="list-style-type: none"> <li>▶ 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</li> <li>▶ 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</li> <li>▶ 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</li> </ul>	
<b>今年度の取組例</b>	<ul style="list-style-type: none"> <li>▶ 「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を支援</li> <li>▶ 関係省庁が協働し、コーポレートガバナンスの一環としてのサイバーセキュリティ経営の位置付け強化に向けた検討を推進</li> </ul>	<ul style="list-style-type: none"> <li>▶ 「サイバーセキュリティお助け隊サービス」の利活用を推進する普及啓発</li> <li>▶ クラウドサービス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普及促進</li> <li>▶ 「インターネットの安全・安心ハンドブック Ver. 5.00 &lt;中小組織向け抜粋版&gt;」の周知</li> <li>▶ 地域SECURITYの更なる強化支援</li> </ul>
		<ul style="list-style-type: none"> <li>▶ ソフトウェア部品の構成表であるSBOMの活用に向けた実証実験を実施</li> <li>▶ IoTシステムのセキュリティ保証やサプライチェーンのトラスト構築等に係る「サイバー・フィジカル・セキュリティ対策基盤」の研究開発・社会実装を推進</li> <li>▶ NICTの「CYNEX」を活用した攻撃情報の分析、人材育成の実施</li> </ul>

## 1. 経済社会の活力の向上及び持続的発展

### 昨年度の取組

- 経営層の意識改革
  - サプライチェーン・リスクへの役割・責任の明確化等に関し、「**サイバーセキュリティ経営ガイドライン**」を改訂
  - 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を公表
  - 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の取りまとめ・公表



⇒

※「プラス・セキュリティ知識補充講座カリキュラム例」（2022年6月NISC）（[https://security-portal.nisc.go.jp/dx/pdf/plussecurity\\_curriculum.pdf](https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf)）

※「サイバー攻撃被害に係る情報の共有・公表 ガイダンス」（2023年3月8日METI）（[https://www.soumu.go.jp/main\\_content/000867112.pdf](https://www.soumu.go.jp/main_content/000867112.pdf)）

- 地域・中小企業対策
  - 地域SECURITYによる、産官学連携の研修やインシデント演習等を実施
  - 「SECURITY ACTION」制度の周知を図るとともに補助金の拡大を実施
  - 「中小企業の情報セキュリティ対策ガイドライン」の普及を進めるとともに、「サイバーセキュリティお助け隊」サービスの創設等を踏まえて改訂
- サプライチェーン等の信頼性確保
  - ソフトウェア部品の構成表であるSBOMの活用に向けた実証実験を実施
  - IoTシステムのセキュリティ保証やサプライチェーンのトラストリスト構築等に係る「サイバー・フィジカル・セキュリティ対策基盤」の研究開発・社会実装を推進
  - NICTの「CYNEX」を活用した攻撃情報の分析、人材育成の実施

## 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

## 今年度の取り組み例

- 経営層の意識改革

- 「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を支援
- 関係省庁が協働し、コーポレートガバナンスの一環としてのサイバーセキュリティ経営の位置付け強化に向けた検討を推進



⇒

※ 「サイバーセキュリティ対策情報開示の手引き」 (2019年6月総務省)  
([https://www.soumu.go.jp/main\\_content/000630516.pdf](https://www.soumu.go.jp/main_content/000630516.pdf))

- 地域・中小企業対策
  - 「サイバーセキュリティお助け隊サービス」の利活用を推進する普及啓発
  - クラウドサービス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普及促進
  - 「インターネットの安全・安心ハンドブック Ver 5.00<中小組織向け抜粋版>の周知
  - 地域SECURITYの更なる強化支援



⇒ 【本編p.45より抜粋】

【今年度の取組】

経済産業省において、サービス内容や価格に関する一定の基準を満たすものとして登録された「サイバーセキュリティお助け隊サービス」の利活用を推進する普及啓発を行う。

総務省において、2021年に策定した「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」及び2022年に策定した「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」について、利用者向けの分かりやすいコンテンツの作成等の普及促進を進める。

総務省・経済産業省において、引き続き、地域SECURITYにおけるセミナーやインシデント演習等の開催を含め、コミュニティの自発的な運営に向けた取組を支援する。

内閣官房において、「インターネットの安全・安心ハンドブックVer 5.00<中小組織向け抜粋版>」の周知を実施する。

- サプライチェーン等の信頼性確保

- SBOMの脆弱性管理や、情報通信分野へのSBOM導入に向けた検討
- 情報セキュリティサービス審査登録制度に「機器検証サービス」を追加
- NICTの「CYNEX」の本年度運用開始に向けたシステム構築、コミュニティ形成

## ■ 2. 国民が安全で安心して暮らせるデジタル社会の実現

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 (2/4)			
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	<ul style="list-style-type: none"> <li>ナショナルサート機能を強化し、「サイバー攻撃被害に係る情報の共有・公表ガイドランス」を取りまとめ・公表するなど、被害の未然防止のための対応を強化</li> <li>サイバー警察局・特別捜査隊を設置</li> <li>「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版の改定</li> <li>マイナポータルで引越手続や旅券のオンライン申請に係るサービスを開始</li> </ul>	<ul style="list-style-type: none"> <li>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）の運用開始及び政府統一基準群の改定を踏まえた「SBDマニュアル」の改定</li> <li>政府機関等によるSNS等の外部サービスの利用拡大を踏まえ、「外部サービス申合せ」を策定</li> <li>GSOCの監視対象基盤の更なる拡大や高度化及び次期GSOCシステムの構築に向けた調査に係る検討を実施</li> </ul>	<ul style="list-style-type: none"> <li>「重要インフラのサイバーセキュリティに係る行動計画」の策定</li> <li>組織統治やサプライチェーンリスク等の観点から安全基準等策定指針の改定に向けた検討を実施</li> <li>「情報共有の手引書」を活用した情報共有体制の更なる改善</li> <li>ランサムウェア攻撃等の対応に係る「分野横断的演習」の実施</li> </ul>
評 価	<ul style="list-style-type: none"> <li>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が必要</li> <li>ISMAPクラウドサービスリストの充実化、制度運用合理化の検討等、政府情報システムのセキュリティ確保のための取組を進めることが必要</li> <li>クラウドサービスやSNS等の外部サービスの利用拡大を踏まえ、統一的な基準を整備するとともに、監査等を通じて、各政府機関等が必要な改善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</li> <li>重要インフラの行動計画に基づく取組につき、今後も関係省庁等の積極的な取組を継続し、一層の推進を図る必要</li> </ul>		
今年度 の取組例	<ul style="list-style-type: none"> <li>サイバー警察局・特別捜査隊による国内外の多様な主体との連携強化</li> <li>金融機関や利用者への注意喚起等の積極的な情報発信・情報共有</li> <li>「NOTICE」の取組の拡充・延長に向けた法案の提出の検討</li> <li>ナショナルサート強化の体制・環境整備</li> </ul>	<ul style="list-style-type: none"> <li>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政府統一基準群の改定、個別マニュアルの改定検討</li> <li>次期GSOCシステムの構築に向けた検討の継続</li> <li>国産セキュリティソフトにより政府端末に係るサイバーセキュリティ情報を収集し、NICTのCYNEXにおいて集約・分析</li> </ul>	<ul style="list-style-type: none"> <li>安全基準等策定指針の改定</li> <li>行動計画に基づく、5つの施策群（情報共有体制の強化等）に関する取組の継続</li> <li>水道分野や金融分野等における関係ガイドライン改定の検討</li> </ul>

### 昨年度の取組例

- 安全・安心な環境構築、 デジタル改革との一体的推進
  - ナショナルサート機能を強化し、「サイバー攻撃被害に係る情報の共有・公表ガイドランス」を取りまとめ・公表するなど、被害の未然防止のための対応を強化
  - サイバー警察局・特別捜査隊を設置
  - 「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版の改定
  - マイナポータルで引越手続や旅券のオンライン申請に係るサービスを開始
- 政府機関等の取組

- 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）の運用開始及び政府統一基準群の改定を踏まえた「SBDマニュアル」の改定
- 政府機関等によるSNS等の外部サービスの利用拡大を踏まえ、「外部サービス申合せ」を策定
- GSOCの監視対象基盤の更なる拡大や高度化及び次期GSOCシステムの構築に向けた調査に係る検討を実施
- 重要インフラの取組
  - 「重要インフラのサイバーセキュリティに係る行動計画」の策定
  - 組織統治やサプライチェーンリスク等の観点から安全基準等策定指針の改定に向けた検討を実施
  - 「情報共有の手引書」を活用した情報共有体制の更なる改善
  - ランサムウェア攻撃等の対応に係る「分野横断的演習」の実施

## 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が必要
- ISMAPクラウドサービスリストの充実化、制度運用合理化の検討等、政府情報システムのセキュリティ確保のための取組を進めることが必要
- クラウドサービスやSNS等の外部サービスの利用拡大を踏まえ、統一的な基準を整備するとともに、監査等を通じて、各政府機関等が必要な改善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
- 重要インフラの行動計画に基づく取組につき、今後も関係省庁等の積極的な取組を継続し、一層の推進を図る必要

## 今年度の取組例

- 安全・安心な環境構築、デジタル改革との一体的推進
  - サイバー警察局・特別捜査隊による国内外の多様な主体との連携強化
  - 金融機関や利用者への注意喚起等の積極的な情報発信・情報共有
  - 「NOTICE」の取組の拡充・延長に向けた法案の提出の検討



- ナショナルサート強化の体制・環境整備
- 政府機関等の取組
  - 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政府統一基準群の改定、個別マニュアルの改定検討
  - 次期GSOCシステムの構築に向けた検討の継続
  - 国産セキュリティソフトにより政府端末に係るサイバーセキュリティ情報を収集し、NICTのCYNEXにおいて集約・分析
- 重要インフラの取組
  - 安全基準等策定指針の改定
  - 行動計画に基づく、5つの施策群
    - （情報共有体制の強化等）に関する取組の継続
  - 水道分野や金融分野等における関係ガイドライン改定の検討

## ■ 3. 国際社会の平和・安定及び我が国の安全保障への寄与

<<<<省略>>>>

## ■ 4. 横断的施策

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	<ul style="list-style-type: none"> <li>経済安全保障重要技術育成プログラムの研究開発ビジョン(第一次)における「領域横断・サイバー空間領域」の支援対象に不正機能検証技術等が示された</li> <li>CRYPTREC暗号リストの改定</li> </ul>	<ul style="list-style-type: none"> <li>「プラス・セキュリティ知識補充講座カリキュラム例」の策定</li> <li>受講者のニーズ等に応じコースを再編した上で、「CYDER」を実施</li> <li>政府機関における政府デジタル人材の人材像を定義し、研修・資格試験の内容の整理等を実施</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>指導用の教材作成や、普及啓発実施主体向けのセミナーを実施</li> <li>「サイバーセキュリティ意識・行動強化プログラム」の見直しを実施</li> </ul>
評価	<ul style="list-style-type: none"> <li>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</li> <li>中長期的なトレンドを捉え、短期的な成果にとらわれないこと、取り組むことが必要</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>政府機関における攻撃被害が多発し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</li> </ul>	<ul style="list-style-type: none"> <li>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、取組状況のフォローアップを踏まえた「意識・行動強化プログラム」の見直し及びそれに基づく取組の重点化や強化が必要</li> </ul>
今年度の取組例	<ul style="list-style-type: none"> <li>「5Gセキュリティガイドライン」の普及啓発の実施及び見直しの検討</li> <li>ユーザの意図に反したスマートフォンアプリ挙動の実態把握に係る課題整理</li> <li>CRYPTREC暗号リストに掲載された暗号技術の監視等を実施</li> </ul>	<ul style="list-style-type: none"> <li>SC3と連携した、「プラス・セキュリティ」の普及に向けた取組</li> <li>大学・高専へモデルとなるカリキュラムの普及・展開等を実施</li> <li>「デジタル田園都市国家構想総合戦略」を踏まえた公共職業訓練の実施</li> <li>「デジタル社会の実現に向けた重点計画」に基づいた、政府デジタル人材の研修等の見直し</li> </ul>	<ul style="list-style-type: none"> <li>「意識・行動強化プログラム」の着実な実施に向け、関係省庁と連携した取組を実施</li> <li>「サイバーセキュリティ対策9か条」や「インターネットの安全・安心ハンドブック」等、各種コンテンツの利活用を促進</li> </ul>

## 昨年度の取組例

- 研究開発の推進
  - 経済安全保障重要技術育成プログラムの研究開発ビジョン(第一次)における「領域横断・サイバー空間領域」の支援対象に不正機能検証技術等が示された
  - CRYPTREC暗号リストの改定
- 人材の確保、育成、活躍促進
  - 「プラス・セキュリティ知識補充講座カリキュラム例」の策定
  - 受講者のニーズ等に応じコースを再編した上で、「CYDER」を実施
  - 政府機関における政府デジタル人材の人材像を定義し、研修・資格試験の内容の整理等を実施



⇒

※ 「CYDER」 (NICT) (<https://cyder.nict.go.jp/course/>)

- 普及啓発、リテラシーの定着・向上
  - 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

- 指導用の教材作成や、普及啓発実施主体向けのセミナーを実施
- 「サイバーセキュリティ意識・行動強化プログラム」の見直しを実施



⇒

※「デジタル活用支援推進事業」（総務省、委託先：デロイトトーマス社）（<https://www.digi-katsu.go.jp/>）

## 評価

- 研究開発の推進
  - 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
  - 中長期的なトレンドを捉え、短期的な成果にとらわれることなく、取り組むことが必要
- 人材の確保、育成、活躍促進
  - 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
  - 政府機関における攻撃被害が多発し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
- 普及啓発、リテラシーの定着・向上
  - 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、取組状況のフォローアップを踏まえた「意識・行動強化プログラム」の見直し及びそれに基づく取組の重点化や強化が必要

## 今年度の取組例

- 研究開発の推進
  - 「5Gセキュリティガイドライン」の普及啓発及び見直しの検討
  - ユーザの意図に反したスマートフォンアプリ挙動の実態把握に係る課題整理
  - CRYPTREC暗号リストに掲載された暗号技術の監視等を実施
- 人材の確保、育成、活躍促進
  - **SC3と連携した、「プラス・セキュリティ」の普及に向けた取組**

- 大学・高専へモデルとなるカリキュラムの普及・展開等を実施
- 「デジタル田園都市国家構想総合戦略」を踏まえた公共職業訓練の実施
- 「デジタル社会の実現に向けた重点計画」に基づいた、政府デジタル人材の研修等の見直し
- 普及啓発、リテラシーの定着・向上
  - 「意識・行動強化プログラム」の着実な普及に向けた取組を実施
  - 「サイバーセキュリティ対策9か条」や「インターネットの安全・安心ハンドブック」等、各種コンテンツの利活用を促進