資料２

東京オリンピック・パラリンピック競技大会等の大規模国際イベントにおける サイバーセキュリティの確保に向けた取組の今後の活用方策に関する有識者会議 第５回会合

新たなサイバーセキュリティ戦略

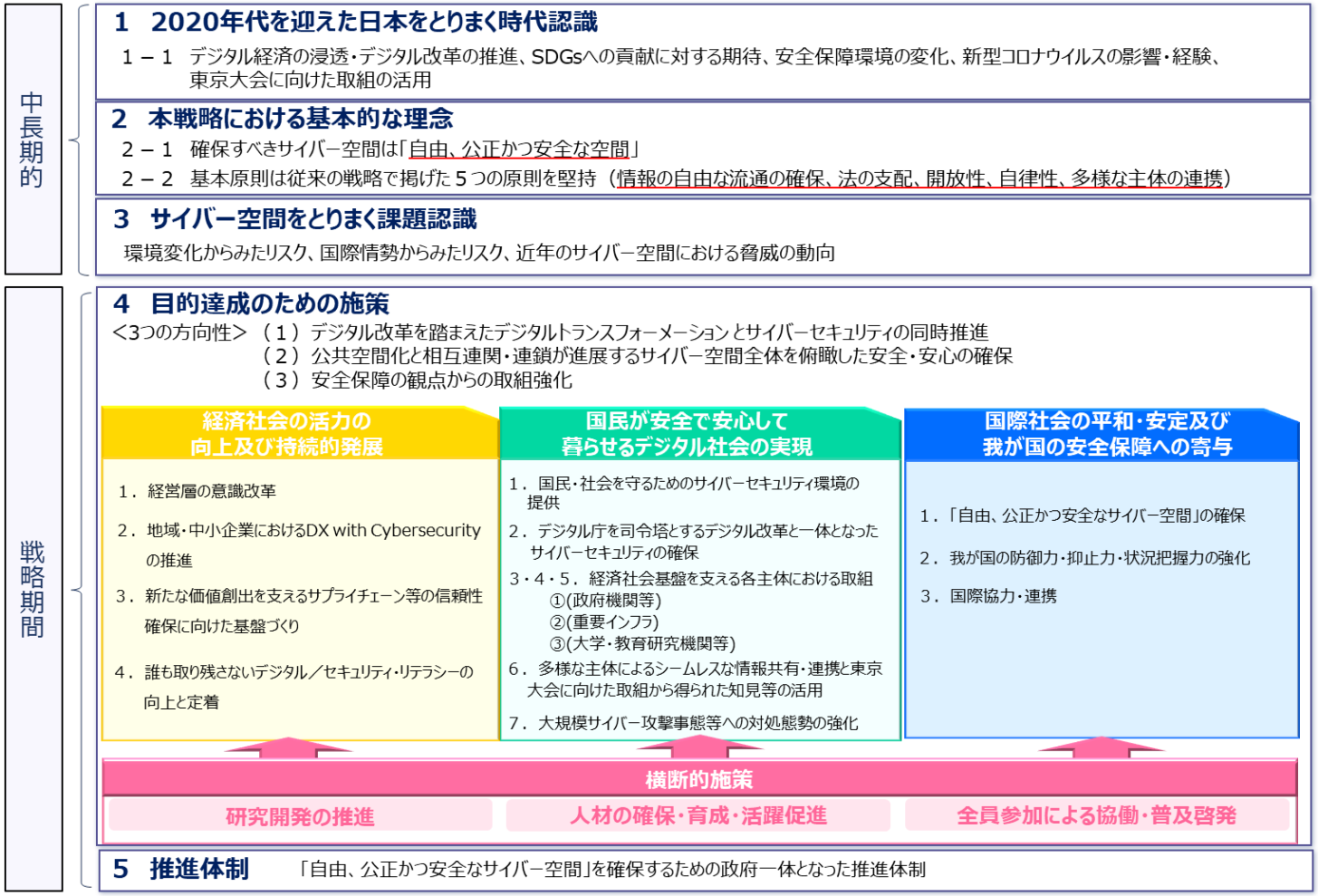
2021年10月

内閣官房　内閣サイバーセキュリティセンター

新たなサイバーセキュリティ戦略

○　９月28日の閣議において、2020年代初めの今後３年間にとるべき諸施策の目標や実施方針を示すものとして、新たなサイバーセキュリティ戦略を決定。

○　当該戦略では、有識者会議での討議等を踏まえ、東京大会等におけるサイバーセキュリティの確保に向けた取組の活用に当たっての方針・方向性を明記。



新たなサイバーセキュリティ戦略の構成

新たなサイバーセキュリティ戦略の課題と方向性

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験
テレワーク、オンライン教育等の進展
- 厳しさを増す**安全保障**環境
- **SDGｓ**への
デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**に向けた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映
国家間競争の場に
安全保障上の課題にも
- 不適切な利用は
国家分断、人権の阻害へ
- 官民の取組の
活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖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

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

国民が安全で安心して暮らせるデジタル社会の実現

課題認識と方向性 － 公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心確保 －

- サイバー空間の**公共空間化**、**相互連関・連鎖の深化**、**サイバー攻撃の組織化・洗練化**。

国は、様々な主体と連携しつつ、①自助・公助による**自律的なリスクマネジメントが講じられる環境づくり**と、②持ち得る手段の全てを活用した**包括的なサイバー防御の展開**等を通じて、**サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築**し、国全体のリスク低減、レジリエンス向上を図る。

主な具体的施策（１）国民・社会を守るためのサイバーセキュリティ環境の提供

① 安全・安心なサイバー空間の利用環境の構築

- サプライチェーン管理のためのガイドライン策定や産業界主導の取組、IoT、5G等の新技術実装に伴う安全確保
- 利用者保護の観点から安全かつ信頼性の高い通信ネットワークを確保するための方策の検討

② 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）

- 政府機関・重要インフラ事業者等向けにクラウド利用の際に考慮すべきセキュリティルール策定
- ISMAPの取組等の民間展開による一定のセキュリティが確保されたクラウド利用の促進
- 信頼性が高く、オープンかつ使いやすい高品質クラウドの整備の推進

③ サイバー犯罪への対策

- サイバー空間を悪用する犯罪者やトレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等の摘発を推進し、実空間と変わらぬ安全・安心を確保
- 警察におけるサイバー事案対処体制の強化

④ 包括的なサイバー防御の展開

- サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化（対処官庁のリソース結集と連携強化、サイバーセキュリティ協議会等の関係機関との連携による官民連携・国際連携強化）
- 包括的サイバー防御のための環境整備（脆弱性対策、技術検証、制御システムのインシデント原因究明機能の整備等）

⑤ サイバー空間の信頼性確保に向けた取組

- 個人情報や知的財産を保有する主体への支援
- 経済安保の視点を踏まえたITシステム・サービスの信頼性確保（政府調達、重要なインフラ、国際海底ケーブル等）

国民が安全で安心して暮らせるデジタル社会の実現

主な具体的施策（２）デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

- デジタル庁が策定する国等の情報システム整備方針にサイバーセキュリティの基本的な方針も示し実装を推進。
- 情報と発信者の真正性等を保障する制度を企画立案し、普及を促進。ISMAP制度を運用し、民間利用の推奨。

主な具体的施策（３）経済社会基盤を支える各主体における取組

①　政府機関等

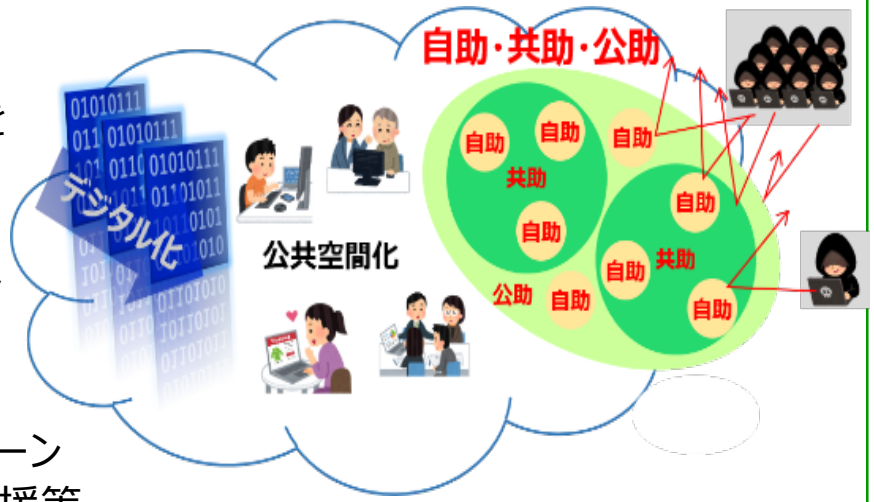
- 政府統一基準群に基づく対策の推進や監査・CSIRT訓練・GSOCによる監視等を通じた政府機関全体としてのセキュリティ水準の向上。
- クラウドサービスの利用拡大を見据えた政府統一基準群の改定・運用やクラウド監視に対応したGSOC機能の強化。

②　重要インフラ

- 「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」を改定し、環境変化に対応した防護の強化や経営層のリーダーシップを推進。
- 地方公共団体情報システムの標準化や行政手続きのオンライン化等に対応したガイドラインの見直し等の諸制度整備。

③　大学・教育研究機関等

- リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策を含む、先端情報を保有する大学等への対策強化支援等。



主な具体的施策（４）多様な主体による情報共有・連携と大規模サイバー攻撃事態等への対処体制強化

- 東京大会での対処態勢や運用により得た知見やノウハウを広く全国の事業者等に対する支援として積極活用。
- 平素から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化。

サイバーセキュリティ戦略における記載内容（東京大会等に向けた取組の今後の活用方策関係）

4　目的達成のための施策

4.2.1　国民・社会を守るためのサイバーセキュリティ環境の提供

（中略）サイバー空間の変容を背景に、インシデントの影響が複雑かつ広範囲に伝播するリスクが顕在化している状況を踏まえ、各サービスの提供主体が、直接の利用者のみならずその先の利用者の存在も見据えつつ、相互連関・連鎖全体を俯瞰してリスクマネジメントの確保に務めることがスタンダードとなるよう、国は、関係主体と連携して環境づくりに取り組んでいく。

国民の安全・安心の根幹に関わる経済社会基盤の防護については、これを担う各主体が役割に応じた機密性、可用性、完全性を確実に保証することが基本であるが、前述のサイバー空間の変容に加え、近年の攻撃手法の組織化・洗練化などの脅威に晒されるなど厳しい環境下では、自助、共助の取組だけで対応することは益々困難となっていることから、国が主体的に関係機関とも連携を図りつつ、攻撃者の視点も踏まえ、持ち得る全ての手段を活用して包括的なサイバー防御を講ずることによって、国全体のリスクの低減とレジリエンスの向上に精力的に取り組む。

(4)　包括的なサイバー防御の総合的な調整を担うナショナルサート機能等の強化

国は、深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまで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。具体的には、対処官庁のリソース結集と連携強化を通じて対処能力の向上と対処に係る一体性・連動性を図るとともに、サイバー関連事業者との連携強化によって組織・分野横断的に影響が波及し得る事案の情報収集や初動を含めた対処調整の迅速化を図る。また、サイバーセキュリティ協議会やサイバーセキュリティ対処調整センター、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関をはじめとした情報共有体制間や海外関係機関との連携を一層推進することで、官民間・国際間での情報共有と対処調整の円滑化を図る。さらに、発生した事案等から得られた課題や気づきを踏まえ、国は、官民を含む関係者と総合的な調整を行い、適時に制度化など必要な政策の立案・措置を講じていく。

これらの取組により、官民を含む関係者からの適宜迅速な情報収集と被害の全体像の迅速な把握力を強化するとともに、国の防御に関する情報発信の訴求力と網羅性の向上、攻撃の特性や深刻度、個々の分野の事情に応じた系統的できめ細かい対応、防御の実効性向上に資する経営から現場レベルまでの様々なニーズに応じた適時な注意喚起や情報提供、サイバー攻撃の無害化等を模索するグローバルなオペレーションへの協力、さらに、円滑な総合調整による迅速な政策立案等の更なる推進を図り、国全体の包括的な防御力を向上する。

サイバーセキュリティ戦略における記載内容（東京大会等に向けた取組の今後の活用方策関係）

4　目的達成のための施策

4.2.6　多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

サイバー空間におけるリスクの高まりを踏まえ、国は、リスクへの感度とレジリエンスを高め、実効性かつ即応性のあるサイバー攻撃対処に資する、時間的・地理的・分野的にシームレスな情報共有・連携を推進し、平時から大規模サイバー攻撃事態等に対する即応力を確保する。

また、新たな攻撃にも国全体として網羅的な対処が可能となるよう、国はナショナルサート（CSIRT/CERT）の枠組み整備の一環として、東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見、ノウハウを活かすことで、大阪・関西万博をはじめとする大規模国際イベント時だけではなく、平時における我が国のサイバーセキュリティ全体の底上げを進める。また、国は東京大会での運用で得られた知見、ノウハウを適切な形で国際的にも共有していく。

(2) 包括的なサイバー防御に資する情報共有・連携体制の整備

サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備の一環として、国はサイバーセキュリティ協議会やサイバーセキュリティ対処調整センター、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関をはじめとした情報共有体制間の連携を進め、外部との連携や調整の在り方について具体的に検討する。

また、国は東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見やノウハウを、東京大会の運営を支える事業者等にとどまらず、広く全国の事業者等におけるサイバーセキュリティ対策への支援等として積極的に活用することで、大阪・関西万博をはじめとする大規模国際イベント時から、平時に至る我が国のサイバーセキュリティ全体の底上げを進める。

4.3.3　国際協力・連携

(1) 知見の共有・政策調整

（略）我が国のサイバーセキュリティ政策等に関する国際的な情報発信も強化し、東京大会における我が国の経験等も他国に共有し国際貢献を果たす。