サイバーセキュリティセミナー ’22 in 東北
基調講演

我が国のサイバーセキュリティ戦略について

内閣サイバーセキュリティセンター

2022年12月

サイバーセキュリティ政策の推進体制

内 閣　内閣総理大臣

国家安全保障会議（NSC）

緊密連携

サイバーセキュリティ戦略本部 (2015.1.9 ｻｲﾊﾞｰｾｷｭﾘﾃｨ基本法により設置) ※

本部長　内閣官房長官

副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣

閣僚本部員
- 国家公安委員会委員長
- 総務大臣
- 経済産業大臣
- デジタル大臣
- 外務大臣
- 防衛大臣
- 国務大臣のうちから、内閣総理大臣が指定する者

有識者本部員

遠藤 信博	日本電気(株)特別顧問
後藤 厚宏	情報セキュリティ大学院大学学長
田中 孝司	KDDI(株)代表取締役会長
中谷 和弘	東京大学大学院法学政治学研究科教授
野原 佐和子	(株)イプシ・マーケティング研究所代表取締役社長
前田 雅英	東京都立大学名誉教授
宮澤 栄一	(株)デジタルハーツホールディングス取締役会長
村井 純	慶應義塾大学教授

※ 構成員は、令和4年6月現在。

緊密連携

デジタル庁

連携

サイバーセキュリティ協議会

官民の多様な主体が相互に連携した、より早期の段階での、サイバーセキュリティの確保に資する情報の迅速な共有等

（事務局）

内閣官房 内閣サイバーセキュリティセンター（NISC） (2015.1.9 内閣官房組織令により設置)

〔各省のサイバーセキュリティ施策の統一性保持のための総合調整〕

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）

副センター長（内閣審議官）

協力

＜重要インフラ所管省庁＞

〔所管重要インフラ事業におけるサイバーセキュリティの確保〕

- 金融庁（金融機関）
- 総務省（地方公共団体、情報通信）
- 厚生労働省（医療、水道）
- 経済産業省（電力、ガス、化学、クレジット、石油）
- 国土交通省（鉄道、航空、物流、空港）

＜その他関係省庁＞

文部科学省（セキュリティ教育）等

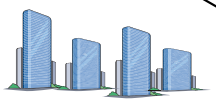
協力

閣僚本部員６省庁

〔各省の所掌に基づくサイバーセキュリティ施策の実施〕

- 警察庁（ｻｲﾊﾞｰ犯罪取締り）
- デジタル庁（ﾃﾞｼﾞﾀﾙ社会形成）
- 総務省（通信・ﾈｯﾄﾜｰｸ政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

重要インフラ事業者等



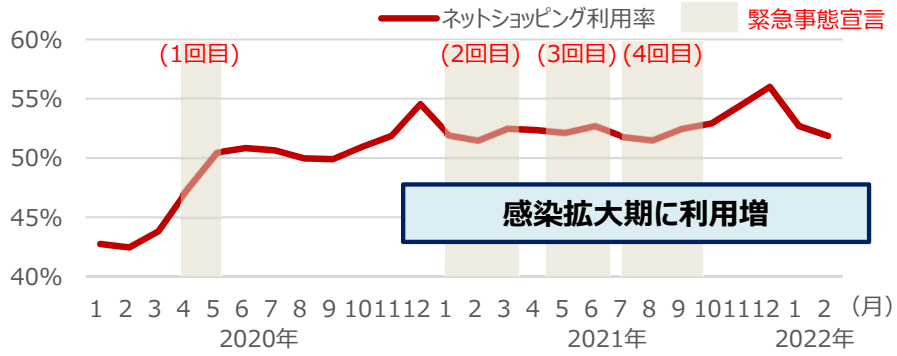
政府機関（各府省庁）

企業

個人

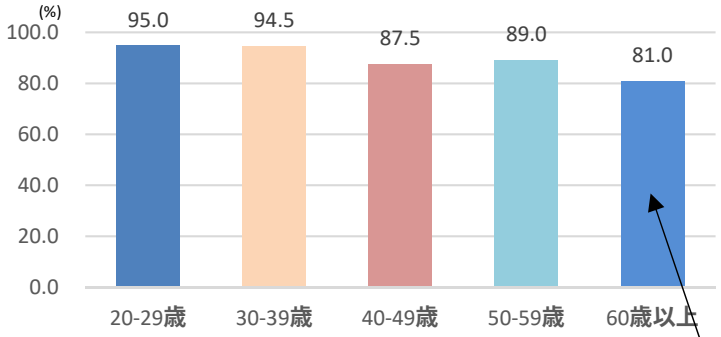
サイバー空間を巡る環境変化

1. ネットショッピング利用世帯の割合



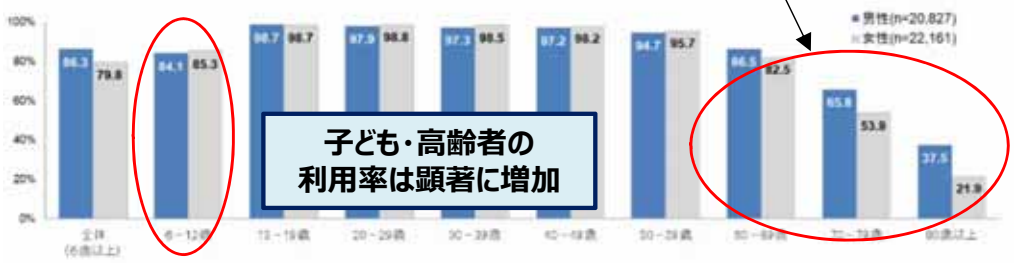
出典：総務省「家計消費状況調査」を基にNISC作成

2. 年齢別スマートフォン保有率



出典：総務省(2021)「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」

3. 年齢別インターネット利用率



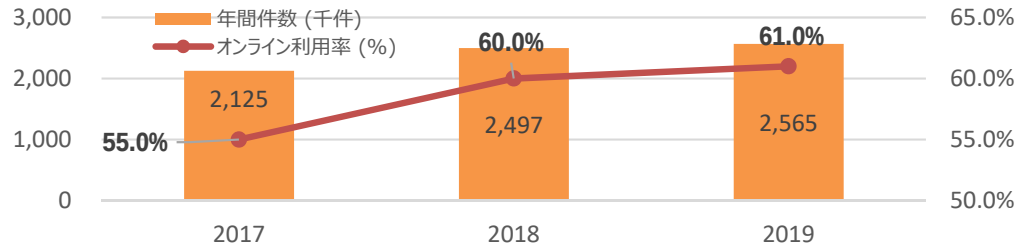
出典：総務省「令和3年通信利用動向調査」を基にNISCで作成

サイバー空間を利用している自覚のないまま脅威に遭遇し、被害に遭っているシニア層が存在する可能性

4. オンライン行政手続件数と利用率

足元で増加、今後も更なる増加が見込まれる

※2025年までに約2万2千の行政手続のオンライン化98%超を目標（2021年6月 政府規制改革推進会議）

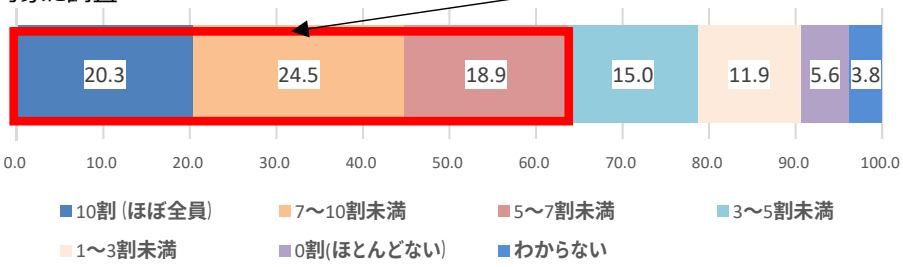


出典：内閣官房IT総合戦略室・総務省「行政手続等の棚卸結果等の概要」を基にNISCで作成

5. 勤務先のテレワーク実施率（第1回緊急事態宣言時）

６割以上の企業で、社員の５割以上が実施

286社を対象に調査



出典：総務省(2021)「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」を基にNISCで作成

6. サプライチェーン複雑化

IoT機器は様々な国の製品で構成されている

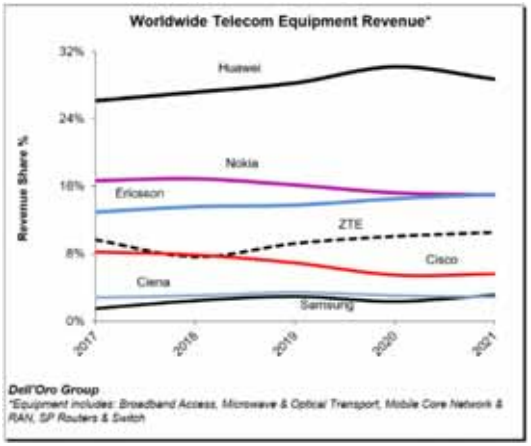
主要通信機器の世界シェア

サーバー(2021年2Q)	
HPE/New H3C【米国/中国】	15.7%
デル【米国】	15.6%
インスパー【中国】	9.4%
レノボ【中国】	7.0%
IBM【米国】	5.0%
その他	47.5%

スマートフォン(2021年)	
サムスン【韓国】	20.1%
アップル【米国】	17.4%
シャオミ【中国】	14.1%
オッポ【中国】	9.9%
ヴィーヴォ【中国】	9.5%
その他	29.1%

出典：IDC

通信ベンダーの世界シェア（収益ベース）



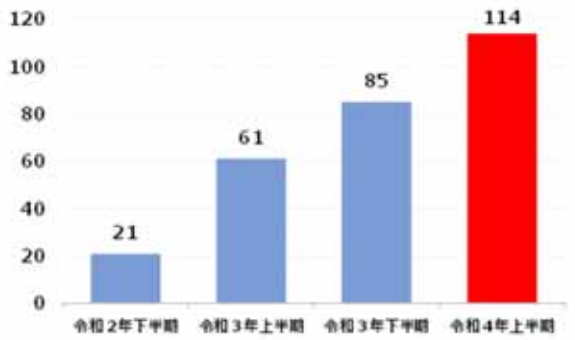
出典：Dell'Oro Group

ランサムウェアやEmotetによる被害拡大

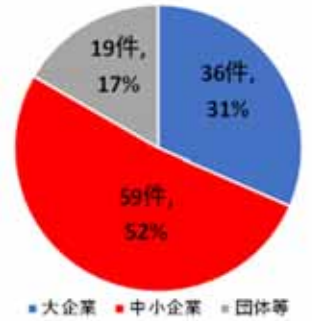
ランサムウェア

- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可にし、その**解除と引換えに金銭を要求**する。
- 近年は新たなランサムウェアとして、システムの**復旧に対する金銭要求**に加え、窃取した**データを公開しない見返りの金銭要求**も行う**二重の脅迫が発生**している。
- 国内事例として、企業・団体等におけるランサムウェア被害として、令和3年に全国の都道府県警察から警察庁に報告があった件数は**114件**であり、前年上期から**約2倍に増加**。
- 被害件数（114件）の内訳は、**大企業が36件（31%）**に対して、**中小企業は59件（52%）と過半数超**。

企業・団体等におけるランサムウェア被害の報告件数の推移



ランサムウェア被害の被害企業・団体等の規模別報告件数（令和４年上半期）

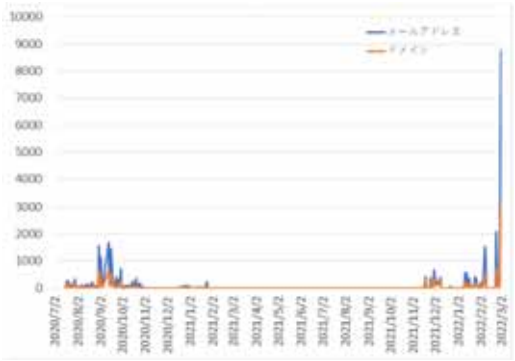


（データ出所）警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について（2022年9月15日）」を基にNISC作成

Emotet

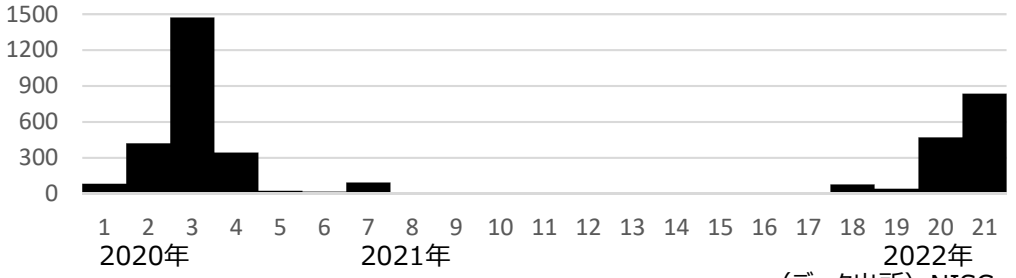
- 2021年11月から再開したEmotetの攻撃活動が、**2022年2月より急増**しており、国内企業・組織から感染被害が公表されている。
- 2022年3月のEmotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の**約5倍以上に急増**。
- 政府機関内においても、Emotetの活動が再開した2021年11月より、**取扱件数が増加傾向**にある。
- Emotetの攻撃メールの手口としては、**Excelファイルのマクロ機能の悪用**、**パスワードZIPファイルの悪用**、**URLリンクのクリックの誘導**等がある。

Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数



（データ出所）
JPCERT/CC「マルウェアEmotetの感染拡大に関する注意喚起(2022年3月14日)」を基にNISC作成

政府機関内におけるEmotet取扱件数の推移（2020年７月～2022年３月）



（データ出所）NISC

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**に向けて行ってきた取組

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

サイバーセキュリティ戦略の構成

中長期的

1　2020年代を迎えた日本をとりまく時代認識

1－1　デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する期待、安全保障環境の変化、新型コロナウイルスの影響・経験、東京大会に向けた取組の活用

2　本戦略における基本的な理念

2－1　確保すべきサイバー空間は「自由、公正かつ安全な空間」

2－2　基本原則は従来の戦略で掲げた５つの原則を堅持（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）

3　サイバー空間をとりまく課題認識

環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向

戦略期間

4　目的達成のための施策

＜3つの方向性＞（１）デジタル改革を踏まえたデジタルトランスフォーメーション とサイバーセキュリティの同時推進
（２）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
（３）安全保障の観点からの取組強化

経済社会の活力の向上及び持続的発展

1．経営層の意識改革

2．地域・中小企業におけるDX with Cybersecurity の推進

3．新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

4．誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

国民が安全で安心して暮らせるデジタル社会の実現

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

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

3・4・5．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)
②(重要インフラ)
③(大学・教育研究機関等)

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

7．大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

1．「自由、公正かつ安全なサイバー空間」の確保

2．我が国の防御力・抑止力・状況把握力の強化

3．国際協力・連携

横断的施策

研究開発の推進　人材の確保・育成・活躍促進　全員参加による協働・普及啓発

5　推進体制

「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

サイバーセキュリティ戦略（経済社会の活力の向上及び持続的発展）

課題認識と方向性　ーデジタルトランスフォーメーションとサイバーセキュリティの同時推進 ー

- 2021年9月に「デジタル庁」が設置され、デジタル化が大きく推進される絶好の機会。
  そのためにも、サイバー空間への信頼を醸成し、参加・コミットメントを得ることが重要。
- また、業務、製品・サービス等のデジタル化が進む中、サイバーセキュリティは企業価値に直結する営為に。
  「セキュリティ・バイ・デザイン」の重要性は一層増し、デジタル投資とセキュリティ対策の一体性は高まる。

⇨ デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進。

主な具体的施策

① 経営層の意識改革

→デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化・インセンティブ付けを行い、更なる取組を促進。

② 地域・中小企業におけるDX with Cybersecurityの推進

→地域のコミュニティの推進・発展、中小企業向けサービスの審査登録制度を通じ、デジタル化に当たって直面する知見や人材等の不足に対応。

③ 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

→Society5.0に対応したフレームワーク等も踏まえ、各種取組を推進。

- サプライチェーン：　産業界主導のコンソーシアム
- データ流通　　：　データマネジメントの定義、「トラストサービス」によるデータ信頼性確保
- セキュリティ製品・サービス：　第三者検証サービスの普及
- 先端技術　　：　情報収集・蓄積・分析・提供等の共通基盤構築

④ 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

→情報教育推進の中、「デジタル活用支援」と連携して、各種取組を推進。

サイバーセキュリティ戦略（国民が安全で安心して暮らせるデジタル社会の実現①）

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・共助による**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）

サイバーセキュリティ戦略（国民が安全で安心して暮らせるデジタル社会の実現②）

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。

（参考）「重要インフラのサイバーセキュリティに係る行動計画」の概要

官民連携による重要インフラ防護の推進

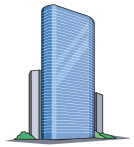
・**任務保証**の考え方を踏まえ、**重要インフラサービスの安全かつ持続的な提供**を実現

・**官民が一体**となって**重要インフラのサイバーセキュリティの確保に向けた取組**を推進

NISCによる総合調整

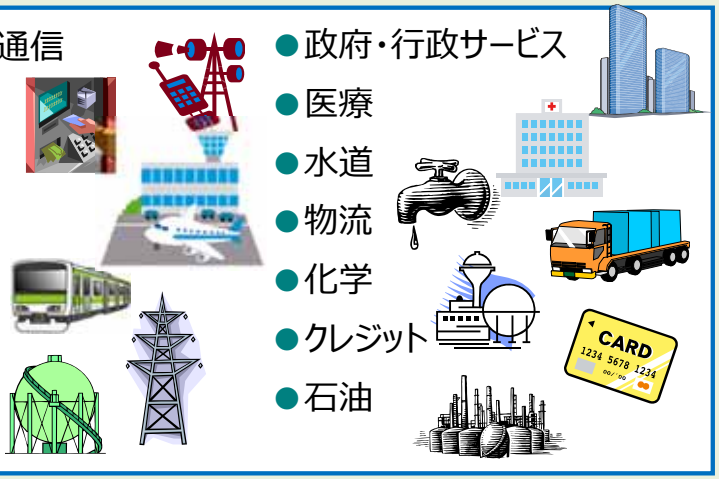
重要インフラ所管省庁

- 金融庁
  ［金融］
- 総務省
  ［情報通信、行政］
- 厚生労働省
  ［医療、水道］
- 経済産業省
  ［電力、ガス、化学、クレジット、石油］
- 国土交通省
  ［航空、空港、鉄道、物流］



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



関係機関等

- サイバーセキュリティ関係省庁
  ［総務省、経済産業省等］
- 事案対処省庁
  ［警察庁、防衛省等］
- 防災関係府省庁
  ［内閣府、各省庁等］
- サイバーセキュリティ関係機関
  ［NICT、IPA、JPCERT/CC等］
- サイバー空間関連事業者
  ［サプライチェーン等に関わるベンダー等］

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

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の障害対応体制の強化を推進

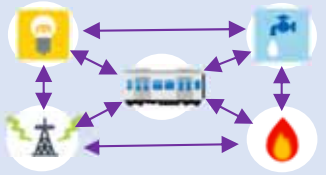
安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

（参考）「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、サイバーセキュリティ戦略（令和３年９月28日閣議決定）を踏まえ、環境変化に適確に対応できるようにするため、令和4年6月17日に開催されたサイバーセキュリティ戦略本部にて、**新たな行動計画を策定**した。

- ◆ **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**

サイバーセキュリティ戦略（国際社会の平和・安定及び我が国の安全保障への寄与①）

課題認識と方向性　－ 安全保障の観点からの取組強化 －

- 我が国をとりまく安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取等を企図したサイバー攻撃を行っているとみられている。
- 一方、同盟国・同志国においても、サイバー脅威に対応するため、サイバー軍や対処能力の強化が進められており、サイバー事案やサイバー空間に関する国際ルール等をめぐる対立等に対して同盟国・同志国等が連携して対抗している。
- 加えて、安全保障の裾野が経済・技術分野にも一層拡大している中で、サイバー空間に関する技術基盤やデータをめぐる争いに対しても、同盟国・同志国が連携して対抗し、「自由、公正かつ安全なサイバー空間」を確保するため、我が国の基本的な理念に沿った国際ルールを形成していく必要がある。

⇨ サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、以下を一層強化する。

「自由、公正かつ安全なサイバー空間」の確保

国際協力・連携

我が国の防御力・抑止力・状況把握力の向上

サイバーセキュリティ戦略（国際社会の平和・安定及び我が国の安全保障への寄与②）

主な具体的施策

① 自由・公正かつ安全なサイバー空間の確保

- サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）
  - 国際法の適用に関する議論・規範の実践の普及、サイバー犯罪に関する条約の普遍化等の推進
- サイバー空間におけるルール形成
  - 信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）や5Gセキュリティ等国際的な取組の進展を踏まえた我が国の基本理念に沿う国際ルールの策定

② 我が国の防御力・抑止力・状況把握力の強化

- サイバー攻撃に対する防御力の向上
  - 防衛省・自衛隊におけるサイバー防衛能力の抜本的強化、自衛隊・米軍のインフラ防護の演習等の実施
  - 先端技術・防衛産業等のセキュリティ確保のための官民連携・情報共有等の強化
- サイバー攻撃に対する抑止力の向上
  - 相手方によるサイバー空間の利用を妨げる能力の活用や外交的手段・刑事訴追等を含めた対応の活用、日米同盟の維持・強化
- サイバー空間の状況把握力の強化
  - 全国的なネットワーク・技術部隊・人的情報を駆使したサイバー攻撃の更なる実態解明の推進

③ 国際協力・連携

- 知見の共有・政策調整
  - 米豪印やASEAN等同志国との府省庁横断的・各府省庁における国際連携の重層的な枠組みの強化
- サイバー事案等に係る国際連携の強化
  - 国際サイバー演習の主導等による国際的なプレゼンスの向上
- 能力構築支援
  - 「基本方針」*に基づく産学官連携や外交・安全保障を含めたASEANを含むインド太平洋地域における取組強化

*「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」

サイバーセキュリティ戦略（横断的施策）

DXとサイバーセキュリティの同時推進

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

安全保障の観点からの取組強化

● 上記の推進に向け、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組む。

1．研究開発の推進

産学官エコシステム構築とともに、それを基盤とした実践的な研究開発推進。
中長期的な技術トレンドも視野に対応。

(2)実践的な研究開発の推進

①サプライチェーンリスクへの対応
②国内産業の育成・発展
③攻撃把握・分析・共有基盤
④暗号等の研究の推進

(3)中長期的な技術トレンドを視野に入れた対応

①AI技術の進展
AI for Security
Security for AI

②量子技術の進展
耐量子計算機暗号の検討
量子通信・暗号

(1)国際競争力の強化 産学官エコシステムの構築

・研究・産学官連携振興施策の活用
・研究環境の充実　等

2．人材の確保、育成、活躍促進

「質」・「量」両面での官民の取組を一層継続・深化させつつ、環境変化に対応した取組の重点化。官民を行き来しキャリアを積める環境整備も。

(1)DX with Cybersecurity の推進

・「プラス・セキュリティ」知識を補充できる環境整備
・機能構築・人材流動に関するプラクティス普及　等
(xSIRT、副業・兼業等)

(2)巧妙化・複雑化する脅威への対処

・人材育成プログラムの強化
SecHack365 / CYDER / enPiT
ICSCoE中核人材育成プログラム 等
・人材育成共通基盤の構築
産学への開放
・資格制度活用に向けた取組 等

優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境の整備

(3)政府機関における取組

外部高度人材活用の仕組み強化
「デジタル区分」合格者の積極採用、研修の充実・強化　等

3．全員参加による協働、普及啓発

デジタル化推進を踏まえ、アクションプランの推進・改善、高齢者への対応を含め見直しの検討。

サイバーセキュリティ2022（年次計画・年次報告）

2022年６月17日
サイバーセキュリティ戦略本部決定

- 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**

東京2020大会に向けたサイバーセキュリティ対策① (大会前・大会期間中の対策)

大会前の対策状況

サイバー攻撃等による影響の未然防止、軽減に向けた対策等を推進

○リスクアセスメントの取組 (事業者等が自主的に実施する取組)

大会に関連する重要サービス事業者等を対象に、リスク評価を実施（2016年から全６回）。

○横断的リスク評価の取組 (NISCが評価する取組)

競技会場や特に重要な事業者を対象に、NISCが主体となって検証（2018年から全５回）。

○スポーツ関係団体に対する勉強会

スポーツ関係団体を対象に、サイバーセキュリティに係る勉強会等を開催（2017年から全17回）。

○サイバーインシデント対応演習

現下のサイバーセキュリティ情勢を踏まえたシナリオを用いた演習を実施（2019年から全５回）。

大会開催期間中における対策の運用等

サイバーセキュリティ対処調整センターを中心に、インシデント発生時には関係組織が一丸となって迅速に対処

○情報共有プラットフォームの運用

関係組織間における脅威情報の共有等を迅速・効率的に行うための情報共有プラットフォーム（JISP）を運用。約350の関係組織がJISPを活用。

○サイバーセキュリティ対処調整センターの運用

関係組織からの連絡に即応できるよう24時間態勢（7/9～9/5）で運用。インシデント発生の際には、情報セキュリティ関係機関と協力して、迅速にインシデント対処を支援。

東京2020大会に向けたサイバーセキュリティ対策②（大会の対策の成果等）

東京大会へのサイバー攻撃に関する被害状況等

大会運営に影響を与えるようなサイバー攻撃を許すことなく、無事に大会を終えることができた。

大会期間中の主なトピック（大会運営への影響なし）

○ **サイバー攻撃に関するSNS上の書き込み等**

大会関係組織に対するサイバー攻撃を呼びかけるSNS上の書き込み等を確認

○ **米国コンテンツ配信サービス企業における障害**

米国コンテンツ配信サービス企業においてシステムの不具合によるサービス障害が発生し、大会公式サイトを含む関係組織のwebサイトが一時的に閲覧不能になったことを確認（7/23　1時間程度）

本件に関しては、同企業からサイバー攻撃によるものではない旨の発表あり

○ **不正な動画配信サイト**

開会式、各競技等の動画配信を装った複数の不正サイトを確認

動画配信サイトの検索結果


サイト接続後に案内される不正なアカウント登録画面

今後の取組方針

●新たな「サイバーセキュリティ戦略」を踏まえ、**「ナショナルサート」の枠組み強化の一環として、東京大会に向けた取組をレガシーとして最大限に活用**。

●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推進。

対象とする領域の拡大

・従来から対象としていた政府機関や重要インフラ事業者等に加えて、**新たなサイバーセキュリティの担い手や重要な情報（知財、個人情報など）を扱う事業者の支援に活用**。

・具体的にはサプライチェーン管理、クラウドサービス、新たな技術も視野に入れて、広く成果を展開。

情報共有の加速化

東京大会に向けた仕組みや参加組織を、**「サイバーセキュリティ協議会」と統合**することで、情報共有を加速化

海外へのノウハウ展開

我が国のサイバーセキュリティ政策に関する国際的な情報発信の中で、**東京大会における我が国の経験等を他国とも共有**

東京2020大会に向けたサイバーセキュリティ対策③（海外での報道事例）

- 2021年8月17日付の「Security Magazine」にて「The Tokyo Olympics are a cybersecurity success story」と題した記事を掲載（※Security MagazineはBNP Media社が発行）
- 記事は「東京オリンピックはサイバーセキュリティの観点からは本当に成功であり、モデルとして見倣うべきである。」と伝えている。
- 執筆は、Maryville University（米国）のDr. Brian Gant准教授。

記事のポイントは次のとおり。

- 最も良い防御は、良い攻撃である。
  （The best defense is a good offense.）

- これまでサイバーセキュリティの分野では、非常に多くの組織が、攻撃を受けるまで待つという共通の問題があった。

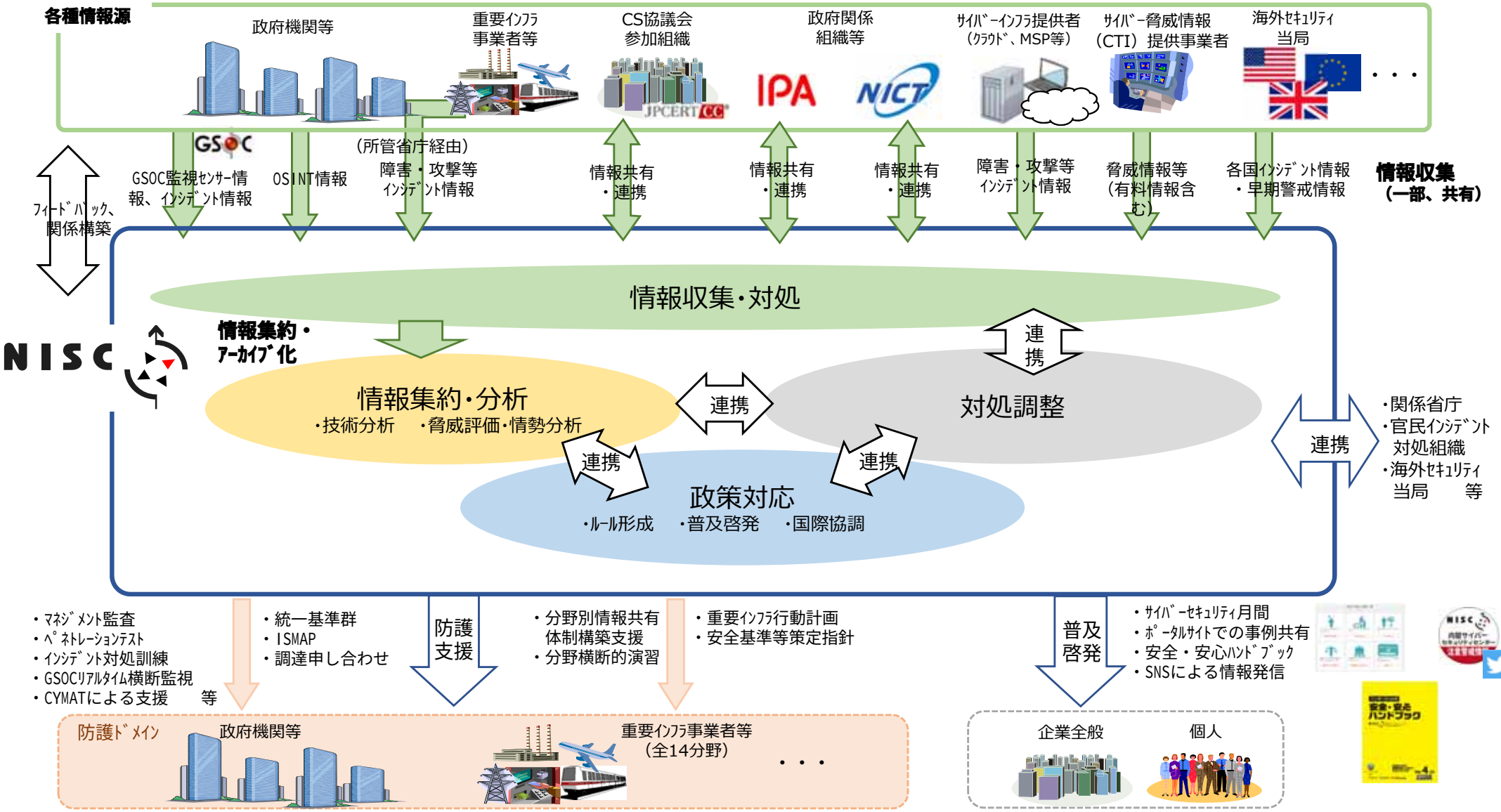
- しかしながら、過去の五輪からの教訓を踏まえ、国際オリンピック委員（IOC）及び東京大会組織委員会（TOC）は同じ過ちを犯さなかった。

- 攻撃者の戦略は絶えず進化しており、我々も過去の栄光に安心することなく、常に緊張感を持ち続けなければならない。

- サイバーセキュリティインシデントが増加する中、東京五輪のような成功例は、明るいニュースとして歓迎すべきであり、消極的な立場に立って過ちを犯しがちな組織にとっては良いモデルになるものである。

ナショナルサートとしてのNISCの機能強化のイメージ

- **4つの機能（①情報収集・共有、利活用、②集約・分析機能、③対処調整、④政策対応）に対応した体制を具備し、情報把握・分析からインシデント対応及び政策措置までの展開を一体的に推進するための総合的な調整を担う機能を整備。**
- **外交・安保当局による抑止対応にも資する観点から、防御から状況把握、抑止までのシームレスな対応に貢献。**



ご清聴頂きありがとうございました。

https://www.nisc.go.jp