資料１

2020 年及びその後を見据えたサイバーセキュリティの在り方
～ サイバーセキュリティ戦略中間レビュー ～

資料１－１　2020 年及びその後を見据えたサイバーセキュリティの在り方についての概要

資料１－２　2020 年及びその後を見据えたサイバーセキュリティの在り方について

2020年及びその後を見据えたサイバーセキュリティの在り方について
－サイバーセキュリティ戦略中間レビュー－

資料１-1

■ 現行戦略策定後の脅威動向等の認識を踏まえ、加速・強化すべき施策を取りまとめ、急ぎ対応が必要と考えられるものから実施（必要な制度面の見直し等を含む。）。
■ 今後は、本レビューを踏まえ、　（必要な制度面の見直しも含め）可能な施策から段階的に実施（1年以内）

脅威等の変化

IoT機器を踏み台にした
サイバー攻撃の顕在化

省庁・分野を越えた情報共有の必要性

2020年東京オリンピック・パラリンピック競技大会に
向けた抜本的対策を見据えた取組の必要

ボット（注）撲滅の推進

■ 効率的かつ効果的な対策につなげるため、官民が連携し、実態の把握、対策の実施・周知、再発防止・環境改善を一体的に実施
- 政府内に体制を構築して継続的かつ広範な実態調査ができるよう、必要な法的整理
- 電気通信事業者等の協力を得た利用者等の特定・注意喚起等の対策の実施、周知（必要な技術的・制度的枠組の構築）
- 迅速な対処の協力の要請（製造事業者・販売事業者等）
- 諸外国との連携を促進し、協調した対策を実施。

（注）ここでは、IoT機器等を外部から遠隔操作するための　不正プログラムを指している。

情報共有・連携ネットワーク（仮称）の構築・運用

■ 官民が連携し、迅速な集約・分析、効果的な対策の共有を行う情報連携体制を構築することにより、サイバー攻撃の被害及び被害拡大を防止
- 効果的な情報連携体制を構築する制度整備。
  - ✓ 情報へアクセス権限を有する民間事業者の責務、官側の役割等
  - ✓ 情報提供を行う際の阻害要因に対処
- 情報提供者にとって提供しやすく、かつ利用者にとって対策しやすい情報の抽出及び環境の整備。
  - ✓ 事案に応じた提供内容をあらかじめ設定し、対策に効果的な内容を適切なタイミングで共有。

2020年東京オリンピック・パラリンピック競技大会に向けた体制の整備

■ サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）の構築（2018年度末目途）
- 組織委員会に対する適切な助言・支援が行えるよう、東京オリンピック競技大会・東京パラリンピック競技大会推進本部との連携等、制度的枠組の検討。
- 一定程度の専任要員（計画的に訓練）
- 200人以上の技術者等（重要サービス事業者、セキュリティ事業者等）との連携態勢。

■ セキュリティ情報センターの構築
- 安全に係る情報を集約、分析・評価を行い、関係機関等に対し必要な情報を随時提供

■ リスクマネジメントの促進
- 横断的リスク評価（2018年度までに全分野で実施）に基づくマネジメントを強力に推進
- 特に影響度が大きい重要サービス事業者について、鳥瞰図的な把握及び検証、リスクの確認及び対策を推進

CSIRT: Computer System Incident Response Team
ﾘｽｸｱｾｽﾒﾝﾄ：ﾘｽｸ（目的に対する不確かさ）を組織的に管理し、損失などの回避、低減を図る方法
ｺﾝﾃｨﾝｼﾞｪﾝｼｰﾌﾟﾗﾝ：提供するｻｰﾋﾞｽに障害が発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等を予め定めたもの

経済社会の活力の向上及び持続的発展

- 安全なIoTシステムの創出による国際競争力の強化（国際標準化）［関係分野の用語・設計・開発等の概念を共通化する国際標準の策定］
- セキュリティに係るビジネス環境の整備［セキュリティ規格に関する要件の策定、セキュリティに係る損害保険の普及の支援］

国民が安全で安心して暮らせる社会の実現

- 深刻度判断基準の策定等によるサイバー攻撃対処態勢の強化［コンティンジェンシープラン策定の支援］
- 政府機関・独法等における効率的・効果的防護体制の再構築［検知精度・対処能力等の監視能力の向上、情報システムの侵入耐性診断時の自衛隊能力の活用］
- 地方公共団体におけるセキュリティ対策向上［セキュリティ人材・体制の確保充実の支援］
- 大学等における情報セキュリティ対策の向上［大学等の相互協力による取組、情報システムの侵入耐性診断実施支援］
- サイバー犯罪・サイバー攻撃対策の強化
- 普及啓発・情報発信［迅速な情報発信・相談対応のための取組強化］

国際社会の平和・安定及び我が国の安全保障

- 組織・分野 横断的な取組等による我が国の安全の確保
- 国立研究開発法人における先端技術の防護のための情報セキュリティ対策の強化
- 海外の多様な主体との多層的な連携の強化
- サイバー犯罪・サイバー攻撃対策の国際的な連携の強化

- 経営層の意識改革や、橋渡し人材等幅広い階層における人材育成・確保の継続的な促進
- 研究開発等の推進

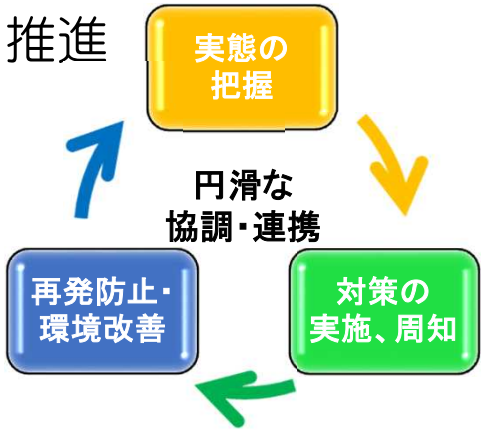
「ボット撲滅の推進」　～IoT機器・システムのセキュリティ対策について～

官民の協調・連携による「ボット撲滅」に向けた体制を構築し、対策を推進

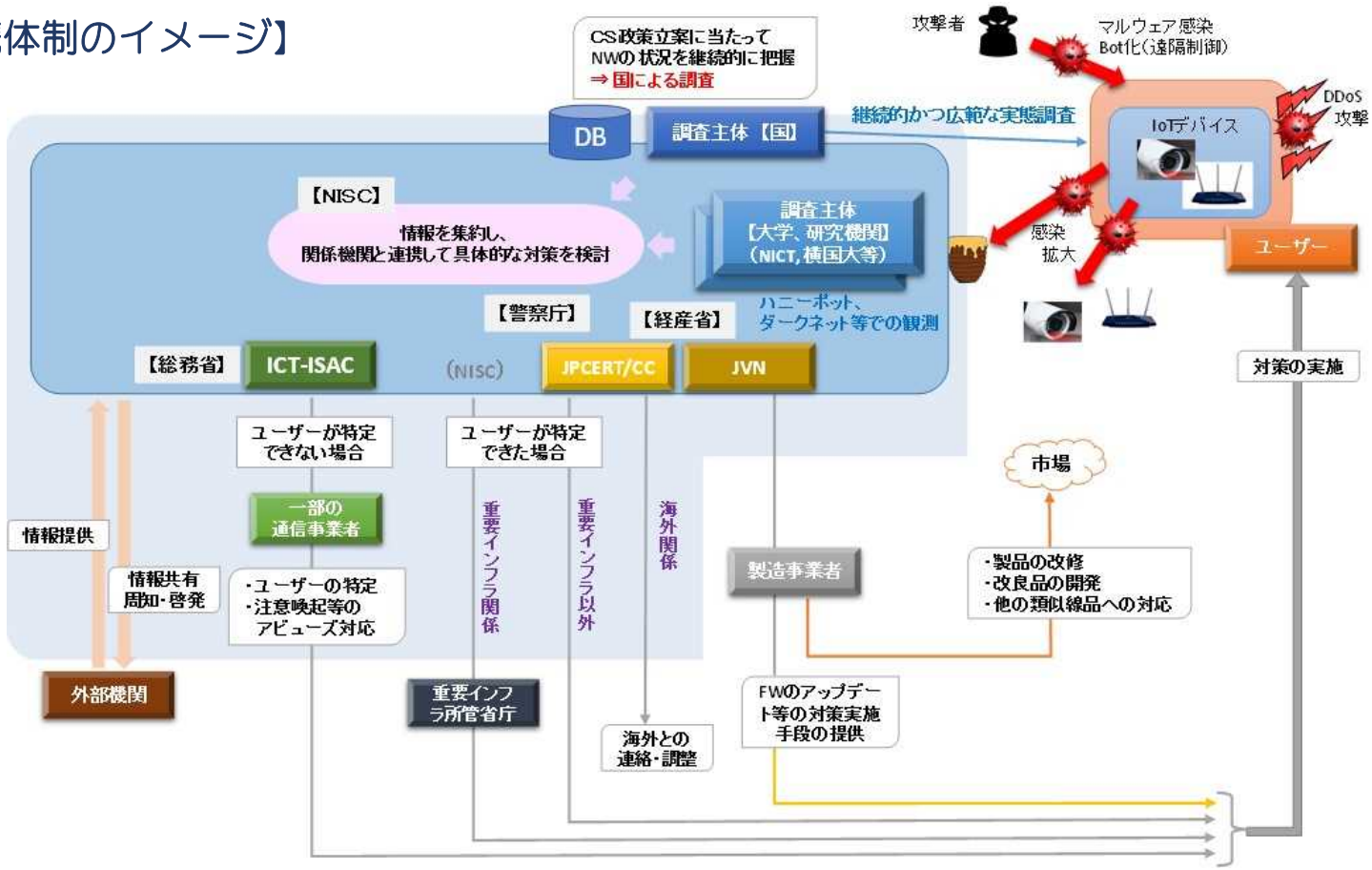
実態の把握：継続的かつ広範な実態調査が実施できるよう、政府内の体制を構築。

対策の実施、周知：関係機関（電気通信事業者、機器の製造事業者、等）の役割を整理し、効率的な対策・周知等を実施。 諸外国との連携を促進。

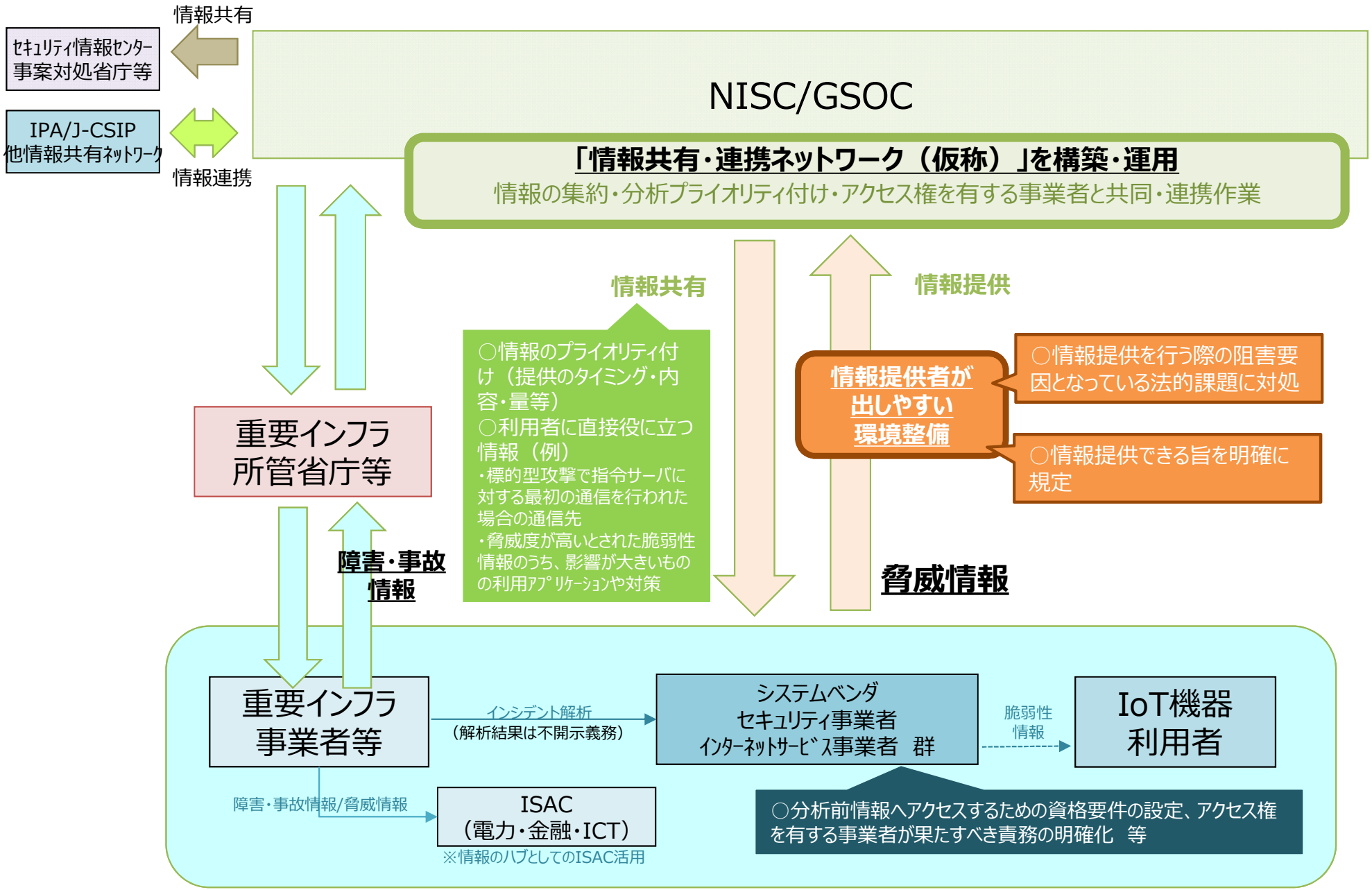
再発防止・環境改善：セキュリティ対策に係る認証等の実施。
IoT推進コンソーシアム等を活用した関係者間での情報共有。



【官民連携体制のイメージ】



2020年に向けた情報共有体制（イメージ）
～情報共有・連携ネットワーク（仮称）～



リスクマネジメントの促進のための取組概要

サイバー攻撃等による2020年東京オリンピック・パラリンピック競技大会の準備・運営への影響の未然防止や軽減等のため、大会を支える周辺サービスを提供する事業者等によるリスクマネジメントの強化を通じ、想定されるサイバーセキュリティ上のリスクへの対策を促進。第２回は対象を１都３県に拡大するとともに、横断的リスク評価を実施するために必要な情報について報告いただく。

○ リスクマネジメントの促進のため、サイバーセキュリティリスクを特定・分析・評価する手順をNISCで作成。

○ 東京大会の開催・運営に影響に与えうる重要サービス分野を、関連する所管省庁と調整の上で選定。

（通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス（地方自治体）、下水道、空港、道路・海上・航空交通管制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給　計19分野）

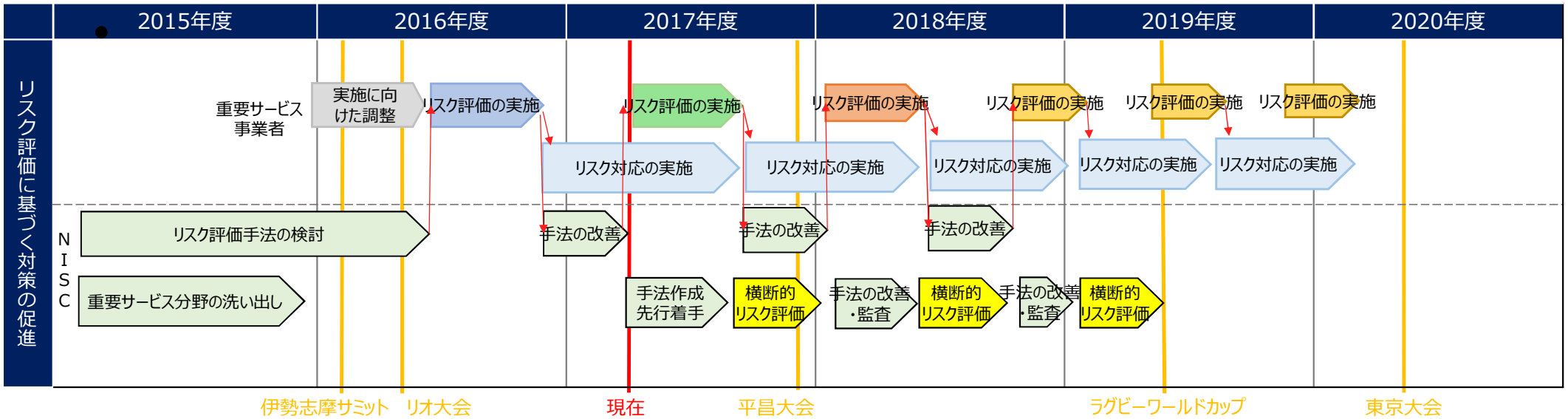
○ 東京大会に向けて、継続的に複数回実施。PDCAサイクルを繰り返す。

○ NISCによる大会全般にわたる横断的リスク評価の実施に向けて、必要な情報の特定や方法の検討を実施。

第1回	第2回	第3回	第4回以降
期間：2016年度下期 対象：東京23区エリア	期間：2017年度第２四半期 対象：東京圏（１都３県）	期間：2018年度上期 対象：東京圏+地方競技会場周辺	期間：2018年度第４四半期 対象：東京圏+地方競技会場周辺

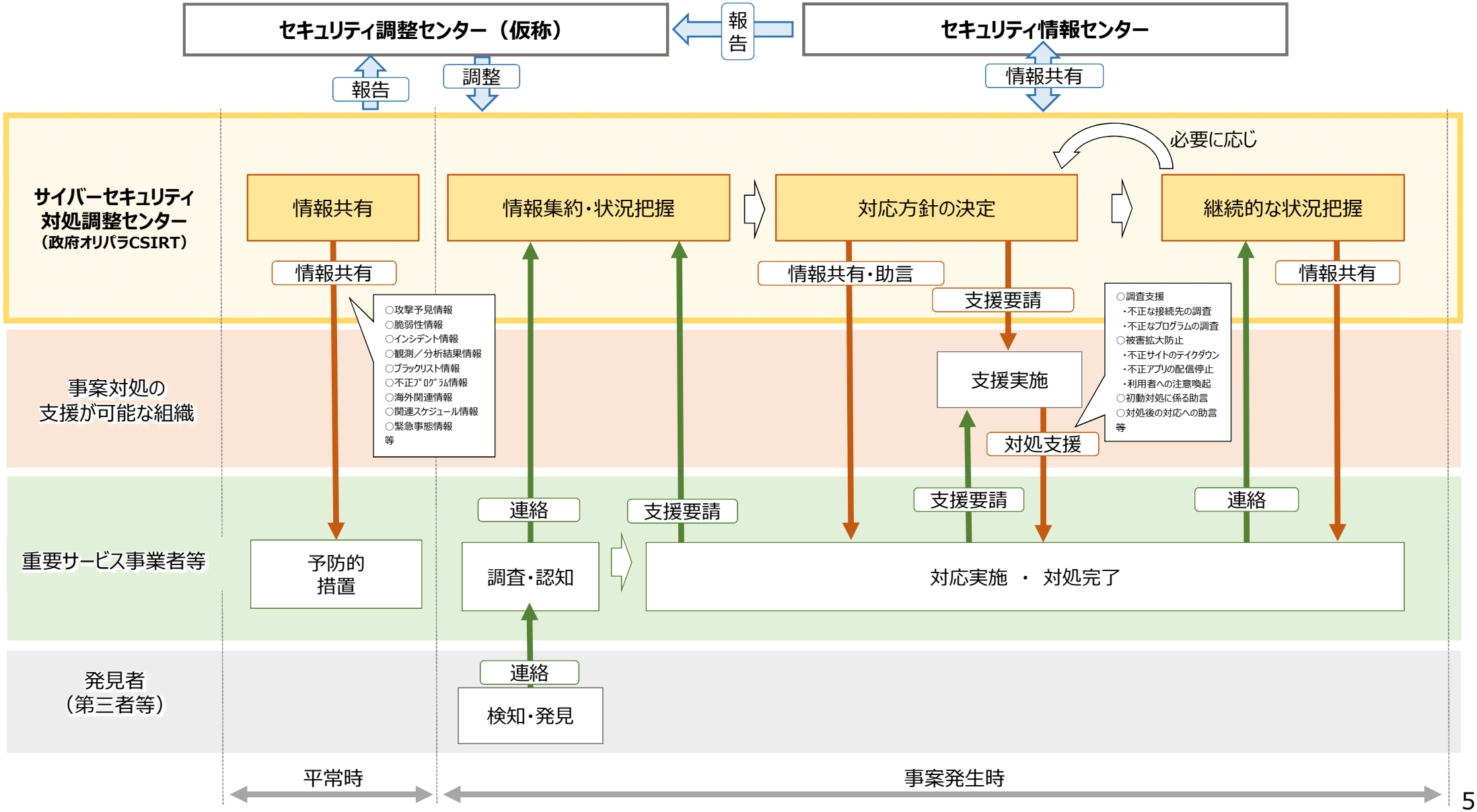
【横断的リスク評価】

サービスの継続的な確保が滞った場合に、大会への影響が重大なサービスを分野を横断して抽出するとともに、それらのサービスに対して、事業者等が自組織におけるリスク評価で設定した満たすべきサービス水準が妥当であるかを検証。検証結果は、事業者等におけるリスク評価結果の妥当性確認や、大会に向けた訓練等に活用。



サイバーセキュリティ対処調整センター（政府オリパラCSIRT）のイメージ

◆ 関係機関との緊密な連携の下、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織。
- ➢ 関係組織の攻撃予見情報・脆弱性情報・事案情報等を情報共有システムを通じて集約し、迅速に共有。
- ➢ 事案対処のための支援が必要な組織に対して、適切かつ円滑に対処を調整。



深刻度判断基準の策定等によるサイバー攻撃対処態勢の強化

○ 深刻度判断基準

○ **概要**

重要インフラサービス障害の深刻度や当該障害に関する情報の重要度に応じて影響範囲や対処行動等が異なってくることも踏まえ、関係主体間で認識の共有を図り、迅速な対応要否等の判断に資するため、第4次行動計画案に基づき、重要インフラサービス障害に係る深刻度の判断基準の具体化に向けた検討を進める。

重要インフラ専門調査会等の場における議論を踏まえ、平成29年度末までに暫定版を策定し、公表する。

○ **目的**

①可視化された深刻度により、発生した事象について関係主体間で共通の理解を助ける（客観性、国際的整合性に留意）
②深刻度レベルを政府の対応を判断する基準とする
③事象に関する情報共有の体制や方法の基準とする

検討のための素案

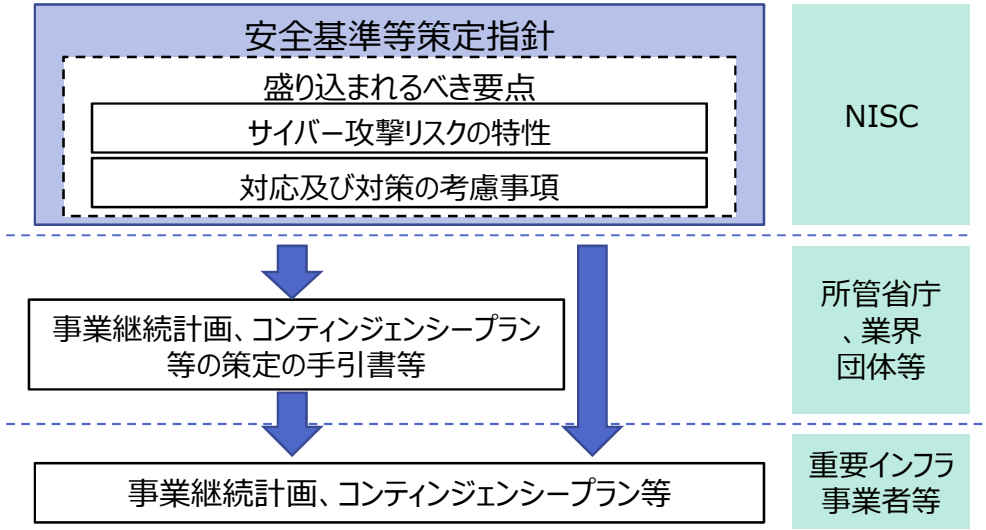
深刻度	国民・社会への影響	システムへの影響	
		非常用系	常用系
レベル５（危機）	国民生活等に広範かつ著しい影響を与えるおそれが切迫		
レベル４（重大）	国民生活等に著しい影響を与える可能性が高い	重要インフラサービスの安全性・持続性への影響により評価	
レベル３（高）	国民生活等に明らかな影響を与える可能性が高い		重要インフラサービスの提供への影響により評価
レベル２（中）	国民生活等に何らかの影響を与える可能性がある		
レベル１（低）	国民生活等に影響を与える可能性は低い		
レベル０（なし）	国民生活等に影響を与える可能性はない		

○ 機能保証の考え方を踏まえた対処態勢整備の促進

○ **概要**

内閣官房・重要インフラ所管省庁は、機能保証の考え方を踏まえて事業継続計画及びコンティンジェンシープランに盛り込まれるべき要点やこれらの実行性の検証に係る観点等を整理し、重要インフラ事業者等に提示するなどの支援を行う。

「盛り込まれるべき要点」については、サイバー攻撃リスクの特性並びに対応及び対策の考慮事項について、平成29年度末に改定する安全基準等策定指針に盛り込む。



○ 関係主体による共同訓練の実施

○ **概要**

重要インフラ事業者等における重要インフラサービス障害対応の実態やニーズに適合した演習・訓練の充実による重要インフラ防護能力の維持・向上を目指す。

政府機関・独法等における防護体制の在り方の検討

背　景

○　政府機関等においては、統一基準群に則り、情報システムにおけるログの取得・管理及び適切な監視、情報システム台帳の整備、主体認証情報の管理について政府機関等自らが措置を講じているところである。

○　一方で、政府機関等においては、依然として情報セキュリティインシデントに係る脅威（機密情報の窃取、行政事務の妨害、データの改ざん）が存在し、脅威は増加傾向にあるとともに、プログラムの脆弱性が発見された直後に攻撃される等、サイバー攻撃の脅威やスピードが増している状況。

○　現在GSOCシステムは第3期目であるが、GSOCシステムに係る予算は、監視能力の強化や監視対象組織の拡大に伴い、増加傾向にあり、予算を分担している各府省庁の負担が増加している状況。

問題意識

○　**GSOCのインターネット接続口の監視（境界監視）で必ずしも全ての不正な通信を検知できているわけではない**。また、境界監視だけではマルウェア感染の**早期検知・広がりや攻撃の成否の確認が困難**であるが故にインシデントの重大さを早期に判断できない状況であるとともに、**政府機関等のシステム構成等を十分に**把握していれば適切な情報提供ができるが、実際は**インシデントが発生した時に初めて把握**する状況であることから、実態として**後手に回り、即応性に欠けることがある。**

⇒　監視能力の向上及び更なる即応化が必要ではないか。

○　今後も監視能力の強化や監視対象組織の拡大に伴い必要な予算が増加することにより、**各府省庁の負担も増加が見込まれ、財源が限られる中、このままでは、立ち行かなくなることが想定される。**

⇒　技術面の要件を満たしつつ、コスト削減も図れないか。

第4期GSOCシステムについて、必要な機能の精査等によるコスト削減を行った上で、政府機関等におけるサイバー攻撃への効果的な対処に資する高度な監視・早期警戒情報の提供を可能とするため、今年度中を目途に、NISCにおいて、関係府省庁と連携して、府省庁が自律的に状況を把握する能力を支えるべく、検知精度及び対処能力等の監視能力の向上及び即応化に資する端末等での新たな監視手法の導入や脆弱性の適切な把握が可能となるような仕組みについて検討するとともに、府省庁のセキュリティ対策状況に応じたGSOCとの高度かつ効率的な連携の可能性についても検討する。

地方公共団体におけるセキュリティ対策の向上

○ 背 景

・2017年度に、地方公共団体におけるマイナンバーの本格的な利用開始（対策強化の必要性）
・近年、地方公共団体へのサイバー攻撃の増加

○ 問題意識

・中小規模の団体を中心に、人員や予算などの資源に制約ある中で、マイナンバー利用事務系等において、高いセキュリテイレベルを確保する必要
・技術的な対策には限界があるものの、ヒューマンエラーによる情報漏えいに対して、できるだけの対策を講じる必要
・現行の国と地方の役割分担の考え方を踏まえ、国による地方への直接の関与（技術仕様、監査等）が、他の機関に比べ限定的な中で、高いセキュリテイレベルを確保する必要

○ 主な取組

・2016年度に、地方公共団体においてセキュリティ強化対策「三層の構え」を実施
① マイナンバー利用事務系について、端末からの情報持ち出し不可設定等
② LGWAN接続系とインターネット接続系を分離
③ 都道府県と市区町村が協力して、インターネットの接続口を一つに集約する「自治体情報セキュリティクラウド」を構築
・2017年度に、セキュリティポリシーガイドラインを更新予定
・2017年度に、自治体情報セキュリティ向上プラットフォームを構築しLGWANのセキュリティレベルを確保

大学等における自律的活動の向上に向けた取組

<背景>

・グローバル化の進展が著しい現状において、大学等における業務の遂行上、情報基盤は必要不可欠。
・不正アクセスによる情報漏えいやWebサイト改ざん等の情報セキュリティインシデントが発生した場合、信用失墜を招き、公共性の高い大学等の運営に影響。
・大学等における情報セキュリティインシデントの発生が増加しており、情報セキュ リティ対策は、経営上の重要課題との認識の下、組織的・計画的に取り組むことが必要。

<取組の基本的方向性>

①各大学等は自ら情報セキュリティリスクを適切に評価、中長期的な視点により情報セキュリティ対策基本計画を策定し、組織全体として組織的・計画的に実施。
②国は、上記①の取組が促進するよう、支援を実施。
③取組の実施に当たっては、教育や研究等の多様性に配慮。

大学等による自主的な取組

- **情報セキュリティ対策基本計画に基づく、組織的・計画的な情報セキュリティ対策を実施。**
- **最高情報セキュリティ責任者の主導の下、組織全体として、以下の取組を実施。**

〈マネジメント面〉

✓ 企画・法務・広報など関係部門と連携したインシデント対応体制の構築と対処能力の向上
✓ 情報セキュリティポリシーや情報の取扱規程等の見直しや組織への浸透
✓ 多様な構成員に対応した教育・訓練や啓発活動の実施
✓ 構成員の役割に応じた自己点検や中立性を有する者による監査の実施

〈技術面〉

✓ 組織内の情報機器の把握と適切なアクセス制御の実施
✓ 重要情報を扱う機器へのアクセス等を監視する機能等の実装
✓ 組織内で利用しているソフトウェアの適切な更新が可能な仕組みの整備

< サポート >

国による支援

- **大学等における自主的な取組の促進の観点から以下の支援を実施。**
  ✓ インシデント対応力の向上やセキュリティ監査手法に関する研修の実施及び機会の充実
  ✓ 情報システムの侵入耐性診断の実施に関する支援
  ✓ 諸会議における周知、啓発及びグッドプラクティスの共有
  ✓ 情報セキュリティ対策基本計画の進捗状況のフォローアップ
  ✓ その他自主的な取組加速のための支援

< 相互の協力 >

大学等の相互協力による取組

- **国立情報学研究所において、大学等と連携し、以下の取組を実施することにより、大学等のインシデント対処能力を向上。**
  ✓ SINETにおけるサイバー攻撃検知システムの運用
  ✓ SINETの実環境を用いた技術職員の実地研修を実施
  ✓ 脅威情報等の共有を促進
  ✓ 連携機関の拡大について、今後、運営上の課題を含めて検討
- **大学間の連携コミュニティの形成による相互協力を実施。**
  ✓ 各大学等の枠を超えてCSIRT担当者同士のコミュニティを形成し、脅威情報の共有や共通課題の検討等を実施予定

SINET：国立情報学研究所が構築・運用している学術情報ネットワーク

情報セキュリティ水準の向上

先端的な技術情報を保有する国立研究開発法人の対策強化

<背景> ・サイバー攻撃が激化する中、国立研究開発法人の保有する先端的な技術情報を保護する対策の強化の必要性。
・独立行政法人に属する国立研究開発法人に対するサイバーセキュリティ基本法の枠組みの下での対策が本格化する中、従来の行政事務系の組織とは異なる研究機関特有の課題に対応する必要性。

<取組の基本的方向性>
① 研究成果である技術情報を守ることは、研究者自らの利益に直結 ⇒ 情報セキュリティ対策は当事者組織自身による取組が肝要であり、これを促進。
② 上記①の取組を、基本法の枠組みの下で国が支援するとともに、共通課題について当事者が相互協力。
③ 研究開発を行いやすい環境と情報セキュリティ確保の両立を追求。

< 当事者 >

マネジメント面

【研究機関】
研究部門と管理部門の異なる性質の部門が存在

≠

【行政事務系組織】
組織内が比較的一様

- **各研究部門の長がガバナンスを効かせ、自らの技術情報を守るための情報セキュリティ対策を推進する体制の構築**
- **研究部門を支えるため、管理部門との一元的な情報セキュリティマネジメントの強化**
- **一般的なマネジメント上の課題に加え、研究機関特有の課題としての以下の取組を推進する**
  - ✓人材の流動性に対応した研究者に対する教育・訓練の充実
  - ✓技術情報の特性に応じた格付けの徹底
  - ✓他の共同研究機関との技術情報共有等のための外部サービス(クラウド等)の利用ルールの明確化やその適切な運用
  - ✓研究開発で用いるソフトウエアの管理

技術面

研究人材の多様性、流動性

- **ユーザの人的取組のみに依存しないシステム面での対策によりセキュリティを強化**
- **一般的な技術上の課題に加え、システム更新時など、適当な投資タイミングにおいて以下の取組を図る**
  - ✓研究者が直接取り扱う情報機器は、ユーザに依存しない対策により、全体的に必要な水準を確保する
    - ・やむを得ず法人支給以外の端末を導入する場合
    - ・上記を法人のネットワーク回線に接続する場合
    - ※端末については、法人支給端末の使用が基本であるものの、研究者の業務スタイルを背景に私物端末を許可している法人が多い。
  - ✓研究用システムなど研究目的に照らして集約になじまないものを除き、インターネット回線への接続口の集約化を推進する

< サポート >

国の監査等による専門的支援

- **サイバーセキュリティ基本法に基づく監査・監視の支援の運用本格化により対策を促進**
  - ✓マネジメント監査と侵入テストの双方を国立研究開発法人を含む全ての独立行政法人等についてオリンピック・パラリンピックまでに一巡させる方針。国立研究開発法人についてはこの期間における早い段階に前倒し。
  - ✓監視については、保有する技術情報の重要性等を踏まえつつ、引き続き、監視・情報共有体制を充実
- **CSIRT研修を通じ各法人のインシデント対処能力を向上**
  - ✓国立研究開発法人を含む独立行政法人等へのCSIRT研修を新たに開始

< 相互の協力 >

国立研究開発法人自らの取組

- **国立研究開発法人共通の課題の検討や知見の共有等について、当事者による相互協力・相互研鑽を行う。**
  - ✓国立研究開発法人協議会(国研協)の場に検討の枠組みを整備済み。
  - ✓今後、国研協の場において、具体的活動を実施予定

情報セキュリティ水準の向上

・重要情報である先端技術情報を保有する大学等に対しても、当該情報の漏えいを防止するための自主的な取組を促すとともに、国の支援を実施

資料１－２

2020年及びその後を見据えたサイバーセキュリティの在り方について
－サイバーセキュリティ戦略中間レビュー－

平成29年7月13日
サイバーセキュリティ戦略本部決定

１　位置づけ等

現在の我が国のサイバーセキュリティ政策は、サイバーセキュリティ基本法（平成26年法律第104号。以下「基本法」という。）の規定に基づき策定されたサイバーセキュリティ戦略（2015年9月4日閣議決定。以下「戦略」という。）の枠組のもとに実施されてきた。

現行の戦略の期間は策定後3年とされており、2018年9月にその期限を迎えることとなる。加えて、2016年10月に施行されたサイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律（平成28年法律第31号。以下「基本法一部改正法」という。）の附帯決議において、同法の施行後2年以内に、サイバーセキュリティ基本法を見直す必要性について検討し、その結果に基づいて、必要な措置を講ずることとされている。

しかし、戦略策定後も、国民生活・経済等のIT依存度はますます高まっており、社会に質的変化を生じさせている。一方で、国内外において、感染力の強いワーム機能を有するランサムウェア（身代金）攻撃、IoT機器を踏み台にしたサイバー攻撃、重要インフラを標的としたサイバー攻撃が発生しているが、これらの脅威は、社会の質的な変化によりもたらされていることも否定できない。

このような中、2020年東京オリンピック・パラリンピック競技大会（以下、「2020年東京大会」という。）の開催を3年後に控え、同大会におけるサイバーセキュリティ対策を万全なものとするためには、その前年に開催されるラグビーワールドカップ2019から対策の枠組が機能するべく取組む必要がある。

このため、現状の認識を踏まえた加速・強化すべき施策を取りまとめ、急ぎ対応が必要と考えられるものから実施していく必要があることから本中間レビューを行うこととした。なお、このレビューの結果については、盛り込まれた施策の実施状況も踏まえ、次期戦略の策定等につなげていくことが適当である。

２　総 論

現行の戦略は、総論部分において、

(1) サイバー空間は、「無限の価値を産むフロンティア」である人工空間であるとともに、いわゆる「連接融合情報社会（連融情報社会）」が到来すると認識。

(2) 戦略の目的としては、「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」に寄与。

(3) 戦略の実施に当たっては、①情報の自由な流通の確保、②法の支配、③開放性、④自律性、⑤多様な主体の連携を基本原則。

としている。

中間レビュー時点においても、これらの考え方は基本的に適当であると考えられることから、これらの考え方に基本的に沿って施策の立案及び実施を行っていくことが適当である。

一方、発展を続けるサイバー空間の中で流通する情報量は爆発的に増加している中、近年のサイバー攻撃の激化などサイバー空間における脅威がますます高まる状況にあり、特定の高度な技術を有する者のみがサイバーセキュリティの対処を行う形態ではもはや対応は困難であることから、その対応の在り方も従来の個別的・離散的なものからサイバー空間における全体的・連続的な状況を踏まえた、いわば「サイバー環境問題」に対するものと考える必要が生じている。また、サイバー空間を構成するネットワーク、コンピュータ等の高性能化に加え、IoT、人工知能（AI）、ブロックチェーンなどの新しい技術は社会経済に対する影響の度合いを急速に増しており、サイバー空間における関係主体の概念にも影響を及ぼす可能性も生じているが、このような急速な技術革新に適時適切に対応する必要がある。また、サイバー空間の関係主体は、サイバー空間上で様々なコンテンツやサービスを提供する事業者や通信サービスを提供する事業者などの技術を有する者だけでなく、一般企業、個人にも拡大し、その数がさらに増加・拡散するとともに、官民データ活用推進基本法（平成 28 年法律 103 号）が成立し、「世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画」（平成 29 年 5 月 30 日閣議決定）が策定され、官民におけるデータの活用がより一層進展することも想定される。

このような状況の変化も踏まえ、以下の方針で加速・強化すべき施策を取りまとめ、国際連携を図りつつこれらを実施していく必要がある。なお、今後予定されている次期戦略の策定に当たっては、各施策の実施状況等を踏まえ、総論部分についての議論を深化させることが適当である。

（1）サイバー空間ガバナンス

サイバー空間が民間部門が主体となって構築・運用している空間であり、データが利活用され、新しいサービス・技術が次々と産み出される場であることを踏まえ、我が国の立場・地位の保持も念頭に置いて、新たな技術・サービスに技術的・経済的に門戸を開放し、特定の関係主体に偏らないよう配慮しつつ、その自律的な発展を支持する。

（2）安全でクリーンなサイバー空間

国民の活動の場、経済活動の場として必要であるサイバー空間の健全な発展を確保するため、セキュリティ・バイ・デザインのより一層の推進を図りつつ、安全でクリーンなサイバー空間の実現を目指す。

（3）多様な関係主体による連携と役割分担

多様な関係主体（マルチステークホルダー）が連携しつつ、適切な役割分担を行いながら自発的・主導的に取り組むことを促す。その際、国は枠組みを整備し、取組を活性化・発展させる結節点の機能を果たす。

（4）グローバルな連携

サイバー空間においては、国境を意識することなく活動できるという長所を損なうことなく、そのセキュリティを確保することが重要であるため、上記の方針に基づく取組を進める上で国外の多様な関係者とも連携する。

３　各 論

（1）経済社会の活力の向上及び持続的発展

［これまでの取組・現状］

インターネットに接続される IoT 機器の種類・台数は年々増加しており、そのセキュリティ対策の強化が急務となっている。こうした中、IoT 推進コンソーシアム・総務省・経済産業省の官

民連携により、「IoT セキュリティガイドライン ver 1.0」(2016 年 7 月) を取りまとめた。また、IoT システムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明確化したものとして、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）において、「安全な IoT システムのためのセキュリティに関する一般的枠組」(2016 年 8 月。以下「一般的枠組」という。）を取りまとめた。

他方、昨年 9 月に、マルウェア「Mirai」に感染した IoT ボットネットによる 1Tbps 超の DDoS 攻撃が発生するなど、IoT 機器を踏み台にしたサイバー攻撃が顕在化しており、その脅威は今後も増大するものと予測される。

日本国内においても、相当数の IoT 機器が、既に感染している、または容易に感染する可能性がある状況と推測されるところ、現にインターネットに接続されている IoT 機器等に関して、全国規模での継続的かつ広範な実態調査が行われておらず、国内の状況を正確に把握できていないおそれがある。また、既にマルウェアに感染している IoT 機器については、その具体的かつ効果的な対策及び対処方法を、責任主体を明確にしたうえで、検討を行う必要がある。

こうした中、2020 年東京大会を控え、例えば、IoT 機器を踏み台にした大規模なサイバー攻撃が発生するような状況とならないよう、インターネットに接続される IoT 機器等の実態を正確に把握し、国際連携を図りつつ効率的かつ効果的な対策を早急に講ずる必要がある。その際、IoT 機器等の利用者、製造事業者、販売事業者、電気通信事業者等の関係主体の対策実施等における役割分担を明確化すべきである。

また、一般的枠組を具体化し、IoT についてのサイバーセキュリティ対策を進めていくためには、IoT に関係する各分野において、用語・定義が異なる現状を踏まえ、これらの用語・定義等について共通する用語の定義を図り、国内における各分野の規格に反映することで我が国の強みである高信頼・高品質を IoT システムにおいても訴求するとともに、これらの国際標準の策定に我が国が積極的に貢献することで国際競争力の強化を目指すことが適当である。

また、戦略の柱の一つである「経済社会の活力の向上及び持続的発展」の実現のためには、セキュリティ産業の活性化を推進するため、需要・供給両面から取組を進め、好循環を生み出していく必要がある。

［取り組むべき施策］

① ボット撲滅の推進

○ NISC、警察庁、総務省、経済産業省、民間企業等が協調・連携し、官民連携による「ボット撲滅」に向けた体制を構築し、対策を推進すること。その際、各関係主体の役割分担を明確化し、実態の把握、対策の実施・周知、再発防止・環境改善を一体的に実施することで、効率的かつ効果的な対策につなげること。

（主な取組）

ア 実態の把握

・政府内に体制を構築して継続的かつ広範な実態調査ができるよう、必要となる法的整理を行うこと。その際、当該調査によるインターネット上のサービスへの影響等を考慮するこ

と。

イ　対策の実施、周知

IoT 機器等と、これらの機器等が接続される情報通信ネットワークの側のそれぞれにおいて取り得る対策の実施・周知について、官民及び民間企業相互間の役割分担・責任関係を整理した上で、これらに必要な技術的・制度的枠組の構築を含めた環境整備を併せて行う。

・既に流通している IoT 機器等について、製造業者、販売業者、電気通信事業者等の協力を得て利用者等を特定し、必要なセキュリティ対策の実施を促す注意喚起ができるようにすること。また、不具合等が発見された場合に、既存の取組も活用しつつ、利用者、製造事業者、販売事業者、電気通信事業者等へ役割に応じた迅速な対処の協力を要請できる枠組みを構築すること。

・諸外国との連携を促進し、協調した対策を実施すること。

ウ　再発防止・環境改善

・利用者が適切な製品・サービスを選択できるよう、セキュリティ対策に係る必要な対策が行われているか確認できるような認証等の仕組みの構築を検討すること。

・IoT 機器等のセキュリティ対策が不十分なことが判明した場合には、利用者、製造関係事業者、販売事業者、電気通信事業者等の責任範囲を整理し、その範囲において、効率的な実態把握と実効性を持った対策が実施されるような制度を検討すること。

・IoT 推進コンソーシアム等を活用した関係主体間での情報共有を促進すること。

② 安全な IoT システムの創出による国際競争力の強化（国際標準化）

○ NISC、総務省、経済産業省が協調し、その他の関係府省と連携しつつ、官民連携により安全な IoT システムの創出に向けた体制を構築し、国際標準化等を推進すること、その際には、IoT を用いる様々な分野の官民の関係者と幅広く連携し、従来のセキュリティ 3 要件（機密性、完全性、可用性）に加え、安全を意識した要求条件を確立すること。

（主な取組）

ア　国際標準化

本部における検討体制と連携し、IoT システムに関係する分野に共通する用語を定義した上で、その設計、開発、運用に係る概念を共通化する取組を国際標準化として進める。

イ　国内の取組への反映

日本国内の様々な関係者が策定する基準やガイドラインについて、整合化を図り、標準のテンプレートをベースとしたものとなるよう促し、展開を図る。

③ セキュリティに係るビジネス環境の整備

○ NISC、総務省、経済産業省が協調し、我が国の政府機関や企業等のサイバーセキュリティの確保に向けて、サイバーセキュリティに係る投資を促進することで、セキュリティ産業における継続的な需要喚起を促す。

（主な取組）

ア　政府調達の拡充

政府が積極的に調達すべき製品・サービス分野及び要件を掲載したリストを改訂し、政府

機関においてこれらの製品・サービスの活用を奨励する。

イ　セキュリティサービスの活用促進

一定品質を備えたセキュリティサービスを認定する仕組みを構築し、供給側の競争力強化を図るとともに、これらのサービスへの活用を促す。

ウ　セキュリティ対策の意識喚起

サイバーセキュリティ経営ガイドライン等の普及啓発によって中小企業も含めた更なる意識改革を図り、需要側の意識喚起を図る。

(2) 国民が安全で安心して暮らせる社会の実現

［これまでの取組・現状］

基本法の施行及びその後の基本法一部改正法の施行により、政府機関に加えて、独立行政法人、特殊法人・認可法人のうち本部が指定するもの（指定法人）が監視・監査・原因究明調査の対象となった。基本法一部改正法の施行に合わせて、政府機関等の情報セキュリティ対策のための統一基準群の改定等、所要の規定の整備等を行った。また、独立行政法人等に対する不正な通信の監視体制を構築・運用するとともに、今年度から政府機関に対する不正な通信に対してもその検知・解析機能の強化等を図っている。

また、重要インフラサービス防護のための取組について、本部において、「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 月サイバーセキュリティ戦略本部決定）を取りまとめ、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、重要インフラ事業者等における先導的取組の推進、2020 年東京大会も見据えた情報共有体制の強化、リスクマネジメントを踏まえた対処態勢整備の推進等の取組を推進することとしている。

他方、政府機関・重要インフラ事業者等に対するサイバー攻撃が年々増加する中、攻撃・脅威情報の共有については、政府機関・重要インフラ事業者等で様々な取組がなされており、着実に進展している一方、情報の提供者が限定される、提供された情報が利用しづらい等の意見も散見されている。

このため、既存の情報共有体制等を活用し、情報の提供者における課題（組織内情報の提供による制度的リスク、提供する利点が少ないこと、類似情報の提供を行うビジネス環境との整合性等）を解消しつつ、利用者がより対策を講じやすい情報を共有することにより、サイバー攻撃の被害及び被害の拡大防止に更に努める必要がある。

2017 年度に、地方公共団体におけるマイナンバーの本格的な利用が開始されることから、サイバーセキュリティ対策強化の必要性がさらに高まっている。2015 年度に、総務省は、地方公共団体におけるセキュリティ強化対策「三層の構え」(※) を各地方公共団体に対して通知し、必要な支援等を行う等の取組を推進してきたが、地方公共団体へのサイバー攻撃が増加している中、中小規模の団体を中心に、人員や予算などの資源に制約がある中で、マイナンバー利用事務系等において、高いセキュリティレベルを確保する必要がある。

※　①マイナンバー利用事務系について、端末からの情報持ち出し不可設定等、②LGWAN 接続系とインターネット接続系を分離、③都道府県と市区町村が協力して、インターネットの接続口を一つに集約して、集中して高度な監視を行う「自治体情報セキュリティクラウド」を構築

グローバル化の進展が著しい現状において、大学等においても業務の遂行上、情報基盤は必要不可欠となっている。大学等の特徴である公共性の高さを鑑みると、不正アクセスによる情報漏えいやWebサイト改ざん等の情報セキュリティインシデントが発生した場合、信用の低下を招き、当該大学等の運営に影響することとなる。近年、大学等における情報セキュリティインシデントの発生が増加しており、情報セキュリティ対策は、経営上の重要課題である。大学等において情報セキュリティ対策を講ずるに当たっては、多様な構成員が、保護すべき情報を取り扱う状況にあるとの認識の下で、情報セキュリティ水準の向上に向け、組織的・計画的に取り組むことが必要である。

なお、地方公共団体や大学等における取組については、自律的な対応を前提として、更なる対策強化のあり方の検討が必要である。

［取り組むべき施策］

①情報共有・連携ネットワーク（仮称）の構築・運用

○　NISCが総務省、経済産業省と連携し、有用な情報を有するセキュリティ機関や民間事業者からのインシデント情報やその脅威情報の提供を促進し、警察庁等と協調しつつ、迅速な集約・分析、効果的な対策の共有を行う情報連携体制を構築することにより、サイバー攻撃の被害及び被害拡大を防止すること。その際、2020年東京大会に向けた対策と連動させるとともに、既存の情報共有体制から得られた教訓を活かした仕組みとすること。

さらに、NISCが官民連携の活性化を進める結節点として機能するよう、専門機関の活用等による体制の抜本的強化を図ることとする。また、一定期間後その効果等を検証し、改めて検討を行うこととする。

ア　官民が一体となって、効果的な情報連携体制を構築するための制度整備を実施。

・情報連携体制における情報へアクセスするための資格要件、アクセス権限を有する民間事業者の責務、官側の役割等を明確化するなどして有用な情報提供を担保。

・第三者提供を前提としない情報の提供及び共有を可能とする等、既存の情報共有体制において情報提供を行う際の阻害要因となっている法的課題に対処。

イ　情報提供者にとって提供しやすく、かつ利用者にとって対策しやすい情報の抽出及び環境の整備。

・事案に応じた提供内容をあらかじめ設定し、対策に効果的な内容(※)を適切なタイミングで共有することで、利用者が措置しやすい環境を整備。

※　標的型攻撃における初期のCCサーバへの通信のURL等の情報（短期）
脆弱性情報の深刻度（攻撃ごとに分類）を加味した情報　（中期）
ネットワーク上での攻撃等を分析した一般的な注意喚起　（長期）等
なお、情報共有は、セキュリティ事業者のビジネスを阻害せず、情報の種別に応じて、利用者の対策に効果的なタイミングを調整・勘案して行う。

・情報提供者・解析者の更なる負担が生じないよう既存の体制とも連携可能なルール、システムの共通化に繋がる仕組みを構築。

②深刻度判断基準の策定等によるサイバー攻撃対処態勢の強化

○　NISC及び重要インフラ所管省庁等が連携して以下の取組を推進し、重要インフラに対するサ

イバー攻撃に係る対処態勢を強化する。

・関係主体間で認識の共有を図り、迅速な対応要否等の判断に資するため、重要インフラサービス障害等の深刻度（レベル０：国民生活等に影響を与える可能性はない　～　レベル５：国民生活等に広範かつ著しい影響を与えるおそれが切迫、といった尺度）の判断基準について、重要インフラ専門調査会等の場における議論を踏まえ、本年度末までに暫定版を策定し、公表する。

・事業継続計画（BCP）及びコンティンジェンシープランの策定・改定時に考慮すべきサイバー攻撃リスクの特性等（攻撃者の存在と多様な攻撃目的、攻撃手口の高度化等）について、重要インフラ専門調査会等の場における議論を踏まえ、本年度末までに改定を行う「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」に盛り込む。

・関係主体による共同訓練を本年度も実施する。

○　NISC 及び重要インフラ所管省庁等と危機管理体制との連携を強化し、サイバー空間、物理空間の両方に影響を与える事象にも適切に対処する。

③政府機関・独法等における効率的・効果的防護体制の再構築

○　統一基準群に則り、政府機関等における情報システムにおけるログの取得・管理及び適切な監視、情報システム台帳の整備、主体認証情報の管理について政府機関等自らが措置を講じているところであるが、政府機関等における更なるセキュリティ対策の向上に向けて、今年度中を目途に、NISC において、関係府省庁と連携して、府省庁が自律的に状況を把握する能力を支えるべく、検知精度及び対処能力等の監視能力の向上及び即応化に資する端末等での新たな監視手法の導入や脆弱性の適切な把握が可能となるような仕組みについて検討するとともに、府省庁のセキュリティ対策状況に応じた GSOC との高度かつ効率的な連携の可能性についても検討する。その際、情報システムの侵入耐性診断を行うに当たり、自衛隊が有する知識・経験の活用等も検討する。

④地方公共団体におけるセキュリティ対策向上

○　中小規模の団体におけるセキュリティ対策について、技術的な対策には限界があるものの、ヒューマンエラーによる情報漏えいに対して、できるだけの対策を講じる必要があり、現行の国と地方の役割分担の考え方を踏まえ、国による地方への直接の関与（技術仕様、監査等）が、他の機関に比べ限定的な中で、高いセキュリティレベルを確保する必要がある。そのため、総務省において、本年度中に、セキュリティポリシーガイドラインを更新し、また、自治体情報セキュリティ向上プラットフォームを構築し LGWAN のセキュリティレベルを確保するとともに、セキュリティ人材及び体制の確保・充実を支援する等の取組を推進する。

⑤大学等における情報セキュリティ対策の向上

多岐に渡る情報資産、多様なシステムの利用実態といった大学等における多様性を踏まえ、当該特性に応じて、大学等の情報セキュリティ対策の強化を促進するとともに、大学等の相互の協力による自律的活動の向上に向けた取組を促す。

具体的には、各大学等は、教育・研究等の多様性に配慮しつつ、中長期的な情報セキュリティ対策基本計画を策定し、マネジメント面及び技術面の取組を推進する。また、大学等の連携

によるサイバー攻撃検知体制の整備や人材育成の取組を推進する。なお、国は、これらの取組に対し、必要な支援に努める。

○　大学等における自主的な取組

ア　マネジメント面

・企画・法務・広報など関係部門と連携したインシデント対応体制の構築と対処能力の向上

・情報セキュリティポリシーや情報の取扱規程等の見直しや組織への浸透

・多様な構成員に対応した教育・訓練や啓発活動の実施

・構成員の役割に応じた自己点検や中立性を有する者による監査の実施

イ　技術面

・組織内の情報機器の把握と適切なアクセス制御の実施

・重要情報を扱う機器へのアクセス等を監視する機能等の実装

・組織内で利用しているソフトウェアの適切な更新が可能な仕組みの整備

○　文部科学省等による支援

・大学等における自主的な取組の促進の観点から、インシデント対応力の向上やセキュリティ監査手法に関する研修の実施及び機会の充実、情報システムの侵入耐性診断の実施に関する支援、諸会議における周知、啓発及びグッドプラクティスの共有並びに情報セキュリティ対策基本計画の進捗状況のフォローアップその他自主的な取組加速のための支援を実施

○　大学等の相互協力による取組

国立情報学研究所において、大学等と連携し、SINET におけるサイバー攻撃検知システムの運用や、同システムの実環境を用いた技術職員の実地研修の実施、脅威情報等の共有促進により、大学等のインシデント対処能力向上を図る。また、連携機関の拡大については、今後、運営上の課題を含めて検討する。

大学等共通の課題の検討や知見の共有等について、各大学等の枠を超えて CSIRT 担当者同士のコミュニティを形成し、脅威情報の共有や共通課題の検討等を実施予定。

⑥サイバー犯罪・サイバー攻撃対策の強化

○　警察庁において、関係省庁と連携しつつ、サイバー攻撃に関する分析に係る人材の育成や、官民連携の枠組みを通じた情報共有、サイバー攻撃の発生を想定した共同対処訓練等の拡充を推進し、サイバー空間における情報収集・分析機能及び緊急対処態勢を強化する。また、民間事業者等における適切な対策を促すための広報啓発活動に加え、犯罪抑止に資する徹底した捜査活動や新たな手法等の検討を推進する。

⑦普及啓発・情報発信

○　NISC において、関係省庁と連携し、今後の IT 社会の一層の進展、IoT の普及等から中小企業、一般利用者等がサイバー社会により触れる機会がより多くなり、これらの利用者がサイバーセキュリティ対策に対する十分な理解・認識が進まないままに、様々なリスクに直面する現状を踏まえ、産官学民の様々な主体との連携を図ることにより普及啓発を行うとともに、評価を通じてより効果的かつ効率的なものとしていく。また、サイバー攻撃発生時や危険度の高い脆弱性が判明した時などに状況や対策についての情報発信や相談対応をより迅速に行えるよう関係機関の連携を図りつつ取組を強化する。

(3) 国際社会の平和・安定及び我が国の安全保障

［これまでの取組・現状］

サイバー空間の脅威は多様化・複雑化しており、海外においては、国家の関与や実空間における軍の活動との連動が疑われる高度なサイバー攻撃の事例も指摘されている。こうした増大するサイバー空間の脅威に適切に対処し、我が国の安全を確保するため、対処機関の能力強化、先端技術の活用や防護、政府機関・社会システムの防護に努めている。

サイバー攻撃が激化する中、国立研究開発法人の保有する先端的な技術情報を保護する対策の強化が必要となっている。独立行政法人に属する国立研究開発法人に対する基本法の枠組みの下での対策が本格化する中、従来の行政事務系の組織とは異なる研究機関特有の課題に対応する必要がある。

先端的な技術情報を守ることは、研究者自らの利益に直結することから、情報セキュリティ対策は当事者組織自身による取組が肝要であり、組織の状況を鑑みて、研究部門の長が研究員に対するガバナンスを効かせ、自らの技術情報を守るための情報セキュリティ対策を推進する体制を構築することが必要である。この様な観点で情報セキュリティ水準の向上を図るため、基本法の枠組みの下で法人の自主的な取組を国が支援するとともに、共通課題について当事者組織が相互協力することが必要である。取組を実施するに当たっては、研究開発を行いやすい環境と情報セキュリティ確保が両立するよう留意することが求められる。

さらに、サイバー空間における脅威は、容易に国境を越えるため、一国のみで対応することは容易ではない。我が国は世界各国との二国間・多国間の様々な枠組みを活用した協力・連携により、国際社会の平和・安定及び我が国の安全保障の実現に向けた取組を進めているが、今後、単にサイバーセキュリティそのものだけではなく、サイバー空間のガバナンスのあり方を含めた検討が求められる。その際、官民の多様な主体が関わることを念頭にマルチステークホルダーにより検討が進められることが重要である。

［取り組むべき施策］

①組織・分野 横断的な取組等による我が国の安全の確保

- ○ 国家の関与が疑われるものも含め、我が国の安全保障を脅かすようなサイバー空間における脅威から国民の安全・権利を守り、サイバー空間の自由かつ安全な利用を確保するため、政治・経済・技術・法律・外交その他の採り得る全ての有効な手段を選択肢として確保する。
- ○ 上記の観点から必要な対応が適時適切にとれるよう、内閣官房及び関係省庁との連携体制を構築し、体制の充実強化及び役割分担の明確化を図りつつ、国全体として、組織・分野横断的な取組を総合的に推進する。また、有志国・機関との連携をさらに推進する。
- ○ サイバー空間の状況把握・分析能力の一層の向上や自衛隊を含む対処機関の能力の質的・量的向上の取組を加速化する。

②先端技術の防護

国立研究開発法人について、先端技術情報を保護する観点から、当該法人のマネジメント面及び技術面の取組を促進するとともに、これら法人相互の協力による自律的活動の向上に向け、新たな取組を開始するこれら法人に対し、基本法に基づく国による支援を本格化させる。

この際、研究機関特有の課題に取り組むことが必要である。具体的には、研究人材の多様性・流動性が高い状況にある中、研究部門においては各研究部門の長によるガバナンスの下で対策を推進する体制を構築し、研究者に対する教育・訓練を充実することに加え、研究開発を行いやすい環境と情報セキュリティの確保の両立を図るべく、ユーザに依存しない対策を強化することが効果的と考えられる。また、組織内での情報セキュリティマネジメントの運用に際しては、研究部門と管理部門を通じた一元的な運用を強化することが重要である。

○　各法人における取組

ア　マネジメント面

・各研究部門の長がガバナンスを効かせ、自らの技術情報を守るための情報セキュリティ対策を推進する体制の構築

・研究部門を支えるため、管理部門との一元的な情報セキュリティマネジメントの強化

・技術情報の特性に応じた格付けの徹底等、研究機関特有の課題への取組を推進

イ　技術面

・ユーザの人的取組のみに依存しないシステム面での対策によるセキュリティの強化

○　国の監査等による専門的支援

・NISC において、基本法に基づく監査･監視の支援の運用本格化により対策を促進

・NISC が主催する CSIRT 研修を通じた各法人のインシデント対処能力の向上

○　国立研究開発法人自らの取組

・国立研究開発法人共通の課題の検討や知見の共有等について、当事者による相互協力･相互研鑽を実施

また、先端的な技術情報を保有する大学等に対しても、サイバー攻撃による当該情報の漏えいを防止するための自主的な取組を促すとともに、支援する。なお、これら取組の実施に当たっては、研究や教育の進展に資するよう、その特性にも配慮する。

③海外の多様な主体との多層的な連携の強化

○　サイバー空間においては、事象の影響が容易に国境を越えうることから、海外で生じたサイバー事案が我が国にも容易に影響を及ぼしうることを踏まえ、NISC 及び関係省庁が連携して、サイバー空間における国際的な法の支配の確立、ルール・規範づくり、信頼醸成、能力構築支援等について、外国政府や民間団体等の多様な主体との多層的な連携を進める。その実現に向け、様々な国際会議について積極的に実施・参加し、サイバー問題に関する情報の共有や意識のすり合わせを行い、海外における最先端の知見の取得を進め、具体的な協力関係を構築し、実際の行動に繋げる。

ア　国際場裡において、我が国サイバーセキュリティ戦略の基本原則である、情報の自由な流通、法の支配、開放性、自律性及び多様な主体の連携に基づき、これまで培われてきたグローバルなサイバー空間のガバナンスや管理のバランス等を擁護し、発展させる。これらを脅かすような国際ルールの変更や資本・インフラの展開、技術標準の形成等を目指す取組みに対しては、同盟国・有志国、民間団体等の多様な主体と連携した多層的な対応により対抗し、自由なサイバー空間そのものを守る。

イ　外交当局間、サイバーセキュリティ当局間、防衛当局間、法執行機関間、CSIRT 間、民間

団体間等による、それぞれのレイヤーにおける多様な主体との連携を強化し、国際連携プロジェクト等、自由、公正かつ安全なサイバー空間を実現するための実際の行動に繋げる。

※具体的な行動の例: 国際場裡におけるルール・規範づくりに関する政策調整、ボットネット撲滅、サイバー事案の深刻度評価指標の国際的整合性確保、IoT 関連の国際標準化、AIS の推進及び関連情報の防護活動への利用、国際サイバー演習等の実施による能力構築やサイバー事案発生時の情報連携体制の確保及び強化、情報共有・連携ネットワーク（仮称）やオリンピック・パラリンピック CSIRT 等の構築・運用における国際連携の重視、任務保障のための重要インフラ防護等の強化、法執行の観点からの国際機関・外国治安情報機関等との情報交換・捜査共助・職員派遣、ISAC 間連携の推進 等

ウ　様々な政策手段を活用し、開発途上国における官民を対象にした能力構築支援を積極的に実施する。能力構築支援に当たっては、「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（基本方針）」（平成 28 年 10 月サイバーセキュリティ戦略本部報告）に留意する。

④サイバー犯罪・サイバー攻撃対策の国際的な連携の強化

○　警察庁及び関係省庁が連携して、サイバー犯罪に関する条約、刑事共助条約、ICPO 等の枠組みを活用した国際機関、外国治安情報機関等との間における国際捜査共助、国際会議を通じた多国間における情報交換、海外への職員派遣等による国際連携を推進し、国境を容易に越えるサイバー空間の脅威に対処する。

(4) 横断的施策

［これまでの取組・現状］

サイバーセキュリティ分野における人材育成については、戦略を踏まえ、サイバーセキュリティ人材育成総合強化方針（2016 年 3 月 31 日サイバーセキュリティ戦略本部決定）において、民間分野、政府機関双方における人材育成の具体的な強化方針を示した。

人材の需要と供給の好循環の形成を基本的な考え方として、人材の需要面では、経営層の意識改革を諮るとともに、経営層と実務者層をつなぐ橋渡し人材層の育成を図ることとした。また、人材の供給面では、産業界で求められる人材層を提示した上で、教育の充実、演習環境の整備、能力の可視化を図ることとした。

また、政府機関における人材育成については、各府省庁における司令塔機能の抜本的強化として、各府省庁において、サイバーセキュリティ・情報化審議官等を設置するとともに、セキュリティ・IT 人材確保・育成計画を作成し、フォローアップを実施することとした。また、橋渡し人材（部内育成の専門人材）の確保・育成を図るため、体制の整備・人材の拡充、研修体系の抜本的整理、適切な処遇の確保等を実施することとした。

民間分野における人材育成については、同強化方針を踏まえて策定したサイバーセキュリティ人材育成プログラム（2017 年 4 月 18 日サイバーセキュリティ戦略本部決定）において、IoT やビッグデータ、AI など、IT を利活用し、新たな価値を創造への対応が求められていることも念頭におきつつ、各階層別に方向性を示しており、経営層の意識改革、橋渡し人材層の育成、チームとなってサイバーセキュリティを推進できる実務者層の人材育成等について取り組むことが重要としている。今後は、同プログラムを踏まえ、人材育成についての全体像を俯瞰しつつ、人

材の不足に対する今後の対応の検討や、モデルとなるカリキュラムの策定をはじめとした施策間連携について、官民が連携して、取り組む。

また、政府機関においても、2016 年 8 月末に「各府省庁セキュリティ・IT 人材確保・育成計画」を策定し、その実施状況について、本年 3 月にフォローアップを実施した。まず、体制の整備として、2017 年度に、本府省庁全体で約 80 の定員増を実現したほか、橋渡し人材候補者等として、5 府省庁で 17 名の職員を新規に採用した。更に、政府全体でのべ約 4,000 名が総務省の情報システム統一研修を受講するとともに、一部の省庁で新たに NISC、IT 室等への出向を実施している。引き続き、「各府省庁セキュリティ・IT 人材確保・育成計画」に基づく取組を進めるとともに、フォローアップを行っていく必要がある。

サイバーセキュリティ分野における研究開発については、様々な人文社会科学的視点も含めた「サイバーセキュリティ研究開発戦略」の策定等の取組を進めてきたところであり、NISC 及び関係府省庁の連携の下、具体的なサイバーセキュリティの研究分野やテーマについて検討を行うなど、同戦略を具体化させるための取組を行う必要がある。その際、人工知能（AI）をはじめ、IoT 技術、AR（拡張現実）・VR（仮想現実）技術、ブロックチェーンなどの革新的な技術は、社会システムを変容させ、人間の本質にせまる課題を内包する可能性があるため、サイバーセキュリティの概念が変化する可能性があることを踏まえた対応が必要である。

［取り組むべき施策］

①経営層の意識改革や、橋渡し人材等幅広い階層における人材育成・確保の継続的な促進

○　サイバーセキュリティ人材の不足（現在 28.1 万人、13.2 万人不足）に対応するため、IT 人材（現在 92 万人）が、その一つの役割としてセキュリティを担えるよう、モデル・カリキュラムの策定等必要な取組の明確化を図る。

○　関係省庁において、高度なサイバーセキュリティの技術を持つ人材のコミュニティの形成に資するよう、高度人材の確保に向けた取組を推進するとともに、各施策間の連携を図る。

○　会社法等の企業経営に係る制度や訴訟・コンプライアンス対応におけるサイバーセキュリティの関わり方等について検討を進め、経営層の意識改革を促すための取組を行う。

○　中小企業等においては、サイバーセキュリティ対策に使えるリソースに限界があることから、外部の能力や知見を活用しつつ、効率的に進める方策の検討が必要である。特に、クラウドサービスの活用等、中小企業のセキュリティを実質的に高めるための取組を行う。

○　組織のサイバーセキュリティ対策や製品開発等に必要なサイバーセキュリティに関わる情報にアクセスしやすいよう、信頼できるセキュリティ人材育成に向けた環境整備を行い。対策の普及啓発に取り組む。

○　各府省庁において、橋渡し人材の適切な処遇の確保等、政府機関における人材確保・育成に引き続き取り組む。

②研究開発等の推進

○　情報システムの進化（つながる（IoT）、知能化する（AI）、広がる(ネットワーク技術)）を見据え、要素技術の研究だけではなく、システムインテグレーションなど研究開発の視野を広げた取組を推進する。

○　人工知能（AI）をはじめ、IoT 技術、AR・VR 技術、ブロックチェーンなどの革新的な技術

は社会システムを変容させ、人間の本質にせまる課題を内包する可能性がある中、単に情報システムへの脅威に対応するだけでなく、「人間」や「社会」を一体として捉え、研究開発の内容を検討することが必要である。多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくため、本年7月に策定する「サイバーセキュリティ研究開発戦略」に基づき、これまでのサイバーセキュリティ技術の専門分野にとどまらず、人文社会科学も含めた国内外の幅広い分野における研究組織や研究者に対し、その内容を発信し、普及啓発活動に取り組むこととする。また、NISC及び関係省庁が連携して、同戦略を踏まえた具体的なサイバーセキュリティの研究分野やテーマの検討などに取り組む。

○ NISC及び関係省庁が連携して、サイバー攻撃の解析等サイバーセキュリティ対策の向上に資する関連技術の研究開発を推進する。

(5) 推進体制

［これまでの取組・現状］

戦略を踏まえ、基本法の一部改正法により、国による監視、監査、原因究明調査の対象を、独立行政法人、サイバーセキュリティ戦略本部が指定する特殊法人・認可法人に拡大することとした。あわせて、同法により、本部の事務のうち、監査又は原因究明調査の一部をIPAに委託することができるとされた。

また、国立研究開発法人情報通信研究機構法（平成11年法律第162号）を改正し、サイバーセキュリティに係る演習の質的向上や継続的・安定的な運用に向け、NICTを演習の実施主体とすることとした。

2020年東京大会のサイバーセキュリティの確保に向けては、重要サービス事業者等を対象としたリスク評価を実施するとともに、サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）の運用に向け、関係府省庁、東京都、大会組織委員会等との協議の上、基本的枠組みを平成28年度に決定し、現在、具体的な調整を開始したところである。

深刻化が続くサイバー攻撃の脅威に対応するため、引き続き、国における体制強化に取り組むとともに、2020年東京大会のサイバーセキュリティの確保に向けた取組を強化する必要がある。

［取り組むべき施策］

①2020年東京オリンピック・パラリンピック競技大会に向けた態勢の整備

○ 「2020年東京オリンピック競技大会・東京パラリンピック競技大会に向けたセキュリティ基本戦略（Ver.1）」に基づき、NISC、関係府省庁、東京都、大会組織委員会等が連携して、以下の取組を推進する。

ア サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）の構築

・セキュリティ調整センター（仮称）による調整の下、物理的な対策と連動しつつ、政府機関・重要サービス事業者等に対するサイバーセキュリティに係る脅威・事案情報の収集・提供及び対処支援調整を行う中核的組織として、サイバーセキュリティ対処調整センターを平成30年度末目途に構築する。また、組織委員会が講じる対策等に対して適切な助言・支援が行えるよう、東京オリンピック競技大会・東京パラリンピック競技大会推進本部との連携等、制度的枠組の検討を併せて行う。

・同センターを中核とする対処のため、同センターに一定程度の専任要員を配置し、計画的に訓練を行うとともに、大会組織委員会と合わせて、関係する重要サービス事業者、セキュリティ事業者等の 200 人以上の技術者等との連携態勢を整備する。

イ　セキュリティ情報センターの構築

・2017 年 7 月を目途に警察庁に設置することとされているセキュリティ情報センターにおいて、国の関係機関の協力を得て、サイバーセキュリティ対処調整センターと相互に緊密に連携し、サイバーセキュリティに係るものを含む 2020 年東京大会の安全に係る情報を集約し、大会の安全に対する脅威及びリスクの分析・評価を行い、関係機関等に対し必要な情報を随時提供する。

ウ　リスクマネジメントの促進

・2020 年東京大会の安全・円滑な準備及び運営並びに継続性の確保のため、リスクの明確化、第三者による監査の支援等を通じた重要サービス事業者等におけるリスクマネジメントを促進するとともに、横断的リスク評価（今年度から開始して 2018 年度までに全分野において実施）を行い、これに基づくマネジメントを強力に進める。その際、サイバー空間における事象が物理空間に影響し得ることも念頭に、特に影響度が大きい重要サービス事業者について、その業務、情報システム、制御システム等の経営資源の安全及び継続性の確保の観点からの鳥瞰図的な把握及び検証を行い、リスクの確認及び対策を進める。

4　今後の予定等

関係省庁は、本レビューを踏まえて、本年度中に取組が可能となるものから開始し、１年以内に施策全体を実施することとする。この際、必要に応じて、制度的な環境整備、予算措置等の具体化を検討する。

また、本レビューに記載の施策の取組状況等を踏まえ、次期戦略策定につなげることとする。

以　上