（参考①）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

その２

官民連携による重要インフラ防護の推進

重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動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。

重要インフラ（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（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

※空港分野については、７月２５日の行動計画改定により追加

ＮＩＳＣによる調整・連携

重要インフラ所管省庁（５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］

関係機関等

- 情報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］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］

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

安全基準等の整備・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	防護基盤の強化
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	連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化	官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化	リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進	重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

（参考②）サイバー攻撃による重要インフラサービス障害等の深刻度評価基準(初版)概要

平成30年７月25日
サイバーセキュリティ戦略本部決定

深刻度評価基準は、サイバー攻撃により発生した重要インフラサービス障害等が国民社会に与えた影響の深刻さを、NISCが評価・公表することにより、事業者、政府関係機関、国民等がその深刻さに関する共通の理解を得て、冷静かつ適切な対応を行えるようになることを目的とする取組。

今回、この取組の第一段階として、重要インフラ専門調査会が作成した「発生したサービス障害が国民社会に与えた影響全体の深刻さ」を『事後に』評価するための基準の試案について、パブリックコメントを経た上で必要な修正を行い、初版として決定。

表１　深刻度表

深刻度	重要インフラサービス障害等による国民社会への影響
レベル４（危機）	サービスの持続性又はサービスに関する安全性に、著しく深刻な影響が発生
レベル３（高）	サービスの持続性又はサービスに関する安全性に、大きな影響が発生
レベル２（中）	サービスの持続性又はサービスに関する安全性に、一定の影響が発生
レベル１（低）	サービスの持続性又はサービスに関する安全性に、ほぼ影響なし
レベル０（なし）	サービスの持続性又はサービスに関する安全性に、影響なし

表２　評価の観点及び評価指標

国民社会への影響	
評価の観点	評価指標
サービスの持続性への影響	提供支障（範囲・時間・代替性等）
	同時多発性
サービスに関する安全性への影響（施設・設備の安全性を含む）	人的・物的被害（人数・被害額等）
	住民避難等（範囲等）
	環境影響（原状回復費用・範囲等）
	同時多発性
その他	サービスに対する信頼低下

表３　評価手法の概要

深刻度	国民社会への影響		
	サービスの持続性への影響	サービスに関する安全性への影響	その他（信頼低下）
レベル４（危機）			
レベル３（高）			
レベル２（中）			
レベル１（低）			
レベル０（なし）			

5～7．2020年東京大会とその後を見据えた取組、情報共有や事態対処に関する取組:取組の例

2020年東京大会とその後を見据えた取組

2020年東京大会のサイバーセキュリティの確保及びその後を見据えた施策を推進

＜内閣官房＞
・「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推進本部」の下の「セキュリティ幹事会」で決定された基本戦略に基づき大会の安全に関する情報の集約等の取組を推進

サイバーセキュリティ対処調整センターの構築

リスクマネジメントの促進

・大会後も各種施策は適用範囲を拡大して引き続き推進し、整備した仕組み、その運用経験及びノウハウはレガシーとして、以降の我が国の持続的なサイバーセキュリティの強化のために活用

従来の枠を超えた情報共有・連携体制の構築

「参加・連携・協働」の観点から、各主体との緊密な連携の下、国はISACを含む既存の情報共有における取組の推進を支援し、新たな役割を果たしていく

＜内閣官房＞
・官民の多様な主体が相互に連携し、安心して相互にサイバーセキュリティ対策に資する情報の共有を図るための体制を構築
・各主体が積極的に情報共有に貢献できる環境整備、処理の自動化等を推進

大規模サイバー攻撃事態等への対処態勢強化

大規模なサイバー攻撃の脅威から国民・社会を守るために、国が一丸となってサイバー空間の脅威への危機管理に臨む

＜関係府省庁＞
・関係府省庁、重要インフラ事業者等が連携したサイバー空間と実空間の横断的な対処訓練の実施

＜警察庁、個人情報保護委員会、経済産業省＞
・官民連携の枠組みを通じた情報共有を推進
・民間事業者等の対処能力の向上を支援する取組を推進

（参考①）2018年平昌オリンピック・パラリンピック競技大会における状況について（概要）

NISCの対応

1．概要

日本の情報セキュリティ関係組織等で検知した攻撃予見情報・観測/分析結果情報を、韓国側窓口に提供。また、大会期間中・終了直後に職員を派遣し、平昌大会におけるサイバーセキュリティ対策・サイバー脅威情勢について情報収集。

2．実施期間

○情報共有
　オリンピック期間　2/2～25　【 大会期間：オリ 2/8～25（開会式2/9、閉会式2/25）】
　パラリンピック期間　3/9～18　【 大会期間：パラ 3/9～18（開会式3/9、閉会式3/18）】
　情報セキュリティ関係機関より大会に関係する**355件の情報を集め**、韓国側窓口へ**111件提供**

○情報収集

KISA（韓国情報保護振興院）、韓国警察庁、平昌大会組織委員会、MPC（メインプレスセンター）、IBC（国際放送センター）等とのミーティングを実施

・大会運営に重大な影響を与えるようなサイバー攻撃は発生せず
・大会準備期間に約６億件、大会期間中に約550万件のサイバー攻撃が発生、開会式においてサイバー攻撃に起因して一部のサービスが利用できなくなったとの報道
　- メインプレスセンター内で一部のネットワークに接続できない不具合
　- 大会公式サイトにおいて一時的に入場チケットを印刷できない状態
　- 内部のインターネット、Wifiが使用できない事態
　- 大会が近づくにつれて、大会に関連するフィッシングメールが増加


国際放送センター


メインプレスセンター

（参考②）サイバーセキュリティ基本法の一部を改正する法律案の概要

趣旨

サイバーセキュリティに対する脅威が一層深刻化する中、我が国におけるサイバーセキュリティの確保を促進し、2020年東京オリンピック・パラリンピック競技大会の開催に万全を期すため、**官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行う**ための協議会を創設する等の措置を講ずる。

概要

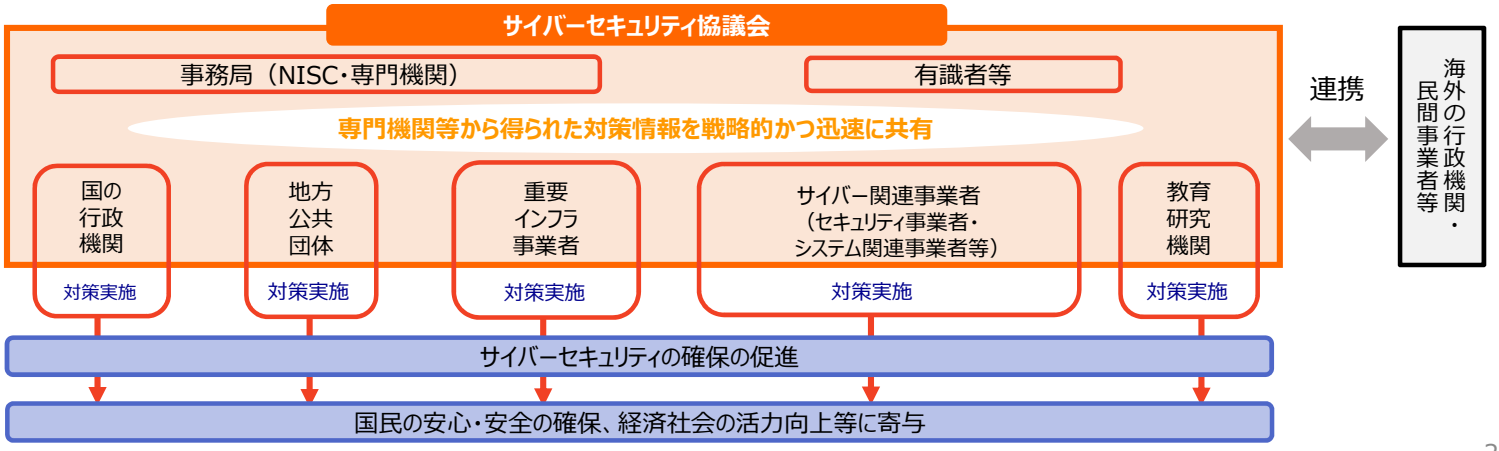
- **サイバーセキュリティ協議会の創設**

官民の多様な主体が相互に連携して情報共有を図り、必要な対策等について協議を行うための協議会を、サイバーセキュリティ戦略本部長等が創設するとともに、構成員に対して遵守事項（秘密保持、情報提供の協力）等を定める。

- **サイバーセキュリティ戦略本部による連絡調整の推進**

本部の所掌事務に、事象が発生した場合における国内外の関係者との連絡調整に関する事務を追加し、当該事務の一部を政令で定める法人に委託することができることとするとともに、当該法人に対して秘密保持義務等を定める。

【施行期日】 公布の日から起算して一年を超えない範囲内において政令で定める日



【4．目的達成のための施策】 「国際社会の平和・安定及び我が国の安全保障」に係る諸施策の目標及び実施方針のポイント

自由、公正かつ安全なサイバー空間の堅持

国際社会の平和・安定及び我が国の安全保障のために、自由、公正かつ安全なサイバー空間は必要不可欠である。自由、公正かつ安全なサイバー空間を堅持するため、国際場裡において我が国の立場を発信し、我が国の安全の確保に取り組み、国際協力・連携を進める。

1．自由、公正かつ安全なサイバー空間の堅持

- 自由、公正かつ安全なサイバー空間の理念の発信
  (我が国の意見表明や情報発信、サイバー空間の発展を妨げる取組への対抗等)
- サイバー空間における法の支配の推進
  (国際法の適用、規範の形成・普遍化についての議論への関与等)

2．我が国の防御力・抑止力・状況把握力の強化

- 国家の強靭性の確保
  (関係機関の任務保証、先端技術等の防護等)
- サイバー攻撃に対する抑止力の向上
  (実効的な抑止のための対応、信頼醸成措置等)
- サイバー空間の状況把握の強化
  (関係機関の能力向上、脅威情報連携等)

3．国際協力・連携

- 知見の共有・政策調整
- 事故対応等に係る国際連携の強化
- 能力構築支援

１．サイバーセキュリティ分野における国際連携：取組の例

サイバー空間に関するグローバルな議論

- サイバー空間における国際法の適用・規範の形成と普遍化、我が国の意見表明や情報発信、最先端の知見の共有、信頼醸成、情報共有等を目的として、Ｇ７、ＯＥＣＤ、インターネット・ガバナンス・フォーラム、国連サイバー政府専門家会合（GGE）、Meridian（※１）、IWWN（※２）、サイバー空間に関する国際会議（ロンドン・プロセス）、ＡＲＦ（※３）等に参加

※１　重要インフラ防護に関する国際連携を推進する場として2005年に英国で始まった会合。我が国の他、欧米やアジアの各国の政府職員が参加し、重要インフラ　防護に関するベストプラクティスの交換や国際連携の方策等について議論

※２　2004年に米国土安全保障省と独連邦内務省の主導により創設された枠組。サイバー空間の脆弱性、脅威、攻撃に対応する国際的取組を促進することを目的とする。先進各国のサイバーセキュリティ担当機関及び国を代表するCSIRT（インシデント対処を行う部門）が参加

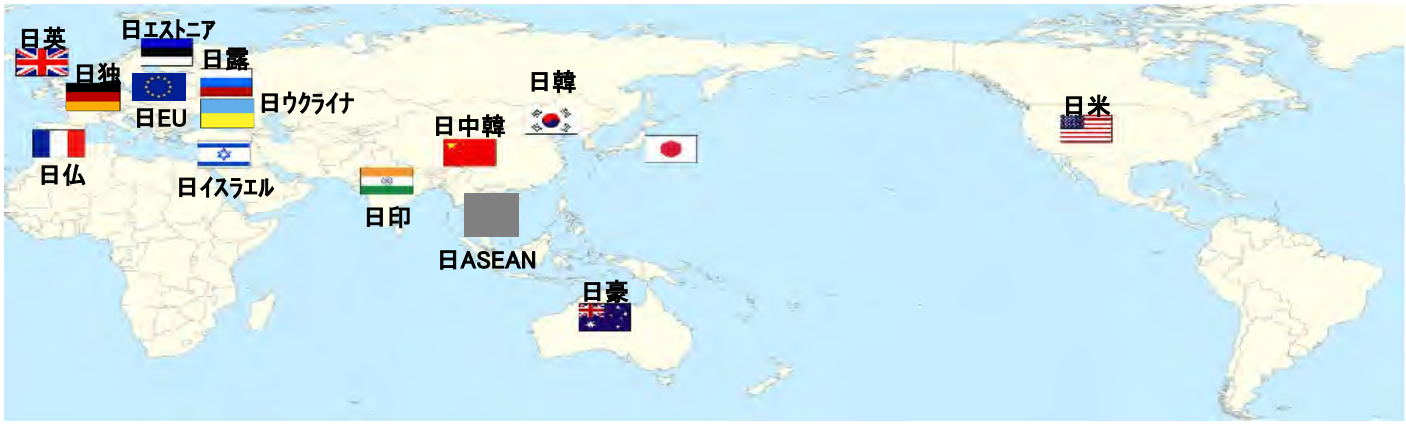
※３　我が国が、2017年にマレーシア・シンガポールと共に立ち上げた「サイバーセキュリティに関するＡＲＦ会期間会合」において、アジア・太平洋地域のサイバーセキュリティに関する安全保障環境を向上させるため、ASEAN地域フォーラムを通じた信頼醸成に取り組んでいる。

二国間協議

- 各国との知見の共有・政策調整を目的として、英国、インド、米国、EU、中韓、イスラエル、仏、エストニア、豪州、ロシア、独、韓及びウクライナとの間でサイバー協議を実施。各国との間で年1回程度の頻度でサイバー空間に関する政府横断的な政策協議を継続的に実施。我が国のサイバーセキュリティ政策を紹介しつつ、具体的トピックを議論

能力構築支援

- セキュリティマネジメント体制の確立、維持、改善などを目的として日ASEANサイバーセキュリティ政策会議等を実施

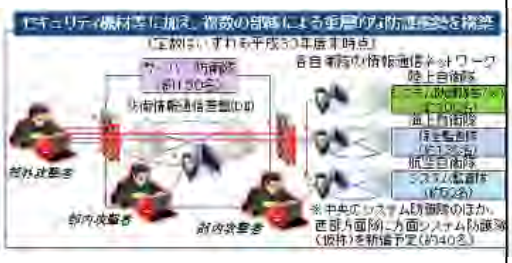


２．我が国の防御力・抑止力・状況把握力の強化:取組の例

サイバー攻撃から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靭性を確保し、国家を防御する力（防御力）、サイバー攻撃を抑止する力（抑止力）、サイバー空間の状況を把握する力（状況把握力）のそれぞれを高める。

国家の強靭性の確保

＜防衛省＞
・サイバー攻撃対処を行う部隊の能力の向上、自らの活動が依存するネットワーク・インフラの防護の強化、自衛隊の任務保証に関係する主体との連携の深化

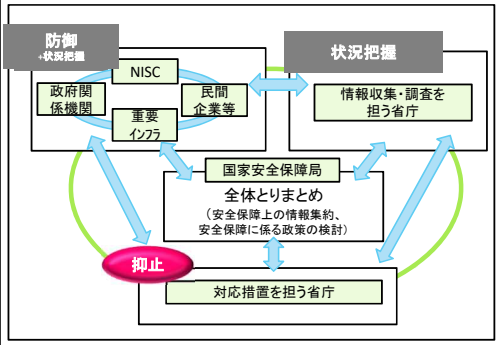


・調達する情報システムに係る情報セキュリティ上のサプライチェーンリスク対策として、調達仕様書に係る関連規則の整備を行う。

サイバー攻撃に対する抑止力の向上

＜内閣官房、関係省庁＞
・同盟国・有志国と連携し、政治・経済・技術・法律・外交その他の取り得るすべての有効な手段と能力を活用し、断固たる対応をとる。

・内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進



＜内閣官房、外務省、関係省庁＞
・ARFや二国間協議等において、政策の共有や連絡体制の構築等を通じた信頼醸成

サイバー空間の状況把握力の強化

＜内閣官房、外務省、警察庁、法務省＞
・諸外国関係機関との情報交換等国際的な連携を通じた、サイバー攻撃に関する情報収集・分析

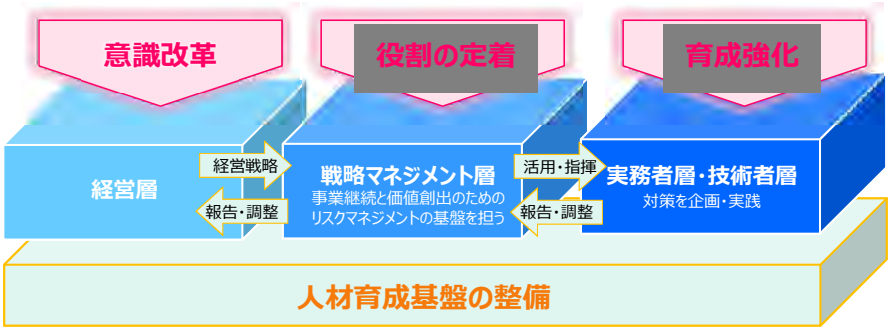
＜警察庁＞
・サイバー空間に関する観測機能の強化等によるサイバーフォースセンターの技術力の向上

サイバーセキュリティに関する共通基盤的な取組の推進

サイバーセキュリティを支える基盤的取組として、横断的・中長期的な視点で、人材育成・確保や研究開発に取り組むとともに、サイバー空間で活動する主体としての国民一人一人が、サイバーセキュリティに取り組むような全員参加による協働を推進

1．人材育成・確保

- 「戦略マネジメント層」の育成・定着
- 実務者層・技術者層の育成
- 人材育成基盤の整備、国際連携の推進
- 各府省庁のセキュリティ人材の確保・育成強化

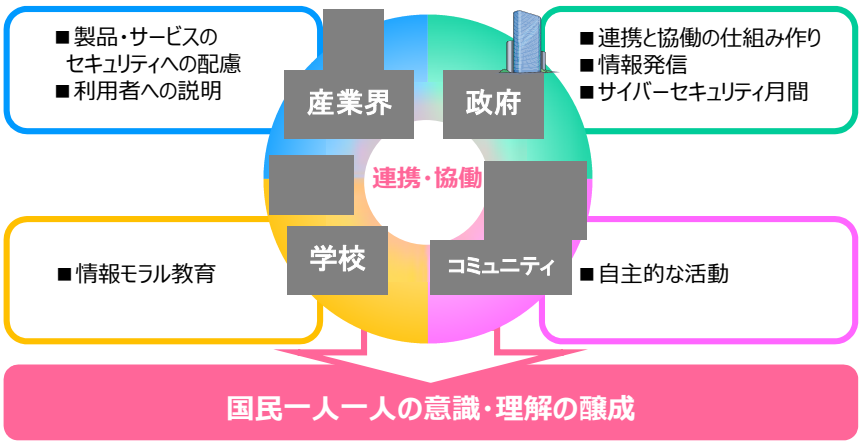


2．研究開発の推進

- 実践的な研究開発の推進
  （検知・防御等の能力向上、不正プログラム等の技術的検証を行うための体制整備等）
- 中長期的な技術・社会の進化を視野に入れた対応

3．全員参加による協働

- サイバーセキュリティの普及啓発に向けたアクションプランの策定とそれに基づく連携・協働
- 「サイバーセキュリティ月間」などを通じた情報発信

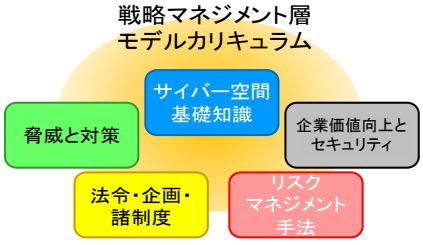


1．人材育成・確保：取組の例（1／2）

人材の需要と供給を相応するための好循環を形成するため、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化

「戦略マネジメント層」の育成・定着

＜内閣官房＞
・戦略マネジメント層育成に向けて、必要な知識・スキルを身に着けるための試行的取組を検討



＜経済産業省＞
・重要インフラ等における実際の制御システム等の安全性・信頼性検証を実施

実務者層・技術者層の育成

＜総務省＞
・NICTに組織した「ナショナルサイバートレーニングセンター」を通じ実践的サイバー防御演習（CYDER）を実施

＜経済産業省＞
・日本ネットワークセキュリティ協会が実施するセキュリティ技術コンテスト「SECCON 2018」の普及・広報支援

人材育成基盤の整備、国際連携の推進

＜文部科学省＞
・新学習指導要領の実施を見据え、発達の段階に応じた情報セキュリティを含めた情報活用能力を培う教育を一層推進する。また、教員等を対象とした研修を実施する。

＜総務省＞
若手セキュリティイノベーター育成プログラム「SecHack365」の実施

＜内閣官房＞
・人材育成に取り組む大学や公的機関等の研究・教育プログラムに係る基準や諸外国との連携方策について検討

1．人材育成・確保：取組の例（２／２）

サイバーセキュリティ人材育成総合強化方針（平成28年3月31日 サイバーセキュリティ戦略本部決定）に基づき、各府省庁におけるセキュリティ人材の着実な確保・育成を継続して進めていく。

「各府省庁セキュリティ・IT人材確保・育成計画」に基づく育成

＜内閣官房・各府省庁＞
「サイバーセキュリティ人材育成総合強化方針」に基づき策定した「各府省庁セキュリティ・IT人材確保・育成計画」について、内閣官房の主導によりPDCAサイクルをさらに充実させ、諸施策をより一層推進する。

① 体制の整備・人材の拡充
- ・セキュリティ・ITに係る体制の整備
- ・ポストに応じた適切な処遇の確保を実施

② 有為な人材の確保
- ・積極的な広報の実施
- ・適性が認められる者の採用

③ セキュリティ・IT人材育成支援プログラム
- ・研修の積極的受講
- ・NISC等への出向、大学院等への派遣の推進

各府省庁セキュリティ・IT人材確保・育成計画

④ 人事ルート例（キャリアパスのイメージ）
- ・高位のポストまでを見据えた人事ルート例を設定

⑤ 一般職員のリテラシー向上
- ・新人研修等でのセキュリティ・IT研修の実施等

サイバーセキュリティ・情報化審議官による司令塔機能の下、毎年度計画の**見直し**を実施！

（参考）サイバーセキュリティ人材育成取組方針（概要）

平成30年6月7日
サイバーセキュリティ戦略本部報告

・「サイバーセキュリティ人材育成プログラム」（平成29年４月決定）、「中間レビュー」（平成29年７月決定）を踏まえ、①経営層によるリスクマネジメントの一環としてのサイバーセキュリティ対策の推進、②戦略マネジメント層の人材像や各人材層におけるモデルカリキュラム等について、それぞれ「セキュリティマインドを持った企業経営WG」（主査：林紘一郎情報セキュリティ大学院大学教授）、「サイバーセキュリティ人材の育成に関する施策間連携WG」（主査：後藤厚宏情報セキュリティ大学院大学学長）において検討を実施。
・ 本取組方針の内容を今夏策定する次期サイバーセキュリティ戦略に反映し、具体的な取組を推進。

	経営層	戦略マネジメント層	実務者層・技術者層
役割	● ビジネスやサービスの着実な遂行（任務保証）が重要 ● 事業継続と価値創出のためのリスクマネジメントの一環として、対策を推進	●事業継続と価値創出に係るリスクマネジメントを中心となって支える役割 ●経営層の方針を踏まえた対策立案、実務者・技術者の指揮	●方針を踏まえたセキュリティ対策の企画・構築・実施
課題	◆リスクマネジメントに向けた、経営層の理解と意識改革の推進 ◆業種・業態の違いを踏まえた、サイバーセキュリティの位置付けの明確化とリスクマネジメントの浸透 ◆取組に対する経営上のインセンティブ付与	◆マネジメント機能の中でサイバーセキュリティリスクを考慮する必要 ◆戦略マネジメント層向けの適切な教材やプログラムが存在しない 人材規模・キャリアパス（需要）と、人材育成施策（供給）の好循環	◆経営層・戦略マネジメント層を支え、他の専門人材とチームの一員として対処できる人材の育成 ◆新たな技術やシステム開発手法の知識・スキルの育成
今後の施策の方向性（産学官の連携）	○**経営層の理解と意識改革の推進** ✓経営層が果たすべき役割、認識の共有 ✓経営層向けのツールの検討 ✓経営層向け伝道師の発掘・派遣 ✓「経団連サイバーセキュリティ経営宣言」の普及 ○**業種・業態別の差異を踏まえた基盤の整備** ✓業種・業態別に対策レベルを示すツールの整備 ✓企業関係法制度の整理に向けた検討 ○**サイバーセキュリティ投資のためのインセンティブ** ✓情報開示の推進（ガイドラインの策定等） ✓税制優遇の執行やサイバー保険活用の検討	○**組織における戦略マネジメント層の定着** ✓戦略マネジメント層の意義に対する経営層の理解の推進 ✓戦略マネジメント層の機能の明確化 ✓戦略マネジメントとセキュリティ対策が調和した指針の整備 ○**カリキュラム・教材開発と学び直しの推進** ○**サイバーセキュリティ人材育成施策の充実・強化と施策間連携の推進** ○**人材育成の「見える化」の推進** ✓ 米国の取組等を参考にしつつ、産学官連携により需要と供給の「見える化」を推進 [例] 人材規模・キャリアパスの明確化、カリキュラム・教材等が一覧になったポータルサイトの整備、育成プログラムの適切な評価基準の策定等	○**経営層・戦略マネジメント層を支える人材育成** ✓産学官連携によるカリキュラムの検討・実施 ○**クラウドや先端技術等の利用に係る人材育成** ✓先端技術等の利用に関わるセキュリティの知識・スキル育成

若年層における教育の充実
＜課題＞ ICTの基本的な原理・仕組みなどを理解し、論理的思考力を育てるとともに、情報モラル教育も重要
＜施策＞ 初等中等教育段階での教育課程内の取組に加え、地域や企業等で、自由に機器・ツールを用いて学べる機会を創出

中小企業関連の取組
＜課題＞ 知識・スキルが十分ではなく、セキュリティ対策への投資が困難。踏み台となった場合、社会への影響が大きい。
＜施策＞ 業種毎のアプローチ、セキュアモデル（クラウド活用等）と一体の対策集の策定・普及、インセンティブの仕組（税制優遇等）の検討

※基本的には、経営層及び中小企業関連の取組については、企業経営WG、それ以外の部分は施策間連携WGの報告書に基づく。

2．研究開発の推進：取組の例（１／２）

・実空間とサイバー空間が一体化していく中、サイバー空間におけるイノベーションの進展とそれに対するサイバー攻撃の脅威を踏まえた、実践的なサイバーセキュリティの研究開発を実施
・併せて、中長期的な技術・社会の非連続的進化を視野に入れた対応も必要である。

IoT社会に対応したサイバー・フィジカル・セキュリティ

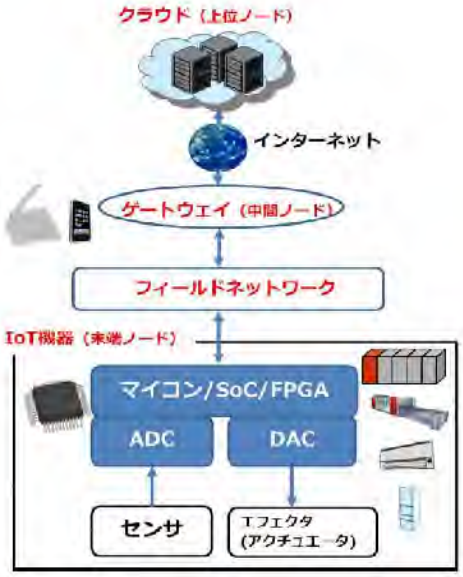
＜内閣府SIP＞

・セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、中小企業を含むサプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及び社会実装を推進。

IoTの安全確保に不可欠なハードウェアセキュリティの確保

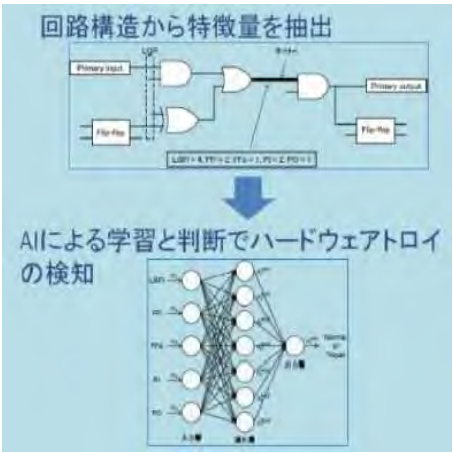
＜経済産業省＞

・高機能暗号や計測セキュリティ、通信制御機器、複製不可能デバイスなどのハードウェアセキュリティ基盤を構築することで、多様なIoT機器からクラウドまでセキュアな環境を実現



＜総務省＞

・IoT機器などのハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発を実施。未知のハードウェアトロイを誤りなく検知することが目標



2．研究開発の推進：取組の例（２／２）

サイバー攻撃誘引基盤の構築（STARDUST）

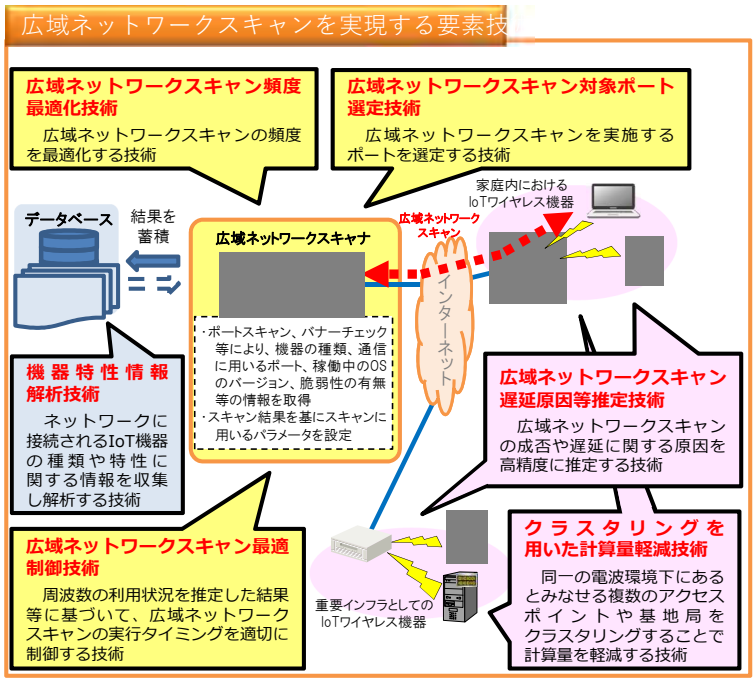
＜総務省＞

・高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能とする高度なサイバー攻撃誘引基盤を構築

広域ネットワークスキャンの軽量化を目指した研究

＜総務省＞

・正常な通信を阻害することなく、セキュリティ対策が必要な脆弱なIoT機器を特定することで、安全なICT基盤を実現



3．全員参加による協働：取組の例

・サイバーセキュリティに関する国民一人一人の理解を促すための集中期間として、「サイバーセキュリティ月間」のさらなる充実を図る。
・また、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、サイバーセキュリティの普及啓発に向けたアクションプランを策定する。

「サイバーセキュリティ月間」の主な活動

NISC主催の普及啓発イベントの開催

○キックオフサミット@六本木
・各地域で活躍する普及啓発団体の取組紹介や啓発活動に関する課題について議論
・イベントの模様をインターネット全国配信。10,000以上のアクセス数を達成


<キックオフサミット>

○アナログハックを目撃せよ！2018@秋葉原
・幅広く国民のサイバーセキュリティに関する意識向上を図るため、官民連携によるイベントを実施。当日は約2,000名が来場


<アナログハックを目撃せよ！2018>

○ NATIONAL 318(CYBER) EKIDEN
・各府省庁対抗による、競技形式のサイバー攻撃対処訓練を実施

官民等による月間関連行事の開催

○30年度は全国で官民による計189件の関連行事を実施（29年度は155件）

○各府省庁の協力を得て、①重要インフラ、②中小企業等、③国民全般の分野における取組を拡大

【主な取組例】
○「金融ISACワークショップ」（約250名）
○「医療・介護　総合EXPO・メディカルジャパン大阪　医療ITソリューション展セミナー講演」（約300名）
○ 「SIP次世代農林水産業創造技術　生産システムフォーラム」（約300名）

著名な作品とのタイアップ

・サイバーセキュリティと親和性の高いTVアニメ『BEATLESS』とタイアップ
・ポスター配布、ウェブバナーを関係機関のウェブページに掲載

「情報セキュリティハンドブック」の普及

・サイバーセキュリティに関する基本的知識を分かりやすく紹介
・無料電子書籍に加え、スマホ・タブレット端末用の無料アプリを配信

内閣サイバーセキュリティセンター（NISC）における情報発信の取組

NISCでは、サイバー攻撃の被害に遭う前に対策をとってもらえるよう、国民向けに、緊急時における注意・警戒情報を含めた情報発信を行っています。

注意・警戒情報発信

Twitter 「内閣サイバー（注意・警戒情報）」
プログラムの更新情報やマルウェアの注意喚起情報を発信
https://twitter.com/nisc_forecast

NISCの取組、サイバーセキュリティ関連情報発信

Twitter 「NISC内閣サイバーセキュリティセンター」
NISCの取組やサイバーセキュリティに関連する情報を発信
https://twitter.com/cas_nisc

Webサイト 「みんなでしっかりサイバーセキュリティ」
サイバーセキュリティに関する基礎知識の紹介、情報発信
http://www.nisc.go.jp/security-site/index.html
※NISCのHP（http://www.nisc.go.jp/）から移動可能

Facebook 「内閣サイバーセキュリティセンターNISC」
NISCの取組やサイバーセキュリティに関連する情報、読み物（１日１回）を発信
https://www.facebook.com/nisc.jp

LINE 「内閣サイバーセキュリティセンターNISC」
NISCの取組やサイバーセキュリティに関連する情報、読み物（１日１回）を発信
ID：@nisc-forecast

<LINEで発信しているイラスト付コラム>

推進体制のポイント

○ サイバーセキュリティの確保を通じて、情報通信技術及びデータの利活用を促進し、経済・社会活動の基盤とすること、我が国の安全保障を万全のものとすることは、従来からの方針。サイバーセキュリティ戦略本部の事務局であるNISCを中心に関係機関の一層の能力強化を図るとともに、各府省庁間の総合調整及び産学官民連携の促進の要となる主導的役割を担う。

○ 各府省庁の施策が着実かつ効果的に実施されるよう、必要な予算の確保と執行を図る。別紙の担当府省一覧を含む各年度の年次計画を作成する。