資料1-1

次期「サイバーセキュリティ戦略」骨子について

（研究開発関係）

令和3年6月

内閣サイバーセキュリティセンター（NISC）
基本戦略第１グループ

次期「サイバーセキュリティ戦略」に向けた検討

○現在、「今後3年間にとるべき諸施策の目標や実施方針」を示す次期「サイバーセキュリティ戦略」の検討が進められている。これまでに**本専門調査会でご議論をいただいた内容や要素を踏まえ**、5月13日に開催された「サイバーセキュリティ戦略本部」において、その**骨子が討議**されたところ。

○本骨子を踏まえ、**政府や関係主体の具体的な取組内容**を含め、本文の検討を進めているところ、本日、委員の皆様には、**骨子を踏まえ、今後に向けた意見交換**を行って頂くとともに、**各省庁における取組の具体的な方向性**に関するご示唆を頂きたい。

サイバーセキュリティ戦略

平成 30 年 7 月 27 日

次ページ以降

本戦略は、こうした今後のサイバーセキュリティに係る我が国としての基本的な立場や在り方を明らかにするとともに、今後３年間の諸施策の目標及び実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるものである。

「1. 策定の趣旨・背景」より抜粋

※骨子文書全体は【参考資料2】を参照。

横断的施策

5/13 第28回 サイバーセキュリティ戦略本部 資料1-1より

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　本専門調査会のスコープ

産学官エコシステム構築とともに、それを基礎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　※2021年度前半に「強化方針」を改定

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、見直しの検討。

経済社会の活力の向上及び持続的発展

5/13 第28回 サイバーセキュリティ戦略本部 資料1-1より

課題認識と方向性 － DX with Cybersecurity －

- 本年9月には「デジタル庁」の設置が予定。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あわせて、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 サプライチェーン等の信頼性確保に向けた基盤づくり

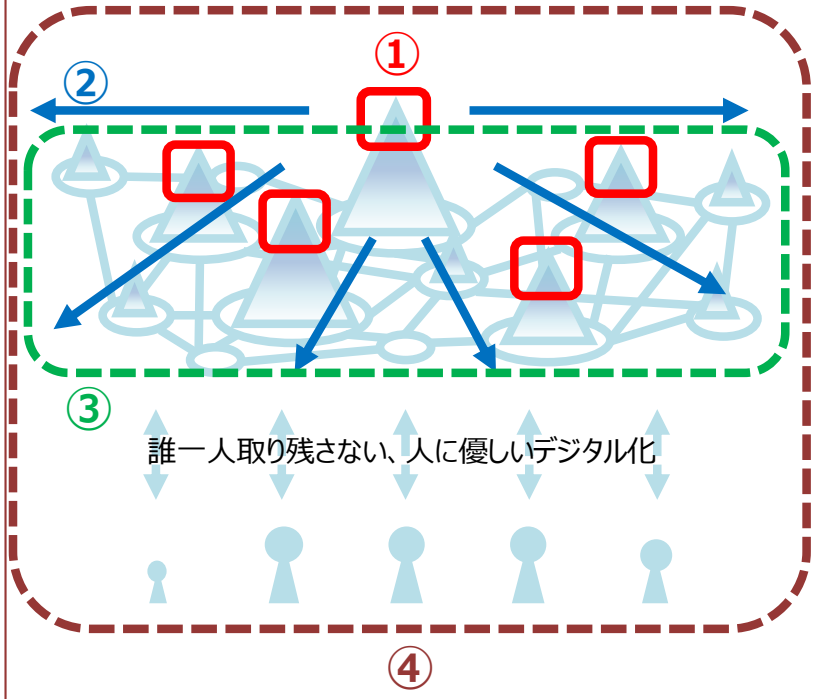
→Society5.0に対応したフレームワーク等も踏まえ、各種取組を推進。

- 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着、「トラストサービス」の普及
- 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

本専門調査会のスコープ

④ インクルーシブなデジタル／セキュリティ・リテラシーの定着

→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。



青字：各記載と紐付く主な取組

４．４　横断的施策

４．４．１　研究開発の推進

- 中長期的観点から研究開発の国際競争力の強化と産学官エコシステムの構築に取り組むとともに、それを基礎とした実践的な研究開発を推進しつつ、中長期的な技術トレンドを視野に入れた対応を行う。

（１）研究開発の国際競争力の強化と産学官エコシステムの構築　←「ｻｲﾊﾞｰｾｷｭﾘﾃｨ研究開発戦略（改訂）」の内容と対応

- サイバーセキュリティ研究分野は、世界的に論文投稿数が急成長するなど若く伸びており、国際共著・産学官連携論文などコラボレーションが活発で、デジタル技術の活用進展と相まって重要な研究分野となっている。
- 我が国でも研究者が増えている一方、経済社会のデジタル化により社会的要請が更に高まっており、我が国のデジタル化及びサイバーセキュリティ対策及び技術の充実・発展・自給に向けて、中長期的観点から研究及び産学官連携を振興し、研究開発の国際競争力の強化と産学官にわたるエコシステムの構築に取り組む。
- 関係府省における研究及び産学官連携振興施策の活用を促進するとともに、研究環境の充実等により、研究者が安心して研究に取り組める環境整備に努める。研究開発の成果の普及や社会実装を推進するとともに、その一環として政府機関における我が国発の新技術の活用に向けて関係府省による情報交換等を促進する。

＜NISC①＞　「研究開発戦略（改定）」を踏まえた取組推進、フォローアップ

＜総務省①＞　戦略的情報通信研究開発推進事業（SCOPE）

＜文部科学省①＞　AIP：人工知能/ビッグデータ/IoT/サイバーセキュリティ統合プロジェクト

４．４　横断的施策

４．４．１　研究開発の推進（続き）

（２）実践的な研究開発の推進　←「サイバーセキュリティ研究・技術開発取組方針」の内容と対応

- サプライチェーン・リスクの増大やサイバーセキュリティ自給など、安全保障の観点を含め我が国を取り巻く現下の課題認識に基づき、以下の方向性で、サイバーセキュリティに係る実践的な研究開発を推進。

①　サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備

＜NISC②＞　オールジャパンの技術検証体制の整備

＜経済産業省②＞　攻撃型手法を含むハイレベルな検証サービスの普及展開へ向けた実証

＜総務省②＞　5Gネットワークのセキュリティ確保に向けた体制整備

＜総務省③＞　チップの設計回路の解析などハードウェア検証技術に係る研究開発

＜内閣府①＞　戦略的イノベーション創造プログラム（SIP）第2期（IoT社会に対応したサイバー・フィジカル・セキュリティ）

②　国内産業の育成・発展に向けた支援策の推進

＜経済産業省②＞　セキュリティ製品の有効性検証、実環境における試行検証

＜経済産業省③＞　情報セキュリティサービス審査登録制度

③　攻撃把握・分析・共有基盤の強化

＜総務省④＞　広域ダークネット（NICTER）や攻撃種別に柔軟に対応するハニーポット技術等を用いたサイバー攻撃観測技術の高度化

サイバー攻撃誘引基盤（STARDUST）の高度化

サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）の構築

④　暗号等の研究の推進

＜総務省⑤・経済産業省＞ CRYPTREC 暗号リスト改定に向けた検討（※量子暗号に関する研究開発等は次項②に別記）

- 戦略期間において、関係府省の取組を推進するとともに、（１）を含め取組状況をフォローアップし、取組のマッピング等による点検と必要な再整理を行う。

＜NISC①＞　「研究開発戦略（改定）」を踏まえた取組推進、フォローアップ

４．４　横断的施策

４．４．１　研究開発の推進（続き）

（３）中長期的な技術トレンドを視野に入れた対応　← 昨年11/26専門調査会での議論と対応

- 「Beyond 5G」 をはじめとするネットワーク技術の高度化など、IT関連技術の進展に応じ、中長期的な視点から技術トレンドを捉え研究開発を推進していくことが重要であり、特に、AI技術・量子技術をはじめとする先端技術の進展を見据えた対応が求められる。

①　AI技術の進展を見据えた対応

・AIを活用したサイバーセキュリティ対策（AI for Security）の取組とAIを使ったサイバー攻撃に対処する観点

＜総務省③＞　ファジング技術等に基づく単体のハードウェアの動作特性の把握による不正機能検出

＜総務省⑤＞　AI 技術を活用した攻撃手法や攻撃傾向自動把握

・AIそのものを守るセキュリティ（Security for AI）の取組

＜内閣府等関係省庁＞　5～10年先に実現を目指す取組（研究課題）の検討

②　量子技術の進展を見据えた対応

・耐量子計算機暗号に関する検討

※（２）④に記載

・原理的に安全性が確保される量子通信・暗号に関する研究開発

＜総務省＞　量子暗号等を活用した量子情報通信ネットワーク技術の確立

＜総務省＞　量子暗号通信の超小型衛星への活用

４．１　経済社会の活力の向上及び持続的発展　～DX with Cybersecurityの推進～

４．１．３　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

（３）セキュリティ製品・サービス

- 自律的な取組が広がりを見せるためには、市場において提供されるセキュリティ製品・サービスが信頼の置けるものであることが前提。また、今後はサプライチェーン・リスクへの懸念もある中、自社製品等の信頼性に対する、第三者による客観的な検証への需要が拡大し、産業として重要になっていくと考えられる。
- こうした観点から、セキュリティ製品・サービスの有効性検証を行う基盤整備や、一定の基準を満たすセキュリティサービスを審査・登録する取組等を通じ、信頼性確保の基盤づくりや日本発の製品・サービスの育成、海外市場への展開支援に取り組む。また、検証事業者の信頼性の可視化手法の検討に取り組む。

＜経済産業省②＞　Proven in Japanの取組

＜経済産業省③＞　情報セキュリティサービス審査登録制度

＜総務省⑥＞　海外展示会等への出展支援

＜総務省⑦＞　国際標準化に向けた取組

（４）先端技術・イノベーションの社会実装

- デジタル化進展の中で、エビデンスが明確で組織内外への説明性の高い、又は自動化等を活用し効率的なセキュリティ対策が一層求められる。こうした社会的要請に応える形で、産学連携が活発に行われるような産学官にわたるエコシステムの構築を推進し、オープンイノベーション活動を活性化していくことが必要。
- また、我が国におけるセキュリティ製品は海外に大きく依存している状態であり、製品・サービスの開発に必要なノウハウや知見の蓄積が困難となっている。こうした状況を打破する一環として、サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築し産学の結節点として開放していく。
- 加えて、IoTシステム・サービス、サプライチェーン全体での活用に向けた基盤の開発・実証の取組について、様々な産業分野を念頭に置いた社会実装を促進する。
- これら新技術の社会実装に向けた取組の一環として、政府機関における新技術の活用に向けた技術検討を促進する。

＜総務省⑤＞　サイバーセキュリティ統合知的・人材育成基盤CYNEX

＜内閣府①＞　戦略的イノベーション創造プログラム（SIP）第2期（IoT社会に対応したサイバー・フィジカル・セキュリティ）

＜内閣官房 IT室①＞　資産管理等強化に向けた技術検討（※戦略全体としては別項に紐付く取組）