資料3-1

次期「サイバーセキュリティ戦略」骨子について

（普及啓発・人材育成関係）

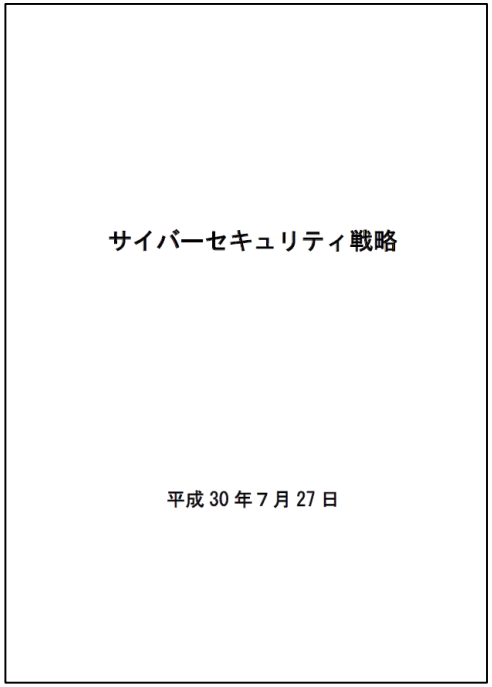
令和3年6月

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、本文の検討に入るところ、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。



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5】を参照。

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。

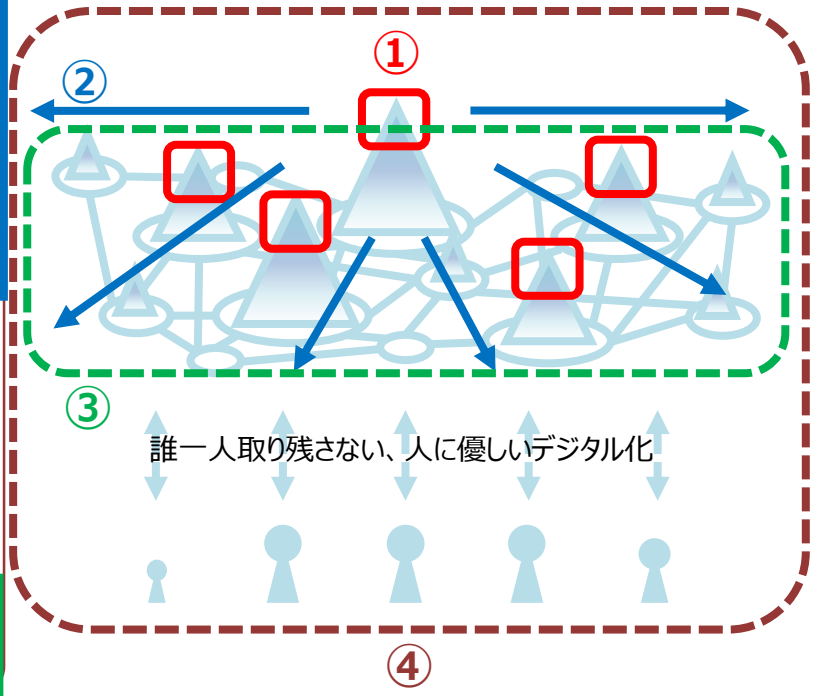
③ サプライチェーン等の信頼性確保に向けた基盤づくり

→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義、「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

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。



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

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。

人材の確保、育成、活躍促進

４．４　横断的施策

４．４．２　人材の確保、育成、活躍促進

- 人材の不足感に関する現状認識やデジタル化に向けた取組の広がりを踏まえれば、「質」・「量」両面での官民の取組を、一層継続・深化させていくことが必要。
- また、サイバーセキュリティに係る人材が、男女を問わず多様な視点や優れた発想で幅広く活躍できる環境をつくり、次代を担う優秀な人材を引きつけられる好循環を生むことが重要。
- このため、環境変化に対応して以下の政策目的に適った取組の重点化を図るとともに、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整備に取り組む。

（１）”DX with Cybersecurity”の推進

- 企業・組織内でのデジタル化推進に伴う人材の需要と人材の供給が車の両輪として好循環を生み出すことが重要。
- また、そのためには、経営者及びDX推進者において、デジタル化とサイバーセキュリティ対策は他人事ではなく、同時達成されるべき、業務と収益の中核を支える基本的事項として認識されることが前提となるところ、意識改革に取り組みつつ、以下の取組を推進。

①　「プラス・セキュリティ」知識の補充　　← **政策課題２の議論を反映**

- 経営層やマネジメントに関わる人材層をはじめとして、ITやセキュリティに関する専門知識や業務経験を必ずしも有していない様々な人材に対して「プラス・セキュリティ」知識が補充され、内外のセキュリティ専門人材との協働等が円滑に行われることが、社会全体で”DX with Cybersecurity”を推進していく上で非常に重要。同時に、経営層の方針を踏まえた対策を立案し実務者・技術者を指導できる人材の確保に向けた取組も重要であり、これらの取組により「戦略マネジメント層」の充実を図る。
- こうした取組の一環として研修・セミナー等の人材育成プログラムを社会的に広く普及させていくため、国や関係機関・団体で需要を喚起する普及啓発を行うことに加え、国による先導的・基盤的なプログラム提供だけでなく、需要者からみて一定の質が確保・期待される仕組みを通じて、人材育成プログラムに係る需要と供給を相応させ市場の形成・発展を目指していくほか、地域におけるコミュニティ形成を通じた「共助」の取組や、人材育成基盤・環境の民間提供等を重点的に進めていく。

＜NISC①＞　経営層やマネジメントに関わる人材層向けのモデルカリキュラムの構築・提供
普及に向けた「普及啓発・人材育成ポータルサイト」等の活用

＜経済産業省⑧＞　戦略マネジメント層向けセミナー等での対応

４．４．２　人材の確保、育成、活躍促進（続き）

②　IT・セキュリティ人材が活躍できる環境の構築　　← 政策課題１・３の議論を反映

- 今後、DXに伴い、業務等のデジタル化、製品等のネットワーク接続、デジタルサービスの開発や他との連携などが増加する中で、新たな開発・監視・対処のプラクティスが必要となり、セキュリティ・バイ・デザインの重要性も増すと考えられる。したがって、これらの動向や人材の偏在等を考慮しつつ、企業・組織内での機能構築やIT・セキュリティ人材の確保・育成に関するプラクティス実践の促進を行っていく。
- また、人材の活躍の場という観点では、兼業・副業といった雇用形態の活用や行政でのデジタル改革業務の機会が今後増していくと考えられる。社会全体で”DX with Cybersecurity”を推進していくためには、業務や製品・サービス等のデジタル化に応じた企業・組織内での適切な開発・監視・対処機能構築のプラクティス実践が図られるとともに、働き方や雇用形態の多様化、デジタル改革の推進を機会としてIT・セキュリティ人材の流動性・マッチング機会の促進が図られる環境整備が必要。このため、新たな時代に応じたプラクティス実践の事例を、先進事例として積極的に共有するとともに、実践に当たって参考となるノウハウやネットワークを提供することを通じ、展開を図る。

＜NISC②＞　サイバー攻撃被害事例等を通じた先進的なプラクティス収集・発信（ポータルサイト活用）

＜経済産業省⑩＞　SC3（サプライチェーン・サイバーセキュリティ・コンソーシアム）の枠組みの下でのサイバー攻撃動向を踏まえた対策検討・プラクティス共有

＜経済産業省⑥＞　「人材確保・体制構築の手引き」の開発・活用促進

＜総務省②・経産省⑤＞「地域SECUNITY」を通じた人材育成・マッチング

＜経済産業省⑨＞　高専連携を通じた人材育成・マッチング

＜総務省③＞　地域における人材エコシステムの構築

＜厚生労働省①＞　教育訓練給付制度を通じた学び直しの機会の提供

（２）巧妙化・複雑化する脅威への対処

- 巧妙化・複雑化したサイバー攻撃の増大、サプライチェーンの複雑化・グローバル化に伴うリスクの増大、制御系システムを対象とする攻撃等もみられる中で実践的な対処能力を持つ人材育成の重要性は一層増している。
- このため、これらの脅威動向に対応し、実践的な対処能力を持つ人材育成プログラムを強化しコンテンツの開発・改善を行うとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学に開放する。
- また、こうした人材の活躍促進の観点から、プログラムに参加した修了生同士のコミュニティ形成や交流の促進、資格制度活用に向けた取組、自衛隊・警察も含む公的機関における専門人材確保の推進もあわせて重要である。

人材育成プログラムの強化（脅威動向に対応したコンテンツの開発・改善）、コミュニティ形成
＜総務省⑤・⑥＞　SecHack365、CYDER
＜経済産業省⑦＞　ICSCoE中核人材育成プログラム
＜文部科学省①＞　en-PiT

＜総務省⑦＞　CYDERのオープンプラットフォーム化（CYNEX）

（３）政府機関における取組

- IT・セキュリティ人材の活躍促進の観点からも、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が重要。この方針を踏まえ、外部の高度専門人材を活用する仕組みの強化や、素養を有する人材がより確保しやすくなる仕組みの早期導入、研修の充実・強化等に向けた方策を新たに示し、取組を推進。
- また、各府省庁の人材確保・育成計画に基づき、「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、定員の増加による体制整備、研修や演習の実施、適切な処遇の確保についても着実に取り組むとともに、毎年度計画の見直しを行い、一層の取組の強化を図る。

＜NISC③＞　政府機関における「IT・セキュリティ人材の確保・育成強化方針」の改定
【総合職試験デジタル区分の創設、人材が民間、自治体、政府を行き来可能な環境整備、研修の充実・強化等】

- 特に、高度なサイバー犯罪や安全保障への対応等を行うため、外部の高度専門人材を活用するだけでなく、政府内部においても独自に高度専門人材を育成・確保する。

＜警察庁①・防衛省①＞　専門人材の育成・確保に向けた取組

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～

経営／
地域・中小

- デジタル改革のビジョンである「デジタルの活用により、一人ひとりのニーズにあったサービスを選ぶことができ、多様な幸せが実現できる社会」の実現に向けて、我が国経済社会は、変革を伴うデジタル・トランスフォーメーションを遂げることが必要。
- そして、その機会と影響が、あらゆる主体に例外なく及ぶ中で、「DX with Cybersecurity」があらゆる主体において意識され、取組があらゆる面で推進されなければならない。
- 経営層の意識改革をはじめ、経済社会全体で意識やリテラシーを高める取組とともに、各主体の自律的取組を推進する観点から、地域・中小企業におけるDX with Cybersecurityの促進や、バリューチェーンの信頼性確保に向けた基盤づくりに取り組む。

４．１．１　経営層の意識改革

- 新型コロナウイルスの影響を経てデジタル化は加速し、今後、企業の競争力としてより付加価値の高いデジタルサービスを生み出す基盤を有しているかが重要に。
- 経営層にとって、デジタル化とサイバーセキュリティ対策は、他人事ではなく、同時達成されるべき業務と収益の中核を支える基本的事項として、両者を理解することが経営の基本的な素養・知識となると想定。サイバーリスクの存在はデジタル化に取り組まない言い訳たり得なくなる。
- デジタル化と一体となったサイバーセキュリティ強化に向けた取組状況が、デジタル経営に向けた行動指針の実践やツールの活用を通じ、サステナビリティを重視する投資家等のステークホルダーに可視化され、かつそうした取組に対しインセンティブが付されることなどにより、経営層によるリスク把握や企業情報開示といったプラクティスの普及促進に取り組む。

＜経済産業省①＞　「デジタルガバナンス・コード」「サイバーセキュリティ経営ガイドライン」の更なる活用の促進
【「可視化ツール」の情報開示への活用の促進、DX企業認定制度・DX銘柄等選定との連動】

＜総務省①＞　「情報開示の手引き」の活用促進

- また、こうした取組を通して、デジタル化とあわせてサイバーセキュリティ対策に取り組む経営層が、自社の競争力の源泉たるデジタルサービスに内在するリスクの所在を把握できるよう、「プラス・セキュリティ」知識を補充できる環境整備を推進する。

p.4の取組に同じ

４．１．２　地域・中小企業におけるDX with Cybersecurityの推進

経営／
地域・中小

- コロナ禍への対応を余儀なくされること等を通じ、ビジネスモデルの変革や働き方・雇用形態のあり方にも変化が及ぶ中で、デジタル化の機会は、地域・中小企業、そしてサイバー空間とは繋がりのなかった業種・業態の企業にも例外なく広がる。
- 一方で、中小企業がデジタル化と同時にサイバーセキュリティ対策に取り組むに当たっては、セキュリティ専任の人材を配置できないなど、リソース（知見・人材）不足に直面。
- 「共助」の考え方に基づくコミュニティ活動を全国に展開し、専門家への相談に留まらず、ビジネスマッチングや人材育成・マッチングなど、リソース不足を踏まえた地域による課題解決・付加価値創出の場の形成を促進する。

＜総務省②・経産省⑤＞　「地域SECUNITY」の推進・発展（ビジネスマッチング、人材育成・マッチング支援等）

- また、中小企業が利用しやすい安価かつ効果的なセキュリティサービス・簡易保険を普及させるため、中小企業を含むサプライチェーン全体のサイバーセキュリティ強化を目的として設立された産業界主導のコンソーシアムとも連携しつつ、一定の基準を満たすサービスの審査・登録制度の運営等の取組を推進。

＜経済産業省④＞　「お助け隊サービス審査登録制度」の活用促進

＜経済産業省②＞　中小企業自らの自己宣言を促す「SECURITY ACTION」の活用促進

- 加えて、今後は、中小企業に広くクラウドサービスの利用が普及することも一つの重要な選択肢となると想定。その利用に当たっては、情報資産が企業外に置かれることに加え、設定等の不備により意図せず流出するリスクも一定程度伴うことから、クラウドサービス利用者が留意すべき事項に関する周知に取り組むとともに、クラウドサービス利用時の設定ミスの防止・軽減のため、クラウドサービス事業者に必要な取組を促すこと等を検討する。

＜経済産業省②＞　「クラウドサービス安全利用の手引き」をはじめとする中小企業向け周知啓発

＜総務省④＞　クラウドサービス事業者による利用者サポートの取組促進

普及啓発等

４．１．４　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

- サイバー空間の基盤は人々のくらしにとっての基礎的なインフラとなりつつある中、「誰一人取り残さない、人に優しいデジタル化」 を進める中で、その恩恵を、インクルーシブに享受していくためには、国民一人ひとりが自らの判断で脅威から身を守れるよう、サイバーセキュリティに関する素養・基本的な知識（リテラシー）を身に付けていくことが必須。
- 一方で、リテラシーは一朝一夕に身に付くものではない。行政のデジタル化、マイナンバーの普及やGIGAスクールの推進等が進み、様々なデジタルサービスに触れる機会が増えていく中、「まずは自分でやってみる」意識を持ち、能動的に体験を積んでいくことが何よりも重要。この際、情報教育が推進される中で、各種取組が進められるべきである。
- 国としても、こうした機会を捉え、デジタル活用支援と連動をしながら、官民で連携して国民への普及啓発活動を実施していく。「GIGAスクール構想」の推進に当たっては、学校における環境整備の支援を行う「ICT支援員」等の配置や教職課程におけるICT活用指導力の充実を図るほか、情報モラルに関する教育を推進する。

＜文科省②＞　GIGAスクール構想における「ICT支援員」の活用、ICT活用指導力の充実、情報モラル教育の推進

- また、インターネット上の偽情報の流布については、個人の意思決定や社会の合意形成に不適切な影響が与えるおそれがあることから、民間の自主的取組の慫慂を含め、幅広く周知啓発を行う。

４．４．３　全員参加による協働、普及啓発

- サイバー空間と実空間の一体化の進展、サイバー攻撃の巧妙化・複雑化の中で、実空間における防犯対策や交通安全対策と同様に、国民一人ひとりがサイバーセキュリティに対する意識・理解を醸成し、様々なリスクに対処できることが不可欠。素養・基本的な知識（リテラシー）を身に付けると同時に、自らの判断で脅威から身を守れるよう、行動強化につながる普及啓発・情報発信が重要。また、様々な関係者がお互いの役割分担の下で連携・協働することが何より重要。
- こうした認識の下で、普及啓発に向け産学官民の関係者が円滑かつ効果的に活動できるよう具体的なアクションプランを策定し、地域・中小・若年層を重点対象として取組を推進。今後、デジタル改革推進により、サイバー空間に参加する層が広がる中で、当該アクションプランプランを推進しつつ継続的な改善に取り組むとともに、状況を踏まえた見直しを検討する。
- 加えて、特に、テレワークの増加やクラウドサービスの普及等に伴い、情報発信・普及啓発のあり方（コンテンツ）についても必要な対応を実施。

＜NISC④・⑤＞　「意識・行動強化プログラム」の推進・継続的改善、サイバーセキュリティ月間やSNS等を通じた情報発信

＜警察庁②＞　　地域社会における安全教育・普及啓発活動

＜総務省⑧・⑨＞ テレワークや無線LANの利用に係るセキュリティガイドラインの活用促進