資料２

人材の確保、育成、活躍促進に向けた
今後の検討の方向性について（全体像）

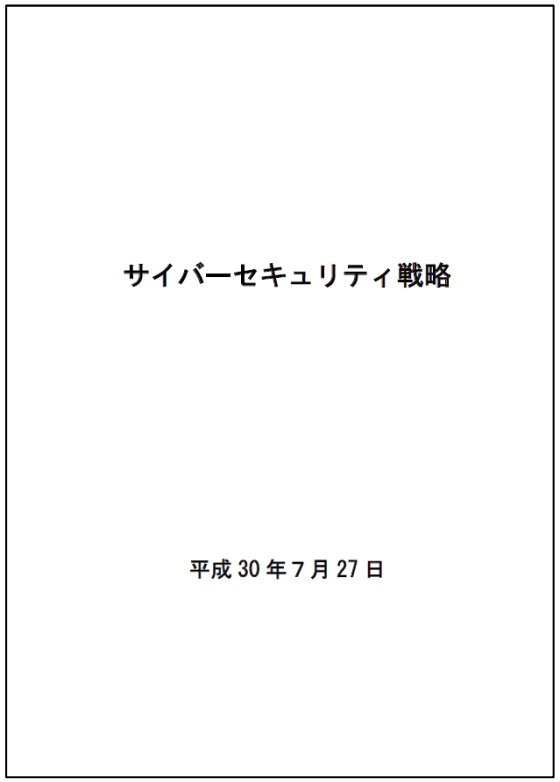
令和3年1月

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

新しい「サイバーセキュリティ戦略」に向けた検討

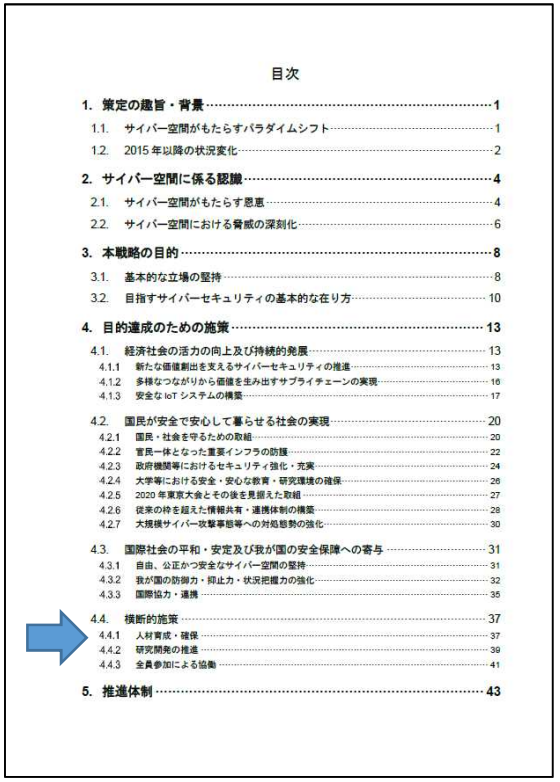
○現行の「サイバーセキュリティ戦略」の閣議決定から2年余りが経過。「3年間の諸施策の目標及び実施方針」を示す文書であるところ、新しい「戦略」に向けた検討を開始するタイミング。

○本日は、「人材の確保、育成、活躍促進に向けた今後の検討の方向性」の全体像について、現状認識を中心に、ご議論をいただきたい。



サイバーセキュリティ戦略

平成 30 年 7 月 27 日



目次

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

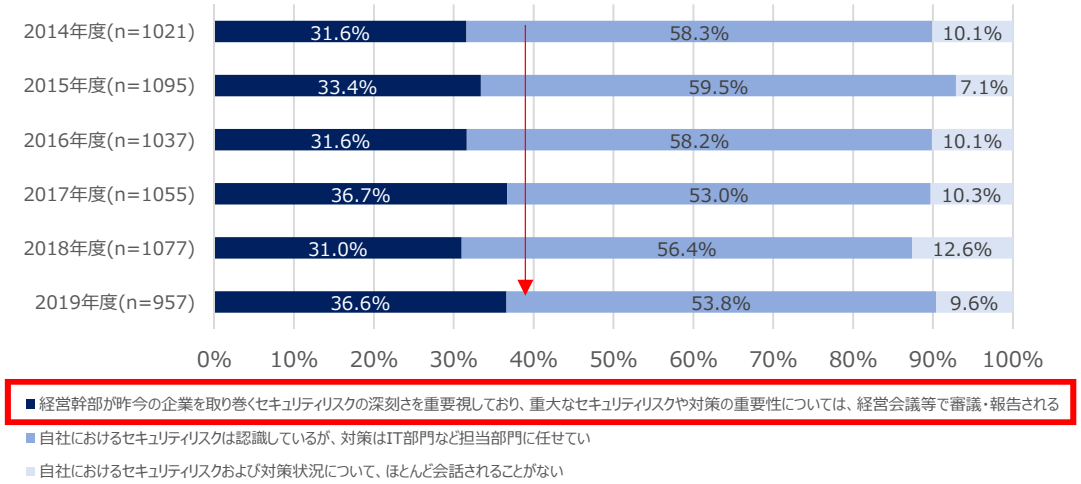
※ 本文関係個所の抜粋は【参考資料3】を参照。

経営層の関与

現状認識

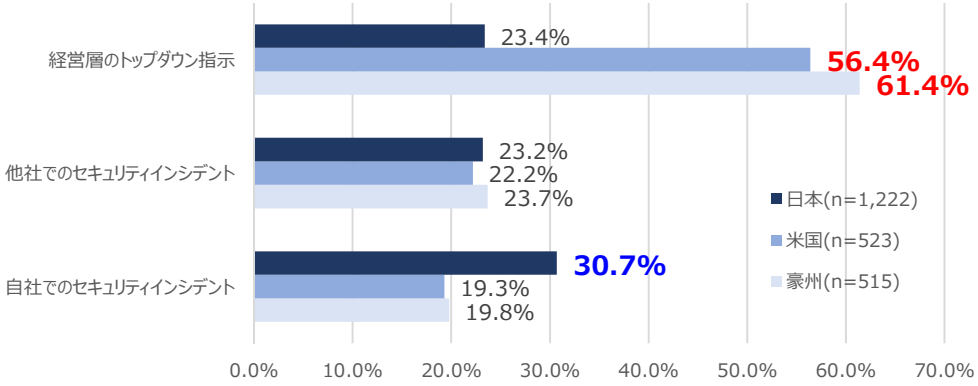
○セキュリティ対策に関し、経営層の関与は大きく進展しておらず、他国と比べてもその水準は低い。

◆セキュリティへの経営層の関与度合い



（データ出所）（一社）日本情報システムユーザー協会「企業IT動向調査報告書」よりNISC作成

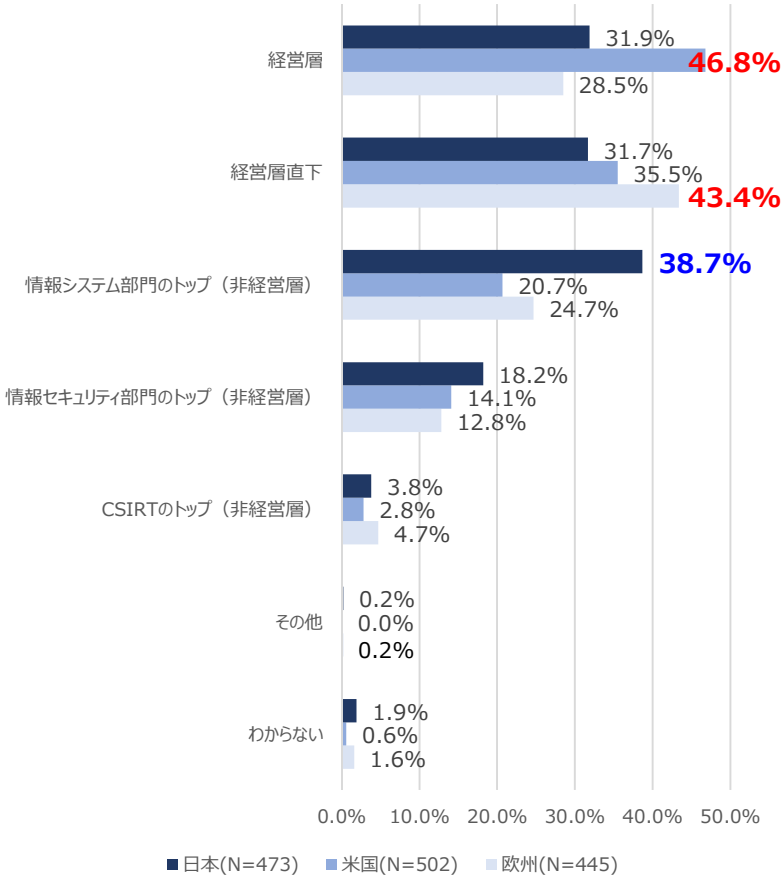
◆情報セキュリティ対策実施のきっかけや理由



（データ出所） NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」2020年12月よりNISC作成

※複数回答あり。

◆CISO等の組織内の位置づけ



（データ出所） IPA「企業のCISOやCSIRTに関する実態調査2017」2017年4月

※複数回答あり。

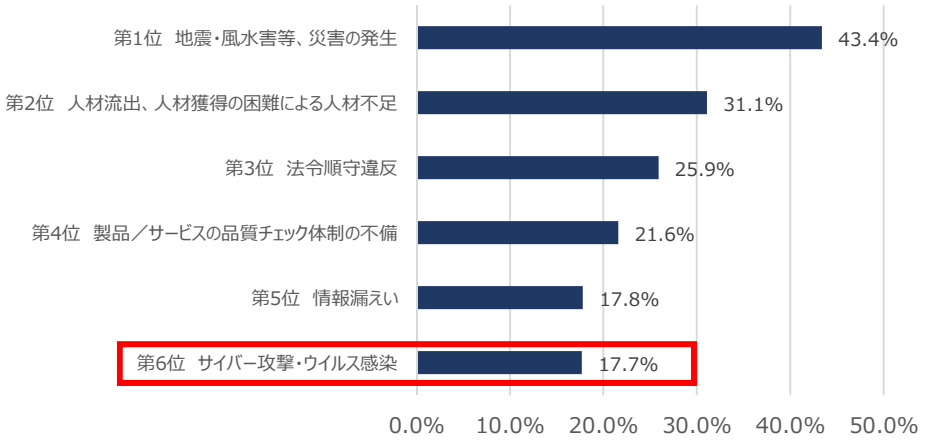
経営上のリスクとしての認識

現状認識

〇多くの企業では主要な経営リスクとみなされておらず、情報開示も他国と比べて進んでいない。

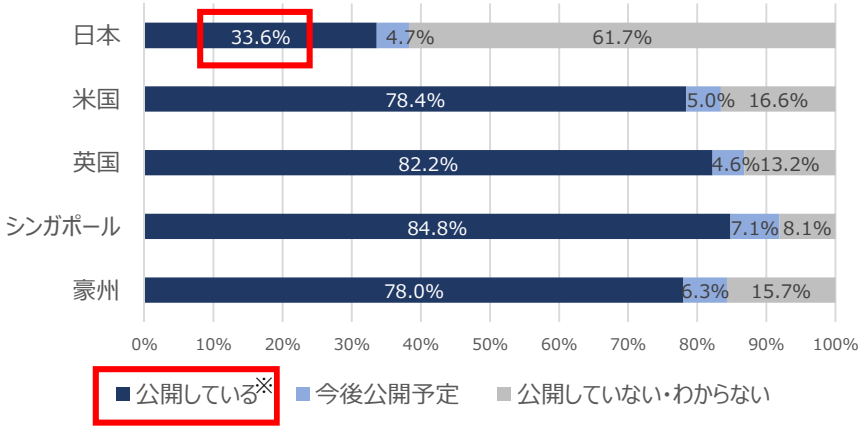
◆優先して着手が必要と思われるリスク（日本）

※下記の順位は昨年度同調査から不変



（データ出所）デロイトトーマツグループニュースリリース（2020年2月19日）よりNISC作成

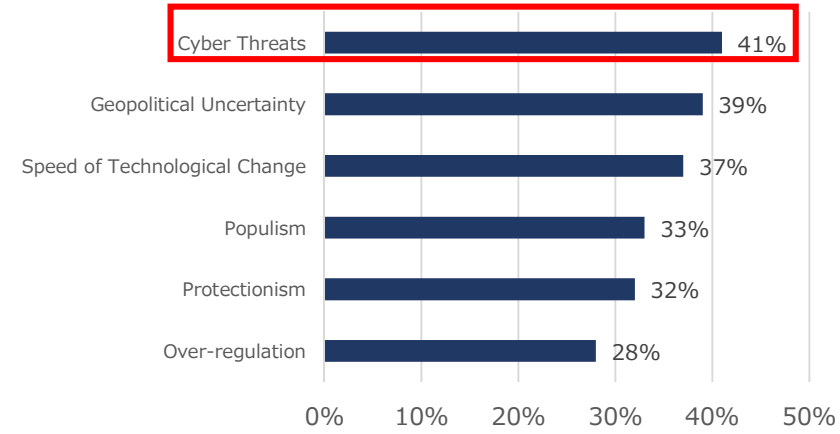
◆セキュリティ対策の情報開示状況



（データ出所）　NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」2018年7月

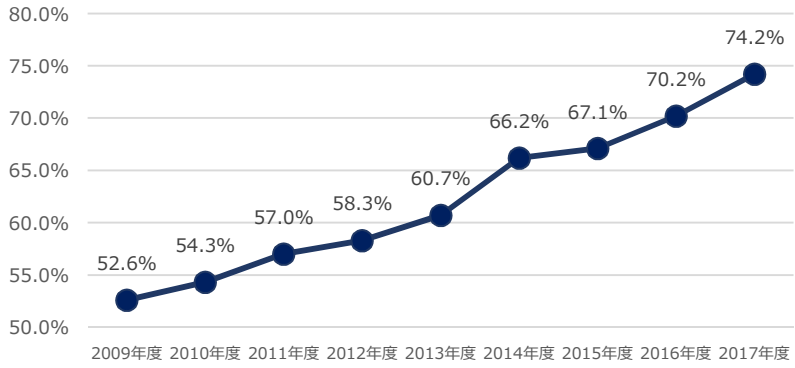
※「企業のWebサイトの情報セキュリティに特化したページ（情報セキュリティ報告書等）で公開している」/「企業のWebサイトの情報セキュリティ以外のページ（CSR、年次報告書等）で公開している」/「業界団体やISAC等のコミュニティ内で公開・共有している」/「講演会やセミナー等で公開している」

cf. 投資家からみたリスク順位（グローバル）



（データ出所）　PwC "2018 Global Investor Survey"よりNISC作成

cf. サイバーセキュリティに関して有価証券報告書に記載をしている企業の割合（日経平均採用銘柄225社）



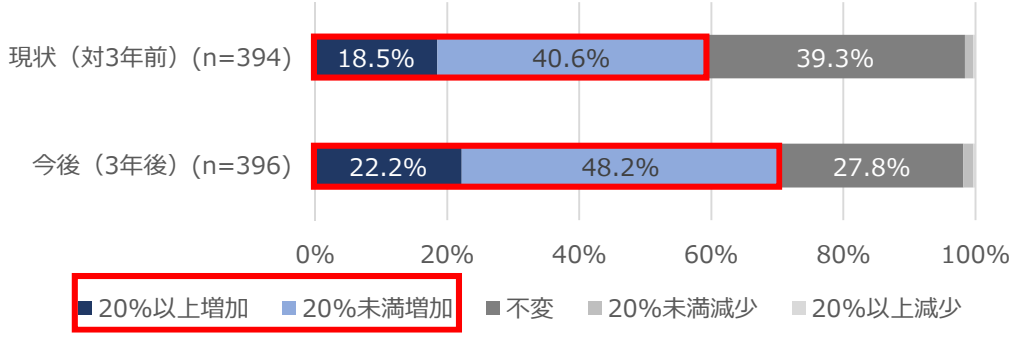
（データ出所）　NISC「平成30年度企業のサイバーセキュリティ対策に関する調査」

DX投資の進展とセキュリティ上の対応

現状認識

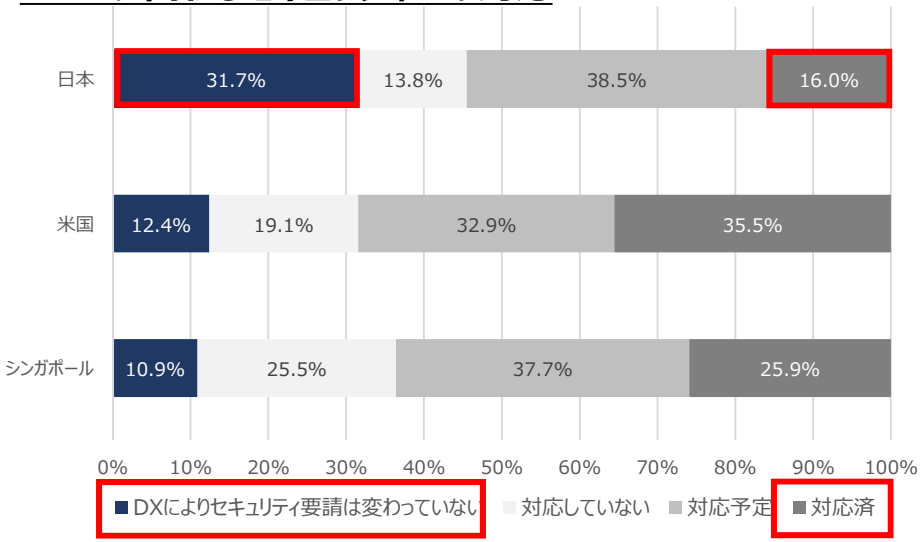
○今後DX投資は増加する見込みである一方、それに対応したセキュリティ対応や開発体制の構築が行われないおそれがある。

◆商品・サービスのデジタル化の予算の増減傾向



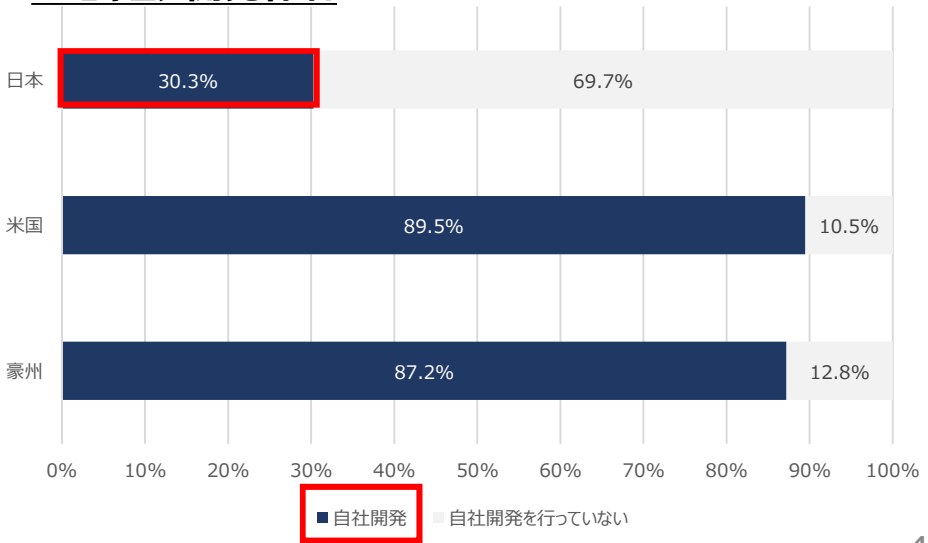
（データ出所）　（一社）日本情報システムユーザー協会
「企業IT動向調査報告書2020」2020年4月

◆DXに関わるセキュリティへの対応



（データ出所）　NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」2019年7月よりNISC作成

◆セキュア開発体制



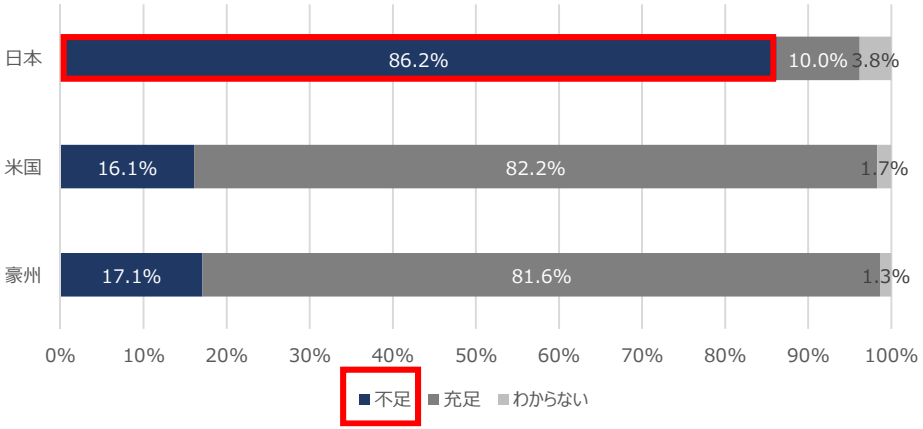
（データ出所）　NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」2020年12月

人材の不足感

現状認識

○他国と比較しても人材の不足感は大きい。セキュリティ対策にあたる実務者層・技術者層の育成は一定の取組の進展がみられるが、例えばユーザー企業では不足傾向が拡大していると考えられる。

◆セキュリティ対策に従事する人材の過不足感



（データ出所） NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」2020年12月

◆不足している人材の種別

	２０１８年	２０１９年	２０２０年
１位	ログを監視・分析して、危険な兆候をいち早く察知できる 57.0%	セキュリティ戦略・企画を策定する人 47.2%	セキュリティ戦略・企画を策定する人
２位	セキュリティ戦略・企画を策定する 52.7%	セキュリティリスクを評価・監査する人 34.1%	セキュリティリスクを評価・監査する人
３位	セキュリティインシデントへの対応・指揮ができる 44.1%	ログを監視・分析する人 34.1%	ログを監視・分析する人

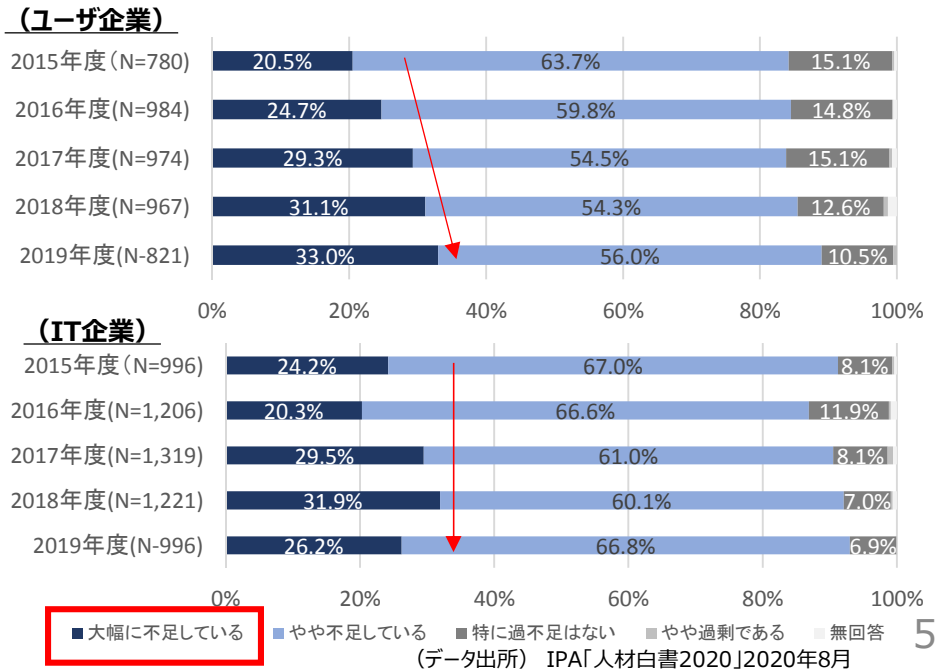
セキュリティ対策にあたる実務者層・技術者層　　戦略・企画を担当する人材

（データ出所） NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」よりNISC作成

◆実務者層・技術者層の育成に向けた取組（例）

- SecHack365　：2017年度以降、累計130名（修了生数・2019年度末時点）
- CYDER（実践的サイバー防御演習）：2017年度以降、累計10,974名（2020年末時点）
- ICSCoE中核人材育成プログラム：
  2017年以降　累計228名（修了生数・2019年度末時点）
- セキュリティキャンプ　：2004年以降、累計921名（2020年末時点）
- 情報処理安全確保支援士制度：
  2016年度以降、累計19,752名（登録者数・2020年10月時点）

◆IT人材の量に関する過不足感



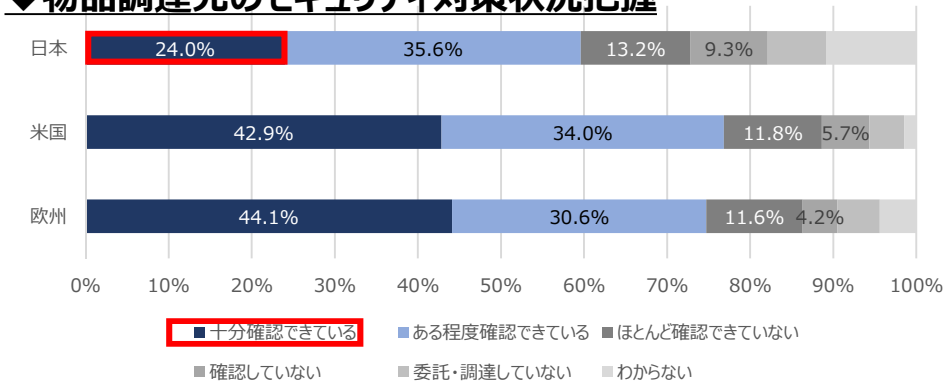
（データ出所） IPA「人材白書2020」2020年8月

サプライチェーンリスクへの対応、中小企業

現状認識

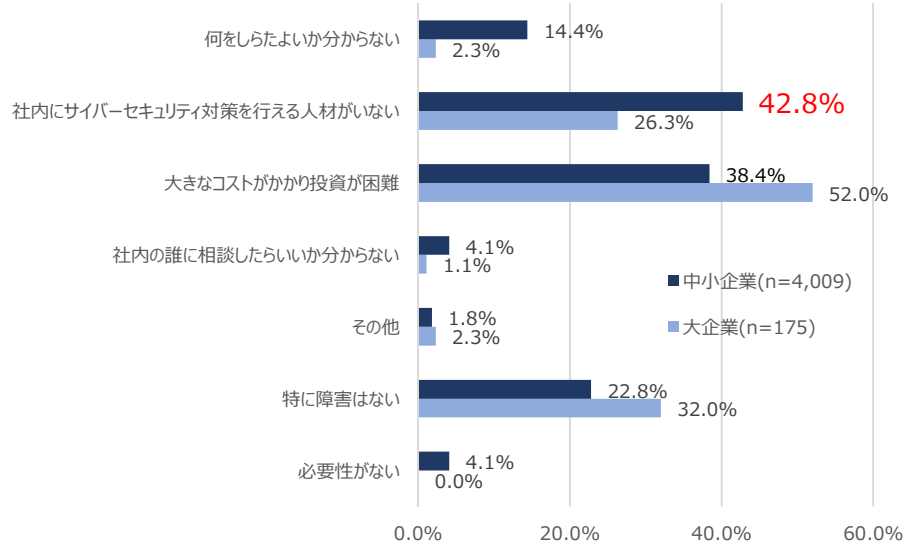
○サプライチェーンリスクへの対応は進んでおらず、また中小企業も人材課題等が制約となり大企業以上にセキュリティ対策が進んでいない。

◆物品調達先のセキュリティ対策状況把握



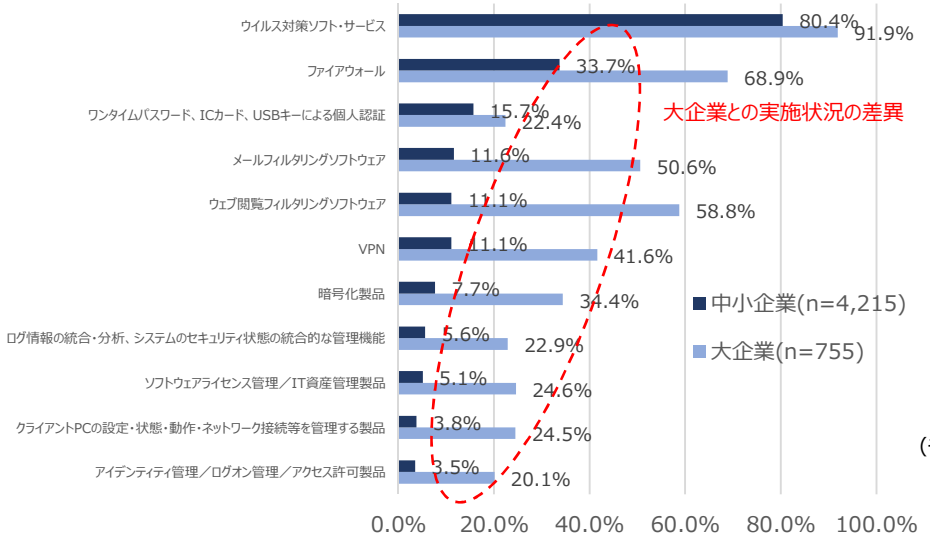
（データ出所） IPA「企業のCISOやCSIRTに関する実態調査2017」2017年4月

◆セキュリティ対策を実施する際の障害



（データ出所） 経済産業省「2018年度版ものづくり白書」

◆中小企業のセキュリティ対策実施状況



（データ出所） IPA「企業のCISOやCSIRTに関する実態調査」2017年4月
IPA「中小企業における情報セキュリティ対策に関する実態調査」2017年7月
より経済産業省作成（NISCにてレイアウトを一部変更）

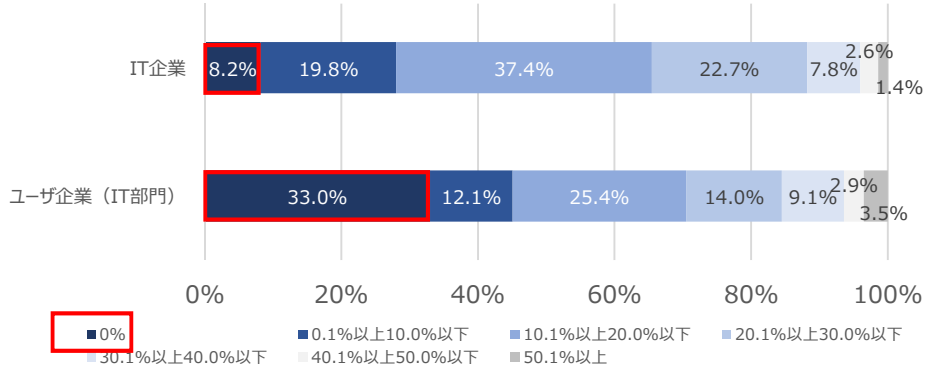
ダイバーシティ

現状認識

○セキュリティ分野に限った統計は見られないが、IT人材全体では、女性割合が徐々に増加しているものの、高い水準にあるとは言えない。

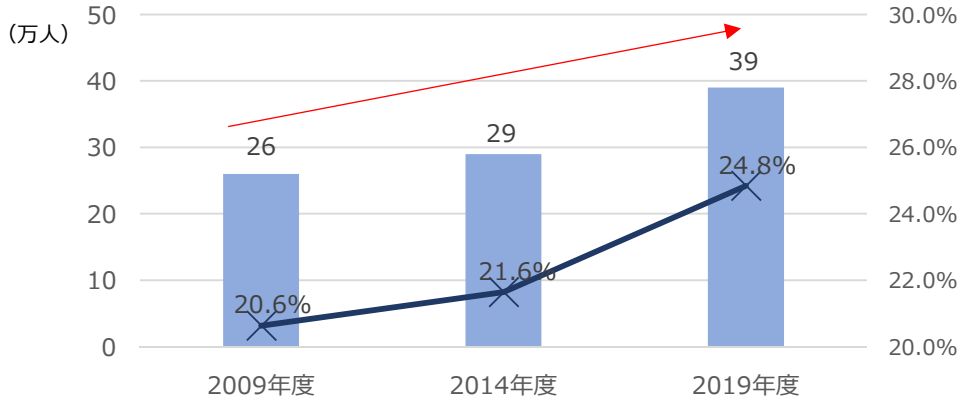
○また、他国においては、サイバーセキュリティ分野において幅広い人材確保の観点から、ジェンダーバランスに言及されている例もある。

◆IT人材に占める女性の割合



（データ出所） IPA「人材白書2020」2020年8月 よりNISC作成

◆情報サービス業の労働人口に占める女性人口とその割合



（データ出所） IPA「人材白書2020」2020年8月（総務省「労働力調査」より作成）よりNISC作成

◆他国の政策文書における言及例（英国）

7.1.6. We will develop and implement a self-standing skills strategy that builds on existing work to integrate cyber security into the education system. This will continue to improve the state of computer science teaching overall and embed cyber security into the curriculum. Everyone studying computer science, technology or digital skills will learn the fundamentals of cyber security and will be able to bring those skills into the workforce. As part of this effort, we will address the gender imbalance in cyber-focused professions, and reach people from more diverse backgrounds, to make sure we are drawing from the widest available talent pool. We will work closely with the Devolved Administrations to encourage a consistent approach across the UK.

（出典）National Cyber Security Strategy 2016 to 2021 (NCSC, 2016)

（参考）基本的な時代認識

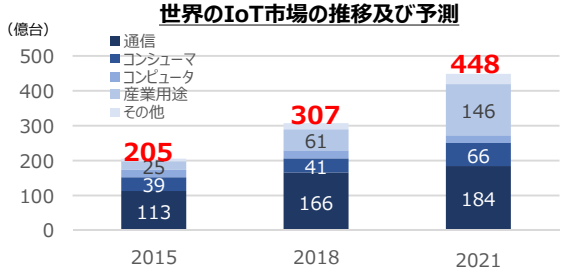
現状認識

◆ 経済社会の環境変化　～デジタル経済の浸透、デジタル改革の推進～

- インターネットの登場により**「サイバー空間」という新たな空間が創出**され、**平成の時代**を通じ**デジタル経済が大きく進展**。
  「**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**」をビジョンに掲げる目指す**デジタル改革を推進**。
- **デジタル経済の影響**は、**人々の生活そのものに波及**。IoTやAI、5G、クラウドサービス等の利用拡大、テレワークの定着、遠隔教育等の実施など人々の行動が変容。
  その先にはサイバー空間と実空間が高度に融合したSociety5.0の実現が期待。

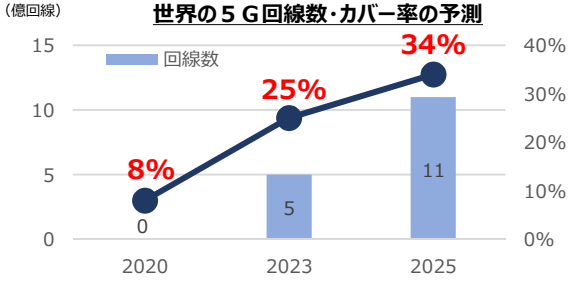
AI,IoT等の活用している企業の割合（資本金100億円以上）　**25%**(2019年度) → **34%**(2020年度)
（データ出所）DBJ「全国設備投資計画調査（大企業）」

世界のIoT市場の推移及び予測



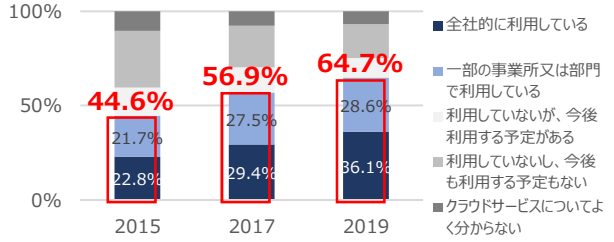
（データ出所）HIS TechnologyよりNISC作成

世界の５Ｇ回線数・カバー率の予測



（データ出所）GSMAよりNISC作成

我が国におけるクラウドサービスの利用状況



（データ出所）総務省「情報通信白書」よりNISC作成

◆ SDGｓへの貢献への期待

- Society5.0の実現により、諸課題が解決された豊かな社会を迎えることができ、国連が掲げる**SDGsにも貢献することが期待**。

◆ 安全保障環境の変化、地政学的課題

- **サイバー空間に対する基本的価値・ガバナンスの在り方に対する国家間対立の激化**。

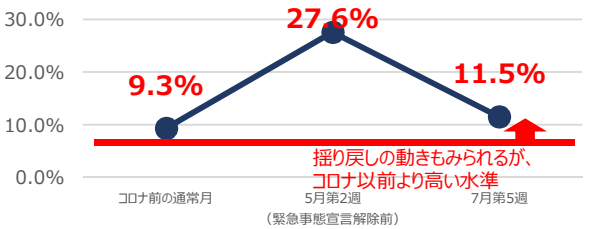
◆ オリンピック・パラリンピックのレガシー

- 2021年に開催される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の**レガシーを活用**。

◆ 新型コロナウイルスの影響・経験

- 新型コロナウイルスの感染拡大に伴い、**テレワークの利用、ICT教育やオンライン診療に係る動きが加速**。パーソナルデータを活用したサービスも活用も進展。

週1日以上在宅勤務の割合



（データ出所）JILPT周燕飛氏資料よりNISC作成

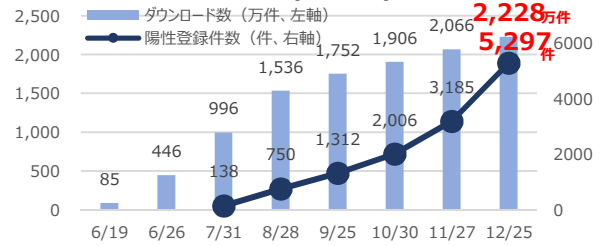
GIGAスクール構想

○2020年度補正予算で約2,000億円を措置し、学校における環境整備の支援を行うGIGAスクールサポーターの配置や、2023年度に達成するとされている端末整備の前倒しを支援。
※小5・6、中1に加え、残りの中2・3、小1～4すべてを措置。

オンライン診療

○2020年4月に、厚生労働省より、「初診から電話や情報通信機器を用いた診療により診断や処方をして差し支えない」とする事務連絡を発出。

新型コロナに係る接触確認アプリ(COCOA)のダウンロード数等推移



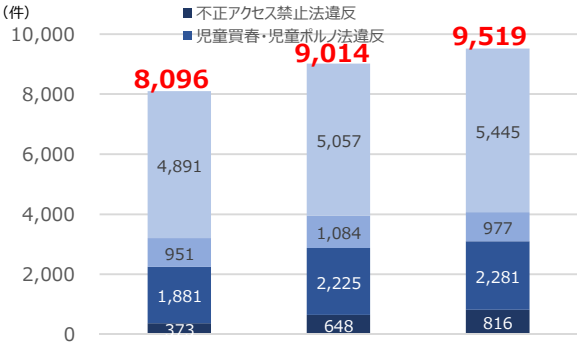
（データ出所）厚生労働省HPよりNISC作成

（参考）環境変化、国際情勢から見たリスク ／ 近年の脅威動向

現状認識

◆ 環境変化をとらえたサイバー攻撃の増加

➢ サイバー犯罪の検挙件数は増加傾向。
2019年中の検挙件数は過去最多。



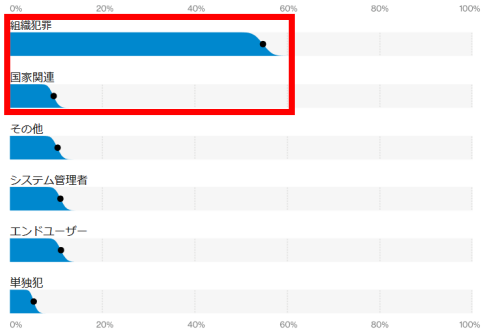
（データ出所）警察庁「令和元年におけるサイバー空間をめぐる脅威の情勢等について」よりNISC作成

➢ テレワークの普及に伴うサイバー攻撃の増加。
リモートデスクトップを狙ったブルートフォース攻撃の件数(米)
2020/3/9 約20万件 ⇒ 2020/4/9 約138万件
(約6.9倍)
（データ出所）Kaspersky

➢ クラウドサービスを標的とした脅威の増加。
クラウド脅威の合計と外部クラウド脅威：
2020年1月～4月にかけて**約7.3倍**
（データ出所）McAfee Labs

◆ サイバー攻撃の組織化 国家の関与が疑われるサイバー攻撃

世界における漏洩/侵害によく見られる攻撃者の種類



（出典）Verizon「データ漏洩/侵害報告書2020」

選挙に関連するサイバー攻撃事例

◆香港（2018年10月）
中国のサイバー情報窃取を行うものが、マルウェア（EVILNEST）により選挙中に香港の組織を攻撃対象とした。

◆米国（2018年11月）
イランを支援する攻撃者とのつながりが疑われるアカウントのネットワークの一部に、米共和党の候補者を装った多数のツイッターアカウントが確認された。

◆欧州（2019年）
選挙関連機関及びメディアに対するスフィアフィッシング攻撃

（データ出所）ファイアアイ

◆ サイバー空間を構成する技術基盤や国際ルール、データ覇権を巡る争い

例 新たなインターネットプロトコル(New IP)に係る議論

○2018年 ファーウェイを中心に、ITU-T次会期（2021～2024年）における新たな検討課題として、「New IP」に係る議論開始を提案。

○2020年12月 SG13・SG11会合において、次会期の新規設置検討課題として提案することは行わず、これ以上の議論は行わないとの結論となった。

（注）報道情報等を基にNISC作成

◆ サプライチェーン複雑化

主要通信機器の世界シェア

サーバー(2019年)	
デル【米国】	17.4%
HPE/New H3C【米国/中国】	15.4%
インスパー【中国】	8.7%
レノボ【中国】	6.4%
ファーウェイ【中国】	5.2%
その他	46.8%

（データ出所）IDC

移動通信インフラ(2018年)	
エリクソン【スウェーデン】	29.0%
ファーウェイ【中国】	26.0%
ノキア【フィンランド】	23.9%
ZTE【中国】	12.0%
サムスン【韓国】	5.0%
その他	4.1%

（データ出所）HIS Marit

◆ 新型コロナウイルス感染拡大に乗じたサイバー攻撃の発生

例 保健所等の専門機関を装った偽メール

2020年1月29日、保健所等の専門機関を装って新型コロナウイルス感染症に関する偽の情報を載せたメールが発見。偽メールは、「通知」という件名で、送信元として「〇〇保健所福祉室」という実在する保健所の名称を使用し、文面には「新型コロナウイルス関連肺炎については、中国武漢市を中心に患者が報告され、国内でも〇〇県で患者が報告されている」等と書かれており、添付のWordファイルを開くとマルウエアEmotetに感染するもの。

（注）報道情報等を基にNISC作成

◆ 従来から見られる攻撃の継続／サプライチェーンリスクの顕在化

情報セキュリティ10大脅威の変遷（組織）

2020年の順位	2017年の順位
1位 標的型攻撃による機密情報の窃取	1位
2位 内部不正による情報漏洩	5位
3位 ビジネスメール詐欺による金銭被害	ランキングなし
4位 サプライチェーンの弱点を悪用した攻撃	ランキングなし
5位 ランサムウェアによる被害	2位

（データ出所）IPA「情報セキュリティ10大脅威」よりNISC作成

◆ 経済社会全体での人材不足・偏在／リテラシーギャップの顕在化

➢ 人材不足感が大きく、IT企業に偏在。

セキュリティ対策に従事する人材の不足感
86% (米16%)
（データ出所）NRIセキュア「企業における情報セキュリティ実態調査」

情報処理・通信に携わる人材がIT企業に所属している割合
72% (米35%)
（データ出所）IPA「IT人材白書2017」

➢ サイバー空間拡大の中、リテラシー浸透が急務。

インターネットの利用時に不安を感じる人の割合
71%
（データ出所）総務省「通信利用動向調査」

インターネットや情報に関する倫理教育を受けたことがある割合
18%
（データ出所）IPA「情報セキュリティに対する意識調査」

（参考）「企業経営のためのサイバーセキュリティの考え方」

現状認識

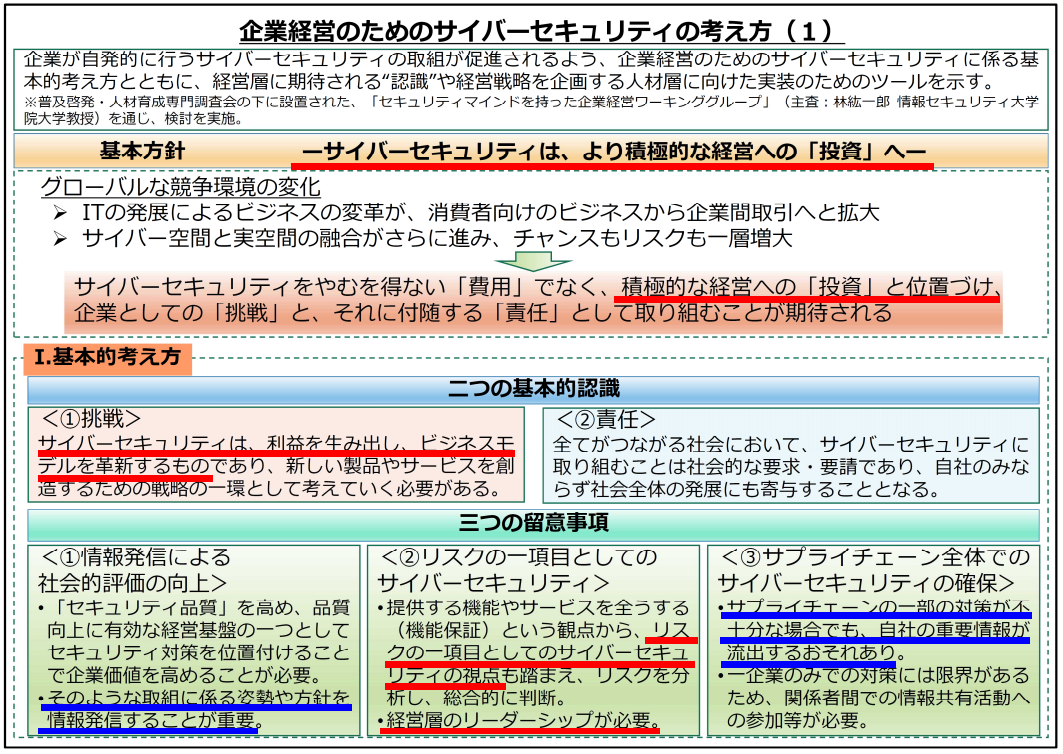
○2016年に示した「企業経営のためのサイバーセキュリティの考え方」は、DXの進展を通じ、より実態に即したものとなっていると考えられる。

→ 経営層の意識に関する現状認識を踏まえれば、その浸透に向け、更なる取組の深化が求められる。

◆「企業経営のためのサイバーセキュリティの考え方」（2016年8月 NISC）

※ 本専門調査会の下に設置された「セキュリティマインドを持った企業経営ワーキンググループ」（主査：林 紘一郎 情報セキュリティ大学院大学教授）を通じた検討を経て、本専門調査会に報告・公表。

※「『サイバーセキュリティ経営ガイドライン』と併せて、経営層に期待される"認識"を示すもの」とされている。



企業経営のためのサイバーセキュリティの考え方（１）

企業が自発的に行うサイバーセキュリティの取組が促進されるよう、企業経営のためのサイバーセキュリティに係る基本的考え方とともに、経営層に期待される"認識"や経営戦略を企画する人材層に向けた実装のためのツールを示す。
※普及啓発・人材育成専門調査会の下に設置された、「セキュリティマインドを持った企業経営ワーキンググループ」（主査：林紘一郎 情報セキュリティ大学院大学教授）を通じ、検討を実施。

基本方針　ーサイバーセキュリティは、より積極的な経営への「投資」へー

グローバルな競争環境の変化
- ITの発展によるビジネスの変革が、消費者向けのビジネスから企業間取引へと拡大
- サイバー空間と実空間の融合がさらに進み、チャンスもリスクも一層増大

サイバーセキュリティをやむを得ない「費用」でなく、積極的な経営への「投資」と位置づけ、企業としての「挑戦」と、それに付随する「責任」として取り組むことが期待される

I.基本的考え方

二つの基本的認識

＜①挑戦＞
サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。

＜②責任＞
全てがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる。

三つの留意事項

＜①情報発信による社会的評価の向上＞
- 「セキュリティ品質」を高め、品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。
- そのような取組に係る姿勢や方針を情報発信することが重要。

＜②リスクの一項目としてのサイバーセキュリティ＞
- 提供する機能やサービスを全うする（機能保証）という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。
- 経営層のリーダーシップが必要。

＜③サプライチェーン全体でのサイバーセキュリティの確保＞
- サプライチェーンの一部の対策が不十分な場合でも、自社の重要情報が流出するおそれあり。
- 一企業のみでの対策には限界があるため、関係者間での情報共有活動への参加等が必要。

＜環境変化を踏まえた評価・観点＞

■ DXやデジタル技術の活用に際するプラクティスとして、セキュリティ・バイ・デザインの考え方の下、DevSecOpsをはじめとした迅速で柔軟な開発・対処体制の構築が求められる中で、セキュリティ対策は「デジタル投資と一体不可分の投資」として位置付けられるべきではないか。

また、ビジネスの革新を伴うサービスのDX進展により、サイバーセキュリティリスクが社業そのものの継続性に直結する中で、セキュリティ対策は将来にわたる安定的な利益の確保につながる度合いが増しているのではないか。

→これまで以上に、経営層自らが全社的な課題として捉え、リーダーシップを発揮して対策を実施する必要性が増しているのではないか。

■ サプライチェーンリスクをはじめ、脅威の高度化・複雑化が深刻さを増す中で、企業のサイバーセキュリティへの取組が可視化され「トラスト」が価値の基盤となることで、投資行動やサプライチェーンを通じた取組の広がりがみられるのではないか。

併せて、これまで以上に中小企業が人材課題をはじめとしたリソース制約に直面する中で、クラウドサービスの利用も重要な選択肢となり得ることを前提とした対策が求められるのではないか。

人材の確保、育成、活躍促進に向けて

○人材の不足感に関する現状認識を踏まえれば、「質」・「量」両面での官民の取組の継続・深化とともに、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進めることで、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ではないか。

（１） ”DX with Cybersecurity”の推進

- 経済社会のデジタル化とセキュリティ確保が一体的に推進されるよう、サイバーセキュリティに係る人材の確保、育成、活躍を促進していく。

→本専門調査会でとりあげた３つの政策課題への対応を、今後「推進方策」としてとりまとめ、それを軸としてプログラムの提供・普及や環境整備等を進めていく。

（１）’ 政府におけるデジタル改革の推進

- 経済社会にデジタル化のメリットを行き渡らせるべくデジタル改革を推進していくため、政府部門においてそれを牽引していく人材の確保が必要。

→「デジタル社会の実現に向けた改革の基本方針」及び2021年度前半に改定される「政府機関におけるセキュリティ・IT人材育成総合強化方針」等に基づき、取組を進める。

（２） 巧妙化・深刻化する脅威への対処

- 組織化・洗練化され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等も見られる中で、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。

→脅威動向に対応したプログラム・コンテンツの開発等を行うとともに、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。