参考資料３

◆「サイバーセキュリティ戦略」（平成 30 年 7 月 27 日閣議決定）（抄）

４．目的達成のための施策

４．１　経済社会の活力の向上及び持続的発展

近年、企業においては、パソコン・スマートフォンを始めとするデジタル端末やインターネットの活用による業務の生産性の向上にとどまらず、経営改革や革新的なサービスの創出といった新たな価値を生み出す動きが進展している。サイバーセキュリティ対策をやむを得ない「費用」ではなく、こうした動きを支える基盤としての「投資」であると捉えて、一体的に取り組むことは、産業の成長及び国際競争力の強化につながり、我が国の経済社会の活力の向上及び持続的発展の観点から重要である。新たな価値創出を支えるサイバーセキュリティの推進サイバー空間と実空間の一体化が進展していく中で、企業が直面するサイバーセキュリティに係るリスクは、これまで以上に高まっていく。こうした中、企業におけるサイバーセキュリティに対する問題意識は、一部の業種や大企業を中心として高まっている。今後は、全ての産業分野において、企業が事業継続を確固なものとしつつ新たな価値を創出していくためには、サイバーセキュリティに取り組む必要があるとの認識を広げ、取組を促進していく必要がある。その際には、サイバーセキュリティに係るリスクは企業が直面する様々なリスクの一つであり、その対策をリスクマネジメントの一環として捉え、業種・業態等の状況に応じて、自然な形で対策が組織に浸透していくことが重要である。

（１）経営層の意識改革

サイバーセキュリティ対策については、その取組自体が利益を生むものではないとの考え方が未だ支配的であると考えられる。この背景には、サイバー空間は自由に何の備えもなく利用できるものであり、散発的にしか起こらない、経営に対して影響が生じるような攻撃への対処は「費用」でしかないという考え方がある。しかしながら、サイバー空間の利用が急速に進展する中、自由であるがゆえに常に脅威が潜んでいるという認識に立って、そのための備えをすることが必須である。また、企業においては、サイバーセキュリティ対策の組織上の位置付けが明確になっていないと取組が進みにくいという側面がある。このため、経営層が、サイバーセキュリティ対策をやむを得ない「費用」ではなく、事業継続や新たな価値創出のために不可欠な「投資」であると捉えられるようにするため、経営層の意識改革が不可欠である。

具体的には、経営層は、取締役会等を通じたサイバーセキュリティに関する積極的な関与が期待されるとともに、リスクマネジメントのために必要となるサイバーセキュリティに関する一定の知識・能力を身に付けることが求められる。その際、経営層に深い技術的な知識やスキルを期待することは必ずしも現実的ではない。このため、経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、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（いわゆる「戦略マネジメント層」）を確保することが重要である。また、経営層は、自社の対策だけでなく、外部委託先やサプライチェーン全体を視野に入れ、リスクマネジメントとして相応しいレベルの対策ができるような体制を整備するとともに、株主等に対してサイバー空間を活用したビジネスの恩恵とリスクを説明できるようにする必要がある。

このような状況を踏まえ、官民が連携して、経営層に対してサイバーセキュリティ対策に関する説明や議論ができる人材を発掘・育成するとともに、経営層向けセミナー等を開催し、経営層の意識改革を促していく。また、国は、サイバーセキュリティに取り組む企業による宣言の促進や、類似の企業の対策状況と比較することで、自社に必要な対策を可視化するためのツールの整備など、経営層に分かりやすくサイバーセキュリティ対策を訴求するための施策を推進する。また、学会等と連携しつつ、企業がサイバーセキュリティ対策の実施において参照すべき法制度に関する整理を行う。

（２）サイバーセキュリティに対する投資の推進

企業がサイバーセキュリティに関わる取組を継続的に実施するためには、それに対応する経営上のインセンティブがあることが重要である。すなわち、財務的な観点を含め、サイバーセキュリティに係るリスクとその対策が可視化され、経営層がその現状を認識し、更に必要な具体的な対策を検討・導入するとともに、市場がその取組を企業価値の向上につながるものとして評価し、サイバーセキュリティに対する投資へのインセンティブが継続的に生まれる、という好循環が形成されることが望ましい。

このため、投資家を意識して、企業が積極的にサイバーセキュリティに関する取組について情報発信・開示を行うことが重要であり、国は、ベストプラクティスの共有やガイドラインを策定するとともに、情報発信・開示の状況についての継続的な把握・評価に取り組む。加えて、投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組み作りを進めていくことも必要である。

また、企業に対するサイバーセキュリティの促進策について、サイバーセキュリティに対する投資のインセンティブが効果的に機能するよう、国はその活用状況をフォローしつつ、必要に応じて所要の措置を検討する。

このほか、サイバーセキュリティのリスクマネジメント手段の一つとして、保険の活用が広がっているが、サイバーセキュリティ対策の実施状況に応じて、適切に保険料が算定される仕組みにより、リスクへの備えに対するコストが明確になっていくため、投資が進めやすくなる可能性がある。こうした点を踏まえ、官民が連携してサイバーセキュリティにおける保険の活用を推進するための方策について検討を行う。

４．４　横断的施策

４．４．１　人材育成・確保

「Society5.0」の実現に向けて新たな価値が創出されていく中、サイバー攻撃の脅威は広がっており、一部の専門家がサイバーセキュリティの確保に取り組むのではなく、それぞれの役割を遂行する観点から、主体的に取り組むことが求められる。

こうしたパラダイムシフトにより生じる将来を見据えつつ、各々の組織の「任務」の遂行や個人の安全な利用を支える観点から、サイバーセキュリティの確保に取り組む各人材層において保有すべき知識や技術の水準を明確化することが求められる。その上で、教育等を通じ、資格・評価基準等によって可視化された確かな知識と実践力を備えた人材が、適切な処遇を受け、更に実務経験を積み重

ねることにより、人材の需要と供給が相応されるといった好循環の形成が必要である。

このため、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・確保を強化していく。その際、イノベーションを推進する観点から、人材の多様性の確保を推進していくことが重要である。

（１）戦略マネジメント層の育成・定着

企業経営においてサイバーセキュリティ対策を進めていくためには、それが単に技術的な課題にとどまらないことから、専門家や実務者任せにすることは適切ではない。経営層が示す経営戦略や事業戦略の下、組織がマネジメントすべき様々なリスクの一つとして、業務やサービス等を実現するために必要なサイバーセキュリティに係るリスクを認識し、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立場として、社内外の実務者・専門家を活用・指揮しつつ、対策や事案への対応を実践する役割を果たし得る人材が求められている。このため、こうした役割を担う層を「戦略マネジメント層」と位置付け、経営層の理解の促進を含め、産業界と連携しつつ、その定着を図る。

また、業種や業態によっては、文化や慣習などの違いにより、業務やサービス等を実現するための既存のマネジメントに対し、サイバーセキュリティ対策を組み込み、実践することに困難を伴う場合がある。このため、多様なビジネスとそのマネジメントの実態があることを踏まえつつ、戦略マネジメント層向けの実践的な教材の開発や、指導者の発掘・育成も含め、学び直しプログラムの実践を推進する。

（２）実務者層・技術者層の育成

戦略マネジメント層が示す方針を踏まえ、システムの企画や構築・運用時における対策等を実践する実務者層や技術者層については、これまで官民において、教育プログラムや資格・試験、演習の実施などの様々な取組が行われてきた。

こうした知識や技術の水準を高める取組は、引き続き強化を図っていく必要があるが、実務者や技術者が戦略マネジメント層に対して貢献できるよう、日々進化する情報通信技術や制御システムの技術、これらに対するサイバー攻撃について理解を深めることはもとより、経営層の方針を理解しつつ、他の専門人材と円滑にコミュニケーションをとりながらチームの一員として対処ができるようにすることが重要である。このため、実務者層・技術者層向けの育成プログラムにおいては、戦略マネジメント層が示す概念的・抽象的な考えを理解し、それを具体化するとともに、様々な関係者と円滑なコミュニケーションができるような学び直しによるスキルの開発や実践的な演習が必要である。

さらに、突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保も引き続き行っていく。例えば、サイバー攻撃に対する防御方法、攻撃手法も含む対処法、情報を収集して分析評価を行う方法の体系化を含む研究を通じ、グローバルに切磋琢磨する機会を広げ、対策を検討できる能力の育成を引き続き推進する。

（３）人材育成基盤の整備

中長期的な情報通信技術の進化を見据え、応用分野であるサイバーセキュリティの土台となる基礎原理の理解を促し、論理的思考力や概念的思考力の育成を充実させる必要がある。このため、サイ

バーセキュリティや情報通信技術に関する基礎的な内容については、産学官が連携して、知識・技術体系やそれに基づくモデルカリキュラムの在り方の検討を行う。

また、サイバーセキュリティや情報通信技術について若年層の教育を強化するため、初等中等教育段階では、小学校段階から必修としたプログラミング教育など、発達の段階に応じてコンピュータなどの情報通信技術の原理や仕組みなどを理解し、プログラミング的思考といった論理的思考力を育てるなど、教育課程内で情報活用能力の育成に着実に取り組む。さらに、こうした情報活用能力の育成に関する履修項目が、教員養成課程において着実に盛り込まれるようにするとともに、教員の研修を充実させる。その際、必要に応じて産業界などの人材の活用も柔軟に進めることが重要である。加えて、近年、若年層によるサイバー犯罪が発生していることから、情報モラル教育も重要な課題である。

さらに、将来、高度なサイバーセキュリティ技術を持つ人材となることが期待される若年層向けに、教育課程外の地域や企業・団体等において、産業界などの人材の能力を柔軟に活用しつつ、自由にサイバー関連ツール、機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備を進める必要がある。同時に、こうした自己実現の環境整備は、倫理教育と併せて実施することで、若年層による興味本位のサイバー犯罪などの防止に効果があると考えられる。また、産学官連携により、大学・高等専門学校等の高等教育段階における情報技術人材の育成を引き続き推進する。

（４）各府省庁におけるセキュリティ人材の確保・育成の強化

政府機関における統一的な方針に基づき、セキュリティ対策を専任で担う「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、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。各府省庁の人材確保・育成計画に基づき、定員の増加による体制整備、レベルに応じて知識・能力を高められる研修や高度なセキュリティ技術者を活用した演習、適切な処遇の確保等について、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。

（５）国際連携の推進

サイバーセキュリティの問題への対応がグローバルな規模で求められていることを踏まえ、我が国のサイバーセキュリティ人材の育成においても、国内で完結するのではなく、可能な限りグローバルな規模で切磋琢磨できるようにすべきである。このため、人材育成に取り組む大学や公的機関等のプログラムについて、国際的な基準に照らして一定の基準があると認められるものを認定し、共同演習の実施や単位互換の認定など海外の人材育成を行う組織との間での様々な連携を促すための仕組み作りを主要国との連携の下で進める。

加えて、海外におけるサイバーセキュリティ人材育成にも貢献をするため、我が国におけるサイバーセキュリティの人材育成等によって得られた知見を活かし、海外におけるサイバーセキュリティ人材の能力構築に貢献する。