「サイバー安全保障」確保のための人材育成

“民間事業者・産業界の連携・協力”

近年サイバー空間における課題は、個人の犯罪から国家が関与する脅威へと、その幅も深さも飛躍的に広がりつつあり、サイバー安全保障分野の対応能力の向上が急がれている。

2022 年 12 月に政府において決定された「国家安全保障戦略」等では「サイバー安全保障分野の対応能力を欧米主要国と同等以上に向上させる」としており、「諸外国や関係省庁及び民間事業者との連携により、平素から有事までのあらゆる段階において、情報収集及び共有を図るとともに、我が国全体としてのサイバー安全保障分野での対応能力の強化を図ることが重要である」としている。

また、「政府全体において、サイバー安全保障分野の政策が一元的に総合調整されていくことを踏まえ、防衛省・自衛隊においては、自らのサイバーセキュリティのレベルを高めつつ、関係省庁、重要インフラ事業者及び防衛産業との連携強化に資する取組を推進する」としている。

これらを踏まえれば、民間事業者・産業界においても、サイバー安全保障及び防衛省・自衛隊の活動と役割に対して連携・協力して取り組む課題や施策を明確にし、我が国が一体としてサイバー安全保障の確保を推進していくことが不可欠と考える。

政府においてサイバーセキュリティに関わってきた我々OB 有志は、このような認識の下、民間事業者・産業界が連携・協力して取り組む課題と推進する施策の方向性を明らかにするため、サイバーセキュリティ問題に詳しい有識者にお集まり頂き、検討を依頼、その提言を受けた。

特に「サイバー安全保障を円滑に強化するための人材育成には、新たな視点に立って、民間事業者・産業界が連携・協力していくことが不可欠である」との指摘は重要であり、今後は提言を一つのたたき台とし、これを実現していくための官民の話し合いの場の設定のための関連事業者等の結束を期待する。

OB有志

齋藤　隆	（元）統合幕僚長
鈴木茂樹	（元）総務事務次官
安藤久佳	（前）経済産業事務次官
島田和久	（前）防衛事務次官
中村　格	（前）警察庁長官

（注：名称は年次順）

報告書確定版
2023 年 6 月 30 日

―サイバー安全保障の円滑な確保に向けて―

～有識者会議の報告と提言～

Ⅰ　サイバー安全保障の円滑な確保に向けた検討の経過とその重点

本有識者会議(以下「本会議」という)は 2023年1月から6月にかけ、2022 年 12 月に政府決定された「国家安全保障戦略」「国家防衛戦略」「防衛力整備計画」[1](以下「国家安全保障戦略等」という)を踏まえつつ、「英国国家サイバー戦略 2022」や「米国国家サイバーセキュリティ戦略」[2]など主要国の戦略を参照し、「ロシアのウクライナ侵略事案」の検証や、自衛隊のサイバー教育の現場である「陸上自衛隊通信学校(横須賀久里浜)」の視察等を行いながら、サイバー安全保障に係る課題について計13回にわたって議論した。

本会議では、特に平時から有事に至る他国の国家主体が関与、又は関与が疑われるサイバー事案に対しては、国を挙げて取り組む必要があるとの認識の下、民間事業者・産業界においてもこれら課題の解決のために如何に効果的に連携・協力の実を挙げるかという観点から、優先的に取り組む事項について提言としてまとめた。

なお、提言はこうした分野に焦点を絞っているが、日本が対応すべきサイバー安全保障に係わる課題は、サイバー攻撃による兵器等の無力化への対応だけでなく、重要インフラへの攻撃のほか、現代戦における特徴である偽情報の拡散を通じた情報戦、平時における認知領域における情報戦[3]等、サイバーインテリジェンスへの対応等も含め、多岐にわたるものであり、こうした新たな視点も踏まえて議論を行ったものであることを付言しておく。

Ⅱ　サイバー空間が抱える課題

まず、サイバー空間が抱える課題について、全体を俯瞰する。「国家安全保障戦略」においては、「サイバー空間・海洋・宇宙空間、技術、情報、国内外の国民の安全確保等の多岐にわたる分野において、政府横断的な政策を進め、我が国の国益を隙

---

[1] 国家安全保障戦略等におけるサイバー安全保障に関する部分の要約（資料編： 1 参照）

[2] 「米国、英国サイバー戦略」の５つの柱（資料編： 2 参照）

[3] 認知領域における情報戦（資料編： 3 参照）
サイバー手段を利用しての偽情報の拡散、あるいは経済的手段等あらゆる手段を組み合わせて仕掛けられる平時におけるハイブリッドの戦いは国家の意思決定にも影響を及す認知領域へと広がりを見せている。

なく守る」としている中で、第一の柱として「サイバー安全保障分野での対応能力の向上」が謳われている。これは軍事と非軍事、有事と平時の境目が曖昧になり、ハイブリッド戦が展開され、グレーゾーン事態が恒常的に生起している、という現在の安全保障環境の特徴を反映したものである。

このような安全保障環境の下、我が国が対処すべき具体的なサイバーセキュリティ事案を想定すると、我が国の意思決定システム、指揮命令システム、防衛省・自衛隊の指揮統制能力、戦力発揮能力などの任務遂行能力を弱体化させることを目的とした、以下のような事案が考えられる。

- 情報通信システムへの DDoS 攻撃等によるシステムダウン
- 情報通信システムへのハッキング・ウイルス侵入による、システムの機能の破壊・停止、データの破壊・盗取・改竄・凍結
- フィッシング等による、ID やパスワードの盗取、機密情報の漏洩・公開、脅迫、経済的利益の要求等
- 上記の単独、複合した手段による、通信、電力等エネルギー、金融、交通、物流等のシステム障害を通じた社会機能の麻痺　等々

Ⅲ 「サイバー安全保障」について検討する視点

1. 基本的認識

「国家安全保障戦略」において「サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障対応能力の強化」が謳われている。

前記したように、想定されるサイバーセキュリティ事案とそれへの対応を網羅的に考慮し、政府が全体を俯瞰しながら対応を主導していくことは、極めて重要である。政府はそれを可能とするための法的及び組織的な課題解決のために動き出している。

一方で産業界の意識は依然として十分ではない。従来、非国家主体によるサイバー犯罪に対しての危機感は共有されているものの、他国の国家主体が係わるようなサイバー事案に対する危機感は低いと思われる。

我が国の情報通信インフラの大半は民間事業者が構築しており、ロシアのウクライナ侵略事案に見られるように、国家主体が係わるような「サイバー安全保障事案」への対応は自己の事業を守るという意味でも避けては通れないと考える。民間事業者・産業界においてもこうした実情に理解を一層深め、サイバー安全保障のための主体的な取組を強化することが求められる。

2. 平時からの対応と武力攻撃事態の抑止

「国家安全保障戦略」においては「サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景と

した形でも平素から行われている」と記載されている。このようにサイバー安全保障に係わるサイバー攻撃は、平素から武力攻撃に至らない時点で我が国の指揮統制機能等の弱体化を図った後に、サイバー攻撃を含む本格的な物理的攻撃（武力攻撃事態）へと移行すると予測され、平素から相手のサイバー攻撃を阻止できる能力を備えておくことが求められる。また、このことが相手の本格的武力攻撃への誘惑を思いとどまらせ、有事の抑止にもつながる。このため予想されるサイバー脅威の動向と攻撃の兆候を見極めるべく常続的にサイバー空間を監視[4]する必要があると考える。

3. 関連施策間の連携強化及び国際連携の必要性

「国家安全保障戦略」では「サイバー安全保障の強化に資する他の政策との連携を強化する。さらに同盟国・同志国等と連携した形での情報収集・分析の強化、 攻撃者の特定とその公表、国際的な枠組み・ルールの形成等のために引き続き取り組む」とされている。この観点からは、サイバーに関する国際規範形成への努力[5]及び安全保障環境の改善のための他の関連施策と連携したサイバー能力構築支援等も重要である。

一方、ロシアによるウクライナ侵攻におけるサイバー攻撃に対して、グローバル企業が有効に対応したと言われている。我が国及び産業界等のシステムがグローバル企業のシステムに依存していること、これら企業のサイバーセキュリティ能力の高さを考慮すると、同盟国・同志国企業との連携・協力を促進していくための仕組みづくり、及びグローバル企業と直接的な関係を有する当該国政府との、より一層緊密な協力体制の構築も重要である。

サイバーセキュリティ分野において、外国政府及び外国企業等との連携・協力を進めるためには、機微な情報の取扱いに係るセキュリティ・クリアランス制度が国・自治体だけでなく、官民連携のもと、機微な情報にアクセスする民間事業者・産業界まで含めた形で早期に実現されることが不可欠である。

このようにサイバー安全保障に関しては、国際的な枠組みの現状、あるいはサイバーセキュリティ能力に関する我が国の現状、安全保障上の我が国の立ち位置を認

---

[4] 警戒監視活動について

自衛隊は周辺海空域の警戒監視活動を 365 日、防衛省設置法の調査・研究等を根拠に実施している。

[5] 国際規範形成への努力（タリンマニュアル）（資料編： 4 参照）

NATO CCD COE（Cooperative Cyber Defense Centre of Excellence）は、2008 年に設立され、エストニアのタリンに本部を置く。本 COE はサイバー空間での規範をタリンマニュアルとして策定している。2023 年 6 月現在「タリンマニュアル 1.0」と「タリンマニュアル 2.0」がある。 なお「タリンマニュアル 3 .0」の検討が 2021 年から開始されている。

識した上で国際連携を図っていくことが必要と考える。

以上のような基本認識のもと、サイバー安全保障「態勢」及び「体制」の整備のために特に重視すべき課題は以下のとおりと考える。

Ⅳ サイバー人材の育成に係る課題

政、官、産、学のすべてにおいて「トップ」に立つ人が、サイバー安全保障に関する「半端でない」認識を向上させ、持続的な指導力を持って、人材の育成をすることが求められている。

その上で防衛省・自衛隊のサイバー要員の養成だけでなく政府や民間事業者・産業界も含めた我が国全体としてのサイバー人材の育成を急ぐ必要がある。従来民間事業者・産業界におけるサイバー教育はサイバー攻撃による経済的損失の回避という受け身的な視点が強かったように思えるが、喫緊の課題は官民連携して「サイバー安全保障」を担える「高度なサイバー能力をもった人材の育成」と、そのための「人材の裾野拡充と人材育成環境の整備」、まさにサイバーの人材需要に応じた質的向上と量的拡大という両面からの人材育成の新たな強化が求められている。

同時に、サイバー職務を従来とは異なる新しい時代の職務として明確に位置付け、官民共通の認識の向上を図り、施策を集中させる必要もある。

1．高度なサイバー能力をもった人材の育成

自らのシステムを守るのみでなく、相手側のサイバー空間を監視、無効化するためにどこまで実施するかの枠組みが政府において検討されている。サイバー安全保障事案に対応できる高度なサイバー能力をもった人材として、「個別のサイバー事案に対応できる優れた実践的な能力をもった人材」及び「サイバー事案全体を俯瞰し上級の意思決定者に今何をすべきか進言できる人材」が求められている。

（1）民間事業者・産業界による教育協力・支援

民間事業者・産業界においては、サイバーセキュリティ人材育成の取組が早くから始まり、人材育成を一定規模で業務として提供している事業者も出現している。ついては、サイバーセキュリティに係る産業界における人材育成サービス[6]の活用が効果的と考える。

特に防衛省・自衛隊が 2027 年度を目途にサイバー部隊約 4000 人とそれを含むサイバー要員約 2 万人を育成することとされており、そのためには、防衛省・自衛隊の内部での教育の強化に加え、従来以上に民間事業者・産業界の力が求められると考えられる。

---

[6] 民間事業者のサービスの例
不正プログラム解析、フォレンジック（証拠の調査・解析）、ペネトレーションテスト等

このため、民間事業者・産業界においても、これに応えられるよう防衛省・自衛隊との一層緊密な関係の構築が必要と考える。

2. サイバー人材の裾野の拡充と人材育成環境の整備

サイバー安全保障人材の育成を行う際、その育成対象の候補者は、一定のデジタルスキルを持つことが想定される。しかし、我が国では、デジタルスキルを持つ人材自体が不足していることが指摘[7]されている。サイバー安全保障人材を強化するには、人材の裾野の拡充と人材育成環境の整備が重要と考える。

(1)各種能力に必要なスキルの明確化

そのためには、まず想定されるサイバーセキュリティ事案から、これに対処するのに必要な各種能力を分析、その能力に必要なスキルとその習得に必要なカリキュラム要素、教材、演習内容等を明確化する必要がある。

(2)カリキュラムの標準化と定期的な更新

その上で、各種サイバー事態に対応できる人員を維持するためには、サイバーセキュリティに係るスキルの分野別、機能別、レベル別の標準的な教育カリキュラム要素の作成が必要になる。

これにより、同じ分野・機能・レベルのスキルを有する人員を組織の壁を越えて集め、稼動させることが可能となり、サイバーセキュリティの組織的能力の向上に資するものと考える。

同時にサイバー技術の進化やニーズの変化に合わせて、定期的な更新を図ることに留意する必要がある。

(3)能力認証制度

また、どのようなサイバーセキュリティ対処能力を各人が有しているかを明らかとするための能力レベルの認証が必要である。

国内においては、産業界においてIPA[8]が七段階のスキルレベルを設定しているほか、システム監査など複数のセキュリティ能力に関する認証制度が存在する。海外においても、CISSP[9]、GIAC、CISAなど著名な団体が運営するグローバルな能力の認証制度が存在し、我が国のサイバーセキュリティ人材も認証を受けている。

---

[7] デジタル競争力ランキング：スイスの国際経営開発研究所（IMD）により、2022年9月28日公開した世界デジタル競争力ランキングでは日本は６３ヶ国中過去最低の２９位だった。ほぼトップ１０に入っているシンガポール、韓国、台湾、香港から大きく遅れており、それに続く中国の背中も遠くなっているのが実態である。（資料編：５参照）。

[8] IPA：独立行政法人情報処理推進機構

[9] CISSP(Certified Information System Security Professional)：サイバーセキュリティ能力の認証制度。著名な団体が世界中に展開。2022年1月現在で、世界で152000人、日本に3300名以上の資格者がいる。（資料編：６参照）

ア　国際的に整合の取れた我が国の能力認証制度

サイバーセキュリティに関して同盟国等と共同、連携するためには、サイバー要員の能力水準を合わせることが必要である。スキルレベルの設定とそれを習得しているという能力の認証制度があることが、組織能力の向上と組織間共同、連携の円滑化の観点から必要である。そのために国内外の能力認証制度等を参照に、我が国におけるサイバー脅威の特徴や安全保障環境などを踏まえつつ、国際的に整合の取れた我が国の能力認証制度の整備が必要である。

イ　能力認証の維持

サイバー領域での技術進歩は急速なことから、能力の認証後も絶えずスキルのブラッシュアップをし、一定のスキルレベルが維持されるような取組は大切である。人材を把握する上で、また官民連携していく上でも共通の能力認証の整備が必要である。

特に能力認証にあたっては、実技経験を踏まえたレベル設定、あるいは各種認証制度を組み合わせることも考慮すべきである。また能力認証へのインセンティブの面からも能力認証者への組織内の処遇等についての配慮が求められる。

（4）サイバー職務の明確な位置付けと処遇

サイバーセキュリティ能力のある貴重な人材が、有効に活用されていないという例が見られる。当該職務の重要性に関して管理者や一般の理解が向上し、多くの人から正しく評価されるような環境整備が必要である。具体的には採用条件、キャリアパス、職位などで魅力のある職務とすることも重要である。特に、サイバー要員の他の職務への配置等による能力の劣化等を回避するためには、危機管理等を含むサイバー関連職務での人事管理、サイバー人材のキャリアアップの整備が必要である。

（5）人材バンクの構築、「リボルビングドア」的な制度、交流機会の促進

サイバー人材を一定の規模で確保し続ける為には、省庁間及び民間との間で行き来を可能にした人材育成、実務経験の蓄積が必要である。そのためには安全保障に関するサイバーセキュリティ人材が官民を行き来できる「リボルビングドア」的な制度[10]や、現状の人材の状況把握（データバンク化）を実現すると共に交流の持続性を維持するため、民間事業者・産業界においても、政府主催のサイバー演習（教育）への一層積極的な参加など交流機会の増加を図ることが必要である。

（6）ｅラーニングの推進

日々進化するサイバーセキュリティを含むデジタル知識を効果的に教育できる指導者の数も限られることから、サイバーセキュリティの基礎的な知識等の習得には

[10] 「リボルビングドア」的な制度：回転ドアを通じて人員が行きできる様に、サイバー人材においても組織間を行き来できるような制度

CBL（Computer Based learning）を含むｅラーニングの活用が有効な手段と考える。

短期間に大量の人員を育成するためには、集合研修によっては研修施設や設備、教員の容量の観点からは厳しい状況が想像される。自衛隊員あるいは企業人を職場から抜いて集合研修を受けさせることは、職場の活動に支障を来すことも懸念され、職場に居ながらに研修を受けることが有効である。

このように人材の裾野を拡充するにはｅラーニングが重要と考えるが、なおその内容は単に受講するという受け身でなく、CTF(Capture the Flag)など実践的な訓練を可能とする工夫が必要である。

その対象として例えば、官民の初級者に対するｅラーニングによる一定のレベルの資格付与、あるいは過去サイバー関連業務、プログラム開発等携わったOB等のリスキリニングのためのｅラーニングが考えられる。

（7）グローバルな人材育成のための外国の大学との交流促進

一般的にサイバーセキュリティ分野においては海外との共通のカリキュラムがないために米国等外国の大学間交流に支障をきたしているとの指摘もある。

同盟国などと連携してサイバーセキュリティ安全保障を確保するためには、外国の大学[11]において学び、知識・技能を身に付けるとともに人的なつながりを作ることは重要である。同時に我が国の交流人材の受け入れ体制の充実や海外の大学との単位の相互承認なども配慮する必要がある。

Ⅴ 「能動的サイバー防御」を支える人材と総合的な態勢構築

一般的にはサイバーセキュリティ事案は、それがサイバー攻撃なのかシステムの不具合なのか、またその実施主体の曖昧性も内在しており、アトリビューション（攻撃者の特定）を含めサイバー空間で今何が起きているか把握するための能力を持つ人材と態勢は極めて重要である。特に「全体を俯瞰し指揮できる人材」そして「個別の事案に対応できる優れた実践的能力を持つ人材」が相当数必要である。

同時に、「能動的サイバー防御」をより効果的に実施するには高度なサイバー人材の育成はもとより、それを法的側面、及び急速に進展しているAI等を利用したシステム等で支える総合的な態勢の構築が求められる。

Ⅵ 政府と重要インフラ事業者等との連携・協調

民間事業者によって支えられている各種重要インフラシステムのサイバーセキュリティの確保は、一義的には各事業者において担われるものであり、セキュリティ対策を講じ、サイバー事案に対処する態勢を整えることが求められる。

一方、政府としては生起しているサイバー事案が、どのように重要インフラ及び国

[11] 米国国防大学のサイバー教育の例（資料編：７参照）

家社会に影響を与えるかを評価し対処する必要がある。

そのために、サイバー安全保障の視点に立って、国、公的機関、特に重要インフラ事業者及び防衛産業等の防護に関しての官と民の連携をいかに強化するがが課題である。

現状では、民間事業者・産業界は、それぞれにサイバーセキュリティ人材の育成を進め、NICT や IPA 等の公的機関がサイバーセキュリティ教育システムや演習基盤等を提供して、CSIRT[12]など部分的には国と民間事業者・産業界が連携した取り組みを始めている。

しかし、グレーな事態から有事までのサイバー事案を想定して、対処シナリオの作成[13]、サイバー教育・人材育成・訓練・演習などを連携・協力して実施している現状にはない。

国、防衛省・自衛隊と民間事業者・産業界、場合によっては同盟国[14]などを含め、サイバーセキュリティ事案に対して共通のシナリオに基づいて対処することを前提として、合同で教育、訓練、演習などが実施できる環境の整備が求められる。

Ⅶ 官民連携の強化

1. 官民連携した国家としての統合力

サイバー安全保障の視点に立った時、特に統制国家が実施してくるサイバー攻撃は、各種専門性を共有、連携し様々な手段を講じてくる可能性がある。それに対応するには一企業、一組織単独では困難である。官民連携の観点では、日本サイバー犯罪対策センター（JC3）の例に見られるようにそれなりに進展しているところもあるが、官の持つ情報と、民の持つ情報を如何に融合するか、関係省庁間の連携を強化し官民連携して国家として統合力を如何に発揮するかが重要である。

2. 官民連携上のセキュリティ・クリアランス

---

[12] CSRT: （Computer Security Incident Response Team）：「コンピュータセキュリティインシデント」に関する報告を受け取り、調査し、対応活動を行う組織体の呼称。

[13]NATO における「サイバー防衛演習」：「Locked Shields」というサイバー防衛演習では、NATO 各国及びパートナー国から参加したチームがサイバーレンジを用いた高度なサイバー防衛演習を毎年行っている。「Locked Shields」の特徴としては、理論的に検討されたサイバー紛争のシナリオを用いて、情報技術のみならず、国際法や国際政治の知識・スキル、および、軍官民連携が高度に求められることがある。（資料編： 8 参照）

[14]日米協力における重要インフラの位置づけ：「日米防衛協力の指針」「サイバー空間の協力」において、「自衛隊及び米軍が任務を達成する上で依拠する重要インフラ及びサービスを防護するために協力する」としている。（資料編： 9 参照）

サイバー事案に関して官民が連携していく上で、民間人のセキュリティ・クリアランスの取得や政府と事業者の間における秘密保持契約は避けて通れない。サイバー安全保障強化のための官民連携にセキュリティ・クリアランスは不可欠であるとの積極的な発想が求められる。

(1)官からの情報提供の指針

サイバーに関連した様々なデータについてこれを効果的に活用できるような管理体制を構築することが必要である。この際、保護すべき機微な情報を明確にするとともにサイバー脅威情報などが広く民間においても防御に不可欠であることなどから、必要な情報は最大限に共有するという観点が重要である。その上でサイバーセキュリティに関する技術開発を推進するためには民では得られないインシデント情報を含むサイバー関連情報を官からより積極的に提供するための指針の整備が求められる。

(2)セキュリティ・クリアランス取得への適切な環境整備

サイバーセキュリティに関し、官民連携でサイバー安全保障に取り組むためには、民間人材によるセキュリティ・クリアランスの取得や政府との秘密保持契約が不可欠であるということを、企業経営者、株主に啓発していく必要がある。同時にセキュリティ・クリアランスを取得した人に対しては適正な情報提供と評価が与えられるなどの必要な環境整備が求められる。

3. 民間事業者・産業界からの情報提供のための枠組みの構築

民間事業者・産業界からの官への情報提供(例えばインシデントが生起した場合の情報)についても、企業のレピュテーションリスクを含めた株主との関係、あるいは個人情報保護法との関係で共有することに消極的な実態があるが、これらを改善するための官側における情報取扱のルールや企業の免責規定の整備等、企業の活動を支援するための制度面での所要の措置が求められる。

4. 官民の信頼(顔の見える)関係の醸成

セキュリティ・クリアランスの問題が解決してもすべての問題が解消するわけではない。政府と民間企業がお互いの役割や立場を理解し、信頼関係を築くことが重要である。秘密情報のみでなく、OSINT(Open Souse Intelligence) 情報等サイバー事案に関する情報等を共有し、提供し合うための政府と民間企業が恒常的に協議できる枠組みを構築し、お互いの顔が見える信頼関係の醸成のための地道な努力が必要である。

5. 民間事業者・産業界の連携強化の枠組みの構築

上記4.に関連して個別に関連企業が官と連携するのではなく、民間事業者・産業界が一体となって政府機関、防衛省・自衛隊との連携の枠組みを設けることが必要である。なおこのような連携組織の構築にあたっては、その持続可能性にも配慮が必要である。

「サイバー安全保障」の円滑な確保に向けた提言

～サイバー安全保障に係る人材育成のための連携・協力～

今後の「サイバー安全保障」への対応に当たっては極めて広範かつ多くの課題を抱えており、我が国としての対応をより高度化させていくために政府は様々な施策を推進している。より有効かつ迅速なサイバー安全保障への対応を実現していくには民間事業者・産業界の連携・協力は不可欠である。

サイバー安全保障に関して、民間事業者・産業界の連携・協力の方向性を、特に喫緊の課題である人材育成を中心に以下のように提言する。

提言Ⅰ　産業界連携の枠組創設と官民連携

「サイバー安全保障」を確保するための諸課題は相互に関連する。民間事業者は、それぞれの得意分野があり、ビジネスとして成り立つのかといった事業者としての個別の判断がある一方、サイバー脅威が深刻化する中、自らのビジネスを守る観点からも政府との連携強化を進めることが重要である。

1. サイバー関連産業界等の連携のための枠組みの創設

「企業間の情報共有」あるいは「事業推進のための一定の方向性」また「官・民連携の架け橋」として、まず民間相互にサイバー安全保障に係る情報連携を含めてエコシステムを構築し、推進するための核となる持続性のある枠組みを創設することを提言する。

2. 民間事業者・産業界と合同で活動できるサイバー環境の整備

民間事業者・産業界が国、防衛省・自衛隊等と連携協力してサイバーセキュリティ事案に対処することを可能とするため、サイバー人材の教育、訓練、シナリオ作成、演習などを合同で実施できる環境を整備することを提言する。

その際、新たな教育・演習等システムの導入も含めて、以下の観点に留意して検討を行い、その結果に最もよく合う形で実現を図ることが適切と考えられる。

ア　システムの目的は何か
　（教育、訓練、演習、研究開発等）
イ　参加者の範囲をどこまで考えるか
　（防衛省・自衛隊、重要インフラ事業者、防衛産業、大学等）
ウ　既存のシステムとの関係をどう構築するか
　（公的なサイバー教育、演習システム、民間企業が提供するシステム等）

エ　同盟国などとの国際的な連携をどう考慮するか
オ　将来のサイバー関連技術開発のプラットフォームへの活用を念頭におくか
カ　技術や環境の急激な変化に対応するための柔軟性や冗長性をどの程度確保すべきか

3. 恒常的に顔の見える、話し合いの場の設定

今後益々複雑になることが予測されるサイバー空間の課題に対して、政府内の一層の連携が求められることは当然であるが、法的あるいは情報部門を束ねる官と技術面で強みを持つ民間企業の連携は一層重要になる。そのためにはまずはサイバー安全保障に対する経営層の理解をより高めることにより、官と民の顔の見える信頼関係を構築することが最も重要である。

その際個別の企業ではなく、前記1. に示すサイバー関連企業等の連携を担う枠組みを介し官と民の情報共有等を目的とした話し合いの場を設けることは一見当たり前で簡単なように見えるが、既存の官民の意思疎通の枠組みとの関係、その重複を回避し、また運営のノウハウや Win-Win の関係性にも考慮しつつ、システムとして「恒常的に顔の見える、話し合いの場」を設定し、これを通じて政府とサイバー関連企業全体の信頼関係を構築することを提言する。

提言Ⅱ　「サイバー安全保障」に係わる高度な人材育成（質的向上）

従来、産業界におけるサイバー人材育成は不正アクセスの防止、ウイルス侵入の排除、認証情報の窃取の防御、身代金等の搾取等からの防護という経済的損失の防止や事業継続性の確保といった視点が強かった。今後はこれらに加えて、「サイバー安全保障」という視点にたった人材の「質的向上」が重要性である。

このような優れた実践的人材育成は、主として自衛隊の「システム通信・サイバー学校（以下「サイバー学校」という）」が基礎的な教育を含めその任務を担うことになると考えるが、同時に防衛省・自衛隊の内部での育成強化に加え、従来以上に民間事業者へのアウトソーシングが求められるものと考えられる。このため、産業界においても、これに応えられるよう協力体制の強化が必要である。

特に「能動的サイバー防御」に関する政府内における検討の結果等を踏まえ、各民間事業者が提供するサイバーセキュリティ教育カリキュラムのモデル化（標準要素の整理）を図ることを提言する。

なお、教育カリキュラムの内容は自衛隊員のみでなく警察や重要インフラ事業者を含む人材の教育においても参照できるような実務性と汎用性を持たせることにより、より重層的な人材育成に資することにも配慮する必要がある。

提言Ⅲ　サイバー人材の拡充と育成環境の整備（量的拡大）

高度な人材を養成するにはそのピラミッドの裾野の拡充と人材育成環境の整備が不可欠である。そのためには教育受講の容易化、カリキュラムの要素の標準化、認証取得の共通化等が必要と考える。

前述した「サイバー関連産業界等の連携のための枠組」を中心に、主体的に以下のような組みを進めることによる国全体のサイバー人材の拡充と育成環境の整備が重要である。

1．各種能力に必要なスキルの明確化

「能動的サイバー防御」も含め、想定されるサイバーセキュリティ事案から、それへの対処に必要な各種能力を分析し、その能力に必要なスキルとその習得に必要なカリキュラム、教材、演習内容等を明確化することを提言する。

2．カリキュラムの標準要素の整理と定期的な更新を可能とする枠組みの構築

様々なサイバー事態に対応できる人員を維持するためには、サイバーセキュリティに係るスキルの分野別、機能別、レベル別の教育カリキュラムに係る標準的な要素を整理することを提言する。

同時にサイバー技術の進化やニーズの変化に合わせてそれを定期的に更新していくことを可能とする枠組みの構築を提言する。

3．国際的に整合の取れた我が国の認証制度の整備

サイバーセキュリティに関して同盟国等と共同、連携するためには、サイバー要員の能力水準を合わせることが必要であり、スキルレベルの設定とそれを習得しているという能力の認証制度があることが、組織能力の向上と組織間共同、連携の円滑化の観点から必要である。そのために国内外の能力認証制度等を参照に、我が国におけるサイバー脅威の特徴や安全保障環境などを踏まえつつ、国際的に整合の取れた我が国の能力認証制度のあり方について継続的に検討し、必要な対応を取ることを提言する。

4．サイバー職務の明確な位置付けと適切な処遇

サイバーセキュリティ能力のある貴重な人材が、有効に活用されるよう、当該職務の重要性に関して管理者や一般の理解が向上し、多くの人から正しく評価されるような環境整備が必要である。具体的には採用条件、キャリアパス、職位などで魅力のある職務とすることも重要である。特に、サイバー要員の他の職務への配置等による能

力の劣化等を回避するためには、危機管理等を含むサイバー関連職務での人事管理、サイバー人材のキャリアアップ体制を整備することを提言する。

5. 人材バンクや「リボルビングドア」的な制度の構築と交流機会の増加

サイバー人材を一定の規模で確保し続けるためには、省庁間及び民間との間で行き来を可能とする人材育成、実務経験の蓄積が必要である。そのためには安全保障に関するサイバーセキュリティ人材が官民を行き来できる「リボルビングドア」的な制度や、現状の人材の状況把握（データバンク化）を実現すること、また民間事業者・産業界においても、政府主催のサイバー演習（教育）や政府が参加する国際的な演習への一層積極的な参加など交流機会の増加を図ることを提言する。

6. e ラーニングの推進

人材の裾野を拡充するには e ラーニングが有効と考えるが、その内容は単に受講するという受け身でなく、CTF(Capture the Flag)など実践的な訓練を可能とする工夫も必要である。その対象として、官民の初級者に対する e ラーニングによる一定レベルの資格付与、あるいは過去サイバー関連業務、プログラム開発等携わった OB 等のリスキリニング等が考えられる。

そのため関連企業が e ラーニングを積極的に拡大、提供することを提言する。

結言

我々有識者会議一同は、「サイバー安全保障を円滑に確保するための人材の育成には、新たな視点にたって、民間事業者・産業界が連携・協力していくことが不可欠であると認識しており、以上の提言が速やかに実現することを願うものである。

令和5年6月30日

サイバー安全保障関連有識者会議　一同

高見澤將林（東京大学公共政策大学院客員教授）
田中　達浩（富士通システム統合研究所　主席研究員　）
谷脇　康彦（インターネットイニシアティブ取締役副社長）
三角　育生（東海大学教授　）
櫻澤　健一（日本サイバー犯罪対策センター業務執行理事）
齋藤　孝道（明治大学教授）

（注：名称は年次順）