産業サイバーセキュリティ研究会（第9回会合）
議事要旨

1. 日時・場所

日時:令和7年5月23日（金）8時30分～10時30分

場所:経済産業省 本館17階国際会議室

2. 出席者

委員　　:村井委員（座長）、田崎様(伊藤委員代理)、遠藤委員、片野坂委員、澤田委員、東原委員、渡辺委員
※欠席であった寺田委員からは書面による事前の意見提出あり。

オブザーバ:内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、警察庁、デジタル庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省、防衛装備庁

経済産業省:大串経済産業副大臣、野原商務情報政策局長、
奥家大臣官房審議官（商務情報政策局担当）、
商務情報政策局 武尾サイバーセキュリティ課長

3. 配付資料

資料1 議事次第・配付資料一覧

資料2 委員等名簿

資料3 事務局説明資料

4. 議事内容

○ 冒頭、村井座長から以下のとおり挨拶。

・ 我が国においては、デジタルトランスフォーメーション(DX)が順調に進んでおり、それによりこれまで縦割りだったものがネットワーク等により接続され、連携が進んでいるところである。このような状況だからこそ、サイバーセキュリティに関する議論は非常に重要になっている。

・ 近年、サイバーセキュリティの脅威やサイバーインシデントが活発に発生しており、発生件数の推移としても増加傾向である。このような脅威にどのように対応していくかという点については、これまで様々な法令や、政府全体の体制を整備するということを課題として議論してきたが、周知のとおり、本国会でサイバー対処能力強化法及び同整備法が成立したことにより、これまで準備してきたサイバーセキュリティに対する政府全体の体制が形になりつつあるとともに、防衛三文書のうち国家安全保障戦略に記述のあった能動的サイバー防御の実施のための 3 項目についてもそれぞれ具現化されたところである。このような状況の中で、本日お集まりいただいて議論いただけるのは大変貴重なことではないかと思う。

・ こうした背景の中で、サイバーセキュリティそのものも重要であるが、サイバーセキュリティを切り口として、我が国のデジタル環境の未来について、あるいはデジタル分野における世界に対する日本の位置づけについて議論するためにも、本日の議題は大変重要なテーマであると考えている。

○ 事務局から、資料３について説明を行った。

○ 各委員から、主に以下の意見があった（欠席委員による書面での事前意見を含む。）。

<u>中小企業を含めたサプライチェーン全体での対策強化に向けた対応の在り方</u>

- サプライチェーンにおける重要性を踏まえた上で満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組み（サプライチェーン強化に向けたセキュリティ対策評価制度）は非常に重要。企業としてサイバー空間におけるリスク評価を行うことは当たり前のことである。そのためには、成熟度の評価をする際に、定義をされる最低レベルの要件としてペネトレーションテストを実施していることを要件にするべきである。
- 弊社は多くの関連サプライヤーを抱えており、セキュリティ対策状況を調査している。ノウハウを持っている企業もいるが、他の製造業からの要求もあるなかで、どうしたらよいかわからないと回答した企業もある。弊社としても、下請法があるなかで強制力も出しにくい現状がある。したがって、サプライチェーン強化に向けたセキュリティ対策評価制度はサプライヤーに対しても有効であるため、是非協力したい。グローバル視点を持って、相互承認まで尽力いただきたい。弊社としても個別に声掛けを行っていきたいので、例えば、ウェブサイトを用意していただき、そこを参照できるようにしていただきたい。
- サイバーセキュリティは中小企業にとっても重要である。産業界へのメッセージは重く受け止めている。「経営層」「専門組織」「実務者担当者」向けとそれぞれに応じた呼びかけは非常にユニークであり、適切である。
- サイバーセキュリティの確保が課題であるが、企業側で何をすればよいか、中小企業として何をすればよいかが伝わっていない。サプライチェーン全体としてクリアにしていくことが重要である。価格転嫁の議論もあるが、セキュリティ対策の実施を第三者がチェックすることも必要となる。その際には、人材が問題になる。シニア IT 人材も活用できるのではないか。
- 企業の分類について、大企業と中小企業の 2 つで分けているが、中小企業も様々である。大手企業のサプライヤーもあれば、二次請け、三次請けの会社もある。下請法や価格転嫁の問題があり視点が変わり得るため、注意されたい。例えば、物流業界では物流手形を使わずに現金を早く支払うべきとの議論がある。きめ細やかな議論が必要となる。
- 中小企業の議論について、中小企業を更にカテゴライズすべきである。サプライチェーンの構成企業と街中の飲食店は異なる。セキュリティに必要なコストも異なる。孫会社や子会社にあたる小さなグループ会社は、親会社が面倒を見ることにもなり得る。系列化やグルーピングも考慮して、議論することが重要である。
- 中小企業の分類では、オンプレミスでシステムを構築できる企業とクラウド上でシステムが完結する企業がある。企業規模に加えて、提供側のサービスの観点からもカテゴライズができるとよい。
- サプライチェーン全体の対策強化や中小企業のセキュリティ対策は重要である。IT 導入補助金(セキュリティ対策推進枠)の要件変更についても感謝している。中小企業はセキュリティ対策の必要性を感じている一方で、コストをかけられないことに加えて、何をすればよいかからない状態である。「人材確保・育成の実践的方策ガイド」を通じて商工会議所や地域の連絡会に経済産業省が呼び掛けていくことによって、経営者にとって自分ごとなることを期待。
- ユーザーとのマッチングのハードルを下げるため、情報処理安全確保支援士のアクティブリストは非常によい取組であり、是非進められたい。また、サプライチェーン強化に向けたセキュリティ対策評価制度も是非進められたい。
- 中小企業のセキュリティ確保に向けて、個社だけでなくサプライチェーン全体での対策が必要である。中小企業のサイバーセキュリティを強化するためには、サイバーセキュリティお助け隊サービスの PR が重要である。現時点で利用件数は約 7000 件とのことで増加傾向にはあるが、中小企業が 300 万社以上いることを考えると十分ではない。引き続き議論していく必要がある。件数を追うだけでなく、広く普及を図ることが重要である。中小企業といっても、街中の飲食店から中堅企業まで、業種や企業規模は様々である。中小企業施策として、どこを対象とするのかをより明確にされたい。
- 中小企業のサイバーセキュリティ対策のレベルには格差がある。東京商工会議所が実施した DX 実態調査において、「サイバーセキュリティ対策について、十分に対策している」と回答した企業は 8 割を超えている。

一方で、対策の内容を確認すると、基本的な対策に留まっている。例えば、教育やセキュリティ診断、訓練までは行っていない場合が多い。セキュリティ対策に対する認識不足やリソースの不足がある。そもそも中小企業は自分ごととして理解していただけていないため、インシデント事例があったとしても、中小企業には響かない。サイバーセキュリティ対策は売上に貢献しないため、金銭を負担したくないとの思いがある。先述の実態調査によると、「セキュリティ対策に投資していない」と回答した企業は 6 割超であり、その必要性を感じていないとのことであった。

<u>セキュア・バイ・デザインの実践の在り方</u>

- 中国製のインバータやバッテリーから不正な通信デバイスが検出されたことをロイター通信が報じていた。日本製の製品であったとしても、部品製造者が機器やシステムを通じて、顧客の情報を入手することが可能という認識に立つべきである。また、EV についても同様である。セキュア・バイ・デザインの面からみて JC-STAR はよい制度であり、是非進めていただきたいが、どの程度広めるかが重要である。Volt Typhoon の事例では既存のアーキテクチャの脆弱性が指摘されている。また、GSMC(Global System for Mobile Communications)レベルで基地局のなりすましができるソフトがイスラエルで開発されていた。海外の製品が日本国内に入ってくる想定で、対処方法について検討すべきである。
- グローバル展開にあたって、JC-STAR と欧州サイバーレジリエンス法の相互承認がなければ状況は前に進まない。IoT 機器にとどまらず、防衛関連の製品等も関連すると考えており、自分ごととして捉えている。これからの取組に期待したい。
- 身の回りのものの多くが JC-STAR の対象になり得る。現行の制度では IoT のイメージが狭いのではないか。今の機器は、ブラウザやファームウェア、インターフェースを持っておりロボット化している。TCP/IP スタックで繋がっている。JC-STAR は重要な役割となるため、ロボットを対象外とするのではなく、海外の製品が日本に入ってくる中で、どのような通信が出ているかを確認する必要がある。JC-STAR の拡大を考える必要があるのではないか。
- IoT の領域では、戦略をもつことがとても重要であり、コミュニケーションネットワークとセットで検討することが肝要である。これは周波数アロケーションの議論にも関係し得る部分である。ロボットの定義にもよるが、オープン領域とクローズド領域の IoT は全く異なるため、目指すところを決めた上で戦略を練るべきである。そして、その目標に向けてステップ・バイ・ステップでどう進めていくべきかを検討することが重要になってくる。

<u>国際連携の在り方</u>

- 国際連携について、インド太平洋地域での米国のプレゼンス低下が予想される中、QUAD(Quadrilateral Security Dialogue)の枠組を活用しつつ、米国のエンゲージメントを高めていくことが必要である。
- 東南アジアでの日本に対する信頼が大きいなか、日本として東南アジアに対してどのような責任を持つのか、どのようなビジネス展開をしていくのかの議論は重要である。この分野の議論は英国でもなされており重要である。
- 日本企業単独でのセキュリティ確保は困難である。東京オリンピックでも 4.5 億回の攻撃が観測された。当時、SOC では 3 重構造を設けており、最奥の層までは攻撃が届かなかったものの、海外の同志国の企業とのコンソーシアムが必要なのではないか。
- 国際関係において、アカデミアの世界では悲鳴が多く聞こえる。米国国立標準技術研究所(NIST)も含めて人材削減の波がきている。日本のアカデミアは米国を頼りにしていたため、影響が大きい。
- JC-STAR について、既に英語化して発信いただいている。その他の施策に関する文書の英語化・発信についても引き続きお願いしたい。

サイバーセキュリティ産業振興の在り方

- 国内での情報セキュリティ製品市場（売上高）は、前年比約 20%増の約 5,300 億円 となった。しかしながらに外資系企業のシェアが 5 割を超えており、国内のサイバーセキュリティ製品はその多くを海外に依存している。同盟国とさらに連携しながら、高品質な国産セキュリティ製品、サービス供給を強化すべきである。
- 「サイバーセキュリティ産業振興戦略」の実現に向けて、製品・サービスのセキュリティや信頼性を確保するための制度構築についてコメントする。米国では、国家防衛やインフラ防御の際に民間事業者に対して FOCI（Foreign Ownership, Control, or Influence）規制がかけられ、サイバー空間も対象となる。IPA にも「情報セキュリティサービス審査登録制度」があるが、米国の対応に比べると弱い。脆弱性診断サービスのようなサービスが普及するよう実効性を担保いただきたい。
- 既に「サイバーセキュリティ産業振興戦略」には盛り込まれているが、国産の供給能力向上が必要である。国産製品の採用や活用を含めて方向性を示していただきたい。
- サイバーセキュリティを生業にしている企業だけでなく、製造業まで対象に広げると「サイバーセキュリティ産業振興戦略」が更に盛り上げる可能性がある。サイバーセキュリティが取り上げられる前には情報セキュリティが取り上げられていた。人の情報に関する感覚が鈍くなるとインシデントも起こり得るため、基本に立ち返りたい。
- 量子コンピュータの発展に伴い、従来広く使われている RSA 暗号が破られるリスクがある。そのため、政府主導で民間とともに PQC（耐量子計算機暗号）への移行に向けたロードマップを描くべきである。
- ロボットについて、Rapidus と絡めた戦略を検討してはどうか。市場側にはロボットのサイバーセキュリティに対するニーズはあるが、国の産業政策の戦略を担っていく主体が決まっていない。半導体とロボットがつながる大戦略をイメージしていただきたい。

サイバーセキュリティ人材の育成・確保の在り方

- サイバーセキュリティの人材強化における産官学の共通認識を持つためにも、諸外国の事例や国内の動きを参考に、政府主導で人材定義の可視化を検討すべきである。また人材定義の可視化とともに教育機関と連携する必要がある。本件は米国、欧州のフレームワーク等を大いに参考すべきである。
- サイバーセキュリティのリテラシー向上や人材育成・確保の視点から、初等教育段階から中等教育までのセキュリティ教育、民間人材の活用を行うべきである。
- セキュリティ人材の即戦力、さらにはトップ人材を広げるためには高専、大学、大学院の人材において質、量を広げる必要がある。例えば、豪州で導入しているサイバーアカデミーを参考にサイバーセキュリティを専門に学べる仕組みを検討すべきである。
- テレワークが普及し、人口減少が迫っているなか、官民一体となったセキュリティ人材の育成を一層強化していくことが重要である。
- IPA の中核人材プログラムを活用して自社内に高度専門人材を育成している企業が多いことを踏まえて、2 カ月程度の人材育成プログラムについて、引き続き検討いただきたい。
- 日本経済新聞において、情報処理技術者に「データマネジメント（管理）」の区分を追加することが報じられた。デジタル活用の人材育成を推進いただきたい。
- 中小企業のサイバーセキュリティ対策は重要であり、地方でも同様である。地方で働く方のリテラシー向上が重要であり、小学校から中学、高校までの DX 教育について、手洗い、うがいのように定着していくとよい。サイバーセキュリティや DX に力をいれるよう国に依頼している。これらの教育によって中小企業、地方が力を持ちやすくなる。

産業データ連携・基盤への期待

- デジタルエコノミーの進展に向けた取組を行っているが、データには競争領域のデータと協調領域のデータがある。協調領域におけるデータの公開が課題となっており、ユースケースを作成している。理解しやすいところとして、EU のデジタルプロダクトに係る環境データがある。材料購入から、製品製造、製品輸送までの炭素データの総量を把握する取組を行っており、このデータは協調領域のデータである。EU サイドと相互認証ができないかという話もある。全世界の CO2 排出量は 300 億トンであるが、日本国内での CO2 排出量は 10 億トンに過ぎない。アジア諸国をプラットフォームに組み込めないかを AZEC(アジア・ゼロエミッション共同体)が検討している。
- 各省庁はデジタルデータを保有している。秘密のデータもあり、守るべきものがある。プライベートなデータがあり、量もある。安全に共有するための枠組を考えていくべき。民間での取組もみられるが、デジタルデータの指令塔は政府である。データは大切なアセットであり、各省庁任せになるのではなく、デジタルデータ全体の流通を考えなければならない。データを安全に共有する時代に入った。
- 産業データスペースについて、どう進めていくか思案中である。産業界が一枚岩になろうとしており、官民の協議会を設定した上で、協議しようとしている。産業界や IPA 等も関連しており、Catena-X が進んでいるところ、GAIA-X をどのように進めるのか。サーキュラーエコノミーは社会実装の段階であるが、初期立ち上げ費用を誰が面倒みるかは決まっていない。官民協議会で検討した上で、実行は産業界でやろうとしている。競争力強化やセキュリティ確保に向けて、日本全体を俯瞰する司令塔があるとよい。
- デジタル庁がリードする構造になっているが、競争領域と協調領域を分けて、協調領域のデータをどのようにまとめていくか。公的にトラスト基盤をどのように作るかが課題。データの保証がなければ、相互接続ができない。ベースの認証が進まないと聞いているため、関係者のお力をお借りしたい。
- 産業サイバーセキュリティ研究会を日本の司令塔と位置付け、全ての問題が集約され、議論される場となるとよい。本研究会をセキュリティやトラスト人材、AI、データスペースなどの議論の集約の場とした上で、社会実装していく上での課題を検討し、各所に対策を割り振っていけるとよい。大きく捉えるべきである。
- 全体のデジタルデータをみて全体のアーキテクチャ、戦略を議論する場所が必要である。私個人としては IPA のデジタルアーキテクチャ・デザインセンターで議論すればよいと考えている。あるいはこの会議体を広げて議論するのか。是非経済産業省にも考えていただきたい。

サイバー対処能力強化法成立を踏まえた政府全体への期待

- 先日、国会でサイバー対処能力強化法及び同整備法が成立した。官民で議論がなされ、安全なサイバー空間作りの新たな一歩を踏み出している。官民連携での枠組や情報共有について、経済界の意見を踏まえたものになっている。下位法令の成立に向けて、政府とのコミュニケーションをより一層深めていきたい。中小企業に含めた企業全体に対して、サイバー安全保障における背景や国家安全保障及び経済安全保障に係る取組について丁寧かつ分かりやすい説明を経済産業省にはお願いしたい。
- 政府全体のサイバーセキュリティは進化しており、官民一体になって検討していく仕組みがあるとよい。先を見通した戦略を作るべく、一緒に検討していきたい。
- サイバーセキュリティにおいて情報は最も重要なファクターである。新たな官民連携の組織体は「give and take」の概念を念頭に、意見交換や人材交流を行い、官民での信頼関係の構築を図るべきである。
- 民間へ提供する情報は経営層の意識決定に有用な情報提供を実施すべきであり、セキュリティ・クリアランス制度も十分に活用すべきである。
- 政府側に入る攻撃に係る情報が多くなってくるため、セキュリティ・クリアランス情報等を咀嚼いただき、民側に情報共有いただけるモデルがあるとよい。
- サイバー対処能力強化法及び同整備法では、基幹インフラ事業者に報告義務を課している。窓口の一本化を

お願いしたい。機微な情報を報告することになるため、情報提供側がリスクを感じることにないようにしていただきたい。情報提供には力をいれていきたい。

- インシデント報告について、監督省庁等により、報告内容が異なり、自由記述の箇所が多く、ファイルの形式も異なる。報告フォーマットの統一に加えて、報告や集約が一元化できる仕組みを行い、効率性を上げるべきである。
- サイバー対処能力強化法及び同整備法では、官民連携強化やアクセス・無害化とともに組織体制整備が盛り込まれている。複雑なサイバー攻撃に対処するためには情報が必要であり、警察庁などの各省と緊密に連携して対応することが重要である。サイバーセキュリティ本部の下に NISC が位置付けられるが、発展的改組に伴うこれらの青写真がでていない。早急に新 NISC が稼働するようにお願いしたい。
- 新 NISC を中心に各府省庁とこれまで以上に連携すべきで、各府省庁のサイバーセキュリティ部門が物理的に同じ執務室で協働することも検討すべきである。
- 中小企業を含むサプライチェーン全体を俯瞰した政府全体での対策強化をお願いしたい。

<u>その他</u>

- 海外の政府と対話をしているとサイバー情報集約分析能力の強化が重要。IPA のサイバーインテリジェンスや、サイバーリスク情報に係る取組の強化に関し、一層加速していただきたい。
- サイバーセキュリティは防衛と同じ扱いでよいのではないか。サイバーセキュリティに関する予算を防衛費に加算してもよいと思うほどである。

○ オブザーバから、以下の発言があった。

＜飯田内閣官房内閣審議官（内閣サイバーセキュリティセンター長代理）＞

- 今回の議論の中でサイバー対処能力強化法の話題があったが、今回の法律は、官民連携、通信情報の利用及びアクセス無害化措置に係る権限が政府に付与されたということではなく、その整備法により、サイバーセキュリティに係る各省庁間の役割分担を変更し、内閣官房が司令塔機能を持つことで、集中的に判断できるような体制を整備するというものである。
- 併せて、同法では官民連携に当たっての政府の責任を強化している。官民連携について、民間の責任を強化した部分もあるが、それ以上に政府の責任を重くしたことが、同法における組織・体制整備のポイントだと考えている。
- その上で、政府側からどのような情報を民間に対して共有できるようにするのかが重要である。今回の法律に基づく権限の下で政府は通信情報の収集をしていくことになるが、収集した情報を前提に、他国からのサイバー空間上でのアプローチに関する情報を秘密として共有するのか、あるいは情報を加工した上でより広く共有するのかについて政府が判断することになるという点においても、政府の責任が非常に大きくなったと考えている。
- デジタル化が進み、かつサイバーセキュリティに係る各国間での競争がある中で、今後の状況を見通しながら官民連携について議論していくことが重要であり、その議論のプロセスでは、官民連携の具体的な成果や双方のメリットをお互いに実感できなければ、官民連携は深まっていかないと考えている。
- 2024 年 7 月に NISC における組織改編を行ったが、新組織においては、検討する前にやるべきことは直ちにやるということをモットーとしており、スピード感をもって施策を進めていきたいと考えている。
- また、サイバーセキュリティ戦略本部では、村井座長や遠藤委員にも御参加いただいた上で、サイバー対処能力強化法以外で政府として実施すべきことを取りまとめることを予定しており、検討については期限を設けて議論を進めていきたいと考えている。
- 本日御議論いただいた経済産業省の政策を取り入れつつ、NISC として政府内の方針を統一した上で、政策を

進めていきたいと考えている。
- 今後の試金石として、サイバー対処能力強化法の施行準備に向けて今夏に新組織を立ち上げた上で、同法に基づく基本方針の作成について議論していく予定である。基本方針では、官民連携の具体化やインシデント報告の一元化について、明確にする予定である。
- 次期サイバーセキュリティ戦略は、サイバー対処能力強化法の施行を念頭に置いて、官民双方でアクショナブルなものにしていきたいと思っている。
- 今後も民間の方々の意見や事業活動に沿った形での運用をしていきたいと考えており、本研究会も含めて、委員の皆さんには今後も忌憚のない意見をいただければと思う。

＜山内総務省サイバーセキュリティ統括官＞
- 今回頂戴した各委員の意見を聞き、総務省としても他人事ではなく、経済産業省と連携を進めていく必要性を改めて認識したところである。
- 2024 年末に相次いで DDoS 攻撃が発生したが、これまで DDoS 攻撃によりネットワークがダウンすることをあまり想定していなかったところ、サービスがダウンする実影響が発生することを示す事例であった。IPA が公表した「情報セキュリティ 10 大脅威 2025」においても、5 年ぶりに DDoS 攻撃の脅威がランクインしており、DDoS 攻撃の脅威の再認識が改めて注意喚起されたものと考えている。
- 本日ロボットのセキュリティに関する話があったが、本日の議論と同様に、総務省における議論においても、ロボットとは何かという線引きをどこに引くかという点が論点となっている。
- IoT のセキュリティ対策についてだが、総務省では通信事業者とともに対策を行っているため、把握の範囲としてグローバル IP アドレスの領域に限定されており、各家庭内までは及んでいない。その上で、総務省として把握できる範囲で最も課題のある IoT 機器はルーターであると考えている。
- 総務省が貢献できる最大の点は、通信やオペレーションの状況を監視できる点であり、これは JC-STAR の前提となる部分である。加えて、総務省では技術基準適合証明制度を所管している。ある製品が経済産業省の JC-STAR には適合するが、総務省の技術基準適合証明には適合しないという事態はあってはならず、両者の整合性を図る必要があると考え、実際に事務レベルで両者の整合について議論しているところである。
- また、具体的な取組の一つとして、総務省では情報通信研究機構（NICT）において、「CYNEX」事業を実施している。これは、情報通信ネットワーク観測などで得られた脅威情報を収集・蓄積・分析し、これをセキュリティ製品開発における検証・評価に活用いただくテストベッド機能を提供するものである。経済産業省の「サイバーセキュリティ産業振興戦略」とも連携しながら、多くの企業に御活用いただきたいと考えている。
- 総務省では、トラストサービスの基盤として、タイムスタンプ及びｅシールのサービスを提供している。特にｅシールについては、米国ではニーズが下がっているが、欧州では留学の際に eIDAS に適合した卒業証明・在学証明の提出が求められており、総務省として対応すべく制度を創設し、データの安心安全な流通基盤の構築に取り組んでいる。
- PQC（耐量子計算機暗号）についても重要であり、経済産業省及び IPA とも一層の連携しながら、対策を進めていきたい。

○ 最後に、大串経済産業副大臣から以下のとおり挨拶。
- 社会全体のデジタル化（DX）の推進や、AI、量子技術といった技術の高度化の影響で、サイバー空間を通じた攻撃のリスクがますます高まっているところである。足元においても、基幹産業の業務停止や情報漏洩など、目に見える形でサイバー攻撃が発生しているところである。
- このようなサイバー攻撃は、無差別に行われるものもあれば、国家的な背景を持つ組織から執拗に攻撃を受ける場合もあり、国家の安全保障を考える上でサイバーセキュリティはこれまで以上に重要なものになってきていると認識している。

・ こうした背景を踏まえて、政府においても欧米主要国と遜色のない、あるいはそれ以上のサイバーセキュリティ対処能力を発揮すべく、今国会においてサイバー対処能力強化法案及び同整備法案を提出し、2025 年 5 月 16 日に成立したところである。これらの法の成立及び施行により政府のサイバーセキュリティに関する司令塔機能が強化され、能動的サイバー防御を実施する体制が整備されることとなる。経済産業省としては、この新たな司令塔組織のもとで関係省庁と連携しながら、中小企業を含めた産業界に向けた政策を企画・実行することによって、我が国全体としてのサイバーセキュリティの強化、そしてサイバー安全保障の確保に貢献していく所存である。

・ 本日の研究会では、企業のセキュリティ対策水準の可視化、サイバーセキュリティお助け隊サービスなどをはじめとする中小企業向けの支援策の拡大などのサイバーセキュリティ全体での対策強化に向けた取組、IoT セキュリティ適合性評価制度である JC-STAR の政府調達への要件化、セキュア・バイ・デザインの実践に向けた取組、IPA における経済インテリジェンス収集能力の強化など政府全体でのサイバーセキュリティ対応体制の強化に向けた取組、政府機関等による有望なスタートアップ製品・サービスの積極活用などのサイバーセキュリティ供給能力の強化に向けた取組などについて、新しい政策の方向性を提案したところである。

・ 本日頂戴した御意見を踏まえて、さらなる取組のブラッシュアップを進めていく所存である。その上で、産業界においても政府の政策の方向性に沿って積極的な取組を行っていただきたく、サイバーセキュリティに対する投資を中長期的な企業価値向上に結び付けることや、サプライチェーン全体での対策強化に向けた中小企業向け政策の積極的な活用を取引先に促すことなど、産業界の各主体に積極的に取り組んでいただきたい事項について、産業界のメッセージとして昨年に引き続きお示ししたところである。本日御参加いただいている皆様には、産業界を代表する立場として本メッセージを広く展開いただき、政府の施策の代表的なユーザーとして、各組織における積極的な取組を促されたい。

以上