資料12－3

構成員からの御意見

総務省　サイバーセキュリティ統括官室

タスクフォース構成員へのアンケート

（問）新たな総合対策を策定するに当たって、以下の４つの観点から、現状、政府として取り組むべきサイバーセキュリティ上の課題とお考えの点について（具体的なものを複数挙げていただいても結構です）御意見、コメント等をいただければと思います。

---

① 民間企業等におけるセキュリティ対策の推進

② 研究開発の推進

③ 人材育成の強化

④ 国際連携の推進

① 民間企業等におけるセキュリティ対策の推進

- ✓ IoTや政府・重要インフラのサイバーセキュリティ対策などは既に議論されている通り非常に重要なテーマではありますが、一方、小規模事業者に対する対策は10年前と比較してもさほど進んでいる状況ではなく、「セキュリティ格差」が実は非常に深刻なものとなっています。小規模事業者は、人、モノ、金、情報が圧倒的に不足しており、近年はサプライチェーン上のリスクになってきている状況にも関わらず事実上は何もしていないというのが実態で、国の政策でもいくつかの試みがありますが実際の所はほぼ変化が無いという状況です。民間のセキュリティベンダーも、利益が薄くリスクが大きい事からほぼ何も施策を打っておらず、もう一歩踏み込んだ政策が必要であると感じています。【鵜飼構成員】

- ✓ 接続サービスを提供する電気通信事業者に対し、利用者（企業ユーザー、コンシューマーを含む）が希望する場合には、当該電気通信事業者のゲータウェイで行う不正通信検知等の提供サービスを充実させるよう働きかけるべき。【岡村構成員】

- ✓ 民間企業等がポジティブなインセンティブを持てる仕組み作り：　政府調達等において「サービス品質」の最優先項目として「セキュリティ品質」を配置し、積極的に推進すべき。【後藤構成員】

① 民間企業等におけるセキュリティ対策の推進

- ✓ レッドチーム活動の普及支援： APT10等の高度で執拗な攻撃が増加しており、リスクベースのセキュリティ対策の重要性が指摘されているが、日本企業の多くはリストベースのセキュリティ対策からリスクベースのセキュリティ大対策に移行が出来ず、脅威に対する適切な対策が取られていない可能性がある。金融業界では「脅威ベースのペネトレーションテスト」（以下、「TLPT」）が普及しつつあり、APT対策に向けた取り組みが始まっている。通信・放送等の重要インフラ事業者においても、TLPTなどのレッドチーム活動により、リスクベースのセキュリティ対策を加速させる必要がある。TLPTなどのレッドチーム活動の普及は、企業等の意識改革が必要であり、国が牽引すべき分野である。TLPT実施に関するガイドライン等を作成し、普及促進をお願いしたい。
  https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf
  【小山構成員】

① 民間企業等におけるセキュリティ対策の推進

- ✓ 日本版SHODAN/Censysの実現に向けて： IoTセキュリティ対策については、NOTICEプロジェクトが開始され、大きな第一歩が踏み出された。この取り組みを「民間企業等におけるセキュリティ対策の推進」に繋げるために、NOTICEプロジェクトやICT-ISACの調査で得られた信頼できる情報を、検索可能なデータベースとして構築し、企業等が自社のIPアドレスレンジを検索して対策に役立てる「日本版SHODAN/Censysの実現」が有効である。また、IoT端末の脆弱性情報について、海外メーカー等の脆弱な機器などの情報についても、ユーザ企業やセキュリティ対策を行う組織で共有できる仕組みを、（日本版SHODANの付加価値として）、NOTICEプロジェクトの第二段目の取り組みとして検討をお願いしたい。【小山構成員】

- ✓ あらゆるものにコンピューターが入り込むようになった現代、これまで以上に製造する側に安全志向が必要。とはいえコストにシビアな現場ではコスト圧力によって作るモノの安全性がなおざりになる可能性が高い。これをそうさせないような制度が必要ではないか。また、プラットフォームやデータ収集の仕組みが生まれたとき、収集するデータの意図した、意図しない汚染などからの保護が必要となるが、データセットの認証やデータのサプライチェーンの保護を促進する仕組みが必要ではないか。同時に「個人情報」の保護にも繋がる。【園田構成員】

① 民間企業等におけるセキュリティ対策の推進

- ✓ IoT時代を鑑み「セキュリティバイデザイン」の考えを、各IoT機器を製造する過程から意識することが重要。【戸川構成員】
- ✓ 個々の民間企業における攻撃解析の高度化（自動化も含む）【中尾構成員】
- ✓ インフラセクター組織間で連携するセキュリティ対策の推進【中尾構成員】
- ✓ 全国規模のCSIRT機能の統合化の推進―NICT成果の活用推進【中尾構成員】
- ✓ やや乱立気味の情報共有コミュニティ（ISAC、NCA、警察、サイバーセキュリティ協議会、その他のコミュニティ等）から共有、サイバーセキュリティ専門会社から調達（購入）、及び公然情報から収集する各種セキュリティ関連情報（サイバー脅威インテリジェンス情報、レポート、IOC等）を、セキュリティ対策やインシデント対処等のためにうまく使いこなせていない状況が散見されるため、セキュリティ関連情報のNeed-to-know原則に基づく配布・蓄積・抽出（クエリ）・分析・出力（レポート）の仕組み及び実務能力の獲得・向上をする必要がある。【名和構成員】

① 民間企業等におけるセキュリティ対策の推進

- ✓ 「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」の施行は、大きな一歩と思われるが、次のステップとしては米国の情報セキュリティ情報共有法のように、「自己のネットワークを安全に維持するのはネットワーク管理者の責務である」との義務付け（そのための権限付与を含む）の方向に進むべきである。【林構成員】

- ✓ 【セキュリティのセミナーなどに来ていただけない中小企業の経営層の方々の啓発が課題】中小企業のセキュリティ対策については、これまでも多くの施策が講じられてきたところですが、継続した取り組みが必要と考えます。特に、専任のセキュリティ担当者を持つのが難しい小規模企業等について、いかにして経営層の皆様に関心をもっていただくかについて、十分な議論と実践が喫緊の課題だと思います。セキュリティ単独の講演やセミナーに来ていただくのは難しいかもしれませんが、他の興味を持っていただけそうなテーマと一緒に、セキュリティの話を聞いていただくなど、新たな工夫を考えるとよいのではないでしょうか。【藤本構成員】

② 研究開発の推進

- ✓ 高齢者世帯が増える中、コンシューマー家庭向けの、電気通信回線の入り口に接続可能なセキュリティ機能オールインワンボックス開発を推進すべき。【岡村構成員】

- ✓ サービスサプライチェーンにおけるデータセキュリティ確保の研究開発：　複数かつグローバルなサービス事業者にまたがる「サービスのサプライチェーン（クラウド等）」におけるデータセキュリティ確保（素性確認からトラストの伝搬、バックトレース、他）は、将来の重要課題。【後藤構成員】

- ✓ AIのサプライチェーンのセキュリティ確保：　今後、AIモデルの軽量化が進み、複製の痕跡を隠蔽することが容易なることが懸念される。重要な知的財産であるAIモデルを、複製・窃用から守る手法の確立することが重要課題。【後藤構成員】

② 研究開発の推進

- ✓ DevOpsやDevSecOpsに対応した研究開発と人材育成のエコシステム：Society5.0向けクラウド利用を前提にソフトウェア開発の内製化が進展し、DevOpsやDevSecOpsの取り組みがDXなど安全安心なデジタル社会の実現に不可欠なものになっていく。また今後のイノベーションやDXはクラウド環境を利用したDevOpsやDevSecOpsの取り組みの中で多く生まれると想定され、同時にセキュリティ対策はPCやデバイスやクラウド上のアプリなどをエンドエンドで守る必要性が増してくる。このためセキュリティの研究開発や人材育成も、新しいイノベーションの流れに適応し、過去の仕事のやり方を変えていく必要がある。【小山構成員】

- ✓ ①に関連して、秘密分散のようなデータそのもの、あるいはデータサプライチェーンの保護の仕組みを研究開発、実装していく必要がある。敵性AI、新たなインフラ、プロトコルを対象とする攻撃技術の研究開発（当然それを上回る防御、検知技術の研究もするが）。それを社会として健全に研究できる環境整備。法律（ウイルス作成罪など）の改定が必要ではないか。研究者が萎縮して、その間海外にどんどん遅れを取る（アカデミー、コミュニティのカンファレンスを見ていると中国の存在感が非常に大きくなっている）。【園田構成員】

② 研究開発の推進

- ✓ 昨今の米国や欧州の動向を見ても、ハードウェアセキュリティあるいはチップセキュリティについて、比較的早期の研究開発が必要。【戸川構成員】
- ✓ 攻撃・攻撃予兆の把握のための研究開発【中尾構成員】
- ✓ 攻撃挙動の高度分析の研究開発(オフェンシブセキュリティも含む)【中尾構成員】
- ✓ セキュリティ対策自動化技術の研究開発【中尾構成員】
- ✓ 暗号基盤の危殆化に備えた基盤技術の研究開発【中尾構成員】
- ✓ Trustシステム構築のための研究開発【中尾構成員】
- ✓ 今後の新たな応用（サービス等）に向けたセキュリティ研究開発（新たな応用における脅威・リスク分析のための検証基盤、検証技術の研究開発を含む）【中尾構成員】

② 研究開発の推進

- ✓ 公的機関やセキュリティ関連企業からサイバー演習の参加機会の提供が行われているが、一つの組織から参加する人数が限られており、それぞれの組織の内情から乖離したシナリオを経験することが多い。そこで、自組織（自治体を含む）で独自に実施しようと考えても、サイバー演習の企画・計画・準備・実施・評価・まとめ（分析）・報告にするにあたっての参考となる文献が非常に少ない。欧米では、公的機関がサイバー演習のノウハウに関する情報、文献、さらには、即時利用可能なテンプレートまで無料で公開されているため、日本でも、サイバー演習の準備・実施・評価に関する知識体系を文献化するための研究開発を推進する必要があると考える。【名和構成員】

- ✓ de factoあるいはconsortium型で標準化が進むと思われるので、その流れに乗り他国をリードできるよう、民間を支援する。【林構成員】

- ✓ 【組織間連携などによる事業開発やサービス提供におけるセキュリティ確保の手法の研究が課題】たとえば、IoT機器の設計開発やAIを活用したサービスなど、多くのケースは組織間で連携して実施されています。その場合のセキュリティ確保が、効果的・効率的に行われるために必要な方法論等の研究が必要と考えます。【藤本構成員】

② 研究開発の推進

- ✓ 世界的にネットワーク探索による情報収集が進む現状から、ネットワーク探索（IoT機器等の発見と脆弱性調査含む）技術の高精度化・効率化、ネットワーク探索に対する防御技術、ネットワーク探索と連動した攻撃の検知、分析技術などを高度化する必要がある。【吉岡構成員】

- ✓ 5Gの本格化を迎え、これを悪用したサイバー攻撃がさらに強力となる可能性があることから、これを想定した対策技術の検討が必要。【吉岡構成員】

- ✓ これまでの様々な対策、施策の効果を測定する技術に関する研究開発が必要。【吉岡構成員】

③ 人材育成の強化

- ✓ CISOを担当できる人材を育成するため、技術面、関連制度面、マネジメント面の総合教育の場、認定資格を作るべき。【岡村構成員】

- ✓ 長期的な人材育成の仕組み作り：　組織文化の改革（上記①）につながる人材の育成は最も時間を要することを認識した人材育成策を推進すべき。経営層の世代交代を含めた組織全体の意識改革のためには四半世紀（25年）を要する。この25年の間に、セキュリティを経営リスクとして的確にとらえ、組織全体をリードする経営者を育成するためには、その素養とともに次世代の経営層を育成する社会的な仕組みが必要。それを25年は続けることにより、社会全体を変革していく長期的な施策が必要。現在進めている人材育成の大部分は短期的な取り組み（即戦力の人材）。これは2020オリパラなど、直近の課題を解決するために重要であるが、経営層と実務層（即戦力）との意識の乖離などの課題を抱えているため、平行して上述のような長期的な取り組みが必要。【後藤構成員】

- ✓ 特に研究開発はDevOpsやDevSecOpsの現場に密着した取り組みを、人材育成はDevOpsやDevSecOpsで競争力ある人材の育成を行うべきであり、セキュリティのエコシステムを支える研究開発と人材育成の在り方について、産業横断的な取り組みを推進していただきたい。【小山構成員】

③ 人材育成の強化

- ✓ 日本サッカー協会のようなライセンス＋研修制度を構築し、優秀なコーチを輩出する必要がある。セキュリティに限定せずIT全般として、IT＋セキュリティが必要な現場に両方できるエンジニアを多数送り込む。
  https://www.jfa.jp/about_jfa/organization/databox/coach.html
  サッカーの登録選手数は90万人、フットサル入れても95万人。エンジニアとしてはもっと欲しいはず。
  https://www.jfa.jp/about_jfa/organization/databox/player.html
  一流の講師、トレーナーを呼ぶのにはそれなりの待遇が必要。政府が絡む場合は現状そこに限界があるので、民間事業化や連携など別な仕組みが必要。
  コーチが日常的に働ける場として、大学等にポスト＝予算が必要では？
  【園田構成員】

- ✓ 情報系学生にとって「セキュリティ」というキーワードは，比較的魅力のあるものだと思われる。産官学が一体となって，さらにセキュリティに明るい人材を育成する施策があっても良い。【戸川構成員】

③ 人材育成の強化

- ✓ 引き続き官民における情報セキュリティ人材の育成の推進（例　NICTが実施中の「CYDER」）【中尾構成員】
- ✓ セキュリティマネジメント人材とセキュリティ技術人材の融合化の推進【中尾構成員】
- ✓ 大学と企業との連携によるセキュリティ教育の強化促進【中尾構成員】
- ✓ 先端的技術の獲得を目指した海外組織との連携促進（研究者の派遣等）【中尾構成員】
- ✓ サイバーセキュリティに関する技術、運用、行動という観点での人材育成は、さまざまな領域で行われているが、同種の教育プログラムが乱立している。しかし、サイバー空間に対する状況認識を網羅的かつ時系列的に把握・分析・報告（展開）するような人材は、他国に比べて極端に少なく、その教育プロクラムも存在しない。多くの領域で、技術に長けたセキュリティ人材が、その専門領域からアクセス可能な情報を収集したものが展開されているような状況がみられる。これを改善しないと、サイバー脅威の広がりに比例して、想定外の領域が拡大していく恐れがある。サイバー空間の状況認識の能力を高める努力を重ねている米英などの支援を仰ぎ、この領域の人材育成に着手する必要があると考える。【名和構成員】

③ 人材育成の強化

- ✓ 企業経営層においてもサイバーセキュリティの重要性の認知度が高まっており、かつてのように人材の絶対的不足を嘆く時代ではなくなりつつある。IoT人材をゼロから育成するよりも、わが国の製造業には優秀な人事がいるので、彼らにセキュリティ・マインドを植え付けることが得策と思われる。【林構成員】

- ✓ 【地域における戦略マネジメント層人材の育成が課題】たとえば、5Gでは、さまざまなユースケース、利用シナリオが検討され、今後進展がみられると思いますが、その際に”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役割”を果たす戦略マネジメント層人材の存在は必要不可欠だと思います。すでに「新世代モバイル通信システム委員会」のもとに「ローカル５G作業班」が設置され技術的条件などの検討が始まったところですが、セキュリティ確保に必要な人材育成についても取り組みを進めていく必要があると考えます。【藤本構成員】

④ 国際連携

- ✓ 日本のサイバーセキュリティベンダーとして海外進出を検討した際、他国と比べても国からの支援を受けることが困難でした。JETROにも協力を仰ぎましたが、最終的にアメリカのVCを紹介され、そこから先の企業へは繋がりませんでした。他国は大使館等の支援を受けビジネスマッチング等を行い、日本に進出してきていました。結果、自らの足で現地のイベント等に赴き、一つ一つのブースを回るという効率的でない手法を取らざるを得ませんでした。日本企業の海外進出には政府の積極的な支援が必要です。【鵜飼構成員】

- ✓ 世界無線通信会議（WRC:World Radiocommunication Conference）に対し、無線通信の標準化について、さらにサイバーセキュリティの観点を導入すべき旨を、日本発の提案として述べるべき。【岡村構成員】

- ✓ 多様な国際連携の仕組み作り：　現状、国としての国際連携が、特定国（や組織）に集中している状況と認識。国際連携では、相手国や相手組織が限定（集中）しないように、多様な連携ルートを持つことが重要。このために、産官学のそれぞれのルートでの長期的なコミュニケーションの仕組み作りと維持と、多様なルートでの連携状況を集約できるような国内会合（または組織）作りを進めるべき。【後藤構成員】

④ 国際連携

- ✓ 国際連携を推進する法制度のありかたについて： サイバーセキュリティ対策で国際連携は重要な取り組みであるが、国内は「通信の秘密」が課題となって、国際的な取り組みに足並みを揃えられる状態にはない。例えば各国が連携し成果を上げている「ボットネットのテイクダウン」についても、日本国内では限定的な取り組みにとどまっている。インターネットは１つであり、自国のサイバー攻撃対策は他国のセキュリティの向上と不可分である。通信事業者等が他国と同様のセキュリティ対策を行い、デジタル社会の安心安全に貢献するために、法制度はどうあるべきか、中長期的な取り組みのロードマップについて、議論をお願いしたい。【小山構成員】

- ✓ 国際連携は非常に重要。2020や2025に向けて、いかに国際的な枠組みを作っていくかは重要な課題。【戸川構成員】

- ✓ 日本と海外のセキュリティ先進国との研究連携の促進（マッチングファンド等）【中尾構成員】

④ 国際連携

- ✓ 海外組織との連携による研究成果の国際標準化推進【中尾構成員】
- ✓ 国際的なISAC連携の強化、推進【中尾構成員】
- ✓ 脅威、インシデントなどの情報共有やその活用を国際レベルで円滑に推進するための枠組み、体制の構築【中尾構成員】
- ✓ アジアの国や地域におけるサイバーセキュリティの取り組みを眺めるとバラツキが大きいように感じるが、個人ベースでは国や地域に関係なく、非常に素晴らしいサイバーセキュリティの研究や運用を推進している。しかし、それをアジア全体で横断的する拠点は少なく、部分集合的な形で複数存在している印象である。そこで、2019年及び2020年にかけて日本が経験する大規模イベントで発生するであろうサイバー攻撃に対する対処経験を集約し、アジアに展開するような学術・運用共同拠点（CoE: Center of Excellence）の設置と複数にわたる段階的な機能拡大をする必要があると考える。【名和構成員】

④ 国際連携

- ✓ 5Gをはじめとした先端技術における国際競争は、貿易管理や調達戦略など、安全保障と密接な関係を持ちつつ展開されている。こうした国際感覚を前提に、個別の判断に誤りなきを期す必要がある。【林構成員】

- ✓ 【国際標準化の取り組みに関する現状の把握と計画的推進が課題】研究開発成果の利用拡大のためにも国際標準化に関する取り組みは重要性を増していると考えます。総務省における施策全体について、セキュリティに関連する国際標準化に関する取り組みの現状を把握し、必要に応じて支援強化などの検討が有用と思います。【藤本構成員】

- ✓ 「② 研究開発の推進」でも触れたネットワーク探索や攻撃の検知は国内のみで実行していても効果が限られる。日本にはNOTICEなど世界的にも例のない活動とその経験がある。一方、海外でも様々なIoTセキュリティ対策が進んでいることから、これらの情報共有、連携した活動をさらに活発化すべき。【吉岡構成員】

⑤ その他

- ✓ IoTは主体なのか、客体なのか、それとも両方の性質を持つ第三の存在なのか、に関する論点を整理し、議論の場を設定する。AI ネットワーク化検討会議の議論（2016年）が、原点かと思われる。【林構成員】