(ア) 重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

- 事務局の**プレゼンテーションに対する意見交換**は主に以下のとおり。

（高度な攻撃に対する支援・情報提供）

- **情報共有はレジリエンス力を高める上で最も重要**。経営者、実務者、アナリストといった階層ごとに適切な情報を提供することが必要。**近年の攻撃は単純なインディケータ情報の共有では検知や対策が困難**になってきており、脅威ハンティングの過程で入手した、より高度な情報（マルウェアのふるまいに関する情報など）の共有が重要
- **クリアランスがあると海外との連携、官民の情報共有が行いやすくなる**。**最大活用を考えてほしい**
- **被害企業から情報を報告してもらうには、インセンティブの設計が大事**。**政府が情報を受け取るだけでなく、率先して情報を示していく**姿を見せるべき
- 現状ではJPCERT/CC、IPA、警察、経済産業省等のそれぞれの観点があることは理解するが、**有事においてはワンボイスで情報発信をすることが重要**
- ISAC（注　業界内の情報共有枠組み）の中でも取組が進んでいるものと、そうでないものがある。**ISAC間のノウハウ共有を政府が支援してはどうか**

（ソフトウェア等の脆弱性対応）

- 豪州では、重要インフラの**資産情報を予め登録させることで、登録情報と適合した脆弱性情報が速やかにフィードバックされる仕組み**となっており、こうした仕組みは迅速な共有を実現する**自動化の取組の一つ**だと考えている
- 米国で**悪用が認められた脆弱性（KEV)がカタログ**として公表されているが、**日本やアジアでのみよく使われているソフトウェアの情報**は掲載されない。このような脆弱性情報を、**日本語で発信することが大事**ではないか
- 情報の共有・流通については、**どういう情報を流通させるかというソースについての整理が必要**。情報の吸い上げ先として、まずベンダが重要であるが、どのようなアライアンスを組むことができるのか、検討が必要

テーマ別会合「官民連携」（第１回）　議論の概要

（政府の情報提供・対処支援を支える制度）

- **行政へのインシデント報告は、これまで監督省庁**へ行われてきたが、セキュリティ担当者のリソースの不足から**リアルタイム性が損なわれる可能性**がある。**報告先の一元化を含めて工夫してほしい**
- 報告を行う被害企業の負担を考慮すると、報告先の一元化に加え、**報告フォーマットの統一化も必要**ではないか
- **事業者に負担をかけずに効率的に情報収集し、フィードバックする仕組みが重要**。サイバー攻撃の情報共有は数分、数十分程度で行う必要があるため、**迅速性**が重要。その鍵は**自動化**であり、自動化は**効率化にも寄与**する
- 非重要インフラについて、海外の事例等も参考に、**ソフトウェアベンダ、防衛産業、重要製造業など、特に重要な者**に対しては、**報告の義務化**などを適用しても良いのではないか
- **提供された情報の取扱いについては、明確な規律が必要**。情報を提供する民間企業側から見ると、他の企業への提供や公表など、提供してからどのように使われるかの予測が立たないと、怖くて出せない

（サイバーセキュリティ戦略本部の機能強化）

- サイバーセキュリティ戦略本部に、一般的な政策立案や助言だけでなく、**事案発生時に、司令塔として関連省庁に指示を出す役割が求められるのであれば、有識者の関わり方を含めて、構成の在り方を検討すべき**ではないか

（重要インフラにおける分野横断的な対策基準）

- **実効性確保には、行政が達すべきと考える水準を基準、ガイドラインとして示し、誘導する**とともに、遵守の実効性を担保するため、**認証、資格、遵守状況の公表など、実効性の高い仕組み**を考えていくことが重要ではないか
- 重要インフラを定義するにあたっては、その役割を踏まえた**優先順位付けや、分類方法を検討するべき**ではないか

テーマ別会合「官民連携」（第１回）　議論の概要

（人材の育成・確保）

- **CISOの位置づけを組織でより重要視していくべき**ではないか。CISOを置くことで組織のセキュリティが強化されるとともに、CXO（経営幹部）の一員になれるという意味で、魅力的なキャリアパスを提示することになる
- デジタルに強い人材は、アプリ開発などに進むことが多いので、**サイバーセキュリティ人材をどう魅力的に見せるかが重要**
- 海外では**産学間の人材の流動性が高く**、日本でも、民間の優秀な人材が大学に来て、さらに専門的な能力を身につけるといった流れが進むと良いのではないか。また、日本でも実績はあるが、より広く一般に周知されることで、人材の流れができるのではないか
- 官民の人材の流動化を進めるうえでは、制度面や給与面だけでなく、**サイバーセキュリティを現場で担う人材のインセンティブが重要**であり、サイバーセキュリティを担当する人達に対してヒアリングを行い、それを集約して政策に活かすことも重要ではないか
- 人材育成については、**非技術者の巻き込みも重要**であり、コンピュータサイエンスに携わる者以外にも活躍の場があることを伝えることで、サイバーセキュリティの層は厚くなるのではないか

（中小企業の対策強化）

- 企業によっては、情報共有を行う内容を調査する能力がない（ログが残ってない、監視体制がない）こともあるので、その**調査ができる人材育成が必要**であると同時に、**調査を支援する必要**があるのではないか
- **首都圏とそれ以外でサイバーセキュリティに対する意識が大きく異なる**ので、そこを埋めるための取組が必要ではないか