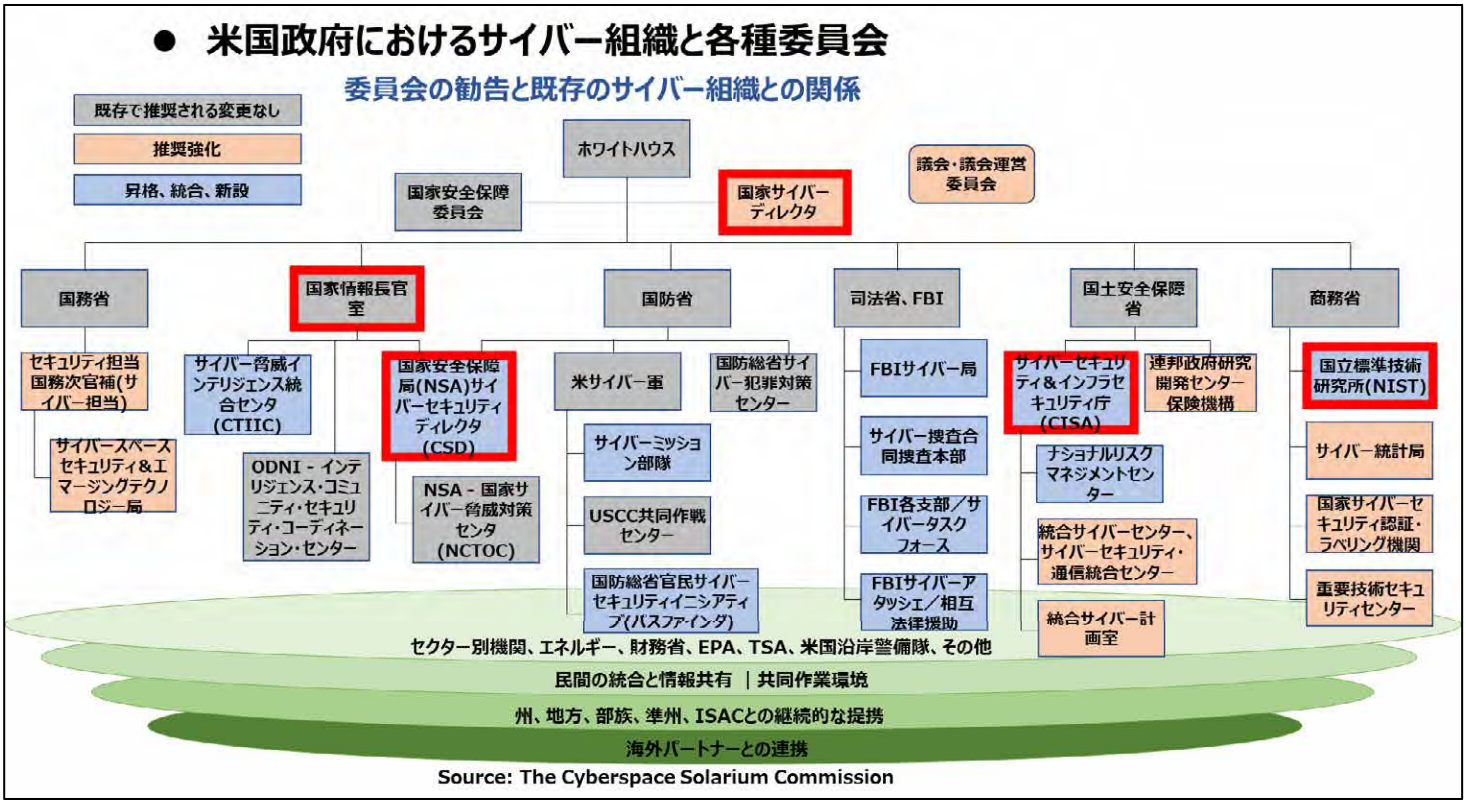

図 1-2-a 米国政府におけるサイバー組織と各種委員会

米国のサイバー防衛能力の構成要素と簡素化して図 1-2-b に示す。ポイントは 3 点である。

- ホワイトハウスのもとに、ナショナル・サイバー・ディレクターを配置する。本ナショナル・サイバー・ディレクターは、各省庁に横断的に指揮するための司令塔の役割を担う。
- 国家情報長官と国防長官のもとに、国家安全保障局（National Security Agency, NSA）とサイバー・コマンドを配置する。NSA/サイバー・コマンドは、有事にならないように平時からの情報収集や事前の実行部隊となるための役割を担う。
- サイバーセキュリティとインフラ・セキュリティ・エージェンシー（Cybersecurity and Infrastructure Security Agency, CISA）のもとに、ジョイント・サイバー・ディフェンス・コラボレーティブ（Joint Cyber Defense Collaborative, JCDC）を配置する。JCDC は、政府機関ネットワーク・オペレーターや、民間企業ネットワーク・オペレーターとの情報共有や調整のための役割を担う。

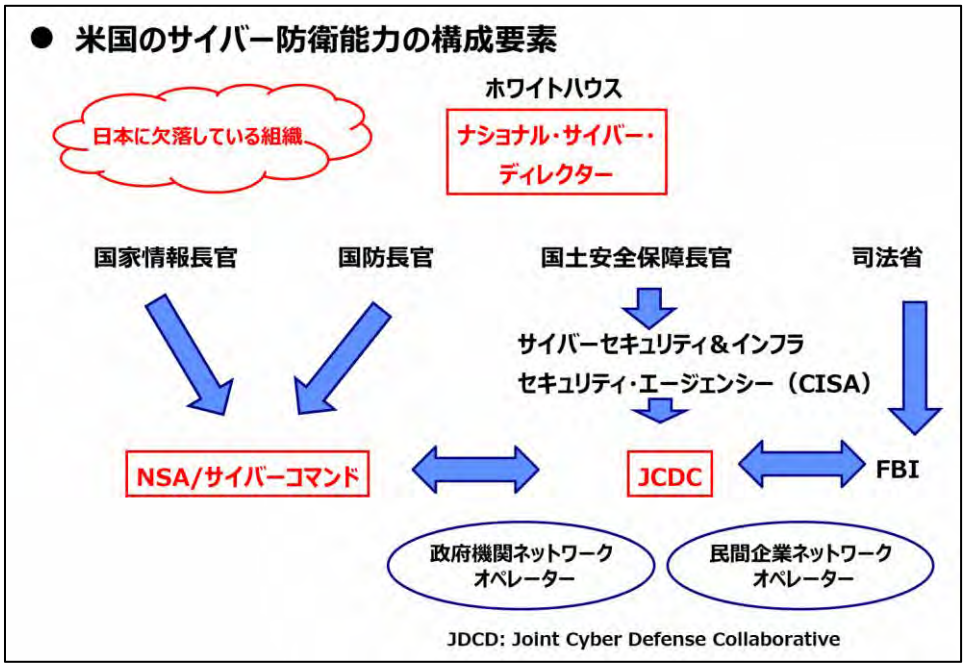

図 1-2-b 米国のサイバー防衛能力の構成要素

日本とのイコールフッティングにおいて、日本に欠落している組織が「ナショナル・サイバー・ディレクター」「NSA/サイバー・コマンド」「JCDC」の 3 つである。

第３節 日本のサイバー防衛能力

日本の省庁の強みと弱みをまとめる。弱みを下線に示す。

内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity, NISC）は、ポリシーや脅威アラートを提供するが、政府機関や民間企業に対するサイバーセキュリティの運用権限はない。また、タイムリーな運用情報を提供しない。さらに、海外との接続が遅く、弱い。

デジタル庁は、政府ネットワーク（防衛省を除く）を集中的に提供しているが、運用上のサイバーセキュリティに関する指令は出せない。

警察庁は、国内のサイバー犯罪を起訴し、児童ポルノ、ATM 窃盗、ランサムウェアなどの国際的なサイバー犯罪についてはインターポールを通じて活動している。

日本におけるサイバー防衛の活動は、憲法解釈と通信規制が日本のネットワークの積極的な防衛を阻んでいる。

米国の NSA や英国の GCHQ（Government Communications Headquarters）に匹敵するサイバー情報機関が日本にはない。防衛省は、サイバー担当者を 800 人から 5,000 人に拡大する計画を発表した。ただし、防衛省は現在、外国のネットワークに侵入する権限を持っていない。

日本の民間企業の強みと弱みをまとめる。弱みを下線に示す。

民間企業では、脅威に対する認識が広まっている NTT ドコモ、ソフトバンク、KDDI などの通信事業者は、ネットワークセキュリティが充実している。JPCERT や ISAC が設置されている。

経済産業省の産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）が、発電所、工場のスタッフに優れたトレーニングを提供し、 米国とのつながりも深い。

三菱電機、NEC といった日本の大手企業が深刻な情報漏えいに見舞われた。中小企業は非常に脆弱である。

日本のサイバーセキュリティ分野は、必要性の大きさに比べて、僅かである。日本では CERT や ISAC といった連携した脅威対応の仕組みが遅れている。

日本のサイバー防衛能力をまとめると図 1-3-a に示す評価となる。多層的なサイバー抑止の評価として、1 番目の行動規範の形成、2 番目の便益の非提供、3 番目のコストの強要のうち、日本の目標は 3 番目のコストの強要であるのに対して、日本の現状は 1 番目の行動規範の形成にありこれから 2 番目の便益の非提供にさしかかるところである。

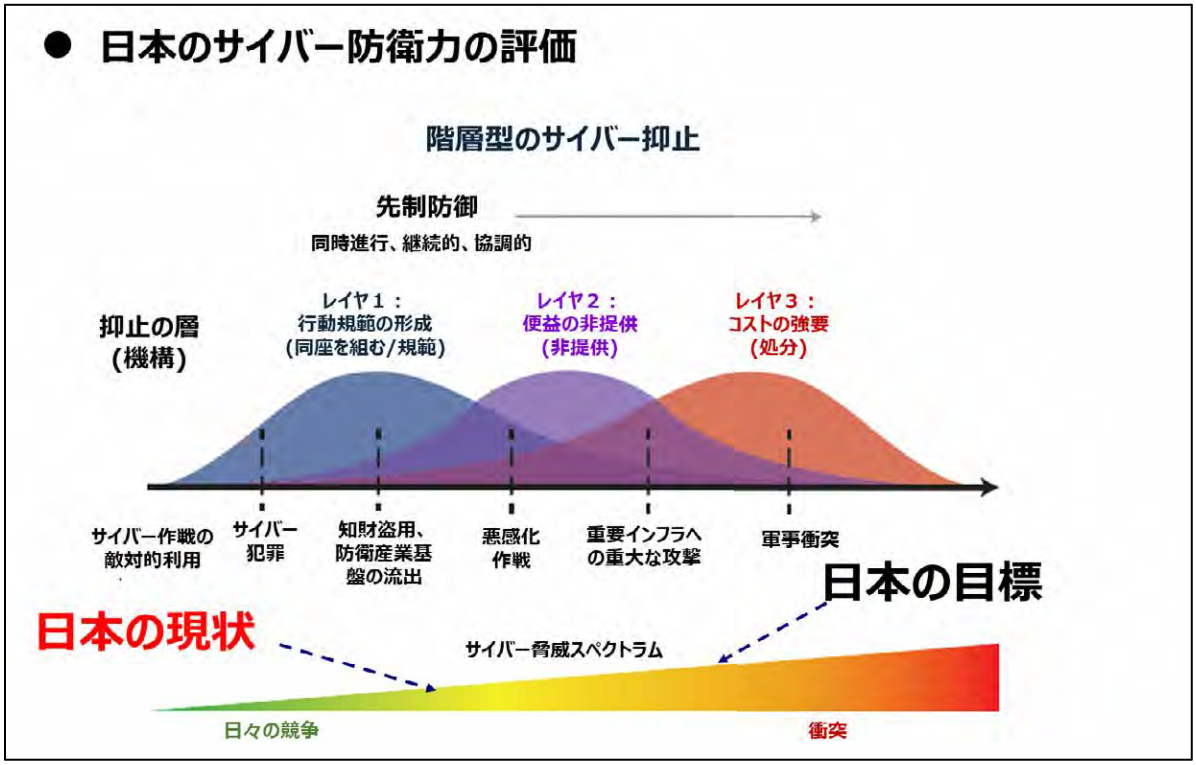

図 1-3-a 日本のサイバー防衛力の評価

第４節 日本のサイバーセキュリティ開発の次のステップ

日本のサイバーセキュリティ開発の次のステップをまとめる。

- 海外と互角なサイバーインテリジェンス機関の設立
  - セキュリティクリアランス制度
  - 出発点 - GCHQ 程度の規模（スタッフ 6,000 人、予算 20 億ポンド） https://www.gchq.gov.uk/

- NISC と JDA（Japan Defense Agency）のどちらの機関が、政府ネットワークのサイバー防衛に関する指揮を執るかを決定する
  - 指揮を執ることが決まった機関への指示権限の付与

- 政府・民間のオペレーションセンターの設立
  - 米国 JCDC（Joint Cyber Defense Collaborative）と同等の機関
  - サイバーセキュリティに責任を持つすべての主要な政府機関を含む
  - 主要な通信事業者を含む
  - 主要なインフラ事業者に拡大する

- 外国のネットワークに侵入するための憲法解釈と法的権限を与える

- 国家サイバー担当大臣を設置
  - 内閣総理大臣の直属の部下
  - 少人数のスタッフ
  - 政府および民間ネットワークにおけるサイバーセキュリティの向上と、脅威への対応の統括を行う

米国情報報告書の 4 分の 3 は、NSA によるものと言われている。サイバーインテリジェンス機関の設立は必須である。さらに、外国のネットワークに侵入することは、ウクライナ経験から導かれたものである。

これらステップを進める上では、日米同盟におけるサイバー防衛のカウンターパートの整備も行う（図 1-4-a）。まず、日本のナショナル・サイバー・ディレクターを新規に置く。つぎに、日本のサイバーインテリジェンス機構を新規に置く。さらに、NISC GSOC や、日本のナショナル CERT、デジタル庁の権限付与と再組織化を行う。

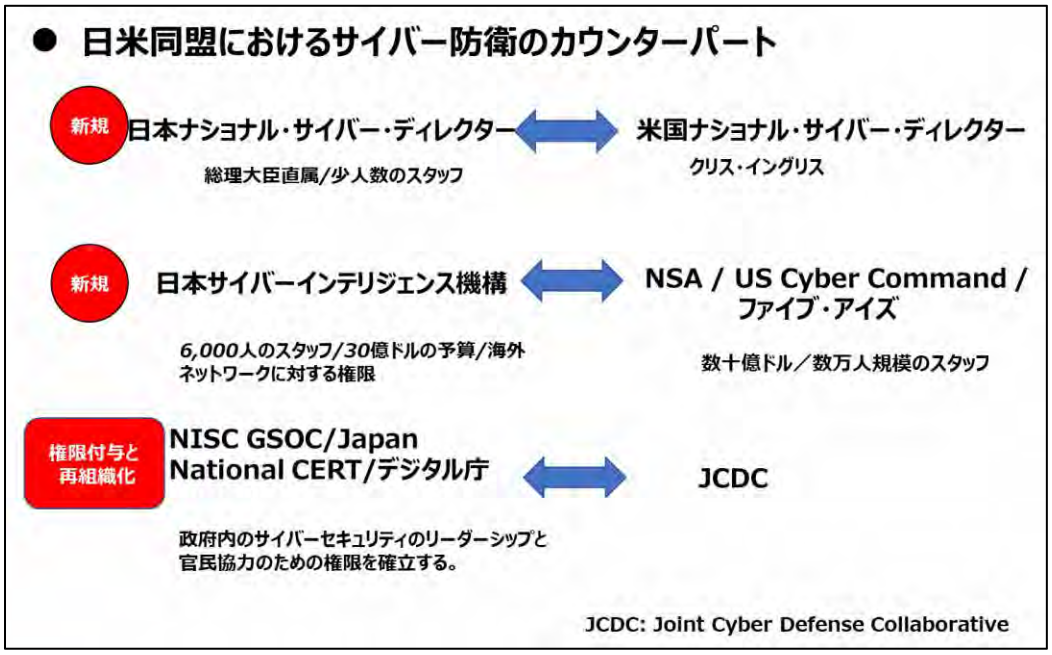

図 1-4-a 日米同盟におけるサイバー防衛のカウンターパート

第５節 国家サイバーインテリジェンスの全体像

日本はサイバーインテリジェンスに貢献できるなら、歓迎される立場にある（図 1-5-a）。そのためには、サイバーインテリジェンスシステムで、クローズド・ソース・インテリジェンスを生み出せること、他国に give できることが必要である。

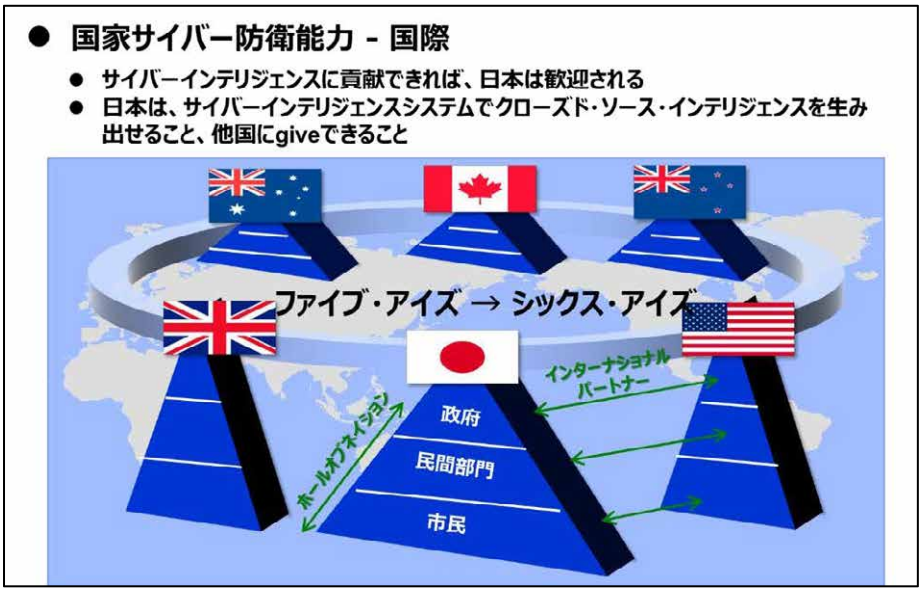

図 1-5-a 国家サイバー防衛能力の国際的な連携

国家サイバーインテリジェンスの全体像を図 1-5-b に示す。国家サイバーインテリジェンスは、大きく４つの階層「政府」「重要インフラ」「民間企業」「住民」で構成する。

「政府」階層では、国家サイバーインテリジェンスセンターを設け、本センタが、民間、防衛、警察を含むトータルな意味での司令塔の役割を担う。本センタは機能として、省庁横断的に、脅威/リスク分析、インシデント追跡、対処協調、インシデント調査、サイバーセキュリティ状況認識、標準整備を行う。さらに、本センタは国際パートナーとの窓口となる役割も担う。さらに以降に述べる、重要インフラ、民間企業、住民の階層における CERT/CSIRT とも連携を行う。

「重要インフラ」階層では、各セクターに設置される CERT/CSIRT が、セクターごとの脅威/リスク分析、インシデント追跡、対処協調、インシデント調査、サイバーセキュリティ状況認識、標準整備を行う。セクター間の連携を行うとともに、前述の政府の階層の CERT/CSIRT とも連携する。

「民間企業」階層では、民間企業や自治体のそれぞれに設置される CERT/CSIRT が、民間企業および自治体それぞれの脅威/リスク分析、インシデント追跡、対処協調、インシデント調査、サイバーセキュリティ状況認識、標準整備を行う。民間企業どうしや自治体どうしの連携を行うとともに、前述の政府の階層の CERT/CSIRT とも連携する。

「住民」階層では、官民連携としての情報共有センタ、情報共有組織、学会、市民社会が脅威/リスク分析、インシデント追跡、対処協調、インシデント調査、サイバーセキュリティ状況認識、標準整備を行う。住民の階層どうしの連携を行うとともに、前述の政府の階層の CERT/CSIRT とも連携する。