サイバーセキュリティ対策

－人材対策を中心に－

主席研究員　田村　賢吾

目　　次

要旨

サイバー攻撃の件数は増加の一途を辿っている。

本稿は、サイバーセキュリティ対策の中で、大きな課題となっているサイバーセキュリティ人材不足の対策を中心に取り上げている。

まず、わが国政府や行政が主導しているサイバーセキュリティ対策を概観した上で、サイバーセキュリティ人材対策の現状と課題を説明した。

次に、米国の連邦政府を中心としたサイバーセキュリティ対策および同国のサイバーセキュリティ人材対策の状況を説明し、わが国の課題解決策のヒントを探っている。

米国では、サイバーセキュリティ人材の流動化に向けたインフラが用意され、人材の需給ギャップを解消する動きが進められている。また、人材不足についても本格的な取組が進んでいる。また、これらを容易にしているのは、多様なサイバーセキュリティ人材のスキルを標準化したNICEフレームワークの存在である。

わが国においても、米国の例などを参考に、国や行政等が主導したサイバーセキュリティ人材の流動化や人材育成を官民連携で推進する体制構築が望まれるとともに、各企業においては自前での人材育成を計画的に進める必要が強まってきていると考える。

なお、補足資料には、各国機関において広く採用されているNISTフレームワークについて説明している。現在検討中の改訂版では、サイバーセキュリティ対策の投資有効性の検証に同フレームワークを活用していくという方向性が示されている。ご参考とされたい。

１．はじめに

インターネットを経由した情報通信技術の発展等に伴い、サイバー攻撃の件数は増加の一途を辿っている。

特に、国家の安全保障にかかわる機密情報や、防衛、原子力プラント、交通、医療、金融決済システムなどの重要な設備に対しての攻撃は、我々の安全を脅かす重大なリスクとなっている。

また、IoT による各種情報端末が幅広く展開するようになり、情報端末を踏み台とした攻撃など、リスクが多様化する中で、サイバー攻撃による重要設備の運用停止などのリスクが顕在化した場合の影響は以前にも増して大きくなっている。

わが国でも 2015 年 1 月からサイバーセキュリティ基本法が施行され官民を挙げた対策が進められているところであるが、2020 年に開催される東京オリンピック・パラリンピックに関連し、関係する施設などやわが国に向けたサイバー攻撃がさらに増加するとの予測も示されている。

このような状況の中で、民間企業においてもサイバーセキュリティ対策の重要性が増しているが、対策の実効性を挙げるには、これを支える人材の確保が必要である。

経済産業省によると、わが国のサイバーセキュリティ対応人材は、2020 年に約 19 万人不足[1]すると予測されている。国家、行政に限らず、広く民間企業においても対応人材の確保・育成が大きな課題となっているが、解決に向けての定量的なシナリオが描けていない状況にある。

本稿は、このサイバーセキュリティ人材不足の対策を中心に取り上げることとした。

また、サイバーセキュリティ対策の策定において多くの国や機関で参考としているのは米国国立標準技術研究所（NIST）のフレームワークである。現在、このフレームワークは設定以来、初めての改訂が進められており、本稿の補足資料として、同フレームワークの概要と改訂動向を紹介した。

なお、本稿における意見・考察は筆者の個人的見解であり、所属する組織を代表するものではないことをお断りしておく。

２．わが国のサイバーセキュリティ対策の現状

サイバーセキュリティ対策は、官民連携での対応が必要[2]であり、サイバーセキュリティ人材対策を推進する上でも同様である。そのため本項ではわが国政府や行政が主導するサイバーセキュリティ対策を説明し、さらにサイバーセキュリティ人材対策に焦点を当て説明する。

---

1 後記 2.（2）参照。

2 サイバー攻撃の一部は国家主導で仕掛けられ、官民連携での対応が不可欠である。国家主導による攻撃としては、例えば、米国は複数の国家に対し、サイバー攻撃を主導していると名指しで非難してきた。最近では、2017 年 12 月に北朝鮮の関与を断定し、わが国もこれを認めている。

（1）サイバーセキュリティ体制

インターネットの急速な利用拡大など、わが国でのIT化が進展する中で、不正アクセスやコンピュータウィルスなど情報セキュリティ対策への必要性から、2000年2月、内閣官房に「情報セキュリティ対策推進室」が設置され、国家施策としてわが国のサイバーセキュリティ対策が始動した。

その後、わが国のサイバーセキュリティ対策についての責務と必要な施策を推進するためにサイバーセキュリティ基本法（以下「基本法」）が2014年11月12日に公布され、2015年1月9日に施行された[3]。

a. サイバーセキュリティ基本法による推進体制と施策

基本法の趣旨は、従来、行政機関ごとに行われていたサイバーセキュリティ対策を、一定の権限を持った機関で統合的に掌握して予防策の始動や効果的なインシデント対策を行うことであり、内閣官房長官を本部長とした「サイバーセキュリティ戦略本部」（以下「戦略本部」）を設置、さらに、その事務局として、「内閣サイバーセキュリティセンター」（NISC）を設置し各行政機関のセキュリティ対策を評価、監視、必要に応じ勧告等を直接行えることとしたものである。

戦略本部を中心としたサイバーセキュリティ推進体制は図表1のとおりである。

基本法に則り、戦略本部はサイバーセキュリティ戦略案の作成および実施推進を行うことが求められ、重要インフラ、研究開発、普及啓発・人材育成等の項目において検討を進めてきた。

また、同本部は重大なインシデントの評価、省庁横断的計画等での総合調整等を行うこととされ、さらに、内閣の高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）および国家安全保障会議（NSC）と緊密に連携をとることが求められている。

その後、戦略本部が策定した「サイバーセキュリティ戦略」は2015年9月4日に閣議決定されている。

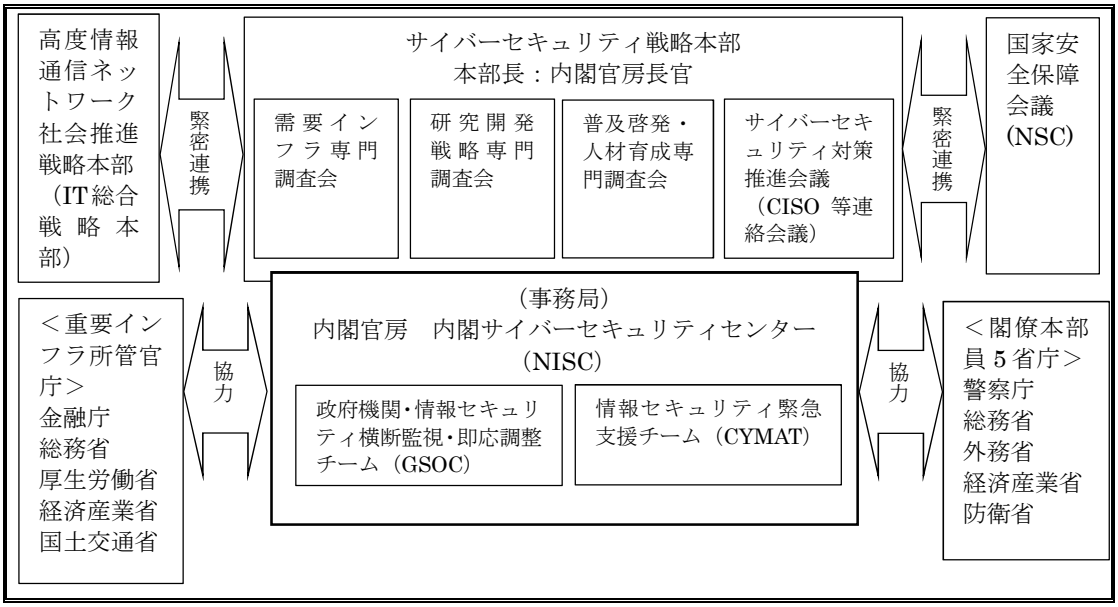
図表2は、同戦略において目的達成のための施策として挙げられた項目である。

この中で、特に民間企業と関係があるのは、①の経済社会の活力の向上および持続的発展である。セキュリティマインドを持った企業経営の推進とは、セキュリティリスクの把握とセキュリティ機能の実装の推進、セキュリティ人材の育成、組織能力の向上等を図ることであり、特に経営層の意識改革、サイバーセキュリティ人材の育成および組織能力の向上を求めている。また、④の横断的施策の中では、国内でサイバーセキュリティに関する業務に従事する技術者が、質的にも量的にも圧倒的に不足しており、人材育成は喫緊の課題であるとし、各種教育段階や職業能力開発に加え、人材の発掘・育成・

[3] その後、基本法は2016年10月21日に一部改正施行されている。主な改正ポイントは、国が行う不正な通信の監視、監督、原因究明調査等の対象範囲の拡大およびサイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）などに委託することである。

確保および人材活躍のための環境整備等を求めている。

図表 1　わが国のサイバーセキュリティ政策の推進体制



（出典：NISC 資料をもとに作成）

図表 2　サイバーセキュリティ戦略の項目

①経済社会の活力の向上および持続的発展
- 健全な IoT システムの創出
- セキュリティマインドを持った企業経営の推進
- セキュリティに係るビジネス環境の整備

②国民が安全で安心して暮らせる社会の実現
- 国民・社会を守るための取組
- 重要インフラを守るための取組
- 政府機関を守るための取組

③国際社会の平和・安定およびわが国の安全保障
- わが国の安全の確保
- 国際社会の平和・安定
- 世界各国との協力・連携

④横断的施策
- 研究開発の推進
- 人材の育成・確保

（出典：内閣府資料をもとに作成）

b. 内閣サイバーセキュリティセンター（NISC）

内閣サイバーセキュリティセンター（以下「NISC」）は、サイバーセキュリティ戦略において、重要インフラ所管官庁[4]とも連携し、各種ガイドライン[5]を公表しているが、

[4] 「重要インフラの情報セキュリティ対策にかかる第 3 次行動計画」（2014 年 5 月 19 日情報セキュリティ政策会議決定、2015 年 5 月 25 日サイバーセキュリティ戦略本部改訂）にて、金融庁、総務省、厚生労働省、経済産業省、国土交通省の 5 省庁を重要インフラ所管官庁（前記 a.図表 1 参照）と位置付けた。

[5] NISC が策定したガイドライン等には、本項で説明したものの他、主なものとして次が挙げられる。
・情報セキュリティ研究開発戦略

その中で、特に民間における対策推進を示しているものについて概要を説明する。

(a)「企業経営のためのサイバーセキュリティの考え方」

本ガイドラインは前記 a.のサイバーセキュリティ戦略を受け、2016 年 8 月 2 日に NISC が公表したもので、経営層に期待される 2 つの基本的認識と 3 つの留意事項を示している（図表 3 参照）。

なお、本ガイドラインは、後記 c.(a)ア.のサイバーセキュリティ経営ガイドラインとの併用を勧めている。

図表 3　企業経営のためのサイバーセキュリティの考え方の基本的認識等

基本的認識
①サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある ②全てがつながる社会において、サイバーセキュリティに取り組むことは、社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる
留意事項
①情報発信による社会的評価の向上 セキュリティ対策を品質向上等に有効な経営基盤の１つとして位置づけるとともに、その取組について各種報告書等を活用して情報発信することが必要である ②リスクの１項目としてのサイバーセキュリティ 経営判断の基準の１つとして、サイバーセキュリティをリスク管理の 1 項目とし、経営者がリーダーシップをとって取り組む必要がある ③サプライチェーン全体でのサイバーセキュリティの確保 サプライチェーンに参画している関係者のなかで、一部でもセキュリティ対策が不十分であれば、自社の重要情報が漏えいするなどのリスクが高まる。そのため、サプライチェーン全体でのサイバーセキュリティ確保が必要である

（出典：内閣府資料をもとに作成）

(b)「サイバーセキュリティ人材育成プログラム」

本ガイドラインは前記 (a) の「企業経営のためのサイバーセキュリティの考え方」を受け、2017 年 4 月 18 日に公表したものである。

本ガイドラインは企業におけるサイバーセキュリティ人材に係る課題とそのあり方を検討して策定されたものであり、詳しくは、後記（2）a.にて説明する。

c. 各省庁の対応

ここでは、重要インフラ所管官庁のうち、民間企業に関係のある経済産業省、総務省および金融庁の対応を説明する。

(a) 経済産業省

・情報セキュリティ普及啓発プログラム
・安全な IoT システムのためのセキュリティに関する一般的枠組

ア．「サイバーセキュリティ経営ガイドライン」

経済産業省と独立行政法人情報処理推進機構（IPA）は、2015 年 12 月 28 日に「サイバーセキュリティ経営ガイドライン」を公表[6]した。このガイドラインは、IT に関するシステムやサービス等を供給する企業および経営戦略上 IT の利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため策定されたもので、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3 原則」（図表 4 参照）および経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）[7]に指示すべき「重要 10 項目」（図表 5 参照）をまとめている。

図表 4　経営者が認識する必要がある「3 原則」

原則 1：経営者は IT 活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
原則 2：自社はもちろんのこと、系列企業やサプライチェーンのビジネスパートナーIT システム管理の委託先を含めたセキュリティ対策が必要
原則 3：平時および緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

（出典：経済産業省資料をもとに作成）

図表 5　経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」

①サイバーセキュリティリスクの認識、組織全体での対応の策定
②サイバーセキュリティリスク管理体制の構築
③サイバーセキュリティ対策のための資源（予算、人材等）確保
④サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
⑤サイバーセキュリティリスクに対応するための仕組みの構築
⑥サイバーセキュリティ対策における PDCA サイクルの実施
⑦インシデント発生時の緊急対応体制の整備
⑧インシデントによる被害に備えた復旧体制の整備
⑨ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策および状況把握
⑩情報共有活動への参加を通じた攻撃情報の入手とその有効活用および提供

（出典：経済産業省資料をもとに作成）

イ．サイバーセキュリティ対策のフレームワーク構築

経済産業省は 2017 年 12 月に産業サイバーセキュリティ研究会を設置し、サイバーセキュリティ対策のフレームワーク構築を開始した。

2017 年度に業態横断的なフレームワークを構築し、その後順次、各業態の基準を策定していくとしている。

---

[6] 同ガイドラインは、2017 年 11 月 16 日に改訂されており、本稿はこの改訂内容を反映している。

[7] CISO とは、Chief Information Security Officer の略であり、組織内で情報セキュリティを統括する責任者を指す。

（b）総務省

総務省は、「IoT サイバーセキュリティアクションプログラム 2017」[8]に基づき、2017 年 10 月 3 日に同省のサイバーセキュリティタスクフォースが取りまとめた「IoT セキュリティ総合対策」を公表した。

本総合対策は NISC が公表した「安全な IoT システムのためのセキュリティに関する一般的枠組」を踏まえるとし、脆弱性対策に係る体制整備、研究開発の推進、民間企業等におけるセキュリティ対策の推進[9]、人材育成の強化および国際連携の推進を具体的施策として挙げている。

その中で人材育成の強化については、若手セキュリティ人材の育成の促進および IoT セキュリティ人材の育成が挙げられ、人材の育成は中長期的に取り組む必要があること、また、通信分野のみならず、各分野において広く IoT セキュリティを担うことができる人材の育成が必要であり、IoT スキルを獲得するための教材作成や研修制度の整備等総合的な対策を産官学の連携により推進するための環境整備が必要であるとしている。

（c）金融庁

ア．「金融分野におけるサイバーセキュリティ強化に向けた取組方針」

金融庁は、2014 年 11 月に基本法が成立したこともあり、金融分野へのサイバー攻撃の脅威に対抗すべく今後取り組むべき方針を明らかにし、保険会社を含む金融機関、金融サービス利用者および関係機関と問題意識を共有するため、2015 年 7 月に 5 つの方針からなる「金融分野におけるサイバーセキュリティ強化に向けた取組方針」を公表した（図表 6 参照）。

これらの方針の中で各保険会社の取組等に関して特に重要と思われる①と④について説明する。

図表 6　金融分野におけるサイバーセキュリティ強化に向けた取組方針

①サイバーセキュリティに係る金融機関との建設的な対話と一斉把握
②金融機関同士の情報共有の枠組みの実効性向上
③業界横断的演習の継続的な実施
④金融分野のサイバーセキュリティ強化に向けた人材育成
⑤金融庁としての態勢構築

（出典：金融庁資料をもとに作成）

[8] 同プログラムは 2017 年 1 月に公表されたもので、IoT/AI 時代に対応したサイバーセキュリティの確立に向け①サイバーセキュリティタスクフォースの開催、②IoT 機器セキュリティ対策の実施、③セキュリティ人材育成のスピードアップ、④総務大臣表彰制度の創設、⑤国際連携の推進からなる。

[9] 民間企業等におけるセキュリティ対策推進のひとつとして、総務省は 2017 年 12 月に情報開示分科会を設置した。同分科会で 2017 年度中に企業がサイバー対策を外部に公表する際の指針を策定するとしている。

（ア）「サイバーセキュリティに係る金融機関との建設的な対話と一斉把握」

方針①について、金融庁は、金融機関等のサイバーセキュリティ管理態勢がより実効性のある優れた取組となるよう建設的な対話を重ねるとしている。この一環として、全ての金融業態・金融市場インフラに対してアンケートも活用した実態把握を実施し、業態ごとの課題を分析する。この結果は、対話等を通じて金融機関等にフィードバックし、自己点検等に繋げていくとしている。

実態把握の調査項目[10]は対処のステップ毎に示されているが、これはNISTのフレームワークの項目に倣っている。なお、NISTフレームワークの概要は、本稿末尾の補足資料を参照願う。

（イ）「金融分野のサイバーセキュリティ強化に向けた人材育成」

方針④については、サイバーセキュリティ強化には、技術担当者だけでなく、経営層およびこれを支える管理部門の職員も、同セキュリティに関する意識と一定の知見を有することが望まれる。

そのため、セミナー等の開催や関係者と連携したサイバーセキュリティ人材の育成策についての検討（キャリアパス、バックグラウンドを含む適性等）を進めるとしている。

イ．「保険会社向けの総合的な監督指針」

金融庁は、基本法の施行等を踏まえ2015年2月13日に「保険会社向けの総合的な監督指針」を一部改正し、情報セキュリティ管理に関する項目を追加した（図表7参照）。

図表7　保険会社向けの総合的な監督指針の主な追加ポイント

①代表取締役がサイバーセキュリティ事案の未然防止および発生時の迅速対応を経営上の重大な課題と認識し、態勢整備しているか ②情報セキュリティ管理に関する方針の策定、態勢整備、PDCAによる継続的な改善、重要情報の管理、セキュリティ教育等が行われているか ③サイバーセキュリティ管理に関する取締役会等による必要な態勢の整備がされているか、また、サイバー攻撃に備える多層防御等、被害拡大防止、システムの脆弱性対策、適切な認証方法、不正防止策、コンティジェンシープランの策定およびサイバーセキュリティに係る人材の育成、拡充の計画の策定や実行がされているか

（出典：金融庁資料をもとに作成）

（2）サイバーセキュリティ人材対策

経済産業省の予測では、わが国の情報セキュリティ人材は2016年の時点で約13万

[10] 調査項目は、①特定、②防御、③検知、④対応・復旧、⑤サービス提供の状況、⑥顧客への働きかけの6区分である。

人が不足し、2020 年にはその不足は約 19 万人まで拡大する[11]としている。

また、日本銀行が金融機関向けに行ったアンケート[12]では、サイバー攻撃対応に係る企画要員が不足している機関は 65.2%、サイバー攻撃対策を整備・推進する上での課題として、人材確保・育成をあげた機関は 24.1%で同質問の第 1 位という結果であった。

このような状況の中で、わが国のサイバーセキュリティ人材の育成等の対応[13]がどのように行われているか概要と課題を説明する。

a. 概要

(a) 「サイバーセキュリティ人材育成プログラム」

本プログラムは、戦略本部が 2017 年 4 月 18 日に公表[14]したもので、現状と課題認識は次のとおりである。

- ○ 脅威は更に深刻化、専門性を高める取組等一層の充実が必要。
- ○ IT の利活用により、新しい価値を創造するビジネスイノベーションと一体となったサイバーセキュリティへの取組が必要。ビジネスの各役割の中で、サイバーセキュリティ全体を俯瞰でき、関連するサイバーセキュリティを実践できる人材の育成が必要。
- ○ ビジネスイノベーションを生み出せるサイバーセキュリティ人材の育成が必要。また、セキュリティに対する意識を若年層から高めることが必要。

取組としては、需要（雇用）と供給（教育）の好循環の形成が必要であり、需要側は、経営層の意識改革、供給側は、橋渡し人材層の配置および人材の量的拡大と質的拡大が必要であるとの方針が示され、図表 8 の各層ごとに、IT の利活用により新たな価値を創造するために必要なサイバーセキュリティ人材育成が示されている。

---

11 経済産業省「IT 人材の最新動向と将来推計に関する調査結果」（2016.6）。なお、前記（1）a.のサイバーセキュリティ戦略では、独立行政法人情報処理推進機構（IPA）の 2013 年 5 月の試算結果を紹介し、国内の情報セキュリティ従事者は約 26.5 万人であるが、必要なスキルを有する人材は 10.5 万人強に留まり、16 万人あまりの人材は教育等が必要である。また、潜在的に約 8 万人のセキュリティ人材が不足している状態としている。

12 日本銀行金融機構局「サイバーセキュリティに関する金融機関の取り組みと改善に向けたポイント」（2017.10）

13 このほか、金融情報システムセンター（FISC）は、2018 年 3 月をめどに金融機関が IT 人材を確保・育成していく上で指針とするべき手引書を作成する予定であり、その中で、サイバーセキュリティ人材の対応についても単独で取り上げる予定としている。

14 前記（1）b.（b）参照。

図表 8　サイバーセキュリティ人材育成の新たな取組

需要（雇用）
○経営層 　サイバーセキュリティを実務者層だけの問題ではなく経営問題として捉えるとともに、新たな価値の創造という「挑戦」に付随する「責任」としてサイバーセキュリティに取り組むという意識改革を図る
供給（教育）
①橋渡し人材層 　経営層・実務者層のコーディネーターにとどまらず、ビジネス戦略と一体となってサイバーセキュリティの企画・立案を行い、実務者層を指揮できる橋渡し人材層の育成に取り組む ②実務者層 　情報セキュリティ技術に関する知識・能力の向上だけでなく、チームとなってサイバーセキュリティを推進するための人材育成に取り組む ③高度人材（高等教育段階を含む） 　高度なセキュリティ技術の専門性を持ちつつ、ビジネスイノベーションを創出する高度人材の育成に取り組む ④初等中等教育段階 　児童生徒の情報活用能力（プログラミング的思考や情報セキュリティ、情報モラルを含む）を培う

（出典：NISC 資料をもとに作成）

（b）産業サイバーセキュリティセンター

経済産業省は、2017 年 4 月に、独立行政法人情報処理推進機構（IPA）に「産業サイバーセキュリティセンター」を設置し、重要インフラや産業基盤分野におけるセキュリティ強化に向けた事業を進めている。

この中核事業の一つとして、セキュリティ人材育成事業が位置づけられている。

同省は、情報系システムから制御系システムまで、システム全体を想定した模擬プラントを設置し、企業等でセキュリティ対策の中核を担う人材がホワイトハッカー[15]や研究者とともにシステムの検証や演習を実施し、セキュリティ対策の中核人材を育成する[16]と説明している。

2017 年度実施のプログラムは図表 9 のとおりである。

図表 9　産業サイバーセキュリティセンター2017 年度実施プログラム

①中核人材育成プログラム 　自社システムの安全性･信頼性を客観的に評価し自社のサイバーセキュリティ戦略の立案や経営リスク･財務リスク等を含めた自社内幹部への説明ができること等を到達目的とした研修プログラムで、1 年程度のトレーニングを行う ②短期プログラム 　CEO、CIO、CISO、部門長等、責任者クラス向けの各テーマで短期間のトレーニングを行う

（出典：経済産業省資料をもとに作成）

[15] ホワイトハッカーとは、コンピュータやネットワークに関する高度な知識や技術を持つ者を指す呼び名である「ハッカー」のうち、特にその技術を善良な目的に活かす者のことを指す。なお、元来、「ハッカー」という呼び名には行いの善悪に関する意味は含まれていない。

[16] 経済産業省の平成 29 年度予算成果目標で、本事業は重要インフラ事業者等において、サイバーセキュリティの総合的な戦略立案を担う人材を毎年 100 人程度育成するとしている。

（c）資格制度の新設

経済産業省は従来から、情報セキュリティ担当者向けの国家資格として「情報セキュリティマネジメント試験」[17]を設けていたが、同省は基本法の成立を受け、サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、サイバーセキュリティ対策の調査・分析・評価やその結果に基づく指導・助言を行う担当者のための新たな国家資格として「情報処理安全確保支援士」を新設し、2017 年 4 月から試験を実施している。

b. わが国における課題

わが国のサイバーセキュリティ人材の不足状況と、前記ａ.の現在の対策を照らし合わせると、課題として挙げられるのは、圧倒的な人材不足数に対して、定量的かつ具体的な解決策が示されていない点である。

前記ａ.の戦略本部のサイバーセキュリティ人材育成プログラムは、民間企業のサイバーセキュリティ人材不足解決のために示され、サイバーセキュリティ人材について、質・量ともに拡充すべきという方向が示されているが、2017 年 4 月の公表以来、現在までのところ決め手となる解決策はいずれの省庁からも示されていない。例えば、産業サイバーセキュリティセンターにおいても、当面の中核人材育成目標は毎年 100 人程度[18]に過ぎない。

サイバーセキュリティ人材の流動化や教育訓練など、官民を挙げての対策が示される必要があると考える。

３．米国のサイバーセキュリティ対策の現状

米国では、クリントン大統領時代の 1993 年に重要インフラ防護に対する物理・サイバー攻撃に関する取組が開始され、さらにオバマ政権発足時からは、サイバーセキュリティ確保は国家の安全保障に関する重要課題と位置付けられ、大統領令等によって、図表 10 のとおり政策が発表・実行されてきた。

本項では、このオバマ政権発足後のサイバーセキュリティ政策について説明する。米国でのサイバーセキュリティ政策は、官民連携も進んでおり、特に民間企業に関係する機関等について全体像を概説する。

17 「情報セキュリティマネジメント試験」および「情報処理安全確保支援士」は独立行政法人情報処理推進機構(IPA)が試験実施を担当する。
18 注 16 参照。

図表 10　米国における主なサイバーセキュリティ政策の経緯

時期	政策等
2008 年 1 月	○包括的全米サイバーセキュリティ・イニシアチブ（Comprehensive National Cybersecurity Initiative：CNCI）
2009 年 5 月	○サイバー空間政策レビュー（Cyberspace Policy Review：CPR）
2013 年 2 月	○重要インフラのサイバーセキュリティ強化に向けた大統領令（大統領令 13636 号および大統領指令 21 号）
2015 年 4 月	○サイバー攻撃に関する金融制裁措置指示の大統領令（大統領令 13694 号）(注 1)
2017 年 5 月	○連邦政府のネットワークおよび重要インフラのサイバーセキュリティ強化に関する大統領令 (注 2)

（注 1）サイバー攻撃等の不正手段を行った組織等に対し、金融制裁の発動を可能としたもの。

（注 2）トランプ政権下において初めて発出されたサイバーセキュリティに関する大統領令。オバマ政権が推進したサイバーセキュリティ政策の方向性を変えるものではなく、サイバーセキュリティ強化に向けた改善策が示されている。

（出典：各種資料、ウェブサイトをもとに作成）

（1）サイバーセキュリティ政策

オバマ大統領の政権第 1 期である 2009 年 5 月には、前政権が策定した包括的全米サイバーセキュリティ・イニシアチブ（Comprehensive National Cybersecurity Initiative：CNCI）[19]の見直しを含むサイバー空間政策レビュー（Cyberspace Policy Review：CPR）[20]を公表した。その後、同政権第 2 期では、重要インフラ保護の立法に向けた取組が始まったが、議会の審議が停滞し主要な立法措置が進まなかったことから、オバマ大統領は 2013 年 2 月 12 日に、重要インフラのサイバーセキュリティ強化に向けた大統領令を発出し、重要インフラ保護強化に向け、官民での情報共有体制構築に向けた作業を国土安全保障省（DHS）、国防省（DOD）および米国国立標準技術研究所（NIST）等に指示した。

---

[19] CNCI では 3 つの綱領を定めており、それらは、①サイバー攻撃に備える前線基地を構築し、ネットワークの脆弱性やサイバー脅威に関する意識を向上させることによるサイバー攻撃の未然防止、②防諜機能を強化し、重要な IT 技術に関するサプライチェーンの情報セキュリティを確保し、様々な脅威に対応できる体制の整備、③サイバー教育の拡大や省庁間での共同研究開発を促進し強固なサイバーセキュリティ環境の構築を目指すことである。

[20] CPR では、次の 10 の短期アクションプランを挙げており、これらの対応が現在のサイバーセキュリティ政策に繋がっている。
①サイバーセキュリティ政策を統括する部門の創設
②国家安全保障政策やサイバー政策の見直し
③連邦政府内でのサイバーセキュリティに関するパフォーマンス評価基準創設
④NSC のサイバーセキュリティ担当局によるプライバシー人権担当者の指名
⑤サイバーセキュリティ関連の優先課題に対する省庁横断的なメカニズムの構築
⑥サイバーセキュリティに関する教育と普及啓発
⑦サイバーセキュリティにおける国際連携強化
⑧サイバーセキュリティ事業への対応能力の強化と官民連携の強化
⑨サイバーセキュリティに関する研究開発の推進
⑩プライバシー人権に対応したサイバーセキュリティ強化

この大統領令による主な指示は図表 11 のとおりである。国家の重要インフラであるサイバー環境の維持について、民間の重要インフラ事業者との間でサイバーセキュリティに関する情報共有を強化、協力してリスク対応の標準化を進める方針を示した点が注目される。先のサイバー空間政策レビューとあわせて、この大統領令により、現在の米国連邦政府のサイバーセキュリティ政策の基礎が示されたものと言える。

図表 11　重要インフラのサイバーセキュリティ強化に向けた大統領令の主要項目

項目	対応等
サイバーセキュリティに関する情報共有	○サイバー脅威情報を的確に収集する手順書の作成 ○サイバー脅威情報を通知先に対象に迅速に広める方法の確立 ○重要インフラ事業者へのサイバー情報提供範囲の拡大 ○重要インフラ事業者の担当者等による当該事業の重大リスク特定 ○サイバー脅威情報の共有のため、政府への民間専門家の一時参加
プライバシーと市民権保護	○公正情報慣行原則等に基づくプライバシーと市民権確保
サイバーセキュリティ・フレームワーク	○重要インフラのサイバーリスクを低減させるためのベースラインフレームワークの構築 ○このフレームワークは米国国立標準技術研究所（NIST）が、産業界と協力し、次のとおり作成する ・サイバーリスクに対処するための方針、事業および手順に沿った一連の標準、技術、手段、工程が含まれること ・自主基準や業界のベストプラクティスを可能な限り最大限組み込むこと ・現在の国際基準等と整合的なものとすること ・重要インフラに適用される横断的なセキュリティ規準とガイドラインの特定に重点を置くこと ・フレームワークを実装した組織のパフォーマンス測定をするためのガイドラインを含むこと ・企業秘密、プライバシーおよび市民権保護に関する方法論を含むこと
自主的な重要インフラサイバーセキュリティプログラム	○重要インフラ事業者に対する自主的なサイバーセキュリティプログラムの採用の支援 ○事業セクター特有のリスク等に関する実装ガイダンスや補助資料の作成 ○事業者参加促進のための方策
重大リスクを有するインフラの特定	○サイバー攻撃が公衆衛生や安全、経済または国家安全保障に対して致命的な影響をもたらしえる重要インフラの特定

（出典：ホワイトハウスウェブサイトをもとに作成）

（2）サイバーセキュリティ体制

現在の米国連邦政府のサイバーセキュリティ体制は、前記（1）で説明した 2013 年 2 月 12 日の重要インフラのサイバーセキュリティ強化に向けた大統領令によって次のとおりとなっている。

a. ホワイトハウス

2009 年 12 月にホワイトハウスに国家のサイバーセキュリティ戦略・活動を統括する責任者のポストとして、サイバーセキュリティ調整官（Cybersecurity Coordinator）が新設された。同調整官は州政府や民間部門を含む全米のサイバーセキュリティの関係者と連携し、サイバー攻撃に対して組織的に統一の取れた対応を行うこと等が求め

られている。

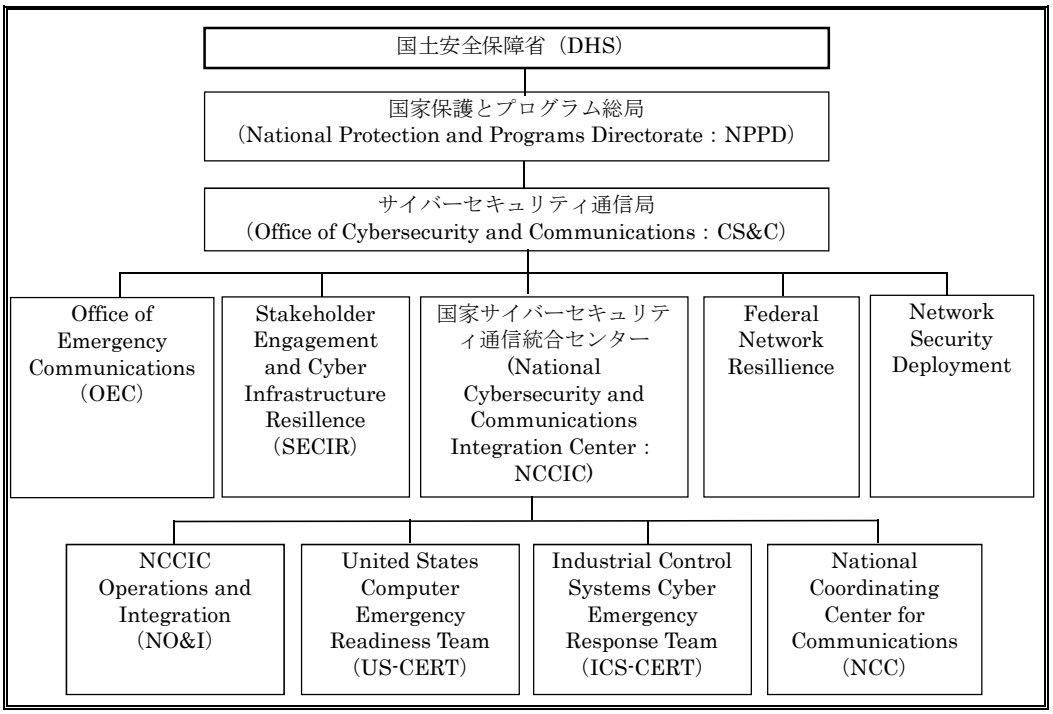
b. 国土安全保障省（DHS）

国土安全保障省（Department of Homeland Security：以下「DHS」）は、9.11 同時多発テロを機に、国土安全保障にかかる活動を統一的に実施するため、国土安全保障法（Homeland Security Act of 2002）により設立された省庁である。連邦政府のネットワーク空間の保護と安全性確保、重要インフラや IT システムのサイバーセキュリティ対策等を遂行する。同省内でサイバーセキュリティを所管するのは、サイバーセキュリティ部（Cyber Security Division：CSD）であり、サイバーセキュリティの戦略目標の設定や連邦政府間および各州との総合調整を行っている。

同省が所管するサイバーセキュリティ関係の組織は図表 12 のとおりである。

この中で、重要インフラに関するサイバーセキュリティ対策を行う組織について説明する。

図表 12　国土安全保障省のサイバーセキュリティ関係組織図



（出典：DHS ウェブサイトをもとに作成）

（a）国家保護とプログラム総局（NPPD）

国家保護とプログラム総局（National Protection and Programs Directorate：以下「NPPD」）は、米国の重要なインフラの安全とそれに対する脅威を軽減することを目的としており、サイバーセキュリティ対策もその任務のひとつとされている。

（b）サイバーセキュリティ通信局（CS&C）

サイバーセキュリティ通信局（Office of Cybersecurity and Communications：以下「CS&C」）は上記（a）の NPPD の下部組織であり、サイバーおよび通信インフラのセキュリティ等に中心的な役割を担う部門として、設置されている。

（c）国家サイバーセキュリティ通信統合センター（NCCIC）

上記（b）の CS&C の下部組織のうち、特に重要インフラを中心としたサイバー情報の集約機関として重要な役割を果たすのが国家サイバーセキュリティ通信統合センター（National Cybersecurity and Communications Integration Center：以下「NCCIC」）である。

NCICC は、米国内のサイバー攻撃情報を集約して注意喚起等を行う組織である United States Computer Emergency Readiness Team（US-CERT）や、主に産業制御システムに関するサイバー攻撃情報を集約する Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）を下部組織に置くとともに、後記 c、d の情報共有分析センター（ISAC）および情報共有分析機関（ISAOs）などの各機関からサイバー攻撃に関する情報を集約し共有する。NCCIC が集約した情報は日本を含む他国とも共有される。

c. 情報共有分析センター（ISAC）

情報共有分析センター（Information Sharing and Analysis Center：以下「ISAC」）は、1998 年 5 月に発出された大統領令の中で、重要インフラが攻撃される可能性を懸念して、所管組織の決定と情報共有の専門組織の設立が推奨されたことに対応し、金融、エネルギーなど重要インフラ分野ごとに設立された機関[21]である。

ISAC はサイバー攻撃に限らず、物理的攻撃も含めた脅威情報を各メンバーから集約、分析し、各メンバーとの情報共有を行うとともに、前記 b.（c）の NCCIC とも連携し情報共有を行っている。

d. 情報共有分析機関（ISAOs）

情報共有分析機関（Information Sharing and Analysis Organizations：以下「ISAOs」）は、前記（1）の 2013 年 2 月 12 日の大統領令に基づき DHS に設置促進が指示されたものである。

ISAOs は ISAC と同様にサイバー脅威に関する情報共有と分析を行う組織であるが、ISAC が組織されていない分野や ISAC のメンバーでない民間企業など幅広い分野を対

[21] 各 ISAC 間の相互連携等を行う目的で、National Council of Information Sharing and Analysis Centers（NCI）が設置されており、現在、21 の ISAC がメンバーとなっている。その中で、金融機関や保険会社等がメンバーとなっている機関としては、金融サービス ISAC（FS-ISAC）が設置されている。

象として情報共有を可能とすることを目的としている。従って、ISAC とは異なり、産業分野毎で関連付けられているものではなく、広く産官学の分野や地域等において団体が組織[22]されている。

ISAOs は前記 b.（c）の NCCIC とも連携し情報共有を行っている。

e. 米国国立標準技術研究所（NIST）

米国国立標準技術研究所（National Institute of Standards and Technology：以下「NIST」）は、1901 年に設立された米国最古の物理科学研究所の一つであり、現在は米国商務省（Department of Commerce：以下「DOC」）に所属している。

前記（1）の 2013 年 2 月 12 日の大統領令により、NIST は重要インフラのサイバーリスクを低減させるためのフレームワークを構築することを指示され、2014 年 2 月 12 日に「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」（Framework for Improving Critical Infrastructure Cybersecurity）初版を発行した。

現在、このフレームワークは米国[23]のみならず各国の監督当局[24]および民間企業におけるサイバーセキュリティ・フレームワークとして広く活用されている。なお、NIST フレームワークの概要は、本稿末尾の補足資料を参照願う。

f. 国防総省（DOD）

国防総省（Department of Defence：以下「DOD」）は、米国の国防、軍事を統合する省庁であり、国家防衛および安全保障という観点から連邦政府機関および軍におけるサイバー空間のセキュリティ強化を図るため、陸海空等の各組織のサイバー部隊を統合し、米国軍の IT インフラへの攻撃 に対応するとともに、サイバー空間全体のセキュリティ強化を通じ米国民の保護も活動の目的としている。

同省では、サイバー空間におけるセキュリティ強化のため、米国サイバー軍（USCYBERCOM）を設置し、2010 年 10 月から本格活動を開始している。

---

[22] ISAOs の標準化を進めるため、2015 年 10 月に非政府組織の ISAO 標準化機構（ISAO Standards Organization：ISAOSO）が設立されている。参加者は現在 55 機関で、ISAOs に加え金融サービス ISAC（FS-ISAC）などの ISAC も参加している。

[23] NIST は外部リサーチ会社の調査結果として、2015 年では米国組織の 30%が NIST フレームワークを使用しており、2020 年までに使用率は 50%に達すると予想されるとしている。
また、2017 年 5 月の連邦政府のネットワークおよび重要インフラのサイバーセキュリティ強化に関する大統領令では NIST フレームワークの使用を連邦政府機関に義務付けている。

[24] 例えば、保険監督者国際会議（IAIS）では、2016 年 4 月公表の“Issues Paper on Cyber Risk of The Insurance Sector”において、保険会社のサイバー攻撃耐性のベストプラクティスとして NIST フレームワークを挙げており、また、前記 2.（1）c.(ｃ)ア.の金融庁「金融分野におけるサイバーセキュリティ強化に向けた取組方針」ではサイバー攻撃への対処を行う各ステップの設定で、同フレームワークを利用している。
また、PwC 発表の「グローバル情報セキュリティ調査 2016（日本版）」によると、世界全体では NIST フレームワークをはじめとした最新のサイバーセキュリティ・フレームワークを採用しているが、日本企業はほとんどが平時のマネジメントを重視する ISO27001 を利用しており、NIST フレームワークの採用率も世界平均が 35%であるのに対し、日本は 9%に留まっているとしている。

g. 国家安全保障局（NSA）

国家安全保障局（National Security Agency：以下「NSA」）は、DOD 内に置かれる諜報活動機関であり、その役割には、機密情報を含む国家安全保障システムに関する情報収集活動が含まれるとともに、サイバー空間の情報保護に関する活動を進めている。

なお、組織の性格上、詳細な活動内容は明らかにされていない。

h. 連邦捜査局（FBI）

連邦捜査局（Federal Bureau of Investigation：以下「FBI」）は、連邦法に関する事案の捜査を任務としており、捜査目的の諜報活動なども行っているが、この対象にはサイバー空間も含まれており、サイバー犯罪の捜査は重要な活動のひとつになっている。

サイバー犯罪捜査は FBI 本部のサイバー部門が統括し、現在、コンピュータとネットワークへの侵入捜査等を優先事項とする一方、インターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）[25]およびサイバーアクションチーム（Cyber Action Team：CAT）[26]等と連携している。

（3）官民連携の取組

上記（2）において、NCCIC 等による官民による情報共有の体制について説明したが、その他の官民連携の取組について説明する。

a. 国立サイバーセキュリティ研究開発（NCCoE）

国立サイバーセキュリティ研究開発（National Cybersecurity Center of Excellence：以下「NCCoE」）は、NIST がメリーランド州およびメリーランド州モンゴメリー郡と共同で 2012 年 2 月 21 日に設置した組織である。

図表 13 で示す目的のもとで、政府機関、学術機関、民間企業[27]が協力し、サイバーセキュリティに関する研究を行っている。

図表 13　NCCoE の目的と主な活動

目的
①実践的なサイバーセキュリティを提供する 　費用対効果等に優れた実用的なサイバーセキュリティソリューションを提供する ②サイバーセキュリティの採用率の向上 　費用を抑えた市販のサイバーセキュリティ技術を採用できるようにする ③効果的なイノベーションの加速 　関係者の協力体制によってサイバーセキュリティ対策を加速させる

[25] インターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）はインターネットによる犯罪行為による苦情や情報を受け付け FBI 等の適切な機関に通報する機関である。
[26] サイバーアクションチーム（Cyber Action Team：CAT）は 2006 年に FBI のサイバー部門によって設立されたサイバー犯罪捜査を専門とする特別チームである。
[27] NCCoE には、インテル、マイクロソフト、IBM など大手ベンダーの多くが参加している。

主な活動
①ビルディングブロック 　複数の分野に影響を及ぼす幅広い技術に関するテーマの研究を行う。そのために様々な業界が参加するプロジェクトとなる ②ユースケース 　分野固有(注)のサイバーセキュリティの課題に取り組む

（注）対象分野の区分は、小売、エネルギー、金融サービス、保健、製造、公衆安全など。
　　金融サービスにおいては、アクセス権管理、IT 資産管理および特権アカウント管理がテーマとなっている。

（出典：NCCoE 資料をもとに作成）

b. サイバーストーム

サイバーストーム（Cyber Storm）は DHS が主導[28]し、政府内のサイバー関係機関と民間機関が参加する大規模なサイバーセキュリティ演習である。

2006 年 2 月に初回の演習を実施し、その後、毎回規模を拡大しながら隔年で実施[29]されている。前回 2016 年 3 月に実施されたサイバーストームⅤの概要は図表 14 のとおりである。

図表 14　サイバーストームⅤの概要

主要目標
○サイバーインシデント対応関連機関の調整メカニズム、情報共有努力、発見状況確認体制の確立および意思決定手続きの確認 ○サイバーインシデント対応機関およびリソースの優先順位付けを管理する指針、手順および財務的内容の確認 ○参加者が組織や関連組織内の手順、相互関係、情報共有の仕組みを評価し改善するためのフォーラムの設定 ○サイバーインシデントにおける DHS やその他の政府機関の役割、機能、能力の評価
演習体制
○世界中の参加者が通常の業務環境で参加できることを可能とする分散型の演習体制をとり、演習の中核は DHC 施設内に設置した ○演習のシナリオは参加者が演習用のウェブサイトから受け取ることで進行し、自組織の対応システム、指針および手順に従って模擬的なサイバー危機に対応することで、発生した影響等を発見する
参加者
参加者は次のとおり。世界中の 100 以上の組織と 1,200 人以上の登録者が参加した。特に、今回からは保健・健康関係および小売関係が初めて参加した ○連邦政府および提携組織 ○法執行機関、政府情報機関および DOD ○州政府 ○国際機関・組織 ○IT、商業、保健・健康、マスコミ関係機関
演習シナリオ
複数の攻撃者を設定し、これらの攻撃者は共同し、時には単独で複雑な新しいマルウエア(注)を配付することで重要インフラ分野に対して重大な影響を与えるように設定した

[28] 前記（2）b.（b）の CS&C が担当する。
[29] 次回は 2018 年春にサイバーストームⅥが計画されている

参加者の活動
○サイバー攻撃の潜在的な影響に対しての組織の準備、保護および対応能力の検証 ○連邦レベルの方針と手続きに従って、インシデント対応の戦略的意思決定と省庁間調整を実施 ○サイバーインシデントの把握、対応、回復情報を収集し伝達するための情報共有と伝達経路の検証 ○国家の安全保障上の利益を損なうことなく、分野間等で機密情報を共有する手段とプロセスの確認

（注）マルウエアとは malicious software の造語であり、不正かつ有害に動作させる意図で作成された悪意あるソフトウエアやコードの総称である。

（出典：DHS 資料をもとに作成）

c. サイバーチャレンジ

サイバーチャレンジ（US Cyber Challenge：以下「USCC」）は、非営利団体である Center for Internet Security（CIS）が DHS の支援を受け、高校生から大学院生を対象としたサイバーセキュリティ人材を育成することを目的に実施しているプログラムであり、全米の産業界、政府機関および学術機関が参加している。

主な実施プログラムはコンテストとサイバーキャンプの 2 つから構成され、概要は次のとおりである。

（a）サイバークエスト

サイバークエストはオンラインコンテストであり、参加者はウェブ上に登録し、全米で同一時間帯に、設定された質問に回答していく形をとっている。

出題内容は、サイバーセキュリティに関する基本的な内容から、システムの脆弱性の判断、コンピュータ・フォレンジック[30]分析および仮想攻撃への対処などの専門的なものまでと幅広い。

また、このサイバークエストは、後記（b）のサイバーキャンプの参加権獲得のための予選という側面も有している。サイバーキャンプの出場希望者は、このサイバークエストに参加し、一定の成績を残すことが必要となっている。

（b）サイバーキャンプ

サイバーキャンプは毎年夏に実施される。2017 年は、デラウエア州、イリノイ州、東部地区の 3 箇所で実施された。

参加者は上記（a）のサイバークエストで一定の成績を残した者であり、かつ米国の当該地域の居住者または学生であることが条件となる。

[30] コンピュータ・フォレンジックとは、コンピュータに関する科学捜査のことで、情報漏洩や不正アクセスなど、コンピュータが関わる犯罪が起きた際に、コンピュータ本体に記録された電子データを収集・分析して、証拠とするための技術のことである。
なお、フォレンジックとは、鑑識、科学捜査の意味で、もともとは警察の犯罪捜査で用いられている用語である。

同キャンプの開催期間は約 1 週間で、大学の教員、システム専門家およびサイバーセキュリティの専門家からの専門トレーニングを受けるとともに、スポンサーからの求職セッションなども用意され、最終日には「キャプチャ・ザ・フラッグ」という競技会が開催される。

4．米国のサイバーセキュリティ人材対策の現状

サイバー攻撃の増加に伴い、サイバーセキュリティ対策の人材不足が世界的に深刻な状態となっており、2021 年までに全世界で 350 万人の新たな需要が発生するとの予想[31]もある。

本項では、米国のサイバーセキュリティ人材について、需給状況を概観し、次いでその対策について説明する。

（1）人材の需給状況

米国においては、2017 年 12 月時点で約 75 万人がサイバーセキュリティの職に就いているが、同時に約 29 万人の求人が発生[32]している。

このような人材不足に伴い、サイバーセキュリティ要員の賃金も上昇しており、2017 年の IT 関係全体のシニア管理職の予想平均賃金の上昇は前年比 3.0%であったのに対し、セキュリティ管理職は同 6.4%と倍以上の伸びを示し、また、セキュリティ担当職員の平均賃金も IT 担当職員全体の平均賃金と比べ約 15%高くなっているという調査結果[33]が示されている。

このような賃金水準の上昇にもかかわらず、ISACA の調査[34]によると、米国では 22%の組織において、必要なサイバーセキュリティ対策要員の補充ができていないとの結果が示されている。

同調査では、組織の求める人材の要件として、最も重視するのは実務経験、その次は保有資格および人物評定という結果が示されている。必要なサイバーセキュリティ対策要員の補充ができない最大の要因は、組織が求めるこれらの要件に合致した応募者が不足しているためであり、ここから、組織の求めるサイバーセキュリティ要員のスキルと応募者のスキルの間にギャップがあることが明らかとなっている。

米国では、このサイバーセキュリティ人材不足の解消に向けた各種取組が行われている。後記（2）、（3）では、その取組の中核ともいえるサイバーセキュリティ教育のための国家計画（National Initiative for Cybersecurity Education：NICE）を中心に説明する。

---

31 Cybersecurity Ventures, “2017 Cybersecurity Jobs Report”
32 Cyber Seek ウェブサイト（http://cyberseek.org/）
33 Computerworld, “IT Salary Survey 2017”(2017.4)
34 ISACA ,“State of Cyber Security2017”

（2）サイバーセキュリティ教育のための国家計画（NICE）

サイバーセキュリティ教育のための国家計画（National Initiative for Cybersecurity Education：以下「NICE」）は、前記 3.（1）のサイバー空間政策レビュー（CPR）で求められた短期アクションプラン 10 項目のうち、サイバーセキュリティに関する教育と普及啓発の実現のため、2010 年 3 月に NIST が設定したものである。

NICE で示される戦略計画は次のとおりである。

① ビジョン

知識豊かで熟練したサイバーセキュリティ対応人材によってデジタル経済を可能とさせる

② ミッション

堅牢なネットワークとサイバーセキュリティ教育、訓練、および労働力開発の協調関係を活性化し促進する

また、この戦略計画に基づいた目標は図表 15 のとおりである。

NIST はこの目標に従い、連邦政府機関とも連携した活動を行っている。主な活動を説明するとともに、後記（3）では NICE サイバーセキュリティ・労働力フレームワークに関係する活動を説明する。

図表 15　NICE の目標

①学習とスキルの開発を加速する ・熟練したサイバーセキュリティ労働者の不足に対処するため、公共部門と民間部門での対応を加速させる ②多様な学習コミュニティを育む ・学習を重視し、成果を測定し、サイバーセキュリティの労働力を多様化するために、全体の教育と訓練を強化する ③キャリア開発と人材計画をサポートする ・雇用者が市場の需要に対応、雇用活動を拡大し、サイバーセキュリティ対応の技能者の確保を強化する。

（出典：NIST ウェブサイトをもとに作成）

a. NICE チャレンジプロジェクト

NICE チャレンジプロジェクトは、学生やサイバーセキュリティの専門家が後記(3)の NICE サイバーセキュリティ・労働力フレームワークをもとに知識、技能および能力のレベルをテストすることができる仮想のチャレンジ環境を提供するために設立された。

同プロジェクトは NIST および NSA が助成するプロジェクトで、非営利団体の University Enterprises Corporation（UEC）がカリフォルニア州と提携し実施している。

同プロジェクトでは、クラウドサーバーに仮想の空間を設け、多様なオペレーション

システムとサービスをベースにしたモデルを構築[35]している。プロジェクトに登録した参加者は自らのコンピュータからアクセスし、与えられた課題解決に取り組むことでその知識、技能および能力のレベルが判定される。

b. 国立総合サイバー教育研究センター（NICERC）

国立総合サイバー教育研究センター（The National Integrated Cyber Education Research Center：以下「NICERC」）は、非営利団体である Cyber Innovation Center の学術・教育部門である。

同センターは、DHS からの資金提供を受け、サイバーセキュリティ教育に関するカリキュラム開発を行い、全国の K-12 教育[36]における教員に対して、カリキュラムと教材[37]を無償で提供している。

c. RAMPS サイバーセキュリティ教育と労働力開発

NIST は地域におけるサイバーセキュリティ人材不足の改善に焦点を当て、後記（3）の NICE サイバーセキュリティ・労働力フレームワークに沿ったサイバーセキュリティ教育と人材育成を行うことを目的に、RAMPS サイバーセキュリティ教育と労働力開発（Regional Alliances and Multi stakeholder Partnerships to Stimulate（RAMPS）Cybersecurity Education and Workforce Development） を推進している。

主な活動は、各地域でサイバーセキュリティ教育等を行っている非営利団体の活動の支援であり、DOC が資金援助[38]を行っている。

d. サイバーセキュリティ人材と教育のための国家イニシアチブ（NICCS）

サイバーセキュリティ人材と教育のための国家イニシアチブ（National Initiative for Cybersecurity Careers and Studies：以下「NICCS」）は、学生、労働者および専門家がサイバーセキュリティの適切な訓練と教育を受けるための機会を提供することを目的に DHS が設置したものである。

NICCS の提供するプログラムの中で主要なものは教育訓練カタログで、全米の教育機関等が提供するサイバーセキュリティの訓練、教育プログラムをウェブ上で検索できるポータルサイトとなっている。

図表 16 は、教育訓練カタログのトップページである。受講希望の地域をビジュアル

---

[35] NICE チャレンジプロジェクトの対象は現在のところ NICE フレームワークカテゴリーの「操作および保守」の分野が完成、「保護と防衛」および「調査」の分野を開発中であり、最終的にはフレームワークの 7 つの全てのカテゴリーをカバーする予定とのことである。

[36] K-12 とは幼稚園（Kindergarten の K）から高等学校を卒業するまでの 13 年間の教育期間のこと。

[37] NICERC のカリキュラムには、サイバーリテラシー、サイバーサイエンス、サイバーソサエティ、コンピュータサイエンス、数学および物理などが含まれる。

[38] 2016 年は、5 団体へ各約 20 万ﾄﾞﾙを提供した。

に絞り込むことが可能であると同時に、検索キーをもとに希望のプログラム[39]を選択することができる。

なお、教育機関がこの教育訓練カタログに登録するには、一定の基準があり、NICCSへ申請し認定を受ける必要がある。

図表 16　教育訓練カタログのトップページ

（出典：NICCS ウェブサイトをもとに作成）

e. アカデミック・エクセレンス国立センター（CAE）

NSA と DHS は共同してアカデミック・エクセレンス国立センター（National Centers of Academic Excellence：以下「CAE」）に資金を拠出し、CAE in Cyber Defense プログラムを実施している。

このプログラムは、サイバーセキュリティ教育を実施する大学等の中から一定の水準に達している教育機関を認定するもの[40]であり、現在 200 以上の大学等が認定されている。

認定教育機関の教育プログラムを終了した学生は、NSA/DHS CAE 認定教育機関による学位等を取得したことを雇用主等に示すことができる。

（3）NICE サイバーセキュリティ・労働力フレームワーク

NIST では、サイバーセキュリティ人材の活用にはサイバーセキュリティ対応人材が定義されこれに基づき評価される必要があるという認識から、サイバーセキュリティの労働力フレームワーク策定を進め、2013 年に The National Cybersecurity

[39] 検索キーとしては、実施機関、地域、専門分野、レベル、通学・オンラインの別などであり、分類は NICE フレームワークに準じている。なお、現在、検索可能なプログラム数は 3, 000 件以上である。
[40] 認定区分は 2 年制レベルの NSA/DHS CAE-2Y、4 年制レベルの NSA/DHS CAE-CDE、および大学院レベルの NSA/DHS CAE-R の 3 区分となる。

Workforce Framework 1.0 を公表、続いて 2014 年にバージョン 2.0 を公表した。

NIST はその後、このフレームワークを全面的に見直し、2017 年 8 月 7 日に NICE サイバーセキュリティ・労働力フレームワーク（National Initiative for Cybersecurity Education（NICE） Cybersecurity Workforce Framework：以下「NICE フレームワーク」）を公表している。

NICE フレームワークは組織、応募者および教育関係機関[41]等が同一の基準のもとでサイバー人材不足の対策を講じることで人材のスキルギャップを改善し、需給のミスマッチを減少させることを狙いとしている。

a. NICE フレームワークの概要

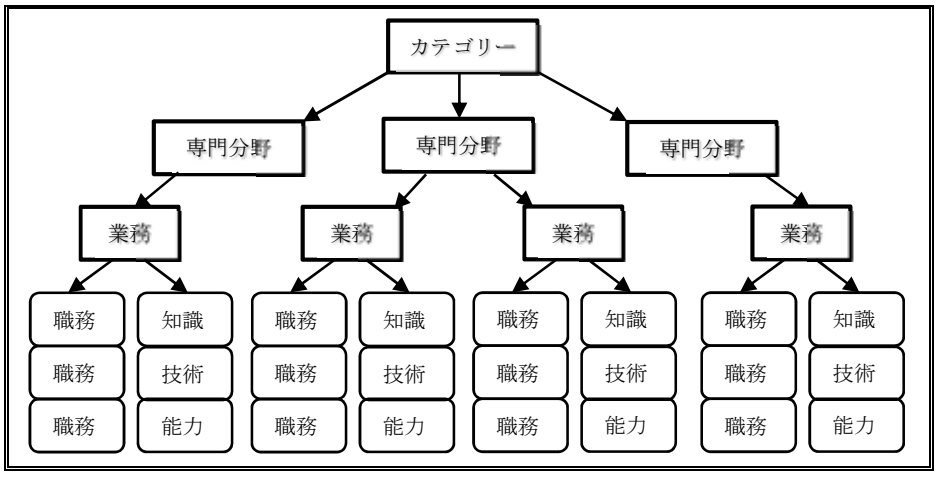
（a）NICE フレームワークの構造

NICE フレームワークは、カテゴリー、専門分野、業務、職務、知識、技術、能力の 7 つの要素から構成されており、この関係は図表 17 のとおりである。

この中で最上層に位置する「カテゴリー」はさらに 7 項目にわけられ、それぞれが下層である専門分野と業務に向ってこれらを細分化させている。

さらに、各「業務」において必要とされる職務、知識、技術、能力が示される形となっている。

図表 17　NICE フレームワークの概念図



（出典：NICE フレームワークをもとに作成）

[41] NICE フレームワークが想定する関係者と、フレームが与える効用は次のとおりである。
①雇用主：必要なサイバーセキュリティ人材の知識、技術、能力の特定に役立つ
②職員（応募者）：組織が求める知識、技術、能力の理解に役立つ
③研修担当：職員等が必要な知識、技術、能力を獲得するために役立つ
④教育機関：カリキュラムや研究開発の際に役立つ
⑤技術プロバイダー：提供するサービス、ハードウエアおよびソフトウエアに関連するサイバーセキュリティ要員の知識、技術、能力の特定に役立つ

（b）NICE フレームワークの構成要素

前記（a）で説明した 7 つの構成要素とその概要を図表 18 に示した。

このうち「カテゴリー」は 7 項目に分類され（図表 19 参照）、また、下層の「専門分野」はさらに 33 項目に分類、続く「業務」は 52 項目に分類され、それぞれの一覧表により定義付けがされている。

知識、技術、能力（以下「KSAs」）と「職務」にも、それぞれ一覧表が示されており、定義付けがされている[42]が、これらは各「業務」に一対一で紐付けるのではなく、フレームワーク全体で網羅的な一覧表が作成され、各業務で必要とする項目をそこからピックアップする形をとっている。

組織が必要とするサイバーセキュリティ人材の検討において NICE フレームワークを活用するには、7 つの構成要素のうち、「業務」で区分された表を用いることが中心となる。

この「業務」は分類された 52 項目ごとに一つのシートができており、このシートには、「KSAs」、「職務」の一覧表に分類された項目のうち、当該業務で求められる項目がピックアップされ記載されている。

図表 18　NICE フレームワークの構成要素

①カテゴリー
- 共通するサイバーセキュリティ機能を最上位のレベルで示したもの

②専門分野
- サイバーセキュリティおよび関係する業務または機能の中で、業務の中心となる範囲を示したもの

③業務
- サイバーセキュリティおよび関連する業務の最も詳細な区分を示したもの
- 必要な職務や知識・技術・能力を示すことができる区分

④職務
- 個別の職員に求められる固有の業務

⑤知識・技術・能力
- 職務遂行において求められるもの
- 一般的には、関連経験や実力の証明が可能な教育および訓練によって示されるもの

（出典：NICE フレームワークをもとに作成）

図表 19　NICE フレームワークのカテゴリー

①基盤構築
- システムまたはネットワーク開発において安全な情報技術（IT）システムを規定、設計、調達または構築する

②操作および保守
- 情報システムのパフォーマンスとセキュリティを効果的かつ効率的に確保するため必要なサポート、管理、および保守を提供する

③監督と統制

[42] KSAs と職務の分類数は現時点で次のとおりと膨大な項目数となっている。
知識：630 項目、技術：374 項目、能力：176 項目、職務：1007 項目

・組織が効果的にサイバーセキュリティ対策を実施できるように、リーダーシップ、管理、指導、または開発と支援の提供をする
④保護と防衛
・内部情報システムまたはネットワークに対する脅威を特定、分析、軽減する
⑤分析
・入手したサイバーセキュリティ情報が有益であるか否かについて、高度に専門的な評価を実施する
⑥収集と操作
・サイバーセキュリティ情報や詐欺情報などの収集を行う
⑦調査
・情報システム、ネットワーク、および電磁的証拠に関連するサイバーセキュリティイベントまたは犯罪を調査する

（出典：NICE フレームワークをもとに作成）

（c）NICE フレームワークの活用

NICE フレームワークの活用について、前記（b）で説明した 52 項目の業務の中から、１つの業務を例に挙げ説明する。

図表 20 は業務のひとつである「承認権限者」（Authorizing Official）のシートである。承認権限者は、カテゴリーが基盤構築、専門分野がリスクマネジメントに属している。

この表では、承認権限者の業務内容が示され、さらに必要な職務と KSAs が掲載されている。なお、職務と KSAs の欄は記号で記載されており、利用に際しては、それぞれの一覧表において当該記号に合致する記載内容を確認することとなる。これらの一覧表の抜粋は、図表 21 および図表 22 に示した。

このシートを活用することにより、雇用主は承認権限者に必要な職務と KSAs が網羅的に確認でき、応募者は雇用主が求めている職務と KSAs を理解することができることとなる。また、研修担当は、現在の承認権限者に求められる研修内容を効率的に理解することが可能となる[43]。

図表 20　業務リスト（抜粋）

カテゴリー	基盤構築
専門分野	リスクマネジメント
業務	承認権限者
業務 ID	SP-RSK-001
業務内容	組織の業務（任務、機能、イメージ、評判を含む）、組織資産、個人、その他の組織、国家に対して許容可能なリスクレベルで情報システムを運用する責任を正式に負う権限を持つ上級管理職または役員
職務	T0145, T0221, T0371, T0495
知識	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059,

[43] NICE は、業務に応じた KSAs を評価するための指標は示していなかったが、2017 年 11 月 8 日にこの指標案となる National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles（Draft NISTIR 8193）を公表、現在は意見の取りまとめ中である。

	K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624
技術	S0034, S0367
能力	A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170

（出典：NICE フレームワークをもとに作成）

図表 21　職務リスト（図表 20 掲載項目の抜粋）

職務 ID	内容
T0145	認定パッケージ（ISO / IEC 15026-2 (注) など）の管理および承認をする。
T0221	承認文書および保証書を確認して、ソフトウェアアプリケーション、システム、およびネットワークごとにリスクレベルが許容範囲内にあることを確認する。
T0371	ソフトウェアアプリケーション、ネットワークまたはシステムの利用範囲を定める
T0495	認定パッケージ（ISO / IEC 15026-2 (注) など）の管理をする。

（注）システムおよびソフトウエアの認証規格

（出典：NICE フレームワークをもとに作成）

図表 22　KSAs リスト（図表 20 掲載項目の抜粋）

KSAID	内容
K0001	コンピュータネットワークの概念とプロトコル、およびネットワークセキュリティの方法に関する知識
K0002	リスク管理プロセスの知識（例えば、リスク評価と緩和のための方法）
S0034	情報システムとネットワークの保護ニーズ（例えばセキュリティ制御）の識別に熟練している
S0367	組織の要件（機密性、完全性、可用性、認証、否認防止に関連する）をサイバーセキュリティとプライバシーポリシーに適用させる技術がある
A0028	組織の目標を達成するための人材要件を評価し、予測する能力がある
A0033	組織のサイバー活動を支援するための法律、規則、方針、基準に準拠したポリシー、計画、戦略を策定する能力がある

（注）知識（「K」）および能力（「A」）は、図表 20 掲載項目の一部のみを記載している

（出典：NICE フレームワークをもとに作成）

b. NICE フレームワークの活用例

前記 a.で説明した NICE フレームワークの活用例として、CyberSeek の事業を説明する。

CyberSeek は、サイバーセキュリティの雇用市場における需要と供給の関係に関する詳細な情報を提供し、求職者と雇用者との間のスキルの認識ギャップを解消させるために設けられたウェブ上のツールであり、非営利団体の CompTIA[44]が NIST の資金援助を受け、2016 年 11 月から開始したものである。

このツールは大きく分けて、サイバーセキュリティ人材・ヒートマップとサイバーセ

[44] 民間職業紹介会社である Burning Glass Technologies との提携事業である。

キュリティ・キャリアパスの 2 つで構成されているが、いずれも NICE フレームワークをベースに構築されている。

(a) サイバーセキュリティ人材・ヒートマップ

サイバーセキュリティ人材・ヒートマップ（以下「ヒートマップ」）のトップページは、図表 23 のように示される。

この図は、地域ごとでのサイバーセキュリティ人材の需給関係を色分けし一覧できるようにしたものである。

利用者は、このマップから州単位または 300 以上の大都市圏単位での需給関係を検索でき、求人数、就業者数、需給バランス、就業者の地理的集中度および求められている職務などを確認することができる。

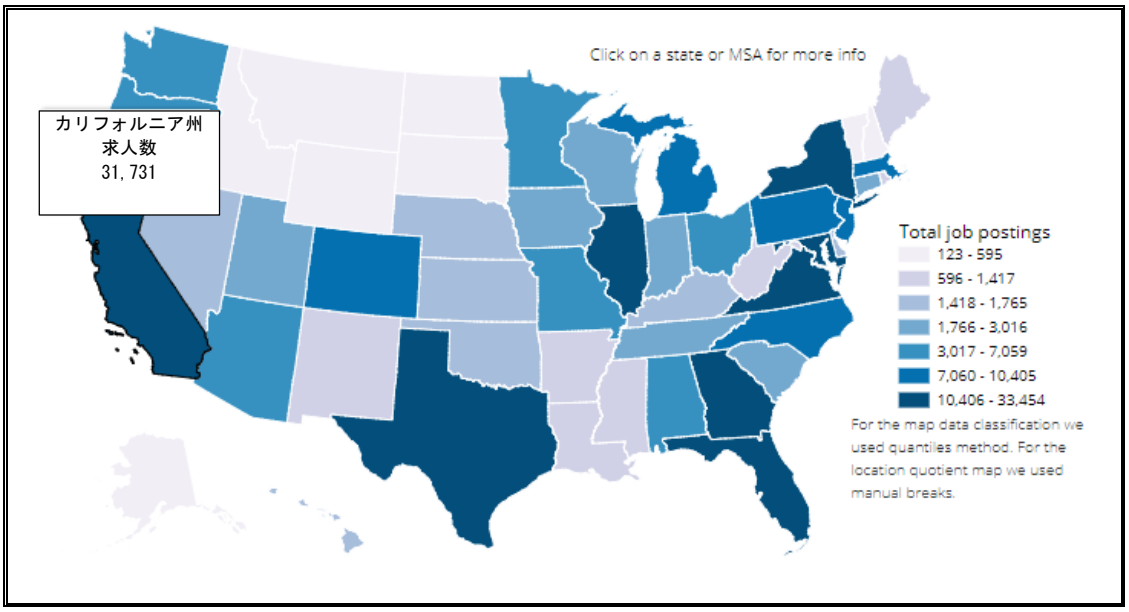
図表 24 は最も求人者数の多いカリフォルニア州の例である。就業者の集中度は各州と比較すると平均的だが、83,413 名の就業者に対し、31,731 名の求人が発生し、需給バランスは極端に供給不足となっていることが分かる。

また、図表 25 は NICE フレームワークのカテゴリーごとの求人数を示している。カリフォルニア州では、基盤構築（Securely Provision）のカテゴリーの求職が最も多いことが分かる。

さらに、このヒートマップでは、図表 26 のとおり、サイバーセキュリティ人材に求められる資格の需給関係も確認できる。各資格の上段は、カリフォルニア州における有資格者数で、下段はその資格保持者に対する求人数であり、CISA および CISM 資格保持者が不足していることが分かる。

このヒートマップは、求職者にとってはどの地域で求職することが有利なのか、また、雇用者は求人や業務展開に適した地域はどこかを確認するためのツールとして活用することができ、これにより人材の需給調整が行われることが期待される。

図表 23　人材・ヒートマップ

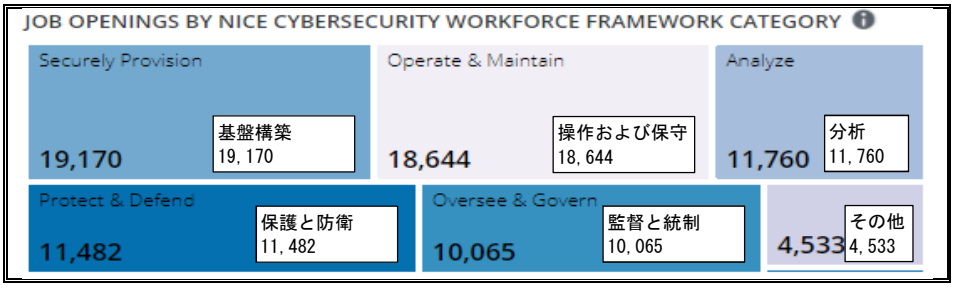


（出典：CyberSeek ウェブサイトをもとに作成）

図表 24　カリフォルニア州のサイバーセキュリティ人材の需給関係

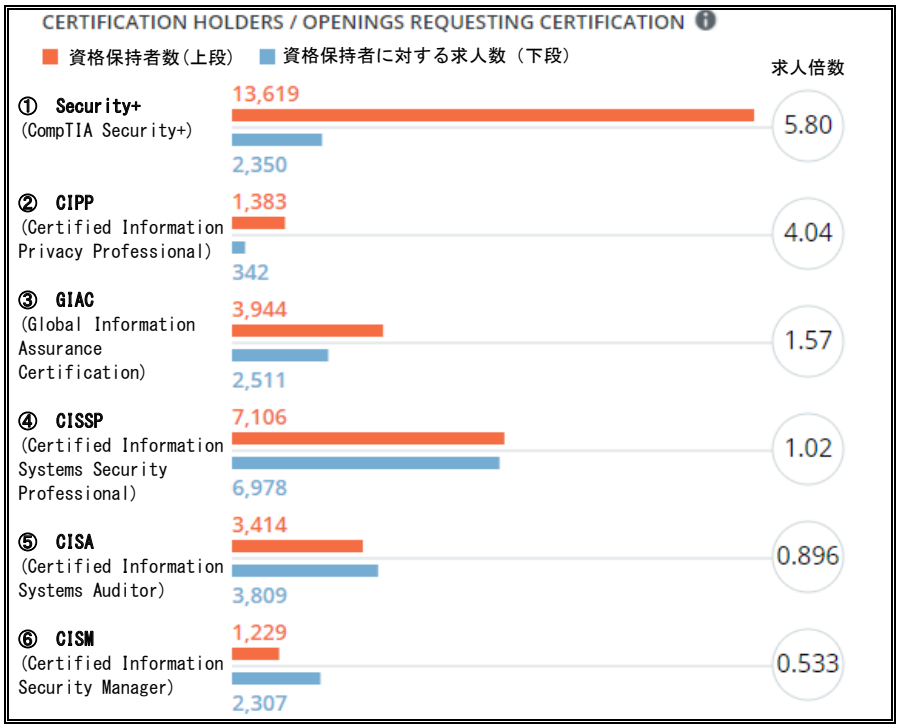
（出典：CyberSeek ウェブサイトをもとに作成）

図表 25　求人のカテゴリー



（出典：CyberSeek ウェブサイトをもとに作成）

図表 26　保有資格の需給バランス



（注）上記資格は次のとおりである。

①Security+：情報セキュリティの基礎的内容を扱う。CompTIA が認定

②CIPP：情報プライバシーに関する資格。IAPP が認定

③GIAC: 情報セキュリティ全般知識、情報セキュリティ監査、侵入検知、インシデント対応等各分野を扱う。SANS Institute が認定

④CISSP：5 年以上実務経験を有し、リスク管理、セキュリティ評価、監査、アクセス管理等の分野を扱う資格。（ISC）[2]が認定

⑤CISA：5 年以上の実務経験を有し、情報システム監査、セキュリティ、システム管理等の分野を扱う資格。ISACA が認定

⑥CISM：マネジメントレベルの情報セキュリティに関する資格。ISACA が認定

（出典：CyberSeek ウェブサイトをもとに作成）

（b）サイバーセキュリティ・キャリアパス

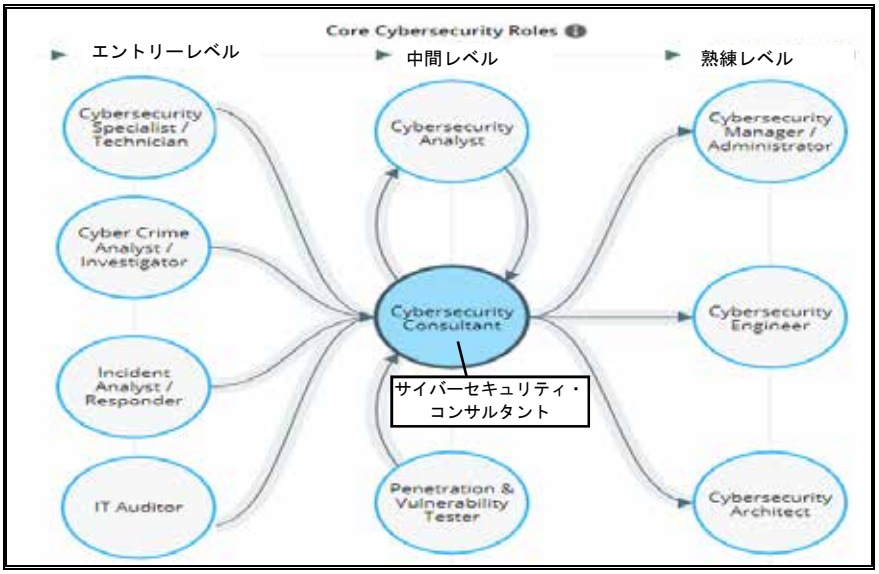
サイバーセキュリティ・キャリアパスは、サイバーセキュリティ業務の従事者やこの業務に興味のある者に対して、キャリアパスが詳細に示されており、サイバーセキュリティにおける職務や各種職務間の移行の機会、および各役職に関連する給与、資格情報、および求められる KSAs に関する情報が示されている。

図表 27 はサイバーセキュリティ・コンサルタントを中心としたキャリアパスを表示した例である。

サイバーセキュリティ・コンサルタントを目標とする者、また、既にこの業務の従

事者で、今後のキャリアアップを検討する者への道筋が示され、また、別シートにおいてそれぞれの業務に求められる資格、KSAs、需給状況や給与水準などの情報が確認できるようになっている。

図表 27　キャリアパスの例



（出典：CyberSeek ウェブサイトをもとに作成）

５．おわりに

米国は、サイバーセキュリティ人材対策を官民の連携によりダイナミックに推進している。

具体的には、サイバーセキュリティ人材の流動化に向けたインフラが用意され、人材の需給ギャップを解消する動きが進められている。また、人材不足についても本格的な取組が進んでいる。その一つは、大学をはじめとした教育機関でのサイバーセキュリティ教育の推進であり、二つ目は、学生や求職者に対するキャリアパスの提示である。

また、これらを容易にしているのは、多様なサイバーセキュリティ人材のスキルを標準化した NICE フレームワークの存在である。

米国の対策を踏まえて、わが国のサイバーセキュリティ人材対策の課題を解決するには次の点が考えられる。

１つ目は、サイバーセキュリティ人材のスキルギャップの解消である。現在、サイバーセキュリティ人材の絶対数が不足している状況にあるが、その中でも、組織が求める人材と応募者との間でのスキルギャップを解消させ、サイバーセキュリティ人材の流動化を進める必要がある。この中には、人材流動化の仕組みの構築および、そのためのスキルの標準化（見える化）が含まれるが、NICE フレームワークやその活用例が参考

となる。

ただし、わが国では、米国と雇用環境が異なり、流動化を一気に進展させることは困難が予想されるため、他の対策も重要である。

2 つ目に挙げるのはインセンティブ付与を伴うサイバーセキュリティ人材の育成である。

企業の若手・中堅層に対しては、明確なキャリアパスを示した上で、教育・訓練に参加させ、また、学生には、将来の進路を明確に示した上で、教育機関のカリキュラムを充実させることが有効である。関連する資格制度などのステータスを示すことも重要である。NICE の取組には、キャリアパスおよび大学を中心とした充実したカリキュラムの提供があり参考となる。

このような国や行政が推進すべき施策とともに、3 つ目として、各民間企業は自前での人材育成を進める必要がある。わが国では外部からの人材供給は限界に近づいており、自前の対策を進めることが必要である。

具体的には、AI をはじめとして急速に発展している IT 技術をサイバーセキュリティ対策に活用すると同時に、社内のセキュリティ人材育成を計画的に進めていくことが求められる。その中には人材の発掘も含まれる。従来、セキュリティ人材の育成候補者として認識されることが比較的少なかった女性やシニアなど多様な人材の活用も検討する必要がある。

これらの 3 つの解決策は同時に進める必要があり、また、米国同様、官民の連携が必要であることを強調しておきたい。

なお、本稿の補足資料として、NIST サイバーセキュリティ・フレームワークの概要を説明している。このフレームワークはサイバーリスク対策を組織全体で計画する際に参考となるツールであり、当然ながらサイバーセキュリティ人材の確保も含まれている。現在検討中の改訂版ではサイバーセキュリティ対策の投資有効性の検証に同フレームワークを活用していくという方向性が示されている。今後、各組織のサイバー保険導入に際しては、組織全体でのサイバーセキュリティ対策コストの中で保険料等の比較検討が一層進むと想定される。ご参考としていただければ幸いである。

＜補足資料＞

NIST サイバーセキュリティ・フレームワーク

（1）NIST フレームワークの適用

2013 年 2 月 12 日の大統領令[45]に基づき、NIST は 2014 年 2 月 12 日に「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」（Framework for Improving Critical Infrastructure Cybersecurity：以下「NIST フレームワーク」）の初版である Ver1.0 を発行した。

現在 NIST フレームワークは、改訂版の検討がされており、NIST フレームワーク Ver1.1 ドラフトが公表[46]されている。後記（2）、（3）では、初版の Ver1.0 をベースに説明し、続く（4）において初版との対比をする形で、Ver1.1 の改訂箇所を説明することとしたい。

（2）NIST フレームワークの概要（Ver1.0）

NIST フレームワークは、重要インフラのサイバーリスク低減を求めたものであるが、幅広い組織において適用可能とさせるため、高い柔軟性を確保しており、業種や技術的な偏りがなく、業界標準とベストプラクティスを含んでいる点で汎用性が高いといわれている[47]。

各組織は NIST フレームワークを活用することでそれぞれのサイバーセキュリティの取組を分析し、常に変化するサイバーリスクに対し、組織にあわせたリスク管理のもと、継続的に取組を改善することが可能となる。

NIST フレームワークは「フレームワーク・コア」、「フレームワーク・インプリメンテーション・ティア」および「フレームワーク・プロファイル」の 3 つで構成されている（図表 28 参照）。

それぞれの関係は、①のフレームワーク・コアが NIST フレームワークの中心であり、このコアで示された項目の組織の達成度合いを測るスケールが②のフレームワーク・インプリメンテーション・ティアである。これらを用い、③のフレームワーク・プロファイルにおいて各組織で求められる成果を示し、運用するという構成となる。

図表 28　NIST フレームワークの構成

①フレームワーク・コア ・全ての重要インフラ分野に共通するサイバーセキュリティ対策のベストプラクティス、求められる成果および参考情報をまとめたもの

[45] 本稿 3.（2）e 参照
[46] 直近版は 2017 年 12 月 5 日に公表された 2nd Draft である
[47] NIST フレームワークの性格上、同フレームワークは、個別のサイバーリスクについて具体的な対策を示しているものではないことに留意する必要がある。

・経営レベルから実務・運用レベルまでの組織全体で共有する
②フレームワーク・インプリメンテーション・ティア
・組織のサイバーセキュリティリスク管理の取組が、NIST フレームワークで示される特性をどの程度まで達成できているかを示すもの
・4 段階で示す
③フレームワーク・プロファイル
・組織がフレームワーク・コアから選択した、各組織に応じた求められる成果を示す
・現在の状況と目標の状態を比較し、改善対策の機会を特定する

（出典：NIST フレームワーク Ver1.0 をもとに作成）

a. フレームワーク・コア

NIST フレームワークは、サイバーセキュリティを把握・管理および表現するための「共通言語」（common language）を提供するもので、サイバーセキュリティリスクを低減させるための行動の特定と優先順位付けのために利用される。

フレームワーク・コア（以下「コア」）は、NIST フレームワークの中で、サイバーセキュリティ対策を達成するための活動の組み合わせと、達成のための参考情報をまとめたもので、文字通り、同フレームワークのコアとなる部分である（図表 29 参照）。

コアの横軸には機能、カテゴリー、サブカテゴリー、参考情報[48]の 4 つの要素（図表 30 参照）があり、また、このうちの機能は、さらに特定、防御、検知、対応、復旧の 5 つに分類（図表 31 参照）され、コアの縦軸に表示される。

図表 29　コア一覧（概要）

機能	カテゴリー	サブカテゴリー
特定	＜資産管理＞ 組織が事業目的を達成することを可能とするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している	・組織内の物理的なデバイスとシステムの一覧表を作成している ・企業内のソフトウエアプラットフォームとアプリケーションの一覧を作成している ・企業内の通信とデータのフロー図がある ・外部情報システムの一覧を作成している等
	＜ビジネス環境＞ 組織のミッション、目標、利害関係者および活動を理解し優先付けを行っている	・サプライチェーンにおける組織の役割を特定し伝達している ・組織のミッション、目標、活動に関して優先順位を決め伝達している等
	＜ガバナンス＞ 組織に対する規制、法律、リスクと組織の環境、運用上の必要事項を管理し、モニタリングするためのポリシー、手順、プロセスを理解し、サイバーセキュリティリスク管理者に伝達している	・情報セキュリティポリシーを策定している ・情報セキュリティ上の役割・責任を組織内外で調整・連携している ・サイバーセキュリティリスクに関する法規制上の要求事項を理解し管理している ・ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している等
	＜リスク評価＞ 組織の業務、資産等に対するサイバーセキュリティリスクを把握している	・資産の脆弱性を特定し文書化している ・情報共有等により脅威と脆弱性に関する情報を入手している等 ・内外からの脅威を特定し文書化している ・事業に関する潜在的な影響とその可能性を特定

[48] 紙面の関係で、図表 29 には参考情報の記載は省略している

機能	カテゴリー	サブカテゴリー
		している ・リスクへの対応を定め優先順位付けしている等
	＜リスク管理戦略＞ 組織の優先順位、制約、リスク許容度、想定を定めている	・リスク管理プロセスが関係者において確立、管理され、承認されている ・組織のリスク許容度を決定し明確にしている等
防御	＜アクセス制御＞ 資産および関連施設へのアクセスについて、承認された利用者、プロセス、デバイスおよび承認された活動、取引に限定している	・承認されたデバイスと利用者の識別情報と認証情報を管理している ・資産に関する物理アクセスおよびリモートアクセスを管理している ・権限最小化および職務分離の原則を取り入れている等
	＜意識向上およびトレーニング＞ 職員等に対し、情報セキュリティに関連する義務と責任を果たすためのサイバーセキュリティ意識向上教育と十分なトレーニングを行っている	・全ての利用者へ情報周知している ・権限者、第三者である利害関係者、上級役員およびセキュリティ担当者等が役割と責任を理解している等
	＜データセキュリティ＞ 情報の機密性、完全性、可用性を保護することを定めたリスク戦略に従い、情報およびデータを管理している	・保存データおよび伝送データを保護している ・資産の撤去、譲渡および廃棄プロセスを管理している ・可用性確保に十分な容量の確保をしている ・データ漏えいに対する保護対策を講じている等
	＜情報保護のプロセスと手順＞ セキュリティポリシー、プロセス、手順を維持し、情報システムと資産の保護管理に使用している	・情報技術および産業用制御システムのベースラインとなる設定を定めている ・システム開発ライフサイクルを導入している等
	＜保守＞ 制御システムおよび情報システムの保守と修理はポリシーと手順に従って実施している	・資産の保守と補修は、承認・管理されたツールを用いてタイムリーに実施し、記録を残している ・遠隔保守は、承認を得て行い記録を残している等
	＜保護技術＞ ポリシー、手順、契約に従い、システムと資産のセキュリティ・耐性・復旧力を確保するための技術的なソリューションを管理している	・ポリシーに従って監査記録やログの記録保存方法を文書化し、実行し、レビューしている ・最小機能の原則を取り入れてシステムと資産へのアクセスを制御している等
検知	＜異常とイベント＞ 異常な活動をタイムリーに検知し、イベントがもたらす可能性のある影響を把握している	・攻撃の標的と手法を理解するための検知したイベントの分析をしている ・イベントがもたらす影響を特定している等
	＜セキュリティの継続的モニタリング＞ サイバーセキュリティイベントを検知し保護対策の有効性を検証するため情報システムと資産を継続的にモニタリングしている	・発生可能性のあるサイバーセキュリティイベントを検知できるよう、ネットワーク、物理環境、職員および外部サービスプロバイダーの活動をモニタリングしている ・権限のない職員、アクセス、デバイスおよびソフトウエアのモニタリングを実施している ・脆弱性のスキャニングをしている等
	＜検知プロセス＞ 異常なイベントをタイムリーかつ正確に検知するためのプロセスおよび手順を維持し、テストしている	・説明責任を果たせるよう、検知に関する役割と責任を明確に示している ・検知活動は必要な全ての要求事項を満たしている等
対応	＜対応計画の作成＞ 検知したサイバーセキュリティインシデントにタイムリーに対応できるための対応プロセスおよび手順があり、維持されている	・イベント発生中または発生後に対応計画を実施している等

機能	カテゴリー	サブカテゴリー
	＜伝達＞ 内外の利害関係者との間で対応活動を調整している	・職員は対応が必要となったときの役割と行動の順番を認識している ・対応計画に従って情報共有している等
	＜分析＞ 適切な対応と復旧活動を支援するための分析を行っている	・検知システムからの通知を分析している ・インシデントによる影響を把握している ・フォレンジックを実施している等
	＜低減＞ イベントの拡大防止および影響緩和のための活動を実施している	・インシデントを封じ込めている ・インシデントを低減している等
	＜改善＞ 過去の意思決定および対応活動から学んだ教訓を取り入れ、改善している	・学んだ教訓を対応計画に取り入れている ・対応計画を更新している等
復旧	＜復旧計画の作成＞ サイバーセキュリティイベントで影響を受けたシステムや資産をタイムリーに復旧するためのプロセスおよび手順があり、維持されている	・イベント発生中または発生後に復旧計画を実施している等
	＜改善＞ 学んだ教訓を将来の活動に取り入れることで復旧計画等を改善している	・学んだ教訓を復旧計画に取り入れている ・復旧計画を更新している等
	＜伝達＞ 内外の関係者との間で復旧活動を調整している	・広報活動を管理している ・イベント発生後にレピュテーションを回復している等

（出典：NIST フレームワーク Ver1.0 をもとに作成）

図表 30　コアの 4 要素

①機能
・基本的なサイバーセキュリティ対策の最上位を構成する 5 つの要素で、これらの機能によって情報を体系化し、サイバーセキュリティの管理を容易にする
②カテゴリー
・機能をサイバーセキュリティ対策の活動別に細分化したもの
③サブカテゴリー
・カテゴリーを技術的または管理的な活動別に細分化したもの
④参考情報
・重要なインフラに共通の標準、ガイドライン、ベストプラクティスをまとめたもの

（出典：NIST フレームワーク Ver1.0 をもとに作成）

図表 31　コアで示される機能

①特定
・システム、資産、データおよび機能に対するサイバーセキュリティリスクの管理に必要な理解を深める
・業務の背景や重要業務の支援リソースおよび関連するサイバーセキュリティリスクを理解し、活動対象と優先順位付けを可能とさせる
②防御
・重要インフラサービスの提供を確実にするための適切な保護対策を検討し実施する
③検知
・サイバーセキュリティイベントの発生を検知するための適切な対策を検討し実施する
④対応
・検知されたサイバーセキュリティイベントに対処するための適切な対策を検討し実施する
⑤復旧
・強靭性を実現するための計画を策定・維持し、サイバーセキュリティイベントで阻害されたあらゆる機能やサービスを復旧するための適切な対策を検討し実施する

（出典：NIST フレームワーク Ver1.0 をもとに作成）

b. フレームワーク・インプリメンテーション・ティア

フレームワーク・インプリメンテーション・ティア（以下「ティア」）は、コアで示される機能に対して組織のサイバーセキュリティリスク管理がどの程度まで達成できているか[49]を示すものである（図表 32 参照）。

図表 32　フレームワーク・インプリメンテーション・ティア

①ティア 1（部分的である） ・組織のサイバーセキュリティリスク対策は確立しておらず、リスク管理は場当たり的に、場合によっては事後的に対処される ②ティア 2（リスク情報を活用している） ・経営層が承認したリスク管理対策はあるが、組織全体でのポリシーとして確立されていない場合がある ・組織レベルでのサイバーセキュリティリスク意識はあるが、管理するための組織全体の取組は確立されていない ③ティア 3（繰り返し適用可能である） ・組織のリスク管理対策はポリシーとして正式に確立している ・サイバーセキュリティリスクを管理するためのプロセスおよび手順が定義され、想定どおりに実施され、またレビューされている ④ティア 4（適応している） ・組織は過去と現在のサイバーセキュリティ対策から学んだ教訓と予測をもとにサイバーセキュリティ対策を調整する ・サイバーセキュリティリスクを管理するための組織文化があり、外部関係者との情報共有を積極的に行う

（出典：NIST フレームワーク Ver1.0 をもとに作成）

c. フレームワーク・プロファイル

フレームワーク・プロファイル（以下「プロファイル」）は、各組織の要件に基づいて調整したコアである[50]。

具体的には、組織がコアから必要なカテゴリーおよびサブカテゴリーを選択し、これに基づきサイバーセキュリティ対策の現在のプロファイル[51]と、目指す目標のプロファイル[52]を作成する。

各組織では、これらのプロファイルを活用し、対策のロードマップ作成に利用することができる。

（3）NIST フレームワークの活用方法

NIST フレームワークは、組織が実施中のサイバーセキュリティ対策のプロセスに取って代わることを必ずしも想定したものではなく、現行のプロセスを使用しつつ、改善

[49] NIST フレームワークではティアの具体的な活用方法が明示されていないが、後記（3）のサイバーセキュリティプログラムにおいて、各組織の実態に合わせたティアを選択し、プログラムを調整することも可能としている。
[50] 前記 a.のコアで示された機能、カテゴリー、サブカテゴリーをもとに組織の実態に合わせて作成する。そのため、NIST ではプロファイルの雛形は示していない。
[51] 後記（3）図表 33 の③ステップ 3 に該当
[52] 後記（3）図表 33 の⑤ステップ 5 に該当

することも想定している。

同フレームワークで示されている組織のサイバーセキュリティプログラムの確立または改善の手順は図表 33 のとおりであり、このプロセスを必要なだけ繰り返す必要があるとしている。

この中で、コアが直接関係するのは、③のステップ 3 において現在のプロファイルを作成し、④のステップ 4 のリスク評価を経て、⑤のステップ 5 で目標のプロファイルを作成するプロセスである。

また、サイバーセキュリティ対策の達成度合いはティアで測定される。

さらに、⑦のステップ 7 で行動計画を実施する際には、コアの参考情報を活用することができる。

図表 33　サイバーセキュリティプログラムの確立プロセス

①ステップ 1（優先順位付けによる範囲を決定する）
- 組織の業務目的とミッションに照らして経営層による優先事項の決定を行う
- 組織はサイバーセキュリティ実施に関する戦略的な意思決定を行い、対策を講じるべき業務範囲およびシステムや資産の範囲を特定する

②ステップ 2（方向付けをする）
- 関連するシステムと資産、規制上の要求事項および全体的なリスクアプローチを特定する
- 対象となるシステムと資産に関する脆弱性を特定する

③ステップ 3（現在のプロファイルを作成する）
- 組織は、コアのカテゴリーとサブカテゴリーの成果のうち、現時点で達成されているかを示す現在のプロファイルを作成する

④ステップ 4（リスク評価を実施する）
- 組織は、サイバーセキュリティイベントが発生する可能性と、それがもたらす影響を把握する
- 組織の全体的なリスク評価や過去のリスク評価で導きだされる場合もある

⑤ステップ 5（目標のプロファイルを作成する）
- リスク評価結果をもとに、サイバーセキュリティの目標について記載する

⑥ステップ 6（乖離を特定、分析し、優先順位付けをする）
- 現在のプロファイルと目標のプロファイルを比較し乖離を特定する
- 次に、乖離を埋めるために必要なリソースを決定する

⑦ステップ 7（行動計画の実施）
- ステップ 6 で埋めるべき乖離があれば対応すべき行動を決定し、目標のプロファイルに照らして、現在のサイバーセキュリティ対策をモニタリングする

（出典：NIST フレームワーク Ver1.0 をもとに作成）

（4）NIST フレームワークの改訂（Ver1.1）

NIST は 2015 年 12 月に NIST フレームワーク Ver1.0 の利用実態、更新の必要性等について広く情報提供を求め、また、その後のワークショップにおける意見を統合するなどし、2017 年 1 月 10 日に NIST フレームワークの改訂版ドラフトである Ver1.1 を公表[53]した。

[53] NIST は 2014 年 2 月 12 日の NIST フレームワークの公表とあわせ重要インフラのサイバーセキュリティ改善のロードマップ（NIST Roadmap for Improving Critical Infrastructure Cybersecurity）を公表しており、この中で、NIST フレームワークは、「生きた文書」であり、各業界がフィードバックを提

さらにこのドラフトは 2017 年 4 月 10 日まで意見募集[54]され、その後のワークショップなどを経て修正が進み、同年 12 月 5 日に Ver1.1 の 2nd Draft（以下「改訂版」）が公表されている。

NIST はこの改訂版への意見を募集しており、これを踏まえ 2018 年の早い段階で確定版を公表するとしている[55]。

本項では、この改訂版の概要を説明する。

a. 改訂版の概要と位置付け

改訂版は、Ver1.0 の記載内容の文言修正は基本的に行わず、新たな項目の追加のみを行っている。そのため NIST は改訂版と Ver1.0 は互換性を有していると説明している。

改訂版の主要な変更点は図表 34 のとおりである。

図表 34　改訂版の主要な変更点

変更点	変更内容
①サイバーセキュリティ測定用言語の明確化	・業務リスクとサイバーセキュリティリスク管理との関係明確化 ・フレームワークを用いたサイバーセキュリティリスクの自己測定というタイトルを新設し、自己評価における測定の役割に重点を置いて、測定方法を示す
②サプライチェーンのサイバーセキュリティを管理するためのフレームワーク明確化	・関係者間でのサイバーセキュリティ要件の共有により、サプライチェーン内のサイバーセキュリティの管理の理解促進をするための説明の追加
③アクセス制御に関するカテゴリー等の変更	・コアのアクセス制御カテゴリーに、認証および識別証明を追加
④脆弱性開示	・脆弱性開示サイクルに関連するサブカテゴリーの追加

（出典：NIST フレームワーク Ver1.1 をもとに作成）

b. フレームワークを用いたサイバーセキュリティリスクの自己測定

前記 a.図表 34 の①の変更について説明する。

NIST フレームワークは、サイバーセキュリティリスクを組織のリスク許容範囲内に削減させることを目的のひとつとしている。

その一方で、サイバーセキュリティ対策への経営判断を求めるには、同対策への投資の有効性と優先順位を示す必要がある。

そのためには、組織の目標と目標達成に関係するサイバーセキュリティ対策の成果との関係を明確に示す必要があるが、今回の改訂で、NIST フレームワークの測定値を

供する中、引き続き更新され、改善されるとしている。

[54] 意見は 129 件寄せられ、保険業界としては全米保険協会（AIA）が、「改訂版は情報セキュリティプログラムの強化につながる。我々はサイバーセキュリティ測定の促進がどのようにサイバーセキュリティ対策の効率化につながるのか期待している」旨の意見表明をしている。

[55] NIST は利用者に対し、改訂版の確定を待つことなく適宜利用しても差し支えないと説明している。

活用しサイバーセキュリティ対策の成果の自己評価を補助することができることが説明され、対策への投資の有効性を検証する一助となるとしている。

具体的な変更箇所としては、図表 35 で示した項目がティアに追加され、組織の目標との相関を評価することなどが示されている。

今回の改訂で、サイバーセキュリティ対策を組織の目標と対比させることを通してサイバーセキュリティ対策の実効性をあげていくという方向性が示されたことは注目すべき点[56]である。

NIST フレームワークは各業界のフィードバックに伴い更新、改善されるという位置付けであり、今後事例を重ねていくことで内容が充実されると思われる。

サイバーセキュリティ対策が組織の目標との相関で評価されることが進めば、各組織ではサイバー保険のコストを含めた費用対効果について内外への説明責任がより求められることになると考えられる。

図表 35　ティアの追加箇所

①ティア 2（リスク情報を活用している）
- 事業目標におけるサイバーセキュリティの考慮は、組織の一定レベルでは認められるが、全てのレベルでは認められない。資産へのサイバーリスク評価は非定期である

②ティア 3（繰り返し適用可能である）
- 資産に対するサイバーセキュリティリスク評価を定期的に行っている
- 上級サイバーセキュリティ担当役員とその他の役員はサイバーセキュリティリスクに関して定期的に情報交換している
- 上級管理職は、組織内のサイバーセキュリティを考慮している

③ティア 4（適応している）
- サイバーセキュリティリスクと業務目標との関係は機関決定の際に明確に理解され考慮されている
- 上級役員はサイバーセキュリティリスクを財務リスクやその他の組織リスクと同列に監視し、組織の予算は現在および将来予想されているリスク環境およびリスク選考の理解に基づき策定されている
- 事業単位は経営陣の指示を実現し、組織のリスク許容範囲のもとシステムレベルのリスクを分析している
- 組織は業務目標、脅威と技術の変化について、リスクベースで迅速かつ効率的に説明できる

（出典：NIST フレームワーク Ver1.1 をもとに作成）

c. サプライチェーンに関するフレームワークの明確化

前記 a.図表 34 の②サイバーサプライチェーンリスク管理（以下「サイバーSCRM」）を目的としたフレームワークの明確化について説明する。

サイバーセキュリティ上の必要事項に関する利害関係者との連携については、既に NIST フレームワーク Ver1.0 で示されているが、今回、サプライチェーンに関する記

[56] 2017 年 1 月に発表された改訂版 1stDraft では、サイバーセキュリティ対策投資と成果の相関を測ることを目的とし、概念的ではあるが、その測定方法を示していたが、具体的な運用方法が示されていない等の意見が寄せられ、2nd Draft においてトーンダウンした記載となっている。

載が大幅に拡充された。

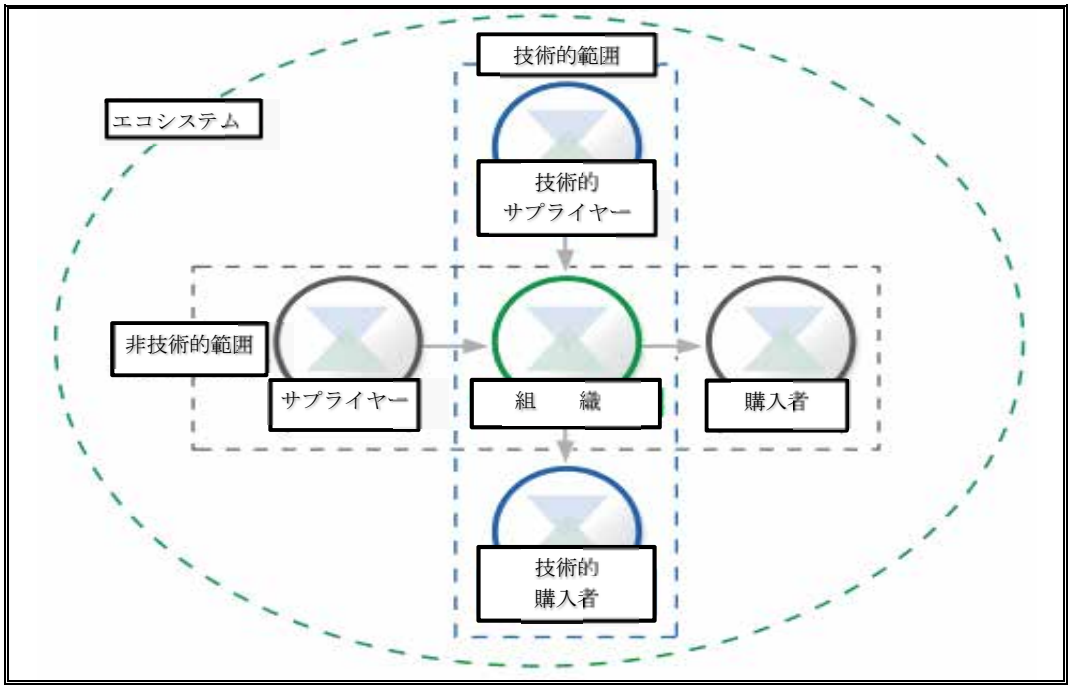
NIST フレームワークでのサイバーSCRM の活動範囲は図表 36 のとおりであり、これらは組織のサイバーセキュリティ・エコシステムを構成している。

購入者とは組織から特定の製品またはサービスの提供を受けるものを指し、サプライヤーとは組織内の利用に限らず、購入者へ提供する製品等にも利用される製品等を提供するものを指す。

なお、これらの関係者は、技術的ベースのあるもの例えば IT ベンダーなどと、技術的ベースに関係しないもの例えば事務用品ベンダーなどとに分けられるが、いずれもがこのエコシステムの範囲内となる。

サイバーSCRM に求められる対応として、コア一覧[57]に図表 37 のカテゴリーが追加[58]され、サプライチェーンおよび関連リスクの管理が明確となっている。

図表 36　サイバーサプライチェーン関係表



（出典：NIST フレームワーク Ver1.1 をもとに作成）

図表 37　コアー覧（サイバーSCRM の追加）

機能	カテゴリー	サブカテゴリー
特定	＜SCRM＞ サプライチェーンリスク管理および関連付けたリスクの確定を支援するため、組織における優先事項、制約、リスク許容度、予測が確立され使用されている。	・サイバーサプライチェーンのリスク管理プロセスが識別、確立、評価、管理され、組織のステークホルダーの合意を得ている ・サイバーサプライチェーンのリスク評価プロセスにおいて利用される重要な情報システムと関

[57] 前記（2）a.図表 29 参照

[58] これにあわせ、ティアの全ての階層において、サイバーSCRM に関する評価が追加されている。

機能	カテゴリー	サブカテゴリー
	組織はサプライチェーンリスクを識別、評価、管理するプロセスを確立している	連装置、サービスのサプライヤーやパートナーの識別、優先順位付け、評価がされている ・サプライヤーとパートナーは、契約で求められた事項のもとで、情報セキュリティプログラムまたはサイバーSCRM の目的に沿った適切な措置を講じている ・要求事項の履行状況についてサプライヤーとパートナーへのモニタリングをし、サプライヤーとパートナーの監査、テストの要約結果、またはその他の評価をレビューしている ・重要なサプライヤーやパートナーとともに、対応および復旧計画とテストが実施されている

（出典：NIST フレームワーク Ver1.1 をもとに作成）

d. アクセス制御に関するカテゴリー等の変更

前記 a.図表 34 の③アクセス制御に関するカテゴリー等の変更は図表 38 のとおりである。

コア一覧の「防御」＜アクセス制御＞[59]の記載内容をもとに、今回追加された箇所を下線で示した。

これにより、識別情報および利用者等の認証管理が明確となっている。

図表 38　コア一覧（アクセス制御に関する変更）

機能	カテゴリー	サブカテゴリー
防御	＜識別管理、認証およびアクセス制御＞物理的、論理的資産および関連施設へのアクセスについては、承認された利用者、プロセス、デバイスおよび承認された活動、取引に限定し、また、非承認の活動と取引による非承認アクセスに関するリスク評価も含め、一貫して管理される	・承認されたデバイスと利用者の識別情報と認証情報を管理している ・資産に関する物理アクセスおよびリモートアクセスを管理している ・権限最小化および職務分離の原則を取り入れている ・識別情報は証明がされ、証明書と一致し、必要に応じ相互に確認可能である ・処理のリスクに合致した利用者、デバイスおよびその他の資産が認証されている

（出典：NIST フレームワーク Ver1.1 をもとに作成）

[59] 前記（2）a.図表 29 参照

＜参考資料＞

・牛窪賢一「サイバーリスクとサイバー保険－米国の動向を中心として」損保総研レポート第 116 号（損害保険事業総合研究所、2016.7）
・牛窪賢一「米国におけるサイバー保険の動向」損保総研レポート第 120 号（損害保険事業総合研究所、2017.7）
・NTT データ経営研究所「金融機関のサイバーセキュリティ対策における経営陣・CISO 等に期待される役割・責任に関する調査結果」（2017.3）
・川口貴久「米国におけるサイバー抑止政策の刷新－アトリビューションとレジリエンス」KEIO SFC JOURNAL - Vol.15（慶應義塾大学湘南藤沢学会、2015.12）
・金融庁「金融分野におけるサイバーセキュリティ強化に向けた取組方針について」（2015.7）
・経済産業省、情報処理推進機構「サイバーセキュリティ経営ガイドライン解説書」（2016.12）
・経済産業省、情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver2.0」（2017.11）
・経済産業省「IoT セキュリティ総合対策」（2017.10）
・経済産業省「IT 人材の最新動向と将来推計に関する調査結果」（2016.6）
・関啓一郎「サイバーセキュリティ基本法の成立とその影響」知的資産創造 2015 年 4 月号（野村総合研究所、2015.4）
・内閣サイバーセキュリティセンター「サイバーセキュリティ対策の強化に向けた対応について」（2016.11）
・内閣サイバーセキュリティセンター「サイバーセキュリティ戦略と重要インフラ防護等の取組」（2016.2）
・内閣サイバーセキュリティ戦略本部「サイバーセキュリティ人材育成プログラム」（2017.4）
・内閣サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」（2014.5）
・内閣サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（2017.4）
・内閣府「企業経営のためのサイバーセキュリティの考え方」（2016.8）
・内閣府「サイバーセキュリティ戦略」（2015.9）
・中沢潔「トランプ政権におけるサイバーセキュリティ政策の現状」ニューヨークだより（情報処理推進機構、2017.9）
・日本銀行金融機構局「サイバーセキュリティに関する金融機関の取り組みと改善に向けたポイント」（2017.10）
・三菱総合研究所「米国のセキュリティ情報共有組織（ISAC）の状況と運用実態に関する調査」（2010.3）
・八山幸司「米国等のサイバーセキュリティに関する動向」（情報処理推進機構、2015.3）
・八山幸司「米国におけるサイバーセキュリティの人材育成と内部脅威に関する取り組みの現状」ニューヨークだより（情報処理推進機構、2016.1）
・PwC「グローバル情報セキュリティ調査 2016（日本版）」（2016.11）
・PwC「グローバル情報セキュリティ調査 2017（日本版）」（2017.11）
・PwC「サイバーセキュリティのための情報共有分析機関（米国 ISAO）に関する調査分析結果および提

言」（2015.7.14）
・PwC「諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書」（2015.3.31）
・矢野薫「日本企業が目指すべきサイバーセキュリティのグローバル標準」DIAMOND　IT&ビジネス（ダイアモンド社、2015.11）
・山下潤「米国のサイバー・インシュアランスの動向」損保総研レポート第 110 号（損害保険事業総合研究所、2015.1）
・和田恭「米国におけるサイバーセキュリティ政策の最新の動向（前編）」ニューヨークだより（情報処理推進機構、2013.4）
・和田恭「米国におけるサイバーセキュリティ政策の最新の動向（後編）」ニューヨークだより（情報処理推進機構、2013.5）
・Computerworld, “IT Salary Survey 2017”（2017.4）
・Cybersecurity Ventures, “2017 Cybersecurity Jobs Report”（2017.5）
・ISACA ,“ISACA Journal Volume 5”（2016.10）
・ISACA ,“ISACA Journal Volume 20”（2017.10）
・ISACA ,“State of Cyber Security2017”（2017.1）
・National Institute of Standards and Technology（NIST）,“Draft NISTIR 8193, National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles”（2017.11）
・National Institute of Standards and Technology（NIST）,“Framework for Improving Critical Infrastructure Cybersecurity Ver.1.0”（2014.2）
・National Institute of Standards and Technology（NIST）,“Framework for Improving Critical Infrastructure Cybersecurity Ver.1.1Draft2”（2017.12）
・National Institute of Standards and Technology（NIST）, “National Initiative for Cybersecurity Education（NICE）Cybersecurity Workforce Framework”（2017.8）
・National Institute of Standards and Technology（NIST）, “NIST Roadmap for Improving Critical Infrastructure Cybersecurity”（2014.2）
・PwC, “ The Global State of Information Security Survey2018”（2017.10）
・The International Association of Insurance Supervisors (IAIS), “Issues Paper on Cyber Risk of The Insurance Sector”（2016.4）

＜参考ウェブサイト＞

・共同通信社　http://www.kyodonews.jp/
・金融 ISAC　http://www.f-isac.jp/
・金融庁　http://www.fsa.go.jp/
・経済産業省　http://www.meti.go.jp/
・情報処理推進機構（IPA）　https://www.ipa.go.jp/

・総務省　http://www.soumu.go.jp/
・損害保険事業総合研究所　https://www.sonposoken.or.jp/
・内閣サイバーセキュリティセンター（NISC）　http://www.nisc.go.jp/
・日本経済新聞社　https://r.nikkei.com/
・日本損害保険協会　http://www.sonpo.or.jp/
・日本ネットワークセキュリティ協会　http://www.jnsa.org/
・日本品質保証機構（JQA）　https://www.jqa.jp/
・American Insurance Assosiation（AIA）　http://www.aiadc.org/
・Burning Glass Technologies　http://burning-glass.com/
・Center of Internet Security（CIS）　https://www.cisecurity.org/
・CompTIA　https://www.comptia.org/
・Cyber Complex　https://www.cybercompex.org/
・Cyber Threat Intelligence Integration Center（CTIIC）　https://www.dni.gov/index.php/ctiic-home
・CyberSeek　http://cyberseek.org/
・Federal Bureau of Investigation Internet Crime Complaint Center（IC3）　https://www.ic3.gov/
・Federal Bureau of Investigation（FBI）　https://www.fbi.gov/
・Financial Services Information Sharing and Analysis Center（FS-ISAC）　http://www.fsisac.com/
・Financial Times　https://www.ft.com/
・Institute of Internal Auditor（IIA）　https://na.theiia.org/Pages/IIAHome.aspx/
・ISACA　http://www.isaca.org/
・ISAO Standards Organization（ISAOSO）　https://www.isao.org/
・National Council of ISACs（NCI）　https://www.nationalisacs.org/
・National Cybersecurity Center of Excellence（NCCoE）　https://nccoe.nist.gov/
・National Institute of Standards and Technology（NIST）　https://www.nist.gov/
・National Integrated Cyber Education Research Center（NICERC）https://nicerc.org/
・National Security Agency（NSA）　https://www.nsa.gov/
・PwC　https://www.pwc.com/
・Reuters　https://www.reuters.com/
・The CAE Community　https://www.caecommunity.org/
・U.S. Strategic Command（USSC）　http://www.stratcom.mil/
・United States Department of Homeland Security（DHS）　https://www.dhs.gov/
・University Enterprises Corporation（UEC）　http://uec.csusb.edu/
・US Cyber Challenge　http://www.uscyberchallenge.org/
・US-CERT　https://www.us-cert.gov/
・White House　https://www.whitehouse.gov/
・White House President Barac Obama　https://obamawhitehouse.archives.gov/