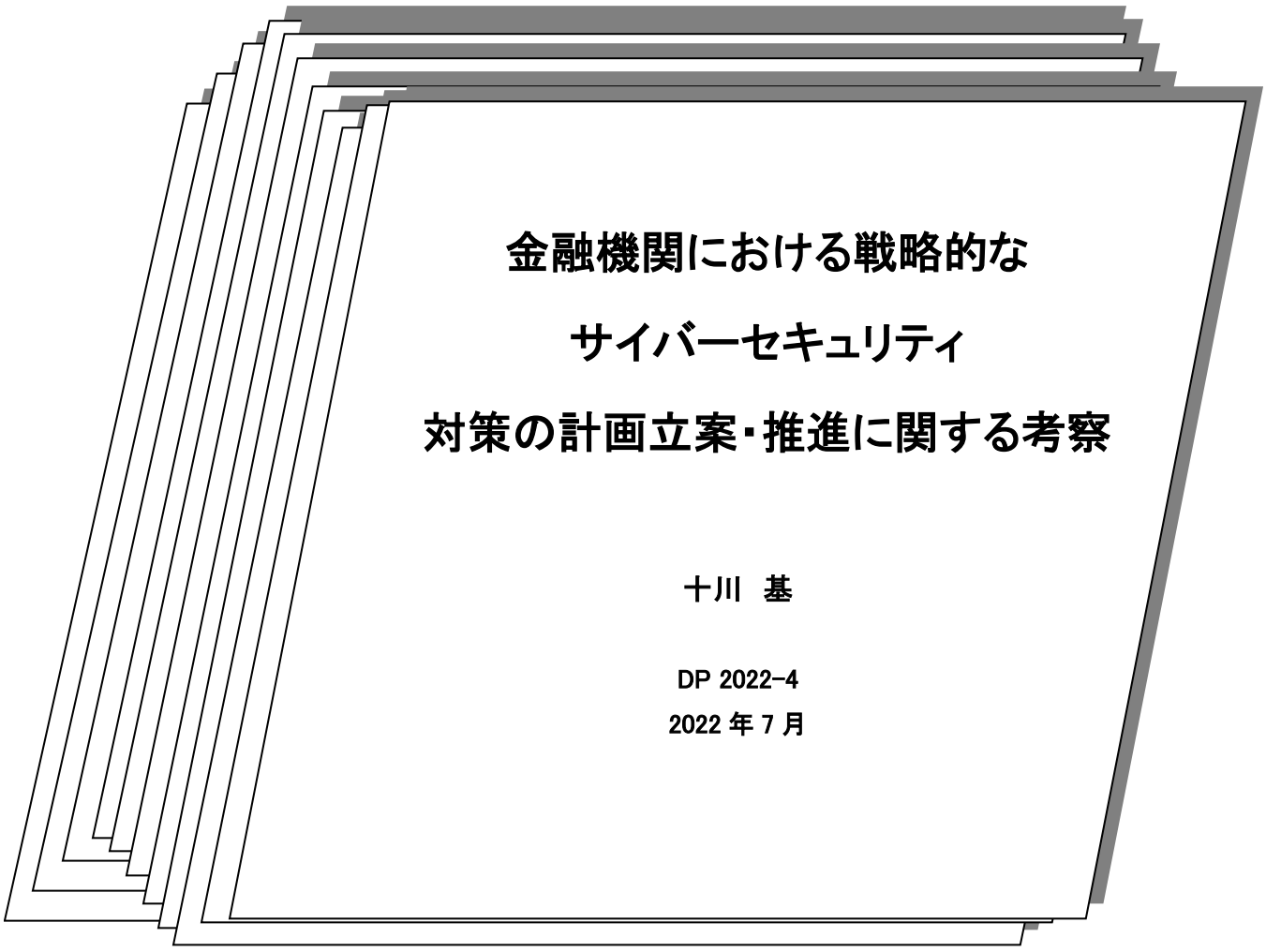
FSA Institute
Discussion Paper Series



金融機関における戦略的な
サイバーセキュリティ
対策の計画立案・推進に関する考察

十川　基

DP 2022-4
2022 年 7 月

金融庁金融研究センター
Financial Research Center (FSA Institute)
Financial Services Agency
Government of Japan

＜金融庁金融研究センター　ディスカッションペーパー DP2022-4（2022 年 7 月）＞

金融機関における戦略的なサイバーセキュリティ対策の計画立案・推進に関する考察

十川　基*

概　　要

近年、サイバーセキュリティに関する脅威は増加しており、国家の関与が推察されるような、長期間にわたる入念な探索や高度な技術が用いられる攻撃も発生している。金融機関は IT を活用し、多くの個人情報や金融資産等を管理しているため、サイバー攻撃の標的になりやすく、被害が発生してしまうケースが少なくない。そのため、サイバーリスクマネジメントは、金融機関における経営課題の中でも重要なテーマの一つとなっている。しかしながら、金融機関は数多くのシステムやサービスを複雑に連携しているため、絶えず変化するサイバー攻撃に対して整合性のとれた網羅的なサイバーセキュリティ対策を迅速に実現することが難しい。そこで本稿では、政府や金融機関等に関連するサイバーインシデントの傾向及び近年の概況と、金融機関のサイバーセキュリティ対策に役立つ文献を調査し、各文献の特徴を取りまとめた。そして、それらを活用して各金融機関に必要なサイバーセキュリティ対策を分析し、その計画立案と推進を行うための具体的な手法の提言を行い、金融機関が自律的にサイバーセキュリティ対策の高度化を継続的に実施できるように解説する。

キーワード：サイバー攻撃、サイバーセキュリティ対策、戦略立案

＊　金融庁金融研究センター研究官

本稿の執筆にあたっては、吉野直行金融研究センター長及び三浦俊調整官、明生拓史総括をはじめとする多くの金融庁スタッフに有益なご意見をいただいた。ここに記して感謝したい。

１．はじめに

近年は、デジタル技術を活用してサービスの付加価値を高めるデジタライゼーションや、ビジネスモデルそのものをデジタル技術で変革するデジタルトランスフォーメーション(DX)が金融業界でも活発化しており、顧客への利便性の向上が期待されている。その一方で、これらの新たなサービスや技術もサイバー攻撃の対象となるため、これまで以上にサイバーセキュリティを十分に考慮した計画や運用が必要となる。

昨今のサイバー攻撃の主な目的は、個人情報や組織の機密情報の窃取、機能停止や改ざんによる妨害、金銭の窃盗や要求等で、攻撃の特徴として、標的企業に対して組織的かつ執拗に攻撃が行われていることが挙げられる。そして、多くの個人情報や金融資産等を保有し、IT を活用している金融機関がその標的となる事案が発生している。また、近年では国家が関与していると推察されるような、長期間にわたる入念な探索や高度な技術が用いられる攻撃も発生しており、サイバーセキュリティに関する脅威は年々増加している。

組織におけるリスク全般の管理の観点では、組織に発生するあらゆるリスクを統合・包括・戦略的に把握し、評価・最適化する、統合的リスク管理が浸透し、リスクマネジメント態勢の一元化が進みつつある。サイバーセキュリティにおけるリスクマネジメントにおいても、特定の事業部門が活用している IT サービスの利用部署や組織の IT 部門に限定した責任とするのではなく、組織の目標に沿って全体的な整合性を取りながら最適化することが求められている。このことは、日本経済団体連合会が公開している「サイバーリスクハンドブック 取締役向けハンドブック 日本版」[1]の原則 1 に「取締役は、サイバーセキュリティを、単なる IT の問題としてではなく、全社的なリスク管理の問題として理解し、対処する必要がある。」と明記しており、サイバーリスクマネジメントは、経済活動を行うすべての組織に関係する重要なテーマの一つであると考えている。

そこで本稿では、増大しつつあるサイバー脅威を正確に認識し、適切にマネジメント出来るように、近年のサイバーインシデントの傾向や、各金融機関が戦略的なサイバーセキュリティ対策の計画立案とその推進を行うために役立つ文献や実践方法について調査を行い、その具体的な手法をまとめた。

各金融機関で戦略的なサイバーセキュリティ対策の立案ができれば、現在のサイバー脅威に対して有効性が不明確なセキュリティ製品やサービスに惑わされることなく、必要十分で効果的な施策により、高いセキュリティレベルを維持することが期待できる。また、サイバーインシデントが発生した場合においても、その対応や復旧等の態勢を平時のうちから適切に整えていれば、有事の際に迅速かつ的確に対応することで被害を極小化することができると考えている。本論文が、金融機関の戦略的なサイバーセキュリティ対策の計画立案の一助になることを願う。

本稿の構成は次のとおりである。まず、第 2 章において、サイバー攻撃の歴史と近年の動向について示し、第 3 章において、代表的な金融機関向けのサイバーセキュリティに関する基準やガイドライン等を紹介し、それぞれの特徴に基づいて分類を行い、 第 4 章にお

いて、戦略的なサイバーセキュリティ対策の計画立案方法について提言し、そして第 5 章では、継続的なサイバー計画のモニタリングについて解説し、最後の第 6 章において、まとめと今後の課題を示す。

２．サイバー攻撃の歴史と近年の動向

サイバー攻撃は、図 1 に示す様に、以前は個人による単純ないたずらや自己顕示欲を満たすために行われていたが、昨今では、国家が関与していることが示唆される攻撃や、組織的な活動と考えられる攻撃が発生し、その目的も悪質化している。

各組織がこれらのサイバー攻撃に対応するためにセキュリティ対策を行い、サイバー攻撃への検知や防御力を向上させると、攻撃者はセキュリティ対策製品・サービスによる検知を回避するための動作や、活動の痕跡を辿られなくするためにシステムの操作履歴等が記録されているログファイルを削除する等、より巧妙な攻撃も見受けられるようになった。また、業務の全面的なデジタル化に伴い、被害が発生すると手作業等による代替手段で実施できる業務に限りがあるため、業務そのものが立ち行かなくなり、顧客や取引先等のステークホルダーに多大な影響を与えてしまうおそれがある。そのことに付け込み、機密情報を盗み出し、システムを停止し、そのシステムの復旧や機密情報を暴露しない見返りとして金銭を要求するランサムウェア攻撃が多く発生している。また、企業や国家の機密情報を盗み出すためのスパイ活動も数多く行われ、日米英欧等が共同でそれらの活動を行ったと考えられる特定の国家を名指しで非難した[1)]。直近では、ロシアによるウクライナ侵攻が開始される前後に、ウクライナ政府機関等のシステムの停止・破壊を狙ったマルウェア等の攻撃により、同国ではサイバー空間においても多数の被害が発生した。そしてその報復としてロシアでも同様に被害が発生した。

ダボス会議として世界的に有名な世界経済フォーラムの年次総会では、サイバー脅威は経済社会に与える影響が大きいことから、重要なテーマの一つとして近年では常に取り上げられ、グローバルリスク報告書[2]にもそのリスクや影響について詳細に記載されており、サイバーセキュリティを取り巻く環境はより厳しくなる傾向が続いている。

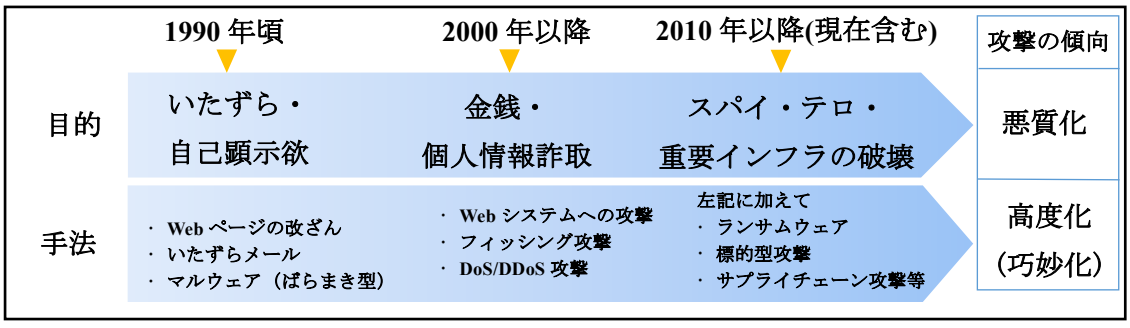


図 1　サイバー攻撃の変遷

1) https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

２．１　2010 年以降における政府・金融機関へのサイバー攻撃事例

サイバー攻撃が深刻化してきた 2010 年以降の政府や金融機関に関係のある主要なセキュリティインシデントを表 1 にまとめた。表に示されているように、金銭的な被害だけではなく、個人情報や機密情報等の窃取やシステムの停止等の被害も発生している。

そして、近年では標的とする企業に対して直接不正アクセスを試みるだけではなく、グループ会社や取引先、利用しているソフトウェアやクラウドサービスの脆弱性等を経由して不正アクセスされる、サプライチェーン攻撃により多数の企業で甚大な被害が発生しているという特徴がある。

金融機関特有のサイバー攻撃の主な目的としては、証券、保険、貸金、資金移動業等では、個人情報に加えて登録されている口座情報及びその認証情報等の窃取が含まれる。銀行、信用金庫等の預金取扱等金融機関等では上記に加えて口座に預けた現金等の窃取(不正送金)が含まれる。

表 1　2010 年以降の各国の政府および金融機関に関係のある主要なインシデント[2)]

時期	概要
2010 年 1 月	**オーロラ作戦(Operation “Aurora”）による知的財産の窃取** 中国のハッキンググループの関与が疑われる、Internet Explorer の脆弱性を狙ったサイバー攻撃により、金融、テクノロジー、メディア、化学など様々な分野の大企業から知的財産等が窃取された。
2010 年 11 月	**マルウェアによるイランの核関連施設への攻撃** イランのウラン濃縮施設にある閉域ネットワーク内のシステムが、USB ストレージ経由にてマルウェア「Stuxnet」に感染、秘密裏に同施設の遠心分離機を誤作動させ、約 1,000 台が物理的に破壊された。
2015 年 5 月	**日本年金機構における標的型メール攻撃による個人情報の流出** 日本年金機構が標的型メールにより、年金管理システムに保管されていた 125 万件の加入者の個人情報(基礎年金番号、氏名、生年月日、住所)が漏洩した。
2016 年 2 月	**バングラデシュ中央銀行における不正送金** バングラデシュ中央銀行が不正アクセスを受け、SWIFT システムを通じて不正送金された。被害額は約 8,100 万ドル。
2017 年 5 月	**ランサムウェア「WannaCry」によるデータの暗号化と身代金の要求** マルウェアに感染した端末が、ネットワークに接続された他の端末にも感染を広げる自己増殖型のマルウェアにより、日本を含む約 150 か国の政府機関、医療機関、企業等がデータを暗号化され身代金を要求された。
2017 年 9 月	**米国信用情報会社からの個人情報漏洩** 米国信用情報会社「エクイファクス」が不正アクセスを受け、米国民約 1 億 4,500 万人分の個人情報（氏名、生年月日、社会保障番号、住所、免許証番号、（一部）クレジットカード番号）等が窃取された。

2) 各種報道に基づき筆者が作成。

時期	概要
2018 年 1 月	**コインチェックの暗号資産取引所への不正アクセスによる暗号資産流出** コインチェックのホットウォレットに保管されていた暗号資産のネム(NEM)が外部からの不正アクセスを受け、580 億円相当が窃取された。
2019 年 9 月	**みずほ銀行 J-Coin Pay への不正アクセスによる情報漏洩** みずほ銀行がサービス提供を行う「J-Coin Pay」の加盟店管理に関わるテスト用システムが不正アクセスを受け、加盟店に関する情報(1 万 8,469 件)が流出した可能性のある事案が発生した。
2020 年 1 月	**三菱電機からの防衛機密情報漏洩** 三菱電機のグループ海外拠点が不正アクセスを受け、その拠点の不正アクセスをきっかけに防衛省の定める注意情報に該当する情報や企業の機密情報、個人情報等が流出した。
2020 年 8 月	**ニュージーランド証券取引所 DDoS 攻撃による一時取引停止** ニュージーランド証券取引所(NZX)がサイバー攻撃(DDoS)を受け、4 日連続で取引を一時中断する事態に追い込まれた。
2020 年 9 月	**ドコモ口座を悪用した不正送金** 悪意ある第三者が NTT ドコモの電子決済サービス「ドコモ口座」の口座開設や口座振替時の認証の弱さを悪用し、銀行口座の預金者になりすまして、銀行口座からドコモ口座へ不正な送金を行った。被害総額は約 2,885 万円。
2020 年 12 月	**Solar Winds 社製品を介した大規模サプライチェーン攻撃** Solar Winds 社製の IT 管理・監視ツール「Orion」の更新プログラムを悪用した大規模な攻撃が発生し、米政府機関やテクノロジー企業を中心とした多くの民間企業が侵害され、電子メールの盗聴や社外秘のツールの窃盗等の被害が発生した。
2021 年 4 月	**日産証券への不正アクセス** オンライントレードシステムが不正アクセスされ、ファイルが暗号化されたため、オンライン取引を停止。注文はコールセンターで代替した。
2021 年 5 月	**内閣サイバーセキュリティセンター(NISC)への不正アクセス** NISC が利用していたプロジェクト情報共有ツールへの不正アクセスにより、情報が外部に流出した。
2021 年 5 月	**仏　AXA から個人情報漏洩** 医療情報や銀行口座情報等の個人データ（3TB 分）を窃取され、ハッキングフォーラム上に一部のデータが暴露された。また、DDoS 攻撃も同時に実行された。
2022 年 2 月	**ロシアによるウクライナ侵攻に関連するサイバー攻撃** ウクライナとロシアの双方の政府機関や金融・国営企業等で DDoS や新種のマルウェアや不正アクセス等によるサイバー攻撃でシステムの停止や改ざん、情報漏洩等が発生した。

２．２　コロナ禍におけるサイバー攻撃

我が国では、2019 年から発生した新型コロナウイルス感染症(COVID-19)の感染拡大により、生活様式が変化する中、これに便乗したサイバー攻撃が国内外で数多く発生している。表 2 にコロナウイルス感染症に関連した代表的なサイバー攻撃の手法を示す。

メール等を用いた標的型攻撃や、偽の Web サイトに個人情報、クレジットカード番号や口座情報等を入力させ、その情報を詐取するフィッシング詐欺は、コロナ禍以前から存在する典型的な攻撃手法である。しかしながら、これまで経験したことのないコロナ禍という状況により、平時であればそのような攻撃に気づき、回避できていた人も、マスクの供給不足や新型コロナウイルスに関する情報をより多く収集したいという心理から、悪意のあるリンク先や添付ファイルを開き、マルウェアに感染してしまうケースや、不正なサイトに個人情報やクレジットカード番号等を入力してしまい、サイバー攻撃が成立してしまうケースも見受けられた。

また、緊急事態宣言の発令で通勤を含む不要不急の外出を自粛する要請により、金融機関においてもテレワークが急速に普及した。テレワークの普及に伴い、自宅等から社内のシステムにアクセスするための VPN 装置等のテレワーク環境の脆弱性を突いた攻撃が活発となった。VPN 装置はインターネットと社内ネットワークとの接続部分に設置されているため、外部からの攻撃対象になりやすく、VPN 装置への攻撃が成功すると、システム構成によっては機微情報が保管されているシステムへも自由にアクセスされてしまうおそれがあることから、これまで以上にこれらの脆弱性情報を定期的に収集し、セキュリティパッチが公開され次第、速やかに適用する等の対応の必要性が高まった。

表 2　コロナウイルス感染症に関連した世界におけるサイバー攻撃事例

攻撃手法	攻撃事例
メール等を用いた標的型攻撃	国立感染症研究所等の公的機関による情報提供や給付金の配布等を騙り、メール等を用いて特定の個人に対してマルウェアへの感染やフィッシングサイト等に誘導する。
フィッシングサイト	マスクの販売や政府機関の公式ホームページに似せた偽サイトにて、クレジットカード情報や個人情報の詐取を行う。
マルウェア	新型コロナウイルス感染症への対策に役立つアプリケーション等に装い、クレジットカード情報や個人情報の窃取を行う。
ランサムウェア	医療機関や研究所等に対してデータの暗号化やシステムを停止させ、復旧のための身代金を要求する。
DoS・DDoS 攻撃	政府機関やワクチン予約等のシステムに対して機能停止を狙い、不必要な大量のアクセス等の攻撃を行う。
不正アクセスによる情報窃取	医療機関や政府機関、研究所等に対して新しい治療法等の機密情報の窃取を行う。
テレワーク環境を狙った攻撃	在宅ワークやリモートアクセス環境の脆弱性を狙って情報の窃取を行う。

２．３　東京 2020 オリンピック・パラリンピック競技大会に関するサイバー攻撃

東京 2020 オリンピック・パラリンピック競技大会では、海外からの観客の受け入れを見送り、首都圏で開催された競技は無観客による開催となったことも影響したと考えられるが、国内外でサイバー攻撃による目立った混乱は発生しなかった。

大会運営に関わるシステムやネットワークに対しては、競技大会後の大会組織委員会と大会のサイバーセキュリティを担当した NTT が共同で行った記者会見にて、大会期間中に 4 億 5,000 万回のサイバー攻撃を観測したこと、攻撃はすべてブロックされ、大会への運営に影響はなかったこと等を明らかにしている。

国内外の企業や個人をターゲットにしたサイバー攻撃としては、大会関係者等を騙るメールや SNS、フィッシングサイト、オリンピックに関連するマルウェア等、いくつかのパターンが大会期間中及びその前後に観測された。しかしながら、昨今の大規模なサイバー攻撃と比較すると攻撃手法に特筆するようなものはなく、目立った被害は発生しなかった。また、大会期間中に DDoS 攻撃の増加傾向が観測されたが、DDoS 攻撃により重要なシステムが停止に至ったという報道は観測されなかった。五輪チケットの購入者情報に関する漏洩が発生したが、10 件程度で東京オリンピック・パラリンピックの大会組織委員会のシステム外からの漏洩であったことが判明している。

我が国の金融機関では、当庁をはじめとする政府機関等から対策強化を促す要請に基づき、大会が 1 年延長され当初の想定よりも長い期間入念に準備を行っていたこともあり、競技大会に関連するサイバー攻撃の被害は発生しなかった。目立った被害がなかったことは注意喚起や対策要請を受け、対応してきた金融機関からすると予想と異なり、対策が無駄に終わってしまったと感じた関係者もいるかもしれない。しかしながら、大きなイベントの期間中に混乱がなかったのは、攻撃者にとって攻撃が成功する確率や成功することで得られる利益と、事前に対策された組織への攻撃の準備や実行に必要な工数や期間、検挙等のリスクのバランスが見合わなかったことも要因と考えられ、入念に事前に対策を行ったことにより得られた成果の一つだと考えている。

その一方で、大会と関連性がない金融機関等を騙るフィッシングサイトの報告等は、平時と同様に発生しており、大会期間中も注意喚起等が行われていた。サイバー攻撃は特定のイベントの有無に関わらず常に発生し、その攻撃手法や IT そのものも常に進化し続けるため、現在のサイバーセキュリティ対策が今後も有効であり続けるとは限らない。

現在は、ランサムウェアによる被害が多く報道されているほか、一度は沈静化した Emotet(エモテット)[3)]と呼ばれるマルウェアも再び増加し、メールアカウントの乗っ取りやシステムの改ざん等の被害にあう企業も発生している。更に加えて、金融を含む国内の重要インフラ事業者を狙った攻撃が模索されているという情報から、内閣サイバーセキュリ

3) https://www.ipa.go.jp/security/announce/20191202.html

ティセンター(NISC)をはじめとする各省庁からサイバーセキュリティ対策の強化について、注意喚起が行われる等､新たなサイバー攻撃に警戒しながら引き続きセキュリティの維持･向上を行う必要がある。

３．金融機関向けのサイバーセキュリティに関する基準やガイドライン等

前章では、サイバー攻撃の変遷について説明し、攻撃の高度化と悪質化していること等について解説を行い、サイバーセキュリティの維持・向上の必要性を述べた。これらのサイバー攻撃の脅威への適切な対策を検討するための参考となる基準やガイドライン等は、既に国内外に数多く存在している。しかしながら、各組織で取り扱う情報やシステムは業種や業態で異なり、必要なサイバーセキュリティ対策は様々である。その一方、金融業界内では規模や業態が異なる場合でも、業務の進め方やシステム、取り扱うデータに類似性があり、規模や業態等に応じて差はあるものの必要なサイバーセキュリティ対策に共通点が数多くある。そのため、金融機関は金融業に関連する基準やガイドライン等が、その組織にあったサイバーセキュリティ対策の立案に役に立ちやすく､それらを活用することで、自組織のサイバーセキュリティに関する適切な目標設定やギャップ分析等ができる。そこで本章では、国内の金融機関等で活用されている代表的な基準・ガイドライン等の概要について紹介する。

３．１　金融機関等コンピュータシステムの安全対策基準・解説書

公益財団法人 金融情報システムセンターが発刊した、金融機関等コンピュータシステムの安全対策基準・解説書 [3]は、1985 年に策定され、金融機関等の情報システムの安全対策に関する自主基準として公開されており、国内金融機関ではデファクトスタンダードとして広く活用されている。本基準は、目的や利用場面に応じて活用しやすいように体系化しており、「統制基準」「実務基準」「設備基準」「監査基準」の 4 編で構成されている。その記載内容の具体例を挙げると、IT ガバナンスやシステム監査やサイバーセキュリティの観点のみならず、防水、防火措置等、コンピュータシステム全体を安全に活用するための幅広い観点での基準が記載されている。そして、最新の第 9 版では、クラウドやスマートデバイス等の最新の技術にも対応した基準が記載されている。

サイバーセキュリティの観点では、図 2 に示す様に、実務基準に情報セキュリティの大項目が設定されているが、その項目以外にも各項目の関連する箇所でサイバーに関する内容がそれぞれ記載されている。また、安全対策基準・解説書のほかにも「金融機関等におけるコンティンジェンシープラン策定のための手引書」[4)]では、サイバー攻撃を想定した計画を策定するためのコンティンジェンシープランへの考慮事項に加え、態勢整備・平時の

4) https://www.fisc.or.jp/publication/book/000120.php

運用・インシデントレスポンスについてもまとめられており、サイバーインシデントにおける対応復旧計画を検討・策定する際に活用できる。

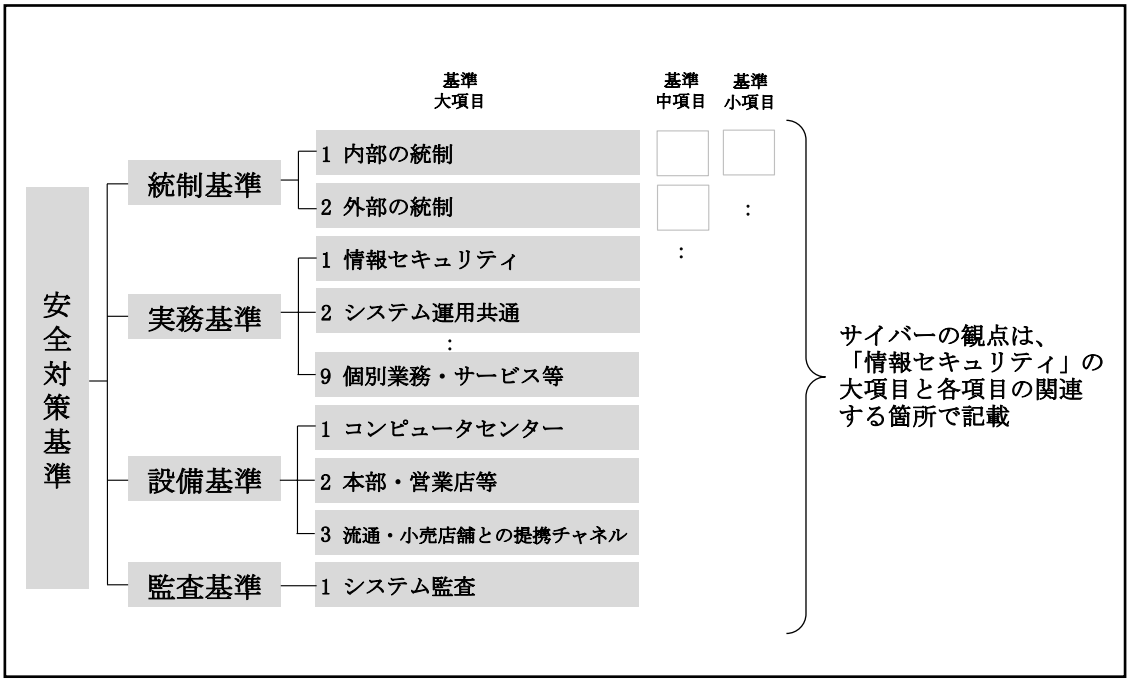


図 2　安全対策基準の構成とサイバーセキュリティの観点の関係

３．２　CYBERSECURITY ASSESSMENT TOOL

CYBERSECURITY ASSESSMENT TOOL(CAT)[5]は、米国連邦金融機関検査協議会(FFIEC)が、金融機関における固有リスクの識別とサイバーセキュリティの成熟度レベルを評価するために公開されているツールである。

本ツールの特徴として、評価対象の金融機関が保有するサイバーセキュリティの固有リスクプロファイルの識別と、その組織のサイバーセキュリティ対策の対応状況が、どの段階にあるかを表すサイバーセキュリティ成熟度の測定という 2 部構成でサイバーセキュリティの対策状況を評価できるように設計されている。そのため、図 3 に示す様に、金融機関は各金融機関が保有する固有リスク(取り扱っている商品・サービスのラインナップ、販売チャネルや態勢等)に合わせて、目指すべきサイバーセキュリティの成熟度と現状との比較や目標設定が可能である。例えば、固有リスクレベルが「軽微」の場合、その企業のリスクアペタイトに応じて、目指すべき成熟度レベルに合わせて「中程度」、「進化途上」、「ベースライン」のいずれかの目標を設定する。一方、固有リスクレベルが最も高い「極めて重大」であった場合は、「革新」若しくは「高度」まで目標を引き上げる必要がある。

5) https://www.ffiec.gov/cyberassessmenttool.htm

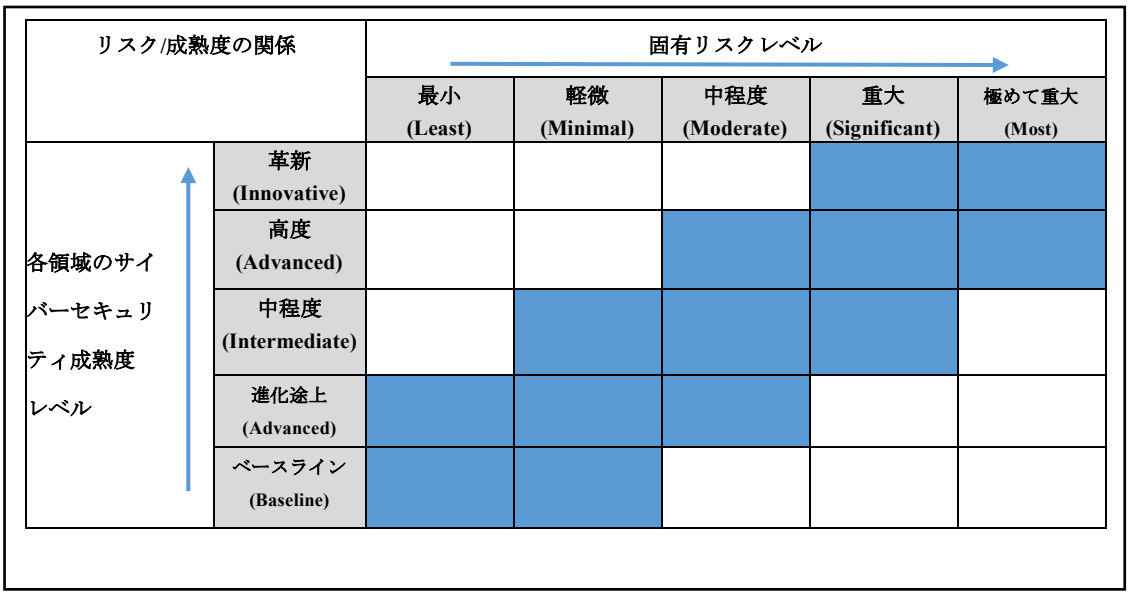


図 3　CAT における固有リスクレベルとサイバーセキュリティ成熟度の関係

米国の多くの金融機関はこのアセスメントツールを活用して、自己評価を始めている。そして我が国の大手金融機関等でも、本アセスメントツールを活用したサイバーセキュリティの評価が行われている。

CAT については金融庁が 2016 年に調査報告書として『FFIEC Cybersecurity Assessment Tool に関する調査研究』 [4]としてまとめているので詳細は本報告書を参照していただきたい。

３．３　Cybersecurity Framework Version 1.1

米国国立標準研究所(NIST)が重要インフラのサイバーセキュリティを改善するために産官学で連携し、「Framework for Improving Critical Infrastructure Cybersecurity Version 1.1」のタイトルで公表された、Cybersecurity Framework(CSF) [5]は、米国のみならず世界的に幅広い組織で活用されている。そして我が国でも情報処理推進機構(IPA)にて「重要インフラのサイバーセキュリティを改善するためのフレームワーク」[6]として翻訳され、重要インフラをはじめ、国内の幅広い業界で組織のサイバーセキュリティ態勢の測定や改善活動に活用されている。

本フレームワークの特徴として「機能」と呼ばれるサイバーセキュリティ対策の構成要素を、「識別」、「防御」、「検知」、「対応」、「復旧」の 5 つに分類している。「機能」の配下には、「カテゴリー」と「サブカテゴリー」がある。また、「参考情報」として、「サブカテゴリー」に該当する他のフレームワークやガイドライン等で関連する項目番号が記載されている。

そして、「サブカテゴリー」に該当するプロセスが存在しているか等を、「ティア」という概念を用いて 4 段階で、ティア 1「部分的である」から、ティア 4「適応している」に分類し、その組織のサイバーセキュリティ態勢がどの程度厳密で、高度なものかを表す。

図 4 にサイバーセキュリティフレームワークのコアの構造とティアのイメージを示す。本フレームワークは、金融業のみならず、電気、水道、物流、通信等の様々な重要インフラ事業のサイバーセキュリティの対策状況を統一的に評価することができるように工夫されている。そのため、本フレームワークは、金融機関が非金融業のグループ会社やサプライチェーンのセキュリティを評価することにも適している。何故ならば、金融業を想定したサイバーセキュリティに関する基準は、金融機関の業務やシステム構成に基づいた記述となっているため金融機関にとっては評価を行いやすいが、非金融業のグループ会社やサプライチェーン等の組織は、業務フローやシステム構成等が異なり、適切に評価することが難しいことがあるためである。また、非金融業に対して、金融業に求められる高いセキュリティ基準を当てはめようとすると、非金融業には受け入れもらえないことや、その業界において対策すべきサイバーセキュリティの観点が正しく評価できず、本来必要な対策の評価に抜け漏れが発生してしまうおそれがある。

本フレームワークは、抽象度の高い記述が含まれている箇所もあるため、評価対象となる組織が回答しやすいように具体的な内容への置き換えや解説を加える等の工夫も必要であるが、様々な業態に適合できるよう設計されているため、金融機関が保有する非金融の国内外のグループ会社やサプライチェーンのセキュリティを同一の基準で横並びの評価を行い、組織全体のサイバーセキュリティの状況を俯瞰した対策を立案することに適している。

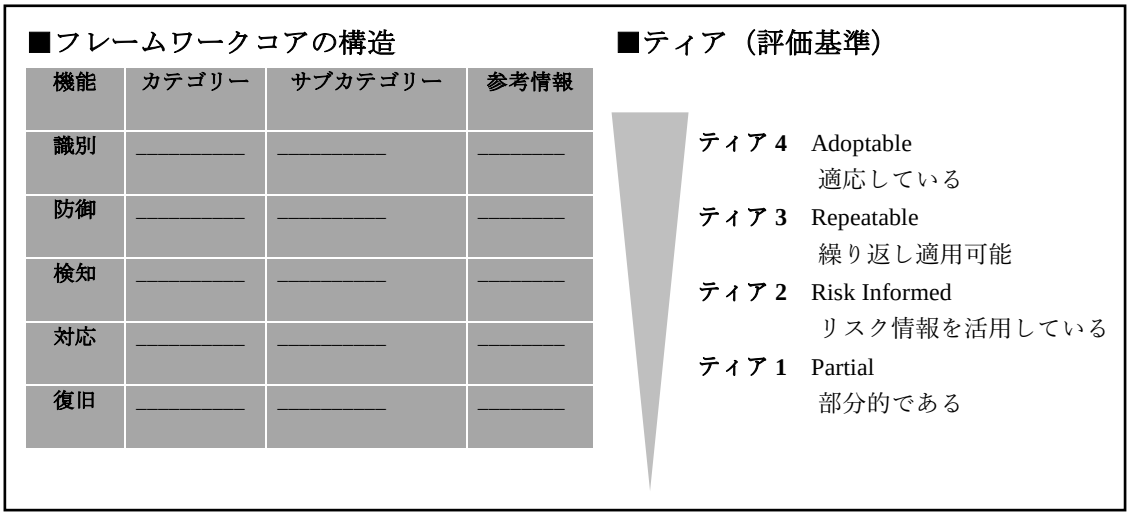


図 4　サイバーセキュリティフレームワークのイメージ

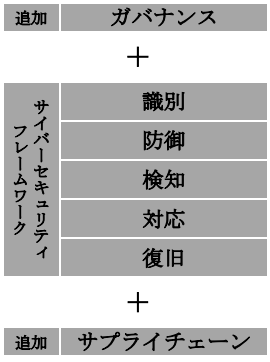
３．４　CRI Profile

CRI Profile[7] は、米国金融サービスセクター連携協議会(FSSCC) が前述の NIST CSF や CPMI-IOSCO[6]による”Guidance on cyber resilience for financial market structures”[7]、関連する監督指針の評価に関する質問項目、ISO/IEC 27001 や 27002 等をベースに作成された新しいフレームワークである。本フレームワークを活用することにより、金融機関の組織の複雑さや規模に見合ったサイバーセキュリティに関するリスク管理を効率的に行うことができる。現在は、CYBER RISK INSTITUTE[8]が CRI Profile の管理や更新を行っている。

CRI Profile では、NIST CSF の機能（識別、防御、検知、対応、復旧）に加えて、「ガバナンス」と「サプライチェーンマネジメント」の項目が明示的に加えられている。また、金融機関が社会に与える影響(ティア[9])の考慮があり、規模に応じた管理基準項目の選択ができるように設計されている。

そのため、CAT ではリスク評価をするための設問数が多いため、実態把握やリスク評価のために多くの工数が必要であったが、CRI Profile では金融機関の規模によって項目が絞られるため、規模に見合ったセキュリティ対策を効率的に測定することができる。図 5 に CRI Profile のフレームワークの構造のイメージと規模の概要を示す。

■フレームワークの構造　■ティア（規模）



ティア	説明
ティア 1	National/Super-National Impact 国家/超国家的影響-北米または世界経済の安定性に影響を与える可能性のある組織 (管理基準項目：277)
ティア 2	Subnational Impact 準国家的影響-米国の金融サービス部門に全国規模で影響を与える可能性のある組織(管理基準項目：262)
ティア 3	Sector Impact セクターへの影響-地域規模で米国の金融サービスセクターに影響を与える可能性のある組織 (管理基準項目：188)
ティア 4	Localized Impact 100 万人未満の顧客で地域的な組織 (管理基準項目：137)

図 5　CRI Profile のイメージ

6) BIS 決済・市場インフラ委員会（CPMI）および証券監督者国際機構（IOSCO）

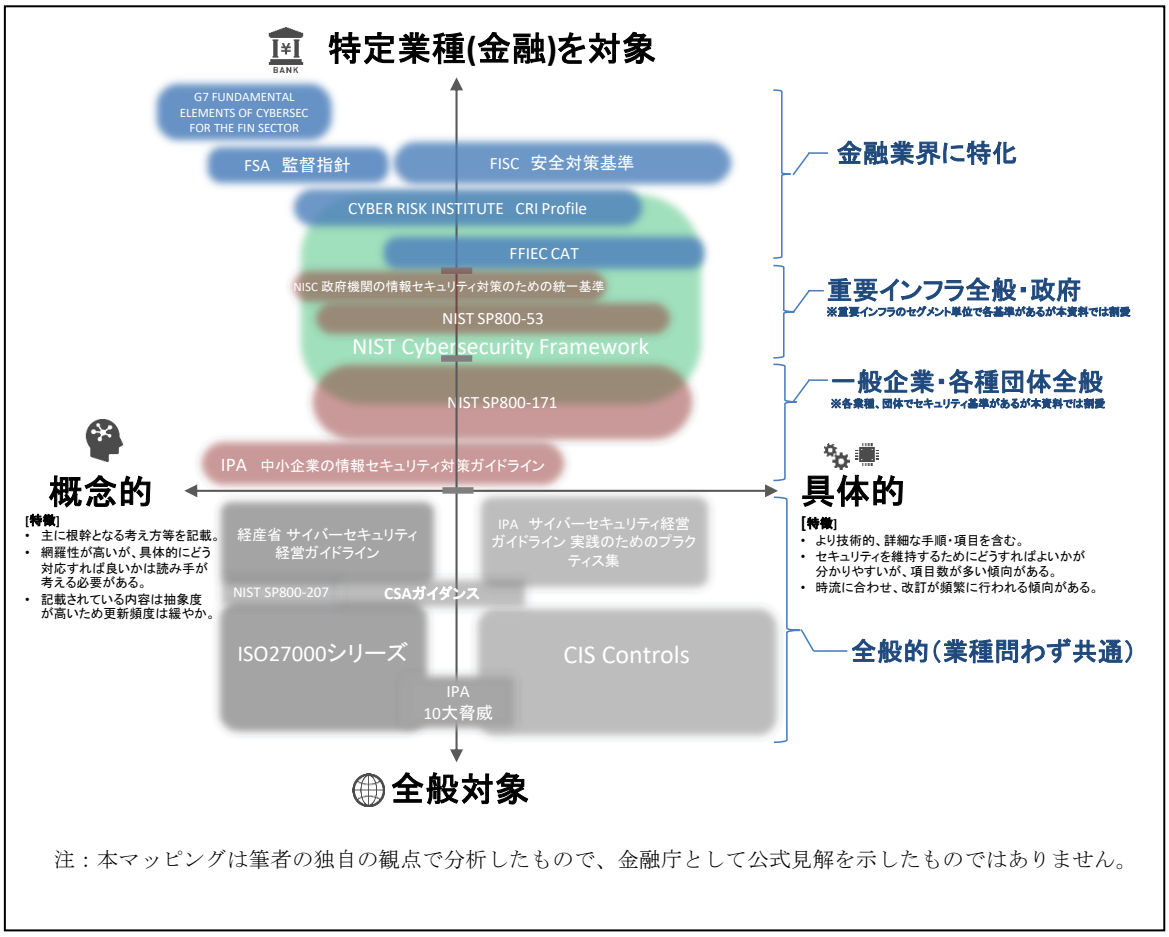
7) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

8) 非営利の金融業界団体。標準化を通じてサイバーセキュリティとレジリエンスを強化し、世界経済を守るために活動している。

9) 前述の NIST CSF の「ティア」はサイバーセキュリティ態勢の状況を示しているが、CRI Profile では金融機関の規模を示しているため、混同しないように注意が必要。

３．５　その他の代表的な基準・ガイドライン等

前節では、金融機関が自組織やグループ会社等のサイバーセキュリティ対策の現状把握や計画立案に役立つ主なフレームワークや基準を紹介したが、それら以外にも有益な基準やフレームワーク、ガイドライン等が数多くある。そこで、これまでに紹介したものに加えて、その他の主要な基準やガイドライン等についてそれぞれの特徴が俯瞰できるように、著者にて、縦軸に汎用性（上側：金融機関に特化した内容。下側：汎用的な内容）、横軸に抽象度（左側：抽象度が高い記載。右側：具体的な対策が記載）として分析・分類したものを図 6 にまとめ、表 3 にその概要を記載した。それぞれのガイドラインで特徴が異なるため、目的に応じて活用していただきたいと考えている。



注：本マッピングは筆者の独自の観点で分析したもので、金融庁として公式見解を示したものではありません。

図 6　各基準・ガイドライン・フレームワーク等の特徴

表 3　金融機関のサイバーセキュリティの向上に役立つ各種ドキュメント

発行元の組織名 ドキュメント名称	概要
Group of Seven (G7) G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR[8]	金融機関が、自らのリスク管理や企業文化に関する認識を踏まえた上で、サイバーセキュリティ・ストラテジーやその運用のためのフレームワークを策定・実施するにあたり、その土台の役割を果たす基礎的要素が記載されている。
金融庁(FSA) 監督指針[9]	金融機関の検査・監督を担う職員向けの手引書として、検査・監督に関する基本的考え方、事務処理上の留意点、監督上の評価項目等を体系的に整理したもの。各金融機関向けにサイバーセキュリティ管理に必要な項目等についても記載されている。
内閣サイバーセキュリティセンター(NISC) 政府機関の情報セキュリティ対策のための統一基準[10]	行政機関や独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みで、情報セキュリティを確保するための対策事項を規定している。
米国国立標準技術研究所(NIST) SP800-53 組織と情報システムのためのセキュリティおよびプライバシー管理策[11]	米国連邦政府の組織およびシステムのための管理策を規定したセキュリティ基準。日本政府も、政府で導入するクラウドサービスに要求するセキュリティ管理基準のひとつとして NIST SP 800-53 を採用する方針を公表している。
SP800-171 非連邦政府組織およびシステムにおける管理対象非機密情報 CUI の保護[12]	米国政府の機密情報以外の重要情報（CUI）を扱う民間企業が実施することが推奨されているセキュリティ対策について記載されている。
SP800-207 ゼロトラスト･アーキテクチャ[13]	これまで行われてきたネットワークベースの境界線防御という概念ではなく、すべてのデータとコンピューティングサービスをリソースとみなし、リソースへのアクセスはセッション単位で付与する等、セキュリティを確保するために必要な考え方を 7 つに整理したものをゼロトラストと定義し、その考え方に基づいたアクセス制御や監視、改善を行うための概念的な定義やユースケース等が記載されている。
経済産業省(METI) サイバーセキュリティ経営ガイドライン[14]	大企業と中小企業の IT システムやサービス等を供給する企業と、IT を利用する企業の経営者を対象に、サイバーセキュリティ対策を推進するために METI と IPA が共同で作成したガイドライン。 本ガイドラインでは、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」、及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）に指示すべき「重要 10 項目」をまとめている。
情報処理推進機構(IPA) サイバーセキュリティ経営ガイドライン 実践のためのプラクティス集[15]	サイバーセキュリティ経営ガイドラインでまとめられた「重要 10 項目」の実践に必要な事例を充実させたプラクティス集。「重要 10 項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例を記載している。

中小企業の情報セキュリティ対策ガイドライン[16]	個人事業主、小規模事業者を含む中小企業が、情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき指針や社内において対策を実践する際の手順や手法をまとめたガイドライン。 経営者編と実践編から構成されており、できる限り専門用語の使用を避け、IT に詳しくない経営者にとっても理解しやすい内容となっている。付録としてリスク分析シート等も含まれており、これらを活用することで幅広い企業で、効率的に自社の情報資産に想定されるリスクの特手や対策について分析することもできる。
情報セキュリティ 10 大脅威[17]	社会的に影響が大きかったと考えられる情報セキュリティに関する事案から、IPA が脅威候補を選出し、情報セキュリティ分野の担当者等で構成される「10 大脅威選考会」が脅威候補に対して審議・投票を行い、毎年決定したもの。その年のサイバーセキュリティの傾向を把握することができる。
Cloud Security Alliance(CSA) クラウドコンピューティングのためのセキュリティガイダンス[18]	Cloud Security Alliance (CSA)が公開している「Security Guidance for the Critical Areas of Focus in Cloud Computingv4.0」の日本語訳。クラウドコンピューティング技術を採用することに伴うリスクとその管理、緩和するための方法等について述べている。
国際標準化機構(ISO) ISO27001[19]/ISO27002[20]	国際標準化機構(ISO)により規格化された、ISO27001:2013「Information security management systems — Requirements」では、組織における情報セキュリティマネジメントシステム(ISMS)を認証するための要求事項が示されている。ISMS とは、組織の情報セキュリティを管理する仕組みのことを指す。我が国では、日本産業規格(JIS)[10]として同内容が JIS Q27001:2014「情報セキュリティマネジメントシステムー要求事項」として和訳、発行されている。 ISO27002:2013「Code of practice for information security controls」は、ISO27001 で示されている要求事項をもとに、具体的な情報セキュリティマネジメントの管理策を示した規格である。我が国では、JISQ27002:2014「情報セキュリティマネジメントの実践のための規範」として和訳、発行されている。 2022 年 2 月に上記の改訂版である、ISO27002:2022「Information security, cybersecurity and privacy protection - Information security controls」[21]が発行され、カテゴリーや管理策等が見直された。JIS 版は本論文の執筆時点(2022 年 6 月)ではまだ発行されていない。
Center for Internet Security (CIS) CIS Controls[22]	米国の Center for Internet Security(CIS)が、情報セキュリティ対策とコントロールにおいて実施すべき内容を取りまとめたガイドライン。本ガイドラインでは、技術的な分野に焦点を当て、具体的な対策内容が示されている。 最新版(v8)ではコントロールに、クラウドやモバイルの技術も含まれている。

10) https://www.jisc.go.jp/index.html

４．戦略的なサイバーセキュリティ対策の計画立案

前章では、金融機関で活用されている代表的な基準・ガイドライン等について概要を紹介した。本章では各金融機関がそれらのドキュメントを活用しながら、どのように目標を定め、実行計画を策定すれば良いかについて述べる。

自組織の戦略的なサイバーセキュリティ対策の計画立案を行うための具体的な活動は、表 4 に示す通り、大きく分けて 3 つのフェーズに分類することができる。

表 4　戦略的なサイバーセキュリティ対策の計画立案を行うための 3 つのフェーズ

フェーズ		概要
1	**現状把握**	組織のサイバーセキュリティ対策状況の把握
2	**分析**	サイバー脅威に対する組織への影響分析
3	**計画立案**	サイバー脅威への対策とその計画の策定

多くの金融機関では、既にリスク評価や対策状況を把握するためにアンケートや定期的なリスク評価等を実施し、その設問に設定された基準を満たすための必要な対策を実施する活動は行われている。戦略的なサイバーセキュリティ対策の計画立案では、既に行われているこれらの活動から更に踏み込み、短期間で実現できる施策のみならず、サイバーセキュリティ対策の全体を俯瞰し、組織全体の整合性を鑑みながら、個別システムからサイバーに関する総合的な組織運営も含めた網羅的な対策を強化するための中長期の計画を策定する。その計画は、組織の文化や将来を見据えたビジネス戦略、IT 計画等とも整合させながら､サイバーセキュリティ対策が本来あるべき姿になるように立案する必要がある。そのため、現状を把握するための調査には、実態を良く把握している現場社員やその管理者の協力が不可欠で、分析・対策計画の立案時には、必要に応じて今後の技術や脅威動向等を把握している第三者の知見や人的リソース等を活用しながら実施することもある。本章では、上記 3 つのフェーズの各手順と各金融機関が実施するにあたり気を付けるべきポイント等について述べる。

４．１　現状把握

サイバーセキュリティの対策の計画を立案するためには、まずはサイバーセキュリティにおける自組織の立ち位置と目標となる姿とのギャップを把握するための現状把握を行う必要がある。自組織の目標となる姿は、前章で紹介した基準やガイドライン等に記載されている考え方や具体的な対策例等を活用することで設定することが出来る。本節では、評価の対象範囲と評価方法について述べる。

４．１．１　セキュリティの評価対象範囲

サイバーセキュリティの対策の現状を把握するための活動を行う前に、評価対象範囲を明確にすることは、サイバーセキュリティ対策の抜け漏れを防ぐ観点で重要な作業である。何故ならば、攻撃者は対策が十分に施されている箇所から侵入や攻撃を試みるだけではなく、むしろ対策が不十分な箇所を探し出して、侵入し、重要なシステムや機密情報等を探索し、その情報の窃取やシステムの停止等を行うためである。そのため、すべてのシステムに対して網羅的かつ深度のあるセキュリティ評価を行う必要がある。その評価を一度に短期間で実施できるのであれば理想的だが、調査するための要員や費用確保の面でも実現するのは難しい。そこで、図 7(左)に示す様に、確保可能なリソースで短期間に組織全体のセキュリティ対策の概況を把握したい場合は、まずは全体を広く調査・把握し、機密情報の取り扱い有無やインターネットとの接続有無、システムの利用者数や対策の概況等を把握し、重点的に調査すべきシステムを選定し、その後、同図(右)に示す様に、深度のある評価を対象ごとに行う方法をとることもできる。また、個別調査する対象があらかじめ選定可能であれば、左図と右図を組み合わせて同時に調査を実施し調査期間を短縮化することもできる。深度のある個別調査は、各金融機関のシステムの規模や調査に割り当て可能なリソースや状況に応じて複数年かけて実施することもある。

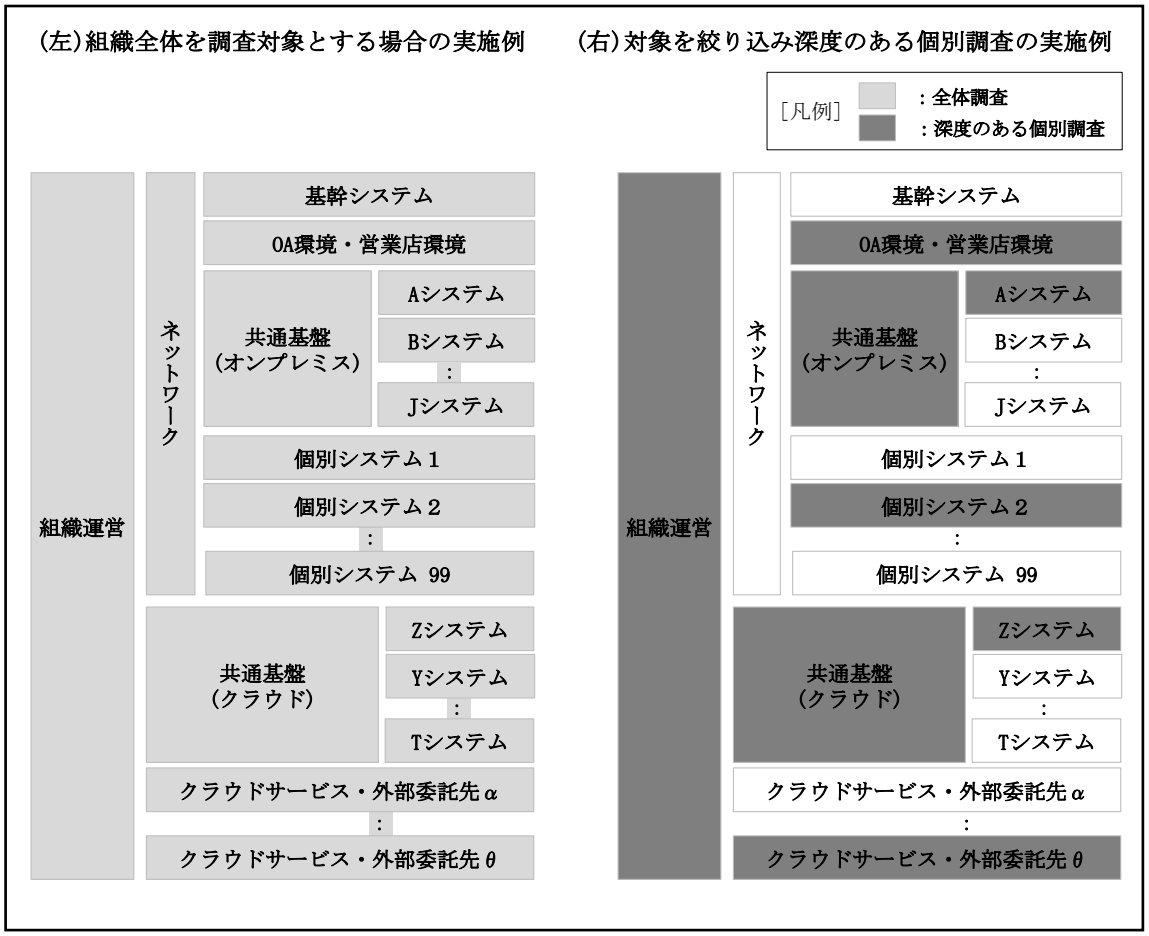


図 7　評価対象の選定と評価の実施方法に関する説明図

数多く存在する各システムのサイバーセキュリティ評価を初めて網羅的に実施する際は、多くの工数を要し作業負荷も高いが、2 巡目以降は前回の評価で対策が不足していた箇所の改善状況や新たなサイバー脅威への対策状況の差分を確認する等、焦点を絞った評価を行うことで効率化ができる。そのため、昨今の情勢を踏まえたサイバーセキュリティの評価が一巡していない金融機関は、まずはサイバーにおけるリスクがどのシステムにどの程度存在しているかの全体像を把握するための活動を行うことが望ましい。

サイバーセキュリティを「組織」として経営課題と認識し、適切に把握して対応しているかを確認するには、サイバーセキュリティに関する取組方針や計画、ガバナンス体制や規程、人材育成・教育等が整備されているかを確認する必要がある。金融機関では、これらは既に一通り揃っていることが多いが、形式的に揃っているだけではなく、その規程や整備内容に実効性があるか、記載内容が組織の実態と整合しているか、現場まで浸透し正しく運用されているか等についても評価する必要がある。

評価対象とするシステムの選定の観点では、金融機関が主たる業務で利用する基幹システムだけではなく、一般文書やメール等を作成、送信する OA 環境や Web 閲覧環境等も含めた評価を行うことが望ましい。何故ならば、多くの金融機関では共同センター等を利用しているため、基幹システムそのものは外部委託先であるベンダの責任にてセキュリティ対策やシステムの堅牢化を行っているが、OA 環境等は自組織若しくは自組織が委託しているベンダに指示等を行い、対策を推進する必要があるためである。そして、サイバー攻撃はインターネットや他企業等との外部の接続点を経由して侵入してくることが多いため、侵入経路となりやすい箇所での防御や検知、対応力等についても正しく評価を行う必要があるためである。

また、業務でクラウドサービスを利用している場合は、それらに重要なデータが保存されているケースも増えているため、そのクラウドサービスそのものが安全か、安全に利用されているか等も評価を行う必要がある。クラウドサービスの安全性を評価するために活用することが出来る、クラウドのセキュリティを解説したガイドライン[18]等もあるが、「政府情報システムのためのセキュリティ評価制度(ISMAP)[11)]」 のセキュリティ基準を満たし登録が認められたクラウドサービスの一覧が公開されている。クラウドサービスを職員が安全に利用できる設定となっているか等の確認は、金融機関で行う必要はあるが、クラウドサービス自体の安全性の評価は、この一覧を活用しながら効率化することもできる。

その他、各システムで利用している情報資産の量やその内容によりサイバー攻撃の影響は大きく変わることから、情報資産の棚卸を行った上で評価対象を選定することも重要である。そして、情報セキュリティを守るための基本方針であるポリシー、対策基準(スタンダード)、その実施手順(プロシージャ)が確立され、定期的に見直しがされているか等につ

11) ISMAP のクラウドサービスリストは定期的に更新され、リストは下記 URL にて閲覧可能。(https://www.ismap.go.jp/csm)

いても評価する必要がある。確認すべき具体的な評価項目等については、前章で紹介したガイドラインやフレームワーク等に詳細に記載されているため、昨今のサイバー攻撃や、これまでのサイバーに関する業務経験を踏まえて、特に確認する必要があると考えているポイントを表 5 に示す。

表 5　評価対象の分類とその確認のポイント

評価対象の分類(例)	確認のポイント
組織	・規程やルールの定期的な見直しが行われ、組織や業務の実態や実効性に応じて改定されているかの確認。 ・規程やルールの存在だけではなく、実運用もそれらに沿って行われているか証跡も含めた確認。 ・サイバーセキュリティに関する人材育成・拡充計画とその内容の確認。
基幹システム	・基幹システムに保存されている機密情報等が漏洩した場合やシステムが停止した場合の業務影響等の把握状況とその対策状況の確認。 ・ベンダに業務を委託している場合は、開発環境と本番環境の分離や、アカウントの管理、アクセス管理、監査等が適切に行われているかの実運用レベルでの確認。
OA 業務 (営業店端末含む)	・OA 業務や営業店端末で利用している情報の重要度と量の確認。 ・個人情報や信用情報等、機微な情報を扱うシステムが個別に存在する場合は、アクセス権やアカウント管理のルールの有無に加えて、運用実態も含めた確認。
クラウドサービス	・クラウドサービスで処理しているデータの重要度に応じたセキュリティ対策や機密性・可用性・完全性等が確保されているかの確認。
業務委託先	・業務の一部を委託先にて実施している場合、委託先に対して情報セキュリティ対策の明示(仕様書の提示)の有無や、責任範囲の取り決め状況等の確認。
新技術(RPA・AI 等)	・情報システム部門が認知・許可していない、現場(各部門)の独自判断で利用されている RPA や AI の有無の確認。 ・新技術を利用するためのルールが定められ、ルールに沿って適切に運用されているかの確認。

４．１．２　セキュリティ評価の実施方法

現状把握の評価方法には様々な方法があるが、大別すると表 6 に示すように、インタビューやアンケート、資料等をもとに確認する「机上評価」と、実機や演習等を通して脆弱性や課題を直接的に確認する、「実機評価」の 2 種類に分類することができる。

表 6　サイバーセキュリティ評価の分類とその手法、特徴について

分類	具体的な手法	特徴
机上評価	・アンケート ・インタビュー ・ドキュメント(規程、経営報告資料、議事録、設計、運用資料等)の精査等	・幅広く効率的に評価することができる。 ・インタビューやアンケートの場合、回答者の自己評価に影響されやすく、ヒアリングした通りに対応できるかの検証は難しいことがあるため、ヒアリング方法に工夫が必要。
実機評価 (演習含む)	・脆弱性診断[12)] ・ペネトレーションテスト[13)] ・TLPT[14)]等 ・サイバー演習	・実機での確認や演習を通して実際に防御、検知、判断等の対応ができているか等の実態を評価することができる。 ・机上評価に比べてより正確な実態を把握できるが、全てのサイバー攻撃の態勢を網羅的に評価することは困難。

４．１．２．１　机上評価

机上評価は、システムや業務の各担当者にアンケートやインタビューを実施したり、関連する資料を確認したりすることでサイバーセキュリティの対策状況を評価する方法である。机上評価を行う場合は、評価者や回答者によって評価結果にばらつきが出ないように、あらかじめ評価基準や定量的に評価するためのスコア等を決め、その評価基準に則り現状を評価することが望ましい。また、ヒアリングを実施する際に、質問に対して抽象的に対応の有無を確認すると、回答者の判断基準によって判定が異なるおそれがある。そのため、どのような対応を行っているのかその内容を具体的に確認し、その対応内容をもとに第三者がその対策の実施有無や良否を評価することが望ましい。サプライチェーンマネジメントの観点で委託先にアンケート等でサイバーセキュリティの対策状況を回答してもらう場合も同様に、委託先の主観により回答の齟齬が発生しない設問にする必要がある。また、

12) システムへの擬似的な攻撃により、主に技術的な脆弱性の有無を調査するためのテスト。

13) システムに対して実際に侵入を試みることで、テスト対象機関のサイバー攻撃の耐性を評価するためのテスト。

14) Threat Led Penetration Test(TLPT)：サイバーレジリエンスの評価と向上を目的として、脅威インテリジェンスを基に実施する、より実戦的なペネトレーションテスト。

必要に応じて回答通りとなっているか現地に赴き、実態を確認することが望ましい。そして、ベンダが提供するセキュリティ製品やセキュリティサービスで対策を行っている場合は、その具体的なサービス名や、その運用方法、そしてその対応を裏付ける手順書や作業履歴や契約内容等も含めて確認し、質問の意図通りの対応ができているかを確認することで、より精度の高い実態を把握することができる。

具体的な事例として、システムの権限の運用確認を行う際に、下記のように設問を設定し、回答を得られた場合を考える。

【抽象度が高く実態を正確に把握することが困難な設問と回答例】

設問	システムの管理者権限の運用管理を適切に行っていますか。
回答欄	管理者権限は特定の社員のみがアクセスできるように適切に行っている。

上記の質問と回答では、設問と回答がシンプルにまとめられて一見すると適切に管理され、問題がないように見えるかもしれない。しかしながら、この回答では具体的にどのようなコントロールを行っているかが分からず、対策の十分性を評価することができない。そのため、管理者権限をどのように管理しているか等を、より具体的にヒアリングする必要がある。より具体的なヒアリング項目や目指すべき姿と自組織との差分を検証できるように、サイバーセキュリティに関する基準やガイドライン等に記載されている考え方や具体的な対策例をもとに作成すると、実効性の高いヒアリングと分析ができる。以下に同様の趣旨の内容を詳細にヒアリングし、その結果をまとめた例を示す。

【実態をより正確に把握するための設問とその回答例】

設問		X システムの管理者権限についてどのように管理しているか下記項目に沿って回答してください。
回答欄	管理者アカウントの発行方法	管理者としてシステム部部長に承認された担当者のみに管理者用のアカウントを個別に発行している。
	管理者アカウントの利用方法	管理者アカウントを利用する際には、利用の都度、上長へのアカウント利用申請が必要で、上長からの利用申請が承認されない限り、システムにアクセスすることができない。また、管理者アカウントの利用後はアクセス出来ないように都度無効化されるようにシステムで制御されている。
	検証方法(作業内容のチェック)	管理者権限で行った作業は、上長にその作業ログが自動で送付され、作業を行った旨の通知と、上長によりその作業内容が検

		証される仕組みが導入されている。作業内容の検証が完了することで一連の作業が完了することとなっており、完了していないとシステムから上長に日次で確認を促す通知メールが送信される。
	管理者アカウントの棚卸	アカウントは人事システムと連携し、異動後は以前所属していたシステムへのアクセス権が自動的に削除される。また四半期毎にアカウントの棚卸を実施している。

上記はあくまで一例で、より機密性の高いシステムの場合は、上記の設問に加えて、通信元端末の制限や特定、多要素認証の有無、専用端末室等を用いた物理的なアクセス方法、運用手順やルールとして文書化されているか等についても必要に応じてさらに確認する。設問を追加する場合の注意点として、様々な観点を増やしたり、設問の粒度を細かくしたりすると、設問数が膨大となり回答者への負担が掛かりすぎることがあるため、設問設計を行う際は、具体的なリスクや脅威を想定した上で、設問内容と設問数を考慮する必要がある。また、回答者と評価者の双方の負担を軽減するために、自由記述式ではなく、想定される回答の選択肢を用意しておく等の工夫も検討することが望ましい。このような活動で得られた確認結果を分析することで、机上評価でも組織のサイバーセキュリティ能力を正確に測ることが可能である。

４．１．２．２　実機評価（サイバー演習含む）

稼働しているシステムに対して直接サイバーセキュリティの対策状況を調査する実機評価は、机上評価に比べ、現時点でのシステムのセキュリティの対策状況の実態をより正確に把握することができる。しかしながら、実機評価は自動化や AI 等の活用により効率化されコストは下がりつつあるものの、机上評価と比べると現時点ではより多くのコストがかかる。また、ホワイトハッカーによる、高度な手法やシナリオを用いた実機評価を行う場合は費用や工数、期間が更に必要なため、評価するシステムの重要度、机上評価の結果や脅威インテリジェンス等をもとに、実機評価の対象範囲や評価手法を決定することが妥当かつ現実的である。

サイバー演習は自組織のルールや手順等が一定程度完成しており、そのルールや手順通りに運用できるかを確認し、サイバーインシデント対応の練度を上げることや、今後の改善に必要な課題抽出のインプットとするために有効である。また、サイバーセキュリティの重要性が組織内で十分理解されていない場合は、経営陣から現場担当者までが参加するサイバー演習を企画・実施することで、サイバーインシデント対応の難しさや事前準備の重要性について演習を通じて組織全体に認知してもらい、今後の計画立案の必要性を理解してもらうために活用することが期待できる。

実機評価について、誤解されやすいことがあるので補足する。実機評価は机上評価より

も組織のサイバーセキュリティ対策の実態を常に正確に把握できるかというと、必ずしもそうであるとは限らない。

例えば、実機評価(脆弱性診断)時にシステムにパッチが適用されていた場合は、脆弱性診断のパッチ適用の観点では問題なしと評価されることとなる。しかしながら、実機評価で、迅速にパッチ適用ができることを保証するものではない。そのため、その補完として机上評価による運用手順書等の精査や運用担当者へのインタビューや作業記録などの確認を行うことで、パッチ適用の明確な判断基準が定まっておらず危険度の高い脆弱性に対する優先順位付けが不足しており、適用するまでの期間が空いていることから、システムが危険に晒されている期間が長い等の懸念が発見されることがある。また、脆弱性診断では、職員が行うオペレーションそのものの評価は行えないため、それらに関する問題点を検出することが難しい。このような例からも分かるように、実機評価を行えば机上評価は不要と判断するのは早計である。考えられるリスクや評価の目的に応じて評価方法を柔軟に選択する必要がある。

４．２　分析

現状把握を行った後は、対策状況の分析を行い、どのような脅威が残存し課題があるかを洗い出す活動を行う。検出されたすべての課題を解決するために一律、同時期に着手し最短で完了することは、人的なリソースや費用の観点からも現実的ではない。また、発見された課題順に対処するのでは、本来早急に対応すべき対策が後手に回ってしまうおそれがある。そのため、検出された課題を分析し、リスクに応じて優先度(順位)をつけて対策に着手すべきである。

分析の方法には、脅威が顕在化する確率や推定される被害額をもとに定量的に算出する方法や、定性的な情報をもとに分析する方法等、様々な方法がある。本稿では、検出された脅威が顕在化する可能性と、脅威が顕在化した際の負の影響度をもとに総合的な可能性を分析し、行うべき対策の優先順位をつける、発生確率・影響度マトリクスと、サイバー攻撃が成立するまでの各攻撃ステップへの対策状況をもとに分析する 2 つの方法について紹介する。

４．２．１　脅威事象の発生可能性とその影響の組み合わせによる分析

IPA が NIST の発行する文書の翻訳を行った「NIST-SP800-30　リスクアセスメントの実施の手引き」[23] では、「脅威事象が発生する可能性」とその「影響レベル」をもとに、リスクのレベルを評価するマトリクスが紹介されている。本文書における脅威事象とは、脅威主体によって引き起こされる負の事象のことを指し、具体例を挙げると、サービス妨害や、悪意のある管理者による意図的な行為、サーバが意に反してオフラインになること等が脅威事象にあたる。影響レベルとは、脅威事象が発生することで顧客や組織に与える負の影響の度合いを示す。これらは各組織や提供している各サービスによってその度合いは

異なる。

例えば、サービス妨害攻撃によりインターネットバンキングが利用できなくなることは金融機関と顧客にとって影響レベルが非常に高いと判断ができるが、同じサービス妨害攻撃であっても、一部の従業員しか利用しておらず、利用不可時は代替手段が確保されているサービスの場合は、影響レベルは低いと判断できる。このように発生確率とその影響レベルはそれぞれの固有の事情を鑑みる必要があるため、本分析を用いる場合は、可能性と影響レベルの認識を組織内で一致させる必要がある。

NIST-SP800-30 では、表 7(左)のように、各項目を 5 段階のレベルに分けている。評価の粒度が細かすぎて分類が困難であると感じた場合は、表 7(右)のように高中低の 3 段階のマトリクスを用いることで、よりシンプルに分類・分析することができるため、金融機関ではこのマトリクスが利用されているケースもある。

表 7(右)のように、低優先から最優先までを 3 段階に分類した場合、発生する可能性と、その影響レベルの双方が「高」であれば、総合的な評価は「高」となり、最優先で取り組むべき課題となる。一方、負の影響度をもたらす可能性が「高」だとしても、影響レベルが「低」の場合は、総合的な評価は「中」なる。同様に、脅威事象が負の影響をもたらす可能性が「低」であったとしても影響レベルが「高」であれば、総合的な評価は「中」となるため、総合的な可能性が「高」の対策に次いで検討することとなる。そして、総合的な評価が「低」と分類された課題については、対策を実施した場合の費用対効果や予算等も鑑みて、ほかの対応を優先し実施時期を遅らせたり、リスク受容も視野に入れて検討したりすることができる。このように、脅威の可能性や影響レベルの双方を組み合わせてリスク分析を行うことで限りあるリソースを効果的に配分するための検討材料の一助になる。

表 7　総合的な可能性の評価　(左表：5 段階　右表：3 段階)

脅威事象が発生する可能性	影響レベル				
	非常に低い	低い	中間	高い	非常に高い
非常に高い	低い	中間	高い	非常に高い	非常に高い
高い	低い	中間	中間	高い	非常に高い
中間	低い	低い	中間	中間	高い
低い	非常に低い	低い	低い	中間	中間
非常に低い	非常に低い	非常に低い	低い	低い	低い

脅威事象が発生する可能性	影響レベル		
	低	中	高
高	中	中	高
中	低	中	中
低	低	低	中

４．２．２　サイバー攻撃の各ステップへの対策状況をもとにした分析

現状把握で検出した課題に対して、どのような攻撃や事象に対してサイバーセキュリティ対策が脆弱であるのかをより具体的に分析することは、サイバーセキュリティ対策を立案する上で、その費用対効果の検証や対策要否を検討する上で重要である。

より具体的なサイバーセキュリティ対策の実態分析・評価を行うために、昨今の攻撃事例等をもとに、特定の脅威シナリオ（例：標的型メールを開封し、情報漏洩やランサムウェアに感染する事例や、DDoS 攻撃、従業員や委託先による内部不正）に沿って態勢があるかを評価する手法もあるが、本節では、Lockheed Martin（ロッキードマーティン）社による Cyber Kill Chain(サイバーキルチェーン)[15)]と、MITRE (マイター) 社による ATT&CK(アタック)[16)] を用いて、組織がサイバー攻撃の各フェーズに対応する防御や検知、対応等の態勢を有しているかを、より具体的に可視化・評価する方法について紹介する。

Lockheed Martin 社は、米国の航空機や防空システム等の開発製造を行っている企業で、同社が開発・公開している Cyber Kill Chain はサイバー攻撃の各ステップで行われる戦術の概要を取りまとめているため、悪意のある攻撃者が行うプロセスの概要を把握することができる。

MITRE 社は、脆弱性に一意の識別番号を採番する「CVE: Common Vulnerabilities and Exposures（共通脆弱性識別子）[17)]」を運用していることで有名な非営利の団体である。MITRE 社の ATT&CK は、2013 年から公開しているナレッジデータベースで、ATT&CK は、Cyber Kill Chain でとりまとめた攻撃の各ステップの概要の説明にとどまらず、戦術を構成する技術や手法(テクニック)についてより詳しく公開している。また、戦術ごとの個別の攻撃技術・手法に対応する、緩和策、検知方法やセキュリティベンダ等レポートのリンク等が記載されている。この戦術とは、偵察、リソース開発、初期アクセス、実行、永続化、特権昇格、防御回避、認証情報アクセス、探索、水平展開、収集、Command & Control(C&C)[18)]、持ち出し、影響に分類されている。さらに、サイバー攻撃を行っている攻撃グループやプラットフォーム(Windows、Linux、Mac、Android、iOS 等)を特定することも可能なため、攻撃グループに着目した分析や、自組織に関連のあるプラットフォームのみに絞り込んで分析することもできる。

Cyber Kill Chain と ATT&CK は、サイバー攻撃に対する概念が共通している部分が多いため、図 8 に Cyber Kill Chain と ATT&CK との関係性を示す。

組織は、Cyber Kill Chain や ATT&CK で示されている一連の攻撃プロセスに対して、攻撃の目的が成立する前に断ち切ることができるか、各ステップに対応する防御策を網羅的

15) https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

16) https://attack.mitre.org/

17) 脆弱性に対して一意に付与される「CVE ID」の識別番号により、各組織が発行する脆弱性対策情報の相互参照や関連付けができるため世界的に利用されている。

18) マルウェア等に感染したコンピュータを攻撃者が遠隔で操作すること。

に有しているか等を評価することで、現在の自組織と本来具備すべき対策のギャップから、組織のどの部分に脆弱な部分があるかを可視化することが可能である。その可視化した情報をもとに対策の必要性とその目的を正確に把握した上で、対策の効果や重要性をもとに、対策要否を判断することができる。

図 8　Cyber Kill Chain と ATT&CK との関係性のイメージ

４．３　計画立案

自組織の分析を行った後、課題や脆弱性に対応するための具体的な対策を立案し、計画、そして実行に移す必要がある。これまでの分析のフェーズで検出された、脅威が発生する可能性とその影響度との分析で総合的な可能性が「高」となっている場合や、Cyber kill

Chain や ATT&CK、特定のサイバー攻撃のシナリオ分析等の結果、サイバー攻撃が目的実行まで成立してしまうおそれがある場合は、できるだけ早く対策に着手する必要がある。しかしながら、予定しているシステム更改の時期や現時点で計画済みのサイバーセキュリティ対策等の全体的な戦略との整合性も鑑みながら対策立案を実施すべきである。例えば、近いうちに大規模なシステム更改を予定している場合や、対応するための体制確保や設計、構築等で、対策が完了するまで長期間かかる施策がある場合は、完了するまでの間、暫定策や監視強化等を行い、リスクが顕在化することを低減させることや、顕在化したとしても影響を局所化できるように対策することが考えられる。そして、脅威が発生する総合的な可能性が低い場合でも、工数や費用が少なく対策ができる内容（例：設定変更や運用フローの修正、軽微なルール・マニュアル整備等）であれば、費用対効果や対応要員への工数の分散可能か等も鑑みて早期に着手することが望ましい。

対策を導入する際は、個々の対策を一つずつ導入するだけではなく、組み合わせて実施することや各部門やグループ各社ごとに導入していた対策を全社的に統合することで、組織全体の底上げとなることに加えて、作業効率が上がりコストを抑えることもできる可能性もある(例 1：構成変更に伴い複数回発生するネットワークの設定変更を一度にまとめて実施することで都度発生する予定だった検証費、作業費や体制費、期間を統合し圧縮。例 2：個別の施策としてそれぞれ実施する予定だったベンダへの提案依頼を、組織全体の整合性を鑑み、統合したセキュリティ対策の提案依頼書にまとめることで検証や導入コスト等の全体コストを低減させる等)。

図 9 に対策立案時に考慮・確認することが望ましい観点について示す。図 9 に示す様に、組織全体的な整合性や脅威と対策のバランスを鑑みながら対策立案を実施することで、より効率的かつ効果的なサイバーセキュリティ対策を実施することができる。

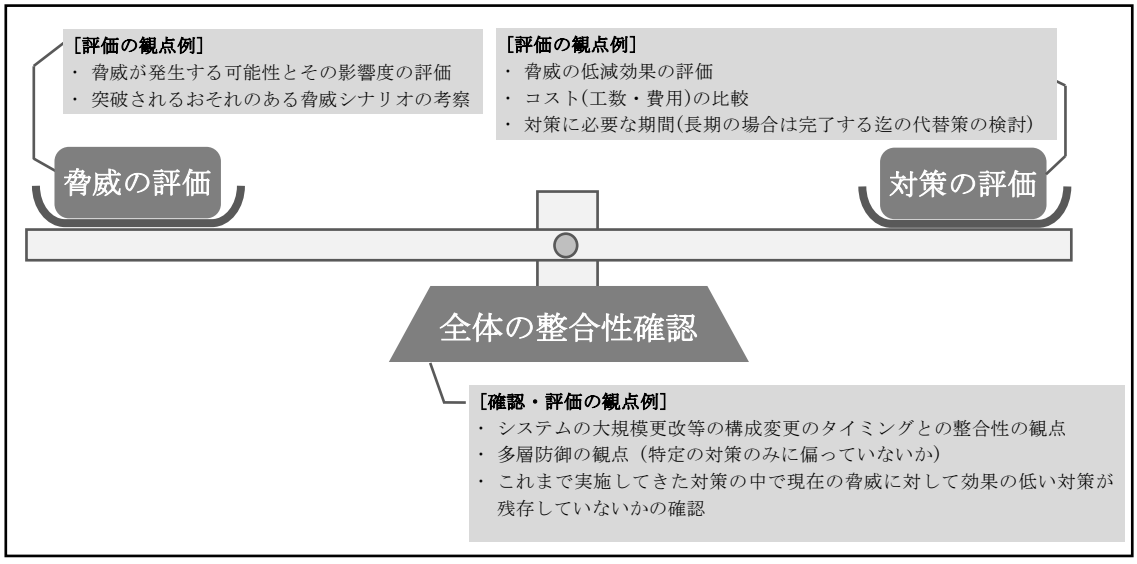


図 9　対策の計画立案時に考慮・確認する観点のイメージ

５．　継続的なサイバー計画のモニタリング

サイバーセキュリティ対策に関する計画の正式な承認後は、IT やサイバー部門に任せきりにするのではなく、予定通りに進捗しているか、課題が発生していないか等を経営陣も主体性を持って定期的に確認すべきである。そして進捗の滞りがないか、また計画通りに対策を進めて問題ないかの確認を行うべきである。

５．１　サイバーセキュリティ対策の定期的な進捗確認

立案したサイバーセキュリティ対策の計画の進捗確認について、担当する IT やサイバー部門等は日々の業務として当然確認するが、経営陣も四半期に一度、少なくとも半年に一度は進捗を確認し、必要に応じて計画の補正や追加の対応を行う必要がある。何故ならば、一年に一度の確認だけでは計画が予定通りに実施できたかの報告のみとなり、その時点では計画に遅れが発生していたとしても選択可能な対応は限られ、計画を補正するための工数や期間が大幅にずれてしまうおそれがある。そして、サイバーセキュリティ対策は事業部門の業務にも少なからず影響を与えるため、部門間に跨る課題が発生している場合は、その事象を正確に把握し、トップダウンで手当てを行うことでその課題を迅速に解消できることもある。特に金融機関では、組織構造が縦割りとなっていることが多いため、部門を跨いだ施策は担当者間では調整に難航するケースがある。そのため、経営陣は CISO や IT・サイバー部門の責任者に対して定期的に報告や議論をする場を与え、IT やサイバー部門の管理責任者は経営陣への定期的な進捗報告を行い、計画に遅れが生じているのであればその真因を分析し、必要であれば経営陣に協力を要請することが望ましい。

進捗報告の際には、経営陣は、計画と実績を短い文書のみで説明させるだけではなく、計画と実績を示したガントチャートや、詳細なタスクまで分解して整理した WBS[19] やコストを EVM[20] 等で管理しているのであれば、プロジェクトの進捗の良否を判断するための参考資料として確認することが望ましい。何故ならば、経営陣への報告資料は進捗が計画に対して遅れている場合は、その部分が正確に表現されておらず問題ないかのように示されていたり、本来伝えるべき情報が抜け落ちてしまっていたりする可能性があるためである。もし進捗管理に関する資料を作成せずにプロジェクトが進められていた場合、進捗が正しく把握できないだけでなく、当初目標としていたことと実施しようとしている施策に齟齬が発生しているおそれもある。そのため、報告内容にもし不足や疑問を感じるのであれば、計画の進捗の概要を示した資料だけではなく、詳細な管理資料をもとに以下のような観点を含めて確認することが望ましい。

【予定していた計画の確認のポイント】

・プロジェクト計画がタスクレベルまで分解され適切に管理されているか。

---

[19] プロジェクトの作業工程を細分化し構造化するプロジェクトマネジメントの管理手法。分解された各作業には担当とその期限等が詳細に設定される。

[20] 作業の到達度を金額に換算し、進捗を管理するプロジェクトマネジメントの管理手法。

・詳細スケジュールに落とし込んだ際に各工程に適切な期間が設定されているか。
　－ 例 1: 設計や構築、テスト等の必要な作業期間や各タスクの前後関係が妥当か。
　－ 例 2: 各工程においてレビューと修正に要する期間が適切に割り当てられているか。
・各タスクに対して担当者が適切に割り当てられているか。
・各タスクの状況(未着手/対応中(進捗率) /完了)が把握できるよう管理されているか。
・計画と実績の全体の差異を把握し、適切に管理されているか。
・計画に遅れが発生していた場合を想定した適切な打ち手が用意されているか。

プロジェクト計画書や WBS はプロジェクトの開始前までに作成・承認されていることが望ましい。しかしながらプロジェクトの承認時点では、計画が概要に留まり、詳細なタスクまで整理や明示されていない場合や、そもそも施策や計画を詳細化するタスクは計画承認後に検討し決定することになっている場合もある。また、承認後の要員手配等の遅れやスコープの変更等で当初の計画からずれが発生していることもある。そのため、そのような場合には詳細な計画が作成又は更新が完了次第、改めて確認すべきである。

そして、サイバーセキュリティを維持するためには、攻撃手法や技術の進歩が早いため、少なくとも一年に一度は予定していた中長期計画を見直す必要がないか、全体との整合性やこれまでの進捗を加味したうえで検討を行い、必要に応じて修正を行うことが望ましい。そして、中長期計画の最終年度は、これまでの中長期計画の総括と新たな中長期計画の立案を行う必要がある。図 10 に継続的な計画の対応イメージを示す。

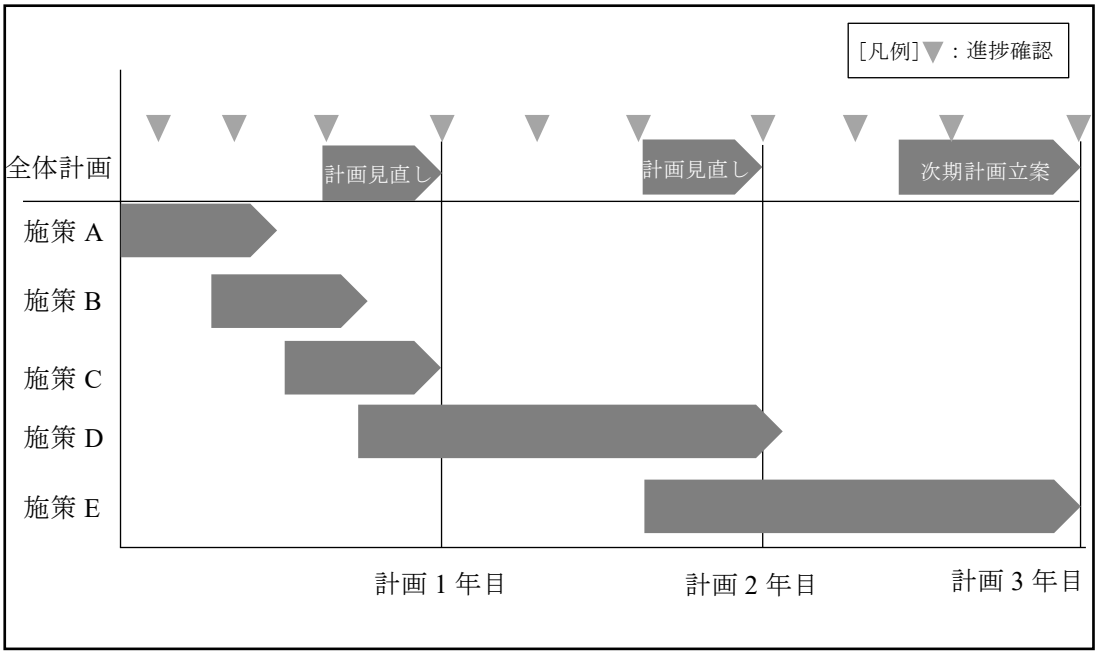


図 10　各施策の進捗確認と計画の定期的な見直しのイメージ

５．２　サイバーを取り巻く素早い環境変化への対応

サイバーセキュリティや IT は環境変化が早く、新たな技術や脅威が突如として出現することがある。そのような素早い環境変化に対応するために、策定した中長期計画が現在および近い将来においても、効率的かつ効果的な対策となるように補正する必要がある。環境変化の察知と計画の補正は、従来からよく言われている PDCA サイクルを回すだけでは不十分な場合がある。そのような場合は、状況を観察(Observe)、状況判断・見当(Orient)、決断(Decide)、行動(Act)する、OODA ループ(ウーダループ)の考え方も取り入れて、必要に応じて動的に計画を補正することが有効である。

OODA ループは、元米空軍大佐の John R. Boyd が提唱した、空中戦における軍事行動の作戦や戦術における意思決定を対象とした理論である[24]。この OODA ループは、人や組織の意思決定段階をモデル化したものであり、Observe、Orient、Decide、Act による一連のサイクルで構成される。OODA ループの概念図を図 11 に示す。

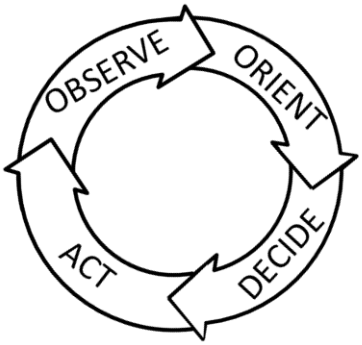


図 11　OODA ループの概要

上図の様に OODA ループの概要では、大きな流れとして、時計回りの一方向に回るループとして説明されることが多いが、OODA ループの各要素とその関係性を詳細に示したものを図 12 に示す。

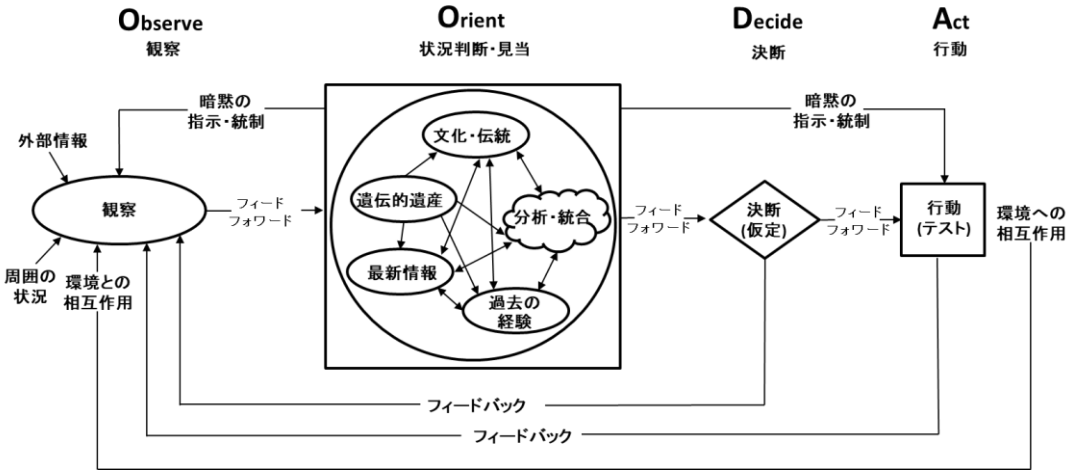


図 12　OODA ループの詳細

図 12 に示した通り、詳細な OODA ループでは各要素が相互に影響しあっている箇所がある。また、Orient(状況判断)をするための分析・統合には、観察した事象だけで決まるものではなく、その意思決定者の過去の経験や文化・伝統等も含めて相互に作用しながら決定していることが分かる。これらは意識的に行われることもあれば無意識のうちに影響していることもある。金融機関におけるサイバーセキュリティの状況判断においては、意思決定者の過去の経験等にとらわれすぎて状況判断や見当を誤ってしまうことがないように、各機関から公表されているベストプラクティスや他社の事例、外部からの知見等を含む最新情報等を十分に加味しながら､的確に判断できるようにすることが必要である｡そして、Decide (決断)や行動したことについて入念に観察を行い、再度状況判断を行い、次の決断や行動に備える必要がある。

この OODA ループの概念を活用し、サイバー攻撃者の戦略が素早く変化し、それに対応する適切な対策が判別しにくいような場合でも、Observe(観察)と Orient(状況判断)を積極的に行い、そして分析結果をもとに、迅速かつ柔軟にサイバーセキュリティ対策を決定することで、変化に適応することができると考えられる。

６．　まとめと今後の課題

本稿では、金融機関における戦略的なサイバーセキュリティ対策の計画立案・推進に関する考察として、計画立案のための現状評価や分析、計画立案方法、そして継続的な改善方法に関する考え方等ついて解説した。

サイバーセキュリティを取り巻く環境は絶えず変化しているため、サイバーセキュリティに関する中長期計画を立てることは難しいが、計画を立てなければ、環境の変化に適時に対応できずに、事後的な対処に終始することになり、その結果、自組織だけではなく顧客をサイバーの脅威から守ることができなくなってしまう。一方で、サイバー空間を取り巻く大きな環境変化が起きたにもかかわらず、既存の計画に拘り過ぎてしまい、本来守るべき顧客や情報資産等が十分に守れないサイバーセキュリティ対策を施行し続けてしまっては本末転倒である。そのような事態にならないためにも、サイバーを取り巻く環境変化を常に観察、分析し、必要に応じて計画を補正しながら自組織や関連する組織、顧客にとって有意義な中長期的なサイバーセキュリティ対策を推進する必要がある。

サイバーセキュリティ対策は、各組織が自主的・自律的に行う必要があるが、各金融機関にとって共通の課題でもあるため、金融機関同士で協力しながら対応する、共助の精神で取り組むことでより効率的に改善することができると考えている。そのため、各金融機関や関係機関、金融庁等との積極的な情報共有やサイバーセキュリティに関する共同利用サービス等の検討等、建設的な対話をしながら、自助・共助・公助の精神をもって、すべての国民にとって安心･安全な金融サービスを提供できるように努力することが望ましい。そして、その安全に利用できる IT をさらに活用し、各金融機関は顧客へのサービス向上の分野で切磋琢磨していただきたいと考えている。

７．　補論

本稿にて、戦略的なサイバーセキュリティ対策の計画立案とその推進の必要性について理解いただけることを願っている。もしそうであれば、読者の方にはその必要性を認知した状態だけで終わらせることなく、具体的な行動に移していただきたいと考えている。

サイバーセキュリティは技術的要素の占める割合が高く、環境変化も早いため、IT やサイバーセキュリティに精通した担当者以外は、扱いにくいと感じている方も多いかもしれない。しかしながら、サイバーセキュリティにおいても、状況認識マネジメント(状況の把握や認識の共有、問題点の分析)、コミュニケーション(情報の伝達と確認)、意思決定(解決策の選択や決定、レビュー)、ワークロードマネジメント(優先順位付けやリソース配分)等の多くの経営陣や管理職が得意としているノンテクニカルスキルを活用することでサイバーセキュリティを高い次元で維持し、効率的な運営を行うことが可能であると考えている。そのため、サイバーセキュリティにおいても、本業である金融事業と同じように、それらのスキルを活用し、本稿で述べた手順を参考にしながら戦略的な計画を立案していただきたいと考えている。

サイバーセキュリティ対策の戦略的な立案の取り組みの状況は、図 13 に示す通り、3 つのレベルに分類できると考えている。

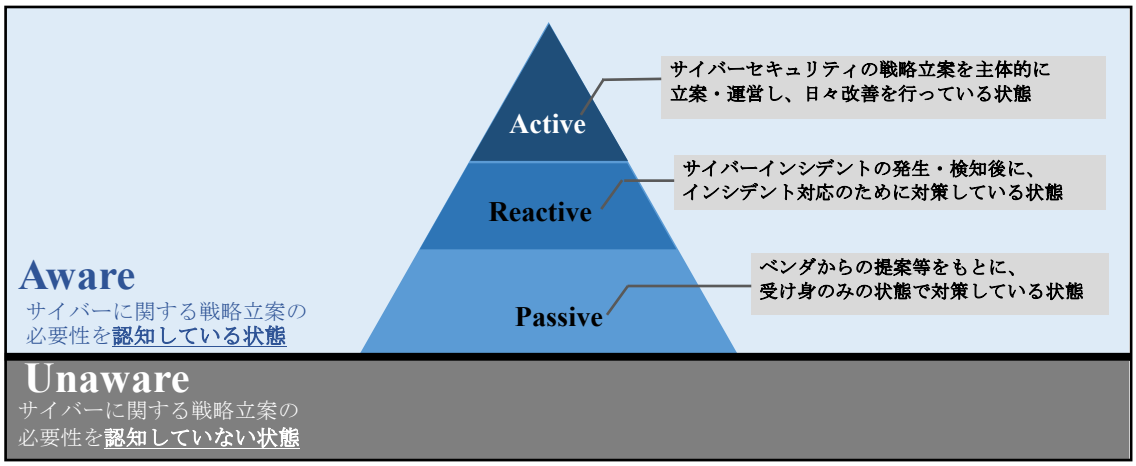


図 13　サイバーの戦略的な対策立案の取り組みの状況 (3 Levels of Engagement)

サイバーに関する戦略立案の必要を認知している状態における、3 つのレベルの最も下段の位置にある Passive のレベルとは、サイバーに関する戦略立案の重要性は知識として理解しているものの、具体的な行動を起こさず、受け身の状態である。例えば、自組織で主体的にサイバーセキュリティに関する計画を立てておらず、ベンダからの提案・営業活動のみに依存してサイバーセキュリティ対策を実施している状態である。このような状態では、その提案ベンダが得意とする対策のみに偏りが生じ、本来必要なサイバーセキュリティ対策に抜け漏れが生じてしまうおそれがある。

中央に位置する Reactive のレベルとは、自組織に深刻なサイバーインシデントが発生してからサイバーセキュリティの重要性を真に理解し、行動を起こす状態である。発生してしまったサイバーインシデントから学び、行動を起こすことは大切であるが、昨今のサイバーインシデントに関する報道や各種レポート等から学習し、そのような事態が発生する前にしっかりと対策や態勢を整えておくべきである。

最上位に位置する Active のレベルとは、サイバーセキュリティの重要性を十分に理解し、攻撃手法やその防御や検知の仕方等を十分に把握し、そして自らが率先して検討、活動、改善を行う状態である。

本論文の読後は知識として蓄えておくだけではなく、Active のレベルを目指して、自組織のサイバーセキュリティ対策状況を把握し、対策を主体的に立案、実施し、そして刻々と変化する環境変化に適応しながら組織運営を行うことで、顧客をはじめ従業員等をサイバーの脅威から守る活動に取り組んでいただけることを願っている。

謝辞

本論文の作成において、金融庁 総合政策局 リスク分析総括課 三浦調整官、明生総括をはじめ、IT・サイバーモニタリングチームの方から多くの有益なコメントを頂戴いたしました。深く御礼申し上げます。

参考文献

[1] 日本経済団体連合会(2019), サイバーリスクハンドブック 取締役向けハンドブック日本版,
（https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html）

[2] World Economic Forum(2022), グローバルリスク報告書 2022 年版,
（https://www.weforum.org/reports/global-risks-report-2022）

[3] 金融情報システムセンター(2021), 金融機関等コンピュータシステムの安全対策基準・解説書（第 9 版令和 3 年 12 月版）,
（https://www.fisc.or.jp/publication/book/005075.php）

[4] 金融庁(2016), FFIEC Cybersecurity Assessment Tool に関する調査研究,
（https://www.fsa.go.jp/common/about/research/20160815-1.html）

[5] NIST(2018), Cybersecurity Framework Version 1.1,
（https://www.nist.gov/cyberframework/framework）

[6] IPA(2018), 重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版,
（https://www.ipa.go.jp/files/000071204.pdf）

[7] CYBER RISK INSTITUTE(2021), The CRI Profile v1.2,
（https://cyberriskinstitute.org/the-profile/）

[8] 金融庁(2016), G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR,
（https://www.fsa.go.jp/inter/etc/20161011-2.html）

[9] 金融庁(2022) 監督指針,
（https://www.fsa.go.jp/common/law/index.html）

[10] 内閣サイバーセキュリティセンター(2021), 政府機関等のサイバーセキュリティ対策のための統一基準群,
（https://www.nisc.go.jp/policy/group/general/kijun.html）

[11] NIST(2020), SP800-53 組織と情報システムのためのセキュリティおよびプライバシー管理策 (IPA による翻訳),
（https://www.ipa.go.jp/files/000092657.pdf）

[12] NIST (2020), SP800-171 非連邦政府組織およびシステムにおける管理対象非機密情報 CUI の保護 (株式会社エヴァアビエーションによる翻訳),
(https://www.eva.aviation.jp/wp-content/uploads/2021/06/NIST-SP800-171Rev.22020FebJpV6.pdf)

[13] NIST (2020), SP800-207 ゼロトラスト・アーキテクチャ (PwC コンサルティング合同会社による翻訳),

（ https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf）

[14] 経済産業省(2017), サイバーセキュリティ経営ガイドライン Ver2.0,
（https://www.meti.go.jp/policy/netsecurity/mng_guide.html）

[15] IPA(2022), サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集 第 3 版,
（https://www.ipa.go.jp/security/fy30/reports/ciso/index.html）

[16] IPA(2021), 中小企業の情報セキュリティ対策ガイドライン,
（https://www.ipa.go.jp/security/keihatsu/sme/guideline/）

[17] IPA(2022), 情報セキュリティ 10 大脅威,
（https://www.ipa.go.jp/security/vuln/10threats2022.html）

[18] CSA(2018), クラウドコンピューティングのためのセキュリティガイダンス,
（https://www.cloudsecurityalliance.jp/guidance.html）

[19] ISO(2013), ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements,
（https://www.iso.org/standard/54534.html）

[20] ISO(2013), ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls,
（https://www.iso.org/standard/54533.html）

[21] ISO(2022), ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls,
(https://www.iso.org/standard/75652.html)

[22] CIS(2021), CIS Controls v8,
（https://www.cisecurity.org/controls/）

[23] NIST(2012), NIST-SP800-30 リスクアセスメントの実施の手引き(IPA による翻訳)
（https://www.ipa.go.jp/files/000025325.pdf）

[24] Col John R. Boyd, USAF, Retired Edited and Compiled by Dr. Grant T. Hammond (2018), A Discourse on Winning and Losing,
(https://www.coljohnboyd.com/static/documents/2018-03__Boyd_John_R__edited_Hammond_Grant_T__A_Discourse_on_Winning_and_Losing.pdf)

金融庁金融研究センター

〒100-8967　東京都千代田区霞ヶ関 3-2-1
中央合同庁舎 7 号館　金融庁 15 階

TEL：03-3506-6000（内線 3552）
FAX：03-3506-6716
URL：https://www.fsa.go.jp/frtc/index.html