NRI

金融ITフォーカス

Financial Information Technology Focus

特別号

金融機関のリスク・レジリエンスの潮流

－経済安全保障推進法「第２の柱」対応－

野村総合研究所
Nomura Research Institute

2023 9

巻頭言

2000年代後半のリーマン・ショックを発端として、個社の影響が金融業界全体へ波及するシステミックリスクの重要性が認識されました。以降、個々の金融機関に影響を与えうる、あらゆるリスクを特定し対応することが求められています。

例えば、本邦では、システム障害が金融サービスの提供に多大な影響を与えかねないことから、システムリスクは重要な管理対象となっています。昨今では、管理対象は「不作為・ミス」から「不正」へと広がり、コンプライアンスのみならず、コンダクト（不公正な行為全般）に関するリスクも注目され始めています。

世界的には、サイバーセキュリティリスクが増加の一途を辿り、また地政学リスクも高まりを見せる中で、オペレーショナル・レジリエンス（業務の強靭性・復旧力）の重要性が叫ばれています。日本も同様で、今春に金融庁が発出した文書では、サイバー攻撃を受けた際の早期復旧や影響範囲の軽減を担保する枠組み、いわゆるサイバー・レジリエンスが挙げられています。

こうした管理強化の流れの中、2022年5月に経済安全保障推進法が公布されました。本法は、安全保障の確保に向けた経済施策を支援と規制の両面から推進するものです。例えば、本法の4つの柱のうち、「重要物資の安定的な供給の確保」は「支援」の位置づけですが、「特定社会基盤役務の安定的な提供の確保」（以下、第2の柱）は「規制」色の濃い制度となっています。本特別号は、金融業界への影響の大きい第2の柱を中心に、対応上のポイントについてまとめたものです。

冒頭の特別対談では、森・濱田松本法律事務所のパートナー弁護士の梅津氏に、第2の柱の要諦である事前審査への対応を中心にお伺いしました。続く第1章で第2の柱の対応ポイントを概説し、その詳細として第2章でシステム開発、第3章でレジリエンス対応の今後について解説しております。最後に、第4章で欧米の動向を紹介し、経済安全保障の世界的な動きを概観しました。

本特別号が、金融サービスの安定提供に向けた活動の一助となれば幸いです。

2023年9月吉日
執行役員
金融ITイノベーション事業本部長
山崎政明

特別対談

経済安保（第二の柱）制度運用開始までに金融機関が準備すべきこと

梅津 英明様
Hideaki Umetsu
森・濱田松本法律事務所
パートナー弁護士

2004年 弁護士登録。09年 シカゴ大学ロースクール修了（LL.M.）。10年 ニューヨーク州弁護士登録。専門は、日本企業による海外M&A・海外進出、海外ガバナンス・コンプライアンス、国際通商・経済安全保障法制、「ビジネスと人権」等。21年 国際法曹協会（IBA）アジア大洋州議会 共同議長（～22年）、日本弁護士連合会 国際活動・国際戦略に関する協議会 委員（～現在）。

堤 順
Jun Tsutsumi
株式会社野村総合研究所
金融リスク管理部長

1991年 野村総合研究所入社。証券会社向けトレーディングシステム開発に従事。96年から2000年まで、NRIヨーロッパに出向し、現地日系証券会社の基幹系システム再開発プロジェクトに参画。03年から06年まで野村證券に出向。06年よりリスクマネジメント、ITガバナンス等のコンサルティングに従事。ERM事業企画部長などを経て、23年4月より現職。

経済安全保障推進法が昨年5月に成立して以後、金融機関に影響のある「基幹インフラ役務の安定的な提供の確保」についても、有識者会議での議論、「基本方針」・「基本指針」などを通して、その制度の中身が明らかになりつつある。制度運用開始まで1年を切った中で、金融機関が準備すべきこと、留意すべきことについて森・濱田松本法律事務所のパートナー弁護士の梅津氏に語っていただいた。（対談収録日：2023年7月6日）

法案可決後の動き

堤　昨年5月、経済安全保障推進法（以下、推進法）が参議院で可決されてから1年が経過しました。はじめにどのような形で進んできたかを教えていただけますか。

梅津　推進法の中には4つの柱が入っています。一つが特定重要物資などと最近話題になっていますが、サプライチェーンの強靱化、一つが基幹インフラ役務の安定的な提供、そして、先端的な重要技術の官民協力での開発、非公開特許の出願です。

推進法はアメ（支援的な施策）とムチ（規制的な施

策）で構成されていますが、アメから施行が優先して進んでおり、サプライチェーンの強靱化、官民協力での技術開発が先行し、既に去年8月に施行されています。

基幹インフラと非公開特許は、今まさに進んでいるところです。「経済安全保障法制に関する有識者会議」（以下、有識者会議）での議論もその順になっています。

4つの柱のそれぞれで「基本指針」を出すことになっており、これも、同じ順番となっています。

堤　4つの柱のうち金融機関への影響が大きいのは、基幹インフラのところです。基幹インフラの基本指針は4月末に閣議決定されました。まず、基本指針の位置づけについて教えていただけますか。

梅津　基本指針は、詳細なルールができる前の基本的な考え方が書かれている資料です。基本インフラに関する「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」の中に、特定社会基盤事業とは何か、特定社会基盤事業者を指定する際の考え方、特定妨害行為をどのように考えて詳細なルールを策定していくのか、事前の届け出の制度の基本的な設計についての考え方、などが書かれています。

基本指針では特定社会基盤事業者について、「事業規模」又は「代替可能性」で見ますということが書かれています。ここで基本的な考え方が示されていますので、事業規模については具体的な数字に落とし込んでいくことになります。代替可能性については、ほかに代替できる者がいるのか、という観点で基幹インフラであるかが見られていくことになります。

さらに、そのときに留意すべき基本的な考え方として2つ示されています。一つは、「適正な競争関係を不当に阻害することがないように」ということ。もう一つは、「中小規模の事業者の指定については、より慎重に検討を行ってください」ということです。

こうした考え方のもと、例えば銀行の特定社会基盤事業者の指定基準として、預金残高が10兆円以上、又は、口座数が1000万口座以上、又はATM台数が1万台以上といった数字が出てきています。

さらに基本指針では、「指定」に関しては、「指定基準を満たすこと」で「機械的に行われるものではなく、特定社会基盤事業の状況や事業者が提供する役務の実態等も踏まえて判断します」と言っています。すなわち、すべての要件に該当するからといって、指定されるのかというと、そうではないということです。要件を満たすけれども指定しない場合は「理由を説明するなどの対応を」所管大臣はしてくださいということも、基本指針に書かれています。

堤　今後は、どのようなスケジュールで進むのでしょうか？

梅津　経済安全保障法制の詳細は有識者会議で議論されています。その有識者会議が6月12日に開催され、その直後にパブリックコメントが始まっています。

パブリックコメントは幾つかに分かれています。6月から7月の半ばまで、特定社会基盤事業の内容を細かく定めた政令、それから特定社会基盤事業者の指定基準や特定重要設備とは何かついての基準を定めた主務省令が、パブリックコメントにかかっています。

秋に第2弾が出て、いろいろなQ＆Aが出されたのち、制度の運用開始は今のところ令和6年の春頃が想定されています。

基幹インフラ事前審査の枠組み

堤　気になるのが、事前審査についてですが、今後の流れについて教えていただけますか。

梅津　特定社会基盤事業者が特定重要設備を導入する場合、また「重要維持管理等」の委託と呼ばれていますが、他の事業者に維持管理等をお願いする場合に、事前審査の届出書を出さなくてはなりません。その届出書は「導入等計画書」と呼ばれています。

この計画書の中に何を書くべきか、設備等のサプライヤー、もしくは重要維持管理等であればその委託先・再委託先について、どこまで情報を書くべきか、今議論がなされています。いずれにしても、それを「提出する」という行為が審査の開始のタイミングになります。

それを提出した後、原則として審査期間は届出の受理から30日間となっています。場合によっては最長4か月まで延ばすことができる、となっています。

ただし、主務官庁に事前相談窓口のようなものが設けられ、届出受理の前に色々なやりとりが生じることが想定されます。

堤　審査の結果が、よろしくない場合には、どうなるのでしょうか？

梅津　審査の結果が出て、もし「中止しなさい」とか「変更しなさい」ということになった場合には、勧告後10日以内に勧告を応諾するかどうかの通知が義務づけられています。

堤　事前審査のために提出する導入等計画書について、有識者会議でもかなり突っ込んだ議論があったかと思います。その辺りはいかがでしょうか？

梅津　具体的に何を書かないといけないかについては、秋頃に出される省令案で決まっていくことになりますが、少しずつその中身が見えてきています。

例えば、新しく特定重要設備を導入する場合に書く内容は、まず「特定重要設備の供給者の名称、住所、設立国」です。これらは会社の情報です。さらに、その周辺の情報も出してくださいということがわかりつつあります。ここが企業の皆様には気になるところだと思います。例えば、「特定重要設備の供給者の議決権の5%以上を直接保有する者に関する情報」として「名称、国籍、議決権保有割合」、同じように、サプライヤーの「役員等の氏名、生年月日、国籍」、サプライヤーが過去3年間において外国の政府・政府機関・地方公共団体といった「外国政府等」と呼ばれる所との売上高が、その供給者の総額の25%以上を占める場合には、「その相手国とその割合、特定重要設備をつくっている国又は地域」の提出が求められます。

ですので、外国の主体からの影響がどれくらいあるかを判断するための情報を出してくださいということです。重要維持管理等の委託先についても同じようなコンセプトが入ってきています。

堤　役員や議決権保有者の国籍などは、ある意味機微情報だと思います。特に、議決権保有者に国籍の提出を供給者等の企業が約束できるのか、という点が気になります。

梅津　役員と株主を分けて考えたいと思います。役員の中でも、自社の役員とサプライヤーの役員でも変わってきます。

まず、自社の役員については通常は出せると思われます。サプライヤーの役員情報も、少なくとも日本国内であれば、聞いて任意で回答してくれれば出せると思います。個人情報保護法の話も、少なくとも日本法上は一定の整理をすることは可能であろうと思います。もちろん、国籍情報が非常にセンシティブな場合もありますので、そのような点を配慮しつつ、必要最低限の範囲で当局に出していくといった留意は必要です。

堤　株主についてはいかがでしょうか？

梅津　非上場会社は、一般的には、定款で譲渡制限をつけて、株主が変更される場合には会社に通知が来て取締役会が承諾して初めて株主が変わります。ですから、株主の変遷を追っていくことは可能で、5%以上を持っている株主を把握することも可能です。

難しいのは上場会社です。上場会社の場合はそもそも、誰がこの瞬間に5%以上保有しているのかわかりません。株主名簿を締めるタイミングは通常は基準日で、株主総会が6月の会社であれば通常は3月末です。それ以外は、毎日変動していますからわかりません。

また、例えば、株主が大量買付けを行い、株主提案で役員候補を指名して、それが可決されてしまった場合どうなるか。会社としては、余り背景を知らない人が役員になってしまい、国籍情報がわからないという場合も、

一応理論上は想定されるかもしれません。

なお、おそらく、5%という数字は意味があるのだと思います。パブリックコメントを詳細に読むと、ほかの制度の基準も考慮しつつ定めていく、といった回答が書かれています。おそらく大量保有報告書等の既存の制度を意識した制度設計がなされていくのだろうと思います。

ただ、例えば、大量保有報告書の基準は「5%超」ですが、こちらでは「5%以上」とされていたり、大量保有報告書では共同保有者と合計して5%超になる場合には出さないといけません。大量保有報告書で言う5%とこちらで言う5%とが本当に一致するのかどうかは、今後詳細を見ないとわかりません。

堤　大量保有の意味だとばかり思っていましたが、そこにも奥深さがあるわけですね。

梅津　大量保有報告書は、外国株主を把握するための制度ではありませんので、今回の趣旨とは異なります。

株主を把握できたとして、株主の国籍情報をどうやって見ていくかが次の課題としてあります。

会社が保有している場合は、設立準拠法国なので、その会社の情報、登記等を見れば、どこに準拠法があって設立されている会社なのかをある程度確定できます。しかし、個人が持っている場合や登記制度がしっかりしていない国の法人が持っている場合の確認方法は今の資料だけでは未知数と言えます。

ただ、参考になる制度が既存の制度にないわけではありません。あくまで私見ですが、例えば放送法や電波法、航空法には外資規制が入っています。放送事業者の一定の役員には外国人は就けないといった制度があります。そこでは、国籍を見ています。ですので、役員や株主の国籍を見る制度はないわけではないです。

ただ、実際上、確認が困難な場合も否定はできないのではないかと思います。

そうすると、最終的に何が問題になるかというと、この届出を出すときに「不明」という記載がどこまで許されるかだと思います。やむを得ず国籍の欄に「不明」と書いて出したときに、それがどのように見られるか等です。審査の中で「不明」という情報が残った場合にどういう判断がなされるのかはまだ分かっていません。

堤　リスク管理措置にもあるので、金融機関と供給者等の企業は、情報提供を契約で約束します。そうなると、ヘッジ文言が入りますよね。

梅津　仮に約束するとしても、適法な、できる範囲において情報を提供することになると思います。適法なあらゆる手段を尽くしたけれども情報が出ないということについては、「不明」と書かざるを得ない場合もあると思います。

堤　確かにそうですね。契約で記載されているからといって違法に入手していいわけはないですよね。

梅津　違法に入手しないと義務違反になることは、契約の建付けとしておかしいと思います。

最終的に、本当に取れる情報なのかというところに行きつくのだと思います。あとは、そのために手段を尽くしたか。株主にアプローチして確認を行った、という証跡を残す。もしくは、間接情報などを提供するといった選択肢もあるかもしれません。

堤　国籍情報は、個人情報保護法の考慮が当然必要になると考えていいですね。

梅津　そうですね。おそらくは実務上は基本的に「本人の同意をもらう」になると思います。強制的に何かを出す手段は考えにくいと思います。

出してもらう情報については、「法律の定める範囲で政府と共有します。特定社会基盤事業の導入等計画書の提出の目的で記載します」という前提で入手します。同意があれば、それを政府に渡したところで、違法な第三者提供に該当するとは基本的には考えられません。ただ、何らかの理由で本人の同意がない場合でも、個人情

報保護法上の一定の例外事由として認められる可能性はあると思います。

ただ、問題は海外です。同意がある場合には、どこの国でも多くは問題にならない可能性が高いと思いますが、一部の国では問題になる可能性もあります。また、同意がない場合や同意が撤回された場合等を含め、各国の法令に基づき慎重に対応する必要があります。

堤　なかなか難しい問題ですね。

梅津　もう一つ重要な要素としては、国籍を提出するといっても、国籍差別をする趣旨ではないということです。

パブコメの政府の回答を見ても、国籍のみを理由に拒絶することはない、あくまで考慮要素の一部です、と書かれています。

推進法以外の動き

堤　推進法以外で、経済安全保障に関連した動きがありましたら教えていただけますか。

梅津　当初、経済安全保障推進法に入るかもしれないといわれていたセキュリティ・クリアランスは、今議論が進められています。6月に、経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議から中間論点整理が出ました。立法に向けた動きが報道されています。

外為法については、物の管理と投資管理の両方があり、そのうちの物の管理が相当動いています。物の管理とは、物、データ、技術の輸出入です。

一つは、半導体の輸出規制です。これまでは、日本政府の輸出管理はあくまで、ワッセナー・アレンジメント（正式名称：通常兵器及び関連汎用品・技術の輸出管理に関するワッセナー・アレンジメント）や、多くの国々が参加している国際レジームの中で、「兵器を管理します」「大量破壊兵器に使われることを管理します」ということで、多数国との協調の中で管理してきました。

今回の半導体の輸出規制は、そうしたレジームとは別に、オランダ、アメリカ等の同盟国・同志国との議論の中で導入していますので、エポックメイキングなことです。

もう一つは、人権を理由とする輸出管理の動きです。日本は今年3月に、アメリカが主導している「輸出管理と人権イニシアチブ」の行動規範に賛同することを公表しました。このイニシアチブは2021年12月に発足し少数国の参加でしたが、この3月に24か国に増えました。英語名称が、Export Controls and Human Rights Initiativeですので、export controlにhuman rightsの観点を入れていきますというイニシアチブです。ただ、日本の外為法は、基本的には国際社会の平和及び安全等を目的とした安全保障貿易管理の枠組みがベースとなっています。今般の半導体の輸出規制も、軍事転用の防止を目的として導入されています。人権を理由とする時に、どのような形で整合性をとるのかが今後議論されていく課題だと思います。

また、推進法で特定重要物資が指定され、それが外為法上の投資管理のコア業種に追加される等の動きもあります。そういう形で推進法と外為法との相互の連携が実例としても出始めていることは今後の動きを推測する上でも重要なことかと思います。

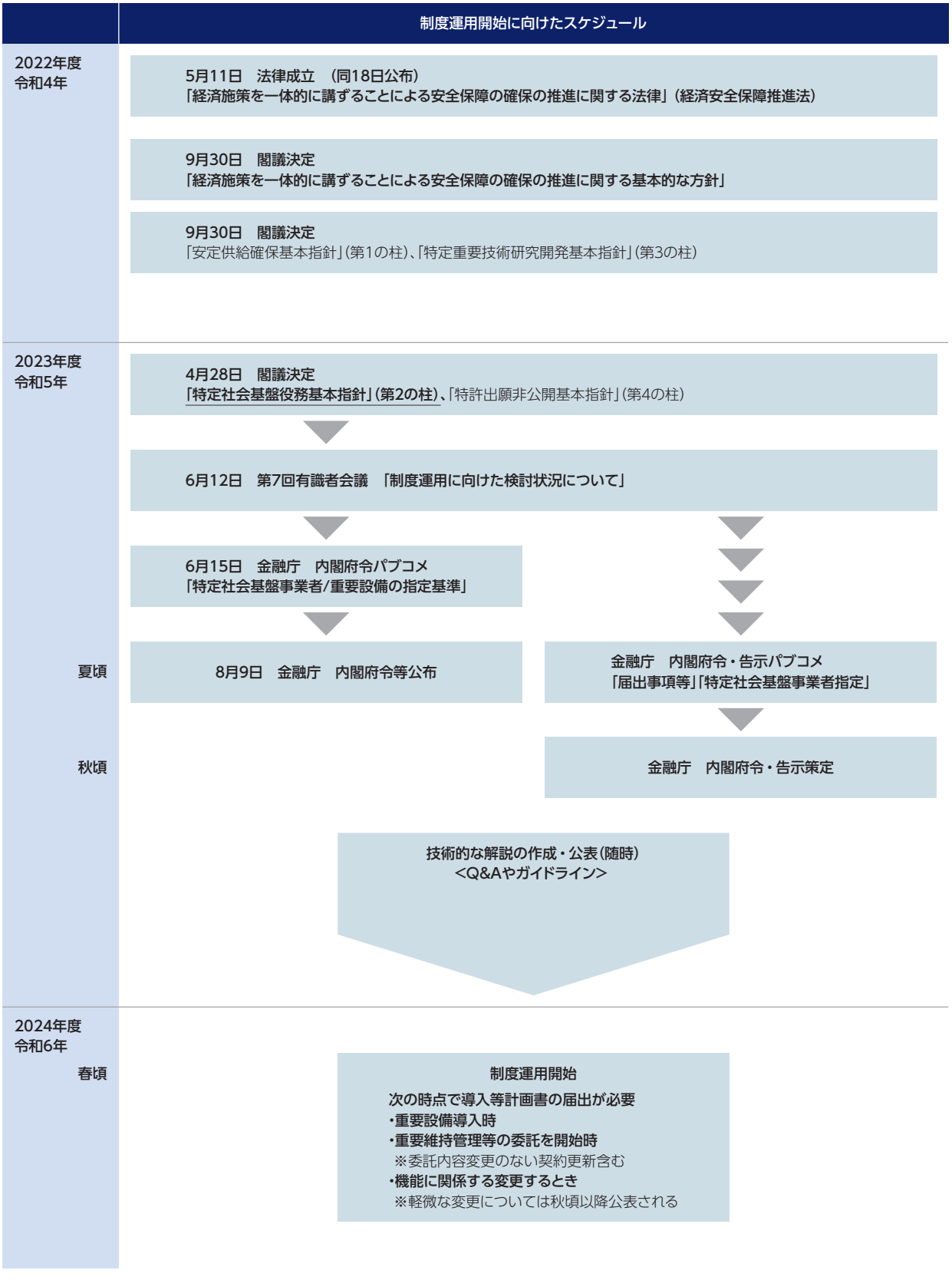
堤　今回の動きは米国が主導しているのでしょうか。

梅津　半導体の輸出管理も、人権を理由とする輸出管理もやはり米国が中心になっている面が強いと思います。ICTセクター、通信等のセクターも、アメリカがかなり強烈な規制を入れており、ほかの国がそれに追従するかどうか様子を見ている感じになっています。欧州も一部ついて行ったり、ついて行かなかったりしていますが、総じて米国・欧州・日本で協調した政策が出ることが多くなっているように感じます。

堤　前回[1)]に続き、今回も貴重なお話をありがとうございました。政省令が出される前から準備をしておかないと間に合わない、ということを改めて感じた次第です。

（文中敬称略）

1）「金融ITフォーカス」2022年7月号対談


制度運用開始に向けたスケジュール
2022年度
令和4年
5月11日　法律成立　（同18日公布）
「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（経済安全保障推進法）
9月30日　閣議決定
「経済施策を一体的に講ずることによる安全保障の確保の推進に関する基本的な方針」
9月30日　閣議決定
「安定供給確保基本指針」（第1の柱）、「特定重要技術研究開発基本指針」（第3の柱）
2023年度
令和5年
4月28日　閣議決定
「特定社会基盤役務基本指針」（第2の柱）、「特許出願非公開基本指針」（第4の柱）
6月12日　第7回有識者会議　「制度運用に向けた検討状況について」
6月15日　金融庁　内閣府令パブコメ
「特定社会基盤事業者/重要設備の指定基準」
夏頃
8月9日　金融庁　内閣府令等公布
金融庁　内閣府令・告示パブコメ
「届出事項等」「特定社会基盤事業者指定」
秋頃
金融庁　内閣府令・告示策定
技術的な解説の作成・公表（随時）
<Q&Aやガイドライン>
2024年度
令和6年
春頃
制度運用開始
次の時点で導入等計画書の届出が必要
・重要設備導入時
・重要維持管理等の委託を開始時
※委託内容変更のない契約更新含む
・機能に関係する変更するとき
※軽微な変更については秋頃以降公表される

第1章 経済安全保障推進法：金融分野における「第２の柱」対応概説

経済安全保障推進法の概要とスケジュール

経済安全保障推進法[1]は2022年5月に公布され、同年8月より段階的に施行されている。本法は、近年の国際情勢の複雑化や社会経済構造の変化等を踏まえ、国家・国民の安全を経済面から確保するために、安全保障の確保に向けた経済施策を総合的かつ効果的に推進していくものである。

金融サービスは、電気、ガスなどと同様に国民生活や経済活動の基盤となる重要インフラのひとつであることから、国が民間に関与する4つの制度（柱）のうち、「特定社会基盤役務[2]の安定的な提供の確保」（以下、第2の柱）において、その施策の詳細が定められている。

第2の柱では、2023年秋頃に対象事業者が指定され、2024年春頃に審査が開始される。本制度は運用が目前に迫り準備期間も短いことから、タイトなスケジュールでの対応が求められる[3]（図表1-1）。

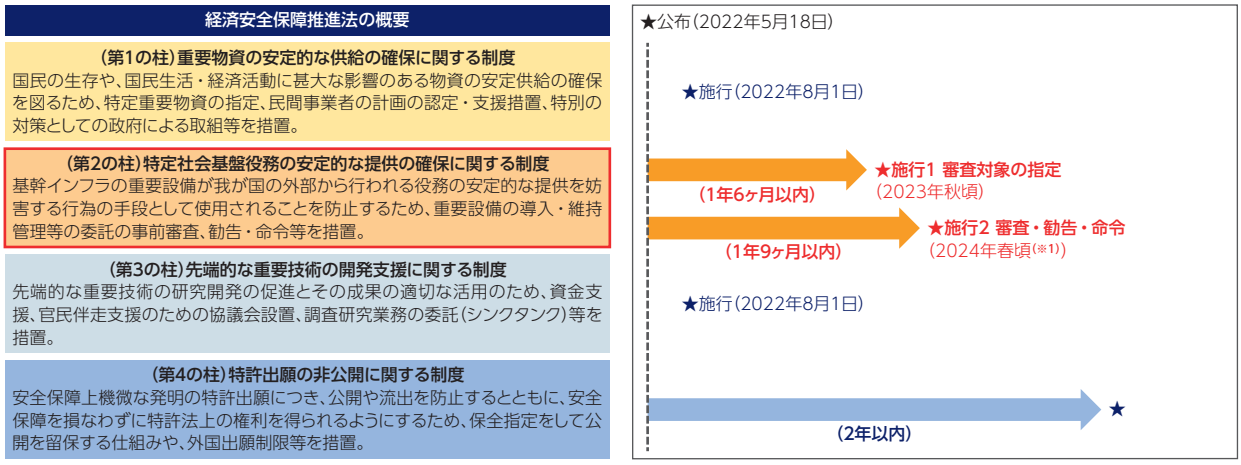
第2の柱における審査の対象は、事業規模等により指定される一部の事業者に限られるが、それ以外の事業者においても主要なサービスの安定的な提供が確保されることが望ましいとされている[4]。第2の柱は、直接の審査対象ではない多くの金融事業者にとっても注視すべき内容といえるだろう。

本稿では、4月28日に閣議決定された第2の柱の「基本指針」[5]、ならびに制度の運用開始に向けた「検討状況資料」[6]に基づき、第2の柱について概説するとともに、金融分野における対応上のポイントも考察したい。

「第2の柱」の要請事項

第2の柱の目的は、国家を背景としたサイバー攻撃の脅威から、国民生活や経済活動の基盤となるインフラ事

図表1-1　経済安全保障推進法の概要とスケジュール



（※1）審査対象の指定か6ヶ月間の経過措置有
（出所）内閣府ホームページ掲載情報を基に野村総合研究所作成

業を守ることにある。国外では、ウクライナの変電所（2015年）、米国のパイプライン事業者、欧州を中心とした物流企業など、サイバー攻撃の被害に遭っている事例が見られる。こうした攻撃の中には、国家を背景とした形で行われるものもある。組織的かつ洗練されたサイバー攻撃の脅威が増大している中において、インフラ事業の安全性・信頼性の確保は、我が国の安全保障においてますます重要な要素となっている。

第2の柱の要請事項をひとことで表現するならば、次のようにいえるだろう。

『特定社会基盤事業者は、特定社会基盤事業に関する役務の提供に際して、特定重要設備の導入及び重要維持管理等の委託を行う場合は、事業所管大臣が行う事前審査を受けなければならない』

「特定社会基盤事業者」とは、事業規模（銀行、保険、証券、信託等）、もしくは代替可能性（取引所や各種決済インフラ等）のいずれかの観点から指定される事業者等のことであり、金融分野では（図表1-2）の通り定められる。なお、事業規模に基づく指定基準[7]は、対

図表1-2　特定社会基盤事業者の指定基準

【事業規模】

事業の指定	指定基準（各々の数値は直近3事業年度の値の平均）	特定重要設備	重要維持管理等
銀行業	•預金残高：10兆円以上 又は •口座数：1,000万口座以上 又は •ATM台数：1万台以上	預金・為替取引システム	•システムの保守点検 •システムの運用
資金移動業	•利用者数：1,000万人以上 かつ •年間取扱額：4,000億円以上	為替取引システム	
保険業	【生命保険業免許を受けた者】 •保険金等支払金(※1)：1兆円以上 又は •契約件数：2,000万件以上 【損害保険業免許を受けた者】 •元受正味保険金：1兆円以上 又は •契約件数：2,000万件以上	保険金支払システム	
第一種金融商品取引業	•預り資産残高：30兆円以上 又は •口座数：500万口座以上	注文約定システム	
信託業	•信託財産額(※2)：300兆円以上	財産管理システム	
第三者型前払式支払手段の発行の業務を行う事業	•年間発行額：1兆円以上 かつ •加盟店数：1万店以上	前払式支払手段の発行に係るシステム	
包括信用購入あっせんの業務を行う事業	•会員契約数：1,000万以上 かつ •年間取扱高：4兆円以上	クレジットカード決済の承認（オーソリゼーション）に係るシステム	

【代替可能性】

事業の指定	指定基準	特定重要設備	重要維持管理等
系統中央機関	系統中央機関の業務を行う者	預金・為替取引システム	•システムの保守点検 •システムの運用
取引所金融商品市場の開設の業務を行う事業	取引所金融商品市場の開設の業務を行う事業を行う者(※3)	売買システム	
金融商品債務引受業	免許又は承認を受けた者	清算システム	
資金清算業	免許を受けた者	資金清算システム	
預金保険法34条に規定する業務を行う事業	事業を行う者	破綻処理業務システム	
農水産業協同組合貯金保険法第34条に規定する業務を行う事業	事業を行う者		
振替業	指定を受けた者	振替システム	
電子債権記録業	指定を受けた者(※4)	電子債権記録システム	

（※1）解約返戻金、その他返戻金及び再保険料を除く
（※2）再信託等した額を除く
（※3）直近3事業年度の有価証券の総売買代金が75兆円未満である者を除く
（※4）直近3事業年度の電子記録債権の残高が1兆円未満である者を除く
（出所）「特定社会基盤役務の安定的な提供の確保に関する制度の運用開始に向けた検討状況について」（内閣官房 経済安全保障法制に関する有識者会議 2023年6月）及び「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律に基づく特定社会基盤事業者の指定等に関する内閣府令」（2023年8月9日）を基に野村総合研究所作成

象の事業者で国内事業の5割超が確保されることを目安として定められている。

「特定重要設備」とは、主要なサービスの提供に用いられる重要な設備、機器、装置またはプログラムの総称である。金融分野では、サービスの中枢を担う情報システムがこれに該当する。こうした設備に対して不正機能が埋め込まれたり、機器の脆弱性に関する情報が意図に反して共有されたりするといった妨害行為を防ぐことが求められる。なお、こうした「特定社会基盤事業に関する役務の安定的な供給を我が国の外から妨害する行為」のことを**「特定妨害行為」**という。

「重要維持管理等」とは、特定重要設備の維持管理または操作のことであり、保守点検、機器・部品の交換、プログラムの更新等のことをいう。金融分野では、システムの保守点検や運用がこれにあたる。こうした業務を外部に委託する場合は、委託先が委託業務を通じて特定妨害行為に加担するおそれのないよう、管理できていることが求められる。

事前審査：審査における考慮要素

第2の柱では、「特定重要設備の導入及び重要維持管理等の委託について、導入等計画書の事前届出を求め（中略）審査を行う」こととされている。事前審査は、

- 外部にある主体から強い影響を受けているか
- リスクに関する評価を自ら行い、リスク管理措置を講じているか
- 構成設備に脆弱性が指摘された例、維持管理に対して不適切性が指摘された例、国内法令や国際的基準で不適切性が指摘された例がないか
- その他、同盟国・同志国に指摘された例がないか

の4要素を考慮して実施される。このもとに、特定重要設備が特定妨害行為の手段として使用されるおそれが大きいと認められた場合は、事業所管大臣より勧告及び命令が行われる場合がある。また、国際情勢の変化その他の事情の変更により、審査後であっても必要な措置の実施を勧告及び命令することができるとされている。

基本指針では、「我が国の外部から行われる妨害行為に着目し、審査を行うに当たっては、我が国の外部にある主体から強い影響を受けている事業者からの設備の導入等について慎重な審査を行う必要があり、国家安全保障戦略等に示されたように、我が国が戦後最も厳しく複雑な安全保障環境に直面していること等も踏まえる」と謳われている。しかしながら、本制度ではいわゆるブラックリスト制度は設けないとされていることから、「外部にある主体からの強い影響」をどのように審査するかまでは分からない。特定社会基盤事業者としては、後述の「リスク管理措置」への対応を通じて、特定妨害行為の防止に向けた十分な管理態勢を整備しておくことが、審査において重要となるだろう[8)]。

事前審査：届出事項

事前審査で届出が求められる導入等計画書への記載事項案は（図表1-3）の通り。ここでは、我が国の外部からの影響の有無や程度を評価するために必要となる情報として、導入や維持管理に関わる事業者等に関する情報の網羅が求められる。

特定重要設備では、その供給者が特定社会基盤事業者に導入するまでに経由する販売会社の名称等を届け出る必要がある。また、その一部を構成する設備（構成設備）についても、設備情報に加えて、供給者の名称や住所等、の届出が必要となる。

重要維持管理等では、最終的に委託を受けた者（N次の委託先）までの網羅が求められる。これ自体は金融当局から以前より求められていることだが、ポイントは届出に際して求められる情報にある。（図表1-3）（3）にあるような議決権保有者の国籍、役員等の生年月日や国籍、外国政府等との取引高の割合及び相手国といった情報は、その機微性から委託元への提供が困難であることも考えられる[9)]。こうした事情に鑑み、機微性を有する情報は、委託先から事業所管大臣へ直接提出することが

図表1-3　導入等計画書の記載事項（案）

	特定重要設備	重要維持管理等
(1) 設備の概要	•**種類、名称、機能、設置及び使用する場所**	–
(2) 内容及び時期	•導入の**目的**、特定重要設備の導入に携わる**事業者の名称**(※1) •導入の**時期**（設計・開発・組立・設置等が完了し役務の提供の用に供する時点）	•重要維持管理等の**目的、業務内容、実施場所** •委託の**時期または期間**（単発・反復の違いや継続性の有無等の内容に応じて時期または期間を記載） •**再委託の相手方に関する事項**(※2)
(3) 供給者／委託の相手方に関する事項 特定社会基盤事業ごとに主務省令で定める	•特定重要設備の供給者または重要維持管理等の委託の相手方の、**名称、住所、設立国** •**議決権の5%以上**を直接保有する者に関する情報（**名称、国籍等、議決権保有保有割合**） •特定重要設備の供給者または重要維持管理等の委託の相手方の、**役員の氏名、生年月日、国籍** •特定重要設備の供給者または重要維持管理等の委託の相手方が、過去3年間において、**一の外国政府等**(※3)**との売上高が、売上高の総額に占める割合の25%以上**を占める場合、その**相手国及び割合**	
	•設備を製造する場所の所在する**国または地域**	•**再委託の相手方に関する事項**(※4)
(4) 構成設備に関する事項 特定重要設備の実態等を踏まえて主務省令で定める	•構成設備(※5)の**概要：種類、名称、機能等** •当該構成設備の**供給者**(※6)**の名称、住所等**	–
(5) 有効な措置に関する事項	•**「リスク管理措置」に関する内容**（（図表1-4）参照）	

(※1) 供給者から導入するまでに経由する事業者までを含む（例えば、販売会社を経由して供給者から調達する場合は、販売会社の名称等を届け出る必要がある）
(※2) 最終的に委託を受けた者（N次の委託先）までを含む（検討状況資料では、同等の事項を記載、とある）
(※3) 外国の政府、外国の政府機関、外国の地方公共団体、外国の中央銀行若しくは外国の政党その他の政治団体
(※4) 最終的に委託を受けた者（N次の委託先）までを含む（検討状況資料では、同等の事項を記載、とある）
(※5) 設備の一部を構成する設備、機器、装置又はプログラムであって特定妨害行為の手段として使用されるおそれがあるもの
(※6) 構成設備と他の機器を一体として組み上げて供給する者も含まれる（検討状況資料では（特定重要設備と）同等の事項を記載、とある）
(出所)「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」（2023年4月28日閣議決定）及び「特定社会基盤役務の安定的な提供の確保に関する制度の運用開始に向けた検討状況について」（内閣官房 経済安全保障法制に関する有識者会議 2023年6月）を基に野村総合研究所作成

できるよう配慮されることとなっている。

事前審査：リスク管理措置

特定妨害行為の防止には、特定社会基盤事業者が自らリスクを評価し措置を講ずることが有効であることから、リスク管理措置の内容も事前審査の対象となる。リスク管理措置は全部で9つの措置からなり、更に個々の措置に対する具体例として、全部で28の項目が定められている（図表1-4）。

リスク管理措置の届出様式案（図表1-5）より、審査では28項目の実施状況の回答に加えて、それを裏付ける資料の添付が求められる。また、特定社会基盤事業者が主体的に実施している取組を記載する項目も設けられる。事前審査では、こうした情報に基づき、管理の実質・実態を重視した評価がなされていくものと考えられる。

以下では、システムリスクやサイバーセキュリティに関する現状の管理態勢との比較において、対応上のポイントになると思われる点を中心に概観する。

【不正な変更の防止】（措置①、④）

措置①と④では、不正な変更や、意図しない変更の防止に関する施策の実施が求められている。

措置①は、製造等の過程を対象としたものである。特定社会基盤事業者としての金融事業者（以下、金融事業者という）にとっての特定重要設備は、サービスの中枢を担う情報システムであるから、その製造等の過程とはシステム開発工程のことである。現状のシステム開発ではテストを通じた品質の検証は十分に行われているが、項目（1）のような悪意あるコード等の不正混入への対応と検証はさほど重要視されてこなかったのではないだろうか。こうした不正なプログラムの埋め込みへの対策としては、ソースコード解析ツールの利用が考えられる。ソースコードの検品過程でバッファオーバーフロー[10]やメモリリーク[11]につながるコードの検知、重大なセキュリティリスクや危険ソフトウェアの脆弱性の検出などを行うことにより、システムの安定的な提供を阻害する要因を未然に洗い出すことが可能となる[12]。

措置④は、システムの運用と維持保守に関する内容である。項目（14）で定められている本番作業統制などは、既に多くの金融事業者で厳格に実施されているも

図表1-4　リスク管理措置

（特定重要設備の導入に係るリスク管理）	
①	**特定重要設備及び構成設備の供給者における製造等の過程で、特定重要設備及び構成設備に不正な変更が加えられることを防止するために必要な管理がなされ、当該管理がなされていることを特定社会基盤事業者が確認できることを契約等により担保している。** **(1)** 悪意のあるコード等の混入の確認（受入検査等の検証体制、導入前の脆弱性テストの実施） **(2)** 情報セキュリティ要件の実装状況の確認（セキュリティパッチの適用、不正プログラム対策ソフトウェアの最新化） **(3)** 品質保証体制の確立　**(4)** 製造工程における不正行為の有無の定期的な確認　**(5)** 製造環境における物理・論理的統制の確認 **(6)** インターネット回線接続時の不正アクセス防止マニュアル等の整備　**(7)** 設備の設置に際しての不正な変更等を防止する体制の確認 **(8)** 不正な変更やそのおそれを発見した場合の詳細調査や立入検査等への協力の確認
②	**特定重要設備又は構成設備について、将来的に保守・点検等が必要となることが見込まれる場合に、当該保守・点検等を行うことができる者が特定重要設備又は構成設備の供給者に限られるかどうか等の実態も踏まえ、供給者を選定している。** **(9)** 供給者によるサービス保証の確認　**(10)** 保守・点検等が受けられなくなった場合を想定した代替手段の検討等
③	**特定重要設備及び構成設備について、不正な妨害が行われる兆候を把握可能な体制がとられており、不正な妨害が加えられた場合であっても、冗長性が確保されているなど、役務の提供に支障を及ぼさない構成となっている。** **(11)** ランサムウェア等に感染した場合の不正な妨害に対する役務提供体制の整備（バックアップの取得・隔離管理、復旧手順、代替設備との交換等） **(12)** 情報の漏洩等の情報セキュリティインシデントが発生した場合の対応方針・体制の整備（マニュアル等、定期的な訓練等） **(13)** アクセス制御と不正アクセス監視の仕組の導入・実装
（重要維持管理等の委託に係るリスク管理）	
④	**委託された重要維持管理等の実施に当たり、委託**（再委託（再委託された重要維持管理等の全部又は一部が更に委託されるものを含む。以下同じ。）を含む。）**を受けた者**（その従業員等を含む。）**によって、特定重要設備について特定社会基盤事業者が意図しない変更が加えられることを防止するために必要な管理等がなされ、その管理等に関する事項を特定社会基盤事業者が確認できることを契約等により担保している。** **(14)** 操作ログや作業履歴等の保管と確認に関する手順の整備、不正行為の有無の定期的または随時の確認 **(15)** 最新のセキュリティパッチの適用等、資産管理の定期的な実施　**(16)** 設計書や設備等の情報への、物理的・論理的な制限 **(17)** 定められた運用要員以外の物理的・論理的な制限　**(18)** サイバーセキュリティ教育・研修等の実施によるリテラシーの維持向上
⑤	**重要維持管理等の再委託が行われる場合においては、再委託を受けた者のサイバーセキュリティ対策の実施状況を確認するために必要な情報が、再委託を行った者を通じて特定社会基盤事業者に提供され、また、再委託を行うことについてあらかじめ特定社会基盤事業者の承認を受けることが契約等により担保されている。** **(19)** 再委託に際しての、特定社会基盤事業者による承認と、最終委託先までの把握 **(20)** 再委託に際しての、再委託を受けた者の委託の相手方と同等のサイバーセキュリティ対策の確保
⑥	**特定社会基盤事業者が、委託の相手方が契約に反して重要維持管理等の役務の提供を中断又は停止するおそれがないかを確認している。** **(21)** 委託先の事業安定性の確認（事業計画、資産状況、提供実績等）
（管理体制の確認のために必要なリスク管理措置）	
⑦	**特定社会基盤事業者が、特定重要設備及び構成設備の供給者や委託（再委託を含む。）の相手方について、過去の実績を含め、我が国の法令や国際的に受け入れられた基準等の遵守状況を確認している。** **(22)** 供給者が、過去3年間の実績を含め、国内の関連法規や国際的に受け入れられた基準に反していないことの確認 **(23)** 委託先が、過去3年間の実績を含め、国内の関連法規や国際的に受け入れられた基準に反していないことの確認
⑧	**特定社会基盤事業者が、特定重要設備及び構成設備の供給や委託（再委託を含む。）した重要維持管理等の適切性について、外国の法的環境等により影響を受けるものではないことを確認している。** **(24)** 供給者が、外国の法的環境や外部主体の指示によって、契約に違反する行為が生じた可能性がある場合、報告することを契約等で担保 **(25)** 委託先が、外国の法的環境や外部主体の指示によって、契約に違反する行為が生じた可能性がある場合、報告することを契約等で担保 **(26)** 監視カメラやドローン等の映像情報を得る機器を設置または使用する場合、当該機器の映像情報の取扱の適切性が影響を受けないことの確認
⑨	**特定社会基盤事業者が、特定重要設備及び構成設備の供給者や委託（再委託を含む。）の相手方に関して、我が国の外部からの影響を判断するに資する情報の提供が受けられることを契約等により担保している。また、契約締結後も当該情報について変更があった場合に、適時に情報提供を受けられることを契約等により担保している。** **(27)** 供給者や委託先の相手方の名称・所在地、役員や資本関係等、事業計画や実績、設備または部品の製造等や維持管理等の実施場所、作業に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）等に関する情報提供を受けられることを契約等で担保 **(28)** (27) の事項について変更があった場合に、適時に情報提供を受けることを契約等で担保

(注) 項目 (1) ～ (28) は、各項目の内容を要約し記載
(出所)「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」(2023年4月28日閣議決定) 及び「特定社会基盤役務の安定的な提供の確保に関する制度の運用開始に向けた検討状況について」(内閣官房 経済安全保障法制に関する有識者会議 2023年6月) を基に野村総合研究所作成

のであろう。一方、共同利用のITサービスの場合は、ログに他の金融事業者の情報が含まれうる等の理由により、金融事業者が直接確認することが困難なケースも考えられる。確認や届出の方法について、検討が必要となるだろう。

また、措置①の項目（3）（4）（5）や、措置④の項目（16）の維持保守等に用いる情報の管理への対策として、システム開発環境の整備とその統制が求められている。具体的には、入退室管理などの物理統制、開発環境へのアクセス制御等の論理統制、開発用端末の外部デバイス接続遮断などであろう。こうした統制はシステム本番環境では一般的なものとなっているが、開発環境で

図表1-5　リスク管理措置の届出様式案

（参考）リスク管理措置の届出様式案（チェックボックス形式）

項目	チェックボックス	備考欄
（1-1）特定社会基盤事業者は、特定社会基盤事業者（※1）又は特定重要設備の供給者において、特定重要設備に悪意のあるコード等が混入していないかを確認するための受入検査その他の検証体制が構築されており脆弱性テストが導入までに実施されることを確認している。	☑	左記と同一でない取組を行っている場合は、その内容を記載

（※1）例えば、導入前の設備のテスト段階において特定社会基盤事業者及び特定重要設備の供給者とは異なる者によって確認した場合を含む
（注）リスク管理措置のうち、一部の事項については、特定社会基盤事業者等を経由することなく、直接、事業所管大臣に対して確認書類を提出することができるものとする
（出所）「特定社会基盤役務の安定的な提供の確保に関する制度の運用開始に向けた検討状況について」（内閣官房 経済安全保障法制に関する有識者会議　2023年6月）より抜粋

も類似の内容が求められている点が目新しいと思われる。このような管理を統合的に実施していくために、システム開発業務は、供給者等によって整備し管理された唯一の環境（機能や権限を必要最小限に制限した環境等）に限定して実施する、といったことも考えられる。

【サイバー・レジリエンス】（措置③）

措置③では、不正な妨害の兆候の把握と、冗長性の確保が求められている。

不正な妨害の兆候の把握は、サイバーセキュリティ対策の適切性と十分性に関する事項である。従前からのサイバー対策に倣い、国内外の動向を踏まえた継続的な対応の高度化が求められる。

一方、冗長性の確保、すなわち事業継続の観点が求められている点が、従前のサイバー対策からもう一段踏み込んだ内容となっている。サイバーセキュリティ対策の基本は、被害の拡大防止にある。「サイバー攻撃を受けた場合を想定して、被害の拡大を防ぐために、サービスを停止する意思決定を適切かつ迅速にできるか」といった訓練を経験されたことのある方もおられるのではないだろうか。

こうした被害の拡大防止とは別の観点として、近年、サイバー分野における事業継続対応への関心が高まっている。2022年12月の金融庁発出文書[13]においてもサイバー・レジリエンスへの言及がなされている。しかしながら、BCP整備におけるサイバー観点の取込はこれから、という金融事業者も多いのではないだろうか。まずは、項目（11）にあるようなランサムウェア等の個別事例から着手し、具体的な検討を積み上げていくのがよいだろう[14]。

【再委託先の管理】（措置⑤）

措置⑤は、再委託先におけるサイバーセキュリティ対策状況の管理に関するものであり、項目（19）では金融事業者による再委託の承認が求められている。

しかしながら、数多くの金融事業者が共同利用しているITサービスでは、再委託の実施に際して、すべての金融事業者から事前に承認を受けるのは難しいといったこともあるのではないだろうか。このような場合は、措置⑤の主旨に則った管理の実効性を担保しながらも、ITサービスの維持向上や機能強化等への対応を損なわないようにしていくことが望まれる。ITサービス事業者には、サイバーセキュリティ対策を含む再委託先の選定基準や管理態勢について、金融事業者の立場からも十分な管理がなされていると判断できるような説明が必要になるだろう。

【外部影響の排除】（措置⑦、⑧、⑨）

措置⑦、⑧、⑨は、我が国の外部からの影響の確認と、そのおそれの排除に関する内容である。これらの内容は、国家を背景とした特定妨害行為のおそれの検証に際して重要な要素となるものである。また、届出事項の節で言及の通り、確認に際して機微性を有する情報が含まれる可能性があることから、その確認方法ならびに情報の慎重な取扱いに留意する必要があるだろう。

【事業継続に資する供給者と委託先】（措置②、⑥）

最後に、措置②と⑥は、供給者及び委託の相手方を事業継続の観点から適切に選定しているかとの内容であ

る。金融事業者においては、従前から管理されている範疇の内容と考えて差し支えないだろう。

運用開始後の対応

事前審査は、新たな特定重要設備の導入や、重要維持管理等の委託開始時のみに求められるものではない。導入等計画書の内容の変更が「重要な変更」にあたる場合は、あらかじめ変更案を事業所管大臣に届け出なければならない。基本指針では、「特定妨害行為の手段として使用されるおそれが大きいかを審査した結果に大きな影響を及ぼし得る事項に関する変更」を重要な変更として定めることが適当とされており、その例として特定重要設備または構成設備の供給者の変更などが該当し得るとされている[15)]。

また、本制度の運用開始時点で導入済の特定重要設備や開始済の重要維持管理等の委託について、事後的な届出義務が課されることはないとされている。ただし、自動更新を含む委託契約の更新は委託の開始にあたることから、事前の届出が必要となる。既に導入済の特定重要設備や重要維持管理等の委託についても、運用開始後のそう遠くない時点で届出が必要になると認識し、準備を進めておく必要があるだろう。

金融分野にもたらす変化は

近年の厳しい安全保障環境や地政学的な緊張の高まりを背景に、国民の生活を守り、また経済・社会秩序の平穏を守っていくために、本制度を通じてインフラ事業の安全性・信頼性を確保していくことは、より一層重要なものとなっていく。このもとに、リスク管理措置に基づく対応態勢の整備は、審査対象の事業者だけではなく、金融業界全体としても期待されるものとなるのではないだろうか。

一方、こうした管理強化の流れが、金融事業者とITサービス事業者の双方に多大な負担を強いることになることも懸念される。基本指針では「自由かつ公正な経済活動を前提に、各主体の経済活動等を過度に制約せず、かつ健全な競争環境や経済合理性に基づくイノベーションや効率性を毀損しないよう」対応を図っていくことが期待されている。管理態勢の強化を図りながらも、経済活動は変わらず活発に推進してくことが求められているのである。

何より、第2の柱の目的は、特定妨害行為を防止し、社会インフラの安定的な提供を確保することにある。チェックリストベースのリスク管理で陥りがちな形式的な対応に拘泥し、コンプライアンス疲れを生じさせることで、実効性が失われないようにしたい。対応すべきはシステムリスクで見られるような不作為やミスではなく、意図的な不正による「攻撃」である。外部環境の変化や技術の進展に対応するために、個々の施策が実効的なものであるかを検証し、継続的な改善を促す管理サイクルの構築が望まれる。

本制度の主旨に基づき、管理の高度化と経済活動の維持向上を両立するためには、各金融事業者や各ITサービス事業者がバラバラに活動することで混乱や輻輳が発生したり、管理負担の過度な増大につながったりすることをいかに避けるかが重要になる。金融分野として共通のコンセンサスを醸成し、このもとに推進していくといった、業界一体としての対応が求められるのではないだろうか。

1) 正式名称、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」。
2) 特定社会基盤役務とは、「国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもの」のことをいう。本稿では、説明の簡略化のために、「主要なサービス」(または単に「サービス」) といった言葉で適宜代替することとする。
　また、対象となる事業分野は、電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、航空、空港、電気通信、放送、郵便、金融、クレジットカードの14分野。
3) 経過措置として審査対象の指定から6ヶ月の準備期間が定められているが、要請事項の内容を鑑みると、いずれにしても事前準備は必要となるだろう。
4) 基本指針の第5章第1節で、次の通り言及されている。「特定社会基盤役務の安定的な提供は、特定社会基盤事業者以外の特定社会基盤事業を行う者においても確保されることが望ましい。特定社会基盤役務の安定的な提供に当たっては、中小規模の事業者も含めたあらゆる事業者が重要な役割を果たしている。このことも踏まえ、内閣総理大臣及び事業所管大臣は、指定基準に該当しない者や設備供給に関わる幅広い者等に対しても適切な情報提供等を行う。」
5) 「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」(2023年4月28日 閣議決定)。
6) 「特定社会基盤役務の安定的な提供の確保に関する制度の運用開始に向けた検討状況について」(内閣官房 経済安全保障法制に関する有識者会議　2023年6月)。
7) 「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律に基づく特定社会基盤事業者の指定等に関する内閣府令」(2023年8月9日)。
8) 事前審査の意義については、「経済安全保障推進法の事前審査の準備に関する留意点」(金融 IT フォーカス 2023年8月号) もご参照いただきたい。
9) 本誌対談において関連する言及がなされているので、あわせてご参照いただきたい。
10) データの一次記憶領域に想定を超えるデータが入力されてしまうことで、誤動作が発生すること。
11) プログラムが確保したメモリ領域の開放を忘れてしまうことで使用可能なメモリ領域が減少し、動作の不具合を招くこと。
12) 第2章はこのテーマに関連した内容となっているので、あわせてご参照いただきたい。
13) 「オペレーショナル・レジリエンス確保に向けた基本的な考え方」(金融庁 2023年5月)。この中の「BOX2：システムリスク管理とサイバーセキュリティ」において、サイバー・レジリエンスに関する言及がある。
14) 第3章はこのテーマに関連した内容となっているので、あわせてご参照いただきたい。
15) 検討状況資料では、届出等を不要とする「軽微な変更」に関する言及があり、この中で導入等計画書に記載された機能の動作に影響を及ぼさない変更・追加に関する内容が、軽微な変更の例として記載されている。

第2章 金融業界におけるシステム開発の実態とこれからの開発スタイル

金融業界に求められるシステム開発の要件

金融業界では、システム構築において、高い安定性、信頼性、堅牢性が求められる。金融取引には、リアルタイム性が必要不可欠であり、些細なシステム異常でも多くの売買機会損失につながりかねない。

これらの安定性、信頼性、堅牢性を保つため、システム開発の現場では様々な品質向上策が実施されている。多角的な観点でテストを実施し、品質を積み上げている。また、1990年ごろから金融機関のシステムへの侵入が多発したこと等から、セキュリティへの対策も実施している。金融業界では、機微な情報を扱うケースも多く、これらが漏洩すると、企業の社会的な信頼失墜にもつながる。

セキュリティ対策に特効薬はなく、多層防御を意識した対策を地道に積み重ねるしかない。設計・開発で脆弱性を埋め込まないようにする予防的な対策や、攻撃を受けた際に素早く検知、回復するといった運用的な対策等、複数の対策を組み合わせる必要がある。なお、多層防御の詳細については第3章を参照されたい。

近年のシステムでは、予防的なセキュリティ対策として、リリース前に脆弱性診断を行う方法が主流となっている。本来は、リリース前の診断に加えて、設計、開発、テストなど、それぞれの工程でセキュリティを意識して対応することが理想である。しかし、セキュリティ人材も少なく、スケジュールに余裕がないことも多いため、最後に専門ベンダーに診断を依頼することにより対策を行っているシステムが多いのが現状だ。

経済安全保障推進法によりさらなるセキュリティ対策の必要性

これまでのセキュリティ対策は、情報の漏えいを中心に考えられてきた。しかし、昨今は地政学リスクの高まりから、経済安全保障推進法においても、明示的に、国外からの妨害行為をリスクと考えており、開発の過程に重きをおいたセキュリティ対策が求められている。経済安全保障推進法では、開発工程（サプライチェーン）にて、悪意のあるコード等が混入してしまうリスクへの対策として、本番稼働しているシステムだけでなく、開発プロセスや体制においてもセキュリティ対策状況の報告を求めている。また、対策を裏付ける資料の提出も求められる。近年のDXの流れによって、低コストかつ短期間でのシステム開発がトレンドとなっている一方で、生産性を維持しつつ、セキュリティ水準も向上させなくてはいけない。

リスク管理措置の具体例に対する解決方法

本稿では、4月28日に閣議決定された「基本指針」[1]、ならびに制度の運用開始に向けた「検討状況資料」[2]に示される28のリスク管理措置の具体例の中から、開発スタイルを見直すことで対策可能な、リスク管理措置①の項目（1）～（3）に対する対策方法を見ていきたい。

リスク管理措置①の項目（1）では、「特定社会基盤事業者は、特定社会基盤事業者又は特定重要設備の供給者において、特定重要設備に悪意のあるコード等が混入していないかを確認するための受入検査その他の検証体

制が構築されており脆弱性テストが導入までに実施されることを確認している。」と記載されている。これには、専門ベンダーより、最新のセキュリティに対応したツールが提供されているため、そうしたツールを活用することが有効だ。独自で対策するには、チェック項目や方法の整備から検討が必要になるが、ツールにより自動で脆弱性テストを実施でき、また証跡も出力できる。

リスク管理措置①の項目（2）では、「特定社会基盤事業者は、特定重要設備の供給者が特定社会基盤事業者によって調達時に指定された情報セキュリティ要件（特定重要設備及び構成設備に最新のセキュリティパッチが適用されているか否か、不正プログラム対策ソフトウェアを最新化しているか否か等）を導入までに実装することを確認している。」と記載されている。これには、脆弱性を含むソフトウェアの利用有無を自動でチェックするツールが提供されており、活用することが有効だろう。これにより、パッチを当てる運用を楽に構築できる。

リスク管理措置①の項目（3）では、「特定社会基盤事業者は、特定重要設備の供給者が、特定重要設備の開発工程において信頼できる品質保証体制を確立していることを確認している。」と記載されている。これまで対策として述べたツールを、開発プロセスに組み込み活用することで体制の強化を図ることができる。

Shift Leftによる品質保証体制の確保

リスク管理措置①の項目（3）では、品質保証体制の確保が求められているが、「Shift Left」という開発手法による対策を推奨したい。Shift Leftにより、リスク管理措置①の項目（1）、（2）も、併せて対応可能である。

Shift Leftとは、システム開発の早い段階でセキュリティ対策を組み込むことで、早期にセキュリティの脆弱性を発見し、リリーススケジュールの遅延や改修コストの増加を防ぐ考え方である。リリース前の診断だけに頼るのではなく、ツールを活用して、開発・テスト工程でもセキュリティチェックを行う（図表2-1参照）。

Shift Leftを実現するには、以下の3つの要素を満たす必要がある。

①プロセス：誰が、いつ、どのようにセキュリティ対策を行うか等、具体的な運用フローを整備する

②技術：セキュリティ対策を内製化、効率化するために、セキュリティチェックの自動化を行う

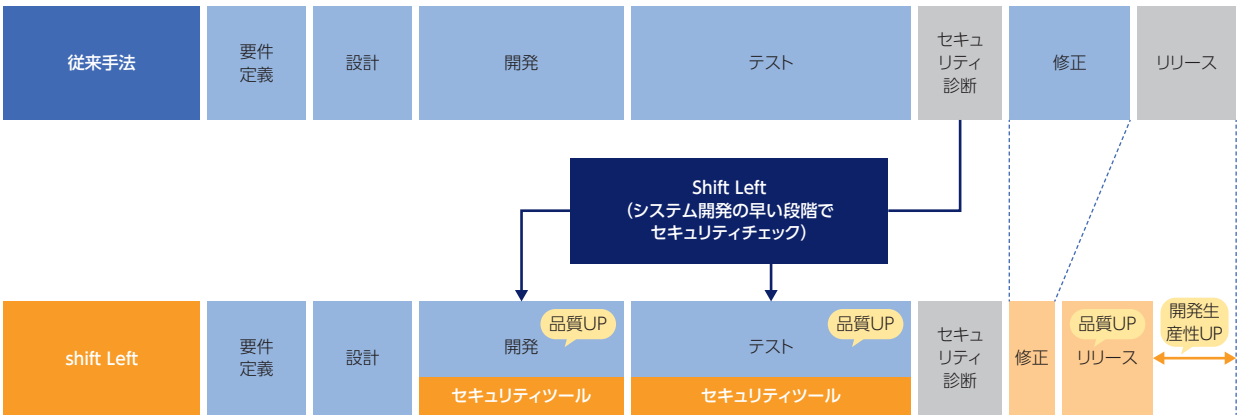
③文化：プロジェクト・組織全体でセキュリティ対策を行う文化を醸成する

それぞれの要素について、簡単に紹介していく。

①プロセスについて

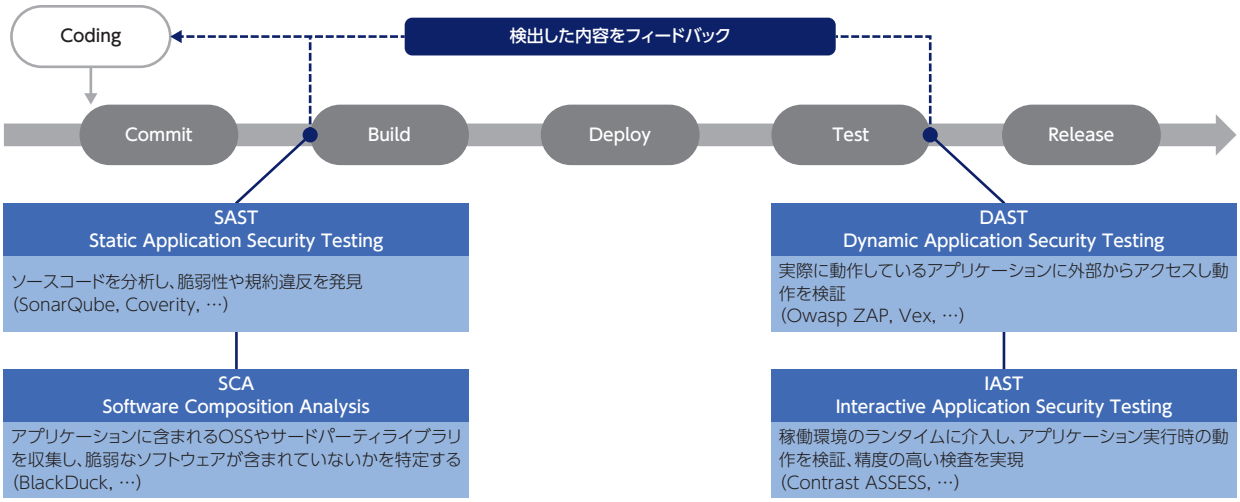
セキュリティ対策が開発工程で確実に実行されるように、対策を開発プロセスに組み込むことが重要だ。どの

図表2-1　Shift Leftの考え方



（出所）野村総合研究所

図表2-2　4種類のセキュリティチェックツール



(出所) 野村総合研究所

タイミングで何を確認するのか、誰が確認するのか、発見した脆弱性の対応要否の判断基準等を開発が始まる前に整備する。後述するセキュリティチェックツールを最大限活用するために、開発工程の中で、自動でツールが動く仕組みを整備することも必要である。

ツールのみではチェックが難しい脆弱性も存在する。設計段階で脆弱性の有無を確認し、リリース前の手動診断も組み合わせる等、開発プロセスの中でどのようにセキュリティ品質を積み上げるかを考える必要がある。

②技術について

開発工程に合わせて、手戻りを防止する効果が高いツールを選定する。ここでは、4種類のツールを紹介する。

1つ目のツールはSAST（Static Application Security Testing）である。SASTは、プログラムの記載内容に、脆弱性を含む書き方がないかをチェックするツールである。開発の初期工程で対策できるため、手戻りを防ぐ効果が高い。セキュリティ観点のチェックだけでなく、品質観点のチェックも実施できるツールも多く存在する。SASTは、リスク管理措置①の項目（1）に記載の受入検査への対策に該当する。開発したソースを受け入れる前にチェックすることで、悪意のあるコード等が混入していないかを検査することができる。

2つ目のツールはSCA（Software Composition Analysis）である。利用しているソフトウェアに、公開された脆弱性を含むものがないかをチェックするツールである。SASTは、自社で開発しているソースに脆弱性がないかのチェックを行うが、SCAはOSSやサードパーティライブラリの脆弱性をチェックする。開発しながら脆弱性への対策ができるので、手戻りを防ぐ効果が高い。SCAには、今後経済安全保障推進法の中で必要になるといわれているSBOM（Software Bill of Materials）[3]の生成ができるものも存在する。またSCAは、リスク管理措置①の項目（1）の受け入れ検査、項目（2）のセキュリティパッチの適用に効果的である。脆弱性を含むソフトウェアが検出された際、即座にパッチ適用判断が可能である。

3つ目のツールはDAST（Dynamic Application Security Testing）である。稼働しているアプリケーションに対して疑似的な攻撃を行い、その応答を見て脆弱性の有無を判断する。

4つ目のツールはIAST（Interactive Application Security Testing）である。こちらは稼働しているアプリケーションに組み込むことで、アプリケーションの挙動を監視して脆弱性を検知するツールである。機能テストを実行する際に動かすことで、脆弱性に関するテス

トも実施できる。SCAの機能も併せ持つものもある。DASTとIASTは、アプリケーションを開発環境に配置するタイミングで脆弱性の確認ができる。SAST、SCAと比べ、チェックできる工程が後になるため、手戻り効果は低くなるが、稼働するアプリケーションに対する解析を行うため、解析の精度が高い。リスク管理措置①の項目（1）における脆弱性テストに該当する。

これらのツールから、費用やリスク等をプロジェクト特性に合わせて選定し、組み合わせて活用するとよい。

③文化について

Shift Leftを継続していくには、開発者全体でセキュリティ対策を行うという意識を共有することが重要である。セキュリティツールを最大限に生かすには、開発者が診断結果を理解し、ボトムアップで対応を進める必要がある。しかし、セキュリティ人材の確保、育成は困難であり、また開発現場ではセキュリティに対する当事者意識が薄くなりがちである。

そこでお薦めなのが、セキュリティチャンピオンと呼ばれる、セキュリティの責任者を置いて、セキュリティチャンピオンを中心にセキュリティの啓蒙を行う方法だ。セキュリティチャンピオンが開発者と一緒にツールの結果を精査することで、開発者達のレベルアップを図る。また、勉強会等を実施することで、セキュリティ初心者の底上げも図る。このように、徐々にプロジェクト全体に浸透させるのがよいだろう。

文化を醸成することができれば、リスク管理措置①の項目（3）にて求められる品質保証体制が確立されたと言って差し支えないだろう。

Shift Leftの導入による更なる効果

Shift Leftという考え方により、リスク管理措置の具体例に対して対策する方法を紹介した。リスク管理措置への対応は今後確実に必要になっていく。企業によっては、一時にすべての対策を実施することは難しいかもしれない。その場合は、SASTやSCA等、セキュリティチェックツールをまずは一つ導入する。そしてプロセス・文化を整備し、その後、別のツールも適用していく、という具合に少しずつShift Leftを進めていくのがよいだろう。

Shift Leftを導入することで、リスク管理措置の対策だけでなく、品質と生産性の向上につながるメリットが得られる。その中でも、次の2つは多いに期待できる。

●各工程でセキュリティチェックを行うため、手戻りを最小限にしながら開発を進めることができる

脆弱性の対応は、工程が進むほど対策工数が増加する。リリース直前に脆弱性が発見された場合は、テストだけでなく、内容によっては設計工程への手戻りにもなりうる。Shift Leftを実践することによりそういった手戻りを回避できる。また、少ない手戻りで修正ができるため、今までより対応できる範囲が増え、品質も向上する。

●セキュリティを常に意識しながら開発するため、セキュリティ人材が育つ

リリース前の診断では、専門ベンダーに診断・対応方針の相談を委託することが多いため、自社内でのセキュリティ知識の定着が難しい。Shift Leftを継続することで、開発者がツールのチェック内容を意識し続けるため、セキュリティ知識が定着する。知識が定着することで、脆弱性を混入させることも少なくなり、品質・生産性ともに向上する。

Shift Leftにより得られる効果は、システム開発において本質的に目指すべき姿に通じる。地政学リスクが増すDX時代において、Shift Leftを取り込んだ開発スタイルは今後、システム開発で主流となっていくだろう。

1）「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」(2023年4月28日 閣議決定)。

2）「特定社会基盤役務の安定的な提供の確保に関する制度の運用開始に向けた検討状況について」(内閣官房 経済安全保障法制に関する有識者会議　2023年6月)。

3）SBOMは、2023年2月28日 第9回 サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース）でも、経済産業省が検討しており、今後国内での活用が予想されている。

第3章 経済安全保障とオペレーショナル・レジリエンスで求められるサイバーセキュリティ

経済安全保障で求められる多層防御のセキュリティ対策

経済安全保障推進法で求められるサイバーセキュリティ上の対応の一つに、「特定社会基盤役務の安定的な提供の確保に関する制度」への対応がある（本制度の詳細については第1章を参照）。

本制度では、特定社会基盤事業者に指定された事業者は、特定重要設備の導入時にどのようなリスク管理措置を講じるか具体的な内容を示すことが望ましいとされているが、政府公表資料[1)]では、具体例として9つのリスク管理措置とそれらに紐づく28の具体例が示されている。これら9つのリスク管理措置の概要と、具体的に求められるサイバーセキュリティ上の対策を整理したものが図表3-1である。

これらの対策を踏まえたリスク管理措置を実施するためには、不正なプログラム混入対策や脆弱性管理、ソフトウェア改ざん検知等の個別の対策ごとに検討することが必要である。しかし、より重要なことは、委託先やサードパーティも含めて、自社サービスの設計開発フェーズから運用フェーズまでの「多層的な統制」を基本とする多層防御の考え方に基づく対応である。

なお、この多層防御の考え方に基づく対応として、既に金融当局が金融機関に対して取組み強化を求めている類似の取組みとして「オペレーショナル・レジリエンス（以下、オペレジ）」がある。サイバーセキュリティ対策強化という観点では、両者が求める対策には重なる点が多く、オペレジで求められている内容について理解を深めておくことが、経済安全保障推進法上の対応にも有益であると考える。次項以降では、国内外のオペレジに

図表3-1　特定重要設備の導入に係るリスク管理措置と求められるサイバーセキュリティ対策

	特定重要設備の導入に係るリスク管理措置	サイバーセキュリティの観点で求められる主な対応例
①	製造等の過程で不正な変更が加えられることを防止するために必要な管理措置	•ソフトウェア開発ライフサイクル全般統制 •不正なプログラム混入対策（バックドア等） •脆弱性管理 •ソフトウェアの改ざん検知 •開発者のeKYC/2要素認証　etc.
②	特定重要設備の保守・点検等を行うことができる者が、特定重要設備又は構成設備の供給者に限られるかどうか等の実態把握、供給者選定	•マルチベンダー等・代替手段の検討と手配 •脅威情報収集・分析
③	不正な妨害が行われる兆候を把握可能な体制、及び不正な妨害が加えられた場合であっても、冗長性の確保など役務の継続性の対応	•サイバーレジリエンス態勢強化 •ランサム等を踏まえたバックアップ・リストア対策 •サイバー訓練　etc.
④	委託を受けた者（従業員を含む）によって、意図しない変更が加えられることを防止するために必要な管理等、及び契約等により担保	•不正コミット監視 •特権アクセスログのモニタリング強化 •不正ふるまい検知 •セキュリティ教育研修　etc.
⑤	再委託を受けた者のサイバーセキュリティ対策の実施状況を確認するために必要な情報について、再委託前での把握・承認・契約等による担保	•委託先・再委託先へのセキュリティ可視化 •委託者等の事業継続性確認 •契約審査強化
⑥	特定社会基盤事業者が、委託の相手方が契約に反して重要維持管理等の役務の提供を中断又は停止するおそれがないかの確認	
⑦	供給者や委託（再委託を含む）の相手方について、過去の実績を含め、我が国の法令や国際的に受け入れられた基準等の遵守状況の確認	•委託・再委託の法人審査強化 •委託・再委託の法令順守状況審査 •契約審査強化
⑧	供給や委託・再委託した重要維持管理等の適切性について、外国の法的環境等により影響を受けるものではないことの確認	
⑨	供給者や委託・再委託した相手方に関して、我が国の外部からの影響を判断するに資する情報の提供が受けられることを契約等により担保	

（出所）NRIセキュアテクノロジーズ

対する取組みについて紹介する。

グローバルにおける金融機関に対するオペレーショナル・レジリエンス

金融庁は2023年4月に、ディスカッション・ペーパーとして、「オペレーショナル・レジリエンス確保に向けた基本的な考え方（以下、基本的な考え方）」を公表している。これは、グローバルのオペレジ確保に関する規制強化を踏まえて日本としての取組方針を示したものである。

オペレジとは、システム障害、サイバー攻撃、自然災害等が発生しても、重要な業務を、最低限維持すべき水準において、提供し続ける能力のことである。想定外の事象が生じた場合に、業務中断が生じることを前提に、利用者目線で早期復旧・影響範囲の軽減を確保する枠組みとして国際的に議論されている。

2021年3月にバーゼル銀行監督委員会が国際原則を策定したが、これと前後して、各国においても本原則を踏まえたオペレジ関連の規制や指針などが金融当局から示されている（図表3-2参照）。

各国の取組みの中でも、特に注目されているのがEUである。EUでは、EU域内に拠点を置く金融機関及び金融機関にサービスを提供するICTサービスプロバイダを対象とする「デジタルオペレーショナルレジリエンス法（DORA）」が2023年1月16日に発効し、2025年1月より適用開始予定となっている。本法は、金融機関に対して主にICTリスク管理やICTサードパーティのリスク管理等を義務付けるものであるが、内容として金融機関は以下の対応が求められる。

ICTリスク管理については、金融機関は「デジタル・オペレーショナル・レジリエンス戦略」を策定することが求められ、具体的には以下の5点について盛込む必要がある。

1. ICTリスクに対する許容度の設定と影響の許容度の分析
2. 情報セキュリティの目標の設定
3. ICT関連のインシデントを検知するためのメカニズムの整備
4. デジタル・オペレーショナル・レジリエンス・テストの実施
5. 開示が求められるICT関連のインシデントが発生した際のコミュニケーション戦略の策定

金融機関の経営者は、上記5点を含む戦略を策定及び承認し、その実施状況を定期的にレビューすることなどが求められる。

また、ICTサードパーティ・リスクに関しても、ICTサードパーティ戦略を採択し、定期的なレビューを実施するとともに、ICTの集中リスク等についても特定、評価することが求められている。本法ではICTサードパーティ自体も規制対象となっており、金融当局が金融機関にとって重要なICTサードパーティを指定した場合、EUの金融機関に対してICTサービスを提供する場合には、

図表3-2　オペレーショナル・レジリエンスに関する諸外国の取組み

(出所) 各種公表情報等を基にNRIセキュアテクノロジーズ作成

EU域内に拠点を設置（第三国に拠点を置く場合は、EU域内に小会社を設立）していることが求められる。

このように、EUにおいては金融機関のオペレジ対応については、指針やガイドラインではなく、法律として対応を義務付けている点が特徴であり、EUの金融機関はオペレジの確保が重要な経営課題となっている。

サードパーティのリスク管理手法としてのサイバーマッピング

オペレジ確保において特に重要な取組みの一つとして位置づけられているのが、「サードパーティ・リスク管理」である。サードパーティの定義は様々あるが、金融庁が公表している「金融セクターにおけるサードパーティのサイバーリスクマネジメントに関するG7の基礎的要素」では、「金融機関と組織との間に結ばれる製品又はサービスを提供するためのあらゆる業務上の関係又は契約（組織内外は問わない）」として定義されている。

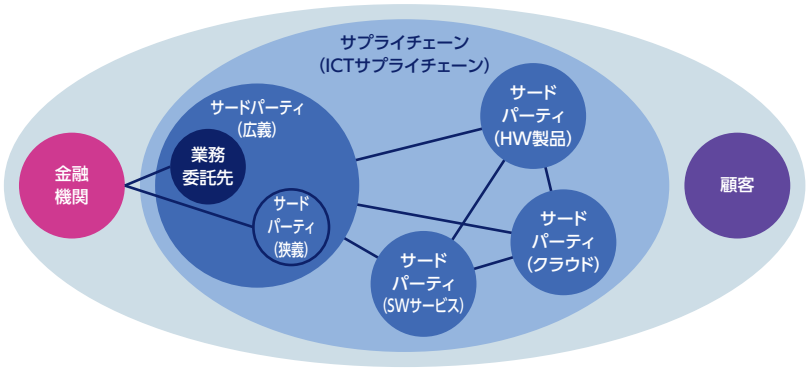
また、サードパーティの類似の概念として、業務委託先、サプライチェーン（ICTサプライチェーン）といった用語もあるが、これらを含めた関係性を整理したのが図表3-3である。金融機関は、業務委託先を含めたサードパーティのリスク管理と合わせて、ICTサプライチェーンを構成するサードパーティも含めて、「サードパーティ・リスク管理」を実施することが求められる。

「サードパーティ・リスク管理」については、前述のEUのDORAのみならず、英国においても2023年2月にイングランド銀行が金融マーケットインフラにおけるサードパーティリスクマネジメントに関するポリシーステートメント[2]を公表し、米国でも2023年6月にFRB、FDIC、OCCがサードパーティのリスク管理のガイダンス[3]を発行する等、近年特に重視されている取組み領域となっている。

これらのガイダンスにおいて、特に重要な取組みとして位置づけられているのが、自社の重要なサービス・機能に関わるアクタの可視化（マッピング）である。金融機関が利用するサードパーティの数が膨大で、クラウドサービスやFintechサービス等との連携も含めて相互依存関係が複雑になっていることを踏まえ、マッピングにより整理しリスクの抜け漏れを防ぐことが非常に重要となる。

マッピングのアプローチとしては、例えば欧州システミックリスク理事会（ESRB）は、オペレジにおけるサイバーリスク低減においてサイバーマッピングが重要であると指摘し、2種類の具体的なマッピング手法を紹介している。一つは、金融システムにおける中核となる重要な機能を提供する機関及びこれらの機関が機能を提供するために依存しているシステムを特定するアプローチである「機能的アプローチ」（例：ノルウェー銀行）。もう一つは、金融ネットワークと重要組織が利用するサードパーティICTプロバイダー間の連携を特定するアプローチである「組織的アプローチ」（例：ドイツ連邦銀行）である[4]。金融機関はこれらのアプローチ等も参考にしながら、自社が保有する経営資源を踏まえて最適な手法を用いてマッピングした上で、自社が提供する重要なサービスに関与するサードパーティのリスク対応状況について精査していくことになる。

図表3-3　サプライチェーンにおけるサードパーティの位置づけ



(出所) 金融庁「金融セクターにおけるサードパーティのサイバーリスクマネジメントに関するG7の基礎的要素」を基にNRIセキュアテクノロジーズ作成

諸外国におけるサイバーストレステストの対応状況

英国やEUでは、オペレジ対応と合わせて、金融当局が実施するストレステストのサイバーセキュリティ版

であるサイバーストレステストを開始する動きもある。

例えば、英国の中央銀行であるイングランド銀行の金融政策委員会は2017年にサイバーストレステストの導入を公表し、2019年よりパイロットを実施し、2021年より、対象の金融機関の自主参加型のサイバーストレステストを実施している。2023年3月に公表された2022年度のサイバーストレステスト実施結果のレポート[5]では、「サイバーストレステストはオペレジとは異なるものであるが補完的な関係にあり、サイバーレジリエンステストのために、オペレジの活動成果を活用する」ことが推奨されており、英国の金融機関は当該ストレステストへの対応も見据えて、オペレジ対応の実施が求められている。

また、欧州中央銀行（ECB）も、2024年からサイバーストレステストを実施する旨公表しており[6]、欧州圏を中心に、金融機関のサイバーセキュリティ強化の動きがより一層強まる見込みである。

日本の金融機関に求められる対応

このように欧米では金融当局が金融機関に対してオペレジ対応やサイバーストレステストへの対応を義務付ける規制強化の動きが進んでおり、今後日本においても規制強化の検討が進む可能性が想定される。

現在日本の金融機関のオペレジ対応については、金融庁が4月に「基本的な考え方」を公表しているものの、具体的な対策については各金融機関にて検討する必要があり、各社は試行錯誤を重ねている状況である。一方で、経済安全保障推進法に基づく対応については、具体的に対応が求められるリスク管理措置の内容は現時点ではまだ不透明な部分が多いものの、今後策定される予定のガイドライン等において、リスク管理措置として求められるサイバーセキュリティ対策項目が示されるものと思われる。したがって、日本においては本ガイドラインに基づく経済安全保障推進法への対応を進めることで、オペレジの強化にもつなげていく、というアプローチが多くの金融機関にとって現実的な進め方になるものと想定される。また、ガイドライン等が示されるまでの準備対応としては、本稿で紹介したEUのDORAをベンチマークとして、DORAで求められるリスク管理措置の内容を確認・検証しておくことも有益だろう。

なお、経済安全保障推進法の対象となるのは「特定社会基盤事業者」であり、特定社会基盤事業者として指定されない金融機関は本法の対象外となる。一方でオペレジは金融機関が広く対象となることから、経済安全保障推進法への準拠は求められないものの、オペレジの対応が求められる金融機関は一定数存在するものと思われる。この場合も、基本的には経済安全保障推進法で求められる対応が参考になると考えられるため、特定社会基盤事業者として指定されなかった場合でも、オペレジへの対応を目的として、本法で求められるリスク管理措置等の内容等を参考に対応強化を進めておくことが有効なアプローチになるだろう。

---

1) 経済安全保障法制に関する有識者会議、「資料1　特定社会基盤役務の安定的な提供の確保に関する制度の運用開始に向けた検討状況について」(2023年6月12日)
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai7/siryou1.pdf
2) Bank of England, “Outsourcing and third party risk management part of the Code of Practice” (2023年2月8日)
https://www.bankofengland.co.uk/paper/2023/outsourcing-and-third-party-risk-management-code-of-practice
3) FRB, “Interagency Guidance on Third-Party Relationships: Risk Management” (2023年6月7日)
https://www.federalreserve.gov/supervisionreg/srletters/SR2304.htm
4) ESRB, “Mitigating systemic cyber risk” (2022年1月)
https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf
5) Bank of England, “Thematic findings from the 2022 cyber stress test” (2023年3月29日)
https://www.bankofengland.co.uk/prudential-regulation/letter/2023/thematic-findings-2022-cyber-stress-test
6) ECB, “Interview with Helsingin Sanomat,” (2023年4月4日)
https://www.bankingsupervision.europa.eu/press/interviews/date/2023/html/ssm.in230404~ff3fe1816e.en.html

第4章 欧米の経済安全保障：その動向と金融サービスへのインパクト

本稿は、欧米の経済安全保障の動向に関する、欧米の専門家による論文の翻訳である。欧米では、本邦とは異なるアプローチで、経済安全保障への対応が進められている。対応方針に違いはあるものの、欧米における金融分野のリスク管理の動向と今後の展望から、参考になる点もあるのではないだろうか。

欧米の経済安全保障の現状

米国やヨーロッパは相当前から、複雑に絡み合った世界経済情勢から生じる経済安全保障について、潜在的な脅威と認識してきた。Bill Clinton米国大統領（当時）は1998年、重要インフラ保護をテーマとする大統領令を発令した。これは、金融セクターを含む現在の分野別計画（SSPs：Sector Specific Plans）の基礎となっている。EUでは、欧州重要インフラ保護プログラム（EPCIP：European Programme for Critical Infrastructure Protection）と、2008年の欧州重要インフラ指令（European Critical Infrastructures）が、EU圏の包括的な枠組みとなっている。一方、EU各国は、政府が独自に計画を立てており、一例としてドイツのIT Security Act 2.0がある。どの枠組みにおいても、金融サービス事業者は、重要インフラの保護に留まらず、経済安全保障においても、中核的な役割を担うとされている。

◇経済安全保障：重要性の急速な高まり

近年、経済安全保障と重要インフラの保護に、新たな注目が集まっている。これは、現在の米国、ヨーロッパ、中国、ロシア間の地政学的な緊張により生じたものであるが、データやデジタル技術が現代経済の生命線となるにつれて、「重要インフラ」の定義が拡大したことも影響している。現在、重要インフラは非常に複雑なものとなっているため、制御が難しく（リスクが高く）、また相互の接続性（依存性）も高いものとなっている。

◇米国とヨーロッパの最近の事例

経済的安全保障への懸念、特にデータ主導となっている現在の重要インフラネットワークに関するリスクは、既に有名となっているいくつかの事案から確認することができる。米国では、HuaweiとZTEの使用が禁止された。重要インフラへのアクセスに利用されるおそれがあるとして、中国資本のByteDance（TikTokの親会社）の使用禁止についても議論がなされている。また、CHIPS法という保護主義的な法律では、中国への高度なチップやその製造技術の販売を禁止している。これは、中国において高度な技術の利用が続けられることで経済や国家安全保障上の脅威をもたらすおそれがあるとの懸念があるからである。

ヨーロッパ諸国も、5Gの技術部品やネットワークの中国による所有を巡って同様の議論や事件に直面してきた。加えて、中国は、一帯一路構想の一環として、ギリシャ、ハンガリー、ジョージアなどの国の港湾や輸送拠点に多額の投資を行っていることから、南欧や東欧では中国の経済的プレゼンスが拡大しているのではないかといった懸念も増大している。一方、ロシアもヨーロッパの経済安全保障にとって脅威となる。特に、重要インフラにおいては、サイバー攻撃やガス・石油パイプラインへの脅威などがリスクとなっている。

EUにとって経済安全保障の重要性は、2023年6月中旬に欧州委員会が共同声明として提案した、新たな欧州経済安全保障戦略（An EU approach to enhance economic security）の枠組みにも表れている。この声明は、経済安全保障に関するEUの考えを戦略的枠組みとしてまとめたものであり、サプライチェーンの強靭性、重要インフラ、技術保護、経済依存関係の武器化、の4つのリスクに焦点をあてている。この声明に拘束力はないが、6月末に行われた欧州理事会の討議からも、このことがEUとして重要な課題となっていることが分かる。

◇経済安全保障への2つのアプローチ

ここで注意すべきは、米国とEUでは経済安全保障へのアプローチは、同一ではないということである。米国は、経済安全保障に対する中国からの明白な脅威と見なされるものに一方的に対処する傾向を示しているが、EUはより多国間的なアプローチを取っている。例えば、EUの新たな経済安全保障の枠組みでは、ロシアからの脅威は明確にしているが、中国に対しては直接的な言及はしておらず、その代わりにEUの経済関係上のリスク回避と経済依存の低減について述べている。中国に対するこのような慎重なアプローチは、中国が経済安全保障にもたらすリスクの性質について、EU内のコンセンサスが得られていないことにも関連している。例えば、6月中旬に発表されたドイツの新しい国家安全保障戦略（NSS：National Security Strategy）では、国家安全保障と経済安全保障を一体的に認識し、中国のことを「パートナーであり、競争相手であり、ライバルでもある」としている。

◇政府と産業：見解の不一致

経済安全保障を巡る議論では、政府と民間部門の間にも重要な意見の乖離がある。米国では、技術や製造の主要部門が、政府の経済保護主義へのシフトに声高に反対してきた。米ハイテク企業NVIDIAの社長兼CEOの台湾系米国人Jensen Huang氏は、中国市場が閉鎖的になった場合、米国業界に甚大な損害をもたらすと警告している。EU経済圏の多くが同様に、中国市場は将来の成長にとって重要であり、ソーラーパネル部品から電気自動車のようなグリーン技術にとって重要なレアアース鉱物まで、あらゆる領域で重要なサプライヤーにもなっている。例えば、ドイツの自動車メーカーVolkswagenの利益の半分は中国市場からもたらされており、同社は2020年に急拡大する中国自動車市場で20%のシェアを獲得している。

現在の状況：金融機関と経済安全保障上のリスク

経済安全保障や重要インフラをめぐる議論において、テクノロジー産業や製造業などの伝統的な産業の果たす役割はよく知られているのに対し、金融サービス業界も、あまり知られてはいないものの、ますます重要な役割を担うようになっている。金融機関は、複雑でリスクの高い状況に置かれている。まず、金融機関は、経済安全保障への広範な対応を担っており、例えば投資スクリーニングや制裁リストへの対応といった形で携わっている。このことは、地政学的な緊張の高まりとともに、経済安全保障と国家安全保障はより一層絡み合い、金融機関は政治的な駆け引きの中に置かれることを意味している。次に、金融機関は、決済システムなどの重要インフラの中核部分を守る責任も負っている。重要インフラの保護は、技術の複雑化とともにますます難しくなっている。

◇政府の監視が強化される金融サービス

経済安全保障は、現在の地政学的状況から、大西洋の両側でかなり複雑なものとなっている。2022年にロシアがウクライナに侵攻した際、欧米諸国はロシアに対する金融制裁を相次いで実施した。欧米の金融機関は、こうした制裁の執行の最前線にいる。ロシアの銀行は、クロスボーダー取引にSWIFT決済システムを利用することを禁じられた。欧米の金融機関は、ロシアの企業や個人に対する制裁措置リストを遵守しなければならず、ロシア企業との取引の多くを禁じられている。

一方、中国と米国の経済関係が悪化する中で、米国の金融機関はバランスを取ることに苦慮している。他の産業と同様に、中国の金融市場には成長の機会があり、多くの米国金融機関が過去数年にわたり中国に多額の投資を行ってきた。しかし、米国政府の関係者にとっては、成長機会があるからといって、潜在的なリスクが軽減されるわけではない。一部の金融機関、特に米国を拠点とする金融機関は、中国での事業拡大から手を引き始めている。Citigroup、JP Morgan、Bank of AmericaのCEOは、いずれも2022年の米下院の金融サービス委員会で、米国政府の要請があれば、政府の指示に従い中国での取り組みを縮小する用意があると証言した。また、Goldman SachsやMorgan Stanleyのような大手投資銀行が、同地域における投資銀行チームの従業員の削減を検討しているとの報道もある。

◇複雑化する技術への対応

金融機関は、広範に経済安全保障を守る責任を負っているだけではなく、最前線で重要インフラを守っている。欧米の金融機関では、この5年間に急速な技術革新があった。こうした技術基盤は、今日の金融機関において重要インフラ保護における課題のひとつであり、また同時にその課題の解決策でもある。今日では、データは金融サービスの原動力となっており、金融サービスの事業モデルはますます複雑なものとなっている。ここには、データ・セキュリティの確保や、サイバー攻撃の脅威に対するオペレーショナル・レジリエンスの確保といった要素も含まれる。一方、金融業界のサプライチェーンも拡大しており、金融サービス事業者が、ITサービスやアウトソーシングサービスを通じて、金融機関をサポートするようになっている。

技術が複雑化することで、金融機関はこうした技術を駆使した攻撃に対してより脆弱になっている。次節で示すように、多くの欧米金融機関が、こうした最新技術に起因する脆弱性の解消に向けて、多大なリソースを費やしている。EUサイバーセキュリティ機関（ENISA）の報告書によると、2021年の脆弱性管理とセキュリティ分析への支出は、EUの銀行や金融サービス機関においてITセキュリティ予算の20%を超えている。

今後の展望：金融機関はどのようにして経済的安全保障上のリスクを低減させることができるか

欧米では、金融機関が重要インフラを最前線で守る役割を担っているが、金融業界の技術やデジタル・トランスフォーメーションの進展によって、この役割の遂行はこれまで以上に難しいものとなる。その解決策は、逆説的になるが、こうした技術変革をできるだけ早く完了させることである。このことは、データ・セキュリティ、オートメーション、システムなどへの支出が増えることを意味する。欧州中央銀行による2022年の調査では、多くの金融機関（61%）がまだデジタル・トランスフォーメーション専用の予算を持っていない。予算を組んでいる金融機関では、IT予算の22%が、デジタル・トランスフォーメーションに使われていた。

一方、ドイツの統計プラットフォームStatistaのレポートでは、銀行のIT予算に新たな技術が占める割合は、北米では2013年の約25%から2019年には37%にまで増加、2022年までに50%近くまで増加する、と報告している。一方、EUではその割合は相対的にやや低く、2013年は13%、2019年には27%、2022年には33%になると推計されている。

欧米の金融機関では、最新技術とデジタル・トランスフォーメーションへの支出増に加え、サイバーセキュリティ対応、リーガル・リスクの削減、リスク・コンプライアンス管理態勢の高度化に多くのリソースを割いている。これらの3つの分野は、すべて重要インフラの保護にとって重要なものとなっている。

◇サイバーセキュリティは重要インフラ保護の鍵

「私は、市場よりもサイバーを気にしている。私たちは多くの攻撃の気配と洗練された攻撃を目の当たりにし

ている。」これは、NBIM CEOであるNicolai Tangen氏が2022年8月にフィナンシャル・タイムズ紙のインタビューで語ったものだ。

サイバーセキュリティの脅威すべてが金融機関の重要インフラの保護に影響するものではないが、その多くが影響を及ぼし、またその数は増加している。世界最大の政府系ファンドを管轄するNorges Bank Investment Management（NBIM）は、フィナンシャル・タイムズ紙において、2022年に1日平均3件の深刻なハッキングに直面しており、その件数は過去2～3年で倍増していると述べた。2022年に行われた別の調査では、脅威となる攻撃が前年比増となった金融機関は調査対象の63%に及び、そのうち60%で、攻撃者がITサービスプロバイダー経由で金融機関のネットワークにアクセスする「アイランドホッピング」攻撃の増加を経験していることが分かった。

こうしたことから、サイバーセキュリティへの支出が急増していることは驚きではない。Bank of AmericaのCEOであるBrian Moynihan氏は、2021年に米銀はサイバーセキュリティだけで10億ドル以上を費やしていると発言した。世界の金融サービス業界の130人のセキュリティリーダーを対象とした2022年の調査によると、20～30%の組織が増大するサイバーセキュリティの脅威に対抗するため次年度予算の増額を計画しており、51%の組織が毎週サイバーセキュリティの「脅威調査」に積極的に取り組んでいると回答している。

◇規制遵守の徹底

次に、重要インフラの保護で重要な点は、規制が急速に変化していく中でも、金融機関が最新の規制を適確に遵守できていることである。例えば、金融機関はアウトバウンドやインバウンドの投資スクリーニングに関する規制の変化や、個人や事業体の制裁リストへの追加に、迅速に対応する必要がある。最新の規制を適確に遵守する必要性から、RegTech（Regulatory Technology）への支出が増加している。金融機関によるRegTechへの世界的な支出は、2022年の680億ドルから2026年には2000億ドル超へと3倍に拡大するとの試算があり、年間5億ドル以上を費やしている大手金融機関もあるとされる。こうしたレベルの支出は必ずしも目新しいものではない。大手金融機関は2015年の時点で、規制遵守を目的とした支出が劇的に増加していると報告していた。

◇リスク・コンプライアンス管理枠組の高度化

最後に、欧米の金融機関の多くは、非財務リスクとコンプライアンスリスクの管理枠組を見直す過程にある。この動きは重要インフラの保護への懸念に直接起因するものではないかもしれないが、間接的に重要インフラの保護の鍵となるものである。GRC（ガバナンス、リスク、コンプライアンス）は、金融機関において重要なテーマであり、ほとんどの大手金融機関が、現場部門・管理部門・内部監査部門の3つの役割のもとに内部統制を推進する「3ラインディフェンス」を導入している。更に、組織全体のリスク事象の監視に役立つ、自動化されたリスク管理プラットフォームに注目する金融機関も増えている。また、コンプライアンス機能の一元化も普及しつつあり、非財務リスク削減に向けたリスク文化の醸成も重視されている。例えば、全従業員に対して、コンダクトリスク（不公正な行動から生じるリスク）の削減方法を含むリスク管理のトレーニングを実施している。

レガシーな技術の刷新と新たな技術への支出は、より重要なものとなっている。2021年のENISAのレポートによると2020年の銀行および金融サービスのITセキュリティ支出の19%がGRCに費やされており、これは脆弱性管理とセキュリティ分析に次ぐものであった。

地政学的な状況が絶えず変化し、各国政府が新たなリスクの評価を迫られる中で、金融機関は重要インフラの保護と経済安全保障の重要な役割を担い続けることになるだろう。デジタライゼーションと最新技術が金融サービスセクターの脆弱性を高める要因となっていることを受けて、金融機関では規制遵守やサイバーセキュリティなどへの支出を強化している。

著者紹介

上杉 信孝
Nobutaka Uesugi
金融デジタルビジネスデザイン部
エキスパートリサーチャー
focus@nri.co.jp
担当：第 1 章、第 4 章翻訳
専門は金融分野のリスクマネジメント

宮原 俊介
Shunsuke Miyahara
aslead 事業部
シニアシステムコンサルタント
focus@nri.co.jp
担当：第 2 章
専門は開発管理効率化、DevSecOps

藤井 秀之
Hideyuki Fujii
NRI セキュアテクノロジーズ
エキスパートセキュリティコンサルタント
focus@nri.co.jp
担当：第 3 章
専門はサイバーセキュリティに関する国内外の規制動向

Onawa Lacewell, Ph.D.
Cutter Associates
ディレクター、エキスパートコンサルタント
focus@nri.co.jp
担当：第 4 章
専門は金融分野のグローバルリスク・コンプライアンス

窪田 瞳
Hitomi Kubota
金融デジタルビジネスデザイン部
コンサルタント
focus@nri.co.jp
担当：第 4 章翻訳
専門は IT ガバナンス、GRCS 全般

金融機関のリスク・レジリエンスの潮流
－経済安全保障推進法「第2の柱」対応－

金融ITフォーカス特別号

発行日　2023年9月4日

発行　株式会社野村総合研究所
〒100-0004　東京都千代田区大手町 1-9-2
大手町フィナンシャルシティ グランキューブ
https://www.nri.com/jp

発行人　山﨑 政明
編集人　末吉 英範
編集　金融デジタルビジネスリサーチ部
デザイン　株式会社ベネクスマーケティング
対談写真　つちだ 耕平
印刷・製本　NRIフィナンシャル・グラフィックス株式会社
問い合わせ先　金融デジタルビジネスリサーチ部
focus@nri.co.jp

NRI