重要性が高まるサイバーセキュリティに関する金融商品の役割

富永　健司

▌要　約▐

1. 近年、サイバー攻撃の被害が深刻化し、多様化している。企業及び投資家がサイバーセキュリティのリスクに対応し、関連する機会を捉えていくにあたり、金融商品の役割の重要性が増している。金融資本市場における、サイバーセキュリティ関連の主要な金融商品として、サイバーファンド、サイバー保険が挙げられる。
2. 米国では 2014 年に世界初のサイバーファンドであるピュアファンズ ISE サイバーセキュリティ上場投資信託が上場された。日本においても、サイバーセキュリティ関連の投資信託が提供されているが、米国におけるサイバーファンド同様、投資先企業は米企業が中心となっている。また、兼松等が 2024 年 2 月に設立を発表したサイバーファンドは、国内のサイバーセキュリティ関連企業を主要な投資対象として想定していると見られ、こうした取り組みが日本企業全体のサイバーセキュリティ対策の強化に寄与していくのか注目される。
3. 他方、サイバー保険に関しては、米国で利用が浸透しているのに比べ、日本では依然として普及余地があると見られている。サイバー保険の加入率向上に向けて、サイバーセキュリティに対する意識向上、サイバー保険の認知度向上等の課題に取り組んでいくことが重要である。
4. 今後、（1）サイバーセキュリティに係る金融商品の開発努力、（2）官民の連携強化による技術革新へのファイナンス支援、等に取り組んでいくことで、サイバーセキュリティに関する金融商品のさらなる発展が期待される。

野村資本市場研究所　関連論文等

・富永健司「企業のサイバーセキュリティリスクとサイバー保険」『野村サステナビリティクォータリー』2023 年秋号。
・ジェイソン・モーティマー「サイバーセキュリティ・エンゲージメント―投資家向けガイド―」『野村サステナビリティクォータリー』2024 年春号。

Ⅰ サイバーセキュリティに関する金融商品の役割

近年、サイバー攻撃の被害が深刻化し、多様化している。例えば足下では、国内のエンターテイメント企業大手が 2024 年 6 月、ランサムウェアを含む大規模なサイバー攻撃を受け、事業への影響が大きくなるとの懸念から同社の株価が大幅に下落するといった事案が発生している[1]。

企業及び投資家がこうしたサイバーセキュリティのリスクに対応し、また同時に関連する機会を捉えていくにあたり、金融商品の役割の重要性が増している。金融資本市場におけるサイバーセキュリティ関連の主な金融商品として、サイバーファンド、サイバー保険が挙げられる。このうち、サイバー保険は、サイバーセキュリティ関連の金融商品の中で最も長い歴史を有し、企業のサイバーリスクへの有力な対応策と考えられる。

本稿では、サイバーファンド、サイバー保険について米国や日本における概況や事例を紹介した上で、サイバーセキュリティ関連の金融商品が発展していくための主な課題を論考する。

Ⅱ サイバーファンドの提供状況

本章では、米国及び日本のサイバーファンドの提供状況を示す。

１．米国におけるサイバーセキュリティ関連の上場投資信託（ETF）

米国では2013～2014年に発生した、小売大手であるターゲットや電子商取引（EC）大手のイーベイに対するサイバー攻撃で発生した大規模な個人情報の流出事件を背景として[2]、企業によるセキュリティ関連投資が活発化するとの見方が示される中、米国においてサイバーセキュリティの分野に対する注目度が高まった[3]。そして、2014 年に、世界初のサイバーファンドであるピュアファンズ ISE サイバーセキュリティ ETF（現アンプリファイ・サイバーセキュリティ ETF）がニューヨーク証券取引所（NYSE）アーカに上場された。その後、2015年にファーストトラスト・ナスダック・サイバーセキュリティETFが上場した（図表 1）。

これらの ETF は、サイバーセキュリティに関連する企業から構成されるサイバー指数に連動したパフォーマンスを目指している。具体的には、アンプリファイ・サイバーセキュリティETFはナスダックISEサイバーセキュリティ・セレクト指数を、ファーストトラスト・ナスダック・サイバーセキュリティ ETF はナスダック CTA サイバーセキュリ

1 「KADOKAWA 株価年初来安値　ハッカー集団が犯行声明」『日本経済新聞』2024 年 6 月 28 日。
2 「米小売り、個人情報流出相次ぐ　イーベイやターゲット」『日本経済新聞』2014 年 7 月 28 日。
3 「セキュリティー銘柄 ETF、サイバー犯罪深刻化で注目」『日経ヴェリタス』2014 年 11 月 23 日。

図表 1　米国におけるサイバーセキュリティ関連の ETF の事例

名称	アンプリファイ・サイバーセキュリティ ETF	ファーストトラスト・ナスダック・サイバーセキュリティ ETF
設定時期	2014 年 11 月	2015 年 7 月
運用会社	アンプリファイ ETFs	ファーストトラスト
上場市場	NYSE アーカ	ナスダック
連動する指数	ナスダック ISE サイバーセキュリティ・セレクト指数	ナスダック CTA サイバーセキュリティ指数
組入銘柄数	23	30
純資産総額	約 16.6 億ドル	約 63.6 億ドル

（注）　2024 年 3 月時点。
（出所）Amplify ETFs, “HACK Amplify Cybersecurity ETF”、First Trust, “First Trust Nasdaq Cybersecurity ETF (CIBR)”、を基に野村資本市場研究所作成

ティ指数をベンチマークとしている。両 ETF の組入銘柄の国別の内訳を見ると、全体の約 7～9 割は米国に本拠を置く企業となっている（2024 年 3 月時点）[4]。

両 ETF がベンチマークとしている指数のうち、ナスダック ISE サイバーセキュリティ・セレクト指数の構成企業は、サイバーセキュリティ関連のサービス提供会社であり、サイバーセキュリティの事業活動が事業全体の主要ドライバーである企業とされる（図表 2）。本指数の構成銘柄数は 2024 年 3 月時点で、23 銘柄である。一方、ナスダック CTA サイバーセキュリティ指数は、サイバーセキュリティ分野に属する企業のパフォーマンスを測定するものである。本指数には、ネットワーク、コンピューター、モバイル端末へのセキュリティサービスの構築・実施・管理を行う企業が含まれる。本指数の構成銘柄数は 30 銘柄となっている。

図表 2　サイバーセキュリティ関連の ETF がベンチマークとするサイバー指数

名称	ナスダック ISE サイバーセキュリティ・セレクト指数	ナスダック CTA サイバーセキュリティ指数
提供	ナスダック	ナスダック
構成銘柄数	23	30
特徴	ISE サイバーセキュリティ業種（世界の上場企業で、サイバーセキュリティ関連の活動による売上の割合が 10%以上であること等）に分類される、サイバーセキュリティ・サービスの提供企業。親指数はナスダック ISE サイバーセキュリティ指数	消費者向けテクノロジー関連の業界団体である全米民主技術委員会（CTA）がサイバーセキュリティ関連企業として分類している企業
その他の基準例	時価総額 10 億ドル以上、参照日から遡って 3 か月間で 1 日の平均取引金額が 100 万ドル以上	時価総額 5 億ドル以上、参照日から遡って 3 か月間で 1 日の平均取引金額が 100 万ドル以上

（注）　2024 年 3 月時点。
（出所）ナスダックウェブサイト、より野村資本市場研究所作成

[4] Amplify ETFs, “HACK Amplify Cybersecurity ETF”; First Trust, “First Trust Nasdaq Cybersecurity ETF (CIBR).”

２．日本におけるサイバーセキュリティ関連の投資信託

投資信託協会が運営する投信総合検索ライブラリーにおいて、サイバーセキュリティ関連ファンドを検索すると 10 件のファンドが確認できる[5]。このうち純資産総額が上位のファンドとして、世界のサイバーセキュリティ関連企業を投資対象とするもの（サイバーセキュリティ株式オープン〔為替ヘッジなし〕）と、セキュリティに関連する幅広い企業を投資対象とするもの（グローバル・セキュリティ株式ファンド〔3 か月決算型〕及びピクテ・セキュリティ・ファンド〔為替ヘッジなし〕）が見られる[6]（図表 3）。

これらのファンドは、サイバーセキュリティ関連の投資対象企業として、サイバーセキュリティ技術を活用した製品・サービスを提供する企業に注目している。投資先企業は、米国におけるサイバーファンド同様、米企業が中心となっており、米国がサイバーセキュリティ分野での主要な位置を占めていることが窺える。

図表 3　日本におけるサイバーセキュリティ関連の投資信託の事例

名称	サイバーセキュリティ株式オープン（為替ヘッジなし）	グローバル・セキュリティ株式ファンド（3 か月決算型）	ピクテ・セキュリティ・ファンド（為替ヘッジなし）
設定時期	2017 年 7 月	2015 年 12 月	2016 年 2 月
運用会社	三菱 UFJ アセットマネジメント	アセットマネジメント One	ピクテ・ジャパン
ファンドの特色	世界のセキュリティ関連企業	日常生活に不可欠な「情報・身体・移動等の安全」を支える製品・サービスを提供する企業	主に世界のセキュリティ関連企業（「暮らしの安心」、「移動の安心」、「情報の安心」へのニーズに応える製品・サービスを提供する企業）
投資対象の詳細（サイバーセキュリティに関連する内容のみ記載）	日本を含む世界のサーバセキュリティ関連企業。具体的にはサイバー攻撃に対するセキュリティ技術を有し、これを活用した製品・サービスを提供するテクノロジー関連企業（ヴォヤ・インベストメント・マネジメントに運用指図の権限を委託）	情報の安全の観点から、コンピューターウイルス対策、ネットバンキングシステム、データベース管理システム等の事業を行う企業	情報の安心（電子決済システム、コンピューターウイルス対策、ネットワーク管理システム）、へのニーズに応える製品・サービスを提供する企業
組入銘柄数	44	50	39
純資産総額	約 3,589 億円	約 536 億円	約 234 億円

（注）　2024 年 4 月時点。
（出所）各投資信託の月次レポートを基に野村資本市場研究所作成

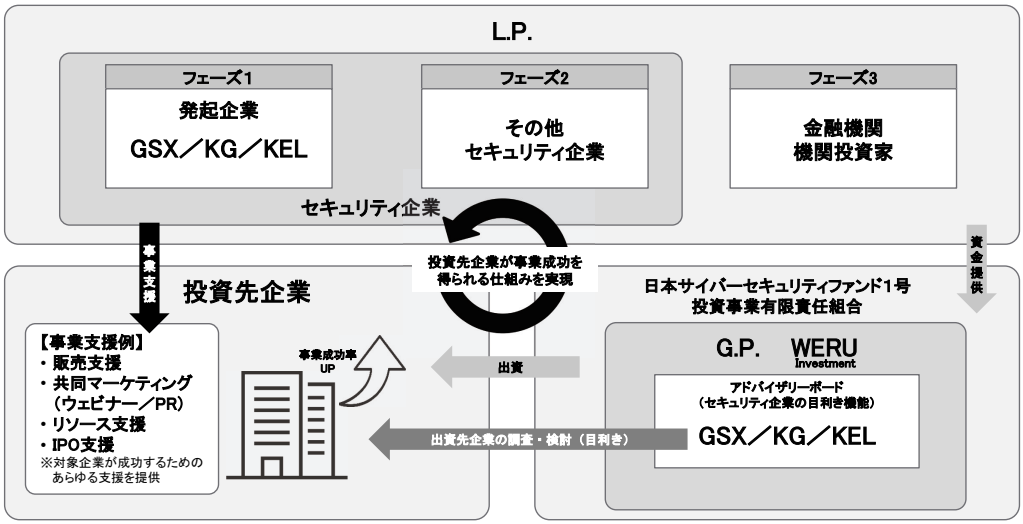
[5] 投信総合検索ライブラリーにおいて、サイバーセキュリティ、セキュリティに関連する投資信託を抽出。2024 年 6 月 28 日時点。
[6] 同一の運用会社でファンドの目的・特色が類似するファンドにおいては純資産総額が最も大きいファンドのみを挙げている。

３．兼松等が設立を発表したサイバーファンド

兼松、兼松エレクトロニクス、グローバルセキュリティエキスパート（GSX）は 2024 年 3 月、ウエルインベストメントを無限責任組合員とした、サイバーセキュリティファンド（日本サイバーセキュリティファンド 1 号投資事業有限責任組合）の設立を発表した[7]。

ファンドの特徴は、GSX をはじめとしたセキュリティ専業企業が出資し、セキュリティ企業に投資を行なうことを目的としている点である。ファンド内には出資企業で構成されるアドバイザリーボードが設置され、業界の経験・知見に基づく投資先企業の調査・検討（目利き）を行う（図表 4）。例えば、アドバイザリーボード内の GSX は準大手・中堅中小企業を中心にサイバーセキュリティコンサルティングを通じた経験・知見を活かす。それと同時に、出資企業が、サービス・販路・経営ノウハウを共有し、投資先企業を支援する。こうした目利きと事業支援の 2 つの要素を通じて、投資先企業の成長を加速させ、事業の成功確率を高める。

図表 4　兼松等が設立を発表したサイバーファンドの概要



（注）　G.P.は無限責任組合員、L.P は有限責任組合員、GSX はグローバルセキュリティエキスパート、KG は兼松、KEL は兼松エレクトロニクス、を指す。

（出所）兼松、兼松エレクトロニクス、グローバルセキュリティエキスパート、ウエルインベストメント「日本初、セキュリティ企業に投資するファンド『日本サイバーセキュリティファンド 1 号投資事業有限責任組合』をウエルインベストメント、兼松、KEL、GSX が中心となり創設～セキュリティ企業の成長を後押し、業界全体を牽引します～」2024 年 3 月 25 日、を基に野村資本市場研究所作成

[7] 兼松、兼松エレクトロニクス、グローバルセキュリティエキスパート、ウエルインベストメント「日本初、セキュリティ企業に投資するファンド『日本サイバーセキュリティファンド 1 号投資事業有限責任組合』をウエルインベストメント、兼松、KEL、GSX が中心となり創設～セキュリティ企業の成長を後押し、業界全体を牽引します～」2024 年 3 月 25 日。

ファンドの投資対象企業は、（1）シード期などこれから立ち上がっていく企業、（2）上場を既に検討している企業、（3）株価が伸び悩んでいる企業、である。投資対象については、「セキュリティ業界全体を盛り立て、日本全国の企業にサービスを届けることで自衛力向上を実現していく」という観点から、幅広い企業が含められている。今後、セキュリティ業界の企業、金融機関、機関投資家に参画を促しながら、上限 100 億円を目標にファンド組成を進めていくことが発表されている[8]。

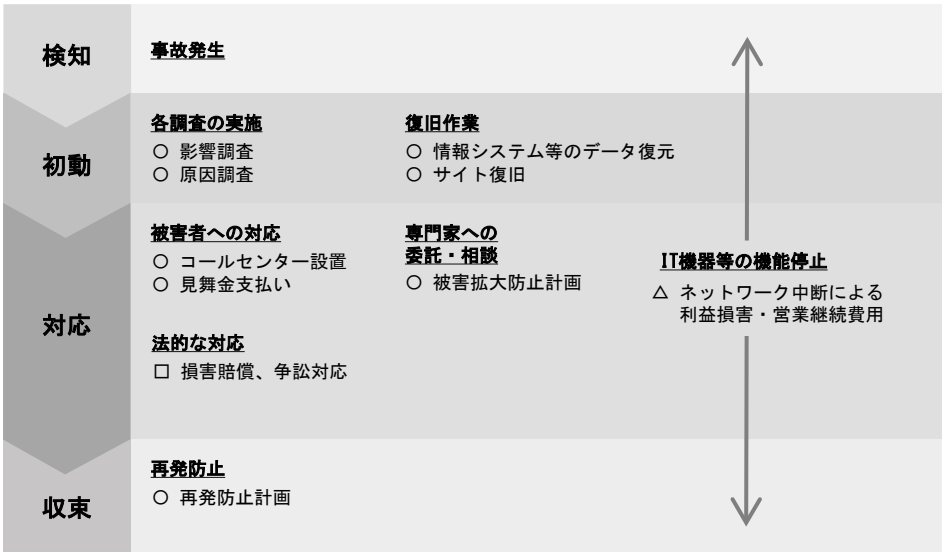
Ⅲ サイバー保険の仕組みと浸透状況

本章では、サイバー保険の仕組みを概観した上で、米国及び日本のサイバー保険の浸透状況を示す[9]。

１．サイバー保険の仕組み

サイバー保険とは、サイバーセキュリティリスクに起因して発生する様々な損害に対応するための保険である[10]。同保険の補償内容は、（1）損害賠償責任、（2）事故対応費用、（3）利益損害・営業継続費用、に大別される（図表 5）。

図表 5　サイバー攻撃への対応の流れ（一例）



（注）　○は事故対応費用、△は利益損害・営業継続費用、□は損害賠償責任。
（出所）一般社団法人 日本損害保険協会「サイバー保険」、より野村資本市場研究所抜粋

[8] 発表されているスケジュールは、2024 年 4 月に「日本サイバーセキュリティファンド 1 号投資事業有限責任組合」が設立（及びファーストクローズ）、2024 年 6 月末にセカンドクローズ（セキュリティ企業が参画）、2024 年中旬以降にファイナルクローズ（金融機関・機関投資家が参画）。

[9] サイバー保険についての詳細は、別稿（富永健司「企業のサイバーセキュリティリスクとサイバー保険」『野村サステナビリティクォータリー』2023 年秋号）を参照。

[10] 一般社団法人日本損害保険協会「サイバー保険」。

損害賠償責任は、被保険者が法律上負担する損害賠償金や、争訟費用等による損害が対象となる。具体的には、顧客や取引先等の第三者に対する損害賠償責任を補償する。事故対応費用は、サイバー事故に起因して一定期間内に生じた費用が対象となる。具体的には、事故原因調査、法律相談等に関連する各種費用を補償する。利益損害・営業継続費用は、ネットワークを構成する IT（情報技術）機器等が機能停止することによって生じた利益損害（喪失利益・収益減少防止費用）や営業継続費用が対象となる。

具体的な事故の例としては、情報漏洩又はその恐れ、ネットワークの所有・使用・管理に起因する他人の業務阻害、サイバー攻撃に起因する他人の身体傷害・財物損壊等が挙げられる。

２．米国と日本におけるサイバー保険の浸透状況

米国においてサイバー保険は、コンピューター誤作動の懸念が指摘された 2000 年問題をきっかけに、米保険大手の AIG が 1997 年に提供を開始した[11]。米国ではサイバー保険の普及が進んでおり、保険監督者国際機構[12]（International Association of Insurance Supervisors、IAIS）の調査によれば、世界のサイバー保険の元受収入保険料（2020 年時点）の約 53%を米国が占めている[13]。米国においては、米国外に本拠を置く保険会社・グループによるサイバー保険の引き受けが積極的に実施されている[14]。

日本では、2012 年頃よりサイバー攻撃による被害を包括的に補償する保険が登場した[15]。具体的な例として、AIG傘下のAIU保険によるサイバーエッジ保険等が挙げられる。同社は 2004 年より個人情報漏洩保険を販売していたが、当該保険により、損害賠償に加えて、サイバー事故の調査による費用や逸失利益等を対象とすると共に、補償対象地域を全世界に広げた。2015 年には、東京海上日動火災保険が国内の大手損害保険会社で初めてサイバー保険を発売した[16]。その後、損害保険各社の参入が本格化し、サイバー保険商品の拡充が進んだ。

他方、サイバー保険の元受収入保険料の日本のシェアは、2020 年時点で約 3%である[17]。日本損害保険協会が公表した国内企業 1,535 社を対象としたサイバーリスク意識・対策実態調査[18]において、サイバー保険に加入していると回答した企業は全体の 7.8%にとどまっており、国内では依然としてサイバー保険の普及余地があるとの見方が示されている。サイバー保険に加入しない理由に関する設問では、「保険の補償内容や保険料についてよ

[11] 独立行政法人情報処理推進機構「米国におけるサイバー保険の現状」2017 年 12 月。
[12] 保険分野の監督に関する原則、基準、ガイダンス等の策定及び実施の支援を行う基準設定機関。200 超の国・地域の保険監督当局がメンバーになっている。
[13] International Association of Insurance Supervisors (IAIS), “Global Insurance Market Report,” November 30, 2021.
[14] 詳しくは、富永健司「企業のサイバーセキュリティリスクとサイバー保険」『野村サステナビリティクォータリー』2023 年秋号、を参照。
[15] 「大手損保各社、サイバー保険を相次ぎ投入―認知度高まり市場活性化」『日刊工業新聞』2015 年 4 月 15 日。
[16] 「サイバー保険、現場に解　東京海上日動の教学大介さん」『日本経済新聞』2023 年 4 月 21 日。
[17] 前掲脚注 13 参照。
[18] 一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」2020 年 12 月。

く知らないため」が 40.7%と最も多かった。また、約 2 割が「サイバー被害を受ける可能性が低いため」としており、回答企業の危機意識の低さについても指摘されている。

Ⅳ 今後の課題

金融資本市場においては、サイバーセキュリティに関連して、サイバーファンド、サイバー保険といった金融商品を通じて、サイバーセキュリティのリスクへ対応し、関連する機会を捉えようとする動きが進展している。現状、サイバー保険の普及及びサイバーファンドの投資対象といった観点から、米国が主要な位置づけを占める一方で、日本においては、サイバーファンドの投資拡大、サイバー保険のさらなる浸透の余地があると見られる。

近年、サイバー攻撃の脅威は大企業だけではなく、サプライチェーンを構成する中小企業にも及んでおり、サプライチェーン全体を通じた対策の推進が求められている[19]。兼松等が 2024 年 3 月に設立を発表したサイバーファンドは、投資先のセキュリティ企業を経営面・販路拡大・マーケティング等の幅広い領域で支援していくことで、国内の大企業のみならず、中小企業のセキュリティ対策の向上を目指している。今後、こうした国内のサイバーセキュリティ関連企業等を投資対象とするサイバーファンドによる支援が、日本企業全体のサイバーセキュリティ対策の強化に寄与していくことが期待される。

他方、国内において企業のサイバー事故は、多種多様な業種において発生しており、同事故が発生した後の資金面の備えを提供するサイバー保険の必要性が高くなっていると考えられる[20]。サイバー保険の加入率の向上に向けて、日本損害保険協会による前述のサイバーリスク意識・対策実態調査の結果から示唆されるサイバーセキュリティに対する意識向上、サイバー保険の認知度向上等の課題に取り組んでいくことが重要である。また、企業のサイバー事故は、不正アクセス行為、サイバー攻撃、システムの誤設定による情報の不正閲覧、メールの誤送信、個人情報を含む情報機器の紛失等と多岐にわたっている。企業は、こうした多様なサイバー事故に対処していくにあたり、サイバー事故の実態を把握・理解し、自社の事業に照らしたリスク認識を行うことが重要と考えられる。

今後、サイバーセキュリティ関連の金融商品が発展していくための主な課題としては、（1）サイバーセキュリティに係る金融商品の開発努力、（2）官民の連携強化による技術革新へのファイナンス支援、が挙げられる。

１．サイバーセキュリティに係る金融商品の開発努力

企業のサイバーセキュリティ対策は、企業活動におけるコストや損失を減らすための必要不可欠な投資であり、将来の事業活動・成長に必要な費用と位置づけられる。したがって、企業はサイバーセキュリティの取り組みを強化し、適切なリスク管理を進めていくこ

[19] 経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」2023 年 3 月 24 日。
[20] 前掲脚注 14 参照。

とが重要である。そして、金融資本市場は、企業のサイバーセキュリティに関連するリスクを管理し、投資機会を提供する金融商品を通じて、企業のサイバーセキュリティの取り組みを支援していくことが求められる。

サイバーセキュリティ関連における新たな金融商品を提供する動きとしては、英損害保険会社であるビーズリーが 2023 年 1 月に発行した、世界初のサイバーセキュリティリスクを対象とする大災害債券（Catastrophe bond、CAT ボンド）が挙げられる[21]。同債券は、損害額が 3 億ドル超の大規模なサイバー事故の発生時に元本が減額され、ビーズリーが保険の支払いに備えることができる仕組みとなっている。その他にも、サイバー攻撃の社会的影響が大きくなっていることや、サイバーセキュリティの分野でセキュリティ評価の活用が広がっていることを踏まえて[22]、例えば、サイバーセキュリティの強化が重視される企業において、サステナビリティ・リンク・ボンド[23]の発行時に選定・設定される重要業績評価指標（KPI）及びサステナビリティ・パフォーマンス・ターゲット（SPTs）に、発行体のサイバーセキュリティの取り組みの評価を組み入れることも検討し得ると思われる。こうしたサイバーセキュリティに関連する新たな商品が、社会におけるサイバーセキュリティのリスクへの対応力強化と関連する機会の獲得につながっていくことが期待される。

２．官民の連携強化による技術革新へのファイナンス支援

昨今、社会のデジタル化の進展や人工知能（AI）技術の活用が進んでおり、企業がサイバーセキュリティへの対応力を強化するにあたって、革新的なセキュリティ技術を取り入れていくことの必要性が高まっている。こうした点を踏まえると、サイバーセキュリティ関連の金融市場の進展には、金融商品そのものの開発・設計だけではなく、企業によるサイバーセキュリティ関連の製品・サービスの技術革新に対するファイナンスを支援する金融手法・仕組みを構築する視点も重要である。

企業による革新的なセキュリティ技術の開発に必要な資金調達の仕組みを考えていく際には、地政学リスクの増大がサイバー攻撃の加速度的な増加につながる可能性があることを踏まえて、官民のイニシアティブによって取り組みを進めることも一つの選択肢になると思われる。

例えば、エストニアは 2007 年に大規模なサイバー攻撃が発生した経験から、サイバーセキュリティの強化に取り組む中、官民が連携し、サイバーセキュリティ関連のスタートアップへの支援を行っている。エストニアは 2008 年に初となるサイバーセキュリティに関する国家戦略（2008~2013 年）を策定し、サイバーセキュリティ強化の方針を打ち出し

[21] Beazley, “Beazley launched market’s first cyber catastrophe bond,” January 9, 2023.
[22] 例えば、野村アセットマネジメントは、サイバーセキュリティ評価の提供会社である Bitsight Technologies と提携して、国際開発金融機関セクターにおける発行体のサイバーセキュリティに関連するパフォーマンスの水準を分析している。詳しくは、ジェイソン・モーティマー「サイバーセキュリティ・エンゲージメント―投資家向けガイド―」『野村サステナビリティクォータリー』2024 年春号、を参照。
[23] あらかじめ定められたサステナビリティの目標を達成することで条件が変化する債券。

た[24]。その後、第 2 次サイバーセキュリティ戦略（2014～2017 年）を経て、エストニアの経済通信省が 2019 年に公表した第 3 次サイバーセキュリティ戦略（2019～2022 年）において、サイバーセキュリティ関連のセクターにおいて、世界的に競争力のあるスタートアップを創出するために研究開発活動を促進する、との目標を掲げた[25]。具体的な取り組みとして、政府が、欧州でも有数のアクセラレーター[26]兼ベンチャーキャピタルであるスタートアップ・ワイズ・ガイズと連携して、2019 年にサイバーセキュリティ関連のプログラムを設立したことが挙げられる[27]。同プログラムは 2019 年及び 2020 年に、15 社のスタートアップを選抜し、事業及び資金調達支援を行った[28]。日本においても、こうした事例を参考にしながら、官民の連携強化により、サイバーセキュリティ分野の革新的な技術に対するファイナンス支援の仕組みを検討することも意義があると言える。

[24] Ministry of Defense Estonia, “Cyber Security Strategy Cyber Security Strategy Committee,” 2008.

[25] Republic of Estonia Ministry of Economic Affairs and Communications, “Cybersecurity Strategy Republic of Estonia 2019-2022.”

[26] アクセラレーターとは、シードステージ（起業前のアイデア・コンセプトの構想段階から、課題解決に向けた仮説検証の段階）以降のスタートアップ等の成長を促進するために、3～6 か月程度のプログラムを提供する組織。スタートアップとは、（1）新しい企業で、（2）新しい技術やビジネスモデル（イノベーション）を有し、（3）急成長を目指す企業、を指す（経済産業省「スタートアップの力で社会課題解決と経済成長を加速する」2024 年 2 月）

[27] Invest in Estonia, “Estonia invites new cyber security startups—a unique cyber security and AI accelerator to be opened,” 2018 November.

[28] Startup Wise Guys, “8 cybersecurity startups to watch—CyberNorth first batch announced,” April, 2019.; Startup Wise Guys, “7 cybersecurity startups to look out for—second Startup Wise Guys CyberNorth batch announced,” March 4, 2020.