NO.832210123

経済産業省商務情報政策局サイバーセキュリティ課　御中

令和4年度サプライチェーン・サイバーセキュリティ対策促進事業（国内セキュリティ関連市場における製品・サービス提供者及び機器検証事業者に関する実態調査）

【調査報告書】

2023年3月31日

株式会社富士キメラ総研
Fuji Chimera Research Institute,Inc.

監修者：田中一志

〒103-0027 東京都中央区日本橋三丁目9番1号 日本橋三丁目スクエア

TEL. 03-3241-3490　FAX. 03-3241-3491

Ⅰ. 調査企画テーマ

・　令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（国内セキュリティ関連市場における製品・サービス提供者及び機器検証事業者に関する実態調査）

Ⅱ. 調査項目

1. 国産セキュリティ製品やサービスの支援策の検討
2. 機器検証事業者の支援策の検討

Ⅲ. 実施方法

・　弊社専任調査員によるプロジェクトチームを編成して調査を実施する。調査手法としては弊社データベースに加え、公開情報などを活用する。

・　国内セキュリティ市場の動向や将来予測に関わる文献としては、弊社で刊行するレポートを活用する。

〈文献例〉

2022 ネットワークセキュリティビジネス調査総覧 市場編

(㈱富士キメラ総研 2022 年 11 月 17 日発刊)

2022 ネットワークセキュリティビジネス調査総覧 ベンダー戦略編

(㈱富士キメラ総研 2022 年 11 月 17 日発刊)

目　　次

1. 事業の目的 1
2. 事業の概要 1
2.1.国内セキュリティ市場の状況と将来予測 1
2.2.産業育成観点での注力領域の設定 1
2.3.経済安保観点での対象市場の設定 1
2.4.検証事業の現状 1

3.国内セキュリティ市場の概況 2
3.1.国内セキュリティ市場規模の算定と推移予測（国内セキュリティ市場概況） 2
3.1.1.国内セキュリティ市場推移(2021～2027 年度) 2
3.1.2.セキュリティ市場を取り巻く環境 3
3.1.3.セキュリティ市場を取り巻く注目キーワード分析 8
3.1.4.セキュリティサービス/ツールのポジション分析 14
3.2.業種別/規模別動向 17
3.3.領域別動向 22
3.4.まとめ 23

4.注力すべきセキュリティ事業領域 24
4.1.設定の考え方（アプローチ方法） 27
4.2.検討結果（5 領域） 28
4.3.ベンダー調査 30
4.3.1.サイバーセキュリティ演習サービス 30
4.3.2.IDaaS 32
4.3.3.Web アプリケーション脆弱性検査ツール 34
4.3.4.端末管理・セキュリティツール(統合エンドポイント管理ツール) 36
4.3.5.クラウドセキュリティ 38
4.4.ヒアリングした企業からの意見まとめ 39
4.5.考察 39

5.強化すべき市場分野と現状 40
5.1.設定の考え方（経済安全保障におけるポイント） 40
5.2.調査対象とした業界とその理由 41
5.3.業界別動向 42
5.3.1.電力業界 42
5.3.2.ガス業界 44
5.3.3.金融業界 45
5.3.4.交通業界 46
5.3.5.情報通信 49

5.3.6.半導体 50
5.3.7.医療機器 52
5.4.まとめ 54
5.5.考察 55

6.IoT 検証機器事業者総括 57
6.1.市場定義(IoT デバイス脆弱性検査サービス) 57
6.2.市場規模推移 57
6.3.IoT 検証事業者の対象ヒアリング選定基準 57
6.4.今後注力する検証対象分野の見解、今後の注力領域、ガイドラインへの見解 58
6.5.考察 59

7.総括 60

1.事業の目的

経済産業省（以下、経産省）では「産業サイバーセキュリティ研究会」WG3（サイバーセキュリティビジネス化）1 での検討結果に基づき、独立行政法人情報処理推進機構によるベンチャー企業を対象とした国産セキュリティ製品・サービスの有効性検証の試行と検証結果の公開 2 や、IoT機器等の脆弱性やセキュリティ対策の妥当性を確認する検証手法や検証サービス事業者及び検証依頼者が実施すべき事項や、二者間のコミュニケーションにおいて留意すべき事項等について整理した「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き 3」を整備し、国産セキュリティ関連事業者を対象とした事業機会の拡大に関わる取り組みを行っている。国産セキュリティ関連事業者から、これらの取り組みが自社の事業拡大に有用であるとの評価に加えて、更なる国内市場展開に向けた支援を求められており、マーケットインに向けた国内セキュリティ市場の実態把握が必要となっている。

こうした背景のもと、本事業では、国内セキュリティ市場において経済安全保障の観点から国産セキュリティ製品・サービスの導入を推進すべき業種・領域の設定と、産業育成の観点から今後市場拡大が見込まれるセキュリティ領域の現状と将来予測、及びIoT製品等の機器を対象とした国内のセキュリティ検証事業の現状に関わる調査等を実施することで、国産セキュリティ関連事業者の市場参入機会の拡大につなげることを目的とした。

2.事業の概要

2.1.国内セキュリティ市場の状況と将来予測

国内セキュリティ市場の状況と将来予測を実施するため、富士キメラ総研の発刊している「2022 ネットワークセキュリティビジネス調査総覧 市場編(2022 年 11 月 17 日発刊)」「2022 ネットワークセキュリティビジネス調査総覧 ベンダー戦略編(2022 年 11 月 17 日発刊)」を参考文献とし、必要に応じて弊社データベースを活用した。

2.2.産業育成観点での注力領域の設定

産業育成の観点で詳細な分析を行う領域を特定するため、以下の項目を数値化し分析、比較した。

- ✓ 2021 年度の市場規模
- ✓ 2021 年度から 2027 年度までの平均成長率
- ✓ 市場規模における国産ベンダーの売上構成比
- ✓ 情報セキュリティ 10 大脅威 2023(組織、IPA が 2023 年 1 月 25 日に公表したものを活用)への影響度

上記の項目における総合スコアが高いセキュリティ分野を注力領域と定め、各領域に参入している企業へのヒアリングを実施した。ヒアリングには訪問、Web 電話といった手法を用い今後の見解や市場拡大における課題をヒアリングした他、公開情報を活用した分析も行った。

2.3.経済安保観点での対象市場の設定

経済安全保障の観点から、重要インフラや国内最大の産業である製造業に対し、サイバー攻撃によるシステム停止や情報漏洩により、「国民の生命・財産」「経済や社会生活の安定」への影響が大きくなると想定された 7 業種を選定し、現状のセキュリティ対策から今後のセキュリティ対策への見解や、セキュリティ対策を実施する上での課題、国の支援に関する見解などの情報をヒアリングした。ヒアリングには訪問、Web 電話といった手法を用い今後の見解や市場拡大における課題をヒアリングした他、公開情報を活用した分析も行った。

2.4.検証事業の現状

弊社の調査にて、国内で IoT 関連の検証事業を実施しているベンダーのシェア上位 5 社の内 3 社から市場全体の動向やトピックをヒアリングするとともに、比較的小規模ながら独自のソリューションを展開しているベンチャー系ベンダー2 社にヒアリングを実施した。ヒアリングには訪問、Web 電話といった手法を用い今後の見解や市場拡大における課題をヒアリングした他、公開情報を活用した分析も行った。

3.国内セキュリティ市場の概況

2019 年後半から始まったコロナ禍により、多くの企業でテレワークが広がった。これにより、従来の一般的なセキュリティモデルであったファイアウォールや UTM などのゲートウェイセキュリティを中核とした境界型防御から、インターネット上にあるクラウド認証基盤から外部や他の拠点につながる非境界型防御へとシフトしている。中でもゼロトラストセキュリティへの関心が非常に高まったことで、大手企業を中心に新たな環境構築に向けたセキュリティコンサルティングや関連ツールの導入が盛り上がっている。

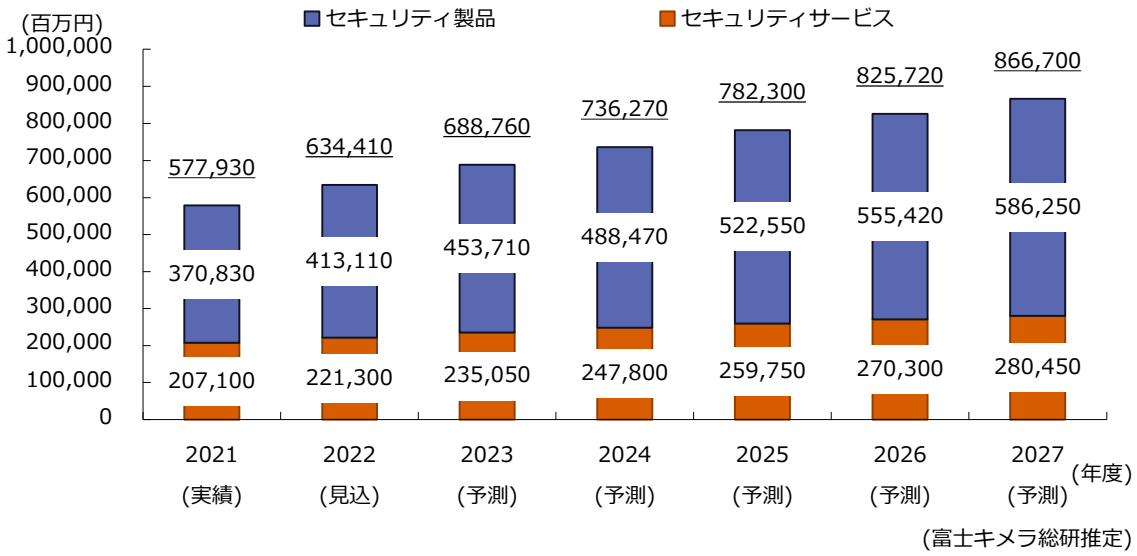
セキュリティツールも従来のソフトウェアやアプライアンスから、クラウドサービスとして提供されるモデルが増加しており、既存環境からのリプレースが増加している。ゲートウェイセキュリティを除く多くのセキュリティ分野でクラウドサービスへの移行が進展しており、ユーザーの運用負荷軽減を含めた需要を獲得しているとみられる。

一方、ゲートウェイセキュリティに関しては依然としてアプライアンスが中心となっている。一部では FWaaS の利用も増加しているが、物理的に置けることで、ネットワークの境界としてわかりやすいことや、ゼロトラストセキュリティに関してもテレワークなどのアクセスが非境界型防御に移行する一方、拠点間通信などは依然として従来型のネットワーク環境が残っているケースも多くなっていることが要因とみられる。

セキュリティ市場を取り巻く環境としては、セキュリティ人材の不足から MSS などのサービスを利用する企業が増加する一方、サービスを提供するベンダー側でのセキュリティ人材不足も深刻化しており、社会全体でのセキュリティ人材育成が急務となっている。ここ数年はコンサルティングファームの参入により、サービスベンダーから人材の流出も多くなっていたが、2022 年に入り、ユーザー企業でも自社でセキュリティ人材を雇用する動きがより活性化している。背景には企業の DX 推進が挙げられ、社内業務を理解していないセキュリティベンダーのサービスでは対処が難しい領域が増加していることとみられる。DX では社内業務を効率化するための取り組みが進む一方、その業務を理解した上でのセキュリティ対策を実施できる人材が求められており、さらなるセキュリティ人材につながっている。

3.1.1.国内セキュリティ市場推移(2021～2027 年度)

図表 1「国内セキュリティ市場規模推移」



(富士キメラ総研推定)

国内のセキュリティ市場は堅調に推移しており、2027 年までの平均成長率は 7.0%を見込んでいる。ゼロトラストへの取り組みが大手企業で活況となっており、特に Web アクセスなど SASE 領域の成長が大きくなっている。また、そのネットワーク環境の構築におけるコンサルティングなども好調となっている。今後はこのゼロトラストへの運用サービス拡大も見込まれる。

セキュリティサービスとしては、コンサルや設計といった上流工程の市場が活況であった。また、セキュリティスコアリングやスレッドインテリジェンスといった比較的新しいサービスも認知度の高まりとともに堅調に推移している。一方、MSS に関してはセキュリティ人材の制約や自動化ツールなどの活用が遅れていることで成長率はやや落ち込みがみられた。ただし、昨今市場をけん引するゼロトラスト関連のツールに関する運用ニーズが徐々に台頭しており、今後も新しいツールの運用支援ニーズの拡大が見込まれる。このため、セキュリティ人材の不足はセキュリティビジネス全体にとって大きな課題となっている。

セキュリティツールとしては SASE や EDR といったツールが市場をけん引している。昨今注目されている XDR や CSPM/CWPP といった新しいツールは認知度がまだ低く導入実績は少ないものの、将来的には大きな成長が見込まれる。ツールはゲートウェイセキュリティを除きクラウド化の進展が顕著となっており、参入ベンダーもクラウド対応を強化している。セキュリティ投資の大きい大手企業ではセキュリティの観点から国内データセンターでのサービス提供を望むケースが多くなっており、ベンダー側でもそれに対応した取り組みを進めている。

また、セキュリティ市場全体の課題としては大手企業の投資が大きく、中堅、中小企業でのセキュリティ投資が伸び悩んでいることが挙げられる。サプライチェーン攻撃などへの対策として、中堅、中小企業でのセキュリティ対策も強化が求められることから、社会全体の課題になっている。

3.1.2.セキュリティ市場を取り巻く環境

1)セキュリティ脅威の変遷とセキュリティ対策

図表 2「国内の IT およびセキュリティに関する経緯」

年	IT 環境	情報セキュリティへの脅威	主なセキュリティ対策
2000～	・ ブロードバンドの台頭、普及 ・ 電子メール利用の一般化 ・ 公衆無線 LAN	・ コンピューターウイルス ・ メール添付/ワーム型 ・ 不正アクセス ・ マルウェア	・ ウイルス対策 ・ スパイウェア対策 ・ インターネット GW 対策 (FW、IPS/IDS) ・ Web レピュテーション/ファイルレピュテーション
2005～	・ モバイル活用	・ フィッシングサイト ・ 標的型攻撃 ・ ボットネット ・ モバイルへの攻撃 ・ DDoS 攻撃	・ フィルタリング ・ ふるまい検知 ・ Web アプリケーション可視化 ・ UTM
2010～	・ 仮想化/クラウドサービス利用 ・ 働き方改革	・ 制御システム向け攻撃/USB 媒介ウイルス(Stuxnet 攻撃) ・ WannaCry/ランサムウェア	・ 脆弱性攻撃対策 ・ データ暗号化 ・ サンドボックス検出技術 ・ ランサムウェア対策
2017	・ IoT/M2M 機器の増加	・ Mirai/IoT 機器のボット化	・ ホワイトリスト
2018	・ 閉域環境のオープン化 ・ SDN-NFV	・ 未知のマルウェア	・ フォレンジック調査(EDR) ・ 潜在的マルウェア対策
2019	・ Society 5.0 や DX 推進	・ サプライチェーンを悪用した攻撃の増加	・ CASB ・ 委託先/取引先企業へのセキュリティ対策強化
2020	・ テレワークの急速な拡大 ・ Web 会議システム利用の増加	・ Emotet などのマルウェア ・ 金融機関に対する攻撃 ・ アカウント乗っ取り	・ ゼロトラスト、SASE、NDR
2021	・ テレワークの定着	・ テレワーク環境への攻撃 ・ 海外拠点へのランサムウェア攻撃 ・ Log4j 脆弱性	・ 脆弱性診断
2022	・ 業務自動化/省力化の推進	・ 内部不正による情報漏えい ・ Emotet の感染再拡大 ・ 紛争に伴うサイバー攻撃増加	・ 操作履歴の監視 ・ 情報リテラシー、情報モラルの強化 ・ サイバー戦への対策
今後	・ DX 推進(AI の活用) ・ IoT の拡大 ・ 自動運転の普及 ・ Web サービスのさらなる普及	・ 新しい DX システムへの攻撃 ・ IoT 環境から IT 領域への攻撃 ・ クラウドや Web サービスへの攻撃増加 ・ テレワーク定着によるなりすましの増加	・ セキュリティ演習によるインシデント発生後の対処 ・ Web アプリケーション脆弱性診断やクラウドセキュリティによる新しいシステムのセキュリティ強化 ・ 端末管理ツールを活用したサイバーハイジーンによる社内攻撃対象となるデバイス管理。 ・ IDaaS による認証強化、なりすまし防止 ・ SOAR、UEBA を活用したセキュリティの自動化対応

IT 環境の整備とともにサイバー攻撃の手段が多様化したことから、個人や組織を狙ったサイバー攻撃は年々増加し、高度化している。時流に応じた対策が求められる中、近年はサプライチェーンに関わるインシデントが注目されており、大手企業とそのグループ会社、子会社まで一貫したセキュリティ対策が検討されてきた。また、個人を狙ったフィッシングや、組織を狙った標的型攻撃や、ランサムウェアによる被害が拡大しており、企業規模や業種を問わず対策が求められている。

情報処理推進機構が発表した「情報セキュリティ10 大脅威」によると、2021 年度は新たにテレワークを実現する Web 会議サービスやネットワークを狙った攻撃がみられた。テレワークの普及に伴い、大手・超大手企業を中心に投資が進むゼロトラストへの取り組みが継続したほか、CSIRT などの体制構築、攻撃検知や監視を行う製品・サービスの導入も進んだ。

2022 年は、サプライチェーン攻撃や内部不正による情報漏えいへの注目が高まっている。内部不正による情報漏えいは、従業員や元従業員による機密情報が不正利用された事例が報道され、重要情報の証跡を監視するニーズが高まっている。また、Emotet の感染が再拡大したことから、攻撃被害の拡大を抑えるために前年度に引き続きセキュリティ体制の構築や攻撃検知を行うツールへの関心が高い。

今後想定される IT 環境の変化としては、DX 推進、IoT の拡大、自動運転の普及、Web サービスのさらなる普及が想定される。これらの新しい領域へはサイバー攻撃が増加すると想定され、セキュリティ対策の強化が求められる。特にインシデント発生時の対処について事前に演習を行うサイバーセキュリティ演習サービスは DX や IoT など新しいシステムへの攻撃を含め重要になるとみられる。また、DX や IoT システムの基盤として普及するクラウドへのセキュリティ対策やその Web サービスの脆弱性診断などの取り組みも盛り上がりが期待される。

テレワークが定着したことで、オンプレミスやクラウド上の社内システムへのアクセス増加が見込まれ、なりすましも増加するとみられる。多要素認証などの取り組みに加え、セキュアなクラウドアクセスのための IDaaS 利用も増加が見込まれる。

攻撃の対象となるデバイスは OS やソフトウェアのバージョンが古いものや、社内ネットワークにつながっているものの、管理、利用されていない PC などが踏み台となるケースが多くなっており、端末管理ツールを導入しサイバーハイジーンとしての取り組み拡大も見込まれる。

セキュリティ人材の不足に関しては、SOC での UEBA、SOAR などの自動化ツールを活用する取り組み拡大が期待される。

〈組織における情報セキュリティ脅威の変遷〉

図表 3「情報セキュリティ 10 大脅威(「組織」向け脅威の順位)」

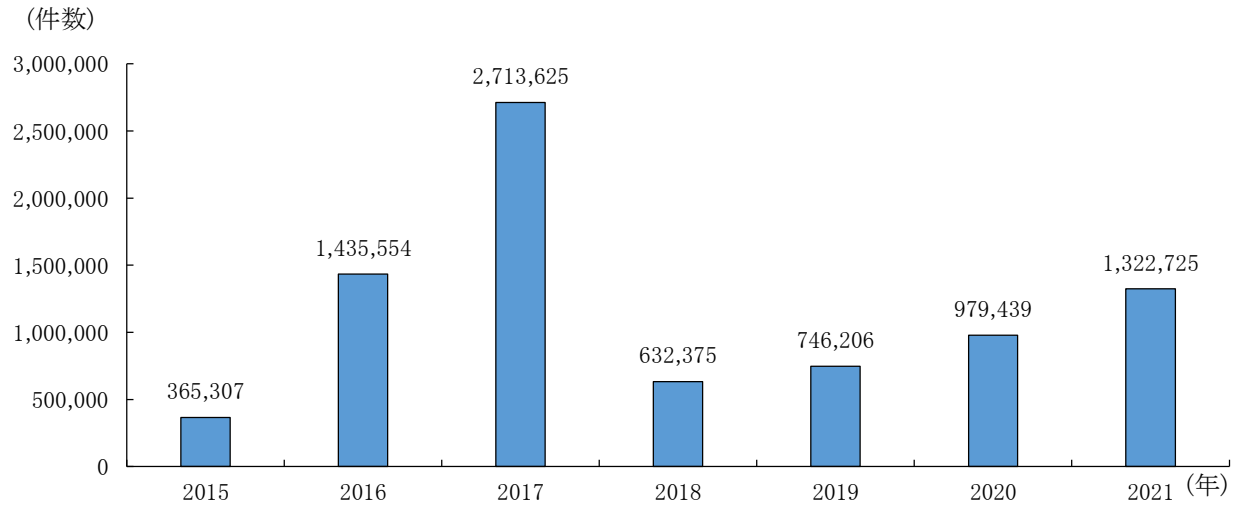
順位	2016 年	2020 年	2023 年
1	標的型攻撃による情報流出	標的型攻撃による機密情報の窃取	ランサムウェアによる被害
2	内部不正による情報漏えいとそれに伴う業務停止	内部不正による情報漏えい	サプライチェーンの弱点を悪用した攻撃
3	ウェブサービスからの個人情報の窃取	ビジネスメール詐欺による金銭被害	標的型攻撃による機密情報の窃取
4	サービス妨害攻撃によるサービスの停止	サプライチェーンの弱点を悪用した攻撃	内部不正による情報漏えい
5	ウェブサイトの改ざん	ランサムウェアによる被害	テレワーク等のニューノーマルな働き方を狙った攻撃
6	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	予期せぬ IT 基盤の障害に伴う業務停止	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
7	ランサムウェアを使った詐欺・恐喝	不注意による情報漏えい(規則は遵守)	ビジネスメール詐欺による金銭被害
8	インターネットバンキングやクレジットカード情報の不正利用	インターネット上のサービスからの個人情報の窃取	脆弱性対策情報の公開に伴う悪用増加
9	ウェブサービスへの不正ログイン	IoT 機器の不正使用	不注意による情報漏えい等の被害
10	過失による情報漏えい	サービス妨害攻撃によるサービスの停止	犯罪のビジネス化(アンダーグラウンドサービス)

出典:独立行政法人情報処理推進機構(以下 IPA)セキュリティセンター「情報セキュリティ 10 大脅威」(「組織」向け脅威の順位)

2)セキュリティ脅威の状況

(1)マルウェア感染

図表 4「IPA に報告が寄せられたコンピュータウイルスの検知数状況」



出典：IPA セキュリティセンター「コンピュータウイルス・不正アクセスの届出状況」

情報処理推進機構の「コンピュータウイルス・不正アクセスの届出状況」によると、コンピュータウイルスの検出数は前年度比約35％増加しており、メール添付ファイルや Web サイトアクセスを通じたマルウェアへの感染が問題となっている。

「情報セキュリティ 10 大脅威 2022」でも、ランサムウェアによる被害は 2021 年に引き続き社会的影響が大きくなっており、2022 年ではランキングで標的型攻撃を抜きトップとなった。国内外で端末のロックやデータの暗号化による被害が報告されており、従来のセキュリティ対策の見直しや、被害を見越した対策を促す活動を推進している。

(2)サプライチェーンリスク

図表 5「国内外におけるサプライチェーン攻撃事例」

年	企業間/社会インフラに対する攻撃事例
2021	・ 米国ネバダ州の上下水道システム(WWS)へのランサムウェア攻撃 ・ 国内光学機器メーカーの米子会社へのランサムウェア攻撃 ・ 米国メイン州の WWS へのランサムウェア攻撃 ・ 建設コンサルティング会社へのランサムウェア攻撃
2022	・ Emotet の感染再拡大 ・ 国内自動車部品メーカーへのランサムウェア攻撃

セキュリティ対策が不足している拠点を狙ったサプライチェーン攻撃への認知が深まっている。特に、2022 年 3 月に発生した自動車部品メーカーに対するランサムウェア攻撃を背景に、大手企業がグループ会社や子会社も含めてセキュリティ投資を進める動きが活発化している。

日本国内での事例は少ないものの、水道などの重要インフラを停止させて広範に影響を及ぼすサプライチェーン攻撃も発生した。IT と OT の統合が進んでいるため、従業員のリモートアクセスアカウント情報を窃取して悪用される場合や、ランサムウェアによる攻撃も行われており、セキュリティ対策の強化が求められている。米国の Cybersecurity and Infrastructure Security Agency(CISA)などを中心に OT 資産や制御システムのセキュリティ強化を進めている。

また、企業間や重要インフラへのサプライチェーン攻撃のほかに IT 機器の脆弱性を狙った攻撃も考えられ、特に IoT の普及とともにサイバー攻撃のリスク増加が見込まれる。IoT に活用される第 5 世代通信システム(5G)の導入にあたっては、サプライチェーンリスクを含むサイバーセキュリティ対策を講じることが定められており、製品の製造過程でセキュリティ上の弱点ができないように取り組まれている。IT 機器の製造過程では、意図的に情報流出を意図した不正プログラムなどを組み込むことも可能であるため、特定の国の製品調達を禁止してリスク回避する事例もみられた。

3)セキュリティビジネスにおける関連法規の状況

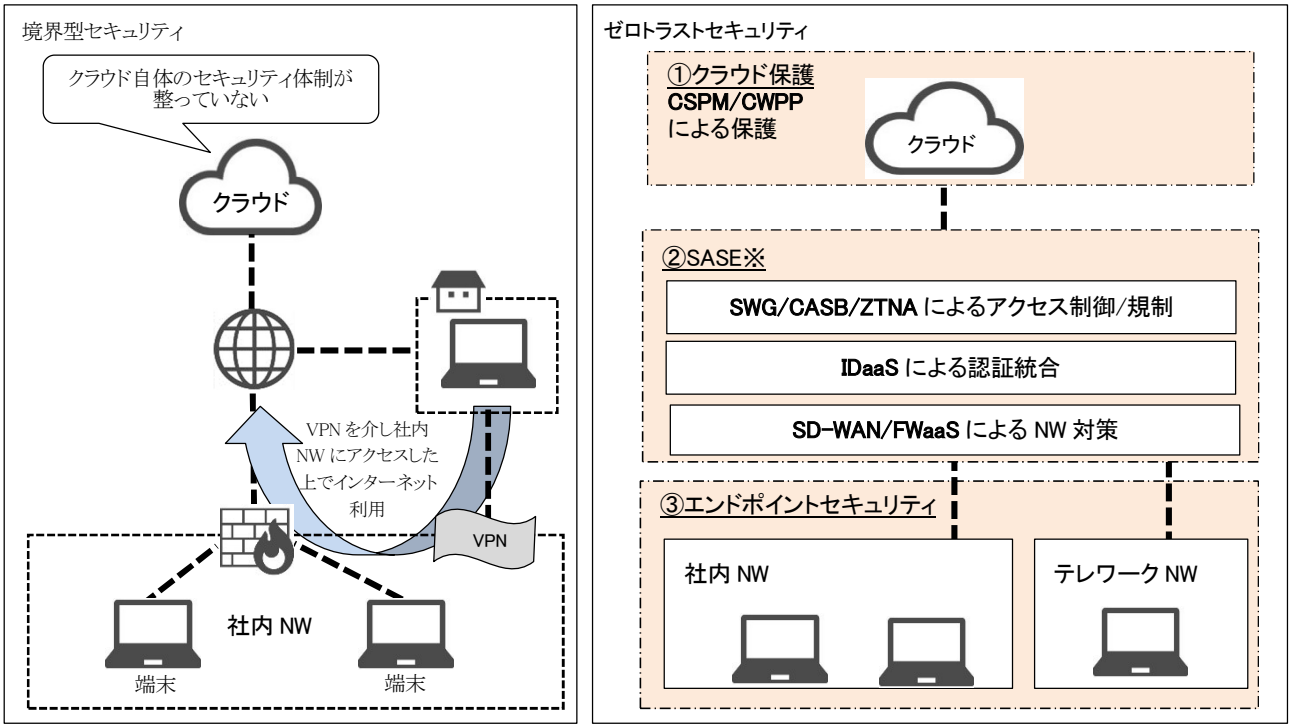
主な法令/基準/ガイドライン	概要
電子署名及び認証業務に関する法律 (2001.4 施行)	・電磁的記録の真正な成立、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑利用の確保による情報の電磁的方式による流通および情報処理の促進を行う。
クラウドサービス利用のための情報セキュリティマネジメントガイドライン (2021.9 改定)	・情報セキュリティの確保のために、クラウド利用者が自ら行うべきことと、クラウド事業者に対して求めるべきことを定めたガイドライン。 2021 年に改定された第 3 版では、クラウドサービスを取り巻く環境の変化を踏まえ、クラウドサービスにおける責任分界の在り方や、国際規格との整合性が見直された。
FISC 安全対策基準 (2022.7 第 10 版)	・金融機関などのコンピューターシステムの安全対策基準・解説書であり、第 10 版では、設備基準において、基準小項目や解説の精査や、リスクベースアプローチに関する記載の拡充、最新の金融機関におけるシステム障害事例分析や、新型コロナウイルス感染症対策の経験から得られる事業継続面の課題への対応などを反映した。
IoT セキュリティガイドライン Ver1.0 (2016.7 経済産業省・総務省)	・業種を問わず IoT の関係者がセキュリティ確保上、取り組むべき基本的な項目を示したガイドライン。
中小企業の情報セキュリティ対策ガイドライン (2019.3 第 3 版)	・経営者編、実践編からなり経営者が認識し実施すべき指針、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ものである。中小企業を対象としたクラウドサービスの充実化などを受け 2019 年 3 月に第 3 版を公開。
サイバーセキュリティ基本法 (2019.4 一部改正)	・サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、サイバーセキュリティ戦略の策定その他当該施策の基本となる事項を規定したものである。 ・2019 年 4 月に一部改正が行われ、東京 2020 オリンピック・パラリンピック開催に向け、サイバーセキュリティ対策を推進する「サイバーセキュリティ協議会」の創設などが追記された。
安全な IoT システムのためのセキュリティに関する一般枠組(2016.8 NISC)	・安全な IoT システムが具備すべき一般要求事項としてのセキュリティ要件の基本的な要素を明らかにすることを目的としたもの。
重要インフラのサイバーセキュリティに係る行動計画(2022.6 NISC)	・「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」を基本としつつ、重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、官民連携に基づく重要インフラ防護の一層の強化を図る。
改正個人情報保護法 (2022.4 施行)	・2020 年の改正では、企業がデータを利用する際に、個人が利用停止を請求する権利が盛り込まれた。また、Web サイト利用時のクッキー提供について、個人の同意が義務付けられた。 ・一方で、データの利活用を後押しするため、個人を識別できないように加工した「仮名加工情報」の一部については、本人によるデータ利用の停止請求対象から外すなどの規定が示された。
サイバーセキュリティ研究開発戦略 (2021 年 5 月改訂)	・研究開発に関わる幅広い層(政府機関から研究者まで)を対象とし、将来的なサイバーセキュリティ研究開発を検討・推進するためのビジョンを提示。最新の改訂では、我が国の研究コミュニティ状況を踏まえた推進方策や、我が国の強み・ポテンシャルと重点的な強化、研究コミュニティの継続的な取り組みが追加された。
サイバーセキュリティ戦略 (2021.9 NISC)	・サイバーセキュリティ基本法に基づき、中長期的視点から 2020 年代初めの今後 3 年間にとるべき諸施策の目標や実施方針を示すとともに、日本のサイバーセキュリティに取り組む決意をあらゆる主体、各国政府、攻撃者に対して発信するものである。
サイバーセキュリティ経営ガイドライン Ver3.0 (2023.3 経済産業省・IPA)	・Ver2.0 で定めた「経営者が認識すべき3原則」と「サイバーセキュリティ経営の重要10項目」の基本的な構成を維持しつつ、最新の状況への認識と対策の実践が可能となるような提言を行っている。
重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針 (2019.5 第 5 版)	・安全基準等の策定・改定に資することを目的として、情報セキュリティ対策において、必要度が高いと考えられる項目および先進的な取り組みとして参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して衆力したもの。

主な法令/基準/ガイドライン	概要
端末設備等規則及び電気通信主任技術者規則の一部を改正する省令 (2020.4 施行)	・ 近年、インターネットにつながる IoT 機器が乗っ取られてサイバー攻撃に悪用され、インターネットに障害を及ぼす事案が増加していることを受けて、IoT 機器の電気通信事業法認証取得に際して、セキュリティ基準要件が新たに追加された。
電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第 2 版) (2020.9 策定 総務省)	・ IoT 機器を含む端末設備の技術基準にセキュリティ対策を追加した端末設備等規則の各規定等に係る端末機器の基準認証に関する運用について明確化を図るガイドラインである。
政府情報システムのためのセキュリティ評価制度(ISMAP) (2020.6 運用開始)	・ 政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入を図ることを目的とした制度である。
政府情報システムにおけるセキュリティ・バイ・デザインガイドライン (2022.6 デジタル庁)	・ 政府情報システムの開発や運用業務に従事する関係者に対して、政府機関のシステム開発の各工程で実施すべきセキュリティ・バイ・デザインとしての実施内容、要求事項を示すことを主目的としている。

3.1.3.セキュリティ市場を取り巻く注目キーワード分析

1)ゼロトラストセキュリティの動向

図表 5「ゼロトラストセキュリティの概念」



従来主流であった境界型セキュリティは、社内ネットワークと社外ネットワークの境界線上にセキュリティ対策を施すものである。昨今、内部からの情報漏洩の多発や、クラウドサービスの利用拡大に加え、2020 年頃より COVID-19 感染症拡大の影響によるテレワークが進展してきたことで、従来の境界型セキュリティでは防ぎきれないセキュリティリスクが拡大し、境界型セキュリティからゼロトラストセキュリティへの移行を進める企業が増加している。

ゼロトラストの概念は、2010 年に米 Forrester Research によって提唱されたもので、企業の情報資産や IT 資産にアクセスするものは全て信用せず検証を行うことで、サイバー攻撃の防御を行う考えである。

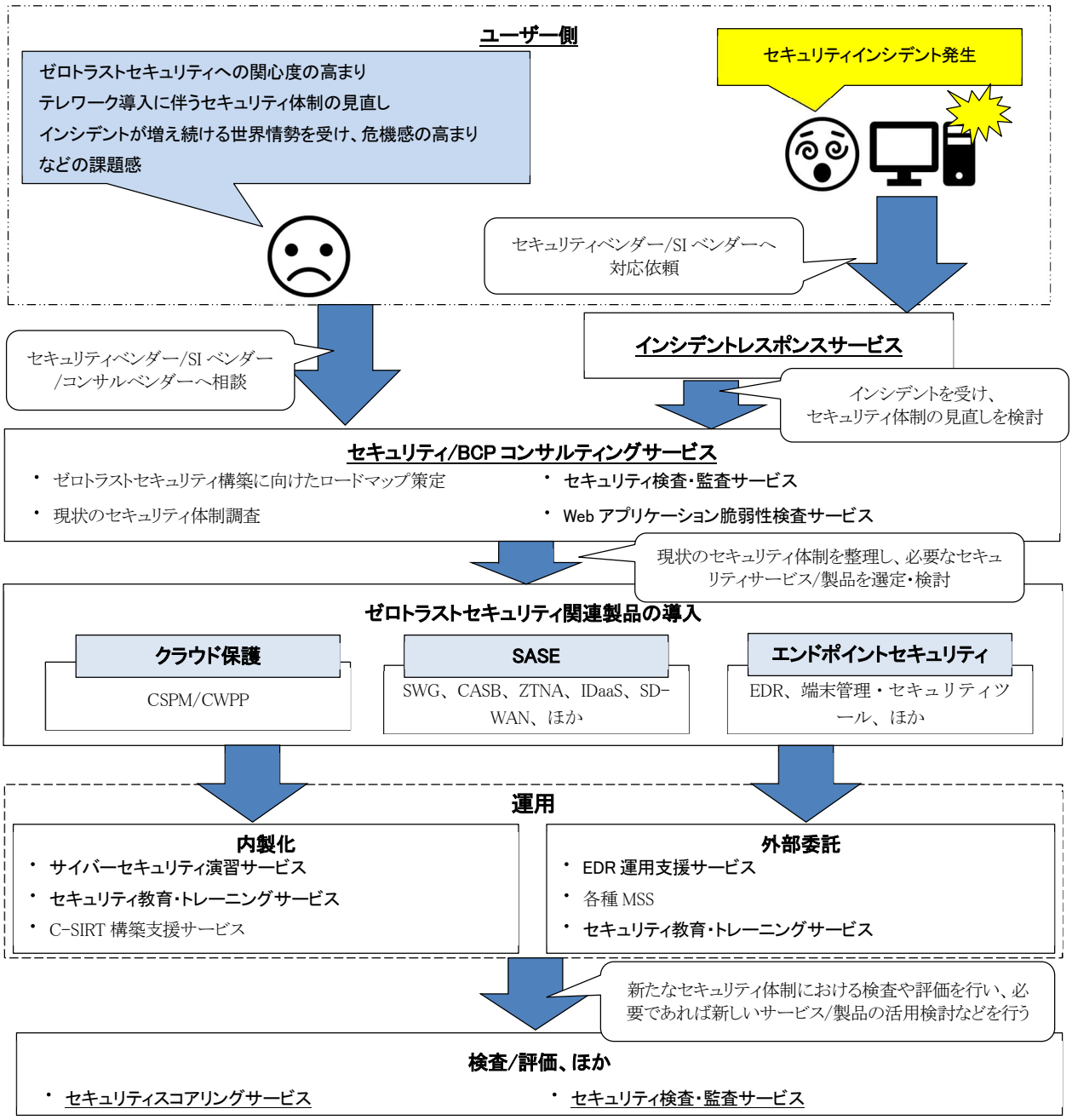
ゼロトラストセキュリティでは、上掲右図に記載した①クラウド保護、②SASE、③エンドポイントセキュリティといった製品が中核となっている。各製品の市場動向を下図にまとめた。

図表 6「各ゼロトラストセキュリティ製品の市場概況」

カテゴリー	対象ツール	市場規模(百万円)		CAGR (27/21) (%)	概要
		2021 年度 (実績)	2027 年度 (予測)		
クラウド保護	2-12.CSPM/CWPP	900	4,000	28.2	・ 市場立ち上げ期となっており、一部企業の利用にとどまっている。今後、DX の基盤技術として IaaS/PaaS の活用が進むことで、CSPM/CWPP を利用して管理を行うニーズが高まっており、市場は拡大傾向で推移すると予測される。
SASE	2-8.CASB 2-9.IDaaS 2-10.Web セキュリティツール 2-11.Web フィルタリングツール	37,600	113,900	20.3	・ CASB、ZTNA、SWG といったさまざまな SASE 製品を組み合わせた形での導入が進んでおり、高い成長率で推移している。
エンドポイントセキュリティ	2-23.EDR 2-25.端末管理・セキュリティツール	49,420	97,860	12.1	・ 2021 年度時点で主要ユーザーである超大手・大手企業への導入が進展しており、運用フェーズに入っているとみられ、MDR についてもニーズが高まっている。今後において、中堅企業への導入も徐々に進展していることから、継続して成長していく市場であるとみられる。

(富士キメラ総研推定)

図表 7「ゼロトラストを構成する製品/サービス」



ゼロトラストセキュリティの構築において、各種プロダクトの導入のみにとどまらず、プロダクト導入前後においてさまざまなサービスが介入している。

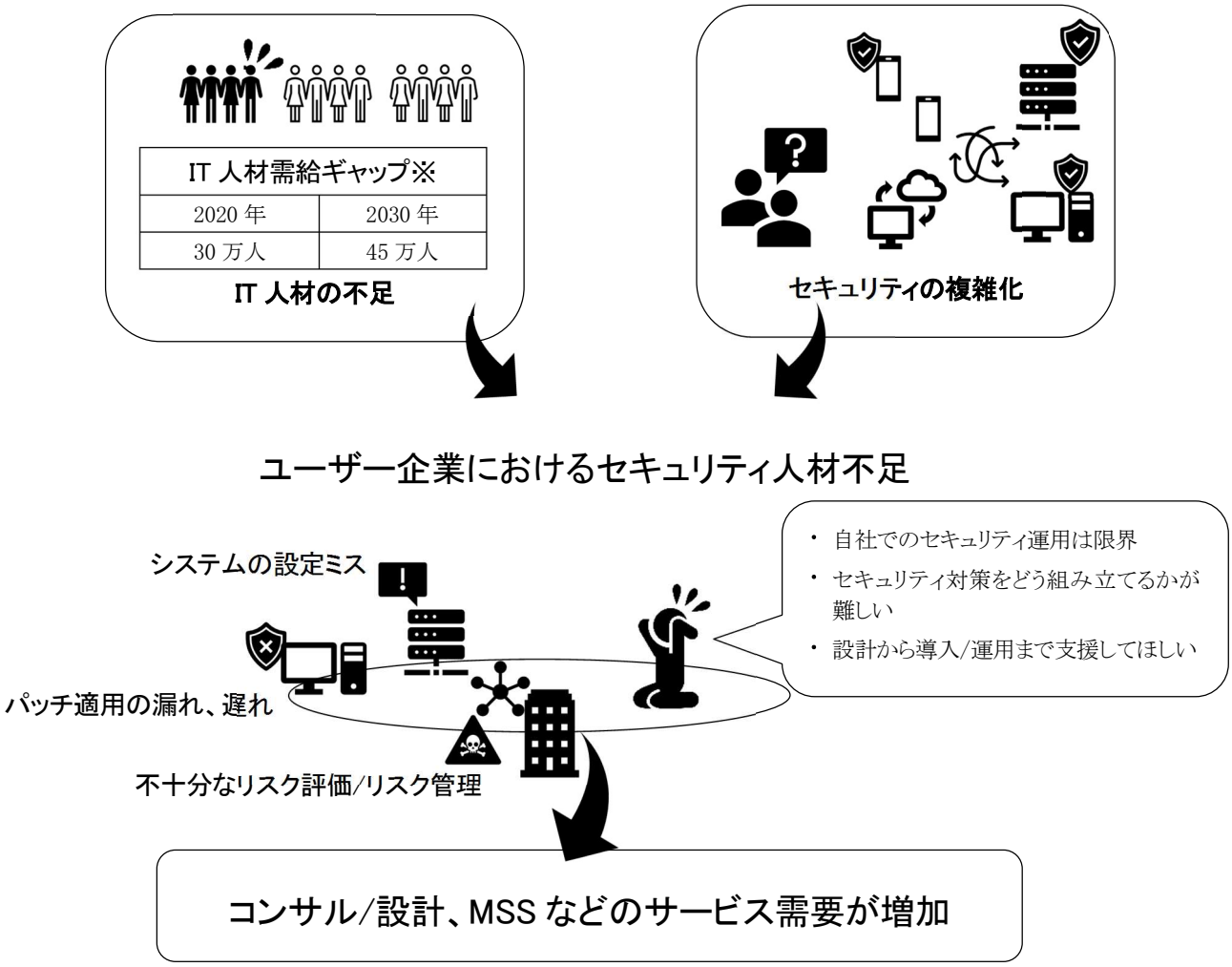
ゼロトラストセキュリティを構築する入口として、ユーザーが自発的にセキュリティ体制の見直しやゼロトラストセキュリティ構築へのニーズを持ち、セキュリティベンダーや SI ベンダー、コンサルティングベンダーに相談するケースと、ユーザーの IT 環境にインシデントが発生し、SI ベンダーやセキュリティベンダーによるインシデントレスポンスサービスを受けたのち、インシデントを踏まえた新たなセキュリティ体制の構築を検討するケースに大別される。

コンサルティングサービスにおいて現状のセキュリティ体制の調査/検査を行い、ロードマップ策定などを経て、各ゼロトラストセキュリティ関連製品の検討・導入を行う。製品運用の際、自社で内製化する場合には社員向け/IT 担当者向けの教育サービスや C-SIRT 構築支援サービス、SI ベンダーやセキュリティベンダーなどの SOC に運用を委託する場合は各 MSS が利用される。MSS では、現状 EDR 運用支援サービスが中心となっており、その他 SASE 製品においてもマネージドサービスが必要とされているものの、国内ユーザーにおいてはまだ利用が進展していないとみられる。

運用フェーズにおいて、稼働状況の確認/評価/検査に向けたセキュリティスコアリングサービスやセキュリティ検査・監査サービスが利用される。確認/評価/検査ののち、さらに見直しが必要な場合は、コンサルティングサービスから再度行われ、サイクル的に進められる。

2)ユーザー企業におけるセキュリティ人材不足の影響

図表 8「人材不足の影響」



※経済産業省「IT 人材需給に関する調査」より作成

セキュリティ人材が不足する背景には、①国内企業における慢性的な IT 人材不足と、②サイバー攻撃の高度化とその対策高度化が挙げられる。

2019 年に経済産業省が行った「IT 人材需給に関する調査」の試算によれば、2020 年の国内 IT 人材の供給は需要に対して約 30 万人不足しており、2030 年には 45 万人の不足に拡大する見込みである。セキュリティ人材についても例外ではなく、多くの企業でセキュリティ担当者はほかの業務との兼任を行っており、特に中小企業においては情報セキュリティ担当者がまったくいないケースも多いものとみられる。

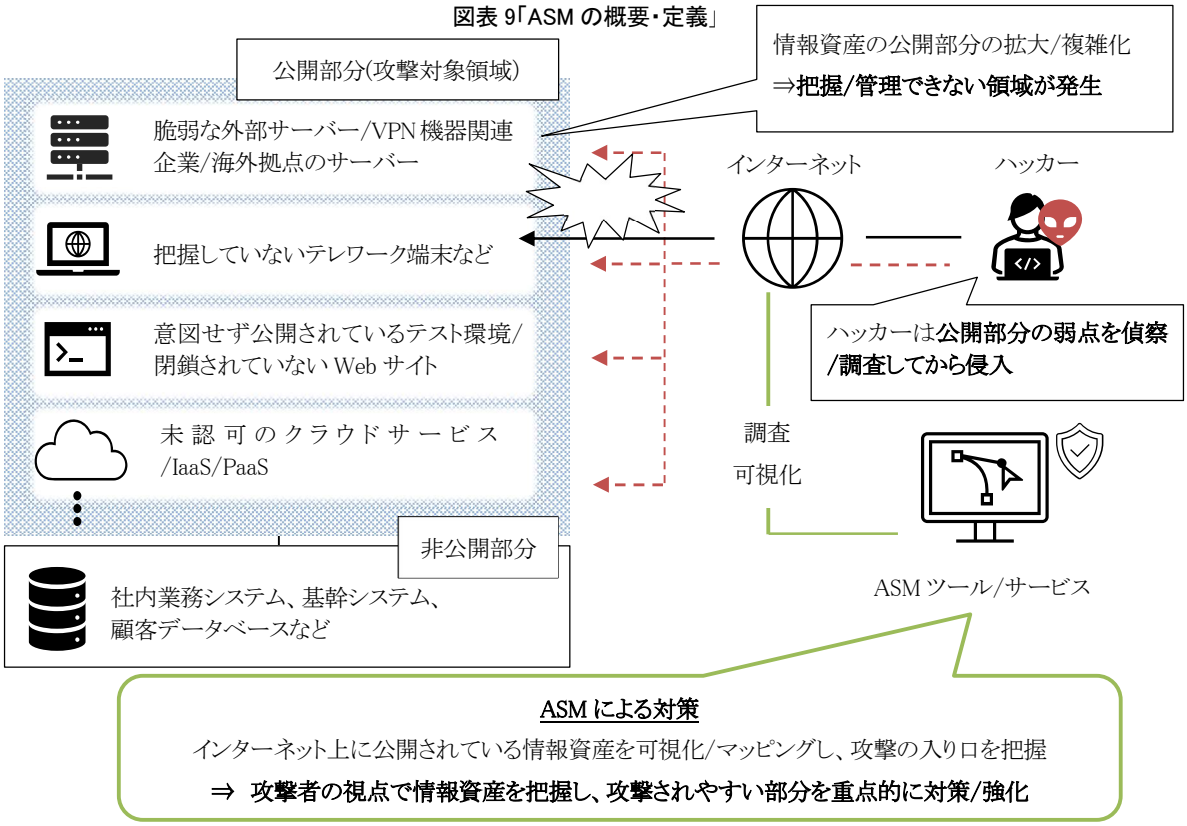
また、近年のサイバー攻撃の高度化に加えて、システムのクラウド化/企業ネットワークの複雑化を背景として、ネットワークセキュリティ製品/サービスの導入、活用はますます煩雑化しており、セキュリティ運用には非常に高いレベルの知識/技能が求められるようになっている。これまで MSS を提供してきた SI ベンダーに加えて、セキュリティツールベンダーにおいても自社製品の運用を行う MSS を提供するケースが増加しており、国内の人材不足を補う手段として各種セキュリティサービス市場は今後さらなる拡大が見込まれる。

DX の推進による新たな動きもみられ、企業の DX 推進とともに、そのセキュリティ対策需要が高まっているが、DX 関連に関しては一般的なセキュリティ対策だけではなく、社内業務フローを理解した上で DX システムとセキュリティ双方に対処する必要があり、外部のセキュリティサービスを活用するのではなく、自社でセキュリティ対策を行うためのセキュリティ人材の雇用が進んでおり、国内全体でのセキュリティ人材不足が深刻化している。

3)ASM の動向

〈ASM の概要・定義〉

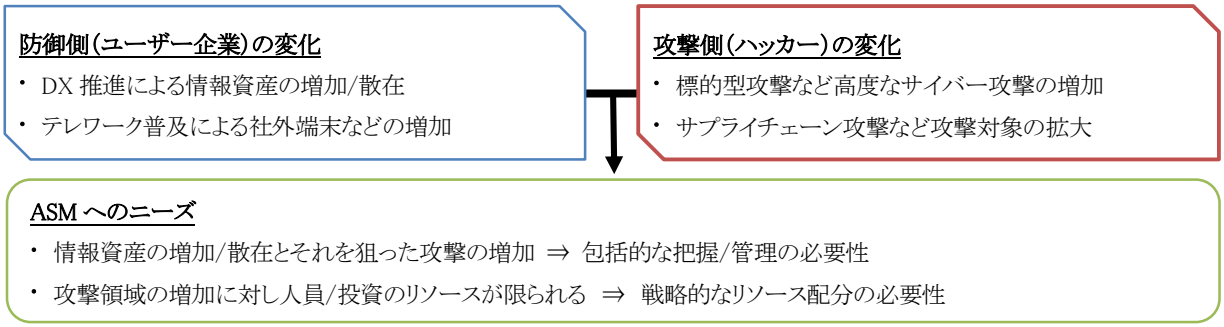
図表 9「ASM の概要・定義」



ASM(Attack Surface Management:攻撃対象領域管理)とは、企業がインターネットに公開している情報資産を把握/管理することで、攻撃を受けうる領域(攻撃対象領域)を可能な限り減らすセキュリティ対策の概念である。ASM を行うことにより、攻撃者の視点から自社の情報資産を把握/管理し、シャドーIT などセキュリティ対策が行われていない領域の発見や、想定されるサイバー攻撃のシナリオの把握が可能となる。

2021 年度頃より、主要ベンダーが ASM を支援/実現する製品/サービスの提供を開始しており、今後市場として一定の規模を確立することが期待されるため、注目キーワードとして取り上げた。

〈ASM への注目の背景〉



ASM への注目度が高まっている背景として、防御側(ユーザー企業)の変化と、攻撃側(ハッカー)の変化の二つがある。

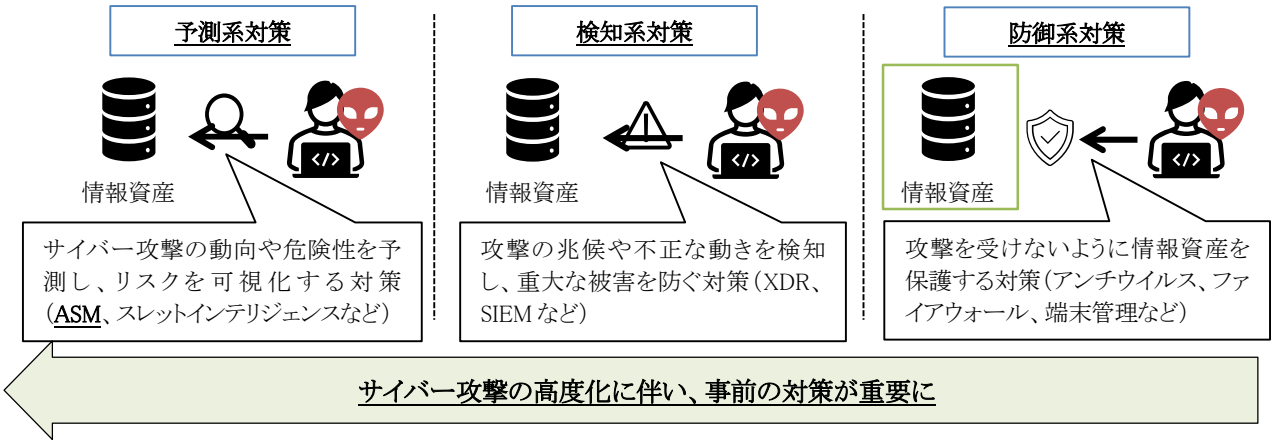
防御側の変化としては、企業が持つインターネット上の情報資産が急速に拡大していることが挙げられる。具体的には、DX 推進により、クラウドサービスの利用やデータ利活用、顧客向けの Web サービスが増加し、情報資産がインターネット上に増加/散在するようになったことが挙げられる。加えて、コロナ禍を契機とするテレワークの普及により、社外の端末/アクセスポイントが増加したことも挙げられる。

攻撃側の変化としては、ゼロデイ攻撃や標的型攻撃などの高度なサイバー攻撃が増加したことや、サプライチェーン攻撃など企業が把握できていない部分を入口とした攻撃が増加し、攻撃の対象領域が増加したことが挙げられる。

上記の二つの変化を背景に、今後は公開されている情報資産を包括的に把握/管理する必要性が高まることから、本製品/サービスへのニーズが高まるとみられる。加えて、本製品/サービスによりリスクの高い情報資産を特定し、セキュリティ対策への人員や投資リソース配分の効率化を実現することが期待されている。

〈ASM ツール/サービスと関連セキュリティ製品/サービスの動向〉

図表 9「ASM ツール/サービスと関連セキュリティ製品/サービスとの比較・分類/関係性」



上図では、関連するセキュリティ製品/サービスを「予測系対策」「検知系対策」「防御系対策」の三つに分類し、比較および関係性を表した。ASM ツール・サービスは Web 上に公開されている情報資産を把握し、攻撃されやすい部分を把握するという意味で「予測系対策」に分類される。

サイバー攻撃の高度化に伴い、従来の検知系/防御系対策や加えて、攻撃の手法や攻撃の入り口を予測・把握し事前的な対策を講じる必要性が高まっている。「予測系対策」により把握したリスクに応じて、検知系/防御系対策の強化を行うことが今後必要になるとみられる。

図表 10「ASM ツール/サービスと関連セキュリティ製品/サービスの市場動向」

サービス、製品名		市場規模（百万円、%）			期待される ASM との連携、関係性
		2021 年度（実績）	2027 年度（予測）	CAGR（21/27）	
ASM		△	3,000	—	—
関連セキュリティ製品/ツール	スレットインテリジェンスサービス	3,300	8,200	16.4	・攻撃者視点でのセキュリティ対策という点で共通点があり、ASM と連携することでより具体的にリスクを把握することが可能となる。
	CSPM/CWPP	900	4,000	28.2	・ASM によって未承認あるいは管理対象外の IaaS/PaaS を検出し、本製品によって管理/保護を行うことで、クラウド領域のセキュリティ対策が効率化される。
	プラットフォーム検査ツール	2,910	5,500	11.2	・ASM により発見された未管理の情報資産について、本ツールでその脆弱性を検査することで診断/管理を一元化することが可能となる。本ツールに ASM の機能が搭載された製品も一部みられる。
	XDR	800	3,900	30.2	・本ツールと ASM との連携により脅威の検知/対応の対象範囲外の領域を削減することが可能となる。
	SIEM	13,500	17,550	4.5	・XDR 同様に、ASM と連携することでログの収集/分析や異常検知の対象外の領域を発見/削減することが可能となる。
	Web アプリケーション脆弱性検査ツール	2,600	6,600	16.8	・ASM によって未承認/管理対象外の Web アプリケーションを検出し、本製品によって脆弱性の検査/診断を行うことで、Web 領域のセキュリティ対策が効率化される。
合計		24,010	48,750	12.5	—

（富士キメラ総研推定）

ASM ツール/サービスは企業の情報資産を監視/検知、可視化するツールであることから、主に ASM ツールで検知した未管理の資産について、関連ツール/製品が診断や異常検知、対策を行うという形で連携するケースが多い。一部ベンダーでは ASM を含む上記の製品/サービスをモジュールとして複数含めたセキュリティプラットフォームとして連携/提供を行っている。

上記製品/サービス群の市場規模については、いずれも 2027 年度に向けて好調な市場拡大が予測されている。連携関係にある ASM ツール/サービスについても、現在の実績は少ないものの、関連ツール/サービスの成長にけん引される形で市場規模が拡大し、2027 年度には約 30 億円の市場規模となることが予測される。

〈主要参入ベンダーの動向〉

ベンダー名	概要
サイファーマ	・ 同社のスレットインテリジェンスサービスの「DeCYFIR」および「DeTCT」にて ASM 機能を含んだサービスとして提供をしている。 ・ 特に、2021 年から提供を開始した「DeTCT」においては、ASM 機能によるリスク可視化をユーザーに訴求している。
ダークトレース・ジャパン	・ 2022 年 3 月に ASM ツールを提供するオランダの Cybersprint を買収し、2022 年 7 月に ASM ツール「Darktrace PREVENT/ASM」の国内提供開始を発表した。 ・ 同社の XDR ソリューション「Darktrace DETECT / RESPOND」と連携し、サイバー攻撃の予防から検知、回復を自律的に一貫して行う「サイバーAI ループ」の確立を目指している。
テナブル・ネットワーク・セキュリティ・ジャパン	・ 2022 年 6 月に ASM を提供していた Bit Discovery を買収し、ASM ツール「Tenable.asm」の提供開始を発表した。 ・ 従来提供している脆弱性管理ソリューション「Tenable.io」「Tenable.sc」などのシリーズと連携し提供を行っている。
日本マイクロソフト	・ 2021 年 7 月に買収した RiskIQ の技術を統合し、2022 年 8 月に「Defender External Attack Surface Management」を発表した。 ・ 同時にスレットインテリジェンス製品「Defender Threat Intelligence」も発表している。
パロアルトネットワークス	・ 2020 年 11 月に ASM を提供していた Expanse を買収し、2021 年度より ASM ツール「Cortex Xpanse」の提供を開始した。 ・ 従来提供している「Cortex」シリーズの他製品や、「Prisma」シリーズとも連携し提供を行っている。
日立ソリューションズ	・ 2020 年 11 月に CyCognito と国内初の販売代理店契約を締結し、同社製品を利用した ASM サービスを提供開始した。製品の販売のみならず、自社導入から保守サポートまで提供を行っている。

外資系ベンダーが ASM の専門ベンダーを買収し、自社製品ラインアップに追加する形で国内での提供を開始するケースが多い。上表のほかに、フォーティネットジャパンやマンディアント、ラピッドセブン・ジャパンも ASM ツール/サービスの提供を行っている。

これに加え、国内の SI ベンダー、セキュリティ専門ベンダーなどが外資系ベンダーのツールを利用し、ASM サービスを提供するケースが散見される。上記のほかに、現在はマクニカ、ユービーセキュア、ラックなどが ASM サービスを提供している。

3.1.4.セキュリティサービス/ツールのポジション分析

1)注目セキュリティ分析

図表 11「サービス市場における平均成長率ランキング」

単位:百万円、%

項番	品目名	2021年度 実績	2027年度 予測	CAGR (27/21)	RANK
1-16	セキュリティスコアリングサービス	2,100	8,300	25.7	1
1-18	スレットインテリジェンスサービス	3,300	8,200	16.4	2
1-10	EDR運用支援サービス	2,500	6,100	16.0	3
1-9-3	電子認証サービス(その他)	800	1,800	14.5	4
1-8	モバイルアプリ検査サービス	2,400	4,800	12.2	5
1-9-4	プライベートCAアウトソーシングサービス	4,500	8,500	11.2	6
1-12	サイバーセキュリティ演習サービス	3,000	5,100	9.2	7
1-5	DDoS攻撃対策サービス	9,700	16,100	8.8	8
1-9-2	電子認証サービス(クライアント証明書)	4,600	7,500	8.5	9
1-7	Webアプリケーション脆弱性検査サービス	15,600	24,000	7.4	10
1-17	インシデントレスポンスサービス	2,000	3,000	7.0	11
1-13	セキュリティ/BCPコンサルティングサービス	25,500	37,500	6.6	12
1-15	セキュリティ検査・監査サービス	6,500	9,400	6.3	13
1-6	WAF運用管理サービス	4,000	5,600	5.8	14
1-4	メールセキュリティサービス	8,000	11,000	5.5	15
1-14	セキュリティ教育・トレーニングサービス	16,000	21,200	4.8	16
1-11	SIEM運用管理サービス	1,600	1,950	3.4	17
1-9-1	電子認証サービス(SSL/TLSサーバー証明書)	7,000	7,600	1.4	18
1-1	ウイルス監視サービス	28,000	30,300	1.3	19
1-2	統合セキュリティ監視サービス	40,100	42,900	1.1	20
1-3	不正アクセス監視サービス	19,900	19,600	-0.3	21

(富士キメラ総研推定)

ネットワークセキュリティサービス市場における各市場の成長率を比較し、上表にまとめた。

サービス市場において、「1-16 セキュリティスコアリングサービス」「1-18 スレットインテリジェンスサービス」「1-10 EDR 運用支援サービス」が高い成長率となる 3 市場となっている。

「1-16 セキュリティスコアリングサービス」は、主に製造業のようなサプライチェーンを有するユーザーを中心に認知度が高まり、導入が進んでいる。今後においても、引き続き自社と取引先のセキュリティ対策状況の現状を把握する目的での利用が進展し、市場が拡大していくと予測される。

「1-18 スレットインテリジェンスサービス」は、ランサムウェアによるサイバー攻撃/被害の増加傾向が引き続いていることや、国際的なサイバー攻撃活動の活発化を背景として、重大なセキュリティインシデントを未然に防ぎたいというニーズによる市場拡大が期待されるものの、サービス費用が高額であることや、ユーザー社内のセキュリティ人材が必須であることからユーザーは超大手/大手企業および一部中堅企業に限られる。

「1-10 EDR 運用支援サービス」は、EDR 製品を利用するユーザーの拡大により、併せてマネージドサービスを導入/検討するユーザーも増加していることで、好調な市場拡大が期待される。

〈製品市場〉

図表 12「製品市場における平均成長率ランキング(2021 年度市場規模 100 億円以上)」

単位:百万円、%

項番	品目名	2021年度 実績	2027年度 予測	CAGR (27/21)	RANK
2-10	Webセキュリティツール	13,400	67,400	30.9	1
2-23	EDR	15,000	51,000	22.6	2
2-24	MDM・EMMツール	12,850	20,600	8.2	3
2-25-1	端末管理・セキュリティツール(統合エンドポイント管理ツール)	30,200	42,800	6.0	4
2-11	Webフィルタリングツール	11,700	16,000	5.4	5
2-22	DaaS	38,500	52,200	5.2	6
2-27-2	統合ログ管理ツール(SIEM)	13,500	17,550	4.5	7
2-4-1	FW/VPN/UTM関連製品(FW/VPNアプライアンス/UTM)	52,200	63,700	3.4	8
2-1-1	ウイルス対策ツール(サーバー/クライアント)	35,900	42,400	2.8	9
2-2	セキュリティ監視ツール	11,000	12,300	1.9	10
2-3-2	標的型攻撃対策ツール(ゲートウェイ)	13,600	11,100	-3.3	11

(富士キメラ総研推定)

本カテゴリーのうち、成長率が高い市場として「2-10 Web セキュリティツール」「2-23 EDR」「2-24 MDM・EMM ツール」が挙げられる。

3 品目ともに、企業におけるテレワークの増加による各端末におけるセキュリティ対策強化の目的や、クラウドサービス利用増加に伴う Web アクセスセキュリティ対策として導入が進展している。

図表 13「製品市場における平均成長率ランキング(2021 年度市場規模 40 億円以上 100 億円未満)」

単位:百万円、%

項番	品目名	2021年度 実績	2027年度 予測	CAGR (27/21)	RANK
2-9	IDaaS	7,800	21,000	17.9	1
2-29	NDR	6,800	18,100	17.7	2
2-8	CASB	4,700	9,500	12.4	3
2-14	WAF	8,800	14,400	8.6	4
2-19	特権ID管理ツール	7,550	11,400	7.1	5
2-13	DDoS攻撃対策ツール	4,250	6,150	6.4	6
2-17	デバイス認証ツール	5,700	7,700	5.1	7
2-20-2	認証デバイス(静脈認証)	5,950	7,800	4.6	8
2-21	ワンタイムパスワード	4,700	6,100	4.4	9
2-16	シングルサインオン	5,100	6,600	4.4	10
2-30-2	検疫ツール(PC検疫ツール)	5,900	7,250	3.5	11
2-18	統合ID管理ツール	4,100	4,800	2.7	12
2-4-2	FW/VPN/UTM関連製品(SSL-VPNアプライアンス)	7,600	8,800	2.5	13
2-7	メールフィルタリングツール	8,400	9,200	1.5	14
2-1-2	ウイルス対策ツール(ゲートウェイ)	7,400	5,700	-4.3	15

(富士キメラ総研推定)

本カテゴリーのうち、成長率が高い市場として「2-9 IDaaS」「2-29 NDR」「2-8 CASB」が挙げられる。

「2-9 IDaaS」「2-8 CASB」においては、ユーザーにおけるクラウドサービスの利用拡大に伴う、認証および ID 管理、アクセス制御/管理の目的での導入に加え、ゼロトラストセキュリティの観点での導入が進んでいる。両製品ともにゼロトラストセキュリティモデルにおける SASE ソリューションとして位置付けられており、今後においてもゼロトラストセキュリティモデルをフックとした導入が進んでいくと推定される。

「2-29 NDR」においては、既に EDR を活用しているユーザーにおいて、エンドポイントだけでなくネットワーク領域の脅威検知・分析も行いたいといったニーズから導入が進んでいるとみられる。

図表 14「製品市場における平均成長率ランキング(2021 年度市場規模 40 億円未満)」

単位:百万円、%

項番	品目名	2021年度 実績	2027年度 予測	CAGR (27/21)	RANK
2-26	XDR	800	3,900	30.2	1
2-12	CSPM/CWPP	900	4,000	28.2	2
2-15	Webアプリケーション脆弱性検査ツール	2,600	6,600	16.8	3
2-28	プラットフォーム検査ツール	2,910	5,500	11.2	4
2-3-1	標的型攻撃対策ツール(エンドポイント)	3,200	4,200	4.6	5
2-30-1	検疫ツール(不正接続防止ツール)	3,450	4,440	4.3	6
2-6	メール暗号化/メール誤送信対策ツール	3,450	4,300	3.7	7
2-5	電子メールアーカイブツール	3,150	3,750	2.9	8
2-27-1	統合ログ管理ツール(SIM)	2,850	3,300	2.5	9
2-25-2	端末管理・セキュリティツール(端末ログ管理ツール)	1,420	1,510	1.0	10
2-20-1	認証デバイス(指紋認証)	700	650	-1.2	11
2-25-3	端末管理・セキュリティツール(持ち出し制御ツール)	2,800	2,550	-1.5	12

(富士キメラ総研推定)

本カテゴリーのうち、成長率が高い市場として「2-26 XDR」「2-12 CSPM/CWPP」「2-15 Web アプリケーション脆弱性検査ツール」が挙げられる。

「2-26 XDR」は、近年さまざまなセキュリティベンダーが参入し、ユーザーへの訴求に取り組んでいる。

「2-12 CSPM/CWPP」は、ゼロトラストセキュリティモデルにおける「クラウド保護」を担うソリューションとなっており、高い市場成長率で推移しているとみられる。

「2-15 Web アプリケーション脆弱性検査ツール」は、国内外問わず Web アプリケーションを活用したビジネスはいずれの企業においても必須となっていることから、堅調な市場拡大が見込まれる。

3.2.業種別/規模別動向

1)規模別動向

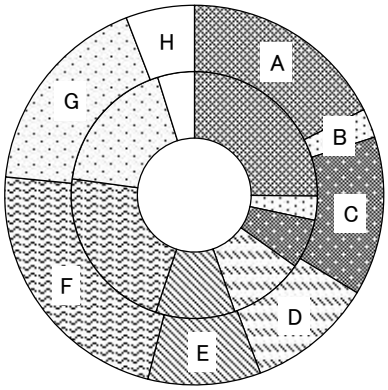
図表 15「規模別動向」

＜超大手＞

単位：百万円、％

領域	年度	2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	57,300	25.1	59,350	17.6
B	メールセキュリティ	7,200	3.2	8,350	2.5
C	クラウド/Webアクセスセキュリティ	14,800	6.5	45,700	13.5
D	Webセキュリティ	22,600	9.9	36,300	10.8
E	認証セキュリティ	23,700	10.4	32,480	9.6
F	端末セキュリティ	50,220	22.0	76,210	22.6
G	サイバーレジリエンス/教育	41,300	18.1	59,500	17.6
H	その他セキュリティ	10,950	4.8	19,700	5.8
合計		228,070	100.0	337,590	100.0

（富士キメラ総研推定）



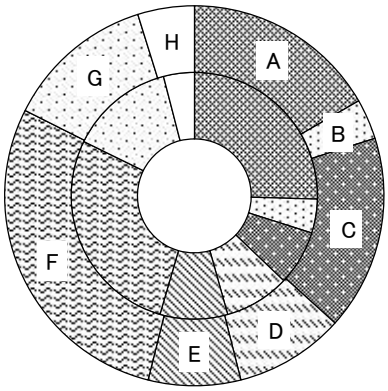
内円：2021年度
外円：2027年度

＜大手＞

単位：百万円、％

領域	年度	2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	45,600	25.4	47,350	16.7
B	メールセキュリティ	8,000	4.5	9,700	3.4
C	クラウド/Webアクセスセキュリティ	12,900	7.2	47,100	16.6
D	Webセキュリティ	15,350	8.6	26,600	9.4
E	認証セキュリティ	15,900	8.9	22,390	7.9
F	端末セキュリティ	49,790	27.8	80,900	28.5
G	サイバーレジリエンス/教育	24,610	13.7	36,200	12.7
H	その他セキュリティ	7,250	4.0	13,700	4.8
合計		179,400	100.0	283,940	100.0

（富士キメラ総研推定）



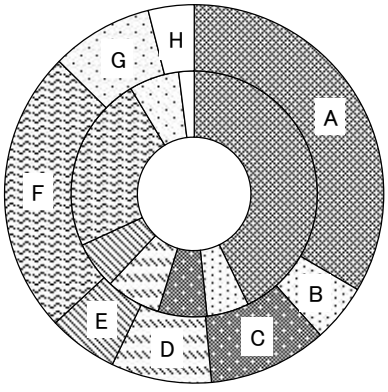
内円：2021年度
外円：2027年度

＜中堅＞

単位：百万円、％

領域	年度	2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	47,550	42.8	53,750	33.4
B	メールセキュリティ	6,150	5.5	7,950	4.9
C	クラウド/Webアクセスセキュリティ	7,150	6.4	16,300	10.1
D	Webセキュリティ	8,000	7.2	13,750	8.6
E	認証セキュリティ	6,900	6.2	9,610	6.0
F	端末セキュリティ	25,850	23.3	39,040	24.3
G	サイバーレジリエンス/教育	7,300	6.6	14,050	8.7
H	その他セキュリティ	2,250	2.0	6,250	3.9
合計		111,150	100.0	160,700	100.0

（富士キメラ総研推定）



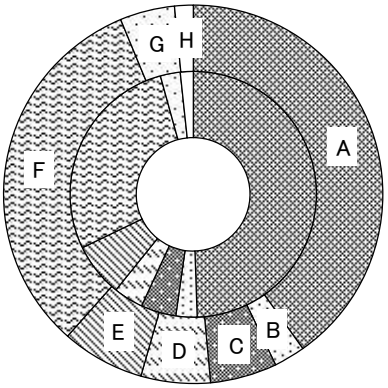
内円：2021年度
外円：2027年度

＜中小＞

単位：百万円、％

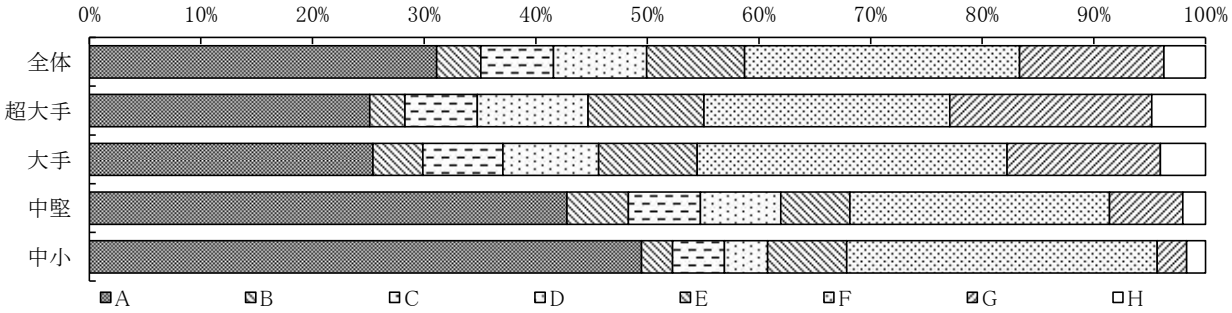
領域＼年度		2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	29,350	49.5	33,950	40.2
B	メールセキュリティ	1,650	2.8	2,250	2.7
C	クラウド/Webアクセスセキュリティ	2,750	4.6	4,800	5.7
D	Webセキュリティ	2,300	3.9	5,000	5.9
E	認証セキュリティ	4,200	7.1	5,970	7.1
F	端末セキュリティ	16,510	27.8	27,210	32.2
G	サイバーレジリエンス/教育	1,550	2.6	3,950	4.7
H	その他セキュリティ	1,000	1.7	1,340	1.6
合計		59,310	100.0	84,470	100.0

（富士キメラ総研推定）

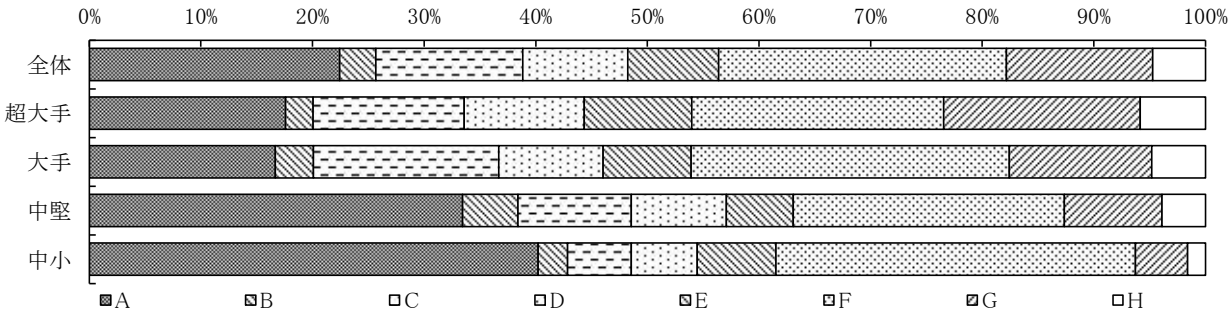


内円：2021年度
外円：2027年度

＜2021 年度における規模別セキュリティ投資領域比較＞



＜2027 年度における規模別セキュリティ投資領域比較＞



記号	カテゴリー	記号	カテゴリー
A	ゲートウェイセキュリティ	E	認証セキュリティ
B	メールセキュリティ	F	端末セキュリティ
C	クラウド/Web アクセスセキュリティ	G	サイバーレジリエンス/教育
D	Web セキュリティ	H	その他セキュリティ

超大手/大手企業においては、ゲートウェイセキュリティ、端末セキュリティに続き、サイバーレジリエンス/教育セキュリティの導入が進展している。ゼロトラストセキュリティの推進に伴い、セキュリティコンサルティングサービス、セキュリティ検査・検査サービスなどのサービスのほか、直近ではその他セキュリティに含まれる XDR といった新しいセキュリティの導入も先行して取り入れるユーザーが多いとみられる。

中堅企業・中小企業においては、ゲートウェイセキュリティに次いで、端末セキュリティの市場規模が大きい。COVID-19 感染拡大の影響によるテレワーク増加に伴い、持ち出し端末に対するセキュリティ対策が進展しているとみられる。

超大手/大手企業では、ゲートウェイセキュリティを中心とした境界型防御から、ゼロトラストをベースとした非境界型防御へとシフトしており、2027 年度に向けてゲートウェイセキュリティの構成比が 20%以下と縮小し、ゼロトラスト関連のクラウド/Web アクセスセキュリティへの投資比率が大きくなるとみられる。それ以外のカテゴリーに関しては大きな構成比の変化はみられない。

一方、中堅/中小企業では一部で大手企業と同じようにゼロトラストへの取り組みを強化する企業がみられるが、全体的な傾向としては従来型の境界型防御のままセキュリティ投資を行うとみられる。このため、すでに UTM など投資を積極的に行ってきたゲートウェイセキュリティ以外のセキュリティに新しい投資が向かうことで、ゲートウェイセキュリティの投資が減少するものの、減少した構成比はさまざまなカテゴリーに分散するため、それぞれ構成比が上昇している。

2)業種別動向

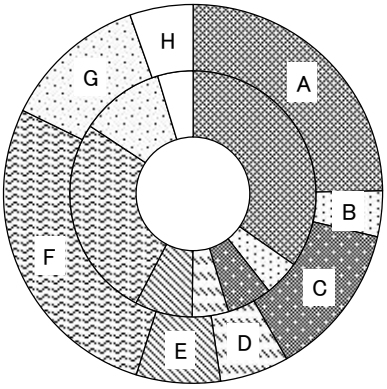
図表 16「業種別動向」

＜製造＞

単位：百万円、％

領域＼年度		2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	46,600	34.7	49,100	24.7
B	メールセキュリティ	6,300	4.7	7,700	3.9
C	クラウド/Webアクセスセキュリティ	7,900	5.9	26,100	13.2
D	Webセキュリティ	6,400	4.8	11,650	5.9
E	認証セキュリティ	10,190	7.6	14,250	7.2
F	端末セキュリティ	35,660	26.6	54,400	27.4
G	サイバーレジリエンス/教育	14,900	11.1	24,500	12.3
H	その他セキュリティ	6,200	4.6	10,700	5.4
合計		134,150	100.0	198,400	100.0

（富士キメラ総研推定）



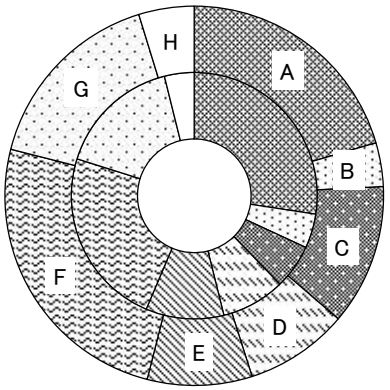
内円：2021年度
外円：2027年度

＜金融＞

単位：百万円、％

領域＼年度		2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	33,700	27.4	36,200	20.5
B	メールセキュリティ	5,530	4.5	6,600	3.7
C	クラウド/Webアクセスセキュリティ	7,200	5.9	21,200	12.0
D	Webセキュリティ	10,300	8.4	15,600	8.8
E	認証セキュリティ	12,620	10.3	15,810	9.0
F	端末セキュリティ	28,830	23.4	44,070	24.9
G	サイバーレジリエンス/教育	20,000	16.3	28,810	16.3
H	その他セキュリティ	4,800	3.9	8,350	4.7
合計		122,980	100.0	176,640	100.0

（富士キメラ総研推定）



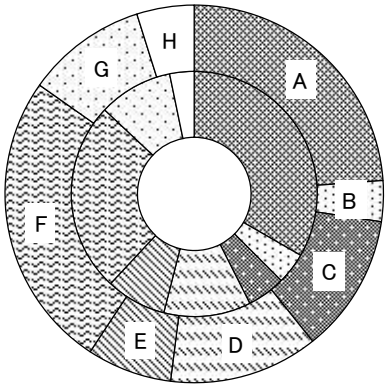
内円：2021年度
外円：2027年度

＜流通＞

単位：百万円、％

領域＼年度		2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	23,800	33.3	25,500	23.9
B	メールセキュリティ	2,950	4.1	3,700	3.5
C	クラウド/Webアクセスセキュリティ	3,600	5.0	12,700	11.9
D	Webセキュリティ	8,200	11.5	13,650	12.8
E	認証セキュリティ	5,660	7.9	7,740	7.2
F	端末セキュリティ	17,910	25.1	27,250	25.5
G	サイバーレジリエンス/教育	6,970	9.8	11,010	10.3
H	その他セキュリティ	2,300	3.2	5,250	4.9
合計		71,390	100.0	106,800	100.0

（富士キメラ総研推定）



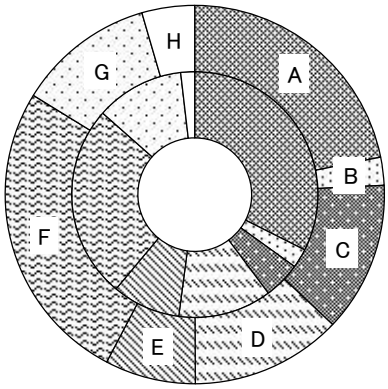
内円：2021年度
外円：2027年度

＜サービス＞

単位：百万円、％

領域 ＼ 年度		2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	15,350	32.5	16,500	21.8
B	メールセキュリティ	1,180	2.5	1,800	2.4
C	クラウド/Webアクセスセキュリティ	2,300	4.9	9,700	12.8
D	Webセキュリティ	5,800	12.3	9,750	12.9
E	認証セキュリティ	4,240	9.0	5,860	7.8
F	端末セキュリティ	12,050	25.5	19,700	26.1
G	サイバーレジリエンス/教育	5,500	11.6	8,860	11.7
H	その他セキュリティ	870	1.8	3,400	4.5
合計		47,290	100.0	75,570	100.0

（富士キメラ総研推定）



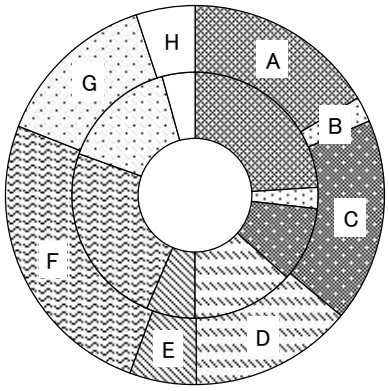
内円：2021年度
外円：2027年度

＜情報通信＞

単位：百万円、％

領域 ＼ 年度		2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	21,650	24.0	23,650	16.4
B	メールセキュリティ	2,500	2.8	3,100	2.2
C	クラウド/Webアクセスセキュリティ	8,900	9.9	25,000	17.4
D	Webセキュリティ	12,050	13.4	20,000	13.9
E	認証セキュリティ	5,770	6.4	8,220	5.7
F	端末セキュリティ	21,710	24.1	36,440	25.3
G	サイバーレジリエンス/教育	13,730	15.2	20,250	14.1
H	その他セキュリティ	3,880	4.3	7,200	5.0
合計		90,190	100.0	143,860	100.0

（富士キメラ総研推定）



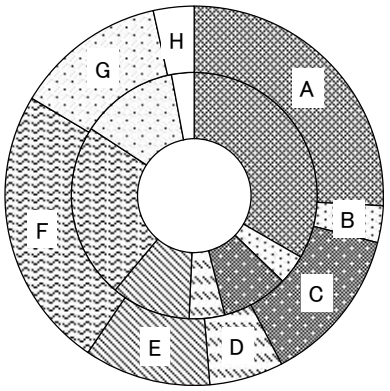
内円：2021年度
外円：2027年度

＜公共＞

単位：百万円、％

領域 ＼ 年度		2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	27,000	33.3	30,100	25.8
B	メールセキュリティ	3,170	3.9	3,650	3.1
C	クラウド/Webアクセスセキュリティ	7,100	8.8	15,600	13.4
D	Webセキュリティ	3,800	4.7	7,350	6.3
E	認証セキュリティ	8,470	10.4	12,580	10.8
F	端末セキュリティ	18,680	23.0	28,070	24.1
G	サイバーレジリエンス/教育	10,450	12.9	15,050	12.9
H	その他セキュリティ	2,400	3.0	4,050	3.5
合計		81,070	100.0	116,450	100.0

（富士キメラ総研推定）



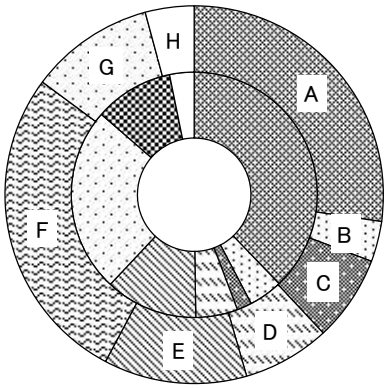
内円：2021年度
外円：2027年度

＜その他＞

単位：百万円、％

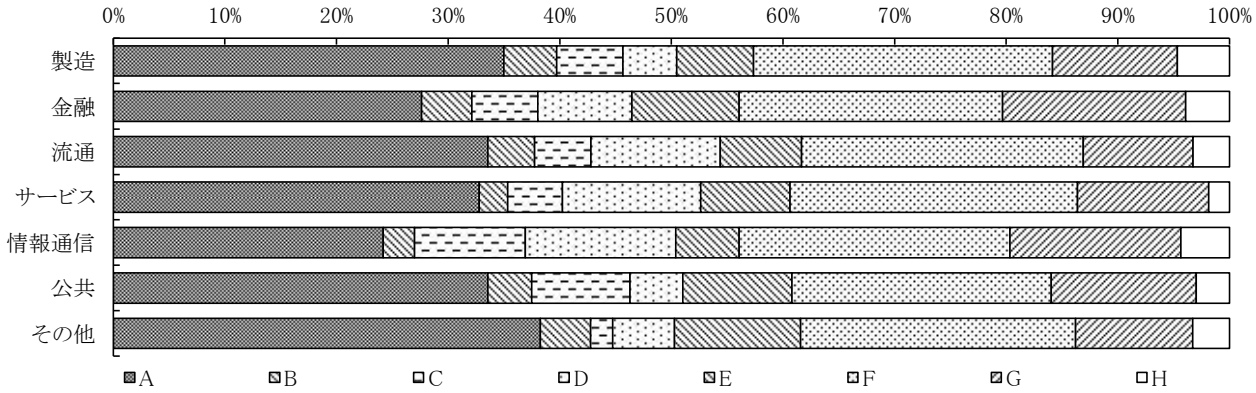
領域	年度	2021		2027	
		実績	比率	予測	比率
A	ゲートウェイセキュリティ	11,700	37.9	13,350	27.3
B	メールセキュリティ	1,370	4.4	1,700	3.5
C	クラウド/Webアクセスセキュリティ	600	1.9	3,600	7.3
D	Webセキュリティ	1,700	5.5	3,650	7.5
E	認証セキュリティ	3,750	12.2	5,990	12.2
F	端末セキュリティ	7,530	24.4	13,430	27.4
G	サイバーレジリエンス/教育	3,210	10.4	5,220	10.7
H	その他セキュリティ	1,000	3.2	2,040	4.2
合計		30,860	100.0	48,980	100.0

（富士キメラ総研推定）

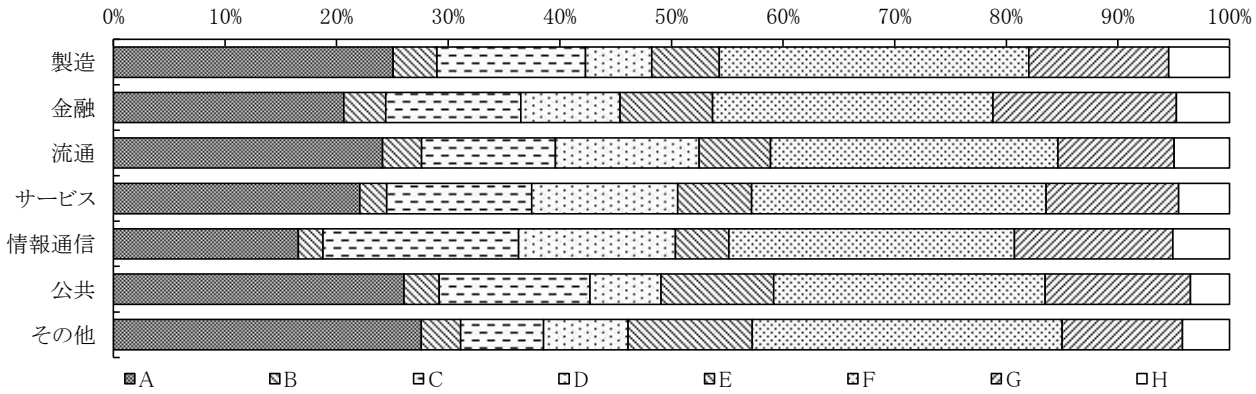


内円：2021年度
外円：2027年度

＜2021 年度における業種別セキュリティ投資領域比較＞



＜2027 年度における業種別セキュリティ投資領域比較＞



記号	領域	記号	領域
A	ゲートウェイセキュリティ	E	認証セキュリティ
B	メールセキュリティ	F	端末セキュリティ
C	クラウド/Web アクセスセキュリティ	G	サイバーレジリエンス/教育
D	Web セキュリティ	H	その他セキュリティ

業種別傾向として、製造業、金融業においてゼロトラストセキュリティを推進するユーザーが増加しており、クラウド/Web アクセスセキュリティの導入が進展しているとみられる。

公共向けでは、デジタル庁による自治体 DX の取り組みが進展することで、自治体によるネットワークセキュリティへの投資が進められると想定される。

業種別で投資傾向は大きく差はないが、情報通信向けでは他業種と比較して Web セキュリティへの投資が大きい傾向にあるとみられる。クラウドサービスを多く取り入れるユーザーが多く、CSPM/CWPP の利用が進展しているほか、Web アプリケーション脆弱性検査ツールなどを活用した脆弱性検査サービスの提供などを行っているユーザーが散見されることなどが要因となっている。

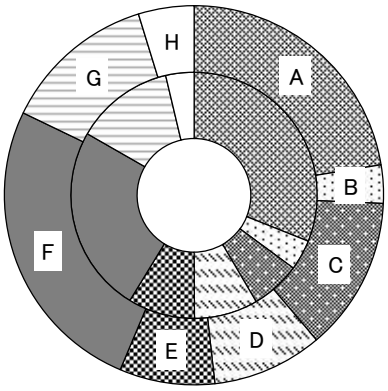
3.3.領域別動向

図表 17「領域別ポジショニングマップ」

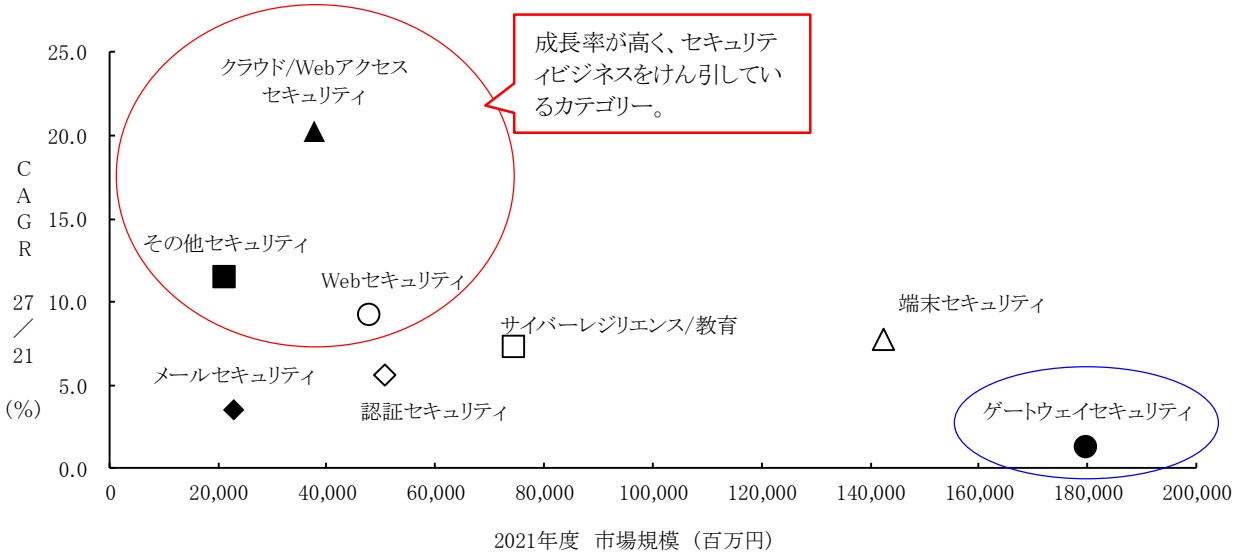
単位：百万円、％

カテゴリー＼年度		2021		2027		CAGR
		実績	比率	予測	比率	(27/21)
A	ゲートウェイセキュリティ	179,800	31.1	194,400	22.4	1.3
B	メールセキュリティ	23,000	4.0	28,250	3.3	3.5
C	クラウド/Webアクセスセキュリティ	37,600	6.5	113,900	13.1	20.3
D	Webセキュリティ	48,250	8.3	81,650	9.4	9.2
E	認証セキュリティ	50,700	8.8	70,450	8.1	5.6
F	端末セキュリティ	142,370	24.6	223,360	25.8	7.8
G	サイバーレジリエンス/教育	74,760	12.9	113,700	13.1	7.2
H	その他セキュリティ	21,450	3.7	40,990	4.7	11.4
合計		577,930	100.0	866,700	100.0	7.0

（富士キメラ総研推定）



内円：2021年度
外円：2027年度



カテゴリー別動向としては、ゲートウェイセキュリティ、端末セキュリティが市場全体をけん引している。特に端末セキュリティに関しては高い成長率を維持したまま市場を拡大させている。テレワークの普及により、EDR などより高度な端末セキュリティへの投資が継続していることや、社外からのアクセスに対し端末の管理を目的とした対策ニーズなどがけん引している。一方、ゲートウェイセキュリティに関しては既存環境のリプレースを中心とした市場となっており、成長率は鈍化している。今後も大きな成長は見込まれないものの、ハイエンドな機器へのリプレースなどで堅調な推移が見込まれる。

成長率ではクラウド/Web アクセスセキュリティが最も高くなった。昨今のセキュリティビジネスにおけるキーワードである「ゼロトラスト」における中核ツールとして SASE 関連の需要が急激に高まっており、大手、超大手企業を中心に導入が進んでいる。単独のツールを利用するようなケースも一部でみられるが、数年スパンで複数のツールを連携させる取り組みを行っている企業が多く、2021 年度だけでなく、2022 年度以降も投資が活発になるとみられる。2022 年度からはこれらの MSS も本格的に展開されるようになっており、ツール、サービス双方でのさらなる市場拡大が見込まれる。

サイバーレジリエンス/教育に関しては、ユーザーのセキュリティ環境の分析やサイバー攻撃後の復旧など、ユーザーのセキュリティに対する考え方の変化から注目が高まっている。攻撃対象となりにくい取り組みや、インシデント発生後の迅速な普及などに関しては、ASM やバックアップなどにも派生している。

Web セキュリティに関しては DDoS 攻撃対策や WAF など定番化したツールに加え、パブリッククラウドの設定管理や統合的なセキュリティ対策を行う CSPM/CWPP が登場している。投資先としては前述のクラウド/Web アクセスセキュリティに比べ普及が遅れているものの、将来的には拡大が期待される領域である。

認証セキュリティに関しては IDaaS との連携などが進んでいる。特に大手、超大手企業など管理 ID が多い企業では IDaaS だけでの ID 運用が難しいため、クラウド、オンプレミス双方でのハイブリッド運用が広がるとみられる。メールセキュリティに関しては PPAP 対策での盛り上がりや、メール基盤のクラウド化による成長がみられた。

3.4.まとめ

業種	取り組み
製造	サプライチェーン攻撃による業務停止などのインシデントが発生しており、大手企業での取り組みだけでなく、中堅、中小企業でのセキュリティ対策が広がるとみられる。海外の大手スマートフォンベンダーでは国内の取引先を含め、得意のベンダーが実施するセキュリティ診断サービスを受け、セキュリティ対策が行われていることを証明しないと取引停止とする取り組みを行っているケースもある。国内ではそこまで厳しい取り組みを進めるケースは少ないとみられるが、中堅、中小企業でのセキュリティの取り組みが進展するとみられる。
金融	FISC が提唱するガイドラインに沿った取り組みが進んでおり、他業種に比べ充実したセキュリティ対策の取り組みが進んでいる。新たな取り組みとしては、PCI DSS がバージョン 4 にアップデートされたことで、関連するセキュリティコンサルティングやセキュリティ診断サービスなども需要拡大が見込まれる。また、大手企業では高度なサイバー攻撃に対する演習ニーズも高まっており、ペネトレーションテストやレッドチーム演習などの需要拡大が見込まれる。 その他の動きとしては、法人向けの融資や保険の検討事項にセキュリティ関連の項目を追加する動きがみられる。すでに融資の際にセキュリティスコアリングサービスを活用し、スコアの低い企業には事業課題としてセキュリティの改善を求めるケースがみられる。海外ではサイバー保険に関する加入する際、保険会社の作成したセキュリティ要件を満たしている企業だけが加入できるような仕様になるケースもみられ、自社だけでなく、他社のセキュリティに関する検査への投資拡大が見込まれる。
流通	製造と同様にサプライチェーン攻撃への対策に関する関心が高まっている。大手企業では取引先やグループ会社へのセキュリティ対策を要求するとともに、セキュリティスコアリングサービスなどを活用しセキュリティ体制のチェックを行う取り組みが拡大するとみられる。 小売では店舗の POS 端末などとしての利用、運輸でのドライバーのアルコールチェックなどを目的に、スマートデバイス活用が増加している。これらの端末向けに MDM や電子証明書を活用したデバイスの管理への投資が拡大するとみられる。 EC サイトを中心に、Web での取引が増加しており、DDoS 攻撃対策や WAF などに加え、Web アプリケーション脆弱診断などの取り組みも拡大が見込まれる。また、PCI DSS がバージョン 4 にアップデートされたことで、関連するセキュリティコンサルティングやセキュリティ診断サービスなども需要拡大が見込まれる。
サービス	サービス業では業務形態からテレワークが遅れていたこともあり、ゼロトラスト関連の取り組みもやや遅れていた。このため、大手企業では今後もゼロトラスト関連の取り組みとして、SWG、IDaaS、SD-WAN、FWaaS、CASB、ZTNA などの導入が進むとみられる。 飲食店ではスマートデバイスを活用した取り組みが進み、EMM/MDM やデバイス管理ツールなどの需要拡大が今後も見込まれる。
情報通信	他業種に比べテレワークが進展しており、SASE やクラウドセキュリティなどへの取り組みが今後も進むとみられる。特に Web サービスなどを中心としたビジネスを行う企業では企業規模を問わずゼロトラストへの取り組みが進展しており、SWG、IDaaS、SD-WAN、FWaaS、CASB、ZTNA、CSPM/CWPP といったツールが今後も広がるとみられる。 大手企業では定着しつつあるテレワークに対し、他人の目がない環境での内部不正対策の取り組みが進むとみられ、ID 管理や DLP、内部不正対策サービスなどの需要拡大が見込まれる。中堅、中小企業では自社サービスのセキュリティ強化への取り組みも進むとみられ、WAF、DDoS 攻撃対策といった外部からの攻撃対策に加え、Web アプリケーション脆弱性診断などの取り組みが進展するとみられる。
公共	自治体強靭化関連の需要から ID 管理や認証デバイス、デバイス管理の需要は高い。検疫ツールに関しては社内ネットワーク構築時に要件定義に含まれるケースが多く、今後も継続した取り組み見込まれる。 2022 年時点で多くの自治体が従来の三層分離を継続した取り組みを行っているが、今後は自治体クラウドなどの活用を含め、新しいネットワーク環境に移行すると想定され、新たなセキュリティとして EDR や端末管理といったエンドポイントセキュリティや仮想ブラウザ、クラウドセキュリティなど新しい取り組みが見込まれる。

4.注力すべきセキュリティ事業領域

1)有望市場分析

図表 18「領域別サービス/製品動向」

(1)ゲートウェイセキュリティ

単位:百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率(27/21)	国産ベンダー比率(2021 年度)
1-1	ウイルス監視サービス	28,000	1.3	96.4
1-2	統合セキュリティ監視サービス	40,100	1.1	94.8
1-3	不正アクセス監視サービス	19,900	-0.3	90.5
2-1-2	ウイルス対策ツール(ゲートウェイ)	7,400	-4.3	60.8
2-2	セキュリティ監視ツール	11,000	1.9	43.6
2-3-2	標的型攻撃対策ツール(ゲートウェイ)	13,600	-3.3	23.5
2-4-1	ファイアウォール/VPN アプライアンス/UTM	52,200	3.4	5.7
2-4-2	SSL-VPN アプライアンス	7,600	2.5	0.0

(富士キメラ総研推定)

(2)メールセキュリティ

単位:百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率(27/21)	国産ベンダー比率(2021 年度)
1-4	メールセキュリティサービス	8,000	5.5	97.5
2-5	電子メールアーカイブツール	3,150	2.9	60.3
2-6	メール暗号化/メール誤送信対策ツール	3,450	3.7	92.8
2-7	メールフィルタリングツール	8,400	1.5	65.5

(富士キメラ総研推定)

(3)クラウド/Web アクセスセキュリティ

単位:百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率(27/21)	国産ベンダー比率(2021 年度)
2-8	CASB	4,700	12.4	5.3
2-9	IDaaS	7,800	17.9	51.3
2-10	Web セキュリティツール	13,400	30.9	1.5
2-11	Web フィルタリングツール	11,700	5.4	98.3

(富士キメラ総研推定)

(4)Web セキュリティ

単位:百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率(27/21)	国産ベンダー比率(2021 年度)
1-5	DDoS 攻撃対策サービス	9,700	8.8	44.3
1-6	WAF 運用管理サービス	4,000	5.8	90.0
1-7	Web アプリケーション脆弱性検査サービス	15,600	7.4	77.6
1-8	モバイルアプリ検査サービス	2,400	12.2	75.0
2-12	CSPM/CWPP	900	28.2	25.6
2-13	DDoS 攻撃対策ツール	4,250	6.4	0.0
2-14	WAF	8,800	8.6	20.5
2-15	Web アプリケーション脆弱性検査ツール	2,600	16.8	38.5

(富士キメラ総研推定)

(4)Web セキュリティ

単位:百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率(27/21)	国産ベンダー比率(2021 年度)
1-9	電子認証サービス	12,400	5.3	21.8
1-9	プライベート CA	4,500	11.2	15.6
2-16	シングルサインオン	5,100	4.4	21.6
2-17	デバイス認証ツール	5,700	5.1	94.7
2-18	統合 ID 管理ツール	4,100	2.7	41.5
2-19	特権 ID 管理ツール	7,550	7.1	70.2
2-20-1	認証デバイス	700	-1.2	81.4
2-20-2	認証デバイス	5,950	4.6	98.3
2-21	ワンタイムパスワード	4,700	4.4	21.3

(富士キメラ総研推定)

(5)端末セキュリティ

単位:百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率(27/21)	国産ベンダー比率(2021 年度)
1-10	EDR 運用支援サービス	2,500	16.0	76.0
2-1-1	ウイルス対策ツール(サーバー/クライアント)	35,900	2.8	46.0
2-3-1	標的型攻撃対策ツール(エンドポイント)	3,200	4.6	28.4
2-3-2	標的型攻撃対策ツール(ゲートウェイ)	13,600	-3.3	23.5
2-22	DaaS	38,500	5.2	74.5
2-23	EDR	15,000	22.6	8.0
2-24	MDM・EMM ツール	12,850	8.2	67.7
2-25-1	端末管理・セキュリティツール(統合エンドポイント管理ツール)	30,200	6.0	76.2
2-25-2	端末管理・セキュリティツール(端末ログ管理ツール)	1,420	1.0	100.0
2-25-3	端末管理・セキュリティツール(持ち出し制御ツール)	2,800	-1.5	92.9

(富士キメラ総研推定)

(6)サイバーレジリエンス/教育

単位:百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率(27/21)	国産ベンダー比率(2021 年度)
1-12	サイバーセキュリティ演習サービス	3,000	9.2	88.3
1-13	セキュリティ/BCP コンサルティングサービス	25,500	6.6	56.1
1-14	セキュリティ教育・トレーニングサービス	16,000	4.8	88.1
1-15	セキュリティ検査・監査サービス	6,500	6.3	84.6
1-16	セキュリティスコアリングサービス	2,100	25.7	0.0
2-26	XDR	800	30.2	12.5
2-27-1	統合ログ管理ツール(SIM)	2,850	2.5	89.5
2-27-1	統合ログ管理ツール(SIEM)	13,500	4.5	2.2
2-28	プラットフォーム検査ツール	2,910	11.2	5.2

(富士キメラ総研推定)

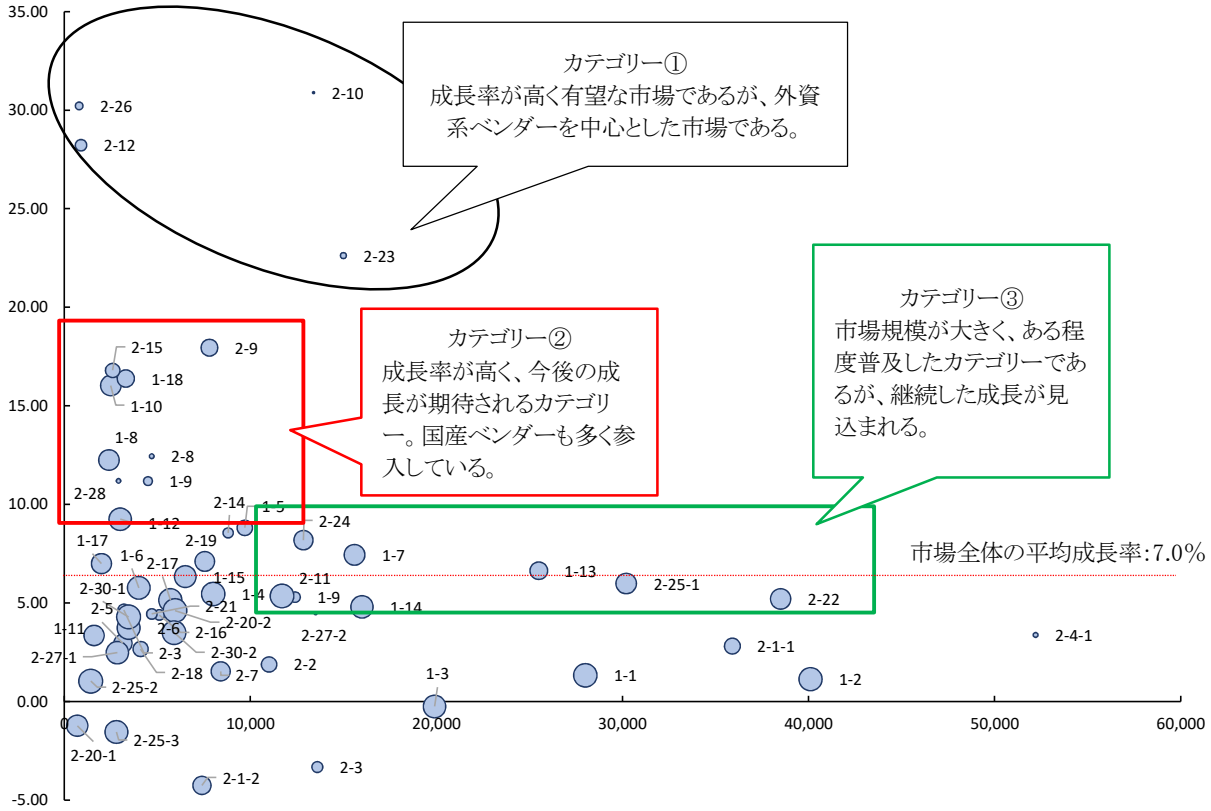
(7)その他

単位:百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率(27/21)	国産ベンダー比率(2021 年度)
1-17	インシデントレスポンスサービス	2,000	7.0	72.5
1-18	スレットインテリジェンスサービス	3,300	16.4	54.5
2-29	NDR	6,800	17.7	0.0
2-30-1	検疫ツール(不正接続防止ツール)	3,450	4.3	100.0
2-30-2	検疫ツール(PC 検疫ツール)	5,900	3.5	98.3

(富士キメラ総研推定)

図表 19「サービス/製品別ポジショニングマップ」



ポジショニングマップの見方

・縦軸:2021 年度から 2027 年度の平均成長率(単位:%)

・横軸:2021 年度の市場規模(単位:百万円)

・円の大きさ:国産ベンダーの売上構成比(単位:%、構成比が 0 の場合は上記ポジショニングマップから除外した)

主要セキュリティサービス/製品の売上や成長率を軸にポジショニングマップを作製した。売上の大きいツールは UTM やファイアウォール、DaaS、ウイルス対策ソフト(エンドポイント)となっている。また、サービスでは UTM などの運用監視を行う統合セキュリティ監視サービスである。この内、DaaS に関してはコロナ禍によるテレワークの増加から新たな需要を獲得している一方、他のサービス/製品は需要の一巡から成長率が低くなっている。

2021 年度から 2027 年度にかけて大きく成長する製品はゼロトラスト関連で注目される SWG を含む Web セキュリティツール、XDR、CSPM/CWPP、EDR などが上位となっている。ここ数年は大手、超大手企業を中心にゼロトラスト関連セキュリティ対策が活況となっており、高い成長率につながっているとみられる。これらの製品は比較的新しいものが多く、外資系ベンダーの売上構成比が高くなっている。これらをカテゴリー①とした。

国産ベンダーが多く成長率が高い、もしくは市場規模が大きいサービス、製品に関しては、成長率が高い領域をカテゴリー②、市場規模が大きく成長率も一定のものをカテゴリー③とした。

4.1.設定の考え方（アプローチ方法）

有望カテゴリーの算出に当たり、各セキュリティカテゴリーにおける 2021 年度の市場規模、2021 年度から 2027 年度に向けた平均成長率、2021 年度における国内ベンダーの売上比率を活用した。上記グラフは各セキュリティサービス/製品を項目別にポジショニングしたグラフで、有望分野としては、

カテゴリー①：平均成長率は 20%以上となる超成長市場

カテゴリー②：平均成長率が 9%以上かつ国内ベンダーの構成比が 35%以上

カテゴリー③：市場規模が 100 億円以上で成長率が 5%以上、国内ベンダー比率が 50%以上

の三つに分けて分析を行った。

図表 20「有望カテゴリー一覧」

〈カテゴリー①〉

単位：百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率（27/21）	国産ベンダー比率（2021 年度）
2-10	Web セキュリティツール	13,400	30.9	1.5
2-12	CSPM/CWPP	900	28.2	25.6
2-23	EDR	15,000	22.6	8.0
2-26	XDR	800	30.2	12.5

（富士キメラ総研推定）

ゼロトラスト関連のセキュリティカテゴリーが集まるグループとなった。市場規模は小さいものもあるが、昨今のセキュリティ関連における注目キーワードなっているものが多くなっている。国産ベンダーの比率は低くなっているものの、トレンドマイクロやソリトンシステムズといったベンダーや中小/ベンチャー企業なども参入している状況にある。

〈カテゴリー②〉

単位：百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率（27/21）	国産ベンダー比率（2021 年度）
1-8	モバイルアプリ検査サービス	2,400	12.2	75.0
1-10	EDR 運用支援サービス	2,500	16.0	76.0
1-12	サイバーセキュリティ演習サービス	3,000	9.2	88.3
1-18	スレットインテリジェンスサービス	3,300	16.4	54.5
2-9	IDaaS	7,800	17.9	51.3
2-15	Web アプリケーション脆弱性検査ツール	2,600	16.8	38.5

（富士キメラ総研推定）

成長率が高く、かつ国産ベンダー比率が 50%以上となるため、国産ベンダーの参入率が高いセキュリティサービスが中心となっている。セキュリティサービスは、国内の SI ベンダーやセキュリティベンダーが中心に市場を形成しており国産ベンダー比率が高いことに加え、近年はユーザーにおけるセキュリティ人材不足が深刻になっており、外部のサービスを利用するケースが増加していることで、成長率も高い状況になっている。

〈カテゴリー③〉

単位：百万円、%

個票番号	サービス/製品	2021 年度市場規模	年平均成長率（27/21）	国産ベンダー比率（2021 年度）
1-7	Web アプリケーション脆弱性検査サービス	15,600	7.4	77.6
1-13	セキュリティ/BCP コンサルティングサービス	25,500	6.6	56.1
2-11	Web フィルタリングツール	11,700	5.4	98.3
2-22	DaaS	38,500	5.2	74.5
2-24	MDM・EMM ツール	12,850	8.2	67.7
2-25-1	端末管理・セキュリティツール(統合エンドポイント管理ツール)	30,200	6.0	76.2

（富士キメラ総研推定）

市場規模が 100 億円以上で、すでに広く普及しているサービスや製品が多い。セキュリティ市場の平均成長率が 7.0%であるが、市場規模が大きくなっているものの、成長率が 5.0%以上と高く、継続した需要を獲得しているサービス/ツールで、国産ベンダー比率も高いことが特徴として挙げられる。

選定方法としては、2021 年度の市場規模など 1-3.セキュリティサービス/製品のポジション分析にて活用した数値に加え、セキュリティサービス/製品カテゴリーごとに、IPA が 2023 年に発表した「情報セキュリティ 10 大脅威 2023」における組織での上位 9 位までの項目に対し、効果がどの程度期待されるかを評価したスコアを合わせて選定した。

〈情報セキュリティ 10 大脅威 2023〉

順位	脅威
1 位	ランサムウェアによる被害
2 位	サプライチェーンの弱点を悪用した攻撃
3 位	標的型攻撃による機密情報の窃取
4 位	内部不正による情報漏えい
5 位	テレワーク等のニューノーマルな働き方を狙った攻撃
6 位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7 位	ビジネスメール詐欺による金銭被害
8 位	脆弱性対策情報の公開に伴う悪用増加
9 位	不注意による情報漏えい等の被害

図表 21「情報セキュリティ 10 大脅威 2023(組織)と各セキュリティサービス/製品の比較」

カテゴリー	個票番号	サービス/製品	順位								
			1	2	3	4	5	6	7	8	9
①	2-10	Web セキュリティツール	—	—	—	○	◎	—	—	—	—
	2-12	CSPM/CWPP	—	—	—	—	○	—	—	—	—
	2-23	EDR	○	○	◎	○	○	○	—	○	—
	2-26	XDR	◎	○	—	—	—	—	—	—	—
②	1-8	モバイルアプリ検査サービス	—	—	○	—	—	○	—	◎	—
	1-10	EDR 運用支援サービス	○	○	◎	○	○	○	—	○	—
	1-12	サイバーセキュリティ演習サービス	○	○	○	○	○	○	○	○	—
	1-18	スレットインテリジェンスサービス	○	—	○	—	○	○	—	○	—
	2-9	IDaaS	—	○	—	◎	—	—	—	—	—
	2-15	Web アプリケーション脆弱性検査ツール	—	—	—	—	—	—	—	◎	—
③	1-7	Web アプリケーション脆弱性検査サービス	—	—	○	—	—	○	—	◎	—
	1-13	セキュリティ/BCP コンサルティングサービス	○	○	○	○	○	○	—	○	○
	2-11	Web フィルタリングツール	—	—	—	○	◎	—	—	—	—
	2-22	DaaS	—	—	—	○	—	—	—	—	—
	2-24	MDM・EMM ツール	—	—	—	○	—	—	—	—	—
	2-25-1	端末管理・セキュリティツール(統合エンドポイント管理ツール)	—	—	—	○	—	—	—	◎	—

影響度：高← ◎ ○ — →低

4.2.検討結果（5 領域）

1)有望セキュリティサービス/製品に関する考察

有望カテゴリーにおける「情報セキュリティ 10 大脅威 2023(組織)」で挙げられた脅威に対し、それぞれの脅威への影響度がトータルで高いセキュリティサービス/製品を有望セキュリティサービス/製品として捉えることとした。

有望セキュリティサービス/製品として、以下を選定した。

個票番号	サービス/製品カテゴリー
1-8	モバイルアプリ検査サービス
1-10	EDR 運用支援サービス
1-12	サイバーセキュリティ演習サービス
1-18	スレットインテリジェンスサービス
1-7	Web アプリケーション脆弱性検査サービス
1-13	セキュリティ/BCP コンサルティングサービス
2-9	IDaaS
2-11	Web フィルタリングツール
2-25-1	端末管理・セキュリティツール(統合エンドポイント管理ツール)
—	クラウドセキュリティ ※

※2-8.CASB[と 2-12.CSPM/CWPP を合わせた市場を対象とした。

この内、5 つのサービス/製品の参入ベンダーにヒアリングを実施し、市場における課題や今後の見解などをヒアリングした。

この中で、影響度の高いサービスは 1-10.EDR 運用支援サービス、1-12.サイバーセキュリティ演習サービスが挙げられる。EDR に関してはエンドポイントセキュリティとして普及しており、その運用サービスは重要なセキュリティサービスとなるが、EDR が外資系

ベンダーを中心とした市場となっており、ツールも含めた国産サービスの比率は非常に少ないことから、除外し、1-12.サイバーセキュリティ演習サービスを選定した。

また、製品では、2-9.IDaaS、2-11.Web フィルタリングツール、2-15.Web アプリケーション脆弱性検査ツール、2-25-1.端末管理・セキュリティツール(統合エンドポイント管理ツール)が挙げられる。この内、2-11.Web フィルタリングツールに関しては公共や文教での利用が多くなっており、用途が限定されることから除外し、残りの 3 つを有望セキュリティツールとして選定した。

また、昨今のクラウド利用の増加とともにクラウド利用におけるサイバー攻撃も多くなっていることから、市場規模が小さいものの、2-12.CSPM/CWPP やクラウド利用におけるセキュリティ対策となる 2-8.CASB やその運用サービスを合わせたクラウドセキュリティを選定した。

4.3.ベンダー調査

4.3.1.サイバーセキュリティ演習サービス

1)調査対象市場の定義/概要

サイバーセキュリティ教育/トレーニングを提供するサービスの中で、仮想環境や専用の演習システム(サイバーレンジ)上でサイバー攻撃や防御の演習を行い、サイバーセキュリティに関する技術やインシデント対応などを学習する演習サービスを「サイバーセキュリティ演習サービス」として定義した。

参入ベンダーが独自のサイバーレンジを開発して提供しているケースと、他社製のサイバーレンジを購入して利用するケースがあるが、本項では両方を対象とした。

なお、サイバーセキュリティに関する知識習得を目的とした教育/研修サービスや、疑似的な標的型メールを送付して対応を訓練するサービスは「セキュリティ教育・トレーニングサービス」として定義して、別項で対象とした。

2)市場規模推移

図表 21「市場規模推移_サイバーセキュリティ演習サービス」

単位:百万円、%

摘要＼年度	2021 実績	2022 見込	2023 予測	2024 予測	2025 予測	2026 予測	2027 予測	CAGR 27/21
金額	3,000	3,500	3,900	4,300	4,600	4,900	5,100	9.2
前年比	—	116.7	111.4	110.3	107.0	106.5	104.1	

(富士キメラ総研推定)

2020 年度はコロナ禍の影響を受けて集合研修の中止/延期が相次いでいたが、2021 年度は各ベンダーにおいてリモート研修への対応が進んだことから、前年度の落ち込みから大きく回復し、市場規模は好調な推移となった。

2022 年度は、製造業におけるサプライチェーン攻撃をはじめとするサイバー攻撃の被害が増加したことから、本サービスへの注目度が高まっている。参入ベンダーもトレンドを取り入れた演習シナリオの提供によるニーズ獲得を図っており、市場の拡大が見込まれる。

企業規模を問わずサイバー攻撃の被害が拡大する中で、サイバー攻撃が発生した際の抵抗力や回復力を強化することで事業継続を可能とする「サイバーレジリエンス」に注目が集まっている。本サービスは実際に攻撃を受ける体験を通じて、対処スキルの向上を図るものであり、今後さらなる需要の拡大が見込まれる。

また、イスラエルや米国などの海外製サイバー演習システムを活用して本市場に新規参入するベンダーも増加しつつあるため、今後も市場規模は拡大傾向で推移するものとみられる。

3)主要参入国産企業

企業名	開発元
AironWorks	サイバーセキュリティ訓練・教育プラットフォーム
NEC	NEC サイバーセキュリティ訓練場演習
S&J	インシデント対応訓練サービス
グローバルセキュリティエキスパート	Micro Hardening:Enterprise Edition
サイバーディフェンス研究所	サイバー演習
サイバーナレッジアカデミー (大日本印刷グループ)	サイバーナレッジアカデミー
情報通信研究機構 ナショナルサイバートレーニングセンター	実践的サイバー防御演習「CYDER」
日立製作所	サイバー防衛訓練サービス
富士通ラーニングメディア	体験!サイバーレンジ～サイバー攻撃・デジタルフォレンジック～
	サイバーレンジによる実践的防御演習基礎
	サイバーレンジによる実践的インシデント訓練
ラック	ラックセキュリティアカデミー
レンジフォース	セキュリティトレーニング

※各社のホームページを参照し作成した。

4)ヒアリングした企業の見解

項目	概要
ターゲット	実践的なセキュリティ演習サービスとなるため、セキュリティ投資が大きく、セキュリティ意識も高い大手、超大手企業をターゲットとするユーザーが多くなっている。近年はサプライチェーン攻撃など中堅、中小企業への攻撃も増加しており、取引先やグループ会社からセキュリティ対策に関する要望を受けるケースも多くなっており、徐々に需要が拡大している。
国産ベンダーの強み	海外ベンダーに関してはグローバルで収集したサイバー攻撃に関する事例などが提供できる点が強みである。一方、国産ベンダーの強みとしてはより日本での事例にフォーカスした演習や、ユーザーの細かな要望に柔軟に対応できる点が強みである。また、レポートやその後のフォローも手厚く行うことで差別化を図っている。 また、国産ベンダーでもセキュリティ先進国であるイスラエルのプラットフォームの活用や技術者と連携した演習など高度なメニューを増加させており、グローバル展開する企業にも一定の需要を獲得している。
業立ち上げの状況と展開に向けた取組と課題	大手、超大手企業を中心に国内外の多くのベンダーが参入しており、今後新たに参入する場合には実績の無さが大きな問題となる。特に演習サービスでは事例数の多さが検討事項に含まれることも多く、大きな課題となっている。 演習円ニューに関しては海外の事例を国産ベンダーが取り入れることも可能であり、品質の差は比較的埋めやすい状況にあるため大きな差にはなっておらず、導入事例に代わる評価があると参入障壁が下がるとみられる。
提供者として事業拡大に向けたシナリオと実現に向けたポイント	大手、超大手企業でのセキュリティに関する取り組みは向上しており、外部にすべて委託するのではなく、ユーザー側でもインシデントへの対応を準備する取り組みが広がっている。このため、大手、超大手企業向けは今後も堅調に拡大するとみている。 また、サプライチェーン攻撃など中堅、中小企業へのサイバー攻撃が大手、超大手企業の事業停止などにつながる事例が増加していることで、取引先やグループ会社にセキュリティ対策強化を要望するケースが増加しており、セキュリティ投資拡大とともに、本サービスの需要につながるとみている。
国に求める支援策、要望など	新規参入する場合、既存のユーザー(特に海外事例も多い外資系ベンダー)と比較された場合、実績が少ないことを理由に負けることが多い。日本独自のセキュリティサービスに関する検定/要件を作成し、合致するサービスには認定を与えるような制度が欲しい。 将来的な事業拡大に向けては、演習の実施、プランの作成を行う人材を増やす必要がある。一方、セキュリティ人材は全体的に不足しており、企業での育成だけでは限度があるため、産学官で連携したセキュリティ人材の育成が本サービスの拡大につながるため、人材育成に関する施策を積極的に行ってほしい。 中堅、中小企業ではセキュリティ予算が限られ、セキュリティ演習サービスを実施できないケースが多い。ユーザー層を広げるためには中堅、中小企業への金銭的な支援が増えると、セキュリティ演習サービスにつながる可能性が高い。

5)考察

期待される取り組み	概要
日本独自のセキュリティ演習サービスに関する認証制度の確立	プラン作成や演習実施、実施後のレポーティングなどに関して要件を作成し、それを満たすサービスに関しては認証資格を与えることや、演習プランを作成する人材向けの検定制度を設け、特定の資格を有する人材が実施する演習サービスとするなど、実績以外の評価軸を提供することで市場に参入しやすくなるとみられる。
セキュリティ人材の育成	セキュリティ人材を増やすことで、演習サービスに係る人材の増員が見込まれ、市場拡大が期待される。大学でのサイバーセキュリティ関連を専攻する部署を増やすことや、サイバーセキュリティに関する大会(SECCON や CTF など)や、IPA が実施するセキュリティ・キャンプなどの取り組みを増やすことが求められる。また、それらに対し日本の学生だけではなく、東アジア、東南アジアといったセキュリティに関心がありITリテラシーがあるもののセキュリティ教育の環境が整っていない諸外国の学生に門戸を広げることで、セキュリティ人材のさらなる増員につながるとみられる。
中堅、中小企業への資金援助	中堅、中小企業を狙うサプライチェーン攻撃などが増加しており、セキュリティ対策強化が求められる一方、セキュリティ投資が限ら UTM やアンチウイルスといった基本的なセキュリティ対策しかできていない企業が多いとみられる。こうした企業に対し、よりセキュリティに特化した補助金は各セキュリティビジネスに直接的な影響は限定的であるとみられるが、セキュリティ意識向上につながるとみられ、将来的には本サービスを含め様々なセキュリティビジネスのユーザー層拡大につながるとみられる。

4.3.2.IDaaS

1)調査対象市場の定義/概要

IDaaS(Identity as a Service)は、クラウド上で ID 管理を行うサービスである。主な機能として、ID 管理、アクセス管理、シングルサインオン(以下 SSO)、多要素認証などがある。

本市場では、オンプレミス環境で構築される ID 管理製品および SSO 製品は対象外とし、クラウドサービスとして ID 管理や SSO などの機能を提供するサービスを対象とした。

2)市場規模推移

図表 22「市場規模推移_IDaaS」

単位:百万円、%

摘要＼年度	2021 実績	2022 見込	2023 予測	2024 予測	2025 予測	2026 予測	2027 予測	CAGR 27/21
ソフトウェア	—	—	—	—	—	—	—	—
前年比	—	—	—	—	—	—	—	
クラウド	7,800	9,400	11,500	14,000	16,500	19,000	21,000	17.9
前年比	—	120.5	122.3	121.7	117.9	115.2	110.5	
アプライアンス	—	—	—	—	—	—	—	—
前年比	—	—	—	—	—	—	—	
合計	7,800	9,400	11,500	14,000	16,500	19,000	21,000	17.9
前年比	—	120.5	122.3	121.7	117.9	115.2	110.5	

(富士キメラ総研推定)

2021 年度は、コロナ禍において企業の柔軟な働き方が求められる中で、クラウドサービスの利用が増加し、セキュリティ強化および利便性向上(シングルサインオン)を目的とした導入が拡大した。各部門でのクラウドサービス利用が増加したことを受け、これまでの手動での ID やアクセスの管理では困難となっており、ID の整理や管理、重複排除などを目的とした利用が拡大した。

2022 年度も同様の傾向がみられるほか、当該製品自体の認知度が向上し、新規導入企業が増加することでの市場拡大が見込まれる。従来は、主に複数のクラウドサービスのシングルサインオン用途として利用されるケースが多かったものの、社内 ID の整理、管理などの ID 管理用途での利用拡大も見込まれる。

2023 年度以降は、よりクラウドシフトが進み、外部クラウドサービスや社内システムへの ID 管理およびログインの利便性向上および多要素認証、リスクベース認証などの認証基盤としての当該製品の利用拡大が予測される。

また、ゼロトラストモデルのセキュリティ対策が重要視される中で、認証はより重要になり、SWG や CASB などのソリューションと連携し、当該製品の導入が進むとみられる。

3)主要参入国産企業

企業名	開発元	製品/サービス名	提供形態		
			S	C	A
GMO グローバルサイン	GMO グローバルサイン	GMO トラスト・ログイン	—	○	—
HENNGE	HENNGE	HENNGE One IdP Edition、HENNGE One Suite	—	○	—
SB テクノロジー	SB テクノロジー	Online Service Gate	—	○	—
アイピーキューブ	アイピーキューブ	CloudLink	—	○	—
インターナショナル システムリサーチ	インターナショナル システムリサーチ	CloudGate UNO	—	○	—
インテック	インテック	ID 認証サービス(認人)	—	○	—
エクスジェン・ネットワークス	エクスジェン・ネットワークス	Extic	—	○	—
サイオステクノロジー	サイオステクノロジー	Gluegent Gate	—	○	—
ソリトンシステムズ	ソリトンシステムズ	Soliton OneGate	—	○	—

ヒアリングを実施した企業を網掛けした　　※各社のホームページを参照し作成した。

4)ヒアリングした企業の見解

項目	概要
ターゲット	テレワークの浸透やクラウドサービス、SaaS アプリケーション利用の拡大を背景として、利用 ID の統合を図る動きが活発化しており、こうした需要動向を背景として当該ビジネスも好調に拡大している。特にクラウドサービスや SaaS アプリケーション利用の増加については、ユーザー規模や業種を問わず拡大する傾向にあり、こうしたサービス利用ユーザーにおいて、IDaaS の潜在的な需要層として想定できる。
国産ベンダーの強み	国産ベンダーにおいては、低価格、高機能、多様なユーザー規模への対応などを訴求することで、コスト課題やスモールスタート対応などを求めるユーザーを取り込み競合との差別化として展開するベンダーやサポート体制の充実や顧客満足度の向上に向けたユーザー利用での支援拡充による差別化など、日系ユーザーの利用環境に柔軟な対応力を訴求することで、海外ベンダーとの差別化を図る動きがみられる。 また、日本製のクラウド認証基盤として国産としての信頼性などを訴求できる強みがある。認証については、セキュリティの側面としてサービス信頼性なども重要な要素であり、日本製サービスとしての優位性を訴求した取り組みを図っている。
業立ち上げの状況と展開に向けた取組と課題	ID 統合を提供するサービスとしては、ユーザーID などを外部環境に委託することへの懸念があり、当該サービス利用の抵抗感が見られたが、クラウドサービスや SaaS サービスの普及などもあり、こうした複数のサービス利用を効率化するツールとしての認知度、認識が高まったことで IDaaS としての需要拡大につながっている。
提供者として事業拡大に向けたシナリオと実現に向けたポイント	企業の利用システムとして、クラウドサービス、SaaS アプリケーションは今後も拡大していくほか、業務システムとしてもさらに一般化していく流れが想定される。こうしたシステム利用環境の中で、ID 統合による安全性、利便性を向上させるニーズも高まっていくとみられ、ID 管理によるシステム利用の安全性強化、利便性向上などの需要を取り込むことで事業拡大が推進される。 IDaaS としては、単独製品としての機能ではなく、クラウドサービス、SaaS アプリケーションの利用環境を ID 統合によって効率化やセキュア化させるものであり、連携するクラウドサービス、SaaS アプリケーションなど事業連携を拡充していくことも今後の需要拡大やユーザー獲得に向けた施策のポイントとなっている。
国に求める支援策、要望など	セキュリティ投資については、投資としてネガティブな側面があるが、業務システムなどを利用する上で、セキュリティ管理や強化は必要不可欠であり、こうしたセキュリティ対策を推進する意識、意欲を向上させる活用なども政府政策として必要な対策である。 国産ベンダー育成の観点では、ID 管理などの基盤となる機能については、国内リージョンでの管理を推奨することや国産ベンダー製品を推奨する方針など国としての方針を明確化することも事業育成としては望ましいと考えられている。

5)考察

期待される取り組み	概要
セキュリティ投資全体における啓蒙	セキュリティ投資全体を啓蒙することで、IDaaS を含めセキュリティ市場全体のビジネス拡大が見込まれる。国として、すでに様々な施策を行っているとみられるが、より具体的な事例をベースに、対策を行わない場合にどのような被害が生じたかを、セキュリティ分野別、業種別などにまとめることで、各業界の経営層に響く資料になるとみられる。
ID 管理、認証におけるガイドライン策定、証明	クラウド利用の拡大、テレワークの普及、内部不正対策などを契機に ID 関連のセキュリティ意識が高まっている。一方、クラウドへのシングルサインオンだけでなく、ID 統合管理などの機能を有する IDaaS に関しては、ID をクラウド上で管理することへのネガティブな見解も多くみられる。 このため、国産ベンダー、国内リージョンで運営しているといった安全なサービスを利用を訴求する方針を打ち出すことや、特定のセキュリティ要件を満たし安全に ID 管理できるサービスであることなどを証明する認証資格を提供するなどすることで、国産ベンダーの支援につながろみられる。

4.3.3.Web アプリケーション脆弱性検査ツール

1)調査対象市場の定義/概要

本項では、Web アプリケーションの脆弱性を検査/診断し、レポートを発行する Web アプリケーション脆弱性検査ツールを対象とした。

なお、Web アプリケーション脆弱性検査ツールには、SAST、DAST、IAST といった種類が存在する。SAST は、プログラムコードを実行せずに、ドキュメントやソースコードなどのチェックによって誤りや脆弱性を検出するテスト手法である。DAST は、プログラムコードを実行し、ソフトウェアのバグ検出や品質評価、動作確認を行う検査ツールである。IAST は、SAST 同様にソースコードの診断を行うが、DAST 同様にアプリケーションがテスト環境などで実行している間にリアルタイムで診断を行う検査ツールである。本項ではいずれのツールも対象とした。

プラットフォーム環境およびネットワーク環境における脆弱性検査を行うプラットフォーム検査ツールは別項で取りまとめたため、本項では対象外とした。また、本製品を活用し、専門家によるマニュアル診断を組み合わせた脆弱性検査サービスにおいては、別項で取りまとめたため対象外とした。

2.市場規模推移

図表 23「市場規模推移_Web アプリケーション脆弱性検査ツール」

単位:百万円、%

摘要＼年度	2021 実績	2022 見込	2023 予測	2024 予測	2025 予測	2026 予測	2027 予測	CAGR 27/21
ソフトウェア	1,900	2,250	2,500	2,750	3,000	3,250	3,500	10.7
前年比	—	118.4	111.1	110.0	109.1	108.3	107.7	
クラウド	700	1,100	1,500	1,900	2,300	2,700	3,100	28.1
前年比	—	157.1	136.4	126.7	121.1	117.4	114.8	
アプライアンス	—	—	—	—	—	—	—	—
前年比	—	—	—	—	—	—	—	
合計	2,600	3,350	4,000	4,650	5,300	5,950	6,600	16.8
前年比	—	128.8	119.4	116.3	114.0	112.3	110.9	

(富士キメラ総研推定)

2020 年度以降、COVID-19 の影響により、対面でのビジネス機会が減少したことで、デジタルコンテンツを活用したビジネスの注力度を高める、もしくは新たに展開するユーザーが増加した。そのため、併せて本製品を導入するユーザーが増加し、本市場が拡大したとみられる。

2021 年度においても、国内外問わず Web アプリケーションを活用したビジネスはいずれの企業においても必須となっていることから、堅調に市場は拡大しているとみられる。2022 年度見込みにおいても、同様の傾向で推移していくとみられる。

同市場は、従来ソフトウェア製品が主流であったが、近年ではクラウド型製品のニーズが高まっており、高い市場成長率で推移しているとみられる。

3)主要参入国産企業

企業名	開発元	製品/サービス名	提供形態		
			S	C	A
アイティーエム	アイティーエム	WebSiteScan	—	○	—
エーアイセキュリティラボ	エーアイセキュリティラボ	AeyeScan	—	○	—
セキュアブレイン	セキュアブレイン	GRED Web セキュリティ診断 Cloud	—	○	—
ビットフォレスト	ビットフォレスト	VAddy	—	○	—
ユービーセキュア	ユービーセキュア	Vulnerability Explorer	○	—	—

※各社のホームページを参照し作成した。

4)ヒアリングした企業の見解

項目	概要
ターゲット	ソフトウェアで提供される高度なツールに関しては、主に本ツールを活用し検査サービスを提供するサービスベンダーや Web サービスを中心としたビジネスを展開する情報通信業向けの実績が高い傾向にある。 一方、クラウドに関しては比較的簡易な検査ツールとなっており、エンドユーザーでの利用も多い傾向にある。コロナ禍以降、EC サイト構築の需要が拡大するとともに、そのセキュリティ対策として需要が大きく拡大している。
国産ベンダーの強み	日本語によるサポートや UI など日本人の使いやすい仕様となっていることが大きな訴求点である。また、国産ベンダーでは日本への攻撃の分析など国内でビジネスを展開する上での細かな対応が可能である点も強みである。
業立ち上げの状況と展開に向けた取組と課題	もともとインターネットを活用したサービスの展開が進んでいた海外で先行して取り組まれていたことから、当初は海外製品が主流となっていた。セキュリティでは実績を重視した選定を行うケースが多く、国内ベンダーが事業を開始しても実績や認知度が不足しており、採用されにくい状況といった課題が挙げられる。
提供者として事業拡大に向けたシナリオと実現に向けたポイント	今後も Web サービスが拡充することで、堅調な拡大が見込まれる。また、本ツールを活用したサービスが年度末など特定の時期に集中することや、Web アプリケーションを定期的に更新することでセキュリティを強化する取り組みが広がるなど、外部に委託するのではなく、自社で本ツールを活用/運用する取り組みが進展することでさらなるユーザー層の拡大が見込まれる。 特に国産ベンダーも多く参入しているクラウド型ツールは開発現場などセキュリティの知見が少ない人員でも活用できるような UI や機能を搭載しており、高い成長が期待される。
国に求める支援策、要望など	新規参入時は認知度/実績の不足から、案件に参加できない、すでに参入しているベンダーと比較され選定されにくくなっている、といった点が大きな課題である。また、すでに導入済の企業では、Web アプリケーションの脆弱性診断における業務フローが固まっており、異なるツールを導入する場合にはその業務フローの見直しが必要となり、既存ツールが継続して利用されるケースが多いといった点も課題となっている。 今後の市場拡大に関する要望としては、Web サイトや Web アプリケーションに関するセキュリティガイドラインの策定や Web アプリケーションに対して定期的な脆弱性診断を行っていることがわかる認証制度の作成などが挙がった。

5)考察

期待される取り組み	概要
実績不足をカバーする評価制度	脆弱性に関する検査手法やデータベースなどに対して要件を満たすツールであることを評価する制度や、IPA などが実際に活用し評価レポートを公開するなどすることで、実績の代替となる支援を行うことが可能となるとみられる。 また、新規参入時は案件も少なく、売上も小さいため、中央省庁や関係機関が数年の契約を結ぶことで、実績が増えつつ、売上拡大による機能強化などにつながるとみられる。
Web サイトや Web アプリケーションに関するガイドラインや認証制度の策定	近年の Web アプリケーションは DevSecOps を意識した取り組み拡大しており、サービス開始後も不定期な更改やバージョンアップによる機能拡張を行いつつ、機能拡張後の脆弱性診断を実施する取り組みが求められている。しかし、脆弱性診断に係る費用を抑えるため、定期的な診断を行わないケースも多く、Web アプリケーション脆弱性診断サービスに関しては毎年 3 月が繁忙期となっている。このため、定期的な診断を義務付けるガイドラインや法規制を整備することで、ユーザーの定期的な脆弱性診断ニーズにつながるとみられ、本市場の拡大が期待される。 また、Web アプリケーションに対して、定期的な脆弱性診断を実施しているアプリケーションに対し、セキュリティ対策を実施していることが視覚的にわかりやすくなる認証マークを付与するなどの取り組みを行うことで、アプリケーションの価値向上につながり、脆弱性診断の需要拡大につながるとみられる。

4.3.4.端末管理・セキュリティツール(統合エンドポイント管理ツール)

1)調査対象市場の定義/概要

統合エンドポイント管理ツールは、クライアント PC のハードウェア構成やソフトウェアなどの IT 資産管理機能を基本として、端末の内部セキュリティに必要な各種機能を搭載する製品である。付随する機能として、後述の端末ログ管理ツールや持ち出し制御ツールとしての機能があるほか、他社エンジンと連携し外部脅威対策機能を提供する製品もある。機能別での売上の切り分けが難しいため、本項では IT 資産管理機能だけでなく、付随する複数のオプション機能による売上も対象とした。ただし、他社エンジンを活用する外部脅威対策機能については算出の対象外とした。

2)市場規模推移

図表 24「市場規模推移_端末管理・セキュリティツール(統合エンドポイント管理ツール)」

単位:百万円、%

摘要＼年度	2021 実績	2022 見込	2023 予測	2024 予測	2025 予測	2026 予測	2027 予測	CAGR 27/21
ソフトウェア	26,500	28,300	29,600	30,400	31,100	31,800	32,500	3.5
前年比	—	106.8	104.6	102.7	102.3	102.3	102.2	
クラウド	3,500	4,900	6,200	7,400	8,400	9,400	10,300	19.7
前年比	—	140.0	126.5	119.4	113.5	111.9	109.6	
アプライアンス	200	100	△	△	△	△	△	—
前年比	—	50.0	—	—	—	—	—	
合計	30,200	33,300	35,800	37,800	39,500	41,200	42,800	6.0
前年比	—	110.3	107.5	105.6	104.5	104.3	103.9	

(富士キメラ総研推定)

本市場はソフトウェア製品の比率が高い。ソフトウェア製品については、2021 年度はコロナ禍を背景とした社内外における利用端末のセキュリティ強化やテレワーク時の労務管理需要が高まり、好調な市場拡大となった。2022 年度もこの傾向が継続すると予測される。ただし、超大手/大手企業への導入は一巡しており、長期的には追加/リプレースを中心とする市場である。2024 年度頃までには上記のテレワーク推進に伴う市場拡大が落ち着き、その後は堅調な市場規模推移となる見込みである。

一方で、クラウド製品の市場規模は今後急速に拡大する見込みである。テレワークの普及に伴い、クラウド環境/インターネットを通じた端末管理のニーズが拡大しており、主要ベンダーもクラウド製品への注力度を高めている。さらに、クライアント端末数の多くない中堅/中小企業ではクラウド型での本製品の採用が増加している。加えて、一部のユーザーではソフトウェア製品からクラウド製品に移行するケースも散見されており、今後クラウド製品の市場拡大をけん引する見込みである。

アプライアンス市場に関しては、一部ベンダーが提供を行っているものの、取り扱いを終了するベンダーも散見される。市場規模としては縮小傾向にあると予測される。

3)主要参入国産企業

企業名	開発元	製品/サービス名	提供形態		
			S	C	A
JAL インフォテック	JAL インフォテック	PalletControl	○	○	—
NTT データ先端技術	NTT データ先端技術	NOSiDE Inventory Sub System 資産管理	○	—	—
Sky	Sky	SKYSEA Client View	○	○	—
		SKYMEC IT Manager	○	—	—
アイ・ティー・ワン	アイ・ティー・ワン/インテリジェント ウェイブ	Gardit	—	○	—
アセットメント	アセットメント	Assetment Neo	—	○	—
インターコム	インターコム	MaLion	○	—	—
		MaLionCloud	—	○	—
インテリジェント ウェイブ	インテリジェント ウェイブ	CWAT	○	—	—
内田洋行	内田洋行	ASSETBASE	○	○	—
エムオーテックス	エムオーテックス	LANSCOPE オンプレミス版	○	—	—
		LANSCOPE クラウド版	—	○	—
		HACONEKO	—	—	○
クオリティソフト	クオリティソフト	QND Premium、QND Standard	○	—	—
		ISM CloudOne	—	○	—

企業名	開発元	製品/サービス名	提供形態		
			S	C	A
コア	コア	ITAM	○	○	—
住友電工情報システム	住友電工情報システム	MCore	○	—	—
ディー・オー・エス	ディー・オー・エス	SS1	○	○	—
ハンモック	ハンモック	AssetView	○	○	—
日立システムズ	日立システムズ	License Guard	○	—	—
日立ソリューションズ	日立ソリューションズ	秘文 統合エンドポイント管理サービス	—	○	—
富士通	富士通	InfoBarrier	○	—	—
ユニアデックス	ユニアデックス	ADMi-21 G7	○	—	—

※各社のホームページを参照し作成した。

4)ヒアリングした企業の見解

項目	概要
ターゲット	大手、超大手向けの導入が中心であるが、徐々に中堅企業向けの導入が増加している。参入ベンダーも既存ユーザーとしては大手以上の企業実績が多くなっているが、次のターゲットとして中堅企業向けの取り組みを検討している。 汎用的なセキュリティツールであり、業種を問わず導入が進んでいる。
国産ベンダーの強み	海外ベンダーと比べ、サポートや製品品質、日本企業の業態に合わせた使い勝手の良さなどが強みとして挙げられる。特に国内市場特有のニーズを取り込み、機能拡張を実施してきたことで、シェア上位も国産企業が多くなっている。
業立ち上げの状況と展開に向けた取組と課題	立ち上げ当時は PC やソフトウェアの管理の重要性が認知されておらず、市場も小さい状況が続いた。契機としては個人情報保護法が挙げられ、社内のセキュリティ対策の関心が高まるとともに、脆弱性となる古いバージョンのソフトや OS などを可視化し対処することへの関心が高まった。
提供者として事業拡大に向けたシナリオと実現に向けたポイント	大手、超大手企業向けにはある程度普及したとみるベンダーもみられたが、昨今のゼロトラスト関連の取り組みの中でエンドポイントセキュリティへの関心が高まっており、EDR などとともに社内の IT 機器の状況を可視化し管理するニーズが高まっていくとみている。また、エンドポイントセキュリティの統合、連携や進んでおり、大手ベンダーでは他のエンドポイントセキュリティツールとの連携強化を進めている。
国に求める支援策、要望など	ある程度ガイドラインや法規制などの指針がないと、新たなセキュリティ対策を行う企業が限定されるため、セキュリティに関するガイドラインなどを定期的に策定することで、新規需要が生まれ、事業拡大につながるとみている。 立ち上げ期に関しては認知度不足に代わる検定資格などがあると、実績の豊富な外資系ベンダーへの対抗になるとみている。また、ISMAP 対応など高額な費用が発生するものの割引、免除などがあると、より実績を高めやすいのではないかとみている。

5)考察

期待される取り組み	概要
セキュリティに関するガイドラインや法規制の策定	今後、市場拡大が見込まれる規模は中堅、中小である。サプライチェーン攻撃などの対策を意識したセキュリティ投資の拡大が見込まれる一方、セキュリティ予算が限られるため、セキュリティ対策として端末管理を選定する可能性は不明瞭である。 そのため、サプライチェーン攻撃のリスクとなる、古いバージョンの OS やソフトといった脆弱性のある PC の有無や、会社が管理できていない野良 PC などを把握し社内ネットワークに攻撃起点となるリスクがある端末をなくすような取り組みが進むことで、市場拡大が期待される。
公共案件への導入支援	民間企業では実績を重視した選定も多く、新規参入の場合には実績を増やすことが難しいとみられる。このため、新規参入した企業のツールを中央省庁や関係機関で利用することで、実績を増やしつつ、売上拡大が期待される。
補助金制度	近年では ISMAP など公的な評価がつくものがあるが、認証されるまでに高額な費用が発生するため新規参入ベンダーでは利用できないケースが多い。新しいセキュリティベンダーが公的な資格を取得する場合の補助金制度があると、新規参入後のマーケティングがより行いやすくなるとみられる。

4.3.5.クラウドセキュリティ

1)調査対象市場の定義/概要

本項では、CASB、CSPM/CWPP およびその運用支援サービスを対象として市場をとらえた。市場規模推移に関しては、ツールの二つを合わせた市場を算出した。

CASB(Cloud Access Security Broker)は「SaaS」を中心としたクラウドサービス向けのセキュリティ対策ツールである。その機能は、「可視化(ディスカバリー)」「データセキュリティ」「コンプライアンス」「脅威防衛」の四つに分けられる。本項では上記の 4 点を主たる機能とする製品を対象とした。

CSPM/CWPP に関しては、IaaS/PaaS におけるセキュリティ設定の管理やワークロードの保護を行う CSPM(Cloud Security Posture Management)および CWPP(Cloud Workload Protection Platform)を対象とした。また、これらの機能を一つのプラットフォームで利用可能な CNAPPs(Cloud Native Application Protection Platforms)も対象とした。

2)市場規模推移

図表 25「市場規模推移_クラウドセキュリティ」

単位:百万円、%

摘要＼年度	2021 実績	2022 見込	2023 予測	2024 予測	2025 予測	2026 予測	2027 予測	CAGR 27/21
CASB	4,700	5,900	7,000	7,800	8,500	9,000	9,500	12.4
前年比	—	125.5	118.6	111.4	109.0	105.9	105.6	
CSPM/CWPP	900	1,450	2,000	2,500	3,000	3,500	4,000	28.2
前年比	—	161.1	137.9	125.0	120.0	116.7	114.3	
合計	5,600	7,350	9,000	10,300	11,500	12,500	13,500	15.8
前年比	—	131.3	122.4	114.4	111.7	108.7	108.0	

(富士キメラ総研推定)

3)主要参入国産企業

(1)ツール

企業名	開発元	製品/サービス名	提供形態		
			S	C	A
NTT テクノクロス	NTT テクノクロス	TrustBind/Cloud Daemon	—	○	—
トレンドマイクロ	Trend Micro	Trend Micro Cloud One Workload Security	—	○	—

(2)運用サービス

企業名	開発元
BeeX	BeeXPlus
CloudBase	Cloudbase
NRI セキュアテクノロジーズ	Netskope CASB 運用支援サービス
	統合クラウドセキュリティマネージドサービス powered by Prisma Cloud from Palo Alto Networks
NTT コミュニケーションズ	WideAngle マネージド CSPM
SB テクノロジー	CASB 向け運用支援サービス- MSS for CASB
SCSK	Smart One Cloud Security Powered by Prisma Cloud from Palo Alto Networks
ネットワンシステムズ	クラウドアクセスセキュリティサービス
日立ソリューションズ	クラウドワークロードセキュリティサービス
テリロジー	CSPM 運用サービス
ニューリジェンセキュリティ	Cloudscort

※各社のホームページを参照し作成した。

4.4.ヒアリングした企業の見解

項目	概要
ターゲット	AWS、GCP、Azure をはじめとしたパブリッククラウド利用が増加するなかで、クラウドセキュリティインシデントの原因は設定ミスによるもの多く、ユーザー社内の膨大なクラウド資産の可視化により、セキュリティリスクを監視・検出することで、設定ミスに伴うリスク低減を実現するソリューションのニーズが高まっている。 クラウドサービス利用については、業種や規模にかかわりなく、DX 推進などにより、様々な事業部門でクラウドサービスを利用するケースが増加している。こうした多様なクラウドサービス利用環境においては、セキュリティ設定の不備、設定ミスなどの確認を人手でチェックすることには限界があり、セキュリティ対策の欠如につながることが想定されるため、CSPM 運用サービスなどクラウド環境のセキュリティを監視していくことのニーズは高まっている。
国産ベンダーの強み	CSPM 自体は海外ベンダー製品が主流であるが、国内ユーザーにおいては、運用負担の低減、セキュリティ運用強化から、マネージドサービス利用への期待は大きいと考えている。こうしたマネージドサービスニーズの中で、国産サービスベンダーとして、国内企業の運用ニーズに合わせたサービス提供や日本語でのサポート対応などを差別化として推進されている。
業立ち上げの状況と展開に向けた取組と課題	サービス認知度の低さやサービス利用によるユーザーメリットなど、サービス利用の理解を得ることの難しさがある。また、新規サービスの場合、対策の必要性など導入に至る意識付けなどが難しいことが多く、セキュリティ投資を促すことの難しさがある。 また、事業拡大を推進するなかで、サービス認知度の向上は、企業としての信頼性向上にもつながっていくとみられ、サービスや企業認知を早急に高めていくことが、ベンチャー企業における事業育成、強化に必要なポイントとして挙げられている。
提供者として事業拡大に向けたシナリオと実現に向けたポイント	セキュリティ対策については、短期的に技術、ノウハウを蓄積することの難しさもあるため、自社単独で対策を実施できるユーザーも限定的である。こうしたユーザー課題を背景として、セキュリティ技術やノウハウを有する専門ベンダーがマネージドサービスとして提供することの価値は高く、専門的なサービスを利用することの有効性やメリットを明確にすることで、CSPM 運用サービスを含めたセキュリティマネージドサービス利用機会の増加につなげたい意向がある。
国に求める支援策、要望など	ベンチャー企業の育成においては、省庁などが実施する施策において、企業認知や製品認知を進めていくために、表彰や官庁における製品、企業信頼性を高めるための証明などを与えていくことも企業育成、産業育成においては重要な点である。 また、サービス利用に際して、ユーザーの導入意欲や投資を促すために、クラウドセキュリティなどの利用において、運用サービスを推奨することやガイドラインなどの対策基準として運用による持続的な対策の維持を促すなどの対策や意識向上の活動が望まれている。

4.5.考察

期待される取り組み	概要
表彰や認定制度の拡充	クラウドセキュリティに関連するツールとしては、各メガクラウドベンダーがオプションとして提供するものを含め、外資系のツールが中心となっている。国内ベンダーではベンチャー企業も多く、認知度向上のため、ツールに関する表彰や認定制度を拡充することで、国内ベンダー企業が営業展開しやすい環境を作ることにつながるとみられる。
クラウドセキュリティの啓蒙	国内のクラウドセキュリティへの意識はまだ低くなっており、IaaS の設定不備(初期パスワードのままなど)による乗っ取りやサイバー攻撃がみられる。IaaS を利用する上で、IaaS 基盤に関してはクラウドサービスベンダーがセキュリティ対策を構築しているものの、その設定状況やアプリケーション層のセキュリティに関しては個別の取り組みが必要であることを啓蒙することで、クラウドセキュリティ全体の取り組み拡大につながるとみられる。

5.強化すべき市場分野と現状

5.1.設定の考え方（経済安全保障におけるポイント）

重要インフラごとにサイバー攻撃を受けた場合の影響度を比較した。比較項目としては、重要インフラとして重視される「国民の生命/財産」「経済や社会生活の安定」を軸として影響度を比較した。それぞれの影響度をスコア化し、より重点的に調査すべき重要インフラを分析した。重要インフラのカテゴリー/対象となる重要システム例は内閣サイバーセキュリティセンター「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」をベースに作成した。各影響度、スコアは富士キメラ総研にて算出した。

図表 26「重要インフラにおけるサイバー攻撃の影響」

重要インフラ		対象となる重要システム例	国民の生命/財産	経済や社会生活の安定	スコア
情報通信		ネットワークシステム オペレーションサポートシステム 編成・運行システム	○	◎	6
金融		勘定系システム 資金証券系システム 国際系システム 対外接続系システム 金融機関相互ネットワークシステム 電子債権記録機関システム 保険業務システム 証券取引システム 取引所システム 振替システム 清算システム 等	◎	◎	7
交通	航空	運航システム 予約・搭乗システム 整備システム 貨物システム	○	◎	6
	鉄道	列車運行管理システム 電力管理システム 座席予約システム	○	◎	6
電力		電力制御システム スマートメーターシステム	◎	◎	7
ガス		プラント制御システム 遠隔監視・制御システム	◎	◎	7
政府・行政サービス		各府省庁及び地方公共団体の情報システム （電子政府・電子自治体への対応	○	○	4
医療		診療録等の管理システム等（電子カルテシステム、遠隔画像診断システム等、医用電気機器等）	◎	△	3
水道		水道施設や水道水の監視システム 水道施設の制御システム等	◎	○	5
物流		集配管理システム 貨物追跡システム 倉庫管理システム	△	○	3
化学		プラント制御システム	△	○	3
クレジット		クレジットカード決済システム	◎	△	3
石油		受発注システム 生産管理システム 生産出荷システム、等	△	◎	5

影響度：高← ◎ ○ △ →低

図表 27「スコア算出方法」

項目＼重要度	◎	○	△
国民の生命/財産	2	1	0
経済や社会生活の安定	5	3	1

より影響の大きいと想定される「経済や社会生活の安定」に関してはスコアを大きくし算出した。双方で大きな影響が見込まれる重要インフラは情報通信、金融、交通(航空/電車)、電力、ガスとなった。

スコアの高い重要インフラ	想定されるサイバー攻撃による被害
情報通信	企業活動において重要となっているネットワークの切断や大規模な個人情報漏洩などが想定される。 2022 年に発生した KDDI の通信障害は、サイバー攻撃ではないものの、最長 61 時間 25 分、音声通話が 2,278 万人以上、データ通信は 765 万人以上、グループ会社の沖縄セルラーでは、音声通話で約 38 万人、データ通信で 10 万人以上の影響が生じた。法人向けでは物流やコネクテッドカー、気象観測や水道などのデータ収集、金融機関の ATM、交通機関での無線機や IC カードなどに影響が生じた。 サイバー攻撃ではこれ以上の影響が想定されるなど、大きな被害が生じる可能性がある。
金融	他の業界に比べFISCを中心とした高度なセキュリティ対策を行っている業界であるが、個人資産への影響や、企業間の支払い、金融商品の取引停止などの大規模な被害が想定される業界である。
交通(航空/電車)	海外では運行管理システムや予約システムへのサイバー攻撃により、電車が動かない、飛行機に搭乗できないといった事例が発生している。 大規模な交通網の停止は、物流や人流に大きな影響を及ぼすと想定される。
電力	個人、法人を問わず電気/ガスの提供が停止する可能性がある。提供が停止されることでさまざまな業界に影響するが、特に製造業や医療関係への影響が大きいと想定される。また、季節によっては一般家庭への影響も大きくなる。
ガス	

また、重要インフラではないものの、国内最大の産業である製造業へのサイバー攻撃は大きな影響をもたらすことが想定され、経済安全保障の観点から、より日本経済への影響が大きいとみられる業種を選定することとした。

重要度の高いとみられる製造業	想定されるサイバー攻撃による被害
自動車	国内でも最大規模の産業であるが、2022 年にサプライチェーン攻撃により、業務停止、納期遅延などの影響が生じた。
半導体	2023 年に海外では半導体に関する重要データが内部不正による漏洩事故が発生しており、国内でも 2014 年に同様の事故が発生するなど、リスクが高い。
医療機器	インシデント事例は稀であるが、サイバー攻撃による工場停止では他の製造業同様に影響が生じることに加え、機器内部に不正なプログラムを組み込まれるリスクなども想定される。
医薬品	サイバー攻撃による工場停止は、安定した医薬品の提供に大きな影響を与え、国民の生命に大きな影響を与えるリスクが想定される。

5.2.調査対象とした業界とその理由

重要インフラの内、サイバー攻撃による「国民の生命/財産」「経済や社会生活の安定」への影響が大きい業界として、情報通信、金融、交通(航空/電車)、電力、ガスを対象とすることとした。

製造業では、公知情報などで情報収集しやすい自動車に関しては本調査対象からは除外した。半導体、医療機器、医薬品の内、内部不正事例や組み込みリスクなど一般企業で実施しているセキュリティ対策とは異なる取り組みを実施している可能性がある半導体、医療機器を対象とした。

5.3.業界別動向

5.3.1.電力業界

1)主な保護対象システムと保護の目的

保護対象システム	保護の目的	所管	概要
受給制御システム	電力供給の維持	送配電事業者	電力使用量と発電量のバランスを維持するための制御システム。 使用量/発電量のバランスが崩れると周波数低下が生じ、結果的に大規模な停電が発生する危険性があることから、極めて重要なシステムに位置づけられる。
系統制御システム	電力供給の維持	送配電事業者	複数の発電所から最も効率的で安定した経路で送配電するための制御システム。 発電所/変電所/送電線を監視/制御するものであり、電力安定供給に直結することから、極めて重要なシステムに位置づけられる。
変電所システム	電力供給の維持	送配電事業者	変電所の制御システム。 超高圧/一時/中間/配電用変電所に区分され、扱う電圧は左から順に下がっていく。特に超高圧変電所は送電の起点となることから重要度が高い。
配電自動化システム	電力供給の維持	送配電事業者	配電線を遠隔地の制御所から監視/制御するシステム。 制御対象のエリアの電力需要が高いほど重要度が高い。
発電所監視制御システム	電力供給の維持	発電事業者	発電所の稼働を監視/制御するシステム。 出力が高いほど停止した場合の影響範囲が広く、重要度が高い。 一方で、一つの発電所が停止した場合も電力融通などにより供給を補うことが可能なため、電力安定供給に与える影響は受給制御/系統制御の方が大きい。
発電所監視制御システム（原子力）	原子力安全の維持	発電事業者	原子力発電所の稼働を監視/制御するシステム。 稼働停止による電力供給への影響に加え、事故発生時の周辺地域への影響が極めて大きいため、重要度が高い。
事務系システム	重要情報の保護、内部不正対策	各事業会社	電力会社の事務系システムの構成は、他業界の企業の事務系システムと概ね同様とみられる。 重要データとしては、顧客情報や関連会社含む経営に関する情報、各種設備の図面情報などが該当する。

2)システム構築やセキュリティ対策製品/サービスの調達における主たる要件と評価事項

導入範囲	要件/評価事項	概要
受給制御システム 系統制御システム 変電所システム 配電自動化システム 発電所監視制御システム	「電力制御システムセキュリティガイドライン」 日本電気技術規格委員会(JESC) 2019 年 7 月改定	左記のガイドラインに準拠して、電力会社とシステム外注を受けたベンダーが具体的な仕様を決定している。 なお、制御系システムはすべてオンプレミス環境で構築されているため、セキュリティ製品もオンプレミス対応のものを利用している。
発電所監視制御システム(原子力)	「原子力発電所におけるサイバーセキュリティ対策導入自主ガイド」 原子力エネルギー協議会(ATENA) 2020 年 3 月発行	左記のガイドラインに準拠して、各事業者はネットワークの外部遮断強化やアクセス管理、マネジメント体制の強化などの安全対策を 2023 年 10 月までに実施する予定となっている。
事務系システム	IPA、JPCERT/CC などが発信するサイバーセキュリティ対策情報、 電力 ISAC などを通じた各社間での情報共有など	他の業界と同様の基準でサイバーセキュリティ対策に取り組んでいる。 なお、サイバーセキュリティ対策の観点から、オンプレミスからクラウドへの移行は慎重にすべきとの見方が多く、一部の企業を除きクラウド活用はあまり進んでいないのが現状とみられる。
全般	一部の国の製品利用を控える、 国内データセンターの利用　など	国産に限定するなどの制限はないが、一部の国(中国/ロシアなど)の製品/サービスの利用を控えているケースが大半とみられる。 また、クラウドを利用する場合は、セキュリティ対策の観点から重要情報の保管は国内データセンターに限定するなどの制限を設けている。

3)国産セキュリティ製品/サービスへの評価

評価	概要
セキュリティ要件を満たす製品/サービスが少ない、存在しない	国内ベンダーが提供するセキュリティ対策製品/サービスはほとんどないため、国内ベンダー製品のみで十分なセキュリティ対策を行うことは難しいのが現状である。

4)今後のビジネス継続におけるセキュリティ面での課題

課題	概要
事務系システムのセキュリティ対策の範囲/レベル/投資規模の決定	一般的にセキュリティ対策には完全な状態が存在しないため、セキュリティ対策の範囲/レベル/投資規模の面で明確な根拠を持って決定することが難しく、どこまで対策すべきかの基準判定が課題となっている。
個社努力でのサイバーセキュリティ対策の限界	現状、社内のセキュリティ対策には十全に取り組んでいるものの、事業に関連する他企業の事情により、十全な対策が実現できないケースも多くある(関連他社においてセキュリティ対策が徹底されていない、など)。 上記に加え、国内全体としてのセキュリティ人材不足などの背景もあり、電力事業者個社としてのサイバーセキュリティ対策には限界がある。 関連省庁からの統一的な見解の提示や、サプライチェーンを含めた業界横断的なサイバーセキュリティ対策支援が望ましい。

5.3.2.ガス業界

1)主な保護対象システムと保護の目的

保護対象システム	保護の目的	概要
プラント制御システム	ガスの安定供給の維持	ガスの製造および、ガス供給ライン圧力/流量の監視やガバナ(圧力調整器)の制御を行う一連のシステム。 安定供給に直結するシステムであることから、極めて重要なシステムに位置づけられる。 一方で、これらの制御システムの停止が即時にガス供給停止につながるわけではない。ガバナの圧力設定機能が機械構造であることから、遠隔制御が不能になった場合でもその時点の設置地が保持されるため、ガス供給は維持される。 同システムは可用性維持を目的として、他の情報系システムやインターネットから分離されているケースが多い。また、ガバナの遠隔制御の通信には専用回線を利用するケースが多いとみられる。 なお、供給制御システムは、運転の自動化と遠隔化による効率向上を目的として導入されるが、供給網が小規模な場合は導入メリットがそれほどないため、中小事業者においては導入していないケースも多い。
供給制御システム		
業務基幹システム	重要情報の保護 内部不正対策	情報系システムの構成は、他業界の企業の事務系システムと概ね同様とみられる。 顧客情報や各種ガス供給設備関連データなどの重要情報を取り扱うため、十全なセキュリティ対策が求められる。
会員サイトなどの 顧客向けシステム	顧客向けサービスの維持 重要情報の保護	同社の利用顧客向けに、各種手続きや会員向け情報提供サービスを提供する各種のシステム。

2)システム構築やセキュリティ対策製品/サービスの調達における主たる要件と評価事項

導入範囲	要件/評価事項	概要
ガス製造および 供給制御システム	「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」 2016 年 7 月改訂 日本ガス協会	左記のガイドラインに準拠して、サイバーセキュリティ対策製品/サービスの導入を決定している。
全般	IPA、JPCERT/CC などが発信するサイバーセキュリティ対策情報、 日本ガス協会や各種関係団体を通じた情報共有	左記の情報共有などをもとに、各種の情報セキュリティ対策を実施している。
	一部の国の製品利用を控える 国内 DC の利用を推奨する	国産に限定するなどの制限はないが、一部の国(中国/ロシアなど)の製品/サービスの利用を控えているケースが大半とみられる。 企業によっては、サポート対応が早いことや、日本語でのサポートが受けられることから、セキュリティ対策製品については国内製品を優先的に導入するケースもある。 また、クラウドを利用する場合は、重要情報の保管は国内データセンターに限定するなどの制限を設けている。

3)国産セキュリティ製品/サービスへの評価

評価	概要
充実/安定したサポート体制、 利用しやすい UI(日本語表記)、 販売/サポート終了などのリスクが低い	前提として、セキュリティ対策製品の選定において、国産/海外産の差が重視されるケースはほとんどないとみられる。 一方で、迅速/充実したサポート体制があることや、UI が利用しやすい点から国産セキュリティ製品の利点とする声もある。特に海外製品のサポートは英語対応が基本のため、特に中小企業などにおいて英語に対応できる人材が少ないケースでは、日本語対応が基本となる国産製品は利用しやすい。 また、言語面での問題のほかに、海外製品は買収などに伴う販売/サポート終了が度々発生するため、その都度製品のリプレース作業をしなければならないなどのリスクが高いとの指摘も多い。

4)今後のビジネス継続におけるセキュリティ面での課題

課題	概要
物理的な制御システムへの攻撃	供給制御システムは外部から分離しているため、インターネットなどの通信を介した攻撃は問題ないが、攻撃者がガバナなどの設備に物理的に接触して危害を加える懸念もあるため、設備の設置個所に入室制限を設けるなどの対策を行っている。
制御系/情報系システムを統括するセキュリティ対策の組織体制整備	現状、全社的なサイバーセキュリティ対策専門部署(CSIRT など)を設置している企業は限られており、システムごとの担当部署が各自でサイバーセキュリティ対策を講じているケースが多いとみられる。 サイバーセキュリティ対策の実施の徹底やインシデント発生時の初動対応の迅速化などを目的として、組織体制の整備が求められている。

5.3.3.金融業界

1)主な保護対象システムと保護の目的

保護対象システム	保護の目的	概要
勘定系システム	銀行業務の維持	預金・為替等の業務処理、勘定処理機能を担う、銀行業務の基幹システム。 サイバー攻撃を受けた場合、金融サービスへの大幅な影響は避けられず、極めて重要なシステムに位置づけられる。 セキュリティ対策の観点から、インターネットなどの外部ネットワークから分離されており、他のシステムとは対外接続系システムを介して接続される。
顧客向け サービスシステム	顧客向けサービスの維持	顧客向けの Web サイトや、オンライン取引に関連する各種サービスシステム。 サイバー攻撃を受けた場合、顧客情報の漏洩や金融サービスへの大幅な影響は避けられず、極めて重要なシステムに位置づけられる。
事務系システム	重要情報の保護 内部不正対策	事務系システムの構成は、他業界の企業と概ね同様とみられる。 顧客情報をはじめとする重要情報の保護のため、十全なセキュリティ対策が求められる。

2)システム構築やセキュリティ対策製品/サービスの調達における主たる要件と評価事項

導入範囲	要件/評価事項	概要
勘定系システム 顧客向けサービスシステム	「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」 (通称:FISC 安全対策基準) 金融情報システムセンター(FISC) 2022 年 12 月改訂	左記ガイドラインに沿って、各社はサイバーセキュリティ対策の要件を決定している。
全般	金融 ISAC を通じた情報共有 IPA、JPCERT/CC などが発信する一般的なサイバーセキュリティ対策情報	その他の事務系システムについては他業種と大きく異なる要件などはないが、IT 化が先行してきた経緯などから、セキュリティ対策の体制などについて他業種と比較して整備が進んでいる。

3）保護対象システムごとのサイバーセキュリティ対策例

保護対象システム	対策例
勘定系システム	・ インターネットからの分離 ・ マイクロセグメンテーションの導入
顧客向け サービスシステム	・ WEB サイトへの DDoS 攻撃対策や WAF の導入 ・ 顧客向けアプリケーションへの FIDO 認証の採用
事務系システム	・ ウイルス対策、メールセキュリティ、EDR、SIEM などの導入 ・ リムーバブルディスクなどの接続の拒否 ・ 業務端末におけるソフトウェアの実行権限の制限 ・ ランサムウェア対策として、定期的なデータのバックアップを実施

4）国産セキュリティ製品/サービスへの評価

評価	概要
サポート面が相対的に優れている	海外ベンダーと比較して、国内ベンダーの製品/サービスは保守/サポート対応相対的に迅速であるなどのメリットがある。
製品/サービスのラインアップが少ない	先述した評価の一方で、セキュリティ製品・サービスは国外の製品も多く流通していると思われるため、国内ベンダーが提供するセキュリティ対策製品/サービスのみに限定した場合、要求を満たす製品が利用できないなど、選択肢が限定されることを懸念している。

5）今後のビジネス継続におけるセキュリティ面での課題

課題	概要
セキュリティ人材不足	金融機関に限らず、社会全体での課題でもあるが、サイバーセキュリティ専門人材の不足やスキルアップが継続的な課題として挙げられる。 各企業における採用活動/人材育成の取り組みだけではなく、育成支援制度などの策定など、国や業界団体主導で何らかの支援があればありがたい。

5.3.4.交通業界

1).主な保護対象システムと保護の目的

(1)鉄道

保護対象システム	保護の目的	概要
列車運行管理システム	列車の安全安定輸送の実現	計画ダイヤをもとに列車の運行を管理する集中制御システム。 サイバー攻撃を受けた場合、安全/安定的な列車運行に大幅に支障が出ることが予測されるため、重要なシステムに位置づけられる。 可用性の維持/セキュリティ対策のため基本的には外部ネットワークから分離されている。 一方で、近年、列車運行情報の共有などを目的として、部分的に情報系システムと接続を行うケースが増加しており、サイバーセキュリティリスクも高まっている。
電力管理システム	車両への安定した 電力供給の実現	車両などに電力供給を行う変電所の監視制御システム。 サイバー攻撃を受けた場合、電力供給の停止による車両や駅設備への影響や設備の破損など、深刻な影響が予測されるため、重要なシステムに位置づけられる。 可用性の維持/セキュリティ対策のため基本的には外部ネットワークから分離されている。

保護対象システム	保護の目的	概要
座席予約システム	列車の安全安定輸送の実現 座席予約サービスの維持	座席指定券の予約や発券を行う情報システム。 サイバー攻撃を受けた場合予約サービスの停止や顧客情報の漏洩などが懸念されるため、保護すべき重要なシステムに位置づけられる。
事務系システム	重要情報の保護 内部不正対策	情報系システムの構成は、他業界の企業の事務系システムと概ね同様とみられる。 制御系システムと接続する場合は、DMZ を設置して情報系システムからの不正侵入を防止するなどの措置をとっている。

(2)航空

保護対象システム	保護の目的	概要
運航システム 整備システム 貨物システム	航空機の安全安定運行の維持	航空機の整備や積み荷の管理など、運航を管理するシステム全般。 サイバー攻撃を受けた場合、離陸前に必要な各種の業務に大幅な支障が出ることが予測され、重要なシステムに位置づけられる。
予約・搭乗システム	航空機の安全安定運行の維持 旅客サービスの維持 顧客情報の保護	航空機の座席予約の管理を行うシステム。 サイバー攻撃を受けた場合旅客機の運用に大幅な支障が発生すると予測され、重要なシステムに位置づけられる。
事務系システム	重要情報の保護 内部不正対策	情報系システムの構成は、他業界の企業の事務系システムと概ね同様とみられる。

2)システム構築やセキュリティ対策製品/サービスの調達における主たる要件と評価事項

(1)鉄道

導入範囲	要件/評価事項	概要
列車運行管理システム 電力管理システム 座席予約システム	「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」 国土交通省 2019 年 3 月改定	左記ガイドラインに沿って、システムの具体的な仕様やサイバーセキュリティ対策製品/サービスの導入を決定している。
全般	IPA、JPCERT/CC などが発信するサイバーセキュリティ対策情報、 交通 ISAC などを通じた各社間での情報共有	左記の情報共有などをもとに、各種の情報セキュリティ対策を実施している。
	一部の国の製品利用を控える、 国内データセンターの利用 など	国産に限定するなどの制限はないが、一部の国(中国/ロシアなど)の製品/サービスの利用を控えているケースが大半とみられる。 また、クラウドを利用する場合は、セキュリティ対策の観点から重要情報の保管は国内データセンターに限定するなどの制限を設けている。
制御系システム	エージェントのインストールを必要としないこと	制御系システムは可用性の維持を最優先事項とするため、可用性に影響を及ぼす懸念のあるエージェントのインストールを必要とするセキュリティ対策ツールの導入については、システム開発を手掛ける外部ベンダーの動作保証外となってしまい、導入が難しいケースが多い。

(2)航空

導入範囲	要件/評価事項	概要
運航システム 整備システム 貨物システム 予約・搭乗システム	「航空分野における情報セキュリティ確保に係る安全ガイドライン」 国土交通省、2019 年 3 月改定	左記ガイドラインに沿って、システムの具体的な仕様やサイバーセキュリティ対策製品/サービスの導入を決定している。
全般	IPA、JPCERT/CC などが発信するサイバーセキュリティ対策情報、 Aviation ISAC、交通 ISAC などを通じた各社間での情報共有	国産に限定するなどの制限はないが、一部の国(中国/ロシアなど)の製品/サービスの利用を禁止しているケースが大半とみられる。
	一部の国の製品利用を控える	一部の国(中国/ロシアなど)の製品/サービスの利用を控えているケースが大半とみられる。

3)保護対象システムごとのサイバーセキュリティ対策例

(1)鉄道

保護対象システム	対策例
列車運行管理システム 電力管理システム	・ インターネットからの分離 ・ 情報系システムとの接続部に DMZ を設置 ・ PC/リムーバブルディスクなどに対するウイルススキャンの実施
情報系システム	・ ウイルス対策、メールセキュリティ、EDR、SIEM などの導入 ・ ランサムウェア対策として、定期的なデータのバックアップを実施

(2)航空

保護対象システム	対策例
運航システム 整備システム 貨物システム	・ インターネット、その他業務システムからのネットワーク分離 ・ クラウドサービスの利用禁止
情報系システム	・ ウイルス対策、メールセキュリティ、EDR、SIEM などの導入 ・ ランサムウェア対策として、定期的なデータのバックアップを実施

4)国産セキュリティ製品/サービスへの評価

評価	概要
製品/サービスのラインアップが少ない	国内ベンダーが提供するセキュリティ対策製品/サービスの製品ラインアップ数が少ないため、価格やセキュリティ要件などの面で海外製品の方が優位となるケースが多い。 現状、政府や業界団体の規制などでは国内製品の導入を義務とするものはないため、今後も規制の内容が大きく変わらない場合は、海外製品優位の状況が続くものとみられる。
一部を除き、優位点はない	日本語の内容に基づいて不正検知を行う内部不正対策などの一部のツールを除き、「国産」であることを理由として優れていると評価できる点はない。 同時に、「国産」であることを理由として海外製品に劣っていると評価できる点もないが、一般的にグローバルで製品展開する海外ベンダーのほうが脅威情報を多く収集できるという点で有利であり、製品の保護性能も高いとの見解である。

5)今後のビジネス継続におけるセキュリティ面での課題

課題	概要
セキュリティ対策の基準、 コスト面での課題	一般的にサイバーセキュリティ対策は完璧と呼べる状態が存在しないため、どの程度の水準までセキュリティ対策を行うべきかどうか、判断の指標に乏しいことが問題となっている。 また、運輸サービスを提供する事業者におけるセキュリティ対策への投資は、顧客に提供するサービスの安定化/向上を図るものであるが、これらの投資による費用負担を運賃などに転嫁すべきか否かなどの問題もある。 適正なセキュリティ対策の水準、かけるべきコストの基準など、妥当性をチェックできるガイドラインなどがあれば参考にしたいとの見解である。
制御系システムの外部接続の増加に伴う、サイバーセキュリティリスクの増大(鉄道分野)	従来、列車運行管理システムや運行管理システムなどの制御系システムは、外部から分離されていることが前提だったが、ユーザー向けに運行情報を Web 上で公開する目的などで、制御系システムと情報系システムを連携するケースが増加しており、外部から侵入されるリスクも拡大している。 一方で、制御系システムの管轄は運用管理の都合上情報系と分離しているケースが多く、かつ外部から分離されてきた歴史的背景から、ユーザー/システム開発ベンダーともに、サイバーセキュリティ対策への意識がそれほど高いとは言えない状況にある。 今後、セキュリティ対策を強化していくにあたっては、制御系/情報系システムの担当部署に加え、システム開発ベンダーとの共同連携が不可欠であり、業界全体として取り組んでいくべき課題である。

5.3.5.情報通信

1)主な保護対象システムと保護の目的

保護対象システム	保護の目的	概要
通信事業用設備システム (通信サービスシステムおよびサービス設備基盤)	通信サービス事業の維持、 可用性の維持	各種の通信サービス/付帯サービスの提供に必要となる設備システム。 システムに障害が発生した場合サービス停止や情報漏洩などが懸念され、保護を必要とする重要システムに位置づけられる。
サービス事業用設備システム (通信以外の付帯サービスシステム)	サービス事業の維持、情報漏洩対策、可用性の維持	
社内業務システム (OA 機器システム)	情報漏洩、機密情報保護、その他	各種社内業務に関連する情報システム。 サイバー攻撃を受けた場合もサービス停止などには直結しないが、企業信頼性やサービス信頼性などの観点から、保護を必要とする重要システムに位置づけられる。

2)システム構築やセキュリティ対策製品/サービスの調達における主たる要件と評価事項

導入範囲	要件/評価事項	概要
通信設備システム サービス設備システム	「電気通信分野における情報セキュリティ確保に係る安全基準」 安全・信頼性協議会 2019 年 12 月改定	左記のガイドラインに準拠して、サイバーセキュリティ対策製品/サービスの導入を決定している。
	「5G セキュリティガイドライン」 総務省 2022 年 4 月発行	
全般	NIST、IPA などが発行する各種ガイドライン/情報発信	左記のガイドラインや情報共有などをもとに、各種の情報セキュリティ対策を実施している。
	ICT-ISAC などを通じた各社間での情報共有など	

3)保護対象システムごとのサイバーセキュリティ対策例

保護対象システム	対策例
通信事業用設備システム （通信サービスシステムおよびサービス設備基盤）	・ セキュリティ対策における事例としては、情報セキュリティ対策や情報管理などの観点から詳細は非開示としている。
サービス事業用設備システム （通信以外の付帯サービスシステム）	
社内業務システム （OA 機器システム）	・ ウイルス対策、メールセキュリティ、EDR、SIEM などの導入 ・ 文書管理ツールの導入による、製品開発データなどの機密情報の保護 ・ ランサムウェア対策として、定期的なデータのバックアップを実施

4)国産セキュリティ製品/サービスへの評価

評価	概要
キャリアグレードに対応していない	プラス/マイナス両面で、国産セキュリティ製品に対する評価は特にない。 通信事業者の場合、導入するシステム、設備やキャリアグレードとなる大量処理、大規模スケール対応など一般企業とは異なる導入基準もあり、こうしたキャリアグレードに対応する国産製品はあまり見られないため、国産製品の導入は難しいのが現状である。

5)今後のビジネス継続におけるセキュリティ面での課題

課題	概要
経済安全保障	経済安保の観点では、法規制や業界ガイドラインなどによる設備調達に関わる規制などが急遽更新されるケースがある。調達設備として、国や業界ガイドラインなどに準じて行くことは重要であるが、事業者によっては設備更新や調達システムの変更など、設備コストの増加を生む要因にもなりえる。
対策の多様化、高度化	フィッシングサイト、フィッシングメール、脆弱な IoT 機器への攻撃、DoS 攻撃、セキュリティ人材と育成、インシデント対応の在り方、セキュリティ啓発、5G ネットワークにおけるセキュリティ対策、大規模イベントに乗じた攻撃への対策など、近年だけでも多くの情報セキュイティリスクが顕在化しており、情報資産保護、ライフラインとして通信サービスを維持するための対策分野は多岐にわたるようになっている。 こうした対策分野へ対応検討や実装、今後の動向を踏まえた対策など情報セキュリティを恒常的に進化させていく努力が必要不可欠となっており、コスト面、人材面など対策を実行するためのコスト、リソースへ課題も大きくなる傾向がある。

5.3.6.半導体

1)主な保護対象システムと保護の目的

保護対象システム	保護の目的	概要
半導体製造システム （半導体製造装置、検査システムなど）	生産ラインの維持 重要データの保護 （半導体回路設計データ/レシピデータ/製造プロセスデータなど）	工場内に構築された、半導体製造に関わる一連のシステム。 サイバー攻撃を受けた場合、半導体製造ラインの停止や半導体設計データの漏洩などの影響が予測されるため、極めて重要なシステムに位置づけられる。 また、半導体工場の設備は非常に高額であるため、設備に損害が生じた場合の経済的損失という観点からも優先的な保護が必要とされる。 サイバーセキュリティ対策を目的として、外部ネットワークから分離されているケースが多いが、企業によっては半導体設計データの共有などを目的として、設計業務を行う情報系システムと接続しているケースも多い。 他の製造業と比較すると各生産設備のネットワーク化/オートメーション化が進んでおり、その分サイバーセキュリティリスクも高い。
情報系システム	重要データの保護 内部不正対策	製造を除いた、各種業務に関連する一連のシステム。 半導体設計データやレシピ、顧客情報などの重要データの漏洩は事業継続や企業信頼に大きく影響するため、十全な保護を必要とする。 製造システムなどの制御系システムと接続する場合は、DMZ を設置することで情報系から制御系システムへの不正な侵入を防止している。

2)システム構築やセキュリティ対策製品/サービスの調達における主たる要件と評価事項

導入範囲	要件/評価事項	概要
半導体製造システム	「SEMI Standards」 国際半導体製造装置材料協会(SEMI)発行 「SEMI E169」 →半導体製造装置及びシステムの情報セキュリティのための規格。 「SEMI E187」 →半導体製造に関わるデータの保護を目的としたファブ装置(半導体製造装置)のサイバーセキュリティ規格。 「SEMI E188」 →工場内システムへのマルウェア感染を予防することを目的とした装置規格。	左記の国際標準規格「SEMI Standards」で定められた、情報セキュリティに関する規格に準拠してセキュリティ対策に取り組んでいる。
制御系システム全般	IEC (ISA) 62443 シリーズ、 NIST SP 800-82 など	その他、IEC などの国際標準規格や、NIST 発行の OT セキュリティ向けガイドラインなどに準拠して制御系システム全般のセキュリティ対策に取り組んでいる。
制御系システム全般	エージェントのインストールを必要としないこと	制御系システムは可用性の維持を最優先事項とするため、可用性に影響を及ぼす懸念のあるエージェントのインストールを必要とするセキュリティ対策ツールの導入については、システム開発を手掛ける外部ベンダーの動作保証外となってしまい、導入が難しいケースが多い。
情報系システム	IPA、JPCERT/CC などが発信する一般的なサイバーセキュリティ対策情報	情報系システムについては、他業種と同様の基準でサイバーセキュリティ対策に取り組んでいる。

3)保護対象システムごとのサイバーセキュリティ対策例

保護対象システム	対策例
半導体製造システム (半導体製造装置、 検査システムなど)	・ 情報系システムとの接続部に DMZ を設置 ・ 工場内 NW のセグメンテーションと、FW による境界防御 ・ 工場内 NW の可視化、SOC による監視/異常検知 ・ 工場内に持ち込む PC/リムーバブルディスクなどに対するウイルススキャンの実施
情報系システム	・ ウイルス対策、メールセキュリティ、EDR、SIEM などの導入 ・ 文書管理ツールの導入による、製品開発データなどの機密情報の保護 ・ ランサムウェア対策として、定期的なデータのバックアップを実施

4)国産セキュリティ製品/サービスへの評価

評価	概要
Web フィルタリングツールなどの一部の製品は、海外産より精度が高い	国産セキュリティ製品の優位点としては、日本国内企業での利用に適している点が挙げられる。 特に Web フィルタリングツールなどは、Web サイト上のコンテンツの内容によってアクセス可否を判定するものであるため、海外製品よりも国産製品のほうが高い精度を有するといった優位点がある。 その他、UI/サポートが日本語であるなどの違いはあるが、製品産地を理由とする機能面での優劣はない。

5)今後のビジネス継続におけるセキュリティ面での課題

課題	概要
制御系システムのセキュリティ対策	今後、業務効率化や製造データ利活用を目的として、制御系システム側にもクラウドサービスなどの導入や事務系システムとの連携が進んでいくものとみられ、さらなるサイバーセキュリティ対策の高度化が求められる。 一方で、可用性が最優先事項である制御系システムでは、セキュリティ対策製品を導入することで制御機器の応答時間が遅延するなどの懸念から、導入した場合はシステム開発ベンダーの補償対象外となるなど、製品導入が進まない現状があり、今後は制御系システムを開発提供する外部ベンダーなどを含めて、業界全体でサイバーセキュリティ対策に取り組んでいく必要がある。

5.3.7.医療機器

1)主な保護対象システムと保護の目的

保護対象システム	保護の目的	概要
工場制御系システム	重要情報の保護 生産ラインの維持	工場内に構築された、医療機器製造に関わる一連のシステム。 サイバー攻撃を受けた場合、生産ラインの停止や機密情報の漏洩などの影響が懸念されるため、保護すべき重要なシステムに位置づけられる。 他の製造業と同様にインターネットや情報系システムと分離して構築することが従来は多かったが、近年データ利活用などを目的として、外部ネットワークとつながるケースが増えている。
情報系システム	重要情報の保護 内部不正対策	研究開発などの業務全般に利用されるシステム群。 重要情報としては各種設計データや顧客情報などが該当し、一般的な企業と同様に保護すべきシステムとして位置づけられる。
製造する医療機器	製造する医療機器の有効性および安全性の確保	医療機器の中でも、他の機器やネットワークと接続して利用されるものについては、外部からの不正なアクセスによる機能停止や、サイバー攻撃の踏み台として悪用されてしまうなどのリスクがあることから、セキュリティ対策が求められる。

2)システム構築やセキュリティ対策製品/サービスの調達における主たる要件と評価事項

導入範囲	要件/評価事項	概要
工場制御系システム 製造する医療機器	「Principles and Practices for Medical Device Cybersecurity」 (通称:IMDRF ガイダンス) 国際医療機器規制当局フォーラム(IMDRF) 2020 年 3 月発行	医療機器製造の分野においては、左記のガイドラインや手引書に沿って、サイバーリスクが懸念される医療機器のサイバーセキュリティの確保に向けた、セキュリティ対策の設計/導入を行っている。
	「医療機器のサイバーセキュリティの確保及び徹底に係る手引書」の別添である「販売製造業向け手引書」 厚生労働省 2021 年 12 月発行	
	「医療機器のサイバーセキュリティの確保に関するガイダンス」 厚生労働省 2018 年 7 月発行	
製造する医療機器	「IoT セキュリティガイドライン」 総務省/経済産業省 2016 年 7 月発行	
情報系システム	IPA、JPCERT/CC などが発信するサイバーセキュリティ対策情報	左記の情報などをもとに、各種の情報セキュリティ対策を実施している。

3)保護対象システムごとのサイバーセキュリティ対策例

保護対象システム	対策例
工場制御系システム	・ 情報系システムとの接続部に DMZ を設置 ・ 工場内 NW のセグメンテーションと、FW による境界防御 ・ 工場内 NW の可視化、SOC による監視/異常検知 ・ 工場内に持ち込む PC/リムーバブルディスクなどに対するウイルススキャンの実施
情報系システム	・ ウイルス対策、メールセキュリティ、EDR、SIEM などの導入 ・ ランサムウェア対策として、定期的なデータのバックアップを実施
製造する医療機器	・ 医療機器開発における、脆弱性診断ツール/脆弱性診断サービスの利用 ・ 販売製品の脆弱性に関する情報収集/顧客への発信、対応窓口の設置

4)国産セキュリティ製品/サービスへの評価

評価	概要
特になし	国産/海外産を基準としてセキュリティ製品の選定を行うことはなく、各種ガイドラインや法規制に沿って、要件を満たすセキュリティ製品の導入を行う企業が大半とみられる。

5)今後のビジネス継続におけるセキュリティ面での課題

課題	概要
OT 分野における サイバー攻撃被害の増加	社会の高度情報化が進む中で、サイバー攻撃による被害件数が増加しており、医療分野においても、病院システムや医療機器を標的とした被害事例が発生するなど、サイバーセキュリティ上のリスクが高まっている。 制御系システムの領域では、近年データ利活用を目的として、多くの設備装置がインターネットに接続されるようになっており、利便性が向上する半面、工場内の機密情報の漏洩やデータ改ざん、不正アクセスによる製造ライン停止などのサイバー攻撃のリスクが増大している。

5.4.まとめ

業界	保護対象システム	保護目的	要件	国産製品への評価	課題
電力	・受給制御システム ・系統制御システム ・変電所システム ・配電自動化システム ・発電所監視制御システム ・発電所監視制御システム（原子力） ・顧客向けサービスシステム	・電力供給維持 ・原子力安全確保	・「電力制御システムセキュリティガイドライン」 ・「原子力発電所におけるサイバーセキュリティ対策導入自主ガイド」	・セキュリティ要件を満たす製品/サービスが少ない、存在しない	・事務系システムのセキュリティ対策の範囲/レベル/投資規模の決定が難しい ・個社努力でのサイバーセキュリティ対策の限界
ガス	・プラント制御システム ・供給制御システム ・顧客向けサービスシステム	・ガスの安定供給の維持 ・顧客向けサービスの維持 ・重要情報の保護	・「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」	・充実/安定したサポート体制 ・利用しやすい UI(日本語表記) ・販売/サポート終了などのリスクが低い	・物理的な制御システムへの攻撃 ・制御系/情報系システムを統括するセキュリティ対策の組織体制整備
金融	・勘定系システム ・顧客向けサービスシステム	・銀行業務の維持 ・顧客向けサービスの維持	・「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」	・サポート面が相対的に優れている ・製品/サービスのラインアップが少ない	・セキュリティ人材不足
交通(鉄道)	・列車運行管理システム ・電力管理システム ・座席予約システム	・列車の安全安定輸送の実現 ・車両への安定した電力供給の実現 ・列車の安全安定輸送の実現 ・座席予約サービスの維持	・「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」	・製品/サービスのラインアップが少ない ・一部を除き、優位点はない	・セキュリティ対策の基準、 ・コスト面での課題 ・制御系システムの外部接続の増加に伴う、サイバーセキュリティリスクの増大
交通(航空)	・運航システム ・整備システム ・貨物システム ・予約・搭乗システム	・航空機の安全安定運行の維持 ・航空機の安全安定運行の維持 ・旅客サービスの維持 ・顧客情報の保護	・「航空分野における情報セキュリティ確保に係る安全ガイドライン」		・セキュリティ対策の基準、 ・コスト面での課題
通信	・通信事業用設備システム ・サービス事業用設備システム	・通信サービス事業の維持、 ・可用性の維持 ・サービス事業の維持、情報漏洩対策、可用性の維持	・「電気通信分野における情報セキュリティ確保に係る安全基準」 ・「5G セキュリティガイドライン」	・高速/大量処理、安定性などのキャリアグレードに対応していない	・経済安全保障 ・対策の多様化、高度化

業界	保護対象システム	保護目的	要件	国産製品への評価	課題
製造（医療機器）	・ 工場制御系システム ・ 製造する医療機器	・ 重要情報の保護 ・ 生産ラインの維持 ・ 製造する医療機器の有効性および安全性の確保	・「Principles and Practices for Medical Device Cybersecurity」 ・「医療機器のサイバーセキュリティの確保及び徹底に係る手引書」の別添である「販売製造業向け手引書」 ・「医療機器のサイバーセキュリティの確保に関するガイダンス」 ・「IoT セキュリティガイドライン」	・ 特になし	・ OT 分野におけるサイバー攻撃被害の増加
製造（半導体）	・ 半導体製造システム	・ 生産ラインの維持 ・ 重要データ（半導体回路設計データ/レシピデータ/製造プロセスデータ など）の保護	・「SEMI Standards」 ・（SEMI E169/E187/E188 など）	・ Web フィルタリングツールなどの一部の製品は、海外産より精度が高い	・ 制御系システムのセキュリティ対策
業界共通	・ 事務系システム全般	・ 重要情報の保護 ・ 内部不正対策	・ IPA、JPCERT/CC などが発信する一般的なサイバーセキュリティ対策情報 ・ 各業界 ISAC を通じた情報交換 ・ 一部の国の製品利用を控える ・ 国内DC利用を推奨する	—	—
	・ 制御系システム全般	・ 可用性の維持	・ IEC 62443 シリーズ、NIST SP 800-82 など ・ 各業界 ISAC を通じた情報交換 ・ 一部の国の製品利用を控える ・ エージェントのインストールを必要としないこと		

5.5.考察

ポイント	概要
・ 国産セキュリティベンダー利用に向けた課題	・ 各業界ともに業界サイバーセキュリティガイドラインを参照し対応するなかで、国産セキュリティベンダーを排除する意向はないものの、対策要件に合致するベンダー、製品が少ない、コスト面、機能面で選定条件とならないなどのケースがみられる。 ・ ガイドライン準拠においても、対策要件や範囲などの明示が少なく個社独自判断であることと対策への投資、意欲などの温度差がみられ、業界統一的な対策が不明瞭であり、対策製品などの選定が個社に依存するなどケースがみられる。 ・ ユーザーにおいては、世界的なデファクトやコスト、機能優位性などが優先されるため、国産ベンダーの強みや優位性であるサポート力や信頼性などの訴求点が薄れるケースもあり、対策として長期運用、安定稼働などの視点に立った対策を促す取り組みが求められる。

ポイント	概要
・ 国産セキュリティベンダー利用に向けた取り組み	・ 守るべきシステムとして業務システムなど IT に近い領域では、海外などメジャーブランドが主流であり、価格面、機能面などから国産セキュリティベンダーの優位性は低い。一方で、制御システムにおける末端のフィールドネットワークにおいては、独自プロトコルでの運用も多いため国産セキュリティベンダーが選択される可能性が高い。 ・ 経済安全保障の観点からも、各業界の制御システムフィールドネットワークにおいては、設備機器の組み込みやファームウエアは国産製品などによる信頼性確保が望まれるほか、導入製品において、長期の運用やサポート対応など制御システムの可用性を確保するための取り組みが必要と考えらえる。 ・ 海外ベンダー製品を利用した場合、ベンダーの国内撤退、製品供給の終了などのリスクが潜在的にみられ、SI ベンダーを含めた国産セキュリティベンダーによる長期かつ安定的な供給体制、サポート体制を強みとした事業優位性を訴求することができる。 ・ 制御システムにおいては、IT とは異なる長期運用などがシステムとして要求されるため、国産セキュリティベンダーとして、こうした電力やガス業界などに対し、制御システムセキュリティ対し長期での運用やサポート保証など、事業継続を意識したビジネスを展開することにより、海外ベンダーとの差別化や独自ビジネスとしての海外ベンダーと伍することができると考えられる。 ・ 制御システムのうちフィールドネットワークなど末端に近いシステムについては、独自プロトコル利用や日本独自仕様も存在するなかで、これらシステムを長期かつ安定的に運用するための基盤技術やサービス開発を行っていくことで、国産ベンダーとしての差別化など、海外ベンダーとの優位性を発揮できる事業モデルが想定され、こうしたユーザー動向や技術開発、サービスニーズについては、次回以降の調査分野として明確化することも必要であると考えらえる。

6.IoT 検証機器事業者総括

6.1.機器検証事業実績（提供状況）

1)市場定義(IoT デバイス脆弱性検査サービス)

IoT デバイス自体の脆弱性検査や診断、セキュリティ耐性の検査などを行う、IoT デバイス脆弱性検査サービスを対象とした。

IoT デバイスのセキュリティ対策では、デバイスの開発段階からもセキュリティ耐性に関する検査を実施することが求められており、多様化するデバイスとそのシステムの脆弱性を診断、検査するサービスとしての提供が進められている。

なお、IoT デバイス製造事業者の独自診断や専用ツールを用いた内製での検査は対象外とした。

6.2.市場規模推移

図表 28「市場規模推移_IoT デバイス脆弱性検査サービス」

単位：百万円、%

摘要＼年度		2020 実績	2021 見込	2022 予測	2023 予測	2024 予測	2027 予測	CAGR 27/20
金額		3,200	4,200	5,200	6,100	7,000	11,000	19.3
	前年比	－	131.3	123.8	117.3	114.8	-	

（富士キメラ総研推定）

近年、工場やコネクテッドカー、重要インフラなどの分野で、制御機器などの各種デバイスをネットワークに接続して制御やデータ収集に活用するケースが増加しており、それに伴い IoT デバイスに対するサイバー攻撃のリスクも高まっている。

こうした状況下で、IoT デバイス自体のセキュリティ対策を強化する取り組みが IoT デバイス製造業者に対して求められており、製品出荷に際しての品質チェックとして当該サービスによりセキュリティ対策を行うケースや、開発の設計段階から当該サービスによる評価を行い、セキュリティ耐性を考慮した製品設計を行うといった取り組みが増加しており、市場を拡大させる要因となっている。

図表 29「市場占有率_IoT デバイス脆弱性検査サービス」

単位：百万円

摘要＼企業名	2020 年度 実績	2020 年度 市場占有率	2021 年度 実績	2021 年度 市場占有率
ベリサーブ	500	15.6	650	15.5
ラック	300	9.4	400	9.5
GMO サイバーセキュリティ by イエラエ	200	6.3	400	9.5
FFRI	100	3.1	150	3.6
サイバートラスト	100	3.1	200	4.8
その他	2,000	62.5	2,400	57.1
合計	3,200	100.0	4,200	100.0

（富士キメラ総研推定）

6.3.IoT 検証事業者の対象ヒアリング選定基準

1：参考資料_IoT 機器検証事業者基礎データをもとに、上位ベンダー3 社を主要参入事業者として抽出し、対象企業として選定した。

2：主要参入企業以外の取り組みを把握する目的として、設立早期の企業であることや企業特徴として、大学発ベンチャー企業、技術コンテストなどで入賞実績を持つ技術系企業などを選定して対象企業とした。

6.4.今後注力する検証対象分野の見解、今後の注力領域、ガイドラインへの見解

＜.IoT 検証事業者の事業区分と検証事業概要＞

摘要	既存ビジネス派生型	ベンチャー企業/技術系企業
対象企業名	・GMO サイバーセキュリティ by イエラエ ・ベリサーブ ・ラック	・Flatt Security ・リチェルカセキュリティ
当該事業特性	・他の既存セキュリティサービス事業を展開 ・当該サービス含めた顧客基盤を持つ ・他サービスを含めた事業ノウハウを持つ	・コンサルなど類似事業からサービス事業を展開 ・既存顧客基盤は限定的 ・専門性や技術優位を訴求した展開
対象とする産業・機器	・自動車や車載機器を対象 ・その他としては、医療機器や家電、ドローンなどの多種多様の IoT デバイス	・自動車や車載機器を対象 ・依頼される案件ベースで対応
検証手法、ツール類/検証期間	・診断ツールとエンジニアの双方で診断 ・おおよそ 2 か月から 3 か月が標準、自動車メーカーに対しては年単位の長期対応も実施	・診断ツールとエンジニアの双方で診断 ・おおよそ2か月から3か月が標準、短期での対応もある
今後の注力分野	・自動車産業が中心 ・自動車については、検証すべき対象拡大、法規制によってはサービス提供範囲も拡大し Tire2 以下における案件の増加も期待	・自動車産業が中心 ・自動車については、検証すべき対象拡大、法規制によってはサービス提供範囲も拡大し Tire2 以下における案件の増加も期待
注力するうえでの課題	・人材不足については、慢性的な課題 ・高度技術を有する人材の確保や育成などに向けた課題解決が事業強化に直結	・人材不足については、慢性的な課題 ・営業面、顧客開拓の面においては、スタートアップ企業などでは営業リソースを多く持てない、人材を割けないなどの課題
政府施策的課題	・意識向上、啓蒙活動は、間接的に検証、診断サービス事業へとつながる ・業界標準的基準を設けることで、最低限の検証を実施する素地を醸成	・意識向上、啓蒙活動は、間接的に検証、診断サービス事業へとつながる ・業界標準的基準を設けることで、最低限の検証を実施する素地を醸成
現状のガイドラインなどに関する見解	・北米、欧州などで出されるガイドライン、法規制対応などを重視するケースが多い ・「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き（赤）」については、参考としている意見は少数	・北米、欧州などで出されるガイドライン、法規制対応などを重視するケースが多い ・「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き（赤）」については、参考としている意見は少数
海外での取り組み	・現状のサービスリソースを考慮すると国内ユーザー案件に対応することが限界 ・国内に限定した方針ではなく、長期的に海外現地ユーザーを含めてサービス提供を展開していく意向、計画などもみられる	・現状のサービスリソースを考慮すると国内ユーザー案件に対応することが限界 ・国内に限定した方針ではなく、長期的に海外現地ユーザーを含めてサービス提供を展開していく意向、計画などもみられる

6.5.考察

ポイント	概要
・ IoT 機器検証の必要性や有用性の認知向上に向けた課題	・ IoT 機器検証については、インターネットにつながる“モノ”が増加するなかで、脅威低減やリスク対策として製品投入における必要な対策であるが、この点について、脅威、リスクへの認識不足や対策コスト負担などの面で実施していない企業も多くみられる。 ・ 製品の安全性や品質向上として IoT 機器検証の必要性や有用性を製品メーカーに広く浸透させ、安心安全な IoT 機器の活用を促進していく活動が求められる。
・ IoT 機器検証の普及に向けた取り組み	・ 現状 IoT 機器検証は自動車分野向けを中心に市場や需要を拡大させている。その背景としては、WP29 など国際規格においてデバイス安全性の確保が求められるなど、安全基準として検証などのセキュリティ対策実装が求められている点が挙げられる。 ・ 国際規格や業界ガイドラインなどにおいて、IoT 機器検証などのセキュリティ対策を推奨していくことで、製品安全性や信頼性、品質向上の有効な手段として活用されることで検証ビジネスの拡大が期待できる。 ・ また、IoT 機器検証においては、実施することでの有用性、効果などが不明瞭なケースがあり、実施に至らないケースもみられる。こうしたケースについては、検証を実施した証明による品質保証など第三者評価としての取り組みも需要拡大に向けた施策として想定される。 ・ このほか中小企業に向けた検証事業の実証実験などの実施は、ユーザーの裾野拡大や検証事業を認知させる機会につながるとの評価も多く、こうした国策として需要層を拡大させ取り組みや検証事業およびサービス認知の向上につながる取り組みは、当該ビジネスを活性化させる一助になるものと考えられる。

7.総括

セキュリティ市場規模推移		
2021 年度	⇨	2027 年度
577,930 百万円		866,700 百万円

市場拡大要因	
想定される脅威	想定される対策
・ 新しい DX システムへの攻撃 ・ IoT 環境から IT 領域への攻撃 ・ クラウドや Web サービスへの攻撃増加 ・ テレワーク定着によるなりすましの増加 ・ 国際情勢の変化から国内の重要インフラや重要産業への攻撃拡大	・ セキュリティ演習によるインシデント発生後の対処 ・ Web アプリケーション脆弱性診断やクラウドセキュリティによる新しいシステムのセキュリティ強化 ・ 端末管理ツールを活用したサイバーハイジーンによる社内攻撃対象となるデバイス管理。 ・ IDaaS による認証強化、なりすまし防止 ・ SOAR、UEBA を活用したセキュリティの自動化対応

より影響の大きいとみられる重要インフラ/産業	
重要インフラ	・ 情報通信 ・ 金融 ・ 交通(航空/電車) ・ 電力 ・ ガス
製造業	・ 自動車 ・ 半導体 ・ 医療機器 ・ 医薬品

注目セキュリティ
・ モバイルアプリ検査サービス ・ EDR 運用支援サービス ・ サイバーセキュリティ演習サービス ・ スレットインテリジェンスサービス ・ Web アプリケーション脆弱性検査サービス ・ セキュリティ/BCP コンサルティングサービス ・ Web フィルタリングツール ・ IDaaS ・ 端末管理・セキュリティツール(統合エンドポイント管理ツール) ・ クラウドセキュリティ

現在のセキュリティ関連の取り組み
・ より強固なセキュリティ対策を実施するため、外資系ベンダーのセキュリティツールの利用が多く、国産ベンダーのセキュリティツール利用は限定的。 ・ 各省庁や ISAC などのガイドラインに準拠した取り組みを進めているが、ガイドラインは方向性のみ示すケースも多く、具体的な指示がないためどのレベルまで対策を実施するか不明瞭である。 ・ OT と IT がつながるケースが増えており、セキュリティのカバー範囲は広がっているが、統制が取れていないケースもみられた。

市場拡大における課題
・ 表彰や認定制度を拡充し、国産ベンダーが営業展開しやすい環境整備 ・ ユーザーのセキュリティ投資拡大に向け、セキュリティに関するガイドラインや法規制を策定やセキュリティ投資全体における啓蒙 ・ ユーザー、ベンダー双方でセキュリティ人材が不足しており、セキュリティへの取り組みを支援するためのセキュリティ人材育成 ・ セキュリティ投資をなかなか増やせない中堅、中小企業へのセキュリティ投資における資金援助