

2019年12月26日

株式会社 富士キメラ総研  
〒103-0001 東京都中央区日本橋小伝馬町  
1番5号 PMO 日本橋江戸通  
TEL. 03-3664-5839 FAX. 03-3661-1414  
<https://www.fcr.co.jp/>

広報課 TEL. 03-3664-5697  
<https://www.fuji-keizai.co.jp/press/>

## 法人向けのネットワークセキュリティ製品・サービス市場を調査

既存セキュリティニーズ増加に加え、クラウド、IoT、5G、サプライチェーン攻撃対応が拡大に寄与  
2023年度の市場は6,617億円（2018年度比31.9%増）

—注目市場 2023年度予測（2018年度比）—

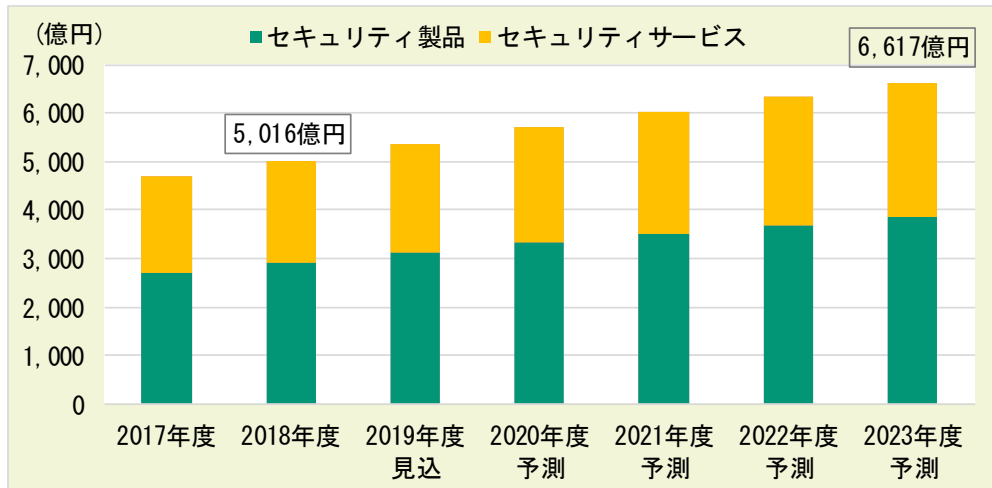
●CASB 100億円（6.7倍）～利用が拡大するクラウドのセキュリティ対策として導入進む～

マーケティング&コンサルテーションの株式会社富士キメラ総研（東京都中央区日本橋小伝馬町 社長 田中 一志 03-3664-5839）は、標的型攻撃やランサムウェア、サプライチェーン攻撃など次々に登場する新たな脅威や高度化／複雑化する脅威への対策として継続的な対応が求められる一方で、クラウドやIoTの利用拡大による新しい需要の創出も期待される法人向けのネットワークセキュリティ製品・サービスの国内市場を調査した。その結果を「[2019 ネットワークセキュリティビジネス調査総覧 市場編](#)」および「[\(同\) 企業編](#)」にまとめた。

市場編ではセキュリティ製品26品目、セキュリティサービス18品目の市場を分析し、将来を展望した。企業編ではセキュリティソリューションプロバイダー29社、セキュリティツールベンダー21社の分析を行った。

<調査結果の概要>

■法人向けネットワークセキュリティ製品・サービスの国内市場



法人向けネットワークセキュリティ製品・サービスの国内市場は、標的型攻撃やランサムウェア、サプライチェーン攻撃など次々に登場する新たな脅威や高度化／複雑化する脅威への対策として継続的な対応が求められることから、継続的な拡大が予想される。一方で、高度なセキュリティサービスの需要増加、サービス案件の増加などにより提供事業者側の技術者が不足しており、需要に対応しきれない状況が続いている。

セキュリティ製品は、クラウド型セキュリティ製品やサービス基盤向け製品の需要が好調である。今後はセキュリティシステム環境の内製化が大手企業を中心に進むとみられることから、堅調な拡大が予想される。

セキュリティサービスは、高度なセキュリティ運用に対する強いニーズがあるが、提供事業者側の技術者不足や、セキュリティ製品のクラウド化などにより、セキュリティ製品と比較し伸び率は低くなるとみられる。

今後既存のセキュリティニーズの増加に加え、クラウドやIoT、5Gなどの活用によるセキュリティ需要の創出、新たな脅威となっているサプライチェーン攻撃の対応として取引先を含めたサプライチェーン全体でのセキュリティ強化などが、今後の市場拡大に寄与するとみられる。特にクラウド、IoT、サプライチェーン攻撃対応による新規需要は2023年度でそれぞれ200億円以上と予測される。

クラウドでは社内外問わず業務を行えるなどシステムの稼働環境が変化するため、それに対応するセキュリティ対策が必要となる。クラウド向けセキュリティ対策ツールCASBの台頭や、シングルサインオン、ワンタイムパスワードなど認証を強化する動きが活発化している。また、クラウドと相性の良いセキュリティ製品・サービスの需要が増加している。

IOTではデバイスがネットワークに接続されることで生まれるリスクへの対策が必要となる。ネットワークを守るUTM関連製品やセキュリティ監視ツールをはじめ、ネットワークに接続される端末数が大幅に増加することから個々のデバイスを防御する端末セキュリティ製品や、認証するための電子認証サービス、IoT専用の産業用制御システム／組み込み型セキュリティ製品の利用が拡大するとみられる。

サプライチェーン攻撃対策では、大手企業からグループ会社や取引先へのセキュリティ強化要請により、基本的なセキュリティ対策製品・サービスであるウイルス監視サービスやウイルス対策ツール、ファイアウォール・UTM関連製品、メールセキュリティサービスなどの導入が中堅、中小企業で増加するとみられる。また、セキュリティリテラシーの向上を目的とした教育サービスの拡大なども期待される。

#### <注目市場>

##### ●CASB (Cloud Access Security Broker)

2018年度	2023年度予測	2018年度比
15億円	100億円	6.7倍

CASBは、利用状況の監視、データ漏えい防止、コンプライアンス監査、セキュリティ脅威への防御などを行うクラウド向けセキュリティ対策ツールである。

働き方改革の一環として、テレワークなどの新しい勤務形態の導入や負担軽減を目的としたクラウドへの移行が増えている。クラウドにより社外での情報共有が容易となる一方で、誤った設定による機密情報の公開、不正アクセスによる情報流出、従業員によるデータ持ち出しなどへの対策の必要性が増しており、このようなセキュリティの課題を解決するソリューションとしてCASBが注目されている。

2018年度は複数のクラウドサービスを利用し、利用状況の把握やシステムの管理に課題を抱える企業を中心に導入が進んだ。2019年度は新規導入だけでなく、部分的な導入後の全社導入や、機能の追加導入など既存ユーザーの拡張が増えており、安全なクラウドを実現するためのツールとして、今後大幅な拡大が予想される。

##### ●EDR (Endpoint Detection and Response)

2018年度	2023年度予測	2018年度比
67億円	217億円	3.2倍

脅威の侵入後対策を目的にエンドポイントを監視し、不審な挙動を調査・検知するツールを対象とした。機能としては、攻撃／感染経路の特定、端末／ネットワーク情報の記録、管理者によるリモートコントロール、マルウェア感染以前の状態へのシステム復旧などがある。

これまでネットワークに接続された端末などエンドポイントのセキュリティとしては、侵入前の対策に重点が置かれており、アンチウイルスやふるまい検知などの標的型攻撃対策ツールが需要の中心であった。しかし、高度化する脅威の侵入を完全に防ぐことは難しいことから、侵入後の対策が重要となってきている。

経済産業省が提唱してきた「サイバーセキュリティ経営ガイドライン」が2017年11月に改訂され、侵入後の対策への取り組みが広く認知されたことから、超大手、大手企業を中心に導入が進み、2018年度、2019年度と市場は急拡大している。

##### ●メール標的型攻撃訓練サービス

2018年度	2023年度予測	2018年度比
21億円	36億円	171.4%

類似的な攻撃メールを送付し、メール標的型に対する訓練を実施するサービスを対象とした。

2017年に取り沙汰されたビジネスメール詐欺によって需要が喚起され、市場拡大につながった。標的型メール攻撃は日々高度化／多様化しており、不審なメールは開封しないと意識づけや開封後の適切で迅速なインシデント対応など、継続した従業員教育の徹底、組織としての体制強化が重要となっている。

安定した更新需要に加え、サプライチェーン攻撃対策として中堅、中小企業を中心に新規需要獲得も期待され、拡大が続くとみられる。

●サイバー保険

2018年度	2023年度予測	2018年度比
135億円	190億円	140.7%

サイバー保険は、サイバー攻撃による損害賠償、費用損害、逸失利益などをカバーする法人向け保険であり、算出はサイバー保険事業者の保険料収入とした。

2011年頃に外資系保険会社によりサービス化されたが、IT分野において保険サービスの明確なメリットが認知されていなかったことから市場は低迷していた。しかし、標的型攻撃など特定企業を狙ったサイバー攻撃の増加やマルウェアによる事業機会の喪失・損害などがメディアなどで大きく取り上げられたことや、個人情報保護法による企業責任の明確化により、サイバー保険に対する見方や意識が変わり、市場は拡大している。

情報漏えいにおける損害賠償や訴訟費用の増加、サイバーインシデントによる利益損害など被害は甚大なことや法規による罰則強化なども進められており、市場は安定的に拡大していくとみられる。

<調査対象>

セキュリティ製品		
・DDoS攻撃対策ツール	・Webアプリケーションファイアウォール	・ワンタイムパスワード
・ウイルス対策ツール	・Webセキュリティツール	・EDR
・検疫ツール	・Webフィルタリングツール	・端末管理・セキュリティツール
・セキュリティ監視ツール	・セキュリティ検査ツール	・モバイルセキュリティ管理ツール
・標的型攻撃対策ツール	・CASB	・産業用制御システム／組み込み型セキュリティ製品
・ファイアウォール／VPN／UTM関連製品	・シングルサインオン	・データベースセキュリティ
・電子メールアーカイブツール	・デバイス認証ツール	・統合ログ管理ツール (SIM/SIEM)
・メール暗号化／メール誤送信対策ツール	・統合ID管理ツール	
・メールフィルタリングツール	・特権ID管理ツール	
	・認証デバイス	
セキュリティサービス		
・DDoS攻撃対策サービス	・電子認証サービス	・セキュリティ教育・トレーニングサービス
・ウイルス監視サービス	・DaaS	・セキュリティ検査・監査サービス
・統合セキュリティ監視サービス	・CSIRT構築支援サービス	・セキュリティ／BCPコンサルティングサービス
・不正アクセス監視サービス	・SIEM運用管理サービス	
・メールセキュリティサービス	・インシデントレスポンスサービス	
・WAF運用管理サービス	・サイバーセキュリティ演習サービス	・メール標的型攻撃訓練サービス
・Webアプリケーション脆弱性検査サービス	・サイバー保険	

<調査方法>富士キメラ総研専門調査員によるヒアリングおよび関連文献、データベース活用による調査・分析

<調査期間>2019年6月～10月

以上

資料タイトル :	<a href="#">「2019 ネットワークセキュリティビジネス調査総覧 市場編」</a> <a href="#">「2019 ネットワークセキュリティビジネス調査総覧 企業編」</a>	
体 裁 :	A4判 市場編 298頁 企業編 316頁	
価 格 :	書籍版 各150,000円+税 書籍／PDF版セット 各170,000円+税 ネットワークパッケージ版 各300,000円+税	
発 行 所 :	株式会社 富士キメラ総研 〒103-0001 東京都中央区日本橋小伝馬町1番5号 PMO日本橋江戸通 TEL:03-3664-5839 (代) FAX:03-3661-1414 URL:https://www.fcr.co.jp/ e-mail:info@fcr.co.jp	
調 査 ・ 編 集 :	第二部 TEL:03-3664-5839 FAX:03-3661-1414	
この情報はホームページでもご覧いただけます。 URL: <a href="https://www.fuji-keizai.co.jp/press/">https://www.fuji-keizai.co.jp/press/</a>		