

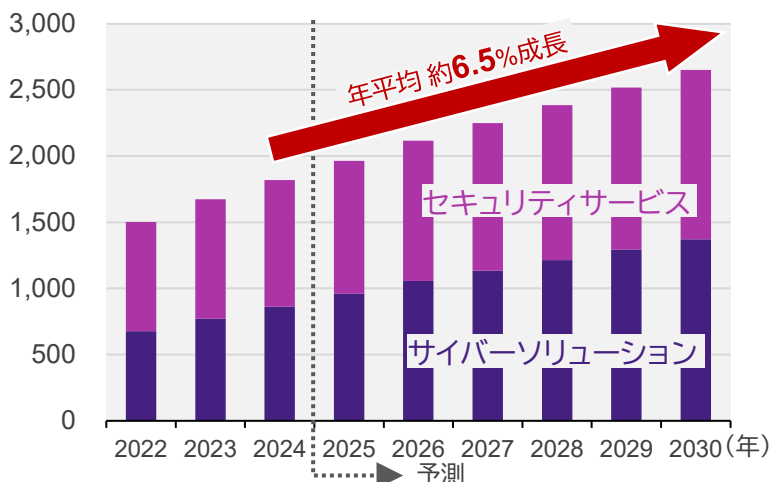
- サイバーセキュリティとは、IT機器やネットワーク、情報をサイバー攻撃や情報漏えいの脅威から守るための総合的な取り組みのことです。
- 主な領域には、ネットワークやアプリケーション、クラウド、データ、エンドポイント(PCやスマートフォン等)などが含まれます。
- インターネットの普及に伴い、生活面だけでなく、企業の業務活動でもデジタル化が進んだ結果、サイバー攻撃への対応はこれまで以上に重要となっています。

世界のサイバーセキュリティ市場

- デジタル技術の進化によりビジネスモデルが発展した結果、サイバー攻撃の種類や頻度が増加しています。こうした脅威に対して、強固な防御の必要性は一段と高まっています。

■ 世界のサイバーセキュリティ市場の推移

2022年～2030年(2025年以降は予測)
(億米ドル)



セキュリティサービス:
フィッシング(偽メール)、マルウェア(悪意あるソフトウェア)、ランサムウェア(身代金要求)など一般的なサイバー犯罪に対し、組織の保護やセキュリティ戦略の強化を目的とした多様なサービス

サイバーソリューション:
ITシステム、データ、ネットワーク、デジタル資産を監視・保護し、サイバー攻撃から守るための自動化されたセキュリティ技術

出所: Statista Market Insights

※グラフは過去のものおよび予測であり、将来を約束するものではありません。

※公開情報など信頼できると判断した情報をもとにアモーヴァ・アセットマネジメントが作成。情報の正確性・完全性について当社が保証するものではありません。

ページ記載の銘柄について、売買を推奨するものでも、将来の価格の上昇または下落を示唆するものでもありません。また、当社ファンドにおける保有・非保有および将来の銘柄の組入れまたは売却を示唆・保証するものでもありません。

2025年9月1日付で、日興アセットマネジメント株式会社から社名変更しました。

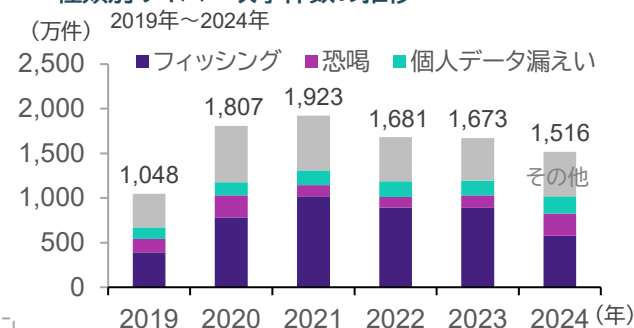
当資料は、アモーヴァ・アセットマネジメントが情報提供を目的として作成したものであり、特定ファンドの勧誘資料ではありません。また、弊社ファンドの運用に何等影響を与えるものではありません。なお、掲載されている見解および図表等は当資料作成時点のものであり、将来の市場環境の変動等を保証するものではありません。投資信託は、値動きのある資産(外貨建資産には為替変動リスクもあります。)を投資対象としているため、基準価額は変動します。したがって、元金を割り込むことがあります。投資信託の申込み・保有・換金時には、費用をご負担いただく場合があります。詳しくは、投資信託説明書(交付目録見書)をご覧ください。

デジタル化の進展に伴い高度化するサイバー攻撃

- 特に2010年台後半ごろから、サイバー攻撃が増加しています。これは、クラウド化やモバイル対応、IoT導入などが進んだことでネットワークや関連システムが増加し、攻撃対象が拡大したことにあります。
- 2020年の新型コロナウイルス感染症危機では、リモートワーク体制が急速に普及したこともあり、サイバー攻撃が急増しました。
- 近年は攻撃種類が変化しており、フィッシングが減少する一方で、ランサムウェアなどの恐喝が増加しています。

右グラフの「その他」には、未払い未配達や投資詐欺、テクニカルサポート詐欺、身元盗用、クレカ詐欺が含まれます。

■ 種類別サイバー攻撃件数の推移



出所: Statista Market Insights, National Cyber Security Organizations, FBI - Federal Bureau of Investigation, IMF

管理型セキュリティサービスとAI活用によるサイバーソリューション

- セキュリティサービスは、組織のセキュリティ要件に合わせて製品やサービスを設計する管理型サービスへの移行が進んでおり、攻撃の複雑化や頻度の増加、専門家不足などを背景に、アウトソース(Deloitte、Infosysなど)する傾向が強まっています。また、コンサルティング(Cognizant、IBMなど)やセキュリティ計画・トレーニング(CompTIA、SANSなど)のニーズも高まっています。
- サイバーソリューションは、AIや機械学習を活用した脅威検知・対応能力の強化が進んでおり、主に以下のソリューションが提供されています。 ※上記、下表においてカッコ内は各分野の主要な企業(一部略称)です。

| | |
|----------------|--|
| アプリケーションセキュリティ | アプリケーションを脅威から保護するセキュリティ対策(Microsoft、Broadcomなど) |
| クラウドセキュリティ | クラウド環境における安全性確保(Tenable、Trend Micro、Palo Alto Networkなど) |
| データセキュリティ | データ暗号化や不正アクセス・データ漏えいの防止(Commvault、Trellix、McAfeeなど) |
| ネットワークセキュリティ | ファイアウォールなどで安全なネットワークを設計し攻撃を防御(IBMなど) |
| エンドポイントセキュリティ | PCなどエンドユーザー機器のセキュリティ対策(CrowdStrike、Microsoftなど) |