GLOBAL X ETFs リサーチ

2022 年も続くと予想される サイバーセキュリティの脅威

ペドロ・パランドラニおよび
アレック・ルーカス

日付：2022 年 1 月 24 日
トピック：テーマ投資

今年は、企業と消費者、そして彼らのデータを狙うサイバー犯罪者の間でのいたちごっこの激化が予想されます。最近では、インターネット・ソフトウェアである Log4j に脆弱性が見つかったことから、全世界で数億台のシステムが危険に晒される可能性があるとの懸念が広がっています。これは、2021 年に米国東部で燃料配送事業を展開する Colonial Pipeline の操業を一時停止に追い込んだランサムウェア攻撃など、注目を集めた複数の侵害事件に続く脅威です。このようなサイバー攻撃事件は、特に重要インフラやサプライチェーンへの攻撃を中心に、その頻度とコストが増加し続けています。また、グローバル経済のオンライン化が進み、機密データが危険に晒されるようになっていることから、脅威のレベルは今後さらに高まることが予想されます。結果として、サイバーセキュリティに対する意識と支出が高まり、サイバーセキュリティというテーマへの長期的な追い風になると考えられます。

重要なポイント：

- 2021 年には、サイバー攻撃が多発し、コストも上昇しましたが、この傾向は 2022 年も続くと思われます。データ侵害にかかるコストの平均は、2020 年の 3.86 百万ドルから 2021 年には 4.24 百万ドルに上昇し、IBM がこれまで「Cost of a Data Breach Report」を発表した 17 年間で最も高い総コストを記録しました。[i]
- 企業、政府機関、そして消費者は、サイバーセキュリティへの取り組みを強化しており、消費者も自分自身を守るための手段を講じています。例えば、企業による支出は、2022 年に 1,720 億ドルに達すると予想されています。[ii]
- サイバーセキュリティの取り組みにおいて、引き続きアイデンティティ、ネットワーク、エンドポイントセキュリティが重要なポイントとなっており、ネットワークセキュリティは 2021 年から 2026 年の間で 24%と最も急速に成長すると予想されています。[iii]

2021 年にデジタル世界の脆弱性が明らかに

現在、世界では 1 日に 2.5 クインテリオン（百京）バイトのデータが生成されていると推定されています。[iv]その結果、ハッカーがこれまで以上に機密データへのエントリーポイントを得ることにつながっており、今後世界のデジタル化が進み、データ量が増加するにつれて、さらに多くの機会を彼らが得ることになると予想されます。特に、IoT（モノのインターネット）デバイスは、データプールへの絶好のアクセス経路となるでしょう。2021 年末時点で、接続されているデバイスは 146 億台にも上ります。[v]この数字は 2022 年に 18%近く増加し、2027 年には 2 倍以上になる可能性があります。[vi]

また、経済が在宅勤務へ移行していることも、サイバー犯罪者にとって大きなチャンスを生み出しています。米国では 2021 年に新型コロナウイルスのパンデミックによるロックダウンが緩和されましたが、45%ものフルタイム従業員が少なくとも部分的に在宅勤務を続けました。[vii]新たな変異株の出現や従業員自身の選択により、在宅勤務制度は今後も維持される可能性があり、結果として予見可能な将来のデータの脆弱性につながる可能性があります。IBM のレポートによると、2021 年に報告されたデータ漏洩の 17.5%はリモートワークがその要因でした。[viii]また、これらの侵害の平均コストは、リモートワークが要因ではない侵害に比べて 16.6%高くなっています。[ix]

2021 年には、いくつかの有名企業がコストの嵩むサイバー攻撃の犠牲になりました。Colonial Pipeline へのランサムウェア攻撃では、攻撃者に 4 百万ドルが支払われたとされています。[x]また、CNA Financial は、ロックアウトされ

たデジタルインフラの一部を解読してもらうため、ランサムウェアのハッカーに 40 百万ドルを支払いました。[xi] さらに、世界最大の食肉メーカーである JBS は、サイバー攻撃を受けて複数の工場の閉鎖に追い込まれました。[xii]これらの例は、昨年企業が被害を受けた主な攻撃のほんの一部にすぎず、時には数百万ドルの損害を被ることもありました。

2021 年の主なサイバー攻撃

（出典）CRN、「The 10 Biggest Cyber And Ransomware Attacks Of 2021」（2021 年 12 月 23 日）
Microsoft、「Microsoft Exchange Server Remote Code Execution Vulnerability」（2021 年 3 月 2 日）

2021 年の主なサイバー攻撃	業種	日付:	要求に対し支払われた金額（百万ドル）
Microsoft Exchange	テクノロジー	2021 年 1 月 5 日	$50.00*
Kia Motors	自動車	2021 年 2 月 13 日	$20.00*
Bombardier	製造（航空機）	2021 年 2 月 23 日	
CNA Financial	金融サービス	2021 年 3 月 21 日	$40.00
Harris Federation	教育	2021 年 3 月 29 日	$8.00*
Colonial Pipeline	エネルギー	2021 年 5 月 7 日	$4.40
Brenntag	化学	2021 年 5 月 11 日	$4.40
JBS	食品	2021 年 5 月 30 日	$11.00
Kaseya	情報技術	2021 年 7 月 2 日	$70.00*
Accenture	テクノロジー	2021 年 8 月 12 日	$50.00*
Acer	テクノロジー	2021 年 10 月 5 日	$50.00*

**要求されたが、全額は支払われていない。*

最近のサイバー攻撃事例がサイバーセキュリティへの投資を後押ししている

最も洗練されたソリューションであっても、すべての脆弱性を排除することはできないかもしれません。しかし、脅威の多くを阻止し、最悪の結果から守ることは可能です。2021 年においては、企業、米国政府、消費者のサイバー脅威に対する認識の高まりと予防策に取り組む姿勢が明らかになりました。

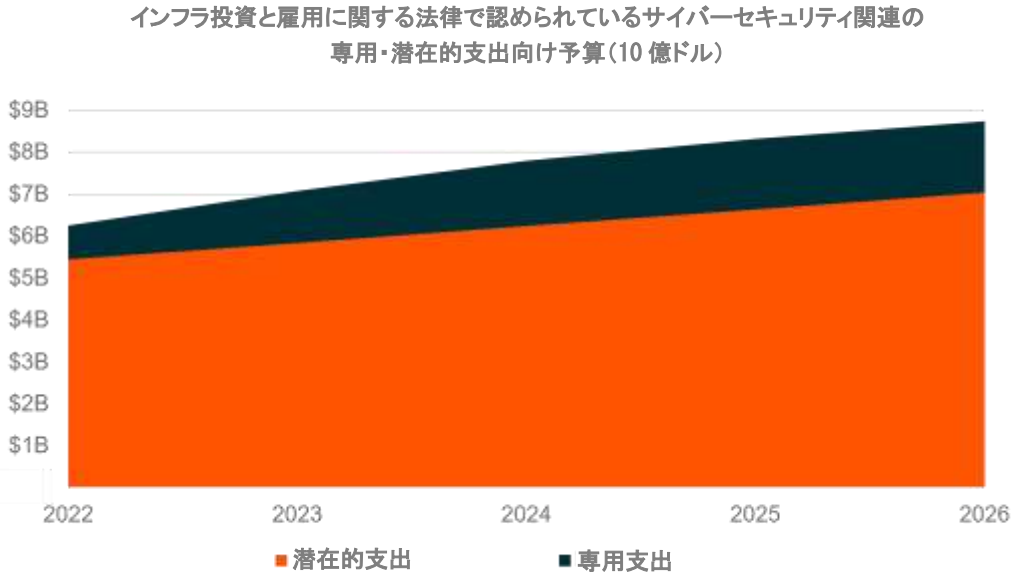
- **企業**：ランサムウェア攻撃の被害者、そのサプライヤー、顧客、そして競合他社は、セキュリティ侵害がもたらす混乱を理解しています。被害によるコストは往々にして、適切なソリューションへの投資のコストを上回ります。大企業は通常、サイバーセキュリティに年間 2 百万ドルから 5 百万ドルを費やしていますが、ランサムウェアの侵入 1 件による被害額は平均 4.62 百万ドルに上ります。[xiii,xiv]3,000 人以上の経営者を対象とした最近の調査で、回答者の 69%が 2022 年にサイバーセキュリティへの支出が増えると予想していますが、このコストが理由のひとつとなっています。[xv]ある試算によると、2022 年のデータ保護とリスク管理に関する支出は、2021 年から 11%増加し 1,720 億ドルに達する可能性があります。[xvi]

- **政府機関**：2021 年 5 月、バイデン大統領は、連邦政府のサイバーセキュリティ能力を近代化しサイバー攻撃への対応戦略を標準化するとともに、政府の請負業者の情報共有要件を引き上げることを目指す大統領令に署名しました。そして 7 月には、バイデン大統領は重要インフラ（特に電力、水、交通）へのサイバー攻撃を防ぐことを目的とした国家安全保障に関する覚書に署名しました。これらの施策は、「インフラ投資と雇用に関する法律」に反映されており、支出先が定められている 17 億ドルと潜在的な支出向けの約 70 億ドルの予算が国家のサイバーセキュリティ向上に向けられています。[xvii]

  また昨年、上院はホワイトハウス初のナショナル・サイバー・ディレクター職の設置を全会一致で承認しました。議会は、2021 年国防権限法案の一部としてこのポジションを創設し、今後の政権においてサイバーセキュリティをより重視する姿勢を示しています。

  .

最近の米国インフラ法案では、約 90 億ドルのサイバーセキュリティ関連支出が認められている



出典：第 117 議会（2021 年～2022 年）「H.R.3684 - インフラ投資と雇用に関する法律（Infrastructure Investment and Jobs Act）」2021 年 6 月、Global X Analysis。

- **消費者**：サイバーセキュリティ関連の支出のうち、消費者によるものは少ないながらも増加傾向にあります。消費者の約 53%が少なくとも 1 件のサイバー犯罪の被害に遭っており、多くの人が個人用 VPN、二要素認証、個人情報保護サービスなどの予防策を講じています。[xviii]新型コロナウイルスのパンデミックにより、消費者のインターネット利用時間が増加し、これに乗じて詐欺師の活動が活発化して個人に対する脅威が増大しました。2021 年 10 月現在、新型コロナウイルス関連の詐欺で米国人は 586 百万ドルを失っています。[xix]しかし、消費者は脅威の高まりを認識しています。昨年は、パンデミックの直接的な影響を受けて、約 40%の成人がオンライン活動の安全を保護する対策を講じました。[xx]パンデミックの際に学んだデジタル保護の習慣は、今後消費者のサイバーセキュリティサービス導入を加速させる可能性があります。

注目すべきサイバーセキュリティの主要分野

- **アイデンティティセキュリティ**:リモートワークの増加に伴い、重要なデータ、リソース、アプリケーションへのアクセスの保護が、企業にとって極めて重要となっています。この分野では、サイバーセキュリティのサブセグメントとして、IAM(アイデンティティおよびアクセス管理)、PAM(特権アクセス管理)、IGA(アイデンティティ・ガバナンスおよび管理)などがあります。これらのサブセグメントは、2021 年から 2026 年にかけて平均 CAGR19%で成長すると予測されています。[xxi]

- **ネットワークセキュリティ**:この分野の企業は、ネットワークの完全性、機密性、およびアクセス権を誤用や侵害から保護する事業を展開しています。承認が過度に緩いネットワークでは、個人が侵害された後、サイバー攻撃が水平方向(ユーザーからユーザーへ)に移動する可能性があります。例えば、「ゼロトラストネットワーク」は、企業のネットワークに接続したり、ユーザーをインターネットに接続したりすることなく、ユーザーに社内アプリケーションへのアクセスを提供します。この分野では、サイバーセキュリティのサブセグメントとして、ゼロトラストネットワーク・アクセス(ZTNA)、ソフトウェア定義ネットワーク(SDWAN)、ネットワーク検知・応答(NDR)、ファイアウォール/NGFW/統合脅威管理(UTM)、セキュアアクセス・サービスエッジ(SASE)などがあります。これらのサブセグメントは、2021 年から 2026 年にかけて平均 CAGR24%で成長すると予測されています。[xxii]

- **エンドポイントセキュリティ**:インターネットに接続された多数のデバイスがハッカーの新たな侵入口となり、企業や個人のセキュリティを効果的に管理するうえで新たな課題や複雑さをもたらしています。IoT の導入を成功させるためには、事前に組み込まれたセキュリティ要件から、機械で生成された機密データの継続的な管理と保護まで、多層的なエンドツーエンドセキュリティが必要となります。この分野のサブセグメントには、サイバーセキュリティのサブセグメントとして、EPP(エンドポイント・プロテクション・プラットフォーム)、EDR(エンドポイント検知・応答)、DLP(データ損失防止)などがあります。エンドポイントセキュリティ分野全体では、2021 年から 2026 年の間に CAGR8%で成長すると予測されています。[xxiii]

これらの主要な分野を超えて、サイバーセキュリティ企業による統合の動きが加速しています。 一般的に、サイバーセキュリティプロバイダは限られた製品に特化しているため、顧客は複数のプロバイダをパッチワークのように使ってデータを保護しなければなりません。このような状況は、コストの嵩む遅延やその他の潜在的な非効率性につながります。実際、2021 年のデータ侵害事例では、それを特定して封じ込めるのに平均で 287 日かかっています。[xxiv]2021 年には、エンドツーエンドで保護能力を向上させるために、複数の有名サイバーセキュリティプロバイダが M&A を行いました。特筆すべき事例には、CrowdStrike Holdings による 352 百万ドルでの Humio 買収や、Rapid7 による 335 百万ドルでの IntSights の買収が挙げられ、これによりそれぞれの会社は統合された脅威検出および修復製品を提供できるようになりました。[xxv,xxvi] このような統合事例の増加傾向は 2022 年にも続くと見られ、ウイルス対策および VPN サービスのプロバイダである Norton と Avast が 80 億ドル以上の規模で合併することが見込まれています。[xxvii]

結論

2021 年には、記憶にある限り最も衝撃的なサイバー攻撃が複数発生しましたが、世界中でデジタルへの移行が進む中、今後も同様の攻撃が発生する可能性が高まっています。しかし、この期間に得られたデジタル保護に関する教訓が、サイバーセキュリティサービスの導入をさらに加速させることになると Global X は確信しています。サイバー犯罪者を阻止するための財政的なコミットメントは 2022 年のサイバーセキュリティ企業の追い風となり、サイバーセキュリティというテーマ全体の長期的な投資妙味を高めると Global X は見ています。

速な陳腐化および業界における激しい競争の影響を受ける可能性があります。国際投資には、通貨価値の不利な変動、一般に公正妥当と認められる会計原則の相違、または他国の社会的、経済的もしくは政治的不安定性を原因とする元本毀損リスクを伴う場合があります。

---

[i]IBM、「Cost of a Data Breach Report 2021」(2021 年 7 月)。
[ii] Soffid、「Cybersecurity Trends for 2022, December 29」(2021 年)。
[iii] 以下の資料に掲載されている平均 CAGR を参考にした指標です:Markets and Markets、「Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2026」(2021 年 2 月)、Research and Markets、「SD-WAN - Global Market Trajectory & Analytics」(2021 年 4 月)、Market Growth Reports、「Global Network Detection and Response (NDR) Market Growth (Status and Outlook) 2021-2026」(2021 年 7 月)、Expert Market Research、「Global Unified Threat Management Market: By Component: Hardware, Software, Virtual; By Service: Consulting, Support & Maintenance, Managed UTM; By Deployment Mode; By Company Size; Regional Analysis; Historical Market and Forecast (2017-2027); Market Dynamics; Competitive Landscape; Industry Events and Developments」(2021 年)、Markets and Markets、「Secure Access Service Edge (SASE) Market with COVID-19 Impact Analysis, by Offering (Network as a Service and Security as a Service), Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2026」(2021 年 8 月)、Global X Analysis。
[iv] CloudTweaks、「Infographic: How Much Data is Produced Every Day?」(2021 年 11 月 15 日に閲覧)。
[v] Ericsson Mobility Visualizer、「Connected Devices」(2021 年 11 月 15 日に閲覧)。
[vi] 同上。
[vii] Gallup、「Remote Work Persisting and Trending Permanent」(2021 年 10 月 13 日)。
[viii] IBM(注 1)。
[ix] IBM(注 1)。
[x] CNBC、「Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate」(2021 年 6 月 8 日)。
[xi] Bloomberg、「CNA Financial Paid $40 Million in Ransom After March Cyberattack」(2021 年 5 月 20 日)。
[xii] CNBC、「Meat supplier JBS paid ransomware hackers $11 million」(2021 年 6 月 9 日)。
[xiii] PCH Technologies、「Cost of Cyber Attacks vs. Cost of Cyber Security in 2021」(2021 年 7 月 7 日)。
https://pchtechnologies.com/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/
[xiv]IBM、「Cost of a Data Breach Report 2021」(2021 年 7 月)。
[xv] PwC、「Global Digital Trust Insights 2022」(2021 年 10 月)。
https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html#findings
[xvi] Gartner、「Gartner IT Symposium/Xpo Americas」(2021 年 10 月)。
https://www.soffid.com/cybersecurity-trends-for-2022/
[xvii] インフラ投資と雇用に関する法案(H.R. 3684, 117th Cong.)(2021 年)。
[xviii] Norton、「2021 Norton Cyber Safety Insights Report Global Results」(2021 年 5 月)。
[xix] CNBC、「Covid-related scams have bilked Americans out of $586 million」(2021 年 10 月 18 日)。
[xx] Norton、「2021 Norton Cyber Safety Insights Report Global Results」(2021 年 5 月)。
[xxi] 以下の資料に掲載されている平均 CAGR を参考にした指標です:Technavio、「Privileged Access Management Solutions Market by Deployment and Geography - Forecast and Analysis 2022-2026」(2022 年 1 月)、Mordor Intelligence、「Identity Governance And Administration Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)」(2022 年 1 月)、Technavio、「Consumer Identity and Access Management (IAM) Market by Deployment and Geography - Forecast and Analysis 2022-2026」(2021 年 12 月)。
[xxii] 以下の資料に掲載されている平均 CAGR を参考にした指標です:Markets and Markets、「Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2026」(2021 年 2 月)、Research and Markets、「SD-WAN - Global Market Trajectory & Analytics」(2021 年 4 月)、Market Growth Reports、「Global Network Detection and Response (NDR) Market Growth (Status and Outlook) 2021-2026」(2021 年 7 月)、Expert Market Research、「Global Unified Threat Management Market: By Component: Hardware, Software, Virtual; By Service: Consulting, Support & Maintenance, Managed UTM;

By Deployment Mode; By Company Size; Regional Analysis; Historical Market and Forecast (2017-2027); Market Dynamics; Competitive Landscape; Industry Events and Developments」（2021 年）、Markets and Markets、「Secure Access Service Edge (SASE) Market with COVID-19 Impact Analysis, by Offering (Network as a Service and Security as a Service), Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2026」（2021 年 8 月）、Global X Analysis。

[xxiii] Mordor Intelligence、「Endpoint Security Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)」（2022 年 1 月）。

[xxiv] IBM、（注 1）。

[xxv] Crowdstrike、「CrowdStrike Completes Acquisition of Humio」（2021 年 3 月 5 日）。

[xxvi] VentureBeat、「Rapid7 acquires threat intelligence platform IntSights for $335M」（2021 年 7 月 19 日）。

[xxvii] Norton、「NortonLifeLock and Avast to Merge to Lead the Transformation of Consumer Cyber Safety」（2021 年 8 月 10 日）。