執筆：
ペドロ・パランドラーニ
リサーチアナリスト

日付：2021年2月2日
トピック：投資テーマ別

GLOBAL X ETFs リサーチ

サイバーセキュリティの進展を率いる4社

今日では、どの企業がいつ深刻なサイバー問題に直面するか分からない時代になりました。ソフトウエア管理会社のソーラーウインズ（SolarWinds）の場合は、2020年12月でした。米国史上最大のサイバー攻撃といわれるこの事件は、サイバー犯罪者が同社の（Orion）ソフトの脆弱性を突いてウイルスを送り込み、それによって同ソフトを稼働させるサーバーに侵入しました。この事件の深刻な問題は、主要な連邦政府機関や組織も攻撃を受けており、国の安全保障が脅かされている可能性があることです。事件発覚後の初期調査では、約250の組織が被害を受けていました。

米国や世界で起こっているサイバー脅威による犯罪は、攻撃範囲が広がりつつあるうえに、手口もますます高度化しています。増加の一途をたどるサイバー攻撃件数に伴い、世界のセキュリティ支出額も、2020年の1,250億ドルから2024年には1,750億ドルに達すると予想されています。[1] セキュリティ費用が拡大している背景には、クラウドへの移行が加速していることがあげられます。現在は、全仕事量の3分の1しかクラウドコンピューター技術を利用していません。しかし今後も、クラウドでの仕事量が増加するとともに、悪意のある攻撃からの防衛手段として、サイバーセキュリティ支出額は増えざるを得ないでしょう。[2] 同様に、インターネット接続型機器の利用が急速に進んでいますが、これはサイバー攻撃者にとっては、重要情報の盗用や情報の身代金要求を図る攻撃対象が増えていることを意味します。

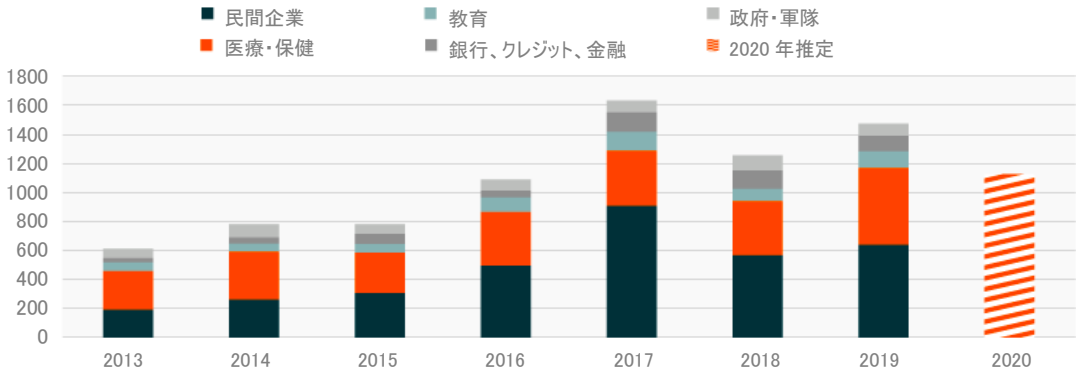
本レポートでは、サイバーセキュリティのテーマで注目する以下の4社に焦点を当てています。

- クラウドストライク（CrowdStrike）：エンドポイント防御プラットフォームの大手
- ゼットスケーラー（Zscaler）：「セキュア・ウェブ・ゲートウェイ」を提供するクラウドネイティブのプラットフォーム企業
- オクタ（Okta）：認証アクセス管理分野の中核企業
- マイムキャスト（Mimecast）：悪意を持つ電子メールを検知・阻止するソリューションの最大手

2020年は推定3億8,000万人分超の個人情報が漏えいとの推計測[3]

米国でのデータ漏えい件数

出典：個人情報盗難情報センター、2020 年



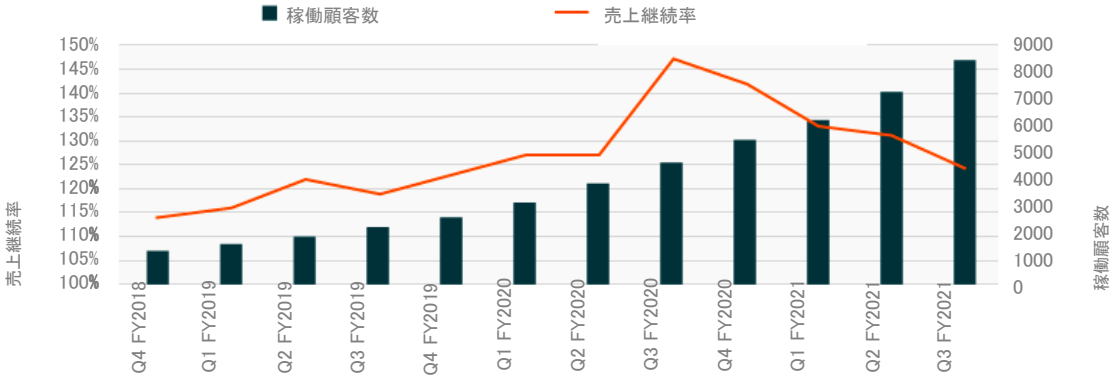
クラウドストライク（CrowdStrike）: エンドポイント防御プラットフォームの大手

クラウドストライクはエンドポイント防御プラットフォーム（EPP）分野を代表するサイバーセキュリティ企業です。顧客が使用するモバイル機器、ラップトップ、サーバーなどのエンドユーザー機器のセキュリティを守ります。同社のソリューションは、脅威を継続的に検知・分析するSaaS（サービスとしてのソフトウエア）です。100%クラウド型の基本設計概念であるため、クラウドを使わないレガシー型の既存ソリューションに対する競争優位性を持ちます。また、多くの異なるIT環境に対応でき、迅速かつ効果的に設定できる強みもあります。例えば、2020年度第4四半期には、新規顧客であるターゲット社でのオンボードをわずか10日間で完了しました。

従来のサイバー攻撃対策は、オンプレミスのウイルス対策ソフトが、エンドポイントファイル内の既知の脅威を監視・スキャンして、サイバー攻撃を阻止していました。しかし、このセキュリティ階層は主に攻撃反応型です。今日の最先端セキュリティソリューションはAIを活用します。クラウドストライクは、「Threat Graph」と呼ばれるAIを提案しています。これは、同社のAI駆動型サイバーセキュリティソリューションを支える頭脳部分です。同社はThreat Graphを使い、週に4兆のサイバー脅威事案を処理、1分間に5,000万件の判断を実行しています。[4] データセットは同社のクラウド上で処理されます。これによって、より多くの顧客データを分析することで、Threat GraphのAI技術が向上すると言うネットワーク効果が生まれています。

クラウド型ソリューションは、安定した収益フローをもたらすと考えて良いでしょう。2020年度第4四半期の決算では、全売上高の92%が定期利用料金収入でした。[5] もう一つの注目点は、2019年第1四半期以降、同社の売上継続率が120%以上で推移していることです。[6] 売上継続率が100%を超えると、既存顧客からの売上高が純増していること（価格引き上げ、または高価格製品への買い換え）を意味します。

クラウドストライクの売上継続率（左目盛）と稼働顧客数（右目盛）動向
出典：Global X ETFs、クラウドストライク社資料



ゼットスケーラー（Zscaler）: セキュア・ウェブ・ゲートウェイの最大手

ゼットスケーラーも、100%クラウド型のサイバーセキュリティを提供するプラットフォーム（サービス基盤）企業です。同社のサービス利用者は、ハードウェアの購入・管理は不要で、プラットフォームは常に更新されます。現在は、1日に175,000件のセキュリティクラウド更新を行っています。[7] 同社のセキュア・ウェブ・ゲートウェイ（SGW）ソリューションの主要サービスでは、ゼットスケーラー・プライベート・アクセス（ZPA）機能を介して、顧客が企業用電子メールなどの社内管理アプリへ安全にアクセスできるようにしています。また、ゼットスケーラー・インターネット・アクセス（ZIA）基盤を使い、顧客関係管理（CRM）ソフトなどの外部アプリ向けソリューションも提供しています。前述のセキュア・ウェブ・ゲートウェイは、外部のウェブアプリから内部ネットワークへの侵入を試みる安全でないトラフィックを阻止します。ユーザーは、自社のネットワークを経由せずにアプリに直接接続できます。この点で、同社のサービスは、仲介者のような役割を果たすと言えます。

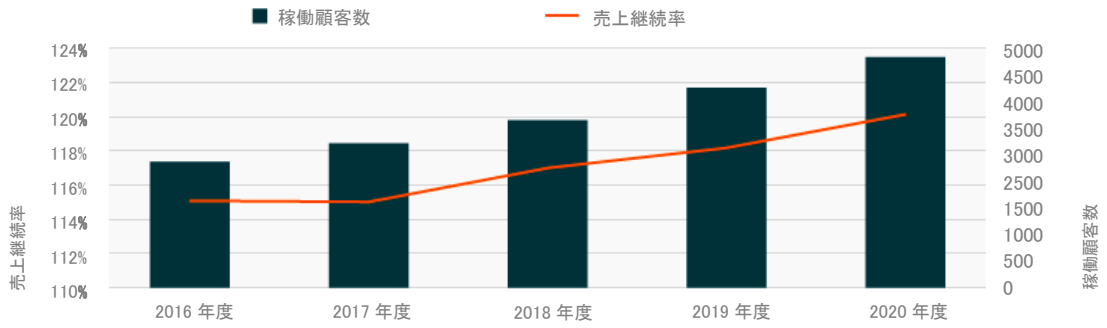
同社が提供する機能が浸透することで、「仮想私設ネットワーク」（VPN）技術の使用がやがては時代遅れとなると予想できます。ZPAソリューションは、配置・設定・管理が容易であるうえに、従来のVPNソリューションよりもセキュリティ面で優れているためです。また、ユーザーは、企業のネットワークに接続したり、インターネットのリスクにさらされたりすることなく、内部アプリにア

クセスできます。さらに、ソリューションの基本設計概念で、サイバー攻撃者が侵入しようとした際に、ネットワーク内での水平移動能力を完全に封じ込めます。同社は、この基本設計概念を、ネットワークを絶対にすべてのユーザーに開放しない「ゼロ・トラスト・ネットワーク」と表現しています。必然的な流れとして、ネットワークが重要視されなくなり、インターネットが新たな企業ネットワークになっていくでしょう。[8]

遠隔勤務や自宅・事務所混合型の仕事が主流になる時代に入りつつあるなか、ラップトップ、スマホ、その他モノのインターネット（IoT）機器を使った内・外アプリへのアクセスに対するセキュリティの強化は、あらゆる組織の最優先課題となっています。調査会社のガートナーによると、2023年までに60%の事業所が遠隔アクセスVPNをほぼ全廃し、ゼットスケーラーのソリューションなどのゼロ・トラスト・ネットワークに切り替える方針です。[9]

2020年度末現在、ゼットスケーラーの売上継続率は120%台に達しています。これは、既存顧客基盤の売上高成長が継続していることを示しています。[10] 注目点は、ZIAとZPAだけで見ても、同社が既存顧客に高額の製品を売れる機会は6倍多いと考えていることです。[11]

ゼットスケーラーの売上継続率（左目盛）と稼働顧客数（右目盛）動向
出典：Global X ETFs、ゼットスケーラー社資料



オクタ（Okta）: 認証アクセス管理分野の急成長企業

オクタは、認証アクセス管理（IAM）分野での大手サイバーセキュリティ企業です。この分野の主眼点は、本物の個人・従業員が、正しい時間に、正しい理由で正しい情報資源にアクセスできることです。[12] マルチ要素認証（MFA）、アプリケーション・プログラミング・インターフェース（API）によるアクセス管理、さらにシングルサインオン（SSO、一元管理ユーザー認証）といった認証ソリューションは、各種アプリへの不正アクセスを阻止する手段として企業の利用が進んでいるソリューションです。

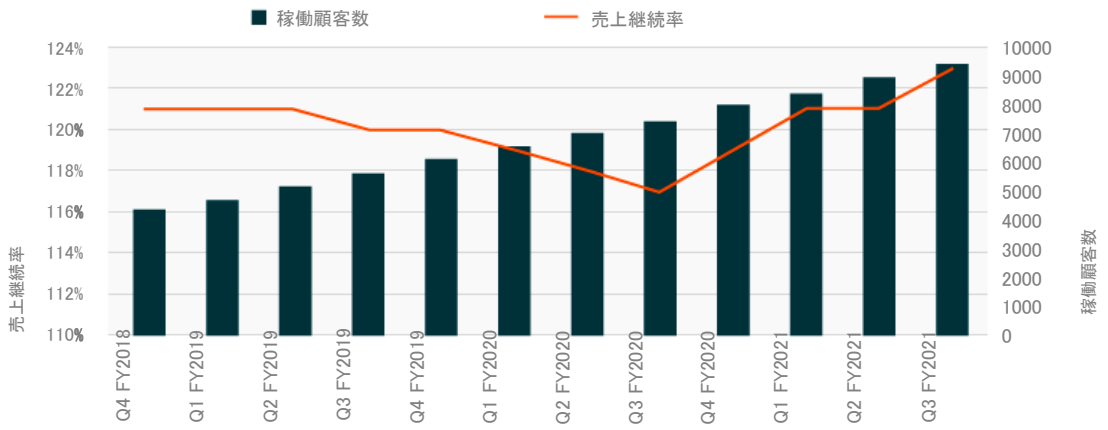
IAM分野の企業も、遠隔勤務や自宅・事務所混合型形態という職場環境の転換はプラス要因になると考えています。異なる勤務地に務める従業員が、さまざまな機器を使ってアプリに接続する現代において、IT部門はIAMを活用し、誰がどのアプリにいつアクセスしているのかを効率的に監視しています。さらに企業も、IAMを利用し、特定の内部アプリにアクセスする必要のある請負業者や顧客に対し、アクセスポイントの監視とセキュリティ確保を実現しています。

最終ユーザーの立場から見ると、オクタのIAMソリューションの長所は、シングルポータル内ですべてのアプリにアクセスできることです。これにより、ヘルプデスクに寄せられるログイン関連の問い合わせ件数を半減させるとともに、新しいアプリにログインして利用する時間が50%短縮できます。[13] 同社は、従業員認証市場全体の潜在的規模は300億ドル、顧客認証市場は同250億ドルと推定しています。[14]

前述のクラウドストライクとゼットスケーラー同様、オクタのソリューションも完全にクラウド環境で稼働します。また、総売上高の94%が経常収益で、サービスの定期利用料金収入がその源泉となっています。2021年度第3四半期における直近12か月の売上継続率は123%、前四半期比で2%増と、前の2社同様に高水準の売上継続率を達成しています。

オクタの売上継続率（左目盛）と稼働顧客数（右目盛）動向

出典：Global X ETFs、オクタ社資料



マイムキャスト（Mimecast）：電子メールセキュリティの最大手

マイムキャストは、サイバーセキュリティ分野でおそらく最も良く知られた類型である「セキュア電子メールゲートウェイ」の最大手企業です。サイバー攻撃の95%は電子メールを使う手口です。電子メールは、攻撃者にとって機会便乗型や標的攻撃で最も利用しやすい通信路となっています。[15] 世界で約10億人の企業電子メールユーザーがいることを考えると、マイムキャストのビジネスチャンスは膨大なものです。[16] 直近の数字で、同社ゲートウェイは約1,500万人の利用者を持ち、世界市場の1.5%を握っています。[17]

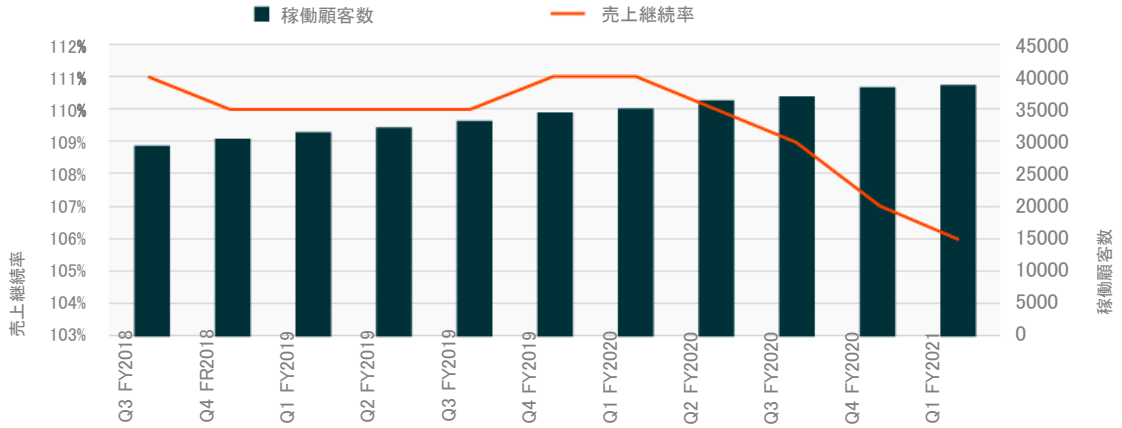
大規模フィッシングや標的型フィッシング攻撃の狙いは、メール受信者に信じやすい内容のメッセージを送り、特定の行動を強要させることです。[18] その結果、攻撃者は、被害者から金を奪うか知的財産といった重要情報を盗み取ります。米連邦捜査局は、2013年10月から2018年5月における電子メール詐欺による被害総額を120億ドルと見積もっています。[19] 電子メールのフィッシング詐欺や、なりすまし詐欺はすでに日常的な問題になっています。しかし、コロナ禍情勢を受けて、インターネットを使う時間が長くなっている現在は、犯罪者にとり「罠」を仕掛けやすい環境にあると言えます。実際、コロナ禍初期の100日間だけで見ても、電子メールフィッシングとなりすまし詐欺件数は30%増加しました。[20]

マイムキャストのソリューションは、既知・未知のマルウェアや犯意を持つURLを仕掛けたり、会社重役や、銀行、連邦政府機関、さらには顧客や供給業者などの第三者機関になりすまして詐欺を図ったりする電子メールを検出、阻止します。同社のソリューションは、従来型の検出技術にAI機能を補完して整備したものです。こうしたAI機能には、業務のセキュリティを脅かす写真やロゴを特定するディープラーニング（深層学習）、電子メールに含まれたリスクのある変則的パターンを検知するマシンラーニング（機械学習）、さらにリスクの高いリンクを類別するスーパーバイズラーニング（教師あり学習）などがあります。

なお、こうしたソリューションも完全クラウド型設計概念を採用しており、魅力のあるビジネスモデルに迅速性も備わった形になっています。ここ数年間、同社は100%を上回る売上継続率を維持しています。この例からも、サイバーセキュリティ企業のビジネスモデルが堅実な成長を達成することを確信できます。[21]

マイムキャストの売上継続率（左目盛）と稼働顧客数（右目盛）動向

出典：Global X ETFs、マイムキャスト社資料



結論

サイバーセキュリティは、注視すべき課題ですが、財務的にも無視できない課題です。増加の一途をたどるサイバー攻撃、そしてその脅威が世界の業界や政府機関にもたらす可能性のある影響を考えると、さまざまな事業機能を安全に運営するためには、サイバーセキュリティツールが不可欠な要素であることが分かります。分野が電子メールであれ、認証管理、内・外部アプリへのアクセス、さらにエンドユーザーが使う機器の保護であれ、本レポートが注目する4社は、加速度的に発展するデジタル世界の防衛に中核的役割を果たしているとともに、サイバーセキュリティ産業の多面的特性を裏打ちする存在だと言えます。

脚注

1. IDC『根強い重要を追い風に堅調な成長が続くセキュリティ製品とサービス（新規IDC支出ガイド報告）』（2020年8月13日）
2. IDG『2020年IDGクラウドコンピューティング調査』（2020年6月8日）
3. 個人情報盗難情報センター『個人情報盗難情報センター：2020年度第3四半期のデータ漏えい分析と要点』（2020年10月14日）
4. クラウドストライク『会社概要』（2020年12月）
5. 同上
6. クラウドストライク（n4）
7. ゼットスケーラー『投資家向け情報：クラウド統計』（2021年1月19日にアクセス）
8. ゼットスケーラー『ゼロ・トラスト・ネットワーク・アクセス概論』（2021年1月19日にアクセス）
9. ゼットスケーラー『VPNに代わる手段』（2020年6月）
10. ゼットスケーラー『ゼットスケーラー　2021年アナリスト懇談会』（2021年1月11日）
11. 同上
12. ガートナー『認証とアクセス管理（IAM）』（2021年1月19日にアクセス）
13. オクタ『シングルサインオン』（2021年1月19日にアクセス）
14. オクタ『2021年度第3四半期決算報告書』（2020年12月2日）
15. マイムキャスト『2020年ガートナー電子メールセキュリティ市場案内』（2021年1月19日）
16. マイムキャスト『マイムキャスト投資家向け資料』（2020年11月）
17. 同上
18. マイムキャスト『電子メールセキュリティが組織を守る』（2021年1月19日にアクセス）

19. 米連邦捜査局『商用電子メール詐欺の被害総額は120億ドル』(2018年7月12日)
20. マイムキャスト『電子メールセキュリティの現状:ダウンロードハブ』(2021年1月19日にアクセス)
21. マイムキャスト(n16)

.