GLOBAL X ETFリサーチ

サイバーセキュリティ入門

執筆者:
ペドロ・パランドラーニ
リサーチアナリスト

日付:2019年10月29日

トピック:テクノロジー

デジタル化の進展に伴い、価値の高い、取扱いに配慮を要するデータの保護の重要性は増す一方です。テクノロジーは形あるものをデジタルの世界に取り込み、人の手で行ってきたプロセスを自動化することにより、生産性を向上させています。しかし、物理的な世界を離れてデジタルの領域に移るものやプロセスが増加するにつれて、新たな種類の犯罪が現れました。サイバー犯罪による損害は、2021年には、世界全体で年間6兆ドルに上る可能性があります。個人や企業、政府は専有データを守るために、最先端のソフトウェアやサービスを提供するサイバーセキュリティ企業と契約し、莫大な費用を負担しています。[1]このような状況を踏まえると、サイバーセキュリティは力強い成長が期待できる分野であり、その成長は、機械学習やクラウドコンピューティング、モノのインターネットなど、データを作成、利用し、データへの接続性を提供している隣接分野の成長によってさらに拡大すると考えられます。

ビッグデータの台頭

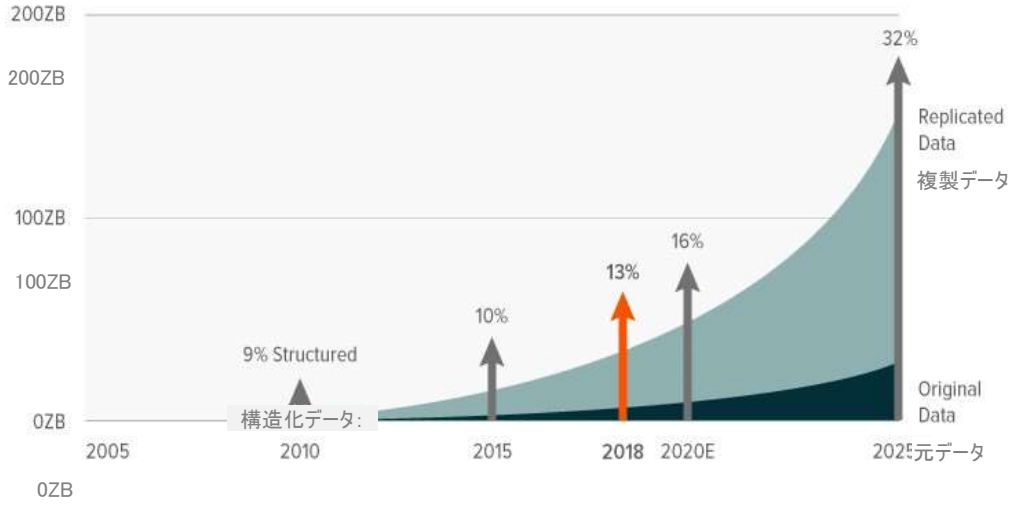
住所や医療記録、財務報告などの重要情報が収められたフォルダーをアルファベット順に書類棚に並べていたのは、そう遠い昔のことではありません。その後、コンピューターとインターネットの登場と共に新たなデジタルの時代が始まり、膨大な情報が「1」と「0」の2つの数字で捕捉され、保存されるようになりました。テクノロジーにより、あたかも一夜にして、クリック1つでデータが利用できるようになったのです。それだけではありません。第1段階は古いデータを物理的な記録媒体からデジタル媒体に移すことでしたが、今では、ほぼすべての活動がデジタルな痕跡を残すに至っています。何を購入するか、何を視聴するか、誰と話すか、どこへ行くか。このようなことすべてが、さまざまなプラットフォームで捕捉されています。ある推計によると、世界全体で250京(2.5×10^{18})バイトを超えるデータが日々生成されています。これは、直近2年間に生成された全データの90%に相当します。[2]別の角度から見ると、2020年には、世界で1日に生成されたデータのバイト数は、観測可能な宇宙空間に存在する星の数の40倍に達するでしょう。[3]

データの爆発的増加を加速させているのが、次に挙げるようなデジタルテクノロジーです。1)モノのインターネット。これは、食器洗い機からテレビに至るまで、日常使用するあらゆる機器をインターネットに接続し、データを収集・送信するものです。2)クラウドコンピューティング。安価で拡張性のある、効率的なデータインフラサービスにより、企業がデータを活用しやすくなっています。3)機械学習と人工知能。膨大なデータセットからさまざまな洞察を引き出すことが可能になり、データの価値がかつてないほど高まっています。

NEW DATA CAPTURED / CREATED / REPLICATED, PER IDC (DATA VOLUME, ANNUAL, GLOBAL (ZB))

捕捉された新データ／生成されたデータ／複製データ（IDCによる）（世界全体の年間データ量（ZB）

出所：Bondcap、Internet Trends 2019。注：1ペタバイト＝100万ギガバイト、1ゼタバイト（ZB）＝100万ペタバイト。構造化データとは、容易に検索できるよう組織化されたデータです。複製データとは、元データから複製されたデータです。



データの増大 = サイバー犯罪の脅威の蔓延

しかし、生成されるデータの価値が高まれば、サイバー犯罪者にとって、データの盗取、ブラックマーケットでの売却、身代金目的での保有、あるいは個人情報の暴露を行う大きな動機となります。サイバー犯罪者が専有データや個人データ、知的財産権（IP）、そして金銭を盗取する際にもっとも一般的に使用するのはデジタルな手段です。しかも、テクノロジーが進化するにつれて、サイバー犯罪の脅威も進化するでしょう。たとえば、モノのインターネットにより身の回りのあらゆるものがインターネットに繋がれば、サイバー犯罪者が利用できる新たな経路が生じます。信号機のハッキングや車両の窃盗、個人の医療機器の操作は、今やすべてが現実に可能なのです。

サイバーセキュリティ企業1社が1日に阻止できる脅威は1億件を超えます。[4]これは1秒当たり1,000件超に相当します。しかし、たった1度の侵入で、企業やユーザーは深刻な被害を被ります。

米ヤフーは2013年から2014年にかけて、2度にわたる攻撃により、全口座30億件をハッキングされました。これは恐らく、21世紀最悪のデータ漏洩事件です。この事件では、ユーザーの氏名、電子メールアドレス、生年月日、電話番号、パスワード、秘密の質問が流出しました。
いささか厄介なのは、米ヤフーがこの事件を公に認めたのが、実際に事件が発生してから3～4年後の2017年だったことです。

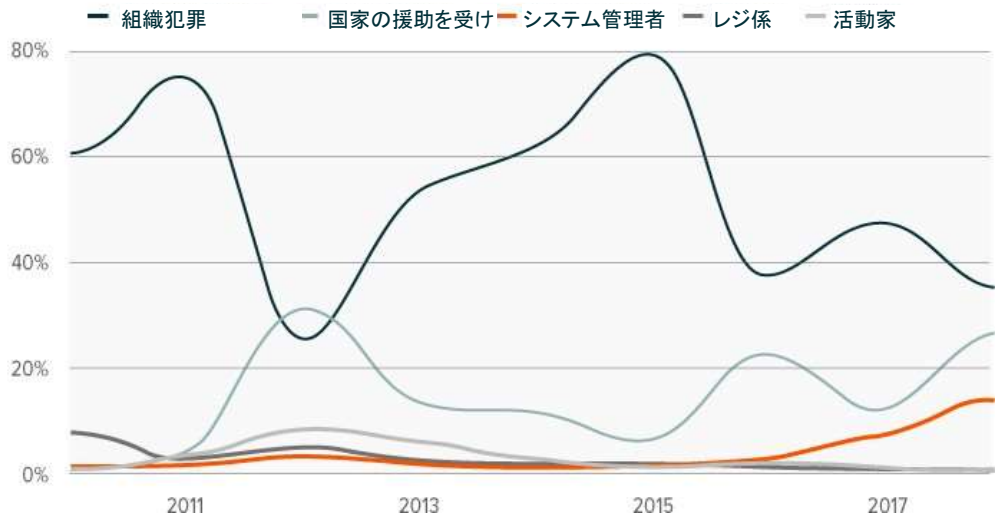
2017年に米国の大手信用情報会社、エクイファクスが公表した情報漏洩事件では、社会保障番号、生年月日、免許証番号の情報が流出し、影響は1億4,300万人の消費者に及びました。2018年11月には、マリオット・インターナショナルが、パスポート番号などの個人情報を含む、5億件の口座情報が流出したと公表しました。

サイバー犯罪の犯人は、通常、外部の人物です。米ヤフーの事件では、国家から援助を受けた人物が犯人でした。これは珍しいことではありません。外国政府の援助を受けたハッカーによるデータ漏洩は、世界全体の約23%を占めています。[5]組織犯罪によるものが39%です。

しかし、懸念すべきなのは外部から攻撃を仕掛けてくる犯罪者だけではありません。個人的な理由や金銭目的で、あるいは、単に人為的なミスの結果として、内部の人物による漏洩も発生します。

データの増大＝サイバー犯罪の脅威の蔓延（データ漏洩）

出所：Verizon、2019 Data Breach Investigations Report。



ソリューションのエコシステムが必要

サイバー犯罪の脅威に対する防御努力は、1つの産業を構成するまでになっています。サイバーセキュリティサービスでは、ネットワークのゲートウェイから、アイデンティティ、電子メール、クラウド、ウェブセキュリティ、エンドポイントに至るまで、あらゆるレベルを保護することに注力します。サイバーセキュリティ企業はさまざまな技術を用いて不正行為や悪意のある行為に対抗しています。以下に挙げる技術のうち1つ、あるいはいくつかの組み合わせです。[6]

- 認証と承認：許可を通じてユーザーの行為を識別し、認証するプロセス
- 暗号技術：数学的関数により通信の安全を確保するプロセス
- 正当な利用パターンの自動分析：利用パターンの自動分析により、異常な動作を管理者に通知する
- 進入検知とリスク低減：悪意者がシステムに侵入するのを防止するための先見的なアプローチ
- データの完全性の検証：データが改変されていないことを確認し、改変された場合にはその内容と被害の範囲を評価するための分析
- コンピューターフォレンジック：サイバー犯罪とその脅威を追跡し、なぜ、どのようにして起こったのかを特定するための事後対応

先見的な防御メカニズムは今後、人工知能（AI）や機械学習（ML）を用いるアプローチを含むものへと進化すると予想されます。AIとMLは、フィッシングの検出や、真正なものを装う偽のウェブサイトやリンクの識別に活用することができます。また、AIとMLを視覚認識技術に適用することで、次世代のサイバーセキュリティ企業が潜在的脅威の探知能力を向上させることができます。当然ながら、AIとMLが進化するためには、大量のデータにアクセスできなければならず、トレーニングのためにはマルウェアのような不正なデータも必要です。

確実に増加するサイバーセキュリティへの支出

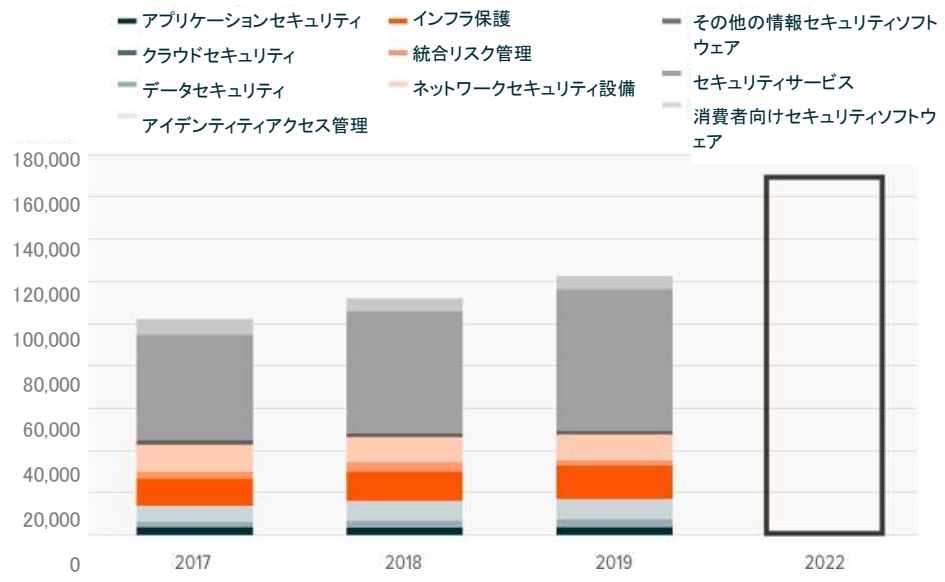
サイバーセキュリティは、IT投資の中でもっとも急速に成長している領域の1つです。米国中の最高情報責任者（CIO）は異口同音に、サイバーセキュリティを最優先の投資対象に挙げています。[7]企業がサイバーセキュリティに多額の費用を投じるのも当然です。2019年には、データ漏洩の平均損害総額は1社当たり390万ドルでした。そのうち36%は、顧客の信頼が失われたために生じたものです。[8]

不正プログラムの件数は過去最高の9億2,500万件を記録していることから、セキュリティ関連のソフトウェアやハードウェア、サービスに対する世界全体の支出額は、年末までに1,240億ドルに達する可能性があります。[9、10]2022年までに、世界全体の支出額は1,704億ドルに達する可能性があり、これは5年間の年平均成長率（CAGR）では、10.9%になります。[11]サイバー犯罪の脅威が拡大していることから、サイバーセキュリティは今や、サイバー攻撃により発生する費用負担と影響を恐れる企業にとって、コスト削減策と考えられることも多いのです。

同様に、サイバーセキュリティ導入のための政府支出も増加しています。2018年5月に発効したEU一般データ保護規則（GDPR）は、個人情報を処理する際に安全性、保護、透明性を確保するよう求めています。

米国ではサイバーセキュリティが優先事項であり、規制当局はGDPRに類似した法令制定に向けて取り組みを継続しています。2019年の連邦予算では、2018年に比べて5億8,340万ドルの増加（4.1%増）となる、150億ドルがサイバーセキュリティに充てられました。[12]サイバーセキュリティは国家レベルの課題でもあるのです。
カリフォルニア州では2018年に、住民に自身のデータを管理する権利を付与する、データ保護法が成立しました。このような法令により企業サイドでは、サイバーセキュリティを早急に向上させ、スキャンダルを回避できるよう対処すべきだという切迫感が高まっています。

2017年～2022年の世界全体の分野別セキュリティ支出額（百万米ドル）
出所：ガートナー、2019年～2022年のデータは予測値。



結論

デジタルトランスフォーメーションがあらゆる業種で起こっていることを踏まえると、サイバーセキュリティ対策が場当たり的なものであってはなりません。先見的なセキュリティ対策が不可欠です。データ漏洩の発生を防ぐことで、望ましくない経済的・政治的影響を軽減することが可能です。日々企てられている、そして複雑になる一方の何百万ものサイバー攻撃の脅威を見れば、サイバーセキュリティ企業のサービスに対する需要が増え続けるであろうことは明らかです。サイバーセキュリティは、世界中の企業や消費者、政府機関のサイバー犯罪対策において中心的役割を担っています。セキュリティや個人情報保護に関する対策・方針を向上させる必要性を考慮すれば、サイバーセキュリティ企業には事業拡大の機会が訪れていると言えるでしょう。

1. サイバークライムマガジン、「Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021（2017年～2021年の世界のサイバーセキュリティ支出は1兆ドルを超える見込み）」2019年6月10日。
2. Domo、「Data Never Sleeps 5.0」2017年。
3. Domo、「Data Never Sleeps 7.0」2019年。
4. 注：Zscaler Cloud Activity Dashboard（データは常に更新されています）より抜粋（2019年10月11日アクセス）。
5. Verizon、「2019 Data Breach Investigations Report」2019年。
6. 注：カーネギーメロン大学言語技術研究所（Language Technologies Institute）が開発したサイバーセキュリティ・タクソノミー。分類にはサイバーセキュリティの技術的側面のみが考慮されている。2019年10月15日アクセス。
7. IDC、「Developing Your Security Fabric: A Transformational Approach for State Government（セキュリティの網を構築する：州政府のための革新的アプローチ）」2019年5月。
8. IBM、「Cost of a Data Breach Report 2019」2019年。
9. ガートナー、「Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019（ガートナーが、世界の情報セキュリティ支出が2019年に1240億ドルをこえると予測）」2018年8月15日。
10. パロアルトネットワークス、「2019 Analyst Meeting（2019年アナリスト会議）」2019年9月4日。
11. ガートナー、「Forecast Analysis: Information Security, Worldwide, 2Q18 Update（予測分析：世界の情報セキュリティ2018年第2四半期）」2018年9月14日。
12. ホワイトハウス、「Cybersecurity Funding（サイバーセキュリティ資金）」。2019年10月24日アクセス。