accenture

2020 サイバー脅威の動向

エグゼクティブ・サマリー

Accenture Security

目次

2020年の所見

この1年間は、これまで誰も経験したことがないほど、企業のセキュリティ戦略とその実践が試されました。

急速に加速するデジタルトランスフォーメーション（DX）、混乱に便乗して横行するフィッシング、企業の情報セキュリティ運用の途絶と財務的な制約などが、COVID-19（新型コロナウイルス感染症）のパンデミックで混乱した世界に拍車をかけています。現状の課題を十分に理解し、組織のセキュリティ戦略をピボット（方向転換）できるCISO（Chief Information Security Officer：最高情報セキュリティ責任者）の存在は、組織にとって大きな強みとなります。

アクセンチュアのサイバー脅威インテリジェンスチーム（以降、「アクセンチュアCTI」）は20年以上にわたり、関連性の高い、タイムリーで実用的な脅威インテリジェンス（サイバー脅威への対策）の作成と提供を続けてきました。現在、アクセンチュア セキュリティ グループには、20年以上にわたる脅威インテリジェンスレポートに加え、2020年3月 にContext Information Security[1]を、2019年6月にシアトルを拠点とするSoT（Security of Things：モノのセキュリティ）企業、Deja vu Security[2]をアクセンチュアが買収したことで、コネクテッドデバイスやIoT（Internet of Things：モノのインターネット）ネットワークのセキュリティを確保するためのテクノロジー、ツール、手法に関する深い専門知識が結集しています。アクセンチュアCTIは、実践的かつ関連性の高い、有意義な情報を提供することで、企業のITセキュリティとビジネスオペレーションの意思決定を支援しています。

前回作成した2019年レポート[3]以降、アクセンチュアCTIとアクセンチュアのインシデント対応チームは、サイバー攻撃者の活動および金銭目的のターゲティングが疑われる多数の事象を調査してきました。調査を通じて、脅威インテリジェンスのアナリストとインシデント対応チームは、サイバー攻撃者が用いているている巧妙な手法、技術や手順を明らかにしてきました。

これにより、直近12か月間[4]のサイバーセキュリティ脅威の変化を的確に捉えています。2020年初旬に始まったCOVID-19のパンデミックにより、世界中のほとんどの企業がリモートワークへの急速な転換を余儀なくされています。計画どおりに実行している企業もあれば、何とか対応したものの多くの課題を抱えている企業や、そもそも計画すらしておらず慌てて導入を試みている企業もあります。リモートワークの普及によって、プラットフォーム、デバイス、データを送受信するネットワークなどにおけるさまざまなセキュリティ課題が浮き彫りになっています。IT環境の利用と操作に不慣れな従業員は、サイバー攻撃者やサイバー犯罪集団の格好の標的となるため、企業のソーシャルエンジニアリング（人の不注意や心理的な隙を突いて情報を盗み出す手法）のリスクは急速に増加しています。世界的な経済およびビジネスの混乱は、企業の財務面にも大きな打撃を与えています。当然、組織のセキュリティ運用にもその影響は波及しており、セキュリティ部門はこれまで以上に厳しい予算と制約の中で、守備範囲を維持、あるいは拡大しなければならない状況に置かれています。

1「Accenture Acquires Context Information Security, a UK-Based Cybersecurity Consultancy（アクセンチュア、英国を拠点とするサイバーセキュリティコンサルティング会社のContext Information Securityを買収）」アクセンチュア、2020年3月6日ニュースリリース
https://newsroom.accenture.com/news/accenture-acquires-context-information-security-a-uk-based-cybersecurity-consultancy.htm

2「Accenture Acquires Deja vu Security, Seattle-Based 'Security of Things' Company（ アクセンチュア、シアトルを拠点とするSoT［Security of Things：モノのセキュリティ］企業のDeja vu Securityを買収）」アクセンチュア、2020年6月17日ニュースリリース
https://newsroom.accenture.com/news/accenture-acquires-deja-vu-security-seattle-based-security-of-things-company.htm

3「2019 Cyber Threatscape Report」アクセンチュア
https://www.accenture.com/us-en/insights/security/cyber-threatscape-report-2019

4 最新調査「2020 Cyber Threatscape Report」は2019年6月～2020年6月の期間で実施しています。

巧妙なサイバー攻撃者は、政権の存続、経済の加速、軍事的優位性、情報操作、サイバースパイ活動など、攻撃者にとっての長年の目的を果たすために新たなTTPsを生み出し攻撃を続けています。本レポートでも後述しますが、アクセンチュアの脅威インテリジェンスのアナリストは、攻撃者がMicrosoft Exchange ServerおよびOWA（Outlook Web Access）環境を対象とする新たなインプラントや、内部プロキシのメカニズムを介して検出を妨害する巧妙なコマンドアンドコントロールなどの技法を開発している状況を明らかにしてきました。

多くのデータやネットワークへの不正アクセスなどの犯行は金銭目的で実行されるため、今日の不況下でサイバー攻撃もより増加する可能性があるでしょう。今年発見された手口の中には、防御をすり抜けるよう設計されたカスタムツールの存在を示す証拠もあり、また、サプライチェーンのセキュリティや既製ツールの脆弱性を突くような手口もますます増えることが予想されます。

人々にとってデータの重要性が高まるにつれ、悪意のある攻撃者の間ではランサムウエアへの期待値が上昇します。「Maze（メイズ）」[5]など、まったく新しい手法のランサムウエアを用いた「Name and Shame（名指し非難）」の攻撃手法が勢いを増しており、従来のコストと混乱を天秤にかけるだけの議論の有効性が揺らぎ始めています。

このようなサイバー脅威に対して企業が安定した事業を維持するためには、CISOによる安全な環境の確立と適切な管理が重要になります。アクセンチュアでは、「安全なマインドセット」「安全なネットワークアクセス」「安全な作業環境」「安全なコラボレーション」というアダプティブセキュリティの4つの要素を特定しています。CISOは組織のサイバーセキュリティにおけるレジリエンスを高めるために、ビジネスリーダーと協力し、適切なリソースと投資に裏打ちされた計画を策定して準備を整え、実践していく必要があります。アクセンチュアは、作業効率を高める業務フローと日常的な組織間の連携が確立された多面的な危機管理戦略こそが、サイバーセキュリティのレジリエンスを向上し、企業をサイバー脅威から保護するために有用であると考えています。

2020年の調査で特定された5つの最新トレンドについて、さらに掘り下げて見ていきましょう。これらのインサイト（洞察）は、セキュリティチームの業務を強化し、セキュリティ技術への投資とセキュリティプロセスおよびビジネス戦略を盤石にし、望ましいレベルのサイバーレジリエンスを達成するために役立ちます。

5 Lawrence Abrams著「Allied Universal Breached by Maze Ransomware, Stolen Data Leaked（Allied Universal、Mazランサムウエア攻撃により、盗まれたデータが流出）」Bleeping Computer、2019年11月21日記事
https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

5つの最新トレンド

「2019　サイバー脅威の動向」では、サイバーセキュリティへの企業の投資は、決して不十分ではないことが示されました。しかし、サイバー犯罪者や国家からの絶え間ないプレッシャーや、サプライヤー、パートナー、買収企業のサイバー防御との態勢のギャップ解消に対処するための優れた脅威インテリジェンスを確立する取り組みに投資が偏重している傾向がありました。

「2020 Cyber Threatscape Report」では、新たにサイバー脅威の状況に影響を与える5つの要素を特定しています。

01 COVID-19（新型コロナウイルス感染症）の影響によりアダプティブセキュリティに対するニーズが加速

パンデミックによって浮き彫りになった問題を瞬時に解決する方法はありません。現在のようなパンデミック下では、社会および企業は人々の健康と人道的側面の保護を優先的に管理します。加えて、企業は、組織全体の財務と事業継続への負荷を緩和する必要があり、中長期的な情報セキュリティ戦略に十分な予算を配分することが難しくなります。COVID-19のパンデミックによって、混乱に便乗したセキュリティ脅威が増え、新たなフィッシングなどのソーシャルエンジニアリングによる被害は拡大しています。すでに事業継続性、移動制限、リモートワークなどの対応に苦慮している企業にとって、これまで経験したことのない負荷がかかっています。悪意のある攻撃者にとって、データは価値と需要の高い「商品」です。セキュリティ責任者は、適切な制御と監視の体制を整えて安全な業務環境を構築するために、アダプティブセキュリティ[6]の導入を早急に検討する必要があります。

6「COVID-19：Emerge stronger with adaptive security（アダプティブセキュリティ導入による強化）」アクセンチュア、2020年6月Now Next
https://www.accenture.com/gb-en/insights/security/coronavirus-adaptive-security

02 事業継続性にリスクをもたらす最新の巧妙な攻撃手口

巧妙なサイバー攻撃者は、クライアントアクセスサーバー（CAS）などのMicrosoft Exchange Server[7]およびOWAに対応したシステムを積極的に標的としており、企業のプラットフォームはまさに包囲されている状態にあると言えます。このようなセキュリティの脆弱性は悪意のある活動の温床となります。一般に外部と通信するウェブ型のデータ集約システムおよびサービスでは、攻撃者が攻撃トラフィックをバックグラウンドノイズに隠すことが容易なため、認証サービスなどがクレデンシャルハーベスティングの踏み台とされる危険性があります。企業のプラットフォームへの攻撃は、必ずしも巧妙な手口ばかりではありません。攻撃者は常に脆弱性を悪用するための手法を進化させており、粗雑で単純なものから高度なものまでさまざまな手口が存在します。政府機関に対する最近のサイバー攻撃では、恐らく防御を回避するために新しく設計されたと見られる、内部ルーティングが可能なコマンドアンドコントロール・インフラストラクチャで構成されたマルウエアファミリーが検出されています。このように進化し続ける攻撃手口への対処は、ネットワークセキュリティ担当者にとって深刻な課題です。国や地域と連携している事業者は、情報を収集するために、ステルス性と継続性を最も重視する必要があります。攻撃の特性と検出回避の手法に対しては、優先度の高い攻撃を特定して追跡し、一連のトランザクションの中からいち早く脅威を見つけ出すことが重要になります。

7 アクセンチュアCTIの内部調査

03 マスキングやノイズが付加されたサイバー攻撃の検出が複雑化

サイバー攻撃者は、企業が活用している既存のツールと身近なテクノロジーを結び付けて巧妙に攻撃を仕掛けるため、攻撃の検出と特定は非常に複雑になります。既製ツールには拒絶性、継続的な有効性、使いやすさなどの利点も多く、当面は企業でも利用を継続していくことになるでしょう。スピアフィッシング攻撃（特定の組織や個人を対象としたフィッシング攻撃）もまた巧妙化しています。すでに認知されている脅威グループは、政府機関や企業を標的として情報を盗み出しています。このような脅威は主にヨーロッパ、北米およびラテンアメリカで活発化しており、新興経済国やインドを標的とした重大なインシデントも確認されています。攻撃者の多くが組織化されたサイバー犯罪グループであり、標的とする企業のサプライチェーンへの攻撃を続けています。マネージドサービスプロバイダーやソフトウエアベンダーは常に標的となりますが、共同プロジェクトに取り組む同業者間の接続環境などもまた悪用される場合があります。特定された攻撃に焦点を当てたインテリジェントなセキュリティアプローチと同様に、戦略から戦術、テクノロジーに至るまで、特定の組織プロファイルに合わせてカスタマイズした個別かつ継続的な脅威インテリジェンスを確立することが、セキュリティ対策における優先課題となります。まずは、一般的なツールと手法、特にネイティブシステムや侵入テストツールを悪用した手法を確実に理解し、企業内でそれらの検出が可能か評価することから始めましょう。

04 ランサムウエアが、より収益性の高い攻撃モデルの台頭を後押し

攻撃者はランサムウエアを企業に感染させるための新たな方法に加え、被害者に支払いをさせるための新しい手法も研究し続けています。米国の大手セキュリティ人材派遣会社は、2019年11月に「Maze」と呼ばれる新種のランサムウエアを用いた攻撃に遭い、企業データを盗まれるとともに、暗号化されたデータを復旧するにあたり攻撃者から脅迫を受けました。データの復号を引き換えとする身代金の支払いを拒否したところ、攻撃者によって盗まれたデータのうち700MB分の情報がインターネット上で公開されてしまいました[8]。「Name and Shame（名指し非難）」の手法では、法的機関やサイバーセキュリティ業界は身代金を支払わないよう助言しているものの、攻撃者は被害者が支払わざるを得ないような状況を作って脅迫してきます。ランサムウエアのリカバリー対応も行っているCovewareの報告では、2020年第1四半期の身代金の平均支払い額は、前年同期比60％増の17万8,254米ドルに達しています[9]。攻撃者だけが不当に利益を上げているのです。状況はさらに悪化する可能性があります。攻撃者の利益が増大することで、より高度なランサムウエアの開発と投資が可能になるため、リモートワーク環境などのさらに大規模な脆弱性を悪用した攻撃が可能になります。アクセンチュアの分析では、2020年以降も「Name and Shame（名指し非難）」の手法を採用する攻撃者は増殖し、ますます進化していくことが予測されます。

8 Lawrence Abrams著「Allied Universal Breached by Maze Ransomware, Stolen Data Leaked（Allied Universal、Mazeランサムウエア攻撃により、盗まれたデータが流出）」Bleeping Computer、2019年11月21日記事 https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

9「Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase（第2四半期は、企業とRasS＜Ransomware-as-a-Service＞間の断絶を突くランサムウエア攻撃が需要と共に増加）」Coveware、2020年8月3日レポート https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report

05 コネクティビティがもたらす負の側面

強力なテクノロジーの普及によって、外部との接続がより増加しました。その結果、多くの重要なシステムをインターネット上で活動するサイバー攻撃者にさらすこととなり、攻撃者は悪用するための新しい手法を日々研究し生み出し続けています。昨今は、修正パッチを適用していないデバイスやセキュリティ検証をしていないデバイスを使用している企業も増えており、それらの企業は攻撃者にとって確実かつ容易に侵入できる格好の標的となります。クラウドやインターネットに接続するデバイスはますます増える一方です。企業のセキュリティ部門では、バグバウンティプログラム（公開しているプログラムにバグがあることを想定して報奨金をかけて公開し、一般人（ホワイトハッカー）がバグを発見して脆弱性を報告して報奨金を受け取るという制度）や検出フレームワークを適用し懸命に対処していますが、OT（運用・制御技術）の脅威は増加傾向にあり、セキュリティ責任者には、より効果的なセキュリティ管理を実践することが求められています。セキュリティ検証は費用が高額になりがちなため、企業内ですべてのデバイスのリスク評価を行うことは困難です。また、メーカーの企業規模によって検証範囲や評価方法が大きく異なる場合もあります。徐々にではありますが、脅威は特定され、確実に対処されています。本レポートでも詳解しているとおり、2020年にベンダーがパッチ適用により対処したOTセキュリティの脆弱性に関する報告件数は増加しています。IoTデバイスに影響を与える一般的なレベルの脆弱性の多くは、少なくとも部分的には解決されているため、同様の対処を該当するすべてのケースに適用することが、現在の最善策と言えるでしょう。セキュリティ責任者は、解決されている対処方法を共有してシンプルかつ統合が容易で標準化された堅牢なセキュリティシステムを構築し、迅速に対処していく必要があります。

本レポートでは、サイバー脅威の最前線のトレンドを調査し、マインドセット、ネットワークアクセス、作業環境、およびコラボレーションを保護するアダプティブセキュリティを企業が適用するために、有用かつ実践的なプラクティスを提示しています。

アクセンチュアCTIは、有意義な情報を提供することで、クライアント、パートナー、コミュニティが、ビジネス、業界、地域に関連するサイバー脅威に対抗できるよう支援しています。

柔軟性の高い未来

2020年に健康と人道的危機が発生し、世界中がその影響を受けるということを、1年前には誰も予測できませんでした。

また、このように前例のない状況が巧妙なサイバー犯罪の発生と進化を助長するということも、誰も予見できませんでした。

サイバー攻撃者は新たにリモートワークに移行した人々を標的として、信頼されている公式サイトなどを模倣しトラップを仕掛けてきます。

セキュリティオペレーションセンターでは、事業継続性を脅かすトレンドやテクノロジーを特定するために、戦術、運用、戦略における脅威インテリジェンスの活用が不可欠だと考えています。

組織がより柔軟性が高く安全な未来を実現するためには、次の取り組みの実践が有効です。

「いつでも、どこでも」という考え方

場所を問わず、すべてのユーザー、デバイス、ネットワークトラフィックに対して、一貫したセキュリティを適用し同じレベルの効果を実現しましょう。安全なネットワークアクセスとアプリケーションを実装する際には、セキュリティ対策を実装する前と同程度の処理能力を維持できるかという点についても十分に考慮する必要があります。

透明性を保つ

ユーザーが必要な時に、必要な情報にアクセスできるようにします。運用変更等の際に、「ユーザー任せで何とかさせる」ということのないように、誰もが正しく理解することができる運用を維持しましょう。

安心と自信を提供する

セキュリティリーダーが組織変革のカタリストとなり、共感と思いやりをもってアジャイルに対応することが大切です。アダプティブセキュリティを採用することで、クラウド活用やリモートでのユーザーアクセスを安心して拡大することができます。

できる限りシンプルに

マネージドサービスの導入を検討し、必要に応じて業務の自動化を推進します。例えば、セキュリティイベントの応答、ツールの展開、ルールの管理などの一次対応を自動化することなども検討してみましょう。

レジリエンスの構築

組織をより強化するためには、目標に沿った事業継続性と危機管理計画の策定が重要です。ビジネスリーダーは、危機は頻繁に発生する可能性があることを想定し、行動しなければなりません。また、セキュリティに対する考え方を変える必要があります。すべてを自社で賄う方法は、本当にコスト効率が良いのでしょうか。エコシステムのセキュリティを確立するのであれば、グローバル企業のテクノロジーやノウハウを利用したほうが効率的な場合もあります。適切なリソースと投資に裏打ちされたより優れたサイバーセキュリティのレジリエンスを獲得するために、ビジネスリーダーと協力しながら計画、準備、実践していきましょう。

これらの取り組みを実践することで、企業は不確実性を克服し、危機的状況から力強く立ち上がり、サイバーレジリエンスを高めることができます。

本レポートについて

「2020 サイバー脅威の動向」は、Context Information Security、Deja vu Securityをはじめ、アクセンチュアが最近買収を完了した企業の多大な貢献のもとで、アクセンチュアのサイバー脅威インテリジェンスチーム（以降、「アクセンチュアCTI」）による調査と分析から得られた主要な知見に基づき作成されました。

本レポートでは、2019年6月～2020年6月までの期間で、アクセンチュアCTIが把握、分析したサイバー脅威トレンドを報告しています。トレンドの概要と展開に関するアクセンチュアCTIの年間予測を詳しく解説しています。

本レポートは、アクセンチュアのサイバー脅威インテリジェンスに基づく関連性の高い実用的な情報を提供することで、組織のITセキュリティ部門および事業運用部門の意思決定を支援するために作成されており、日々のインテリジェンスレポートを戦略的に補完する資料として活用することができます。本レポートを通じてITセキュリティ部門、事業運用部門、組織のリーダーに、サイバー関連の新たなトレンドと脅威を周知し、未来のビジネスのカギとなるサイバーセキュリティの開発および実装を促進します。アクセンチュアでは、状況に適した一次的および二次的な公開資料を使用し、組織がセキュリティ評価コストを軽減するための、さまざまなソリューションも用意しています。

アクセンチュアについて

アクセンチュアは、デジタル、クラウドおよびセキュリティ領域において卓越した能力で世界をリードするプロフェッショナル サービス企業です。40を超える業界の比類のなき知見、経験と専門スキルを組み合わせ、ストラテジー＆コンサルティング、インタラクティブ、テクノロジー、オペレーションズサービスを、世界最大の先端テクノロジーセンターとインテリジェントオペレーションセンターのネットワークを活用して提供しています。アクセンチュアは51万4,000人の社員が、世界120カ国以上のお客様に対してサービスを提供しています。アクセンチュアは、変化がもたらす力を受け入れ、お客様、社員、株主、パートナー企業や社会へのさらなる価値を創出します。

ウェブサイトを見る：**www.accenture.com/jp**

アクセンチュア セキュリティ グループについて

アクセンチュア セキュリティ グループは、高度なサイバー防御、アプライドサイバーセキュリティソリューション、マネージドセキュリティオペレーションなど、エンドツーエンドのサイバーセキュリティサービスを提供するリーディングプロバイダーです。高度なテクノロジーとインテリジェント・オペレーションセンターのネットワークを通じた世界規模のデリバリーとサポートによって、お客様企業のセキュリティを革新します。アクセンチュアは、企業が安全にイノベーションを推進し、サイバーレジリエンスの構築と力強い持続可能な成長を実現するために、高度なスキルを備えた専門家チームによる支援サービスを提供しています。

詳しくはウェブサイトをご参照ください：
www.accenture.com/jp-ja/services/security-index

www.accenture.com