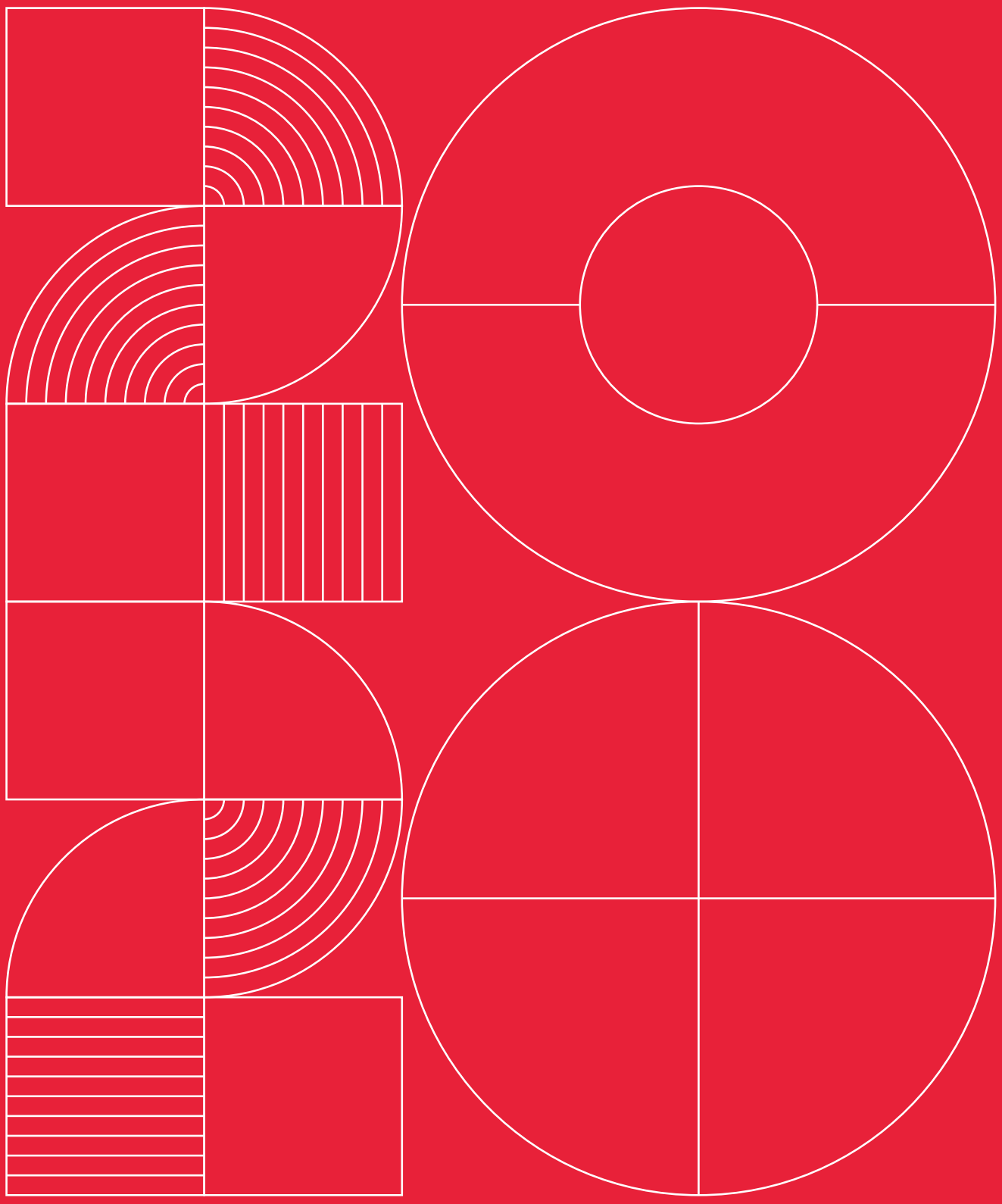


2020年セキュリティ脅威予測

TREND MICRO | research

Published by Trend Micro Research

Stock images under license from Shutterstock.com

最近の注目すべき事例や傾向は脅威の転換期を意味しており、2020年は新たな脅威の10年を迎える節目になるでしょう。2020年以降のサイバーセキュリティは、さまざまな視点から捉える必要があり、その範囲は攻撃者およびサイバー犯罪者の動機や手口から、技術の進歩や全世界の脅威インテリジェンスまで多岐にわたります。これらを網羅することで、サイバー犯罪の主要な手口、脅威の大きな変化、新たな脅威の登場を予測することが可能になります。

社内ネットワークがファイアウォールの隔離だけでよかった時代は過去のものとなり、企業のアプリケーションがわずかな数に限られていた時代は終わりました。今やさまざまな種類のアプリ、サービス、プラットフォームが入り乱れ、それらすべてにセキュリティ対策が求められています。多様な実装やシステム全体の変化に対応する多層防御は、これら広範囲の脅威に対抗するために欠かせないものとなるでしょう。

今までもネット恐喝、難読化、フィッシングなどの手法が成果をあげてきた一方、これからは、さらに新たな手法が登場してくるでしょう。例えば、クラウド移行の増加に伴い、設定ミスなどのヒューマンエラーによるリスクの増大が懸念されます。ネットにつながる膨大な資産やインフラが深刻なセキュリティの課題を生み、それによって脅威に晒されることとなります。さらに企業を騙す詐欺手口の中でAIが悪用されるなど、従来のセキュリティリスクと新たな技術が融合することで、企業が直面する脅威はさらに複雑さを増していくことが予測されます。

本レポートは、現在の脅威、新たに登場してくる脅威や技術に関し、当社のセキュリティ専門家の知見をもとに想定される技術発展や脅威の巧妙化の観点から、将来予測されるシナリオを解説しています。さらに本レポートは、2020年および今後数十年で直面するセキュリティ課題において、企業の適切なセキュリティ戦略および意思決定に必要な情報を提供することを目的としています。

※註: 本レポートに掲載される通貨の換算レートは特に断りが無い場合、本レポートの執筆時点（2019年11月24日付け1米ドル108.6円）のレートとなります。

複雑化する脅威

長年にわたる脅威の巧妙化が、利益のためにシステムを侵害する攻撃者を防ぐことは困難であることを示しています。攻撃者はこれからも、企業やユーザの先手を取るため、手をかえ品をかえ、さまざまな攻撃経路や攻撃手法を駆使してくるでしょう。

不完全な修正パッチを狙う攻撃の増加

システム管理者は修正パッチ適用のタイミングだけでなく、修正パッチの品質にも注意する必要があります。重要なシステムに低品質の修正パッチが適用されることで、基幹となる機能が破損したり、修正パッチの欠陥に伴う障害が発生したりする可能性があります。また、修正パッチ適用の遅れは、既知の脆弱性が悪用されるリスクにつながります。修正パッチに問題がある場合は攻撃者の侵入箇所が放置されることになりますが、今後予測されるのはこうしたリリース後の修正パッチの品質が十分でなく、攻撃が行われてしまうケースの増加です。例えば、攻撃者が修正パッチ内のコード数行を変更するだけで、対象の脆弱性を再び悪用できます。2018年にMicrosoft社のデータベースエンジン「Jet Database Engine」のゼロデイ脆弱性（当時）へ修正パッチが適用された際、品質に問題があったため、修正が不十分となり、脆弱性が悪用されるリスクを完全に排除できませんでした[1]。さらに2019年には、Cisco社のルータの脆弱性が攻撃されており、後日修正パッチが不完全であったことが判明しています[2]。

また、攻撃者はオープンソースのライブラリを利用するユーザが修正パッチを見過ごすケースを狙ってくるでしょう。さらに修正パッチリリース後から適用されるまでの期間も狙ってきます。これは脆弱性のあるライブラリを使用している製品に対して、修正パッチが届くまでに時間を要するためです[3]。なお、修正パッチで解決されない場合や製品への適用までに時間を要する場合、仮想パッチで既知および未知の脆弱性の対策を講じることが可能です。

サイバー犯罪者がアンダーグラウンドの取引にブロックチェーンを利用

サイバー犯罪が活発化することでアンダーグラウンドは発展を続けていきます。高いリスクが伴う取引で信頼性に依拠した「審査支払い」や「エスクロー支払い」が実施[4]されていることから、アンダーグラウンド市場では「信頼」が今後さらに重要な役割を果たすことになります。今後はブロックチェーンが買い手と売り手の間での分散型トラストシステムを確立する新たな手段となるでしょう。ブロックチェーンでスマートコントラクトを用いることにより、サイバー犯罪者は仮想通貨の支払いを正式なものとし、支払い履歴をブロックチェーンによって記録することができます。さらには匿名性を保持して出口詐欺のリスクを減らす上でも、取引で分散型の手段が利用できるブロックチェーン市場にサイバー犯罪者が注目してくるでしょう[5]。なお、ランサムウェアや「サービスとしての犯罪（Crime-as-a-Service）」のビジネスモデルのような脅威も、簡単に金銭的利益を得たいサイバー犯罪者によって今後も長く用いられることになるでしょう。

---

1 https://www.zdnet.com/article/microsoft-jet-vulnerability-still-open-to-attacks-despite-recent-patch/
2 https://www.securityweek.com/cisco-improperly-patched-exploited-router-vulnrabilities
3 https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping/
4 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/your-word-is-your-bond-trust-and-ethics-in-underground-forums
5 https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene

オープンバンキング普及でATMマルウェアに狙われる銀行システム

2020年はオンラインバンキングや決済システムを狙うモバイル向けのマルウェア攻撃が増加してくるでしょう。欧州においては多くの銀行がモバイル決済に対応していくことで、こうしたオンライン決済がさらに増加すると考えられます[6]。欧州連合(EU)では「改訂版決済サービス指令(PSD2)」が既に施行され、他の国々も追随する中[7]、こうしたオープンバンキングはさらに広く普及していくでしょう。他方、これに伴い、バンキングAPIの欠陥からフィッシング詐欺の新たな手口まで、セキュリティの課題が銀行に大きく影響することが予測されます[8]。金融業界の関係者は、設計上安全なソフトウェアの開発、定期的なセキュリティ監査の実施など、さまざまな対策を講じる必要があります。

その他、ATMマルウェアが広く利用され、主要なマルウェアの地位を確立することになるでしょう。既に「Cutlet Maker」、「HelloWorld」、「WinPot」といったATMマルウェアの亜種を販売する広告が確認されています。これらのATMマルウェアファミリーが、アンダーグラウンドで大きな存在感を示してくることが予測されます[9]。

企業を欺く次なる手口はディープフェイク

ビジネスメール詐欺[10]などメールによる手口は、西アフリカ地域を拠点とする詐欺集団に長く利用されてきました[11]。こうしたメールによる詐欺は継続するとともに、2020年はAIのような新たな技術を駆使した詐欺手口の巧妙化が予測されます。例えばAIを利用すれば、本人がしていない言動をあたかも本人がしたような本物そっくりの音声や動画を再現することが可能になります。AIを駆使したこれらの偽装は「ディープフェイク」[12]と呼ばれ、その影響が懸念されています。ディープフェイクは有名人の偽のポルノ動画を作るためだけでなく、今後は企業の従業員や業務手順を欺くために利用される可能性があります。

2019年にはAIで生成した音声によるソーシャルエンジニアリングの手法を用いたサイバー犯罪が報じられました。この事例では、エネルギー企業の最高経営責任者(CEO)の声をAIで模倣し[13]、24万3,000米ドル(約2,640万円)の被害が生じたと伝えられています。AIを利用する手口は今後さらに増加してくるでしょう。ディープフェイクを用いて企業の経営幹部になりすまし、偽の送金や意思決定を指示する手口が、従来のビジネスメール詐欺(BEC)[14]やサポート詐欺にも導入されていくと考えられます。攻撃者はこれまでのなりすましメールだけでなく、視聴覚へ訴えるディープフェイクによる巧妙ななりすましを駆使してきます。そして、特に電話、会議、メディア出演、オンラインビデオなどで露出の多い経営幹部がなりすましの対象となるでしょう[15]。

---

6 https://support.apple.com/en-gb/HT206637
7 https://www.pwc.com/it/en/industries/banking/future-open-banking.html
8 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2
9 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground
10 https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf
11 https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds
12 https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html
13 https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
14 https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)
15 https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/

ディープフェイク検出でセキュリティリサーチャーを支援するため、Googleでは既に膨大な量のディープフェイク関連動画のデータを公開しています[16]。ディープフェイクを用いた詐欺は初期段階であるとはいえ、企業では音声のイントネーションやスピード、動画上の人工的な肌質など、ディープフェイクが疑われる要素には細心の注意が必要です。送金等の業務プロセスでは、追加の認証ステップが重要となります。

マルウェア拡散やサプライチェーン攻撃のため狙われるMSP

企業の外部委託が増加傾向にある現在、委託先などから企業に侵入することで、企業のセキュリティ対策の回避や業務プロセスを侵害[17]するサプライチェーン攻撃の不安が高まっています。特にマネージドサービスプロバイダ(MSP)のようなサードパーティでは、安易な信頼がセキュリティ上の大きなリスクとなります。

これまでサプライチェーン攻撃では、ソフトウェアのアップデートの乗っ取りや、不正なコードを標的企業へ送り込むためにサードパーティのサービスを侵害するなど、さまざまな手法がとられてきました[18]。特にサードパーティのサービス侵害では、主に中小企業で被害が起こると予測しています。中小企業ではインフラや業務の一部を外部委託していることが多く、サプライチェーン攻撃によって、これらを踏み台に侵入される可能性があるからです。

MSPを狙うサプライチェーン攻撃の場合、被害がさらに広がる可能性があります。攻撃者はサードパーティのサービスプロバイダを狙い、サイトに不正なコードを読み込ませて顧客の機密データを窃取します。また、セキュリティが手薄なディストリビューターやサプライヤーを見つけ、顧客企業へマルウェアを拡散させたりしてくるでしょう。2019年はソフトウェアプロバイダのセキュリティを侵害することで、数百に及ぶ歯科医院のシステムへランサムウェアを拡散させた被害事例が報じられました[19]。この傾向は衰えることなく、今後も継続するでしょう。

こういったマルウェア拡散による攻撃を防ぐため、企業は自社のシステムにアクセス可能なプロバイダや従業員に対するセキュリティチェックを厳守し、その上で定期的な脆弱性チェック、リスクアセスメント、予防措置などを実施する必要があります。

ワーム化とデシリアライズの脆弱性を悪用

2019年5月にMicrosoft社は、リモートコード実行(RCE)が可能となる重大な脆弱性に対する更新プログラムをリリースしました。この脆弱性はCVE-2019-0708として採番され、「BlueKeep」の名称で呼ばれています。同社は同様に、リモートデスクトップサービス(RDS)に関する複数の脆弱性に対しても更新プログラムを提供しています。これらの脆弱性を悪用してマルウェアをワーム化することで[20]、ランサムウェア「WannaCry」のように素早く拡散させることが可能になります。その一方で、BlueKeepを悪用した攻撃コードを作るには高度な技術が必要です。この脆弱性を悪用する「Metasploit」のモジュールがリリースされたものの、「EternalBlue」とは違い、使い勝手が悪いことが確認されています[21]。

---

16 https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html
17 https://www.trendmicro.com/vinfo/us/security/definition/business-process-compromise
18 https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/
19 https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/
20 https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/
21 https://arstechnica.com/information-technology/2019/09/exploit-for-wormable-bluekeep-windows-bug-released-into-the-wild/

それでもBlueKeepを悪用する脅威はさらに登場し、それ以外で深刻度が高い既知の脆弱性を悪用する攻撃が出てくることが予測されます。 Server Message Block（SMB）や上述のRDPなど、広く使用されているプロトコルは、脆弱性を悪用したシステム侵害を狙う攻撃者に注目されるでしょう。SMBはWannaCryやランサムウェア「NotPetya」に利用されていました。RDPもランサムウェア攻撃に利用されており[22]、ランサムウェア「SamSam」の事例では、RDP接続の公開デバイスをスキャンする手法が使われていました[23]。

その他、デシリアライズの脆弱性が企業の重大な懸念になると予測しています。信頼できないデータのデシリアライズ等の脆弱性が悪用された場合、企業では攻撃者によるデータ改変や攻撃者によるコード実行が可能となります[24]。シリアライズとは、多くのプログラミング言語が、オブジェクトをアプリケーション上で保存もしくは送信可能な形式に変換する際に用いる技術です。従って、デシリアライズとはその逆を意味し、保存もしくは送信可能な形式に変換されたオブジェクトをもとの状態に復元する手段です。この場合のリスクは、アプリケーション向けにシリアライズされたオブジェクトがデシリアライズされる際、不正な入力であっても事前検証がなされない点です。技術力の高い攻撃者であれば、不正なオブジェクトをアプリケーションのデータストリームに挿入し、アプリケーションサーバ上で実行させることができます。

攻撃者は複数の脆弱性を組み合わせて不正なコードを実行するよりも、代わりにデシリアライズの脆弱性を悪用してくるでしょう。これによって、複雑な環境に対しても容易に遠隔操作の権限を取得し、不正コードを実行できるからです。シリアライズとデシリアライズの仕組みは、Javaアプリケーション、多くのWebアプリケーションやミドルウェア製品で使用されています。この仕組みが導入されているプラットフォームを持つ企業は、直ちに修正パッチや仮想パッチ[25]を適用し、システムやソフトウェアが悪用されるリスクを認識しておく必要があります。

---

22 https://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-crysis-ransomware/
23 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/samsam-ransomware-suspected-in-atlanta-cyberattack
24 https://cwe.mitre.org/data/definitions/502.html
25 https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited

インターネットへの露出に伴う脅威

新旧の攻撃および手法が、情報技術（IT）と運用技術（OT）の双方において深刻な脅威となるでしょう。

諜報活動や恐喝を目的にIoTデバイスが狙われる

機械学習やAIを駆使するサイバー犯罪者や攻撃者が、今後企業内に設置されているスマートテレビやスピーカーなどのIoTデバイスを狙ってくることが予測されます。この場合、言語認識やオブジェクト識別を介して、個人的な会話やビジネス上の会話が傍受されることになるでしょう。その上で、サイバー犯罪者や攻撃者は特定の標的に狙いを定め、企業に対する恐喝や諜報活動などを遂行します。

サイバー犯罪者は、IoTを狙って金銭的な利益を得るため、5Gネットワークだけでなく、IoTが利用される幅広い範囲を対象に攻撃を展開してくるでしょう。IoTを狙う攻撃による収益化は始まったばかりです。サイバー犯罪者は、これからも多種多様な手口を試み、その中でもネット恐喝は、最も利用される可能性が高い手口となるでしょう[26]。

既にアンダーグラウンドでは、サイバー犯罪者の間で、さまざまなIoTデバイスを巡る金銭取得の手口が議論されています。まず個人ユーザ向けのデバイスでこれらの手口が試され、その後、企業向けの産業機械が狙われることになるでしょう。すでに製造業の機械を制御するProgrammable Logic Controller(PLC)を狙う手口に関し、アンダーグラウンドでの議論が確認されています[27]。

ルータなどのIoTデバイスは、ボットネット化されることで、サービスとして利用可能な分散ネットワークとして別のサイバー犯罪者に提供され、サイバー犯罪者の収益につながります。また、ボットネット化されたルータは、Domain Name Server(DNS)の乗っ取り、フィッシング攻撃などの攻撃のサービスとしても提供されます。その他、アンダーグラウンドで提供されるものに、Webカメラのビデオストリームや、改変されたファームウェアのスマートメーターへのアクセス権があります。インターネットへ露出したこれらのデバイスは、セキュリティ対策が手薄な点や、さまざまな攻撃を受けるリスクがある点などから、IoTセキュリティの対策を講じるべき領域として注目され、同時にサイバー犯罪者の間でも、格好の標的として議論の中心となっていくでしょう。

5Gの課題はSDNの移行に伴うセキュリティ導入

2020年、5Gの導入が本格化する中、関連するコードや環境間の動的なスイッチングの新たな技術において、多様な脆弱性が出てくることが予測されます。5G導入に伴う自動化の技術でも、コードの欠陥などといった問題が避けられないだけでなく、関連する脅威に対するベンダ自体の対策が不十分である点も課題となるでしょう。

5Gの環境では、ユーザや接続デバイスへ高帯域幅かつ高速接続を提供するSoftware-Defined Network(SDN)が用いられ、5Gネットワーク自体が、幅広い範囲でさまざまなアプリケーションや業種に利用

[26] https://www.trendmicro.com/vinfo/us/security/definition/digital-extortion
[27] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground

されることが期待されています。5Gネットワークは脆弱性が存在する可能性のあるソフトウェアやサプライヤーで管理されるため、脅威はまず脆弱性のリスクがあるソフトウェアや接続デバイス、攻撃経路などのネットワークトポロジーを起点に引き起こされる可能性があります。そのため、攻撃者が5Gネットワークを乗っ取る場合は、まずネットワークを管理するソフトウェアを狙ってきます。5G関連のデバイスやネットワークの更新は、スマートフォンのソフトウェア更新プログラムに類似しており[28]、そこには常に脆弱性が生じる可能性があります。実際に5Gの脆弱性を悪用する手法は、既にセキュリティリサーチャーによって、低コストのハードウェアやソフトウェアのプラットフォームを用いたデモで実証されています[29]。サイバー犯罪者が実証された手法を悪用するのも時間の問題でしょう。5Gネットワークにおけるセキュリティ対策の不備は、機密性（データやトラフィックの諜報活動）、整合性（送信データの改変）、可用性（各セクターを結ぶネットワークの中断）などの範囲に及び、さまざまなタイプの脅威が、より一層深刻化する可能性があります[30]。

こうした一方で、国やベンダのレベルでは、セキュリティ対策を後回しにしてでも一刻も早く5Gを実現すべきだという機運が高まっているようにも見えます。しかし、5Gのセキュリティ対策を後回しにした場合、拙速な移行と不十分な設定も相まって、この技術に依存する多くのサービスでさまざまな問題が生じてくる危険性があります。さらに、セキュリティ対策を5G展開後のインフラに導入させる場合、最初から5Gの展開と並行して導入する場合よりも、かえって複雑な状況を招く危険性もあります[31]。そして、こうした結果による不十分な対策のリスクを軽減させるためには、SDN特有の問題を特定できる専門家が必要となってきます[32]。ネットワーク機能が動的にシフトする場合、同様にセキュリティも動的であることが求められます。例えば、ネットワーク機能仮想化（NFV）や、アプリケーション仮想化を介したネットワークサービスが動的にシフトする場合、そのセキュリティも迅速なアプリケーション展開で対応する必要があります。

増加するサイバー攻撃と稼働停止に悩まされる重要インフラ

公益事業やその他の重要インフラは、2020年にサイバー犯罪者による恐喝の標的となるでしょう。ランサムウェアによるネット恐喝も、企業へ深刻なリスクをもたらすことから、引き続きサイバー犯罪者に利用されることになると考えられます。また、工場などの場合では、長期にわたる操業停止は多額の金銭的損失につながり、システムの復旧状況によっては、生産ラインが数週間ストップする可能性があります。攻撃者はボットネットを構築して、工場などの運用技術（OT）のネットワークに対して分散型サービス拒否（DDoS）攻撃などを仕掛けることが可能です。さらに、クラウドサービスプロバイダを採用している製造企業ではサプライチェーン攻撃のリスクもあるでしょう。攻撃者は、セキュリティが手薄なプロバイダを狙うことで、生産ラインをストップさせられるからです。そして、インフラでは最優先事項である可用性が危険にさらされます。こうした中、とりわけ「産業用モノのインターネット（IIoT）」を導入している企業でのセキュリティ対策が、より一層強く求められてくるでしょう[33]。

---

28 https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/
29 https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf
30 https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/eu-report-highlights-cybersecurity-risks-in-5g-networks
31 https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/
32 https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-enterprises-for-5g-connectivity
33 https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/securing-the-industrial-internet-of-things-protecting-energy-water-and-oil-infrastructures

ここ数年、さまざまな攻撃者が、諜報活動の攻撃キャンペーンを駆使して、世界中のエネルギー施設を標的にしています[34]。これらの攻撃キャンペーンでは、標的型攻撃においてランサムウェアによる攻撃を仕掛けるため、「産業用制御システム（ICS）」や、その一部の「監視制御およびデータ取得システム（SCADA）」を狙い、認証情報や施設運用情報を窃取します。こうして、セキュリティ侵害の影響は、重要インフラシステム内だけでなく、関係機関全体を巻き込み、地域の発電施設やエネルギー施設にも及び[35]、幅広い範囲に被害がもたらされることになります。

こういった攻撃によるシステム障害などの被害は公益事業にとどまりません。管理運用の中でIoTアプリケーションやヒューマンマシンインターフェイス（HMI）の利用が増えるにつれ、食料生産、輸送、製造施設など、さまざまな業界にも同様のリスクがもたらされることになるでしょう。

公的な重要インフラや政府系のITインフラは、民間セクターに比べて資金が不足する傾向があるため、セキュリティ対策が手薄になりがちです。諜報活動の攻撃キャンペーンで事前に窃取された各種情報を活用することで、インフラ全般だけでなく、特定の公共サービスや政策業務などの領域を含む広範囲に影響が及ぶ可能性があります。

ホームオフィスやテレワークで変わるサプライチェーン攻撃の手口

企業が講じるセキュリティ対策の境界線が曖昧となることから、在宅勤務やインターネットに接続された家庭用機器によってもたらされるリスクには注意が必要です。在宅勤務の場合、自宅のネットワーク環境は、企業と比べて安全性は劣ります。公共のワークスペースなど、社外で仕事をする場合も、セキュリティが脆弱なWi-Fi環境などのリスクが懸念されます。こういったオープンネットワークの領域では、機密情報や関連ファイルが公開されたままとなり、同一ネットワーク内の他のユーザに閲覧される可能性があります[36]。リモートデバイスの場合、デバイスがマルウェアに感染した状態で企業内ネットワークに持ち込まれることで、機密情報などが窃取される危険性があります。

現在のテレワークの普及により、従来のようにオフィスでPCに束縛されることがなくなりました。また、これまでのBYODとも異なり、今や在宅勤務の従業員は、接続された複数のデバイスを駆使し、クラウドベースのアプリやコミュニケーションツールへも自由にアクセスできます。スマートテレビ、スピーカー、アシスタントデバイスなど、多数の機器が業務でも使用できるようになるかもしれないことを考慮すると、これらのコネクテッドホームデバイスが、今後企業への攻撃経路として悪用される可能性は否定できません。こうした攻撃に対処するためにも、企業は機密情報を扱うための適切なセキュリティポリシーを設定することが必要になります。

サイバー犯罪者は既に盗んだ個人情報を駆使して、標的となる企業の従業員になりすまし、ホームネットワークやパブリックネットワークの双方を介して攻撃を仕掛けてきます。今後こうした攻撃手法は巧妙化し、ビジネスメール詐欺やビジネスプロセスを侵害する詐欺にも利用されるでしょう。従業員の自宅環境がサプライチェーン攻撃の起点となることが予測されます。

---

[34] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton
[35] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/
[36] https://www.cnet.com/news/weworks-weak-wi-fi-security-leaves-sensitive-documents-exposed/

設定ミスがもたらす脅威

クラウドとDevOpsへの移行はメリットがある一方、デプロイメントパイプラインのセキュリティの必要性を十分に認識していない企業は、さまざまなリスクに直面するでしょう。

DevOpsチームの重要課題はコンテナの脆弱性

コンテナ[37]の分野は急速です。リリースは素早く、アーキテクチャは継続的に統合され、ソフトウェアのバージョンは定期的に更新されます。そうした中、従来のセキュリティ対策はこういったスピードに対応できないでしょう。

コンテナの技術が企業にとって重要となり、これまでの方法が通用しなくなるにつれて、DevOpsを担う部門ではDevSecOpsの原則が重要になります。DevOpsによる急速な開発サイクルでは、セキュリティ対策や脆弱性診断などを実施する余地がほとんどなくなる危険性があります。また、企業は異なるクラウド環境上の仮想マシンに分散された数百のコンテナに安全性が求められることがあるかもしれません。企業はランタイム（Docker、CRI-O、Container、runC[38]等）、オーケストレーター（Kubernetes等）、ビルド環境（Jenkins等）の脆弱性など、コンテナアーキテクチャが有するさまざまなコンポーネントに関する課題に直面することになるでしょう。攻撃者はこれらの脆弱性に狙いを定め、DevOpsのプロセスを侵害する手口を見つけ出してくると考えられます。

また、広く使用されているコンテナイメージに脆弱性が存在する場合は、それらがダウンロードされることで、企業全体のプロセスに影響が及びます。コンテナイメージの修正がサードパーティに依存し、それが安全だと信頼している企業は、コンテナの修正パッチに気をつけなければなりません。さらに、コンテナ化されたアプリケーションの脆弱性は、コンテナのコードやエンジンだけでなく、スタック全体にわたる多数のコンポーネントへ影響が及ぶため、攻撃者はこれらを悪用してセキュリティ侵害を試みてくるでしょう。

サーバレス導入に伴う設定ミスや脆弱なコードが攻撃経路に

サーバレスのプラットフォームを採用することで、クラウドアプリケーションを統合し、コスト削減を目指す企業が増えています。調査機関「Gartner」は、2020年までに全世界の企業の20%以上が、こうしたサーバレスの技術を導入するだろうと予測しています[39]。サーバレスのプラットフォームは、企業が本来は自前のサーバで確保する機能を社外からのサービスで利用するモデルを意味します。これにより、企業の開発者は、自前のサーバやコンテナの準備で必要となるはずの費用を負担せずに、サービスを利用してコードを実行することができます[40]。ただし、サーバレスに移行したとしても、セキュリティ対策の問題がなくなるわけではありません。

---

37 https://www.trendmicro.com/vinfo/us/security/definition/container

38 https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-5736-runc-container-escape-vulnerability-provides-root-access-to-the-target-machine

39 https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras

40 https://www.zdnet.com/article/what-serverless-computing-really-means-and-everything-else-you-need-to-know/

サーバレスのアプリケーションでも、これまで同様に古くなったライブラリ、設定ミス、既知および未知の脆弱性などが攻撃経路となることが予測されます。攻撃者は依然として、これらを狙って機密情報の窃取や企業内ネットワークへの侵入が可能になります[41]。

サーバレスのプラットフォームでは、コンテナ、サーバレス機能、その他のさまざまな依存関係が影響するため、より一層複雑な形で脅威がもたらされる危険性があります。サーバレスが提供する機能では、特にそれらがオープンソースや、ステートレスであるため、アクセス許可の監視や機密情報の保存が企業にとって最大の課題になってきます。そのため、サーバレスのアプリケーションには、ネットワークの可視化だけでなく、プロセスの改善、ワークフローの文書化が必要となります。

こういったサーバレスの技術はコンテナベースでもあるため、展開に際してはDevSecOps部門の役割が重要となってきます。サーバレスの環境は、DevSecOps部門が目指す継続的な統合および利便性に合致するため、さまざまなメリットがあります[42]。一方、実際にサーバレスを導入して関連機能を展開していく上では、サーバレスのインフラに注力するため、オープンソースのアプリケーションにおける依存関係や脆弱性に対するセキュリティを講じることも重要になるでしょう。

設定ミスやサードパーティの不備で生じるクラウドのリスク

システムが定期的に更新され、適切な対策が講じられていても、展開時に設定ミスや認証の問題があれば、企業は深刻な事態に直面します。セキュリティ対策の基本が正しく実践されていないだけで、企業の情報は深刻な脅威にさらされることになるのです。

クラウドサービスの弱点によって企業のネットワークが侵害される被害が、増加していくことが予測されます。クラウドストレージの設定ミスによる情報漏えいは、2020年も引き続き、企業の大きな課題となるでしょう。例えば、不十分なアクセス制限、アクセス制御の不適切な運用、ログイン管理の不備、さらには誤って公開された機密情報など、これらは企業におけるクラウドネットワーク設定時に発生し得るミスのほんの一部に過ぎません。クラウドサービスに関連するこうしたミスや過失により、企業では膨大な数の機密情報が漏えいし、場合によっては罰金や懲罰が科せられるケースもあります。これらのリスクはインフラの適切な展開や設定を始め、クラウド上のセキュリティ対策を基本から見直し、業界基準のベストプラクティスの実施などによって回避することができます。

多くの企業や製造施設などでクラウドへの移行が進むにつれ[43]、サードパーティのサービスプロバイダに依存する企業が増加してくるでしょう。しかし、こうした企業では従来のプロセスやシステムに慣れている一方、クラウドには精通しておらず、こうしたインフラで講じるべきセキュリティ対策に長けていないことがリスクとなります。攻撃者はクラウドサービスの障害を狙い、サービスプロバイダに対して、ボットネットを駆使したDDoS攻撃を仕掛けてくることが予測されます。

41 https://www.theregister.co.uk/2018/05/15/stale_serverless_functions/
42 https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/serverless-applications-what-they-mean-in-devops
43 https://www.forbes.com/sites/willemsundbladeurope/2019/07/18/smart-manufacturing-creating-a-hybrid-cloud-edge-strategy/#2a437658af5a

クラウドプラットフォームがコードインジェクションの餌食に

2020年クラウドプラットフォームは、コードへの直接的な攻撃やサードパーティのライブラリを介したコードインジェクションの攻撃により、さまざまなセキュリティ侵害の被害に見舞われることになるでしょう。クラウド上のファイルや情報の盗聴または制御を試みる中で、不正なコードのインジェクションが行われます。クラウドサービスのWebアプリケーションを狙った一般的な攻撃としては、クロスサイトスクリプティング、SQLインジェクションなどが挙げられます。攻撃に成功すると、企業の機密情報が遠隔操作で取得されたり、データベースのコンテンツが改変されたりします。さらに、サードパーティのライブラリを狙った場合では、インジェクション攻撃された不正コードが、利用者にダウンロードされるなどして、他の組織へも被害を及ぼす可能性があります[44]。

こうして、クラウド上の情報を狙う攻撃は、これからも増加していくことが予測されます。「サービスとしてのソフトウェア(SaaS)」、「サービスとしてのインフラ(IaaS)」、「サービスとしてのプラットフォーム(PaaS)」など、クラウドサービスをベースにしたさまざまなビジネスモデルが広く展開されてくる中、これらのサービスへ標的を絞った攻撃が増加してくるでしょう。企業のデータがクラウドに移行するに従い、攻撃者の関心もそちらへ移行していきます。こういったクラウドを狙ったセキュリティ侵害を阻止するためには、開発者の責任の明確化、プロバイダやプラットフォームの慎重な選定、クラウドセキュリティに対する考え方の改善など、総合的に対応していくことが求められます。

[44] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets

総合的な防御力

セキュリティ対策に求められるスキルと知識:
安全な環境を構築するためには、リスク管理と総合的な脅威インテリジェンスが必要になります。

予測や挙動による検知がファイルレス攻撃の対抗策

ブラックリストによる従来型の検出手法を回避するため、環境寄生型の攻撃は継続するでしょう[45]。そのため、企業は挙動検知、サンドボックス、トラフィック監視などを備えたセキュリティソリューションを検討する必要があります。環境寄生型の攻撃の場合、レジストリへの書き込みやシステムのメモリへの展開、さらには「PowerShell」や「Windows Management Instrumentation(WMI)」など、ホワイトリストに登録されたツールを悪用するため、特定の実行イベントや挙動といったファイルと異なる指標をもとにする検知が鍵となります。ファイルレス攻撃はバンキングトロジャン[46]、コインマイナー[47]、ランサムウェア[48]を展開する攻撃手法として、今後も利用されるでしょう。

LinuxではIoTデバイスをボットネット化してDDoS攻撃に悪用する脅威だけでなく[49]、企業のプラットフォームの一部において[50]、オープンソースのシステムが重要になるにつれて、Linux向けのマルウェアが増加するでしょう。さらに、企業のネットワークに深く侵入するために必要な情報を窃取する手段として、情報窃取型のマルウェアの亜種が増加してくると考えられます。さらなる攻撃に向けた準備を行いながら、ファイルレスを含むさまざまな手法で企業のシステムを執拗に攻撃してくる脅威が続くことが予測されます。

セキュリティ評価の重要な役割を担うMITRE ATT&CK

攻撃者の手法や戦術の分析をもとに作られたフレームワーク「MITRE ATT&CK」は、今後セキュリティの評価に関して業界レベルで総合的な枠組みを提供していくことになります。MITRE ATT&CKの公開ナレッジベースは、既知の攻撃にもとづいて、攻撃者の戦術や技術が総合的に分類・説明されている点で注目されています[51]。これからは多くの企業が、MITRE ATT&CKのフレームワークによって、脅威モデル、セキュリティ製品、組織リスクなどを評価することになるでしょう。このフレームワークは、脅威に関する攻撃手法やパターンを把握できるだけでなく、緩和策およびセキュリティ対策の有効性を測定する観点からも活用できます。さらにMITRE ATT&CKの公開ナレッジベースは、セキュリティマネージャーおよびサイバーセキュリティプロバイダの共通リソースとして機能し、攻撃手法および防御手段の情報共有における合理化が実現されるでしょう。

---

45 https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats
46 https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/
47 https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/
48 https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/
49 https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/
50 https://www.zdnet.com/article/microsoft-developer-reveals-linux-is-now-more-used-on-azure-than-windows-server/
51 https://attack.mitre.org/

総合的な対策のために高まる脅威インテリジェンスの必要性

2020年以降、企業を狙う攻撃はより綿密に計画され、広範囲への影響を意図し、多様な戦術が駆使されることが予測されます。こうした中、企業がプロアクティブに攻撃者の戦略を把握し、セキュリティ上の不備の特定や侵入のリスクとなるつながりの排除といった対策を講じていくためには、脅威インテリジェンスおよびセキュリティ分析が、これまで以上に重要となってくるでしょう。こういったセキュリティ対策およびリスク管理に取り入れられるべき総合的な脅威インテリジェンスは、攻撃発生前にリスクを軽減したい企業にとっては不可欠な要素となります。

優れた知見と防御策が用意されていれば、巧妙な脅威、執拗なマルウェア攻撃、フィッシング攻撃、潜在的なゼロデイ攻撃、その他のさまざまな攻撃を防ぐことができます。また、企業では環境を完全に可視化することで、脅威をリアルタイムで検出し、攻撃を阻止する効果的な防止策も可能になります。これは、エンドポイントを超えて、メール、サーバ、クラウドワークロード、ネットワークを含む総合的なセキュリティ対策を意味します。

企業は不足するサイバーセキュリティのスキルと不十分なセキュリティ環境が、2020年の脅威状況において重要な要素であることを認識するでしょう。企業の意思決定者やIT管理者は、自社の環境で何が起きているかを把握することが、これまで以上に強く求められています。こうした中、脅威インテリジェンスを用いた相関関係の分析や総合的な視点を得るため、Security Operation Center（SOC）の分析チームのようなセキュリティ専門家の役割が、これからはより一層重要になってくるでしょう。

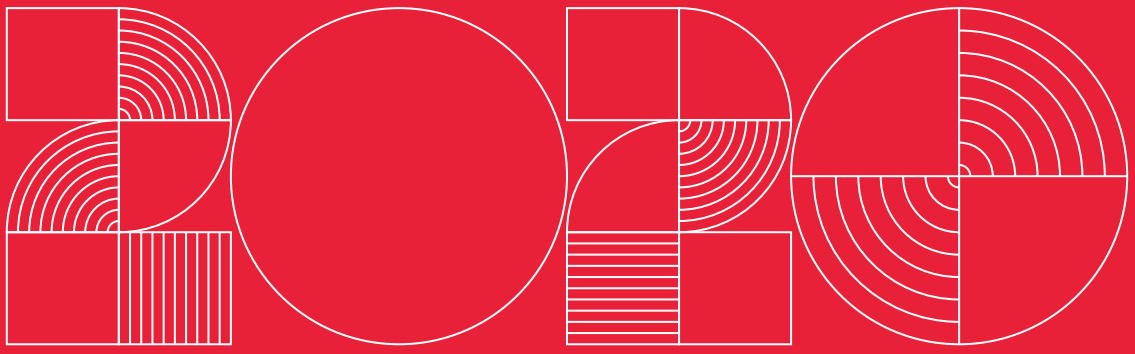
2020年のセキュリティ対策

企業のインフラにおける全領域でリスクを軽減するためには、セキュリティ専門家との協力体制が不可欠です。これにより、企業のセキュリティ部門および開発部門の双方において、接続デバイスの可視化や制御が可能になり、それらのデバイスに関する問題点にも対処できます。既知および未知の脅威をプロアクティブに特定する上でも、リアルタイム検出やゼロアワー検出も重要になります。

絶え間なく変化する脅威状況へ対処するには、以下のセキュリティ技術を活用したクロスジェネレーションによる多層防御、そして組織のネットワーク、エンドポイント、ハイブリッド型のクラウド環境を全方位で可視化するConnected Threat Defenseが必要です。

- 全方位の可視化:影響の緩和やリスク軽減のツール、専門知識を活用し、脅威の優先順位付けや最適化が施された評価を提供する
- 自動連携防御:視覚化され、特定された脅威を、マルウェア対策、機械学習とAI、アプリケーションコントロール、Webレピュテーション、スパム対策技術と連携して自動的に阻止する
- MDR(Managed Detection and Response):脅威の把握、総合的な分析、即時修復のため、脅威インテリジェンスを駆使しながらアラートと検知を相互に関連づけるセキュリティの専門性を提供する
- 挙動監視:巧妙化されたマルウェアや関連手法をプロアクティブにブロックし、関連する不審な挙動を検知する
- エンドポイントセキュリティ:サンドボックス、侵害検出、エンドポイントセンサーなどの機能により攻撃を阻止してデータを保護する
- 侵入検出と防止: コマンド&コントロール(C&C)通信やデータ流出などの不審なトラフィックを阻止する

TREND MICRO | research



TREND MICRO

〒151-0053

東京都渋谷区代々木2-1-1　新宿マインズタワー

大代表 TEL:03-5334-3600 FAX:03-5334-4008

https://www.trendmicro.com

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。