2021クラウドメール脅威レポート

Trend Micro Cloud App Security Threat Report

はじめに

本レポートでは弊社で提供する「Trend Micro Cloud App Security™」[1]サービスの全世界における統計データを元に、主に法人で利用されるクラウドメールサービス上で2020年に確認された注目すべきメール脅威動向についてまとめ、その有効な対策について考えます。

2020年1年間で1,670万件以上のハイリスクのメール脅威を確認するなど、「Trend Micro Cloud App Security™」サービスでは、ビジネスメール詐欺(BEC)[2]やクレデンシャルフィッシングなど、様々なメール経由の脅威を捉えています。

2020年には新型コロナウイルス(Covid-19)の世界的流行により、個人や企業の日常業務に大きな支障が生じました。外出自粛や海外への渡航制限の中でビジネスを維持するために、多くの組織にとってテレワークが不可欠なものとなると共に、クラウドコンピューティングは信頼できるプラットフォームになってきています[3]。

このようにクラウドコンピューティングがデジタルトランスフォーメーション(DX)の中心となる中、攻撃者もこの状況に注目しクラウドインフラストラクチャを攻撃対象としています。近年、サイバー犯罪者は、より巧妙かつ複雑な攻撃方法を駆使しているものとされています。しかし一方では、クラウド技術を利用する攻撃経路の中でも最もシンプルで信頼性が高く、最もわかりやすいEメールが依然として悪用されており、フィッシングメール、不正スパムメール、ソーシャルエンジニアリング攻撃など、試行錯誤の中で洗練されてきた攻撃手法も猛威を振っています。

1 https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/email-andcollaboration/cloud-app-security.html
「Trend Micro Cloud App Security™」サービスは Microsoft Exchange Online やGmail へ第二の防御層を提供するAPIベースのソリューションです。同時にOneDrive for Business、SharePoint Online、Teams、Google Drive、Box、Dropbox など、さまざまなクラウドベースのアプリケーションやサービスも保護します

2 https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

3 https://www.trendmicro.com/vinfo/us/security/news/security-technology/the-cloud-what-it-is-and-whatit-s-for

2020年のクラウドメール脅威の概況

下図が示すように、「Trend Micro Cloud App Security™」サービスでは2020年の1年間で1 ,670 万件以上のハイリスクなメール脅威を検知・ブロックし、前年比で32%の増加となりました。またマルウェア、フィッシング、クレデンシャルフィッシングの攻撃が2020年に急増した一方、BEC ではわずかな減少が確認されました。

テレワークの普及により、クラウドベースのメールサービスの利用が増えています。インターネットの利用者が増え、世界中で何百万人もの人々が在宅勤務をするようになり、仲間や顧客とのコミュニケーションにメールを使うことが必須となっています。

残念ながら、これらのメールの大部分は不正なもので占められているものと考えられます。

攻撃者は、世界的なパンデミックでもたらされた不確実性や恐怖にいち早くつけ込み、Covid-19関連の脅迫メールを送信して、金銭、個人識別情報（PII）、認証情報などを窃取しています。

クラウドベースのシステムやサービスには、脅威の検知やセキュリティの機能がすでに組み込まれていますが、何百万もの脅威がこれらのセキュリティフィルタを回避していたことを「Trend Micro Cloud App Security」サービスの検知結果は示しています。2020年に約1万人の Microsoft 365ユーザを抱えるある組織において、「Trend Micro Cloud App Security」サービスは Microsoft 365に実装されたセキュリティ機能によるスキャンを通過した75万5,000通以上のハイリスクメール脅威を検出しました。 これはもし「Trend Micro Cloud App Security」 サービスによる追加のスキャンが無ければ、1ユーザあたり75通が着弾したことを意味します。

この組織で検知・ブロックされた脅威のほとんどは不正な URL やフィッシングリンクでしたが、約1万件の不正プログラムファイルと 4 ,300件以上の BEC も含まれていました。この事例だけを見ても、個人ユーザ、企業、組織が、さまざまな種類の脅威を阻止するためには、セキュリティに対して多層的なアプローチが有効であることがわかります。

	顧客 A	顧客 B	顧客 C	顧客 D
	Microsoft 365 E3	Microsoft 365 E5	Microsoft 365 E3 サードパーティゲートウェイ	Gmail
	ユーザ数1万 12ヶ月間	ユーザ数8万 12ヶ月間	ユーザ数12万 12ヶ月間	ユーザ数1万 12ヶ月間
BEC	10,916	89,579	12,249	3,210
マルウェア	360,726	151,193	74,362	27,877
フィッシング	4,387	6,679	1,220	2,652
高リスクメール関連脅威	755,149	343,434	143,129	53,153

Cloud App Security を使用した顧客による2020年の検出数

18% BECを示唆する検出件数の減少率
（BECの攻撃者は、より大規模で洗練され標的を絞った攻撃に備えているのかもしれません）

37% 既知のクレデンシャルフィッシングリンクの増加率

14% 既知のマルウェア検出件数の増加率

17% 未知のマルウェア検出件数の増加率

Cloud App Security からのデータ

巧妙化が進み、増加を続けるクレデンシャルフィッシング攻撃

テレワークが広く普及する中、クラウドの認証情報を狙うクレデンシャルフィッシング攻撃が顕著化してきました。攻撃者が偽のログインページにより従業員のメールアカウントの認証情報を窃取するクレデンシャルフィッシング攻撃は、2020年、増加傾向を示しています。

クレデンシャルフィッシングとは、フィッシングの中でも特にユーザが使用しているサービスなどのアカウントID、パスワードといった認証情報の窃取を狙う攻撃を指します。

「Trend Micro Cloud App Security」サービスのデータによると、2020年、546万 5,969 件のクレデンシャルフィッシング攻撃が検出・ブロックされ、前年比 14%増となっています。また、中でも特に未知のリンクを含むクレデンシャルフィッシングは全体の34%となり、2019年よりも割合を減らしました。

残念ながら、クラウド型メールサービスに実装されたセキュリティフィルタの突破を試みる脅威は多数存在しています。こうした中、クラウド型メールサービスの1つである Microsoft 365は、常にクレデンシャルフィッシング攻撃の標的となっています。「Trend Micro Cloud App Security」サービスの利用者における 2020年の事例では、ある Microsoft 365ユーザ1万人規模の組織からは31万4 ,302件のクレデンシャルフィッシング攻撃、ある Microsoft 365ユーザ550人の組織からは2 ,585 件のクレデンシャルフィッシング攻撃を検知・ブロックしました。注目すべきは、どちらの組織においても、検知・ブロックしたフィッシング脅威の大部分がクレデンシャルフィッシング攻撃であったことです。

また、クレデンシャルフィッシング攻撃の数が増えただけでなく、攻撃手法の巧妙化も確認されました。例えば、サイバー犯罪者グループ SideWinder[4] は、不正な LNK ファイルを不正サーバに配信していました。この不正サーバは、ネパールやアフガニスタンの政府機関や軍を標的としたクレデンシャルフィッシングページのホスティングに使用されていました。

トレンドマイクロ社の調査によると、これらのフィッシングページは、被害者の Web メールのログインページからコピーされており、フィッシング攻撃がより効果的になる工夫が施されていました。

具体的なクレデンシャルフィッシングの攻撃キャンペーンの事例としては、2020年5月、攻撃者が企業の幹部社員を狙い、偽の Microsoft 365パスワードの有効期限レポートを含むメールを送信し、被害者を騙してユーザ名とパスワードを窃取する攻撃をトレンドマイクロでは確認していします[5]。トレンドマイクロ社の調査によると、このクレデンシャルフィッシング攻撃キャンペーンの被害者の中には、日本、米国、英国、カナダ、オーストラリア、ヨーロッパの製造業、不動産、金融、政府、技術系の企業が含まれていました。

4 https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issuesfor-spear-ph.html
5 https://blog.trendmicro.co.jp/archives/2718

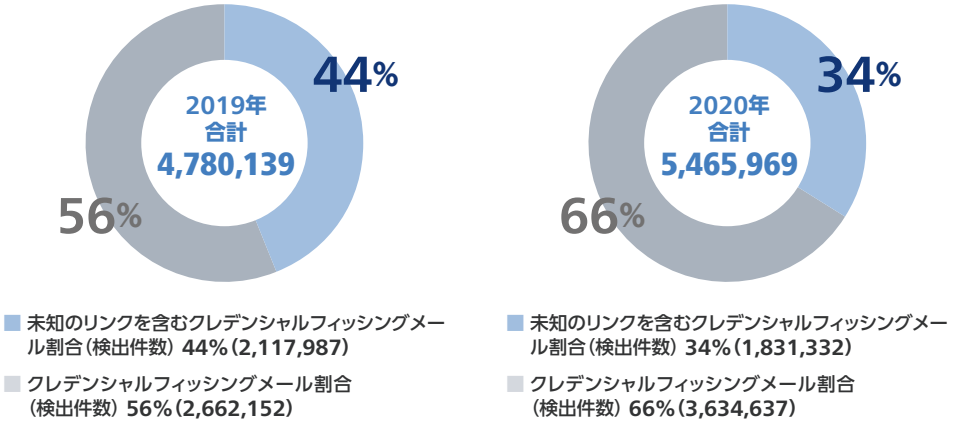


図2:クレデンシャルフィッシングの検出数とその内訳（全世界）

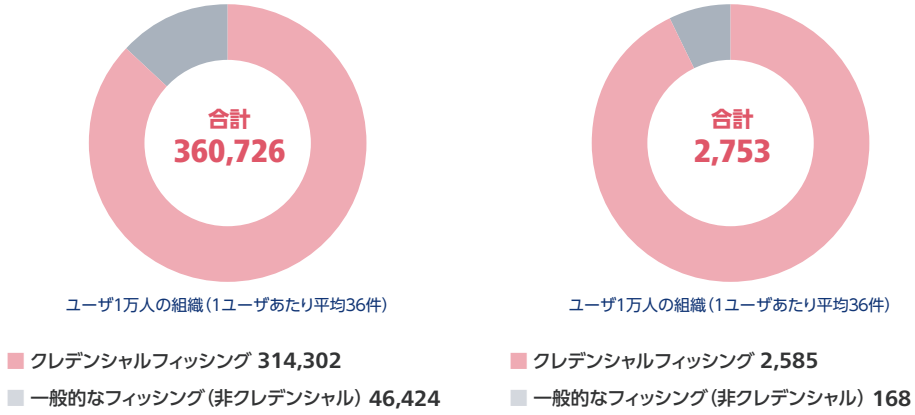


図3:2件の「Trend Micro Cloud App Security」サービス利用者事例におけるフィッシングメール件数とその内訳

ビジネスメール詐欺、件数減少の背後にさらなる標的型化の可能性

2020年、ビジネスメール詐欺（BEC）[6]の件数はわずかに減少しましたが、引き続き企業に多額の損失をもたらしています。

BECは取引先や企業内の取締役などに成りすまし、偽の送金指示によって金銭をだまし取るメール詐欺の手法です。「Trend Micro Cloud App Security」サービスは、2020年に31万7,574件に及ぶBEC攻撃をブロックしており、これは、前年よりも18%少ない件数となっています。ただし、件数が減少したからといって企業や組織が安心してもよいと言うことではありません。むしろ、BECの攻撃者はより狡猾となり、より限定的に標的を絞った巧妙な攻撃を行うように変化している可能性が懸念されるからです。

2020年、「Trend Micro Cloud App Security」サービスは、6,679件のBEC攻撃から約8万人規模のMicrosoft 365E5ユーザの組織を保護しました（1ユーザあたり平均12件の攻撃を阻止）。また、4,387件のBEC攻撃から約1万人規模のMicrosoft 365E3ユーザの組織を保護しました。

2020年、セキュリティ企業「IBM X-Force」は、IMG形式もしくはディスクイメージ形式のファイルが添付された偽請求書を使用するBEC攻撃キャンペーンを確認しました[7]。この場合、ユーザがIMGファイルをクリックすると、リモートアクセスツール（RAT）である「NetWire」がユーザの端末にダウンロードされます。また別の事例[8]では、BECにより、プエルトリコ政府が約2ヶ月間で合計420万ドル（約4億6,500万円相当）の被害を受けました。この攻撃では、政府の財務担当者のメールアカウントのハッキングにより実行されました。

このようにサイバー犯罪者がより大規模な標的を絞った攻撃の準備に傾倒していることも、件数減少につながっている可能性があります。

6 Business E-mail Compromise
7 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/netwire-rat-hiddenin-img-files-deployed-in-bec-campaign
8 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/puerto-rico-losesmillions-in-email-scam

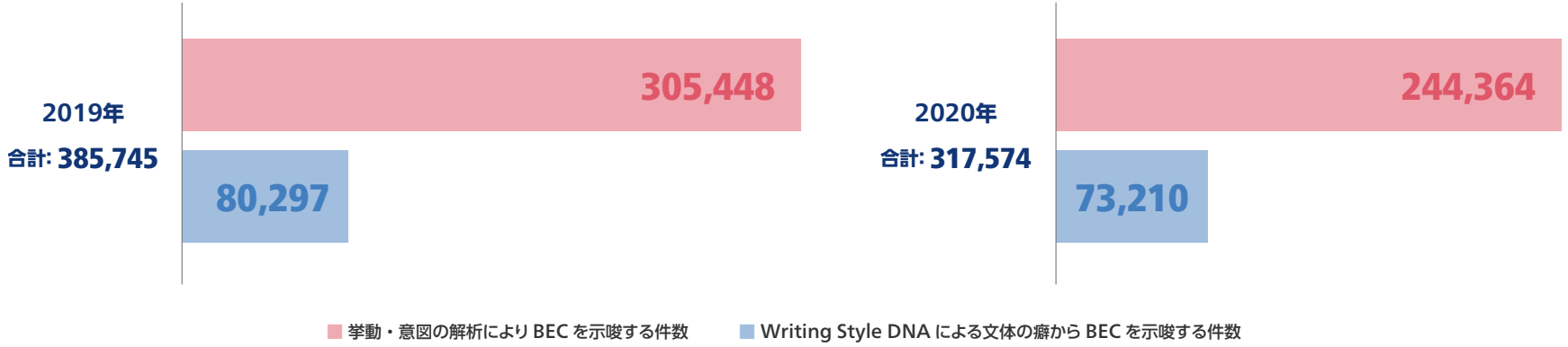


図4:BEC の検出数推移（全世界）

複雑化しながら増加するマルウェア攻撃

2020年、高リスクメールの関連脅威の確認に伴ってブロックされたマルウェアの検出数は16%増加しました。その数は、110万件以上のマルウェア検出数に達し、「Trend Micro Cloud App Security」サービスが検出・ブロックしたマルウェアは、着弾時点で検出対応済み（既知）のもので14%、検出未対応（未知）のもので17%増加していることが分かりました。

2020年初旬、マルウェアの攻撃者は、スパムメール攻撃キャンペーンにおいてマルウェア「Emotet」を利用する際、新型コロナウイルスの偽装通知メールを活用しました[9]。この場合、受信者にマルウェアをダウンロードさせるため、Covid−19の予防策のリストがあると称する偽の添付ファイルのダウンロードを促しました。

スパムメールを駆使するマルウェア活動の背後には、このように新型コロナウイルスの世界的な大流行を利用して被害者を騙すだけでなく、技術的な手法を継続的に開発している攻撃者もいます。

例えば、遠隔操作を実現するボットマルウェアである「Trickbot」[10]は、検出回避、スクリーンロック、リモートアプリケーションの認証取得などの機能が追加されていました。さらにまた、別のTrickbotによる攻撃キャンペーンでは、ファイルレス型バックドア「BazarBackdoor」[11]をスパムメールやソーシャルエンジニアリング技術を駆使して拡散していたケースも確認されています。

興味深いことに、2020年に検出・ブロックされたマルウェアの総数が前年を上回っているにもかかわらず、2020年にブロックされたランサムウェア[12]のファイル数は、2019年のそれと比較して大幅に減少しています。「Trend Micro Cloud App Security」サービスは、2020年、確認されたメール内で17万8,893件のランサムウェアの脅威を検出・ブロックしました。

こうした逆説的な傾向[13]は2017年以降から見られるようになっており、ランサムウェアのように明らかなマルウェアをメールに直接添付しようとするサイバー犯罪者は減少していることを示しているものと言えます。また、感染活動に成功した主要なランサムウェアファミリーの数自体は少ないものの、攻撃者は、これらの主要なランサムウェア活動だけで大きな報酬を得ています。最近のランサムウェア[14]は、可能な限り多くの潜在的な被害者にスパムメールでランサムウェアを送信するという「ばらまき型」ではなく、被害者のターゲットをより慎重かつ意図的に選定し、機密情報のために大金を支払う可能性の高い企業や組織に絞って感染させる「標的型」となっています[15]。また、被害者の企業や組織全体にランサムウェアを拡散する「内部活動」ためにフィッシングメールを攻撃経路に使用するなど、多段階の攻撃[16]も行っています。

こうした点からも、2020年に「Trend Micro Cloud App Security」サービスが企業や組織で検出・ブロックしたランサムウェア脅威数の傾向が把握できます。

9https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/emotet-usescoronavirus-scare-in-latest-campaign-targets-japan

10https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trickbot-spreadsas-dll-comes-with-upgrades-targeting-windows-10

11https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/group-behindtrickbot-spreads-fileless-bazarbackdoor

12 https://www.trendmicro.com/vinfo/us/security/definition/ransomware

13https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2017-annual-roundup-the-paradox-of-cyberthreats

14https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-onmanufacturing-networks.html

15https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-ofransomware-2020-s-catch-22

16https://www.trendmicro.com/en_us/research/19/h/heatstroke-campaign-uses-multistage-phishingattack-to-steal-paypal-and-credit-card-information.html

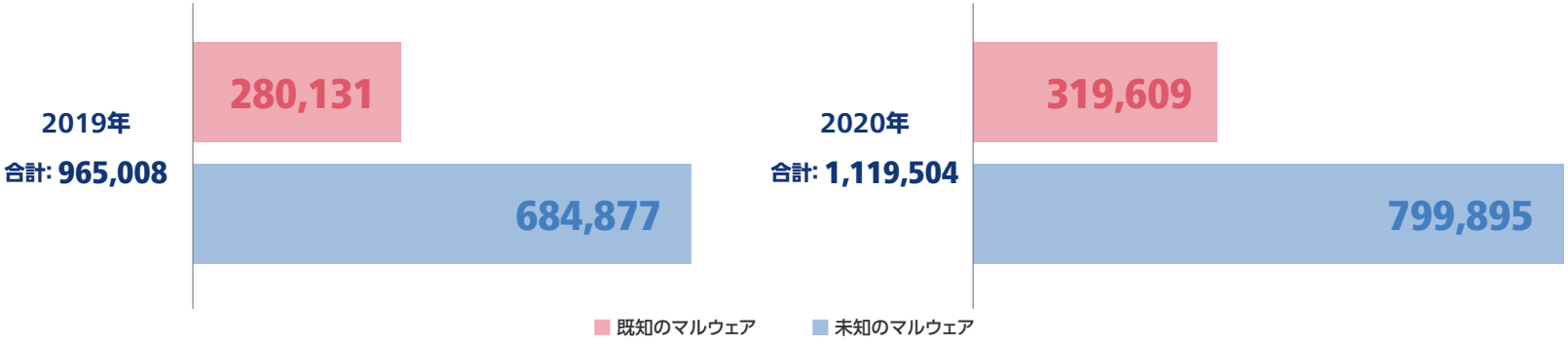


図5:メールと添付ファイルからのマルウェア検出数推移（全世界）

Covid-19 やテレワークに便乗したフィッシング攻撃

「Trend Micro Cloud App Security」サービスでは、2020年、692 万 4,324 件のフィッシング攻撃を傍受し、前年比 19%増となりました。特筆すべきは、一般的なフィッシング攻撃の数は前年比41%増と全体の増加率を上回っている点です。

コロナ禍において多くの人々が在宅勤務に従事する中、攻撃者は、そうした環境でのセキュリティや可視性の欠如に付け込んで、メールによるフィッシング攻撃を行っているようです。

さらにサイバー犯罪者は、こうしたパンデミックの中、オンラインショッピングへの依存度が高まっていることにも付け込み、個人や企業に対して悪質な攻撃キャンペーンを展開しています。

例えば、26か国が被害を受けた国際郵便局フィッシング攻撃キャンペーン[17]では、クレジットカード情報を盗むことを目的に、攻撃者がフィッシングメールを送信し、被害者をフィッシングサイトに誘導していました。

また2020年、フランスの小売企業の顧客からクレジットカード情報を窃取する事例では、攻撃者が独自のソーシャルエンジニアリング手法を用いて、被害者の自宅の住所と電話番号を含めた個人情報を入手する手口も確認されました。調査によると[18]、サイバー犯罪者は、約1,000ユーロ（執筆時点で1,200米ドル以上相当、13万3,000円相当）の偽のオンライン注文の詳細を記載したフィッシングメールを送信し、被害者に「Cancel my order（注文をキャンセルする）」ボタンを選択させようとしました。このボタンを選択すると、Darty 社のウェブサイトを模したフィッシングページが表示されます。

さらにトレンドマイクロ社では、Netflix の偽ページ[19]を利用して被害者にアカウント情報の更新を促すことで、個人認証情報（PII）やクレジットカードの情報を窃取するフィッシング攻撃も確認しました。この事例からは、コロナ禍で自宅での娯楽を求める人々のニーズにサイバー犯罪者が付け込んでいることが明らかになりました。実際、2020年の最初の3か月間で、1,600万人のユーザ 20 が、この偽ページのオンラインストリーミングサービスに登録しました。

17 https://www.trendmicro.com/en_us/research/21/a/post-office-phishing-hits-credit-card-users-in-26-countries.html

18 https://www.trendmicro.com/en_us/research/20/l/scammers-use-home-addresses-of-targets-infrance.html

19 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/phishing-site-usesnetflix-as-lure-employs-geolocation

20 https://www.bbc.com/news/business-52376022

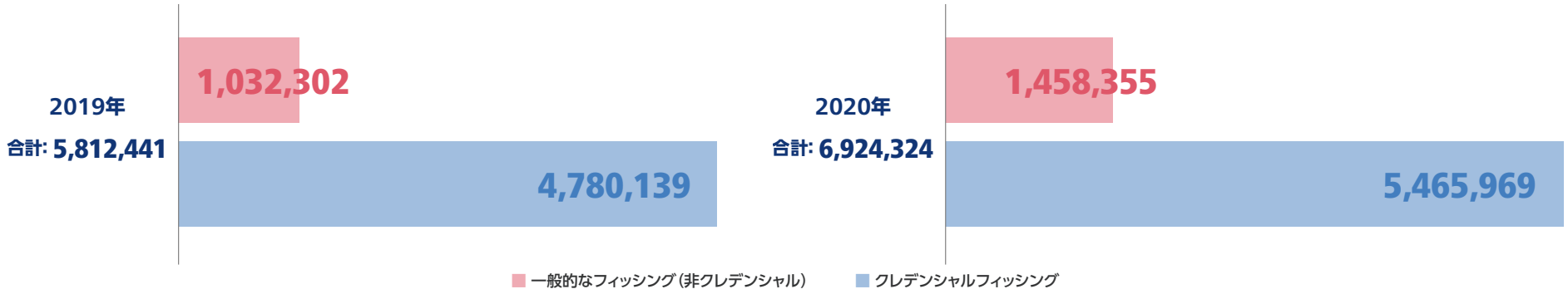


図6:フィッシングの検出数推移（全世界）

総論：2020年のクラウドメール脅威

世界的なパンデミックの危機の中でも、サイバー犯罪者は、メールを駆使した攻撃の手を緩めることはありません。むしろ、この状況を格好の機会として不正な利益を得ています。

2020年、Covid-19 関連のマルウェアがスパムメールにより何百万人もの人々に送信されました。実際、2020年最初の5か月間、Covid-19 を利用したサイバー脅威の92%は、スパムメールやフィッシングメールを利用したものでした[21]。「Trend Micro Cloud App Security」サービスでは、合計111万9 ,504件ものマルウェア関連脅威が阻止されました。

また、2020年の BEC 攻撃件数自体は減少したにもかかわらず、被害額の点では、攻撃者は BEC からより大きな報酬を得ています。2020年の第1四半期、不正な電信送金の平均被害額が8万183米ドル（約887万2,248円相当）に跳ね上がりました。

一方、クレデンシャルフィッシング攻撃は、前年比14%増の546万5,5969件となりました。

注目すべきは、クレデンシャルフィッシング攻撃の大半が既知のリンクへの誘導であること、つまり同じフィッシングサイトを使い回していることです。また2020年には、ヴィッシングや偽の Microsoft 365パスワードの有効期限報告などのユニークな手口を使用していることも確認されました。

パンデミック時[22]はもちろん、それ以降も、規模の大小にかかわらず、セキュリティはすべての企業にとって優先事項であるべきです。現在、多くの企業や組織は、テレワークで高い生産性を維持するため、クラウドベースのメールサービスやツールに大きく依存しています。

そうした中、企業や組織は、ネットワーク、デバイス、接続を安全に保つため、全社的なセキュリティトレーニングや、全従業員のためのチェックリスト[23]を用意することに加え、進化し続ける多様な脅威を抑えるため、多層的なアプローチを導入する必要があります。

21 https://www.trendmicro.com/en_us/research/20/i/are-employees-the-weakest-link-in-your-securitystrategy-train-t.html

22 https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securingthe-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report

23 https://www.trendmicro.com/vinfo/us/security/news/security-technology/cso-insights-liggettconsulting-s-mark-liggett-on-connectivity-and-visibility-in-securing-remote-work

有効な対策

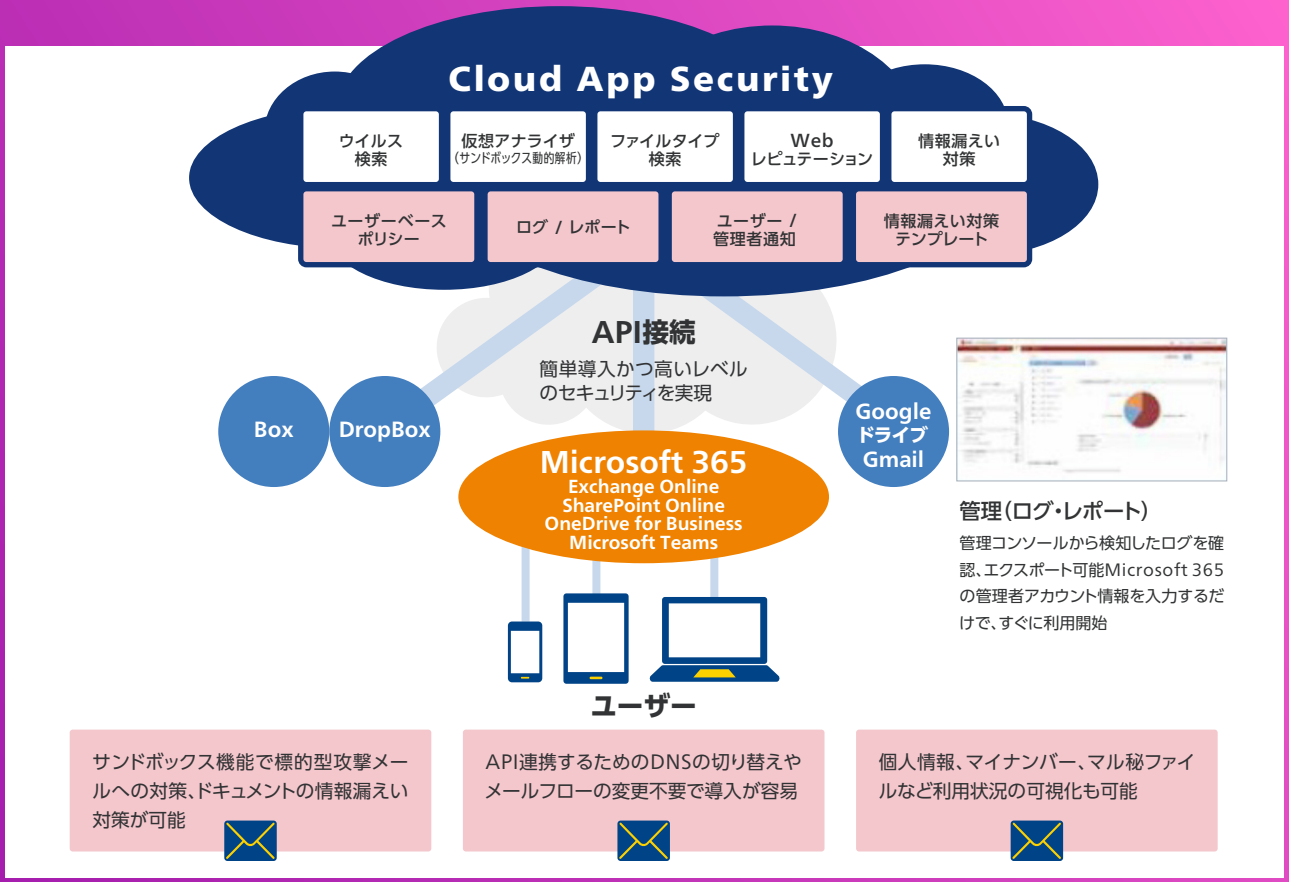
クラウドメール・コラボレーションツール向けサービス:「Trend Micro Cloud App Security」

企業や組織のクラウドメールやコラボレーションツールを守る包括的かつ多層的なセキュリティソリューションである「Trend Micro Cloud App Security」サービスは、Microsoft 365(旧 Office 365) や Google Workspace（旧 G Suite）などのメールやコラボレーションプラットフォームにあらかじめ備わっているセキュリティ機能を補完するものであり、機械学習を用いてメールのメッセージ本文や添付ファイルに含まれる不審なコンテンツを分析・検知します。

また、メールやファイルが Microsoft 365や Gmail 内蔵のセキュリティを通過した場合の第二の防御層としても機能します。

Microsoft 365や PDF ドキュメントに隠されたマルウェアに対しては、サンドボックス型マルウェア解析、ドキュメントエクスプロイト検知、ファイル・メール・Web レピュテーションテクノロジーなどの技術を用いて検知します。さらに Box、Dropbox、Google Drive、SharePoint Online、OneDrive for Business向けにデータ損失防止（DLP）や高度なマルウェア対策を提供するとともに、複数のクラウドベースのアプリケーションで一貫したDLP ポリシーを実現します。また、企業や組織における既存のクラウド設定とのシームレスな統合を実現し、ユーザと管理者の機能を完全に維持し、ベンダーの API を介して直接クラウド間の統合を可能にします。さらにまた、サンドボックスのマルウェア解析の前に脅威のリスクを評価することで、追加リソースの必要性を最小限に抑えます。

また、BEC やクレデンシャルフィッシングといったメールによる主要な脅威についても、機械学習を用いた対策機能を提供します。「Writing Style DNA」[24]は、機械学習（ML）を活用することで、過去のメールをもとにユーザの文体をチェックし、疑わしいメールを照らし合わせ、メールが正当なものかどうかを判断します。一方、「Computer vision」[25] は、画像解析と ML を組み合わせて、ブランディング要素やログインフォームなどのサイトコンテンツをチェックします。さらに、この情報をサイトレピュテーション要素や光学式文字認識（OCR）にプールし、偽サイトや悪意のあるサイトをチェックすることで、誤検知のケースを減らし、クレデンシャルフィッシングメールを検出します。



「Trend Micro Cloud App Security」サービスには、高度で拡張されたセキュリティ機能が搭載されており、エンドポイント、メール、サーバを対象とした調査・検知・対応を行うことができます。

24 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/curbing-the-becproblem-using-ai-and-machine-learning
25 https://blog.trendmicro.com/stop-office-365-credential-theft-with-an-artificial-eye

Cloud App Security

クラウドサービスを安心してご使用いただくために社外に置かれるメールやクラウド共有ストレージデータのセキュリティを補完！

◆Microsoft 365環境をはじめとするクラウドアプリのセキュリティをまとめてパワーアップ！

◆メール環境のセキュリティを強化したい！

◆ポータルおよびクラウドストレージのセキュリティを強化したい！

詳細はこちら

お申し込み・お問い合わせはこちら