法務・コンプライアンス・テクノロジー
責任者必読

そのメール、危険かもしれません

新型コロナウイルス感染症（COVID-19）
パンデミックに乗じて拡大しつつある
フィッシングメールの脅威に備えるために

EY
Building a better working world

新型コロナウイルス感染症（COVID-19）により、私たちの仕事や日常生活は一変しました。世界的な混乱を利用して抜け目なく動くサイバー犯罪者は、リモートワークへの移行や人々のウイルスに対する恐怖心に付け込み、フィッシング攻撃を急増させています。

本稿は特に以下の読者を想定しています。

弁護士
社内セキュリティ担当者
情報セキュリティ責任者
コンプライアンス責任者
リスクマネジメント責任者
内部監査室

新型コロナウイルス感染症パンデミックを悪用する詐欺師たち

以前から、サイバー犯罪の最も一般的かつ効果的な手口の1つとしてフィッシングメールが利用されてきました。これらの悪用によってデマの拡散、金銭の不正取得が行われるほか、標的の個人情報や機密情報が盗まれ続けています。社員がフィッシングの被害にあった場合は、社員貸与PCのみならず、組織のネットワーク全体から重要な社内データが流出する恐れがあります。

今、新型コロナウイルス感染症パンデミックに対する不安を利用して、新たな詐欺の手口を生み出すサイバー犯罪者が出てきています。詐欺師は、世界保健機関（WHO）、米国疾病予防管理センター（CDC）、その他政府当局などの公的機関を偽装してメールを送信します。

フィッシングメールは、ほぼ例外なく受信者にリンクのクリックまたは添付ファイルの開封を求めてきます。どちらの場合も、マルウェアに感染するか、あるいは機密情報を入力させるためのウェブサイトに誘導される可能性が高いです。

新型コロナウイルス感染症関連の詐欺以外で代表的な詐欺：

- **会計関連：**経理部、財務部や上長から来る請求書払い、仕訳、その他の財務取引の承認依頼
- **ソーシャルメディアにおけるなりすまし：**友達申請や新規投稿などを知らせる、「こちらをご覧ください」というリンク付きのソーシャルメディアからの通知
- **宅配通知：**受取人に対し、配達の確認や荷物の追跡のためにリンクをクリックするよう求める通知
- **オンラインショッピングサイトのなりすまし：**オンラインショッピング用のアカウント（Amazon、Apple等）に不正アクセスがあったとし、確認のためにリンクをクリックするよう求める通知
- **パスワードのリセット：**不正アクセスによりロックされたオンラインのソーシャルメディアアカウント（Facebook、Instagram等）に再度アクセスできるようにするため、リンクをクリックするよう求める通知

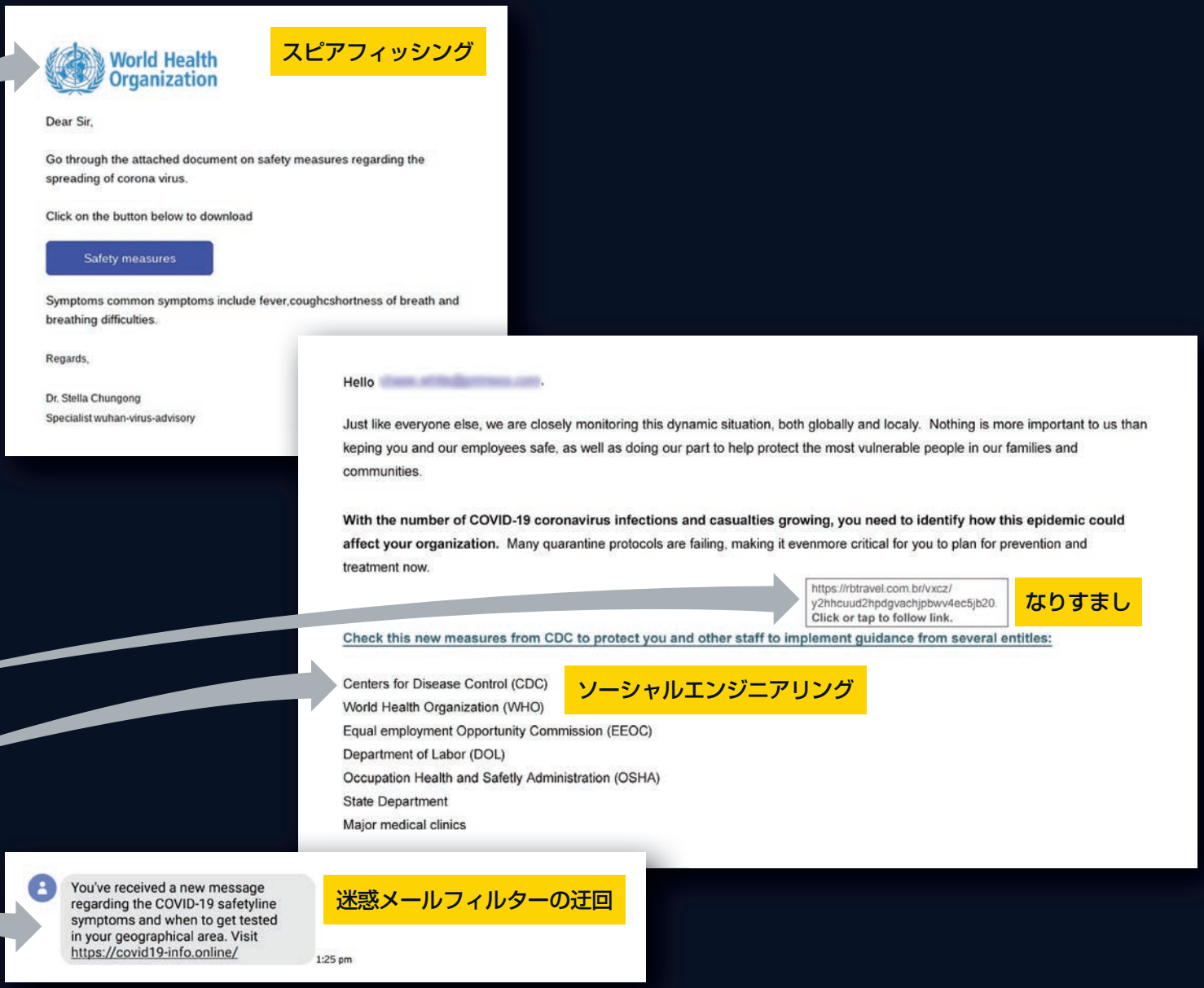
フィッシング攻撃の一般的な形態

ほとんどのフィッシング攻撃がそうであるように、犯人は信頼できる組織から発信された情報に見せかけて、標的にリンクをクリックするよう仕向ける手口を多用します。リンクは公式サイトのURLに偽装しており、クリックすると悪意あるサイトに誘導して被害者のPCにマルウェアを感染させ、PC内のデータを抜き取ります。

また、危機的状況のなか情報を求める人々を標的にして、重要な健康情報を掲載していると偽り、添付ファイルを送信するフィッシング攻撃もあります。被害者がこの添付ファイルをクリックすると、仕込まれていた不正なコードによって気付かないうちに第三者にPCを乗っ取られ、遠隔操作されてしまうことになるのです。

フィッシング攻撃にはさまざまな手口があります。そのなかでも最もよく使われる手口をご紹介します。

- **スピアフィッシング**：信頼できる送信者を装い、標的の機密情報を要求するメールや、パスワードを不正に収集するサイトまたはマルウェアを仕込んだサイトに誘導するリンクを含むメールを送信する詐欺
- **なりすまし**：実在の社員に似せた氏名、本物のEメールアドレスに類似したアドレス、公式サイトとそっくりなレイアウト、悪意あるサイトのドメインを含むまたはそのドメインに差し替えたURLを用いる詐欺
- **ソーシャルエンジニアリング**：LinkedInほかの公開された情報から企業内での上下関係を探り出し、その知識を悪用する巧妙ななりすまし詐欺
- **迷惑メールフィルターの迂回**：フォントサイズを0 ptにした文字の使用などにより設定されたスパムフィルターをすり抜ける、より高度ななりすましに分類される手口


スピアフィッシング
World Health Organization
Dear Sir,
Go through the attached document on safety measures regarding the spreading of corona virus.
Click on the button below to download
Safety measures
Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.
Regards,
Dr. Stella Chungong
Specialist wuhan-virus-advisory
Hello
Just like everyone else, we are closely monitoring this dynamic situation, both globally and localy. Nothing is more important to us than keping you and our employees safe, as well as doing our part to help protect the most vulnerable people in our families and communities.
With the number of COVID-19 coronavirus infections and casualties growing, you need to identify how this epidemic could affect your organization. Many quarantine protocols are failing, making it evenmore critical for you to plan for prevention and treatment now.
https://rbtravel.com.br/vxcz/y2hhcuud2hpdgvachjpbwv4ec5jb20.
Click or tap to follow link.
なりすまし
Check this new measures from CDC to protect you and other staff to implement guidance from several entitles:
Centers for Disease Control (CDC)
World Health Organization (WHO)
Equal employment Opportunity Commission (EEOC)
Department of Labor (DOL)
Occupation Health and Safetly Administration (OSHA)
State Department
Major medical clinics
ソーシャルエンジニアリング
You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/
1:25 pm
迷惑メールフィルターの迂回

リモートワークへの移行により フィッシング攻撃のリスクが上昇

フィッシングは特別目新しい脅威ではありませんが、新型コロナウイルス感染症パンデミックにより攻撃が増加しているという報告がセキュリティの専門家から出されています。ソーシャルディスタンスを実践し、リモートワークを継続することで、フィッシング被害に遭うリスクが上昇しているのです。対面でのやり取りがオンラインやリモートに移行したことから、社員が会社から貸与されたPCを業務以外の目的で使用する機会が増えるかもしれません。社員が貸与PCで私的なメールアカウントを使用した結果、ウイルス感染したサイトにアクセスしてしまい、機密情報が盗まれる可能性があります。

企業は、同僚や上司を騙るフィッシングメールの脅威に長らく晒されてきました。同僚からの送信に見せかけて、「送金」や「財務データの共有」、あるいは「製品の機密情報へのアクセス許可」を依頼するメールを社員が受け取るかもしれません。以前なら隣の席の同僚に声を掛けて確認することができましたが、そういった選択肢がないのであれば、機械的にリンクをクリックしてしまう人もいるでしょう。対面で直接やり取りができない場合、社員が詐欺行為の被害に遭うリスクは飛躍的に上昇するのです。

> DustyFreshというハンドルネームのセキュリティ研究者が、先週いくつかのドメインの追跡を開始しました。
>
> この研究者がオンラインで共有したリストによると、詐欺師らは3月14日から18日の間に新型コロナウイルスを含む新規ドメインを3,600以上作成していました[1]

[1] 出典: https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/

詳細については、EY Japan Forensic & Integrity Services Technologyチームにお問い合わせください。

E-mail : **forensics.cyber@jp.ey.com**
Tel : **03 3503 3292**

慎重な対応でフィッシング攻撃を防ぐ

- 会社のアドレス宛てに届いた不審なメールに対し、社内のセキュリティ対策を有効活用してください。例えば、多くの企業ではすぐに確認できないメールにフラグを付けるツールが利用されています。
- 社内のサイバーセキュリティガイドラインを見直し、必要に応じて研修を実施してください。
- インスタントメッセージや共同作業用フォルダーなど、メールの代わりになる社内専用ツールがある場合は、そちらを利用してください。このようなツールをうまく使いこなせていないのであれば、今こそ活用法を習得する時です。
- 送信者のメールアドレスのドメイン名が正しいものかどうか確認してください。例えば、**real.employee@acme.com**が**realemployee@acmee.com**になっていたら偽物です。
- 宛先が特定されていない汎用的なメールに注意してください。
- 文法間違いやスペルミスだらけのメールの場合、その信頼性に疑問を持つようにしてください。
- ほとんどのメールソフト（Microsoft Outlook等）は、不審なメールを受信したら警告を発します。メールソフトからの警告を無視しないようにしてください。
- 不審なメールの差出人と思われる同僚への連絡には、インスタントメッセージや電話を使用してください。
- 請求書や銀行取引明細書などのファイルをダウンロードするよう指示された場合は、注意してください。
- 貼られているURLが正規サイトのアドレスと同じかどうか確認し、確信が持てるまでは絶対にリンクを開かないようにしてください。
- 確認しないまま通常のワークフローから外れた対応（支払処理のための送金等）を取ることは、絶対に避けてください。
- 個人情報を要求するメールには返信しないでください。公的機関が機密情報の提出を依頼する際は、データを暗号化する安全なリンクを送ってくるはずです。
- 確認せずに添付ファイルを開くことがないようにしてください。まずは、電話や安全な社内のコミュニケーションツールを使って送信者に文書の真正性を確かめてみましょう。

EY | Assurance | Tax | Transactions | Advisory

EYについて

EYは、アシュアランス、税務、トランザクションおよびアドバイザリーなどの分野における世界的なリーダーです。私たちの深い洞察と高品質なサービスは、世界中の資本市場や経済活動に信頼をもたらします。私たちはさまざまなステークホルダーの期待に応えるチームを率いるリーダーを生み出していきます。そうすることで、構成員、クライアント、そして地域社会のために、より良い社会の構築に貢献します。

EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。EYによる個人情報の取得・利用の方法や、データ保護に関する法令により個人情報の主体が有する権利については、ey.com/privacyをご確認ください。EYについて詳しくは、ey.comをご覧ください。

EY Japanについて

EY Japanは、EYの日本におけるメンバーファームの総称です。EY新日本有限責任監査法人、EY税理士法人、EYトランザクション・アドバイザリー・サービス株式会社、EYアドバイザリー・アンド・コンサルティング株式会社などから構成されています。なお、各メンバーファームは法的に独立した法人です。詳しくはwww.eyjapan.jp をご覧ください。

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務およびその他の専門的なアドバイスを行うものではありません。EY Japan株式会社および他のEYメンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家にご相談ください。

本書は*That email may be infected too*を翻訳したものです。英語版と本書の内容が異なる場合は、英語版が優先するものとします。

eyjapan.jp

Contacts:

Global
Todd Marlin
todd.marlin@ey.com

Americas（北・中・南米）
Shawn Fohs
shawn.fohs@ey.com

Manish Khera
manish.khera@ca.ey.com

Asia Pacific（アジア・パシフィック）
Chi Chen
chi.chen@cn.ey.com

Jack Jia
jack.jia@hk.ey.com

Nick Robinson
nick.robinson@hk.ey.com

杉山 一郎
ichiro.sugiyama@jp.ey.com

Matthew Westwood-Hill
matthew.westwood-hill@au.ey.com

EMEIA（欧州、中東、インド、アフリカ）
Lorenz Kuhlee
lorenz.kuhlee@de.ey.com

Bodo Meseke
bodo.meseke@de.ey.com

Brenton Steenkamp
brenton.steenkamp@nl.ey.com