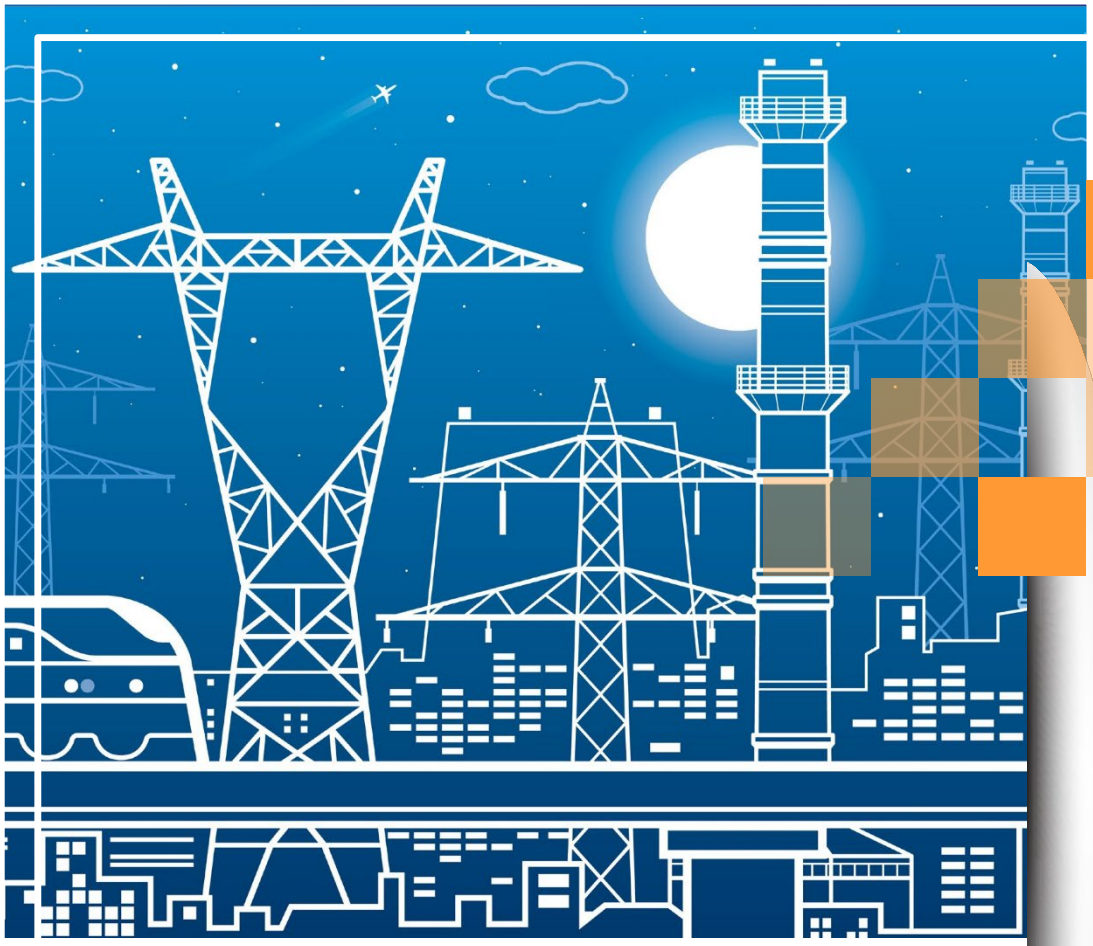
KnowBe4

# Cyber Attacks On Infrastructure
# インフラへのサイバー攻撃
## The New Geopolitical Weapon
## 新たな地政学的武器



# インフラへのサイバー攻撃

## 新たな地政学的武器

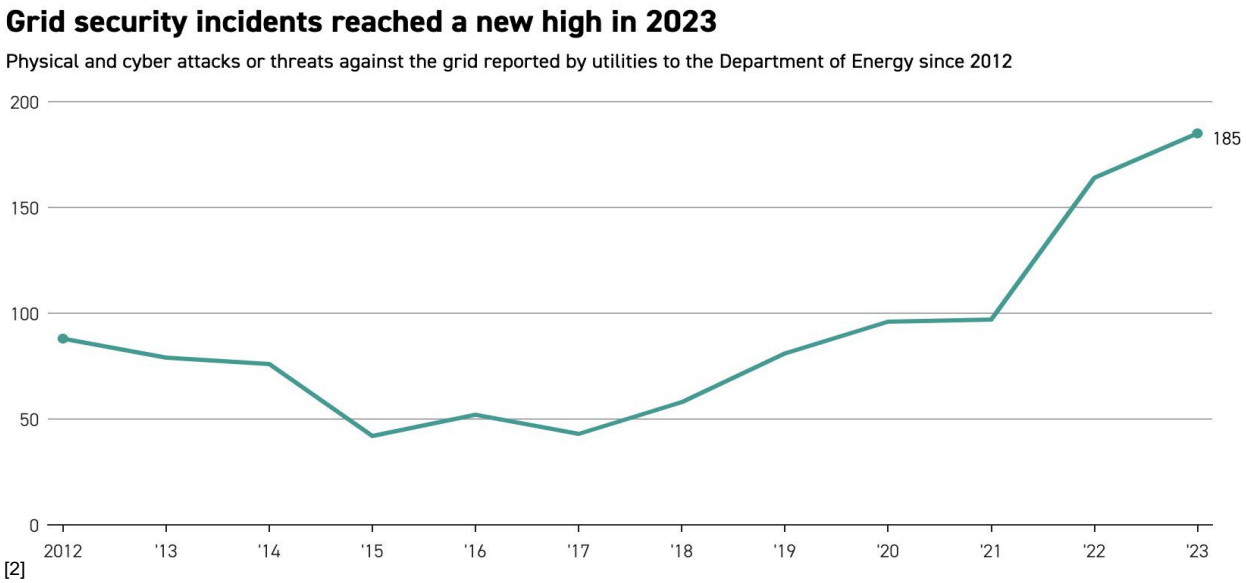
重要インフラとは、社会の機能を維持するためのシステムや物理的資産のことで、電力網、通信システム、物流網、港湾システムなどの広大な社会基盤システムが含まれます。どれか1つのセクターがダウンすれば、社会全体が麻痺してしまうことになります。例えば、交通網を結ぶ通信システムが崩壊すれば、航空管制官が突然、飛行機と連絡が取れなくなります。物流網を構成する港湾や航路が凍結して、通行できなくなれ、食料品やその他の物資の供給が滞り、経済が大混乱に陥ります。また、電力需要の急激な増加により送電網がダウンすれば、何百万もの家庭が暗闇に陥り、通信が遮断され、銀行口座にアクセスできなくなり、病院が閉鎖されるかもしれません。このようなシナリオは、事実上、広範囲に及ぶ社会不安を引き起こす要因となります。

大規模なシステムのシャットダウンは、医療や救急サービス、政府機関などの重要なサービスを世界規模で混乱させる可能性があります。多数の病院がデータへのアクセスに問題を抱え、予約や手術が遅れることもあります。サイバー犯罪者は、この重要インフラの持つ潜在的なリスクを巧みに利用しようとします。先進国のインフラ基盤は、デジタル技術との相互接続が進むにつれて、その能力と機能性が大幅に向上していますが、しかしこれは、反面、サイバー攻撃への新たな脆弱性を生み出し、エネルギー、輸送、通信はサイバー攻撃者にとっての新たな主要な標的となっています。地政学的対立が進む中、地政学上の敵対勢力は、これらの標的のいずれかが攻撃された場合の深刻な結果を熟知しています。この上で、この脆弱性を利用する態勢を整え、重要インフラへのサイバー攻撃をデジタル兵器の１つとして新たに加えようとしています。

最も恐ろしい出来事のひとつは、発電、水処理、電力生産、その他の相互接続されたプラットフォームを含むエネルギー基盤への攻撃でしょう。この攻撃は、地域社会を大混乱に陥れる可能性があります。突然電力が停止すれば、病院や救急隊、軍事基地の運営に大きな支障をきたす可能性があります。これは、私たちが考えているほど突飛なシナリオではありません。

2023年11月、パリに本部を置く国際エネルギー機関（IEA）の報告書によると、世界全体で2020年から2022年にかけて、電気・ガス・水道などの公益事業者に対するサイバー攻撃が毎週平均2倍以上に増加し、2023年にはさらに倍増しています。2024年4月4日、北米電力信頼度協議会(NERC: North American Electric Reliability Corporation)は、米国の送電網（Power Grids）でサイバー攻撃を受けやすい脆弱ポイントの数が1日あたり約60箇所の割合で増加していると報告しています。2022年には、影響を受けやすい脆弱ポイントの数は21,000から22,000に増加しました。現在は23,000から24,000に達しています。[1]

1 Kierney, Laila, "US electric grid growing more vulnerable to cyberattacks, regulator says," Reuters, April 4, 2024, https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04.



[2]

ロシアのウクライナ侵攻以来、ヨーロッパの電力網は何千回もの攻撃を受け、「サイバー攻撃の大洪水」の状態にさらされています。ヨーロッパ最大の電力会社のひとつであるE.ONの最高経営責任者レナード・ビルンバウム氏は昨年11月、「詐欺師たちの手口は日に日に巧妙になっている」と述べ、「私は今不安であり、将来はさらに不安になるだろう」と付け加えました。[3]

昨年5月、デンマークのエネルギーインフラが組織的な攻撃によって侵害され、攻撃者は一部の企業の産業用制御システムにアクセスしました。「攻撃者は、誰を標的にするかを事前に知っており、毎回的中させた」と述べています。

ポーランドのエネルギー省副大臣イレネウシュ・ジスカ氏は、昨年11月、米国のニュースメディアであるポリティコの取材に応じ、核攻撃から守るために地下3階に埋められたポーランドの送電網運用拠点を最近訪れたときのことを回想して、次のように述べています。「私は...エネルギー網に対する何千もの攻撃を生中継で見ていました。これらの攻撃は、ロシア連邦のほか、独裁政権や封建制などの非民主主義国家から行われ

2 Morehouse, Catherine, "Tensions at home and abroad poses growing threat to US grid," E&E News, April 8, 2024 https://www.eenews.net/articles/tensions-at-home-and-abroad-pose-growing-threat-to-us-grid/

3 Jack, Victor, "Europe's grid is under cyberattack deluge, industry warns," Politico, November 23, 2023 https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/

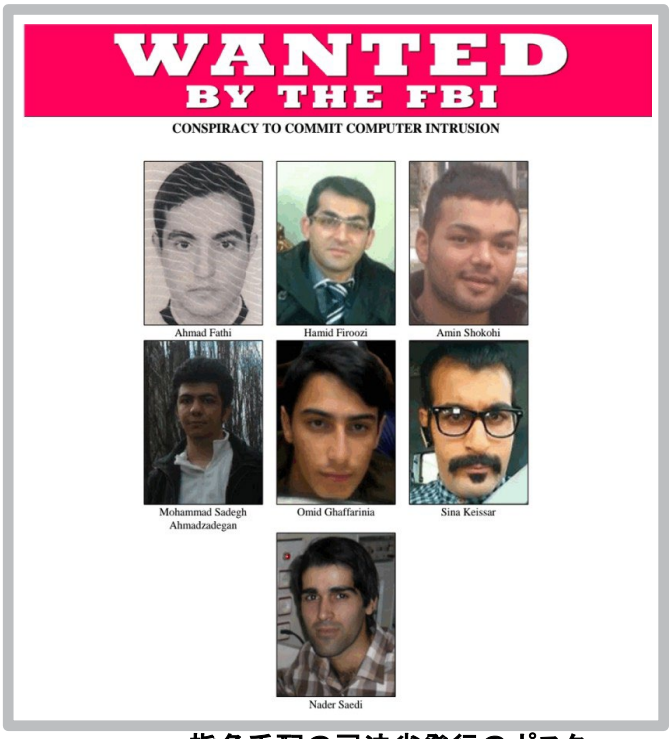
ていることは明らかです。EUの民主主義国家をサイバー攻撃し、大混乱を引き起こそうとする特殊工作チームが結成されたのです。」また、2023年9月、カナダのニュースサイトであるThe Recordは、不特定多数のアジア諸国の国家電力網が攻撃され、ここでは中国の国家安全保障省と人民解放軍につながるハッキング・グループAPT41が使用するShadowPadマルウェアの兆候が見られたと報じました。[4] この侵入は6カ月間発見されず、その間にハッカーはストレージデバイスへのアクセスを拡大し、システムの認証情報を収集し、痕跡を隠蔽しました。

また、米国のサイバーセキュリティ会社であるRecorded Futureの調査によると、中国とインドがラダックとチベットの東部付近で国境紛争に関与していたため、インドの電力基盤の大部分が標的とされたことを突き止めいます。ShadowPadは2020年の1年間も使用されており、電力需給を調整するインドの地域負荷分散センター4カ所を含む、10の異なる電力セクターが侵入されました。さらに、攻撃者は高圧送電変電所、石炭火力発電所、2つの港湾も狙ったとみられています。この調査によると、少なくとも 5 つの中国国家支援グループがスパイ目的で ShadowPad を使用していることが指摘されています。[5]

## 急増するターゲット

重要インフラに対するサイバー攻撃は、情報を求めているのではなく、混乱させる目的で制御システムへのアクセスを求めることがほとんどです。海外テロであれ、国内テロであれ、あるいはスパイ目的の機密へのアクセスであれ、このような攻撃は世界的に増加していますが、決して新しいものではありません。

2013年、イランのハッカーがニューヨーク州ライブルックにあるボウマン通りダムのコマンド・コントロール・センターに侵入し、水門の制御権を手中におさめています。 2016年、米司法省は、これが計画のほんの一部であったことを示す起訴状を公開しました。2011年から2013年にかけて、イランのイスラム革命防衛隊に所属する7人のイラン人が46の米国企業や公的機関にサイバー攻撃を仕掛けていたのです。起訴状によると、ボウマンアヴェニュー・ダムに侵入したハッカーのハミド・フィロオジは、ダムをインターネットに接続するセルラー・モデムを介して、同ダムの監視制御・取得データ（SCADA）システムへにアクセスに成功しています。




**指名手配の司法省発行のポスター (FBI.gov)**

4 Greig, Jonathan, "Power grid of Asian nation shows signs of intrusion by espionage group," The Record.media, September 12.2023, https://therecord.media/power-grid-asian-nation-cyber-espionage-redfly-shadowpad

5 Janofsky, Adam, "China-linked Hackers Target India's Power Grid Amid Border Clashes," The Record, February 28, 2024 https://therecord.media/china-linked-hackers-target-indias-power-grid-amid-border-clashes

フィロオジは、"水位や水温に関する情報、水位や流量を制御する役割を担う水門の状態など、ダムの状態や操作 "に関する情報にリモートアクセスしました。マンハッタン連邦検事のプリート・バハラ氏は、以下のコメントを発表しています。
「当時、ダムへの侵入は、サイバー犯罪の恐ろしい新境地を象徴していました。私たちは今、インフラや生活インフラに対する壊滅的な攻撃が、マウスのクリックひとつで世界中のどこからでも可能な世界に生きているのです」。

2017年、産業インフラに対する最も危険な可能性のあるサイバー攻撃の1つである「Tritonマルウェア攻撃」によって、ロシアのハッカーがプラントの安全システムを乗っ取り、遠隔操作することに成功しました。このサイバー攻撃は、サウジアラビアの石油化学施設の大破壊を引き起こしそうになりましたが、寸前に防止することができました。現場に呼ばれたオーストラリアのセキュリティ・コンサルタントは、彼が発見したものは「血の気が引くようなものだった 」とその脅威を語っています。

ハッカーは2014年以来、企業のITネットワークから工場内のネットワークに移動し、おそらく従業員のログイン認証情報を傍受して、エンジニアリング・ワークステーションに侵入し、基幹ネットワークに侵入していたようです。幸運なことに、マルウェアのコードに欠陥があったため、ハッカーは計画を実行する前に退却を余儀なくくされましが。その攻撃とは、プラントの安全チェックに過剰な負荷をかけ、有毒な硫化水素ガスを放出させるか、大規模な爆発を引き起こすことだったようです。

**MITテクノロジー・レビュー**によると、サイバーセキュリティの世界で、人命を危険にさらすために意図的に設計されたコードを見たのはこれが初めてだったとのことです。[6]

その後に、この攻撃はロシア連邦の研究所による国家支援であったことが判明しました。この攻撃が設定ミスによるものなのか、スピアフィッシングによるものなのか、諸説あります。

2020年、Covid-19の最盛期で熱波のさなか、ハッカーは2つの地方にあるイスラエル水道局の5つの施設の産業制御システム（ICS）を乗っ取ろうとし、ポンプ場、廃水プラント、農業用ポンプのシステムを侵害しようとしました。この攻撃は被害が出る前に発見されました。もし成功していたら、この地域の重要な時期の水の供給に大きな支障をきたし、病院はパニック状態に陥ったに加えて、農作物は壊滅的な打撃を受けていたでしょう。この攻撃の犯人は、特定されていません。

2021年、米国最大のパイプラインであるコロニアルオイル・パイプラインが大規模な標的型ランサムウェア攻撃を受けました。このパイプラインは、アメリカ東海岸のガス、ディーゼル、ジェット燃料の45％以上を供給しています。500万ドルの身代金を支払った後、パイプラインは停止を余儀なくされ、11日間オフラインになりました。11,000ヵ所のガソリンスタンドへガソリン供給が止まり、4つの州で非常事態宣言が発令され、燃料価格が過去6年間で最も高騰しました。この攻撃は、ロシアのハッカー集団DarkSideによって行われました。

---

6 Giles, Martin, "Triton is world's most murderous malware, and it's spreading," MIT Technology Review, March 5, 2019, https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

これらは、重要インフラに対する攻撃として話題となったものですが、その全貌を明らかにするものではありません。重要インフラへの攻撃の数は、年々加速的に増加しています。Forescout ResearchのVedere Labsによると、2023年1月から2024年1月にかけて、世界の重要インフラは4億2,000万回以上、さまざまな規模の攻撃を受けたことを明らかにしています。

総論として、重要インフラへの攻撃は163カ国に影響を与えました。主な標的は米国で、英国、ドイツ、インド、日本がこれに続いています。重要インフラをターゲットとする脅威者が最も集中しているのは中国で、次いでロシア、イランとなっています。[7]

## サイバー戦争

重要インフラの脆弱性を脅かす工作は、国家主導であるか否かにかかわらず、ロシアやイランのハッカー集団を巧みに偽装させ、あたかも子供の遊びのように見せてしまう脅威があります。

2023年5月、米国が中国によって打ち上げられたスパイ気球を撃墜した頃、検査官は米国の港に影響を与えた侵入活動を調査中にあるものを発見しました。グアムには広大な軍事基地があり、中国が台湾に侵攻した場合、アメリカが対応する中心的な拠点となります。このコードは、中国の政府ハッキング・グループによってインストールされたものでした。

7 2023 Global Threat Roundup Forescout-Vendere Research, January 24, 2024, https://www.forescout.com/resources/research-report_2023-threat- roundup


**米空軍B-52Hストラトフォートレス爆撃機**

**ニューヨーク・タイムズ紙**によると、この作戦は、侵入の追跡を困難にするため、時には家庭用ルーターやその他の一般的なインターネット接続された消費者向け機器を経由して流れるなど、非常にこっそりと実行されたとようです。ウェブ・シェル（サーバーにリモートアクセスできる悪意のあるスクリプト）を使用するなど、アメリカの国家安全保障局は、オーストラリア、イギリス、ニュージーランド、カナダの国家安全保障局とともに、この発見について24ページに及ぶ勧告を発表しています。アメリカ政府関係者は、今回の侵入は「サイバースペース、宇宙空間、そして今回の気球事件でアメリカ人が発見したように、大気圏下にも及ぶ中国の膨大な情報収集活動」の一環であると指摘しています。[8]

戦略国際問題研究所（CSIS）の所長兼プリツガーチェアのジェームズ・A・ルイスは、潜在的な敵対国の重要インフラを特定するために、我々は驚くような行動をとるべきではないと述べています。攻撃者の標的を特定し、サイバー攻撃の可能性に備えることは、「能力のある国なら誰でも行うような偵察 」です。

グアム攻撃で異例なのは、攻撃がグアムのインフラを狙ったものではなかったことだとルイスは言います。グアムでもアメリカでも、主な標的は台湾上空での交戦において米軍を支援するものでした。中国がこのような侵入を攻撃的な手段で行ったという証拠はありません。しかし、台湾をめぐる紛争が拡大していることを考えると、米国の民間インフラに対するサイバー行動は軍事作戦に必要な通信や物資の流れを混乱させるのに役立つと中国は判断していると思われるとルイス氏は述べています。[9]

そのような判断がなされた場合、中国が最初の標的とするのはおそらく電力施設でしょう。2番目は米国本土のパイプラインと鉄道で、3番目は、軍需品や軍用機を製造するサプライチェーンを支える物流・通信ネットワークと思われます。その他の主な標的は、カリフォルニア州、ハワイ州、ワシントン州など、海軍基地や空軍基地がある都市や地域の通信システムが想定されます。もちろん、その代償として、米国との全面的な軍事交戦のリスクが生じます。そう考えると、中国は大規模なサイバー攻撃は行わず、スパイ活動のためにサイバー活動を留保することも考えられます。

---

8 Sanger, David E., "Chinese Malware Hits Systems on Guam.Is Taiwan the Real Target?" New York Times, May 24, 2023, https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html

9 Lewis, James A, "Cyberattack on Civilian Critical Infrastructure in Taiwan Scenario," Center for Strategic and International Studies, August, 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-08/230811_Lewis_Cyberattack_Taiwan.pdf.

# 私たちの役割

グローバルな敵対勢力による重要インフラへのサイバー攻撃は、21世紀における紛争の進化とその性質の変化を明確に示しています。第二次世界大戦で空爆や軍事占領が市民の生活を混乱させたように、このような攻撃を受けた国の市民は、紛争によって最も大きな影響を受ける集団となる可能性があります。

まだ幸いにも壊滅的なレベルには至っていませんが、各個人とビジネスコミュニティ全体が、自分たちの生活と業務を守る役割を担っています。政府機関や外交官が他の指導者と協力して次の攻撃の潜在的な影響を軽減する一方で、外国の敵対者による私たちの生活への侵入に対する最も強力な防御策の1つは、セキュリティ文化の共有です。

上記の複数の攻撃は、家庭用ルーターを使用して、安全確認や水の安全を制御するシステムに侵入しています。安全なパスワードでセキュアに設定されていないルーターがリビングルームにあると、敵にドアを開けてしまう可能性があります。eBayでルーターの出所を知らずに購入することも同様に危険です。

自国のインフラのごく一部を生産している組織のIT管理者も同様に、セキュリティの甘さによって、自国のインフラに敵が侵入する門戸を開いてしまう可能性があります。

このような小さな「セキュリティホール」によって、脅威行為者は大規模なシステムに侵入し、時には何年もそこに留まりながらシステムを巡回し、情報を収集したり、悪意のあるソフトウェアを仕込んだりします。侵入がその時点では気づかれなかったとしても、後々、多くの人々に甚大な影響を及ぼす可能性があります。

国家がスポンサーとなっているものも含め、すべてのハッカーはフィッシングやソーシャルエンジニアリングを好んで使い、認証情報を盗んだり、システムに侵入するためのその他の情報を収集したりします。コミュニティや組織におけるサイバーセキュリティに対する意識の欠如は、侵入に対してアタックサーフェス（攻撃対象領域）の門戸をひらいてしまうことなります。

国家がスポンサーとなっているものも含め、すべてのハッカーはフィッシングやソーシャルエンジニアリングを好み、それを使って認証情報を盗んだり、システムに侵入するための情報を集めたりします。コミュニティや組織におけるサイバーセキュリティに対する意識の欠如は、侵入に対してアタックサーフェス（攻撃対象領域）の門戸をひらいてしまうことなります。

強固なセキュリティ文化の構築には、組織内での議論に加えて、セキュリティ文化に関するレポートやホワイトペーパーといったものが必要となりますが、これだけでは実現できるものではありません。これは、政府や企業だけの仕事ではありません。家庭であれ職場であれ、個々のユーザーがセキュリティ文化をどう捉えるかが重要な出発点です。KnowBe4は毎年、ユーザーのオンライン行動を分析し、セキュリティ意識向上トレーニングを受けていない個人がフィッシングメールの不正リンクをクリックしやすいかどうかの基準値を算定しています。2024年業界別フィッシングベンチマークレポートでは、KnowBe4 がさまざまな業界や規模の1,100 万人のユーザーの行動を分析しました。この分析では、フィッシング詐欺やソーシャルエンジニアリング詐欺に引っかかる可能性のある従業員の割合を示すPhish-prone™ Percentage（以下PPP：フィッシング詐偽ヒット率）を測定しています。これによると、セキュリティ意識向上トレーニングを受けていないユーザーの34.3%、つまり3人に1人以上が、フィッシングメールに含まれる不正なリンクをクリックしてしまうと結果が出ています。ここには、個人的な問題だけでなく、職務上の責任や地域社会に対する責任も生じます。

良いニュースは、ここでの朗報として、継続的なセキュリティ意識向上トレーニングと模擬フィッシング演習を組み合わせたKnowBe4プログラムを90日間実施したところ、結果は顕著に変化し、フィッシングに引っかかりやすいユーザーの割合は全業種で18.4%に低下しました。1年以上の継続的なトレーニングの結果、フィッシングメールに引っかかるユーザーの割合は全業種で4.5%に減少しました。

# 防御対策の強化

重要インフラに対するサイバー攻撃の継続的かつ量的に拡大する傾向は、広範な社会的・経済的混乱を引き起こす世界的な脅威となっています。この増大するリスクに立ち向かい、サイバー侵害が成功するリスクを低減するためには、世界の組織は、テクノロジー、プロセスに加えて、人的防御対策を含む多層防御戦略を採用することが求められています。

**以下のステップを実施することで、サイバーレジリエンスを強化し、より強靭なサイバーセキュリティ防御対策プログラムを実践することができます。**

- 継続的なセキュリティトレーニングと評価を通じて強固なセキュリティ文化を醸成
- 機密情報および知的資産管理の実施
- すべての重要システムへのアクセスに多要素認証（MFA）を導入
- インシデント対応プレイブックの作成と定期的な更新
- 定期的なサイバー攻撃演習とシミュレーションの実施
- セキュアなバックアップシステム、テスト、復旧手順の確立
- 脅威インテリジェンスを共有するための業界パートナーや政府機関との協力
- 新たな脅威に対処するためのセキュリティ対策の継続的な評価と更新

これらの対策を統合することで、重要インフラは、進化するサイバー脅威に立ち向かうためのサイバーレジリエンスを大幅に向上させることができます。

脅威の状況は日々変化しています。社会が日々依存している重要なシステムを保護し続けるためには、日々の変化に対応したサイバーセキュリティ戦略は実施することは不可欠です。

# インシデント対応プレイブック

組織は、潜在的なインシデントや災害に備えなければなりません。IT チームとサイバーセキュリティチームによって作成されたインシデント対応プレイブックは、既知の攻撃に対する手順を概説し、リスクとダウンタイムを最小限に抑えます。すべての大災害を予測することは不可能ですが、災害復旧プログラムには、通常業務を迅速に復旧するためのインフラが必要です。

災害復旧プログラムには、「プレイブック」にまとめられ、復旧手順、連絡網、 Bitlockerコードや管理者パスワードのような重要な情報が含まれています。単一障害点を避けるため、安全なハードコピーを複数の場所に保管すること推奨します。

IT、OT、ビジネスの各チームが参加する定期的な訓練や卓上演習は、インシデント発生時のスタッフの準備態勢を確保するのに役立ちます。資産のインベントリ管理、MFA の導入、強固なセキュリティ文化の醸成など、サイバーセキュリティの基本的なプラクティスを取り入れることで組織、特に重要なインフラに携わる組織は、進化するサイバー脅威に立ち向かうためのサイバーレジリエンスを大幅に向上させることができます。

## その他の関連情報

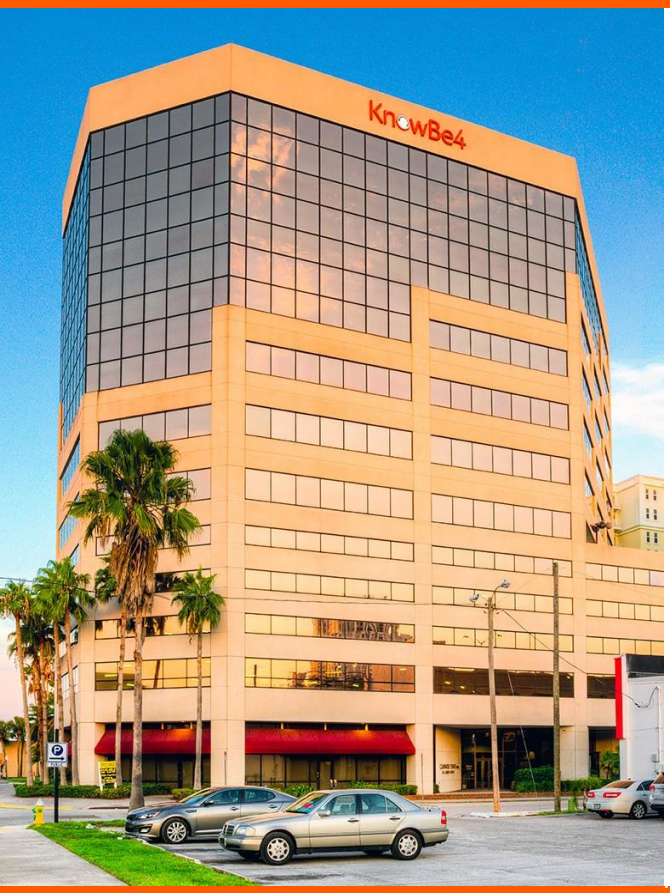
**フィッシングセキュリティテスト**
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。.

**セキュリティプログラムビルダー**
あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。

**Phish Alertボタン**
あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。

**無償Email Exposure Checkツール**
あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。

**無償なりすましドメインテスト**
ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。




## ＜KnowBe4について＞

KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4プログラムは、偽装攻撃によるベースラインテスティング、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、ビッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

2020年7月現在、金融機関、製造業、エネルギー産業、医療機関、官公庁、生損保などで、3万3千社を超える企業や団体がKnowBe4を採用して、防御 の最終ラインとして「人」による防御壁を構築して、日々求められるセキュリティ上の的確な意志決定を可能にしています。

**詳しくは、www.KnowBe4.jp**をアクセスしてください。

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社　〒100-6510 東京都千代田区丸の内1－5－1
新丸の内ビルディング10F EGG 内
Tel: 03-4586-4540 | www.KnowBe4.com／www.KnowBe4.jp |