2010年-2025年フィッシング詐欺の攻防史：単純な詐欺からAI駆動型サイバー戦争への進化

エグゼクティブサマリー：単純な騙りからAI駆動型戦争へ至る15年間の軍拡競争

本レポートは、2010年から2025年に至る15年間のフィッシング詐欺の軌跡を分析する。この期間において、フィッシングは大量送信・低品質な迷惑行為から、高度に標的化され、産業化し、AIによって増強された脅威へと劇的に進化した。本レポートの中心テーマは「軍拡競争」である。これは、防御側の技術革新（例：多要素認証）が攻撃側の対抗策（例：AiTM攻撃）を生み、それが次世代の防御策（例：FIDO2）を促すという、継続的かつ反応的なサイクルである。本稿の結論として、現在のAI駆動時代はこのサイクルを指数関数的に加速させており、セキュリティパラダイムを「ゼロトラスト」へと根本的に転換する必要性を提示する。

表1：フィッシングの手口と対策の時系列進化（2010年-2025年）

時代	主要な攻撃戦術	主要なソーシャルエンジニアリング原理	主要な防御技術・戦略	攻撃者の対抗戦術・次の進化
2010-2014年：マスマーケット時代	大量メール配信、認証情報窃取	広範な緊急性の演出、権威の偽装	利用者教育、静的ブラックリスト、スパムフィルター	ドメインホッピング、スピアフィッシングへの移行
2015-2019年：標的型精密攻撃時代	スピアフィッシング、ビジネスメール詐欺（	個別化された文面、信頼関係の悪用、業務プロ	送信ドメイン認証（SPF, DKIM, DMARC）、初期の多要素認証（	正規アカウントの乗っ取り、MFA回避技術

	BEC）	セスの悪用	MFA）	の開発
2020-2023年：技術的エスカレーション時代	MFA疲労攻撃、中間者攻撃（AiTM）、セッションハイジャック	心理的疲労の誘発、利便性の悪用（QRコード）	フィッシング耐性MFA（FIDO2/WebAuthn）、高度なエンドポイント保護	攻撃ベクトルの多様化（スミッシング、ビッシング、クイッシング）
2024-2025年以降：**AI**・産業化時代	生成AIによる文面作成、ディープフェイク、Phishing-as-a-Service（PhaaS）	超個別化（ハイパー・パーソナライゼーション）、音声・映像による信頼の構築	AIによる脅威検知（振る舞い検知、意味解析）、ゼロトラストアーキテクチャ	自律型攻撃エージェント、AIによる防御回避技術

第1章：マスマーケット・フィッシングの時代（2010年-2014年）：価値より量

1.1 初期フィッシングの解剖学：ドメイン偽装と認証情報窃取

2010年代初頭のフィッシングは、その後の高度な攻撃の原型を形成した。主要な手口は、金融機関や大手オンライン小売業者といった著名なブランドを装った電子メールを不特定多数に送りつけ、ユーザー名とパスワードを収集する認証情報窃取（Credential Harvesting）であった[1]。技術的な策略は比較的単純で、電子メールの送信元情報を偽装する「スプーフィング」や、正規サイトを模倣した偽のウェブサイト（フィッシングサイト）が用いられた。これらのサイトは、侵害されたウェブサーバーや、正規ドメインに酷似した「いとこドメイン（cousin domain）」にホストされることが多かった[2]。

この時期のソーシャルエンジニアリングは、広範なターゲットに共通する心理的トリガー、すなわち「緊急性」や「不安」を利用するものであった[3]。例えば、「アカウントがロックされました」「不正なアクセスが検出されました」といった件名でユーザーの注意を引き、偽サイトへのクリックを促した。Anti-Phishing Working Group（APWG）の2010年第1四半期の報告によれば、金融サービスと決済サービスが最も標的とされた業種であり、月間数万件のユニークなフィッシングサイトが検出されていた。これは、この初期段階においてもフィッシングが既に大規模な問題であったことを示している[1]

。

1.2 基礎的な防御：利用者教育と静的フィルタリングの優位

初期のフィッシングに対する防御策は、技術的な限界から、主にエンドユーザーの注意力に依存していた。当時のセキュリティガイダンスは、基本的なデジタル衛生（Digital Hygiene）の徹底に重点を置いていた。具体的には、推測されにくいパスワードの使用、見知らぬ送信元からのリンクを安易にクリックしないこと、そして送信元情報を手動で確認することなどが推奨された [5]。このアプローチは、セキュリティの責任を個人に大きく委ねるものであり、巧みなソーシャルエンジニアリングの前では不十分であることが後に証明される。

技術的な防御策は、既知の悪意のあるドメインやIPアドレスをリスト化した静的ブラックリストと、特定のキーワード（例：「パスワード」「更新」）に基づいてメールをフィルタリングする初期のスパムフィルターが中心であった [8]。これらの防御策は本質的に「事後対応」であり、新たな攻撃が出現してからリストが更新されるまでのタイムラグが、攻撃者にとっての好機となった。

1.3 初期の産業対応：軍拡競争の始まり

静的ブラックリストの限界は、攻撃者によって即座に悪用された。彼らはドメインやIPアドレスを頻繁に変更する「ドメインホッピング」戦術を用い、ブラックリストを容易に回避した。この攻撃側の適応に対し、防御側はより動的なシステムへと進化を遂げる。複数の脅威情報をリアルタイムで集約・共有する「リアルタイムブラックホールリスト（RBL）」や、送信元の過去の振る舞いに基づいて信頼性をスコアリングするレピュテーションリストが開発された [8]。

同時に、防御の主戦場はメールクライアントからウェブブラウザへと拡大した。Google Safe Browsingのようなサービスは、ユーザーが既知の悪意のあるサイトにアクセスしようとすると警告を表示する機能を提供し、重要な防御層となった [9]。これにより、たとえユーザーがメール内のリンクをクリックしてしまっても、ブラウザが第二の防衛線として機能する構造が生まれた。

この2010年代初頭の攻防は、その後の15年間の軍拡競争の基本的なパターンを確立した。それは、攻撃者が防御技術そのもの（例：暗号化）を破るのではなく、その実装の隙間やシステム間の連携の不備を突くというパターンである。この初期の動向は、後に登場するAiTM攻撃のように、MFAを破るのではなくその認証プロセスを乗っ取る、より洗練された攻撃手法を予見させるものであった。また、利用者教育への過度な依存とその失敗は、単なる戦略ミスではなく、当時の技術的未熟さを暗黙のうちに認めるものであった。このユーザー中心モデルの破綻こそが、業界がより堅牢で自動化されたプロトコルレベルのセキュリティ制御へと舵を切る直接的な触媒となったのである。

第2章：精密攻撃への転換（2015年-2019年）：スピアフィッシングとビジネスメール詐欺（BEC）の脅威

2.1 投網から銛へ：高価値な企業標的へのシフト

2010年代半ば、フィッシング攻撃の戦略は大きな転換点を迎えた。ベイジアンフィルタやヒューリスティック分析といった、より高度なスパムフィルタリング技術が普及し始めると、不特定多数を狙う大量配信型フィッシングの投資対効果（ROI）は低下した[8]。これに対応し、攻撃者は特定の個人や組織を狙い撃ちにする「スピアフィッシング」へと戦術を高度化させた[13]。

スピアフィッシングは、ソーシャルメディアや公開情報などを通じて標的を入念に調査（ソーシャルエンジニアリング）し、その情報を基に極めて説得力のある偽装メールを作成する[14]。例えば、業務に関連する内容や、標的の個人的な関心事を装うことで、警戒心を解き、悪意のある添付ファイルを開かせたり、偽サイトへ誘導したりする[3]。攻撃の目的も、単なる個人認証情報の窃取から、企業ネットワークへの侵入、機密情報の窃取、ランサムウェアなどの高度なマルウェアの展開へと拡大した[17]。

2.2 BECの解体：信頼、権威、そして欠陥のある業務プロセスの悪用

スピアフィッシングの中でも、最も金銭的被害が甚大であったのが「ビジネスメール詐欺（Business Email Compromise, BEC）」である。BECは、企業の経営幹部（CEO詐欺）や取引先になりすまし、経理・財務部門の従業員を騙して、攻撃者が用意した口座へ不正に送金させる手口だ[20]。

BECの成功は、高度な技術的ハッキングよりも、人間の心理と組織の業務プロセスの脆弱性を突くことに依存している。攻撃者は「機密のM&A案件」や「至急の支払い」といった口実で緊急性を演出し、正常な承認プロセスを迂回させる[24]。技術的な側面では、表示名を偽装したり、正規のドメイン名に酷似したドメイン（例：

example.comに対してexamp1e.comや、mをrnに見せかける）を使用したり、あるいは事前にフィッシングで窃取した正規のアカウントを乗っ取って信頼された送信元からメールを送るなどの手法が用いられた[26]。

日本航空（JAL）が約3億8,000万円の被害に遭った事例は、BECがいかに深刻な損害をもたらすか

を象徴している[21]。FBIのデータによれば、2015年1月から8月だけでBECによる全世界の報告被害額は270%増加しており、この脅威が急速に拡大したことがわかる[28]。BECの台頭は、サイバーセキュリティ技術そのものの失敗というよりは、むしろビジネスプロセスのセキュリティにおける致命的な欠陥を露呈した。攻撃者は、企業の階層構造、緊急性への対応、そして人間同士の信頼関係といった、いわば「ヒューマンAPI」を悪用したのである。この脅威に対する最も効果的な防御策は、新たなソフトウェアの導入以上に、「支払い先の変更依頼は、必ずメール以外の別の通信手段で再確認する」という単純かつ厳格な業務プロセスの徹底であった。これは、攻撃対象領域がデジタル空間だけでなく、組織の行動様式そのものにまで及んでいることを示している。

2.3 防御の進化：送信ドメイン認証（SPF, DKIM, DMARC）の台頭

BECやスピアフィッシングで中心的な役割を果たした「なりすまし」に対抗するため、業界は送信ドメイン認証技術の導入を推進した。これらは、メールが正当な送信元から送られたものであることを受信側が検証するための技術的枠組みである。

- **SPF (Sender Policy Framework):** 送信元メールサーバーのIPアドレスが、そのドメインからメールを送信することを許可されているかを検証する[29]。
- **DKIM (DomainKeys Identified Mail):** 電子署名を用いて、メールが送信途中で改ざんされていないことを保証する[29]。
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** SPFとDKIMの認証結果に基づき、認証に失敗したメールの取り扱い（隔離や拒否など）をドメイン所有者がポリシーとして宣言できるようにする。また、自ドメインがどのように利用されているかについてのレポートを受信できる[27]。

これらの技術は、ドメインの直接的な偽装を技術的に困難にし、防御における大きな一歩となった。しかし、その効果は送信者と受信者の両方による広範な導入と正しい設定に依存するため、普及には時間がかかった[31]。DMARCの普及が遅々として進まなかった背景には、サイバーセキュリティにおける経済的・協調的な課題が存在する。DMARCは主にドメイン所有者のブランドが偽装されるのを防ぐが、その導入コストは所有者が負担する一方で、その恩恵は主に潜在的な被害者である他者が受ける。このようなインセンティブの不一致は、集団的な行動を必要とするセキュリティ対策の導入を妨げる大きな要因であり、攻撃者に継続的な機会を与え続ける構造的な問題となっている。

2.4 高度な認証の第一波：初期MFAの約束と限界

メール認証技術と並行して、アカウント自体を保護するための「多要素認証（Multi-Factor Authentication, MFA）」が標準的な対策として広く推奨されるようになった[29]。SMSで送信される確認コードや、アプリが生成するワンタイムパスワード（OTP）といった初期のMFAは、パスワードのみ

に依存した認証を過去のものとし、単純な認証情報窃取型フィッシングに対しては非常に効果的だった。パスワードが盗まれても、第二の要素がなければアカウントにアクセスできないため、攻撃者は再びその手法を進化させることを余儀なくされた。

第3章：技術的エスカレーション（2020年-2023年）：セッションを巡る攻防

3.1 防御の迂回：MFA疲労攻撃とAiTM攻撃の出現

MFAの普及は、サイバーセキュリティにおける重要な防衛ラインとなったが、攻撃者はそれを破るのではなく、迂回する新たな手法を開発した。これにより、認証の戦いは新たな段階へと突入した。

- **MFA疲労攻撃（MFA Fatigue / Prompt Bombing）:** この攻撃は、まず何らかの手段でユーザーのパスワードを窃取することから始まる。その後、攻撃者はそのパスワードを使って繰り返しログインを試行し、ユーザーのスマートフォンや認証デバイスにMFAのプッシュ通知を大量に送りつける[36]。深夜や業務多忙な時間帯を狙い、ユーザーが疲労や混乱から誤って「承認」をタップしてしまうことを狙う。時には、「ITサポート」を名乗る電話を併用するなど、ソーシャルエンジニアリングと組み合わせて行われることもある[38]。
- **中間者攻撃（Adversary-in-the-Middle, AiTM）フィッシング:** これはMFA疲労攻撃よりもはるかに巧妙で、技術的に高度な攻撃である。攻撃者は、正規サービスと被害者の間に介在するリバースプロキシとして機能するフィッシングサイトを構築する。被害者はこの偽サイトとは気づかずにID、パスワード、そしてMFAコード（OTPなど）を入力する。偽サイトはこれらの情報をリアルタイムで正規サイトに中継し、認証を成功させる。正規サイトは認証成功の証として「セッションCookie」を発行するが、これを攻撃者のプロキシが傍受・窃取する[41]。一度セッションCookieを奪われると、攻撃者はパスワードやMFAデバイスなしで、そのセッションが有効な限り被害者のアカウントにアクセスし続けることが可能となる。これにより、MFAによる保護は完全に無力化される。

この攻撃手法の進化は、防御側が「認証情報」の保護に注力していたのに対し、攻撃側が現代のウェブアプリケーションにおける真の「王国の鍵」が「セッション」そのものであることを見抜いたことを示している。認証が成功した後に生成されるセッションCookieを奪う方が、認証プロセス自体を破るよりも容易であるという攻撃者の洞察が、AiTMという手法を生み出した。この認識の変化は、セキュリティ業界に「安全なMFAとは何か」という定義そのものを見直すことを強いた。

3.2 業界の対抗策：フィッシング耐性MFA（FIDO2/WebAuthn）の重要性

AiTM攻撃の出現は、全てのMFAが等しく安全ではないという事実を突きつけた。SMS、OTP、単純なプッシュ通知といった「フィッシング可能なMFA」は、中間者攻撃に対して脆弱であることが明らかになった。これに対する業界の回答が、真にフィッシングに耐性を持つMFA標準、すなわちFIDO2とその中核をなすWebAuthnの推進であった [46]。

FIDO2/WebAuthnは、公開鍵暗号方式に基づいている。ユーザー登録時に、秘密鍵がユーザーのデバイス（スマートフォンやセキュリティキー）内のセキュアな領域に生成・保管される。認証時には、サービス側（Relying Party）が「チャレンジ」と呼ばれるランダムなデータを送信し、デバイスが秘密鍵でこれに署名して返信する。このプロセスの決定的に重要な点は、署名がウェブサイトのドメイン情報（オリジン）に紐付けられていることである [46]。そのため、たとえユーザーが偽のドメインを持つフィッシングサイトにアクセスしても、そのサイトは正規ドメインに対する有効な署名を得ることができない。これにより、AiTMのリバースプロキシ攻撃は原理的に成立しなくなり、セッションハイジャックに対する根本的な技術的対抗策となる。

表2：多要素認証（**MFA**）方式の比較とフィッシング耐性

認証方式	セキュリティ原理	認証情報窃取への脆弱性	AiTM（セッションハイジャック）への脆弱性	ユーザー体験	総合フィッシング耐性評価
パスワードのみ	知識要素	非常に高い	非常に高い	良い	不可
SMS/Email OTP	知識要素＋所持要素	中	高い（コードを中継される）	普通	低い
プッシュ通知（単純承認）	所持要素	低	高い（MFA疲労攻撃、誤承認）	非常に良い	低い
TOTP（認証アプリ）	所持要素＋時間同期	低	高い（コードを中継される）	普通	低い

FIDO2/WebAuthn（パスキー）	所持要素＋生体/知識要素（公開鍵暗号）	非常に低い	非常に低い（オリジンバインディング）	非常に良い	非常に高い

3.3 攻撃ベクトルの多様化：スミッシング、ビッシング、クイッシングの拡散

メールとセッションCookieを巡る攻防が激化する一方で、攻撃者はユーザーが比較的警戒心の薄いチャネルへと攻撃の起点を多様化させた。

- スミッシング（**SMS Phishing**）：SMS（ショートメッセージサービス）を利用して悪意のあるリンクを送信する手口。宅配便の不在通知や金融機関からの緊急連絡などを装い、ユーザーのクリックを誘導する[50]。
- ビッシング（**Voice Phishing**）：電話（自動音声を含む）を用いて被害者を騙し、情報を聞き出したり、不正な操作を行わせたりする。他のフィッシング手法と連携して、信頼性を高めるために使われることも多い[51]。
- クイッシング（**QR Code Phishing**）：近年急速に増加している脅威。攻撃者は悪意のあるURLを埋め込んだQRコードを作成し、それをメールで送信したり、公共の場所にポスターとして掲示したりする。ユーザーはスマートフォンでQRコードを手軽にスキャンするため、URLの文字列を目視で確認するプロセスを省略しがちである。これにより、URLフィルタリングや人間の視覚的な警戒網をすり抜け、フィッシングサイトへ直接誘導されてしまう[52]。クイッシングは、ユーザーがQRコードを「単なる便利なショートカット」と認識し、攻撃ベクトルとは見なしていないという、認識と技術的現実との間のギャップを巧みに悪用した傑作と言える。

第4章：サイバー犯罪の産業化（2020年-2025年）：フィッシング・エコシステム

4.1 Phishing-as-a-Service (PhaaS)：参入障壁の崩壊

2020年代に入り、フィッシングはもはや個々のハッカーの活動ではなく、高度に専門化されたサービス産業によって支えられるようになった。その象徴が「Phishing-as-a-Service（PhaaS）」である。PhaaSプラットフォームは、正規のSaaS（Software-as-a-Service）ビジネスを模倣し、洗練された

フィッシングキット、インフラ、さらには顧客サポートまでをサブスクリプション形式で提供する[58]。

これらのプラットフォームは、何千ものブランドを模倣したテンプレート、攻撃キャンペーンの自動展開機能、そしてAiTMプロキシによるMFA回避や、セキュリティ製品によるスキャンを回避するためのボット検知機能といった高度なツールを提供する[60]。EvilProxyやTycoon 2FAといった著名なPhaaSは、ダークウェブやTelegramを通じて月額数百ドルで販売されており、これにより技術的スキルの低い犯罪者でも高度な攻撃を実行できるようになった[58]。このPhaaSモデルは、犯罪経済が「ツールベース」から「サービスベース」へと根本的に移行したことを示している。これは防御側にとって深刻な意味を持つ。もはや個別の静的な攻撃と戦っているのではなく、市場競争に基づいて常に進化し、専門的に管理される「サービス」と対峙しているからだ。一つのPhaaSプラットフォームが閉鎖されても、その顧客は単に競合他社に乗り換えるだけであり、脅威の継続性が確保されてしまう。

4.2 犯罪のサプライチェーン：専門分化、分業、そしてダークウェブ市場

現代のフィッシング攻撃のライフサイクルは、合法的なサプライチェーンと同様に高度に専門化・分業化されている[63]。

- 開発者: フィッシングキットやマルウェアを開発・販売する。
- 展開者（フィッシャー）: PhaaSのサブスクリプションを購入し、攻撃キャンペーンを実行する。
- インフラ提供者: 攻撃の痕跡を消すための防弾ホスティング（Bulletproof Hosting）やボットネットを提供する。
- 認証情報販売者: 窃取した認証情報をダークウェブ市場で販売する。
- 資金洗浄屋（マネーミュール）: 不正に得た資金を、追跡が困難なクリーンな資産に変換する。

このような分業体制は、攻撃の効率性と耐障害性を飛躍的に向上させる。法執行機関がサプライチェーンの一部分を摘発しても、他の専門グループがその役割を代替するため、犯罪エコシステム全体を無力化することは極めて困難である[63]。

4.3 収益化：暗号資産ミキサーとチェーンホッピングによる資金洗浄

攻撃の最終段階は、窃取した資産の収益化である。その匿名性と国際的な送金の容易さから、暗号資産（仮想通貨）は不正資金の洗浄（マネーロンダリング）に最適な手段として広く利用されている[66]。

攻撃者は、Chainalysisなどのブロックチェーン分析企業の報告で詳述されているように、不正資金の流れを隠蔽するために様々な技術を駆使する[68]。

- ミキサー/タンブラー: 多数のユーザーからの暗号資産を一つのプールに混ぜ合わせ、ランダム

に再分配することで、資金の出所と送金先の間のオンチェーン上の繋がりを断ち切るサービス[71]。
- チェーンホッピング: クロスチェーンブリッジを利用して、資金を異なるブロックチェーン間（例：イーサリアムからビットコインへ）で移動させ、追跡をさらに複雑化させる手法[68]。
- 規制の緩い取引所: AML（アンチマネーロンダリング）やKYC（顧客確認）の規制が緩い暗号資産取引所を通じて、不正な暗号資産を法定通貨に換金する[66]。

この犯罪サプライチェーンの専門化は、防御戦略に新たな視点をもたらす。フィッシングサイトの閉鎖はいたちごっこに過ぎないが、資金洗浄インフラ（例：Tornado Cashのようなミキサーへの制裁[72]、AML規制の緩い取引所への圧力[66]）を標的にすることは、犯罪者が利益を得る能力そのものを阻害する可能性がある。これは、効果的なフィッシング対策が、サイバーセキュリティ企業だけでなく、法執行機関、金融規制当局、そして国際的な協力を必要とする、学際的な取り組みであることを示唆している。

第5章：AIフロンティア（2024年-2025年以降）：攻撃と防御の新パラダイム

5.1 攻撃的AI：生成モデルによる超個別化された誘導とディープフェイク

GPT-4に代表される強力な大規模言語モデル（LLM）の登場は、ソーシャルエンジニアリングの様相を一変させた。攻撃者は現在、AIを次のように活用している。

- 完璧な文章の生成: 文法的に誤りがなく、文脈に即し、極めて説得力のあるフィッシングメールを大規模に自動生成する。これにより、古典的なフィッシングメールの兆候であった「不自然な日本語」は過去のものとなった[75]。学術研究によれば、AIが生成したフィッシングメールは、人間の専門家が作成したものと同等かそれ以上のクリック率を達成することが示されている[78]。
- 超個別化（ハイパー・パーソナライゼーション）: 偵察プロセスを自動化し、LinkedInなどのソーシャルメディアや公開情報を収集・分析することで、個人の役職、担当プロジェクト、人間関係に合わせてカスタマイズされたスピアフィッシングメールを瞬時に作成する[75]。
- ディープフェイク音声・映像: ビッシングやBEC攻撃において、AIはわずかな音声サンプルから経営幹部の声を忠実にクローンできるようになった。これにより、説得力のある留守番電話メッセージを残したり、リアルタイムで電話をかけて不正な送金を指示したりすることが可能になる[81]。香港で発生した事例では、ディープフェイク技術を用いた偽のビデオ会議によって、従業員が約38億円（2500万米ドル）を送金させられるという被害が報告されている[84]。

生成AIの導入は、高度な攻撃の経済性を根本的に変えた。従来、高品質なスピアフィッシングは、調査と文面作成に多大な時間と人的労力を要するため、その規模は限定的だった。しかしAIは、API コール一回分のコストで、オーダーメイドの高品質なソーシャルエンジニアリングを可能にする。これは、大量・低品質な攻撃と、少量・高品質な攻撃という従来の区別を無意味にし、「大量生産される高品質なスピアフィッシング」という新たな脅威カテゴリーを生み出した。

5.2 自律型脅威の夜明け：自己増殖型フィッシングキャンペーンへ

次のフロンティアは、自律的に動作するAI駆動型の攻撃エージェントの開発である。これらの「マルチエージェント」システムは、最小限の人間の介入で、偵察、標的選定、誘導メールの作成・送信、チャットボットによる被害者との対話、そして防御策に応じた戦術の適応まで、キャンペーン全体を自己完結的に管理する能力を持つ可能性がある[80]。まだ概念実証の段階にあるものが多いが、基盤となる技術は急速に成熟している。

5.3 防御的AI：機械学習とLLMを活用した高度な脅威検知

防御側においても、AIは不可欠なツールとなっている。セキュリティベンダーは、機械学習とLLMを駆使して、次のような高度な防御を実現している。

- 異常検知: シグネチャベースの検知を超え、メールの文脈、意味、そして意図を分析する。これにより、たとえ文章が完璧であっても、その要求が疑わしいものであればフラグを立てることができる[87]。ChatSpamDetectorのようなシステムは、フィッシングメールの検知において99%を超える精度を実証している[88]。
- ユーザーおよびエンティティの振る舞い分析（**UEBA**）: 正常なユーザーやシステムの振る舞いをプロファイリングし、フィッシング成功後のアカウント乗っ取りを示すような逸脱行動を検知する[75]。
- グラフニューラルネットワーク: 送信者、受信者、IPアドレスといったエンティティ間の関係性をモデル化し、個別のトランザクションでは見えない複雑な不正パターンを検出する[91]。

5.4 新たな課題：AI生成フィッシングコンテンツの検出

軍拡競争の新たな戦線は、AIによって生成されたコンテンツ自体の検出である。研究によれば、BERTやRoBERTaのような深層学習モデルはフィッシング全般の検出に非常に効果的である一方、

人間が書いたフィッシングメールとAIが生成したそれとの間には文体的な差異が存在することが示されている [92]。LLMを用いて従来のフィルターを回避しようとする攻撃者に対抗するためには、AIが生成したサンプルを含むデータセットで検知モデルを訓練することが不可欠になりつつある [95]。

このAIを巡る攻防は、デジタルコミュニケーションにおける「信頼の危機」をもたらすだろう。ディープフェイクの音声や映像が本物と見分けがつかなくなると、「電話で声を聞いたから本人だと確信した」といった伝統的な本人確認手法は完全に信頼性を失う [81]。これは、組織が高リスクな通信や取引において、誤りやすい人間の知覚への依存から脱却し、暗号技術に基づいた検証可能なアイデンティティシステムの導入を加速させることを強いることになる。

第6章：ゼロトラストの未来に向けた戦略的必須事項

6.1 意識向上を超えて：技術、プロセス、そして人間のレジリエンスの統合

フィッシングの15年間の歴史は、利用者へのセキュリティ意識向上トレーニングが必要不可欠である一方で、それ単体では不十分であることを明確に示している [50]。現代の防御戦略は、以下の要素を統合した包括的なアプローチを必要とする。

- **技術:** ユーザーが最終的には騙されることを前提とした、強力でフィッシング耐性のある技術的制御。
- **プロセス:** 金銭取引における帯域外での承認義務化など、チェック・アンド・バランス機能を提供する安全な業務プロセス。
- **人間のレジリエンス:** 単にクリックを避けるだけでなく、不審なアクティビティを報告することに重点を置いた、脅威と共に進化し続ける継続的なトレーニング。

6.2 レジリエンスのためのアーキテクチャ：フィッシング対策におけるゼロトラスト原則の役割

現代のフィッシング脅威に対する究極的な戦略的回答は、「ゼロトラスト」セキュリティアーキテクチャの採用である [98]。ゼロトラストは、「信頼する、しかし検証する（Trust but Verify）」という従来のセキュリティモデルを覆し、「決して信頼せず、常に検証する（Never Trust, Always Verify）」という原則に基づいている。

これは、たとえ攻撃者がフィッシングによって認証情報を窃取したとしても、その被害を最小限に抑えることを意味する。あらゆるユーザー、デバイス、場所からのすべてのアクセス要求が信頼できないものとして扱われ、個別に認証・認可されなければならない。このアプローチにより、フィッシング成功時の被害範囲（Blast Radius）を封じ込め、ネットワーク内での横方向への侵攻（Lateral Movement）を防ぐことができる [98]。ゼロトラストは単なる製品ではなく、15年間の防御の軍拡競争から導き出された論理的結論としての戦略哲学である。利用者教育、スパムフィルター、パスワード、そしてフィッシング可能なMFAといった、過去の防御層の失敗はすべて、「ユーザーを信頼する」「社内ネットワークを信頼する」「認証情報を信頼する」といった欠陥のある信頼の仮定に基づいていた。フィッシングの執拗な成功はこれらの仮定を組織的に破壊し、すべてを検証するアプローチを唯一の実行可能な道として残した。

6.3 認証の未来：フィッシング耐性プロトコルの義務化

従来のMFAの脆弱性が証明された今、ゼロトラスト戦略の中核をなすのは、フィッシング耐性を持つMFA、具体的にはFIDO2/WebAuthnの全社的な導入である [46]。これにより、認証は共有秘密（パスワードやOTP）に依存するモデルから、暗号学的証明に基づくモデルへと移行する。これは、AiTMやその他の高度な攻撃に対する唯一信頼できる防御策である。

6.4 国境を越えた協力と脅威情報共有のための提言

フィッシングは国境を越える、産業化されたグローバルな犯罪である。犯罪エコシステムは世界中に分散し、被害者もまたグローバルに存在する [100]。単一の組織や国だけでこれに対抗することは不可能である。

したがって、官民連携と国際協力の重要性は計り知れない。日本のAPWG（フィッシング対策協議会）、JPCERT/CC、JC3や、INTERPOL（国際刑事警察機構）、Europol（欧州刑事警察機構）といった国際機関は、脅威情報の共有、フィッシングインフラのテイクダウン調整、そして国境を越えた犯罪者の追跡において極めて重要な役割を果たしている [101]。これらの協力体制を強化することは、効果的なグローバル防衛体制を構築するための必須条件である。PhaaSエコシステムやAI駆動型攻撃の速度と適応性を鑑みれば、一部の侵害は避けられない。したがって、成功する戦略とは、完璧な防御を約束するものではなく、フィッシングによる侵害を壊滅的な損害が発生する前に検知、封じ込め、そして復旧できる能力を持つ戦略である。これは、セキュリティオペレーションセンター（SOC）やインシデント対応能力、そしてゼロトラストのような攻撃の被害範囲を限定するアーキテクチャの重要性を一層高めるものである。

引用文献

1. Phishing Activity Trends Report, 1st Quarter / 2010 - APWG, 8月 19, 2025にアクセス、https://docs.apwg.org/reports/apwg_report_Q1_2010.pdf
2. Anti-Phishing Working Group, 8月 19, 2025にアクセス、https://docs.apwg.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf
3. フィッシング攻撃 - Rapid7, 8月 19, 2025にアクセス、https://www.rapid7.com/ja/fundamentals/phishing-attacks/
4. A Tale of the Three *ishings: Part 1 – What is Phishing? - SANS Institute, 8月 19, 2025にアクセス、https://www.sans.org/blog/a-tale-of-the-three-ishings-part-1-what-is-phishing
5. フィッシング詐欺とは？ | 国民のためのサイバーセキュリティサイト, 8月 19, 2025にアクセス、https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/risk/04/
6. フィッシング詐欺とは？その手口や被害に遭わないための対策方法を解説！ - りそな銀行, 8月 19, 2025にアクセス、https://www.resonabank.co.jp/kojin/column/credit/column_0007.html
7. フィッシング詐欺被害とは？メールによる手口とその対策方法 - SAXA-DX Navi - サクサ, 8月 19, 2025にアクセス、https://www.saxa.co.jp/saxa-dx_navi/trend/tr0049-security-u01-n003-n010.html
8. スパムメールへの対策技術とその変遷とは？最新ツールの技術を解説！ - ITトレンド, 8月 19, 2025にアクセス、https://it-trend.jp/anti_spam/article/explain
9. Choose your Safe Browsing protection level in Chrome - Android - Google Help, 8月 19, 2025にアクセス、https://support.google.com/chrome/answer/9890866?hl=en&co=GENIE.Platform%3DAndroid
10. Google Safe Browsing, 8月 19, 2025にアクセス、https://safebrowsing.google.com/
11. Safe Browsing site status - Google Transparency Report, 8月 19, 2025にアクセス、https://transparencyreport.google.com/safe-browsing
12. 迷惑メール（スパム）対策技術の変遷, 8月 19, 2025にアクセス、https://www.jnsa.org/jnsapress/vol13/13_03-08.pdf
13. スピアフィッシングとは？特徴や対策について徹底解説！ | Winserverのススメ, 8月 19, 2025にアクセス、https://www.winserver.ne.jp/column/about_spear-phishing/
14. スピアフィッシング攻撃とは？手口や4つの対策・フィッシングとの違いを解説 - 不正検知サービス, 8月 19, 2025にアクセス、https://frauddetection.cacco.co.jp/media/knowhow/12777/
15. スピアフィッシングとは？高精度な標的型攻撃の手口と対策 - SMSデータテック, 8月 19, 2025にアクセス、https://www.sms-datatech.co.jp/securitynow/articles/blog/sec_spearphishing/
16. スピアフィッシングとは？対策やフィッシングとの違いを解説 - wiz LANSCOPE ブログ, 8月 19, 2025にアクセス、https://www.lanscope.jp/blogs/cyber_attack_cp_blog/20240131_18829/
17. スピアフィッシング（Spear Phishing）とは？意味とセキュリティ対策 | Proofpoint JP, 8月 19, 2025にアクセス、https://www.proofpoint.com/jp/threat-reference/spear-phishing
18. スピアフィッシング VS フィッシング - MailData, 8月 19, 2025にアクセス、https://maildata.jp/blog/blog-2023-07-21.html
19. JPCERT/CC 活動概要 [2015 年4 月1 日 ～ 2015 年6 月30 日], 8月 19, 2025にアクセ

ス、https://www.jpcert.or.jp/pr/2015/PR20150714.pdf
20. フィッシング攻撃とは？種類と事例 - Wallarm, 8月 19, 2025にアクセス、https://www.wallarm.com/jp/what/types-of-phishing-attacks-and-business-impact
21. BEC＝ビジネスメール詐欺は「メール監視」から始まっている | サイバーセキュリティ, 8月 19, 2025にアクセス、https://www.nec-solutioninnovators.co.jp/ss/insider/column10.html
22. ビジネスメール詐欺（BEC）とは？実際の被害事例や対策方法について解説 - Fortinet, 8月 19, 2025にアクセス、https://www.fortinet.com/jp/resources/cyberglossary/business-email-compromise
23. 経理担当者にこそ知ってほしい「ビジネスメール詐欺＝BEC」の実態 - ASCII.jp, 8月 19, 2025にアクセス、https://ascii.jp/elem/000/001/660/1660128/
24. ビジネスメール詐欺（BEC）とは？手口や被害事例、企業がとるべきセキュリティ対策を解説, 8月 19, 2025にアクセス、https://www.cybersolutions.co.jp/product/securitysuite/cmss-blog/24237/
25. ビジネスメール詐欺(BEC)とは？手口や被害事例、対策を解説 - wiz LANSCOPE ブログ, 8月 19, 2025にアクセス、https://www.lanscope.jp/blogs/cyber_attack_cpdi_blog/20231212_17267/
26. ビジネスメール詐欺「BEC」に関する事例と注意喚起 - IPA, 8月 19, 2025にアクセス、https://www.ipa.go.jp/archive/files/000058478.pdf
27. AI技術の発展で再注目されるBECについて - インテリジェントウェイブ, 8月 19, 2025にアクセス、https://www.iwi.co.jp/blog/security/cybersecurity_measures/20230615/
28. Phishing Activity Trends Report, 1st – 3rd Quarters 2015 - APWG, 8月 19, 2025にアクセス、https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf
29. フィッシング対策 | 警察庁Webサイト, 8月 19, 2025にアクセス、https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html
30. 【コラム】DMARCとは？なりすましメール対策で注目される理由や導入のメリットを解説 - Fujifilm, 8月 19, 2025にアクセス、https://sp-jp.fujifilm.com/contents_school/column/column43.html
31. DMARCとは？メリットや普及率設定方、SPFとDKIMとの違い - faxdm屋ドットコム, 8月 19, 2025にアクセス、https://www.faxdmya.com/mkwords/dmarc
32. DMARC導入を例に解説 | メールセキュリティの難しさと対策 - NRIセキュア, 8月 19, 2025にアクセス、https://www.nri-secure.co.jp/blog/dmarc
33. 総務省 | 令和6年版 情報通信白書 | 送信ドメイン認証技術の導入状況, 8月 19, 2025にアクセス、https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/nd21a240.html
34. 情報セキュリティ10大脅威 2022 - IPA, 8月 19, 2025にアクセス、https://www.ipa.go.jp/security/10threats/ps6vr7000000avnh-att/000096899.pdf
35. ボイスフィッシングとは？被害事例や対策を解説|セキュリティニュースのセキュリティ対策Lab, 8月 19, 2025にアクセス、https://rocket-boys.co.jp/security-measures-lab/what-is-voice-phishing-and-social-engineering-tactics/
36. 多要素認証疲労攻撃(MFA疲労攻撃)とは？概要とリスク、対策を解説 - 株式会社アクト, 8月 19, 2025にアクセス、https://act1.co.jp/column/0291-2/

37. 多要素認証疲労攻撃とは？MFA疲労攻撃とも呼ばれる攻撃手段と対策を解説, 8月 19, 2025にアクセス、https://cybersecurity-jp.com/column/72896
38. 【次はあなたかも?!】急増する《多要素認証疲労攻撃》の実態とは？ ～PassLogicによる新たな対策, 8月 19, 2025にアクセス、https://passlogic.jp/passlogic_blog/mfa-fatigue-attack/
39. MFA回避の技術：攻撃者はどのようにして二要素認証を突破するのか - Blog | Menlo Security, 8月 19, 2025にアクセス、https://www.menlosecurity.com/ja-jp/blog/mfa-e5-9b-9e-e9-81-bf-e3-81-ae-e6-8a-80-e8-a1-93-ef-bc-9a-e6-94-bb-e6-92-83-e8-80-85-e3-81-af-e3-81-a9-e3-81-ae-e3-82-88-e3-81-86-e3-81-ab-e3-81-97-e3-81-a6-e4-ba-8c-e8-a6-81-e7-b4-a0-e8-aa-8d
40. MFAを狙った攻撃に注意してください - RSA Security, 8月 19, 2025にアクセス、https://www.rsa.com/ja/resources/blog/multi-factor-authentication/beware-mfa-fatigue/
41. AiTM攻撃とは？ 10分でわかりやすく解説 - ネットアテスト, 8月 19, 2025にアクセス、https://www.netattest.com/aitm-attack-2024_mkt_tst
42. 「AiTM攻撃」：最新ITキーワード - NECフィールディング, 8月 19, 2025にアクセス、https://www.fielding.co.jp/column/latest_it_keyword/202306_1/
43. 中間者攻撃(AiTM攻撃)とは？多要素認証で防げない理由と対策を解説, 8月 19, 2025にアクセス、https://rocket-boys.co.jp/security-measures-lab/aitm-attack-explained-mfa-limitations-countermeasures/
44. Adversary in the middle（AiTM攻撃）とは？多要素認証を回避する新手のフィッシング詐欺を解説, 8月 19, 2025にアクセス、https://cybersecurity-jp.com/column/80980
45. Microsoft が多要素認証を回避するフィッシング攻撃「Adversary-in-the-Middle（AiTM）」について発表 | BLOG - サイバートラスト, 8月 19, 2025にアクセス、https://www.cybertrust.co.jp/blog/certificate-authority/client-authentication/aitm-phishing-and-mfa.html
46. パスキーとは FIDO認証との違い、3つのメリットと課題 - WOR(L)D ワード - 大和総研, 8月 19, 2025にアクセス、https://www.dir.co.jp/world/entry/passkey
47. FIDO2とは？仕組みやFIDOやパスキーとの違い、メリットとデメリットなどを解説, 8月 19, 2025にアクセス、https://corp.capy.me/blog/passkey/2025/03/fido2%E3%81%A8%E3%81%AF%EF%BC%9F%E4%BB%95%E7%B5%84%E3%81%BF%E3%82%84fido%E3%82%84%E3%83%91%E3%82%B9%E3%82%AD%E3%83%BC%E3%81%A8%E3%81%AE%E9%81%95%E3%81%84%E3%80%81%E3%83%A1%E3%83%AA%E3%83%83%E3%83%88/
48. フィッシング耐性の高い多要素認証（MFA）の必要性 - Okta, 8月 19, 2025にアクセス、https://www.okta.com/jp/blog/2022/10/the-need-for-phishing-resistant-multi-factor-authentication/
49. ワンタイムパスワードでは防げない、リアルタイムフィッシングの脅威～パスキーによるフィッシング耐性の本質とは - Nat Zone, 8月 19, 2025にアクセス、https://www.sakimura.org/2025/06/7160/
50. A Tale of the Three *ishings: Part 02 – What is Smishing? - SANS Institute, 8月 19, 2025にアクセス、

https://www.sans.org/blog/a-tale-of-the-three-ishings-part-02-what-is-smishing
51. 自動音声を併用するボイスフィッシングが多発 〜ネットバンキングの法人口座を守る〜, 8月 19, 2025にアクセス、https://stealthmole.jp/blog/view/page/1/id/140
52. APWG Q1 Report: Phone-Based Phishing Grows Explosively, Shifting the Cybercrime Threatscape | Newswire, 8月 19, 2025にアクセス、https://www.newswire.com/news/apwg-q1-report-phone-based-phishing-grows-explosively-shifting-the-22336457
53. QRコード詐欺（クイッシング）とは？手口や実例、対策方法について解説 | フォーティネット - Fortinet, 8月 19, 2025にアクセス、https://www.fortinet.com/jp/resources/cyberglossary/qr-code-fraud
54. QRコード詐欺（クイッシング）とは？主な手口や対策を解説 - wiz LANSCOPE ブログ, 8月 19, 2025にアクセス、https://www.lanscope.jp/blogs/it_asset_management_emcloud_blog/20240517_20610/
55. クイッシングとは？QRコードを使ったフィッシング詐欺の事例 - Tigers-net.com, 8月 19, 2025にアクセス、https://www.tigers-net.com/support/security/article/000177.html
56. クイッシングとは？ QRコードを使ったフィッシング詐欺の事例 - ネット詐欺総研, 8月 19, 2025にアクセス、https://netsagisoken.jp/feature/20240809/
57. QRコード詐欺（クイッシング）とは？よくある手口や対策について解説 - Trend Micro News, 8月 19, 2025にアクセス、https://news.trendmicro.com/ja-jp/news-phishingscam-qrcode202409/
58. Everything you need to know about Phishing-as-a-Service | Barracuda Networks Blog, 8月 19, 2025にアクセス、https://blog.barracuda.com/2025/06/11/everything-need-know-phishing-as-a-service
59. What is Phishing-as-a-Service (PhaaS) and How To Protect Against It - Heimdal Security, 8月 19, 2025にアクセス、https://heimdalsecurity.com/blog/what-is-phishing-as-a-service-phaas/
60. Account Compromise Arms Race: The Rise of Phishing-as-a-Service - Abnormal AI, 8月 19, 2025にアクセス、https://abnormal.ai/blog/account-compromise-phishing-as-a-service
61. Phishing-as-a-Service (PhaaS): A Cybercrime Subscription Service - Trustwave, 8月 19, 2025にアクセス、https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/phishing-as-a-service-phaas-a-cybercrime-subscription-service/
62. How Phishing Kits Work: Unpacking Cybercriminal Tools in 2024 - Abnormal AI, 8月 19, 2025にアクセス、https://abnormal.ai/blog/how-phishing-kits-work
63. 「仕掛け人」と「被害者」だけではない、フィッシング詐欺の分業体制 | SHIFT SECURITY, 8月 19, 2025にアクセス、https://www.shiftsecurity.jp/blog/20220914
64. サイバー攻撃の対策方法とは？攻撃方法のトレンドから対策まで解説, 8月 19, 2025にアクセス、https://www.hcnet.co.jp/column/detail50.html
65. サイバー空間の安全の確保 - 警察庁, 8月 19, 2025にアクセス、https://www.npa.go.jp/hakusyo/r03/pdf/03_tokushu02.pdf
66. 暗号資産交換業最大手バイナンスがマネロン対策違反で米政府に罰金支払い, 8月 19, 2025にアクセス、https://www.nri.com/jp/media/column/kiuchi/20231201.html

67. 暗号資産交換業者への不正送金対策の強化に関する金融機関への要請について - 警察庁, 8月 19, 2025にアクセス、https://www.npa.go.jp/bureau/cyber/koho/news/20240206.html
68. 2024 Crypto Money Laundering Report - Chainalysis, 8月 19, 2025にアクセス、https://www.chainalysis.com/blog/2024-crypto-money-laundering/
69. 2025 Crypto Crime Mid-year Update: Stolen Funds Surge as DPRK Sets New Records, 8月 19, 2025にアクセス、https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/
70. 2025 Crypto Crime Trends from Chainalysis, 8月 19, 2025にアクセス、https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/
71. Mixers and Tumblers: Regulatory Overview and Use in Illicit Activities | Merkle Science, 8月 19, 2025にアクセス、https://www.merklescience.com/blog/mixers-and-tumblers-regulatory-overview-and-use-in-illicit-activities
72. Cryptocurrency tumbler - Wikipedia, 8月 19, 2025にアクセス、https://en.wikipedia.org/wiki/Cryptocurrency_tumbler
73. Bitcoin mixer - Bitcoin Wiki, 8月 19, 2025にアクセス、https://en.bitcoin.it/wiki/Bitcoin_mixer
74. Crypto mixers and crosschain bridges: How hackers launder stolen assets - Cointelegraph, 8月 19, 2025にアクセス、https://cointelegraph.com/explained/crypto-mixers-and-crosschain-bridges-how-hackers-launder-stolen-assets
75. AI-Powered Phishing Kits: The New Frontier in Social Engineering - Seceon Inc, 8月 19, 2025にアクセス、https://seceon.com/ai-powered-phishing-kits-the-new-frontier-in-social-engineering/
76. AI Phishing Attacks: How Big is the Threat? (+Infographic) - Hoxhunt, 8月 19, 2025にアクセス、https://hoxhunt.com/blog/ai-phishing-attacks
77. The Rise of AI Phishing and What it Means for the Future of Scammers - Transactional Email API Service For Developers | Mailgun, 8月 19, 2025にアクセス、https://www.mailgun.com/blog/email/ai-phishing/
78. AIが“超高精度”のフィッシングメールを自動生成：クリック率50%超を達成 | Ledge.ai, 8月 19, 2025にアクセス、https://ledge.ai/articles/ai_spear_phishing_campaigns_click_rate_study
79. LLM-Powered Intent-Based Categorization of Phishing Emails This research was funded by the European Union as part of the Horizon Europe project SYNAPSE (GA No. 101120853). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European - arXiv, 8月 19, 2025にアクセス、https://arxiv.org/html/2506.14337v1
80. AIに攻撃される未来はすぐそばに？AIが攻撃を仕掛ける時代に備えるためには - KnowBe4, 8月 19, 2025にアクセス、https://www.knowbe4.jp/blog/ai-attacks-are-coming-in-a-big-way-now
81. ディープフェイクとは？危険性や被害事例、見分け方を解説 - LANSCOPE, 8月 19, 2025にアクセス、https://www.lanscope.jp/blogs/cyber_attack_dt_blog/20250228_25331/

82. まるで本人の声で詐欺電話が？音声ディープフェイクが広がる今、私たちにできる対策とは, 8月 19, 2025にアクセス、https://www.knowbe4.jp/blog/warning-voice-deepfakes-continue-to-improve
83. いったいこれは誰の声？生成 AI による音声なりすましが新たなビッシング攻撃に利用される, 8月 19, 2025にアクセス、https://cloud.google.com/blog/ja/topics/threat-intelligence/ai-powered-voice-spoofing-vishing-attacks
84. フィッシング攻撃の多様化とAIの悪用について - サービス&セキュリティ株式会社, 8月 19, 2025にアクセス、https://www.ssk-kan.co.jp/topics/?p=15243
85. AIマルウェアと戦うには | IBM, 8月 19, 2025にアクセス、https://www.ibm.com/jp-ja/think/insights/defend-against-ai-malware
86. サイバーセキュリティ最前線～サイバー攻撃×生成AIの最新動向～ | DATA INSIGHT | NTTデータ, 8月 19, 2025にアクセス、https://www.nttdata.com/jp/ja/trends/data-insight/2025/013101/
87. URL に基づく機械学習を用いたフィッシングサイト判別の精度向上ー差異係数に着目した特徴量選定, 8月 19, 2025にアクセス、https://www.jc.u-aizu.ac.jp/news/management/gr/2024/03.pdf
88. ChatSpamDetector: 生成AIによるフィッシングメール検出 | NTTセキュリティテクニカルブログ, 8月 19, 2025にアクセス、https://jp.security.ntt/tech_blog/chatspamdetector-ai
89. Enhancing Phishing Email Identification with Large Language Models - ResearchGate, 8月 19, 2025にアクセス、https://www.researchgate.net/publication/388847613_Enhancing_Phishing_Email_Identification_with_Large_Language_Models
90. ChatSpamDetector: Leveraging Large Language Models for Effective Phishing Email Detection - arXiv, 8月 19, 2025にアクセス、https://arxiv.org/html/2402.18093v1
91. 金融犯罪対策の最前線！AI不正検知の最新技術トレンド - SREホールディングス, 8月 19, 2025にアクセス、https://ac.sre-group.co.jp/blog/financial-crime-measures
92. In-Depth Analysis of Phishing Email Detection: Evaluating the Performance of Machine Learning and Deep Learning Models Across Multiple Datasets - MDPI, 8月 19, 2025にアクセス、https://www.mdpi.com/2076-3417/15/6/3396
93. Analysis and prevention of AI-based phishing email attacks - arXiv, 8月 19, 2025にアクセス、https://arxiv.org/html/2405.05435v1
94. Analysis and Prevention of AI-Based Phishing Email Attacks - ResearchGate, 8月 19, 2025にアクセス、https://www.researchgate.net/publication/380475287_Analysis_and_Prevention_of_AI-Based_Phishing_Email_Attacks
95. Evolution of Phishing Detection with AI: A Comparative Review of Next-Generation Techniques - arXiv, 8月 19, 2025にアクセス、https://arxiv.org/html/2507.07406v1
96. Machine Learning and Watermarking for Accurate Detection of AI-Generated Phishing Emails - MDPI, 8月 19, 2025にアクセス、https://www.mdpi.com/2079-9292/14/13/2611
97. SANS Report Reveals Social Engineering as Top Security Risk - TECHx Media, 8月

19, 2025にアクセス、https://techxmedia.com/en/sans-report-reveals-social-engineering-as-top-security-risk/
98. ゼロトラストセキュリティとは？ メリット・デメリット、課題と解決策を解説 - HENNGE, 8月 19, 2025にアクセス、https://hennge.com/jp/service/one/glossary/zerotrust/
99. Zero Trustは - ゼロトラストセキュリティのアーキテクチャとは - Cloudflare, 8月 19, 2025にアクセス、https://www.cloudflare.com/ja-jp/learning/access-management/how-to-implement-zero-trust/
100. INTERPOL releases new information on globalization of scam centres, 8月 19, 2025にアクセス、https://www.interpol.int/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres
101. 日本クレジットカード協会と連携したフィッシング被害防止の啓発キャンペーンを開始しました。, 8月 19, 2025にアクセス、https://www.jc3.or.jp/threats/topics/article-606.html
102. フィッシング対策に関する協力 | お知らせ | NEWS, 8月 19, 2025にアクセス、https://www.jc3.or.jp/news/2022/20220113-424.html
103. 国内CSIRT、関係組織との連携によるサイバー脅威対策の強化 - JPCERT コーディネーションセンター, 8月 19, 2025にアクセス、https://www.jpcert.or.jp/about/06_7.html
104. 不正送金に係るフィッシング犯行グループの観測と〈みずほ〉の対策, 8月 19, 2025にアクセス、https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_2_1_yako_takeuchi_endo_jp.pdf
105. Phishing Activity Trends Report, 4th Quarter 2024 - APWG, 8月 19, 2025にアクセス、https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf
106. Fighting cybercrime in a connected world - Interpol, 8月 19, 2025にアクセス、https://www.interpol.int/News-and-Events/News/2019/Fighting-cybercrime-in-a-connected-world