アクモス標的型攻撃メール訓練・教育サービスVol.2

標的型攻撃メール訓練・教育サービス

2026年版・お役立ち資料

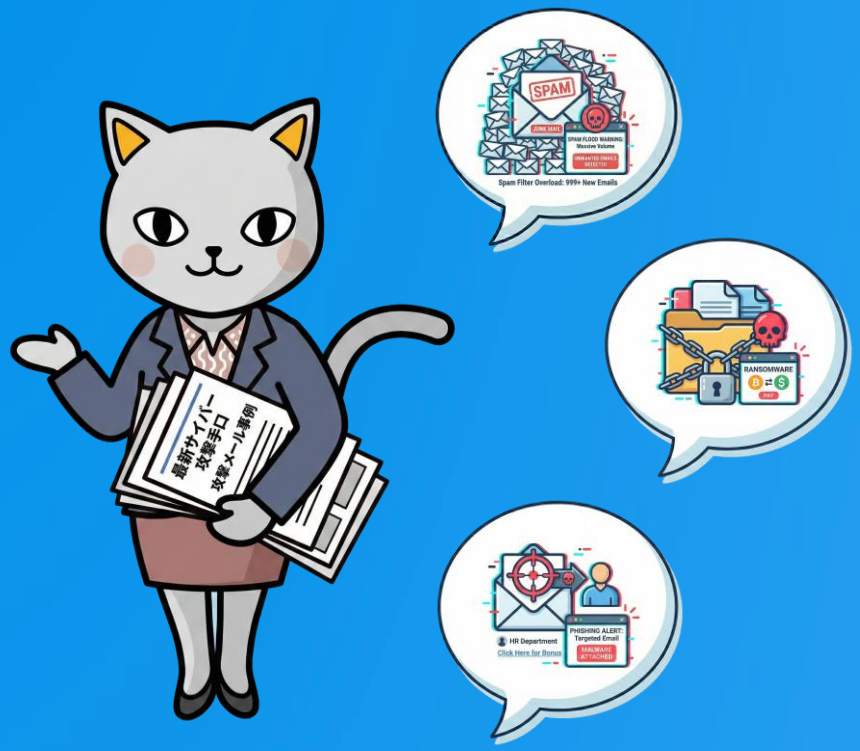
企業・団体を狙う メール攻撃の最新事例

アクモス 株式会社

本資料の目的・留意事項

Purpose and Notes

定番から最新のメール攻撃の手口を知り、
技術の限界を補う『人のセキュリティ対策』
を学ぶための資料です。



攻撃者は、実際の企業やサービス、果てはあなたの会社の「取引先」や「業務」になりすまし、従業員の無防備なクリックを虎視眈々と狙っています。一度侵入を許せば、事業停止や数十億円規模の損失に加え、取引先からの信頼失墜という取り返しのつかない事態を招きかねません。本資料では、実際に届いた最新の攻撃・迷惑メール事例を公開します。

「技術的な対策だけでは防げない領域」があることを認識いただき、組織全体で取り組むべき最終防衛ライン――「従業員のセキュリティリテラシー向上」の必要性を検討するための判断材料としてお役立てください。

現状の把握

最新の脅威トレンドを知り、自社のセキュリティ対策に「抜け穴（人的リスク）」がないかを再点検

社内への啓蒙

具体的な被害事例や攻撃メールの文面を共有し、経営層や従業員へ「明日は我が身」という危機意識を醸成

対策の立案

技術的な防御に加え、組織として取り組むべき「教育・訓練」の具体的な手法を検討

※本資料は、一部生成AIを使用した画像が含まれています。
※組織内部での参考資料としてご活用ください。第三者への無断配布やネット上での再配布などは禁止しています。
※事例として掲載しているメールはすべて詐欺・詐称されたメールであり、実際の企業・団体のメールではありません。
　また、メールに記載されたURLにアクセスしたり、メールアドレスへの送信は絶対におやめください。

攻撃メールの現状

ランサムウェアを筆頭に、企業・組織に重大な被害をもたらす事案が多数発生しています

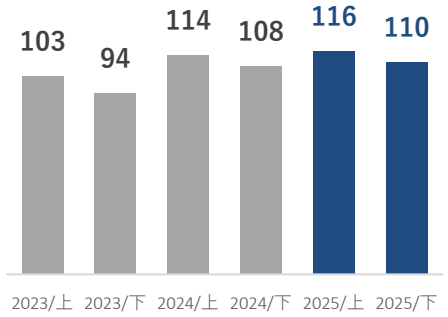
代表的なセキュリティ被害Top5とランサムウェア被害状況

IPAの10大脅威で1位のランサムウェアは、令和7年上半期の被害が過去最多水準で推移。RaaS普及により攻撃者層が広がり手口も巧妙化しています。中小企業の被害が顕著ですが、大企業が大きな被害を受けるケースも目立ちます。

- 1位 ランサムウェアによる被害
- 2位 サプライチェーンや委託先を狙った攻撃
- 3位 AIの利用をめぐるサイバーリスク
- 4位 システムの脆弱性を悪用した攻撃
- 5位 機密情報を狙った標的型攻撃

出典元：IPA独立行政法人情報処理推進機構 「情報セキュリティ10大脅威 2026」より

-ランサムウェア被害報告件数-

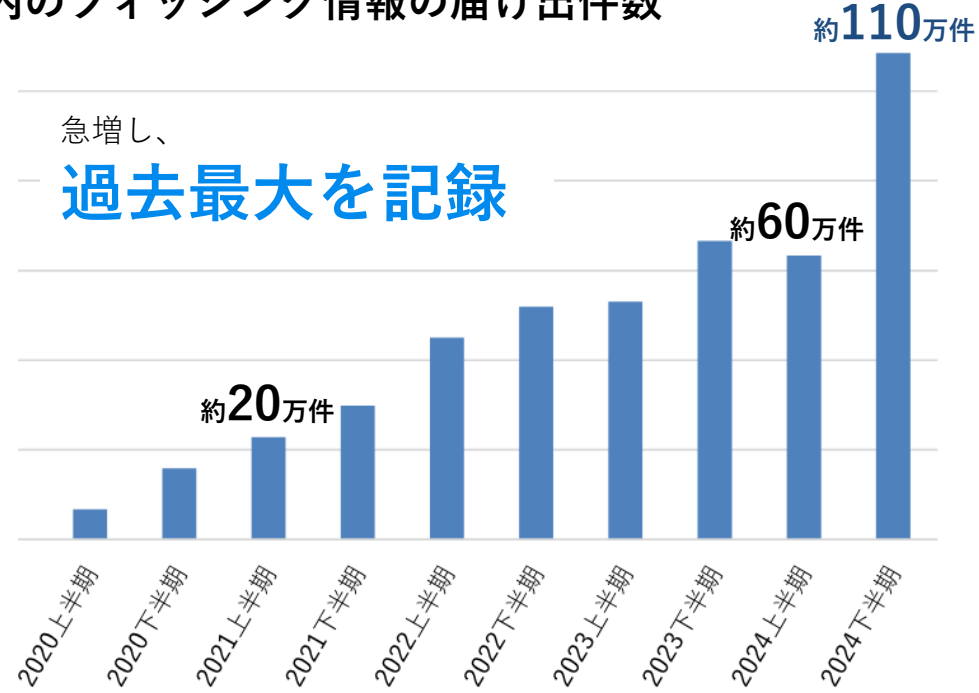


出典元：警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について」より

国内のフィッシング動向

【フィッシング協議会・フィッシングレポート2025】

国内のフィッシング情報の届け出件数



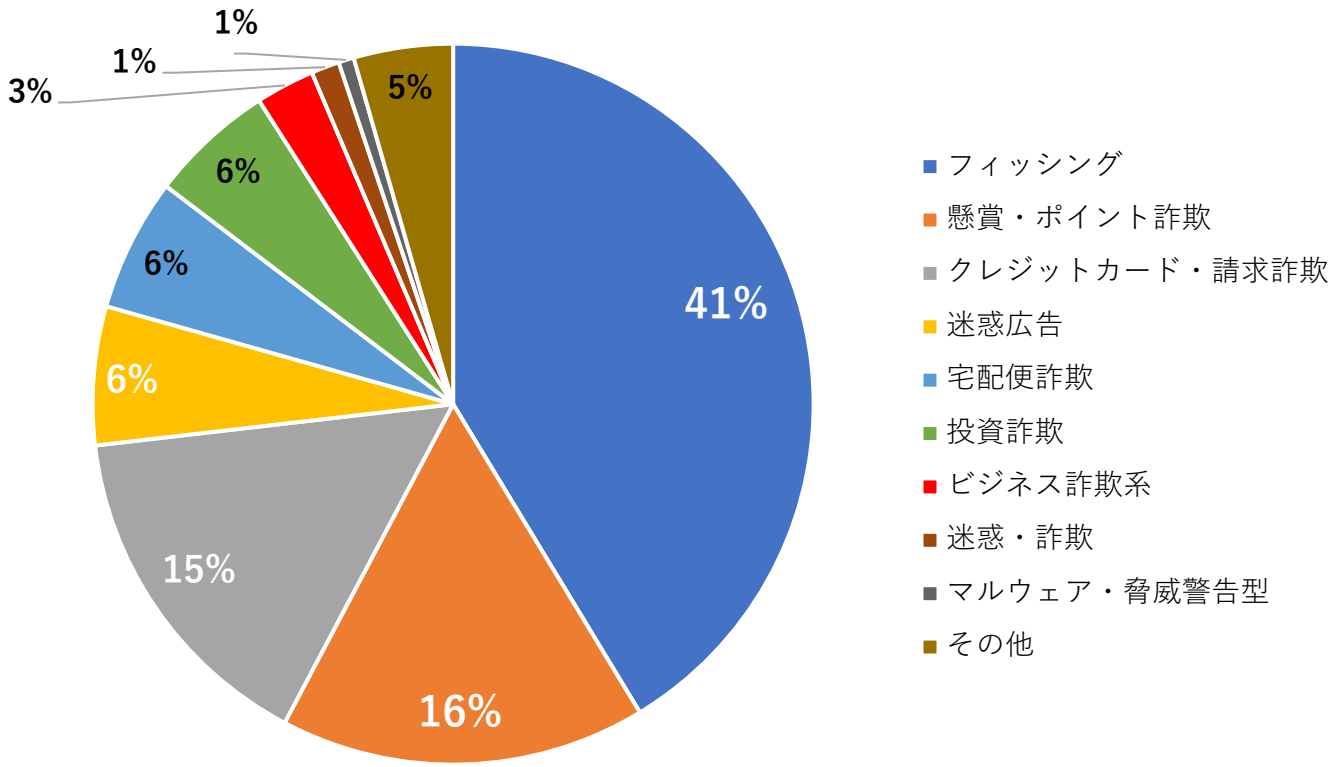
出典元：フィッシング協議会「フィッシングレポート2025」より

実際に届いた攻撃・迷惑メールの分析

有名企業・サービスを装う大量のメールと、緊急性をあおる標的型攻撃が同時に仕掛けられています

【2025年下半期：当社メールに実際に届いた攻撃・迷惑メールの件数】

	分類	件数
大量型	**フィッシング**（アカウント・認証）	**10,689**件
大量型	**懸賞・ポイント詐欺**	**4,243**件
大量型	**クレジットカード・請求詐欺**	**3,991**件
大量型	**偽広告**	**1,606**件
大量型	**宅配便詐欺**	**1,542**件
大量型	**投資詐欺**	**1,451**件
標的型	**ビジネス詐欺系**（なりすましなど標的型）	**682**件
大量型	**迷惑・詐欺**	**328**件
大量型	**マルウェア・脅威警告型**	**179**件
大量型	**その他**	**1,151**件
	合計	**25,862件**



・2025年9月～2025年12月まで、１つのアカウントに届いたメールを集計
・自社調べ／自社の専用アカウントに届いた実際のメールを計測。単なるPR・広告メールは省いています。

2025年の主な被害事例

アクモス 株式会社

メールなどをきっかけに発生したと考えられる、主な被害事例です。

Case.1

無線通信機器メーカー

被害内容

- 社員の**電子メールアカウントが乗っ取られ**、メール情報が窃取された。
- アカウントを悪用し、**顧客宛てに994通の標的型攻撃メールが送信**された。
- 窃取されたデータには、**個人情報**（会社名、氏名、電話・FAX番号、メールアドレス）や、**製品価格・契約内容**などの機密情報が含まれていた。

原因

2024年9月24日、社員が取引先からのメールを装った**フィッシングメールに記載されたURLにアクセスし、自身のIDとパスワードを入力してしまったこと**により、攻撃者にログイン情報を窃取されたことが原因だった。

影響

- 顧客や取引先の個人情報、契約内容などの**機密情報が漏えい**
- 被害アカウントの遮断、パスワード変更、社外アクセス制限を実行
- 標的型攻撃メールを受信した顧客への連絡・謝罪、個人情報保護委員会への報告、全従業員への注意喚起を実施

Case.2

私立大学

被害内容

- 大学のネットワークシステムの保守・管理を委託していた業者の**管理サーバが不正アクセスを受けた**
- **ランサムウェア攻撃**により、委託先サーバ内の一部ファイルが暗号化
- サーバに保存されていた大学の学生、保護者、教職員などの**個人情報を含むファイルが外部へ漏洩。システム停止**などの被害も拡大。

原因

攻撃者が**フィッシングメールで職員から窃取した管理者アカウントを悪用**。委託先のリモートメンテナンス環境から侵入したことに加え、委託先がルールに反して大学のデータを社内へ持ち帰っていたことや、大学側の委託先管理が不十分だったことが、個人情報漏洩の要因となった。

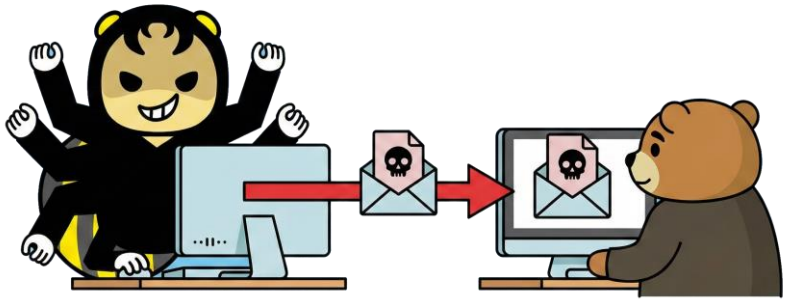
影響

個人情報漏えい：**保護者、役員・教職員など、約19万件以上**
停止アカウント：**約4万件以上**
システム、業務停止：**約3カ月**

メールによる攻撃手口

アクモス 株式会社

01 添付ファイル型



手口

- 実際のサービスや取引先を装い、添付ファイル付きメールを送信
- Word/Excelファイルなどを開かせ、悪意あるマクロを有効化させウイルス感染
- メールやPDFなどファイル内にリンクを貼り、悪意あるサイトへ誘導させたり、別の不正ファイルをダウンロードさせる

対策

- 「コンテンツの有効化」を押さない
- 不審なメールは確認を優先し、違和感があれば添付やURLは開かない
- メールやファイルに記載された指示に従わない（マルウェア実行の罠の可能性が高い）

02 フィッシング詐欺

手口

- 実在する組織を装ったメールやSMSでユーザーを信用させる
- 本物そっくりの偽サイトへ誘導し、認証情報やカード情報を入力させる
- 入力された情報を悪用し、金銭被害や不正利用につなげる

対策

- 送信元やリンク先URLを事前に確認する
- メール内のURLはクリックしない
- メール経由で開いたサイトでは認証情報を入力しない

メールによる攻撃手口

アクモス 株式会社

03 ビジネスメール詐欺（BEC）

被害内容

- 取引先を装い、偽口座へ送金させる
- 経営層になりすまし、緊急送金を指示する
- メール盗聴を悪用し、取引に紛れて詐欺を行う

対策

- 普段と違う送金依頼は、別手段で必ず確認する
- 多要素認証や電子署名で、なりすましを防ぐ
- 送金は複数名承認を必須とする

04 SMS・クイッシング詐欺

被害内容

- 実在する企業やサービスを装ったSMSに張り付けたQRコードで偽サイトへ誘導
- 緊急性や不安をあおる文面で読み取りを促す
- 偽サイトでIDやパスワード、クレジット情報を入力させて盗み取る

対策

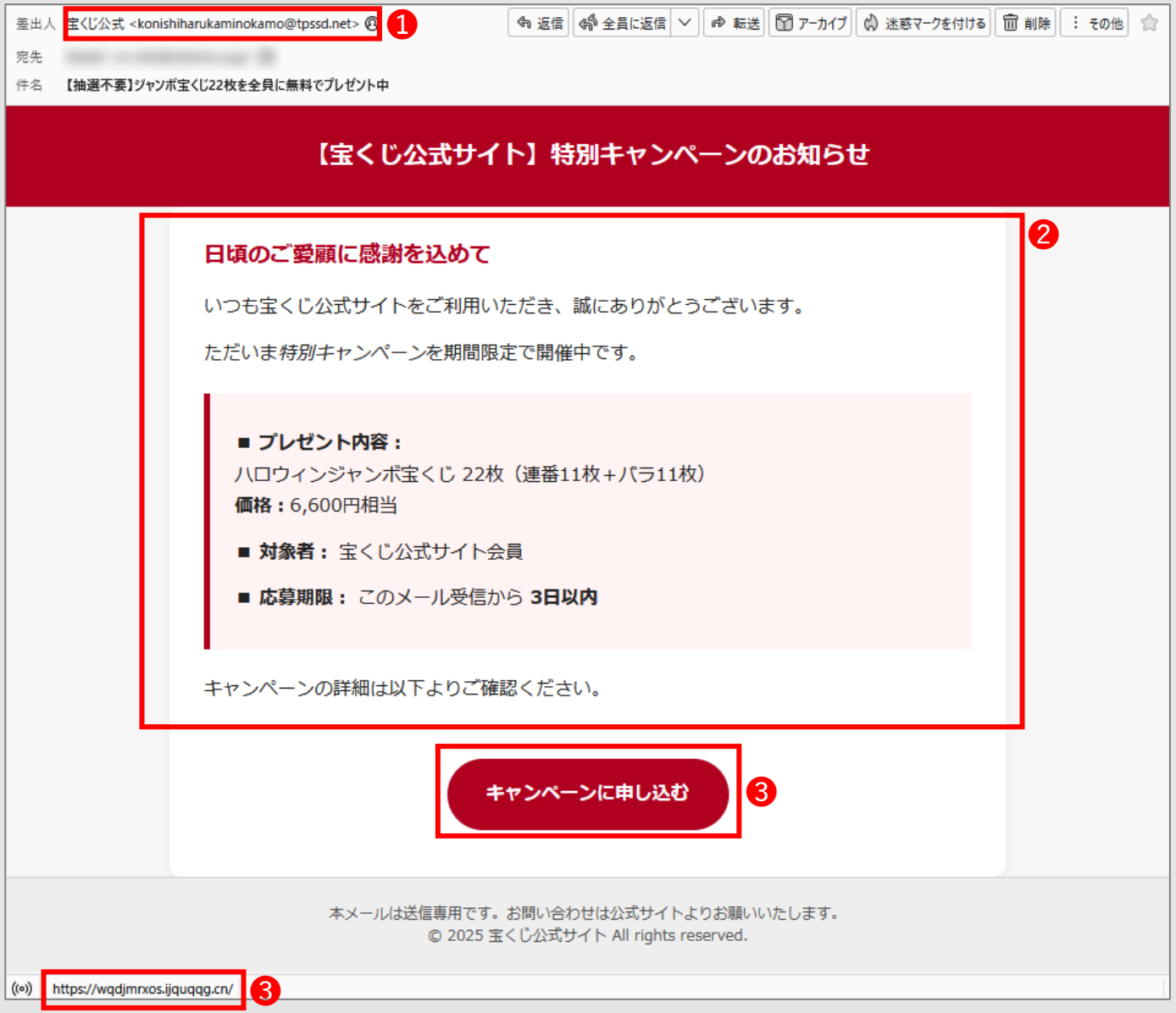
- SMS内のリンクは安易にクリックしない、QRコードも読み取らない
- 公式アプリやブックマークから直接アクセスする
- スマホの画面だけでなく、偽のQRコードシールや印刷物にも注意

実際に届いた
攻撃・詐欺・迷惑メール
事例８選

P.4でご紹介した実際に届いた約2.6万件の攻撃・詐欺・迷惑メールのなかから、８つの事例をご紹介します。

様々な形・切り口で送られてきますが、ある程度傾向や手口は似通っており、その見分け方も共通するため、事例を見て今後の防御や訓練のネタにしていただければ幸いです。

実際の攻撃・詐欺メール集 (1)



フィッシングメール

不審点

❶送信元

ドメインが公式や実在の組織と不一致

❷メール本文・構成の不審点

本文構成： 宛名・署名・連絡先など基本情報が不足

内容の不自然さ： 条件や業務内容の記載が曖昧

心理的な煽り： 短い期限や脅迫で不安を煽る

確認の阻害： 「返信不可」を強調し確認を妨害

信憑性の欠如： 証拠不足や説明の矛盾が存在

❸リンク先（URL）

URLが公式サイトとは無関係なドメイン

❹添付ファイル

ファイルの偽装： ファイル名などが不自然、ウイルスが存在

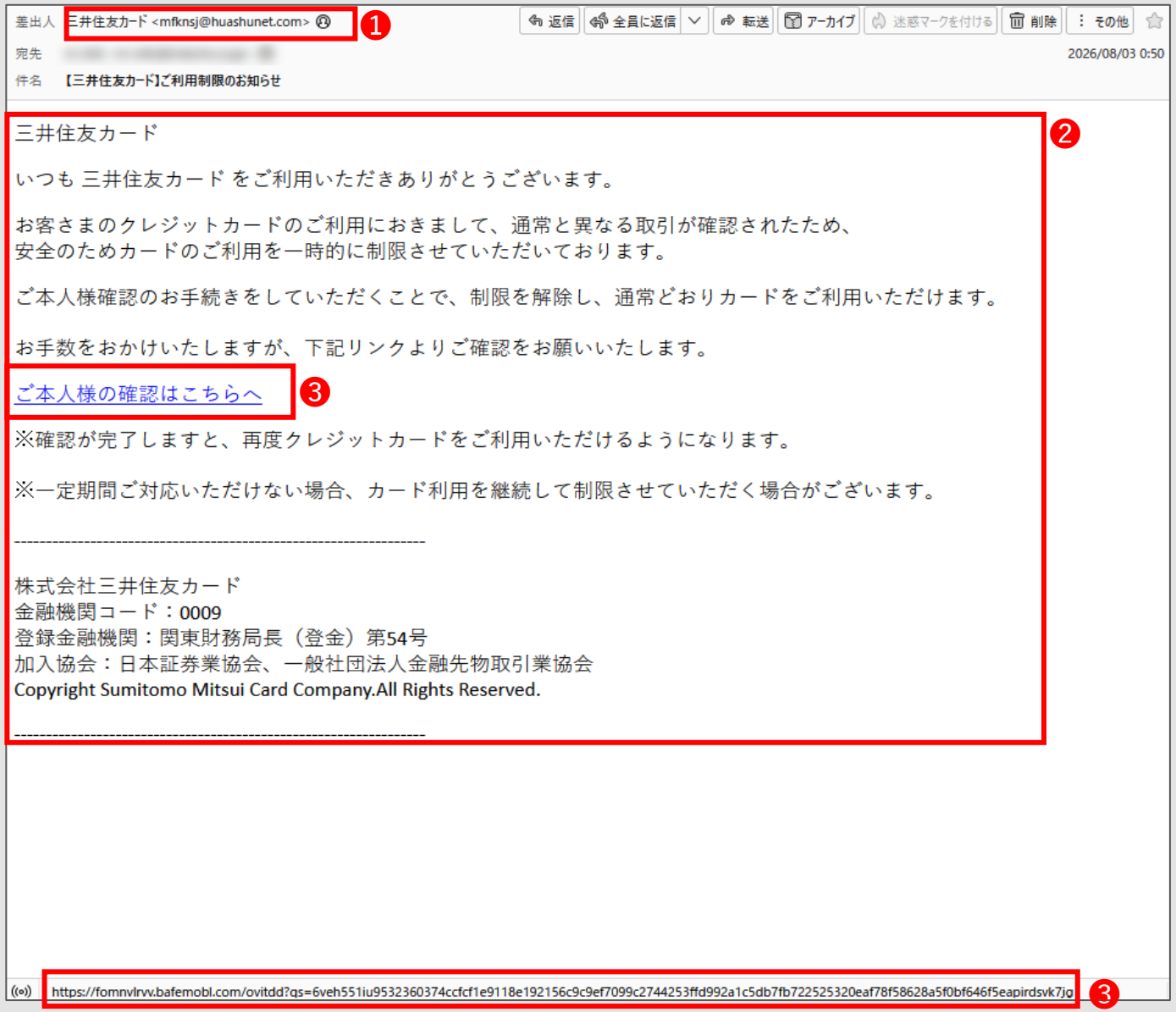
中身の不備： 実在組織を装った文書でも、不自然な誤りが存在

解説

宝くじ公式サイトを装い、会員に対して「ハロウィンジャンボ宝くじ22枚を無料でプレゼントする特別キャンペーン」への応募を促す内容の不審なメールです。

キャンペーンに申し込むボタンを押した先は、複数の**Webサイト安全性評価チェッカーで「危険・フィッシング」と表示**されました。

実際の攻撃・詐欺メール集 (2)



差出人 三井住友カード <mfknsj@huashunet.com> ❶
返信 | 全員に返信 | 転送 | アーカイブ | 迷惑マークを付ける | 削除 | その他
宛先
2026/08/03 0:50
件名 【三井住友カード】ご利用制限のお知らせ

❷

三井住友カード

いつも 三井住友カード をご利用いただきありがとうございます。

お客さまのクレジットカードのご利用におきまして、通常と異なる取引が確認されたため、
安全のためカードのご利用を一時的に制限させていただいております。

ご本人様確認のお手続きをしていただくことで、制限を解除し、通常どおりカードをご利用いただけます。

お手数をおかけいたしますが、下記リンクよりご確認をお願いいたします。

ご本人様の確認はこちらへ ❸

※確認が完了しますと、再度クレジットカードをご利用いただけるようになります。

※一定期間ご対応いただけない場合、カード利用を継続して制限させていただく場合がございます。

株式会社三井住友カード
金融機関コード：0009
登録金融機関：関東財務局長（登金）第54号
加入協会：日本証券業協会、一般社団法人金融先物取引業協会
Copyright Sumitomo Mitsui Card Company.All Rights Reserved.

---

https://fomnvlrvv.bafemobl.com/ovitdd?qs=6veh551iu9532360374ccfcf1e9118e192156c9c9ef7099c2744253ffd992a1c5db7fb722525320eaf78f58628a5f0bf646f5eapirdsvk7jg ❸

クレジットカード詐欺

不審点

❶送信元

ドメインが公式や実在の組織と不一致

❷メール本文・構成の不審点

本文構成： 宛名・署名・連絡先など基本情報が不足

内容の不自然さ： 条件や業務内容の記載が曖昧

心理的な煽り： 短い期限や脅迫で不安を煽る

確認の阻害： 「返信不可」を強調し確認を妨害

信憑性の欠如： 証拠不足や説明の矛盾が存在

❸リンク先（URL）

URLが公式サイトとは無関係なドメイン

❹添付ファイル

ファイルの偽装： ファイル名などが不自然、ウイルスが存在

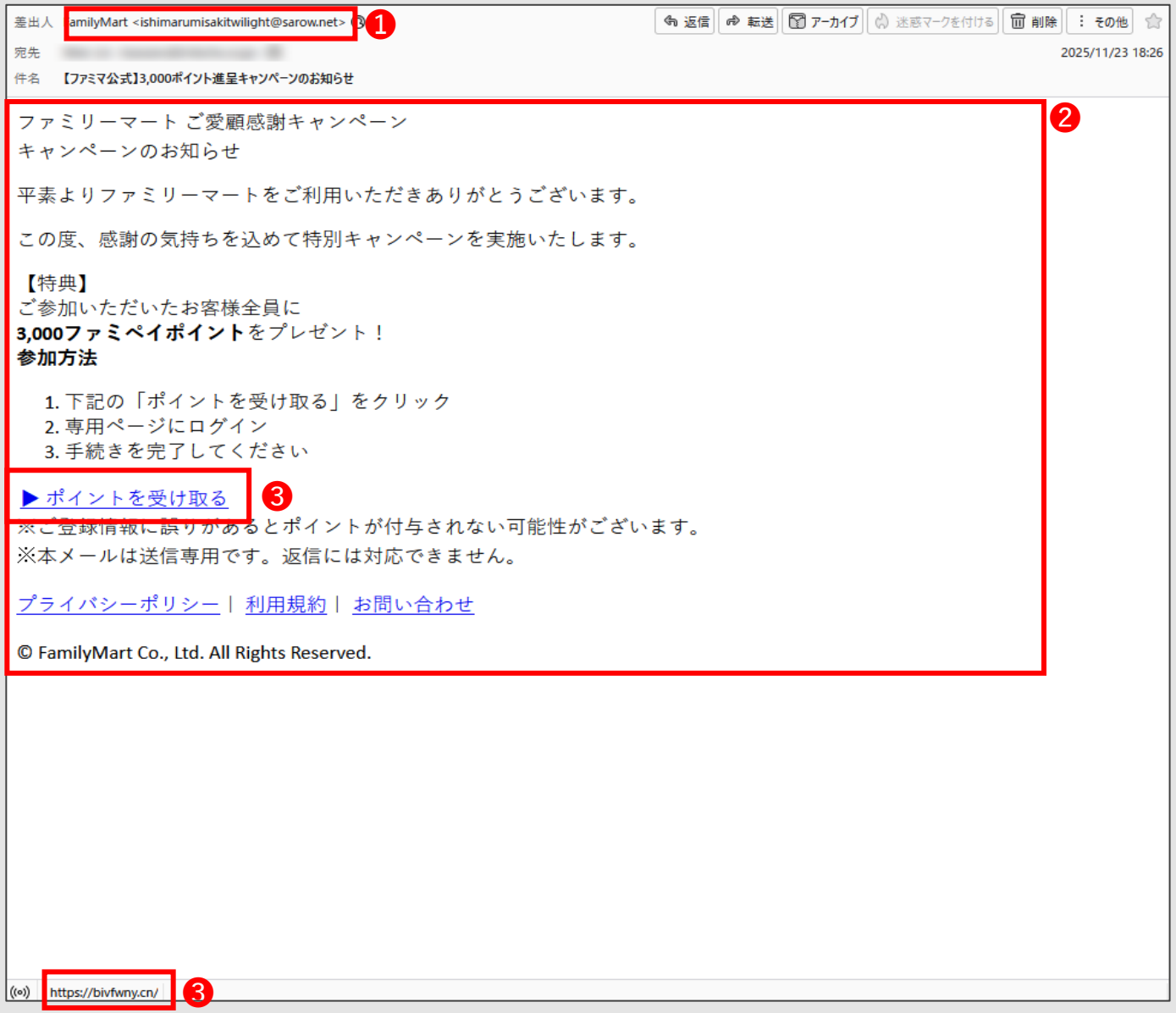
中身の不備： 実在組織を装った文書でも、不自然な誤りが存在

解説

三井住友カードを装い、不正利用を理由にカード利用を制限したとして、本人確認を名目に不審なリンクへ誘導するフィッシングメールです。

リンク先は、複数のWebサイト安全性評価チェッカーで「危険・フィッシング」と表示されました。

実際の攻撃・詐欺メール集 (3)



差出人 amilyMart <ishimarumisakitwilight@sarow.net> ❶
返信 転送 アーカイブ 迷惑マークを付ける 削除 その他
宛先
2025/11/23 18:26
件名 【ファミマ公式】3,000ポイント進呈キャンペーンのお知らせ

❷

ファミリーマート ご愛顧感謝キャンペーン
キャンペーンのお知らせ

平素よりファミリーマートをご利用いただきありがとうございます。

この度、感謝の気持ちを込めて特別キャンペーンを実施いたします。

【特典】
ご参加いただいたお客様全員に
3,000ファミペイポイントをプレゼント！
参加方法

1. 下記の「ポイントを受け取る」をクリック
2. 専用ページにログイン
3. 手続きを完了してください

▶ ポイントを受け取る ❸
※ご登録情報に誤りがあるとポイントが付与されない可能性がございます。
※本メールは送信専用です。返信には対応できません。

プライバシーポリシー | 利用規約 | お問い合わせ

© FamilyMart Co., Ltd. All Rights Reserved.

https://bivfwny.cn/ ❸

ポイント・キャンペーン詐欺

不審点

❶送信元

ドメインが公式や実在の組織と不一致

❷メール本文・構成の不審点

本文構成： 宛名・署名・連絡先など基本情報が不足

内容の不自然さ： 条件や業務内容の記載が曖昧

心理的な煽り： 短い期限や脅迫で不安を煽る

確認の阻害： 「返信不可」を強調し確認を妨害

信憑性の欠如： 証拠不足や説明の矛盾が存在

❸リンク先（URL）

URLが公式サイトとは無関係なドメイン

❹添付ファイル

ファイルの偽装： ファイル名などが不自然、ウイルスが存在

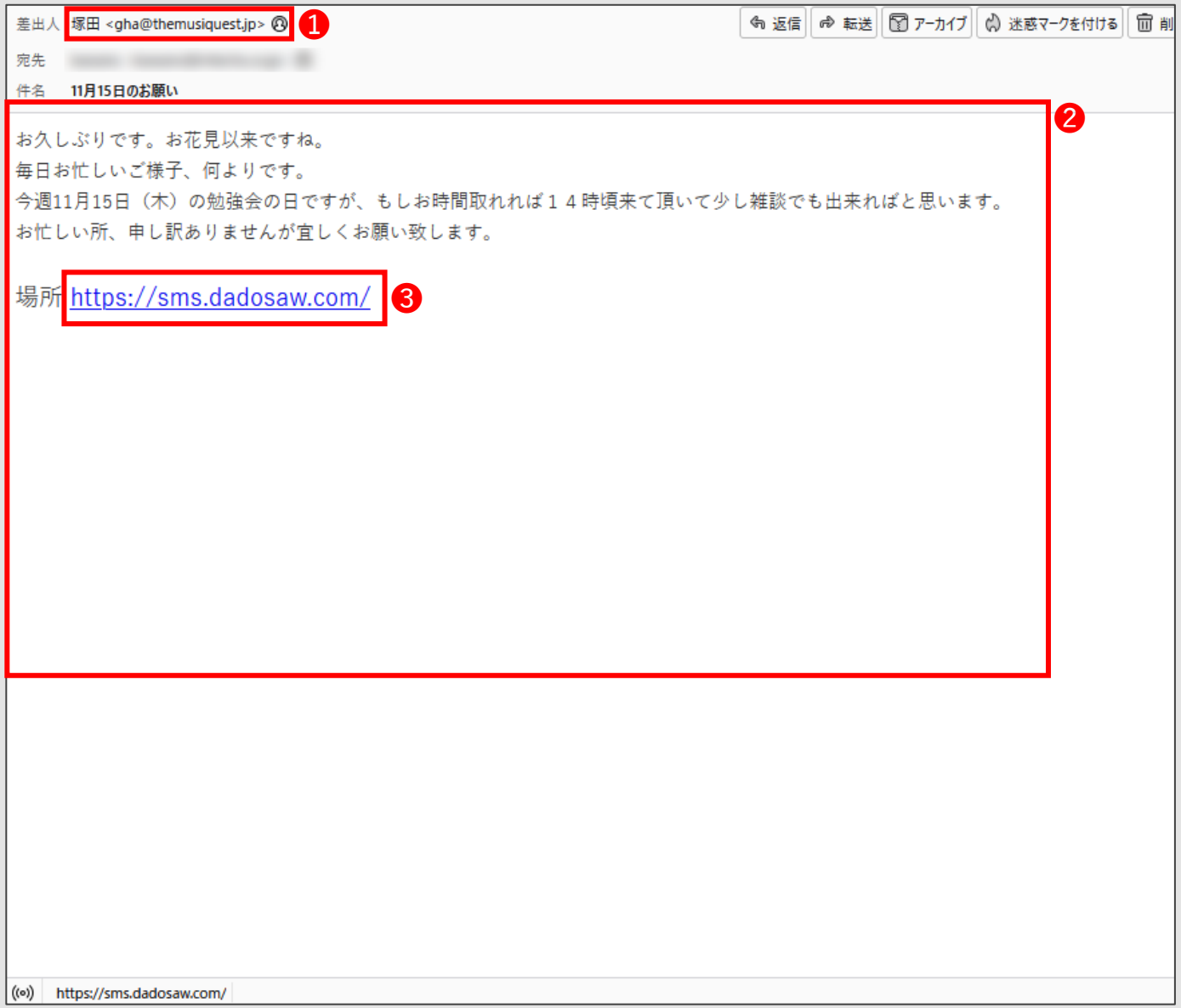
中身の不備： 実在組織を装った文書でも、不自然な誤りが存在

解説

コンビニのサービスを装い、3,000ポイントがもらえる特別キャンペーンへの参加を名目に不審なリンクへログインさせようとするフィッシングメールです。

リンク先は、複数の**Webサイト安全性評価チェッカーで「危険・フィッシング」と表示**されました。

実際の攻撃・詐欺メール集 (4)



詐欺メール

不審点

❶送信元

ドメイン・組織は実在するが、内容とは合わず不自然

❷メール本文・構成の不審点

本文構成： 宛名・署名・連絡先など基本情報が不足

内容の不自然さ： 条件や業務内容の記載が曖昧

心理的な煽り： 短い期限や脅迫で不安を煽る

確認の阻害： 「返信不可」を強調し確認を妨害

信憑性の欠如： 証拠不足や説明の矛盾が存在

❸リンク先（URL）

URL先は不審な情報詐取サイト

❹添付ファイル

ファイルの偽装：ファイル名などが不自然、ウイルスが存在

中身の不備：実在組織を装った文書でも、不自然な誤りが存在

解説

知人を装って勉強会への参加を依頼し、詳細確認のために不審な外部リンクへ誘導する内容で、個人宛を装ったメールです。

リンク先は、複数の**Webサイト安全性評価チェッカーで「危険・フィッシング」と表示**された、海外の情報詐取サイトです。

実際の攻撃・詐欺メール集 (5)

差出人 immunologiedd@freesulf.de ❶
宛先
件名 口座からのお支払い
返信 転送 アーカイブ 迷惑マークを付ける 削除 その他
2025/11/15 1:35

❷

初めまして！

残念なお知らせをするために、ご連絡を差し上げております。
僕は、約２～３ヶ月前にネット閲覧用に貴方が利用しているデバイスにアクセスし、その後ずっとネット行動を追跡していました。

アクセスするまでの経緯は、
少し前にハッカーからメールアカウントへのアクセスを購入したからです（最近では、そういったものをネット上で購入するのは、かなり単純です）。
だから、貴方のメールアカウント（[redacted]）にも簡単にログインができました。

ログインの１週間後には、既にトロイの木馬というマルウェアを、貴方のメールと繋がっている全てのデバイスのオペレーティングシステムにインストールしました。
実際、やってみると全く難しくありませんでしたよ。（受信トレイのメールのリンクを何も問題なくたどっていただき、ありがとうございました。）
巧妙な手口は意外と全て単純なのです。(^ ^)

そのソフトウェアによって、貴方のデバイスの操作を全て可能になりました（例えば、マイク、ビデオカメラ、キーボードの操作）。
既に、貴方の個人情報、データ、写真、ウェブ閲覧履歴を僕のサーバーにダウンロードし保存してあります。
貴方のメッセンジャー&# 12289;SNS、メール、チャット履歴、連絡先一覧の全てにも僕はアクセス済みです。
僕のウイルスはドライバレベルで動作し署名を継続的に更新するため、ウイルス対策ソフトウェアでは検知されません。

同様に、この手紙がなぜウイルス対策のソフトウェアに検出されなかったのかの理由も、今ではご理解いただけていると思います・・・

貴方の情報を収集している間に、貴方はアダルトサイトの大ファンだということを発見しました。
ポルノサイトを訪問して、とてつもない快楽に耐えながら、興奮するような動画を閲覧するのが本当にお好きなようですね。
偶然にも、貴方の卑猥なシーンを録画することに成功したので、貴方の自慰行為と絶頂に達する姿を見せるような動画数本をモンタージュにしました。

もし嘘だと思うのであれば、僕のマウスを数回クリックするだけで、全ての動画が貴方の友人、同僚や親戚とシェアできることを実現

セクストーション（偽）

不審点

❶送信元

ドイツの無料または適当なドメインを使用

❷メール本文・構成の不審点

本文構成： 宛名・署名・連絡先など基本情報が不足

内容の不自然さ： 条件や業務内容の記載が曖昧

心理的な煽り： 短い期限や脅迫で不安を煽る

確認の阻害： 「返信不可」を強調し確認を妨害

信憑性の欠如： 証拠不足や説明の矛盾が存在

❸リンク先（URL）

URL先は不審な情報詐取サイト

❹添付ファイル

ファイルの偽装：ファイル名などが不自然、ウイルスが存在

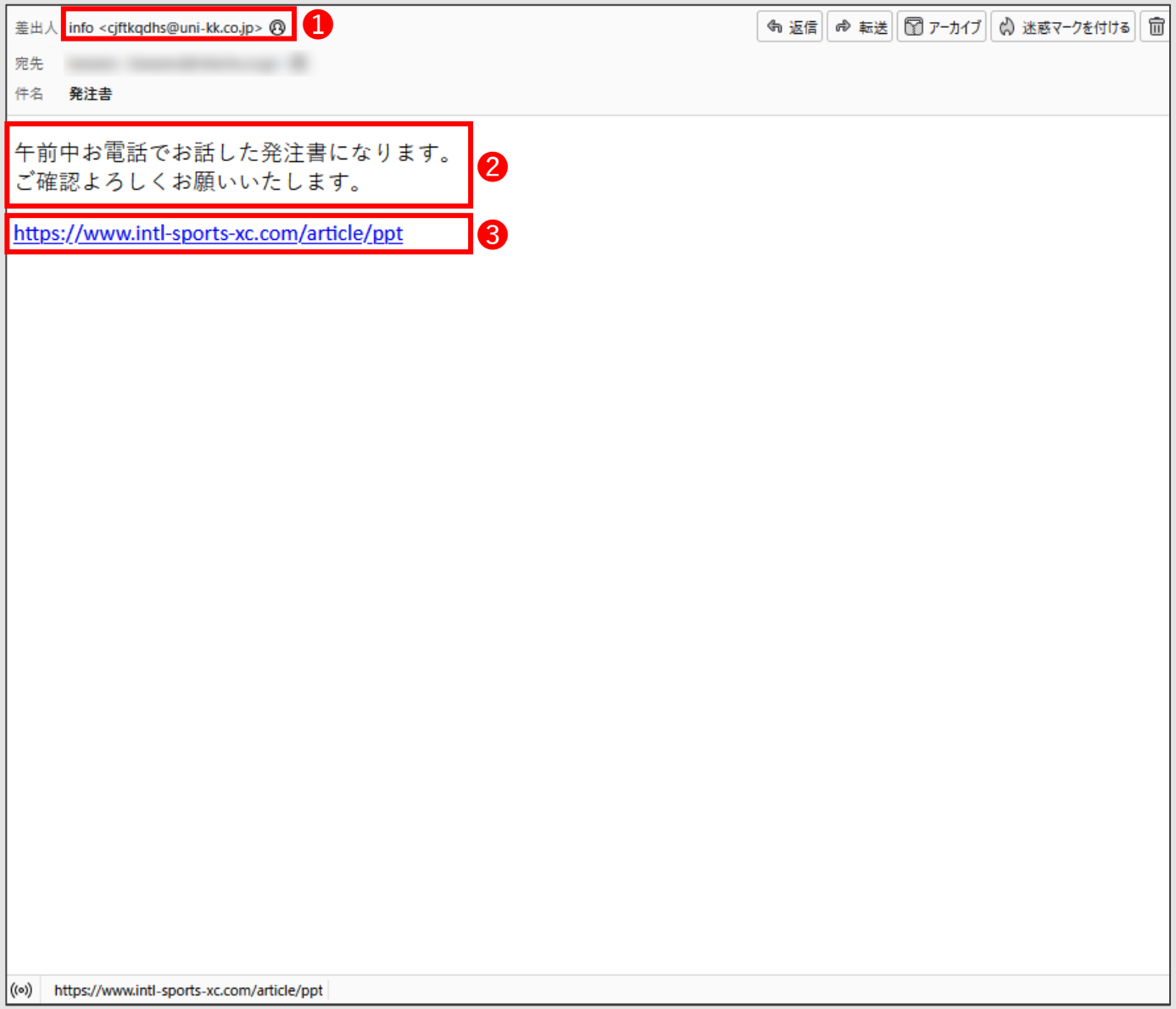
中身の不備：実在組織を装った文書でも、不自然な誤りが存在

解説

このメールは、あなたのデバイスをハッキングして恥ずかしい動画を撮影したと嘘をつき、その**拡散を盾に金銭を要求する「セクストーション（性的脅迫）」と呼ばれる典型的な迷惑メール（スパム）**。基本的にすべてウソの内容であり、間違っても連絡をしたり、金銭を振り込んではいけません。

※本当にカメラを乗っ取り撮影したものを送り付ける脅迫メールも存在します

実際の攻撃・詐欺メール集 (6)



ビジネス詐欺

不審点

❶送信元

ドメインがランダムな文字列になっており不自然

❷メール本文・構成の不審点

本文構成： 宛名・署名・連絡先など基本情報が不足

内容の不自然さ： 条件や業務内容の記載が曖昧

心理的な煽り： 短い期限や脅迫で不安を煽る

確認の阻害： 「返信不可」を強調し確認を妨害

信憑性の欠如： 証拠不足や説明の矛盾が存在

❸リンク先（URL）

URL先は不審な情報詐取サイト

❹添付ファイル

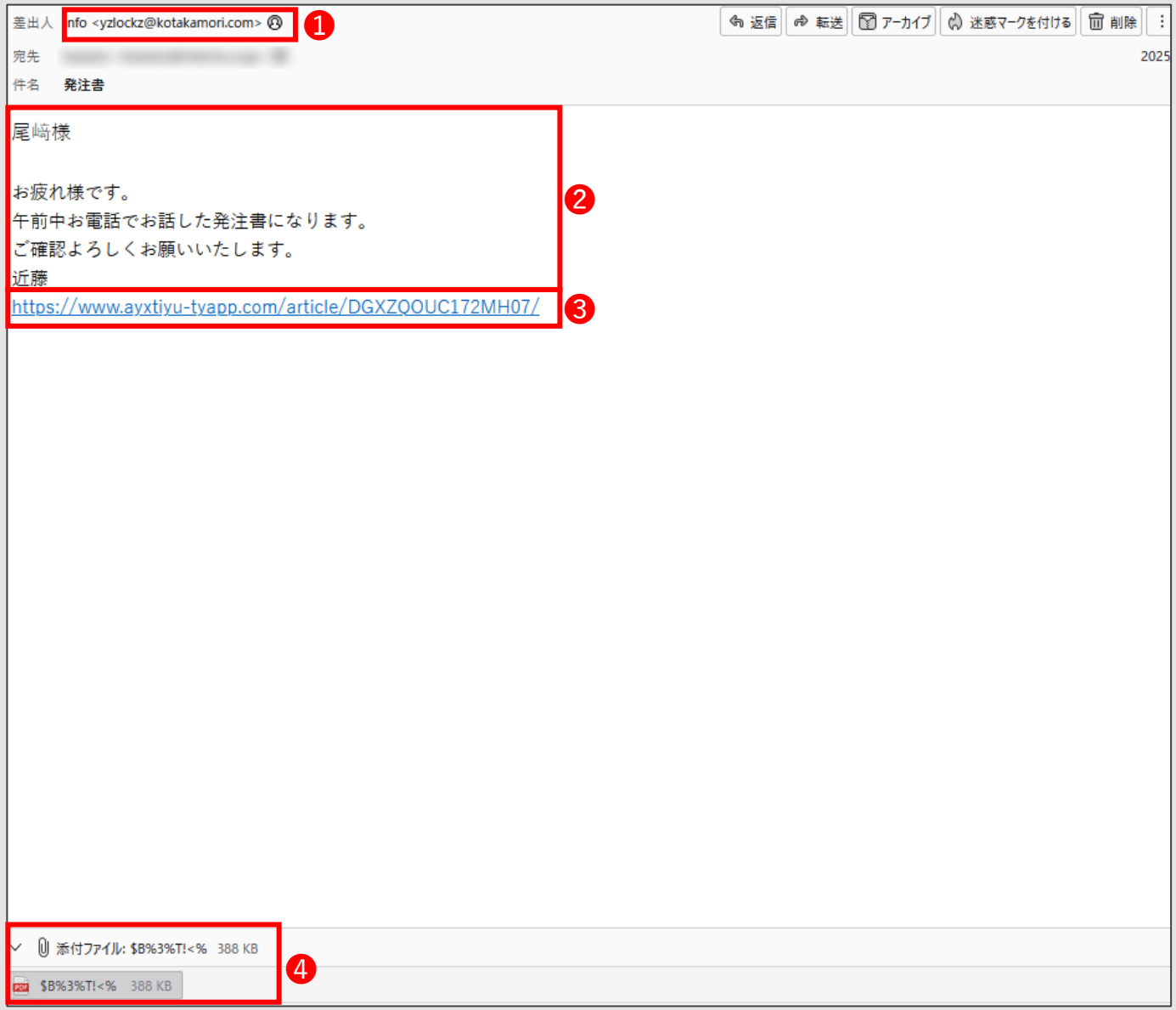
ファイルの偽装：ファイル名などが不自然、ウイルスが存在

中身の不備：実在組織を装った文書でも、不自然な誤りが存在

解説

心当たりのない「電話での約束」を口実にして、リンクをクリックさせてウイルスに感染させたり個人情報を盗もうとしたりする、典型的ななりすまし詐欺（フィッシング）メールです。リンク先は米国のサーバーに設置されたサイトで、複数のWebサイト安全性評価チェッカーで「危険・フィッシング」と表示されました。

実際の攻撃・詐欺メール集 (7)-1



ビジネス詐欺

不審点

❶送信元

アドレス名がランダムな文字列になっており不自然

❷メール本文・構成の不審点

本文構成： 宛名・署名・連絡先など基本情報が不足

内容の不自然さ： 条件や業務内容の記載が曖昧

心理的な煽り： 短い期限や脅迫で不安を煽る

確認の阻害： 「返信不可」を強調し確認を妨害

信憑性の欠如： 証拠不足や説明の矛盾が存在

❸リンク先（URL）

URL先は不審な情報詐取サイト

❹添付ファイル

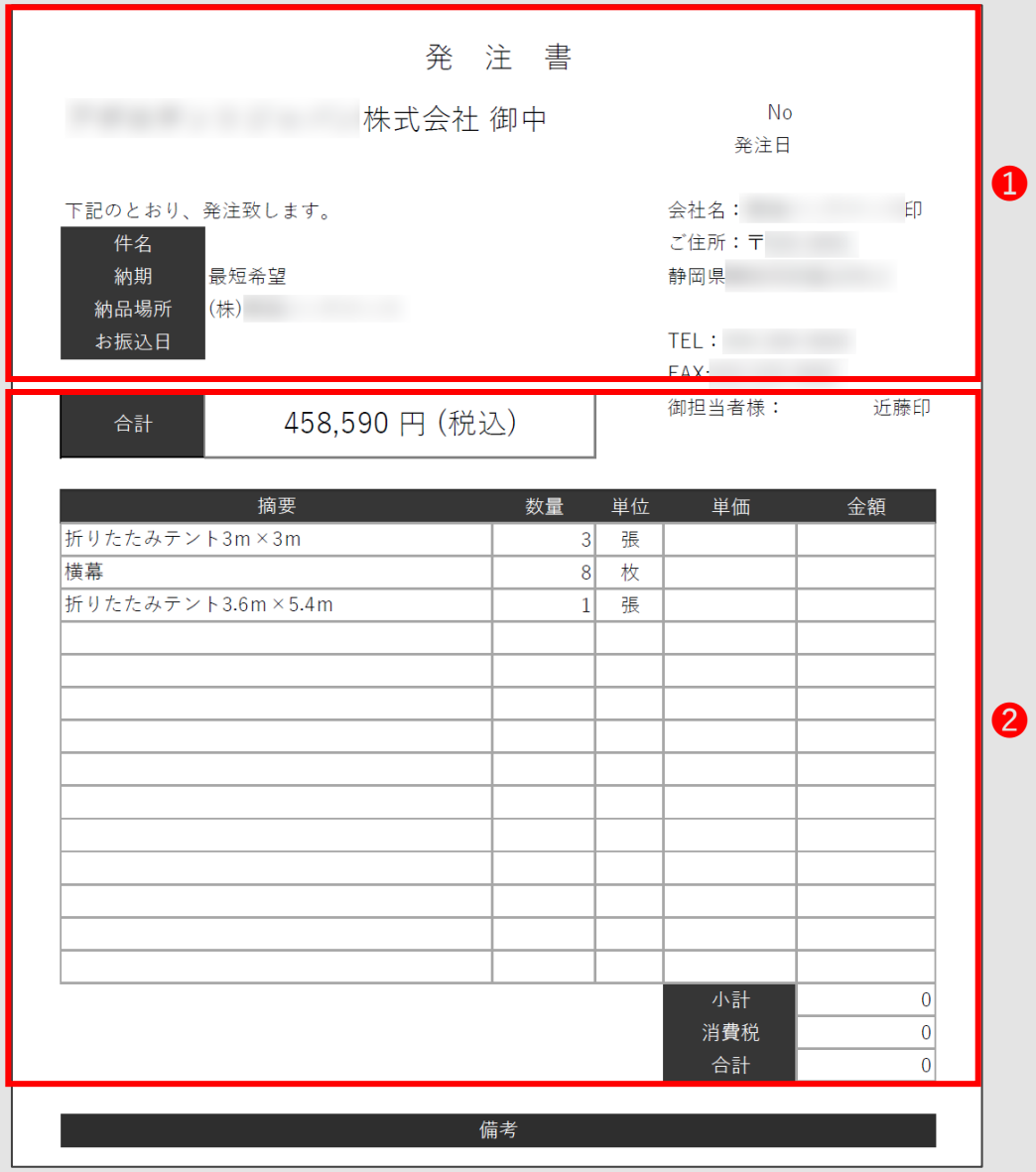
ファイルの偽装：ファイル名などが不自然、ウイルスが存在

中身の不備：実在組織を装った文書でも、不自然な誤りが存在

解説

実在する組織や担当者を装い「電話で話した発注書」という嘘の口実で、ウイルス感染や情報窃取を目的とした有害なリンクや添付ファイルを開かせようとする詐欺メール。URL先はフィッシングサイトであるほか、添付のPDFファイルは偽物の発注書です（次ページで解説）。

実際の攻撃・詐欺メール集 (7)-2



発　注　書

[redacted]株式会社 御中

No
発注日

下記のとおり、発注致します。

件名	
納期	最短希望
納品場所	(株)[redacted]
お振込日	

会社名：[redacted]印
ご住所：〒[redacted]
静岡県[redacted]
TEL：[redacted]
FAX：[redacted]
御担当者様：　近藤印

合計	458,590 円 (税込)

摘要	数量	単位	単価	金額
折りたたみテント3m×3m	3	張		
横幕	8	枚		
折りたたみテント3.6m×5.4m	1	張		

小計	0
消費税	0
合計	0

備考

❶

❷

ビジネス詐欺/(7)の添付ファイルの中身

不審点

❶実在の組織名などを使用

記載されている住所や電話番号などは、すべて実在する企業の情報が使用されている。ただ、送信元メールアドレスのドメインがまったく別のものであるため、実在する企業を騙った「なりすまし」の発注書。

❷不自然な内容

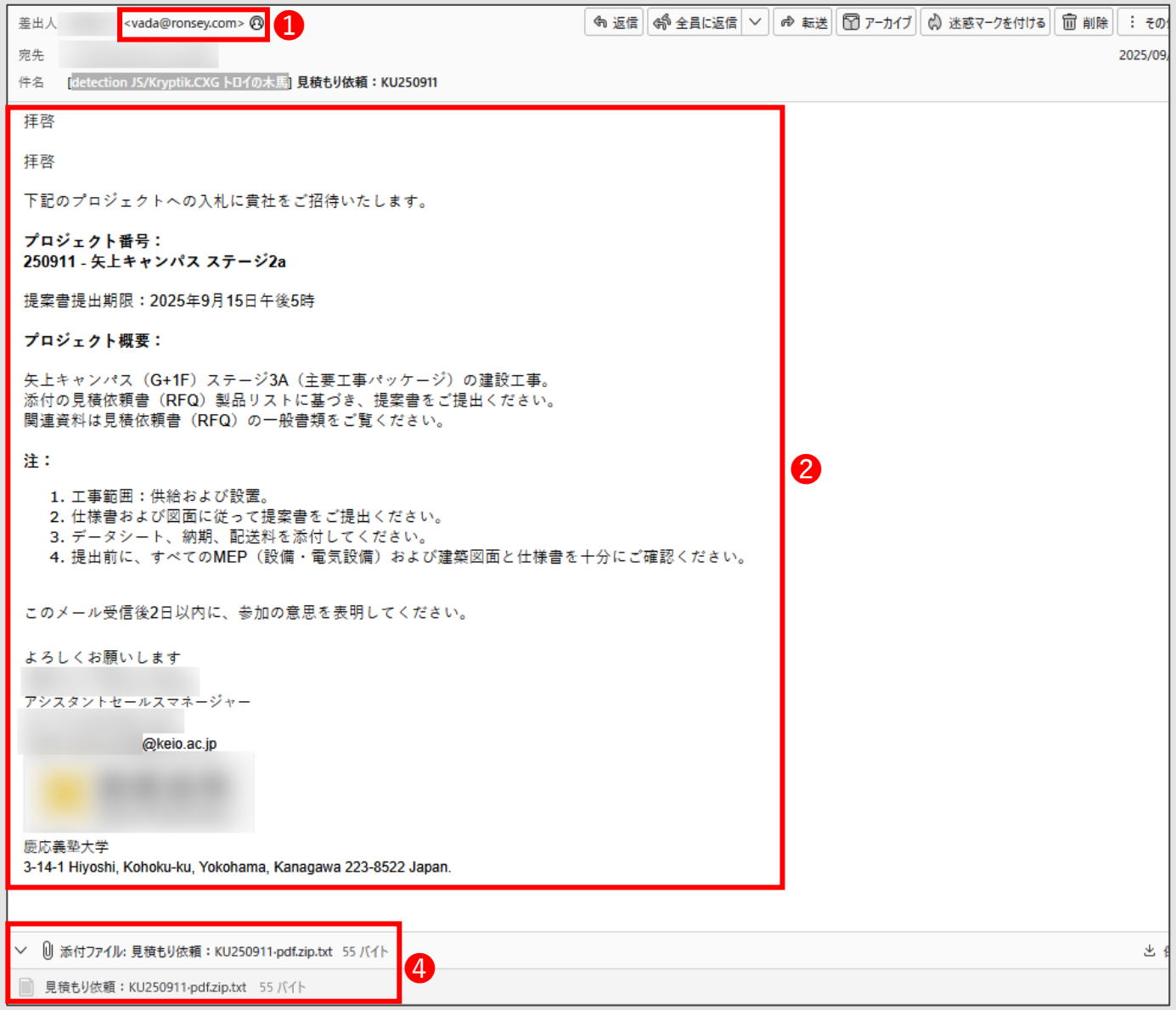
PDF内の合計金額は「458,590円(税込)」と記載。

しかし、明細テーブル内の「小計」「消費税」「合計」はすべて「0」となっており、計算が全く合ってない。

解説

実在する会社名・住所・電話番号を使用し、あたかも本物の発注書であるかのように作り込まれています。不特定多数に送信されていれば取引先ではないため不自然だと気づきやすいものの、仮に実在する取引先を装ったピンポイントの標的型攻撃であった場合、信用してしまい被害に遭う可能性が高くなります。

実際の攻撃・詐欺メール集 (8)


差出人 <vada@ronsey.com> ❶
返信 | 全員に返信 | 転送 | アーカイブ | 迷惑マークを付ける | 削除
宛先
2025/09/
件名 [detection JS/Kryptik.CXG トロイの木馬] 見積もり依頼：KU250911

拝啓

拝啓

下記のプロジェクトへの入札に貴社をご招待いたします。

プロジェクト番号：
250911 - 矢上キャンパス ステージ2a

提案書提出期限：2025年9月15日午後5時

プロジェクト概要：

矢上キャンパス（G+1F）ステージ3A（主要工事パッケージ）の建設工事。
添付の見積依頼書（RFQ）製品リストに基づき、提案書をご提出ください。
関連資料は見積依頼書（RFQ）の一般書類をご覧ください。

注：

1. 工事範囲：供給および設置。
2. 仕様書および図面に従って提案書をご提出ください。
3. データシート、納期、配送料を添付してください。
4. 提出前に、すべてのMEP（設備・電気設備）および建築図面と仕様書を十分にご確認ください。

❷

このメール受信後2日以内に、参加の意思を表明してください。

よろしくお願いします

アシスタントセールスマネージャー

@keio.ac.jp

慶応義塾大学
3-14-1 Hiyoshi, Kohoku-ku, Yokohama, Kanagawa 223-8522 Japan.

添付ファイル: 見積もり依頼：KU250911-pdf.zip.txt 55 バイト
❹
見積もり依頼：KU250911-pdf.zip.txt 55 バイト

ビジネス詐欺

不審点

❶送信元

送信元と署名メールアドレスの不一致

❷メール本文・構成の不審点

本文構成： 宛名・署名・連絡先など基本情報が不足

内容の不自然さ： 条件や業務内容の記載が曖昧

心理的な煽り： 短い期限や脅迫で不安を煽る

確認の阻害： 「返信不可」を強調し確認を妨害

信憑性の欠如： 証拠不足や説明の矛盾が存在

❸リンク先（URL）

URL先は不審な情報詐取サイト

❹添付ファイル

ファイルの偽装：ファイル名などが不自然、ウイルスが存在

中身の不備：実在組織を装った文書でも、不自然な誤りが存在

解説

実在の組織や「電話での約束」を装い、不自然なリンクやマルウェアの疑いがある添付ファイルを開かせてウイルス感染や情報窃取を狙う、典型的な標的型攻撃（ビジネスメール詐欺）です。**添付ファイルにはウイルスが仕込まれており**、ウイルス対策ソフトによって駆除されています。

攻撃・詐欺メールに対する基本対策と対応

内容を確認する

- 送信元のチェック
- 文章や内容の不審点
- リンク先のURLをプレビュー確認
- メッセージソースの確認

安易に操作しない

- URLリンクはクリックせず、正規のサイトやアプリからログインする
- 怪しい添付ファイルは開いたり、実行しない

偽サイトを開いた場合

- IDやパスワード、クレジットカード情報を入力しない
- 入力する前にWebサイト安全性チェッカーなどで確認する

入力・添付を開いた場合

- すぐにパスワードを変えたり、クレジットカードを止めるなどの対応
- PCをネットワークから切断し、すぐにシステム担当に報告

アクモスの会社概要

私たちは輝くICTサービスで 社会の向上に貢献します

確かな開発基盤・技術力

企業の業務システム、自治体のITソリューション、宇宙関連システムなど、重要な社会・情報インフラを支えるシステムを手掛けています。

安心できる開発・サービス提供環境

情報セキュリティマネジメントの国際規格「JISQ27001:2014」やプライバシーマークなど取得済みです。

信頼性と透明性が高い企業運営

東証スタンダード市場に上場。IR情報の公開やコーポレートガバナンスの整備により、信頼性抜群の企業運営に努めています。

商号	**アクモス株式会社** 東証スタンダード市場（証券コード：6888）
設立	1991年8月23日
資本金	6億9,325万円
代表	代表取締役社長 兼 COO　清川　明宏
社員数	308名(単体) ／ 490名(連結)　2025年6月現在
事業内容	ITソリューションサービス（IT基盤・構築・SI・運用・保守） グループ事業マネジメント
本社(本店)所在地	東京都港区虎ノ門1-21-19 東急虎ノ門ビル8F
その他事業所	茨城本部・茨城開発センター・つくばオフィス
取得認証	QMS（JIS Q9001:2015） プライバシーマーク（JIS Q15001:2023） ISMS（JIS Q27001:2023）
加盟団体	サイバーセキュリティ協議会 / 一般社団法人 高度ITアーキテクト育成協議会 一般社団法人 日本情報システム・ユーザー協会 一般社団法人 茨城県情報サービス産業協会 / 茨城県高度情報化推進協議会 茨城県情報通信ネットワークセキュリティ協議会
ホームページ	https://www.acmos.co.jp

詳細はお気軽にお問い合わせください。

無料体験プランもお申し込み受付中です！

お問い合わせ先

アクモス株式会社 営業本部　首都圏営業部

東京都港区虎ノ門1-21-19 東急虎ノ門ビル8F
TEL：03-5539-6480
E-Mail：acmos-sales-support@acmos.jp

https://cloud-srv.acmos.co.jp/

サービスサイトはこちら