不審メールがもたらす脅威

KIS Security株式会社

（2026年4月）

電子メールが使われる主なサイバーセキュリティ攻撃

KIS SECURITY

✓フィッシング攻撃

フィッシング詐欺とは、金融機関などの有名企業を詐称したメールを送り付け、本文のURLをクリックさせることで偽サイトに誘導し、不正にIDとパスワードなどを詐取する詐欺行為のこと。

✓スパムメール攻撃

スパムとは、受信者の意図とは関係なく、大量に配信されるメッセージのこと。

✓マルウェアによる攻撃

マルウェア（malware）とは、悪意のある（malicious）ソフトウェア（software）を合わせた造語で、感染対象に対して有害な作用をもたらすことを目的に作成されたソフトウェアの総称である。

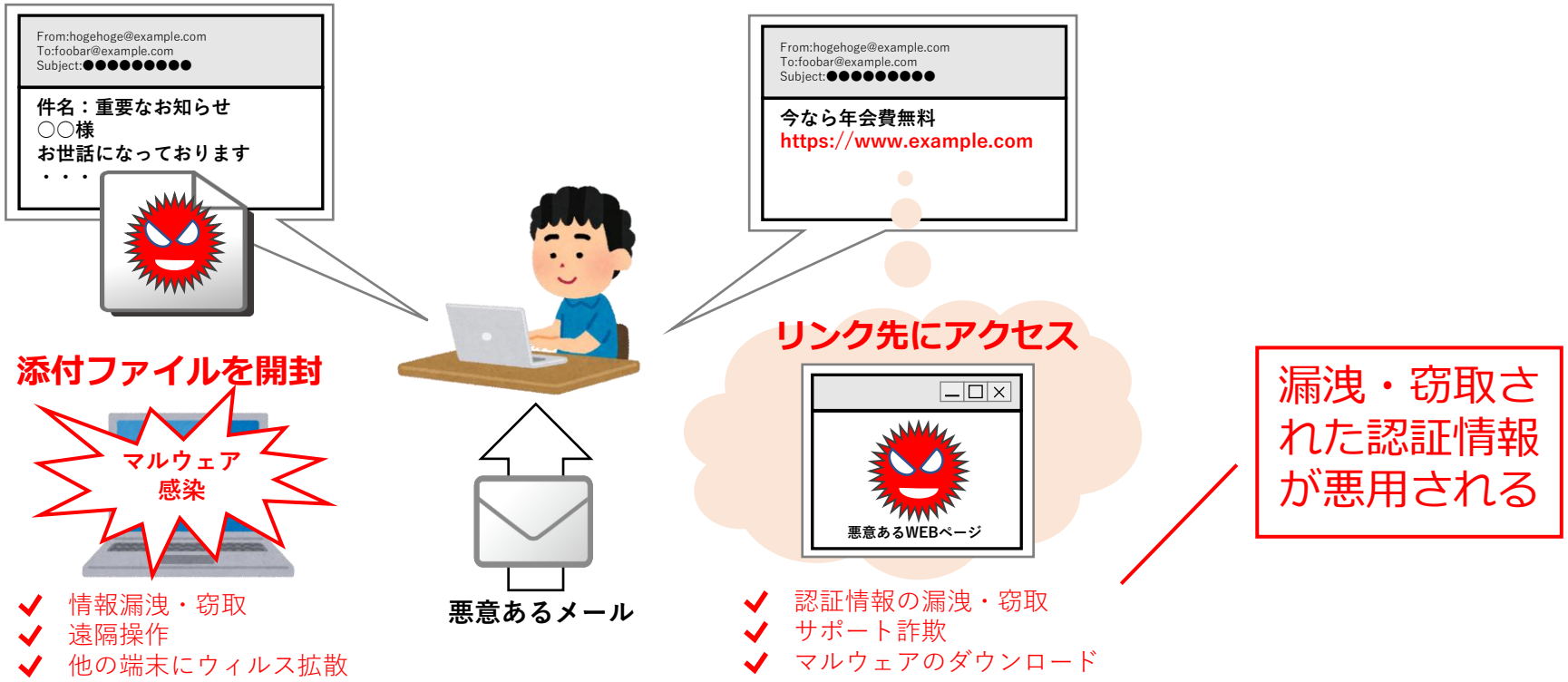
✓標的型攻撃メール

標的型攻撃メール攻撃とは、不特定多数の対象にばらまかれる通常の迷惑メールとは異なり、対象の組織から重要な情報を盗むことなどを目的として、巧妙に作り込まれたウイルス付きのメールのこと。また、メールに記載のURLから悪意あるWebサイトへ誘導し、マルウェアに感染させる場合もある。

電子メールによるサイバー攻撃例

KIS SECURITY

- 電子メールによるマルウェア感染
- 電子メールのリンク先でマルウェア感染、認証情報が窃取



認証情報、個人情報を窃取する
フィッシングメール

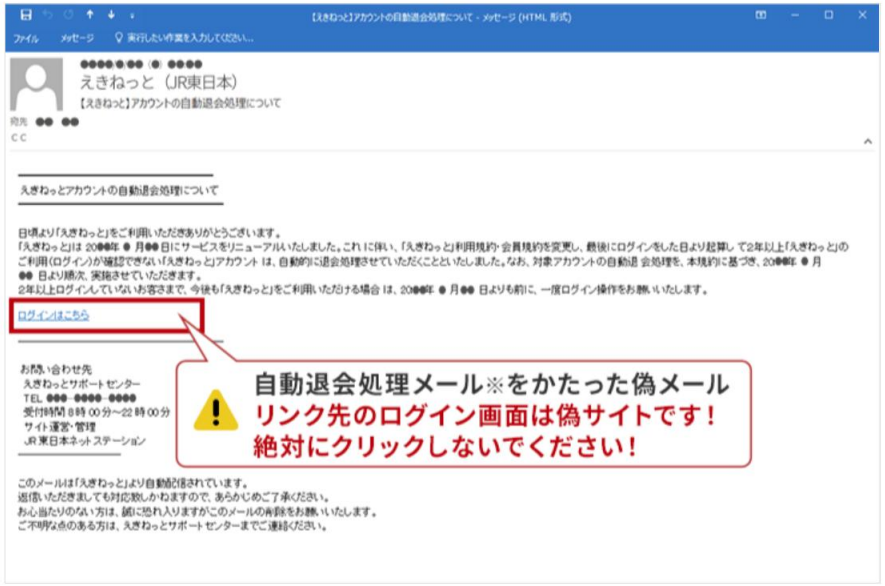
某交通機関のサイトを「騙ったフィッシング

KIS SECURITY

自動退会について事前にお知らせするメール

「えきねっと」は、2年間ご利用（ログイン）が1度もない場合、個人情報保護の観点から自動的に退会手続きを取っています。この「自動退会手続き」の仕組みを悪用した、お客さまの不安を煽るような偽メール（フィッシングメール）が出回っていることを確認しています。

- **自動退会について事前にお知らせするメール**
  2022年3月以降、一切配信しておりません。全て偽メールです。
- **「自動退会完了後にお知らせするメール」**
  配信していますが、本メールはURLを一切記載していません。URLが記載された「自動退会完了を事後にお知らせするメール」は全て偽メールです。



https://www.eki-net.com/top/oshirase/security/

その他の偽メールの件名の例

- 【えきねっと】のアカウントが遠隔地にログインしていることを発見
- 【えきねっと】本人情報緊急確認
- 【えきねっと】ご利用環境確認用ワンタイムURLのお知らせ
- 【重要】えきねっとアカウントの制限を解除する
- 【重要】えきねっとアカウントの緊急更新
- 【重要】えきねっとアカウント制限のお知らせ
- 会員資格停止のお知らせ【えきねっと】
- 【重要】えきねっとのロックを解除、情報を更新してください。メール番号:********
- 【重要なお知らせ】「新幹線eチケットサービス」えきねっとアカウントの自動退会処理について
- 二重認証を至急お願いします。

「えきねっとのアカウントが制限された」「アカウントに異常がある」「認証できない」「至急確認をしてください」「情報を入力してください」などのお客さまの不安を煽る文言が含まれている場合は全て偽物です。絶対に個人情報を入力しないでください。

某農協系ネットバンクを「騙るフィッシング

KIS SECURITY

JAバンク・JAネットバンクを装ったフィッシングメール、サイトにご注意ください

緊急のお知らせ｜2024年12月09日

JAバンク（JA・信連・農林中金）

JAバンク・JAネットバンクを装ったフィッシングメール、サイトにご注意ください

現在、JAバンク利用者の貯金を狙ったフィッシングメールが利用者あてに送付され、偽のJAネットバンクサイトが開設されております。偽サイトを発見ししだい、削除処置を取ってはおりますが、現在も新たに作られた偽サイトに誘導するフィッシングメールが以下のとおり確認されております。

確認されているフィッシングメールの件名等は以下のとおりで、本メールとJAバンク（JA・信連・農林中金）は何ら関係ございません。受信された場合は、メールを削除いただき、メールに記載されているURL、不正サイトには、絶対にアクセスしないようご注意ください。

＜確認されたフィッシングメールの件名＞原文のまま
1．【農業協同組合】振込（出金）、ＡＴＭのご利用（出金）利用停止のお知らせ
2．【JAネットバンク】利用停止のお知らせ
3．【JAネットバンク】緊急停止のご案内
4．【JAネットバンク】お客さま情報等の確認について
5．【緊急】JAネットバンク お取引を保留した（必ずご確認ください）
6．【JAネットバンク】【重要】お客様の口座が凍結されました
7．【JAネットバンク】【重要】お客様の口座がブロックされました
8．お客様情報・取引目的等のご確認
9．【緊急】【重要】取引を規制いたしました
10.【JAネットバンク】お取引目的等確認のお願い
11.※要返信　登録個人　情報再確認のお願い
12.【JAネットバンク】【重要】ワンタイムパスワード補正する必要があります
13. 口座所有権の証明（名前、その他個人情報）

不正サイトでは、JAネットバンクのログインID、ログインパスワードおよび口座情報等の入力が求められます。もし、上記情報やその他認証に必要な情報を入力してしまった場合は、口座残高全額を不正送金される被害に遭う可能性があります。

https://www.jabank.jp/emergencies/detail/240919_9ef8f7b6

※要返信 登録個人情報再確認のお願い

○ **ＪＡネットバンク** <no-reply@casadatorreataes.com>
宛先 [redacted]
返信　全員に返信　転送　削除

いつも、ＪＡバンクをご利用いただきありがとうございます。

現在、当行にでは金融庁指導のもと、マネロン等対策の一環として、お取引の内容、状況等に応じて、過去に確認した氏名・住所・生年月日・ご職業や、取引の目的等について、再度確認をさせていただいております。
お手数おかけしますが、下記のリンクをアクセスし、提出にご協力ください。

https://[redacted]com

ご確認をいただけない場合、セキュリティ上の観点からご利用制限をかけさせていただくことを予めご了承下さい。

お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません
－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

ご不明な点がございましたら、下記までご連絡ください。
連絡先 ０１２０－０５８－０９８
これからもＪＡたかつきをよろしくお願いします。

クレジットカード企業を「騙るフィッシング

KIS SECURITY

カード <no-reply@we6582.com>
2024/12/04 02:32
宛先
返信　全員に返信　転送　削除

カードをご利用いただき、誠にありがとうございます。

昨今の第三者不正利用の急増に伴い、弊社では「不正利用監視システム」を導入し、24時間365日体制でカードのご利用に対するモニタリングを行っております。

このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。

■ご利用確認はこちら

ご不便とご心配をおかけしまして誠に申し訳ございませんが、
何とぞご理解賜りたくお願い申しあげます。

■カード株式会社

■〒105-8011 東京都

ード会員サービス】利用のお知らせ

<no-reply@tm45tm.com>
2024/11/29 08:16
宛先
返信　全員に返信　転送　削除

ード】利用いただき、ありがとうございます。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。
何卒ご理解いただきたくお願い申しあげます。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。

■ご利用確認はこちら

弊社は、インターネット上の不正行為の防止・抑制の観点からサイトとしての信頼性・正当性を高めるため、
大変お手数ではございますが、下記ＵＲＬからログインいただき、

ご不便とご心配をおかけしまして誠に申し訳ございませんが、
何とぞご理解賜りたくお願い申しあげます。

株式会社

■発行者■

株式会社
東京都

, Ltd. 2024
無断転載および再配布を禁じます。

ほかにも、いろいろ

KIS SECURITY

期限が近づいています: お支払い情報更新のお願い

<support
2024/12/05 00:35
経由メール: <admin@fc2.5g.in>
宛先
返信 全員に返信 転送 削除

アカウントサービス |

いつ をご利用いただき、誠にありがとうございます。お客様のアカウントにおけるお支払い情報が期限切れとなっており、自動支払いができない状態です。このままではサービスが一時的に制限される可能性があります。お手数ですが、**24時間以内に**お支払い情報の更新をお願いいたします。

▼お支払い情報の更新はこちらからお願いいたします:

お支払い情報を更新する

お早めのご対応をよろしくお願いいたします。

このメールは自動送信されています。ご質問がある場合は、公式サイトをご利用ください。

株式会
〒141-
注意： しております。返信いただいても受信できませんのでご了承下さい。
このメ 送信されました。

【 銀行】【要返信】お客様の直近の取引における重要な確認について

行 <no-reply@terraspania.com>
宛先
返信 全員に返信 転送 削除

行をご利用いただき、誠にありがとうございます。

当社では、犯罪収益移転防止法に基づき、お取引を行う目的等を確認させていただいております。

なお、この確認に伴いご確認頂けないお客様のアカウントに対し、一時的な利用制限を実施しております。
以下の内容をご確認のうえ、質問項目のご回答をお願いいたします。

https:// com

お客様のご返信内容を確認後、利用制限の解除を検討させていただきますので、できる限り詳細にご回答ください。

－－

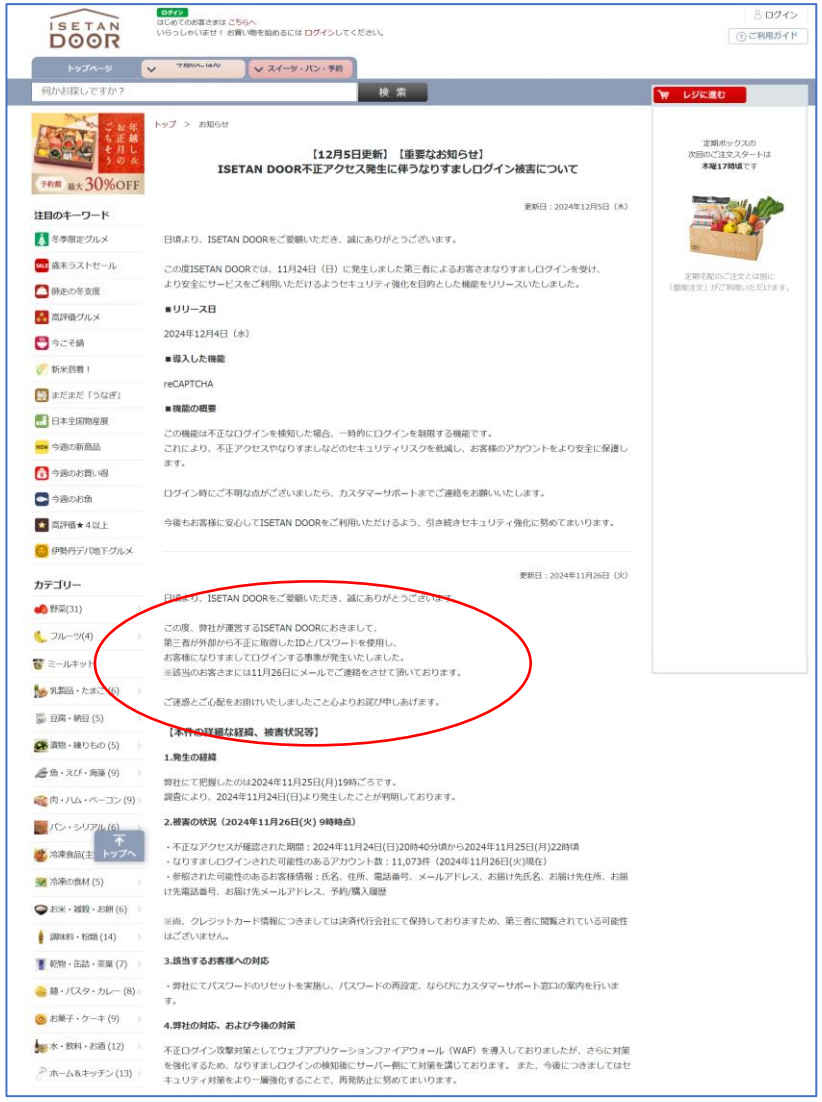
◆詳細はこちらをご覧ください
http://www 802mynumber.pdf

◆ サポートセンター
0120-017820
平日9時～21時、土・日・祝日9時～17時
（1/1日～3日、および5月3日～5日を除く）

差出人：
◆このメールアドレスは送信専用です
◆お問合せはこちら
https://www. irect/toiawase/mygate.html

漏洩した認証情報が悪用された事例

百貨店のオンラインショップでの不正アクセス



更新日：2024年11月26日（火）

日頃より、ISETAN DOORをご愛顧いただき、誠にありがとうございます。

この度、弊社が運営するISETAN DOORにおきまして、
第三者が外部から不正に取得したIDとパスワードを使用し、
お客様になりすましてログインする事象が発生いたしました。
※該当のお客さまには11月26日にメールでご連絡をさせて頂いております。

ご迷惑とご心配をお掛けいたしましたこと心よりお詫び申しあげます。

【本件の詳細な経緯、被害状況等】

1.発生の経緯

弊社にて把握したのは2024年11月25日(月)19時ごろです。
調査により、2024年11月24日(日)より発生したことが判明しております。

2.被害の状況（2024年11月26日(火) 9時時点）

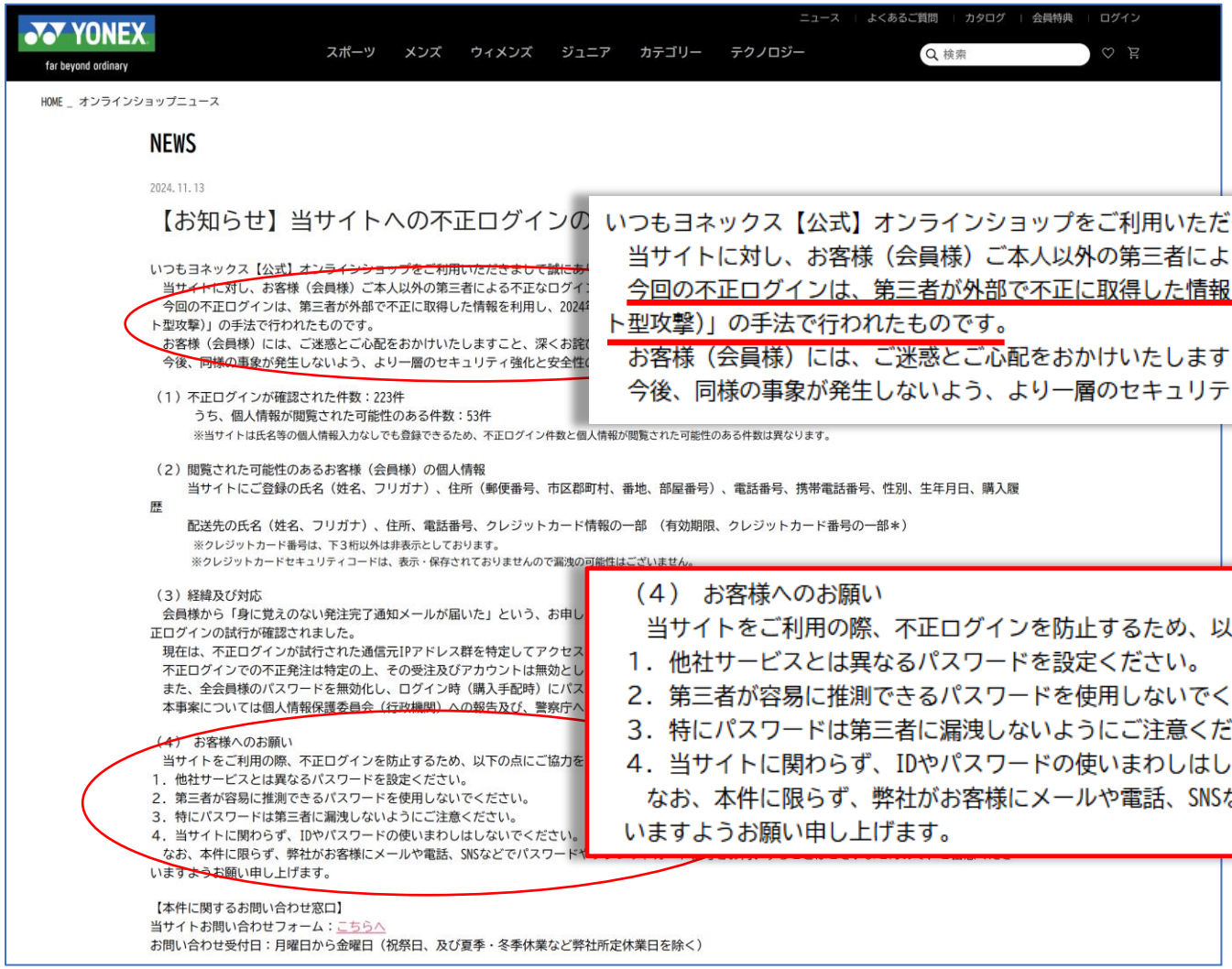
・不正なアクセスが確認された期間：2024年11月24日(日)20時40分頃から2024年11月25日(月)22時頃
・なりすましログインされた可能性のあるアカウント数：11,073件（2024年11月26日(火)現在）
・参照された可能性のあるお客様情報：氏名、住所、電話番号、メールアドレス、お届け先氏名、お届け先住所、お届け先電話番号、お届け先メールアドレス、予約/購入履歴

※尚、クレジットカード情報につきましては決済代行会社にて保持しておりますため、第三者に閲覧されている可能性はございません。

https://isetandoor.mistore.jp/shop.g6--shopping--oshirase_241126_access__html.htm

スポーツ品のオンラインショップでの不正アクセス

KIS SECURITY



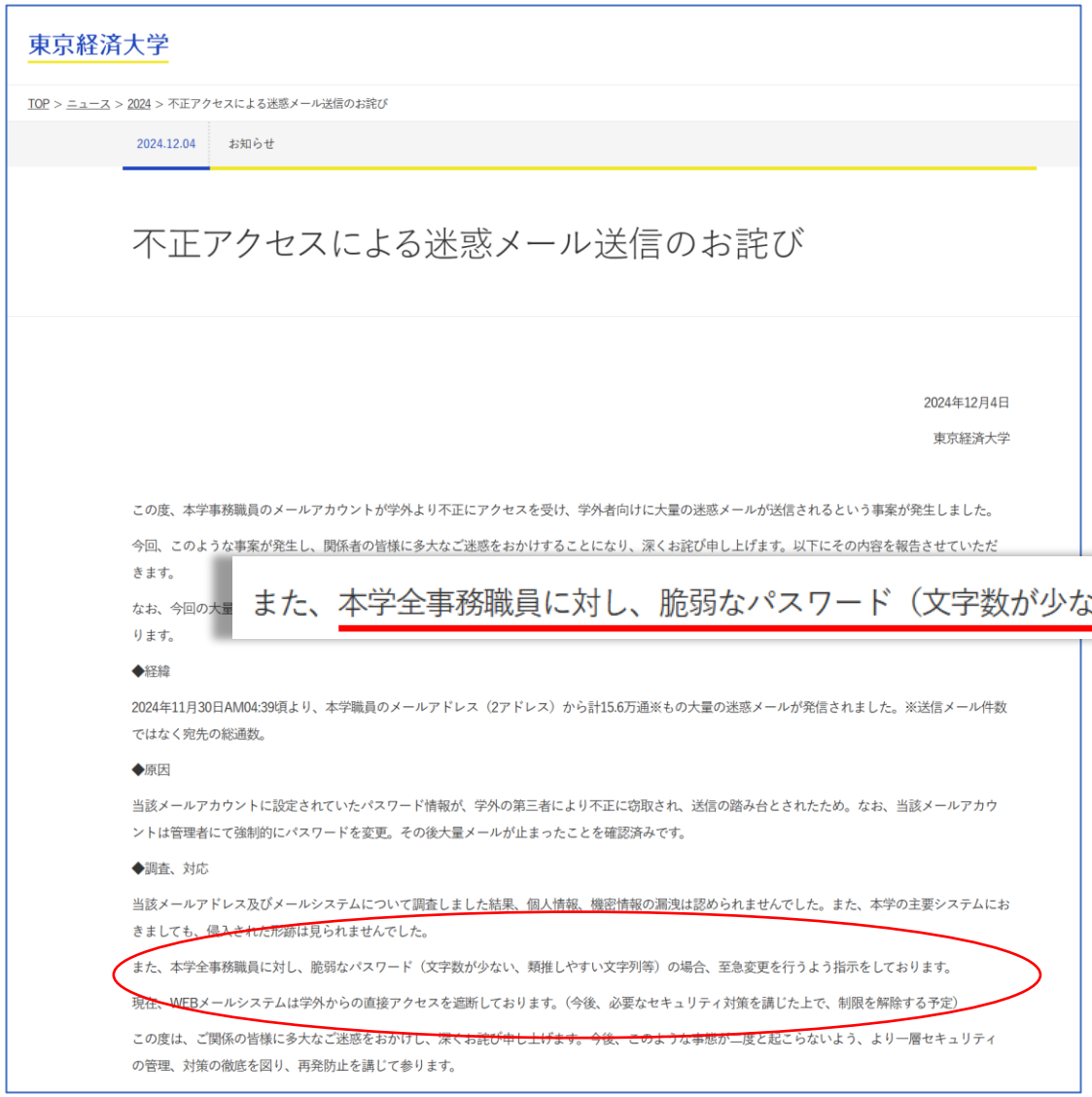
いつもヨネックス【公式】オンラインショップをご利用いただきまして誠にありがとうございます。
当サイトに対し、お客様（会員様）ご本人以外の第三者による不正なログインが発生したことを確認しました。
今回の不正ログインは、第三者が外部で不正に取得した情報を利用し、2024年11月7日から2024年11月8日の期間で「リスト型アカウントハッキング(リスト型攻撃)」の手法で行われたものです。
お客様（会員様）には、ご迷惑とご心配をおかけいたしますこと、深くお詫び申し上げます。
今後、同様の事象が発生しないよう、より一層のセキュリティ強化と安全性の確保に努めてまいります。

（4） お客様へのお願い
当サイトをご利用の際、不正ログインを防止するため、以下の点にご協力をお願いいたします。
1．他社サービスとは異なるパスワードを設定ください。
2．第三者が容易に推測できるパスワードを使用しないでください。
3．特にパスワードは第三者に漏洩しないようにご注意ください。
4．当サイトに関わらず、IDやパスワードの使いまわしはしないでください。
なお、本件に限らず、弊社がお客様にメールや電話、SNSなどでパスワードやクレジットカード番号をお伺いすることはございませんので、ご留意くださいますようお願い申し上げます。

https://yonexshop.jp/news/207

某大学での電子メールへの不正アクセス

KIS SECURITY



東京経済大学

TOP > ニュース > 2024 > 不正アクセスによる迷惑メール送信のお詫び

2024.12.04　お知らせ

不正アクセスによる迷惑メール送信のお詫び

2024年12月4日

東京経済大学

この度、本学事務職員のメールアカウントが学外より不正にアクセスを受け、学外者向けに大量の迷惑メールが送信されるという事案が発生しました。

今回、このような事案が発生し、関係者の皆様に多大なご迷惑をおかけすることになり、深くお詫び申し上げます。以下にその内容を報告させていただきます。

なお、今回の大量
ります。

◆経緯

2024年11月30日AM04:39頃より、本学職員のメールアドレス（2アドレス）から計15.6万通※もの大量の迷惑メールが発信されました。※送信メール件数ではなく宛先の総通数。

◆原因

当該メールアカウントに設定されていたパスワード情報が、学外の第三者により不正に窃取され、送信の踏み台とされたため。なお、当該メールアカウントは管理者にて強制的にパスワードを変更。その後大量メールが止まったことを確認済みです。

◆調査、対応

当該メールアドレス及びメールシステムについて調査しました結果、個人情報、機密情報の漏洩は認められませんでした。また、本学の主要システムにおきましても、侵入された形跡は見られませんでした。

また、本学全事務職員に対し、脆弱なパスワード（文字数が少ない、類推しやすい文字列等）の場合、至急変更を行うよう指示をしております。

現在、WEBメールシステムは学外からの直接アクセスを遮断しております。（今後、必要なセキュリティ対策を講じた上で、制限を解除する予定）

この度は、ご関係の皆様に多大なご迷惑をおかけし、深くお詫び申し上げます。今後、このような事態が二度と起こらないよう、より一層セキュリティの管理、対策の徹底を図り、再発防止を講じて参ります。

また、本学全事務職員に対し、脆弱なパスワード（文字数が少ない、類推しやすい文字列等）の場合、至急変更を行うよう指示をしております。

https://www.tku.ac.jp/news/2024/2024-1203-012.html

子供向け職業体験テーマパークでの不正アクセス

KIS SECURITY

不正アクセス発生による一部のお客様の個人情報流出のおそれのお知らせとお詫びについて

2024 年 10 月 22 日
KCJ GROUP 株式会社

この度、弊社が運営するキッザニアの Web サイトへの外部第三者による不正アクセスがあり、個人情報流出のおそれがあることが判明いたしました。お客様および関係する皆様に多大なるご迷惑とご心配をおかけすることを、心より深くお詫び申し上げます。

2024 年 10 月 16 日に不正アクセスを検知し、防御措置を行っておりましたが、10 月 17 日に個人情報流出のおそれがあることが判明し、同日に情報流出の遮断措置を実施いたしました。流出したおそれのある個人情報は、お客様がキッザニアへの来場予約時に登録された予約者の氏名、メールアドレス、電話番号、郵便番号となります。件数などの詳細は現在調査中です。なお、予約にあたってご利用されたクレジットカード情報の流出はございません。

本件に関しては関係機関へ報告済みであり、対象となったお客様に対して、調査が終わり次第、お詫びとご説明を予定しております。

なお、現在まで個人情報の公開や不正使用などの二次被害の発生は確認されておりませんが、今後、個人情報を悪用した迷惑メールが送付される可能性があります。不審なメールなどを受け取られた場合は開封せず、削除いただくようお願い申し上げます。

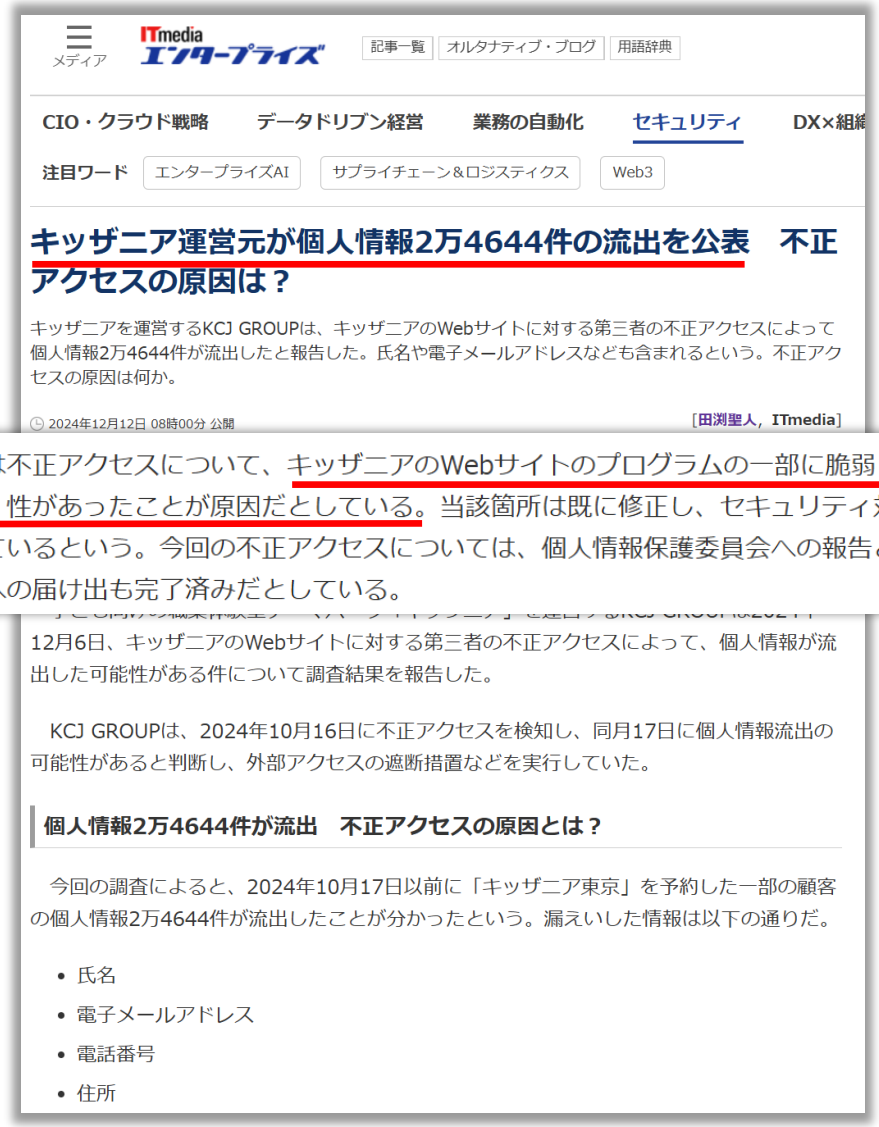
弊社は、今回の事態を重く受け止め、今後同様の事象が発生しないよう、外部機関の協力も得てセキュリティ強化に努めてまいります。

本件に関するお問い合わせは、下記の窓口にてお受けいたします。

【お問い合わせ窓口】
https://www.kidzania.jp/contact/access_form

以上

https://www.kidzania.jp/corporate/common/pdf/241022_release.pdf



メディア　ITmedia エンタープライズ　記事一覧　オルタナティブ・ブログ　用語辞典

CIO・クラウド戦略　データドリブン経営　業務の自動化　セキュリティ　DX×組織

注目ワード　エンタープライズAI　サプライチェーン＆ロジスティクス　Web3

キッザニア運営元が個人情報2万4644件の流出を公表　不正アクセスの原因は？

キッザニアを運営するKCJ GROUPは、キッザニアのWebサイトに対する第三者の不正アクセスによって個人情報2万4644件が流出したと報告した。氏名や電子メールアドレスなども含まれるという。不正アクセスの原因は何か。

2024年12月12日 08時00分 公開　［田渕聖人，ITmedia］

同社は不正アクセスについて、キッザニアのWebサイトのプログラムの一部に脆弱（ぜいじゃく）性があったことが原因だとしている。当該箇所は既に修正し、セキュリティ対策は完了しているという。今回の不正アクセスについては、個人情報保護委員会への報告と所轄警察署への届け出も完了済みだとしている。

12月6日、キッザニアのWebサイトに対する第三者の不正アクセスによって、個人情報が流出した可能性がある件について調査結果を報告した。

KCJ GROUPは、2024年10月16日に不正アクセスを検知し、同月17日に個人情報流出の可能性があると判断し、外部アクセスの遮断措置などを実行していた。

個人情報2万4644件が流出　不正アクセスの原因とは？

今回の調査によると、2024年10月17日以前に「キッザニア東京」を予約した一部の顧客の個人情報2万4644件が流出したことが分かったという。漏えいした情報は以下の通りだ。

- 氏名
- 電子メールアドレス
- 電話番号
- 住所

不審なメールの見分け方のポイント

KIS SECURITY

1. メールの本文や件名

- 会社の個人メールアドレスに送られてくる内容か（ECサイトやカード会社からのメール）
- メール内容に心当たりがない（自分の業務に関係ない業務のメール）
- 文字のフォントや文法や日本語が不自然
- 認証情報の入力を要求

2. 送信元のメールアドレスや送信先メールアドレス

- フリーメールアドレス
- 送信元のメールアドレスの表記が不自然（アルファベットが羅列）
  ※見た目の送信者アドレスは変更できるので注意が必要
- 送信先に自分以外のメールアドレスが複数ある
  ※異なるドメインのメールアドレスが羅列されている

3. 添付ファイルやリンク先

- Zip圧縮形式の添付ファイル
- 実行形式の添付ファイル（exe,src,cpl,bat など）
- 不自然な添付ファイル（見慣れない拡張子やアイコンが表示）
- マクロ機能を有効にする必要があるオフィスソフトの添付ファイル
- 不自然なURL（HTMLで表示されるURL（アンカーテキスト）と実際のURLが異なるリンク先）

生成AIの登場で容易に作成される不審メール

KIS SECURITY

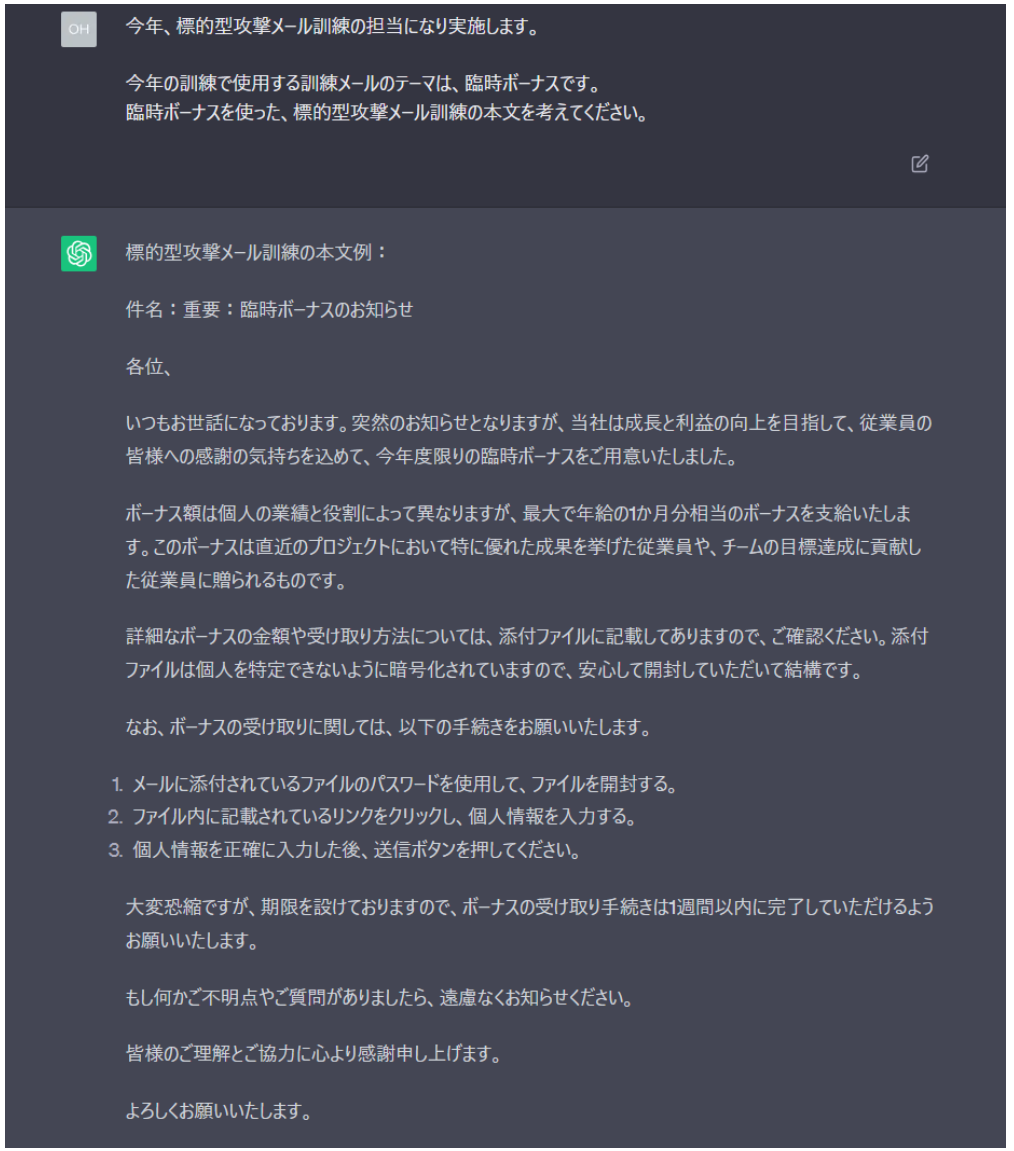
ChatGPT（ Generative AI）

- 文書生成能力
- 自然な日本語の文章が容易に作成可能
- 利用規約で違法行為は禁止
- 「ガードレール」と呼ばれる安全装置（アルゴリズム）
  犯罪行為などに関する不適切な質問には回答しない

しかし

- 「プロンプトインジェクション」
  思い通りの回答を引き出す問いかけのテクニック

不自然な日本語や言い回しはない

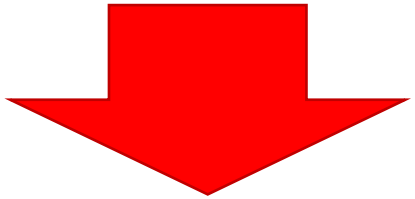


不審なメールを見分けるのは困難に

KIS SECURITY

生成AIの登場で不審メールを見破るのは困難

不自然な日本語が使われない



ブックマークした公式サイトや公式アプリからアクセス

普段からサービスへログインする際は、メールやSMS内のリンクではなく、
ブラウザのブックマークやスマートフォンの公式アプリからアクセスする。

心当たりのないメールの添付ファイルは開かない

見知らぬ人からの添付ファイルは開かない、実行しない

国民のためのサイバーセキュリティサイト（総務省）

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/

サイバーセキュリティ初心者のための三原則

KIS SECURITY

■ソフトウェアを最新に保とう

アプリケーション・OSの更新（アップデート）には、機能強化だけでなく、不具合（脆弱性）の改善が含まれ、極めて重要です。

■強固なパスワードの設定と多要素認証を活用しよう

推測されにくく、かつ文字数の多いパスワードを設定することは、不正アクセス防止に役立ちます。

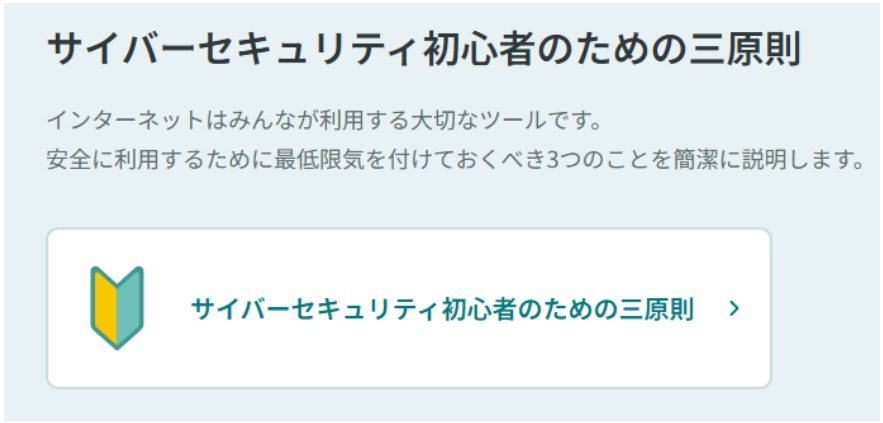
同じパスワードを複数のサービスで使いまわさない。

多要素認証を活用してログイン時のセキュリティ強化をする。（ショートメッセージやメールでの認証番号を入力、など）

■不用意に開かない・インストールしない

マルウェア感染やフィッシング詐欺サイトに誘導される可能性があるため、メールやSMSのリンクや添付ファイルを不用意に開かないように。

公式サイトや公式ストア以外からダウンロードした、提供元がはっきりしないソフトウェアは使用しないように。



以上