標的型攻撃メール訓練サービス「KIS MailMon」

訓練シナリオ ガイド（1）

・本書は、シナリオギャラリーの新着や人気のシナリオの中から**「リンク＆データ送信」型をピックアップ**し紹介しています。

・初級・上級レベルのシナリオを用意しています。

・訓練の型・内容により以下に分けてあります
　・フィッシングタイプ　　：フィッシングメールを模したもの
　・クリックフィックスタイプ：クリックフィックスを模したもの
　・サポート詐欺タイプ　　：サポート詐欺メールを模したもの
　・ワンポイント教育タイプ　：簡単な教育コンテンツを画面2で表示

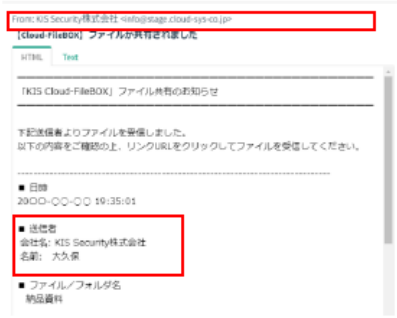
※シナリオは、全て**お客様でカスタマイズ可能**です。カスタマイズされる場合はカスタマイズガイドを参考にしてください。
　ご不明な点がございましたら、サポート窓口までお問い合わせください。

KIS Security 株式会社

2026/06/16

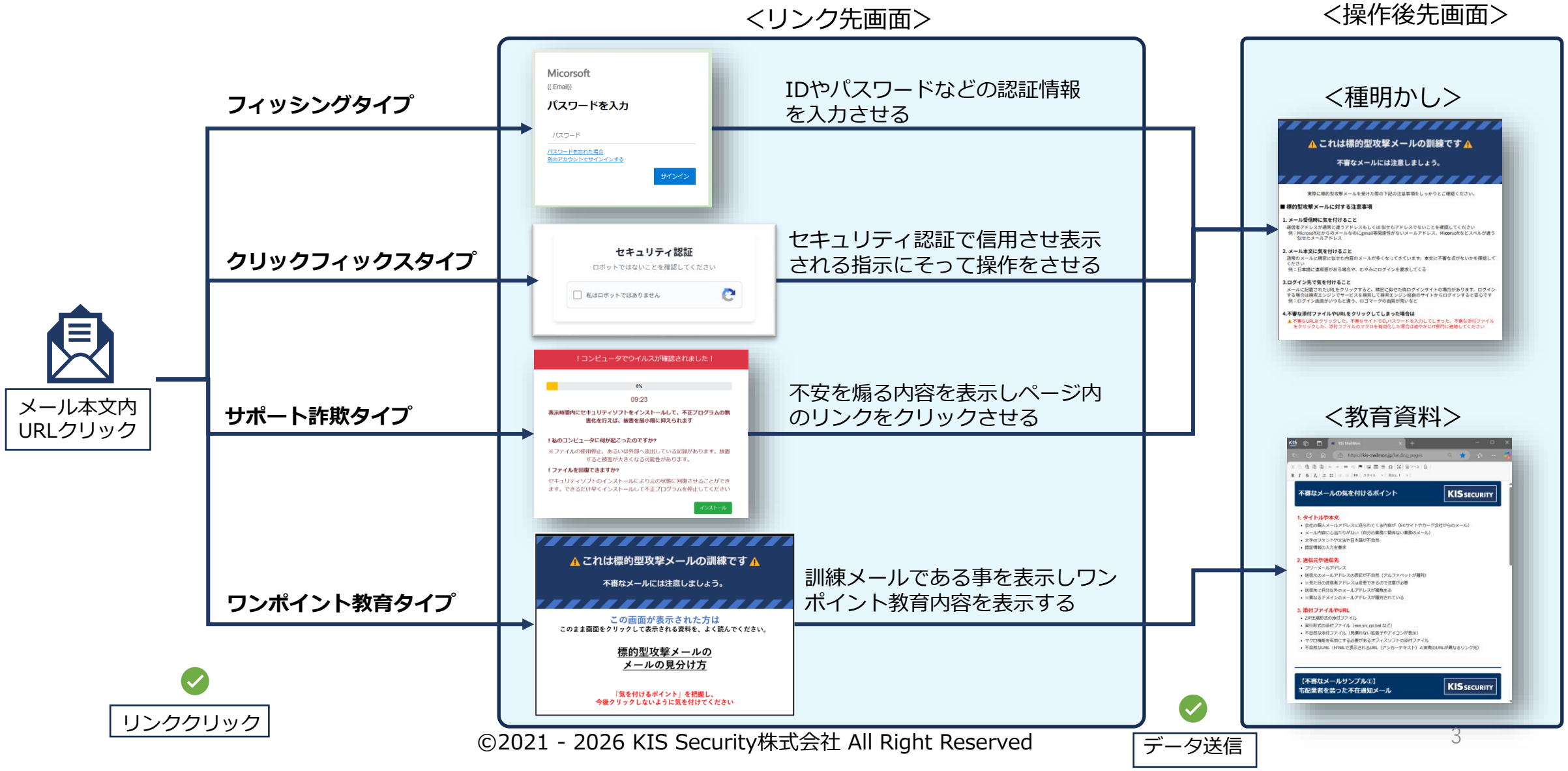
目次

レベルについて

初級	見分けやすい内容		送信元のドメイン：アルファベット16桁 メール本文：明朝体
中級	注意すれば見分けれる内容（忙しいときに見落としてしまう）		メール本文のシグネチャと送信元が違う 送信元：CSTサービス＜info@office-system-co.jp＞ シグネチャ：クラウドシステック株式会社 その他、初級・上級に**分類されないもの**
上級	見分けにくい内容		メール本文のシグネチャと送信元が同じであるがメールアドレスが違う 送信元：KIS Security株式会社＜info@cloud-sys-co.jp＞ シグネチャ：KIS Security株式会社

URLリンク&データ送信型の訓練の流れ

4つのタイプの訓練の流れと記録のタイミングはそれぞれ以下の通りです



シナリオ一覧

	シナリオ名	レベル	型	ジャンル	ページ
フィッシングタイプ	2601E：アカウント停止にご注意ください（データ入力）	初級	リンク＆データ送信型	外部組織	5
	2601D：アカウント停止にご注意ください（QRコード＋データ入力）	上級	リンク＆データ送信型	外部組織	6
	2601C：重要：サーバ上に隔離されたメールがあります（データ入力）	上級	リンク＆データ送信型	社内業務連絡	7
	2601B：【重要】生成AI業務利用に関するガイドライン（データ入力）	上級	リンク＆データ送信型	社内業務連絡	8
	2601A：【重要】多要素認証（MFA）の再設定が必要（QRコード＋データ入力）	上級	リンク＆データ送信型	外部組織	9
	2510D：メールサービス仕様変更に伴うアカウント設定確認のお願い（データ入力）（初級）	初級	リンク＆データ送信型	通知系	10
	2510C：メールサービス仕様変更に伴うアカウント設定確認のお願い（データ入力）（上級）	上級	リンク＆データ送信型	通知系	11
	2510B：メールアドレスを確認してください。（データ入力）（初級）	初級	リンク＆データ送信型	外部組織	12
	2510A：メールアドレスを確認してください。（データ入力）（上級）	上級	リンク＆データ送信型	外部組織	13
	2507I：【緊急・要対応】Intar-mart アカウントのパスワードがまもなく失効します（データ入力）	上級	リンク＆データ送信型	外部組織	14
	2507G：FadEX配達のお知らせ（QRコード＋データ入力）	上級	リンク＆データ送信型	外部組織	15
	2507E：SarviceNowチケット通知（データ入力）	上級	リンク＆データ送信型	通知系	16
クリックフィックスタイプ	2510I：セキュリティ修正プログラム適用のお願い（CF2-2）	上級	リンク＆データ送信型	社内業務連絡	17
	2510H：セキュリティ修正プログラム適用のお願い（CF2-1）	上級	リンク＆データ送信型	社内業務連絡	18
	2510G：Micorsoft 365 アカウントのセキュリティ更新（CF1）	上級	リンク＆データ送信型	外部組織	19
	2510F：【緊急】Windows Updateのお願い（CF1）	上級	リンク＆データ送信型	社内業務連絡	20
	2510E：【緊急・重要】セキュリティ更新プログラムの適用に関するお願い（CF1）	上級	リンク＆データ送信型	外部組織	21
サポート詐欺タイプ	2507U：最大50,000ポイントプレゼント（サポート詐欺１）	上級	リンク＆データ送信型	その他	22
	2507T：最大50,000ポイントプレゼント（サポート詐欺２）	上級	リンク＆データ送信型	その他	23
	2507S：最大50,000ポイントプレゼント（サポート詐欺３）	上級	リンク＆データ送信型	その他	24
	2507R：お支払い口座登録のお願い（サポート詐欺１）	上級	リンク＆データ送信型	外部組織	25
	2507Q：お支払い口座登録のお願い（サポート詐欺２）	上級	リンク＆データ送信型	外部組織	26
	2507P：お支払い口座登録のお願い（サポート詐欺３）	上級	リンク＆データ送信型	外部組織	27
	2507O：健康保険組合 被保険者の皆様へ（サポート詐欺１）	上級	リンク＆データ送信型	外部組織	28
	2507N：健康保険組合 被保険者の皆様へ（サポート詐欺２）	上級	リンク＆データ送信型	外部組織	29
	2507M：健康保険組合 被保険者の皆様へ（サポート詐欺３）	上級	リンク＆データ送信型	外部組織	30
ワンポイント教育タイプ	2507L：お荷物のお届けに関する重要なお知らせ（ワンポイント教育１）	初級	リンク＆データ送信型	社外/取引先	31
	2507K：新バージョンに関する問い合わせ（ワンポイント教育２）	上級	リンク＆データ送信型	社内業務連絡	32
	2507F：【楽大証券】ログインシステムのセキュリティ更新：ご協力をお願いします（ワンポイント教育３）	上級	リンク＆データ送信型	外部組織	33

シナリオ名：
2601E：アカウント停止にご注意ください（データ入力）

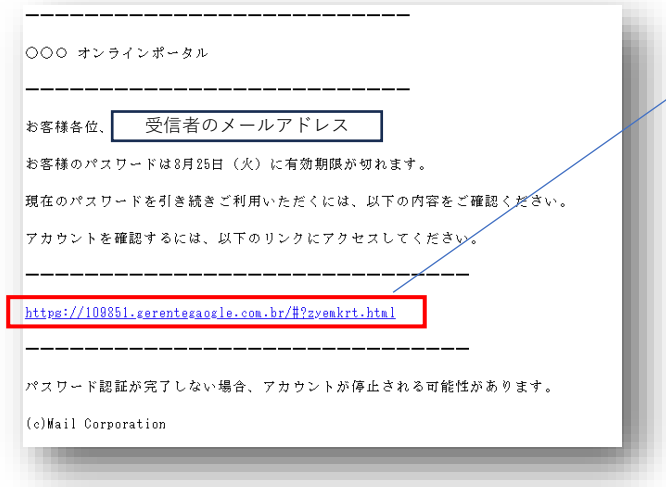
リンク＆データ送信型
外部組織
初級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2601E**」と入力して検索してください

＜メール＞
送信元：
<no-replay@yxwhitotupfruxxe.com>

リンク
クリック



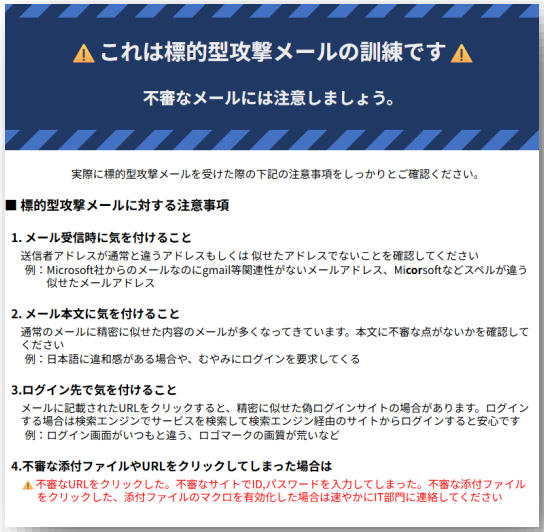
メールのリンクをクリックすると
「**リンククリック**」**が記録**され、リンク先画面が表示

＜リンク先画面（*1）＞

本人確認のためメールアドレスを入力を促す画面が表示されます。
メールアドレスを入力し「次へ進む」をクリックすると「**データ送信**」**が記録**され、種明かし画面が表示

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



シナリオ名：
2601D：アカウント停止にご注意ください（QRコード+データ入力）

リンク＆データ送信型
外部組織
上級

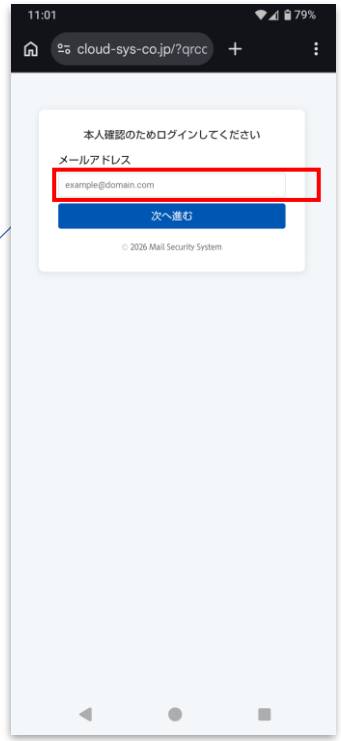
KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2601D**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

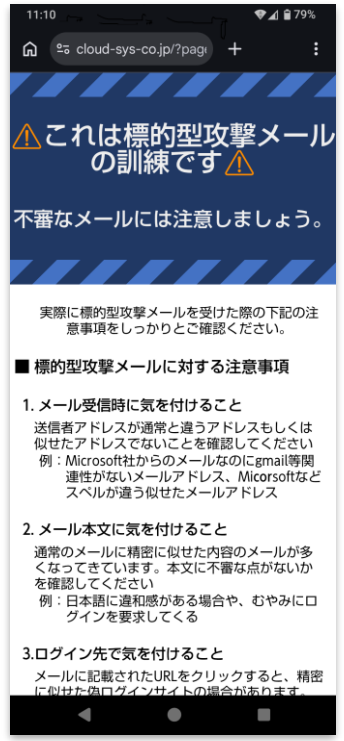
メールのQRコードをスマートフォンで読み取り、表示されるURLをタップすると「**リンククリック**」**が記録**され、リンク先画面が表示

＜リンク先画面（*1）＞



本人確認のためメールアドレスを入力を促す画面が表示されます。
メールアドレスを入力し「次へ進む」をクリックすると「**データ送信**」**が記録**され、スマートフォンの画面に種明かし画面が表示

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



シナリオ名：
2601C：重要：サーバ上に隔離されたメールがあります（データ入力）

リンク＆データ送信型
社内業務連絡
上級

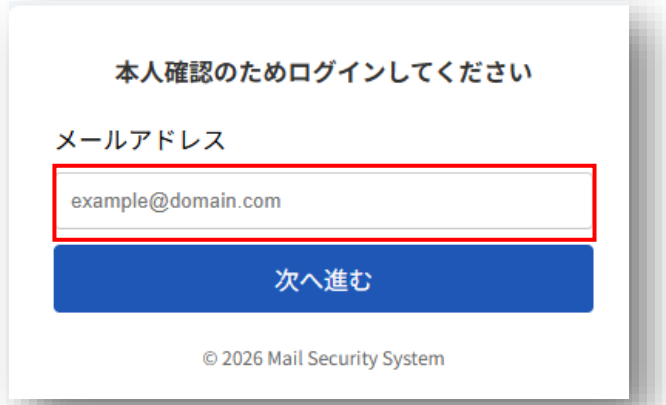
KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2601C**」と入力して検索してください

＜メール＞
送信元：情報システム部
<info@system-grp.com>

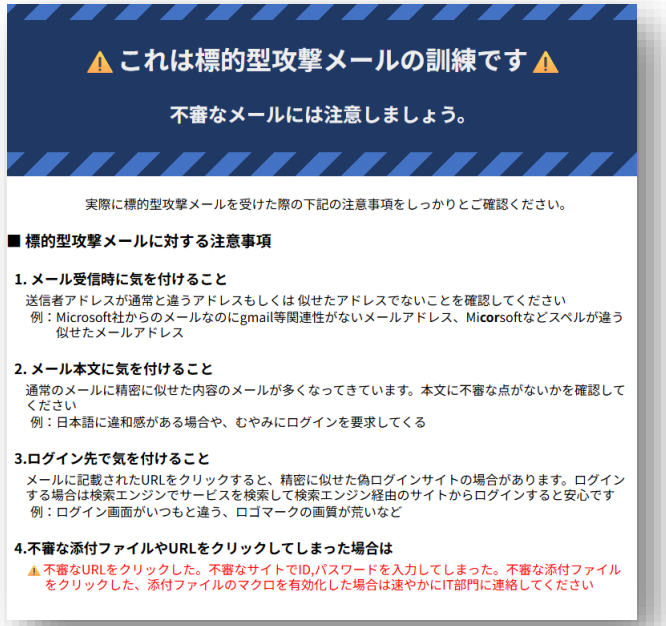
リンク
クリック

＜リンク先画面（*1）＞



データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



「メッセージを確認する」または
「サポートへ連絡」をクリックすると
「**リンククリック**」**が記録**される

本人確認のためメールアドレスを入力を促す画面が表示されます。
メールアドレスを入力し「次へ進む」をクリックすると「**データ送信**」**が記録**され、
種明かし画面が表示

シナリオ名：
2601B：【重要】生成AI業務利用に関するガイドライン（データ入力）

リンク＆データ送信型
社内業務連絡
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2601B**」と入力して検索してください

＜メール＞
送信元：情報システム部
<info@system-grp.com>

リンク
クリック

社員の皆様

お疲れ様です。 XXX部より重要なお知らせです。

2026年1月付で、社内の「生成AI利用（Copilot等）に関するセキュリティガイドライン」が改定されました。

昨今の情報漏洩事故の多発を受け、セキュリティ強化の一環として、全社員に対して新規定への同意が義務付けられています。

つきましては、下記の手順に従い、期限内に承認手続きを完了してください。

【提出期限】 2026年X月XX日 17:00まで ※未対応の場合、アカウントの一部機能が制限される可能性があります。

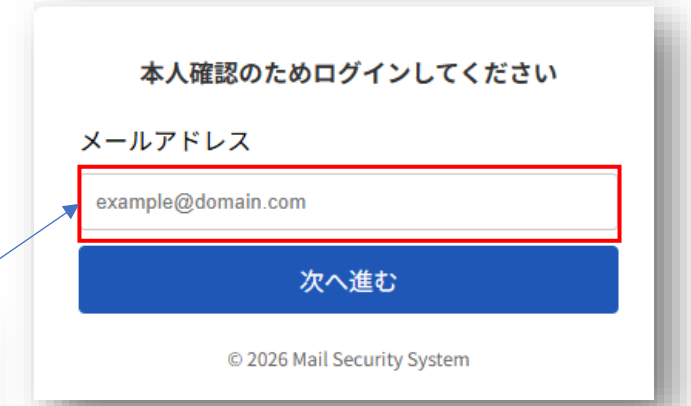
【対応手順】

1. 以下のリンクより、改定内容（PDF）を確認する
2. 同ページ内の「同意する」ボタンを押下する

社内ポータル（ガイドライン同意ページ） ※社外ネットワークからもアクセス可能です。

メールのリンクをクリックすると
「**リンククリック**」**が記録**され、リンク先画面が表示

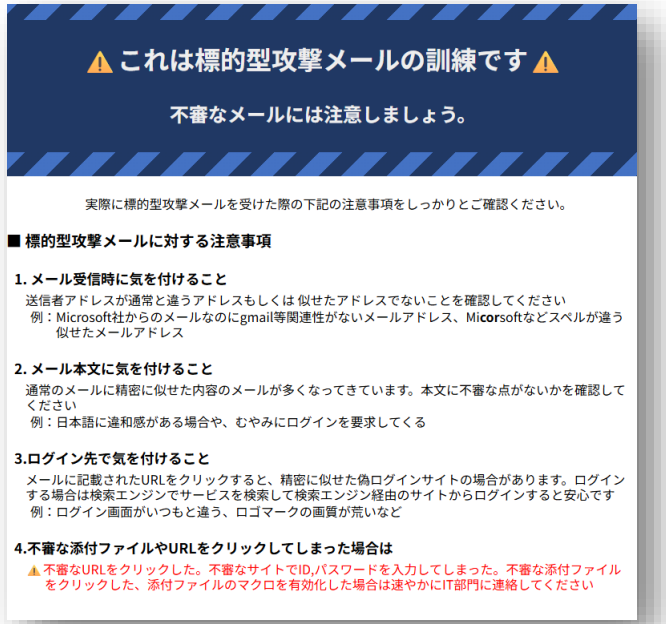
＜リンク先画面（*1）＞



データ
送信

本人確認のためメールアドレスを入力を促す画面が表示されます。
メールアドレスを入力し「次へ進む」をクリックすると「**データ送信**」**が記録**され、種明かし画面が表示

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



シナリオ名：
2601A：【重要】多要素認証（MFA）の再設定が必要（ QRコード+データ入力）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2601A**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

メールのQRコードをスマートフォンで読み取り、表示されるURLをタップすると「**リンククリック**」**が記録**され、リンク先画面が表示

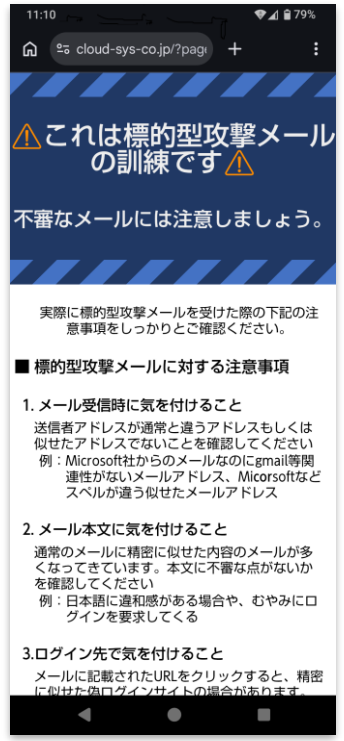
リンク
クリック

＜リンク先画面（*1）＞

スマートフォンの画面に受信者のメールアドレスが表示されたログイン画面が表示されます。
パスワードを入力し、「サインイン」をクリックすると「**データ送信**」**が記録**され、
スマートフォンの画面に種明かし画面が表示
※訓練実施者の管理画面では、QRコード付きの訓練であることやスマートフォンで開封されたことが確認できます。

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



シナリオ名：

2510D：メールサービス仕様変更に伴うアカウント設定確認のお願い（データ入力）（初級）

リンク＆データ送信型

通知系

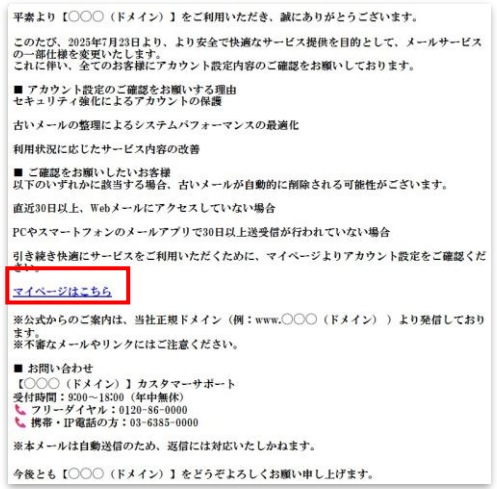
初級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510D**」と入力して検索してください

＜メール＞

送信元：
<no-replay@yxwhitotupfruxxe.com>



平素より【〇〇〇（ドメイン）】をご利用いただき、誠にありがとうございます。

このたび、2025年7月23日より、より安全で快適なサービス提供を目的として、メールサービスの一部仕様を変更いたします。
これに伴い、全てのお客様にアカウント設定内容のご確認をお願いしております。

■ アカウント設定のご確認をお願いする理由
セキュリティ強化によるアカウントの保護

古いメールの整理によるシステムパフォーマンスの最適化

利用状況に応じたサービス内容の改善

■ ご確認をお願いしたいお客様
以下のいずれかに該当する場合、古いメールが自動的に削除される可能性がございます。

直近30日以上、Webメールにアクセスしていない場合

PCやスマートフォンのメールアプリで30日以上送受信が行われていない場合

引き続き快適にサービスをご利用いただくために、マイページよりアカウント設定をご確認ください。

マイページはこちら

※公式からのご案内は、当社正規ドメイン（例：www.〇〇〇（ドメイン））より発信しております。
※不審なメールやリンクにはご注意ください。

■ お問い合わせ
【〇〇〇（ドメイン）】カスタマーサポート
受付時間：9:00～18:00（年中無休）
フリーダイヤル：0120-86-0000
携帯・IP電話の方：03-6385-0000

※本メールは自動送信のため、返信には対応いたしかねます。

今後とも【〇〇〇（ドメイン）】をどうぞよろしくお願い申し上げます。

メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

リンク
クリック

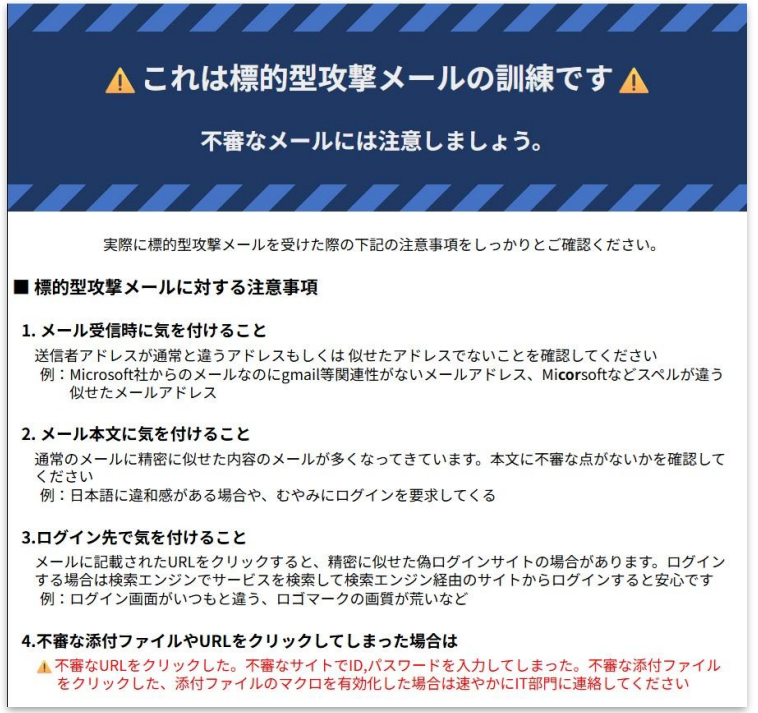
＜リンク先画面（*1）＞

以下の操作をすると「**データ送信**」**が記録**され、種明かし画面が表示。
・「ファイルダウンロード認証」にメールアドレス、パスワード入力し「ダウンロード」をクリックする。
・「ファイルダウンロード認証」にメールアドレス、パスワード入力した状態で表示されているいずれかのサービスのアイコンをクリックする

データ
送信

＜リンク先画面(種明かし画面)＞

リンク先画面(*1)でpage2として指定



⚠ これは標的型攻撃メールの訓練です ⚠

不審なメールには注意しましょう。

実際に標的型攻撃メールを受けた際の下記の注意事項をしっかりとご確認ください。

■ 標的型攻撃メールに対する注意事項

1. メール受信時に気を付けること
送信者アドレスが通常と違うアドレスもしくは 似せたアドレスでないことを確認してください
例：Microsoft社からのメールなのにgmail等関連性がないメールアドレス、Micorsoftなどスペルが違う似せたメールアドレス

2. メール本文に気を付けること
通常のメールに精密に似せた内容のメールが多くなってきています。本文に不審な点がないかを確認してください
例：日本語に違和感がある場合や、むやみにログインを要求してくる

3.ログイン先で気を付けること
メールに記載されたURLをクリックすると、精密に似せた偽ログインサイトの場合があります。ログインする場合は検索エンジンでサービスを検索して検索エンジン経由のサイトからログインすると安心です
例：ログイン画面がいつもと違う、ロゴマークの画質が荒いなど

4.不審な添付ファイルやURLをクリックしてしまった場合は
⚠ 不審なURLをクリックした。不審なサイトでID,パスワードを入力してしまった。不審な添付ファイルをクリックした、添付ファイルのマクロを有効化した場合は速やかにIT部門に連絡してください

シナリオ名：

2510C：メールサービス仕様変更に伴うアカウント設定確認のお願い（データ入力）（上級）

リンク＆データ送信型

通知系

上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510C**」と入力して検索してください

＜メール＞

送信元：
<support@office-system-co.jp>

平素より【〇〇〇（ドメイン）】をご利用いただき、誠にありがとうございます。

このたび、2025年7月23日より、より安全で快適なサービス提供を目的として、メールサービスの一部仕様を変更いたします。
これに伴い、全てのお客様にアカウント設定内容のご確認をお願いしております。

■ アカウント設定のご確認をお願いする理由
セキュリティ強化によるアカウントの保護

古いメールの整理によるシステムパフォーマンスの最適化

利用状況に応じたサービス内容の改善

■ ご確認をお願いしたいお客様
以下のいずれかに該当する場合、古いメールが自動的に削除される可能性がございます。

直近30日以上、Webメールにアクセスしていない場合

PCやスマートフォンのメールアプリで30日以上送受信が行われていない場合

引き続き快適にサービスをご利用いただくために、マイページよりアカウント設定をご確認ください。

マイページはこちら

※公式からのご案内は、当社正規ドメイン（例：www.〇〇〇（ドメイン））より発信しております。
※不審なメールやリンクにはご注意ください。

■ お問い合わせ
【〇〇〇（ドメイン）】カスタマーサポート
受付時間：9:00～18:00（年中無休）
フリーダイヤル：0120-86-0000
携帯・IP電話の方：03-6385-0000

※本メールは自動送信のため、返信には対応いたしかねます。

今後とも【〇〇〇（ドメイン）】をどうぞよろしくお願い申し上げます。

メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

リンク
クリック

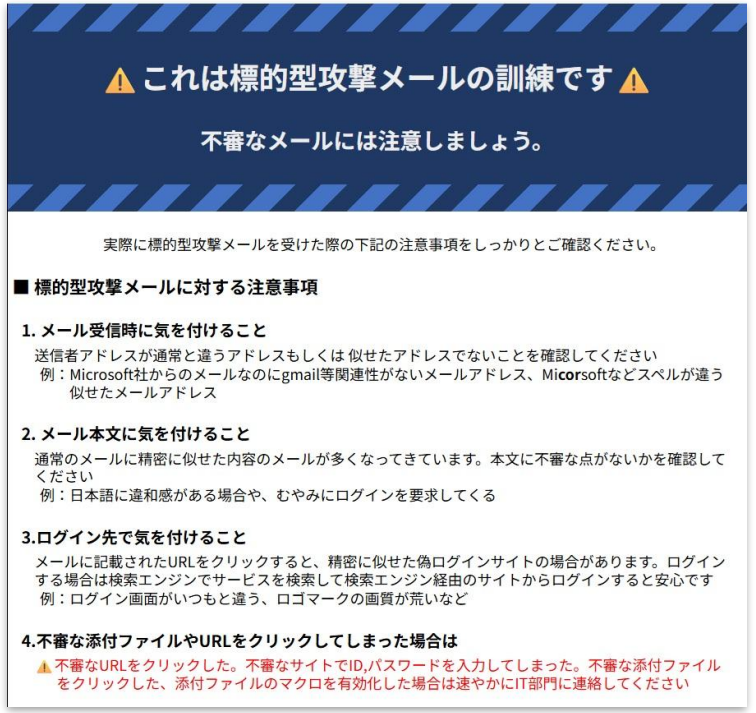
＜リンク先画面（*1）＞

以下の操作をすると「**データ送信**」**が記録**され、種明かし画面が表示。
・「ファイルダウンロード認証」にメールアドレス、パスワード入力し「ダウンロード」をクリックする。
・「ファイルダウンロード認証」にメールアドレス、パスワード入力した状態で表示されているいずれかのサービスのアイコンをクリックする

データ
送信

＜リンク先画面(種明かし画面)＞

リンク先画面(*1)でpage2として指定



⚠ これは標的型攻撃メールの訓練です ⚠

不審なメールには注意しましょう。

実際に標的型攻撃メールを受けた際の下記の注意事項をしっかりとご確認ください。

■ 標的型攻撃メールに対する注意事項

1. メール受信時に気を付けること
送信者アドレスが通常と違うアドレスもしくは 似せたアドレスでないことを確認してください
例：Microsoft社からのメールなのにgmail等関連性がないメールアドレス、Micorsoftなどスペルが違う似せたメールアドレス

2. メール本文に気を付けること
通常のメールに精密に似せた内容のメールが多くなってきています。本文に不審な点がないかを確認してください
例：日本語に違和感がある場合や、むやみにログインを要求してくる

3.ログイン先で気を付けること
メールに記載されたURLをクリックすると、精密に似せた偽ログインサイトの場合があります。ログインする場合は検索エンジンでサービスを検索して検索エンジン経由のサイトからログインすると安心です
例：ログイン画面がいつもと違う、ロゴマークの画質が荒いなど

4.不審な添付ファイルやURLをクリックしてしまった場合は
⚠ 不審なURLをクリックした。不審なサイトでID,パスワードを入力してしまった。不審な添付ファイルをクリックした、添付ファイルのマクロを有効化した場合は速やかにIT部門に連絡してください

シナリオ名：
2510B：メールアドレスを確認してください。（データ入力）（初級）

リンク＆データ送信型
外部組織
初級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510B**」と入力して検索してください

＜メール＞
送信元：
<no-replay@yxwhitotupfruxxe.com>

いつも〇〇〇（ドメイン）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【メールアドレス】に関する確認手続きのご案内です。

現在、システム上の確認が必要な状態となっております。
お手数をおかけいたしますが、以下のリンクよりアカウントの確認をお願いいたします。
アカウント確認はこちら

※ 所要時間は数秒程度です。

ご不便をおかけし申し訳ございませんが、何卒ご理解・ご協力のほどよろしくお願い申し上げます。
ご不明な点がございましたら、下記カスタマーサポートまでお気軽にお問い合わせください。

■ 〇〇〇（ドメイン）カスタマーサポート
受付時間：8:00～18:00（年中無休）
フリーダイヤル：0120-86-0000
有料番号：03-6385-0000（携帯・IP電話可）

今後とも変わらぬご愛顧を賜りますよう、心よりお願い申し上げます。
敬具

〇〇〇（ドメイン）株式会社
カスタマーサポートセンター
Copyright © 2025 All Rights Reserved.

メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

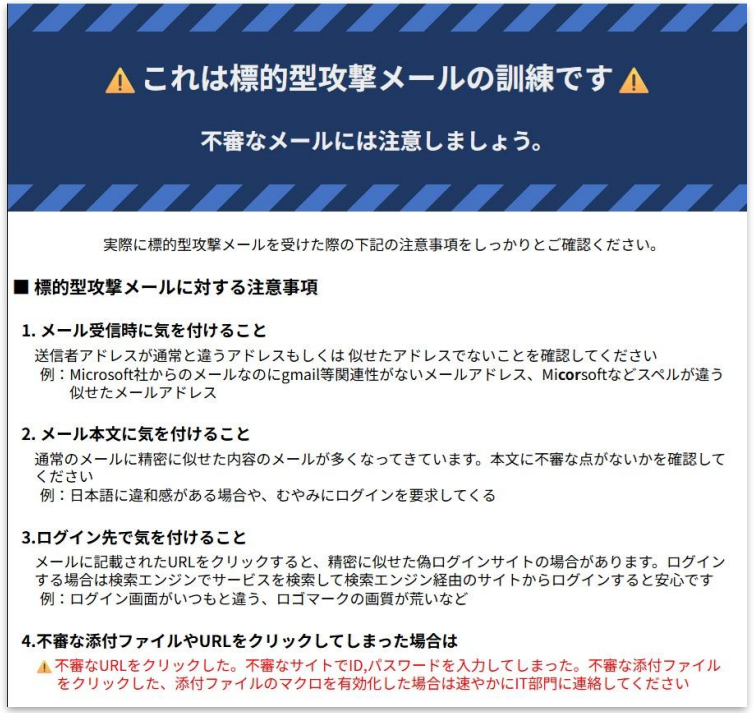
リンク
クリック

＜リンク先画面（*1）＞

以下の操作をすると「**データ送信**」**が記録**され、種明かし画面が表示。
・「ファイルダウンロード認証」にメールアドレス、パスワード入力し「ダウンロード」をクリックする。
・「ファイルダウンロード認証」にメールアドレス、パスワード入力した状態で表示されているいずれかのサービスのアイコンをクリックする

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



⚠ これは標的型攻撃メールの訓練です ⚠

不審なメールには注意しましょう。

実際に標的型攻撃メールを受けた際の下記の注意事項をしっかりとご確認ください。

■ 標的型攻撃メールに対する注意事項

1. メール受信時に気を付けること
送信者アドレスが通常と違うアドレスもしくは 似せたアドレスでないことを確認してください
例：Microsoft社からのメールなのにgmail等関連性がないメールアドレス、Micorsoftなどスペルが違う似せたメールアドレス

2. メール本文に気を付けること
通常のメールに精密に似せた内容のメールが多くなってきています。本文に不審な点がないかを確認してください
例：日本語に違和感がある場合や、むやみにログインを要求してくる

3.ログイン先で気を付けること
メールに記載されたURLをクリックすると、精密に似せた偽ログインサイトの場合があります。ログインする場合は検索エンジンでサービスを検索して検索エンジン経由のサイトからログインすると安心です
例：ログイン画面がいつもと違う、ロゴマークの画質が荒いなど

4.不審な添付ファイルやURLをクリックしてしまった場合は
⚠ 不審なURLをクリックした。不審なサイトでID,パスワードを入力してしまった。不審な添付ファイルをクリックした、添付ファイルのマクロを有効化した場合は速やかにIT部門に連絡してください

シナリオ名：
2510A：メールアドレスを確認してください。（データ入力）（上級）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510A**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

いつも○○○(ドメイン) 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 **[メールアドレス]** に関する確認手続きのご案内です。

現在、システム上の確認が必要な状態となっております。
お手数をおかけいたしますが、以下のリンクよりアカウントの確認をお願いいたします。

アカウント確認ページはこちら

※ 所要時間は数秒程度です。

ご不便をおかけし申し訳ございませんが、何卒ご理解・ご協力のほどよろしくお願い申し上げます。
ご不明な点がございましたら、下記カスタマーサポートまでお気軽にお問い合わせください。

■ ○○○（ドメイン）カスタマーサポート
受付時間：9:00～18:00（年中無休）
フリーダイヤル：0120-86-0000
有料番号：03-6385-0000（携帯・IP電話可）

今後とも変わらぬご愛顧を賜りますよう、心よりお願い申し上げます。
敬具

○○○（ドメイン）株式会社
カスタマーサポートセンター
Copyright © 2025 All Rights Reserved.

メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

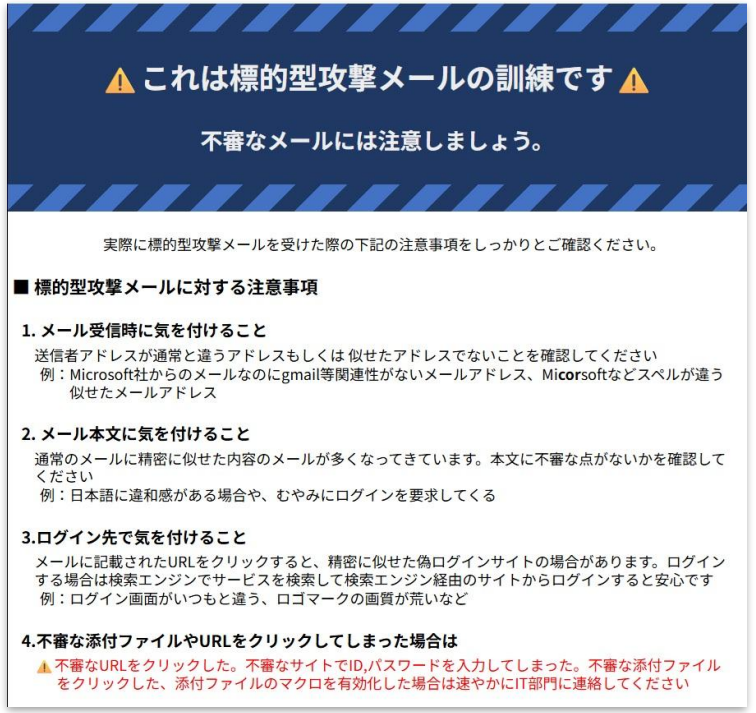
リンク
クリック

＜リンク先画面（*1）＞

以下の操作をすると「**データ送信**」**が記録**され、種明かし画面が表示。
・「ファイルダウンロード認証」にメールアドレス、パスワード入力し「ダウンロード」をクリックする。
・「ファイルダウンロード認証」にメールアドレス、パスワード入力した状態で表示されているいずれかのサービスのアイコンをクリックする

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



⚠ これは標的型攻撃メールの訓練です ⚠

不審なメールには注意しましょう。

実際に標的型攻撃メールを受けた際の下記の注意事項をしっかりとご確認ください。

■ 標的型攻撃メールに対する注意事項

1. メール受信時に気を付けること
送信者アドレスが通常と違うアドレスもしくは 似せたアドレスでないことを確認してください
例：Microsoft社からのメールなのにgmail等関連性がないメールアドレス、Micorsoftなどスペルが違う似せたメールアドレス

2. メール本文に気を付けること
通常のメールに精密に似せた内容のメールが多くなってきています。本文に不審な点がないかを確認してください
例：日本語に違和感がある場合や、むやみにログインを要求してくる

3.ログイン先で気を付けること
メールに記載されたURLをクリックすると、精密に似せた偽ログインサイトの場合があります。ログインする場合は検索エンジンでサービスを検索して検索エンジン経由のサイトからログインすると安心です
例：ログイン画面がいつもと違う、ロゴマークの画質が荒いなど

4.不審な添付ファイルやURLをクリックしてしまった場合は
⚠ 不審なURLをクリックした。不審なサイトでID,パスワードを入力してしまった。不審な添付ファイルをクリックした、添付ファイルのマクロを有効化した場合は速やかにIT部門に連絡してください

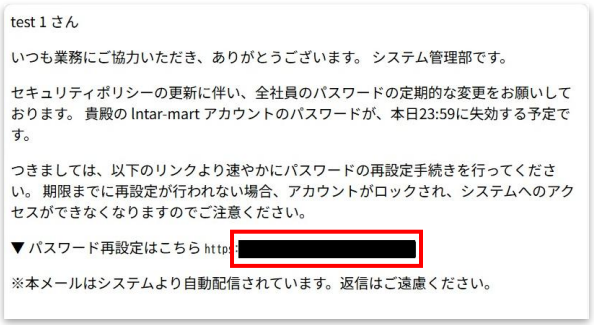
シナリオ名：
2507I：【緊急・要対応】Intar-mart アカウントの パスワードがまもなく失効します（データ入力）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507I**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>



メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

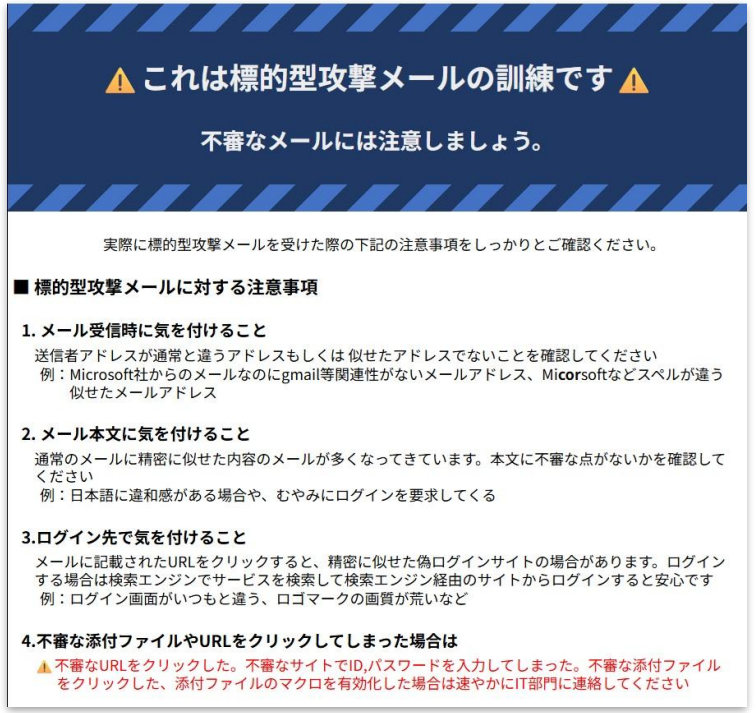
＜リンク先画面（*1）＞

リンク クリック

データ 送信

ユーザー名、パスワード入力し、「ログイン」をクリックすると「**データ送信**」**が記録**され、種明かし画面が表示。

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



シナリオ名：
2507G：FadEX配達のお知らせ（QRコード+データ入力）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507G**」と入力して検索してください

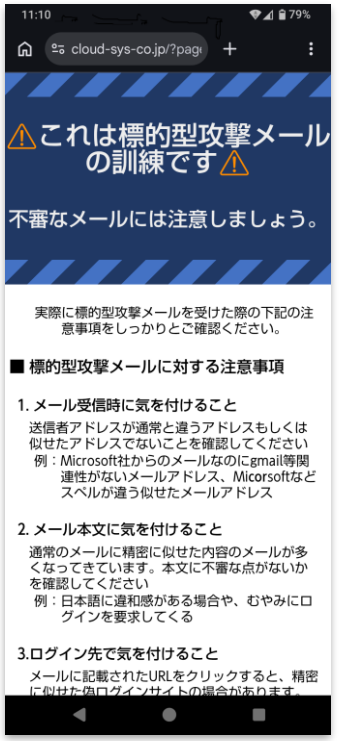
＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

リンク
クリック

＜リンク先画面（*1）＞

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



メールのQRコードをスマートフォンで読み取り、表示されるURLをタップすると「**リンククリック**」**が記録**され、リンク先画面が表示

ユーザーIDとパスワードを入力を促す画面が表示されます。
ID、パスワードを入力し「ログイン」をクリックすると「**データ送信**」**が記録**され、スマートフォンの画面に種明かし画面が表示

シナリオ名：
2507E：ServiceNowチケット通知（データ入力）

リンク＆データ送信型
通知系
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507E**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

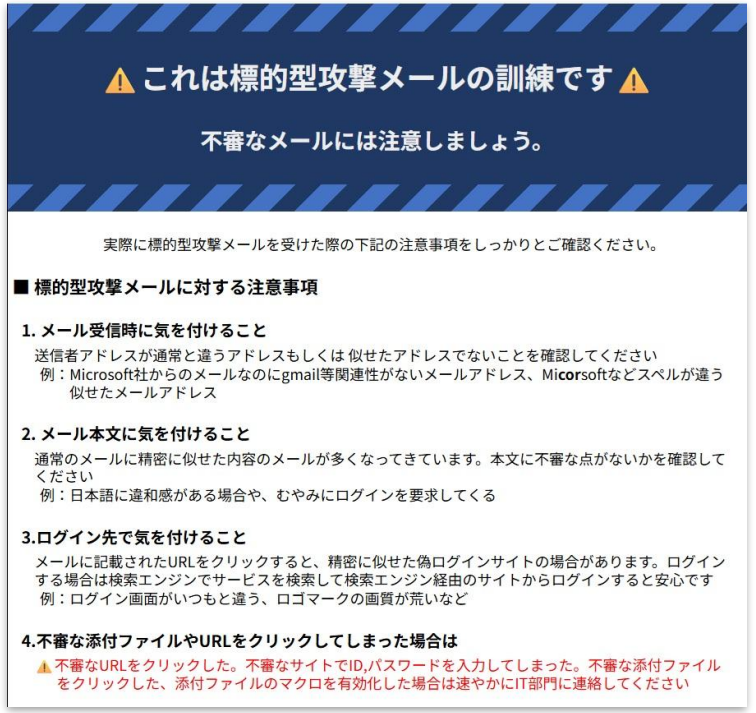
メール中の「インシデント表示」をクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

＜リンク先画面（*1）＞

リンク
クリック

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



ユーザー名、パスワード入力し、「ログイン」をクリックすると「**データ送信**」**が記録**され、種明かし画面が表示。

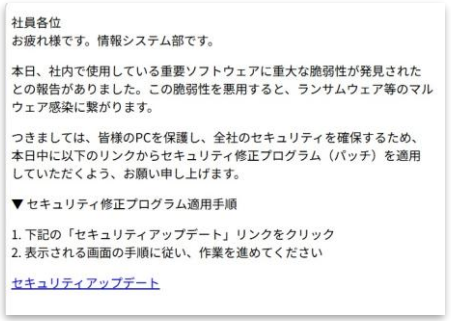
シナリオ名：
2510I：セキュリティ修正プログラム適用のお願い（CF2-2）

リンク＆データ送信型
社内業務連絡
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510I**」と入力して検索してください

＜メール＞
送信元：情報システム部
<info@system-grp.com>



メール中のリンクをクリックすると、
「**リンククリック**」**が記録**され、リンク先画面が表示される

＜リンク先画面（*1）＞

リンク
クリック

チェックボックスに
チェックを入れると、
下に画面が展開される

キーボードから
「CTRL＋R」

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定

キーボードから「**CTRL＋R**」を入力すると、
「**データ送信**」**が記録**され、種明かし画面が表示される（CTRL+V、Enterはダミー）

シナリオ名：
2510H：セキュリティ修正プログラム適用のお願い（CF2-1）

リンク＆データ送信型
社内業務連絡
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510H**」と入力して検索してください

＜メール＞
送信元：情報システム部
<info@system-grp.com>

社員各位
お疲れ様です。情報システム部です。

本日、社内で使用している重要ソフトウェアに重大な脆弱性が発見されたとの報告がありました。この脆弱性を悪用すると、ランサムウェア等のマルウェア感染に繋がります。

つきましては、皆様のPCを保護し、全社のセキュリティを確保するため、本日中に以下のリンクからセキュリティ修正プログラム（パッチ）を適用していただくよう、お願い申し上げます。

▼セキュリティ修正プログラム適用手順

1. 下記の「セキュリティアップデート」リンクをクリック
2. 表示される画面の手順に従い、作業を進めてください

セキュリティアップデート

リンク
クリック

メール中のリンクをクリックすると、
「**リンククリック**」**が記録**され、リンク先画面が表示される

＜リンク先画面（*1）＞

チェックボックスに
チェックを入れると、
下に画面が展開される

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定

キーボードから
「CTRL＋R」

データ
送信

キーボードから「**CTRL＋R**」を入力すると、
「**データ送信**」**が記録**され、種明かし画面が表示される（CTRL+V、Enterはダミー）

シナリオ名：
2510G：Micorsoft 365 アカウントのセキュリティ更新（CF1）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510G**」と入力して検索してください

＜メール＞
送信元：
<IT@system-grp.com>

メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

リンク
クリック

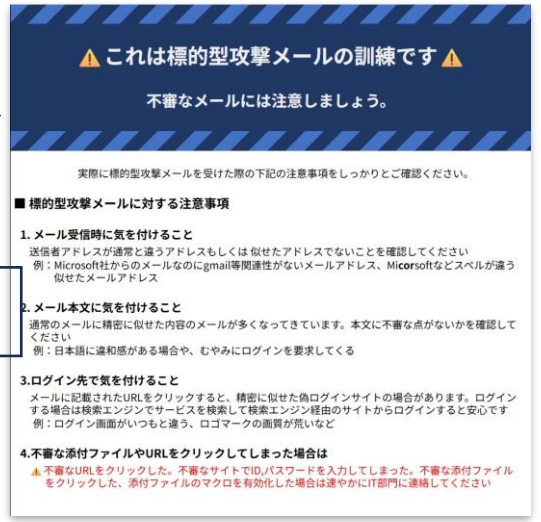
＜リンク先画面（*1）＞

チェックボックスに
チェックを入れると、
画面自動切換

「Windows＋R」で
開く画面

コピー＆ペースト

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



データ
送信

表示される画面に沿って操作すると、
「**データ送信**」**が記録**され、種明かし画面が表示。
※操作：キーボードから「**Windows＋R**」を入力し、
画面に表示されている文字列（URL）をコピー
＆ペーストして実行

※ご注意）本パターンのシナリオをカスタマイズされる場合は、
本シナリオでインポートしたページを直接編集ください。
リンク先画面(*1)のリダイレクト先設定で別の「URL」や「Page2」を指定すると、
「データ送信」が記録がされません）。

シナリオ名：
2510F：【緊急】Windows Updateのお願い（CF1）

リンク＆データ送信型
社内業務連絡
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510F**」と入力して検索してください

＜メール＞
送信元：情報システム部
<info@system-grp.com>

従業員各位

マイクロソフト社よりEdgeやOutlookに関わる
緊急のWindows updateが公開されました。

EdgeやOutlookの脆弱性が見つかりました。
今回のWindows updateではゼロデイ脆弱性に対応し、
複数の脆弱性が修正されています。

セキュリティリスクが高いためWindows Updateの
実施をお願いします。

Windows Updateの方法は以下よりご確認ください。

Windows Update

以上、よろしくお願いします。

メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

リンク
クリック

＜リンク先画面（*1）＞

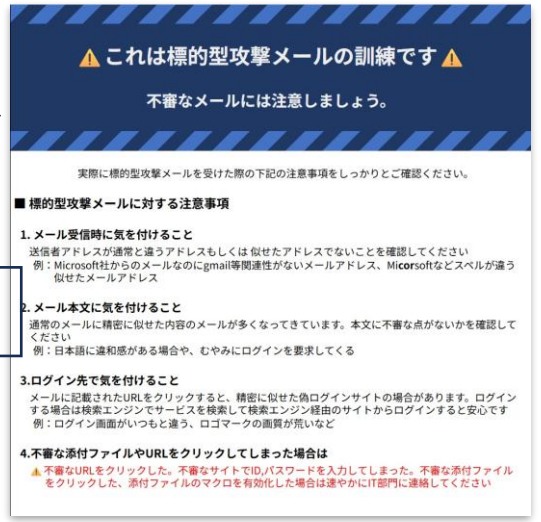
チェックボックスに
チェックを入れると、
画面自動切換

「Windows＋R」で
開く画面

コピー＆ペースト

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



表示される画面に沿って操作すると、
「**データ送信**」**が記録**され、種明かし画面が表示。
※操作：キーボードから「**Windows＋R**」を入力し、
画面に表示されている文字列（URL）をコピー
＆ペーストして実行

※ご注意）本パターンのシナリオをカスタマイズされる場合は、
本シナリオでインポートしたページを直接編集ください。
リンク先画面(*1)のリダイレクト先設定で別の「URL」や「Page2」を指定すると、
「データ送信」が記録がされません）。

シナリオ名：
2510E：【緊急・重要】セキュリティ更新プログラムの適用に関するお願い （CF1）

リンク＆データ送信型
社内業務連絡
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2510E**」と入力して検索してください

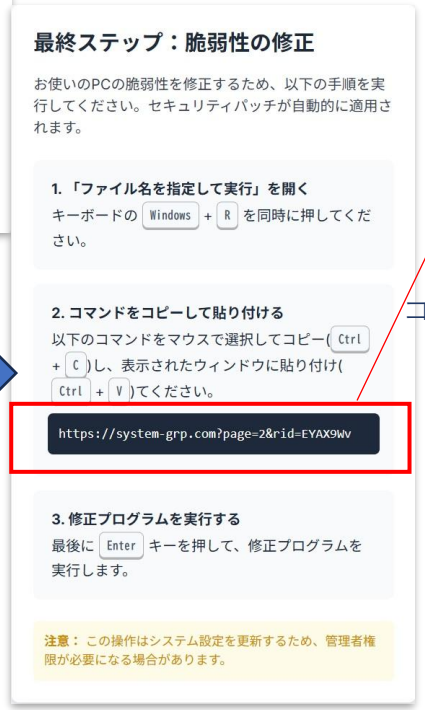
＜メール＞
送信元：情報システム部
<info@system-grp.com>

メール中のリンクを
クリックすると
「**リンククリック**」
が記録され、
リンク先画面が表示

＜リンク先画面（*1）＞

リンク
クリック

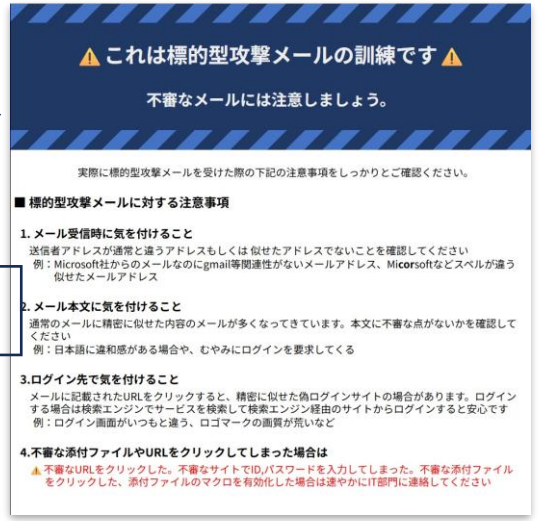
チェックボックスに
チェックを入れると、
画面自動切換



「Windows＋R」で
開く画面

コピー＆ペースト

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



データ
送信

表示される画面に沿って操作すると、
「**データ送信**」**が記録**され、種明かし画面が表示。
※操作：キーボードから「**Windows＋R**」を入力し、
画面に表示されている文字列（URL）をコピー
＆ペーストして実行

※ご注意）本パターンのシナリオをカスタマイズされる場合は、
本シナリオでインポートしたページを直接編集ください。
リンク先画面(*1)のリダイレクト先設定で別の「URL」や「Page2」を指定すると、
「データ送信」が記録がされません）。

シナリオ名：
2507U：最大50,000ポイントプレゼント（サポート詐欺１）

リンク＆データ送信型
その他
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507U**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

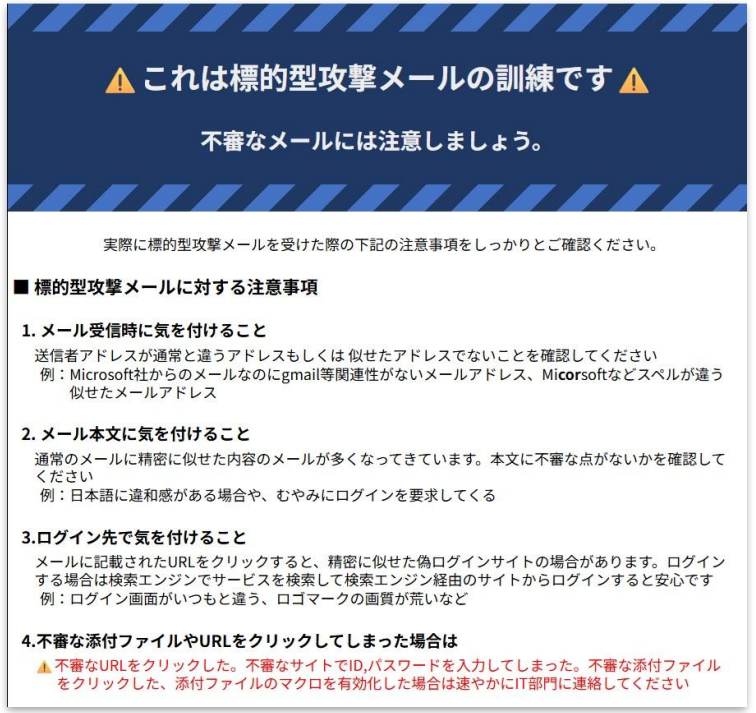
リンク
クリック

「今すぐ参加」をクリックすると
「**リンククリック**」**が記録**され、
リンク先画面を表示。

＜リンク先画面（*1）＞

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



「問い合わせはこちら」をクリックすると「**データ送信**」**が記録**され、
種明かし画面が表示。

シナリオ名：
2507T：最大50,000ポイントプレゼント（サポート詐欺２）

リンク＆データ送信型
その他
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507T**」と入力して検索してください

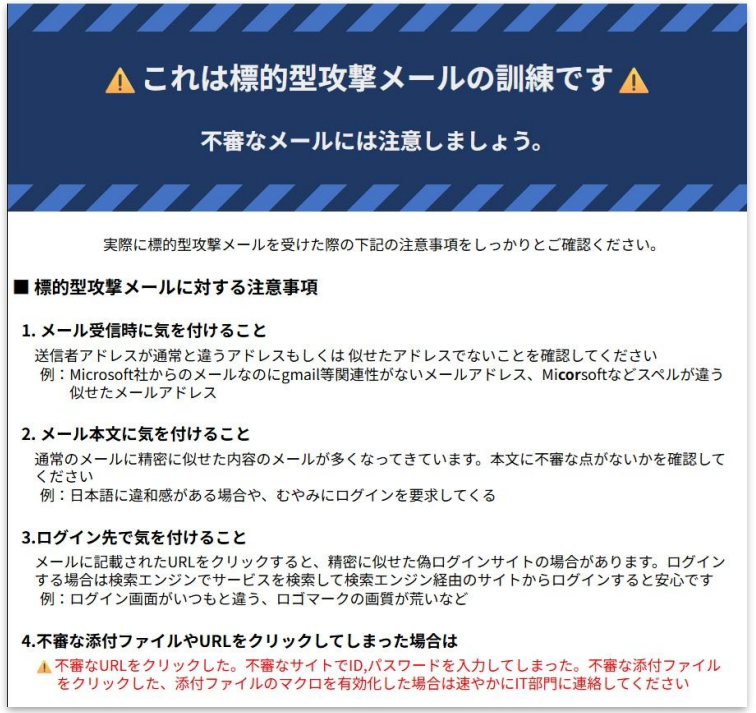
＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

リンク
クリック

＜リンク先画面（*1）＞

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



「今すぐ参加」をクリックすると
「**リンククリック**」**が記録**され、
リンク先画面を表示。

「問い合わせはこちら」をクリックすると「**データ送信**」**が記録**され、
種明かし画面が表示。

シナリオ名：
2507S：最大50,000ポイントプレゼント（サポート詐欺３）

リンク＆データ送信型
その他
上級

KIS SECURITY

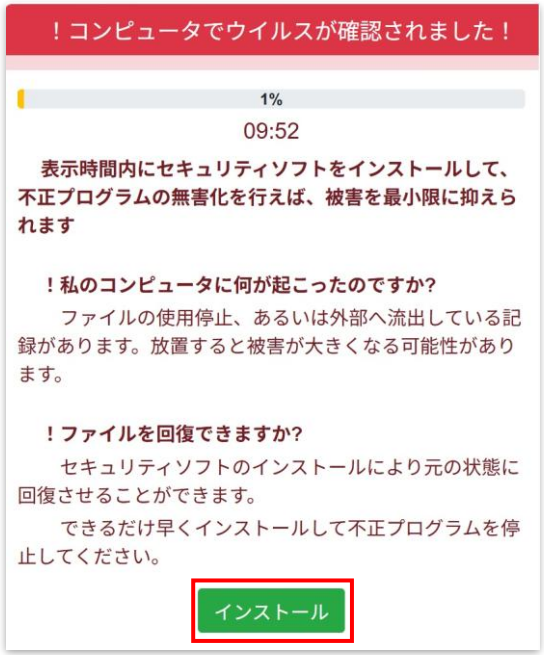
シナリオギャラリーでの検索方法：検索窓に「**2507S**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

リンク
クリック

「今すぐ参加」をクリックすると
「**リンククリック**」**が記録**され、
リンク先画面を表示。

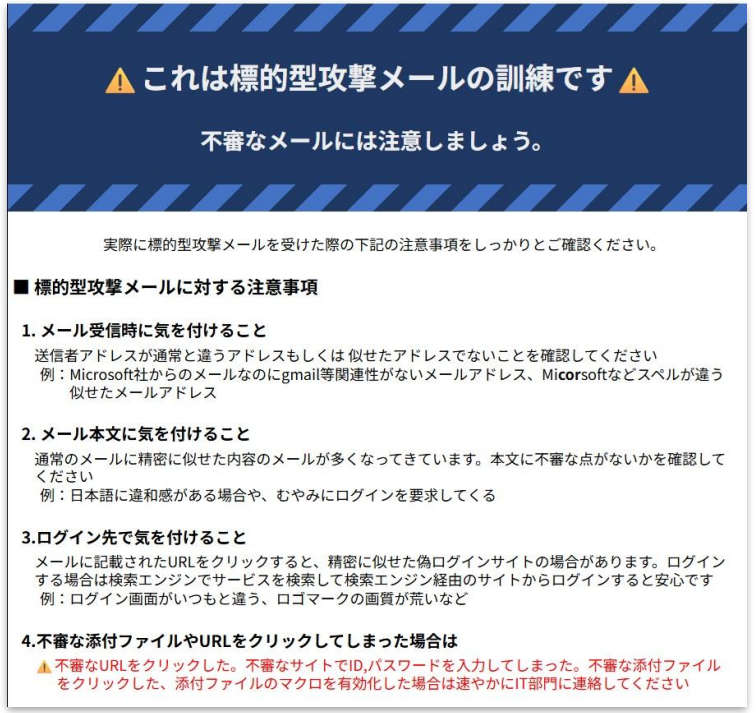
＜リンク先画面（*1）＞



データ
送信

「インストール」をクリックすると「**データ送信**」**が記録**され、
種明かし画面が表示。

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



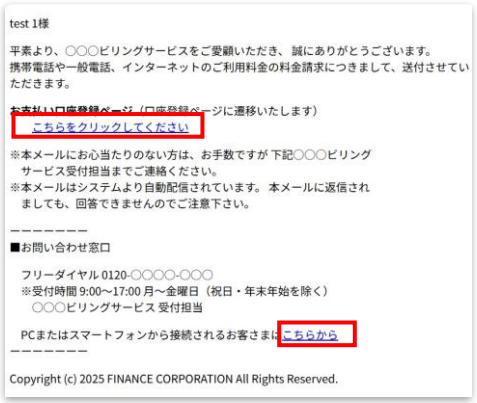
シナリオ名：
2507R：お支払い口座登録のお願い（サポート詐欺１）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507R**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>



リンク
クリック

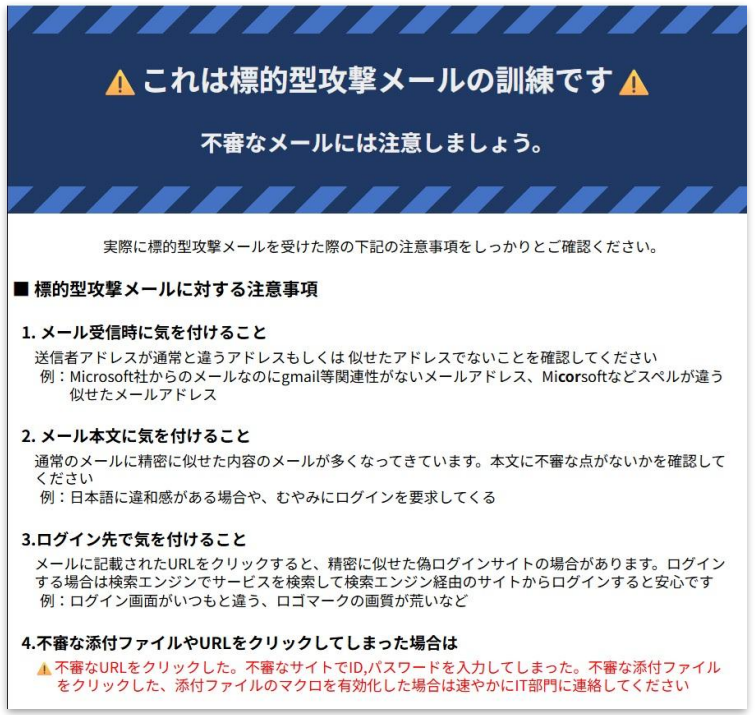
メール中の「こちらをクリックしてください」又は、「こちらから」をクリックすると「**リンククリック**」**が記録**され、リンク先画面を表示。

＜リンク先画面（*1）＞

データ
送信

「問い合わせはこちら」をクリックすると「**データ送信**」**が記録**され、種明かし画面が表示。

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



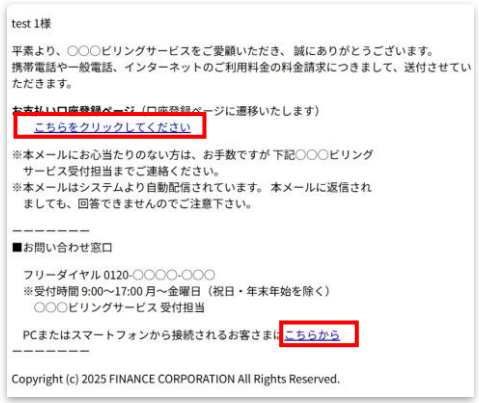
シナリオ名：
2507Q：お支払い口座登録のお願い（サポート詐欺２）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507Q**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>


test 1様

平素より、〇〇〇ビリングサービスをご愛顧いただき、誠にありがとうございます。
携帯電話や一般電話、インターネットのご利用料金の料金請求につきまして、送付させていただきます。

お支払い口座登録ページ（口座登録ページに遷移いたします）
こちらをクリックしてください

※本メールにお心当たりのない方は、お手数ですが 下記〇〇〇ビリング
サービス受付担当までご連絡ください。
※本メールはシステムより自動配信されています。本メールに返信されましても、回答できませんのでご注意下さい。

――――――――
■お問い合わせ窓口

フリーダイヤル 0120-〇〇〇〇-〇〇〇
※受付時間 9:00～17:00 月～金曜日（祝日・年末年始を除く）
〇〇〇ビリングサービス 受付担当

PCまたはスマートフォンから接続されるお客さまはこちらから
――――――――
Copyright (c) 2025 FINANCE CORPORATION All Rights Reserved.

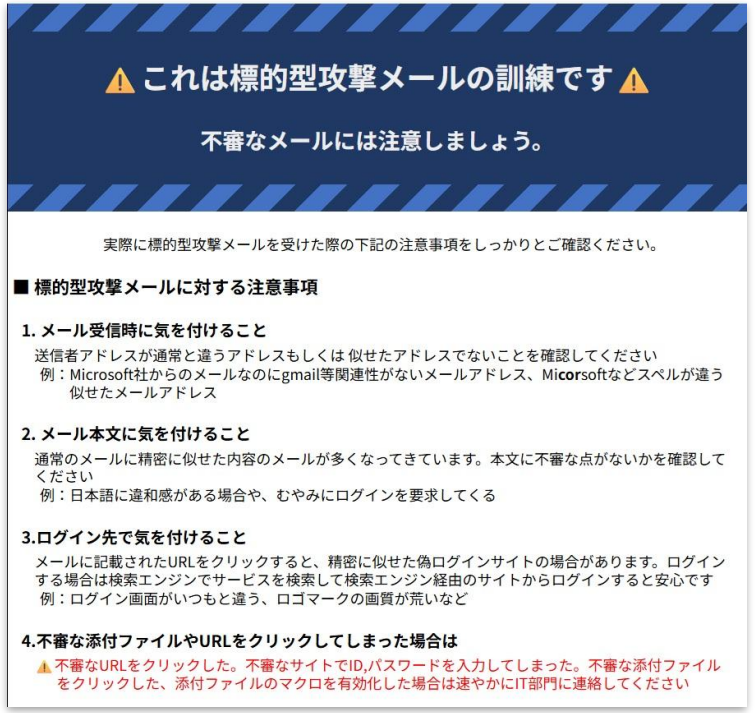
リンク
クリック

メール中の「こちらをクリックしてください」又は、「こちらから」をクリックすると「**リンククリック**」**が記録**され、リンク先画面を表示。

＜リンク先画面（*1）＞

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定


⚠ これは標的型攻撃メールの訓練です ⚠

不審なメールには注意しましょう。

実際に標的型攻撃メールを受けた際の下記の注意事項をしっかりとご確認ください。

■ 標的型攻撃メールに対する注意事項

1. メール受信時に気を付けること
送信者アドレスが通常と違うアドレスもしくは 似せたアドレスでないことを確認してください
例：Microsoft社からのメールなのにgmail等関連性がないメールアドレス、Micorsoftなどスペルが違う似せたメールアドレス

2. メール本文に気を付けること
通常のメールに精密に似せた内容のメールが多くなってきています。本文に不審な点がないかを確認してください
例：日本語に違和感がある場合や、むやみにログインを要求してくる

3.ログイン先で気を付けること
メールに記載されたURLをクリックすると、精密に似せた偽ログインサイトの場合があります。ログインする場合は検索エンジンでサービスを検索して検索エンジン経由のサイトからログインすると安心です
例：ログイン画面がいつもと違う、ロゴマークの画質が荒いなど

4.不審な添付ファイルやURLをクリックしてしまった場合は
⚠ 不審なURLをクリックした。不審なサイトでID,パスワードを入力してしまった。不審な添付ファイルをクリックした、添付ファイルのマクロを有効化した場合は速やかにIT部門に連絡してください

「問い合わせはこちら」をクリックすると「**データ送信**」**が記録**され、種明かし画面が表示。

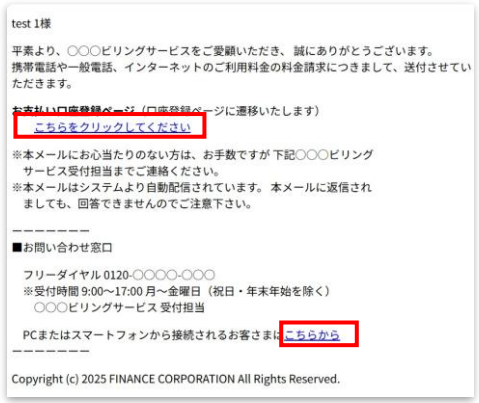
シナリオ名：
2507P：お支払い口座登録のお願い（サポート詐欺３）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507P**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>



test 1様

平素より、○○○ビリングサービスをご愛顧いただき、誠にありがとうございます。
携帯電話や一般電話、インターネットのご利用料金の料金請求につきまして、送付させていただきます。

お支払い口座登録ページ（口座登録ページに遷移いたします）
こちらをクリックしてください

※本メールにお心当たりのない方は、お手数ですが 下記○○○ビリング
サービス受付担当までご連絡ください。
※本メールはシステムより自動配信されています。本メールに返信されましても、回答できませんのでご注意下さい。

ーーーーーーー
■お問い合わせ窓口

フリーダイヤル 0120-○○○○-○○○
※受付時間 9:00～17:00 月～金曜日（祝日・年末年始を除く）
○○○ビリングサービス 受付担当

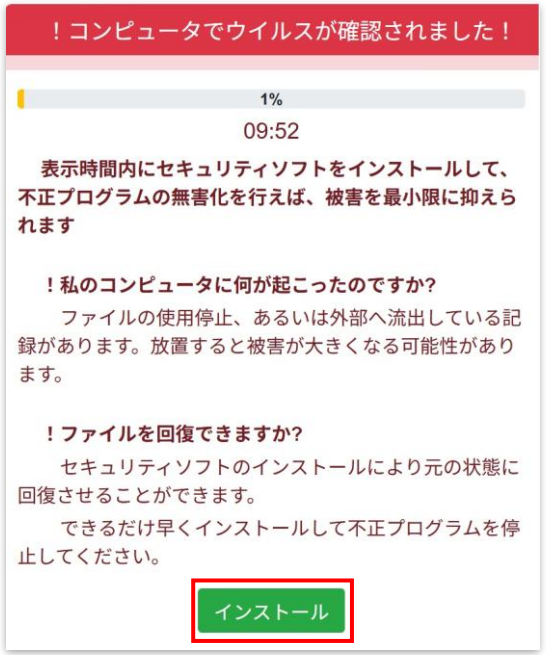
PCまたはスマートフォンから接続されるお客さまは こちらから
ーーーーーーー

Copyright (c) 2025 FINANCE CORPORATION All Rights Reserved.

リンク
クリック

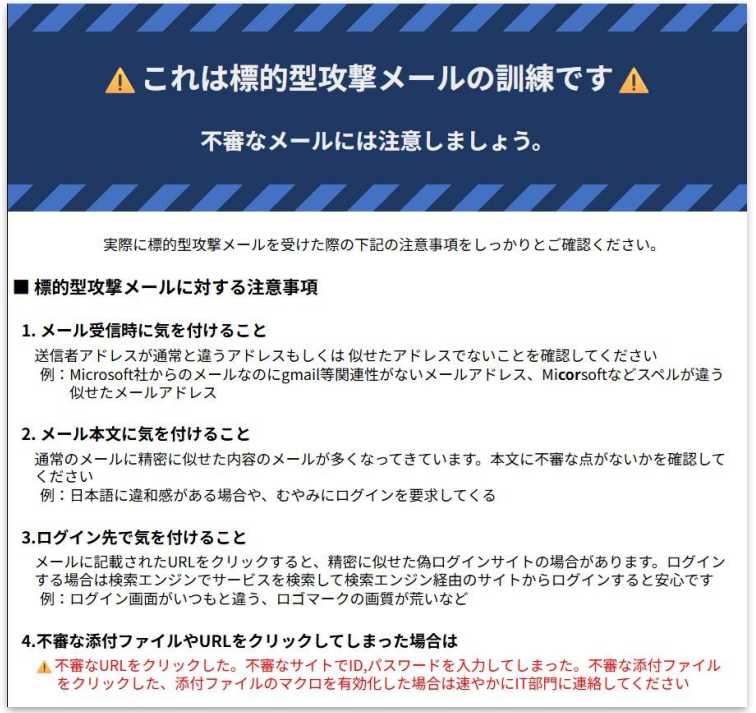
メール中の「こちらをクリックしてください」又は、「こちらから」をクリックすると「**リンククリック**」**が記録**され、リンク先画面を表示。

＜リンク先画面（*1）＞



データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



「インストール」をクリックすると「**データ送信**」**が記録**され、
種明かし画面が表示。

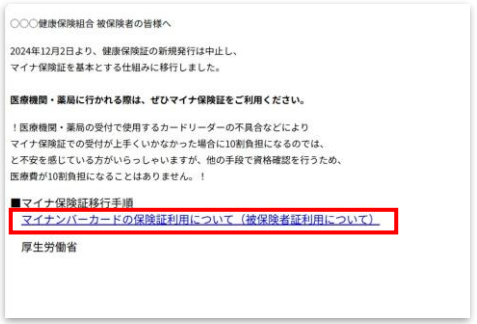
シナリオ名：
2507O：健康保険組合 被保険者の皆様へ（サポート詐欺１）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507O**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>



リンク
クリック

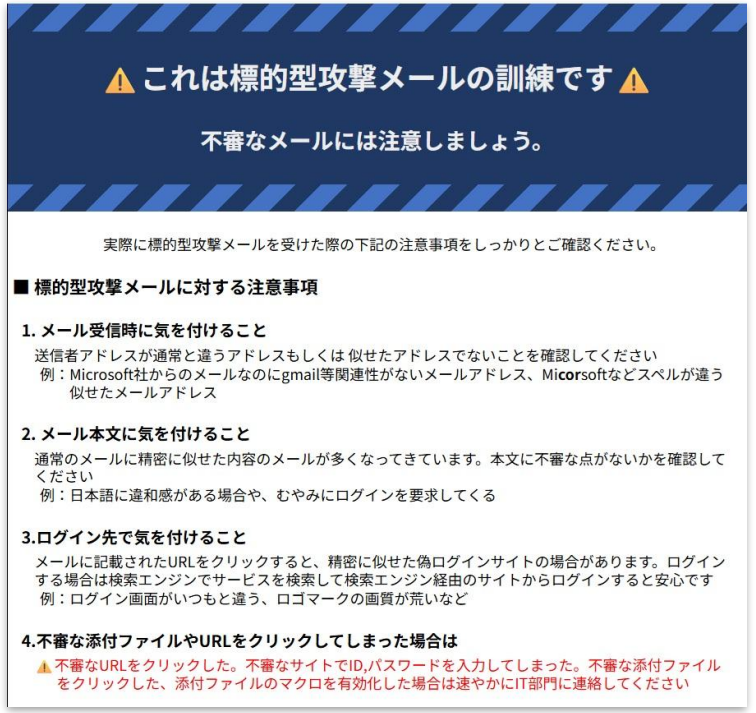
メール中のリンクをクリックする
と「**リンククリック**」**が記録**され、
リンク先画面を表示。

＜リンク先画面（*1）＞

データ
送信

「問い合わせはこちら」をクリックすると「**データ送信**」**が記録**され、
種明かし画面が表示。

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



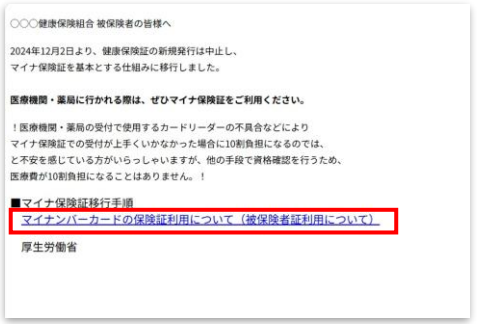
シナリオ名：
2507N：健康保険組合 被保険者の皆様へ（サポート詐欺２）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507N**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>

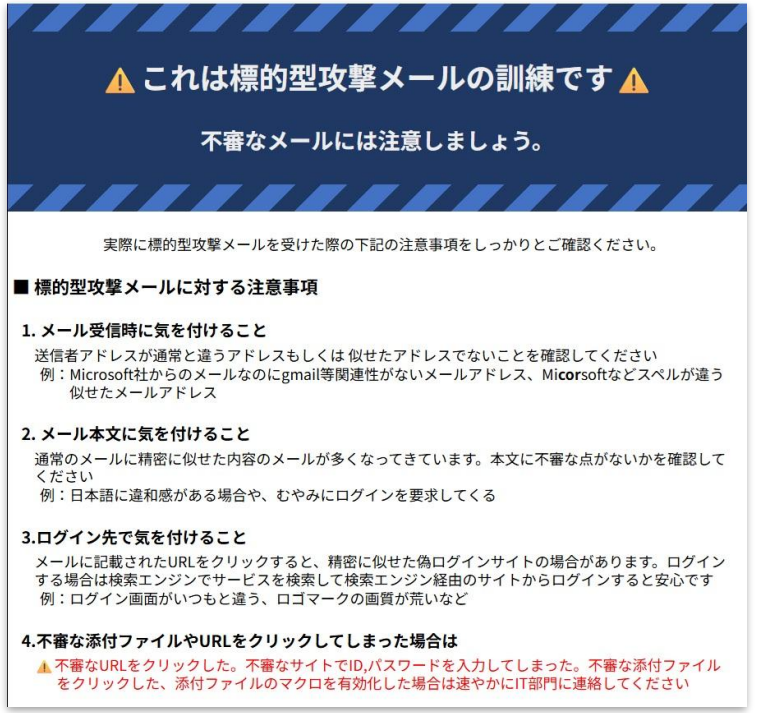


リンク
クリック

＜リンク先画面（*1）＞

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



メール中のリンクをクリックすると「**リンククリック**」**が記録**され、
リンク先画面を表示。

「問い合わせはこちら」をクリックすると「**データ送信**」**が記録**され、
種明かし画面が表示。

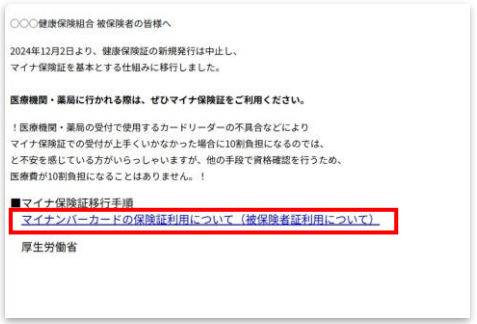
シナリオ名：
2507M：健康保険組合 被保険者の皆様へ（サポート詐欺３）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507M**」と入力して検索してください

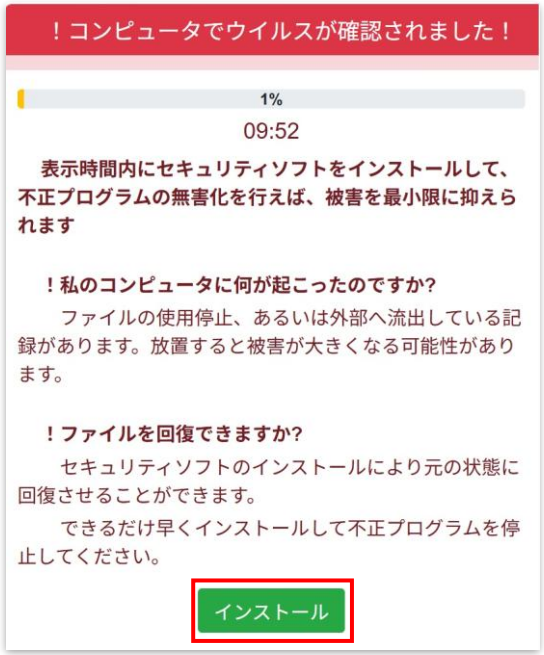
＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>



リンク
クリック

メール中のリンクをクリックすると「**リンククリック**」**が記録**され、リンク先画面を表示。

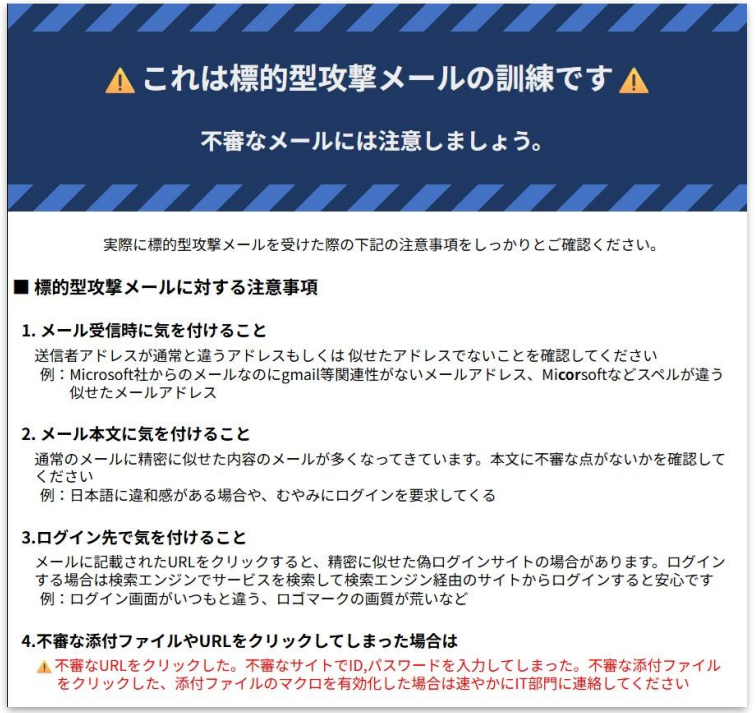
＜リンク先画面（*1）＞



データ
送信

「インストール」をクリックすると「**データ送信**」**が記録**され、種明かし画面が表示。

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



シナリオ名：
2507L：お荷物のお届けに関する重要なお知らせ（ワンポイント教育１）

リンク＆データ送信型
社外/取引先
初級

KIS SECURITY

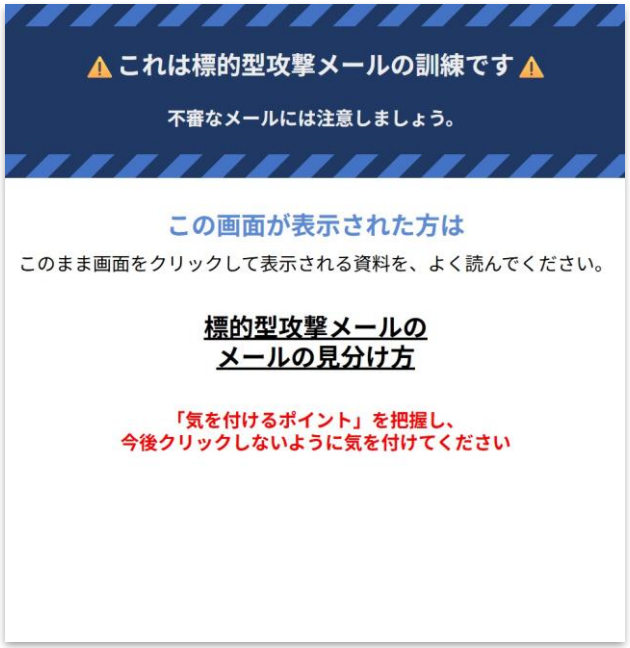
シナリオギャラリーでの検索方法：検索窓に「**2507L**」と入力して検索してください

＜メール＞
送信元：佐山運輸
<support@yxwhitotupfruxxe.com>

メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

リンク
クリック

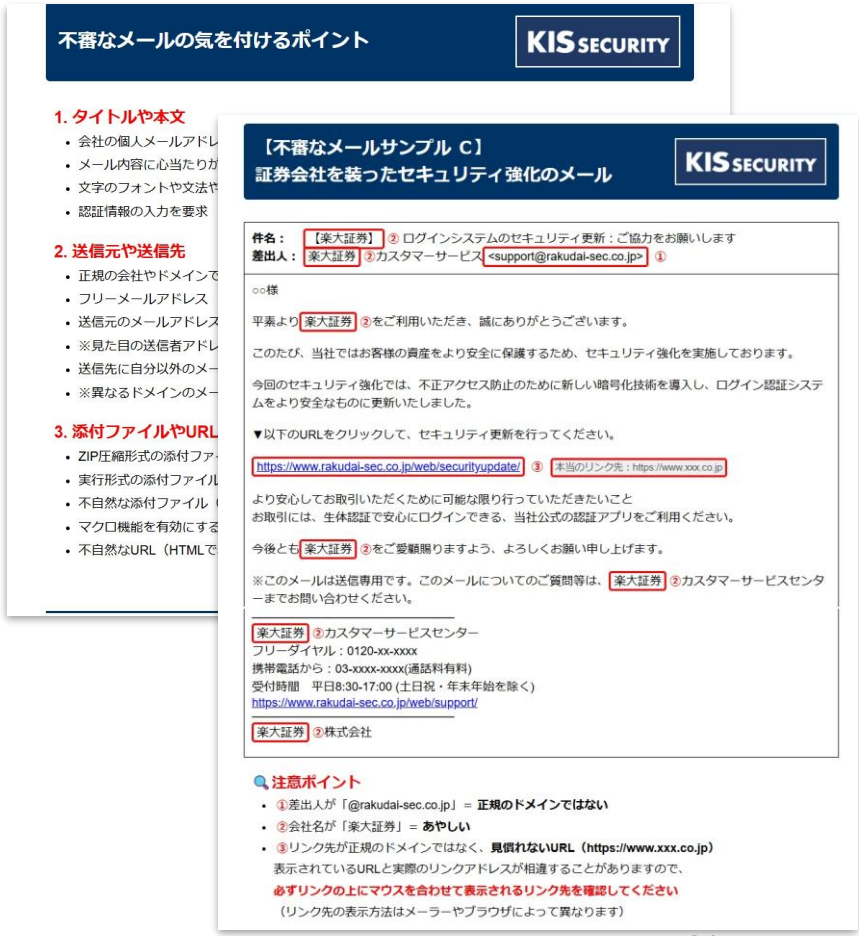
＜リンク先画面（*1）＞



クリックすると「**データ送信**」**が記録**され、教育用の画面が表示。

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



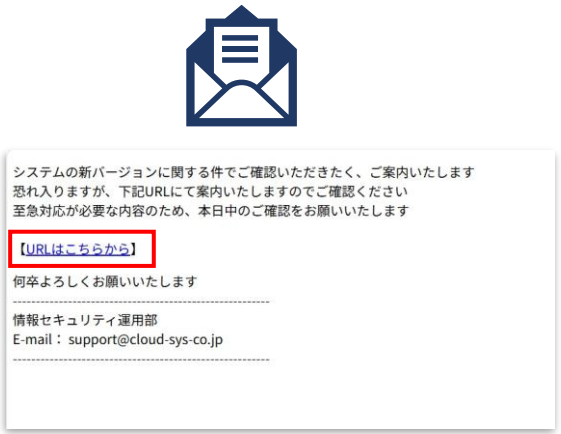
シナリオ名：
2507K：新バージョンに関する問い合わせ(ワンポイント教育２)

リンク＆データ送信型
社内業務連絡
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507K**」と入力して検索してください

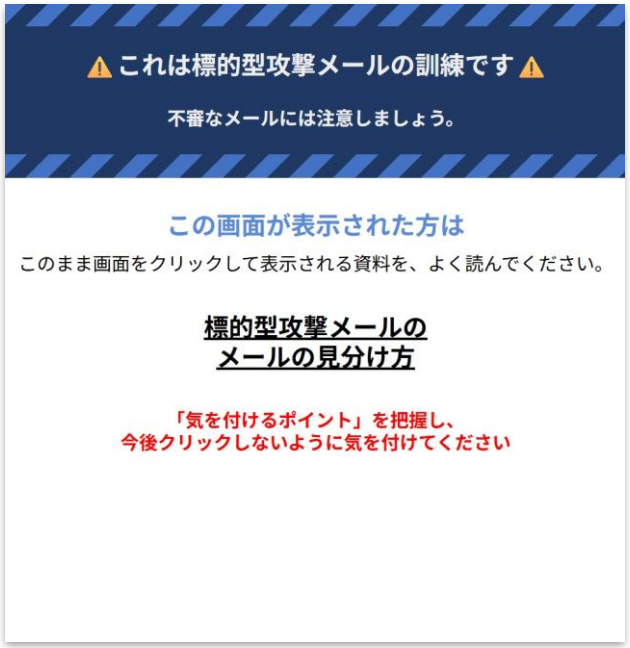
＜メール＞
送信元：情報セキュリティ運用部
<support@cloud-sys-co.jp>



メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

リンク
クリック

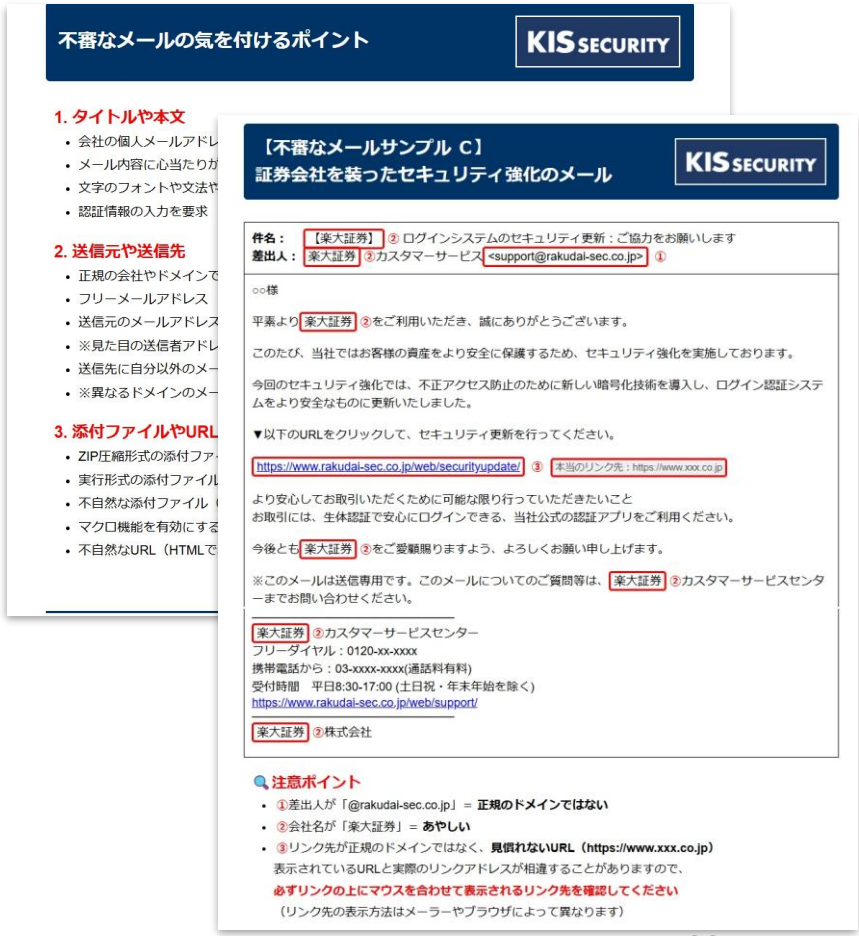
＜リンク先画面（*1）＞



クリックすると「**データ送信**」**が記録**され、教育用の画面が表示。

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定



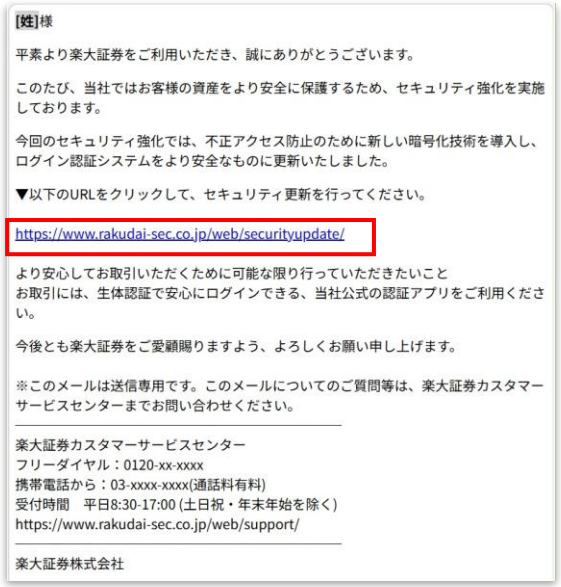
シナリオ名：
2507F：【楽大証券】ログインシステムのセキュリティ更新：ご協力をお願いします（ワンポイント教育３）

リンク＆データ送信型
外部組織
上級

KIS SECURITY

シナリオギャラリーでの検索方法：検索窓に「**2507F**」と入力して検索してください

＜メール＞
送信元：クラウドシステック
<info@cloud-sys-co.jp>


[姓]様

平素より楽大証券をご利用いただき、誠にありがとうございます。

このたび、当社ではお客様の資産をより安全に保護するため、セキュリティ強化を実施しております。

今回のセキュリティ強化では、不正アクセス防止のために新しい暗号化技術を導入し、ログイン認証システムをより安全なものに更新いたしました。

▼以下のURLをクリックして、セキュリティ更新を行ってください。

https://www.rakudai-sec.co.jp/web/securityupdate/

より安心してお取引いただくために可能な限り行っていただきたいこと
お取引には、生体認証で安心にログインできる、当社公式の認証アプリをご利用ください。

今後とも楽大証券をご愛顧賜りますよう、よろしくお願い申し上げます。

※このメールは送信専用です。このメールについてのご質問等は、楽大証券カスタマーサービスセンターまでお問い合わせください。

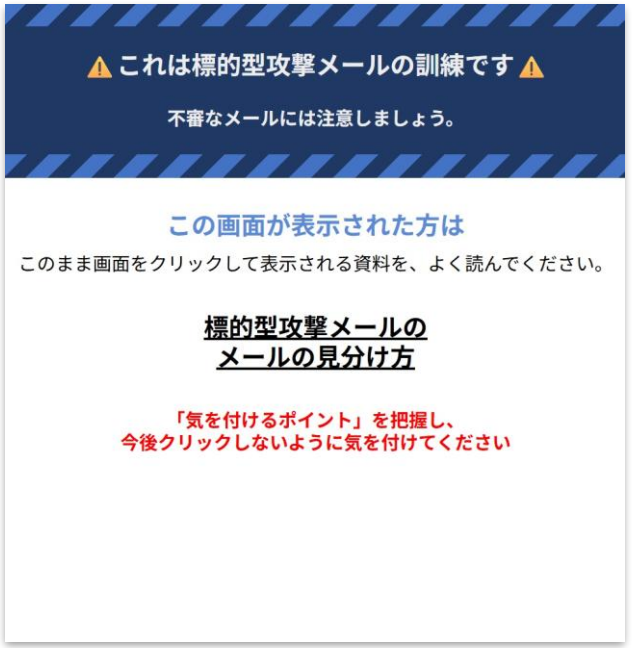
楽大証券カスタマーサービスセンター
フリーダイヤル：0120-xx-xxxx
携帯電話から：03-xxxx-xxxx(通話料有料)
受付時間　平日8:30-17:00 (土日祝・年末年始を除く)
https://www.rakudai-sec.co.jp/web/support/

楽大証券株式会社

メール中のリンクをクリックすると、「**リンククリック**」**が記録**され、リンク先画面が表示される

リンク
クリック

＜リンク先画面（*1）＞


⚠ これは標的型攻撃メールの訓練です ⚠

不審なメールには注意しましょう。

この画面が表示された方は

このまま画面をクリックして表示される資料を、よく読んでください。

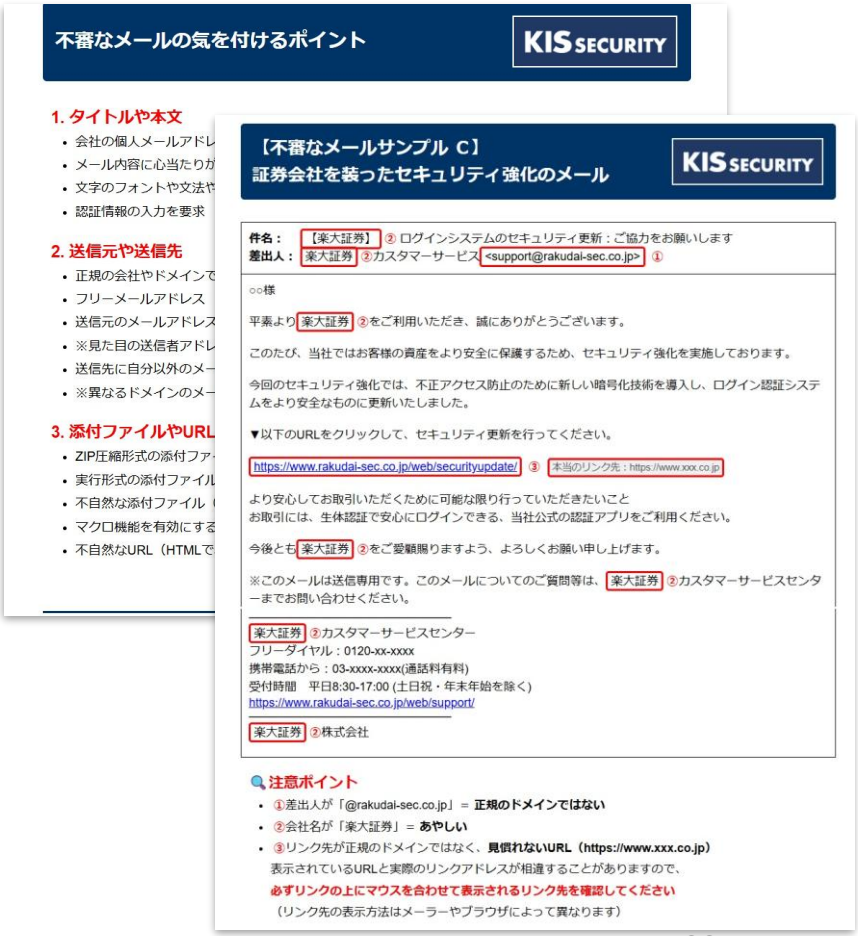
標的型攻撃メールの
メールの見分け方

「気を付けるポイント」を把握し、
今後クリックしないように気を付けてください

クリックすると「**データ送信**」**が記録**され、教育用の画面が表示。

データ
送信

＜リンク先画面(種明かし画面)＞
リンク先画面(*1)でpage2として指定


不審なメールの気を付けるポイント

KIS SECURITY

1. タイトルや本文
2. 送信元や送信先
3. 添付ファイルやURL

【不審なメールサンプル C】
証券会社を装ったセキュリティ強化のメール

KIS SECURITY

件名：【楽大証券】② ログインシステムのセキュリティ更新：ご協力をお願いします
差出人：楽大証券 ②カスタマーサービス<support@rakudai-sec.co.jp> ①

○○様

平素より楽大証券 ②をご利用いただき、誠にありがとうございます。

このたび、当社ではお客様の資産をより安全に保護するため、セキュリティ強化を実施しております。

今回のセキュリティ強化では、不正アクセス防止のために新しい暗号化技術を導入し、ログイン認証システムをより安全なものに更新いたしました。

▼以下のURLをクリックして、セキュリティ更新を行ってください。

https://www.rakudai-sec.co.jp/web/securityupdate/ ③ 本当のリンク先：https://www.xxx.co.jp

より安心してお取引いただくために可能な限り行っていただきたいこと
お取引には、生体認証で安心にログインできる、当社公式の認証アプリをご利用ください。

今後とも楽大証券 ②をご愛顧賜りますよう、よろしくお願い申し上げます。

※このメールは送信専用です。このメールについてのご質問等は、楽大証券 ②カスタマーサービスセンターまでお問い合わせください。

楽大証券 ②カスタマーサービスセンター
フリーダイヤル：0120-xx-xxxx
携帯電話から：03-xxxx-xxxx(通話料有料)
受付時間　平日8:30-17:00 (土日祝・年末年始を除く)
https://www.rakudai-sec.co.jp/web/support/

楽大証券 ②株式会社

注意ポイント
- ①差出人が「@rakudai-sec.co.jp」＝ **正規のドメインではない**
- ②会社名が「楽大証券」＝ **あやしい**
- ③リンク先が正規のドメインではなく、**見慣れないURL（https://www.xxx.co.jp）**

表示されているURLと実際のリンクアドレスが相違することがありますので、
必ずリンクの上にマウスを合わせて表示されるリンク先を確認してください
（リンク先の表示方法はメーラーやブラウザによって異なります）