明治安田

明治安田における全役職員のセキュリティ意識向上と行動変容へ向けた取組み

従来水準を「超えよう」～金融業界トップレベルのアウェアネスをめざして～

明治安田生命保険相互会社
リスク管理統括部（サイバー・システムリスク統括担当）サイバー・システムリスク統括G
中西 拓実

本日の次第

０．会社概要ー明治安田のサイバーセキュリティ

１．サイバーセキュリティは全員参加。私たちが重視する“アウェアネス”
　～生保で初のフィッシング被害。被害に遭って改めて気付いたこと～

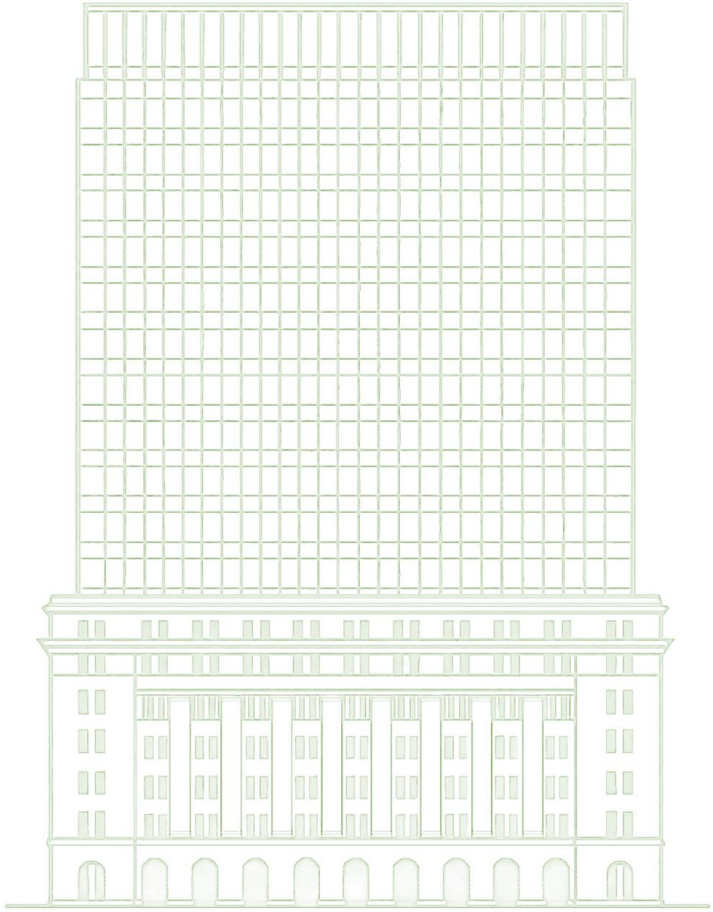
２．おカネに頼らず、独自のアイデアと想いで勝負する
　～意識向上と行動変容、具体的な４つの取り組みを紹介～

３．めざすべき好循環。「超えよう。」は終わなき永遠のテーマ

４．ビギナー向け サイバーセキュリティ企画部署で働く魅力

５．情報セキュリティが学べる！ 明治安田オリジナルボードゲーム実践

自己紹介



名前：中西（ナカニシ）　拓実（タクミ）

所属：明治安田生命保険相互会社
　　リスク管理統括部（サイバー・システムリスク統括担当）
　　サイバー・システムリスク統括G

略歴：2022年に新卒入社後、地方で支社勤務、営業を経験
　　したのち、昨年度より現職

主な参画団体：
・三菱CC研究会　サイバーセキュリティ研究部会
・フィッシング対策協議会　被害事例共有WG
・日本シーサート協議会　インシデント対応園主訓練WG
・金融ISAC　インシデント対応WG

明治安田の概要

- 明治安田では、生命保険会社の役割を超えて全国の地元へ安心と元気をお届け
- お客さまの大事な（情報・金融）資産を守るという責任が存在すると同時に、これらの基盤を活かした情報セキュリティの啓発・普及が今後の重要課題

明治安田 規模数値

グループ保険料	3兆4,094億円
連結従業員数	5万4,048人
営業職員	3万6,964人
お客さま数	1,227万人
国内営業拠点数	1,150拠点
実態・企業等との連携協定	1,174協定
海外保険グループ会社数	4カ国、6社

企業スローガン

経営理念	確かな安心を、いつまでも
企業ビジョン	信頼を得て選ばれ続ける、人に一番やさしい生命保険会社
ブランドステートメント	生命保険会社の役割を超えていく。

だから明治安田生命は、
生命保険会社の役割を超えていく。

ひとに健康を、まちに元気を。

明治安田生命から、明治安田へ。

明治安田のサイバーセキュリティ管理体制

◘ サイバー攻撃は、グループ全体に差し迫った経営課題であるとの認識のもと、「自助・共助・公助」の枠組みを活用し、２線部署主導で対応

リスク管理統括部の体制

※2025年10月時点

リスク管理統括部

オペレーショナルリスク・情報資産管理統括担当

- 情報管理態勢の整備・推進
- サードパーティ管理

サイバー・システムリスク統括担当

サイバー・システムリスク統括グループ

サイバーセキュリティ、システムリスク管理態勢の整備・推進

- ロードマップ（中期計画）策定
- サイバー人財の育成・教育計画
- 耐量子計算暗号対応の策定・推進
- インシデント発生時の経営報告
- 態勢検証、第三者評価（PMI対応含む）

サイバーセキュリティ管理グループ

サイバーセキュリティに係る管理・運用

- 経営層向けランサムウェア対応訓練
- クラウドサービス導入支援（審査）
- セキュリティソリューション導入推進
- SOC運用
- 脆弱性対応

サイバーセキュリティを担当

システムリスク・品質管理グループ

システムリスク、品質管理に係る管理・運用

基本スタンス

◘ 自助・公助・共助の視点での態勢高度化
ー積極的な社外活動・コミュニティへの参画を勧奨

◘ 「組織的対策」、「技術的対策」、「演習・評価」を３本柱とした中期計画を策定し、経営主導のもと、対策を高度化

明治安田のサイバーセキュリティ管理体制

- 明治安田のブランドステートメントは「超えよう。」
- 生命保険を販売するという従来の枠組みを超えるという想いで、ブランド名称を「明治安田生命」から「明治安田」に変更

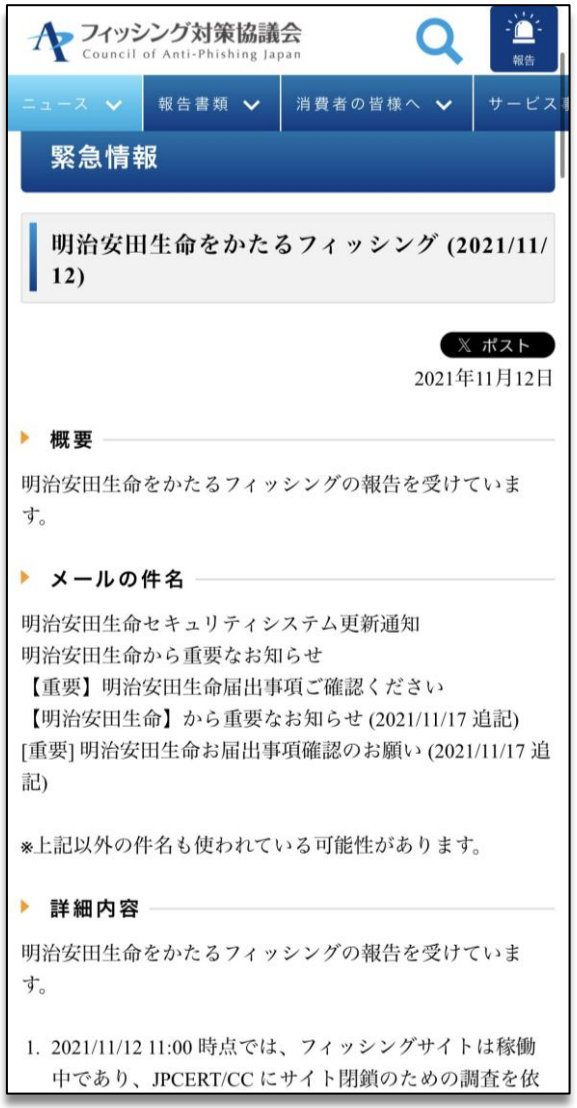
What do we go beyond in the cybersecurity field？

では、サイバー分野における「超えよう。」とは？

本日の次第

０．会社概要ー明治安田のサイバーセキュリティ
１．サイバーセキュリティは全員参加。私たちが重視する“アウェアネス”
～生保で初のフィッシング被害。被害に遭って改めて気付いたこと～
２．おカネに頼らず、独自のアイデアと想いで勝負する
～意識向上と行動変容、具体的な４つの取り組みを紹介～
３．めざすべき好循環。「超えよう。」は終わなき永遠のテーマ
４．ビギナー向け サイバーセキュリティ企画部署で働く魅力
５．情報セキュリティが学べる！明治安田オリジナルボードゲーム実践

２０２１年１１月、
生保業界で初めてフィッシング被害（実害）に遭いました



フィッシング対策協議会
Council of Anti-Phishing Japan

報告

ニュース　報告書類　消費者の皆様へ　サービス

緊急情報

明治安田生命をかたるフィッシング (2021/11/12)

X ポスト

2021年11月12日

概要

明治安田生命をかたるフィッシングの報告を受けています。

メールの件名

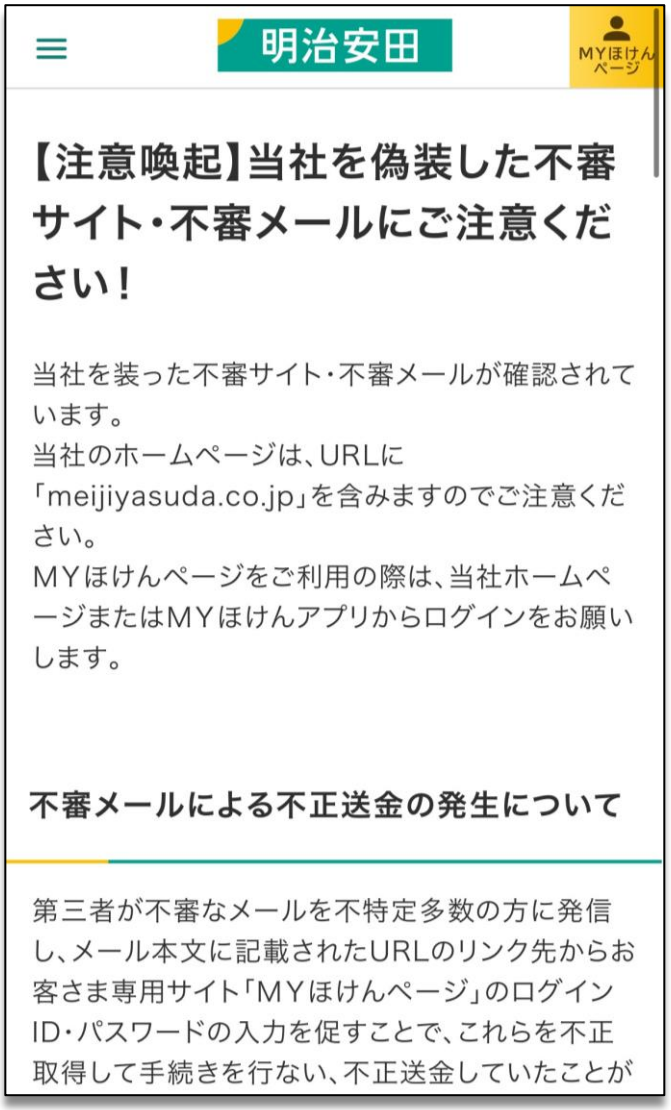
明治安田生命セキュリティシステム更新通知
明治安田生命から重要なお知らせ
【重要】明治安田生命届出事項ご確認ください
【明治安田生命】から重要なお知らせ (2021/11/17 追記)
[重要] 明治安田生命お届出事項確認のお願い (2021/11/17 追記)

※上記以外の件名も使われている可能性があります。

詳細内容

明治安田生命をかたるフィッシングの報告を受けています。

1. 2021/11/12 11:00 時点では、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依



明治安田

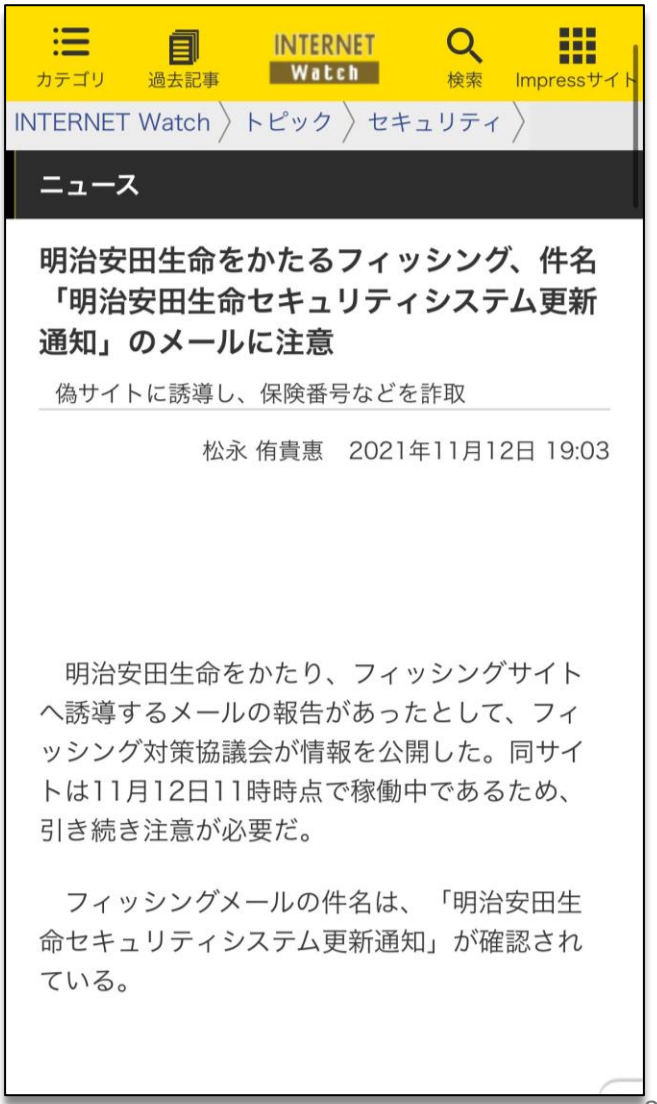
MYほけんページ

【注意喚起】当社を偽装した不審サイト・不審メールにご注意ください！

当社を装った不審サイト・不審メールが確認されています。
当社のホームページは、URLに「meijiyasuda.co.jp」を含みますのでご注意ください。
MYほけんページをご利用の際は、当社ホームページまたはMYほけんアプリからログインをお願いします。

不審メールによる不正送金の発生について

第三者が不審なメールを不特定多数の方に発信し、メール本文に記載されたURLのリンク先からお客さま専用サイト「MYほけんページ」のログインID・パスワードの入力を促すことで、これらを不正取得して手続きを行ない、不正送金していたことが



カテゴリ　過去記事　INTERNET Watch　検索　Impressサイト

INTERNET Watch 〉トピック 〉セキュリティ 〉

ニュース

明治安田生命をかたるフィッシング、件名「明治安田生命セキュリティシステム更新通知」のメールに注意

偽サイトに誘導し、保険番号などを詐取

松永 侑貴恵　2021年11月12日 19:03

明治安田生命をかたり、フィッシングサイトへ誘導するメールの報告があったとして、フィッシング対策協議会が情報を公開した。同サイトは11月12日11時時点で稼働中であるため、引き続き注意が必要だ。

フィッシングメールの件名は、「明治安田生命セキュリティシステム更新通知」が確認されている。

業界で初めてフィッシング被害に遭って改めて気付いた、サイバーセキュリティは全層参加でアウェアネス（意識）を向上させることが重要（「超えよう。」の答え）

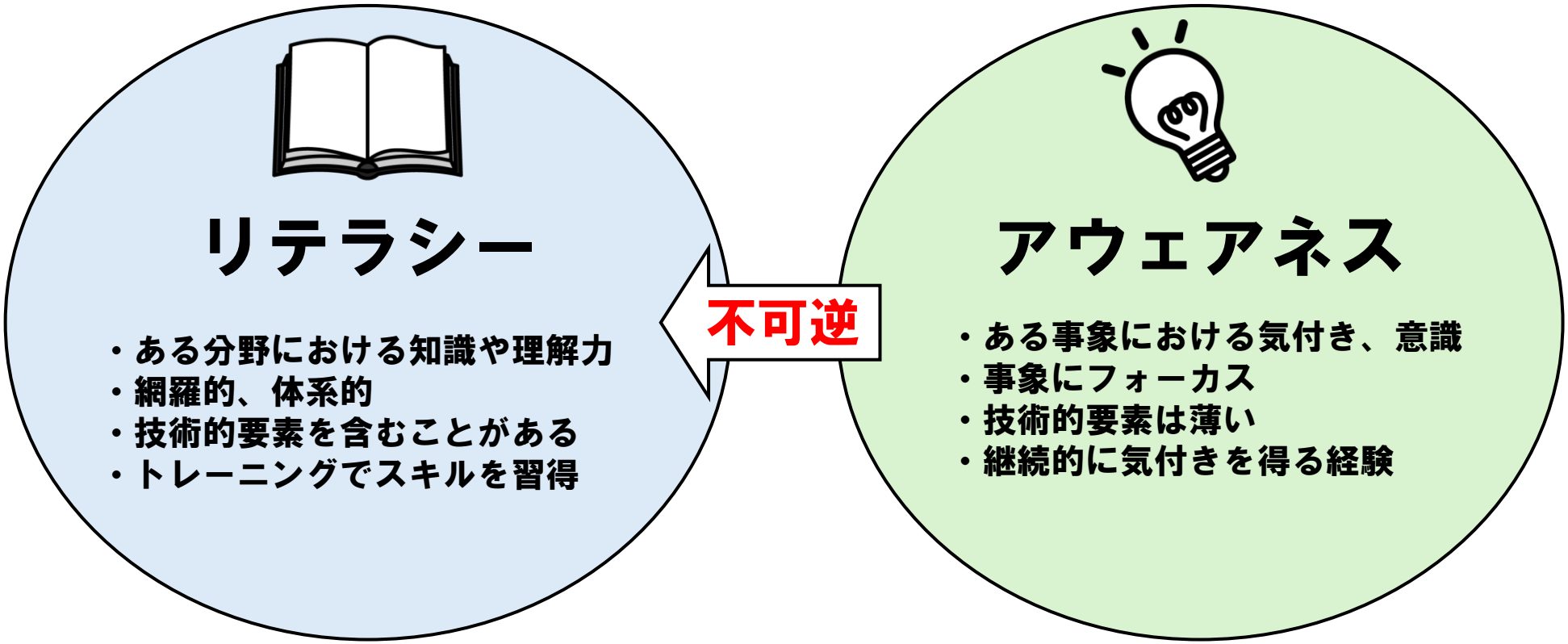
全役職員において

- セキュリティに対する当たり前のレベルをあげること。
  そのために、アウェアネス醸成のデザインが必要

さらに、担当者として、会社として

- 全国の営業職員・お客さまの存在を強く意識し、ひろく社会に貢献できる啓発活動ができないか考える
- 社外で同じ志を持つ仲間を探し、自分たちだけでできないことを可能にする（共助・公助）

一般職員がまず身に着けるべきは、「アウェアネス」。「リテラシー」を先に求め、途方に暮れていないか？



（参考）経営層のためのサイバーセキュリティ実践入門

「リテラシー」があれば不審メールを見分けられるかもしれない。
しかし、一般職員に判別を求めることは推奨されない。
まず重要なのは、不審メールに抱くべき違和感、「アウェアネス」

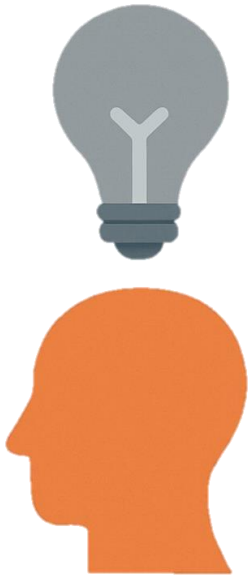
一般職員に「アウェアネス」がない状態・ある状態
アウェアネス醸成に必要なのは、インシデントになり得る契機ともたらす結果（怖さ）をなるべく端的に伝えること

【不審メール受信に関するアウェアネスの例】

契機と結果	不審メールのファイル開封等により、ウイルス感染の恐れがある

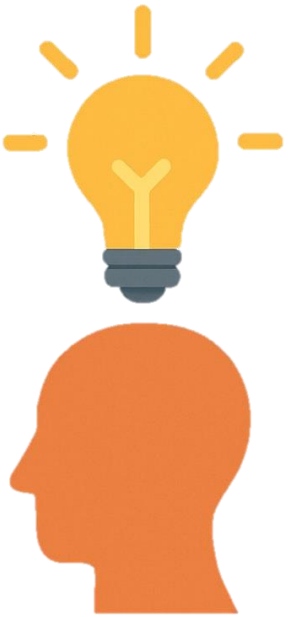
アウェアネスがない場合の思考

◆まさか自分にも不審メールが来ると思っていない
◆ウイルス対策はシステム部署が対策しているはずだ
◆不審メールがランサムウェア事案の契機になるなんて知らない
◆プログラム実行やインストール指示に違和感がわかない
◆何か異変を感じてから報告すれば良い
◆メール訓練に真剣に取り組んでおらず、報告方法が不明



アウェアネスがある思考

◆不審メールが増加していることを知っている
◆技術的対策ですべての不審メールを防げるわけではない
◆怪しいマクロ等のプログラム実行指示、インストールに抵抗を示すことができる
◆報連相を早めにすることで、ほかの誰かを守ることに繋がる
◆不審な挙動時にも、報告しやすい職場の心理的安全性を意識している



セキュリティを身近に。ともに考える機会を見逃さない。セキュリティへのよくある認識に対し、担当者が大事にすべきこと

よくある誤謬

- 訓練と、形骸化したアンケートでのみかかわるもの
- サイバーセキュリティは、ユーザビリティの障壁
- 一般職員・経営層は専門的なことはわからないから何を言っても無駄
- 担当者レベルの対策事項であり、経営としての課題認識は薄い

我々が大事にしたいこと

- ✓ 社内外で巻き起こる重要テーマを見逃さない
- ✓ 我々が話題にしなければ、「異世界」は「異世界」のまま。
  行動変容はおろか、アウェアネス向上も果たせない
- ✓ 全役職員を巻き込む。ともに考える機会を。１分１秒でも長く考える仕掛けを。基本的なことでも飽きるまで何度も言い続ける（これが、存在感・信頼感を生めるかどうかの岐路）

本日の次第

０．会社概要ー明治安田のサイバーセキュリティ
１．サイバーセキュリティは全員参加。私たちが重視する“アウェアネス”
　～生保で初のフィッシング被害。被害に遭って改めて気付いたこと～
２．おカネに頼らず、独自のアイデアと想いで勝負する
　～意識向上と行動変容、具体的な４つの取り組みを紹介～
３．めざすべき好循環。「超えよう。」は終わなき永遠のテーマ
４．ビギナー向け サイバーセキュリティ企画部署で働く魅力
５．情報セキュリティが学べる！ 明治安田オリジナルボードゲーム実践

サイバーセキュリティは全員共通・全員参加。
だから各層へ最適なアウェアネス向上の仕掛けが不可欠

一般職員向け

サイバーセキュリティという「異世界」へのインタフェース（接点）を増やし、アウェアネス向上を企図

- ◆ サイバーセキュリティポータル
- ◆ 月間サイリス新聞
- ◆ サイバーセキュリティを学べるボードゲーム
- ◆ 自社内 e-ラーニング
- ◆ 私のキャリアログ（職員経歴を自伝形式で紹介）
- ◆ 標的型攻撃メール訓練
- ◆ 本社部横断的なサイバーセキュリティワーキング
- ◆ サイバーセキュリティ月間運営

経営層向け

サイバーセキュリティは、経営上の課題であると認識し、リーダーシップと影響力ある推進協力を期待

- ◆ 経営層へのサイバーセキュリティにかかる定期的なレポーティング
- ◆ 経営層ランサムウェア対応訓練
  （シナリオ事前非開示、リアルタイム実施）
- ◆ 経営層勉強会（耐量子計算暗号　等）

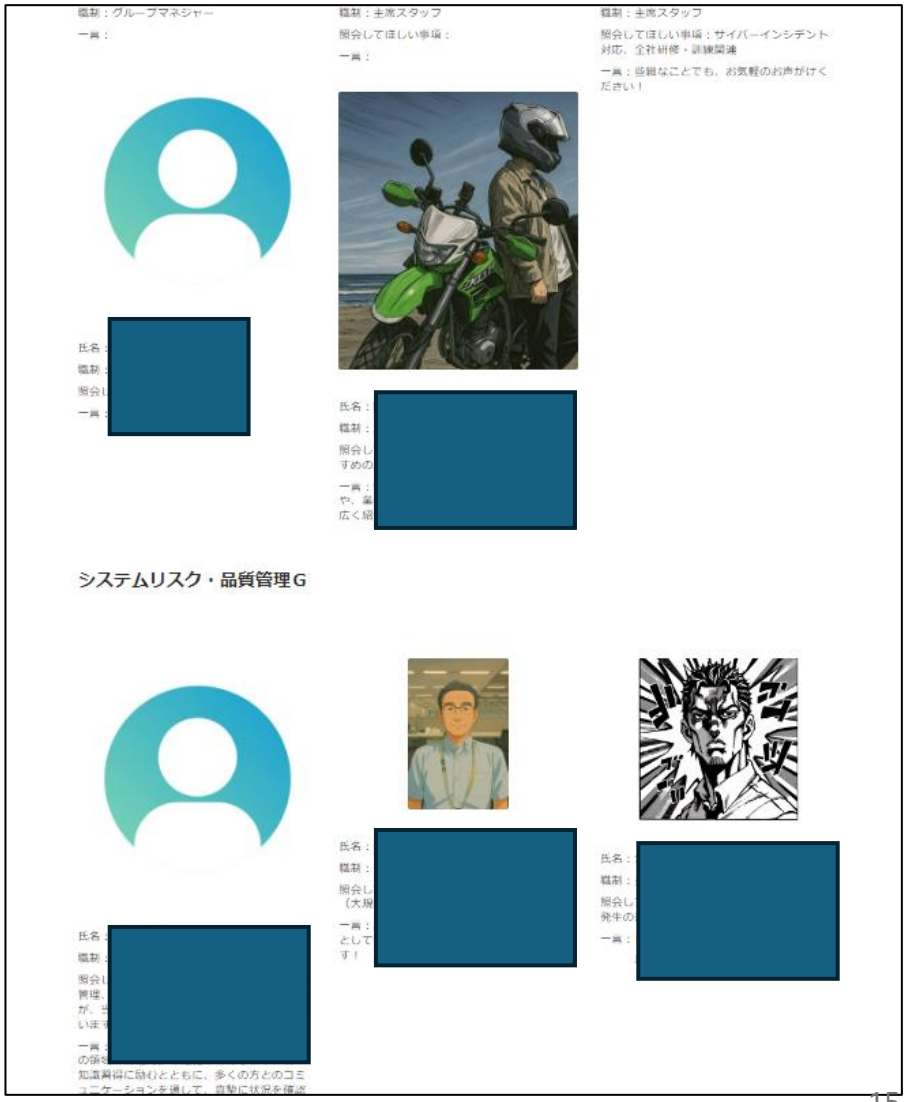
セキュリティ担当者

積極的な社外活動がしやすい風土を育み、知見と刺激、同志を得てひろく社会貢献をめざす

- ◆ トモダチ作戦/社外活動成果報告会

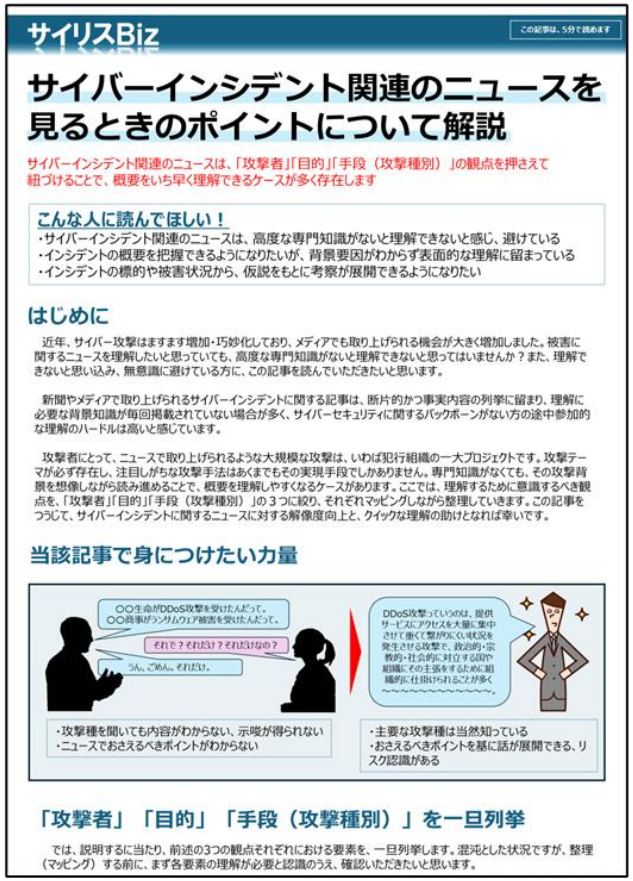
今後高度化が期待される領域　**お客さま・地域リレーション等社外ステークホルダー向け**

❶サイバーセキュリティポータルサイト
ー全役職員にひらかれた情報提供・照会プラットホーム



❶サイバーセキュリティポータルサイト
ー全役職員にひらかれた情報提供・照会プラットホーム

サイリスBiz



サイリスBiz

この記事は、5分で読めます

サイバーインシデント関連のニュースを見るときのポイントについて解説

サイバーインシデント関連のニュースは、「攻撃者」「目的」「手段（攻撃種別）」の観点を押さえて紐づけることで、概要をいち早く理解できるケースが多く存在します

こんな人に読んでほしい！
・サイバーインシデント関連のニュースは、高度な専門知識がないと理解できないと感じ、避けている
・インシデントの概要を把握できるようになりたいが、背景要因がわからず表面的な理解に留まっている
・インシデントの標的や被害状況から、仮説をもとに考察が展開できるようになりたい

はじめに

近年、サイバー攻撃はますます増加・巧妙化しており、メディアでも取り上げられる機会が大きく増加しました。被害に関するニュースを理解したいと思っていても、高度な専門知識がないと理解できないと思ってはいませんか？また、理解できないと思い込み、無意識に避けている方に、この記事を読んでいただきたいと思います。

新聞やメディアで取り上げられるサイバーインシデントに関する記事は、断片的かつ事実内容の列挙に留まり、理解に必要な背景知識が毎回掲載されていない場合が多く、サイバーセキュリティに関するバックボーンがない方の途中参加的な理解のハードルは高いと感じています。

攻撃者にとって、ニュースで取り上げられるような大規模な攻撃は、いわば犯行組織の一大プロジェクトです。攻撃テーマが必ず存在し、注目しがちな攻撃手法はあくまでもその実現手段でしかありません。専門知識がなくても、その攻撃背景を想像しながら読み進めることで、概要を理解しやすくなるケースがあります。ここでは、理解するために意識する観点を、「攻撃者」「目的」「手段（攻撃種別）」の３つに絞り、それぞれマッピングしながら整理していきます。この記事をつうじて、サイバーインシデントに関するニュースに対する解像度向上と、クイックな理解の助けとなれば幸いです。

当該記事で身につけたい力量

「攻撃者」「目的」「手段（攻撃種別）」を一旦列挙

では、説明するに当たり、前述の3つの観点それぞれにおける要素を、一旦列挙します。混沌とした状況ですが、整理（マッピング）する前に、まず各要素の理解が必要と認識のうえ、確認いただきたいと思います。

- サイバーセキュリティに関する考え方や最新の情報が短時間でわかる
- 一般職員向けにわかりやすく解説

私のキャリアログ

私のキャリアログ

①

高まる重要性を感じ、自ら志願してサイバーセキュリティの世界へダイブ

世界的に流行したランサムウェアから力業で企業を守った経験が使命感を醸成

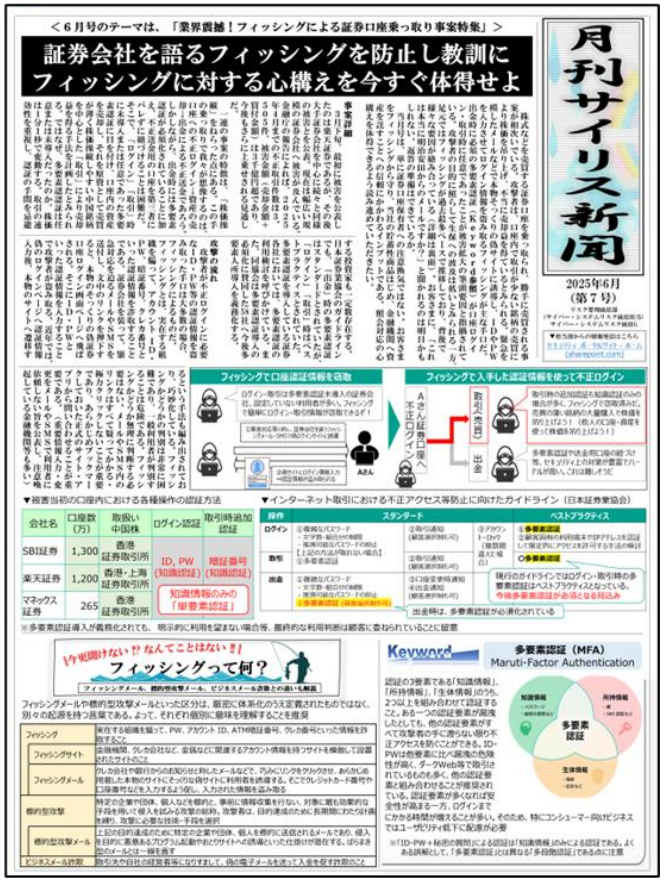
をめざし日々情報発信をし サイバーセキュリティ専門

ています。また、サイバー 部署を立ち上げることになセキュリティと一口にいっ り、初期メンバーに自ら志

「WaanaCry」感染時の身代金要求画面

- サイバーシスリス職員にスポットをあて、業務への想いやポイントを発信
- サイバー人財志願者はもちろん、普段情報セキュリティにかかわらない人財にも読んでおもしろく、解像度向上が可能

月間サイリス新聞



＜６月号のテーマは、「業界震撼！フィッシングによる証券口座乗っ取り事案特集」＞

証券会社を語るフィッシングを防止し教訓にフィッシングに対する心構えを今すぐ体得せよ

月刊サイリス新聞

2025年6月（第７号）

フィッシングで口座認証情報を窃取

フィッシングで入手した認証情報を使って不正ログイン

▼被害当初の口座内における各種操作の認証方法

会社名	口座数（万）	取扱い中国株	ログイン認証	取引時追加認証
SBI証券	1,300	香港証券取引所	ID、PW（知識認証）	暗証番号（知識認証）
楽天証券	1,200	香港・上海証券取引所	知識情報のみの「単要素認証」	
マネックス証券	265	香港証券取引所		

▼インターネット取引における不正アクセス等防止に向けたガイドライン（日本証券業協会）

操作	スタンダード	ベストプラクティス
ログイン	・英数字混在パスワード ・定期的なパスワードの変更 ・類似の暗号パスワードの禁止 ・【上記の方法が取れない場合】 ・少なくとも２回の入力	・多要素認証 ・証券会社の利用端末やEメールアドレスを認証して限定的にアクセスを許可する手法の検討
取引	・英数字混在パスワード ・定期的なパスワードの変更 ・類似の暗号パスワードの禁止 ・多要素認証（必須）	・多要素認証
出金	・英数字混在パスワード ・定期的なパスワードの変更 ・類似の暗号パスワードの禁止 ・多要素認証（必須）	・多要素認証

現行のガイドラインではログイン・取引時の多要素認証はベストプラクティスとなっている。
今後多要素認証が必須となる見込み

出金時は、多要素認証が必須化されている

※多要素認証導入が義務化されても、明示的に利用を望まない場合等、最終的な利用判断は顧客に委ねられていることに留意

1分更開けない!? なんてことはない！

フィッシングって何？

フィッシングメール、標的型攻撃メール、ビジネスメール詐欺との違いも解説

Keyword 多要素認証（MFA） Maruti-Factor Authentication

- 多要素認証（MFA）を導入する
- 多要素認証（MFA）を導入しない

- アウェアネス醸成が必要な需要テーマを中心に毎月深堀り
- 所属内の注意喚起にそのまま使える

❶サイバーセキュリティポータルサイト
ー全役職員にひらかれた情報提供・照会プラットホーム

社外

サイバーセキュリティ担当部署

【めざす姿】当社サイバーセキュリティのプロ集団として、高い使命感で全社のアウェアネス向上をデザインする

社外へ「超えよう」

業務意識の変化

働き甲斐。社内外に発信したくなるベストプラクティスとなる業務を志向（「超えよう」の発想）

サイバーセキュリティ担当部署の認知向上

専門家として社内でのプレゼンス向上。存在感ある頼られるプロ集団

フィードバック・モニタリング

サイトアクセス確認・各部や経営層とのコミュニケーションを通じた内容の高度化・見直し

社外での人脈構築・情報交換

社内外で情報交換（提供・収集）し、高い視座の獲得と刺激を自社へ持ち帰り

アウェアネス向上に資する情報発信（セキュリティポータル）

ポータルを駆使して各層へ情報発信

情報収集の感度向上

アンテナ高く知見集積・世間の興味関心を能動的にキャッチでいるようになる

- 全国の営業職員・お客さまの存在を強く意識し、ひろく社会に貢献できる啓蒙活動ができないか考える
- 社外で同じ志を持つ仲間を探し、自分たちだけでできないことを可能にする

その他各部等

【めざす姿】セキュリティに対する当たり前のレベルをあげ、自律的に情報漏洩等を防ぐことができる

アウェアネス向上

どのような日常行動・考えがインシデントにつながるか端緒と帰結の認識（アウェアネス）

行動変容

従前軽視していたセキュリティ上のヒヤリハットや、点検やアンケートへ積極取組

社外に学びを還元し、広く社会に貢献し、「信頼して選ばれる」生命保険会社に向けた情報提供を行なう

❷月間サイリス新聞
ー旬のテーマを逃さず、＋「考え方、継承」を散りばめる

■月間サイリス新聞は、毎月サイバーセキュリティに関連する時節のテーマをピックアップし、社内イントラのトップメニューに掲載のうえ周知

時期	テーマ	テーマ決定の背景
2024年11月	MYほけんページ（弊社のご契約者さま向けWebサイト）を模したフィッシング事案	2021年に発生し、お客さまに被害があった同事案から3年が経過したことをふまえ
12月	2024年流行したサイバー攻撃、事案振り返り	金融庁のガイドライン公表や、複数のランサムウェア事案が発生ことをふまえ
2025年1月	DDoS攻撃	年末年始、金融機関や航空会社でDDoS攻撃が横行したことをふまえ
2月	標的型攻撃メール訓練	2024年度下期に実施した標的型メール訓練の結果が出たことをふまえ
4月	情報セキュリティに関連する自己点検項目について	年度始を迎え、改めて当部自己点検項目の趣旨・注意点を周知するため
5月	大阪・関西万博、国際イベントと連動するサイバー事案	大規模な国際イベント開催に伴いサイバー攻撃の増加が懸念されたため
6月	証券業界におけるフィッシング事案	証券業界でフィッシングによる口座乗っ取り事案が大きな影響を与えたため
7月	2025年度経営層向けランサムウェア対応訓練	シナリオ非開示、実時間軸という業界で類を見ない訓練の振り返りのため
8月	ボイスフィッシング（電話を用いたフィッシング）	2025年度始に、地域金融機関で電話によるフィッシングが横行したため
9月	証券業界のフィッシング事案を受けての当局要請	証券業界での口座乗っ取り事案をふまえ、認証強化等の当局要請が発令され、当社お客さま向けサービスにも影響があることをふまえ
10月	ソーシャルエンジニアリング	過去最多ペースで推移するフィッシングや特殊詐欺、海外グループ会社での被害事例をふまえ

＜2025年５月号＞テーマ：関西万博

＜5月号のテーマは、「万博特集/新年度、情報セキュリティリテラシー総点検特集②」＞

２０２５ 大阪・関西万博ついに開幕！ 国際イベントで「脈々」と発生したサイバー攻撃に警戒せよ

▲画面：主な内容は大阪万博と関連性がないが、URLに「expo」や「osaka」を用いたサイト例（2025年3月確認）。何らかの不正活動の準備段階の可能性がある

「世界中が注目するイベントが開催されるとき、その影響力に便乗し、己の技術力や思想を誇示しようとサイバー攻撃を試みる者は必ずいます。」そう語るのは、サイバーセキュリティ管理G 栢森主席スタッフだ。４月12日、大阪府夢洲で、１５０を超える国と地域が参加する大阪万博が約半世紀ぶりに開幕した。物理空間における警備はもちろんのこと、サイバー空間についてはどうだろうか。

会場では、夢洲やその周囲半径１キロメートル内のドローン飛行を禁止したり、飛行の阻害電波を流す等、物理空間におけるセキュリティやテロ対策が進められている。サイバー空間においても、官民合同でサイバーインシデント対応訓練が実施されるなどの動きがみられた。幸いなことに、開幕以降、際立って社会に大きな影響を及ぼすようなサイバーインシデントが発生しているわけではない。しかしながら、２０２０年10月には、日本国際博覧会協会に対して不正アクセスが確認されており、攻撃者はメールアカウントを乗っ取り、約６万３千件のフィッシングメールを国外のメールアドレスに向けて送信した。この事例から想定されるように、攻撃者は数年前から周到な準備をしており、被害が顕在化するおそれもある。また、万博関係者への「国家背景型の諜報組織」による攻撃も確認されている。これらは氷山の一角にすぎない可能性が高い。

当記事においては、①万博開催にあたり想定されるサイバー攻撃、②万博関連の攻撃動向の現況、③過去、国際イベントと同時期に発生したサイバーセキュリティ事案について、注意喚起を交え解説する。

＜万博開催にあたり想定されるサイバー攻撃＞

想定事象① DDoS攻撃によるチケット販売をはじめとしたイベント用サービスの停止

DDoS（Distributed Denial of Service）攻撃は、最も発生が予想される攻撃である。DDoS攻撃は、設定が脆弱なIoT機器を乗っ取り、それらを踏み台にして、Webサイト等へアクセスを集中させ、「重くて繋がりにくい」状況を意図的に発生させる攻撃だ（詳細は1月号）。この攻撃は、ハクティビスト（特定の政治的・宗教等の思想に基づいた主張の代替手段としてサイバー攻撃を実施する者）のプロパガンダとして悪用されやすいという特性がある。多数の国や地域、企業や利権が絡む大規模なイベントであればあるほど発生の蓋然性は上昇する。2024/2025年末年始、メガバンクや航空会社、通信事業者で断続的に発生したことは記憶に新しい。公共交通機関や金融インフラなどのサービスが同様に被害に遭う可能性があり、すでにフィージビリティが検証されているといえる。また、DDoS攻撃は侵入を目的としたものではないため比較的容易な攻撃手法であり、攻撃代行業者の存在も確認されており、懸念を加速させる。迷惑な話だが、彼らにとって万博は格好の攻撃技術披露の「展示会（EXPO）」だ

（参考）（【全社/連絡】月刊サイリス新聞１月号　＜年末年始世界を混乱に陥れたサイバー攻撃～ＤＤｏＳ攻撃特集～＞）

想定事象② 参加国・地域、協賛企業等関係者を標的にした情報窃取、クラッキング（破壊行為）

攻撃者がより高度な技術力を持ち合わせている場合、DDoS攻撃といった単なる妨害から、侵入による情報窃取や侵入後の破壊行為（クラッキング）が懸念される。侵入の手段は様々であるが、2月以降、大阪・関西万博の公式サイトドメイン「expo2025.or.jp」に似せるために、「expo」や「osaka」の文字列を含んだ偽ドメインが確認されている。攻撃者は、なりすましメールでこうした偽サイトへ誘導し、PW等の認証情報を入力させて、それを使って不正に侵入を試みるとみられる。2025年国際博覧会協会に対しては、すでに2020年10月に不正アクセスが確認されている。攻撃者はメールアカウントを乗っ取り、約6万3000件のフィッシングメールを国外のメールアドレスに向けて送信した。不正アクセス後、攻撃者の思い通りにいけば、被害者の情報・資金が窃取されたり、攻撃を受けた組織が持つ情報資産が暗号化され、ランサムウェア被害に発展するおそれがある。

当新聞でも繰り返し注意喚起しているが、不安を煽るような緊急性を謳ったメールやSMS内のリンクへ触れたり、記載の電話番号へ架電することは避け、ブラウザ等から別途公式サイトへアクセスを試みることが被害を被る可能性を低減させる判断といえる

＜過去、国際イベントと同時期に発生したサイバー事案＞

▼国際イベントと同時期に発生したサイバーセキュリティ事案の例

攻撃の類型		過去の事例
妨害行為	DDoS攻撃	・大会システムを標的としたDDoS攻撃(東京五輪(2021.7.21-9.5))・パリ五輪(2024.7.26-9.8)) ・官公庁WebサイトへのDDoS攻撃(広島サミット(2023.5.19-23))
妨害行為	インフラへの攻撃	・海底インターネットケーブル切断（2024.7.28-29）(パリ五輪)
情報・資金窃取	標的型攻撃	・特定の国における問題を議論した政府関係者への標的型攻撃（広島サミット）
情報・資金窃取	フィッシング攻撃	・チケット販売を装ったフィッシングサイト（東京五輪・パリ五輪）
情報・資金窃取	ランサムウェア攻撃	・JOC内でのランサムウェア事案(2021.4下旬)（東京五輪関連）
情報・資金窃取	脆弱性攻撃	・参加者用アプリ「MY2022」へ脆弱性攻撃（北京五輪）
影響力工作		・IOC批判動画（ディープフェイク拡散）（パリ五輪）

▼ミラーフェイス（Earth Kasha）概要

名称	ミラーフェイス（Earth Kasha）
日本国内の活動傾向	・2019年から日本国内でのみ観測されていた標的型攻撃（2023年に台湾・インドに拡大） ・初期侵入として標的型メールを使用していたが、2023年より公開機器の脆弱性を悪用した攻撃を開始 ・2024年には、標的型攻撃メールを初期侵入の手法として再度使用
活動期間	2019年12月～
主な攻撃対象地域	日本、台湾、インド
主なターゲット業種	・2023年まで：公共関連組織、国際関係の組織・個人、メディア関係組織・個人 ・2023年：公共関連組織や先端技術を持つ企業・組織など ・2024年：政治関連組織や研究機関、シンクタンクに属する個人や国際関係に関連する組織

＜万博関連の攻撃動向の現況＞

動向① 万博と直接関係ない組織による万博を想起させるドメイン取得

インターネット上では、開催前から「expo2025.or.jp（公式ドメイン）」とは別に、「expo」や「osaka」などの文字列を含んだドメインが取得されたり、関連性がないWebサイトが確認されている。これらは、断定できないものの、今後資金や情報窃取を目的としたなりすましメールに記載されるURL、すなわち偽サイトの前身である可能性が指摘されている

動向② 2025年日本国際博覧会に対する不正アクセス

2020年10月7日から翌8日にかけて、外部からの不正アクセスによって、同協会のメールアカウントの一つから、約6万3千件のフィッシングメールが国外のメールアドレスに向けて送信される事案が発生した

動向③ 国家背景型の諜報活動組織による万博関係者への攻撃

2024年11月には、欧州連合（EU）の関係者をねらって外交関連機関に攻撃メールを送付しており、そのなかで添付されたファイルを開封すれば、マルウェアに感染するとみられています。そのファイル名は、「The EXPO Exhibition in Japan in 2025.zip」である。また、eset（セキュリティベンダ）の研究者によれば、日本を主な標的とする国家背景型の諜報活動組織（ミラーフェイス（詳細は左記））によるものと指摘されている。警視庁は、当該組織に対する異例の注意喚起を今年1月8日に実施している

おわりに

万博開催にあたり、「各部からのお知らせ」にて当部から注意喚起を発信している。関連する標的型攻撃メールやフィッシングメールの増加が予測されるためだ。裏面の不審メール受信時の注意点を読み、報告方法について確認されたい。当社は標的とされやすい重要インフラ事業者に含まれており、三菱未来館（パビリオン名称）を出展する三菱企業の一員でもある。担当部の意識はどうか。「万博開催にあたり、当部では有事の連絡体制について事前確認を実施いたしました。開催期間はいつもより緊張感をもって過ごします。」（サイバーセキュリティ管理G中村グループマネジャー）

特に注意が必要な日程

開会式	4月12日（土）	ジャパンデー	7月3日（木）
開幕日	4月13日（日）	閉幕式	10月13日（火）

月刊サイリス新聞

2025年5月（第６号）

リスク管理統括部
（サイバー・システムリスク統括担当）
サイバー・システムリスク統括G
明治安田生命ビル　２８階

▼担当部からの情報発信はこちら
セキュリティ ポータルサイト - ホーム (sharepoint.com)

インシデントかも？と思ったら
私たちが来た！もう大丈夫
MY-SIRT
すぐ報告！すぐ対応！頼れる正義の味方！
窓口 MY-SIRT<mysirt@meijiyasuda.co.jp>

＜2025年７月号＞テーマ：経営層訓練

＜７月号のテーマは、「シナリオ非開示は大手金融機関で初！経営層関与のサイバー訓練特集」＞

シナリオ事前非開示は大手金融機関で初！ 経営層関与のサイバー訓練の全容を刮目せよ

企業におけるサイバーセキュリティは、経営者自らがそれをリスクマネジメントにおける重要課題であることを認識し、対策を推進することが求められている。また、インシデントを想定した訓練においても同様、事業継続を揺るがす脅威に発展するという認識にたった経営層の関与が、当局のガイドラインでも「基本的な対応事項」とされている。当社においては、経営層含めた本社各部を巻き込んだランサムウェア対応訓練を、当部主導で例年実施している。

当月号では、その進歩の歴史を振り返るとともに、５月２６日（火）に開催された今年度訓練と、そのなかにおける新たな試みを紹介したい。当月号を通じ、当社が経営課題として取り組んでいるランサムウェア対応訓練の現在地と全容を把握し、自身や自組織が有事の業務継続にどれほどコミットメントできるかを考える機会としていただきたい。

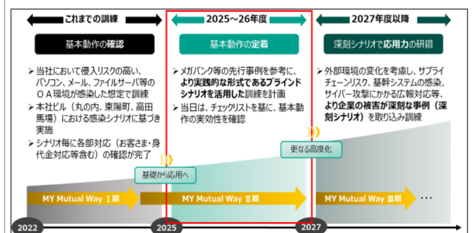
経営層向け訓練概要

経営層向けのサイバーインシデント対応訓練は、「ランサムウェア対応訓練」というのが例年の正式名称だ。ランサムウェア攻撃により当社に危機事象が発生し、その対応を担う緊急の会議体に経営層が出席し、各部門の状況報告・経営判断を協議するという初動対応までが大まかな開催の流れである。訓練開始当初は、その会議体において有事の際に必要な報告内容や審議内容を事務局が読み上げて示し完結する、というスタートであったが、年々関係者の理解を得ながら工夫と進化を遂げている。一昨年度は記者会見を含むメディア向け訓練を開催し、いまや本社各部担当者を巻き込んだ形式へと高度化している。

当年度訓練の概要

訓練の歴史については裏面で詳細するが、当年度訓練のテーマは、昨年度までの「基本動作の確認」から、「基本動作の定着」へと高度化した。今回の訓練では、その検証のために、大手金融機関でも類を見ない次の２点のようなリアリティを追求するポイントを試行した。１点目は、「シナリオの事前非開示」である。これまでの訓練では、本社３拠点（丸の内、東陽町、高田馬場）のうちどこかでランサム被害が発生し、関連部を中心に対応が必要となる想定であったが、今回は当日まで被災拠点は非開示とした。２点目は、「リアルタイム性の追求」である。当日は、東陽町勤務の職員が朝不審メールを開封し、ランサムウェア感染を起点に、各部門で影響調査やエスカレーション、経営判断が進められた。各担当者においては、マイルストーンである経営層が参加する緊急の会議体開催に向けて、自身の担当執行役に求められる情報の収集およびそれに基づく報告資料の作成に向けて、臨場感・緊張感漂う雰囲気のもと訓練が進められたが、関係者全員の努力で無事に終えることができた。

▼訓練の現在地（当社経営層向けサイバー訓練高度化ロードマップ）



‖最先端訓練の舞台裏‖ 訓練の全容を大解剖

Cybersecurity Executive Training 2025

２０２５年５月２６日（月）　経営層向けランサムウェア対応訓練

訓練の目的：基本動作の定着
- 実際の時間軸で行なうことによる、実効性の検証
- 事前のシナリオ非開示による実践的取組み

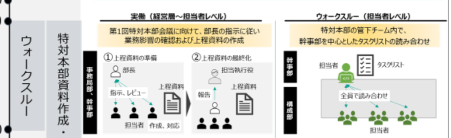
訓練の流れ：訓練当日の朝にインシデント発生が発覚し、午後に第1回特別対策本部会議を開催する時間軸で実施

シナリオ（当日開示（シナリオ事前非開示））
- ベースシナリオ：過去に実施した本社3ビル（丸の内、東陽町、高田馬場）のいずれかで感染被害が発生し、緊急停止措置およびビルのネットワークの遮断を実施するシナリオより選定*1
- 追加要素：最新の外部動向を取り込む予定

タイムライン

事前準備：各部で有事に想定されるタスクリストを作成

- 9:30 インシデント発覚
  - 東陽町勤務の職員が朝のメールチェック時にランサムウェア感染
  - システム障害発生時の危機対応部であるサイバーシスリスと情シスを中心に調査含む初動対応開始
  - **ランサムウェアを確認**：ファイルの暗号化確認、公式Instagramで身代金要求・脅迫文受信（当社契約者情報５万件の情報窃取を主張）
  - **ランサムウェア被害による緊急停止措置**
    - 全社（全拠点）において、社内外のメール送受信、インターネット閲覧、ファイルサーバの利用を停止。加えて東陽町ビルのネットワークを停止
    - 東陽町ビルのネットワーク停止により、東陽町ビルの個人保険事務およびシステム開発業務等が停止。なお、システム保守・運用業務（稼動監視、オペレーション等）は、別系統のネットワークのため停止せず業務を継続
- 11:00 特対本部の設置
- 11:30～11:50 第1回関連部長打合わせ
  - **シナリオ判明**
  - ○ 発生事象や復旧の見通し等を伝達
    - 参加者：特対本部事務局構成部・チーム幹事部の部長
    - 概要：発生事象等の共有、当面の対応事項と第 1回特対本部会議の議題の確認
  - 「MYほけんページ」にDDoS攻撃発生(ランサムウェアの注意をそらす・対応要員分散の陽動作戦)
- 13:00～14:00 ウォークスルー／13:00～14:30 特対本部資料作成・報告



すべての部門において、締切までに資料作成・報告・提出が完了！ 過去訓練の積み重ねと、「チーム明治安田」の底力を発揮！

- 14:30 資料の提出締切
- 15:00～16:30 第1回特対本部会議
  - **経営層が出席する緊急の会議体開催**
  - 【参加者】特対本部のメンバー(会長、特対本部事務局構成部・チーム幹事部の部長は会議室で陪席、国内グループ会社社長・理事長はTeamsで陪席)
  - 【概　　要】議題に沿って担当執行役、事務局から報告・審議
  - 【開催方法】丸の内：実参加（30A会議室）／ その他：Teams参加（各ビル会議室）

▼システム停止時の特対本部の構成部署

組織名	構成部（◎は幹事部、〇は副幹事部）
事務局	◎企画、〇リス統（サイバーシスリス）、広報、調査、志向統、コン統、リス統、リス統（オペリス情管）、法務
情報システムチーム	◎情シス、情シス（企保シス）、リス統（サイバーシスリス）
広報対応チーム	◎ブラ戦、広報、人事
個人営業・事務業務維持チーム	【チャネル機能班】 ◎営企、営人、業務、ＭＹＲＡ業推 【事務機能班】 ◎事務企、事務オペ、サ相談、情シス、情シス（企保シス）、ＣＣ、ＭＹオフィス
法人営業・事務業務維持チーム	【チャネル機能班】 ◎法営企、総法業、公法業、金法業 【事務機能班】 ◎法人事務企、法人事務オペレ、団年Ｃ、情シス、情シス（企保シス）
資産運用業務維持チーム	◎運企、融資、債投、株投、特保商品運用、不動産、運審、運サ、収益
関連事業支援チーム	◎関連
海外事業支援チーム	◎海外企、北米推進、北米開発、欧州アジア

月刊サイリス新聞

2025年7月（第８号）

リスク管理統括部
（サイバー・システムリスク統括担当）
サイバー・システムリスク統括G

▼担当部からの情報発信はこちら
セキュリティ ポータルサイト - ホーム (sharepoint.com)

インシデントかも？と思ったら
MY-SIRT
すぐ報告！すぐ対応！頼れる正義の味方！

＜2025年6月号＞テーマ：証券業界におけるフィッシング事案

＜６月号のテーマは、「業界震撼！フィッシングによる証券口座乗っ取り事案特集」＞

月刊サイリス新聞

2025年6月
（第７号）
リスク管理統括部
（サイバー・システムリスク統括担当）
サイバー・システムリスク統括G

▼担当部からの情報発信はこちら
セキュリティ ポータルサイト - ホーム (sharepoint.com)

証券会社を語るフィッシングを防止し教訓に フィッシングに対する心構えを今すぐ体得せよ

株式などを売買する証券口座を乗っ取られ、勝手に売買される事案が相次いでいる。攻撃者は、口座内で取引が少ない銘柄の売買により株価を吊り上げ、不当に売却益を得ているとみられる。緊急を模したメールなどで本物そっくりの偽サイトに誘導し、ＩＤやＰＷを入力させてログイン情報を盗み取るフィッシングが主な手口だ。出金時に必須の多要素認証（Ｋｅｙｗｏｒｄ参照）がログイン・取引時に任意であったことが被害拡大の筆頭要因と指摘されている。攻撃者の目的に照らして生保への波及は低いとみられる一方、足元ではフィッシングが過去最多ペースで推移しており、背後で様々な要因が絡み合っている（詳細は裏面）。お客さまに、「これは本当に明治安田からのメールですか？」と聞かれるのは明日かもしれない。返答の準備はできているか。

当月号は、単に証券口座保有者への注意換気ではない。お客さまをフィッシングから守り、当社の貯蓄性商品はじめ、金融機関へ資産を託すことへの信頼にかかわるインプットである。フィッシングに対する構えを体得できるよう読み進めていただきたい。

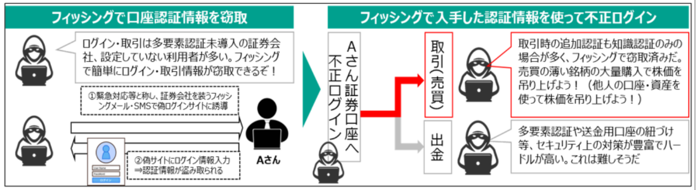
事案詳細

３月下旬、最初に被害を公表したのは楽天証券であるが、その後大手証券会社を中心に続々と同様の被害を公表。現在は幅広い規模の証券会社へ被害が及んでいる。金融庁の報告によれば、２０２５年４月までの不正取引件数は３，５０５件、被害金額（売却金額＋買付金額）は３千億円超であり、今後もさらに上乗せされる見通しだ。

一連の事案の特徴は、「株価操縦」をねらった点にある。この手の乗っ取りで我々が想像するのは、口座への不正ログイン→資産の売却→出金による不正送金であろう。しかしながら、出金時には多要素認証が必須化されていることに加え、不正送金用の口座を第三者にバレずに紐づけることは困難だ。そこで、「ログイン」「取引」時に未導入または任意であった多要素認証に目を付け、口座内の資産を売却し、それを原資として売買が薄く株価操縦しやすい中国銘柄を中心とした「取引」により売却益を得る手法を計画したとみられる。ではなぜ、多要素認証は任意または未導入だったのか。株価は１分１秒で変動する。取引の即時性を重視し、認証の手間を忌避する投資家も一定数存在する。日本証券業協会のガイドラインでも、「出金」時の多要素認証はスタンダードとされていたが、「ログイン」「取引」時はベストプラクティスとされていた。多要素認証を導入している証券各社においては、多要素認証の利用検討を呼びかけている。また、同協会は多要素認証導入の必須化に賛同した58社へ多要素人所導入を義務化する。

攻撃の流れ

攻撃者が不正ログインに必要なＩＤ・ＰＷ等の認証情報を盗み取った手口は大多数の場合、フィッシングによるものだ。フィッシングとは、実在する組織を騙って、アカウントＩＤ・ＰＷ、暗証番号、クレカ番号といった認証情報を詐取することである。証券会社を装い、認証情報入力を迫るメールやＳＭＳを送付し、文中のリンクから本物のそっくりの偽証券口座ログイン画面ページ等へ飛ばされる。そこにＩＤ・ＰＷといった認証情報を入力することで攻撃者が盗み取る。近年では、偽のログインページへ認証情報を入力した後、本物のサイトへ遷移するという手法も編み出されており、巧妙化している。フィッシングかどうかの判別は非常に困難であり、一般利用者が判別することは危険である。フィッシングかどうか無理に判断する必要はない。メールやＳＭＳ内のリンクはすべて疑ってかかる・極力クリックしないことが重要であり、あらかじめブックマークしておいた正式のサイト・アプリから問い合わせることが重要である。（重要情報入力・変更をメールやＳＭＳで利用者に依頼しない旨を公表し、注意喚起している金融機関等も多い）



▼被害当初の口座内における各種操作の認証方法

会社名	口座数（万）	取扱い中国株	ログイン認証	取引時追加認証
SBI証券	1,300	香港証券取引所	ID, PW（知識認証）	暗証番号（知識認証）
楽天証券	1,200	香港・上海証券取引所		
マネックス証券	265	香港証券取引所		

知識情報のみの「単要素認証」

▼インターネット取引における不正アクセス等防止に向けたガイドライン（日本証券業協会）

操作	スタンダード			ベストプラクティス
ログイン	①複雑なパスワード ・文字数・組合せの制限 ・推測可能なパスワードの抑止 【上記の方法が取れない場合】 ①多要素認証	②取引通知（顧客選択制も可）	③アカウント・ロック（複数間違えた場合）	①多要素認証 ②顧客固有の利用端末やIPアドレスを認証して限定的にアクセスを許可する手法の検討
取引		②取引通知（顧客選択制も可）		○多要素認証
出金	①複雑なパスワード ・文字数・組合せの制限 ・推測可能なパスワードの抑止 ②多要素認証（顧客選択制も可）	③口座変更時通知 ④出金通知（顧客選択制も可）		

現行のガイドラインではログイン・取引時の多要素認証はベストプラクティスとなっている。今後多要素認証が必須となる見込み

出金時は、多要素認証が必須化されている

※多要素認証導入が義務化されても、明示的に利用を望まない場合等、最終的な利用判断は顧客に委ねられていることに留意

‖今更聞けない⁉ なんてことはない‼‖ フィッシングって何？

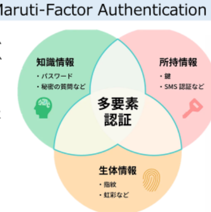
フィッシングメール、標的型攻撃メール、ビジネスメール詐欺との違いも解説

フィッシングメールや標的型攻撃メールといった区分は、厳密に体系化のうえ定義されたものではなく、別々の起源を持つ言葉である。よって、それぞれ個別に意味を理解することを推奨

フィッシング	実在する組織を騙って、PW、アカウント ID、ATM暗証番号、クレカ番号といった情報を詐取すること
フィッシングサイト	金融機関、クレカ会社など、金銭などに関連するアカウント情報を持つサイトを模倣して設置されたサイトのこと
フィッシングメール	クレカ会社や銀行からのお知らせと称したメールなどで、巧みにリンクをクリックさせ、あらかじめ用意した本物のサイトにそっくりな偽サイトに利用者を誘導する。そこでクレジットカード番号や口座番号などを入力するよう促し、入力された情報を盗み取る
標的型攻撃	特定の企業や団体、個人などを標的と、事前に情報収集を行ない、対象に最も効果的な手段を用いて侵入を試みる攻撃の総称。攻撃者は、目的達成のために長期間にわたり計画を練り、攻撃に必要な技術・手段を選択
標的型攻撃メール	上記の目的達成のために特定の企業や団体、個人を標的に送信されるメールであり、侵入を目的に悪意あるプログラム起動やおとりサイトへの誘導といった仕掛けが潜在する。ばらまき型のメールとは一線を画す
ビジネスメール詐欺	取引先や自社の経営者等になりすまして、偽の電子メールを送って入金を促す詐欺のこと

Keyword 多要素認証（MFA） Maruti-Factor Authentication

認証の3要素である「知識情報」、「所持情報」、「生体情報」のうち、2つ以上を組み合わせて認証すること。ある一つの認証要素が漏洩したとしても、他の認証要素がすべて攻撃者の手に渡らない限り不正アクセスを防ぐことができる。ID・PWは他要素に比べ漏洩の危険性が高く、ダークWeb等で取引されているものも多く、他の認証要素と組み合わせることが推奨されている。認証要素が多くなれば安全性が高まる一方、ログインまでにかかる時間が増えることが多い。そのため、特にコンシューマー向けビジネスではユーザビリティ低下に配慮が必要



※「ID・PW＋秘密の質問」による認証は「知識情報」のみによる認証である。よくある誤解として、「多要素認証」とは異なる「多段階認証」である点に注意

核心 CORE フィッシング増加の背景を探る

過去最多ペースで推移するフィッシング報告の背後に潜む要因とは？

フィッシング攻撃に関する報告が、１日あたり８千件超と過去最多の水準で推移している。証券関係の報告が約４分の１にのぼり、１２ブランドで悪用が確認された。フィッシング対策協議会によれば、４月に寄せられた報告は２４万６５８０件。過去最多となった前月の２４万９９３６件から１.３％減となり、月ベースで過去２番目に多い件数だ。一方、１日平均に換算すると８２１９.３件で、前月の８０６２.５件を上回る水準で推移している。背後に潜む要因に迫る

多要素認証の不在

要因① 証券口座数の増加

資産運用立国へ向けた推進事項として、昨年より新ＮＩＳＡ(小額投資非課税制度)が開始された。非課税期間の無期限化や上限額の拡大により証券口座数は増加している。２０２４年末時点の口座数は２５６０万であり、２３年末の２１２４万より２０％増加。今後もプラチナＮＩＳＡ等が実現すればさらに増加が見込まれる

要因② 高性能フィッシングキットの流行

高度な検知回避技術をもつ洗練されたフィッシングキットＧｏＧＵＩによるメッセージが、１月以降、数十万から数千万送信されているとみられている。今回の証券会社のフィッシング事案との関連性は断定できないものの、特定の地域のみをねらうことができ、「相互関税」をキーワードにした誘導も多数確認されている

要因③ 日本を標的とするフィッシングアクター

セキュリティベンダーのプルーフポイント（米）によれば、「要因②」で説明したフィッシングキットＧｏＧＵＩの利用者は中国語を話す脅威アクター（攻撃組織）によるキャンペーンと分析されている。海外においても、日本語話者や日本企業を狙っていることが多いとされている

要因④ 生成ＡＩの進歩

日本語は世界の言語のなかでも比較的難しいとされている。そのため、海外の攻撃者にとって完璧かつ自然な日本語でフィッシングメール文を作成することは困難であり、一種の参入障壁となっていた。しかしながら、近年の生成ＡＩの発展は目覚ましく、日本も標的の例外ではなくなってきているといわれている

▼フィッシング報告件数の推移（フィッシング対策協議会）
直近2年間の、フィッシングの報告件数は急増している

事業会社にとっては、フィッシングと誤認されないための努力も重要

フィッシングが警戒されればされるほど、悪意のない送付者にとって、フィッシングと誤認されないための工夫が不可欠となる。当社では、主管部がメール・ＳＭＳをお客さまに一斉配信する際の注意点や事前申請について以下の規程等で規定しているため確認いただきたい。また、外部サービス利用に伴い、外部から当社職員やお客さまへメール送信をする際は、不審メール報告されないよう事前周知を推奨する。攻撃者だけによらず、自ら当社のレピュテーションリスク（風評リスク）を低下させないよう、注意いただきたい。

メール･SMS送付上の注意	システムリスク管理細則.docx（第５４条）
SMS送付申請	SMS申請手順･解説書 0003850370 (mylinc.local)

COLUMN フィッシング対策協議会公式サイト 緊急情報（注意喚起情報）を確認しよう

フィッシング対策協議会のサイト内「緊急情報」では、日々全国から寄せられたフィッシング被害や報告を取集し、注意喚起を行なっている。下記は、個別の注意換気詳細画面である。概要（標的企業名）・フィッシングメール件名・文面・スクリーンショットが掲載されている。繰り返すが、フィッシングかどうか自身で判断することは非推奨であるが、現在どのような企業を装ったフィッシングが横行しているのか、確認するには有効だ。また、月次報告書では、月次の報告件数や手口の傾向といった情報収集に役立つ。

▶ **楽天証券をかたるフィッシング注意喚起画面（2025/04/01）**

フィッシング対策協議会とは、フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策の促進を目的とする組織であり、全国から寄せられた報告を基に、公式サイトでフィッシング関連の様々な情報発信を行なっている。<会員・オブザーバー数136（うち正会員：107 社、リサーチパートナー：5 名、関連団体：17 組織、オブザーバー：7 組織) 2025 年 5 月時点。当社加入済み>

フィッシングへの心構え

～自身とお客さまをフィッシングから守るための心得～

フィッシングへの心構え五か条

一．フィッシングかどうかの判断は専門家でもない限り非常に危険かつ困難。「これは本当に明治安田からのメールですが？」ときかれても、自身での判断は避けるべし
二．メールやＳＭＳ内のリンクは極力触らず、どうしても確認が必要ならブックマークしておいた正規サイトやアプリ経由で問い合わせるべし
三．当社が電子メールでＩＤやＰＷ、個人情報などをお伺いすることは決してないことを知っておくべし
四．フィッシングメールが届くということは、アドレスが漏洩している可能性あり。状況に応じてアドレス変更を検討すべし
五．多要素認証の利用を積極的に検討すべし。多少の手間・即時性と（資産を失う）リスクを自身に問うこと

【まとめ】
フィッシングメールは本物メールをコピーして作成することも多く、見分けることは非常に困難です。また、手法は日々巧妙化しており、専門家でもない限り、自身で判断することは推奨されません。メールやSMS内のリンクや認証情報変更を促すものはゼロトラスト（信頼しない前提）で対峙し、どうしても無視できない場合にのみブックマークしておいた正規のサイトやアプリを経由して照会しましょう。なお、アプリやWebサイトコンテンツを作成する側は、その時に備え、注意喚起情報の掲載場所、照会対応がしやすい、といったWebサイト設計（UI／UX）が期待されています。また、当社では、電子メールでIDやパスワード、個人情報などをお伺いすることはないことをHP上で開示している（明治安田｜フィッシング詐欺にご注意ください (meijiyasuda.co.jp)）ため、この機会にぜひ確認しておきましょう。

＜2025年８月号＞テーマ：ボイスフィッシング

＜８月号のテーマは、「億単位の実害も！銀行装い猛威振るうボイスフィッシング～多様なフィッシング特集①～」＞

月刊サイリス新聞

2025年8月
（第９号）
リスク管理統括部
（サイバー・システムリスク統括担当）
サイバー・システムリスク統括G

▼担当部からの情報発信はこちら
セキュリティ ポータルサイト - ホーム (sharepoint.com)

インシデントかも？と思ったら
MY-SIRT
すぐ報告！すぐ対応！
頼れる正義の味方！

ワンタイムパスワード突破し億単位の実害も 銀行装うボイスフィッシングに要注意

慣れた丁寧な口調の女性オペレーターのガイダンスにより、銀行口座情報更新操作の説明があり、操作の過程で認証情報を無意識に提供した、という電話のやり取りをするのは明日の自分かもしれない。これは、ボイスフィッシングと呼ばれるフィッシング攻撃における一幕であり、電話等音声のやり取りなかで認証情報を窃取することが特徴だ。通常のフィッシングとは異なり、人間の肉声を用いることで警戒心が薄れるという人の心理的な脆弱性を悪用している。上記の理由から、とくに警戒が必要なため、特別に名前が付けられ分類されている。実際に、今年に入り被害が増えており、億単位の実害も出ている。

月間サイリス新聞8月号では、ボイスフィッシングについて特集する。通常のフィッシングと手口や警戒するポイントは違えど、フィッシングに対する基本的な対処方法は変わらない。証券会社の口座乗っ取り事案を特集した6月号に記載のフィッシングへの心構え5か条を思い出しながら、最後まで読んでいただき、貴所属の会計担当者に教えていただければ幸いである。

おさらい～フィッシング攻撃とは～

ボイスフィッシングを論じる前に、フィッシングの概要についておさらいしたい。フィッシングとは、実在する組織を騙って、パスワード、アカウントＩＤ、ＡＴＭ暗証番号、クレカ番号といった情報を詐取することの総称である。最も有名なのは、認証情報の更新が必要と謳い、メール（フィッシングメール）やＳＭＳで受信者を偽サイト（フィッシングサイト）へ誘導し、認証情報を入力させるといった手口である。フィッシングメールやサイトは本物をコピーして作られることが多く、素人での真贋判別はほぼ不可能と認識のうえ、正規サイト・アプリ等から直接確認することが唯一の安全策といっても過言ではない。

ボイスフィッシングとは

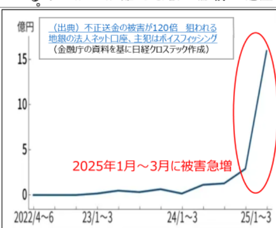
では次に、ボイスフィッシングについて説明する。ボイスフィッシングは、冒頭記載のとおり、攻撃者が認証情報窃取の過程で、電話等音声情報を用いるというのがその定義であり特徴である。縮めてビッシングとも呼ばれる。また、ＩＤ・ＰＷの入力後、追加の認証のために発行されるワンタイムパスワードすらも、電話で聞きだされるため、こういった対策も無に帰す点が脅威である。（通常ワンタイムパスワードは端末に縛られないため、攻撃者含む誰の端末でも使用可）

具体的な手法について、実際に１億円超の被害が発生した山形鉄道の事例を基に以下解説する。

なぜいま、ボイスフィッシングか？

今回ボイスフィッシングを取り上げた理由は、２０２４年秋以降、被害が急拡大しているためだ。地方銀行の法人口座からインターネットバンキングで不正送金される被害が目立っており、２０２５年１～３月の被害金額が16億円余りと前年同期（１３００万円）の１２０倍に膨らみ、このうち約13億円がボイスフィッシングによるものだ。ではなぜ、いま被害が拡大しているのか？考察の域を出ないが、生成ＡＩの高性能化が注目されている。日本語は、世界で相対的に見て難解な言語であり、攻撃者も少ないことから、攻撃者にとって自然な文面のフィッシングメールや音声ガイダンスの作成が困難であった。昨今、生成ＡＩの登場・高性能化に伴い、これまで言語の壁に守られてきた日本での脅威が高まっている。また、そのせいもあり、日本企業では、フィッシング耐性のある認証について、海外に比べて導入が遅れているとの指摘もある。加えて、法人においては、個人口座に比べて送金限度額が高く設定されているといった事由から、標的とされた可能性が高いとみられている。

▲インターネットバンキングによる預金等不正払戻し（法人被害状況）



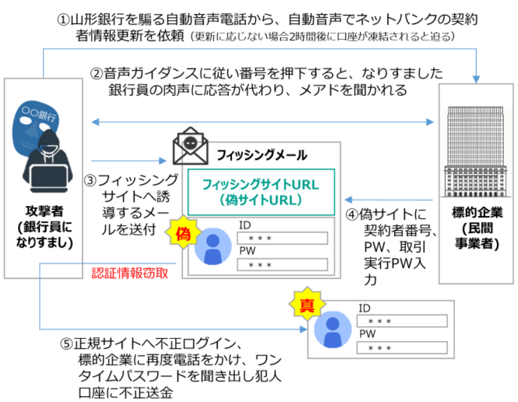
また、海外では、機械学習によるディープフェイクを悪用し、社長や上司を騙って送金を促す大胆な手口による被害も確認されており、今後も攻撃が高度化するおそれがある。

▼今年3月以降ボイスフィッシングによる実害を公表した金融機関

なりすまされた金融機関	発生日	判明した被害額
山形銀行	3月10日	1億円超（山形鉄道など）
高松信用金庫	3月12日	5,000万円（香川県内の企業）
武蔵野銀行	3月31日以降	非公表
琉球銀行	4月1日	1億円程度 （沖縄県内の企業1社で5,000万円の被害）
阿波銀行	4月2日	なし
筑波銀行	4月3日	非公表

【図解】ボイスフィッシングの詳細手口

【山形銀行を騙ったボイスフィッシングで山形鉄道が被害に遭った際の事例をもとに説明】



事案詳細

- フィッシング詐欺の被害にあったのは山形県内のローカル線であるフラワー長井線を運営する第三セクターの山形鉄道。被害額は約1億円にのぼることが筆頭株主である山形県より、3月12日に開かれた議会総務常任委員会内で公表
- 同社に対して山形銀行を装った自動音声の電話があり、応答すると同行ヘルプデスクを名乗る人物より山形鉄道の担当者のメールアドレスが聞き出され、その後そのアドレスに対して山形銀行の偽のサイトにつながるURLがかかれたメールが送られた。偽サイトへ誤ってログインに必要な情報（ID、パスワード）を入力をしてしまい、さらにワンタイムパスワードも電話を通じて聞き出されてしまったことから他行口座に同社の口座より1億828万円が不正に送金される事態となった
- 山形銀行においては法人インターネットバンキング（ネットEB）で他行あての即時振り込み機能を当面停止し、他行口座への振り込みは予約振込や総合振込を利用するよう呼びかけが行われている。（急な対応が必要な場合は窓口にて手続きを行うとしている。）
- 山形銀行では、自動音声による案内は一切行っておらず、顧客へメールや電話、SNSなどで契約情報やログイン情報を求めることも一切ないとして注意喚起を実施している
- 同日、複数の山形県内の複数企業に同じ手口を用いようとしていたとみられる被害が発生していると報じられた

（参考）piyolog「1億円を不正送金された山形鉄道への音声フィッシングについてまとめてみた」3.13

▼インシデントタイムライン

日時	出来事
3月10日午前	山形鉄道へ自動音声でフィッシング詐欺の電話（同様の不審電話が山形県内中心に複数の組織へ行われる）
同日	山形鉄道の口座より不正送金が行われる
同日夕方	山形鉄道より山形県へ不正送金被害に関する報告
3月12日	山形県議会で山形鉄道のフィッシング詐欺による被害が取り上げられる

国際電話の仕組みを理解しよう

その電話、ボイスフィッシングかもしれません！

みなさんは、電話番号の仕組みはご存じでしょうか？見慣れない国際電話（国をまたいで電話をかける場合に使う番号体系）は、注意が必要です。一口に国際電話に注意といっても、その仕組みを理解していなければ注意しようがなく、簡単に電話番号の仕組みを記載します。なお、フィッシングに対する心構えとして、自分で判断することは禁物であり、電話番号にさえ注意すればよいわけではなく、対策の十分性を確保するものではないことにご留意ください。

基本構造（国際電話の場合） 国際電話識別番号－国番号－ **基本構造（日本の場合）**（市外局番－市内局番－加入者番号）

項目	説明
国際電話識別番号	電話をかける相手国の識別番号(日本は「010」)
国番号	各国に割り振られた番号

項目	説明
市外局番	地域を特定する番号 （例：03は東京）
市内局番	地域内の電話交換局を区分
加入者番号	実際の契約者を識別する番号

種類	番号例	説明
固定電話	03-xxxx-xxxx	地域ごとの番号
携帯電話	090、080など	移動体通信向け
IP電話	050-xxxx-xxxx	インターネット回線を利用
フリーダイヤル	0120-xxxx-xxxx	着信者が通話料負担
ナビダイヤル	0570-xxxx-xxxx	全国共通で発信者が通話料金負担

▼国際電話　着信件数ランキング（2025年4月、トビラシステムズ調べ）

順位	国番号	国・地域名	主な手口の例
1	+1	北米地域（米国・カナダ等）	事業者や官公庁をかたる特殊詐欺
2	+86	中国	航空会社をかたる詐欺
3	+888	未割当	末尾が「0110」の警察をかたるオレオレ詐欺
4	+870	衛星通信サービス	事業者や官公庁をかたる特殊詐欺
5	+44	イギリス	統いや暗号資産に関する詐欺

ボイスフィッシングへの心構え

～ボイスフィッシングから当社資産を守るための心得～

ボイスフィッシングへの心構え四か条

一．知らない電話番号からの着信は信用しない
二．銀行担当者をかたる者から連絡があった場合は、銀行の代表電話番号、問い合わせ窓口で確認する
三．インターネットバンキングにログインする場合、メールに記載されているリンクではなく、公式サイトやアプリケーションからアクセスする
四．多くの銀行では、なりすましによるボイスフィッシングからお客さまを守るため、顧客へメールや電話、ＳＮＳなどで契約情報やログイン情報を求めることはない旨を注意喚起していることを覚えておく

【おわりに】

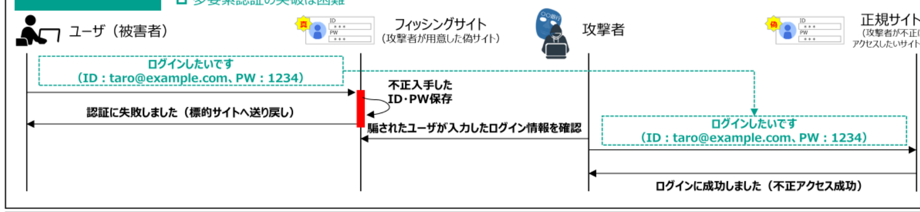
6月号で取り上げた、証券会社の口座乗っ取り事案で用いられたフィッシングは、自身や家族がNISA等をやっており、証券会社に口座を持っている人を中心に読んでいただきたかったという想いがありました。こちらは、業務中に警戒すべき攻撃であり、多くの職員に直接差し迫った脅威であるといえると思います。当部独自の情報網では、大手銀行でもボイスフィッシングを仕掛けられた事案の情報を入手しており、標的の従業員個人以外は正規のサイトが表示されるという驚きの手口もあるようです（それにより、調査が困難なため悪質）。フィッシングは、種類に限らず、自身で判別が困難であることを自覚することが重要です。安易な判断を避け、注意するポイントや抱くべき違和感（アウェアネス）を常日頃から情報収集しましょう。この新聞を読むことも情報収集です。

電話不要！リアルタイムフィッシングの仕組みを解説

ここでは、ボイスフィッシングのように電話や音声を使わずとも、利用者（被害者）がフィッシングサイトに認証情報（ＩＤ・ＰＷ等）を入力してしまったことを自動で攻撃者に通知し、その後ワンタイムパスワード要求画面を表示させるといった手口の「リアルタイムフィッシング」について解説する。通常のフィッシングとリアルタイムなフィッシングの手口について見比べて、巧妙化する多様なフィッシング攻撃について理解を深めよう。

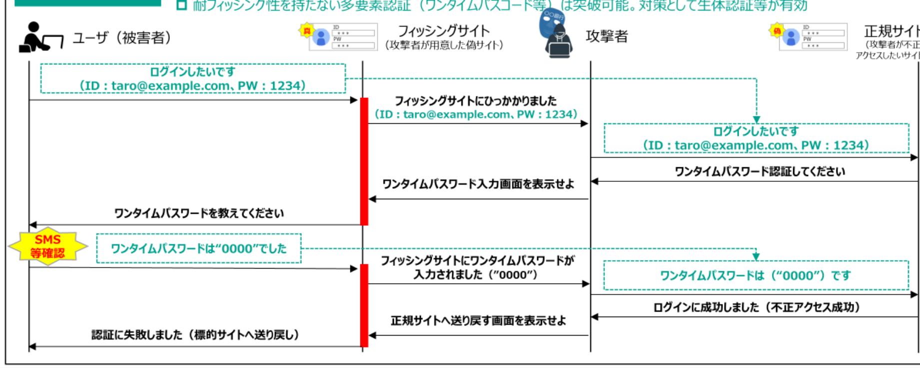
通常のフィッシング

- ☐ 入力されるIDやパスワード、クレジットカード番号を収集（窃取）
- ☐ 多要素認証の突破は困難

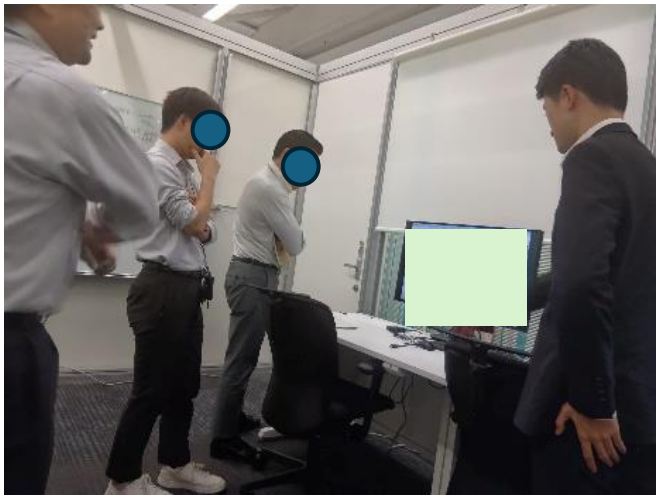


リアルタイムフィッシング

- ☐ ボイスフィッシングは、電話越しに被害者の操作を確認しながら認証情報入力へと誘導するが、攻撃者が自動で通知を得ながらリアルタイムに画面を表示させ、入力へ誘導するフィッシングおよびツール・攻撃代行サービス（Phaas:Phising as a Service）も存在
- ☐ 耐フィッシング性を持たない多要素認証（ワンタイムパスコード等）は突破可能。対策として生体認証等が有効



❸経営層ランサムウェア対応訓練
ー本社全層参加、シナリオ事前非開示、リアルタイム実施

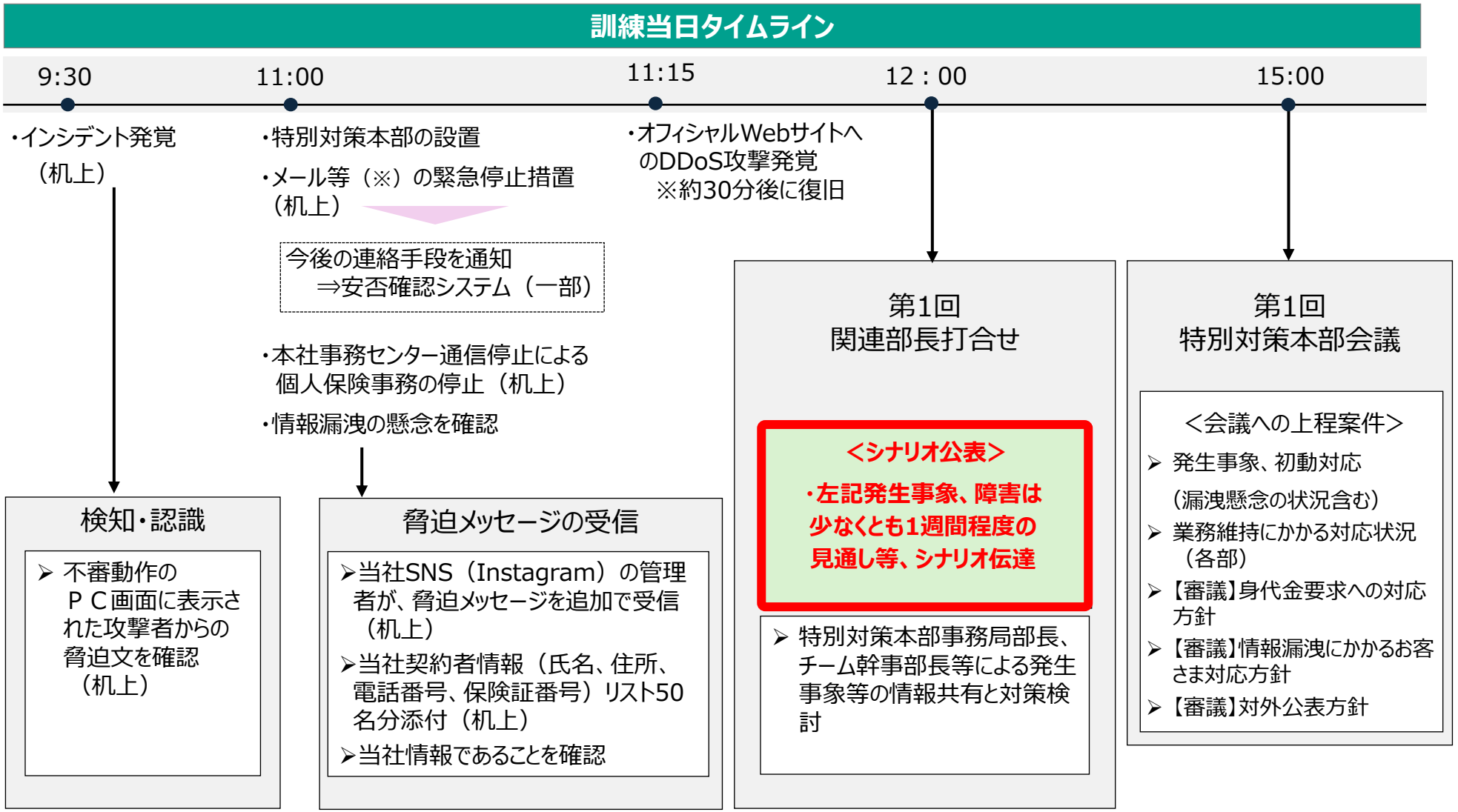


〈社内報に記載した概要〉
今年度は、訓練テーマを「基本動作の確認」から「基本動作の**定着**」へと高度化させ、その検証に向けて、他金融機関でもあまり類を見ない、以下のようなリアリティを追求する形式を試行しました。

【シナリオの事前非開示】
これまでの訓練では、インシデント発生の全容を事前に開示し、基本的な対応の流れを確認することが主な目的となっていましたが、今年度は、「基本動作の定着」を検証するために、**大手金融機関でもあまり類を見ない、シナリオ非開示**の訓練を実施しました

【リアルタイム性の追求】
訓練は、当日朝のインシデント発生からリアルなタイムテーブルに沿って、各部門で影響調査やエスカレーション、経営判断が進められました。関連部署では終日対応に追われ、臨場感・緊張感漂う雰囲気のもと対応が進められましたが、関係者全員の努力で無事に訓練を終えることができました

❸経営層ランサムウェア対応訓練
ー本社全層参加、シナリオ事前非開示、リアルタイム実施



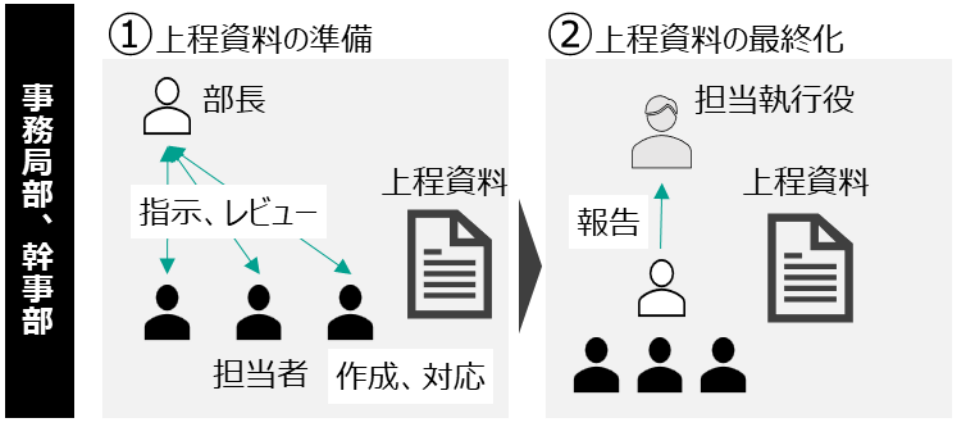
（※）社内メール・社外メール・インターネット・ファイルサーバを全社一斉停止。加えて、ランサム感染ビルである事務センタービルのネットワークを遮断

❸経営層ランサムウェア対応訓練
ー各部が事前用意したタスクリストを用いて対応手順を確認

＜訓練当日の参加者の動き＞

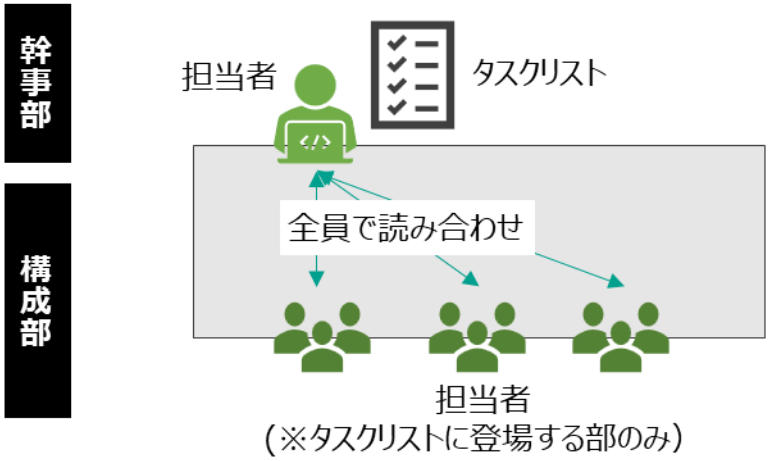
実働（経営層～担当者レベル）

第1回特対本部会議に向けて、部長の指示に従い
業務影響の確認および上程資料の作成



ウォークスルー（担当者レベル）

特対本部の管下チーム内で、
幹事部を中心としたタスクリストの読み合わせ



❸経営層ランサムウェア対応訓練
ー各部が事前用意したタスクリストを用いて対応手順を確認

＜タスクリストの作成＞

災害時対応用

特別対策本部 災害時対応チェックリスト

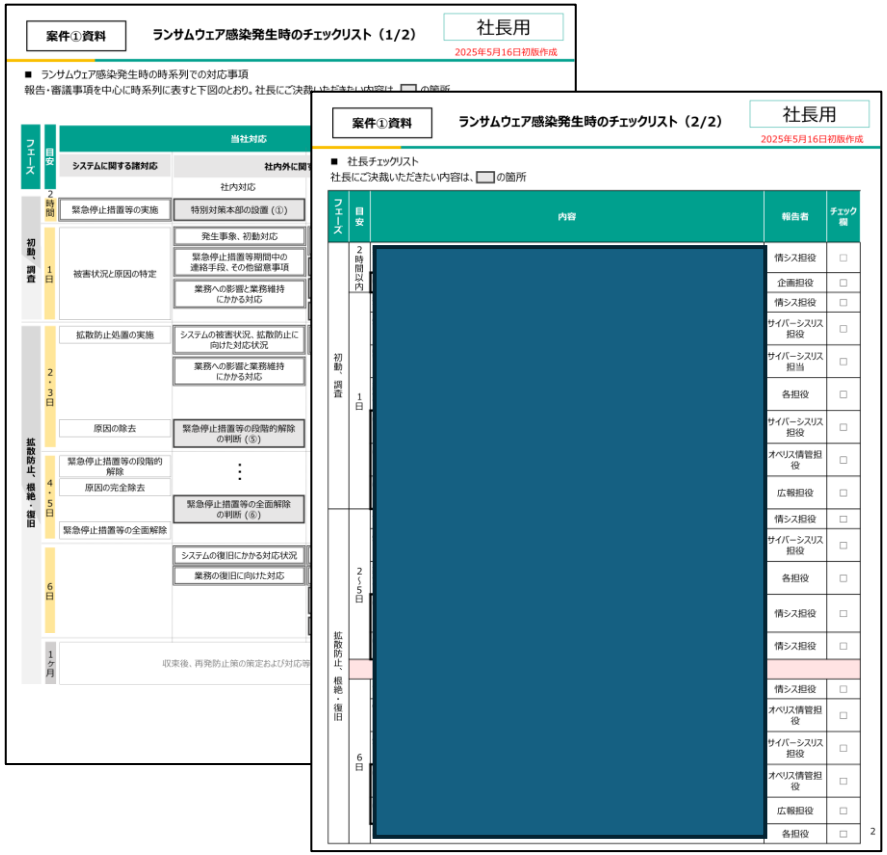
チーム・班名	特別対策本部	発災時間	勤務時間内	本部設置場所	責任

（1日目）第1回・第2回特別対策本部会議

時間	実施項目（★本部長（社長）決裁事項）	実施者	実施内容	チェック
30分～以内	社長報告（特別対策本部立ち上げ・第1回特別対策本部会議開催）	企画担当（総務部長・リスク統括責任） ⇒社長	・特別対策本部立ち上げ、チーム・班の設置： ①内線電話　②災害時優先電話（緊急連絡先一覧を使用）　③衛星電話 ※チーム・班等の体制は災害対策規則に基づくものとし、社長が臨機執行 ・第1回特別対策本部会議の開催（発災から3時間以内を目処）	□
〃	事務局への連絡・指示	企画担当（総務部長・リスク統括責任） ⇒事務局	・特別対策本部立ち上げ・第1回本部会議開催の連絡を指示	□
〃	特別対策本部メンバー、チーム・班への連絡	事務局⇒対象者	・特別対策本部の立ち上げ、チーム・班の設置、第1回特別対策本部会議の開催（開始時間・出席対象者等）をメールにて連絡	□
〃	全社への連絡	事務局⇒全社	・特別対策本部の立ち上げをメールにて連絡	□
3時間～以内	第1回特別対策本部会議開催 ※災害開催時を連絡			
〃	1. 特別対策本部体制の報告	事務局（企画）	・特別対策本部体制（チーム・班の構成等）の報告	□
〃	2. 発生事象の概要、国内の被害状況の報告	事務局（総務）	・発生事象の概要、国内の被害状況の報告	□
〃	3. 被災地域の状況報告			
〃	①役職員安否確認状況	人事	・役職員（LC等含む）安否確認状況の報告 ・実施期間後の判定者の状況の報告（受理中・予定者を含）	□
〃	②建物の被害状況	不動産・管理	・本社系3ビルの建物・設備の被害状況報告（不動産） ・本社系3ビル以外の拠点の建物・設備の被害状況報告（総務）	□
〃	③システムの被害状況	情シス	・各種システムの稼働状況、メインシステムセンターの被害状況報告（IS） （IS：ホスト等のバックアップシステムの起動、共通インフラ（メール・ｅファイル等）のバックアップシステムへの切替等に関する報告を含む）	□
〃	④社内物流にかかる状況	総務	・社内物流にかかる対応状況の報告（社内便の発着店舗状況、東京方面への郵送停止指示状況、事業者の対応態勢の確認状況） ・通関および郵送手段の確保状況報告	□
〃	⑤陸電経路にかかる交通状況	人事	・通勤（陸電及び陸路等）および公共交通機関の被害状況報告	□
〃	⑥社会・金融情勢	広報	・社会情勢及び報道での当社への対応や反響報告	□
〃	⑦決済サービス関連の状況の把握および資金繰り対策	収益	・全銀システム、主要な資金決済の利用銀行、オーバーナイトコール先状況、「本社経理システム」の稼働状況と利用可否 ・効果措置の妥否	□
〃	⑧L/C市場の被災状況と資金調達の対応、1週間先の資金繰り状況、証券市場の状況	運金	・L/C市場の被災状況と資金調達の対応状況（利用可否等を知悉会社、日本証券業協会等に確認）、1週間先の資金繰りの状況 ・証券市場の状況	□
〃	4. 本社系3ビルの当社来客者への対応状況	総務	・本社系3ビルの当社来客者（IS）への対応状況の報告 （IS）相談窓口来店者、応援室・応援スペース来客者	□
〃	5. 本社系3ビルの当社施設来場者・避難者への対応状況	総務	・本社系3ビルの当社施設来場者・避難者への対応状況の報告	□
〃	6. 役職員への指示事項等			
〃	①社内情報・備電方針	人事	・被災地内の役職員（LC等を含む）の社内待機・備電方針の報告 ・備電時のPC（Wi-Fi）・スマホ、マイスター・Myフォンの持参指示 ・在宅勤務者に対する指示	□
〃	②決定事項伝達の方法	人事	・発災現状以降の役職員（LC等含む）の電気（IS）の勤務利用について	□
〃	③各ホテルの建物状況	人事、大阪室	・本社系3ビル周辺、大阪のホテル建物状況の報告	□
〃	7. 政府・当局・生保協会等からの要請等	調査	・政府・当局・生保協会等からの要請・指示事項、協会の業務体制の報告	□
〃	8. 被災状況に応じた拠点の区分 ★	事務局	・建物・システム等の被害状況に応じた被災地域の拠点の区分と基本スタンスの起案（本部長決裁）	□
〃	9. 非被災地域における業務運営方針（全社共通）	事務局	・社内外における会食・イベント、会議・研修等の自粛	□
〃	10. 特別措置いの実施			
〃	①個人保険	事務金	・災害救助法適用を前提とした個人保険事務の取扱い （保険料払込猶予期間延長、支払手続き事務の一括省略）	□
〃	②企業保険	法人事務金	・災害救助法適用を前提とした企業保険事務の取扱い （保険料払込猶予期間延長、支払手続き事務の一括省略）	□
〃	11. 懸付委員への参集予告・受入準備状況（個人保険）	事務金 ⇒ 米大阪事務Cと連携	・個人保険事務の懸付委員に対する参集予告と受入準備に関する報告	□
〃	12. 懸付委員への参集予告・受入準備状況（企業保険）	法人事務金 ⇒ 米大阪法人事務サービスと連携	・企業保険事務の懸付委員に対する参集予告と受入準備に関する報告	□
〃	13. CC業務の対応状況	CC	・受電体制の変更に向けた準備状況	□
〃	全社への連絡			
〃	①全社メールの発信	事務局⇒全社	第1回特別対策本部会議決定事項の連絡	□
〃	②退メールの発信	各チーム ⇒全社、業務ライン	被災地内外の所属へ担当業務に関する詳細について連絡	□
8時間～以内	第2回特別対策本部会議開催 ※災害開催時を連絡			
〃	1. 発生事象の概要、国内の被害状況の追加報告	事務局（総務）	発生事象の概要、国内の被害状況の報告	□
〃	2. 被災地域の状況追加報告			
〃	①役職員安否確認状況	人事	・役職員（LC等含む）安否確認状況の報告 ・電陽死/現病/非罹患の自宅/在宅勤務/出張/管理中/予定者を現に	□

活用
・
作成

サイバー（ランサムウエア）用



案件①資料　ランサムウェア感染発生時のチェックリスト（1/2）　社長用

2025年5月16日初版作成

■ ランサムウェア感染発生時の時系列での対応事項

報告・審議事項を中心に時系列に表すと下図のとおり。社長にご決裁いただきたい内容は、□の箇所

フェーズ	目安	当社対応	
		システムに関する諸対応	社内外に関す
			社内対応
初動、調査	2時間	緊急停止措置等の実施	特別対策本部の設置（①）
	1日	被害状況と原因の特定	発生事象、初動対応
			緊急停止措置等期間中の連絡手段、その他留意事項
			業務への影響と業務維持にかかる対応
拡散防止、根絶・復旧	2・3日	拡散防止処置の実施	システムの被害状況、拡散防止に向けた対応状況
			業務への影響と業務維持にかかる対応
		原因の除去	緊急停止措置等の段階的解除の判断（⑤）
	4・5日	緊急停止措置等の段階的解除	⋮
		原因の完全除去	
		緊急停止措置等の全面解除	緊急停止措置等の全面解除の判断（⑥）
	6日	システムの復旧にかかる対応状況	
		業務の復旧に向けた対応	
	1ケ月	収束後、再発防止策の策定および対応等	

案件①資料　ランサムウェア感染発生時のチェックリスト（2/2）　社長用

2025年5月16日初版作成

■ 社長チェックリスト

社長にご決裁いただきたい内容は、□の箇所

フェーズ	目安	内容	報告者	チェック欄
初動、調査	2時間以内		情シス担役	□
			企画担役	□
			情シス担役	□
	1日		サイバーシリス担役	□
			サイバーシリス担当	□
			各担役	□
			サイバーシリス担役	□
			オペリス情管担役	□
			広報担役	□
			情シス担役	□
			サイバーシリス担役	□
拡散防止、根絶・復旧	2～5日		各担役	□
			情シス担役	□
			情シス担役	□
	6日		情シス担役	□
			オペリス情管担役	□
			サイバーシリス担役	□
			オペリス情管担役	□
			広報担役	□
			各担役	□

❸経営層ランサムウェア対応訓練
ー実現までの過程は一朝一夕にあらず。地道な訴求が重要

＜経営層へのサイバーセキュリティ対策の必要性訴求のあゆみ＞

No.	年度	題目	講演者	開催
1	2019	サイバーセキュリティ専担組織について	担当部長	経営会議
2	2020	最近のサイバーセキュリティ状況	社外講師	経営会議
3	2021	サイバー攻撃の傾向と当社の対応状況	担当部長	経営会議
4	2022	ランサムウェア攻撃の初動にかかる取組み	社外講師	経営会議
5	2022	ランサムウェア被害企業による講演	社外講師	経営会議
6	2023	当社のサイバーセキュリティ管理態勢	担当部長	取締役会
7	2024	（グループ会社役員向け） サイバー攻撃の傾向と当社の対応状況	上級 専門人財	説明会

❸経営層ランサムウェア対応訓練
ー実現までの過程は一朝一夕にあらず。地道な訴求が重要

＜経営層へのサイバーセキュリティ対策の必要性訴求のあゆみ＞

年月	訓練概要	訓練目的
2023年度（上期）	・シナリオ事前開示（ランサム）、報告資料を事前作成 ・丸の内本社ビル（役員・企画・人事・総務・経理・資産運用等）の緊急停止措置	・ランサムウェア対応の流れ、具体的実施事項の経営層との共有 ・すべての本社ビル（丸の内、東陽町、高田馬場）の緊急停止措置 ・チェックリスト（対応事項）の重大な不備・課題の検出・改善 ・報告資料フォームの蓄積・活用
2023年度（下期）	・シナリオ事前開示（ランサム）、報告資料を事前作成 ・東陽町ビル（個人保険事務、情報システム）の緊急停止措置	
2024年度	・シナリオ事前開示（ランサム）、報告資料を事前作成 ・高田馬場ビル（法人事務、コールセンター）の緊急停止措置	
2025年度	・シナリオ非開示（ランサムウェア攻撃、DDoS攻撃、東陽町ビル緊急停止措置）、実時間軸での報告資料作成、上長への報告	・対応スピードの体感（上長への報告を含む） ・チェックリストの実効性検証（役員・部長等の役割発揮）

（参考）「演習」と「訓練」は異なる概念

演習 (Exercise)	**訓練** (Drill)
✓ 「**検証**」と「**改善**」を重視	✓ 「**確認**」と「**習熟度の向上**」を重視
✓ 主な目的は総合的な対処能力の向上、学びと気づき、検証にもとづく改善	✓ 主な目的は対処能力の評価、手順の遵守・定着
✓ **想定外**の事象も扱う場合あり	✓ 主に**想定内**の事象を扱う
✓ 「うまくいかなかったこと」は良いこと (**改善に繋がる成果**)	✓ 「うまくいかなかったこと」は良くないこと (**問題・課題**)

100点満点をめざして取り組むのが「訓練」である一方で、
能動的に課題を洗い出したりするなかで高度化を目指すのが「演習」。
どちらも組織的な対処能力向上に資する取組である点で共通

（出典）日本シーサート協議会 - サイバー攻撃演習訓練実施マニュアル（https://www.nca.gr.jp /activity/pub_doc /drill_manual.html）

❹サイバーセキュリティを学べるボードゲーム
ービギナー向けにアウェアネス向上を企図して独自作成

ゲーム名称

Secure or Riske？

プレイ人数

問わない（1人～∞人）

プレイ時間

各テーマ10分～15分程度（全４テーマ）

プレイ対象

高校生・大学生、
普段セキュリティに馴染みのない社会人

ルール

各テーマごとに、７～８枚のカードが存在。カードには、テーマに沿った情報セキュリティに関する動作・考え方が示されており、それぞれを「Secure」か「Risky」か判断するクイズ形式のゲーム。クイズを通じてアウェアネス醸成が期待できる

ポイント

①アウェアネス醸成がテーマ
②学生層も気軽に取り組める
③ルールがシンプル（説明ほぼ不要）
④遊ぶ相手によっていろいろな考えが予想され、議論が深まる
⑤実践に即したクイズのため、日常生活に活きる

❹サイバーセキュリティを学べるボードゲーム
ービギナー向けにアウェアネス向上を企図して独自作成

SECURE OR RISKY?
CYBERSECURITY BOARD GAME
PRESENTED BY 明治安田

説明書		
プレイ人数	プレイヤー	1人以上
	進行役	とくに不要
プレイ時間	1テーマ10分～15分（全4テーマ）	
プレイ対象	高校生以上	

ゲームの目的

このゲームは、皆さんの日常生活において、情報セキュリティ事故に繋がりかねない事象や考え方に対して、注意・警戒心といった意識（アウェアネス）を向けさせることを目的に作られたゲームです。情報セキュリティといえば、今や情報の大部分がデジタル化されていることから、サイバーセキュリティをはじめとした高度なITリテラシーが求められていると思われがちですが、アウェアネスは誰でも身に着けることができるものです。アウェアネス醸成に向けては、リテラシーよりも、情報セキュリティ事故に繋がりかねない事象や考え方、引き起こされる事態を認識しておくことが重要です。このゲームを遊び終えるころには、日常生活において、今まで以上に、情報セキュリティ事故を未然に防ぐためのアウェアネスが醸成されているでしょう。なお、このゲームは主に高校生以上の学生向けに作られたものですが、普段情報セキュリティに馴染みのなかった社会人の方にも十分お楽しみいただけます

コンポーネント

・ゲームボード
・説明書（本紙）
・補足解説資料

＜別途用意する物＞
・筆記用具

ルールと流れ

ルールは非常にシンプルです。各テーマごとに、７～８枚のカードが存在しており、カードには、テーマごとの情報セキュリティに関する動作・考え方が示されています。カードごとに書かれていることが、「Secure」か「Risky」か判断し、「Secure」だと思うものを選びます。カードの背後には答えが隠されています。選んだカードが「Secure」であれば1pt、「Risky」であった場合は-1ptとカウントし、最終的に獲得したポイントを競います。ひとりでも遊ぶことができますが、複数人で班にわかれたりする等、議論しながらプレイを進めることで、より議論を深めることができるでしょう。なお、ゲームボードのクイズは、なるべく公的機関の資料等をもとに作成していますが、組織や個人によっては考えが異なることが予想されます。著作権・商標権の範囲内で自由に書き換えていただいてご利用いただけます。

テーマ①	テーマ②	テーマ③	テーマ④
認証情報の設定・管理	不審メール受信時の対応	SNS利用時の注意点	実践編！キャンパス生活の日常

アウェアネスが求められる背景

クレジット表記

すべて中西とAIで内製

❹サイバーセキュリティを学べるボードゲーム
ー各所での体験会を通じて、自社ブランドでリリース予定

セキュリティベンダ

＜参加者からの声＞
・セキュリティ教育関連のサービスを売り物にしているが、これだけシンプルかつみんなで楽しめたため、正直悔しいと感じた
・サイバーセキュリティを一般の職員に浸透させるためには、アウェアネスという考え方が重要と知り、それを醸成するためにデザインされたボードゲームまで作っているという徹底ぶりに驚かされた

日本シーサート協議会

＜参加者からの声＞
・特定の企業のために協賛することは組織の特性上難しいが、しっかりと明治安田さまとして展開ができれば、当組織でも体験会やサイバー関連のボードゲームをまとめた展示会に来ていただきたい
・サイバーセキュリティは考え方が分かれる部分もあるため、オープンソースでカスタマイズ性ありきでリリースするのであれば、文句は出にくいと思う

社内ではさまざまなボードゲームの体験実施

＜その他＞組織内での情報共有コミュニティへの参画勧奨

目次

サイバーセキュリティ情報共有コミュニティHANDBOOK
2025年度版

3．情報共有コミュニティごとの説明

3－1｜担当業務別分類

本章では、具体的にコミュニティごとに個別で紹介していくが、本項では、担当業務ごとに有用と考えられるコミュニティについて分類する。なお、これらは各コミュニティのしおりに記載している事項からの推察も含まれるため、必ずしも参画のうえ得られた情報とは限らない。また、分類の粒度上、網羅的にならないことにもご留意いただきたい。

〈フィッシング〉
〈インシデントレスポンス〉
〈脅威インテリジェンス〉
〈演習・訓練〉
〈SIRT高度化〉

[コラム]コミュニティにおけ

ここでは、前述の情報共有コミュニティにおける留
Give&Take）」について詳細する。これは、執筆
ティにおいてとくに重視される原則であると認識して

"Information sharing communities fai
（情報共有コミュニティは、受け取るだけで提供しな
出典：FS-ISAC Operational Guidelines / US DHS

FS-ISAC は、上記を「コミュニティの存亡に関わ
情報は、提供者（Provide）が減ると直ちに枯
して、実際の崩壊事例を提示している。しかしなが
てそうではない。以下に、参画者・運営者にとって

- **Give（情報提供）の中身は、大きな情報で**
  －NIST と ENISA は、共有すべき情報は "Per
  Intelligence と定義。小片でも、複数社から集まれば 攻撃キャンペーンの早期検知 が可能になるとしている
- **Take（受領）の責務は、情報を活用して返すこと**（US DHS ISAO Best Practices, FS-ISAC Sharing Handbook）
  －受け取った側にも明確な責務があるとしており、自社内で迅速に検証・活用する（SIEM/EDR/WAF 等へ即反映）、誤情報・不明点があればフィードバックを返す、重要度・再現性を整理しコミュニティに還元することで、価値の循環が生まれる
- **Give を促す仕組み（インセンティブ設計）をデザインする**（FS-ISAC "Member Incentives Program" / US DHS ISAO Framework）
  －世界の成熟コミュニティが共通して採用する仕組みとして、"Give した組織ほど得をする" 状態つくることがコミュニティ維持の必須条件（例：貢献ランキング・貢献バッヂ・年次表彰等貢献の可視化）

2025年度版

サイバーセキュリティ
情報共有コミュニティ
HANDBOOK

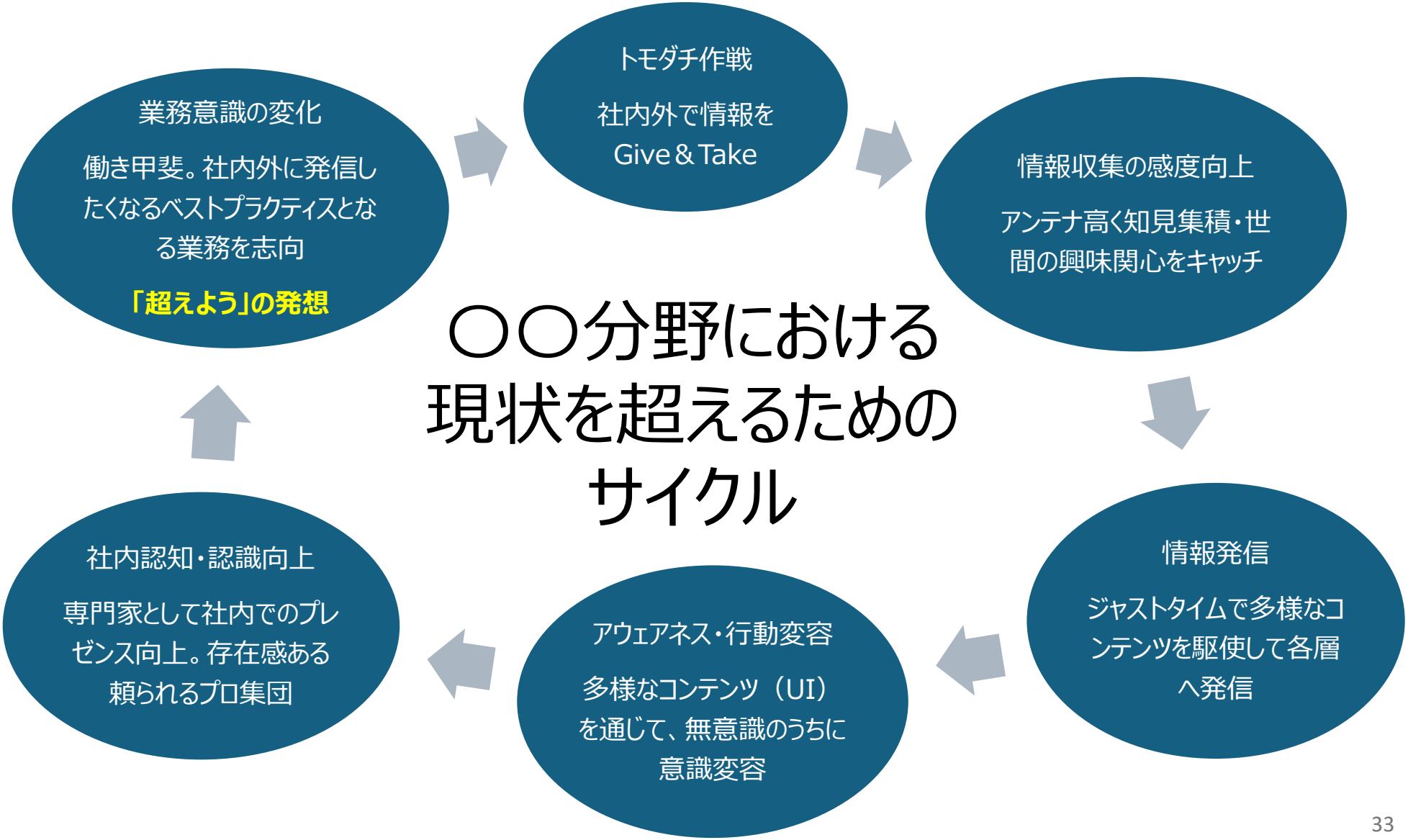
For Mitsubishi Group company

SAMPLE

三菱CC研究会 Mitsubishi Computer Communication Research Association

※貢献度・成果の可視化が重要※
明治安田では、スタッフ層は最低ひとつ以上外部コミュニティへ参画を勧奨。年度末には得た学びを部長の前で発表

めざすべき好循環。「超えよう。」は終わなき永遠のテーマ
実は、サイバーセキュリティ分野に限らない普遍的サイクル



本日の次第

０．会社概要ー明治安田のサイバーセキュリティ
１．サイバーセキュリティは全員参加。私たちが重視する“アウェアネス”
　～生保で初のフィッシング被害。被害に遭って改めて気付いたこと～
２．おカネに頼らず、独自のアイデアと想いで勝負する
　～意識向上と行動変容、具体的な４つの取り組みを紹介～
３．めざすべき好循環。「超えよう。」は終わなき永遠のテーマ
４．ビギナー向け サイバーセキュリティ企画部署で働く魅力
５．情報セキュリティが学べる！明治安田オリジナルボードゲーム実践

<ビギナー向け> 事業会社のサイバーセキュリティ企画部門で働く魅力

- 新たな脅威や当局要請が日々絶えないサイバーセキュリティ分野の業務は、常にチャレンジングなフロンティア領域
- 多くの事業会社ではサイバー人財が不足しており、多様なスキル・日々の学習が求められる反面、協同領域として社内外の関係者と相互研鑽できる魅力がある

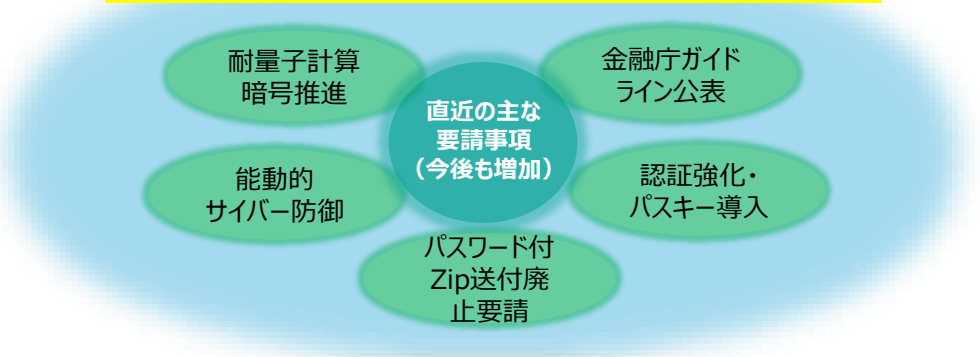
01 専門知識の習得	➢ 現在日本で17万人の不足が指摘されるサイバー人財の一員となり、将来的に貴重な戦力として活躍が期待できる
02 幅広いスタッフ能力の習得	➢ 多くの企業でサイバー人財が不足しており、業務が細分化されていない傾向あり。そのため、企画・調査・推進といった幅広いビジネス素養が身につく ➢ 高い挑戦意欲があれば、年齢関係なく活躍できる可能性を秘めている
03 全社最適なリスク管理の視点獲得	➢ 比較的経営層に近いところで執務できるため、高い視座に基づく社会・全社最適なリスクマネジメント、サイバーセキュリティの在り方について考えを深めることができる
04 社外の共助組織等への参画	➢ 自助・公助・共助（協働分野という特性）の枠組みを活かし、社外のさまざまなサイバー人財とかかわりながら知見を蓄積し、使命感を醸成することができる

＜ビギナー向け＞サイバーセキュリティ分野の業務でとくに重要と考える姿勢（文系人財）

- 新たな脅威や当局要請が日々絶えないサイバーセキュリティ分野の業務では、デイリーレベルの情報アップデートが大切
- ビジネスマンに求められる素養が膨大な現代において、社内外の関係者との折衝や推進力はとくに重要であり、高度な共感力・コミュニケーション能力が重要

情報のアップデートの重要性

当局等からの要請の増加



大規模サイバーインシデントの多発

社内外の関係者との協力

ほとんどの人にとって、サイバーセキュリティは詳しくなく、割ける脳の領域は一部に過ぎない可能性大

財務・会計知識、ITの知識、ビジネス法務、一般教養、サステナビリティ、DE＆I、経済、金融・FP知識、経済安全保障、個人情報保護、内部統制、地政学、コミュニケーション、体力マーケティング、マネジメント…、そしてサイバーセキュリティ

普段から存在感を発揮し、周囲との信頼関係を築き、巻き込んで推進する共感力、意思疎通が重要

- ✓ 普段から社内外の重要テーマをキャッチして発信。存在感と信頼感を醸成
- ✓ 相手の立場に立って考え、それ応じた言葉で取組の重要性を訴求
- ✓ 社内外での情報収集を欠かさない（社内で答えが得られることは限られている）
- ✓ サイバー投資にもヒト・モノ・カネ・情報が重要だが、実はもっと重要なのが、この根底にある経営層・周囲の「イシキ」

敵は世界、標的はいち事業会社や個人。
だから、サイバーセキュリティは共助・公助

本日の次第

０．会社概要ー明治安田のサイバーセキュリティ
１．サイバーセキュリティは全員参加。私たちが重視する“アウェアネス”
　～生保で初のフィッシング被害。被害に遭って改めて気付いたこと～
２．おカネに頼らず、独自のアイデアと想いで勝負する
　～意識向上と行動変容、具体的な４つの取り組みを紹介～
３．めざすべき好循環。「超えよう。」は終わなき永遠のテーマ
４．ビギナー向け サイバーセキュリティ企画部署で働く魅力
５．情報セキュリティが学べる！明治安田オリジナルボードゲーム実践

SECURE OR RISKY?

CYBERSECURITY BOARD GAME

PRESENTED BY

明治安田

PRESENTED BY 明治安田

説明書		
プレイ人数	プレイヤー	１人以上
	進行役	とくに不要
プレイ時間	１テーマ10分～15分 （全4テーマ）	
プレイ対象	高校生以上	

ゲームの目的

このゲームは、皆さんの日常生活において、情報セキュリティ事故に繋がりかねない事象や考え方に対して、注意・警戒心といった意識（アウェアネス）を向けさせることを目的に作られたゲームです。情報セキュリティといえば、今や情報の大部分がデジタル化されていることから、サイバーセキュリティをはじめとした高度なITリテラシーが求められていると思われがちですが、アウェアネスは誰でも身に着けることができるものです。アウェアネス醸成に向けては、リテラシーよりも、情報セキュリティ事故に繋がりかねない事象や考え方、引き起こされる事態を認識しておくことが重要です。このゲームを遊び終えるころには、日常生活において、今まで以上に、情報セキュリティ事故を未然に防ぐためのアウェアネスが醸成されているでしょう。なお、このゲームは主に高校生以上の学生向けに作られたものですが、普段情報セキュリティに馴染みのなかった社会人の方にも十分お楽しみいただけます

コンポーネント

・ゲームボード
・説明書（本紙）
・補足解説資料

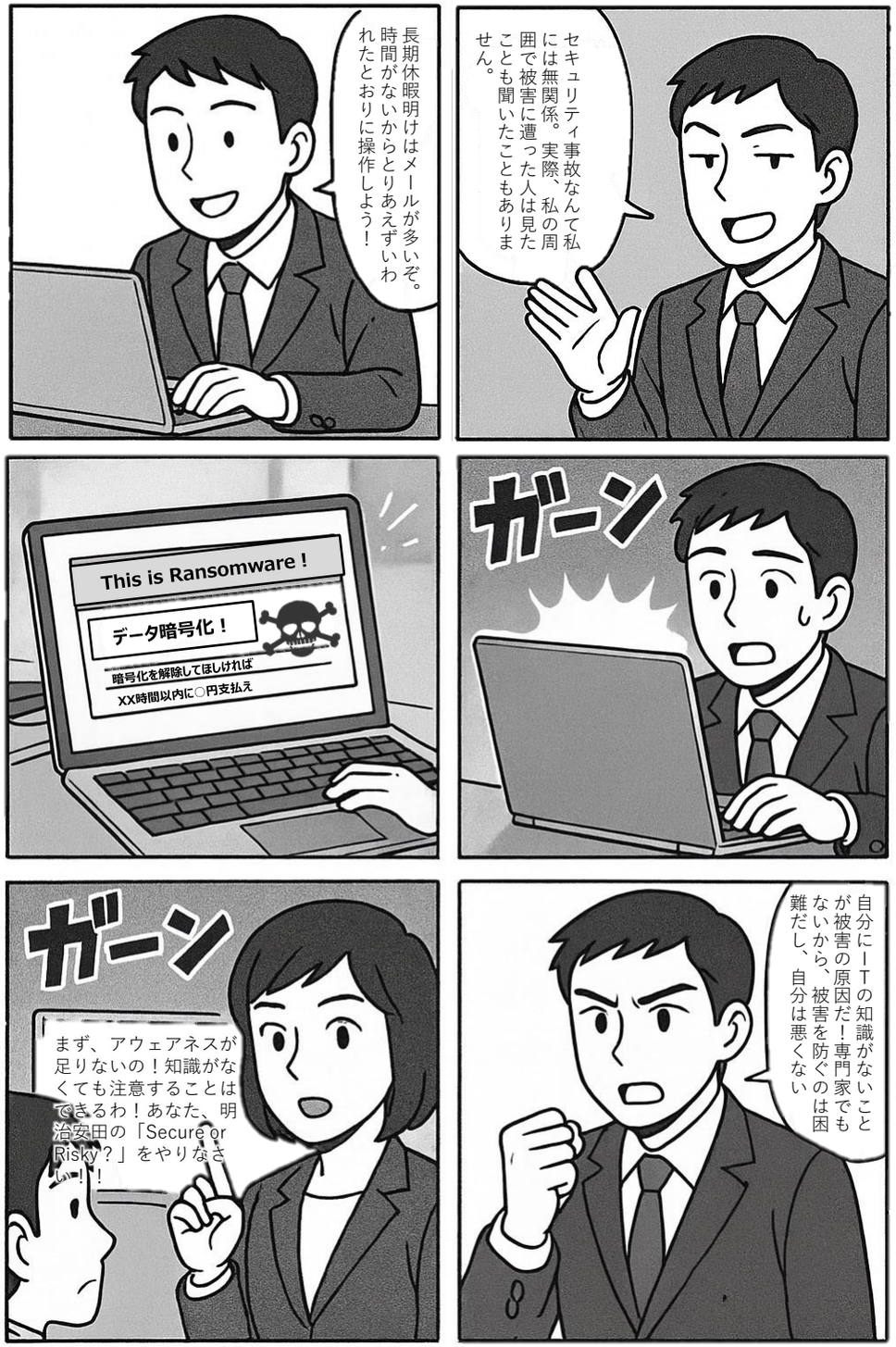
＜別途用意する物＞
・筆記用具

ルールと流れ

ルールは非常にシンプルです。各テーマごとに、７～８枚のカードが存在しており、カードには、テーマごとの情報セキュリティに関する動作・考え方が示されています。カードごとに書かれていることが、「Secure」か「Risky」か判断し、「Secure」だと思うものを選びます。カードの背後には答えが隠されています。選んだカードが「Secure」であれば1pt、「Risky」であった場合は-1ptとカウントし、最終的に獲得したポイントを競います。ひとりでも遊ぶことができますが、複数人で班にわかれたりする等、議論しながらプレイを進めることで、より議論を深めることができるでしょう。
なお、ゲームボードのクイズは、なるべく公的機関の資料等をもとに作成していますが、組織や個人によっては考えが異なることが予想されます。著作権・商標権の範囲内で自由に書き換えていただいてご利用いただけます。

テーマ①	テーマ②	テーマ③	テーマ④
認証情報の 設定・管理	不審メール受信時 の対応	SNS利用時の注意点	実践編！ キャンパス生活の日常

アウェアネスが求められる背景



クレジット表記

テーマ

認証情報の設定・管理

普段使用しているログイン時の認証情報（ID、パスワード等）は、いわば家や金庫の「鍵」に相当します。第三者の手に渡らないよう適切に設定・管理することが非常に重要です。これら認証情報を適切に設定・管理するために必要なことは何か理解しておきましょう。

明治安田

Secure だと考えた枚数 ＿＿＿＿ 枚

そのうち Secure ＿＿＿＿ 枚 ・・・①

そのうち Risky ＿＿＿＿ 枚 ・・・②

①－②＝ ＿＿＿＿ pt 獲得

PRESENTED BY
明治安田

1-1 Q Secure or Risky ?

生体認証とパスワード認証の両方を導入している場合、パスワード認証のみを導入している場合と比較して、パスワードを簡単にしてもよい。

明治安田

1-2 Q Secure or Risky ?

定期的なパスワード変更を要求することによるリスクは存在していない。

明治安田

1-3 Q Secure or Risky ?

紙媒体でのパスワード管理はサイバー攻撃からの対策として有効であるため、付箋にスマートフォンのパスワードを書いて、スマートフォンとカバーケースの間に入れて保管している。

明治安田

1-4 Q Secure or Risky ?

「パスワード」と「秘密の質問」は異なる認証要素であり、組み合わせることが重要だ。

明治安田

1-5 Q Secure or Risky ?

攻撃者が、有効期限付きのワンタイムパスワードを直接聞き出すことは考えにくい。

明治安田

1-6 Q Secure or Risky ?

自身の端末に送付されてくる有効期限付きのワンタイムパスワードは、他人の端末では使用できない。

明治安田

1-7 Q Secure or Risky ?

自身のオンラインバンキングに、見覚えのないアクセス履歴がないか定期的に確認し、誰かがログインした際は自身のメールに通知が来るよう設定している。

明治安田

1-8 Q Secure or Risky ?

利用するクラウドストレージサービスにおいて、ファイルを「リンクを知っている人なら誰でも閲覧可能（サインイン不要）」という権限設定で共有した場合、受信者がそのリンクURLを第三者へ共有しない限りは、安全な共有方法である。

明治安田

テーマ

認証情報の設定・管理

普段使用しているログイン時の認証情報（ID、パスワード等）は、いわば家や金庫の「鍵」に相当します。第三者の手に渡らないよう適切に設定・管理することが非常に重要です。これら認証情報を適切に設定・管理するために必要なことは何か理解しておきましょう。

明治安田

Secure だと考えた枚数 ＿＿＿＿ 枚

そのうち Secure ＿＿＿＿ 枚 ・・・①

そのうち Risky ＿＿＿＿ 枚 ・・・②

①－②＝ ＿＿＿＿ pt 獲得

SECURE OR RISKY? CYBERSECURITY BOARD GAME

PRESENTED BY 明治安田

1-1 Q Risky

生体認証も不正に回避される可能性があるため、パスワードの強度は依然として重要です。また、生体認証等を不正に解除する攻撃も存在することも理由のひとつです

明治安田

1-2 Q Risky

定期的なパスワードの変更を要求することで、利用者がパターン化されたり推測しやすいパスワードを設定する危険性があります。また、パスワードを使いまわす危険性もあります

明治安田

1-3 A Risky

紙媒体はデータとして保存していないためインターネット上での盗聴・窃取リスクが低い点では安全ですが、この保管方法では、スマートフォンを紛失したときの不正アクセスのリスクが高く危険です。

明治安田

1-4 A Risky

どちらも同じ、「知識認証」要素です。一つの認証要素のみである場合、漏洩時のリスクが急激に高まるため、ほかの認証要素（生体認証・所有物認証等）を組み合わせることで安全性が向上します。

明治安田

1-5 A Risky

ワンタイムパスワードは多くの場合、自身の端末以外にも届くおそれがあり、それを使って他者が他者の端末でログインできる可能性があります。攻撃者が電話や偽のログイン画面を使ってワンタイムパスワードを盗み出す攻撃に注意が必要です。

明治安田

1-6 A Risky

ワンタイムパスワードは多くの場合、自身の端末以外にも届くおそれがあり、それを使って他者が他者の端末でログインできる可能性があります。攻撃者が電話や偽のログイン画面を使ってワンタイムパスワードを盗み出す攻撃に注意が必要です

明治安田

1-7 A Secure

適切な対応ですが、事後的な対応といえますので、あらかじめ強固な認証方法を設定し、対策しておくことが有効です。不正ログインされた際は、ほかのID・パスワードが漏洩している懸念があります。

明治安田

1-8 A Risky

リンク共有はURL自体が認証情報であり、設定や環境によっては検索エンジンに拾われて全世界に公開される恐れがあるため、「転送されなければ安全」とはいえません。機密性確保のため、参照権限は最小限に留めて設定することが重要です

明治安田

テーマ

不審メール受信時の対応

悪意あるメールのリンク押下や、ファイル開封が原因でインターネットウイルスに感染するリスクがあることはご存じですか？適切な対応をしなければ、被害が拡大したり、加害者になることもあります。不審なメールの特徴や、受信時の対応について、意識向上をめざしましょう。

明治安田

Secure だと考えた枚数		枚
そのうち	Secure	枚 ・・・①
そのうち	Risky	枚 ・・・②
①－②＝		pt 獲得

SECURE OR RISKY? CYBERSECURITY BOARD GAME

PRESENTED BY 明治安田

2-1 Q Secure or Risky ?

ある日、学内の教授を名乗る人物から、「あなたの研究テーマに興味があるため、ぜひファイルを共有してほしい」といわれたため取り急ぎ送付し、後日直接本人に確認した。

明治安田

2-2 Q Secure or Risky ?

大学のポータルサイトからメールでシステム変更に伴い「再ログイン」が必要と促され、不審に思ったため、メールに記載の電話番号へ確認した

明治安田

2-3 Q Secure or Risky ?

国勢調査に回答しなければ統計法の違反となるため、メールでの依頼に回答した。

明治安田

2-4 Q Secure or Risky ?

不審メール受信時は、記載のメールアドレスを以前受信したときのものと目視で見比べ、正規のものかどうか判断している。

明治安田

2-5 Q Secure or Risky ?

不審メールかどうかは、不自然な日本語の有無や旧字体等の表記をみて判断できる

明治安田

2-6 Q Secure or Risky ?

メールやSMSで認証情報（ID、パスワード等）の入力を促すもののうち、こころあたりがあり注意の必要性を感じたものは、契約時に通知された正規のサイトやマイページ、電話経由で確認するようにしている。

明治安田

2-7 Q Secure or Risky ?

不審メール受信時は、同様の被害から家族やクラスメイトを守ることにつなげるため、彼らに適宜転送している。

明治安田

テーマ

不審メール受信時の対応

悪意あるメールのリンク押下や、ファイル開封が原因でインターネットウイルスに感染するリスクがあることはご存じですか？適切な対応をしなければ、被害が拡大したり、加害者になることもあります。不審なメールの特徴や、受信時の対応について、意識向上をめざしましょう。

明治安田

Secure だと考えた枚数 ＿＿＿＿枚

そのうち Secure ＿＿＿＿枚 ・・・①

そのうち Risky ＿＿＿＿枚 ・・・②

①－②＝ ＿＿＿＿pt 獲得

SECURE OR RISKY? CYBERSECURITY BOARD GAME

PRESENTED BY 明治安田

2-1 Q Risky

送付前に本人に直接確認することが望ましいです。教授に成りすました攻撃者からのメール（標的型攻撃メール）である可能性があります。また、研究情報は秘匿性が高い場合もあるため取り扱いには注意が必要です

明治安田

2-2 Q Risky

よくあるフィッシング手法です。フィッシングメールに記載の連絡先は、それ自体が虚偽である可能性があるため、電話をかけるのは危険。正規の連絡先へ問い合わせましょう。

明治安田

2-3 A Risky

国勢調査をメールで依頼されることはなく、フィッシング攻撃である可能性が非常に高いです。

明治安田

2-4 A Risky

表示するアドレス・差出人等は簡単に詐称できます。また、「I」と「ｌ」といったように文字列の微妙な違いに気づけないこともあるため、目視での判断は危険です。

明治安田

2-5 A Risky

以前なら通用した可能性がありますが、生成AIの進歩により、比較的言語の難易度が高いといわれていた日本語のフィッシング文面も自然な文章となってきており、十分な判断基準とはいえません

明治安田

2-6 A Secure

正しい判断です。巧妙な文面で、受信者の不安を煽ったり、個人情報入力へ自然と誘導されます。確認の必要性を感じた場合は、正規の連絡先へ問い合わせましょう。

明治安田

2-7 A Risky

不審メールを然るべき報告先以外に転送してしまうと、受信者が記載のリンク等を開いてしまう可能性があります。情報共有は必要ですが、逆にウイルス感染リスクをばらまかないようにしましょう

明治安田

テーマ

インターネット詐欺

SNSやインターネットを通じた投資詐欺の勧誘や特殊詐欺等の詐欺行為、情報漏洩が後を絶ちません。とくに、比較的金融に関する知識が未熟な学生が狙われる事案が多発しています。安易な儲け話やお得な話に乗らず、アウェアネスを働かせて消費者トラブルや情報漏洩から身を守りましょう。

明治安田

Secure だと考えた枚数 ＿＿＿＿ 枚

そのうち **Secure** ＿＿＿＿ 枚 ・・・①

そのうち **Risky** ＿＿＿＿ 枚 ・・・②

①－②＝ ＿＿＿＿ pt 獲得

SECURE OR RISKY? CYBERSECURITY BOARD GAME

PRESENTED BY 明治安田

3-1 Q Secure or Risky ?

金融機関等所属アナリストのブランドや本人を名乗る投資勧誘を受けた場合は、当人の実在有無や実績を確認し安全性を確認している。

明治安田

3-2 Q Secure or Risky ?

メールと比較して、警察や銀行等の電話番号偽装表示（なりすまし）は考えにくい。

明治安田

3-3 Q Secure or Risky ?

「副業紹介アカウント」のプロフィールに「金融庁登録済」「FX講師」とあれば信頼性は高い。

明治安田

3-4 Q Secure or Risky ?

SNSで詐欺にあった場合、警察や消費者センターに相談することは適切である。

明治安田

3-5 Q Secure or Risky ?

インターネットショッピングの際、銀行振り込みが指定されている場合、詐欺サイトであると判断する要素として有用である。

明治安田

3-6 Q Secure or Risky ?

現在使用される主要なSNS、メールソフト、ブログでは自身の写真をアップロードする際、位置情報等は自動で削除される。

明治安田

3-7 Q Secure or Risky ?

金融商品を日本の居住者に勧誘する場合、海外の金融業免許があれば国内登録は不要である。

明治安田

テーマ

インターネット詐欺

SNSやインターネットを通じた投資詐欺の勧誘や特殊詐欺等の詐欺行為、情報漏洩が後を絶ちません。とくに、比較的金融に関する知識が未熟な学生が狙われる事案が多発しています。安易な儲け話やお得な話に乗らず、アウェアネスを働かせて消費者トラブルや情報漏洩から身を守りましょう。

明治安田

Secure だと考えた枚数 ＿＿＿＿ 枚

そのうち Secure ＿＿＿＿ 枚 ・・・①

そのうち Risky ＿＿＿＿ 枚 ・・・②

①－②＝ ＿＿＿＿ pt 獲得

SECURE OR RISKY? CYBERSECURITY BOARD GAME

PRESENTED BY 明治安田

3-1 Q Risky

よくあるサポートを装った詐欺の手口です。指示の過程で個人情報を搾取されたり、不正なアプリをインストールさせられる、過度な料金を請求されることがあるため注意が必要です。

明治安田

3-2 Q Risky

電話番号は発信側が自由に番号情報を送れる仕組みのため、偽の番号を表示させる「番号なりすまし」が可能です。詐欺電話や偽SMSで悪用され、実在する企業や警察の番号を装うケースもあるため、不審に感じ無視できない場合は、一旦電話を切って正規の電話番号等からかけ直しましょう

明治安田

3-3 A Risky

登録番号の偽装や虚偽資格の記載は詐欺師がよく使う手です。手間だと感じても、金融庁のページで実在確認が大切です。

明治安田

3-4 A Secure

詐欺被害は早期相談が重要です。警察には被害届、消費生活センターにはトラブルの相談をすることで、二次被害を防ぎ、被害回復の情報提供や支援が受けられる可能性があります。

明治安田

3-5 A Risky

住所・顔写真・履歴書などの個人情報を搾取されるケースや、振り込み詐欺の加担者にされるケースもあるため、このような情報提供を依頼された場合は注意しましょう。

明治安田

3-6 A Risky

主要なSNSは自動削除されることが多いですが、メールソフトやブログ等では対応していない場合も多いため要注意です。また、写真に写り込んだユニークな建物や電柱、マンホールといった情報からも位置情報特定が可能なため注意が必要です。

明治安田

3-7 A Risky

SNSやマッチングアプリで知り合った相手からの暗号資産の紹介に伴う詐欺被害が増加しています。金融庁Webサイトで事前に登録業者か否確認し、仕組みを理解したうえで始しましょう。

明治安田

テーマ

実践編！キャンパス生活の日常

今回は、個別の学習テーマではなく、「キャンパス生活の日常」というシーンをテーマとして、日常生活のなかに潜む情報セキュリティリスクの認識、必要なアウェアネスの習得をめざします。これを通じ、情報セキュリティが身近で重要な事柄であると感じることができるでしょう。

明治安田

Secure だと考えた枚数		枚	
そのうち	Secure	枚	・・・①
そのうち	Risky	枚	・・・②
①－②＝		pt	獲得

SECURE OR RISKY? CYBERSECURITY BOARD GAME

PRESENTED BY 明治安田

4-1 Q Secure or Risky ?

学内の図書館で課題をしており、トイレで離席する際、私有ノートパソコンの画面をきちんとロックした（画面ロックはWindowsならショートカットキート「Windows」＋「L」で可能）。

明治安田

4-2 Q Secure or Risky ?

インターネットを通じてファイルをアップロードするだけであれば、脅威は存在しない

明治安田

4-3 Q Secure or Risky ?

取得したWebサイトのドメイン（インターネット上の住所）は永続的に管理できるため、たとえ古くても信頼できる企業が出所の二次元コードを読み取り、Webサイトへアクセスするうえでの脅威は存在しない

明治安田

4-4 Q Secure or Risky ?

カフェや公共施設でフリーWi-Fiを使って作業をしているが、盗聴されるリスクを考慮し、メールの利用に限って利用を控えてその他作業を実施した。

明治安田

4-5 Q Secure or Risky ?

アルバイトで利用している宣伝用SNSの共用アカウントは、1年に1回誰がログインできるか状態になっているかの確認をしている

明治安田

4-6 Q Secure or Risky ?

学内で落とし物と思われるUSBメモリを発見した場合、自身のパソコンで中身を確認し持ち主へ返却するようにしている。

明治安田

4-7 Q Secure or Risky ?

万が一自分のスマートフォンを紛失したときのために、キャリアのサポート電話番号をメモに書いて常時携帯している。

明治安田

4-8 Q Secure or Risky ?

購入したおぼえのない配達物を受け取った場合、同封物のQRコード等から持ち主を確認し、見覚えがなければ処分するようにしている。

明治安田

テーマ

実践編！キャンパス生活の日常

今回は、個別の学習テーマではなく、「キャンパス生活の日常」というシーンをテーマとして、日常生活のなかに潜む情報セキュリティリスクの認識、必要なアウェアネスの習得をめざします。これを通じ、情報セキュリティが身近で重要な事柄であると感じることができるでしょう。

明治安田

Secure だと考えた枚数 ＿＿＿＿ 枚

そのうち Secure ＿＿＿＿ 枚 ・・・①

そのうち Risky ＿＿＿＿ 枚 ・・・②

①－②＝ ＿＿＿＿ pt 獲得

SECURE OR RISKY? CYBERSECURITY BOARD GAME

PRESENTED BY 明治安田

4-1 Q Risky

私有端末携行時の注意点

無人状態で端末を放置すると、端末ごと盗難されたり、不正アクセス操作をされることがあります。自宅のような鍵のかかってない場所では、端末を持って離席するようにしましょう。

明治安田

4-2 Q Risky

インターネットへのファイルアップロード時の注意

情報漏洩の危険性があります。自身が投稿しようとしているファイル内容、ファイル名称、投稿先、参照範囲等をきちんと確かめることが重要です（ファイル共有サービス自体が危険な場合もあり）。

明治安田

4-3 Q Risky

二次元コードの読み取り

二次元コードは、ドメイン情報の表示形式を画像に変更したものです。古くなったドメインは、すでに他人が取得・使用しており、危険なサイトになっている場合があります。

明治安田

4-4 Q Risky

フリーWi-Fiの利用

秘匿化されていない通信は、Webサイトの閲覧履歴や入力内容（ID、パスワード、個人情報等）が盗聴される危険があり、メールに限らず、フリーWi-Fiの使用自体あまり推奨されません。

明治安田

4-5 Q Risky

権限設定

共有アカウントは、共有している人のうち誰が操作したか等、事後確認の観点等で情報セキュリティ上好ましくありません。退職者がログインできる状態は危険であり、即時の権限設定変更を徹底することが重要です

明治安田

4-6 Q Risky

詳細不明デバイスの接続

挿入しただけでマルウェア感染のリスクがあり、プライバシーの観点でトラブルになる可能性もあります。接続せずに持ち主を探し、見つからない場合は情報システム担当者や警察に提出しましょう。

明治安田

4-7 Q Secure

端末紛失時への備え

スマホやPCを紛失した際、第三者が操作できないよう遠隔でロックをかけたり、データを削除することができるサービスもあります。手書きメモからすぐにほかの電話等で依頼しましょう。

明治安田

4-8 Q Risky

ブラッシング攻撃・クイッシング攻撃

漏洩した個人情報をもとに商品を送り付け、商品の売買実績を不当に吊り上げたり、同封のQRコード等から情報窃取を試みる手法です。

明治安田