社外秘

第7期システム移行しました！！

公社における情報システム使用に関する周知事項(令和6年度 その３)

企画総務課システム担当　広瀬

本動画の目的

①業務上の誤った機器操作などによるご自身や組織への不利益が生じないよう、ＩＴリテラシー向上に役立つ情報をお伝えします

②「個人情報保護」の観点から、公社のＩＴ環境を含めてご留意いただきたい事柄などをお伝えします

③この動画は公社情報セキュリティ対策要綱第３条、並びに公社情報セキュリティ規定第６条に定める職員の教育等に寄与することを目的としています

社外秘

本動画の流れ

１　2024年のＩＴセキュリティ重大事件

２　公社にも身近なサイバー攻撃

３　求められる個人情報保護

最後に

1　2024年のＩＴセキュリティ重大事件

報道で見る重大事件（1～6月）

1月

○能登半島地震にともないSNS上で虚偽(デマ)のSOS投稿が拡散された

5月

○ハウスメーカーの更新停止HPへ不正アクセス、約83万件の個人情報流出

○札幌市の中学校で名簿を体育館に置き忘れ。撮影された画像がSNSへ流出した

○オンラインストア数社への不正アクセスでクレジット情報が流出

6月

○出版・エンターテインメントグループ企業への不正アクセス（ランサムウェア）により動画配信サイトが長期間停止、計約25万件の個人情報流出

○西日本の自治体から多くの業務委託を受けていた情報処理・機器サービス事業者への不正アクセス（ランサムウェア）により約150万件の個人情報流出

社外秘

1　2024年のＩＴセキュリティ重大事件

報道で見る重大事件（7～12月）

７月

○都内ガス会社と関連子会社で不正アクセスにより計約416万件の個人情報流出

○セキュリティメーカーのアップデート誤配信により世界各地でシステム障害

８月

○不動産企業の元社員が転職先へ個人情報持ち出し、約25,000件の個人情報流出

１０月

○関東の多くの自治体から業務委託を受けていた保育事業者への不正アクセスにより約16万件の個人情報流出

○職業体験型テーマパーク企業への不正アクセスにより約25,000件の個人情報流出

１２月

○中学生２人がDDoS攻撃代行サービスを利用して摘発

社外秘

～共通する落とし穴～

○ハウスメーカーの更新停止HPへ不正アクセス、約83万件の個人情報流出

○西日本の自治体から多くの業務委託を受けていた情報処理・機器サービス事業者への不正アクセス（ランサムウェア）により約150万件の個人情報流出

二つのインシデントに共通する要素は「外部から参照されないと思い込んでいたデータにアクセスされた」こと。

特に情報処理・機器サービス事業者のケースでは、本来契約時の仕様で削除するはずのデータを業務効率のために無断で残していたことが被害拡大につながった。

防ぐには…

参照・保管期限が過ぎた機密情報は確実な方法で削除または隔離する(させる)こと

例：管理簿を付ける、削除後画面のハードコピーを提出させる、など

社外秘

1　2024年のＩＴセキュリティ重大事件

昨年の事件の調査結果や判決も

大手通信事業者子会社での内部不正(2023年10月初報)

元派遣社員が長期間にわたって不正に派遣先受託事業の個人情報を持ち出し

全国で計約923万件、足立区では「国民健康保険 特定健康診査受診勧奨事業委託(H29年度)」において最大約7,000件の個人情報が第三者の名簿事業者へ流出した

大手学習塾元講師による盗撮・ＳＮＳ投稿(2023年8月初報)

元学習塾講師が勤務先に通う生徒を盗撮し、勤務先のデータベースから不正入手した詳細な個人情報を添えてSNSへ画像をアップロードしていた

大手通信アプリケーション事業者への不正アクセス(2023年11月初報)

委託先へ貸し出したアカウントへの不正アクセスをきっかけとして、確定分：約35万件、残り推定：約17万件のメッセージ本文を含む個人情報が流出した

社外秘

1　2024年のＩＴセキュリティ重大事件

昨年の事件の調査結果や判決も

大手通信事業者子会社での内部不正(

元派遣社員が長期

委託

た

大

ースから入手

し

稼セアップロードして

大ーション事業者への不正アクセス(2023年

初報)

委託先へ貸し出したアカウントへの不正アクセスをきっかけとして、確定：約35万件、残り推定：約17万件のメッセージ本文を含む個人情報が流出した

行政指導

社外秘

～“拡散・炎上”の時代～

○能登半島地震にともないSNS上で虚偽(デマ)のSOS投稿が拡散された

○札幌市の中学校で名簿を体育館に置き忘れ。撮影された画像がSNSへ流出した

○大手学習塾元講師による盗撮・SNS投稿(2023年8月初報)

三つのインシデントは、いずれもSNSで第三者を介して広範囲に影響を及ぼした。

SNSでは当事者が思うより各ユーザーが過敏な反応を示し、ネガティブな表現・出来事に対してはいわゆる炎上状態に発展する可能性がある。

LGBTQ…　べき論…　働き方…

特定政党…　一方的な価値観…

防ぐには…

① インシデントを察知したら最悪の事態を念頭において迅速に対応すること

② SNSで炎上した際には個人の判断で反論等のリアクション行為を行わないこと

社外秘

～手軽さが仇となる？～

Google フォーム

Google社のクラウドサービス群に「Googleフォーム」という機能があります。

この機能はGoogleユーザーなら誰でも入力フォームを作成し、その回答を収集できるというもので、公社ＨＰの申し込みフォームに似た機能を有しています。

ビジネスユースにも耐える非常に便利な機能である反面、設定ミスが個人情報の漏洩を引き起こすケースも急増しているようです。

【漏洩した法人の例(2024年のみ)】

都内国立大学、中部地方公立大学、関西私立大学、川崎市、鎌倉市、山形市、大手芸能プロダクション、Ｊリーグ加盟サッカーチーム（２チーム）、など

防ぐには…

大規模なアクセスが見込まれる場合は別途ご相談ください。

業務上のオンラインフォームは公社HPの申し込みフォームを使用しましょう

※Googleフォームを利用する場合は、設定をしっかり確認しましょう

社外秘

1　2024年のＩＴセキュリティ重大事件

2024年の世相のまとめ

報道ベースではランサムウェア一強

企業にとっては「感染＝致命傷」のサイバー攻撃として不動の横綱級。

特に６月の出版・エンターテインメントグループ企業への被害がセンセーショナルかつ長期にわたって報じられたことが印象的。

標的型メール攻撃が劇的な進化を遂げる

従来の学習型ＡＩに加えて生成ＡＩやディープフェイク技術が、より説得力のある偽メールの作成を実現しつつある。

細かな記事ではサポート詐欺による個人情報流出が猛威を振るう

学校や自治体の委託先を中心としてサポート詐欺による被害報告が後を絶たない。

攻撃者にとっては、目論見が成功すれば他のサイバー攻撃より確実かつ容易に相手のネットワークに侵入できるため、今後も手口の洗練・進化が懸念される。

社外秘

８月周知の資料より

キングオブサイバー攻撃「ランサムウェア」

【名前の由来】

身代金(ransom)とマルウェア(malware)を合わせた造語です

※マルウェアとは不正なソフトウェアの総称です

【ランサムウェアの特徴】

〇感染したPC・ネットワーク内のファイルを暗号化してしまう

〇暗号化と並行してファイルのデータを攻撃者側のネットワークへ持ち出す

〇暗号化したファイルの復号・返還と引き換えに金銭を要求する(二重脅迫型)

社外秘

2　公社にも身近なサイバー攻撃

年々巧妙になる「標的型メール」攻撃

手口のおさらい

　標的型メールとは、もっともらしい文面の偽メールを作成し、受け取った相手に思いどおりの行動をさせるメールのことです。

　大体の場合、その被害は次の二つに大別されます。

①URLで有害なWebサイトなどへ誘導し、機密情報を入力させる

②添付ファイルを実行させることでマルウェアに感染させる

メールの文面で金銭振込などへ誘導するビジネスメール詐欺(BEC)という派生形もあります

今後はより“もっともらしい”メールが増える？

　生成ＡＩ技術の登場・進歩により、外国人攻撃者でも違和感のない日本語の文章を作成することが可能になりました。

　このことから、今後は見破りにくいメールが増えることが予想されます。

社外秘

更新 返信 全員に返信 転送 メール操作 絞り込みなし

1 / 1 表示: 100件

件名	送信者
法人様向け特価商品（PC、液晶ディスプレイ等）のご案内	ソニーネットワークコミュニケーシ
【Alpha-prm.jp by OTSUKA】メールボックスのストレージ容量が少	OTSUKAカスタマーサポート

はいはい、なりすましメールね～

件名 【Alpha-prm.jp by OTSUKA】メールボックスのストレージ容量が少ない -

送信者 "OTSUKAカスタマーサポート" <no-reply@alpha-prm.jp>

メールボックスのサイズがクォータ制限に達しました

注意 ： mailer-daemon@kousya.jp

メールボックスのサイズがクォータ制限に達しました - クォータ
うに、ログインしてクォータを更新してください

メールサービスの中断を防ぐため、早急な更新が必要です。

メールクォータを更新する

検索タイプ　検索キーワード

alpha-prm.jp　検索

［ドメイン情報］
ALPHA-PRM.JP

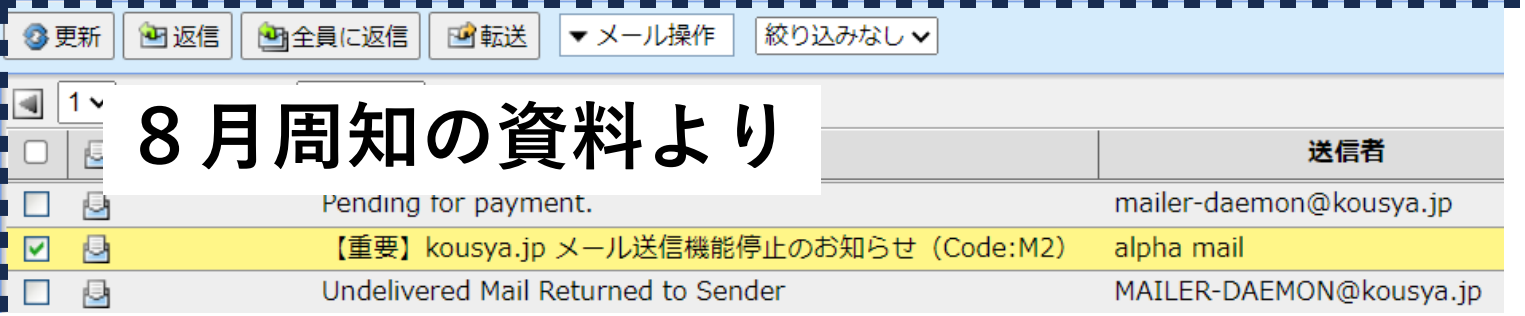
株式会社　大塚商会
Otsuka Corporation

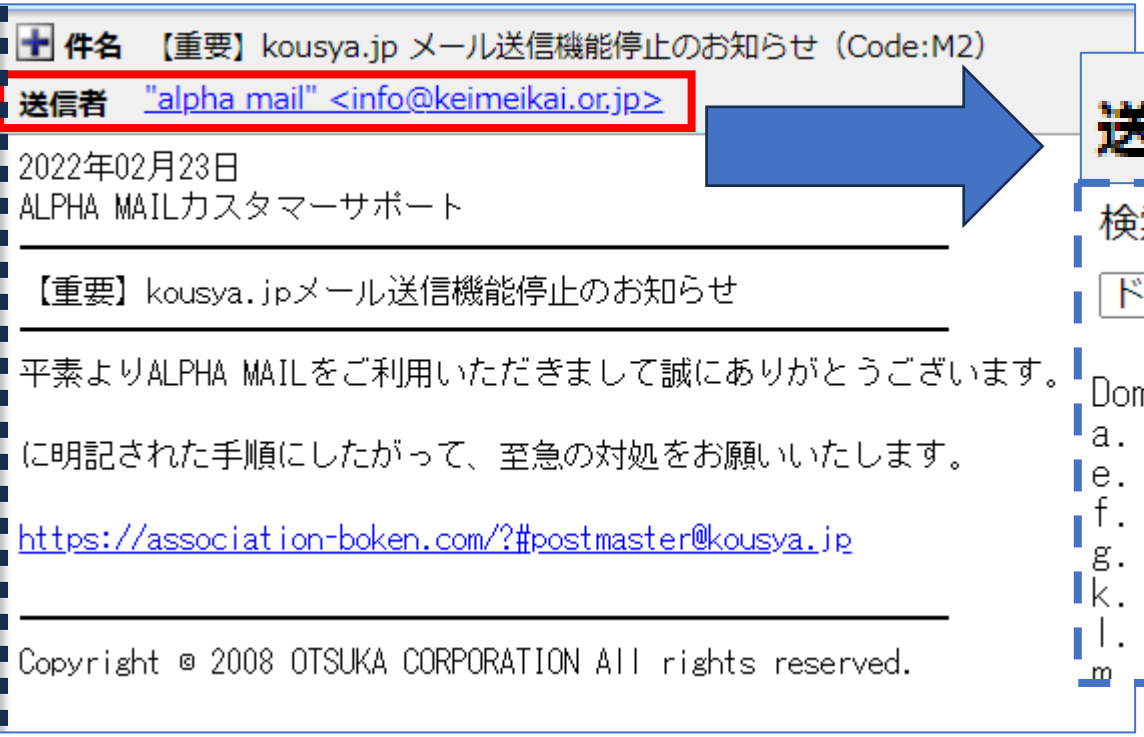
本物!?

※案の定、なりすましメールでした

８月周知の資料より

送信者の表示名を
そのまま信じると・・・

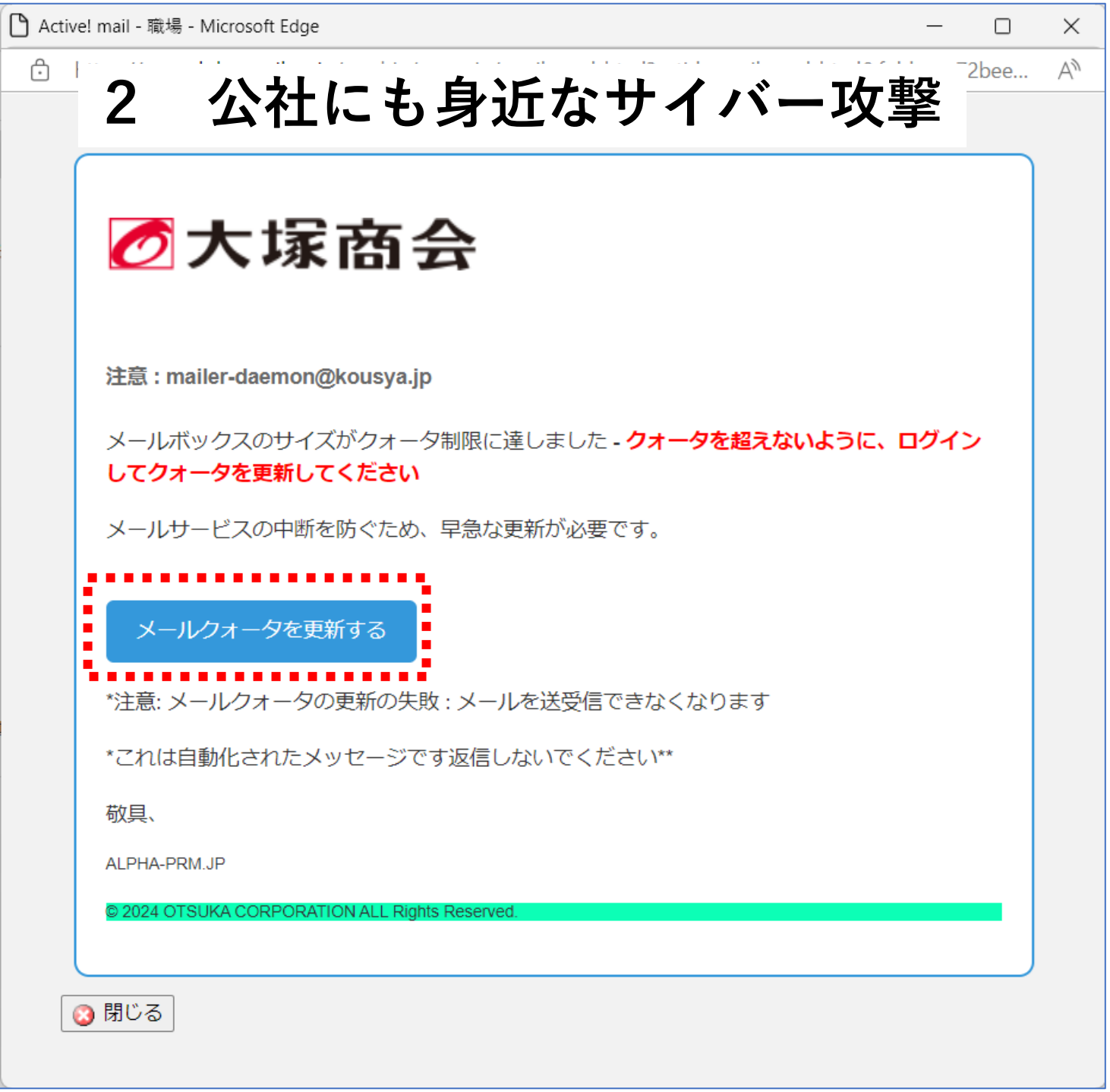




送信者欄に表示される名称は送り手が指定することができます
返信する前に、できればメールアドレスも確認しましょう

社外秘

2　公社にも身近なサイバー攻撃



メールをHTML表示したものです。

恐らく「メールクォータを更新する」というボタンをクリックすると、ログイン画面に見せかけて何かしらの情報を入力する画面へ誘導するクレデンシャルフィッシング詐欺の類だろうと思われます。

ボタンのURLは次のとおりです。

https://url-shield.securence.com/?p=1.0&r=adrienne@amg-law.com&sid=1690213621887-022-00172088&s=g53hchkx&n=brgejkixh&ms=0.5,0.0,0.0,0.5&u=http://www.Kousya35698900.stbasil.techiex.com/?vc=mailer-daemon@kousya.jp

長い…
キモい…

アルファメール関係のURLなら製品名を示唆する文字列が入るはずなのですが、どこにも見当たらないので怪しいと感じました。

※クリックしてみたらi-FILTERがはじいてくれました

社外秘

2　公社にも身近なサイバー攻撃

サポート詐欺に騙されるな！！

サポート詐欺については別の動画で集中的に取り上げています。
お時間のある方はぜひご覧ください。

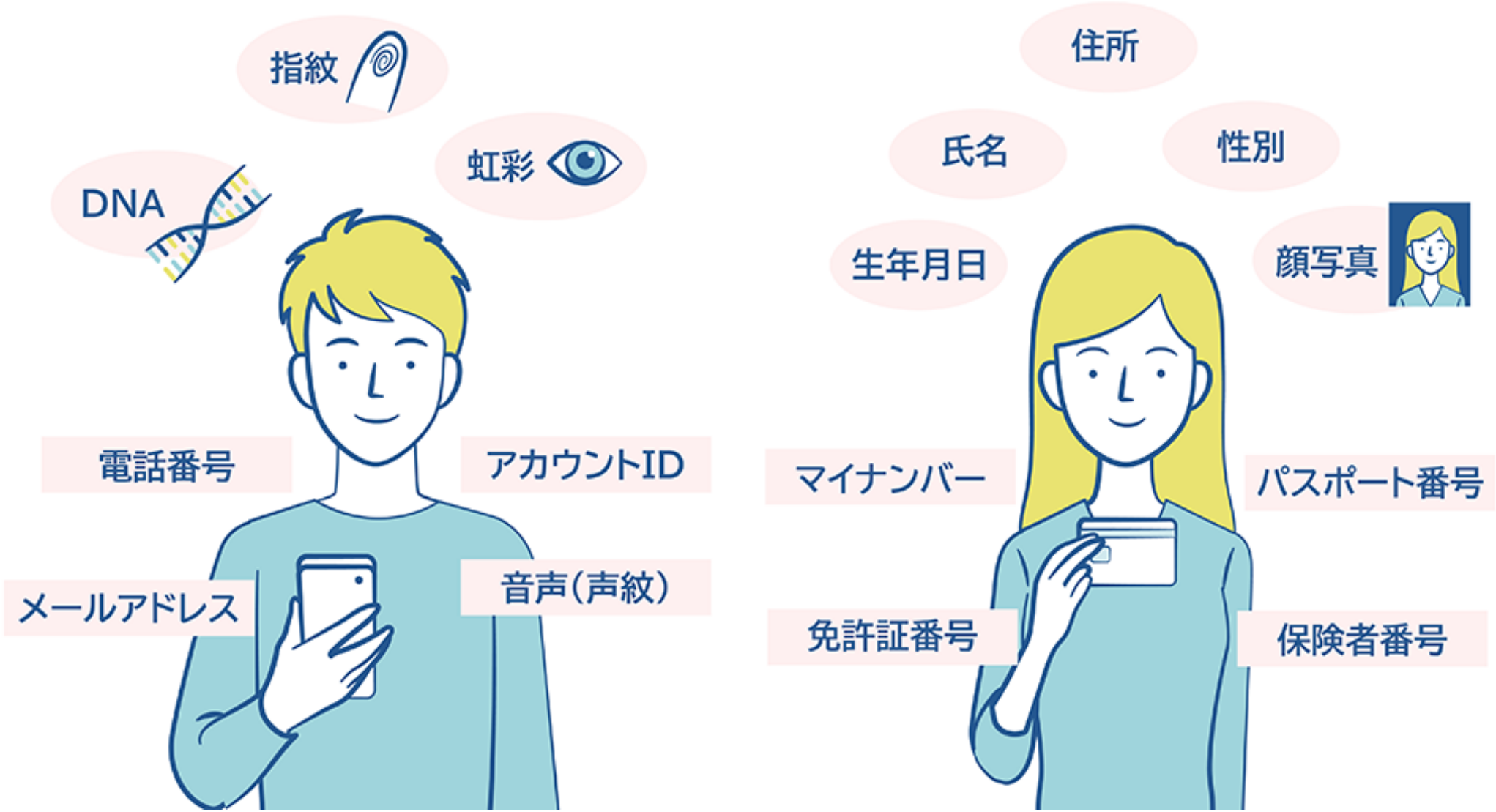
公社における情報システム使用に関する周知事項(令和6年度 その３)

番外編

企画総務課システム担当　広瀬

社外秘

3　求められる個人情報保護



出展：政府広報オンライン(https://www.gov-online.go.jp/useful/article/201703/1.html)を一部加工

社外秘

3　求められる個人情報保護

個人情報とは

個人情報とは、個人情報保護法において次のように定義されています。

個人情報保護法 第二条一項(要約)

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの（他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む。）、または個人識別符号が含まれるもの。

単体、または組み合わせて個人を特定できる情報が個人情報なのです。

3　求められる個人情報保護

個人識別符号とは

個人識別符号を簡単にまとめると次のとおりです。

① 特定の個人に固有の身体的特徴についての情報

例：DNA、指紋、静脈、声紋、虹彩、骨格、歩行パターン、など

② 公的機関が特定の個人に割り当てた符号(番号)

例：マイナンバー、基礎年金番号、旅券番号、在留カード番号、など

マイナンバーは個人番号法に定める取り扱いを

個人識別符号の中でも、特にマイナンバー(個人番号)は特定個人情報として、取り扱う事業者には法令及びガイドラインに則った厳密な管理が求められています。

例：**事務スペースの物理的隔離、取得可能事業の限定、**
取得～廃棄の管理簿の整備、など

社外秘

3　求められる個人情報保護

本人(保護者)の意志を尊重して取得しましょう

個人情報は利用目的を予め明確にした上で取得し、その目的の範囲内のみで利用することが求められます。

その中でも要配慮個人情報に位置付けられる項目は取得に先立って本人(保護者)の同意を得ることが必要です。

要配慮個人情報とは

当該事実の公開によって、本人が差別的な扱いを受ける恐れのある情報です。

【要配慮個人情報の例】

人種、国籍、信条、信教、性的マイノリティ指向、診療・健診情報や調剤情報などの病歴、前科・前歴、犯罪被害など

「本人が気にしてないから～」は通用しません！

社外秘

３　求められる個人情報保護

「そんなつもりじゃなかったのに」流出へつながることも

自分のSNSを投稿しただけなのに…

〇2015年、市役所職員がSNSへ投稿した職場の風景写真に税務情報が写り込み

〇2024年、都立高の卒業証書を筆耕した事業者が制作物を撮影してSNSに投稿

アプリは閉じたつもりだったのに…

〇2023年、特別区の納税案内センターにおいて、施設管理者が卓上のスマートフォンの動画配信アプリを起動したまま約２時間半にわたって業務にあたり、計５名に電話業務の内容などを視聴された

ちょっと置いておくだけのつもりだったのに…

〇2024年、特別区においてレイアウト変更にともなう一時的な設置が長期化した結果、個人情報が含まれた文書保存箱が1か月あまり、職員以外も立ち入り可能な非常用スペースに放置された

社外秘

3　求められる個人情報保護

こんなところからも個人情報は漏れるかも

何気ない会話から…

例えばホームページからの申し込みに関する問い合わせで考えてみます。

Q1：「入力した住所と建物名って、何て書いてましたか？」
A1：「えーっと、〇〇３丁目の△△マンションになってますね」

アウト！

Q2：「二人申し込んだはずなんですけど、二人目誰になってますか？」
A2：「お二人目は●●様のようですね」

アウト！

意外と厳しい個人情報開示のルール

正式に収受して公社保有となった個人情報については、本人であっても開示請求を経なければ本来は教えることができません。

このような問い合わせへの対応プロトコルは予めご検討ください。

社外秘

3　求められる個人情報保護

個人情報保護委員会
Personal Information Protection Commission

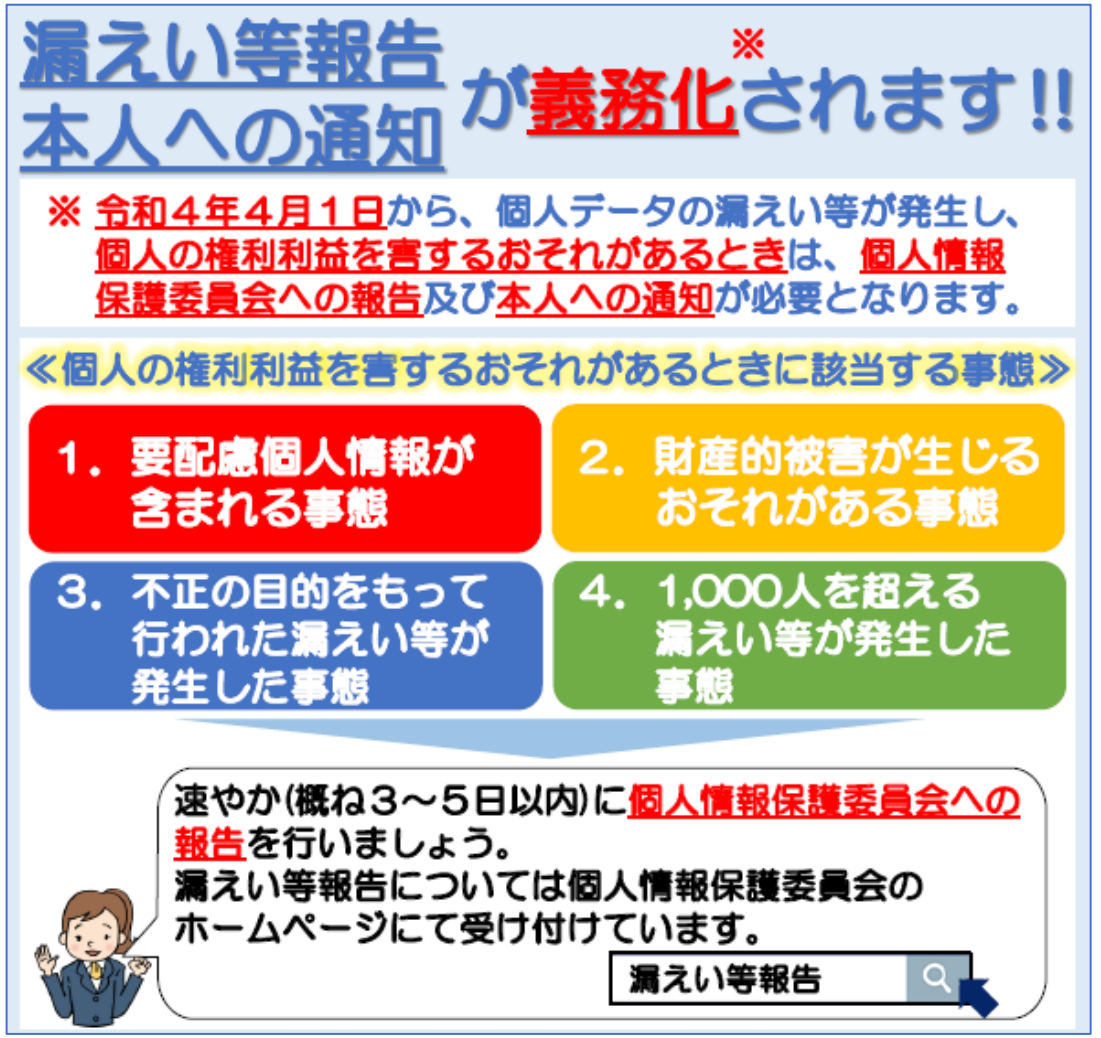
個人情報が流出した場合の対応とは①

個人情報保護法の定めに沿った対応

重大な流出事案と見なされる場合は、個人情報保護委員会に速報・確報を行うとともに、本人への通知も必要となります。

特に、③の「不正な目的をもって～」はサイバー攻撃も対象に含まれます。

そのため、ランサムウェア、サポート詐欺などの種別を問わず、サイバー攻撃の影響が個人情報のデータ領域に及んだ時点で、実害の有無に関わらず報告と本人通知を行う必要があります。



出典：個人情報保護委員会
令和2年改正個人情報保護法の周知チラシ（一部抜粋）

社外秘

3　求められる個人情報保護

個人情報が流出した場合の対応とは②

世間一般で求められる対応

　個人情報が流出した場合、個人情報保護法の定めによらず、世間一般では特に関係者へ向けた誠意ある対応として、概ね次のアクションが要求されます。

【一般的には…】

- 被害発生時の事実と状況の速報
- 調査が進んだ際の続報
- 事態沈静化及び被害影響範囲の確報
- 再発防止策の提示

ほとんどの場合で自組織ホームページに掲載

- どのくらいの頻度で更新？
- どのくらい詳しい内容？
- どのくらいの期間掲載？

最悪の場合…

　流出被害当事者による原告団や関係企業による訴訟が提起されることも…。

例：2014年の大手教育事業者顧客情報流出に対する集団訴訟

ランサムウェア被害に遭った企業におけるホームページ上での公式発表

プライバシーマーク付与の一時停止について		2024.12.24 | お知らせ
不正アクセスによる個人情報漏えいに関するお詫びとご報告	← 確報	2024.10.04 | お知らせ
ISO27001認証及びISO27017認証の一時停止について		2024.09.02 | お知らせ
ランサムウェア被害の発生について（続報2）	← 続報	2024.07.03 | お知らせ
ランサムウェア被害の発生について（続報）	← 続報	2024.06.06 | お知らせ
ランサムウェア被害の発生について	← 速報	2024.05.29 | お知らせ

社外秘

1. 概要

2024年5月26日、悪意のある攻撃者による不正アクセスを受け、当社の情報処理センター及び全国営業拠点の端末やサーバがランサムウェアによって暗号化された事を確認いたしました。2024年6月18日には攻撃者グループのリークサイトで、攻撃者が窃取したとされる情報を公開するためのダウンロード用URLが掲載されました。

ダウンロード用URLから公開された情報は調査の結果、当社のサーバから流出したものであり、一部のお取引先様の顧客に関する個人情報が含まれている事が判明しました。ダウンロードファイルは2024年10月4日現在消失しており、ダウンロードができないことを確認しております。

2. 原因

VPNからの不正アクセスにより当社ネットワークに侵入した攻撃者によって、当社が一部のお取引先様の受託業務の作業工程で発生した帳票データや検証物の一部の情報が窃取されました。当該情報を取り扱ってはならないサーバに作業の効率を図るため便宜的に保管し、また業務終了後には速やかに削除すべきデータを削除することができておりませんでした。当社の情報の取り扱いが原因で、攻撃者によるデータの窃取を許すこととなり、多大なご迷惑をおかけすることになりましたこと、重ねてお詫び申し上げます。

なお、現時点で、本件に起因する個人情報を用いた不正利用等の二次被害については、確認されておりません。引き続きお取引先様名、または当社名を騙る不審な電話や郵便物等による勧誘や詐欺には十分にご注意いただき、不審に思われた場合は最寄りの警察にご相談いただくようにお願い申し上げます。

3. 再発防止策

侵入経路となりましたVPNを使用しない体制とし、さらに認証強化を図り不正アクセスが起こらない環境を構築いたします。環境構築までの間は外部ネットワークとの接続を制限し業務対応を行います。

受託業務におけるデータの取り扱いについては管理区域外へデータの移送ができない環境を構築し、業務上必要なデータについては、保管期限など取り扱いルールを明確に定め業務終了後にデータを確実に削除します。そして、これらのルールが遵守されるよう監査を徹底してまいります。

また、社員に対して個人情報を含む情報セキュリティに関する教育とルール遵守に関する研修を行い、再発防止の徹底を行います。

同じ企業のホームページにおける最終報(確報)の内容です。

これより前段で外部のセキュリティ事業者による調査が完了した旨も記載されていました。

社外秘

3　求められる個人情報保護

1. 概要

2024年5月26日、悪意のある攻撃者による不正アクセスを受け、当社の情報処理センター及び全国営業拠点の端末やサーバがランサムウェアによって暗号化された事を確認いたしました。2024年6月18日には攻撃者グループのリークサイトで、攻撃者が窃取したとされる情報を公開するためのダウンロード用URLが掲載されました。
ダウンロード用URLから公開された情報は調査の結果、当社のサーバから流出したものであり、一部のお取引先様の顧客に関する個人情報が含まれている事が判明しました。ダウンロードファイルは2024年10月4日現在消失しており、ダウンロードができないことを確認しております。

　リークサイトとはダークウェブに属するWebサイトの一つで、サイバー犯罪者が窃取した情報を掲載する場所です。

　特別な方法でアクセスするWebサイトなので広く一般の目に触れることこそないものの、ここに掲載された情報をさらに別のサイバー犯罪者が悪用することで被害の拡大・長期化につながる可能性があります。

社外秘

3　求められる個人情報保護

2. 原因

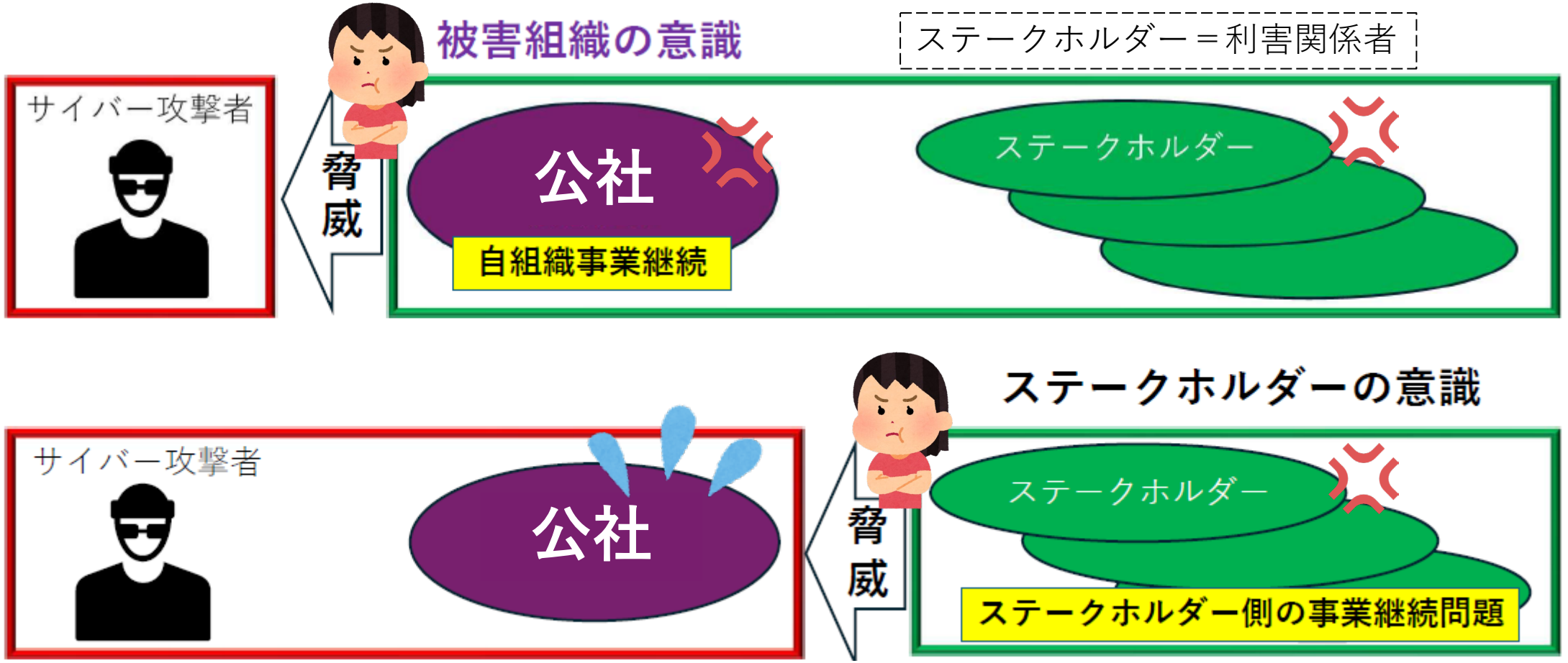
VPNからの不正アクセスにより当社ネットワークに侵入した攻撃者によって、当社が一部のお取引先様の受託業務の作業工程で発生した帳票データや検証物の一部の情報が窃取されました。当該情報を取り扱ってはならないサーバに作業の効率を図るため便宜的に保管し、また業務終了後には速やかに削除すべきデータを削除することができておりませんでした。当社の情報の取り扱いが原因で、攻撃者によるデータの窃取を許すこととなり、多大なご迷惑をおかけすることになりましたこと、重ねてお詫び申し上げます。
なお、現時点で、本件に起因する個人情報を用いた不正利用等の二次被害については、確認されておりません。引き続きお取引先様名、または当社名を騙る不審な電話や郵便物等による勧誘や詐欺には十分にご注意いただき、不審に思われた場合は最寄りの警察にご相談いただくようにお願い申し上げます。

　不正アクセスによるデータ窃取の原因としてとても残念なのが「業務終了後にデータを削除する」というルールが守られていなかったという点です。

　一部報道によると業務効率を優先してデータ削除を怠る状態が慢性化していたとのことですが、どうやらサイバー犯罪者の作業効率も上げてしまったようですね。

社外秘

3　求められる個人情報保護



（出典：株式会社ディアイティ　Security Days Fall 2024 Tokyo講演資料
「脅威となるサイバー攻撃・ランサムウェアに備える脆弱性対策とは～事業継続に必要な『事前対策と事後対応』～」）

被害組織であっても“被害者ヅラ”が許されるとは限りません。

「**調査・報告・復旧**」と「**事業継続**」のどちらも待ってはくれないことでしょう。

最後に

今回は2024年のサイバー攻撃に関する世相を振り返りながら、その根本にある個人情報保護について触れさせていただきました。

公社も多くの個人情報を保有する事業者の一つなので、職員全員でその自覚を強く持たねばならないと考えています。

また、引き続き「何かおかしいと感じたら迷わずLANケーブルを抜く」にご協力をお願いいたします。

本動画は以上となります。

ご視聴ありがとうございました

最後にWebページから視聴アンケートを送信してください。

社外秘