国立大学法人　佐賀大学　御中

2023年度　情報セキュリティ講習会

～標的型攻撃メール対応訓練フォローアップ～

２０２４年2月

QTnet

第１章　情報セキュリティ対策の必要性と事故事例

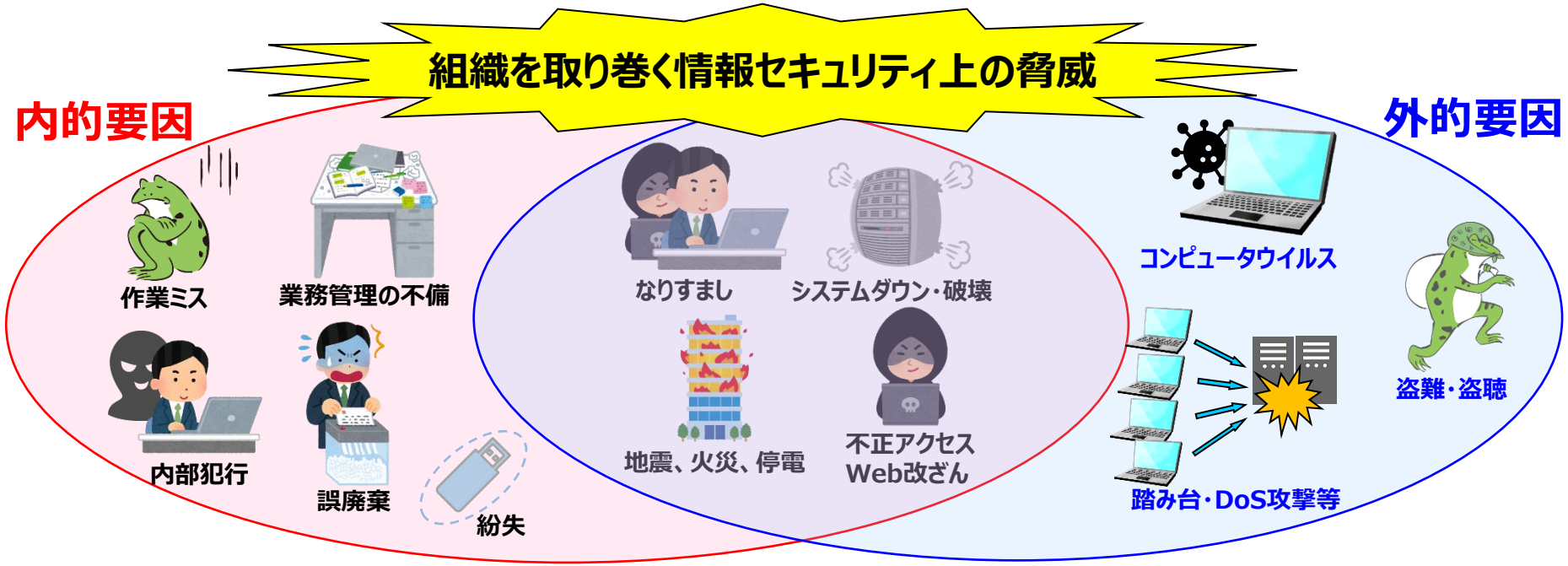
第２章　サイバー攻撃の傾向と攻撃手法

第１章

情報セキュリティ対策の必要性と事故事例

１．１　情報セキュリティ対策の必要性

«情報セキュリティ対策の必要性»
日常の業務を行う中で生じる日々刻々と変化する情報セキュリティ上の脅威から、
継続的に情報資産を守り続けていくために必要



もし、情報セキュリティ事故が発生したら

- 情報漏えい
- 不正な業務処理
- 資産損失
- システム(業務)の停止　etc

その結果・・・

- 物的損害
- 金銭的損害（賠償責任）
- 信用喪失・風評被害
- 刑事責任、etc

1．2　近年の情報セキュリティ事故の傾向

➤情報セキュリティ 10大脅威 2024年（組織）

「情報セキュリティ10大脅威 2024」は、2023年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。
「組織」向け脅威の種類も、全て前年と同じでした。

順位	「組織」向け脅威	初選出年	10大脅威での取扱い（2016年以降）	前年順位
1	ランサムウェアによる被害	2016年	9年連続9回目	1
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目	2
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目	4
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目	3
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目	6
6	不注意による情報漏えい等の被害	2016年	6年連続7回目	9
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目	8
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目	7
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目	5
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目	10

経済産業省が所管する独立行政法人「情報処理推進機構（IPA）」が毎年公表する資料であり、具体的な対策案が記されているため、国内の組織にて広く参考とされている。

「組織に対する脅威」に
「電子メール」を通じた
標的型攻撃による脅威が
多数ランクイン

近年、
「電子メール」を通じた脅威、
「電子メール」を悪用した脅威
が継続している

本資料の引用元：独立行政法人情報処理推進機構（2024年1月24日）
https://www.ipa.go.jp/pressrelease/2023/press20240124.html

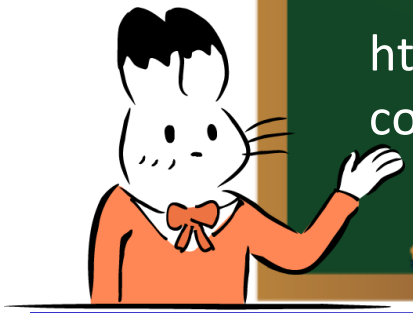
１．２　近年の情報セキュリティ事故の傾向

佐賀大学にとっての３大脅威

- 情報セキュリティ関連規程・ガイドラインの理解不足
- メール等によるウイルス感染
- USB メモリ紛失などによる情報漏えい

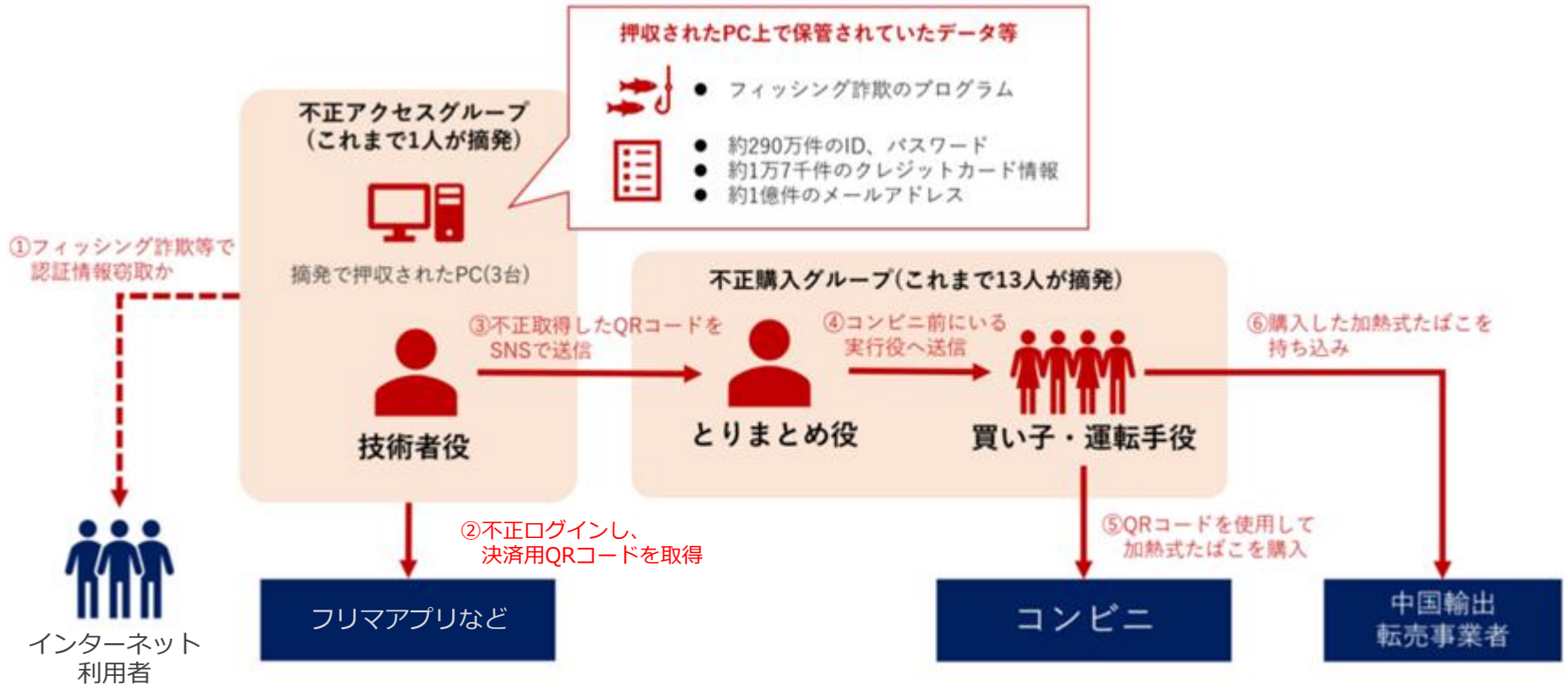
【佐賀大学情報セキュリティガイドブック】
＞センター利用案内
　＞情報セキュリティ
　　＞佐賀大学情報セキュリティ対策ガイドブック

https://www.cc.saga-u.ac.jp/cms/wp-content/uploads/2023/01/info-security-guidebook.pdf



1．3　最新の事故事例（情報漏えい事故）

約１億件のメールアドレスが漏えい



逮捕された犯人のPCに約1億件のメールアドレスが保存されていたことが判明
1億件のメールアドレス中には、大学のドメイン「ac.jp」のメールアドレスも含まれていた
窃取された情報は、売買される可能性があり新たな攻撃を受ける可能性がある

【引用】 https://www.asahi.com/articles/ASR5231DGR4YULOB00C.html?iref=pc_photo_gallery_bottom
https://piyolog.hatenadiary.jp/entry/2023/05/02/004654

1．３　最新の事故事例（情報漏えい事故）

東京大学のケース

2023年10月24日
東京大学

東京大学大学院総合文化研究科・教養学部（以下、「当該部局」という）が保有するPCが、標的型攻撃メールによりマルウェアに感染し、調査の結果、PC内の情報窃取の形跡が発見され、情報漏洩した可能性があることが判明いたしました。

上記判明後、漏洩した可能性のある情報の調査を慎重に進めてまいりました。調査結果の概要は以下のとおりです。 ご関係の皆さまには多大なご迷惑とご心配をお掛けすることになり、深くお詫び申し上げます。

本学では、今回の事態を重く受け止め、より一層、情報管理体制の強化や情報セキュリティ対策の適切な管理に努めて参ります。

1．本件発生の経緯

2023年1月18日、標的型攻撃メールの事案を調査していた専門機関からの指摘を受け、当該部局が保有するPC（当該部局所属の教員1名（以下、「利用者」という）が在宅勤務で使用していたもの）が2022年7月19日に受信した標的型攻撃メールによりマルウェアに感染していたことが発覚いたしました。

感染発覚後、当該PCを隔離保全し、同機関ならびに別の専門機関により、PC内の情報漏洩等に関する調査を行いました。調査の結果、2023年5月23日にPC内の情報窃取の形跡が発見され、以下の情報が漏洩した可能性があることが判明いたしました。

2．漏洩した可能性のある情報

(1) 本学教職員、学生、卒業生等の情報（氏名、所属、身分、学年、教職員番号、学生証番号、生年月日、性別、住所、電話番号、メールアドレス、学歴、職歴等のうち1つ以上の情報が含まれるもの）：2,409件
(2) 利用者が在籍する学会会員、学会主催イベント等参加者の情報（氏名、所属、身分、生年月日、性別、住所、電話番号、メールアドレス、学歴・職歴等のうち1つ以上の情報が含まれるもの）：1,082件
(3) 利用者が他大学で非常勤講師等として担当する授業の受講学生の情報（氏名、所属・学年、学生証番号、生年月日、性別、住所、電話番号、メールアドレス等のうち1つ以上の情報が含まれるもの）：796件
(4) 過去の当該部局の学生成績・評価、過去の試験問題：24件
(5) 当該部局所属教員の評価等：30件

標的型攻撃メールによりマルウェアに感染した事案が発生
偽の講演の日程調整をやり取りする中でマルウェアに感染した

https://www.u-tokyo.ac.jp/focus/ja/press/z0109_00952.html
https://piyolog.hatenadiary.jp/entry/2023/10/25/164100

ランサムウェアの被害

ランサムウェア：身代金を要求する不正プログラム

感染し被害が発生

データの暗号化

攻撃者への情報漏えい

脅迫

暗号化解除と引き換えに金銭要求

機密情報の外部公開と引き換えに金銭要求

被害の影響

▼**金銭の損失**：復旧作業経費や取引先･顧客からの損害賠償

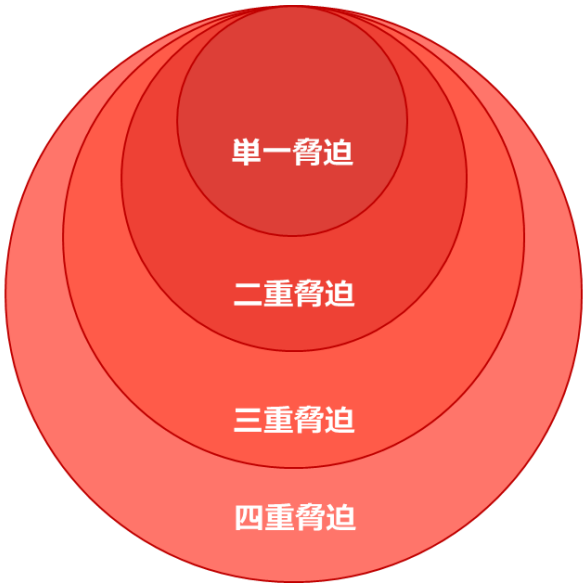
▼**信用の喪失**：情報流出による信用喪失･風評被害

▼**業務の停止**：復旧作業による納期遅れや営業機会損失

ランサムウェア被害を受けると

攻撃者から見れば、ランサムウェア攻撃はビジネス形態の一つ。
攻撃者は、手を変え品を変え、新たな被害者から金銭を巻き上げるために努力を続けています。

【多様化するランサムウェア】



単一脅迫：暗号化

ロック解除してほしければ
お金を払え

二重脅迫：窃取情報の暴露

データ公開されたくなければ
お金を払え

三重脅迫：DDoS攻撃

DDoS攻撃やめてほしければ
お金を払え

四重脅迫：他社情報の漏えい

顧客や利害関係者等の
情報を流出させたくなければ
お金を払え

［参考］https://www.eset.com/jp/topics-business/new-double-extortion-ransomware/
https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/ransomware.htm
https://enterprisezine.jp/article/detail/18549?p=2

１．４　ランサムウェア被害増加

MAKE NEW STANDARDS.
東海国立大学機構

東海国立大学機構への不正アクセスによる個人情報流出について

2022年11月18日

このたび、東海国立大学機構で運用している情報システムのアカウントを管理するサーバーが、第三者による不正アクセスを受け身代金要求型マルウェア（ランサムウェア）に感染し、データの一部が改変されるという事案が確認されました。その際に、機構が保有する個人情報が漏えいした可能性がありますので、現在の状況と今後の対応についてお知らせします。

令和4年10月18日（火）、当該サーバーのログを確認したところ、不正アクセスによるパスワード総当たり攻撃を受けていたことが判明しました。アクセスログ解析の結果、当該サーバーに保存されていた、機構アカウントや氏名等を含めた個人情報が約40,000件漏えいした可能性があります。

大学組織において、第三者による不正アクセスによりランサムウェアに感染
個人情報漏えいした可能性がある事案が発生

【引用】東海国立大学機構HP　https://www.nagoya-u.ac.jp/info/20211029_jimu.html

重大な情報漏えい事故が発生した組織における、
年間の平均被害額は・・・

約3億2850万円

※セキュリティインシデントによってもたらされる情報漏えいや
システム・サービスの停止、訴訟といった二次被害・三次被害、
再発防止のための改修コストまでを含めた**年間平均被害額**

信頼の損失はプライスレス

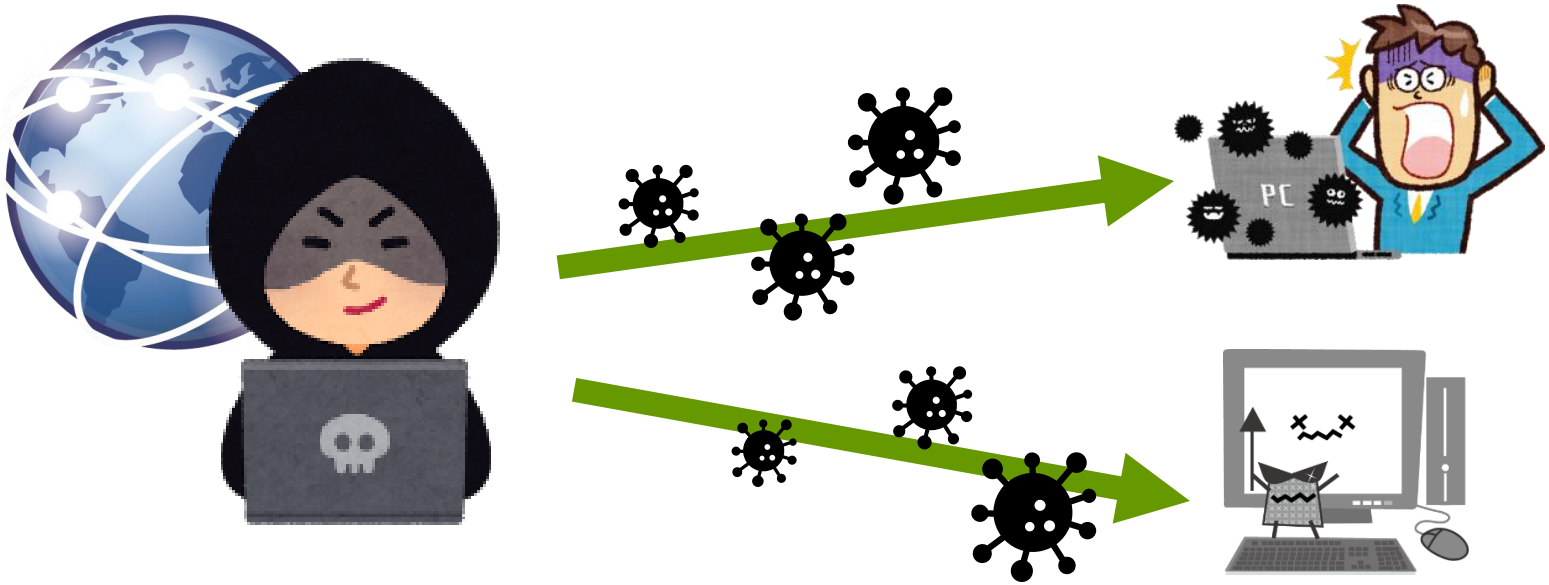
[引用] https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20221207-01.html

第２章

サイバー攻撃の傾向と攻撃手法

【サイバー攻撃】

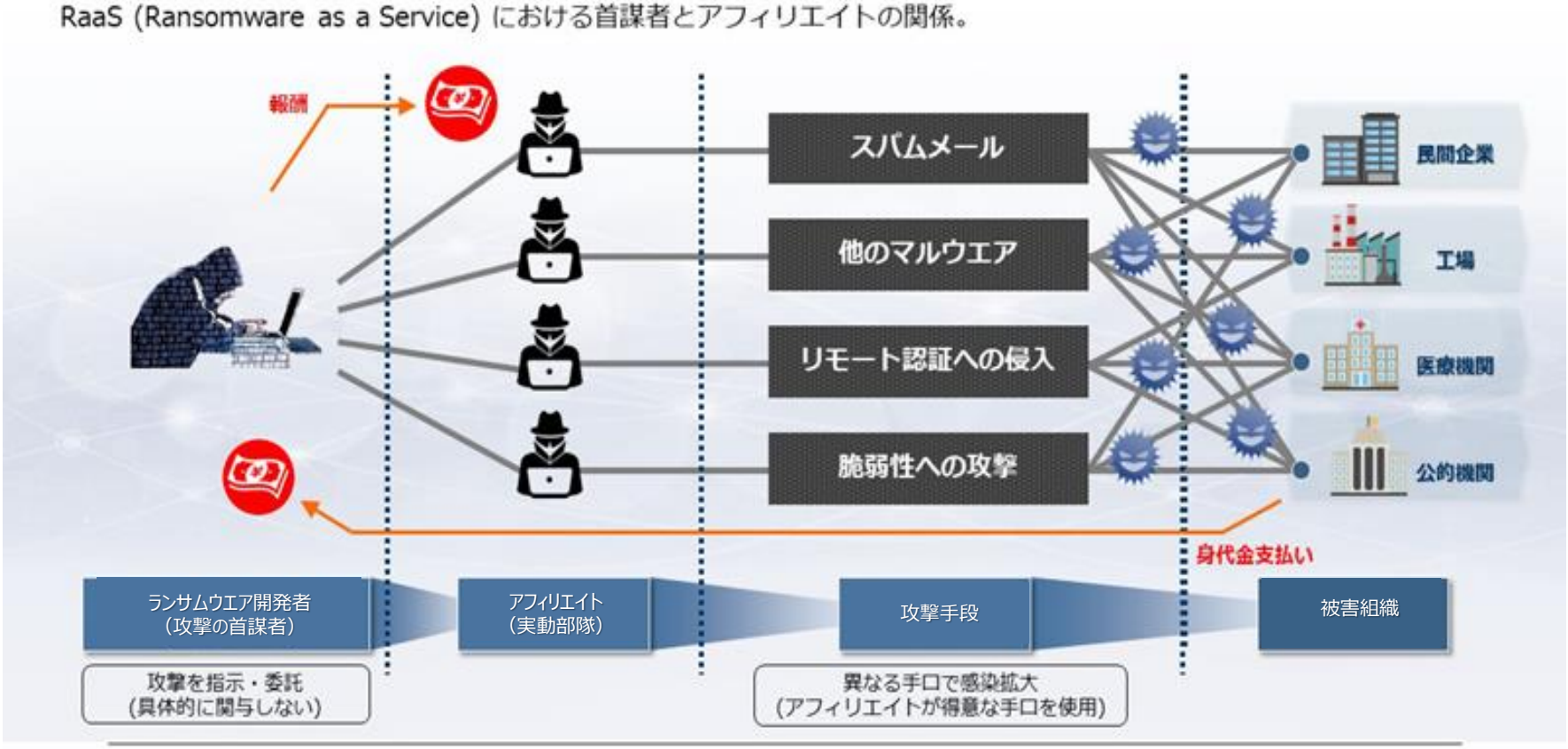
コンピュータやインターネットなどを利用して、
攻撃対象のコンピュータやネットワークに不正に侵入し、
データの窃取や破壊、改ざんなどを行なったり、システムを機能不全に陥らせること



２．１　サイバー攻撃の傾向

サイバー攻撃は犯罪ビジネスとして確立しており、専門分野ごとに分業化。

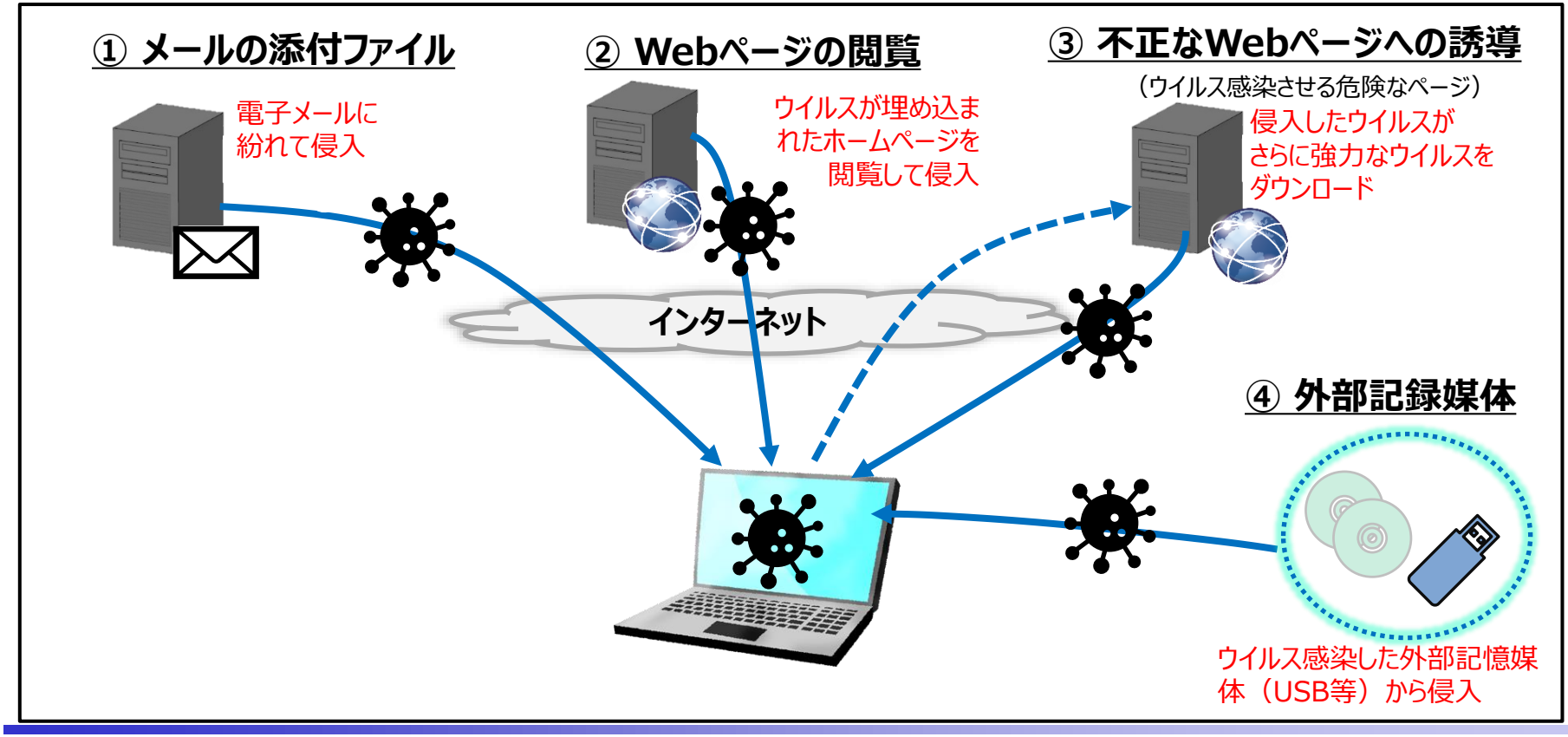
RaaS (Ransomware as a Service) における首謀者とアフィリエイトの関係。



[出典]https://ascii.jp/elem/000/004/095/4095916/

２．２　サイバー攻撃に用いられるコンピュータウイルスの感染経路

① 電子メールの添付ファイル開封による感染
② ウイルスが埋め込まれたWebページの閲覧による感染
　（著名企業のホームページで感染する場合もあり）
③ メールやWebページのURLリンクから不正なWebページへ誘導され感染
④ 外部記憶媒体（USBメモリ等）から感染



標的型攻撃メールとは

攻撃者が**業務のメールになりすまして**ターゲットにメールを送り、メールに添付されているファイルやURLを開封させることにより、標的とする組織のPCに**ウイルスを感染させようとする攻撃**です。

教職員に関連する業務依頼(入試業務・就職支援業務など)を装うなど、受信者が興味を持つ**巧妙な文面**でメールを送り、添付ファイルやURLを開封させようとします。
他にも公的機関であれば信用する人も多いため、公的機関になりすましたメールを送信しウイルスに感染させるなど、**あらゆる騙しのテクニックを用いて攻撃**してきます。

標的型と言われる理由

- 標的の傾向(業務内容、興味)を数か月かけ調査することもある
- 特性のウイルスを用いて対策ソフトをすり抜ける
- 感染後は長期的に侵害範囲を広げ、目的の情報窃取まで気づかせない

２．４　標的型攻撃メールに対する確認ポイント

身に覚えのあるやりとりの件名か、不用意に煽るような件名でないか確認

差　出　人　：システム本部　システム担当 <◇◇◇@gmail.com>
件　　名　：インターネットエクスプローラーアップデートの実施
添 付ファイル：アップデート.pdf　　.exe

差出人を確認

ファイル名を確認
拡張子など偽装している可能性も

お疲れ様です。システム本部です。

昨日公開されたインターネットエクスプローラーの脆弱性に対応するため
以下の手順に従い、本日中にアップデートをお願いします。

１．以下URLへ接続
http://xxxx.xxxxx.com/IE-update/

URLリンク先を確認

2．更新画面が表示されたら「インストール」をクリック

文章が不自然な日本語でないかを確認

業務でお忙しいかと思いますが、迅速な対応をお願いいたします。

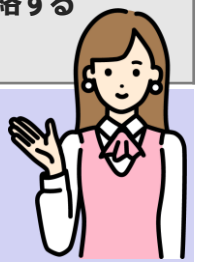
存在する部署であるかを確認

システム本部　システム担当
TEL：△△ー△△△△

少しでも、何かあやしいと感じたら・・・

メールの差出人を知っている場合は、本人に電話等で確認する（メールで返信しない）	周囲の人に同じようなメールが届いていないか確認する	開封してしまった場合は、パソコンからLANケーブルを外し、無線LANをOFFにする	管理者に連絡する

佐賀大学 CSIRTへ速やかにご連絡ください
電話　0952－28－8149（内線8149）
電子メール　CSIRT@mail.admin.saga-u.ac.jp



佐賀大学情報セキュリティ対策ガイドブック

０５　メールのリンクや添付ファイルに注意しましょう

現実　メールを発端とする標的型攻撃が脅威となっています

標的型攻撃は特定の個人や組織を狙った攻撃で、おおむね以下の過程で攻撃が行われます。

❶ メールの添付ファイルやリンクをクリックしてウイルスに感染
❷ ウイルスが他のウイルスをダウンロードして進化
❸ 進化したウイルスが組織内の他のパソコンから情報を集めて外部に送信

様々な官公庁、民間企業が被害にあっていますが、❶のメールの文章が巧妙なため、攻撃に気付き難いというのが現状です。

対策　怪しいメールは疑い、総合情報基盤センターに確認を取りましょう

メールは簡単にニセモノを作ることができますので、知った相手からのメールと思っても、簡単に信用しないようにしましょう。特に知らない差出人から届いたメールにおいて、以下の場合は要注意です。

- 件名に緊急、重要、限定などと書かれている。
- 本文にリンクや添付ファイルが含まれている。

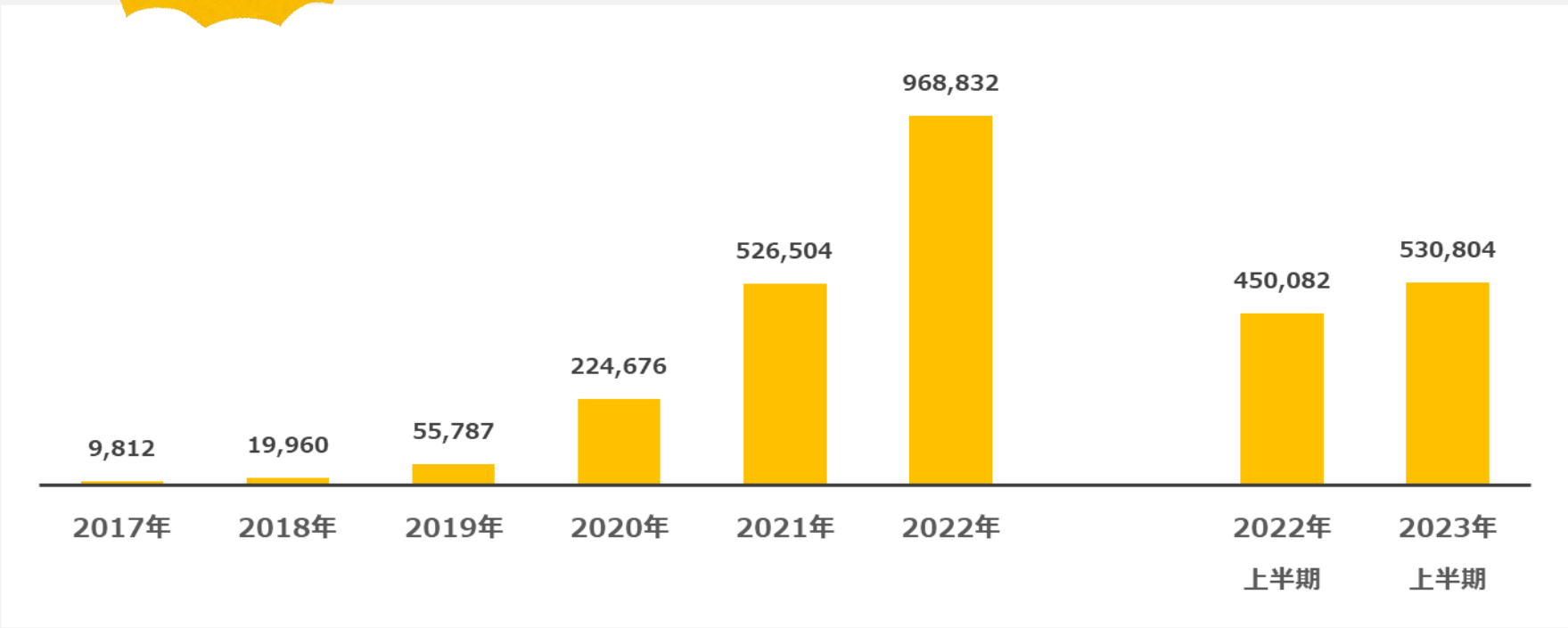
佐賀大学では、毎年、標的型攻撃メール訓練を実施しています。

人を騙して情報を窃取する
「フィッシングメール」を利用した
標的型攻撃の巧妙な手口について

２．５　フィッシング詐欺の報告件数

フィッシング詐欺の報告件数は年々増加しており、深刻な状況となっている。

全国で被害相談急増中!!

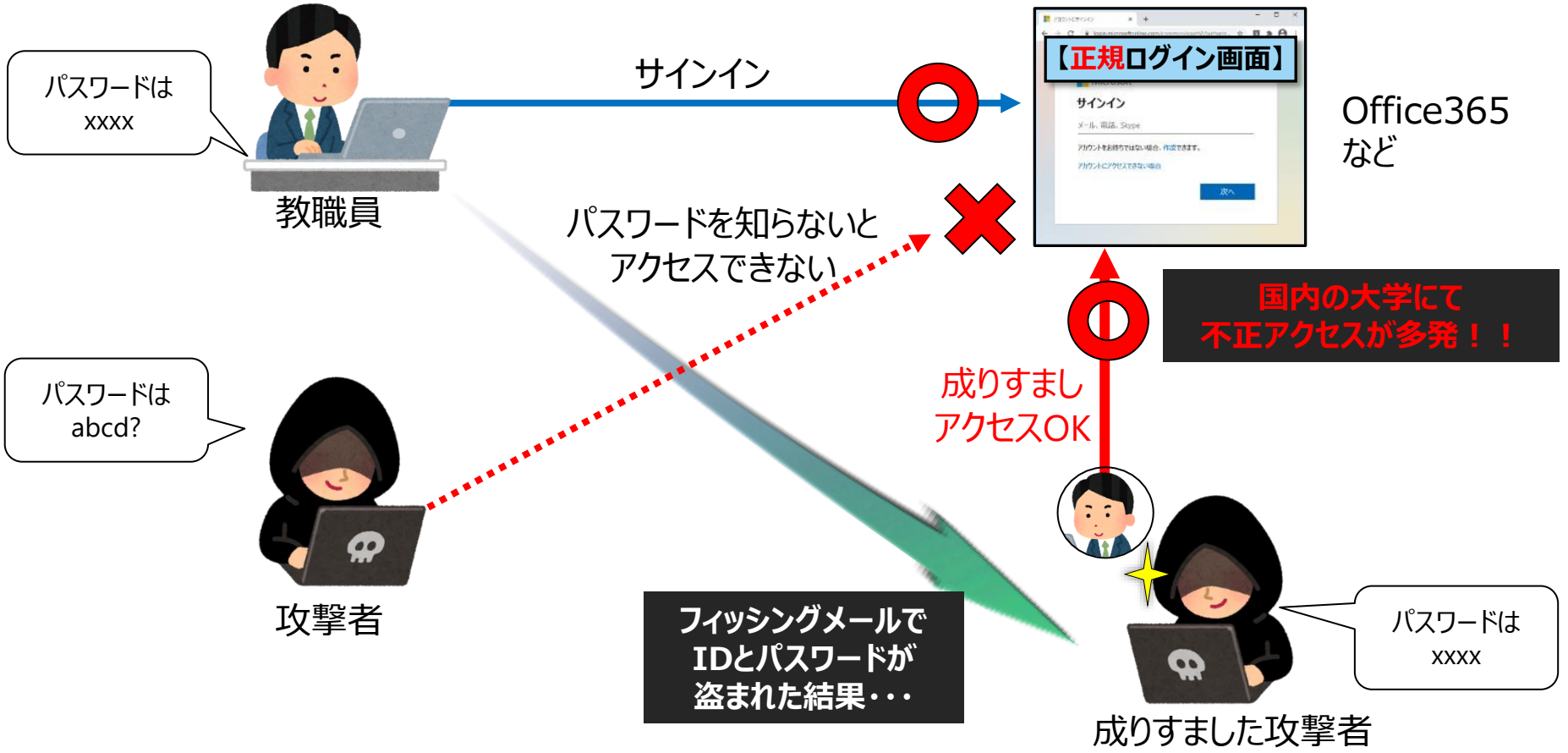


フィッシング報告件数

出典：警察庁　令和５年上半期におけるサイバー空間をめぐる脅威の情勢等についてより
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

２．６　標的型攻撃の巧妙な手口（「フィッシングメール」を用いた攻撃）

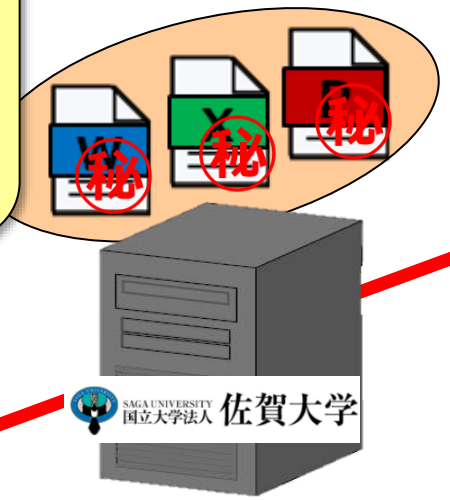
教職員に対する「フィッシングメール」により IDとパスワードが窃取された場合



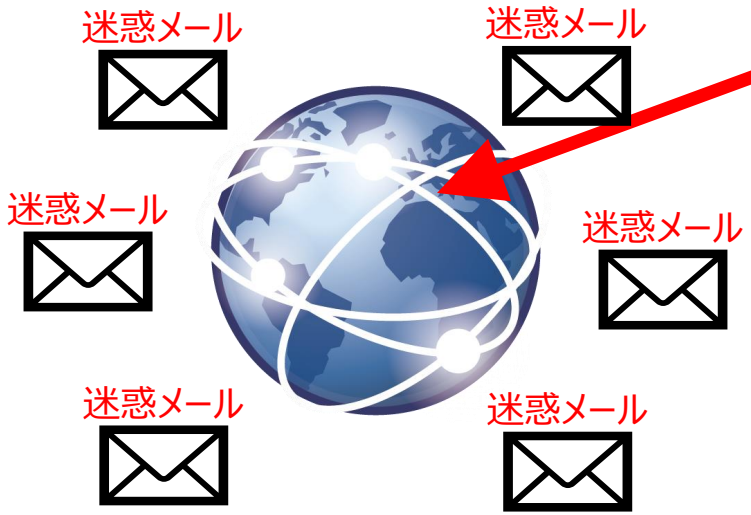
２．６　標的型攻撃の巧妙な手口（「フィッシングメール」を用いた攻撃）

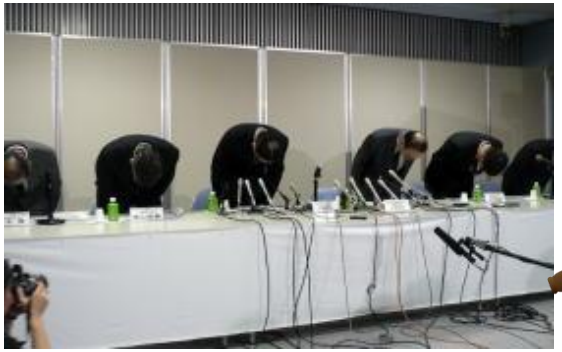
攻撃者が学内システムから機密情報の窃取や外部への迷惑メール送信等を行い、組織の情報や迷惑メールが拡散し、組織や個人が多大な損害を受ける

金銭的な損害以外にも、
大学のブランド力低下に伴う、
研究予算の獲得や学生・教職員
募集への影響が懸念される



攻撃者





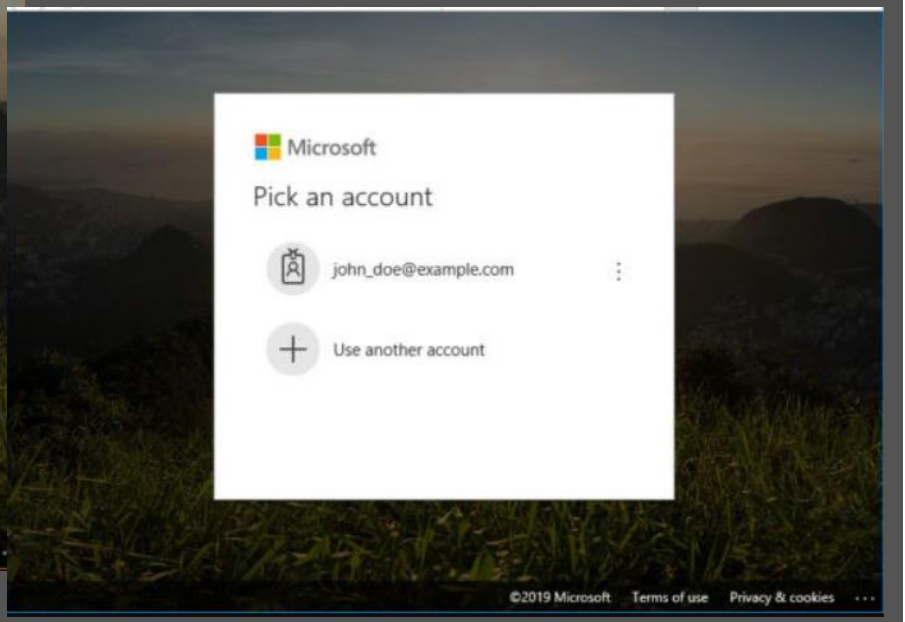
謝罪・関係者の処分

訴訟・補償

（参考）実際のフィッシングサイト

正規のサイト

フィッシングサイト



フィッシングメールと疑われるメールについて、メール本文内容を
正規のホームページ等で再確認することが重要となります。

２．７　標的型攻撃の脅威への備え

標的型攻撃は、新種のウイルスや未知の脆弱性を利用しつつ、
人間心理を悪用する等、巧妙化の一途をたどっており、
技術的対策で完全に防ぐことは不可能

↓

技術的対策だけではなく、組織の教職員全員が
標的型攻撃の脅威に備える必要がある

↓

標的型攻撃を疑似体験する「メール訓練」が有効

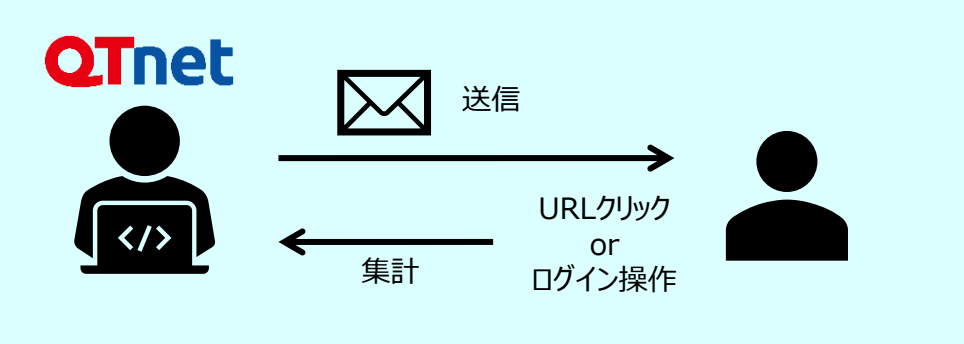
↓

攻撃を体感することで、誰もが狙われる可能性がある
ことを認知し、連絡・相談方法を把握することが重要

２．８　標的型攻撃メール訓練

（１）実施内容

標的型攻撃メールを模擬した訓練メールを送信し、その開封結果を集計（フィッシング模擬）



（２）対象アドレス

1回目：　2,795 アドレス

2回目：　2,810 アドレス

（３）訓練期間

1回目：2023年7月24日(月)　10：00　～　2023年7月28日(金)　17：00

2回目：2023年11月13日(月)　10：00　～　2023年11月17日(金)　17：00

（４）開封結果集計の仕組み

訓練メール本文内「URLリンク押下」によるWebアクセス件数（開封者数）および
フィッシング画面内「ログインボタン押下」によるWebアクセス件数（ログイン者数）を集計

2．8　標的型攻撃メール訓練（2023年度 1回目）

（1）訓練メール文、偽ログイン画面（2023年7月実施）

差出人	lovecamp@miadomin.saga-u.ac.jp　ドメイン名の一部を貴学ドメイン名に詐称
件名	【緊急】[佐賀大学統合認証システム]パスワード有効期限切れ予告通知
本文	緊急性を強調 このメールは、佐賀大学統合認証システムより自動送信されています。 ユーザID：　（宛先のメールアドレス） ７月２８日（金）17時に、あなたのパスワードの有効期限が切れます。 パスワードの有効期限が切れると佐賀大学の全ての情報システムにログインできなくなります。　対応しない場合のペナルティ 有効期限（expiration date）：2023-7-28 17:00　短い期限 パスワードの有効期限が切れる前に、下記のホームページからパスワードの有効期限を更新してください。 https://support-system.jp/operation/password-change.html?***** 学外のドメイン名 偽ログイン画面へ誘導 署名がない

2．8　標的型攻撃メール訓練（2023年度 2回目）

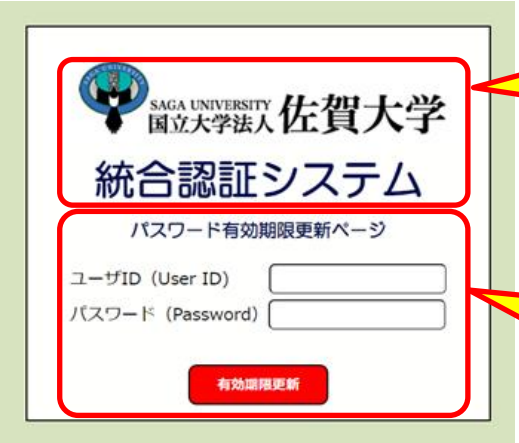
（1）訓練メール文、偽ログイン画面（2023年11月実施）

差出人	osirase@mladmin.saga-u.ac.jp　ドメイン名の一部を貴学ドメイン名に詐称
件名	[sadaiall:99999]【重要】佐賀大学からのお知らせ(2023/11/13) 学内周知に詐称　重要性を強調
本文	佐賀大学教職員各位 佐賀大学からの重要なお知らせです。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 対象：全学 １.【通知】 タイトル：ノートパソコン５０台の無償譲渡について リンク先URL： https://support-system.jp/utilize/login.html?***** 貴学のドメインではない 偽ログイン画面へ誘導 所管課・係：情報機器有効活用対策室 存在しない組織名

2．８　標的型攻撃メール訓練

2023年度（1回目）

偽ログイン画面



正規のロゴと、同じもので実施

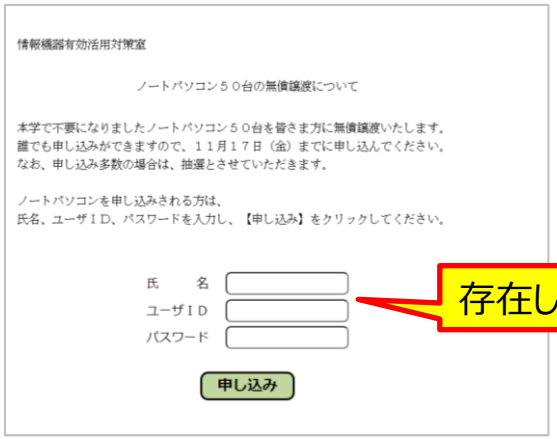
普段と異なる入力フォーム

正規のログイン画面

引用元
https://www.cc.saga-u.ac.jp/redirect

2023年度（2回目）

偽ログイン画面



存在しないWebサイト

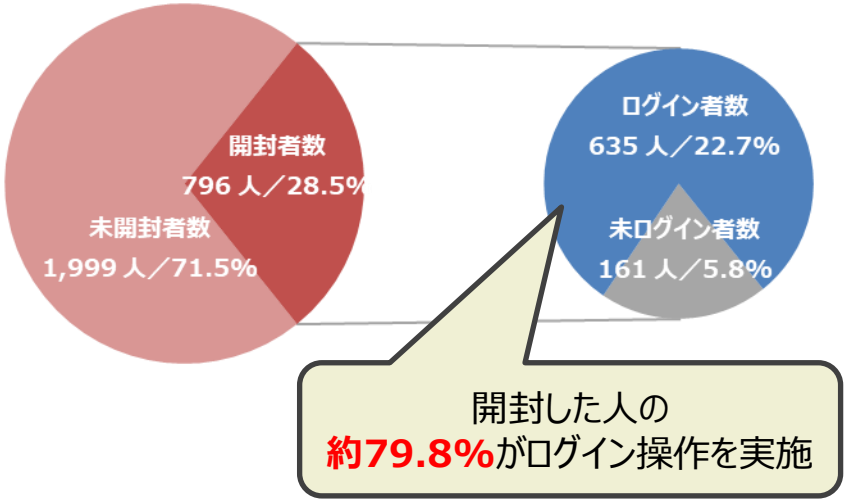
2．8　標的型攻撃メール訓練結果

開封率（全体総括）

【開封の定義】：訓練メール本文のURLリンクをクリック
【ログインの定義】：フィッシング画面(偽ログイン画面)にてログインボタンをクリック

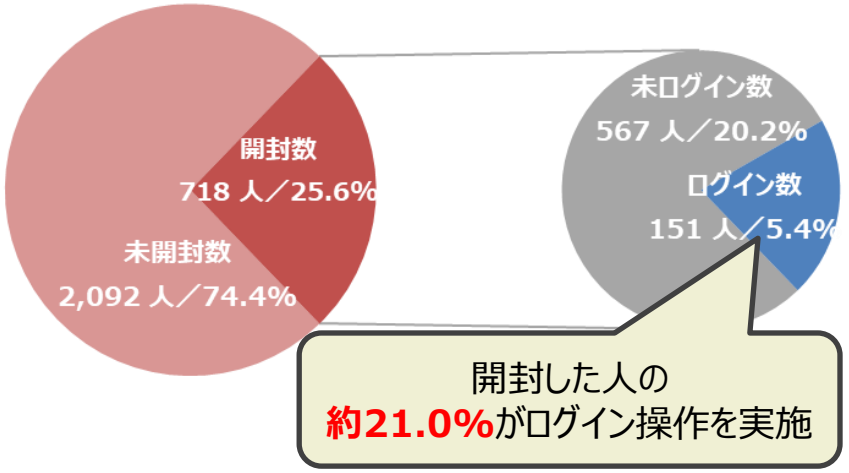
2023年度（1回目）

全2,795人のうち
開封者：796人（28.5%）
ログイン者：635人（22.7%）



2023年度（2回目）

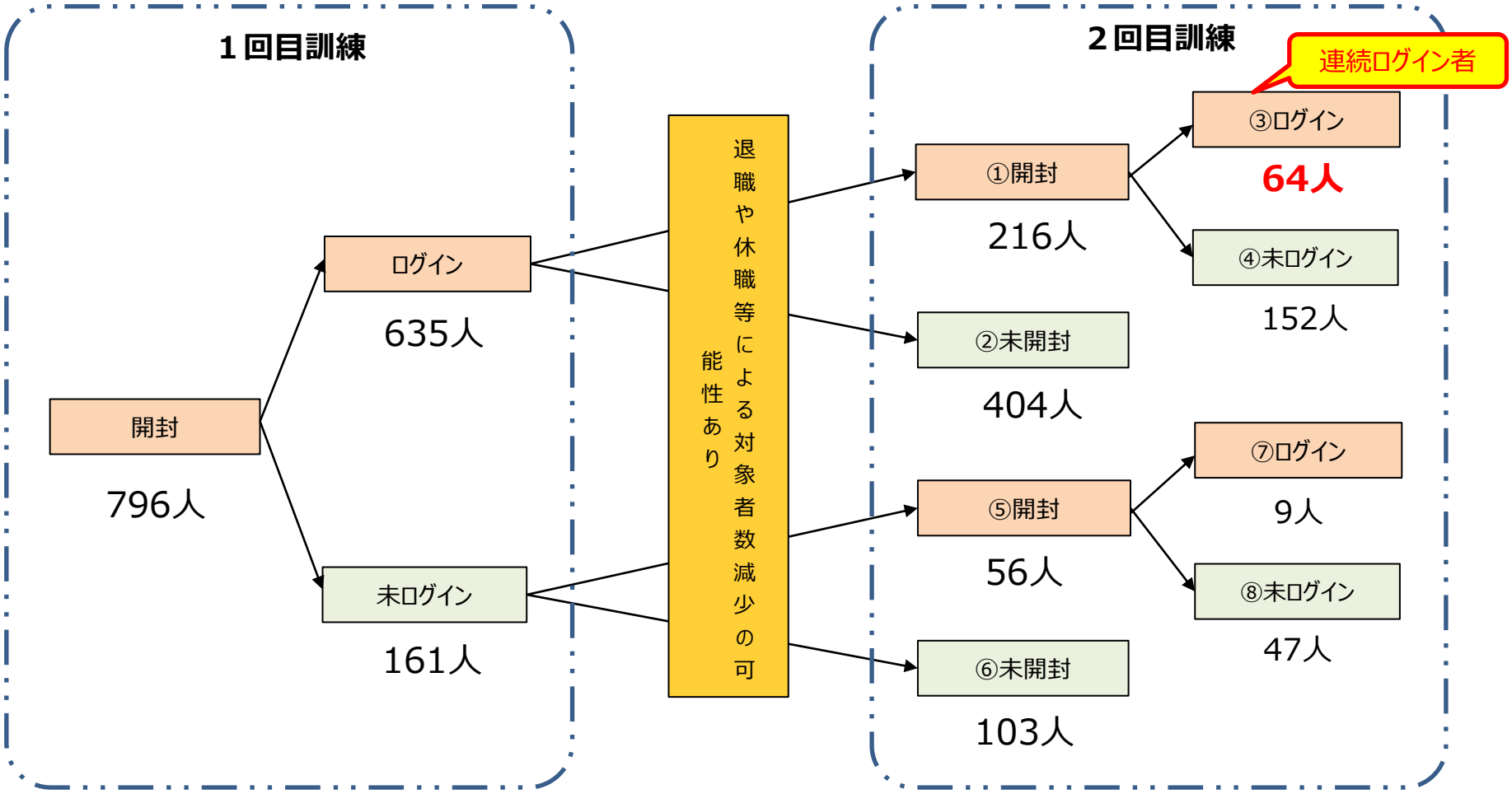
全2,810人のうち
開封者：718人（25.6%）
ログイン者：151人（5.4%）



・「ログイン操作」まで実施した割合は、「教育機関の平均（8.0%）※」に対し、
　1回目は「22.7%」と上回り、2回目は「5.4%」と下回った。
・1回目は開封者のうち約79.8%がログイン操作を実施した為、改善が必要。
　（他大学でも同様に4~5割程度）

※㈱ QTnetにて標的型メール訓練サービスを実施した、5つの大学の過去訓練実績の総計に対する平均

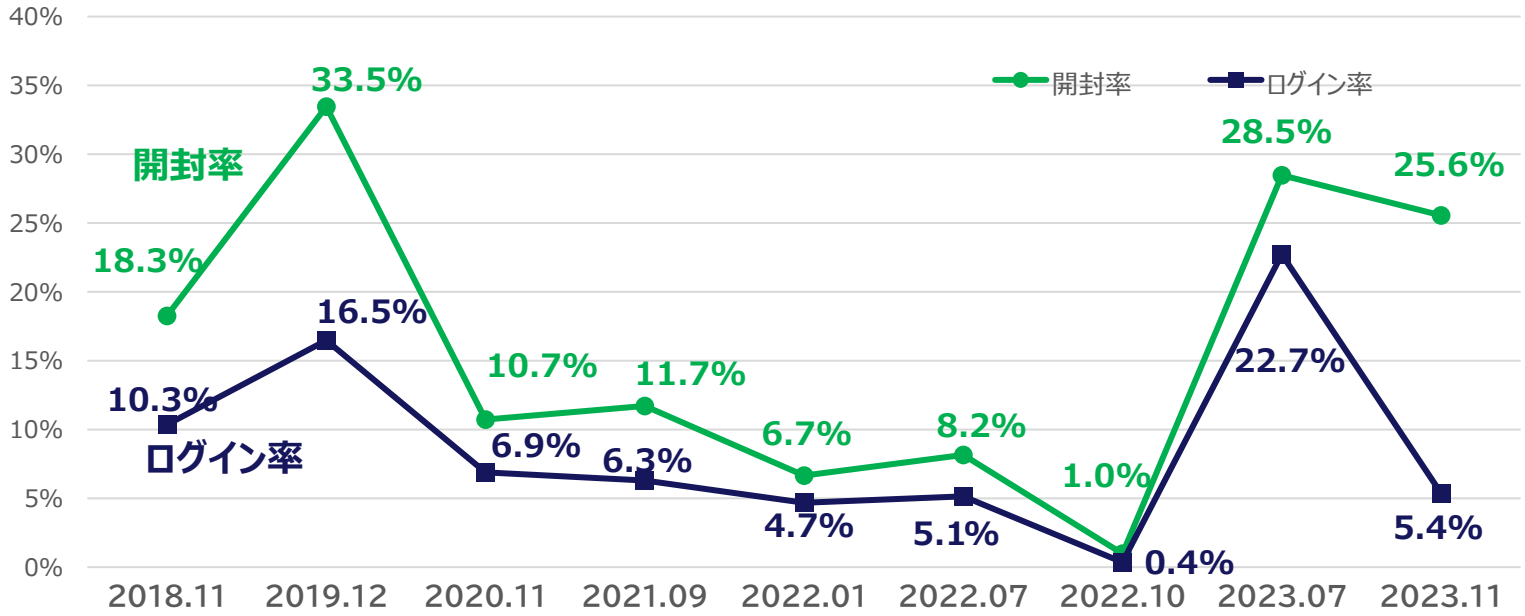
２．８　標的型攻撃メール訓練結果



本来、「1回目の訓練で開封もしくはログイン」した場合は、「2回目訓練では未開封」が望ましいですが、残念ながら、「1回目および2回目の連続ログイン者（図中③）」が64名見受けられました。

２．８　標的型攻撃メール訓練結果

「開封率・ログイン率」の推移



「開封率」、「ログイン率」

2023年の訓練結果（開封率、ログイン率）は、2022年度の訓練結果を上回った。
上回った要因として、以下があげられる。

・学内で周知されるメールフォームに酷似していた事
・システム関連以外の内容で実施した事

近年の標的型攻撃メールは見抜くポイントが難しく巧妙化しています。
引き続き、標的型攻撃メールに注意しましょう！

２．８　標的型攻撃メール訓練結果

【標的型メール訓練内容】
訓練を2回実施。URLクリック者には偽ログイン画面を表示し、フィッシング攻撃を模擬体験頂いた。

【開封率およびログイン率】
■1回目
昨年度の訓練よりも、1回目の開封率は27.5ポイント増加、ログイン率22.3ポイント増加
■2回目
今年度1回目の訓練よりも、開封率は2.9ポイント減、ログイン率は17.3ポイント減
➡訓練内容を比較し、次の傾向が得られた
メール文面・・・システム関連以外の内容で実施すると開封率が高い
偽ログイン画面・・・訓練者にとって見慣れている画面で実施するとログイン率が高い

【注意事項】
・1回目、2回目ともに開封・ログインした、連続開封者が存在する
➡実際にフィッシングメールが届いてしまった場合でもメールを開封し、機密情報を入力してしまうリスクが高い
・訓練メールの着信から、短期間で多数の教職員が開封する傾向が見受けられる
➡実際攻撃を受けた場合、メールの着信から「ID窃取またはウイルス感染」までの時間が短いと想定される

２．８　標的型攻撃メール訓練結果

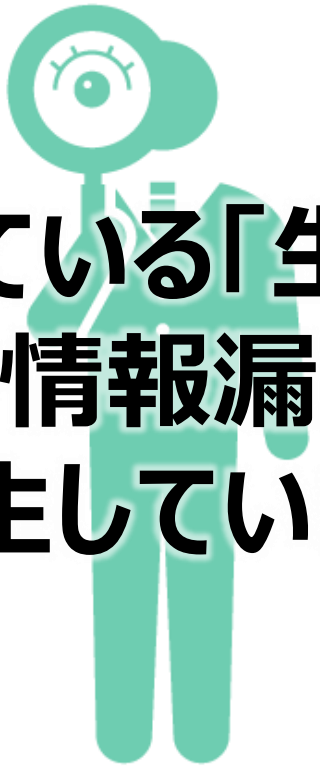
もし「学内のIDが窃取された」または
「PCがウイルス感染した」としても

被害範囲を最低限に留めることを目標に、学内における不審メール等を「速やかに」通報し、「速やかに」初動対応できる体制が望まれます。

不審メール着信やPCの不審動作を
通報する組織文化の醸成が重要

少しでも、何かあやしいと感じたら・・・

佐賀大学 CSIRTへ速やかにご連絡ください
電話　0952－28－8149（内線8149）
電子メール　CSIRT@mail.admin.saga-u.ac.jp



注目されている「生成AI」の利用に伴う情報漏えい事故が発生しています

生成AIについて、生成AI利用に伴う注意点をご紹介します。

生成AI

生成AI（Generative AI）とは、データから学習して新たな情報やアウトプットを生み出す種類のAIのことを指します。例えば、文章、画像、音楽やその他のメディアを生成することが可能です。AIが学んだデータパターンを基に、新たなコンテンツを作り出します。

ChatGPTのようなオープンな生成AIサービスだけでなく、
企業内でのクローズドな利用を目的としたカスタム生成AIの開発も進んでいます

オープンAI	公開されたデータを利用し、一般に開放されるAI。多くの人が利用可能ですが、プライバシーやセキュリティに注意が必要です。
クローズドAI	特定の企業や組織内だけで利用されるAI。自社ビジネスに特化した開発が可能ですが、一般には非公開です。

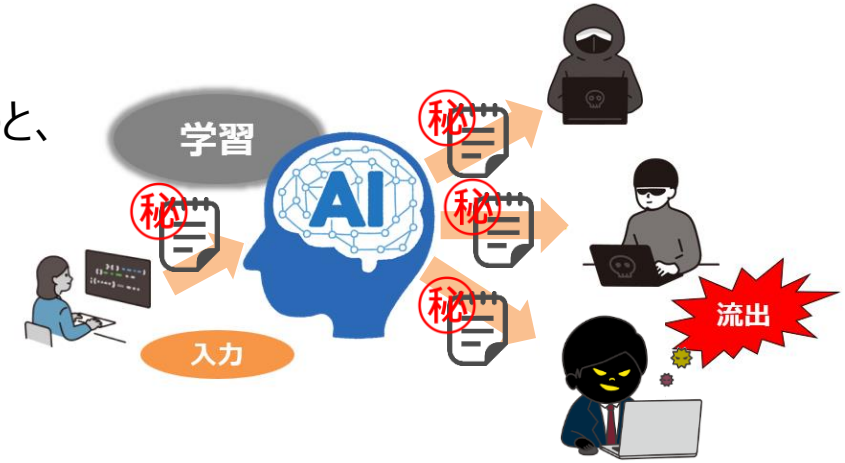
※生成AI・オープンAI・クローズドAIの説明は実際にAIに作成してもらった文章です

生成AIの利用リスク

ChatGPTをはじめ、多くの企業で生成AIが注目されてますが
利用の際には以下のリスクがあります。

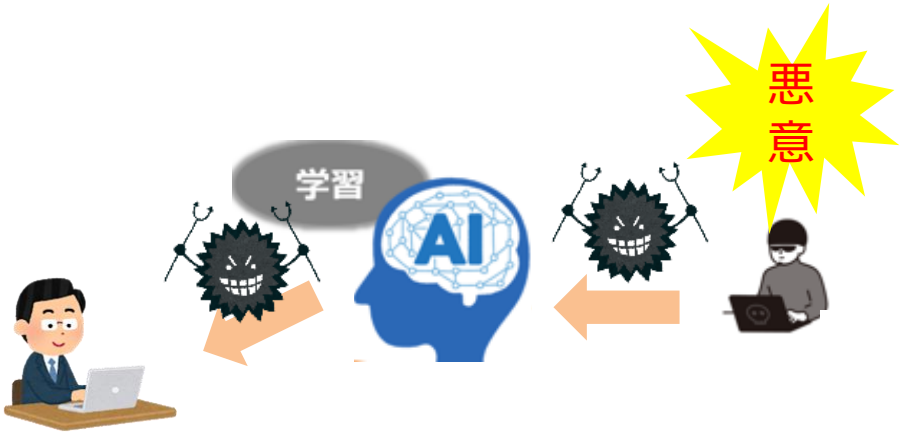
■ 生成AIに入力する情報

生成AIに個人情報や、機密情報を入力してしまうと、
「許可なく無断で利用される可能性」、
「外部に漏えいする可能性」
などリスクがあります。



■ 生成AIから出力される情報

生成AIが出力した情報の中には
「誤った情報」、
「デマやフィクション」、
「悪意のあるURL」
などが含まれている、というリスクがあります。



生成AI利用に伴う情報漏えい事例

2023年4月
韓国のサムスン電子は、「ChatGPT(チャットGPT)に機密情報をアップロードした事で情報漏えいが発生した。」と公表した

【経緯】

▼従業員がChatGPTに機密情報をアップロードしたことが発覚。
具体的には、以下の情報をアップロードした。

1）バグがある半導体データベースのソースコードをコピーして修正を依頼

2）機密コードをコピーして欠陥のある機器の修正プログラムを依頼

3）会議音声をチャットボットに投げて、議事録の作成を依頼

▼アップロードした事により、機密情報が漏えい。どのような情報を含んでいたかは不明。サムスンの担当者はコメントを控えた。

▼情報漏えい後、生成ＡＩツールの利用を原則禁止する新たなポリシーを策定した。社所有のコンピューターやタブレット、携帯電話、社内ネットワークでの生成AIの使用を禁止し、個人所有の端末でChatGPTなどを利用する従業員に対しては、サムスンの知的財産と分かる可能性のある会社関連の情報や、個人データを入力しないよう求めた.

この事件を受け、ＪＰモルガン・チェースやバンク・オブ・アメリカ、シティグループを含むウォール街の銀行数行がChatGPTを禁止もしくは制限した。

問題点

生成ＡＩプラットフォームに送信されたデータは外部サーバーに保存されるため、
回収・削除が難しく、他のユーザーに開示されてしまう恐れがある

[出典] https://onl.sc/9zWnM27

◆生成AIの入力情報、出力情報について

生成AIに企業秘密等や、個人情報など、外部に漏らしてはいけない情報を入力する事はやめましょう。
※判断に迷う場合は入力を控えましょう。

生成AIから出力された情報は、一度吟味するようにしてください。
誤った情報や悪意のあるURL等を含んでいる可能性があります。
出力した情報は必ず正しいとは限りません。
安易に信じるのではなく、参考情報として扱いましょう。

おわりに

皆さまの職場におけるセキュリティ対策は、
職場を守るだけではなく、
皆さまの私生活を守るうえでも役立ちます。

「インターネットは便利だけど怖い」
と感じていただくことが、
皆さまを守る第１歩になります。

パソコンへのウイルス感染が疑われる場合や
標的型攻撃と思われるメールを受け取った場合は
速やかに以下へ連絡してください。

佐賀大学　ＣＳＩＲＴ
電話　０９５２－２８－８１４９（内線８１４９）
電子メール　CSIRT@mail.admin.saga-u.ac.jp

情報セキュリティ講習会は終了です
おつかれさまでした

本講習会の資料および映像は
2025年3月末日まで
国立大学法人佐賀大学に属するすべての方がご利用になれます

きらきら、つながる。

QTnet