情報セキュリティ研修

情報資産を守る『情報セキュリティ対策』

教育・研究機関で扱う守るべき情報資産
- ■ 学生・生徒情報
- ■ 業務情報
- ■ 研究情報
- ■ 校友父母情報
- ■ 取引先情報　　等

情報セキュリティ

情報資産の**機密性**・**完全性**・**可用性**を維持すること

本研修における『情報セキュリティ』は情報資産のうち**デジタルデータ**が対象

機密性 (confidentiality)	許可された者だけが情報にアクセスできるようにすること	→ **情報漏洩 不正アクセス**
完全性 (integrity)	保有する情報が正確であり完全である状態を保持すること	→ **情報改ざん 情報滅失**
可用性 (availability)	許可された者が必要なときにいつでも情報にアクセスできるようにすること	→ **サービス停止 業務停止**

情報セキュリティ対策

情報セキュリティ事故の発生要因となる**情報セキュリティの脅威**から情報資産を守るための**人的**・**物理的**・**技術的**対策

情報セキュリティ事故：情報セキュリティを損なう(可能性のある)事象

人的セキュリティ	“人”の過失の発生を抑止する	・規程・ガイドラインを整備する ・教育・研修をおこなう　等
物理的セキュリティ	触れる“物”に対する対策	・PCを盗難防止用ワイヤーで固定する ・PC設置場所の入室管理をする　等
技術的セキュリティ	触れない“データ”に対する対策	・セキュリティ対策ソフトを導入する ・パスワードを設定する　等

情報セキュリティの脅威

本研修で扱う脅威

- 学内で事故事例があるもの
- 教育研究機関において
  特に注意が必要なもの

サイバー攻撃　★マルウェア　★フィッシング　★偽警告　★標的型攻撃

人的ミス　★ 不注意による情報漏洩

内部不正

IPA（独立行政法人情報処理推進機構）『情報セキュリティ10大脅威』

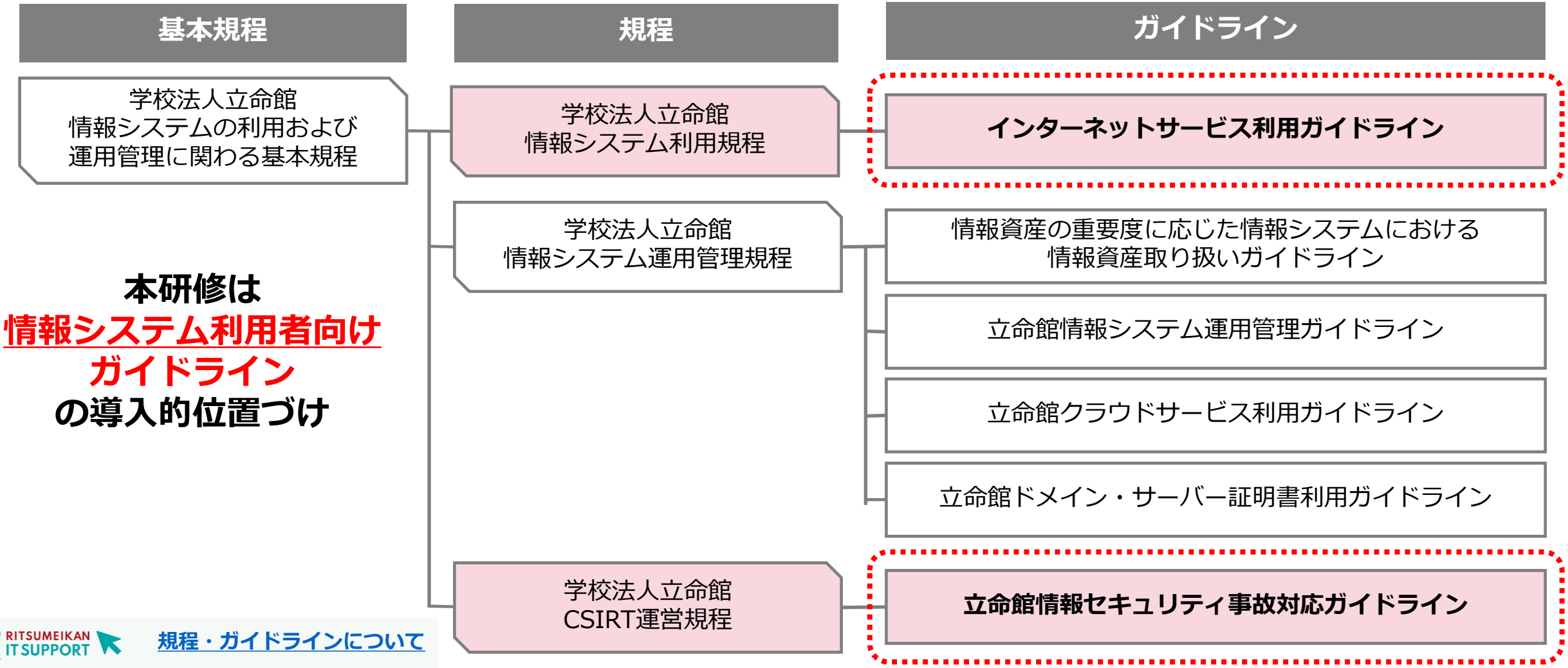
情報事故の報告を受け付け各種情報(注意喚起、脆弱性等、具体的対策等）を発信するIPAが脅威候補を選出

セキュリティの専門家や企業の実務担当者等が選考委員となり**各年の脅威を[個人][組織]に分けてランキング**

昨年順位	個人	順位	組織	昨年順位
1位	フィッシングによる個人情報等の詐取 ★	**1位**	ランサムウェアによる被害 ★★	1位
2位	ネット上の誹謗・中傷・デマ	**2位**	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	標的型攻撃による機密情報の窃取 ★★★	2位
4位	クレジットカード情報の不正利用	**4位**	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	**5位**	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによるスマートフォン利用者への被害	**6位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺 ★	**7位**	ビジネスメール詐欺による金銭被害 ★★	8位
8位	インターネット上のサービスからの個人情報の窃取	**8位**	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン ★	**9位**	不注意による情報漏えい等の被害 ★	10位
圏外	ワンクリック請求等の不当請求による金銭被害	**10位**	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

情報セキュリティ10大脅威 2023：IPA 独立行政法人 情報処理推進機構　https://www.ipa.go.jp/security/vuln/10threats2023.html

情報システム関連 規程・ガイドライン(体系図)



本研修は
情報システム利用者向けガイドライン
の導入的位置づけ

RITSUMEIKAN IT SUPPORT 規程・ガイドラインについて

情報システム利用者向けガイドライン

インターネットサービス利用ガイドライン

情報セキュリティ事故を
未然に防ぐために取り組むべき
具体的な情報セキュリティ対策について
事例を交えながら解説

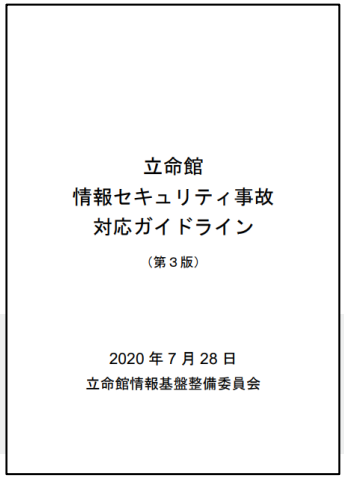
チェックリストで
自身の理解度を確認すること！

対策1 ★	マルウェア(ウイルス)	対策6 ★	アクセス権(共有)
対策2 ★	IDとパスワード	対策7	スマートフォンなどのモバイル端末
対策3 ★	Web	対策8	個人情報と権利侵害
対策4 ★	メール	対策9	サービス利用
対策5	通信と保存（暗号化）	対策10	その他

RITSUMEIKAN IT SUPPORT [インターネットサービス利用ガイドラインについて]

立命館情報セキュリティ事故対応ガイドライン

情報セキュリティ事故発生時に
求められる対応の流れと対応内容について
情報システム利用者向け
情報システム運用管理者向けの
それぞれについてまとめたガイドライン


立命館
情報セキュリティ事故
対応ガイドライン
（第３版）
2020 年 7 月 28 日
立命館情報基盤整備委員会

事故発生時の迅速な対応のために
何をすべきかを事前に確認してすること！

第2章	情報セキュリティ事故発生を想定した事前準備 1.情報セキュリティ事故発生時の対応体制の把握 2.情報セキュリティ事故発生時の連絡フローの把握
第3章 ★	情報セキュリティ事故発生時の迅速かつ適切な対応 １.情報システム利用者向け　対応の流れと対応内容 (2.情報システム運用管理者向け 対応の流れと対応内容)
第4章	情報セキュリティ事故発生後の振り返りと情報共有

RITSUMEIKAN IT SUPPORT [立命館情報セキュリティ事故対応ガイドライン]

本研修で扱う内容

【A】情報セキュリティの脅威と事故事例

【A-1】サイバー攻撃「マルウェア」
- 被害と発生要因
- 事例（Emotet）

【A-2】サイバー攻撃「フィッシング」
- 被害と発生要因
- 事例

【A-3】サイバー攻撃「偽警告」
- 被害と発生要因
- 事例

【A-4】サイバー攻撃「標的型攻撃」
- 被害と発生要因
- 事例（フィッシング＋ランサムウェア）

【A-5】人的ミス

【B】情報セキュリティ対策

【B-1】メール・Web利用時の注意
- 常に詐欺やフィッシングを疑う
- セキュリティ設定を緩めない
- 利用環境を『最新』の状態にする

【B-2】適切なアカウントの管理
- 適切なパスワードの設定管理
- 多要素認証の設定
- サインイン履歴の確認

【B-3】ファイル共有時の注意
- 人的ミスに注意する
- 適切なファイル共有方法の選択
- 適切なアクセス権の設定

【C】事故発生時の対応

情報セキュリティの脅威と事故事例

マルウェアの被害と発生要因

【A-1】

マルウェア 悪意のある(malicious)ソフトウェア(software)の総称

被害 マルウェア感染すると…

- データ破壊
- 不正通信(リモート操作)で情報窃取

⚠ **マルウェア感染した状態でネットワークに接続していると…**

ネットワークを介して
他の端末やシステム・サービスに
感染が拡大する可能性も

大規模な情報漏洩・業務停止の危険性

要因 マルウェア感染経路

マルウェアが仕込まれたファイルやソフトウェアを
ダウンロード・インストールしてしまった

メールの添付ファイル
Webサイトからインストール

脆弱性対策を怠っていたためマルウェア感染

- 古いOSやアプリケーション、Webブラウザ等を利用していた
- PCやWebブラウザのセキュリティ機能を緩めてしまっていた
- セキュリティ対策ソフトを導入していなかった

代表的なマルウェア

ボット	ウイルス	プログラムの一部を改ざんして自己増殖する
	ワーム	単体で存在して自己増殖する
	トロイの木馬	有用なプログラムなどを装って侵入する
キーロガー	スパイウェア	PC内に潜伏して情報を盗み取る
	バックドア	PCを外部から操作できるようにする
偽警告	アドウェア	不正な広告等を勝手に表示する
Emotet	ボットネット	処理を自動実行するボットの集合群
	ランサムウェア	ファイルを暗号化し解除と引き換えに金銭要求

✓ **Emotet**
2019年頃から世界的に流行
国内でも多くの教育機関で情報漏洩事案が発生

事例

✓ **ランサムウェア**
標的型攻撃に使用され
大規模な業務停止事案に発展している

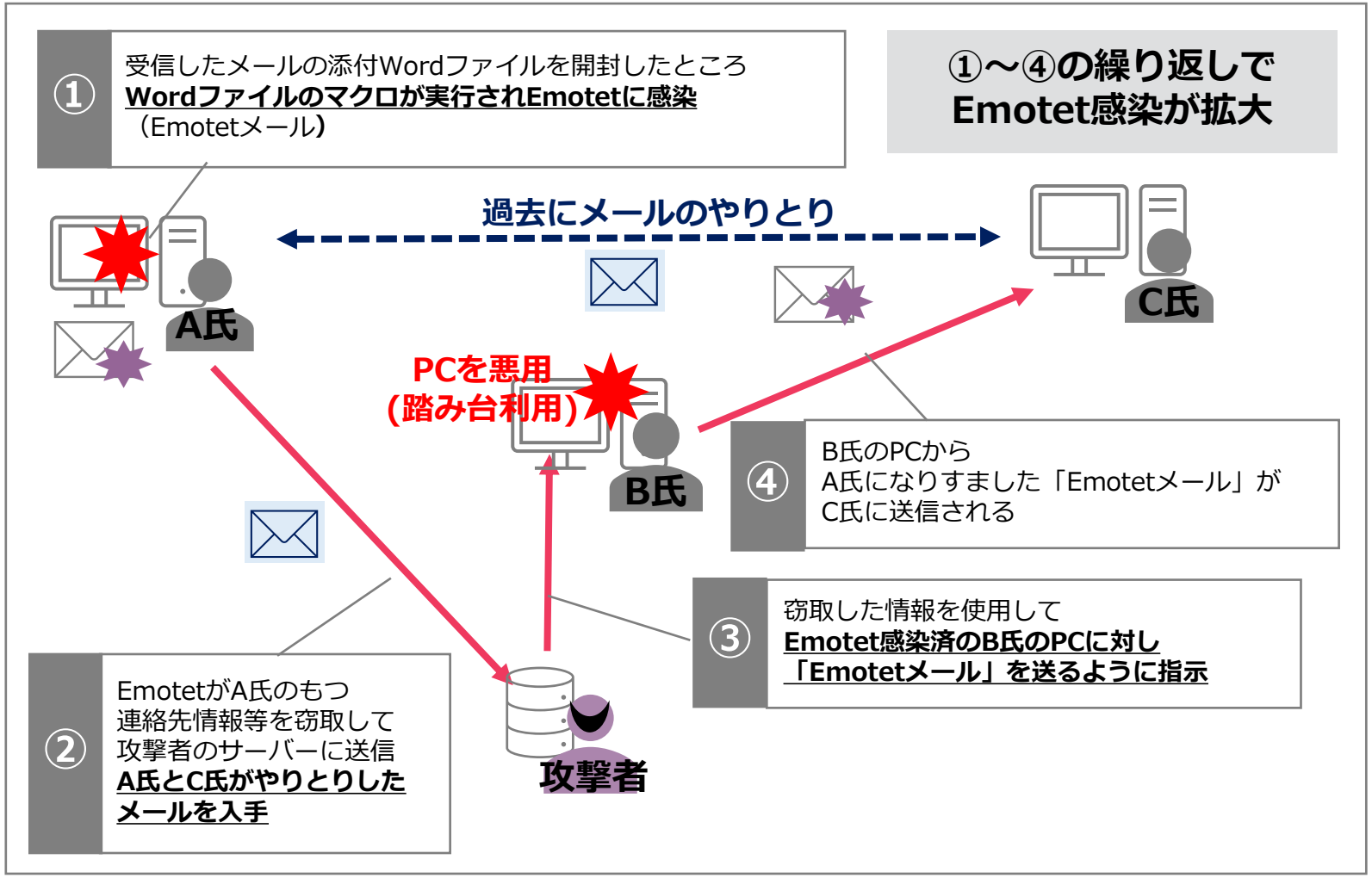
事例

Point

- 日々新たなマルウェアが生み出されセキュリティ対策ソフトでも検知しきれない
- 「一個人の被害」から「組織を狙った大規模攻撃」まで
- 大半の事故が**個人のメールとWeb利用**に起因

事例 マルウェア『Emotet』

【A-1】



- メールに悪性なWord形式のファイルが添付されており、Wordのマクロを実行すると攻撃者の侵入経路ができてしまいEmotetに感染する
- Emotetに感染すると**ID/パスワード情報や個人情報等が窃取**されるだけでなく、**メールアカウントを踏み台利用**されて「Emotet」メールを組織内外の拡散に悪用されてしまう
- Emotetメールは**過去にやり取りしたメールを窃取してそのメールに返信する形で送信される**ため、受信者はEmotetメールであることに気付きづらい

対応策

メール受信時
- **添付ファイルを安易に開封しない**

メールの利用環境
- **OS・ソフトウェアを常に最新の状態にする**
- **セキュリティ対策ソフトを導入する**

フィッシングの被害と発生要因

【A-2】

フィッシング　実在する組織を装って偽のWebサイトに利用者を誘導し、個人情報を入力させて窃取する不正行為

被害　窃取される情報と情報の悪用

フィッシングサイトに**入力した情報**
ex）氏名、住所、メールアドレス、
クレジットカード情報、ID/パスワード

⚠ **窃取された情報は…**

闇市場(ブラックマーケット)で売買され
様々な攻撃に悪用される可能性も

⚠ **ID/パスワードが窃取された場合…**

ID/パスワードを利用する
システム・サービスの不正アクセスを受ける可能性も

立命館のID/パスワードの使い回し禁止

要因　フィッシングに多いパターン

- **実在組織を騙るメール・SMS**を受信
  ex) 金融機関、ECサイト、郵便・宅配会社、行政機関
  自組織のシステム部門・システム管理者
  メール・ストレージサービス等からのシステム通知
- すぐに対処しないと被害を受ける等の**危機感を煽る内容**
- **メールの本文中のURL**にアクセスすると**偽サイト**が表示される

ID/パスワードを窃取する目的で偽の認証画面を表示するケースも

⚠ メールアドレスやURLを本物に偽装されたり
メール本文は不自然さがなく本物に類似している等
年々巧妙化して判別しづらくなっている

Point
- 危機感を煽る内容のメール・SMSに要注意
- 窃取された情報は様々な形で攻撃者に悪用されてしまう

事例 フィッシング

【A-2】

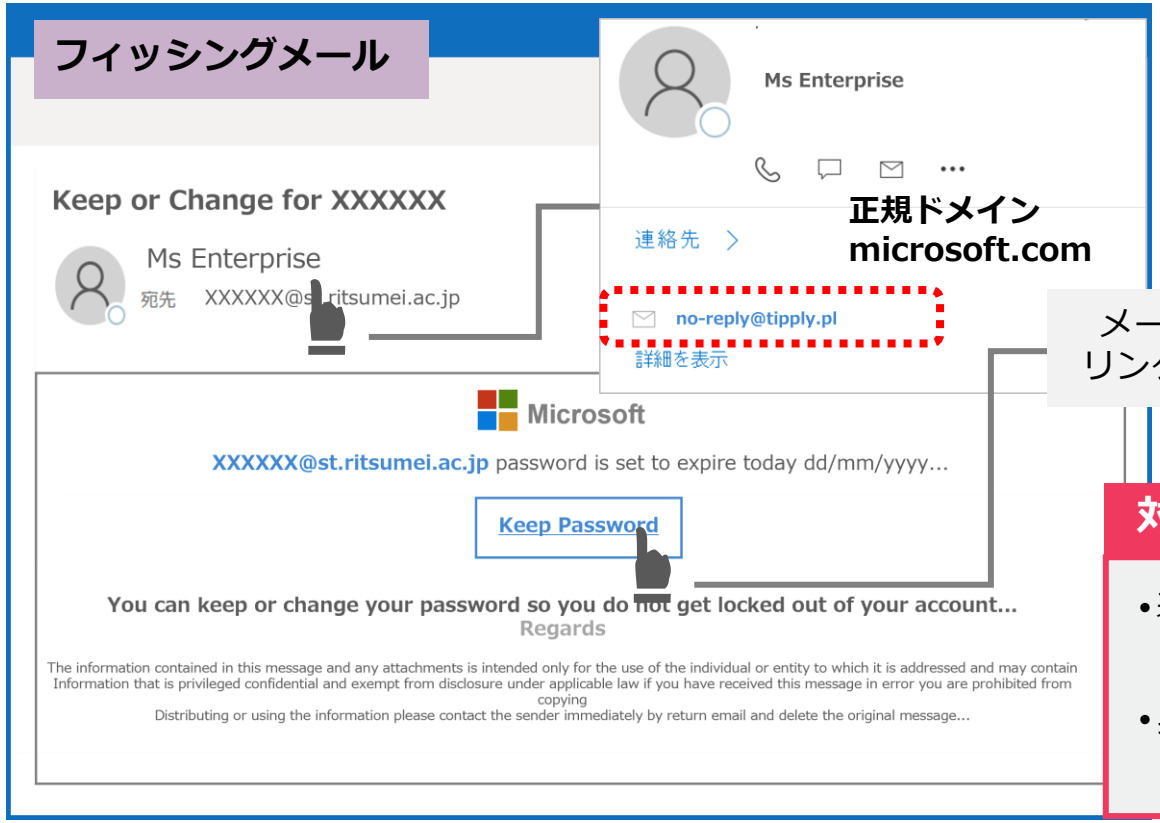
NG 表示されている差出人名は「MS Enterprise」だが
メールアドレスのドメインはMicrosoftの正規のものと異なる

⚠ **立命館のシステム管理者を騙るケース**も確認されている

正規ドメイン https://login.microsoftonline.com/common/oauth...

NG URLのドメインが**Microsoftの正規**のものと異なる

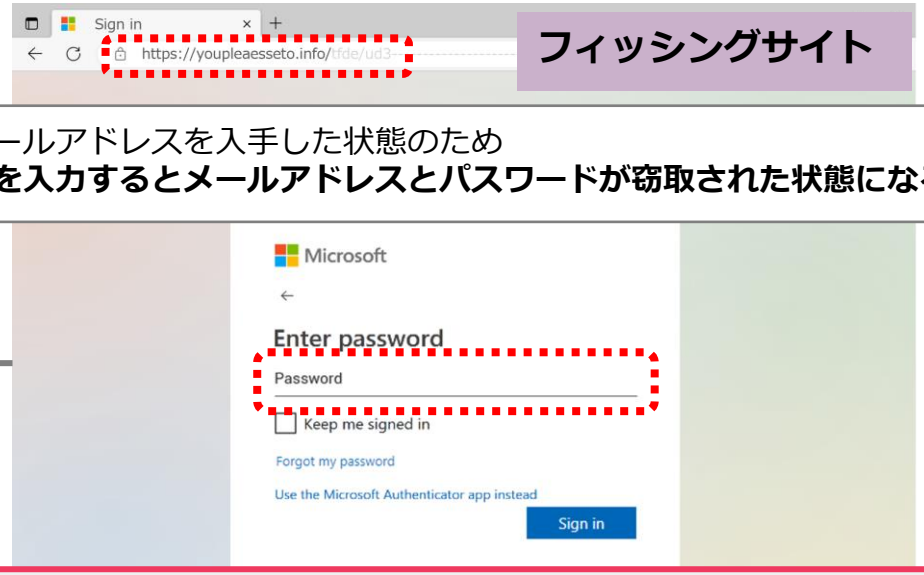
フィッシングメール



正規ドメイン
microsoft.com

メール本文中の
リンクにアクセス

フィッシングサイト



攻撃者はメールアドレスを入手した状態のため
パスワードを入力するとメールアドレスとパスワードが窃取された状態になる

対応策

- 表示される差出人名やリンクは詐称されている可能性があるため
  メールアドレスやリンク先のURLのドメインを確認すること
- 身に覚えがないメールが届いたら
  送信元の組織の公式窓口に直接問合せすること

ドメイン

インターネット上のコンピュータや
ネットワークを識別するために登録された
インターネット上の名前や住所にあたるもの

公式ドメイン	学校	ドメイン
	立命館大学/附属校	ritsumei . ac . jp
	立命館アジア太平洋大学	apu . ac . jp
	学校法人立命館	ritsumeikan-trust . jp

Point

ドット(.)とスラッシュ(/)の区切りで確認する
〔URL〕“https://”のあとの最初のスラッシュ(/)まで
〔メールアドレス〕 @以下

信頼性の高いドメイン例		
	ac.jp	高等教育機関および学校法人
	ed.jp	初等中等教育機関および 18 歳未満を対象とした教育機関
	go.jp	日本の政府機関や各省庁所管の研究所、特殊法人、独立行政法人
	lg.jp	地方公共団体と、それらの組織が行う行政サービス

OK

RITSUMEIKAN ITサポートサイトの「インターネットサービス利用ガイドライン」のPDF掲載ページ
https://**it.support.ritsumei.ac.jp**/hc/article_attachments/4410975757593/guideline-internetservice.pdf
└ **ドメイン** ┘ └ 表示するファイルの場所 ┘ └ 表示するファイルの名前 ┘

NG

公式ドメインに似せるために
ドメイン部分にハイフンを使用
https://**it.support.ritsumei-ac-jp.com**/~~~
└ **ドメイン** ┘

ドメイン以外の部分に
公式ドメインと同じ字を使用
https://**it.support.com**/ritsumei/ac/jp/~~~
└ **ドメイン** ┘

ドメインがac.jpではない
https://**it.support.ritsumei.xyz**/~~~
└ **ドメイン** ┘

⚠ 立命館が提供しているサービスであっても公式ドメインを使用していないサービスもありますので
正規のサービスか判別ができないときは対象サービスの問合せ窓口に問合せして確認してください

偽警告の被害と発生要因

【A-3】

偽警告　Web サイト閲覧時に偽の警告メッセージを表示して不安を煽る攻撃手法

被害　警告通知のメッセージに従うと…

⚠ 警告通知をクリックしたら…

マルウェア配布用のWebサイトに
アクセスしてしまい**マルウェア感染**

⚠ 偽のサポート窓口に問合せしてしまい…

案内に従って不正なソフトウェアを
インストールさせられ
リモート操作権限が奪われ
マルウェアを設置され、**情報を窃取**された
サポート料として金銭を要求された

（サポート詐欺）

要因　偽警告に騙されてしまう理由

なぜ偽警告が表示されるのか？

- Web閲覧時に**Webブラウザの通知設定**を
  意図せず追加・変更してしまっている
- 偽警告を表示させるアドウェア(マルウェア)
  に感染している

なぜ偽警告に騙されるのか？

不安を煽る通知内容・通知方法であるため
冷静な判断ができない状況に追い込まれる

不安を煽る偽警告の特徴

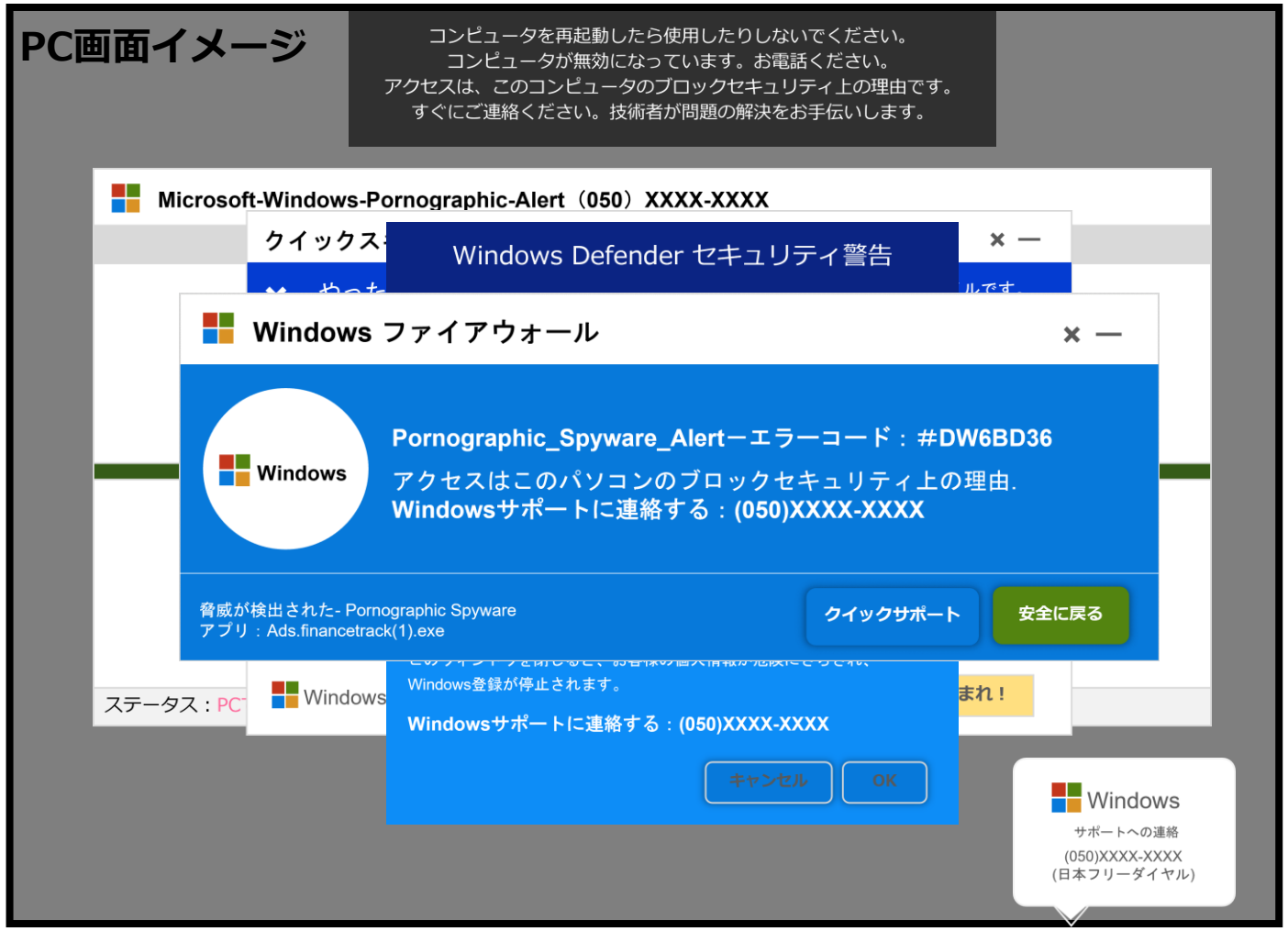
- 警告通知が次々と連なって開く
  通知は全画面表示で固定されており
  「閉じる」ボタンが隠れて
  画面を消すことができない
- 大音量の警告音や警告アナウンスが
  延々と流れる
- 実在する企業やサービスの
  ロゴを使用しており、
  特にPCのセキュリティ機能や
  ウイルス対策ソフトのものなどが
  使用されることが多い

Point

不安を煽る通知内容・通知方法に騙されずに
冷静な対処ができるように事例を知っておくこと

事例 偽警告

【A-3】



セキュリティ警告通知が次々に表示され、
警告音やアナウンスが大音量で流れる

表示されている電話番号に連絡すると
片言の日本語を話すオペレーターに繋がる

ソフトウェアをインストールさせ遠隔操作をおこない
異常が発生していると虚偽の説明をする

有償のサポート契約を勧める、偽サイトに個人情報を入力させる

対応策

- 安易にWebブラウザの通知を許可しない
- 警告通知を安易にクリックしない
  （マルウェア感染の危険性あり）
- 警告通知記載の電話番号に電話をかけない
  （通常、正規の警告画面に電話番号が記載されていることはない）

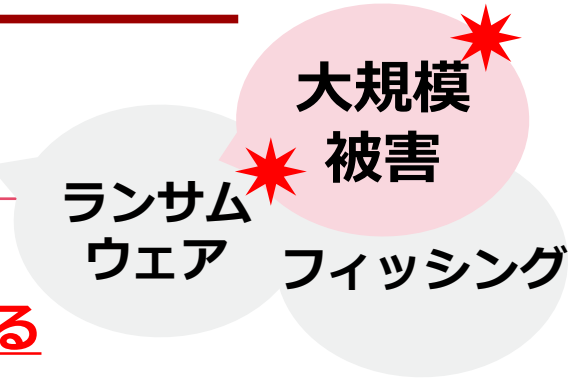
遠隔操作されてしまった場合
- どのような攻撃を仕掛けられているかの
  特定が難しいため**PCの初期化推奨**

標的型攻撃

【A-4】

標的型攻撃

特定組織の機密情報の窃取や業務妨害を目的としたサイバー攻撃
より巧妙化された攻撃手法で組織内部に侵入する



- 特定組織に対して効果的な攻撃を仕掛けられるため**攻撃に気づきづらい**
- **学生・生徒情報**や**研究情報**を有する**教育・学術機関は攻撃者から狙われている**

組織の“**個人**”を狙い
マルウェア感染や
アカウント窃取を
大規模攻撃の
糸口とする

学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）
内閣サイバーセキュリティセンター（NISC）/警察庁サイバー警察局　令和4年11月30日

特徴

- 実在する組織の社員・職員をかたり、**イベントの講師、講演、取材等の依頼メールや資料・原稿等の紹介メール**が送られてくる。
- 日程や内容の調整に関するやりとりのメールの中で、**資料や依頼内容と称した URLリンク**が本文に記載されたり、**資料・原稿等という名目のファイルが添付**されたりする。当該 URL をクリックしたり添付ファイルを開いたりすると、マルウェアに感染する。

ex）送信メールアドレス

- 表示名(詐称対象の人物名)＜見覚えのない不審なメールアドレス＞
- ＜詐称対象の人物名＞@＜詐称対象の組織略号＞.com
- ＜詐称対象の人物名＞@＜詐称対象の組織略号＞.org
- ＜詐称対象の人物名＞@＜著名なフリーメール※のドメイン＞

※yahoo.co.jp、gmail.com、outlook.com 等

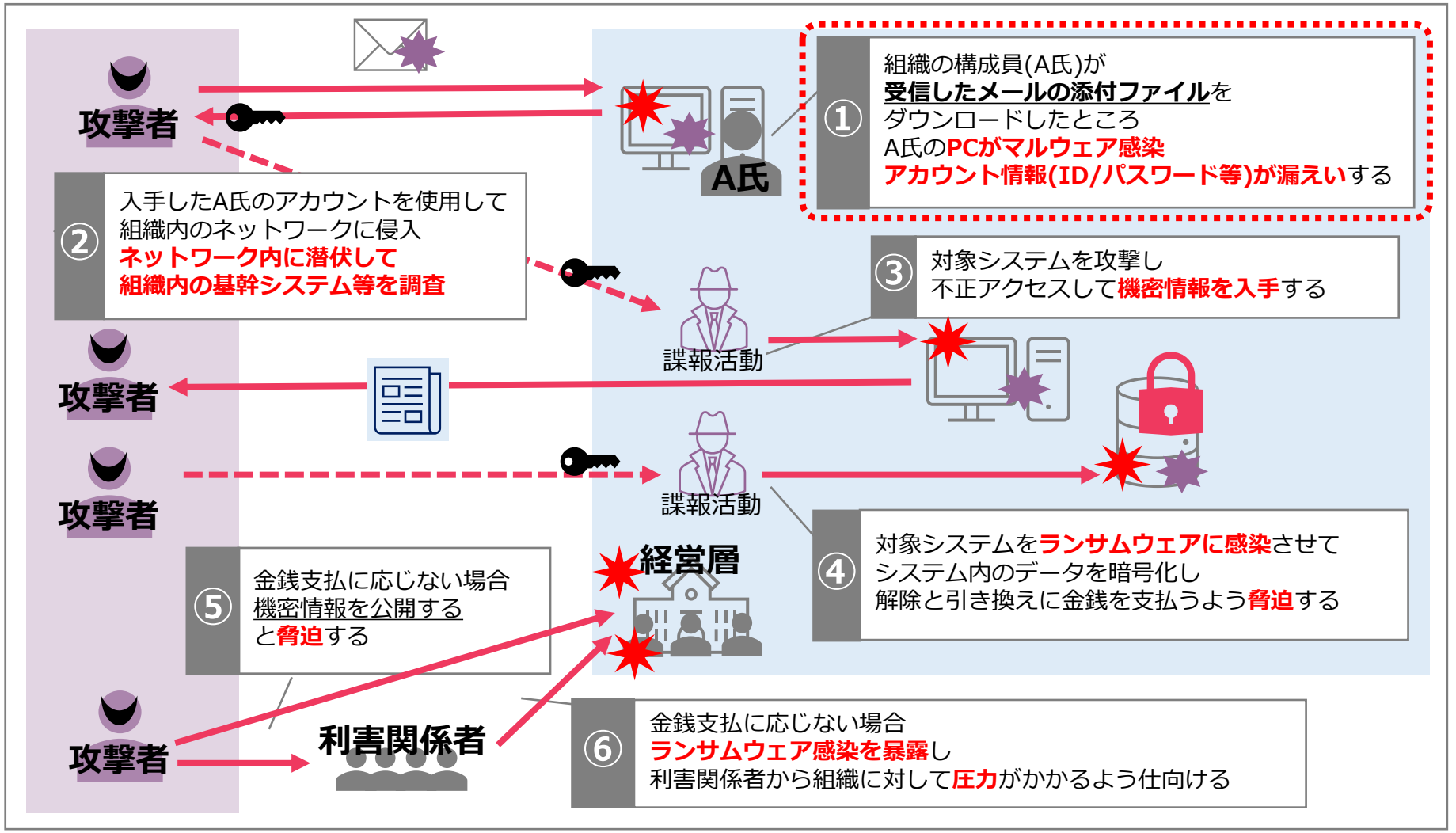
ex）メール件名

- 【依頼】インタビュー取材をお願いします
- 研究会へのゲスト参加のお願い【●●●●●●※】
- 【ご出講依頼】●●●●●●※勉強会

※ ●には実在する組織名等が入る

事例 標的型攻撃

【A-4】



A氏を標的にしたメール例　標的型メール

- A氏が実際に受信する可能性がある実在する組織の社員を騙ったなりすましメール
- 窃取した別のメールアカウントを使用し過去のやりとりした内容をもとに関係性のあるメール送信する

標的型攻撃の目的

対個人
- 学術関係者の研究情報

対組織
- 学生・生徒の個人情報の窃取
- 業務情報等の機密情報の窃取
- 金銭要求
- 業務妨害

ランサムウェア

対応策

アカウント窃取を防ぐ
マルウェア・フィッシング対策

事例 人的ミス

【A-5】

事例①
メールの一斉送信をおこなうときに
宛先をBCCに設定すべきであったが
誤ってCCに設定して送付してしまい
連絡先メールアドレスがメール受信者全員に
見られる状態になってしまった

メール送信前に
宛先確認する習慣
をつけていれば…

事例②
学生と共有するPCで
個人のメールやOneDriveに
サインインしたまま他利用者に貸してしまい
学生がメールやOneDriveを閲覧可能な状態に
なっていた

共有PCを利用する
場合のルールを
明確にしておけば…

事例③
情報資産を含むファイルが入った
USBメモリを紛失してしまった

ファイルにはパスワードを設定していたが
容易に推測可能な**単純なパスワード**であった

強度の高い
パスワードを
設定していたら…

事例④
情報資産を含むファイルを
オンラインストレージ(学外サービス)に
保管してその**リンクをメールで共有**した

オンラインストレージには
アクセス権の設定をしておらず
メール受信者であれば誰でもアクセスできる
状態であった

アクセス権を
適切に設定した
オンラインストレージを
利用していたら…

事例⑤
情報資産を含むファイルをメール添付で送付したが
Gmailのメールアドレスを誤って
「～@gmai.com 」として送付してしまった

**ドッペルゲンガー
ドメイン問題**

添付ファイルはパスワード付Zipにしていたが
パスワードも誤ったメールアドレス宛に送付
してしまった

**PPAP
問題**

Point
人的ミスを“発生させない”だけでなく
発生してしまったとしても”**情報漏洩を最小限に抑えるための対策**が必要不可欠！

情報セキュリティ対策

メール・Web利用時の注意

【B-1】

常に詐欺やフィッシングを疑う

✓**メールを開封する前**
✓**添付ファイルをダウンロードする前**
✓**メール本文中のリンクにアクセスする前**

「怪しい」と疑うポイントをおさえて
安易にアクセス・ダウンロードしないようにすること

- メールアドレスやURLの**ドメインが正しいか確認する**こと
- アカウント情報や請求情報を確認するときは
  メール本文中のリンクからはアクセスせず
  公式サイトから直接アクセスして確認すること

セキュリティ設定を緩めない

立命館のメールはMicrosoftのセキュリティ機能で
マルウェア・フィッシングの疑いのあるメールは
受信BOXに届く前に検疫して隔離されます（メール検疫機能）
検疫通知メールを確認し、明らかに誤検知と思われるメール以外は[リリースの要求]をしないようにしてください

RITSUMEIKAN IT SUPPORT メールの検疫について

利用環境を『最新』の状態にする

✓**ソフトウェア（OS・アプリケーション）**
✓**Webブラウザ**
✓**ネットワーク機器（ルーター等）**

サイバー攻撃の侵入経路となる脆弱性をなくすために
最新のバージョンを使用すること**（自動アップデート推奨）**

立命館で報告を受けたサイバー攻撃事例や
行政機関等から提供されたセキュリティ関連情報は
立命館CSIRTから発信される注意喚起情報を確認してください

RITSUMEIKAN IT SUPPORT RITSUMEIKAN ITサポートサイト お知らせ

認証　利用者が本人であるかを確認する

認証方法	①	知識情報	本人のみが知っている情報	パスワード、PIN番号、秘密の質問　等
	②	所持情報	本人のみが所持している物品	スマートフォン、ハードウェアトークン、社員証、ICカード　等
	③	生体情報	本人の身体的特徴	指紋、顔、光彩、網膜、静脈　等

立命館のIDは①と②による多要素認証

多要素認証

セキュリティの強度を高めるために
①～③の異なる認証方法を
複数組み合わせて使用する認証方法

- 不正アクセスを防ぐためには
  それぞれの認証方法が
  高い強度で守られている必要がある
- 知識情報はサイバー攻撃により
  窃取される危険性が高い
  - フィッシング
  - マルウェア感染
  - アカウントリスト攻撃
  - ブルートフォース攻撃(総当たり攻撃)

不正アクセスを未然に防ぐために
- **適切なパスワードの設定管理**
- **多要素認証の設定**
- **アクセス履歴の確認**

認可　許可された利用者のみがアクセスできるようにする

ファイル共有時の
- **適切なファイル共有方法の選択**
- **適切なアクセス権の設定**

適切なアカウントの管理

【B-2】

適切なパスワードの設定管理

- 推測されにくい**強度の高いパスワードを設定**する
- 他サービスへの**パスワードの使い回し禁止**
- パスワードの**他人への共有禁止**

パスワード設定時のポイント
- 辞書にある単語や固有名詞を使わない
- 文字数は 8 文字以上にする（12 文字程度を推奨）
- 文字の種類は大文字、小文字、数字、記号を組合せる
- 覚えやすいように変換ルールやアナグラムを使う

パスワードの使い回しは
他サービスからパスワードが漏洩する可能性があり
サイバー攻撃を受けるリスクが高まる

参考）**Have I Been Pwned** https://haveibeenpwned.com/
過去の個人情報漏洩事件でアカウント情報
(メールアドレス・パスワードの組み合わせ)
が漏えいしているかを調べることができるWebサイト

多要素認証の設定

立命館のアカウントは多要素認証必須
他サービスを利用する際も可能なものは
多要素認証を設定すること

心当たりのない多要素認証要求があった場合は
要求を許可せずにサインイン履歴を確認してください
心当たりのないサインインがあった場合は
速やかにパスワード変更をしてください

サインイン履歴の確認

Microsoft365
自分のサインイン(プレビュー)
https://mysignins.microsoft.com/

日常的な利用でどのようなサインイン履歴が残るのか事前に把握し
定期的に不審な履歴がないか確認すること

立命館のアカウントで不審なサインインが検知された場合
通知メールが送付されます
メールを受信したら速やかにセキュリティ対応を実施し
心当たりのないサインインがあった場合は
RAINBOWサービスデスクに報告してください

ファイル共有時の注意

【B-3】

人的ミスに注意する

宛先設定ミス、メールアドレス間違い等の
誤送信による情報漏洩が発生しないように注意すること

メール添付でのファイル共有は人的ミスが発生しやすく
「送信ミス＝情報漏洩」になってしまうため
情報漏洩を最小限に抑えるための対策が不可欠！

適切なファイル共有方法の選択

本学の情報資産の取扱いルール(関連規程)に応じた
適切なファイル共有方法を選択すること

低
機密性
高

- **メール添付**
  メールの性質(通信経路で盗聴される可能性)も考慮して
  機密性の高い情報は扱わないようにすること
- **オンラインストレージ**
  学外ネットワーク上に保存する状態となるため
  保存する期間は必要最低限にとどめ
  適切なアカウントの管理、
  適切なアクセス権の設定をおこなうこと
- **事務ファイルサーバ**（事務端末のみ）
  学内ネットワーク上に保存する状態となるため
  適切なアクセス権の設定をおこなうこと

機密性の高いファイルをメール送付する方法として
慣例化されている
**「メールにパスワード付zipファイルを添付して送付」は
セキュリティの観点から非推奨**であるため
オンラインストレージによるファイル共有を利用すること
（詳細は次スライド参照）

学内サービス利用方法 RITSUMEIKAN IT SUPPORT OneDriveを活用しよう

適切なアクセス権の設定

誰にアクセスさせてよい情報なのかに留意し
適切なアクセス権を設定すること（認可）

PPAP

メール添付で**パスワード付Zip暗号化ファイル**を送付し、
パスワードをメールで送付する方法

PPAPは昨今のセキュリティの脅威に対しては有効ではなく
送信者・受信者双方にとってセキュリティリスクの高い手段
であるため使用しないようにすること

P：Password付zip暗号化ファイルを送ります
P：Passwordを送ります
A：Aん号化(暗号化)
P：Protocol

非推奨な理由

⚠ **ファイルが暗号化されていると**
メールシステムのマルウェア検知機能やセキュリティ対策ソフトが有効に機能しない

⚠ パスワード付zipとパスワードを同手段(メール)で送付することが慣例となっており、
送信先間違いやアカウント窃取対策としても有効ではない

- 宛先を間違えた場合、同宛先にパスワードを送っているため受信者はファイルを開封できてしまう
- 送信者or受信者が情報セキュリティ事故を起こしている場合
  メールアカウントが窃取されている、メールを攻撃者に自動転送する設定をされている

Point

ファイルを送付(共有)する際にはセキュリティリスクの高い「PPAP」はおこなわず
アクセス権を適切に設定したオンラインストレージ(OneDrive等)を活用すること
ファイル共有後はオンラインストレージに保管したままにせず削除すること

事故発生時の対応

事故発生時の対応

【C】

「事故が発生してしまったかもしれない」と思った時点で迅速な初動対応をおこなうことで被害を最小限に抑えられる！

アカウント窃取　マルウェア感染

初動対応

① **ネットワーク抜線(切断)**
② **パスワード変更**
③ **マルウェアスキャン(駆除)**
④ **アクセス履歴の確認**
⑤ **アカウント設定の確認**

時系列に添って報告できるように
対応内容を記録しておくこと！

RITSUMEIKAN IT SUPPORT パスワードの変更とメールシステム設定を確認する

立命館CSIRTへの報告

- **事故発生の経緯**
  なぜ事故が発生したと思ったのか
  何をしているときに発生したのか
- **初動対応内容**
  報告前にどのような対処をしたのか
- **被害状況**
  どのような環境で利用していたのか
  事故発生時に接続していたネットワーク
  利用していた機器
  被害を受けた可能性がある情報資産は何か

RITSUMEIKAN IT SUPPORT 【学内の方へ】立命館CSIRT 情報セキュリティ事故緊急連絡受付窓口(PoC)

二次対応

立命館CSIRTからの対応指示

※**個人情報漏洩**の可能性あり
→**総務課**への報告が必要