

FIDO2セキュリティキーによる パスワードレス・キャンパスネットワークの 構築とその応用

Implementation of FIDO2 Server and
Passwordless Network Using
Campus ID Type Security key

城西大学経営学部教授

杉本 理(すぎもとおさむ) : sam@josai.ac.jp



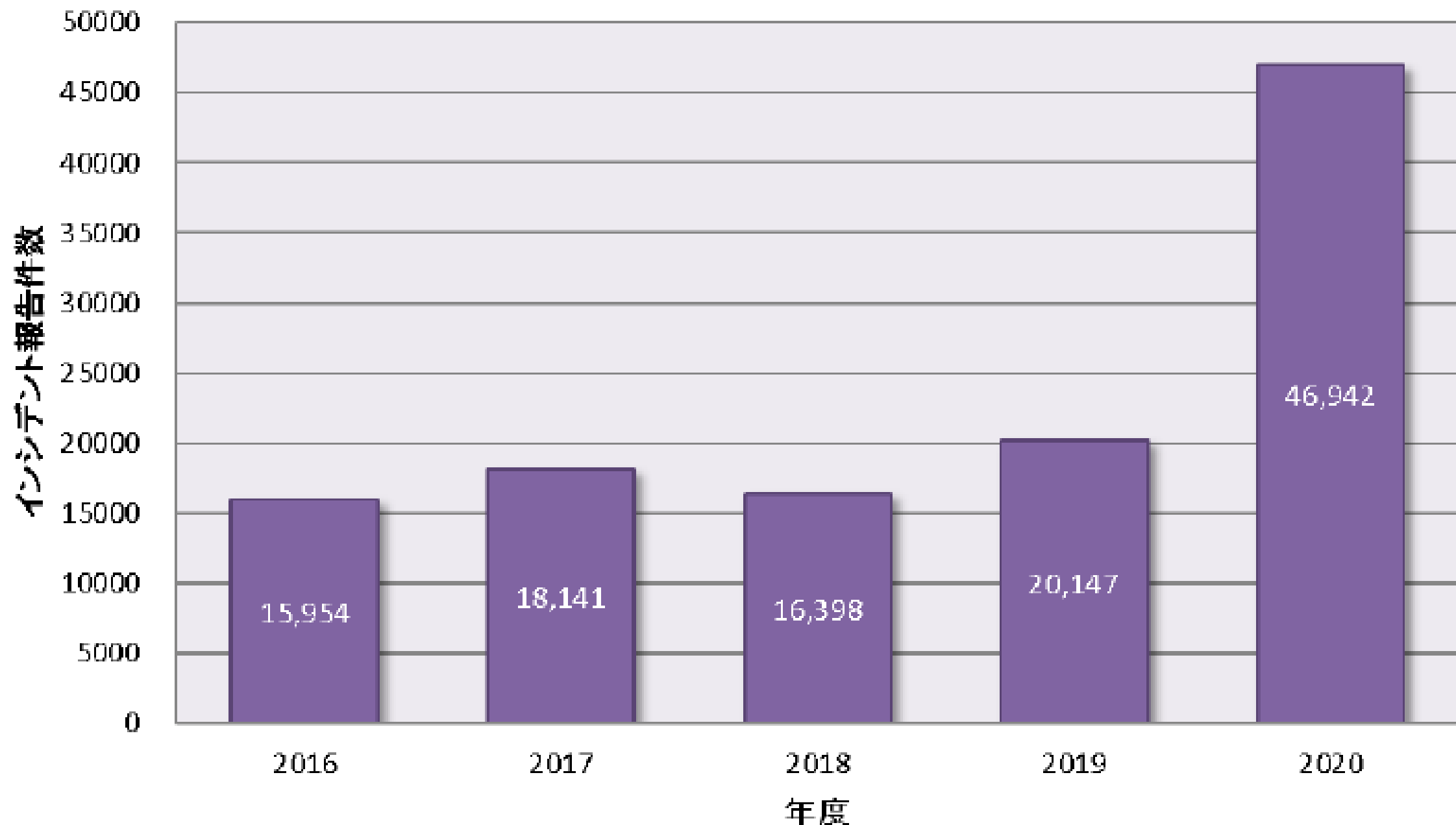
1.概要

大学のキャンパス・ネットワークをターゲットにしたサイバー攻撃は後を絶たず、海外の例では身代金約5000万円を支払った例も報告されている。これらの攻撃のほとんどがフィッシングなどによるパスワードの漏洩に起因する。人的及び金銭的リソースが限られる大学等教育機関において情報資産を保護するためのベストプラクティスは何であるか。本研究ではサイバー攻撃の被害実態とその要因、高度なセキュリティと利便性を両立するパスワードレス・キャンパスネットワークに必要なFIDO2サーバーの実装とその応用について提案する。

2. 研究の背景

2.1 増え続けるサイバー攻撃

年間報告件数の推移

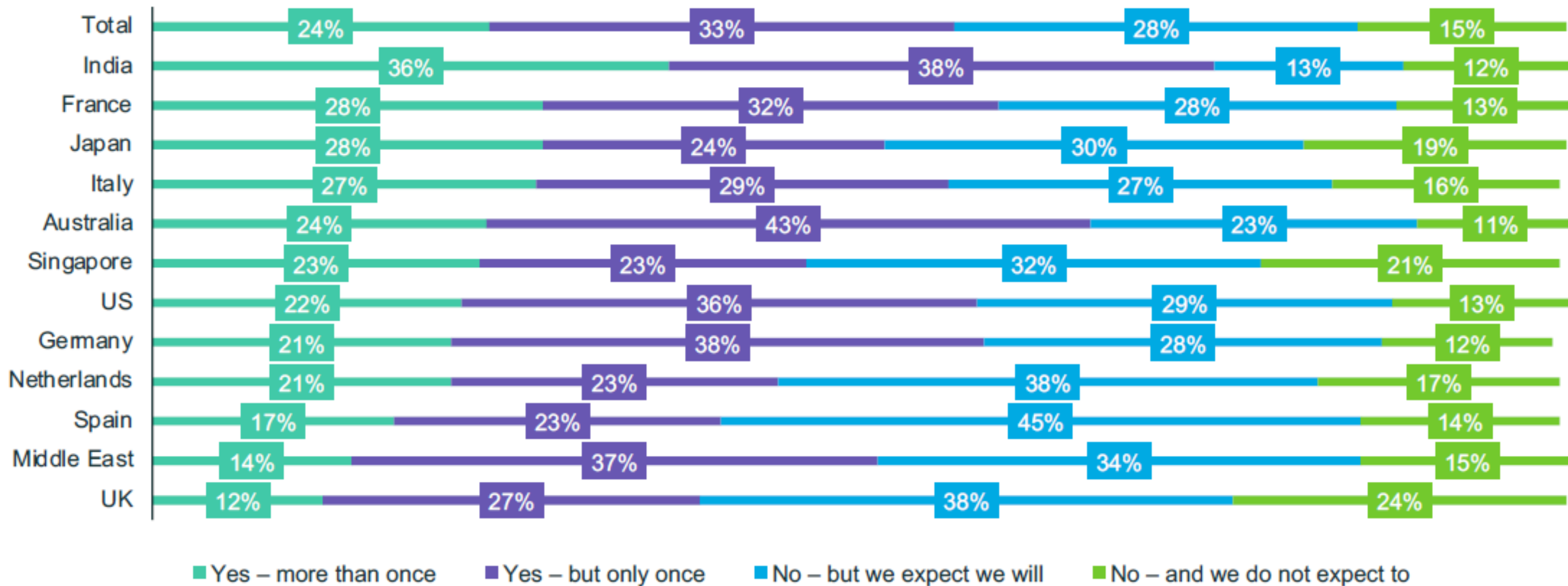


JPCERT/CC インシデント報告対応レポートより

Copyright Josai University

2.2 ランサムウェア

Approaching six in ten (56%) respondents work for an organization that has suffered a ransomware attack during the last 12 months



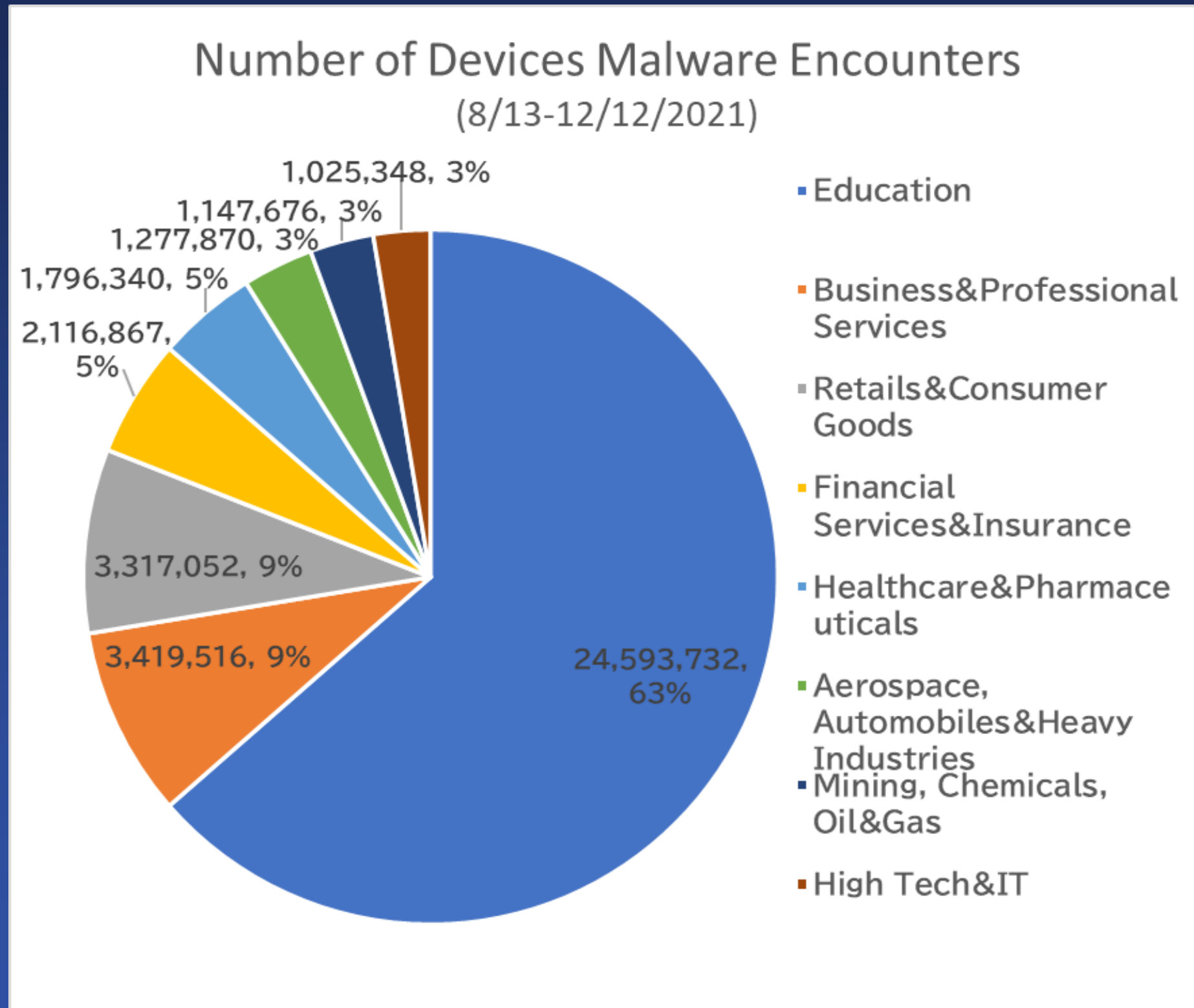
2.2 ランサムウェア

日本企業の52%が過去12カ月以内にランサムウェアの攻撃を受けているほか、ランサムウェアの被害に遭った日本企業の32%が身代金の支払いに応じているという。またその平均額は117万ドル(約1億2300万円)にのぼる。

2.3 攻撃対象の変化

最近では攻撃の対象が身代金を払わざるを得ない中小の組織である地方自治体、ライフライン、NGO、そして教育機関にシフトしてきている(Deloitte Touche Tohmatsu Limitedより)。

教育機関が63% (直近4ヶ月)



2.4 大学へのサイバー攻撃

- お茶の水女子大学の例

2019年7月1日、お茶の水女子大学は所属教員1名のメールアドレスが何者かの不正アクセスを受け、ID・パスワードが盗まれたことでアカウントが乗っ取られた。犯人は奪ったメールアドレスを利用し、合計2,215件のスパムメールを送信。さらにメールボックス内を閲覧されたことで以下のような被害が出た。

- ・ 機密情報（氏名・所属・メールアドレス・電話番号など）

- ・ 内訳：教職員62件、学生88件、学外者77件

2.4 大学へのサイバー攻撃

- 慶應義塾大学の例

2020年9月湘南藤沢キャンパスの情報ネットワークシステムおよび授業支援システム(SFC-SFS)において、何らかの方法でシステムの利用者19名(教職員)のIDおよびパスワードが窃取され、それを用いた外部からの不正アクセスと授業支援システムの脆弱性をついた攻撃により、同システムから利用者の個人情報情報が漏洩した可能性があることが判明した。

学生情報5088件、同顔写真18636件、単位取得情報4493件、教員情報2276件など

学術機関における被害としては過去最大規模

2.4 大学へのサイバー攻撃

- 城西大学の例

同様にサイバー攻撃によるセキュリティ・インシデントがあり、二次被害が出ている。

- ① 2019年2月に学生のメールアカウントが19件乗っ取られ、踏み台となったため9,800通以上の迷惑メールが送信された。
- ② 2019年6月「教室コントロールシステム」に対する不正アクセスによって登録している利用者情報が外部に漏洩した。

2.4 大学へのサイバー攻撃

- 東京農工大学
- 東京理科大学
- 明治大学
- 横浜市立大学

2.4 大学へのサイバー攻撃

- ユタ大学の例

2020年7月サーバー上の約0.02%のデータが漏洩

その後、学生の機密情報がブラックマーケットに晒されたことで身代金（解決金）約5000万円を支払った。

⇒米国では身代金を払う大学とそうでない大学が二分

Paid: Columbia College Chicago, UC San Francisco

Not to pay: Michigan State

2.4 大学へのサイバー攻撃

Times up. #NetWalker leaked data from the MSU (@michiganstate) ransomware incident. The first part of the leak is now available for download. This is just a taste to show how sensitive the info is. It's likely that more MSU leaks will follow, if the ransom is not paid. <https://t.co/AUoZtE72hb>

— Ransom Leaks (@ransomleaks) June 4, 2020

2.5 感染経路

“Phishing, the delivery mechanism of choice for ransomware and other malware” (Deloitte Touche Tohmatsu)

“最近のランサムウェアはフィッシングやエクスプロイトを用いて侵入する”
(トレンドマイクロ)

About 70% is Phishing(2021 / 2Q)

Category	Number	Ratio
Phishing	4,841	69.4%
Web Site Tampering	251	3.6%
Malware Site	38	0.5%
Scan	1,385	19.9%
DoS/DDoS	8	0.1%
Control System	0	0.0%
Targeted Threat	5	0.1%
Others	449	6.4%

Ref: JPCERT/CC Incident Report(2Q2021)

2.6 被害の要因 #1

- 巧妙化するフィッシング
 - リアルタイム・フィッシングが主流
- * ハードトークンなどのTOTPは役に立たない



リアルタイム・フィッシング

kyufukin.soumugo.jp / soumu-go-jp など

特別定額給付金



オンラインで申請する

(マイナンバーカードをお持ちの方)



マイナポータルから
オンライン申請を行う場合は、
以下の準備が必要になります。

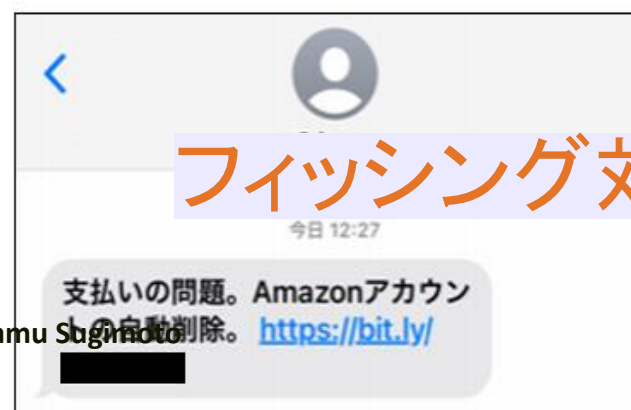
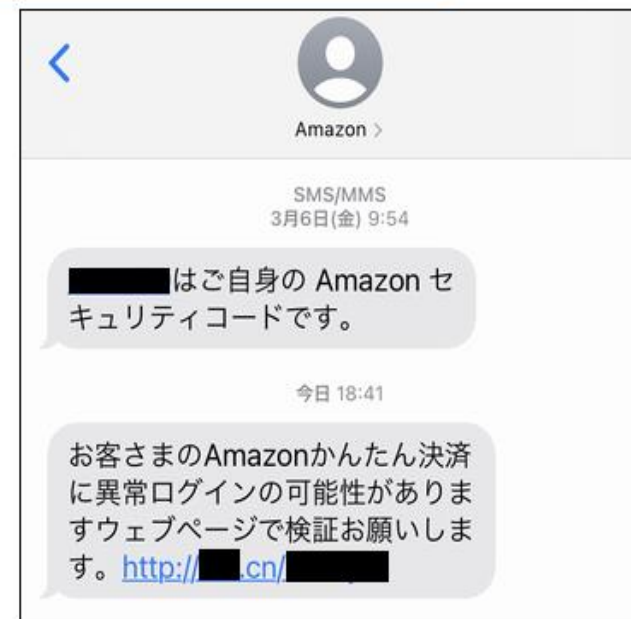
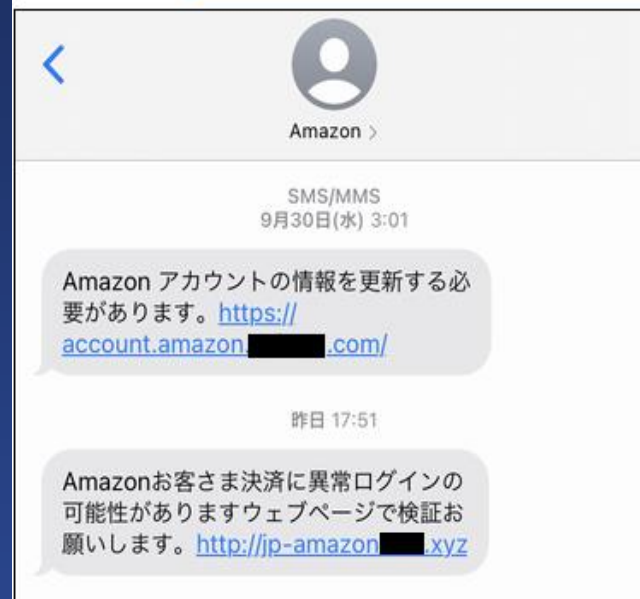
- 給付対象者と受給権者**
給付対象者: 基準日(令和2年9月27日)時点で、住民基本台帳に記録されている/者/在
日労働者/在日留学生(半年以内に日本から出国しないもの)
受給権者: 給付対象者の属する世帯の世帯主
- 申請表必要事項を入力します。
- 免許/保険証/パスポートなどの本人確認書類をアップロード。
- 申請完了、給付金ご指定された銀行カード/口座に振り込まれます。(支給日は、各市区町村により異なります)

オンライン申請

Copyright Josai University

リアルタイム・フィッシング アマゾン:2017~

SMS 文面の例



フィッシング対策協議会より

リアルタイム・フィッシング アマゾン:2017～

フィッシングサイトの例

amazon.co.jp

ログイン

[パスワードを忘れた方](#)

Eメールまたは携帯番号アカウントの番号

Amazonのパスワード

☒ パスワードを表示

☐ ログインしたままにする [詳細](#)

ログイン

続行することで、Amazonの[利用規約](#) および[プライバシーポリシー](#)に同意するものとみされます。

Amazonは初めてご利用ですか?

新しいAmazonのアカウントを作成

検索・閲覧履歴

[利用規約](#) [プライバシー規約](#) [パーソナライズド広告規約](#)

© 2000-2020, Amazon.com, Inc. and its affiliates

amazon.co.jp

問題が発生しました。
使用制限ポリシーに違反している可能性があることが検出されました
アカウントを確認してください

住所を確認する

氏名

郵便番号

都道府県を選択してください

住所1

住所2

会社名: (オプション)

電話番号

住所を確認

amazon.co.jp

クレジットカード情報を確認します

クレジットカード名義人

カード番号

セキュリティコード

有効期限:

01 2020

カードを確認

amazon.co.jp

情報認証を通過しました

今は必要なすべてのステップが完了しているので、あなたのアカウントにアクセスできます。

注:

- Amazonは自動的にホームページにジャンプします。
- うまくジャンプできなかったら「続行」をクリックしてください

続行

2.6 被害の要因#2

- パスワードの多さ

- * 城西大学(11個以上):

WiFi、共有PC、Web財務、JUNavi(Campusmate)、WebClass、Cypochi(CMS)、給与明細システム、DataBrain、VPN、図書館システム、科研費、各種学会

- * 慶應大学SFC(7個以上)

WiFi、WiFi(研究室)、Eduroam、CANVAS、CNS、keio.jp、科研費、各種学会

2.6 被害の要因#3

- パスワードの使いまわし(IPA:2020年度情報セキュリティの脅威に対する意識調査)

プライベートな情報を書き込むアカウント (パソコン利用者)

自分で記憶してる人の使いまわし割合 (抜粋)				紙に記録してる人の使いまわし割合 (抜粋)			
	複数所有	使いまわしてる	%	複数所有	使いまわしてる	%	
2-5個	416	174	41.83%	308	125	40.58%	
6-10個	284	129	45.42%	229	81	35.37%	
11-20個	217	95	43.78%	206	74	35.92%	
21-50個	196	81	41.33%	177	53	29.94%	
51-100個	42	18	42.86%	43	13	30.23%	
101個以上	22	9	40.91%	11	1	9.09%	

金銭のやりとりを行うアカウント(パソコン利用者)

自分で記憶してる人の使いまわし割合 (抜粋)				紙に記録してる人の使いまわし割合 (抜粋)			
	複数所有	使いまわしてる	%	複数所有	使いまわしてる	%	
2-5個	429	197	45.92%	389	163	41.90%	
6-10個	335	158	47.16%	306	116	37.91%	
11-20個	261	117	44.83%	268	96	35.82%	
21-50個	236	95	40.25%	253	81	32.02%	
51-100個	43	17	39.53%	53	16	30.19%	
101個以上	25	10	40.00%	14	1	7.14%	

2.7 Research Question

- 人的・金銭的リソースが限られている大学のキャンパスネットワーク環境において、学生の情報など情報資産を守るベストプラクティスは何か？
- 海外大学ではどうしているのか？
- 例えば多要素認証を導入した場合の問題点や課題は何か？解決方法は？

3. 大学における ベストプラクティス



3.1 多要素認証(MFA)の導入

Microsoft社とGoogle社の例

Microsoft社では同社のクラウドサービスに対して一日3億程度の悪意のあるサインイン攻撃があり、同社の研究によるとMFAを適用することでこれらの99.9%は防御可能であると発表。

Google社はリカバリー用電話番号とそれを用いたSMSによるMFAを有効化するだけでもボットによるGoogle Accountへの攻撃の100%、フィッシングの99%、標的型攻撃の66%を防御できると発表。

3.2 Stanford/MITの例

Duoによる2要素認証

Stanford University

Stanford | Login

Two-step authentication is required to log in



[What is this?](#) [Add a new device](#) [My Settings & Devices](#) [Need help?](#)

Powered by Duo Security

Device:

Choose an authentication method

☒ Duo Push recommended	Send Me a Push
☐ Call Me	Call Me
☐ Passcode	Enter a Passcode

☐ Remember me for 90 days

Important Security Information: Logging in lets you access other protected Stanford websites with this browser, not just the website you requested.

- [LOGIN HELP](#)
- [TWO-STEP HELP](#)
- [TWO-STEP DEVICE UNAVAILABLE?](#)

Use of this system is subject to Stanford University's rules and regulations. See the [Stanford Administrative Guide](#) for more information.

10:02 AM 87%

Login Request
Protected by Duo Security



Stanford University
Two-Step



171.66.214.130
Stanford, CA, US



10:02:11 AM PDT
April 12, 2018



Approve



Deny

3.3 MFAの問題点とパスワードレス

- 多要素認証は複数デバイスによる認証がほとんど

⇒パスワードのみに比べて利便性に欠けるため普及を阻害

- パスワードレスによる多要素認証は複数デバイスによる認証の必要はない＝ワン・デバイス

⇒パスワードレス認証はFIDO2セキュリティ・キーを利用してワン・デバイスで多要素認証を実現＝利便性を損なわない・もちろんパスワードも流出しない

3.4 Campus ID=Security Key

1. Something you have:身分証

2. Something you are:指紋



3.4 Campus ID=Security Key

大学環境では「生体」+「所持」の2要素認証がMust

⇒ AuthenticatorやDuoは「なりすまし」や「代返」防止にならない(友人のスマホを持ち歩く)

⇒ 非生体型のセキュリティキーも「なりすまし」や「代返」防止にならない(友人のキーを持ち歩く)

⇒ 「所持」がExtra Itemにならない(身分証)

⇒ 忘れた時に事務室で対応可能:運用

⇒ 紛失時に届けられる可能性大:運用

4. FIDO2サーバーの 構築とその応用

Josai Attendance Management System (JAMS)

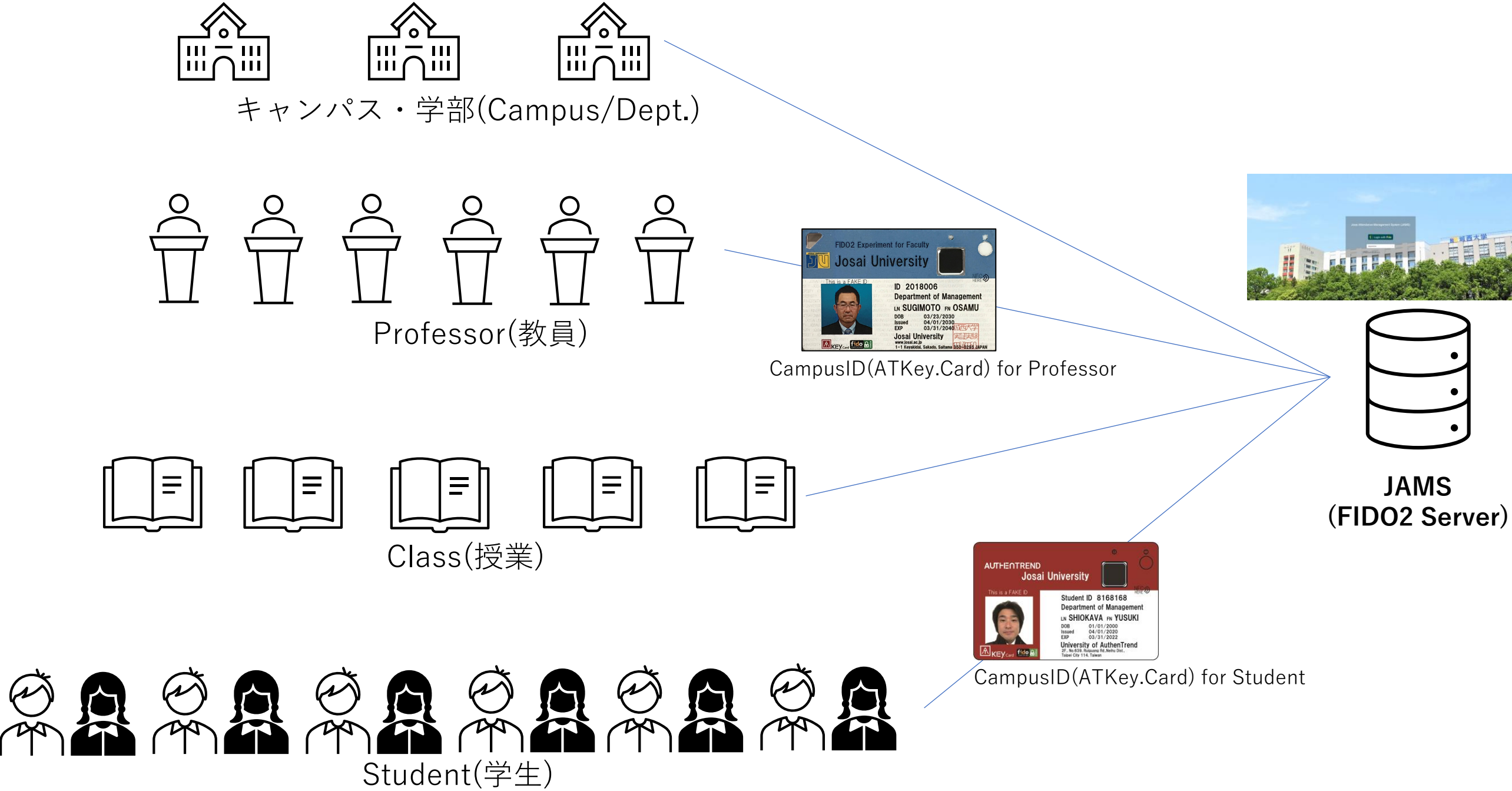
 | Login with **fido**

English

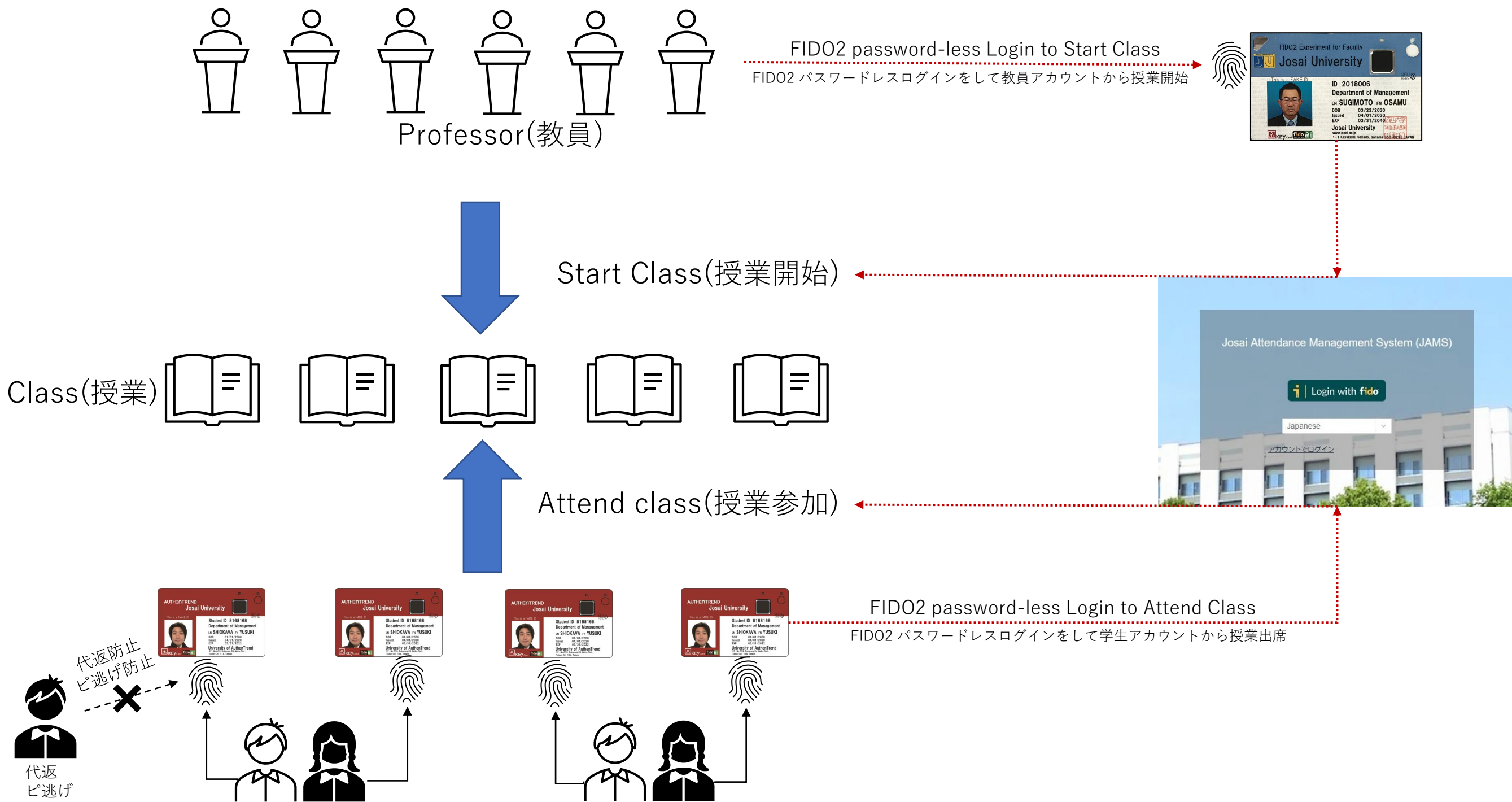


[Login with Account](#)

Josai Attendance Management System(JAMS)



Josai Attendance Management System(JAMS)



Attendance by the student him/her FIDO2 SecurityKey ID card with his/her registered fingerprint.(学生本人による本人の指紋が登録されたFIDO2セキュリティキーで出席)

4.1 JAMS機能（一部）

- 学術機関としては(たぶん)世界初のFIDO2アプリケーション・サーバー(ハイブリッド授業にも対応)
- アドミン・教員・学生の3レベルの権限
- アドミン: キャンパス(学部)、時間割、授業、教員・学生の登録
- 教員: 授業の詳細登録(遅刻限界時間、受講者など)
- 学生: 自身の受講科目への出席・出席状況の閲覧など

4.2 JAMSの運用手順

1.学生の 指紋登録

- Windowsの【設定】→【アカウント】→【サインインオプション】→【セキュリティキー】から教員の端末にて登録
- ベンダー支給のアプリから教員の端末にて登録

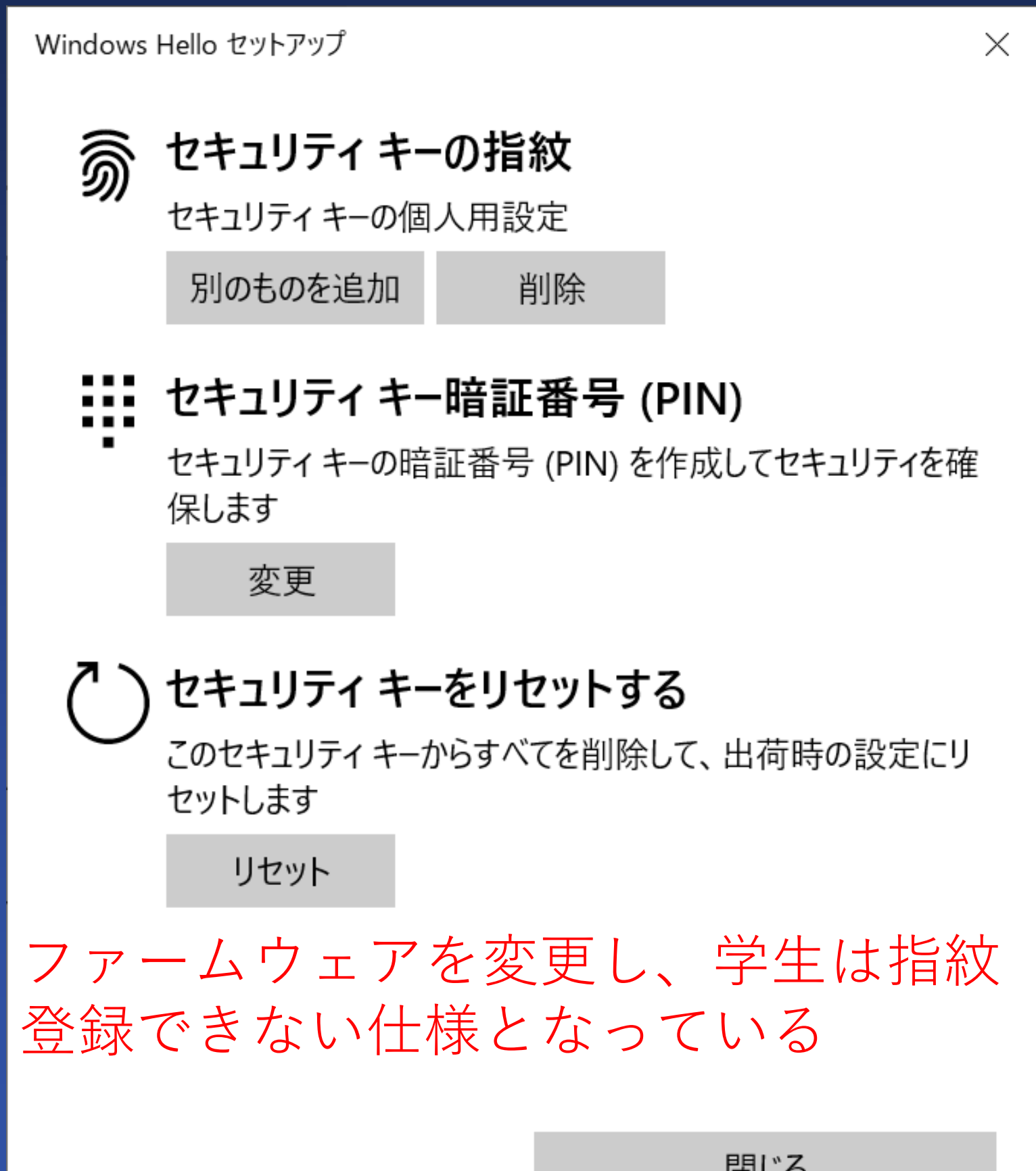
2.JAMSへのセキュ リティキー登録

- 時間割や遅刻・欠席条件・授業を設定・登録
- 学生ごとにセキュリティキー（Campus ID）を登録

3.出席管理

- 教員がJAMS上で授業開始
- 学生が自身の端末もしくは教員の端末にて出席登録

4.2.1 指紋の登録

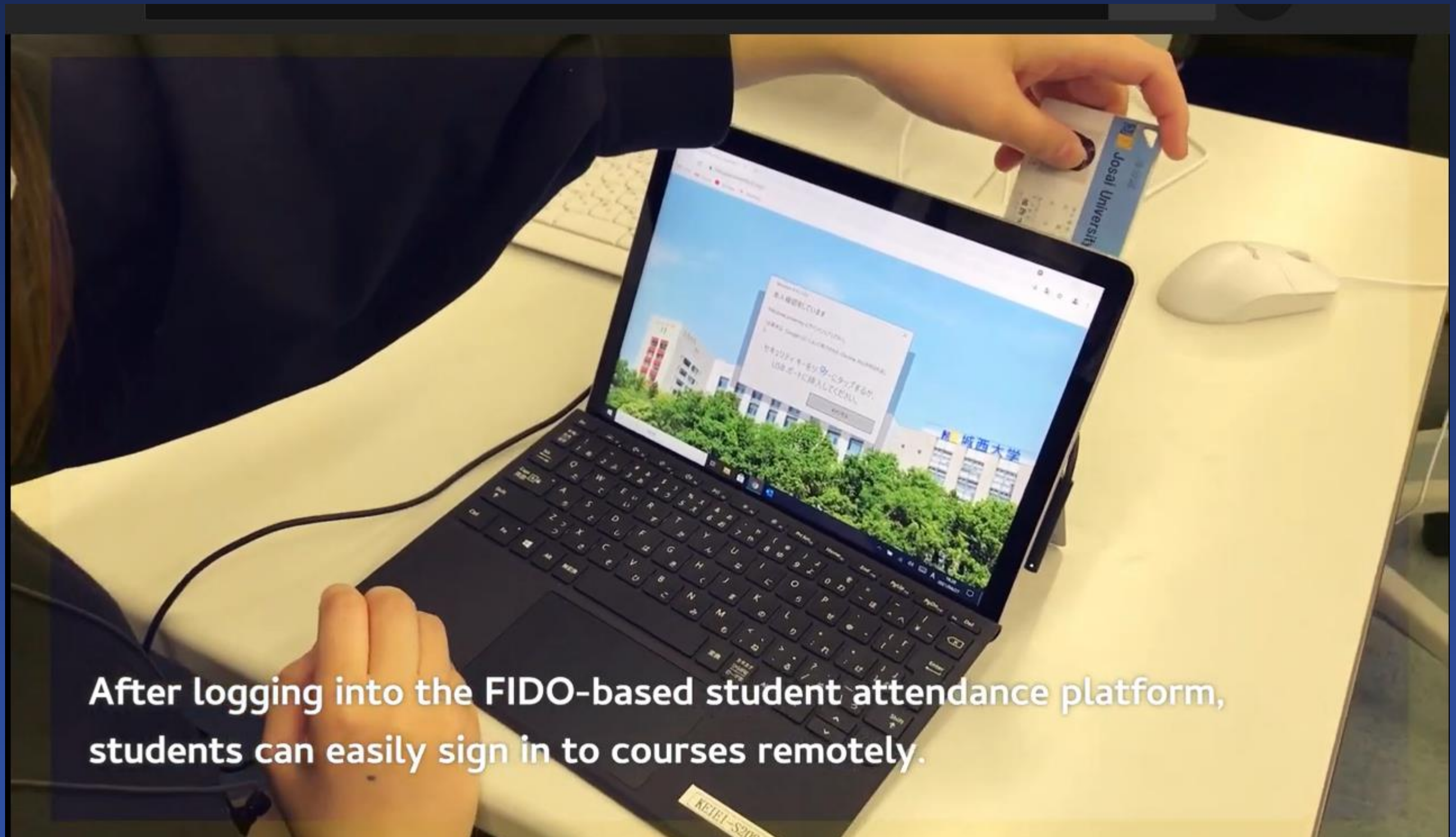


4.2.2 セキュリティキーの登録

The screenshot shows a web browser window with the address bar displaying `https://fido.josai.university/#/user/zm18999`. The page title is "Josai Attendance Management System (JAMS)". The user is logged in as "Osamu Sugimoto" with a "Logout" button. The left sidebar contains navigation links: "Classes", "Users" (highlighted), and "Profile". The main content area shows the breadcrumb "Users > osamu_student" and a "Back to list" button. Under "User Information", the details are: Name: osamu_student, ID: zm18999, Type: Student. Below this are three tabs: "Security Keys" (active), "Login Record", and "Classes". Under the "Security Keys" tab, there is a red-bordered button labeled "Add Security Key". Below the button is a table with the following data:

Security Key Name	Add Time	Actions
pro_student_sam1	2021/04/21 20:03:09	Delete

4.2.3 出席登録



After logging into the FIDO-based student attendance platform, students can easily sign in to courses remotely.

4.3 JAMS:トラブル対応

- 学生がCampus ID(セキュリティキー)を忘れた・紛失した時

⇒事務室やITセンターで予備のセキュリティキーを付与

- 指紋認証ができなくなった時(できない学生含む)

⇒Windowsの設定から指紋を再登録

⇒指紋ではなくPINで対応(75人中1名)

JAMS Demo

<https://www.youtube.com/watch?v=CUn0LJYKftc>



FIDO2 Windows Login Demo

<https://www.youtube.com/watch?v=GpIGtFsczEA>



4.4 JAMSの応用

- 学内開催の検定試験（日商）にも採用予定（12月）
- 面接入試試験への応用を検討中（12月～1月）
⇒次スライド
- 薬剤室等入退室管理への応用を検討中（薬学部）

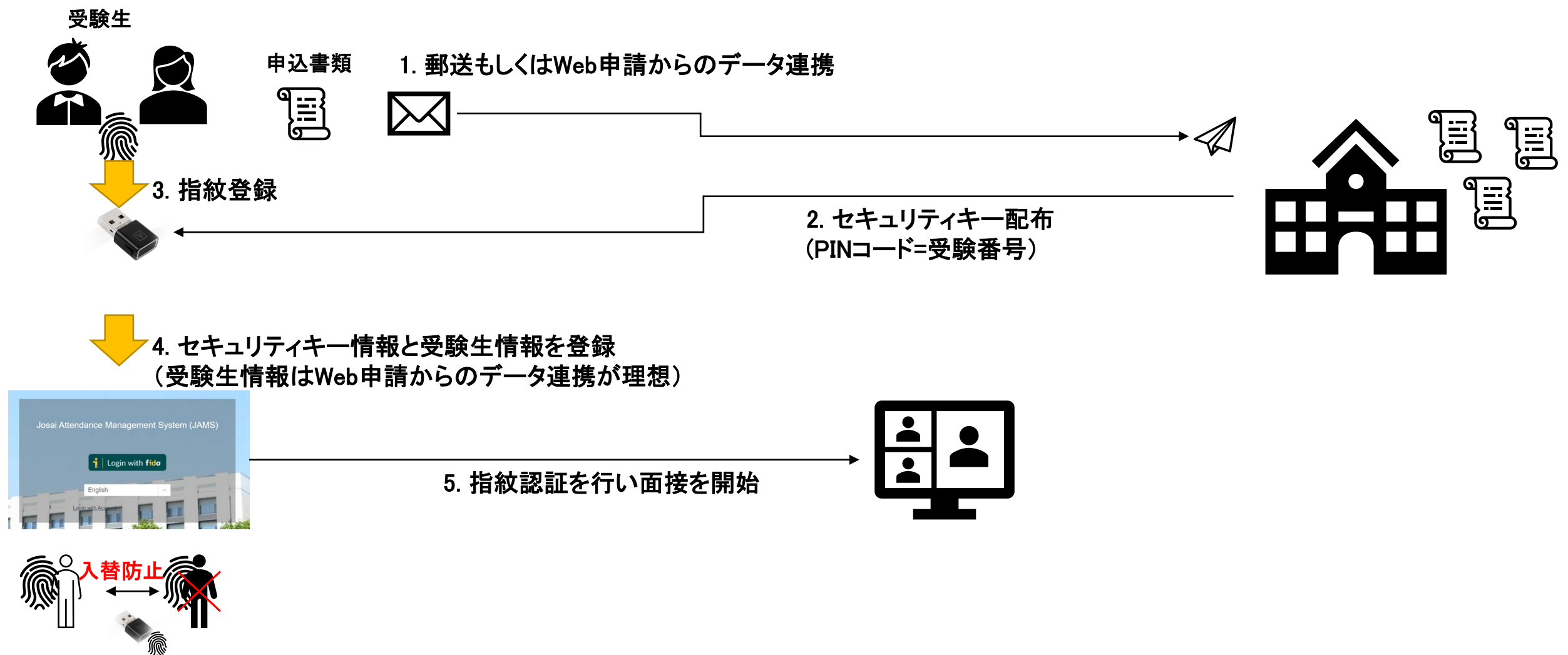
4.4 JAMSの応用

- オンライン面接入試試験



オンライン面接入試プロセス

- * 指定校入試やスポーツ推薦入試を対象とし、高校のPC教室での受験とする
- * あらかじめ本学教職員が先方のPC教室にて動作確認を行う
- * 面接入試なのでカメラと併用となる



5. 結論

- CSIRT (Computer Security Incident Response Team)を中心にMFA対応(理想的にはパスワードレス)をすべき
- 米国では身代金を支払うかどうかで大学の対応が分かれた。日本においても対応を協議しておくべき
- JAMSによって「代返」や「なりすまし」が無くなり、学びの質が上がることで退学者防止につながる可能性がある。現在データを収集中: 次の機会に報告したい
- JAMSは他大学の利用も可能な仕様になっている。利用してみたい大学関係者はぜひご連絡いただきたい

参考文献(抜粋)

- 五味, 大神. (2018). FIDO認証とその技術. IEICE Fundamentals Review, V12#2
- IPA(独立行政法人 情報処理推進機構). (2020). 2019年度情報セキュリティの脅威に対する意識調査.
- JPCERT/CC. (2021). インシデント報告対応レポート
- MagazinePC. (2020年11月18日). 2020's Most Common Passwords Are Laughably Insecure. 参照先: PC Magazine: <https://www.pcmag.com/news/2020s-most-common-passwords-are-laughably-insecure>
- Yahoo! JAPAN. (2019年2月20日). 「安全・安心・便利」FIDO(ファイド)を使ったパスワードレスログインとは. 参照先: 「安全・安心・便利」FIDO(ファイド)を使ったパスワードレスログインとは: <https://about.yahoo.co.jp/info/blog/20190220/fido.html>
- フィッシング対策協議会. (2021年1月). 2021/01 フィッシング報告状況. 参照先: フィッシング対策協議会: <https://www.antiphishing.jp/report/monthly/202101.html>

Thank you!



城西大学