

電子メールシステム

多要素認証 設定は これでOK!

この講習会は情報セキュリティ基礎講習会を兼ねています

上繁義史 (ICT基盤センター 情報基盤デザイン部門長 准教授)

今回のおはなし

1. 導入の背景
2. 多要素認証ってナニモンだ！？
3. 多要素認証の設定
 - ① 共通の操作
 - ② 認証アプリ
 - ③ SMSの利用
 - ④ 電話
 - ⑤ ~~アプリパスワード~~
4. 上手くいったかの確認 & 設定の変更・追加・削除
5. 多要素認証の国外利用での注意
6. お問い合わせはこちら

【訂正とお詫び】

アプリパスワードは「全学必須化」以後でないことが確認されたので、本講習会の内容からは削除いたします。
当方の確認不足によりご迷惑をおかけしまして、誠に申し訳ございません。

1. 導入の背景

あちらこちらでID・パスワードが盗まれています

- 長大IDも例外ではありません
- フィッシング詐欺により窃取されるケースも発生しています

長崎大学としても、セキュリティ強化は喫緊の課題です

- 標的型攻撃メール対策訓練を2年にわたり実施してきました
- 学内ネットワーク更改に伴って、セキュリティ強化対策を実施しています

Microsoftのメールにおいて、現行の基本認証(ID・パスワード認証)が2022年10月以降非推奨となります(2022年1月6日現在)



1. 導入の背景

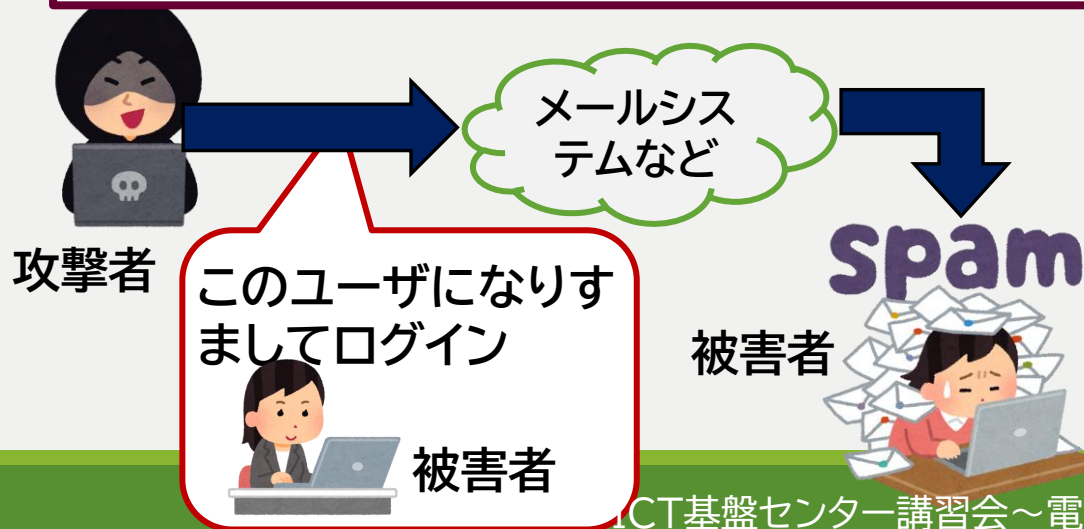
ID・パスワード認証の限界

ID・パスワード認証だけではセキュリティの維持が困難です

- すでに多要素認証が当たり前サービスのサービスも
- Google, Yahoo ほか

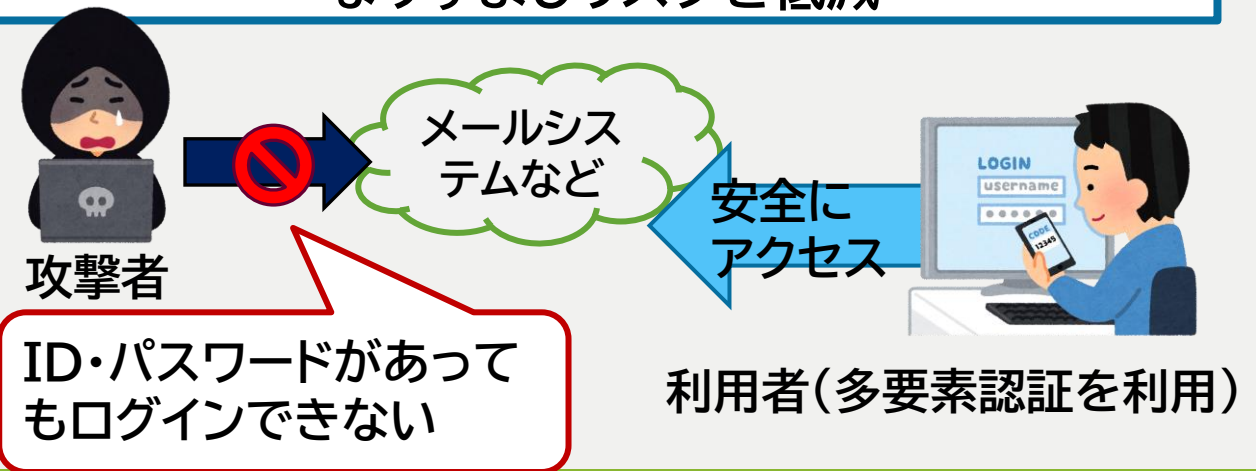
ID・パスワード認証

ID・パスワードを盗めば、なりすましてアクセスが可能(標的型攻撃メールなどを撃つかも)



多要素認証

ID・パスワードに加えてスマートフォンなどで認証
なりすましリスクを低減



2. 多要素認証とはナニモンだ！？

下記の認証方式のうち、**複数の方式を用いた認証**です

- 本学のケースでは、ID・パスワード認証→スマホや電話での認証なので、「2段階認証」とも言えます

記憶に基づく認証

例：ID・パスワード認証

PASSWORD...



所有物による認証

例：ICカード認証



身体的・行動的特徴に基づく認証

例：生体認証



2. 多要素認証とはナニモンだ！？ 本学で導入する多要素認証とは

このような形態です

第1の要素: ID・パスワード



- ① ID・パスワードを入力
ID:
長大ID@ms.nagasaki-u.ac.jp
パスワード
長大IDのパスワード

第2の要素: 専用アプリ, SMS, 電話

パターン1
専用アプリでの
認証



- ② 専用アプリに通知 ③ アプリ上の承認ボタンをタップ

パターン2
SMSでの認証
※フィーチャフォン
でも可



- ② 登録したスマホにSMS通知 ③ SMS上の数値をパソコンに入力

パターン3
電話での認証
※フィーチャフォン,
固定電話でも可



- ② 登録した番号に電話がかかってくる ③ 電話の音声で指示されたボタンを押す

2. 多要素認証とはナニモンだ！？ 全員設定しないといけないのですか？

本学発行のメールアドレスを有する全員に設定いただきます

「私は関係ない」と考えたいお気持ちも分かるのですが・・・

- 「学外からメールを使わない」
 - 利用者本人はそうでも、攻撃者は情け容赦なくアクセスしてきます
- 「見られてもマズい情報は入っていない」
 - 不正ログインされれば、その利用者の名前で不正メールがバンバン出ます
- 「複雑なパスワードを設定している」
 - ある程度安全ですが、標的型攻撃などで窃取されれば無意味です

セキュリティ強化は「全員が行うこと」により有効となります

蟻の一穴から長崎大学全体がサイバー攻撃の危険にさらされます

2. 多要素認証とはナニモンだ！？ 導入のスケジュール

以下の2段階で導入を進めてまいります

周知・設定期間

令和4年1月～

- 各自で多要素認証の設定作業をおねがいします
- **設定作業後も、これまでのID・パスワード認証が利用できます**
- 設定作業のマニュアルや講習会など、ICT基盤センターのHPをご参照ください

全学必須化

令和4年5月以降(予定)

- 多要素認証の**設定が必須**になります
- 周知・設定期間で設定していない方は設定作業が必要です
- **学外からのアクセスでは多要素認証**を時々求められます

3. 多要素認証の設定

本講習会では3つの方式を説明します

- 各方式の設定作業は5分～10分程度で行えます

2種類以上の認証方式の設定を強くお勧めします

- **スマホなどをなくした場合でも、自力で立ち直れます**
 - 電話で認証を行い、認証アプリなどの設定を再度行えばOKです
 - これができないと、利用者は手も足も出せなくなり、「詰んだ状態」になります
 - 詰んでしまったら、ICT基盤センターにて再設定を行う必要があります
- **推奨する認証の組み合わせ**
 - スマートフォンをご利用の方は1の方が良いと思います
 - 1. 認証アプリでの認証 + 電話での認証
 - 2. SMSでの認証 + 電話での認証

3. 多要素認証の設定

全学必須化以降、「ときどき」多要素認証を要求されます

以下のケースでは、第2の要素の認証が省略されます

1. 学内LANに接続して、メールを利用する場合
 - 学内からのアクセスでも、モバイルルータなどを介する場合は「学外扱い」です
2. 学外であっても、直近で多要素認証で認証を行ったパソコンを利用している場合
 - 「ある程度の安全性が担保されている」と判断されるためです

3. 多要素認証の設定

① 共通の操作(1)

1. Microsoft365 のポータルにサインインします

- URL: <http://portal.office.com/>

IDの項には
長大ID@ms.nagasaki
-u.ac.jp
パスワードは
長大IDのパスワード
を入力します

長崎大学 Office 365

組織アカウントを使用してサインインしてください

aa @ms.nagasaki-u.ac.jp

パスワード

サインイン

この画面が表示されたら
「いいえ」をクリックします

Microsoft

aa! @ms.nagasaki-u.ac.jp

サインインの状態を維持しま

これにより、サインインを求められる回数を減らすことができます。

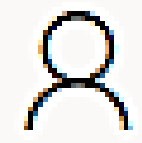
今後このメッセージを表示しない

いいえ

はい

3. 多要素認証の設定

① 共通の操作(2)

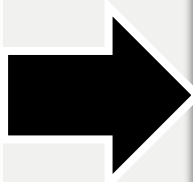
2. 画面右上に表示されているアイコンのうち  (右端)をクリックして、「アカウントを表示」をクリックします

3. マイアカウントの画面にて「セキュリティ情報」をクリックします

ここが最初は  となっています。ここをクリックします

「セキュリティ情報」をクリックします

「アカウントの表示」をクリックします



3. 多要素認証の設定

① 共通の操作(3)

4. この画面が表示されたら、「方法の追加」をクリックしてください
これ以降は認証アプリ, SMS, 電話の設定に進みます

3. 多要素認証の設定

② 認証アプリ (1)

1. 「方法を追加します」のダイアログが表示されたら、「認証アプリ」を選択します
2. スマートフォンにMicrosoft Authenticatorをインストールします

方法を追加します

どの方法を使用しますか?

方法を選択します

認証アプリ

電話

代替の電話

会社電話

✓をクリックして、「認証アプリ」を選びます

Microsoft Authenticator

最初にアプリを取得します

お客様の電話に Microsoft Authenticator アプリをインストールします。今すぐダウンロード

デバイスに Microsoft Authenticator アプリをインストールした後、[次へ] を選択します。

別の認証アプリを使用します

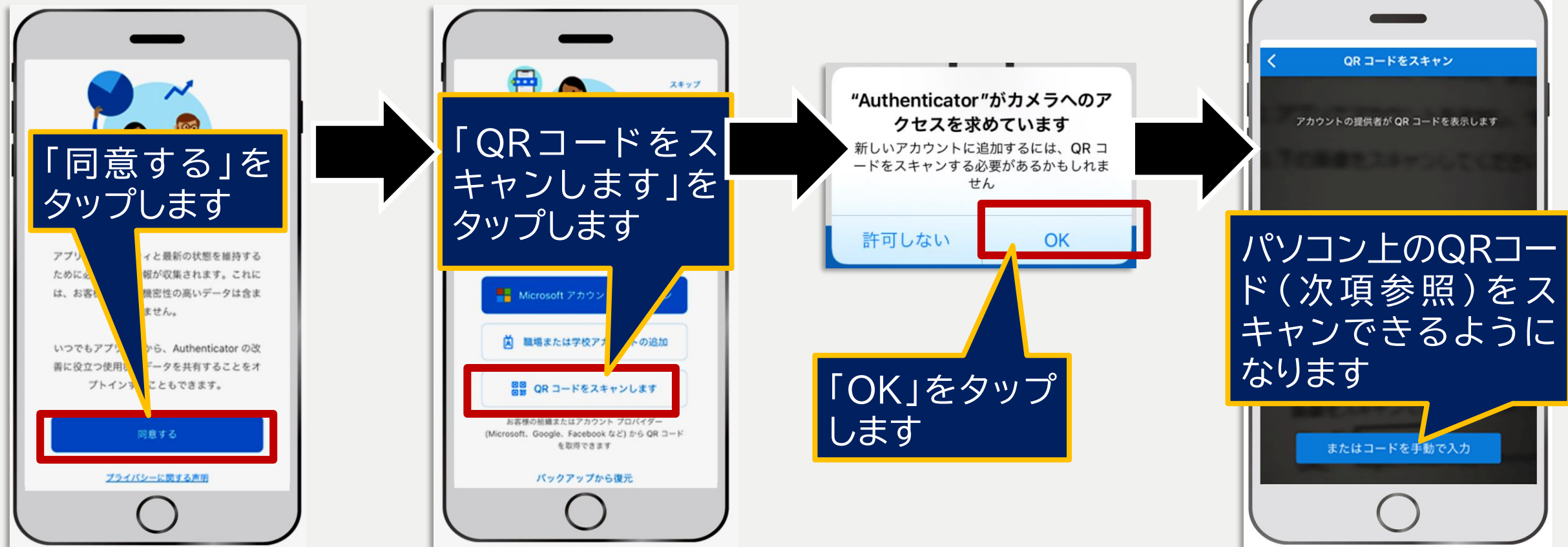
キャンセル 次へ

スマートフォンにMicrosoft Authenticatorをインストールしたら「次へ」をクリックします

3. 多要素認証の設定

② 認証アプリ (3)

3. こちらを参考にスマートフォンを操作してください



3. 多要素認証の設定

② 認証アプリ (4)

4. パソコン画面上的のQRコードをスマートフォンにてスキャンします

Microsoft Authenticator

QRコードをスキャンします

Microsoft Authenticator アプリを使用して QR コードをスキャンします。これにより、Microsoft Authenticator アプリとご自分のアカウントがつながります。

QRコードをスキャンした後、[次へ] を選択します。

こちらのQRコードをスマホでスキャンします

「Authenticator」は通知を送信します。よろしいですか？
通知方法は、テキスト、サウンド、アイコンバッジが利用できる可能性があります。
通知方法は「設定」で設定できます。

許可しない 許可

「許可」をタップします

「Nagasaki University」の項に自分の長大IDが表示されていたら、うまくいっています

Microsoft Authenticator

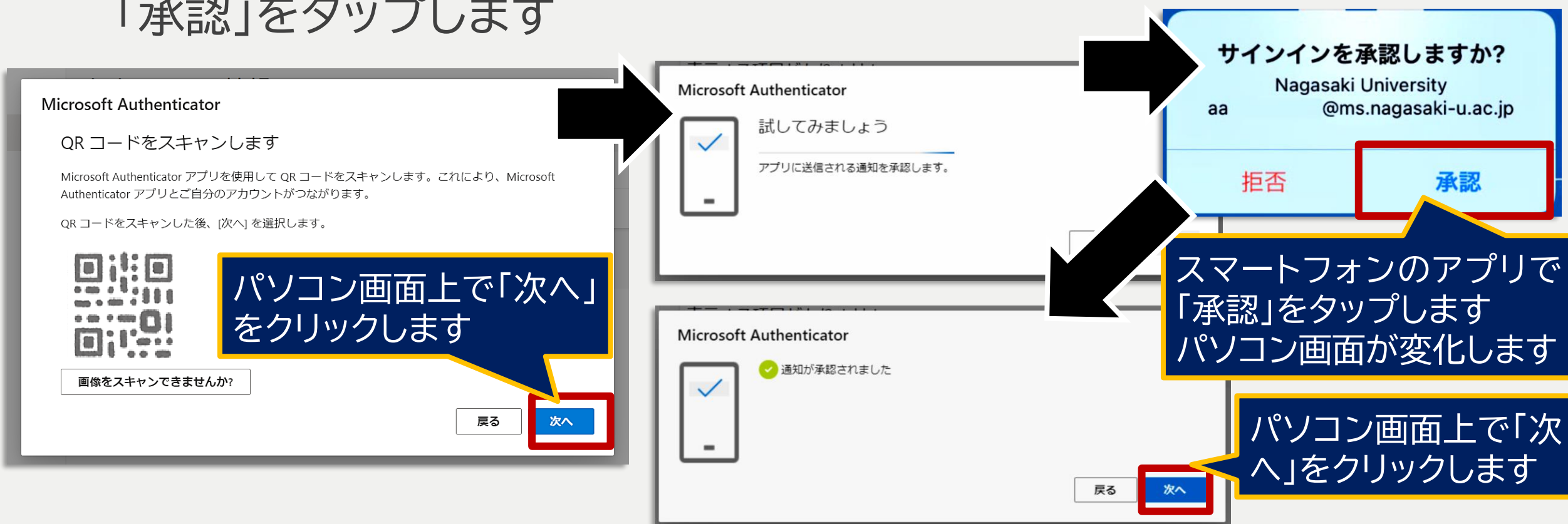
Nagasaki University
aa @ms.nagasaki-u.ac.jp

Authenticator パスワード アドレス

3. 多要素認証の設定

② 認証アプリ (5)

5. パソコン画面で「次へ」をクリックしてから、スマートフォンのアプリで「承認」をタップします



3. 多要素認証の設定

② 認証アプリ（6）

6. パソコンの画面上でこちらのように表示されたら設定完了です

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方法です。

[既定のサインイン方法を設定します](#)

+ 方法の追加

Microsoft Authenticator 削除

Microsoft Authenticator アプリが正常に登録されました

Mon, 20 Dec 2021 01:04:32 GMT

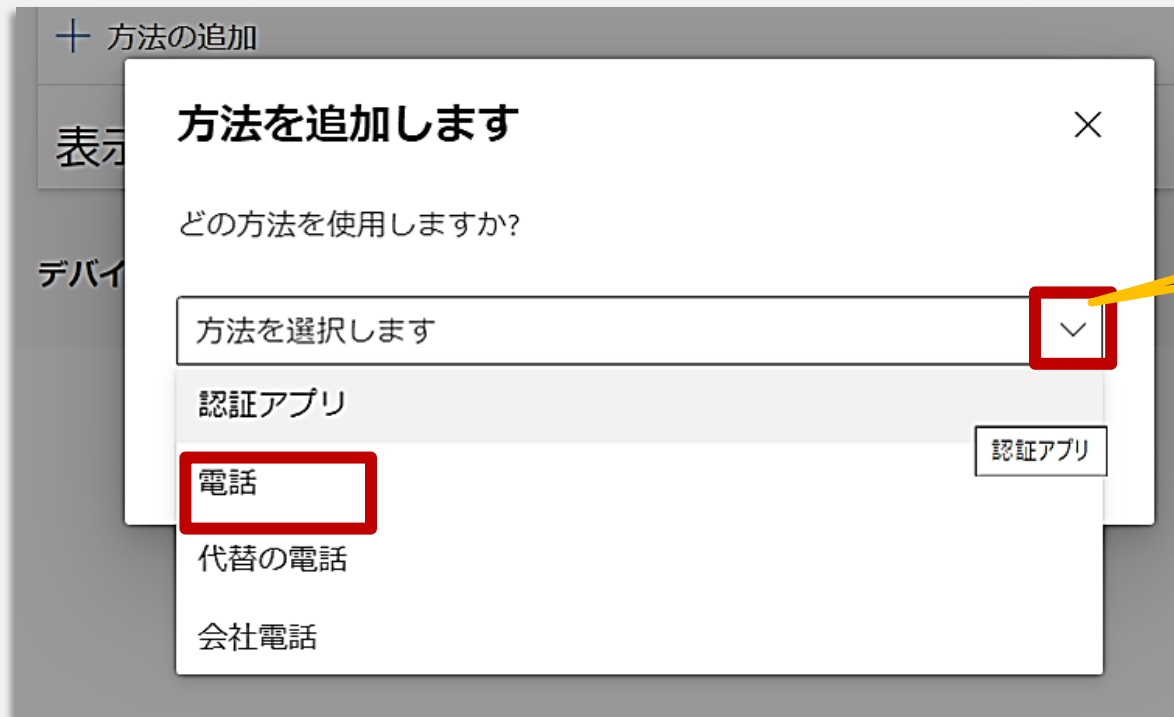
【注意】

携帯電話を紛失したり、認証アプリを移行せずに機種変更したりした場合、この画面からMicrosoft Authenticatorの設定を削除して、再度設定を行ってください

3. 多要素認証の設定

③ SMSを利用 (1)

1. 「方法を追加します」のダイアログが表示されたら、「電話」を選択します



▼ をクリックして、「電話」
を選びます

3. 多要素認証の設定

③ SMSを利用 (2)

2. 設定画面にてご自身の携帯電話番号を入力します

3. 「コードをSMS送信する」にチェックを入れ「次へ」をクリックします

「日本(+81)」を選択します

「コードをSMS送信する」に
チェックを入れます

The screenshot shows a registration form titled "電話" (Phone). It contains the following elements:

- A dropdown menu for country selection, currently set to "日本 (+81)".
- A text input field for the phone number, containing "09012345678".
- Two radio button options: "コードをSMS送信する" (selected) and "電話する".
- Buttons for "キャンセル" (Cancel) and "次へ" (Next).

Red boxes highlight the country dropdown, the phone number field, the selected radio button, and the "次へ" button. Yellow callout boxes provide instructions for each of these elements.

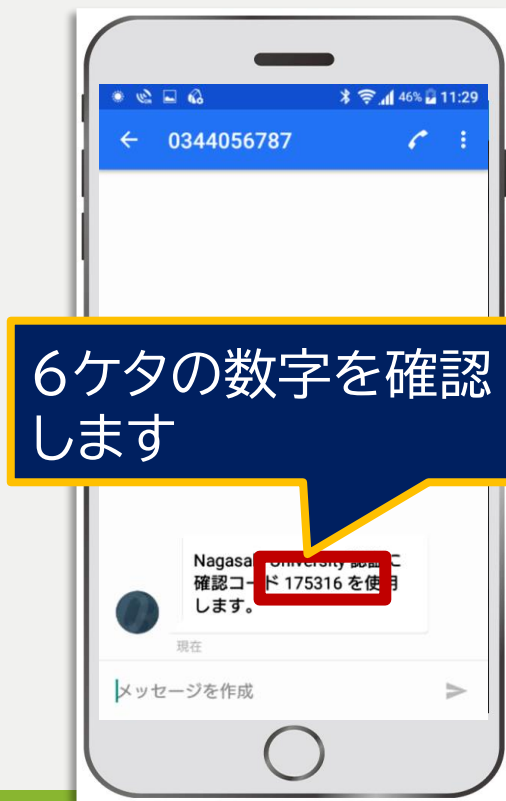
電話番号をハイフンなしで入力
します
(スマートフォン, フィーチャー
フォンのいずれもOKです)

「次へ」をクリックします

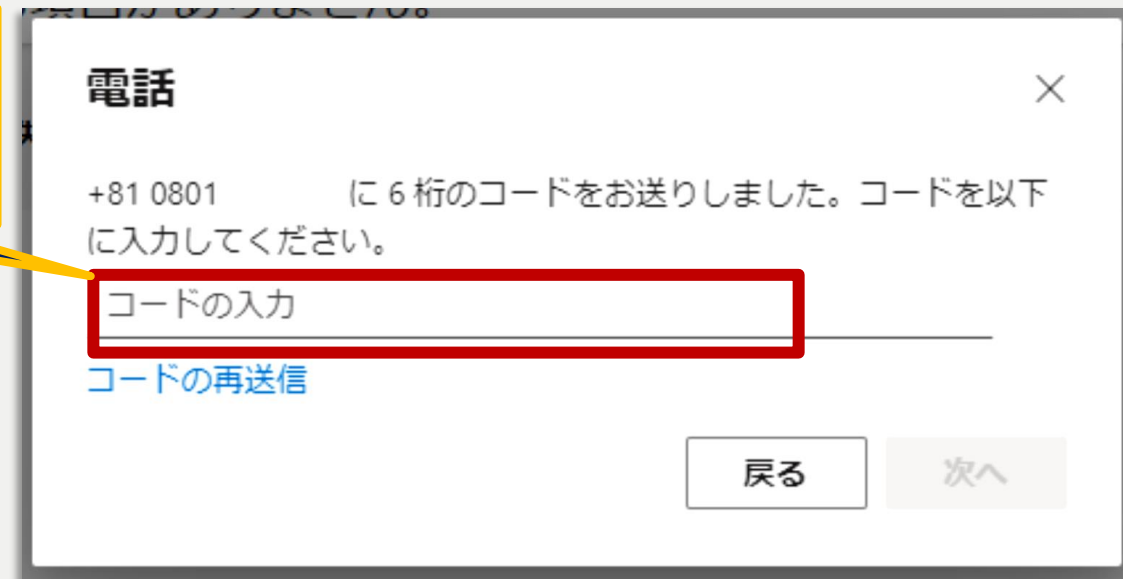
3. 多要素認証の設定

③ SMSを利用 (3)

4. 指定した携帯電話にSMSが届きますので、そちらに記載された6ケタのコードをパソコンの画面に入力します



6ケタの数字をパソコンの画面に入力します



3. 多要素認証の設定

③ SMSを利用 (4)

5. パソコンの画面上に左下のように表示されたら、「完了」をクリックしてください

The image shows a two-part interface. On the left is a notification window titled '電話' (Phone) with a green checkmark and the text 'SMS が検証されました。お使いの電話が正常に登録されました。' (SMS has been verified. Your phone has been registered normally.) A blue button labeled '完了' (Completed) is highlighted with a red box. A large black arrow points from this button to the right. On the right is the 'セキュリティ情報' (Security Information) page. It has a sub-header '既定のサインイン方法を設定します' (Set your default sign-in method). Below this is a section '+ 方法の追加' (Add method) containing a list item for '電話' (Phone) with the number '+81 0801'. The '電話' text is highlighted with a red box. A blue callout bubble points to this box with the text '「電話」が追加されていることがわかります' (You can see that 'Phone' has been added). At the bottom of the page, there is a note: 'デバイスを紛失した場合 すべてサインアウトしてください' (If you lose your device, sign out of everything).

「完了」をクリックします

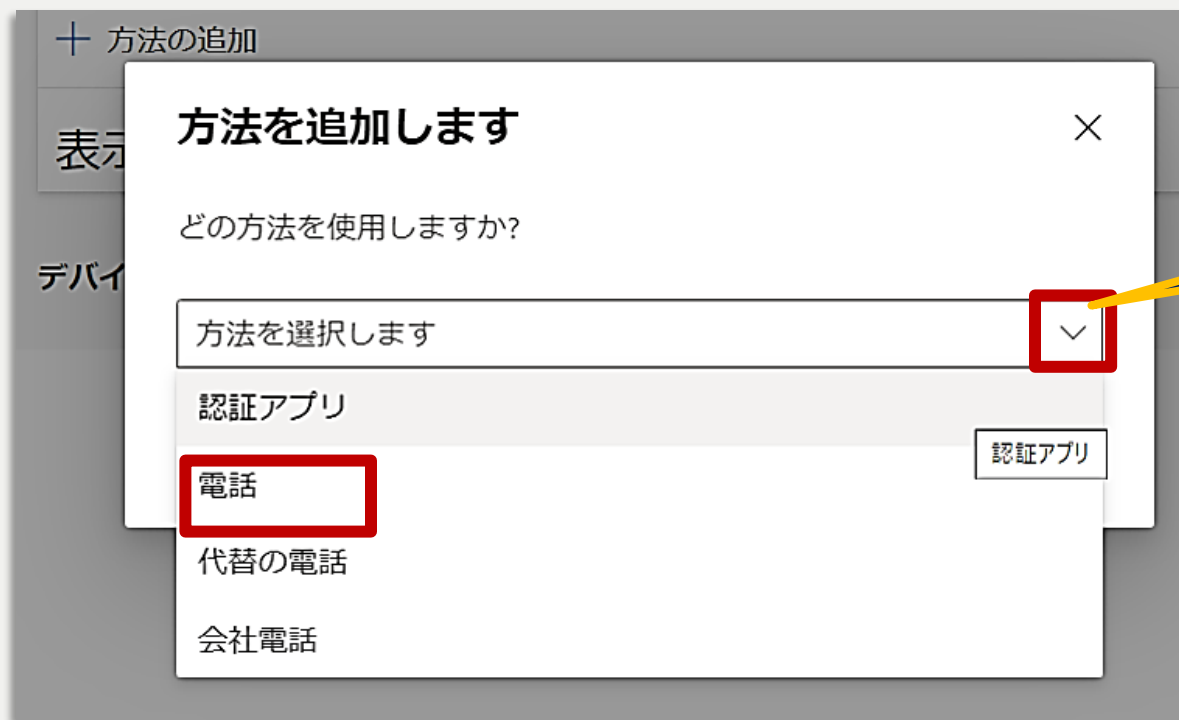
【注意】

携帯電話の番号が変わったときは、この画面から電話の設定を削除して、再度設定を行ってください

3. 多要素認証の設定

④ 電話 (1)

1. 「方法を追加します」のダイアログが表示されたら、「電話」を選択します



▼ をクリックして、「電話」を選びます

3. 多要素認証の設定

④ 電話 (2)

2. 設定画面にてご自身の電話番号(固定電話でもOK)を入力します

3. 「電話する」にチェックを入れ「次へ」をクリックします

「日本(+81)」を選択します

「電話する」にチェックを入れます

電話はご自身のスマートフォン・職場など2つ以上の登録をおすすめします！

電話

電話で呼び出しに応答するか、携帯ショートメール (SMS) によるコードの送信により、本人確認ができます。

どの電話番号を使用しますか？

日本 (+81) 095819

コードをSMS送信する

電話する

メッセージとデータの通信料が適用される場合があります。[次へ]を選択すると、次に同意したことになります: [サービス使用条件](#) および [プライバシーとCookieに関する声明](#)。

キャンセル 次へ

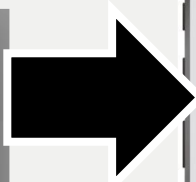
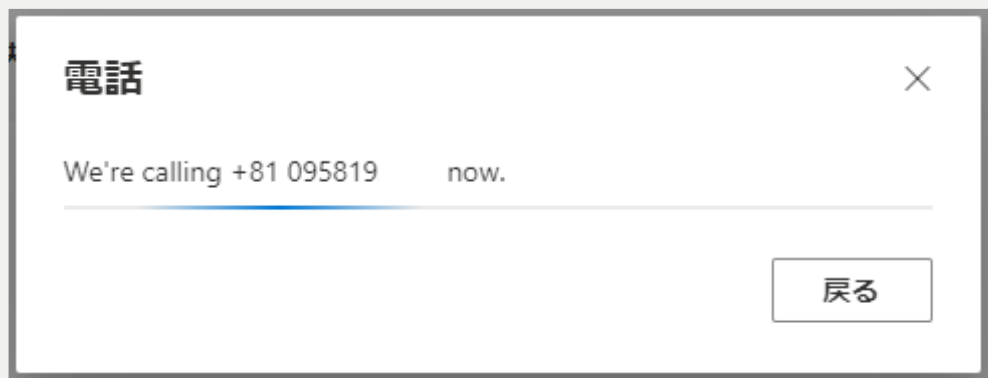
電話番号をハイフンなしで入力します
(スマートフォン、フィーチャーフォン、固定電話のいずれもOKです)

「次へ」をクリックします

3. 多要素認証の設定

④ 電話 (3)

1. 設定した番号に電話がかかってきますので、電話の指示にしたがって#を押します



固定電話の場合、トーン信号を送出できる必要があります
(内線電話など、別途電話機の操作が必要となる場合があります)

3. 多要素認証の設定

④ 電話 (4)

5. パソコンの画面上に左下のように表示されたら、「完了」をクリックしてください

The image shows a computer screen with a security information page. On the left, a white dialog box titled '電話' (Phone) is open, displaying a green checkmark and the text '通話に応答しました。お使いの電話が正常に登録されました。' (Call answered. Your phone is registered normally). A blue button labeled '完了' (Done) is highlighted with a red box. A blue callout bubble points to this button with the text '「完了」をクリックします' (Click 'Done'). A black arrow points from the dialog box to the main page. The main page is titled 'セキュリティ情報' (Security Information) and contains the text 'これは、ご自分のアカウントへのサインインやパスワードリセットに使用される電話番号です。既定のサインイン方法を設定します' (This is the phone number used for signing in to your account or resetting your password. Set your default sign-in method). Below this is a section '+ 方法の追加' (+ Add method) with a red box around the '電話' (Phone) icon. A blue callout bubble points to this icon with the text '「電話」が追加されていることがわかります' (You can see that 'Phone' has been added). Below the phone icon, the number '+81 0801' is displayed, along with '変更' (Change) and '削除' (Delete) buttons. At the bottom of the page, there is a note: 'デバイスを紛失した場合 すべてサインアウトしてください' (If you lose your device, sign out of everything).

「完了」をクリックします

「電話」が追加されていることがわかります

【注意】

携帯電話の番号が変わったときは、この画面から電話の設定を削除して、再度設定を行ってください

3. 多要素認証の設定

アプリパスワードについて

アプリパスワードはご利用のメールソフトが多要素認証に対応していない場合に設定するものです

- 多要素認証(①～④)が可能な方は設定しなくてかまいません
- 未対応ソフトの例:
 - macOS/iOS標準のメールソフトをExchange以外(IMAP/POPなど)で利用
 - OAuth2に未対応のメールソフト

こちらは**全学必須化の後に設定可能となります**

4. 上手くいったかの確認 & 設定の変更・追加・削除

1. Microsoft365 のポータルにサインインします

- URL: <http://portal.office.com/>

IDの項には
長大ID@ms.nagasaki
-u.ac.jp
パスワードは
長大IDのパスワード
を入力します

長崎大学 Office 365

組織アカウントを使用してサインインしてください

aa97225855@ms.nagasaki-u.ac.jp

パスワード

サインイン

この画面が表示されたら
「いいえ」をクリックします

Microsoft

aa97225855@ms.nagasaki-u.ac.jp

サインインの状態を維持しま

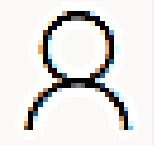
これにより、サインインを求められる回数を減らすことができます。

今後このメッセージを表示しない

いいえ

はい

4. 上手くいったかの確認 & 設定の変更・追加・削除

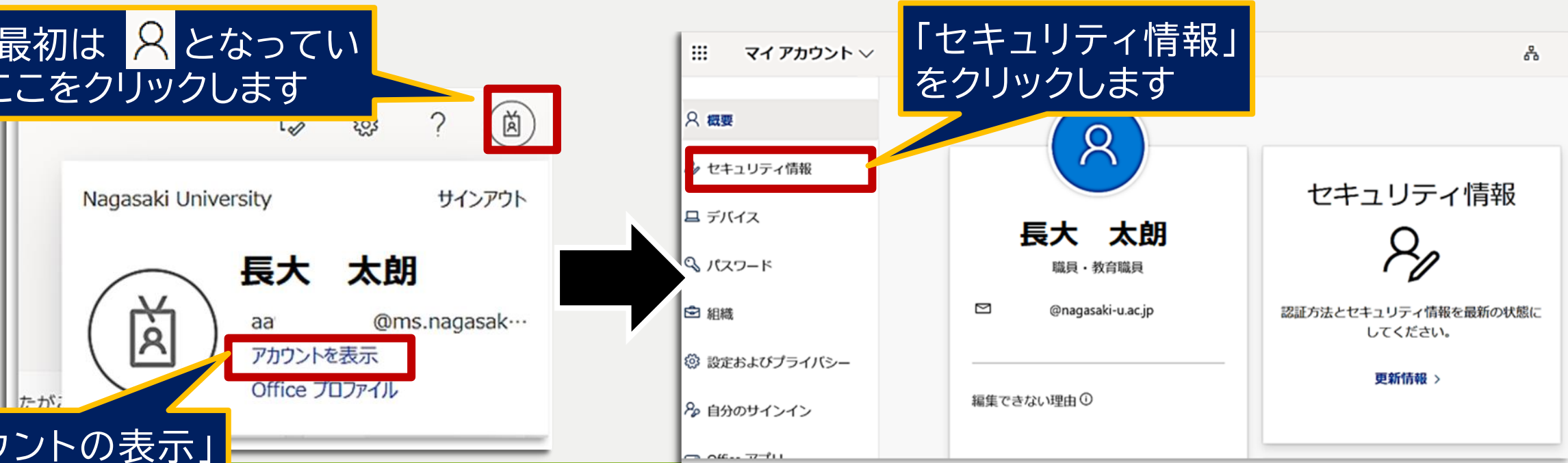
2. 画面右上に表示されているアイコンのうち  (右端)をクリックして、「アカウントを表示」をクリックします

3. マイアカウントの画面にて「セキュリティ情報」をクリックします

ここが最初は  となっています。ここをクリックします

「セキュリティ情報」をクリックします

「アカウントの表示」をクリックします



4. 上手くいったかの確認 & 設定の変更・追加・削除

上手くいったかの確認

1. 「サインイン要求を承認」と表示されますので、登録した承認方法でサインインしてください
 - 認証アプリの場合、スマートフォン上で承認します
 - 電話, SMSの場合は「Microsoft Authenticator アプリを現在使用できません」をクリックしてください
 - すると右下のような表示になります
 - 確認方法として表示されるのは、既にご自身で登録したもののみとなります
 - 図の例では、認証アプリ, SMS, 電話のすべてを登録しております
2. サインインが成功したら設定が上手くいったことが分かります



4. 上手くいったかの確認 & 設定の変更・追加・削除 設定の変更

認証方法を変更は以下の画面から行うことができます

The screenshot shows the 'Security Information' page in a Microsoft account interface. A callout box points to the 'Change' button for the current sign-in method. Another callout box points to a dialog box for selecting a new sign-in method.

自分のサインイン

概要

セキュリティ情報

組織

デバイス

プライバシー

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方

既定のサインイン方法: Microsoft Authenticator - 通知 **変更**

+ 方法の追加

電話	+81 7012345678	変更	削除
会社電話	+81 0951234567	変更	削除
アプリパスワード	AppPasswd		削除
Microsoft Authenticator	※スマホの名称等		削除

既定の方法を変更しま

どの方法を使用してサインインし ますか?

- Microsoft Authenticator - 通知
- 電話 - 通話 +81 095 1234567
- 電話 - 通話 +81 7012345678
- 電話 - テキスト +81 7012345678
- Microsoft Authenticator - 通知
- Authenticator アプリまたはハードウェア トークン - コード

「変更」をクリックします

認証方法を選択します

4. 上手くいったかの確認 & 設定の変更・追加・削除 設定の追加・削除

認証方法を追加や削除も以下の画面から行うことができます

The screenshot shows the 'Security Information' page in a Microsoft account interface. The left sidebar contains navigation links: '自分のサインイン', '概要', 'セキュリティ情報', '組織', 'デバイス', and 'プライバシー'. The main content area is titled 'セキュリティ情報' and includes a sub-header '既定のサインイン方法: Microsoft Authenticator' with a link to '通知 変更'. Below this is a table of authentication methods. A red box highlights the '+ 方法の追加' button. Another red box highlights the '削除' buttons for each method in the table. Two callout boxes provide instructions: one for adding a method and one for removing a method.

自分のサインイン

概要

セキュリティ情報

組織

デバイス

プライバシー

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの

既定のサインイン方法: Microsoft Authenticator [通知 変更](#)

+ 方法の追加

電話	+81 7012345678	変更	削除
会社電話	+81 0951234567	変更	削除
アプリ パスワード	AppPasswd		削除
Microsoft Authenticator	※スマホの名称等		削除

認証方法を追加する場合には「方法の追加」をクリックします
以後の操作方法は「3. 多要素認証の設定」をご覧ください

認証方法を削除する場合には「削除」をクリックします

5. 多要素認証の国外利用での注意

「アタリマエだ！」とお叱りを受けるかもしれませんが・・・

多要素認証の設定や利用にお金はかかりません

ですが、国内での話です

国際ローミングの場合、別途通信料金が発生する場合があります

- 海外にてSMSや電話音声で認証するケースでは要注意かも

携帯電話の契約内容をご確認ください



携帯電話を使って電話音声・ショートメッセージ(SMS)で認証している方で、国外での音声通話やショートメッセージの受信ができない場合は、現地で利用可能な電話・SIMカードをレンタルしておき、「代替の電話」として登録しておくなどの対応が必要となります

6. お問い合わせはこちら

ご清聴ありがとうございました



設定に困ったら、まずはWebをご参照ください

- ICT基盤センター特設ページ「Microsoft365多要素認証の有効化について」
 - http://www.cc.nagasaki-u.ac.jp/service/info_outlet/microsoft365-authentication_01.html

解決が困難な場合、メールでお問い合わせください

- ICT基盤センター事務室
 - メール portal@ml.nagasaki-u.ac.jp