スーパーコンピュータ「富岳」
スタートアップガイド 1.11 版

理化学研究所計算科学研究センター

2025 年 02 月 25 日

目次:

第 1 章

はじめに

1.1 本資料の目的

本書ではアカウント登録が完了した後に、スーパーコンピュータ「富岳」を使うために必要な設定について説明しています。

本書にしたがってクライアントなどの初期設定を行ってください。初期設定が終わりましたら、富岳ウェブサイト (https://www.fugaku.r-ccs.riken.jp/) にアクセスし「利用手引書」を参照ください。

1.2 本書で使用する表記

- コマンド実行において、操作対象の利用者端末、ログインノードを、プロンプトで表現しています。

プロンプト	操作対象
[terminal]	利用者の端末でコマンドを実行することを意味します
[_LNlogin]	ログインノード（共通）でコマンドを実行することを意味します

- ホームディレクトリは ~（チルダ）で表現しています。

1.3 商標について

1.4 更新履歴

本書の更新箇所を示します。

1.11 版 2025 年 2 月 25 日

- 「2.2.3 Chrome への証明書のインストール（Windows）」に証明書マネージャーの画面例を追加しました。
- 「2.4.3 アクセス方法」に注釈を追加しました。

1.10 版 2024 年 9 月 4 日

- 「2.3 富岳ウェブサイトへの接続手順」に Mac のキーチェーン使用時のパスワードの説明を追加しました。

1.09 版 2023 年 12 月 12 日

- https://www.fugaku.r-ccs.riken.jp/ の呼称を「利用者ポータル」から「富岳ウェブサイト」に変更しました

1.08 版 2023 年 3 月 22 日

- 「2.4.1 鍵ペア（秘密鍵／公開鍵）の作成」の puttygen の画面例を更新しました。
- 「2.4.3 アクセス方法」の PuTTY の画面例を更新しました。

1.07 版 2023 年 3 月 15 日

- 「2.4.1. 鍵ペア（秘密鍵／公開鍵）の作成」に RSA 鍵使用時の参照ページを追加しました。

1.06 版 2022 年 6 月 22 日

- 「2.1 概要」に流れ図を追加しました

1.05 版 2022 年 6 月 8 日

- 「2.4.1 鍵ペア（秘密鍵／公開鍵）の作成」に RSA の使用を禁止する予定であることを記載しました

1.04 版 2022 年 5 月 23 日

- 「2.4 ログイン」にパーミッションに関する注釈を追加しました

1.03 版 2022 年 4 月 6 日

- 「2.3 富岳ウェブサイトへの接続手順」に Chrome@Mac 使用時の注釈を追加しました

1.02 版 2022 年 4 月 3 日

- 「2.4.6. 「富岳」運用情報のメール配信」を追加しました

1.01 版 2021 年 4 月 15 日

- 「2.2. クライアント証明書のインストール」の「クライアント証明書のパスフレーズ」の説明を更新しました

1.00 版 2021 年 3 月 4 日

- ログインノードのホスト名を変更しました
- 「2.2.3 Chrome への証明書のインストール（Windows）」の手順 1 を更新しました
- 「2.4.2 公開鍵登録」の手順を更新しました

0.2 版 2020 年 11 月 27 日

- 「更新履歴」を追加しました
- 「2.3. 富岳ウェブサイトへの接続手順」の注釈を更新しました
- 「2.4.2. 公開鍵登録」の手順 5 を更新しました

第 2 章

システム利用

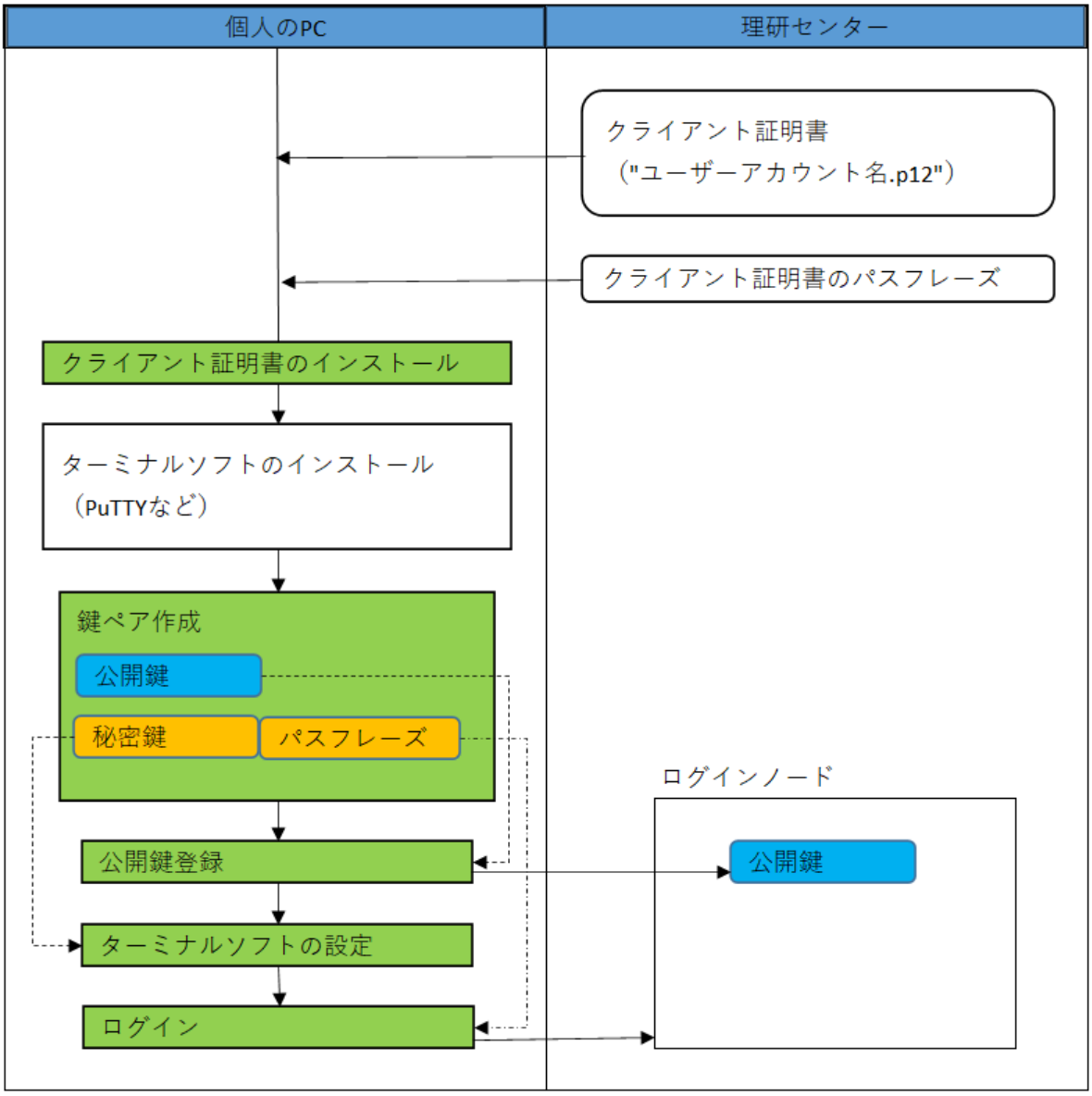
スーパーコンピュータ「富岳」の利用にあたり、システムへのログインなど、基本事項について手順を示します。

2.1 概要

スーパーコンピュータ「富岳」を利用するためには、富岳ウェブサイトやログインノードを利用します。

ここでは、富岳ウェブサイト利用時に必要となるクライアント証明書のインストール方法、ログインノードの接続に必要となる SSH 公開鍵の作成および登録方法を示します。

設定の流れを次に示します。



項目	参照先
クライアント証明書のインストール	クライアント証明書のインストール
鍵ペア作成	鍵ペア（秘密鍵／公開鍵）の作成
公開鍵登録	公開鍵登録
ターミナルソフトの設定	ログインノード（*PuTTY*）
ログイン	ログインノード（*PuTTY*）

2.2 クライアント証明書のインストール

クライアント証明書は富岳ウェブサイトをアクセスする時に使用します。富岳ウェブサイトをアクセスするブラウザにインストールしてください。

スーパーコンピュータ「富岳」の富岳ウェブサイトにアクセスするために必要なクライアント証明書のインストール方法を示します。

クライアント証明書をインストールする前に次の二つを用意してください。

- クライアント証明書:"ユーザーアカウント名.p12"ファイル
- クライアント証明書のパスフレーズ

クライアント証明書 アカウント発行が完了すると申請時に記載したメールアドレス宛てにクライアント証明書が電子メールで送付されます。電子メールに添付されている"ローカルアカウント名.p12"ファイルを、クライアント証明書をインストールする機器（パソコンなど）に保存してください。"ローカルアカウント名.p12"ファイルには、クライアントの秘密鍵、クライアント証明書（公開鍵）、クライアント証明書発行局のルート証明書が含まれています。

クライアント証明書のパスフレーズ パスフレーズは、クライアント証明書とは別に、書面または PDF ファイルで送付されます。パスフレーズはクライアント証明書をインストールする時に必要となります。安全な場所に保管してください。

ここでは、富岳ウェブサイトの推奨ブラウザにクライアント証明書を登録する手続きについて説明します。

注釈: 指定のブラウザと異なるものを利用する場合は、自身でブラウザの証明書管理方法を確認し、利用するブラウザにクライアント証明書のインストールを行ってください。

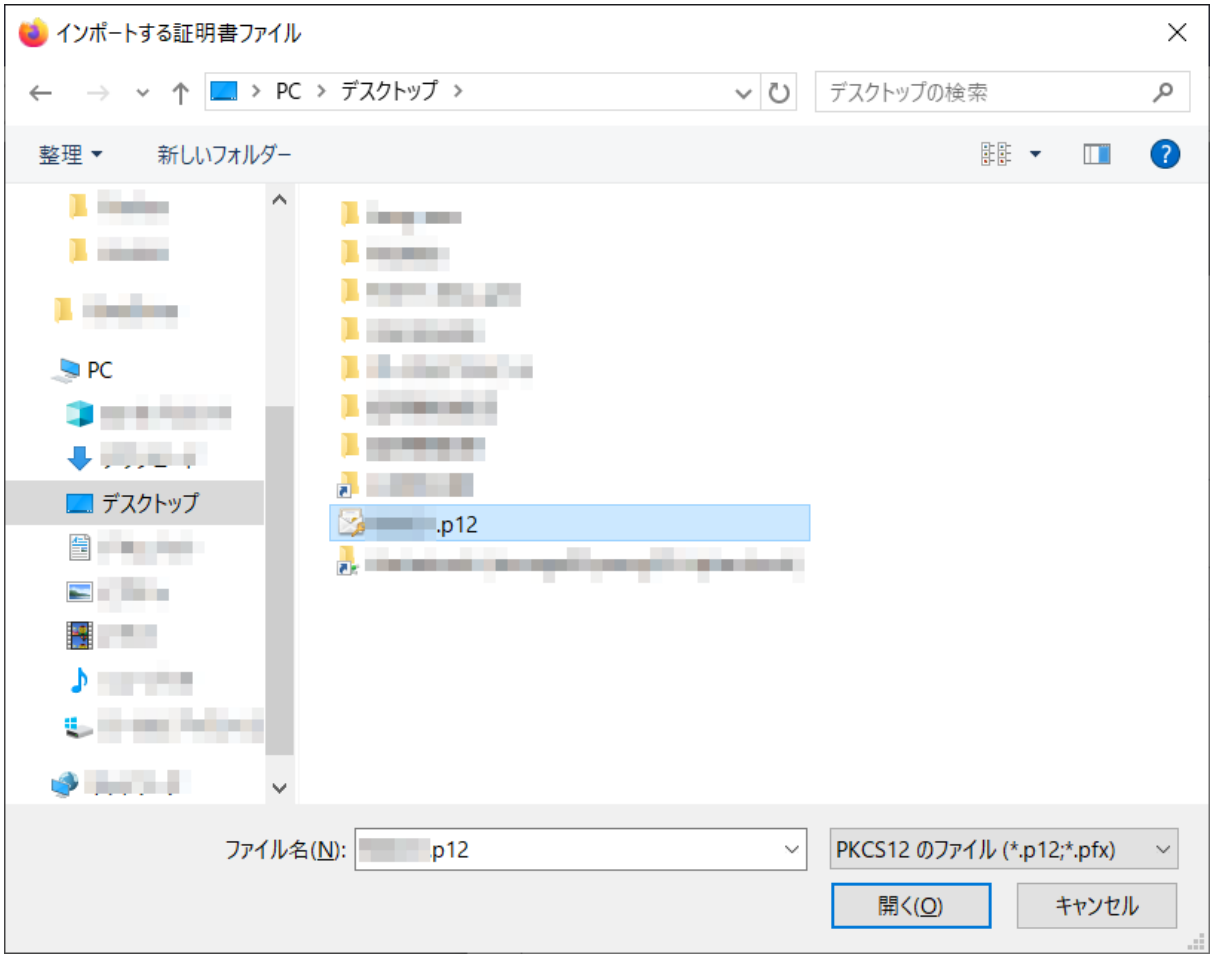
2.2.1 Firefox への証明書のインストール（Windows）

Microsoft Windows で Firefox を利用する場合のインストール手順を示します。Firefox のバージョンによって画面に差異がある場合があります。画面が異なる場合は Firefox の情報を確認して作業を実施してください。

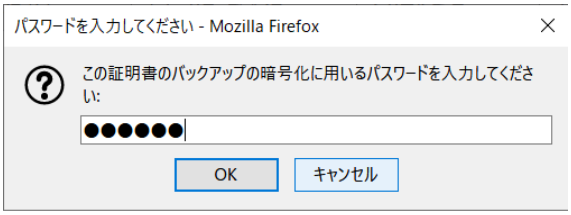
1. Firefox を起動し、*[**オプション**]* の画面を開きます。*[**プライバシーとセキュリティ**]* の *[**証明書を表示**]* をクリックします。

2. 証明書マネージャが起動したら、*[**あなたの証明書**]* を選択して、*[**インポート...**]* をクリックします。

3. クライアント証明書:"ローカルアカウント名.p12"ファイルを選択し *[開く]* をクリックします。

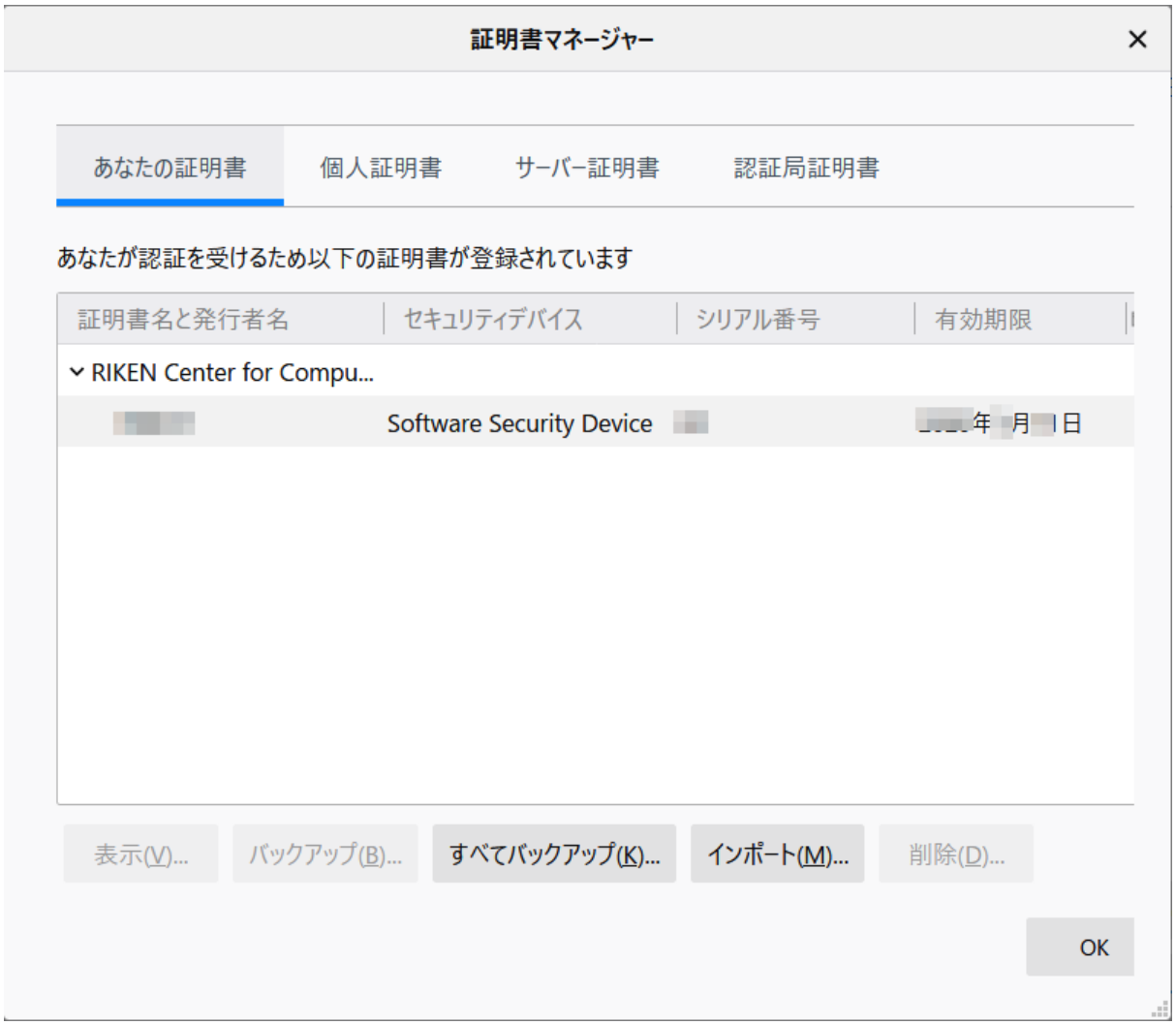


4. クライアント証明書のパスフレーズを **パスワード欄**に入力し、*[OK]* をクリックします。

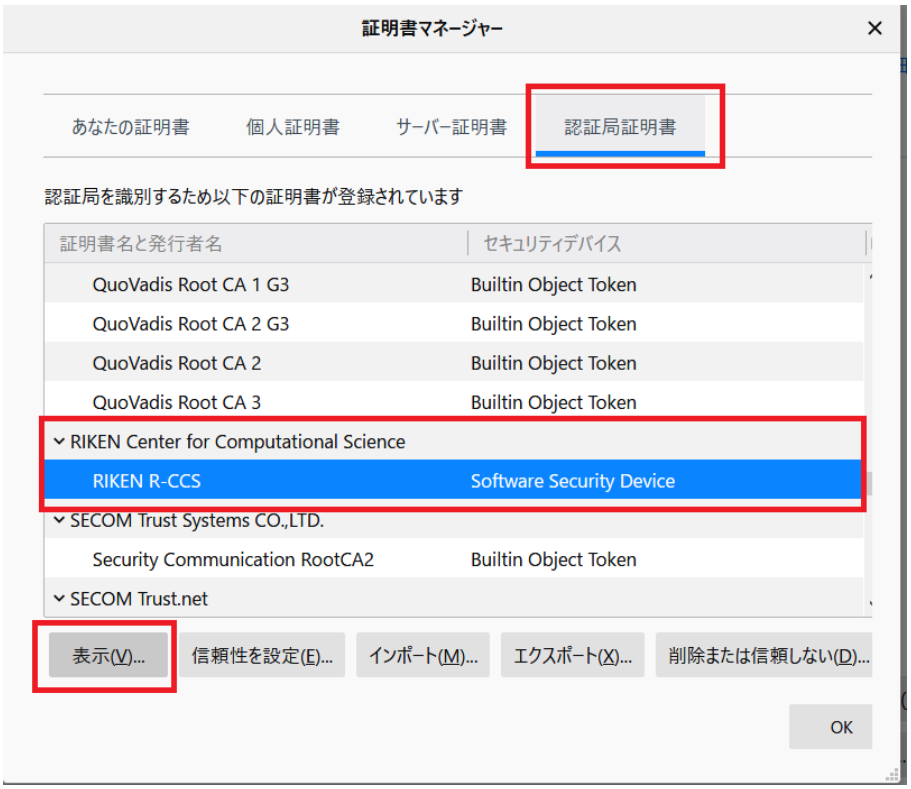


> **注意:** クライアント証明書のパスフレーズが正しくない場合エラーが表示され、次の画面に進めません。

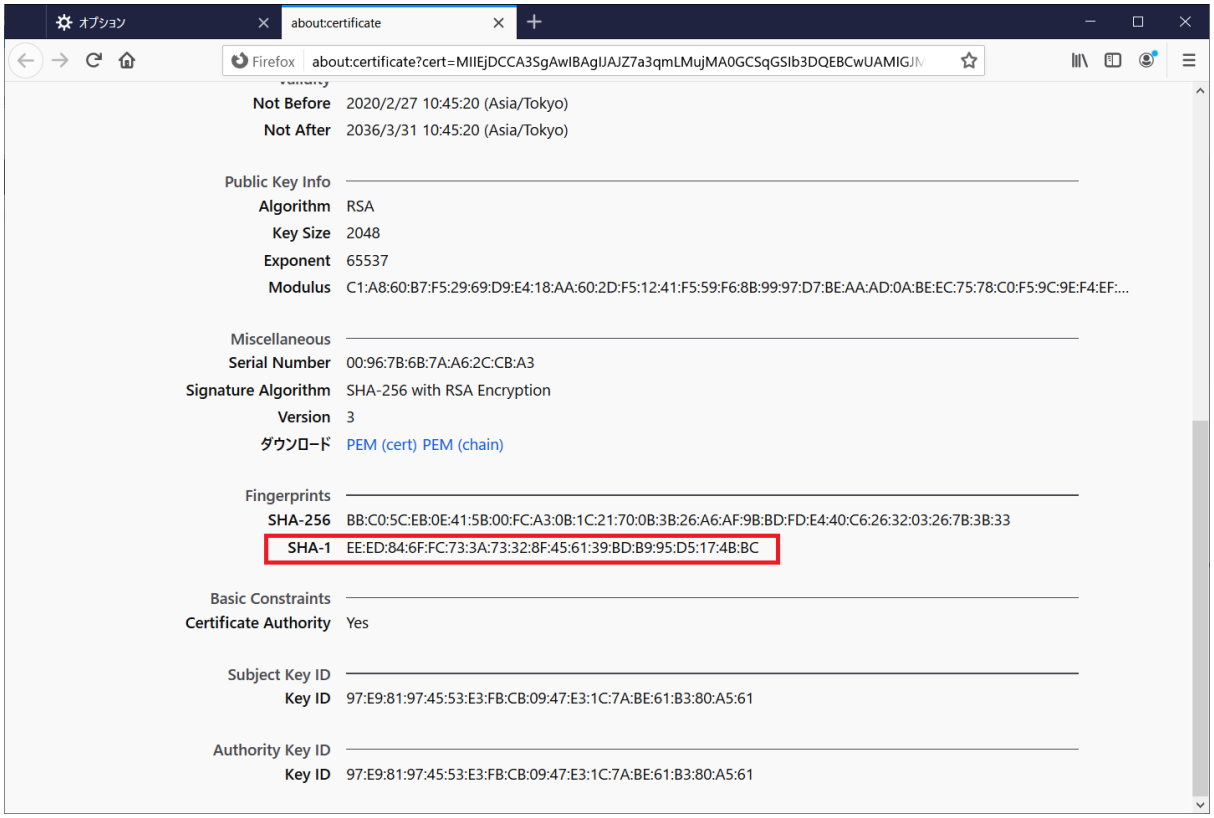
5. クライアント証明書が登録されたことを確認してください。



6. **[認証局証明書]** を選択し表示される一覧から「RIKEN R-CCS」を選択して**表示**をクリックします。



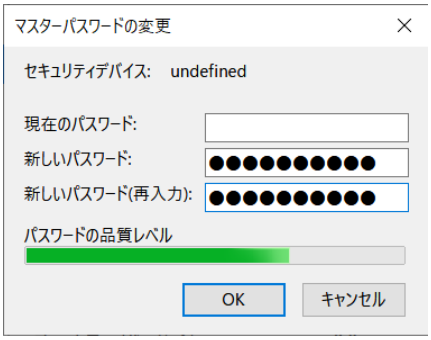
7. 証明書の Fingerprints が (SHA-1): EEED846F FC733A73 328F4561 39BDB995 D5174BBC であることを確認してください。



8. 続けて、クライアント証明書利用時に入力するパスワードを設定します。**セキュリティデバイス...** をクリックします。

9. デバイスマネージャが起動したら、*Software Security Device* を選択し、**パスワードを変更...** をクリックします。

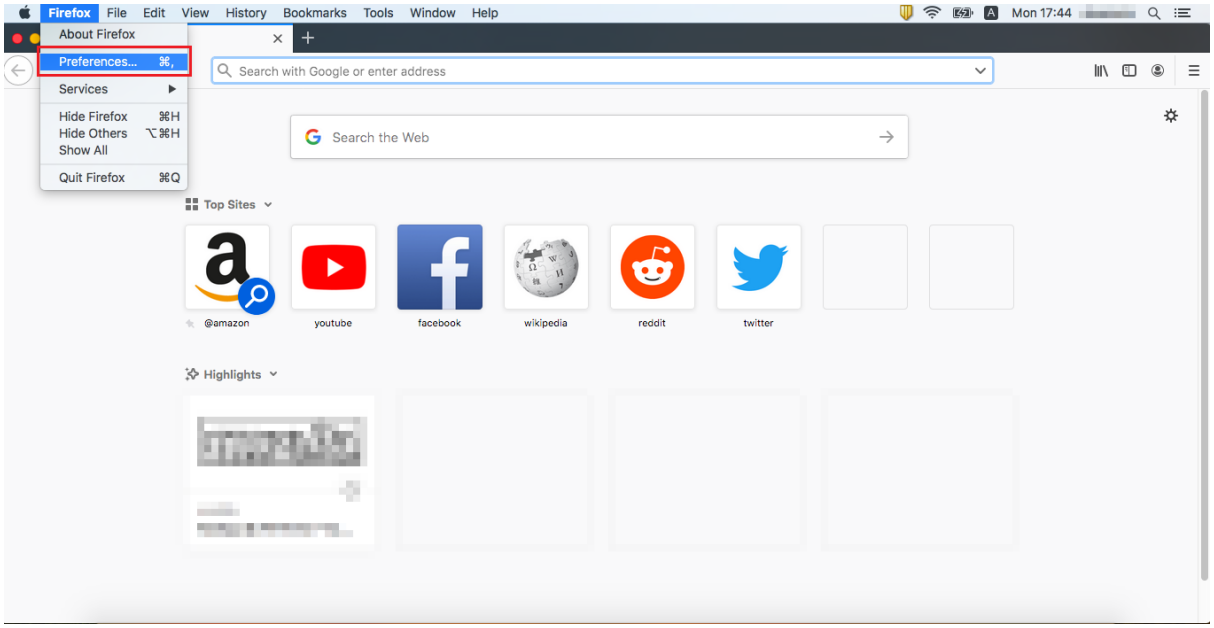
10. クライアント証明書利用時に要求される任意のパスワードを設定し、*OK* をクリックします



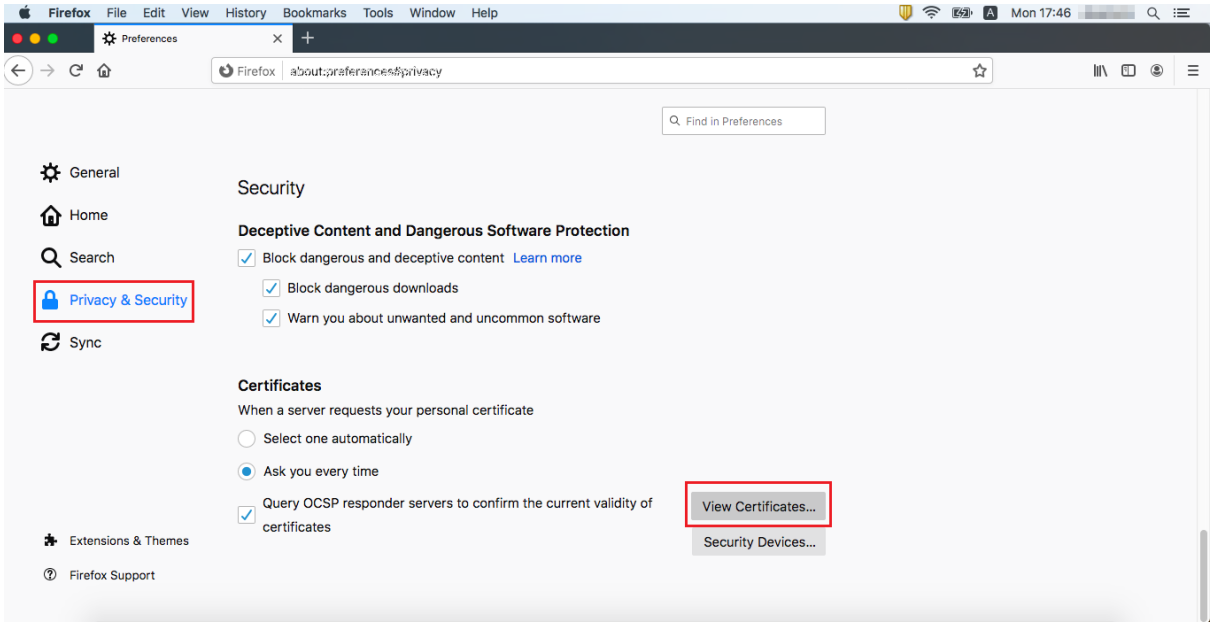
11. パスワードの登録が完了したら、デバイスマネージャを閉じます。クライアント証明書利用時のパスワードの設定作業は以上です。ここで設定したパスワードはクライアント証明書を利用するときに使用します。

2.2.2 Firefox への証明書のインストール（Mac）

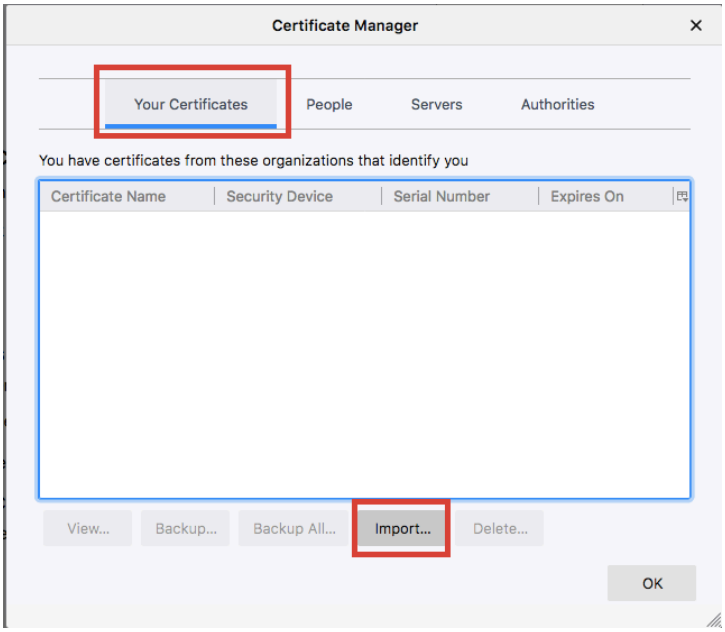
1. Firefox を起動し、メニューから *[**環境設定**...]* をクリックします。



2. **プライバシーとセキュリティ**タブの *[**証明書を表示**...]* をクリックします。

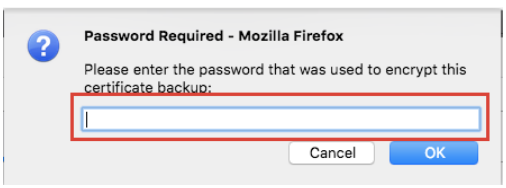


3. 証明書マネージャが起動したら、*[**あなたの証明書**]* を選択して、*[**読み込む**...]* をクリックします。



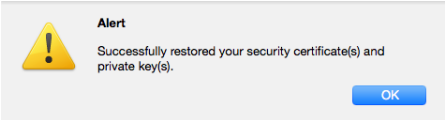
4. パソコンに保存した"ローカルアカウント名.p12"ファイルを選択し、*[開く]* をクリックします。

5. 入手したクライアント証明書のパスフレーズを **パスワード欄**に入力し、*[OK]* をクリックします。

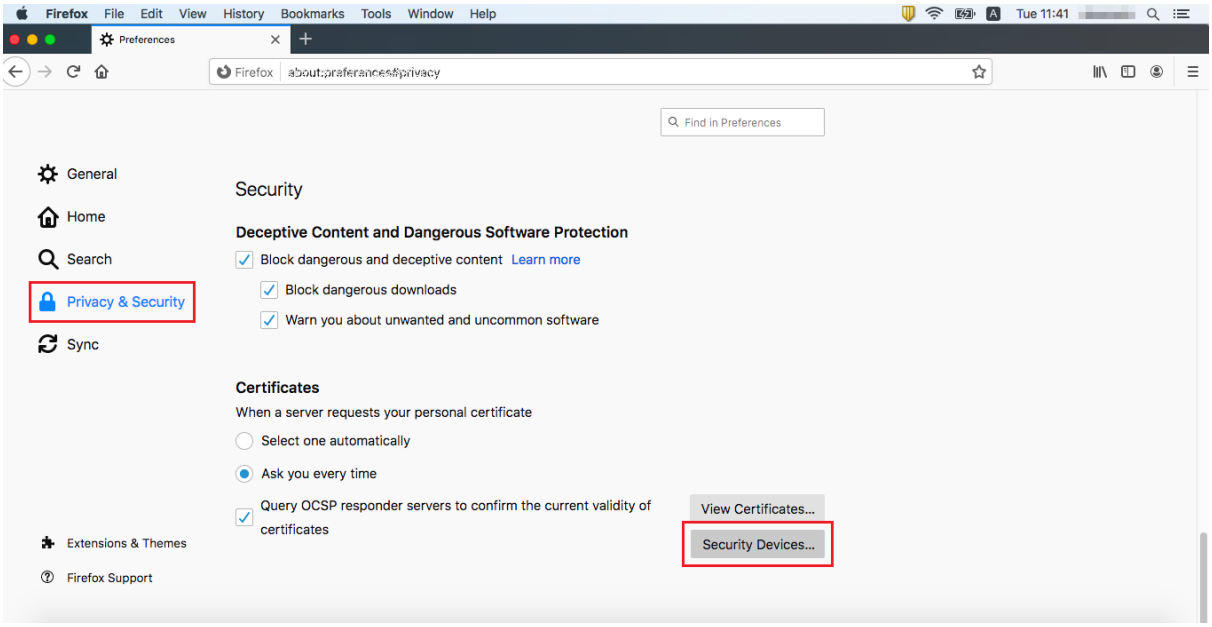


> **注意:** クライアント証明書のパスフレーズが正しくない場合エラーが表示され、次の画面に進めません。

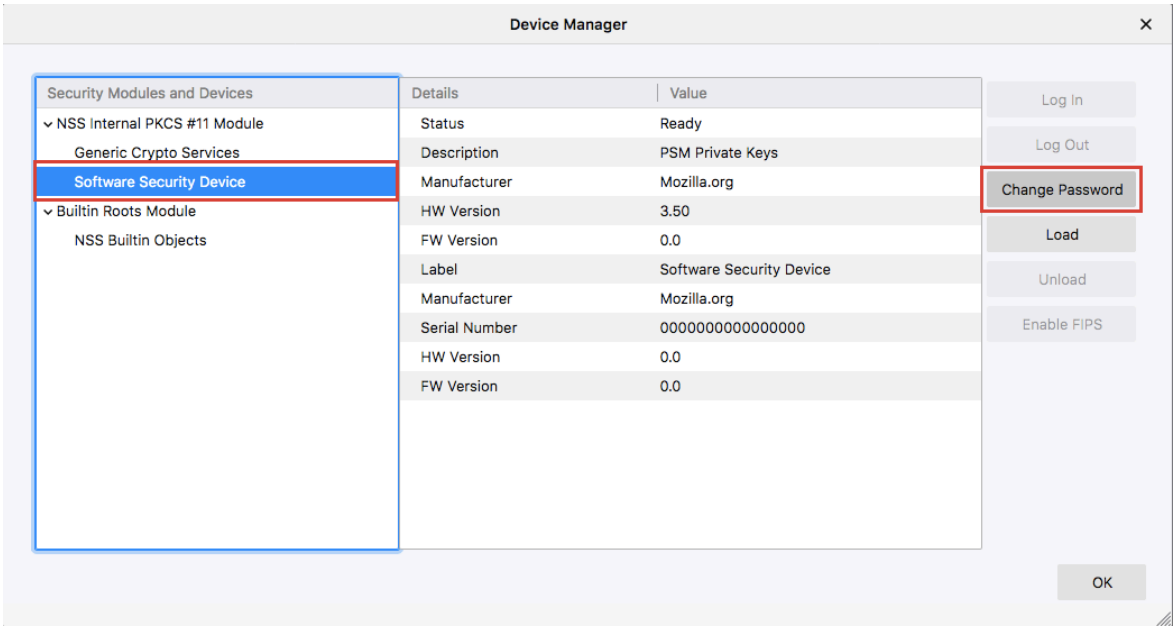
6. クライアント証明書が登録されたことを確認し、*[OK]* をクリックして証明書マネージャを終了します。以上で、クライアント証明書のインストール作業は完了です。



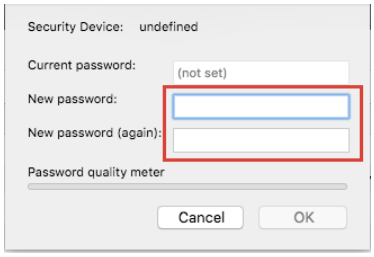
7. 続けて、クライアント証明書利用時に入力するパスワードを設定します。**セキュリティデバイス...** をクリックします。



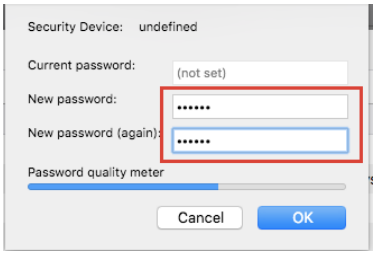
8. デバイスマネージャが起動したら、*Software Security Device* を選択し、**パスワードを変更...** をクリックします。



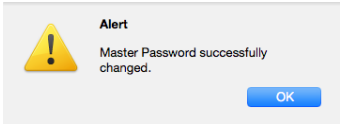
9. クライアント証明書利用時に要求される任意のパスワードを設定し、*OK* をクリックします



10. *OK* をクリックします。



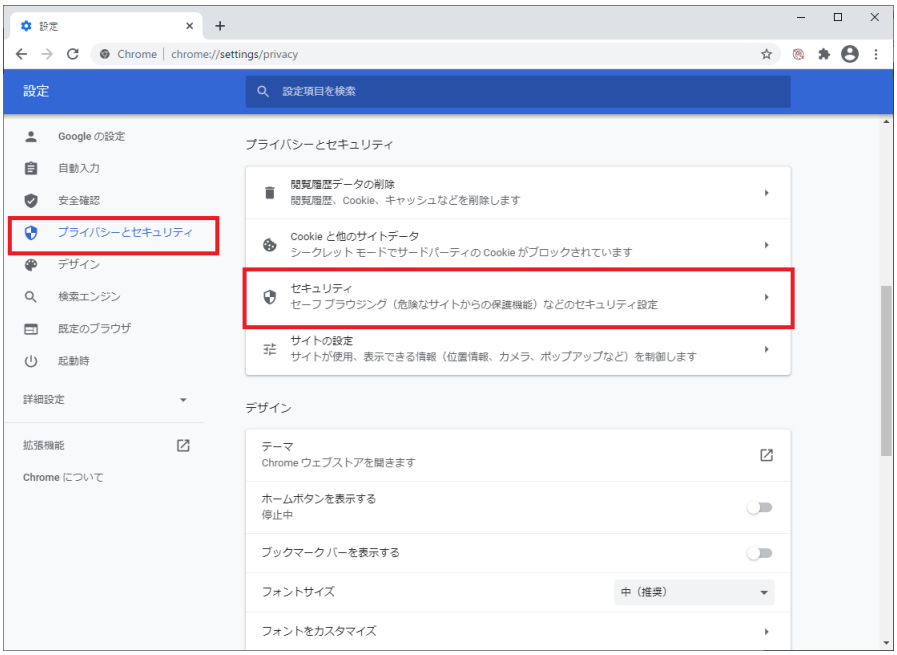
11. *OK* をクリックして、デバイスマネージャを閉じます。クライアント証明書利用時のパスワードの設定作業は以上です。



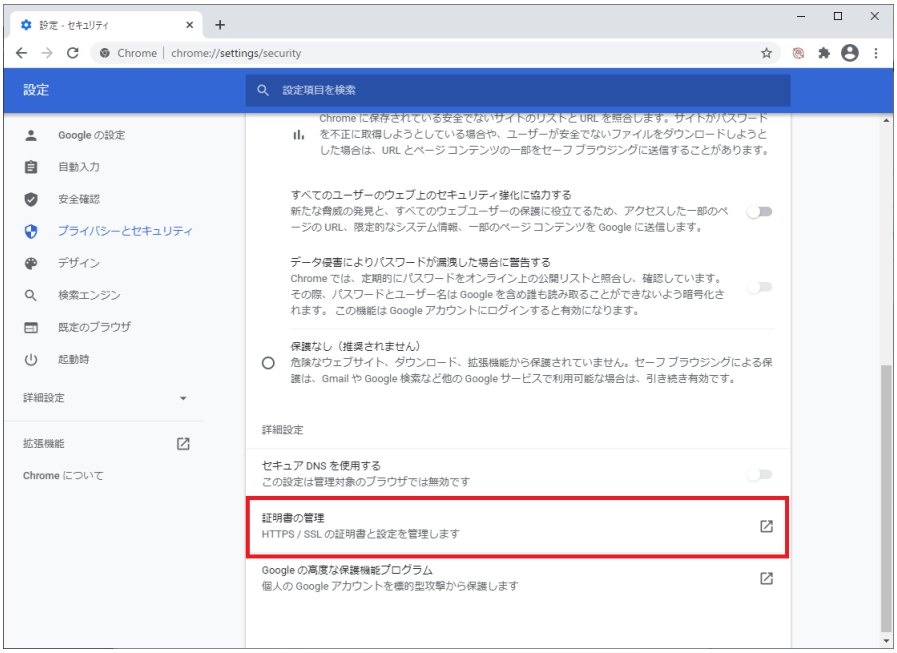
2.2.3 Chrome への証明書のインストール（Windows）

Microsoft Windows で Chrome を利用する場合のインストール手順を示します。Chrome のバージョンによって画面に差異がある場合があります。画面が異なる場合は Chrome の情報を確認して作業を実施してください。

1. Chrome を起動し、*[**設定**]* の画面を開きます。*[**プライバシーとセキュリティ**]* の *[**セキュリティ**]* をクリックします。

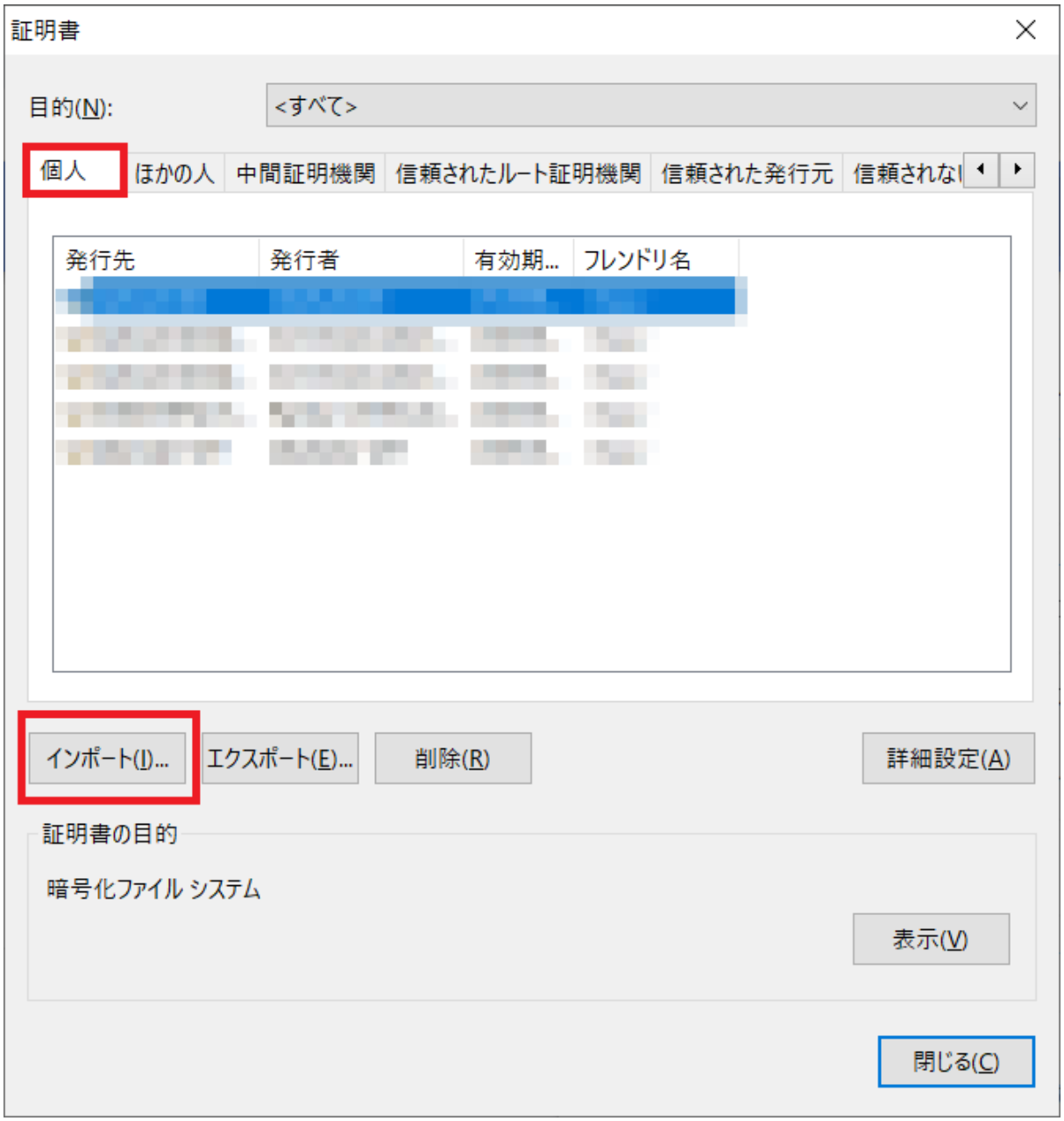


2. *[**証明書の管理**]* をクリックします。

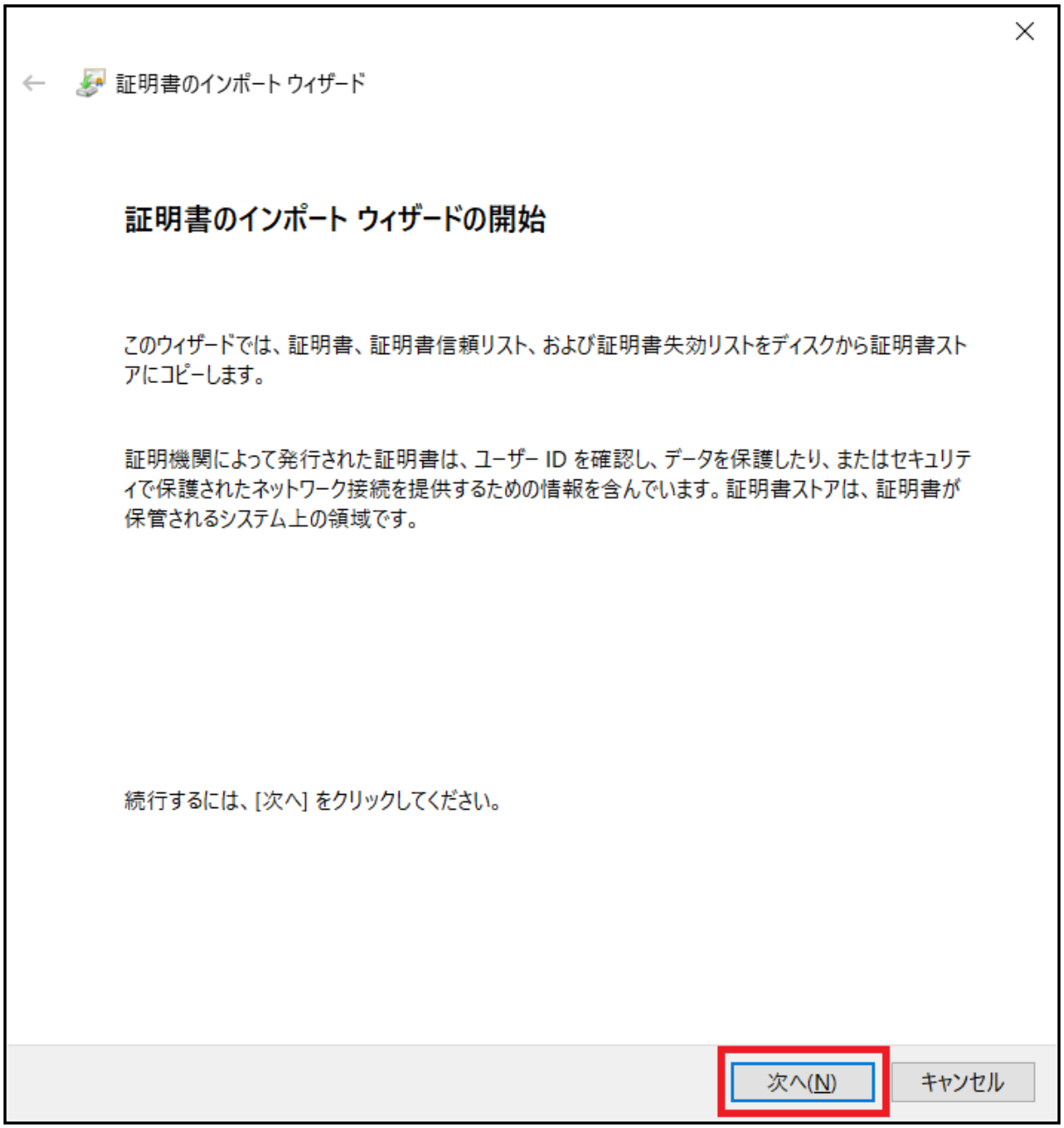


3. *[Windows* **からインポートした証明書を管理する***]* をクリックします。

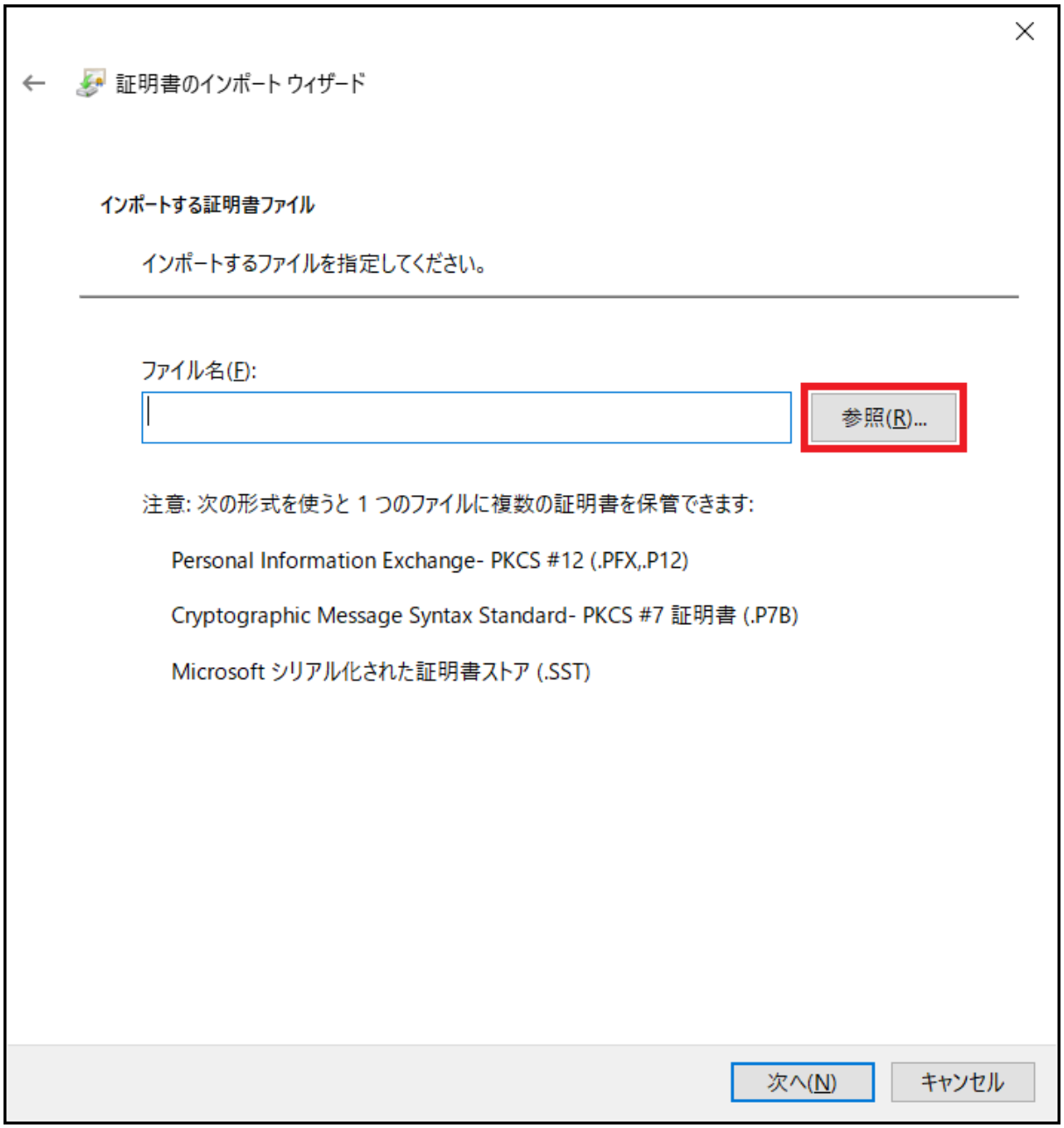
4. 証明書マネージャが起動したら、*[***個人***]* を選択して、*[***インポート***...]* をクリックします。



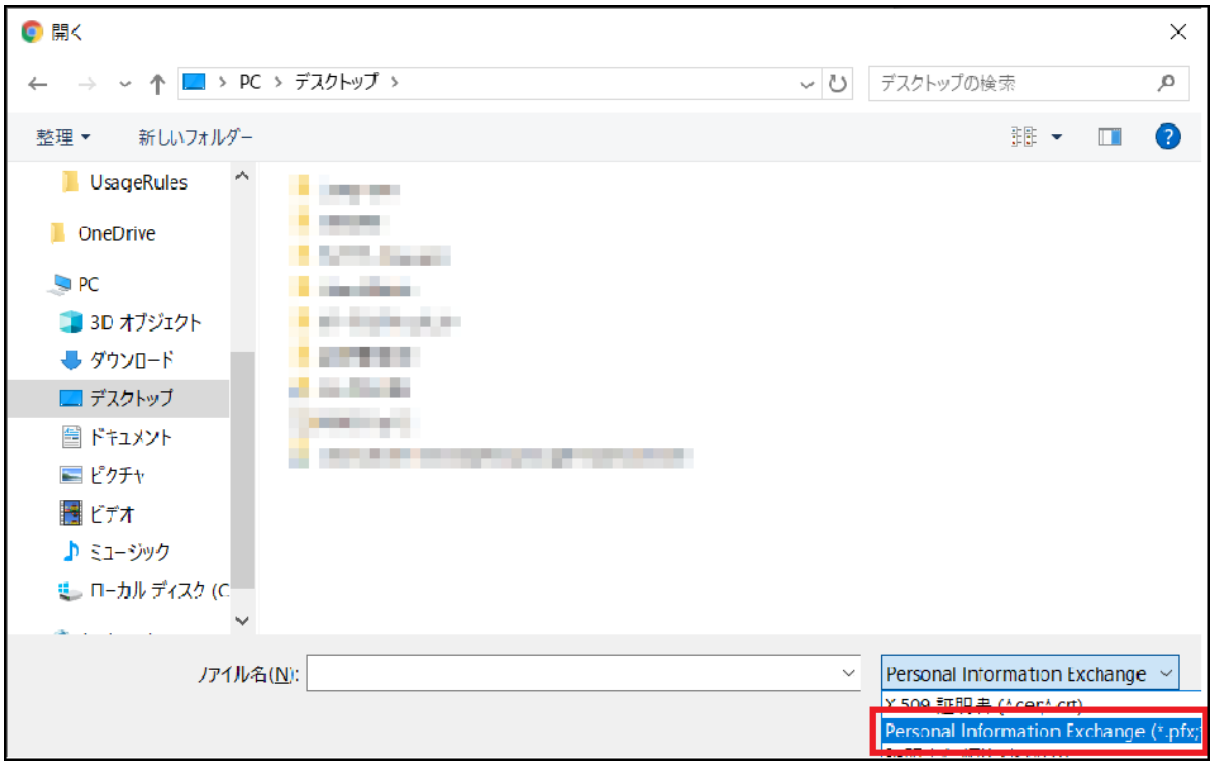
5. 証明書のインポートウイザードが開いたら *[次へ]* をクリックします。



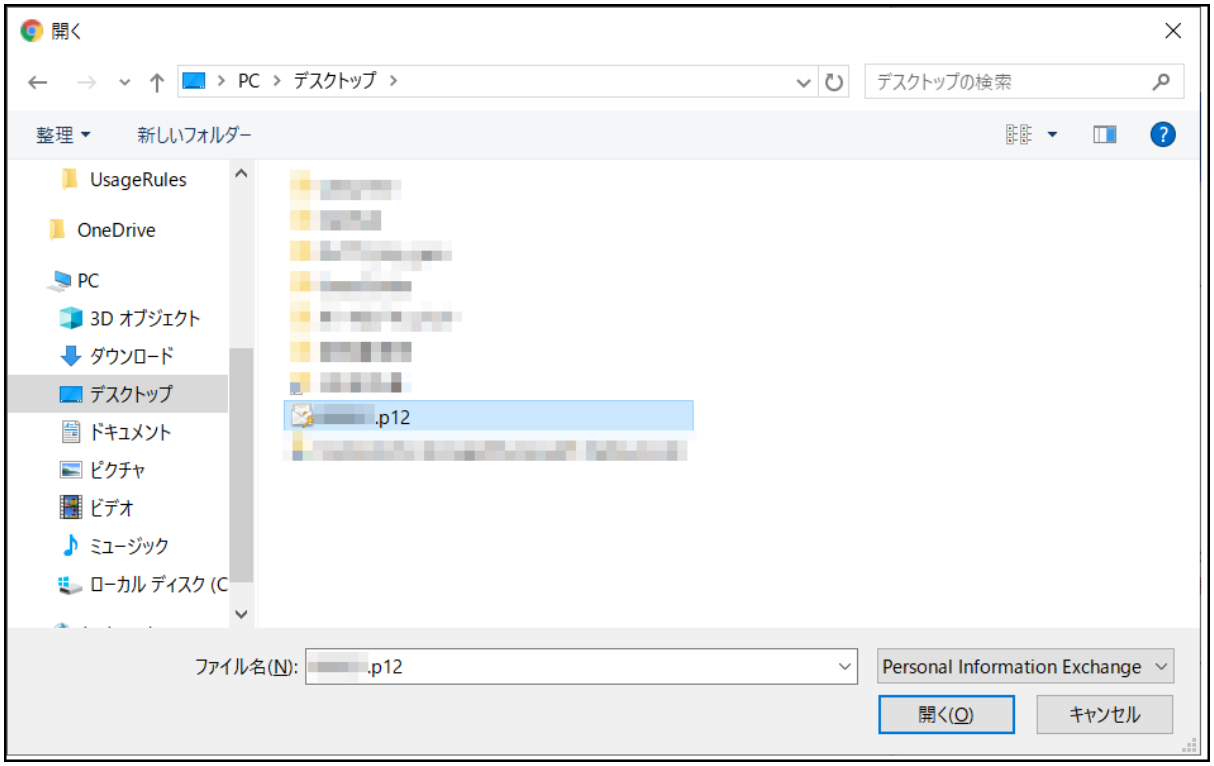
6. *[参照]* をクリックします。



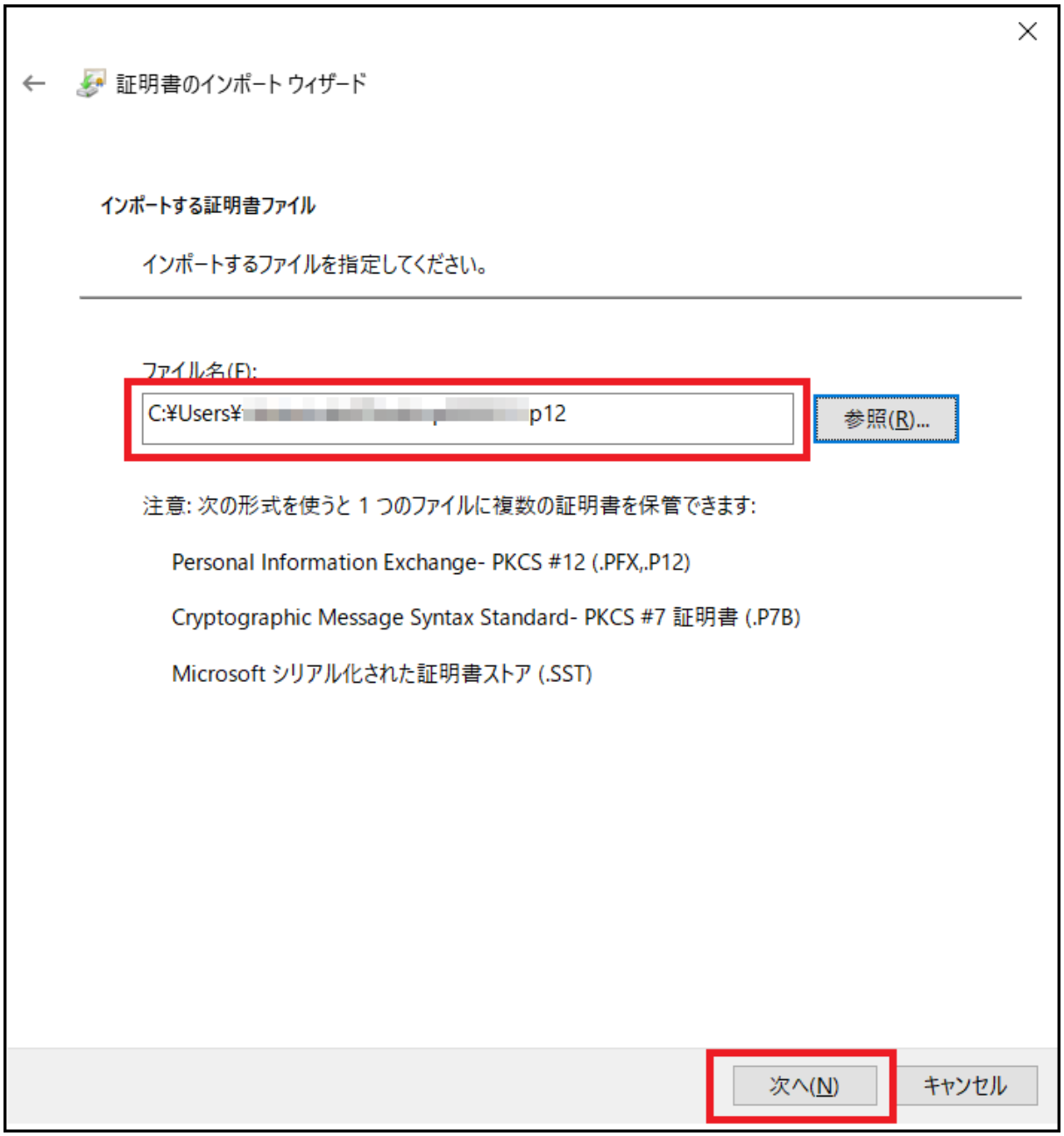
7. ファイルの種類を *[Personal Information Exchange(*.pfx,*.p12)]* に変更します。



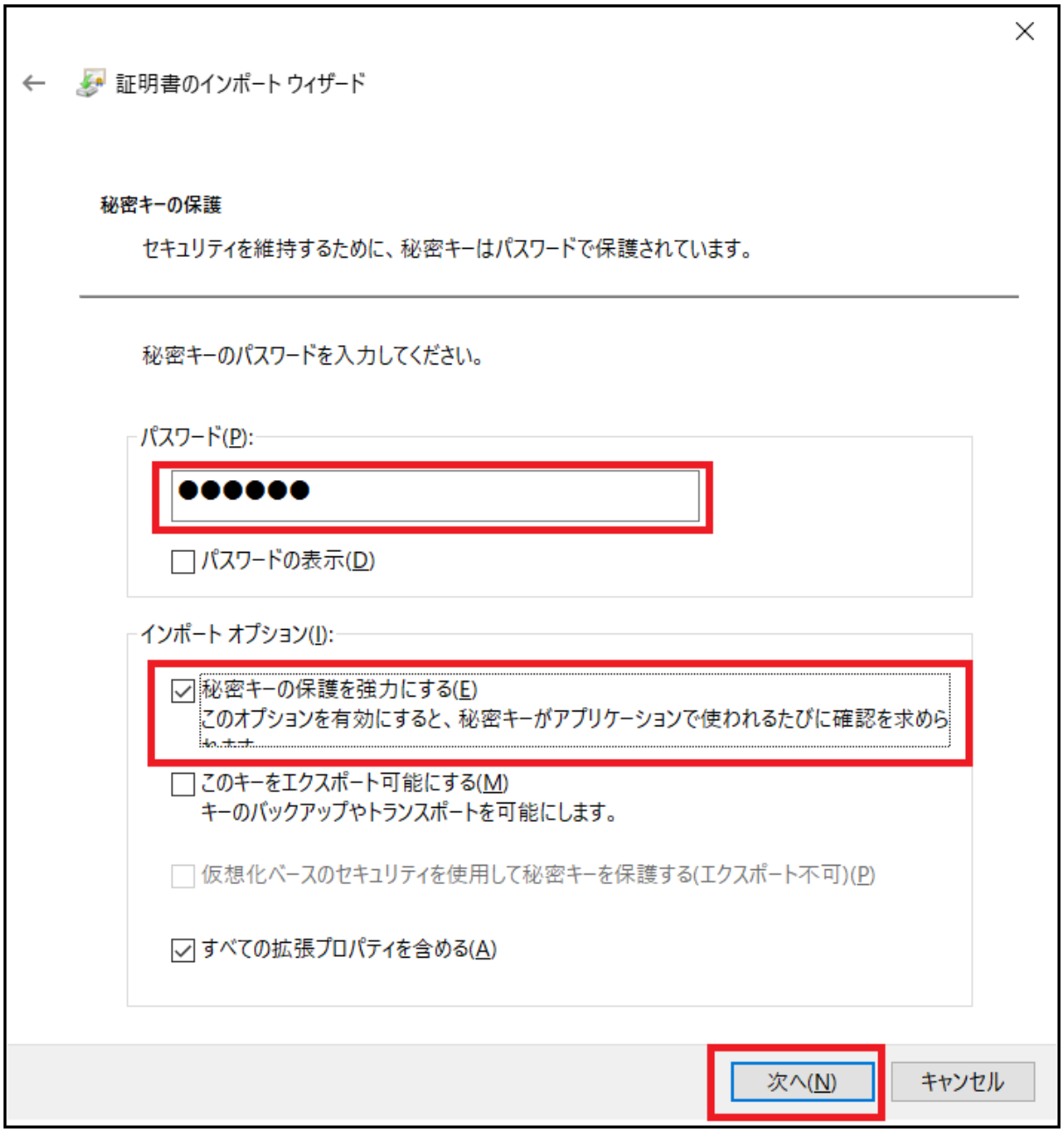
8. "ユーザーアカウント名.p12"ファイルを選択し、*[開く]* をクリックします。



9. ファイル名を設定した後、*[次へ]* をクリックします。

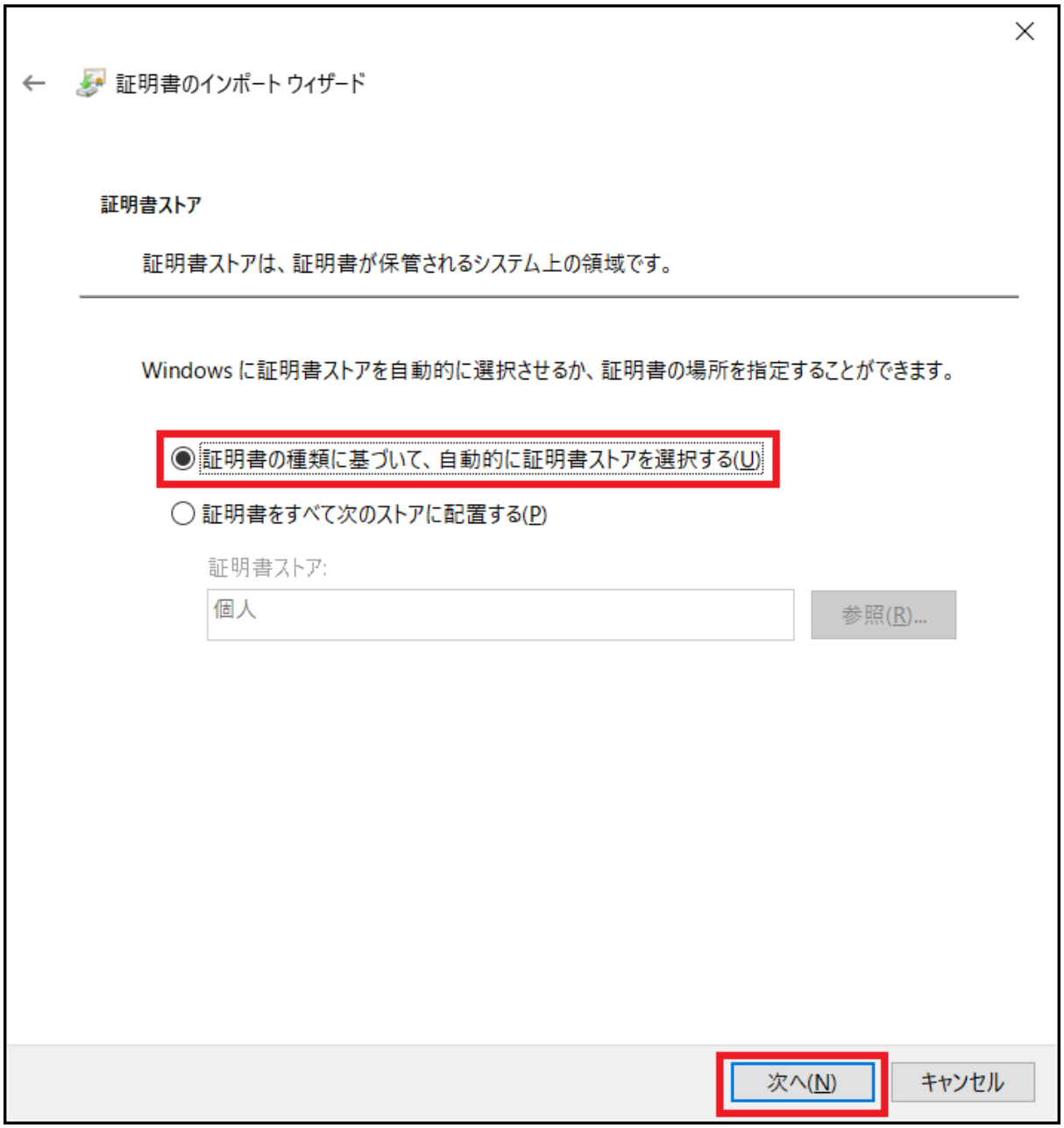


10. クライアント証明書のパスフレーズを**パスワード欄**に入力し、インポートオプションの *[**秘密キーの保護を強力にする**にチェックを付け、**次へ**]* をクリックします。

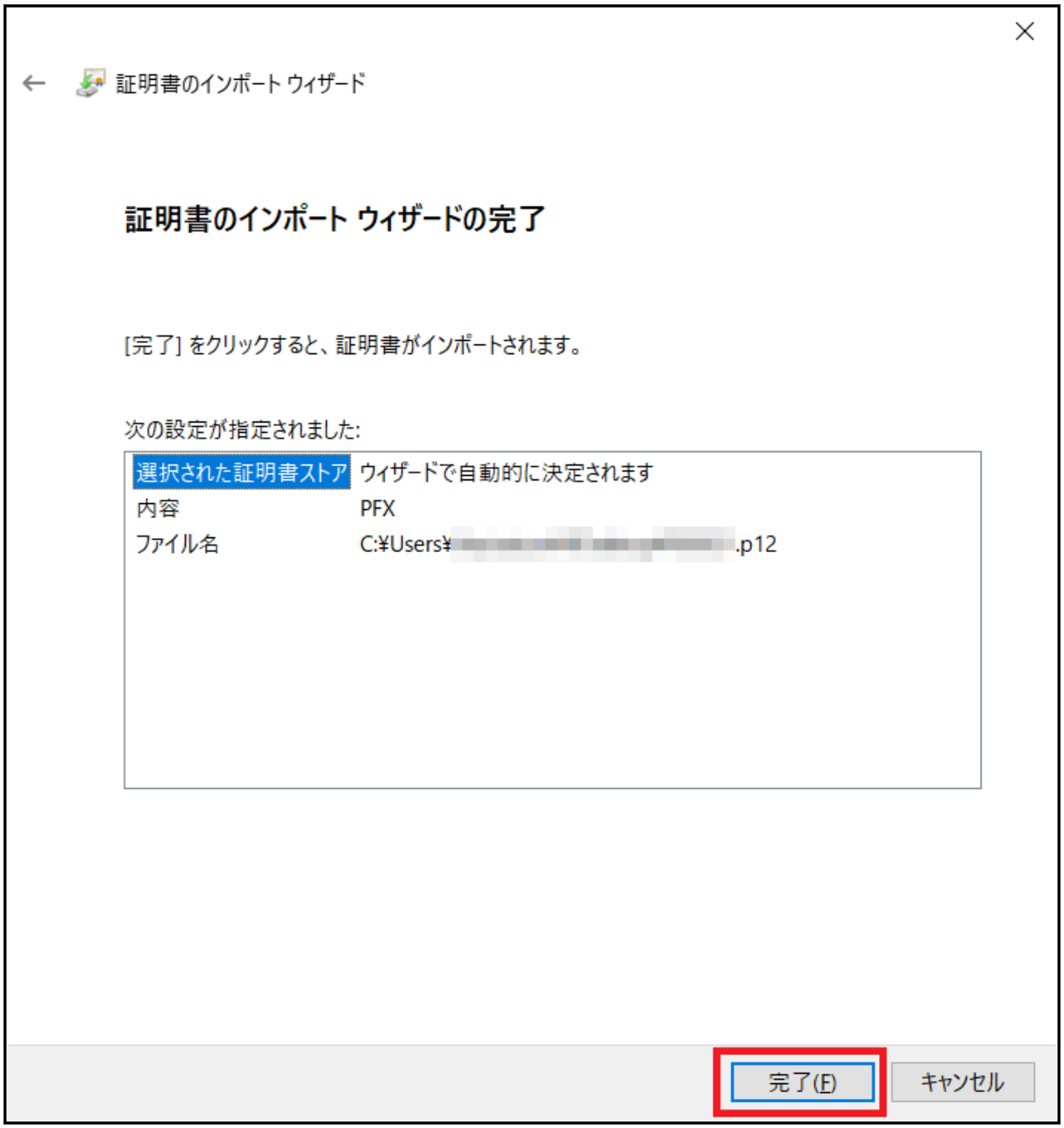


> **注意:** クライアント証明書のパスフレーズが正しくない場合エラーが表示され、次の画面に進めません。

11. **証明書の種類に基づいて、自動的に証明書ストアを選択する**をチェックし、*[次へ]* をクリックします。

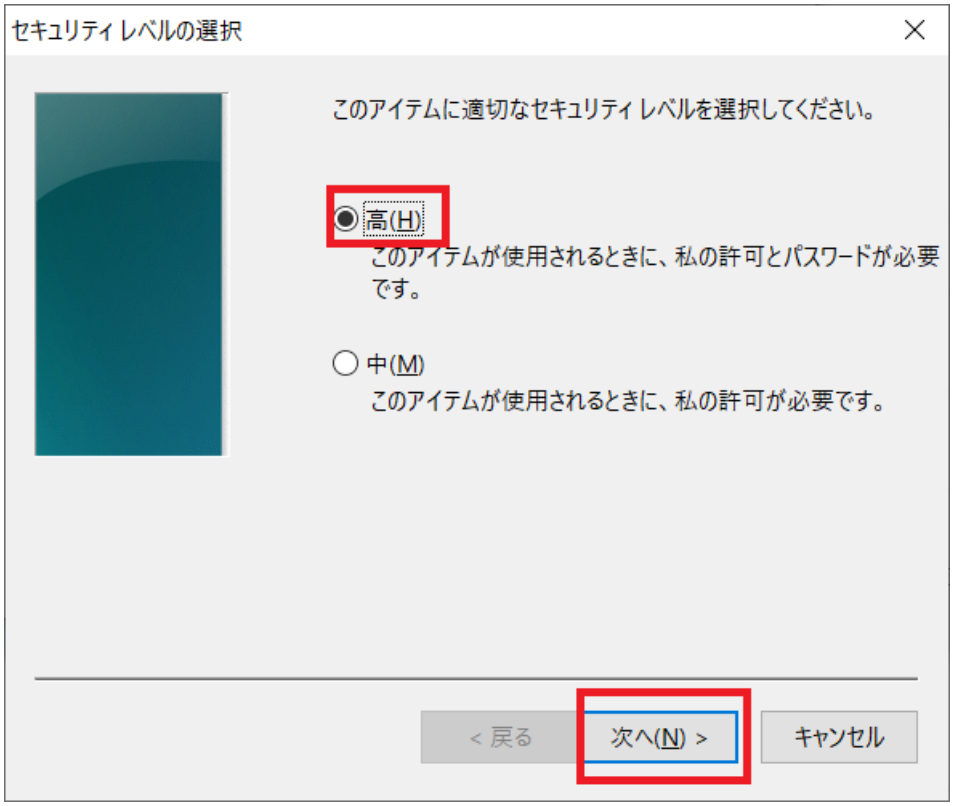


12. *[完了]* をクリックします。



13. 引き続き「新しい秘密交換キーをインポートします」画面が表示されますので、*[**セキュリティレベルの設定**]* をクリックします。

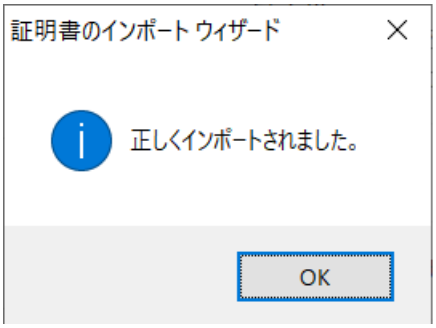
14. *[高]* をチェックし、*[次へ]* をクリックします。



15. パスワードを設定し、*[完了]* をクリックします。

16. *[OK]* をクリックします。

17. *[OK]* をクリックします。



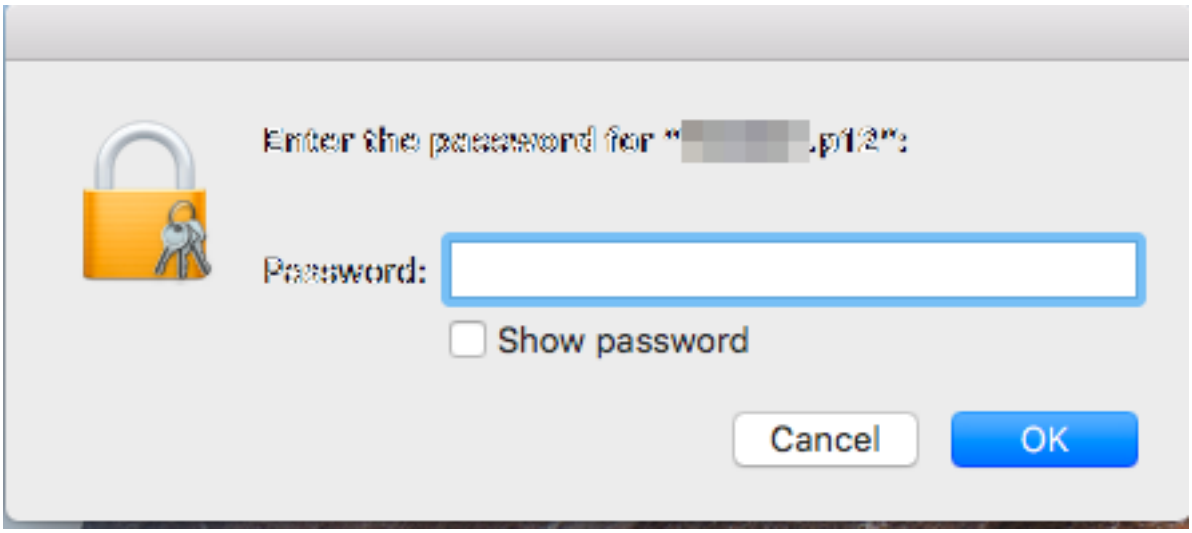
18. セキュリティ警告が出た場合は、拇印が (SHA-1): EEED846F FC733A73 328F4561 39BDB995 D5174BBC であることを確認したうえで、*[はい]* をクリックします。

19. 以上でクライアント証明書のインストールは完了です。

2.2.4 Chrome への証明書のインストール（Mac）

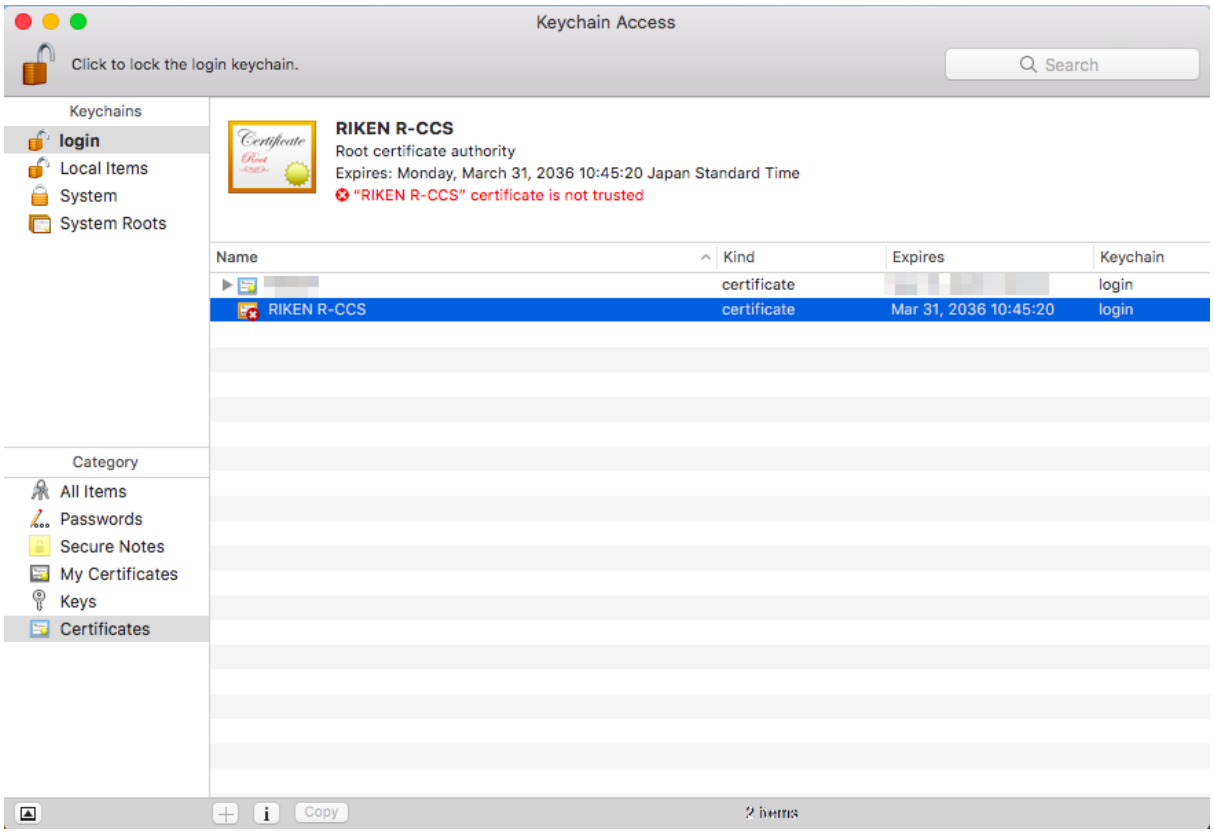
Mac で Chrome を利用する場合のインストール手順を示します。macOS では、クライアント証明書を「キーチェーンアクセス」で管理しています。

1. クライアント証明書:"ユーザーアカウント名.p12"ファイルをダブルクリックします。最初にパスワード入力画面が表示されます。クライアント証明書のパスフレーズを入力し、*[OK]* をクリックします。



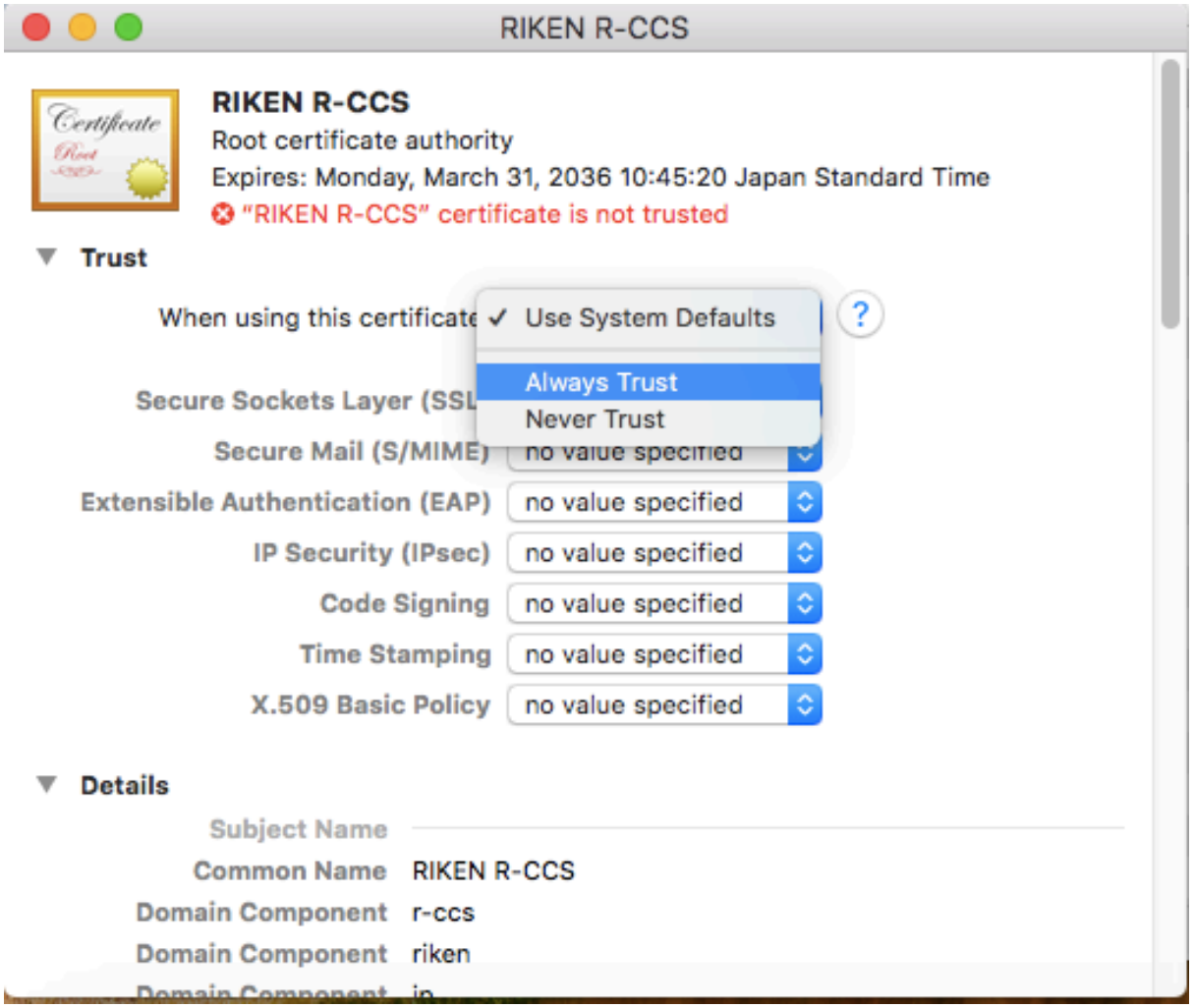
> **注意:** クライアント証明書のパスフレーズが正しくない場合エラーが表示され、次の画面に進めません。

2. 「キーチェーンアクセス」画面を開き、クライアント証明書を発行したサーバの証明書（RIKEN R-CCS）をダブルクリックします。

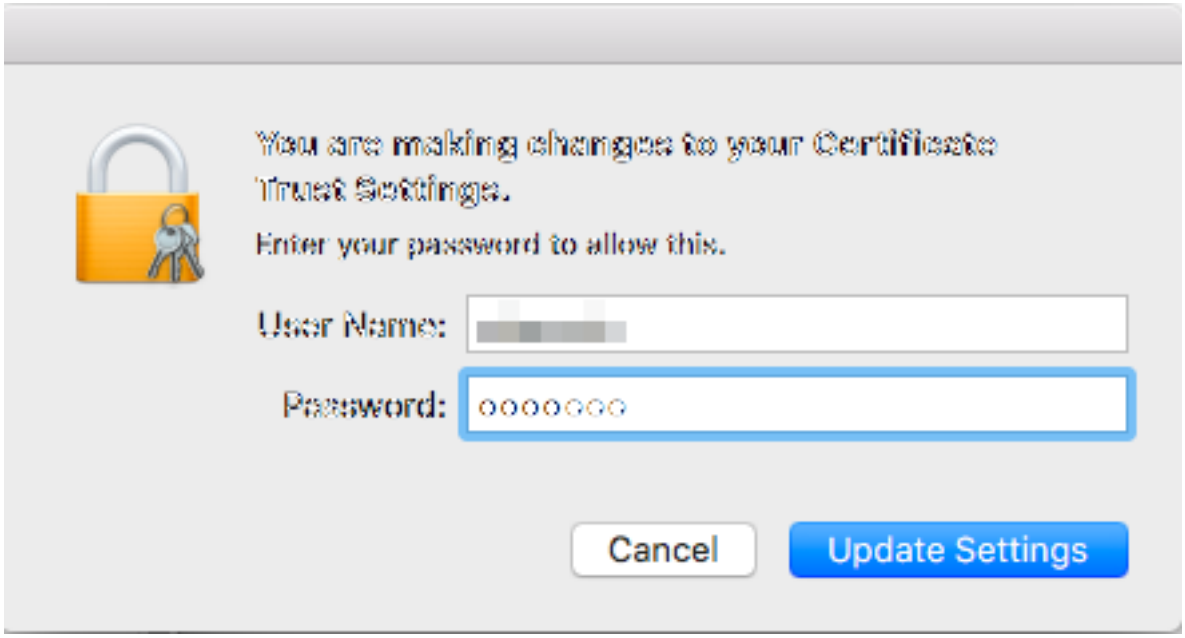


3. 「ルート認証局」の「信頼」をクリックし、「この証明書を使用するとき：」のリストから「常に信頼す

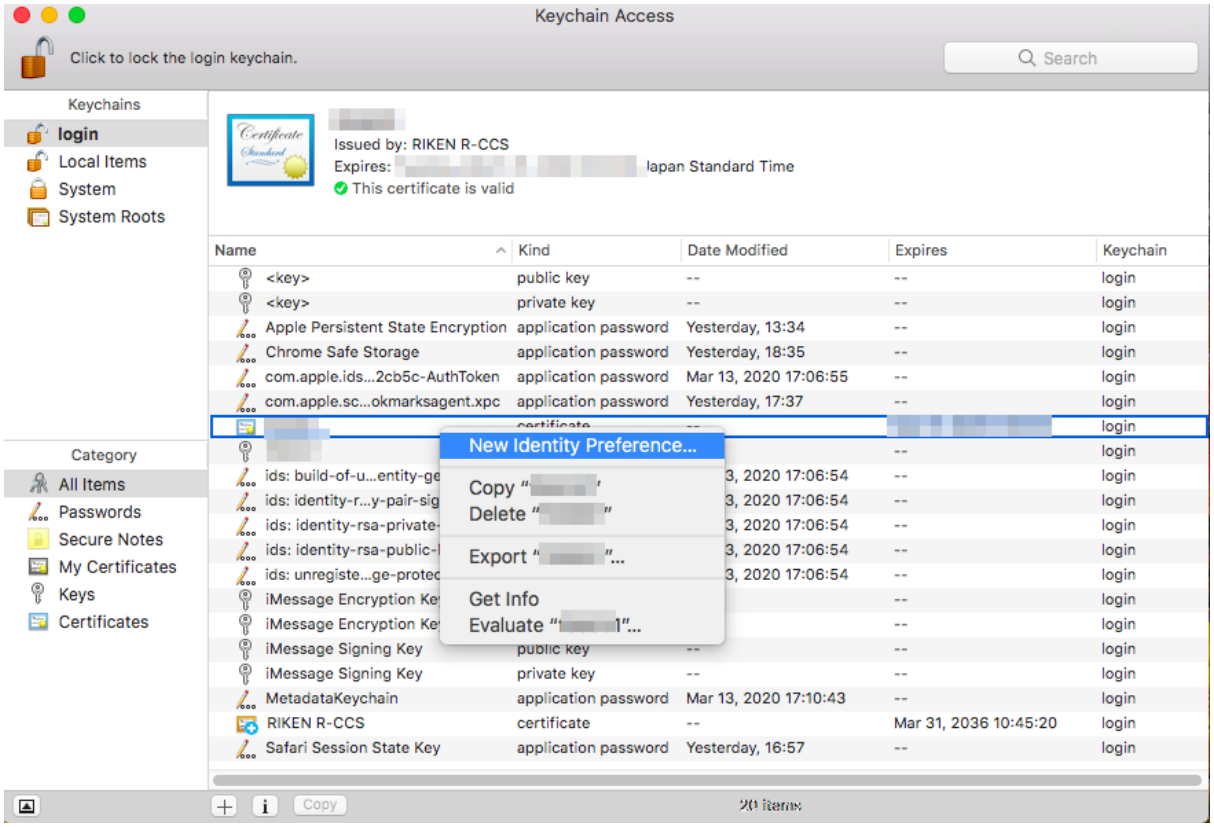
る」を選択して、画面を閉じます。



4. 信頼設定の変更を反映するため、Mac の管理者ユーザ名とパスワードが要求されます。これらを入力し、［**設定をアップデート**］をクリックします。

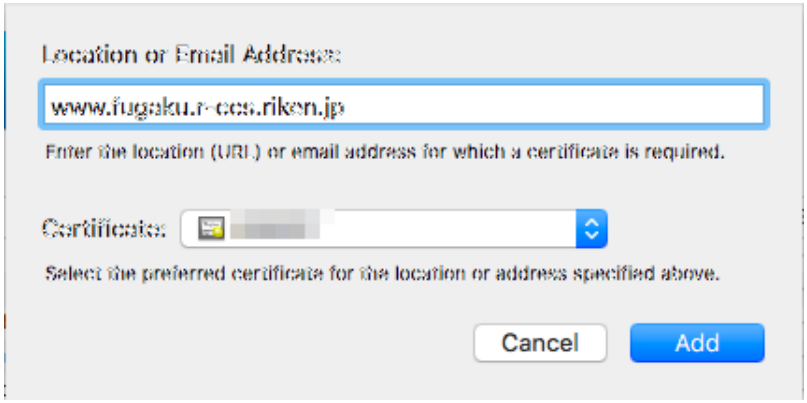


5. 「キーチェーンアクセス」画面で、Control キーを押しながらクライアント証明書（名前欄にローカルアカウント名が表記されたもの）をクリックし、**「新規識別プリファレンス」**を選択します。

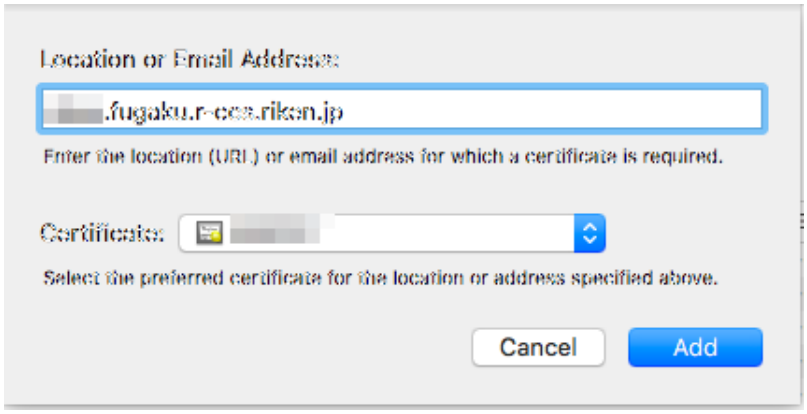


6. 「場所またはメールアドレス：」に「https://www.fugaku.r-ccs.riken.jp/」と入力し、*[追加]* をクリック

します。



7. 同様の手順で「https://api.fugaku.r-ccs.riken.jp/」を登録します。



8. 「キーチェーンアクセス」に入力した「https://www.fugaku.r-ccs.riken.jp/」「https://api.fugaku.r-ccs.riken.jp/」の「識別プリファレンス」が追加されたことを確認し、画面を閉じます。インストール作業はこれで完了です。

2.3 富岳ウェブサイトへの接続手順

ここでは、富岳ウェブサイトへのアクセス方法について説明します。

1. ブラウザを用いて、次の URI へアクセスします。

   https://www.fugaku.r-ccs.riken.jp

注釈:

- 富岳ウェブサイトは、Mozilla Firefox と Google Chrome で動作確認を実施しています。他のブラウザをご利用の場合に動作に不具合が発生した場合は、動作確認済のブラウザをご利用ください。

なお、Microsoft Internet Explorer を利用した場合は公開鍵登録で異常終了することが確認されています。

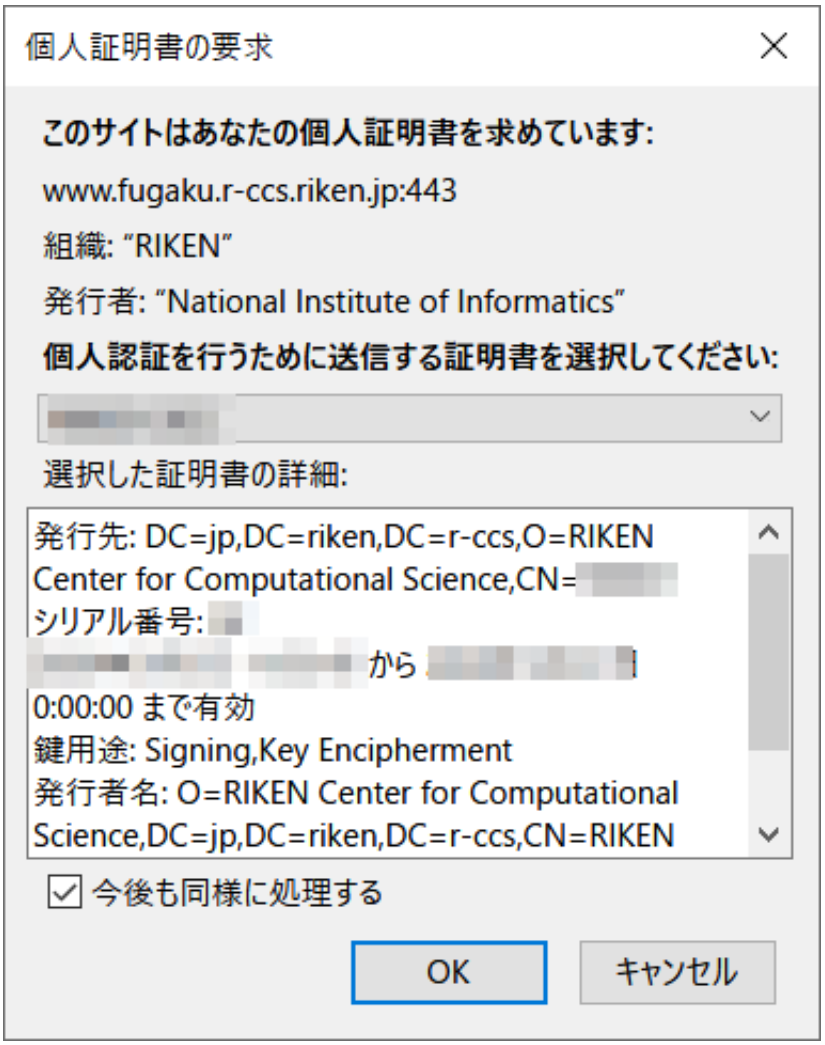
- 脆弱性対応のため、富岳ウェブサイトでは古い SSL 接続を禁止しており、TLS 1.2 または TLS1.3 接続のみ受け付けます。お使いのブラウザの設定によっては接続できない場合があるので、以下のとおり TLS 1.2 以降を使用するように適宜設定を変更してください。

[Firefox の設定変更方法]

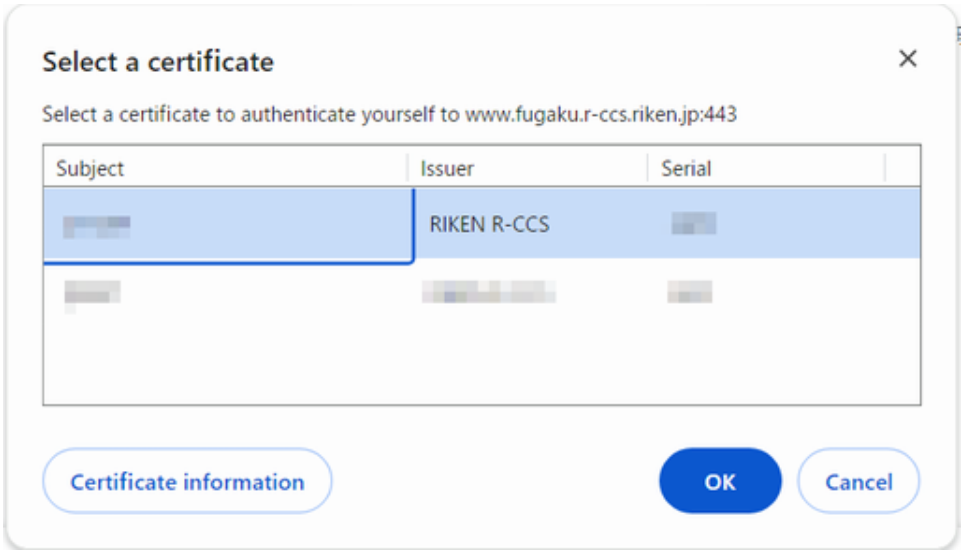
1. アドレスバーに **about:config** と入力し Enter キーを押す
2. security.tls.version で検索する
3. 「*security.tls.version.max*」が 4（TLS 1.3 まで有効）になっていることを確認する
4. 4 より小さい値の場合は、4 を設定します

2. クライアント証明書の選択ダイアログが表示されたら、利用するローカルアカウントのクライアント証明書を選択します。

- Firefox のダイアログ例

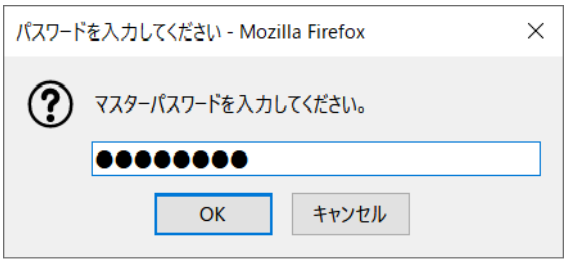


- Chrome のダイアログ例



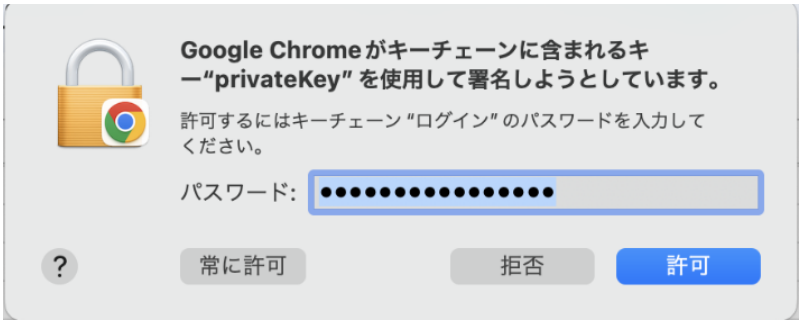
3. パスワードの入力ダイアログに、クライアント証明書のインストール時に登録した秘密鍵のパスワードを入力します。macOS のキーチェーンを利用している場合はキーチェーンのパスワードを入力します。

- Firefox のダイアログ例



- キーチェーン（macOS）のダイアログ例

  キーチェーンのパスワード（通常はパソコンのログインパスワードと同じ）を入力します。



注釈: Mac で Chrome 利用時にキーチェーンのパスワード入力を何度も求められる場合は、パスワード入力ダイアログで [常に許可] をクリックしてください。

4. クライアント証明書の認証に成功すると、次のような画面が表示されます。

2.4 ログイン

ローカルアカウントを使用してスーパーコンピュータ「富岳」へログインするには、ログインノードに SSH Version2（公開鍵認証）でログインします。

事前に利用者の端末にて SSH の鍵ペア（公開鍵と秘密鍵）を作成し、公開鍵を富岳ウェブサイト画面から登録してください。登録するのは公開鍵のみです。秘密鍵が登録された場合、安全対策としてログインの一時停止等の処理を実施する場合があります。

注釈: ログインノードのホームディレクトリ配下の次に示すディレクトリ、および、ファイルのパーミッションを変更すると ssh でログインできなくなります。

- ホームディレクトリのパーミッション（700）
- ~/.ssh ディレクトリのパーミッション（700）
- ~/.ssh/authorized_keys のパーミッション（600）

これらのパーミッションを変更しないように注意してください。

2.4.1 鍵ペア（秘密鍵／公開鍵）の作成

スーパーコンピュータ「富岳」を利用する場合は利用者端末で秘密鍵と公開鍵のペアを作成します。生成する鍵の種類は次のいずれかを推奨します。

- Ed25519
- ECDSA（NIST P 521）
- RSA（鍵長 2048bit 以上）：RSA 鍵の利用は富岳ウェブサイトの「ログインノードの ssh アクセスに関する運用変更」も参照ください。

UNIX ／ Linux（OpenSSH）および Windows（puttygen）を使用した Ed25519 の鍵ペア（公開鍵／秘密鍵）の作成手順を示します。puttygen を使用する場合には、ターミナルエミュレータ PuTTY（パティ）を事前にインストールする必要があります。

Unix ／ Linux ／ Mac (OpenSSH)

利用者の端末にて **ssh-keygen** コマンドを実行し、秘密鍵と公開鍵のペアを作成します。

1. ターミナルを起動して、**ssh-keygen** コマンドを実行します。
   - Mac（OS X）の場合は、Terminal（**アプリケーション** → **ユーティリティ** → **ターミナル**）を起動して **ssh-keygen** コマンドを実行します。
   - UNIX ／ Linux の場合は、端末エミュレータを起動して **ssh-keygen** コマンドを実行します。

```
[terminal]$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/username/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):  # パスフレーズを入力
Enter same passphrase again:                 # もう一度同じパスフレーズを入力
Your identification has been saved in /home/username/.ssh/id_ed25519.
Your public key has been saved in /home/username/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:khbWyIyUqMnyjK1Ok78l8EivKbQLNgP3vyhjYBgvif8 namehostname
The key's randomart image is:
+--[ED25519 256]--+
|   ...           |
|  ...+ o         |
|.o  . * .        |
|=.   . o         |
```

(次のページに続く)

(前のページからの続き)

```
|=@    + S        |
|@o%  . .         |
|=%.= .           |
|*=O =            |
|+=+=Eo.          |
+----[SHA256]-----+
```

注釈:

- パスフレーズはパスワード同様に他人が推測しにくい文字列を設定してください。また、必ずパスフレーズを設定するようお願い致します。パスフレーズの長さは 15 文字以上を推奨します。

2. **ssh-keygen** を実行すると、ホームディレクトリ配下の.ssh ディレクトリに秘密鍵（id_ed25519）と公開鍵（id_ed25519.pub）の 2 種類が作成されます。

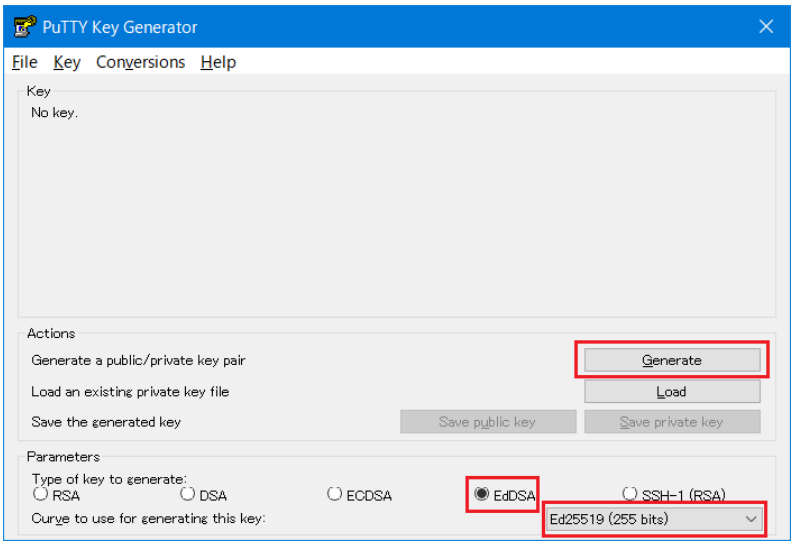
   公開鍵（id_ed25519.pub）を富岳ウェブサイトを利用して登録します。

Windows (PuTTYgen)

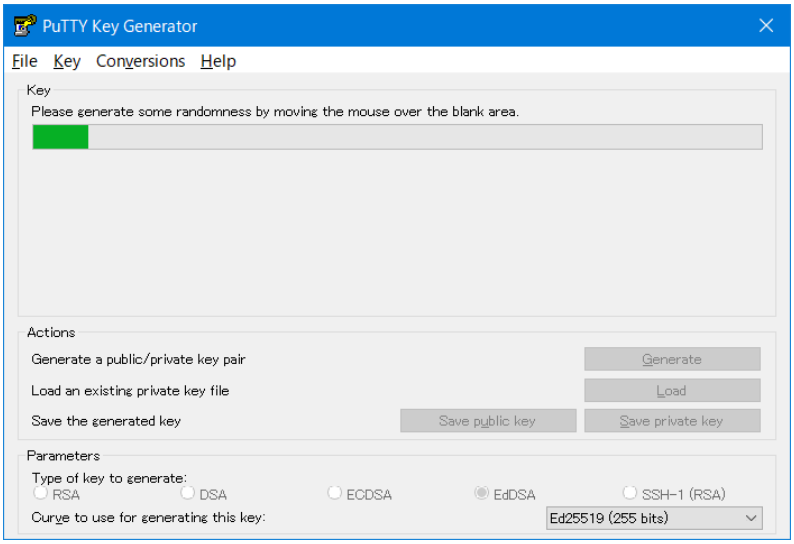
PuTTY ／ WinSCP で利用可能な秘密鍵／公開鍵を puttygen により作成します。

1. puttygen を起動します。

   鍵の種類（Type of key to generate）として「*EdDSA*」を選択し「*Ed25519 (255 bits)*」カーブを選択し、「*Generate*」ボタンをクリックします。



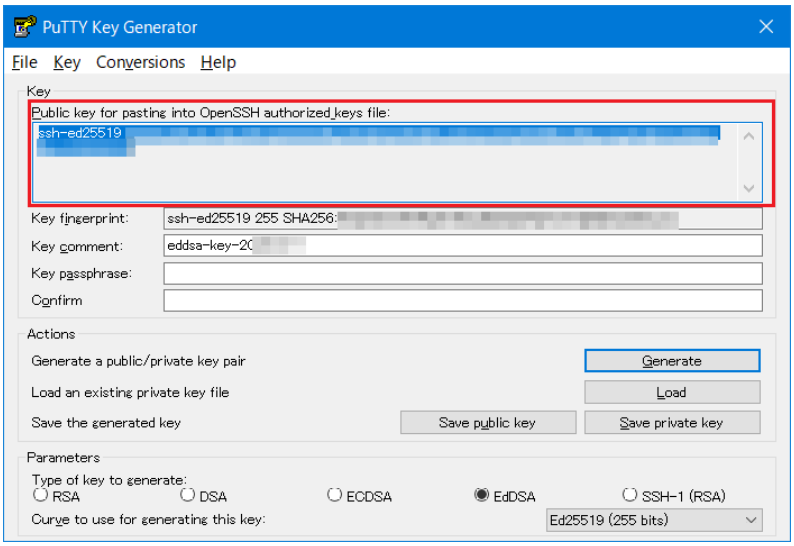
2. マウスカーソルをランダムに動かします。



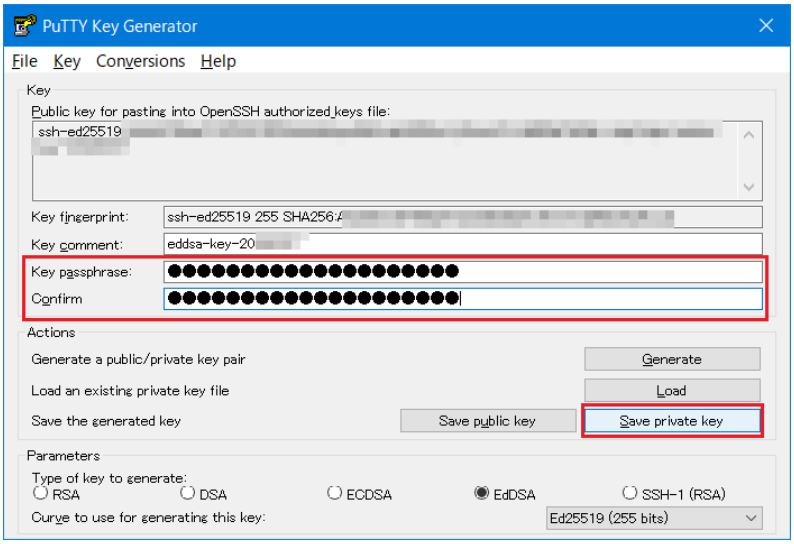
3. 公開鍵を保管します。

   「Public key for pasting in to OpenSSH authorized_keys file:」に表示される内容を、クリップボードにコピーします（メモ帳を起動し貼り付けておくことをお勧めします）。

   クリップボードに張り付けた内容（公開鍵となります）を、富岳ウェブサイトを利用して登録します。

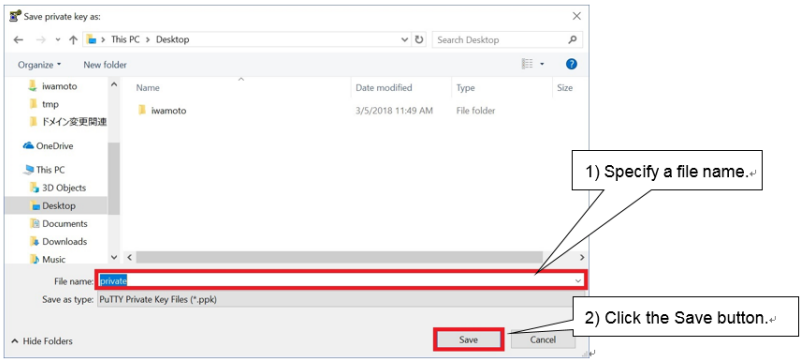


4. 「*Key passphrase*」および「*Confirm passphrase*」に、パスフレーズを入力します。入力後、「*Save private key*」ボタンをクリックし、秘密鍵を保管します。パスフレーズは、ログインノードへのログイン時に入力を求められますので、忘れないようにしてください。



注意: パスフレーズはパスワード同様に他人が推測しにくい文字列を設定してください。また、必ずパスフレーズを設定するようお願い致します。パスフレーズの長さは 15 文字以上を推奨します。

5. 秘密鍵を保管するファイル名を「**ファイル名** *(N)*」に入力し、「**保存** *(S)*」ボタンをクリックします。秘密鍵が保管されます。



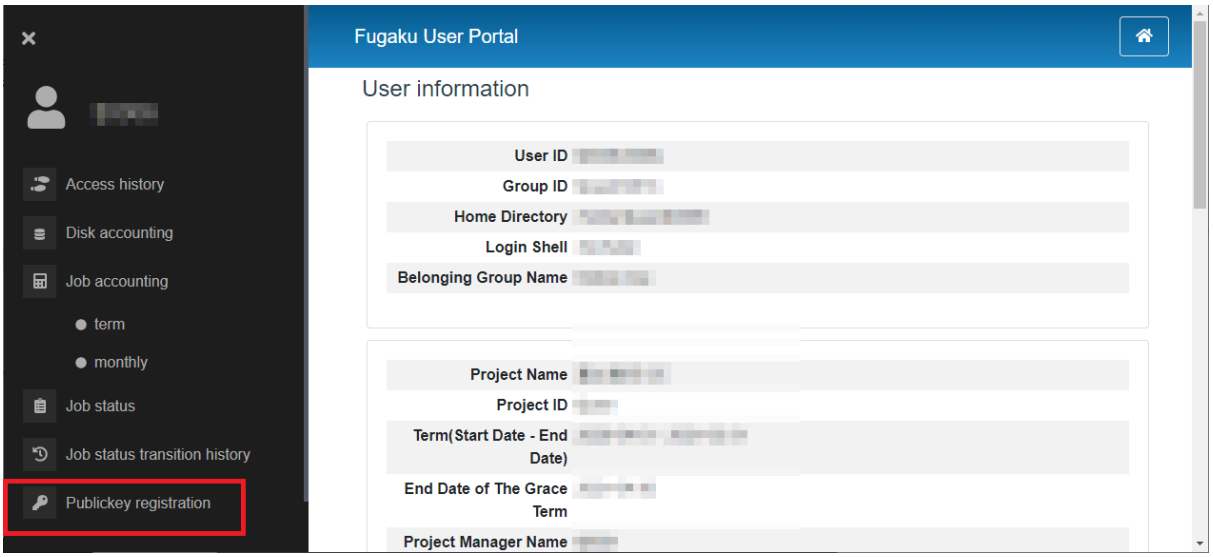
2.4.2 公開鍵登録

- 富岳ウェブサイトを利用した登録
- 公開鍵の追加登録

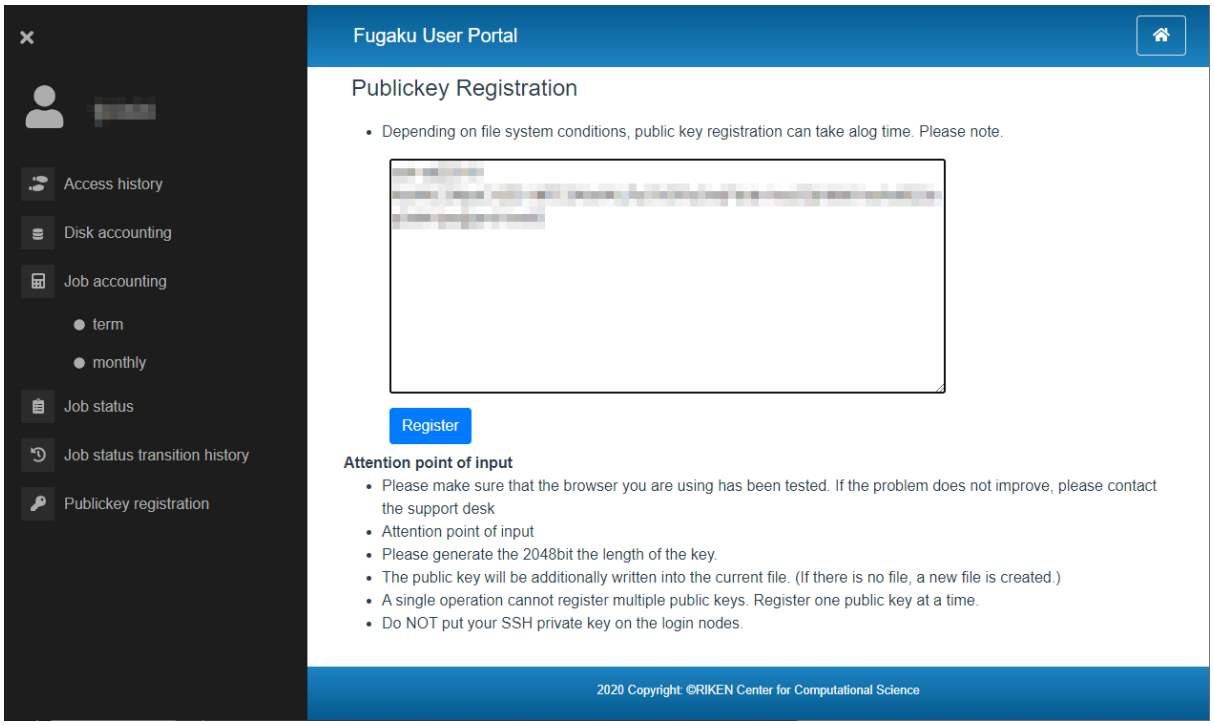
富岳ウェブサイトを利用した登録

1. 富岳ウェブサイト（https://www.fugaku.r-ccs.riken.jp/）にログインし、メニューから *[利用者ポータル]* をクリックします。

2. メニューから *[Publickey registration]* をクリックします。

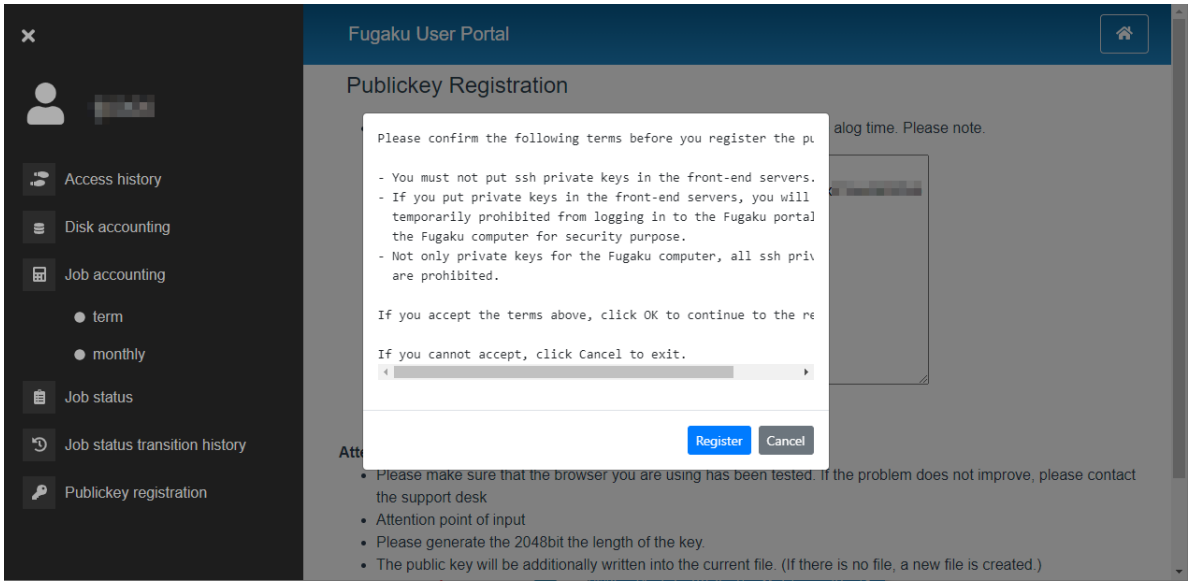


3. 「*Publickey Registration*」欄に利用する公開鍵をコピー＆ペーストします。

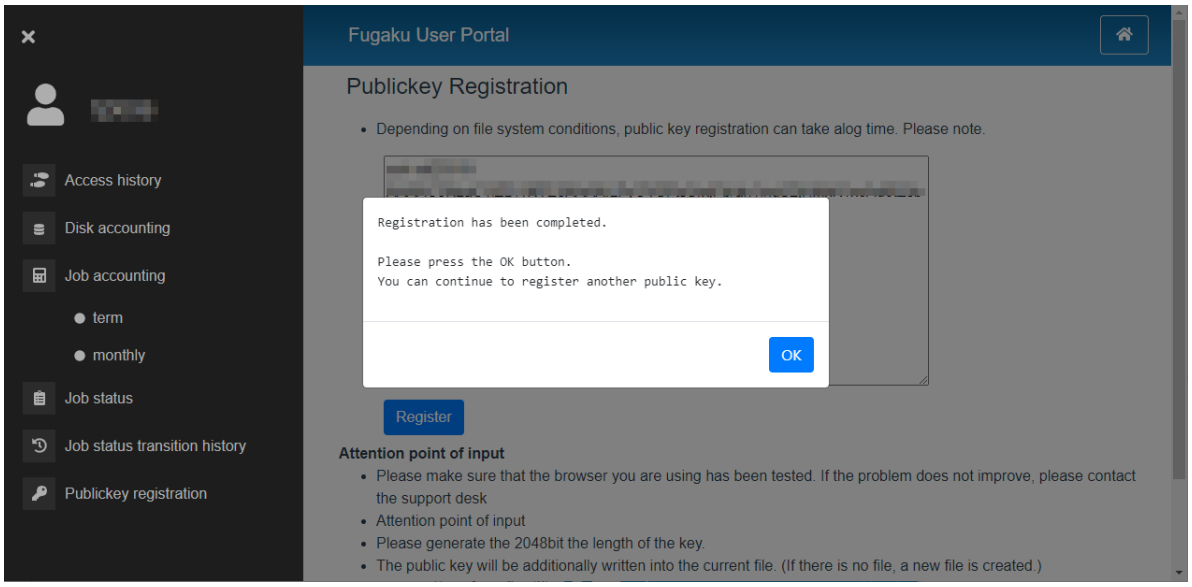


4. *[Register]* ボタンを押します。

5. 内容を確認のうえ *[Register]* ボタンを押します。

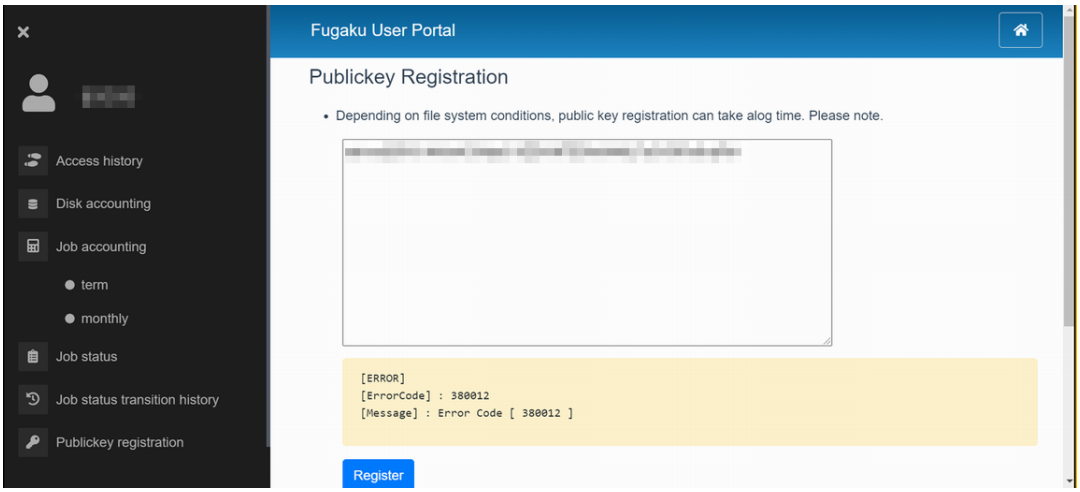


6. 「Registration has been completed.」の画面が表示されると、公開鍵の登録作業は終りです。



注釈: 公開鍵は 1 回の操作で 1 個しか登録できません。2 回目以降の操作では、追加登録となります。2 個以上の公開鍵を登録したい場合には、同様の操作を繰り返してください。

7. 公開鍵が正しくない場合はエラーメッセージが表示されます。公開鍵を確認して再度登録処理を実行してください。



公開鍵の追加登録

ログインノードに公開鍵を追加登録する手順を示します。
富岳ウェブサイトを利用して追加登録する方法と、ログインノードにログインして直接ファイルを編集する方法があります。ここでは、ログインノードでファイルを編集する方法を示します。

1. ログインノードで`~/.ssh/authorized_keys` を編集します。

```
[_LNlogin]$ vi  ~/.ssh/authorized_keys



[i] キーを押下し、vi エディタのインサートモードにします
マウスの右クリックを押下し、.ssh/id_ed25519.pub の内容を貼り付けます

[esc] キーを押下し、[wq!] を入力し、[Enter] キーを押下します
```

2. 公開鍵を登録した authorized_keys のパーミッションを変更します。

```
[_LNlogin]$ chmod  600  ~/.ssh/authorized_keys
```

2.4.3 アクセス方法

スーパーコンピュータ「富岳」へのアクセス方法を示します。

ログインノードにログインするには、「**鍵ペア（秘密鍵／公開鍵）の作成**」の手順を実施し、ログインノードに公開鍵が登録されている必要があります。

プログラム開発（プログラム作成／コンパイル）およびジョブ操作（ジョブ投入／ジョブ状態表示／ジョブ削除）は、ログインノードから実施します。

ログインノード

利用者の端末から、次のホスト名でアクセスします

ホスト名：login.fugaku.r-ccs.riken.jp

ssh コマンドの実行例を示します。

【公開鍵認証】

```
[terminal]$ ssh  username@login.fugaku.r-ccs.riken.jp
The authenticity of host 'XXXXXX (nnn.nnn.nnn.nnn)' can't be established.
XXXXX key fingerprint is XX: XX: XX: XX: XX: XX: XX: XX: XX:XX:XX:XX:XX:XX:XX:XX.
Are you sure you want to continue connecting (yes/no)? yes   # yes を入力（初回）
Enter passphrase for key '/home/groupname/username/.ssh/id_ed25519':  # パスフレーズを入力
[_LNlogin]$
```

1. 初回ログイン時、ホスト鍵の登録について、確認のメッセージ（Are you sure you want to continue connecting）が表示されます。「yes」を入力します。
2. ログインノードへの接続時に X11 Forwarding 機能を有効とする場合は、**ssh** のオプション`-X`を指定してください。
3. ログインノードへの接続時に SSH Agent-forwarding 機能を有効とする場合は、**ssh** のオプション`-A`を指定してください。
4. 複数台のログインノードを運用しています。ホーム領域（`/home`）、データ領域（`/data`）は、各ログインノードで共用します。また、言語ソフトウェアの環境も同じです。

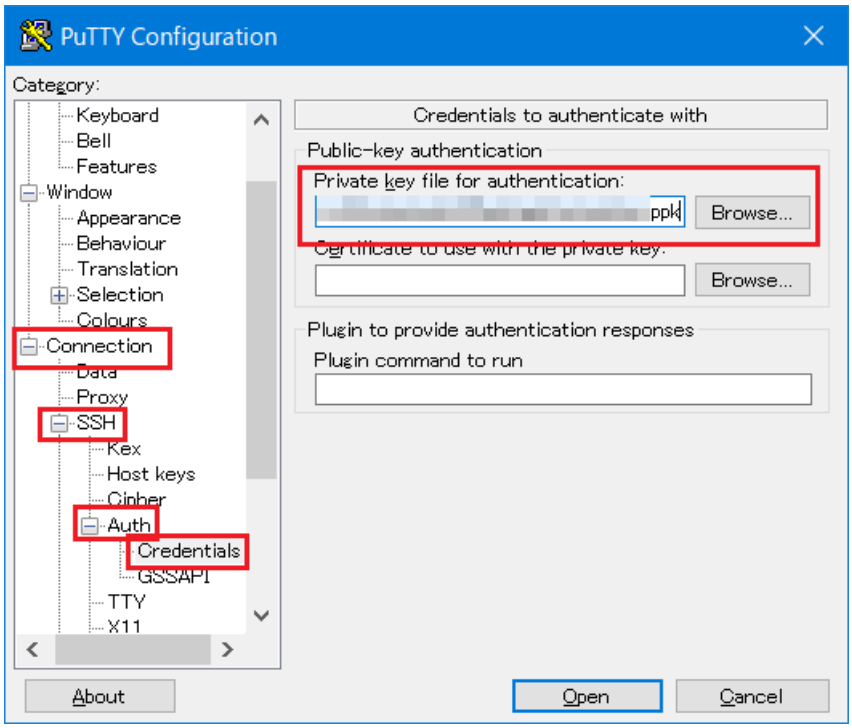
注釈: 鍵ペアの作成時に鍵ファイルのファイル名を入力して作成した場合は、**ssh** コマンドの`-i`オプションで鍵ファイルのファイル名を指定してください。

```
[terminal]$ ssh -i key_filename username@login.fugaku.r-ccs.riken.jp
```

ログインノード（PuTTY）

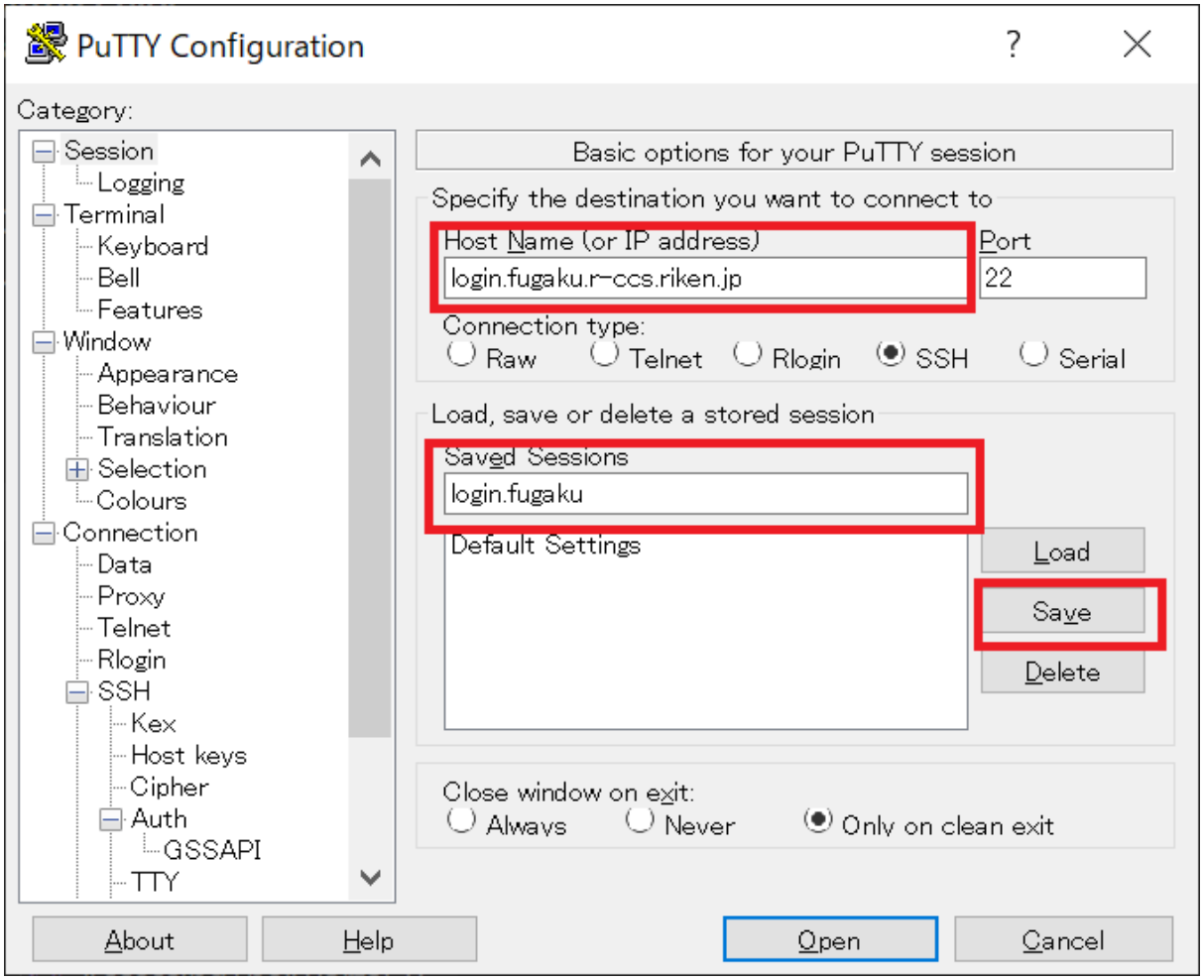
Windows（PuTTY）を使用して、ログインノードにログインする方法を示します。

1. PuTTY を起動します。利用者の端末に保管されている秘密鍵を設定します。
   「*Connection*」 → 「*SSH*」 → 「*Auth*」 → 「*Credentials*」から「*Browse*」ボタンをクリックします。
   puttygen で作成した秘密鍵を選択します。

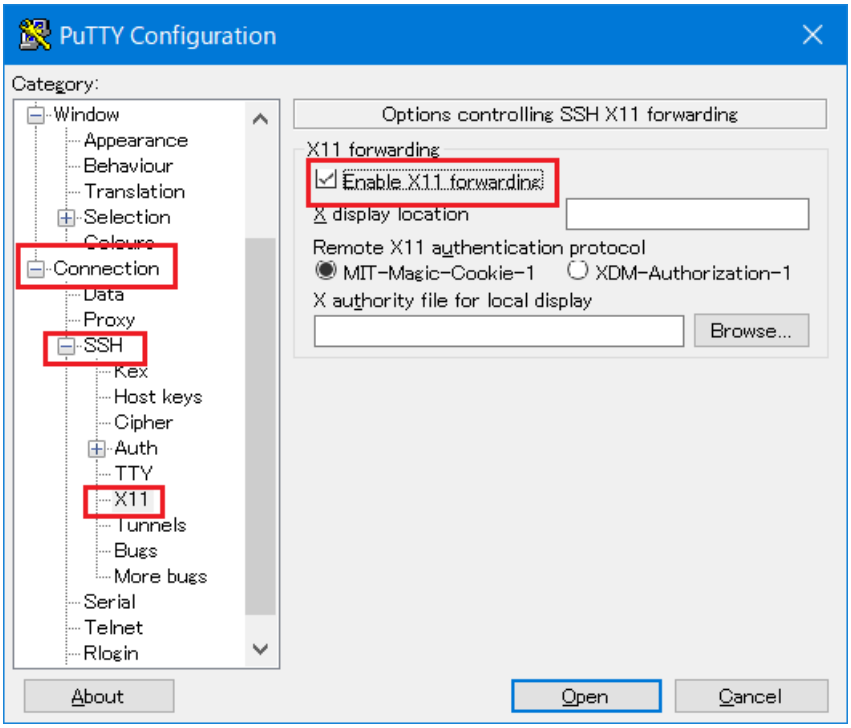


2. 「*Session*」を選択します。

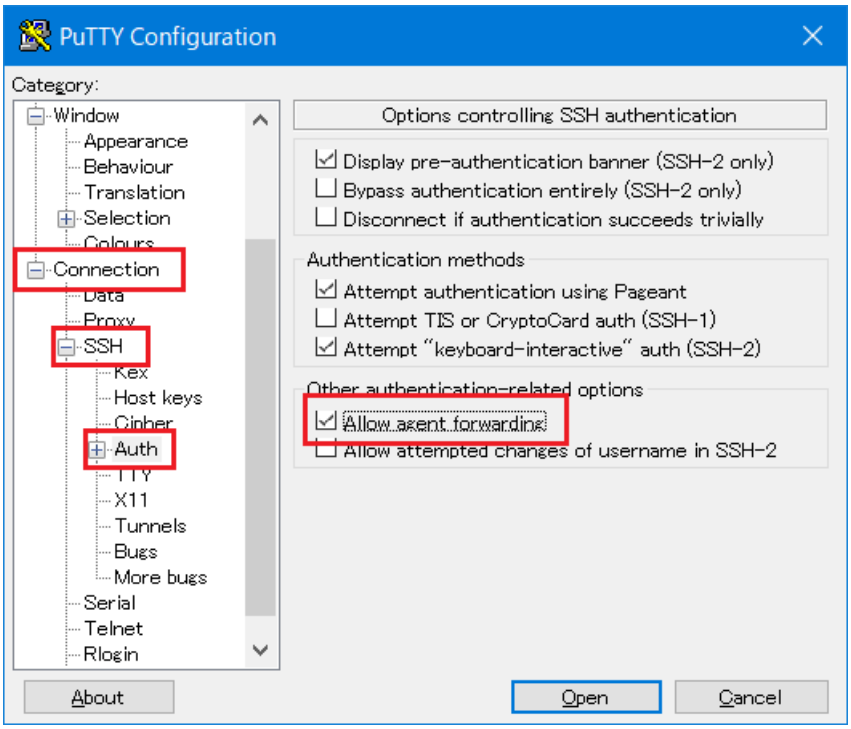
   「*Host Name(or IP address)*」に、ログインノードのホスト名を入力します。設定した内容を保管するため、「*Saved Sessions*」に保管する名前を入力し、「*Save*」ボタンをクリックします。2 回目以降のログイン時は保存した名前を選択し、「*Load*」ボタンをクリックします。



3. ログインノードへ接続時に X11 forwarding 機能を有効とする場合は「*Open*」をクリックする前に「*Connection*」 → 「*SSH*」 → 「*X11*」を開き「*Enable X11 forwarding*」にチェックを入れてください。

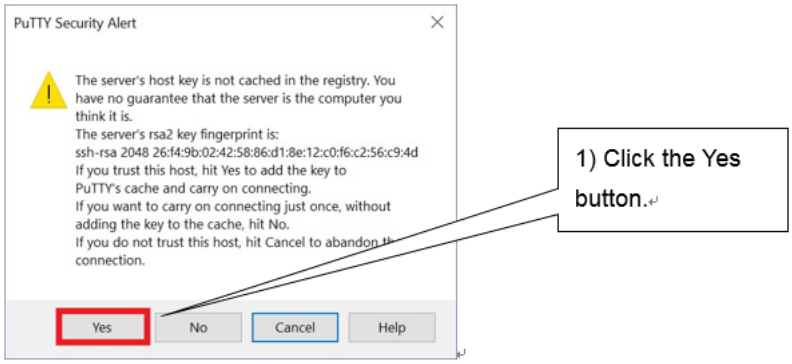


4. ログインノードへ接続時に Agent-forwarding 機能を有効とする場合は「*Open*」をクリックする前に「*Connection*」 → 「*SSH*」 → 「*Auth*」を開き「*Allow agent forwarding*」にチェックを入れて下さい。



5. 「*Open*」ボタンをクリックします。ログインノードへの接続が開始されます。

6. 初回ログイン時、ホスト鍵の登録について、確認画面が表示されます。**「はい (*Y*)」**をクリックします。



8. ローカルアカウント名とパスフレーズを入力し、ログインノードにログインします。

```
login as: username                                    # ローカルアカウント名を入
力
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key": passphrase     # パスフレーズを入力
Last login: Tue Mar 27 09:57:12 2018 from xxx.xxx.xxx.xxx
login$
```

2.4.4 ファイル転送方法

利用者端末にインストールされているファイル転送プログラム（scp ／ sftp）を利用して、ログインノードを経由したファイル転送が可能です。転送には `login.fugaku.r-ccs.riken.jp` を使用できます。

セキュリティに脆弱性のあるプロトコル（ftp ／ r 系コマンド）の利用は禁止しています。

ファイル転送は「**鍵ペア（秘密鍵／公開鍵）の作成**」の手順を実施し、ログインノードに公開鍵が登録されている必要があります。

- **ファイル転送（*sftp*）**
- **ファイル転送（*scp*）**
- *Windows (WinSCP)*

ファイル転送（sftp）

1. **sftp** コマンドの実行例

```
[terminal]$ sftp username@login.fugaku.r-ccs.riken.jp
Enter passphrase for key '/home/groupname/username/.ssh/id_ed25519':  # パスフレーズを入力
sftp>
```

2. ファイル転送例（**put**）

```
sftp> put a.f90
Uploading a.f90 to /home/groupname/username/a.f90
sample.f90                                    100%   18     0.0KB/s   00:00
sftp>
```

3. ファイル転送例（**get**）

```
sftp> get sample.sh.o9110
Fetching sample.sh.o9110 to /home/groupname/username/sample.sh.o9110
sample.sh.o9110                               100%   18     0.0KB/s   00:00
sftp>
```

ファイル転送（scp）

1. **scp** コマンドの実行例を示します。（端末からログインノードへ）

```
[terminal]$ scp  local_file  username@login.fugaku.r-ccs.riken.jp:remote_file
Enter passphrase for key '/home/groupname/username/.ssh/id_ed25519':  #  パスフレーズを入力
[terminal]$
```

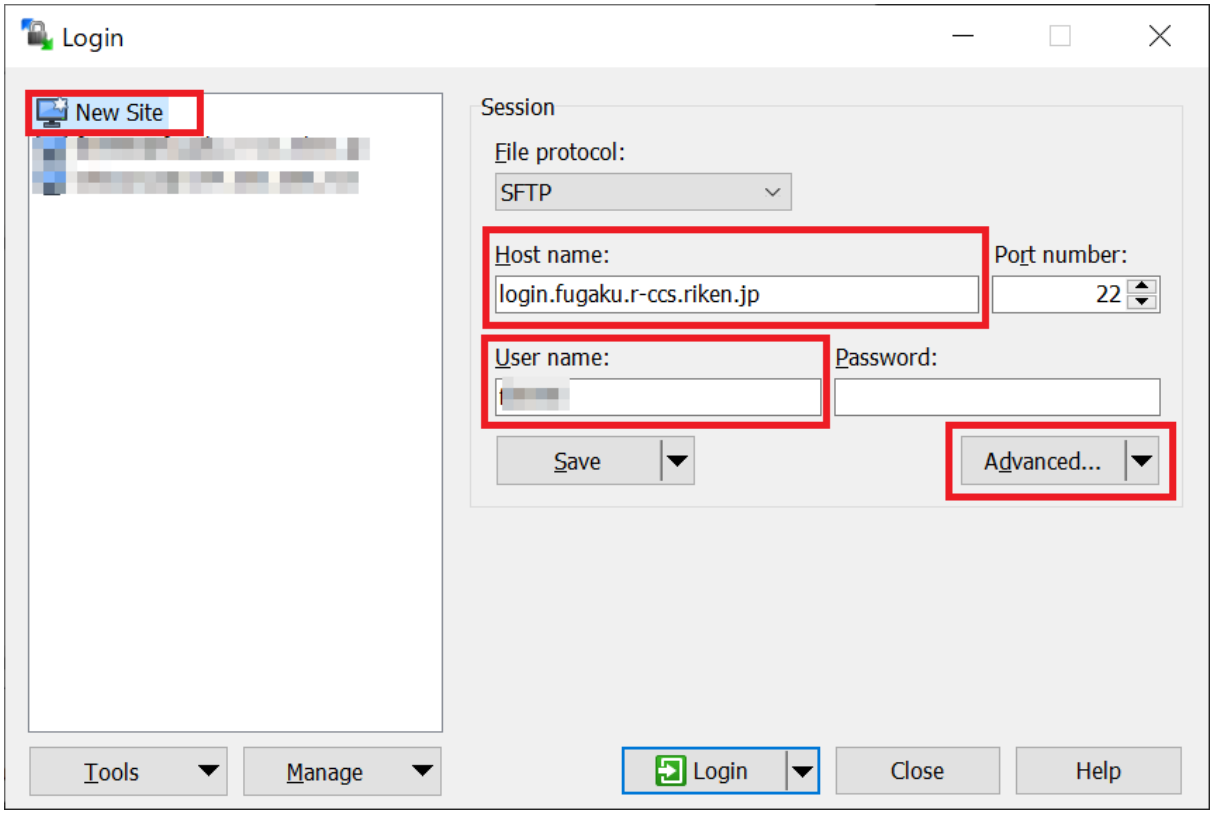
2. **scp** コマンドの実行例を示します。（ログインノードから端末へ）

```
[terminal]$ scp  username@login.fugaku.r-ccs.riken.jp:remote_file  local_file
Enter passphrase for key '/home/groupname/username/.ssh/id_ed25519': #   パスフレーズを入力
[terminal]$
```

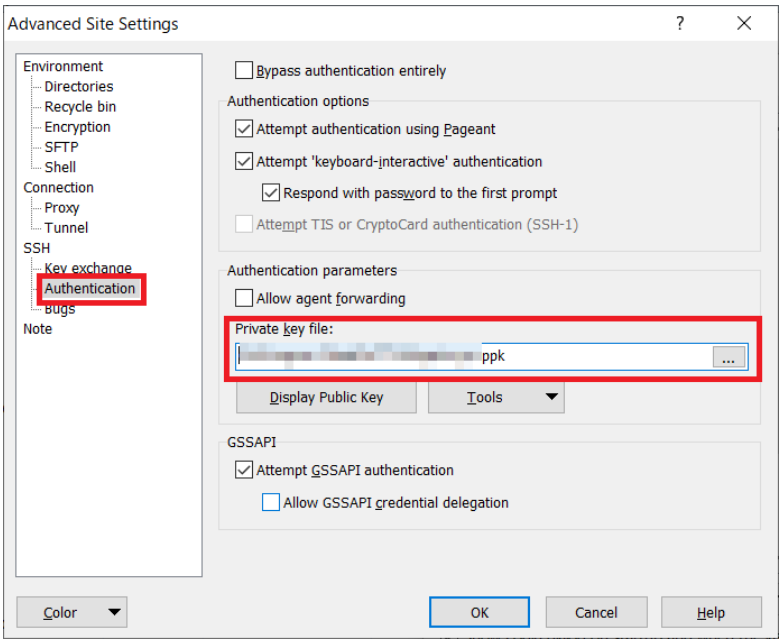
Windows (WinSCP)

Windows 系の場合、WinSCP などのファイル転送プログラムを使用して、ログインノードへファイルを転送します。WinSCP での接続例を示します。

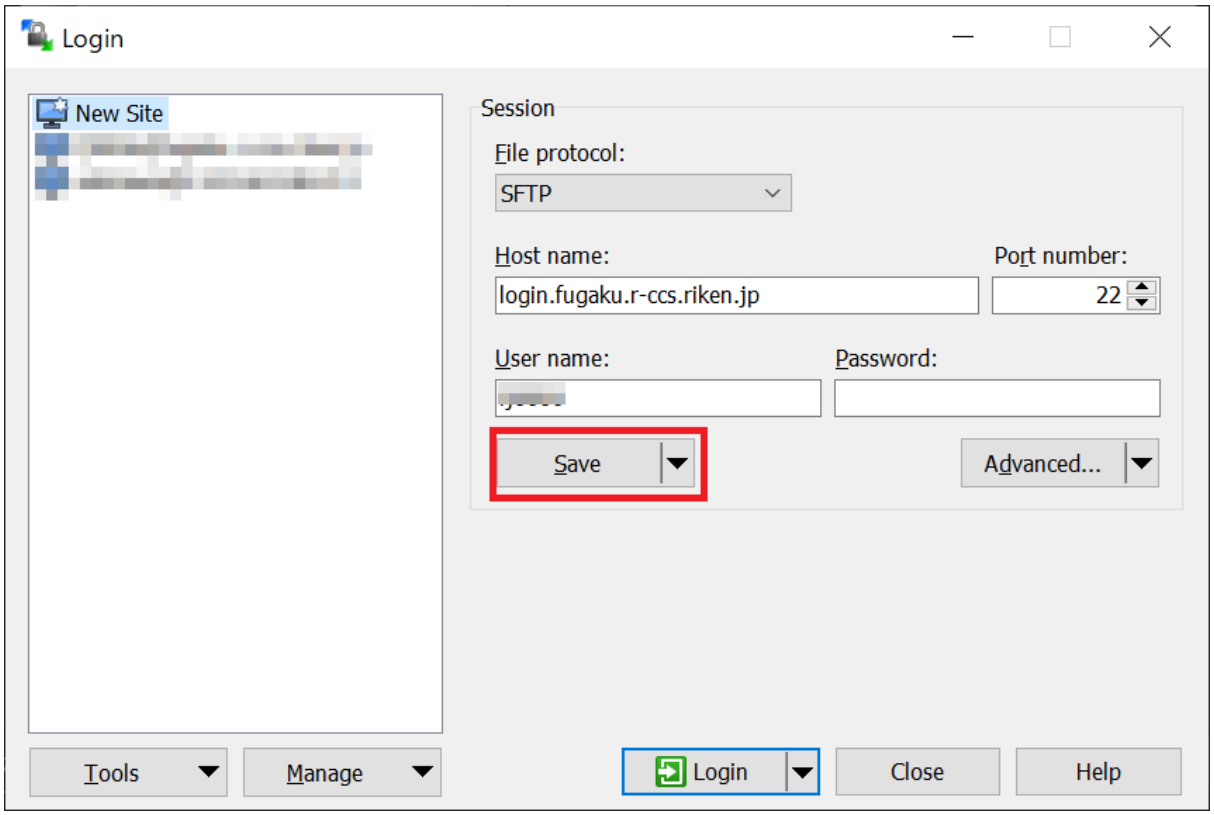
1. WinSCP を起動し、*[New Site]* を選びます。
2. 「*Host name*」にログインノードのホスト名（`login.fugaku.r-ccs.riken.jp`）を入力します。
3. 「*User name*」にユーザ名を入力します。
4. *[Advanced...]* をクリックします。



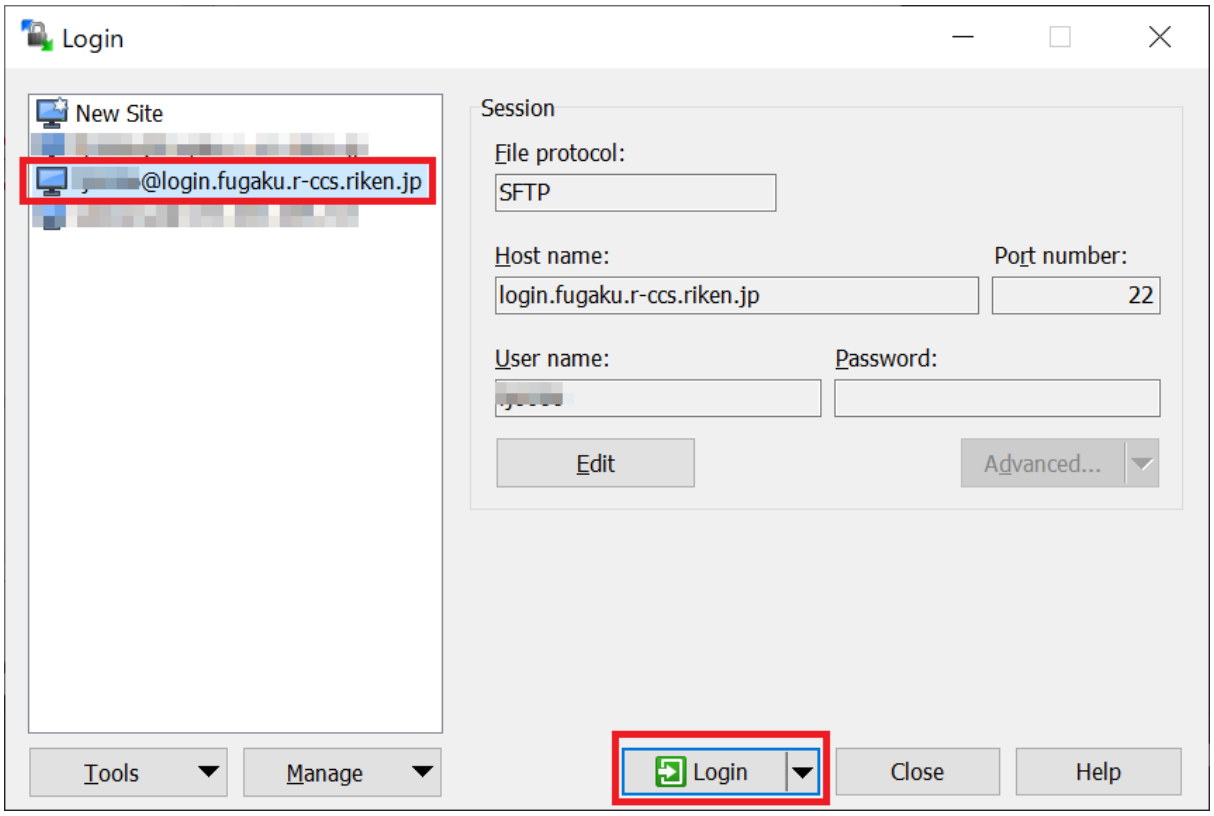
5. *[Authentication]* の「*Private key file*」に putty の秘密鍵ファイル名を設定し、*[OK]* をクリックします。



6. 「*Save*」をクリックし、設定値を保存します。



7. 保存した設定値を選択し、「*Login*」をクリックし接続します。



8. 接続完了後、エクスプローラに似た画面が表示され、ファイルをドラッグ＆ドロップして転送できるようになります。

2.4.5 ログインシェル

ログインシェルは /bin/bash です。

2.4.6 「富岳」運用情報のメール配信

運用情報に関するメールが「富岳」のアカウント（uid）宛に配信されます。
受信するためには、ユーザ自身で転送先のメールアドレスを登録する必要があります（登録しない場合、メールは廃棄されます）。

下記の運用情報に関するメールを配信します。配信内容は順次拡充します。

- システム障害の影響を受けたジョブ情報
- お知らせ情報
- その他

【メールアドレスの登録方法】

ユーザのホームディレクトリに「.forward」ファイルを作成し、転送先のメールアドレスを記載してください。「.forward」の記載例やフィルタリングの設定例などは FAQ を確認してください。

```
[_LNlogin]$ vi ~/.forward
*****@*****.com
```