# 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
1.1	本資料の目的	1
1.2	本書で使用する表記	1
1.3	商標について....................................	1
1.4	更新履歴	2
第2章	システム利用	4
2.1	概要	4
2.2	クライアント証明書のインストール	6
	2.2.1 Firefox への証明書のインストール (Windows)	6
	2.2.2 Firefox への証明書のインストール (Mac)	13
	2.2.3 Chrome への証明書のインストール (Windows)	17
	2.2.4 Chrome への証明書のインストール (Mac)	30
2.3	富岳ウェブサイトへの接続手順....................................	34
2.4	ログイン	37
	2.4.1 鍵ペア(秘密鍵/公開鍵)の作成	38
	2.4.2 公開鍵登録	41
	2.4.3 アクセス方法	45
	2.4.4 ファイル転送方法	49
	2.4.5 ログインシェル	53
	2.4.6 「富岳」運用情報のメール配信	53

# 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

文中の社名、商品名等は各社の商標または登録商標である場合があります。その他の記載されている商標および登録商標については、一般に各社の商標または登録商標です。本資料に掲載されているシステム名、製品名などには、必ずしも商標表示(TM、(R))を付記しておりませんので、ご注意ください。

スタートアップガイド 1.11 版

## 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

©2020 - 2025 理化学研究所 計算科学研究センター

本マニュアルに記載されている内容の無断転載・複製を禁じます。

# 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。

# 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



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

7

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。

## 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

	☆	オプション	× +	-	l		×
¢	$\rightarrow$	C' 🕜	Sirefox aboutpreferences#privacy	111\	•	۲	≣
							^
	ጵ ଜ	一般 ホ−ム	<ul> <li>Firefox があなたに代わって未送信のクラッシュレポートを送信することを許可する(C)</li> <li>詳細情報</li> </ul>				
[	Q  	検索 プライバシーとセキュリ	セキュリティ 「ディ 詐欺コンテンツと危険なソフトウェアからの防護				
		Sync	<ul> <li>✓ 危険な詐欺コンテンツをブロックする(B) 詳細情報</li> <li>✓ 危険なファイルのダウンロードをブロックする(D)</li> <li>✓ 不要な危険ソフトウェアを警告する(C)</li> </ul>				
			<ul> <li>証明書</li> <li>サーバーが個人証明書を要求したとき</li> <li>自動的に選択する(S)</li> <li>毎回自分で選択する(A)</li> </ul>				ļ
	<b>*</b>	拡張機能とテーマ Firefox サポート	✓ OCSP レスホノターサーハーに向い合わせ(証明書の現在の正当性を確認する(Q) 証明書を表示(C) セキュリティデパイス(D)				
							~

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。

		証明書マネージャー			
あなたの証明書	個人証明書	サーバー証明書	認証局証明書	<b>₽</b>	
あなたが認証を受けるため	め以下の証明書	が登録されています			
証明書名と発行者名	セキ	ュリティデバイス	シリアル番号	有効期限	
表示( <u>V</u> ) バッ	7 <i>ア</i> ップ( <u>B</u> )	すべてバックアップ( <u>K</u> )	インポート( <u>M</u> )	削除( <u>D</u> )	
表示( <u>U</u> ) バック	7アップ( <u>B</u> )	すべて <i>バッ</i> クアップ( <u>K</u> )	インポート( <u>M</u> )	削除( <u>D</u> )	OK

スタートアップガイド 1.11 版

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。

●● インポートする証明書ファイル	×
← → × ↑ 🔜 > PC > デスクトップ > 🗸 ∨ ひ	デスクトップの検索・
整理 ▼ 新しいフォルダー	
PC TXDFvyT Image: plane in the plane in	
ファイル名( <u>N</u> ): p12 ~	PKCS12 のファイル (*.p12;*.pfx) 〜 開く( <u>O</u> ) キャンセル

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。

パスワード	を入力してください - Mozilla Firefox	$\times$					
?	この証明書のバックアップの暗号化に用いるパスワードを入力してくださ い:						
	ОК <b></b> <i><b>†</b><i>тути</i></i>						

**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。

スタートアッフカイト 1.11 fi
--------------------

		証明書マネージャー			×
あなたの証明書	個人証明書	サ−バ−証明書	認証局証明書		
あなたが認証を受けるため	り以下の証明書は	が登録されています			
証明書名と発行者名	セキコ	リティデバイス	シリアル番号	有効期限	
✓ RIKEN Center for	ompu				
1000	Softwa	are Security Device		年月1日	
表示( <u>V</u> ) バック	7アップ( <u>B</u> )	すべてバックアップ( <u>K</u> )…	インポート( <u>M</u> )	削除( <u>D</u> )	
				(	ЭК

## 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。

## スタートアップガイド 1.11 版

		証明書マネージャ	-	×
あなたの証明	書個人証明書	サーバー証明	書認証局証	E明書
認証局を識別す	るため以下の証明書が登	録されています		
証明書名と発	行者名	t	?キュリティデバイス	
QuoVadis	s Root CA 1 G3	Bu	iltin Object Toker	ı '
QuoVadis	s Root CA 2 G3	Bu	iltin Object Toker	1
QuoVadis	s Root CA 2	Bu	iltin Object Toker	ı
QuoVadis	s Root CA 3	Bu	iltin Object Toker	1
✓ RIKEN Center	er for Computational S	cience		
RIKEN R-	ccs	So	ftware Security D	evice
✓ SECOM Trus	st Systems CO.,LTD.			
Security C	Communication RootC	A2 Bu	iltin Object Toker	1
✓ SECOM Trus	st.net			•
表示( <u>V</u> )	信頼性を設定( <u>E</u> )	インポート( <u>M</u> )	エクスポート( <u>X</u> )	削除または信頼しない(D)
				ОК

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。

🔆 オブション X about:ce	tificate × +	-		×
$\leftrightarrow \rightarrow$ C $\textcircled{o}$ $\textcircled{o}$ Firefox abo	ıt:certificate?cert=MIIEjDCCA3SgAwIBAgIJAJZ7a3qmLMujMA0GCSqGSIb3DQEBCwUAMIGJN	il\ 🗊	۲	≡
Not Before	2020/2/27 10:45:20 (Asia/Tokyo)			^
Not Alter	2030/3/31 10:43:20 (130) 10(30)			
Public Key Info		-		
Algorithm	RSA			
Key Size	2048			
Exponent	65537			
Modulus	C1:A8:60:B7:F5:29:69:D9:E4:18:AA:60:2D:F5:12:41:F5:59:F6:8B:99:97:D7:BE:AA:AD:0A:BE:EC:75:78:C0:F5:9C:9E	:F4:EF:		
Miscellaneous		_		
Serial Number	00:96:7B:6B:7A:A6:2C:CB:A3			
Signature Algorithm	SHA-256 with RSA Encryption			
Version	3			
ダウンロード	PEM (cert) PEM (chain)			
Fingerprints		_		
SHA-256	BB:C0:5C:EB:0E:41:5B:00:FC:A3:0B:1C:21:70:0B:3B:26:A6:AF:9B:BD:FD:E4:40:C6:26:32:03:26:7B:3B:33			
SHA-1	EE:ED:84:6F:FC:73:3A:73:32:8F:45:61:39:BD:B9:95:D5:17:4B:BC			
Basic Constraints	Vac			
Certificate Authority	Tes			
Subject Key ID		-		
Key ID	97:E9:81:97:45:53:E3:FB:CB:09:47:E3:1C:7A:BE:61:B3:80:A5:61			
Authority Key ID				
Key ID	31,23,01,31,43,23,23,13,22,03,41,23,1C,1A,02,01,03,01,01			~

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。

		Q オプションを検索
✿ 一般	Firefox にパーソナライズされた拡張機能のおすすめを許可する 詳細情報	
<b>∧</b> ±_/.	Firefox に調査のインストールと実行を許可する Firefox 調査を確認する	
	Firefox があなたに代わって未送信のクラッシュレポートを送信することを許可する(	<u>C</u> ) 詳細情報
<b>Q</b> 検索		
🔒 プライバシーとセキュリティ		
	セキュリティ	
Sync	詐欺コンテンツと危険なソフトウェアからの防護	
	✓ 危険な詐欺コンテンツをブロックする(B) 詳細情報	
	✓ 危険なファイルのダウンロードをプロックする(D)	
	✓ 不要な危険ソフトウェアを警告する(C)	
	証明書	
	サーバーが個人証明書を要求したとき	
	○ 自動的に選択する(S)	
	<ul> <li>毎回自分で選択する(A)</li> </ul>	
	✓ OCSP レスポンダーサーバーに問い合わせて証明書の現在の正当性を確認する(Q)	】 証明書を表示…( <u>C</u> )
▶ 拡張機能とテーマ		セキュリティデバイス…( <u>D</u> )
⑦ Firefox サポート		

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。

## スタートアップガイド 1.11 版

	デバイスマネーシ	ゲヤー	
セキュリティモジュールとデバイス	詳細	[1] [值] [] [] [] [] [] [] [] [] [] [] [] [] []	ログイン( <u>N</u> )
<ul> <li>NSS Internal PKCS #11 Module</li> </ul>	状態	ログイン済み	ログアウト(〇)
Generic Crypto Services	詳細説明	PSM Private Keys	
Software Security Device	製造元	Mozilla.org	パスワードを変更( <u>P</u> )
<ul> <li>Builtin Roots Module</li> </ul>	ハードウェアバージョン	3.50	· 自力17(1)
NSS Builtin Objects	ファームウェアバージョン	0.0	λ⊡/JH( <u></u> L)
	ラベル	Software Security Device	削除( <u>U)</u>
	製造元	Mozilla.org	FIPS を有効にする(F)
	シリアル番号	000000000000000000000000000000000000000	
	ハードウェアバージョン	0.0	
	ファームウェアバージョン	0.0	
			ОК

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

マスターパスワードの変更			×
セキュリティデバイス: unde	fined		
現在のパスワード:			
新しいパスワード:	•••••	•••••	
新しいパスワード(再入力):	•••••	•••••	
パスワードの品質レベル			
	ОК	キャンセル	

 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。

🗯 Firefox File Edit	t View History B	ookmarks Tools	Window Help	1				چ 🌗	Ka A	Mon 17:44		Q ::	Ξ
About Firefox	×	+											
Preferences	🕷, 🔍 Search w	ith Google or enter	address						~		lii\ 🗊	۲	≡
Services	•												
Hide Firefox Hide Others Show All	ЖН ЖН	G Search the	Web				$\rightarrow$					¢	
Quit Firefox	жQ												
	Top Sites 🗸												
	<ul> <li>emazon</li> <li>Highlights &gt;</li> </ul>	youtube	facebook	wikipedia	reddi	twitter							

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。

Ś.	Firef	ox File	Edit	View	History	Bookmarks	То	ols Win	wob	Н	Help											0 1	<u></u>	② A	Mon 1	7:46	100		Q #	Ξ
••		\$ F	reference	5	>	× +																								
€⇒	• •	" @			<b>O</b> Firefox	about:prei	ferenc	esäprivad	y															☆			111	1	۲	≡
																Q F	ind in P	reference	!S											
×	<b>b</b> 0	General			Secu	irity																								
ú	ን ዞ	lome			Decep	ptive Cont	tent a	and Dan	gero	ous	s Sol	ftwai	re Pro	otectio	on															
C	λs	earch			V Blo	ock danger	ous ar	nd decep	tive c	cont	ntent	Lear	n more	е																
í í	} ₽	rivacy 8 Sync	Securi	ty	✓ ✓	Block dan Warn you	igerou abou	us downlo t unwante	ads ed an	nd u	unco	mmor	n softw	vare																
					Certif	ficates																								
					When a	a server rec	quest	s your pe	rsona	al ce	certifi	cate																		
					🔵 Se	elect one au	toma	tically																						
					As	sk you every	/ time													_										
		vtension	& Thom	105	✓ Qu cer	uery OCSP r rtificates	respo	nder serv	ers to	:o c	confir	m the	e curre	ent valid	dity of		View	Certifi	cates											
		ALCHISION:	oc men	10.0													Sect	unty De	vices											
G	υF	irefox Su	oport																											

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。

スタートアップガイド 1.11 版

		Ce	rtificate M	lanager				
	Your Certific	ates	People	Serve	rs	Authoriti	ies	
Certificate N	Name	Security [	Device	Serial N	umber	Exp	ires On	E
View	Backup	Backu	ıp All	Import	Delet	e		
View	Backup	Васки	ıp All	Import	Deleti	ê		ок

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。

2	Password Required - Mozilla Firefox
	Please enter the password that was used to encrypt this certificate backup:
	Cancel OK

**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。

1	Alert Successfully restored your security certificate private key(s).	(s) and
		OK

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。

🗯 Firefox File Edit View	History Bookmarks Tools Window Help	U 🗟 😡 🛛	Tue 11:41 Q :Ξ
Preferences	× +		
← → ♂ ✿	Sirefox about:preferences#privacy	\$	II\ ⊡ ® ≡
☆ General û Home	Q. Find in Preferences Security Deceptive Content and Dangerous Software Protection		
<b>Q</b> Search	✓ Block dangerous and deceptive content Learn more		
Privacy & Security Sync	<ul> <li>Block dangerous downloads</li> <li>Warn you about unwanted and uncommon software</li> </ul>		
<ul> <li>Extensions &amp; Themes</li> <li>Firefox Support</li> </ul>	Certificates         When a server requests your personal certificate         Select one automatically         Ask you every time         Query OCSP responder servers to confirm the current validity of certificates         View Certificates		

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。

## スタートアップガイド 1.11 版

	Device Ma	nager	
Security Modules and Devices	Details	Value	Log In
<ul> <li>NSS Internal PKCS #11 Module</li> </ul>	Status	Ready	
Generic Crypto Services	Description	PSM Private Keys	Log Out
Software Security Device	Manufacturer	Mozilla.org	Change Password
Builtin Roots Module	HW Version	3.50	
NSS Builtin Objects	FW Version	0.0	Load
	Label	Software Security Device	Unload
	Manufacturer	Mozilla.org	
	Serial Number	000000000000000000000000000000000000000	Enable FIPS
	HW Version	0.0	
	FW Version	0.0	
			-
			OK

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

Current password:	(not set)
New password:	
New password (again	):
Password quality met	er

10. OK をクリックします。

Current password:	(not set)
New password:	
New password (again)	
Password quality mete	er

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。

• 設定 × +			-		×
$\leftrightarrow$ $\rightarrow$ C $\odot$ Chrome   chrome://sett	tings/privacy	☆	0	* 6	) :
設定	Q 設定項目を検索				
L Google の設定	プライバシーとセキュリティ				
<ul> <li>■ 日販入刀</li> <li>● 安全確認</li> </ul>	■ 問見理歴データの剤除 問見理歴、Cockle、キャッシュなどを削除します	•			
<ul> <li>プライバシーとセキュリティ</li> <li>デザイン</li> </ul>	Cookle と他のサイトデータ シークレット モードでサードパーティの Cookle がブロックされています	+			
<ul> <li>Q、 検索エンジン</li> </ul>	<ul> <li>セキュリティ</li> <li>セーフブラウジング(危険なサイトからの保護機能)などのセキュリティ設定</li> </ul>	•	]		
<ul> <li>         一 既定のブラウザ     </li> <li>         ① 起動時     </li> </ul>	サイトの設定     サイトが使用、表示できる情報(位置情報、カメラ、ボッブアップなど)を制御します	•			
詳細設定	デザイン				
拡張機能	テーマ Chrome ウェブストアを競さます	Ø			
	ホームボタンを表示する 停止中				
	ブックマーク バーを表示する				
	フォントサイズ 中 (推奨)	-			
	フォントをカスタマイズ	•			

2. [証明書の管理] をクリックします。

## スタートアップガイド 1.11 版

		-	I		×
$\leftarrow$ $\rightarrow$ $C$ $\odot$ Chrome   chrome://settin	ngs/security	0	*	θ	:
設定	Q、 設定項目を検索				
<ul> <li>Google の設定</li> <li>自動入力</li> <li>安全確認</li> <li>プライパシーとセキュリティ</li> <li>デザイン</li> <li>快索エンジン</li> <li>同たのブラウザ</li> <li>(リ 起動時</li> <li>詳細設定</li> </ul>	Chrome に称すされている安全でないサイトのリストとURL を務合します。サイトガリスクード II. を不正に取得しようとしている場合や、ユーザーが全空でないフィリルをがウンロードしようと した場合は、URL とページコンテンツの一部をセーフブラウジングに送信することがあります。 すべてのユーザーのウェブ上のセキュリティ猩化に協力する 新たな脅威の発見と、すべてのウェブユーザーの体膜に協立てるため、アクセスした一部のペ ージの URL、限定的なシステム情報、一部のページコンテンツを Google に送信します。 データ受害により(スワードが満受した場合に警告する Chrome では、定期時にパスワードをオンライン上の公開リストと居合し、確認しています。 その際、「スワードとユーザー名は Google を含め進せ詰み取ることができないよう暗号化さ れます。この機能は Google アカウントにログインすると有効になります。 伊護なし (推奨されません) 〇 危険なウェブサイト、ダウンロード、鉱活機能から停躇されていません。セーフブラウジングによる保 選は、Gmail や Google 検索など他の Google サービスで利用可能な場合は、引き技き有効です。				•
拡張機能 [2]	詳細設定				
Chrome (こついて	ゼキュア DNS を使用する この設定は管理対象のブラウザでは無効です				
	証明書の管理 HTTPS / SSLの証明書と設定を管理します				
	Google の高度な保護機能プログラム     図       個人の Google アカウントを標的型攻撃から保護します     ビ				Ţ

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。

0	証明書マネージャ		
	ローカル証明書	ユーザーの証明書	
<b>1</b>	ユーザーの証明書	クライアント証明書は、他のサーバーに対してユーザーの認証を行う証明書です。	
0	Chrome Root Store	ウインドウ	
		Windows からインポートした証明書を表示する	•
		Windows からインポートした証明書を管理する	Ľ

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。

## 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

証明書						×	
目的( <u>N</u> ):	<すべて>					~	
個人 ほかの人 中日	間証明機関(言	頼されたルート証	明機関	信頼された	発行元	信頼されな	
発行先	発行者	有効期	フレンド	リ名			
10000							
1000	5.55 (7						
インポート( <u>1</u> )… エクスネ	ポート( <u>E</u> )	削除( <u>R</u> )				詳細設定( <u>A</u> )	
証明書の目的							
						表示( <u>V</u> )	
						閉じる( <u>C</u> )	

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。

←   髪 証明書のインポート ウィザード	×
証明書のインポート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明 アにコピーします。	月書スト
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセ ィで保護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明 保管されるシステム上の領域です。	キュリテ 明書が
続行するには、[次へ] をクリックしてください。	
次へ(N)	キャンセル

6. [**参照**] をクリックします。

←   髪 証明書のインポート ウィザード	×
インポートする証明書ファイル	
インポートするファイルを指定してください。	
ファイル名( <u>F</u> ): 参照( <u>R</u> )…	
注意:次の形式を使うと1つのファイルに複数の証明書を保管できます:	
Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)	
Microsoft シリアル化された証明書ストア (.SST)	
次へ( <u>N</u> ) キャンセノ	L

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

スタートアップガイド 1.11 版

◎ 開<			×
← → ~ ↑ 🗖 > PC > デスクトップ >	~ 0	デスクトップの検索	,o
整理 ▼ 新しいフォルダー			?
<ul> <li>UsageRules</li> <li>OneDrive</li> <li>PC</li> <li>3D オブジェクト</li> <li>ダウンロード</li> <li>デスクトップ</li> <li>デスクトップ</li> <li>ドキュメント</li> <li>ビクチャ</li> <li>ビブテオ</li> <li>シュージック</li> <li>ローカルディスク (C</li> </ul>			
Jアイル名( <u>N</u> ):	~	Personal Information Exchan Y 509 短阳史 (Acertacit) Personal Information Exchan	ge ge (*.pfx;

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。

◎ 開<			×
← → ∨ ↑ 🗖 > PC > デスクトップ >	~ Ū	デスクトップの検索	م
整理 ▼ 新しいフォルダー			
<ul> <li>UsageRules</li> <li>OneDrive</li> <li>PC</li> <li>3D オブジェクト</li> <li>ダウンロード</li> <li>デオスクトップ</li> <li>デキュメント</li> <li>ビクチャ</li> <li>ビブオ</li> <li>ミュージック</li> <li>ローカル ディスク (C</li> </ul>			
ファイル名(N):p12	~	Personal Information Ez	xchange 〜 キャンセル

9. ファイル名を設定した後、[次へ]をクリックします。

← 🛿 参 証明書のインポート ウィザード	×
インポートする証明書ファイル	
インポートするファイルを指定してください。 	
ファイル名(F): C:¥Users¥p12 参照( <u>R</u> )	
注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます: Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)	
Microsoft シリアル化された証明書ストア (.SST)	
次へ( <u>N</u> ) キャンセノ	

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。 スタートアップガイド 1.11 版

←   髪 証明書のインポート ウィザード	×
秘密キーの保護 セキュリティを維持するために、秘密キーはパスワードで保護されています。 	
秘密キーのパスワードを入力してください。	
パスワード( <u>P</u> ): ●●●●●●● □ パスワードの表示( <u>D</u> )	
インポート オプション(!): 「 秘密キーの保護を強力にする(E) このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を や、キュー	求めら
<ul> <li>□ このイ モエンスボ ト う 能に う る(<u>M</u>) キーのバックアップやトランスポートを可能にします。</li> <li>□ 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(<u>P</u>)</li> <li>☑ すべての拡張プロパティを含める(<u>A</u>)</li> </ul>	
次へ( <u>N</u> )	キャンセル

**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。

<i>§</i> 7	証明書のインポート ウィザード	
証	明書ストア	
	証明書ストアは、証明書が保管されるシステム上の領域です。	
	Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。	5
	● 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(U)	
	○ 証明書をすべて次のストアに配置する( <u>P</u> )	
	աዓ音ストア: 個人 参照( <u>R</u> )	
	次へ(N) キャ	ッンセル

12. **[完了]** をクリックします。

←   髪 証明書のインポート ウィザード		×
証明書のインポート ウィザードの完了		
[完了] をクリックすると、証明書がインポートされます。		
次の設定が指定されました:		
選択された証明書ストア ウィザードで自動的に決定されます		
内容 PFX	10	
ファイル名 C:¥Users¥	.p12	
	完了(E) キャンセ	211

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。

新しい秘密交換	奥キーをインポートします	×
	アプリケーションは保護されたアイテムを作成しています	t.
	CryptoAPI 秘密キー	
	セキュリティ レベル - 中 セキュリティ レベルの	設定( <u>S</u> )
	OK キャンセル 詳細	細( <u>D</u> )

14. [高] をチェックし、[次へ] をクリックします。

セキュリティレベルの選択	×
	このアイテムに適切なセキュリティレベルを選択してください。
	●高(日) このアイテムが使用されるときに、私の許可とパスワードが必要 です。
	○中(M) このアイテムが使用されるときに、私の許可が必要です。
	< 戻る 次へ( <u>N</u> ) > キャンセル

15. パスワードを設定し、[完了] をクリックします。

スタートアップガイド 1.11 版

パスワードの作成		$\times$
	このアイテムを保護するための、パスワードを作成します。	
	このアイテム用に新しいパスワードを作成する。 CryptoAPI 秘密キーのパスワード:	
	パスワード: ●●●●●●●●●● 確認入力: ●●●●●●●●●●	
	< 戻る 完了(E) キャンセル	,

16. [OK] をクリックします。

新しい秘密交打	奥キーをインポートします		×
	アプリケーションは保護された	とアイテムを作成しています。	
	CryptoAPI 秘密キー		
	セキュリティ レベル - 高	セキュリティ レベルの設定(	<u>S</u> )
	OK	キャンセル 詳細( <u>D</u> )	

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。

セキュリティ	整告	$\times$
	発行者が次であると主張する証明機関 (CA) から証明書をインストールしようと しています:	
	RIKEN R-CCS	
	証明書が実際に "RIKEN R-CCS" からのものであるかどうかを検証できません。 "RIKEN R-CCS" に連絡して発行者を確認する必要があります。次の番号はこ の過程で役立ちます:	
	拇印 (sha1): EEED846F FC733A73 328F4561 39BDB995 D5174BBC	
	警告: このルート証明書をインストールすると、この CA によって発行された証明書は自 動的に信頼されます。確認されていない拇印付きの証明書をインストールするこ とは、セキュリティ上、危険です。[はい] をクリックすると、この危険を認識したこと になります。	
	この証明書をインストールしますか?	
	はい(Y) しいいえ(N)	

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。

スタートアップガイド 1.11 版

証明書				×
目的( <u>N</u> ):	<র্বে^<>			~
個人 ほかの人 中	間証明機関 信頼さ	れたルート証明機関	信頼された発行元	信頼されな
発行先	発行者 RIKEN R-CCS	有効期 2020/0	J名	
インポート(」) エクス	スポート( <u>E</u> ) 削除	:( <u>R</u> )		詳細設定( <u>A</u> )
証明査の日的				表示( <u>V</u> )
				閉じる( <u>C</u> )

## 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。

Enter the password for "p1/2":	
Pozsword:	
Show password	
Cancel	ОК

**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。

Click to lock the login keychain.       Q. Search         Keychains       RiKEN R-CCS         Local Items       System         System       RikeN R-CCS" certificate authority         System Roots       RikeN R-CCS" certificate is not trusted         Name       Kind       Expires       Key         Regence       RikeN R-CCS       certificate       login         Name       Kind       Expires       Key         Regence       Category       RikeN R-CCS       certificate       login         All Items       Secure Notes       My Certificates       Vertificates       Local Items         Keys       Certificates       Local Items       Local Items       Local Items       Local Items       Local Items       Key         Category       All Items       Keys       Local Items       Local	•••		Keychain Access				
Keychains       PIKEN R-CCS         System       System Roots         Regeneration       PIKEN R-CCS" certificate is not trusted         Regeneration       PIKEN R-CCS" certificate is not trusted         Regeneration       Riken R-CCS" certificate is not trusted         Regeneration       Riken R-CCS" certificate is not trusted         Regeneration       Riken R-CCS         Category       Riken R-CCS         All Items       Passwords         Secure Notes       Nortificates         Wy Certificates       Vertificates         Keys       Certificates         Certificates       Vertificates         Keys       Certificates	Click to lock the lo	ogin keychain.	chain.			Q Search	
Name       Kind       Expires       Key         Certificate       logir       logir       logir         RIKEN R-CCS       certificate       Mar 31, 2036 10:45:20       logir         All Items	Keychains fogin focal Items System System Roots	Certificate Suit	RIKEN R-CCS Root certificate authority Expires: Monday, March 31, 2036 10:45:20 Japan Sta RIKEN R-CCS" certificate is not trusted	indard Time			
Category       All Items         All Items       Secure Notes         Wy Certificates       Wy Certificates         W Keys       Category		Name	^	Kind	Expires	Keychain	
Category       All Items         ▲ All Items       Secure Notes         ■ My Certificates       War 31, 2036 10:45:20         ● Secure Notes       Secure Notes         ■ My Certificates       Secure Notes         ● Keys       Secure Inficates		▶ 📴		certificate		login	
	Category All Items L. Passwords Secure Notes My Certificates Keys Certificates						
i Copy     2 items		+ i Co	Dy	2 items			

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

スタートアップガイド 1.11 版

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。

$\bigcap_{i=1}^{n}$	You are making changes to your Certificate Trust Settings.	
2	Enter your password to allow this.	
	User Name:	
	Pazeword: 0000000	
	Cancel Update Settings	

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。

•	•	Keychain Access		
	Click to lock the lo	gin keychain.	Q Sear	ch
<b>-</b>	Keychains Iogin Local Items System System Roots	Certificate Guadad Control Con		
		Name   Kind Date Modified	Expires	Keychain
		P <key> public key</key>		login
		<pre></pre>		login
		🛴 Apple Persistent State Encryption application password Vesterday, 13:34		login
		🛴 Chrome Safe Storage application password Yesterday, 18:35		login
		🛴 com.apple.ids2cb5c-AuthToken application password Mar 13, 2020 17:06:55		login
		🛴 com.apple.scokmarksagent.xpc application password Yesterday, 17:37		login
		cartificata		login
	Category	P New Identity Preference		login
R	All Items	Loopy " 3, 2020 17:06:54		login
1	Passwords	lids: identity-ry-pair-sig		login
-	Secure Notes	ids: identity-rsa-private- 3, 2020 17:06:54		login
1	My Cortificator	k ids: identity-rsa-public- Export " 3, 2020 17:06:54		login
(2)	Wry Certificates	k ids: unregistege-protec 3, 2020 17:06:54		login
T	Keys	iMessage Encryption Ke     Get Info		login
<b>10</b>	Certificates	iMessage Encryption Ke     Evaluate "1		login
		iMessage Signing Key public key		login
		iMessage Signing Key private key		login
		MetadataKeychain application password Mar 13, 2020 17:10:43		login
		RIKEN R-CCS certificate	Mar 31, 2036 10:45:20	login
		🔏 Safari Session State Key application password Yesterday, 16:57		login
		+ i Copy 20 items		

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

スタートアップガイド 1.11 版

します。

Enter the location	m (URL) or email address for which a certificate is required
Certificate:	
Select the prefe	rred certificate for the location or address specified above

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

fer the location (URL) or email a	address for which a certificate is required.
artificate:	<b>C</b>
elect the preferred certificate for	r the location or address specified above.

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 ヘアクセスします。

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

個人証明書の要求	×
このサイトはあなたの個人証明書を求めています:	
www.fugaku.r-ccs.riken.jp:443	
組織: "RIKEN"	
発行者: "National Institute of Informatics"	
個人認証を行うために送信する証明書を選択してくださ	い:
	$\sim$
選択した証明書の詳細:	
発行先: DC=jp,DC=riken,DC=r-ccs,O=RIKEN Center for Computational Science,CN= シリアル番号: 0:00:00 まで有効 鍵用途: Signing,Key Encipherment 発行者名: O=RIKEN Center for Computational	^
Science,DC=jp,DC=riken,DC=r-ccs,CN=RIKEN	$\sim$
☑ 今後も同様に処理する	
OK キャンセル	

• Chrome のダイアログ例

Subject	Issuer	Serial	
	RIKEN R-CCS	100	
-			

- 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

パスワード	を入力してください - Mozilla Firefox >	<
?	マスターパスワードを入力してください。	
	•••••	]
	OK キャンセル	

- 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。

	Google Chr ー"privatek 許可するにはキ	<b>rome がキーチ</b> <b>Key" を使用し</b> ーチェーン "ログ	・ <b>ェーンに含まれ て署名しようと</b> `イン" のパスワー	<b>1るキ</b> 2 <b>しています。</b> ドを入力して	
	くたさい。 パスワード:	•••••	•••••		
?	常に許可		拒否	許可	

**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。

💠 運用状況	重要なお知らせ	
通常運用中 「富岳」運用ステータス 前 運用ス	2024-08-28 運用情報	ログインノードのメンテナンス(Intel oneAPI Toolkit アップデート)(8/28 10:00 - 17:00)(終了) 🖉
	お知らせ	
23 利田考支援	2024-09-03 システム	▶ 【サテライト富岳】ログインノードにログインできない(9/3) ☑
	2024-09-02 イベント	第28回「富岳」利用セミナー(中級編)単体性能の最適化手法2
Open OnDemand	2024-09-02 バグ	ASSOCIATE構文の選択子にベクトル添字が現れた場合にFortranコンパイラが異常終了する
利用者ポータル	2024-09-02 システム	廊吉 🛛 accountd コマンドの -m オプションによる出力に誤りがありました 💆 🧬
成果発表	2024-09-02 システム	席書 ファイルシステム障害によるログインノードおよびジョブからのレスポンス低下などの発生(vol0003) 🛛 🤔
申請利用に関して	2024-08-30 >ステム	ログインノードおよびcsgwノードのLD_LIBRARY_PATH環境変数およびC_INCLUDE_PATH環境変数に不備がありました 図
お問い合わせ	2024-08-30 運用情報	2024年9月中規模ジョブ実行期間(09/04 15:00 - 09/08 15:00)
	2024-08-30 イベント	システムメンテナンスお知らせ【2024年10月】
	2024-08-28 運用情報	■ ログインノードのメンテナンス(Intel oneAPI Toolkit アップデート)(8/28 10:00 - 17:00)(終了) <i>役</i>
<b>三 富岳</b>	2024-08-28 運用情報	緊急メンテナンス (2024年8月28日 18:00-19:00)(終了)
システム構成	2024-08-28 運用情報	ファイルシステム保守によるログインノードおよびジョブからのレスポンス低下などの発生(vol0005) 🔗
リソースグループ	2024-08-26 運用情報	【サテライト富岳】ネットワークメンテナンスのお知らせ(9/4-5)
ジョブ調整率	2024-08-26 運用情報	- 2024年8月中規模ジョブ実行期間(08/23 15:00 - 08/27 15:00)(終了) 🕄
計算資源利用状況	2024-08-21	2024年08日1/2規模ジュブ宇行期期(08/20 15:00 - 08/23 15:00)(終了) 2

# **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)
- Windows (PuTTYgen)

### 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:khbWyIyUqMnyjK10k7818EivKbQLNgP3vyhjYBgvif8 namehostname
The key's randomart image is:
+--[ED25519 256]--+
  . . .
                 | ...+ 0
                 L
.0.*.
                 |=. . 0
```

(次のページに続く)

(前のページからの続き)

|=@ + S | |@o% . . | |=%.= . | |\*=0 = | |+=+=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。

PuTTY Key Generator	×
<u>F</u> ile <u>K</u> ey Con <u>v</u> ersions <u>H</u> elp	
Key No key.	
Actions	
Generate a public/private key pair	Generate
Load an existing private key file	Load
Save the generated key	Save p <u>u</u> blic key <u>S</u> ave private key
Parameters	
Type of key to generate: O RSA O DSA O ECDS	
Curve to use for generating this key:	Ed25519 (255 bits) 🗸 🗸

2. マウスカーソルをランダムに動かします。

スタートアップガイド 1.11 版

				×
ile <u>K</u> ey Con <u>v</u> ersions <u>H</u> elp				
Key Please generate some randomness by m	ioving the mouse over	r the blank area.		
Actions			Generate	
Actions Generate a public/private key pair			<u>G</u> enerate	
Actions Generate a public/private key pair Load an existing private key file			<u>G</u> enerate Load	
Actions Generate a public/private key pair Load an existing private key file Save the generated key		Save p <u>u</u> blic key	<u>Q</u> enerate Load Save private key	
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters		Save p <u>u</u> blic key	Qenerate Load Save private key	

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。

😴 PuTTY Key Generator					
<u>File K</u> ey Con <u>v</u> ersions <u>H</u> elp					
Key					
Public key for pastin ssh-ed25519	ε into OpenSSH autł	norized_keys file:		······	
				$\sim$	
Key fingerprint:	ssh-ed25519 255 3	SHA256:			
Key <u>c</u> omment:	eddsa-key-20				
Key p <u>a</u> ssphrase:					
Confirm					
Actions					
Generate a public/p	rivate key pair			<u>G</u> enerate	
Load an existing priv	ate key file			Load	
Save the generated	key		Save p <u>u</u> blic key	≦ave private key	
Parameters					
Type of key to gener O RSA	rate: O DSA	O ECDSA	EdDSA	🔾 SSH-1 (RSA)	
Cur <u>v</u> e to use for ger	nerating this key:		Ed	d25519 (255 bits) $\vee$	

*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。

🚰 PuTTY Key Gene	rator				$\times$
<u>-</u> Eile <u>K</u> ey Con <u>v</u> ersi	ons <u>H</u> elp				
Key Public key for pastin ssh-ed25519	g into OpenSSH auth	norized_keys file:			
Key fijngerprint:	ssh-ed25519 255 S	SHA256:4			
Key <u>c</u> omment:	eddsa-key-20				
Key p <u>a</u> ssphrase:					
Confirm	••••••				Ē
Actions					-
Generate a public/pr	rivate key pair			<u>G</u> enerate	
Load an existing priv	ate key file			Load	
Save the generated	key		Save p <u>u</u> blic key	Save private key	
Parameters					
Type of key to gener	rate: O DSA	○ ECDSA	🖲 EdDSA	O SSH-1 (RSA)	
Cur <u>v</u> e to use for ger	nerating this key:			Ed25519 (255 bits)	1

**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。

Save private key as:			×
-> 👻 🕇 🍹 > This PC > Desktop	v U	Search Desktop	P
Organize - New folder		8	· 0
<ul> <li>iwamoto Name へ</li> <li>tmp iwamoto</li> <li>ドメイン変更関連</li> </ul>	Date modified 3/5/2018 11:49 AN	Type File folder	Size
ConeDrive This PC B 3D Objects			1) Specify a file name.
Desktop Documents Documents Downloads			
Music V K			· ·
Save as type: PuTTY Private Key Files (*.ppk)			
II de Feldere		- (m) -	2) Click the Save butto

## 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。

✿ 運用状況	重要なお知らせ	
道常運用中 前 運用スケジュ	2020-12-25 変形的版	共用開始に向けたファイルシステム構成見直しに伴うデータの移動のお願い
	お知らせ	
🚢 利用者向け	2021-03-04 202010	ユーザボータルデザイン変更のお知らせ
利用者ポータル	2021-03-04	Compute nodes available
成果発表	2021-03-04 22用始展	Large scale job execution period
中請	2021-03-04 2001018	Compute nodes available
利用に関して	2021-03-04 200001	Large scale job execution period
お問い合わせ	2021-03-04 20/04/16	Compute nodes available
	2021-03-04 97750	ファイルシステム障害によるログインノードおよびジョブからのアクセス不可の発生(復旧済み)
-	2021-02-26 20用始期	プリポスト環境利用開始のお知らせ
	2021-03-03 200001	Fugaku maintenance Updated
システム構成 ジョブクラス	2021-03-03	ファイルシステム障害によるログインノードおよびジョブからのアクセス不可の発生(御旧済み) Resolved Updated
Antatt		
0.0000	最近のお知らせ	
運用情報	NEELO/03/ND > C	
システム障害	運用状況	
1(3	システムは「運用中」で	ia.
制限事項		

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

×		Fugaku User Portal	*	^
		User information		l
		User ID		I
Ì,	Access history	Group ID		I
-	Dick accounting	Home Directory		1
E	Disk accounting	Login Shell		
⊟	Job accounting	Belonging Group Name		
	● term			
	monthly	Project Name		
Ê	Job status	Project ID		
ъ	Job status transition history	Term(Start Date - End Date)		
۶	Publickey registration	End Date of The Grace		
		Project Manager Name		-

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

×	Fugaku User Portal
<b>L</b> ===	Publickey Registration     Depending on file system conditions, public key registration can take alog time. Please note.
<ul> <li>Access history</li> <li>Disk accounting</li> <li>Job accounting         <ul> <li>term</li> <li>monthly</li> </ul> </li> <li>Job status</li> <li>Yob status transition history</li> </ul>	Register Attention point of input
Publickey registration	<ul> <li>Please make sure that the browser you are using has been tested. If the problem does not improve, please contact the support desk</li> <li>Attention point of input</li> <li>Please generate the 2048bit the length of the key.</li> <li>The public key will be additionally written into the current file. (If there is no file, a new file is created.)</li> <li>A single operation cannot register multiple public keys. Register one public key at a time.</li> <li>Do NOT put your SSH private key on the login nodes.</li> </ul>

- 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。

×	Fugaku User Portal
<b>A</b> 1000	Publickey Registration
	Please confirm the following terms before you register the pu
Ccess history	- You must not put ssh private keys in the front-end servers. - If you put private keys in the front-end servers, you will
Disk accounting	temporarily prohibited from logging in to the Fugaku portal the Fugaku computer for security purpose.
Job accounting	- Not only private keys for the Fugaku computer, all ssh priv are prohibited.
● term	If you accept the terms above, click OK to continue to the re
monthly	If you cannot accept, click Cancel to exit.
Job status	
Dob status transition history	Atto Cancel
Publickey registration	<ul> <li>Please make sure that the browser you are using has been tested. If the problem does not improve, please contact the support desk</li> </ul>
	Attention point of input     Please generate the 2048bit the length of the key
	The public key will be additionally written into the current file. (If there is no file, a new file is created.)

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。

スタートアップガイド 1.11 版



**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。

×		Fugaku User Portal	*
		Publickey Registration	
		Depending on file system conditions, public key registration can take alog time. Please note.	
Ĝĝ	Access history	an explore an an english a providence of the set	
0)	Disk accounting		
₩	Job accounting		
	● term		
	monthly		
Ê	Job status		
3	Job status transition history	[EnrorCode] : 380012 [EnrorCode] : Error Code [ 380012 ]	
P	Publickey registration		
		Register	

#### 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
- ログインノード (PuTTY)

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】

スタートアップガイド 1.11 版

- 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。

🕵 PuTTY Configuration	×
Category:	
Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Colours Connection Data Proxy SSH Kex Host keys Cinher Auth Credentials GSSAPI TTY X11	Credentials to authenticate with Public-key authentication Private key file for authentication: Certificate to use with the private key.  Plugin to provide authentication responses Plugin command to run
About	<u>O</u> pen <u>C</u> ancel

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。

スタートアップガイド 1.11 版

	on	×
Category: 		Options controlling SSH X11 forwarding         X11 forwarding         X display location         Remote X11 authentication protocol         MIT-Magic-Cookie-1       XDM-Authorization-1         X authority file for local display         Browse
About	~	Open Cancel

 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。

🔀 PuTTY Configurat	ion		×
Category: 	^	Options controlling SSH authentication Display pre-authentication banner (SSH-2 only) Bypass authentication entirely (SSH-2 only)	
Connection 		Disconnect if authentication succeeds trivially     Authentication methods     Attempt authentication using Pageant     Attempt TIS or CryptoCard auth (SSH-1)     Attempt "keyboard-interactive" auth (SSH-2)	
Kex Host keys Cinber ⊕-Auth		Other authentication-related options	
X11 Tunnels Bugs More bugs Serial			
Telnet Rlogin	~		
<u>A</u> bout		<u>O</u> pen <u>C</u> ancel	

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。

PuTTY Security Alert	×
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.	
The server's rsa2 key fingerprint is: ssh-rsa 2048 26:f4:9b:02:42:58:86:d1:8e:12:c0:f6:c2:56:c9:4d If you trust this host, hit Yes to add the key to	1) Click the Yes
PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, hit No.	button.₊/
If you do not trust this host, hit Cancel to abandon the connection.	
Yes No Cancel Help	

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。

# ローカルアカウント名を入
# パスフレーズを入力

## 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)

スタートアップガイド 1.11 版

### 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。

🖫 Login		- 🗆 🗙
New Site	Session File protocol: SFTP Host name: login.fugaku.r-ccs.riken.jp User name: Password:	Po <u>r</u> t number:
	<u>S</u> ave ▼	A <u>d</u> vanced <b>▼</b>
<u>T</u> ools ▼ <u>M</u> anage ▼	🔁 Login 🔻 Close	Help

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。

## スタートアップガイド 1.11 版

dvanced Site Settings		?	×
Environment - Directories - Recycle bin - Encryption - SFTP - Shell Connection - Proxy - Tunnel	Bypass authentication entirely Authentication options Attempt authentication using Pageant Attempt 'keyboard-interactive' authentication Respond with password to the first prompt Attempt TIS or CryptoCard authentication (SSH-1)		
Authentication Bugs	Authentication parameters Allow agent forwarding Private key file: ppk		
	Display Public Key     Tools       GSSAPI       ✓ Attempt GSSAPI authentication       Allow GSSAPI gredential delegation		
<u>C</u> olor ▼	OK Cancel	<u>H</u> e	elp

6. 「Save」をクリックし、設定値を保存します。

🔩 Login		- 🗆 X
New Site	Session File protocol: SFTP Host name: login.fugaku.r-ccs.riken.jp User name: Save	Po <u>r</u> t number: 22 ♥ Password: Advanced ♥
<u>T</u> ools ▼ <u>M</u> anage ▼	🔁 Login 🛛 🔻	Close Help

7.保存した設定値を選択し、「Login」をクリックし接続します。

🖺 Login		- 🗆 X
New Site	Session  File protocol:  SFTP  Host name:  login.fugaku.r-ccs.riken.jp  User name:  Edit  Edit	Po <u>r</u> t number: 22 Advanced
<u>T</u> ools ▼ <u>M</u> anage ▼	Login ▼ Close	Help

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】

スタートアップガイド 1.11 版

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