OpenPGPを使用した署名検証方法の解説

1 署名検証方法の概要

デジタル署名の検証は、署名検証用ソフトをインストールし、インボイス制度適格請求書 発行事業者公表サイトで公開する公開鍵を取得したうえで(①~③)、ダウンロードした データ(全件・差分)を署名検証用ソフトで確認する(④~⑥)、という手順で行います。

≪署名検証用ソフトのインストールと公開鍵の取得≫



≪署名検証用ソフトによる検証≫



2 Windows 版パソコンでの操作方法

イ 署名検証用ソフト(Gpg4win)のインストール

① 「https://gpg4win.org/」にアクセスし、「DownloadGpg4win 3.1.15」をクリックします。

Gpg4win - Secure email and file < ×	+				0	-	٥	7	×
← → C 🗎 gpg4win.org				11 Be	☆	٥	*		:
	What's new Version 3	About Gpg4win Community	Support Download						Å
[Download Gpg4win 3.1.15		2021-01-12 Gpg4win 3.1.15 released 3002-11-25 Gpg4win 3.1.14 released Archived News						
	Gpg4win - a secure solution								ł
	and can be installed with just a few mouse clic	ks.							
	Discover Gpg4win	Getting started	Join the community						
	Learn what Gpg4win is and read more about the features of our solution! About Gpg4win ≽	We help you to use Gpg4win. Learn the basics about Gpg4win and get in the world of cryptography. The best point to start is with the illustrative Gpg4win Compendium.	Gpg4win is Free Software. Join the community! We recommend subscribing to the Gpg4win announcement mailing list to be automatically informed about new releases						•

②「\$0」をクリックし、「Download」をクリックします。

C e gpg4win.org/get-gpg4win.html		•							0	-	0		×
Image: Community Support Download Under & Download Download Gpg4win 3.1.15 (2021-01-12) You can also use this installer to update an older version. Keys and configration will be kept.	g4win.org/ge	et-gpg4win.html						₫ _E	☆	0	*	-	:
Please donate for Gpg4win to support maintenance and development! Pay what you want – Thank you! Donate with PayPal Bitcoin Bank transfer USD EUR onetime monthly	Ho	et-gpg4win.html ome > Download Download You can also use this in Play what you wanti Donate with Pay Pay Bitcoin Bitco	What's new Version 3 Installer to update an older v for Gpg4win to support I – Thank you!	About Copywin 1.1.15 (2021- orsion Kays and confign t maintenance and or 1 10 \$15 \$ EUK om	Community -O1-12) tition will be kept. development!	Support	EB English Teutsch Download		*	0	*	2	:

③ ダウンロードされます。				
Gpg4win - Thanks for download × +	0	-	٥	×
← → C	☆	0	* =	÷
Gi English 🔤 Deutsch				*
What's new About Gpg4win Community Support Download				
Home » Download				
Thank you for downloading Gpg4win.				
If the download of Gpg4win 3.1.15 doesn't start automatically, click here.				
Get started – your next steps:				
1. Check integrity of the downloaded Gpg4win installer!				
2. Install Gpg4win.				. 1
Create an OpenPGP key pair with Kleopatra. Sign/encrypt a file and email to yourself for testing.				. 1
 Read more about the public key method (see chapter 1-5 in Gpg4win Compendium). 				. 1
Ask your questions and report your problems to Gpg4win Community.				
				ad.
All Downloads About GpgAvin Community Support Misc About GpgAvin Community Support Docate				
Facetor opyrini Contribute to Ggg4win License				
System Requirements - Reporting Bugs Source Code Documentation - Building of OpgAwin Wiki				
Processed Advantage Maintaining Maintaining Maintain Processed Plantage Advantage Advantag			べて表示	×

④「gpg4win-3.1.15.exe」を右クリックし、「管理者として実行(A)」を選択します。
 ※ここでは、ダウンロードファイルをC:¥PGPに移動して実行しています。

📙 🕑 📙 🖛	管理	C:¥PGP			-	n x
ファイル ホーム 共有	表示 アプリケーション ツ	-JL				~ 🥐
テ クイック アクセス コピー 貼りた にピン留めする クリッフ	】		▲ 100 新しいアイテム・ 1 ショートカット・ カット・ フォルダー 新規	ブロパティ □ 開く ▼ □ 湯県	すべて選択 ::::::::::::::::::::::::::::::::::::	
← → ~ ↑ 📴 > PC	C → ローカル ディスク (C:) → PG	P			✓ O PGPの検索	Q
🖈 クイック アクセス	名前	更	新日時 種類	サイズ	gpg4win-3.1.15.exe	
🔜 デスクトップ 🛛 🖈	gpg4win-3.1.15.exe	20	121/05/23:13:22 アブリケーション 聞く(O)	29.240 KB	アフリケーション	
🗒 F#1X7F 🛛 🖈			管理者として実行(A)		\mathbf{O}	
🖊 ダウンロード 🛛 🖈			互換性のトラブルシューティング(0		
📰 ピクチャ 🛛 🖈			スタート メニューにピン留めする			
PC			12 共有			
🔿 ネットワーク			タスク バーにビン留めする(K) 以前のパージョンの復元(A)		更新日時: 2021/05/23 13:22 サイズ· 28.5 MB	
			シス 前りの パー クヨク の ほうし(マ)		作成日時: 2021/05/23 13:22	
			送る(N)	<u> </u>		
			切り取り(T)			
			ショートカットの作成(S)			
			^{利(ホ(D)} 名前の変更(M)			
			2070-1(h)			
1 個の項目 1 個の項目を	蠶択 28.5 MB					

⑤ インストーラが起動しますので、「Next>」をクリックします。

🔒 Gpg4win Setup	– 🗆 X
Gpg4win	Welcome to the installation of Gpg4win
GnuPG for Windows	Gpg4win is an installer package for Windows for EMail and file encryption using the core component GnuPG for Windows. Both relevant cryptography standards are supported, OpenPGP and S/MIME. Gpg4win and the software included with Gpg4win is Free Software.
	Click Next to continue.
	This is Gpg4win version 3.1.15 Release date 2021-01-12
	Next > Cancel

⑥ インストール対象を選択する画面が表示されますので、「GpgOL」「GpgEX」「Kleopatra」のチェックを外し、「Next>」をクリックします。

※「GpgOL」「GpgEX」のチェックを先に外さないと、「Kleopatra」のチェックは外せません。 (GnuPG以外のチェックを入れた場合、不要なソフトがインストールされますが署名検証 は可能です。)

🔒 Gpg4win Setup		-		\times
Gpg4win	Choose Components Choose which features of Gpg4wir	n you want to in:	stall.	
Check the components yo install. Click Next to conti	ou want to install and uncheck the com nue.	ponents you dor	n't want to	
Select components to inst	tall: CPUPG Kleopatra CPA GpgOL GpgEX Browser integration	Description GNU Privacy	Guard	
Space required: 60.1 MB				
Gpg4win-3,1.15	_F			
	< <u>B</u> ack	<u>N</u> ext >	Cance	el

⑦ インストール先を選択する画面が表示されますので、インストール先を選択後、 「Install」をクリックします。

Gpg4win Setup			-		×
0	Choose Install L	_ocation			
Gpg4win	Choose the folde	er in which to inst	tall Gpg4win.		
Setup will install Gpg4win and select another folder	in the following folder . Click Install to start	r. To install in a o the installation.	lifferent folder, d	ick Browse	
Destination Folder	6)¥Gpg4win		Brov	/se	
Space required: 60.1 MB Space available: 19.3 GB					
Gpg4win-3.1.15		< <u>B</u> ack	Install	Cano	el

⑧ インストールが完了したら、「Next>」をクリックします。

🔒 Gpg4win Setup	- 🗆 ×
Gpg4win	Installation Complete Setup was completed successfully.
Completed	
Paste V Clipboard G	Names Include GpgOL IS
From To	testuser@example.com testuser2@example.com ypt emails in Outlook with GpgOL.
Gpg4win-3,1,15	< Back Next > Cancel

⑨「Finish」をクリックすると、完了となります。

🔒 Gpg4win Setup	- 🗆 ×
Gpg4win	Completing Gpg4win Setup
GnuPG for Windows	Gpg4win has been installed on your computer.
	Click Finish to close Setup.
	Show the README file
	Go to Gpg4win's webpage
	< <u>B</u> ack Einish Cancel

- ロ インボイス制度適格請求書発行事業者公表サイトの公開鍵取り込み
 - 「インボイス制度適格請求書発行事業者公表サイト」にアクセスし、公開されている 公開鍵のデータをコピーして、テキストファイルとして保存します。このファイルが公開鍵 ファイルとなります。

なお、保存場所、ファイル名は共に任意です。ここでは、それぞれ以下のように設定 をしたとして、説明します。

≪保存場所≫ C:¥GPG

≪ファイル名≫ invoice-public.key

また、画面上に表示されている「フィンガープリント」の値は、この後の手順で必要に なるため手元に控えておいてください。

インボイス制	度適格請求書発行事業者公表サイト			
鍵ID	2A8AE3340980AA0C	_		
鍵タイプ	RSA 2048bit		手元に	控えておいて
フィンガープリン	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		くにろい	°0
	BEGIN PGP PUBLIC KEY BLOCK mOENBF/9WUMDCACXMOCUU2X/JguCh3C37R9yB8Q5SZAyTRwu8RPWNm3PtX4KYJa sAQIU+btPXDRQaz/HSI/qCScn6XLZnq910RpPP8scDwcaqeHr8uP1CVbjapzR2Zy 7vnJ7QakCZkaoLiheGAQZW0vSAQ819QZDdjimJUITufEUboXLQ3BuQdoRS12432			
	21h9nNmQwjE4NQYhWjTWVPyjf04zq1U9w4oZ4tkuE196mI6FK1IhauIsa3o73su3 dD9u/4UU195XVqMvDii11yaW7UVoY2FV70R4bGrFisE7c0HQJPAEttBzooVDY1iE yAsmiVCHFKuQFgs9VzSuZM7MjgE18kmG2WFXABEBAAGOG05hdG1vbmFs1FRheCBB	<	┘ コピー 、ファイ	してテキスト ルに貼りつけ
公開鍵	22VuY3kgSWS2b21 j2YkB6wQ0AwgABgUCX/1a4wAKCRAqiuMOCYCQDAqwB/ivHCVR Ic1VxE3A8ViGOTw90t06MVdeaxCM354ImVTPNdJBoh+r2qmR2iiN+QmARFcCq/aw p74EAvwCS2Ix+TrFhDYdYiPf0hBabZnEQ9ok0KsHR1WU/NwHFL04ZCtQJmbUhxET CYH33sxK58TPT+P4yEb0k1aFH2L0sn61+Z2bCpuP27SDe18Xm0Kq9RYrf180Tbug IvAy6DKPaPhrAIvmzU1xnY8oVoaDRixmFn6HnaNtw8Y54j/31qegL30y87ZT9A17 I15bK/qYbu4+W74vCpn2jUX1CE1R3n0v9GUB60U88nAzd0c25iMHj303a09eZVM		たうえ くださ	で、保存して い。
	Seadq11cHB1VEUW= =OWtx END PGP PUBLIC KEY BLOCK			
有効期限	無期限			

 ② パソコンの左下にあるスタートメニューから、「Windows システムツール」ー 「コマンドプロンプト」を起動してください。
 (操作が不明な場合は、「ここに入力して検索」欄(虫メガネアイコン)に「cmd」と入力して、 Enter キーを押しても起動できます。)



 ③ 以下のコマンドを実行し、コマンドプロンプト上で、公開鍵ファイルを保存したフォルダ (①の操作で保存したフォルダ)に移動します。

≪実行コマンド≫ cd C:¥GPG



④ 以下のコマンドを実行し、公開鍵ファイル(invoice-public.key)があることを確認します。
 ≪実行コマンド≫ dir



⑤ 以下のコマンドを実行し、公開鍵ファイルをGPGに取り込みます。

⑥ 以下のコマンドを実行し、⑤で取り込んだ公開鍵のフィンガープリントを出力します。 このとき、⑤の操作で手元に控えた鍵IDをコマンドの一部に使用します。

≪実行コマンド≫ gpg --fingerprint 2A8AE3340980AA0C

C-XGPG engfingernrint 2484E3340980440C	
9736 ADBF DAC1 6800 B22A 773C 2A8A E334 0980 AA0C	
uid I /тия I National Iax Agency Invoice	
u, turuz	

画面上に表示されたフィンガープリントが、①で手元に控えたインボイス制度適格 請求書発行事業者公表サイト上のフィンガープリントと一致することを確認してください。

- ⑦ 最後に⑤で取り込んだ公開鍵の信頼性を設定します。
 以降の処理は対話型(プログラムがユーザに入力を求める)で進められます。
 a)はじめに以下のコマンドを実行し、対話型処理を開始します。
 - ≪実行コマンド≫ gpg --edit-key 2A8AE3340980AA0C

C:¥GPG <mark>}gpgedit-key 2A8AE3340980AAOC</mark>	ĥ
gps (Gnure) 2.2.27; Copyright (C) 2021 g10 Code GmbH This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.	
pub rsa2048/2A8AE3340980AA0C 作成・2021-01-12 有効期限:無期限 利用法: SC 信用:不明の 有効性:不明の [不明 」(1). National Tax Agency Invoice	
gpg>	~

処理開始時点では、「信用」項目が「不明の」という状態であることを確認します。

b) 画面上に「gpg>」と表示されたら、以下のコマンドを実行します。

≪実行コマント≫ trust		
pub rsa2048/2A8AE3340980AA0C 作成: 2021-01-12 有効期限: 無期限 信用: 不明の 有効性: 不明の [不明](1). National Tax Agency Invoice	利用法: SC	
spe> <mark> trust </mark>		Ļ

c)「他のユーザの鍵を正しく・・・」という文書が表示され、「あなたの決定は?」という形で、「1」~「m」の何れかを入力するように求められますので、以下の値を入力します。 《入力値》 5



d) 続けて、「本当にこの鍵を究極的に信用しますか? (y/N)」と問われるので、以下の値
 を入力します。
 ≪入力値≫ √

あなたの決定は2.5	
本当にこの鍵を究極的に信用しますか?(y/N)y	
	N

e)「信用」項目が「究極」となったことを確認し、以下のコマンドを実行し、対話型処理を 終了します。

	≪実行コマンド≫ quit
pub	rsa2048/2A8AE3340980AA0C 作成:2021-01-12 有効期限: 無期限 利用法: SC 信用: 究極 有効性: 不明の
[フ ブロ とい	↑呀 〕(1). National Tax Agency Invoice グラムを再起動するまで、表示された鍵の有効性は正しくないかもしれない、 うことを念頭においてください。
gpg>	quit

⑧ 最後に以下のコマンドを実行し、コマンドプロンプトを終了します。

≪実行コマンド≫	exit	
gpg> quit		
C:¥GPG <mark>exit</mark>		Ļ

以上でインボイス制度適格請求書発行事業者公表サイトの公開鍵取込作業は完了です。

- ハ ダウンロードしたファイルの署名検証
 - ① データのダウンロード

インボイス制度適格請求書発行事業者公表サイトに公表されている、データファイル (zip 形式で圧縮済)をダウンロードし、解凍すると、2つのファイル(拡張子が「.csv」 または「.xml」または「.json」と、「.asc」)が表示されます。 ※ダウンロードは任意の場所で構いません。 ※ここでは、ダウンロードした公表情報ファイルの名称が「diff_20211101_csv.zip」で、 C:¥GPGフォルダに解凍したものとします。

≪解凍後の状態≫

C:¥GPG¥diff_20211101_csv

- ⊢ diff_20211101.csv.asc
 - └ diff_20211101.csv
- ② スタートメニューから「コマンドプロンプト」を起動し、コマンドプロンプト上で、ダウン ロードしたデータを保存したフォルダ(①の操作で保存したフォルダ)に移動します。 ≪実行コマンド≫ cd C:¥GPG¥diff 20211101 csv

📼 אָדער דער ד	_	×
Microsoft Windows [Version 10.0.18363.1500] (c) 2019 Microsoft Corporation. All rights reserved.		^
C:¥ <mark>]cd_C:¥GPG¥diff_20211101_csv_</mark>		
C:¥GPG <mark>{diff_20211101_csv>}</mark>		~

③ 以下のコマンドを実行し、ダウンロードファイルを検証します。

《実行コマンド》 gpg --verify <u>diff_20211101.csv</u>.asc <u>diff_20211101.csv</u>

(下線部は検証するファイルにあわせて変更してください。また、「.asc)ファイルを先に 記述してください。)

C:¥GPG¥diff_20211101_csy_sps <u>verify_diff_20211101.csv.asc_diff_20211101.csv</u>	
gpg: 2021/04/19 19:36:15 JSTに加きれた者名	
gpg: RSA鏈2A8AE3340980AA0Cを使用	
spg: 信用データベースの検査	
gpg: marginals needed: 3 completes needed: 1 trust model: pgp	
gpg: 深さ・0 右効性・ 1 署名・ 0 信田・0- 0a 0a 0m, 0f, 1u	
gpg: "National Tax Agency Invoice"からの正しい署名 [究極]	
C:¥GPG¥diff 20211101 csv>	
	\mathbf{v}
このにも、安仁妹田にして「エレい男々」にいる立言がまこされてこした疎認したす	
このとさ、美行結果として上しい者名」という人言が衣木されることを唯認します。	
T = T + T + T + T + T + T + T + T + T +	

万一、何らかの形で改さんされていた場合は、以下のように「*不止な*者名」という 文言が表示されます。

- ¥GPG¥diff_20211101_csv>gr gg: 2021/04/19 19:36:15 JS diff_20211101.csv.asc diff_20211101.csv た署名 04400を使用! ps: <mark>"National Tax Agency Invoice"からの*不正な*署名[究極]</mark> :¥GPG¥diff_20211101_csv>
- ④ 旦後にいてか。

4)	最後に以下のコマンドを	き実行し、コマントフロンフトを終了します。	
	≪実行コマンド≫	exit	
	C:¥GPG¥diff_20211101_csv}exit		~

- **3** Macintosh 版パソコンでの操作方法
 - イ 署名検証用ソフト(GPG Suite)のインストール
 - ① 「https://gpgtools.org/」にアクセスし、「Download for macOS 10.14 11.x」をクリック するとダウンロードが開始されます。

••• • < >	O	gpgtools.org	S		û + C
🔒 gf	PGTools		Support	Twitter	
		GPG Suite			
		One simple package with everything you need, to protect your emails and files.			
		Download formac051014-11x By downedding, you agree to confirms of Matrocom			
		Includes a 30-day trial of GPG Mail. For continued use of GPG Mail, please purchase a support plan			

 GPG Suiteのダウンロードファイルをクリックし、インストール画面を表示し、「Install」を クリックします。



③「"インストーラ"から・・・」というメッセージが表示された場合、「OK」をクリックします。



④ 初期画面表示後、「続ける」をクリックします。



⑤ 使用許諾契約を確認し、「Continue」をクリックします。

• • •	GPG Suiteのインストール	8
	Software License Agreement	
● はじめに	English	
• 使用許諾契約	GPG Suite is a software product developed and	
 インストール先 インストールの種類 	company established and existing under the laws of Austria	
● インストール	By continuing with the installation of GPG Suite you	
•	confirm that you are agreeing to be bound to our terms of distribution.	
	Terms of Distribution: <u>https://gpgtools.org/legal</u>	
GPG ^{TOOLS}	Print Save Go Back Continue	

⑥ 画面の内容を確認し、「Agree」をクリックします。

• • •	GPG Suiteのインストール	
	Software License Agreement	
● はじめに	English	
• 使用許諾契約	GPG Suite is a software product developed and	
To continue insta software license Click Agree to co the Installer.	alling the software you must agree to the terms of the agreement. ntinue or click Disagree to cancel the installation and quit	15
Read License GPGT00LS	Disagree Agree Print Save Go Back Co	ntinue

⑦ 画面の内容を確認し、「カスタマイズ」をクリックします。(インストール先を変更する場合は、「インストール先を変更」をクリックしてください。)

• • •	GPG Suiteのインストール	8
	"Macintosh HD"に標準インストール	
 はじめに 使用許諾契約 インストール先 インストールの種類 インストール 概要 	この操作には、コンピュータ上に62.9 MBの領域が必要です。 ディスク"Macintosh HD"にこのソフトウェアを標準インストールす るには、"インストール"をクリックしてください。	
GPGTOOLS	インストール先を変更 カスタマイズ 戻る インストール	

⑧ インストール対象を選択する画面が表示されますので、「GPG Mail 5」のチェックを外し、「インストール」をクリックします。

※これは、GPG Mailが有料機能で1ヶ月トライアルとなっているためです。

	GPG Suiteのインストール		8
	"Macintosh HD"にカスタムインストール		
	バッケージ名	アクション サイズ	٦.
● はじめに	GPG Mail 5	スキップ 6.7 MB	
 使用許諾契約 	GPG Services	インストール 3.2 MB	
● インストール先	GPG Keychain	インストール 5.7 MB	
● インフトールの種類	GPG Suite Preferences	インストール 2.3 MB	
	✓ MacGPG	インストール 31.5 MB	
● インストール			
• 概要			
	必要な空き領域: 53.3 MB Installs to: /Library/Mail/Bundles Description: OpenPGP for Apple Mail. macOS: 10.14–11.0	残り: 961.69 GB	
GPG ^{TOOLS}	標準インストール	戻る インストール	D

⑨ インストールが完了したことを確認し、「閉じる」をクリックします。

	GPG Suiteのインストール	
	インストールが完了しました。	
● はじめに	For new users we recommend our <u>First Steps</u> tutorial.	
 使用許諾契約 	On macOS Big Sur GPG Mail will be automatically enabled	
 インストール先 インストールの種類 	On other versions of macOS, make sure to enable GPG	
 インストール 	Mail manually via Mail > Preferences > General >	
• 概要	GPGMailLoader_5.mailbundle	
GPGI00LS		
GFG		

- ロ インボイス制度適格請求書発行事業者公表サイトの公開鍵取り込み
 - 「インボイス制度適格請求書発行事業者公表サイト」にアクセスし、公開されている 公開鍵のデータをコピーして、テキストファイルとして保存します。このファイルが公開鍵 ファイルとなります。

なお、保存場所、ファイル名は共に任意です。ここでは、それぞれ以下のように設定 をしたとして、説明します。

≪保存場所≫ /Users/testuser/Documents/gpg

≪ファイル名≫ invoice-public.key

※ファイルを保存する際は、メニューバーの「フォーマット」メニューを選択し、標準 テキストで保存してください。

また、画面上に表示されている「フィンガープリント」の値は、この後の手順で必要に なるため手元に控えておいてください。

インボイス制度	適格請求書発行事業者公表サイト			
 鍵ID	2A8AE3340980AA0C	-		
鍵タイプ	RSA 2048bit		手元に	控えておいて
フィンガープリント	9736 ADBF DAC1 6800 B22A 773C 2A8A E334 0980 AA0C	5	ください	°
公開鍵	BEGIN PGP PUBLIC KEY BLOCK mQENBF/9WuMDCACXMOCuU2X/JguCh3C37R9yp88Q5SZAyTRwu8RPWNm3PtX4KYJa sAQIU+btPXDRQaz/HS1/qCScn6KJZ.nq910RpPP8scDwcaqeHr8uP1CVbjapzR2Zy 7vnJ70qkCZkqoLihgGAQZXw0ySAQ8T9QZDdjimJUITufEUpoXLQ3BuQdoRS12432 21h9nNmQwjE4NOYhWjTWVPyjf04zq1U9w4oZ4tkuE196m16FK11hau1sa3o73su3 dD9u/4UU195XVqMvDji11yaW7Uv07EV70R4bGrFisE7c0HQJPAEttBzooVDY1iE yAsmiVCHfKuQFgs9VzSuZM7MjgE18kmG2WFXABEBAAG0G05hdGivbmFs1FRheCBB Z2Vu73kg5W52b21j2YkBGWQ0AwgABgUCX/1a4wAKCRAqiuMOCYCqDAqmkJivHCVR Ic1VxE3A8Vi6OTw90t06MVdeaxCM3541mVTPNdJBoh+r2qmR2iiN+qmARFcCq/aw p74EAvvGS21x+TrFhDYdYiPf0hBabzhE09ok0KsHR1WU/NwHfLdZctGJmbUhxET CYH33sxK58TP1+P4yEbQk1aFH2L0sn61+Z2bCpuP27SDe18XmQKq9RYrf180Tbug IvAy60KPaPhrAIvmzU1xnY8oVoaDRixmFn6HnaNtw8Y54j/31qegL30y87ZT9A17 115bK/qYVbJ4+W74vCpn2jUX1CE1R3n0v9GUB60U88nAzd0Cz51MHj3Q3a09eZVM 3edCqiicHBIvEUw= =0Wtx	<	コピー ファイ たうえ くださ!	してテキスト ルに貼りつけ で、保存して い。
有効期限	END PGP PUBLIC KET BLUCK			

② パソコンの左下にある「Launchpad」から、「その他」-「ターミナル」を起動してください。





③ 以下のコマンドを実行し、ターミナル上で、公開鍵ファイルを保存したフォルダ(①の 操作で保存したフォルダ)に移動します。

≪実行コマンド≫	cd /Users/testuser/Documents/gpg	
• • •	🔵 gpg — -zsh — 100×5	
Last login: Wed May 26 17:19 [testuser@khusernoiMac ~ % cd testuser@khusernoiMac gpg %	:41 on ttys000 /Users/testuser/Documents/gpg]

④ 以下のコマンドを実行し、公開鍵ファイル(invoice-public.key)があることを確認します。
 ≪実行コマンド≫ ls
 Last login: Wed May 26 17:47:04 on ttys000
 Itestuser@khusernoiMac ~% cd /Users/testuser/Documents/gpg
 Itestuser@khusernoiMac gpg %]
 Invoice-public.key
 Itestuser@khusernoiMac gpg %]

⑤ 以下のコマンドを実行し、公開鍵ファイルをGPGに取り込みます。

≪実行コマンド≫ gpg --import invoice-public.key
Cの操作で、画面上に表示される鍵IDを控えてください。鍵IDは、「鍵」で始まる文字
列の「鍵」を除いた部分です。ここでは、「2A8AE3340980AAOC」が鍵IDです。
testuser@khusernoiMac gpg % gpg --import invoice-public.key
gpg: keybox'/Users/testuser/.gnupg/pubring.kbx'か作成されました
gpg: 無効な外装ヘッダー: mgGNBF/9WUMDCACXM@CUU2X/JguCh3C37R9yB8055ZAyTRwu8RPWNm3PtX4KYJa\r\n
gpg: 28AE33409808AAOC: 公開鍵 "National Tax Agency Invoice"をインボートしました
gpg: インボート: 1
gpg: インボート: 1
gpg: インボート: 1 署名: 0 信用: 0-, 0q, 0n, 0m, 0f, 1u
testuser@khusernoiMac gpg %

⑥ 以下のコマンドを実行し、⑤で取り込んだ公開鍵のフィンガープリントを出力します。 このとき、⑤の操作で手元に控えた鍵IDをコマンドの一部に使用します。

《実行コマンド》 gpg --fingerprint 2A8AE3340980AA0C
 [testuser@khusernoiMac gpg % gpg --fingerprint 2A8AE3340980AA0C
 pub rsa2048 2021-01-12 [SC]
 9736 ADBF DAC1 6800 B22A 773C 2A8A E334 0980 AA0C
]

uid [不明] National Tax Agency Invoice testuser@khusernoiMac gpg %

画面上に表示されたフィンガープリントが、①で手元に控えたインボイス制度適格 請求書発行事業者公表サイト上のフィンガープリントと一致することを確認してください。

⑦ 最後に⑤で取り込んだ公開鍵の信頼性を設定します。
 以降の処理は対話型(プログラムがユーザに入力を求める)で進められます。
 a)はじめに以下のコマンドを実行し、対話型処理を開始します。

《実行コマンド》 gpg --edit-key 2A8AE3340980AA0C [testuser@khusernoiMac gpg % gpg --edit-key 2A8AE3340980AA0C gpg (GnuP6/MacGPG2) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law. pub rsa2048/2A8AE3340980AA0C 作成: 2021-01-12 有効期限:無期限 利用法: SC 信用:不明の 有効性:不明の [不明] (1). National Tax Agency Invoice

gpg>

処理開始時点では、「信用」項目が「不明の」という状態であることを確認します。

 b) 画面上に「gpg>」と表示されたら、以下のコマンドを実行します。
 ≪実行コマンド≫ trust 作成: 2021-01-12 有効期限: 無期限 利用法: SC 信用: 不明の 有効性: 不明の
 [不明] (1). National Tax Agency Invoice
 gpg> trust

- c)「他のユーザの鍵を正しく・・・」という文書が表示され、「あなたの決定は?」という形 で、「1」~「m」の何れかを入力するように求められますので、以下の値を入力します。 ≪入力値≫ 5 [apa> trust 19pg> trust pub rsa2048/2A8AE3340980AA0C 作成: 2021-01-12 有効期限: 無期限 信用: 不明の 有効性: 不明の [不明](1). National Tax Agency Invoice 利用法: SC 他のユーザの鍵を正しく検証するために、このユーザの信用度を決めてください (パスポートを見せてもらったり、他から得たフィンガープリントを検査したり、などなど) 1 = 知らない、または何とも言えない 2 = 信用し ない 3 = まぁまぁ信用する 4 = 充分に信用する 5 = 究極的に信用する m = メーン・メニューに戻る あなたの決定は? 5
- d) 続けて、「本当にこの鍵を究極的に信用しますか? (y/N)」と問われるので、以下の値 を入力します。 ≪入力値≫ У あなたの決定は? 5 本当にこの鍵を究極的に信用しますか? (y/N) y
- e)「信用」項目が「究極」となったことを確認し、以下のコマンドを実行し、対話型処理を 終了します。 ≪実行コマンド≫ quit pub rsa2048/2A8AE3340980AA0C pub tsa20469/2A0AE3349906AAB3 作成:2021-001-12 有効期限:無期限 利用法:SC 信用:究極 有効性:不明の [不明] (1). National Tax Agency Invoice プログラムを再起動するまで、表示された鍵の有効性は正しくないかもしれない、 ということを念頭においてください。

gpg> quit

⑧ 最後に以下のコマンドを実行し、ターミナルを終了します。 ≪実行コマンド≫ exit [gpg> quit testuser@khusernoiMac gpg % exit

以上でインボイス制度適格請求書発行事業者公表サイトの公開鍵取込作業は完了です。

]

- ハ ダウンロードしたファイルの署名検証
 - ① データのダウンロード

- ②「Launchpad」から「ターミナル」を起動し、ターミナル上で、ダウンロードしたデータを 保存したフォルダ(①の操作で保存したフォルダ)に移動します。 ≪実行コマンド≫ cd /Users/testuser/Documents/gpg/diff_20211101_csv
 ●●● ■ ■ diff_20211101_csv - -zsh - 100×5
 Last login: Wed May 26 17:48:04 on ttys000 [testuser@khusernoiMac ~ % cd /Users/testuser/Documents/gpg/diff_20211101_csv testuser@khusernoiMac diff_20211101_csv * ■
- ③ 以下のコマンドを実行し、ダウンロードファイルを検証します。

≪実行コマンド≫ gpg --verify <u>diff 20211101.csv</u>.asc <u>diff 20211101.csv</u> (下線部は検証するファイルにあわせて変更してください。また、「.asc」ファイルを先に 記述してください。) [testuser@khusernoiMac diff_20211101_csv % gpg --verify diff_20211101.csv.asc diff_20211101.csv]] gpg: 月 4/19 19:36:15 2021 JSTに施された電名 gpg: RSA键 2A8AE3340980AA0Cを使用 gpg: 備用データベースの検査 gpg: marginals needed: 3 completes needed: 1 trust model: pgp gpg: <u>深さ: 0 有効性: 1 異名: 0 信用: 0-, 00, 0n, 0n</u>, 0f, 1u gpg: <u>"National Tax Agency Invoice"からの正しい署名 [究極]</u>

このとき、実行結果として「正しい署名」という文言が表示されることを確認します。 万一、何らかの形で改ざんされていた場合は、以下のように「*不正な*署名」という

文言が表示されます。

[testuser@khusernoiMac diff_20211101_csv % gpg --verify diff_20211101.csv.asc diff_20211101.csv gpg: 月 4/19 19:36:15 2021 JSTに施された署名 gpg: RSA鍵 2A8AE3340980AA0Cを使用 gpg: "National Tax Agency Invoice"からの*不正な*署名 [究極] testuser@khusernoiMac diff_20211101_csv %

④ 最後に以下のコマンドを実行し、ターミナルを終了します。
 ≪実行コマンド≫ exit
 testuser@khusernoiMac diff_20211101_csv % exit