

WebNACCS_パスキー認証導入に関する想定問答

No	カテゴリ	質問	回答
1	事前手続き	NACCS掲示板で申込フォームが確認できず、申込方法がわかりません	お申込み方法については現在検討中のため、決まりましたら掲示板にてお知らせいたします。申し訳ありませんが今しばらくお待ちください。
2	事前手続き	パスキー登録時に行う認証手順を教えてください。	①NACCS掲示板の専用ページにアクセス（パスキー認証ページ： https://bbs.naccscenter.com/webnaccs/passkey-security.html ） ②パスキー登録用ユーザーID/パスワード申請 ③パスキー登録用ユーザーID/パスワード入力 ④生体認証登録 ⑤WebNACCSログインの順で進みます。
3	スケジュール	いつまでにパスキー認証を設定すればよいですか	一定期間は従来のログイン方式との併用運用となりますが、併行期間終了後はパスキー認証の設定が必須となりますので併用運用期間内にご対応ください
4	スケジュール	どのタイミングでパスキー認証を行いますか	デジタル証明書認証後にパスキー認証を行います。
5	導入背景・仕様	なぜ新しくパスキー認証が追加されるのですか	セキュリティ強化のため、従来のクライアント証明書認証に加え、パスキー認証（生体認証等）を導入します。
6	導入背景・仕様	今回の変更でWebNACCSの操作は変わりますか	WebNACCSの操作の変更はありません。追加されるのはWebNACCS接続前の認証です。
7	導入背景・仕様	ログインが3段階になるのはなぜですか	端末認証（デジタル証明書）、本人認証（パスキー）、業務認証（WebNACCS用 ID/PW）で認証確認するためです。
8	導入背景・仕様	WebNACCSの推奨環境について教えてください。	推奨環境については、以下のリンクを参照してください。 「スマートフォンやタブレットでのNACCS利用（第7次用WebNACCS）」 URL： https://bbs.naccscenter.com/qanda/docs/2025061700025/
9	認証・仕組み	パスキー登録は必須ですか	一定期間は従来のログイン方式との併用となりますが、併用期間終了後はパスキー認証の設定が必須となります。お手数ですが、併用期間内にご対応いただきますようお願いいたします。
10	認証・仕組み	パスキー認証とは何ですか	生体認証で本人確認を行い、端末に保存されたパスキーを用いて認証する方式です。
11	認証・仕組み	パスキー登録とは何ですか	ログイン時の本人確認に使用する「パスキー」を、利用端末または対応するパスキー保存先に作成・保存する設定です。 登録後は、パスキー認証の際に生体認証（指紋認証・顔認証など）を利用してログインできます。
12	認証・仕組み	iCloudの設定をしていなくても、パスキーでログインできますか	iPhoneの場合、パスキーはiCloudキーチェーンに保存・同期される仕組みのため、iCloudキーチェーン（パスワード）が有効である必要があります。

13	認証・仕組み	Googleアカウントの設定をしていなくても、パスキーでログインできますか	Androidの場合、パスキーはGoogleパスワードマネージャーに保存・同期される仕組みのため、「Googleパスワードマネージャー」が有効である必要があります。
14	認証・仕組み	新たに覚えるパスワードはありますか	ありません。端末に設定されている生体認証を使用します。
15	認証・仕組み	WebNACCSへログインする端末とは別のスマートフォンを用いてパスキーを登録する方法は	<ul style="list-style-type: none"> スマートフォンを利用したクロスデバイス認証（複数端末を跨いで利用する運用）を実施してください。 WebNACCSにアクセスし、パスキー登録画面を表示したうえで、保存先を選ぶ画面で、別のデバイス（iPhone/Android等）を選択してください。 画面に表示されるQRコードを携帯端末（スマートフォン）で読み取ると、スマートフォン側で認証操作（指紋・顔認証）が求められます。認証が完了すると携帯端末（スマートフォン）にパスキーが登録され、以降はその端末を用いてパスキー認証を行うことができます。
16	認証・仕組み	パスキー登録後にブラウザや端末を変更した場合に影響がありますか	端末変更時の影響は、パスキーの保存先によって異なります。同一アカウントで同期される保存先（例：Google Password Manager）を利用している場合は、新しい端末でもそのまま利用することができます。一方、端末内のみ保存されている場合は、パスキーの再登録が必要となります。
17	認証・仕組み	パスキー登録に利用できる端末数に制限はありますか	原則として、パスキーを登録できる端末数に明確な制限はありません。複数の端末で利用する場合は、それぞれの端末ごとにパスキー登録を行ってください。ただし、セキュリティ管理の観点から、必要以上の端末への登録は控え、適切に管理してください
18	アカウント管理	パスキー登録は会社の端末以外でも実施できますか	対応している端末であれば、会社支給端末以外（個人所有のPCやスマートフォン）でもパスキー登録・利用は可能です。ただし、セキュリティ管理の観点から、利用可否や条件については所属組織のルールに従ってください。
19	アカウント管理	一人の利用者が、複数のWindows端末を利用する場合のパスキー登録方法を教えてください	パスキーはWindows端末ごとに紐付いて管理されます。利用するWindows端末ごとにパスキー登録用IDを取得し、パスキー登録が必要です。
20	アカウント管理	パスキーを他の人と共有することはできますか	できません。パスキーは利用者本人の端末および生体認証等と紐付く個人専用の認証情報であり、他の人との共有はできません。
21	アカウント管理	利用者A・B・Cのように複数人で利用するケースの注意点は	パスキーは個人単位で管理し、共用しないことが前提です。
22	アカウント管理	スマートフォンを機種変更した場合はどうすればよいですか	新端末で再登録が必要となりますので、NACCS掲示板に掲載されているフォームから、ユーザーID/パスワードの申込手続きを行ってください。 URL： https://bbs.naccscenter.com/webnaccs/passkey-security.html
23	アカウント管理	パスキー登録用のID/パスワードは誰が発行しますか	NACCSセンター側で発行し、事業所の管理責任者様へ通知されます。
24	アカウント管理	WebNACCS利用者本人に直接ID/パスワードは通知されますか	いいえ。管理責任者様に通知されます。

25	アカウント管理	管理責任者が1名の場合、利用者管理はどうなりますか	管理責任者様から各利用者様へ、パスキー登録用のユーザーID/パスワードを配布する流れとなります。
26	アカウント管理	パスキー登録用のユーザーID/パスワードを再発行したい場合はどうなりますか	NACCS掲示板に掲載されているフォームから、再度ユーザーID/パスワードの申込手続きを行ってください。管理責任者様へ再通知されます。
27	アカウント管理	WebNACCSのID/パスワードを忘れた場合はどうすればいいですか	WebNACCSにログインするパスワードの変更については、従来どおりNSSからお手続きください。
28	アカウント管理	パスキー登録用のユーザーIDはどのように取得しますか	NACCS掲示板に掲載されているフォームから、お客様自身で申請のうえ、取得していただきます。以下のページをご確認ください。 URL : https://bbs.naccscenter.com/webnaccs/passkey-security.html
29	トラブル	パスキー登録用のユーザーID/パスワードが届いていない場合は	管理責任者様に通知メールが届いているかを確認してください。届いていないようであれば、再度ユーザーID/パスワードの申込手続きを行ってください。管理責任者様へ再通知されます。
30	トラブル	パスキー登録ができない主な原因は何ですか	生体認証が未設定等が考えられますので、掲示板に掲載されている手順書を基に再度設定を実施してください。
31	トラブル	生体認証（指紋・顔認証）が使えない場合はどうなりますか	生体認証（指紋・顔認証）が利用できない場合でも、バックアップとして端末に設定されたPIN（暗証番号）などによる認証が可能です。また、端末自体に認証機能がない場合は、別の対応端末での登録・利用をご検討ください。
32	問い合わせ先	パスキーに関する問い合わせ先はどこですか	ヘルプデスク（0570-055-794）にご連絡ください。
33	認証・仕組み	<ul style="list-style-type: none"> 顔認証や指紋認証は、対応機器があれば必ず使えますか？ カメラ付きのPCなら顔認証は使えますか？ 	<p>単にカメラや指紋センサーが搭載されているだけでは利用できません。</p> <p>WebNACCSへログインするWindows端末にパスキーを登録するには、顔認証または指紋認証がWindows Helloに対応し、当該機能を用いてOSへログイン可能であることが必須条件です。</p> <p>特に、一般的なWebカメラのみを搭載した端末では顔認証は利用できないため、ご注意ください。（通常のWebカメラは映像用であり、生体認証用には非対応であることが想定されるため）</p>