

パスワードレス認証・ワンタイムパスワード認証について

KDH20220201

PCAでは、個別認証時に従来のIDとパスワードによる認証に加え、パスワードレス認証・ワンタイムパスワード認証に対応しています。よりセキュリティを強化したい場合に設定を行ってください。
※製品連携する際には連携元製品と連携先製品でパスワードレス認証・ワンタイムパスワード認証の有効化状況を揃えて使用することを推奨しています。

◆パスワードレス認証とは

FIDO認証を使用したログオン方法です。「サーバーとユーザーで秘密の情報を共有しない」ため、サーバーからのID・パスワードの漏洩やフィッシングやマルウェアによるパスワードの盗み出しを防ぎ、安全で簡単にログオンが可能になります。

PCAでは、Windows Hello を利用した認証（顔認証、指紋認証、PINによる認証）によってPCA製品へのログオン認証を行います。

注意・制限事項

- 1.Windows Helloを利用した生体認証を行うため、Windows Helloが利用できない環境（OSバージョンが古い場合や認証機器未搭載の場合）では利用できません。
（従来でのパスワードによる認証となります）
また、リモート環境上でも Windows Hello を利用することができません。

◆ワンタイムパスワード認証とは

時間によってワンタイムパスワードを生成する仕組み（TOTP：Time-based One-Time Password）を利用してログオンする方法です。

専用アプリに届いたパスワードを入力するだけなので、操作性に悩むことなくセキュリティを高めることができます。

- ・ Google Authenticator
- ・ Microsoft Authenticator

といった、スマートフォンやタブレット、iOS、Android で利用可能な一般的な認証アプリケーションを利用してPCA製品へログオン認証を行います。

注意・制限事項

- 1.「Google Authenticator」「Microsoft Authenticator」などスマートフォン等で使用可能な認証アプリケーションを準備しておく必要があります。
- 2.『PCA 給与シリーズ』『PCA 人事管理シリーズ』『PCA 法定調書シリーズ』のいずれかと『マイナンバー管理ツール』の両方をご利用になる場合、各製品で「ワンタイムパスワード認証の有効化」を行う前に、『マイナンバー管理ツール』の運用準備（セットアップ、起動、『マイナンバー管理ツール』でのデータ領域の作成）を済ませておいてください。
※すでに各製品で「ワンタイムパスワード認証の有効化」を行った場合は、「ワンタイムパスワード認証の有効化」で認証を一旦無効にしてから、『マイナンバー管理ツール』の運用準備を行い、再度「ワンタイムパスワード認証の有効化」を行ってください。

◆パスワードレス認証 運用開始までの流れ

1. [システムユーザー] Windows Helloの準備

ログオンするPCそれぞれでWindows Helloのセットアップが必要です。
セットアップ方法はMicrosoft社のウェブサイト等をご確認ください。



2. [システム管理者] パスワードレス認証の有効化を行う

「システムツール」－「パスワードレス認証の有効化」機能でパスワードレス認証を有効化します。
併せて、各ユーザーにパスワードレス認証の利用を強制するかどうかの設定も行うことが可能です。



3 [システムユーザー] パスワードレス認証設定を行う

「セキュリティ」－「システムユーザーの登録」でパスワードレス認証の設定を行います。
ログオンするPCそれぞれで設定を行う必要があります。
利用が強制の場合には
※Windows Helloに対応していないPCでは「このコンピューター、OSアカウントではパスワードレス認証を使用しない」を設定します。
①認証キー名を設定します。他のPCAソフトでパスワードレス認証設定を行う場合に、登録した認証キー名を入力することで、共通の認証設定を使用することができます。
②使用する認証方法（指紋認証・顔認証・PINによる認証）で認証の登録を行います。



4. [システムユーザー] パスワードレスでログオン

パスワードレス認証の設定を行ったPCから指紋認証、顔認証、PINによる認証などでログオンを行います。

◆ワンタイムパスワード認証 運用開始までの流れ

1. [システムユーザー] 認証アプリケーションの準備

「Google Authenticator」「Microsoft Authenticator」など認証アプリケーションを準備します。
操作方法は各アプリケーションのサイト等をご確認ください。



2. [システム管理者] ワンタイムパスワード認証の有効化を行う

「システムツール」－「ワンタイムパスワード認証の有効化」機能で「認証アプリケーション」を選択することでワンタイムパスワード認証の使用が有効となります。
併せて、各ユーザーにワンタイムパスワード認証の利用を強制するかどうかの設定も行うことが可能です。



3 [システムユーザー] ワンタイムパスワード認証設定を行う

「セキュリティ」－「システムユーザーの登録」でワンタイムパスワード認証の設定を行います。

- ①ワンタイムパスワード認証の「利用区分」を「使用する」に設定し、「秘密鍵」を生成します。
- ②確認画面が表示されますので、認証アプリケーションでQRコードを読み込みます。
- ③登録時に「コードの確認」画面が表示されますので、認証アプリケーションに表示された認証コードを入力します。



4. [システムユーザー] ログオン画面でワンタイムパスワードを入力

ログオン画面で通常のパスワードと認証アプリケーションに表示されたワンタイムパスワード両方を入力します。

ログオンできない場合には？

スマートフォンなどの故障や紛失等で認証アプリケーションが利用できない場合に備えて、事前にバックアップコードを生成しておくことが可能です。1度だけ利用できる数値8桁のバックアップコードを10個出力できます。

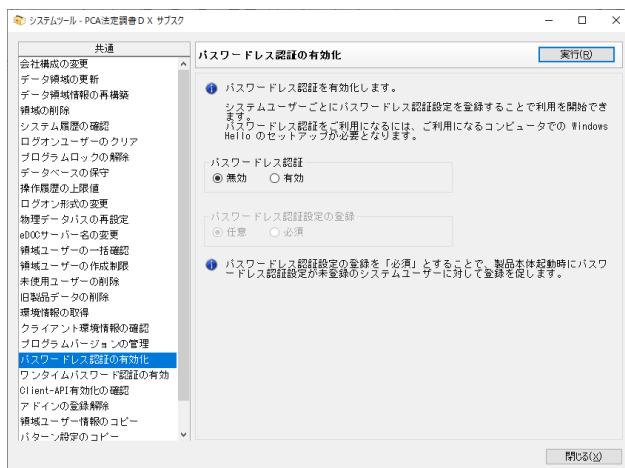
ログオン時にバックアップコードの1個を使用してログオンします（一度使用したバックアップコードは使用できなくなります）。

一般ユーザーがログオンできない場合にシステム管理者がバックアップコードを生成して提供することも可能です。

バックアップコードは再生成可能ですが、再生成すると以前出力したバックアップコードは使用できなくなります。

◆システムツール

◇パスワードレス認証の有効化



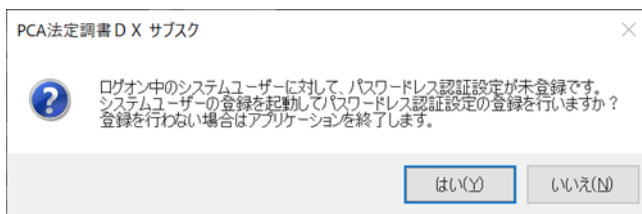
①処理メニューから「共通」－「パスワードレス認証の有効化」を選択します。

②パスワードレス認証を「無効」「有効」から選択します。

③パスワードレス認証を「有効」にした場合、パスワードレス認証設定の登録を「任意」「必須」から選択します。

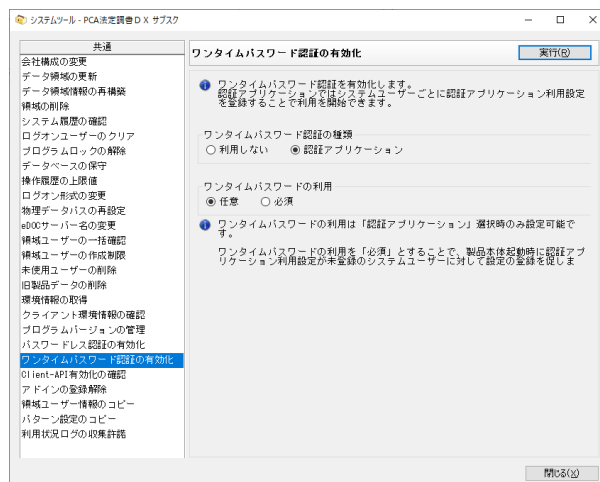
- ・任意：各ユーザーの任意のタイミングで設定を行うことができます。
- ・必須：製品起動時に認証設定を促す画面が表示されます。「システムユーザーの登録」でパスワードレス認証設定を登録しない場合には、起動ができなくなります。

※起動するコンピューター、OSアカウントが異なる場合には毎回確認画面が表示されます。



④設定した内容で実行する場合は、[実行] ボタンをクリックします。

◇ワンタイムパスワード認証の有効化



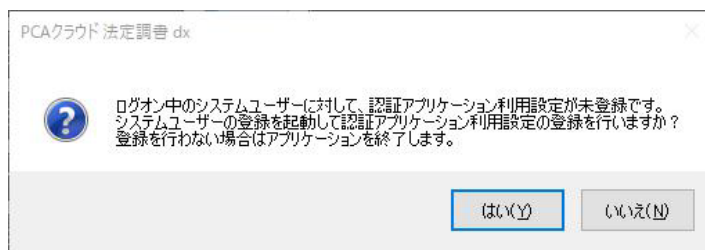
①処理メニューから「共通」－「ワンタイムパスワード認証の有効化」を選択します。

②ワンタイムパスワード認証の種類を「利用しない」「RSA SecurID サービス」「認証アプリケーション」から選択します。

※「RSA SecurID サービス」はクラウド版（on AWSを除く）の場合に表示されます。

③ワンタイムパスワード認証の種類を「認証アプリケーション」にした場合、ワンタイムパスワードの利用を「任意」「必須」から選択します。

- ・任意：各ユーザーの任意のタイミングで設定を行うことができます。
- ・必須：製品起動時に認証設定を促す画面が表示されます。「システムユーザーの登録」で認証アプリケーション設定を登録しない場合には、起動ができなくなります。



④設定した内容で実行する場合は、[実行] ボタンをクリックします。

◆システムユーザーの登録

ここでは、「パスワードレス認証」「ワンタイムパスワードレス認証」に関する項目部分を説明しています。

その他の項目は各ソフトのマニュアルをご確認ください。

◇パスワードレス認証設定

①パスワード認証設定の各項目を設定します。

- ・利用区分：「利用する」「利用しない」から選択します。
- ・登録件数：登録済み件数が表示されます。
- ・登録済みキー名：登録済みのキー名が表示されます。未登録の場合やキーを変更する場合には、[設定] ボタンをクリックします。

② [設定] ボタンをクリックすると「パスワードレス認証設定」画面が表示されます。

認証キー名を入力します。同じコンピューター上で複数のPCAソフトを同じシステムユーザーでご利用の場合には、他のソフトで登録済みの認証キーを入力することで同じ認証を使用できます。

Windows Helloがご利用になれない環境の場合には「このコンピューター、OSアカウントではパスワードレス認証を利用しない」にチェックマークを付けます。

③ [登録] ボタンをクリックすると、お使いのOSで設定した認証方法（指紋認証・顔認証・PINによる認証）での確認画面が表示されますので、それぞれの方法で確認を行います。

④ 確認に成功すると、メッセージが表示され、メイン画面に戻ります。

◇ 認証アプリケーション設定（ワンタイムパスワード認証）

① 認証アプリケーションの各項目を設定します。

- ・ 利用区分：「利用する」「利用しない」から選択します。
- ・ 秘密鍵：[自動生成] ボタンをクリックして自動で生成するか [手動で入力] ボタンをクリックして、「秘密鍵の入力」画面で秘密鍵を入力します。
※ [自動生成] を推奨しています。[手動で入力] は同じシステムユーザーが複数のシステム領域で同じ設定を行う場合にご使用ください。

② [登録] ボタンをクリックします。

③ 「コードの確認」画面が表示されますので、認証アプリケーションでQRコードを読み取ります。

→ 認証アプリケーションに表示された認証コードを入力して、[OK] をクリックします。



④ [バックアップコード] ボタンをクリックすると、スマートフォンなどの紛失などに備えてバックアップコードを出力することができます。「保存先の選択」画面が表示されますので、安全な場所に保存してください。

※ バックアップコードは再生成可能ですが、再生成すると以前出力したバックアップコードは使用できなくなります。

※ 新規購入されたスマートフォンやタブレット端末で認証アプリケーションを使用する場合、[QRコードの表示] ボタンをクリックし、表示されたQRコードを使用することで認証アプリケーションの設定を進めることができます。

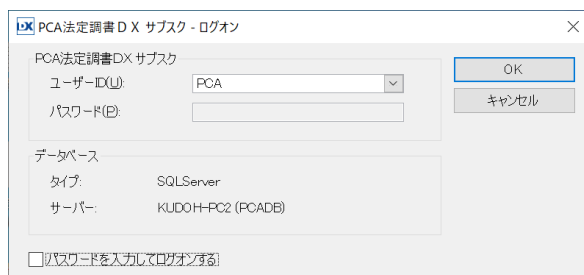
◆システムユーザーの確認リスト

「システムツール」の「パスワードレス認証の有効化」「ワンタイムパスワード認証の有効化」でパスワードレス、ワンタイムパスワードを有効にしている場合に「パスワードレス認証」「認証アプリケーション」欄が表示され、利用状況を確認できます。

◆ログオン画面

◇パスワードレス認証でのログオン

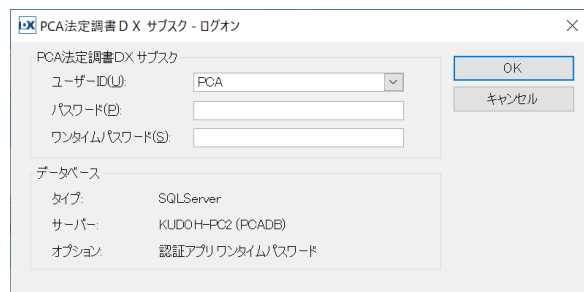
- ①ログオン画面でユーザーIDを選択して [OK] ボタンをクリックします。
従来のパスワードによる認証でログオンする場合には「パスワードを入力してログオンする」にチェックマークを付け、パスワードを入力します。



- ②ユーザーを確認する画面が表示されますので、設定した認証方法（指紋認証・顔認証・PINによる認証）でログオンします。

◇ワンタイムパスワード認証でのログオン

- ①ログオン画面でユーザーIDを選択して、パスワードと認証アプリケーションに表示されたワンタイムパスワードを入力します。
※ワンタイムパスワード欄に事前に保存したバックアップコードを入力することも可能です。
一度使用したバックアップコードは使用できなくなります。



◆システム領域の作成・更新

◇パスワードレス認証の場合

ユーザーIDを設定する画面で、パスワードレスでの認証が可能です。

〔次へ〕 ボタンをクリックすると、ユーザーを確認する画面が表示されます。

従来のパスワードによる認証を行う場合には「パスワード認証」を行うにチェックマークを付けパスワードを入力します。

システム領域の作成・更新 (1 / 8)

システム領域情報表示

現在のシステム領域の状態:

項目	値
アプリケーション	PCA法定調書D×サブスク
サーバー	KUDOH-P02
インスタンス	PCA00
システム領域	作成済み
システム情報	登録済み
プログラムバージョン	2.0.0004
データバージョン	1.0
共通データバージョン	2.41
認証方法	独自認証
システム管理者 (独自認証)	登録済み
システム管理者 (OS認証)	登録されていません

次のステップへ進むには、PCA法定調書D×サブスク に対するユーザーIDを入力する必要があります。

ユーザーID (U)

パスワード (P)

☐ パスワード認証を行う

〔次へ〕 を選択すると、認証方法の選択へ進みます。

< 戻る(B) 次へ(N) > キャンセル ヘルプ(F1)

◇ワンタイムパスワード認証の場合

ユーザーIDを設定する画面で、ワンタイムパスワードでの認証が可能です。

パスワードとワンタイムパスワードを入力します。

※ワンタイムパスワード欄に事前に保存したバックアップコードを入力し、進めることも可能です。

一度使用したバックアップコードは使用できなくなります。

システム領域の作成・更新 (1 / 8)

システム領域情報表示

現在のシステム領域の状態:

項目	値
アプリケーション	PCA法定調書D×サブスク
サーバー	KUDOH-P02
インスタンス	PCA00
システム領域	作成済み
システム情報	登録済み
プログラムバージョン	2.0.0005
データバージョン	1.0
共通データバージョン	2.41
認証方法	独自認証
システム管理者 (独自認証)	登録済み
システム管理者 (OS認証)	登録されていません

次のステップへ進むには、PCA法定調書D×サブスク に対するユーザーIDとパスワードを入力する必要があります。

ユーザーID (U)

パスワード (P)

ワンタイムパスワード (S)

〔次へ〕 を選択すると、認証方法の選択へ進みます。

< 戻る(B) 次へ(N) > キャンセル ヘルプ(F1)