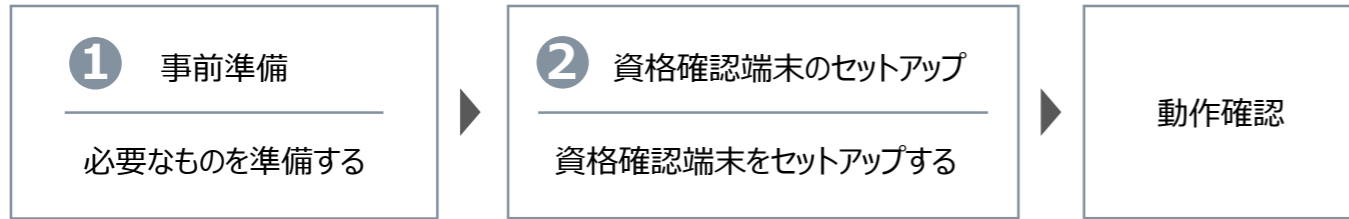


資格確認端末のセットアップ

本資料では、資格確認端末セットアップ手順を説明します。

作業の流れ

資格確認端末セットアップの作業の流れについて説明します。



事前準備

以下のものが揃っているか、確認してください。



● 資格確認端末（パソコン）

資格確認端末は、オンライン資格確認等システムを利用するために必要です。動作を確認している環境は、以下のとおりです。

- Windows10 IoT Enterprise 2019 LTSC 64bit版
- Windows10 Enterprise 2019 LTSC 64bit 版
- ※Windows10のOSセットアップは完了しておいてください。

最新版のMicrosoft Edgeが必要です [▶▶ 別紙 トラブルシューティング 補1](#)



● 顔認証付きカードリーダー装置

顔認証付きカードリーダー装置（以下、「顔認証機器」）は、オンライン資格確認等システムで顔認証を利用する場合に必要です。資格確認端末に接続して使用します。

● 通信回線

通信回線は、オンライン資格確認等システムを利用するために必要です。資格確認端末にIP-VPN又はIPsec+IKEにより接続して、オンライン資格確認等システムのサーバーとつなぐために使用します。



● マスタアカウントの通知書

マスタアカウントの通知書は、オンライン資格確認等システムを利用するアカウント作成のために必要です。



● 電子証明書、各種インストーラー

電子証明書は、各医療機関等で用意してください。
各種インストーラー（拡張プラグイン、連携アプリケーション、配信アプリケーション）は、医療機関等ベンダーより入手し、資格確認端末のデスクトップ等にコピーしてください。
※各インストーラーのファイル名は変更しないでください。変更してセットアップを行った場合、配信アプリケーションによる自動更新の動作保証外となります。

（ご参考）オンライン資格確認等システム利用までの全体の流れは本資料の操作12に
＜電子申請からオンライン資格確認等システム利用開始までの流れ＞を用意しています。

資格確認端末のセットアップ

[▶▶](#) 参照先を記載しています。

以下の順で、資格確認端末の接続に必要なソフトウェアをインストールします（複数の端末を使用する場合は、台数分同じ作業を実施してください）。



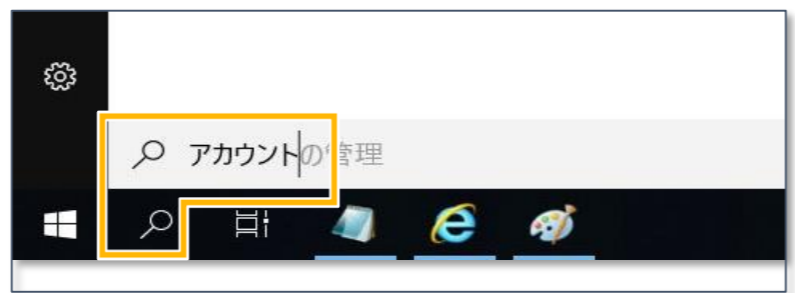
1 Windows10にユーザアカウントを追加する

オンライン資格確認等システムを利用するため、Windowsに以下のユーザ情報を登録します。

	ユーザ名	OqsComApp	※大文字小文字を識別します。 左記のとおり指定してください
	パスワード	任意	

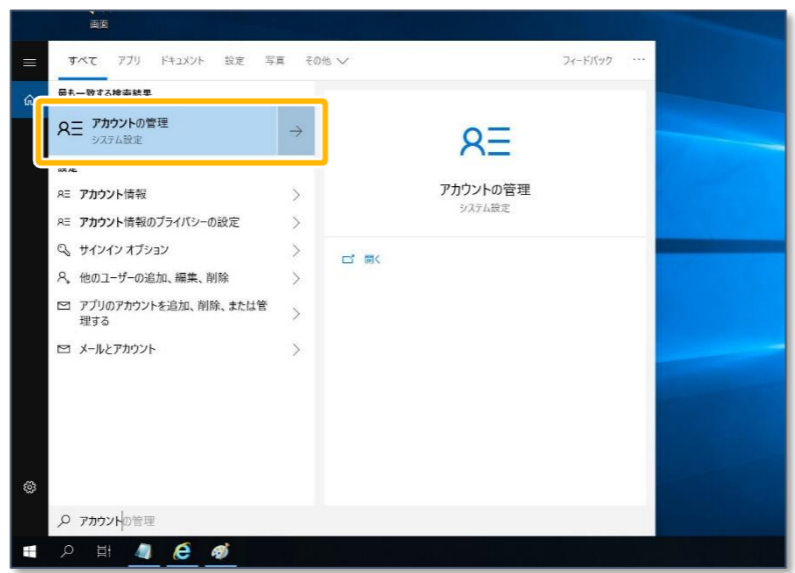
1 Windowsを起動します。

検索をクリックし、検索ボックスに**アカウント**と入力します。



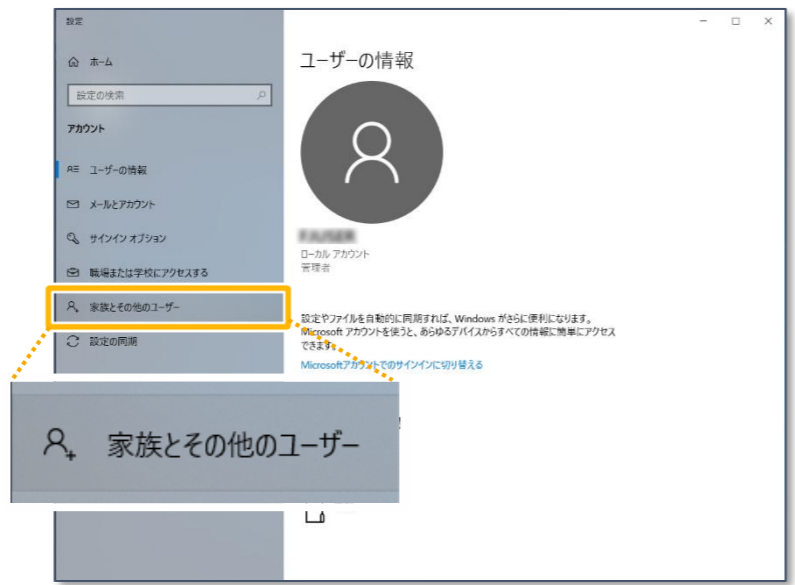
2 検索結果が表示されます。

アカウントの管理をクリックします。



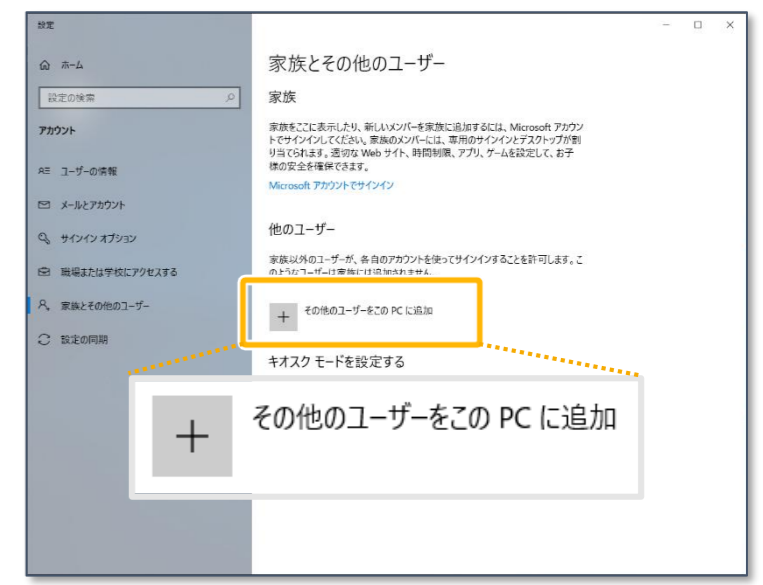
3 ユーザーの情報が表示されます。

家族とその他のユーザーをクリックします。



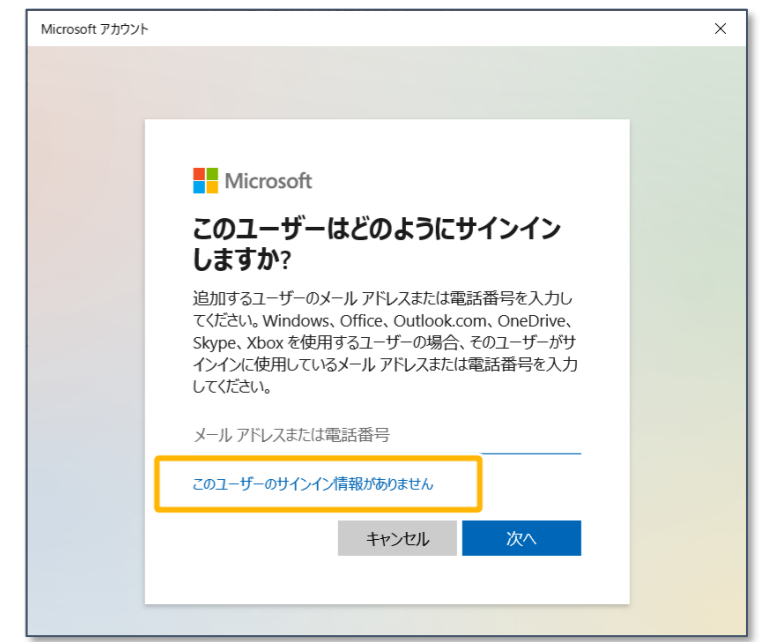
4 家族とその他のユーザーが表示されます。

その他のユーザーをこのPCに追加 をクリックします。



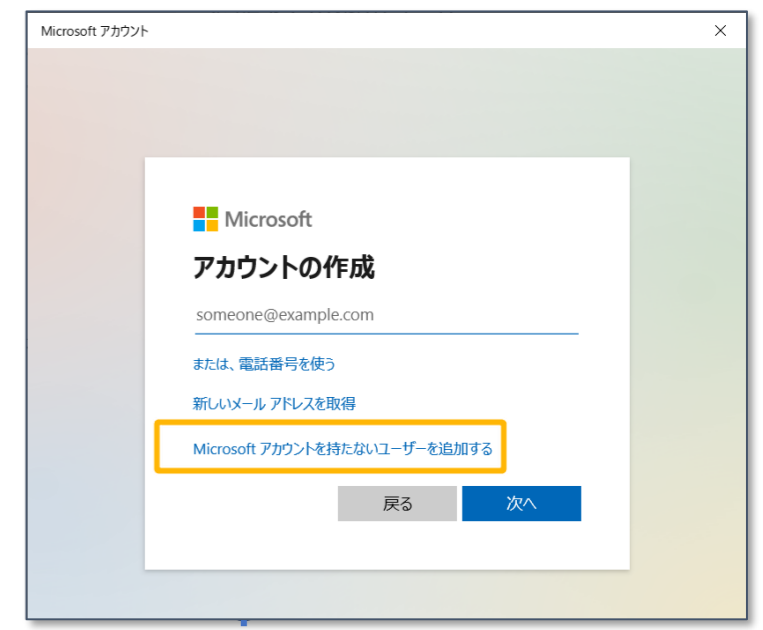
5 このユーザーはどのようにサインインしますか?が表示されます。

このユーザーのサインイン情報がありません をクリックします。



6 アカウントの作成が表示されます。

Microsoftアカウントを持たないユーザーを追加する をクリックします。



7 へ進む

1 Windows10にユーザアカウントを追加する (つづき)

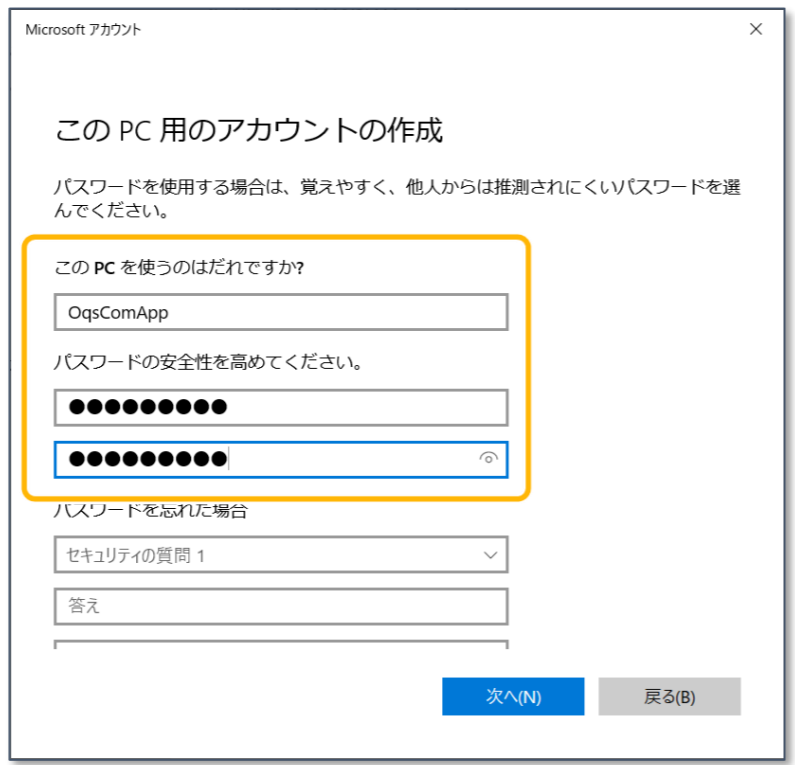
7 このPC用のアカウントの作成が表示されます。

このPCを使うのはだれですか? に、OqsComAppと入力します。

注意
ユーザ名は大文字と小文字を区別します。

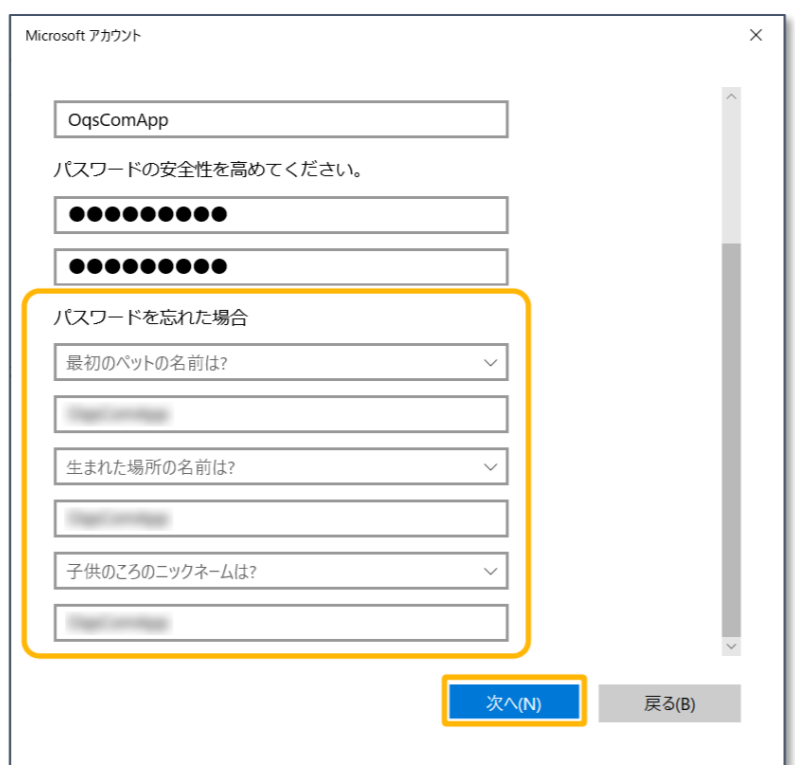
パスワードは任意のパスワードを入力します (2か所)。

注意
「医療情報システムの安全管理に関するガイドライン」、医療機関・薬局のセキュリティポリシー等に従い、Windowsの設定を行ってください。



8 7で設定したパスワードを忘れた場合の、「質問」とそれに対応する本人しか知らない「答え」を設定します。

セキュリティの質問を選択し、答えを入力します (3か所)。設定後、次へ をクリックします。



9 家族とその他のユーザーが表示されます。

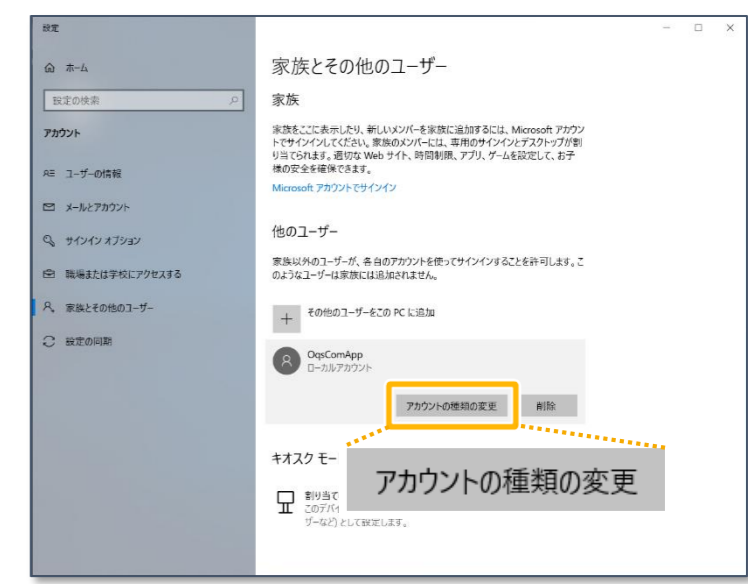
OqsComApp というユーザーが作成されたことを確認します。



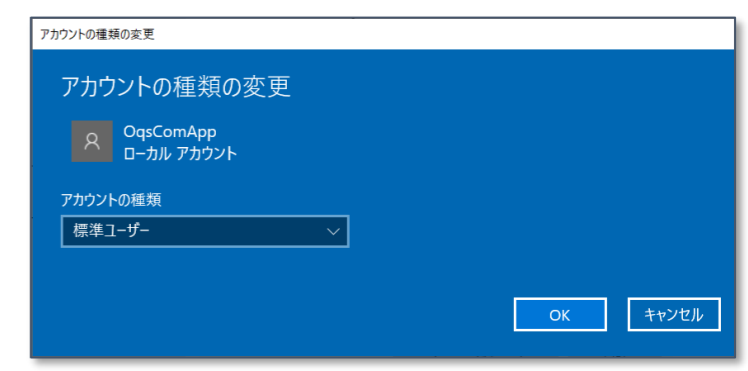
アカウントの種類を変更します

作成したOqsComAppユーザーのアカウントを管理者として設定します。

1 作成したOqsComApp をクリックし、表示されるボタンから、アカウントの種類の変更 をクリックします。



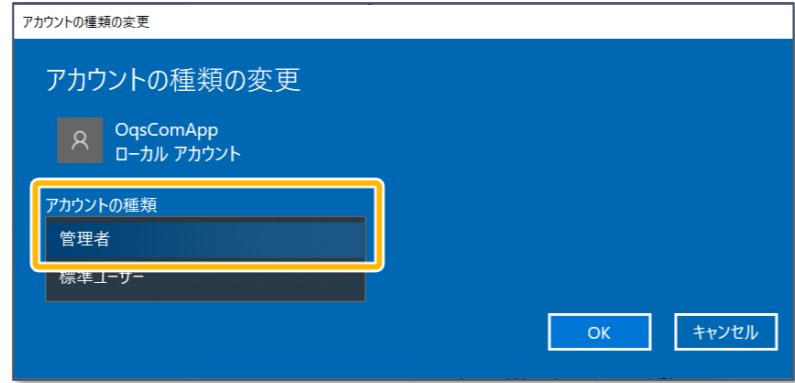
2 アカウントの種類の変更が表示されます。



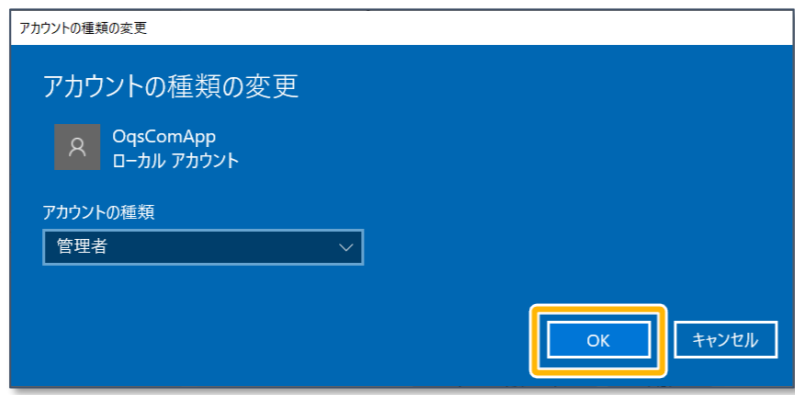
3 へ進む

1 Windows10にユーザアカウントを追加する (つづき)

3 アカウントの種類をクリックし、**管理者**をクリックします。



4 **OK**をクリックします。



5 家族とその他のユーザーが表示されます。

OqsComAppに管理者 - ローカルアカウントと表示されたことを確認します。

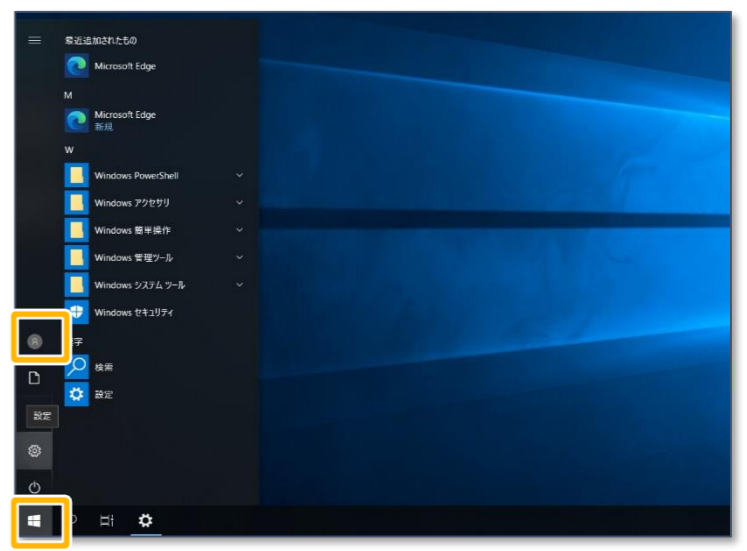


Windows10にユーザーが追加されました。
作成したユーザーでログインし直します。

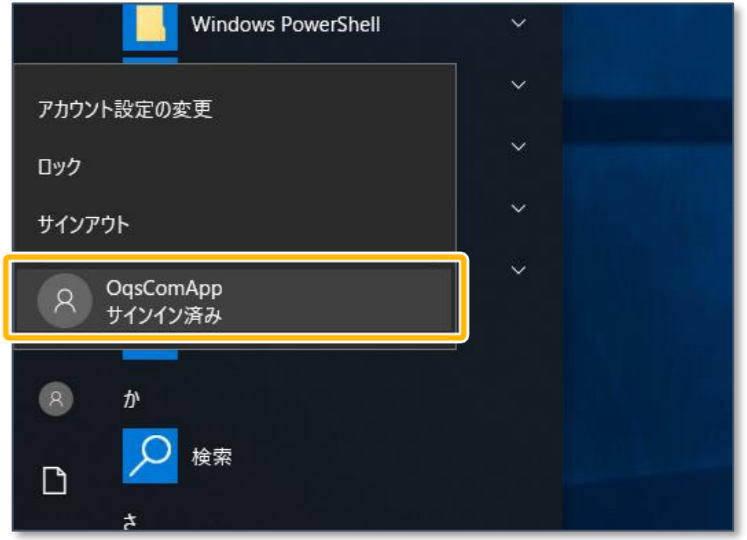
作成したアカウントでログインし直します

作成したアカウントで、Windowsにログインし直します。

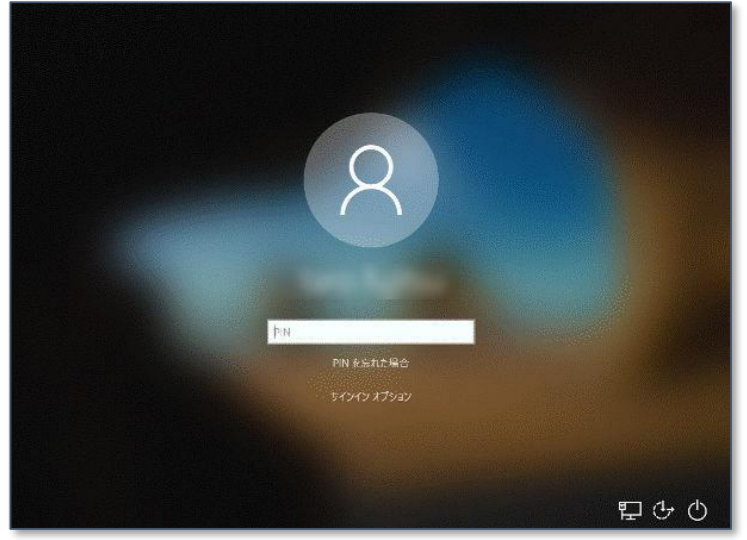
1 スタートボタンをクリックし、アカウントアイコンをクリックします。



2 作成したユーザー (ここでは、OqsComApp) をクリックします。



3 ログイン画面が表示されたら、作成したユーザーでログインします。



作成したユーザーでログインできました。

2 ブラウザ (Microsoft Edge) を設定する に進みます

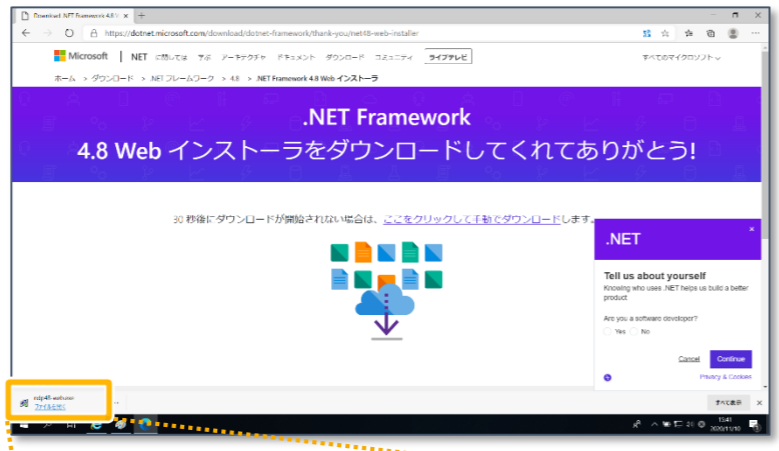
2 ブラウザ (Microsoft Edge) を設定する

.NET Framework4.8をインストールします

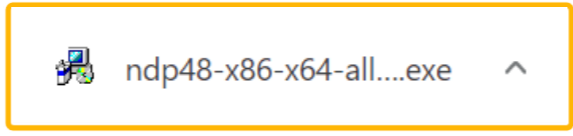
- 1 .NET Framework4.8のインストーラー (ndp48-x86-x64-allos-enu.exe) は医療機関等ベンダーにてダウンロードしていただき、入手してください。

.NET Frameworkのダウンロードサイト
<https://go.microsoft.com/fwlink/?linkid=2088631>

- 2 .NET Framework4.8のインストールファイルのダウンロードが開始されます。



- 3 ダウンロードされた.NET Framework4.8のファイルを開くをクリックします。



インストールが実行されます。

こんなときは！
メッセージ画面が表示された場合
 「このアプリがデバイスに変更を加えることを許可しますか？」というメッセージ画面が表示された場合は、YESボタンをクリックしてインストールを続行します。

- 4 インストールが完了したら、完了をクリックします。

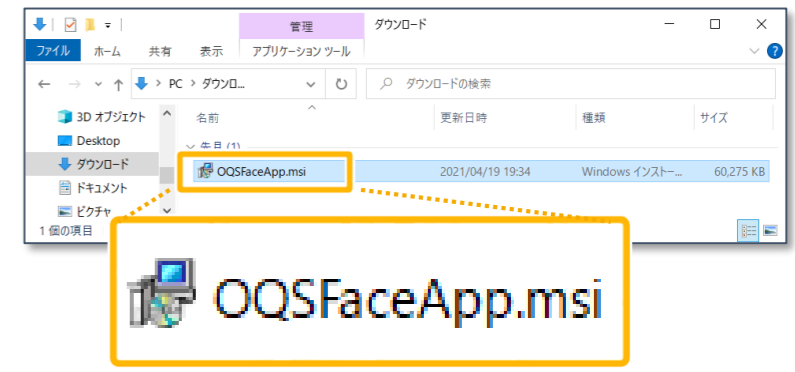


ブラウザ拡張ツールを実行します

医療機関等ベンダーより拡張プラグインインストーラー (OQSFaceApp.msi) を入手、実行し、ブラウザ設定と次項で設定する拡張プラグインをコピーします。

注意
 ZIP形式のインストーラーを提供しておりますが、セットアップで利用するのはinstall.batおよびcopyOqsSetting.batではなく、**OQSFaceApp.msi** です。

- 1 OQSFaceApp.msiをダブルクリックします。



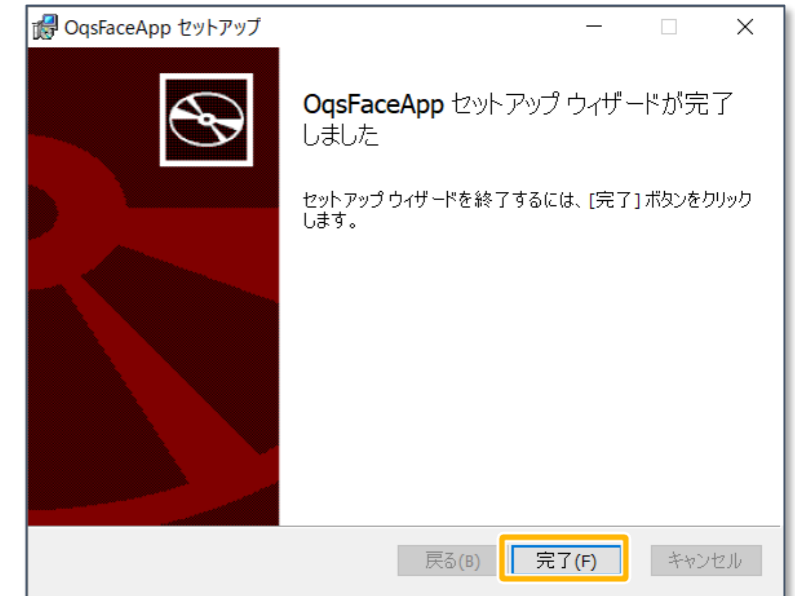
- 2 OqsFaceApp セットアップが表示されます。

ソフトウェア使用許諾条件の内容をよく読み、同意する場合は**使用許諾契約書に同意します**をチェックして、**インストール**をクリックします。



- 3 セットアップが完了すると、セットアップウィザード完了が表示されます。

完了をクリックします。



- 4 設定を有効にするため、Windowsを再起動します。

2 ブラウザ (Microsoft Edge) を設定する (つづき)

注意

拡張プラグインインストーラー (OQSFaceApp.msi) の実行により、スマートカードからの証明書の伝達をオンにするのポリシーが無効になります。そのため、証明書伝達サービス (CertPropSvc) が利用できなくなりますので、以下の機能を利用されている場合は、別紙「トラブルシューティング 補4「証明書伝達サービス (CertPropSvc) を利用するアプリケーションを利用したい」に従ってポリシーを有効にしてください。

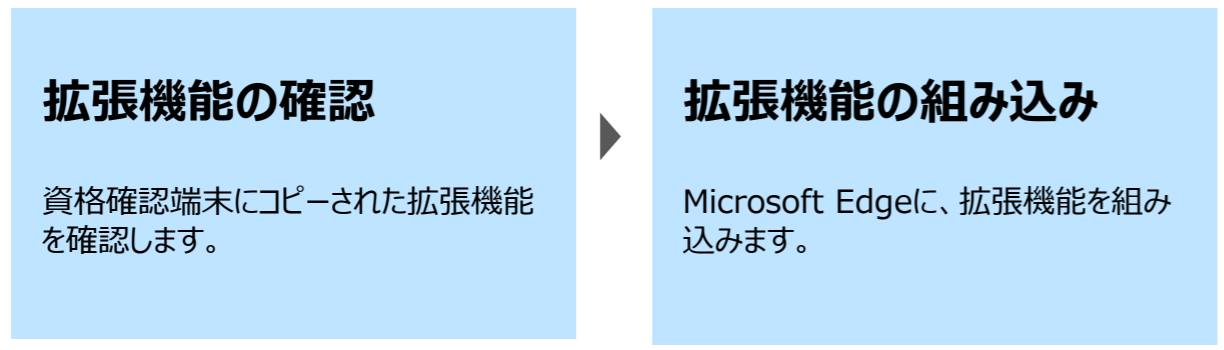
▶▶ 別紙「トラブルシューティング 補4」

■ 証明書伝達サービス (CertPropSvc) が利用できなくなることで影響する機能の一例

- ・マイナンバーカード以外のスマートカード (ICカード) による電子証明書の認証
- ・外部セキュリティキー (FIDO2 セキュリティキー) による認証
- ・SIM のご利用

ブラウザ拡張プラグインを設定します

ブラウザ拡張プラグインを設定します。ブラウザ拡張プラグインは、資格確認 (マイナンバーカードの暗証番号入力有り/顔認証) のときに使用します。以下の流れで設定します。

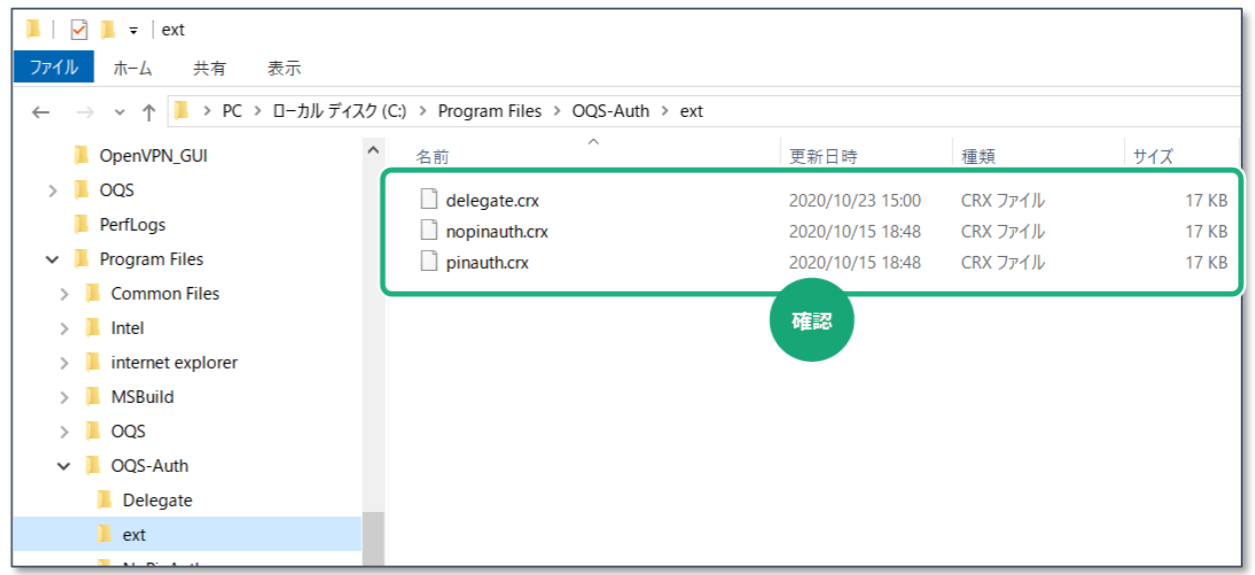


01 拡張機能の確認

資格確認端末にコピーされた拡張機能を確認します。医療機関等ベンダーより入手したインストーラー (OQSFaceApp.msi) を実行することで以下のフォルダに拡張機能 (3種類) がコピーされます。

以下のフォルダを開き、3つのファイルがコピーされていることを確認します。

フォルダ名	ファイル名	説明
c:\Program Files\OQS-Auth\ext	delegate.crx	目視確認操作アプリケーション
	nopinauth.crx	顔認証用アプリケーション
	pinauth.crx	暗証番号認証用アプリケーション

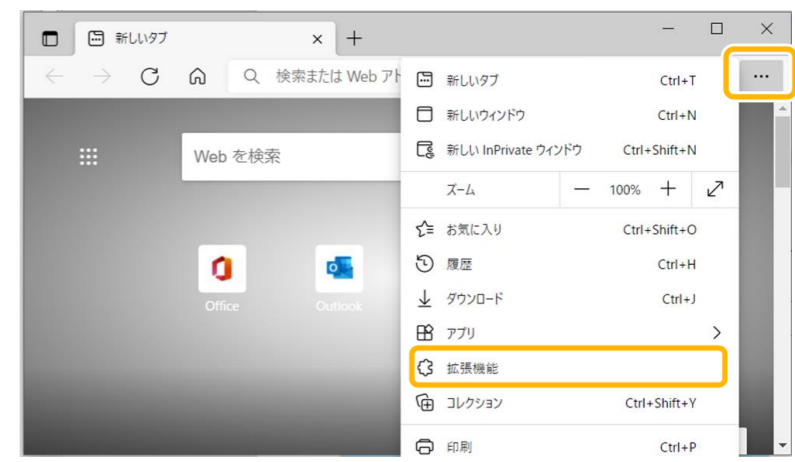


02 拡張機能の組み込み

Microsoft Edgeの拡張機能に、前ページで確認した3つのブラウザ拡張プラグインを追加します。

ブラウザ拡張プラグインを組み込みます

- 1 Microsoft Edgeを起動し、**...** (設定など) から**拡張機能**をクリックします。



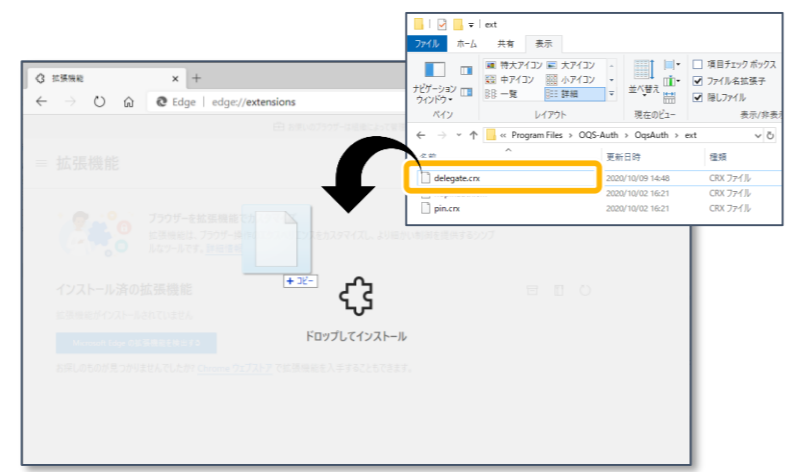
- 2 拡張機能が表示されます。
開発者モードの設定を有効 (トグルボタンが右側にある状態) にします。



▶▶▶ 3 へ進む

2 ブラウザ（Microsoft Edge）を設定する（つづき）

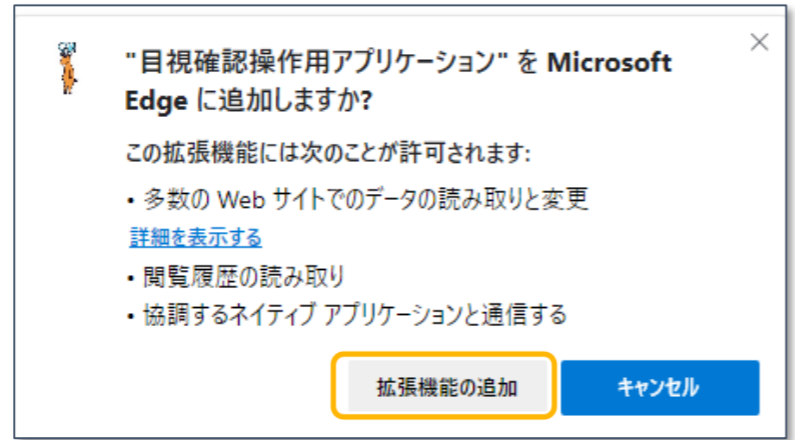
3 エクスプローラーで、ブラウザ拡張プラグインがコピーされたフォルダーを開きます。



delegate.crxをMicrosoft Edgeの画面にドラッグしてドロップします。

4 確認メッセージが表示されます。

拡張機能の追加をクリックします。



5 追加完了メッセージが表示されます。

×（閉じる）をクリックします。



6 Microsoft Edgeに拡張機能（目視確認操作アプリケーション）が追加されました。

同様に、**nopinauth.crx**、**pinauth.crx**を追加します。
3～6の操作を繰り返します。

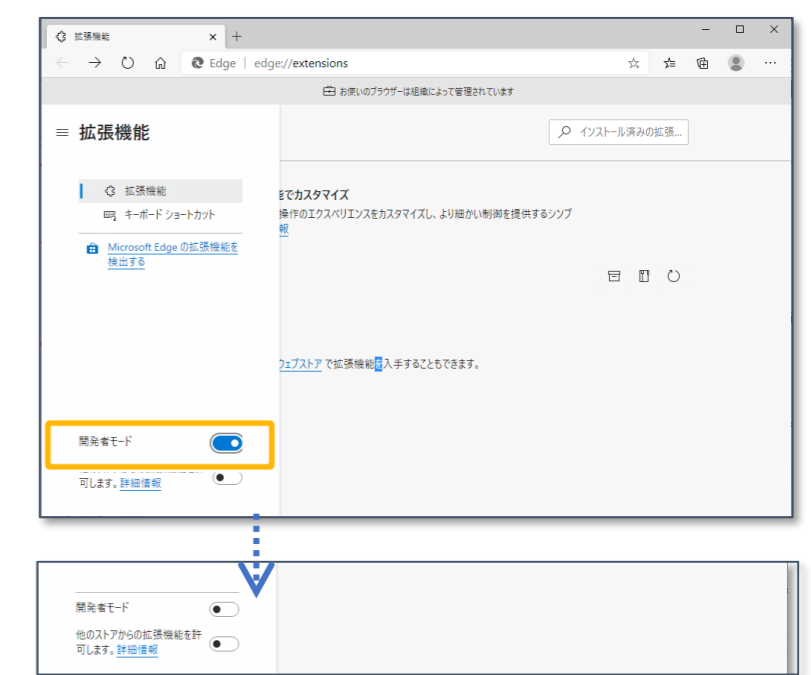


7 すべての拡張機能が組み込まれると、右図のように3つの機能が表示されます。



8 拡張機能のメニューを表示します。

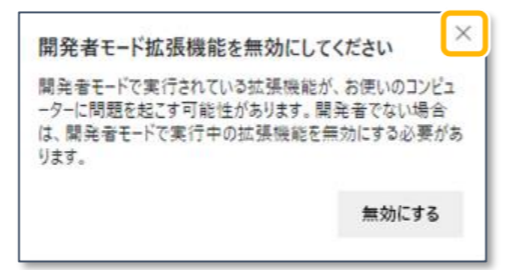
開発者モードの設定を無効（トグルボタンが左側にある状態）にします。



2 ブラウザ（Microsoft Edge）を設定する（つづき）

注意

ブラウザ再起動時に、開発者モードの無効を促すメッセージが表示される場合があります。開発者モードの無効を促すメッセージが表示された場合は、× ボタンをクリックしてメッセージを閉じてください。



ブラウザの拡張プラグインの組み込みが完了しました。

3 Windowsの設定を変更する（配信アプリケーション準備等）に進みます

3 Windowsの設定を変更する（配信アプリケーション準備等）


配信アプリケーションインストールのための準備およびオンライン資格確認等システムにおける画面、テキスト、項目サイズ等について以下のWindowsの設定を変更します。

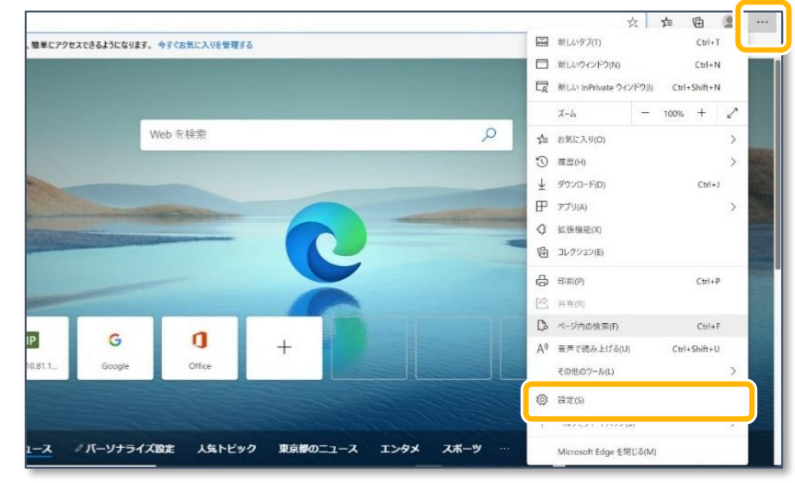
- プロキシサーバーの設定
 - ■ スリープ設定、高速スタートアップの設定の無効化
 - 時刻設定の変更
 - ■ ディスプレイの設定
 - 再起動スケジュールの設定
 - WindowsUpdateの自動化の設定
 - WindowsUpdateのアクティブ時間の設定
- すべての医療機関等で設定してください
- 資格確認端末の電源ON・OFFを自動で行う医療機関等は追加で設定してください
- 資格確認端末の電源ON・OFFを手動で行う医療機関等は追加で設定してください

以下の医療機関等について、●の付いた項目は必須です。以外の項目は必要に応じて設定してください。

- ・レセプトコンピュータと資格確認端末を兼用する医療機関等
- ・資格確認端末のOSがWindows10 Proの医療機関等

プロキシサーバーを設定します

1 Microsoft Edgeを起動し、（設定など）から**設定**をクリックします。



2 設定が表示されます。
システムをクリックします。



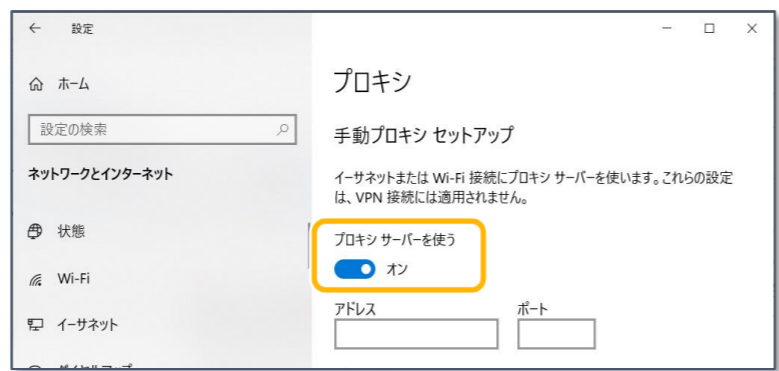
3 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

3 システムが表示されます。
コンピューターのプロキシ設定を開く をクリックします。



4 プロキシが表示されます。
手動プロキシ セットアップ のプロキシサーバーを使うの設定を有効（トグルボタンが右側にある状態）にします。



! プロキシ設定の内容は利用される配信方法（ネットワーク構成）に応じて異なります。ご利用の環境がどの構成に当てはまるかご確認の上、次の 5 の設定を行ってください。

- ① 配信拠点起点の構成
 → 本手順のとおり設定してください（次の 5 の設定を行ってください）。
- ② ネットワーク事業者起点の構成
 → 提供するネットワーク事業者にお問い合わせください。
- ③ 医療機関等起点の構成
 → 医療機関システム管理者、もしくはシステムベンダーへお問い合わせください。
 また、プロキシサーバーが以下の要件を満たす必要があります。併せてご確認ください。
 - ・ 手動プロキシ セットアップによるプロキシサーバー指定が可能であること
 - ・ 「d2vhvuj0j7c8bh.cloudfront.net」への接続が許可されていること
 ※ 上記以外にも、医療機関等の環境に応じて許可が必要なアドレスがある場合は設定してください。
 - ・ プロキシ認証が不要であること

使用する回線に応じて、構成は以下のとおり分類されます（2021年6月時点）。

■ IPsec+IKEサービス提供事業者（インターネット接続方式）

事業者名	構成
株式会社NTT PC コミュニケーションズ	配信拠点起点
株式会社NTTデータ中国	ネットワーク事業者起点
富士通株式会社	配信拠点起点
三菱電機 インフォメーション ネットワーク 株式会社	ネットワーク事業者起点

■ IP-VPN接続方式（光回線）

事業者名	構成
NTT東日本・西日本	配信拠点起点
中部テレコミュニケーション 株式会社（CTC）	配信拠点起点
株式会社Q Tnet	配信拠点起点

■ その他

医療機関・薬局等のプロキシサーバー等を使用し、インターネットを経由して、配信クラウド、マイクロソフトに直接アクセス（構成：医療機関等起点）

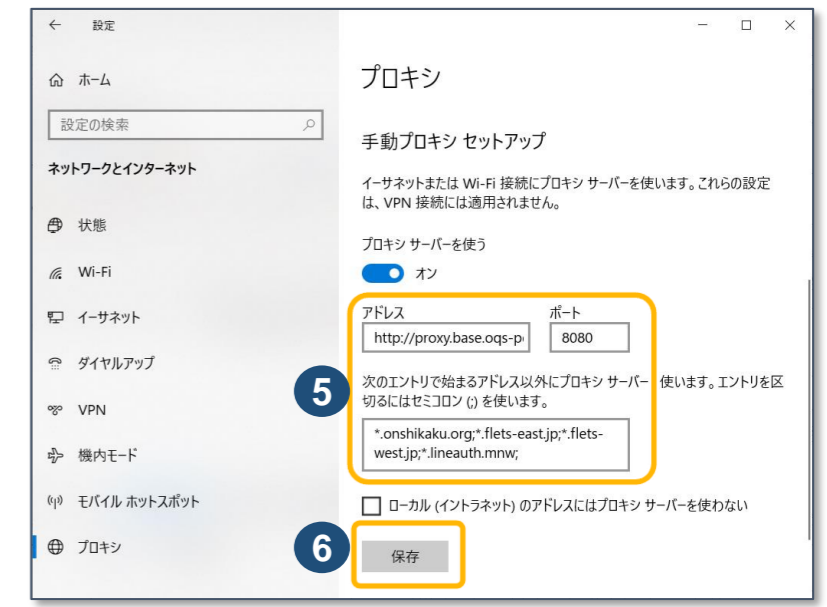
5 以下の内容を入力します。

アドレス
 proxy.base.oqs-pdl.org
ポート 8080

次のエントリで始まるアドレス以外にプロキシサーバーを使います。…

- *.onshikaku.org;
 - *.flets-east.jp;
 - *.flets-west.jp;
 - *.lineauth.mnw;
 - *.obn.managedpki.ne.jp;
 - *.cybertrust.ne.jp;
 - *.secomtrust.net;
 - *.rece;
- pweb.base.oqs-pdl.org

6 保存 をクリックします。



! **こんなときは！**
プロキシサーバーを使用しないアドレスの登録について
 左記以外にも、医療機関等の環境に応じて登録が必要なアドレスがある場合は追加してください。
 複数のアドレスを登録する場合、アドレスごとに区切り文字（セミコロン（;））を必ず入力してください。

7 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

7 コマンドプロンプトを起動します。

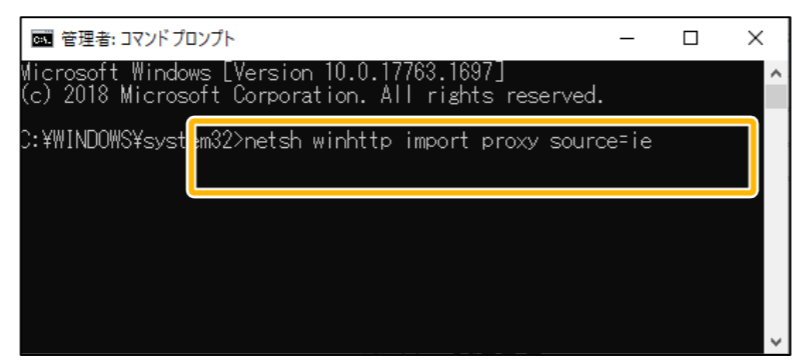
スタートボタンをクリックし、表示されるメニューから**Windowsシステムツール**を選択します。
コマンドプロンプトメニューを右クリックし、**その他**→**管理者として実行**をクリックします。



8 管理者：コマンドプロンプトが表示されます。

以下のコマンドを入力し、Enterキーを押します。

```
netsh winhttp import proxy source=ie
```



9 以下の内容が表示されたことを確認します。

表示内容

現在の WinHTTP プロキシ設定
 プロキシ サーバー : http://proxy.base.oqs-pdl.org:8080
 バイパス一覧 : *.onshikaku.org;*.flets-east.jp;*.flets-west.jp;
 .lineauth.mnw;.obn.managedpki.ne.jp;
 .cybertrust.ne.jp;.secomtrust.net;
 *.rece;pweb.base.oqs-pdl.org



※バイパス一覧は表示内容確認のため、アドレスごとに任意の箇所で行っています（実際は改行されません。）。

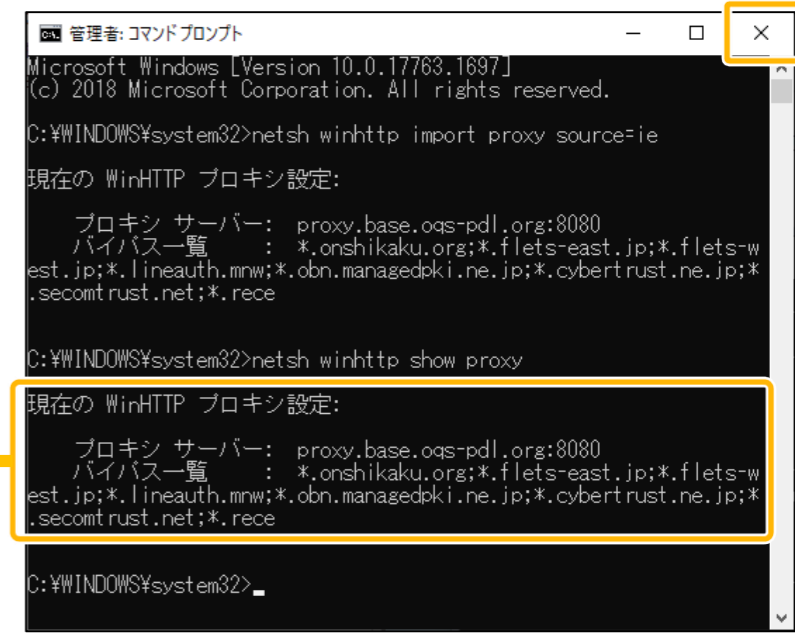
10 以下のコマンドを入力し、Enterキーを押します。

```
netsh winhttp show proxy
```



11 以下の内容（9と同じ）が表示されたことを確認します。

確認が完了したら、右上の×（閉じる）をクリックして画面を閉じます。



表示内容

現在の WinHTTP プロキシ設定
 プロキシ サーバー : http://proxy.base.oqs-pdl.org:8080
 バイパス一覧 : *.onshikaku.org;*.flets-east.jp;*.flets-west.jp;
 .lineauth.mnw;.obn.managedpki.ne.jp;
 .cybertrust.ne.jp;.secomtrust.net;
 *.rece;pweb.base.oqs-pdl.org

※バイパス一覧は表示内容確認のため、アドレスごとに任意の箇所で行っています（実際は改行されません。）。

注意

4 (!) で記載したネットワーク事業者起点の構成 又は医療機関等起点の構成の場合は、問い合わせた内容どおりに設定されていることを確認してください。

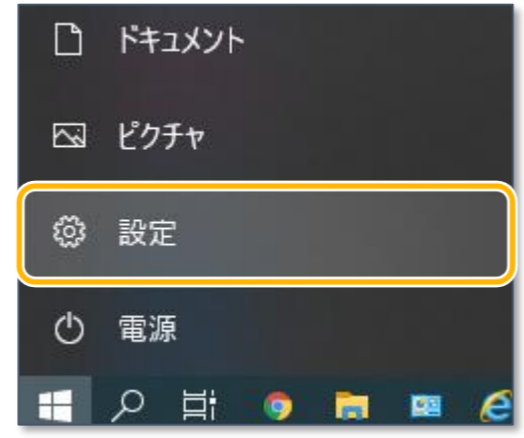
プロキシサーバーが閉塞している期間は、Windows Updateがエラーになります。プロキシサーバーの運用スケジュールは、医療機関等向けポータルサイトを確認してください。

プロキシサーバーの設定が完了しました。

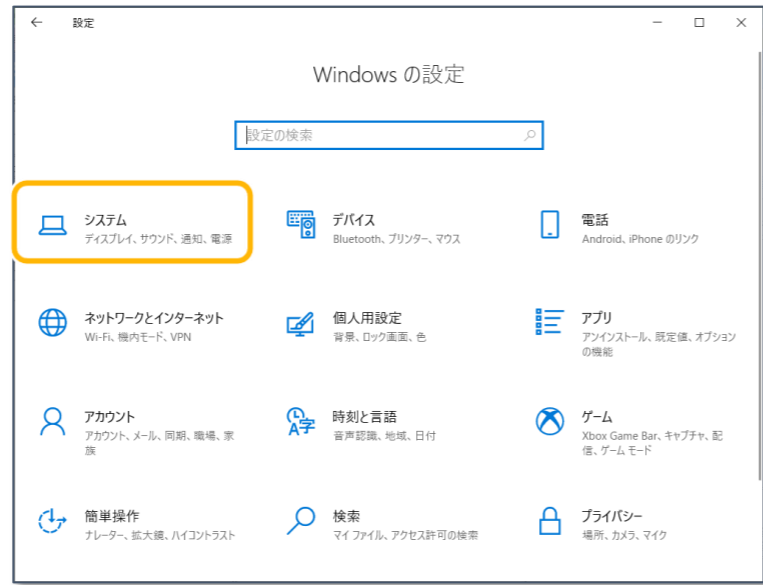
3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

スリープ設定と高速スタートアップを無効にします

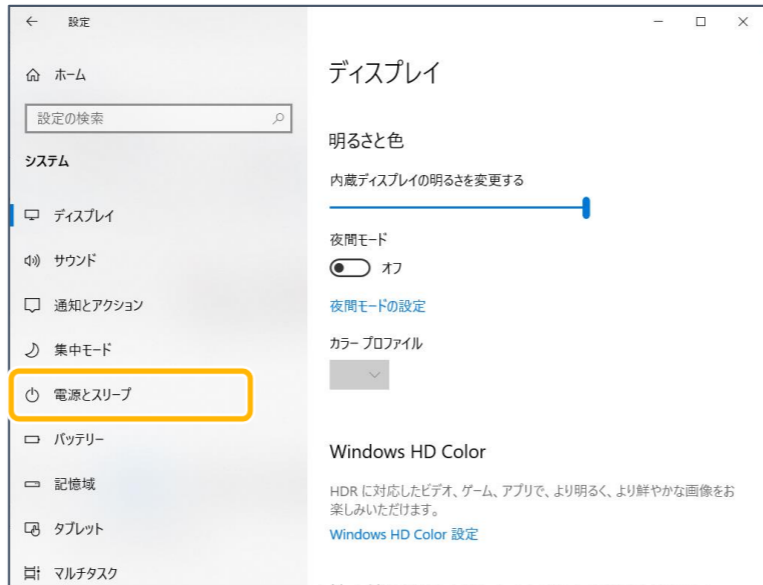
1 スタートメニューの**設定**をクリックします。



2 Windowsの設定が表示されます。
システムをクリックします。

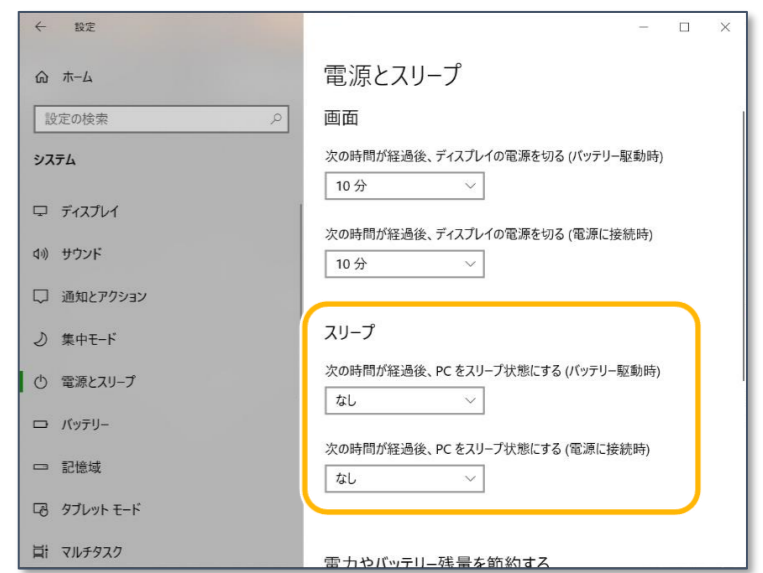


3 設定が表示されます。
電源とスリープをクリックします。



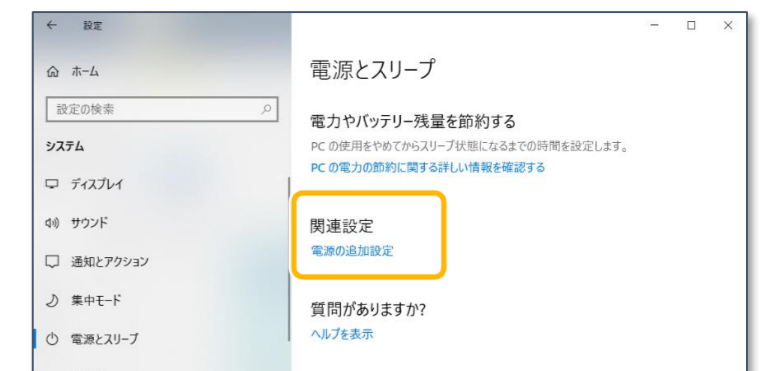
4 電源とスリープが表示されます。

スリープの次の時間が経過後、PCをスリープ状態にする（バッテリー駆動時）ボックスと、次の時間が経過後、PCをスリープ状態にする（電源に接続時）ボックスから**なし**を選択します。



こんなときは！
デスクトップPCの場合
次の時間が経過後、PCをスリープ状態にする（電源に接続時）ボックスのみ設定します。
※（バッテリー駆動時）のメニューはありません。

5 関連設定の**電源の追加設定**をクリックします。



6 電源オプションが表示されます。

電源ボタンの動作を選択するをクリックします。

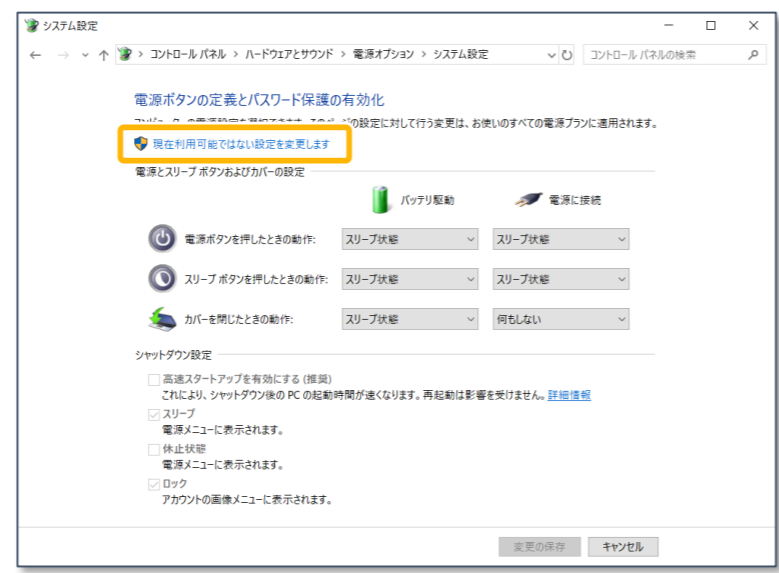


7 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

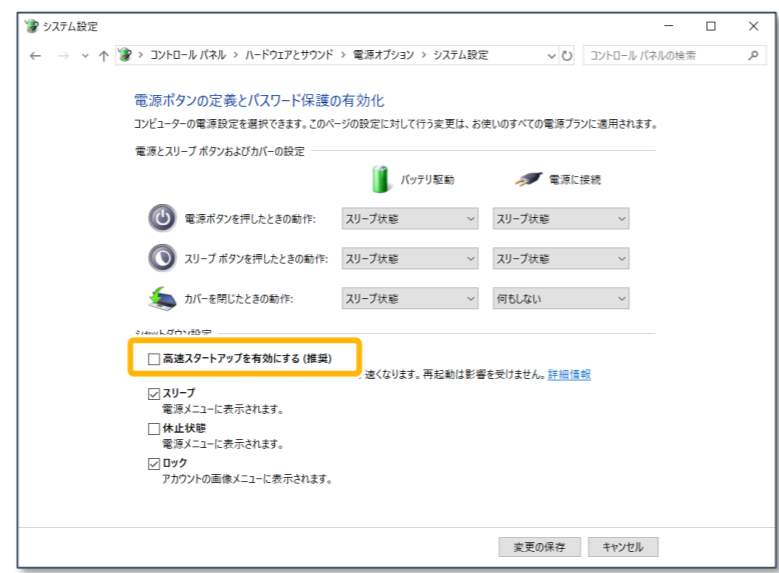
7 システム設定が表示されます。

現在利用可能ではない設定を変更します をクリックします。

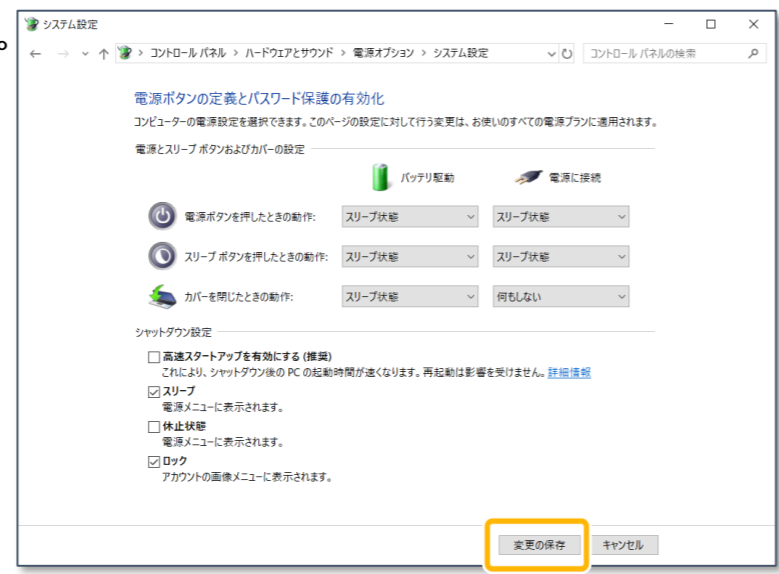


8 シャットダウン設定にある高速スタートアップを有効にする（推奨）をクリックし、チェックを外します。

注意
高速スタートアップが有効の場合、連携アプリケーションや配信アプリケーションが正しく動作いたしません。必ずチェックを外してください。



9 変更の保存をクリックします。

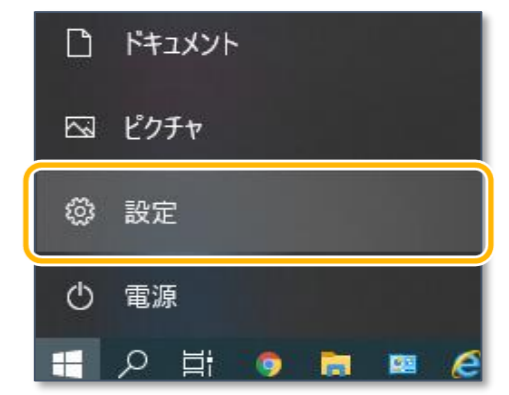


スリープ設定と高速スタートアップの無効化が完了しました。

時刻の設定を変更します

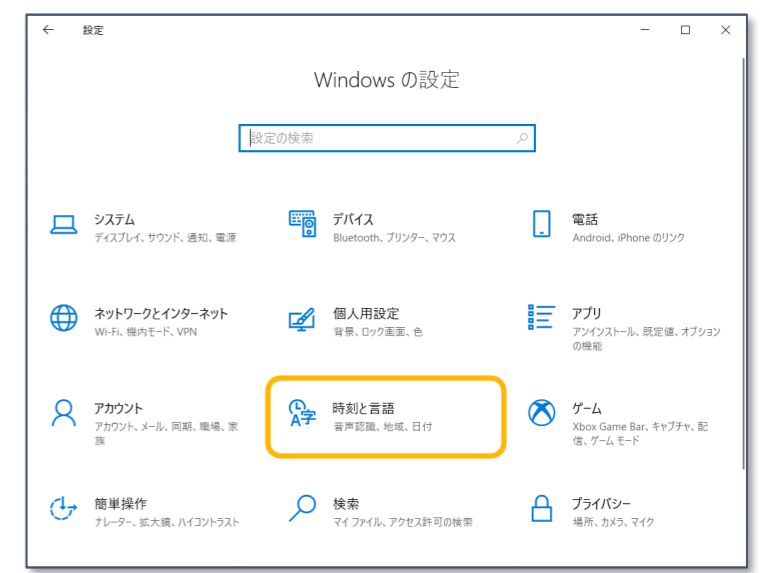
ネットワーク事業者起点の構成、又は医療機関等起点の構成の場合、5 の代替として指定可能なインターネット時刻サーバーが存在するかを構成ごとの問い合わせ先にご確認ください。存在しない場合は本設定をスキップしてください。

1 スタートメニューの設定をクリックします。



2 Windowsの設定が表示されます。

時刻と言語をクリックします。



3 日付と時刻が表示されます。

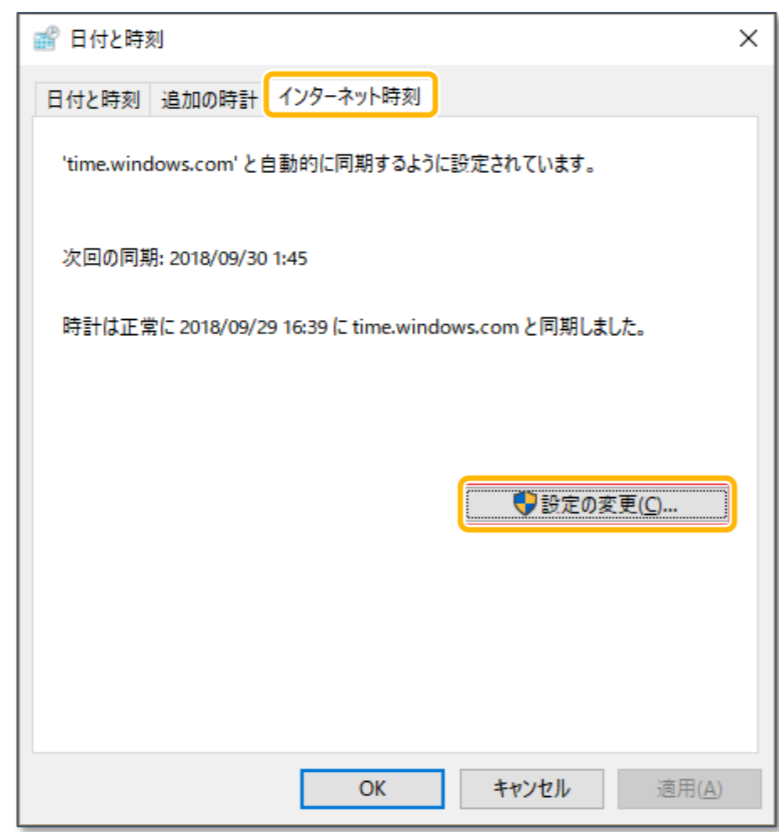
別のタイムゾーンの時計を追加する をクリックします。



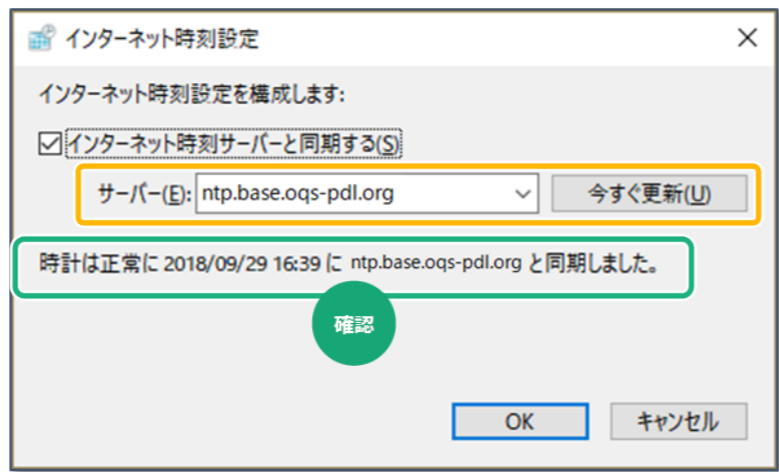
4 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

4 日付と時刻が表示されます。
インターネット時刻タブをクリックし、設定の変更をクリックします。



5 インターネット時刻設定が表示されます。
サーバーに以下の内容を入力し、今すぐ更新をクリックします。
ntp.base.oqs-pdl.org



6 右図のメッセージが表示されたことを確認します。

こんなときは！ 同期が失敗した場合
「ntp.base.oqs-pdl.org と同期中にエラーが発生しました。ピアは解決されていません。」と表示されます。
<対処方法>
入力内容に誤りがないか確認してください。解消しない場合は、通信回線の設定が正しくされていることを確認（ネットワーク事業者より提供されたマニュアルを参照）してください。

こんなときは！ ご利用のネットワーク機器がDNSラウンドロビン非対応の場合
配信拠点のNTPサーバはDNSラウンドロビンにより、複数のIPアドレスを応答します。該当する場合、別紙トラブルシューティングをご確認ください。

別紙 **トラブルシューティング 補24**

時刻の設定変更が完了しました。

！ 自動でパソコンの電源ON・OFFを行う医療機関等は本設定を実施してください。

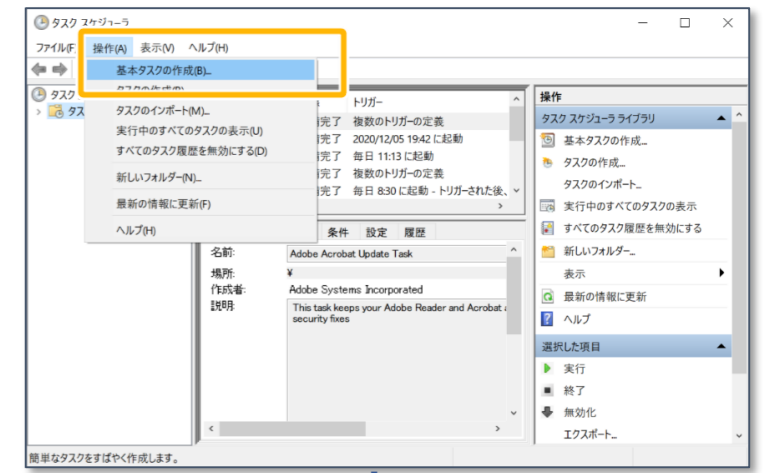
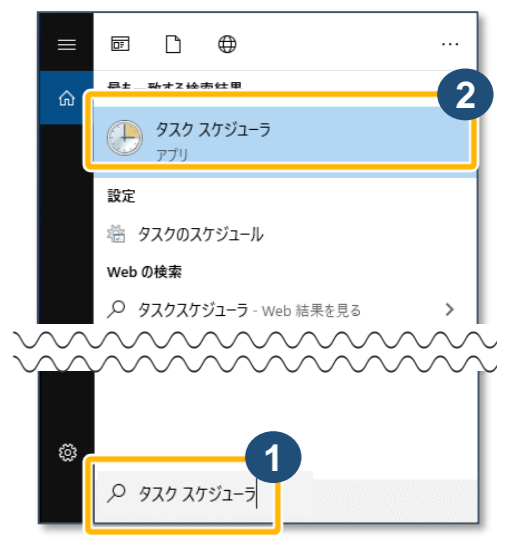
再起動スケジュールを追加します

タスクスケジューラにパソコンの再起動を自動で実行する設定を行います。パソコンの再起動によって、配信アプリケーションによる各種アプリケーションの自動更新の適用を行います。

1 検索をクリックし、検索ボックスにタスクスケジューラと入力します。

2 検索結果から、タスクスケジューラをクリックします。

3 タスクスケジューラが表示されます。
メニューバーの操作から基本タスクの作成をクリックします。

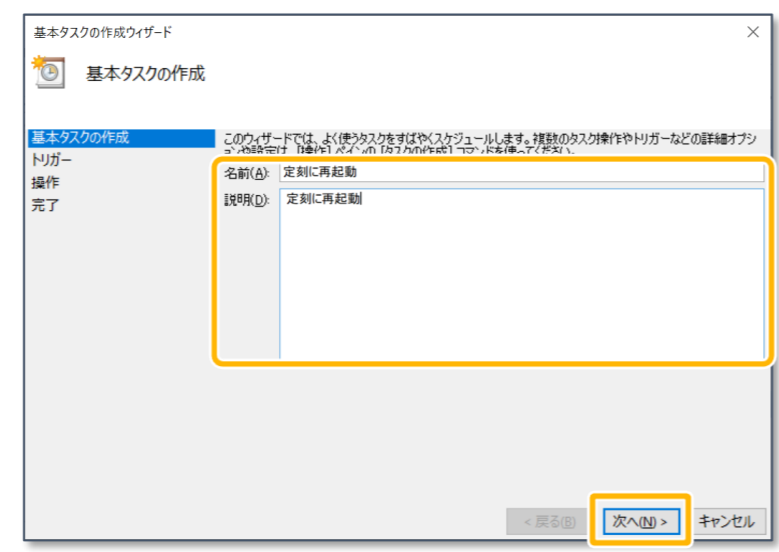


4 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

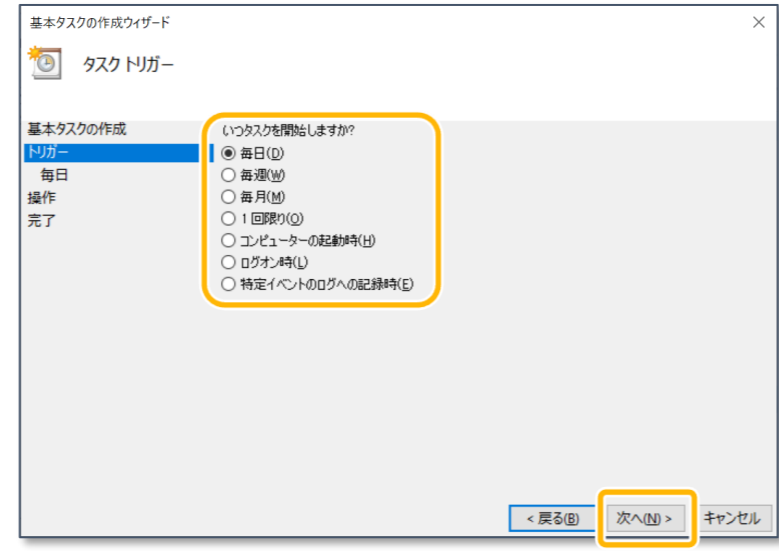
4 基本タスクの作成ウィザードが表示されます。

名前と説明に定刻に再起動と入力し、次へをクリックします。



5 タスクトリガーが表示されます。

タスクの開始を毎日を選択し、次へをクリックします。



6 毎日が表示されます。

タスクの開始日時に、現在時刻が初期表示されているため、業務に支障がないよう診療（業務）時間外で再起動の時刻を設定します。

間隔は1日になっていることを確認します。

次へをクリックします。

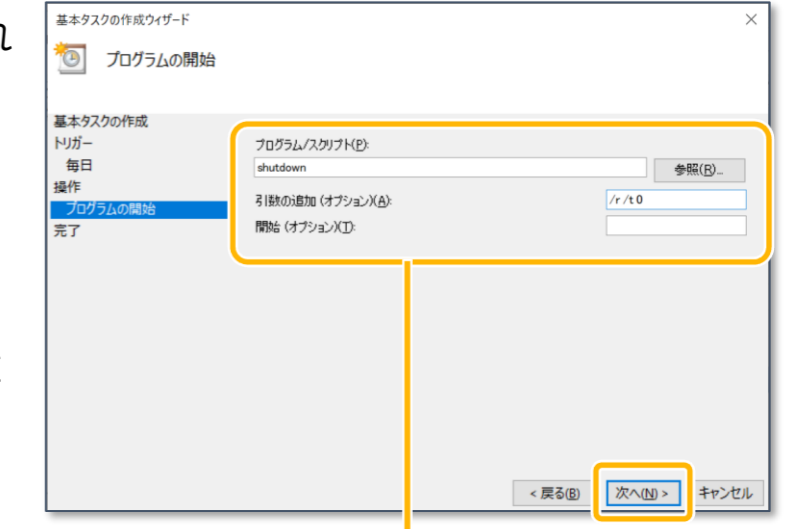


注意
3:50~4:10の間はアクセスが集中するため、この時間帯を避けて時間を設定してください。時間(分)の末尾を0と5以外を指定いただくようお願いいたします。

7 操作が表示されます。
プログラムの開始になっていることを確認します。
次へをクリックします。



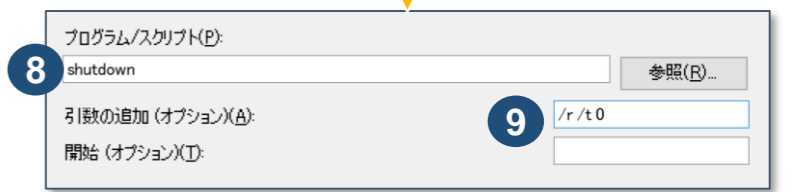
8 プログラムの開始が表示されます。
プログラム/スクリプトに shutdown と入力します。



9 引数の追加（オプション）に /r /t 0 と入力します。

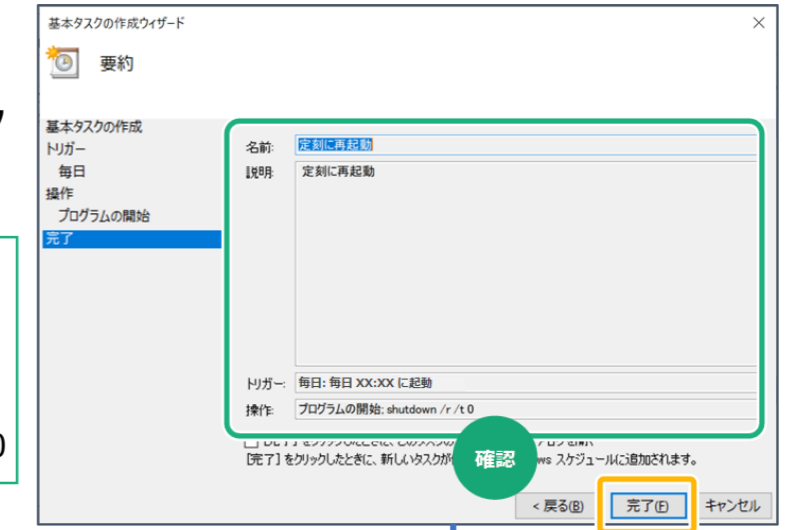
※ /r /t 0 (rの後ろ、tの後ろに半角スペース：「」が必要です)

次へ をクリックします。



10 要約が表示されます。
設定内容を確認し、完了をクリックします。

設定内（例）
名前 : 定刻に再起動
説明 : 定刻に再起動
トリガー : 毎日 XX:XX(※)に起動
※⑥で設定した時刻が表示されていること
プログラムの開始 : shutdown /r /t 0



11 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

11 タスクスケジューラが表示されます。

タスクスケジューラライブラリをクリックし、**タスク一覧**に登録したタスク名（右図の場合、**定刻に再起動**）が表示されたことを確認します。

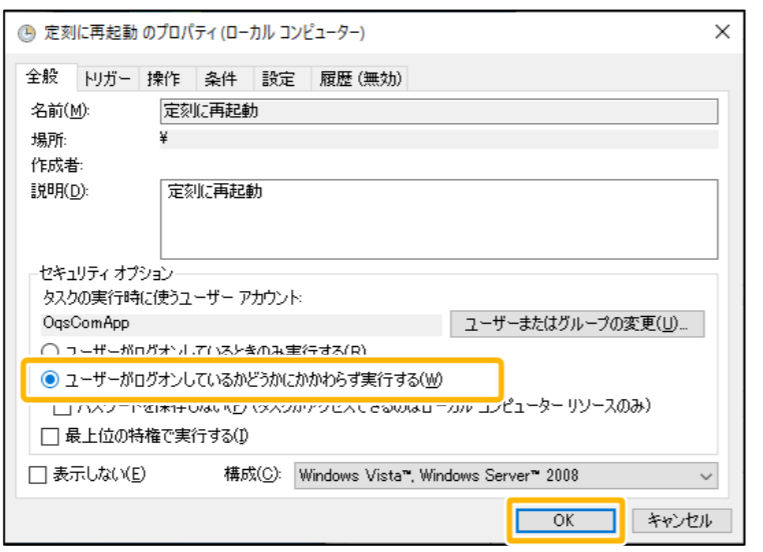
登録したタスク名をダブルクリックし、プロパティを表示します。



12 登録したタスク名（右図の場合、**定刻に再起動**）のプロパティが表示されます。

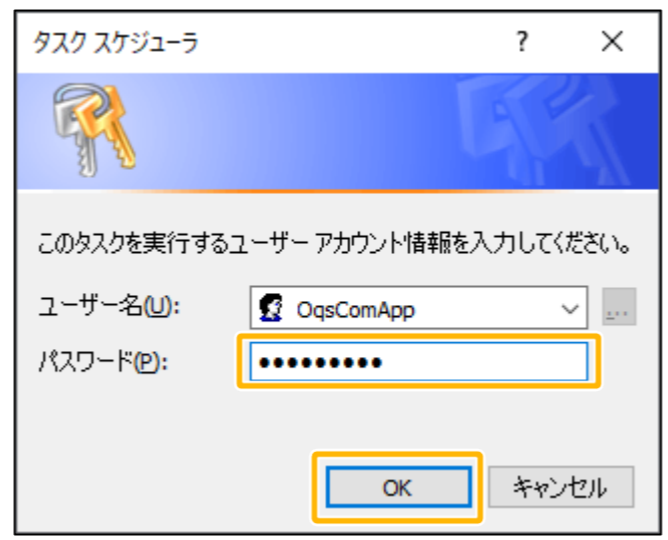
ユーザーがログオンしているかどうかにかかわらず実行する(W)を選択します。

OK をクリックします。



13 パスワード入力画面が表示されます。

OqsComAppのパスワードを入力し、**OK** をクリックします。



再起動スケジュールの設定が完了しました。

! 自動でパソコンの電源ON・OFFを行う医療機関等は本設定を実施してください。

WindowsUpdateの自動化を設定します

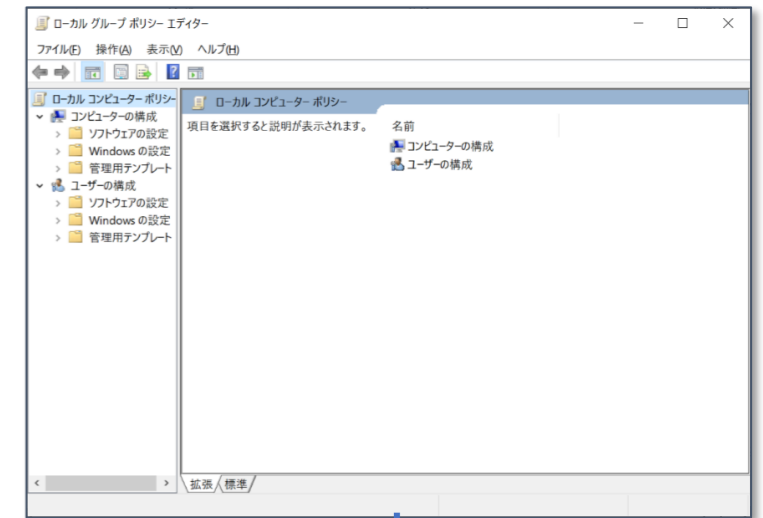
1 検索をクリックし、検索ボックスに**グループポリシー**と入力します。
▲ 半角又は全角スペースを入れてください。

▲ 半角又は全角スペースを入れてください。

2 検索結果から、**グループポリシーの編集**をクリックします。



3 ローカルグループポリシーエディターが表示されます。



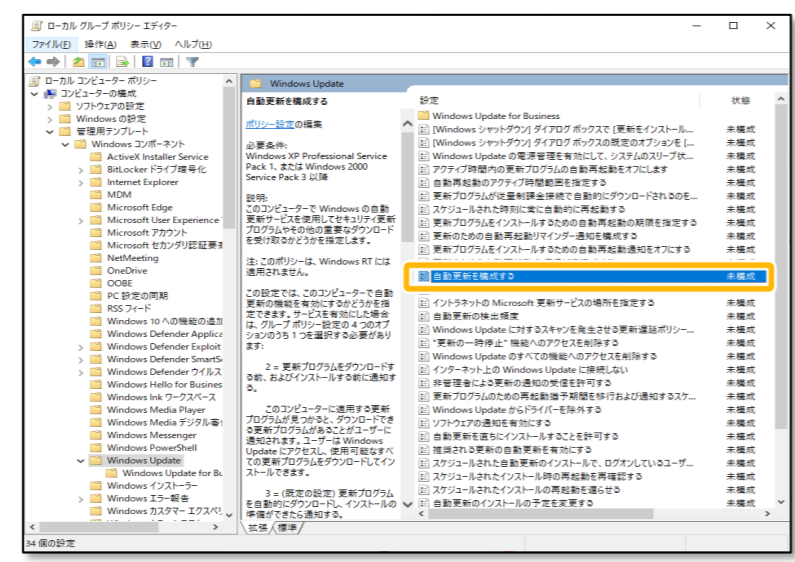
4 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

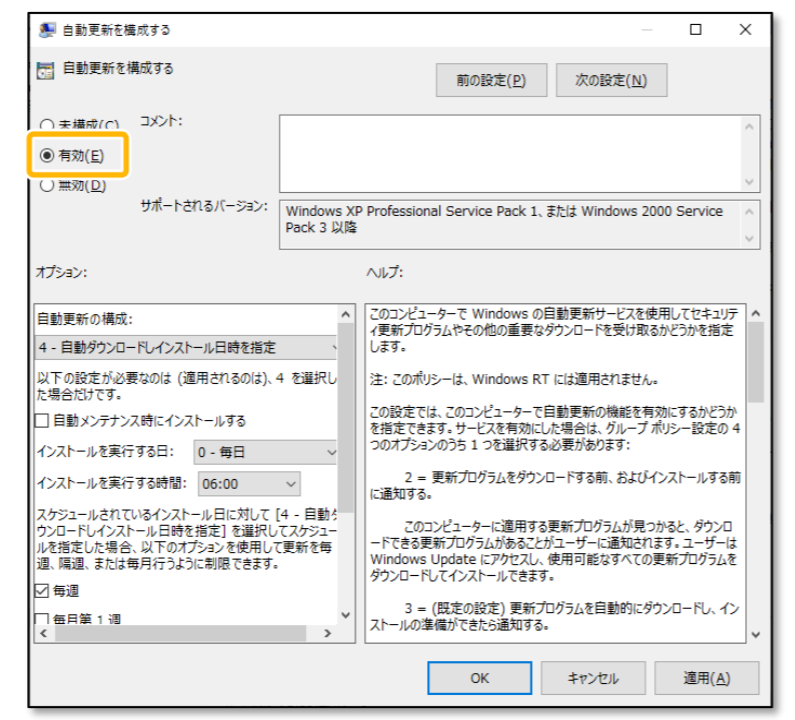
4 メニューから、**コンピューターの構成**→**管理用テンプレート**→**Windowsコンポーネント**→**WindowsUpdate**の順で選択します。



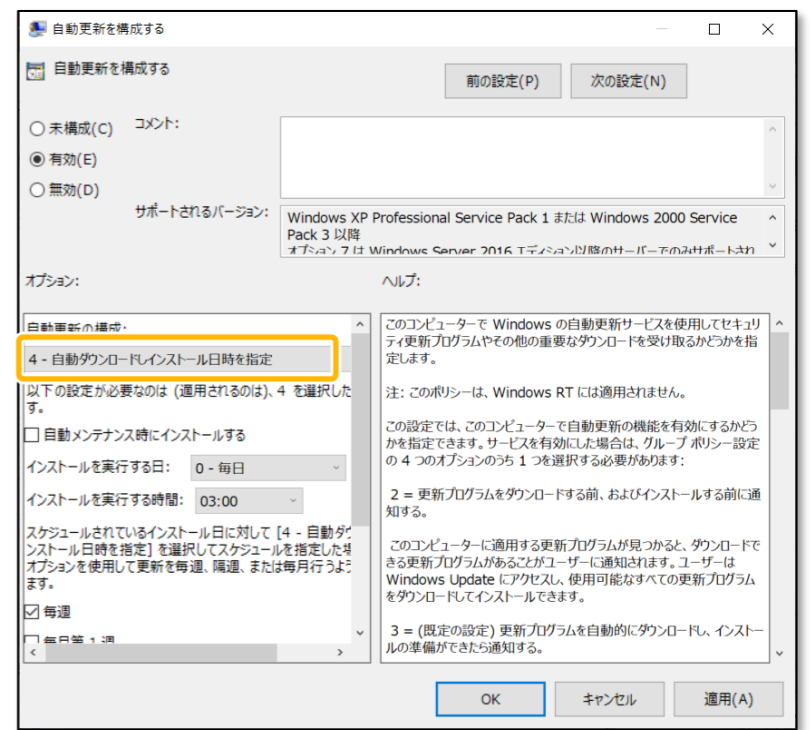
5 **自動更新を構成する** をダブルクリックします。



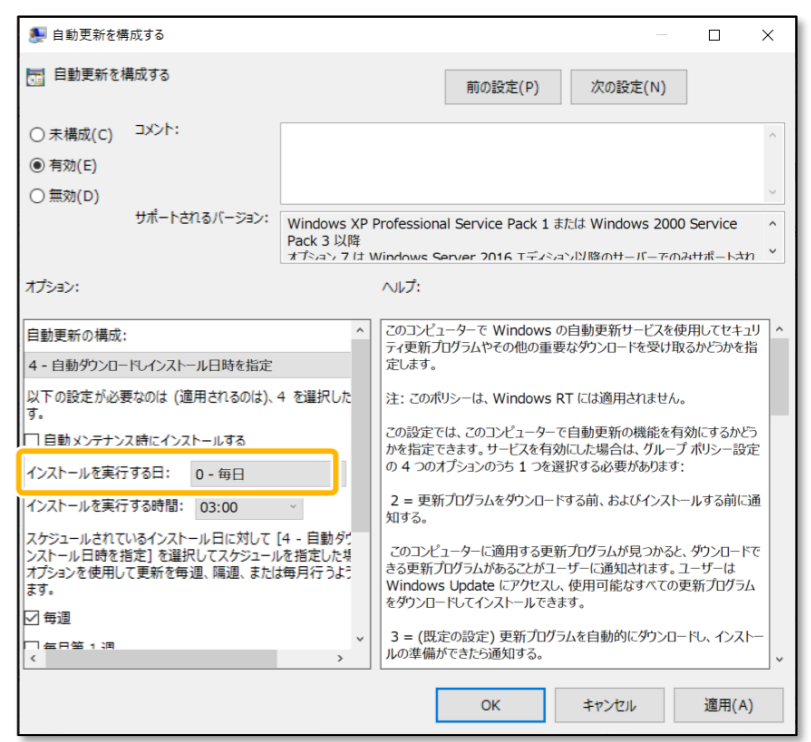
6 自動更新を構成するが表示されます。**有効**を選択します。



7 オプションにて、「**自動更新の構成:**」のプルダウンから、**4 - 自動ダウンロードしインストール日時を指定**を選択します。



8 「**インストールを実行する日:**」のプルダウンから、**0 - 毎日**を選択します。



9 へ進む

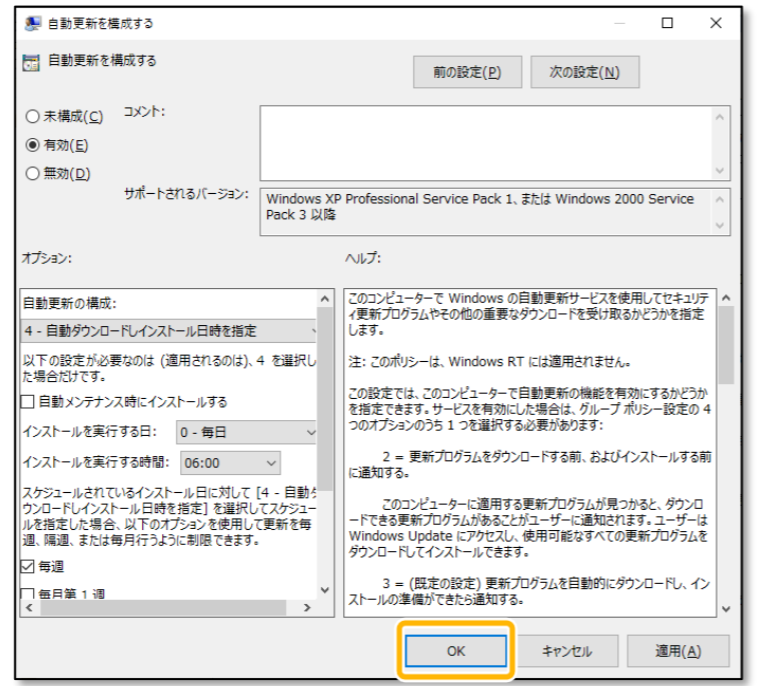
3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

9 「インストールを実行する時間:」のプルダウンから、業務に支障がないよう診療（業務）時間外で再起動の時刻を設定します。

注意
タスクスケジューラによる再起動スケジュール時刻（医療機関等向けセットアップ手順書参照）の後、業務開始より前の時刻を選択してください。



10 OKをクリックします。

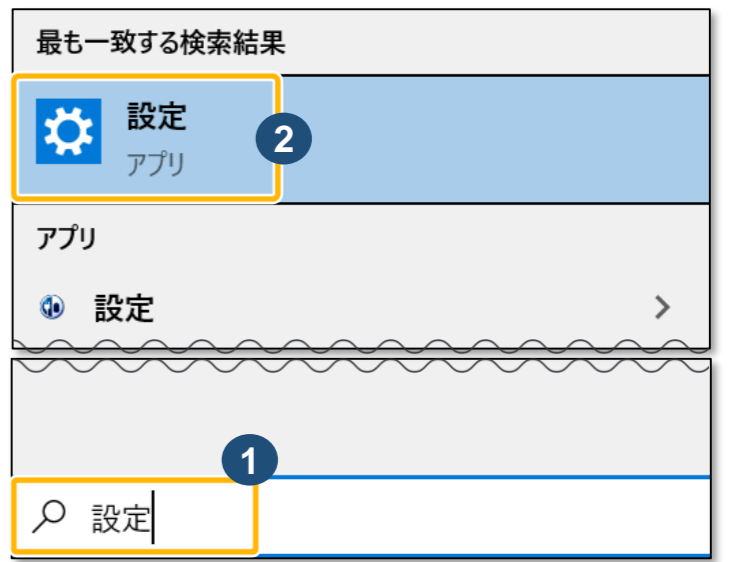


WindowsUpdateの自動化の設定が完了しました。

⚠ 手でパソコンの電源ON・OFFを行う医療機関等は本設定を実施してください。

WindowsUpdateのアクティブ時間を設定します

1 検索をクリックし、検索ボックスに設定と入力します。



2 検索結果から、設定をクリックします。

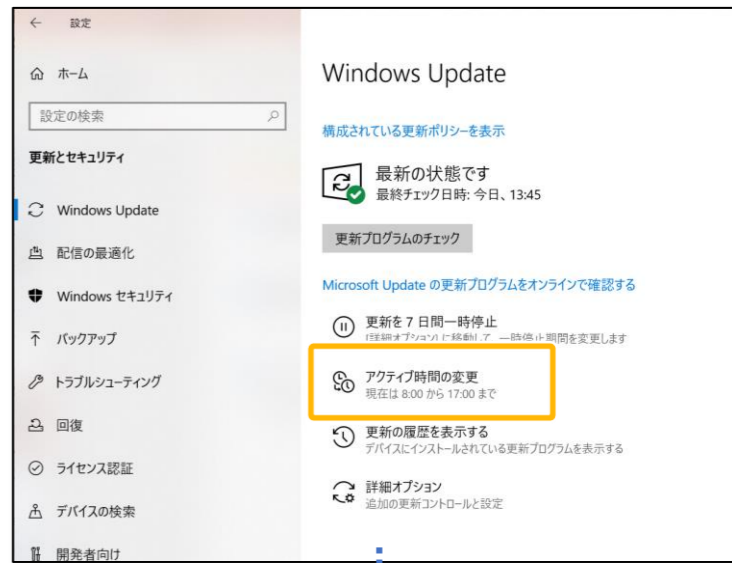


3 Windowsの設定が表示されます。

メニューからの更新とセキュリティをクリックします。

4 WindowsUpdateが表示されます。

右メニューからアクティブ時間の変更をクリックします。

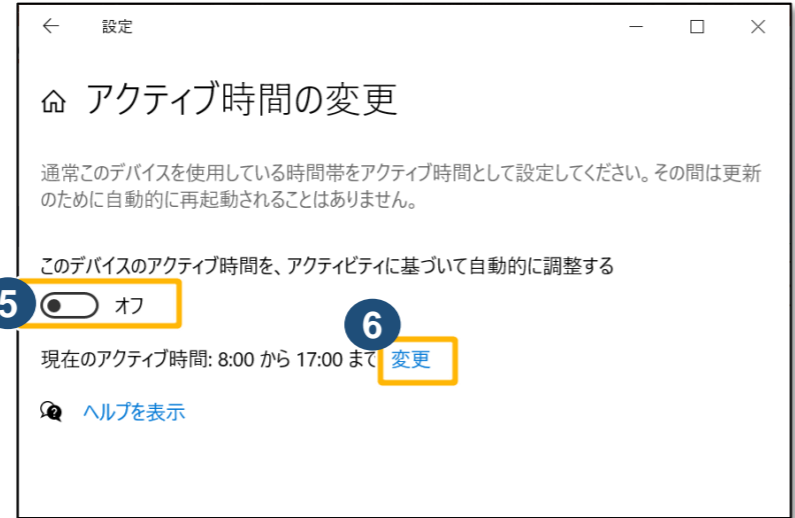


5 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

- 5 アクティブ時間の変更が表示されます。

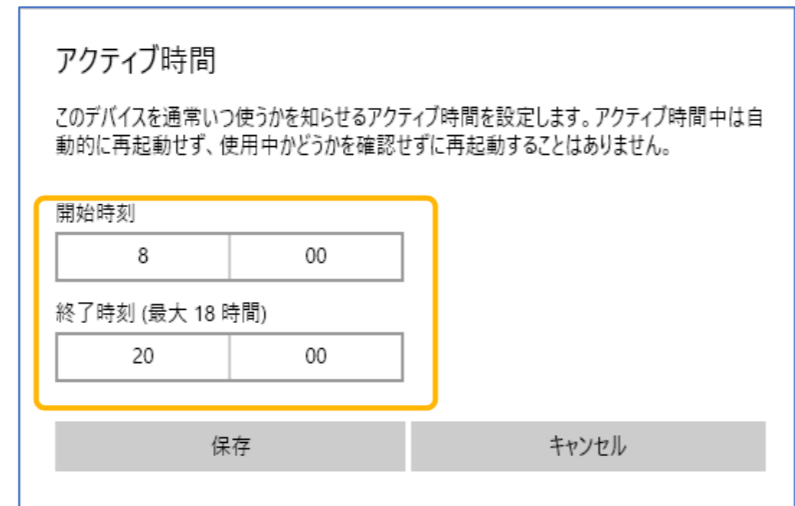
このデバイスのアクティブ時間を、アクティビティに基づいて自動的に調整するを**オフ**にします
- 6 現在のアクティブ時間：**の変更**をクリックします。



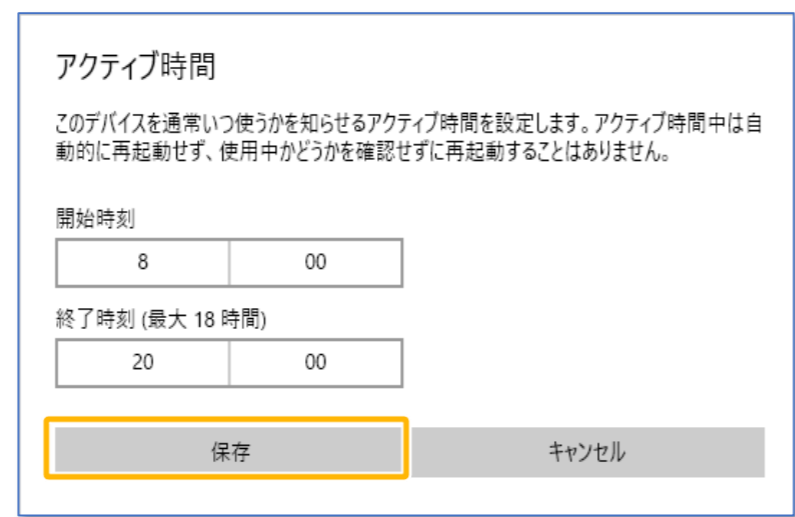
- 7 アクティブ時間が表示されます。

業務に支障が無いよう端末の再起動を抑制したい時間帯を入力します。

例)
開始時刻に**08:00**を選択。
終了時刻に**20:00**を選択。



- 8 **保存**をクリックします。



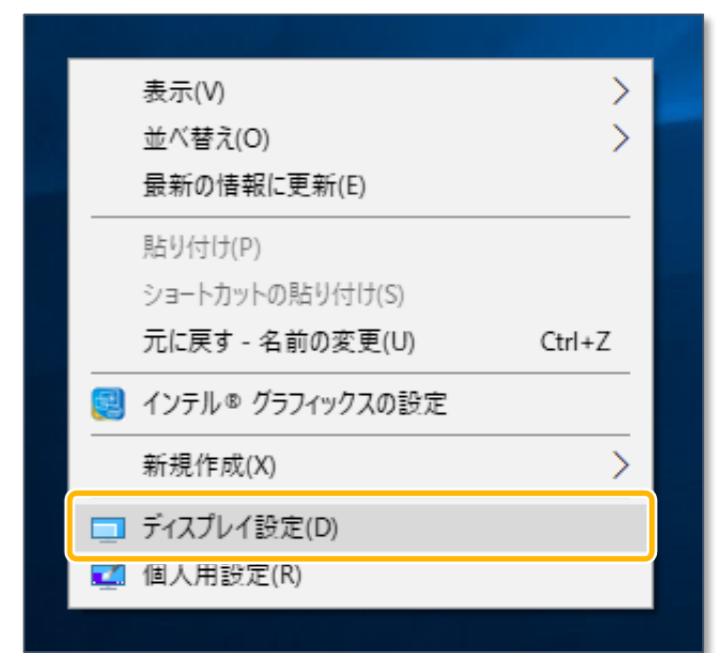
配信アプリケーション準備のためのWindows設定変更が完了しました。

ディスプレイ設定を変更します

オンライン資格確認等システムにおける画面、テキスト、項目等のサイズをディスプレイ設定で100%に設定します。
設定しない場合、下図右側のようにボタンが収まらず、スクロールが発生することがあります。



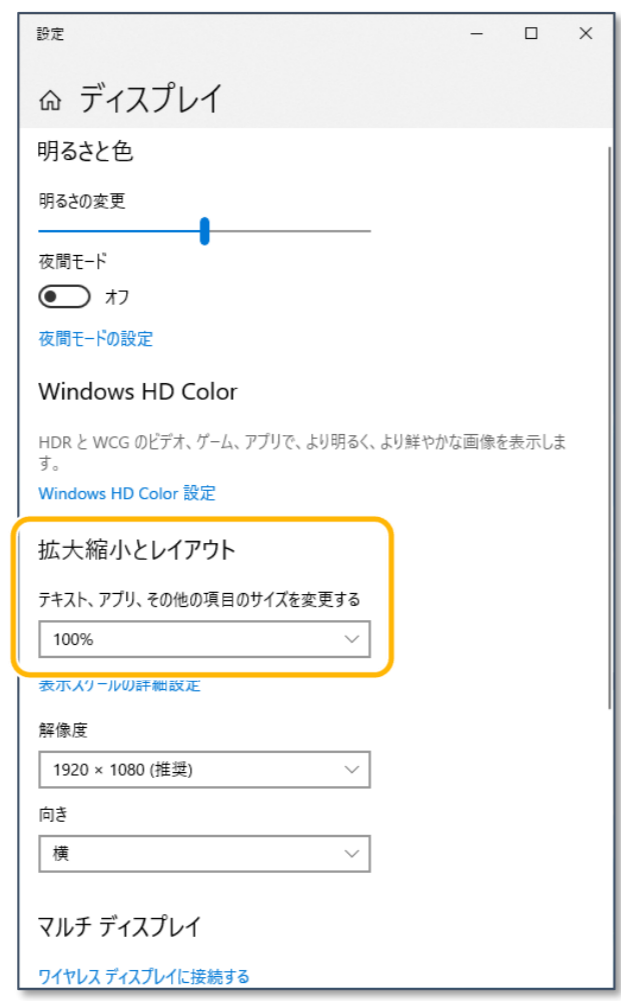
- 1 資格確認端末のデスクトップで右クリックし、表示されるメニューから**ディスプレイ設定**をクリックします。



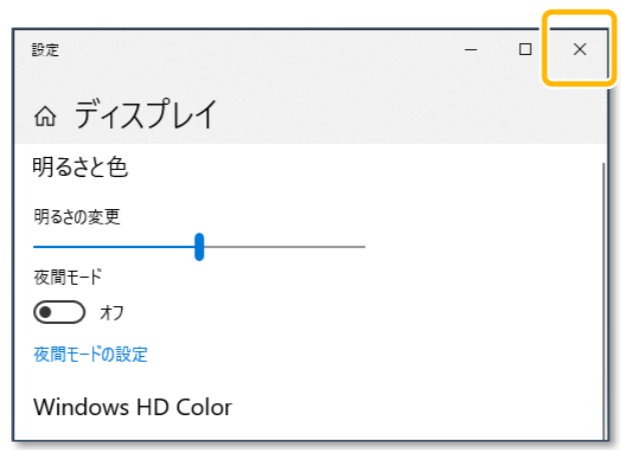
2 へ進む

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

- 2 設定が表示されます。
拡大縮小とレイアウトのテキスト、アプリ、その他の項目のサイズを変更するを100% にします。



- 3 ✕（閉じる）をクリックします。



オンライン資格確認等システムにおける画面、テキスト、項目サイズ等に関するWindows設定変更が完了しました。

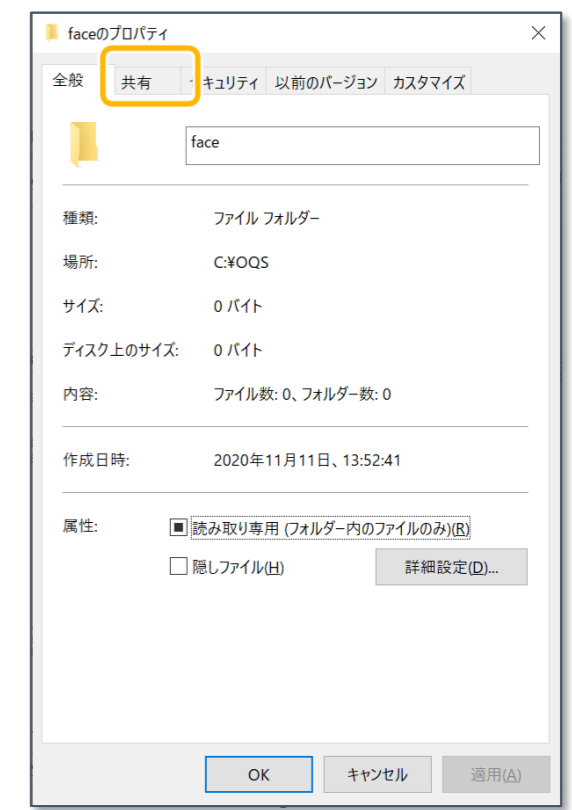
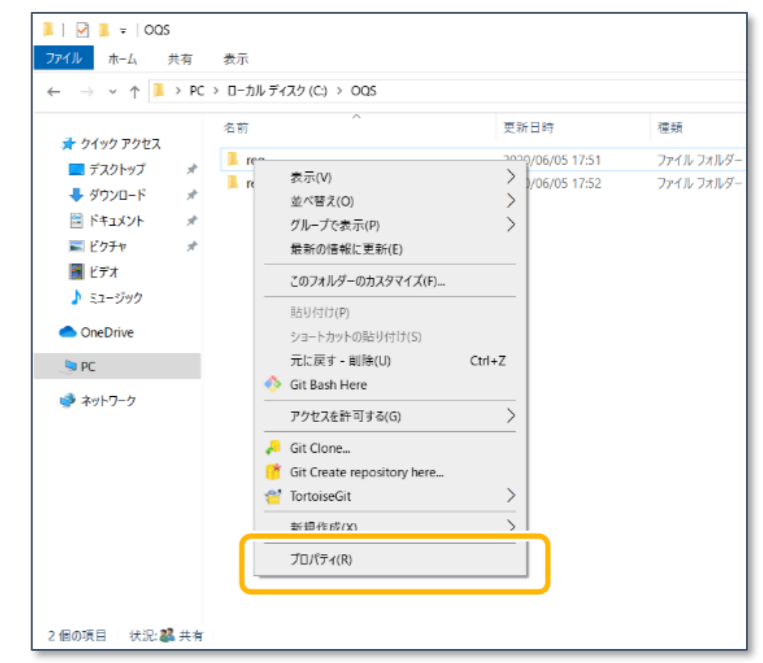
➡➡ 4 顔認証機器利用のための設定をする に進みます

4 顔認証機器利用のための設定をする

顔認証機器を導入する医療機関等は、顔認証連携アプリが資格確認結果を格納するフォルダ（C:¥OQS¥face）の共有設定を行います。

フォルダの共有設定をします

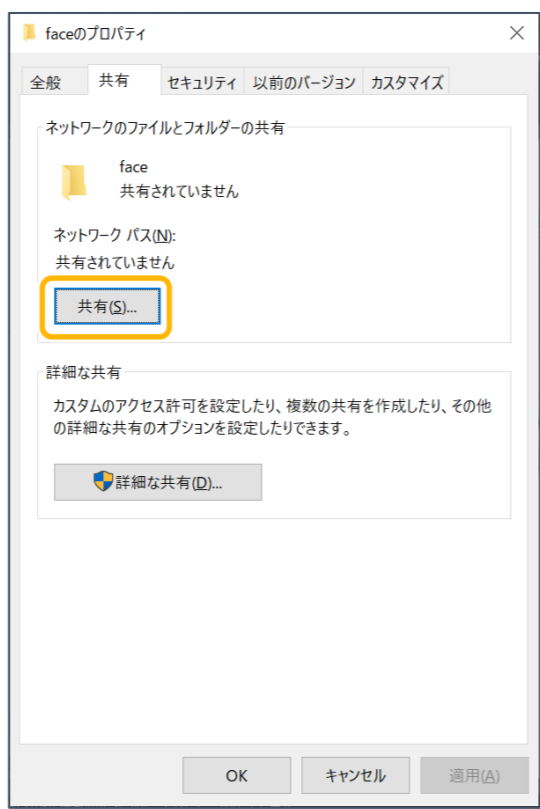
- 1 エクスプローラーで、**ローカルディスク（C:）にあるOQSフォルダを開きます。**
- 2 **faceフォルダを右クリックし、表示されるメニューからプロパティをクリックします。**
- 3 **プロパティが表示されます。共有タブをクリックします。**



4 へ進む

4 顔認証機器利用のための設定をする (つづき)

4 共有タブが表示されます。
共有をクリックします。



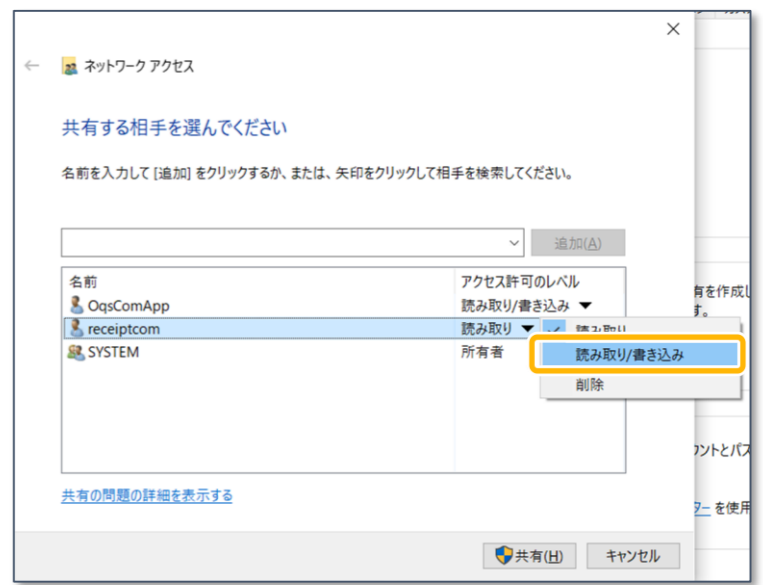
5 ネットワークアクセスが表示されます。

共有を許可するアカウント名 (※医療機関で個別に決定したレセプトコンピュータからアクセスするアカウント名) を選択し、追加をクリックします。

例) receiptcomを選択



6 アクセス許可のレベルの▼をクリックし、読み取り/書き込みを選択します。

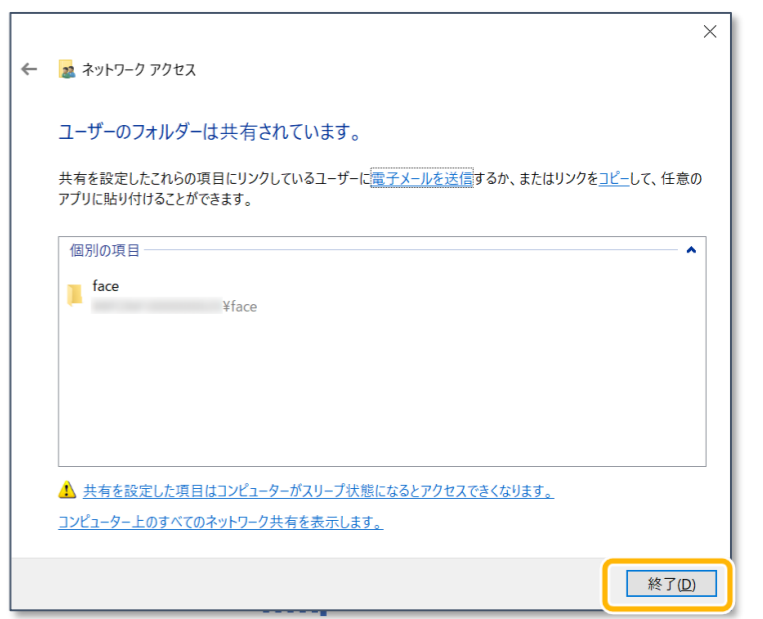


7 アクセス許可レベルに、読み取り/書き込みと表示されます。

共有をクリックします。



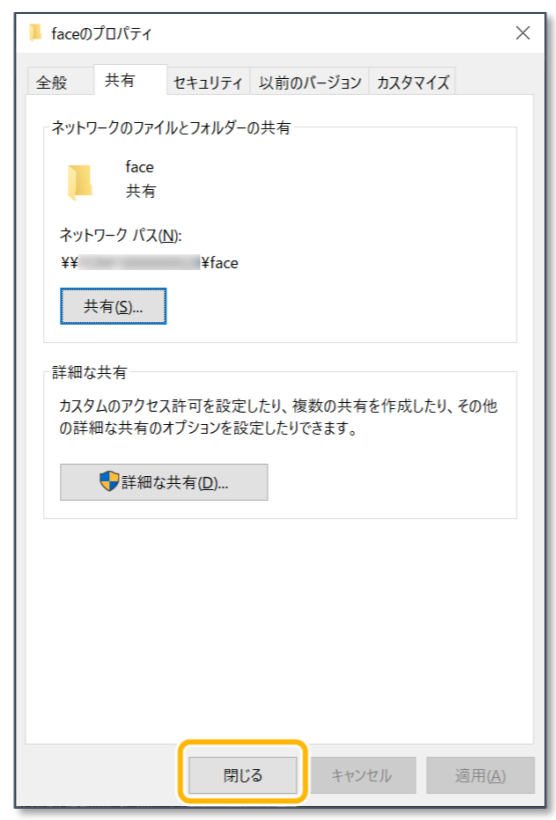
8 終了をクリックします。



9 へ進む

4 顔認証機器利用のための設定をする (つづき)

- 9 プロパティが表示されます。
閉じるをクリックします。



フォルダの共有設定ができました。

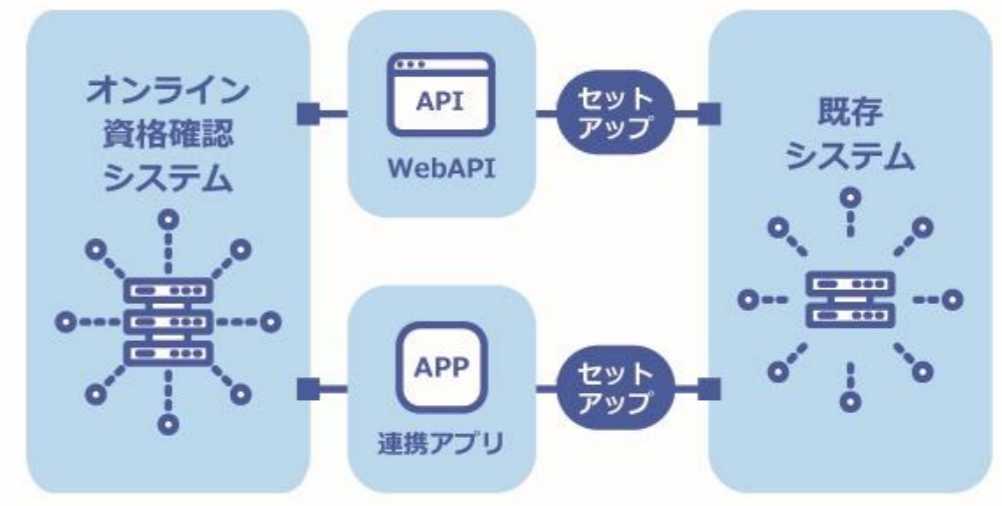
5 連携アプリケーションをインストールする に進みます

こんなときは!
共有するフォルダを変更したい場合やフォルダ格納時に暗号化の設定をしたい場合
共有するフォルダの場所などは、既定の場所以外を設定することができます。また、データ格納時に暗号化するなどセキュリティ設定をすることもできます。これらの設定をする場合は、**顔認証DLL定義説明書**を参照してください。

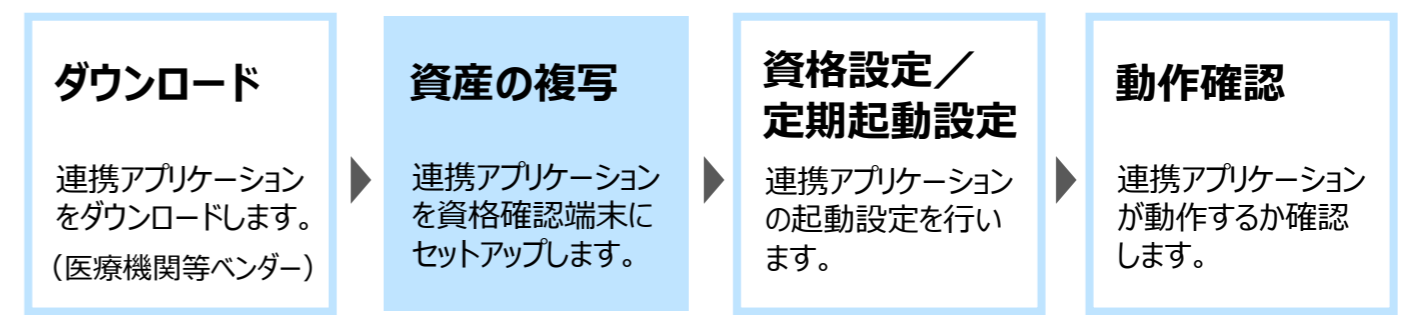
こんなときは!
結果データファイルが共有フォルダに表示されない、操作できない場合
別紙 トラブルシューティングをご確認ください
別紙 **トラブルシューティング 補9**

5 連携アプリケーションをインストールする 作業が必要な医療機関等のみ

HIS等、既存システムから接続する場合の連携アプリケーションを設定します。



連携アプリケーションのインストールは以下の流れで実施します。本項では資産の複写の手順を説明します。



※本項で説明します

注意
資格設定および連携アプリケーションの定期起動の設定については、操作8のアカウント作成で連携アプリ用アカウントを作成した後の設定となります。操作12の資格確認できるか確認で実施します。

注意
電子処方箋管理サービスを利用するには、連携アプリケーションのインストールが必要です。既にインストール済みの場合は、再インストール不要です。

5 連携アプリケーションをインストールする（つづき）

注意
 ZIP形式のインストーラーを提供しておりますが、セットアップで利用するのはinstall.batおよびInstall_after.batではなく、**OQSComApp.msi** です。
 Install.batは、連携アプリケーションが既にインストール済みの場合において、最新バージョンへのアップデート等の上書きインストール時に使用します。

01 連携アプリケーションインストーラーの実行

医療機関等ベンダーより連携アプリケーションを入手しセットアップします。

- 1 連携アプリケーションの**セットアップファイル**をダブルクリックします。



OQSComApp.msi

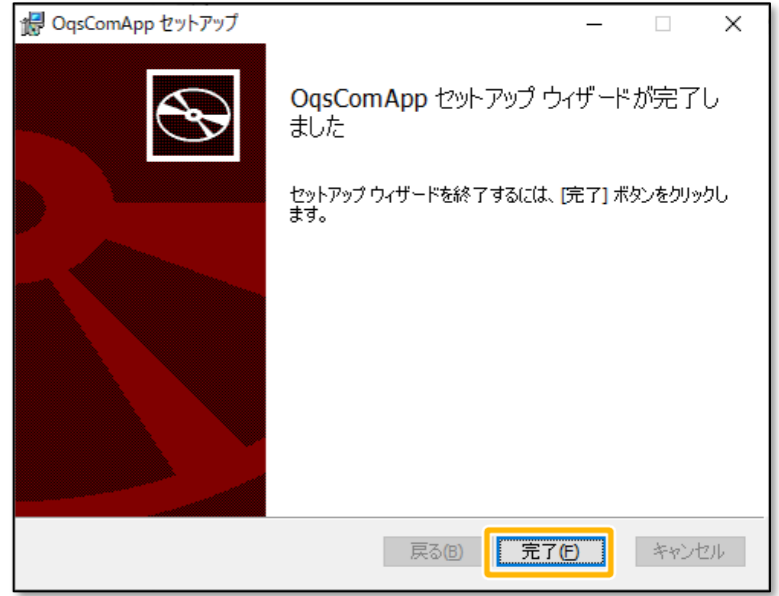
こんなときは！
メッセージ画面が表示された場合
 WindowsによってPCが保護されましたというメッセージ画面が表示された場合は、**実行ボタン**をクリックしてインストーラーを続行します。

- 2 OqsComApp セットアップが表示されます。
 ソフトウェア使用許諾条件の内容をよく読み、同意する場合は**使用許諾契約書に同意します**をチェックして、**インストール**をクリックします。



こんなときは！
メッセージ画面が表示された場合
 このアプリがデバイスに変更を加えることを許可しますか？というメッセージ画面が表示された場合は、**はい**をクリックしてインストールを続行します。

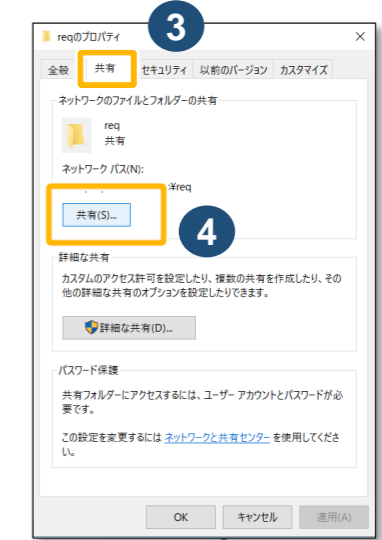
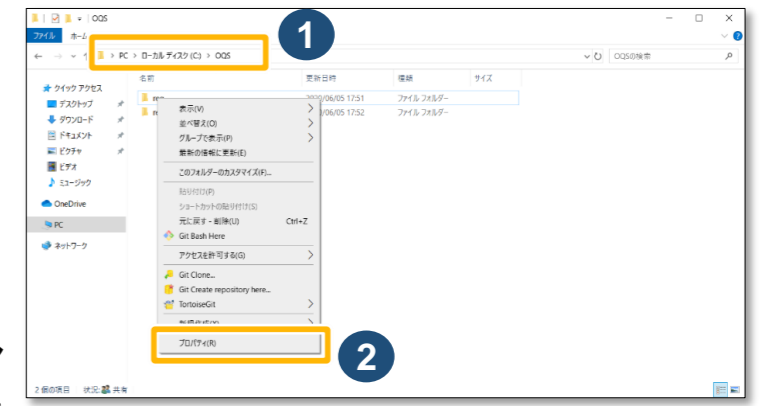
- 3 セットアップが完了すると、**セットアップウィザード完了**が表示されます。
完了をクリックします。



02 共有フォルダの設定

要求データファイルや結果データファイルを格納するフォルダ（C:¥OQS¥req、C:¥OQS¥res）を共有する場合、インストールで生成されたフォルダに共有の設定を行います。

- 1 エクスプローラーで、**ローカルディスク (C:)**にある**OQSフォルダ**を開きます。
- 2 **reqフォルダ** 又は **resフォルダ**を右クリックし、表示されるメニューから**プロパティ**をクリックします。
- 3 **プロパティ**が表示されます。**共有**タブをクリックします。
- 4 **共有**タブが表示されます。**共有**をクリックします。



5へ進む

5 連携アプリケーションをインストールする（つづき）

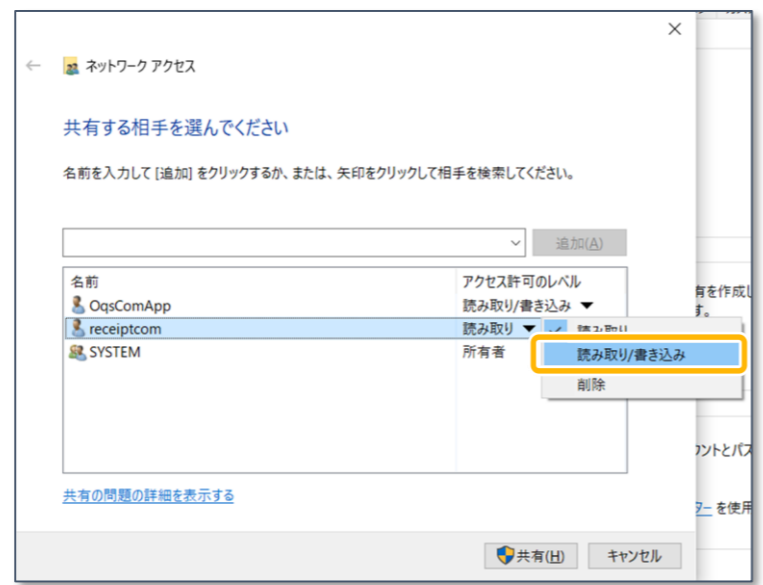
5 ネットワークアクセスが表示されます。

共有を許可するアカウント名（※医療機関で個別に決定したレセプトコンピュータからアクセスするアカウント名）を選択し、**追加** をクリックします。

例)
receiptcomを選択



6 アクセス許可のレベルの▼をクリックし、**読み取り/書き込み**を選択します。

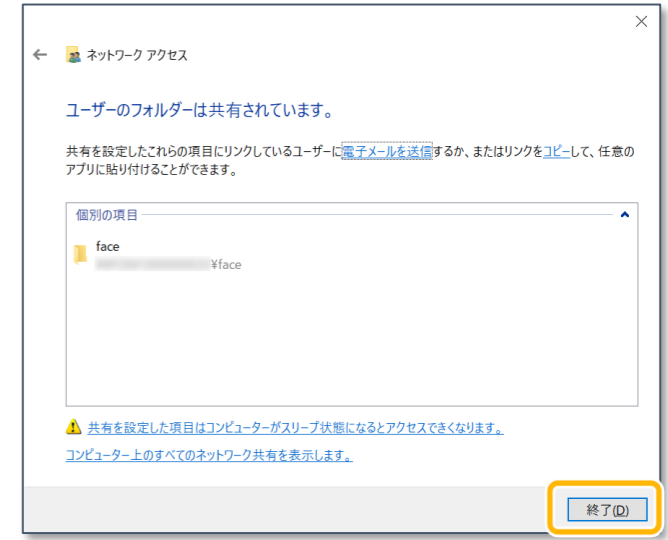


7 アクセス許可レベルに、読み取り/書き込みと表示されます。

共有 をクリックします。



8 終了をクリックします。



9 プロパティが表示されます。
閉じる をクリックします。



連携アプリケーションのインストールが完了した又はインストールが不要な場合は次のステップに進みます。

6 認証局の電子証明書をインストールする に進みます

💡 こんなときは！

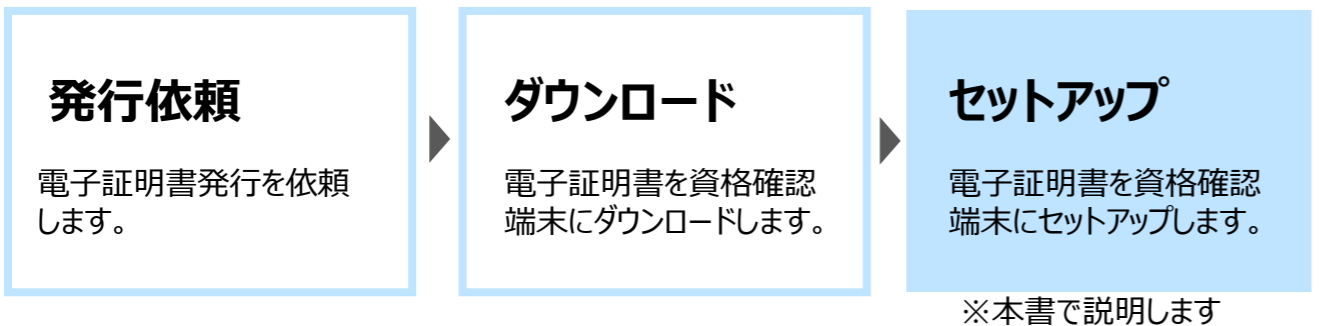
共有するフォルダを変更したい場合やフォルダ格納時に暗号化の設定をしたい場合

共有するフォルダの場所などは、既定の場所以外を設定することができます。また、データ格納時に暗号化するなどセキュリティ設定をすることもできます。これらの設定をする場合は、**連携アプリケーション導入手順書** を参照してください。

6 認証局の電子証明書をインストールする

認証局の電子証明書をインストールします。電子証明書はお使いの端末が、資格確認端末としてセットアップされていることを証明するために必要です。電子証明書をまだ取得していない場合は、以下のサイトから発行依頼またはダウンロードを行い、セットアップしてください。

- 電子証明書発行申請サイトURL : <https://cert.obn.managedpki.ne.jp/p/rcr>
- 電子証明書の取得サイトURL : <https://cert.obn.managedpki.ne.jp/p/rcd>



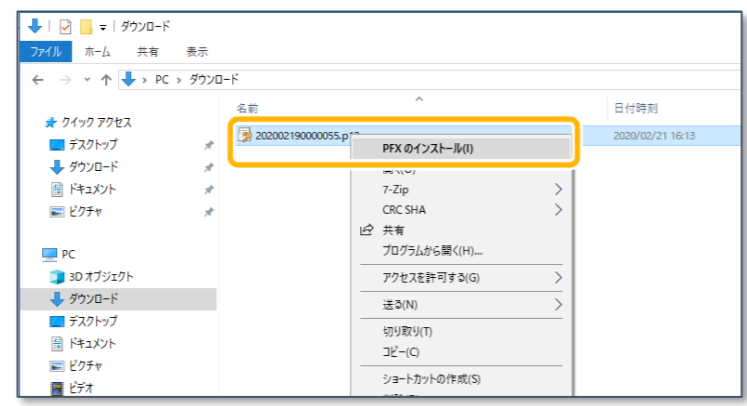
電子証明書の発行依頼については、**オンライン請求ネットワーク関連システム共通認証局電子証明書の発行等申請の手引き**を、電子証明書の取得、更新等の手順については、**オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアル**を参照してください。

01 セットアップ

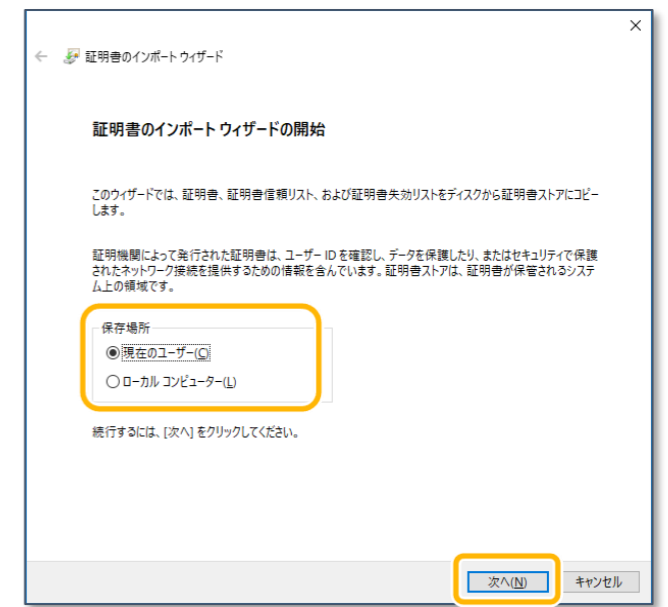
電子証明書を資格確認端末にセットアップします。

- 1 保存した電子証明書ファイルが保存されているフォルダを開きます。

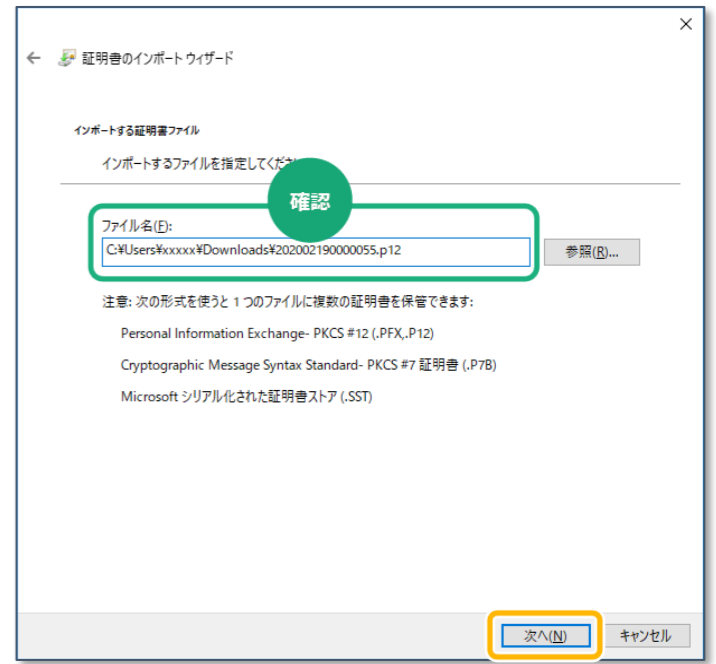
電子証明書ファイルを右クリックし、表示されたメニューから**PFXのインストール**をクリックします。



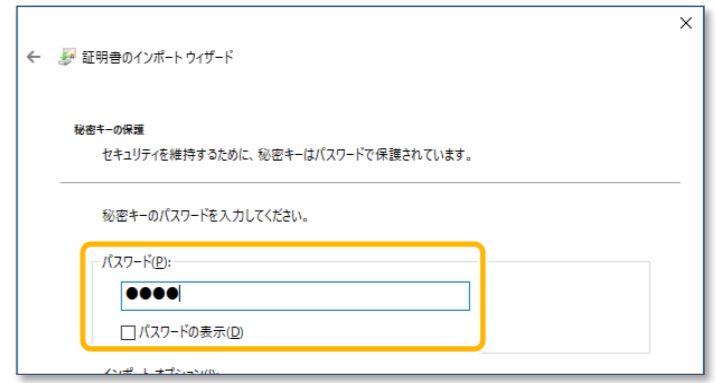
- 2 証明書のインポートウィザードが表示されます。
保存場所は現在のユーザーを選択し、**次へ**をクリックします。



- 3 インポートする証明書ファイルが表示されます。
ファイル名に電子証明書のファイル名が表示されていることを確認し、**次へ**をクリックします。



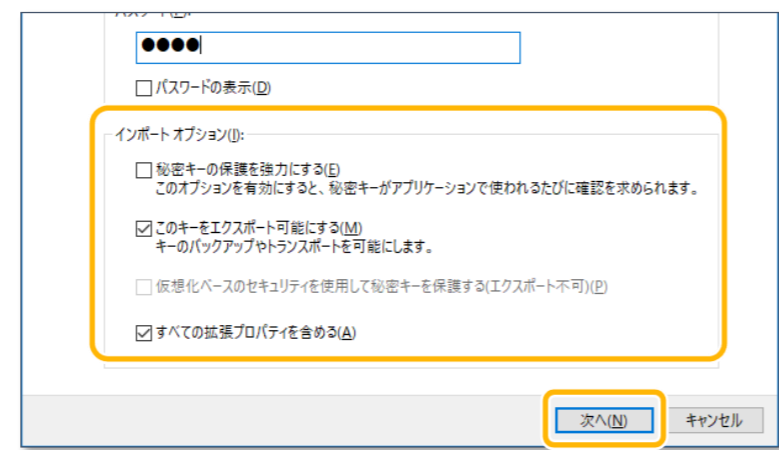
- 4 秘密キーの保護が表示されます。
パスワードに電子証明書ダウンロード時に設定した証明書パスワードを入力します。



6 認証局の電子証明書をインストールする (つづき)

5 インポートオプションについて、以下の内容を設定します。設定後、次へをクリックします。

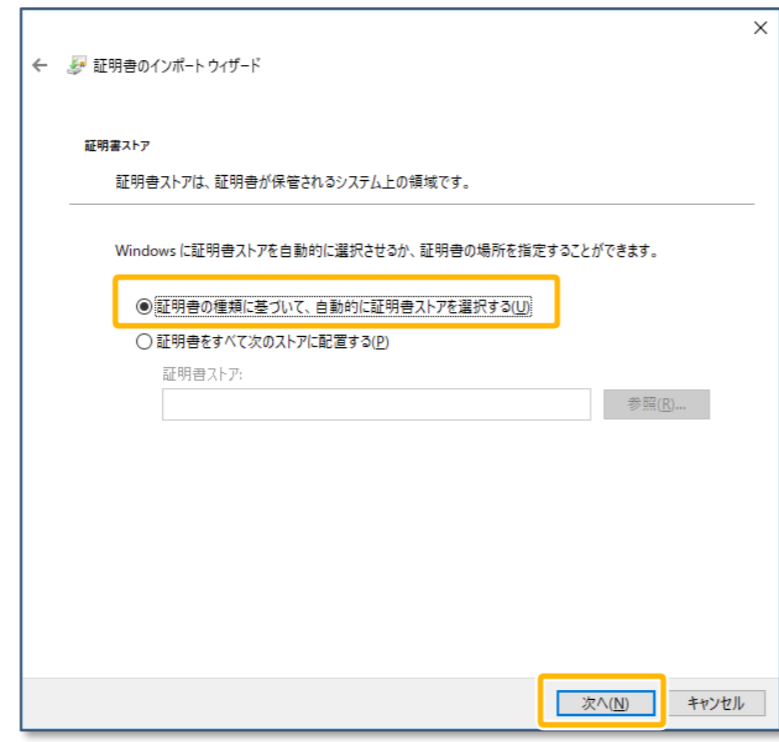
- 秘密キーの保護を強力にする
: チェックをしない
- このキーをエクスポート可能にする
: チェックをする
- すべての拡張プロパティを含める
: チェックをする



💡 こんなときは!
秘密キーの保護を強力にするのチェックを外せない場合
 セキュリティを強化する設定がされているため、**オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアルのPage 8を参照し、パスワードを設定します。**

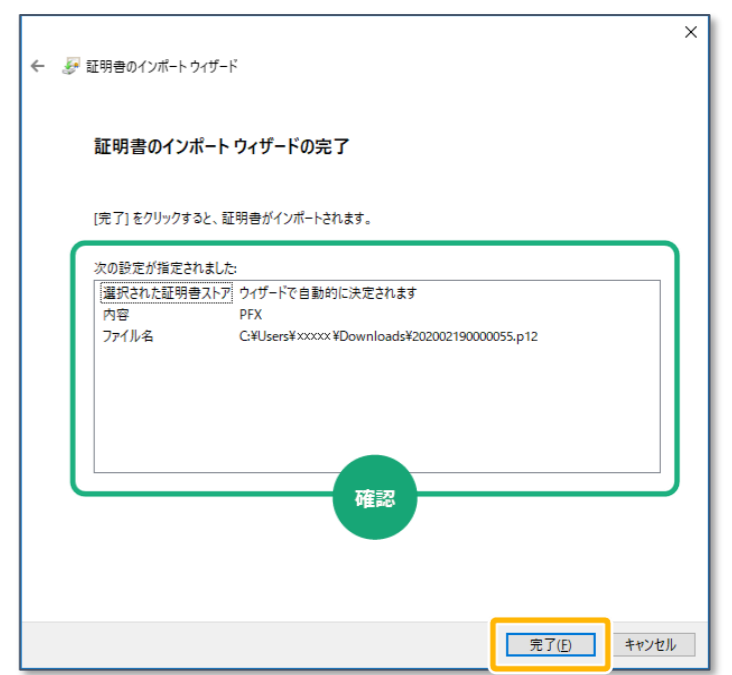
6 証明書ストアが表示されます。

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選択し、次へをクリックします。



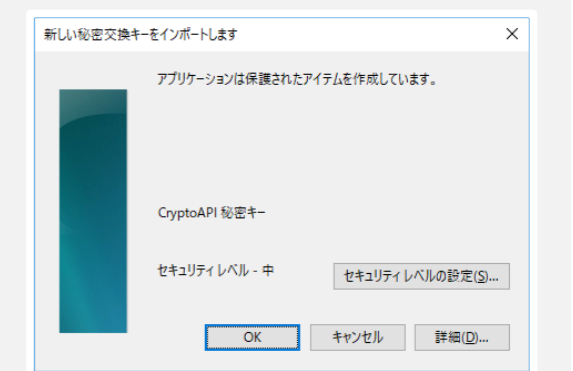
7 証明書のインポートウィザードの完了が表示されます。

電子証明書のファイル名等を確認し、完了をクリックします。



💡 こんなときは!

新しい秘密交換キーをインポートします。が表示された場合
 既存のオン請求端末などをセットアップした場合、右図の画面が表示されることがあります。この場合は、**オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアルのPage 8の(7)～(9)を参照してください。**



8 セキュリティ警告が表示されます。

※本画面が表示されず正しくインポートされました画面が表示された場合は、次に進んでください。

Windowsの信頼されたルート証明機関に証明書発行者(認証局)の証明書を登録するため、はいをクリックします。

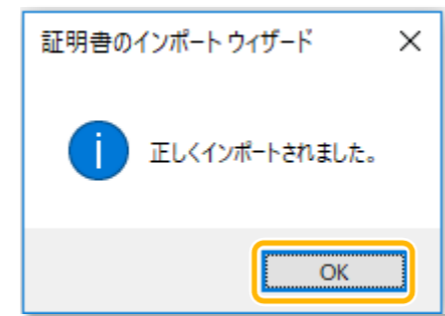


9 へ進む

6 認証局の電子証明書をインストールする (つづき)

注意
いいえ をクリックした場合は、インストール中止となり、電子証明書がセットアップされません。電子証明書のインストールを再度実施する必要があります。
①に戻り、再セットアップしてください。

9 正しくインポートされました。
が表示されます。
OKをクリックします。



3 証明書が表示されます。
個人タブに、発行者が Online Billing NW Common Root CAと表示されている証明書が登録されていることを確認します。

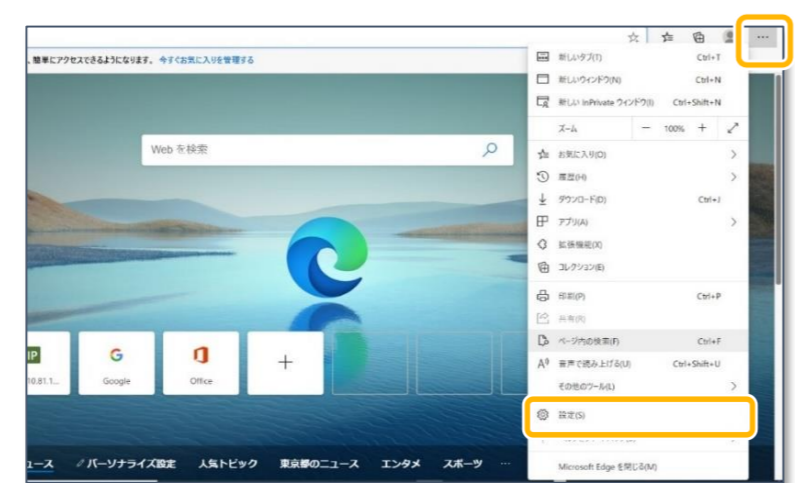


確認後、閉じるをクリックします。

02 セットアップ結果の確認

電子証明書が、ブラウザに正しく登録されたかを確認します。

1 Microsoft Edgeを起動し、
... (設定など) から設定をクリックします。



2 設定が表示されます。
プライバシー、検索、サービスから証明書の管理をクリックします。



注意
MPKIクライアント (Cybertrust Managed PKI Client) のインストール
MPKIクライアントとは、電子証明書の有効期限が到来する前に更新通知を送信したり、電子証明書の更新時期が到来した際に、更新を簡単に行うことができる機能です。以下のマニュアルを参照し、インストールしてください。
【重要】電子証明書に関するお知らせ
更新が必要な電子証明書があります。このメッセージをクリックして証明書を更新してください。
Cybertrust Managed PKI Client
(参照先) オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアル 1.5 MPKIクライアントインストール

注意
MPKIクライアントによる証明書の更新と顔認証機器の更新
証明書の更新を行った場合、顔認証機器の再設定が必要になります。なお、設定にあたっては各社の取扱説明書、操作マニュアル等を参照してください。



電子証明書をセットアップできました。

続いて、オンライン資格確認等システムに接続できるかを確認します。

7 オンライン資格確認等システムに接続するに進みます

7 オンライン資格確認等システムに接続する

オンライン資格確認等システムに接続します。また、本番環境に接続するためのショートカットをデスクトップに作成します。

本番環境 <https://hweb.oqs.onshikaku.org/web/>

注意

IP-VPN接続方式（フレッツ光接続）でオンライン資格確認等システムに接続する医療機関等の方へ

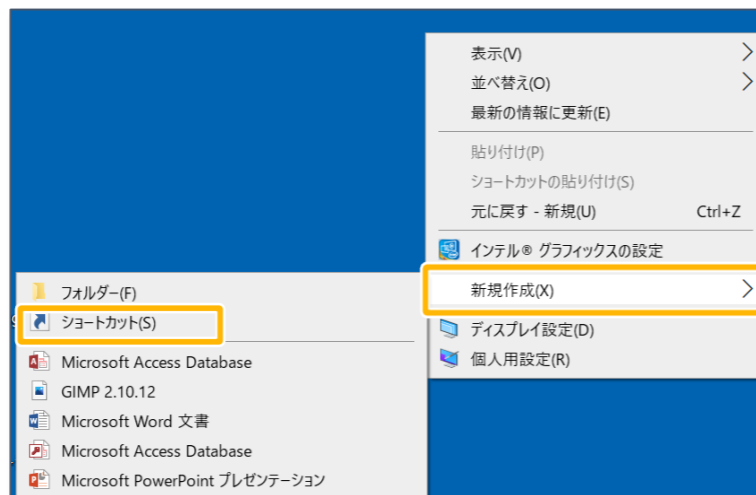
IP-VPNでオンライン資格確認等システムに接続する場合は、「回線認証接続」を行う必要があります。「回線認証接続」は以下を参照してください。

(参照先) オンライン資格確認等システム接続ガイド(IP-VPN接続方式) 3-1回線認証接続

ショートカットを作成する

オンライン資格確認システムに接続するためのショートカットを、デスクトップに作成します。

- 1 デスクトップで右クリックします。表示されるメニューから**新規作成**→**ショートカット**をクリックします。

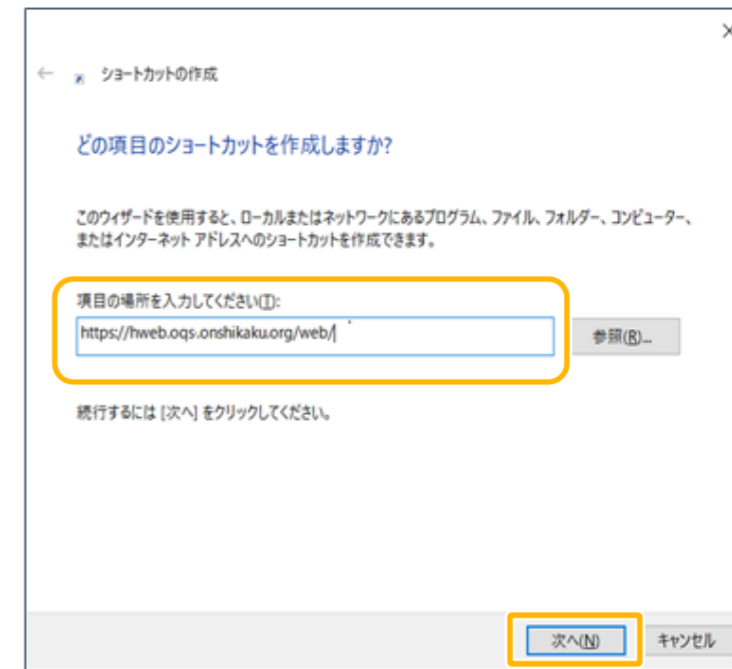


- 2 ショートカットの作成が表示されます。

項目の場所を入力してくださいに以下の内容を入力します。

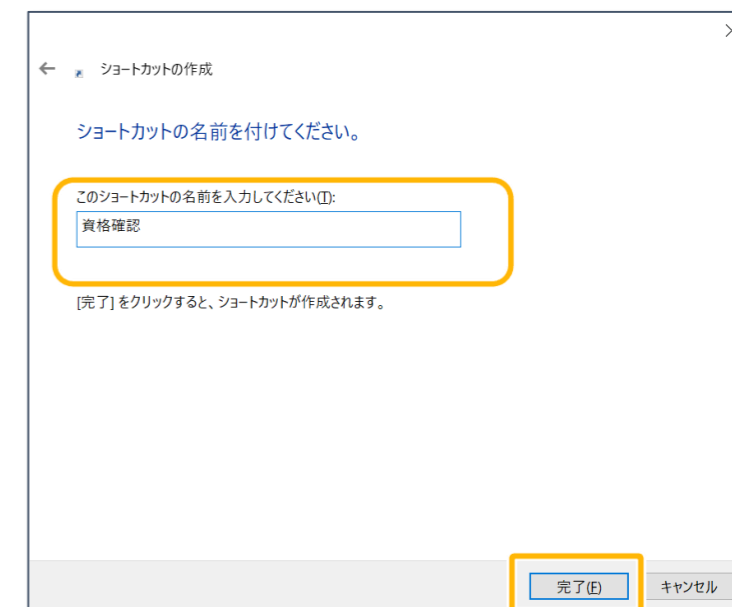
`https://hweb.oqs.onshikaku.org/web/`

入力後、**次へ**をクリックします。



- 3 **このショートカットの名前を入力してください**に、任意のショートカットの名前を入力します。
※右図では**資格確認**としています。

入力後、**完了**をクリックします。



- 4 デスクトップにショートカットが作成されました。



7 オンライン資格確認等システムに接続する（つづき）

オンライン資格確認等システムにログイン

オンライン資格確認等システムにログインできることを確認します。

- 1 作成されたショートカットをダブルクリックします。



- 2 認証用の証明書の選択が表示されます。

認証用の証明書をクリックし、OKをクリックします。



こんなときは！

認証用の証明書の選択画面が表示されない
証明書が正しくインストールされていることを確認してください。

- 3 システムの利用を始める→をクリックします。



こんなときは！

ログイン画面が表示されない／「接続検証環境」又は「医療情報閲覧用端末」と表示される

ショートカット作成時に入力したURLに誤りがないか確認してください。

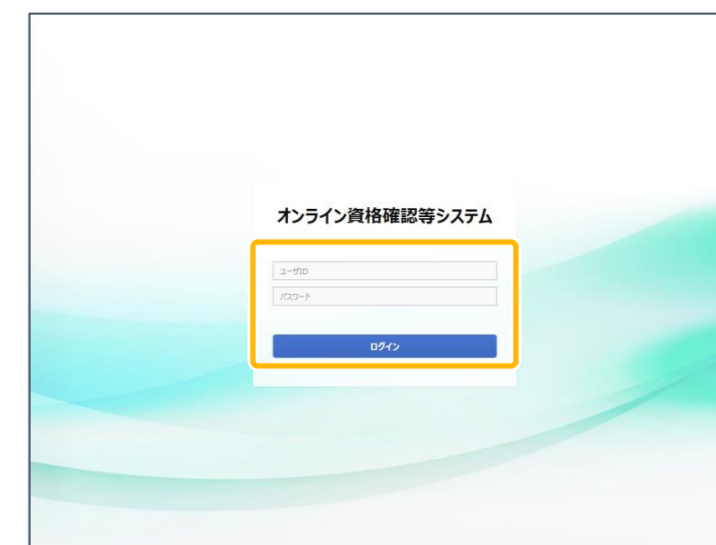
《確認方法》

ショートカットアイコンを右クリックし、表示されるメニューからプロパティを選択します。表示されるプロパティ画面のURLを確認してください。



- 4 ログイン画面が表示されます。

利用申請時に入手した**マスターアカウントのIDとパスワード**を入力し、**ログイン**をクリックします。



こんなときは！

エラーが表示される

入力したID、パスワードに間違いがないか確認してください。

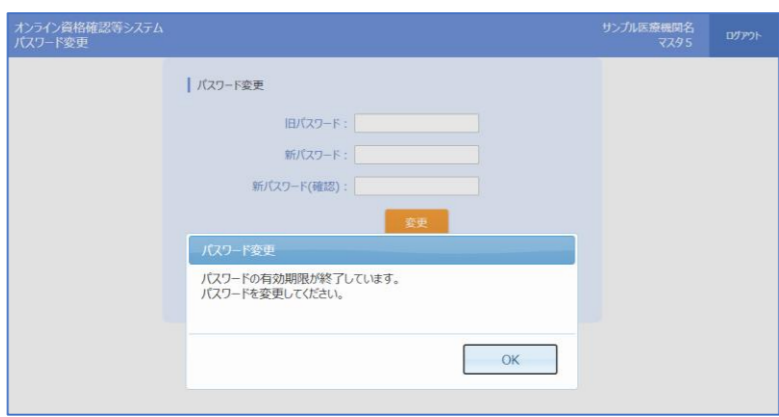


7 オンライン資格確認等システムに接続する (つづき)

注意

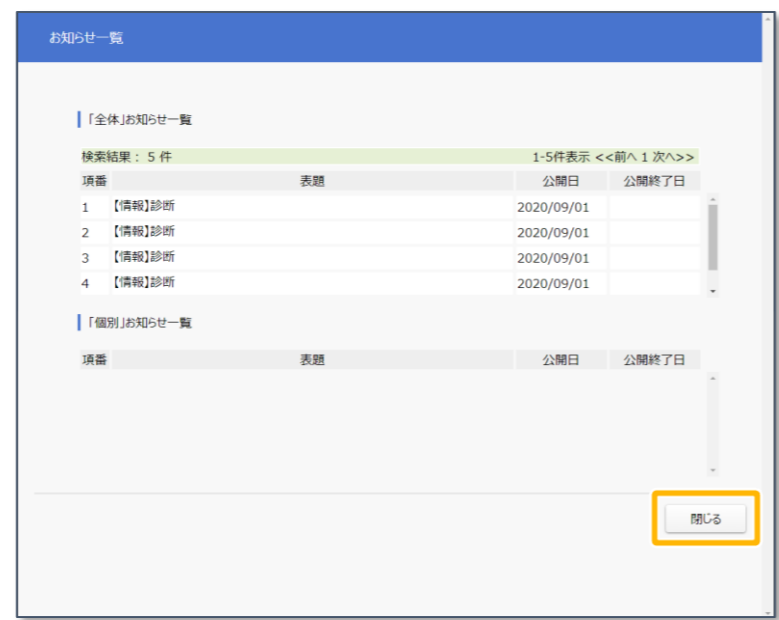
オンライン資格確認等システムに、一定期間マスタアカウントでログインしていなかった場合、以下のようなメッセージ画面が表示されますので、パスワードの変更を行ってください。

別紙 トラブルシューティング 補6



5 新しいお知らせが登録されている場合は、お知らせ一覧が表示されます。お知らせが登録されていない場合はメニューが表示されます (6 に進みます。)

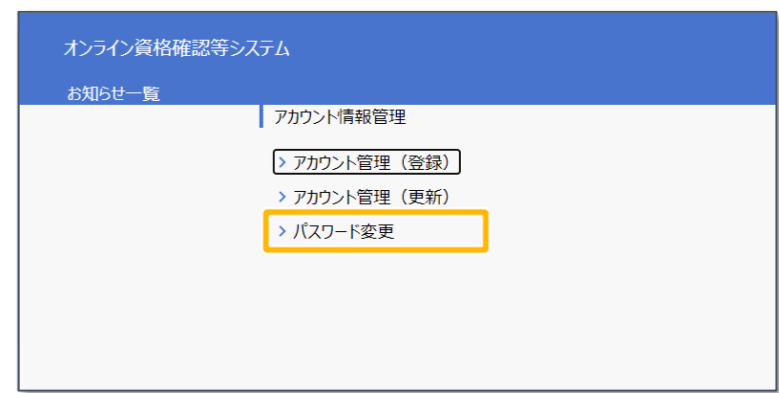
閉じるをクリックします。



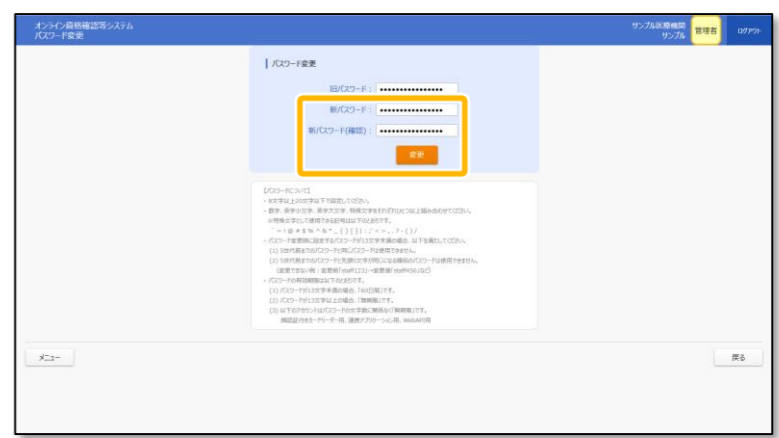
6 メニューが表示され、オンライン資格確認等システムにログインできました。



7 マスタアカウントのパスワードの変更を行う場合は、パスワード変更をクリックします。



8 パスワード変更が表示されます。新パスワード、新パスワード(確認)に新しいパスワードを入力し、変更をクリックします。



オンライン資格確認等システムへの接続が完了しました。

8 アカウントを作成する に進みます

1台の資格確認端末を複数の職員で共有する場合で、職員ごとにWindowsのログインIDを切り替えて使用するときは (マルチアカウント)、

「操作1 Windows10にユーザアカウントを追加する」～「操作7 オンライン資格確認等システムに接続する」の操作を職員数分操作して登録します。

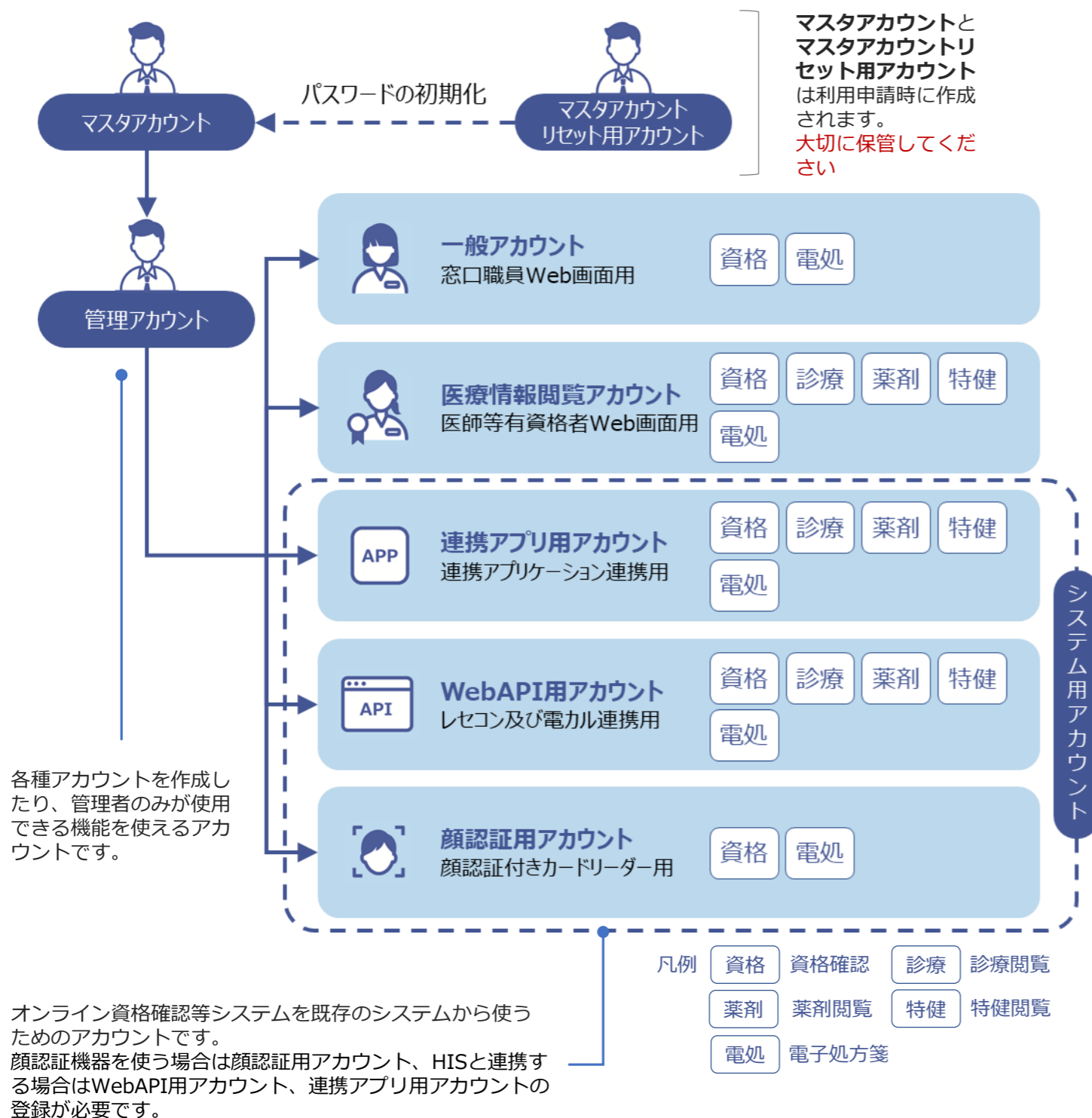
ただし、以下については、OqsComAppアカウントで実行済みのため必要ありません。

- 操作2 ブラウザ (Microsoft Edge) を設定する <ブラウザ拡張ツールを実行します>
- 操作5 連携アプリケーションをインストールする

8 アカウントを作成する

注意 新機能の本番環境利用は、下記の利用開始を予定しております。
2023年1月予定 電子処方箋管理サービスの利用

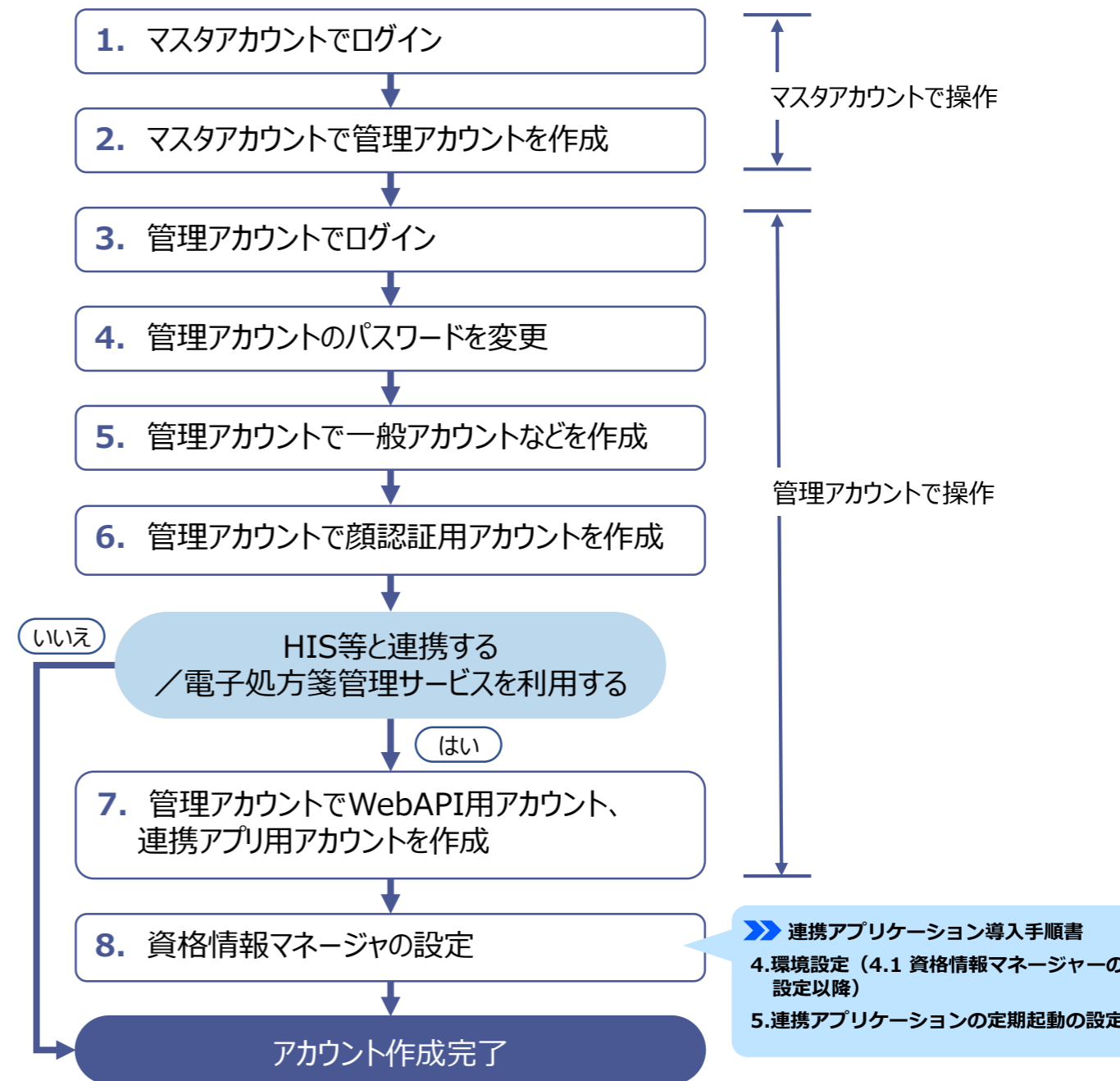
オンライン資格確認等システムを利用する利用者、顔認証機器、連携アプリケーションなどのアカウントを登録します。
一般アカウント、医療情報閲覧アカウントは個人ごとに、連携アプリ用アカウント、WebAPI用アカウントは資格確認端末ごとに、顔認証用アカウントは顔認証機器ごとにアカウントを作成します。



アカウント作成のながれ

アカウントの作成は、以下の流れで実施します。
アカウント作成操作の詳細は、操作マニュアル管理者編を参照してください。

医療機関等向け オンライン資格確認等システム操作マニュアル 管理者編 2章 アカウントを管理する



アカウントの作成が完了しました。

9 文字コード、特健情報等の閲覧同意、電子処方箋管理サービスの利用有無を設定するに進みます

9 文字コード、特健情報等の閲覧同意、電子処方箋管理サービスの利用有無を設定する

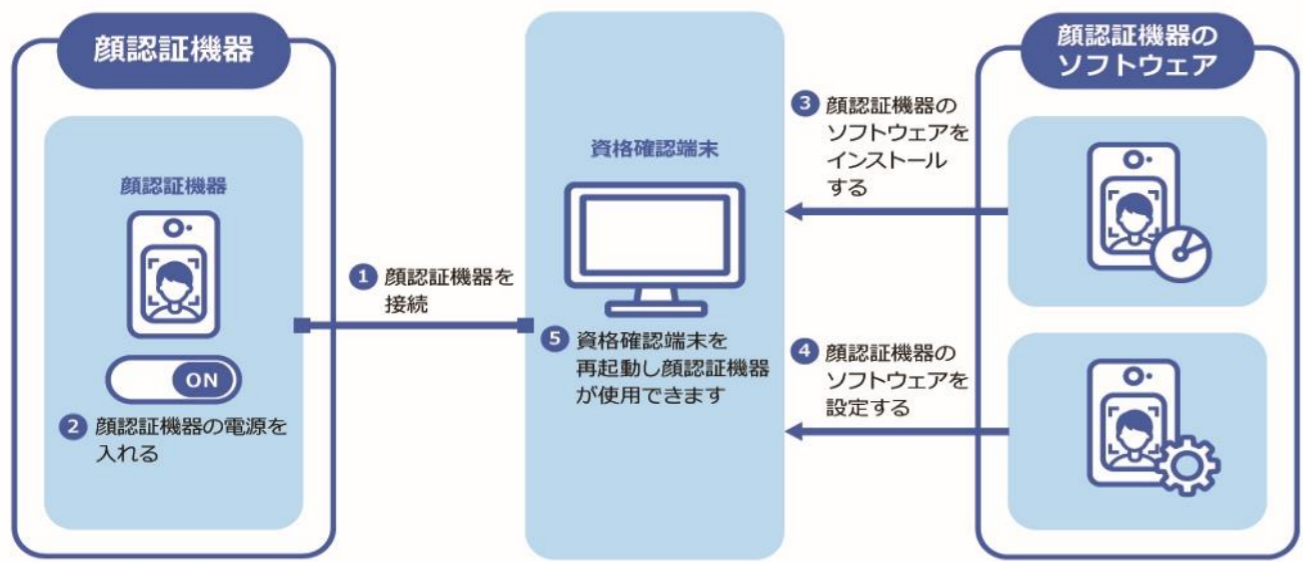
オンライン資格確認等システムの文字コードは、初期値として**UTF-8**を使用しています。文字コードを**Shift-JIS**に変更する必要がある場合は、**操作マニュアル**を参照してください。また、薬剤情報、診療情報、特定健診情報、特定疾病療養受療証、電子処方箋管理サービスの情報を利用する場合は、情報を利用するか否かの設定も合わせて行ってください。

▶▶ 医療機関等向け オンライン資格確認等システム操作マニュアル 管理者編 3章 環境情報を設定する
※文字コードの変更は管理アカウントでのみ実施可能です。

注意
診療情報、電子処方箋管理サービスについては、初期設定として「**利用しない**」が設定されています。

10 顔認証機器を設定する

顔認証機器を設定します。資格確認端末に必要なソフトウェア等をインストールし、顔認証機器を使用できるようにします。なお、設定にあたっては各社の取扱説明書、操作マニュアル等を参照してください。



▶▶ 富士通Japan社製：インストールマニュアル、スタートアップガイド
アルメックス社製：設置マニュアル
パナソニックコネクト社製：取扱説明書（準備編、本体編）
キャノンマーケティングジャパン社製：顔認証付きカードリーダーHi-CARA セットアップマニュアル
アトラス情報サービス社製：EXC-9000 取扱説明書

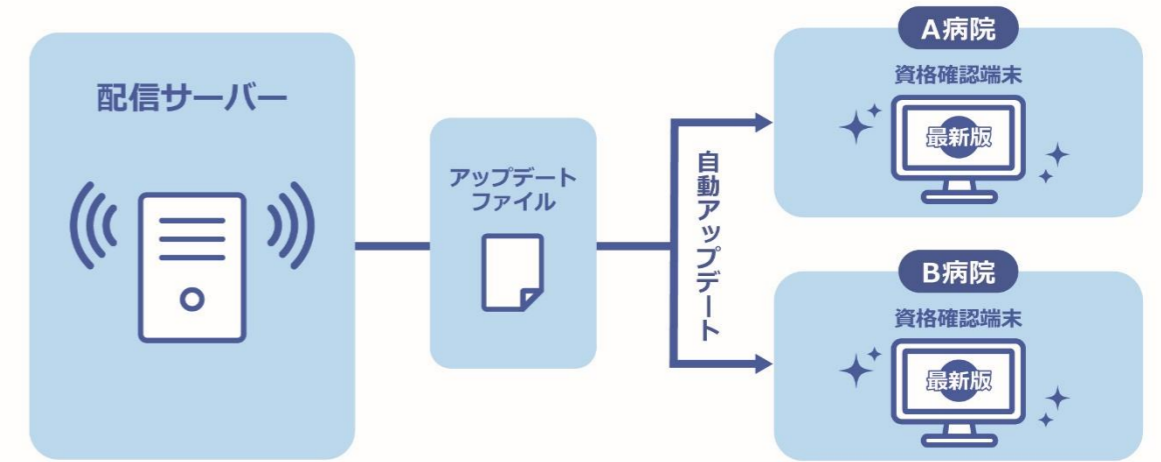
注意
顔認証機器のソフトウェアのインストールおよび実行権限は以下に従ってください。
(1) OqsComAppでログインのまま顔認証機器のソフトウェアをインストールする。
(2) 顔認証機器のソフトウェアの実行権限は変更しない。

顔認証機器の設定が完了しました。

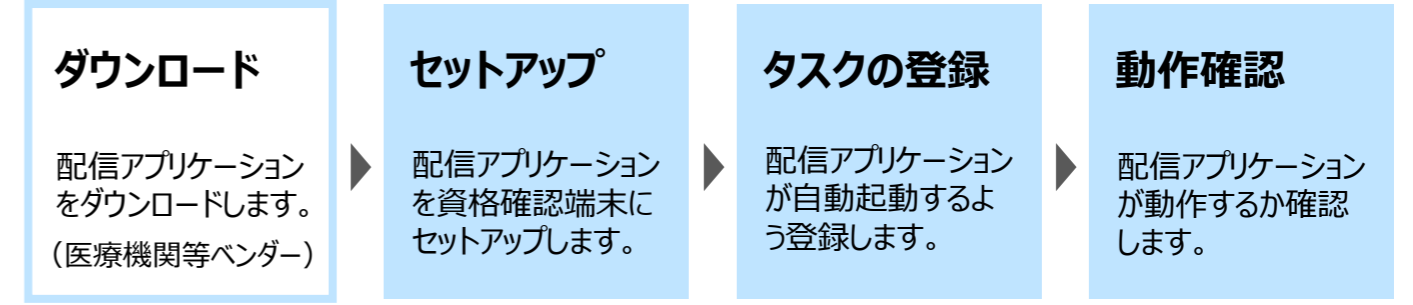
▶▶ 11 配信アプリケーションをインストールする に進みます

11 配信アプリケーションをインストールする

配信アプリケーションをインストールします。配信アプリケーションとは、各医療機関等の資格確認端末の最新化など、ソフトウェアのインストール、ファイル等を自動配付し、実行する機能です。



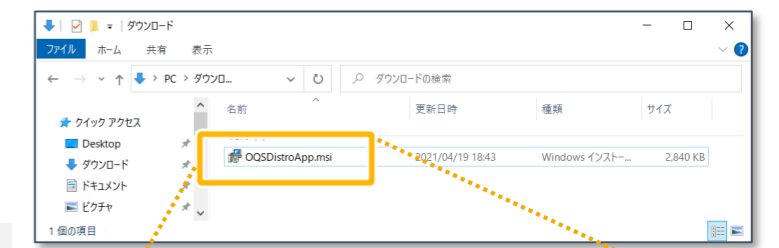
配信アプリケーションのインストールは以下の流れで実施します。本項ではセットアップ以降の手順を説明します。



01 セットアップ

医療機関等ベンダーより配信アプリケーションを入手しセットアップします。

1 配信アプリケーションの**セットアップファイル**をダブルクリックします。



こんなときは！
メッセージ画面が表示された場合
WindowsによってPCが保護されましたというメッセージ画面が表示された場合は、**実行ボタン**をクリックしてインストールを続行します。

OQSDistroApp.msi

2へ進む

11 配信アプリケーションをインストールする (つづき)

2 OqsDistroApp セットアップが表示されます。

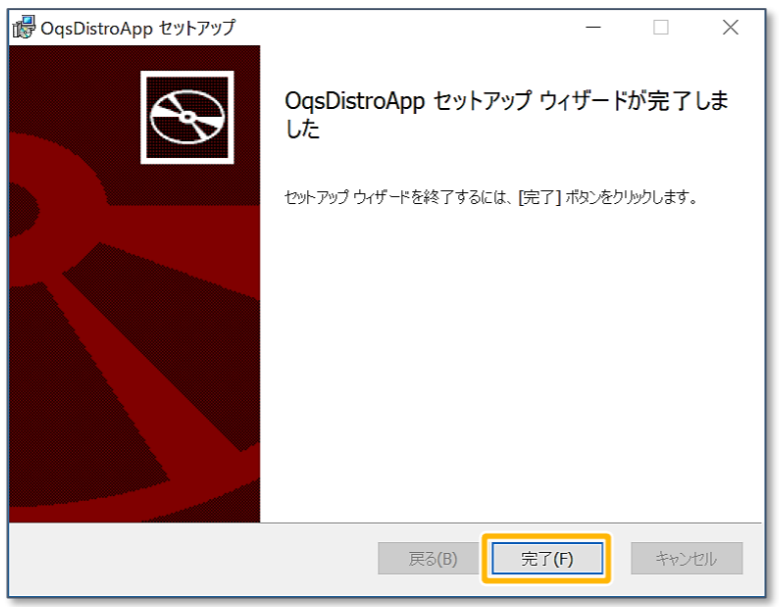
ソフトウェア使用許諾条件の内容をよく読み、同意する場合は**使用許諾契約書に同意します**をチェックして、**インストール**をクリックします。



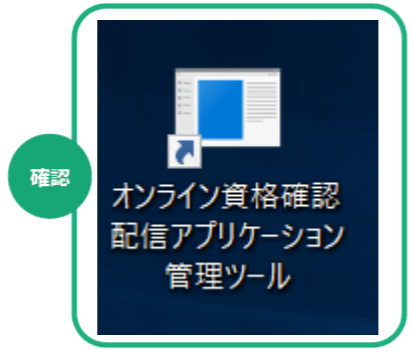
こんなときは!
メッセージ画面が表示された場合
 このアプリがデバイスに変更を加えることを許可しますか?というメッセージ画面が表示された場合は、**はい**ボタンをクリックしてインストールを続行します。

3 セットアップが完了すると、セットアップウィザード完了が表示されます。

完了をクリックします。



4 Windowsのデスクトップに**オンライン資格確認配信アプリケーション管理ツール**のショートカットが作成されたことを確認します。



ネットワーク事業者起点の構成 又は医療機関等起点の構成の場合のみ実施

下表の○が付いた**ネットワーク事業者起点の構成** 又は**医療機関等起点の構成**の場合のみ、本手順を実施してください。(配信拠点起点の構成の場合は、「02 タスクの登録」に進みます。)

使用する回線に応じて、構成は以下のとおり分類されます。

■ IPsec+IKEサービス提供事業者 (インターネット接続方式)

事業者名	構成
株式会社NTTPC コミュニケーションズ	配信拠点起点
株式会社NTTデータ中国	ネットワーク事業者起点 ○
三菱電機 インフォメーション ネットワーク 株式会社	ネットワーク事業者起点 ○
富士通株式会社	配信拠点起点

■ IP-VPN接続方式 (光回線)

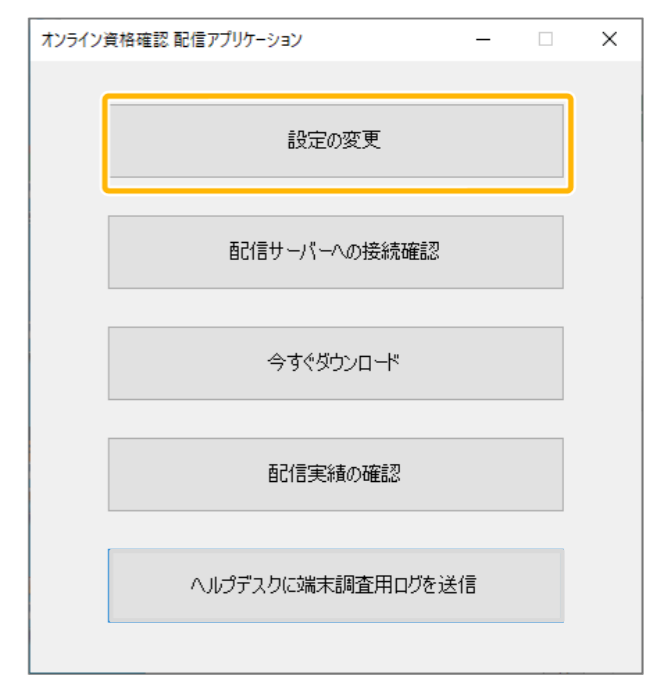
事業者名	構成
NTT東日本・西日本	配信拠点起点
中部テレコミュニケーション 株式会社 (CTC)	配信拠点起点
株式会社QTnet	配信拠点起点

■ その他

医療機関・薬局等の**プロキシサーバー**等を使用し、**インターネットを経由して、配信クラウド、マイクロソフトに直接アクセス** (構成: **医療機関等起点**) ○

1 ショートカットから**オンライン資格確認配信アプリケーション管理ツール**を起動し、**オンライン資格確認配信アプリケーション管理ツール**を表示します。

設定の変更をクリックします。



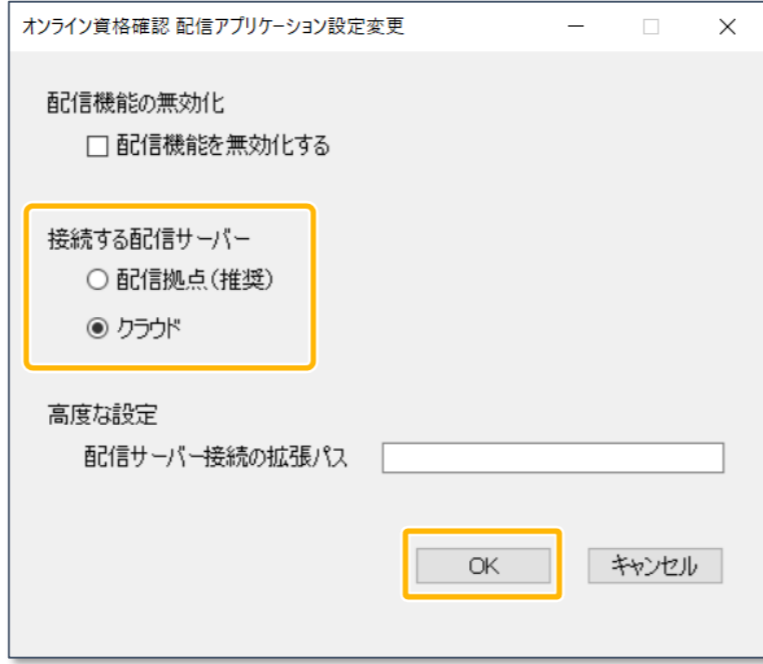
2 へ進む

11 配信アプリケーションをインストールする (つづき)

2 オンライン資格確認配信アプリケーション設定変更が表示されます。

接続する配信サーバーでクラウドを選択し、OKをクリックします。

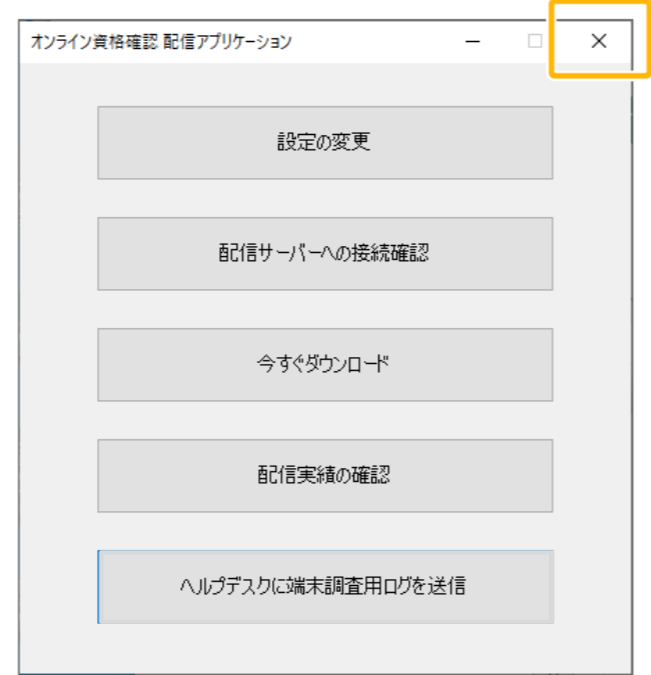
注意
高度な設定にある、配信サーバー接続の拡張パスは、別途案内がない限り設定しないでください。



注意
以下の医療機関等の方々には配信アプリケーションによる自動更新を停止してください。
 ・レセプトコンピュータと資格確認端末を兼用する医療機関等の方
 ・資格確認端末のOSがWindows10 Proの医療機関等の方
 ・最新資産のクライアントアプリケーションを手動で適用している方
 >>> 別紙 トラブルシューティング 補2

3 オンライン資格確認配信アプリケーション管理ツールが表示されます。

管理ツール右上の × (閉じる) をクリックし、管理ツールを終了します。



配信アプリケーションのセットアップができました。

02 タスクの登録

Windows起動時、配信アプリケーションが自動起動するようにタスクを登録します。

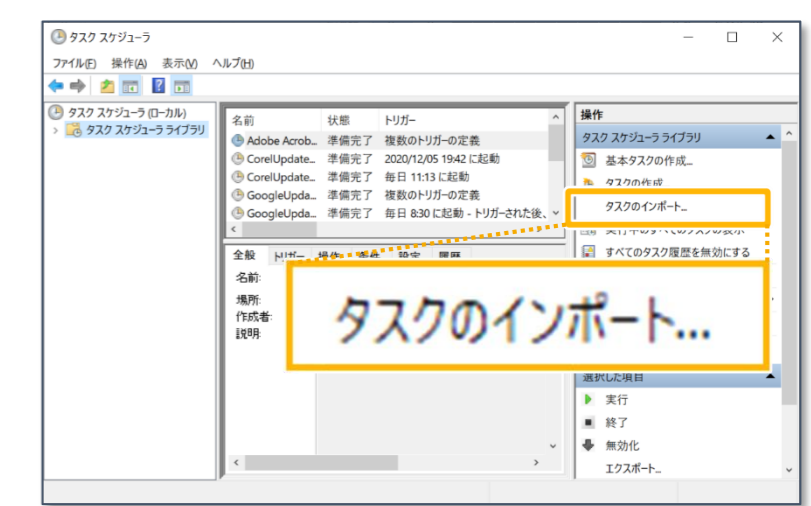
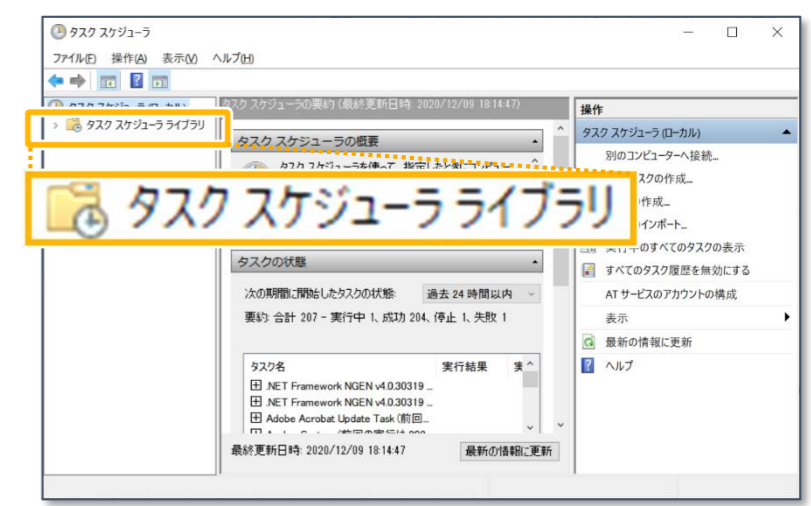
1 検索をクリックし、検索ボックスにタスク スケジューラと入力します。

2 検索結果から、タスク スケジューラをクリックします。

3 タスク スケジューラが表示されます。

左側の領域から、タスク スケジューラ ライブラリをクリックします。

4 操作から、タスクのインポートをクリックします。

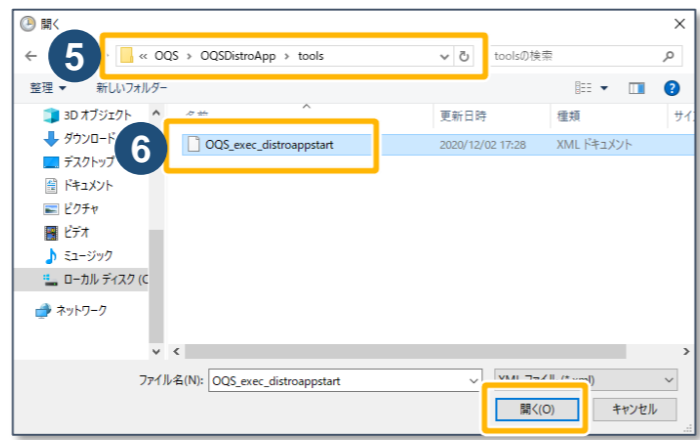


5 へ進む

11 配信アプリケーションをインストールする (つづき)

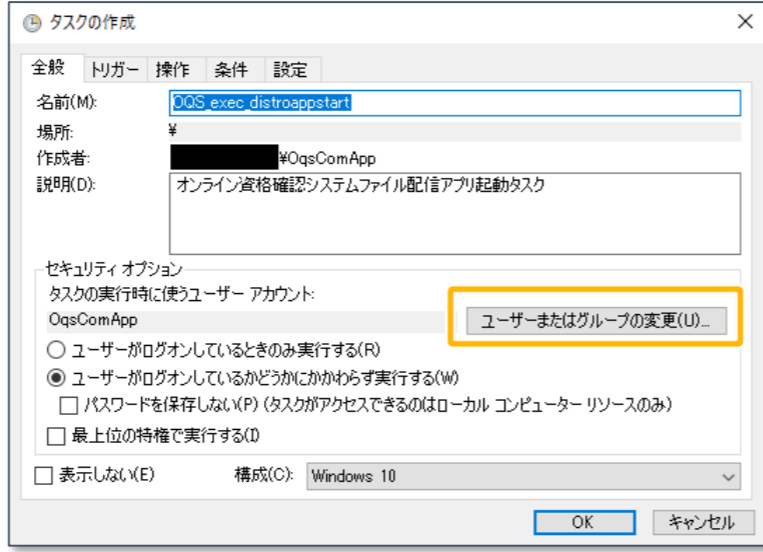
5 開くが表示されます。
ファイルの場所から、以下のフォルダに切り替えます。

C:¥Program Files¥OQS
¥OQSDistroApp¥tools

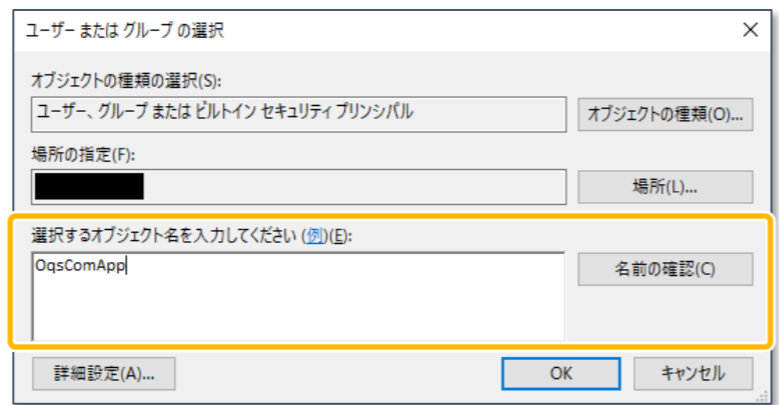


6 フォルダにある OQS_exec_distroappstart.xml をクリックし、開く をクリックします。

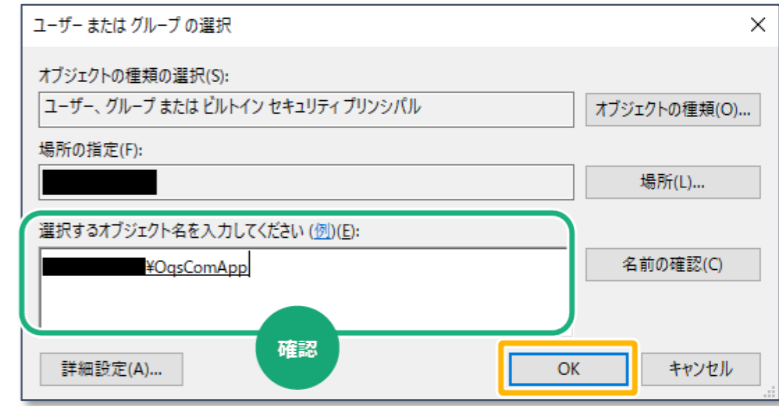
7 タスクの作成が表示されます。
ユーザーまたはグループの変更(U)... をクリックします。



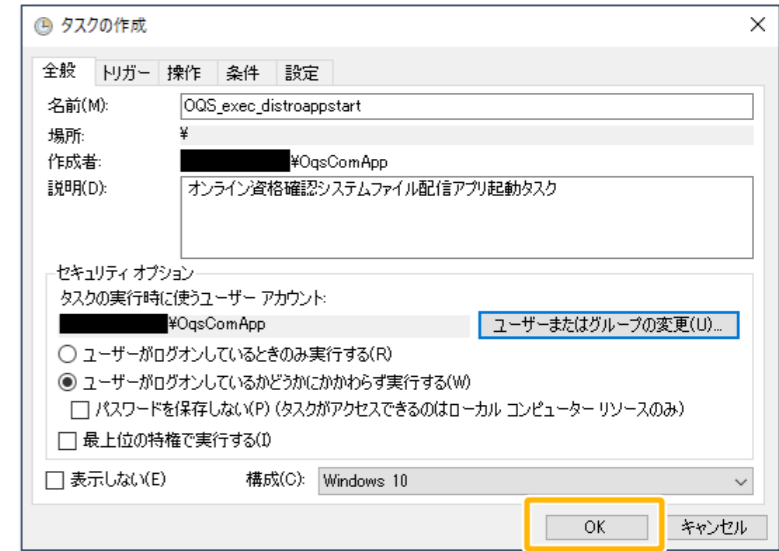
8 ユーザーまたはグループの選択が表示されます。
選択するオブジェクト名を入力してくださいに OqsComApp と入力し、名前の確認 をクリックします。



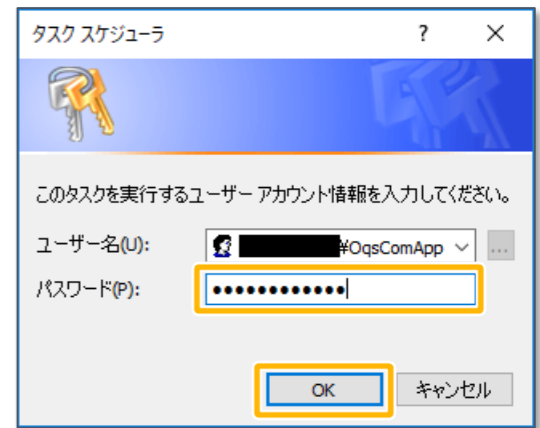
9 OqsComApp に下線が表示されたことを確認します。
OK をクリックします。



10 タスクの作成が表示されます。
OK をクリックします。



11 パスワード入力画面が表示されます。
OqsComApp のパスワードを入力し、OK をクリックします。



12 設定を有効にするため、Windows を再起動します。

配信アプリケーションのタスクが登録されました。

11 配信アプリケーションをインストールする (つづき)

03 動作確認

配信アプリケーションが正しく動作するか確認します。

注意

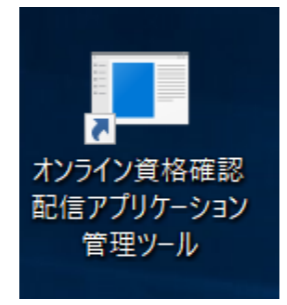
ネットワーク事業者起点の構成 又は医療機関等起点の構成を利用している医療機関等の方へ

配信アプリケーションのバージョンが1.0.4より前のバージョンをインストールしている場合、配信アプリケーションの再インストールが必要です。操作11 配信アプリケーションをインストールするを参照して、最新の配信アプリケーションをインストールしてください。

注意

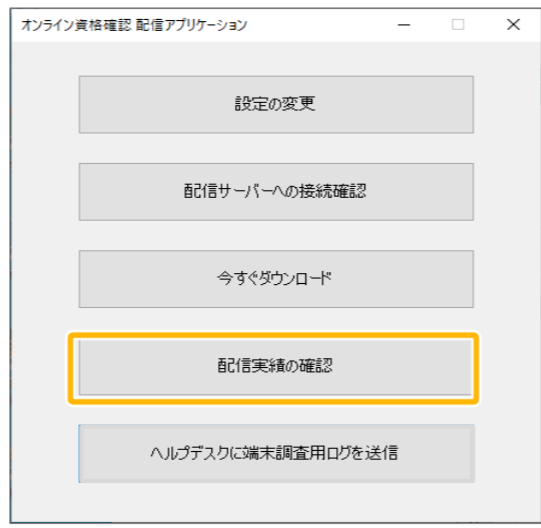
配信サーバーに接続の信号を送り、サーバー接続に成功すると「接続成功」と表示されます。
 ※ 表示まで時間がかかる場合があります。
 1分待つて「接続成功」と表示されない場合や、「接続失敗」と表示された場合は、時間をおいて再度確認（本手順を実施）してください。解消しない場合は通信回線の設定が正しくされていることを確認してください。

1 スタートメニュー又はショートカットから**オンライン資格確認配信アプリケーション管理ツール**を起動します。

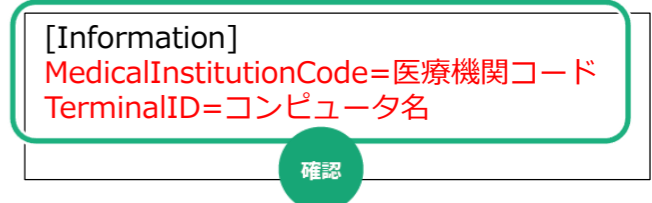


2 オンライン資格確認配信アプリケーション管理ツールが表示されます。

配信実績の確認をクリックします。



3 メモ帳が起動します。
医療機関コード、コンピュータ名が出力されていることをご確認します。

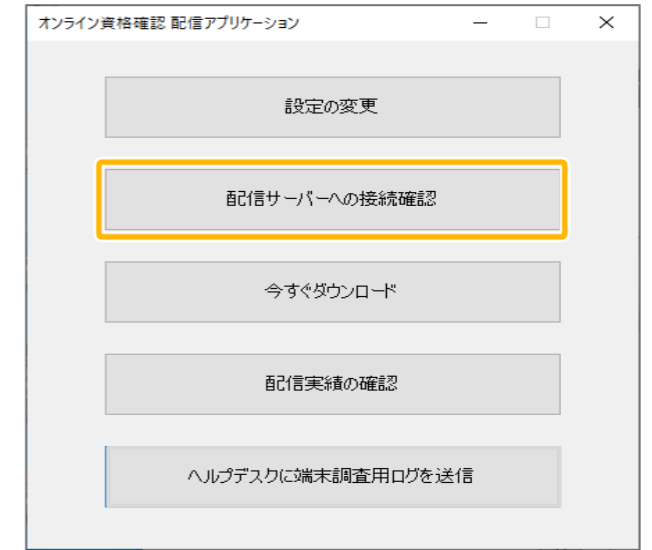


こんなときは！

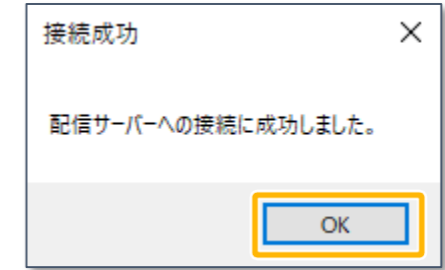
出力されていない場合の確認観点について

- 操作3 <スリープ設定と高速スタートアップを無効にします>の⑧高速スタートアップを無効化が正しく行われていることを確認してください。
- 操作6 認証局の電子証明書をインストールするが正しく行われていることを確認してください。
- 操作11 「02 タスクの登録」が正しく行われているかを確認してください。

4 オンライン資格確認配信アプリケーション管理ツールの**配信サーバーへの接続確認**をクリックします。



5 接続成功が表示されます。
OKをクリックします。



オンライン資格確認配信アプリケーション管理ツールが表示されたら、右上の **×**（閉じる）をクリックし、管理ツールを終了します。

こんなときは！

配信アプリケーションの接続が失敗した場合について

資料「配信アプリケーションの確認について」をご参照ください。

11 配信アプリケーションをインストールする（つづき）

💡 こんなときは！

セットアップ時に使用した各種インストーラーについて

医療機関等ベンダーより入手し、資格確認端末のデスクトップ等にコピーした各種インストーラー（拡張プラグイン、連携アプリケーション、配信アプリケーションをインストールするためのファイル）は、セットアップ後、不要となるため、削除しても構いません。

配信アプリケーションのインストールが完了しました。

➡ 12 資格確認できるか確認をする に進みます

12 資格情報できるか確認する

資格確認端末に接続した顔認証機器、連携アプリケーションの連携について動作確認をします。本書ではブラウザからの資格確認手順のみを説明しています。

① 顔認証機器
で資格確認

顔認証して資格確認できるか確認します。

② 汎用カードリーダー
で資格確認

汎用カードリーダーで資格確認できるか確認します。

③ 被保険者証、処方箋、ブラウザで
資格確認

被保険者証又は処方箋の情報を入力し、資格確認できるか確認します。

④ 既存システムで
資格確認

既存システムから資格確認できるか確認します。
被保険者証、処方箋 + 連携アプリケーションを使用します。

医療機関等で導入する環境に併せて実施してください

12 資格確認できるか確認する (つづき)

オンライン資格確認システムの本番環境に接続し、資格確認ができることを確認します。
※実在する資格が表示されますので、ご注意ください。

01 資格確認 (マイナンバーカード + 顔認証機器)

用意するもの

マイナンバーカード、顔認証機器、資格確認端末

マイナンバーカードと顔認証機器を使って資格確認を行います

マイナンバーカードと、顔認証機器を資格確認端末に接続し、資格確認ができることを確認します。

※顔認証機器のセットアップは、付属のマニュアル等をご確認ください。

顔認証機器の運転モードを確認する

オンライン資格確認端末で運転モードが**無人運転**になっていることを確認します。

- 1 オンライン資格確認等システムにアクセスします。



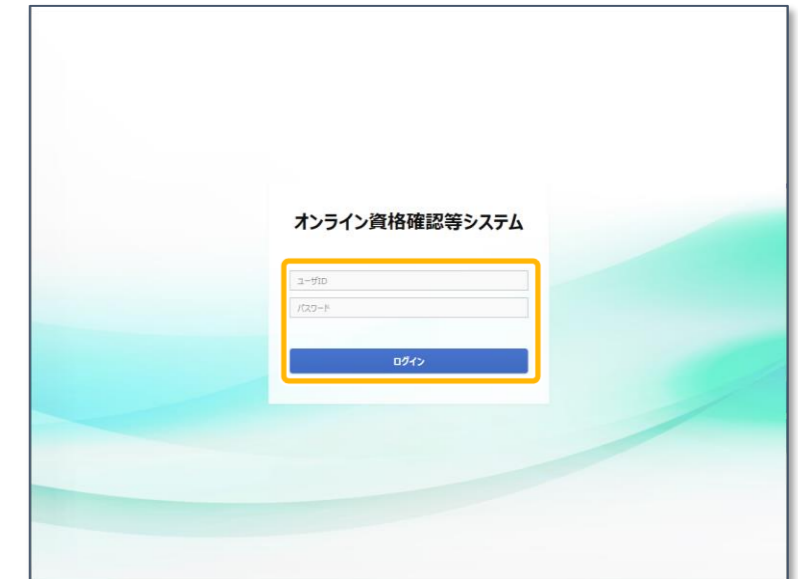
- 2 システムの利用を始める→をクリックします。



- 3 ログイン画面が表示されます。

以下のいずれかの**ユーザID**と**パスワード**を入力し、**ログイン**をクリックします。

- 一般利用者
- 管理者



- 4 メニューが表示されます。

顔認証付きカードリーダー操作をクリックします。



- 5 顔認証付きカードリーダー操作が表示されます。

無人運転が緑色のボタンになっていることを確認します。



💡 こんなときは！

無人運転になっていない場合

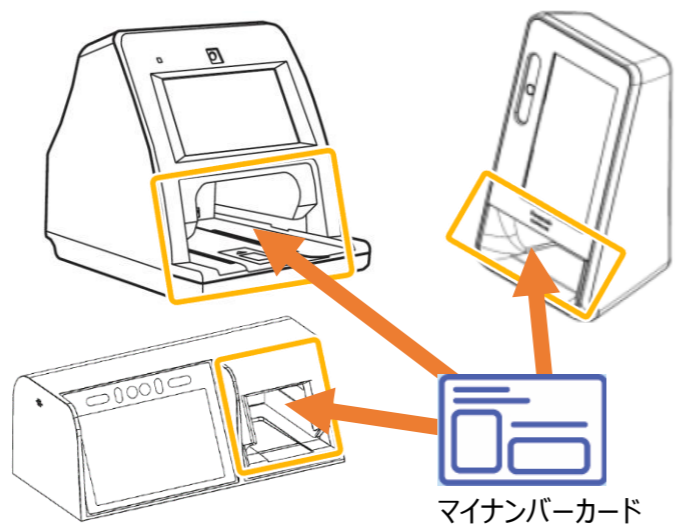
無人運転のボタンが緑色になっていない場合は、ボタンをクリックして、無人運転に切り替えます。

12 資格確認できるか確認する (つづき)

顔認証機器で資格確認をする

オンライン資格確認端末に接続されている顔認証機器で資格確認ができることを確認します。

- 1 顔認証機器に、マイナンバーカードを置きます。
- 2 顔認証機器に表示されるメニューをタップして、顔認証を実施し、**確認が完了しました**のメッセージが表示されることを確認します。



💡 こんなときは!
資格情報が文字化けした場合
 資格情報の表示内容が?など正しく表示されない場合、資格確認端末の言語設定が日本語以外になっている可能性があります。別紙 補7 言語設定を日本語に、地域設定を日本にしたいを参照して設定を確認してください。

➡ 別紙 トラブルシューティング 補7

既存システム端末でオンライン資格確認等システムのセットアップを行った場合、資格情報が既存システムへ取り込まれていることを確認してください。既存システム上での操作は、それぞれのシステムにより異なります。既存システムのマニュアルを参照ください。

顔認証機器で資格確認が完了しました。

02 資格確認 (マイナンバーカード+汎用カードリーダー)

用意するもの
 マイナンバーカード、汎用カードリーダー、資格確認端末

マイナンバーカードと汎用カードリーダーを使って資格確認を行います

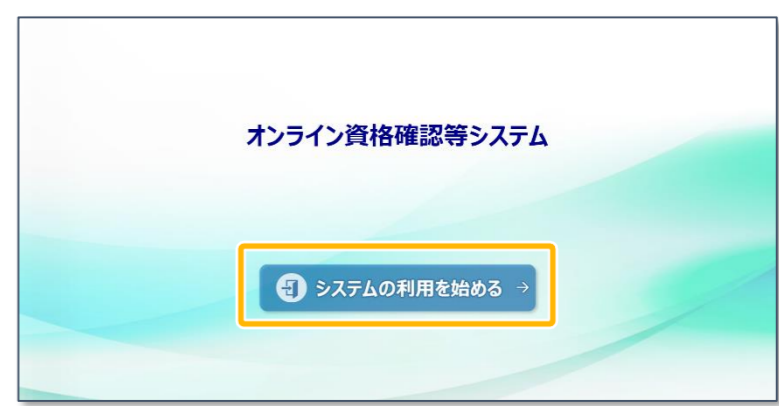
マイナンバーカードと汎用カードリーダーを資格確認端末に接続し、資格確認ができることを確認します。作業は、以下の2つを実施してください。

- (1) マイナンバーカードと汎用カードリーダーで資格確認
 - (2) マイナンバーカードと汎用カードリーダーで暗証番号を入力し資格確認
- ※汎用カードリーダーのセットアップは、汎用カードリーダーに付属のマニュアル等をご確認ください。

- 1 オンライン資格確認等システムにアクセスします。



- 2 システムの利用を始める→をクリックします。



- 3 ログイン画面が表示されます。

以下のいずれかの**ユーザID**と**パスワード**を入力し、**ログイン**をクリックします。

- 一般利用者
- 管理者



4 へ進む

12 資格確認できるか確認する (つづき)

4 メニューが表示されます。

マイナンバーカードで確認
をクリックします。

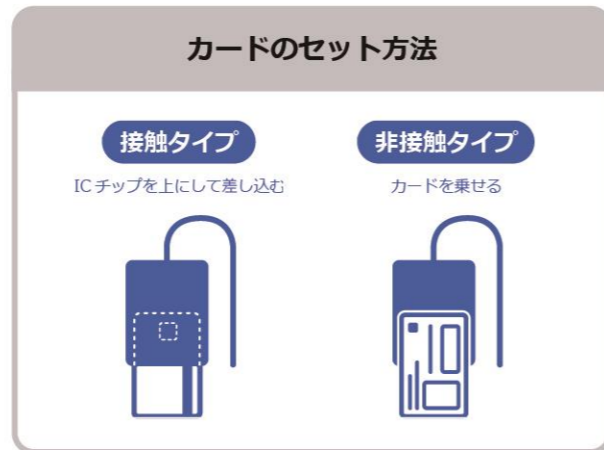


5 資格情報照会 (マイナンバーカード) が表示されます。

本人確認のマイナンバーカードの券面で目視確認をクリックして選択し、目視で本人確認完了にチェックを付けます。



6 資格確認端末に接続された汎用カードリーダーに、マイナンバーカードを差し込むか、かざします。



7 資格情報確認が表示され、資格情報の内容が表示されます。

戻るをクリックします。



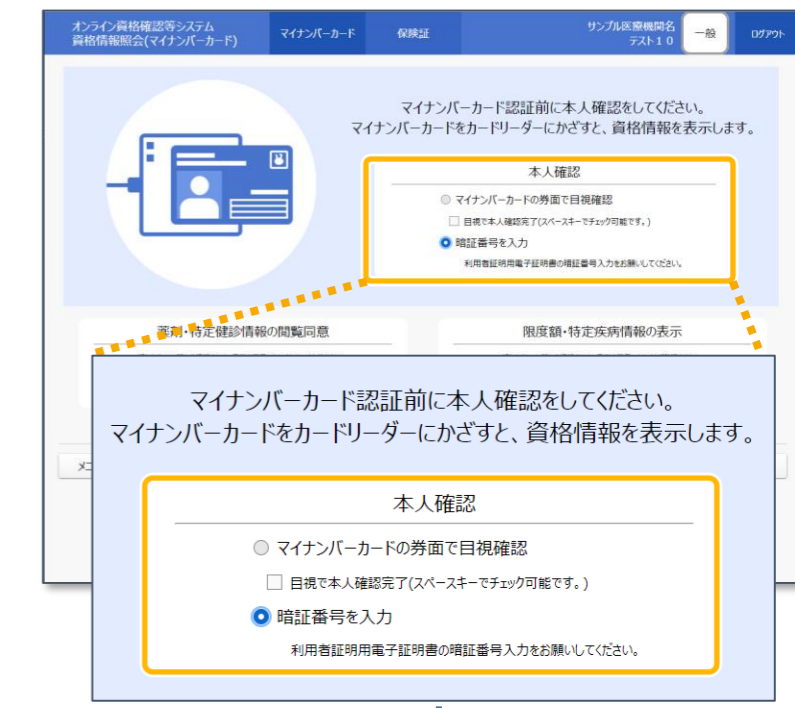
8 資格情報照会 (マイナンバーカード) が表示されます。



マイナンバーカードの暗証番号を入力し、資格確認できるか確認します

1 資格情報照会 (マイナンバーカード) を表示します。

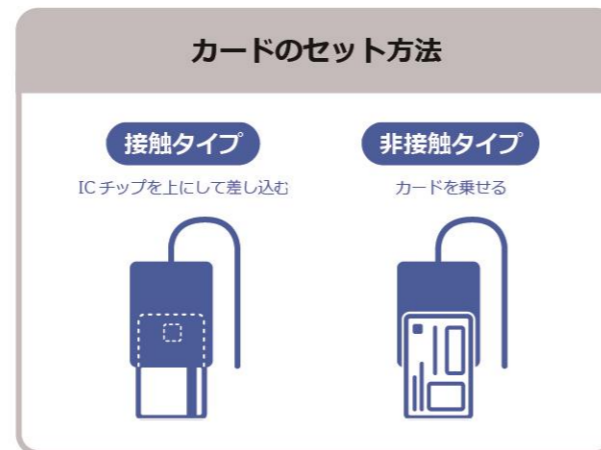
本人確認の暗証番号を入力をクリックします。



2 へ進む

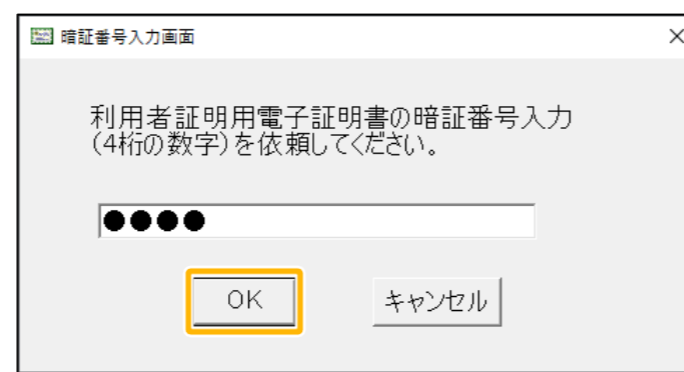
12 資格確認できるか確認する (つづき)

- 汎用カードリーダーに、マイナンバーカードを差し込むか、かざします。



- 暗証番号入力画面が表示されます。

利用者証明用電子証明書の暗証番号（4桁の数字）を入力し、**OK**をクリックします。



- 資格情報確認が表示され、**資格情報の内容が表示**されます。



マイナンバーカードと汎用カードリーダーで資格確認ができました。

03 資格確認（保険者証、処方箋、ブラウザ）

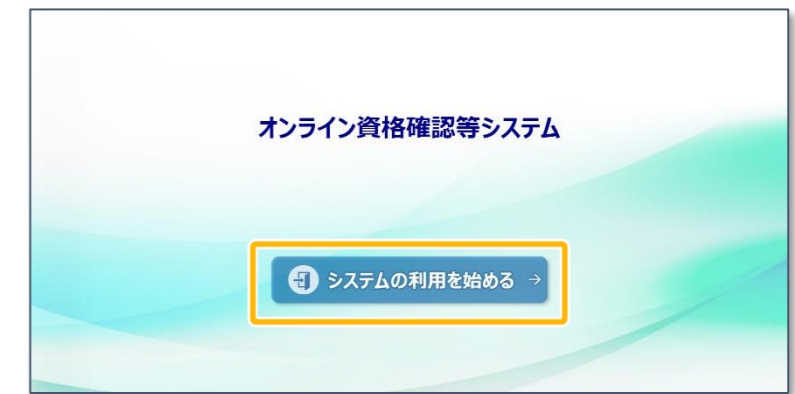
用意するもの
被保険者証又は処方箋、資格確認端末

被保険者証又は処方箋の健康保険証情報を入力し、資格確認ができることを確認します。資格確認可能な被保険者証情報を入力して確認してください。

- オンライン資格確認等システムにアクセスします。



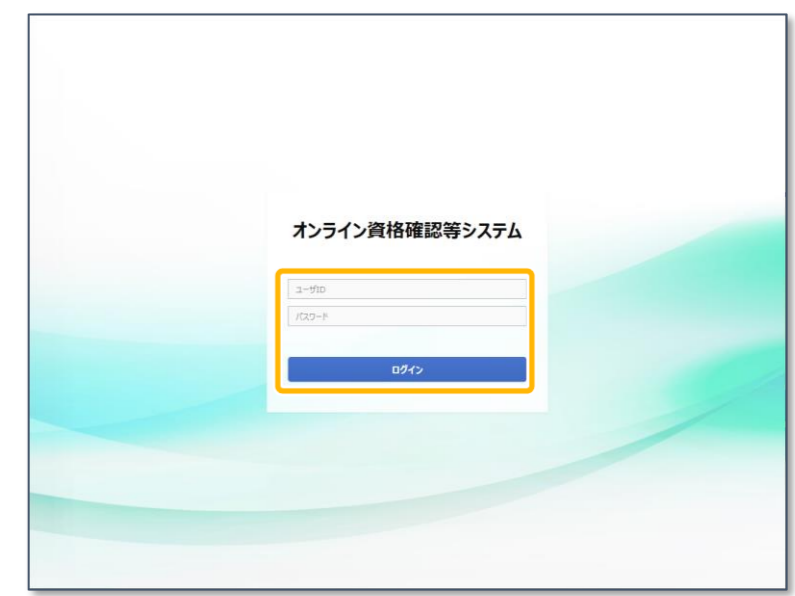
- システムの利用を始める→をクリックします。



- ログイン画面が表示されます。

以下のいずれかの**ユーザID**と**パスワード**を入力し、**ログイン**をクリックします。

- 一般利用者
- 管理者



↓
4 へ進む

12 資格確認できるか確認する (つづき)

4 メニューが表示されます。
保険証/処方箋で確認をクリックします。



5 検索条件が表示されます。
資格情報の内容(※)を入力します。入力後、**検索**をクリックします。



6 資格情報確認が表示され、**資格情報の内容**が表示されます。

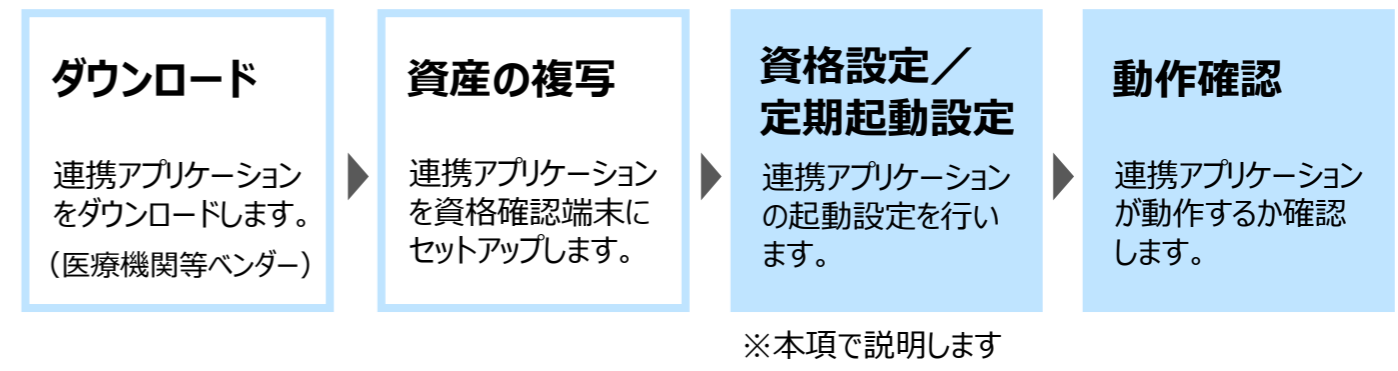


こんなときは!
資格情報が表示されない
 資格情報が表示されない場合、検索条件を正しく指定していない可能性があります。検索条件画面に戻って、再度検索してください。

04 資格確認 (既存システムから)

連携アプリケーションから被保険者証で資格確認を行う場合

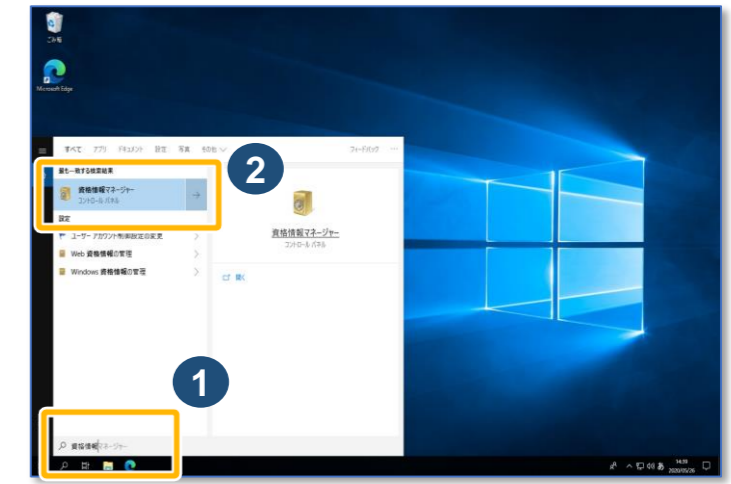
連携アプリケーションから被保険者証で資格確認を行う場合、セットアップの続きを行ってください。詳細な設定については、**連携アプリケーション導入手順書**を参照してください。



※本項で説明します

資格情報マネージャーの設定を行います

1 検索をクリックし、検索ボックスに**資格情報マネージャー**と入力します。



2 検索結果が表示されます。
資格情報マネージャーをクリックします。

3 資格情報マネージャーが表示されます。



Windows 資格情報をクリックします。

4 へ進む

被保険者証又は処方箋で資格確認ができました。

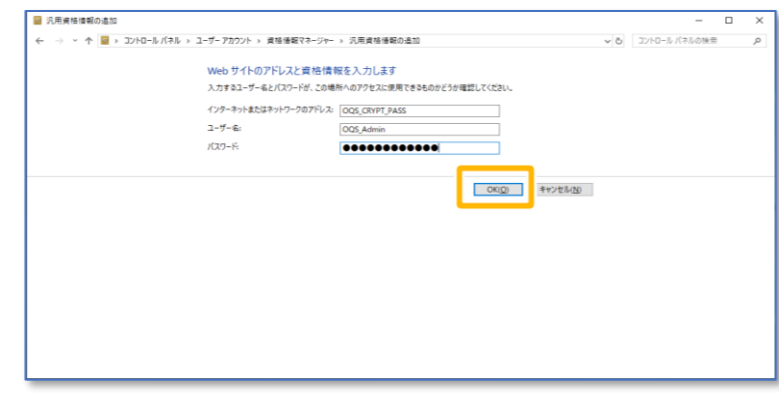
12 資格確認できるか確認する (つづき)

4 汎用資格情報の追加 をクリックします。



5 資格情報を入力します。

入力後、OK をクリックします。



以下の表に示す4つの「設定内容」の、「インターネットまたはネットワークのアドレス」、「ユーザ名」、「パスワード」を入力し、OKをクリックして各設定内容を登録してください。

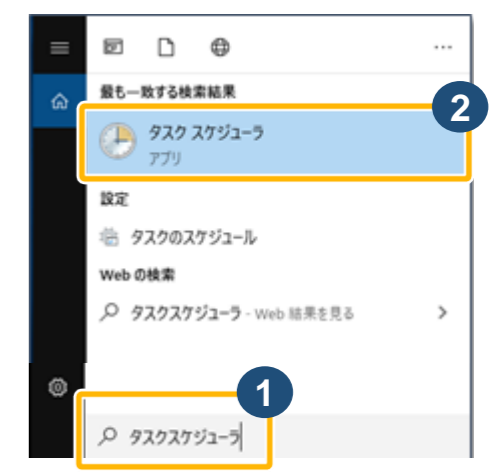
設定内容	インターネットまたはネットワークのアドレス	ユーザー名	パスワード	必須
連携アプリ用アカウントのID、パスワード	OQS_LOGIN_KEY	連携アプリ用アカウントのID(R0またはR1から始まるアカウントID)を設定する	連携アプリ用アカウントのパスワードを設定する	○
医療機関コード	OQS_MEDICAL_INSTITUTION_CODE	OQS_Admin	数字10桁の医療機関コード	○
要求データファイルの復号、結果データファイルの暗号化パスワード	OQS_CRYPT_PASS	OQS_Admin	・半角英数字 ・12桁以内 ※記号など半角英数字以外の文字を含めると連携アプリケーションによる資格確認の際にエラーとなります	×
共用フォルダのパスワード管理	OQS_NAS_LOGIN_KEY	3.2で設定した共用フォルダにアクセスするユーザー名を入力する	3.2で設定した共用フォルダにアクセスするユーザーのパスワードを入力する	×

連携アプリケーションの定期起動の設定

連携アプリケーションを定期起動するように下記タスクを登録します。

- ・ 消し忘れファイル機能定期実行用タスク (OQS_exec_comappdelfile_periodic)
- ・ 消し忘れファイル機能PC起動時実行用タスク (OQS_exec_comappdelfile_running)
- ・ 連携アプリ定期実行用タスク (OQS_exec_comappstart)

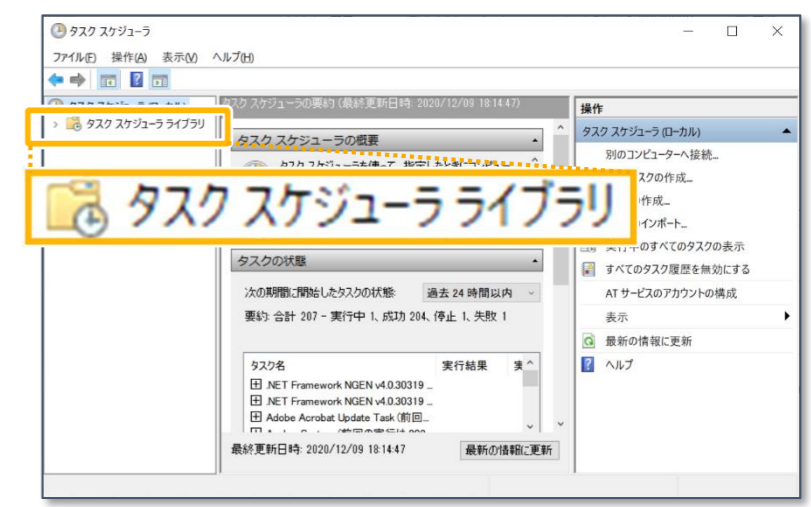
1 検索をクリックし、検索ボックスにタスク スケジューラ と入力します。



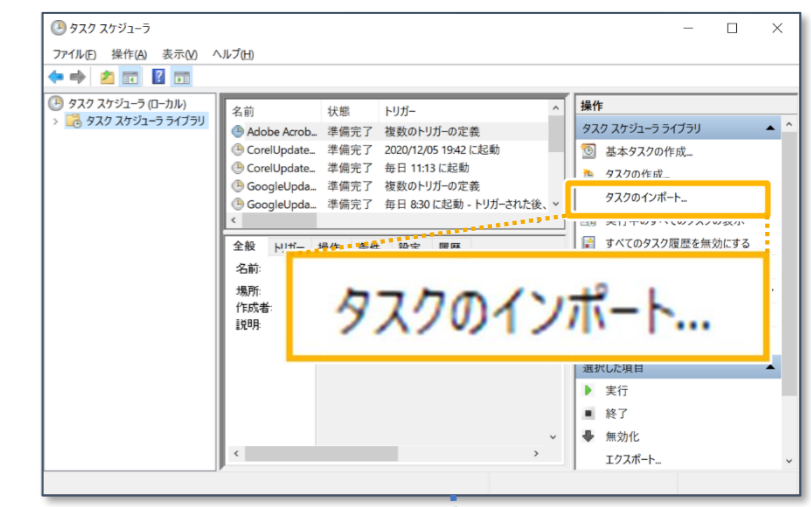
2 検索結果から、タスク スケジューラ をクリックします。

3 タスク スケジューラ が表示されます。

左側の領域から、タスク スケジューラ ライブラリ をクリックします。



4 操作から、タスクのインポート をクリックします。



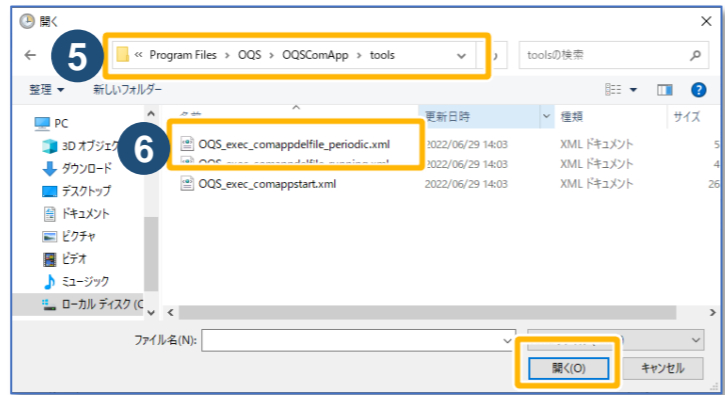
5 へ進む

12 資格確認できるか確認する (つづき)

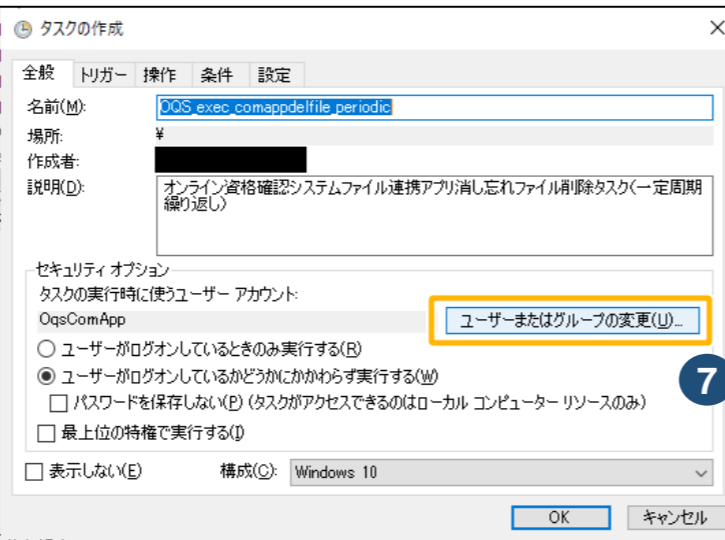
5 開く が表示されます。

ファイルの場所から、以下のフォルダに切り替えます。

C:¥Program Files¥OQS ¥OQSComApp¥tools

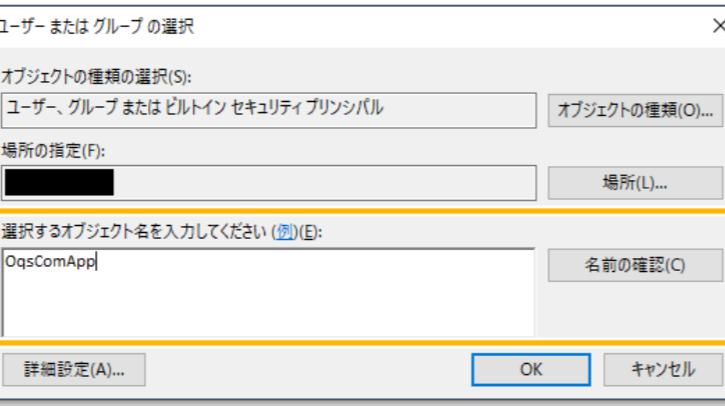


6 フォルダにある OQS_exec_comappdelfile_periodic.xml をクリックし、開く をクリックします。



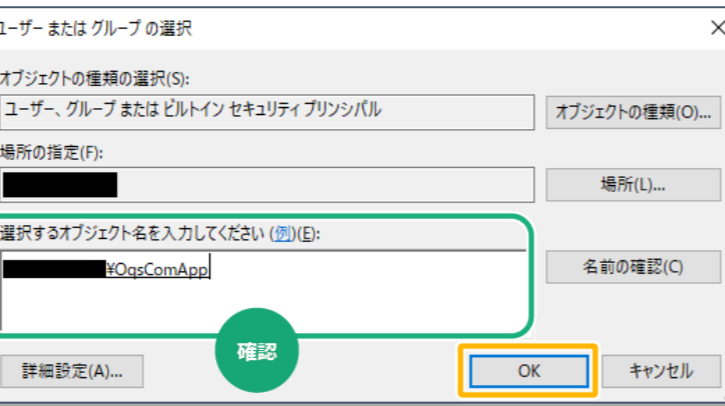
7 タスクの作成が表示されます。

ユーザーまたはグループの変更 をクリックします。



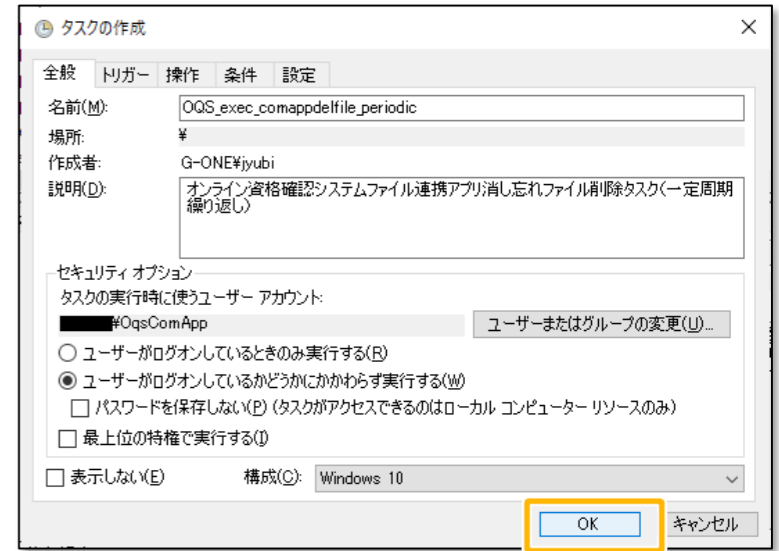
8 ユーザーまたはグループの選択が表示されます。

選択するオブジェクト名を入力してくださいに OqsComApp と入力し、名前の確認 をクリックします。



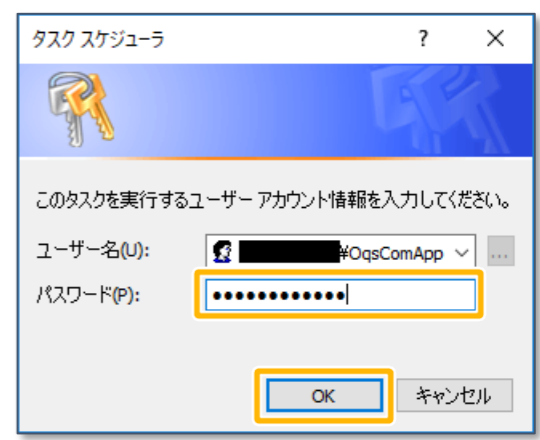
9 OqsComApp に下線が表示されたことを確認します。 OK をクリックします。

10 タスクの作成が表示されます。 OK をクリックします。



11 パスワード入力画面が表示されます。

OqsComApp のパスワードを入力し、OK をクリックします。



12 同様に、他の2つのタスクについても、登録します。

既存システム端末でオンライン資格確認等システムのセットアップを行った場合、既存システムからの資格確認ができることを確認します。既存システム上での操作は、それぞれのシステムにより異なります。既存システムのマニュアルを参照ください。

💡 こんなときは！

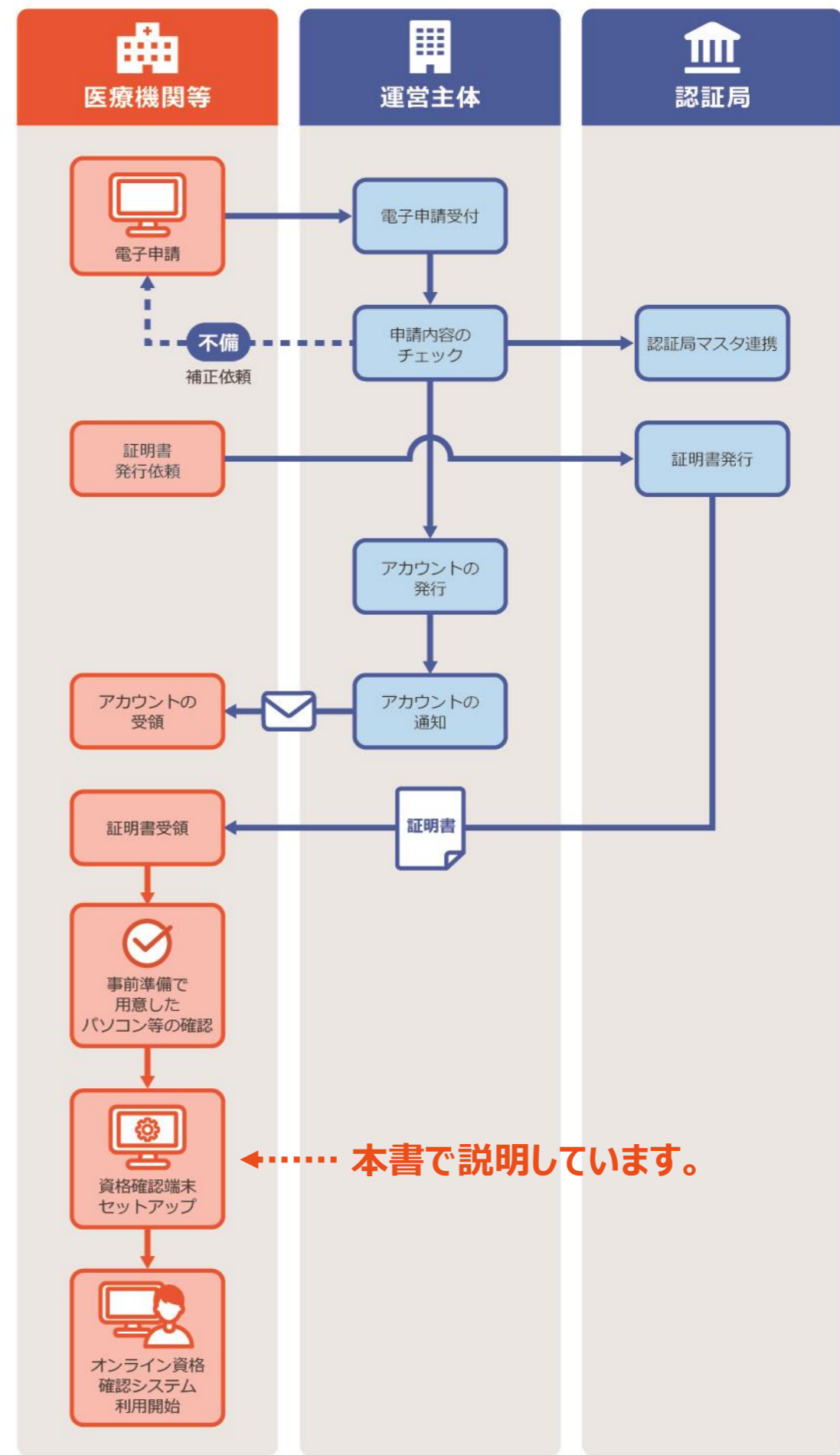
連携アプリケーションが動作しない
連携アプリケーションが動作しない場合、別紙 **トラブルシューティング 補16** を参照ください。

結果データファイルが操作できない
結果データファイルが操作できない場合、別紙 **トラブルシューティング 補9** を参照ください。

資格確認が完了しました。

資格確認端末のセットアップが完了しました。

電子申請からオンライン資格確認等システム利用開始までの流れ



⚠ セットアップ後はドキュメントに記載している状態で動かしてください。以下のような削除、変更などを行った場合は、正しく動作しないことがあります。その場合は、手順書に従って再度セットアップしてください。

- ・セットアップで展開された資材のこちらが想定しない改変を実施(削除、アクセス権変更等)
- ・クライアント証明書を削除
- ・有効期限が切れた古いクライアント証明書を使用している
- ・複数の端末にて共通のクライアント証明書を使用している
- ・.NET Frameworkの無効化 (アプリが動作できなくなります)
- ・TCPとUDPの53ポート (DNS) 、80ポート (HTTP:証明書申請用) 、123ポート (NTP) 、443ポート (HTTPS) 、8080ポート (プロキシ) を閉じた場合 (httpsのダウンロード等がエラーになります)
- ・バッテリーのみでの使用 (AC電源につないで使用してください)