

配信アプリケーションの確認について

背景

- ✓ 導入準備をいただいている医療機関・薬局から、配信アプリケーションを利用したアップデート（顔認証付きカードリーダーアプリケーション、顔認証ライブラリ、連携アプリケーション等）に関するお問合せを複数受領しております。
- ✓ また、配信アプリケーションは、オンライン資格端末等にインストールしているアプリケーションのバージョンが常に最新で稼働するために重要な機能です。
- ✓ 配信アプリケーションは、運用開始にあたってだけでなく、運用開始後も継続的に利用するものであることを踏まえて、利用に係る手順を改めて周知いたしますとともに、下記の点についての確認をお願いいたします。

対象の医療機関等

- ✓ 本資料は以下の環境の医療機関等が対象です。
 - 資格確認端末（パソコン）
 - Windows10 IoT Enterprise 2019 LTSC 64bit版
 - Windows10 Enterprise 2019 LTSC 64bit 版
 - 配信アプリでの配信方法（ネットワーク構成）
 - 配信拠点起点の構成
 - － 株式会社NTTPCコミュニケーションズ、富士通株式会社のIPsec+IKEサービスを利用している場合
 - － NTT東日本・西日本、中部テレコミュニケーション株式会社、株式会社QTnetのIP-VPN接続方式を利用している場合
 - ネットワーク事業者起点の構成
 - － 株式会社NTTデータ中国、三菱電機インフォメーションネットワーク株式会社のIPsec+IKEサービスを利用している場合
 - その他
 - 資格確認端末とレセプトコンピュータ端末が別端末であること（資格確認端末とレセプトコンピュータ端末を兼用していないこと）

確認事項

配信アプリケーションの利用開始にあたっては、下記2つの確認を行ってください。

- 1 支払基金の配信サーバーへの接続確認
- 2 各種アプリケーションのバージョン確認

➡➡ P.2

➡➡ P.3

バージョン

1.06版(2022年6月30日更新)

1. 確認手順 ①支払基金の配信サーバーへの接続確認

- ✓ 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、「配信サーバーへの接続確認」を押下することで、接続状況を確認してください。

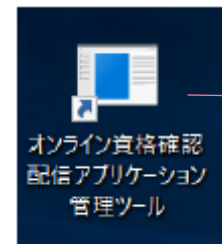
手順の概要

操作イメージ

1

ツール起動

- 医療機関等にある資格確認端末のデスクトップ画面にある、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。

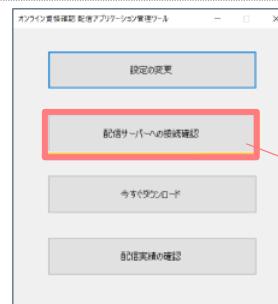


アイコンを押下することで、ツールを起動

2

接続状況の確認

- 「配信サーバーへの接続確認」を押下することで、支払基金の配信サーバーへ接続できているかどうかを確認するために信号を送ります。

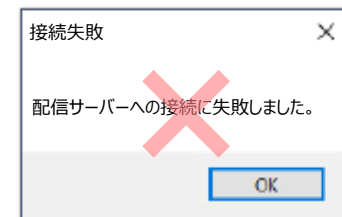
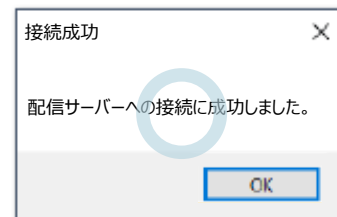


配信アプリケーション管理ツールの「配信サーバーへの接続確認」ボタンを押下

3

接続結果の確認

- 支払基金の配信サーバーへの接続に成功したか、失敗したか結果が表示されるため、表示内容を確認します。
 - 「接続成功」と表示されたら、当該対処は完了です。
 - 「接続失敗」と表示されたら、P.4の対処方法を実施します。



➡➡ P.4

1. 確認手順 ②各種アプリケーションのバージョン確認

- ✓ 現在インストールされているアプリケーションのバージョンが最新のバージョンと一致しているかを確認してください。
- ✓ 一致していなければ、アップデート処理を行ってください。

手順の概要

操作イメージ

1

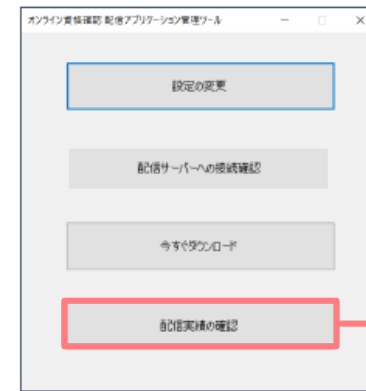
端末にある
現在の
バージョン
確認

- オンライン資格確認配信アプリケーション管理ツールから、医療機関等の資格確認端末に入っている、下記のアプリケーションの現在のバージョンを確認します。

- 配信アプリケーション
- 連携アプリケーション
- 顔認証ライブラリ

※ 手動でアップデートした場合、以下のバージョン情報ファイルをテキスト形式で開き、バージョンを確認してください。

- 連携アプリケーション (OqsComApp) C:\Program Files\OQS\OqsComApp\Version.info
- 配信アプリケーション (OpsDistroApp) C:\Program Files\OQS\OqsDistroApp\Version.info
- 顔認証 (OqsFaceApp) C:\Program Files\OQS-Auth\Version.info



[Information]
MedicalInstitutionCode= [REDACTED]
TerminalID= [REDACTED]

[DistributionApp]
Name= 配信アプリケーション
Version=1.0.4
UpdateDate=2021/03/02 16:04

[CooperationApp]
Name= 連携アプリケーション
Version=1.0.7
UpdateDate=2021/03/02 16:04

[FacialIdentificationLibrary]
Name= 顔認証ライブラリ
Version=1.0.6
UpdateDate=2021/03/08 18:29

- 医療機関等でお使いの顔認証付きカードリーダーの管理画面から、アプリケーションのバージョンを確認します。

- 顔認証付きカードリーダーアプリケーション

※ 別紙「顔認証付きカードリーダーのソフトウェアバージョンの確認手順」に詳細を記載



表示内容を確認

2

最新
バージョンを確認

- 医療機関等向けポータルサイトから、1で確認した4種のアプリケーション・ライブラリの最新バージョンを確認します。

(URL : <https://www.iryohokenjyoho-portalsite.jp/download/post-12.html> 最下部「アプリケーションバージョン情報」)

アプリケーション名	バージョン
1 連携アプリケーション	1.0.9
2 配信アプリケーション	1.0.4
3 顔認証ライブラリ	1.0.6
4 顔認証付きカードリーダーアプリケーション	1.0.4

3

アップデート
要否を確認

- 1で確認した4種のアプリケーション・ライブラリが、公開されている最新バージョンと一致しているかどうか確認します。
- 不一致であれば、P.8をもとにアップデートを行います。 >>> P.8

2. 確認できない場合の対処方法 ①配信サーバーへの接続に失敗するケース（1/4）

- ✓ よくある失敗例と解消法を以下に示します。
- ✓ 不具合が解消しない場合や不明点がある場合は、資格確認端末の設定作業を行った業者へお問合せください。

よくある失敗例

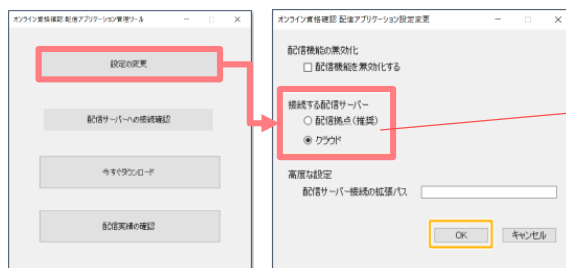
失敗例

解消手順の概要

操作イメージ

接続先の
配信サーバーの
選択を
誤っているケース

- オンライン資格確認配信アプリケーション管理ツールから、「設定の変更」を押下し、右記を参照の上、接続先が正しく設定されているか確認します。



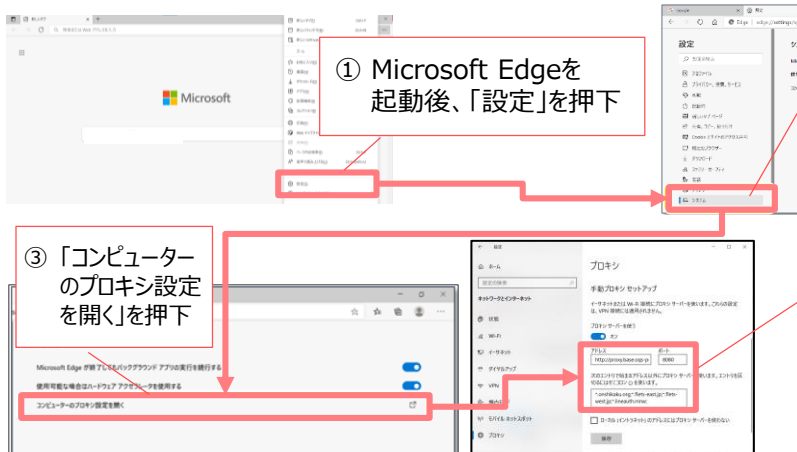
- ✓ 以下に該当する場合、「配信拠点(推奨)」を選択
 - IPsec+IKE サービス提供事業者
 - ・株式会社NTTPCコミュニケーションズ
 - ・富士通株式会社
 - IP-VPN 接続方式（光回線）
 - ・NTT東日本・西日本
 - ・中部テレコミュニケーション株式会社（CTC）
 - ・株式会社QTnet
- ✓ 以下に該当する場合、「クラウド」を選択
 - IPsec+IKE サービス提供事業者
 - ・株式会社NTTデータ中国
 - ・三菱電機インフォメーションネットワーク株式会社
 - その他

プロキシの例外
設定を誤っている
ケース

- 上記で接続先に「配信拠点(推奨)」を選択した場合、プロキシの例外設定内容が、正しく設定されているか確認します。
- なお、これまで発生している既知事象は以下の通りです。

【既知事象】

- ✓ 例外設定していないアドレスがある
- ✓ 設定値のセミコロンが抜けている



②「システム」を押下

- ④ 以下の内容を入力の上、保存します。
 - アドレス：proxy.base.oqs-pdl.org
 - ポート 8080
 - 以下のもの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

2. 確認できない場合の対処方法 ①配信サーバーへの接続に失敗するケース (2/4)

よくある失敗例

失敗例

プロキシ設定
のコマンドを
実行して
いなかったケース

必要な契約が
不足している
ケース

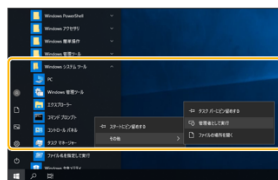
解消手順の概要

- 前頁で接続先に「配信拠点(推奨)」を選択しており、「医療機関等向けセットアップ手順書（資格確認端末編）」（URL：<https://www.iryohokenjyoho-portalsite.jp/download/post-12.html>「資格確認端末のセットアップ手順」）操作3においてプロキシ設定のコマンドを実行していなかった場合、実行します。

3 Windowsの設定を変更する（配信アプリケーション準備等）（つづき）

- 7 コマンドプロンプトを起動します。

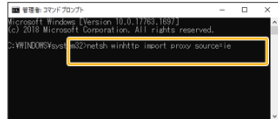
スタートボタンをクリックし、表示されるメニューからWindowsシステムツールを選択します。
コマンドプロンプトメニューを右クリックし、その他→管理者として実行をクリックします。



- 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。

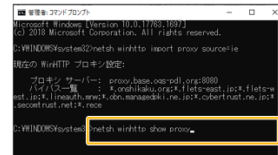
表示内容

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;
.reco;.web.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われています（実際は改行されません）。

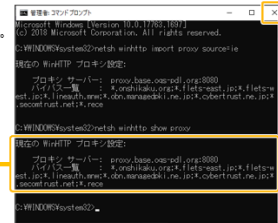
- 10 以下のコマンドを入力し、Enterキーを押します。

```
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Xボタン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;
.reco;.web.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われています（実際は改行されません）。

注意

P.12の①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、開いた内容とどりに設定されていることを確認してください。

プロキシサーバーの設定が完了しました。

P.13

- IP-VPNでNTT回線を使用している場合、フレッツ・v6オプション契約がされていない可能性があります。フレッツ・v6オプション契約の詳細は以下の資料をご確認ください。
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)
<https://www.iryohokenjyoho-portalsite.jp/download/post-12.html>

2. 確認できない場合の対処方法 ①配信サーバーへの接続に失敗するケース（3/4）

よくある失敗例

失敗例

解消手順の概要

接続先DNSの 設定を誤っている ケース（1/2）

- 「IP-VPN接続方式(フレッツ光による接続)」のIPv6（オンライン資格確認等システム接続）をご利用の場合、接続先DNSが正しく設定されているか確認します。
- ルータにてIPv6の接続先DNSを設定する場合
ドメイン毎に、以下の通り接続先のDNS指定を行います。
※「ローカルドメイン問合せテーブル」等を利用して設定します。設定方法については、ご利用いただくルータの取扱説明書をご確認ください。
※ 最新の設定値は「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)」（URL：<https://www.iryohokenjyoho-portalsite.jp/download/post-12.html>）を参照してください。
- a. 光回線（NGN）のDNSサーバーを設定
 - ＜NTT東日本エリアの場合＞
ドメイン名：flets-east.jp
優先DNSサーバー 2404:1a8:7f01:a::3
代替DNSサーバー 2404:1a8:7f01:b::3
 - ＜NTT西日本エリアの場合＞
ドメイン名：flets-west.jp
優先DNSサーバー 2001:a7ff:5f01::a
代替DNSサーバー 2001:a7ff:5f01:1::a
- b. 以下の6つのドメインは、オンライン資格確認NW基盤のDNSサーバーを設定
ドメイン名：onshikaku.org / lineauth.mnw / base.oqs-pdl.org
managedpki.ne.jp / cybertrust.ne.jp / secomtrust.net
 - ＜NTT東日本エリアの場合＞
優先DNSサーバー 2404:01A8:F583:0D00::53:1
代替DNSサーバー 2404:01A8:F583:0D00::53:2
 - ＜NTT西日本エリアの場合＞
優先DNSサーバー 2001:a7ff:f014:d00::53:1
代替DNSサーバー 2001:a7ff:f014:d00::53:2

2. 確認できない場合の対処方法 ①配信サーバーへの接続に失敗するケース (4/4)

よくある失敗例

失敗例

解消手順の概要

- ▶ 資格確認端末にてIPv6の接続先DNSを設定する場合
右記を参照の上、接続先のDNS指定を行います。

※ 最新の設定値は「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)」(URL : <https://www.iryohokenjyo-ho-portalsite.jp/download/post-12.html>) を参照してください。

接続先DNSの
設定を誤っている
ケース (2/2)

操作イメージ

① 「Windowsボタン」を押下後、「設定ボタン」を押下

② 「ネットワークとインターネット」を押下

③ 「状態」を押下後、「アダプターのオプションを変更する」を押下

④ 該当するイーサネットを右クリックし「プロパティ」を押下

⑤ 「インターネットプロトコルバージョン 6 (TCP/IPv6)」にチェック

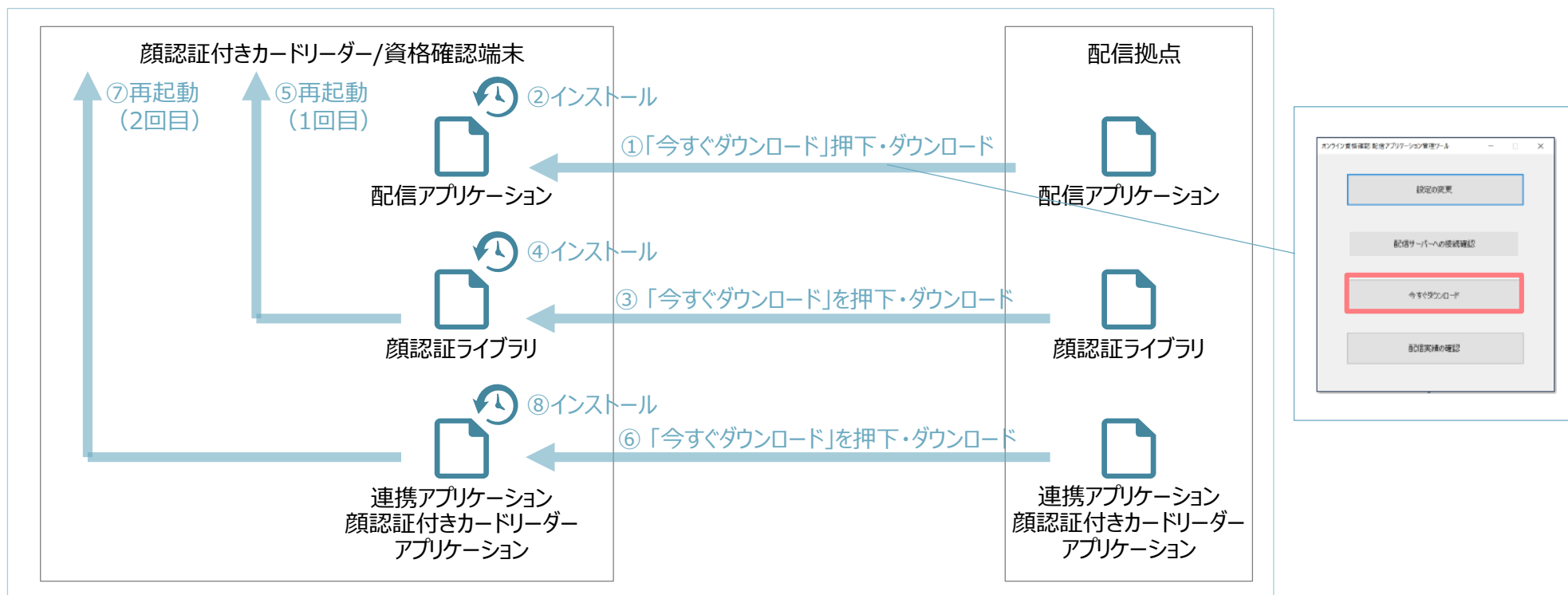
⑥ 「次のDNSサーバーのアドレスを使う」にチェックをいれ、以下の設定を行い、「OK」をクリック
＜NTT東日本エリアの場合＞
優先DNSサーバー
2404:01A8:F583:0D00::53:1
代替DNSサーバー
2404:01A8:F583:0D00::53:2
＜NTT西日本エリアの場合＞
優先DNSサーバー
2001:a7ff:f014:d00::53:1
代替DNSサーバー
2001:a7ff:f014:d00::53:2

2. 確認できない場合の対処方法 ②アプリケーションをアップデートできていないケース（1/3）

- ✓ 配信アプリケーション又は顔認証ライブラリを含む、複数のアプリケーションをアップデートする際、以下の対処方法を参考にアップデートしてください。
- ✓ なお、バージョンアップしたアプリケーションの配信開始当日は、多くの医療機関等からのアクセス集中が想定されることから、「今すぐダウンロード」のご利用はお控えください。導入作業に限りご利用いただきますよう、ご協力をお願いいたします。

対処方法

（例）配信アプリケーション、顔認証ライブラリ、連携アプリケーション・顔認証付きカードリーダーアプリケーションをそれぞれアップデートが必要な場合 ※ すでに最新バージョンになっている場合は、その手順を実施する必要はありません。



※ダウンロードとインストールで20分程度

2. 確認できない場合の対処方法 ②アプリケーションをアップデートできていないケース（2/3）

注意点

- ✓「今すぐダウンロード」を押下し、ダウンロード及びインストールに20分程度※要するため、時間をおいてから再起動を行ってください。バージョンアップできていない場合、再度時間をおいて再起動してください。
（配信アプリケーションのバージョンが1.0.10以降の場合、次ページの再起動通知が表示されます。再起動通知が表示され次第、資格確認端末を再起動していただいて問題ありません。）
- ✓「今すぐダウンロード」を押下し、エラーが発生した場合、表示されるエラーメッセージ毎に、対処をお願いいたします。

エラーメッセージ

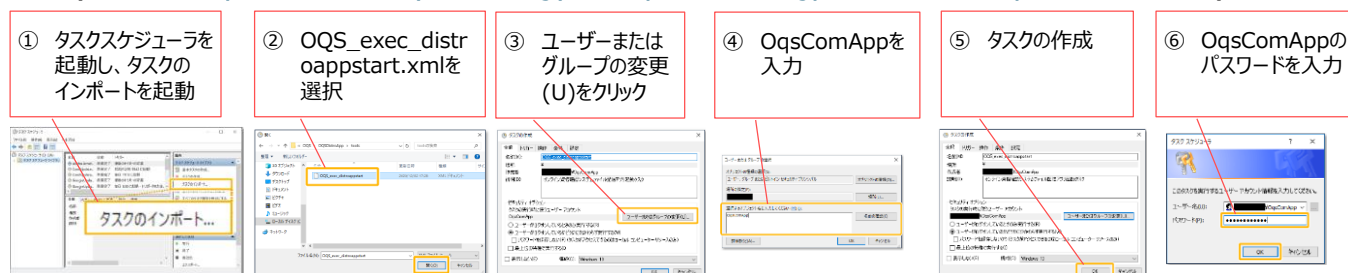
対処方法

管理ツールに異常が発生しました。
管理ツールを終了します。

オンライン資格確認システムファイル配信アプリ起動タスクを登録してください。

※詳細は「医療機関等向けセットアップ手順書（資格確認端末編）」を確認してください。

(URL : <https://www.iryohokenjyoho-portalsite.jp/download/post-12.html>)



配信サーバーへの接続に失敗しました。

ネットワーク設定を確認してください。

※詳細は本資料の「2. 確認できない場合の対処方法 ①配信サーバーへの接続に失敗するケース」(p.4-p.7)を確認してください。

配信実績管理ファイルが見つかりません。

C:\¥ProgramData¥OQS¥OQSDistroApp¥config¥OQSDistroApp.iniファイルが無い場合、復旧には再インストールが必要となります。

(当該ファイルがある場合、[オンライン資格確認等コールセンターへお問い合わせ](#)、又は医療機関等ONSの障害報告登録をお願いします。)

2. 確認できない場合の対処方法 ②アプリケーションをアップデートできていないケース (3/3)

- ✓ セットアップ時に配信アプリケーションVer1.07以前または連携アプリケーションVer1.09以前をインストールした医療機関等において、前頁の対処方法により解消しない場合、タスクスケジューラに登録しているタスクの実行に失敗している可能性があります。以下の対処を実施してください。

対処方法

手順の概要

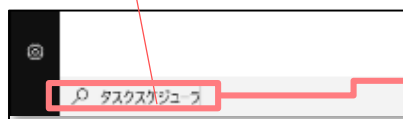
- ご利用の資格確認端末で、タスク スケジューラを起動します。

操作イメージ

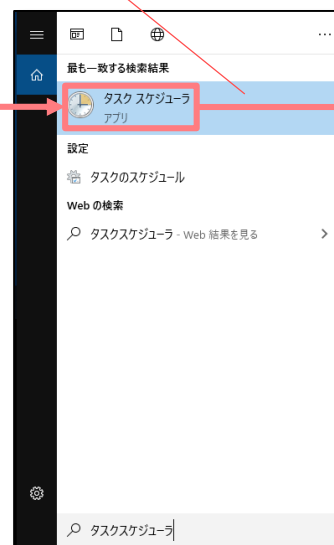
1

タスク スケジューラの 起動

- ① 検索ボックスに「タスク スケジューラ」と入力



- ② 検索結果から「タスク スケジューラ」を押下し、タスク スケジューラを起動



- ③ 左側の領域から、タスク スケジューラ ライブラリを押下



次頁へ続く

2. 確認できない場合の対処方法 ②アプリケーションをアップデートできていないケース (3/3)

- ✓ セットアップ時に配信アプリケーションVer1.07以前または連携アプリケーションVer1.09以前をインストールした医療機関等において、前頁の対処方法により解消しない場合、タスクスケジューラに登録しているタスクの実行に失敗している可能性があります。以下の対処を実施してください。

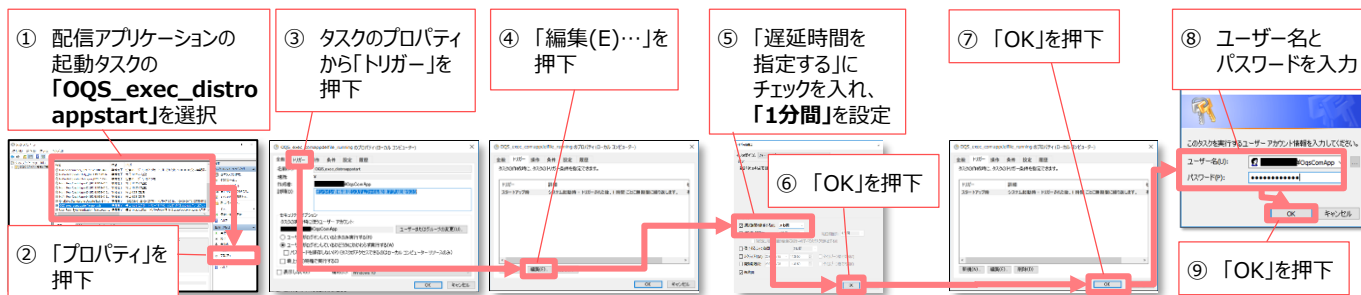
対処方法

手順の概要

- タスク スケジューラから、スタートアップ時に起動する以下の2つのタスクに対して、それぞれ遅延時間を設定します。
 - 「OQS_exec_distroappstart」の遅延時間を「1分間」に設定
 - 「OQS_exec_comappdelfile_running」の遅延時間を「30秒間」に設定

タスクの設定変更

操作イメージ



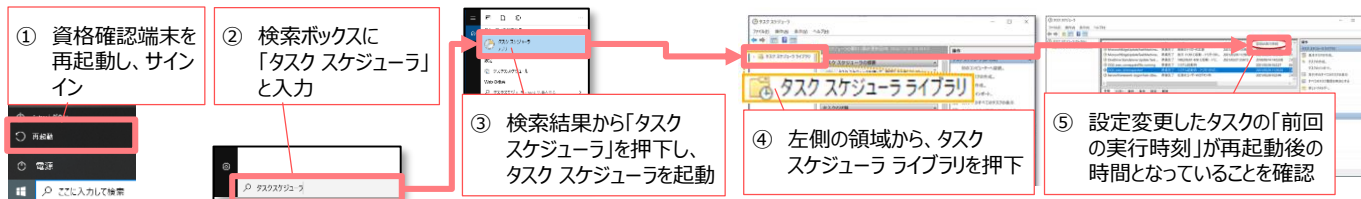
※赤字以外は上記 配信アプリ起動タスクの設定変更 と同じ手順

- ①タスク スケジューラ ライブラリからOQS_exec_comappdelfine_running を選択し、プロパティをクリックします。
- ②タスクのプロパティが表示されます。トリガー をクリックします。
- ③トリガーが表示されます。編集(E)…をクリックします。
- ④「遅延時間を指定する」にチェックを入れ、「30秒間」を設定し、OK をクリックします。
- ⑤トリガーが表示されます。OKボタンをクリックしてください。
- ⑥タスクを実行する実行アカウントの入力が表示されます。ユーザー名(U):とパスワード(P):を入力した後、OKをクリックします。

3

タスクの状態確認

- 資格確認端末を再起動し、再起動後にタスクが実行されていることを確認します。

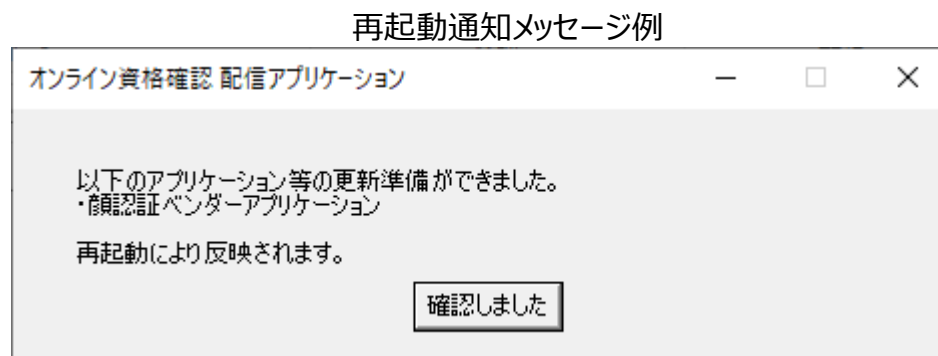


3. アプリケーションのアップデートがあったときの対処方法

対処方法

- ✓ アプリケーションのアップデートに伴って、資格確認端末の再起動が必要である場合、再起動通知を行います。当該通知が表示された場合、医療機関等にて手動で再起動していただくようお願いいたします。

対象アプリケーション：顔認証ライブラリ・連携アプリケーション・顔認証ベンダーアプリケーション



※「確認しました」ボタンや×ボタンの押下等により、資格確認端末が再起動されることはありません。

※また、通知が表示された際、診療時間外等の影響がないタイミングで適宜資格確認端末を再起動し、最新のアプリケーションを適用するようにお願いいたします。

【別紙】 顔認証付きカードリーダーのソフトウェアバージョンの確認手順

顔認証付きカードリーダーのソフトウェアバージョンの確認手順について、各社の確認手順を次頁以降でご確認ください。

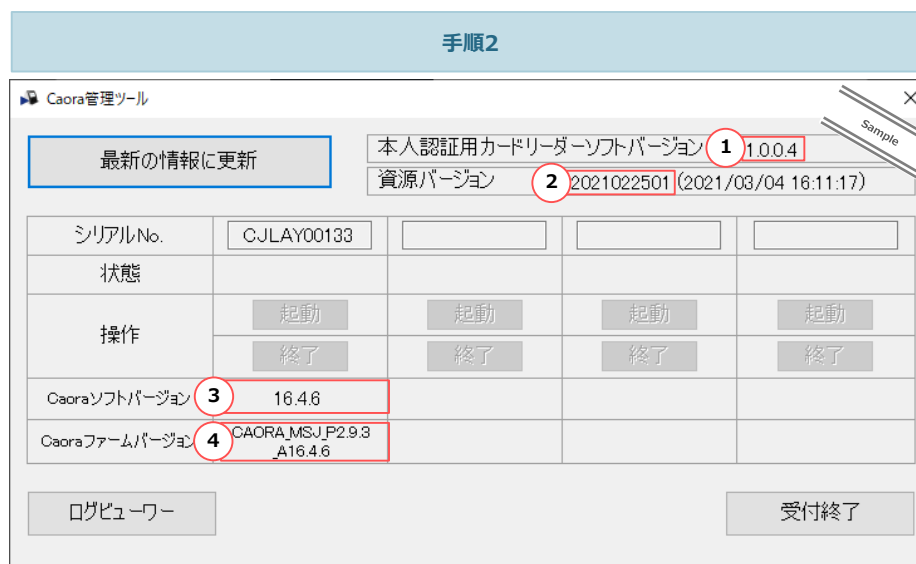
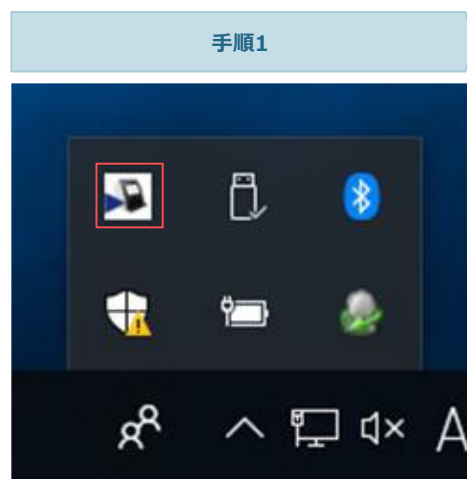
【別紙】 顔認証付きカードリーダーのソフトウェアバージョンの確認手順

富士通Japan株式会社

バージョン情報確認手順

1. 資格確認端末のタスクトレイよりCaora管理ツールを起動してください
 2. 表示されるCaora管理ツールにてバージョン情報をご確認ください
 - ① 本人認証用カードリーダーソフトバージョン
 - ② 資源バージョン
 - ③ Caoraソフトバージョン
 - ④ Caoraファームバージョン
- ※複数台接続時は、右の列に順に表示されます。

画面イメージ



【別紙】 顔認証付きカードリーダーのソフトウェアバージョンの確認手順

パナソニックコネクト株式会社

バージョン情報確認手順

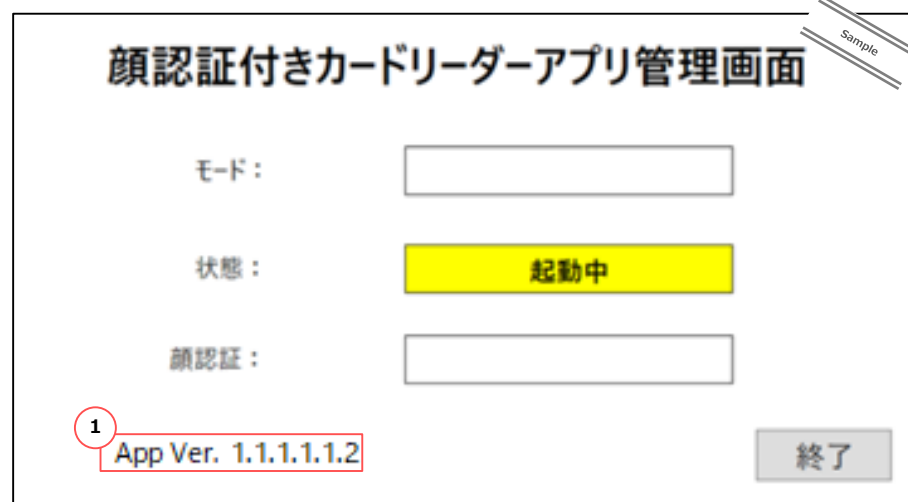
1. 資格確認端末のデスクトップ画面で、「顔認証付きカードリーダーアプリ」のアイコン（ショートカット）をダブルクリックして起動してください
2. 表示される顔認証付きカードリーダーアプリ管理画面にてバージョン情報をご確認ください
 - ① App Ver.

画面イメージ

手順1



手順2



【別紙】 顔認証付きカードリーダーのソフトウェアバージョンの確認手順

株式会社アルメックス

バージョン情報確認手順

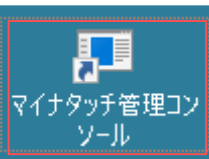
1. 資格確認端末のデスクトップ画面で、「マイナタッチ管理コンソール」のアイコン（ショートカット）をダブルクリックして起動してください
2. 表示されるマイナタッチ管理コンソール左上の「ヘルプ」を押下してください
3. ヘルプメニューより、「バージョン情報」を押下してください
4. 表示されるバージョン情報画面にてバージョン情報をご確認ください
 - ① 管理コンソール
 - ② アップデート管理ツール
 - ③ カードリーダー本体 ※複数台接続時は、接続台数分表示されます。

画面イメージ

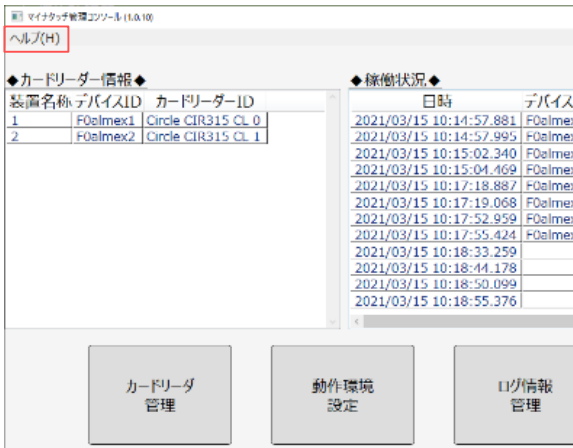
手順1

手順2,3

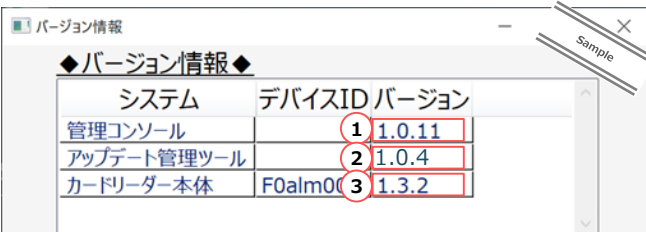
手順4



マイナタッチ管理コンソール



画面イメージ: マイナタッチ管理コンソール (1.0.10) のヘルプメニュー。ヘルプ(H)ボタンが赤枠で囲まれている。ヘルプメニューには「カードリーダー情報」および「稼働状況」の項目があり、それぞれ詳細なデータが表示されている。



画面イメージ: バージョン情報画面。バージョン情報が赤枠で囲まれている。

システム	デバイスID	バージョン
管理コンソール		1.0.11
アップデート管理ツール		1.0.4
カードリーダー本体	F0alm00	1.3.2

【別紙】 顔認証付きカードリーダーのソフトウェアバージョンの確認手順

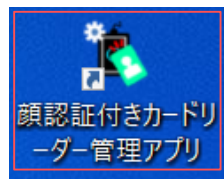
キヤノンマーケティングジャパン株式会社

バージョン情報確認手順

1. 資格確認端末のデスクトップ画面で、「顔認証付きカードリーダー管理アプリ」のアイコン（ショートカット）をダブルクリックして起動してください
2. 環境設定画面より該当のカードリーダーの接続状態が「接続中」であることを確認してください
3. 画面左端の下から2つ目のアイコンを選択してください
4. バージョン情報画面よりバージョン情報をご確認ください（※複数台接続時は、⑤よりカードリーダー名を選択してください）
 - ① 顔認証付きカードリーダー管理アプリケーション
 - ② ログ収集コマンドアプリケーション
 - ③ 顔認証付きカードリーダーアプリケーション
 - ④ 顔認証付きカードリーダーOSソフトウェア

画面イメージ

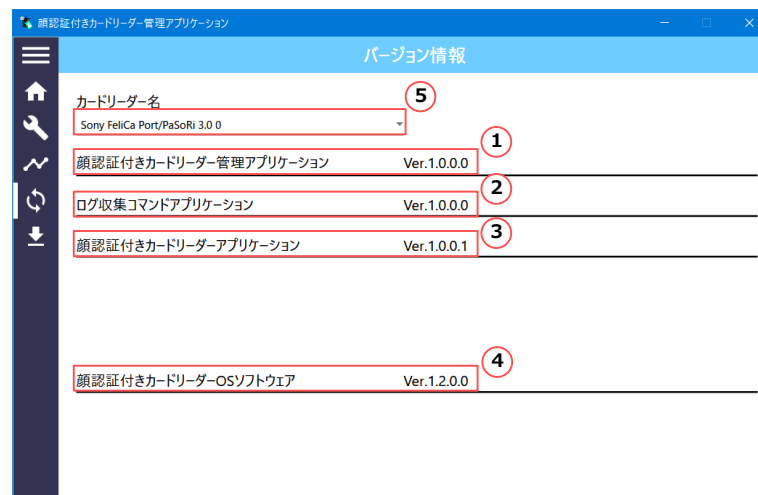
手順1



手順2,3



手順4



【別紙】 顔認証付きカードリーダーのソフトウェアバージョンの確認手順

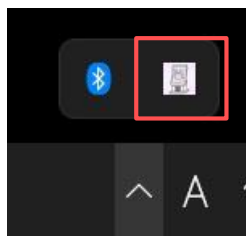
アトラス情報サービス株式会社

バージョン情報確認手順

1. 資格確認端末のタスクトレイより「顔認証付きカードリーダー-EXC-9000管理ツール」のアイコンをクリックし、管理ツールを表示してください。
2. 状態が「受付可能」であることを確認してください。
3. 表示される内容にて、バージョン情報をご確認ください。
 - ①顔認証付きカードリーダー-EXC-9000管理ツール
4. 設定ボタンをクリックしてください。
5. 表示される内容にて、バージョン情報をご確認ください。
 - ②EXC-9000アプリケーション

画面イメージ

手順1



手順2,3



手順4

