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

(Windows IE)

Version 1.2.0

令和3年3月22日

目次

はし	じめに		4
0.	事前	〕準備	4
1.	証明	目書の取得とインストール	5
1	. 1.	証明書のダウンロード	5
1	. 2.	証明書のインストール	7
	1.2.	1 こんなときは!10	0
1	. 3.	登録した証明書の確認1	1
1	. 4.	証明書のバックアップ1	2
1	. 5.	MPKI クライアントインストール (更新時に簡単に更新ができるツール)1	3
1	. 6.	認証用の証明書の選択画面が表示された場合10	6
2.	証明]書の更新1'	7
2	. 1.	MPKI クライアントを利用した更新1	7
	2.1.	1 こんなときは!18	8
	2.1.	2 MPKI クライアント利用時の証明書バックアップ 1	9
2	. 2.	更新申請画面からの更新	2
	2.2.	1 こんなときは!	5
3.	証明]書の失効	6
4.	証明]書の削除2'	7
5.	サホ	ペート情報	9
5	. 1.	MPKI クライアント利用環境	9
5	. 2.	ご利用にあたっての注意事項29	9
	5.2.	1 MPKI クライアントインストール時の注意事項	9
	5.2.	2 セッション無効時の対応トラブルシューティング	9

Date	Version #	Summary of Changes
2020/12/14	1. 0. 0	初版
2020/1/4	1. 1. 0	・「1.1 証明書ダウンロード」のダウンロード方法の追記
		・手順案内様式の変更
2021/3/22	1. 2. 0	・「3 証明書の失効」の修正

はじめに

本書は、オンライン請求ネットワーク関連システム共通認証局(以下、「共通認証局」という。)において、利用者がオペレーションできる証明書の取得、更新、および更新ツール(MPKI クライアント)について記述したものです。

0. 事前準備

証明書の取得には、レセプトオンライン請求ネットワークの接続設定を行う必要がありま す。未設定の方は、システムベンダ等へご確認の上、設定ください。

● レセプトオンライン請求の場合

[ネットワーク接続設定と端末のセットアップ設定]

オンライン請求システムセットアップ CD-ROM に同梱の「オンライン請求システム操作手順書」参照

1. 証明書の取得とインストール

1.1. 証明書のダウンロード

オンライン請求ネットワークへ接続の端末(レセプトオンライン請求用端末)で証明書を 取得します。

・オンライン請求システムのログイン画面



・電子証明書ダウンロードサイト

オンライン請求システム専用認証局 電子証明書ダウンロードサイト
ログイン
ユーザロとバスワードを入力して下さい。 ユーザロ バスワード
 お問合せ ながったい、ボデスクム、ルブデスクタン 電話番号:0120-60-7210 く特定健診・保健指導システムヘルプデスク> 電話番号:0120-109-957 新しい電子証明書の発行申請はこちらをクリックしてください。 <u>電子証明書の発行申請サイト </u> 証明書の発行申請サイト 証明書の発行申請サイト 証明書の空行申請サイト

1. <u>レセプトオンライン請求端末</u>からダウンロ ードサイトにアクセスします

【ダウンロードサイト】

https://cert.obn.managedpki.ne.jp/p/rcd

オンライン請求システムのログイン画面または 電子証明書ダウンロードサイトよりアクセスで きます。



1.2. 証明書のインストール

名前 更新日時	1. ダウンロードした証明書ファイルを右クリ
202011270094998.p12 PFX のインストール(I) 開く(O) S Skypeで共有	ックし、「PFX インストール」 をクリックします。
★ 顧明書の12ポートウイザード	2.「 現在のユーザー 」を選択し、「 次へ 」をクリ ックします。
証明書のインボート ウィザードの開始	
このウイザードでは、証明巻、証明巻信頼リスト、および証明巻矢効リストをディスクから証明巻ストアにコピー します。 証明機関によって辛行された証明者は、ユーザーIDを確認し、データを保護したり、またはヤキュリティで保護	
型が成果により、そうにでいた型が目的よう。クロンを知らい、クジにない、こくならにてコンパイはな されたさかりつう接接を含んでいます。証明書ストアは、証明書が保留されるシステ ム上の環境です。 ② 原を処于 ○ ローカル コンピューター(」)	
※行するには、(次へ)をクリックしてくたさい。 次へ(N) キャンセル	
X - 多 証明者のインボートウィザード	3. フィル名に証明書のファイル名が表示され
インボートする証明書ファイル インボートするファイルを指定してください。	くいることを確認し、「 次へ 」 をクリックします。
77イル名(E): CHUsersHoucoxiHDownloadsH202020190000055,p12 参照(E)	
注意:次の形式を使うと 1 20ファイルに複数の証明書を保管できます:	
Felsonal information Certainge Finder # LorAn (2) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P78) Microsoft シリアル化された証明書ストア (.SST)	

	× 4. [パスワード]に「1.1.証明書のダウンロー
← 😺 証明書のインポート ウィザード	ド」で設定したパスワードを入力します。
とおよりえる維持するために、秘密キーはパスワードで保護されています。 水田本 中のパスワードを入力してください。 パスワードを入力してください。 パスワードであ示() パスワードの表示() パンボートオブション(): 小ビホートオブション(): 小ビホートオブション(): 小ビホートオブション(): 小ビホートオブション(): 小ビホートオブション(): 小ビホートオブション(): 小ビホートオブション(): 小ビホートオブション(): 小ビホートオブション(): 小ビホーション(): 小い(): (): (): (): (): (): ():	[秘密キーの保護を強力にする]の チェックを外す [このキーをエクスポート可能にする]を チェックする [すべての拡張プロパティを含める]を チェックする 「次へ」をクリックします。 【こんなときは!】 「秘密キーの保護を強力にする」のチェッ クが外せない場合は、セキュリティを強化 する設定がされているため、P10「1.2.1 こ んなときは!」を参照
 ★ ● 証明書のインボート ウィブード ビ明書ストアと 証明書ストアは、証明書が保管されるシステム上の領域です。 Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。 ● 証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。 ● 証明書気トアを自動的に選択させるか、証明書の場所を指定することができます。 ● 証明書気トアで、回動的に証明書ストアを直訳する(j) ● 証明書気トアで、回動的に証明書ストアを直訳する(j) ● 証明書気トア: ● 証明書入下: ● 評価()… ● 評価()… ▼ 評価()… ▼ 評価()… ▼ 次へ(い) ▼ オッンセル ▼ 次へ(い) ▼ 次のののののののののののののののののののののののののののののののののののの	5.「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」を選択後、「次へ」をクリッ クします。

 ぼ明書のインボートウィザード × i 正しくインボートされました。 KLインボートされました。 KLインボートされました。 KLインボートされました。 KLT = 100000000000000000000000000000000000	
 	
セキュリティ書告 ※行きが次であると主張する証明機関 (CA) から証明書をインストールしよ うとしています: Online Billing NW Common Root CA-G1 証明書が実際に "Online Billing NW Common Root CA-G1": からのものであるかどうかを検証できません。"Online Billing NW Common Root CA-G1": 連絡して発行者を確認する必要があります。 であること、たた体認 (ご住田のブラウボデ	した
 	t、

1.2.1 こんなときは!

※証明書インストール時に「新しい秘密交換キーをインポートします」と表示された場合は、次の操作を行ってください。

新しい秘密交換キーをインポートします ×	1.「 セキュリティレベルの設定 」をクリックし
アプリケーションは保護されたアイテムを作成しています。 CryptoAPI 秘密キー セキュリティレベル - 中 セキュリティレベルの設定(S)	ます。
OK キャンセル 詳細(D)	
バスワードの作成 × このアイテムを保護するための、パスワードを作成します。	2.任意のパスワードを入力し、「 完了 」をクリ ックします。
このアイテム用に新しいパスワードを作成する。 CryptoAPI 秘密キー のパスワード: パスワード: 確認入力:	【※重要※】 作成したパスワードは、今後の証明書の更 新時に利用するため、忘れないよう大切に 保管ください。
< 戻る 完了(E) キャンセル	
新しい秘密交換キーをインボートします ×	3.「 OK 」をクリックします。
アブリケーションは保護されたアイテムを作成しています。	
CryptoAPI 秘密キー	
セキュリティレベル - 高 セキュリティレベルの設定(<u>S</u>)	
OK キャンセル 詳細(<u>D</u>)	

1.3. 登録した証明書の確認



1.4. 証明書のバックアップ

外部記録媒体等へ証明書をバックアップします。バックアップした証明書はパソコンが故 障した際などに他のパソコンにインストールします。その際には、「1.1.証明書のダウンロ ード」で設定したパスワードも必要となるため、忘れないように保管ください。



表示(V) 並べ替え(O) グループで表示(P) 最新の情報に更多

アクセスを許可する(G

 WinMerge
 新提作成(X プロパティ(R) 1. インストールを行った証明書ファイルを選 択し右クリックで「**コピー**」を選択します。

2.外部記録媒体等のフォルダを開き、「**貼り付**

け」を選択します。

【注意】

■ デスクトップ
 ■ デスクトップ
 ■ デスクトップ
 ■ デスクトップ
 ■ デスクトップ
 ■ ドキュメント
 ■ ビクチャ

E 177*

「証明書」「証明書発行通知書」「証明書の取得画面で入力した証明書パスワード」は厳重に管理して ください。証明書の情報が第三者に知られると、証明書が不正に使用される恐れがあります。 証明書を紛失した場合、または、第三者に知られた可能性がある場合は、速やかに証明書失効申請を 行ってください。また、パソコンを紛失した場合も証明書が不正に使用される恐れがあります。速や かに証明書失効申請を行ってください。



1.5. MPKI クライアントインストール

(更新時に簡単に更新ができるツール)

【MPKI クライアントとは】

MPKI クライアントを使用すると、有効期限の前に更新をお知らせする機能や証明書の更新 を簡易に行う機能が利用できます。 MPKI クライアントをインストールできる対象の OS は、<u>Windows8</u>と <u>Windows10</u>です。 利用環境の詳細は「5.1 MPKI クライアント利用環境」を参照ください。



妃 Cybertrust Managed PKI Client – 🗆 🗙	
Cybertrust Managed PKI Client セットアップ ウィザード しょうこそ	4. Cybertrust Managed PKI Client セットア
	ッフワイサード」が開始されます。「次へ」をク
インストーラーは Cybertrust Managed PKI Client をインストールするために必要な手順を示します。	リックします。
この製品は、著作権に関する法律および国際条約により保護されています。この製品の全部 または一部を無断で複製したり、無断で複製物を頒布すると、著作権の侵害となりますのでご	
++ンセル 〈戻る(B) 次へ(W) >	
體 Cybertrust Managed PKI Client — X	5.「 次へ 」をクリックします。
インストール フォルターの選択	
インストーラーは次のフォルダーへ Cybertrust Managed PKI Client をインストールします。	
このフォルターにコンストールするにはない、そうしゅうしていため、もかのフォルターにインストールするには、アドレスを入力するか「参照」をクリックしてください。	
U:#Users#terakawa#AppData#Local#Programs#UyDertrustMIFKICIII 参照(R)	
ディスク領域(<u>D</u>)	
キャンセル 〈 戻る(B) (次へ(N) >	
妃 Cybertrust Managed PKI Client — 🗆 🗙	6 「次へ」をクリックします。
インストールの確認	
Cybertrust Managed PKI Client をインストールする準備ができました。	
「次へ」をクリックしてインストールを開始してください。	
キャンセル 〈 戻ろ(B) (次へ(N) >	

# Cybertrust Managed PKI Client - □ × インストールが完了しました。	7.「 閉じる 」をクリックします。
Cybertrust Managed PKI Client は正しくインストールされました。 終了するには、【閉じる】をクリックしてください。	
Windows Update で、NET Framework の重要な更新があるかどうかを確認してください。 キャンセル く戻る(B) 開じる(C)	
8 D S Cybertrust	8. MPKIクライアントのインストールが完了す ると、スタートメニューに以下が追加されます。
● 新規 ① Cybertrust Managed PKI Client 新規	

1.6. 認証用の証明書の選択画面が表示された場合

認証用	の証明書の選択	1.「証明書の選択」画面で発行者が
サイト cert.obn.managedpki.ne.jp: では資格情報が必要です:		「Online Billing NW Common Root CA」となっ
S	TEST Client 003 KRS GP CA 2014 TEST 2014/6/20	ていることを確認し、「 OK 」をクリックしてく ださい。
ģ	TEST Client 001 KRS GP CA 2014 TEST 2014/6/20	
	Online Billing NW Common Root CA - G1 2020/7/3	
証明書	- 情報 OK キャンセル	

2. 証明書の更新

2.1. MPKI クライアントを利用した更新

証明書の有効期限が迫ると、お知らせが表示されます。有効期限が切れる前に、「2.2.証明 書の更新手順」の作業を行ってください。

【お知らせが表示される条件】

有効期限が切れる 90日前、60日前、30日前、15日前、7日前から毎日

有効期限が切れた場合

【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	1.「 証明書に関するお知らせ 」通知をクリック します。 【こんなときは!】
証明書の新規登録(N) 証明書の更新(U) パージョン情報(V)	お知らせが表示されていない場合は、タス クトレイのアイコンを右クリックから操作 できます。表示される以下のメニューか ら、[証明書の更新] をクリックします。
Cybertrust Managed PKI Client × 「直辺明書 – 覧」から更新対象の証明用書を選択し、「証明書更新」ボタンをグリックしてください。 更新された証明書は、自動でインストールされます。 正印用書 – 覧 (し: 証明用書 – 覧 (し: ※ 発行先 発行者 有効期限 20000005 CN-Online Diffice NM Co. 2023/05/26 1201:39 回11A123456 CN=Online Diffice NM Co. 2023/05/26 1201:39	2. 更新したい証明書を選択し、「証明書更新」 をクリックします。
Cybertrust Managed PKI Client × 1003 選択した証明書を更新します。よろしいですか? はいY いいえ(N)	3.「はい」をクリックします。

Cybertrust Managed PKI Client × 1004 証明書の更新が完了しました。	4.「 OK 」をクリックします。
Cybertrust Managed PKI Client × 1006 更新前の証明書を削除しますか?	5.「 はい 」をクリックします。
	6.「 OK 」をクリックします。
1005 更新前の証明書の削除が完了しました。	
OK	

2.1.1 こんなときは!

※パスワードの入力が求められた場合は、証明書のインストール時「1.2.1 こんなとき

は!」で設定したパスワードを入力します。

Windows セキュリティ × 資格情報が必要です 秘密キーへのアクセスをアプリに許可するには、パスワードを入力してください:	 パスワードを入力し、「許可」をクリックします。 ※パスワードは、証明書のインストール時「1.2.1 こんなときは!」で設定したパスワー
キーの説明 : CryptoAPI 秘密キー パスワード /パスワード /パスワードの入力	ドです。
許可許可しない	

2.1.2 MPKI クライアント利用時の証明書バックアップ

ファイル名を指定して実行(R) シャットダウンまたはサインアウト(U) > スタート デスクトップ(D) ・ CCIC/C/(20,55)	1. 画面の左下の Windows ボタンを右クリック し、「 ファイル名を指定して実行 (R) 」をクリッ クします。
 ファイル名を指定して実行 実行するプログラム名、または開くフォルダーやドキュメント名、イン ターネット リソース名を入力してください。 名前(Q): certmgr.msc / OK キャンセル 参照(B) 	2.「certmgr.msc」を入力し、「OK」ボタンを クリックします。
 □ certmgr - [証明書 - 現在のユーザー] ファイル(F) 操作(A) 表示(V) ヘルプ(H) マー・ □ □ □ 証明書 - 現在のユーザー ○ □ 証明書 ○ □ 信頼されたルート証明機関 ○ □ エンタープライズの信頼 ○ □ 中間証明機関 □ 中間証明機関 □ □ ロー・ □ □ = f = ±ブ≤/エ/2 	3.「 個人 」から「 証明書 」をクリックします。
発行先 発行者 有効期限 011111111 Online Billing NW Common Root CA 2024/03/22 開<(O)	4. 発行者が「Online Billing NW Common Root CA」の <u>有効期限が新しい証明書</u> を選択し、右クリ ック後、「 すべてのタスク 」−「エクスポート」を クリック。

← 夢 証明書のエクスポート ウィザード	5.「 次へ 」をクリックします。
証明書のエクスポート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リストおよび証明書失効リストを証明書ストアからディスクにコピーします。	
証明機関によって発行された証明書は、ユーザーIDを確認し、データを保護したり、またはセキコリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保留されるシステ ム上の領域です。	
統行するには、「次へ」をクリックしてください。	
次へ回 キャンセル	
★	6. はい、秘密キーをエクスボートします」を
松舎キーのエクスポート	選択し、「次へ」ホタンをクリックします。
秘密キーを証明書と一緒にエクスボートすることができます。	
秘密キーはパスワードで保護されています。秘密キーを証明音と一緒にエクスポートする場合は、パスワードを	
入力する必要があります。 証明書と一緒に秘密キーをエクスポートしますか?	
 (すい、秘密キーをエクスポートします(2)) 	
○ いいえ、秘密キーをエクスボートしません(◎)	
次へ(12) キャンセル	
×	7. [Personal Information Exchange -
← 🛷 証明書のエクスポート ウィザード	
	PKCS#12(.PFX)」を選択し、「証明のパスにある
エクスポート ファイルの形式	証明書を可能であればすべて含む」と「証明書
さなさえる ノアイル ルガス く 延 明智をエクス ハート ぐさえ 9 。	のプライバン、大大神に十て、たち、かたう
使用する形式を選択してください。	のノフィハシーを有効にする」にフェックを八
DER encoded binary X.509 (.CER)(D)	れて「 次へ 」ボタンをクリックします。
Base 64 encoded X.509 (.CER) (§)	
○ Cryptographic Message Syntax Standard - PKCS #7 証明會 (.P7B)(_)	
□ 証明のバスにある証明書を可能であればすべて含む() ◎ Parconal Information Exchange_ BK/C5 ±10 / DEV/DB	【こんなときは!】
●「FEISONEI IIIUMINEUOLI LATIBIIGE - PALS = L4 (FFA(L)) 正明のパスにある証明書を可能であればすべて含む(U)	
□ 正しくエクスポートされたときは秘密キーを削除する(<u>K</u>)	非汗枕(ガレーアウト)で選切できわい坦
□ すべての拡張プロパティをエクスポートする(<u>A</u>)	クドロエ(クレーノンド) (迭八てさな) 物
 Microsoft シリアル化された証明書ストア (.SST)(I) 	合は、管理者権限を持っているユーザで再
	度バックアップ手順を実施してください
次へ(N) キャンセル	

×	8.「バスリード」と「バスワードの確認」を入
← 参 証明書のエクスポート ウィザード	力し、「 次へ 」ボタンをクリックします。
セキュリティ セキュリティを維持するために、セキュリティブリンシバルで秘密キーを保護するかパスワードを使用しなけれ ビキュリティング	
はなりません。 」グループまたはユーザー名 (推奨)(G)	
:是70(点)	
的除(图)	
✓ J(32-F(P):	
/ ハリートの確認(L): ●●●●●	
镭号化: TripleDES-SHA1 ~	
次へ(<u>U)</u> 年ャンセル	
	0. 「 会昭 」ボタンを力計ッカーで、証明書をバ
× ← <i>影</i> 証明者のエクスポート ウィザード	3. 「今駅」 かクマ をクリック して、 証明書をハ
7074-1427-14	ックアップするフォルダを選択し、「次へ」をク
エクスポートするファイルの名前を入力してください	リックします。
ファイル名():	
Ci¥Users¥paku¥Desktop¥更新後の証明書.pfx	
<u> 次へ(b)</u> キャンセル	
×	10.「 完了 」 ボタンをクリックします。 「正しく
← 🦻 証明書のエクスポート ウィザード	エクスポートされました。」が表示され、「OK」
ないゆみてわつぎ しん ぼ じんゆつ	た カ 川 、 カ 」 ナ 十
証明書のエジスホートウイリートの売」	<i>と</i> クリックします。
証明書のエクスポートウィザードが正常に完了しました。	
次の設定が指定されました	
クティル名 CANsersy キーのエクスポート はい	
組織のバスにあるタインの組み合と言うです。 ファイルの形式 Personal Informatic	
< >>	
売了(E) キャンセル	
証明書のエクスポート ウィザード ×	
正しくエクスポートされました。	
ОК	

2.2.	更新申請画面からの更新	
2.2.	大利11-16日回10-000天初	

		- a ×		
ିତ୍ର ଶା ଜନ୍ମନମ୍ଭ × 🗖	- £ 0] (em	_e+]©☆⊕ <mark>@</mark>		見新対象の証明書かインストールされた端
🕽 msn	R	urses @	末から	っ更新申請画面へアクセスします。
HDC/ayr UCAban Weeder/s American	R Const	+	https	s://cert.obn.managedpki.ne.jp/p/ru
認証用の証明書の選択		×	2.更	夏新対象の証明書を選択し、「 OK 」をクリ
サイト cert.obn.managedpki.ne.jp では資格情報	が必要です:		ックし	、ます。
011T123456			Ж Г0n	nline Billing NW Common Root CA 」と表
Tonine Billing NW Common Root (2020/9/3	ок <i>‡</i> ту	tu	ĒC ≧ ∦ ι	していることを推認
Cybertrust Manage	ed PKI		3.「≢	証明書更新申請」をクリックします。
証明書の更新 サイバー 証明書更新申請 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	・トラストマネ	ベージドP		
更新後証明書の取得サイバートラ	ラスト マネージドPKI	の証明書の		
	う いの証明書の更新申請を送信	します。		

鍵更	新申請情報の確認	4.「Submit」をクリックします。
以下の内容で証明書更 よろしければ「Submi	新申請を送信します。 t」ボタンをクリックしてください。	
Common Name Organizational Unit Organizational Unit Organization Country	0110119153 medical hokkaido ReceiptOnline JP	
通知用メールアドレス 中請用データ	Test@cybertrust.co.jp	
	Submit	
	送信完了	5.証明書ステータスが「発行済み」となれば証 明書が発行されます。
申請 証明書の	情報を受け付けました。 発行申請はこれで完了です。	証明書ステータスは、「 鍵生成中」→「発行要求 中」→「発行済み」と遷移します。
	申請の受付情報	
リクエストID	202012140100076	
リファレンス ID	zigLUVC29Q	
証明書ステータス 発行済み		
受け付けた申請情報の	詳細は以下のとおりです。	
Common Name 0110119153		
Organizational Unit	medical	
Organizational Unit	hokkaido	
Organization	ReceiptOnline	
Country	JP	

鍵の取得	6 .「蠅の取得」画面に遷移後、 任息のハスワー ド半角数字4桁 を入力し、「Submit」をクリック
ダウンロードしたい鍵の発行申請時のリクエスト ID と、鍵を暗号化す るパスワードを入力してください。	します。
リクエスト ID 202012140100076 パスワード パスワードの確 認 Submit	
鍵の取得	7. Download」をクリックし、証明書を保存します。
鍵をダウンロードします。鍵のダウンロードまたはインストールを行う には、「Download」ボタンをクリックしてください。	
Download	
8. 証明書のインストールは、「1.2 証明書のイ	ンストール」を参照ください。
	水口17人 ノ ユ ^ヘ ・シュ 、

9. 「4. 証明書の削除」を参照し、古い証明書を削除ください。

2.2.1 こんなときは!

証明書または鍵の更新作業中に、ネットワークやシステム等の障害で証明書または鍵の取 得に失敗した場合は、再度証明書または鍵を取得してください。

	更新申請情報	の一覧		
1 件	中1-1件目を表え	示しています	•	
リクエスト ID Common Nam 202012140100076 0110119153	e 証明書更新申請日時 2020.12.14 17:39:00 202	有効期限 24.03.14 17:39:0	ステータス 7 発行済み	取得 Download key
Previous 20			Next 20)

Cybertrust Managed PKI الجوبا		トップへ ログアウト
日明時度の更新 証明度更新申請 更新(注証明度の取得	サイバートラスト マネージドPKI サイバートラストマネージドPKIの証明書の更新面面です。 証明書更新中語 現在お使いの証明書の更新申請考述信します。 更新後証明書の取得 更新した証明書を取得します。	cvbertrust
		-

1. 更新申請画面の「**更新後証明書の取得**」をク リックします。

○一覧に情報が表示されている場合は、対象の 更新済み証明書の「Download Key」ボタンをク リックして証明書を取得してください。

・一覧に情報が表示されていない場合は、更新 申請が完了していませんので、「2.2. 更新申請 画面からの更新」からやり直してください。

3. 証明書の失効



4. 証明書の削除

0- 648	<u>。</u> 1. Internet Explore を起動し、画面右上の
印刷(P) > ファイル(F) > 拡大(Z) (90%) > セーフティ(S) > Microsoft Edge で開く(E) Ctrl+Shift+E サイトをアブリビューに追加(I) ダウンロードの表示(N) グウンロードの表示(N) Ctrl+J アドオンの管理(M) F12 開発者ツール(L) ビン留めサイト(G) 互換表示設定(B) インターネット オブション(O) パージョン情報(A)	「⑩」ボタンから「 インターネットオプション 」 をクリックします。
インターネット オブション ? × 全般 セキュリティ ブライバシー コンテンツ 接続 ブログラム 詳細設定 証明書	2.「 コンテンツ 」タブを選択し、「 証明書 」をク リックします。
 証明書 目的(N): <すべて> 個人 体間証明機関 信頼されたルート証明機関 信頼された発行元 信頼されない発行元 発行先 発行者 有効期限 フレンドリ名 2024/03/10 cn=1619931494, 2033/01/31 cn=161931494, 2033/01/31 cn=161931494001 20000000000000000000000000000000000	 4.「個人」タブを開き、有効期限が古い証明書 を選択し、「削除」をクリックします。 ※発行者が「Online Billing NW Common Root CA」が含まれる表記となっていることを確認し ます。
	<u>'</u>

証明書 × ・ 証明書を使って暗号化データの暗号化を解除できません。証明書を削除し ますか? はい(Y) いいえ(N)	5.「 はい 」をクリックします。
証明書 ×	6. 削除を行った証明書が一覧から削除されて
目的(N): <すべて> ~	いることを確認し、「 閉じる 」をクリックします。
④人 ほかの人 中間証明機関 信頼されたルート証明機関 信頼された発行元 信頼されない発行元 発行先 発行者 有効期限 フレンドリ名 よびに the two provided in the two p	

5. サポート情報

5.1. MPKI クライアント利用環境

対応 0S				
		32bit	64bit	
	Windows 8.1	0	0	
	Windows 10	0	0	
				_
依存するソフトウェア	MPKI クライアントを利用するためには、ご			
	使用の PC に「Micr	icrosoft .NET Framework		
	3.5」以上がインスト	、ールされ [、]	ている必要	そが
	あります。			
表示言語	日本語のみ			
サポートする Proxy 認証の種類	MPKI クライアント	がサポート	、する Pro	оху
	認証の種類は、以下のとおりです。			
	・Basic 認証			
	・NTLM 認証			

5.2. ご利用にあたっての注意事項

5.2.1 MPKI クライアントインストール時の注意事項

闄 Cybertrust Managed PKI Client ×	左記のエラー画面が表示された場合は、「終了」
値 をキー た書き込めません。その キーへの十分なアクセスがあることを確認するか、またはサポート担当者に問い合 わせてください。	をクリックし、再度インストールを実施くださ
	<i>ل</i> ،
終了(X) 再試行(T) 統行(O)	

5.2.2 セッション無効時の対応トラブルシューティング

セッション無効	画面上の操作状態で一定時間作業を行わない場
	合は、セッションが無効であることを示す画面
セッションがタイムアウトしました。 最初のページに戻ってください。	が表示されます。このような状態では引き続き
Standovi (an Paulifier Groupskaatoden	作業ができないため、右上の「×」をクリック
	し、ブラウザを閉じた後再度ブラウザからユー
	ザー用 URL ヘアクセスし直してください。