群馬県立学校 ICT 環境整備業務

BYOD 接続手順

macOS

ネットワンシステムズ株式会社
東日本第 1 事業本部
第 1 営業部

令和 3 年 2 月 25 日

目次

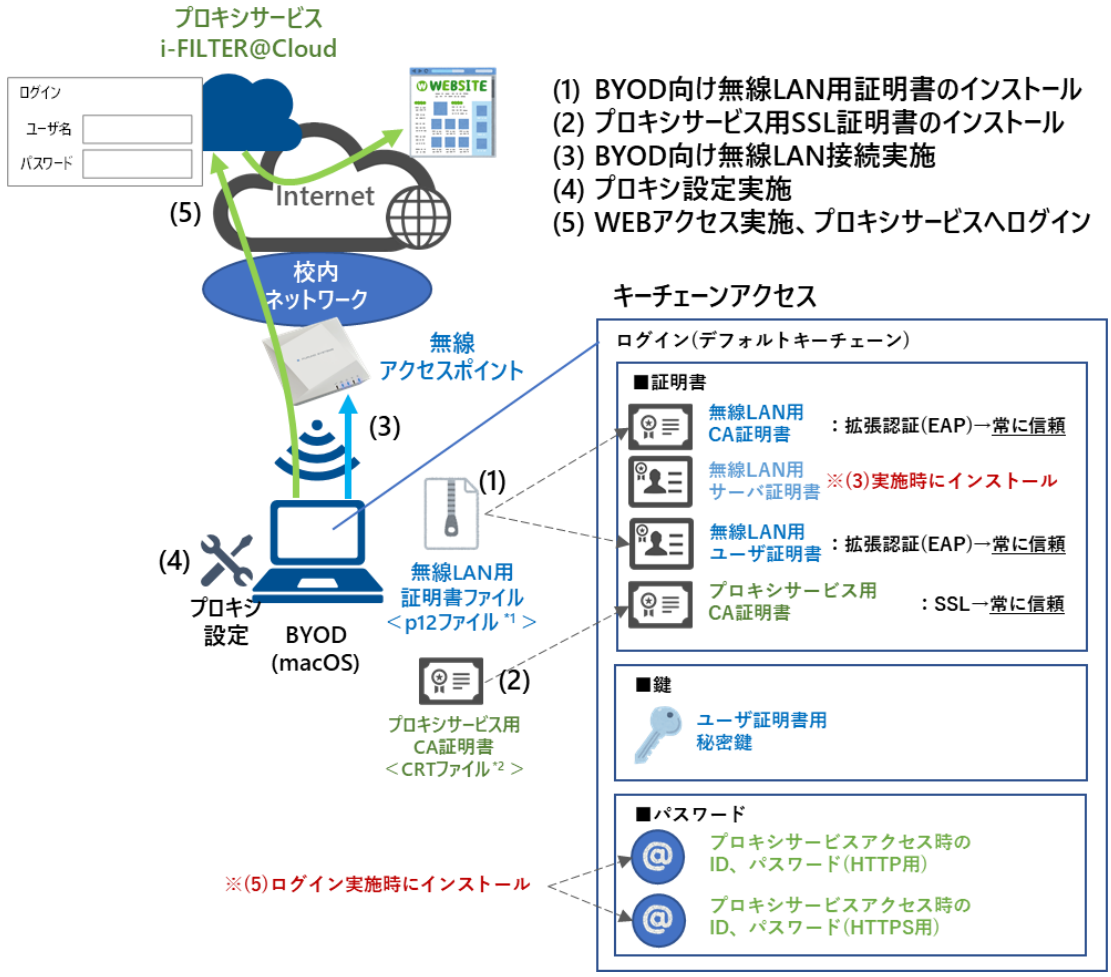
1. はじめに

1.1. 本書の目的

本書は、macOS の持ち込み端末(BYOD)における学校利用に必要な接続手順を記載します。

2. 接続手順

BYOD 接続時の手順について説明します。接続手順のイメージは下図の通りとなります。



*1 p12 ファイルとは、パスワードに基づく鍵(暗号)により保護された秘密鍵と、それに関連する公開鍵証明書を保管するために一般に利用されるファイルです。今回のファイルには、無線 LAN 用のユーザ証明書、秘密鍵および、CA 証明書が含まれます。

*2 CRT ファイルとは、証明書ファイル形式の一つです。

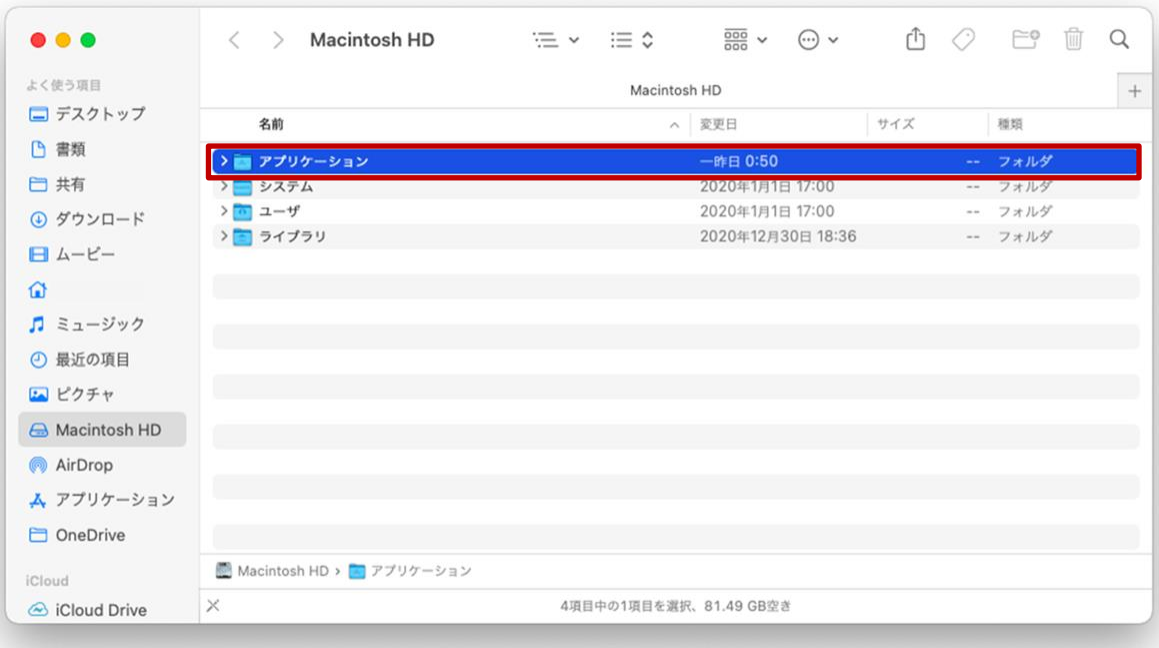
※BYOD 利用申請後に、『BYOD パスワード通知書』、『無線 LAN 用証明書ファイル』、『プロキシサービス用 SSL 証明書（CA 証明書）ファイル』が用意されます。
学校の担当の先生よりメール等で配布された『無線 LAN 用の証明書ファイル』（2.1. BYOD 向け無線 LAN 用証明書のインストール）、『プロキシサービス用 SSL 証明書（CA 証明書）ファイル』（2.2. プロキシサービス用 SSL 証明書のインストール）はインストールのために BYOD 上に移してください。

2.1. BYOD 向け無線 LAN 用証明書のインストール

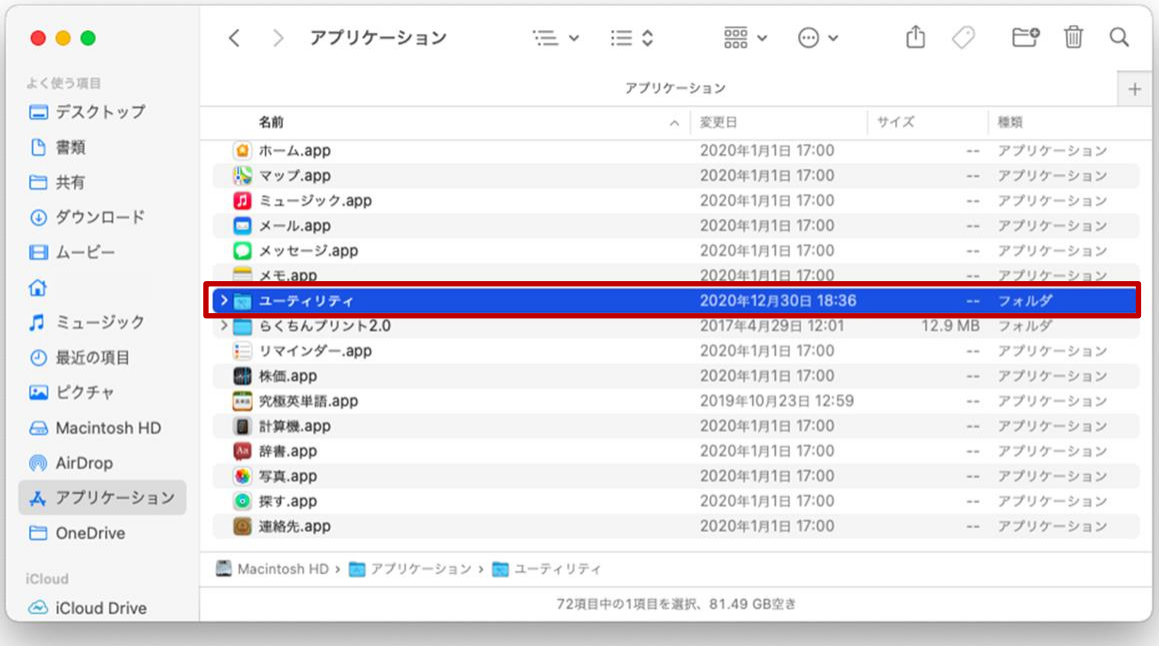
ここでは、BYOD 向け無線 LAN 用証明書のインストール手順を説明します。

(1) デスクトップにある「Macintosh HD」のアイコンをクリックして「キーチェーンアクセス」を起動します。

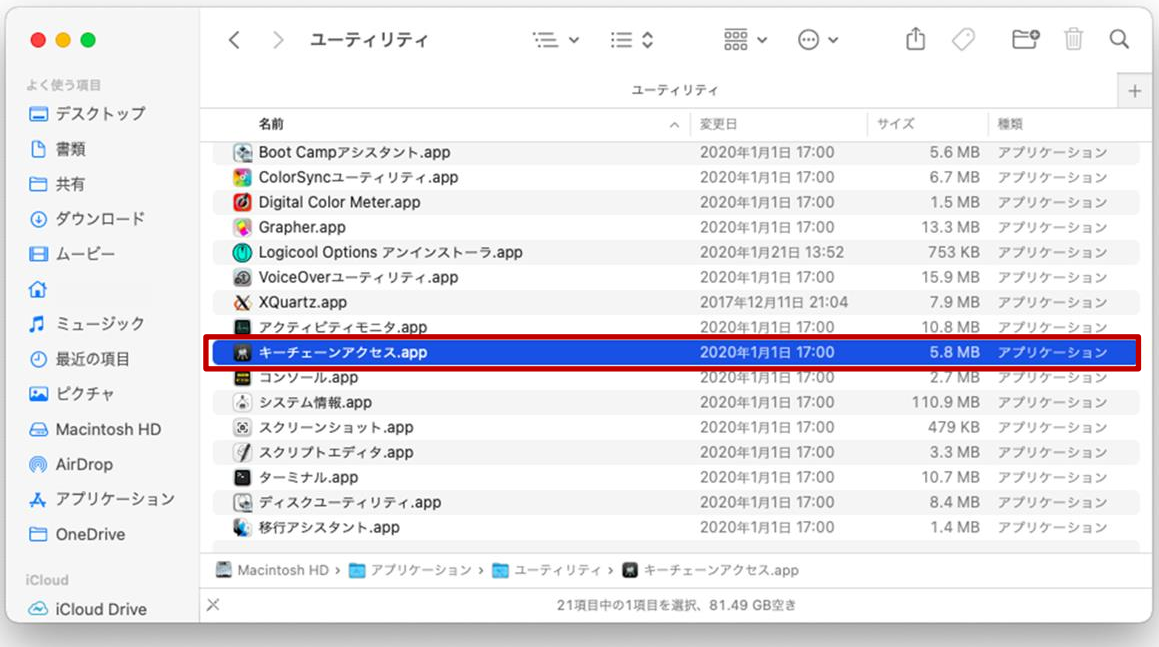
(2) “Macintosh HD”画面が表示されたら「アプリケーション」をクリックします。



(3) “アプリケーション”画面が表示されたら「ユーティリティ」をクリックします。

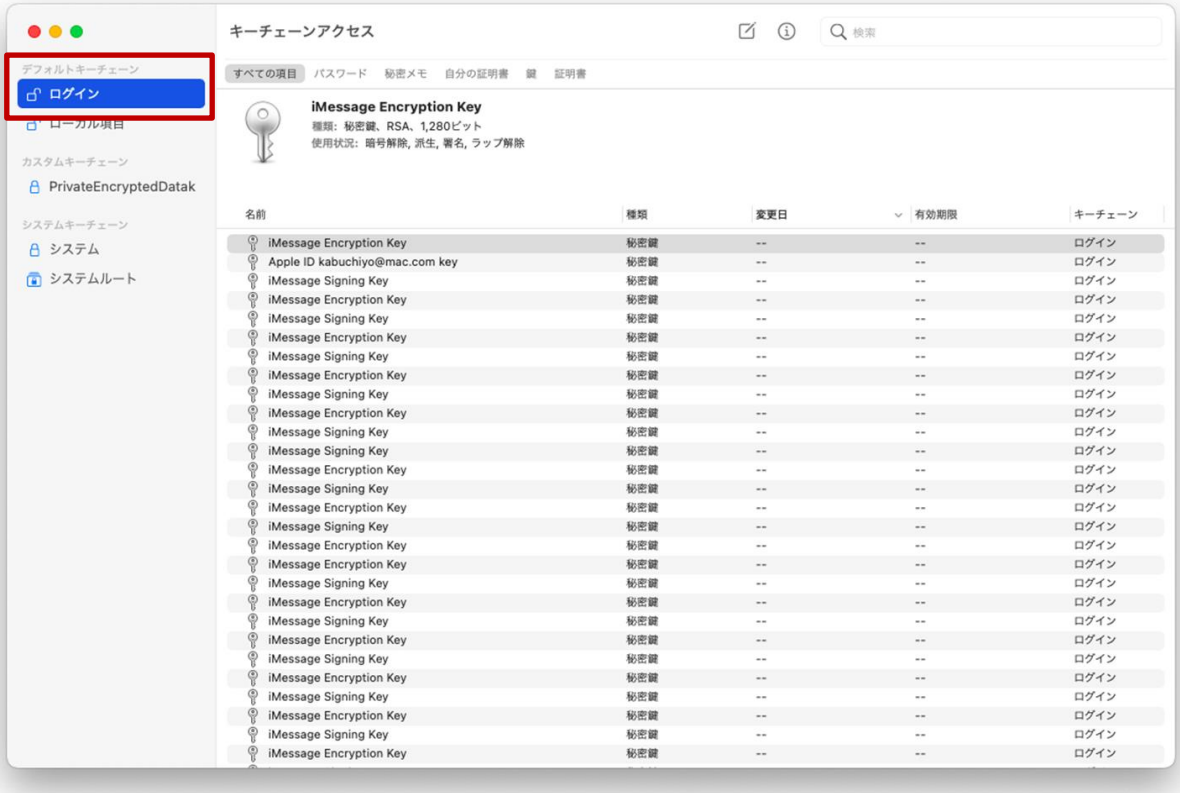


(4) “ユーティリティ”画面が表示されたら「キーチェーンアクセス.app」をダブルクリックします。

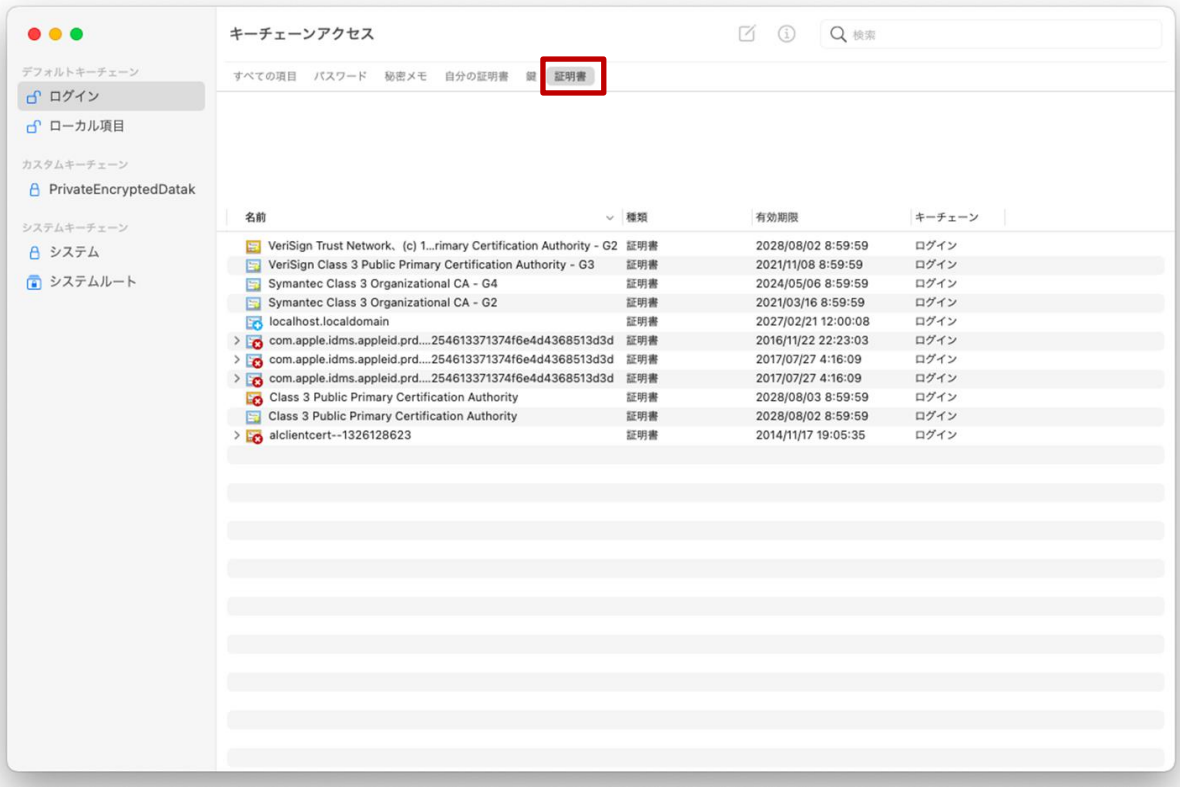


(5) “キーチェーンアクセス”画面が表示されたら、左上にあるデフォルトキーチェーンの「ログイン」をクリックして、デフォルトキーチェーンの一覧を表示します。

※「デフォルトキーチェーン」の「ログイン」画面以外は使用しないでください！



(6) キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の上段にある「証明書」タブをクリックして、証明書一覧を表示します。

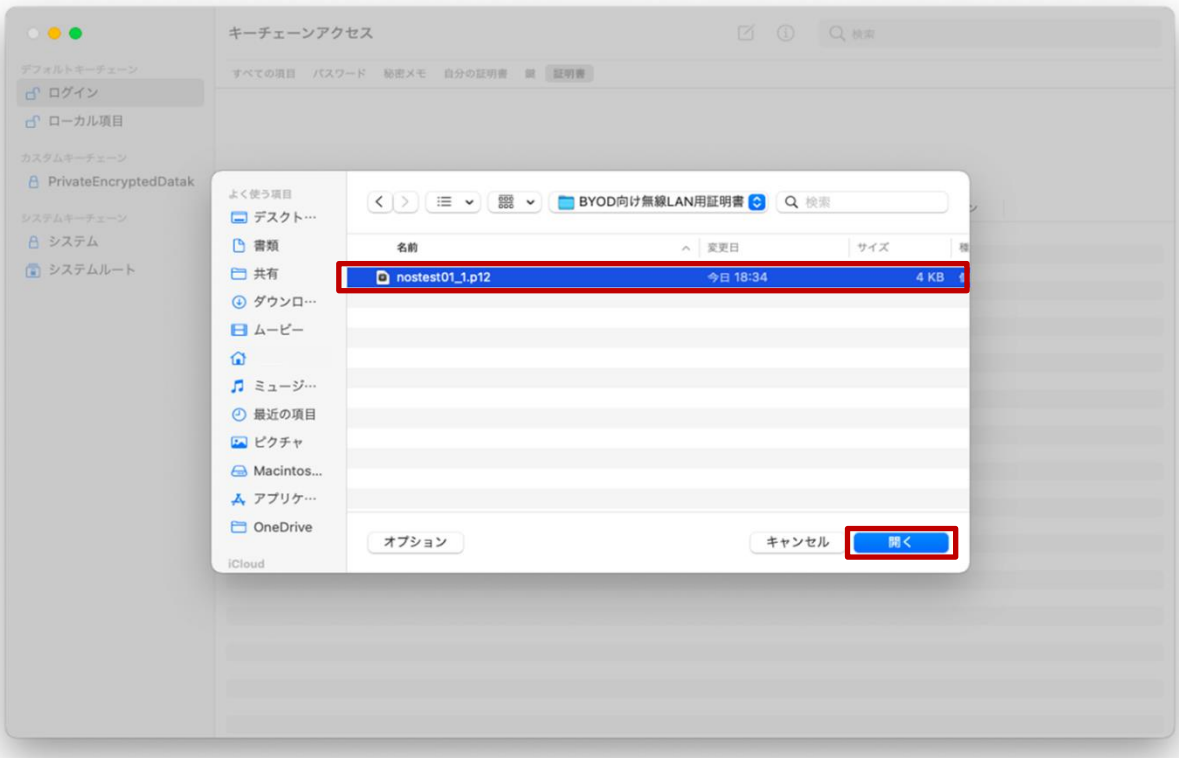


(7) 画面上にあるメニューバーの「ファイル」をクリックして「読み込む・・・」を選択します。

(8) ポップアップが表示されたら、インポートする BYOD 向け無線 LAN 用証明書のファイルを選択し「開く」をクリックします。

BYOD 向け無線 LAN 用証明書のファイル名は「<ログイン ID>_1.p12」となります。

※この手順書では BYOD 向け無線 LAN 用証明書のファイル名は「nostest01_1.p12」で記述しております。

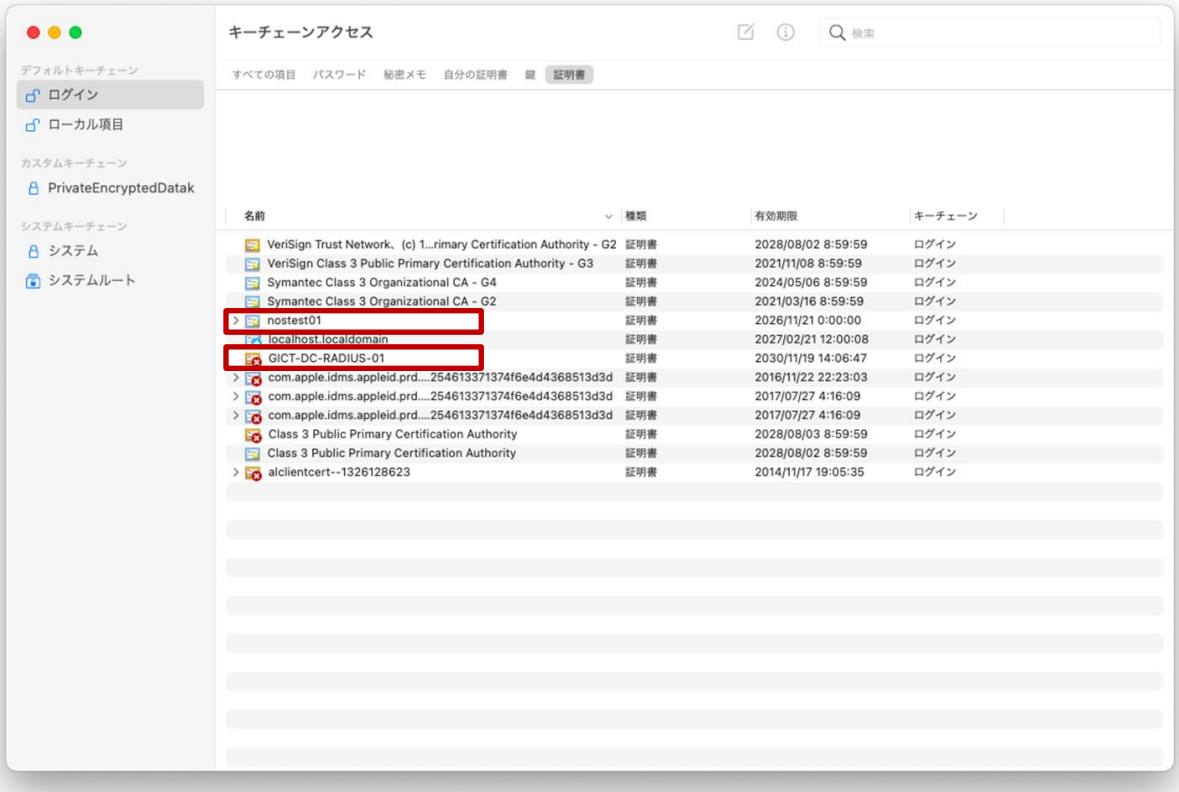


(9) パスワードを入力する画面が表示されるので、『BYOD パスワード通知書』に記載されている「証明書設定用パスワード」を入力します。入力が完了したら「パスワードの表示」にチェックを入れて、パスワードが正しく入力されていることを確認し「OK」をクリックします。

(10) キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の証明書一覧に、BYOD 向け無線 LAN 用ユーザ証明書「<アカウント名>」と CA 証明書「GICT-DC-RADIUS-01　※アイコン黄色枠」が追加されます。

※この手順書では BYOD 向け無線 LAN 用ユーザ証明書は「nostest01」で記述しております。

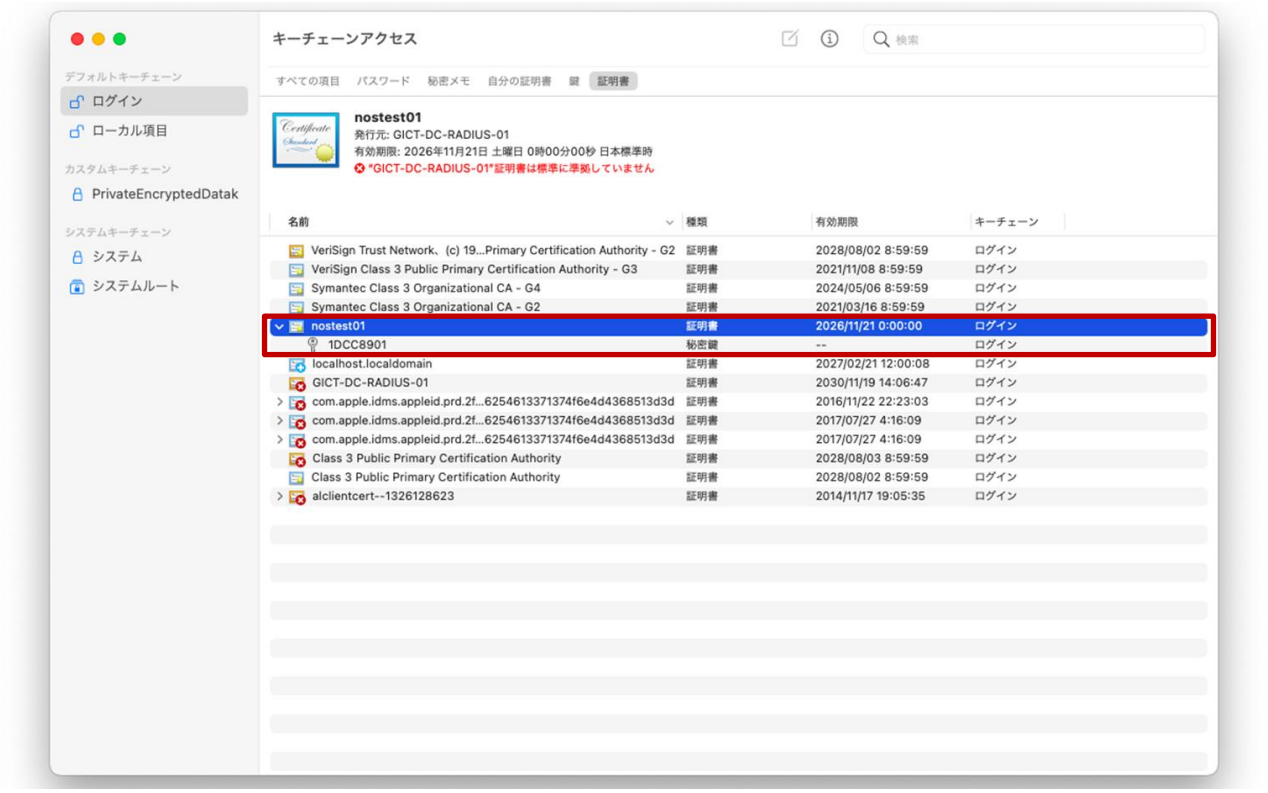
※「GICT-DC-RADIUS-01」は、(8)(9)の手順を実行すると自動で登録(インストール)されます。



(11) 次にユーザ証明書の秘密鍵の確認と、拡張認証を信頼済みに設定します。

証明書一覧の中のユーザ証明書の左側にある［>］をクリックして「秘密鍵」が入っていることを確認します。※秘密鍵の名前は任意の文字列となります。

次にユーザ証明書の拡張認証を設定します。証明書一覧の中のユーザ証明書をダブルクリックします。

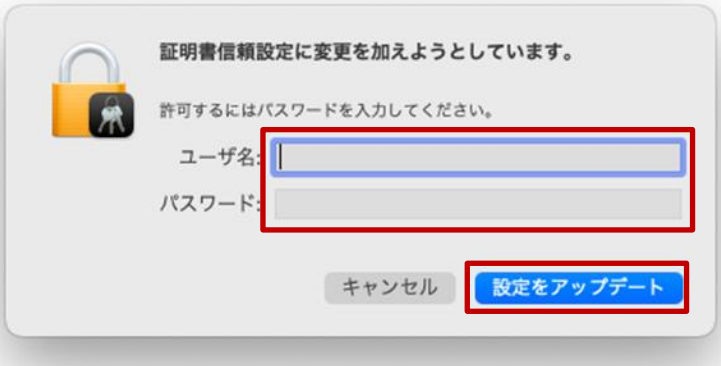


(12) ユーザ証明書の設定画面が表示されたら「信頼」の左側にある［>］をクリックします。

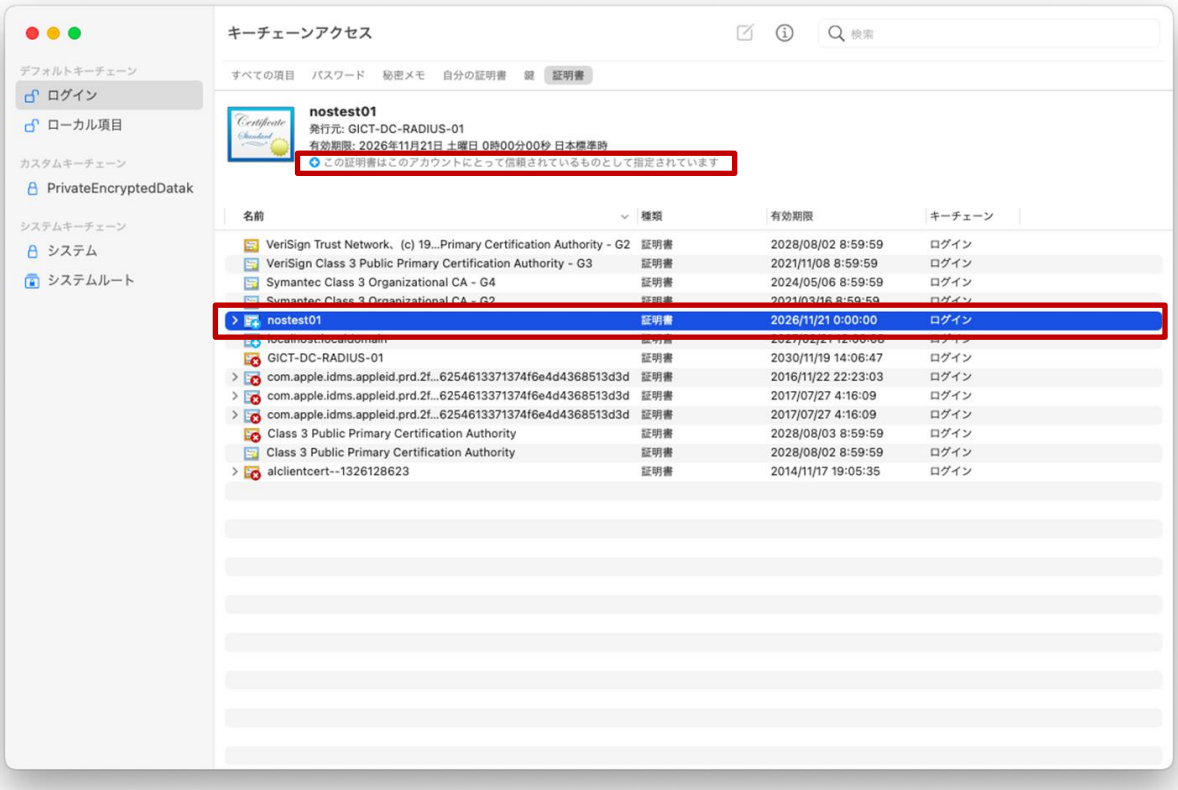
(13)信頼設定画面が表示されたら「拡張認証（EAP)」をクリックして「常に信頼」を選択します。

(14)「拡張認証（EAP)」が「常に信頼」に変更されていることを確認して、左上の「●」をクリックして画面を閉じます。

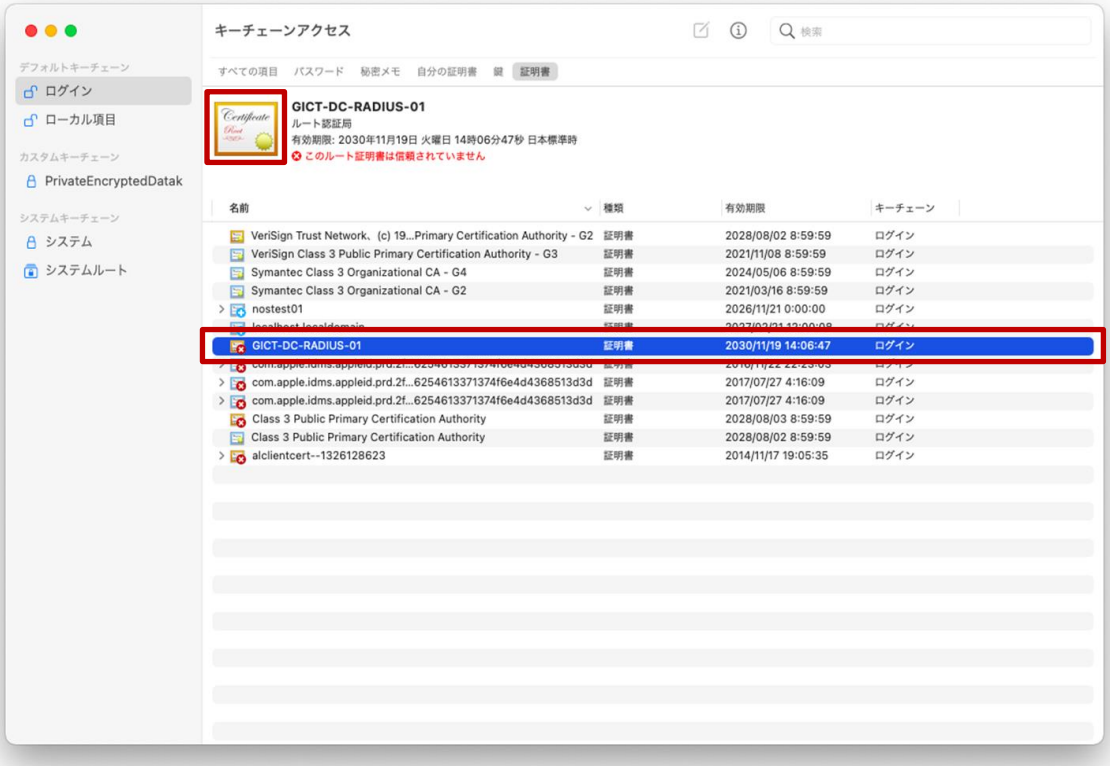
(15)「●」をクリック後に、証明書の信頼設定を変更する場合には、端末のユーザ ID とパスワードを入力する必要があるため、「ユーザ名」と「パスワード」にご自身の端末（BYOD）を起動するときに入力するログイン ID とパスワードを入力して「設定をアップデート」をクリックします。



(16) キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の証明書一覧にあるユーザ証明書「<アカウント名>」をクリックして、アイコンのコメントが「この証明書はこのアカウントにとって信頼されているものとして指定されています」に更新されていれば、設定変更は完了です。

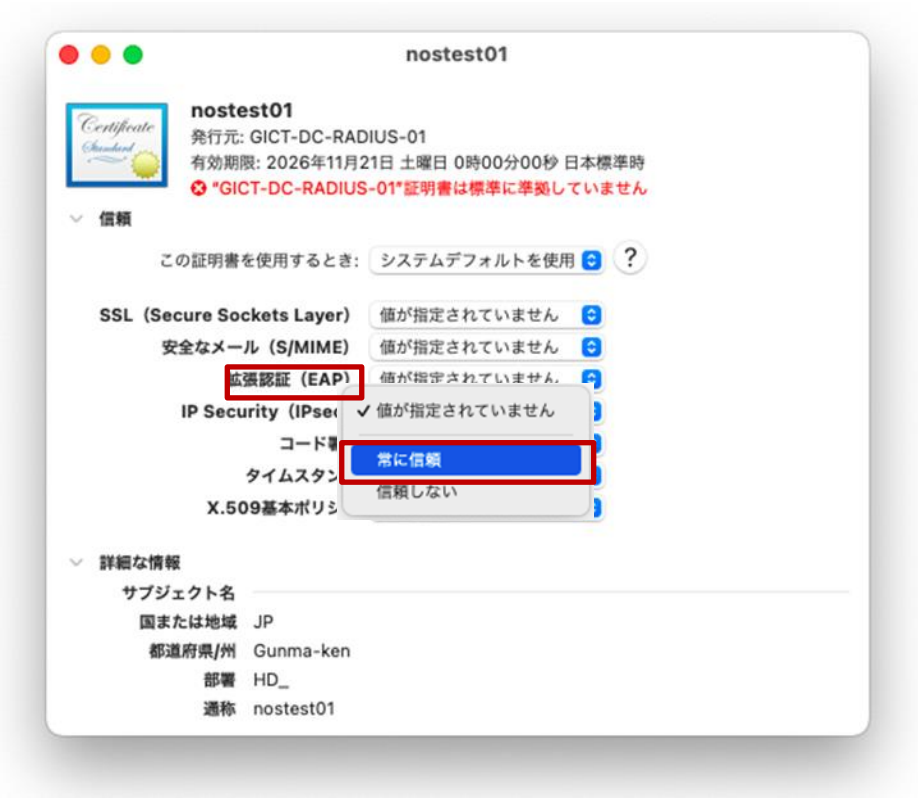


(17)次に CA 証明書「GICT-DC-RADIUS-01」の拡張認証を設定します。
キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の証明書一覧の中の CA 証明書「GICT-DC-RADIUS-01　※アイコン黄色枠」をダブルクリックします。



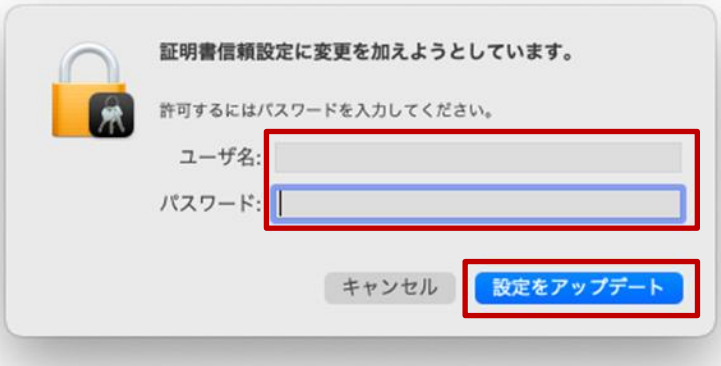
(18)CA 証明書の設定画面が表示されたら「信頼」の左側にある［>］をクリックします。

(19)信頼設定画面が表示されたら「拡張認証（EAP)」をクリックして「常に信頼」を選択します。

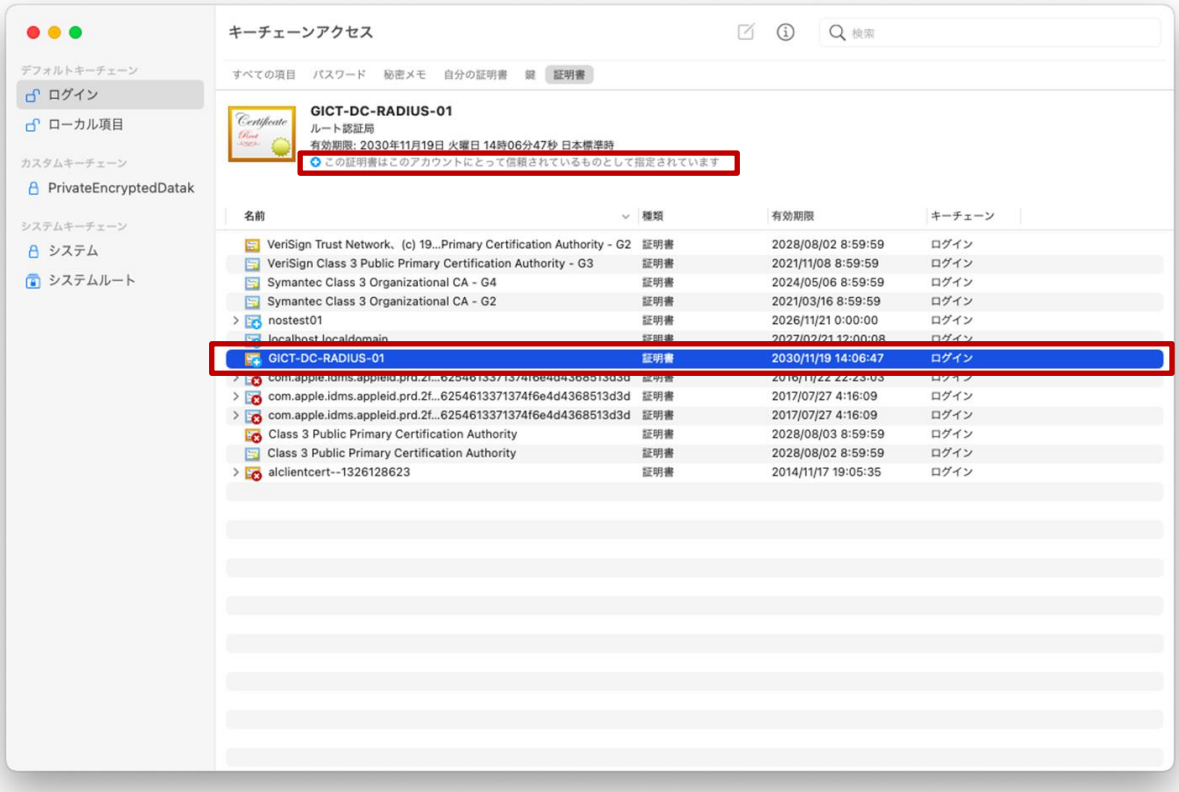


(20)「拡張認証（EAP)」が「常に信頼」に変更されていることを確認して、左上の「●」をクリックして画面を閉じます。

(21)「●」をクリック後は、下図の画面が表示されますので、「ユーザ名」と「パスワード」にご自身の端末（BYOD）を起動するときに入力するログイン ID とパスワードを入力して「設定をアップデート」をクリックします。



(22) キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の証明書一覧にある CA 証明書「GICT-DC-RADUS-01　※アイコン黄色枠」をクリックして、アイコンのコメントが「この証明書はこのアカウントにとって信頼されているものとして指定されています」に更新されていれば、設定変更は完了です。



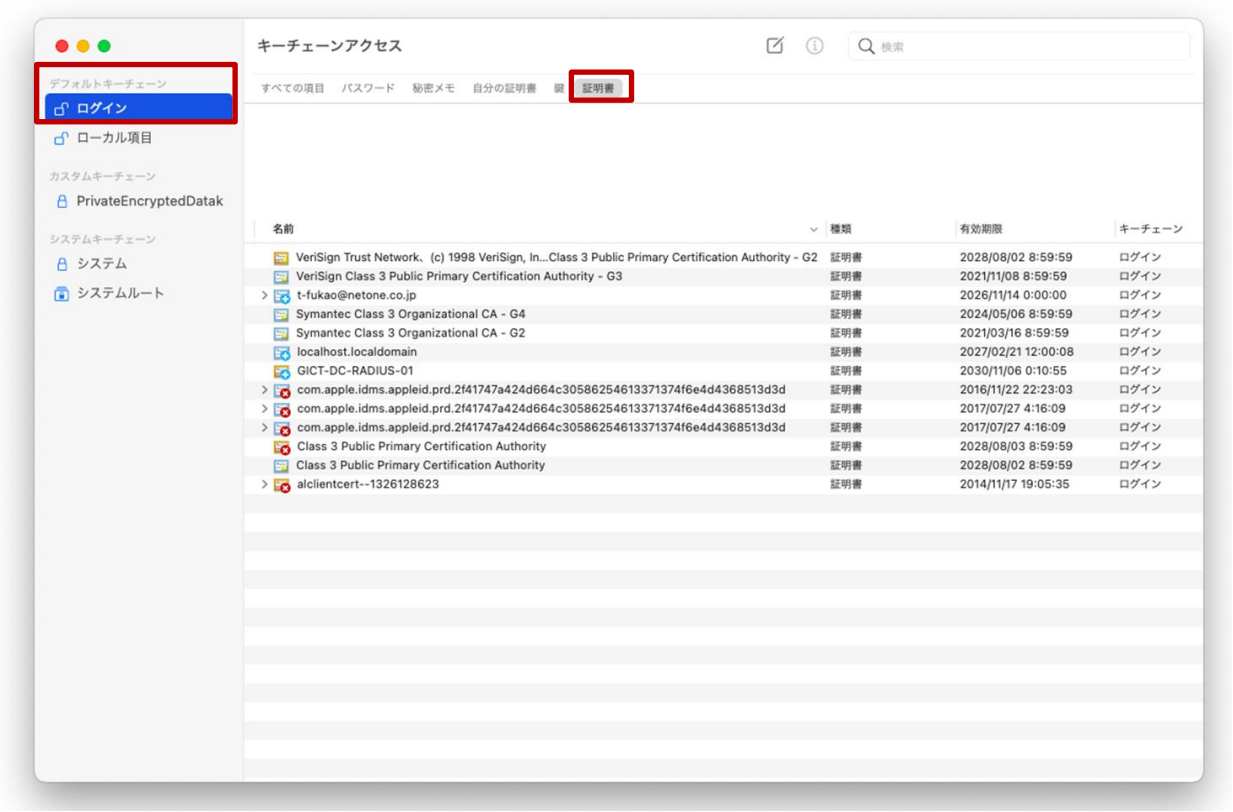
BYOD 向け無線 LAN 用証明書のインストールは以上となります。
引き続き【2.2.プロキシサービス用 SSL 証明書のインストール】を実施してください。

2.2. プロキシサービス用 SSL 証明書のインストール

ここでは、プロキシサービスである i-FILTER@Cloud 用の SSL 証明書のインストール手順を説明します。

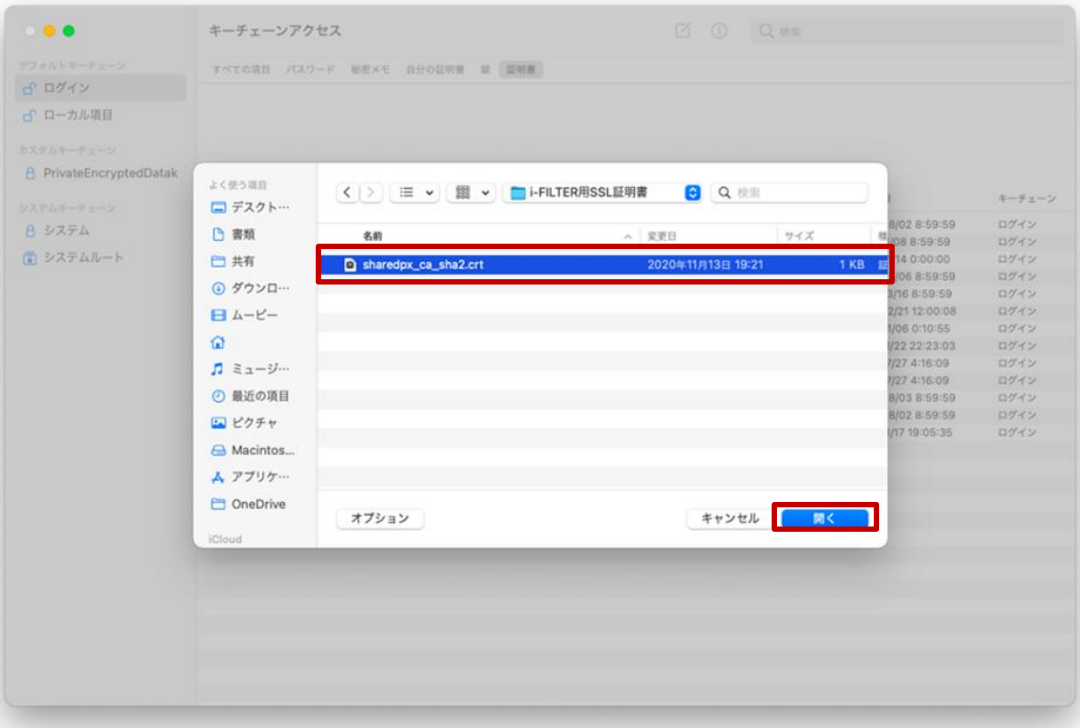
(1) “キーチェーンアクセス”画面の左上にあるデフォルトキーチェーンが「ログイン」になっていることを確認して、上段にある「証明書」タブをクリックして、証明書一覧を表示します。

※「デフォルトキーチェーン」の「ログイン」画面以外は使用しないでください！

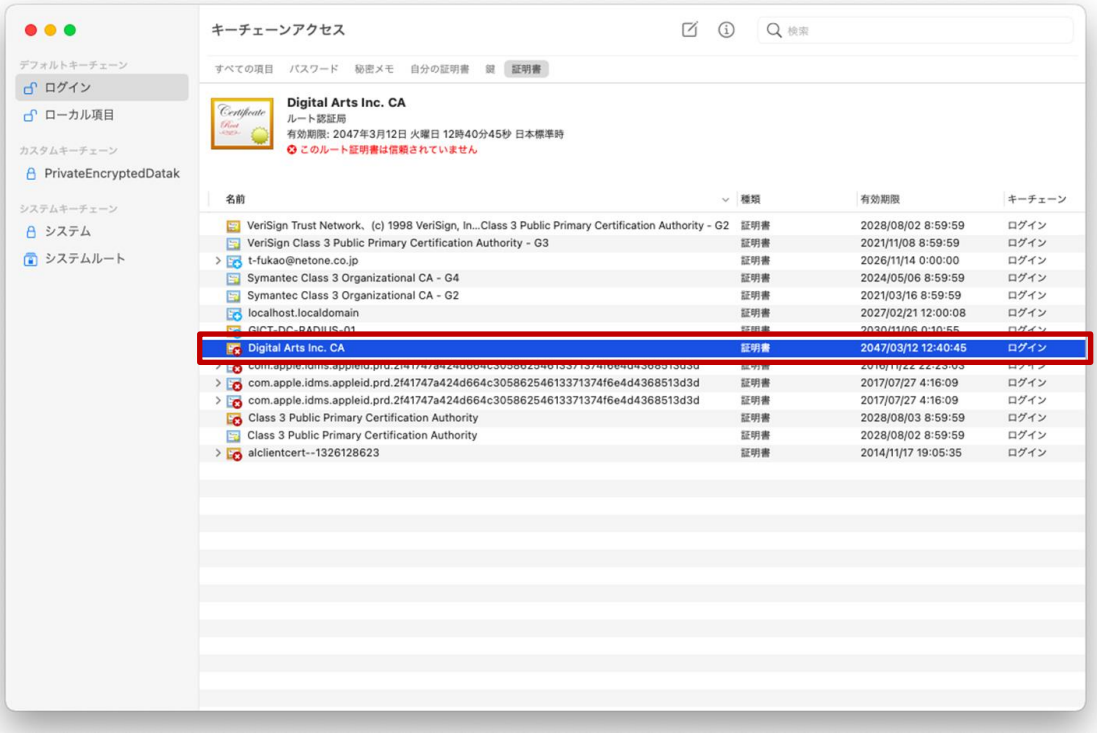


(1) 画面上にあるメニューバーの「ファイル」をクリックして「読み込む・・・」を選択します。

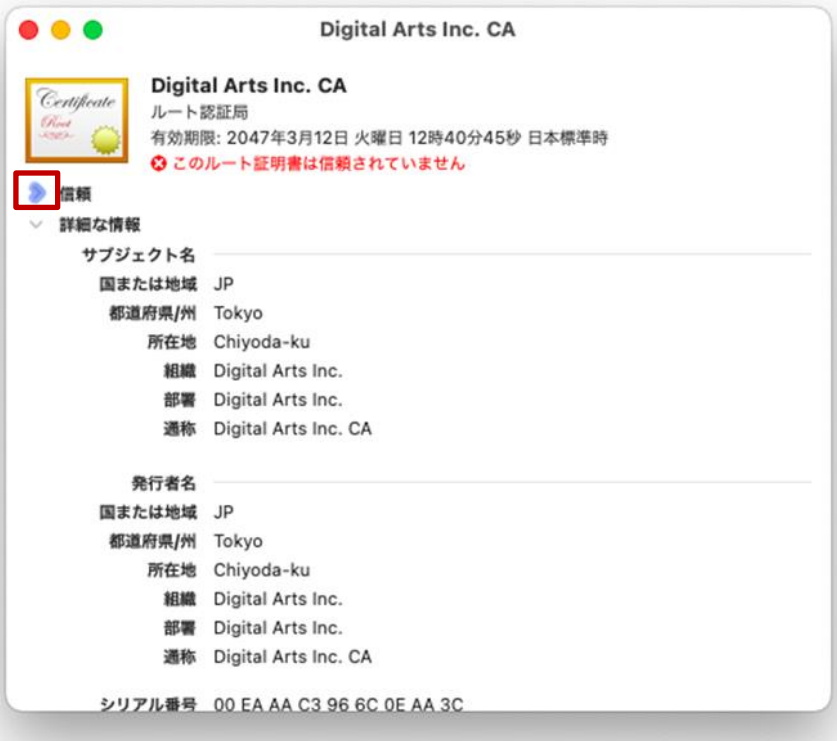
(2) ポップアップが表示されたら、インポートする i-FILTER@Cloud 用の SSL 証明書を選択し「開く」をクリックします。
i-FILTER@Cloud 用の SSL 証明書のファイル名は「sharedpx_ca_sha2.crt」となります。



(3) キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の証明書一覧に i-FILTER 用 SSL 証明書「Digital Arts Inc. CA　※アイコン黄色枠」が追加されていることを確認します。
次に i-FILTER 用 SSL 証明書の SSL 認証を設定します。証明書一覧の中の i-FILTER 用 SSL 証明書をダブルクリックします。

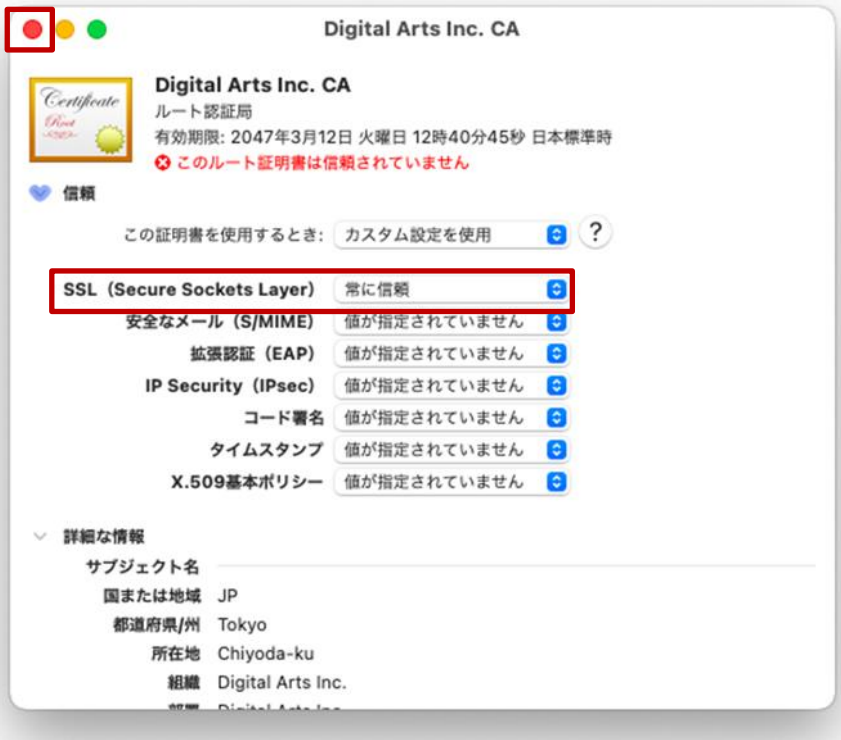


(4) i-FILTER 用 SSL 証明書の設定画面が表示されたら「信頼」の左側にある［>］をクリックします。

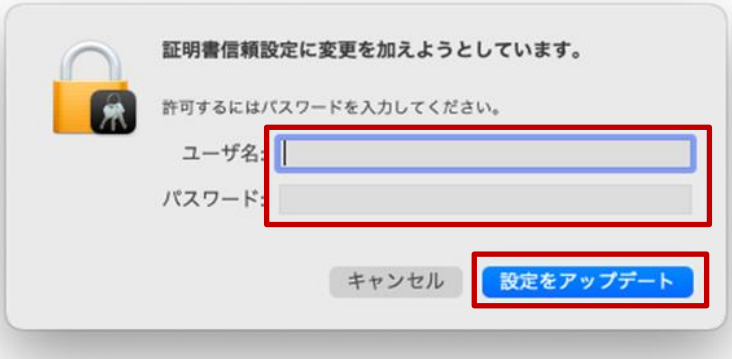


(5) 信頼設定画面が表示されたら「SSL（Secure Sockets Layer)」をクリックして「常に信頼」を選択します。

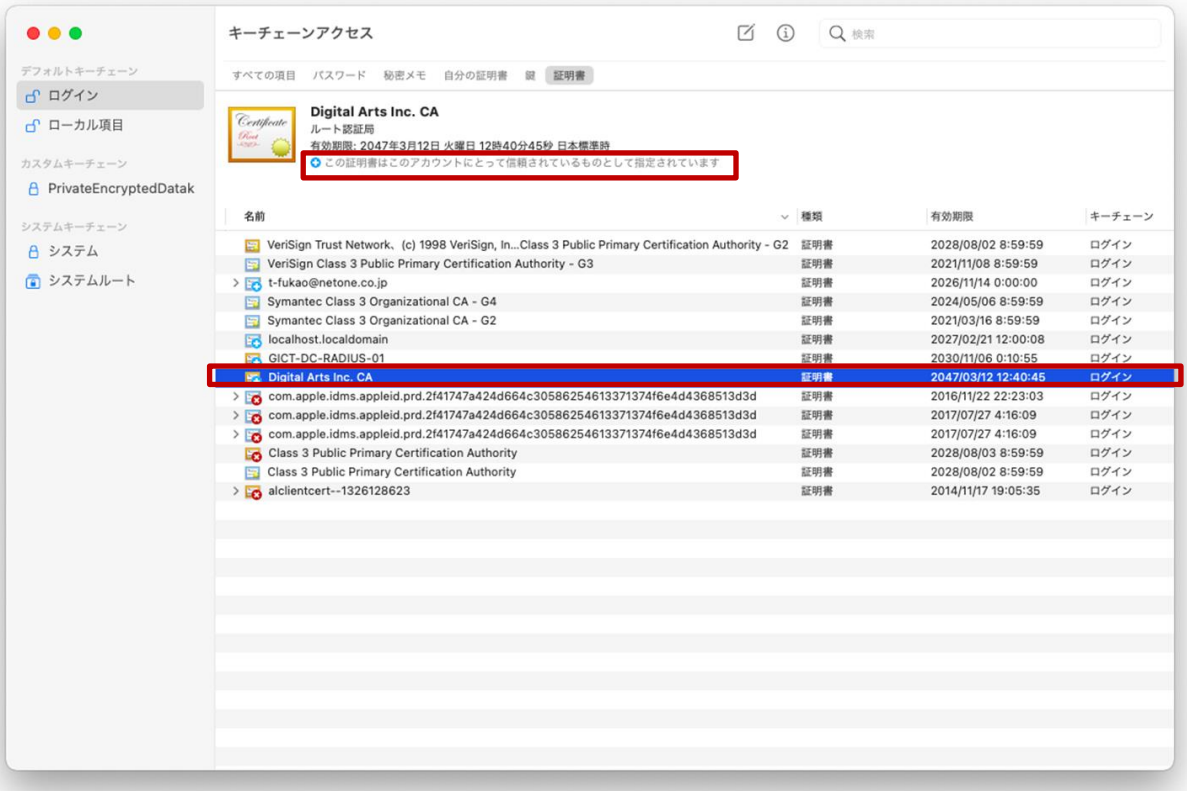
(6) 「SSL（Secure Sockets Layer)」が「常に信頼」に変更されていることを確認して、左上の「●」をクリックして画面を閉じます。



(7) 「●」をクリック後は、下図の画面が表示されますので、「ユーザ名」と「パスワード」にご自身の端末（BYOD）を起動するときに入力するログイン ID とパスワードを入力して「設定をアップデート」をクリックします。



(8) キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の証明書一覧にある i-FILTER 用 SSL 証明書「Digital Arts Inc. CA　※アイコン黄色枠」をクリックして、アイコンのコメントが「この証明書はこのアカウントにとって信頼されているものとして指定されています」に更新されていれば、設定変更は完了です。



(9) 画面上にあるメニューバーの「キーチェーンアクセス」から「キーチェーンアクセスを終了」を選択して閉じてください。

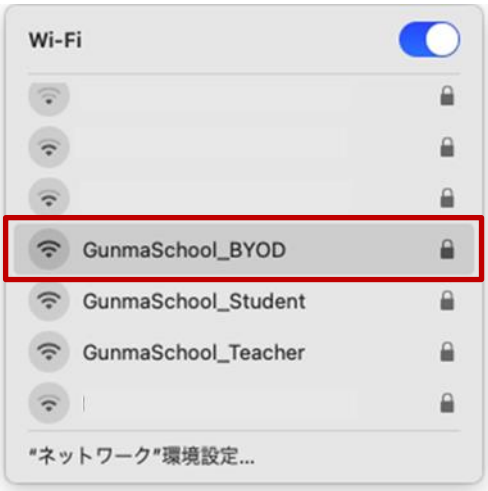
プロキシサービス用 SSL 証明書のインストールは以上となります。

2.3. BYOD 向け無線 LAN 接続実施

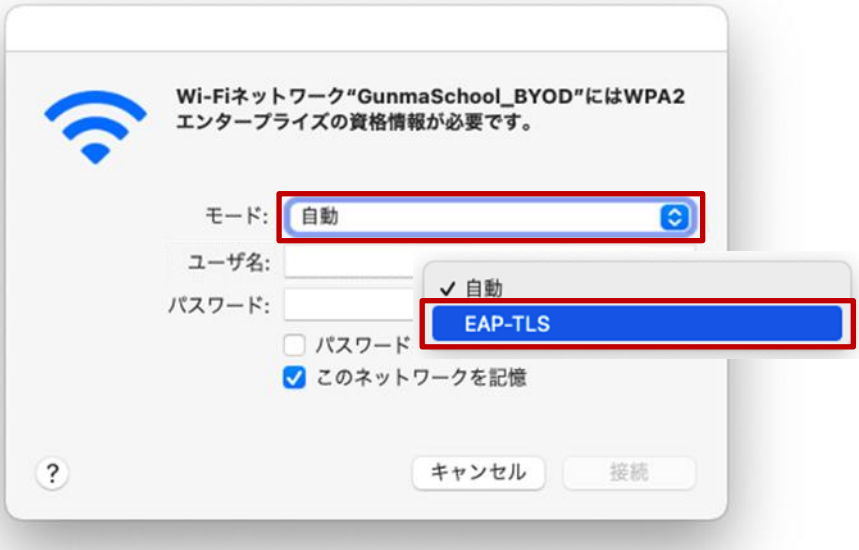
ここでは学校の無線 LAN 環境（BYOD 向け無線 LAN）へ接続する手順を説明します。

(1) デスクトップ画面にあるメニューバーの「ネットワーク」アイコン（扇状マーク）をクリックします。（未接続時の「ネットワーク」アイコンはグレーになっています）

(2) Wi-Fi 一覧が表示されたら、BYOD 向けの SSID（GunmaSchool_BYOD）を選択します。

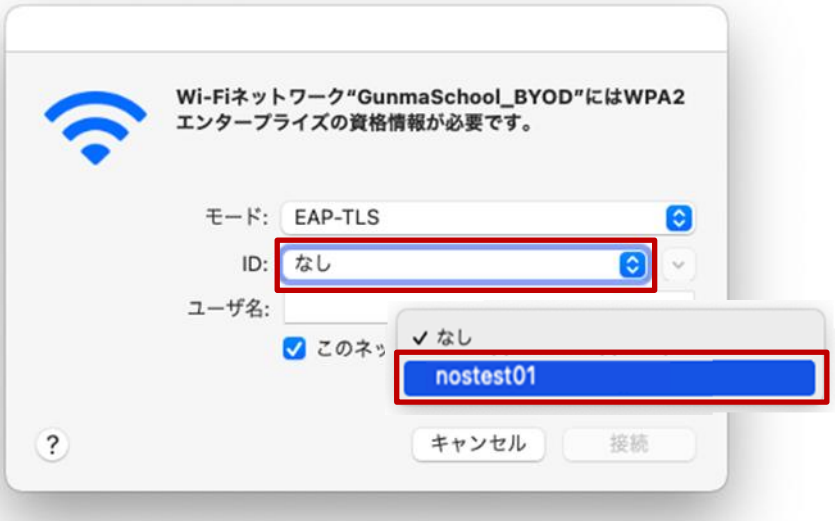


(3) Wi-Fi の設定画面が表示されたら、「モード」をクリックして「EAP-TLS」を選択します。



(4) 次に「ID」をクリックして「BYOD 用クライアント証明書（自身のログイン ID）」を選択します。

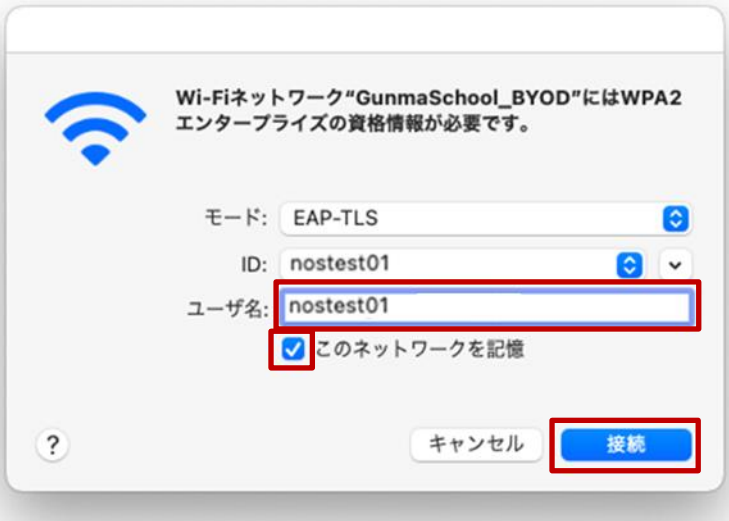
※この手順書では接続するログイン ID は「nostest01」で記述しております。



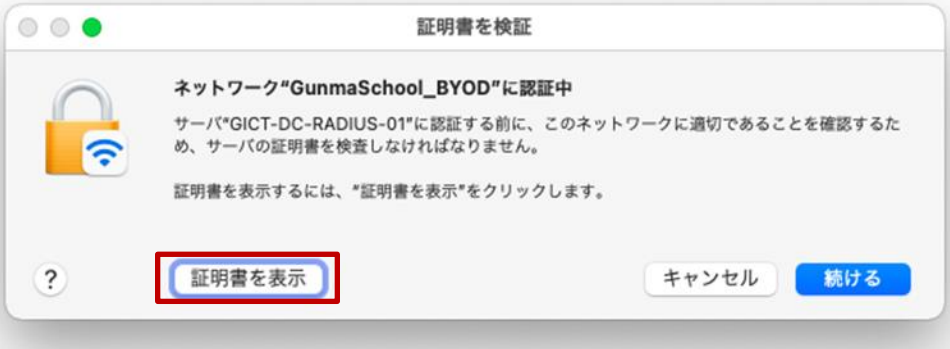
(5) 次に、「ユーザ名」を入力しますが、ここは ID と同じ文字列を入力します。

「モード」、「ID」、「ユーザ名」に誤りがないことを確認して「このネットワークを記憶」にチェックを入れて「接続」をクリックします。

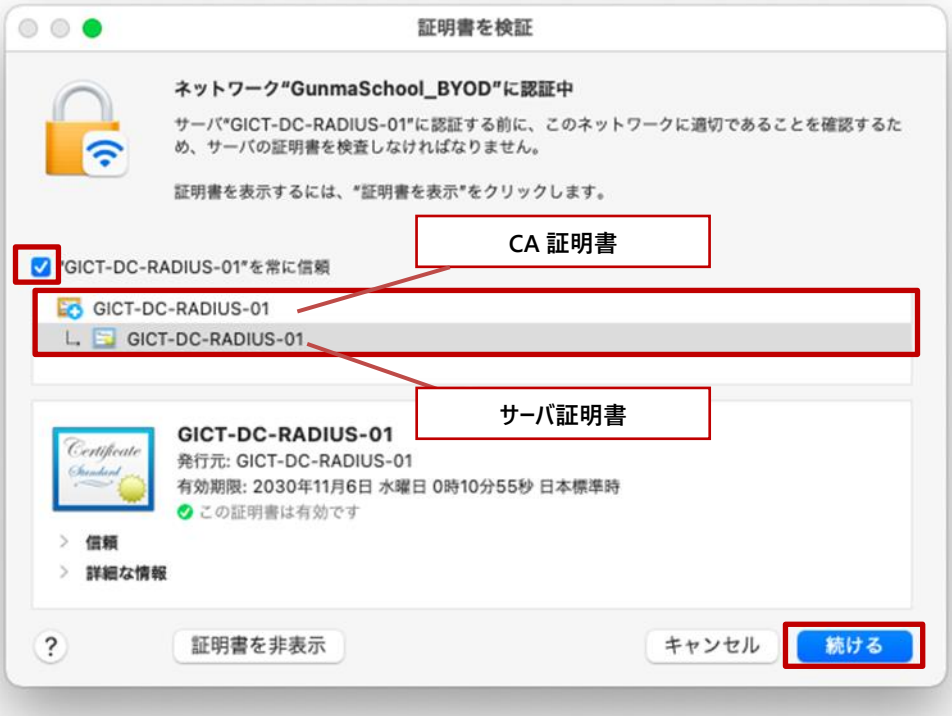
※この手順書では接続するユーザ名（自身のアカウント名）は「nostest01」で記述しております。



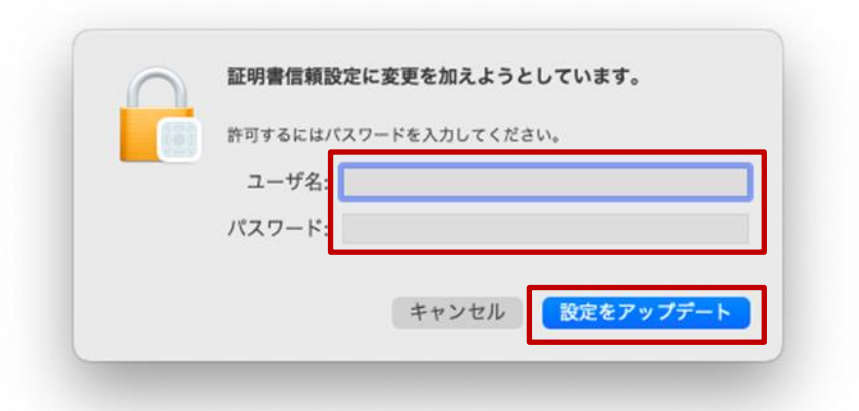
(6) 次に、無線 LAN 用サーバ証明書をインストールします。
”証明書を検証”画面が表示されたら、左下の「証明書を表示」をクリックします。
※「2.接続手順」の図にある「無線 LAN 用サーバ証明書 ※(3)実施時にインストール」手順になります。



(7) 中段にある CA 証明書「GICT-DC-RADIUS-01　※アイコン黄色枠」とサーバ証明書「GICT-DC-RADIUS-01　※アイコン青色枠」が下図のように紐づけされていることを確認します。「"GICT-DC-RADIUS-01"を常に信頼」にチェックが入っていることを確認して「続ける」をクリックします。



(8) 「●」をクリック後は、下図の画面が表示されますので、「ユーザ名」と「パスワード」にご自身の端末（BYOD）を起動するときに入力するログイン ID とパスワードを入力して「設定をアップデート」をクリックします。



(9) パスワードを入力する画面が表示されるので、「パスワード」にご自身の端末（BYOD）を起動するときに入力するパスワードを入力して「常に許可」をクリックします。

(10) 画面上にあるメニューバーの「ネットワーク」アイコン（扇状マーク）が黒色になり、優先するネットワークに「GunmaSchool_BYOD」が表示され、鍵マークがついていれば無線 LAN へ接続は完了です。

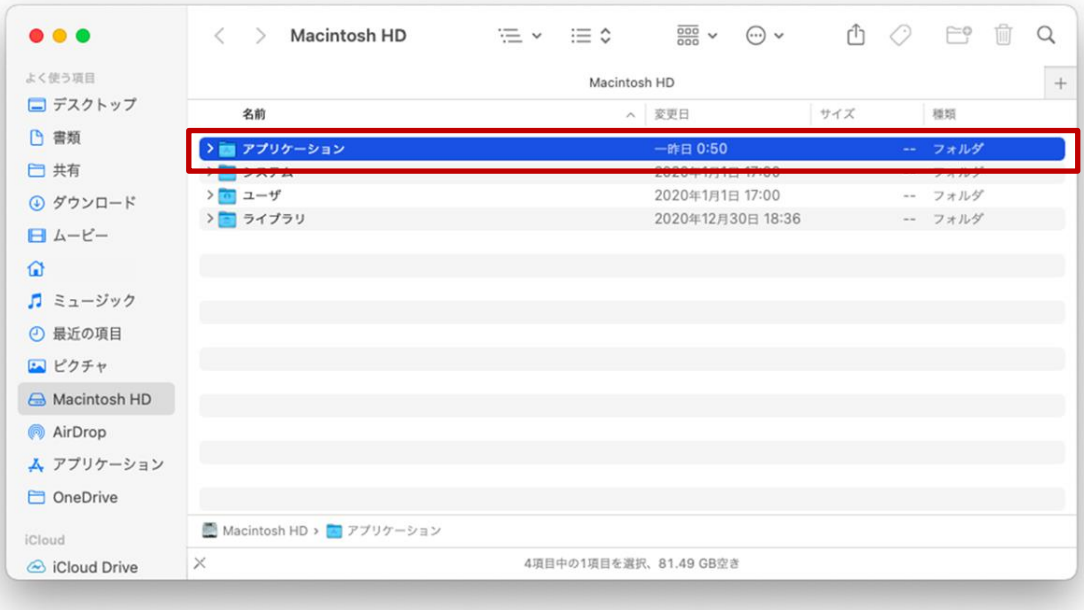
macOS における BYOD 向け無線 LAN 接続手順は以上となります。

2.4. プロキシ設定実施

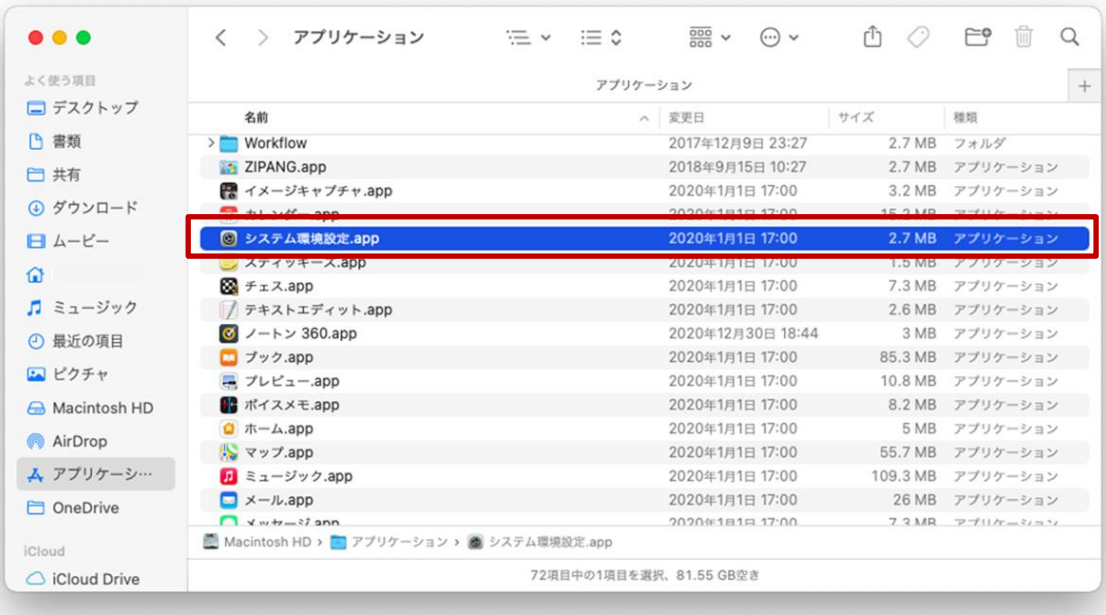
ここでは macOS のプロキシ設定の手順を説明します。学校で BYOD を利用する際はプロキシ設定の自動検出を有効にする必要があります。

(1) 「システム環境設定」を起動します。デスクトップにある「Macintosh HD」のアイコンをクリックします。

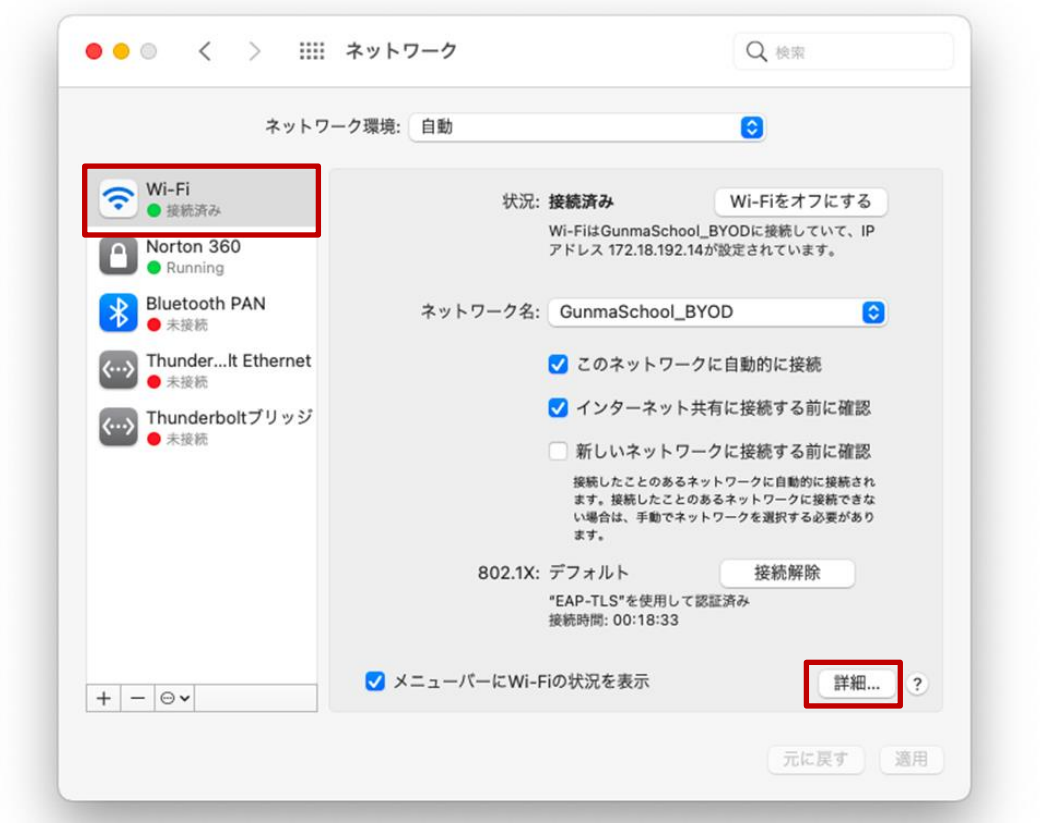
(2) “Macintosh HD”画面が表示されたら「アプリケーション」をクリックします。



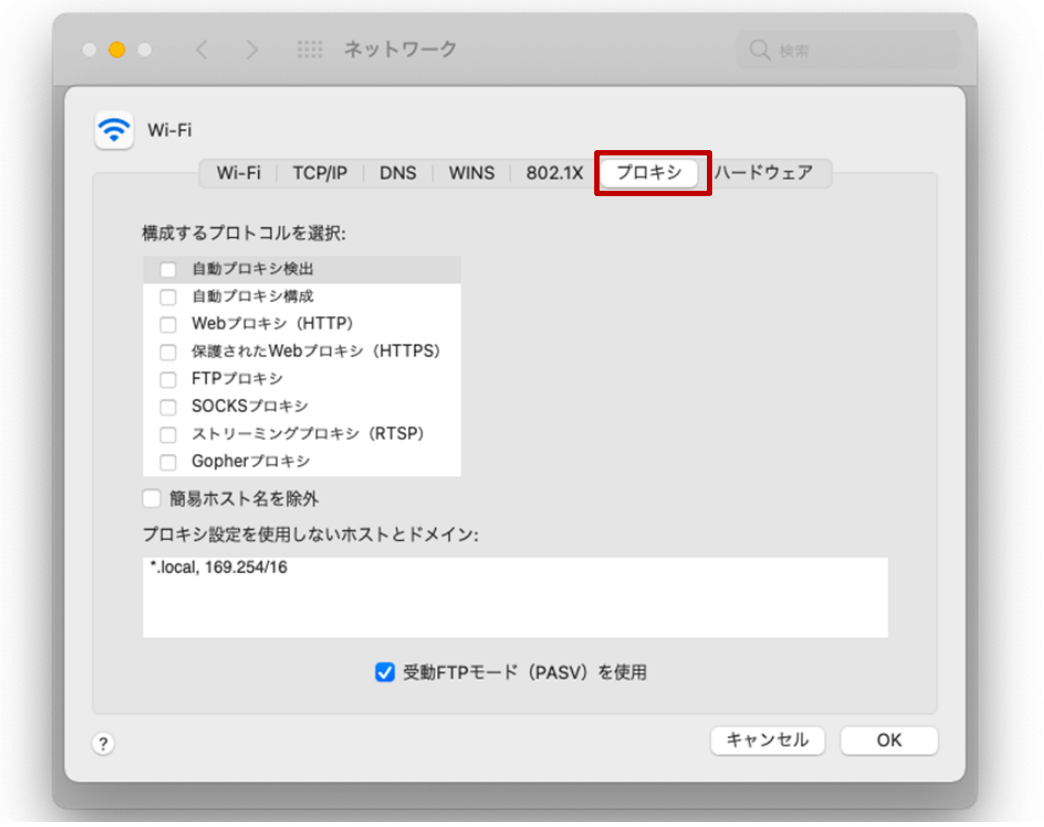
(3) “アプリケーション”画面が表示されたら「システム環境設定.app」をクリックします。



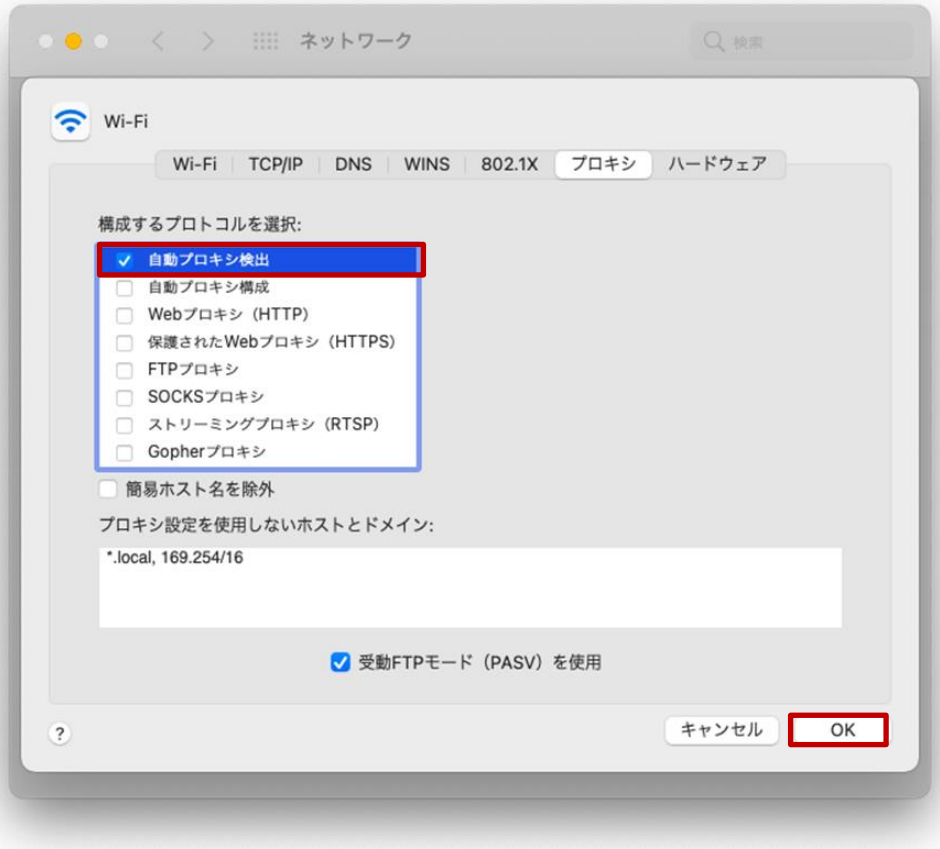
(4) “ネットワーク”画面が表示されたら、左側にある「Wi-Fi」アイコンを選択して、「詳細」をクリックします。



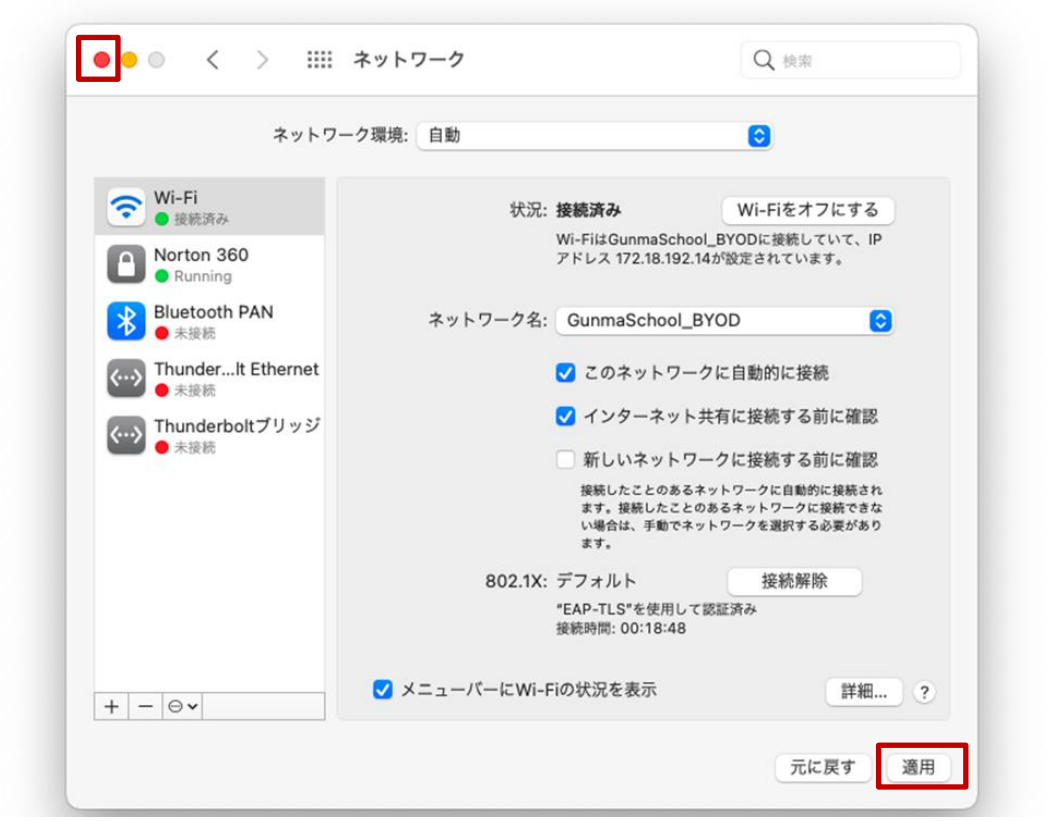
(5) Wi-Fi の詳細画面が表示されたら「プロキシ」タブをクリックしてプロキシを表示します。



(6) 構成するプロトコルを選択の「自動プロキシ検出」にチェックを入れて「OK」をクリックします。



(7) 「適用」をクリックして、左上の「●」をクリックして画面を閉じます。



(8) 次にプロキシの ID、パスワードを OS に登録するためにインターネットにアクセスを行います。デスクトップ画面にある「Safari」アイコンをクリックします。

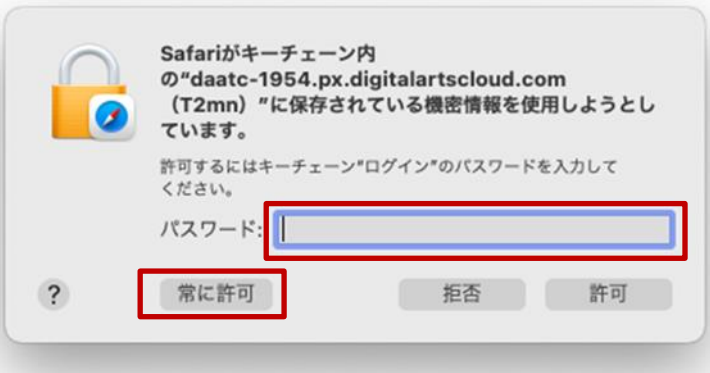
(9) 「プロキシ認証が必要です」のエラーメッセージが表示されたら、プロキシ認証を行なう必要があるため「システム環境設定」をクリックします。

(10) ユーザ ID とパスワードを入力するポップアップが表示されたら、プロキシサービスである i-FILTER@Cloud のユーザ名およびパスワードを入力します。ユーザ名には『BYOD パスワード通知書』の「i-FILTER アカウント」を、パスワードには、『BYOD パスワード通知書』の「パスワード」をそれぞれ入力して「OK」をクリックします。

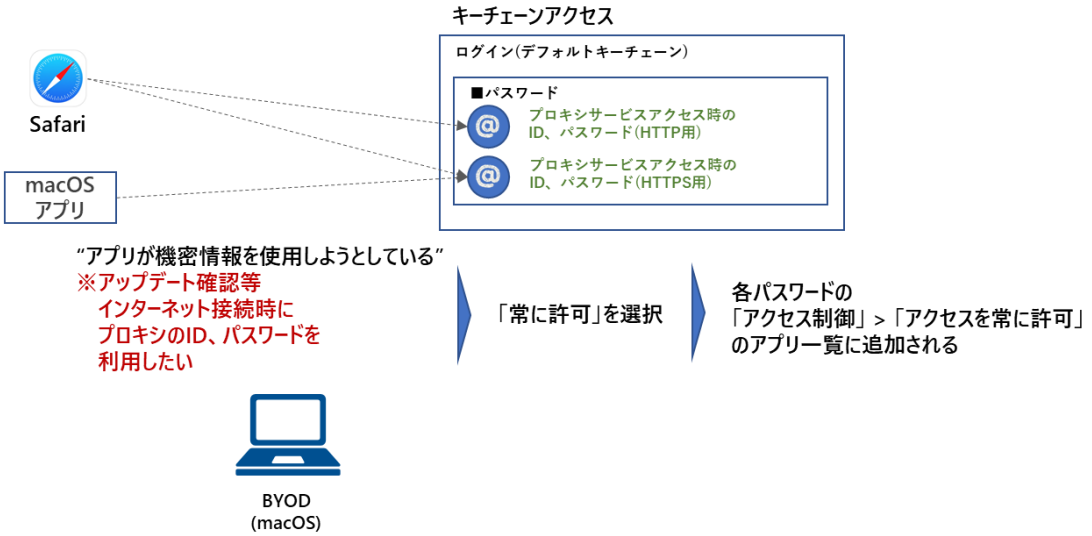
2.4.1. プロキシ設定後の注意点

プロキシ設定後に、macOS のアプリがプロキシサービス（キーチェーン内）の ID、パスワード機密情報を使用しようと下図のようなポップアップが表示されます。

(11) パスワードを入力する画面が表示されるので、「パスワード」にご自身の端末（BYOD）を起動するときに入力するパスワードを入力して「常に許可」をクリックします。



これは下図のように、アップデート確認等で macOS アプリがインターネット接続時にプロキシの ID、パスワードを利用したいために、上記のポップアップが表示されますので「パスワード」にご自身の端末（BYOD）を起動するときに入力するパスワードを入力して「常に許可」を選択してください。



※尚、Chrome ブラウザはプロキシアクセス時のログイン ID、パスワードについてキーチェーンアクセスを参照しません。

2.5. WEB アクセス実施、プロキシサービスへログイン

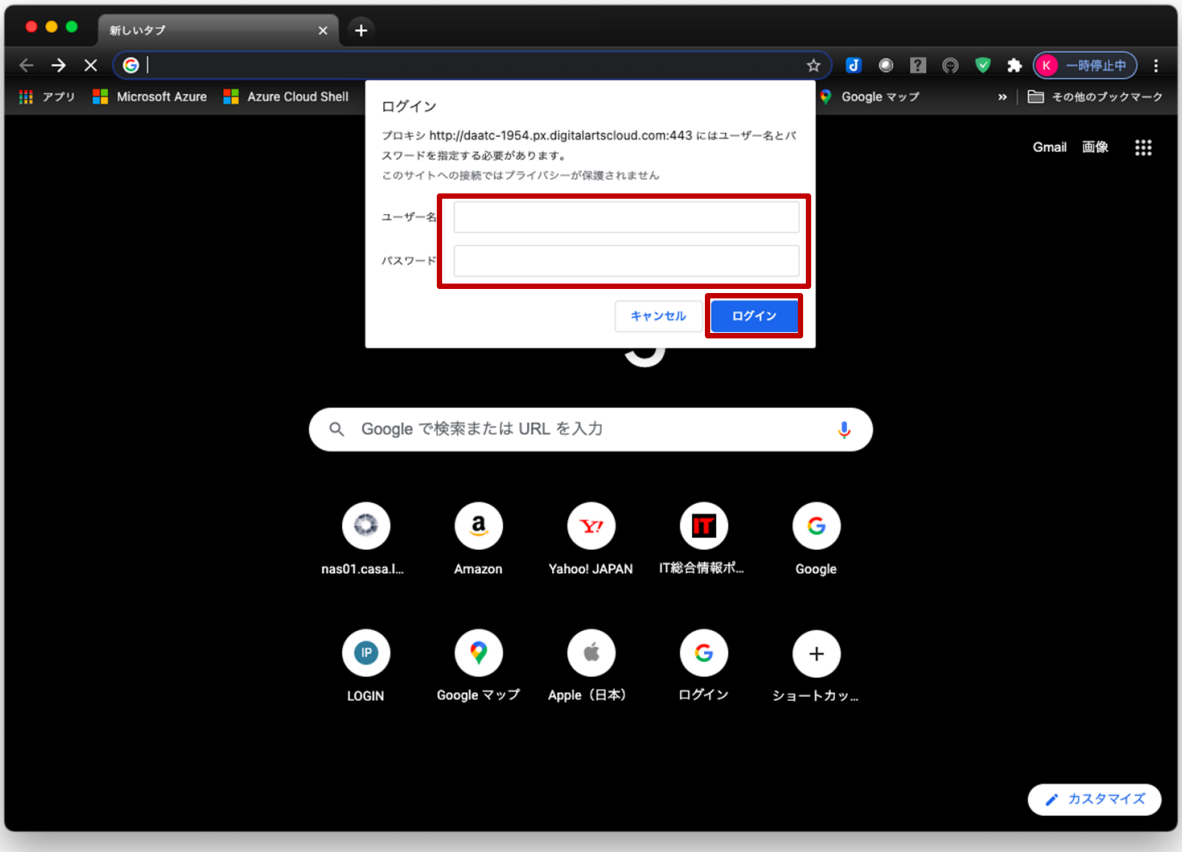
学習で必要な Google アプリは Chrome ブラウザで利用するため、ここでは Chrome を使って WEB にアクセスする手順を説明します。Chrome ブラウザを立ち上げて Web アクセスを実施すると下図のようなプロキシサービス利用の認証画面が表示されますので、ID とパスワードを入力してください。認証が成功すると WEB ページが表示されます。

(1) デスクトップ画面にある「Google Chrome」アイコンをクリックします。

※「Google Chrome」がインストールされていない場合は、自身でインストールしてください。

(2) ブラウザからホームページアクセス時に下図の認証画面が表示されます。ユーザー名には『BYOD パスワード通知書』にある「i-FILTER アカウント名」を、パスワードには『BYOD パスワード通知書』の「パスワード」をそれぞれ入力してログインをクリックします。

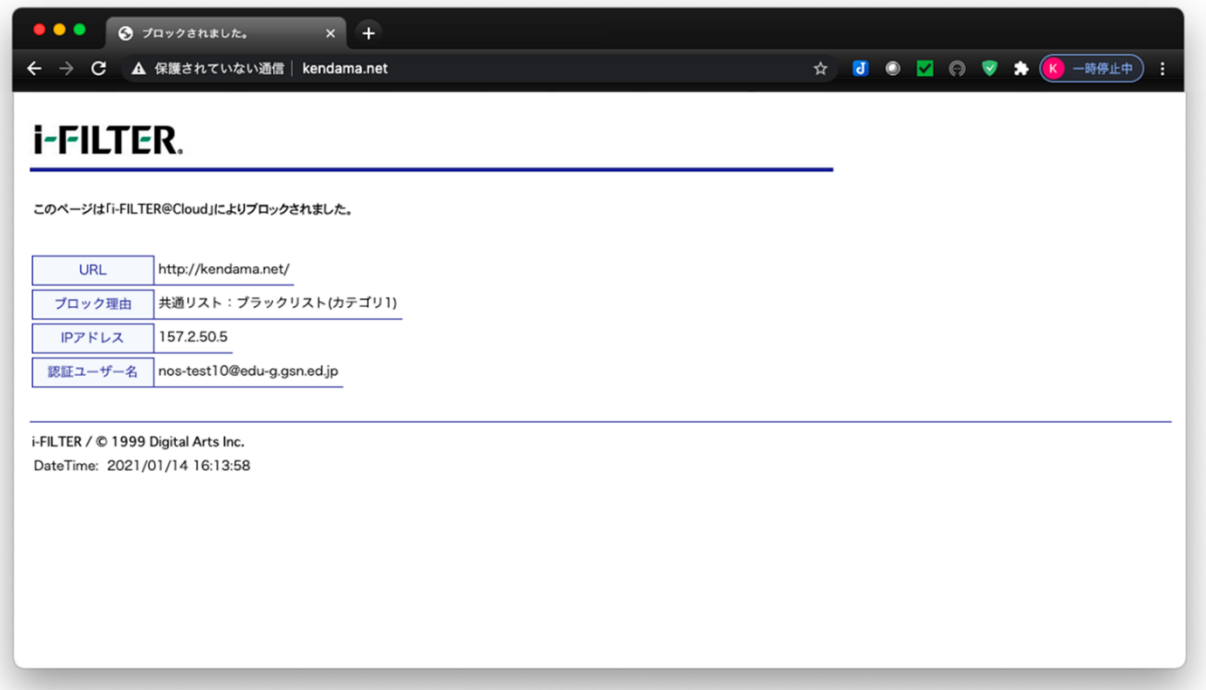
※Chrome ブラウザのプロキシ ID、パスワードは、キーチェーンの ID、パスワードを参照しないため、インターネットアクセス接続時に下の画面が表示されます。



(3) ログインに成功すると、プロキシサービス経由で WEB アクセスが可能となり、アクセス許可のサイトの場合は下図のように WEB ページが表示されます。

※下図はアクセス許可のサイトが表示された場合の例となります。

※下図はアクセス不許可のサイトを開いた場合の例となります。

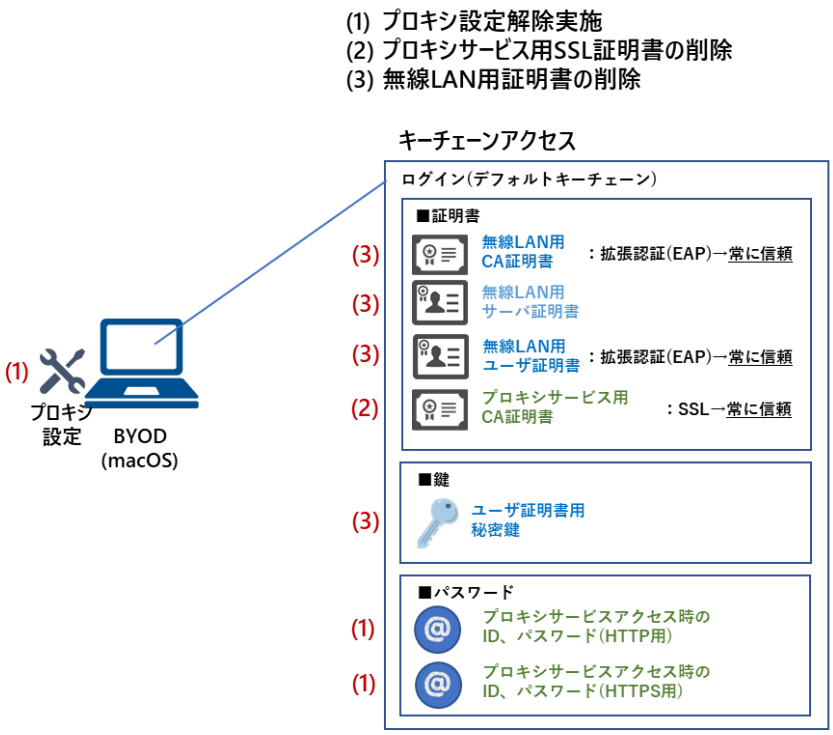


macOS における BYOD の web アクセス手順は以上となります。

3. 証明書削除手順

県立学校を卒業及び転校等で群馬県立学校から離れる場合、BYOD にインストールした証明書を削除する場合の手順を説明します。削除手順のイメージは下図の通りとなります。

注意：以降の作業を実施すると校内無線 LAN 環境に接続できなくなります。

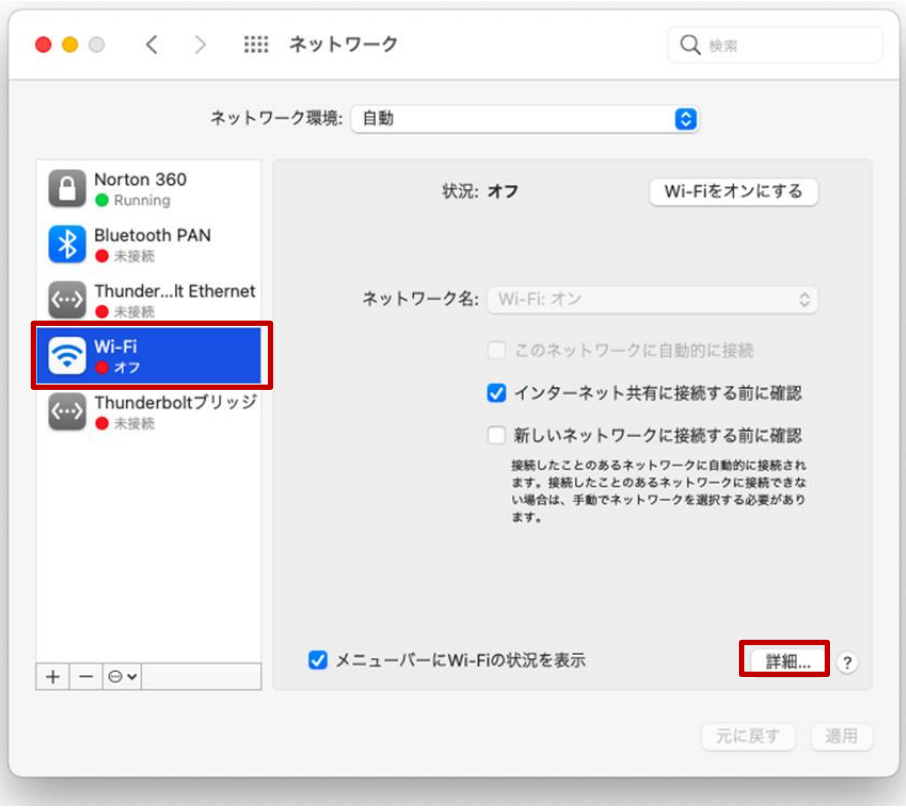


3.1. プロキシ設定解除実施

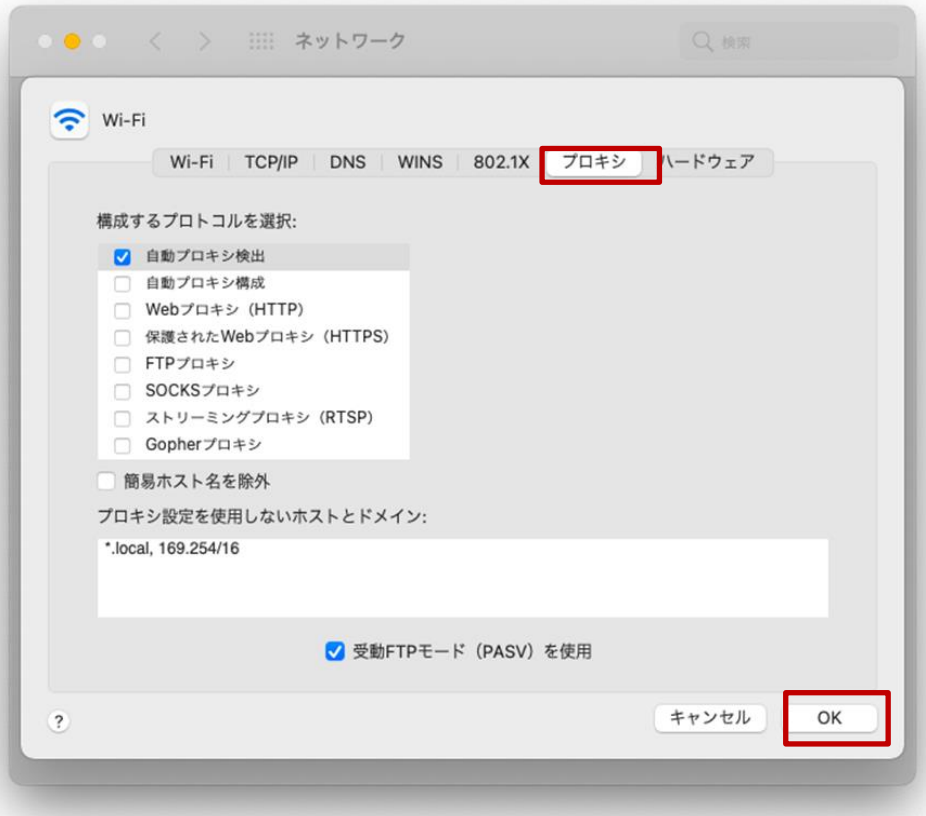
ここでは macOS のプロキシ設定の解除手順を説明します。

(1) システム環境設定の「ネットワーク」を起動します。※「ネットワーク」の起動手順は「2.4.プロキシ設定実施」の(1)～(3)を参照ください。

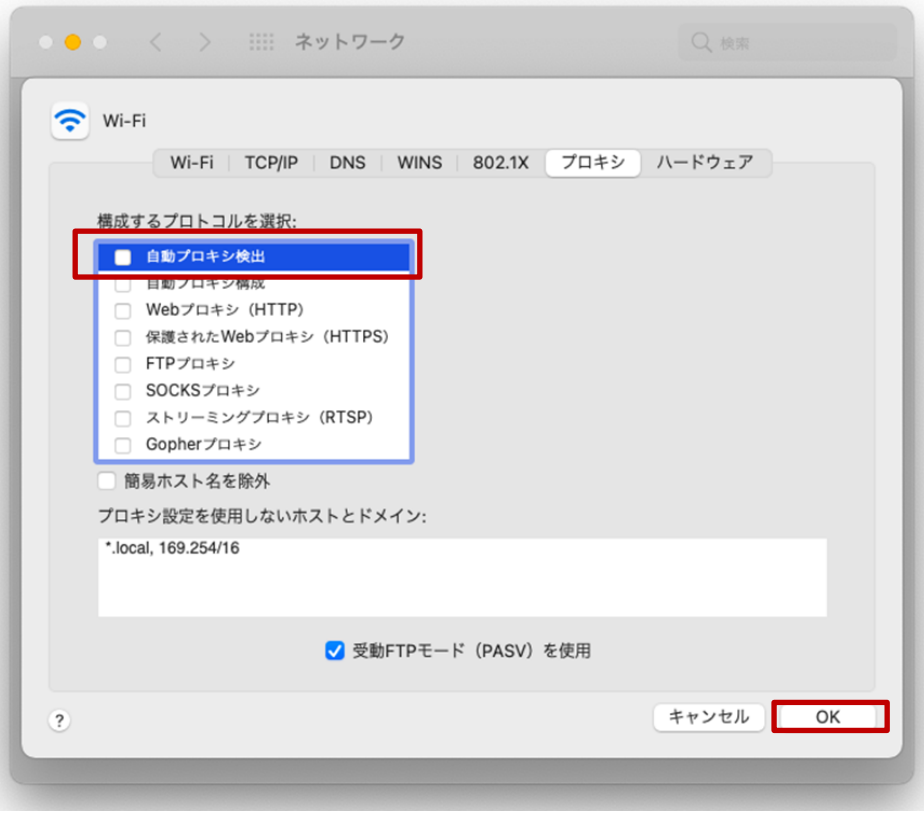
(2) “ネットワーク”画面が表示されたら、左側にある「Wi-Fi」アイコンを選択して、右下にある「詳細」をクリックします。



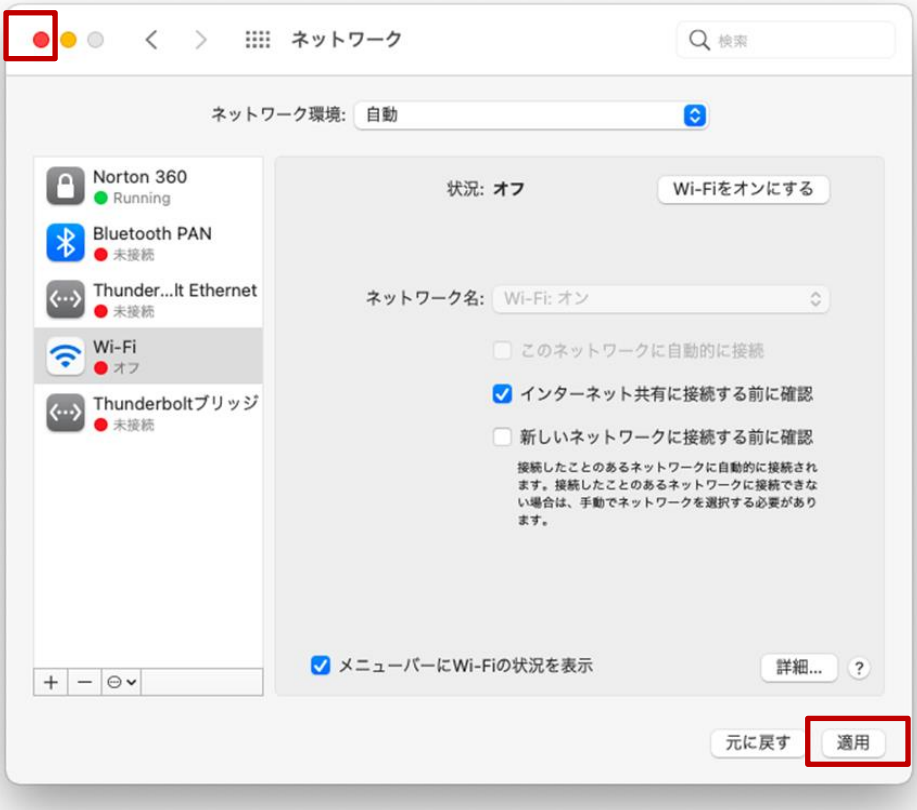
(3) Wi-Fi の詳細画面が表示されたら「プロキシ」タブをクリックしてプロキシを表示します。



(4) 「構成するプロトコルを選択」の「自動プロキシ検出」のチェックをはずして「OK」をクリックします。

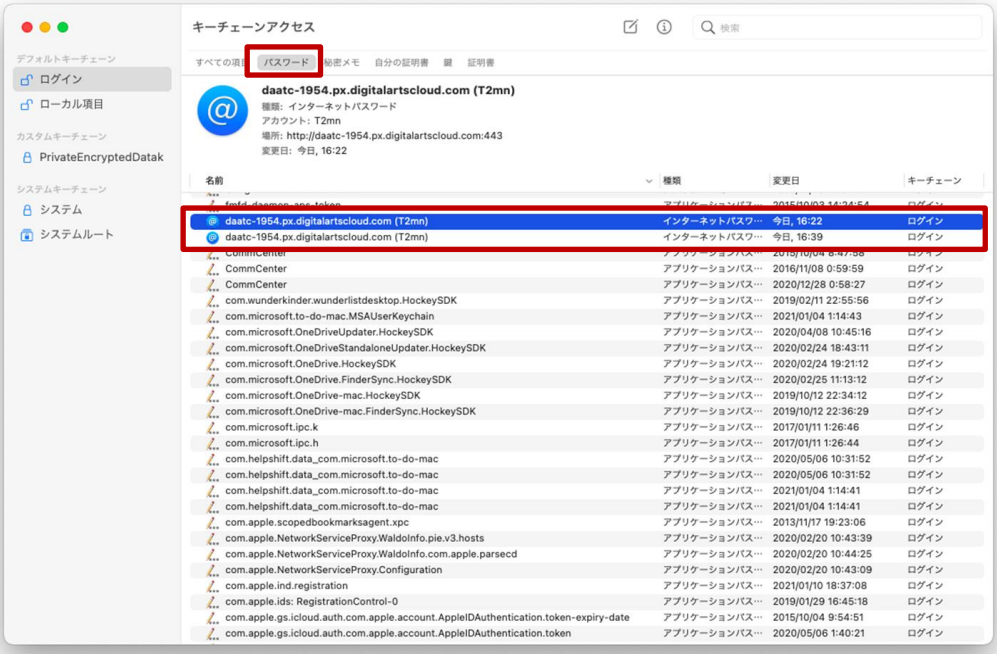


(5) 「適用」をクリックして、左上の「●」をクリックして画面を閉じます。

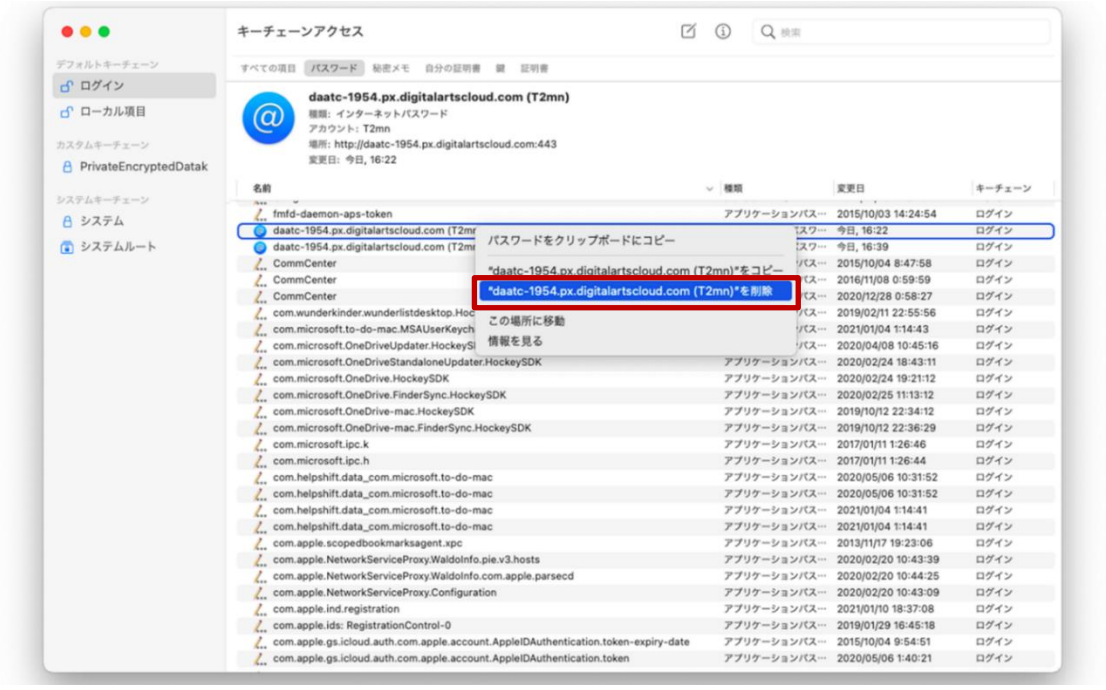


(6) 次にプロキシのパスワードを削除します。
「キーチェーンアクセス」を起動します。※「キーチェーンアクセス」の起動手順は「2.1.BYOD 向け無線 LAN 用証明書のインストール」の(1)～(5)を参照ください。

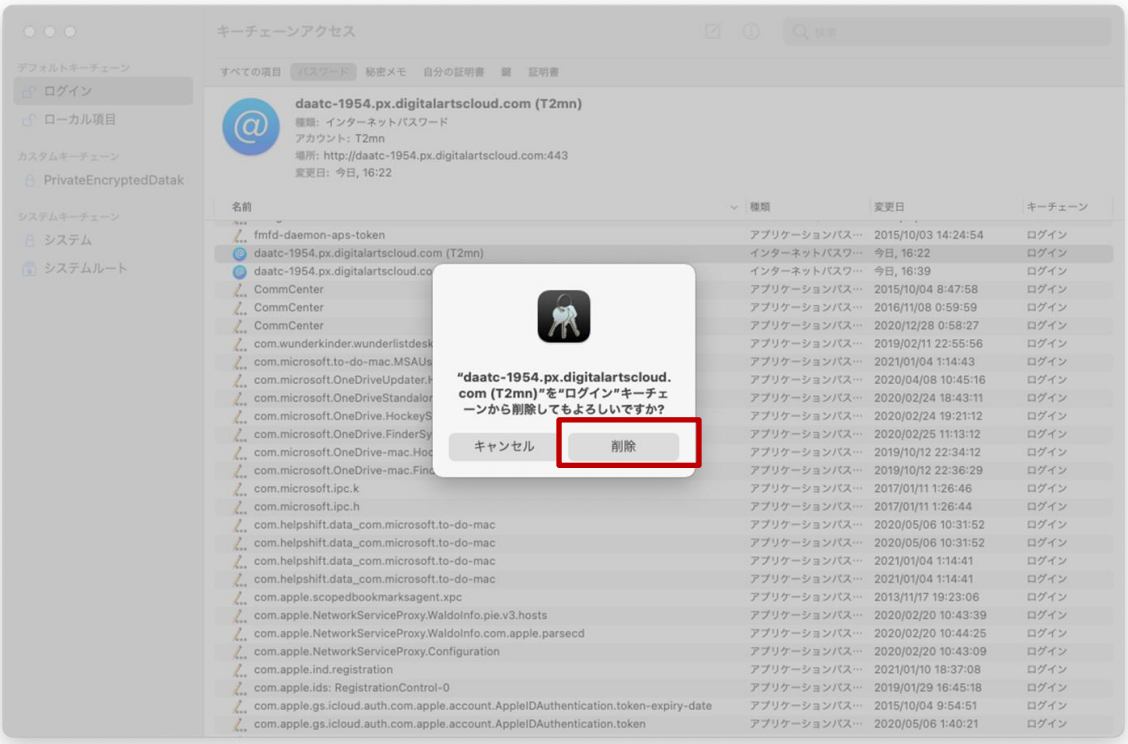
(7) キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の上段にある「パスワード」タブをクリックしてパスワード一覧を表示します。プロキシのパスワードは、HTTP 用と HTTPS 用の 2 つがありますのでどちらも削除します。



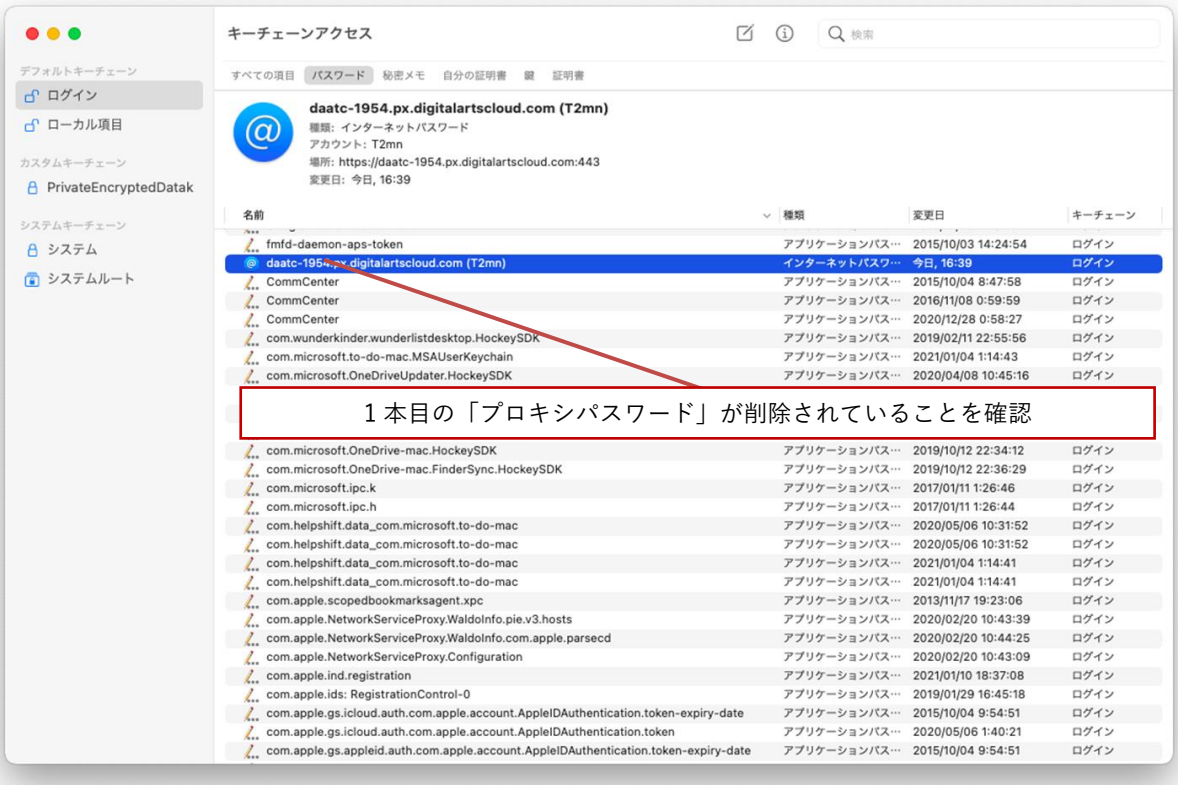
(8) 一覧の中の 1 本目の「プロキシパスワード：daatc-1954.px.digitalartshloud.com(＜i-FILTER アカウント名＞)」にカーソルをあわせて右クリックし「削除」を選択します。
※この手順書では i-FILTER アカウント名は「T2mn」で記述しております。



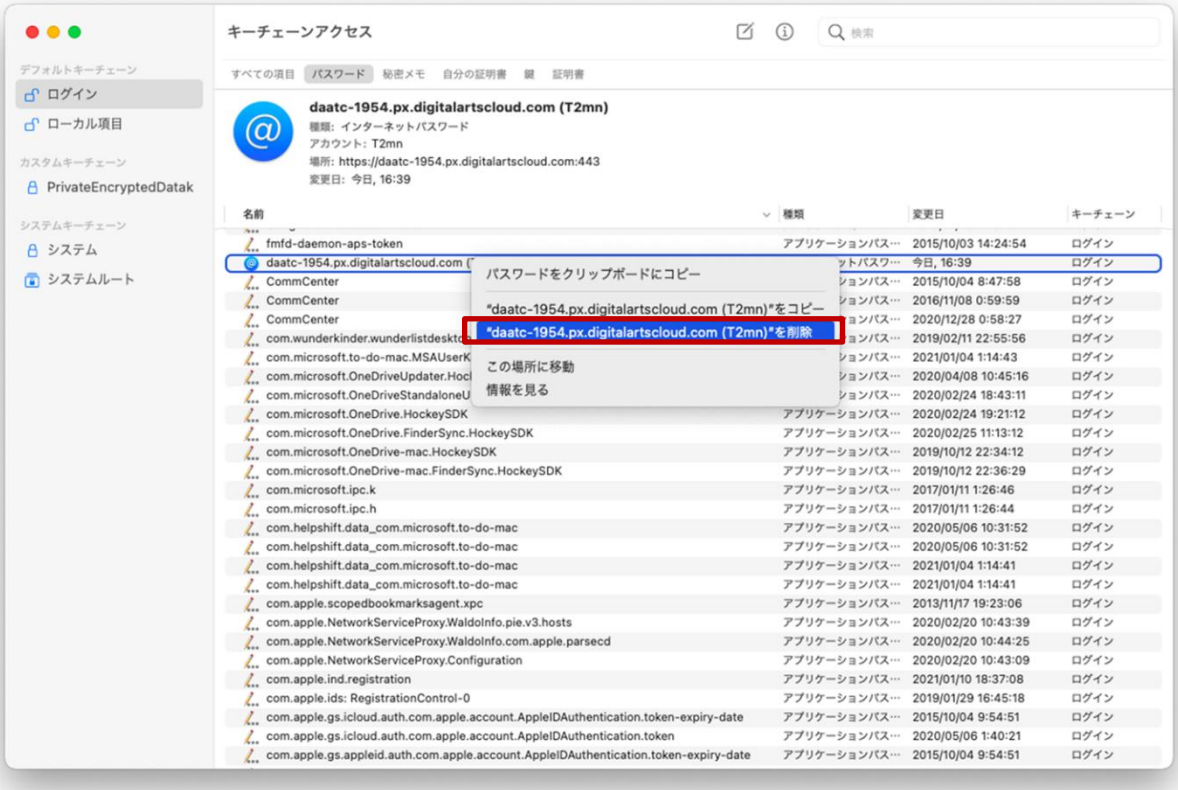
(9)　「プロキシパスワード：daatc-1954.px.digitalartshloud.com(＜i-FILTER アカウント名＞)」の削除を続行する場合は「削除」をクリックします。



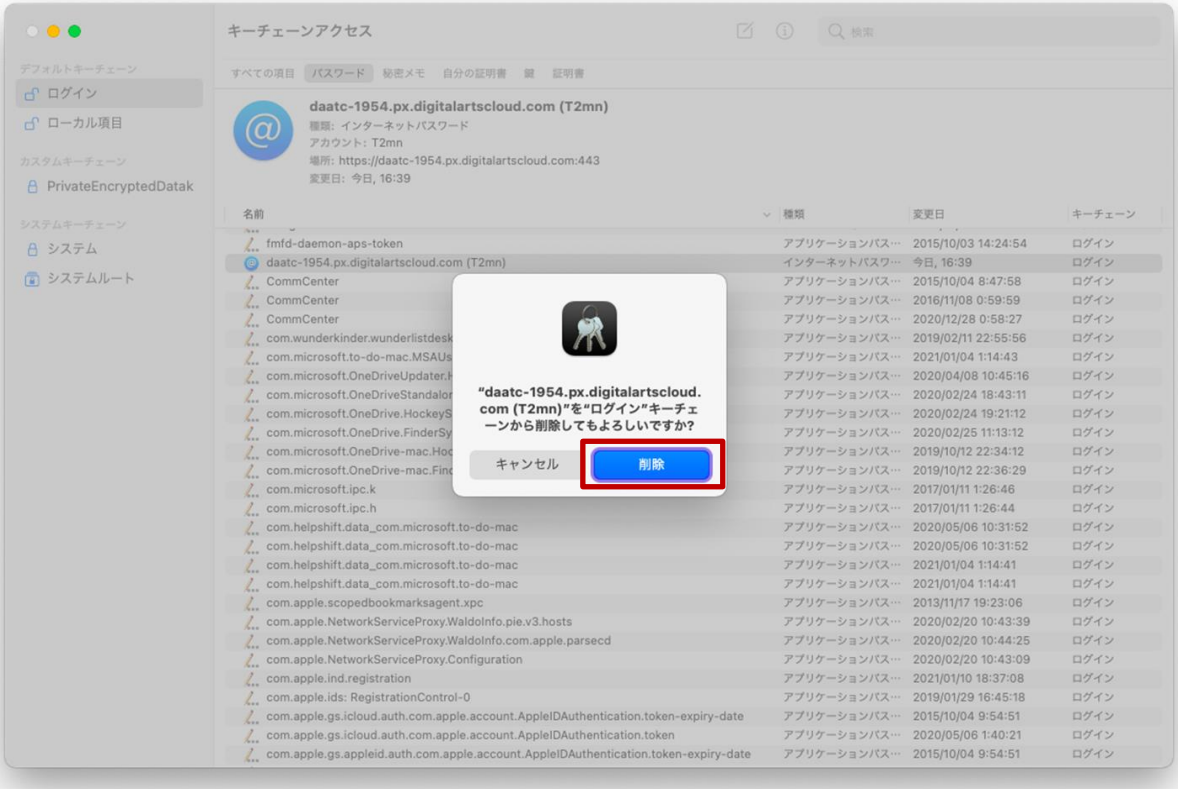
(10)「プロキシパスワード：daatc-1954.px.digitalartshloud.com(＜i-FILTER アカウント名＞)」が削除されていることを確認します。



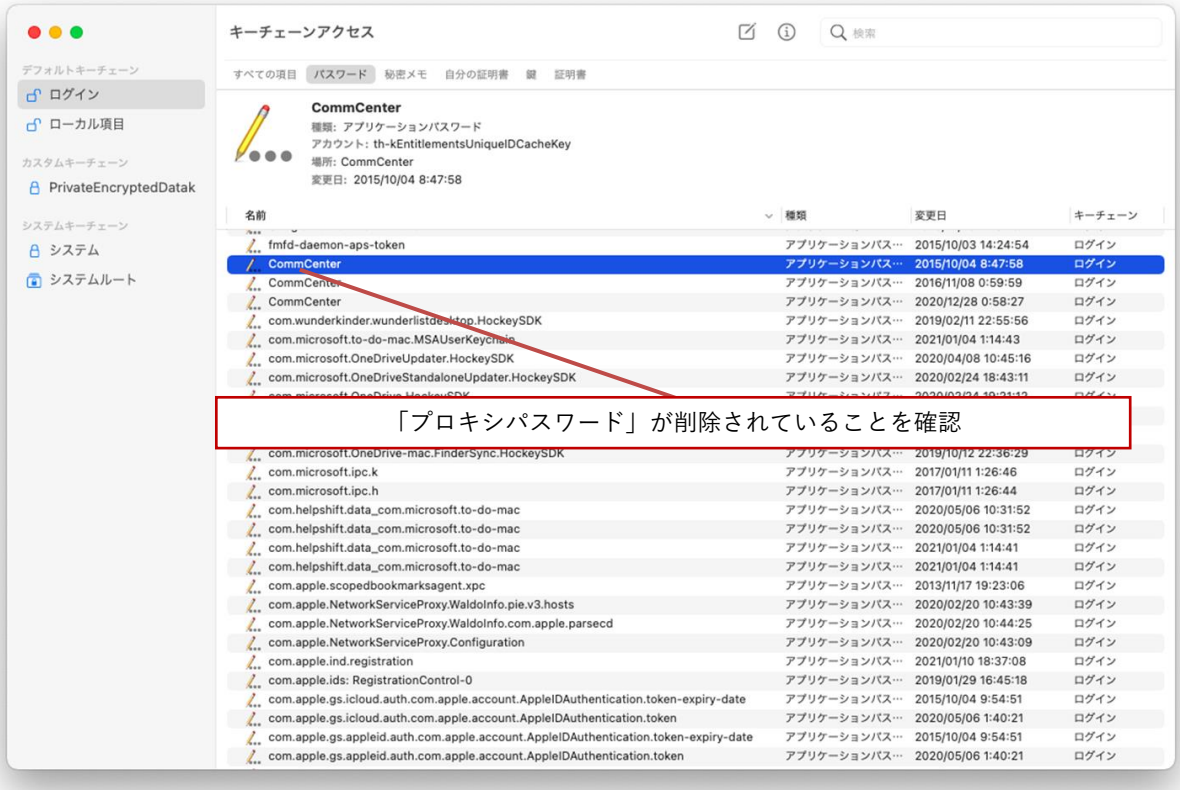
(11)2 本目の「プロキシパスワード：daatc-1954.px.digitalartshloud.com(＜i-FILTER アカウント名＞)」にカーソルをあわせて右クリックし「削除」を選択します。



(12)「プロキシパスワード：daatc-1954.px.digitalartshloud.com(＜i-FILTER アカウント名＞)」の削除を続行する場合は「削除」をクリックします。



(13)「プロキシパスワード：daatc-1954.px.digitalartshloud.com(＜i-FILTER アカウント名＞)」が削除されていることを確認します。



(14) プロキシの設定解除は完了です。

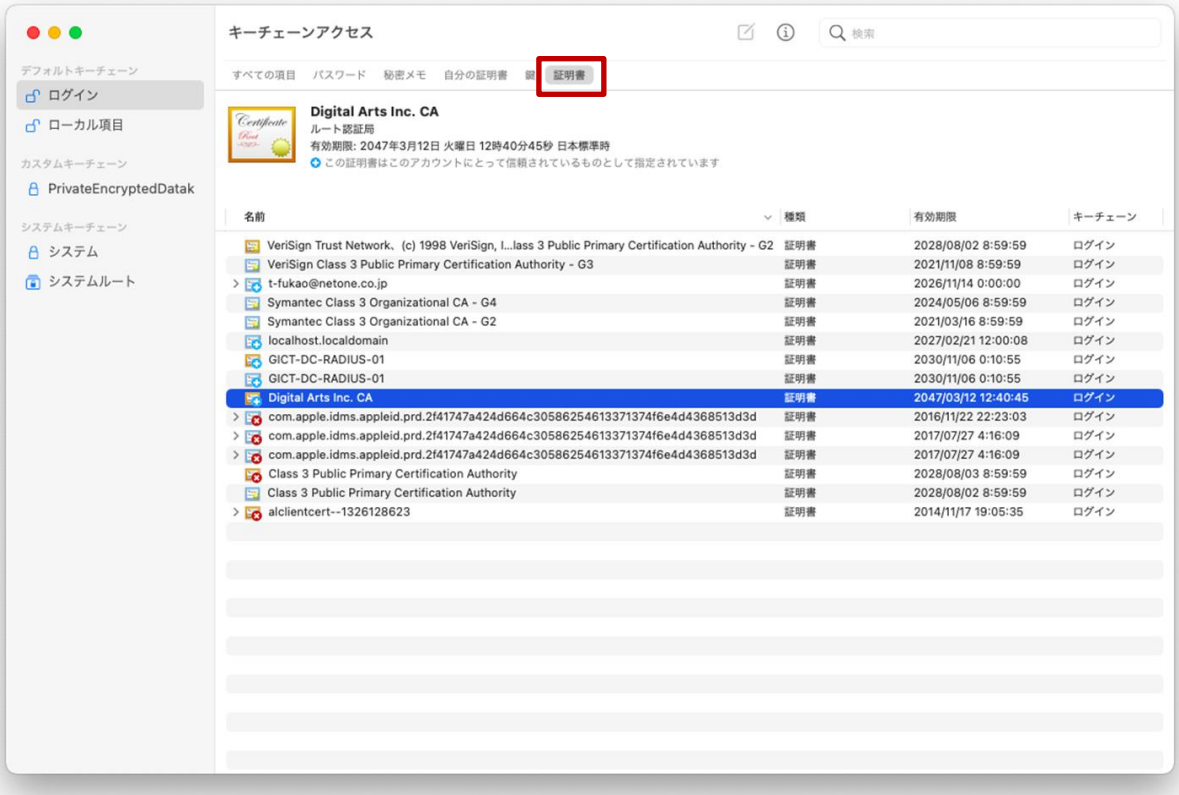
画面上にあるメニューバーの「キーチェーンアクセス」から「キーチェーンアクセスを終了」を選択して閉じてください。

3.2.　プロキシサービス用 SSL 証明書の削除

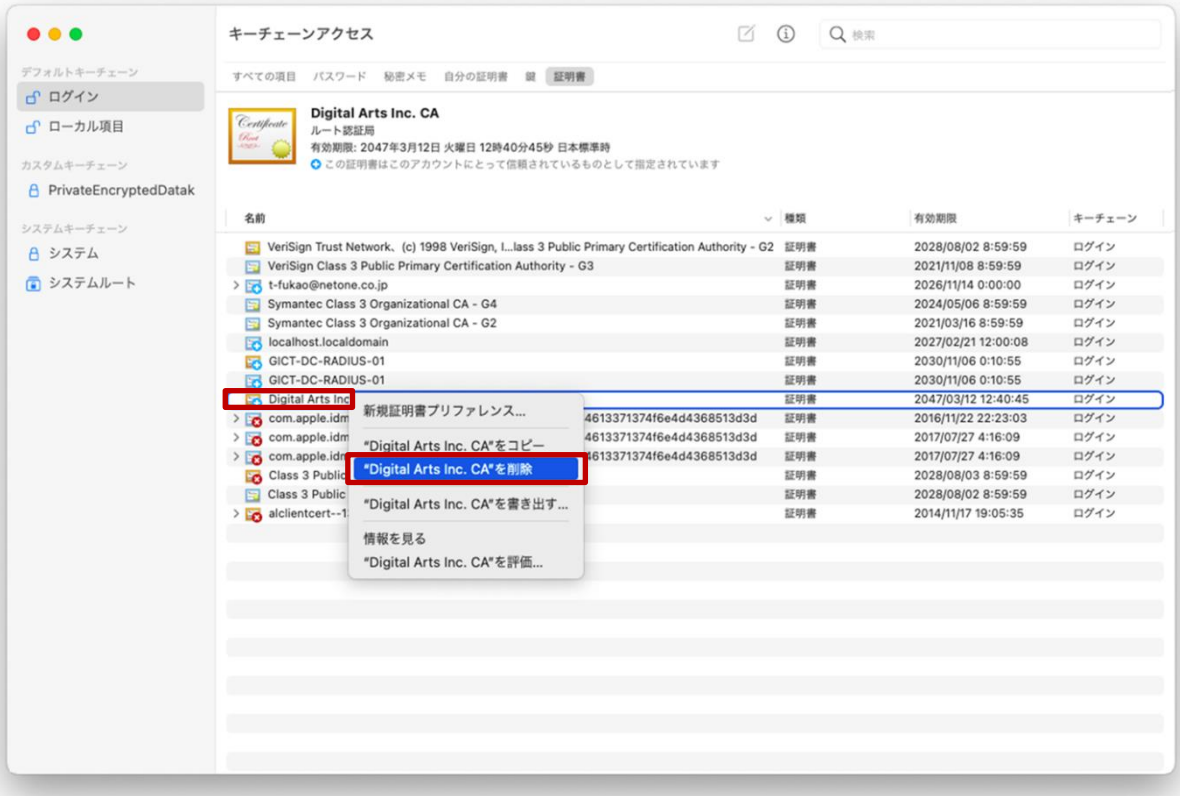
ここでは、プロキシサービスである i-FILTER@Cloud 用の SSL 証明書の削除手順を説明します。

(1)　「キーチェーンアクセス」を起動します。※「キーチェーンアクセス」の起動手順は「2.1.BYOD 向け無線 LAN 用証明書のインストール」の(1)～(5)を参照ください。

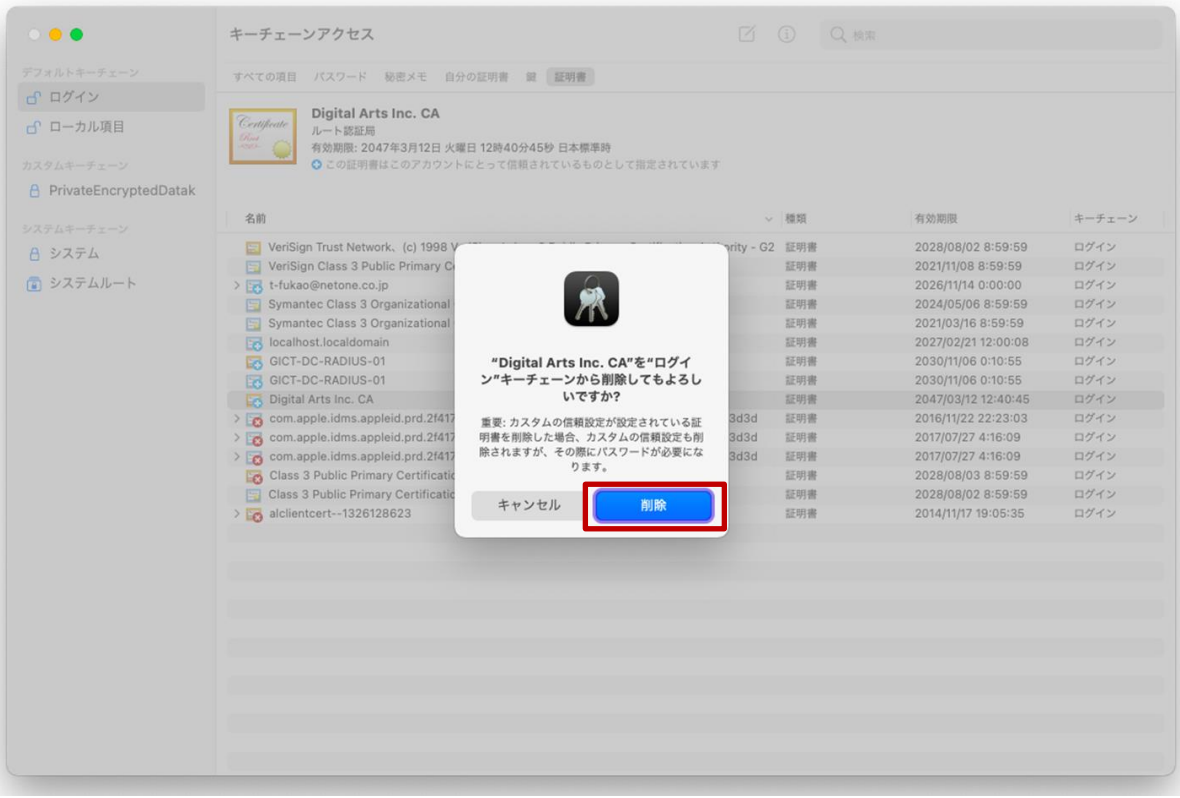
(2)　キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の上段にある「証明書」タブをクリックして、証明書一覧を表示します。
※「Digital Arts Inc. CA　※アイコン黄色枠」となっている証明書が i-FILTER 用の SSL 証明書です。それ以外の証明書の削除はしないでください！



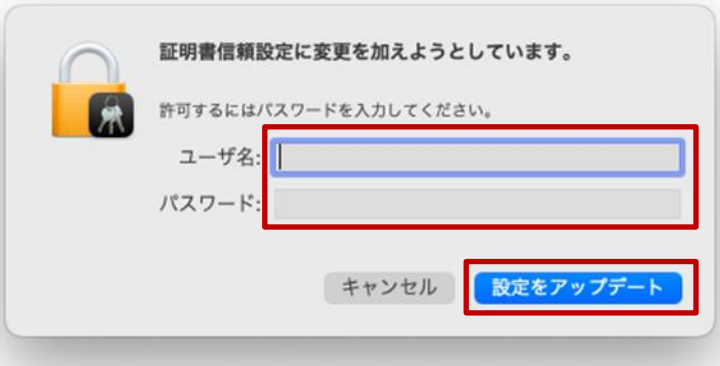
(3) 証明書一覧の中の i-FILTER@Cloud 用の SSL 証明書「Digital Arts Inc.CA　※アイコン黄色枠」にカーソルをあわせて右クリックし「削除」を選択します。



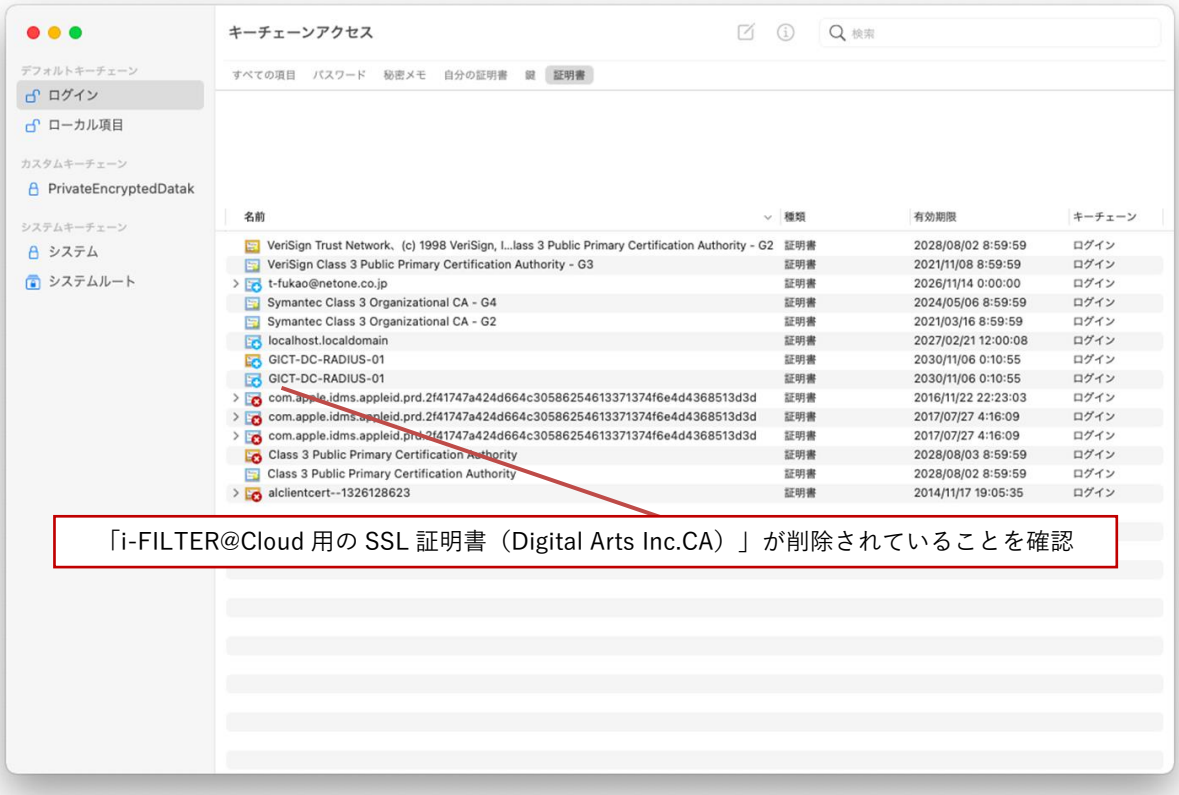
(4) 「i-FILTER@Cloud 用の SSL 証明書：Digital Arts Inc.CA」の削除を続行する場合は「削除」をクリックします。



(5) 証明書の設定を変更する場合には、ユーザ ID とパスワードを入力する必要があるため、「ユーザ名」と「パスワード」にご自身の端末（BYOD）を起動するときに入力するログイン ID とパスワードを入力して「設定をアップデート」をクリックします。



(6) i-FILTER@Cloud 用の SSL 証明書「Digital Arts Inc.CA　※アイコン黄色枠」が削除されていることを確認します。

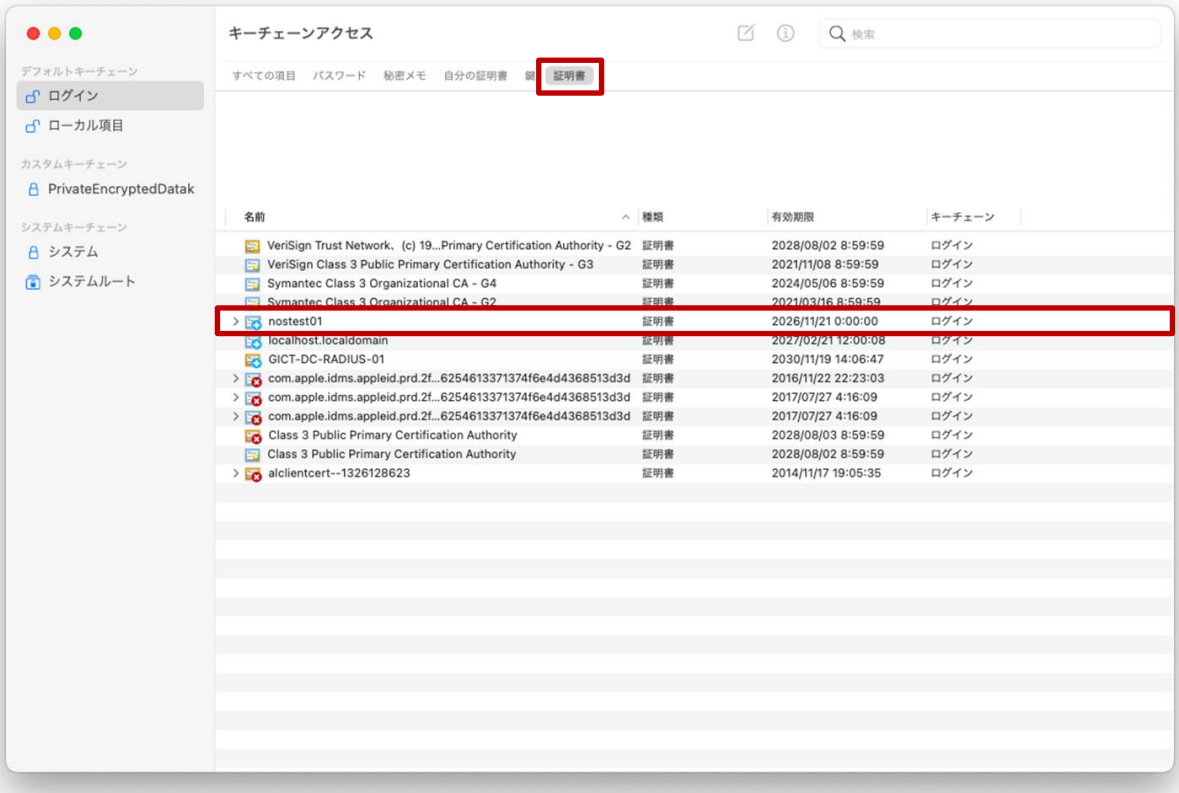


引き続き【3.3.BYOD 向け無線 LAN 用証明書の削除】を実施してください。

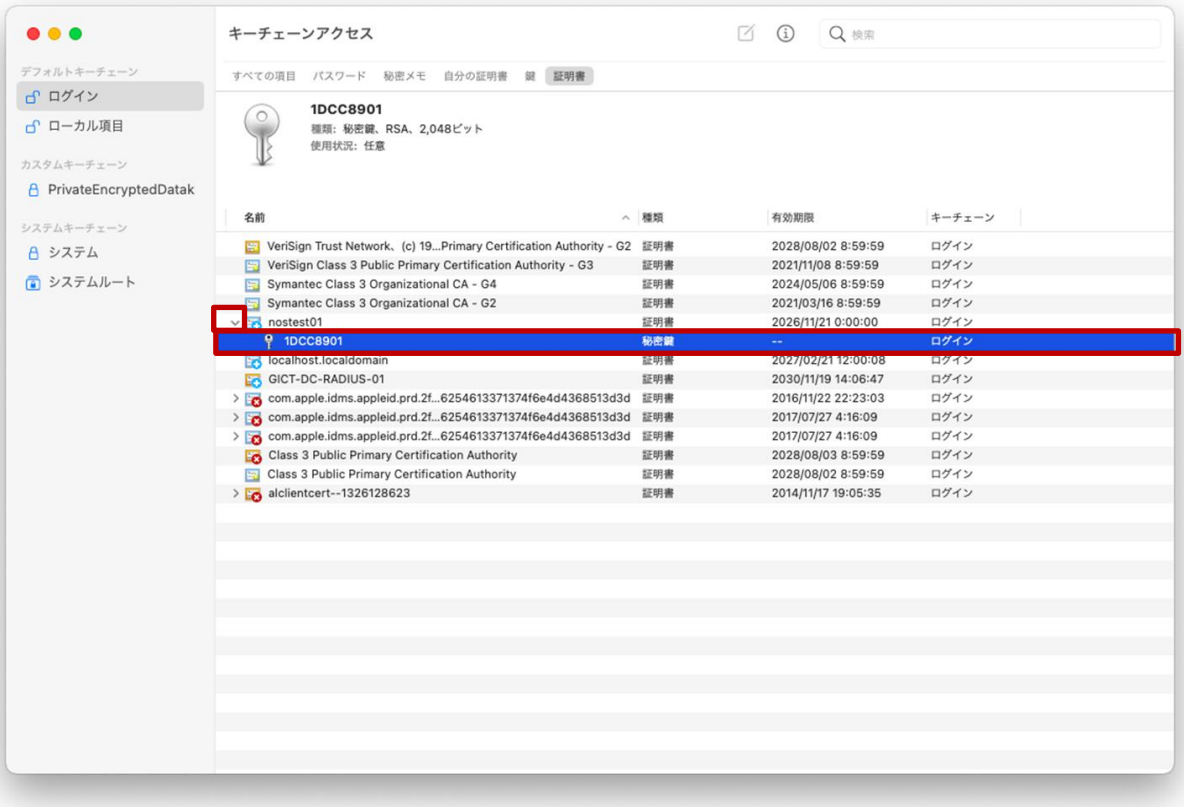
3.3. BYOD 向け無線 LAN 用証明書の削除

ここでは、BYOD 向け無線 LAN 用証明書の削除手順を説明します。

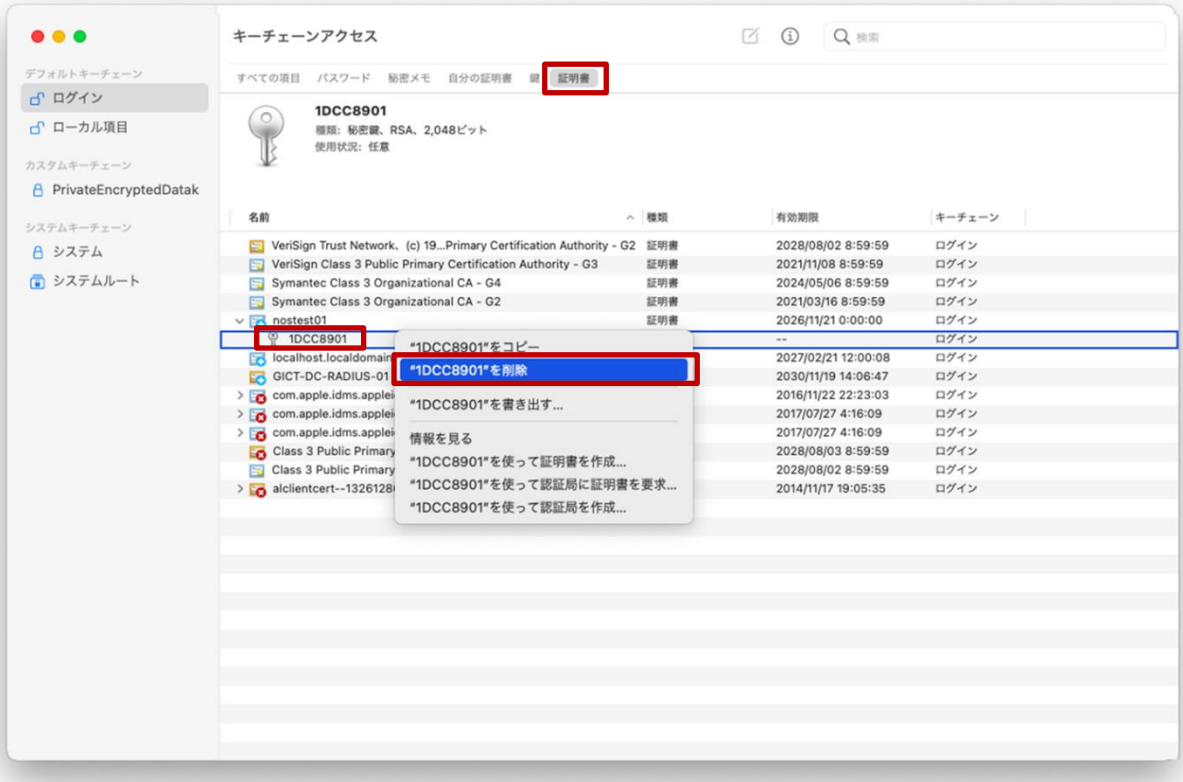
(1) キーチェーンアクセス（デフォルトキーチェーン：ログイン）画面の上段にある「証明書」タブをクリックして、証明書一覧を表示します。
名前が<ログイン ID>となっている証明書が無線 LAN 用ユーザ証明書となります。
※この手順書では BYOD 向け無線 LAN 用のユーザ証明書のファイル名は「nostest01」で記述します。これ以外の証明書の削除はしないでください！



(2) 最初に秘密鍵「＜この手順書では「1DCC8901」＞」を削除します。
ユーザ証明書「<アカウント名>」の左側にある［>］をクリックして「秘密鍵」が入っていることを確認します。

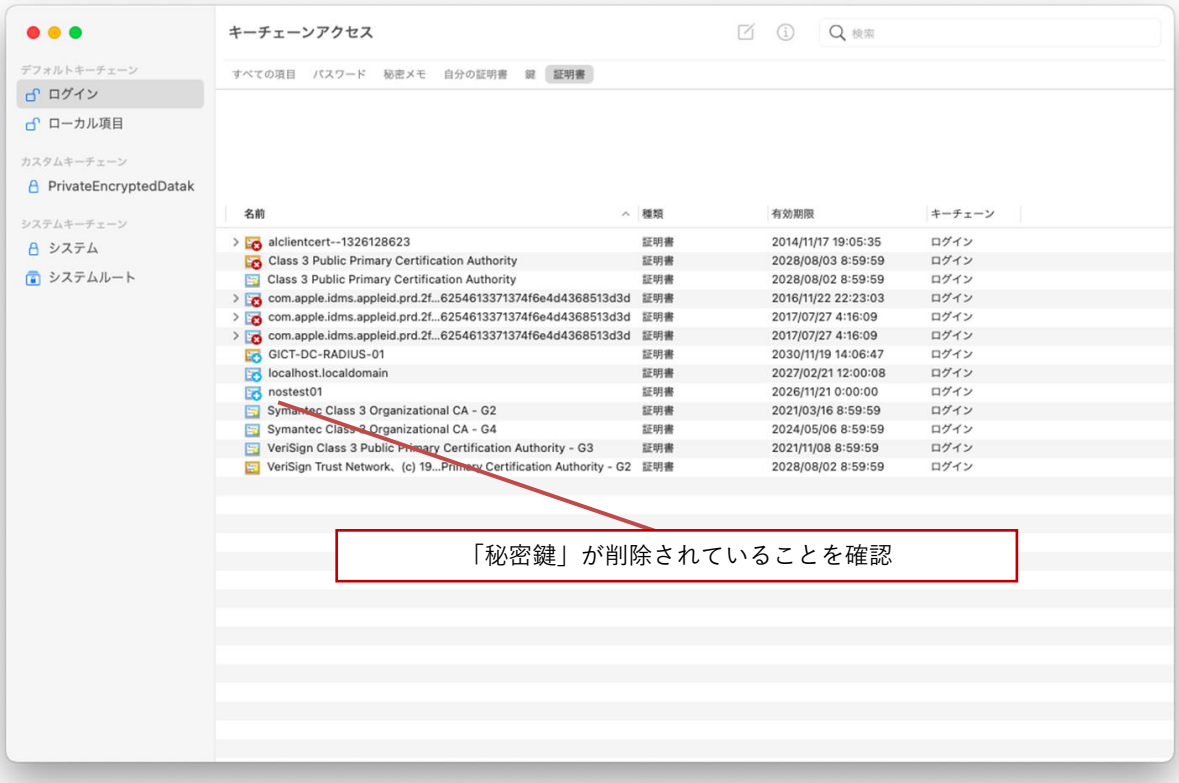


(3) 「秘密鍵」にカーソルをあわせて右クリックし「削除」を選択します。

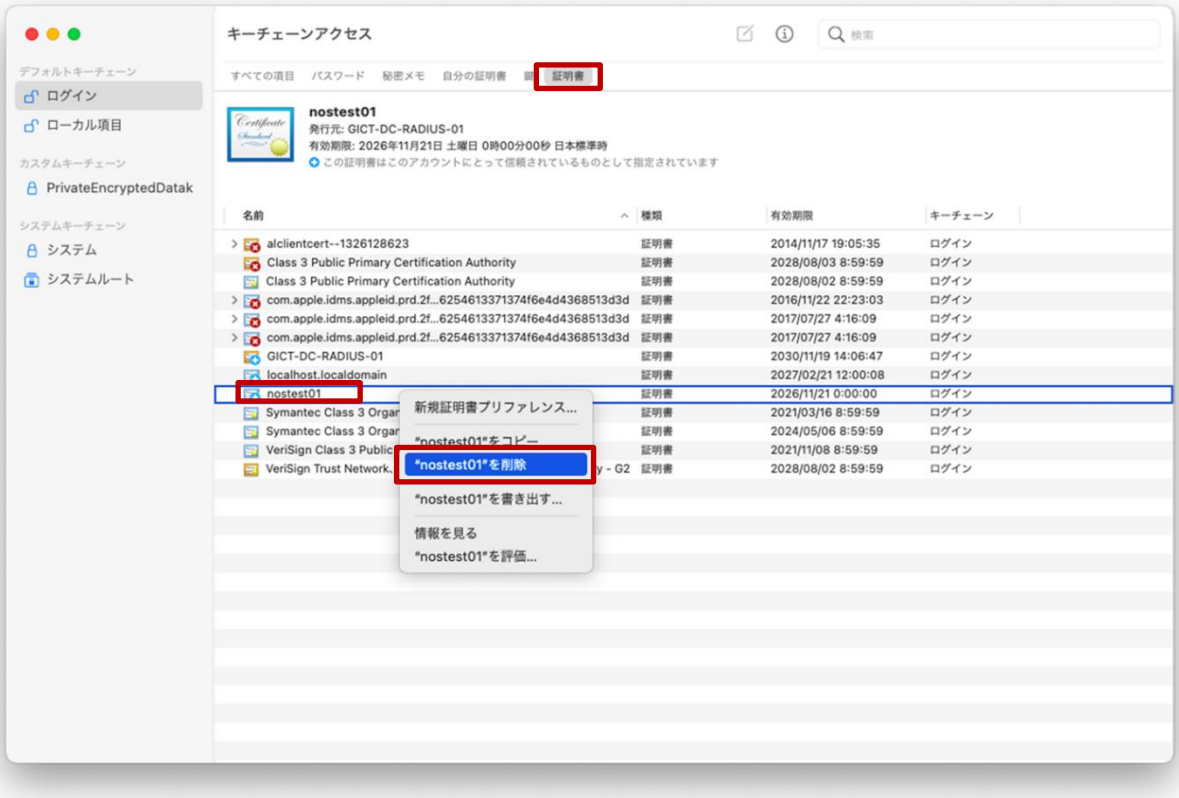


(4) 「秘密鍵」の削除を続行する場合は「削除」をクリックします。

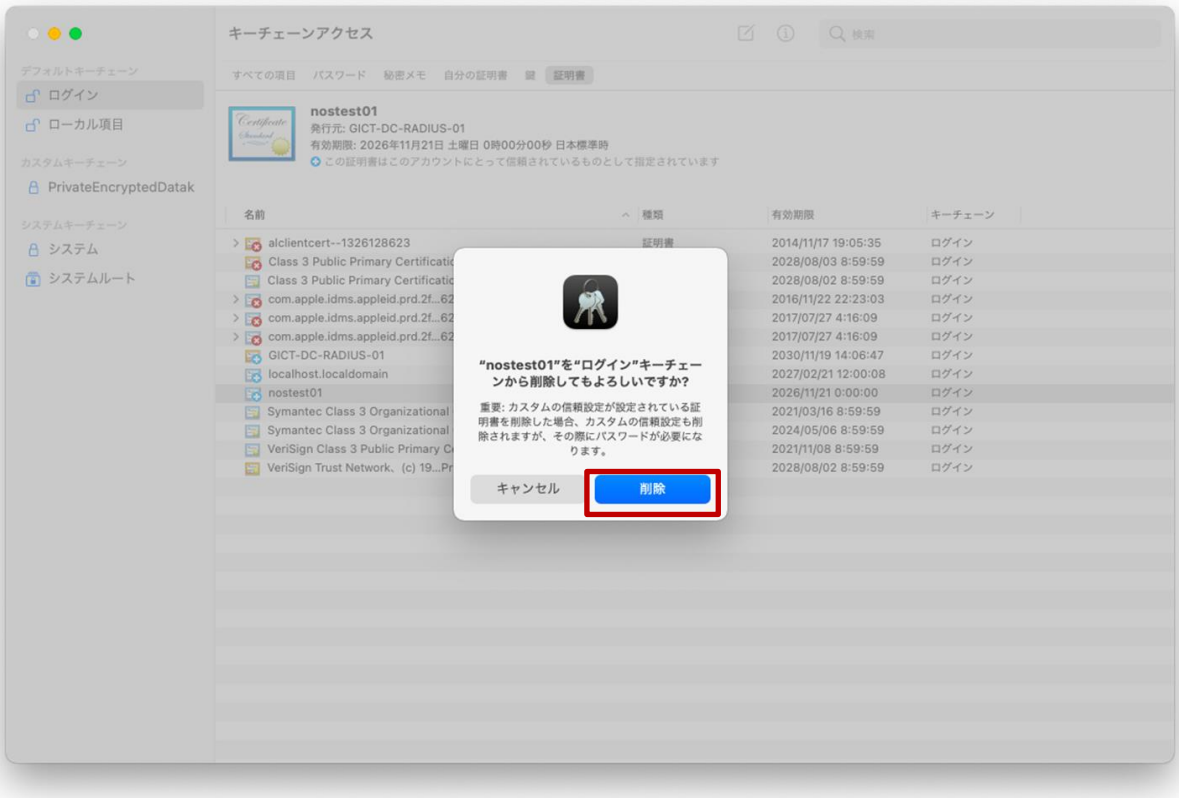
(5) 「ユーザ証明書：<アカウント名>」から「秘密鍵」が削除されていることを確認します。



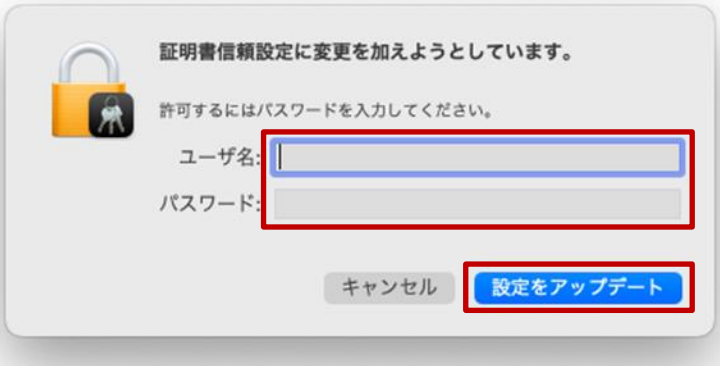
(6) 次にユーザ証明書「<アカウント名>」を削除します。
証明書一覧の中にあるユーザ証明書「<アカウント名>」にカーソルをあわせて右クリックし「削除」を選択します。



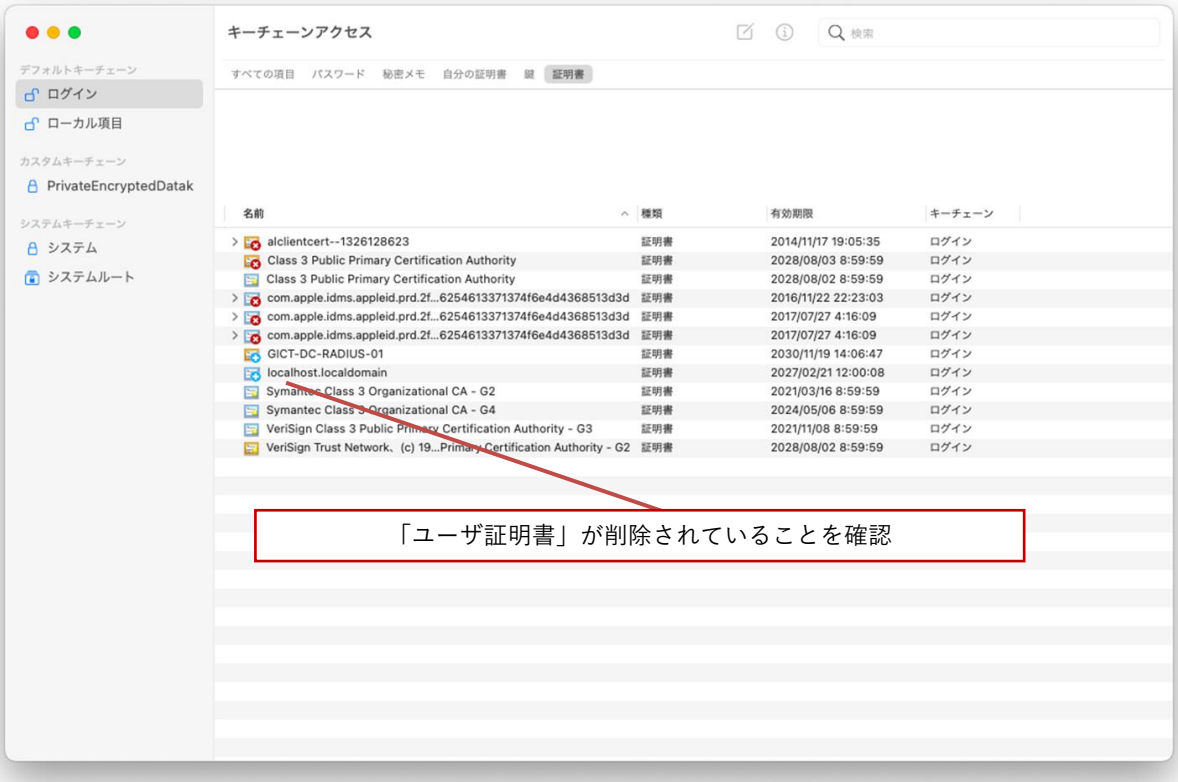
(7) ユーザ証明書「<アカウント名>」の削除を続行する場合は「削除」をクリックします。



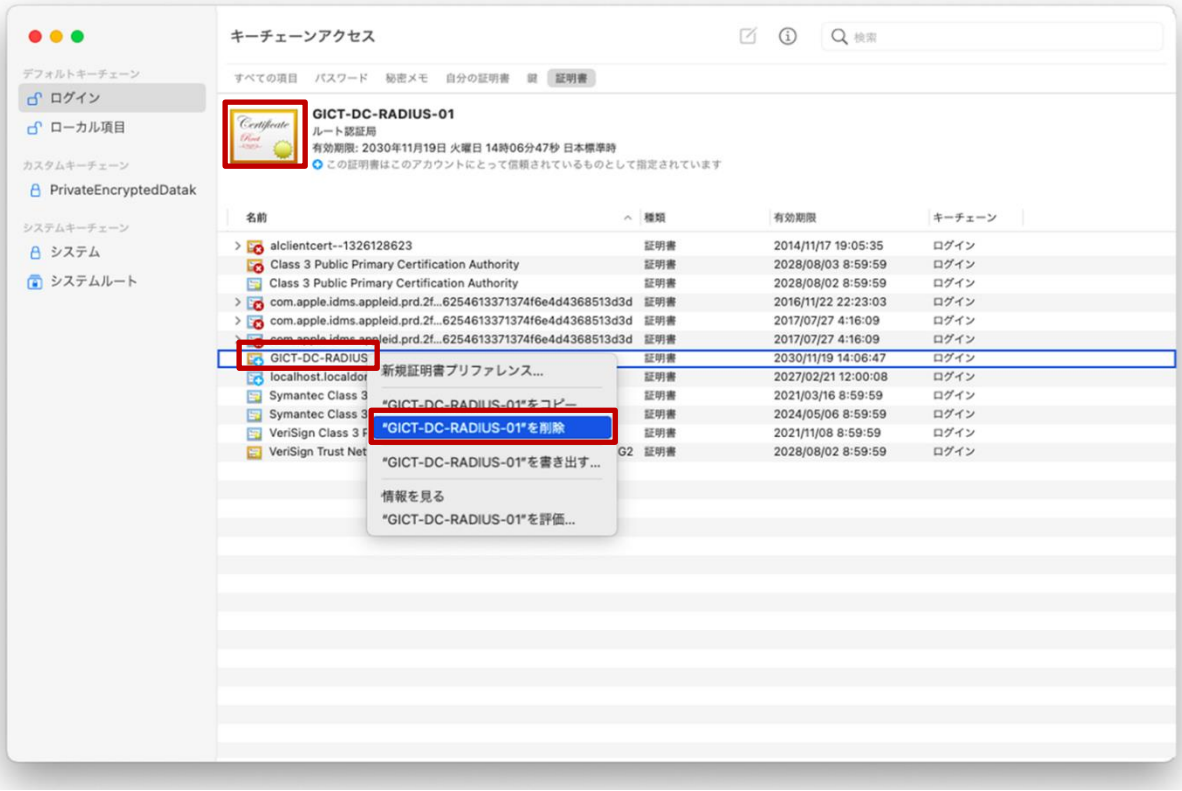
(8) 証明書の設定を変更する場合には、ユーザ ID とパスワードを入力する必要があるため、「ユーザ名」と「パスワード」にご自身の端末（BYOD）を起動するときに入力するログイン ID とパスワードを入力して「設定をアップデート」をクリックします。



(9) 証明書一覧のユーザ証明書「<アカウント名>」が削除されていることを確認します。

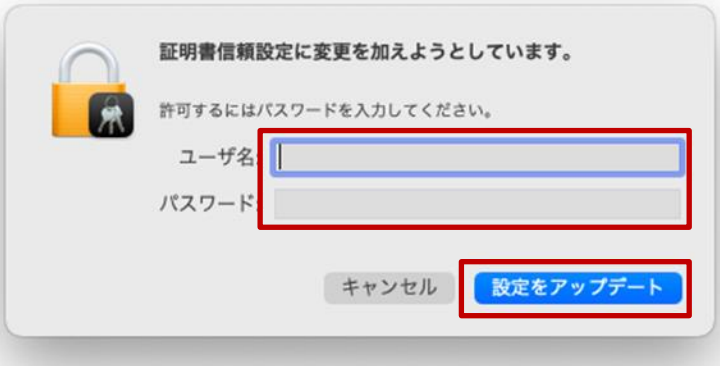


(10)次に無線 LAN 用 CA 証明書を削除します。「GICT-DC-RADIUS-01　※アイコン黄色枠」となっている証明書が CA 証明書です。※それ以外の証明書の削除はしないでください！
証明書一覧の中の CA 証明書「GICT-DC-RADIUS-01　※アイコン黄色枠」にカーソルをあわせて右クリックし「削除」を選択します。

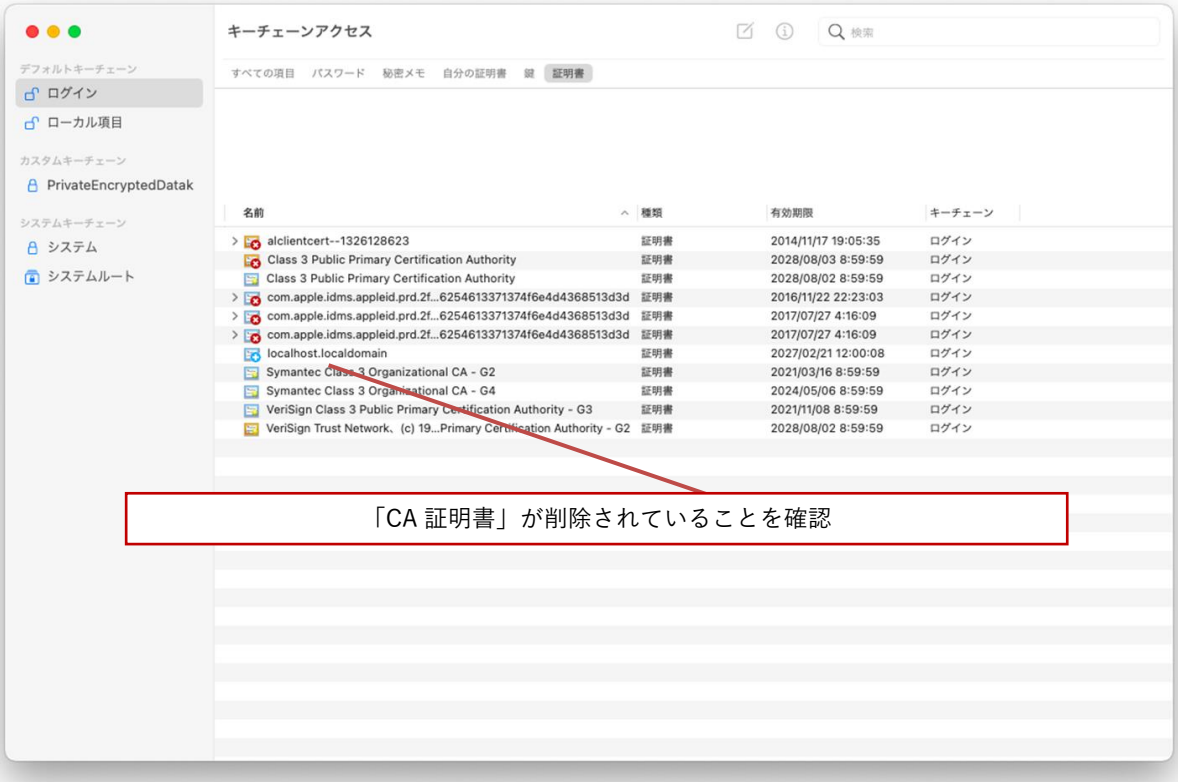


(11)CA 証明書の削除を続行する場合は「削除」をクリックします。

(12) 証明書の設定を変更する場合には、ユーザ ID とパスワードを入力する必要があるため、「ユーザ名」と「パスワード」にご自身の端末（BYOD）を起動するときに入力するログイン ID とパスワードを入力して「設定をアップデート」をクリックします。

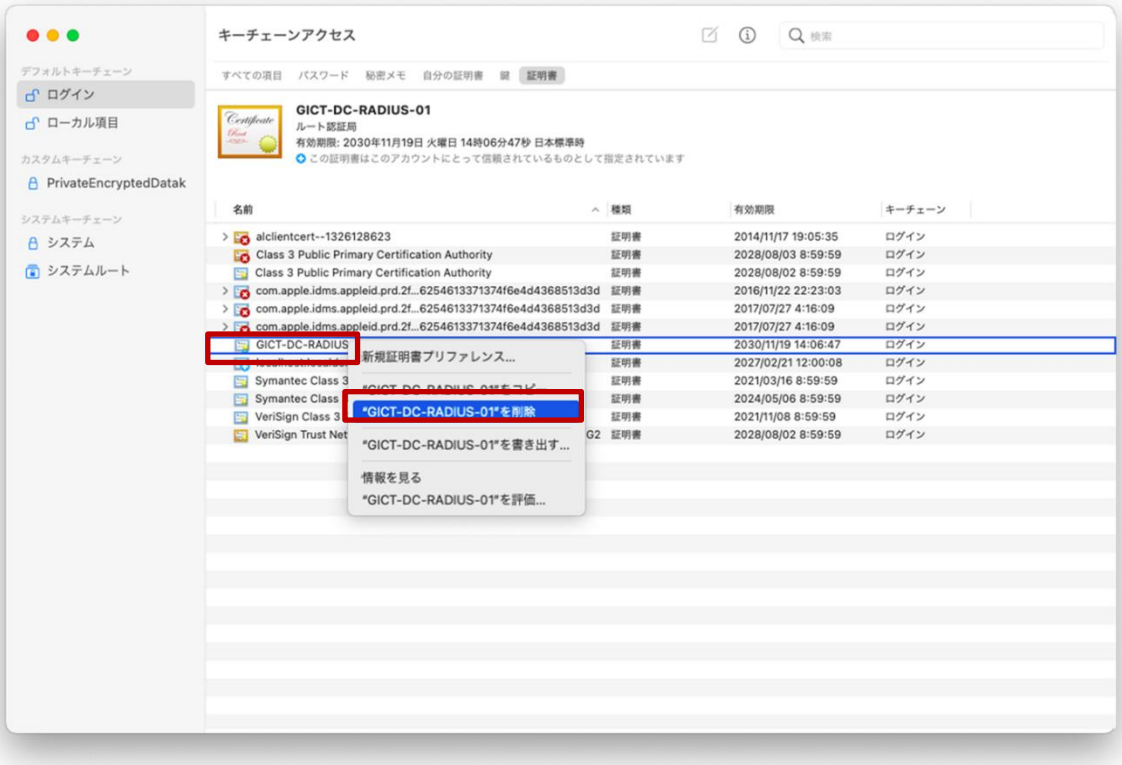


(13) 証明書一覧の中の CA 証明書「GICT-DC-RADIUS-01　※アイコン黄色枠」証明書が削除されていることを確認します。

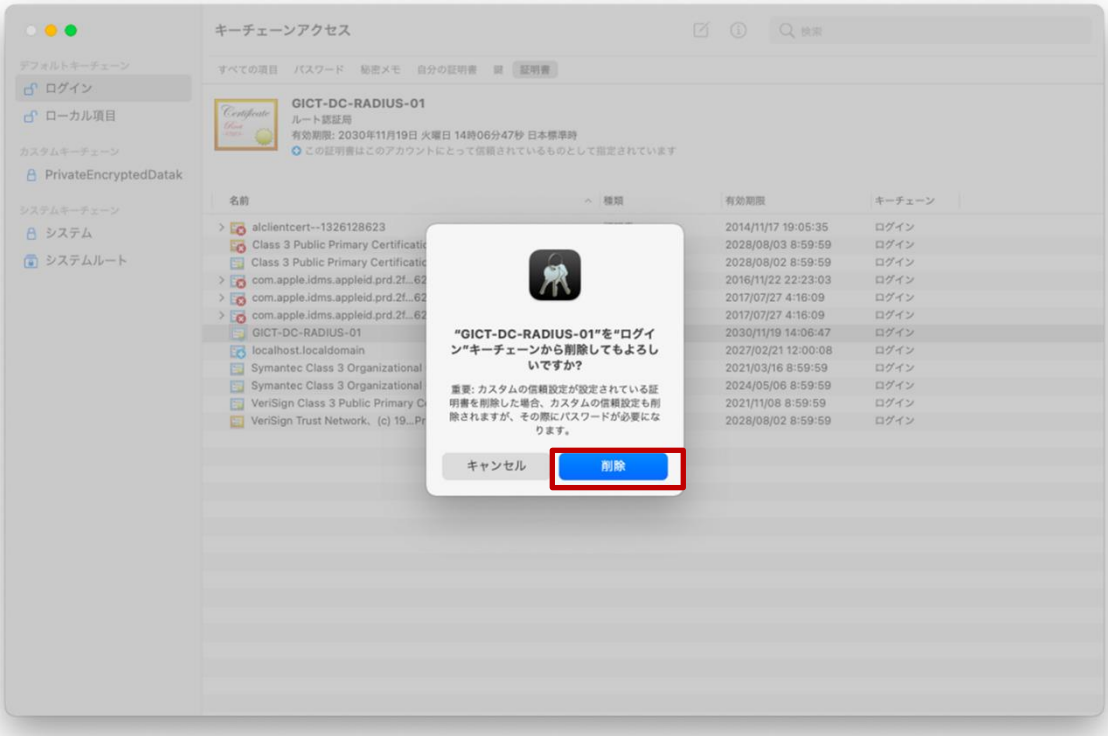


(14) 次にサーバ証明書「GICT-DC-RADIUS-01　※アイコン青色枠」を削除します。証明書一覧の中のサーバ証明書「GICT-DC-RADIUS-01　※アイコン青色枠」にカーソルをあわせて右クリックし「削除」を選択します。

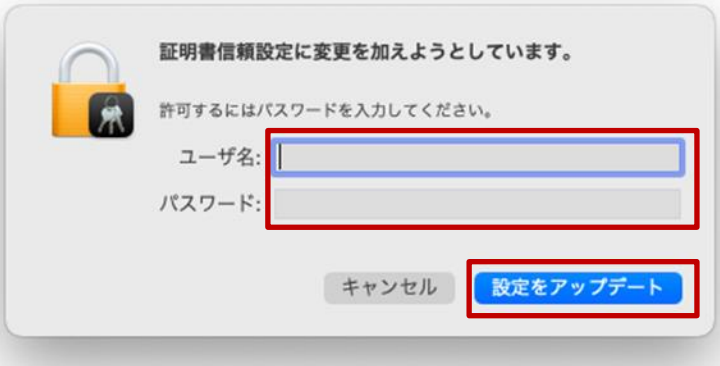
※それ以外の証明書の削除はしないでください！



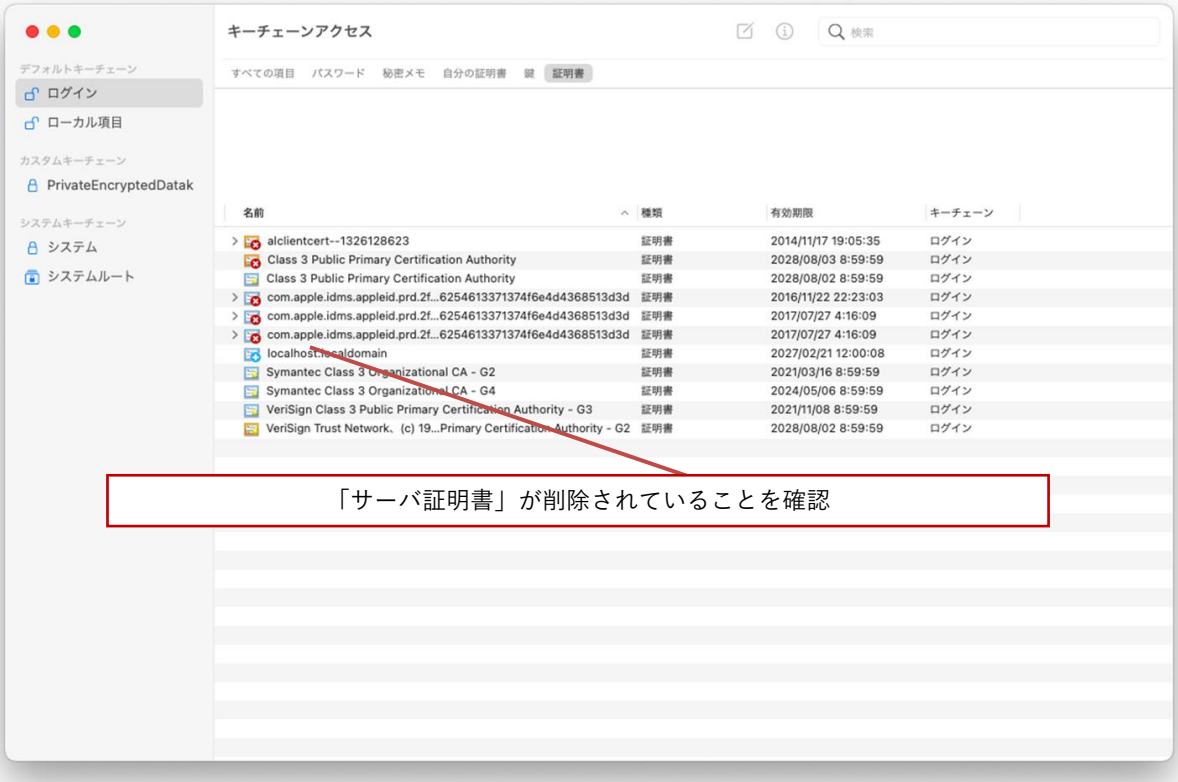
(15) サーバ証明書「GICT-DC-RADIUS-01」の削除を続行する場合は「削除」をクリックします。



(16) 証明書の設定を変更する場合には、ユーザ ID とパスワードを入力する必要があるため、「ユーザ名」と「パスワード」にご自身の端末（BYOD）を起動するときに入力するログイン ID とパスワードを入力して「設定をアップデート」をクリックします。



(17) 証明書一覧の中のサーバ証明書「GICT-DC-RADIUS-01　※アイコン青色枠」証明書が削除されていることを確認します。



(18) 証明書の削除は完了です。

画面上にあるメニューバーの「キーチェーンアクセス」から「キーチェーンアクセスを終了」を選択して閉じてください。

以上

ネットワンシステムズ株式会社
https://www.netone.co.jp/