

HTTPS フィルタリング

目次

1. HTTPS フィルタリング	2
2. 証明書のダウンロード・適用	4
2.1 証明書のダウンロード	4
2.2 証明書の適用 (Chrome/edge の場合)	5
2.3 証明書の適用 (FireFox の場合)	11
2.4 証明書の適用 (Android の場合)	14
2.5 証明書の適用 (iOS の場合)	16
3. 対象外 URL/IP 設定	19
3.1 対象外 URL 設定	19
3.2 対象外 IP 設定	22
3.3 対象外 URL/IP 設定確認	25

1. HTTPS フィルタリング

本項では、HTTPS（暗号化された Web サイト）のフィルタリング設定の手順について記載します。

※HTTPS フィルタリングを使用する場合、特定の Web サイトが閲覧できなくなる場合があります。その際は P.19～24 を参照していただき、そのサイトを対象外に設定してください。

- ① 管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS 通信』をクリックします。



- ② 『利用する』を選択し、『次へ』をクリックします。



③ 内容を確認し、正しければ『確認』をクリックして設定は完了です。

表示/確認 設定 再起動 ログアウト	
設定 ネットワーク設定 WAN 無線LAN 有線LAN ルーティング VPN リモートアクセス 詳細 セキュリティ設定 URLフィルタリング IPフィルタリング 振る舞い検知 HTTPS通信 メール設定 今回のみ接続を許可 ホワイトリスト処理 グループ設定 ブリッジ設定 メンテナンスアドレス アクセス許可リスト 動作切替 一括設定 パスワード変更	セキュリティ設定 HTTPS通信（暗号化通信） デフォルトグループ 設定しますか？ ウェブ (HTTPS) <input type="radio"/> 利用する HTTPS 通信の場合IPフィルタリングを無効にする。 <input type="radio"/> 利用しない <input type="button" value="確認"/> <input type="button" value="戻る"/>

2. 証明書のダウンロード・適用

本項では、HTTPS フィルタリング機能で使用する証明書のダウンロード手順、適用手順について記載します。

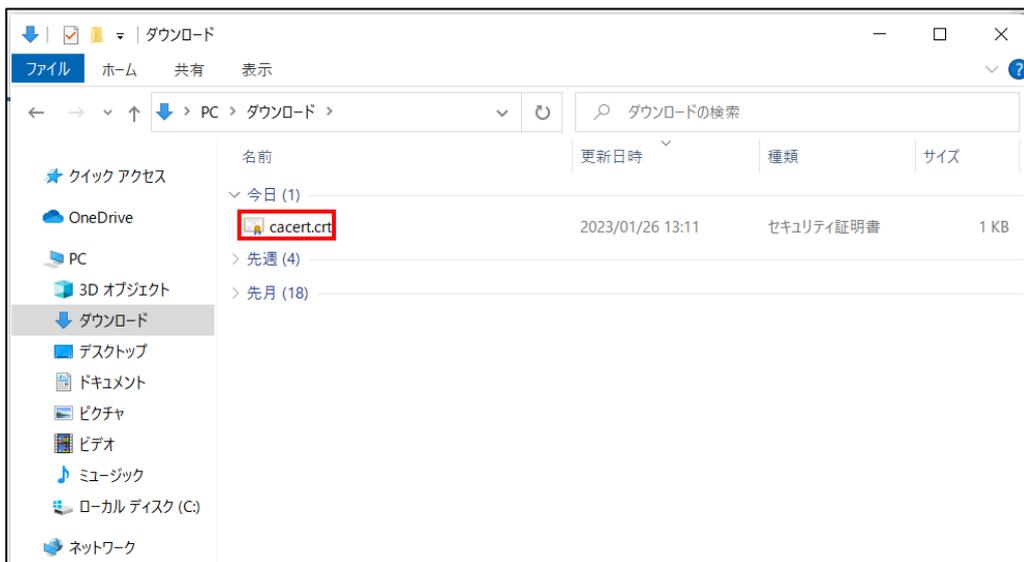
2.1 証明書のダウンロード

本項では、HTTPS フィルタリング機能で使用する証明書をダウンロードする手順について記載します。

① 管理画面にログイン後、左側『情報』をクリックし、『証明書ダウンロード』をクリックします。



② cacert.crt (証明書) がダウンロードされていることを確認して完了です。



2.2 証明書の適用（Chrome/edge の場合）

本項では、ダウンロードした証明書を適用する手順について記載します。

① ダウンロードした証明書をダブルクリックします。



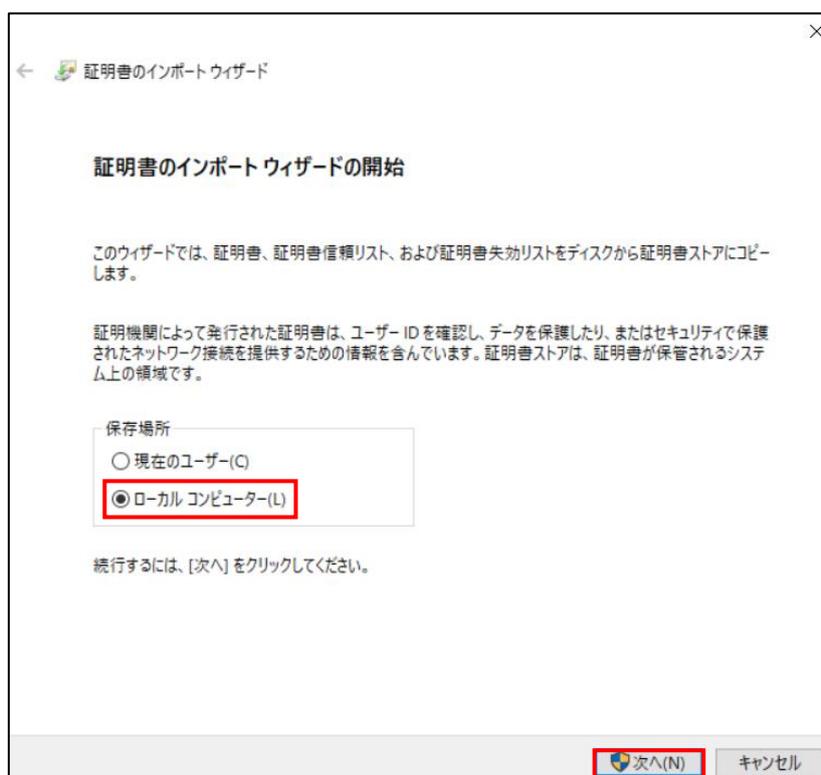
② 『開く』をクリックします。



- ③ 『証明書のインストール』をクリックします。



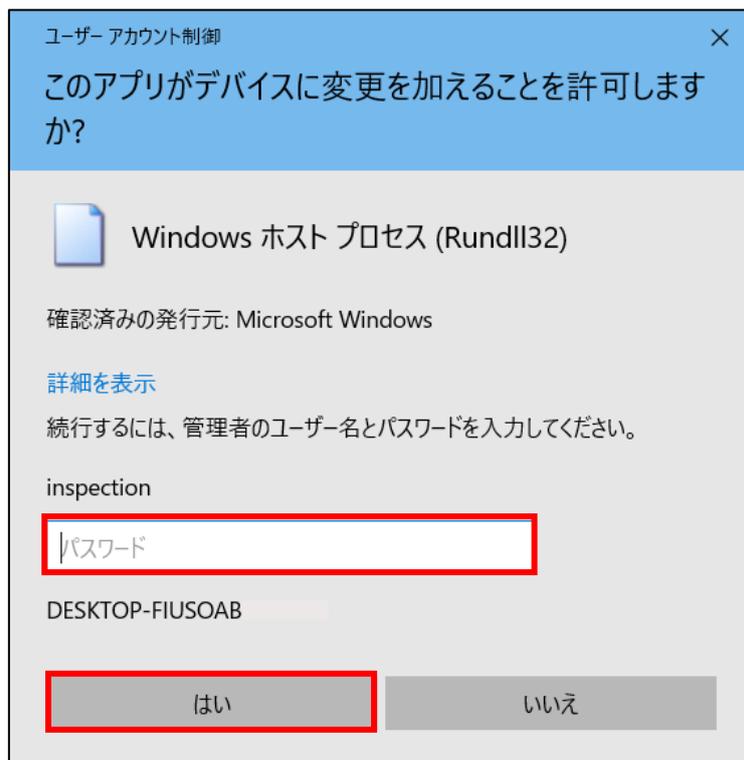
- ④ 『ローカルコンピューター』を選択し、『次へ』をクリックします。



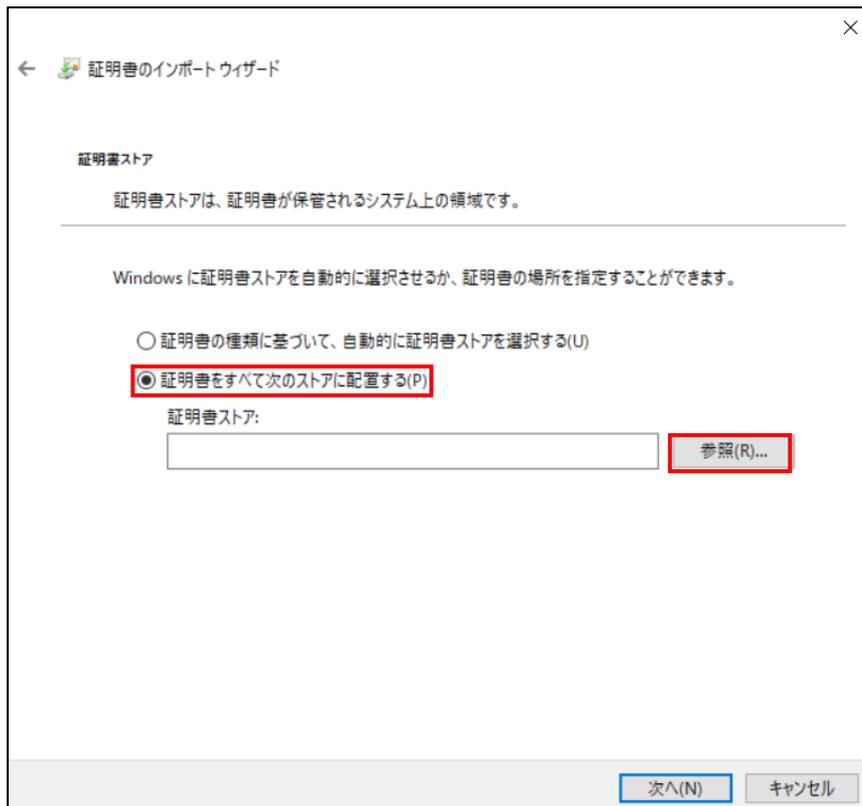
- ⑤ ユーザーアカウント制御が表示されますので、『はい』をクリックします。



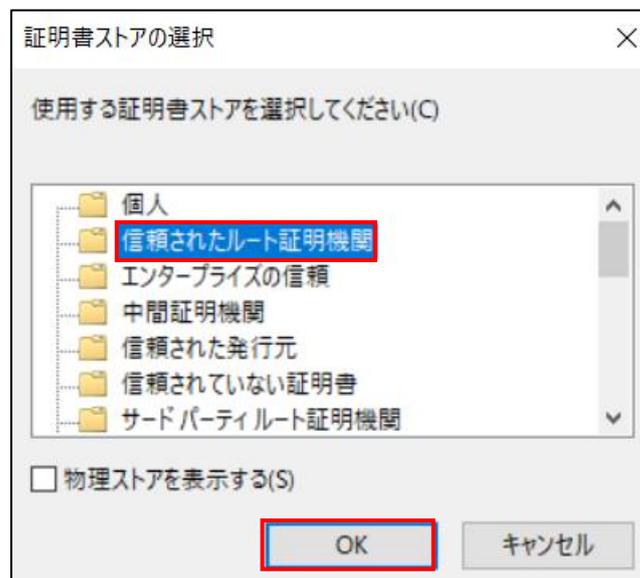
※標準アカウントの場合は、以下のように管理者アカウントのパスワードを要求されます。
管理者の方にご確認ください。



- ⑥ 『証明書すべて次のストアに配置する』を選択し、『参照』をクリックします。



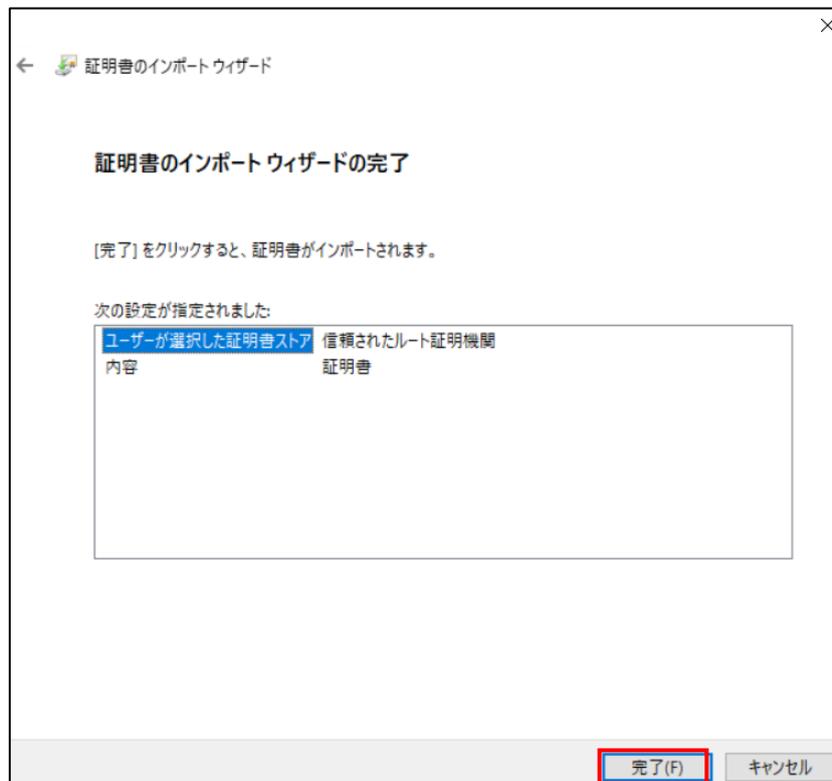
- ⑦ 『信頼されたルート証明機関』を選択し、『OK』をクリックします。



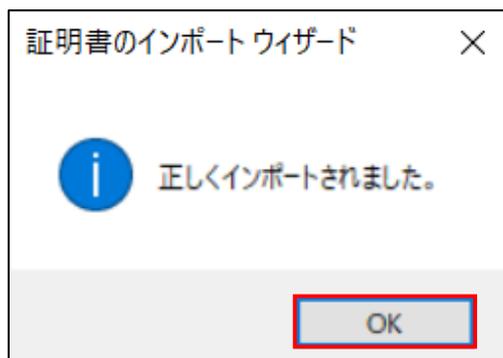
⑧ 『次へ』をクリックします。



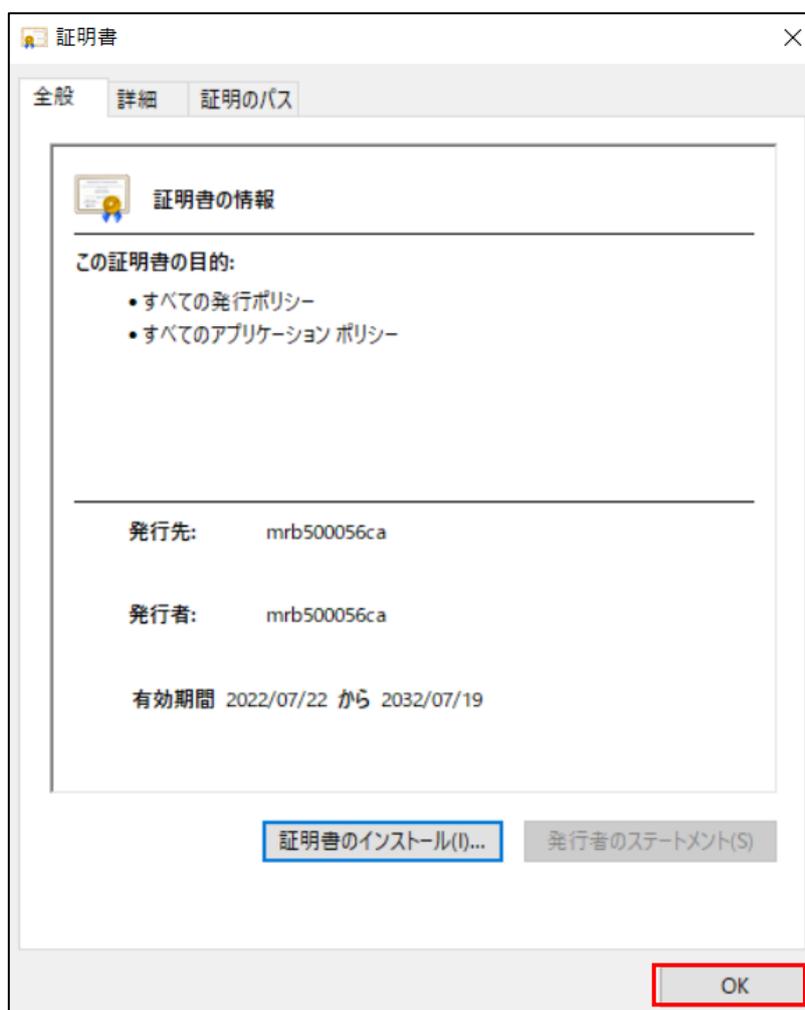
⑨ 『完了』をクリックします。



- ⑩ ポップアップが表示されますので、『OK』をクリックします。



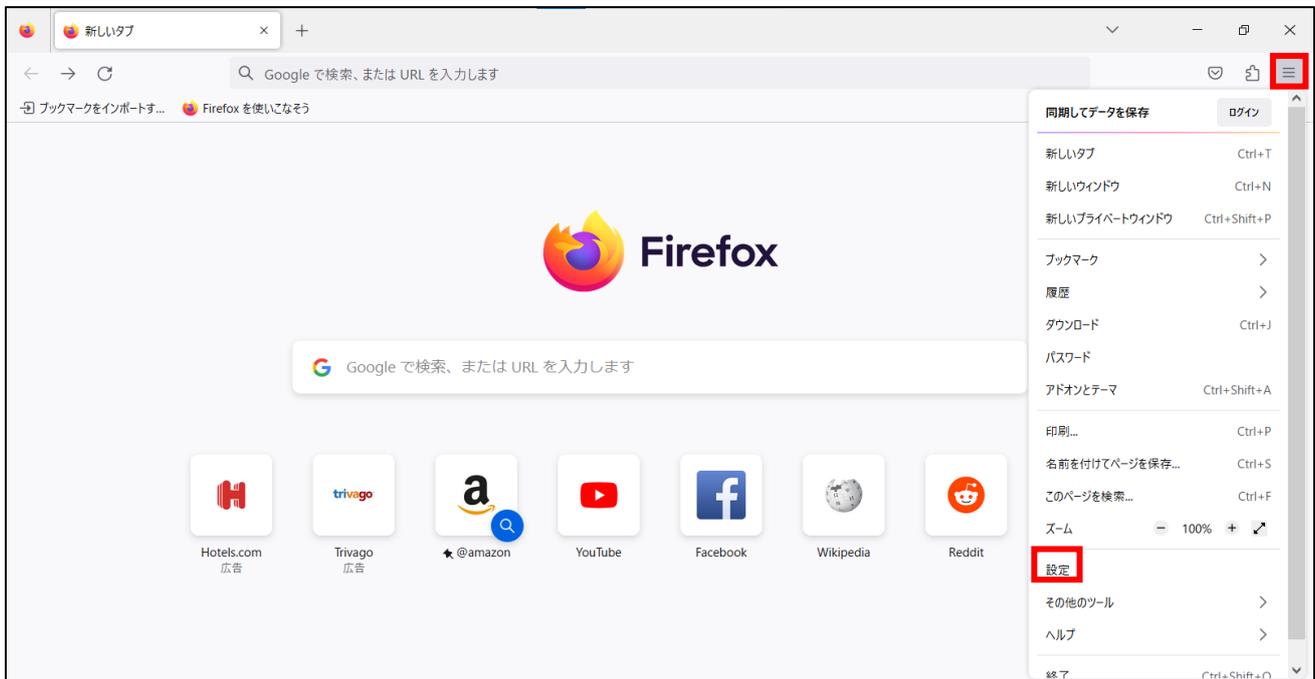
- ⑪ 『OK』をクリックして、証明書の適用作業は完了です。



2.3 証明書の適用 (Firefox の場合)

本項では、ダウンロードした証明書を適用する手順について記載します。

① Firefox のブラウザを開き、右上の『メニュー』より『設定』をクリックします。



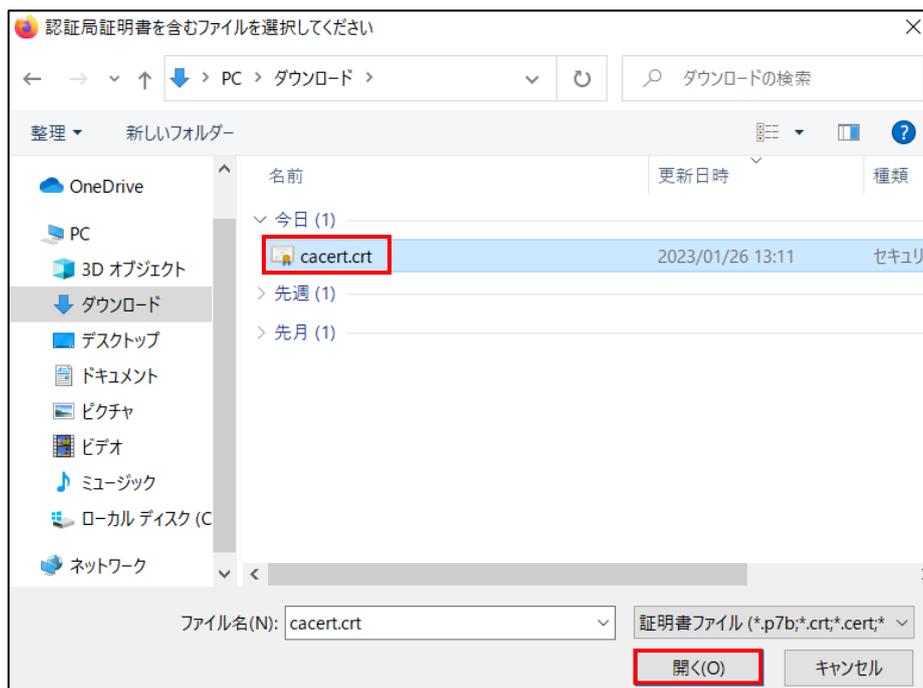
② 『プライバシーとセキュリティ』をクリックし、下へスクロールして、『証明書を表示』をクリックします。



- ③ 『認証局証明書』タブより、『インポート』をクリックします。



- ④ ダウンロードした証明書を選択し、『開く』をクリックします。



- ⑤ 表示される全てのチェックボックスにチェックを入れて『OK』をクリックします。

証明書のインポート

新しい認証局 (CA) を信頼するよう求められています。本当にこの認証局を信頼しますか？

"mrb500056ca" が行う認証のうち、信頼するものを選択してください。

この認証局によるウェブサイトの識別を信頼する

この認証局によるメールユーザーの識別を信頼する

認証局を信頼する場合はその目的に関わらず、認証局の証明書が間違いないこと、認証ポリシーや認証実施規定に問題がないことを確認してください。

証明書を表示 認証局の証明書を審査してください

OK キャンセル

- ⑥ 証明書一覧に発行者名"Technol"の『mrb500056ca』という証明書があることを確認したら、『OK』をクリックして証明書の適用は完了です。

証明書マネージャー

あなたの証明書 認証の決定 個人証明書 サーバ証明書 認証局証明書

認証局を識別するため以下の証明書が登録されています

証明書名と発行者名	セキュリティデバイス	民
TWCA Root Certification Authority	Builtin Object Token	^
TWCA Global Root CA	Builtin Object Token	
▼ Technol		
mrb500056ca	Software Security Device	
▼ Telia Finland Oyj		
Telia Root CA v2	Builtin Object Token	
▼ TeliaSonera		
TeliaSonera Root CA v1	Builtin Object Token	▼

表示...(V) 信頼性を設定...(E) インポート...(M) エクスポート...(X) 削除または信頼しない...(D)

OK

2.4 証明書の適用（Android の場合）

本項では、Android をご利用の場合の証明書を適用する手順について記載します。

① アプリメニューより『設定』をタップします。



② ユーザー設定内の『セキュリティ』をタップします。



③ 認証情報ストレージ内の『(機器メモリーか)SD カードからインストール』をタップします。

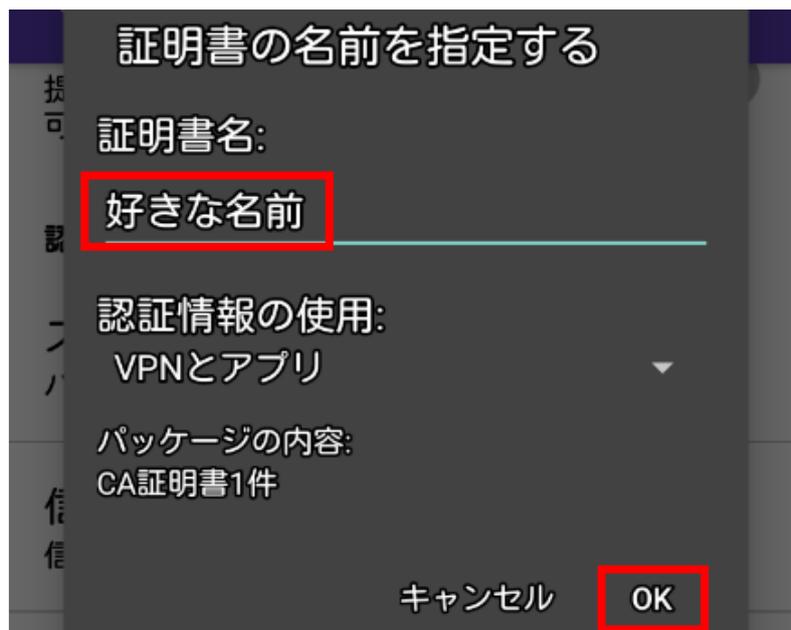


- ④ ”/ Download”フォルダ内から『mrb 機械番号 6 桁.crt』というファイルを探し、タップします。



⑤

- ⑥ 証明書の名前を指定するというポップアップが表示されますので、任意の証明書名を入力し、『OK』をクリックして証明書の適用は完了です。



2.5 証明書の適用 (iOS の場合)

本項では、iOS をご利用の場合の証明書を適用する手順について記載します。

- ① MRB 管理画面で『証明書ダウンロード』をクリック後、ダイアログが表示されますので右上『インストール』をタップします。



- ② 右上『インストール』をタップします。



③ 右上『完了』をタップします。



④ iOS 設定画面を開き、『情報』をタップします。



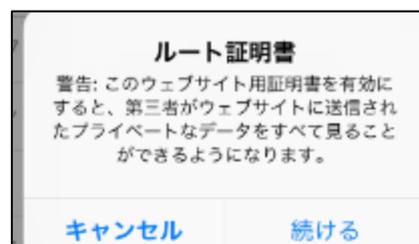
- ⑤ 『証明書信頼設定』をタップします。



- ⑥ 『mrb(6桁の数字)ca』のスイッチをタップします。



- ⑦ 『続ける』をタップして証明書の適用は完了です。



3. 対象外 URL/IP 設定

本項では、ネットバンキング等でサーバ証明書を使用する場合に行う設定について記載します。

3.1 対象外 URL 設定

本項では、URL 指定でサーバ証明書を使用する設定を行う手順について記載します。

- ① 管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS 通信』をクリックします。



- ② 『対象外 URL』をクリックします。



③ 『追加』をクリックします。



④ URL 記入欄にサーバ証明書を使用する接続先の URL を入力し、『追加』をクリックします。



⑤ 内容を確認し、正しければ『追加』をクリックして設定は完了です。

[表示/確認](#) [設定](#) [再起動](#) [ログアウト](#)

設定

ネットワーク設定
[WAN](#)
[無線LAN](#)
[有線LAN](#)
[ルーティング](#)
[VPN](#)
[リモートアクセス](#)
[詳細](#)

セキュリティ設定
[URLフィルタリング](#)
[IPフィルタリング](#)
[振る舞い検知](#)
[HTTPS通信](#)
[メール設定](#)
[今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定
[メンテナンスアドレス](#)
[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

セキュリティ設定

HTTPS 対象外URL

デフォルトグループ

設定しますか?

URL technol.co.jp

追加
戻る

3.2 対象外 IP 設定

本項では、IP 指定でサーバ証明書を使用する設定を行う手順について記載します。

- ① 管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS 通信』をクリックします。



- ② 『対象外 IP』をクリックします。



- ③ 『追加』をクリックします。

The screenshot shows the 'セキュリティ設定' (Security Settings) page. The left sidebar contains a navigation menu with categories like 'ネットワーク設定' (Network Settings), 'セキュリティ設定' (Security Settings), 'ブリッジ設定' (Bridge Settings), and '一括設定' (Batch Settings). The main content area is titled 'セキュリティ設定' and includes sections for 'HTTPS 対象外IP' (HTTPS Excluded IP) and 'デフォルトグループ' (Default Group). Under 'デフォルトグループ', there are buttons for 'ファイルの選択' (Select File), 'アップロード(置換)' (Upload (Replace)), and 'アップロード(追加)' (Upload (Add)). Below this is a 'ダウンロード' (Download) button. At the bottom of the main content area, there are buttons for '戻る' (Back), '消去' (Delete), '追加' (Add), '修正' (Edit), and '削除' (Delete). The '追加' button is highlighted with a red box.

- ④ IP 記入欄にサーバ証明書を使用する接続先の IP アドレスまたはネットワークアドレスを入力し、『追加』をクリックします。

The screenshot shows the 'セキュリティ設定' (Security Settings) page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'セキュリティ設定' and includes sections for 'HTTPS 対象外IP' (HTTPS Excluded IP) and 'デフォルトグループ' (Default Group). Under 'デフォルトグループ', there is a text input field labeled 'IP' which is highlighted with a red box. Below the input field are buttons for '消去' (Delete) and '戻る' (Back). To the right of the '消去' button, the '追加' (Add) button is highlighted with a red box.

⑤ 内容を確認し、正しければ『追加』をクリックして設定は完了です。

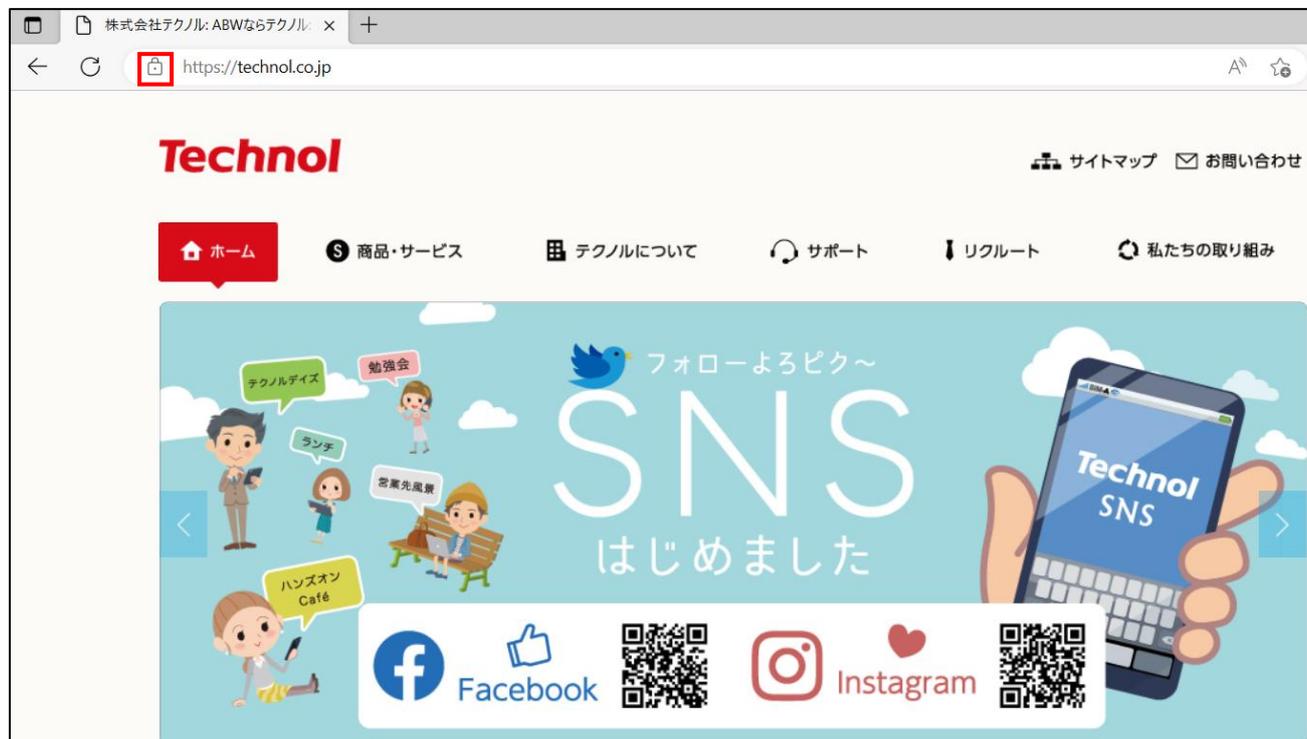
[表示/確認](#) [設定](#) [再起動](#) [ログアウト](#)

<p>設定</p> <p>ネットワーク設定 WAN 無線LAN 有線LAN ルーティング VPN リモートアクセス 詳細</p> <p>セキュリティ設定 URLフィルタリング IPフィルタリング 振る舞い検知 HTTPS通信 メール設定 今回のみ接続を許可</p> <p>ホワイトリスト処理</p> <p>グループ設定</p> <p>ブリッジ設定 メンテナンスアドレス アクセス許可リスト</p> <p>動作切替</p> <p>一括設定</p> <p>パスワード変更</p>	<h3 style="text-align: center;">セキュリティ設定</h3> <p>HTTPS 対象外IP</p> <p>デフォルトグループ</p> <p>設定しますか？</p> <p>IP 202.230.200.207/32</p> <div style="text-align: right; margin-top: 20px;"><input style="border: 2px solid red; padding: 2px 10px;" type="button" value="追加"/> <input style="padding: 2px 10px;" type="button" value="戻る"/></div>
--	---

3.3 対象外 URL/IP 設定確認

本項では、対象外に設定した URL/IP でサーバの証明書が利用されていることを確認する手順について記載します。

① Web サイトにアクセスし、URL バー左の『鍵マーク』をクリックします。



② 『接続がセキュリティで保護されています』をクリックします。



- ③ 証明書のアイコンをクリックします。



- ④ 対象外に設定されている場合は、以下のように表示され、サーバの証明書が利用されていることが分かります。



- ⑤ 対象外に設定されていない場合は、以下のように表示され、MRB の証明書が利用されていることが分かります。

証明書ビューアー: edge01.yahoo.co.jp

全般(G) 詳細(D)

発行先

共通名 (CN)	edge01.yahoo.co.jp
組織 (O)	Yahoo Japan Corporation
組織単位 (OU)	<Not Part Of Certificate>

発行者

共通名 (CN)	mrb500056ca
組織 (O)	Technol
組織単位 (OU)	MR

有効期間

発行日	2023年1月29日 日曜日 17:09:29
有効期限	2024年1月29日 月曜日 17:09:29