HazardFilter Chromebook で Web アクセスを行う際の設定と注意点

株式会社 YE DIGITAL

【 質問 】

HazardFilter で、Chromebook で Web アクセスを行う際の設定と注意点を教えてください。

【 回答 】

Chromebook で Web アクセスを行う際の設定

※今後 Chromebook の仕様変更に伴い下記設定手順が変更になる可能性がございます。予めご了承ください。

※Chrome Enterprise（Chrome Education/Chrome Nonprofit）をご利用の場合を前提としています。
その場合、[Google 管理コンソール]にて、遠隔設定が可能です。

１．プロキシの設定

HazardFilter でフィルタリングを行うために必要な設定です。

[Google 管理コンソール]の[端末管理]-[ネットワーク] の各種ネットワーク接続、または、[Google 管理コンソール]の[端末管理]-[Chrome 管理]-[ユーザー設定]-[ネットワーク] で設定します。

端末管理のネットワークに設定した場合は、端末を利用する全てのユーザー、および Chrome OS が行う通信にプロキシが適用されます。

ユーザー設定のネットワークに設定した場合は、指定のユーザーアカウントに対して適用されため、ゲストユーザーには適用されません（ゲストユーザーの端末利用は許可しないことを推奨します）。

バックグラウンドで Chrome OS が行う通信の一部にも、ユーザー設定のプロキシが適用されない場合があります。

２．認証局証明書の登録

HTTPS サイトへのアクセス規制時、および HTTPS デコードを行う場合に、証明書警告を非表示化するための設定です。

認証局証明書は、[Google 管理コンソール] の[端末管理]-[ネットワーク]-[証明書] で登録します。

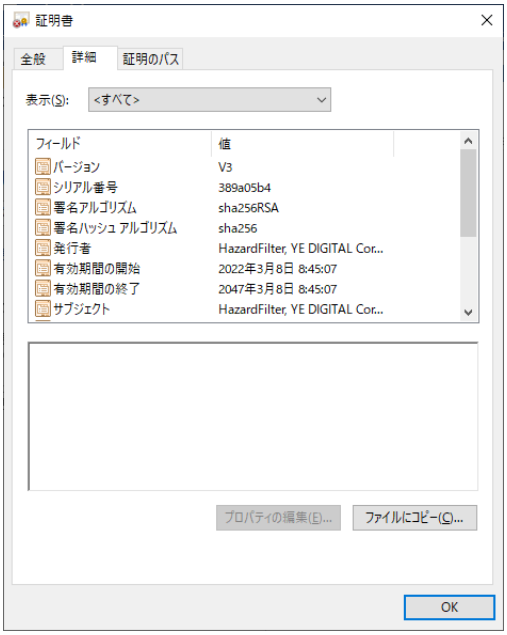
登録後に「HTTPS の認証局としてこの証明書を使用します。」をチェックしてください。
ここで登録した証明書は、指定のユーザアカウントに対して適用されます。
バックグラウンドで Chrome OS が行う通信の一部には、証明書が適用されない場合があります。

※ 証明書は PEM 形式（Base64 形式）で登録する必要があります。
HazardFilter の管理画面にログインして [共通アクセス管理]-[HTTPS 規制設定] から DER 形式の証明書

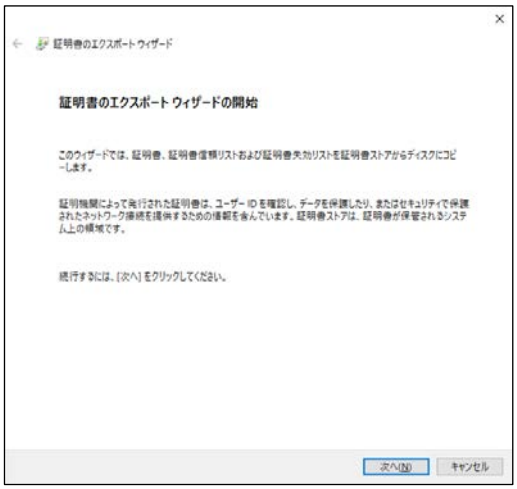
をダウンロード後に、openssl コマンド、または以下の手順で形式変換を行ってください。

1．cacert.cer ファイルを Windows 上でダブルクリックで開きます。

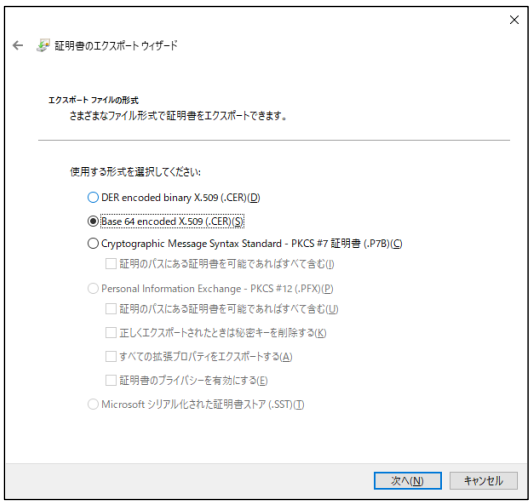
2．証明書の[詳細]タブで [ファイルにコピー] をクリックします。



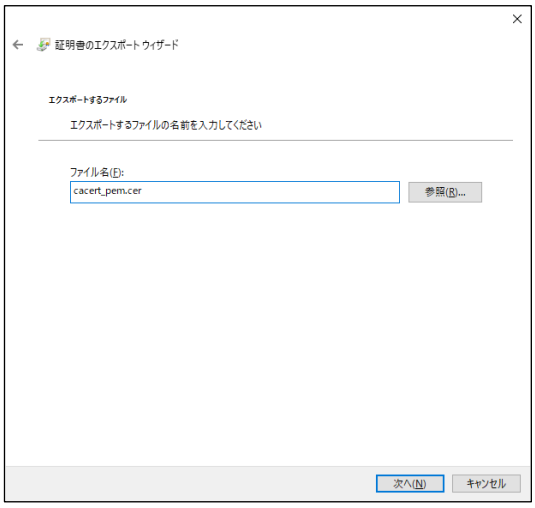
3．[次へ] をクリックします。



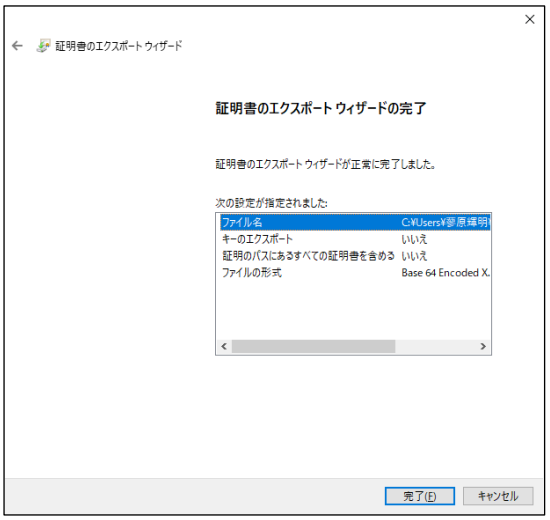
4．ファイルの形式に［Base 64 encoded X.509（.CER）］を選択して[次へ] をクリックします。



5．ファイル名を入力して[次へ] をクリックします。



6．[完了] をクリックします。



■Chromebook で Web アクセスを行う際の注意点

・NTLM 認証（Windows NT LAN Manager 認証）は利用できません。

HazardFilter でのユーザー識別には、IP アドレス認証、または Basic 認証(※)をご利用ください。

(※)Chrome ブラウザ以外の通信では認証が行えません。

・プロキシの認証フォームを繰り返し表示させたくない場合は、認証情報を Chrome 上に保持してください。

Chrome Enterprise をご利用の場合は［端末管理]-[Chrome 管理]-[ユーザー設定]-[セキュリティ］でパスワードマネージャを有効にする必要があります。

・プロキシ経由の通信がエラーとなる場合は、Chrome のプロキシ設定にバイパスリストを追加、または HazardFilter 側でのフィルタリングバイパス、HTTPS デコード除外、接続許可ポートの追加などが必要となります。

設定方法は添付 URL をご参照ください。

【参考情報】プロキシ経由でエラーが確認された通信先の例

m.google.com　HTTPS デコード不可　※Chrome Enterprise のポリシー更新に必要な通信先

mtalk.google.com　HTTPS 通信にデフォルト以外のポート（:5228）を使用

talk.google.com　HTTPS 通信にデフォルト以外のポート（:5222）を使用

talkx.l.google.com　HTTPS 通信にデフォルト以外のポート（:5222）を使用

talk.google.com　脆弱なプロトコル（SSLv2）を使用

talkx.l.google.com　脆弱なプロトコル（SSLv2）を使用

*.googleapis.com　Basic 認証不可

www.gstatic.com　Basic 認証不可

clients*.google.com　Basic 認証不可

※上記例は今後変更になる場合がございます。

・G Suite をご利用の場合は、必要に応じて各サービスで使用されるドメインへのアクセス許可やフィルタリングバイパス、HTTPS デコード除外の設定を行ってください。

【参考情報】G Suite のサービスで使用されるドメインの例

google.com　ポータル関連の通信

*.google.com　各種サービス関連の通信

*.googleapis.com　システムコンテンツ関連の通信

*.google.co.jp　検索ポータル、ニュース関連の通信

*.youtube.com　Youtube 関連の通信

*.gstatic.com　システムコンテンツ関連の通信

*.googleusercontent.com　システムコンテンツ関連の通信

.gvt.com　　システムコンテンツ、ビーコン関連の通信

*.doubleclick.net　　システムコンテンツ関連の通信

*.google-analytics.com　　Google Analytics の通信

*.googlevideo.com　　Youtube の動画ファイルの通信

※上記例は今後変更になる場合がございます。

ユーザ登録で IP レンジを登録して運用している場合、HazardFilter に登録している IP レンジ以外の PC から、アクセスすると認証画面が表示されず、未登録ユーザのルールが適用されます。