セキュリティ対策の強化について

当行では、昨今のインターネットバンキングを利用した悪質な犯罪が急増している状況に対応し、より安心いただける環境をご提供するため、インターネットバンキングサービスのセキュリティ対策の強化を目的として、Ｗｅｂサイトのセキュリティ製品（インターネットバンキングへの攻撃と思われるアクセスを検知・遮断する仕組み）を令和５年２月２０日(月)より導入いたします。

導入にあたり、お客さまがお使いのセキュリティ対策ソフトによる誤検知等により正常に利用できなくなる可能性がございます。つきましては、該当のセキュリティ対策ソフトをお使いのご利用者さまは、下記の回避手順をご確認いただき、設定の変更をお願いします。

１．対応が必要となるセキュリティ対策ソフト

・カスペルスキー

・SOPHOS

・AppGuard

２．設定手順

【カスペルスキーの場合】

①タスクトレイにあるカスペルスキーのアイコンをクリック。

②「設定」をクリック。

③「セキュリティ設定」をクリック。

④「ネットワーク設定」をクリック。

⑤「信頼するアドレス」をクリック。

⑥ドメイン名の追加を実施。「www3.suitebank3.finemax.net」を入力、ステータスが有効であることを確認して、追加をクリック。

⑦信頼するアドレスに追加が完了。

【SOPHOS の場合】

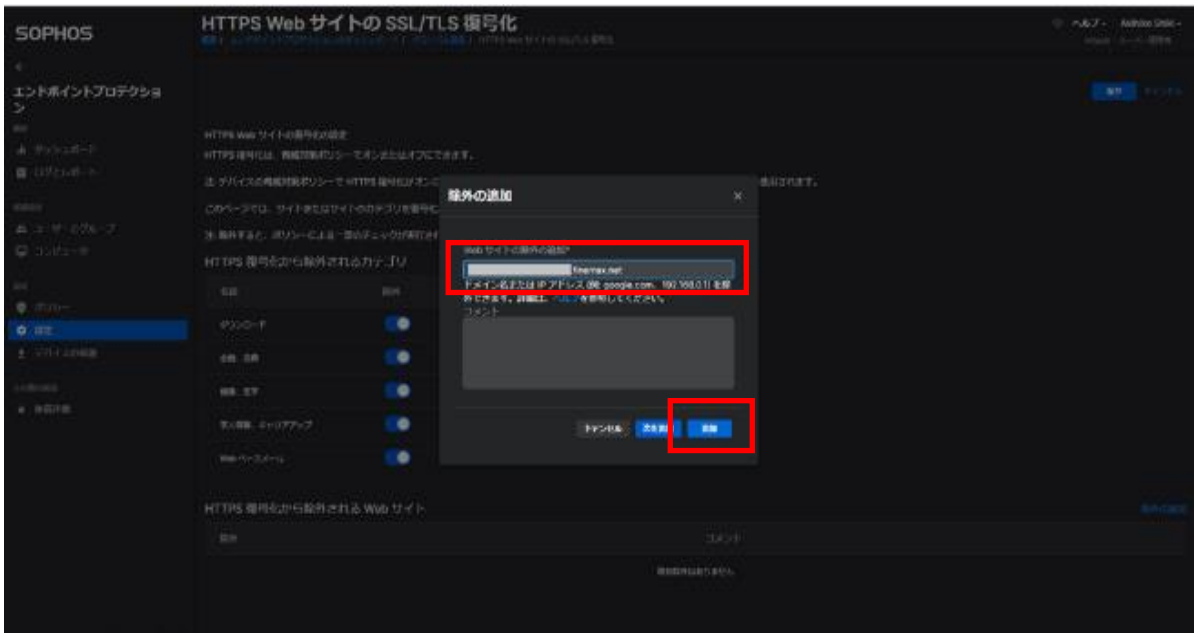
「HTTPS Web サイトの SSL/TLS 復号化」の設定値をデフォルト値(OFF)から変更し（ON）にしている場合にエラー事象が発生します。

①ブラウザを起動し、「SOPHOS」の設定画面にアクセス。

②「設定」より「HTTPS Web サイトの SSL/TLS 復号化」メニューを開く。

③「除外の追加」をクリック。

④「www3.suitebank3.finemax.net」を入力し、「追加」をクリック。

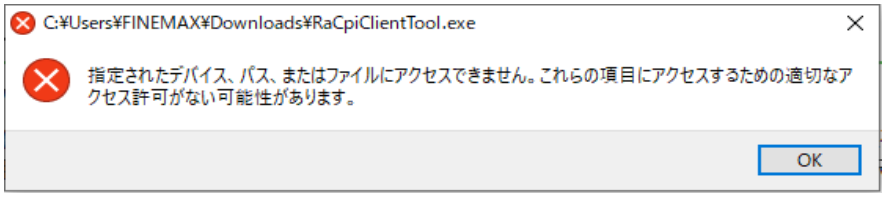


⑤ドメインが追加されたことを確認。

⑥上部の保存ボタンを押下して、設定を保存して完了。

【AppGuard の場合】

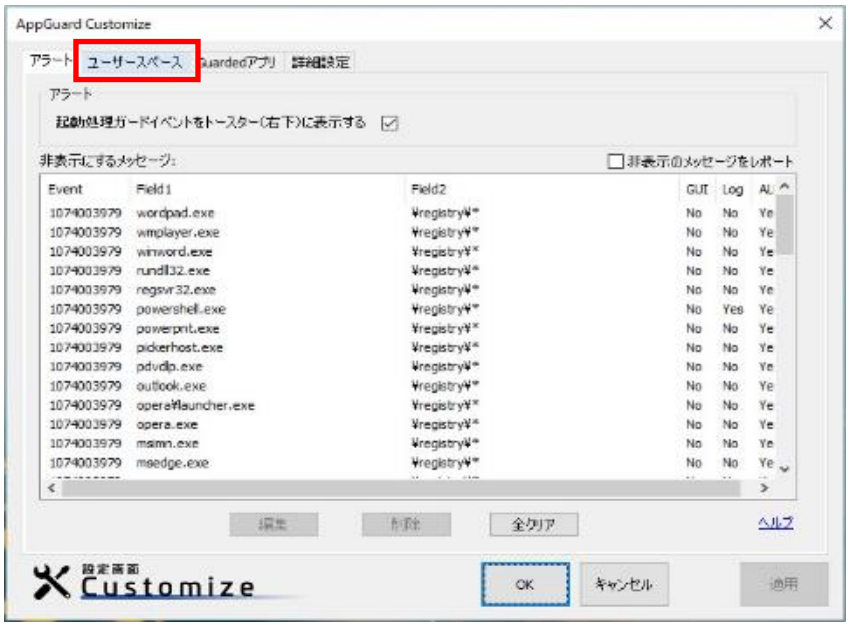
セキュリティ対策ソフト「AppGuard」をインストールした端末で、電子証明書取得実行画面または電子証明書更新実行画面の「ダウンロード」でダウンロードした専用アプリケーション（RaCpiClientTool.exe）を起動すると、以下のダイアログが表示され、起動することができません。



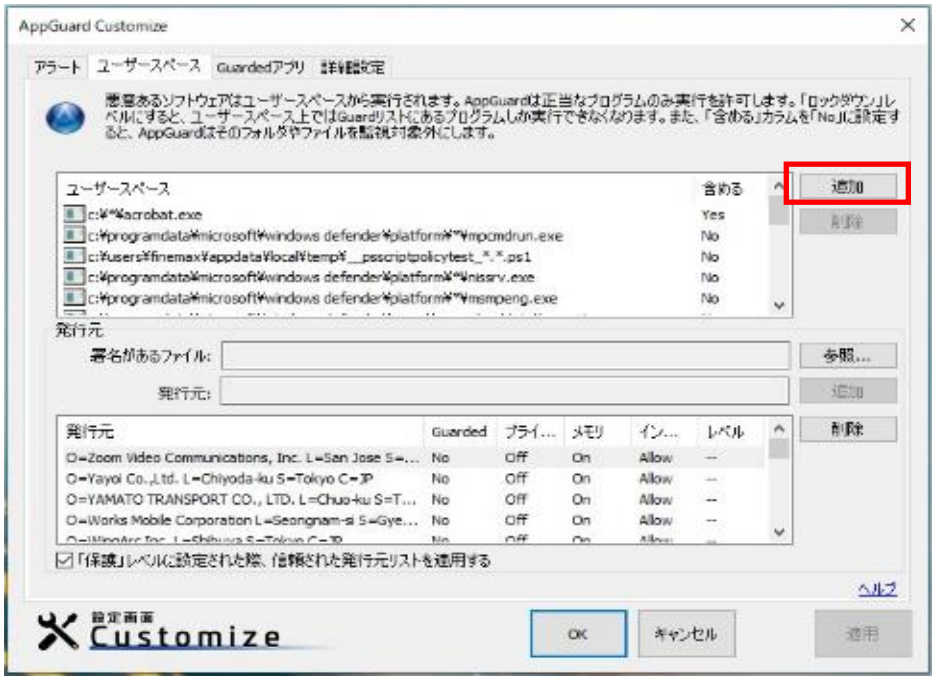
①AppGuard のメイン画面を起動。

②AppGuard メイン画面の「設定」ボタンをクリック。

③「AppGuard Customize」画面で「ユーザースペース」タブをクリック。



④「追加」ボタンをクリック。

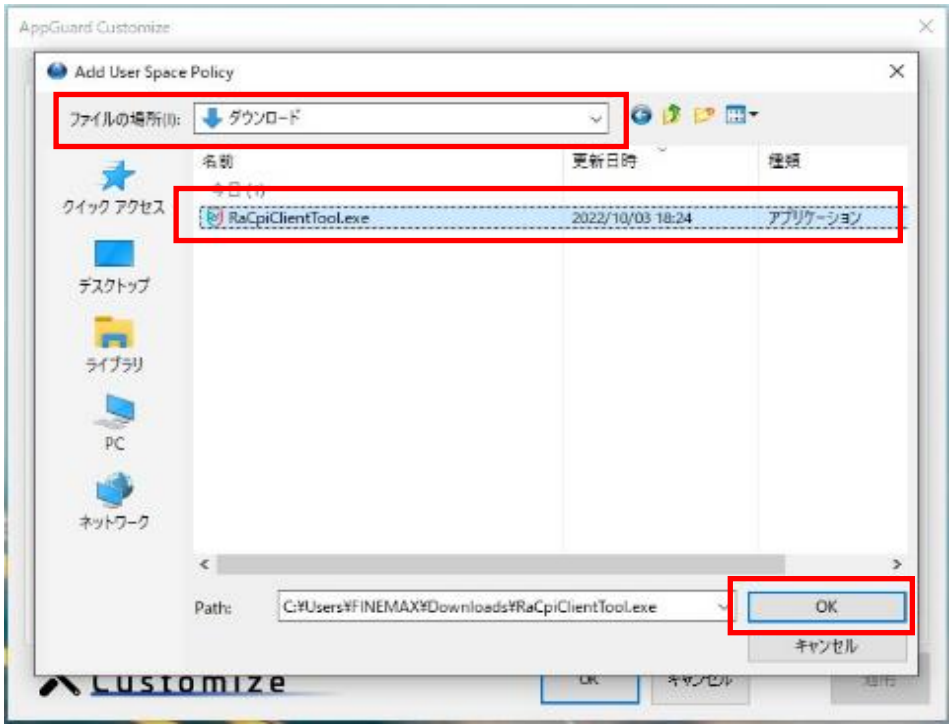


⑤「Add User Space Policy」画面で以下のファイルを選択し、「OK」ボタンをクリック。

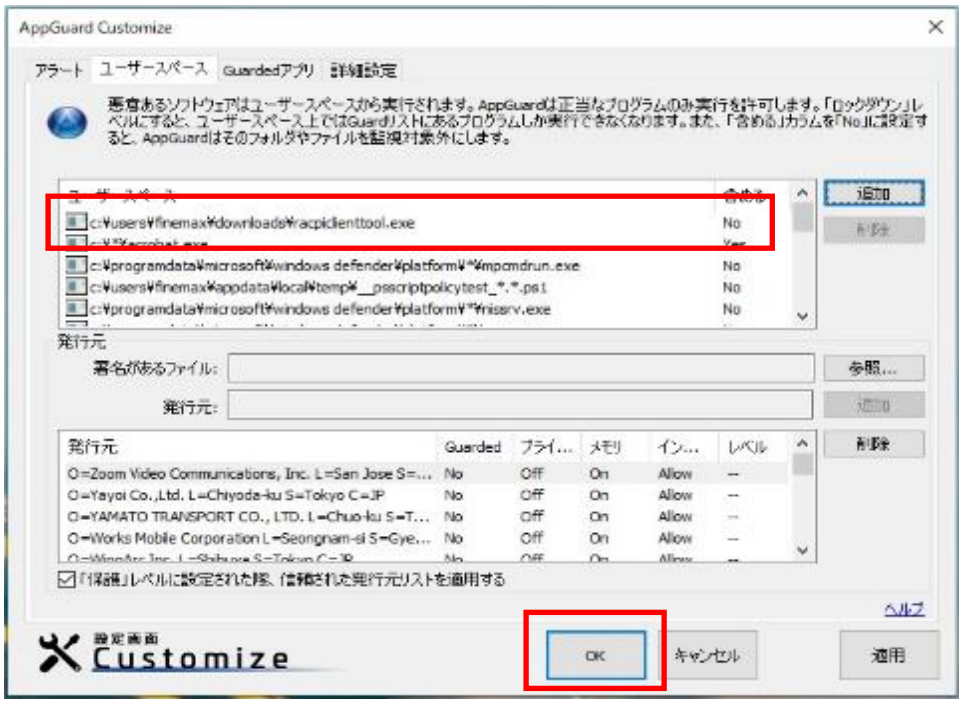
・ファイルの場所：ダウンロード

・ファイルの名前：RaCpiClientTool.exe

※「ファイルの場所」は専用アプリケーションをダウンロードした場所を指定してください。



⑥「ユーザースペース」の一覧に専用アプリケーションが追加されたことを確認し、「OK」ボタンをクリック。



⑦AppGuard メイン画面に戻ったら「×」で終了します。

【本件に関するお問い合わせ】
かがわＥＢセンター
フリーダイヤル 0120-100-459（通話料無料）
平日（銀行営業日）　9:00～17:00