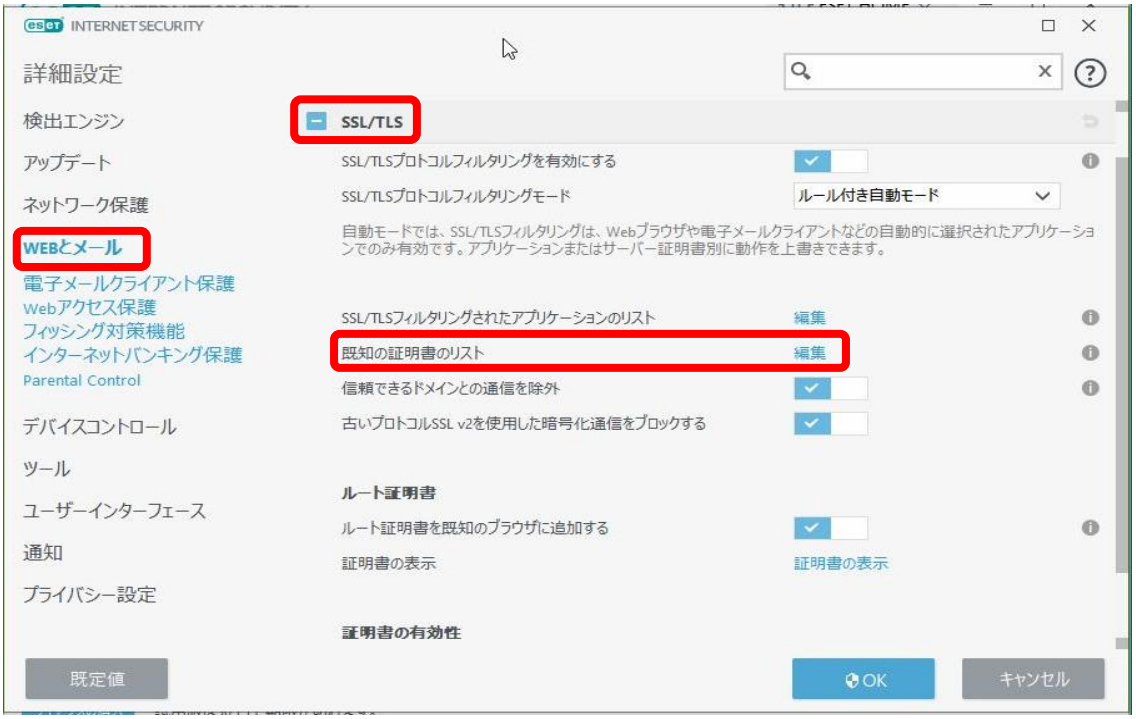
セキュリティ対策ソフトの回避策（ESET、カスペルスキー）

１．ESET の回避策

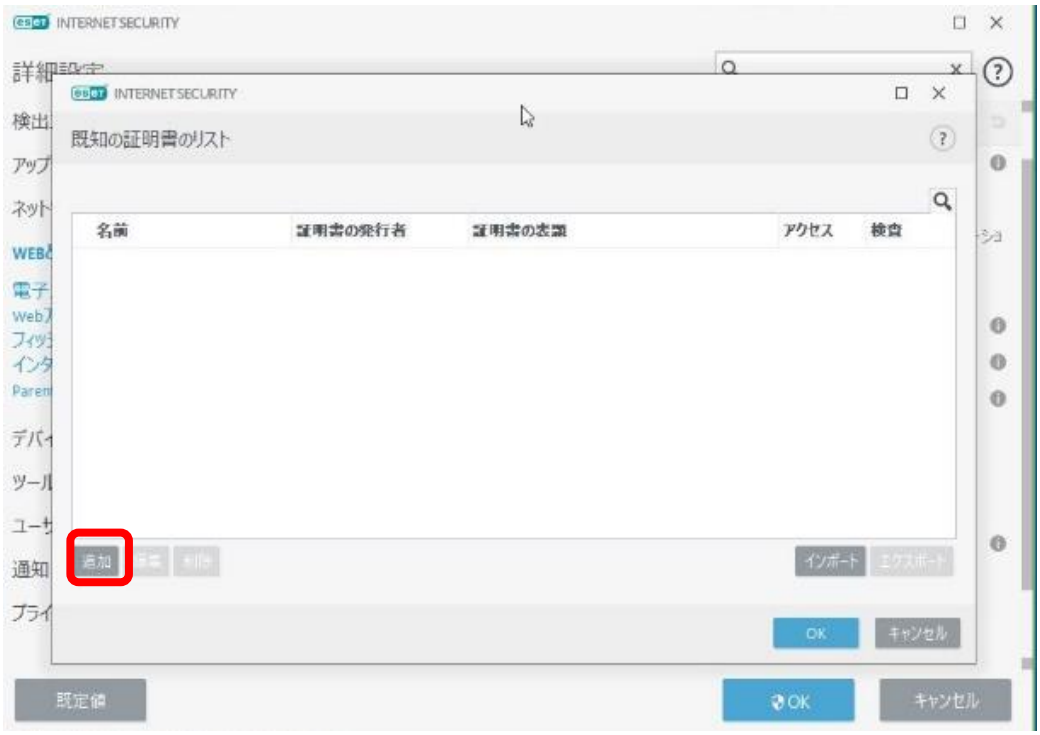
ESET 社からの回答に基づいた回避策によって本事象が発生しなくなることを確認しております。
回避策は以下の設定手順を実施ください。

＜設定手順＞
①ESET を開き、[設定]-[詳細設定]をクリック

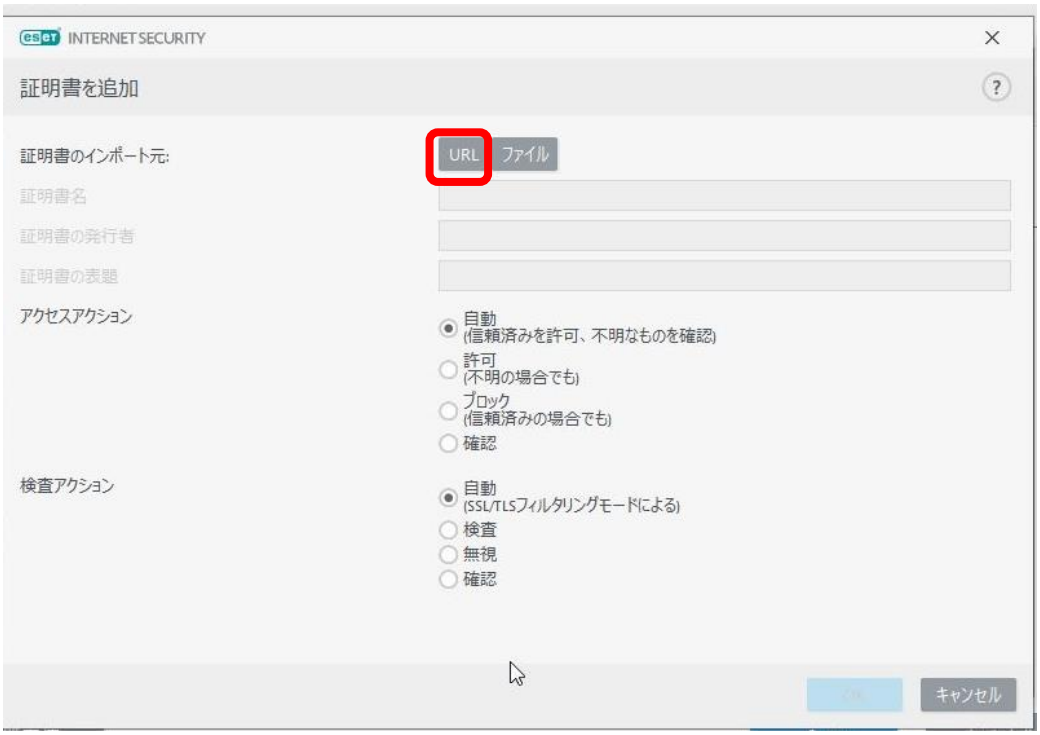
②[WEB とメール]-[SSL/TLS]の既知の証明書リストの[編集]をクリック



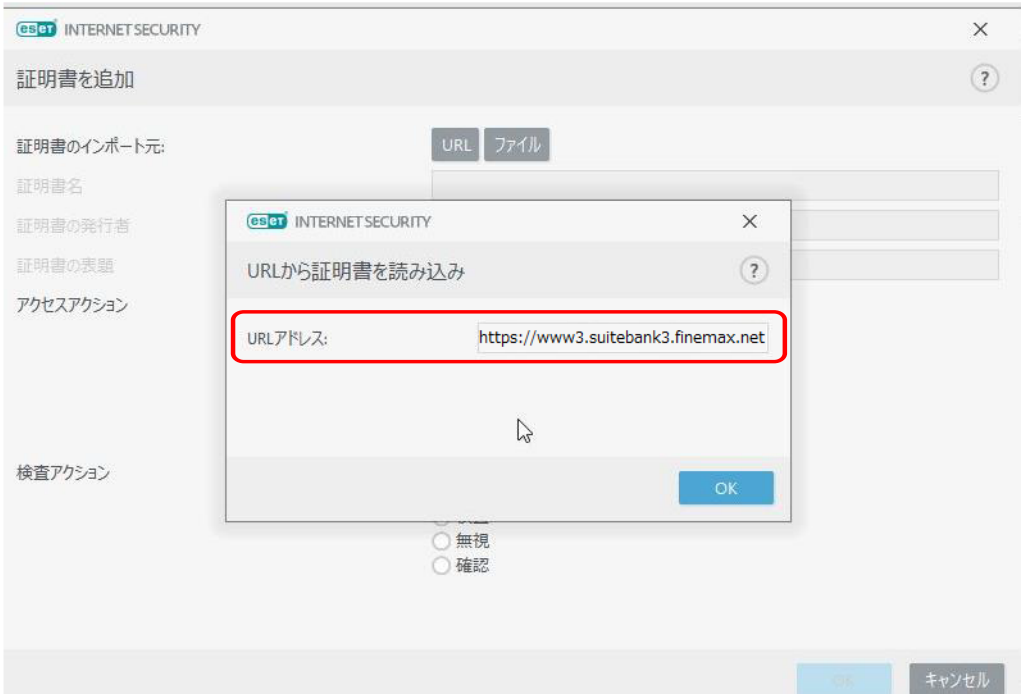
③[既知の証明書のリスト]が表示されたら[追加]をクリック



④[証明書を追加]が表示されたら、証明書のインポート元の「URL」をクリック



⑤[URL から証明書を読み込み]が表示されたら、URL アドレスに[https://www3.suitebank3.finemax.net]を指定し[OK]をクリック



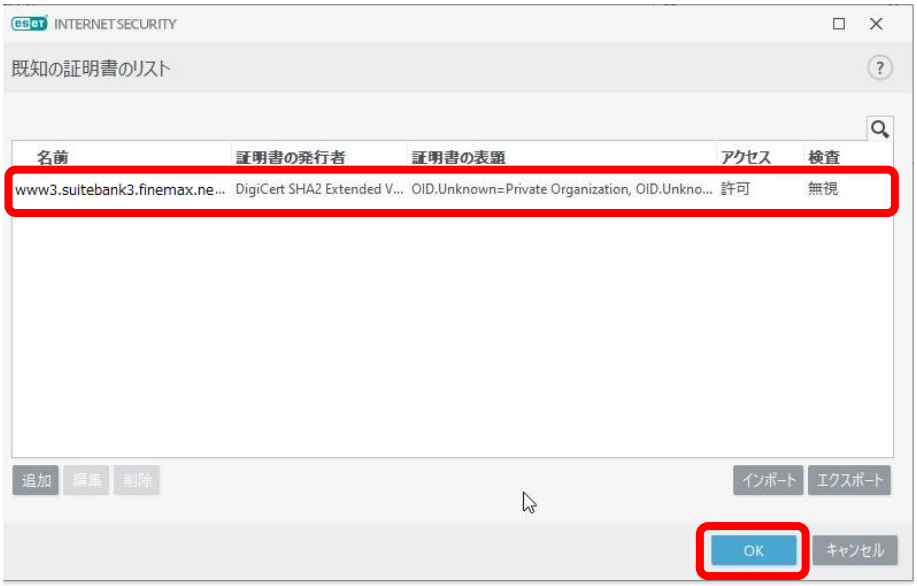
⑥証明書のインポート元の[証明書名][証明書の発行元][証明書の表題]の証明書情報を確認できたら、[アクセスアクション:許可]「検査アクション:無視」を選択し「OK」をクリック

⑦既知の証明書リストで以下が確認できたら[OK]をクリック

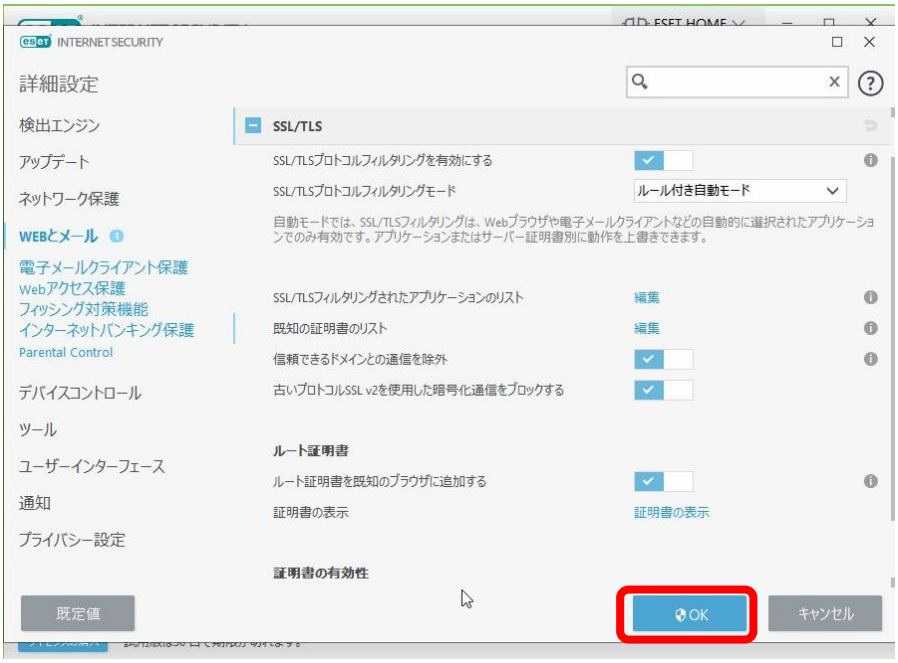
・[www3.suitebank3.finemax.net]の証明書が追加できたこと

・[アクセスアクション:許可]になっていること

・「検査アクション:無視」になっていること



⑧詳細設定が表示されたら「OK」をクリック



2．カスペルスキーの回避策

公開されている「カスペルスキー」のサポート情報に基づいた回避策によって本事象が発生しなくなることを確認しております。

回避策は、https://support.kaspersky.com/KIS/2018/ja-JP/157530.htmを実施ください。
また、以下に設定手順を示します。

＜設定手順＞

①ネットワーク設定より、「信頼するアドレスを選択」。

②ドメイン名の追加を実施。「https://」以降のドメイン部を入力、ステータスが有効であることを確認して、追加を押下。

③信頼するアドレスに追加が完了。

－ 以上 －