

Microsoft Office Outlook編

改版履歴			
版数	日付	内容	担当
V.1.0	2015/4/1	初版	NII
V.1.1	2016/12/26	認証局「NII Open Domain S/MIME CA」の追加に伴う修正	NII
V.2.0	2018/2/26	対応環境をMicrosoft Office Outlook 2013以上に変更	NII
V.2.1	2019/8/9	暗号化アルゴリズムを[3DES]から[AES(256-bit)]に変更	NII
V.2.2	2021/10/22	証明書発行元を変更	NII

目次

- 1. S/MIME証明書のインストール手順
 - 1-1. 動作環境について
 - 1-2. 前提条件
 - 1-3. インストール手順
- 2. デジタル署名付きメールの送信
 - 2-1. デジタル署名付きメールの送信手順
 - 2-2. 送信したデジタル署名付きメールの確認手順

1. S/MIME証明書のインストール手順

1-1. 動作環境について

本マニュアルでは以下の環境における操作手順のみ記載しています。

対応環境
Microsoft Office Outlook 2013以上

1-2. 前提条件

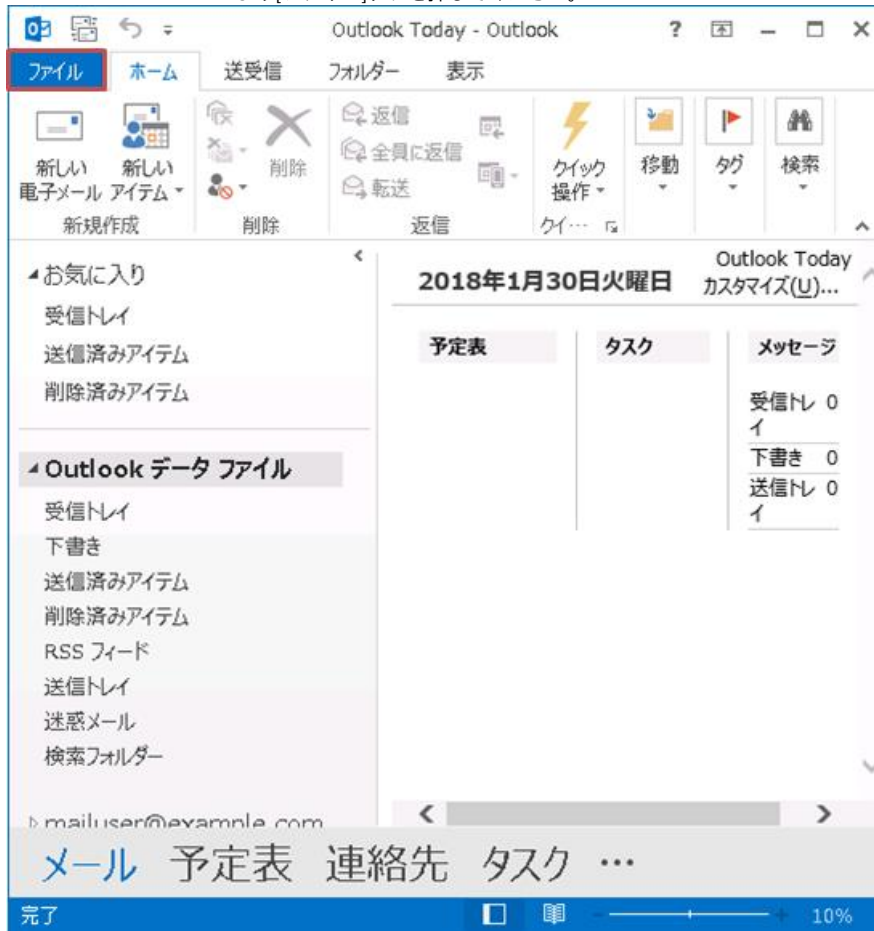
Microsoft Office OutlookでS/MIME証明書を使用する場合の前提条件について記載します。S/MIME証明書を利用する環境に合わせて、適宜手順の読み替えを行ってください。（本マニュアルではMicrosoft Office Outlook 2013での実行例を記載しております。）

前提条件
1. S/MIME証明書がWebブラウザへインストールされていること (Webブラウザへのインストールマニュアル_Microsoft Internet Explorer編に記載) 2. Microsoft Office Outlook 2013以上がインストールされていること

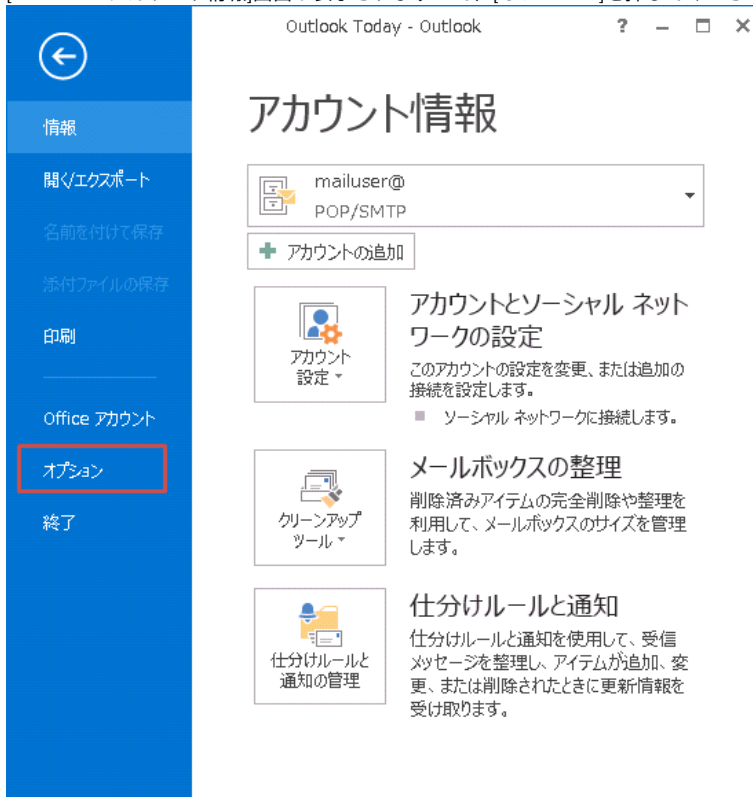
1-3. インストール手順

証明書のインストール手順

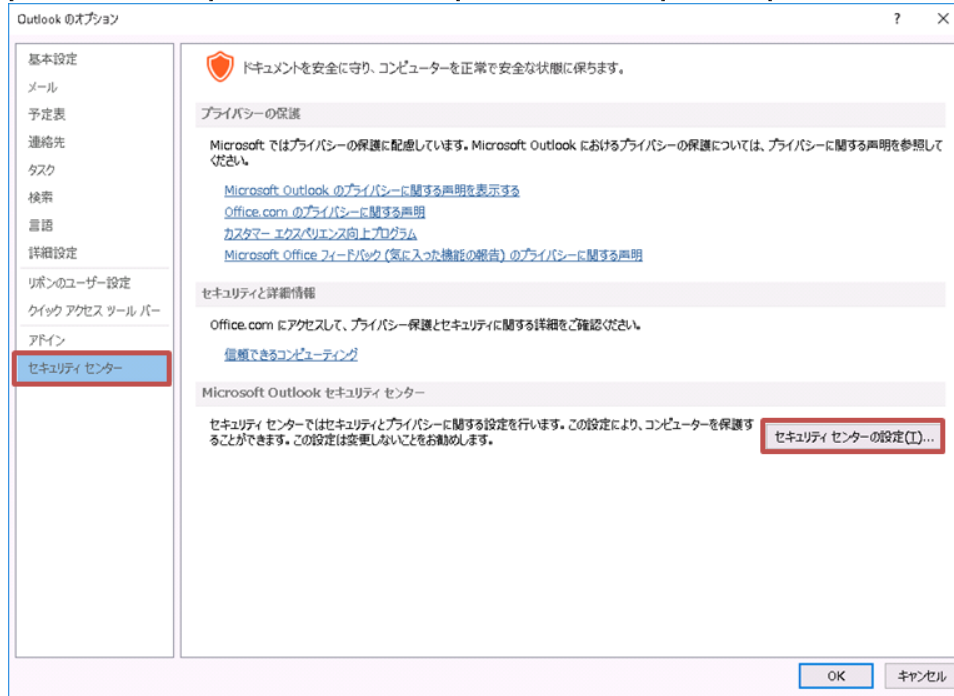
1. Microsoft Office Outlookより[ファイル]タブを押してください。



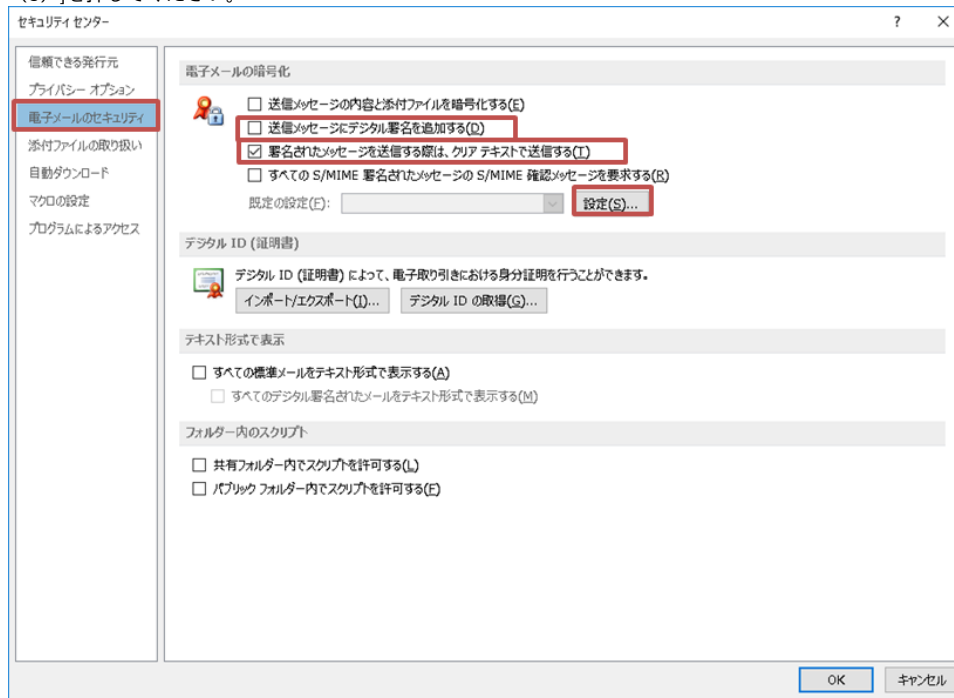
2. [Outlookのアカウント情報]画面が表示されますので、[オプション]を押してください。



3. [Outlookのオプション]画面が表示されますので、[セキュリティセンター]を選択し、[セキュリティセンターの設定(T)]を押してください。



4. [セキュリティセンター]画面が表示されますので、[電子メールのセキュリティ]を選択してください。
[送信メッセージにデジタル署名を追加する(D)]と[署名されたメッセージを送信する際は、クリアテキストで送信する(T)]にチェックをし、[設定(S)]を押してください。



5. [セキュリティ設定の変更]画面が表示されますので、[セキュリティ設定名(S)]に任意の文字列を入力してください。
[この暗号化メッセージ形式の既定のセキュリティ設定として使用する(T)]と[すべての暗号化メッセージの既定のセキュリティ設定として使用する(M)]にチェックをし、[選択(C)]を押してください。

セキュリティ設定の変更

保護されたメッセージの形式

セキュリティ設定名(S):
mailuser

暗号化の形式(F): S/MIME

☒ この暗号化メッセージ形式の既定のセキュリティ設定として使用する(T)
☒ すべての暗号化メッセージの既定のセキュリティ設定として使用する(M)

セキュリティ ラベル(U)... 新規作成(N) 削除(D)

証明書とアルゴリズム

署名証明書: 選択(C)...

ハッシュ アルゴリズム(A):

暗号証明書: 選択(H)...

暗号化のアルゴリズム(L):

☒ 署名済みメッセージで証明書を送信する(E)

OK キャンセル

6. [Windowsセキュリティ]画面が表示されますので、S/MIME証明書を選択し、[OK]を押してください。

Windows セキュリティ

証明書の選択

mailuser

発行者: SECOM Passport for Member PUB CA8
有効期間: 2021/01/30 から 2023/06/02

証明書のプロパティを表示します

OK キャンセル

7. [ハッシュアルゴリズム(A)]より[SHA256]、[暗号化アルゴリズム(L)]より[AES(256-bit)]を選択し、[署名済みメッセージで証明書を送信する(E)]にチェックをし、[OK]を押してください。

セキュリティ設定の変更

保護されたメッセージの形式

セキュリティ設定名(S): mailuser

暗号化の形式(F): S/MIME

☒ この暗号化メッセージ形式の既定のセキュリティ設定として使用する(T)

☒ すべての暗号化メッセージの既定のセキュリティ設定として使用する(M)

セキュリティ ラベル(U)... 新規作成(N) 削除(D)

証明書とアルゴリズム

署名証明書: mailuser 選択(C)...

ハッシュ アルゴリズム(A): SHA256

暗号証明書: mailuser 選択(H)...

暗号化のアルゴリズム(L): AES (256-bit)

☒ 署名済みメッセージで証明書を送信する(E)

OK キャンセル

※[ハッシュアルゴリズム(A)]はご利用の環境に合わせて選択してください。

8. [OK]を押してください。

セキュリティセンター

信頼できる発行元
プライバシー オプション
電子メールのセキュリティ
添付ファイルの取り扱い
自動ダウンロード
マクロの設定
プログラムによるアクセス

電子メールの暗号化

☐ 送信メッセージの内容と添付ファイルを暗号化する(E)

☒ 送信メッセージにデジタル署名を追加する(D)

☒ 署名されたメッセージを送信する際は、クリア テキストで送信する(I)

☐ すべての S/MIME 署名されたメッセージの S/MIME 確認メッセージを要求する(B)

既定の設定(E): mailuser 設定(S)...

デジタル ID (証明書)

デジタル ID (証明書) によって、電子取り引きにおける身分証明を行うことができます。

インポート/エクスポート(I)... デジタル ID の取得(G)...

テキスト形式で表示

☐ すべての標準メールをテキスト形式で表示する(A)

☐ すべてのデジタル署名されたメールをテキスト形式で表示する(M)

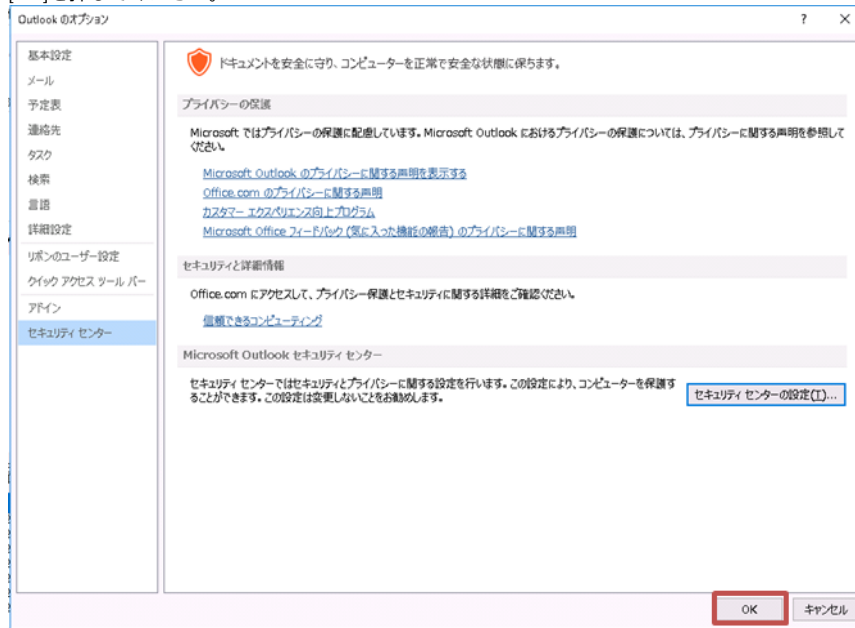
フォルダー内のスクリプト

☐ 共有フォルダー内でスクリプトを許可する(L)

☐ パブリック フォルダー内でスクリプトを許可する(E)

OK キャンセル

9. [OK]を押してください。



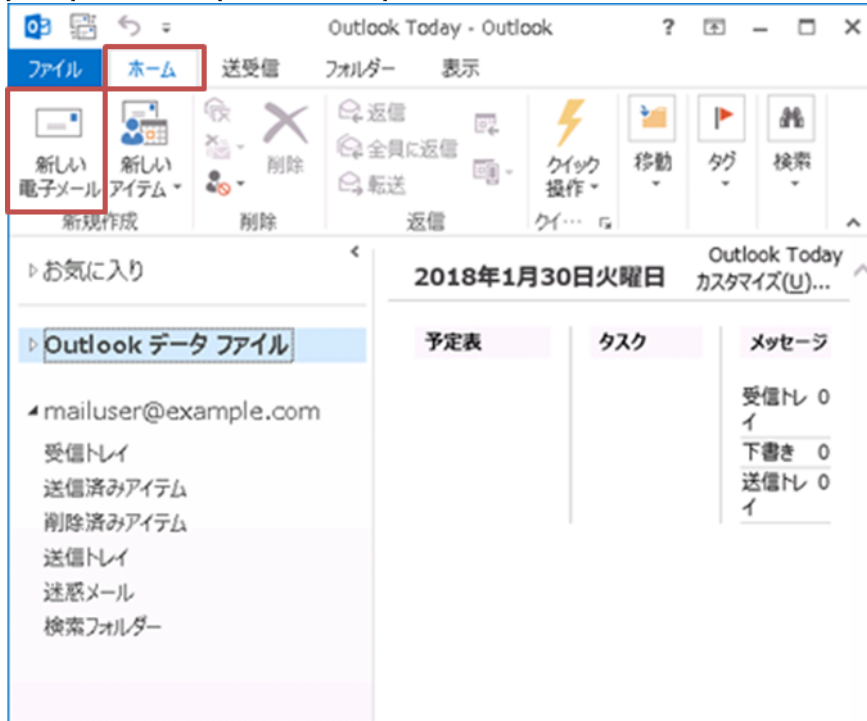
以上でS/MIME証明書のインストールは完了です。

2. デジタル署名付きメールの送信

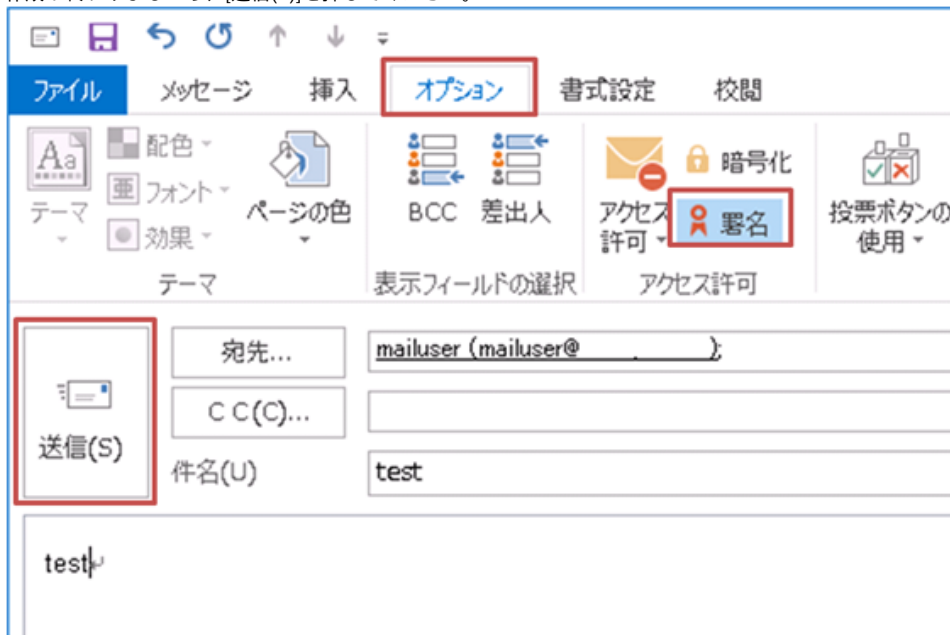
2-1. デジタル署名付きメールの送信手順

デジタル署名付きメールの送信手順

1. [ホーム]タブを選択し、[新しい電子メール]を押してください。



2. [メッセージ]画面が表示されますので、[オプション]タブより[署名]が設定されていることを確認し、メールを作成します。作成が完了したら、[送信(S)]を押してください。



※デジタル署名付きメールを送信しない場合は、[署名]を押して設定を解除してから[送信(S)]を押してください。

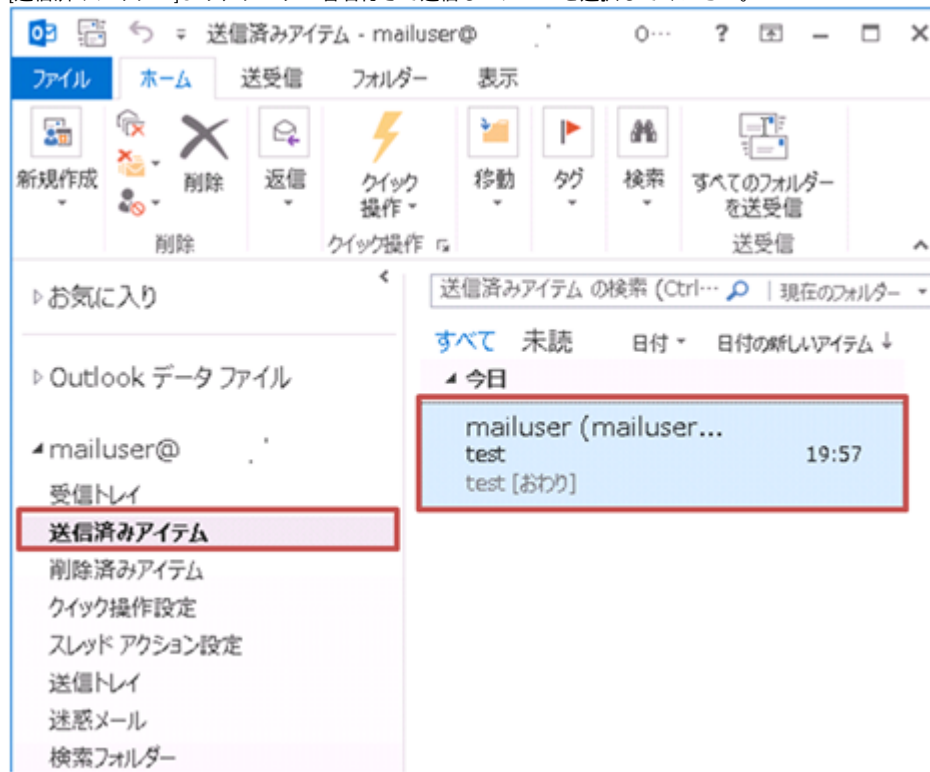
以上でデジタル署名付きメールの送信は完了です。

2-2. 送信したデジタル署名付きメールの確認手順

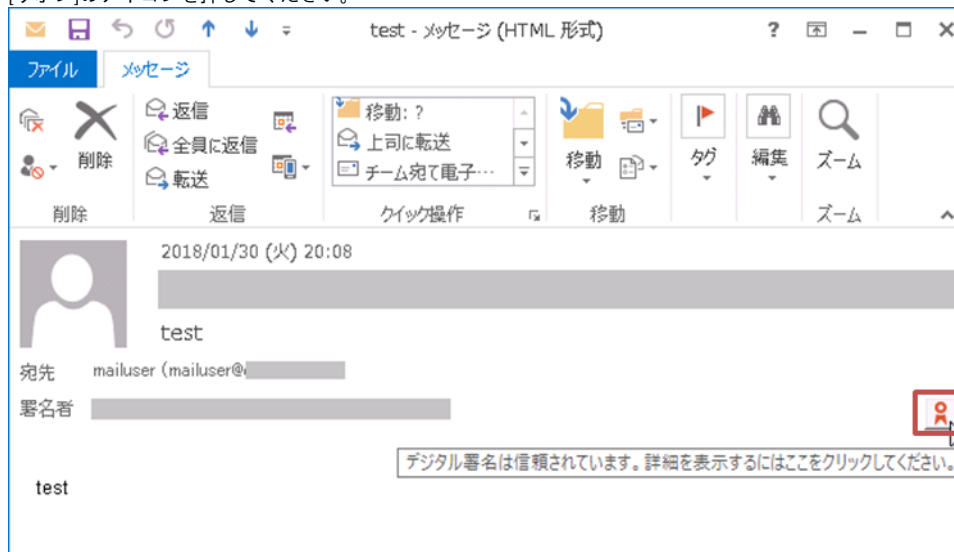
送信したデジタル署名付きメールの確認手順

--

1. [送信済みアイテム]より、デジタル署名付きで送信したメールを選択してください。



2. [リボン]のアイコンを押してください。



3. [デジタル署名]の画面が表示されますので、[詳細(D)]を押してください。

デジタル署名: 有効

件名: test

差出人:

署名者:

 このメッセージのデジタル署名は、有効で信頼されています。

メッセージのデジタル署名に使用された証明書の詳細については、[詳細]をクリックしてください。

☐ メッセージを開く前に、デジタル署名された電子メールのエラーについて警告する(W)

[詳細\(D\)...](#)

[閉じる\(C\)](#)

4. [メッセージセキュリティのプロパティ]画面が表示されますので、[詳細の表示(V)]を押してください。

メッセージセキュリティのプロパティ

 件名: test

メッセージには暗号化およびデジタル署名の層が含まれている場合があります、各デジタル署名の層には複数の署名が含まれている可能性があります。

セキュリティ層

選択した層の説明が表示されます(S)

- ✓ 件名: test
 - ✓ デジタル署名層
 - ⚠ 署名者:

内容(D):

下のボタンをクリックして、選択した層の詳細情報を表示したり、設定を変更できます。

[信頼性の編集\(E\)...](#) [詳細の表示\(V\)...](#) [信頼する証明機関\(T\)...](#)

☐ デジタル署名された電子メールのエラーを警告する(W) [閉じる\(C\)](#)

5. [全般]タブを選択し、[詳細書の表示(V)]を押してください。

署名

全般

詳細

 署名情報

メッセージ形式: S/MIME

署名者:

署名の状況:

署名日時: 20:08:28 2021/01/30

ダイジェストのアルゴリズム: SHA256

署名のアルゴリズム: RSA (2048-ビット)

 証明書の情報

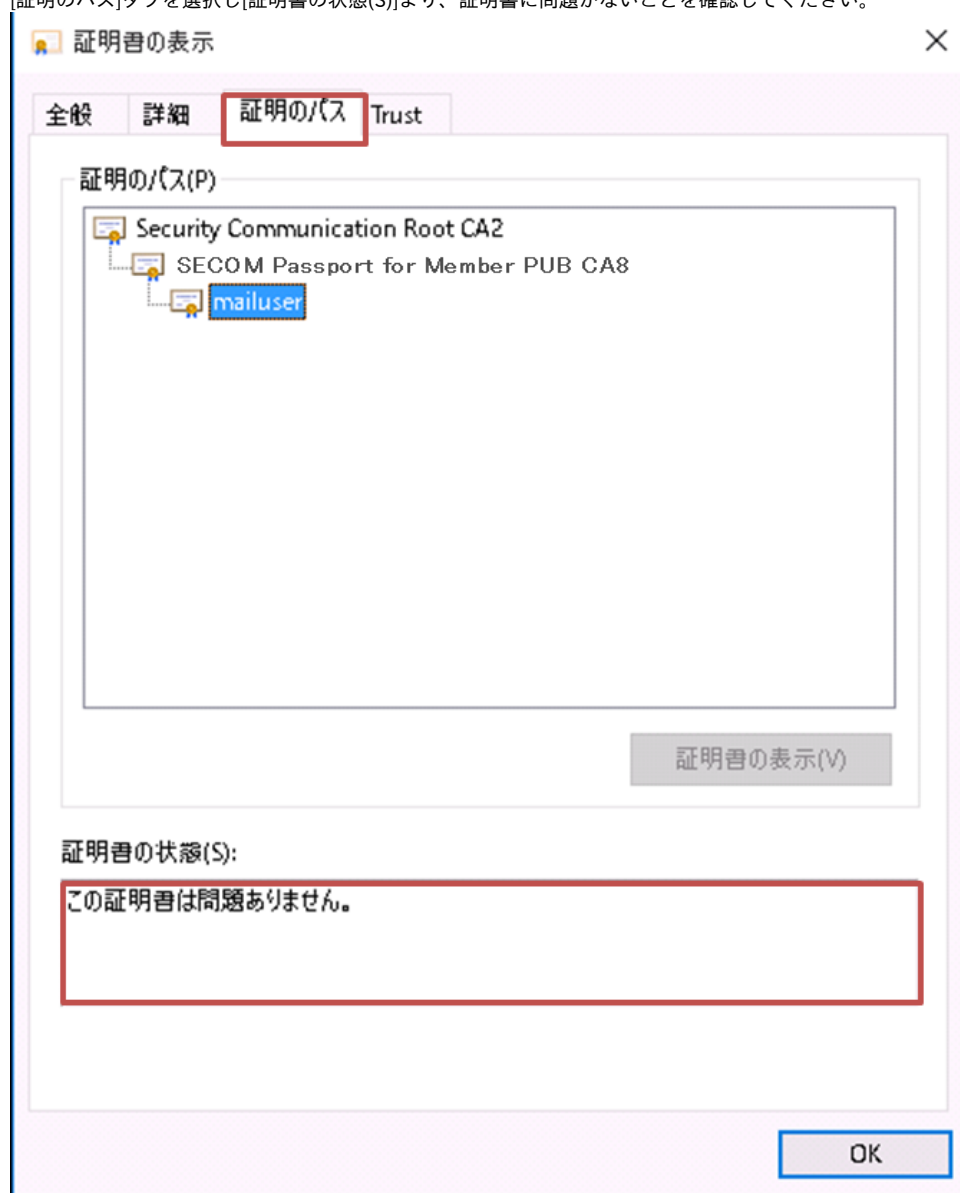
発行者: SECOM Passport for Member PUB CA8

証明書の状況:

証明書の表示(V)...

閉じる(C)

6. [証明のパス]タブを選択し[証明書の状態(S)]より、証明書に問題がないことを確認してください。



以上で送信したデジタル署名付きメールの確認は完了です。