メールソフトShurikenの設定

取得した電子証明書について、メールソフトで利用する方法を 「Shuriken」を例に説明します。

設定の流れは以下の通りです。

- ① 電子証明書のメールソフトへのインポート
- ② インポートした電子証明書とメールアカウントとの関連づけ
- ③ 電子署名したメールの送信
- ④ 暗号化したメールの送信
- ⑤ 電子署名および暗号化メールの受信について

メールの電子署名と暗号化は、どちらか片方ずつの利用、また は両方併用することが可能です。

1. 電子証明書のインポート

Shurikenを起動し、「ツール」 →「証明書管理」をクリックし てください。

メール(M)	編集(E)表示(\	/) フォル	ダ(F) 仕	分け(W)	設定(S)	୬–	ル(L) ヘルプ(H)	
新規送信	に 返信	全員返信	▲ 転送	昌	前 メール削除	№ →迷惑	8 11	アドレス帳(<u>A</u>) メールからアドレス帳に追加(<u>B</u>)	F11 Shift+F11
								着信監視(工)	+
								Shurikenアテンション(<u>L</u>)	•
								データ修復(<u>M</u>)	•
								証明書管理(<u>C</u>)	
								フォルダ内のメールを整理(E)	
								サーバーから受信済みメールを削除	*(<u>R</u>)
								バックアップ(<u>U</u>)	•
								リストア(<u>S</u>)	

③ 「次へ」をクリックしてください。

② 「個人」タブを選択した状態 で「インポート」をクリックしてく ださい。

月書	and the second se			
]的(N): /图	<すべて>			•
1回入 はかの人 1年	間証明機関 信頼されたル、	- 卜註山明幾関 1言	頼された発行元	「言頼されない発行元」
発行先	発行者	有効期限	フレンドリ名	
インポート(0) エ	クスポート(E) 削除(R			詳細設定(A)
証明書の目的				
				表示(V)



1	ンポートする証明書ファイル
	インボートするファイルを指定してください。
	ファイル名(F):
	参照(R)
	注意: 次の形式を使うと1 つのファイルに複数の証明書を保管できます:
	Personal Information Exchange- PKCS #12 (.PFX.P12)
	Cryptographic Message Syntax Standard- PKCS #7 証明書 (P7B)
	Microsoft シリアル化された証明書ストア(SST)
1. FE	月書ファイルの形式の詳細について表示します。

⑤「Personal Information Exchange(*.pfx;*.p12)」を 選択してください。

▶ 關<	
Corrected line clientAll	✓ 4→ ClientAllの検索
整理 ▼ 新しいフォルダー	8≕ ▾ 🗔 🔞
☆ お気に入り ^ 名前	更新日時 種類
🚺 ダウンロード	韓索条件に一致する項目はありません。
■ デスクトップ E 1911 最近表示した場所	
🎘 ライブラリ	Personal Information Exchange (*.pfx;*.p12)
▶ ドキュメント	証明書信頼リスト (*.stl)
📓 ピクチャ	証明書失効リスト (*.crl)
📑 ビデオ	Microsoft シリアルビされた証明書ストア (*.sst) PKCS #7 証明書 (* spc:* n7b)
_h ≥¬-ジック ▼ (·····································
ファイル名(N):	▼ X.509 証明書 (*.cer;*.crt) ▼
	聞く(0) キャンセル

⑥ 項目6で取得した電子証明 書を選択し、「開く」をクリック してください。

⊞ BI<		Mar and all and a	x
O I I I I I I I I I I I I I I I I I I I	- 49	clientAllの検索	Q
整理 ▼ 新しいフォルダー		JE • 🗍	0
	更新日時	種類	
ダウンロード	2017/01/17 12:03	Personal Information Exchar	1ge
デスクトップ E			
1911 最近表示した場所			
🍞 ライブラリ			
F#1×>>			
1000000000000000000000000000000000000			
ビデオ			
1 ≥1-5wh * *			
ファイル名(N):	•	Personal Information Excha	ar 🔸
		開く(0) 🔻 キャンセ	11

⑦「次へ」をクリックしてください。

証明書のインボート ウィザード
インボートする証明書ファイル
インボートするファイルを指定してください。
7r1/JA(F):
C.¥Users¥furuyas¥Desktop¥clientAll¥
注意:次の形式を使うと1つのファイルに複数の証明書を保管できます:
Personal Information Exchange- PKCS #12 (.PFX,P12)
Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
Microsoft シリアル化された証明書ストア(SST)
証明書ファイルの形式の詳細について表示します。
< 戻る(B) 次へ(N) > キャンセル







証明書ストア	
証明書ストアは、証明書が保管され	れるシステム上の領域です。
Windows (ご証明書ストアを自動的	コに選択させるか、証明書の場所を指定することができます。
◎ 証明書の種類に基づいて、	自動的に証明書ストアを選択する(U)
◎ 証明書をすべて次のストアに	2配置する(P)
証明書ストア:	
個人	参照(R)
和明書ストアの詳細を表示します	

⑩「完了」をクリックしてください。

証明書のインポート ウィザード	X
	証明書のインボート ウィザードの完了
	I党で 7 をクリックすると、証明書がインボートされます。 次の設定が指定されました: ユーザーがの説化した証明書ストア 個人 内容 PFX ファイル・名 Ci¥Users¥■■● JDesktop¥clic
	к <u>ш</u>
	< 戻る(B) 売了 キャンセル

① 正しくインポートされているか
 ②のウインドウを開いて「個人」タブに電子証明書があることを確認してください。

正明書				— ×
目的(N): 個人 ほかの人 日	<すべて> つ間証明機関 信頼されたルート語	正月機関 (言語	頼された発行元	「信頼されない発行元
発行先	発行者 ■ NII Open Domain S/M	有効期限 2019/02/	フレンドリ名	•
インボート(D) [I 証明書の目的	.クスポート(E)) 削除(R)			[詳紀語文定(A)
証明書の詳細について	<u>表示します。</u>			表示(V) 閉じる(C)

2. メールアカウントとの関連づけ

 Shurikenを起動し、「設定」
 →「アカウント登録設定」を クリックしてください。



② 「セキュリティ」の「標準の証 明書」を選択して、「編集」 をクリックする。

■ アカウント登録設定	· ##75228 ##72464	85	
アカウント(A) ・ @yamanashi.a	c.jp ▼ 登録・編集(M)▼		
グループ(G)	設定一覧(L)		
 アカウント情報 受信 	設定項目	設定値	
	※仕取った証明日本た白針的に証明日本フトマム (無)後の証明日本	しない	
 一次一方(10)/ 一 受け取り通知 一次 かたっりライ 	活行使証明に証明書の大知人服を目期的に	. Utati	
B- 041994	分離型署名(multipart/signed)を使用 暗号化に利用するアルゴリズム	する Triple-DES	
	メールを送信するときは常にデジタル署名を付加	しない	
	メールを送信するときは常に暗号化	しない	
	[編集]をクリックして、いつも使う証明書を指定します。		∧ 編集(E)
▼詳細設定(D)			
級的込み(C) 級法(S) 解認後(R)			
			OK キャンセル ヘルプ(H)

③ 自身のクライアント証明書を選 択して、「OK」をクリックしてくだ さい。

2019/02/17	

④ 「受け取った証明書を自動的に 証明書ストアへ登録」を、「編 集」から設定値を「する」に変更 して「OK」をクリックしてください。

アカウント(<u>A</u>)	@yamanashi.ac.j	jp	
ブループ(<u>G</u>)		設定一覧(L)	
アカウンド情報 受信 受信 ジェル作成 受け取り通 マグに マグに マグに マグに マグ ジ ジ ジ ジ ジ	題 10 9	設定項目 設定値 受け取った証明書を自動的に証明書ストアへ登録 する 端年のほど内害 なる 第名作成正式取用書の大効状態を自動的に確認 なる 分離型署名(multipart/signed)を使用 する 時号化に利用するアルゴリズム Trole-DES メールを送信するとをは常に評当りい場名を行加 しない	
2]詳細設定(D) 対込み(C)	(「信頼できる証明書を受け取ったときに自動的に証明書ストアに登録するかどうかを指定します ▲ 編	i集(E)
		ОК # #>/2// Л	ルプ(日)

3. 電子署名したメールの送信

① 新規メールを起動して、メールを作成してください。
 ② 「ツール」→「デジタル署名する」をクリックしてください。
 ③ 「送信」で電子署名したメールを送信します。



4. 暗号化したメールの送信

① 新規メールを起動して、メールを作成してください。
 ② 「ツール」→「暗号化する」をクリックしてください。
 ③ 「送信」で暗号化したメールを送信します。



【注意1】

メールの暗号化を行うには、送信先の証明書が必要です。事前に電子署名を 付与したメールを送信先から受信しておく必要があります。

【注意2】

受信した暗号化メールを復号するには、自身の証明書をインポート設定した メールソフトを利用する必要があります。未設定の場合は暗号化メールを復号 できない(閲覧できない)ので注意してください。

また、Office365 Webアプリの現時点の設定では、S/MIMEを利用できません。



電子署名および暗号化メールを受信した場合、該当 メールを選択すると下図が表示されます。「復号・署名 確認」をクリックしてください。



② 電子署名または暗号化された電子証明書を確認したい 場合、以下のアイコンをクリックしてください。

@yamanashi.a... 送信日時: 2 🔤 🖳 🖛 🚽 📑

③必要に応じて各証明書の内容を確認してください。

デジッタ素名と暗号化に関する情報	「証明書の内容	
デジタル署名 署名 デジタル署名に使われた証明書(S)… この文書はデジタル署名されています。 文書がなざんされていないことは、デジタル署名によって確認されました。 「デジタル署名に使われた証明書」をクリックすると、デジタル署名そのものの 信頼性を確認できます。 暗号化	概要 詳細 証明書パス この証明書に問題はありません。(失効の確認)本物/を勿り/ウすると、証明書が失効/ ストに登録されているかどうが確認します。 * po@yamanshia.co.p から送信されたメールのデジタル著名を確認することができます。 * po@yamanshi.ac.p から送信されたメールのデジタル著名を確認することができます。 失効の確認(R)_ 発行元 NII Open Domain S/MIME CA	←電子署名の例 発行元:NII Open Domain S/MIME CA 発行先:Information Systems Division メールアドレス:ipc@yamanashi.ac.jp
暗号化に使われた証明書(E) この文書は暗号化とれています。 「暗号化に使われた証明書」をクリックすると、この文書の暗号化・復号化に 使われた証明書の内容を確認できます。 閉じる(C) ヘルプ(H)	C=JP, L=Academe, O=National Institute of Informatics, CN=NILOper 発行先 Information Systems Division C=JP, L=Academe, O=University of Yamanashi, OU=Organization f メールアドレス ipc@yamanashi.ac.jp 有効期限 2017/01/16 ~ 2019/02/16 閉じる(C) ヘルプ(H)	8 8