

暗号メールの設定方法

(Outlook Expressの場合)

1

デジタルID

デジタルID は、利用者の公開鍵証明書、秘密鍵、およびCAの公開鍵証明書から成る。

Personal Information Exchange (pfx)

IEやNetscapeが使用した「証明書＋秘密鍵」ファイルであり、PKCS#12の前身にあたる。ファイルの拡張子は「*.pfx」である。

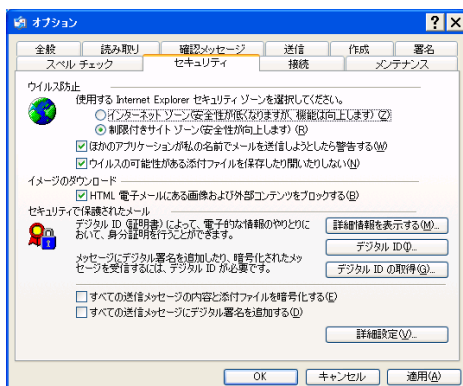
PKCS#12

証明書と秘密鍵のファイル化を行ったものであり、ファイルのImport/Export時にファイルの暗号化を行える。複数の証明書を格納する事ができ、自分の証明書その他、CAの証明書等を格納する。ファイルの拡張子は「*.p12」である。NetscapeやIEなどで使われている。

2

証明書のインポート

Outlook Expressを起動し、[ツール]－[オプション]で表示されるダイアログの[セキュリティ]タブを開く。デジタル証明書をインポートするには、[デジタルID]をクリックする。



3

証明書のインポート

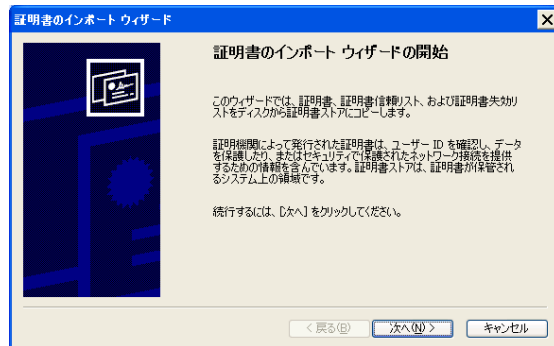
証明書の一覧が表示されるが、最初は個人用のデジタル証明書はインストールされていないので、[個人]タブには何も表示されない。そこで、[インポート]をクリックして、証明書をインポートする。



4

証明書のインポート

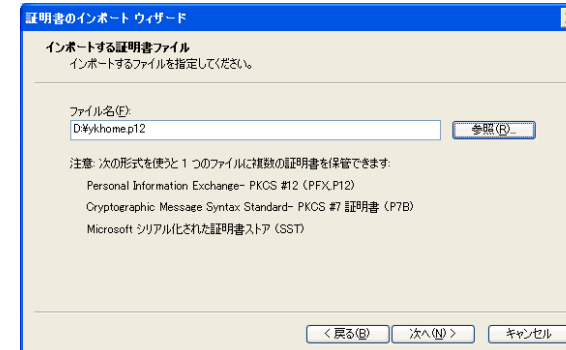
[証明書のインポート ウィザード] が起動される。



5

証明書のインポート

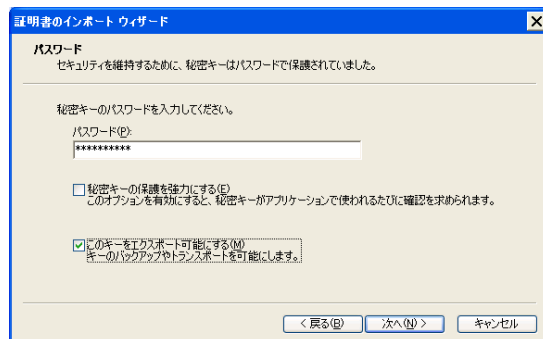
インポートするデジタル証明書のファイルを指定する。



6

証明書のインポート

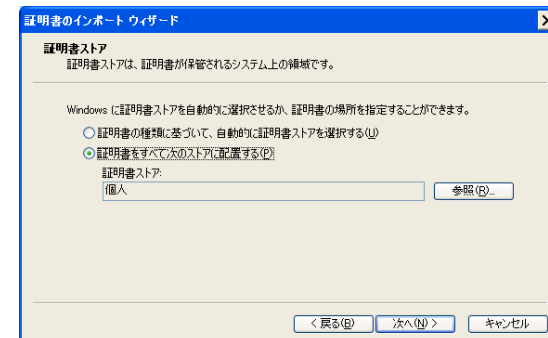
秘密鍵を暗号化してファイル化した場合は、復号するためのパスワード入力が必要される。



7

証明書のインポート

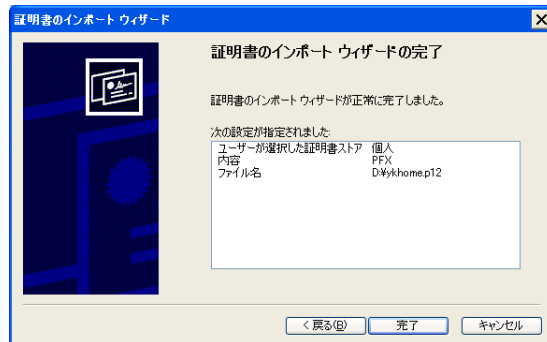
デジタル証明書のストア先を決める。署名と暗号化にデジタル証明書を使用する場合、通常は[個人]にストアして問題ない。ここまでの設定を行うと、ウィザードによってデジタル証明書がOutlook Expressにインポートされる。



8

証明書のインポート

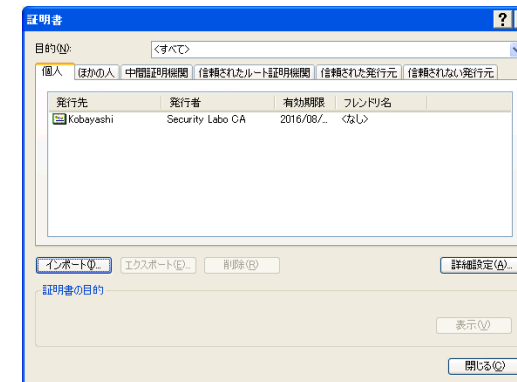
インポートウィザードの完了



9

証明書のインポート

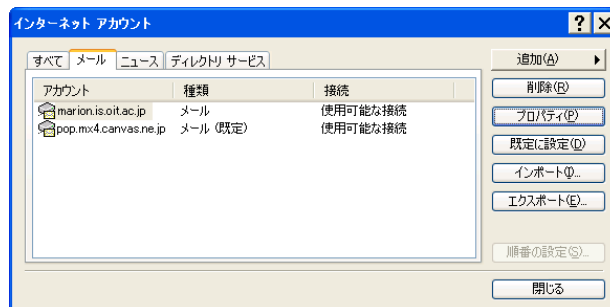
デジタル証明書がインポートされたことを確認する。



10

アカウントへの証明書設定

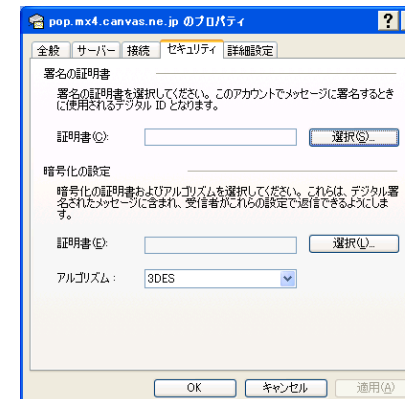
アカウントを選択し、プロパティをクリックする。



11

アカウントへの証明書設定

証明書を選択する。



相手側での署名検証に
使用する公開鍵証明書

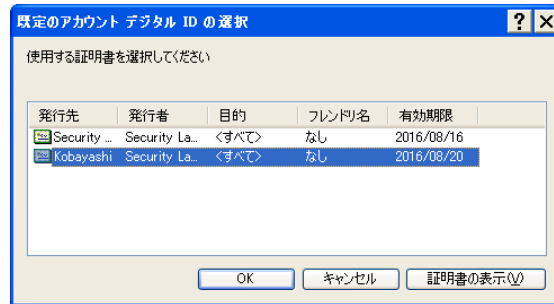
相手側での暗号化に使用
する公開鍵証明書

共通鍵暗号アルゴリズム

12

アカウントへの証明書設定

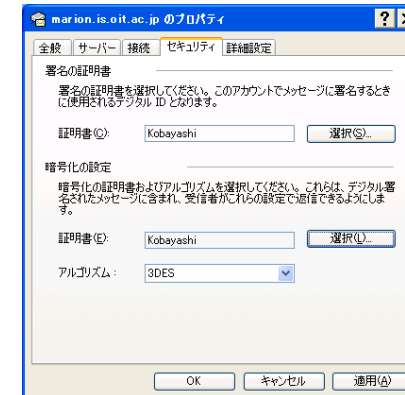
証明書を選択する。



13

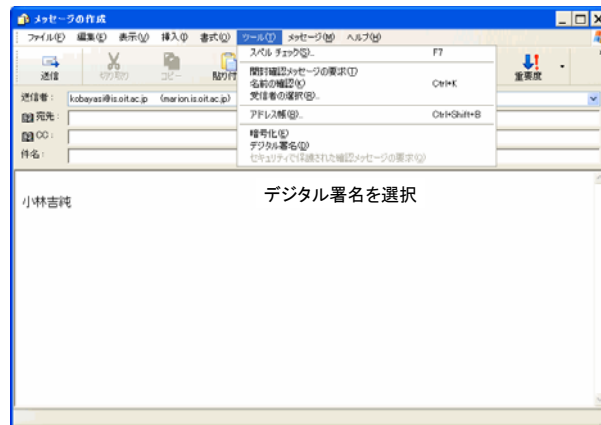
アカウントへの証明書設定

証明書の選択結果



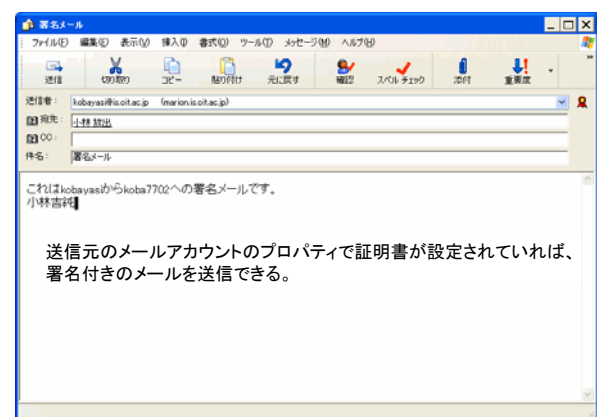
14

署名付きメール(送信側)



15

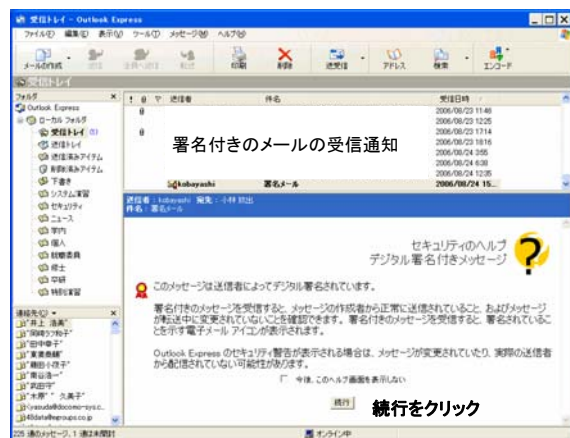
署名付きメール(送信側)



署名付き

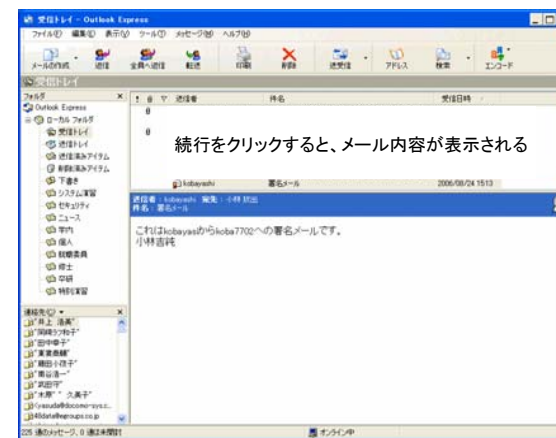
16

署名付きメール(受信側)



17

署名付きメール(受信側)



18

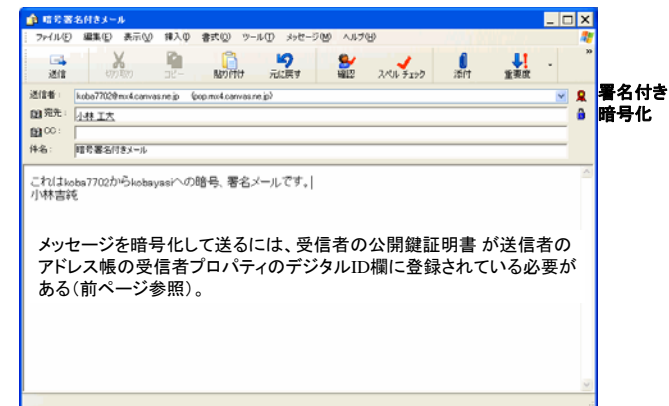
アドレス帳への登録(受信側)

Outlook Express では、デジタル署名付きメールを受信すると、送信者の公開鍵証明書がアドレス帳の送信者アドレスのプロパティのデジタルID欄に自動的に追加される。証明書の「ほかの人」欄にも設定される。



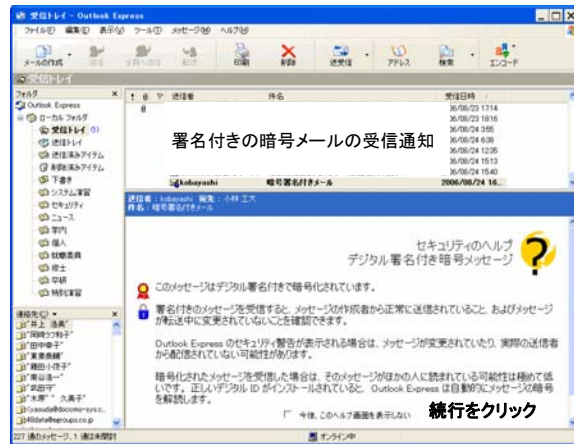
19

署名付き暗号メール(送信側)



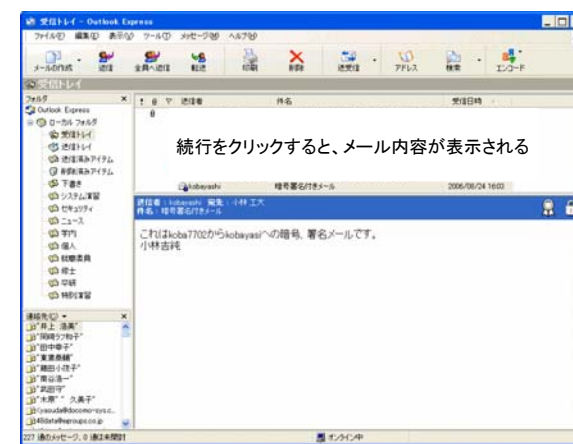
20

署名付き暗号メール(受信側)



21

署名付き暗号メール(受信側)



22