

メール暗号化：秘密鍵・公開鍵の作成

作業手順

Outlook Express

秘密鍵・公開鍵の作成

作業の手順

1. 暗号化されたメールを受け取れる(復号できる)環境を設定する

認証局(UMINセンター)より**デジタル証明書**を発行

デジタル証明書を設定 お使いのメールソフトで設定します。

受信用の**秘密鍵**を設定 お使いのメールソフトで設定します。

2. 暗号化してメールを送信する

送信先の**公開鍵**の取得する。

公開鍵を設定する お使いのメールソフトで設定します。

暗号化して送信する お使いのメールソフトでの送信になります。

秘密鍵・公開鍵の作成

(設定の流れ)

A . 秘密鍵・公開鍵、認証局のルート証明書の取得とパソコンへの設定

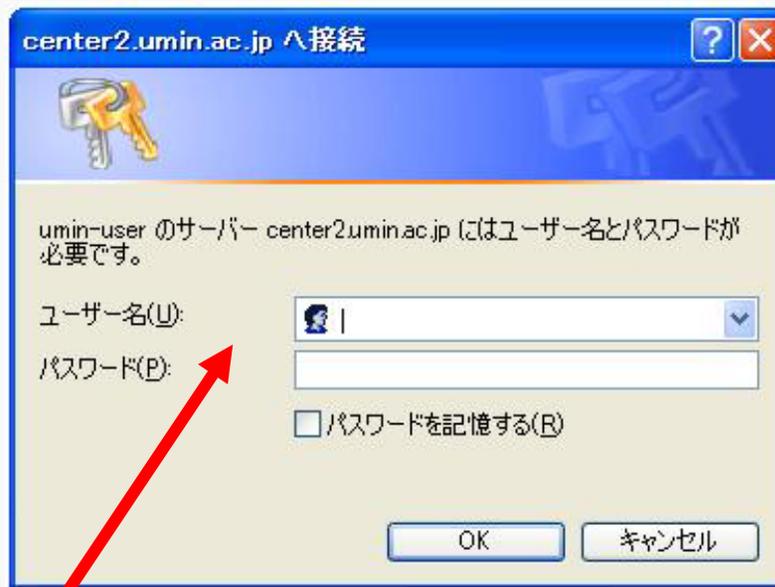
B . 暗号化されたメールを「受信」できるように設定する。
(自分の秘密鍵をご使用のメールソフトへの設定する)
(1)アウトルックエクスプレス(Microsoft Outlook Express)

C . 暗号化してメールを「送信」できるように設定する。
(他の人の公開鍵を取得してメールソフトへ設定する。)
公開鍵の取得 ~
~ (1)アウトルックエクスプレス(Microsoft Outlook Express)

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行

<https://center2.umin.ac.jp/cgi-bin/ca/index.cgi> のURLから
「公開鍵証明書管理機能」の画面に入ります。



ユーザー名に UMIN IDを入力
パスワードに UMINのパスワードを入力

A . 秘密鍵・公開鍵の作成

「秘密鍵・公開鍵の作成、破棄および検索」画面



トップページ「登録者用ページ」

XXXX-XXX@umin.ac.jp用証明書

XXXX-XXX@umin.net用証明書

公開鍵検索の入力枠

ルート証明書

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行

トップページ

UMIN ID: ■■

■ ■ tky@umin.ac.jp用証明書 ... 【未発行】

● [秘密鍵と公開鍵の作成](#)

■ ■ tky@umin.net用証明書 ... 【未発行】

● [秘密鍵と公開鍵の作成](#)

お持ちのUMINメールアドレスに
該当する証明書の

「**秘密鍵と公開鍵の作成**」をクリック

してください。

(本マニュアルのモデルケースは、
umin.ac.jpを使用している場合です。)

お持ちのUMINメールアドレスに合致するほうを選択してください。

XXXX-XXX@umin.ac.jp

XXXX-XXX@umin.net

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行

UMIN S/MIME用公開鍵証明書の発行

UMIN ID:

下記のデータで公開鍵証明書が作成されます
よろしければ発行ボタンをクリックしてください

- 国名コード: JP
- 都道府県: Tokyo
- 市町村: Bunkyo-ku
- 組織名: University Hospital Medical Information Network
- 名前:
- 電子メールアドレス:
- 有効期間:

内容確認 → (Red arrow pointing to the list of data)

有効期間を選択 → (Blue arrow pointing to the dropdown menu)

「発行」をクリック → (Green arrow pointing to the 発行 button)

[登録者用ページに戻る](#) [UMINホームページに戻る](#)

ご要望はお問い合わせフォームまでお寄せください

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行

公開鍵証明書が発行
されました。

登録者用ページ
(初期画面)へ
戻って確認してください。

UMIN S/MIME用公開鍵証明書の発行

UMIN ID: ■■■-tky

公開鍵証明書を発行しました

初期画面で現在の状態を確認してください

[登録者用ページに戻る](#) [UMINホームページに戻る](#)

ご要望は[お問い合わせフォーム](#)までお寄せください

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行

(登録者用ページ トップページ)

【発行済】 表記になり、

・作成した秘密鍵・公開鍵
(公開鍵証明書)の破棄

・pkcs12形式の
クライアント証明書の
ダウンロード

が可能になりました。

UMIN 秘密鍵・公開鍵の作成、破棄および検索

UMIN ID: *****

- tky@umin.ac.jp用証明書 … **【発行済】**
 - 作成済みの秘密鍵及び公開鍵(公開鍵証明書)の破棄を行う
 - pkcs12形式のクライアント証明書をダウンロードする
- tky@umin.net用証明書 … **【未発行】**
 - 秘密鍵と公開鍵の作成

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行

(登録者用ページ トップページ)

秘密鍵と公開鍵をお使いのメールソフトに
設定するため、**2つの証明書**を
ダウンロードしてください。

pkcs12形式のクライアント証明書

ルート証明書

次ページより、
それぞれの証明書の
設定方法を説明します。

UMIN 秘密鍵・公開鍵の作成、破棄および検索

UMIN ID: []

--- @umin.ac.jp用証明書 ... 【発行済】

- 作成済みの秘密鍵及び公開鍵(公開鍵証明書)の破棄を行う
- pkcs12形式のクライアント証明書をダウンロードする

--- @umin.net用証明書 ... 【未発行】

- 秘密鍵と公開鍵の作成

公開鍵検索

検索するUMIN IDを入力して検索ボタンを押してください

UMIN ID: [] [検索]

ルート証明書
こちらよりダウンロードして下さい

UMINホームページに戻る

ご要望はお問い合わせフォームまでお寄せください

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行

(クライアント証明書の発行)

「pkcs12形式の
クライアント証明書の
ダウンロード」

をクリックします。

保存先を指定して保存
します。

UMIN 秘密鍵・公開鍵の作成、破棄および検索

UMIN ID: [input field]

- tky@umin.ac.jp用証明書 ... 【発行済】
 - 作成済みの秘密鍵及び公開鍵(公開鍵証明書)の破棄を行う
 - pkcs12形式のクライアント証明書をダウンロードする
- tky@umin.net用証明書 ... 【未発行】
 - 秘密鍵と公開鍵の作成

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行

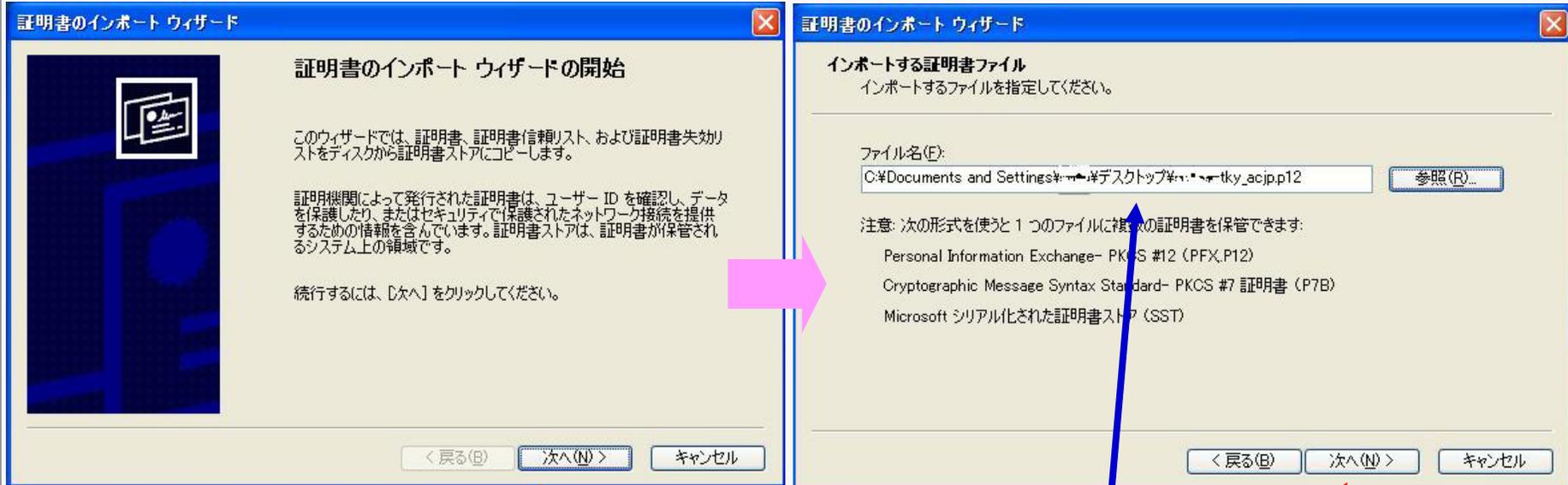


鍵マークのついた「～.p12」形式ファイルがダウンロードされたことをご確認ください。

ダブルクリックで「証明書のインポートウィザード」が開始します。

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行 (証明書インポート)



「証明書のインポート ウィザード」が開始されます。
「次へ」をクリック

インポートする証明書ファイルのファイル名が
表示されます。「次へ」をクリックしてください。

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行(証明書インポート)

【証明書のインポート ウィザード】

証明書のインポート ウィザード

パスワード
セキュリティを維持するために、秘密キーはパスワードで保護されていました。

秘密キーのパスワードを入力してください。

パスワード(P):

秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。

このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。

< 戻る(B) 次へ(N) > キャンセル

証明書のインポート ウィザード

証明書ストア
証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、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配置する(P)

証明書ストア:

参照(R)...

< 戻る(B) 次へ(N) > キャンセル

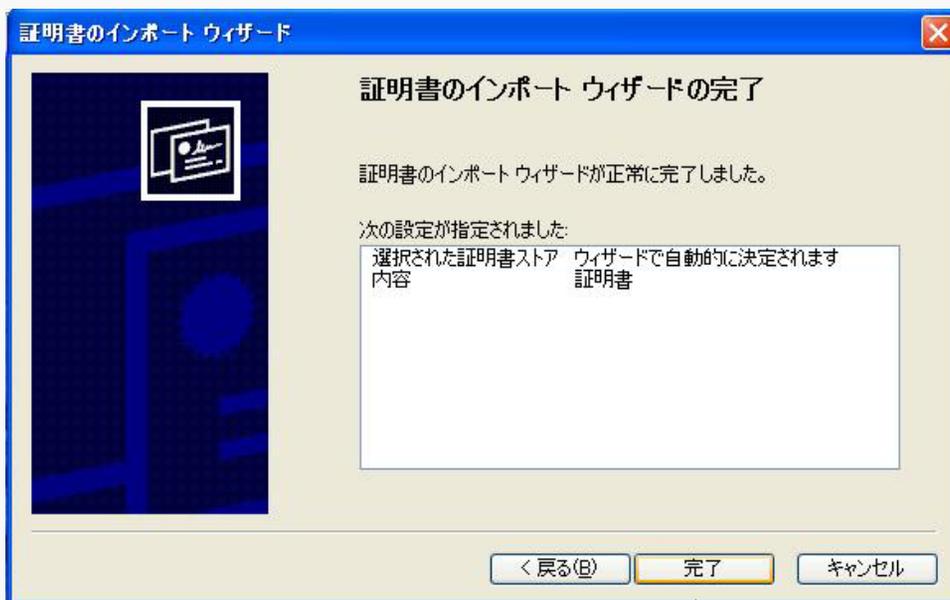
「パスワード」には何も入力せずに
そのまま「次へ」をクリック

「証明書の種類に基づいて、自動的に証明書ストアに
選択する」を選んで「次へ」をクリック

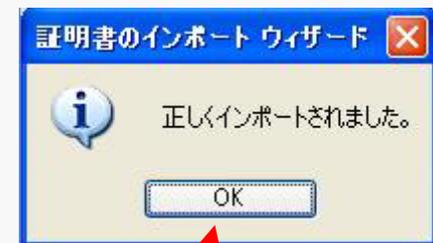
A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行（証明書インポート）

【証明書のインポート ウィザード】



証明書のインポート ウィザードが完了しました。
「完了」をクリックしてください。



インポートの終了画面が
表示されます。
「OK」をクリックして
インポート終了です。

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行(証明書インポート)

【ルート証明書のインポート ウィザード】

登録者用トップページから
ルート証明書 →
をダウンロードします。

UMIN 秘密鍵・公開鍵の作成、破棄および検索

UMIN ID:

■ [@umin.ac.jp用証明書](#) ... 【発行済】

- [作成済みの秘密鍵及び公開鍵\(公開鍵証明書\)の破棄を行う](#)
- [pkcs12形式のクライアント証明書をダウンロードする](#)

■ [@umin.net用証明書](#) ... 【未発行】

- [秘密鍵と公開鍵の作成](#)

公開鍵検索

検索するUMIN IDを入力して検索ボタンを押してください

UMIN ID:

ルート証明書
こちらよりダウンロードして下さい

[UMINホームページに戻る](#)

ご要望はお問い合わせフォームまでお寄せください

A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行(証明書インポート)

[ルート証明書のインポート ウィザード]



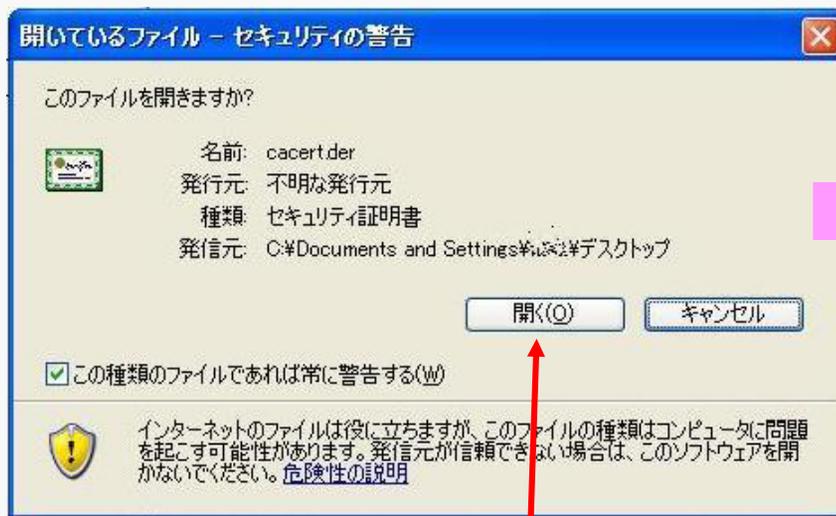
証明書アイコンの「cacert.der」形式ファイルがダウンロードされたことをご確認ください。

ダブルクリックで「証明書のインポートウィザード」が開始します。

A . 秘密鍵・公開鍵の作成

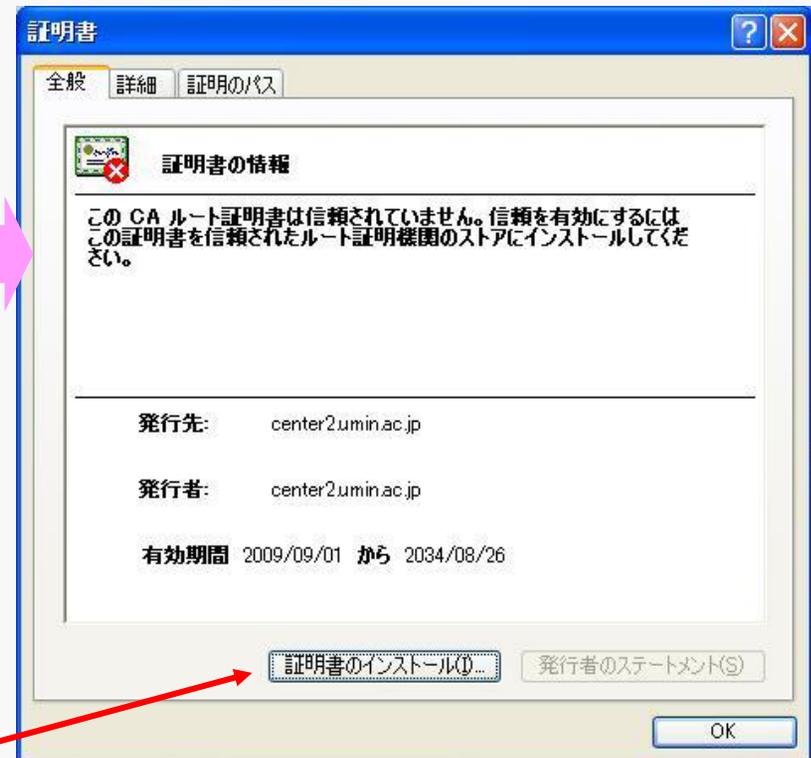
秘密鍵・公開鍵の発行(証明書インポート)

【ルート証明書のインポート ウィザード】



ルート証明書のファイル「cacert.der」を開きます。

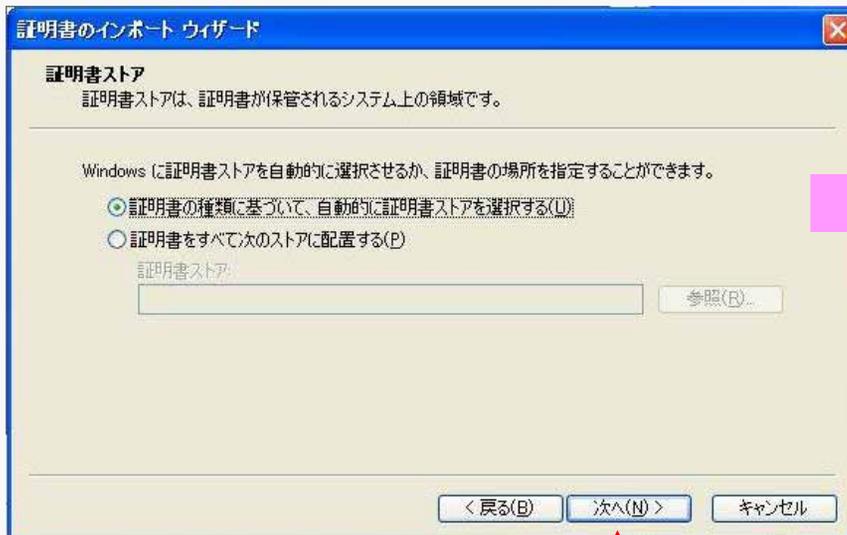
証明書のインストールを開始します。



A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行(証明書インポート)

【ルート証明書のインポート ウィザード】



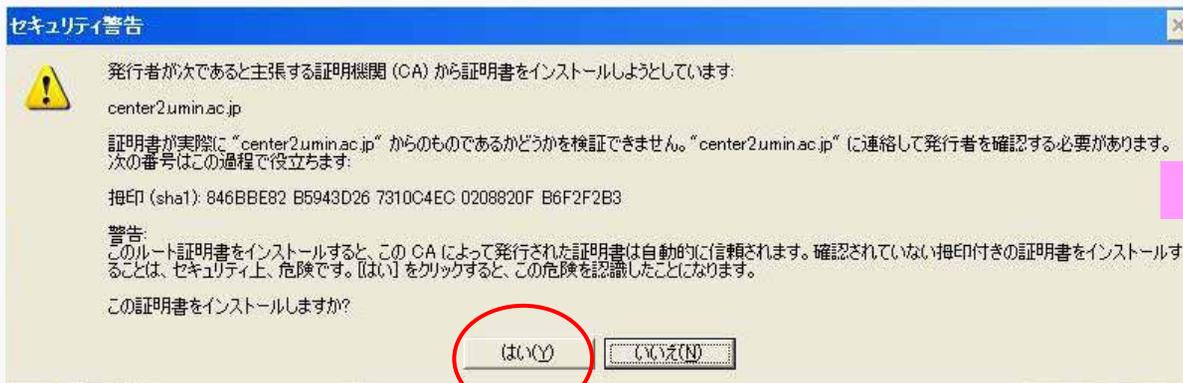
証明書のインポートのウィザードを進行します。
「次へ」をクリックしてください。

「完了」をクリックしてください。

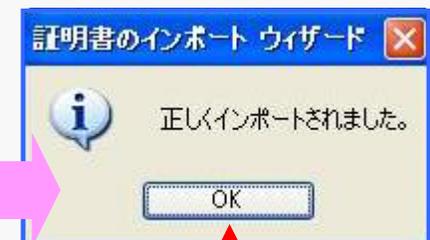
A . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行(証明書インポート)

【ルート証明書のインポート ウィザード】



center2.umin.ac.jp発行の証明書のインストール許可の確認画面です。
「はい」で進行してください。



「OK」のクリックで
インポート完了です。

拇印 (sha1) はFAQ . Q4をご確認ください。
(<http://www.umin.ac.jp/cipher/faq/index.html>)

B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定

(1) Microsoft Outlook Express

メールソフトにおける設定の説明です。

B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定

(B 1 - 1) Microsoft Outlook Express
アウトルック エクスプレス 使用の場合

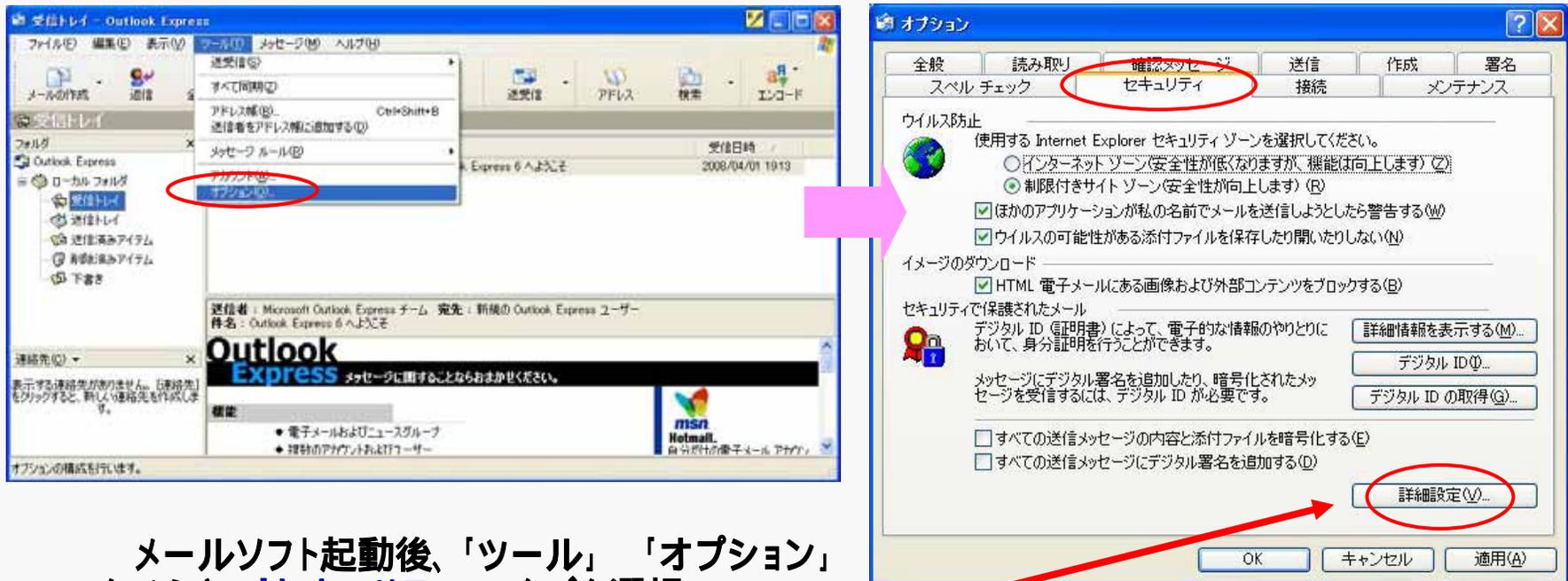


メールソフトを起動し、デジタル証明書がインポートされたことを確認します。

アカウントごとにデジタル証明書を有効にすることにより、メールへの署名や暗号化が可能になります。

B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B1 - 2) Microsoft Outlook Express デジタル証明書の確認



The image shows two screenshots from Microsoft Outlook Express. The left screenshot shows the 'Tools' menu with 'Options...' selected. The right screenshot shows the 'Options' dialog box with the 'Security' tab selected. A pink arrow points from the 'Options...' menu item to the 'Security' tab, and a red arrow points from the 'Security' tab to the 'Advanced Security Settings...' button.

メールソフト起動後、「ツール」「オプション」
をひらき、「セキュリティ」のタブを選択、
「詳細設定」をクリックします。

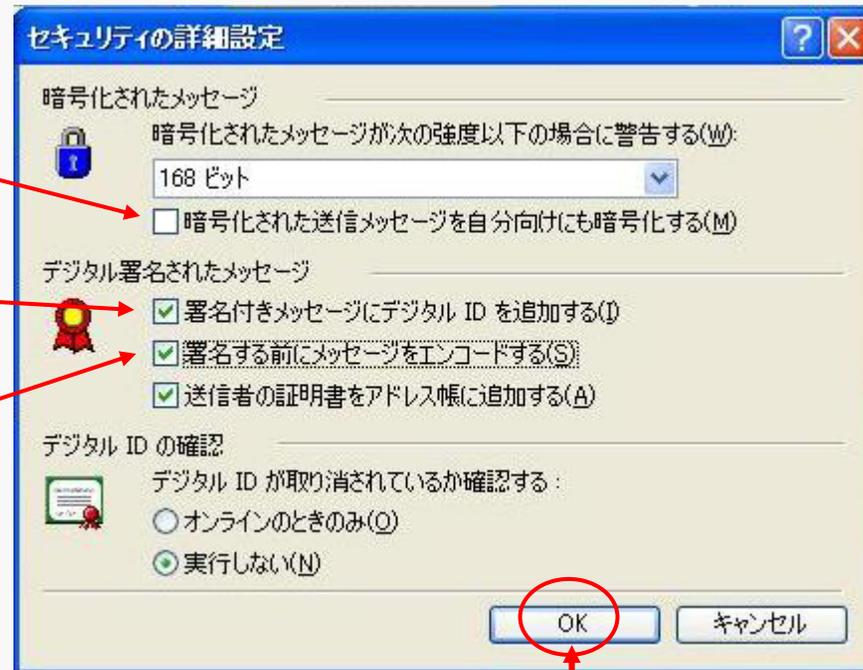
B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定 (B 1 - 3) Microsoft Outlook Express デジタル証明書の確認

「暗号化された送信
メッセージを自分向けにも
暗号化する」
の**チェックを外します**。
(送信済のメールを読めるように
するためです。)

「署名付きメッセージに
デジタルIDを追加する」
に**チェックをいれます**。

「署名する前にメッセージを
エンコードする」
に**チェックをいれます**。

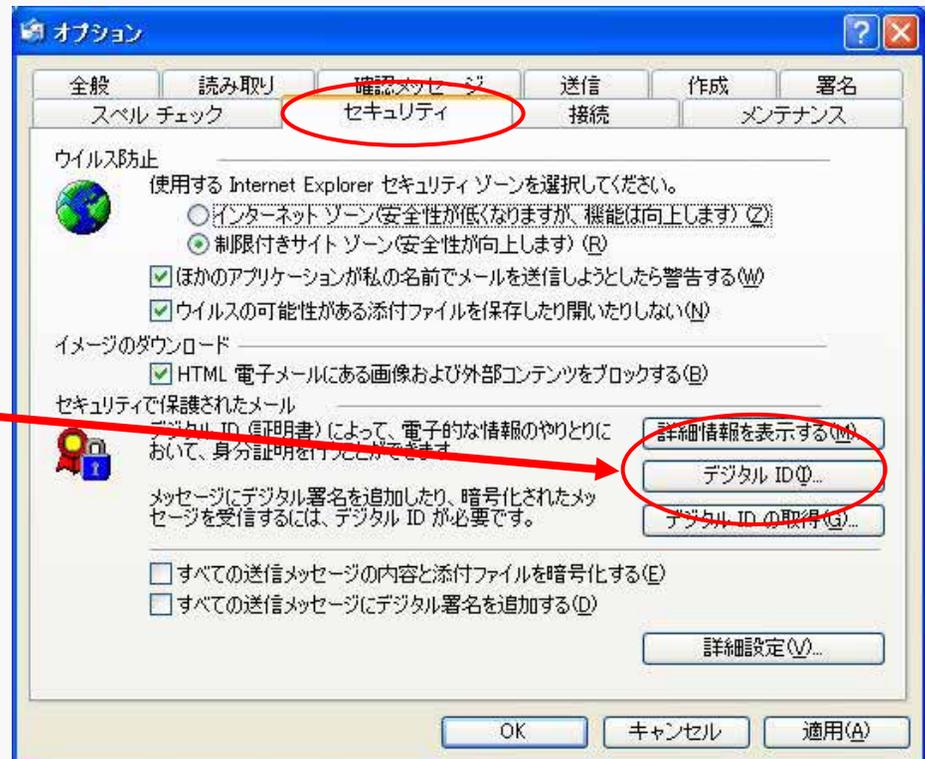


「OK」で確定してください。

B . 秘密鍵・公開鍵の作成

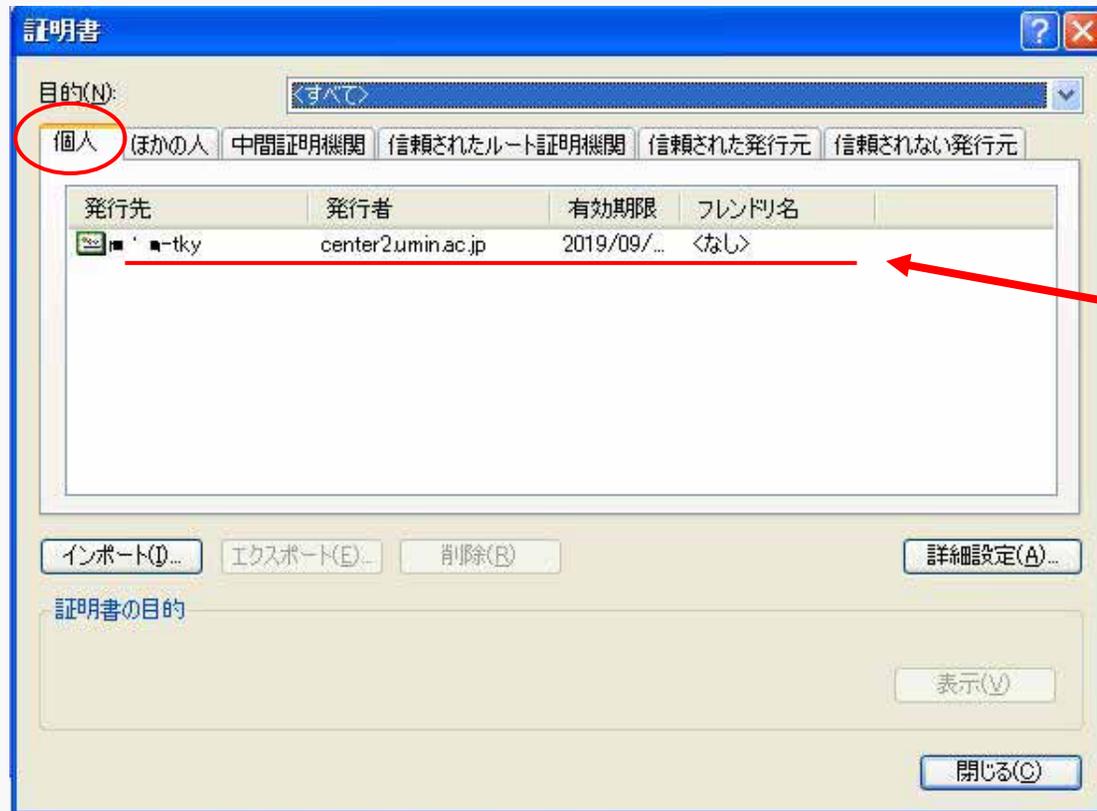
各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B 1 - 4) Microsoft Outlook Express デジタル証明書の確認

メールソフト「ツール」「オプション」
「セキュリティ」のタブに戻りますので、
「デジタルID」をクリックします。



B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B 1 - 5) Microsoft Outlook Express デジタル証明書の確認



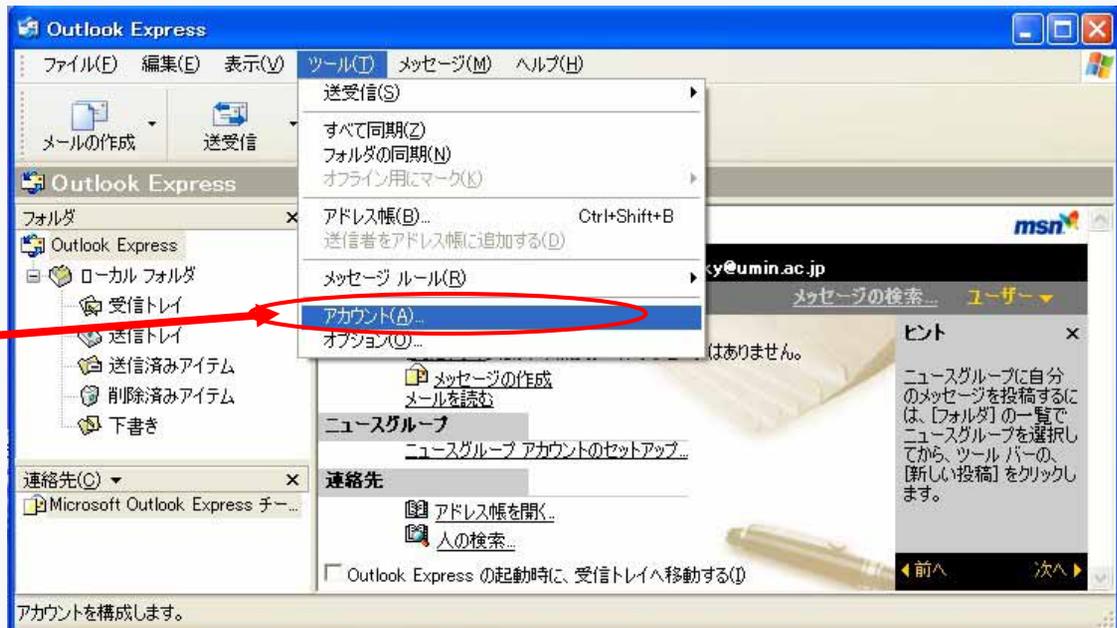
「デジタルID」の「個人」タブにデジタル証明書が追加されていることを確認します。

B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B1 - 6) Microsoft Outlook Express アカウントごとに
デジタル証明書を有効にする

各アカウントごとに
デジタル証明書を有効に
する必要があります。

まずメイン画面
「ツール」「アカウント」
を選択して開きます。

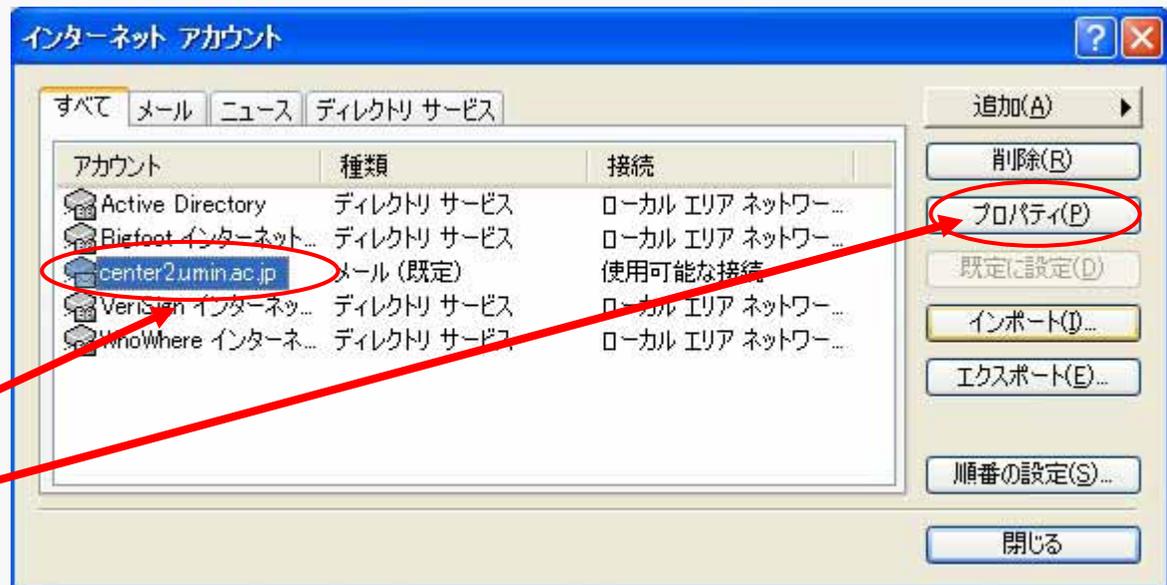


B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B 1 - 7) Microsoft Outlook Express アカウントごとに
デジタル証明書を有効にする

暗号化を設定したい
アカウントを選択します。
(複数ある場合は
同様の作業を繰り返して
ください。)

メールのアカウントを
選択し、
「プロパティ」を
クリックします。



B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B 1 - 8) Microsoft Outlook Express アカウントごとに
デジタル証明書を有効にする

メールアカウントのプロパティを開いた後、
「セキュリティ」のタブを選択
してください。

「署名の証明書」

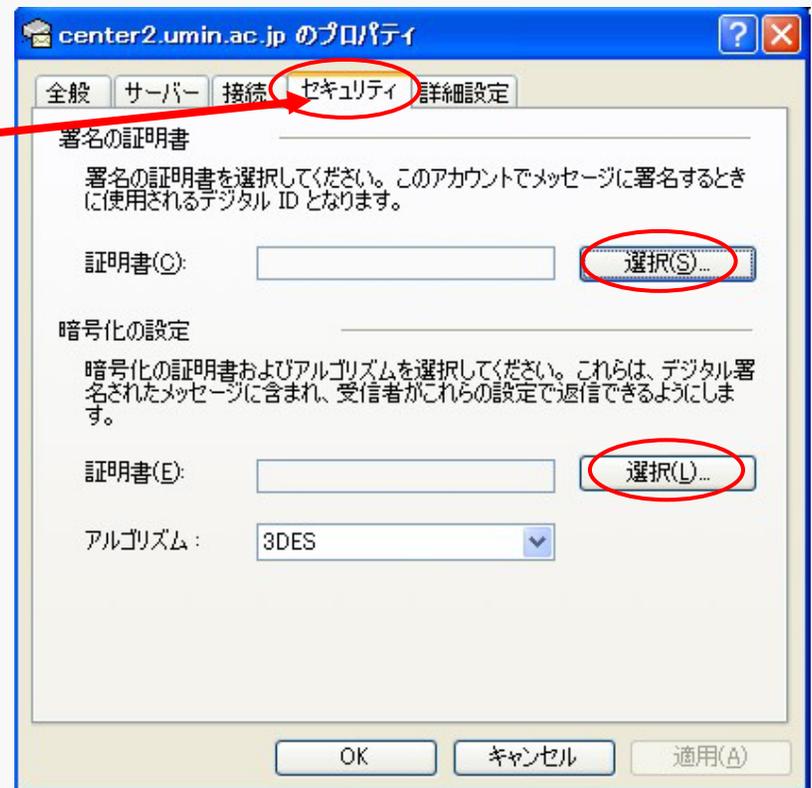
このアカウントでメッセージに署名するときに
デジタルIDとして使用されます。

「選択」をクリックして署名の証明書を決定
してください。(次ページで説明)

「暗号化の設定」

デジタル署名されたメッセージ
に含まれ、受信者がこれらの設定で返信で
できるようにします。「選択」をクリックして
暗号化の証明書を決定してください。

(次ページで説明)



B . 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B1 - 9) Microsoft Outlook Express アカウントごとに
デジタル証明書を有効にする

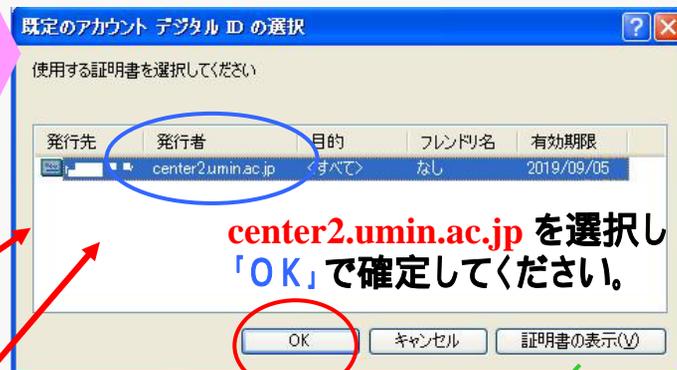
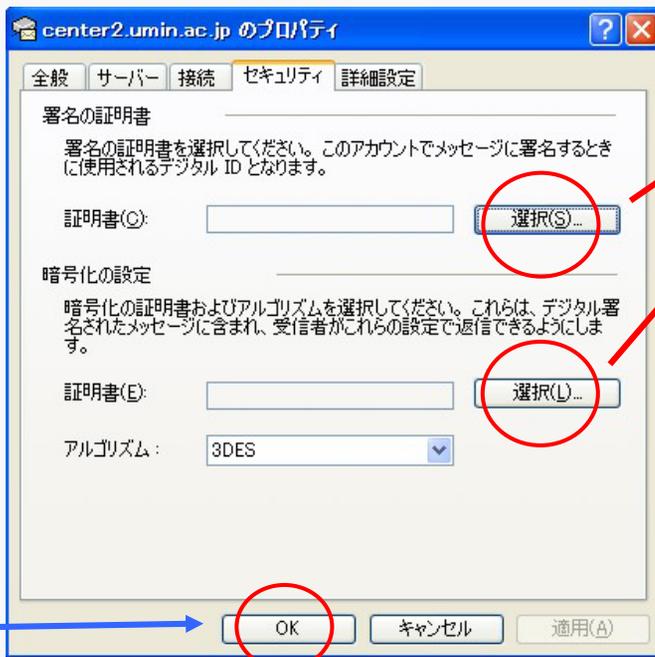
メールアカウント
プロパティ
「セキュリティ」タブ

「署名の証明書」
「暗号化の設定」

それぞれ
「選択」から証明書
を選択してください。

「OK」で確定
してください。

以上で公開鍵により暗号化されたメールを受信(解読)する準備ができました。



C . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行：証明書の検索

〈暗号化してメールを送信する〉

送信相手に、暗号化したメールを送信する場合

相手の**公開鍵**でメールを暗号化し、送信します。

UMIN-IDから、相手の公開鍵を**検索**できます。

(送信相手が、公開鍵を発行している必要があります。)

C . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行：証明書の検索

送信相手のUMIN-IDを検索し、公開鍵の設定がされていれば、公開鍵証明書をダウンロードし、メールソフトに設定することで、暗号化して送信することができます。
(送信相手が発行した公開鍵で暗号化したメールの送信ができます)

(登録者用ページ トップページ)

公開鍵検索

検索するUMIN IDを入力して検索ボタンを押してください

UMIN ID:

ルート証明書

[こちらよりダウンロードして下さい](#)

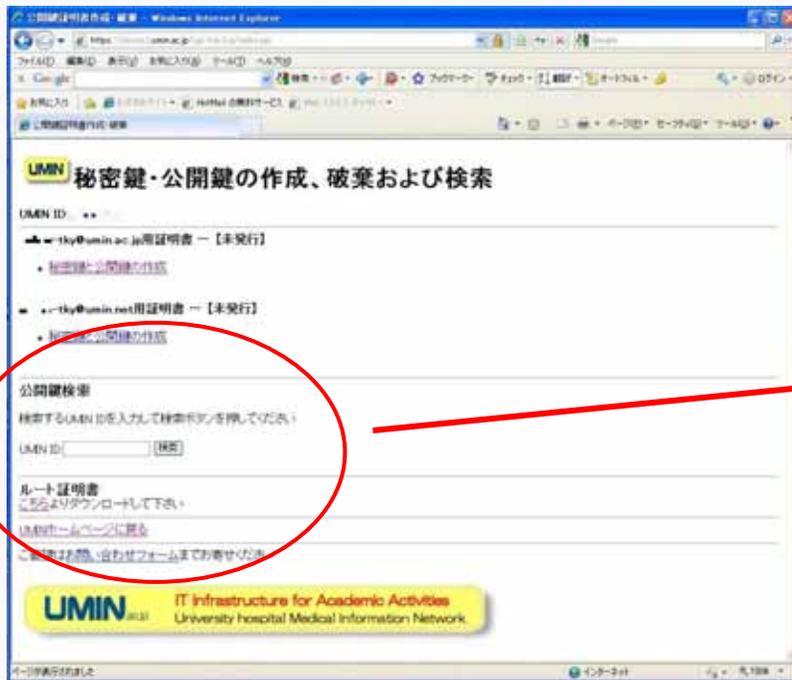
[UMINホームページに戻る](#)

ご要望は[お問い合わせフォーム](#)までお寄せください

C. 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行：証明書の検索

（ 登録者用ページ トップページ ）



トップページの「公開鍵検索」に送信相手のumin-IDを入力する。(メールアドレス: ~@umin.ac.jpの~部分)

公開鍵検索

検索するUMIN IDを入力して検索ボタンを押してください

UMIN ID:

ルート証明書

[こちら](#)よりダウンロードして下さい

[UMINホームページに戻る](#)

ご要望は[お問い合わせフォーム](#)までお寄せください

C . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行：証明書の検索

相手のumin-IDを入力する。相手の「公開鍵」が存在していれば、検索結果が表示される。

UMIN 公開鍵検索結果

UMIN ID: ■■■■

検索対象ユーザ: ■■■■

- @umin.ac.jpのS/MIME公開鍵証明書をダウンロードする

[登録者用ページに戻る](#) [UMINホームページに戻る](#)

[ご要望はお問い合わせフォームまでお寄せください](#)

相手先の公開鍵証明書をダウンロードします。



ファイル名:
XXXX-XXX.ac.jp.cer

お使いのメールソフトに設定します。

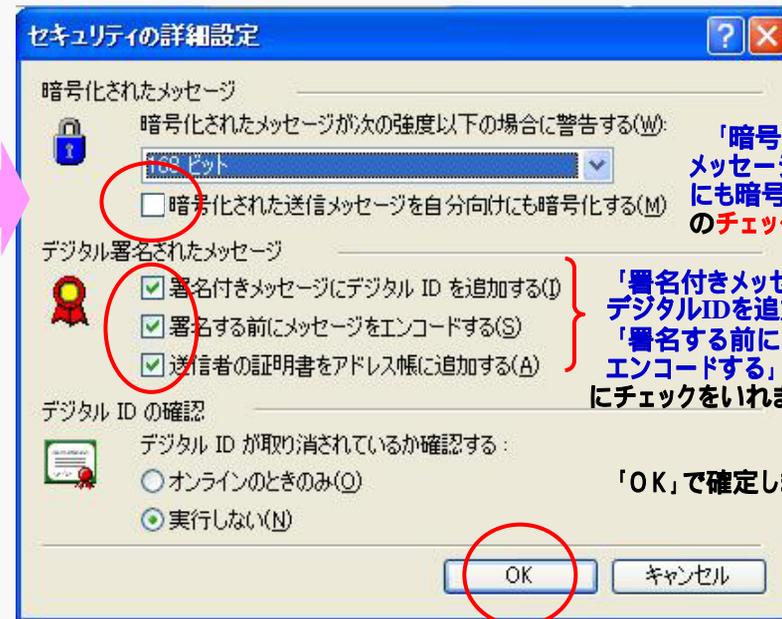
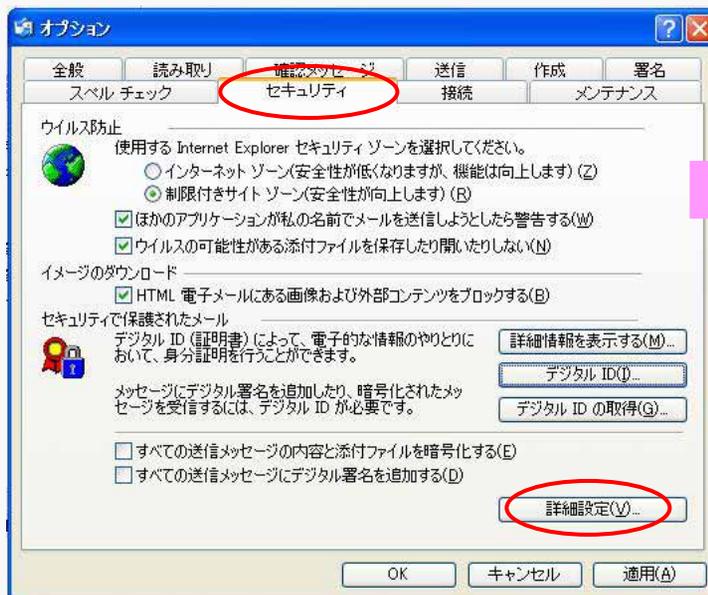
C . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行：証明書の検索

（ 特定の送信相手の公開鍵を設定し、暗号化してメールを送信する ）

(C1 - 1) Microsoft Outlook Express

メールソフト起動後、「ツール」「オプション」をひらき、「セキュリティ」のタブを選択し、「詳細設定」をクリックします。



「暗号化された送信メッセージを自分向けにも暗号化する」のチェックを外します。

「署名付きメッセージにデジタルIDを追加する」「署名する前にメッセージをエンコードする」にチェックをいれます。

「OK」で確定します。

C . 秘密鍵・公開鍵の作成

秘密鍵・公開鍵の発行：証明書の検索

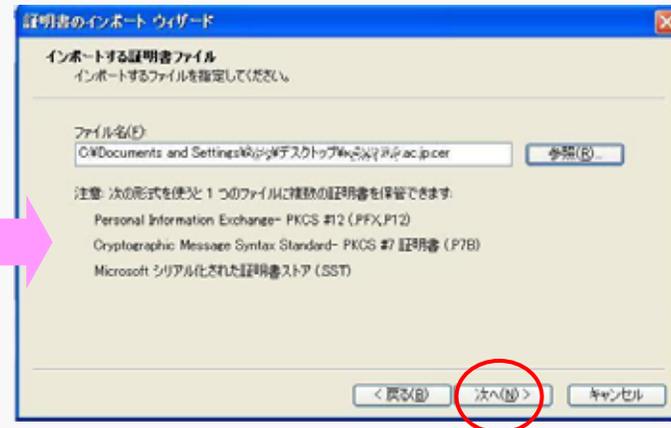
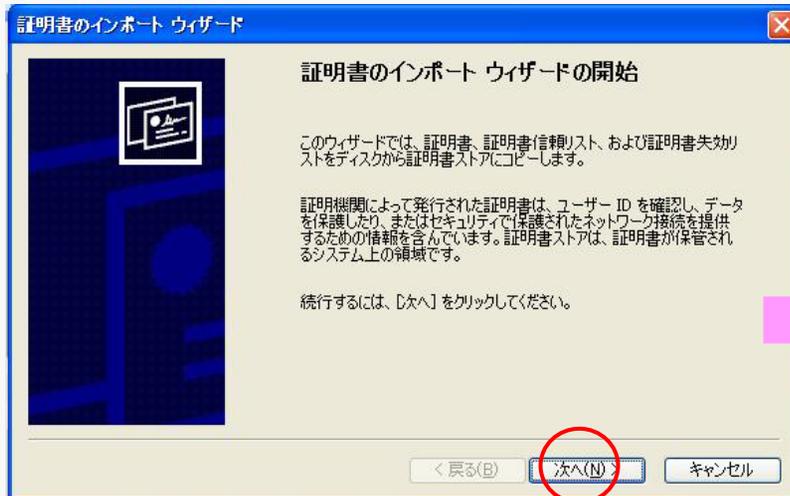
（特定の送信相手の公開鍵を設定し、暗号化してメールを送信する）

(C1 - 2) Microsoft Outlook Express



事前にダウンロードした**XXXX-XXX.ac.jp.cer**
(送信相手の公開鍵)ファイルを**ダブルクリック**してください。

インポートウィザードが開始されます。

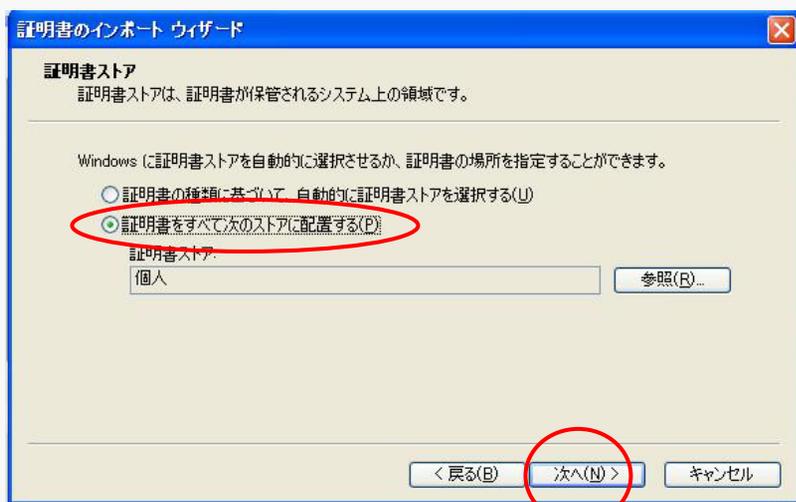


C . 秘密鍵・公開鍵の作成

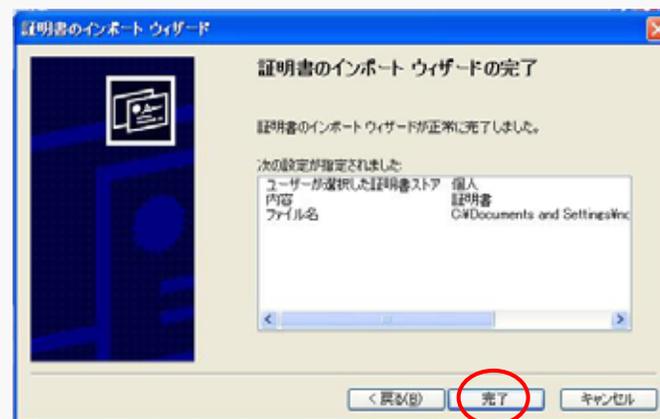
秘密鍵・公開鍵の発行：証明書の検索

(特定の送信相手の公開鍵を設定し、暗号化してメールを送信する)
(C 1 - 3) Microsoft Outlook Express

「証明書をすべてストアに配置する」を選択。
証明書ストアは「個人」。



「次へ」をクリックします。



「完了」をクリック

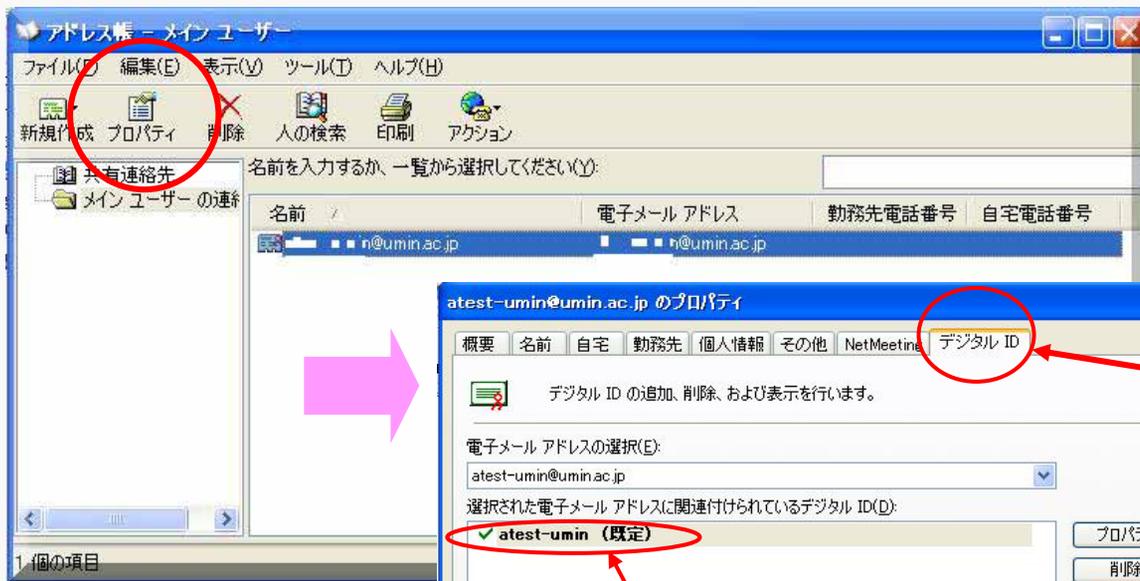


メッセージ
「正しくインポート
されました」



C . 秘密鍵・公開鍵の作成

(C1 - 4) Microsoft Outlook Express 署名、暗号化したメールの作成
メール送信相手をアドレス帳に登録して、相手の公開鍵と連携させます。



送信相手のメールアドレスを
アドレス帳に登録します。

該当のアドレスを選択後、
「プロパティ」をクリックします。

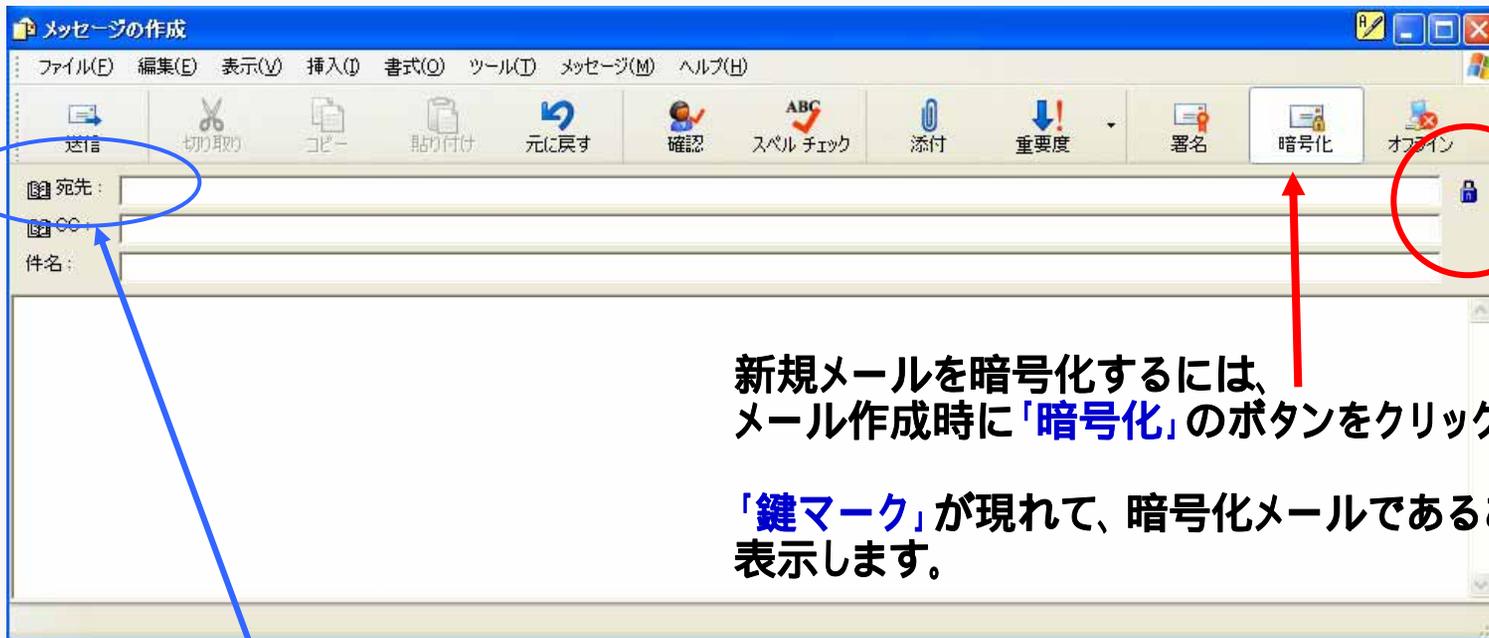
プロパティ内の「デジタルID」のタ
グを開け、該当の公開鍵 (XXXX-
XXX.cer) をインポートします。

デジタルIDが追加されました。

(以上で、暗号化メールの
送信準備ができました)

C . 秘密鍵・公開鍵の作成

(C1 - 5) Microsoft Outlook Express 署名、暗号化したメールの作成
メールを暗号化して送信するために、**送信するメール**に設定を行います。



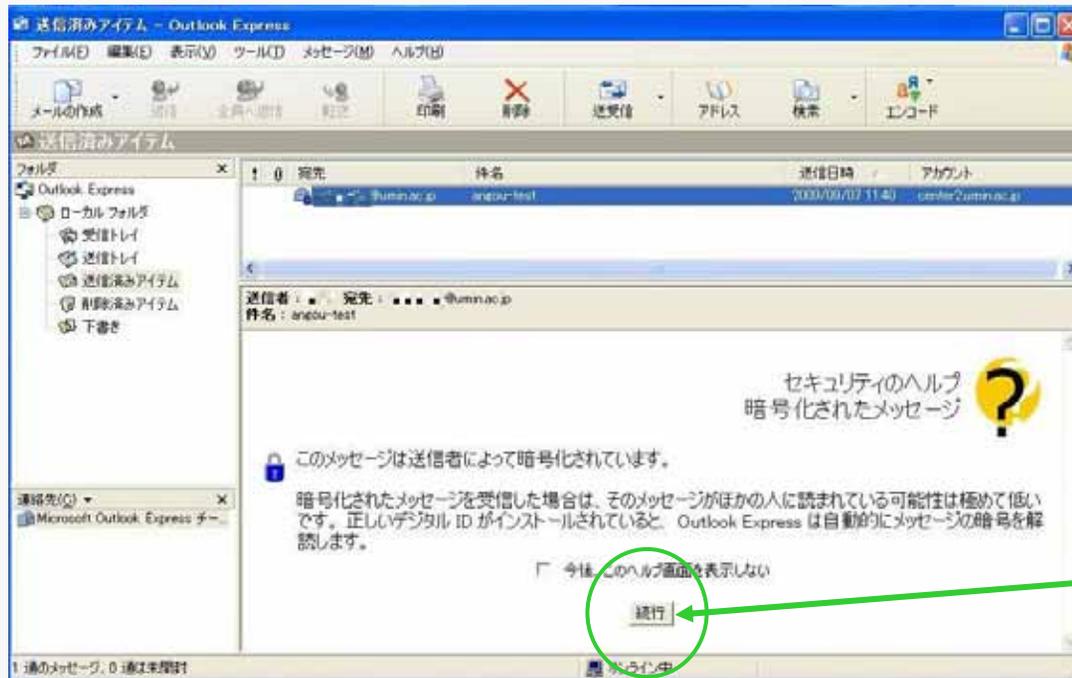
新規メールを暗号化するには、
メール作成時に「暗号化」のボタンをクリックします。

「鍵マーク」が現れて、暗号化メールであることを
表示します。

送信先アドレスは、事前に「アドレス帳」登録し、
公開鍵をインポートしておく必要があります。(前ページ C1 - 4で手順説明)

C . 秘密鍵・公開鍵の作成

(C 1 - 6) Microsoft Outlook Express 署名、暗号化したメールの作成



送信後のメールは左のように表示されます。

「続行」をクリックすると、内容が表示されます。

メール暗号化:秘密鍵・公開鍵の作成

作業完了