

メール暗号化：秘密鍵・公開鍵の作成

作業手順

Outlook 2007

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2007 (Outlook 2007)

**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①～④
⑤～⑧ (1) アウトルック2007 (Outlook 2007)

A. 秘密鍵・公開鍵の作成

①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。



The screenshot shows a web browser window titled "center2.umin.ac.jp へ接続". The page has a blue header with a key icon. The main content area is light yellow and contains the following text: "umin-user のサーバー center2.umin.ac.jp にはユーザー名とパスワードが必要です。". Below this, there are two input fields: "ユーザー名(U):" and "パスワード(P):". The "ユーザー名(U):" field has a dropdown menu with a blue icon and a red circle with the number 1 next to it. The "パスワード(P):" field has a red circle with the number 2 next to it. A red arrow points from the bottom left towards the password field. Below the input fields, there is a checkbox labeled "パスワードを記憶する(R)". At the bottom right, there are two buttons: "OK" and "キャンセル".

- ①ユーザー名に UMIN IDを入力
- ②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

②「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」

① XXXX-XXX@umin.ac.jp用証明書

② XXXX-XXX@umin.net用証明書

③ 公開鍵検索の入力枠

④ ルート証明書

A. 秘密鍵・公開鍵の作成

③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

④秘密鍵・公開鍵の発行

UMIN S/MIME用公開鍵証明書の発行

UMIN ID: ■ -tky

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

内容確認

- 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: ■ -tky
- 電子メールアドレス: ■ -tky@umin.ac.jp
- 有効期間: 10年

①有効期間を選択

②「発行」をクリック

発行

10年
3年
1年

[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

⑤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。

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

⑥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

⑦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。

The screenshot shows the UMIN website's 'Secret Key and Public Key Creation, Deletion, and Search' page. The page is titled 'UMIN 秘密鍵・公開鍵の作成、破棄および検索'. It displays the user's UMIN ID as 'tly'. Under the 'Issued' section, there is a link to 'Download the PKCS12 format client certificate' which is circled in red. Below this, under the 'Not Issued' section, there is a link to 'Create secret key and public key'. At the bottom, there is a 'Public Key Search' section with a search box and a 'Search' button. A red arrow points from the 'ルート証明書' (Root Certificate) text to a link labeled 'ルート証明書' which is also circled in red.

A. 秘密鍵・公開鍵の作成

⑧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。

The screenshot shows the UMIN web interface for managing keys. The title is "秘密鍵・公開鍵の作成、破棄および検索". Below the title, there is a section for "UMIN ID" with a dropdown menu. The main content area is divided into two sections: "tky@umin.ac.jp用証明書 ... 【発行済】" and "tky@umin.net用証明書 ... 【未発行】". The first section contains a list of actions: "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" and "pkcs12形式のクライアント証明書をダウンロードする". The second section contains a list of actions: "秘密鍵と公開鍵の作成". A red circle highlights the "pkcs12形式のクライアント証明書をダウンロードする" link, and a red arrow points from the text on the left to this link.

UMIN 秘密鍵・公開鍵の作成、破棄および検索

UMIN ID: [dropdown]

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

⑨秘密鍵・公開鍵の発行

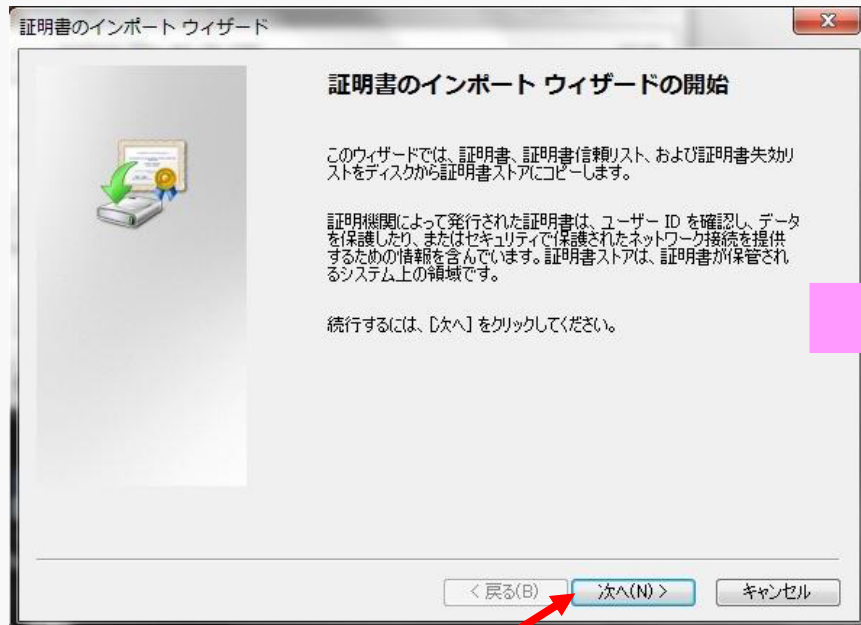


鍵マークのついた「～.p12」形式ファイルがダウンロードされたことをご確認ください。

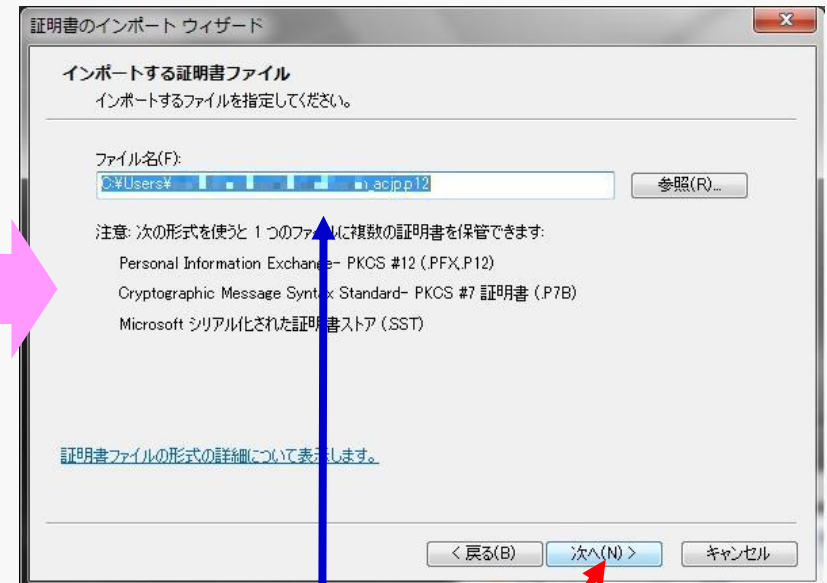
ダブルクリックで「証明書のインポートウィザード」が開始します。

A. 秘密鍵・公開鍵の作成

⑩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

⑪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】

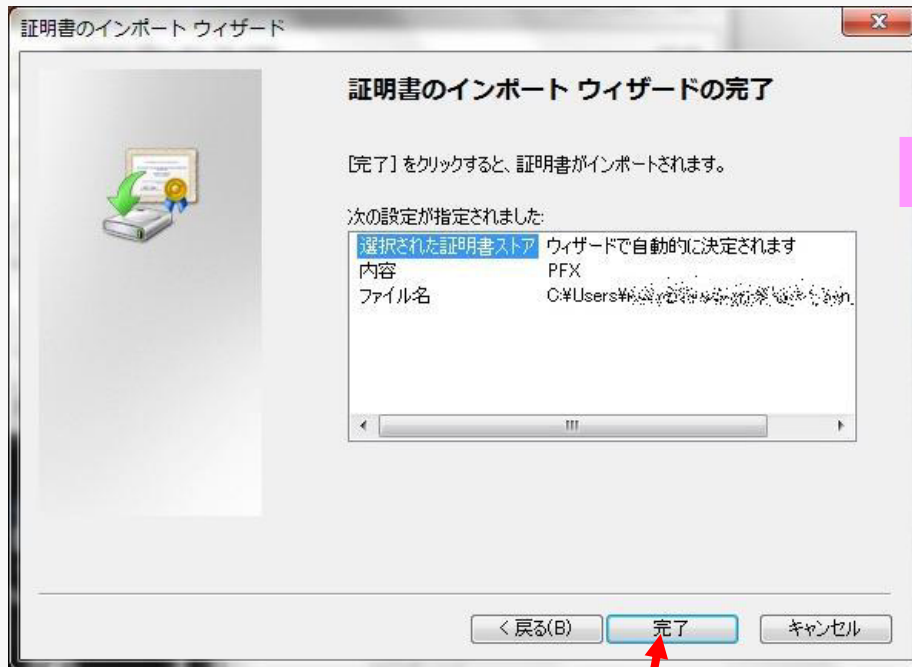
「パスワード」には何も入力せずに
そのまま「次へ」をクリック

「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

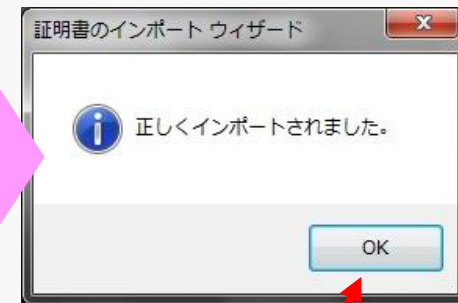
A. 秘密鍵・公開鍵の作成

⑫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

⑬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

⑭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]



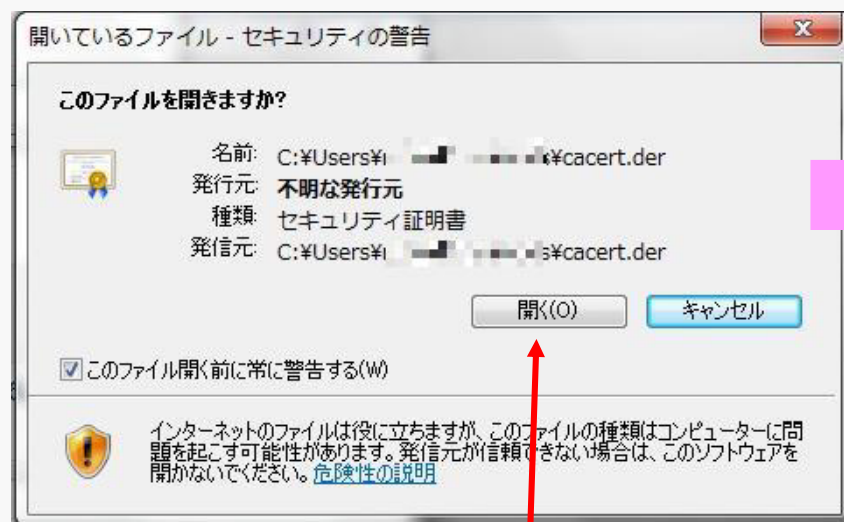
証明書アイコンの「cacert.der」形式ファイルがダウンロードされたことをご確認ください。

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

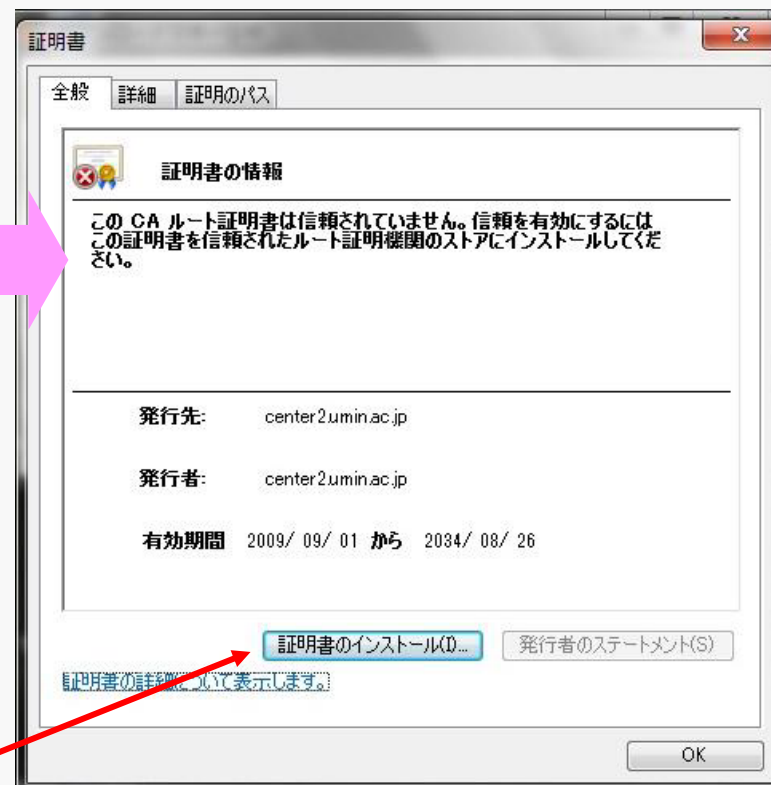
⑮秘密鍵・公開鍵の発行 (証明書インポート)

【ルート証明書のインポート ウィザード】



①ルート証明書のファイル「cacert.der」を開きます。

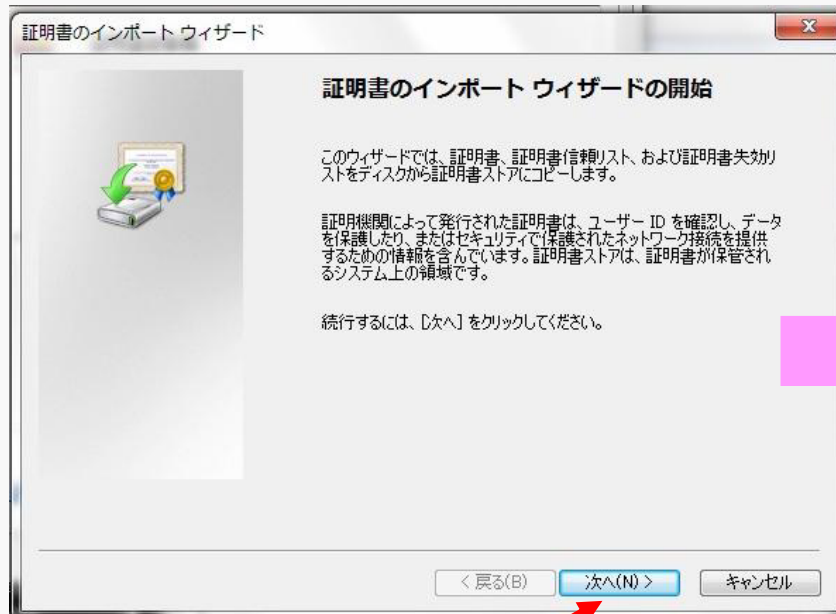
②証明書のインストールを開始します。



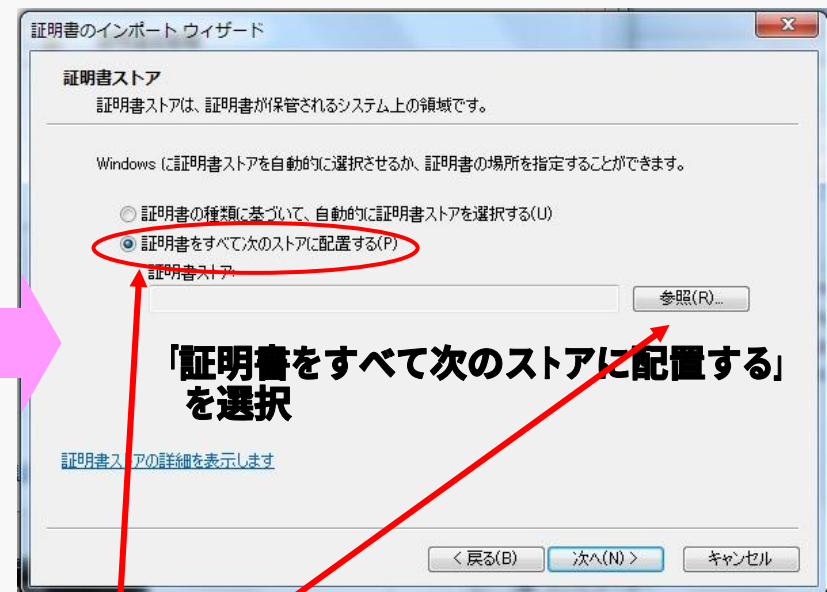
A. 秘密鍵・公開鍵の作成

⑩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】



- ① 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。

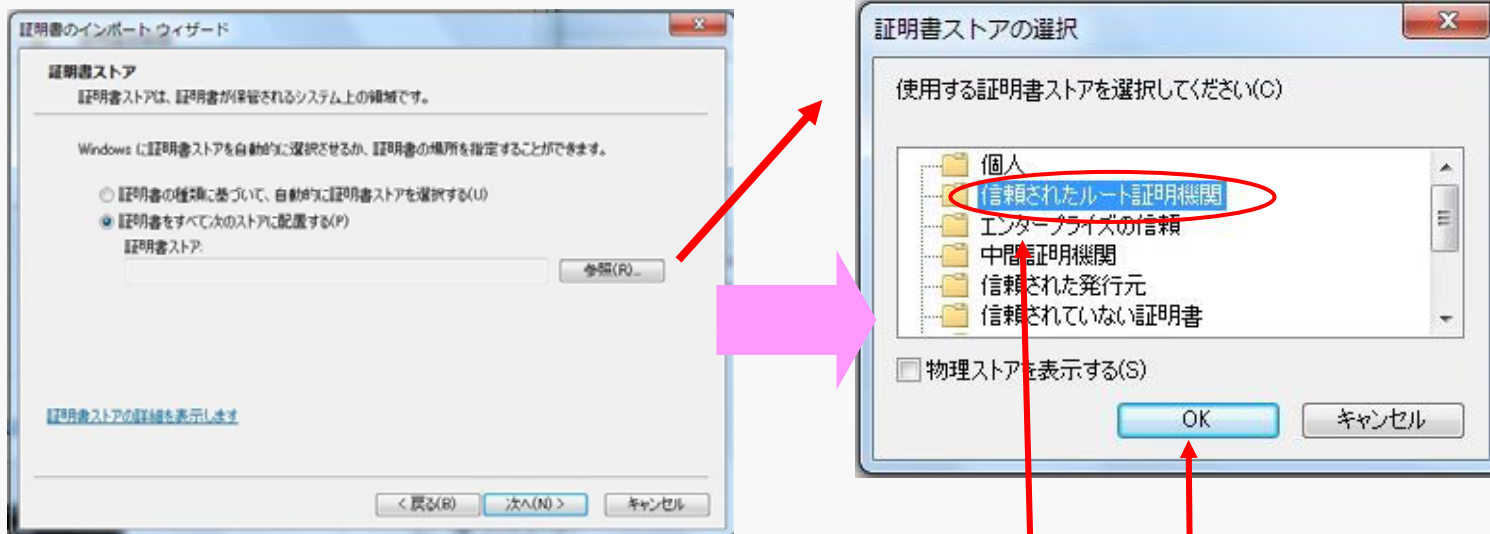


- ② 「証明書をすべて次のストアに配置する」を選択し、「参照」をクリックします。

A. 秘密鍵・公開鍵の作成

⑩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】



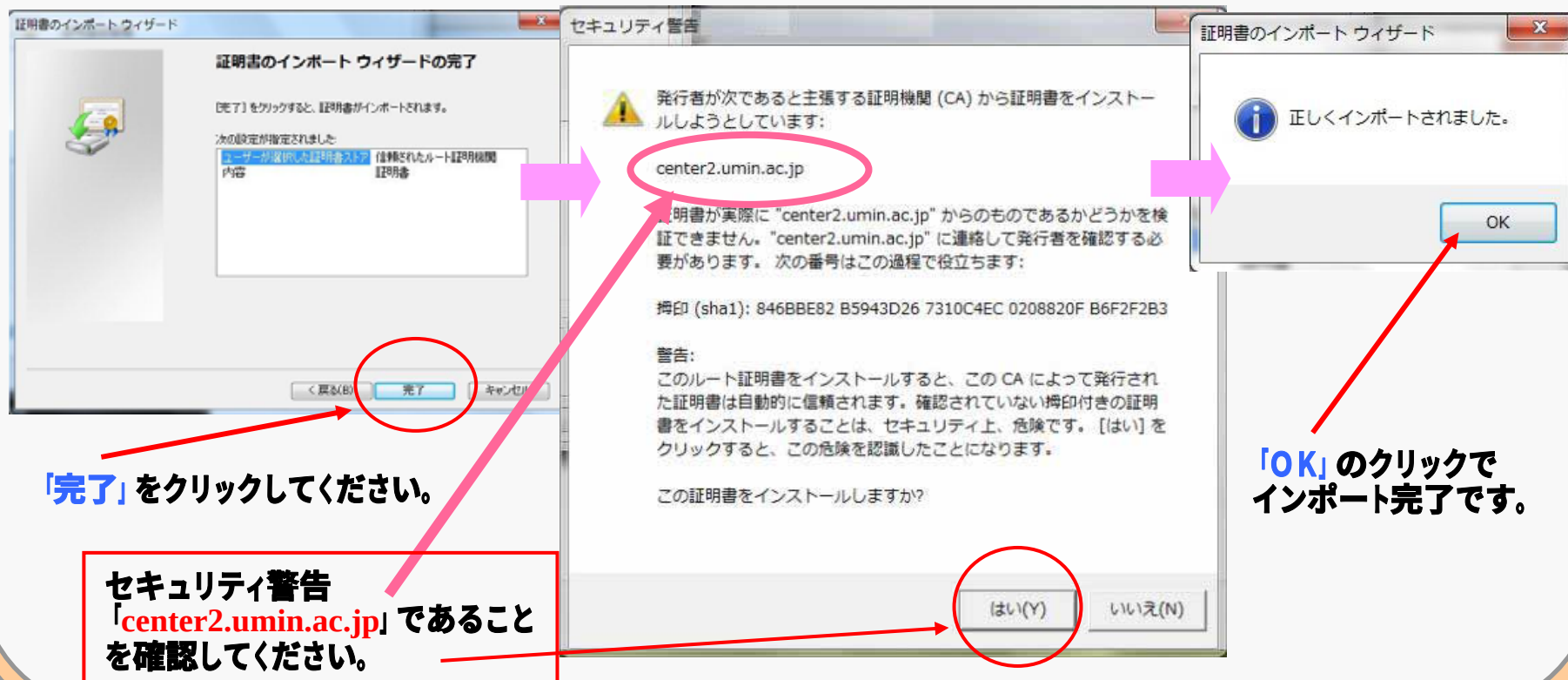
①「参照」をクリックすると「証明書ストアの選択」が開きます。

②「信頼されたルート証明機関」を選択し、「OK」をクリックしてください。

A. 秘密鍵・公開鍵の作成

⑰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】



「完了」をクリックしてください。

セキュリティ警告
「center2.umin.ac.jp」であることを
確認してください。

「OK」のクリックで
インポート完了です。

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

(B1-1) Outlook 2007 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。

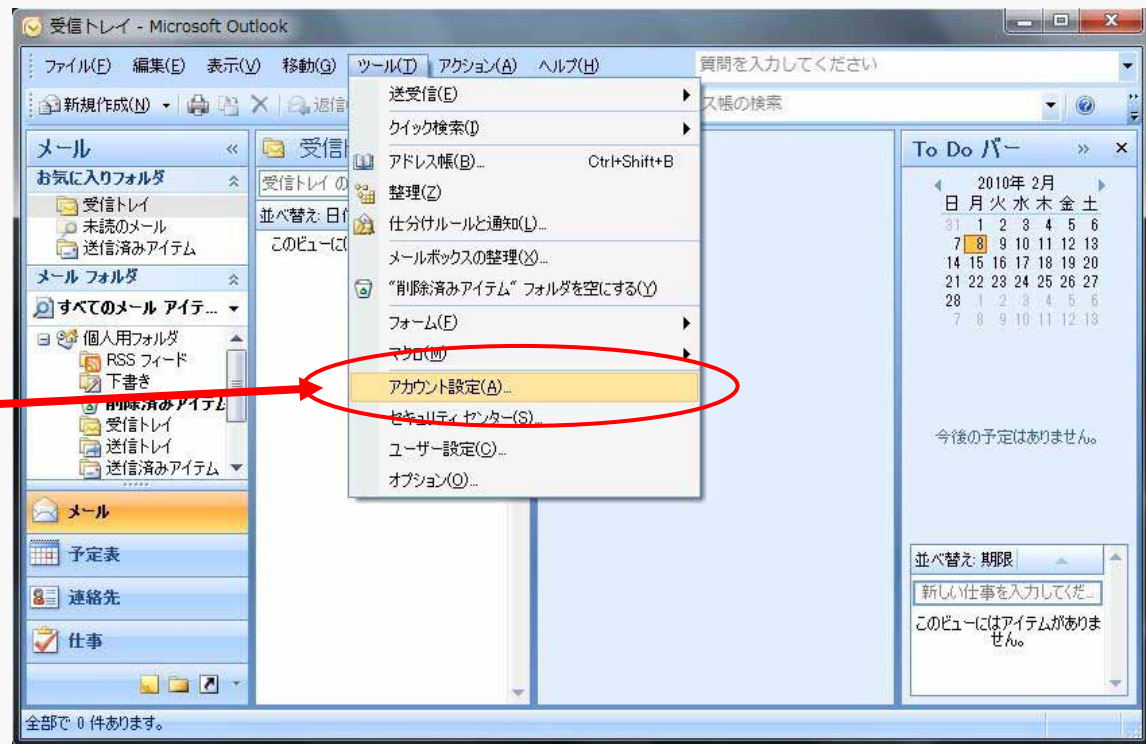
アカウントごとにデジタル証明書を有効にすることにより、メールへの署名や暗号化が可能になります。

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) Outlook 2007 メール 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」→「アカウント設定」
を選択して開きます。

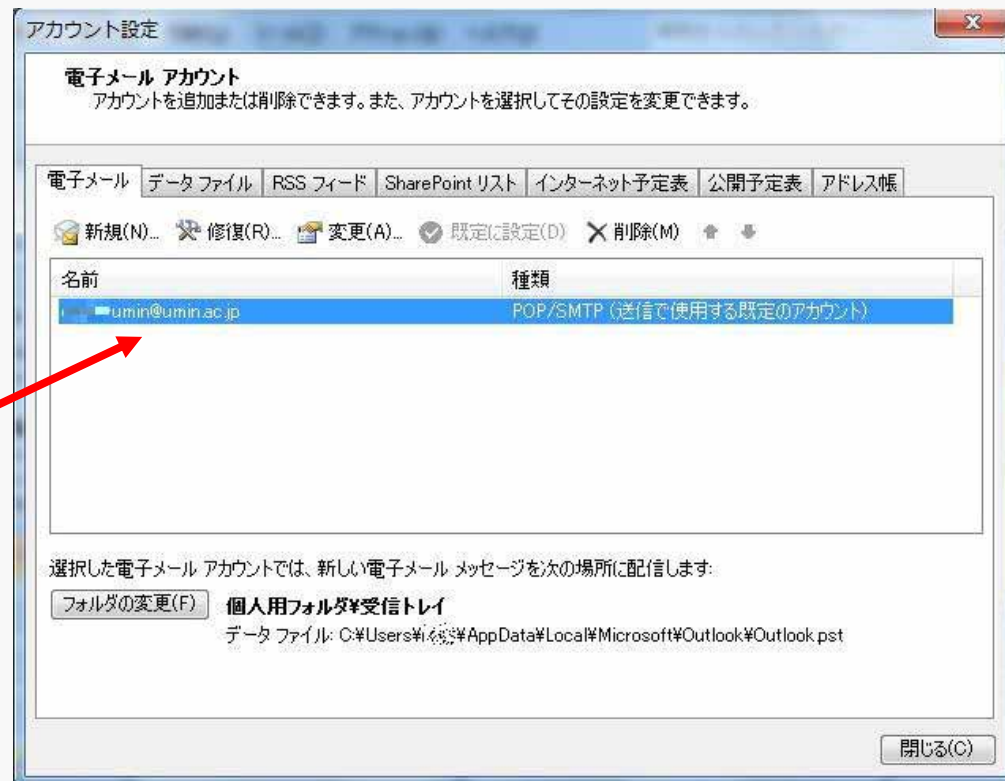


B. 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B1-3) Outlook 2007 メール アカウントごとに
デジタル証明書を有効にする

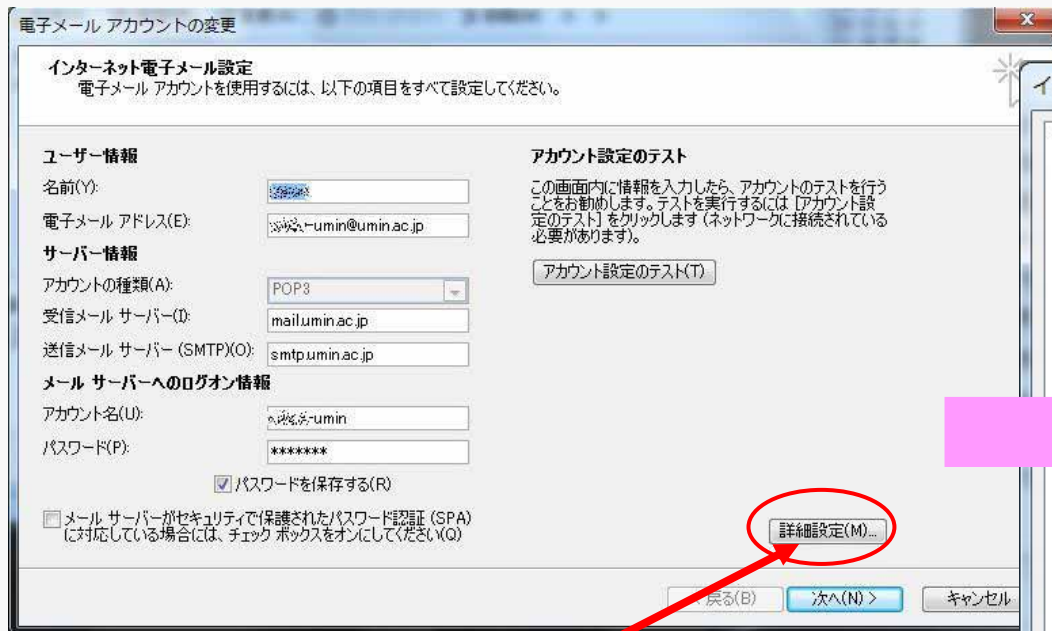
暗号化を設定したい
アカウントを選択します。
(複数ある場合は
同様の作業を繰り返して
ください。)

メールのアカウントを
ダブルクリックして
開きます。

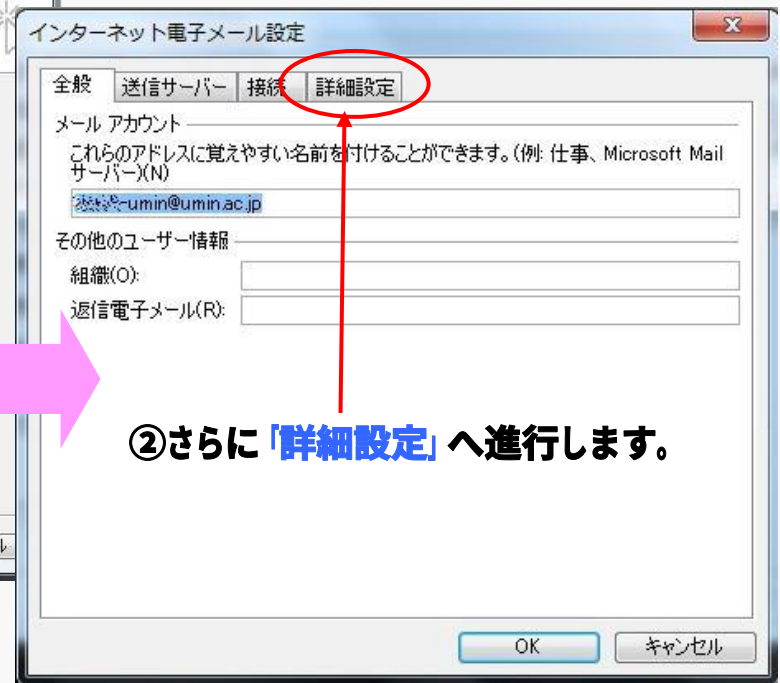


B. 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B1-4) Outlook 2007 メール アカウントごとに
デジタル証明書を有効にする



① 「詳細設定」をクリックして次の画面へ



②さらに「詳細設定」へ進行します。

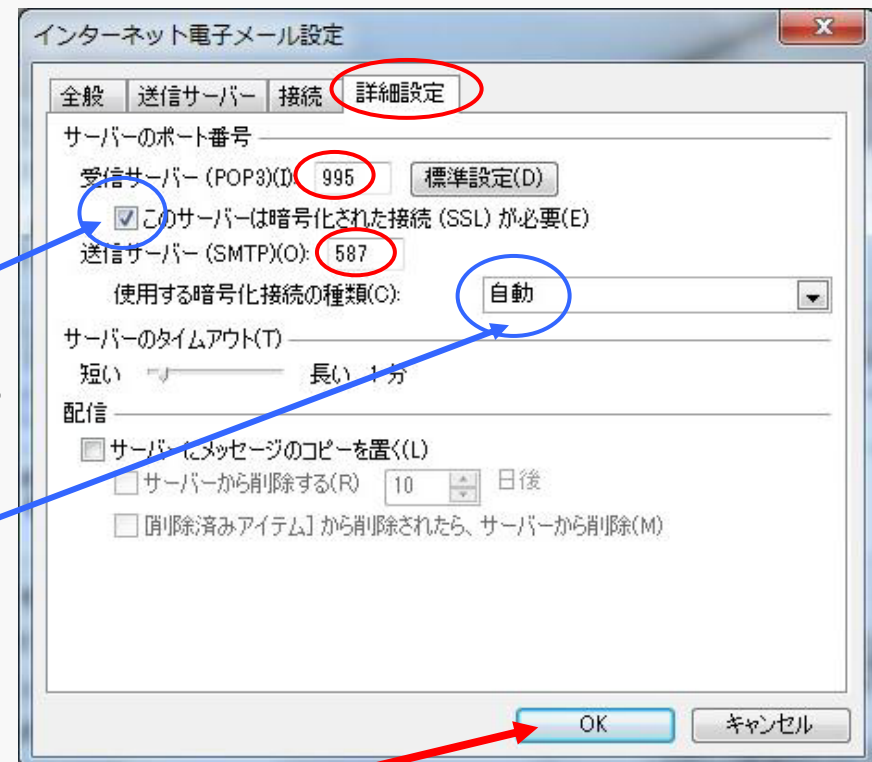
B. 秘密鍵・公開鍵の作成

各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B1-5) Outlook 2007 メール アカウントごとに
デジタル証明書を有効にする

インターネット電子メール設定
「詳細設定」のタブを選択して開いた後、

①受信サーバー (pop3×I) 「995」を確認。
「このサーバーはセキュリティで保護された
接続 (SSL) が必要」にチェックを入れてください。

②送信サーバー (SMTP×O) 「587」を確認。
使用する暗号化接続の種類 「自動」
にしてください。



③ 最後に「OK」をクリックしてください

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
(B1-6) Outlook 2007 メール アカウントごとに
デジタル証明書を有効にする

電子メール アカウントの変更

インターネット電子メール設定
電子メール アカウントを使用するには、以下の項目をすべて設定してください。

ユーザー情報

名前(Y): [text box]

電子メール アドレス(E): [text box]

サーバー情報

アカウントの種類(A): [dropdown menu: POP3]

受信メール サーバー(I): [text box: mail.umin.ac.jp]

送信メール サーバー (SMTP)(O): [text box: smtp.umin.ac.jp]

メール サーバーへのログイン情報

アカウント名(U): [text box: umin]

パスワード(P): [password box: *****]

☒ パスワードを保存する(R)

☐ メール サーバーがセキュリティで保護されたパスワード認証 (SPA) に対応している場合には、チェック ボックスをオンにしてください(Q)

アカウント設定のテスト

この画面内に情報を入力したら、アカウントのテストを行うことをお勧めします。テストを実行するには [アカウント設定のテスト] をクリックします (ネットワークは接続されている必要があります)。

アカウント設定のテスト(T)

詳細設定(M)...

< 戻る(B) **次へ(N) >** キャンセル

①「次へ」で確定してください。

電子メール アカウントの変更

セットアップが完了

アカウントのセットアップに必要な情報がすべて入力されました。
ウィザードを終了するには、[完了] をクリックしてください。

< 戻る(B) **完了**

②セットアップが完了しました。「完了」をクリックしてください。

C. 秘密鍵・公開鍵の作成

①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ことが必要です。)

C. 秘密鍵・公開鍵の作成

②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

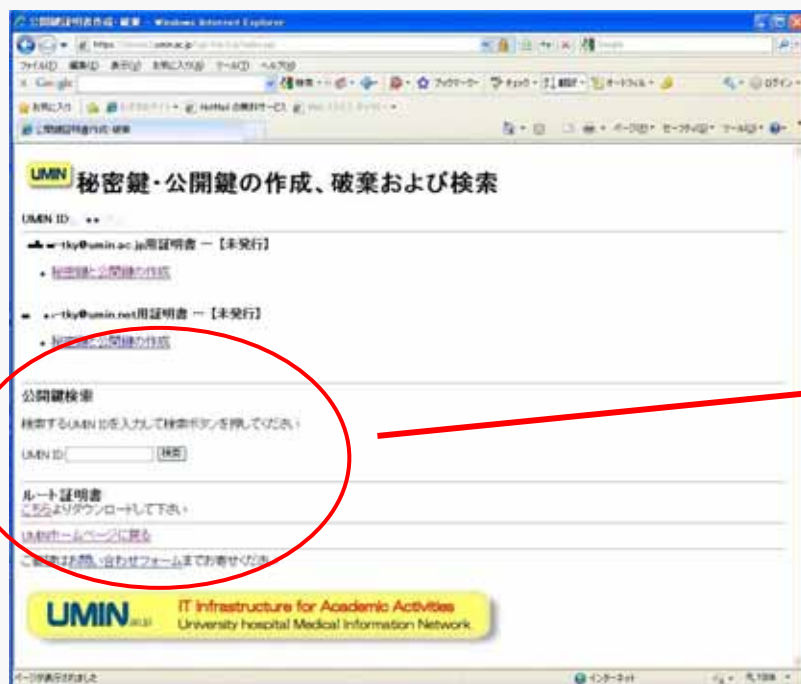
[UMINホームページに戻る](#)

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

③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

④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。

 **公開鍵検索結果**

UMIN ID: ■■■■■■

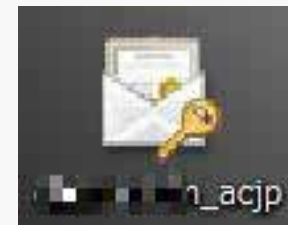
検索対象ユーザ: ■■■■

- @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。

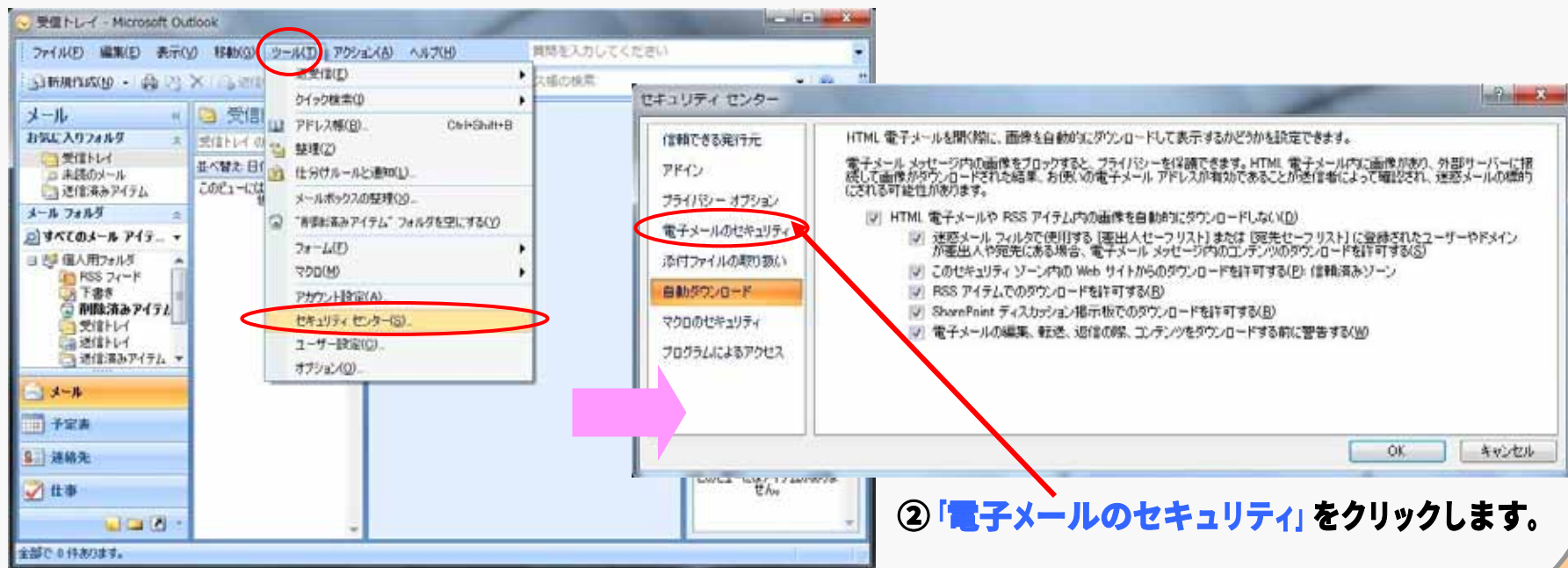
C. 秘密鍵・公開鍵の作成

⑤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 〉

(C2-1) Outlook 2007

①Outlook 2007起動後、「ツール」→「セキュリティセンター」を開きます。



②「電子メールのセキュリティ」をクリックします。

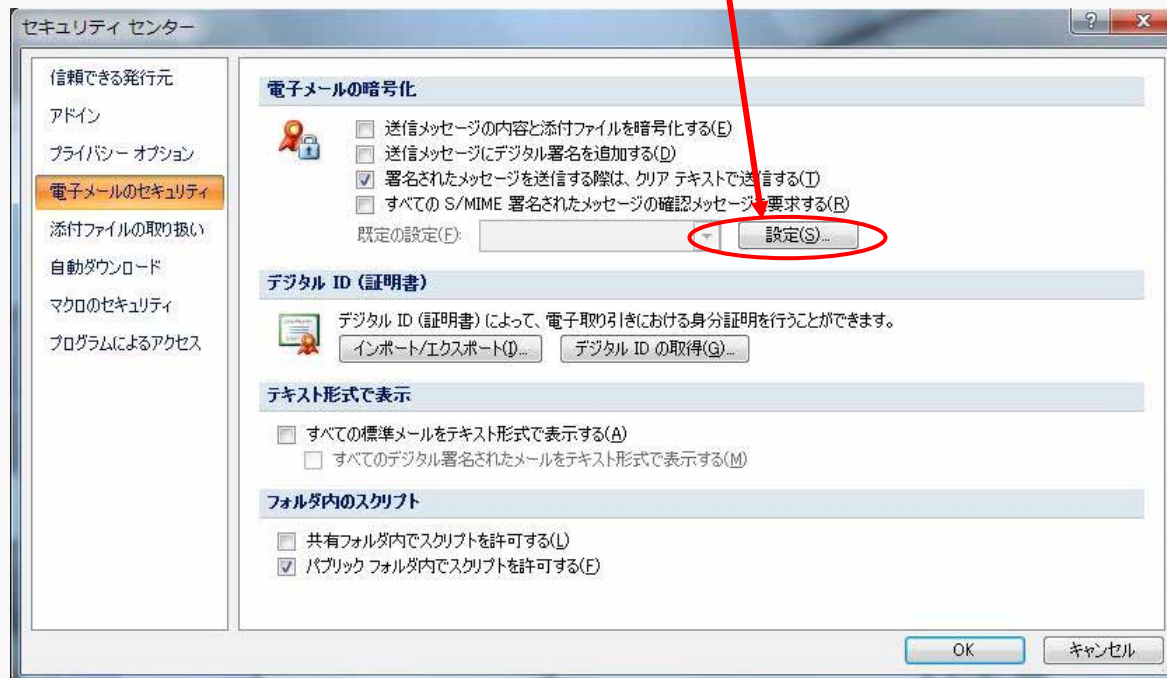
C. 秘密鍵・公開鍵の作成

⑤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 〉

(C2-2) Outlook 2007

①「電子メールのセキュリティ」画面：暗号化の「設定」をクリックします。

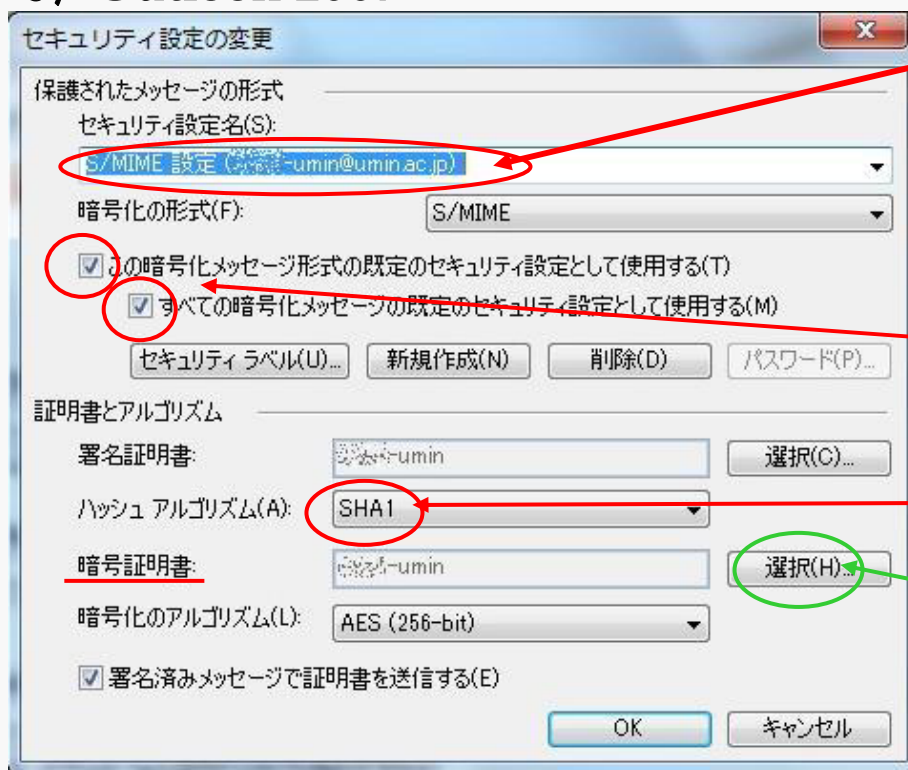


C. 秘密鍵・公開鍵の作成

⑤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 〉

(C2-3) Outlook 2007



①利用するメールアドレスであることを確認。

②「この暗号化メッセージ形式の規定セキュリティ設定として使用する」
「すべての暗号化メッセージの規定セキュリティ設定として使用する」

に[チェック]が入っていることを確認。

③ハッシュアルゴリズムが「SHA1」であることを確認します。

④利用する証明書を選択します。

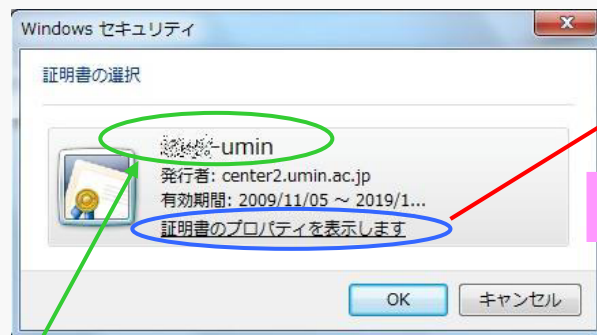
【署名証明書を使用する場合も同様の確認作業をします】

C. 秘密鍵・公開鍵の作成

⑤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 〉

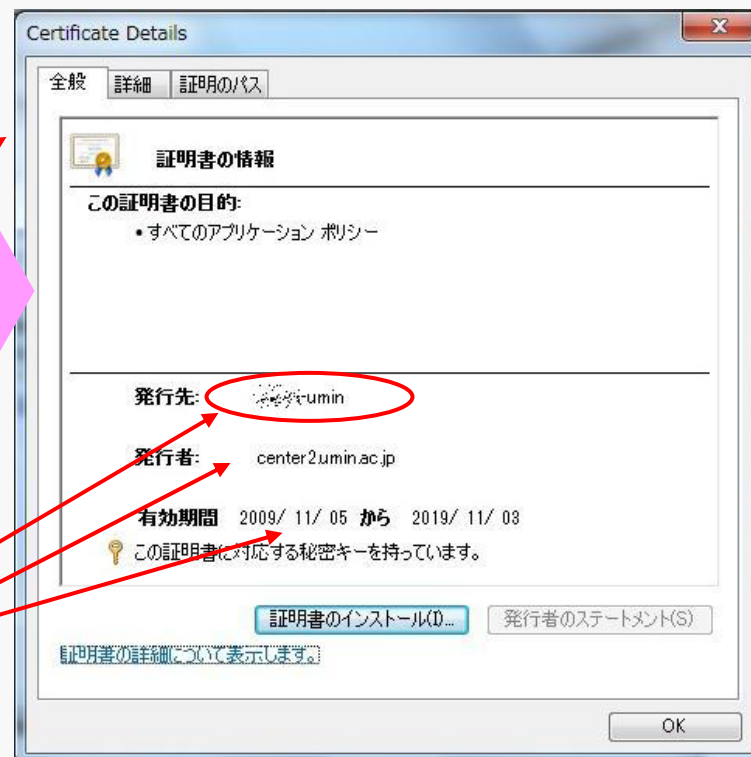
(C2-4) Outlook 2007



①使用する証明書であることを確認。

②証明書のプロパティも確認します。

[署名証明書を使用する場合も
同様の確認作業をします]

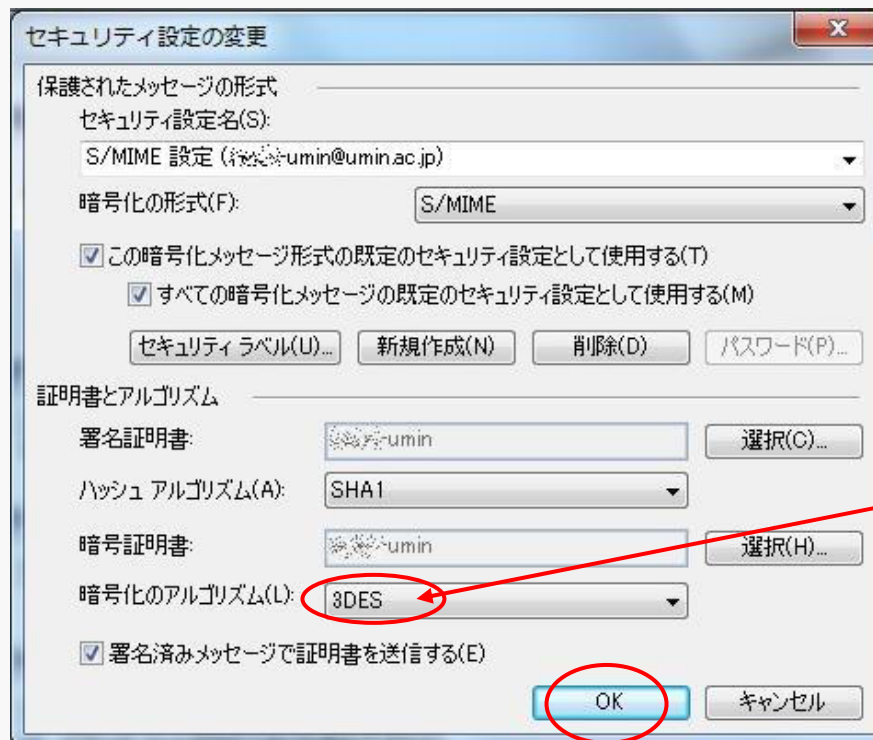


C. 秘密鍵・公開鍵の作成

⑤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 〉

(C2-5) Outlook 2007



暗号化のアルゴリズムを
「3DES」に設定します。

変更が完了したら
「OK」をクリックします。

C. 秘密鍵・公開鍵の作成

⑤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 〉

(C2-6) Outlook 2007



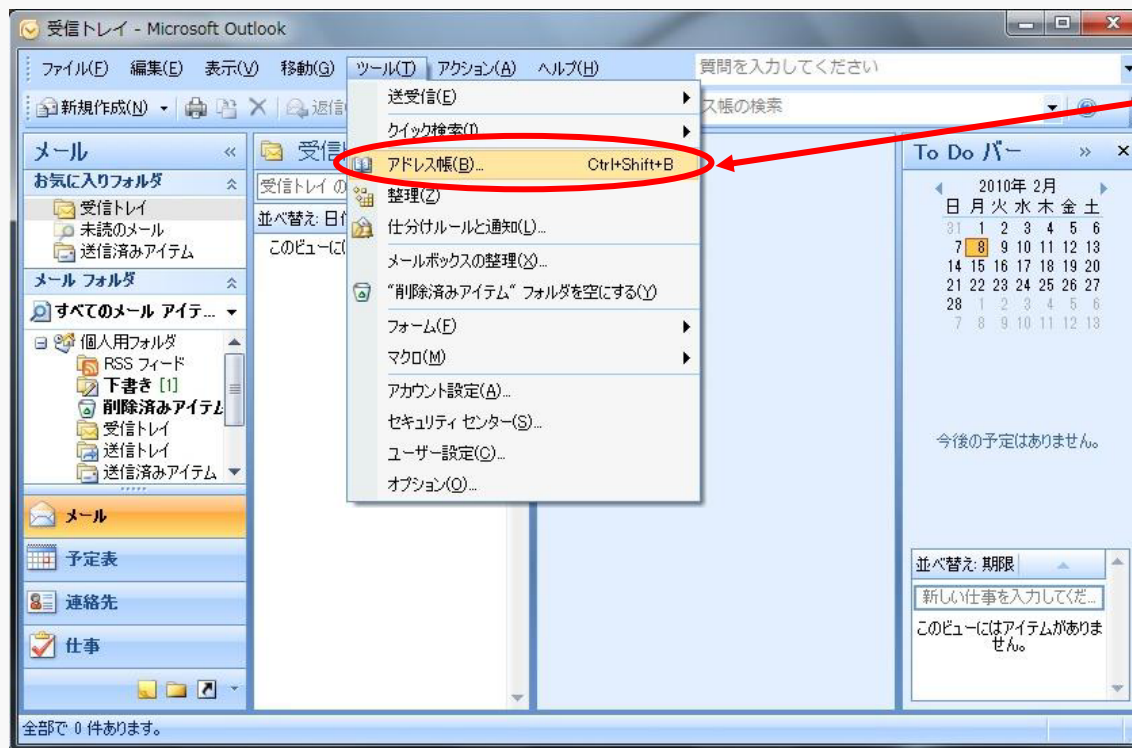
規定の設定が
利用するメールアドレスに
なっていることを確認します。

以上で
送信相手の公開鍵
の設定が完了
しました。

C. 秘密鍵・公開鍵の作成

(C2-7) Outlook 2007 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。



暗号化メールを送信するために
送信相手のメールアドレスを
アドレス帳に登録しておく必要
があります。

アドレス帳に登録したアドレスに
設定済みの相手の公開鍵を
連携させることで

暗号化メールを送信できるよう
になります。

C. 秘密鍵・公開鍵の作成

(C2-8) Outlook 2007 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。

①暗号化して
送信する相手の
メールアドレスで
あることを確認
します。



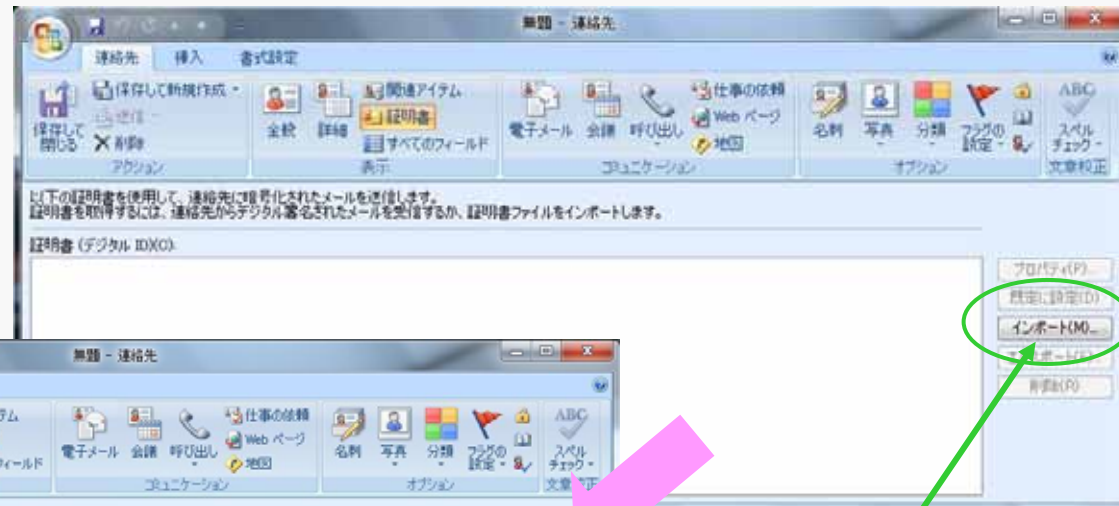
②「証明書」を
クリックします。

C. 秘密鍵・公開鍵の作成

(C2-9) Outlook 2007 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。

①証明書追加の
ウィンドウが
開きます。



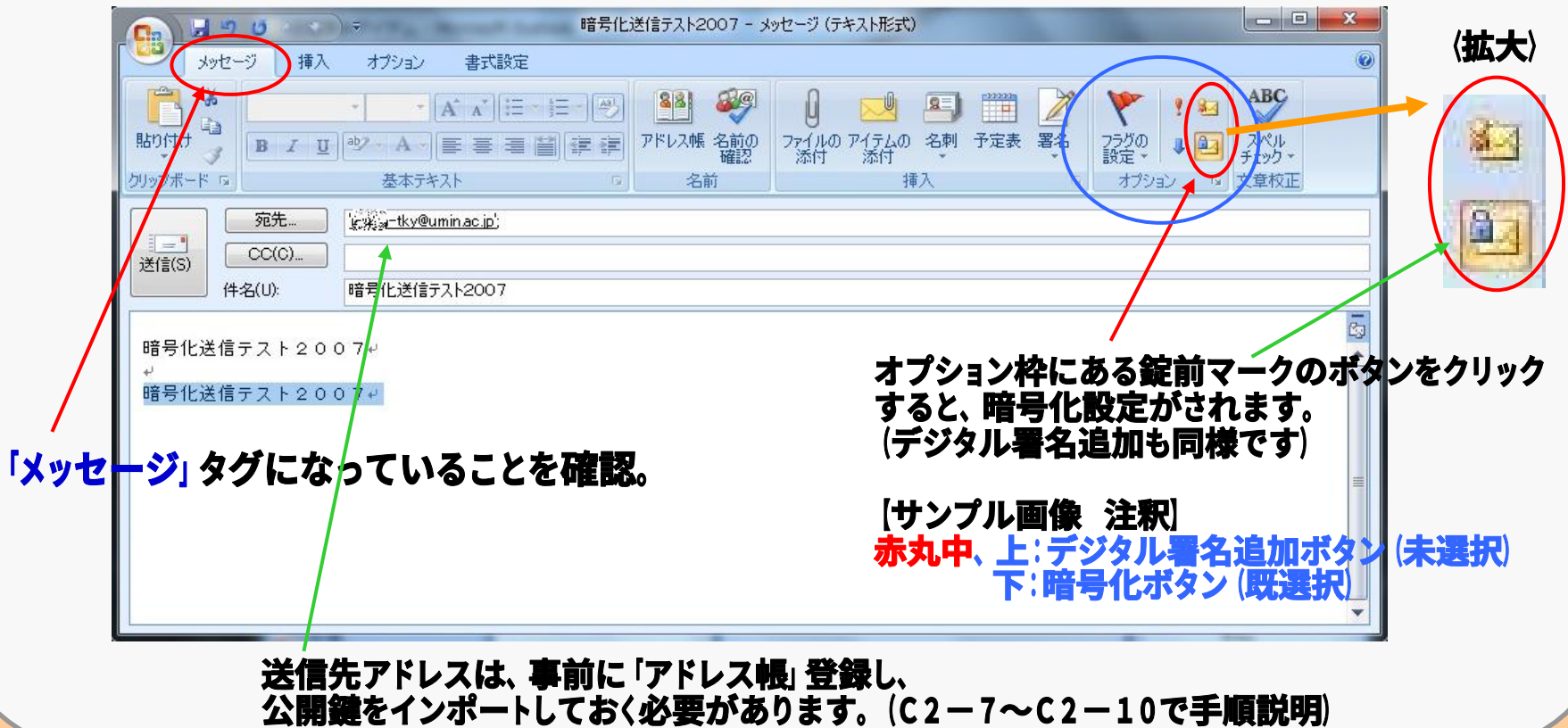
②「インポート」をクリックし、
既にダウンロード済みの
該当先の公開鍵 (XXXX-XXX.ac.jp.cer)
を開くと、この欄に追加されます。

(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

(C2-10) Outlook 2007 暗号化メールの作成

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。



メール暗号化:秘密鍵・公開鍵の作成

作業完了