

メール暗号化:秘密鍵・公開鍵の作成

作業手順

Windows Live メール

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

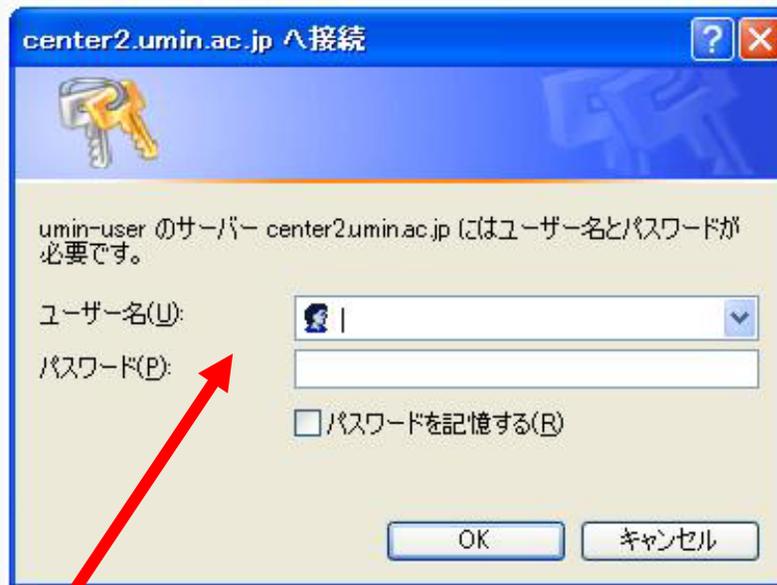
B . 暗号化されたメールを「受信」できるように設定する。
(自分の秘密鍵をご使用のメールソフトへの設定する)
(1) Windows Live メール(Windows Live mail)

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) Windows Live メール(Windows Live mail)

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 ID: @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

(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

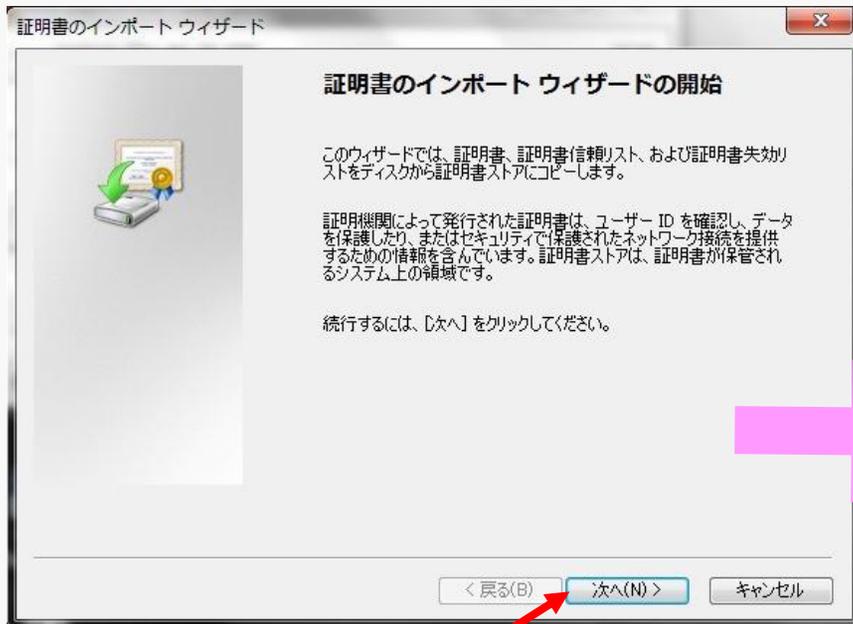


鍵マークのついた「～.p12」形式ファイルがダウンロードされたことをご確認ください。

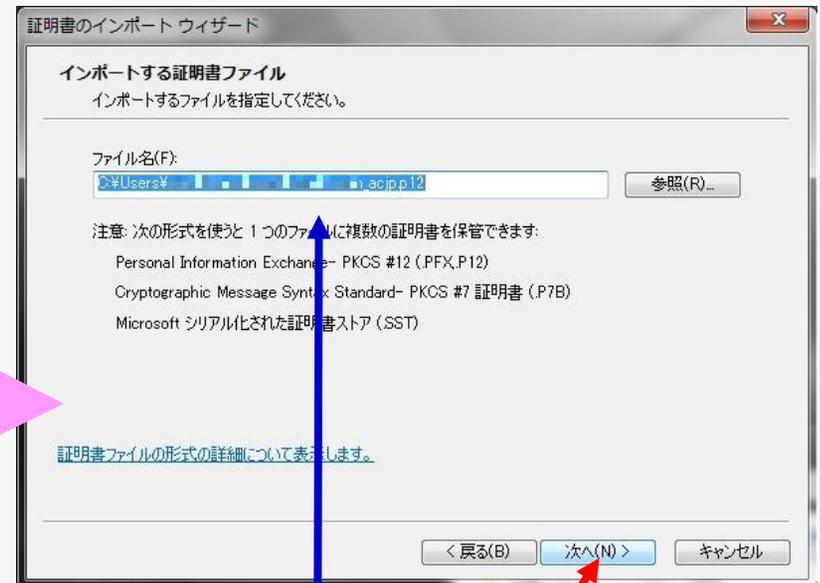
ダブルクリックで「証明書のインポートウィザード」が開始します。

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す。

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。

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。

すべての拡張プロパティを含める(A)

[プライベートキーの保護の詳細について表示します。](#)

< 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)...

[証明書ストアの詳細を表示します](#)

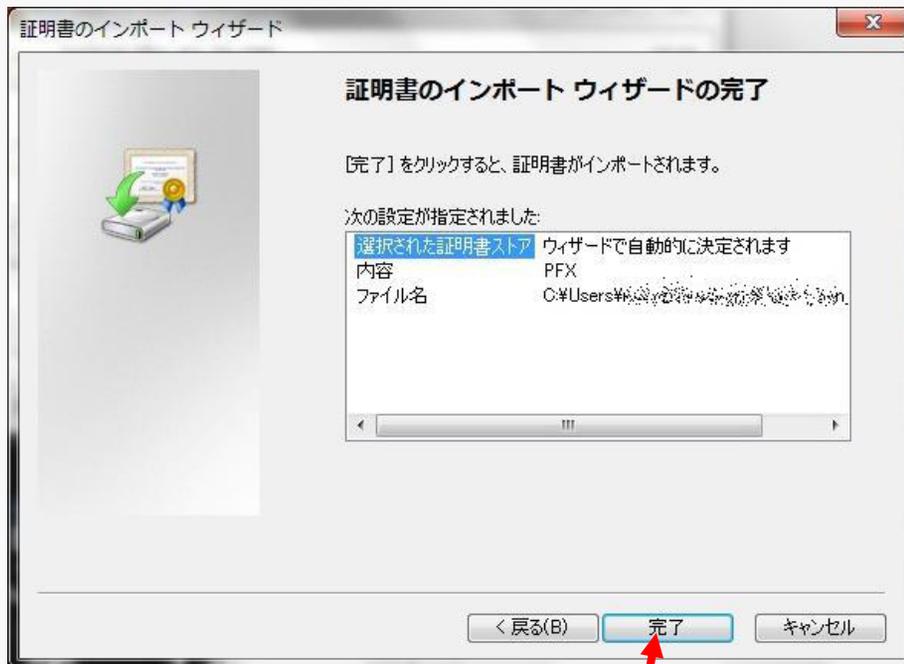
< 戻る(B) 次へ(N) > キャンセル

「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

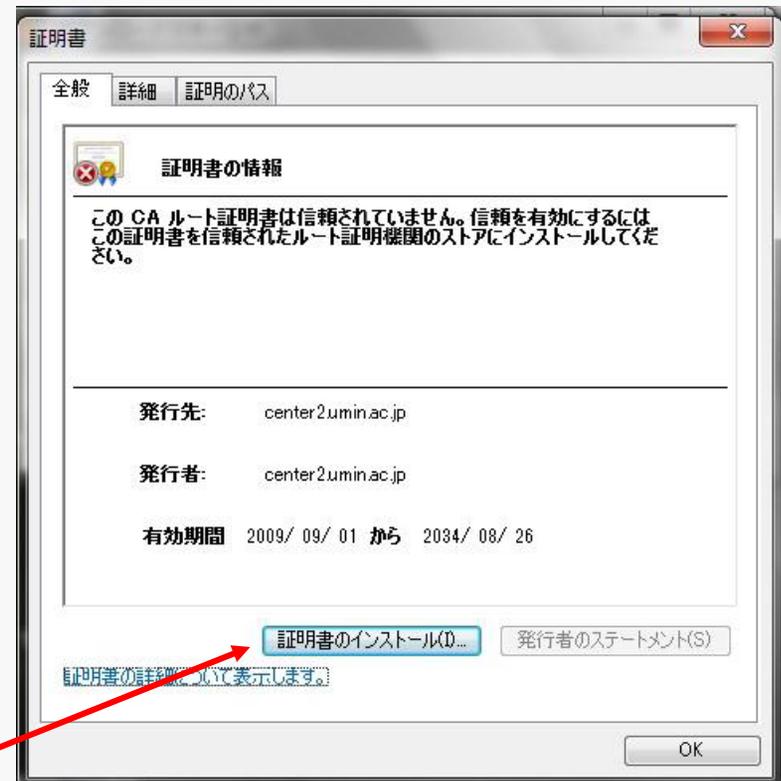
秘密鍵・公開鍵の発行(証明書インポート)

【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。

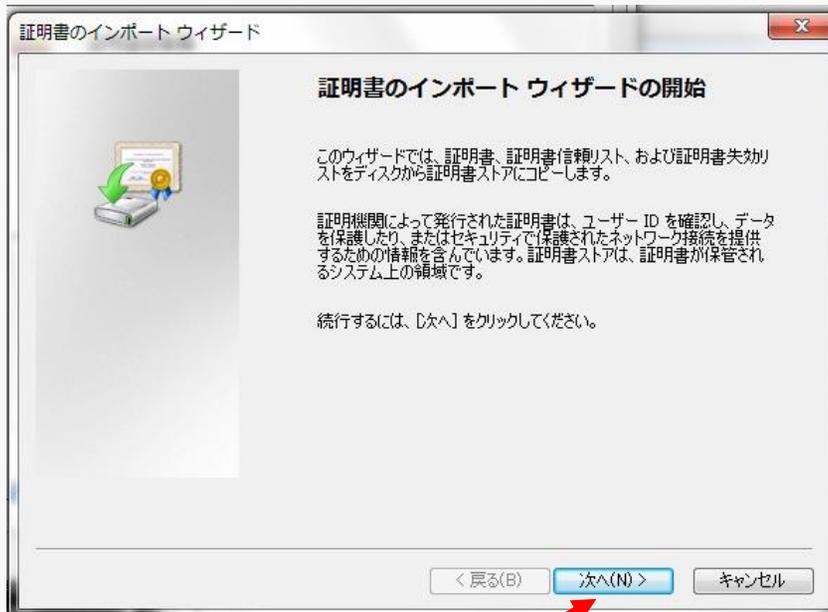
証明書のインストールを開始します。



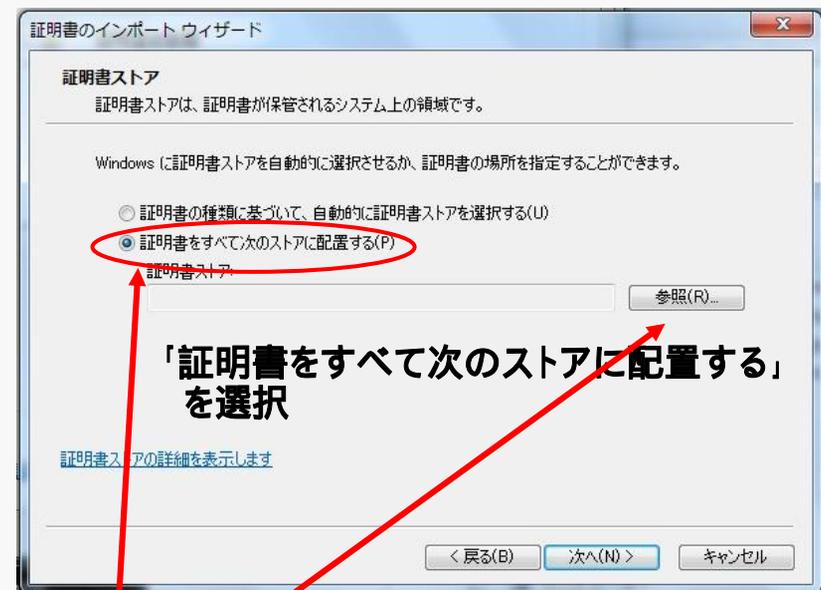
A . 秘密鍵・公開鍵の作成

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。

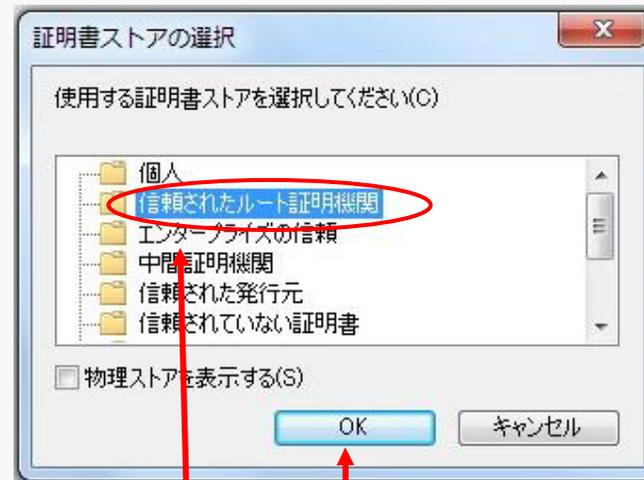
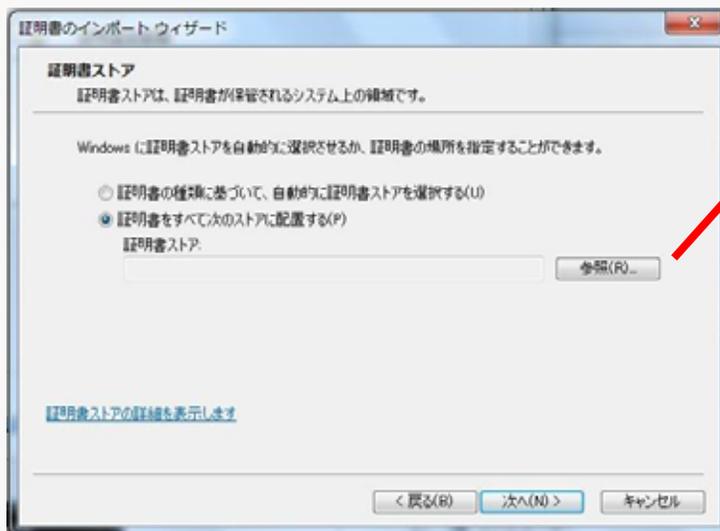


「証明書をすべて次のストアに配置する」を選択し、
「参照」をクリックします。

A . 秘密鍵・公開鍵の作成

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】



「参照」をクリックすると「証明書ストアの選択」が開きます。

「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

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】

The image shows a sequence of three windows from a Windows operating system. The first window on the left is titled '証明書のインポート ウィザード' (Certificate Import Wizard) and shows the '完了' (Completed) step. A red circle highlights the '完了' button, with a red arrow pointing to it from the text '「完了」をクリックしてください。'. The middle window is a 'セキュリティ警告' (Security Warning) dialog box. It contains a warning icon and text: '発行者が次であると主張する証明機関 (CA) から証明書をインストールしようとしています:' followed by 'center2.umin.ac.jp' which is circled in red. Below this, it says '証明書が実際に "center2.umin.ac.jp" からのものであるかどうかを検証できません。"center2.umin.ac.jp" に連絡して発行者を確認する必要があります。次の番号はこの過程で役立ちます:' and lists a SHA1 hash: '846BBE82 B5943D26 7310C4EC 0208820F B6F2F2B3'. A '警告:' section follows, stating that installing certificates from this CA will automatically trust them, which is a security risk. At the bottom, the question 'この証明書をインストールしますか?' is shown with 'はい(Y)' and 'いいえ(N)' buttons. A red circle highlights the 'はい(Y)' button, with a red arrow pointing to it from the text '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。'. The third window on the right is another '証明書のインポート ウィザード' window showing '正しくインポートされました。' (Imported successfully.) with an 'OK' button. A red arrow points from the 'OK' button to the text '「OK」のクリックでインポート完了です。'.

「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

(1) Windows Live メール

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) Windows Live メール 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。

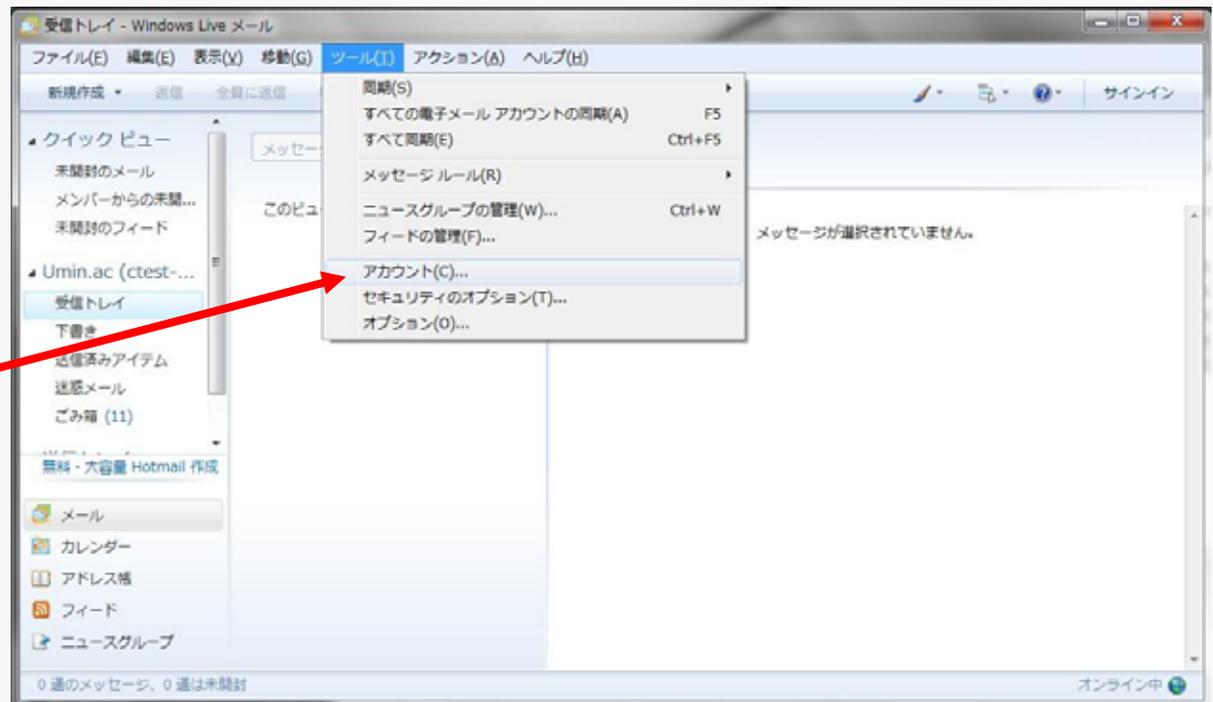
アカウントごとにデジタル証明書を有効にすることにより、メールへの署名や暗号化が可能になります。

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) Windows Live 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」
を選択して開きます。

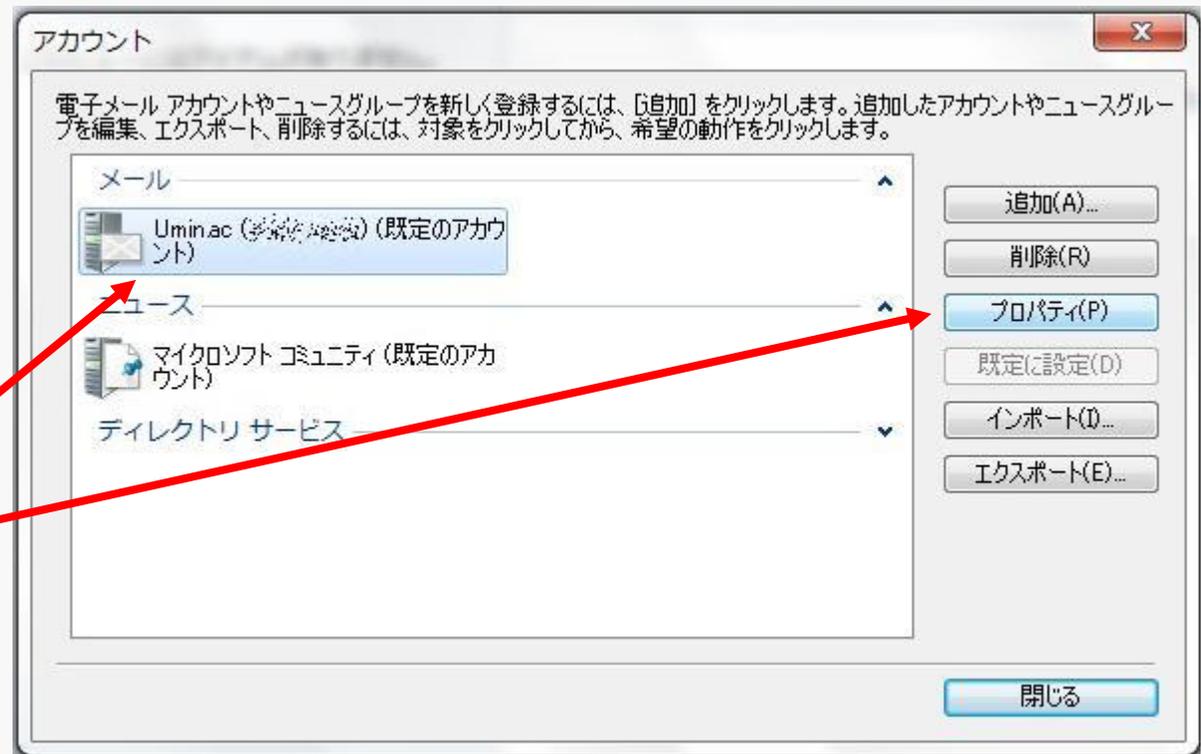


B . 秘密鍵・公開鍵の作成

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 - 3) Windows Live 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
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

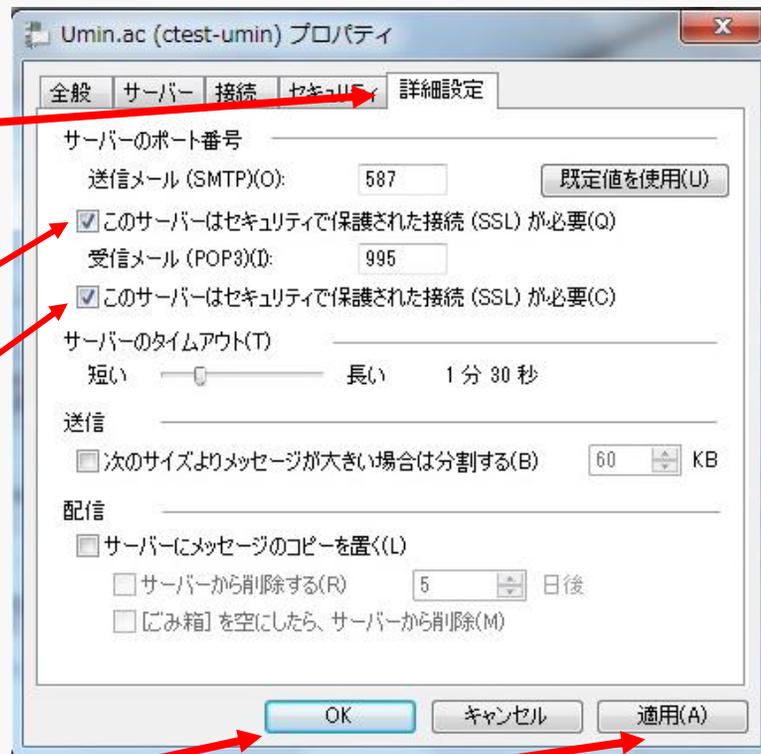
各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B1 - 4) Windows Live メール アカウントごとに
デジタル証明書を有効にする

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

「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」

「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」

にチェックが入っていることを確認してください。



最後に「適用」、「OK」の順に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 - 5) Windows Live メール 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」

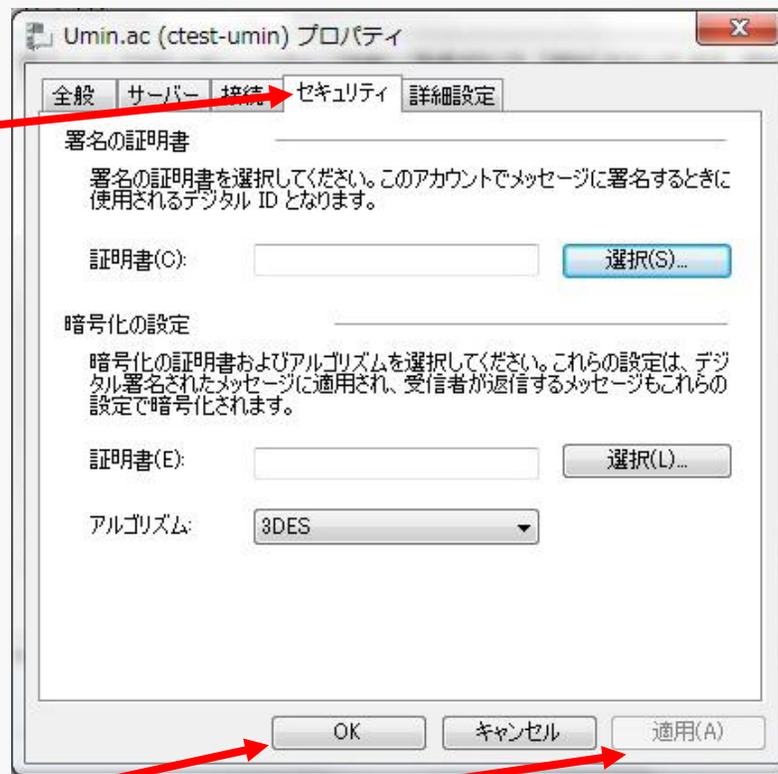
このアカウントでメッセージに署名するときに
デジタルIDとして使用されます。

「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)



最後に「適用」、「OK」の順にクリックしてください

B . 秘密鍵・公開鍵の作成

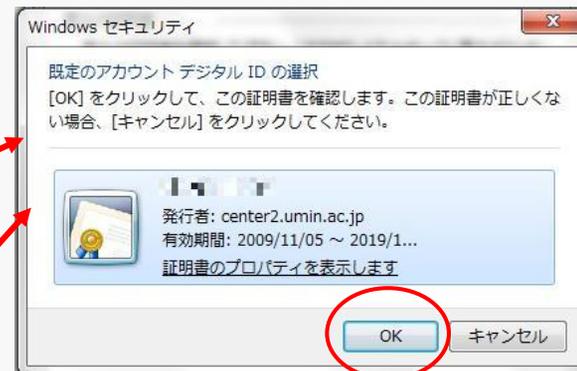
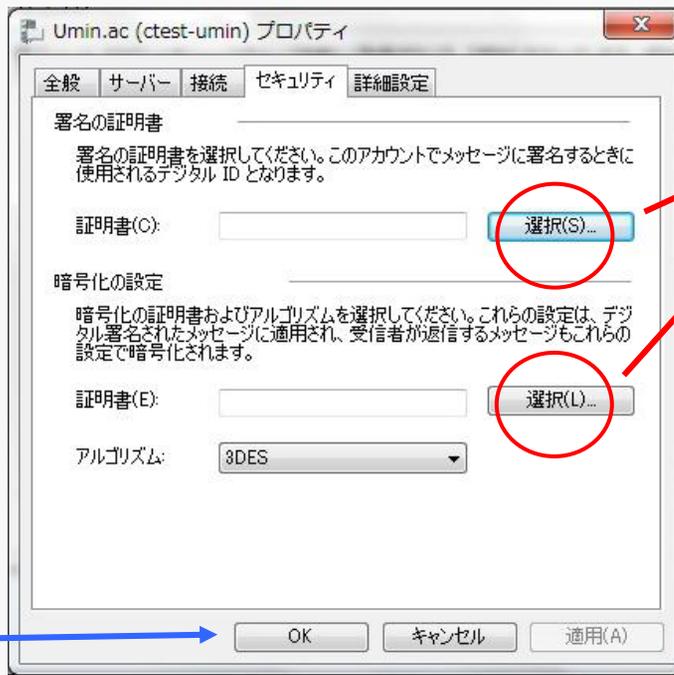
各メールソフトにおける、デジタル証明書、秘密鍵の設定
(B1 - 6) Windows Live メール アカウントごとに
デジタル証明書を有効にする

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。



center2.umin.ac.jp を選択し
「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](#)

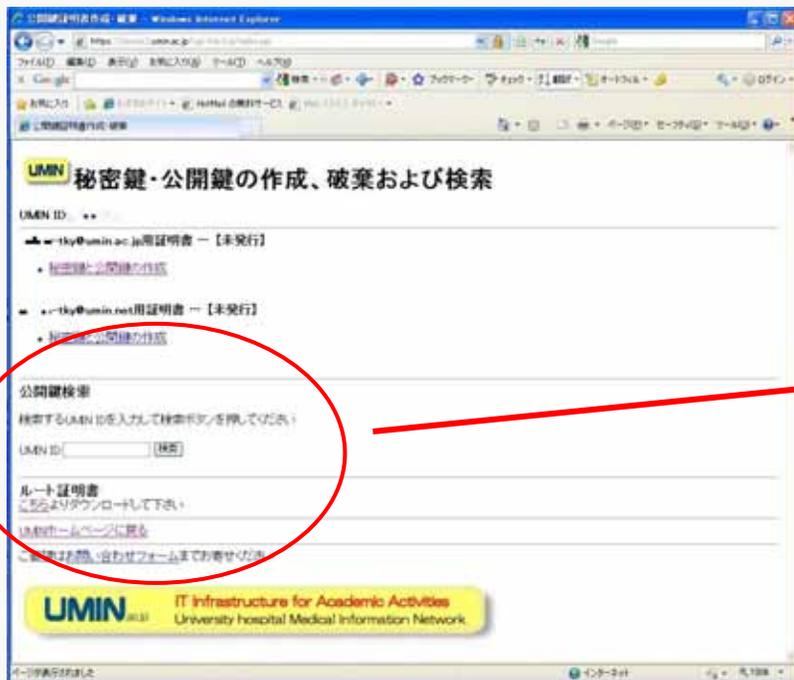
[UMINホームページに戻る](#)

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。

相手先の公開鍵証明書をダウンロードします。

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](#)



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。

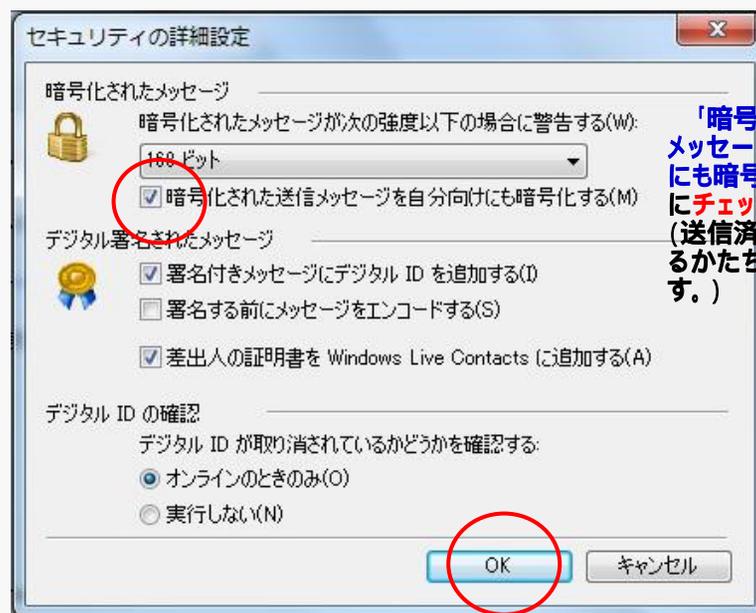
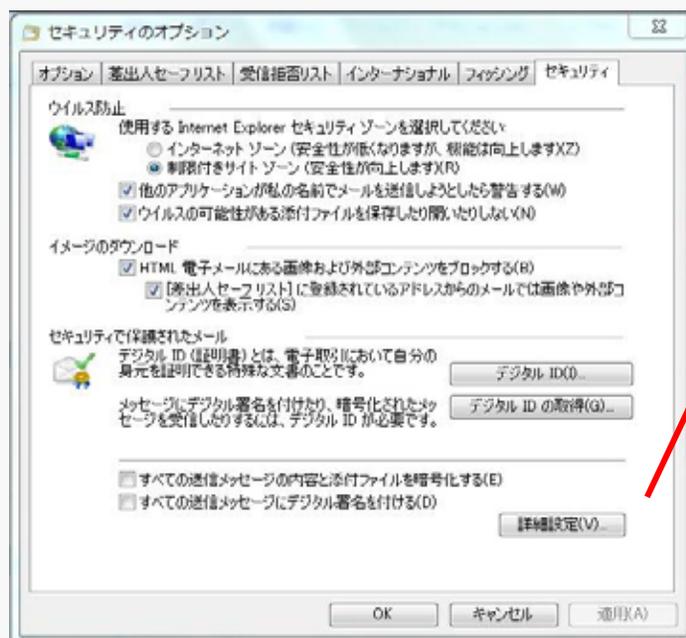
C. 秘密鍵・公開鍵の作成

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) Windows Live メール

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」にチェックを入れます。(送信済メールを読めるかたちにするためです。)

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) Windows Live メール



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。



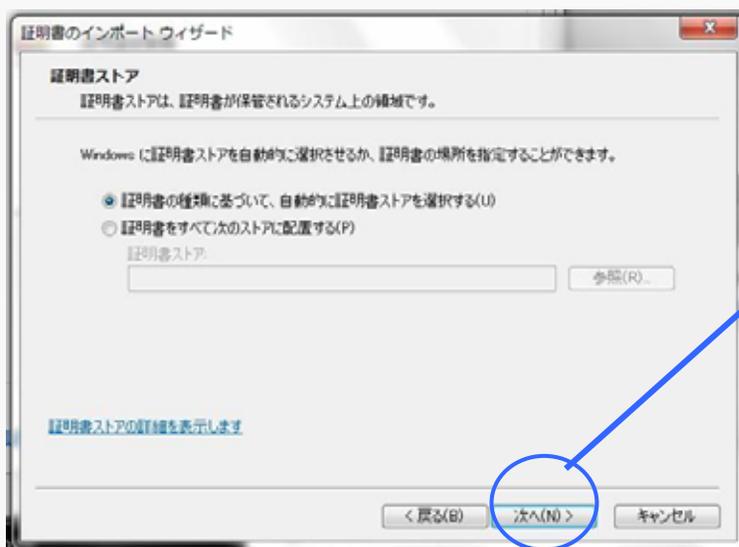
インポートウィザードが開始されます。

C . 秘密鍵・公開鍵の作成

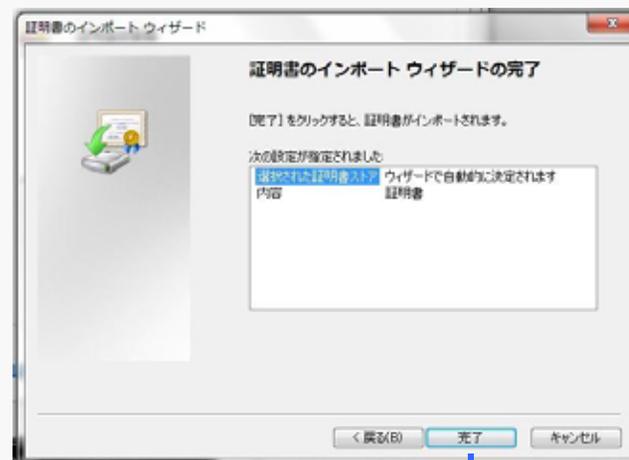
秘密鍵・公開鍵の発行：証明書の検索

（ 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) Windows Live メール

「証明書～自動的に証明書ストアを選択する」を選択。

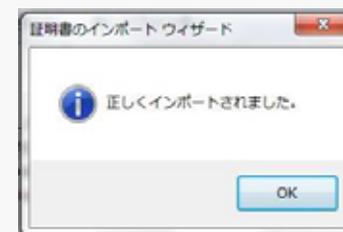


「次へ」をクリックします。



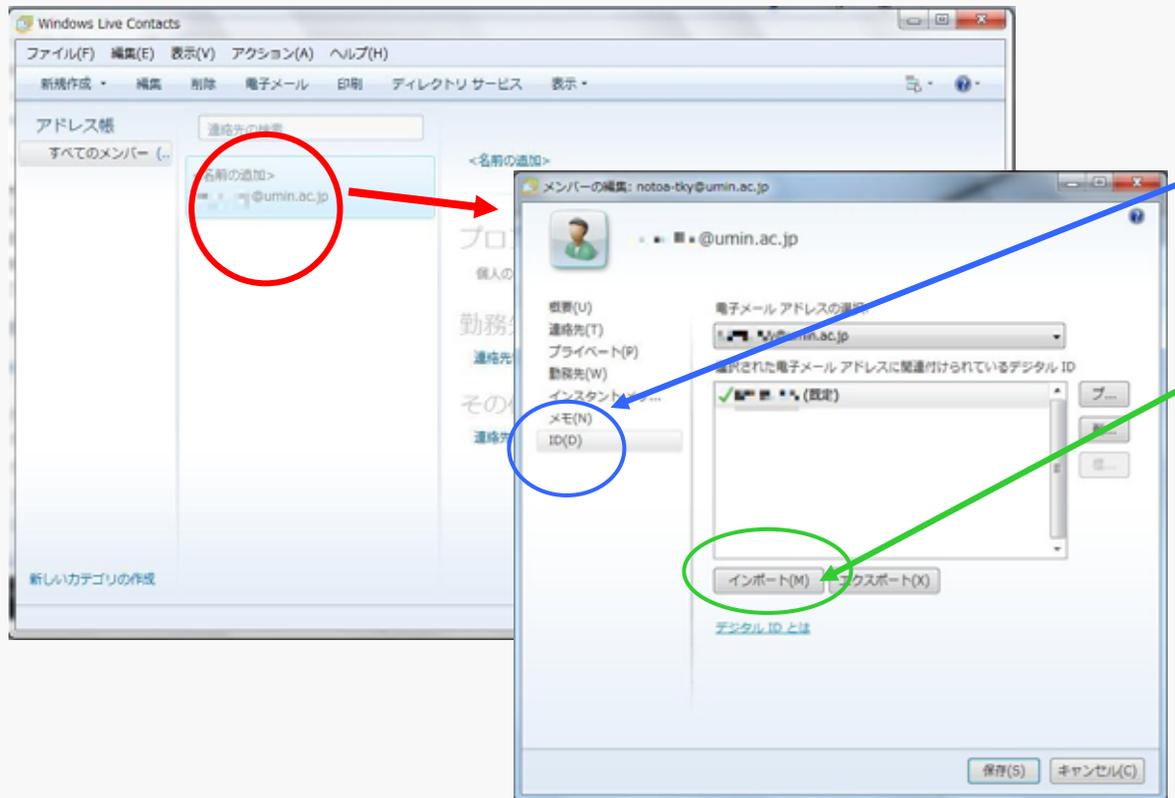
「完了」をクリック

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) Windows Live メール 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。

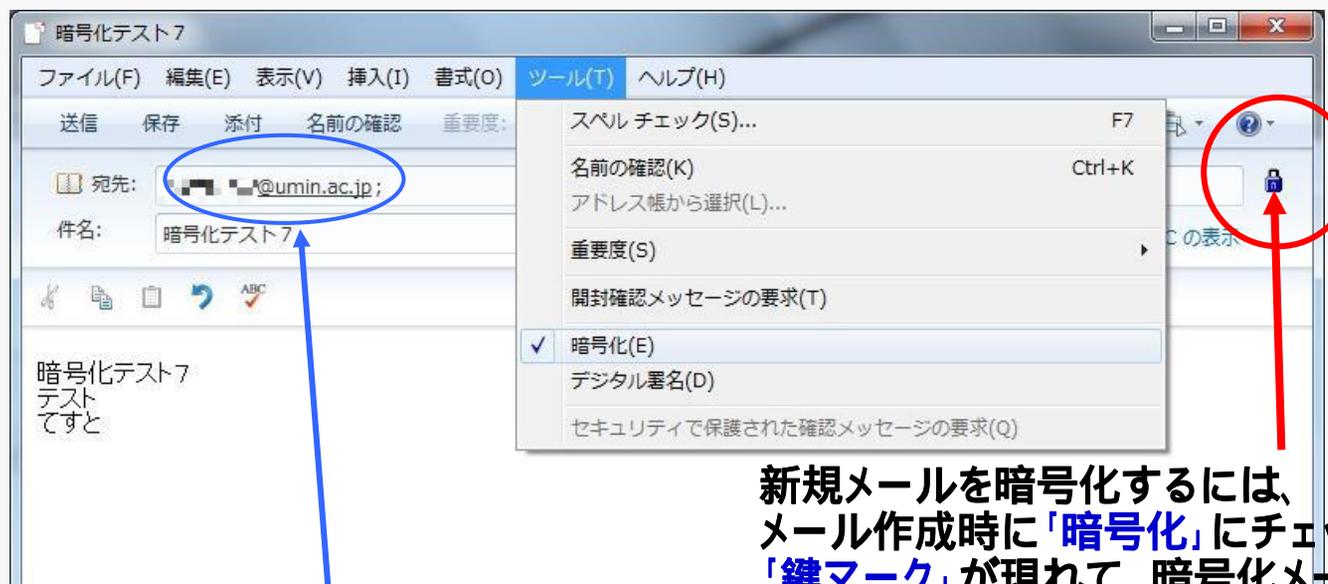
該当のアドレスをダブルクリック
して「メンバーの編集」を開き、
「ID」をクリックします。

「インポート」をクリックし、
「インポートするデジタルIDファイルの選択」
の中から、
該当の公開鍵 (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

(C1 - 5) Windows Live メール 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。



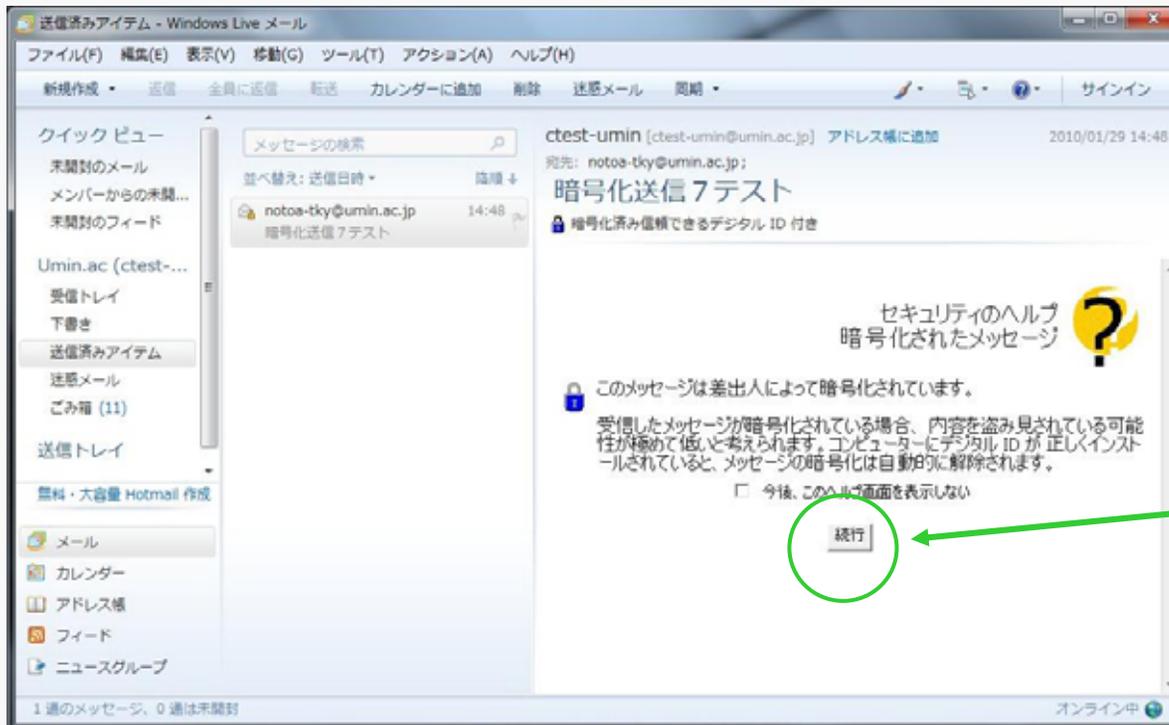
鍵マーク

新規メールを暗号化するには、
メール作成時に「暗号化」にチェックを入れておきます。
「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

(C1 - 6) Windows Live メール 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