メール暗号化：秘密鍵・公開鍵の作成

作業手順

Becky! Internet mail

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）ベッキー！２（Becky! Internet mail）

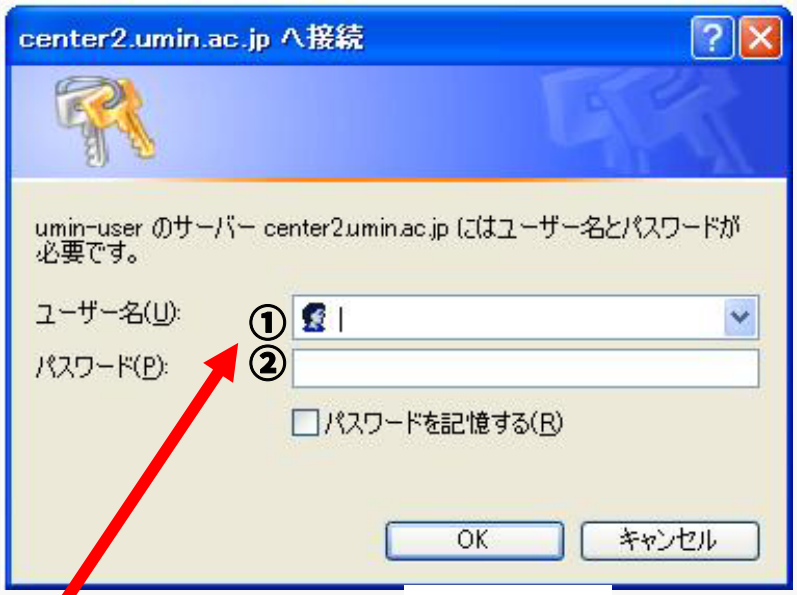
C．暗号化してメールを「送信」できるように設定する。
（他の人の公開鍵を取得してメールソフトへ設定する。）
公開鍵の取得①～④
⑤～⑧（1）ベッキー！ ２（Becky! Internet mail）

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。



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

①

②

③

④

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

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

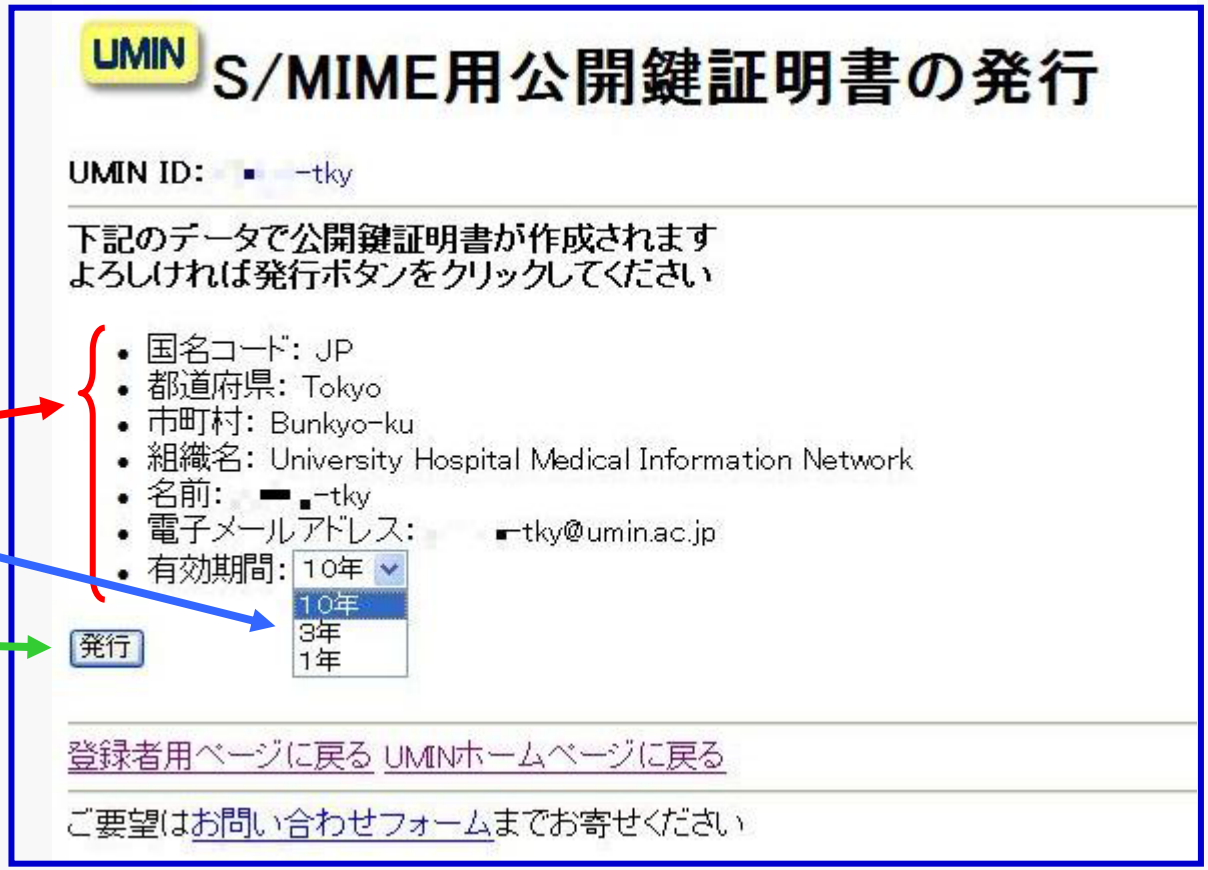
A．秘密鍵･公開鍵の作成

④秘密鍵･公開鍵の発行

内容確認

①有効期間を選択

②「発行」をクリック



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。

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。

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。

A．秘密鍵･公開鍵の作成

⑧秘密鍵･公開鍵の発行

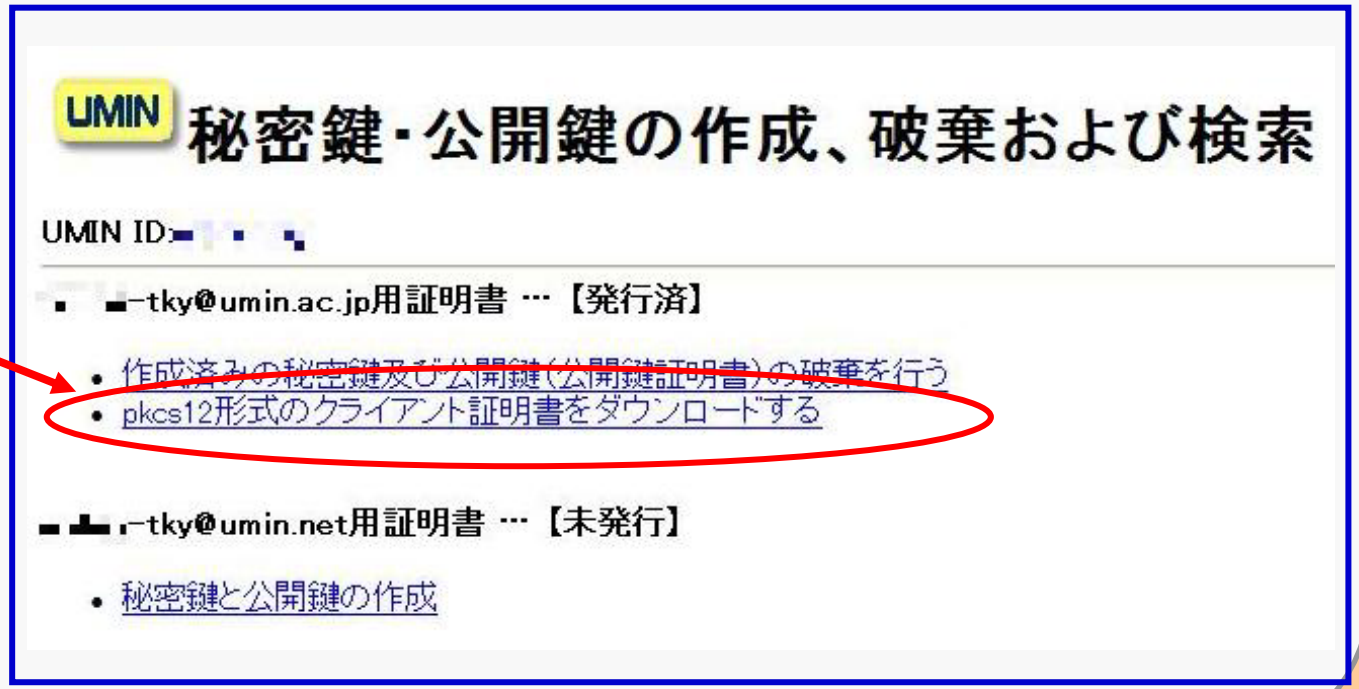
《クライアント証明書の発行》

「･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。



A．秘密鍵･公開鍵の作成

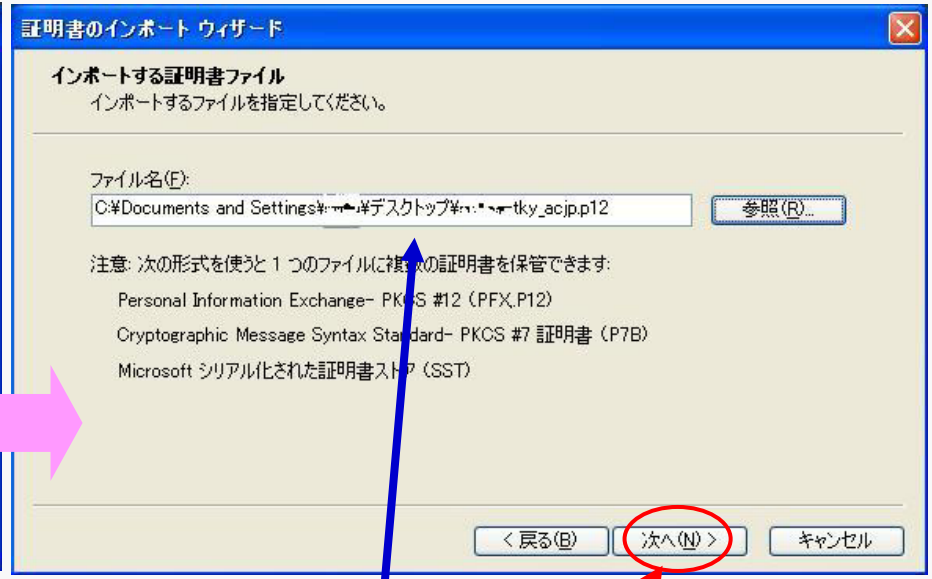
⑨秘密鍵･公開鍵の発行

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　ウイザード」が開始されます。
「次へ」をクリック

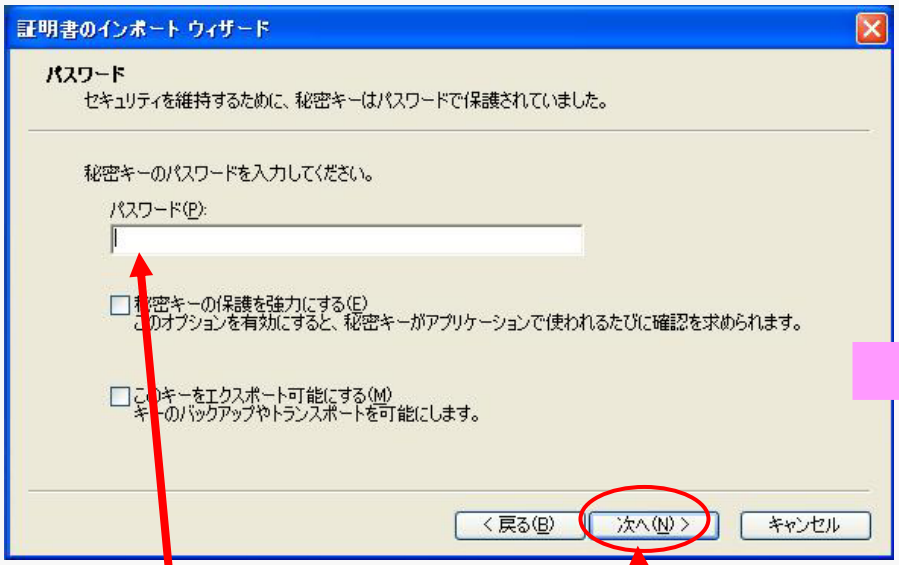
インポートする証明書ファイルのファイル名が表示されます。　「次へ」をクリックしてください。

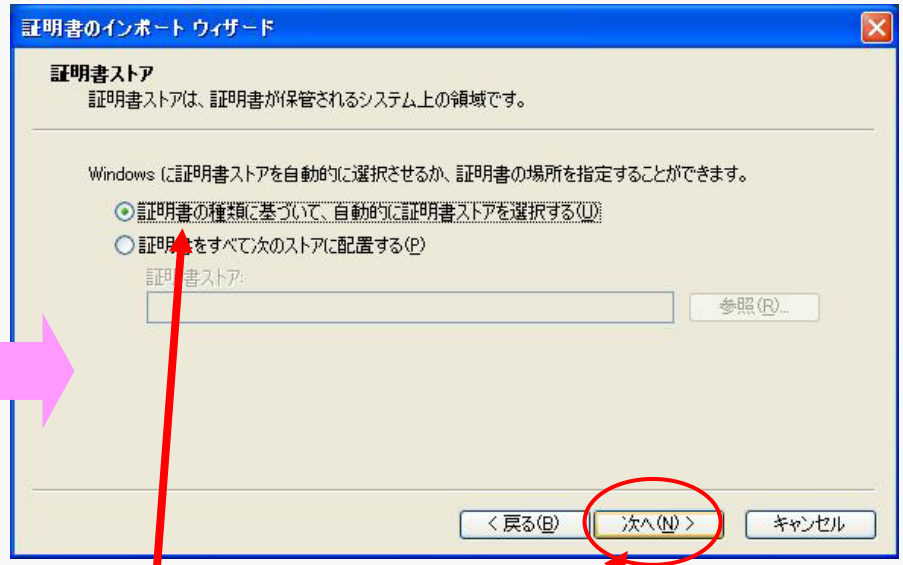
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

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

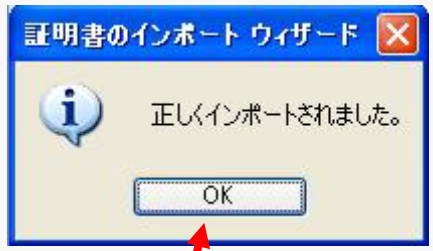
「証明書の種類に基づいて、自動的に証明書ストアに選択する」を選んで「次へ」をクリック

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

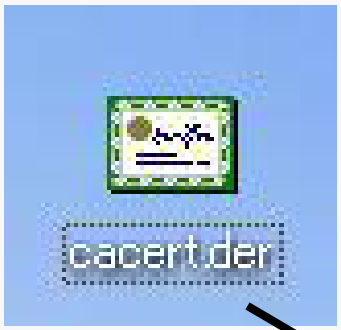
ルート証明書 →

をダウンロードします。

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】



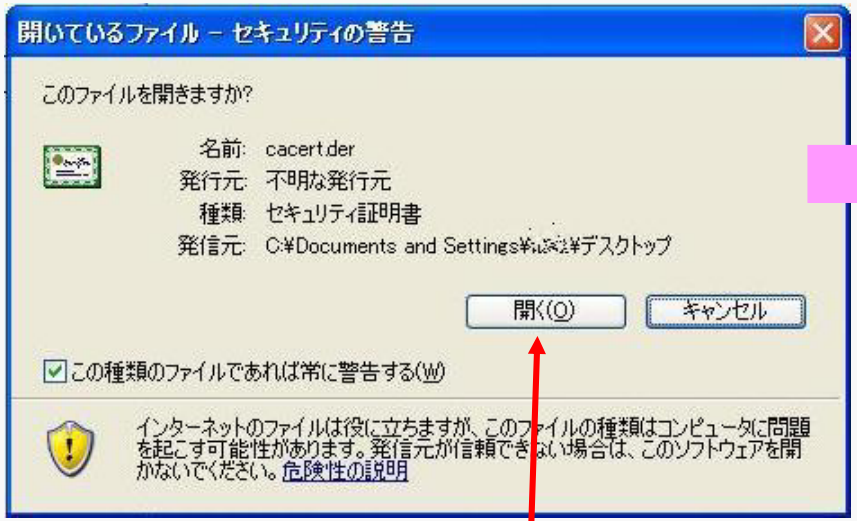
証明書アイコンの「cacert.der」形式ファイルが
ダウンロードされたことをご確認ください。

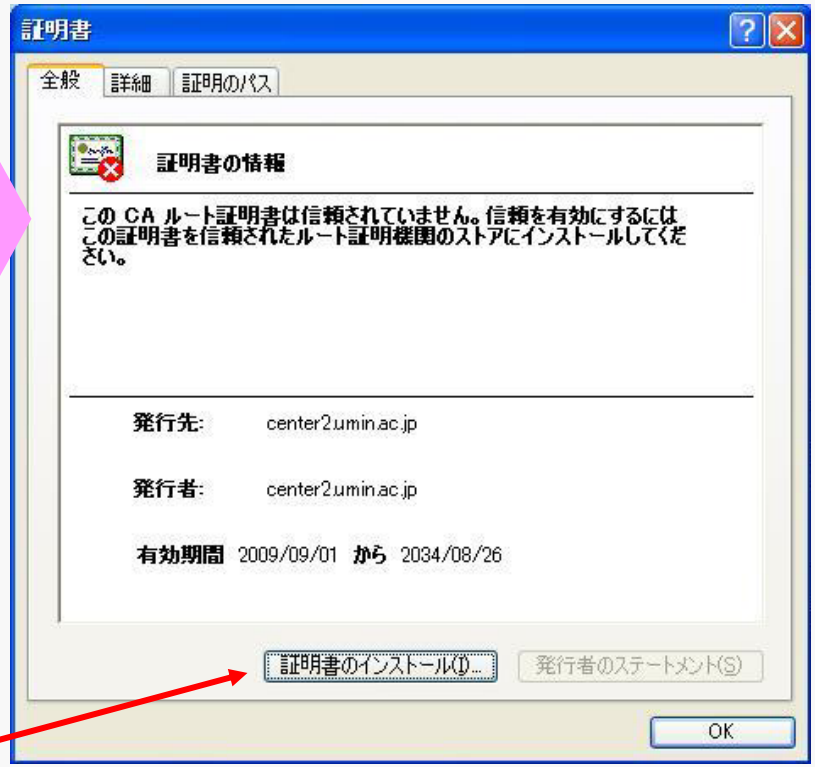
ダブルクリックで　「証明書のインポートウィザード」　が開始します。

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】





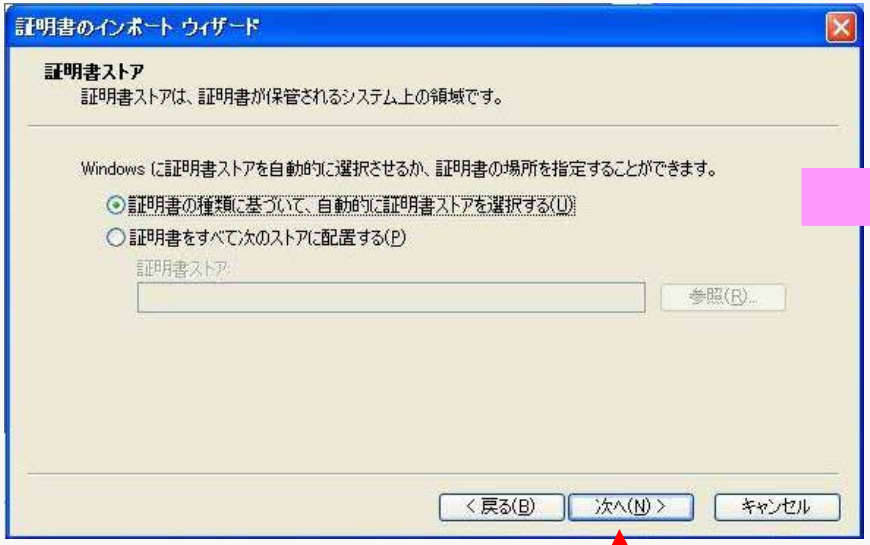
①ルート証明書のファイル「cacert.der」を開きます。

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

⑯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】



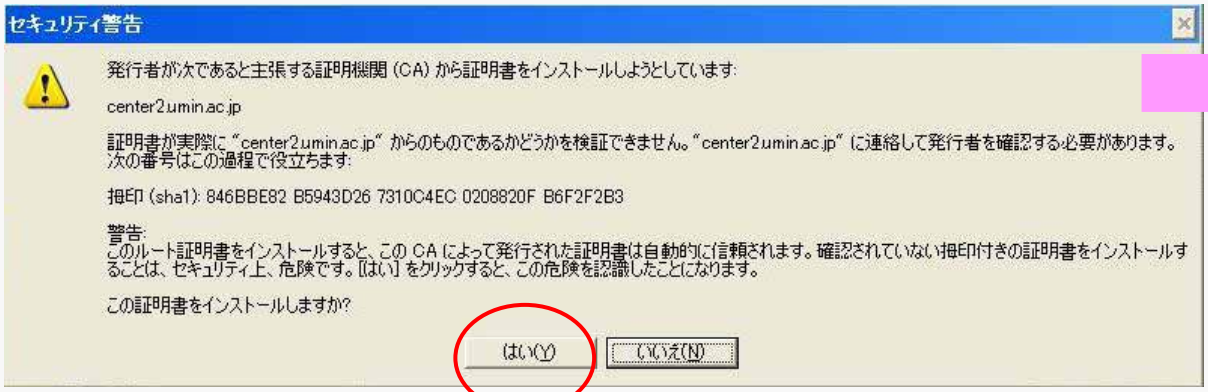
①証明書のインポートのウィザードを進行します。
「次へ」をクリックしてください。

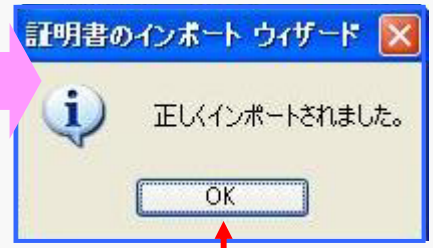
②「完了」をクリックしてください。

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】





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

（B１－１）Becky! Internet mail
ベッキー！ インターネットメール　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。

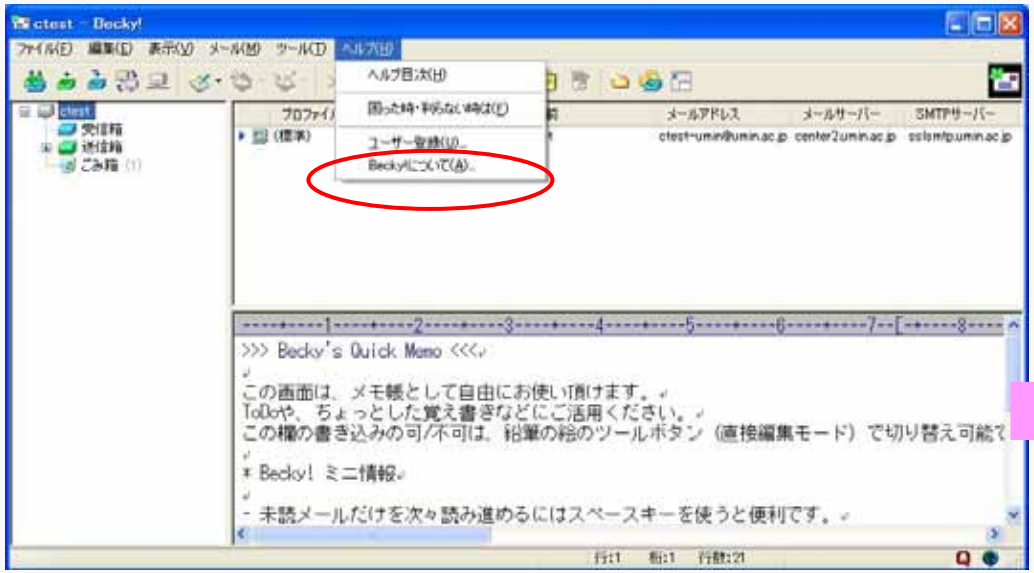
アカウントごとにデジタル証明書を有効にすることにより、メールへの署名や暗号化が可能になります。

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

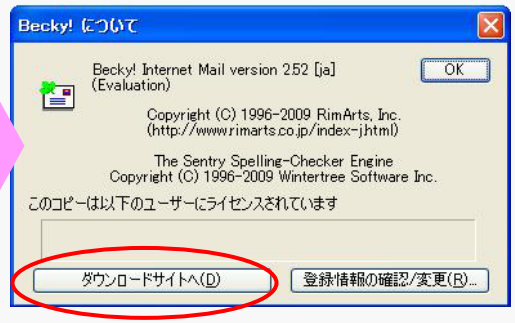
（B１－２）Becky! Internet mail　プラグインの導入

Beckey! Internet mailでは、UMINで使用している暗号（S/MIME）の形式にするため、プラグインを設定する必要があります。



メイン画面の

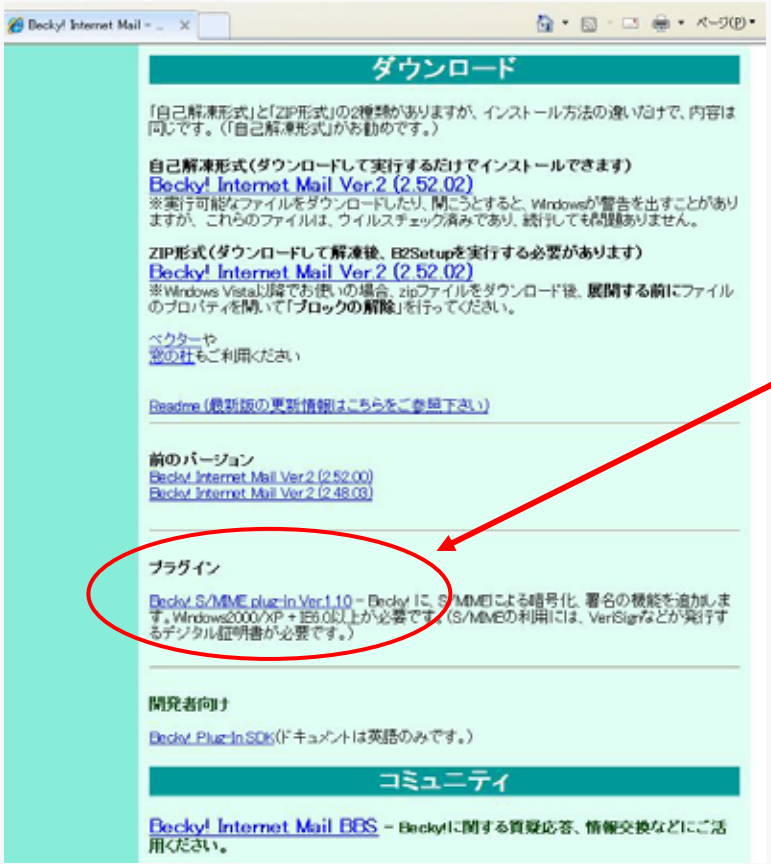
「ヘルプ（H）」から
「Beckyについて」
を選択し、インターネットより
プラグインのデータをダウンロードします。



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

（B１－３）Becky! Internet mail　プラグインの導入



ダウンロードのページが開きます。
http://www.rimarts.co.jp/becky-j.htm#download

Becky! S/MIME plug-in Ver.1.10
をダウンロードして、解凍します。
（「実行」で自動解凍）

【同サイトおよびプラグインのバージョンは2009年12月現在のものです】

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

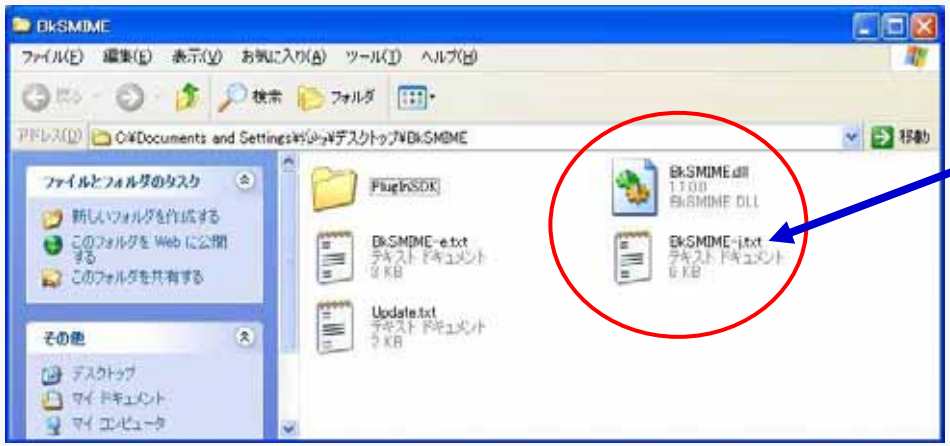
（B１－４）Becky! Internet mail　プラグインの導入

解凍後、以下のフォルダに、BkSMIME.dllと、BkSMIME-j.txt　をコピーして下さい。

[Becky!のプログラムがインストールされているフォルダ]¥PlugIns¥
(例：C:¥Program Files¥RimArts¥B2¥PlugIns¥)

インストールすると、同じPCでBecky!を使用するユーザー全てが使用することができます。

ダウンロードしたフォルダ「BkSMINE」



※本プラグインについては、BkSMIME-j.txt
に詳細が記載されていますので
ご確認ください。

B．秘密鍵･公開鍵の作成

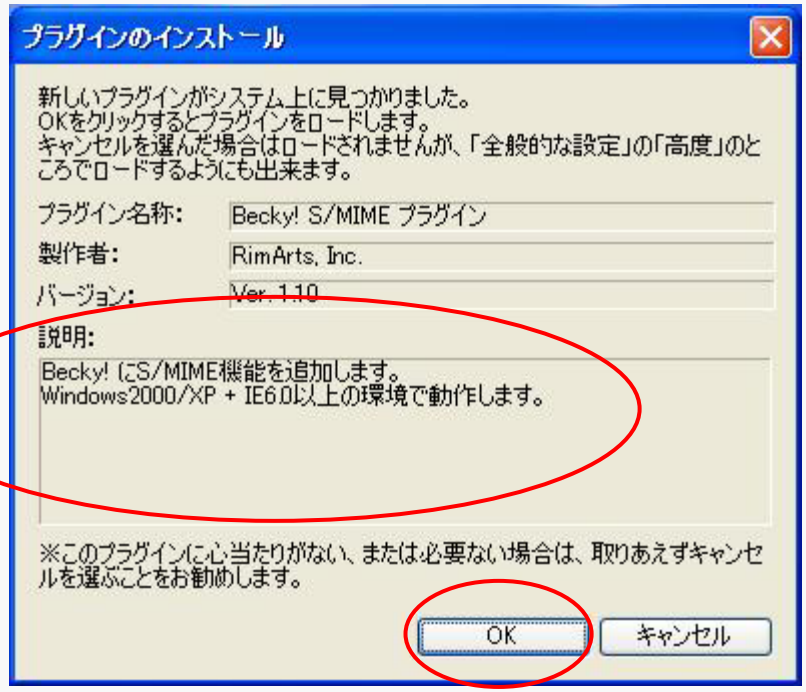
各メールソフトにおける、デジタル証明書、秘密鍵の設定

（B１－５）Becky! Internet mail　プラグインの導入

Becky! Internet mail　を再起動します。

再起動後、プラグインの確認画面が
表示されます。

確認後、「OK」で進行します。



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

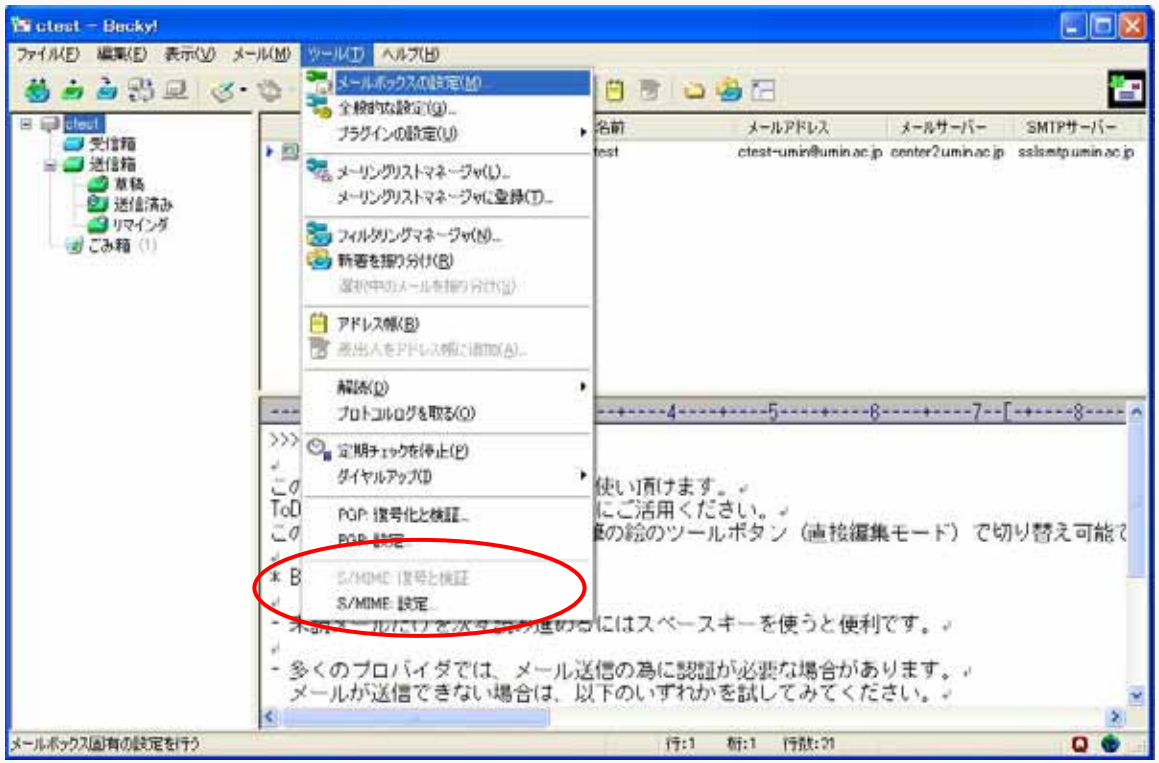
（B１－６）Becky! Internet mail　プラグインの導入

プラグインが導入されたことを確認します。

「ツール」内に

「S/MINE～」の部分が追加されました。

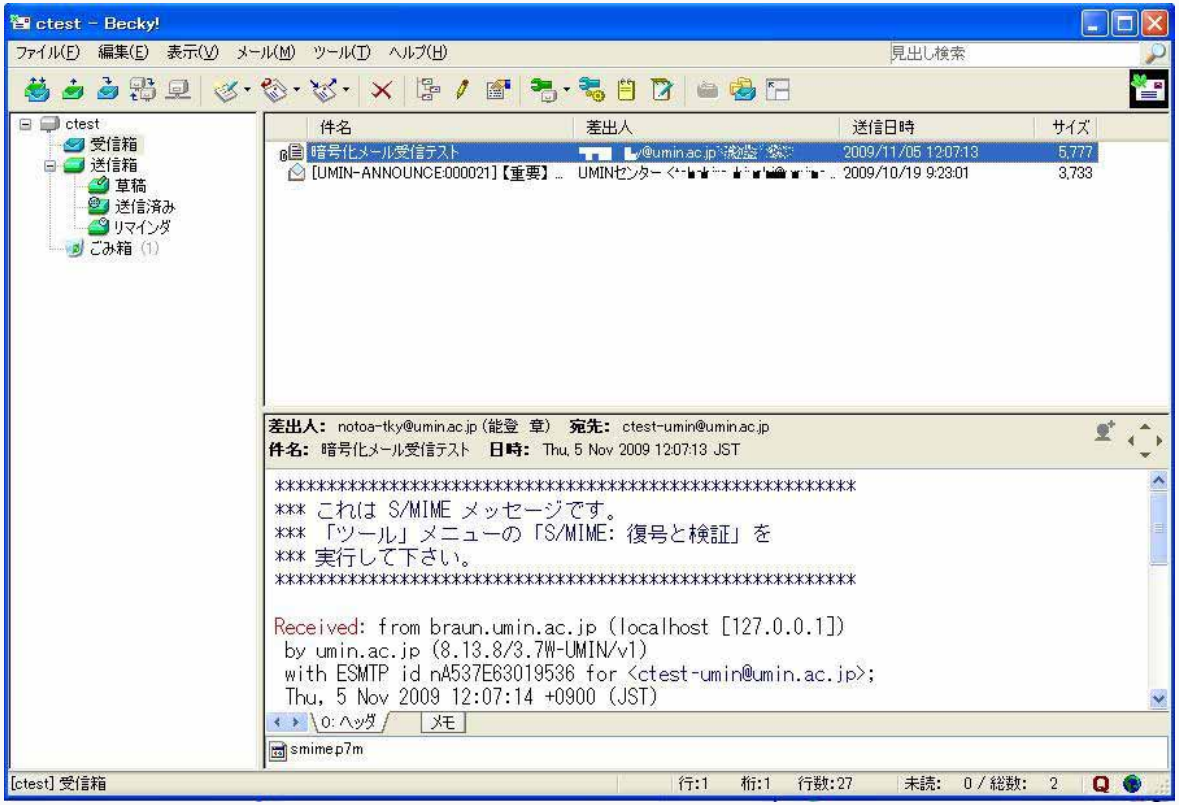
以上で、受信環境が設定されました。



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

（B１－７）Becky! Internet mail　暗号化されたメールの受信

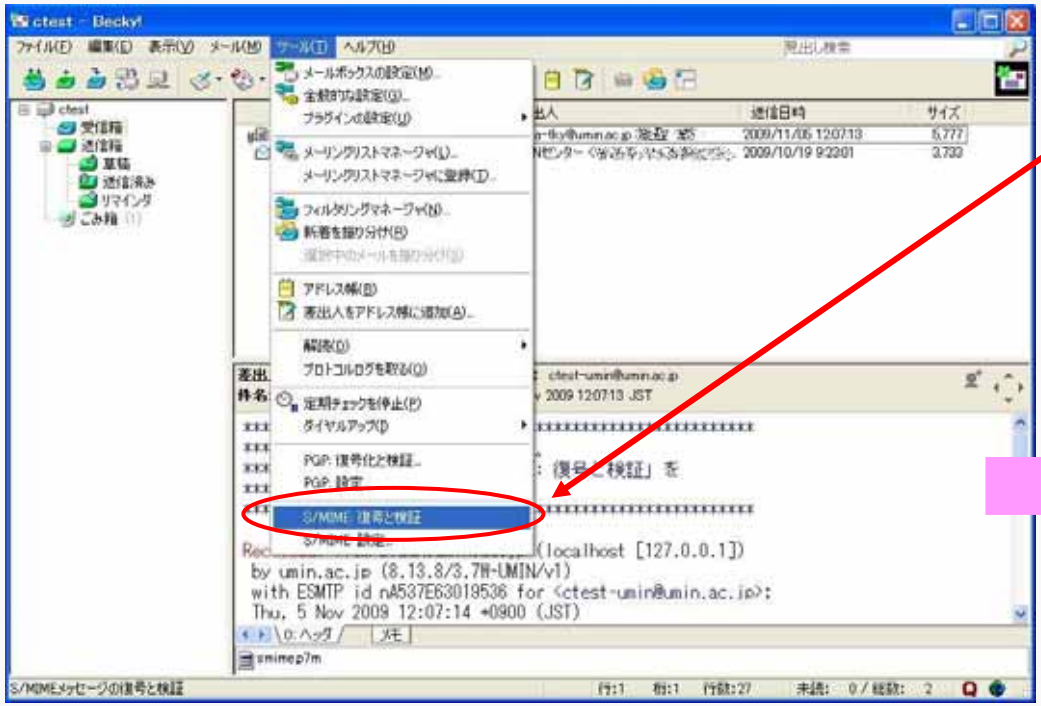


S/MIMEにて暗号化された
UMINのメールは受信すると
このように表示されます。

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

（B１－８）Becky! Internet mail　暗号化されたメールの受信



① ツール
→ S/MIME 復号と検証

をクリックします。

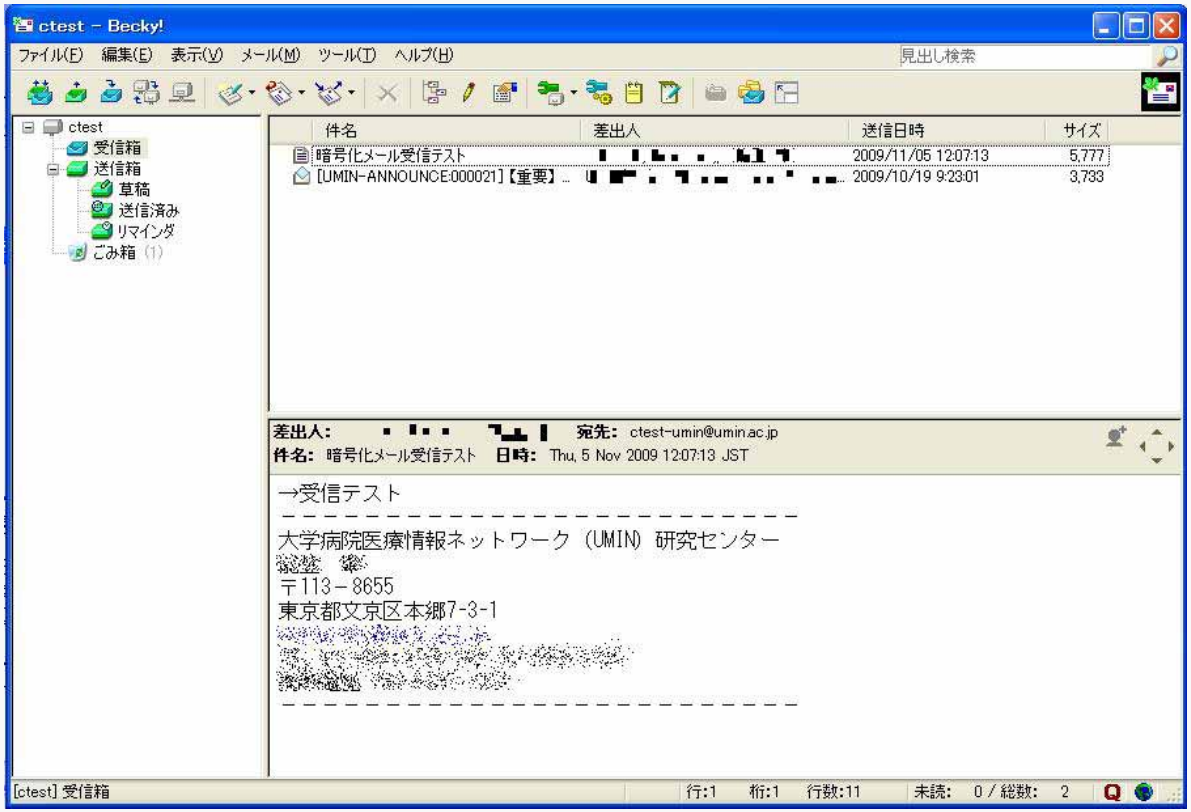
②自動復号されます。

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

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）Becky! Internet mail　暗号化されたメールの受信



メールが
復号化されました。

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

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

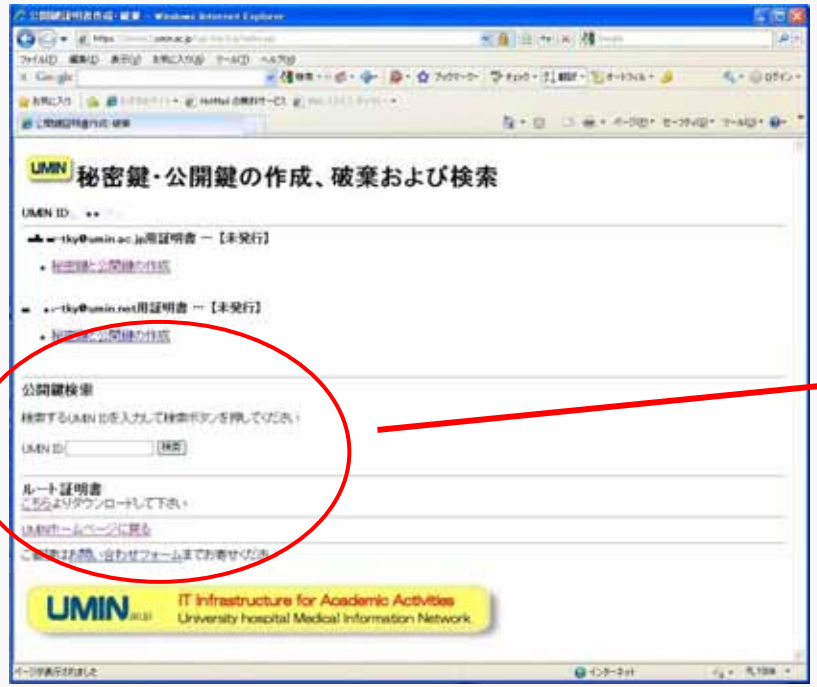
送信相手のUMIN IDを検索し、公開鍵の設定がされていれば、公開鍵証明書をダウンロードし、メールソフトに設定することで、暗号化して送信することができます。
（送信相手が発行した公開鍵で暗号化したメールの送信ができます）

《 登録者用ページ　トップページ 》

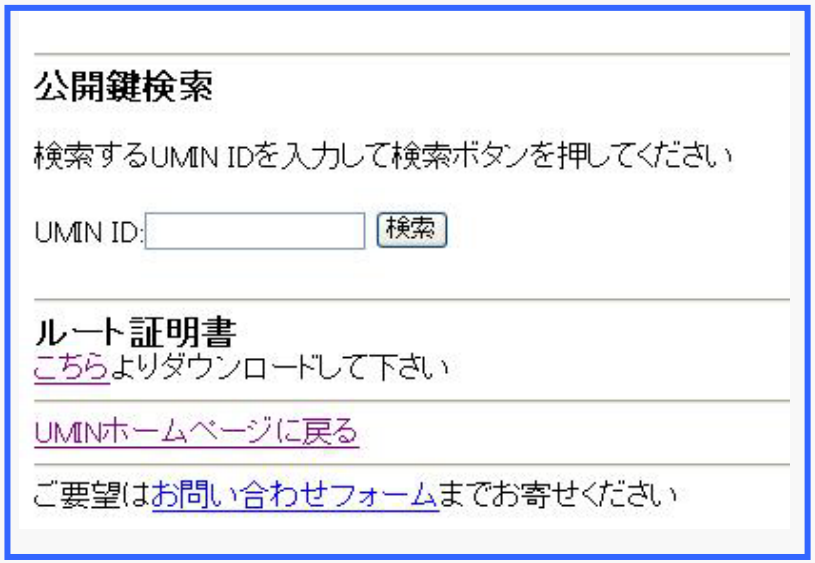
C．秘密鍵･公開鍵の作成

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）



UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

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。

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

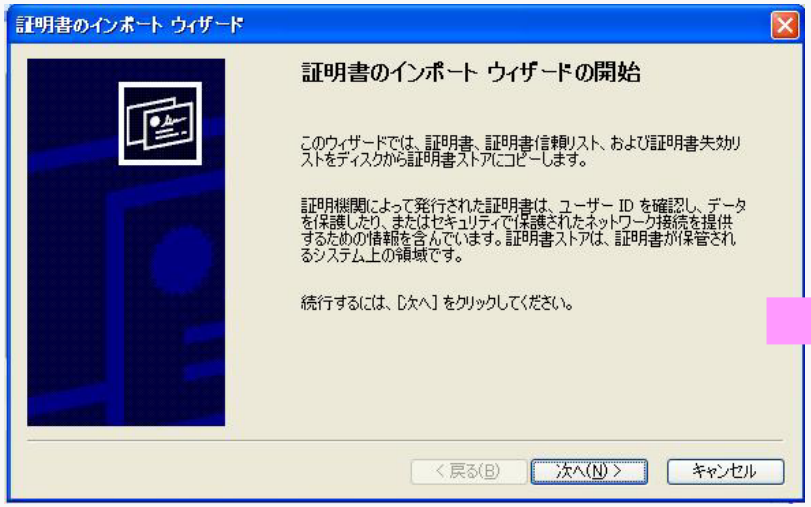
⑦秘密鍵･公開鍵の発行：証明書の検索

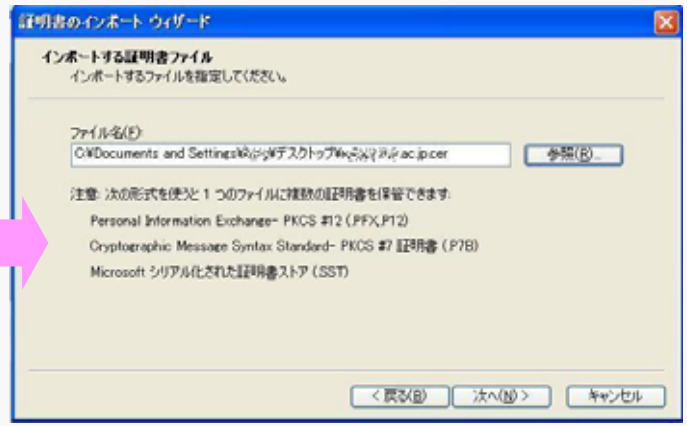
《 特定の送信相手の公開鍵を設定し、暗号化してメールを送信する 》

(C1－1) Becky! Internet mail　相手先の公開鍵の設定

事前にダウンロードしたXXXX-XXX.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。





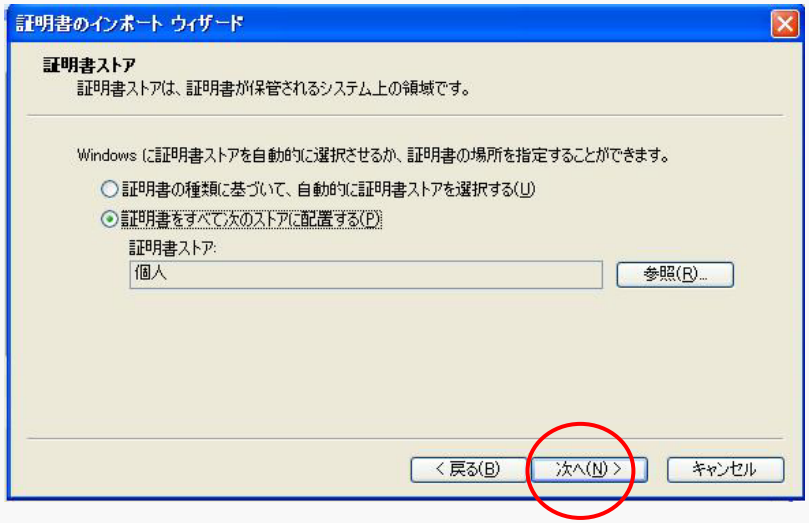
C．秘密鍵･公開鍵の作成

⑧秘密鍵･公開鍵の発行：証明書の検索

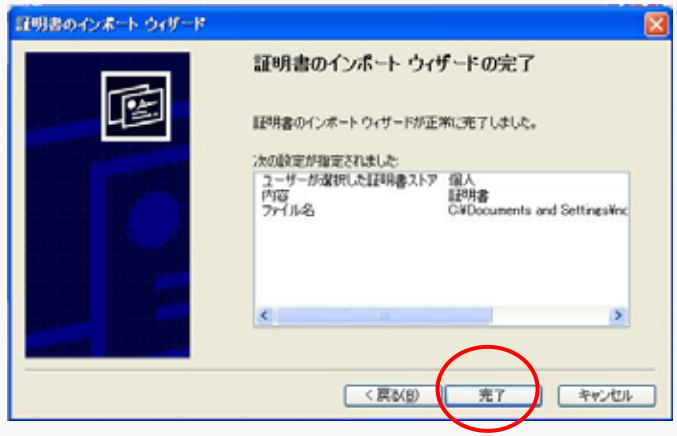
《 特定の送信相手の公開鍵を設定し、暗号化してメールを送信する 》

(C１－２) Becky! Internet mail

①「証明書をすべてストアに配置する」を選択。
②証明書ストアは「個人」。



③「次へ」をクリックします。



「完了」をクリック

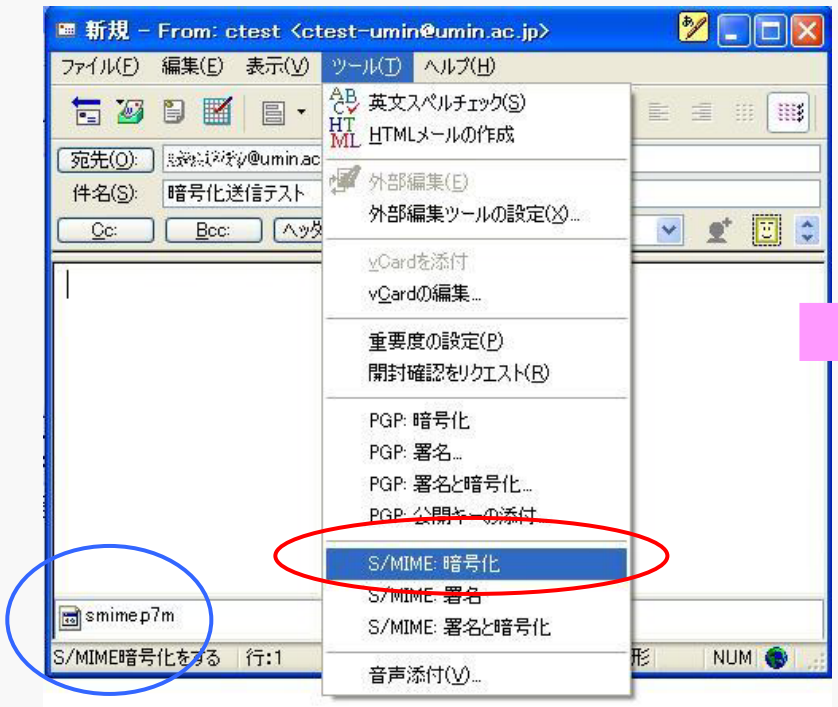
メッセージ
「正しくインポートされました」

C．秘密鍵･公開鍵の作成

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 》

(C1－3) Becky! Internet mail 送信



①Becky! Internet mail を起動し、
暗号化送信するメールを作成します。
作成後、

ツール → S/MIME暗号化

を選択し、クリックします。

②メール文が暗号化され、
添付文書化されました。通常のメール同様
送信作業を行ってください。

(※一度暗号化された文章は変更できません。
変更時は再作成が必要となります。)

メール暗号化：秘密鍵・公開鍵の作成

作業完了

Becky! Internet mail