メール暗号化：秘密鍵・公開鍵の作成

作業手順

Thunderbird

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

© UMIN Center

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。

© UMIN Center

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）モジラ　サンダーバード（Mozilla Thunderbird）

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）モジラ　サンダーバード（Mozilla Thunderbird）

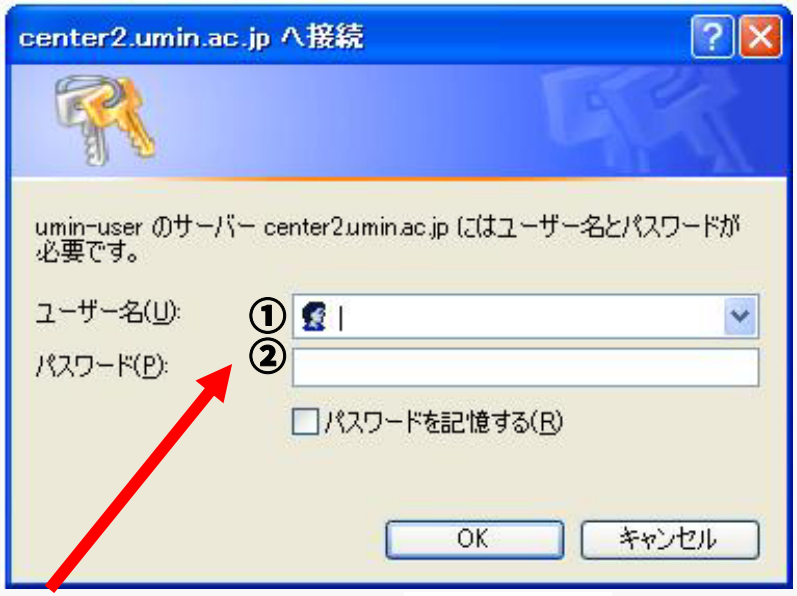
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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

© UMIN Center

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

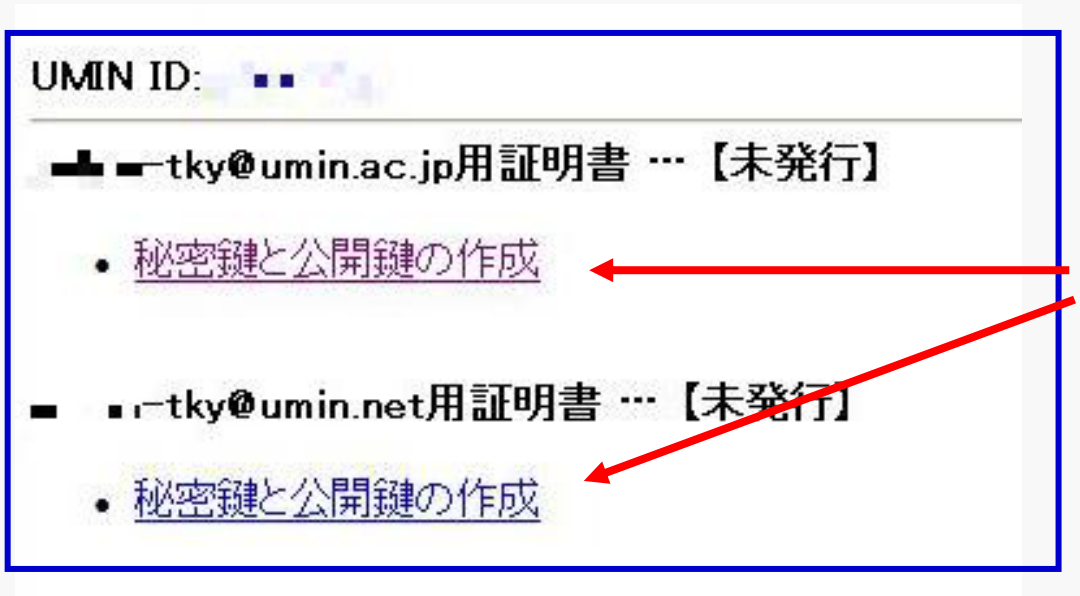
④ルート証明書

© UMIN Center

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

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

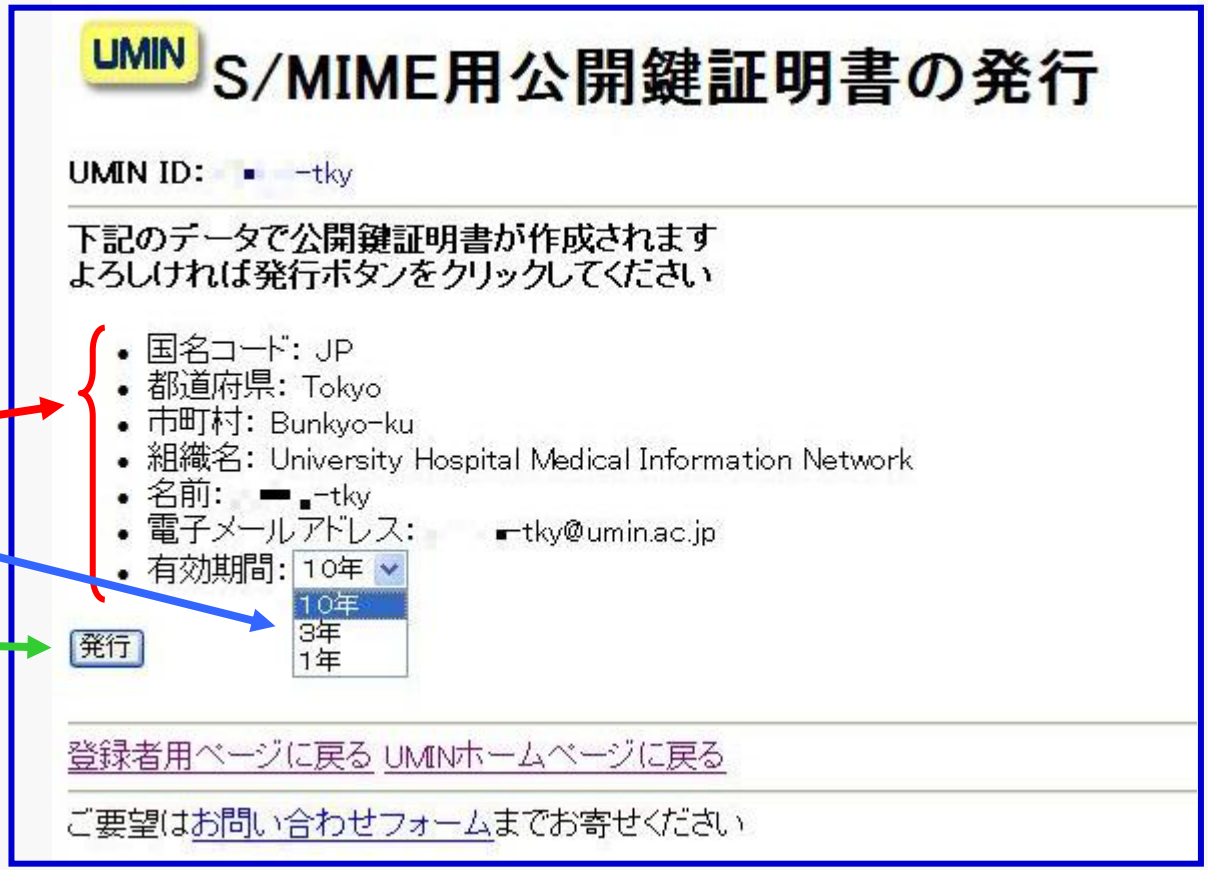
A. 秘密鍵・公開鍵の作成

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



© UMIN Center

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。

© UMIN Center

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 Center

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。

© UMIN Center

A．秘密鍵･公開鍵の作成

⑧秘密鍵･公開鍵の発行

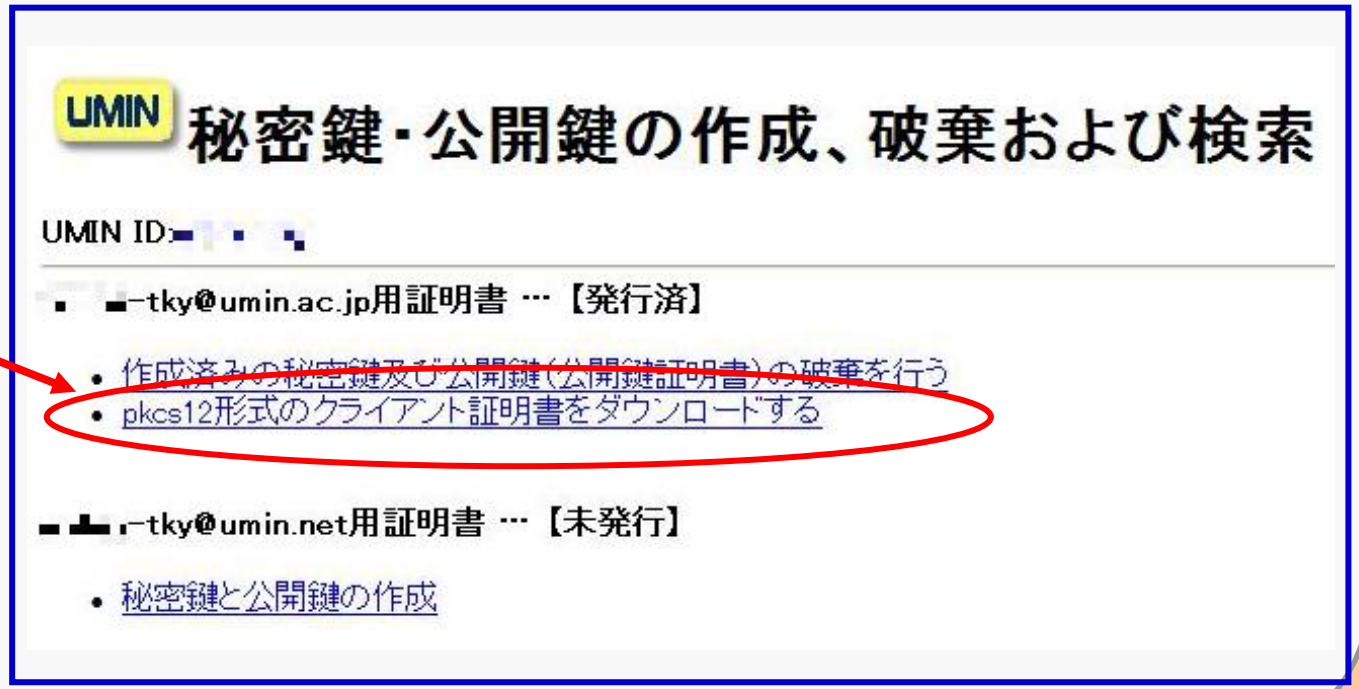
《クライアント証明書の発行》

「･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。



© UMIN Center

B．秘密鍵･公開鍵の作成

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) Mozilla Thunderbird　モジラ　サンダーバード　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。

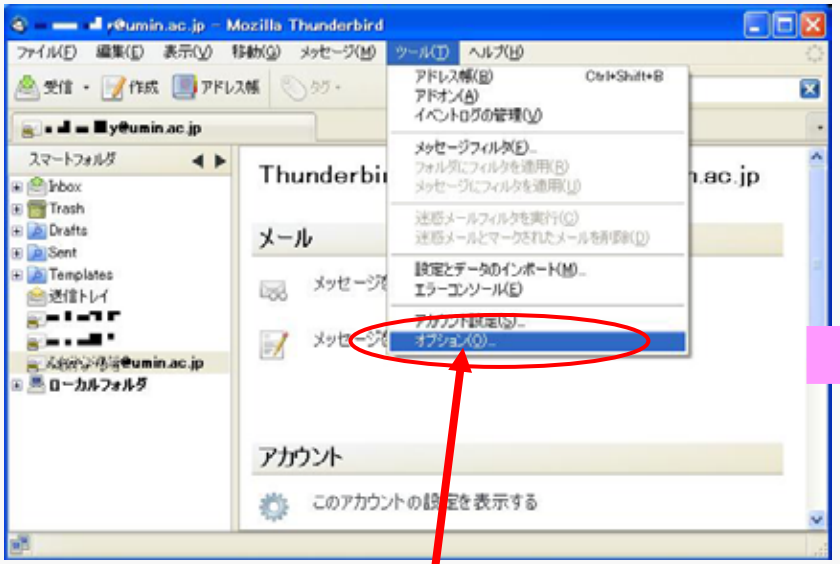
アカウントごとにデジタル証明書を有効にすることにより、メールへの署名や暗号化が可能になります。

© UMIN Center

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) Mozilla Thunderbird　モジラ　サンダーバード　使用の場合
(クライアント証明書とルート証明書をダウンロードした後)



①メールソフト起動後、
「ツール」→「オプション」をクリックして
表示させます。

②「詳細」を選択します。

③「証明書を表示」を
クリックして証明書マネージャをひらきます。

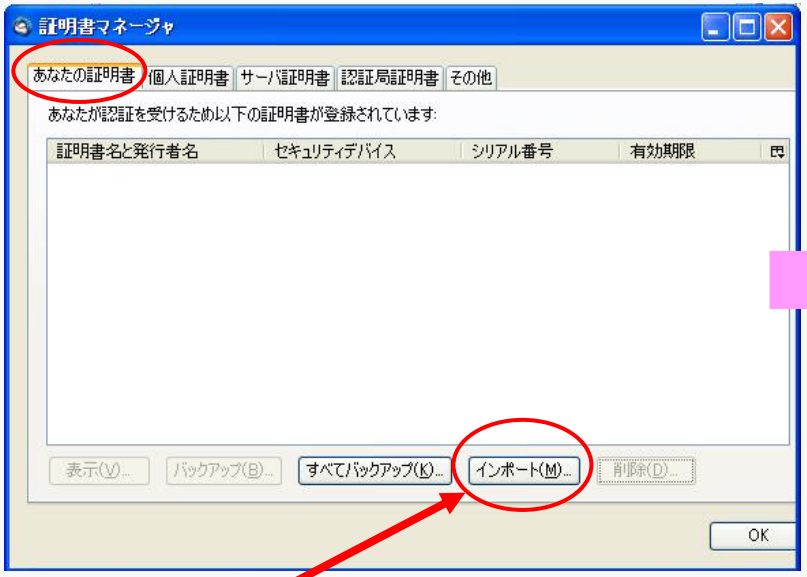
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

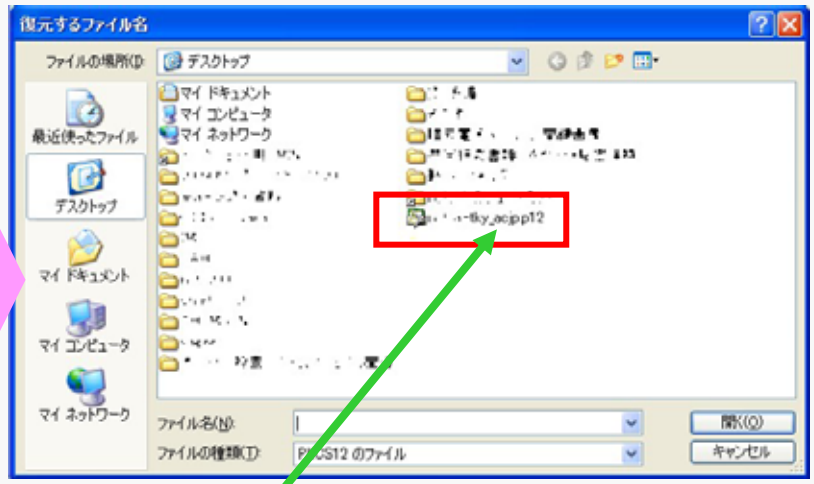
© UMIN Center

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）Mozilla Thunderbird　モジラ　サンダーバード　使用の場合





①「インポート」をクリックし、証明書を追加します。

②ダウンロードした場所を開き
「～.p12」ファイル選択し、
「開く」をクリックしてください。

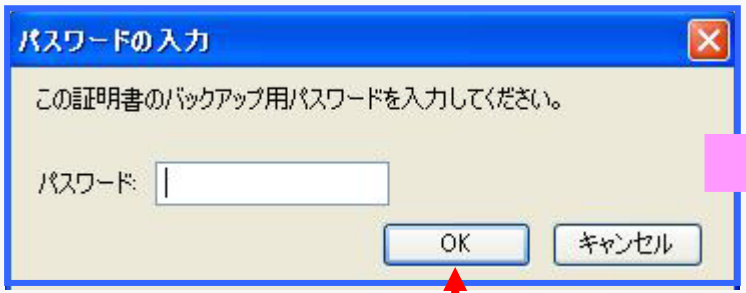
（例は、～.p12 ファイルをデスクトップに
ダウンロードしていた場合です。）

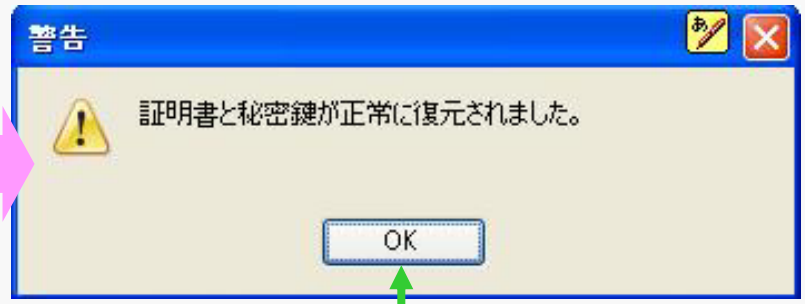
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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）Mozilla Thunderbird　モジラ　サンダーバード　使用の場合





①そのまま何も入力せずに
「OK」をクリックします。

②証明書と秘密鍵が復元されるので、
「OK」で終了します。

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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）Mozilla Thunderbird　モジラ　サンダーバード　使用の場合

①証明書が追加されたことを確認します。

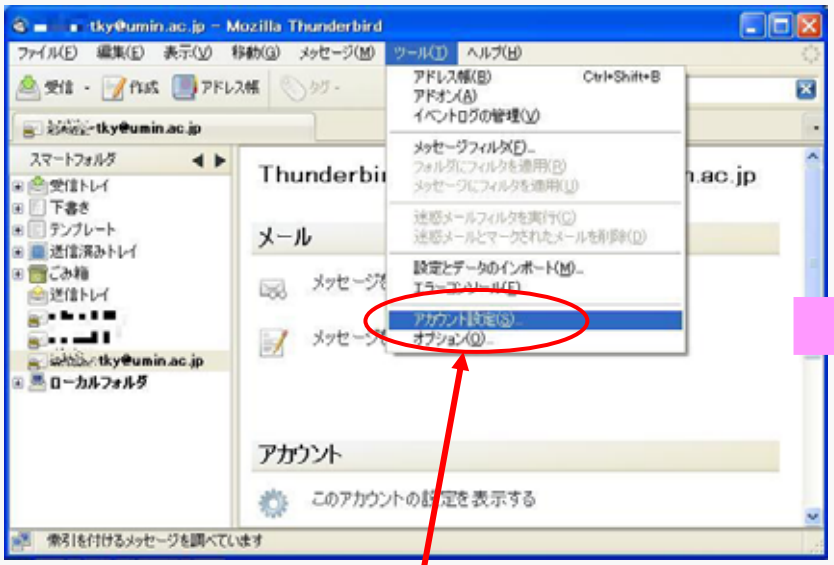
②「OK」をクリックして次へ。

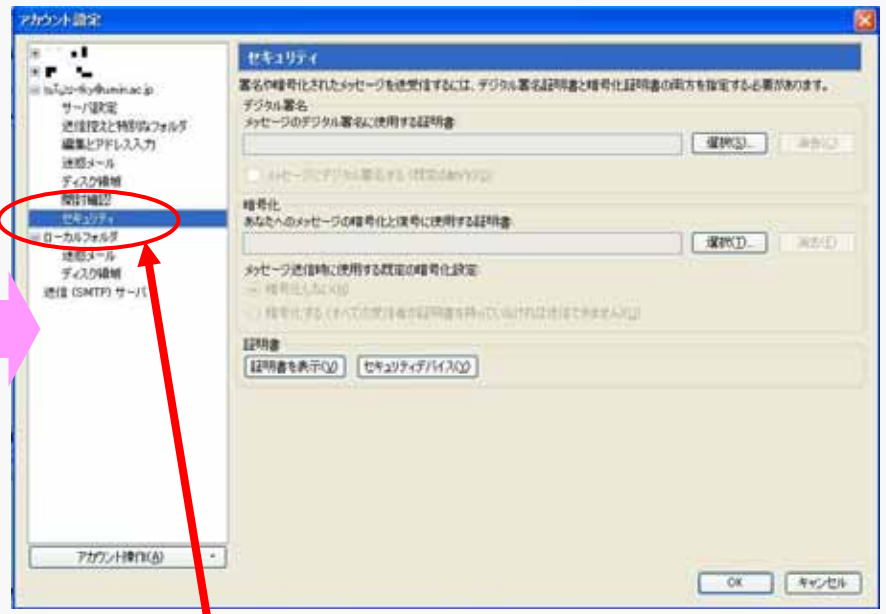
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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）Mozilla Thunderbird　モジラ　サンダーバード　使用の場合





①「ツール」→「アカウント設定」で
アカウント設定画面を開きます。

②アカウント設定
「セキュリティ」をクリックしてください。

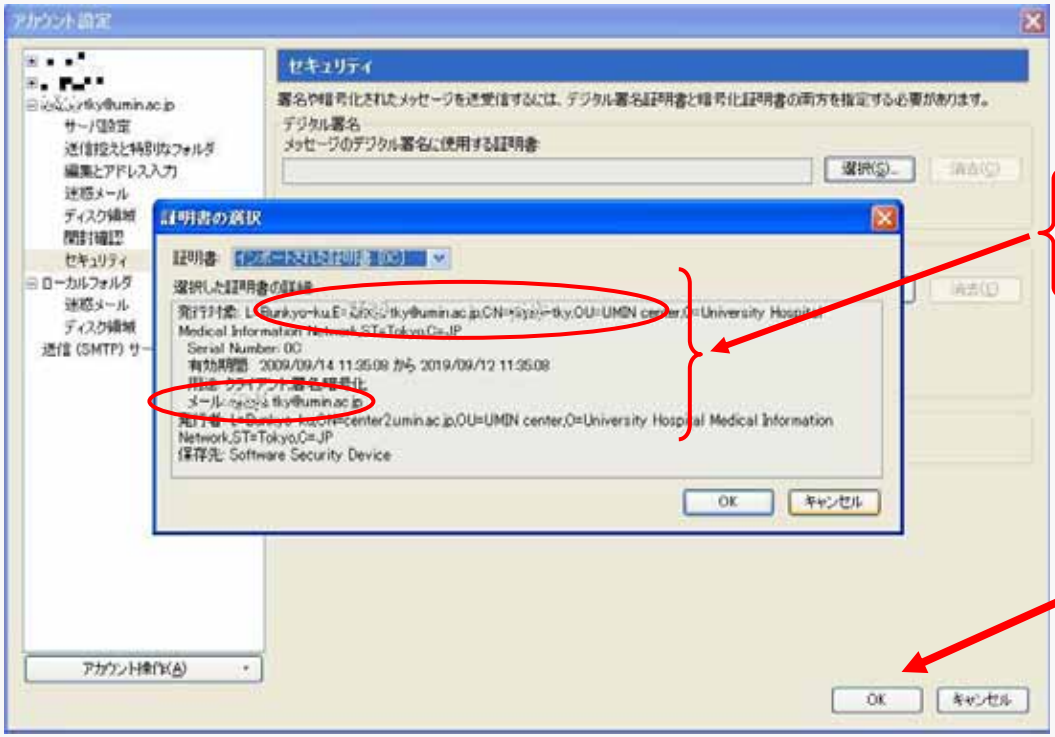
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

© UMIN Center

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）Mozilla Thunderbird　モジラ　サンダーバード　使用の場合



①インポートされた証明書を選択します。

発行対象：L=Bunkyo-ku,E=自分のメールアドレス,OU=UMIN center

：

：

メール：自分のメールアドレス

E＝自分のメールアドレス
メール：自分のメールアドレス

であることを確認してください。

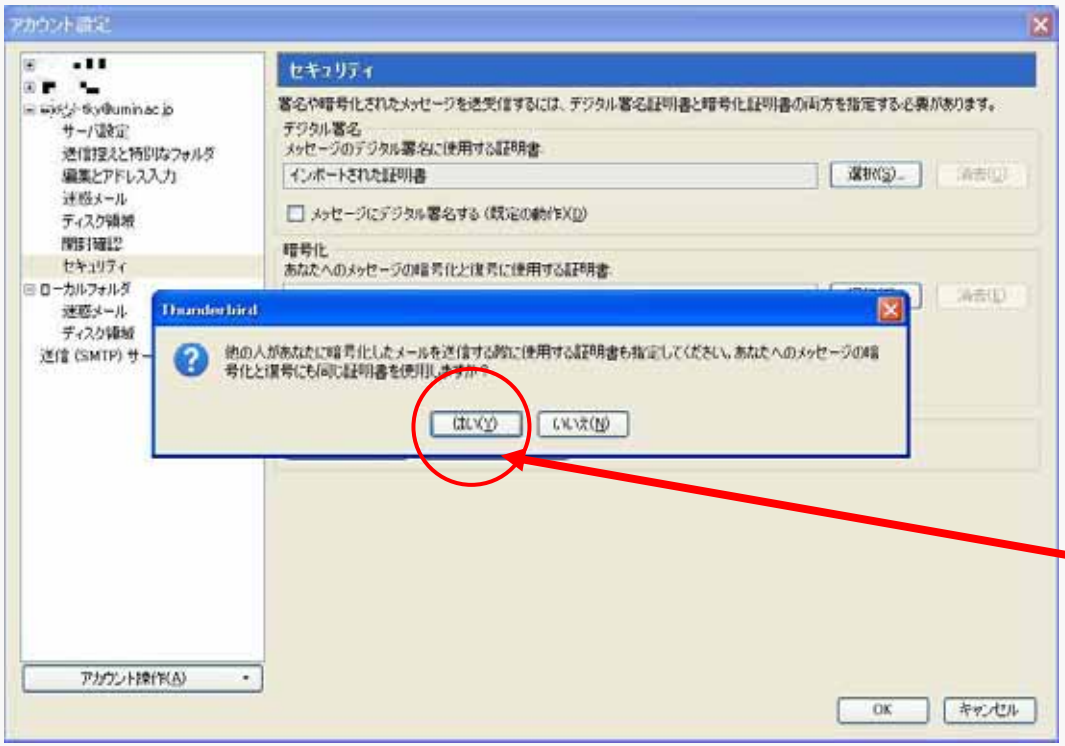
②「OK」をクリックします。

© UMIN Center

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）Mozilla Thunderbird　モジラ　サンダーバード　使用の場合



①メッセージ
「他の人があなたに暗号化したメールを送信する際に使用する証明書も指定してください。あなたへのメッセージの暗号化と復号にも同じ証明書を使用しますか？」

「はい」をクリックします。

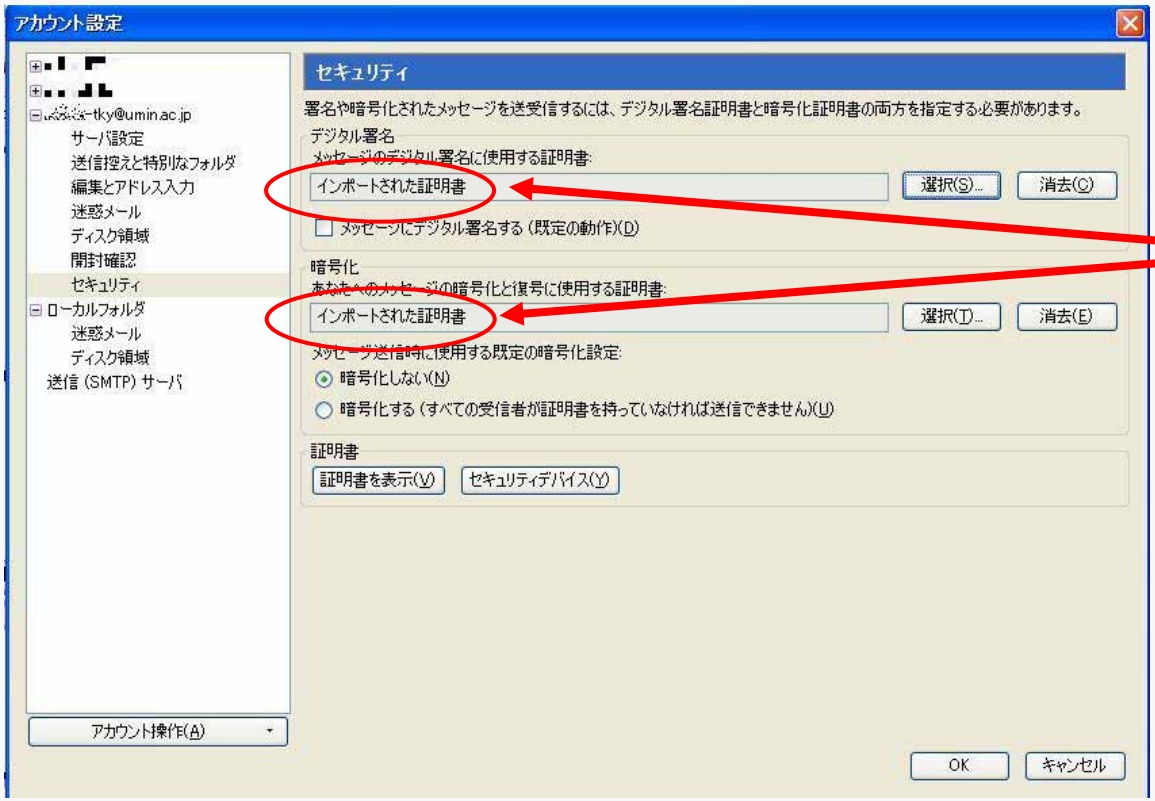
以上で、「クライアント証明書」インポートされました。

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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）Mozilla Thunderbird　モジラ　サンダーバード　使用の場合



「インポートされた証明書」
の表示を確認。

次ページより
「ルート証明書」
をインポートします。

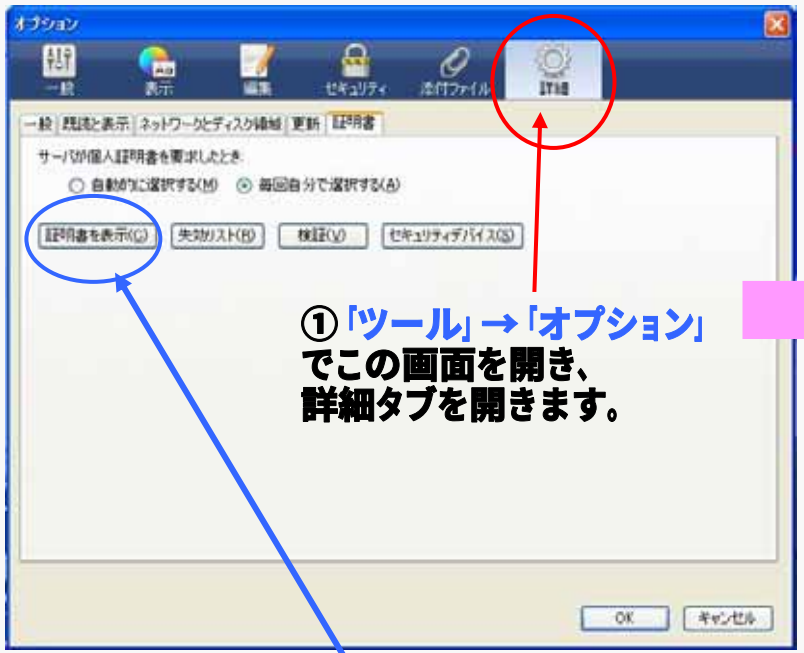
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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

(B1－10) Mozilla Thunderbird　モジラ　サンダーバード　使用の場合

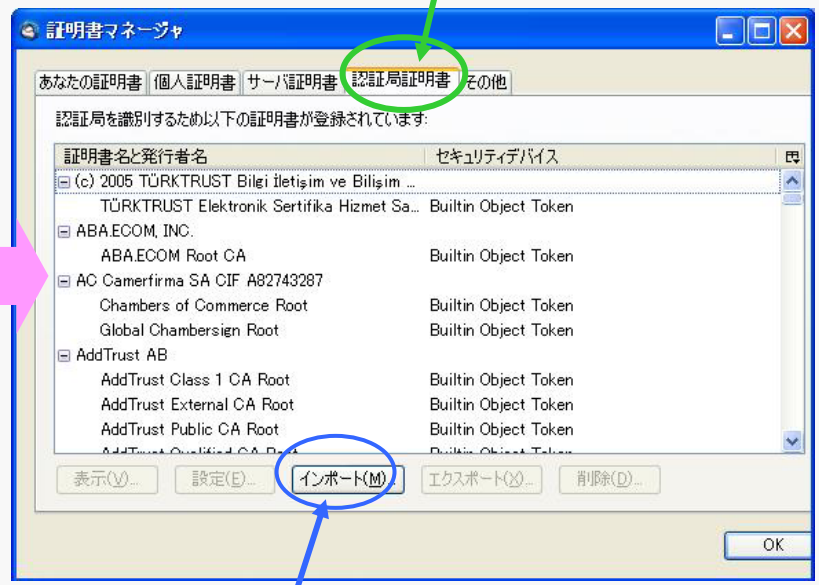
ルート証明書 (認証局証明書) のインポートをします。



①「ツール」→「オプション」でこの画面を開き、詳細タブを開きます。

②「証明書を表示」をクリック

③「認証局証明書」を選択します。



④「インポート」をクリック

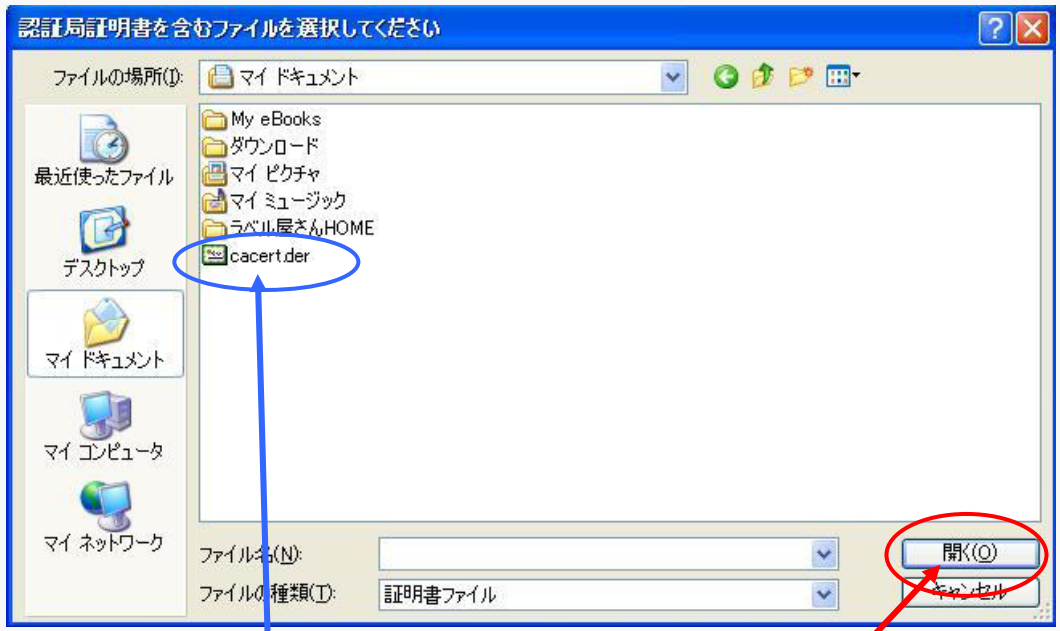
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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

(B1－11) Mozilla Thunderbird　モジラ　サンダーバード　使用の場合

(続き) ルート証明書 (認証局証明書) のインポートをします。



(例は、cacert.der ファイルを
「マイドキュメント」フォルダに
ダウンロードしていた場合です。)

①「cacert.der」を選択

②「開く」をクリック　→　インポート画面が開きます。

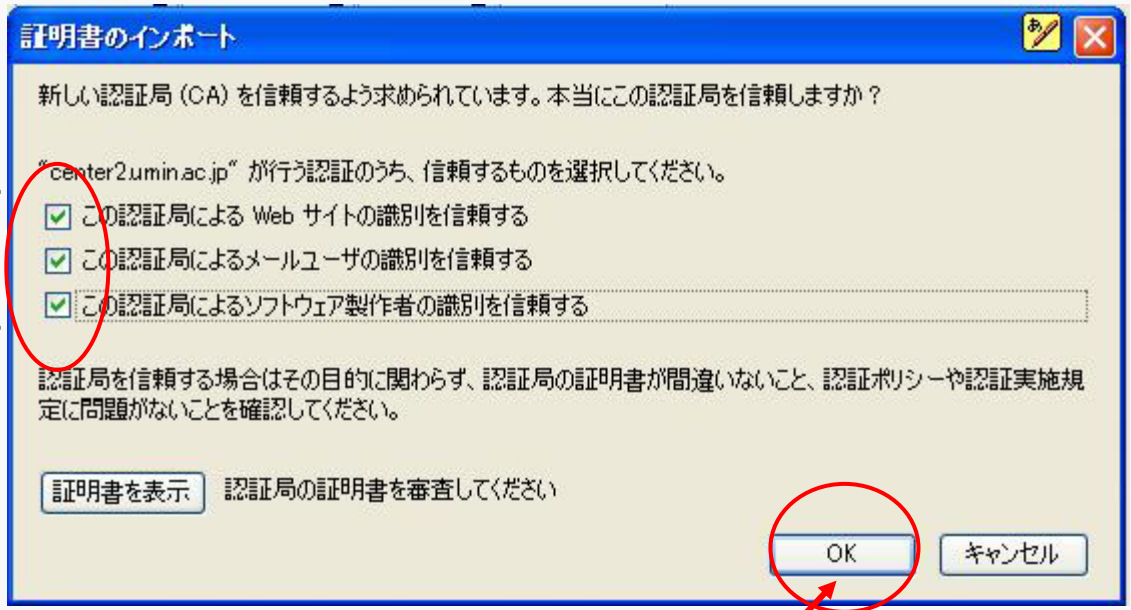
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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

(B1－12) Mozilla Thunderbird　モジラ　サンダーバード　使用の場合

(続き) ルート証明書 (認証局証明書) のインポートをします。



①3ヵ所全てにチェックをいれます。

②「OK」をクリック

以上で、「クライアント証明書」「ルート証明書」がインポートされ、

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。

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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。

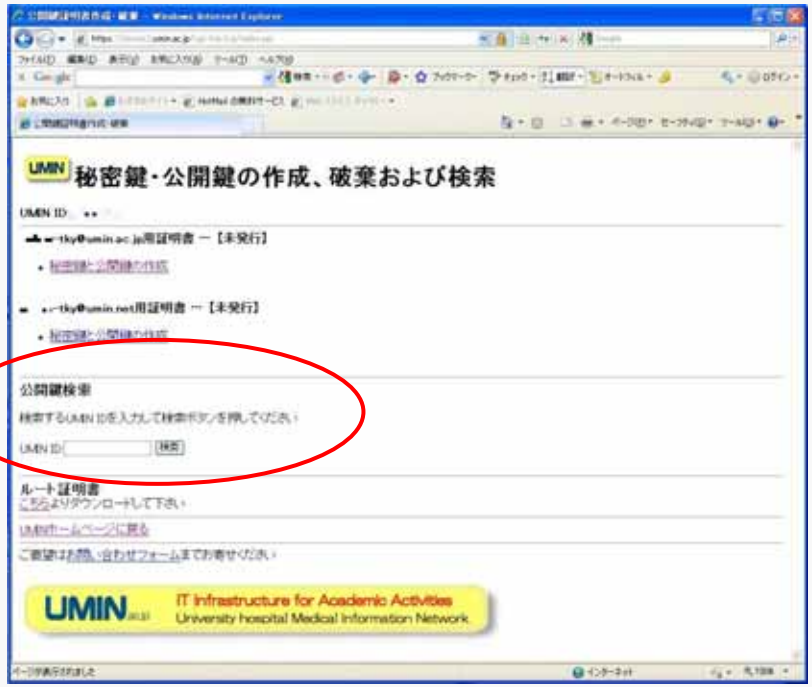
（送信相手が、公開鍵を発行していることが必要です。）

© UMIN Center

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

《 登録者用ページ　トップページ 》



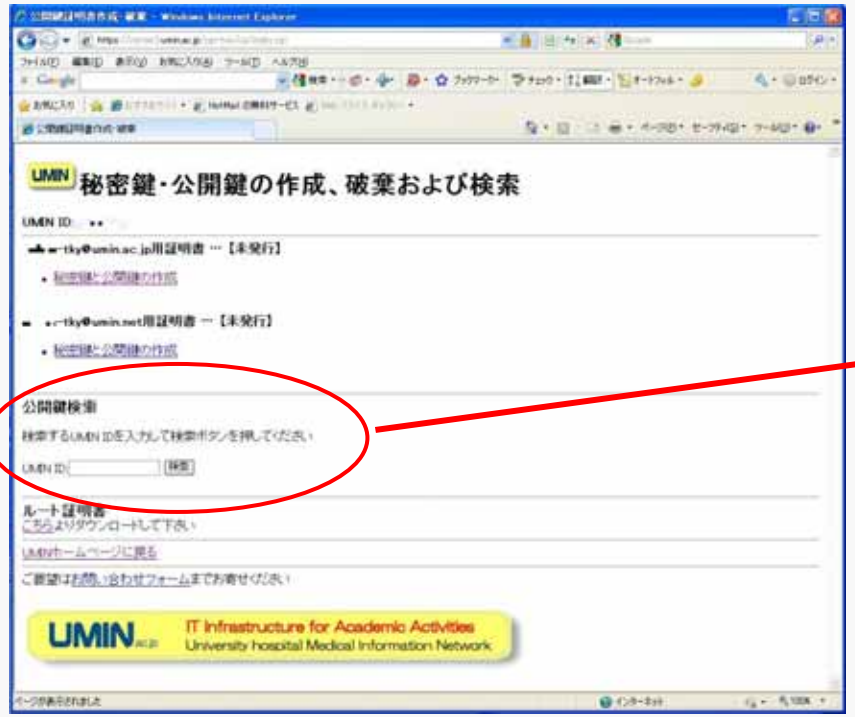
送信相手のUMIN-IDを検索し、
公開鍵の設定がされていれば、
公開鍵証明書をダウンロードし、
メールソフトに設定することで、
暗号化して送信することができます。
（送信相手が発行した公開鍵で
暗号化したメールの送信ができます）

© UMIN Center

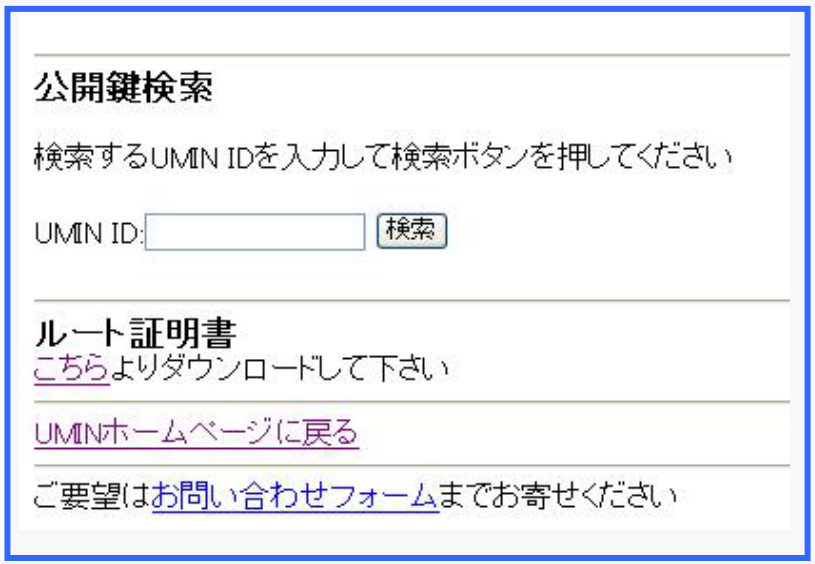
C．秘密鍵･公開鍵の作成

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／～@umin.netの～部分）



UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

© UMIN Center

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。

（～umin.netの場合、ダウンロードしたファイル名は ～.net.cer になります。）

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

C．秘密鍵･公開鍵の作成

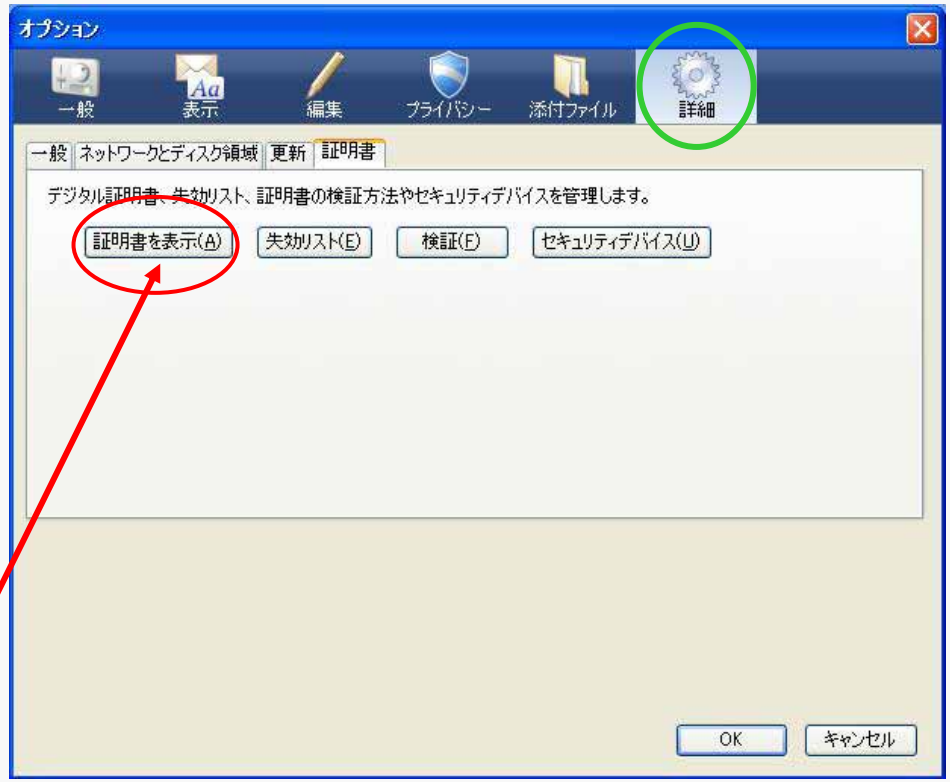
⑤秘密鍵･公開鍵の発行：証明書の検索

《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》

（C１－１）Mozilla Thunderbird

【あらかじめ、C－①～④により
送信相手の公開鍵証明書
（XXXX-XXX.ac.jp.cer）
をダウンロードしてください】

ソフトを起動し、
「ツール」→「オプション」を
クリックすると右の画面が開きます。
「詳細」タブを選択し
「証明書を表示」ボタンをクリックして
ください。



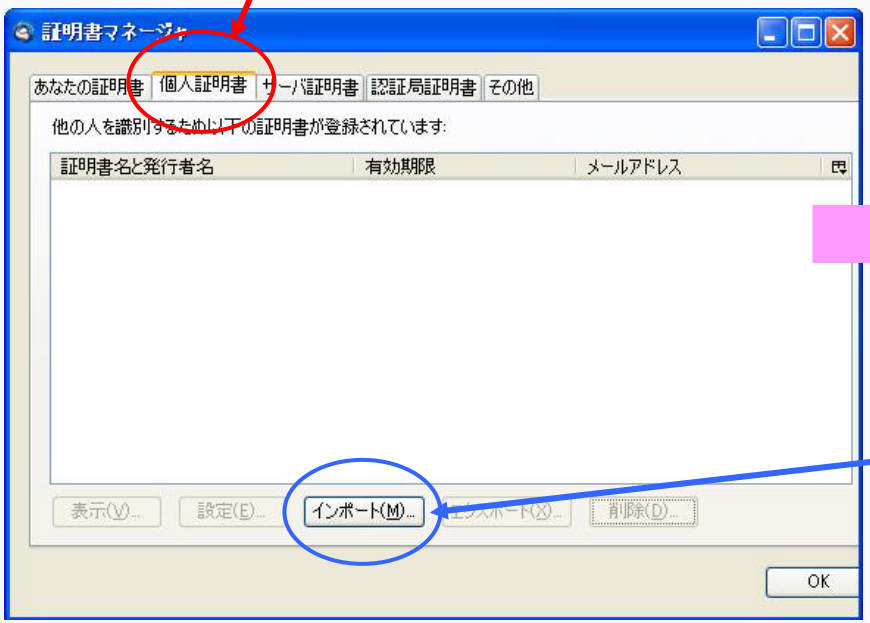
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

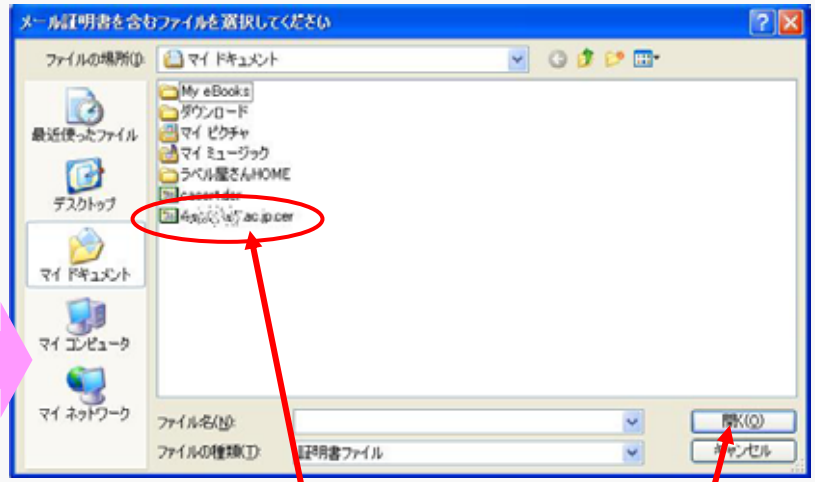
C．秘密鍵･公開鍵の作成

⑥秘密鍵･公開鍵の発行：証明書の検索

(C１－２) Mozilla Thunderbird　署名、暗号化したメールの作成

「証明書マネージャ」が開きます。
「個人証明書」タブをクリックします。





「インポート」ボタンをクリックします。

あらかじめダウンロードした証明書ファイル
（XXXX-XXX.cer　送信相手の公開鍵）を
選択し、「開く」をクリックします。

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

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

(C1－3) Mozilla Thunderbird　署名、暗号化したメールの作成

送信相手の証明書がインポートされました。

「OK」をクリックしてください。

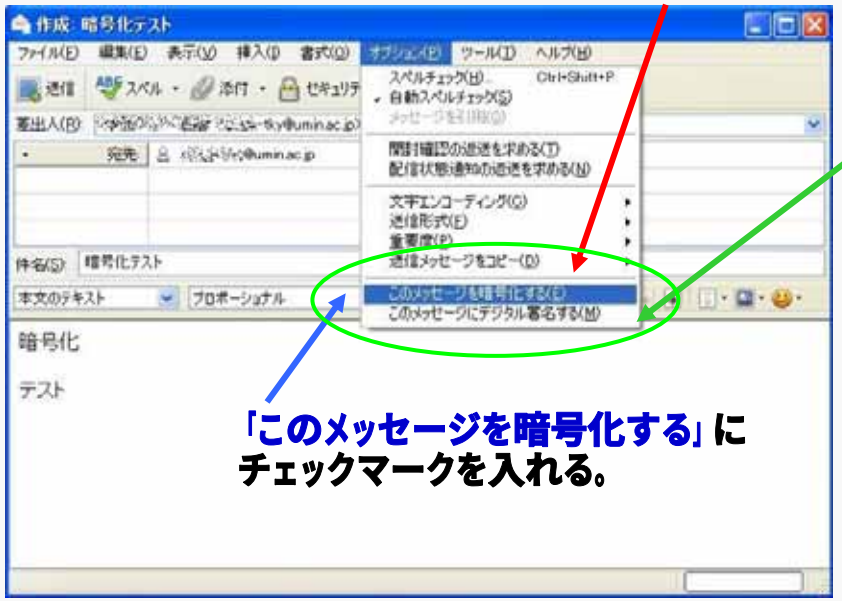
UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center

C．秘密鍵･公開鍵の作成

(C１－４) Mozilla Thunderbird　署名、暗号化したメールの作成

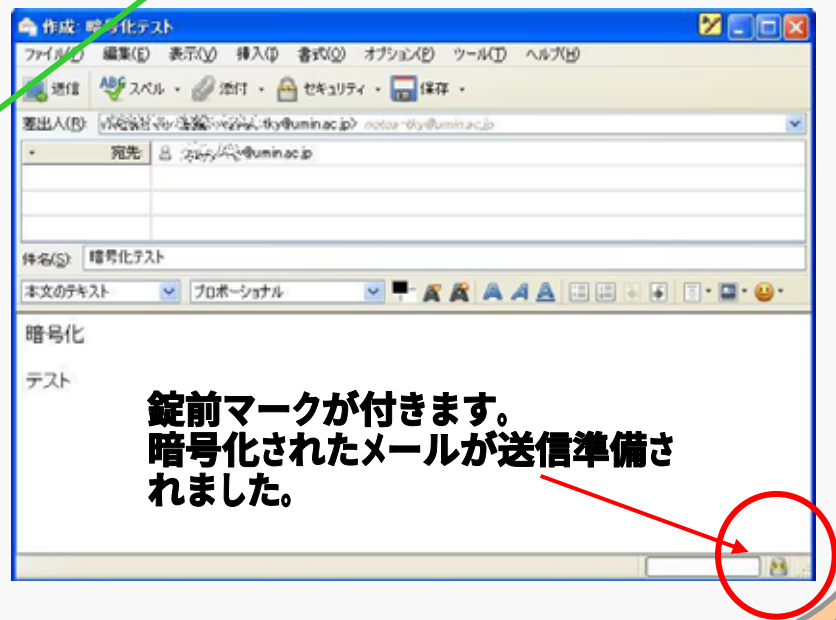
メールを暗号化して送信するために、送信するメールに設定を行います。

送信文を用意し、相手先のアドレスを入力し、送信準備をします。
「ツール」→「オプション」を開き、
「このメッセージを暗号化する」にチェックをいれます。



「このメッセージを暗号化する」に
チェックマークを入れる。

「このメッセージにデジタル署名する」
にチェックを入れるとデジタル署名が
追加されます。



錠前マークが付きます。
暗号化されたメールが送信準備さ
れました。

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network

© UMIN Center

メール暗号化：秘密鍵・公開鍵の作成

作業完了

UMIN Infrastructure for Academic Activities
University hospital Medical Information Network
© UMIN Center