

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<mark>公開鍵</mark>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。

No.2 UMIN Infrastructure for Academic Activities University hospital Medical Information Network

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)モジラ サンダーバード(Mozilla Thunderbird)

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

No.4 UMN Infrastructure for Academic Activities University hospital Medical Information Network

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

| 2 2008년(2년)감위 K- Will - Windows Internet Explorer | | |
|--|-----------------------------|-------------------------|
| • B. Mar Chemic Lunit and p fraction of a finite out | 🖉 🎒 🔂 🕂 🗶 🖓 hear | (A) * |
| 7+(MD 編集(D 県市(A) お死に入が(A) ?-A(D へん?08 | | |
| Congle din to the second secon | Ø · Ø 3202-0 | S. 0050. |
| Station is a station of the second se | · ▲·回:□ ●· <-700・セー774回・ | • 9~A(Q) • 🚱 • " |
| UMIN 秘密鍵・公開鍵の作成、破棄 | および検索 | トップページ「登録者用ページ」 |
| 📥 tky@umin.ac.jp用証明書 【未発行】 | | XXXX-XXX@umin.ac.in用証明書 |
| 秘密時に公開時の作成 | | |
| ■ •tky@umin.net用証明書【未発行】 | | XXXX-XXX@umin.net用証明書 |
| ・ 秘密部と公開部の作成 | | |
| | | 公開建協委の入力枠 |
| 公開鍵検索 | | |
| 検索するUMINIDを入力して検索ボタンを押してください | | |
| UMIN ID [[HER] | | レート証明書 |
| ルート証明書 <u>こちら</u> よりダウンロードして下さい | | |
| いわれームページに戻る | | |
| こ要望はお問い合わせフォームまでお寄せげたさい | | |
| | | |
| I INAINI IT Infrastructure for Academic | Activities | |
| University hospital Medical Inform | ation Network | |
| | | |
| 一切が表示されました | @ +2,4=+3+ | ra + 10,100 + |





No.7 UMIN Infrastructure for Academic Activities University hospital Medical Information Network



No.8 UMIN Infrastructure for Academic Activities University hospital Medical Information Network



No.9 UMIN Infrastructure for Academic Activities University hospital Medical Information Network



MIN Infrastructure for Academic Activities University hospital Medical Information Network

No.10



No.11 UMIN Infrastructure for Academic Activities University hospital Medical Information Network

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



Mozilla Thunderbird

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)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)



Infrastructure for Academic Activities University hospital Medical Information Network

No.13

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



No.14 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 - 4)Mozilla Thunderbird モジラ サンダーバード 使用の場合

| | 警告 | 🔀 ೧(೫ಕು. | スワードの入力 この証明書のバックアップ用パスワードを入力してくた |
|-------|-----------------|-------------|--------------------------------------|
| | ОК | **>セル | パスワード: OK |
| ぇるので、 | 証明書と秘密鍵が復元されるので | 入力せずに | そのまま何も入 |
| | 「UK」で終了しま9。 | します。 | 'OK」をクリックし |
| | | | |

No.15 UMN Infrastructure for Academic Activities University hospital Medical Information Network



No.16 UMN 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 - 6)Mozilla Thunderbird モジラ サンダーバード 使用の場合



No.17 UMN 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 - 7)Mozilla Thunderbird モジラ サンダーバード 使用の場合

| a • • • • · · · | ヤキュリティ | |
|--|---|--|
| とないよれ、のuminacip サーバ型を定 送信控えた特別はなフォルダ 編集とアドレス入力 | 署名や経営化されたメッセージを活動信するには、デジタル署名証明書と総合化証明書の両方を指定する必要があります。 デジタル署名 メッセージのデジタル署名に使用する証明書 | インポートされた証明書を選択します。 |
| 注応メール ディスク領域 開封確認 セキュリティ ローカルフォルダ 選択した証明 | | 発行対象:L=Bunkyo-ku,E=目分のメールアドレス,OU=UMI center |
| 建築メール ディスカ編載 通信(SMTP)サー 本が規範 用したシールのac ストル ac ストル ac ストル ac | Control - Lucie - Log - Lucie - L | E = 自分のメールアドレス メール: 自分のメールアドレス メール: 自分のメールアドレス |
| 3#1495.301 | OK THEY'RE | であることを確認してください。 |
| | | 「OK」をクリックします。 |
| アカウンド律作(点)・ | OK ##JES | |
| | | _ |

Infrastructure for Academic Activities University hospital Medical Information Network

No.18

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

| ALC: NO REAL | × | |
|---|--|---|
| | セキュリティ | |
| ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ | 客名や暗号化された大ッセージを迭受信するには、デジタル客名証明書と暗号化証明書の両方を指定する必要があります。 デジタル客名、 メッセージのデジタル署名に使用する証明書。 インボートされた証明書 選択(3) ホッセージにデジタル署名する(数定の動作に20) 暗号化 あたたへのメッセージの暗号化と復気に使用する証明書。 ハンボあたた(暗号化したメールを送信する数に使用する証明書も指定してください、あたたへのメッセージの暗 ハンボのたた(暗号化したメールを送信する数に使用する証明書も指定してください、あたたへのメッセージの暗 (はいな) (はいなび) (はいな) | 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。 |
| アカウント操作(A)・ | | 以上で、「クライアント証明書」 |

No.19

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

| アカウント設定 | | |
|--|---|--|
| ●●●●●● ● 、 本録会・株y@umin.ac.jp サーバ設定 送信控えと特別なフォルダ 編集とアドレス入力 迷惑メール ディスク領域 開封確認 セキュリティ ● ローカルフォルダ 迷惑メール ディスク領域 送信 (SMTP) サーバ | セキュリティ 署名や暗号化されたメッセージを送受信するには、デジタル署名証明書と暗号化証明書の両方を指定する必要があります。 デジタル署名 ッセ・ジのデジタル署名に使用する証明書: インボートされた証明書 タッセージにデジタル署名する(既定の動作)(D) 暗号化 本誌やのカンビージの暗号化と復号に使用する証明書: インボートされた証明書 ダンセージと送信時気に使用する証明書: インボートされた証明書 ダンセージと信頼する既定の暗号化設定: ・ 暗号化しない(N) ・ 暗号化しない(N) ・ 暗号化しない(N) ・ 暗号化しない(N) ・ 暗号化しない(N) ・ 暗号化しない(N) ・ 暗号化を表示(Y) セキュリティデパイス(Y) | - 「インポートされた証明書」 の表示を確認。 |
| アカウント 排作(A)・ | OK 本ヤンセル | 次ページより 「 <mark>ルート証明書」</mark> をインポートします。 |

No.20

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 (B1-10)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。



No.21 UMN 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 - 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。

No.22

| र्ग २७२७-७ | ファイル4 6(N): ファイルの 種類(T): acert.der」を | [証明書ファイル 選択 | | | ▼ ▼ 】 | | インポート画面が開きます。 |
|-------------|---|---------------------------|---|----|-------------|-----|---|
| デスクトップ | Cacert.der | | | | | | (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。) |
| していたつ たつアイル | My eBooks ダウンロード マイ ピクチャ マイ ミュージック ラベル屋さんHOMI | | | | | | |
| ファイルの場所(1): | 📋 マイ ドキュメント | en de Deder | ~ | 00 | • 🖭 👏 | | |
| 認証局証明書を含 | むファイルを選択して | ください | | | | ? 🛛 | |

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 - 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。

No.23



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ことが必要です。)

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

(登録者用ページ トップページ)

| A STREET BUILDING OF THE PARTY AND ADDRESS OF THE PARTY ADDRESS OF THE | | 16 JD |
|--|--|-----------------------------|
| O C + K Her. merks, a reserve | 大臣(注(す)を)構(です | 18 |
| 7+14D #B/D #E() ##L/4() *-4() -47() | and do D. Anno. Sec. Hat. Same | A |
| | an info A. M. A muss. A mouther Dammer A | d. 0.611 |
| Everya | Rent Contractor | |
| B Castlinguit an | and a second trave | 6. 1. M. 6. |
| WMN 秘密鍵・公開鍵の作り | 成、破棄および検索 | |
| A settle basis of the Billing at a Spicial | | |
| | | |
| MCENNEL 2/FORMER/1915 | | |
| | | |
| · ···································· | | |
| 相定線と公開線の作成 | | |
| | | |
| 公詞鍵検索 | | |
| 林安するCADN Dを入力して検索モダンを用いていたみ | | |
| 1000 | | |
| (MNID) (MR) | | |
| 1 | | |
| こちちょりタウンロートして下さい | | |
| いたなホームページに見る | | |
| この頃はお読い合わせフォームまでお寄せくだあ。 | | |
| | | |
| I IA AIA I IT infrastructure | for Academic Activities | |
| University hospital | Medical Information Network | |
| A Second Se | | |
| (-10851231.5 | 0 () - 14 | A. 8.100 |
| The second | 12754H | a contraction of the second |

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)



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 COMPANY OF THE WORKS DISCOUT DESIGNATION を入力する。 - B B(4) X 8 HAD BED ARD NECTOR THE ANTE (メールアドレス: ~ @umin.ac.jp / ~ @umin.netの~部分) 4 · 0 8545 · · Q * 12 - 13 @ * H-088* 8-0942+ 9-603* @* A CONTINUE AND AND 秘密鍵・公開鍵の作成、破棄および検索 UMIN ID ... 公開鍵検索 ▲ - thy@umin.ac. jp川证明書 … [未受行] ・和安保と公開時の作成 検索するUMIN IDを入力して検索ボタンを押してください --tky@umin.net用证明書 -- (未発行) 秘密部と公開制の作品。 検索 UMIN ID: 公開鍵操術 林奈するLMAN IDを入力して林奈市タンを押してください UMPH ID: ルート証明書 こちらよりダウンロードして下さい ルート証明者 こちらよりダウンロートして下さい LAADVカームページに見る UMINホームページに戻る ご要望はお聞い合わせフォーム主でお寄せください IT Infrastructure for Academic Activities UMIN ご要望はお問い合わせフォームまでお寄せください University hospital Medical Information Netwo -008-2010-0.5 ()8+\$# 14 - A.108

No.26 UMN Infrastructure for Academic Activities University hospital Medical Information Network



UNIVERSITY HOSPITAL MEDICAL INFORMATION NETWORK

No.27

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



No.28 UMN Infrastructure for Academic Activities University hospital Medical Information Network

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

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



No.29

Infrastructure for Academic Activities University hospital Medical Information Network

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

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

No.30

| 証明書名と発行者名 | 有効期限 | メールアドレス | 送信 | 自相手の証明書が |
|---|-----------------------|------------------------|----|-----------|
|] University Hospital Medical 法演会rumin | Informa 2019/11/03 | ്ള്ള്,∺umin@umin.ac.jp | イン | ポートされました。 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Infrastructure for Academic Activities University hospital Medical Information Network

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。 「このメッセージにデジタル署名する」 「ツール」「オプション」を開き、 にチェックを入れるとデジタル署名が 「このメッセージを暗号化する」にチェックをいれます。 追加されます。 ▲ 作成:暗号化テスト 200 作成 暗分化テスト ファイル(E) 編集(E) 表示(y) 挿入(D 書式(D) オブリッシュ(E) ツール(D) ヘルプ(E) ファイルシン 編集(E) 表示(V) 挿入(D 書式(Q) オブション(P) ツール(D ヘルプ(H) スペルチェック(日) Otrl+Shitt+P ■ 通信 🦉 スペル ・ 🖉 添付 ・ 🔒 セキュリテ 通信 🖑 スペル ・ 🖉 添付 ・ 🖂 セキュリティ ・ 🥅 保存 ・ 自動スペルチェック(S) 憲出人(R) Profit Participation (Participation) 差出人(B) 《论说话》得《法编》、《论学》、北小母uminacip》 notce-Wy-duminacip 開封確認の過速を求める(1) 第一 名 xillix Hirthuminacip 宛先 8 math Quminacip 配信状物通知力语诱考求协选(N) 文字エンコーティング(0) 送信形式(E) き信メッセージをコピー(D) (件名(S) 暗号化テスト 件名(S): 暗号化テスト このメッセージを暗号化する(ロ 本文のテキスト ブロボーショナル - 🖾 - 😂 本文のテキスト プロポーショナル このパッセージにデジタル署名する(M) 暗号化 暗号化 テスト テスト 錠前マークが付きます。 「このメッセージを暗号化する」に 暗号化されたメールが送信準備さ チェックマークを入れる。 れました。

No.31 UMIN Infrastructure for Academic Activities University hospital Medical Information Network

