（4）ＰＤＦ署名ライブラリ概説

MEDI-Papyrus(HPKI 版)および飯塚病院版地域医療基盤推進事業対応プログラムに組み込んだ市販の HPKI ライブラリは以下の概要である

[MEDI-Papyrus(HPKI 版)に組み込んだ HPKI ライブラリ概要]

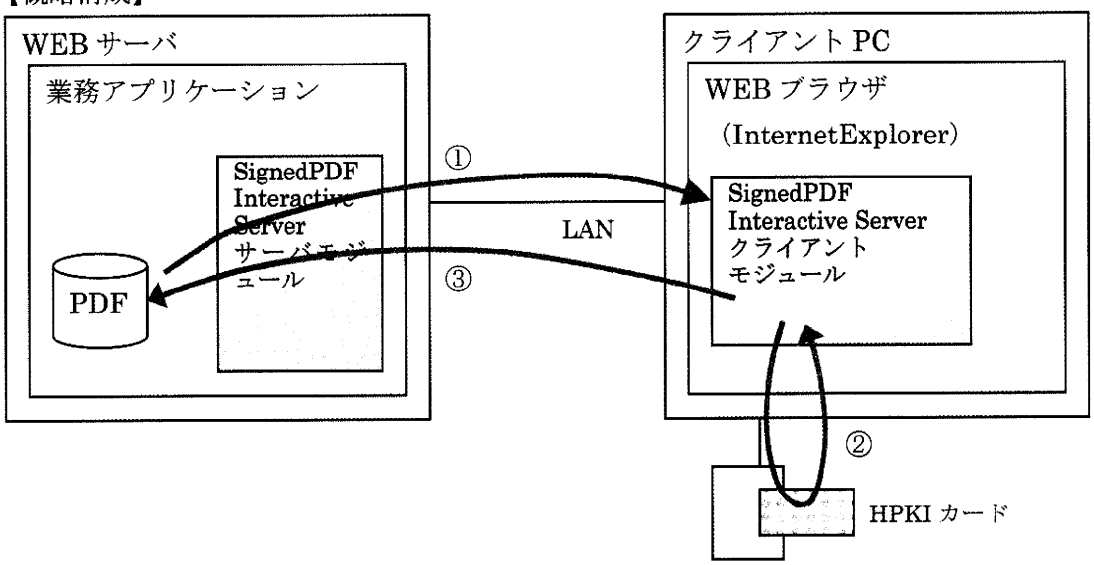
1）MistyGuard<SignedPDF Interactive Server> 4.00

【機能概要】

本ライブラリ製品は WEB 型のアプリケーションにおいて、サーバ側にある PDF ファイルに対し、クライアントの WEB ブラウザ上にて、PDF への電子署名を付与するライブラリである。電子署名の形式は CAdES（CMS Advanced Electronic Signatures）フォーマットのベースとなる EBS 署名である。

署名はクライアントに接続された IC カード RW に挿入された IC カード（HPKI カード）により署名演算されて、署名データがサーバに送付され、PDF 内に署名データが格納される。

【概略構成】



① サーバにある PDF ファイルのダイジェスト（ハッシュ値）をクライアントモジュールに送付

② ダイジェストに対し HPKI カードに対し署名演算要求を行い、IC カードの PIN 入力操作を行い署名値を求める。

③ 求まった署名値をサーバに返送し、署名対象 PDF ファイル内の署名値エリアに格納して、署名済み PDF ファイルを生成

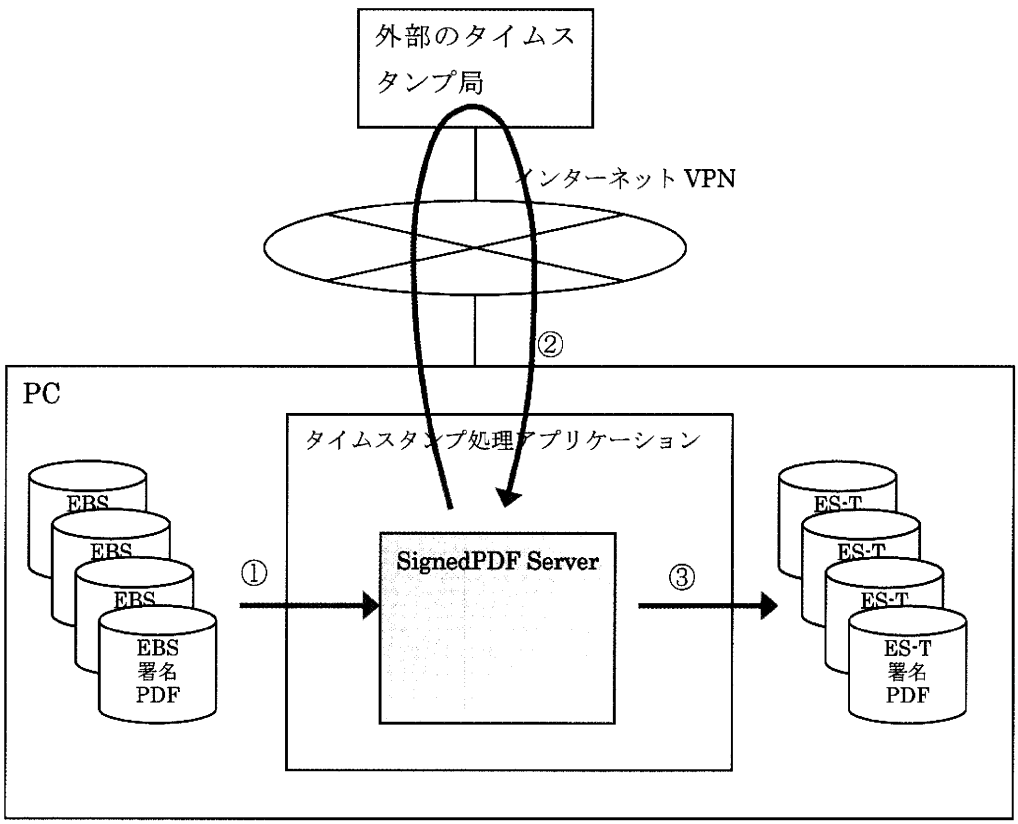
2）MistyGuard<SignedPDF Server>PureJava 2.00

【機能概要】

PC 内で稼働する PDF 署名処理を構築するための署名ライブラリである。主に自動的な PDF 署名処理の構築が目的のライブラリ。電子署名の形式は CAdES(CMS Advanced Electronic Signatures)フォーマットに対応し、タイムスタンプ取得機能がありタイムスタンプを包含した ES-T 署名形式に対応。

MistyGuard<SignedPDF Interactive Server> 4.00 等で作成した EBS 形式の PDF 署名に対し、タイムスタンプを取得して ES-T 形式の PDF 署名に更新することができる。

【概略構成】



① EBS 署名済みの PDF ファイルを読み込む

② EBS 署名値のダイジェスト（ハッシュ値）をタイムスタンプ局に送付し、タイムスタンプ署名値を求める。

③ タイムスタンプ署名を含めた ES-T 署名形式を生成し署名 PDF の署名データを更新。

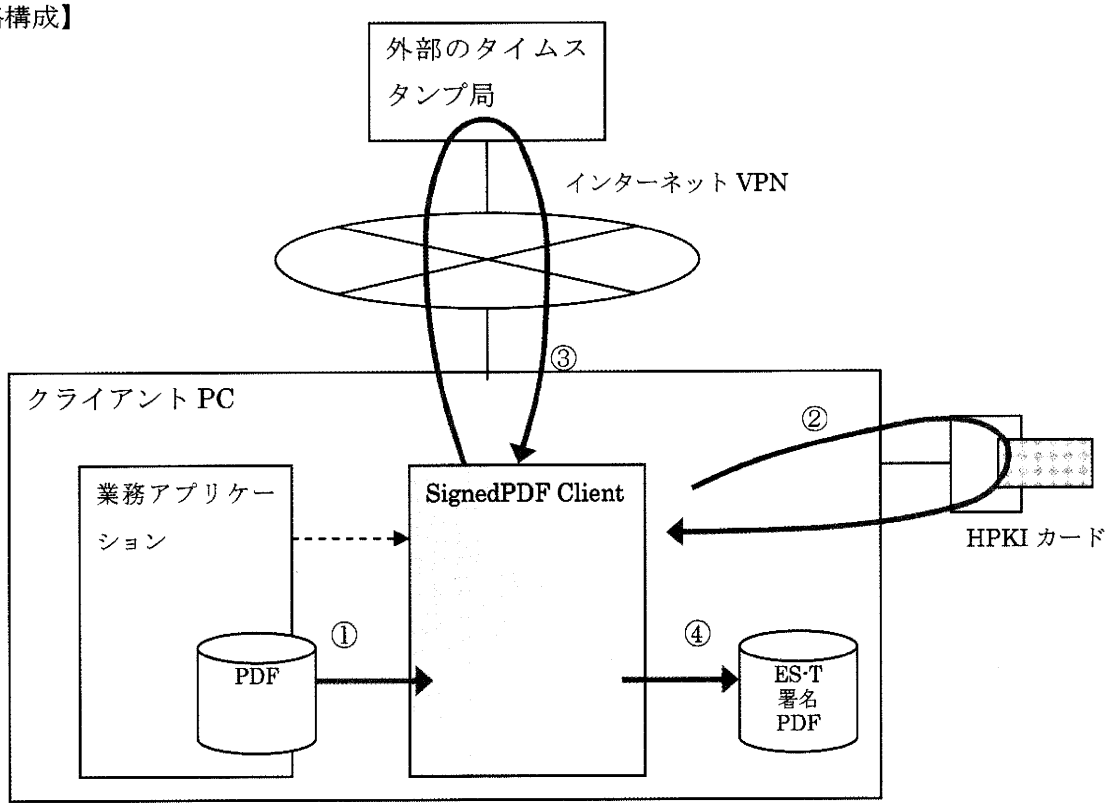
[飯塚病院版地域医療基盤推進事業対応プログラムに組み込んだ HPKI ライブラリ概要]

SignedPDF Client 1.00

【機能概要】

本製品はクライアント PC 上で単独に PDF 署名を行うアプリケーション製品。電子署名の形式は CAdES(CMS Advanced Electronic Signatures)フォーマットに対応し、タイムスタンプ取得機能がありタイムスタンプを包含した ES-T 署名を行うことができる。また、タイムスタンプ機能を用いない場合には EBS 署名を生成する。署名はクライアントに接続された IC カード RW に挿入された IC カード（HPKI カード）により署名演算を行う。本製品は他のアプリケーションと連携して動作するための API（アプリケーションインタフェース）を装備しており、文書作成業務アプリケーション等との連動が行える。

【概略構成】



①署名する PDF ファイルを読み込む

②PDF ファイルのダイジェスト（ハッシュ値）を求め HPKI カードに対し署名演算要求を行い署名値を求めます。IC カードの PIN 入力操作が必要です。

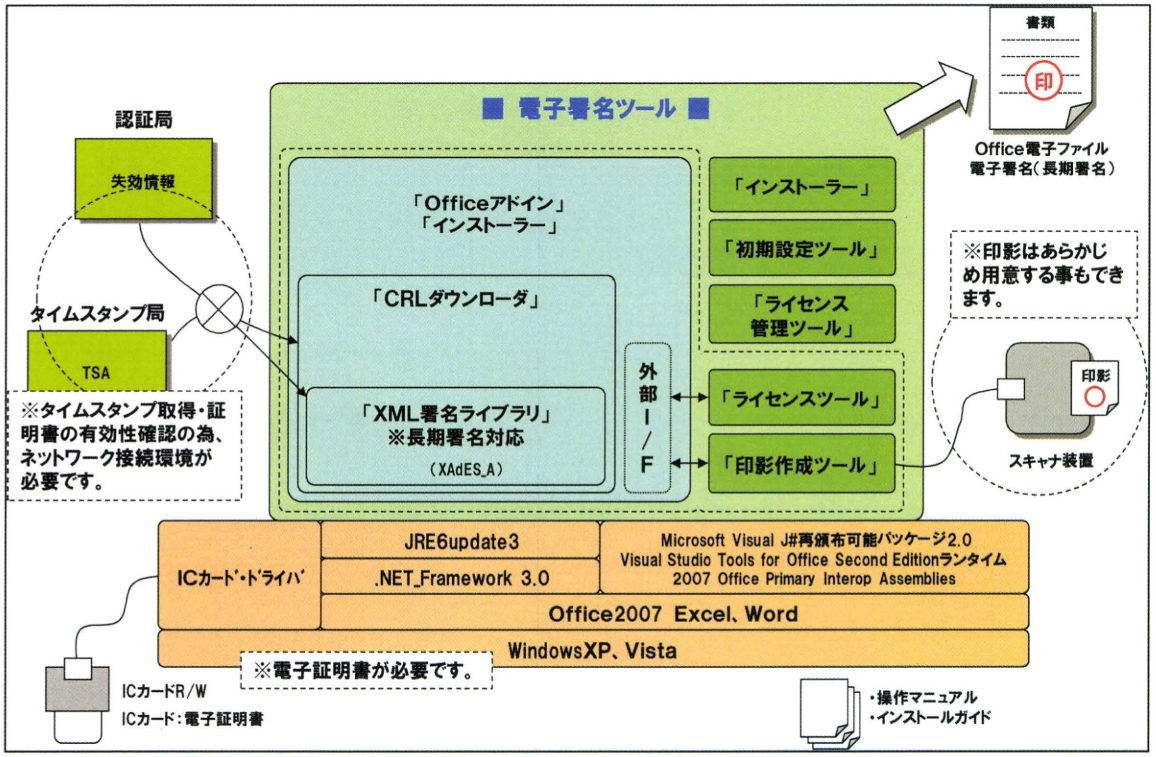
③署名値のダイジェスト（ハッシュ値）をタイムスタンプ局に送付し、タイムスタンプ署名値を求める。

④タイムスタンプ署名を含めた ES-T 署名形式を生成し PDF に署名データを格納して署名 PDF を出力する。

（５）Microsoft Office ＨＰＫＩ版　診断書作成システム　概説

恵寿総合病院の情報システムにおいては従来より Microsoft Office Excel により診断書を作成しており、本研究においては MicirosoftOffice2007 で作成した文書に IC カードを使用して電子署名及び印影の押印を実現する XML 署名 Office2007（Word・Excel）アドインプログラム適用した。適用した商品の概要は以下である。

【システム構成】



【機能】

① HPKI カードを使用したセキュアな電子署名

HPKI カードに格納された証明書・秘密鍵を使用して署名を行う仕様。署名者証明書が HPKI 証明書（証明書ポリシーID にて判別）であるかどうか判別し、HcRole に記載されている国家資格を表示する。

② 長期署名に対応した XML 署名

XAdES（XML Advanced Electronic Signatures の略）を利用した署名、タイムスタンプ、アーカイブタイムスタンプを組合せた XML 署名を行う事により電子署名の長期署名機能を有している。タイムスタンプに加えてアーカイブタイムスタンプを付加し署名延長を繰り返すことで長期署名が可能な XAdES_A の署名フォーマットの署名と検証が可能である。

③ Office2007（Word・Excel）と一体化

Office2007（Word・Excel）で編集中の文書を、PDF 変換等を行わず、また画面を切り替える事なくそのまま、署名する事が可能。

④ 動的印影作成

ハードディスクに格納した印影を文書内の任意の位置に表示することが可能。

⑤ 失効情報（CRL）の自動取得

署名文書の検証では、署名者証明書、タイムスタンプ証明書の失効検証のため、最新の失効情報（CRL）をインターネット経由で取得して検証している。

⑥ XAdES_A の対応

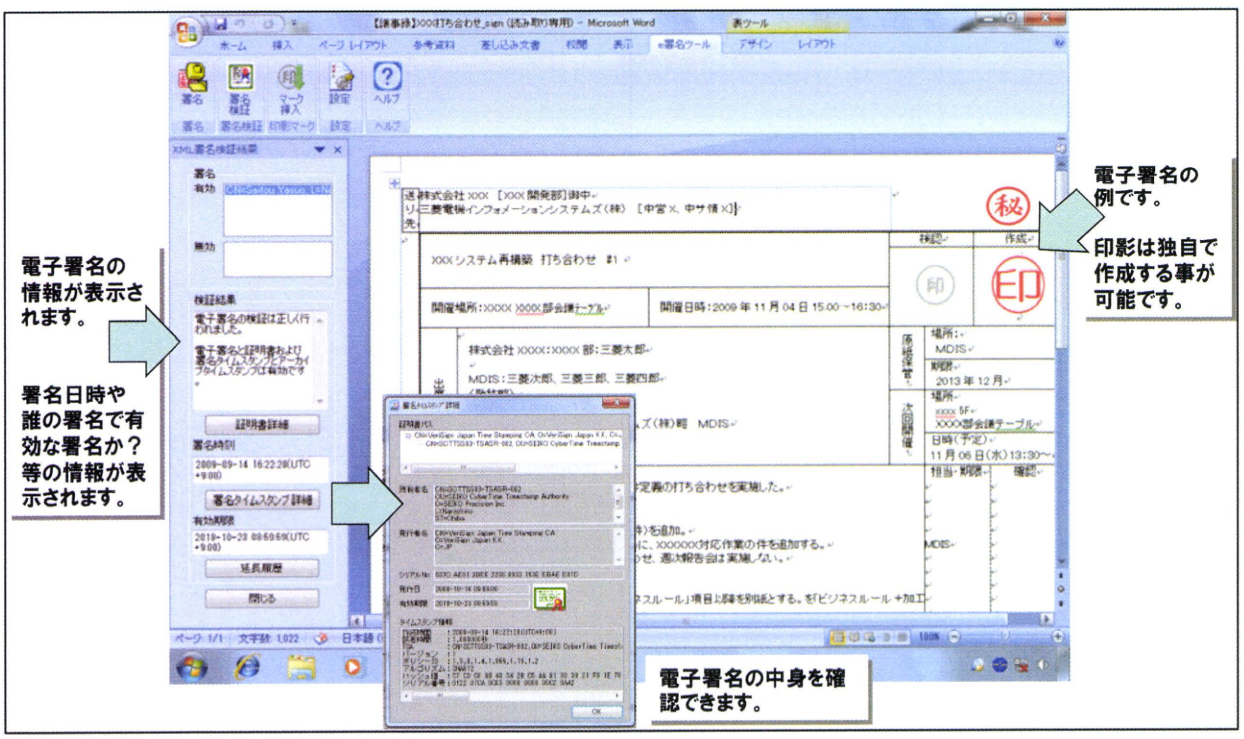
タイムスタンプとアーカイブタイムスタンプを検証し、タイムスタンプ情報と延長履歴情報を表示することが可能となっている。

⑦ ES 署名から ES-T を生成する機能への対応

タイムスタンプ付与作業について、複数の電子文書に効率的に実施できるソフトウェア環境の提供を目的として、ES 署名文書に自動的にタイムスタンプを付けて ES-T 署名にすることが可能。

＊ES-T フォーマット ：ES の署名部分に署名タイムスタンプ（T）を付加したもの

【操作画面】



６－４．診断書の外部送信アプリケーション概説（タイムスタンプ取得）

電子データで診断書を処理するためには、電子署名およびタイムスタンプが必要である。このうち、タイムスタンプの取得は病院外部にあるタイムスタンプサービスを利用する必要がある。しかし、セキュリティ対策として病院内システムに繋がる端末は外部接続が出来ない場合が多い。そのため、院外に直接接続できない病院に対し、電子署名の処理とタイムスタンプ取得の処理を別々に実施する事とする。電子署名は医師の HPKI カードにて署名を行なうため、院内システム上で実施するが、タイムスタンプの取得は外部接続可能な端末を専用に準備し、その端末にてタイムスタンプを取得する必要がある。生命保険会社側への送信に関しても、タイムスタンプ取得用の端末が外部接続可能であるため、その端末より送信できるように設計した。

また、タイムスタンプの取得にあたっては、アプリケーションで作成された診断書のうち、どの診断書が対象となるか識別するには操作する事務員がその診断書を実際に閲覧する事になるため、効率が悪く誤りを起こす可能性が高い。そのため、診断書を作成するアプリケーション側にて、診断書のファイル命名規則に従って作成してもらい、そのファイル名に従ってタイムスタンプ取得の判断を行なう一括タイムスタンプ取得機能を開発した。

診断書のファイル命名規則は以下のとおりとなっている(PDF の場合)。

・整理番号_医療機関名称_文書 ID_患者 ID.pdf （p47 による）

このうち、整理番号については LIAJ という文字列（生命保険会社）と３桁の保険会社番号の組み合わせで始まるものとしているため、タイムスタンプ取得時には、この整理番号から対象となる診断書を抽出する事とした。今回の実証事業では、送信対象となる生命保険会社は日本生命保険相互会社(保険会社番号：001)のみであるため、LIAJ001 で始まる診断書のみがタイムスタンプ取得の処理対象となる。それ以外の診断書は送信対象外となるため、タイムスタンプを取得せずファイルそのものを削除する。今回は日本生命保険相互会社のみであったが、他の保険会社でもその会社に対応するファイル名の接頭文字が決まっていれば対応可能である。

また、個人情報保護の観点より、今回の実証事業では実際の患者個人情報ではなくダミーの患者情報にて処理を行なうケースがある。そのため、ダミーの患者情報のみタイムスタンプ取得処理を行なう機能を追加し、ダミーの患者情報かの判断は、ダミーの患者用 ID を作成し、ファイル名にその患者 ID が含まれているかで判断した。

外部送信に関しては、ジャパンネット社のセキュアデータ交換サービスを利用する。セキュアデータ交換サービスでは、特別のアプリケーションを必要とはせず、ブラウザを利用して操作するものとした。

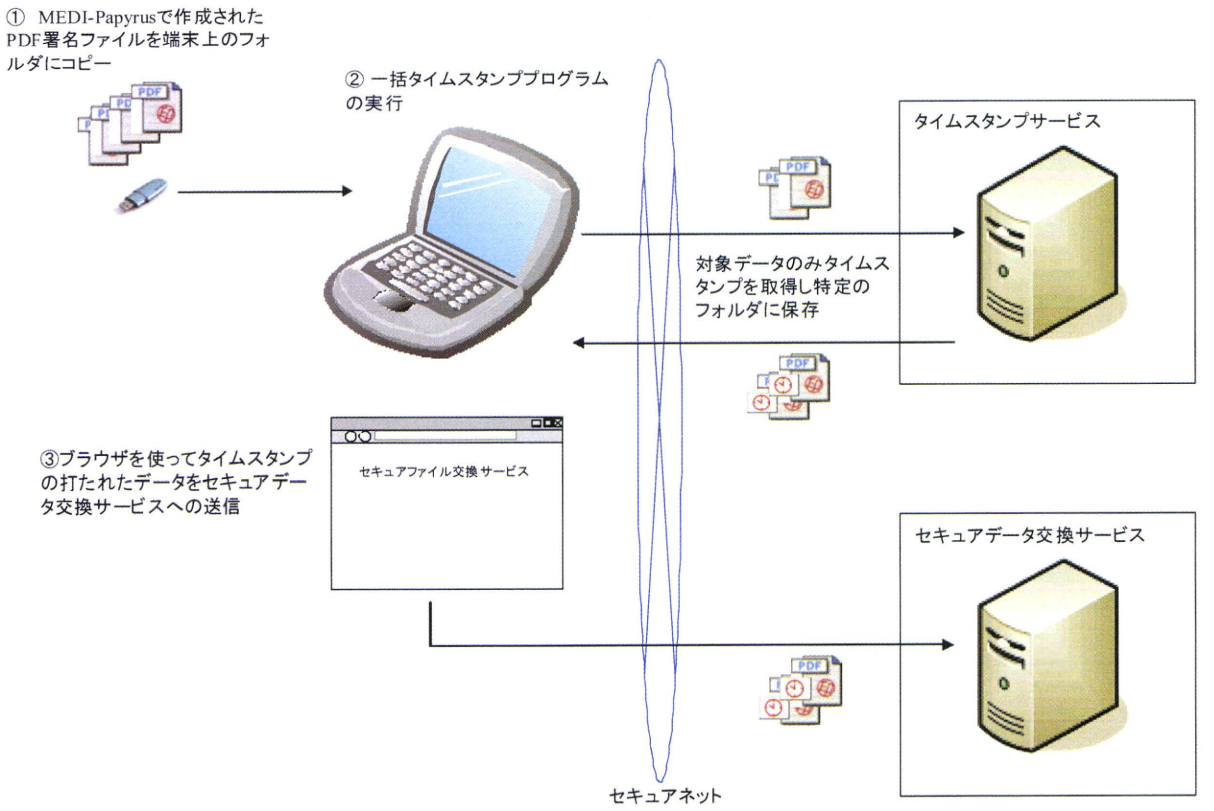
タイムスタンプの取得および外部送信の操作は以下のとおりである。

① 診断書作成アプリケーション等で作成された電子署名済みファイルを、USB モリリ等で外部送信端末の特定フォルダに移動を行なう。

② 一括タイムスタンプ取得プログラムを実行する。対象のファイルのみタイムスタンプを取得し、出力フォルダに保存される。対象外のファイルは削除される。

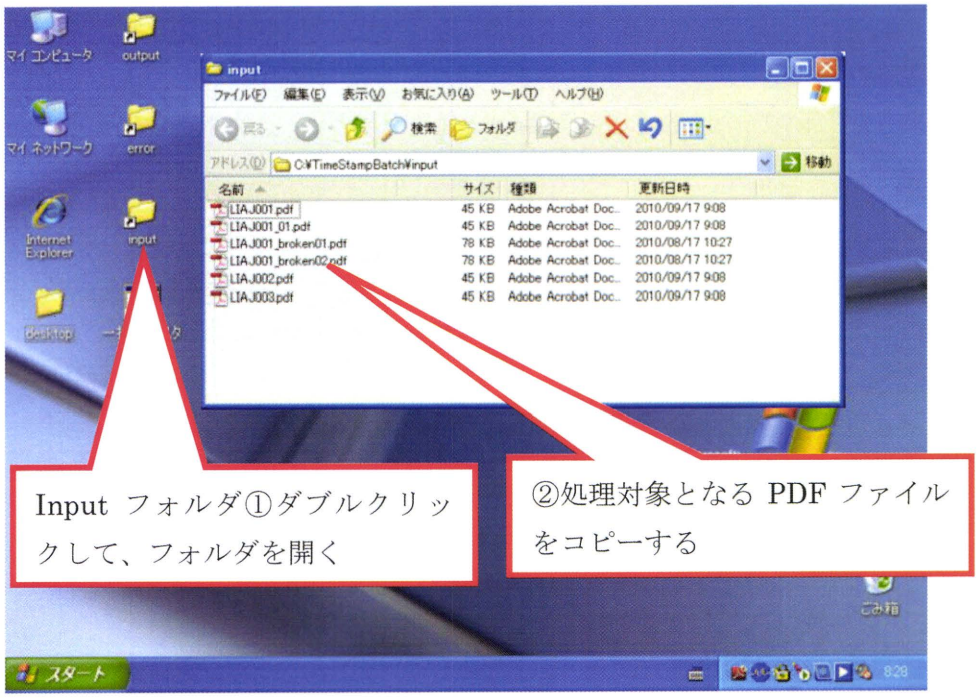
③ ブラウザを起動し、セキュア交換サービスに接続する。一括タイムスタンプ取得プログラムで作成されたファイルをセキュア交換サービスにアップロードする。

[システム構成図・運用図]

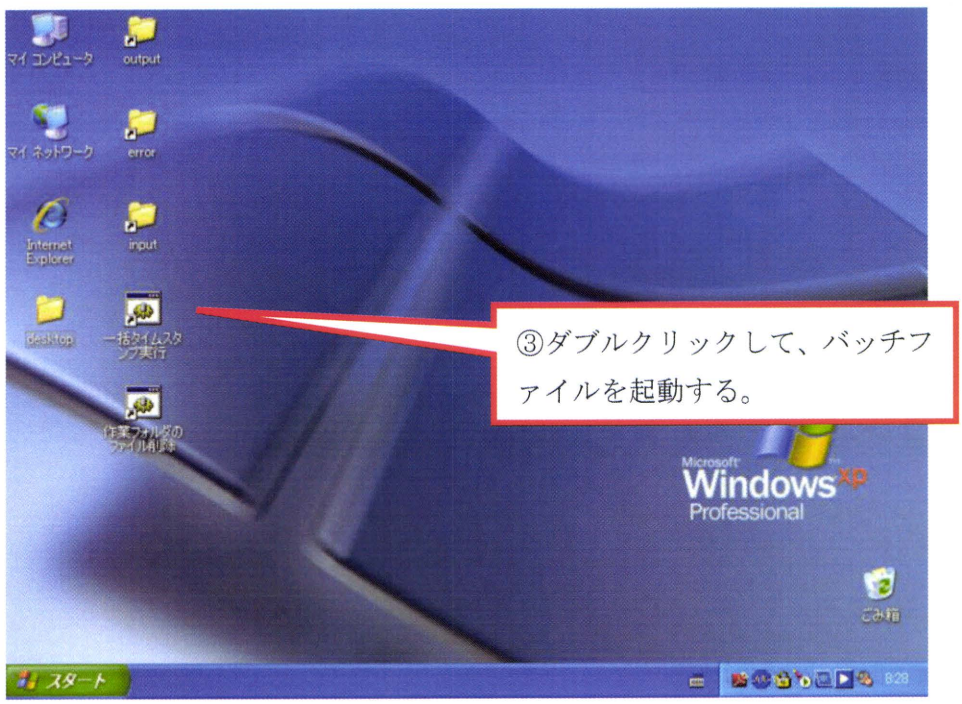


[操作画面]

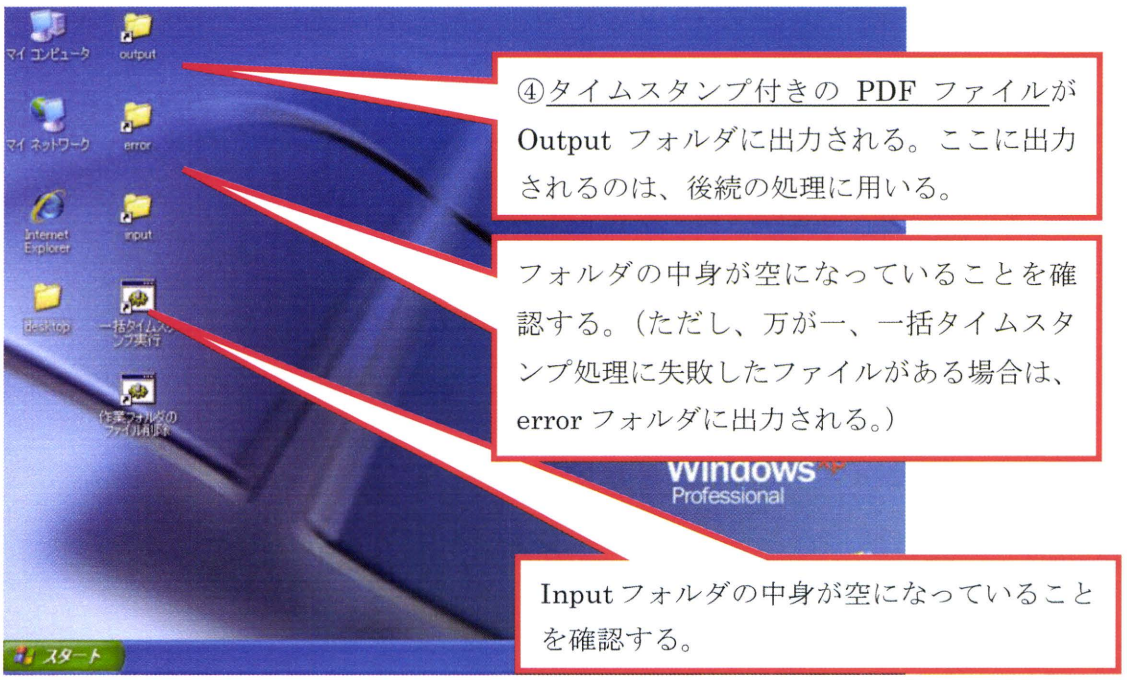
① 外部媒体またはネットワークを通して処理対象のファイルを Input フォルダにコピーする。



② バッチファイルを起動しタイムスタンプを取得する。

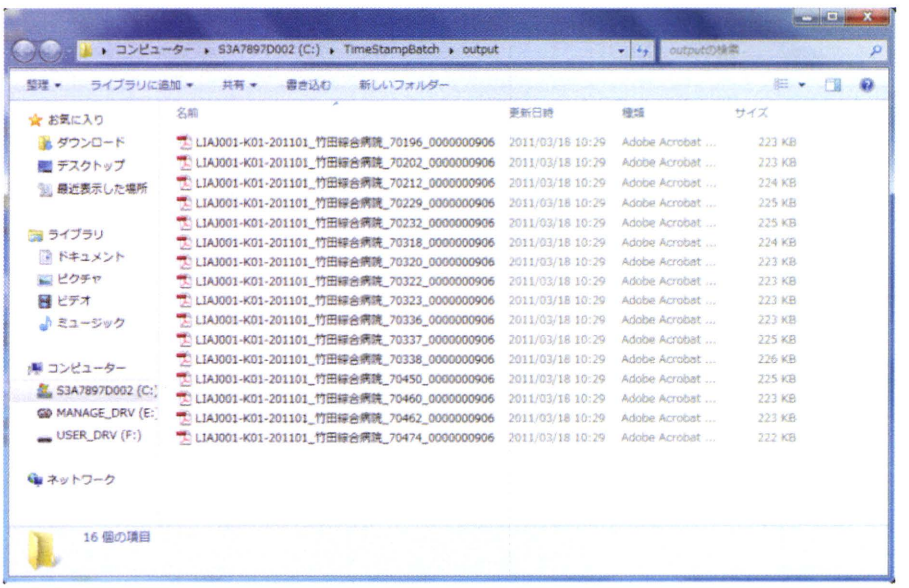


③ 取得したファイルは Output フォルダに出力され、当該フォルダ内のファイルは別途生命保険会社へ送信される。当該作業にあたり、エラーが検出されたファイルは Error フォルダに収納される。作業は、Input フォルダがからになったことを確認して終了する。

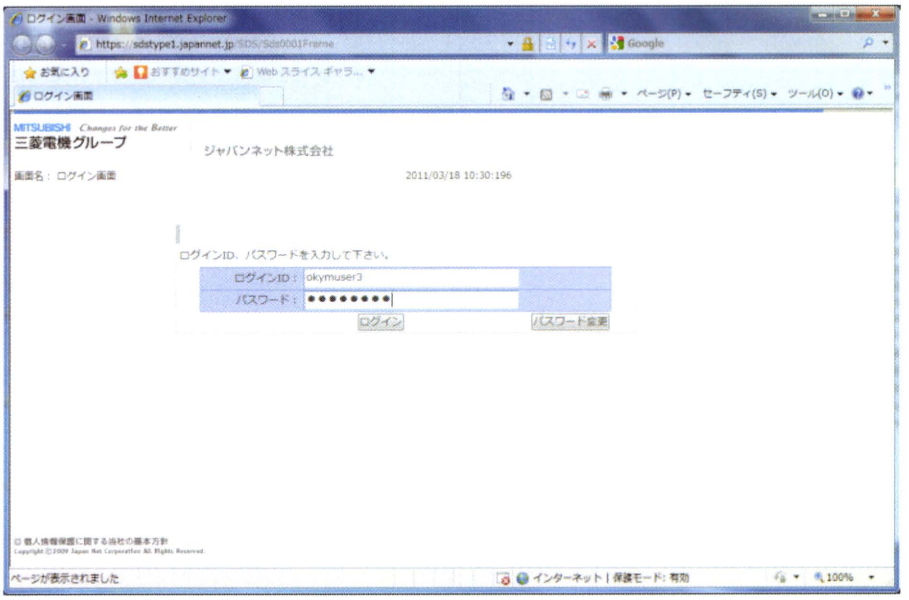


④ タイムスタンプ取得後、生命保険会社への送信

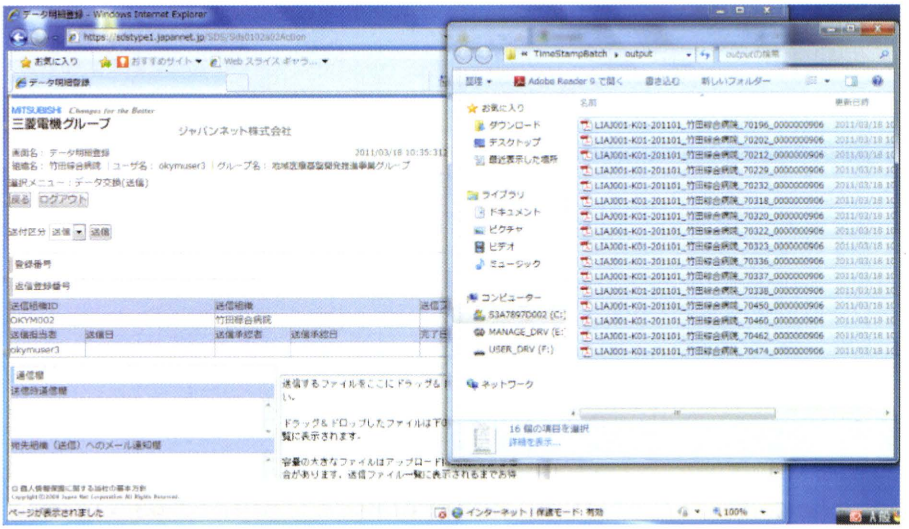
Output フォルダ



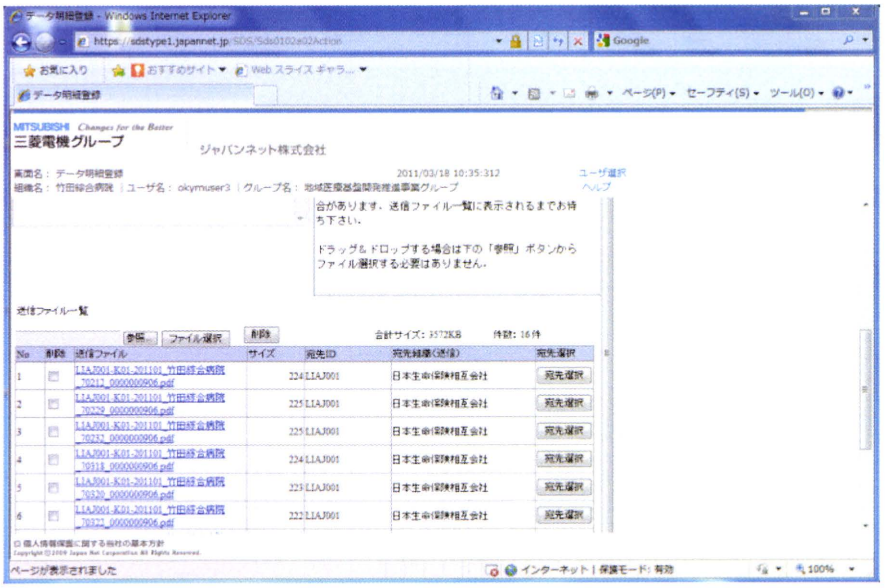
⑤ 送信アプリケーションの起動



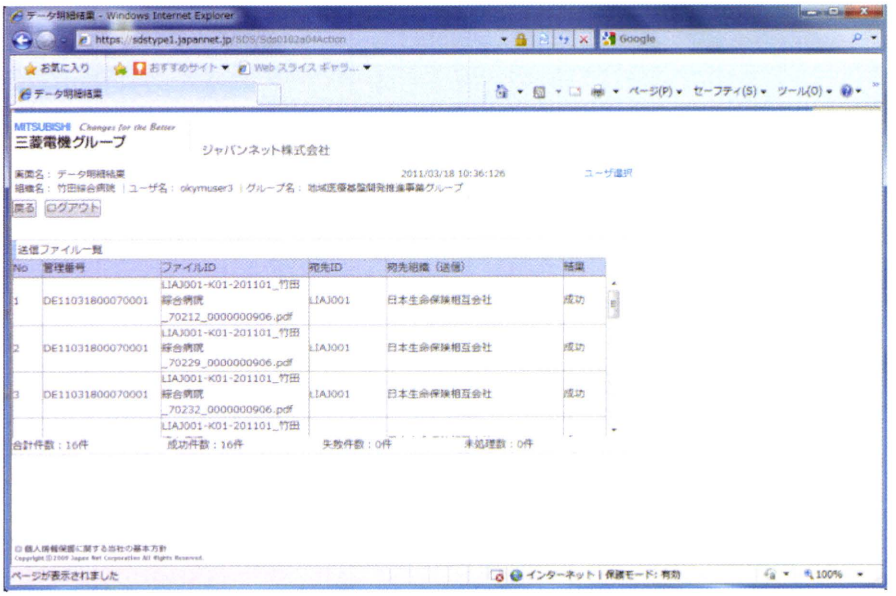
⑥ 送信データ明細登録（ファイルの選択）



⑦ 送信ファイル一覧（送信前）



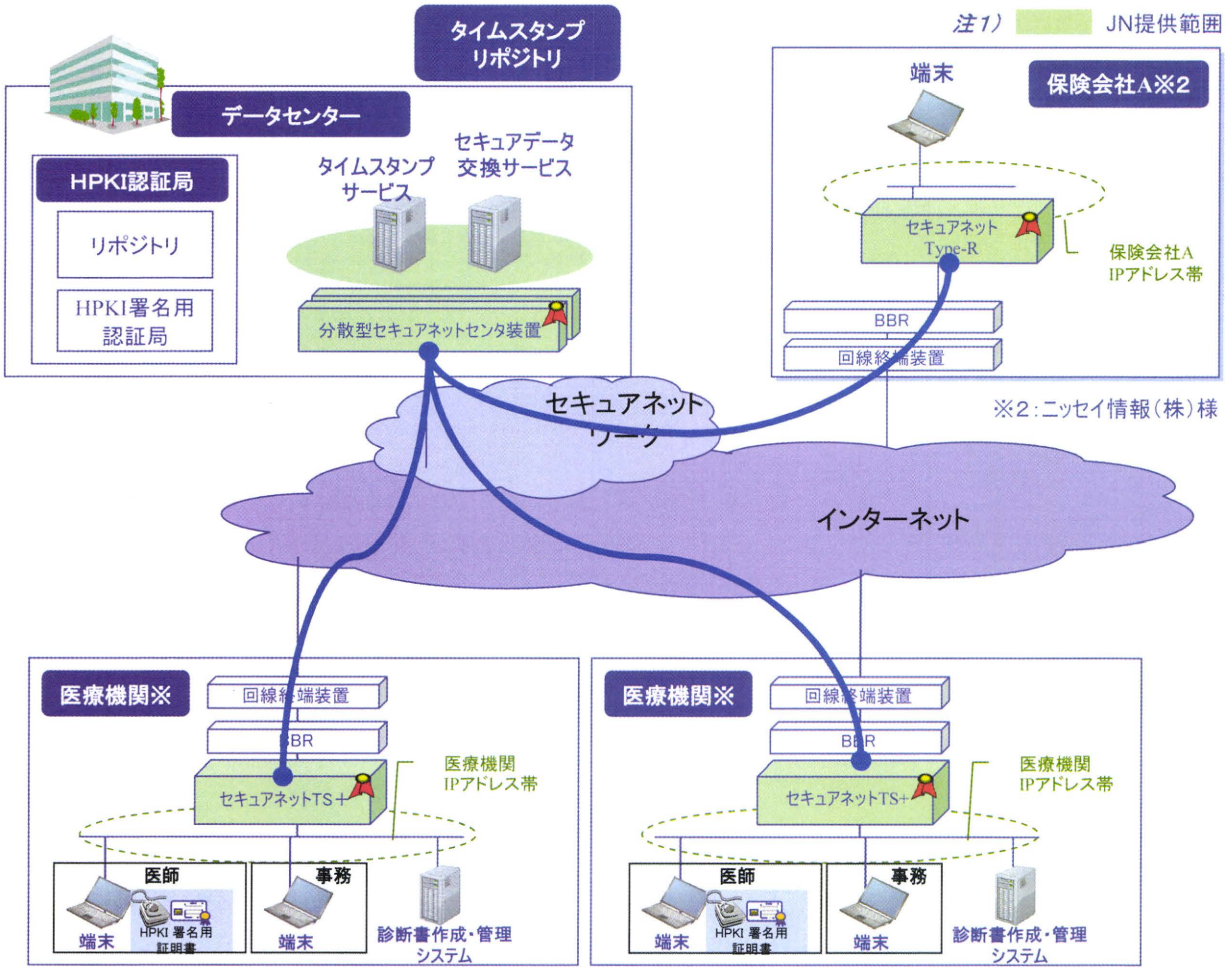
⑧ ファイル一覧（送信後）



６－５．セキュアネットワークとデータ交換サービス　概説

本実証事業においては、「医療システムの安全に関するガイドライン」に基づき、既に市場に提供されている安全対策を実施した、ネットワークおよびデータ交換サービスを採用した。

【論理ネットワーク構成全体像】



※：音羽病院様、麻生飯塚病院様、恵寿総合病院様、亀田総合病院様、竹田総合病院様

【利用したサービス】

1）セキュアネットワークサービス概要

セキュアネットワークサービスは、インターネットを活用して容易に医療関係のASPサービスと利用者である医療機関を安全に接続するために開発された。サービスは、「医療情報システムの安全に関するガイドライン」（最新版）で規定されているネットワークへの安全対策を実施しガイドラインに準拠している。

ＩＰｓｅｃ＋ＩＫＥによる暗号化を行い情報の漏洩を防止するとともに、ＰＫＩを用いた電子証明書で認証を行い不正アクセスを防止する。導入にあたってはセキュア

ネットワークサービスを利用するために必要とされるネットワーク機器が提供される。

特徴として、

① 安全なネットワークサービスの提供

・IPSec+IKE による通信の暗号化(盗聴防止)

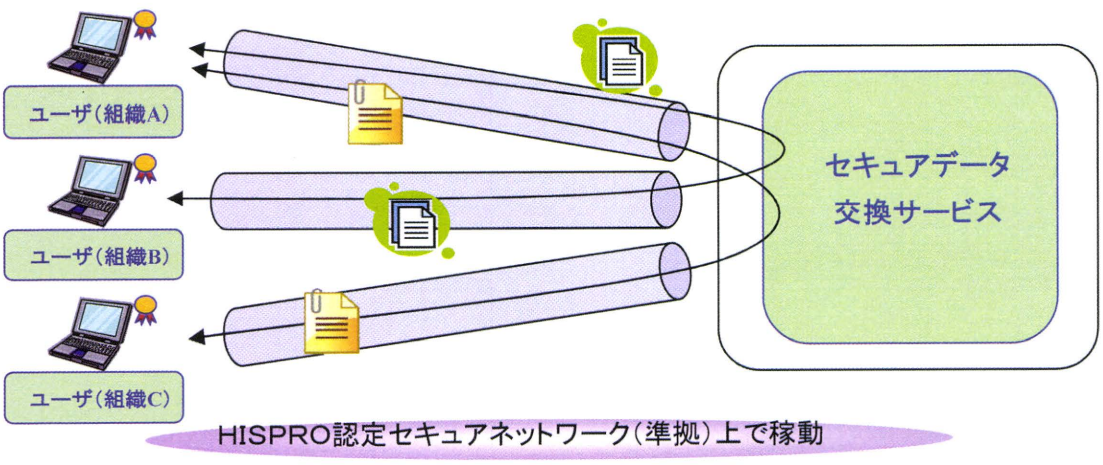
・電子証明書によるユーザ認証(なりすまし防止)

② 高度な情報セキュリティを求められる医療 ASP サービスと医療機関(病院、診療所、保険薬局など)との情報交換をオンラインにて安全に実現します。

③ セキュアネットワークサービスを利用するにあたって必要なインターネット環境は、インターネットプロバイダを選ばない“プロバイダフリー”タイプである。

2）セキュアデータ交換サービス（SDS）概要

セキュアデータ交換サービスとはセキュアなネットワーク上で、医療文書等を安全に送受するデータ交換サービス。予め組織間でデータ交換相手を登録（グループ化）し、グループ内で安全なデータ交換を行なうことが可能なサービスである。



特徴として

① セキュアなネットワーク基盤

ネットワーク基盤は厚生労働省「医療情報システムの安全管理に関するガイドライン」でインターネット利用時の接続方法として示されている IPSec+IKE 方式のインターネット VPN で、HISPRO（保健医療福祉情報安全管理適合性評価協会）の認定を受けたセキュアネットワークサービスと同一のネットワークを利用可能である。また、インターネットのようなオープンネットワークでも「盗聴」、「改ざん」、「なりすまし」対策がなされ、安心・安全に利用が可能である。

② セキュアな組織認証

組織認証には電子証明書を利用した SSL クライアント認証にて組織を特定し、なりすましを防止することが可能である。

③ セキュアなデータ交換

データ交換相手を予め登録（グループ化）しておくことで、誤送信を防止することが可能。また、組織単位で送受信の設定が可能であり、例えば特定の組織に対しては送信のみに限定するといった設定が可能。なお、送信宛先指定はファイル名に予め決定した宛先 ID を付与することで、自動判別することも可能である。

④ 大容量データの送受信

1 度の送受信操作で複数のファイルが扱うことができ、ファイル合計で 10MB（1 ファイルのサイズの上限値は 5MB）までのデータの送受信が可能である。

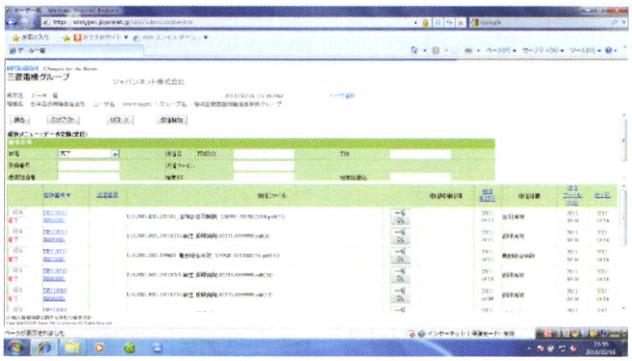
⑤ 送受信データのステータス管理

送受信したデータのステータスを WEB 画面上で確認することが可能であり、送受信した日時を特定することができる。

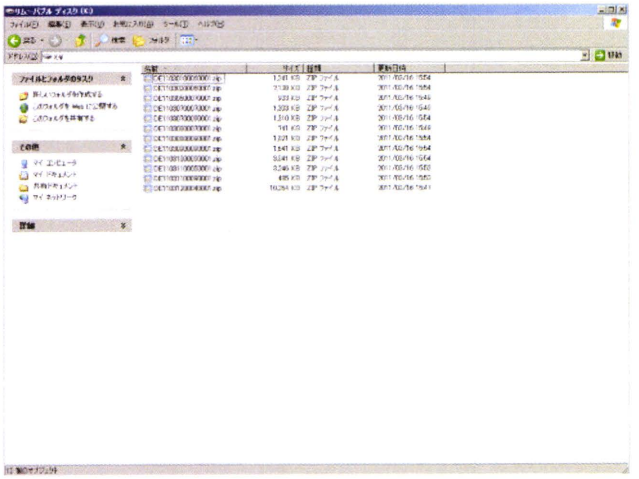
【生命保険会社で受信】

セキュアネットワークサービス、セキュアデータ交換サービスを経由して受信した、生命保険会社側で受信可能となっているシステム画面は以下の通りである。尚、本実証研究中は、問題は発生していない。

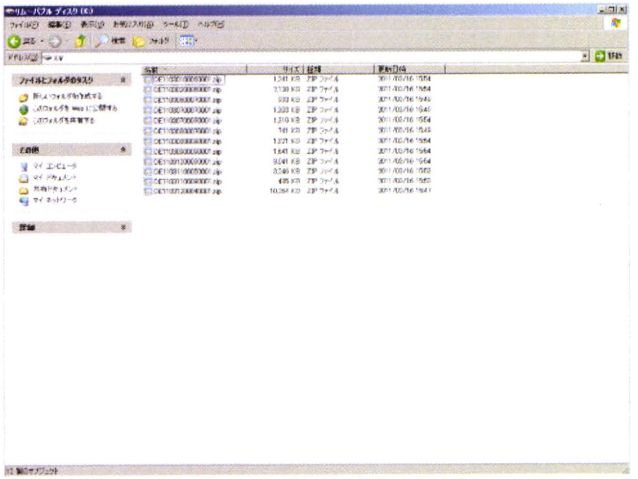
① 未受信一覧



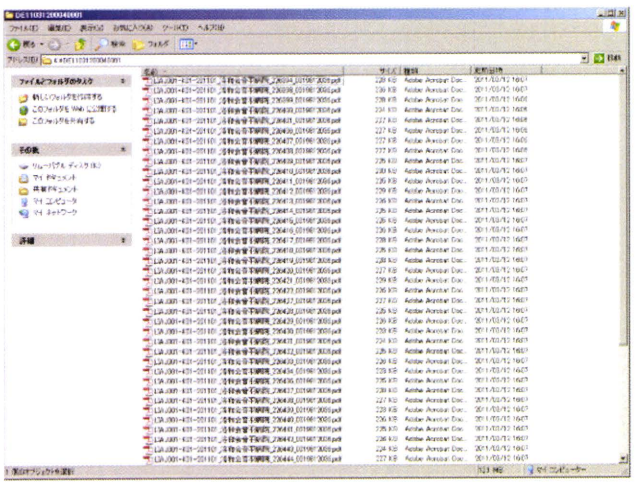
② 受信完了



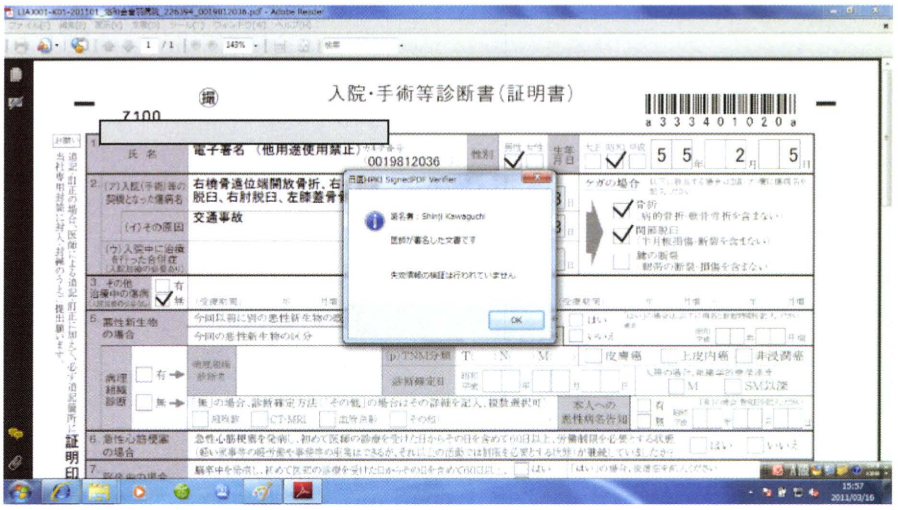
③ ダウンロードデータ



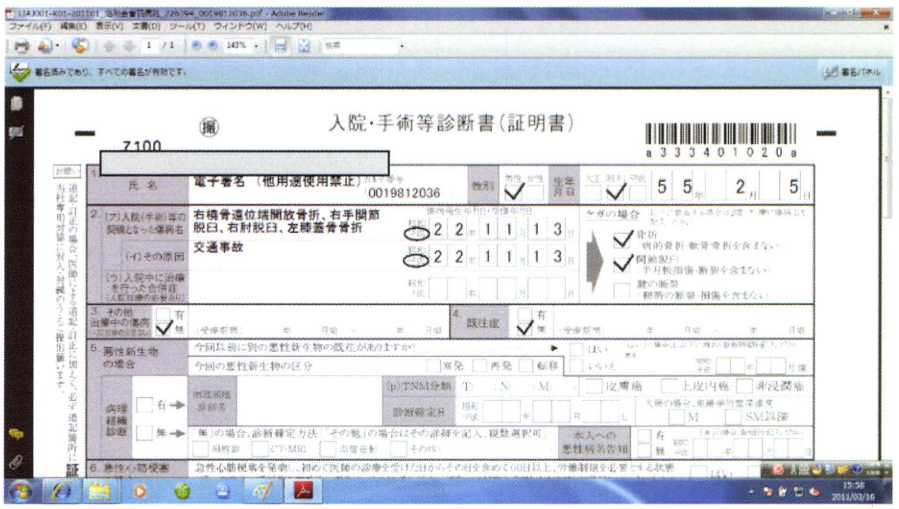
④ ダウンロード内容



⑤ 受信された診断書の内容



（署名認証確認）



（診断書画面）

7．実証事業のまとめと２３年度の継続研究予定

（1）まとめ

本年度は、実証研究において協力いただいた５病院にて、

① HPKI 署名が可能な情報システムを開発導入した。

② 導入した情報システムを用いて、HPKI 署名の生命保険会社向け診断書を作成しセキュアな環境にて電子送信を行う研究を行った。

③ HPKI 導入にあたり、従来の運用フローと新規に設計した HPKI 用運用フローを比較し、普及向けて現場における課題などの抽出を行った。

④ 今後医療情報（診断書）の電子化などにより期待される効果を検討、患者側の反応をアンケートにより確認をした。

結果として、

① 設計した運用は大きな問題なく実施可能であった。

② 診断書の電子化については、医療側・患者側いずれも積極推進するべき、あるいは将来の動向として受け入れる用意があるとの確認を行うことができた。

③ 診断書の送信にあたって、今回構築したネットワーク・システムでは問題が発生しなかった。

一方、当初の予定であった生命保険会社での運用を含めた業務の効率化について検証を行うまでには至らなかった。２３年度に実施すべき課題である。

また、今年度の研究において

① 現場（病院）の負担が大変大きいことがあらためて確認された。

・システム構築導入に対する対応

・個人情報を取り扱うための対応

・研究参加者に対する広報、教育

② 運用に関する設計の課題が確認された。

概念的（紙上）な運用設計上の問題はなかったが、実際の運用にあたっては、例えば利用できる端末の制限などにより、研究結果にバイアスが掛かる可能性が示唆された。

③ HPKI カード発行に関する課題が確認された。

（2）２３年度の継続研究予定

前記２２年度の研究結果を踏まえ、２３年度は以下の内容で研究を継続する予定である。

① 生命保険会社における電子受信と保険金支払いまでの運用を検証する。
参加する生命保険会社についても、複数社に打診を行い進める。

② ２２年度協力いただいた各病院にて運用を継続する。

・本年度は業務負荷の問題提議から、診療科を絞るなどして運用の範囲を制限した。広くデータを取得するため運用範囲の拡大を検討、実施する。

・生命保険会社向け診断書に絞って実施したが、その他の書類に対して実施可能かを研究する

・電子署名、送信の安全性について理解を深めてもらう手段（広報手段）の研究を行う。

③ HPKI カード発行に関する提案を整理する。

④ 新規の研究参加病院

２２年度の研究成果を踏まえ、新規研究参加病院に適用する。

参加病院としては、岡山大学病院など大規模な公的病院も視野にいれる。また、それにともない今回参加しなかったベンダによる診断書作成アプリケーションにも適用する。

本実証研究の、統括、協力者

本研究の統括、および協力いただいた各病院の担当を記載する

全体統括	岡山大学　医療情報学	教授	太田　吉夫
	岡山大学　病院経営戦略支援部	教授	合地　明
協力病院担当	財団法人　竹田綜合病院 情報システム課ソフトウェア開発係	係長	須藤　浩也
	医療法人　鉄蕉会　亀田総合病院 経営管理本部　カスタマーリレーション部	部長代理	山田　剛士
	社会医療法人財団　董仙会　恵寿総合病院 本部事務局　総務部　企画開発課	課長	直江　幸範
	医療法人社団　洛和会　音羽病院 洛和会ヘルスケアシステム	副本部長	児島　純司
	株式会社　麻生　飯塚病院 情報システム室	室長	久川　広則

HPKI のアドバイザとして

日本医師会　総合政策研究機構　主任研究員　矢野　一博

参考資料

1．日医総研　ＨＰＫＩワークショップ　講演資料

実証事業にあたり日医総研より専門家を招聘してワークショップを開催

（日本医師会総合政策機構　矢野一博様　ご提供資料を掲載する）