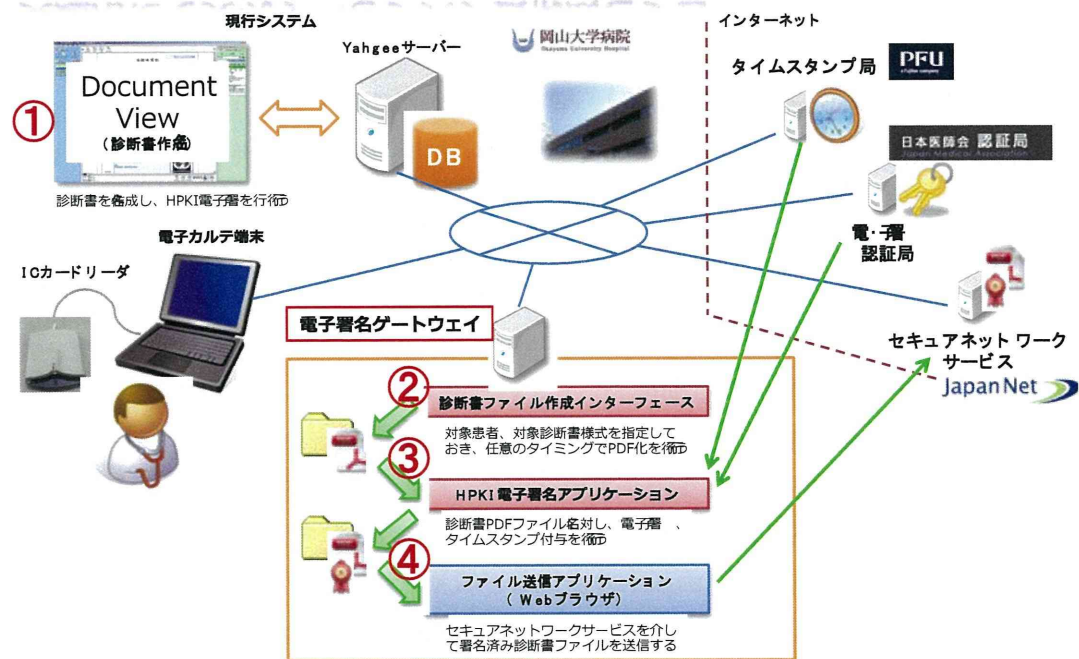


4. 課題と考察

- 一方、実運用にて実現すべき環境としては、診断書作成後、直ちに作成者が電子署名を行う、もしくは代行入力者が承認者である医師に署名依頼を出し、速やかに電子署名を行う、という事を、日常の診療業務上でストレス無く行う事ができなくてはならない。これを実現するには、まず、電子カルテ端末そのもので、電子署名を行う機能を実装する必要がある。実現すべきシステム構成及びフローを図8に示す。
- 今回、既存の診断書アプリケーション及び実証において開発した電子署名アプリケーションにて機能自体は満たせるが、上記の実運用を行う上では、いくつかの課題を解決しなければならない事がわかった。

HPKI 実証事業対応システム概要

実運用にて実現すべきシステム構成とフロー



11/9/26

4

図8 実現すべきシステム構成及びフロー

4.1 HPKI の電子カルテへの組み込み

- ・ 医師の診断書作成もしくは承認において、HPKI電子署名を通常診療業務の一連のワークフローに取込む必要がある。これには、電子カルテ端末に対するHPKIカードリーダーの接続とドライバ等関連ファイルのインストールやセットアップが必要であり、診断書システムのみでは対応できない課題である。
- ・ 実際に、電子カルテ端末への展開を考えた場合、そのセットアップ作業や費用をどのような役割分担で行うかも、重要な課題であると考ええる。
- ・ さらには、診断書の署名だけにHPKIを用いるだけでは、周知徹底の問題や運用上のストレスも想定されるため、電子カルテへのログインそのものをHPKIカードにするなど、抜本的なHIS全体及び運用への取込みが必要であると考ええる。

4.2 HPKI 電子署名、タイムスタンプ処理の非同期化

- ・ 現在のHPKIの仕様では、署名時にPINコードの入力が必須となっている。まとめて複数の診断書を承認するには、都度同じPINコード入力を要求する仕組みでは、医師への負担が高いと考える。例えば、電子カルテへのログイン時に使用したパスワードでそのまままとめて電子署名ができるといった仕組みが必要である。
- ・ 加えて承認処理には、タイムスタンプの取得も必要であり、現状のフローでは1通1通の処理に時間がかかり過ぎると思われる。このようなシーケンシャルな同期処理では無理があると思われるので、電子署名に必要な情報をまとめておき、事後にまとめてバッチ処理（非同期処理）ができるような仕組みが必要と考える。

4.3 署名から送信までの自動化

- ・ 承認処理が医師の診療業務ワークフローの中で速やかに行われる事も重要だが、その後の送信までの処理も、できる限り手順を少なく行える事が理想的である。今回の実証環境にて確認した機能上では、HPKIのPINコード入力、セキュアネット利用時のVPN接続時のPINコード入力や、画面上の操作など煩雑な面がいくつか見られた。上記の非同期化に加え、自動化を進める事で、運用に耐え得る環境が実現できると考えられる。

4.4 オンライン提出におけるセキュアネットワーク

- ・ 岡山大学病院では、院内LANからファイアウォールを介してインターネットに接続できるようなネットワークとなっており、実際に診断書作成から電子署名、タイムスタンプまでは、院内LAN環境下にて動作を確認する事ができた。
- ・ セキュアネットについても同環境にて、USBトークンによる接続（専用線やルータ等ハードウェアを用いないソフトウェア的な接続）を試みたが、接続が確立できなかった。

- ・セキュアネットが接続できなかった理由としては、院内LANのファイアウォールの設定が影響していると思われる。試しに別ネットワーク(学内LAN)を経由して接続した所、問題無く接続でき、診断書の送信を完了する事ができた。
- ・実際にセキュアネットにて診断書送信処理を行った際、操作手順の煩雑さ、レスポンススピード等、実運用において疑問が残る所があった。設定の確認や十分な検証ができていないが、改善の余地はあると思われる。

4.5 診断書電子化メリットの提示

- ・上記の諸々の課題が解決したとしても、実際の運用を想定すると、医師や代行入力者に新たな負担がかかる事は必至である。納得感を持って協力を得るためには、システム化による明らかなメリットの提示が必要と思われる。電子化のメリットという側面で考えれば、せっかく項目毎の電子データとして診断書が作成されているので、項目単位で保険会社に送信され、保険会社側の処理も自動化され、保険の支払い処理が早くなる、もしくは簡便になる等の、保険支払い全体に関わるような改善が必要と思われる。

5. 結論

- ・HPKI、診断書システム、セキュアネットを用いて診断書作成から電子署名、オンライン送信までを実証した。
- ・機能の確認を行う事ができたが、実運用に展開するには、HPKIの仕様の改善や電子カルテシステムそのものへの取込み、医師や入力者の納得のいく理由付け等、基本的かつ広範囲に対応すべき課題がある事がわかった。
- ・具体的には、非同期でのHPKI電子署名や、ファイル送信までを含めたシステムの自動化、診断書の電子データ交換化による根本的なメリットの提示等が必要であると考える。

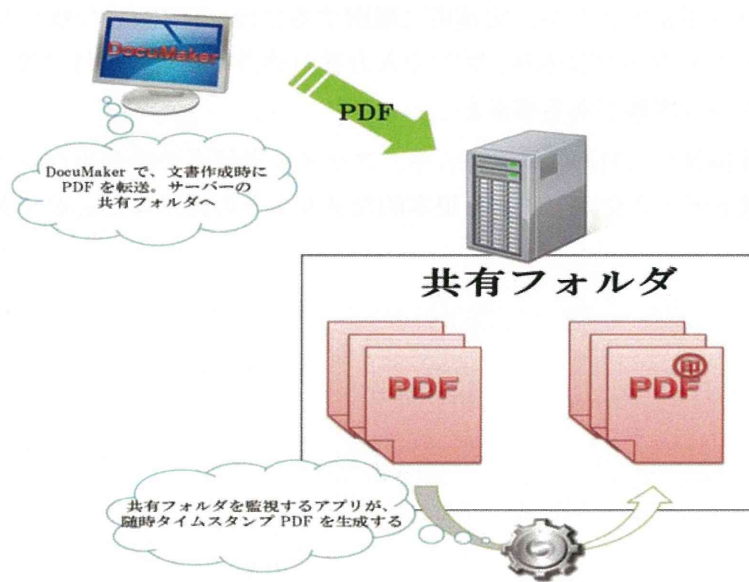
3. 株式会社ピーエスシー

院内ドキュメント作成管理システム DocuMaker HPKI 版 概説

「DocuMaker (HPKI版)」とは、院内ドキュメント作成管理システムに三菱インフォメーションシステムズ社製の電子署名ライブラリを組み込んだものである。実証事業に際して、職員の負荷軽減の為、患者属性情報及び診療情報等のHIS連携を行い、PDF出力機能及びファイル名自動付与機能の組み込みも行った。

本実証事業においてDocuMaker (HPKI版) を利用する医療機関は、既にDocuMakerを導入利用している医療法人財団健和会柳原リハビリテーション病院、実証実験にあわせてDocuMakerを導入する医療法人蒼龍会井上病院である。実証実験にあたっては、両病院共に本系を改造することによる運用面への影響を考慮し、実証実験端末を限定して、本系とは別にDocuMaker (HPKI版) を院内環境に構築を行った。また、DocuMaker (HPKI版) で作成したデータは実証事業終了後も継続して利用できるようにするため、本系のデータベースは共用とし、データの更新・参照を可能とするよう設定した。

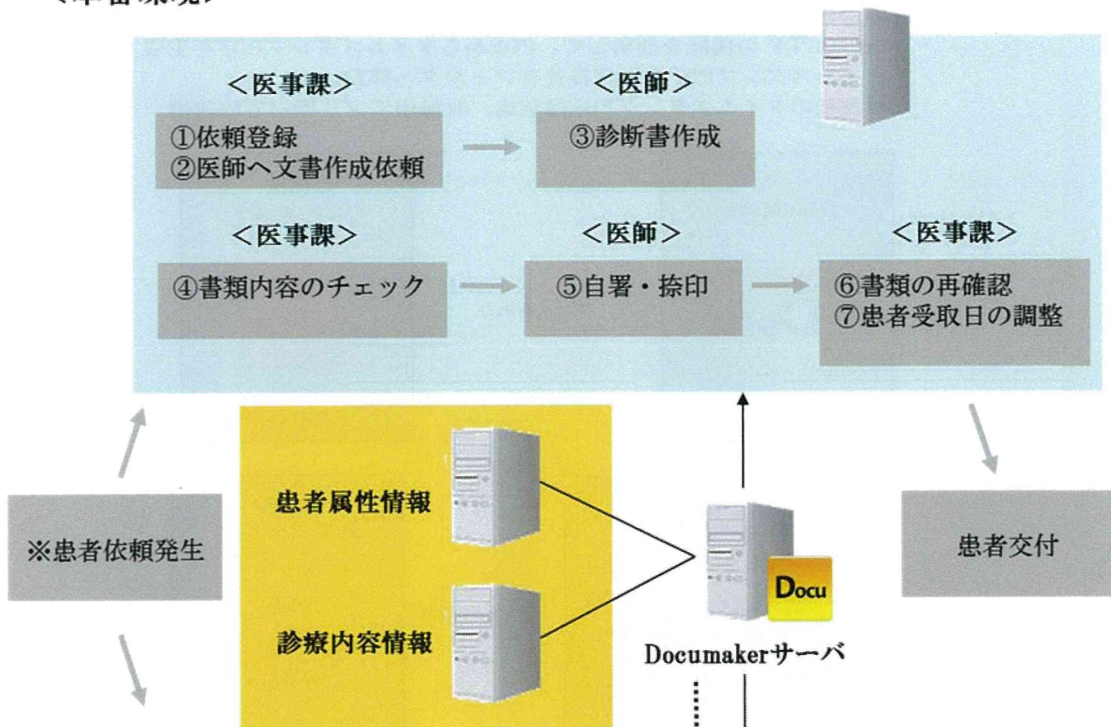
タイムスタンプ機能概要



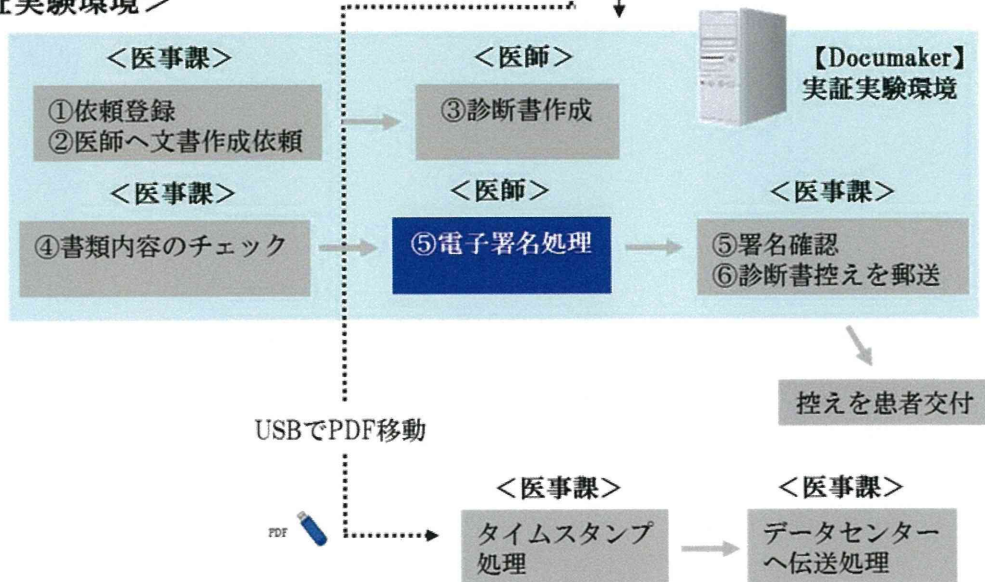
タイムスタンプ処理には、三菱電機グループ 株式会社テクノウェア社のSignedPDF Client - Advanced Edition- を使用しています。
SignedPDF は三菱電機インフォメーションシステムズ株式会社の商標です。

【システム概要】

<本番環境>

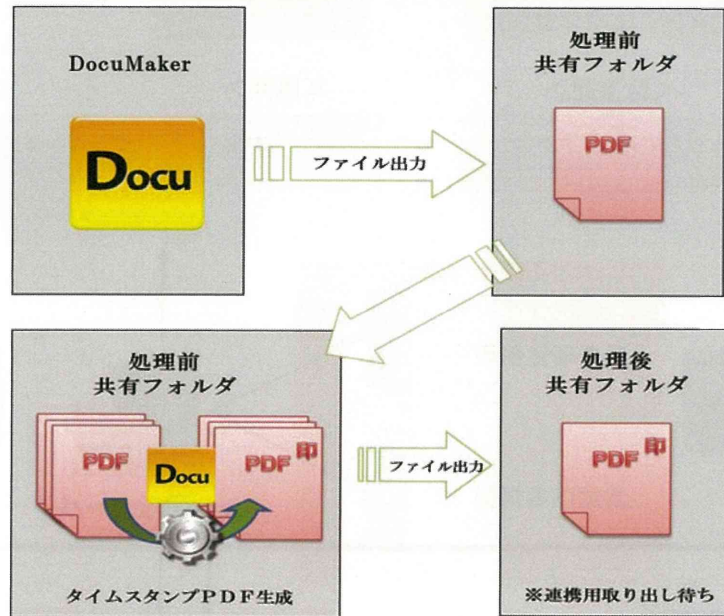


<実証実験環境>



ファイル編集仕様概要

- ・ DocuMaker から処理前共有フォルダへ転送されるPDFを常時監視
- ・ 転送されたPDFを随時作業フォルダへ移動
- ・ SignedPDF の機能を使用して、PDFからタイムスタンプPDFを生成
- ・ タイムスタンプPDFを処理後共有フォルダへ移動
- ・ 処理後のタイムスタンプPDFは別途、取得用アプリ等で外部連携



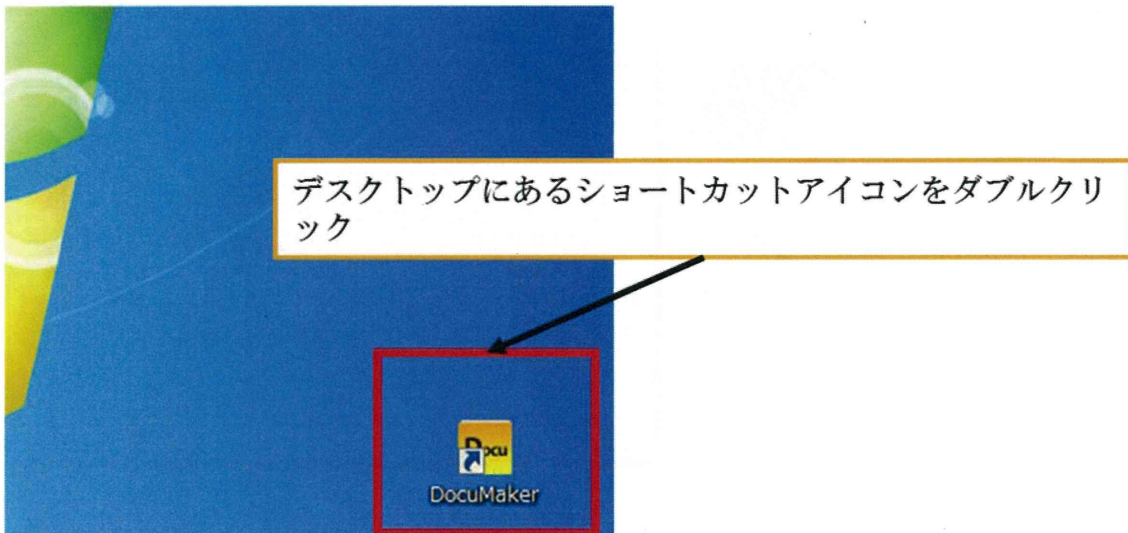
1. DocuMaker (HPKI版) 追加機能

< 1 > 電子署名処理

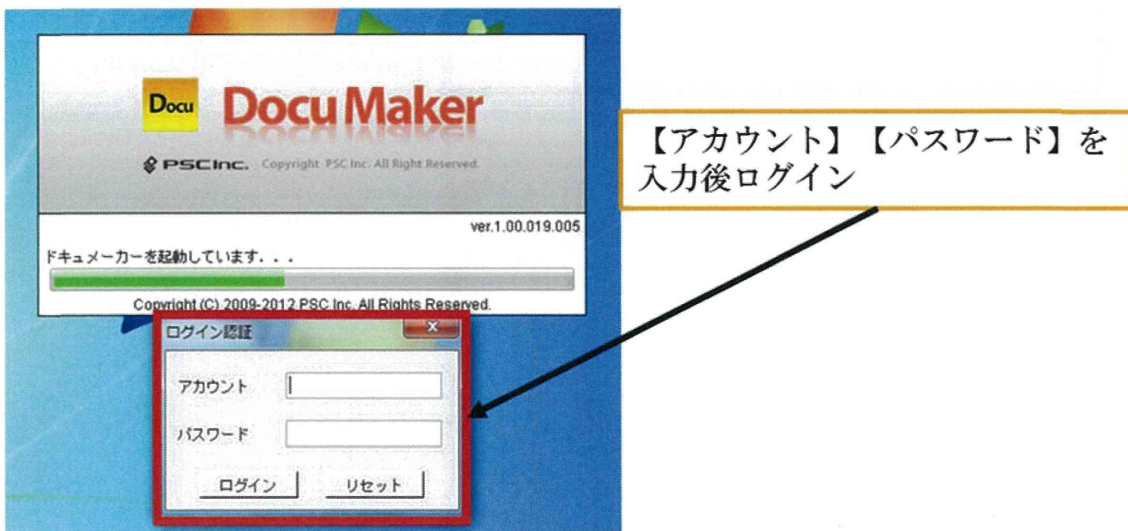
診断書登録後の印刷処理時に紙媒体を印刷すると共に電子署名を行えるようにした。

※システム操作方法

① Documaker (HPKI版) 起動方法



② Documaker (HPKI版) へのログイン方法



③書類検索方法

【過去一覧】を押下

過去書類選択画面

患者番号	患者氏名	診療科	書類名	作成者	作成日時
00004	テスト 患者4 (テスト カンジ)		ペーチェット	院内ドキュ. 管理者	2011/01/3 13:23:02
00004	テスト 患者4 (テスト カンジ)		黄色封筒	院内ドキュ. 管理者	2011/1/1 20:59:01
00004	テスト 患者4 (テスト カンジ)		看護データ	院内ドキュ. 管理者	2011/1/7 19:07:02

書類を選択してください

④書類の選択

患者番号	患者氏名	プロジェクト	書類名	書類属性	作成者	書類作成日時
00004	テスト 患者4 (テスト カンジ)		ペーチェット	院内ドキュ.	管理者	2011/01/3 13:23:02
00004	テスト 患者4 (テスト カンジ)		黄色封筒	院内ドキュ.	管理者	2011/1/1 20:59:01
00004	テスト 患者4 (テスト カンジ)		看護データ	院内ドキュ.	管理者	2011/1/7 19:07:02
00004	テスト 患者4 (テスト カンジ)		死亡証明書	院内ドキュ.	管理者	2012/1/20 14:41:32

7100 裏面あり 死亡証明書

(届出先) 日本生命保険相互会社

氏名 テスト 患者4 昭和 48 年 1 月 25 日

死亡年月日 年 月 日 時 分 年 月 日

死亡時刻 年 月 日 時 分

死亡の理由 1 病院 2 診療所 3 老人保健施設 4 助産所 5 老人ホーム 6 自宅 7 その他

死亡の場所 1 病院 2 診療所 3 老人保健施設 4 助産所 5 老人ホーム 6 自宅 7 その他

死亡の種別 1 自然死 2 病死 3 事故死 4 その他

備考 1-3の項目の名称

備考 4-7の項目の名称

備考 8-9の項目の名称

備考 10の項目の名称

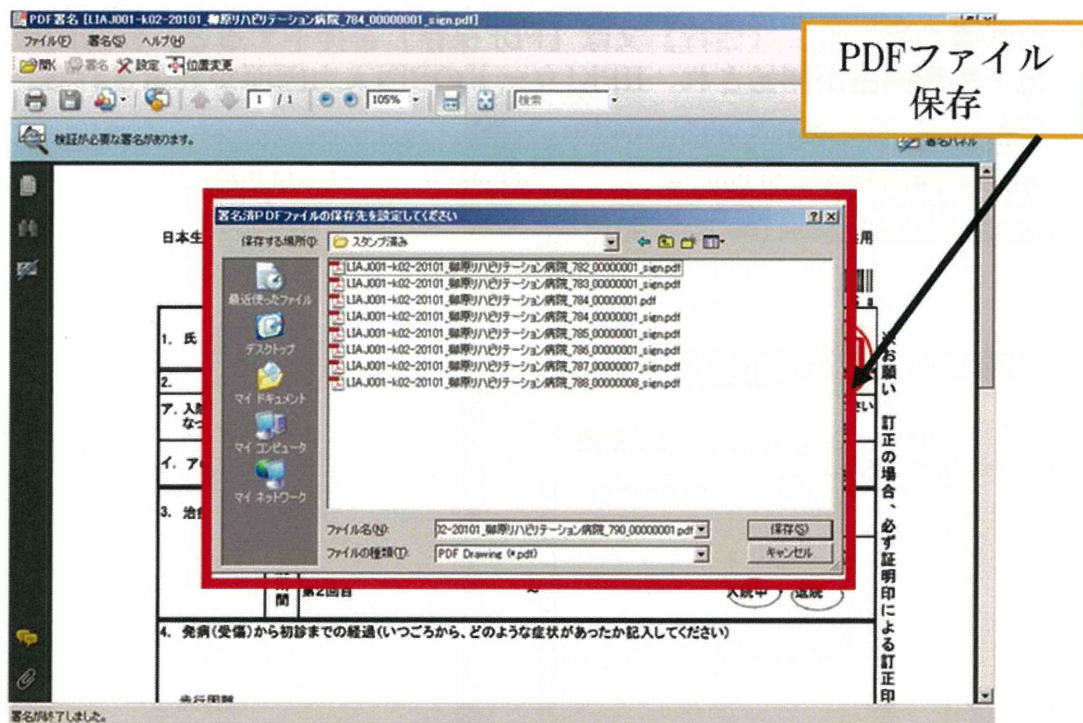
PDF保存 発行 修正・記録

⑤電子署名の実行方法

診断書を選択後、【発行】又は【PDF保存】を押下すると、自動的に電子処理画面が開始され、HPKIカードのPIN入力画面が表示される。

⑥PINの入力

⑦署名済みPDFファイル保存先外部出力フォルダの指定



<2>電子署名済みPDFの外部フォルダへの出力処理
電子署名済みPDFをデータ伝送用の格納フォルダへ出力可能であり、当実証実験にあたっては下記出力フォルダとする。

電子署名付きPDFの出力フォルダ

C:\¥SignedPDF¥スタンプ済み

<3>データ伝送用PDFファイル名の命名規則
データ伝送用の電子署名済みPDFファイル名については、以下の規則でファイル名の付与を行う。

NO	パターン	PDFファイル名規則
1	整理番号あり	整理番号_医療機関名称_文書ID_患者ID.pdf

<サンプルファイル名>

NO	パターン	PDFファイル名規則
1	整理番号あり	LIAJ001-k02-20101_〇〇病院_783_00000001.pdf

2. Documaker (HPKI版) 運用方法

本実証実験におけるDocuMaker (HPKI版) を使用した際の院内運用方法について以下を想定。

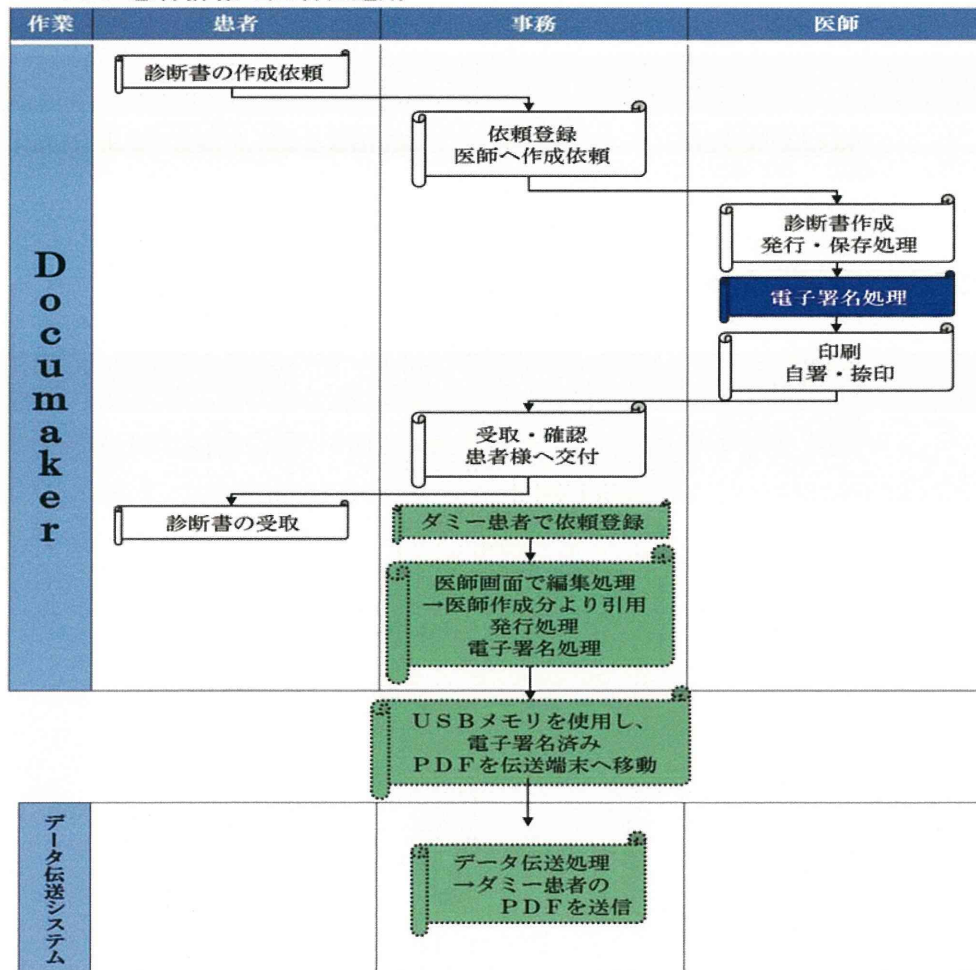
< 1 > 患者情報の匿名化運用

電子署名、及び署名済みPDFのデータ伝送を行う対象データの患者情報をダミーの患者情報にて再作成し匿名化を行うこととした。

ダミー患者での作成にあたっては、既に医師が発行している診断書よりコピーを行い、患者属性情報以外は同一の内容となるように作成したものを発行、および電子署名処理を行ったものを送信する。

【運用フロー】

< 1 > 患者情報の匿名化運用



4. ジャパネット株式会社

1. はじめに

本書は「平成 23 年度厚生労働科学研究補助金（地域医療基盤開発推進研究事業）」における弊社が実施した作業内容を報告するものである。

2. 作業内容

2.1 セキュアネットワークサービス

次に掲げる医療情報の送信/受信を行う施設のネットワーク状況をヒアリング（別紙「セキュアネットワーク導入チェック項目」を参照）し、各施設に適応したセキュアネットワーク（医療情報システムの安全管理に関するガイドラインに準拠したセキュアなネットワーク）を構築し、タイムスタンプ機能を含めたサービスとして提供した。

セキュアネットワーク導入施設（構築日順に記載）

① 亀田総合病院

- ・構築日：平成 22 年度導入済み
- ・導入構成： 4

（既存の施設（病院）内ネットワークにルータを導入する構成）

② 日本生命保険相互会社

- ・構築日：2011 年 11 月 17 日（木）
- ・導入構成： 1

（既存の施設（病院）内ネットワークには導入しない。

別に回線を用意して外部接続する構成）

③ 佐世保中央病院

- ・構築日：2011 年 11 月 22 日（火）
- ・導入構成： 1

（既存の施設（病院）内ネットワークには導入しない。

別に回線を用意して外部接続する構成）

④ 井上病院

- ・構築日：2011 年 12 月 01 日（木）
- ・導入構成： 2

（既存の施設（病院）内ネットワークにはルータは導入しない。

ただし、既設の回線のみ使用して外部接続する構成）

⑤ 柳原リハビリテーション病院

- ・構築日：2011 年 12 月 02 日（金）
- ・導入構成： 2

(既存の施設(病院)内ネットワークにはルータは導入しない。
ただし、既設の回線のみ使用して外部接続する構成)

⑥ 南町田病院

- ・構築日：2011年12月15日(木)
- ・導入構成：2

(既存の施設(病院)内ネットワークにはルータは導入しない。
ただし、既設の回線のみ使用して外部接続する構成)

⑦ 岡山大学病院

- ・構築日：2011年12月12日(火)、13日(水)
- ・導入構成：USBトークン

セキュアネットルータ構築の準備は実施していたが、ルータの導入は実施せず、既存のネットワークから外部接続できるようにPC接続型のUSBトークンを導入した。

2. 2 セキュアデータ交換サービス

医療情報の送信/受信(※)が可能な環境としてセキュアデータ交換サービスを2.1に掲げた7施設に提供した。別紙1にデータ交換された実績を報告する。

※受信可能な施設は日本生命保険相互会社のみ

3 まとめ

- ① 施設内のネットワークにセキュアネットルータを導入する場合、既存ネットワーク機器の設定変更や外部ネットワークと接続する際のセキュリティポリシーの変更が伴い、ルータを導入できない施設があると今後も考えられる。その場合、ルータではなく、USBトークンタイプの導入で対応できることが確認できた。
- ② 弊社が想定した5構成(ルータの4構成+USBトークン)で各施設(病院)にセキュアネットを導入することが出来た。なお、構築後は特段トラブルなく、ご利用頂けたと考えている。
- ③ セキュアネットルータ導入時のヒアリング(構成確認)に関しては関係者(外部業者含む)との調整に時間が掛かるため、前広に時間をとる必要があると感じた。
- ④ 医療情報の送信/受信に関しては、各実証状況の報告から改善点を見出していければと考えている。

5. 三菱電機インフォメーションシステムズ株式会社

(以下 MDIS)

(1) 実施した事業概要

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。MDIS では PDF に電子署名を行うアプリケーション SignedPDF を有しており、その機能を使うことにより電子署名を行うことが可能である。SignedPDF は日本医師会から発行される HPKI カードでの署名に対応しており、医師の署名に対応できるアプリケーションとなっている。本実証事業ではワークフローシステム内に組み込むモジュール (SignedPDF Interactive Server) および端末で直接署名を行うアプリケーション(SignedPDF Client)を提供した。SignedPDF の利用を行った病院は以下のとおりである

2010 年度(SignedPDF Interactive Server)

- 竹田総合病院
- 亀田総合病院
- 洛和会音羽病院

2010 年度(SignedPDF Client)

- 麻生飯塚病院

2011 年度(SignedPDF Interactive Server)

- 南町田病院
- 佐世保中央病院

2011 年度(SignedPDF Client)

- 柳原リハビリテーション病院
- 井上病院

タイムスタンプの取得に関しては、院内のセキュリティ上直接外部接続が出来ない病院がある。その機関では、外部接続できる端末にデータをコピーし、その端末上でタイムスタンプを取得する。タイムスタンプを個別に実施するには作業者の負荷がかかるため、MDIS では外部接続を行う端末に対して一括してタイムスタンプを取得できる機能を 2010 年度に開発し、各病院に組み込みを行った。組み込みを行った病院は以下のとおりである。

2010 年度

- 竹田総合病院
- 洛和会音羽病院
- 麻生飯塚病院

2011 年度

- ・ 南町田病院
- ・ 佐世保中央病院

一方、生保会社では取得した診断書に対して、正しい署名およびタイムスタンプが行われていることを確認する必要がある。通常、診断書毎に閲覧するアプリケーションを起動して、検証機能を使って検証された結果を目視確認する必要があるが、処理する量が多い場合、1 件ずつ確認するのでは業務負荷が高くなる。そこで、バッチ処理によって一括して検証する機能を 2011 年度に開発し、日本生命保険相互会社に組み込みを行った。

(2) 各機能の詳細

一括タイムスタンプ機能

一括タイムスタンプ機能は、特定のフォルダーにある署名済み PDF ファイルに対して、一括してタイムスタンプを取得できるプログラムである。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する。

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

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する。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する。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する。

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。

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 メモリ等で外部送信端末の特定フォルダーに移動を行なう。
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、出力フォルダーに保存される。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。

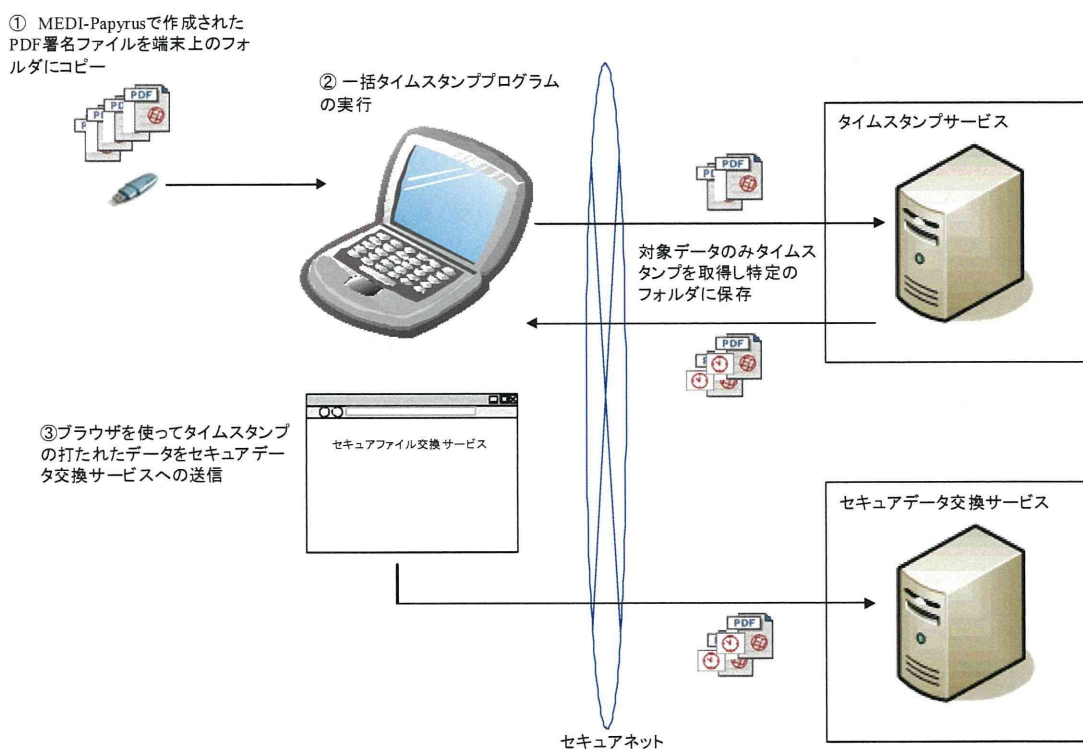


図 病院職員の一括タイムスタンプ機能を使った業務フロー

一括検証機能

生命保険会社ではセキュアネット交換サービス経由で取得した診断書に対して、正しい署名およびタイムスタンプが行われていることを確認する必要がある。通常であれば 1 件ずつ PDF ファイルを開き内容の確認と共に署名検証を行うが、大量に送付された PDF に対して 1 件ずつ確認する場合、作業負荷が高くなる。そこで、バッチ処理によって一括して検証する機能を作成することで作業負荷を下げると共に、将来的にフローに組み込むことが可能となる。

本事業では、特定のフォルダーにある PDF ファイルに対して、署名の検証を行い正しく検証できた PDF ファイルのみ指定のフォルダーに出力し、それ以外の PDF は別のフォルダーに出力することで検証の結果をわかりやすくする。

一括検証機能では以下の確認を行っている。

- ・ 署名された PDF であるか
- ・ 日本医師会から発行された証明書で署名されているか
- ・ 署名された証明書が失効されていないか
- ・ タイムスタンプが付与されているか
- ・ タイムスタンプを付与した証明書に問題はないか
- ・ 多重署名されていないか

ベースとなる検証機能は弊社製品である SignedPDF Server を使用しているため、別製品で署名された PDF が正しく検証できない場合がある。特に PFU が署名した PDF ファイルは長期署名フォーマット (ES-A) にて署名・タイムスタンプが付与されているため、弊社製品では検証自体できなかった。そのため、ES-A で署名された PDF は別途対象外の PDF とみなし、対象外フォルダーとして別に出力して ES-A の署名検証が行えるアプリケーションで別途処理することとする。

一括検証機能の操作および業務は以下のとおり

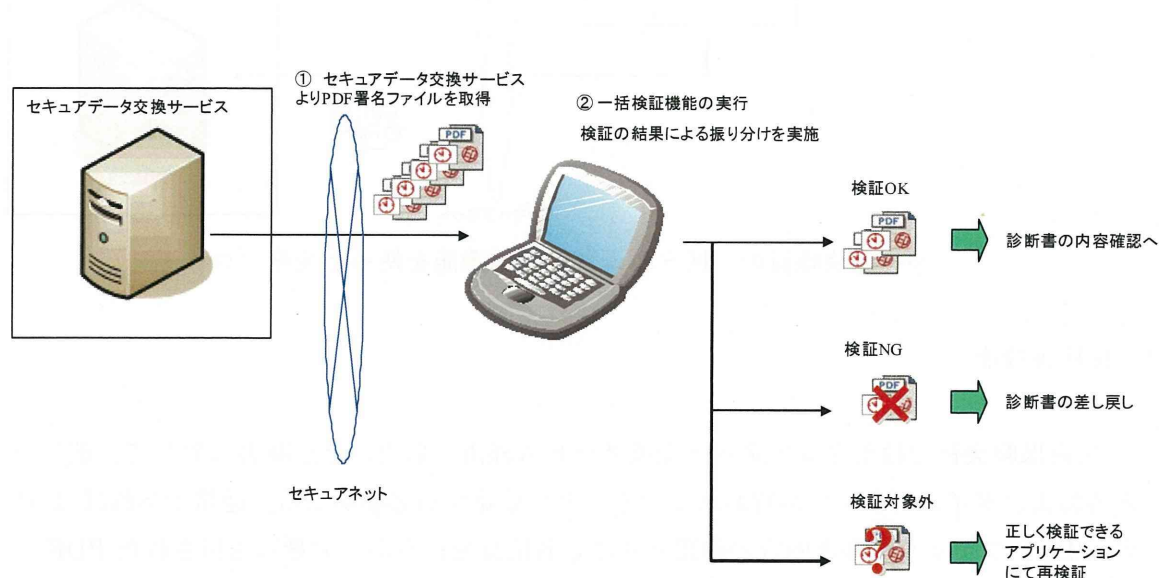


図 生命保険会社での一括検証機能を使った業務フロー

```

C:\WINDOWS\system32\cmd.exe

C:\VerifyBatch>cd C:\VerifyBatch

C:\VerifyBatch>set CLASSPATH=C:\VerifyBatch\VerifyBatch_lib;C:\VerifyBatch\VerifyBatch_lib\CAAdESLibrary.jar;C:\VerifyBatch\VerifyBatch_lib\certpath.jar;C:\VerifyBatch\VerifyBatch_lib\cms.jar;C:\VerifyBatch\VerifyBatch_lib\CMSSignedData.jar;C:\VerifyBatch\VerifyBatch_lib\mcertpath.jar;C:\VerifyBatch\VerifyBatch_lib\mjca.jar;C:\VerifyBatch\VerifyBatch_lib\mjce.jar;C:\VerifyBatch\VerifyBatch_lib\pfu\tslib.jar;C:\VerifyBatch\VerifyBatch_lib\SystemTimeModifier.jar;C:\VerifyBatch\VerifyBatch_lib\ToolsLibrary.jar;C:\VerifyBatch\VerifyBatch_lib\CRLManagerLib.jar;C:\VerifyBatch\VerifyBatch_lib\DVCSLog.jar;C:\VerifyBatch\VerifyBatch_lib\AdESLibrary.jar;C:\VerifyBatch\VerifyBatch_lib\spdfs.jar

C:\VerifyBatch>java jp.co.mdis.mistyguard.spdfs.cri.SPDFCRLDownloader
[2Signed_PDF.pdf]多重署名されたファイルです
[hoge.txt]PDFファイルではありません
[HPKIサンプル.pdf]検証成功しました
[HPKIサンプル_ES-A.pdf]SignedPDFで処理対象外のファイルです
[LIAJ001.PDF]検証結果に問題がありました：署名者証明書の上位証明書が存在しない、もしくは上位証明書が有効期限外でした。
[LIAJ056-B01-200807_〇〇病院_600.pdf]タイムスタンプが付与されていません
[test.pdf]検証成功しました
[verify-sample.pdf]SignedPDFで処理対象外のファイルです

*****
実行終了
SignedPDFで処理対象外のファイルが2件ありました
[c:/VerifyBatch/etc]にそのファイルが出力されています

処理ファイル数：6
エラー件数：4
[c:/VerifyBatch/output]に正しく検証されたファイルが出力されています
[c:/VerifyBatch/error]にエラーが発生したファイルが出力されています
*****
続行するには何かキーを押してください . . .

```

各ファイルの検証結果が表示されます

最終結果としてのサマリが表示されます

図 結果出力画面

(3)成果と課題について

署名アプリケーションに関しては、利用環境に合わせ SignedPDF Interactive Server や SignedPDF Client を適用することで、多くの病院に適用することができた。HPKI カードとの相性もよく、診断書が PDF にて発行できる場合には MDIS のアプリケーションはきわめて有効であると考えられる。

一括タイムスタンプ取得機能に関しては、概ね必要な機能を満たしていると考えられる。セキュアネット交換サービス側で自動的に登録できるような API があれば、一括タイムスタンプ取得から外部送信までを自動化することが可能であり、病院側の負担も軽減できると考える。

一括検証機能については、署名検証の対象範囲が ES-T までとなっており他社製品の署名された ES-A フォーマットでの互換性を確保できなかった。ES-A への対応や Office 等の PDF 以外のフォーマットにも対応して一元的に検証できることができれば生命保険会社の業務効率も上がるものと考えられる。