JAHIS

ＪＡＨＩＳ標準　１６－００２

ＪＡＨＩＳ
シングルサインオンにおける
セキュリティガイドライン
Ｖｅｒ．１．０

２０１６年６月

一般社団法人 保健医療福祉情報システム工業会
医療システム部会　セキュリティ委員会
シングルサインオンWG

ＪＡＨＩＳ
シングルサインオンにおけるセキュリティガイドライン
ま　え　が　き

昨今、多くの病院情報システムがマルチベンダーによる複数のシステム（医事会計、オーダエントリ、電子カルテ、薬剤・検査・放射線・手術・リハビリ・食事などの部門システム）で構成されるようになってきています。通常は利用するシステムごとに複数回のサインオンを行う必要がありますが、主に利便性の観点から、１回の操作で複数のシステムにサインオンする仕組み、すなわちシングルサインオンの採用が進んでいます。医療分野においては、それぞれのシステムに機微な個人情報が格納されていることが一般的であり、シングルサインオン導入時も医療機関とベンダー双方がセキュリティ対策を講じる必要があります。

JAHIS セキュリティ委員会ではシングルサインオン WG を発足させ、医療分野におけるシングルサインオンのあり方と情報セキュリティマネジメントと個人情報保護の視点から、医療機関とベンダーがそれぞれどのようなセキュリティ対策を行うべきか検討を行ってきました。

その成果として、2012 年度には JAHIS 技術文書「シングルサインオン実装ガイド」（JAHIS 技術文書 12-105）を制定しました。本ガイドラインでは、上記で示された文書を踏襲し、より踏み込んだ内容の JAHIS 標準として新たに制定を行いました。

このガイドラインを参考にすることで、ベンダー各社がシングルサインオン技術による利便性が高く、かつ安全なシステムを構築することの手助けとなれば幸いです。

２０１６年６月

一般社団法人　保健医療福祉情報システム工業会
医療システム部会　セキュリティ委員会
シングルサインオン WG

<<　告知事項　>>

本ガイドラインは関連団体の所属の有無に関わらず、ガイドラインの引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い、本ガイドラインに準拠する旨を表現することは厳禁するものとします。

本ガイドラインに基づいたシステムの導入・運用についてのあらゆる障害や損害について、本ガイドライン作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本ガイドラインについての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

目　　次

1. はじめに

本ガイドラインは下記を目的として記述した。

- 現在、一般的に考えられているシングルサインオン（以下 SSO とする）の概念を整理し、その実現のために利用可能な技術的選択肢を紹介、解説することで、SSO 技術を採用した利便性の高いシステムの普及のための啓発を行う。
- SSO を利用することで業務の利便性が向上すると考えられるユースケースを例示し、システム構築に SSO を適用するためのヒントを与える。
- 既存の SSO 技術を用いた典型的なシステムの実装モデルを例示することで、システム構築のイメージを想起させる。
- それらを用いて実運用を行う場合に想定されるリスクと、その対応への考え方を示し、啓発を行う。

本ガイドラインで対象とする読者は、病院情報システムの企画・設計者および SSO 策定の際に技術選択を担当するシステムインテグレーターのプロジェクトマネジャとする。これは医療機関の管理者と言うよりは、システム構築と、そのリスク管理に携わるベンダー側のプロジェクトマネジャのイメージが強いと考える。

本ガイドラインを読むために前提とする知識は、病院情報システムの業務ワークフロー、ネットワークを介した情報処理機器間のデータ通信の基本的な内容、利用者の認証と情報アクセスの認可に関する基本的な概念とする。

2. 概要

本ガイドラインは、医療系（基本的には院内限定）における SSO のユースケースに基づいて比較的厳密な実装モデルの例（院内のシステム全部は網羅していない）を複数示し、それぞれについて、特に SSO に起因する部分にフォーカスを絞ったリスクアセスメントの例を示す。リスク対応については厚生労働省の「医療情報システムの安全管理に関するガイドライン」（以下、安全管理ガイドラインとする。）への遵守を前提とした記述とする。

3. 適用範囲

3.1. 適用範囲

本ガイドラインにおいては、主として院内で運用管理されている各種の情報システムにおける SSO を適用範囲とするが、外部保存、ASP/SaaS 等（場合によっては地域連携を含む場合もあるかもしれない）に関しては、ユースケースの一部に含まれる場合も考慮する。

3.2. 適用除外

本ガイドラインにおいては、下記に関する内容は除外する。

- 認証方式そのもの、およびその強度等に関する内容
- 利用者の権限管理、およびその実装方法に関連する内容
- 利用可能なソフトウェアライブラリ等の紹介と解説
- 一度サインオンした後の、一括してのサインオフ（シングルサインオフ）

4. 主な用語

読者が IT に関する基礎知識を持っていることを前提とし、検索エンジンで調査可能な用語については特に記載しない。また、本書では「ログオン」と「サインオン」の２つの用語を同義として扱う。これは、２つの用語を無理に統一すると固有名詞として各々の用語が使用されている場合に不自然となるためである。

- サインオン
  通常のコンピュータシステムに自分の身元を示す情報を入力し、接続や利用開始を申請することを意味する「ログオン」と同じ意味で用いる。サインオンには情報システムの利用者が何らかの入力装置を操作して行うものと、それを契機として、またはそれとは関係なくシステムが自動的に他のシステムに対して行うものが考えられるが、本書ではどちらもサインオンとして扱う。
- サインオフ
  「サインオフ」は「サインオン」と同様に「ログオフ」もしくは「ログアウト」の意味で用いる。
- 外部保存
  厚生労働省の「安全管理ガイドライン」に記載されている、法的に保存義務のある診療録等の文書を、医療機関外に保存することを言う。
- 地域連携
  電子化された診療情報等を複数の医療機関の間で共有すること。
- Web システム
  Web アプリケーションを使用したシステム。Web サーバに配置したアプリケーションをクライアントである Web ブラウザで利用する。サーバとクライアント間の通信プロトコルは HTTP/HTTPS を用いる。
- レガシーシステム
  本書では Web システムではないシステムを指す。例えば、専用のクライアント・アプリケーションがデータベースサーバにアクセスして処理を行うクライアント/サーバシステムのようなもの。

本書では、次の記号および略語・表記を用いる。

- ASP　Application Service Provider(アプリケーションサービスプロバイダ)
- HIS　Hospital Information System(病院情報システム)
- HTTP　Hypertext Transfer Protocol (Web 送受信プロトコル)
- PACS　Picture Archiving and Communication Systems(画像保存通信システム)
- PKI　Public key infrastructure(公開鍵暗号基盤)
- RIS　Radiology Information System(放射線科情報システム)
- SaaS　Software as a Service（サービス型ソフトウェア）
- XML　Extensible Markup Language(拡張可能なマーク付け言語)

5. シングルサインオンの仕組みと要件

本章では、SSO の概要を説明した後、複数存在する SSO の実現方式の仕組み、SSO 実現のためのシステム要件を説明する。

5.1. シングルサインオン概説

5.1.1.認証の位置付け

認証という用語は識別と狭義の認証の２つの要素を含むと考える場合がある。また、関係の深い用語に認可がある。それぞれの意味を次に示す。

（１）識別（identification）:
利用者が誰であるかを特定すること。システムにアクセスしてきた利用者が、予め利用者（端末や装置等を含む）毎に割り当てられ管理されたどの識別子（ユーザ ID など）に該当するかを判別する。

（２）狭義の認証（authentication）:
利用者が本物かどうかを判定すること。システムにアクセスしてきた利用者が、その識別子に該当する正当な利用者であるか否かを判定する。判定は、その識別子に該当する利用者のみが保有する認証情報（パスワード、生体情報、電子署名、それらの組み合わせなど）をシステムに提示することによって行なう。

（３）認可（authorization）:
利用者がリソースを利用できるかどうかを判定すること。識別子とアクセス規則に基づいて、その利用者がリソース（サービスや情報）にアクセス可能か否かを判定する。利用者の持つ属性に基づいてアクセスの可否を判定する場合もある。

通常、識別、狭義の認証、認可はこの順に処理が進められる（図５．１－１）。識別と狭義の認証を合わせた広義の認証を単に認証と表す場合がある。本書では認証という用語を広義の認証の意味で用いることとする。

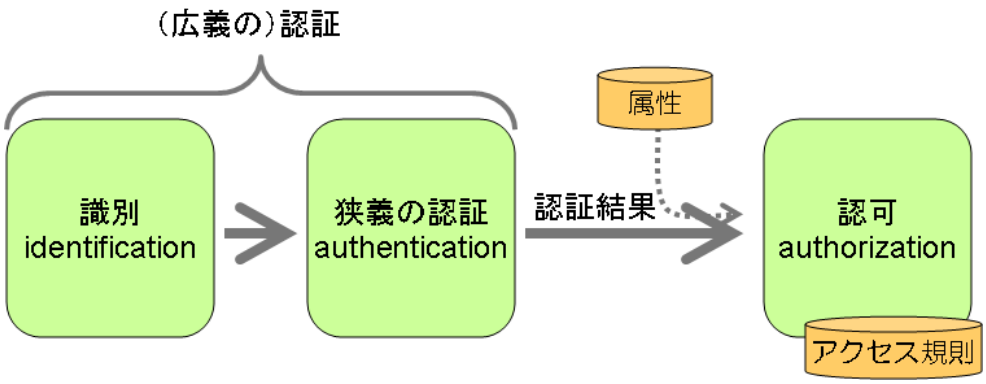


図５.１－１　認証の位置付け

5.1.2.シングルサインオンとは

SSO とは、ID とパスワードなどによる認証を必要とする複数のシステム（アプリケーション）に対して、最初に１回だけ認証を行うことにより、その後の認証をすべてシステムにより自動化する技術である。

5.1.3.シングルサインオン技術出現の背景

現代の IT 環境には様々なシステム（アプリケーション）が存在し、セキュリティを確保する為にそれぞれのシステムで認証機能が実装されている。認証機能には、ID とパスワードを利用する方法の他、ワンタイムパスワード、IC カード、指紋や掌紋などのバイオメトリックスを利用する方法など数多くの方法が提供されており、またそれらを複数組み合わせる方法が用いられる場合もある。

一人で複数のシステムを使う利用者は、使うシステムの数だけ、例えば ID／パスワードといった認証情報を管理しなければならい。そのため利用者にとって次のような問題が発生している。

- 多数の認証情報を管理しなければならない負荷の問題
- 個々のシステム毎に、利用を開始する度に認証のためのログオン操作を行なわなければならない負荷の問題
- 認証情報管理の不備により他人が本来の利用者に成りすまして重要データにアクセスするなどのセキュリティの問題

また、ID／パスワードを利用するシステムでは、システム管理者の日常業務の少なくない割合がパスワードの問い合わせやパスワードをリセットする作業に費やされていると言われており、煩雑な認証情報の管理への要求がシステム管理者に負担をかけているという問題も報告されている。

SSO は上記のような問題を解決するために考案された技術である。

5.1.4.シングルサインオン導入による効果

SSO の導入により、次に示す効果が期待される。

（１）利用者の利便性・生産性向上

利用者は一つの認証情報を一度だけ入力することにより、アクセスを許可された複数のシステムに自動的にログオンできる。このため、複数の認証情報を管理しなければならない負荷から解放される。これに伴ってログオン操作も一度で済むため、異なるシステムの利用を開始する度にログオン操作を行なう負荷から解放され、システムに対する迅速なアクセスが可能となり利便性・生産性が向上する。

（２）セキュリティのレベルの向上

利用者が管理しなければならない認証情報を一つにする事により、例えばパスワードを利用する場合、定期的な更新を徹底でき、他人にわかりにくいより複雑なパスワードを設定できるようになり、対象システム全体のセキュリティのレベルを引き上げることができる。

（3）アクセス権解除の迅速化

SSO で認証の可否を制御することにより、退職した職員等の全てのシステムに対するアクセス権を即座に解除することができる。

（4）システム管理者の負荷軽減と利用者の待ち時間短縮

SSO の導入により、利用者のパスワード忘れ等による、システム管理者の認証情報の再設定を一括して行なえるようになり、作業負荷を減少させることができる。認証情報の再設定が一括して行なわれるため、利用者にとっては待ち時間の短縮につながる。

（5）ログオン履歴の集約

各々のシステムに対する全てのアクセスを SSO システムが管理している場合、全てのログオンの履歴を集約して管理することができる。ただし、ログオン履歴の集約については、SSO システム単独で行うよりも、別途ログ統合管理システムを設置して他のログと合わせて管理する方が望ましい。

5.2. シングルサインオンの各方式

SSO の実現には複数の方式があり、本章では各々の方式についての仕組みと SSO 実現の為のシステム要件を説明する。

5.2.1.代理ログオン方式

（1）方式

個別のサービスでユーザの認証情報は個別に管理されている環境において、ユーザはそれぞれの認証情報をユーザに代わり集中保管するアプリケーションやサーバを介してログオンする方法である。

ユーザは認証情報を管理するアプリケーションやサーバにログオンするだけで、各サーバへの認証はアプリケーションやサーバが行うため、ユーザの認証を一度のみにすることができる。

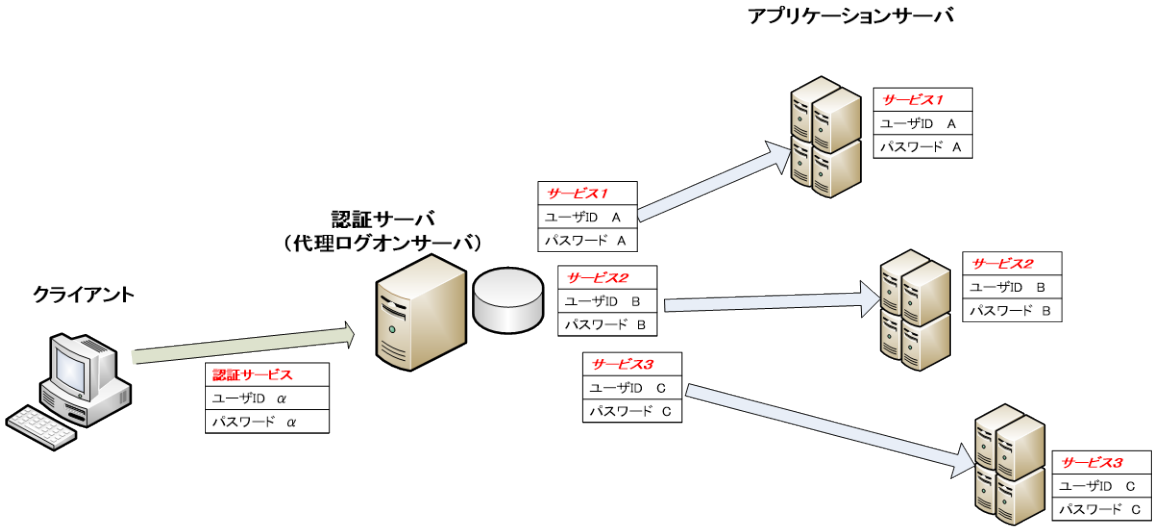


図５．２－１　代理ログオン方式

（2）メリット

- 既に個別の認証情報でサービスが運用されている場合であっても、サービス側の変更がほぼ不要なため、導入が容易である。
- 認証機能が弱い、あるいは実装されていないシステムにおいて、新たに適切な認証機能を加えることができるため、システムのセキュリティを向上させることが可能である。

（3）デメリット

- 認証情報が各サービスに分散されている状況に変わりがないため、認証情報の更新などを各サービス及び、代理ログオンを行うアプリケーションやサーバで管理する必要がある。
- サービスが追加されると、そのサービスに応じた認証方式を代理ログオンサーバが実装する必要があり、対応が困難な場合がある。

5.2.2.リバースプロキシ方式

（1）方式

各サービスに対するアクセスをプロキシに集約し、プロキシでユーザ認証を行う方法である。プロキシでユーザからの認証要求を受け付け、これをパスした場合のみ、ユーザから要求があったサービスに接続し、また、そのサービスからの応答をユーザに返信する。

※代理ログオン方式との違い

代理ログオン方式では、代理ログオンサーバは認証のみを担うが、リバースプロキシ方式では、クライアントとアプリケーションサーバ間の全通信が認証サーバ（プロキシ）を通過する。

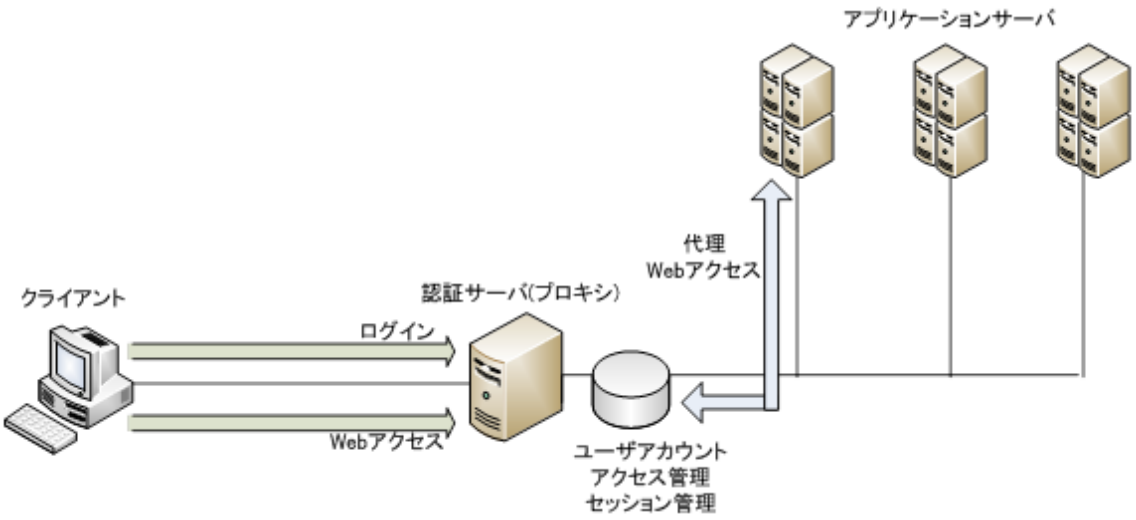


図５．２−２　リバースプロキシ方式

（2）メリット

- サービス側に特別な仕組みを実装する必要がない。
- サーバはクライアントから直接アクセスできないため、ファイアウォールの機能も果たす。

（3）デメリット

- 各サービスは、Web アプリケーションとして実装されている必要がある。
- 各サービスは、プロキシを介してのみアクセス可能なネットワーク構成に変更する必要がある。
- 各サービスがプロキシ経由となるため、プロキシがボトルネックとなる可能性があり、負荷分散の仕組みを考慮する必要がある。
- 各サービスにとって、サービスを利用しているユーザが誰なのか確認が必要な場合、その情報をその都度プロキシから入手するような仕組みを取り入れたり、サービスの利用記録とプロキシのアクセス記録との整合性の確認を行ったりする必要がある。

5.2.3.エージェント方式

（1）方式

ユーザはまず認証サーバに対して認証処理を行い、認証済みであることを示すチケットを受け取る。一方各サーバは認証サーバが発行したチケットを検査するためのエージェントモジュールを組み込む。ユーザが各サーバにアクセスすると、チケットが検査されアクセスが許可される。

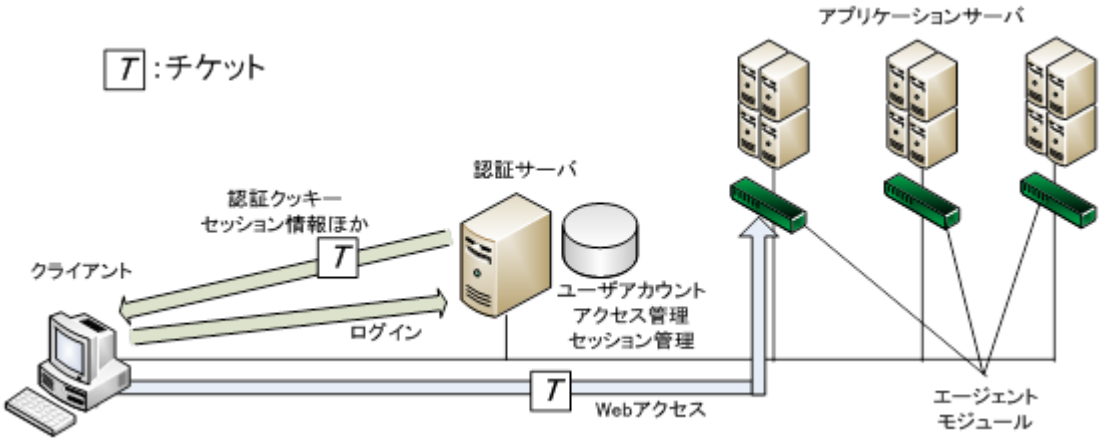


図５．２−３　エージェント方式

（2）メリット

- ユーザからの要求は、認証処理以外は直接各サーバに向かうため、レスポンスのボトルネックとなる個所が少なく、スケーラビリティに優れている。
- SSO 導入前と比較して、ネットワーク構成変更の必要がない。
- ユーザの利用記録は、認証サーバから提供される認証状態をセッション情報として利用することで特定が容易となる。

（3）デメリット

- 各サービスのサーバは、SSO 導入前のアプリケーションの認証機能に代わってエージェントモジュールが組み込める物である必要がある。

5.3. 標準化されたシングルサインオン方式

5.3.1.Kerberos 方式

（1）方式

Kerberos 認証とは、IETF RFC 1510 で規定されており、ユーザ認証と共通鍵を用いた通信経路の暗号化の機能を持ち、認証サーバとチケット発行サーバからなるキー配付センター（KDC：Key Distribution Center）の発行するチケットを用いることによって、SSO を実現することを特徴とする認証方式である。

Kerberos による認証フローは以下の通りである。

① ユーザは認証サーバ（AS：Authentication Server）に認証処理を要求。
② AS はユーザに TGT(Ticket-Granting Ticket)を発行。
③ ユーザはその TGT をチケット発行サーバ（TGS：Ticket-Granting Server）に提出。
④ TGS はユーザにサービスチケットを発行。
⑤ ユーザはサービスチケットを目的のサービスへ提出してサービスを利用。

ユーザが続けて別のサービスも利用したい場合には、既に AS から配布されている TGT を TGS に提出し、利用したいサービス用のチケットを入手する。なお、TGT には有効期限が定められており、有効期限内は利用可能である。

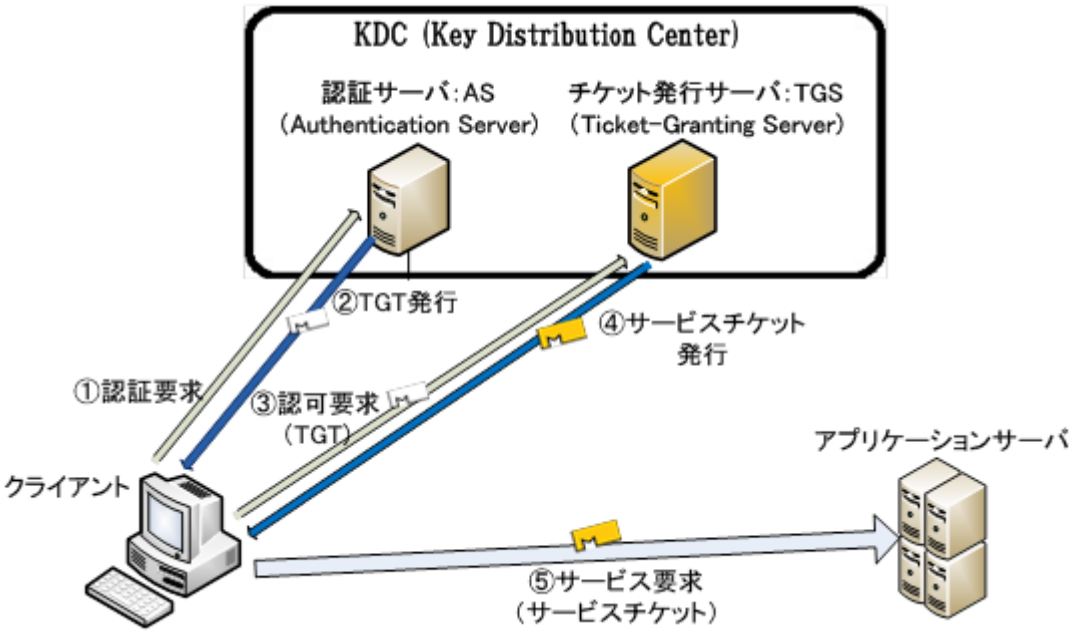


図５．３－１　Kerberos 方式

（2）メリット

- Web アプリケーション以外にも適用が可能。
- 標準化されているので、導入が容易である。
- 比較的低コストで、大規模システムに適用可能である。

（3）デメリット

- 既存のシステムに関しては、サーバだけではなくクライアント・アプリケーションも変更が必要。

5.3.2.SAML 方式

（1）方式

SAML(Security Assertion Markup Language)とは、標準化団体 OASIS により策定されている認証情報を安全に交換するための XML ベースのフレームワークである。

なお、SAML では認証のための情報は特定されておらず、ID とパスワードによる認証や X.509 証明書を利用した PKI など、目的に応じて選択できる。

また、SAML Assertion（XML ベースの認証情報）を共有するためのメッセージの送受には HTTP もしくは SOAP が利用できる。SAML では、認証サーバとアプリケーションの間で、認証情報、属性情報、認可情報を伝達することで SSO を実現する。

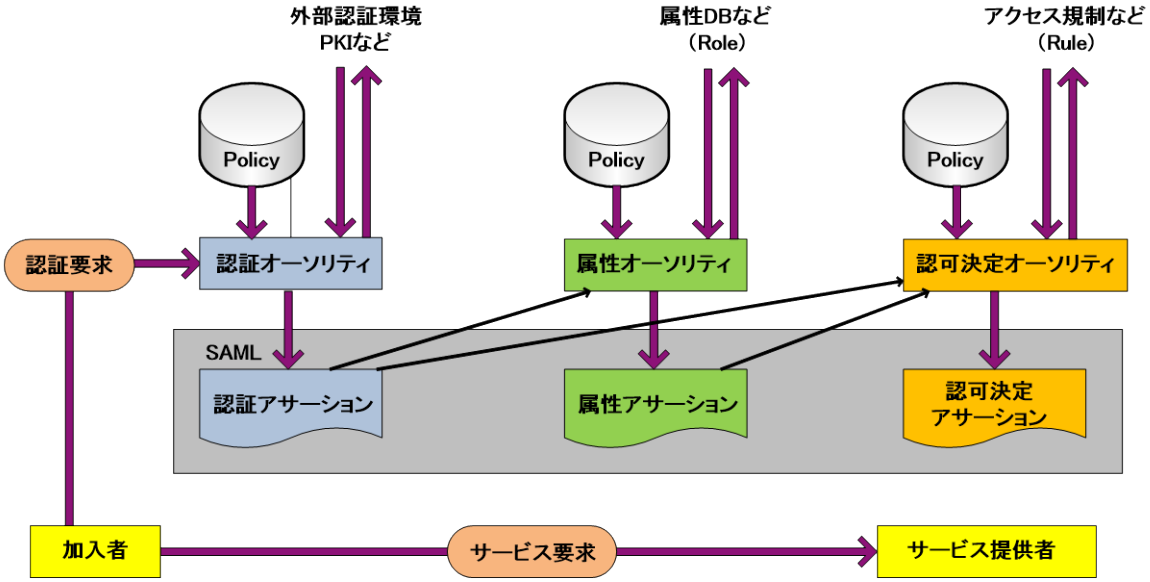


図５．３－２　SAML 方式

SAML の実装方式は、メッセージの交換フローの違いから Artifact 方式や POST 方式などに分けられる。

Artifact 方式の例

① クライアントはサーバにリソース要求する。
② サーバから認証サーバにリダイレクトして認証される
③ 認証サーバはサーバにリソース要求を返し、Artifact（Cookie や URL に付与する文字列）を発行する。
④ サーバは認証サーバに Assertion を要求する。
⑤ 認証サーバはサーバに Assertion 応答する。
⑥ サーバはクライアントにリソース要求に対する応答をする。

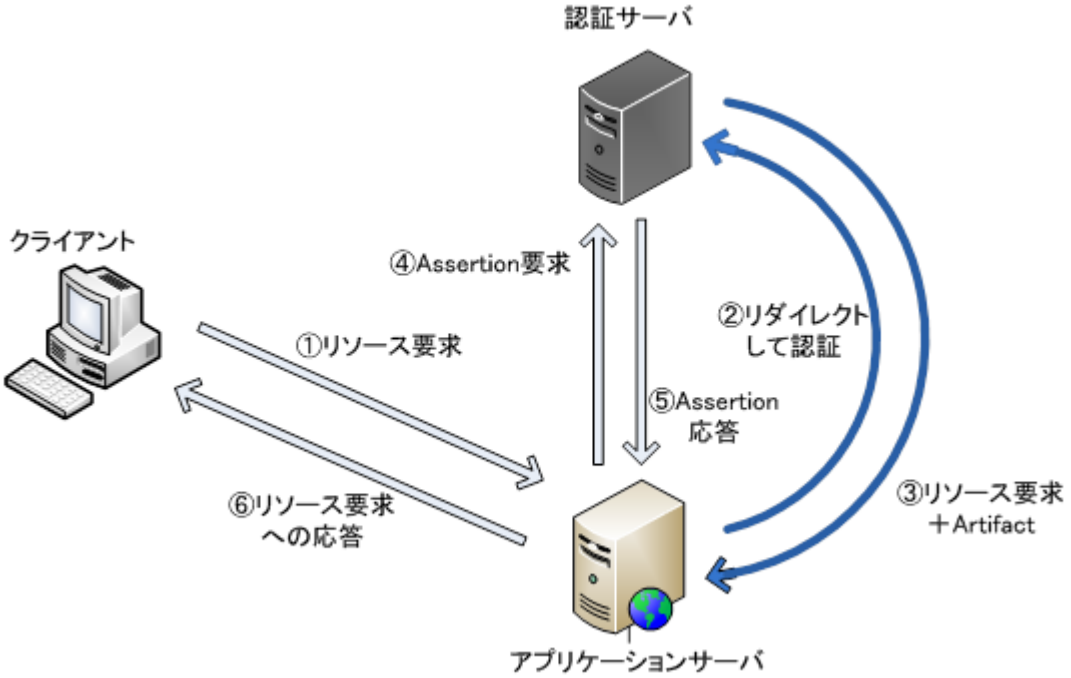


図５．３－３　SAML Artifact 方式

POST 方式の例

① クライアントは認証サーバにログオンする。
② 認証サーバはクライアントに Assertion を発行する。
③ クライアントは Assertion をサーバに渡し（HTTP-POST）し、リソース要求する。
④ サーバはクライアントにリソース要求に対する応答をする。

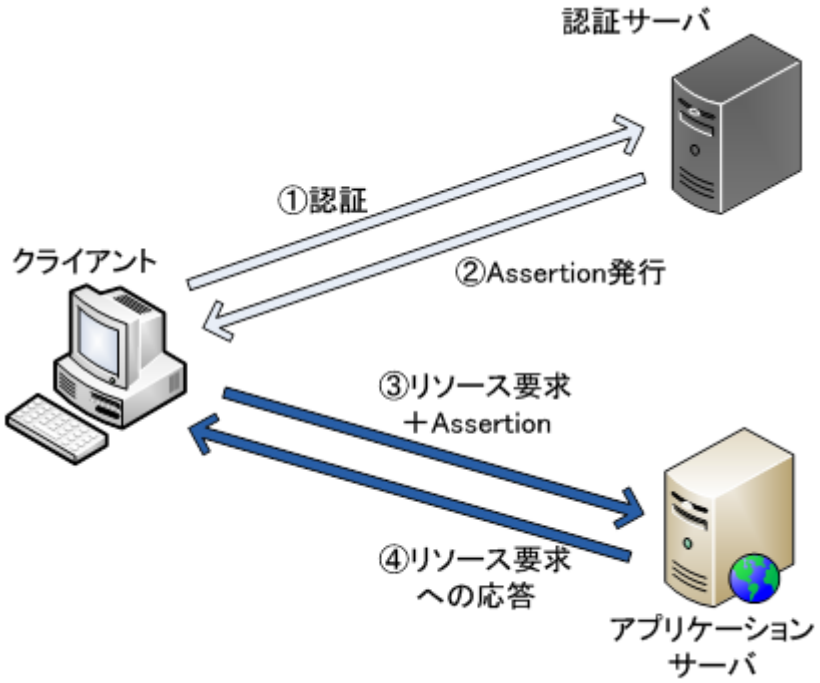


図５．３－４　SAML POST 方式

（２）メリット

SAML 全般

・ 情報の形式や要求・応答のプロトコルが標準化されているため、高い相互接続性を保証する。

Artifact 方式

・ クライアント端末上に情報を保持しない為、POST 方式よりセキュアな環境を構築出来る。

POST 方式

・ シーケンスがシンプルなため、性能への影響が比較的少ない。

（３）デメリット

SAML 全般

・ アプリケーションは HTTP 上の Web アプリケーションや SOAP を用いた Web サービスでは導入しやすいが、レガシーシステムへの導入は困難で、比較的に高コストになる。

Artifact 方式

・ リダイレクトが多く、また認証サーバとサービスの間での通信も発生するため性能の悪化が懸念される。

POST 方式

- クライアント端末上に情報を保持するため、Artifact 方式より若干セキュリティが懸念される。

5.4. シングルサインオンを実現するためのシステム要件

本節では、SSO を実現するためのシステム要件について述べる。なお、SSO 化されていない状態でも必要となるシステム要件に関しては言及しない。

システム形態としては、Web システムとレガシーシステムで分ける。

5.4.1.各方式においての共通要件

（1）ネットワーク構成

（a）他システムとネットワーク接続できること

SSO を行う他の業務システムや SSO システムとネットワークで接続する必要がある。他のシステムとは隔離されたクローズドなネットワークで運用しなくてはならない業務システムは、SSO を実現することはできない。

5.4.2.代理ログオン方式においての要件

（1）システム形態

（a）特に要件無し

Web システムでもレガシーシステムでも利用可能。

（2）ネットワーク構成

（a）クライアントから認証サーバにアクセスできること

代理ログオンのために新たに認証サーバを構築する場合は、その認証サーバへアクセスできる必要がある。

（b）クライアントから代理ログオンサーバにアクセスできること

代理ログオンサーバを介してログオンする場合は、その代理ログオンサーバにアクセスできる必要がある。

（3）アプリケーションサーバ側の要件

（a）認証情報の入力インターフェースを変更できること

認証情報が代理ログオンサーバや代理ログオン用のアプリケーションからアプリケーションサーバに直接渡される場合、業務システムが用意している認証情報の入力インターフェースを省略して、渡された認証情報を処理することが必要となる。

例えば、ID とパスワードの入力画面を省略して、代理ログオンサーバから渡される ID とパスワードを処理することが必要となる。

（4）クライアント側の要件

（a）認証情報の入力インターフェースを変更できること

認証情報が業務システムの用意するクライアントを経由してアプリケーションサーバに渡される場合、業務システムのクライアントは代理ログオン用のアプリケーションから認証情報を取得するインターフェースを用意する必要がある。

（5）システム改修の有無

（a）サーバ側

必要有り：代理ログオンサーバや代理ログオン用のアプリケーションから受け取った認証情報を処理することが必要となる。

（b）クライアント側

必要有り：認証情報をアプリケーションが入力するインターフェースが無い場合は用意する必要がある。

5.4.3.リバースプロキシ方式においての要件

（1）システム形態

（a）Web システムであること

リバースプロキシ方式の SSO では、Web ブラウザからのリクエストを、一度プロキシが受け、そのリクエストを Web サーバに中継する仕組みを採る。そのため、SSO の対象となる業務システムは Web システムである必要がある。

（2）ネットワーク構成

（a）クライアントから業務システムへのアクセス経路がプロキシ経由となること

各業務システムへのアクセスが必ずプロキシ経由となるようにネットワーク構成を変更できる必要がある。

（3）アプリケーションサーバ側の要件

（a）セッション管理機能を備えていること

リバースプロキシ方式の SSO では、各業務システムのサーバへのアクセスは全てプロキシ経由となる。よって、業務システムへのアクセスのソースアドレスを頼りにセッション管理を行っている場合には、その他の方式（たとえば HTTP クッキーを利用する等）でのセッション管理機能を備える必要がある。

（4）クライアント側の要件

（a）HTTP クッキーが有効であること

セッション管理に HTTP クッキーを用いるシステムの場合、HTTP クッキーが Web ブラウザの設定で無効になっているとセッション管理の機能が正しく動作しないため、HTTP クッキーの設定を有効にしておく必要がある。

（5）システム改修の有無

（a）サーバ側

必要有り：認証機能を SSO システムの用意するものに置き換える必要がある。

（b）クライアント側
必要無し（ただし、クライアント側の要件を満たす Web ブラウザが必要）

5.4.4.エージェント方式においての要件

（1）システム形態
（a）特に要件無し
Web システムでもレガシーシステムでも利用可能である。

（2）ネットワーク構成
（a）クライアントから認証サーバにアクセスできること
認証のために、認証情報のやり取りをクライアントと認証サーバで直接やり取りするタイプのエージェント仕様の場合は、クライアントから認証サーバにアクセスできる必要がある。認証情報をエージェントが中継して認証サーバに問い合わせる場合は、業務システムにアクセスできればよい。

（3）アプリケーションサーバ側の要件
（a）エージェントが組み込めること
既製品のエージェントを利用する場合は、エージェントが組み込み先の Web サーバやアプリケーションサーバの環境（OS やサーバ・アプリケーションの種類、バージョン等）に合ったものである必要がある。
そして、エージェントが想定する仕様に基づいて業務システムを対応させる必要がある。例えば、セッション管理において、エージェントがセッション情報を認証サーバに問い合わせる場合には、エージェントと連携したセッション管理が必要となる。

（4）クライアント側の要件
（a）HTTP クッキーが有効であること（Web システムの場合）
セッション管理に HTTP クッキーを用いるシステムの場合、HTTP クッキーが Web ブラウザの設定で無効になっているとセッション管理の機能が正しく動作しないため、HTTP クッキーの設定を有効にしておく必要がある。

（b）HTTP リダイレクト機能が有効であること（Web システムの場合）
認証情報の入力を認証サーバにリダイレクトさせて行う方式のエージェントの場合、Web ブラウザの HTTP リダイレクト機能が必要となる。

（c）エージェントが組み込めること（Web システム、レガシーシステムの場合）
エージェントが認証のために管理しているチケットをクライアント側でもハンドリングしなくてはならない場合、クライアント側にもエージェントを組み込む必要がある。その際、既製品を利用する場合は、サーバ側と同様にクライアントの環境に合ったものが必要となる。

（5）システム改修の有無
（a）サーバ側
必要有り：エージェントを組み込み、認証機能を SSO システムの用意するものに置き換える必要がある。

（b）クライアント側
必要有り：クライアント側にもエージェントの組み込みが必要な場合のみ。

6. 医療分野におけるシングルサインオン

6.1. 医療分野でシングルサインオンが必要となる背景

医療機関においては、様々なシステムや装置を利用することで、効果的で効率的な医療を行うことが求められる。例えば、オーダ系、カルテ系、検査系、画像系、会計系などのシステムや装置であるが、これらは専門性が非常に高く、病院情報システム全体としては、異なるベンダーの製品を組み合わせた複合システムとして構築されている場合が多い。

これらのシステムや装置が有機的に連携し情報をやりとりすればさらに有効な運用が可能であるが、現状互いに十分に連携が取れているとは言い難い。

そのため、利用者が複数（多数）のシステムや装置を渡り歩き、業務を行っている。利用者は複数のシステムや装置を利用する毎に利用者認証を受けなくてはならならず、その手間が面倒との理由で安易な利用者認証を行っているケースが少なからず存在し、医療情報という非常に機微な情報を扱う上で重篤なぜい弱性となっている可能性が高い。

また、効率化の面でも、複数回利用者認証を行うことで無駄な時間が発生することは医療サービス提供の作業効率を低下させ、さらに個別のシステムや装置で別々に利用者管理を行うことで管理コストがあがることにより医療機関の経営を圧迫する。

以上のような背景により、医療分野ではこれらの課題を解決する技術として SSO による効率化が期待されている。

6.2. シングルサインオンが適用可能なユースケース

6.2.1.ユースケース記載の考え方

ここでは医療機関における典型的なユースケースを次のような観点で記載した。

（1） １人の操作者が行う独立した一連の業務で、複数のシステムを同時に利用するケースを対象とする
（2） 利用される物理的な端末およびクライアント・アプリケーション
（3） 利用されるシステム（サーバ・アプリケーション）
（4） システムへのログオンのタイミング
（5） 各システムに出されるリクエストの内容、およびタイミング

具体的な記載ルールは次のとおりとする。

（a）前提条件
（1）１人のオペレータを中心に考える。
（2）互いに独立した複数のシステムを利用する場合に限定する。
（3）最初のシステム利用から、最後のシステムをリリースするまで、１人のオペレータが端末を専有するものとする。
（4）複数業務を混在させず、１つの業務に対して一点一葉で記述する。

（b）特定すべき構成要素

（1）部門名

（2）オペレータの属性（病棟医師、読影医、病棟看護師、放射線技師、等々）

（3）機能端末およびクライアント・アプリケーション

（4）システム名（HIS、RIS、PACS、モダリティ、等々）

（5）アクション（システムへのリクエストであり情報の流れではない）

（6）ログオン（オペレータによる認証）

（7）ログオン（オペレータ以外による認証）

この記載ルールに従った凡例と記載例を、それぞれ図６．２−１と図６．２−２に示す。

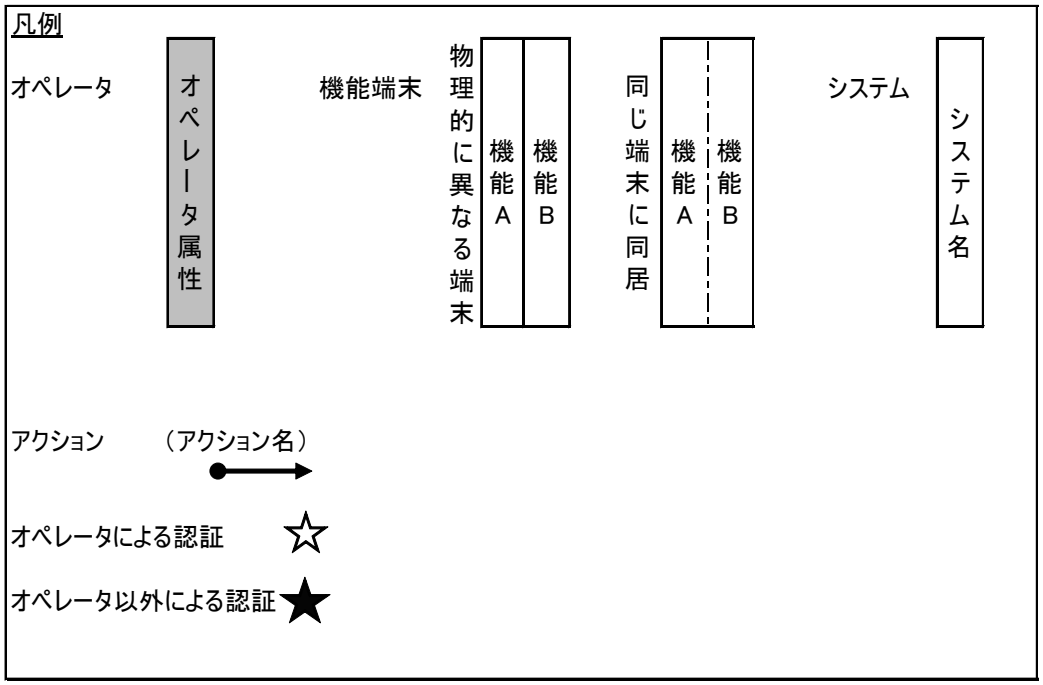


図６．２−１　業務フロー記載に用いる凡例

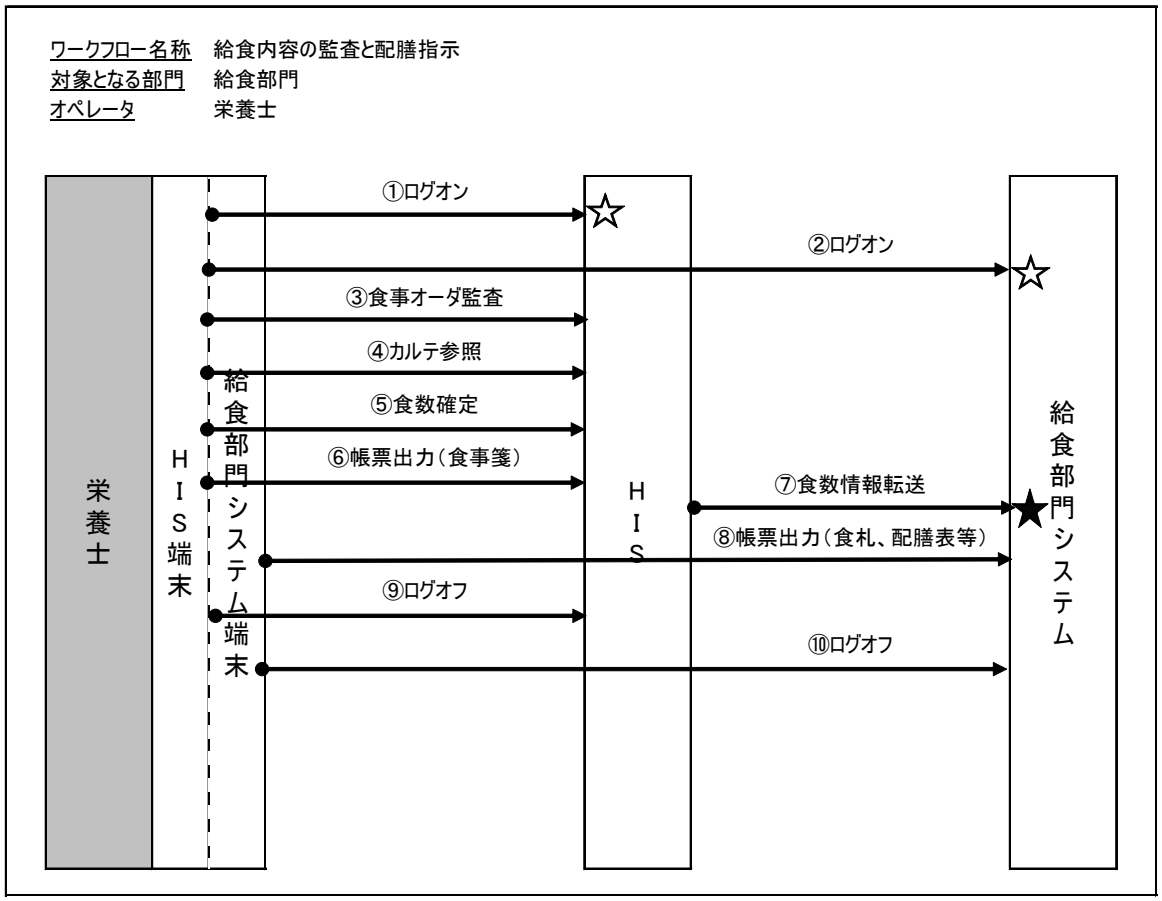


図６．２−２　業務フロー記載の例

（ｃ）対象としたユースケース

ここでは典型的な医療機関におけるユースケースとして、経済産業省　平成 16 年度　先導的分野戦略的情報化推進事業「シングルサインオン実装仕様書」（平成１７年３月）※より参考にしたケース（４件）、及び新規ケース（２件）をリストアップした。

（１）病棟看護　※
（２）放射線医師による読影　※
（３）放射線治療を行う医師による治療計画立案と照射準備　※
（４）生理検査判読　※
（５）外来診察前準備
（６）手術開始から終了まで

記述したユースケースの業務の流れにおいて、実際にシステム間では暗黙の認証が行われている場合があるが、ここではあえてそれらの認証（オペレータ以外による認証）についても明示的に示していることに留意されたい。

6.2.2.ユースケース１　病棟看護

＜前提条件＞

- 該当の患者に対し看護オーダが既に出されている。
- 医師は既に看護に必要なオーダ情報やカルテ情報（患者のアレルギー情報や診断、治療方針など）を入力済である。
- 患者は入院患者として登録されており、該当の看護師が担当患者の当日の受持ち患者として登録されている。

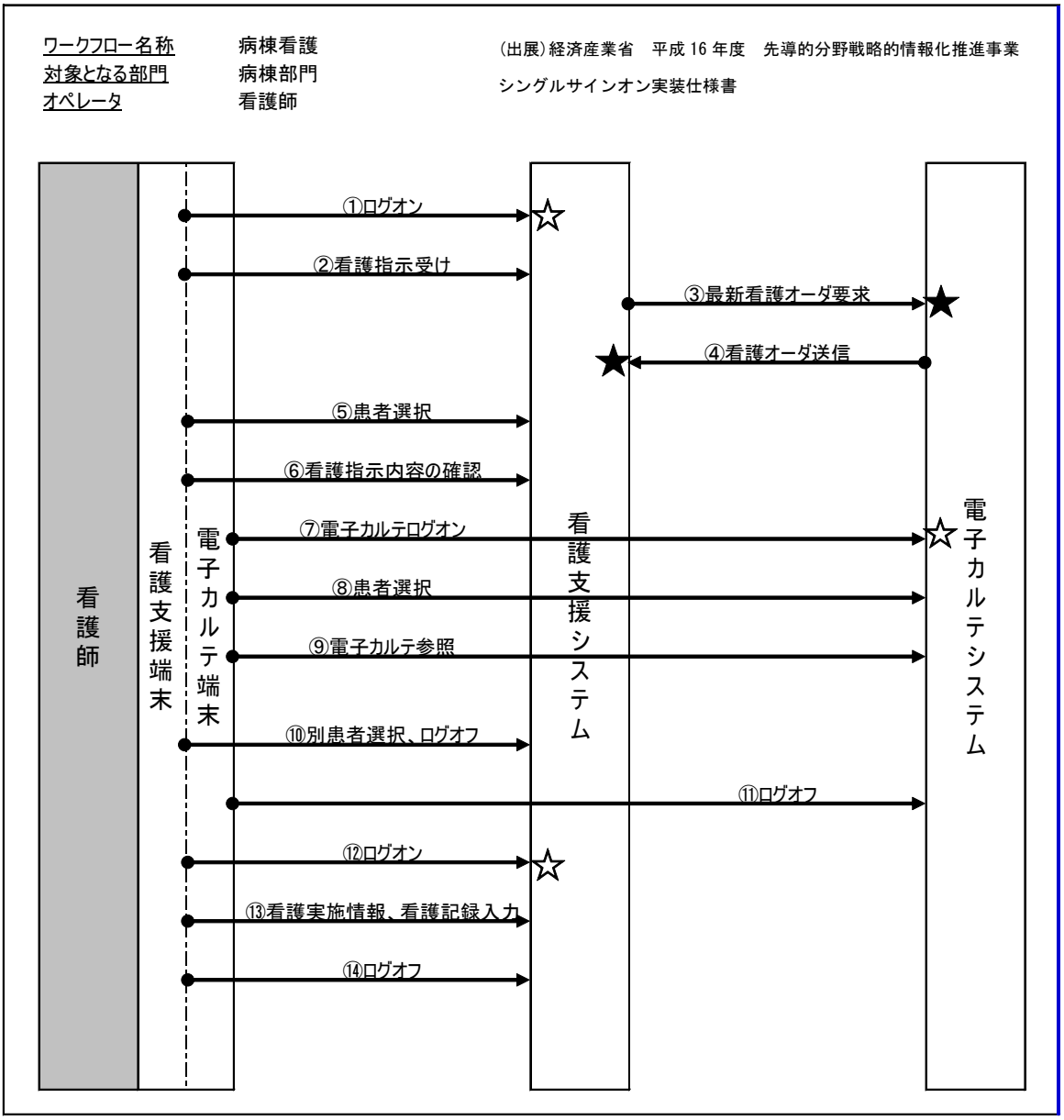


図６．２−３　病棟看護ワークフロー

＜業務の流れ＞

① 看護師は看護支援システムにログオンする。
② 電子カルテシステムからの最新の看護指示情報の取り込み処理を指示する。
③ 看護支援システムから電子カルテシステムへ看護情報送信依頼情報を送信する。
④ 電子カルテシステムから看護支援システムに最新の看護指示情報が取り込まれる。
⑤ 看護師は自分の受持ち入院患者リストから対象の患者を選択する。
⑥ 看護師は該当患者の看護指示内容を確認する。
⑦ 看護師は電子カルテシステムを起動（ログオン）する。
⑧ 看護師は電子カルテシステムにて受け持ち入院患者を選択する。
⑨ 電子カルテシステムの経過記録参照画面が開き、該当の患者のカルテ情報が表示される。
⑩ 看護師は看護支援システムのログオフを行う。
⑪ 電子カルテシステムの参照が終了した為、電子カルテシステムよりログオフする。
⑫ 看護実施情報を登録するために、看護支援端末にログオンする。
⑬ 看護師は看護実施情報を登録する。
⑭ 看護師はログオフする。

＜SSO の必要性に関する考察＞

- 利用するシステムは２つである。
- 看護支援端末と電子カルテ端末は同一である。
- 利用する端末数は少なく、通常は数台の端末を複数の操作者が使いまわしている。
- 看護指示受け作業の業務の流れの１つとして電子カルテシステムを使用した看護指示内容の確認作業があり、看護支援システムにログオンした ID で電子カルテシステムへもシームレスにログオンできると利便性が高まる。

6.2.3.ユースケース２　放射線医師による読影

＜前提条件＞

- 医師は PACS 端末で検査実施を確認する。
- 検査情報は放射線科情報システムに存在し、詳細な情報は放射線科情報システムを参照する。
- 患者情報は HIS に存在し、詳細な情報は HIS を参照する。
- 過去画像は PACS に保存されている。
- 過去レポートはレポートシステムに保存される。
- PACS とレポートシステムは同一端末で参照可能。
- レポートは最終的に HIS に送られる。

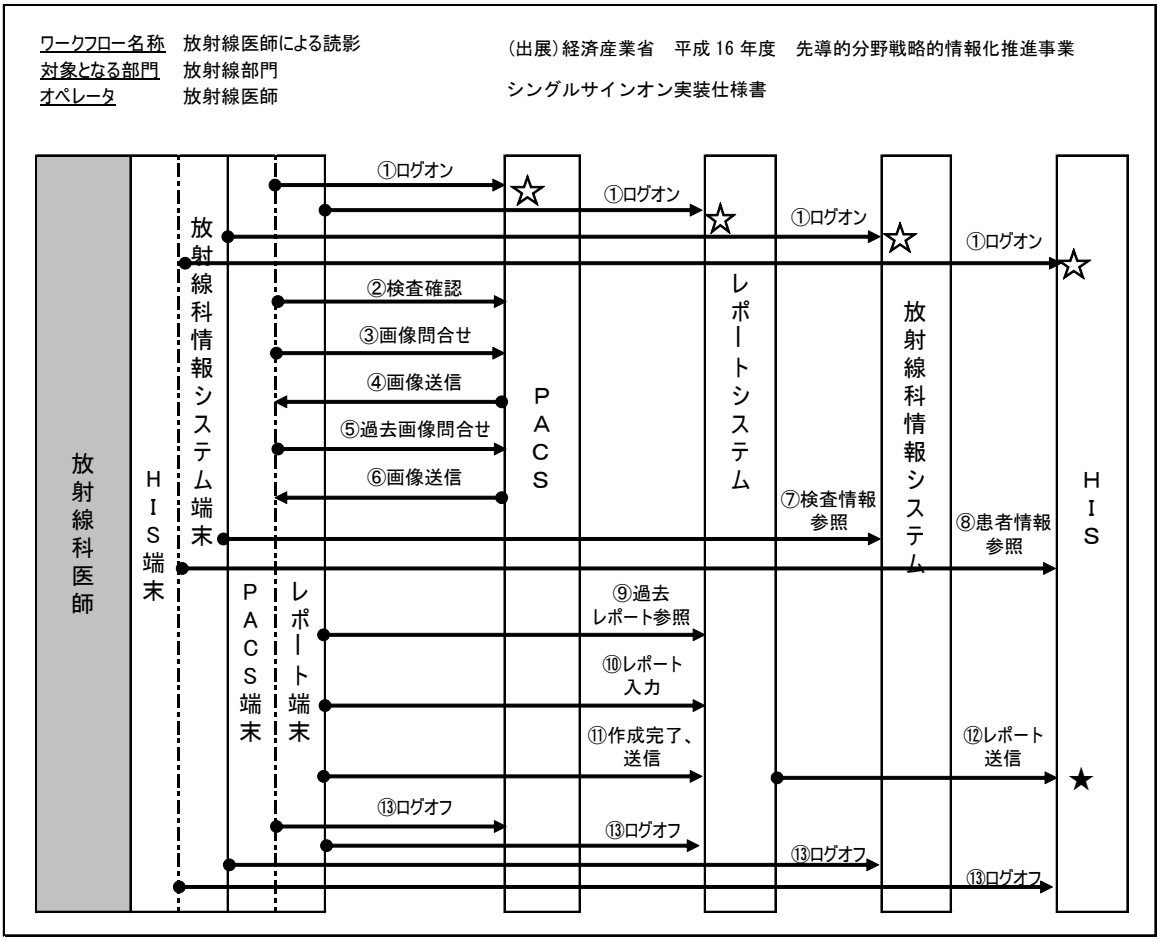


図６．２−４　放射線医師による読影ワークフロー

＜業務の流れ＞

① PACS、レポートシステム、放射線システム、HIS にログオンする。
② PACS で検査実施を確認する。
③ PACS に画像を問い合わせる。
④ PACS から画像が送信される。
⑤ PACS に過去画像を問い合わせる。

⑥ PACS から過去画像が送信される。
⑦ 放射線科情報システムに詳細な検査情報を参照する。
⑧ HIS に詳細な患者情報を参照する。
⑨ レポートシステムに過去レポートを参照する。
⑩ レポートを入力する。
⑪ レポート作成完了し、HIS への送信を指示する。
⑫ レポートシステムから HIS へレポートが送信される。
⑬ 一日の検査が終了後あるいは離席時に、PACS、レポートシステム、放射線科情報システム、HIS からログオフする。

＜SSO の必要性に関する考察＞

- 利用するシステムは４つである。
- PACS 端末とレポート端末は同一、放射線科情報システム端末と HIS 端末は同一である。
- 通常は１台の端末を複数の操作者が使い回す。
- それぞれのシステムにはログオン操作が必要であり、利用者の ID で行われる。
- PACS、レポートシステム、放射線科情報システム、HIS へのログオンは SSO が適用されると利便性が向上すると考えられる。
- これを操作者の ID カードを挿すだけのような簡便な形態で SSO を実現することで、運用管理のレベルを向上させることが可能になる。

6.2.4.ユースケース３　放射線治療を行う医師による治療計画立案と照射準備

＜前提条件＞

- 治療計画装置、シミュレータ、治療装置のある部屋において各装置の端末を操作する。
- その際に、治療 RIS、画像、電子カルテの情報を参照する必要がある。
- 各装置の操作は複数日に渡って行われることがある。

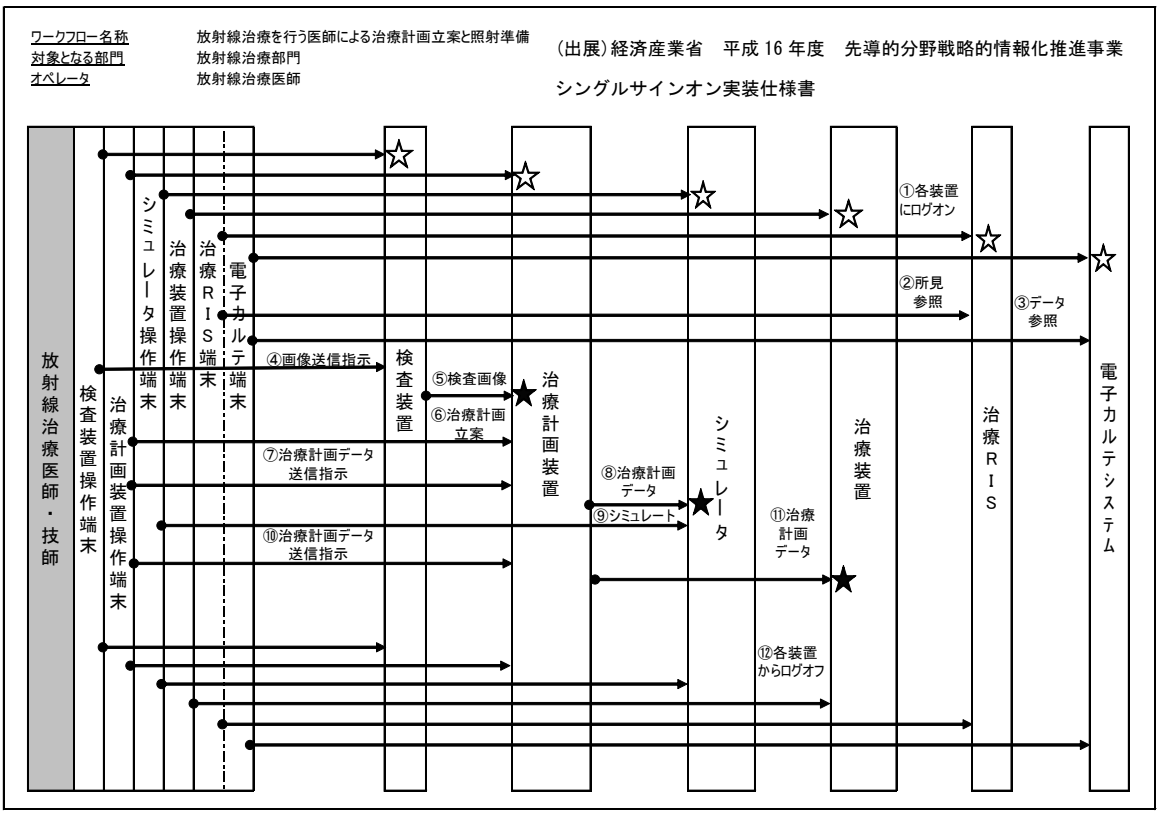


図６．２−５　放射線治療を行う医師による治療計画立案と照射準備ワークフロー

＜業務の流れ＞

① 治療計画立案のため、各装置にログオンする。
② 治療 RIS にて所見を参照する。
③ 電子カルテにてデータを参照する。
④ 検査装置に治療計画用の検査画像の送信を指示する。
⑤ 検査装置より治療計画用の検査画像を送信する。
⑥ 治療計画をデータ入力する。
⑦ 治療計画装置に治療計画データのシミュレータへの送信を指示する。
⑧ 治療計画装置がシミュレータに治療計画データを送信する。
⑨ シミュレータに治療計画内容のシミュレーションを指示する。
⑩ 治療計画装置に治療計画データの治療装置への送信を指示する。
⑪ 治療計画装置より治療装置に治療計画データを送信する。
⑫ 各装置からログオフする。

＜SSO の必要性に関する考察＞

- 一人の操作者が扱う多数の操作端末と対象データサーバが存在する。
- 専用機能の装置操作には似通った表示がなされる。
- 誤操作防止のため利用装置の明示的な認識が必要であること、また表示情報量が多いため、操作端末を兼用することはない。
- このため、使用頻度の高い装置に対し、SSO 導入の需要は少ないものと思われる。
- 情報系システムの２サーバに対する SSO は有用性があると思われる。

6.2.5.ユースケース４　生理検査判読

＜前提条件＞

- 検査オーダがあり、患者の主訴、外来所見が記録されている。
- 検査が完了し、結果が参照できる状態にある。

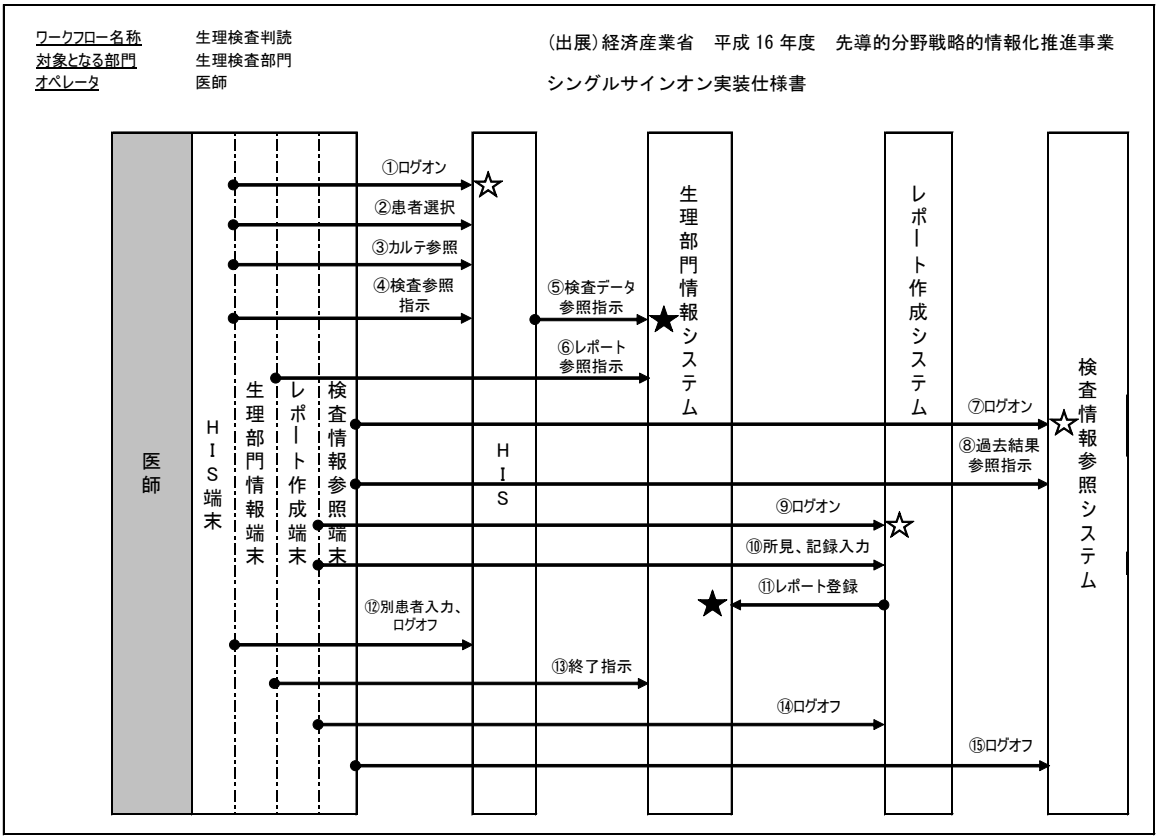


図６．２−６　生理検査判読ワークフロー

＜業務の流れ＞

① HIS にログオンする。
② 患者を選択する。
③ 問診、主査、所見、アレルギー、禁忌、バイタルなどカルテを参照する。
④ 過去検査の参照の指示を行う。
⑤ HIS から生理部門情報システムを起動し、検査データを参照する。
⑥ ⑤で起動した生理部門情報システムにて過去検査レポートを参照する。
⑦ 過去の検査結果を見るために検査情報参照端末にログオンする。

⑧ 過去の検査結果を参照する。
⑨ 検査レポートを作成するため、レポート作成システムにログオンする。
⑩ カルテの内容、今回行った検査結果、過去データから検査の所見をレポート作成端末に入力する。
⑪ レポート作成システムから生理部門情報システムへレポートを送信し登録する。
⑫ 別の患者を選択するか、検査を終了するため HIS からログオフする。
⑬ HIS から起動した生理部門情報システムを終了する。
⑭ レポート作成端末からログオフする。
⑮ 検査情報参照端末からログオフする。

＜SSO の必要性に関する考察＞

- 利用するシステムは４つである。
- 利用する端末数は少なく、通常は１台の端末を医師、技師が共用する。
- それぞれのシステムにはログオン操作が必要であるが、検査レポートの表示には HIS から部門への呼出しボタンによる電文連携で行われる運用が多い。
- 判読目的の HIS 端末から生理部門情報システムへのログオンは固定的であり、明示的に行われるケースはあまり多くないと思われる。
- 検査情報参照システムと HIS は独立しており、パスワード管理は個別に行うか、電文通信で行うことが多い。
- この運用では上記⑤及び⑪のような過程で情報の参照者、登録者がシステム間で明確に伝達されない傾向があり、運用管理上好ましくない。
- これを操作者の ID カードを挿すだけのような簡便な形態で操作者を特定して認証を実現することで、運用管理のレベルを向上させることが可能になる。

6.2.6.ユースケース５　外来診察前準備

＜前提条件＞

- 前回の診察時に画像撮影オーダ依頼が出されている。
- 撮影が完了し、画像参照ができる状態にある。
- 読影が完了し、レポートが参照できる状態にある。
- 医師はカルテ画面の画像オーダ履歴より、撮影された画像もしくは読影レポートを呼び出す。

＜ワークフロー＞

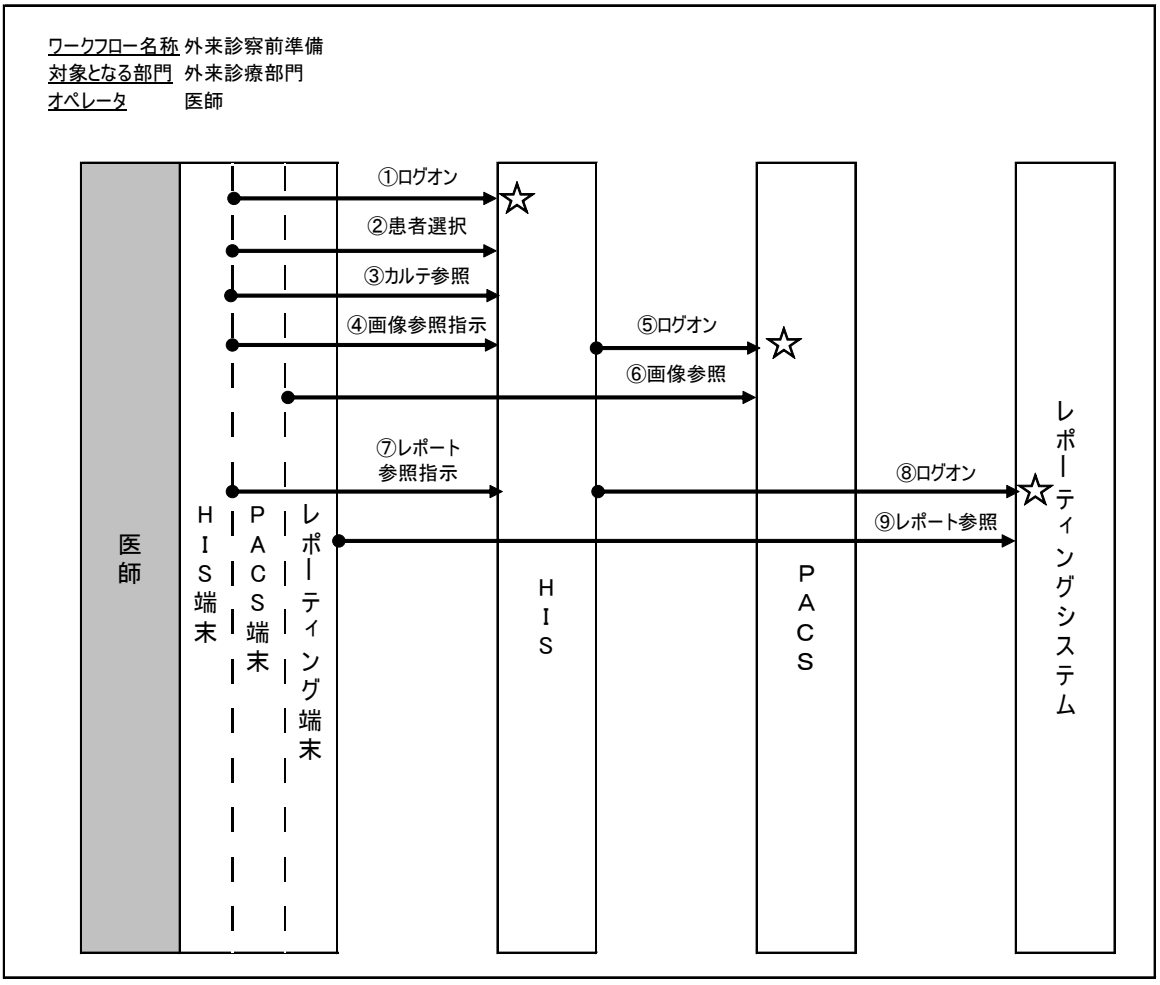


図６．２−７　外来診察前準備ワークフロー

＜業務の流れ＞

① 医師は電子カルテシステムにログオンする。
② 医師は自分の担当の診察待ち患者リストから対象の患者を選択する。
③ 医師は過去のカルテ内容を確認する。
④ 医師は電子カルテシステムの画像検査結果参照ボタンを押下する。
⑤ 電子カルテシステムから PACS システムが起動し、ログオンする。その際、患者 ID、画像検査オーダ番号が受け渡される。

⑥ 電子カルテシステム端末上に、PACS システムの画像参照画面が開き、該当の画像が表示される。
⑦ 医師は電子カルテシステムのレポート参照ボタンを押下する。
⑧ 電子カルテシステムからレポーティングシステムが起動し、ログオンする。その際、患者 ID、オーダ番号が受け渡される。
⑨ 電子カルテシステム端末上に、レポーティングシステムのレポート参照画面が開き、該当のレポートが表示される。

＜SSO の必要性に関する考察＞

- 利用するシステムは３つである。
- 電子カルテ端末とＰＡＣＳ端末、レポーティング端末は同一である。
- 利用する端末はほぼ医師専用の端末が用意される。
- 診察前準備の業務の流れの 1 つとして PACS システムを使用した画像参照、レポーティングシステムを使用したレポート参照があり、それぞれのシステムに SSO を適用することで、シームレスなアクセスが可能になる。

6.2.7.ユースケース６　手術開始から終了まで

＜前提条件＞

- 該当患者に対して電子カルテシステムで手術オーダが発行されている。
- 該当患者の輸血情報は輸血システムへ登録されている。
- 該当患者の手術オーダ情報は電子カルテシステムから麻酔記録システムへ転送されている。

＜ワークフロー＞

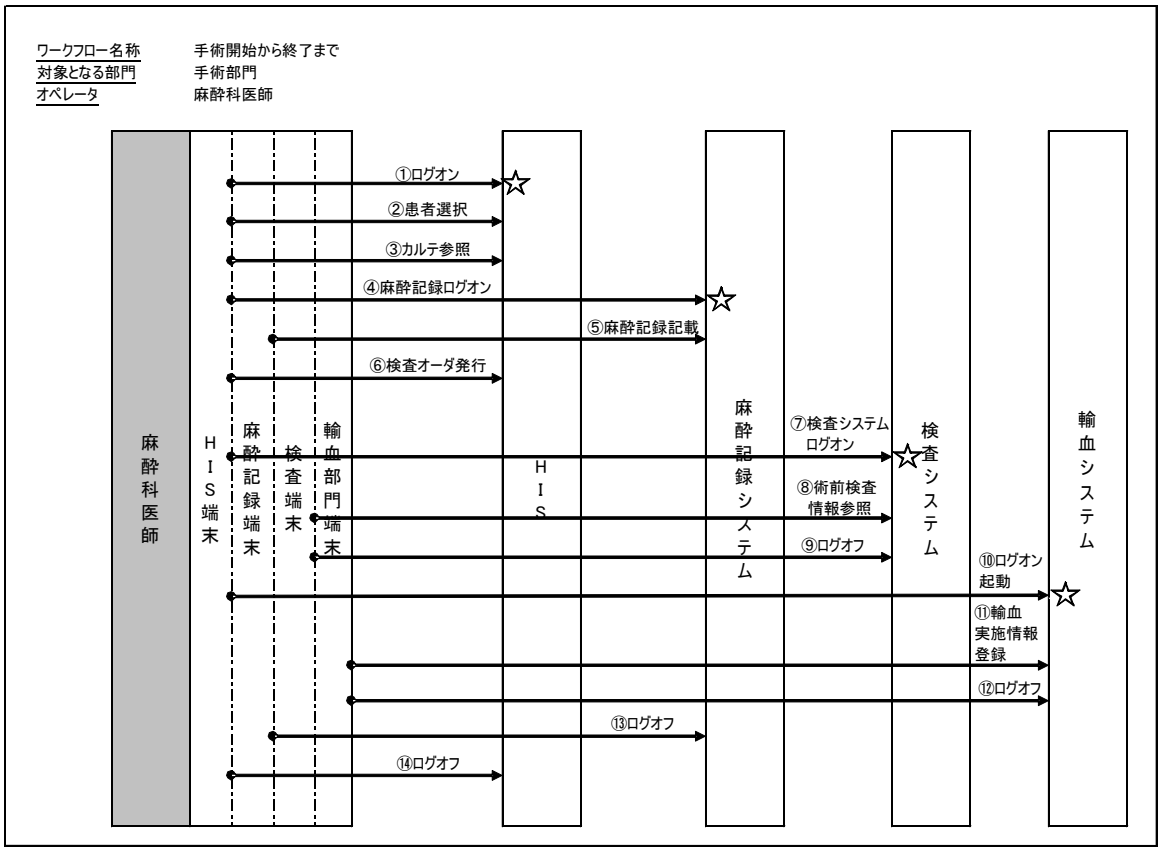


図６．２−８　手術開始から終了までのワークフロー

＜業務の流れ＞

① 麻酔科医師は HIS へログオンする。
② 患者を選択する。
③ 問診、所見、術前確認など電子カルテを参照する。
④ 作業中の HIS 端末より麻酔記録システム起動（ログオン）する。この際に HIS で HIS へのログオンユーザ ID、選択された患者 ID が麻酔記録システムへ渡される。
⑤ 挿管、ルート、薬剤、輸液などの術中麻酔情報を麻酔記録システムへ登録する。
⑥ 術中検査用の検査オーダを HIS へ発行する。
⑦ 作業中の HIS 端末より検査システム起動（ログオン）する。この際に HIS で HIS へのログオンユーザ ID、選択された患者 ID が検査システムへ渡される。
⑧ 術前検査情報を参照する。
⑨ 検査システムを終了（ログオフ）する。

⑩　作業中 HIS 端末より輸血システム起動（ログオン）する。この際に HIS で HIS へのログオンユーザ ID、選択された患者 ID が輸血システムへ渡される。
⑪　輸血システムへ輸血の実施情報の登録を行う。
⑫　輸血システムを終了（ログオフ）する。
⑬　麻酔記録システムを終了（ログオフ）する。
⑭　HIS を終了（ログオフ）する。

＜SSO の必要性に関する考察＞

- 利用するシステムは４つである。
- 全てのシステムは単一の端末上で運用している。
- 端末は麻酔器に搭載されている。
- 麻酔科医は手術中、麻酔器、該当患者から離れることはなく、麻酔に関する全ての情報の閲覧、入力が出来なくてはならないため、これらのシステムに SSO を適用することで、シームレスなアクセスが可能となる。

6.3. 実装モデル

ここでは６．２節で例示したユースケースから３つを選び、５．２節で紹介した SSO の仕組みを適用して、利用者の操作を簡略化するモデルを示す。読者には、６．２節に記述のある同名のユースケースの業務の流れを参照しながら、SSO を適用することで、どのように業務の流れが簡略化されるかを追いかけていただきたい。

6.3.1.実装モデル１　生理検査判読

6.2.5 で示したユースケース：生理検査判読の実装モデルについて例示する。

＜前提条件＞

（１）SSO 方式

代理ログオン方式

（２）利用者マスタ

以下のいずれかを満たしている。

- 各システムの利用者マスタと同期されている。
- 全システムの利用者情報が登録されおり、各システムの利用者マスタとのマッピングテーブルを持つ。

（３）構成システム

HIS	：レガシーシステム
生理部門情報システム	：レガシーシステム
レポート作成システム	：レガシーシステム
検査情報参照システム	：Web システム

（４）システム起動／認証方式

- レガシーシステムの場合、予めベンダー間で取り決められた I/F で起動および認証を行う機能を持つ。
- Web システムの場合、HTTP 通信（GET または POST）により予めベンダー間で取り決められた I/F で起動および認証を行う機能を持つ。

＜SSO 実装＞

（１）　HIS へのログオン

- 利用者（医師）は HIS へ一度だけログオン操作を行う。
- HIS は利用者が提供した利用者情報で認証を行う。
- 認証後、利用者識別子に従って、使用可能な機能の確認が行われる。
- 患者選択、カルテ参照動作は HIS に依存する。

（２）　生理部門情報システムへのログオン

- 利用者の検査データ参照操作により、HIS から生理部門情報システムが起動される。その際、利用者情報と検査データのキー情報が受け渡される。
- 生理部門情報システムは HIS から受け取った利用者情報で認証を行った後、検査データのキー情報を基に検査データを表示する。
- 過去レポートの参照動作は、生理部門情報システムに依存する。

（３）　検査情報参照システムへのログオン

・ 利用者の検査結果参照操作により、HIS から WEB ブラウザを使用して検査情報参照システムが起動される。その際、利用者情報と過去検査結果のキー情報が受け渡される。
・ 検査情報参照システムはブラウザから受け取った利用者情報で認証を行った後、過去検査結果のキー情報を基に検査結果を表示する。

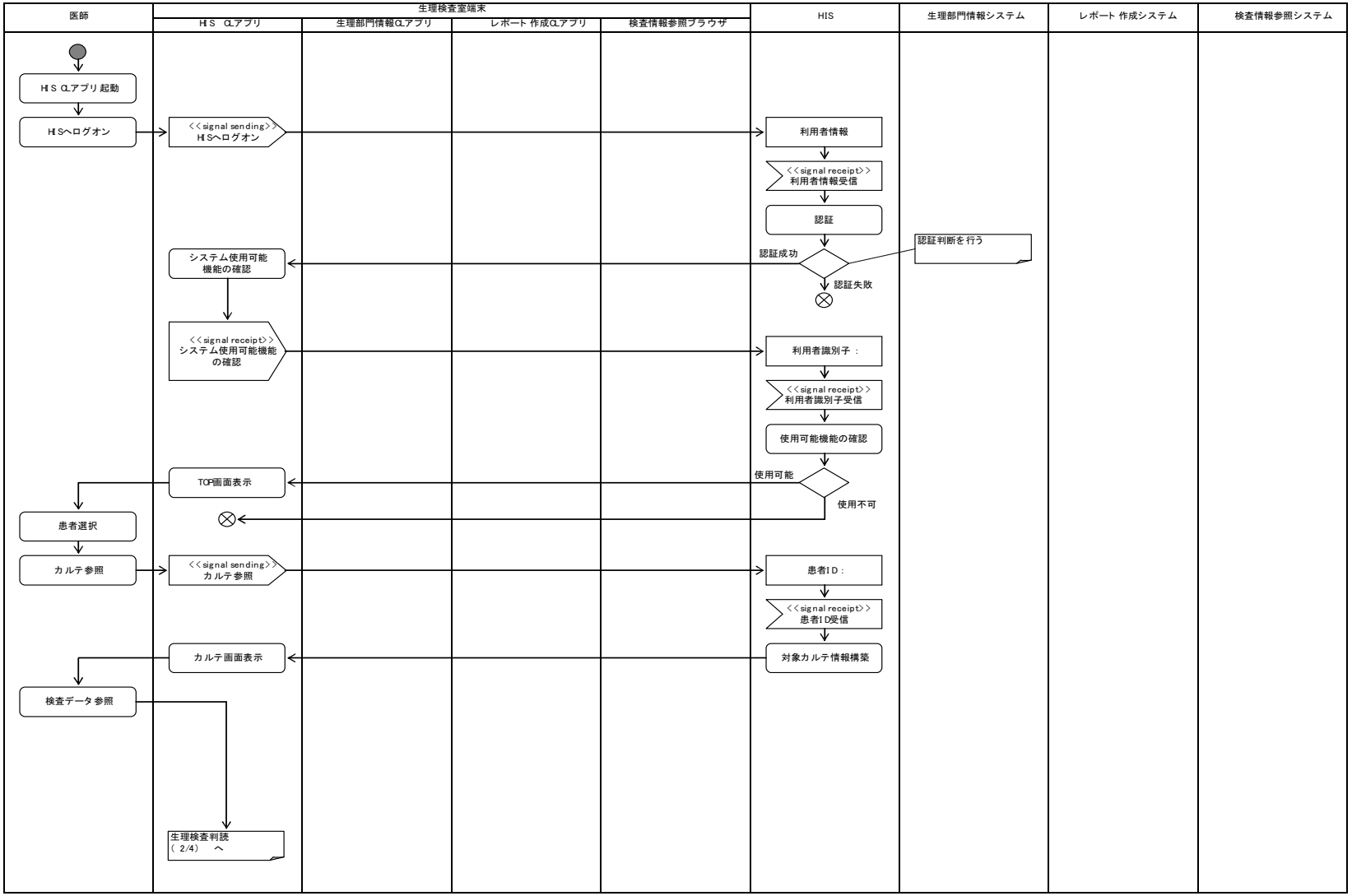
（4） レポート作成システムへのログオン
・ 利用者のレポート作成操作により、HIS からレポート作成システムが起動される。その際、利用者情報とレポートのキー情報が受け渡される。
・ レポート作成システムは HIS から受け取った利用者情報で認証を行った後、レポートのキー情報を基にレポート作成画面を表示する。
・ レポートの作成および登録はレポート作成システムに依存する。

（5） レポート作成システムから生理部門情報システムへのレポート登録
・ レポート作成システムにレポートが登録された後、自動的に生理部門情報システムへレポートが登録される。
・ レポートの登録は電文通信で行われ、ログオン処理は行われない。

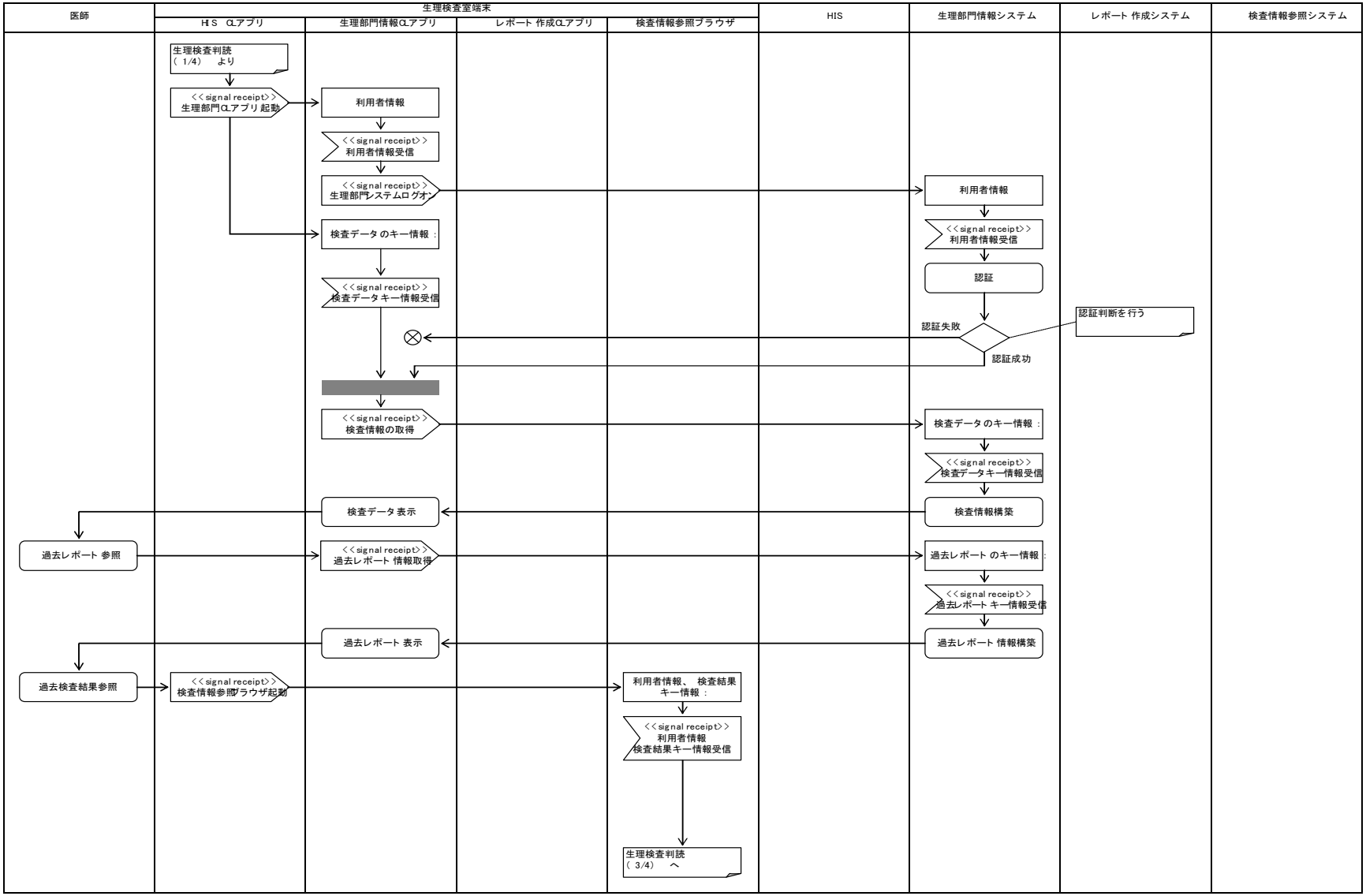
＜アクティビティ図＞

生理検査判読の実装モデルの例を UML のアクティビティ図で示す。

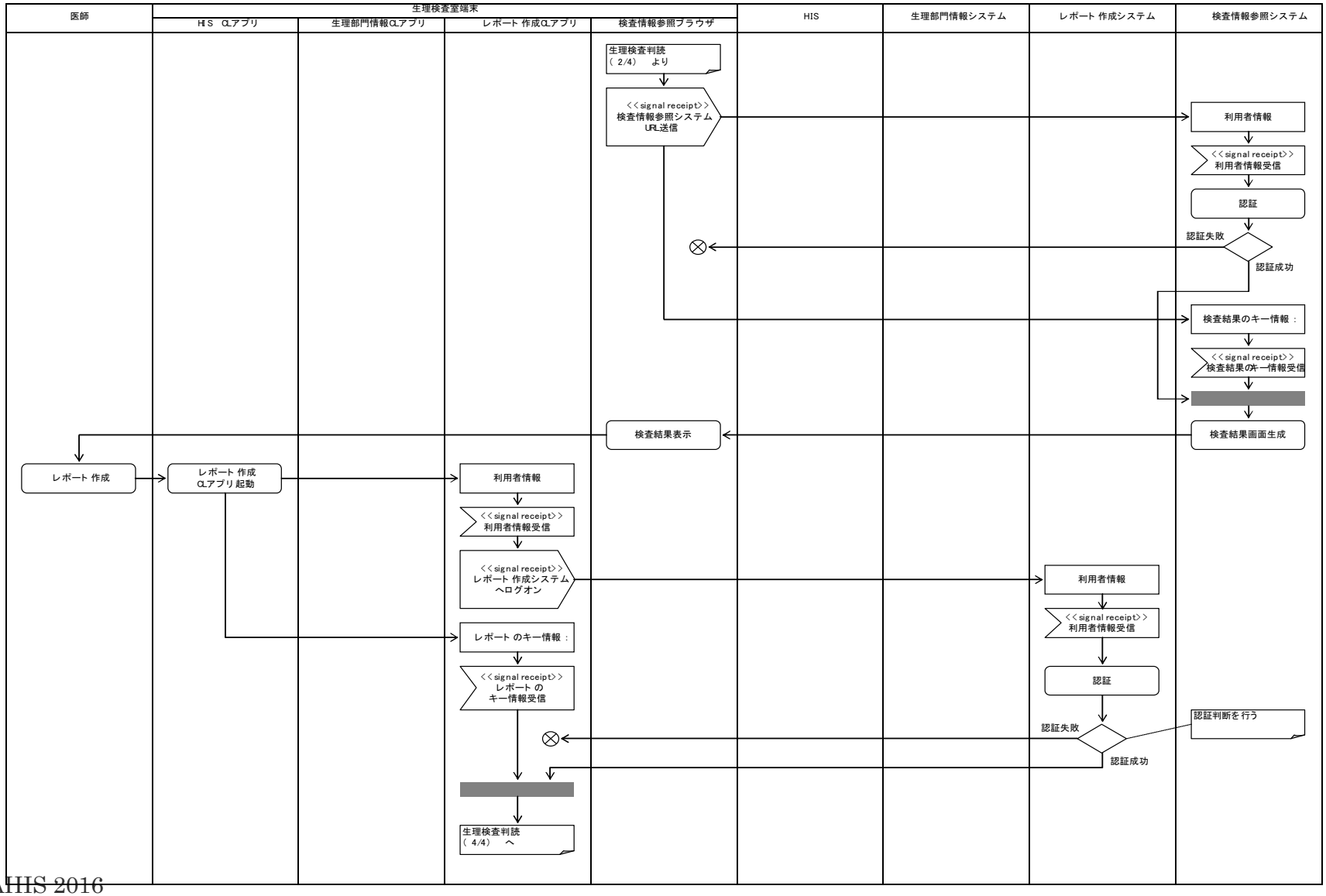
生理検査判読：アクティビティ図（１／４）



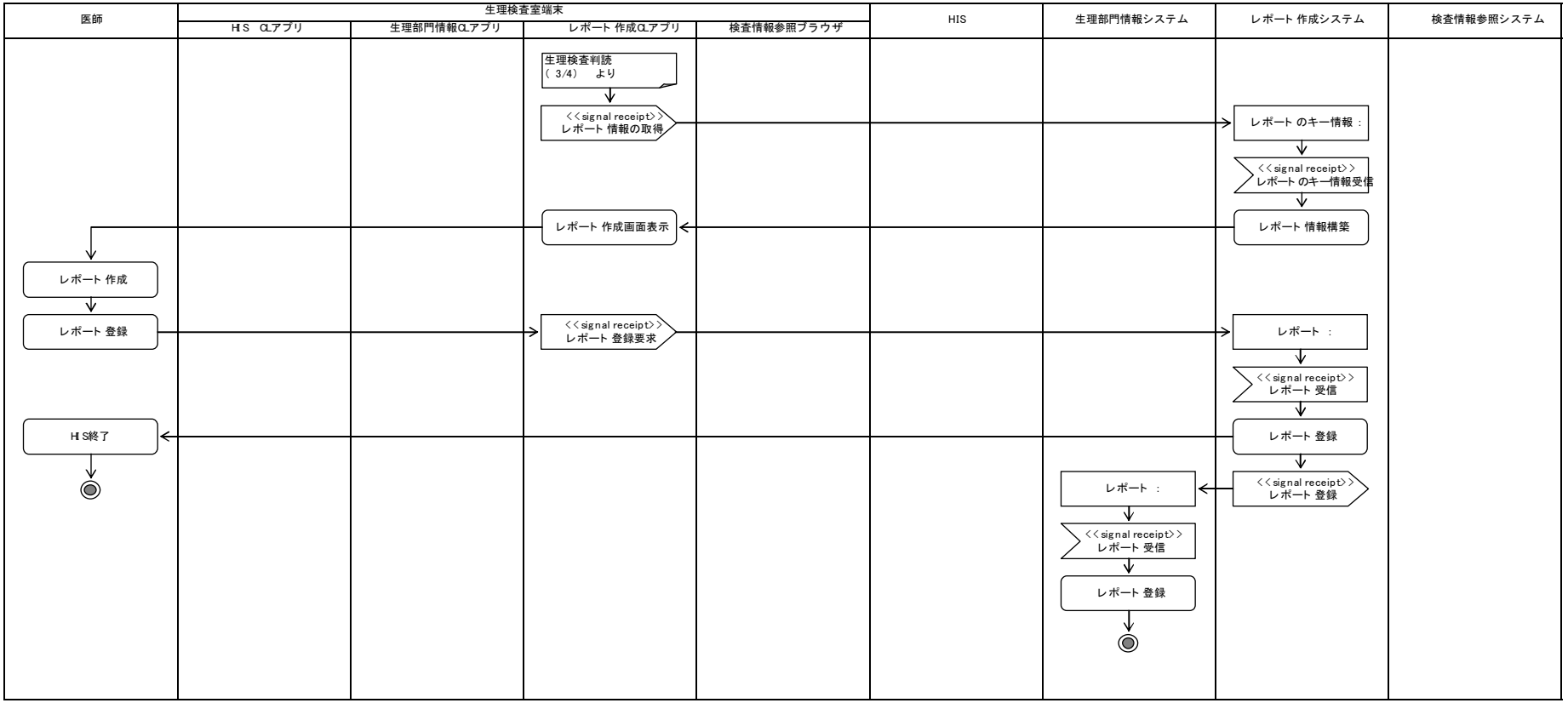
生理検査判読：アクティビティ図（２／４）



生理検査判読：アクティビティ図（３／４）



生理検査判読：アクティビティ図（４／４）



6.3.2.実装モデル２　外来診察前準備

6.2.6 で示したユースケース：外来診察前準備の実装モデルについて例示する。

＜前提条件＞
（1）SSO 方式
Kerberos 方式

（2）利用者マスタ
以下の条件を満たしている。
- Windows Server 上の Active Directory サービス(AD サービス)で管理されている。

（3）構成システム

HIS	: レガシーシステム
PACS	: レガシーシステム
レポート参照システム	: Web システム

（4）システム起動／認証方式
- レガシーシステムの場合、Kerberos 認証要求可能なモジュールを包含し、起動時に認証を行う。
- Web システムの場合、サーバへの HTTP 通信後 Kerberos 認証用のネゴシエーションにより認証を行い、サーバへアクセスする。

＜SSO 実装＞
（1）OS(Windows)へのログオン
- 利用者（医師）は OS(Windows)へログオン操作を行う。
- Windows Server の AD サービスが KDC の AS として機能し、認証を実施する。
- 認証成功となった場合、端末に TGT を渡す。

（2）HIS へのログオン
- 利用者は HIS クライアントを起動する。
- HIS クライアントは KDC の TGS に対して、TGT と要求サービスを渡す。
- TGS は要求サービスを判別し、HIS 用のサービスチケットを HIS クライアントに渡す。
- このチケットを用いて、HIS クライアントは HIS サーバにアクセスする。
- 利用者は HIS クライアントを操作し、患者を選択後、カルテを参照する。

（3）PACS へのログオン
- 利用者は PACS クライアントを起動する。
- PACS クライアントは KDC の TGS に対して、TGT と要求サービスを渡す。
- TGS は要求サービスを判別し、PACS 用のサービスチケットを PACS クライアントに渡す。
- このチケットを用いて、PACS クライアントは PACS サーバにアクセスする。
- 利用者は PACS クライアントを操作し、患者画像を選択後、画像を参照する。

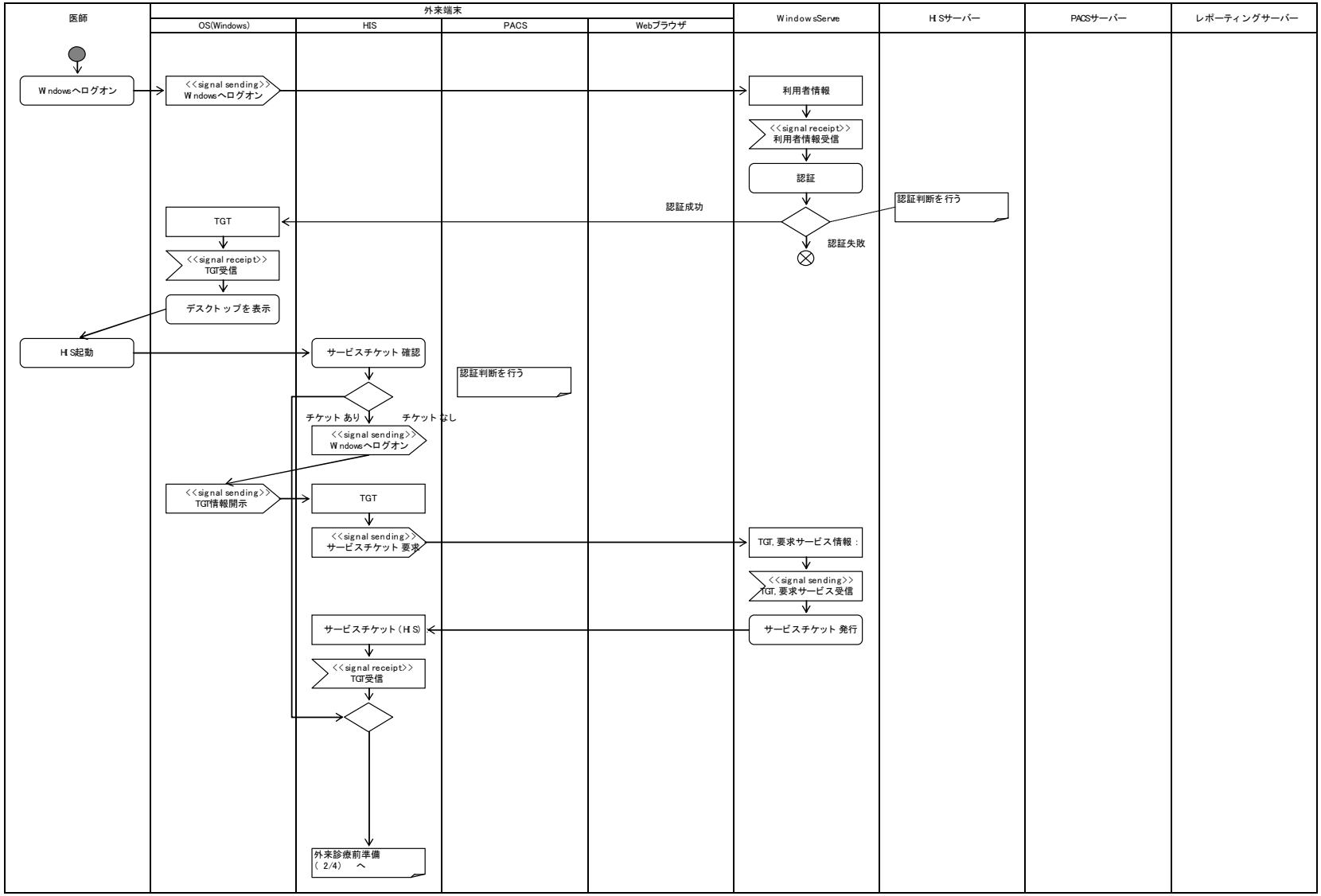
（4）レポート参照システムへのログオン
- 利用者は Web ブラウザからレポート参照システムの URL を入力することにより、レポーティングサーバにアクセス要求を行う。

- レポーティングサーバは認証ネゴシエーション要求を Web ブラウザに返す。
- Web ブラウザは要求サービスと TGT を KDC の TGS に渡す。
- TGS は要求サービスを判別し、レポーティングシステム用のサービスチケットを Web ブラウザに返す。
- Web ブラウザは得られたチケットを用いてレポーティングシステムにアクセスする。
- 利用者は Web ブラウザを操作し、患者レポートを選択後、レポートを参照する。

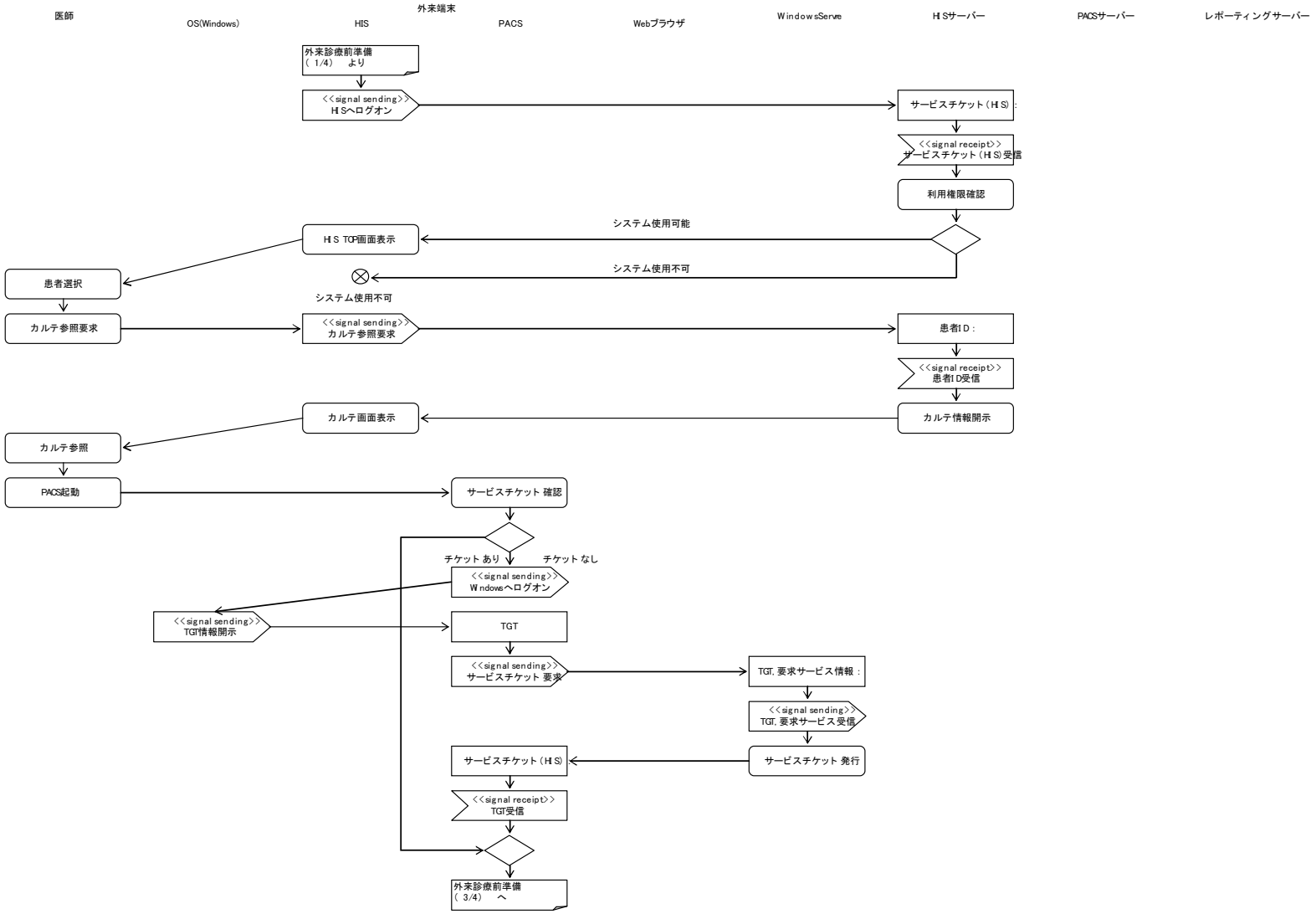
＜アクティビティ図＞

外来診察前準備の実装モデルの例を UML のアクティビティ図で示す。

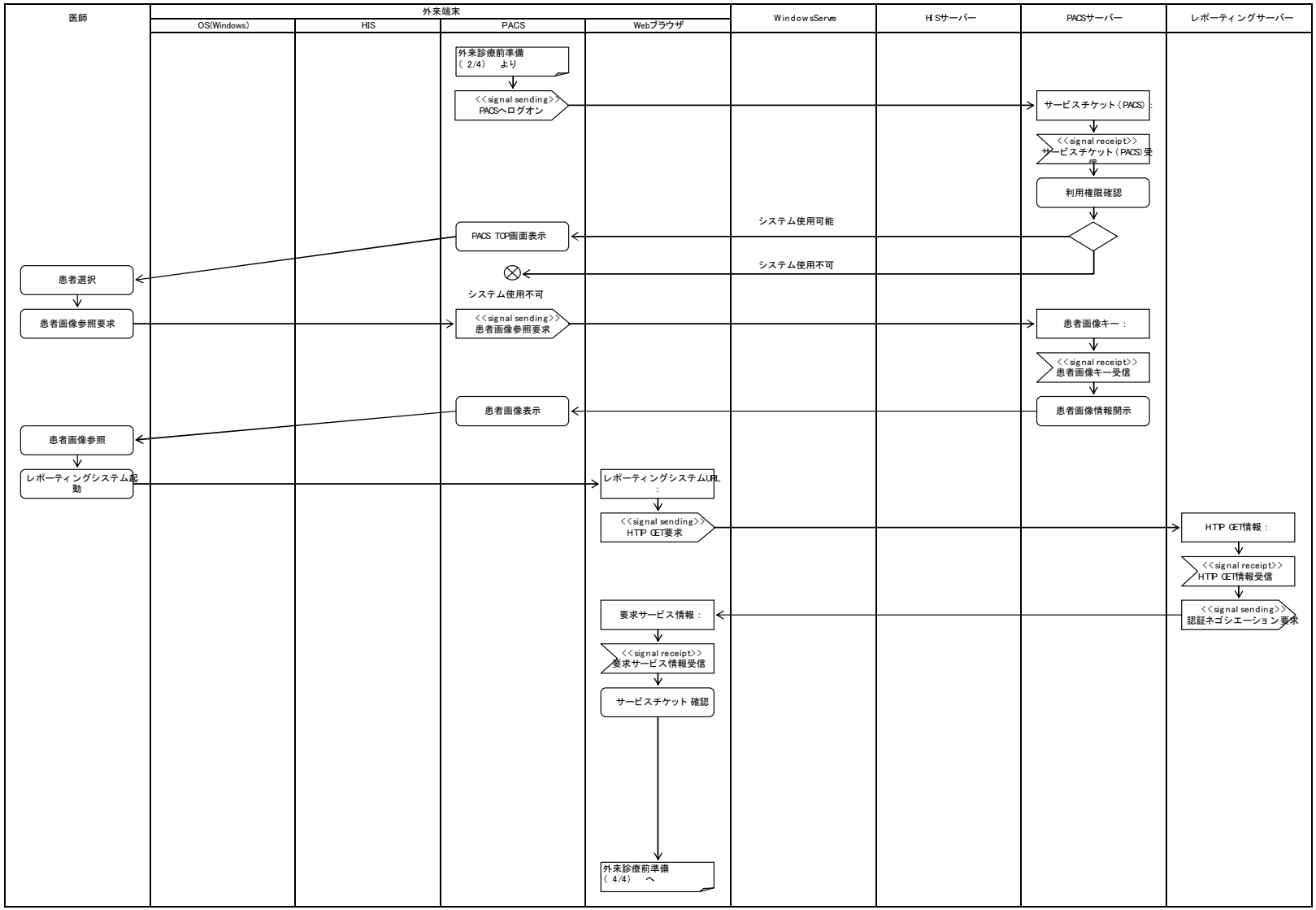
外来診察前準備：アクティビティ図（１／４）



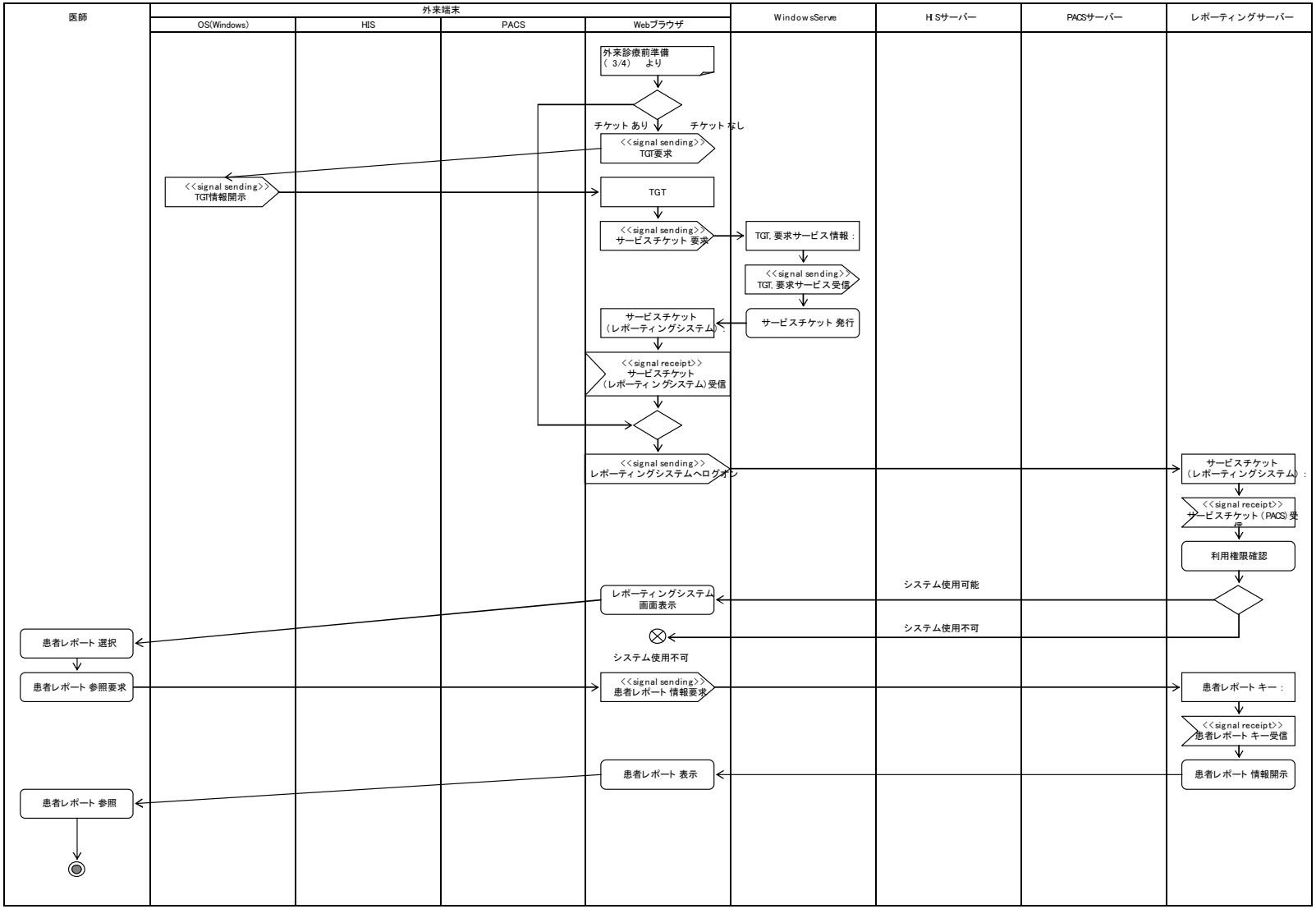
外来診察前準備：アクティビティ図（２／４）



外来診察前準備：アクティビティ図（３／４）



外来診察前準備: アクティビティ図(4 ／ 4)



6.3.3.実装モデル３　手術開始から終了まで

6.2.7 で示したユースケース：手術開始から終了までの実装モデルについて例示する。

＜前提条件＞

（1）SSO 方式

代理ログオン方式（権限管理は各システムにて保持）

（2）利用者マスタ

以下の要件を満たしている。

- 各システムの利用者マスタと利用者識別子が同期されている。
- 全システムの利用者情報が登録されおり、各システムの利用者マスタとのマッピングテーブルを持つ。

（3）構成システム

HIS	：レガシーシステム
検査システム	：レガシーシステム
麻酔記録システム	：レガシーシステム
輸血システム	：レガシーシステム

（4）システム起動／認証方式

- 運用開始時にHISをフロントエンドとして認証サーバに対して利用者情報の認証を行う。
- 各システムは、HIS より起動され、利用者識別子をキーとして各サービスの利用権限を判断する。

＜SSO 実装＞

（1）HIS へのログオン

- 利用者（医師）は HIS へ一度だけログオン操作を行う。
- HIS は利用者が提供した利用者情報を認証サーバへ送信し認証を行う。
- 認証後、利用者識別子に従って、使用可能な機能の確認が行われる。
- 患者選択、その後の動作は利用者識別子をキーに HIS を起点に行う。

（2）麻酔記録システムへのログオン

- 利用者の麻酔記録起動操作により、HIS から麻酔記録システムが起動される。その際、利用者識別子と手術オーダ情報が受け渡される。
- 手術部門システムはHISから受け取った利用者識別子をキーに利用可能機能の確認を行い、手術オーダ情報を基に麻酔記録情報を表示する。
- 麻酔記録上の動作は、麻酔記録システムに依存する。
- 麻酔記録システム終了処理は麻酔記録システムに依存し、認証サーバへのログオフ通知は行わない。

（3）検査システムへのログオン

- 利用者の検査システム起動操作により、HIS から検査システムが起動される。その際、利用者識別子と手術オーダ情報が受け渡される。
- 検査システムはHISから受け取った利用者識別子で利用可能機能の確認を行った後、手術オーダ情報を基に検査結果を表示する。
- 検査情報の参照機能は検査システムに依存する。

- 検査システム終了処理は検査システムに依存し、認証サーバへのログオフ通知は行わない。

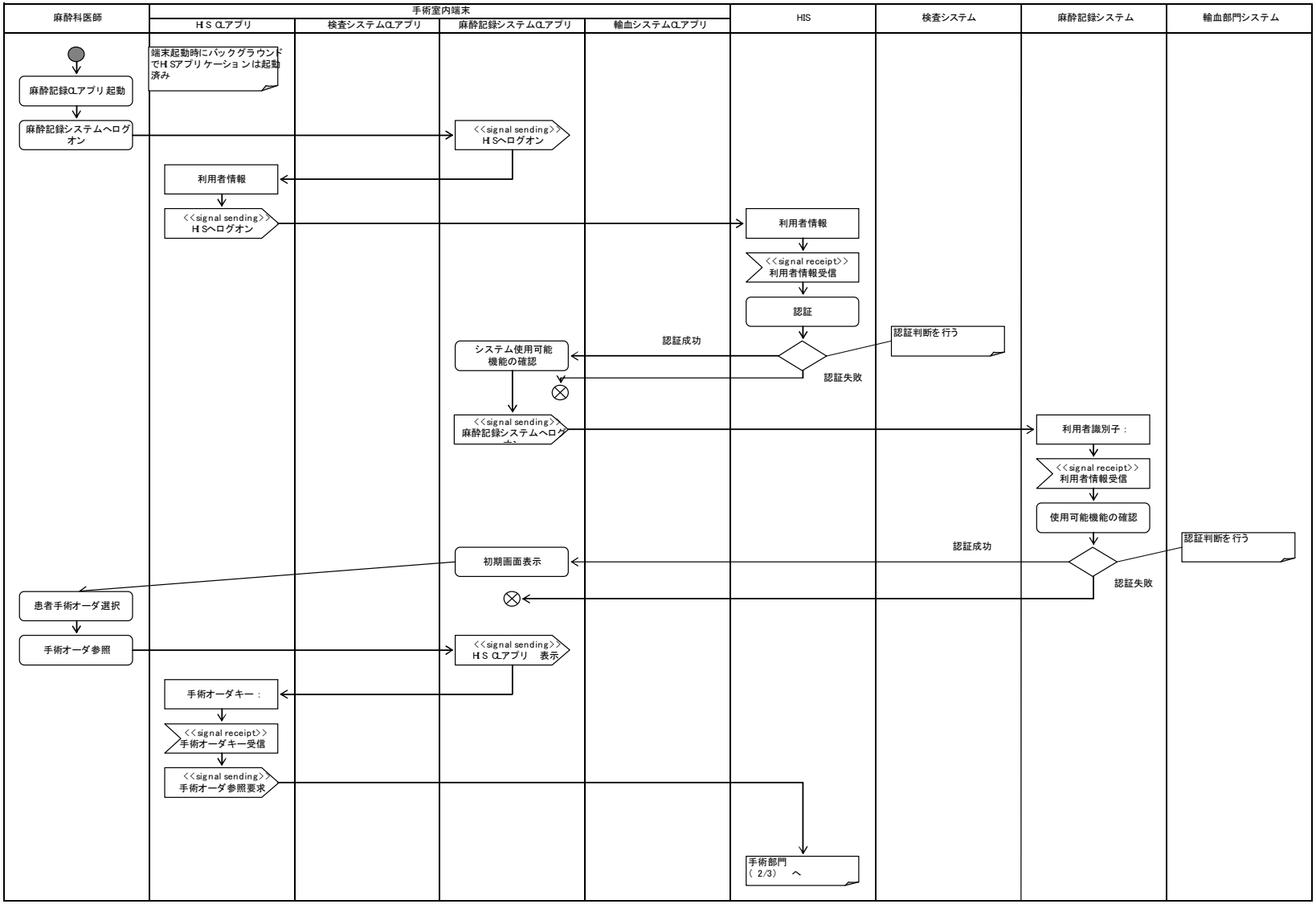
（4）輸血システムへのログオン

- 利用者の輸血システム起動操作により、HIS から輸血システムが起動される。その際、利用者識別子と手術オーダ情報が受け渡される。
- 輸血システムはHISから受け取った利用者識別子で利用可能機能の確認を行った後、手術オーダ情報を基に輸血登録情報を表示する。
- 輸血情報の参照及び登録は輸血システムに依存する。
- 輸血システム終了処理は輸血システムに依存し、認証サーバへのログオフ通知は行わない。

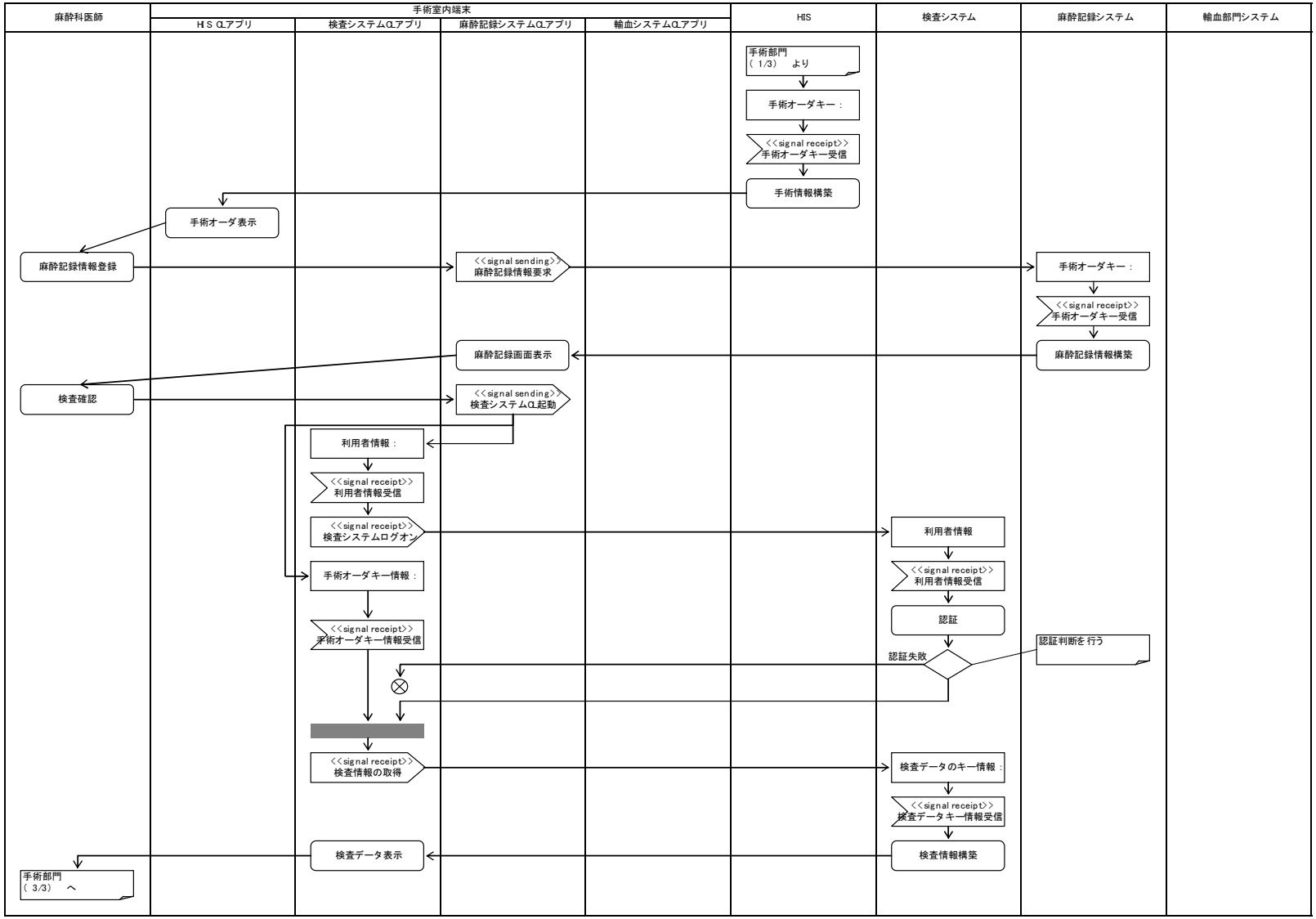
＜アクティビティ図＞

手術開始から終了までの実装モデルの例を UML のアクティビティ図で示す。

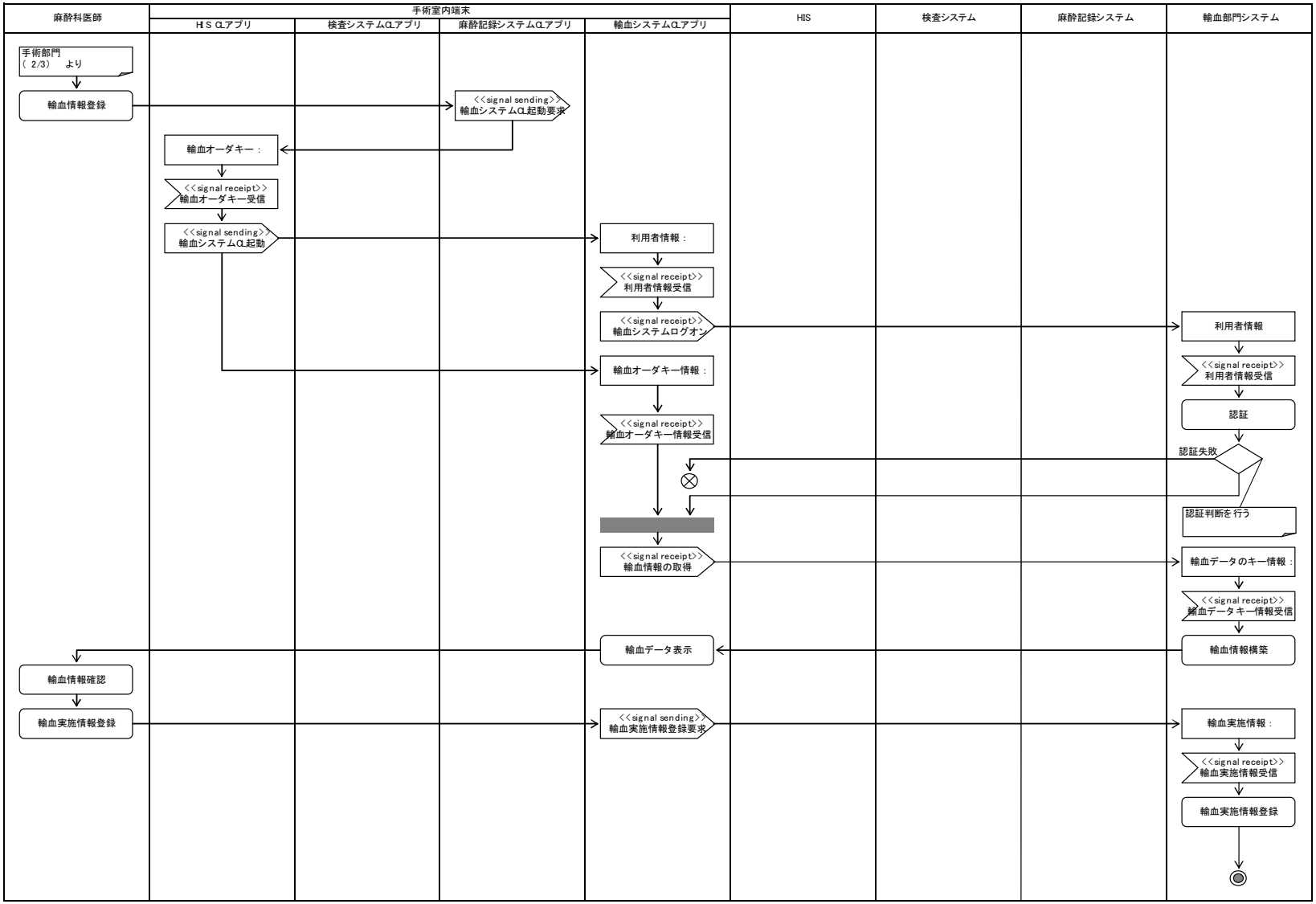
手術開始から終了まで: アクティビティ図（１／３）



手術開始から終了まで: アクティビティ図（２／３）



手術開始から終了まで: アクティビティ図(3 ／ 3)



7. 医療分野のシングルサインオンにおけるセキュリティマネジメント

7.1. 法的なセキュリティ要件

セキュリティマネジメントを行う際の外部要件として、国の制度上の要求事項を遵守することは必須要件である。医療情報システムを取り扱う際に遵守すべきガイドラインとして、厚生労働省が「安全管理ガイドライン第 4.2 版」を平成 25 年 10 月にリリースしている。SSO を実施するにあたっても本ガイドラインの遵守は必須である。また、その上位ガイドラインである、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（平成 22 年 9 月改正　厚生労働省）や個人情報保護法と呼ばれている、「個人情報の保護に関する法律」（平成 15 年法律第 57 号、平成 17 年 4 月全面施行）の理解が前提にあることは言うまでもない。

上記「安全管理ガイドライン」は医療機関が総合的な管理策を実施したうえで実現されるものであるため、医療情報システムベンダーが提供する SSO のシステムにおいてすべての要求事項に技術的対策を施すことが義務付けられているわけではない。しかしながら、システム側でより適切な技術的対策を施すことで、医療機関側の技術的対策以外の対策にかかるコストを低減することが可能になることから、コストバランスを踏まえた最適化されたシステムを構築することが望まれる。

7.2. シングルサインオン実装に関するリスクアセスメント

7.2.1.リスクアセスメントの手法

情報セキュリティに関するリスクアセスメントには幾つかの手法があるが、SSO の実装に関するリスクアセスメントを実施するにあたり、ISMS において一般的に参照される、「IT セキュリティマネジメントのガイドライン－第 3 部 : IT セキュリティマネジメントのための手法（JIS TR X 0036-3:2001）」で定義される 4 つのリスク分析手法を考察する。

（1）ベースラインアプローチ
国内外の標準や基準をもとに対策基準を設け、チェックしていく方法。選択する標準によっては要求される対策のレベルに差がある。

（2）非形式的アプローチ
セキュリティ専門職やコンサルタントの経験や判断によりリスクアセスメントを行う方法。属人的な手法や判断に偏ることがある。

（3）詳細リスク分析
対象の情報資産に対して、「資産価値」「脅威」「ぜい弱性」「セキュリティ要件」を識別しながらリスクを評価していく方法。時間と工数がかかるが、厳密なリスク評価を行うことができる。

（4）組み合わせアプローチ
上記の方法を組み合わせて行うリスク評価の総称。特に、ベースラインアプローチと詳細リスク分析の併用が多く用いられている。

SSO 導入前と導入後のリスクアセスメントを比較するにあたり、どちらも同じ手法、同じ粒度での評価を行わなければならない。特に SSO の実装に関するリスクアセスメントでは、アプリケーションの機能やネットワーク構成等が変わることにより、個別に脅威とぜい弱性の評価を行うことが必要になるため、上記（3）の詳細リスク分析によるアプローチが望ましい。

7.2.2.シングルサインオン導入時リスクアセスメントに関する留意点

SSO の実装に関するリスクアセスメントの実施にあたり、SSO 導入前と比較して不必要となる情報資産とぜい弱性、新たに追加される情報資産と新たに考慮しなければならないぜい弱性に留意する必要がある。

（1）代理ログオン方式
ユーザの認証情報が集中保管される代理ログオンサーバが追加されることにより、各アプリケーションサーバへの認証レベルは統一されるが、可用性の担保といったシステム稼働の強化も求められる。

（a）新たに追加される情報資産の例

・ 代理ログオンサーバ

（b）新たに考慮しなければならない脅威の例
・ 代理ログオンサーバの機能停止
・ ログオン情報の一括漏えい
・ ログオン情報の不整合によるサービス利用不能

（c）新たに考慮しなければならないぜい弱性の例
・ 代理ログオンサーバにおける不要サービスの実行
・ 代理ログオンサーバにおける管理者アカウントの管理不備
・ 代理ログオンサーバと各アプリケーションサーバ間での認証情報更新のタイムラグ

（2）リバースプロキシ方式
プロキシを行う認証サーバにより、SSO 配下のすべてのアプリケーションサーバのユーザアカウントとセッション情報が一元管理されるため､ネットワーク負荷や安定したシステム稼働に考慮したシステム設計が求められる。

（a）新たに追加される情報資産の例
・ 認証サーバ（プロキシ）

（b）新たに考慮しなければならない脅威の例
・ 認証サーバ（プロキシ）の機能停止
・ 認証サーバ（プロキシ）への負荷集中によるサービス遅延
・ 認証サーバ（プロキシ）に繋がるネットワーク経路切断によるサービス停止

（c）新たに考慮しなければならないぜい弱性の例
・ 認証サーバ（プロキシ）における不要サービスの実行
・ 認証サーバ（プロキシ）における管理者アカウントの管理不備
・ 統合されたアカウント管理システムの不備
・ 統合された証跡システムの不備
・ ネットワーク負荷による可用性の低下

（3）エージェント方式
アプリケーションサーバの追加などに高いスケーラビティを持つエージェント方式では、認証サーバの安定した稼働と、認証チケットの安全な有効期間の設定が求められる。

（a）新たに追加される情報資産の例
・ 認証サーバ
・ エージェントモジュール
・ 認証チケット（セッション情報、クッキー等）

（b）新たに考慮しなければならない脅威の例
・ 認証サーバの機能停止

（c）新たに考慮しなければならないぜい弱性の例
・ 認証サーバにおける不要サービスの実行

- 認証サーバにおける管理者アカウントの管理不備
- 統合されたアカウント管理システムの不備
- 認証チケットの不適当な有効期間の長さ
- 認証チケット更新時における認証サーバへの未到達

7.2.3.シングルサインオンに関する脅威とリスクへの対応

SSO の実装により新たに追加された情報資産に対し、それぞれが潜在的にもつぜい弱性に関連するリスクとその発生頻度から、対応策を検討しなければならない。特に、SSO 導入前では発生頻度が低かったリスクが、ネットワーク型攻撃の脅威など SSO 導入後に高リスクとなるものへの対応は重要となる。

次ページ以降で実施した「シングルサインオン導入前後のリスクアセスメント」に関して、以下に基づき読み解くことにより、導入後の情報セキュリティ向上の一助を担うことが可能となる。

＜「付録－１　シングルサインオン導入前後のリスクアセスメント」の読み解き方＞

- 「7.2.1　リスクアセスメント手法」記載の「詳細リスク分析」によるアプローチにて、ISO27005 ISMS（情報セキュリティマネジメントシステム）に基づき実施している。
- 然しながら、SSO 導入前後での脅威・脆弱性を明確に把握する為に、「アクティビティ図による SSO 導入前後でのフロー差異」「SSO 導入前後での資産増減表」の二つを軸とした差分表記を採用した点が、従来の手法と大きく異なっている点である。
- その為、読者が「SSO 導入前後の資産増減表」を軸に「リスク分析表」を読み解く際は、『SSO 導入時には、リスク分析表のスコアが多いものには対策を行うべきである。（従来のリスクアセスメントとは異なり、スコアを受容ポイントまで下げることが本リスク分析結果の目的ではない）』という観点で読み解いて欲しい。

さらに、新たに考慮しなければいけない脆弱性への対策だけではなく、SSO 導入前に試算されたすべてのリスク値を見直し対策を施す（施設全体でリスクアセスメントの再整理を実施する）ことで、SSO の導入が利便性の向上のためだけではなく施設全体の情報セキュリティの向上に繋がることが期待できる。

付録－１　シングルサインオン導入前後のリスクアセスメント

シングルサインオン導入前後のリスクアセスメントは、以下のステップで実施した。

「7.2.3.シングルサインオンに関する脅威とリスクへの対応」に記載の読み解き方を参考にしながら、本ガイドライン内ユースケースで実施したリスクアセスメント結果を参考にして欲しい。

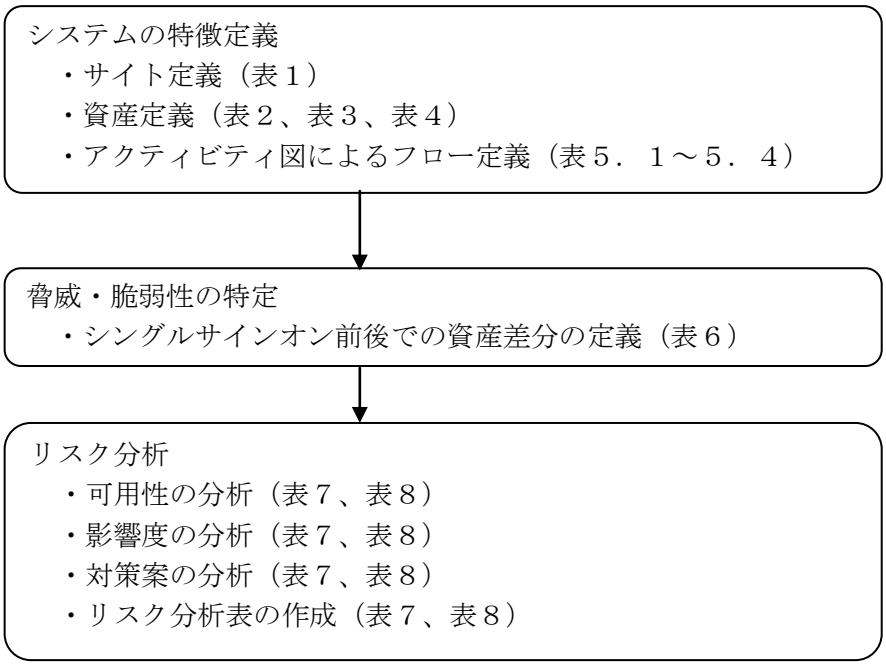


表１．シングルサインオン導入前後の「サイトと前提」

記号	サイト名	前提
A	（病院内）クライアント	「医療情報システムの安全管理に関するガイドライン」に基づき、運営されていることとする。
B1	（病院内）アプリケーションサーバ【HIS】	
B2	（病院内）アプリケーションサーバ【生理部門情報システム】	
B3	（病院内）アプリケーションサーバ【レポート作成システム】	
B4	（病院内）アプリケーションサーバ【検査情報参照システム】	
B5	（病院内）アプリケーションサーバ【PACS】	
B6	（病院内）アプリケーションサーバ【レポーティング】	
C	（病院内）認証サーバ	
D	（病院内）利用者 ID 管理サーバ&クライアント	
E	（病院内）人事給与サーバ	
F1	（病院内）ネットワーク【院内】	
F2	（病院内）ネットワーク【DMZ】	
F3	（外部）ネットワーク	
G1	（外部）認証サーバ	
G2	（外部）タイムスタンプサーバ	
G3	（外部）証明書失効リスト配布点	

記号	サイト名	前提
G4	（外部）タイムサーバ	
H1	（外部）業務サーバ	
H2	（外部）患者ディレクトリサーバ	

表２．シングルサインオン導入前後の「資産の分類」

記号	資産内容
a	メモリ・ディスク・画面上の PHI
b	暗号アルゴリズムと鍵と鍵配送方式
c	メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙
d	メモリ・ディスク・画面上の PHI のバックアップ
e	PHI を扱うソフトウェア
f	PHI を扱う機器
g	PHI を扱う機器の環境設備
h	PHI を扱う操作者
i	メモリ・ディスク・画面上の認証情報
j	メモリ・ディスク・画面上の認可情報
k	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙
l	メモリ・ディスク・画面上の認証情報のバックアップ
m	認証情報を扱うソフトウェア
n	認可情報を扱うソフトウェア
o	認証情報を扱う機器
p	認証情報を扱う機器の環境設備
q	認証情報を扱う操作者
r	外部サイト通信トレース上の PHI
s	外部サイト通信トレースのメモやプリントアウトの紙
t	外部サイト通信トレースのバックアップ媒体
u	ネットワーク機器のソフトウェア
v	ネットワーク機器
w	ネットワーク機器の環境設備
x	ネットワーク機器の操作者
y	HCF 内部ネットワーク上の PHI

上記「資産の分類」に対し、ユースケース単位でさらに細分化を実施した。各アプリケーションサーバおよび認証サーバに対応する資産を以下の通り分類し、クライアントと各サーバ間での資産の増減に視点をあてていることがポイントである。

表３．ユースケース単位での「資産の分類」の細分化

記号		資産内容
b	b-B1	暗号アルゴリズムと鍵と鍵配送方式(HIS)
	b-B2	暗号アルゴリズムと鍵と鍵配送方式(生理部門情報システム)
	b-B3	暗号アルゴリズムと鍵と鍵配送方式(レポート作成システム)
	b-B4	暗号アルゴリズムと鍵と鍵配送方式(検査情報参照システム)

記号		資産内容
	b-B5	暗号アルゴリズムと鍵と鍵配送方式(PACS)
	b-B6	暗号アルゴリズムと鍵と鍵配送方式(レポーティング)
	b-C	暗号アルゴリズムと鍵と鍵配送方式(認証サーバ)
i	i-B1	メモリ・ディスク・画面上の認証情報（HIS）
	i-B2	メモリ・ディスク・画面上の認証情報（生理部門情報システム）
	i-B3	メモリ・ディスク・画面上の認証情報（レポート作成システム）
	i-B4	メモリ・ディスク・画面上の認証情報（検査情報参照システム）
	i-B5	メモリ・ディスク・画面上の認証情報（PACS）
	i-B6	メモリ・ディスク・画面上の認証情報（レポーティング）
	i-C	メモリ・ディスク・画面上の認証情報（認証サーバ）
j	j-B1	メモリ・ディスク・画面上の認可情報（HIS）
	j-B2	メモリ・ディスク・画面上の認可情報（生理部門情報システム）
	j-B3	メモリ・ディスク・画面上の認可情報（レポート作成システム）
	j-B4	メモリ・ディスク・画面上の認可情報（検査情報参照システム）
	j-B5	メモリ・ディスク・画面上の認可情報（PACS）
	j-B6	メモリ・ディスク・画面上の認可情報（レポーティング）
	j-C	メモリ・ディスク・画面上の認可情報（認証サーバ）
k	k-B1	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(HIS)
	k-B2	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(生理部門情報システム)
	k-B3	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(レポート作成システム)
	k-B4	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(検査情報参照システム)
	k-B5	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(PACS)
	k-B6	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(レポーティング)
	k-C	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(認証サーバ)
m	m-B1	認証情報を扱うソフトウェア（HIS）
	m-B2	認証情報を扱うソフトウェア（生理部門情報システム）
	m-B3	認証情報を扱うソフトウェア（レポート作成システム）
	m-B4	認証情報を扱うソフトウェア（検査情報参照システム）
	m-B5	認証情報を扱うソフトウェア（PACS）
	m-B6	認証情報を扱うソフトウェア（レポーティング）
	m-C	認証情報を扱うソフトウェア（認証サーバ）
n	n-B1	認可情報を扱うソフトウェア（HIS）
	n-B2	認可情報を扱うソフトウェア（生理部門情報システム）
	n-B3	認可情報を扱うソフトウェア（レポート作成システム）
	n-B4	認可情報を扱うソフトウェア（検査情報参照システム）
	n-B5	認可情報を扱うソフトウェア（PACS）
	n-B6	認可情報を扱うソフトウェア（レポーティング）
	n-C	認可情報を扱うソフトウェア（認証サーバ）

表２と表３に基づき、各サイトにおける資産を抽出し表４に示す。表４中の〇印で示した資産を今回のリスクアセスメントの対象とし、その他の資産は、１）～８）の理由で除外した。

◆ 除外理由

１）認証情報のバックアップ(l)は、クライアント(A)上で操作しないユースケースをモデルとしたため除外した。

２）アプリケーションサーバ(B1～B6)および認証サーバ(C)の管理者は管理端末上で操作しないユースケースをモデルとしたため各々の資産(c,h,k,q)を除外した。

３）認証サーバ(C)上に PHI は存在しないため資産(a,c～h,r,y)を除外した。

４）認証サーバ(C)上に認可情報は存在しないため資産(j,n)を除外した。

５）利用者 ID 管理サーバ＆クライアント(D)上に PHI は存在しないユースケースをモデルとしたため資産(a,c～h,r,y)を除外した。

６）本ガイドラインは病院内におけるシングルサインオン導入にフォーカスしているため、外部のサイト(F2～H2)の全ての資産と各サイトの資産(r～t)の組み合わせを除外した。

７）本ユースケースに存在しない人事給与サーバ(E)を除外した。

８）ネットワーク【院内】(F1)に関係しない資産(a～q)を除外、資産(u～y)に集約し、それ以外のサイトも除外した。

表４．ユースケース単位での資産抽出表

	サイト																		
記号	A	B1	B2	B3	B4	B5	B6	C	D	E	F1	F2	F3	G1	G2	G3	G4	H1	H2
a	○	○	○	○	○	○	○	3)	5)	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
b	○	○	○	○	○	○	○	○	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
c	○	2)	2)	2)	2)	2)	2)	2)3)	5)	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
d	○	○	○	○	○	○	○	3)	5)	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
e	○	○	○	○	○	○	○	3)	5)	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
f	○	○	○	○	○	○	○	3)	5)	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
g	○	○	○	○	○	○	○	3)	5)	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
h	○	2)	2)	2)	2)	2)	2)	2)3)	5)	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
i	○	○	○	○	○	○	○	○	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
j	○	○	○	○	○	○	○	4)	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
k	○	2)	2)	2)	2)	2)	2)	2)	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
l	1)	○	○	○	○	○	○	○	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
m	○	○	○	○	○	○	○	○	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
n	○	○	○	○	○	○	○	4)	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
o	○	○	○	○	○	○	○	○	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
p	○	○	○	○	○	○	○	○	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
q	○	2)	2)	2)	2)	2)	2)	2)	○	7)	8)	6)	6)	6)	6)	6)	6)	6)	6)
r	6)	6)	6)	6)	6)	6)	6)	3)6)	5)6)	6)7)	6)	6)	6)	6)	6)	6)	6)	6)	6)
s	6)	6)	6)	6)	6)	6)	6)	6)	6)	6)7)	6)	6)	6)	6)	6)	6)	6)	6)	6)
t	6)	6)	6)	6)	6)	6)	6)	6)	6)	6)7)	6)	6)	6)	6)	6)	6)	6)	6)	6)
u	8)	8)	8)	8)	8)	8)	8)	8)	8)	7)8)	○	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)
v	8)	8)	8)	8)	8)	8)	8)	8)	8)	7)8)	○	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)
w	8)	8)	8)	8)	8)	8)	8)	8)	8)	7)8)	○	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)

	サイト																	
記号	A	B1	B2	B3	B4	B5	B6	C	D	E	F1	F2	F3	G1	G2	G3	G4	H1	H2
x	8)	8)	8)	8)	8)	8)	8)	8)	8)	7)8)	○	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)
y	8)	8)	8)	8)	8)	8)	8)	3)8)	5)8)	7)8)	○	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)	6) 8)

表５－１．生理検査：アクティビティ図（SSO 導入前）1/4

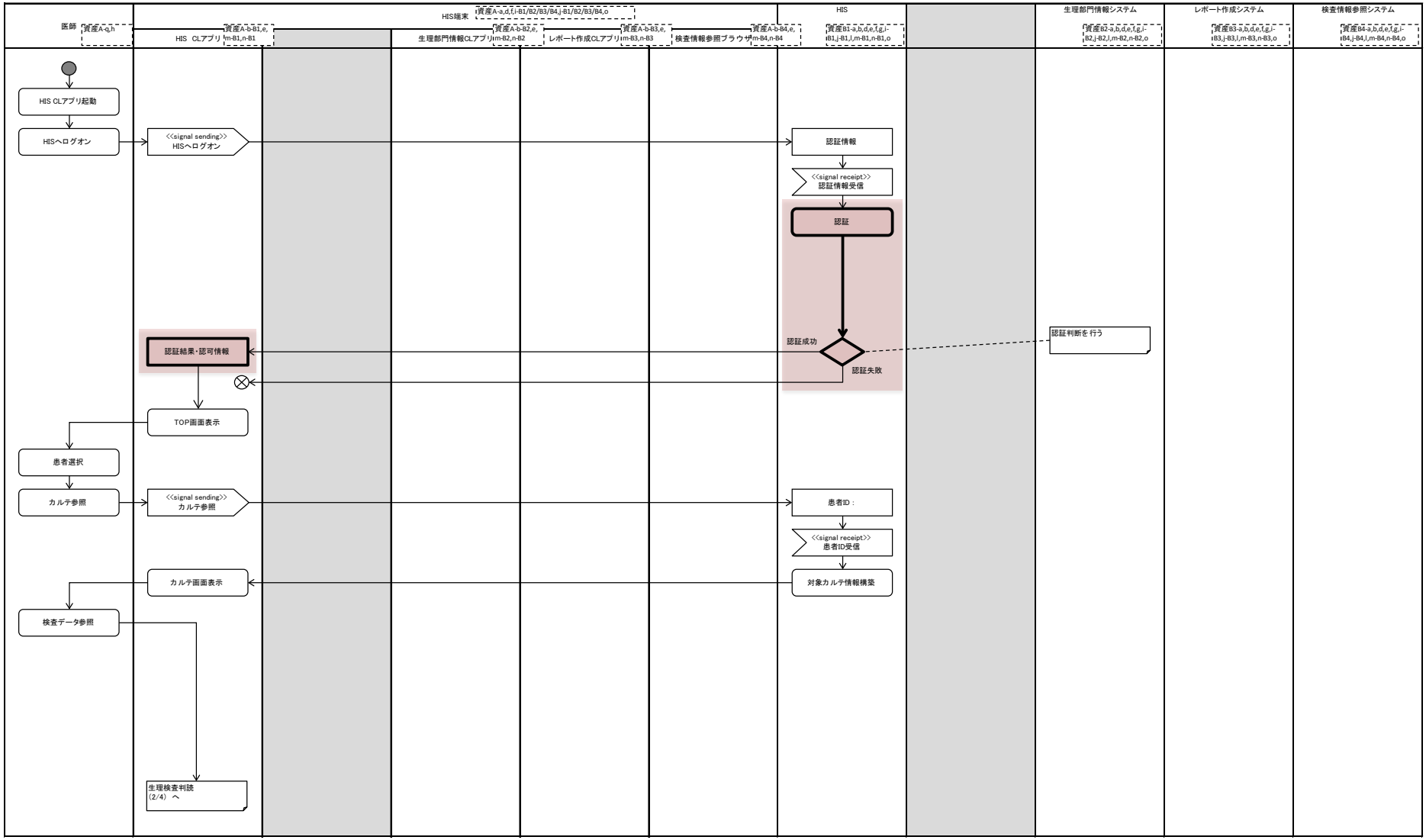


表５－１．生理検査：アクティビティ図（SSO 導入前）2/4

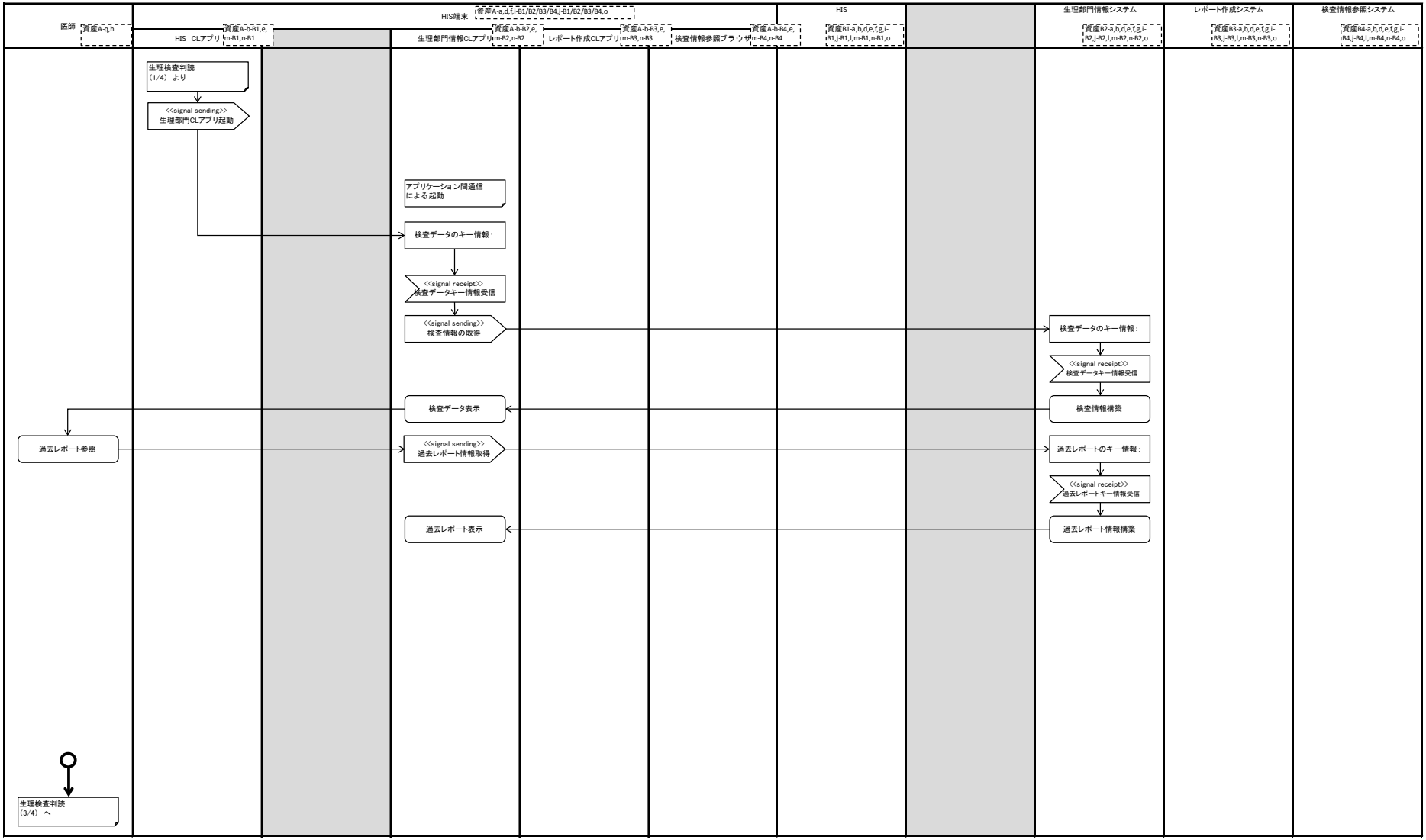


表５－１．生理検査：アクティビティ図（SSO 導入前）3/4

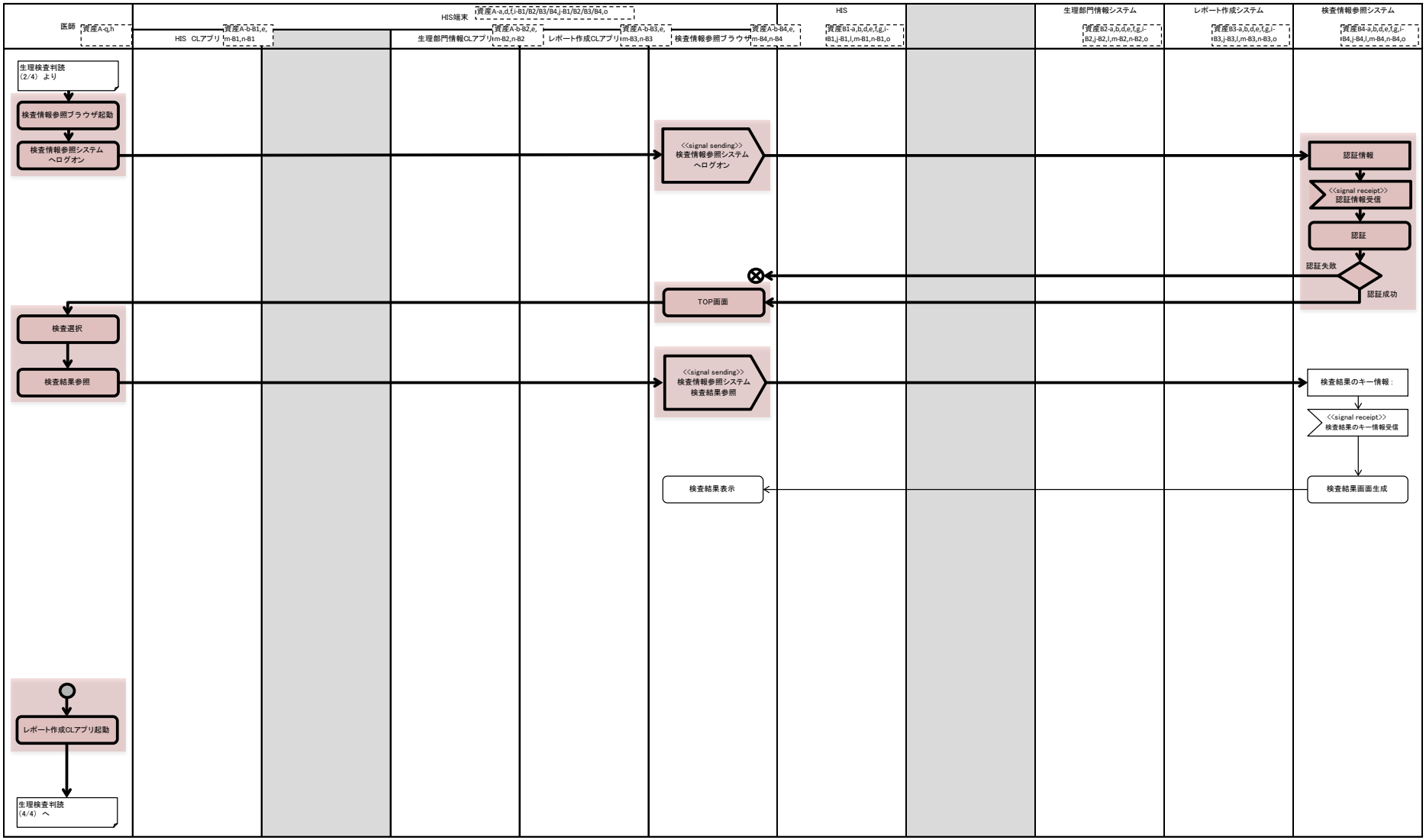


表５－１．生理検査：アクティビティ図（SSO 導入前）4/4

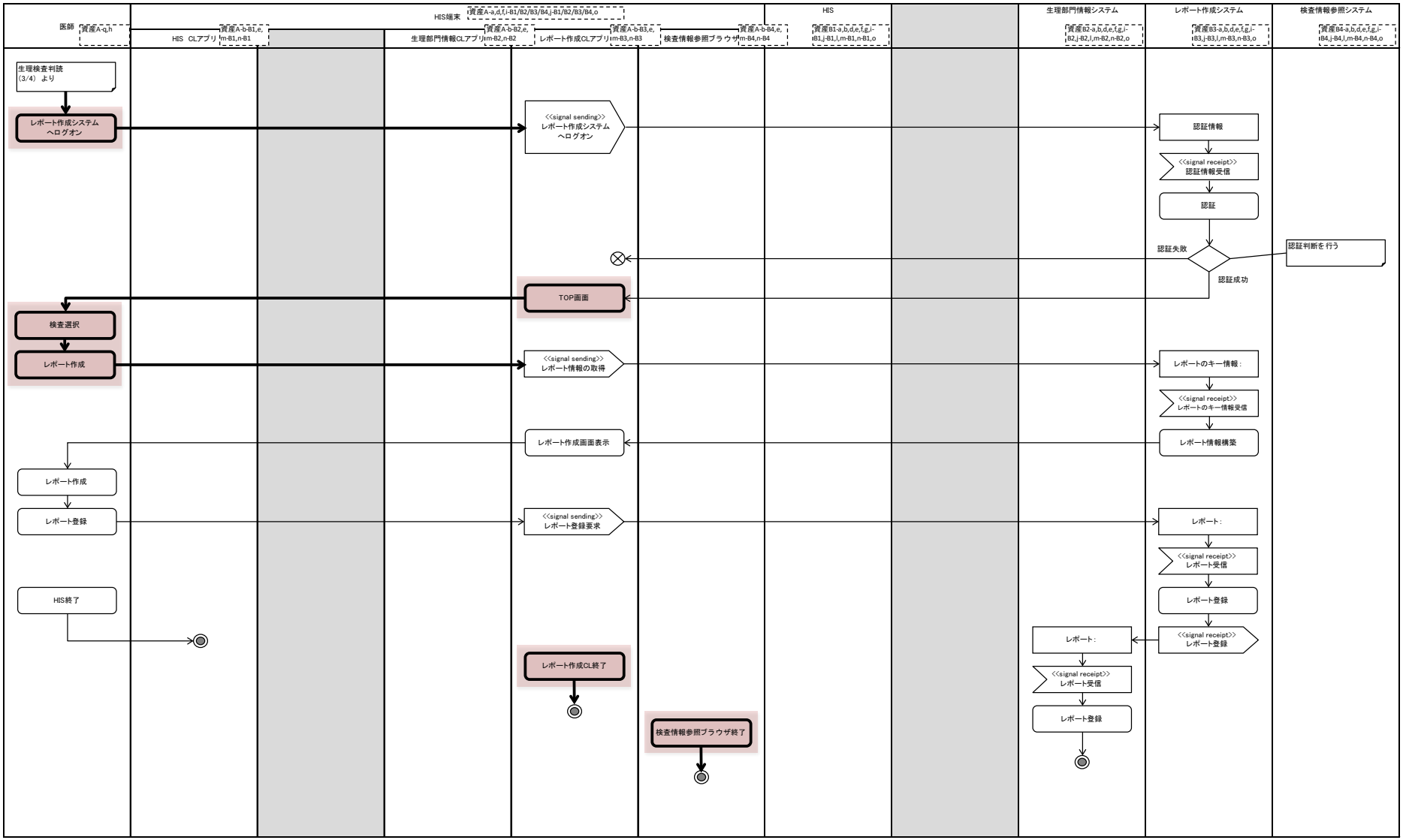


表５－２．生理検査：アクティビティ図（SSO 導入後）1/4

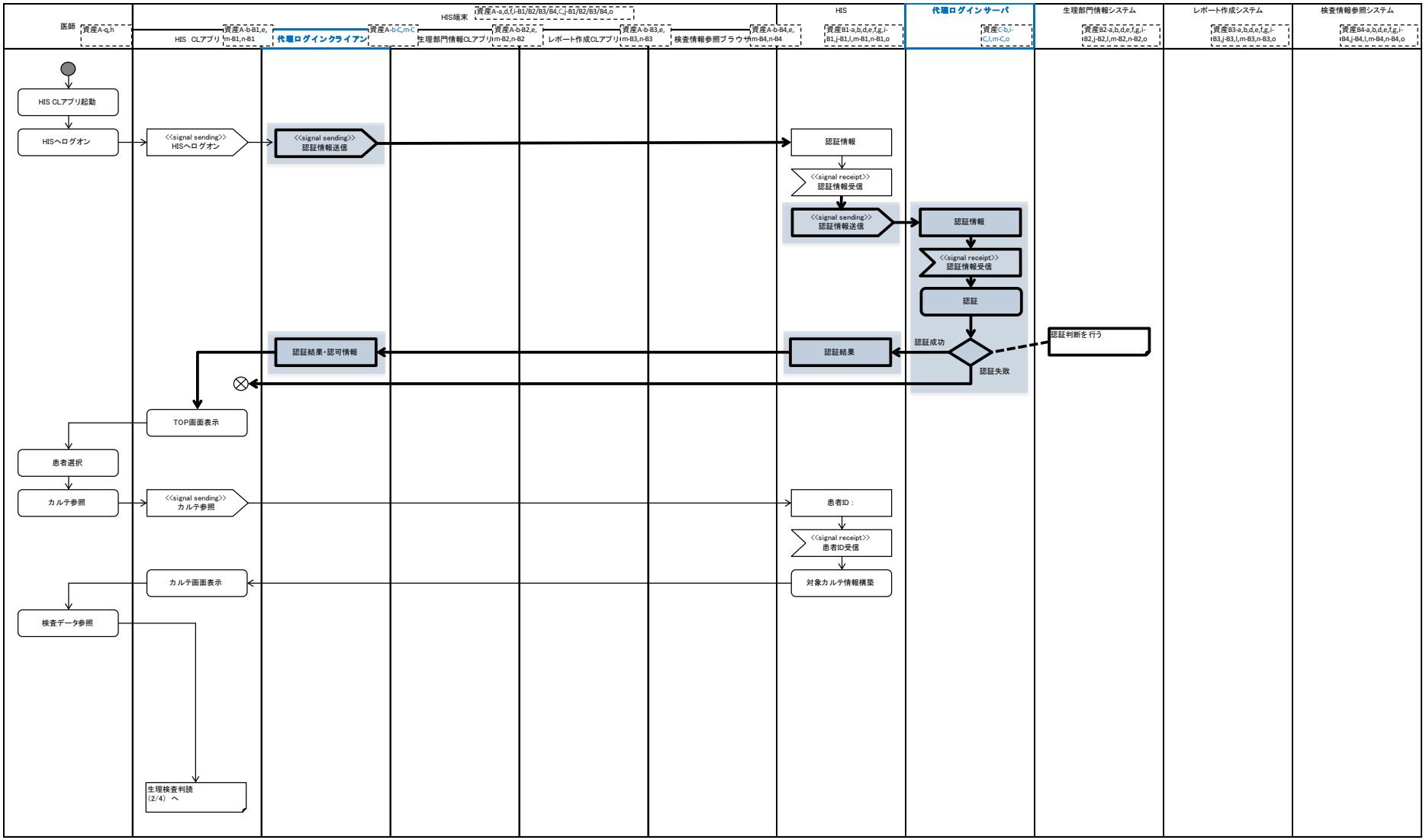


表５－２．生理検査：アクティビティ図（SSO 導入後）2/4

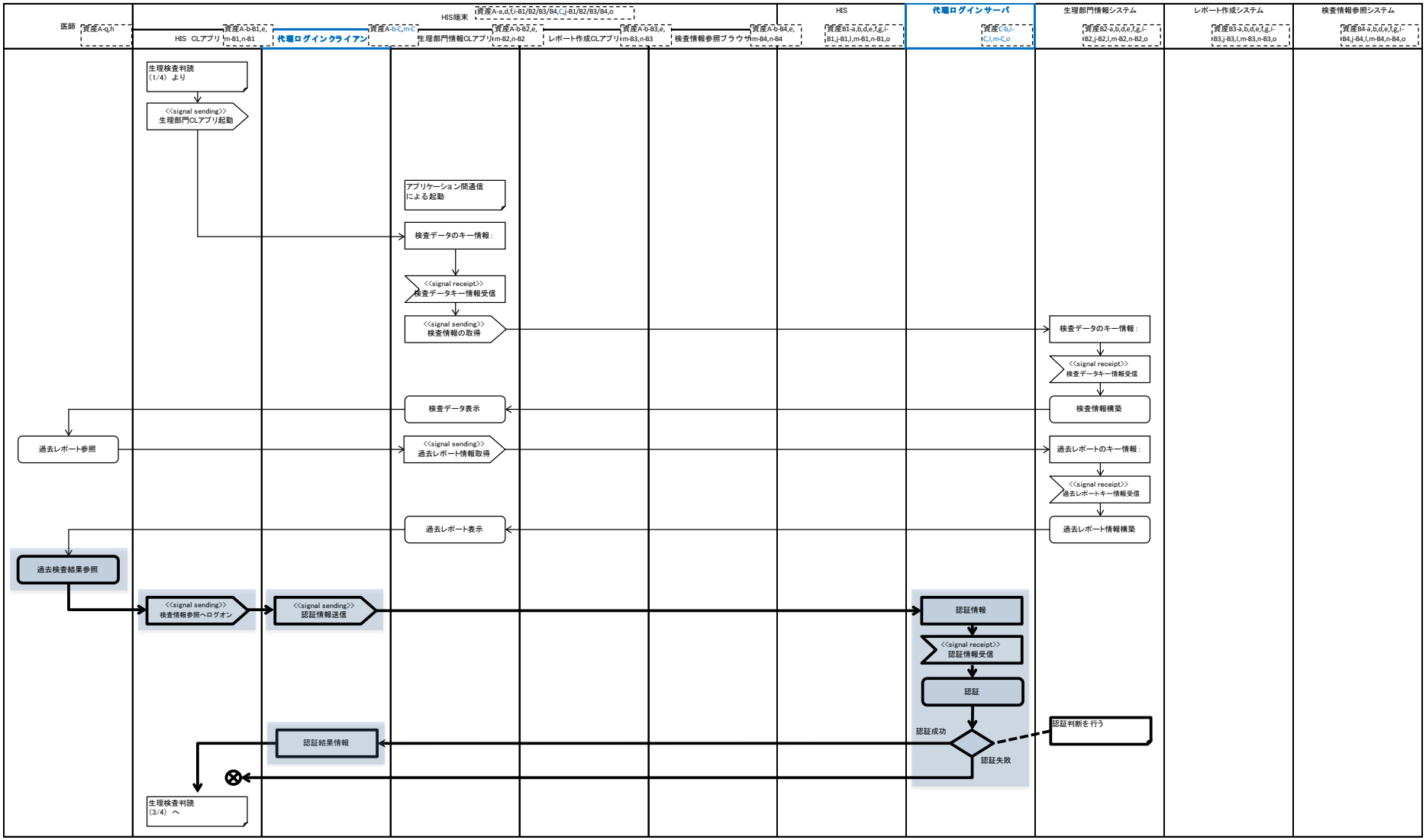


表５－２．生理検査：アクティビティ図（SSO 導入後）3/4

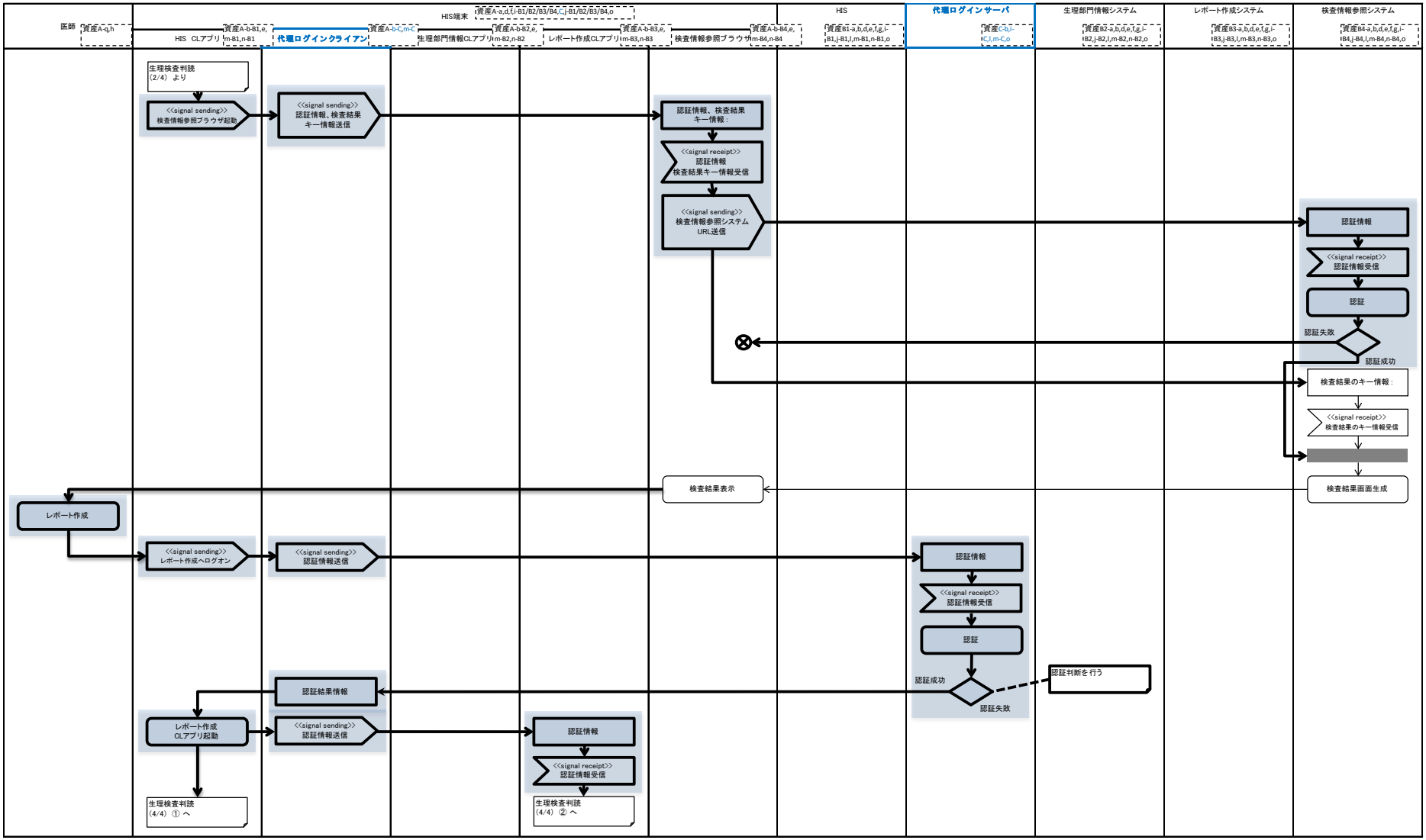


表５－２．生理検査：アクティビティ図（SSO 導入後）4/4

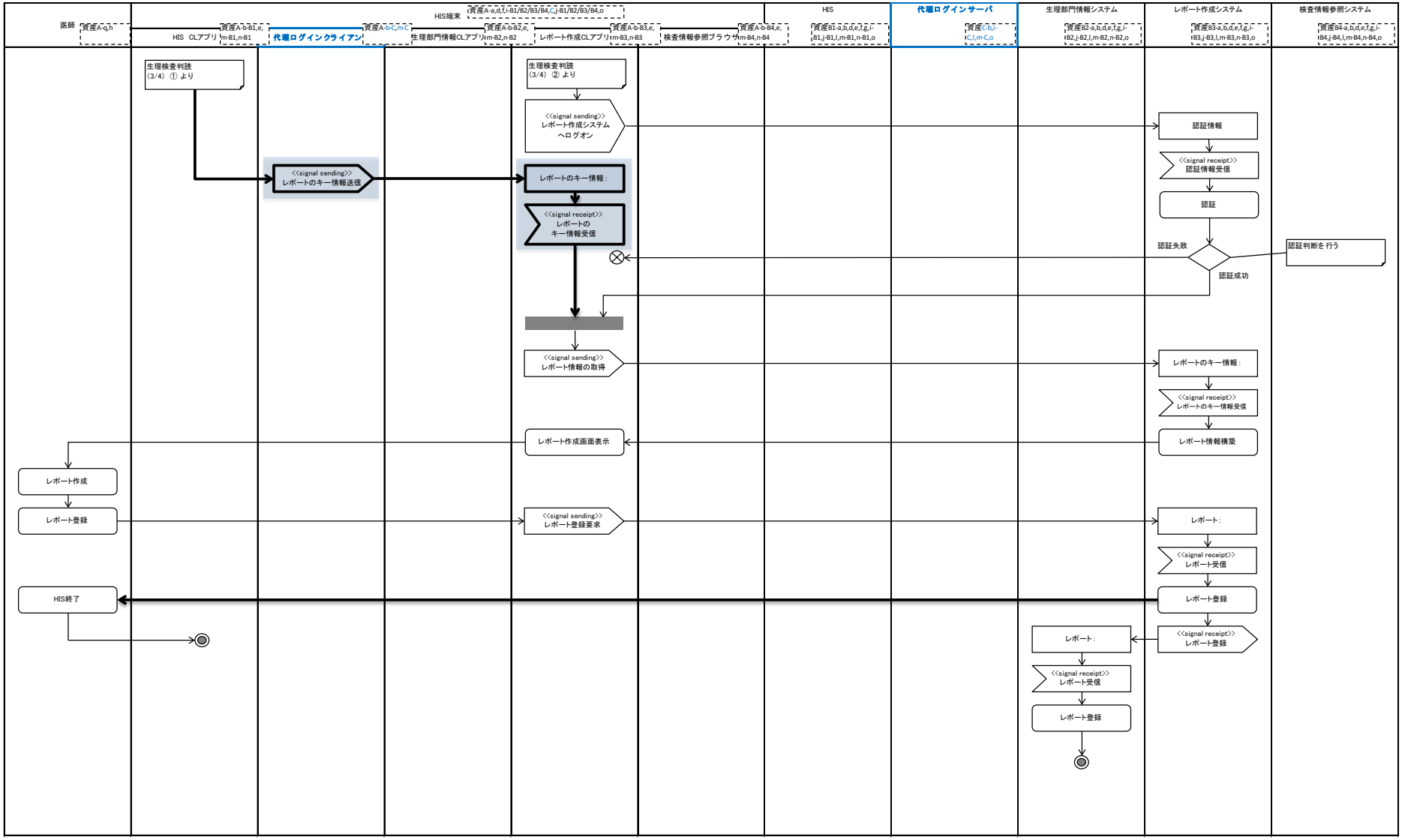


表５－３．外来診察前準備：アクティビティ図（SSO 導入前）1/3

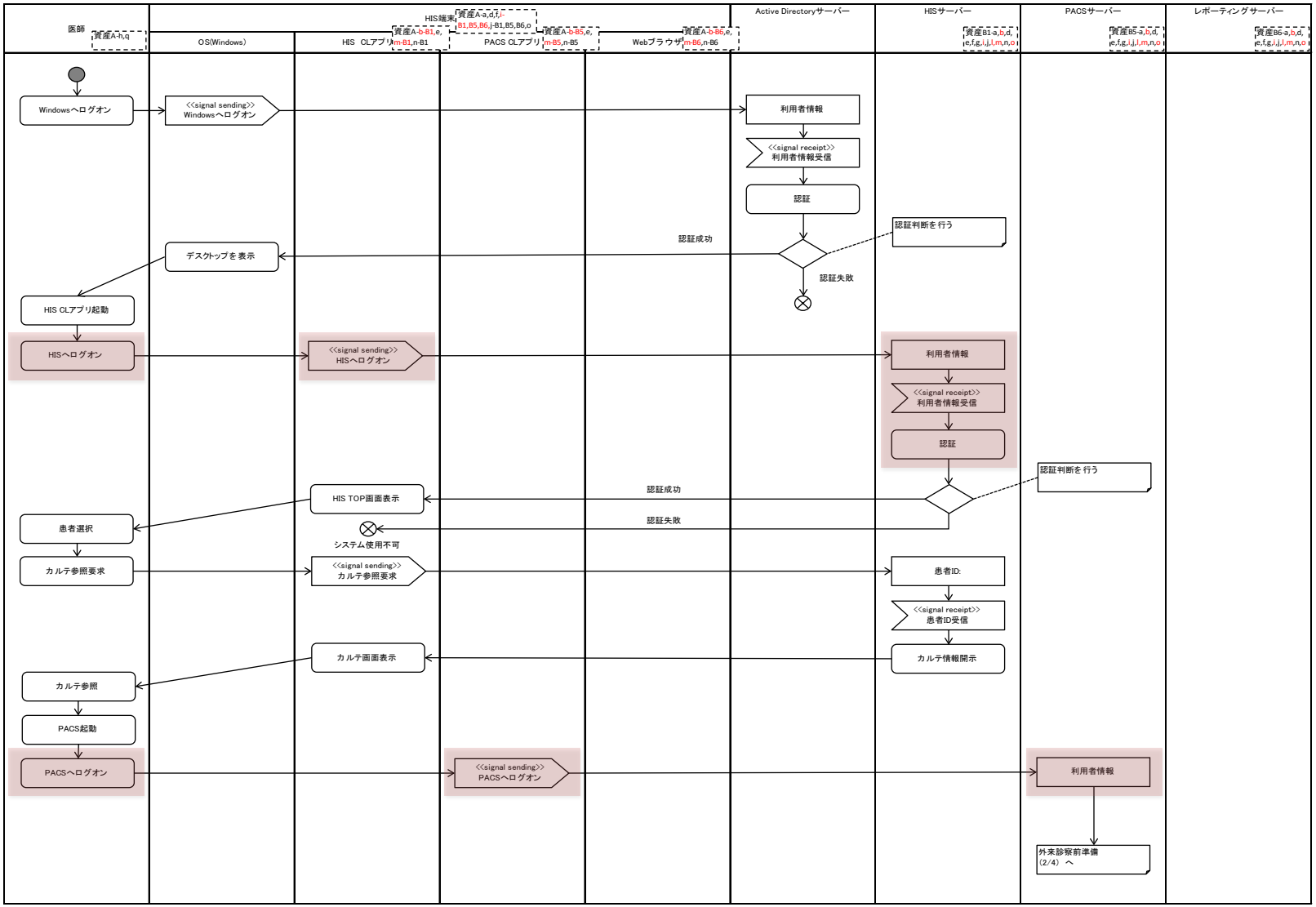


表５－３．外来診察前準備：アクティビティ図（SSO 導入前）2/3

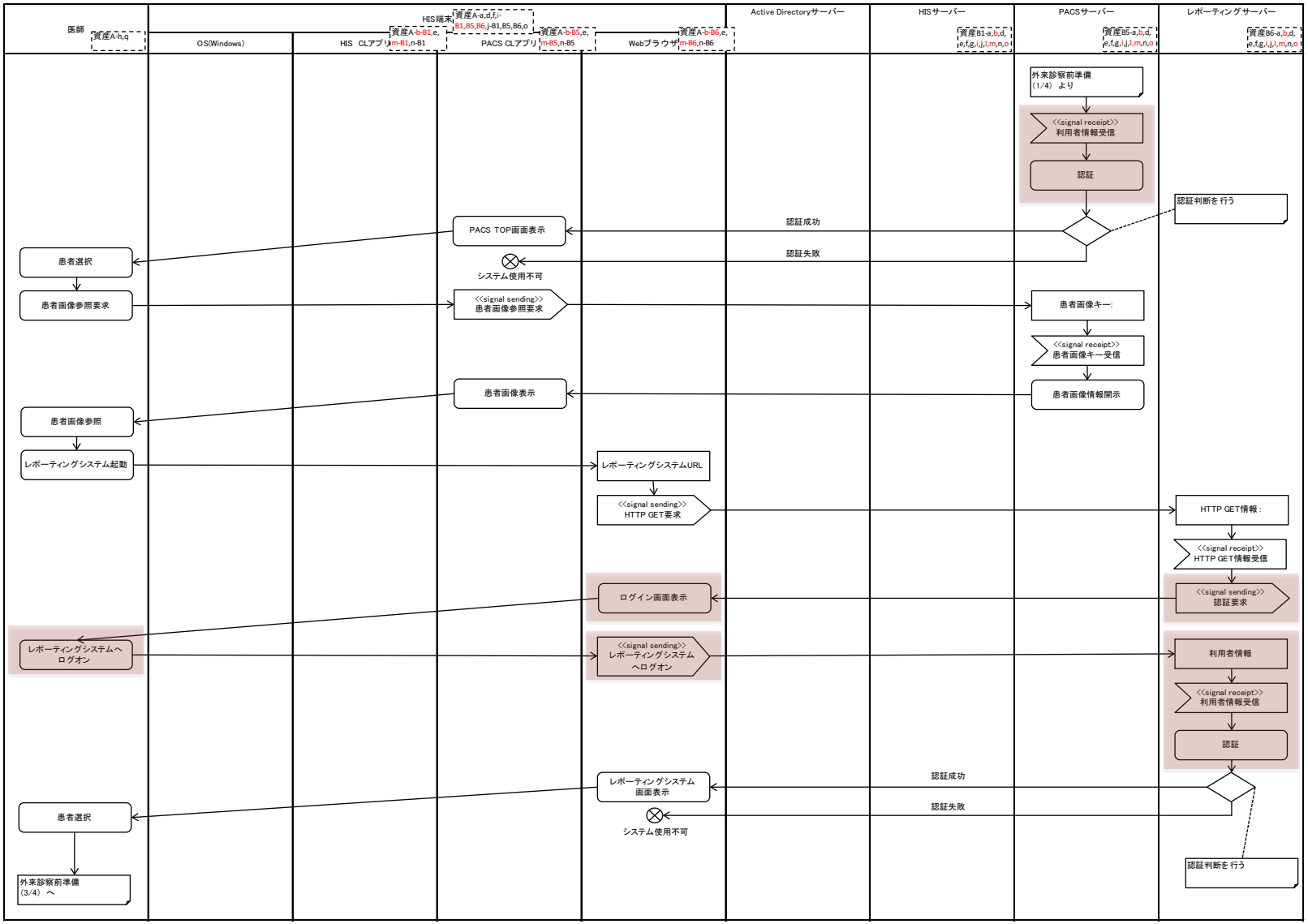


表５－３．外来診察前準備：アクティビティ図（SSO 導入前）3/3

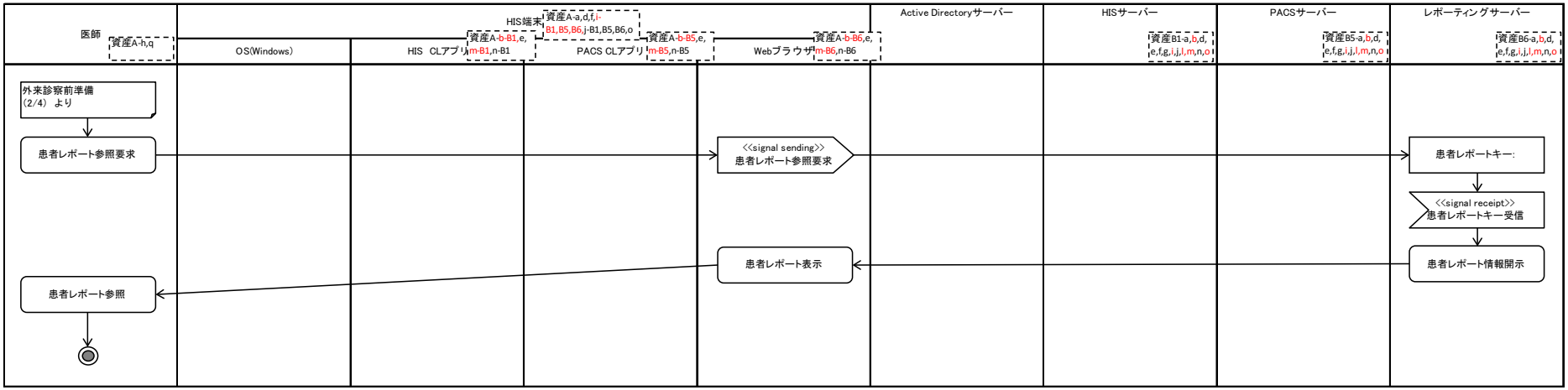


表５－４．外来診察前準備：アクティビティ図（SSO 導入後）1/4

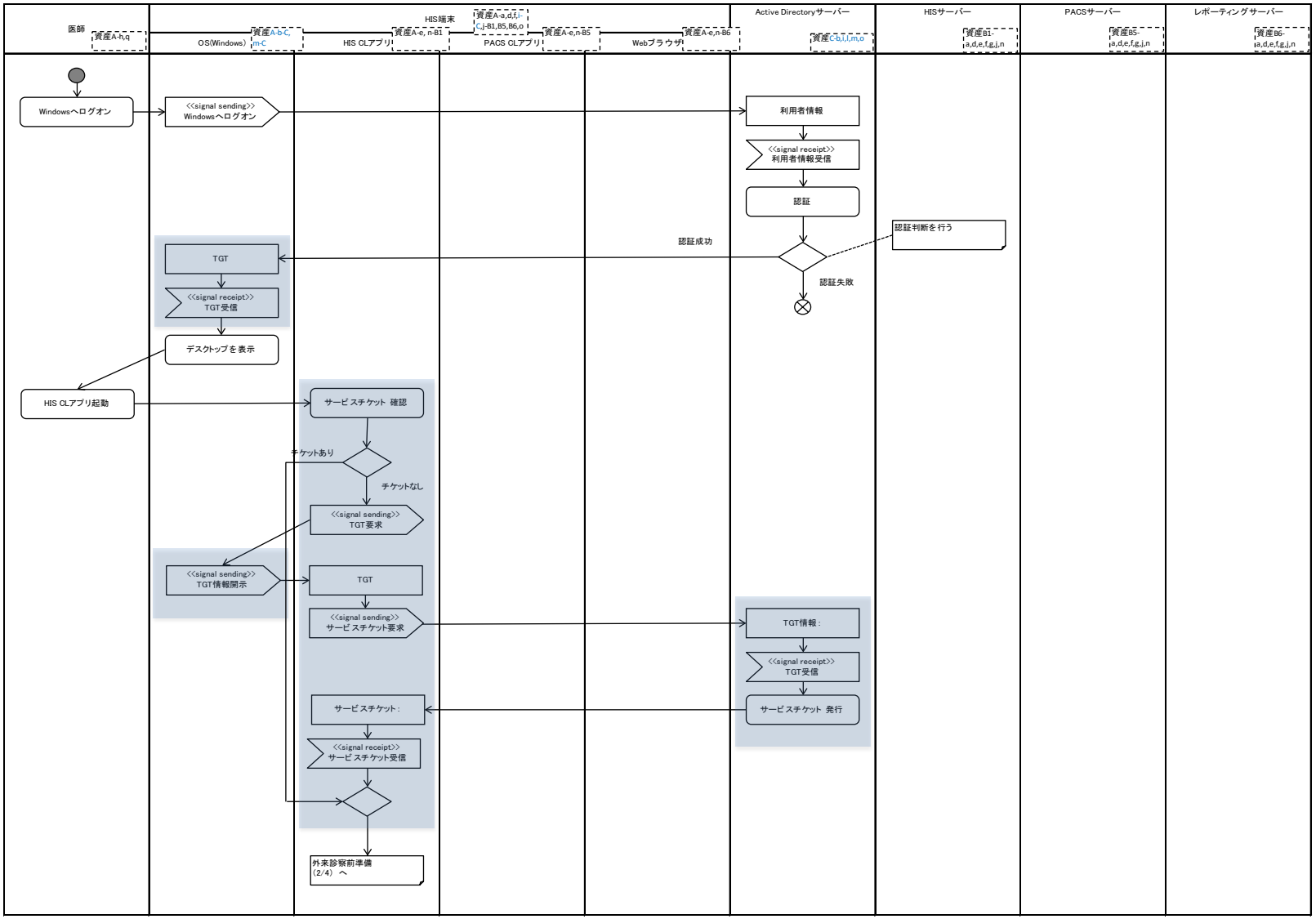


表５－４．外来診察前準備：アクティビティ図（SSO 導入後）2/4

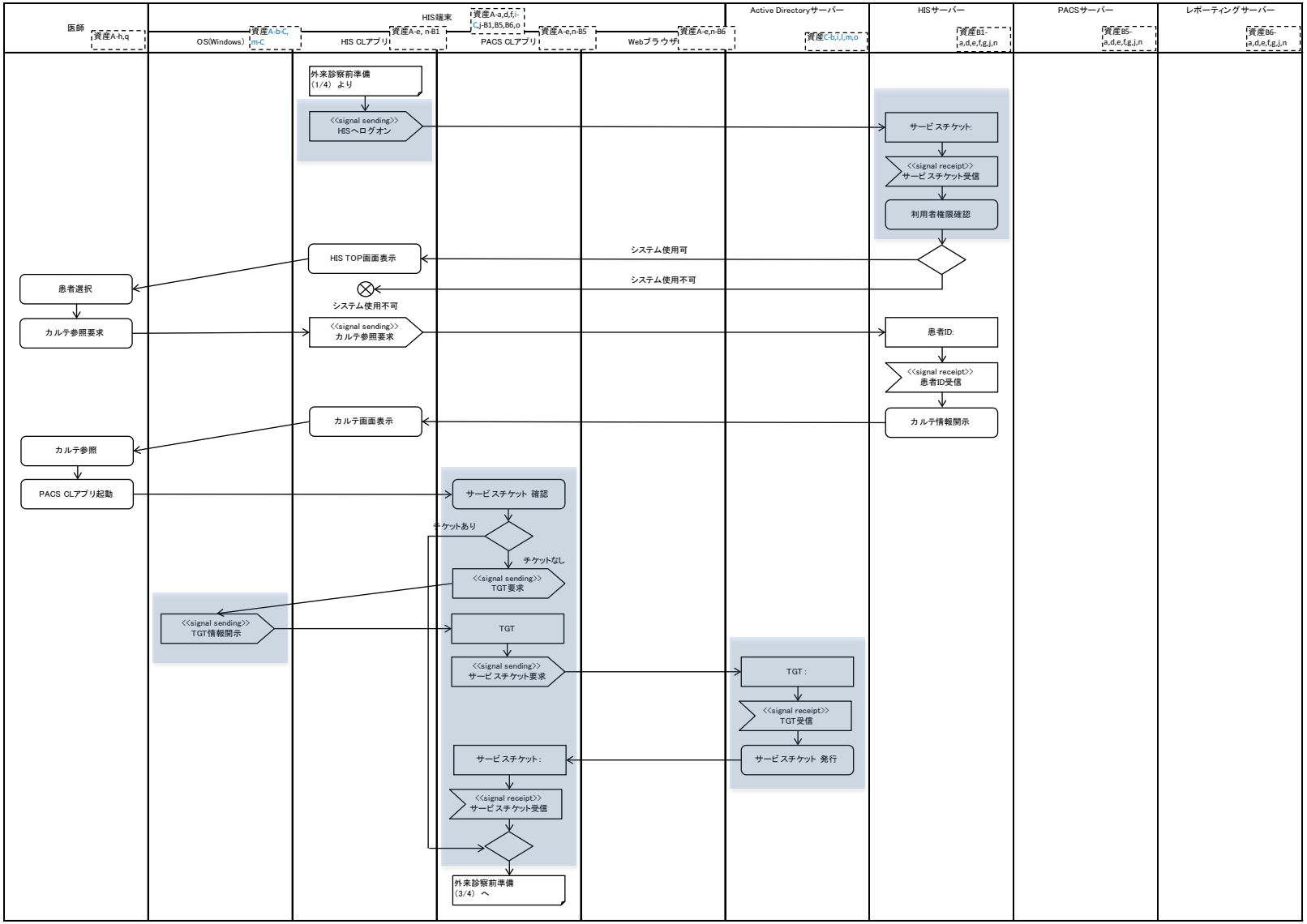


表５－４．外来診察前準備：アクティビティ図（SSO 導入後）3/4

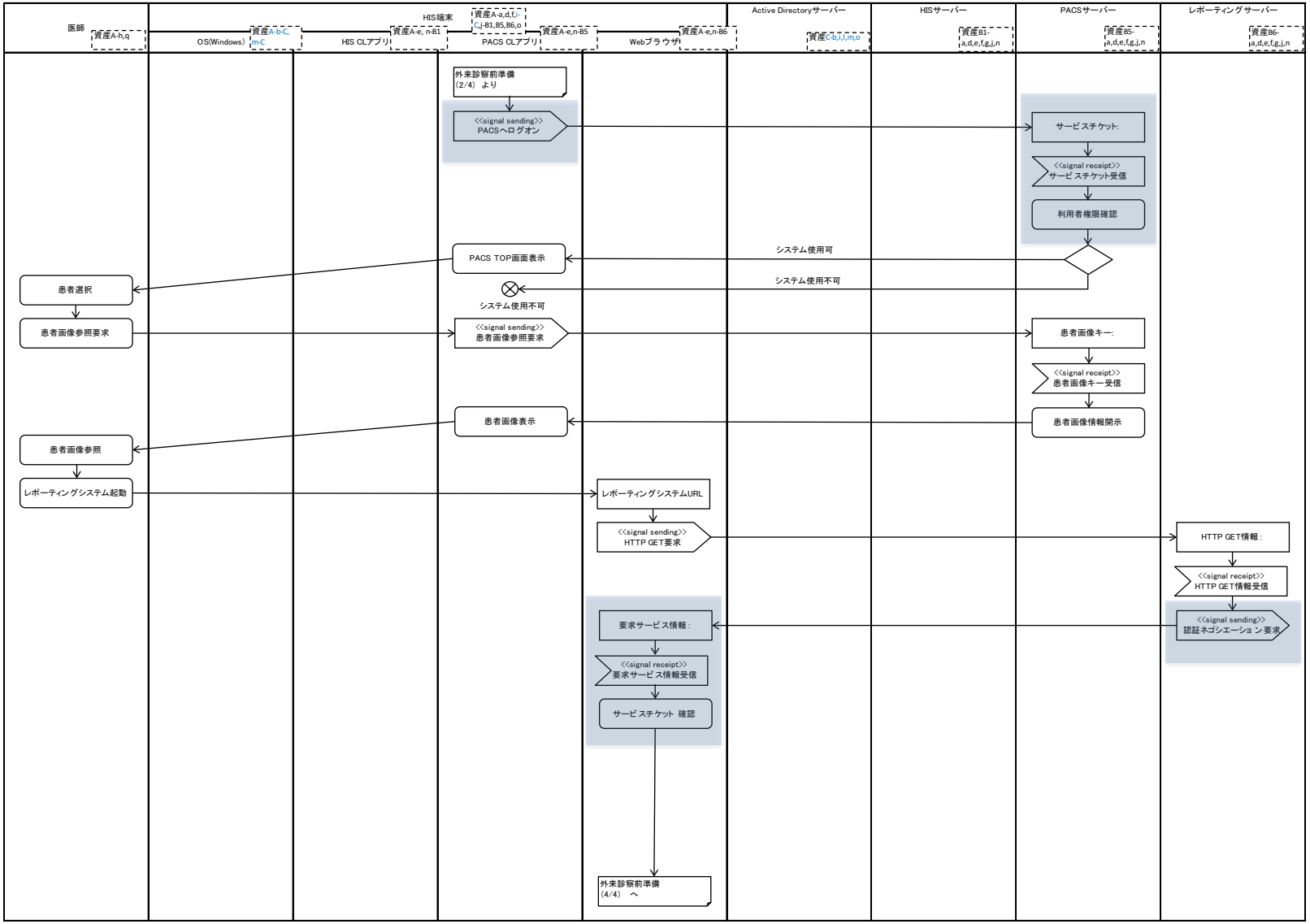


表５－４．外来診察前準備：アクティビティ図（SSO 導入後）4/4

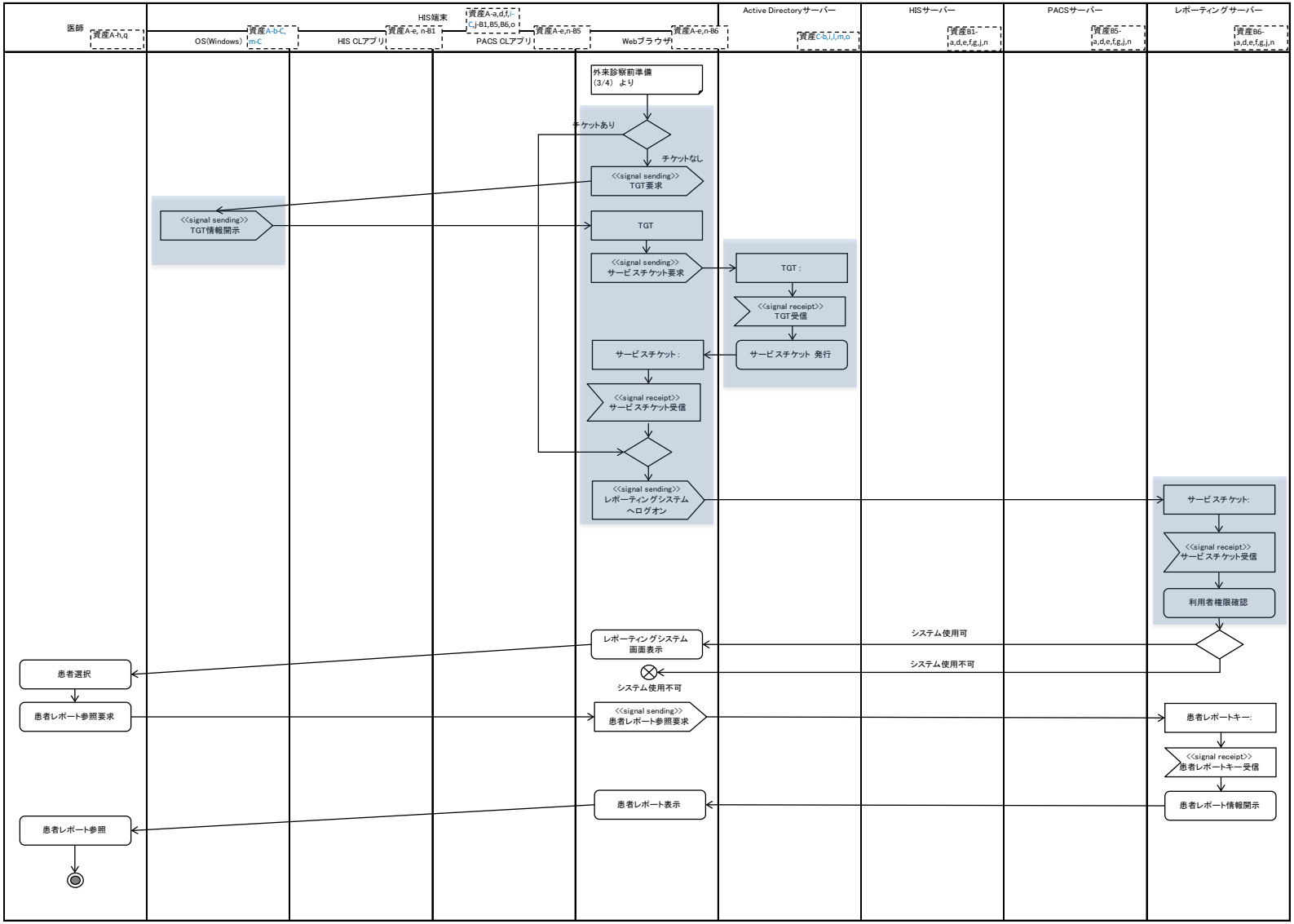


表６．シングルサインオン導入前後の「サイト／資産」比較（増減）

＜記号の定義＞

◆ 導入前欄、導入後欄に記載した記号の定義は以下とする。

○　：　SSO 導入前または SSO 導入後に確実に存在する資産
△　：　安全管理のガイドラインを遵守していれば存在しない資産
－　：　SSO 導入前または SSO 導入後に存在しない資産
（ユースケース上、存在しない資産を含む）

◆ 増減欄に記載した記号の定義は以下とする。

↑　：　SSO 導入前後で増加した資産
→　：　SSO 導入前後で変化がない資産
↓　：　SSO 導入前後で減少した資産
－　：　ユースケース上、存在しない資産

サイト		資産		生理検査判読（代理ログオン）			外来診察前準備（Kerberos）		
記号	サイト名	記号	資産内容	導入前	導入後	増減	導入前	導入後	増減
A	（病院内）クライアント	a	メモリ・ディスク・画面上の PHI	○	○	→	○	○	→
		b-B1	暗号アルゴリズムと鍵と鍵配送方式(HIS)	○	○	→	○	-	↓
		b-B2	暗号アルゴリズムと鍵と鍵配送方式(生理部門情報システム)	○	○	→	-	-	-
		b-B3	暗号アルゴリズムと鍵と鍵配送方式(レポート作成システム)	○	○	→	-	-	-
		b-B4	暗号アルゴリズムと鍵と鍵配送方式(検査情報参照システム)	○	○	→	-	-	-
		b-B5	暗号アルゴリズムと鍵と鍵配送方式(PACS)	-	-	-	○	-	↓
		b-B6	暗号アルゴリズムと鍵と鍵配送方式(レポーティング)	-	-	-	○	-	↓
		b-C	暗号アルゴリズムと鍵と鍵配送方式(認証サーバ)	-	○	↑	-	○	↑
		c	メモリ・ディスク・画面上の PHI のメモやプリントアウトの紙	○	○	→	○	○	→

サイト		資産		生理検査判読（代理ログオン）			外来診察前準備（Kerberos）		
記号	サイト名	記号	資産内容	導入前	導入後	増減	導入前	導入後	増減
A	（病院内） クライアント	d	メモリ・ディスク・画面上の PHI のバックアップ	○	○	→	○	○	→
		e	PHI を扱うソフトウェア	○	○	→	○	○	→
		f	PHI を扱う機器	○	○	→	○	○	→
		g	PHI を扱う機器の環境設備	○	○	→	○	○	→
		h	PHI を扱う操作者	○	○	→	○	○	→
		i-B1	メモリ・ディスク・画面上の認証情報（HIS）	○	○	→	○	-	↓
		i-B2	メモリ・ディスク・画面上の認証情報（生理部門情報システム）	○	○	→	-	-	-
		i-B3	メモリ・ディスク・画面上の認証情報（レポート作成システム）	○	○	→	-	-	-
		i-B4	メモリ・ディスク・画面上の認証情報（検査情報参照システム）	○	○	→	-	-	-
		i-B5	メモリ・ディスク・画面上の認証情報（PACS）	-	-	-	○	-	↓
		i-B6	メモリ・ディスク・画面上の認証情報（レポーティング）	-	-	-	○	-	↓
		i-C	メモリ・ディスク・画面上の認証情報（認証サーバ）	-	○	↑	-	○	↑
		j-B1	メモリ・ディスク・画面上の認可情報（HIS）	○	○	→	○	○	→
		j-B2	メモリ・ディスク・画面上の認可情報（生理部門情報システム）	○	○	→	-	-	-
		j-B3	メモリ・ディスク・画面上の認可情報（レポート作成システム）	○	○	→	-	-	-
		j-B4	メモリ・ディスク・画面上の認可情報（検査情報参照システム）	○	○	→	-	-	-
		j-B5	メモリ・ディスク・画面上の認可情報（PACS）	-	-	-	○	○	→
		j-B6	メモリ・ディスク・画面上の認可情報（レポーティング）	-	-	-	○	○	→
		j-C	メモリ・ディスク・画面上の認可情報（認証サーバ）	-	-	-	-	-	-
		k-B1	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(HIS)	△	-	↓	△	-	↓
		k-B2	メモリ･ディスク･画面上の認証情報のメモやプリントアウトの紙(生理部門情報システム)	△	-	↓	-	-	-

サイト		資産		生理検査判読 （代理ログオン）			外来診察前準備 （Kerberos）		
記号	サイト名	記号	資産内容	導入前	導入後	増減	導入前	導入後	増減
A	（病院内） クライアント	k-B3	メモリ･ディスク･画面上の認証情報のメモやプリントアウトの紙(レポート作成システム)	△	-	↓	-	-	-
		k-B4	メモリ･ディスク･画面上の認証情報のメモやプリントアウトの紙(検査情報参照システム)	△	-	↓	-	-	-
		k-B5	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(PACS)	-	-	-	△	-	↓
		k-B6	メモリ･ディスク･画面上の認証情報のメモやプリントアウトの紙(レポーティング)	-	-	-	△	-	↓
		k-C	メモリ･ディスク･画面上の認証情報のメモやプリントアウトの紙(認証サーバ)	-	△	↑	-	△	↑
		m-B1	認証情報を扱うソフトウェア（HIS）	○	○	→	○	-	↓
		m-B2	認証情報を扱うソフトウェア（生理部門情報システム）	○	○	→	-	-	-
		m-B3	認証情報を扱うソフトウェア（レポート作成システム）	○	○	→	-	-	-
		m-B4	認証情報を扱うソフトウェア（検査情報参照システム）	○	○	→	-	-	-
		m-B5	認証情報を扱うソフトウェア（PACS）	-	-	-	○	-	↓
		m-B6	認証情報を扱うソフトウェア（レポーティング）	-	-	-	○	-	↓
		m-C	認証情報を扱うソフトウェア（認証サーバ）	-	○	↑	-	○	↑
		n-B1	認可情報を扱うソフトウェア（HIS）	○	○	→	○	○	→
		n-B2	認可情報を扱うソフトウェア（生理部門情報システム）	○	○	→	-	-	-
		n-B3	認可情報を扱うソフトウェア（レポート作成システム）	○	○	→	-	-	-
		n-B4	認可情報を扱うソフトウェア（検査情報参照システム）	○	○	→	-	-	-
		n-B5	認可情報を扱うソフトウェア（PACS）	-	-	-	○	○	→
		n-B6	認可情報を扱うソフトウェア（レポーティング）	-	-	-	○	○	→
		n-C	認可情報を扱うソフトウェア（認証サーバ）	-	-	-	-	-	-

サイト		資産		生理検査判読（代理ログオン）			外来診察前準備（Kerberos）		
記号	サイト名	記号	資産内容	導入前	導入後	増減	導入前	導入後	増減
A	（病院内） クライアント	o	認証情報を扱う機器	○	○	→	○	○	→
		p	認証情報を扱う機器の環境設備	○	○	→	○	○	→
		q	認証情報を扱う操作者	○	○	→	○	○	→
B1	（病院内） アプリケーションサーバ 【HIS】	a	メモリ・ディスク・画面上の PHI	○	○	→	○	○	→
		b	暗号アルゴリズムと鍵と鍵配送方式	○	○	→	○	-	↓
		d	メモリ・ディスク・画面上の PHI のバックアップ	○	○	→	○	○	→
		e	PHI を扱うソフトウェア	○	○	→	○	○	→
		f	PHI を扱う機器	○	○	→	○	○	→
		g	PHI を扱う機器の環境設備	○	○	→	○	○	→
		i-B1	メモリ・ディスク・画面上の認証情報	○	○	→	○	-	↓
		j-B1	メモリ・ディスク・画面上の認可情報	○	○	→	○	○	→
		l	メモリ・ディスク・画面上の認証情報のバックアップ	○	○	→	○	-	↓
		m-B1	認証情報を扱うソフトウェア	○	○	→	○	-	↓
		n-B1	認可情報を扱うソフトウェア	○	○	→	○	○	→
		o	認証情報を扱う機器	○	○	→	○	-	↓
		p	認証情報を扱う機器の環境設備	○	○	→	○	-	↓
B2	（病院内） アプリケーションサーバ 【生理部門情報システム】	a	メモリ・ディスク・画面上の PHI	○	○	→	-	-	-
		b	暗号アルゴリズムと鍵と鍵配送方式	○	○	→	-	-	-
		d	メモリ・ディスク・画面上の PHI のバックアップ	○	○	→	-	-	-
		e	PHI を扱うソフトウェア	○	○	→	-	-	-
		f	PHI を扱う機器	○	○	→	-	-	-
		g	PHI を扱う機器の環境設備	○	○	→	-	-	-
		i-B2	メモリ・ディスク・画面上の認証情報	○	○	→	-	-	-
		j-B2	メモリ・ディスク・画面上の認可情報	○	○	→	-	-	-

サイト		資産		生理検査判読（代理ログオン）			外来診察前準備（Kerberos）		
記号	サイト名	記号	資産内容	導入前	導入後	増減	導入前	導入後	増減
B2	（病院内）アプリケーションサーバ【生理部門情報システム】	l	メモリ・ディスク・画面上の認証情報のバックアップ	○	○	→	-	-	-
		m-B2	認証情報を扱うソフトウェア	○	○	→	-	-	-
		n-B2	認可情報を扱うソフトウェア	○	○	→	-	-	-
		o	認証情報を扱う機器	○	○	→	-	-	-
		p	認証情報を扱う機器の環境設備	○	○	→	-	-	-
B3	（病院内）アプリケーションサーバ【レポート作成システム】	a	メモリ・ディスク・画面上の PHI	○	○	→	-	-	-
		b	暗号アルゴリズムと鍵と鍵配送方式	○	○	→	-	-	-
		d	メモリ・ディスク・画面上の PHI のバックアップ	○	○	→	-	-	-
		e	PHI を扱うソフトウェア	○	○	→	-	-	-
		f	PHI を扱う機器	○	○	→	-	-	-
		g	PHI を扱う機器の環境設備	○	○	→	-	-	-
		i-B3	メモリ・ディスク・画面上の認証情報	○	○	→	-	-	-
		j-B3	メモリ・ディスク・画面上の認可情報	○	○	→	-	-	-
		l	メモリ・ディスク・画面上の認証情報のバックアップ	○	○	→	-	-	-
		m-B3	認証情報を扱うソフトウェア	○	○	→	-	-	-
		n-B3	認可情報を扱うソフトウェア	○	○	→	-	-	-
		o	認証情報を扱う機器	○	○	→	-	-	-
		p	認証情報を扱う機器の環境設備	○	○	→	-	-	-
B4	（病院内）アプリケーションサーバ【検査情報参照システム】	a	メモリ・ディスク・画面上の PHI	○	○	→	-	-	-
		b	暗号アルゴリズムと鍵と鍵配送方式	○	○	→	-	-	-
		d	メモリ・ディスク・画面上の PHI のバックアップ	○	○	→	-	-	-
		e	PHI を扱うソフトウェア	○	○	→	-	-	-
		f	PHI を扱う機器	○	○	→	-	-	-

サイト		資産		生理検査判読（代理ログオン）			外来診察前準備（Kerberos）		
記号	サイト名	記号	資産内容	導入前	導入後	増減	導入前	導入後	増減
B4	（病院内） アプリケーションサーバ 【検査情報参照システム】	g	PHI を扱う機器の環境設備	○	○	→	-	-	-
		i-B4	メモリ・ディスク・画面上の認証情報	○	○	→	-	-	-
		j-B4	メモリ・ディスク・画面上の認可情報	○	○	→	-	-	-
		l	メモリ・ディスク・画面上の認証情報のバックアップ	○	○	→	-	-	-
		m-B4	認証情報を扱うソフトウェア	○	○	→	-	-	-
		n-B4	認可情報を扱うソフトウェア	○	○	→	-	-	-
		o	認証情報を扱う機器	○	○	→	-	-	-
		p	認証情報を扱う機器の環境設備	○	○	→	-	-	-
B5	（病院内） アプリケーションサーバ 【PACS】	a	メモリ・ディスク・画面上の PHI	-	-	-	○	○	→
		b	暗号アルゴリズムと鍵と鍵配送方式	-	-	-	○	-	↓
		d	メモリ・ディスク・画面上の PHI のバックアップ	-	-	-	○	○	→
		e	PHI を扱うソフトウェア	-	-	-	○	○	→
		f	PHI を扱う機器	-	-	-	○	○	→
		g	PHI を扱う機器の環境設備	-	-	-	○	○	→
		i-B5	メモリ・ディスク・画面上の認証情報	-	-	-	○	-	↓
		j-B5	メモリ・ディスク・画面上の認可情報	-	-	-	○	○	→
		l	メモリ・ディスク・画面上の認証情報のバックアップ	-	-	-	○	-	↓
		m-B5	認証情報を扱うソフトウェア	-	-	-	○	-	↓
		n-B5	認可情報を扱うソフトウェア	-	-	-	○	○	→
		o	認証情報を扱う機器	-	-	-	○	-	↓
		p	認証情報を扱う機器の環境設備	-	-	-	○	-	↓
B6	（病院内） アプリケーションサーバ 【レポーティング】	a	メモリ・ディスク・画面上の PHI	-	-	-	○	○	→
		b	暗号アルゴリズムと鍵と鍵配送方式	-	-	-	○	-	↓
		d	メモリ・ディスク・画面上の PHI のバックアップ	-	-	-	○	○	→

サイト		資産		生理検査判読（代理ログオン）			外来診察前準備（Kerberos）		
記号	サイト名	記号	資産内容	導入前	導入後	増減	導入前	導入後	増減
B6	（病院内） アプリケーションサーバ 【レポーティング】	e	PHI を扱うソフトウェア	-	-	-	○	○	→
		f	PHI を扱う機器	-	-	-	○	○	→
		g	PHI を扱う機器の環境設備	-	-	-	○	○	→
		i-B6	メモリ・ディスク・画面上の認証情報	-	-	-	○	-	↓
		j-B6	メモリ・ディスク・画面上の認可情報	-	-	-	○	○	→
		l	メモリ・ディスク・画面上の認証情報のバックアップ	-	-	-	○	-	↓
		m-B6	認証情報を扱うソフトウェア	-	-	-	○	-	↓
		n-B6	認可情報を扱うソフトウェア	-	-	-	○	○	→
		o	認証情報を扱う機器	-	-	-	○	-	↓
		p	認証情報を扱う機器の環境設備	-	-	-	○	-	↓
C	（病院内） 認証サーバ	b	暗号アルゴリズムと鍵と鍵配送方式	-	○	↑	-	○	↑
		i-C	メモリ・ディスク・画面上の認証情報	-	○	↑	-	○	↑
		l	メモリ・ディスク・画面上の認証情報のバックアップ	-	○	↑	-	○	↑
		m-C	認証情報を扱うソフトウェア	-	○	↑	-	○	↑
		o	認証情報を扱う機器	-	○	↑	-	○	↑
		p	認証情報を扱う機器の環境設備	-	○	↑	-	○	↑
D	（病院内） 利用者 ID 管理サーバ & クライアント	b	暗号アルゴリズムと鍵と鍵配送方式	○	○	→	○	○	→
		i	メモリ・ディスク・画面上の認証情報	○	○	→	○	○	→
		j	メモリ・ディスク・画面上の認可情報	○	○	→	○	○	→
		k	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙	○	○	→	○	○	→
		l	メモリ・ディスク・画面上の認証情報のバックアップ	○	○	→	○	○	→
		m	認証情報を扱うソフトウェア	○	○	→	○	○	→
		n	認可情報を扱うソフトウェア	○	○	→	○	○	→
		o	認証情報を扱う機器	○	○	→	○	○	→

サイト		資産		生理検査判読 （代理ログオン）			外来診察前準備 （Kerberos）		
記号	サイト名	記号	資産内容	導入前	導入後	増減	導入前	導入後	増減
D	（病院内） 利用者 ID 管理サーバ& クライアント	p	認証情報を扱う機器の環境設備	○	○	→	○	○	→
		q	認証情報を扱う操作者	○	○	→	○	○	→
F1	（病院内） ネットワーク【院内】	u	ネットワーク機器のソフトウェア	○	○	→	○	○	→
		v	ネットワーク機器	○	○	→	○	○	→
		w	ネットワーク機器の環境設備	○	○	→	○	○	→
		x	ネットワーク機器の操作者	○	○	→	○	○	→
		y	HCF 内部ネットワーク上の PHI	○	○	→	○	○	→

表７．生理検査判読のリスク分析表

記号	サイト名	記号	資産内容	脅威	脆弱性	リスク	対策	資産価値	起こり易さ	つけこみ易さ	リスク評価
A	（病院内）クライアント	b-C	暗号アルゴリズムと鍵と鍵配送方式（認証サーバ）	暗号化の解読	暗号アルゴリズム、鍵や鍵配送方式の強度不足	暗号化の解読によって漏洩した認証情報による不正ログイン、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	認定暗号アルゴリズムと安全な鍵や鍵配送方式の採用	+1	0	0→-1	+1→0
		i-C	メモリ・ディスク・画面上の認証情報（認証サーバ）	辞書攻撃を用いた不正ログイン	アクセス管理不備	不正ログインによるクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	アクセス管理（ログイン）により権限の無い者の操作を防止	+1	+1	0→-1	+2→+1
				漏洩したパスワードを用いた成りすまし	パスワード強度不足	成りすましによるクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	パスワードの定期的な変更によりパスワードの強度を維持すること	+1	+1	0→-1	+2→+1
		k-B1	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(HIS)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるクライアントまたはアプリケーションサーバ【HIS】内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	■ ■ ■ – ■ ■ ■ ■ ■	■ ■ ■ ■ ■ ■	■ ■ ■ – ■ ■ ■ ■ ■	■ ■ ■ – ■ ■ ■ ■ ■
		k-B2	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(生理部門情報システム)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるクライアントまたはアプリケーションサーバ【生理部門情報システム】内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	■ ■ ■ ■ ■ ■	■ ■ ■ – ■ ■ ■ ■ ■	■ ■ ■ ■ ■ ■	■ ■ ■ – ■ ■ ■ ■ ■
		k-B3	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(レポート作成システム)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるクライアントまたはアプリケーションサーバ【レポート作成システム】内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	■ ■ ■ – ■ ■ ■ ■ ■	■ ■ ■ ■ ■ ■	■ ■ ■ – ■ ■ ■ ■ ■	■ ■ ■ – ■ ■ ■ ■ ■
		k-B4	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(検査情報参照システム)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるクライアントまたはアプリケーションサーバ【検査情報参照システム】内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	■ ■ ■ ■ ■ ■	■ ■ ■ ■ ■ ■	■ ■ ■ ■ ■ ■	■ ■ ■ ■ ■ ■
		k-C	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(認証サーバ)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	+2	+1	+1→0	+4→+3
C	（病院内）認証サーバ	b	暗号アルゴリズムと鍵と鍵配送方式	暗号化の解読	暗号アルゴリズム、鍵や鍵配送方式の強度不足	暗号解読による認証情報が解読され、不正ログイン、成りすましによるクライアントまたはアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	認定暗号アルゴリズムと安全な鍵や鍵配送方式の採用	+2	0	0→-1	+2→+1
		i-C	メモリ・ディスク・画面上の認証情報	第3者、利用者による認証サーバへの辞書攻撃を用いた不正ログイン	アクセス管理不備	不正ログインによるクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	アクセス管理（ログイン）により権限の無い者の操作を防止	+2	+1	0→-1	+3→+2
					監査ログの未確認		監査ログの確認による抑止効果	+2	+1	0→-1	+3→+2
				第3者、利用者によるクライアントの漏洩パスワードを用いた成りすまし	パスワード強度不足	成りすましによるクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	パスワードの定期的な変更によりパスワードの強度を維持すること	+2	+1	0→-1	+3→+2
		I	メモリ・ディスク・画面上の認証情報のバックアップ	バックアップの持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	不正ログイン、成りすましによるクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	+2	+1	+1→0	+4→+3
					入室管理不足		入室管理による権限の無い者の入室防止	+2	+1	+1→0	+4→+3
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	+2	+1	+1→0	+4→+3
		m-C	認証情報を扱うソフトウェア	バックドアや情報を盗み出す不正なプログラムの挿入	コンピュータウイルス対策不足	不正プログラム(I)によって漏洩した認証情報による不正アクセス、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	コンピュータウイルス対策によりバックドアや情報を盗み出すプログラムを検出し駆除	+2	+1	0→-1	+3→+2
				ソフトウェアの不具合、誤作動	仕様不備、バグ	認証機能不能(A)	受け入れ要件の確立、障害時運用の確立	+2	+1	0→-1	+3→+2
		o	認証情報を扱う機器	機器の持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	機器の持出によって漏洩した認証情報による不正ログイン、成りすましによるクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	+2	+1	+1→0	+4→+3
					入室管理不足		入室管理による権限の無い者の入室防止	+2	+1	+1→0	+4→+3
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	+2	+1	+1→0	+4→+3
				故障	点検未実施、老朽化	認証機能不能(A)	保守点検、バックアップにより故障等を予防し認証不能を予防	+3	+1	+1→0	+5→+4
				被災	防災対策不足、事業継続計画未策定	認証機能不能(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	+3	0	+1→+1	+4→+4
				破壊	施錠保管の不徹底	認証機能停止(A)	施錠保管により権限の無い者の接触を防止	+3	+1	+1→0	+5→+4
		p	認証情報を扱う機器の環境設備	故障	点検未実施、老朽化	認証機能不能(A)	保守点検、バックアップによる故障等の予防	+3	+1	+1→0	+5→+4
				被災	防災対策不足、事業継続計画未策定	認証機能不能(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	+3	0	+1→+1	+4→+4
				破壊	施錠保管の不徹底	認証機能停止(A)	施錠保管による権限の無い者の接触を防止	+3	+1	+1→0	+5→+4

表８．外来診察前準備のリスク分析表

記号	サイト名	記号	資産内容	脅威	脆弱性	リスク	対策	資産価値	起こり易さ	つけこみ易さ	リスク評価
A	（病院内）クライアント	b	暗号アルゴリズムと鍵と鍵配送方式	暗号化の解読	暗号アルゴリズム、鍵や鍵配送方式の強度不足	認証情報が漏洩し、不正ログイン、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	認定暗号アルゴリズムと安全な鍵や鍵配送方式の採用	+1	0	0→−1	+1→0
		i	メモリ・ディスク・画面上の認証情報	内部情報への不正アクセス	不正アクセス可能となっている	認証情報が漏洩し、不正ログイン、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	クライアントPCポリシーの変更等による不正アクセス防止	+1	0	0→−1	+1→0
		k−B1	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(HIS)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるHISクライアントまたはアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	−	−	−	−
		k−B5	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(PACS)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるPACSクライアントまたはアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	−	−	−	−
		k−B6	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(レポーティング)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるレポーティングアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	−	−	−	−
		k−C	メモリ・ディスク・画面上の認証情報のメモやプリントアウトの紙(認証サーバ)	認証情報の覗き見／持出による不正ログイン、成りすまし	認証情報のメモやプリントアウトの紙の放置等	不正ログイン、成りすましによるクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	パスワードのメモ書きの禁止	+2	+1	+1→0	+4→+3
		m	認証情報を扱うソフトウェア	バックドアや情報を盗み出す不正なプログラムの挿入	コンピュータウイルス対策不足	不正プログラムによって漏洩した認証情報による不正アクセス、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	コンピュータウイルス対策によりバックドアや情報を盗み出すプログラムを検出し駆除	+1	0	0→−1	+1→0
				ソフトウェアの不具合、誤作動	仕様不備、バグ	認証機能不能(A)	受け入れ要件の確立、障害時運用の確立	+1	−1	0	−
B1	（病院内）アプリケーションサーバ【HIS】	b	暗号アルゴリズムと鍵と鍵配送方式	暗号化の解読	暗号アルゴリズム、鍵や鍵配送方式の強度不足	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	認定暗号アルゴリズムと安全な鍵や鍵配送方式の採用	−	−	−	−
		i−B1	メモリ・ディスク・画面上の認証情報	内部情報への不正アクセス	不正アクセス可能となっている	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	サーバーパスワードの定期的な変更、パスワードポリシーの変更	−	−	−	−
		l	メモリ・ディスク・画面上の認証情報のバックアップ	バックアップの持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	−	−	−	−
					入室管理不足		入室管理による権限の無い者の入室防止	−	−	−	−
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	−	−	−	−
		m−B1	認証情報を扱うソフトウェア	バックドアや情報を盗み出す不正なプログラムの挿入	コンピュータウイルス対策不足	不正プログラムによって漏洩した認証情報による不正アクセス、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	コンピュータウイルス対策によりバックドアや情報を盗み出すプログラムを検出し駆除	−	−	−	−
				ソフトウェアの不具合、誤作動	仕様不備、バグ	認証機能不能(A)	受け入れ要件の確立、障害時運用の確立	−	−	−	−
		o	認証情報を扱う機器	機器の持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	−	−	−	−
					入室管理不足		入室管理による権限の無い者の入室防止	−	−	−	−
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	−	−	−	−
				故障	点検未実施、老朽化	システム使用不可(A)	保守点検、バックアップによる故障等の予防	0	0	0	−
				被災	防災対策不足、事業継続計画未策定	システム使用不可(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	0	0	0	−
				破壊	施錠保管の不徹底	システム使用不可(A)	施錠保管により権限の無い者の接触を防止	0	0	0	−
		p	認証情報を扱う機器の環境設備	故障	点検未実施、老朽化	システム使用不可(A)	保守点検、バックアップによる故障等の予防	0	0	0	−
				被災	防災対策不足、事業継続計画未策定	システム使用不可(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	0	0	0	−
				破壊	施錠保管の不徹底	システム使用不可(A)	施錠保管による権限の無い者の接触を防止	0	0	0	−

記号	サイト名	記号	資産内容	脅威	脆弱性	リスク	対策	資産価値	起こり易さ	つけこみ易さ	リスク評価
B5	(病院内) アプリケーションサーバ 【PACS】	b	暗号アルゴリズムと鍵と鍵配送方式	暗号化の解読	暗号アルゴリズム、鍵や鍵配送方式の強度不足	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	認定暗号アルゴリズムと安全な鍵や鍵配送方式の採用	–	–	–	–
		i-B5	メモリ・ディスク・画面上の認証情報	内部情報への不正アクセス	不正アクセス可能となっている	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	サーバーパスワードの定期的な変更、パスワードポリシーの変更	–	–	–	–
		l	メモリ・ディスク・画面上の認証情報のバックアップ	バックアップの持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	–	–	–	–
					入室管理不足		入室管理による権限の無い者の入室防止	–	–	–	–
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	–	–	–	–
		m-B5	認証情報を扱うソフトウェア	バックドアや情報を盗み出す不正なプログラムの挿入	コンピュータウイルス対策不足	不正プログラムによって漏洩した認証情報による不正アクセス、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	コンピュータウイルス対策によりバックドアや情報を盗み出すプログラムを検出し駆除	–	–	–	–
				ソフトウェアの不具合、誤作動	仕様不備、バグ	認証機能不能(A)	受け入れ要件の確立、障害時運用の確立	–	–	–	–
		o	認証情報を扱う機器	機器の持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	–	–	–	–
					入室管理不足		入室管理による権限の無い者の入室防止	–	–	–	–
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	–	–	–	–
				故障	点検未実施、老朽化	システム使用不可(A)	保守点検、バックアップによる故障等の予防	0	0	0	–
				被災	防災対策不足、事業継続計画未策定	システム使用不可(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	0	0	0	–
				破壊	施錠保管の不徹底	システム使用不可(A)	施錠保管により権限の無い者の接触を防止	0	0	0	–
		p	認証情報を扱う機器の環境設備	故障	点検未実施、老朽化	システム使用不可(A)	保守点検、バックアップによる故障等の予防	0	0	0	–
				被災	防災対策不足、事業継続計画未策定	システム使用不可(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	0	0	0	–
				破壊	施錠保管の不徹底	システム使用不可(A)	施錠保管による権限の無い者の接触を防止	0	0	0	–
B6	(病院内) アプリケーションサーバ【レポーティング】	b	暗号アルゴリズムと鍵と鍵配送方式	暗号化の解読	暗号アルゴリズム、鍵や鍵配送方式の強度不足	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	認定暗号アルゴリズムと安全な鍵や鍵配送方式の採用	–	–	–	–
		i-B6	メモリ・ディスク・画面上の認証情報	内部情報への不正アクセス	不正アクセス可能となっている	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	サーバーパスワードの定期的な変更、パスワードポリシーの変更	–	–	–	–
		l	メモリ・ディスク・画面上の認証情報のバックアップ	バックアップの持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	–	–	–	–
					入室管理不足		入室管理による権限の無い者の入室防止	–	–	–	–
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	–	–	–	–
		m-B6	認証情報を扱うソフトウェア	バックドアや情報を盗み出す不正なプログラムの挿入	コンピュータウイルス対策不足	不正プログラムによって漏洩した認証情報による不正アクセス、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	コンピュータウイルス対策によりバックドアや情報を盗み出すプログラムを検出し駆除	–	–	–	–
				ソフトウェアの不具合、誤作動	仕様不備、バグ	認証機能不能(A)	受け入れ要件の確立、障害時運用の確立	–	–	–	–
		o	認証情報を扱う機器	機器の持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	–	–	–	–
					入室管理不足		入室管理による権限の無い者の入室防止	–	–	–	–
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	–	–	–	–
				故障	点検未実施、老朽化	システム使用不可(A)	保守点検、バックアップによる故障等の予防	0	0	0	–
				被災	防災対策不足、事業継続計画未策定	システム使用不可(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	0	0	0	–
				破壊	施錠保管の不徹底	システム使用不可(A)	施錠保管により権限の無い者の接触を防止	0	0	0	–
		p	認証情報を扱う機器の環境設備	故障	点検未実施、老朽化	システム使用不可(A)	保守点検、バックアップによる故障等の予防	0	0	0	–
				被災	防災対策不足、事業継続計画未策定	システム使用不可(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	0	0	0	–
				破壊	施錠保管の不徹底	システム使用不可(A)	施錠保管による権限の無い者の接触を防止	0	0	0	–

記号	サイト名	記号	資産内容	脅威	脆弱性	リスク	対策	資産価値	起こり易さ	つけこみ易さ	リスク評価
C	(病院内) 認証サーバ	b	暗号アルゴリズムと鍵と鍵配送方式	暗号化の解読	暗号アルゴリズム、鍵や鍵配送方式の強度不足	認証情報が漏洩し、不正ログイン、成りすましにより各サーバ内のPHIの暴露(C)や改竄(I)に繋がる	認定暗号アルゴリズムと安全な鍵や鍵配送方式の採用	+2	0	0→−1	+2→+1
		i−C	メモリ・ディスク・画面上の認証情報	内部情報への不正アクセス	不正アクセス可能となっている	認証情報が漏洩し、不正ログイン、成りすましにより各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	サーバーパスワードの定期的な変更、パスワードポリシーの変更	+2	+1	0→−1	+3→+2
		I	メモリ・ディスク・画面上の認証情報のバックアップ	バックアップの持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	+2	+1	+1→0	+4→+3
					入室管理不足		入室管理による権限の無い者の入室防止	+2	+1	+1→0	+4→+3
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	+2	+1	+1→0	+4→+3
		m−C	認証情報を扱うソフトウェア	バックドアや情報を盗み出す不正なプログラムの挿入	コンピュータウイルス対策不足	不正プログラムによって漏洩した認証情報による不正アクセス、成りすましによりクライアントまたは各アプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	コンピュータウイルス対策によりバックドアや情報を盗み出すプログラムを検出し駆除	+2	0	0→−1	+2→+1
				ソフトウェアの不具合、誤作動	仕様不備、バグ	認証機能不能(A)	受け入れ要件の確立、障害時運用の確立	+3	+1	+1→0	+5→+4
		o	認証情報を扱う機器	機器の持出により不正に入手された認証情報による不正ログイン、成りすまし	施錠保管の不徹底	認証情報が漏洩し、不正ログイン、成りすましによりアプリケーションサーバ内のPHIの暴露(C)や改竄(I)に繋がる	施錠保管による権限の無い者の接触を防止	+2	+1	+1→0	+4→+3
					入室管理不足		入室管理による権限の無い者の入室防止	+2	+1	+1→0	+4→+3
					守秘義務契約の未締結		守秘義務契約締結による操作者の不正行為を牽制	+2	+1	+1→0	+4→+3
				故障	点検未実施、老朽化	全システム使用不可(A)	保守点検、バックアップによる故障等の予防	+3	+1	+1→0	+5→+4
				被災	防災対策不足、事業継続計画未策定	全システム使用不可(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	+3	0	+1→+1	+4→+4
				破壊	施錠保管の不徹底	全システム使用不可(A)	施錠保管により権限の無い者の接触を防止	+3	+1	+1→0	+5→+4
		p	認証情報を扱う機器の環境設備	故障	点検未実施、老朽化	全システム使用不可(A)	保守点検、バックアップによる故障等の予防	+3	+1	+1→0	+5→+4
				被災	防災対策不足、事業継続計画未策定	全システム使用不可(A)	防災対策、事業継続計画による被害損失の最小化と早期回復	+3	0	+1→+1	+4→+4
				破壊	施錠保管の不徹底	全システム使用不可(A)	施錠保管による権限の無い者の接触を防止	+3	+1	+1→0	+5→+4

付録－２　引用規格・引用文献

（１）Kerberos（IETF RFC 1510）　http://datatracker.ietf.org/doc/rfc4120/

（２）IT セキュリティマネジメントの手法　JIS TR X 0036-3:2001

（３）経済産業省　平成 16 年度　先導的分野戦略的情報化推進事業
（医療情報システムにおける相互運用性の実証事業）（システム共通基盤）
シングルサインオン実装仕様書

（４）情報セキュリティのリスクマネジメント　ISO/IEC 27005

付録－３　作成者名簿

作成者（社名五十音順）

下野　兼揮	(株)グッドマン	
松本　義和	サイバートラスト(株)	
西田　慎一郎	(株)島津製作所	
福井　利晃	日本アイ・ビー・エム(株)	
別府　嗣信	日本光電工業(株)	
梶山　孝治	(株)日立製作所	
山岡　弘明	富士通(株)	◎主査
喜多　紘一	(一社)保健医療福祉情報安全管理適合性評価協会	
平田　泰三	(一社)保健医療福祉情報システム工業会（特別委員）	
宮崎　一哉	三菱電機(株)	
茗原　秀幸	三菱電機(株)	

改定履歴		
日付	バージョン	内容
2016年6月	Ver. 1.0	初版

（ＪＡＨＩＳ標準　１６－００２）
２０１６年6月発行

ＪＡＨＩＳ　シングルサインオンにおける
セキュリティガイドライン　Ｖｅｒ．１．０

発行元　一般社団法人　保健医療福祉情報システム工業会
〒１０５－０００４　東京都港区新橋２丁目５番５号
（新橋２丁目ＭＴビル５階）

電話　03-3506-8010　　FAX　03-3506-8070