Evidian

PERSPECTIVES

機密情報の保護：病院におけるアクセス制御

このホワイトペーパーでは、大学病院が医療従事者用スマートカードを用いて設定する、アイデンティティとアクセス管理システムについて説明します。

医療従事者カードに責任を持つ政府組織によって実施されたケーススタディに基づきます。

機密情報の保護

多くの国で医療制度内の患者データの機密保持に関する法律が制定されています。ヨーロッパでは、これらの法律の多くが、欧州連合のデータ保護に関する 1995/46/EC ディレクティブに基づいています。

病院では、患者の機密情報を確実に保護するために、臨床医による医療データへのアクセス方法を考え直さなければならない場合があります。

これは一方で、病院の情報システムのさまざまな面を近代化する良い機会でもあります。多くの場合、法律はアプリケーションへの個人のアクセス、アクセスの追跡可能性、医療データのプライバシーの保護など、常識的な推奨事項を公的に定めているにすぎません。

目標が明確に定められている場合でも、納得のいくタイムリーで実用的な結果を低コストで実現するには、適切なプロジェクト計画が必要です。このドキュメントでは、Evidian のソリューションを使用した、このプロジェクト計画の例を紹介します。

このホワイトペーパーは、医療従事者向け国内 ID スマートカードを扱っているフランスの公的機関によって実施された実際のカード調査を要約したものです。調査では、Evidian のアイデンティティとアクセス管理ソリューションを使用して、スマートカードアクセス制御を情報システムに展開している大学病院について説明しています。

ASIP Santé は、医療情報システムに向けて医療従事者のアイデンティティと資格を認定するフランスの公的組織です。この組織は、フランスの医療従事者に従事者用 ID スマートカード「CPS」を発行しています。CPS を携帯していると、医療アプリケーションやその他の従事者によって安全な方法で認証されます。

ASIP Santé は 「Shared Directory of Healthcare Professionals 」（RPPS：医療従事者の共有ディレクトリ）の実装も行っています。RPPS は、医療従事者 ID のフランス国内のリポジトリとして使用される予定です。

詳細な情報は、www.asipsante.fr をご参照ください。

病院

包括的な情報システム

この病院は病床数 1,500 の大学病院です。この病院では 900 人の医療および薬剤スタッフ メンバーと 4,540 人の非医療スタッフ メンバー（そのうち 3,500 人が健康管理に割り当てられています）を雇用しています。

- 患者レコード管理 （McKesson）、人事、財務管理、イメージング、スケジューリングなどの 140 のアプリケーションをホストする 60 台の物理サーバーがあります。
- 病院アプリケーションには 31,400 の認可があります。
- 4,500 のアカウントが名前でディレクトリにリストされています。通常、各アカウントは情報システムの名前付きユーザーと 1 対 1 で対応しています。
- 病院のスタッフは 2,400 台の PC を使用できますが、そのうちの 1,400 台ではスマートカードによるアクセスの保護が必要です。スマートカードで保護されていない PC は医療レコードにアクセスできません。

病院のセキュリティ アプローチ

この病院では、数年前に独自のスマートカードを使用する識別および認証システムを構成しました。

病院の第 1 の目的は、就業時間の管理でした。1998 年以降は、カードベースの物理アクセス制御を展開して就業時間および欠勤の計算を自動化してきました。

その後、アクセス カードの使用を Windows ワークステーションに拡張しました。論理アクセス制御システムは、最初はシングルサインオンによって拡張され、その後は患者レコード管理アプリケーションのアカウントを自動更新することにより拡張されました。

病院は最後に、医療従事者用の国内 ID スマートカードを使用できるようにシステムを拡張しました。また、医療スタッフが頻繁に使用する事例を考慮してシステムを変更しました。

その結果、セキュリティ、機密性、およびアクセス制御に積極的アプローチを採用して、規制の制約に事前に対処しました。この病院では、法規制の大部分は常識的な基準を公的に定めたものと見なされています。

プロジェクト

開始点：セキュリティ ポリシーの実装

医療施設はそのアイデンティティとアクセス管理システムを最適化する必要があります。これには、データ プライバシー、パスワード排除による使いやすさ、臨床医名別の手順の追跡、ヘルプデスク コストの削減などが含まれます。

国の法律では、これらの目標のいくつかが正式に定められています。特に、IT 部門で注意が必要なのは次の 2 つのポイントです。

- **患者の医療情報にアクセスするために、医療従事者用スマートカードによる認証が必須**
  つまり、医療アプリケーションにアクセスするためには、スマートカードによる事前認証が必要になります。医者や看護師が使用するスマートカードは正式な CPS カードですが、インターンや実習生は病院が管理するカードを使用します。

- **アプリケーションの指名認証**
  すべての医療スタッフ メンバーには独自のアプリケーション用アカウントが必要です。汎用アカウントを排除すれば、医療行為の追跡可能性が向上します。

実際、これらのガイドラインの実装中には、次のような問題に直面することがよくあります。

- **国内 ID スマートカードをサポートしていないアプリケーションはどうしたらよいのでしょうか？**
  CPS カードをサポートしているソフトウェア ベンダーとサポートしていないベンダーがあります。また、病院が何年も前に院内で開発したアプリケーションを使用していることがよくあります。多くの場合、これらのアプリケーションの使用を中止したり、アプリケーションを修正することはできません。

- **汎用アカウントはどうなるのでしょうか？**
  潜在的なユーザーは人事などで認識されますが、すべての人が病院ディレクトリに個人のアカウントを持っているわけではありません。代わりに、これらのユーザーは汎用アカウントを使用します。場合によっては、実際のユーザー数がアカウント数の 10 倍になることもあります。これらの汎用アカウントはしばしば便宜上（迅速で容易なアクセス、一時的に部門を支援するスタッフ メンバー用など）使用されます。これらの使用事例をすべて考慮する必要があります。

- **共有ワークステーション（キオスク、緊急処置室）はどのようにするのでしょうか？**
  「1 ユーザー、1 PC」の規則に従う病院など存在しません。PC へのアクセスを単純に特定のスマートカードの所有者に制限することはできません。ユーザーは、カート、室内、または ER で、他のユーザーの後に PC を使用します。また、ユーザーの切り替え（セキュリティが十分でないステーションでは当然時間はかかりません）にかかる時間は数秒以内でなければなりません。

- **アカウントの作成、配布、および管理はどのようにするのでしょうか？**
  いくつかの汎用アカウントを何百もの名前付きアカウントに置き換えると、アカウントの管理に関連する作業負荷が大幅に増えます。
  これらのアカウントは作成するだけでなく、定期的に更新（変更、削除など）する必要もあります。

- **スマートカードは情報システムでどのように管理および使用するのでしょうか？**
  スマートカードをディレクトリ内のユーザー アカウントに簡単にリンクさせる方法が必要です。システムでは、国家組織の公式ブラック リストの更新を処理する必要があります。

これらの技術的な問題だけでなく、潜在的な人的問題も忘れてはなりません。実際、医療従事者は、アプリケーションが常に開いている（したがっていつでも利用可能な）安全ではないモードから、スマートカードによるログインを要求されるモードに切り替えます。これは、治療を行う上で障害と考えられる場合があります。

したがって、これから説明するテクニカル ソリューションは、説明会およびトレーニング セッションと併せて展開することが不可欠です。パイロット ユーザーを慎重に選択し、医療スタッフ メンバーと準備のミーティングを開く必要があります。ソリューションの使用を促進するためには、ソリューションがスタッフ メンバーに実際の付加価値を提供するものであることが重要です。

ユーザーには、情報セキュリティが施設の医療目標に役立つ付加価値であることも知らせる必要があります。セキュリティにより、医療従事者間の協力体制の改善、病院の資産保護、およびリスクの制御が実現します。これらの原則は、施設のセキュリティ ポリシーの中心となります。

アンサー：アイデンティティとアクセス管理

大学病院では、アイデンティティとアクセス管理の統合ソリューションによって、これらの必要条件に一貫性のある技術的な方法で対処することが分かりました。このソリューションを使用すると段階的なアプリケーションへのアクセスのための指名管理を実施できます。この管理は、CPS スマートカードにより制御され、アクセス試行が記録される一元管理されたログを使用します。

これらの操作の制約に対応するための、病院の主な必要条件は次のとおりです。

- スマートカードを使用してパスワードの負担をなくす。このため、スマートカードによるログインはユーザーに実際のサービスを提供し、容易に受け入れられます。
- 医療または管理アプリケーションを変更しない。
- 人事がユーザーの管理に使用している手順を変更しない。
- サポート担当者を介さずにアクセス（欠勤、緊急時対応策など）を委譲可能にする。
- 二重管理を回避するために、スマートカードをユーザーにすばやくリンクできるようにする。
- 簡易ログインで十分な猶予時間を設ける。
- キオスク ワークステーションを使用するスタッフ メンバーが数秒以内に認証され、アプリケーションにアクセスできるようにする。

このようなソリューションを実装するには、従来から次の 3 つの段階が必要です。現在は何百もの顧客に対して構築されています。

1. **人事などの既存のデータベースとの同期による完全なアイデンティティ リポジトリの構築**
   このリポジトリには病院の既存のディレクトリを使用することができ、拡張して新しいユーザーを保存できます。

2. **スマートカード認証と組み合わせたシングルサインオン（SSO）の展開**
   この方法では、使用中のアプリケーション アカウントが汎用アカウントであっても、アプリケーションに対して名前に基づく認証を行い、使用履歴を管理します。

3. **アプリケーション アカウントの自動更新**
   これにより汎用アカウントおよび認証なしアカウントの排除が可能になります。段階 2 の使用状況ログに基づいてユーザーにアカウントが割り当てられます。この割り当ては、ユーザーのロール、部門、または施設に基づいて実行することをお勧めします。

いくつかのプロジェクトでは段階 2 と 3 が逆になります。ただし、このアプローチはお勧めできません。段階 2 で構築した実際のアクセスに関する情報がない状態でアクセスポリシーを定義するには時間がかかり、プロセスも複雑になります。

シングル サインオンを使用する理由

アイデンティティとアクセス管理ソリューションに欠かすことのできないシングルサインオン（SSO）では、アプリケーションへのアクセス時にユーザーではなく SSO がユーザー名とパスワードを入力します。

SSO は、スマートカード認証を使用する理由をユーザーに理解してもらうための**強力な根拠**になります。セキュリティに SSO を加えると、ユーザーは特定の PC アクセス機能で使用するときに「自分のカードが自分のすべてのパスワードの代わりになる」および「自分のカードで自分の作業セッションにアクセスできる」ことに気づきます。つまり、このソリューションはユーザーにとって役に立つものであり、障害ではありません。

技術的な観点から見ると、ユーザー名とパスワードは中央のデータベースや病院のディレクトリなどの仮想「金庫」に安全に保管されます。PC にインストールされている SSO クライアント ソフトウェアはこの情報を使用して、従業員を適切に認証した後に、ユーザーの代わりにパスワードを管理 （パスワードの変更など）します。

このように、ソフトウェアで病院のセキュリティ ポリシーに対応できます。管理者は、ユーザーのロールと使用されているワークステーションの種類に基づいてポリシーを主に定義します。

病院によっては、このローカル ソリューションを Web アプリケーション用のクライアントレス SSO で拡張します。これにより、医師は自宅から PKI 証明書を使用して認証を受け、電子メールや患者レコードなどの病院の Web アプリケーションにアクセスすることができます。

ニーズの定義

アイデンティティとアクセス管理システムはどのように選択し、選択後にサービス プロバイダーがそのシステムを適切に展開するにはどうしたらよいのでしょうか？ 実際は、ジョブを実行する必要のある医療スタッフ メンバーに展開しているシステムが頭痛の種と思われないようにする必要があります。

したがって、この病院では使用事例に基づく方法を導入しました。何人かの医療スタッフ メンバーの行動を記述することで、ソリューションは用途に十分に対応できるようになります。

ワークステーションの機能インベントリー

最初に、ワークステーションのインベントリーを作成します。作成されたインベントリーは、PC とその用途の類型（専用または共有、固定またはモバイル、および有用性または ISO 14644 規格などの清浄度制約）になります。

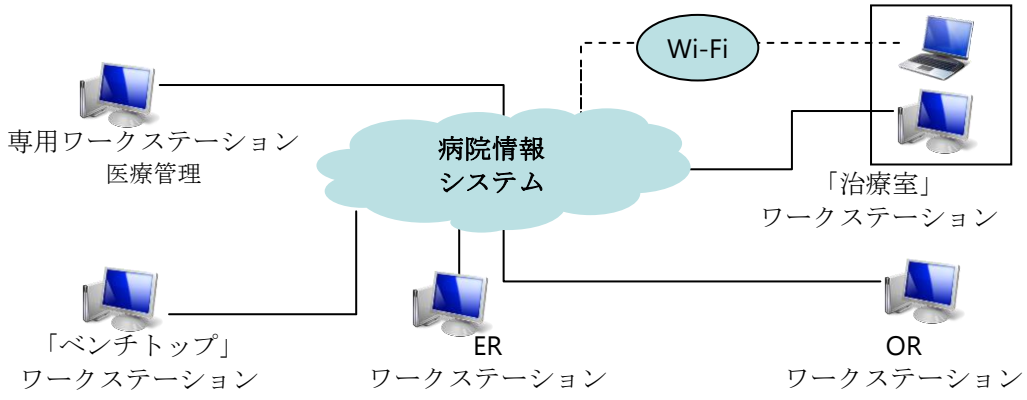

図 1: ワークステーションの類型

通常、これらのワークステーションでは、次のような複数のユーザー アクセス タイプが存在します。

- *固定モード：* 1 台の PC に 1 人のユーザー
- ローミング モード：複数台の PC に 1 人のユーザー
- キオスク モード：*1 台の PC に複数のユーザー*
- リモート アクセス モード：特定の時間に 1 台の PC に 1 人のユーザー（VPN を使用する場合など）

このインベントリーを使用して使用事例を文書化した後に、スマートカード リーダーの展開を計画します。以下の例は意図的に簡易なものにしています。実際には、使用制約とワークステーションのタイプはこれより詳細になります。

ワークステーションのタイプ	主要なアクセス タイプ	制約
専用ワークステーション	固定	低
「ベンチトップ」ワークステーション	固定	低
「治療室」ワークステーション	ローミング キオスク	瞬時にユーザーを切り替える必要有り
「緊急」ワークステーション	キオスク（集中）	瞬時にユーザーを切り替える必要有り 、有用性
「手術室」ワークステーション	キオスク	衛生

アクセス セキュリティの機能ニーズ

この最初の区分では、シングルサインオン（SSO）などのアクセス セキュリティの観点から見たニーズを明確にします。次の機能は、特定のタイプのワークステーションに制限する必要があります。たとえば、固定ワークステーションでは瞬時にユーザーを切り替える必要性がありません。

- セッションを開くときまたは再度開くときの強固な認証。
- スマートカードが取り出されると、すぐにセッションがロックされます。アプリケーションは開いたままの場合と閉じる場合があります。アプリケーションは別のユーザーがログインすると閉じます。
- スマートカードが取り出された場合でもセッションは開いたままですが、一定の時間（無操作期間）が経過した後セッションは閉じます。
- 瞬時にセッションを切り替え。セッションがロックされているかどうかは関係ありません。
- 猶予時間：最初の強固な認証の後、ユーザーは一定期間 PIN を入力せずに再認証されます。猶予時間は、ある PC から別の PC へユーザーを「フォロー」します。
- 必要なインフラストラクチャがインストールされている場合（Citrix XenApp など）、そのインフラストラクチャはローミング セッションをサポートする必要があります。

対象機能アーキテクチャーの選択

一貫性を保つため、認可とアイデンティティに関するすべての情報はリポジトリとして使用されるディレクトリに保存されます（PC およびアプリケーションへのログイン試行と管理処理の履歴はリレーショナル データベースに保存されます）。

このディレクトリは「正式な」（「authoritative」）データベース（人事など）から同期メカニズムで自動的に更新、または認可とロールを管理する管理者によって更新されます。

認可は、従業員が現在使用中のアプリケーションとリソースにすでに存在しているアカウントと比較されます。これらの比較は、同期（「synchronization」）と調整（「reconciliation」）により行われます。

アカウントの更新は、手動か自動（最も一般的に使用されるアプリケーションの場合）かに関係なく、アプリケーションで定期的にトリガされます。これにより、孤立したアカウントまたは汎用アカウントを削除できます。

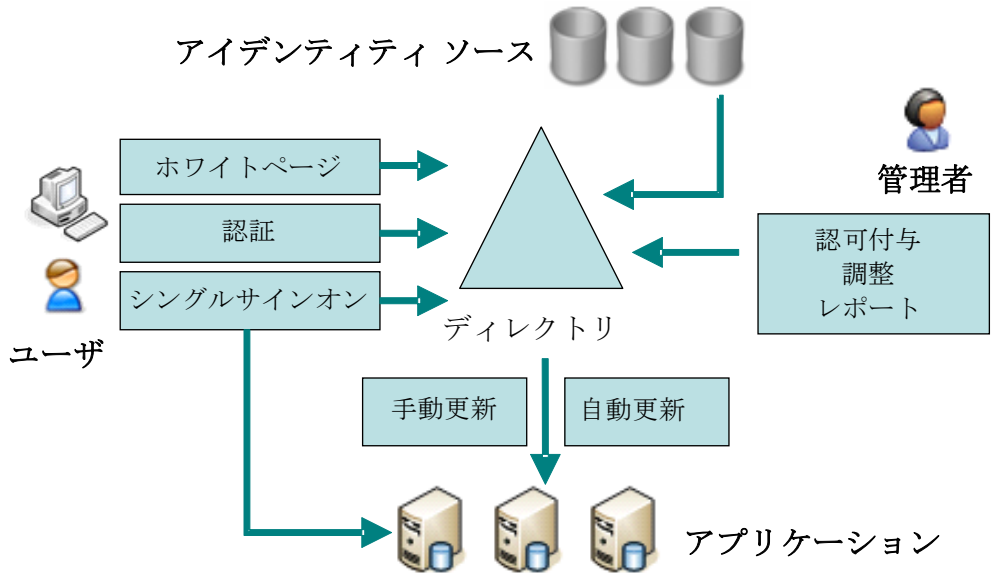

図 2: 機能アーキテクチャーの概略

この病院では、Evidian IAM ソフトウェア スイートでアイデンティティとアクセス管理を処理します。このソフトウェア スイートのシングルサインオン モジュールは Evidian Enterprise SSO 、様々な論理アクセス ケースに対応する認証強化 モジュールは Evidian Authentication Manager です（このホワイトペーパーで表記する「SSO」は Evidian Authentication Manager と Evidian Enterprise SSO の組み合わせを指しております）。このソリューションの利点は、アイデンティティ同期 （Evidian ID Synchronization）、アプリケーション上のアカウント プロビジョニングまたはセキュリティ ポリシーの管理（Evidian Policy Manager）、およびユーザーからアクセス リクエストの管理ツール（Evidian Request Manager – 認可ワークフロー）とネイティブに統合される点です。

セキュリティ ポリシー：必須要素

アイデンティティとアクセス ソリューションは病院のセキュリティ ポリシーをサポートしますが、セキュリティ ポリシーの代わりにはなりません。このソリューションでは、すべての PC とすべてのユーザーがポリシーに確実に準拠しなければなりません。また、従業員を困惑させることなく、セキュリティ規則を厳格化することもできます。

最後に、ソリューションにはセキュリティ規則の有効性を表すレポートと一元管理される指標が必要です。これにより実施可能な修正を迅速に展開できるようになります。

完全なセキュリティ ポリシーは、基本原則と一般規則で構成され、リスク分類、物理セキュリティ、緊急時対応策などの多くの領域に対応します。コンピュータ セキュリティはこの包括的なポリシーのほんの一面です。

ここで説明する使用事例は、病院の IT セキュリティ ポリシーの一部です。次のことを実行するために策定されます。

- PC へのアクセスを許可する前に、すべてのユーザーは機密性に関する義務を規定するユーザー*契約*に署名する必要があります。
- 病院の内外を問わず、すべてのユーザーが*一意に識別され*、ユーザーの出勤、欠勤、退勤が監視されます。
- アクセス権限は、定期的に見直される*プロファイル*および規則（ジョブまたはミッション、割り当て、および活動領域）に基づいて割り当てられます。
- プライマリ認証は、*証明書*に基づいて実行されます。
- アプリケーションのパスワードは*複雑*で、ユーザーはパスワードを知りません。
- *緊急アクセス モード*では、医療のニーズがセキュリティよりも優先される場合にアクセス権限を付与します。

このポリシーには、セッションを開くときの保護、アクティブでないセッションのロック、監査可能なトレースなどのいくつかの技術的なメカニズムが含まれています。

使用事例

以下の使用事例は、*実際の使用シナリオ*に基づいています。ここで示す要約では、操作制約に基づくソリューションの予測される動作を説明します。これらが正式に定められると、これらの説明が仕様の機能部分の原則を示し、実装中に参照として使用することができます。

当事者

この使用事例では、産婦人科に属する先輩／後輩医師であるパトリシアとロバートに焦点を当てます。2 人は、日中に病院内の何人かの医療スタッフ メンバーとやりとりします。スタッフ メンバーも情報システムを使用します。

	パトリシア、産婦人科医		**ロバート**、インターン
	クララ、麻酔専門看護師		**エリザベス**、創傷ケア看護師
	メアリー、助産師		**エリック**、生物学者

08:00	ロバートとパトリシアは先輩／後輩医師としてペアで働いています。彼らは病院に出勤し、スタッフ ミーティングに参加します。
08:30	彼らは手術室にいます。2 件の帝王切開と 1 件の子宮摘出がスケジュールされています。クララとエリザベス が同じチームに属しています。
13:15	昼食
14:00	パトリシアは診察を開始します。
17:00	パトリシアは事務処理とレポートの作成を行います。
18:00	パトリシアは手術室でロバートに会い、引き継ぎを準備します。2 人は退出する同僚と話し合い、ケース ファイルを渡されます。
18:20	ロバートはメアリーとともに病院内に巡回します。
19:30	ロバートは再診察を開始します。
20:15	ロバートは ER に呼び出されます（子宮外妊娠の疑い）。エリックが行う解析の結果が必要です。
21:30	ßHCG のテスト結果は陽性でした。ロバートはパトリシアを呼び、パトリシアは患者を診察し、診断を確認します。
22:10	手術室に戻ります。

a) 初回のアクセスと患者ファイルの閲覧

プロセス

1. パトリシアとロバートは部門のミーティングに参加しています。同僚と話し合い、同時に患者のファイルにアクセスしています。

2. 手術室で、クララがシステムにログインし、患者ファイルを開いて、最初の手術に必要な医療情報（患者が最近食事しているか、アレルギーがあるか、薬物配合禁忌など）を確認します。

3. 手術室で、数分後にエリザベスが別のワークステーションで同じ作業を行い、必要な情報（手順、アレルギーなど）を閲覧します。

リソースの使用

ロバート、パトリシア、エリザベス、クララの場合、これがこの日の最初の認証になります。

したがって、彼らはセッションが開いていないワークステーションで CPS スマートカード（ロバートはインターン用のスマートカード）と PIN を使用して強固な認証を実行します。

b) 手術室のワークステーションでの閲覧

プロセス

4. ロバートとパトリシアはエリザベスが使用しているワークステーションで、患者が待機している手術室に入る前に患者のファイルを調べます。

5. 手術中、クララは患者の診療録にログインし、医療情報を入力します。

リソースの使用

ロバート、パトリシア、エリザベス、クララは、キオスク モードで利用可能なワークステーションで、手術室内でファイルを閲覧します。

エリザベスはカードを取り出してセッションをロックします。次に、ロバートがカードを挿入し、SSO で認証されます。

手術室のワークステーションはスタッフ ミーティングで使用した PC と同じグループに属していないため、ロバートは強固な認証（スマートカードと PIN 入力）を実行します。

ワークステーションは無操作期間の後にロックされるか、またはキーボードやスマートカードを使用してロックされます。非接触型カードが使用されている場合、非接触型カードをもう一度かざすとワークステーションがロックされます。

c) 手術レポートの作成

プロセス

6. 手順の後、ロバートは手術レポートを作成し、そのレポートをパトリシアが検証します。ロバートは適切なコードに基づいて実行された手順をファイルに書き込みます。

リソースの使用

ロバートは手術前と同じワークステーションで認証されます。このワークステーションではセッションがロックされていました。彼は自分のスマートカードで SSO を介して「*簡易認証*」（PIN の入力を省略）を実行します。

ロバートには猶予時間が与えられています。その期間、システムにログインするには簡易認証で十分です。この猶予時間の有無（およびその長さ）は病院がセキュリティ ポリシーで定義します。

ロバートはパトリシアの責任の下で仕事をしています。パトリシアは自分のアイデンティティを使用してレポートをサインオフする必要があります。

d) オフィスのワークステーションと病院の IT アクセス

プロセス

7. 午後になると、パトリシアは患者を診察したり、患者のファイルにアクセスしたり、ワークステーションのオフィス ツールを使用したりします。彼女はこれらの手順を請求用に該当のコードを入力します。

リソースの使用

パトリシアは自分のオフィスで専用の PC を使用した後に、診察室にあるキオスク モードで利用可能なワークステーションを使用します。パトリシアは自分のワークステーションで SSO を介して強固な認証（スマートカードと PIN の入力）を実行します。

次に、開いているセッションのないキオスク ワークステーションで簡易認証（スマートカードのみ）を行います。ここで PIN 入力の省略が可能なのは、ワークステーションがパトリシアのオフィスの PC と同じグループに属しているからです。

e) 患者ファイルの情報交換

プロセス

8. パトリシアとロバートは同僚と話し合いをしました（伝達）。この場合コンピュータへのログインは不要です。

9. 病院内の巡回と再診察中に、ロバートとメアリーはモバイル ワークステーションまたはいくつかの「治療室」ワークステーションを使用して、医療ファイルにアクセスします。

リソースの使用

ロバートとメアリーは、キオスク モードで利用可能なモバイル ワークステーションを使用します。

病院内または手術室等で SSO を介して簡易認証（スマートカードのみ） で患者ファイルにアクセスします。
ロバートとメアリーは*瞬時なユーザー切り替え*により、同じワークステーションをキオスク モードで交互に使用できます。

Windows セッションは同じですが、ロバートとメアリーにはそれぞれ独自の SSO セッションが割り当てられています。患者ファイルへのアクセス制御はユーザー名で識別されるため、病院は監査を実行してアプリケーションにアクセスした人を確認できます。

f) 生物学的解析でのやりとり

プロセス

10. ER でロバートは患者を診察したり、超音波走査を実行したり、緊急検査を依頼したりします。彼は病院のコンピュータ システムにログインします。

11. エリックは、ロバートから依頼された生物学的解析を行って、結果を検証します。

12. ER からロバートは結果を閲覧します。パトリシアに電話します。

リソースの使用

夕方、ロバートは ER で キオスク モードで利用可能なワークステーションを使用します。

ロバートは SSO を介して強固な認証を実行します。この最初の強固な認証が必要なのは、ER ワークステーションが、以前彼が使用したグループと同じグループに属していないためです。

エリックは自分のオフィスでワークステーションを使用し、SSO を使用するスマートカード認証で生物学的解析の結果を入力します。

後から、ロバートは ER の瞬時ユーザー切り替えによる非接触簡易認証を使用します。その後、キオスク ワークステーションで解析の結果を閲覧します。

実際の展開

カードの自己登録

ユーザーにスマートカードが発行されたら、このカードをディレクトリ内のユーザー名とリンクさせる必要があります。基本的に、スマートカードはユーザーの従来のログインに代わるものです。

しかし、病院の管理の作業負荷を増やすことなく、これらの対応を作成および維持するためにはどのようにしたらよいのでしょうか？

これを実現するため、病院は互換性のある SSO ソフトウェアを使用する*自己登録*メカニズムを選択しました。公的フランス政府組織である ASIP Santé は、ソリューションが提供する柔軟性に基づいてこの選択をサポートします。

シナリオは次のとおりです。自分の Windows パスワードを知っていて、スマートカードを所有しているユーザーについて取り上げます。

1. 医療従事者は自分のスマートカードをワークステーションに挿入し、SSO により表示されるログオン ダイアログに PIN を入力します。

2. 次に、通常セッションを開くときに使用するユーザー名とパスワードを入力します。

3. これ以降は、従来のユーザー名とパスワードではなく、スマートカードと PIN でセッションにアクセスできます。

当然、この対応を有効にする前に、SSO ソフトウェアがバックグラウンドで多数の検証を実行します。

a. SSO ソフトウェアは、RPPS ID などのカードの証明書の内容に基づいて LDAP または Active Directory アカウントを識別します。RPPS はフランスの医療従事者アイデンティティが保存される将来の国内リポジトリです。

b. SSO ソフトウェアで、ユーザー名とパスワードが有効であるか検証されます。

c. 証明書がチェックされ、その参照が病院のディレクトリに追加されます。

d. 最後に、SSO ソフトウェアはユーザーのプライマリ アカウントのパスワードを変更します。

このメカニズムの主な利点は、管理オーバーヘッドが低いという点です。施設のディレクトリは自己更新されるため、大量のインポートは不要です。

ワークステーションで認証された後に同様のメカニズムが採用されて、ユーザーがすでに知っているアプリケーション パスワードが SSO ソフトウェアに「*伝播*」されます。ユーザーはこれらのユーザー名とパスワードを最後に一度だけ入力し、再び入力する必要はありません。その後、SSO がユーザーの代わりにパスワードを変更します。

アカウントのプロビジョニング

プロビジョニング プロセスでは、ユーザーのロールから導かれたユーザーのニーズに基づいてアプリケーション アカウントの作成・更新がトリガーされます。

この機能には、アイデンティティとアクセス管理ソリューションの有用な追加機能として、いくつかの規制に関する利点があります。セカンダリ ユーザー名がアプリケーションに自動的に伝播されるので、医療スタッフ メンバーを容易に識別できます。

したがって、国の医療従事者識別番号は、EHR （「Electronic Health Record」：電子医療レコード）アプリケーションの医療従事者が行っているアクションに関連付けられます。

また、SSO と組み合わせると、プロビジョニングによってアプリケーションの展開とセキュリティが容易になります。

- 病院に出勤するインターンは非常にすばやくアクセス権を得られるようになります。新しく作成したアカウントのユーザー名とパスワードをインターンに教える必要はありません。プロビジョニング プロセスによってこの情報はすでに SSO ソフトウェアに伝播されています。

- アプリケーションのパスワードを複雑化または頻繁に変更することが可能になります。SSO を使用すると、ユーザーはパスワードを知ることがなくなるので、これを目にすることはありません。

SSO とプロビジョニングはセキュリティ チェーンの強力なリンクです。ただし、これらはほんの一部にすぎません。アプリケーションの欠落部分を補うことができるだけです。アプリケーションそのものが基本のセキュリティ規則（パスワードの送信、データ ストレージなど）に準拠する必要があります。

病院リソースへの外部 Web アクセスの保護

シフトが終わり病院を退勤するときに、医師および医療従事者は必ずしも仕事を中断するわけではありません。自宅、オフィス、その他どこからでも、患者ファイルに入力したり、解析結果を閲覧したり、内部のメールを読むことができる必要があります。

病院は、医師や医療従事者が、特に医療業務オフィスの PC から病院の Web アプリケーション（電子メール、患者ファイル管理など）にアクセスできるようにしたいと考えています。アクセス セキュリティはスマートカードで補強されます。当然、アクセスには SSO を使用するため、医師はアプリケーション パスワードを入力する必要はありません。

テクニカルな観点から、病院は Web データが通過するゲートウェイを設置します。ゲートウェイを複製して高可用性を実現できます。すべての Web トラフィックはこのゲートウェイを通じて暗号化される必要があります。病院は、このためにアプリケーションを再設定したくないと考えています。

ゲートウェイのデータ（パスワード、アカウントなど）は SSO ソリューションで共有されます。これにより、この情報を同期したり、インポートする必要がなくなります。たとえば、内部の SSO で Web アプリケーションのパスワードを変更した場合、外部の Web アクセス SSO は透過的に機能する必要があり、その反対も同様です。

展開から得た教訓

単なるツールではないセキュリティ

アイデンティティとアクセス管理ソリューションは、病院のセキュリティ ポリシーの一要素でなければなりません。したがって、計画段階で**実装の決断**を下し、時には妥協する必要があります。次に例を挙げます。

- **認証**：PIN が不要の猶予時間は特に非接触モードで役立ちますが、原理的に認証の強度を下げます。ただし、このメカニズムにより以前は実現できなかった認証の簡略化を実現できるようになります。
- **機密性**：適切に設計された SSO ツールのインフラストクチャでは、それ自身によって大きな脆弱性は生じません。ただし、既存の情報システムに固有の他のリスクとして、アプリケーション データ フロー（特に部分的に Wi-Fi ネットワーク上にある場合）、データ ストレージなどが存在します。したがって、リスクの分析を情報システム全体に対して実行する必要があります。
- **追跡可能性と証拠の保存**: SSO ソリューションは、アプリケーションと PC へのログイン試行およびアクセス権限の管理に限定された部分的なログを保持します。ログが保存される状況が最適であることを確認する必要もあります。

信頼のチェーンに含まれる多くのリンク

信頼のチェーンでは、様々な要素が様々なタイプのリスクに対応します。

アプリケーション

スマートカードベースの制御システムでは、セキュリティ ポリシーに基づいて適切なユーザーが適切なアプリケーションを使用します。プロビジョニング システムでは、これらのユーザーに適切なアプリケーション プロファイル（看護師、インターンなど）を自動的に割り当てることができます。

ただし、アプリケーションそのものだけで、プロファイルを使用して識別および認証されるユーザーの行動を制御できます。これには次が含まれます。

- アプリケーションの整合性
- 職責／信頼性
- 否認不可
- 持続可能性
- アプリケーションの可用性
- アプリケーション情報の保存
- アクションのタイム スタンプ作成

アイデンティティとアクセス管理

スマートカードベースの制御システムでは、適切なプロファイルを使用した病院リソースへのアクセスを重視します。

- 関係者の識別
- 認証
- アクセス制御による機密性
- ワークステーションおよびアプリケーション アクセスのタイム スタンプ作成
- アクセスの可用性（キャッシュなど）
- アクセスの証拠の保存

その他のドメイン

信頼のチェーンの他の面を明確に分析し、必要に応じて修正する必要があります。

- データ フローの機密性
- データベースの機密性、整合性、可用性、および持続可能性

展開において人的側面を軽視しない

展開を成功させるには、病院の従業員を協力者として扱うことが必要です。このためには、人的および組織的側面を予測しなければなりません。

- **病院の情報システムへのアクセスの継続性に関する信頼を築く**
  スマートカードをどのように更新しますか？ カードがなくなったり、盗難にあった場合どうしますか？ このような場合は、新しい手順（緊急アクセスなど）を作成および配布する必要があります。

- **いくつかの部門の長からの特定のリクエストに対応する**
  これらのリクエストにはできるだけ早い段階で（パイロット インストールなど）対処し、SSO ソリューションで構成する必要があります。

- **非常に特殊なビジネス コンテキストに対応する**
  ER および手術室ではソリューションをどのように使用するのでしょうか？ 多くの場合、この答えは、瞬時なユーザー切り替え、非接触型カードなどの機能になります。

- **リストに載っていないスタッフ メンバーや学生にスマートカードを割り当てる**
  インターンはすでに仮カードを持っていますが、他のすべての人はどのようにするのでしょうか？ これは、大学や政府組織と話し合う問題です。

39 J2 62LV 03 – Duplicopy

© Eviden. Evidian is the registered trademark of Eviden. All products, brand names, service marks, trademarks and other names mentioned in this document are proprietary to their respective owners and are protected by applicable trademark and copyright laws. Evidian reserves the right to modify the characteristics of its products without prior notice.