7R-8

異なる医療情報ネットワークドメインにおけるアクセス制御と権限付与に関する研究

佐藤守[1]　谷内田益義[1]　鈴木裕之[1]　小尾高史[2]　山口雅浩[1]　大山永昭[1]　喜多紘一[1]
[1]東京工業大学像情報工学施設　[2]東京工業大学大学院総合理工学研究科

1. はじめに

近年、目覚ましい情報技術の発達に伴い、医療分野においても電子カルテに代表される業務の電子化が進められている。今後は電子化されたシステムを、インターネットのようなオープンなネットワークを通じて連携させることで、より高度なサービスを安全かつ低コストで利用可能な医療システムの実現が期待されている。しかし、現状のシステムを相互運用させるためには、ベンダーによる仕様の相違、セキュリティを確保するコスト、データ標準化の未整備等、多くの問題が存在する。標準化に関しては、徐々に整備されつつあり、仕様の違いも標準的なデータ形式やプロトコルを用いて解決する方向にあるが、セキュリティに関しては医療機関各自のネットワーク（ドメイン）中での整備にとどまっている。

このようなネットワークシステムにおけるセキュリティに関しては、大きく二つの課題が存在する。主体（利用者や機器）の特定と、通信路であるネットワークの安全性の確保である。これらの課題に対し本研究では、異なるアクセス制御ポリシーを持つ医療情報ドメイン間でポリシーを調整することにより適切なアクセス権限を付与する手法と、多機能 IC チップを応用したオンデマンド VPN (OD-VPN) [1]を利用した安全かつ大規模に伝送路を確保する手法とを組み合わせることにより、異なる医療情報ネットワークドメインでの安全なアクセス制御を可能とするシステムを提案する。

2. 研究課題と解決手法

一般的にネットワークを経由して安全に情報を伝送する際には、専用線や VPN を用いる。VPN は暗号通信を行うことで、ネットワークに安全な通信路を確保する技術であり、IP-VPN、IPsec-VPN など様々な技術が存在する。しかし、これらの VPN は設定が複雑であり、フレキシブルな設定変更に対応していないため、医療ドメインのような多数のエンティティ間を、必要に応じて動的に VPN 接続することが困難である。そこで本研究では、通信の安全性を確保するための対策として、ルータに内蔵した IC チップによる機器認証を用いることにより正当なルータにのみ VPN 接続を可能とする OD-VPN を適用する。OD-VPN では、インターネット上に設置された VPN 管理局が、IC チップ内の機器情報によって正当な機器であると認証されたルータに対して、動的且つ遠隔で VPN 設定を行うため、医療ドメイン間を安全に接続することが可能となる。

また、現在の医療ドメインにおいては、ドメインごとにアクセス制御ポリシーが異なるため、アクセス制御を行うための人や機器の特定を行うためには、相互のポリシーに対して整合性を取る必要がある。医療分野の特徴として、利用者が医療従事者として公的な資格を有していることがあげられるが、実際のシステム利用においては、資格ではなく“役割（ロール）”も重要である。またロールの中には、「院長」や「事務局長」などのような肩書きとしてのロールと、「主治医」、「ホームドクター」等の実務におけるロールの区分がある[2]。このようなロールに基づいてアクセス制御を行う手法を Role Based Access Control（RBAC）と呼ぶ。本研究では、ドメイン間の RBAC を用いたアクセス制御手法を提案し、制御ポリシーの異なるドメイン間でアクセス権の付与を実現するシステムについて検討する。

3. ロールマッピングアルゴリズム

制御ポリシーが異なってもアクセス権限を付与するためには、両ドメインにおいて独自に決められたロールの違いを吸収できるよう、お互いのロールをマッピングする必要がある。医療分野では肩書き（Structural Role）と実務での役割（Functional Role）が存在すると考えられるが、ネットワーク利用が想定される診察支援システムでは最終的なアクセス権限は Functional Role に対応付けされると仮定する[2]。また、RBAC のロール構造は木構造で表現され、Structural Role はドメインが異なっても構造、名称共に変化は少ない。以上の理由により、本稿では、医療従事者の Structural Role を手がかりに、同様のアクセス権限を持つ Functional Role へのマッピングを行う手法を提案する（図１）。また、標準的な XML ベースのプロトコルである、Security Assertion Markup Language（SAML）、eXtensible Access Control Markup Language（XACML）[3]を用いて実装を行う。

ただし、ロールのマッピングの際には、ロール構造と権限のほかに様々な条件を考慮する必要がある。たとえば、患者データを参照するにも、救急時と平常時では異なるアクセス制御が必要となる。

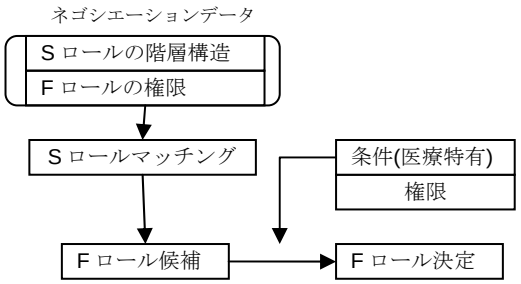

図１：ロールマッピングの概略

4. システム構成

提案手法の実現可能性を示すために実験システムの構築を行った。実験システムでは、ある医療従事者が、本人が所属する医療ドメインとは異なるドメインで管理された患者データに対してアクセスするシーンを想定する。今回の検証では OD-VPN 対応ルータを利用した安全な通信路上で、前章で述べたロールマッピング機能を実装した。アクセス制御の結果は認可チケットとして発行され、患者データを保持する DB に対してチケットを提示することでアクセスが許可または拒否される。チケットは XML であり、SAML Assertion の形式で記述されている。また、ロールマッピングに利用されるネゴシエーションデータ（図 1 参照）やロールとそれに対応する権限は、XACML の RBAC Profile PolicySet 形式で記述した。

さらに、医療分野で考えられる付加条件として、救急時と患者意志の確認を実装した。ここでいう患者意志の確認とは、情報主体者である患者の積極的な情報開示意志を確認するものであり、実験システムでは公的個人認証サービスを利用した患者の電子署名で意志確認を表すものとする。

実験システムは以下に示される 4 つのエンティティから構成される。

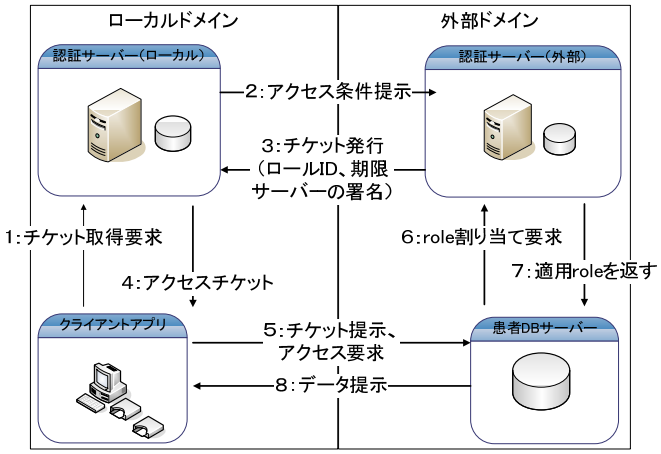

図２：システム構成図

- **患者データ閲覧アプリケーション**
  患者データを参照するアプリケーション。データ要求に加えて、IC カード読み取り機能やチケットリクエスト機能を有する。
- **内部認証サーバー**
  クライアントアプリケーションと同一のドメインで認証を行うサーバー。利用者の認証と他のドメインへのリクエストのための権限データを生成する。
- **外部認証サーバー**
  DB サーバーと同一ドメインにある認証サーバー。他のドメインからのリクエストに関して、ロールマッピングとアクセス許可チケット生成を行う。また、チケットの検証も担当している。
- **患者 DB サーバー**
  患者情報を保有する DB サーバーであり、クライアントアプリケーションとは異なるドメインに存在する。チケットを受け取り、認証サーバーの指示に従って、適切な患者データの送付を行う。

システムの流れは、以下の通りとなる。

1) アプリケーション内で外部ドメインの患者データへのアクセスが指定されると、内部認証サーバーにチケット取得要求を出す。
2) 内部サーバーはネゴシエーションデータを生成し、外部認証サーバーへチケット要求を行う。
3) 外部サーバーは提示されたデータからロールマッピングを行う。マッピングにおいて、外部認証サーバーから内部認証サーバーに対して、患者の意志確認要求が発生する。
4) 内部サーバーはクライアントアプリに患者 IC カードの挿入を要求する。患者の意志確認がある場合は、患者署名を検証し、正当なものであればマッピングの調整結果に反映する。その後、結果を DB に記録し、チケットを発行する。
5) アプリケーションはチケットを患者 DB へ提示し、患者 DB では外部認証サーバーにこれを問い合わせる。

5. 評価

実験システムに関して、アクセス制御とセキュリティの 2 点から評価を行った。

① アクセス制御評価

利用者の資格や条件によって、正しくアクセス制御が行われているかを評価した。

表１：アクセス制御シナリオ

資格	利用時の条件	期待されるアクセスレベル
看護師	なし	アクセス不能
看護師	救急	Minimum（救急用）
医師	なし	患者の同意した通常の範囲
医師	患者意志あり	患者の同意した最大の範囲

各パターンに関して検証した結果、資格やロール、さらに条件によって患者情報へのアクセスが、異なるドメインにおいても適切に行われていることを確認した。従来の RBAC ではこのようなドメインを越えたアクセスを行う場合は、ポリシーを共有するか、もしくはアクセス先のポリシーで静的に定められた権限を付与されることしかできなかった。しかし、提案手法によって、事前に登録がなくてもロールのマッピングの際に公開鍵基盤に基いた資格を確認し、付加条件を考慮することで、アクセス権限を動的に割り当てることができた。

② セキュリティ評価

本システムにおけるデータの通信路では、ドメイン間の通信は OD-VPN による暗号通信を想定しているため、高い安全性が確保されていると考えられる。また、悪意ある攻撃者や不正な利用者による脅威については、表２の項目にしたがって評価を行った。

表２：脅威に対する対策と効果

脅威	対策	結果
利用者成りすまし	本人認証	◎
チケットの不正発行	本人認証、 発行者電子署名	◎
チケットの再生攻撃	有効期限 識別番号	◎
制御ポリシーの外部流出	チケット記載情 報の工夫	◎
不正な患者意志確認	本人認証、 患者電子署名	◎
有資格者による不正利用	ログ	○

本システムにおける本人認証は、IC カードによる PIN 認証を用いており、一定の安全性を有するものであると言える。また、認可チケットを悪用した攻撃等に対応するために、発行者の電子署名を付与する、チケットにドメインのポリシーに関する情報を記載しない等の対策を行っている。正当な権限を有する利用者の悪意に対しては、アクセスログを保管することで対処している。アクセスログは機器の認証、利用者の認証の結果を含んでおり、不正利用の抑止効果が期待できる。

従来の手法は、事前の利用者登録が必要であったり、アクセスされる側のルールのみに従わざるを得ないなどの制限を受けていた。それに対して、提案手法は、従来手法の制限を緩和し、アクセスの自由度を拡大したが、セキュリティは保たれていることが、評価から確認できた。

6. まとめ

本研究では、医療情報システムのマルチドメイン利用に関するセキュリティ要件の検討を行い、RBAC における利用者の事前登録不要なアクセス手法を提案した。また、提案手法に基づいて実験システムを構築し、動作実験と評価を行った。

評価の結果から、提案手法の有効性を確認し、システム化の可能性を示すことが出来た。

参考文献

[1] 釜仲　他：“機器の認証に基づく安全な VPN 構築技術の提案、” 2004-CSEC-27, 情報処理学会 (2004)
[2] ISO22600 「Healthcare Informatics - Privilege management and access control - 」
[3] OASIS http://www.oasis-open.org/