M-016

異なる医療情報ネットワークドメイン間に属する機器の接続方法に関する研究

Healthcare network system to interconnect equipments in different domains

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]
Mamoru Sato[1] Masuyoshi Yachida[1] Hiroyuki Suzuki[1] Takashi Obi[2] Masahiro Yamaguchi[1]
Nagaaki Ohyama[3] Kouichi Kita[1]

1. はじめに

近年、情報技術の発達により様々な分野でシステム化が行われている。さらに、インターネットを代表とするネットワーク技術を導入することにより、データやシステムのネットワークを通じた利用が可能となり、われわれは多大な恩恵を得ている。このような情報技術の利用は特に産業分野でめざましいが、医療分野においても電子カルテや診療支援システムを代表とする数々のシステムが導入され始めた。今後は医療分野においても、ネットワークを利用した大規模なシステムに発展するものと予想されている。具体的には、カルテデータの共有や医療機器の遠隔操作、遠隔診断などが検討され、一部で利用が始まっている。地域など複数の医療施設が連携することで、利便性と医療水準の向上が期待される。

一方、個人情報保護法が施行されたことにより、個人情報保護に留意しつつネットワークを通じた情報交換を実現する必要が生じている。医療情報は医師等の公的な資格を持った医療従事者によって扱われることを前提としている。また、医療機器等は資格に応じて取り扱いが制限されているため、機器に応じた個別のアクセス管理が必要となる。

本研究では、ＩＣチップを用いた機器認証と利用者の属性認証、さらにオンデマンドＶＰＮ[1]における情報分散管理を組み合わせたフレームワークを提案し、柔軟に連携する医療情報ネットワークを実現することを目的としている。

2. システム要件

医療分野での導入においては、大きく分けて二つの課題がある。

① 異なるセキュリティポリシーを持つドメインに属する機器の安全な接続
② 資格や役割による情報への柔軟なアクセス制御方法、または特権管理

医療施設ではすでに個別の情報システムが導入され、自身のポリシーによって管理が行われている。すべてのシステムやポリシーを統一することはできないことから、異なるシステム方式やセキュリティポリシーを持つドメイン間を結びつける技術が必要となる。ドメイン間の通信路の安全性にも留意する必要がある。現在はこのようなセキュアな通信路を実現する方法にＶＰＮが利用され始めている。安価で高速なインターネット等の回線を暗号化通信によって安全にする技術である。しかし既存のＶＰＮ技術では、接続先ごとに静的に設定を行う必要があり、大多数のエンティティが存在する広域医療システムでは導入が難しい。また、機器やドメインの特定のための情報には、ＩＰアドレスやＭＡＣアドレスを用いるのが一般的である。しかし、管理範囲の異なるドメイン間において固定ではない、あるいは偽装されうるこれらの情報のみを機器の特定に用いることは、確実なアクセスを保証するものではない。

前述の通り、医療情報の取り扱いに公的な資格が必要であることが大きな課題として挙げられる。従来のアクセス制御では、事前に登録してあるＩＰアドレスやパスワードの組み合わせで接続者を識別する方法が一般的である。しかしこれでは、資格等を考慮したアクセス制御が行えないため、接続者に付随する属性情報の認証が不可欠となる。もう一つの課題に、システムにおいて大多数の医療機関がエントリーする場合、すべての利用者の権限情報をお互いに持ち合うことは困難であり、また自身の情報を他者に保持させるのはセキュリティの観点からも避けるべきである。ゆえに、事前登録のない場合でも、適切な特権を得て情報資源へアクセスできなければならない。

以上２つの観点はお互いに無関係ではなく、セキュリティポリシーには利用者の属性情報も加味されるべきであると考えられる。今回想定するのは完全に管理範囲の異なるドメイン間接続であることから、接続許可に関しては厳重な制御が行われなければならない。医療施設間の安全な機器あるいは端末との接続をネットワークレベルで保障するだけでなく、アプリケーションやサービスで要求される資格を確認することが、特に事前の利用者の設定なしに実施するためには必須となる。

3. 提案手法

以上を踏まえて、システム実現のために解決すべき要件は、

- 利用者の本人認証に加えて、資格の認証を行う
- 利用される機器がドメイン管理下にあることを明らかにする
- 異なるセキュリティポリシーを考慮したマッチングを行う

となる。本手法では、これらを満たすフレームワークを提案する。

[1]東京工業大学像情報工学施設
[2]東京工業大学総合理工学研究科

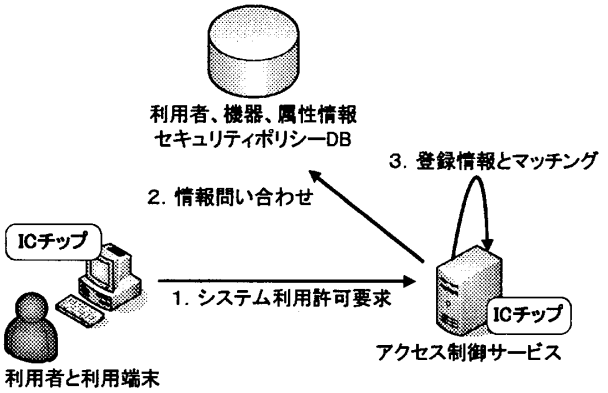

図１：ドメイン内部でのアクセス制御

図１にドメインの内部におけるアクセス制御の概要を示す。ドメイン内においても、医療情報にアクセスする際には本人認証と資格の認証、利用している機器の認証を行う。利用者情報はＩＣカード等に記録されているものとする。機器認証とは、耐タンパー性を持つＩＣチップを内蔵した機器を想定し、安全に保持された情報を認証に用いる技術である。通常は公開鍵証明書などが用いられる。認証が成功すると、セキュリティポリシーに従った特権が付与される。

ドメイン内部でのフレームワークはＳＡＭＬ（Security Assertion Markup Language）の認可モデルに従っている。この場合、要求の許可、不許可を決めるポリシー決定点（Policy Decision Point、以後 PDP）がアクセス制御サービスとなり、実際にアクセス制御を行うポリシー実行点（Policy Enforcement Point、以後 PEP）はアプリケーションとなる。異なるドメインへのアクセスでは、この役割は変更される。

外部接続要求があった場合には、アクセス制御サーバビスからオンデマンドＶＰＮ管理局に接続要求クエリーが送信される。ＶＰＮが構築されれば、ドメイン間の通信の安全性が確保できる。オンデマンドＶＰＮはＩＣチップを内蔵したセキュアルータと管理局の間で、ＶＰＮ構築情報を要求に応じて配送する技術である。広域医療ネットワークのように多くのエンティティが存在する際に、接続に応じて任意多地点でＶＰＮ接続を行える。オンデマンドＶＰＮを用いて、事前登録によってドメイン内の特定の機器へアクセスすることも可能だが、本提案ではＶＰＮ管理局は各ドメインのアクセス制御サービスへの接続までを保証し、その後の接続は各ドメインのアクセス制御サービスが責任を持つ分散管理モデルを提案する。これによって、ドメインの管理責任を明確化することができる。異なるドメイン間の接続において、責任範囲の明確化は非常に重要となる。

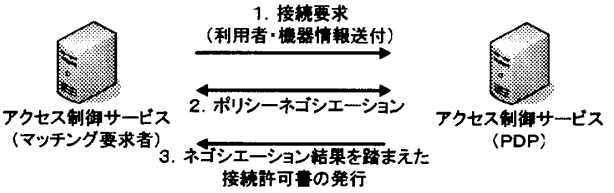

図２：ポリシーネゴシエーション

外部ドメインとのコネクションが確立した後は、ポリシーのネゴシエーションを行う。処理の手順は以下のようになる。

① アクセス制御サービスが相互認証を行う
② 外部ドメインへ属性情報、機器証明情報を送付する
③ アクセス制御サービスは証明情報をもとに、ポリシーを作成、提示する
④ ドメイン同士のポリシーネゴシエーションを行う
⑤ 外部アクセス制御サービスはネゴシエーションの結果を返す
⑥ ローカルドメインのアクセス制御サービスは、その結果を利用者へ返す
⑦ 外部資源へアクセスし、実際にアクセス制御を受ける
⑧ 両ドメインでログをとることによって、フォレンジックを確保する

ローカルドメインと外部ドメインでは、同じ属性の利用者に対して、同じ権限が与えられているわけではない。利用できる資源が異なったり、特別な権限が与えられたりする場合が考えられる。利用者にとっては、ローカルと同様に資源を利用したいが、外部ドメインから見れば、ポリシーに反する資源利用を許すことはできない。そこで、ポリシーのネゴシエーションを行う必要が生じる。ポリシーのネゴシエーションを行うことにより、両者の同意の上に、適切な権限をもって資源を利用することができる。

ポリシーネゴシエーションの具体的な方法については、現在検討中であるが、あらかじめ項目を決めた同意書（Policy Agreement Document）を照らし合わせる方法などを検討している。この場合、医療分野における制度や実務レベルで適切な項目を設定する必要がある。

4. まとめ

ＩＣチップを用いた機器認証と資格に関する属性認証を組み合わせることにより、異なるドメイン間の機器、資源への接続を安全に可能とするシステムフレームワークを提案した。また、ドメインの管理責任をシステム的に分割することを可能とした。現在課題であるポリシーネゴシエーションについて、技術的な検討を進めており、プロトタイプによる検証を行う予定である。

5. 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)