社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2008－ＤＰＳ－134　(40)
2008－CSEC－ 40　(40)
2008／3／7

レイヤ間認証連携、および、マルチレイヤ認証をベースとしたアクセスポリシー管理方式について

園田俊浩、猪俣彰浩、尾崎楽人
富士通株式会社　ネットワークサービス事業本部
〒144-8588 東京都大田区新蒲田 1-17-25
e-mail: toshihiro@jp.fujitsu.com

医療機関や金融機関など機密性の高い情報にネットワークを介してアクセス可能とするためには、信頼できる認証方式、および、認証をベースとした認可の仕組みが必要である。認証に関しては、利用者認証に加え、アプリケーション、機器、ネットワークなど利用者環境の認証が統合された認証が必要であり、この統合された認証をベースとしたアクセスポリシー管理の仕組みが必要である。このような仕組みを実現するために、複数の認証を統合的に扱う「複数認証連携」方式、および、その認証に応じてネットワークを最適に制御する「ポリシーやコンテンツに応じたネットワーク制御」方式を設計し、一部実証を行ったのでその結果を報告する。

Integrated Authentication for Multi-Layers and Management of Access Policy Based on the Authentication

Toshihiro Sonoda, Akihiro Inomata, Gakuto Ozaki
Fujitsu Ltd. Network Service Business Unit.
Shinkamata 1-17-25, Oota-ku, Tokyo, 144-8588, Japan
e-mail: toshihiro@jp.fujitsu.com

Trusted method of authentication and delegation of authority is needed so that we can treat sensitive information such as medical or financial one. Further to authentication of a user, we should have the integrated authentication among multi-layers, which include applications, devices, network environment and so on, and establish the framework so that the authority can be transferred according to the result of the integrated authentication. This paper describes the technology of the integrated authentication among multi-layers and management of access policy based on the authentication.

1. はじめに

インターネットの普及、および、価格低下より、ネットワークを利用した情報流通、商取引などの機会が増加している。また、医療、金融などいわゆるミッション・クリティカルな分野にもその利用が拡大し、遠隔診断、リアルタイム受発注などでの応用も計画されている。一方、インターネット上での詐欺や情報不正入手など、いわゆるネット犯罪も増加傾向にあり、健全なネットワーク社会の発展への影響が懸念されている。

ネットワークの危険性が高まる中、より高いセキュリティが通信システムにも求められている。現在の通信システムは、ID/パスワードや電子証明書など、単一の認証システムにより運用されているケースが多いが、脅威に対応するためにはこれらを複合的に利用し、セキュリティ強度を高めていく必要がでてきている。

複数の認証技術・機関にまたがる認証技術を統合的に扱うためには、アプリケーションにおける利用者認証、利用している機器、ネットワークの利用環境など、各レイヤでの認証を統合的に管理する仕組みが必要となる。

このようなシステムを実現するためには、PKIや ID/パスワードなどの認証方式の相違、本人、機器など認証対象による認証技術の相違、認証対象毎に認証管理機関が異なっていた場合の運用の相違を吸収するシステムの実現が課題となる。

本研究では、このような課題を解決するために必要となる「複数認証連携」技術と「ポリシーやコンテンツに応じたネットワーク制御」技術について研究開発を行った。

2. 研究開発分野の現状

2.1. TCG (Trusted Computing Group)

マイクロソフト、インテルなどITベンダが参加し、コンピュータのセキュリティに関する枠組

みを検討している団体として、TCG (Trusted Computing Group) [1]という技術検討コンソシアムがある。ここでは、パソコンや周辺機器で情報を扱う際、改ざんや不正利用などの防止のために、機器IDや機器の構成情報(ディスク、BIOS、接続機器など)を認証することが検討されている。そのひとつの技術として、TPM (Trusted Platform Modules)[2]といわれるセキュリティチップを利用したハードウェア構成の保護技術があり、多くのPCにセキュリティ対策として内蔵されている。

現在、これらのセキュリティをチェックするポリシー情報は、ローカル機器内の保護された領域に格納され、ローカル機器内のみで認証されている。TCGではこの枠組みをネットワーク上に設置された認証システムとネットワークを通して連携する仕組みが検討され始めている。

これらの仕様は策定中であり、本研究で利用、連携していくことを顧慮し、広く普及することを目指す。

2.2. ポリシー管理

ポリシー管理はポリシーによってコンピュータ・システムやネットワークを管理する技術であり、ポリシーとは条件・動作型の規則の並びである。ポリシー管理は、1990年代から活発に研究が開始され、90年後半に、DMTF (Desktop Management Task Force)と IETF (Internet Engineering Task Force)において標準化の対象になった[3]。

IETFでは、ポリシーに基づいて決定を行う対象を PDP (Policy Decision Point)、決定を適用するポイントを PEP (Policy Enforcement Point)と呼び、決定を要求する方式として、アウトソース方式とプロビジョン方式を定義している。IETFでは、ポリシーに関する要求・配布のためのサーバ・機器間等で使用する COPS[4]プロトコルを標準化し、アウトソース方式の用法である COPS-RSVP[5]とプロビジョン方式のための用法である COPS-PR[6]が標準化されている。

本研究では、これまでの研究をベースにマルチレイヤ認証をベースとしたアクセス管理方式について検討を行う。

2.3. 次世代ネットワーク(NGN, Next Generation Network)

IT企業を中心として次世代ネットワーク(NGN, Next Generation Network)の検討が行われている。NGNでは、ネットワーク管理システムと連携して、ネットワーク制御を行っていくアーキテクチャが検討されている。このアーキテクチャでは、管理システムが上位のアプリケーションと連携することによって、より最適なネットワーク環境を提供していくことも考えられている。

本研究で検討している複合認証やネットワーク制御機能を、このアーキテクチャと連携することで、より広範囲で高度なアプリケーションとネットワークを融合した総合的なセキュリティシステムが実現できる。

3. 複合認証の実現方式について

レイヤ間認証を連携し、マルチレイヤ認証を用いたアクセスポリシー管理を実現するための基本モデルを図 1に示す。

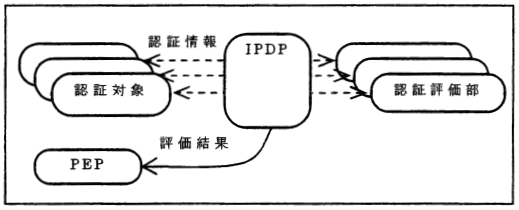

図 1 基本モデル

図 1に示すように、複数の認証対象が存在する場合に課題となるのは、認証方式、認証技術、認証機関による相違をどのように統合し、動作を決定し、ポリシー実行ポイント(以後、PEP)に転送するかである。今回は、認証方式を統一するのではなく、個々の認証対象の情報を収集し、それらを認証評価部で評価し、さらに各認証結果を統合し動作を決定する統合ポリシー決定ポイント(以後、IPDP)を配置する。IPDPで、全体の認証状態を管理し、その結果に基づいてポリシーを決定する。全体の流れは以下のようになる。

- ✓ 複数の認証対象の情報(ユーザ、電子証明書、ID/パスワード、IPアドレスなど)を収集し、認証評価部に転送
- ✓ 認証評価部では、認証情報に基づき評価
- ✓ IPDPでは、各認証評価を統合してPEPの最終動作を決定し、PEPに通知
- ✓ PEPでは、決定された評価に従って動作

認証対象毎に認証情報を収集でき、認証情報毎に検証できる仕組みを構築することで、様々な認証方式、認証機関に対応可能となることを目指す。また、新たな認証対象が発生した際も容易に追加が可能であることを目指す。

4. 課題分析

4.1. レイヤ間認証連携について

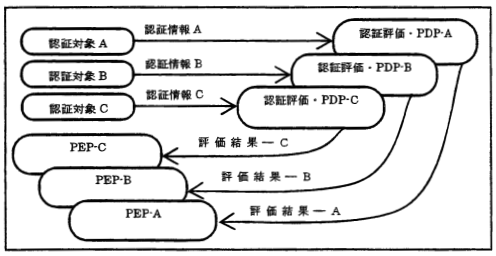

図 2 現状の認証モデル

現状、利用者、機器、ネットワークなど認証対象が複数のレイヤにおいて存在する場合、図 2

のようにそれぞれ個別の PDP と PEP が、評価とアクセス制御を行っている。この方式は、それぞれのシステムを別々に導入するだけで簡単に構築できるが、利用者や管理者にはそれぞれが独立して見えるために、一貫したポリシー適用が難しい。

そこで、複数の認証情報を統合して扱う連携機能をモジュール化し、それぞれの認証はこのモジュールを介して行い、各ポリシーの結果から統合的に判断する統合ポリシー決定ポイント(IPDP)を配置する。図 3に構成を示す。

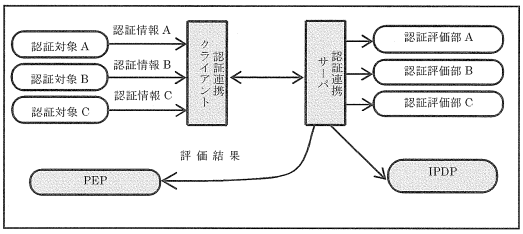

図 3 レイヤ間認証を統合したモデル

認証情報は認証対象毎に収集され、認証証携クライアントがそれらをひとまとめにして認証連携サーバに送信する。認証連携サーバは、認証情報を対応する個別の認証評価部に転送する。認証連携サーバは、認証評価部の評価結果を収集し、IPDP が PEP の最終的な動作を決定する。

このアーキテクチャでは、以下の 3 点が重要なポイントになる。

4.1.1. 認証情報収集部～認証連携クライアント間のインタフェースの共通化

認証対象の認証情報を収集する部分は、様々な認証対象に対応するために独自に開発できる必要がある。そのため、認証連携クライアントは認証情報を収集する統一されたインタフェースを提供する必要がある。

4.1.2. 認証連携サーバ～認証情報評価部間のインタフェース共通化

認証評価部は、取り扱う認証情報のそれぞれについて独自に開発できる必要がある。そのため、認証連携サーバは認証情報を転送する統一されたインタフェースを提供する必要がある。

4.1.3. 通信セキュリティ確保

認証連携クライアントは、認証連携サーバとの間で認証情報を、ネットワークを介して交換することになるが、そこでは盗聴や改ざんといった脅威への対策が必要となる。

PEP は、認証連携サーバから転送されてくる動作ポリシーの指示に従って処理を実施するが、ここでも同様に盗聴や改ざんといった脅威への対策が必要となる。

4.2. マルチレイヤ認証を用いたアクセスポリシー管理について

4.1 節で考察した構成において、複数の認証情報の評価結果からアクセス制御動作を決定するのは、認証連携サーバと IPDP の部分である。認証連携サーバは、複数の評価結果を各認証評価部から受け取った後に、IPDP が管理する統合ポリシーに照らし合わせることで、最終的な PEP の動作を決定する。

動作ポリシー管理に関しては、以下の点が重要なポイントになる。

4.2.1. 複数の認証情報に対する認証結果を組み合わせて動作を決定できる柔軟性

単一の認証情報から動作を決定するシステムにおけるポリシー記述方式は、認証の結果が比較的単純であるため、「条件-動作型」の規則の並びで十分であった。しかし、認証情報が複数になると条件の組み合わせが複雑になるために、柔軟なポリシー記述方式が必要である。

5. 課題に対するアプローチ

本節では、4 節の各課題に対するアプローチを説明する。

5.1. レイヤ間認証連携について

4.1 節の課題に対して以下のような対策を行った。

5.1.1. 認証情報収集モジュール部～認証連携クライアント間のインタフェースの共通化

認証情報収集モジュール部～認証連携クライアント間のインタフェースの共通化では、認証情報収集モジュール部が能動的に認証連携クライアントに認証情報を渡す形式もあるが、即時性の面から認証連携クライアントが各認証情報収集モジュール部の機能を呼び出して認証情報を集める形式とする。このとき、どのような認証情報収集モジュール部があるかを認証連携クライアント側が認識している必要がある。

通常時の認証において、認証情報収集モジュール部と認証連携クライアント間でやりとりが発生する箇所の流れは以下のようになる。

- ✓ 認証連携クライアントは、情報収集モジュールを指定した設定ファイルによって、どのような認証情報収集部があるかを発見（発見）
- ✓ 認証連携クライアントは、認証情報収集モジュールを起動（起動）
- ✓ 認証連携クライアントは、認証情報収集モジュールから認証情報を受信（認証情報受信）
- ✓ 認証連携クライアントは、認証情報評価モジュールの応答を認証連携サーバ経由で、対応する認証情報評価モジュールに通知(応答通知)

✓ 認証連携クライアントは、認証連携サーバから認証・評価手続きの終了を知らされると認証情報収集モジュールを終了（終了）

認証連携クライアントは、上記に示すように、認証情報収集モジュールに対して、発見、起動、認証情報受信、応答通知、終了の共通インタフェースを提供する。

5.1.2. 認証連携サーバ～認証情報評価部間のインタフェースの共通化

認証連携サーバとPDPのやり取りは以下の流れとなる。

✓ 認証連携サーバは、情報評価モジュールを指定した設定ファイルによって、どのようなPDPがあるかを発見（発見）
✓ 認証連携サーバは、PDPを起動（起動）
✓ 認証連携サーバは、認証連携クライアント経由で受信した認証情報を対応するPDPに通知（認証情報通知）
✓ 認証連携サーバは、PDPの応答を認証連携クライアント経由で、対応する認証情報収集モジュールに送信（応答送信）
✓ 認証連携サーバは、認証・評価手続きが終了次第、PDPを終了（終了）

認証連携サーバは、上記に示すように、PDPに対して、発見、起動、認証情報通知、応答送信、終了の共通インタフェースを提供する。

5.1.3. 通信セキュリティ確保

認証連携クライアント～認証連携サーバ間、および、認証連携サーバ～PEP間の通信では、以下のセキュリティを考慮する必要がある。

✓ 通信内容を第三者が計測できた場合でも内容が推測困難であること
✓ 通信内容を第三者が改ざんできたとしても、受信した側がそれを検出可能であること
✓ 第三者が成りすましして通信しようとしても、それを検出可能であること

以上を実現するために、認証・暗号化の標準として広く利用されているSSL/TLSを利用する。

5.2. マルチレイヤ認証を用いたアクセスポリシー管理について

4.2節の課題に対して以下のような対策を行った。

5.2.1. 複数の認証情報に対する認証結果を組み合わせて動作を決定できる柔軟性

アクセス制御ポリシー記述言語として、XACML (eXtensible Access Control Markup Language)[8]が規定されており、基本的なデータフローはその定義を参考にしている。IPDPが複数の認証に対応し、認証結果を組み合わせて利用できるように認証対象をカテゴリ分けできるようにする。

例えば、利用者認証に対して、「医者」「看護師」「患者」というカテゴリを指定し、認証評価部で結果を返せるようにする。認証連携サーバは、ポリシーを参照し、カテゴリの組み合わせによってPEPの動作を決定する。

6. 評価結果

6.1. レイヤ間認証連携に関する評価結果

5節のアプローチの有効性を確認するために、実験システムを試作し、動作検証を行った。システムの構成は図 4の通りである。

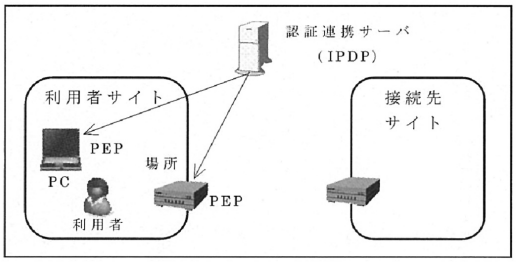

図 4 システム構成

本実験システムでは、認証対象として、利用者、機器(PC)、場所を想定した。認証連携サーバには、各認証対象に対する認証評価部をセットアップし、IPDPで柔軟なポリシー管理が可能であることを検証した。

利用者は、ID/パスワードとICカードの証明書を利用した認証を行う。機器(PC)は、PCから抽出した機器固有IDによる認証を行う。場所は、ルータのIPアドレスによる認証を行う。これらの認証情報を認証連携サーバに通知し、認証結果の組み合わせによって、PC側の利用アプリケーションの制限、および、ネットワークアクセス制御のコントロールを確認した。

以下の点を確認した。

✓ 利用者AをICカードで認証、かつ、利用している機器がPC-Aであることを認証、かつ、場所がWhere-Aであることを認証できた場合、利用者は、接続サイトAに接続でき接続サイトAのWebサーバにアクセスできうること（ポリシーが一致）
✓ 上記の条件で、ICカードが登録済みでない場合は、接続サイトAへのアクセスが拒否されること（利用者ポリシーが一致しない）
✓ 端末がPC-B(登録許可されていない端末)の場合は、接続サイトAへのアクセスが拒否されること（端末ポリシーが一致しない）
✓ 場所がWhere-B（許可されていない場所）の場合は、接続サイトAへのアクセスが拒

否されること（場所ポリシーが一致しない）

6.2. マルチレイヤ認証を用いたアクセスポリシー管理に関する評価結果

5.2 節のアプローチの有効性を確認するために、実験システムを試作し、動作検証を行った。構成は、6.1 節で示したシステムと同じ環境である。

- ✓ IC カードがなければ ID/パスワードでも接続でき領にポリシーを変更し、機能すること
- ✓ どの端末でも接続できるようにポリシーを変更し、機能すること
- ✓ ルータやグローバルアドレスに関係なく接続できるようにポリシーを変更し、機能すること

7. 今後の課題

現状、各レイヤでの認証とそれに伴う認可は、レイヤ毎に実装・開発されるために、レイヤ間の認証結果を統合して評価し、その結果に基づいて統一されたポリシーを適用することは困難である。今回はこのような課題を解決するために、複数レイヤでの認証を統合して扱えるアーキテクチャを設計し、試作システムの開発と検証を行った。

現在、認証対象の認証情報を収集するモジュールのインテグリティーチェックが行われていないために、モジュールの正当性が保証されていない。この点に関しては、機器側に搭載される TPM と連携し、モジュールの正当性を保証していく予定である。また、ポリシーの表記方法は認証との関係を考慮し、認証対象をカテゴライズする仕組みを取り入れた。今後は、PDP は PEP に認可を与えるだけでなく、認可された実行に対する責務を課すための検討も必要である。

今後は、医療機関など認証とその認可が重要となる分野で本システムを導入し、様々なフィールド・ニーズに対応できるかを検証していく予定である。

謝辞

本研究は、独立行政法人情報通信研究機構の委託研究「ネットワーク認証型コンテンツアクセス制御技術の研究開発」として行われたものである。ここに記して謝意を表す。

参考文献

[1] Trusted Computing Group, "TCG Specification Architecture Overview", https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf
[2] Trusted Computing Group, "Trusted Platform Modules Strengthen User and Platform Authenticity"
[3] 金田泰, IETF 標準化を中心としたポリシー管理技術の動向, 電子情報通信学会 2002
[4] D.Durham, Ed., J.Boyle, R.Cohen, S.Herzong, R.Rajan, A.Sastry: The COPS (Common Open Policy Service) Protocol, RFC 2748
[5] K.Chan, J.Seligson, D.Durham, S.Gai, K.McCloghrie, S.Herzog, F.Reichmeyer, R.Yavatkar, A.Smith: COPS usage for Provisioning (COPS-RP), RFC 3084
[6] S.Herzog, Ed., J.Boyle, R.Cohen, D.Durham, R.Rajan, A.Sastry: COPS usage for resource Reservation Protocol (COPS-RSVP), RFC 2749
[7] Matt Bishop: Computer Security, Addison-Wesley, Pearson Education, Inc.
[8] OASIS, "eXtensible Access Control Markup Language (XACML) Version 2.0", OASIS Standard, 1 Feb 2005