L-005

公開鍵基盤に基づくロボットの認証及びアクセス制御手法の提案

A Proposal for PKI-based Robot Authentication and Access Control Method

三宅 一正† 平野 学†
Kazumasa Miyake Manabu Hirano

1．まえがき

様々な種類のロボットが医療現場，災害救助，老人介護あるいは家庭でのエンターテイメントに至るまで幅広く開発されてきている．ロボットが広く普及するに従い，ロボットに関するセキュリティ機能の必要性が増してきている．例えば，操作を行おうとしている人間が本当に信頼できる利用者であるかどうかを確認する認証 （Authentication）や利用者の権限に応じて命令を実行するかどうかを判断するロボットのアクセス制御（Access Control）といったセキュリティ機能が，ロボットのネットワーク化に伴い要求されつつある．本研究ではこのようなネットワーク型ロボットを対象とした認証とアクセス制御をシンプルに実現する手法を提案し，実用的なプロトタイプ実装を示すものとする．本研究ではインターネットでの電子商取引や住民基本台帳ＩＣカード等で実績のある公開鍵基盤（PKI, Public Key Infrastructure）の技術を用いたスケーラブルな認証とアクセス制御の手法を提案する．特に，本研究では従来の公開鍵証明書を用いた認証をロボット制御に適用する例を示す他，公開鍵証明書に含まれる属性情報を利用した新たなアクセス制御手法を提案するものとする．本研究ではこれらのセキュリティ機能を，ロボット本来が持つ機能と独立して設計することで，既存のロボットシステムに容易に組み込み可能なセキュリティモジュールを提案するものとする．

2．関連研究

ロボットを対象としたセキュリティ研究が様々な分野で行われてきている．例えば，米国の火星探査プロジェクトでは着陸船とオペレーションセンター間の通信を NASA 公開鍵基盤を利用した SSL 暗号化通信路で実現している[1]．この研究は公開鍵基盤とインターネットで一般的に使われている認証プロトコルを宇宙での安全な通信に適用する新たな試みであった．

3. ロボットの認証及びアクセス制御のモデル化

我々が提案するロボットを対象とした認証及びアクセス制御のモデルを図１に示す．AUTH は認証処理を示しており，ロボットが利用者の本人確認をする処理である．認証処理には単純なパスワード，ＩＣカードのようなトークンシステム及び生体認証（Biometrics）との組み合わせが利用できる．AC はアクセス制御処理を示しており，認証で本人確認が完了した後に，利用者が持つ権限に応じて命令のアクセス制御が行われる部分である．AC（Access Control）によって権限に応じたきめ細かいアクセス制御が実現できる．CP（Control Program）はロボット

豊田工業高等専門学校 情報科学専攻

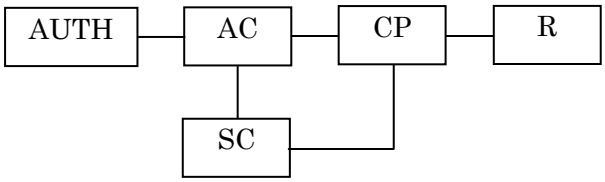

図１　認証及びアクセス制御モデル

に搭載された制御プログラムを示している．R（Robot）はロボットを示しており，認証とアクセス制御の過程を経て伝達された命令は最終的にロボットが実行することになる．AC 及び CP は SC（Secure Communication）つまり暗号化通信路によって保護される．SC は第三者による盗聴や通信路上での命令の改竄を防ぐ役割を担っている．特に AC はユーザが意識する必要が無いのが望ましい．よって，ユーザは CP へ直接命令を送るが，実際はユーザと CP との間に AC があり，AC によって権限によるアクセス制御が実現されるものとする．

4. ロボットの認証及びアクセス制御手法の提案

4.1 既存システムへの組み込みが容易なセキュリティモジュールの実現

本論文で示す提案の目的は，インターネット経由でロボットを遠隔制御する際の利用者とロボット間の相互認証と利用者の権限に応じたアクセス制御の枠組みをロボット本来が持つ機能と独立して設計することで，既存のロボットシステムに容易に組み込み可能なセキュリティモジュールを提案することである．

図１のモデルに示した AUTH と SC は実績のある認証及び暗号化通信を実現するための TLS（Transport Layer Security）プロトコルに利用者の電子的な身元確認データ（公開鍵証明書と秘密鍵）を格納した IC カードを組み合わせて実現する．公開鍵証明書は第三者機関によって発行される電子的な本人確認のための身分証明書である．公開鍵証明書はインターネットにおける電子商取引や官公庁における公的書類の電子申請システム等で実績がある技術である．公開鍵証明書を利用することで，単純な ID とパスワードを用いたシステムよりも安全に認証システムを構築できるようになる．本提案では IC カードに認証情報の基礎となる秘密鍵を格納することで認証情報の漏洩を防ぐものとする．また，逆に利用者がロボットを認証するためにロボット側にもロボットの ID を格納した公開鍵証明書とそれに対応する秘密鍵を持たせるものとする．これにより利用者とロボットの双方向認証が実現する．

本論文で示すプロトタイプ実装ではロボットの操作はウェブブラウザ経由で行うものとし，アクセス制御の処理部

には Java のフィルタと呼ばれる機構を用いる．フィルタを用いることでユーザはアクセス制御処理を意識せずにロボットの制御を行うことができるようになる．以上の機構により，既存のロボット制御システムへの変更を最小限に抑えながら，認証とアクセス制御の処理を追加可能となる．

4.2 グループ情報に基づくアクセス制御

本研究では従来の公開鍵証明書を用いた認証の他に，新たに公開鍵証明書に記載の所属情報に基づく，ロボットのアクセス制御手法を提案する．公開鍵証明書の識別名フィールドの CN (Common Name) はユーザ名を示しているが，OU (Organization Unit) 及び O (Organization) からは所属情報が得られる．本研究では OU と O をアクセス制御に利用できるプロトタイプ実装を示す．これにより，グループ単位，すなわち個人より粒度の高いレベルでの権限によるロボットのアクセス制御が実現できるようになる．提案システムでは，例えばメンテナンス業者の持つ権限ではロボットを管理するための特別な命令を実行できるが，一般ユーザの権限では通常の操作しか実行できない，といった実用的なアクセス制御の機能を実現できるようになる．

5. 実装

本研究ではネットワークロボットとして Evolution Robotics 社の ER-1 を対象としてプロトタイプシステムを構築した。ER-1 は図２に示すようにノート型コンピュータに USB で接続して制御されるモータ，カメラ，ロボットアーム，センサから構成されている．ロボット制御用コンピュータは無線 LAN でインターネットに接続するものとし，ユーザの持つ制御用端末から実際の操作命令がロボットに送信されるものとする．今回のプロトタイプ実装のシステム構成を図３に示す．制御用端末とロボット制御用コンピュータの間は TLS プロトコルによる双方向認証と暗号化通信が行われる．最初に，ロボットがユーザを認証する処理は IC カードに格納されたユーザの公開鍵証明書と秘密鍵によって実現する．次に，ユーザがロボットを認証する処理はロボット制御用コンピュータに格納されたロボットの公開鍵証明書と秘密鍵によって実現する．以上で TLS を用いたユーザとロボットの双方向認証が完了する．

次に Java 言語で記述されたアクセス制御用のフィルタプログラムがアクセス制御を実現する。アクセス制御フィルタプログラムは，TLS 通信の認証で得た公開鍵証明書から識別名の情報を取得し，所属情報（O と OU）を取り出す．得られた所属情報とアクセス制御リストを比較して，権限に応じたアクセスが認められるかを判定する．Java フィルタプログラムの役割は，ユーザの権限に基づいて透過的にロボット制御プログラムへのアクセスを拒否または許可する機構を提供することである．Java 言語のフィルタプログラムを採用することで，開発者はロボット制御プログラムを開発する際にはアクセス制御処理を組み込む必要は無く，制御用プログラムのみを記述すればよいことになる．他方，ユーザから見るとフィルタプログラムの存在は意識されず透過的に扱われる為，ユーザに余計な手間をかけることなくシステムにセキュリティ機能を付加できるようになる．

図２　ネットワークロボット ER-1

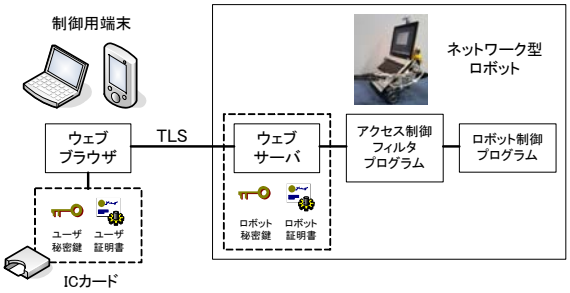

図３　プロトタイプ実装のシステム構成

図４　操作画面の GUI

6. まとめ

開発したプロトタイプシステムの実行画面を図４に示す。本研究ではロボットの前進後退、及び左右への移動、及びカメラ画像のリアルタイム取得を実現した。本論文で提案したアクセス制御方式によって、IC カードに格納された公開鍵証明書の権限によって、あるユーザはカメラ画像が閲覧できるが、ロボットの操縦は出来ない。また、他のユーザは両方を実行できる、といった権限に基づくアクセス制御が実現できることを確認できた。

参考文献

[1] P. Backes and J. Norris and J. Slostad and R. Bonitz and K. Tso and G.Tharp, Mars Polar Lander Mission Distributed Operations, IEEE Aerospace, 2005.