3B-1

利用権管理技術を用いたリモートアクセス制御方式の考察

釜坂　等[†]　　北上　眞二[†]
三菱電機(株) [†]

１．はじめに

近年、インターネットに接続可能なネット対応家電が出てきており、宅外から簡単にアクセスできる環境となってきた。このアクセスにおける成りすまし等の脅威に対して、SSL 技術等による相互認証を行って対処しているが、正しい通信相手からの不正なアクセスは防止できない。

そこで、利用権管理技術を用いて、認証した相手からの不正なリモートアクセスを防ぐ方式について考察したので報告する。

２．アクセス制御の課題

インターネットで安全に通信する SSL 技術では、クライアントおよびサーバの公開鍵証明書を用いた暗号通信/署名技術/相互認証により、盗聴/改ざん/成りすましの脅威に対処している。

次の脅威として、認証されたサイトからの不正なアクセスある。これに対処するための要件は以下の通りである。

1. ユーザがサイトに対して許可したコマンドしか実行させないこと(例えば、リモート診断では運転ログへのアクセスコマンドの実行は不許可とし、エラーログしかアクセスさせないなどにより、不正なアクセスを制限する)
2. ユーザがサイトに対して許可した条件でしかコマンドを実行させないこと(例えば、エラーログへのアクセスは、月に一度だけなどとし、誤操作等による予定外のアクセスを防ぐ)
3. 上記が確実に実行されるためのアクセス制御基盤が必要。

３．利用権管理技術によるセキュリティ

デジタルコンテンツの著作権を守る技術として利用権管理技術(DRM: Digital Rights Management)がある。これは、コンテンツの正規の購入者(利用者)による不正コピーなどを想定して、不正を制御するためのシステムである[1]。

具体的には、利用権管理技術は、コンテンツの暗号化・暗号を解くための鍵を含むライセンス・コンテンツの専用ビューアの 3 つの技術から構成される。利用者からみた動作は以下のとおりである。

(1) 暗号化されたコンテンツを入手
(2) 機器認証等を行い、ライセンスを受け取る。
(3) コンテンツの専用ビューアは、ライセンスの復号鍵でコンテンツを復号して表示する。

上記の処理により、ライセンスを持たない利用者の不正利用等を防ぐことができる。

４．利用権管理技術の機器アクセスへの適用

４．１　アクセス制御の課題解決案

利用権管理技術の特長である、正規の利用者による不正利用を想定したセキュリティの仕組みを、機器へのアクセス制御へ適用する。

まず、前述の要件を以下のように解決する。

1. 指定したコマンドを個別の鍵で暗号化して特定化し、コマンドの特定(=コマンドの復号ができる）ができた場合のみ実行可能とする。
2. 指定した実行条件(以下利用条件とする)と上記の暗号化したコマンドとを紐付けて指定可能とする
3. 暗号化コマンドを利用条件で実行する仕組みを提供する。

つまり、それぞれ機器を制御するコマンドの暗号化・暗号を解くための鍵を含む機器利用のライセンス・コマンド制御モジュールと考えると利用権管理技術が適用できると考えられる。

４．２　利用権管理技術の適用時の問題

デジタルコンテンツの利用権管理技術を機器アクセスへ適用した場合のセキュリティの観点から比較したものが図 1である。

図 1に示すように、デジタルコンテンツの視聴制御では、コンテンツを守りたい主体はサーバ側に位置し、不正実施を想定する主体は利用者側に位置する。これに対し、機器へのアクセス制御では、機器を守りたい主体は利用者側に位置し、不正実施を想定する主体はサーバ側に位置している。

"Machine Access Policy Management System"
[†]HITOSHI KAMASAKA
SHINJI KITAGAMI
Mitsubishi Electric Corp. Information Technology R&D Center.

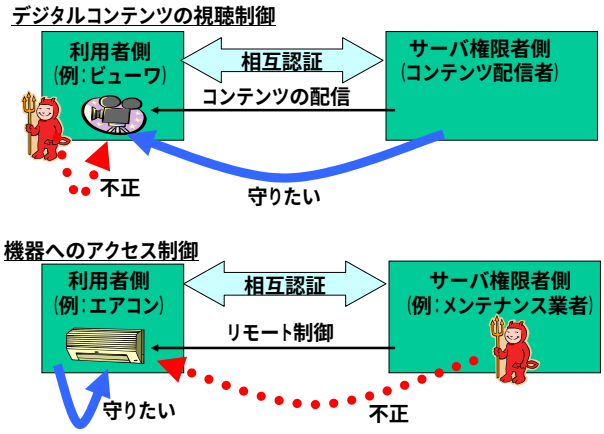

図 1　セキュリティの観点での比較図

これをまとめたのが表 1である。つまり、保護対象と関係者との関係が異なるため、デジタルコンテンツの視聴制御の利用権管理技術を、機器へのアクセス制御にそのままでは適用することは出来ない。

表 1　セキュリティの観点での比較のまとめ

	デジタルコンテンツ視聴制御	機器へのアクセス制御
保護対象	コンテンツの著作権(および売上)	機器そのもの、機器によって得られる快適生活
保護主体	サーバ側権限者(著作権者(および販売者))	利用者(機器所有者)
脅威	不正なコピー(不正流通)など	機器の破壊、機器の不正設定による危険やセキュリティ上の危険
想定不正実施者	利用者(デジタルコンテンツ購入者)	サーバ側権限者(リモートメンテナンス運用者など)

4．3　利用者側主動の利用権管理技術を適用

利用権管理技術はそのまま適用できないが、保護主体である利用者主動の観点で、利用権管理技術の適用方法を見直すことにより、アクセス制御への適用は可能である。それぞれの適用技術の実装場所を整理し直したのが表 2であり、図示したのが図 2である。

表 2　利用権管理技術の適用の整理

適用技術	適用場所
機器を制御するコマンドの暗号化	保護対象の機器のある利用者側で暗号を実施
暗号化コマンドのライセンスに従った複号と実行を行う制御モジュール	コマンドが動作する利用者側で制御モジュールを動作
機器利用のライセンス	利用の制限をさせたい主体の利用者側で作成

認証された利用者の不正なアクセスを防止するための利用者からみた動作は以下の通りである（図 2参照)。

(1) コマンドを暗号化する
(2) サーバ側権限者に、適切な利用条件(実行日時や回数、不在時のみ実行可能などの条件等)と上記暗号化コマンドの複号鍵とを付加したライセンスを配信する。
(3) サーバ側からの当該ライセンス送付によりリモート制御を受ける。制御モジュールは、ライセンスの復号鍵でコマンドを復号して実行する。なおライセンスに紐づいた機器情報や利用条件が照合した時のみ複号する。

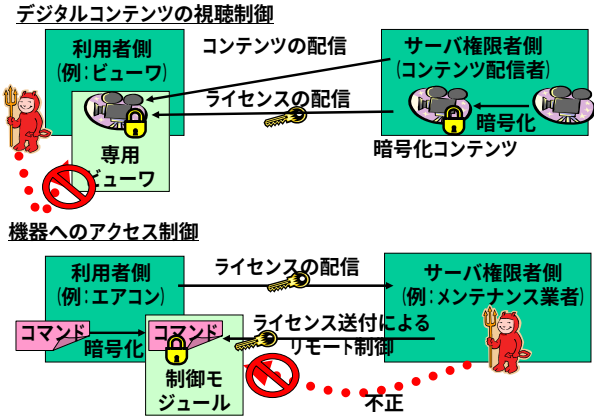

図 2　利用権管理技術の適用

以上の動作により、ユーザがサイトに対して許可したコマンドおよび許可した条件でしか実行させないアクセス制御基盤を提供する。これによりサーバ側の不正なアクセスを防止することができる。

5．　まとめと今後の課題

利用権管理技術を機器へのアクセス制御に適用し、認証された通信相手からの不正なアクセスを防ぎ、かつ利用条件の指定によりきめ細かな制御を可能となることを示した。

今後は、本検討システムを構築し、運用の課題点などの明確にする。

参考文献

[1]釜坂他:"ライセンス管理機能を独立させたデジタルコンテンツ利用権管理システム",情報処理学科第 65 回全国大会,2003/3