RL-003

機器の遠隔制御コントロール－機器利用権－

Remote Access Control for Appliance – Device Control Rights–

釜坂　等†　安田　晃久†　北上　眞二†　嵩井　秀夫†　石本　貴之‡
Hitoshi Kamasaka, Akihisa Yasuda, Shinji Kitagami, Hideo Kasai, Takayuki Ishimoto

1.はじめに

情報家電をはじめとする各種機器がネットワークにつながり,オープンな環境においてサービス提供(遠隔監視など)を受けることが可能な環境がそろってきた.しかし,ネットワーク接続可能機器の普及によって, (1)制御内容のセキュリティの検討が不十分,(2)アクセス制御が不十分といった課題が明らかになってきた.

そこで,デジタルコンテンツのアクセス制御(DRM)の考えを,機器のアクセス制御に適用することにより,制御内容のセキュリティとして「サービスの安全性」を定義し,また,オープンな環境でもきめ細かなアクセス制御を実現する機器利用権を定義したので報告する.

2.課題

本章では,オープン環境でのリモート制御における従来の脅威と,新たに考慮すべき脅威について示す.

従来から,リモート制御において,(a)不正なユーザからの脅威,(b)“ 成りすまし” による不正操作や不正な情報収集,(c)通信データの“ 改ざん” や“ 盗聴” などがあった.これらの脅威に対して,SSL (Secure Socket Layer)技術等を用いた相互認証および通信データの暗号化技術により,ネットワーク上の安全性は確保されてきた.

しかし,リモート制御サービスの台頭・複雑化によって,(d)正当なサービス提供者からの脅威(つまり,サービス契約内容以外の不正な操作(誤操作,システムの不具合を含む)の考慮が必要となってきた.つまり,認証をした正当な相手からのサービス契約に基づかない制御(御操作や不具合服務)を受ける可能性を防御できない.

3.DRM 技術の機器アクセス制御への適用

前述のような認証後の制御機能として,デジタルコンテンツの利用権管理技術(あるいは,デジタル著作権管理(DRM : Digital Right Management)技術とも呼ぶ)がある.そこで,DRM のアクセス制御の考えを機器のリモート制御に適用することを考えた.

デジタルコンテンツの利用制御と機器の利用制御において,以下に示すように,保護対象と保護主体(保護対象を守りたい人)および想定不正者(保護対処に不正アクセスを試みる人)との関係が異なる.

表１　コンテンツ制御との比較

	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(著作権)	機器そのもの
保護主体	著作権者(サーバ側)	利用者(機器側)
脅威	不正コピーなど	機器の不正利用
想定不正実施者	利用者(機器側)	サービス提供者(サーバ側)

そのため,利用権管理技術はそのままでは適用できない.

そこで,保護主体である利用者主導の観点で,ライセンスを利用者が発行し,そのラインセンスを用いてリモート制御することで,コンテンツの利用権管理技術を機器のアクセス制御に適用できる.なお,コンテンツに対応するものとして機器を制御するコマンド,ビューワに対応するものとしてコマンド実行機構を考える.

表２　適用方法の整理

適用技術	適応箇所
機器制御コマンドの暗号化	保護対処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復号と実行を行う	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利用者側で作成

以上のように,DRM の考えを機器のリモート制御に適用できることを示した[1].

4.サービスの安全性と機器利用権

前述の正当なサービス提供者からの脅威に対する安全性を,「サービスの契約内容に逸脱しないサービスが提供されること」と定義し,この安全性を確保するためには,サービス契約外の操作をチェックし,防止する機能を提供する必要がある.

その為にはサービス契約の内容を機器が判断可能な表現方式－機器利用権－を定義した.機器利用権は,XML(eXtensible Markup Language)表記によって操作内容を規定する.規定内容としては,DRM 技術に準拠し,サービス識別情報(操作はどのサービス契約に基づくものか),操作対象機器(家庭内のどの機器を操作するのか),操作対象情報(操作許可する機能－エアコンならば設定温度,動作モード,電源 ON/OFF 等),操作内容(設定あるいは情報読取か)等を指定可能とした.機器利用権メッセージを構成するタグを以下に示す.

表３　機器利用権の行使のメッセージ形式(概要)

タグ	意味
<?xml>	XML 宣言
<RCRM>	機器利用権メッセージ形式であることを示す
<SignedUse>	機器利用権の行使表現
<Use>	行使内容
<SignedRight>	機器利用権の許諾表現
<Right>	制御許諾内容
<ServiceID>	サービス提供者の指定
<Device>	制御対象の指定
<GW_Info>	ゲートウェイの指定
<Device_Info>	制御対象機器の指定
<Action>	操作内容の指定
<Property>	操作許可内容の指定(複数指定可)
<Condition>	利用条件の指定
<Signature>	機器所有者の署名
<ExecAction>	操作内容
<Property>	実際に操作する内容
<Signature>	サービス提供者の署名

† 三菱電機株式会社
‡ 三菱電機インフォメーションシステムズ株式会社

具体的な指定例を以下に示す

- 操作対象の Device の指定例を以下に示す.なお,Device の指定や Action の指定の具体的な値は,Ehconet[2]のオブジェクトおよびメソッドを利用した.

```
<Device_Info ClassGroupCode="0x03" ClassCode="0x01" InstanceCode="0x01" />
```

図 1　機器の指定例

- 実際に制御する<execAction>の指定例を以下に示す.これは,許可した<Action>のサブセットである必要がある.

```
<ExecAction>
  <Property Code="0xB3" Method="Set" Value="0x1C"/>
</ExecAction>
```

図 2　制御内容の指定例

5. 機器利用権によるサービスの安全性の実現

5.1　制御手順

機器利用権を用いたリモート制御手順を以下に示す.

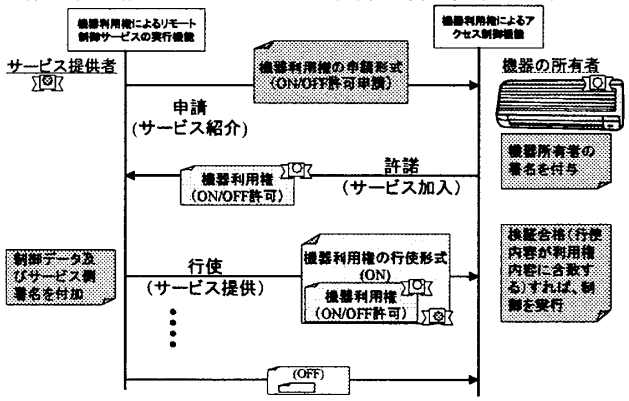

図 3　リモート制御の手順

1. サービス提供者からのサービス情報提供：サービス提供者は,サービス契約内容を公開する.この契約内容は,機器利用権の形式で公開される.
2. ユーザのサービス加入：ユーザは,サービス情報を確認(該当するリモート制御内容が許可できる場合)し,サービスの加入を行う.この時,サービス契約内容,つまりサービス事業者と機器所有者の合意内容を記載した機器利用権を発行する.
3. サービス提供者からのサービス提供：サービス加入にて得た機器利用権に,具体的な制御コマンドを付加して,機器に送付することによって,サービス提供,つまりリモート制御を行う.このとき,制御内容が,サービス契約内容(＝機器利用権)から逸脱していないかどうかをチェックし,正しい場合に実行する.

5.2 サービスの安全性の仕組み

サービスの安全性を守るために,下記の検証を行う.

①利用権行使に付与されたサービス提供者の署名の検証により,データの改竄,なりすましを検出する.

②利用権に付与された所有者の署名の検証により,利用権改竄や他人の発行した利用権との混同を検出する.

③利用権の発行先のサービス提供者情報と,利用権行使を行っているサービス提供者が一致していることを確認し,成りすましを検出する

④操作内容が,機器利用権の利用条件を満足している,つまり,サービス契約内容に合致していることを確認し,サービスの安全性を検出する.

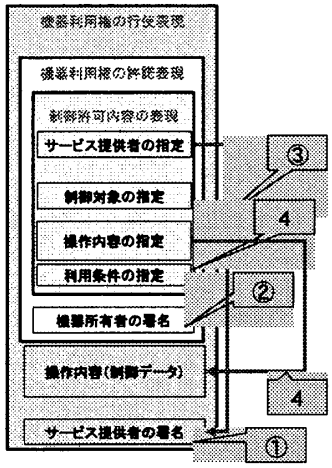

図 4　安全性の仕組み

6. 省エネのためのリモート制御サービス

本機器利用権を用いたサービスの安全性・利便性を評価するに当たって,省エネのリモート制御サービスを検討した.本サービスでは,ユーザはサービス契約時にサービス事業者に対して事前に機器利用権を発行しておく.ユーザが外出先から機器を制御する場合はこのサービス事業者の提供するWebアプリを介して機器制御を実行する.

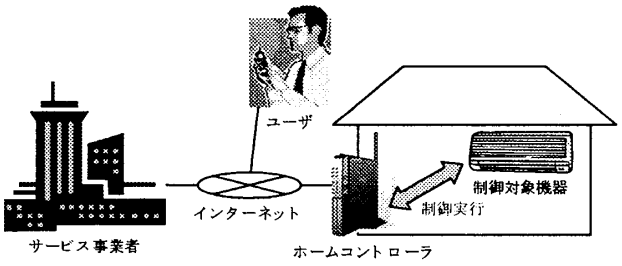

図 5　サービスシナリオのシステム構成図

7.おわりに

リモート制御サービスの普及に必要な,サービスの安全性について定義し,それを実現するための機器利用権を定義した.また,この機器利用権を用いた安全なリモート制御サービスが実現できることを示した.

参考文献

[1]釜坂他,“ リモート制御サービスの安全性を表現する機器利用権” , DICOMO2007,1B-2,pp.41-48, July(2007)

[2] ECHONET CONSORTIUM,“ エコーネット規格書 Ver3.21(日本語版)” , http://www.echonet.gr.jp/8_kikaku/index.htm

謝辞

本開発は,独立行政法人 新エネルギー・産業技術総合開発機構(NEDO)の「デジタル情報機器相互運用基盤プロジェクト/デジタル情報機器の統合リモート管理基盤技術の開発」で取り組んでいる委託研究成果の一部である.