N-031

宅内ネットワークにおける PKI ベース DRM の一提案

A Proposal of DRM Based on PKI in Home Network

堀　吉宏†　　小出　哲久‡　　岩田　彰‡
Yoshihiro Hori　Norihisa Koide　Akira Iwata

１．まえがき

コンテンツのデジタル化を支える仕組みとして、コンテンツを不正な利用から保護するデジタル著作権管理(DRM: Digital Rights Management)が実用化されている。現在、実用化されている DRM は、デジタル記録メディア、コンテンツ配信サービスあるいは機器間インタフェースをターゲットとして開発された。そして、ターゲットの特質に特化することで仕組みを提供するシステムが主流である。

一方、家庭内の機器を IP ネットワークなどで繋いで家庭内にあるデジタルコンテンツを家庭内の各機器で共有するための宅内ネットワーク、特に DLNA（Digital Living Network Alliance）[1]が注目を集めている。このような宅内ネットワークに接続された機器間でのデジタルコンテンツの共有を円滑に行うためには、コンテンツ伝送・記録を管理する DRM が必要である。DLNA では、コンテンツ伝送のために DTCP-IP (Digital Transmission Content Protection over Internet Protocol）[2]および WMDRM-ND (Windows Media DRM for Network Devices) を採用している。これらの DRM は、それぞれの生い立ちに依存した特徴を持ち、コンテンツの伝送から記録までを総合的に保護する仕組みではない。

我々は、総合的に保護する仕組みの開発を目指す。SAFIA (Security Architecture for Intelligent Attachment Device）コンテンツ保護技術[3][4]は、デジタル記録媒体をターゲットとして開発された。しかし、予めネットワークを意識して、ネットワークと親和性の良い PKI (Public Key Infrastructure)を採用している。我々は、この技術を宅内伝送にネットワーク対応に拡張するための検討を行った。本報告では、拡張した宅内ネット網における機器間認証方式について提案する。これによってデジタルコンテンツ宅内伝送と記録を総合的に扱える DRM の提供できる。

２．ホームドメインの要件

私的利用に限定した宅内ネットワーク空間（以下ではホームドメインと呼ぶ）内であれば、コンテンツ権利者の権利を侵すことなくユーザの利便性を向上させることができる。１つのコンテンツを複数の機器で共有して利用すること、携帯機器に記録して持ち出して宅外で利用することも可能である。そのためにはドメイン管理機能を備えた DRM が必要となる。この DRM を構成する機器に求められる機能要件を、以下に記載する。

（1） 正当な機器であることが証明できること、
（2） 機密漏洩に際して機器のリボークが可能なこと、
（3） Usage Rule に従った利用制御が可能なこと、
（4） ドメインへの参加・離脱を自立的に認識すること、
（5） ネットワークから切り離された状態でコンテンツが利用できること。

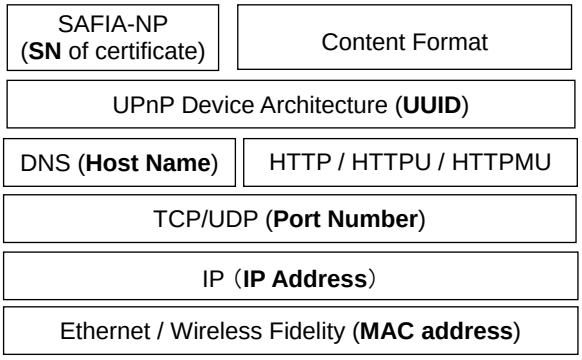
本報告では、主に要件(4)及び(5)に対する機能について基礎検討を行う。尚、ベースとする SAFIA コンテンツ保護技術が、要件(1)、(2)、(3)に対する基本機能を提供している。

†三洋電機（株）デジタルシステム研究所
‡名古屋工業大学

３．機器の参加・離脱の認識

3.1　ドメイン識別情報の考察

ホームドメインへの機器の参加・離脱を判定するための機器から取得するドメイン識別情報について考察する。ネットワークに接続されている機器から取得可能な識別情報を、そのままドメイン情報として転用すると効率的である。図１に、DLNA における階層化モデルとそこで運用される識別情報の関係を示す。最上位層は、コンテンツを対象としたアプリケーション層である。



SAFIA-NP: SAFIA network Protocol, SN: serial Number,
UPnP: Universal Plug & Play, UUID: Universal Unique Identifier,
DNS: Domain Name System, HTTP: Hyper Text Transfer Protocol,
TCP: Transmission Control Protocol, IP: Internet Protocol,
UPT: User Datagram Protocol, MAC: Media Access Control

図 1. ネットワーク階層モデルと識別情報

- SN of certificate: 公開鍵証明書のシリアル番号、
- UUID: オブジェクト毎にユニークな識別子、
- Host Name: IP address に対して付けるニックネーム、
- Port Number: 同一通信機器で動いているプロセスを特定する番号、
- IP address: ネットワーク上の通信機器を識別する番号、サブネット分割により空間を限定することができる、
- MAC address: ネットワーク機器（ハードウェア）毎にユニークな識別子。

ドメインは、はネットワーク上の１つのサブ空間である。ドメインへの参加・離脱の判断には、同一のサブ空間内に対象とする機器が存在するか否かを認識することで実現できる。IP address は、サブネットマスクの活用により、サブネット空間を作ることができる。このサブネット空間を１つのドメインとする。ルータを導入すれば、ルータ下に１つのサブネットが構成されるため、家庭への導入もスム

ースである。他の識別情報は、ドメインの参加を判断するにはドメイン構成機器としての登録が必要となるため不適切ではない。従って送信側の機器 (Primal Device) が、受信側機器 (Inceptive Device) が同じドメインに参加しているか判断する情報として IP address を用いる。

3.2. 転送手順

SAFIA コンテンツ保護技術は、Unidirectional Transfer モード[5]の転送手順をベースに拡張を行う。コンテンツデータは暗号化されて扱われる。これを復号するコンテンツ鍵と利用ルール記述子は、Usage Pass と呼ばれるデータパッケージに納められている。転送手順は、Usage Pass を転送する手順である。図１の SAFIA-NP が本転送手順である。図２に本転送手順を示す。E（K,D）は鍵 K でデータ列 D を暗号化した結果を示すデータ列を、H（D）はデータ列 D に対するハッシュ値を示すデータ列、X || Y はデータ列 X とデータ列 Y の連結を示す。なお、公開鍵暗号方式は EC-DH（Elliptic Curve Diffie-Hellman）が採用されている。拡張したステップは CS5 である。

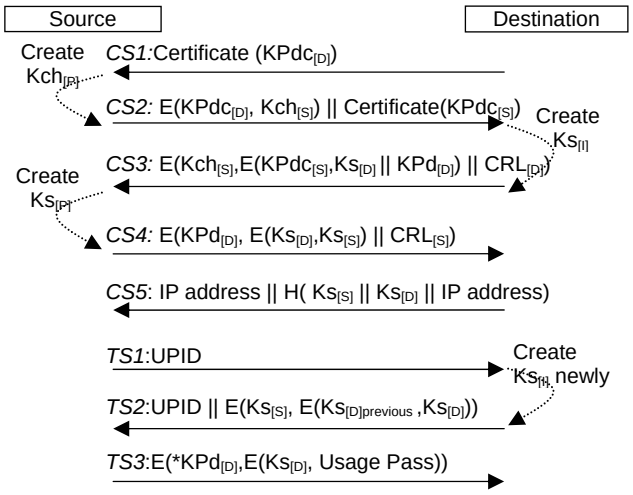


図 2 Usage Pass 送信手順

［接続ステップ］

CS1: Destination の証明書 Certificate ($KPdc_{[D]}$) が Primal Source へ送られ認証される。

CS2: Source は、チャレンジ鍵 $Kch_{[S]}$を乱数生成し、証明書のデバイスクラス公開鍵 $KPdc_{[D]}$で暗号化して、証明書 Certificate($KPdc_{[S]}$) と共に Destination に送る。Destination は証明書 Certificate($KPdc_{[S]}$) を認証する。次いで、復号処理を行い $Kch_{[S]}$を取り出す。

CS3: Destination は、セッション鍵 $Ks_{[D]}$を乱数生成し、これと自身のデバイス公開鍵 $KPd_{[D]}$ を、証明書のデバイスクラス公開鍵 $KPdc_{[S]}$で暗号化する。さらに、保持する $CRL_{[D]}$と共に、$Kch_{[S]}$で暗号化して、Source に送る。Source は、復号して $Ks_{[D]}$、$KPd_{[D]}$ および $CRL_{[D]}$を取り出す。この時 $CRL_{[D]}$が保持する $CRL_{[S]}$より新しければ、$CRL_{[S]}$を $CRL_{[D]}$に書き換える。

CS4: Source は、セッション鍵 $Ks_{[S]}$を乱数生成し、これをデバイス公開鍵 $KPd_{[D]}$ で暗号化する。さらに、保持する $CRL_{[S]}$と共に、$Ks_{[D]}$で暗号化して、Destination に送る。CS3 で取り出した $CRL_{[D]}$ が保持する $CRL_{[S]}$より新しければ、$CRL_{[S]}$は省略する。Destination は、$Ks_{[S]}$ および $CRL_{[S]}$を復号して取り出す。$CRL_{[S]}$が含まれる場合、取り出した $CRL_{[S]}$で、保持する $CRL_{[D]}$を書き換える。この時点で双方は、$Ks_{[S]}$、$Ks_{[D]}$、および、デバイス公開鍵 $KPd_{[D]}$ を用いた EC-DH によって共有した鍵*$KPd_{[D]}$ を共有する。

CS5: Destination は、自身の IP Address と双方で共有した２つのセッション鍵 $Ks_{[S]}$、$Ks_{[D]}$ を連結したデータのハッシュ値を求め、自身の IP Address と共に Source に送信する。Source は、内部に保持している鍵 $Ks_{[S]}$、$Ks_{[D]}$を用いて、IP address の改ざん確認を行う。IP address の改ざんがなく、自身と同じサブネットに属していれば同じホームドメイン内に登録された機器であると判断する。そして、Usage Pass 転送ステップ(TS)に移行する。他の場合は、共有した鍵をすべて破棄して終了する。尚、Usage Pass 転送ステップについては説明を省略する。

Source は、ステップ CS5 において Destination が同一のドメインに参加しているか、離脱ししているかう正確に判断することができる。そして、ドメイン内の機器に対してのみ、Usage Pass を転送する。

４．離脱機器の再生

ネットワークから切り離しを、ホームドメインからの離脱と考え再生を禁止すると、携帯装置での視聴ができない。したがって、ネットワークから切り離された状態でも、視聴を保証する必要がある。他のドメインに接続した場合に、コンテンツの移動による流入を防ぐ仕組みが必要である。利用ルール記 Move control of Storage Device 記述子の追加し、移動の運用を制限する（表１：太字）。

表１．利用ルール of Usage Pass

Name	Value	Description
Generation Count	**0h**	No more copy
	1h	One generation
	2h	Two generation
	Fh	Not assert
Move control of Storage Device	00b	Move is allowed
	01b	Move is prohibited in BT mode
	10b	Move is prohibited in UT mode
	11b	Move is prohibited

５．まとめ

SAFIA コンテンツ保護技術をベースに、IP ネットワークに対応した SAFIA-NP の提案を行った。実用化には評価は必要である。ホームドメイン制御が適切に制御できる DRM があれば、コンテンツの利用制限が緩和による、ユーザの利便性の向上が期待できると考える。

【参考文献】

[1] http://www.dlna.org/

[2] http://www.dtcp.com/

[3] http://www.safia-lb.com/

[4] T. Hirai and Y. Hori, “An HDD-base Removable Medium and its AT-Attachment Interface Architecture for Copyright Protection, “ IEEE Transaction on Consumer Electronics, Vol.49, No.4, pp1161-1168, Nov 2003

[5] T. Hirai, Y. Hori, Y. Shimizu, I. and Takemura, “Over view of Content Protection Technology for an Intelligent Attachment Device,” ICCE paper No.3.1-2, Jan 2006