コンピュータセキュリティ 17－8
（２００２．５．２３）

MPEG-21/IPMP による多面的安全性の実現手法

金子 格(Itaru-k@acm.org)†, 白井克彦‡
†早稲田大学理工学総合研究センター,‡早稲田大学

[要旨]著者等は急速に利用が広がるブロードバンド・ネットワーク等、社会インフラとなるような大規模な AV サービスにおいて考慮されなければならない、より多様な安全性の問題を分析することが可能なモデルとして、多面的安全性モデルを提案している。本報告では、モデルの形式的表現を試みる。また MPEG-21/IPMP による実現手法についても、最新の仕様に基づいて検討する。

Multi-lateral Security and implementation in MPEG-21/IPMP

Itaru Kaneko†, Katsuhiko Shirai‡
Research Institute for Science and Engineering Waseda University†, Waseda University‡

Abstract: Authors are proposing Multi-Lateral Security Model(MLSM) which may analyze more variety of security issues those need to be considered in large scale audio visual services such as broadband multimedia services which is rapidly evolving and must be considered as a social infrastructure. In this report, we will show the formal representation of the model, and also describe implementations using MPEG-21/IPMP based on the latest specification.

1. はじめに

著者等は以前より、社会インフラとなるような大規模な AV サービスにおける多面的安全性の一般的な定義付けとその定義に基づくシステムの分析について論じてきた[1)2)3)4)5)]。

社会インフラとしての広がりをもつような大規模な AV サービスにおいて必要となるシステム間の相互運用性、社会インフラとしての安全性や公平性、文化インフラとしての永続性、一般性など多様な特性に配慮し、従来の一面的安全性モデル(ULSM:Uni Lateral Security Model)に代わり、安全性に対する多面的な要求を総合的にモデル化できる、より現実に近い安全性のモデルを提案し、多面的安全性モデル(MLSM: Multi Lateral Security Model)と呼ぶこととした。

本報告では、特にその形式的な表現を試みる。また MPEG-21/IPMP の標準化状況を示し、MPEG-21/IPMP の MLSM 安全性について検討する。

2. MLSM における拡張

ULSM から MLSM への拡張を図 1と図 2を用いて説明する。

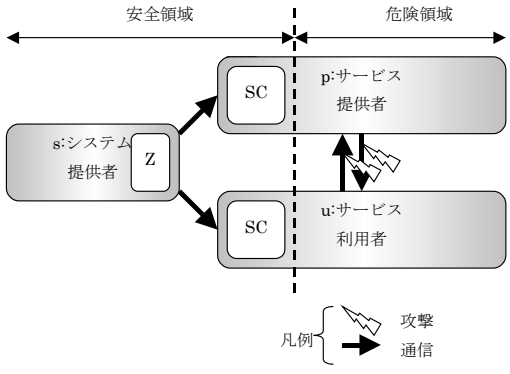

図1 一面的安全性:ULSM
uni-lateral security

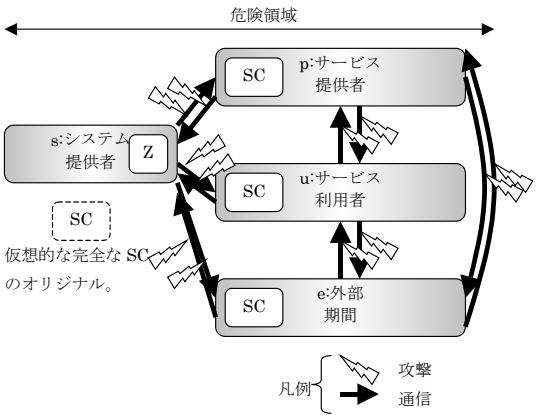

図2 多面的安全性:MLSM
multi-lateral security

(1)外部機関の追加

MLSM ではサービス提供者、サービス利用者、システム提供者のほかに、ULSM で直接通信モデルに含まれなかった著者や作曲家なども外部機関としてモデルに含まれる。

(2)セキュリティ・モジュールの欠陥

MLSM では完全な(欠陥のない)セキュリティー・モジュールが伝送時に改変を受ける可能性を仮定することで、ULSM で考慮されなかったセキュリティ・モジュールの欠陥もモデル化する。

(3)PL 分析による安全性評価

ULSM では「到達可能性」を安全性の判断基準とするが、MLSM では PL(利益損失)による確率分布を評価基準とする。

3. MLSM の形式的記述

次に MLSM の形式的記述を試みる。攻撃経路 S_i は状態遷移の組み合わせとし、式 1で表現する。すると、経路確率 p_j,と経路利得 g_j,は式 2式 3のように表現できる。

$$S_i = [t_{i,1}, t_{i,2}, \cdots, t_{i,n}] \quad \text{式1}$$

$$p_j = p(S_i) \quad \text{式2}$$

$$g_i = \sum g(t_{i,j}) \quad \text{式3}$$

すべての攻撃の経路確率式 4と経路利得式 5により攻撃の利得/確率分布式 6が得られる。

$$P = \{p_j\} \quad \text{式4}$$

$$G = \{g_j\} \quad \text{式5}$$

$$P(g) = \sum_{for\ all\ j\ g_j = g} p_j \quad \text{式6}$$

利得確率分布に基づいて収支分析を行うことで安全性を判定する。対象となるシステムの特性は、この P と G でほぼ記述できるので式 6のように、これを L で表す。

$$L =< P, G > \quad \text{式7}$$

多面的安全性では各利害関係者は、安全性に関して異なる情報を有し、異なる意見を持つ。そこで a を利害関係者を表す指標とすると式 8～式 12のように各主体は異なるモデルをもつことになる。

$$p_{a,i} = p_a(S_i) \quad \text{式8}$$

$$g_{a,i} = \sum g_a(t_{i,j}) \quad \text{式9}$$

$$P_a = \{p_{a,j}\} \quad \text{式10}$$

$$G_a = \{g_{a,j}\} \quad \text{式11}$$

$$L_a =< P_a, G_a > \quad \text{式12}$$

以上の形式を用いれば、ULSM と MLSM のモデルの違いを表 1のようにあらわせる。

表 1 ULSM と MLSM の違い

系	ULSM	MLSM
特性	$L =< P, G >$	$L_a =< P_a, G_a >$
経路確率	$p(S) \in \{0,1\}$	$p(S) \in \Phi$
経路収支	$g(S) \in \{0,1\}$	$g(S) \in \Phi$
分析方法	E{G}=0	任意

ULSM では経路確率は{0,1}(可能か不可能)の 2 値であるのに対し、MLSM では実数値を与える。ULSM では経路収支の大小は考慮されず、表では{0,1}としているが、MLSM では実数値を与える。ULSM では想定される特性は一意的であり、分析は従って単純化された利益が 0 であることを判定することで行われる。

MLSM では安全性の分析方法は任意であり、先の論文では手法のいくつかを示した。

静的 PL 分析は、式 13のように収支の平均がマイナスであることを条件とする。

$$\mathrm{E}\{g\} < g_0 \quad \text{式13}$$

動的 PL 分析では、系に属する仮想的な攻撃者の挙動を L_a によって特徴づけ、**c** が 0 近くで安定することを条件とする。ここで **c** は様々なタイプの攻撃者の数、λは L に依存する **c** の変化である。

$$\mathbf{c}_{i+1} = \Phi(\mathbf{c}_i, L) \quad \text{式14}$$

4. MLSM の特徴

4.1. モデル化の容易性

MLSM では各利害関係者 a に応じた L_a は個々の a 毎に独立である。したがって L_a は a の主観であって、

必ずしも正確である必要はなく、実際の確率と一致する必要すらない。ULSM では L_a をどう決定するかがまず問題となるが、MLSM においては主観的な L_a をそのままモデルに採用することができるので、意見の不一致によりシステムの評価が定まらないということはない。

一般に、システム提供者は設計情報を元に L_a を直接的に推定し、他の利害関係者はシステム提供者や検査代行者から得た意見と、それらの利害関係から、間接的に L_a を推定する。

また L_a は攻撃方法毎の成功確率を確率的に表現したものであるから、システムの一部について性能が明確でない場合も、推定値と推定誤差の確率を用いてモデルの構築が可能である。たとえば IC カードの秘密鍵が読み取られる確率を厳密に求めることは不可能だが、読み取りに必要な平均的なコストは算出することが可能である。このように MLSM においては、限られた取得情報からでもモデルに基づく安全性を推定することができる。

4.2. 巾広い分析対象

MLSM は、モデルがより一般的であることにより、これまでよりも幅広い分野の分析が可能である。MLSM により、始めて分析が可能となる性質の例として、以下をあげる。

(1) 応用規模と必要なセキュリティ強度の関係。

デコーダ数や利用者数が増加した場合に、同程度のセキュリティを守るために個々のセキュリティ機能の耐性を高める必要があるが、この具体的関係を MLSM を用いれば記述できる。

(2) 内部不良の抑制方法

いわゆる組織的問題で不良が発生する場合があるが、利害関係者間のゲーム理論的分析により、内部不良を防ぐインセンティブを定量的に分析できる。

4.3. MLSM の外部依存性

MSLM によれば、外部環境がシステムの安全性に影響する。

たとえば、インターネットの普及により特定のコピー制限解除ツールの配布コストが安くなったり、またコピー防止解除したコンテンツをインターネットで交換できる仕組みが整ったとすれば、攻撃のコストが変化したことになり、同様に G_a の変化に相当する。

また、G_a に関して利害関係者一人一人が異なる見解を持ちえるから、コンテンツ配信システムへの新たな参加者は、常にこれまでの参加者と異なる意見 L_a =<P_a,G_a >を持つ可能性がある。

このように MLSM 安全性は一定ではなく、環境によって常に変動を受ける。MLSM を前提にシステムの安全性を一定に保とうとすれば、最初から未来永劫にわたって十分な安全性を有するシステムを構築するか、あるいは運用を続けながら、状況の変化に合わせてセキュリティを強化する必要がある。

5. MPEG-21/IPMP による MLSM の実現

現在筆者等は MLSM 安全性に着目しながら MPEG-21/IPMP の標準化作業に加わっている[7][8][9][10][11][12][13]。また先の報告では MLSM 安全性を実現するには、拡張性と、利害関係者間の利害関係に基づいたセキュリティの管理が重要であることを示した。また、これらの点から、セキュリティ・モジュールの交換性が高く、拡張性の高い IPMP アーキテクチャーが優れていることを指摘した。本章では、その IPMP アーキテクチャーの標準化の最新状況を示す。

5.1. MPEG-21/IPMP

先の報告で示したように、MPEG では IPMP version 1 を拡張する IPMP Extension[6]の標準化を進め MPEG-21/IPMP への適用も検討している。IPMP Extension では先の IPMP で単一のモジュールであった IPMP システムを、さらに細かい IPMP tool と呼ぶユニットの集合とする。図 3はそのブロック図を示す。個々の IPMP tool が MLSM における SC と考えることができる。

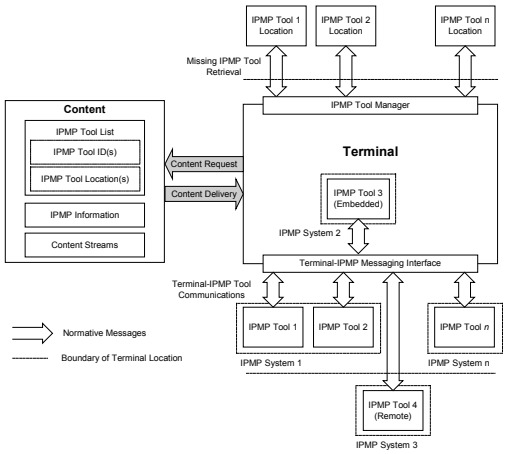

図 3 MPEG/IPMP extension

またこの方式では多重 SC 運用に関して以下の利点がある。

(1) 個々の IPMP tool は単純で分析も交換が容易である。このことが SC 交換や SC 分析の費用を下げ、安全性に有利に働く。

(2) IPMP システムのうち、安全性に関し重要な部分を選択的に交換可能とすることで、最小の費用で安全性を効果的に高めることができる。

(3)IPMP tool の動的追加が可能であり、検査者の作業を援助する IPMP tool を導入することで、運用開始後に安全性を強化することが可能である。

たとえば、図 4に示すように、複数の IPMP tool を同時に使用したり、図 5に示すように IPMP tool のうちの一つを、プライバシー保護等に利用したりする構成が可能である。

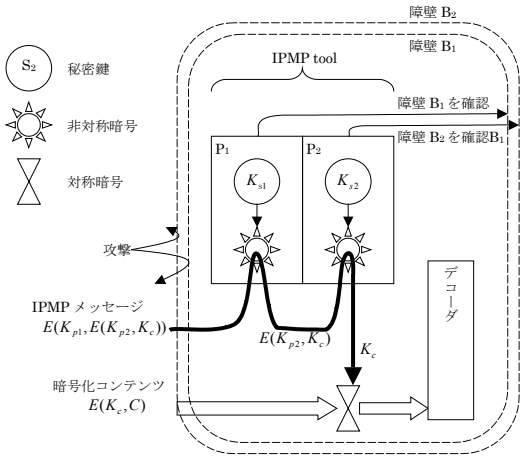

図 4 IPMP Extension におけるセキュリティのスケーラビリティ

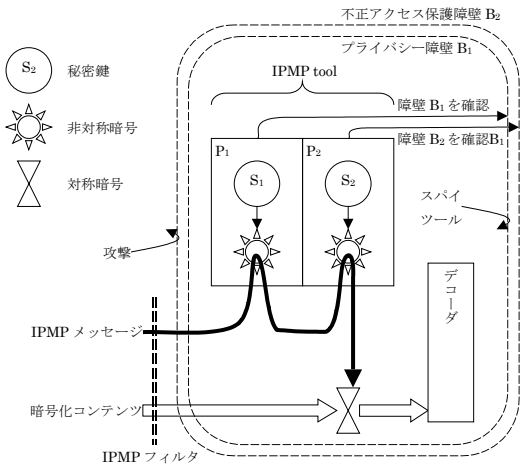

図 5 IPMP Extension による利用者保護の方法の一つ

5.2. MPEG-21 IPMP の実現

MPEG-21/IPMP としては、現在 FPDAM 段階にある MPEG-4/IPMP Extension をより汎用的な形に改めることが検討されている。MPEG-4/Extension では、MPEG-4 のビットストリームを拡張し、IPMP 関係の情報を組み込む方法と、IPMP Tool 間のメッセージ交換の方法が規定されている。

表 2　IPMP Extension

ObjectDescriptorBase + IPMP_ToolListDescriptor
BaseDescriptor + IPMP_Tool
DecoderSpecificInfo + IPMPToolES_DecoderConfig
IPMP_ToolES_AU
IPMP_Initialize
BaseDescriptor + IPMP_ToolDescriptorPointer + IPMP_ToolDescriptor
BaseCommand + IPMP_ToolDescriptorUpdate + IPMP_ToolDescriptorRemove
DecoderSpecificInfo + IPMPDecoderConfiguration
IPMP_StreamDataUpdate
DateClass
TrustSecurityMetadata

表 3　IPMP Extension Message

IPMP_ToolSecureMessage
(Instantiation and Notification Messages) IPMP_GetTools IPMP_GetToolsResponse IPMP_GetToolContext IPMP_GetToolContextResponse IPMP_ConnectTool IPMP_DisconnectTool IPMP_ToolConnectNotification
(Event Notification Messages) IPMP_AddToolNotificationListener IPMP_RemoveToolNotificationListener IPMP_NotifyToolEvent
(IPMP Information Delivery Functions) IPMP_MessageFromBitstream IPMP_ToolDescriptorFromBitstream
(Consumption Permission) IPMP_CanProcess
(User Interaction Messages) ToolToUserMessage UserToToolMessage
(Mutual Authentication Messages) IPMP_InitAuthentication IPMP_Mutual_Authentication
Key Descriptor
AlgorithmDescriptor
(Parametric Messages) IPMP_ToolParamCapabilitiesQuery IPMP_ToolParamCapabilitiesResponse

MPEG-4 のビットストリームに IPMP に関する情

報を組み込む方法としては表 2の syntax が規定されている。

また IPMP_Tool 間には表 3に示すメッセージが規定されている。

5.3. IPMP の MLSM 安全性の検討

次に、IPMP の MLSML 安全性を検討する。先の報告[14]で、筆者等はシステム提供者以外の利害関係者にとっての安全性が、セキュリティシステムの交換容易性によって大きく改善される場合があることを示した。この関係が常に成立するという十分な説明は行っていないが、仮にこの関係が多くの場合に成り立つならば、IPMP アーキテクチャーは IPMP tool 間のメッセージを標準化することにより、IPMP tool の交換容易性を向上し、セキュリティの強化に貢献すると期待できる。

また、MPEG-21 においては現在 REL(Rights Expression Language)の標準化が進んでいる。REL は権利記述言語と呼ばれているが、実際にはもっと汎用的な論理記述言語であり、量化子の指定などを含む述語論理による記述能力を備えている。

MLSM 安全性に基づくならば、REL の述語論理的記述能力を IPMP tool と結びつけることにより、MLSM 安全性の向上に適したアーキテクチャーが構築可能と思われるので、このことについて説明する。

コンテンツの再生は、利害関係者の合意のもとに行われる必要がある。そこで仮に R をコンテンツが再生される条件とすると、R はのように著すことができる。

$$R = r_{a_1} \wedge r_{a_2} \wedge r_{a_3}$$

一方 MLSM 安全性においては、安全性を記述するパラメータ L_a =<P_a,G_a >は利害関係者 a 毎に異なっている。そこで安全性に関する要求項目も、再生の条件に含めることが考えられる。

$$R = r_{a_1} \wedge \hat{r}_{a_1} \wedge r_{a_2} \wedge \hat{r}_{a_2} \wedge r_{a_3} \wedge \hat{r}_{a_3}$$

ここでr_aはコンテンツ再生の経済的条件であり、$\hat{r}_a$はコンテンツ再生のためのセキュリティ面での条件である。たとえば特定のセキュリティツールが作用することを、コンテンツ再生の条件とする、というような記述である。また REL の機能を利用すれば、これらの条件をきめ細かく指定することができる。また IPMP アーキテクチャーを利用すれば、それぞれの安全性に関する条件を、実装上の保護機能と連動させることができる。このように、IPMP と REL の機能を融合すると、各コンテンツに関してそれぞれの利害関係者がそれぞれ安全性についても条件を設定し、条件にあった環境でだけコンテンツを再生させることが可能となる。

このようにきめ細かい制約条件指定できるようにすることは、コンテンツ利用の制約を増やすと誤解されるが、そうではない。

コンテンツ提供者やコンテンツ消費者等の利害関係者から見ると、特定のコンテンツの提供/供給については平均的な利益よりは、リスクにより敏感に反応する傾向がある。つまり、平均的に小さなリスクであっても、「万が一」といった恐れがあれば、コンテンツの供給や消費は必要以上に抑制されると考えられる。しかも、リスクに関する要求条件は様々である。現状では、万人が絶対に安全だと考えられるようなシステムを構築すれば、非常に割高なものになってしまう。

安全性に関する制約条件をコンテンツ毎、利用者毎にきめ細かく指定できれば、個々のコンテンツ、利用者は必要十分な安全性を指定するだけでよく、結果的により多くのコンテンツがそのような条件下で消費可能となると考えられる。このような関係を分析すれば、具体的にどのような条件が成立した時に個別のシステムを開発するのに比べて IPMP+REL のようなシステムが経済的となるかを明らかにできると考えられる。

6. まとめ

本論文では、前半で先の論文で示した多面的安全性 MLSM を、数学的な形式で示した。後半では、IPMP Extension と MPEG-21/IPMP の最新状況を紹介し、MLSM 安全性の面からその有用性を検討した。

大規模な AV サービスでは今後様々な新たな安全性の課題が生じると考えられる。MPEG/IPMP の IPMP Tool によるフレキシビリティが有効であると考えられる理由の一つが、本報告で示されたのではないかと考える。

また、MPEG-21 における IPMP と REL の有用性を MLSM 安全性の面からも検討した。IPMP、及び REL を実装するコストと、個々のセキュリティツールの実装コスト、及び利害関係者間の安全性要求条件の間にどのような関係がある場合に、IPMP+REL が経済的となるかについては、今後さらに分析を進めたい。

謝辞:本研究においては、情報技術調査会 SC29/OICI 小委員会、ISO/IEC JTC1/SC29/MPEG 委員会のメンバーには標準化作業を通じて多くの示唆を得ている。

また早稲田大学白井研究室の方々には弛まないご支援を頂いている。謹んで感謝の意を表したい。

1) 金子 格,” 高度デジタル AV フレームワークの多面的安全性とその特性”,IPSJ, Vol. 41, No. 11, 2000
2) 金子 格,”高度 AV サービスの多面的安全性とその実現”,IPSJ CSEC No.9-3,2000
3) 金子 格,”高度ディジタル AV フレームワークの多面的安全性とその特性”,EIP No.9-2, 2001
4) Itaru Kaneko, Katsuhiko Shirai,” The Multi-lateral Security Framework for the Ubiquitous Internet Multimedia”, IASTED IMSA2001, 340-075, 2001
5) Itaru Kaneko, Katsuhiko Shirai, “THE MULTI-LATERAL SECURITY FRAMEWORK”, IEEE SMC2001, 2001 FOR THE UBIQUITOUS AUDIOVISUAL SERVICES
6) ISO/IEC “ISO/IEC 14496-1 PDAM3 – IPMP extension”, http://mpeg.telecomitalialab.com/public/mpeg-4_ipmp_cd.zip
7) 金子 格、阪本秀樹、白井克彦,” 本格化した MPEG-21 標準化とユビキタス・マルチメディアの将来”,映像情報メディア学会誌 2002 年 2 月号
8) MPEG, “MPEG-21 Overview”, http://mpeg.cselt.it/, MPEG,2001
9) ISO/IEC FCD 21000-3: (MPEG-21) -- Part 3: Digital Item Identification, http://www.itscj.ipsj.or.jp/sc29/open/29view/29n4703c.htm
10) MPEG-21 Part-2 DID, Text for Final Committee Draft, http://www.itscj.ipsj.or.jp/sc29/open/29view/29n4533c.htm
11) MPEG,”IPMP Overview”, MPEG/N2614 , http://www.cselt.it/mpeg/public/w2614.zip
12) MPEG: "MPEG-21 workshop", http://www.cselt.it/mpeg/events/mpeg-21/(2000)
13) ISO/IEC “MPEG-21 Intellectual Property Management and Protection”, http://mpeg.telecomitalialab.com/working_documents.htm#MPEG-21
14) 金子 格他,” ユビキタス・マルチメディアに必要な多面的安全性と MPEG/IPMP によるその実現”, 情報処理学会 CSEC 研究会,