5D－1

情報家電で必要となるセキュリティと技術的側面
Security requirements and it's technical aspects of IT consumer devices

金子 格[+]
Itaru Kaneko[+]

[要旨]情報家電機器によるデジタルコンテントや電子商取引などのデジタルサービスの利用が広がり、セキュリティがより重要な課題となった。しかし、これまでデジタルサービス運営者が他者からの攻撃からシステムやサービスを守るという、一方向的な安全性に視野が限られていた。本論ではそれら以外の多様な方面に係わる安全性を含めた「多面的安全性」について考察する。また多面的安全性の技術的側面についても考察する。

1. はじめに

パソコンとインターネットにより、高品質のデジタルコンテンツがネットワークを通じて全世界に配信され、また日常的にデジタルコピーが行われるようになった。また電子商取引の利用も拡大しつつある。今後はデジタルテレビ、次世代携帯電話など、パソコンと同等以上のデジタルサービス能力を持つ機器の普及が目前となっている。[1)]

パソコン等を利用したデジタルサービスでは、暗号等を利用してサービスの安全性を確保する技術が発展してきた。ハードウェア性能の向上で暗号の利用が容易になり、ネットワークや電子決済の普及で、条件視聴や電子商取引の実用化の条件が整った[2),3),4)]。デジタルサービスの重要性はますます高まっている。

しかし、デジタルサービスがさらに広く利用され、他の大規模な経済活動と比較しうる規模に拡大すると、他の経済活動と同様に社会的影響やリスクにも配慮する必要が生じると予想される。たとえば大規模なシステムは、個人よりも組織的な攻撃や内部不正の脅威にさらされやすい。またテロ、反社会的行為、人権抑圧にも利用されやすい。さらに、システムの運用に若干の不安が生じただけでも、影響が広範囲に及ぶだけに社会的影響も大きい。

本論では、システム運営者の外部からの安全性が一面的であるのに対し、これらの多方面に対する安全性を「多面的安全性」としてとらえる。またそれを実現するための技術的側面についても考察する。

2. デジタルコンテントの将来像

まず、情報家電で特に進歩が著しいと考えられる、デジタルコンテントの将来像を考える。

すでにパソコン等でデジタルオーディオ・ビデオコンテントが容易に扱えるようになり、インターネットを通じて世界中のコンテントを利用できるようになった。デジタル放送、高速モデム、W-CDMA などの普及により、ますます大量のデジタルコンテントが日常的に扱われるようになるだろう。

[+] 早稲田大学 Waseda University/(株)アスキー
http://www.shirai.info.waseda.ac.jp:8001/~itaru-k/

1999 年に国際標準化が終了した ISO/IEC 14496 MPEG-4 では、あたかもウェブとテレビを融合したような強力なデジタルオーディオビジュアル表現が実現される。その概念を図 1に示す。[5),6),8),7),9)]

MPEG4 では動画、静止画、音声、テキスト、CG、合成音などを「オブジェクト」として自在に組み合わせることが可能である。これらの各「オブジェクト」の再生位置や再生タイミングは、自由に正確に指定することができ、端末側で自由に加工して表示することができる。また、世界中の様々な場所から送信されたビデオデータを「オブジェクト」として URL 指定して画面にはめ込む事も可能である。

このようなデジタルならではの高度な表現力は今日 MPEG4 に限らない。XML、SMIL, JAVA, MHEG など、概ね MPEG4 と同様にマルチメディアコンテントを自在に組み合わせてリアルタイム表示する能力を備えている。近い将来ネットワーク中のオーディオビジュアルコンテントが縦横無尽に組み合わされ、高度利用されるようになるだろう。このようなデジタルコンテント利用の高度化も、より柔軟で強力なセキュリティ技術が求められている一因である。[8),9)]

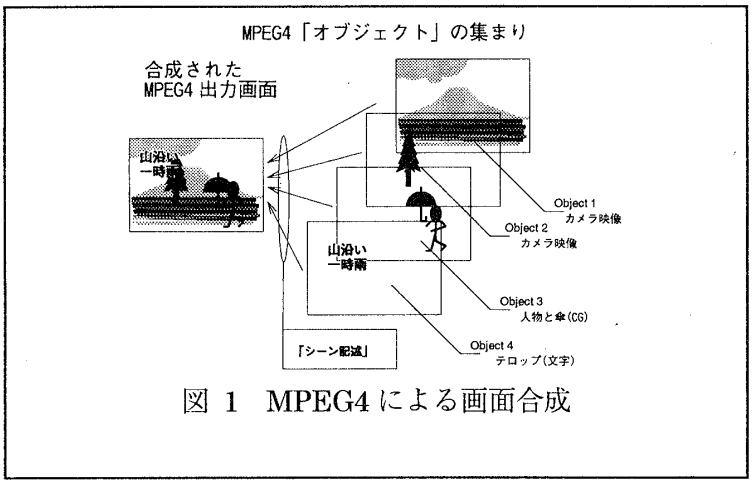

図 1　MPEG4 による画面合成

3. 情報家電セキュリティの要求条件

3.1. 要求条件の多様性

このように様々な形で高度化されていくデジタルサービスにおいて、セキュリティには重大な関心が持たれている。しかし従来その関心は、サービスを外部から防衛する能力に視野が限られていたように思われる。特定の小規模のデジタルサービスでは、それで問題はない。しかしデジタルサービスの規模が拡大するについれ様々な他の問題が意識されるようになった。[10),11),12),13)]

すなわち、情報家電機器といえども人間が運営する以上、その経済規模が一定規模に達すれば、他の大規模な経済活動と同様に社会的配慮を伴ったシステムに成長することが求められるように思われる。

そのいくつかを以下に示す。

3.2. 知的財産権

特許、著作権、意匠権などの知的財産権の保護が必要である。これらに関して、システム運営者が自発的に保護する仕組みについてはすでに多く議論されているので、本論では特に説明しない。

一方で知的財産権は、個々のケースについては常に異論の余地がある権利である点にも配慮が必要である。たとえば盗作である可能性もあるし、特許が無効である可能性もあるし。また一種の不公正取引を形成する場合もある。利用方法に半強制的要素があれば、相応の責任が生じる。

3.3. 不正競争

セキュリティ機能の実現方式によっては不正競争の防止に対する配慮が必要となる。

本論は不正競争の説明が主題ではないが、どのように関連するかを説明するために簡単な例をあげる。たとえば、洗剤を独占的に製造している A 社が、洗剤の購入者と、この洗剤は A 社の衣料品にしか使用を許可しないという契約を結べたとすると、A 社は必需品である洗剤の独占により、衣料品も有利に販売きる。

また、衣類メーカーが相談をし、1 種類の衣類しか作らないと「合意」できたとすると、消費者に選択の余地がなくなり、やはり「合意」に参加した者の利益となる。

これらが自由競争を妨げることは明らかで、自由

経済圏の法制度と行政がこれらの行為を禁ずる所以である。

ところがデジタルサービスのセキュリティの実現方法によっては、ユーザー端末の使用方法を制約する必要が生じる。ユーザーに端末の改造を許すと、セキュリティ機能を無効化される可能性がある。しかし契約で端末の改造を禁止すると、A 方式のデコーダで B 方式を再生する改造も妨げ、間接的に前半に述べた反競争的行為に利用できる。

各社共通のセキュリティ方式を採用すればこの問題は解決する。しかし、同一の規格による製品を供給することに「合意」してしまうと、今度はカルテルとの境界があいまいになる。

本論では特定の法制度を論じることが目的ではないので、これ以上立ち入らない。自由にサービスが創造でき、サービス間の自由な競争を妨げないことを、望ましい特質として認識できれば、以下の議論を進めるには十分である。

3.4. 法制度の変化

デジタル技術の急速な変化により、デジタルサービスに関連する法制度自体が常時微妙な調整を余儀なくされる。

たとえば、デジタルコンテント(ビットの列)が著作物として扱われるようになったのはそれほど昔ではない。その後データベースやソフトウエアも新たに著作物の範疇に加えられた。

その他「特許」「プライバシー」「関税」「消費税」「傍聴」など、デジタルサービスに関して今後も微妙な調整が予想される分野は多数存在する。デジタルサービスのセキュリティ方式については法制度に関連する部分も多く、今後の要求の変化に柔軟に対応し得ることが望ましい。

3.5. 消費者保護

消費者ももちろん様々な保護を必要とする。

第 1 に、契約に際して十分な信頼できる情報が得られる必要がある。また支払いをしたら、サービスが確実に約束された品質で行われる必要がある。またサービスが約束とおり行われなければ賠償や払い戻しを受けられる保証が必要である。

このため、たとえばデジタルコンテントの品質、内容、品質、責任能力が適切に表示され、契約内容が記録される必要がある。

3.6. 反社会性

全く新しい機能を持つシステムの場合、既存の法制度上問題がなくても大きな反社会的効果を伴う場合がある。たとえばあるシステムの導入により殺人、誘拐、脅迫、暴動、テロ、などの犯罪を極端に拡大したり、基本的人権を脅かす危険が高いことがあり得る。既存法上問題がないからといって、そのようなシステムを何も対策を講ぜずに導入するのは、賢明とはいえない。

3.7. 政治性

デジタルサービスがある面で非常に強力であることにより、政治性を持つ場合がある。犯罪捜査や税の徴収とプライバシーのバランス、差別情報の扱い等の問題は常に懸念されている。システム設計が終わりの無い政治的対立に絡め取られないために、システムの能力が極端な能力を持たないほどほどのレベルが保たれる、なども望ましい性質に含められる。

4. 技術的側面の考察

次に以上のような課題に関する技術的側面について考察する。

4.1. 多面的安全性

すでに示したように、情報家電のセキュリティには様々な要因が関係する。サービスを外的脅威から守る安全性が 1 面的であるのに対比して、このような安全性を本論では多面的安全性と呼ぶ。

多面的安全性の個々の要求条件には様々な議論があり、社会的なコンセンサスも得られていない。本論文も、個々の要求条件は問題にしないこととする。

しかし、サービスの外部からの一面的な保護以外に、多面的安全性が必要なことは、定性的性質として示されたと考える。したがって、以下では一般的な意味での多面的安全性の必要性を仮定し、それに適した基本機能と運営スキームを考察する。

4.2. 4者モデル

多面的安全性を 4 者の関係としてモデル化する。4 者とは、コンテント提供者、利用者、システム運用者、外部者である。これらの 4 者はそれぞれ独自の利害関係を持ち、それぞれの間で互いの認証や動作の正当性を確認する必要がある。(図 2)

表 1に、4 者間の関係においてセキュリティの課題を整理して示す。セキュリティの多様な課題ををそれぞれの異なる 2 者間における安全性の課題として整理することができる。

多面的安全性とは、従来システム運営者のユーザーに対する安全性や認証のみを考えていたのに対し、表 1におけるその他の行に示される安全性についても同様に保証することである。

表 1　4者間の安全性

送信	受信	伝送内容	想定されるセキュリティ上の問題
利用者	システム運用者	サービス注文情報	個人の利用情報が漏洩される
			利用統計などの営業機密が第三者にもれる
			他人の ID の不正利用
システム運用者	利用者	サービス内容表示 注文内容確認	個人の利用情報が漏洩される
			利用統計などの営業機密が第三者にもれる
			サービス内容を虚偽表示、誤請求
利用者	コンテント提供者	注文内容	個人の利用情報が漏洩される
			利用統計などの営業情報が第三者にもれる
			利用統計が捏造・水増しされる
コンテント提供者	利用者	サービス内容表示 サービス本体	個人の利用情報が漏洩される
			サービス内容の虚偽表示
			コンテント利用 ID を解析して、不正利用
利用者	外部社会	合法利用記録 (電子印紙、電子公証)	高額商品を利用して脱税
			公的機関によるプライバシーの侵害
			身分を隠してテロ・誘拐・脅迫など不法行為に利用
外部社会	利用者	合法利用の許諾証明	高額商品を利用して脱税
			公的機関によるプライバシーの侵害
			身分を隠してテロ・誘拐・脅迫など不法行為に利用
システム運用者	コンテント提供者	売上記録	コンテント売上の虚偽報告。中ぬき。
			CM 放映回数の虚偽報告。
			無許諾のコンテント利用。
コンテント提供者	システム運用者	内容表示 著作物 ID 著作者 ID	コンテント内容の虚偽表示。
			盗用(他人のコンテントを自作として提供)
			盗用・不正コンテントの証拠隠滅、責任遺棄
システム運用者	外部社会	合法性記録 経理記録・報告	売上の過小報告(税の申告漏れ)
			売上の過剰報告(粉飾決算)
外部社会	システム運用者	各種報告の受領証	売上の過小報告(税の申告漏れ)
			売上の過剰報告(粉飾決算)
コンテント提供者	外部社会	合法性記録 著作権、著作物、著作者 ID	違法なコンテントの頒布
			検閲、表現の自由
			選挙違反
外部社会	コンテント提供者	合法性記録の受領証 著作権、著作物、著作者 ID	違法なコンテントの頒布
			検閲、表現の自由
			選挙違反

4.3. 公開部分と秘密部分

4 者モデルにおいて、4 者間相互の安全性が必要とすると、システム全体を 1 運営者が秘密裏に構築し管理することは不可能である。なぜなら第 3 者の目が届かないところでシステムを構築、管理する者は、いかなる安全性も脅かせるからである。

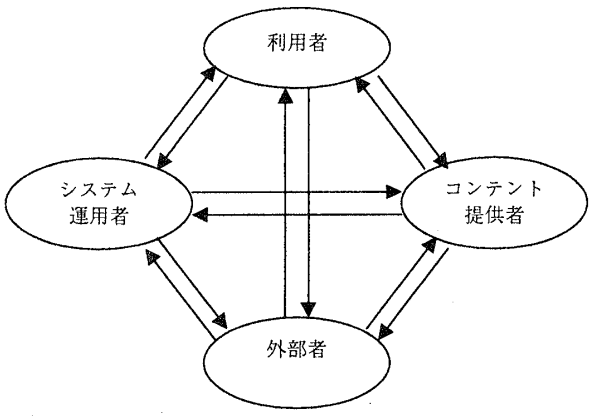

図 2 安全性の諸関係

第 3 者にとって安全確認が可能なためには、IC カードシステムのように基本構造は公開とし、特定のサービス固有の情報のみをカードの秘密領域に格納する構造が必要である。秘密情報サービス毎に守られる事で、個々のサービスの独立性と秘密性が守られ、構造が公開であることにより、第 3 者もその安全性を客観的に評価できる。

情報家電においても同様に、システムの基本構造と API を「公開部分」とし、サービス固有の情報のみをシステムの「秘密部分」として明確に区別して運用する事が必要だろう。

また結果的に「公開構造」は様々な方式で量産が可能となり、コストダウンと性能向上が期待できる。また「秘密部分」の多重化により、多数の事業者が独自にセキュリティを管理することができる。

4.4. ゲーム理論的安全性

大規模システムの最大の弱点は人的要素である。どんなに強固、安全と思われるシステムも、内部の攻撃には驚くほど脆弱である。また経済活動が

大規模になれば、外部の攻撃よりも内部からの脅威にさらされやすくなる。

このような脅威に対抗するためには、不正が暴かれ、不正がゲーム理論的にペイしないようにシステムを設計し、それによってそもそも不正を企画する意欲を失わせることが重要だろう。

その一つのアプローチとして、競争原理が考えられる。同一ハードウエアで独立した事業者が類似のサービスを運営でき、監査機関も複数設置可能とする。このような状況であればサービス事業者は競争的環境下で多面的なセキュリティに努力せざるをえない。監査機関も威信維持のために誠実に監査をせざるを得ない。もし一方の監査機関だけが問題を見逃せば、信用が失墜する。それぞれの威信のために公正で精密な監査を行うだろう。

4.5. サービス規模

政治性や社会的リスクの問題の多くは、一つの事業者に管理されるサービスの規模が巨大化することに原因がある。多数の小規模なデジタルサービスの運営者が、それぞれ独立性を保っていれば、政治性や社会的リスクは薄められる。だからといってサービスの規模を抑制することは、別の政治性を生じるし、本論や技術的解決策の範疇を明らかに逸脱する。

しかし、サービスへの参入を阻む技術障壁がなければサービス規模は自動的に一定規模に収まるかもしれない。出版や運送業のように参入コストが少ない業種では、1 事業者の規模は小規模で安定している。ユーザーはそれほど個別のサービスを求めていないし、かといってそれほど画一的なサービスにも満足しないからである。

サービス規模が中庸に留まれば、規模の問題は存在しない。

4.6. プログラマビリティ

サービス固有のセキュリティ管理方式はプログラマブルでフレキシブルであることが望ましい。各デジタルサービスがセキュリティを独立して保持すると同時に、サービスを制御するプログラムも独自に持つことを可能とすれば、各サービスが独自にシステムの改修を行うことが可能となる。知財権に係わる法制度の微妙な調整にも個別に柔軟に対応していくことが可能になる。

5. プラットフォームの例

本節では、以上のべた多面的安全性を実現するために最も近い距離にあると思われる、セキュリティ技術を二つ示す。

5.1. OPIMA

OPIMA(Open Platform Initiative for Multimedia Access)では、デジタルテレビのためのオープンなセキュリティシステム仕様を策定している。[14]

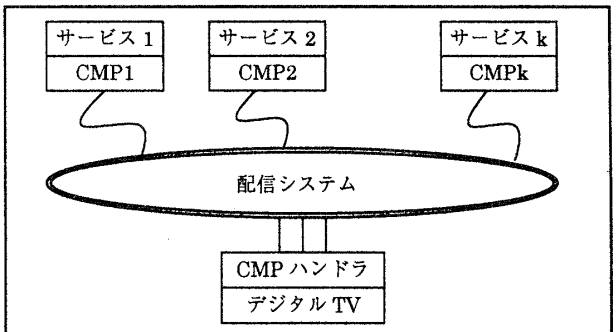

図 3 OPIMA 概念図

図 3に示すように。OPIMA では複数のセキュリティサービスが想定されている。OPIMA では、CMP ハンドラの実装方法は明確に規定していないので、本論で述べたような第 3 者から見て安全なシステムにはならない。しかし、その実装方法の一つが規定されれば、本論でのべた多面的安全性の実現方法の一つとなる。

5.2. Elate OS

本論で述べた多面的安全性を実現するのに適したシステムの一例として、英国 TAO Systems 社の開発による Elate (一部アスキーとの共同開発) を紹介する。[15]

Elate は VP(Virtual Processor)と呼ばれる仮想マシンをベースに実装されており、以下の特徴を持っている。

(1) Java, C, C++, アセンブラその他の複数プロ

グラム言語のプログラムを VP コードにコンパイルし、共通の仮想マシン上で実行できる。

(2) VP コードはすべての CPU で同一とすることが可能で、すべてのハードウエア環境で共通のバイトコードを利用することができる。

(3) 仮想マシン上にセキュリティ機能を組み込む余地がある。

(4) VP コードはトランスレーションにより高速に実行が可能で、H.263 などのビデオ複号化もリアルタイム実行可能である。

以上のように VP をベースにすべてのソフトウエアを実行することが可能であり、VP 実行機能に基本的なセキュリティ機能を組み込めば、セキュリティの基本構造が実現できる。

Elate をセキュリティ機能のベースとした場合、VP コードが使用する DSP や CPU によらない点がメリットとなる。サービス毎に提供されるセキュリティに関連したバイトコードの種類が増えれば、検証作業も比例して増え、またバイトコード 1 種類あたりの利用数が少ない分信頼性度も下がる。すべての言語、CPU で共通のバイトコードが使用できるという Elate の特徴は、間接的にではあるが多面的安全性を実現する上で大きな利点になる。

また、Elate は C 言語、Java を共通の枠組みで扱えるという点も、既存のソフトウエア資産を活用できるという点で大きな利点である。

ただし現状で Elate が本論で示した要求項目に対応しているわけではない。Elate の開発元である英国 Tao 社は優れた暗号技術を有しており、(株)アスキーは今後英国 Tao 社と協力して Elate のセキュリティ技術の拡充を進めていく方針である。

6. まとめ

将来の情報家電機器の普及に備えて、サービスの外部からの保護以外の多面的安全性について論じた。またその技術的側面を考察し、OPIMA や Elate の多面的安全性に向く特徴を紹介した。

謝辞:本研究を進めるにあたり、勤務先のアスキーの方々に多大なご支援を頂いた。謹んで感謝の意を表したい。

1) 郵政省:"地上デジタルＴＶ放送方式について電気通信技術審議会から答申", http://www.mpt.go.jp/pressrelease/japanese/housou/990524j701.html(1999)

2) Brad Cox, Superdistribution,Objects as Property on the Electronic Frontier, Addison-Wesley 1996

3) Ryoich Mori and Masaji Kawahara "Superdistribution: An Electronic Infrastructure for the Economy of the Future" 情報処理学会論文誌 Vol38 No7 July 1997

4) 山中喜義、高嶋洋一:「電子透かし技術と著作権保護への適用における課題」情報処理学会 電子化知的財産社会基盤研究グループ 2-10(1997/10/4)

5) MPEG N2197 公開文書(現在非公開) " Overview of MPEG-4 functionalities supported in MPEG-4 Version 2" 1998 年

6) MPEG プレスリリース(1998 年 10 月) http://www.cselt.it/mpeg/atlantic_city/atlantic_city_press.html

7) 金子格：「MPEG4 の最新動向」アスキー;OpenNetwork 1997 年 6 月号(要約: http://www.mpeg.rcast.u-tokyo.ac.jp/openmpeg/mpeg4/index.htm/)

8) MPEG N2614 公開文書 IPMP 概要 http://www.cselt.it/mpeg/public/w2614.zip

9) 金子 格、工藤育男、「MPEG-4 における著作権識別管理の標準化動向について」情報処理学会 研究報告 98-EIP-1 pp.75-82

10) 森亮一:「ディジタル情報の無証拠性とその影響-非関所型防御の必要性-」情報処理学会 電子化知的財産社会基盤研究グループ 1-5(1997/6/7)

11) 名和小太郎: デジタル・ミレニアムの到来,丸善,丸善ライブラリー291(1999)

12) マイクロソフト: "マイクロソフトのプライバシーに関する取り組み", http://www.microsoft.com/japan/win98/security/custletter2.htm(1999)

13) 著作権法令研究会「著作権関係法令集」（平成 9 年度版）社団法人著作権センター

14) OPIMA: OPIMA ホームページ, http://www.cselt.it/ufv/leonardo/opima/(1999)

15) アスキー: Elate ホームページ, http://www.ascii.co.jp/tao/(1999)