コンテンツ配信システムのセキュリティ
Secure Content Distribution System

特集

遠藤　直樹
ENDOH Naoki

今日，インターネット，ディジタル圧縮技術，コンピュータネットワーク技術は，音楽の配信ビジネスを成立させる段階まで発展してきた。しかし，音楽などコンテンツの著作権保護は，適正なキャッシュフローを実現するため，従来以上に重い課題になった。この課題の解決のため，情報セキュリティ技術をベースとしたコンテンツ保護・課金メカニズムを導入，時とともにアップグレードしていく必要がある。当社では，セキュアなディジタルコンテンツ配信システムの実現に必要な暗号認証システムなどの情報セキュリティ技術を開発するとともに，認証システムのリニューアル技術も確立した。

Internet, digital compression, and computer network technologies have recently reached the level required for establishing the music distribution business. However, protecting intellectual property rights for contents such as music has become a more important task than ever before, in order to guarantee the appropriate cash flow throughout the entire industry. For this reason, content distribution systems should be equipped with content protection and/or secure billing functions, which could be upgraded over time, based on the most advanced information security technologies.

This paper outlines a secure digital content distribution system and the information security technologies required therein.

1 まえがき

現在のインターネット，および今後現れる次世代インターネットなどを利用して，音楽や映像，テキスト，プログラムなど各種のコンテンツ配信を行うビジネスが発展していくのは確実である。このビジネスはコンテンツ配信システムによって実現されるが，それは，コンテンツデータベース(DB)，課金管理サーバ，利用者のプラットフォーム(例，パソコン)などから成る。ディジタルコンテンツの流通を行わせるときには，そのコンテンツの保護，利用許諾条件の完全な履行のためにセキュリティ機能を明確化し，それにあった技術を導入する必要がある。このとき，セキュリティレベルは，時とともに向上させていく必要性が発生しうる。これは，一般に，セキュリティ機能へのアタックの質も向上していくと見るべきだからである。

2 コンテンツ配信システム

図1は，制作されたディジタルコンテンツが利用者からの要求に基づいて，利用料金と引換えに利用者に配信されるモデルである。

2.1 ネットワークを介した利用者および機器認証

2.1.1 基本機能　正当なハードウェアまたはソフトウェアで構成されているか確認できる(機器認証)。正当な利用者により利用されようとしているか確認できる(利用者認証)。

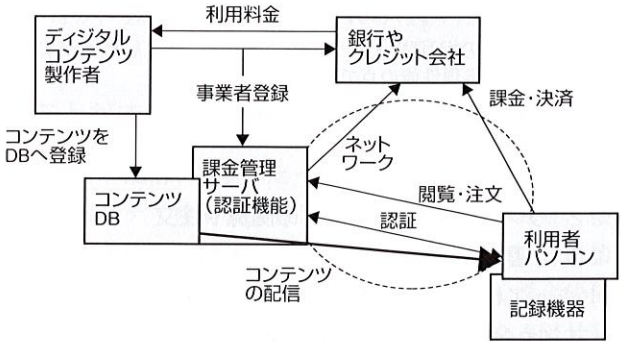


図1．コンテンツ配信システムのモデル　コンテンツDB，課金管理サーバ，利用者などの相互関係を示す。
Content distribution system model

2.1.2 特徴　認証プロトコルとしては，コンテンツのコピー管理情報を扱える必要がある。例えば，パソコンやAV機器向けにDFS(事実上の標準)化されたIEEE 1394 Contents Protection技術(DTCP規格)[1]を，インターネットのTCP/IP(Transmission Control Protocol/Internet Protocol)に適合させることにより実現できる。製造業者にとっては製造上の大きな負担なく共通のソフトウェアやハードウェアを活用した事業展開が可能である。

認証局の階層構造はビジネスの規模，すなわち，加入者数や地域的管理的広がりを考慮しながら，特に処理時間の点で最適化する必要がある。すなわち，利用者の使い勝手

を維持しながらビジネス規模により妥当な投資額のコンテンツ配信システムを明確な基準で設計するべきである。海外など異なる公開鍵インフラ上にある認証局との相互認証も考慮される(図2)。

これにより，国境の壁を越えた事業参入が可能になる。この結果，海外との間で，ディジタルコンテンツの双方向性のあるやり取りも可能でコンテンツDBに蓄積されるコンテンツはバラエティに富んだものになる。利用者の加入のモチベーションを高めることができる。

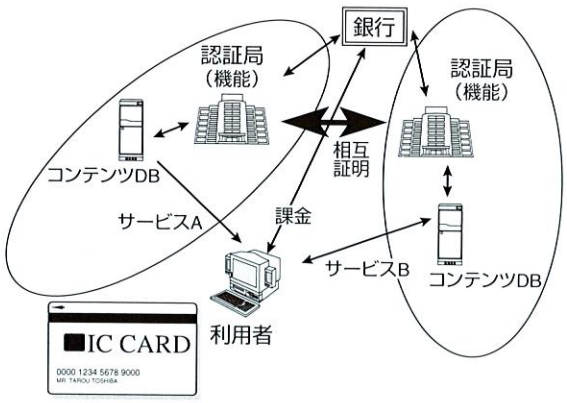


図2．認証局間の相互認証　階層数の少ない認証局機能が実現されないと投資や処理性能の点で不利である。
Mutual authentication between certificate authorities

2.2 ディジタルコンテンツの閲覧や注文

2.2.1 基本機能　コンテンツ配信を受けたい利用者はセキュアにユーザー登録をすることができる。多くの商品(コンテンツ)の中から自分の好みのコンテンツをスムーズに探すことができる。他人を気にしたり不安な気持ちになることなくコンテンツ配信を注文することができる。

2.2.2 特徴　目的の商品にたどりつくまでの検索回数の軽減，利用者が自分の状況をモニタしたい項目(購入履歴など)の研究，I/F(インタフェース)アプリケーションソフトウェアの操作性の問題点，閲覧や注文に伴うプライバシ暴露の阻止などが重要である。I/Fアプリケーションソフトウェアについては，ユーザーのハードウェア環境が自動的にチェックされ，この環境に適合したアプリケーションソフトウェア(適合バージョン)が自動インストールされるような，ユーザーの親和性を向上させる技術が重要となる。

2.3 コンテンツの送受信や蓄積型利用

2.3.1 基本機能　第三者による盗聴が困難。不正コピーが困難。万一，不正コピーされた場合，原因追跡が可能。

2.3.2 特徴　ディジタルコンテンツの配信ビジネスが成功するためには，配信されるディジタルコンテンツが高付加価値なものでなくてはならない。著作権者にとって高付加価値なコンテンツはアタッカーにとっても高付加価値であるため，伝送過程の盗聴(横取り)やいったん利用者のパソコンに受けてからの不正なコピーの生成は魅力的な作業となる。

盗聴を防ぐためには，安全性の高い暗号技術を用いてコンテンツを暗号化した後に利用者に届けることがまず必要である。高セキュリティで高データレート，低トラフィックを実現できる暗号の実現が必要である。一方，暗号の安全性とともに，暗号化に用いた鍵(かぎ)のセキュアな伝送が，もうひとつのポイントになる。例えば，楕円曲線暗号に基づく安全で高速な暗号鍵配送(送信側と受信側とでの鍵共有)技術が良い。楕円曲線暗号は安全性については問題ないと考えられるが，一般に，演算量がきわめて大きいため，モンゴメリ演算法を発展させた高速アルゴリズムなどが好ましい。

利用者に届けられ暗号化が復号された高付加価値コンテンツは，通常，情報圧縮のデコーダを通して映像や音声として利用者に提供される。また，パソコンの中のハードディスクやCD-R，さらには記録可能なDVD，SmartMediaのような半導体メディアといった大容量記憶媒体に蓄積されることもある。後者の蓄積される場合では，不正コピーを確実に阻止できるしくみが不可欠である。

万一，不正コピーが実行された場合の追跡手段として，電子すかし技術があることが知られている。だれが不正コピーの実行者であるかを特定することも，今後は必要とされる場合がでてくる。暗号認証技術と電子すかし技術との融合による高機能化，高効率化を図る必要がある。

2.4 コンテンツの利用に関する課金決済

2.4.1 基本機能　課金の対象となる情報，課金の対象となる利用方法を規定できる。他人になりすませない。お金の偽造ができない。

2.4.2 特徴　配信されたディジタルコンテンツが利用者側で利用される形態として，さまざまな場合がある。例えば，別な媒体にコピーして他のパソコン上で再生する場合や，コピー先が文書ファイルや動画ファイルなどであって他のコンテンツと融合して利用されるような場合である。もちろん，一切のコピーを許可しない場合もある。コンテンツは，その許可された利用形態を示す情報(ライセンス情報)と不可分な形で暗号化され伝送されることが必要で，ライセンス情報が改ざんされた場合，コンテンツ自体は利用不能となることが要請される。このような要請を満足するコンテンツ配信フォーマットとそのライセンス情報フォーマット，利用者側でのライセンス情報処理システムとがすべて規定される。

一方，ライセンス情報の示す許可された利用形態は，コ

ンテンツ自体の価値と密接に関連する。許可された利用形態が多様なほどその価値は高いと考えられる。よって，課金においては，与えられたライセンスの内容が密接に関連することになり，結果として，課金はライセンス情報の内容をベースとしたものとなる。課金に用いられる電子マネー方式は，このようにして，デジタルコンテンツそのものの価値と許可された利用形態の価値とを扱える新しい構造になる(図3)。

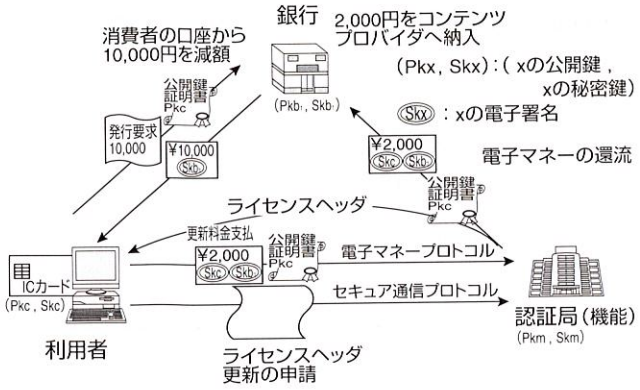


図3．ライセンス情報による課金システム　コンテンツのライセンス情報に依存した課金が必要である。
Billing system based on license information

3 暗号認証リニューアル技術

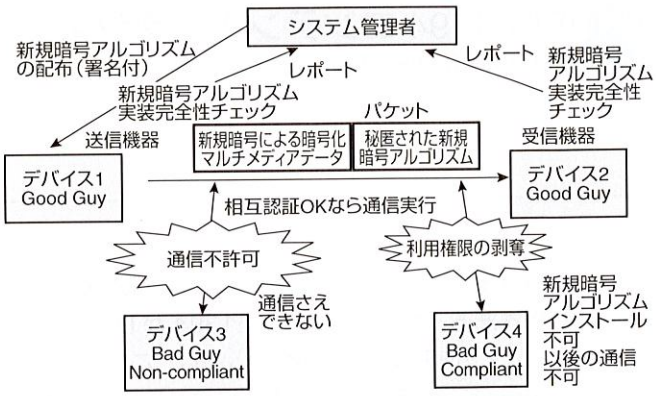
従来型システムは，規格標準化などの理由によりシステムの仕様が一度決まると，それと同時に，システムで使用する暗号認証方式が固定されるため，システムのセキュリティレベルが固定される。さらに，従来のシステムでは，システムの暗号認証方式の更新が一般には容易ではない。

また，コンテンツ配信システムを介して送信する情報は，音楽，映像，テキスト，プログラムなどのマルチメディア情報など多様化しており，情報の価値を考慮した効率的な暗号化ができないのが現状である。

このような理由で，暗号認証システムをリニューアルする技術が今後きわめて重要となる。

この技術は，概略以下のようなしくみを実現する[2]。

暗号認証方式を変更する際，システムの管理機構として，対象となるデバイスを認証し，照合可能な形で秘匿された暗号認証方式を配布する。各デバイス間では相互認証を試み，相手が正当なデバイスと確認されたら所定のパケットによりマルチメディアデータと秘匿された暗号認証アルゴリズムを通信する。この通信にあたり，新規暗号認証方式が正常にインストールされているかが検査される。インストールに失敗している場合，システムの管理機構は再



Good Guy：正当な端末　Bad Guy：認められていない端末
Compliant：ルールに従っている端末

図4．暗号認証リニューアルメカニズム　送りたい情報に適合した，新しい暗号認証アルゴリズムが随時インストールされる。
Cryptographic authentication renewal mechanism

度新規暗号認証方式の配布を試みるなど，必要な措置をとる。各デバイス間で相互認証できないような不正機器は通信が拒絶される。また，認証はできるが破られた秘密を使用している機器では，新規暗号認証方式がインストールできないほか，以後の通信が拒絶される(図4)。

4 あとがき

コンテンツ配信システムとそのセキュアな実現に必要な情報セキュリティ技術を概説した。利用者・機器認証，閲覧や注文のセキュリティ，コンテンツの送受信や蓄積に関する秘匿やコピー管理，ライセンス情報に基づく課金決済がポイントである。さらに，これらのベースとなる暗号認証システムのリニューアル技術が必要となることを指摘した。これら技術の開発に今後とも努力していきたい。

文　献

(1) Digital Transmission Content Protection Specification White Paper, http://www.dtcp.com/
(2) 栃窪孝也，他．“マルチメディア通信に適したリニューアル可能な暗号認証システムの検討”，情報処理学会　第58回全国大会，1999.

遠藤　直樹　ENDOH Naoki
情報・社会システム社 SI技術開発センター 戦略企画担当主幹。情報セキュリティ技術およびその応用システム技術の研究・開発に従事。電子情報通信学会，日本セキュリティマネジメント学会会員。
System Integration Technology Center