6R-03

カプセル化コンテンツ流通システム RightsShell を用いたコンテンツ販売サービス

細見格[†]　中江政行[†]　谷幹也[†]　市山俊治[†]　嶌村忍[††]　佐川健太郎[†††]
[†]日本電気(株)　[††]共同印刷(株)　[†††]リッチピクチャーズ(株)

1. はじめに

インターネットショップ digiGach@(デジガチャ)は、NEC、共同印刷(株)、リッチピクチャーズ(株)の3社が共同で構築した超流通型のデジタルコンテンツ販売サイトであり、現在は http://www.digigacha.com/ で試験運用中である。超流通型のコンテンツ販売システムを構築する上では特に次のような点で配慮が必要となる。

1. **課金の対象はコンテンツ自体ではなくその利用権**
2. **ユーザ端末に暗号技術を用いた専用ソフトが必要**

本稿ではこれらに関わる諸問題と対策について論じる。

2. インターネットショップ digiGach@(デジガチャ)

2.1. digiGach@の概要

digiGach@は、写真や音楽、電子書籍など様々なデジタルコンテンツをオンラインで販売するインターネットショップである。コンテンツ自体は digiGach@サイトからダウンロードするほか、CD-ROM での配布などどのような配布手段を用いても構わない。ただし、NEC 独自のカプセル化コンテンツ流通システム RightsShell [1]を採用することによって各コンテンツはカプセル化(暗号化)してあるため、専用ソフトの RightsShell クライアントでチケットと呼ぶデータをチケットサーバからオンラインで取得しなければ再生することができない(図 2-1)。

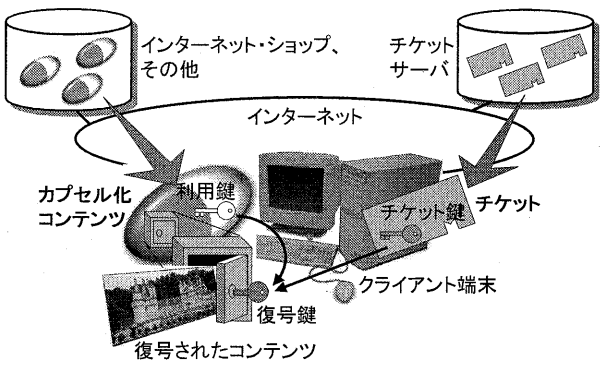

図 2-1　RightsShell によるコンテンツ配信

How To Build A Digital Contents Sales System with RightsShell based on Superdistribution Architecture.
Itaru Hosomi, Masayuki Nakae, Mikiya Tani, Shunji Ichiyama, NEC Corp., Shinobu Shimamura, Kyodo Printing Co.Ltd., Kentaro Sagawa, Rich Pictures Co.Ltd.

このチケットがコンテンツの利用権に相当する。ユーザの端末上で RightsShell クライアント(以下 RSC)を起動しカプセル化されたコンテンツを再生しようとすると、RSC は自動的に適切なチケットを取得し、そのチケットが有料であれば支払い手続きを開始する。支払いはオンライン決済のみである。チケットには有料のものと無料のものがあり、RSC のウインドウ上で選択できる。有料チケットは一度取得すればユーザの端末に保存されるので、支払いが済んだ後は対応するコンテンツを何度でもオフラインで視聴できる。逆にお試し用の無料チケットは毎回オンラインで取得する必要がある。同じコンテンツでも無料チケットを取得した場合と有料チケットを取得した場合とでは視聴できる内容が異なる。

コンテンツの再生にはその復号鍵が必要であり、復号鍵はチケットに含まれるチケット鍵とカプセル化コンテンツに同梱されている利用鍵から生成される(図 2-1)。この一連の処理は全て RSC 内部で行なうため、ユーザは代金支払いを含む正規の手続きを経なければコンテンツを再生することができない。さらに、復号後のコンテンツもその流出を防止する専用ビューアで再生し、他の手段では再生できないようにしている。

2.2. システム構成

図 2-2に digiGach@のシステム概略図を示す。

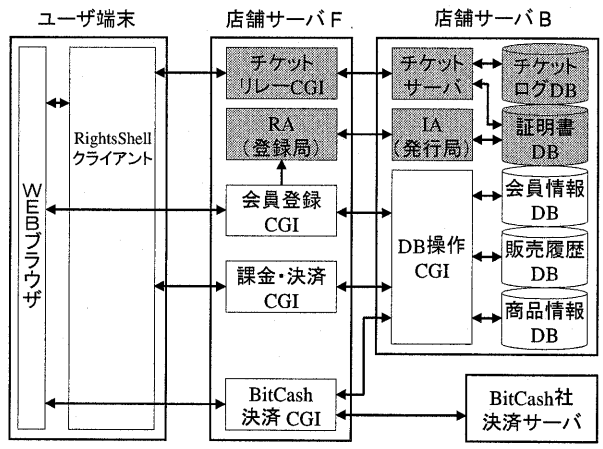

図 2-2　システム概略図 (DB はデータベースの略)

digiGach@はインターネット上に公開したフロントエンド・サーバ(店舗サーバF)と店舗サーバFからのアクセスのみを受け付けるバックエンド・サーバ(店舗サーバB)から成る。ただし、図 2-2のグレーのコンポーネント群はRightsShellのチケット配信とPKIに関する部分であり、厳密には店舗サーバとは独立した機能である。

3. 利用権の販売

3.1. 現在の決済サービスの仕組みと導入方法

現在のdigiGach@はBitCash[2]というプリペイドカード型のオンライン決済サービスに対応している。オンライン決済を導入するには、一般に店舗サーバ上に各々専用のバイナリプログラムを組み込む必要がある。また、従来の多くのインターネットショップでは決済が完了すると商品がダウンロード可能になったり商品発送や領収書などに関する通知が送信されるが、digiGach@では取得したチケットを使用可能にするための特別なデータをRSCに送信する必要がある。さらに、このデータは不正防止のため各チケットとユーザに対して一意かつ偽造困難という要件を満たす必要がある。

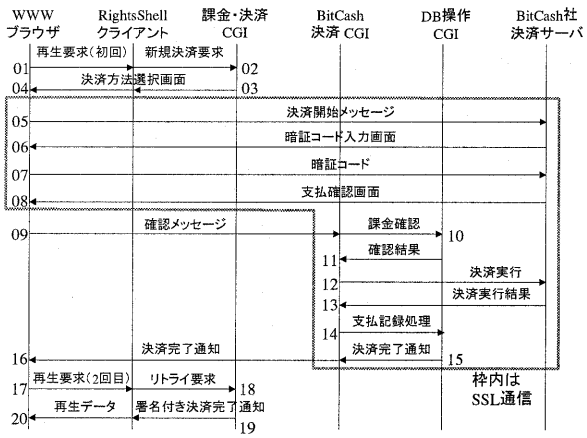

図 3-1 BitCash決済処理フロー

図3-1はdigiGach@における決済処理の流れを示した図である。決済完了後に、店舗サーバからの偽造防止用デジタル署名付き決済完了通知(19)をRSCが受信することでチケットが利用可能となり、コンテンツが復号・再生される(20)。決済完了通知は以下のような情報を含み、その一意性を保証している。

取引ID, チケットID, 決済額, 店舗サーバ名, 発行日時

図中のグレーの枠内はSSL(HTTPS)で通信しており、BitCash以外の決済サービスを用いる場合にはこの部分が置き換わる。即ち、RSCが関わる決済の初期段階(01～04)と最終段階(17～20)での処理は決済サービスの種類に依存しないため、店舗サーバ側CGIの追加・変更のみで他の決済サービスにも対応できる。

3.2. 運用時の問題と対処策

図3-1からも分かるように決済処理は多くの過程を要するが、その途中で何らかの障害が発生する可能性は十分にある。特に、決済サーバでの処理は完了しているが店舗サーバやユーザ端末で署名付き決済完了通知が得られない場合、即ち図 3-1で13～19のいずれかのメッセージが正しく受信されなかった場合、料金の引き落としや請求はあるがコンテンツは再生されない。

この問題に対してdigiGach@では、決済手続きの開始時に過去の決済処理の履歴(図 2-2の販売履歴DB)を参照し、有効期限内に同じユーザと商品に関する記録があれば以降の決済処理をパスして署名付き決済完了通知を発行するようにしている。これによってコンテンツ再生のリトライに対する二重課金を防いでいる。

4. 暗号技術利用製品の配布に関する制約

RSCは基本的にオンラインで配布しているが、標準的なPKIに基づくユーザ認証を行なうために輸出規制対象となる暗号技術を実装している。しかし、インターネットでアクセスしてくるユーザが国内居住者か否かを厳密に判断することは困難である。

この問題に対してdigiGach@では、インターネットでRSCを配布する際に、店舗サイト上の注意書きに対するユーザの同意とアクセス元ドメイン名の制限を以て、配布先を日本国居住者に限定する手段としている。

5. おわりに

超流通型のデジタルコンテンツ販売システムについて、主に決済機構に関する実装と運用上の問題および対処策を述べた。決済処理の信頼性や輸出規制への対応については更なる強化が必要と考えており、今後も検討と改良を進めていく。

参考文献

[1] 中江,他:ユーザ要求に適合したサービスを提供するカプセル化コンテンツ, 情処研報 EIP-3, pp.79-86, 1998.

[2] http://www.bitcash.co.jp/