利用期限付きデジタルコンテンツ利用システムのための通信と同期的処理

古井陽之助*，五百蔵重典*，渡邊信彦**，速水治夫*
*神奈川工科大学, **NTT エレクトロニクス

Communication and Synchronization Processes for a Time-Limited Digital Content Providing System

Younosuke Furui*, Shigenori Ioroi*, Nobuhiko Watanabe**, Haruo Hayami*
*Kanagawa Institute of Technology, **NTT Electronics Corporation

1. はじめに

本稿は，利用者や利用期間が限定されたデジタルコンテンツを，インターネットを介して配布するための仕組みについて述べるものである．

PC 等の高性能化や World-Wide Web に代表される情報基盤の普及を背景に，動画像，音楽，電子化された書籍などのデジタルコンテンツの流通・販売が広く行われている．しかし，デジタルコンテンツは複製が容易であるために，不正な複製による著作権や肖像権の侵害が社会問題として関心を集めており，また未公表の技術資料や個人情報などの機密を保持する上でも危険が伴いやすい．

そこで本研究では，デジタルコンテンツについて利用者の範囲や利用期間を制限することのできるシステムの開発を進めている[1]．このような制限を確実に行うためには，利用者を識別したり利用期間を制限したりする処理への不正な干渉を排する仕組みが必要である．本研究では，時計機能や暗号処理機能などを IC チップに封じ込め，その耐タンパ性によって不正な干渉に抗するという仕組みを考えた．今日広く普及している IC カードや携帯電話などに内蔵された IC チップはこのような機能を内蔵しないが，昨今における技術の発展の速さを考慮して，このような IC チップが数年後には（実際に普及するかどうかは別のこととして）実用化できるものと仮定した．本稿では，そのような IC チップを含めてどのような仕組みがあれば本研究の目標を達成できるかを検討した．

なお，このようなシステムの応用例としては次のようなものが考えられる．

図書館的な共同利用

従来から人間社会において著作物を活用する形態の一つとして図書館がある．例えば国や地方自治体の図書館や大学付属の図書館などでは，書籍・新聞・雑誌・ビデオテープ・CD などを取り揃え，地域住民や学生・教員に期限付きで貸し出すことで文化の発展に寄与する．デジタルコンテンツについてもこのようなサービスを実現するためには，貸し出し期限を過ぎたコンテンツは確実に返却されることや，コンテンツごとの同時に利用されている部数が所定の上限を超えないことなどの保証が不可欠である．

部外秘書類の配布

発売前の製品情報，未発表の発明，顧客の個人情報など，部外秘の情報が記載された書類の取り扱いには注意を要する．このような書類については，限定された範囲の関係者にのみ配布するように，また場合によっては所定の期限が来たら回収するようにする必要がある．このような書類の取り扱いには本システムが応用可能であると考える．

教育機関における教材の配布

学校教育や社員研修などの授業では，機密保持のためや出席への動機付けのために，授業に出席した人々にのみ資料を配布する場合がありうる．また，場合によっては所定の期間が終了したら資料を回収する必要がある．このような書類の取り扱いには本システムが応用可能であると考える．

本稿では特に，図書館のように利用期間や同時に利用可能な数に制限を設けた上でコンテンツを共同利用に供するサービスをインターネット上で実現する場合を主な応用として想定し，その実現方法を技術的に検討した．本稿の構成は次の通りである．まず取り組むべき課題を 2 章で明らかにする．次にシステム設計において検討した諸事項を 3 章で述べ，これに基づいて定めた通信プロトコルを 4 章で説明する．5 章で総括する．

2. 課題

本研究では，デジタルコンテンツ（以下，単に**コンテンツ**）の所有者・管理者（以下，**権利者**）の権利と，コンテンツの利用者（以下，単に**利用者**）の利益を守ることを目指す．そこで，これを実現するシステムの要件を次のように定めた．これらのうち，要件(1)(2)(3)によって権利者の権利を，また要件(3)(4)によって利用者の利益を守る．これらの要件を満たす方式は具体的にどのようなものであるかが本稿の扱う課題である．

*(1) 所定の利用者のみがコンテンツを利用できること．*各利用者を識別し，所定の利用者にしかコンテンツを配布しないようにし，事故や不正な方法などによってそれ以外の人物にコンテンツが渡らないようにする方法が必要である．正規の利用者による不正な行為が権利者の権利を損なうような場合についても対策を講じなければならないことに注意する．

*(2) コンテンツの同時利用可能な数の上限および利用期限が守られること．*コンテンツごとの同時に利用されている数（**同時利用数**）が所定の上限を越えないように，また所定の利用期限を過ぎたコンテンツは閲覧できないようにする．ただし，利用期限前であっても利用者が不要になったコンテンツの利用を自主的に停止できるようにする．さらに，利用期限や現在日時を偽るための不正な行為にも対策を講じる．

*(3) コンテンツの同一性が守られること．*コンテンツが利用者に渡るまでの経路において不正に改変されることの無いようにしなければならない．これには二つの意味がある．一つは，コンテンツを改変する権利は権利者側に属するので，その侵害を防ぐこと．もう一つは，利用者の希望するコンテン

ツが確実に利用者に渡るようにすること．後者は，偽装により不正なコンテンツが配布されるような場合の対策も含む．

*(4) 利用者がどこにいてもコンテンツの利用が可能であること．*権利者の利益を損なわない限りにおいて，すなわち前出の要件(1)(2)(3)に反しない限りにおいて，利用者がコンテンツを様々な場面で利用できるようにする．例えば，利用者が移動などによりコンピューティング環境を切り替えた場合や，モバイル環境を使っている場合などにも対応する．

3. システムの設計

3.1. コンテンツ利用の基本的な流れ

本研究において想定した，コンテンツを利用する際の基本的な流れを図 1 に示す．まずコンテンツを共同利用に供するためのサーバ（以下，**配布サーバ**）をネットワーク上に用意し，これに各種のコンテンツを置く．配布サーバではコンテンツごとに同時利用数の上限が設定される．利用者があるコンテンツを入手するためには，ネットワークを介して自分の PC 等(以下,**利用者 PC**)を配布サーバに接続して要求を送る．配布サーバは，まずその時点におけるコンテンツの同時利用数を調べ,もしそれが上限に達していたら利用者 PC にエラーを返す．同時利用数がまだ上限に達していなければ，配布サーバは利用期限を設定し,コンテンツとともに利用者 PC に送信する．これは通常の図書館での貸出処理に相当する．利用者 PC では,利用期限までは専用の閲覧ソフトウェア等(以下,**閲覧ソフト**）を使ってそのコンテンツを利用することができる．利用期限を過ぎるか，利用者が自主的にコンテンツの利用を止めてその旨を配布サーバに通知すると，そのコンテンツは利用できなくなる．これは通常の図書館での返却処理に相当する．

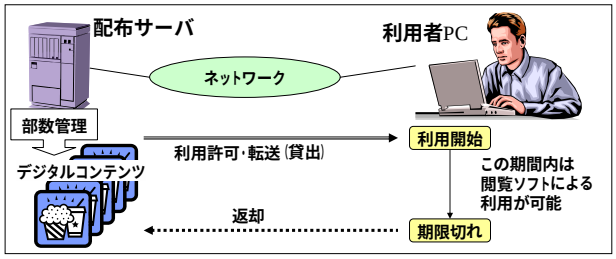

図 1: コンテンツ利用の基本的な流れ

3.2. 技術的な検討

本システムの技術的な詳細を決定していくにあたって，次に挙げるような事項をそれぞれ検討した．

(a) 第 3 者による覗き見・不正な複製の防止

配布サーバ - 利用者 PC 間の通信が覗き見られることや,利用者 PC に受信されたコンテンツが複製されて不正に利用されることを防がなくてはならない．

そこで，配布サーバは共通鍵方式による**コンテンツ暗号鍵**を作り,これでコンテンツを暗号化した上で利用者 PC に送る．利用者 PC ではコンテンツを暗号化された状態で保存するようにすれば，第 3 者がこれだけを複製しても利用することはできない．また，このコンテンツ暗号鍵自体は，利用者の公開鍵で暗号化された状態で利用者 PC に送られ,利用者の秘密鍵を持つ者すなわち利用者のみが復号化できる．

(b) 第 3 者によるなりすましの防止

正規の利用者になりすますことでコンテンツを入手したり,配布サーバになりすますことで利用者に偽のコンテンツを渡したりといった不正を防がなくてはならない．

そこで，配布サーバと利用者はともに公開鍵方式による電子署名を用いることにして，両者間で送受信されるデータには必ず各々の秘密鍵による署名を付けるようにする．なお,これらの電子署名を確認するために必要な公開鍵は，データ送受信に先立って交換しておく必要がある．この交換そのものがなりすましの危険に晒されることがあってはならない．そこで，配布サーバと利用者はネットワークを介さない安全な方法で事前に公開鍵を交換するようにする．

(c) 復号化されたコンテンツの不正な複製の防止

利用者 PC 側でいったん復号化されたコンテンツが,正規の利用者によって不正に複製されたり正規の利用者以外の人物によって利用されたりすることを防がなくてはならない．厳密にはこれは不可能と言って良いが，容易には複製されないように障壁を設けることはできると考える．そのための工夫としては，コンテンツの復号化は必要に応じて適当な大きさの部分ごとに行われるようにしてコンテンツ全体が一度に復号化されないようにする，コンテンツに電子透かしを入れて不正な複製を検出しやすくする，などが考えられる．

(d) 暗号鍵の漏洩・改ざんの防止

(a)(b)で述べたコンテンツ暗号鍵・利用者の秘密鍵・配布サーバの公開鍵といった鍵を利用者側で記憶する必要がある．これらの鍵が漏洩したり改ざんされたりすることを防がなくてはならない．

そこで，これらの鍵は耐タンパ性を持つデバイスの中に記憶するようにする．本研究ではこのようなデバイスとして IC チップ内蔵の IC カードや情報端末など（本稿では単に **IC カード**と表記）を想定する．また，暗号処理の際に IC カードからこれらの鍵をいちいち取り出すのでは漏洩・改ざんの防止は望めないので,暗号処理機能もまた IC カードに内蔵されるものとする．つまり，配布サーバから暗号化された状態で送られたコンテンツ暗号鍵は，IC カード内で復号化されてそのまま IC カード内に記憶される．コンテンツもまた IC カード内で復号化される．

(e) 通信障害への対策

ネットワークの不調などのために通信障害が起きても，最低限のこととして権利者の権利を守るため，処理の順序に注意を払う．

例えば，配布サーバから利用者への貸出処理においては,まず配布サーバ側から IC カードに必要な情報を送信し，IC カードからの Ack を確認した上でそれらを保存する（後の図 2 を参照）．このような順序で処理すれば，仮に通信障害のために途中で送受信が途切れても，配布サーバが把握しないまま IC カード側で利用できたり,逆に配布サーバが許可したにも拘らず IC カード側では利用できなかったりということは起こらない．

また返却処理においては,まず IC カード側で各情報を無効化した上で,それを配布サーバに通知する(後の図 5 を参照)．このような順序で処理すれば，仮に通信障害のために通知が途切れても,配布サーバが把握しないまま IC カード側ではコ

ンテンツを復号化可能であり続けるということは無い.

(f)　利用期限後の確実な利用停止

所定の利用期限を過ぎたコンテンツは確実に利用できなくなるようにしなければならない．そのために利用者側では，現在時刻が利用期限より後ならば復号化処理できないようにする必要がある．ここで，時計を意図的に遅らせることによってコンテンツを利用し続けるような不正行為についても対策が必要である.

そこで,本研究で想定する IC カードは時計機能をも内蔵するものとする.前述の通りコンテンツの復号化機能は IC カード内にあるが,この機能は IC カード内にある時計を参照して,コンテンツの利用期限が過ぎていれば復号化は行わないようにする．この方法の利点は，IC カードの耐タンパ性により時計が不正な操作から守られるので,配布サーバと IC カードは同期的な処理のために時計を信頼することができ，ネットワーク接続による同期を要しなくなる点である.利用者 PC がモバイルなどのためスタンドアロン状態で使用されていても，IC カードは期限切れによる利用停止処理を確実に行うことができ，また配布サーバはそれを把握することができる.

(g)　利用者の移動や携帯性への配慮

前述の通り，コンテンツは暗号化された状態でダウンロードされ，コンテンツ暗号鍵を持つ利用者以外は復号化・利用できない．したがって，暗号化された状態のコンテンツがいくら複製されても権利者の権利は損なわれない．そこで，コンテンツは利用期限前であれば何度でもダウンロードできるようにする.利用者は，出張先の PC など普段使用しないコンピューティング環境でも，利用許可処理を行った際に使った IC カードを携帯していればコンテンツを入手・利用できる.

本項と(d)(f)を合わせて，利用者が普段のコンピューティング環境から移動した場合や，モバイル環境にある場合の利便性を確保する．利用者が必ず携帯しなければならないのは IC カードのみであり，特定の PC を使い続ける必要は無い。コンテンツを入手するためにはいったんは配布サーバにネットワーク接続しなければならないが，そのコンテンツの復号化や期限切れによる利用停止処理のためにはネットワークは不要である.

3.3.　課題への解答

本システムの方式は，2 章において挙げた要件(1)～(4)を次のようにして満足する.

(1) 配布サーバと利用者の IC カードは事前に互いの公開鍵を交換して，通信時には相手の公開鍵で電子署名を確認するので，なりすましによって通信を覗き見られることは無い.コンテンツは配布サーバによって暗号化された状態で利用者 PC にダウンロードされ，利用の際にのみ復号化されるので,正規の利用者以外は利用できない．利用者が持たなければならないコンテンツ暗号鍵・利用者の秘密鍵・配布サーバの公開鍵・暗号処理機能はいずれも IC カード内に置かれるので,IC カードの耐タンパ性によって漏洩や改ざんから守られる.

(2) 配布サーバは各コンテンツの同時利用数を把握しており,コンテンツの利用が所定の上限を超えて許可されることを防ぐ.利用者の持つ IC カードは時計を内蔵して,利用期限を過ぎたコンテンツは復号化しないので,配布サーバと IC カードは期限切れによる利用停止処理を同期的に行うことができる.ただし利用期限より前であっても，利用者は自主的にコンテンツの利用を止めて配布サーバに通知することができる.

(3) (1)と同様に電子署名と暗号化によりコンテンツの覗き見や改変は防がれるので，コンテンツの同一性は守られる.

(4) 利用者は，IC カードを持ってさえいれば，利用期限前のコンテンツを配布サーバから何度でも入手できるので，出張等で移動してもその移動先でコンテンツを入手し直すことができる.コンテンツの利用期限確認と復号化は IC カードによってのみ行われるので，コンテンツを利用し続けるためにはネットワーク接続を要しない.

4.　通信プロトコル

本システムの技術的な要点は IC カードと通信プロトコルにある．このうち IC カードについては論文[1]に譲る．本稿では通信プロトコルの詳細について述べる.

4.1.　利用者の初期登録

配布サーバと利用者の IC カードはネットワークを介さない安全な方法で事前に公開鍵を交換しておく必要がある．そこで，本システムではこれを，IC カードを利用者に渡すまでに初期登録として行うこととした.この初期登録においては,まず IC カードリーダを使うなどして配布サーバと IC カードを直接的に接続する.次に両者は,それぞれが内部的に生成した公開鍵を，互いの識別情報とともに交換する.

4.2.　コンテンツの利用許可（貸出手続き）

利用者は配布サーバからネットワークを介してコンテンツの利用許可を得ることができる（図 2）.

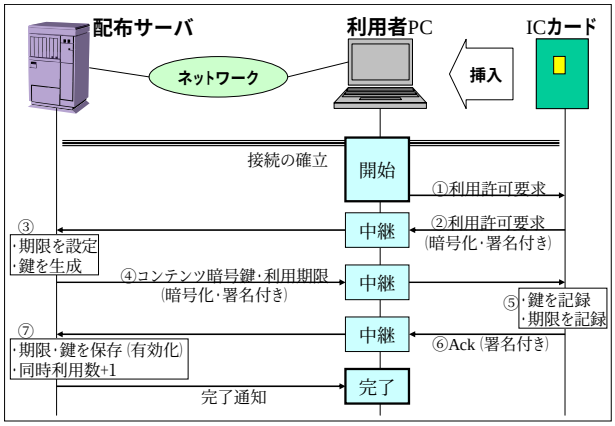

図 2: コンテンツ利用許可フロー図

① 利用者は利用者 PC に IC カードを挿入した状態で閲覧ソフトを実行してコンテンツの利用許可を要求する．閲覧ソフトはネットワークを介して配布サーバとの接続を確立し，IC カードに利用許可要求を送る.

② IC カードは，この利用許可要求に IC カードの秘密鍵による電子署名を付け，配布サーバの公開鍵によって暗号化して，配布サーバに送信する．なお，配布サーバ－IC カード間の通信は閲覧ソフトが中継する.

③ これを受信した配布サーバは，電子署名の確認と復号化

を行った上で，当該コンテンツの利用期限を設定し，またコンテンツ暗号鍵を生成する．なお，この時点ではまだ当該コンテンツの利用は許可されていない．

④ 配布サーバは，生成したデータに配布サーバの秘密鍵による電子署名を付け，IC カードの公開鍵で暗号化して，IC カードに送信する．

⑤ これを受信した IC カードは，電子署名の確認と復号化を行った上で，データを保存する．

⑥ IC カードは配布サーバに Ack を送信する．

⑦ Ack を受信した配布サーバは，利用期限情報とコンテンツ暗号鍵を有効なものとして保存する．この時点で初めて当該コンテンツの利用が許可されたことになる．

4.3. コンテンツの転送（貸出）

所定の利用期限を過ぎるまでは，利用者は何度でも配布サーバからコンテンツをダウンロードすることができる（図 3）．

① 利用者は利用者 PC に IC カードを挿入した状態で閲覧ソフトを実行してコンテンツのダウンロードを要求する．閲覧ソフトは配布サーバとの接続を確立し，IC カードに転送要求を送る．

② IC カードは配布サーバに転送要求を送信する．

③ これを受信した配布サーバは，4.2 で設定された利用期限を過ぎていないことを確認し，また 4.2 で生成されたコンテンツ暗号鍵でコンテンツを暗号化する．

④ 配布サーバは暗号化された状態のコンテンツを閲覧ソフトに送信する．閲覧ソフトは受信したコンテンツを保存する．なお，この時点ではコンテンツはまだ復号化されていない．

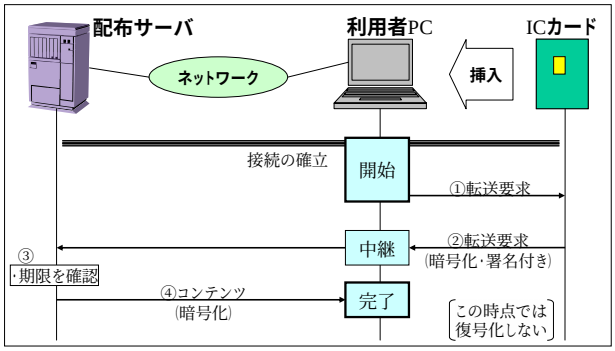

図 3: コンテンツ転送フロー図

4.4. コンテンツの復号化と期限切れによる利用停止（返却）

所定の利用期限を過ぎるまでは，利用者は閲覧ソフトを使ってそのコンテンツを利用することができる（図 4）．

① 利用者は利用者 PC に IC カードを挿入した状態で閲覧ソフトを実行してコンテンツの利用を要求する．閲覧ソフトは IC カードにコンテンツの復号化要求を送る．

② IC カードは，内蔵時計に照らしてコンテンツの利用期限が過ぎていないことを確認した上で，コンテンツの復号化を行う．

③ IC カードは復号化の結果を閲覧ソフトに返す．

④ 所定の利用期限を過ぎると，配布サーバではそのコンテンツは返却されたものとして，コンテンツ暗号鍵を無効にするなどの処理を行う．

⑤～⑦ 閲覧ソフトが IC カードにコンテンツの復号化要求を送っても，IC カードは復号化を行わずエラーを返す．

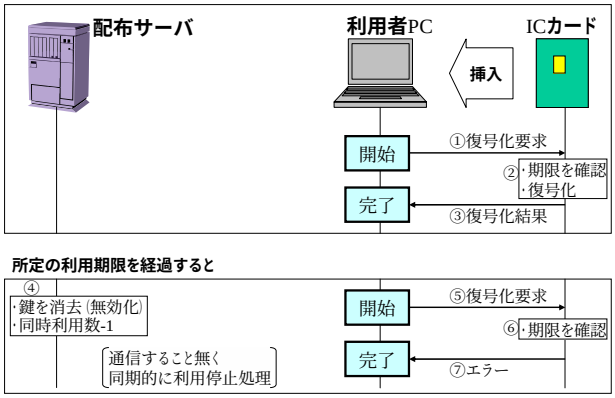

図 4: コンテンツ復号化フロー図

4.5. コンテンツの自主的な利用停止（返却）

利用期限より前であっても，利用者は自主的にコンテンツの利用を停止することができる（図 5）．

① 利用者は利用者 PC に IC カードを挿入した状態で閲覧ソフトを実行してコンテンツの利用停止を要求する．閲覧ソフトは配布サーバとの接続を確立し，IC カードに利用停止要求を送る．

② IC カードは記録しているコンテンツ暗号鍵と利用期限情報を消去する．

③ IC カードは配布サーバに利用停止要求を送信する．

④ これを受信した配布サーバは，コンテンツ暗号鍵を無効にするなどの処理を行う．

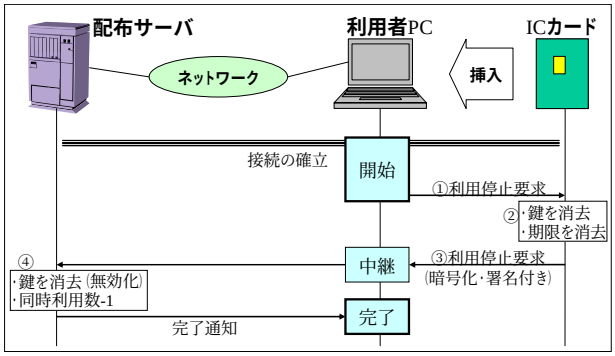

図 5: コンテンツ利用停止フロー図

5. おわりに

本稿は，利用者や利用期間を制限しつつインターネットを介してデジタルコンテンツを配布するためのシステムについて，その要件，設計方針を論じ，また通信プロトコルを中心に具体的な仕組みを述べた．時計や暗号処理などの機能を内蔵する IC カードを含め，実装・評価を行うことが今後の課題である．

参考文献

[1] 五百蔵重典，古井陽之助，原大介，速水治夫：時間管理機能を有する IC カードを用いたデジタルコンテンツの図書館的共同利用サービスの提案．マルチメディア，分散，協調とモバイル（DICOMO2005）シンポジウム．(発表予定)