情 報 メ デ ィ ア 36－5
電子化知的財産・社会基盤 7－5
（2000．1．29）

著作権保護に応用される暗号技術

申吉浩
富士ゼロックス株式会社

本稿は、技術及びシステムの観点から、デジタル著作物の著作権保護に関して述べることを目的とする。特に、デジタル著作物へのアクセス制御を目的とする著作権保護システムに議論の焦点を当てる。デジタル著作物へのアクセス制御は、データ保護・著作権管理・アクセス資格認証の三機能から構成される。この内、アクセス資格の認証機能を提供するシステムをプラットフォームとして実現することでコストメリットを期待することが可能であり、デジタル著作物の流通の促進に大きく寄与するものと考えられる。本稿は、アクセス資格認証システムが満足すべき、セキュリティ上、アーキテクチャ上の要件を整理するとともに、システムの実例として、富士ゼロックスのアクセスチケットシステムを紹介する。

Application of cryptographic technologies to the protection of intellectual property rights

Kilho Shin
Fuji Xerox Co., Ltd.

This paper discusses those systems which aim to augment access control to digital works for the protection of intellectual property rights of the digital. The function of the access control comprises three sub-functions of protection of data, rights management and authentication of access rights. In particular, implementation of the sub-function of the authentication of access rights as a platform system would expectedly accelerate free and fair distribution of digital works in a worldwide scale. This paper presents several requirements from security and architecture points of view which such a platform system should satisfy. Also, as an example, Access Ticket System by Fuji Xerox is briefly illustrated.

1. はじめに

インターネットが、一部研究者にとっての研究素材や単なるメールシステムという役割から脱却し、万人に開放された情報網インフラとしてその真価を発揮するには、WWW (World Wide Web)の登場をまたなければならなかった。当初、WWWは学術情報の流通手段として出発したが、その商業的価値は entrepreneur の関心の埒外に留め措かれるにはあまりに魅力的であった。Electronic Commerce の登場は、インターネット上で流通するデジタル著作物の取り扱い、とりわけ、その著作権の保護・遵守の問題に、新たな重要性とともに多様性を付け加えつつある。著作権の保護はデジタル著作物を商品とするビジネスにとっての大前提であり、また、現実の商習慣や流通構造を反映させることでデジタル著作物の著作権の取り扱いは飛躍的に多様かつ複雑になるからである。

本稿では、技術及びシステムの観点から、デジタル著作物の著作権保護に関して述べる。特に、デジタル著作物へのアクセスを制御することにより、著作者の許諾を超えてデジタル著作物が濫用されることを防止するシステムに議論の焦点を当てる。

本稿は以下の構成をとる。まず、デジタル著作物の著作権の保護・遵守を目的としたシステム的方法論として、デジタル著作物へのアクセス制御と、不正アクセスに対する追跡の二つがあることを見る。次いで、アクセス制御を目的とした場合、データの保護・著作権管理・アクセス資格の認証の三つの機能がシステムに要求されることを見る。この内、データ保護と著作権管理が、デジタル著作物の種別や価値などに応じて、適用する技術や実施の様態の選択が行われるのとは対照的に、アクセス資格の認証の機能はプラットフォームとして共通化することができる。本稿では、アクセス資格の認証のための機能を個別のビジネスやアプリケーションに依存しないプラットフォームの機能として構築することの利点に着目し、当目的に供するシステムが満たすべき要件を、セキュリティとアーキテクチャの二つの観点から整理する。最後に、このようなプラットフォームシステムの一例として、富士ゼロックスが開発したアクセスチケット™システムを紹介する。

2. デジタル著作物の著作権保護への二つのアプローチ

概観すると、デジタル著作物の著作権保護には、デジタル著作物への不正アクセスを事前に防止することを目的とするアプローチと、不正アクセスを追跡する機能を実現することで抑止効果を狙うアプローチの二つがある。

2.1. デジタル著作物へのアクセス制御

アクセス資格を有する利用者が許諾された内容のアクセスのみを行い得ることを保証するために、デジタル著作物へのアクセスをシステムによって制御することを狙いとする。

デジタル著作物へのアクセス資格は、著作者（または、その代理人）によってデジタル著作物の利用者に対して授与され、利用者がデジタル著作物を利用する際に必ず確認される。このアクセス資格の授与から確認までの機能を提供するシステムを構築することが、このアプローチの目標である。成り済ましやハッキングといった攻撃に対して適切な安全性を確保するために、暗号技術・セキュリティ技術・耐タンパー（ソフトウェア）技術[1]がシステム構築に当たって駆使される。

2.2. デジタル著作物への不正アクセスの追跡

デジタル著作物への不正なアクセスが行われた場合、事後(after-the-fact)に、不正行為者と不正アクセスの内容とを特定し、追跡する機能を実現することを狙いとする。デジタルウォーターマーク技術を利用して、アクセスに関する情報を除去不可能な形式でデジタルデータに刷り込むことで海賊行為の抑止を狙う方法は、このアプローチの典型的な一例である。

完全なアクセス制御を実現することは技術的に困難であり、また、不正アクセスの追跡による抑止力も決定的であるとは考えられない。そのため、現実のシステムでは、アクセス制御機能とアクセスの追跡機能が併用されることが多い。その意味で、両方のアプローチは等しく重要であるが、本稿ではアクセス制御のアプローチに焦点を当てて議論を進める。

3. デジタル著作物へのアクセス制御を実現する三つの機能

デジタル著作物へのアクセスの制御を目的としたシステムの実例として、米 InterTrust 社の InterRights™ Point[1,2]、米 IBM 社の Cryptolope™[3]、米 Xerox 社の ContentGuard™[4]、富士ゼロックスのアクセスチケット™システム[5,6,7]などを挙げることができる。これらのシステムは、おのおの独自のアーキテクチャに基づいているものの、①データの保護、②著作権管理、③アクセス資格の認証の三機能を有するという点では共通である。

3.1. データの保護

デジタル著作物へのアクセスを制御するためには、まず、システムによるアクセス制御を迂回した不正なアクセスを防止する必要がある。そのために、TLS[8]などの場合と同様、暗号化によるデー

[1] Tamper-resistant (software) technology. Tamper とは改変の意。攻撃者による機密データの窃取やプログラムの改変を防止するように、ハードウェアやソフトウェアを構築する技術。

タの保護が行われる。しかしながら、通信路上でのデータの保全を目的とするTLSなどとは異なり、デジタル著作物の著作権保護の目的には、単にデータを暗号化するだけでは不充分である。デジタル著作物の利用者は仮想的な攻撃者とみなされることから、利用者の手許において暗号化されたデータを安全に復号しレンダリング（表示・再生）するためのセキュアな環境が必要となるのである。

このように、著作権保護を目的としたデータ保護では、デジタル著作物のデータは、配信から利用に到る全ての過程で一貫して保護される必要がある。この特徴を際立たせるために、著作権保護を目的に暗号化されたデジタル著作物を、**デジタルコンテナ**や**カプセル**など、特別な呼称で呼ぶことが多い[1]。コンテナやカプセルは特殊なプログラムによってレンダリングされるが、本稿ではこれらのプログラムを、総じて**セキュアコンテンツプレイヤ**と表現する。

さて、デジタル著作物のデータ保護には、データの種別や価値、利用や流通の形態に応じて、コストとパフォーマンスとを考慮した多様な実施の様態がとられる。例えば、オーディオ・ビデオなどストリーム系のデータの保護には、パフォーマンスの観点からストリーム暗号アルゴリズムが適しているとされ、文書データ・プログラムなどファイルとして取り扱われるデータの保護にはブロック暗号アルゴリズムを用いることが多い。また、インターネットを介してセキュアコンテンツプレイヤを配布するためには、法律で定められた規制値より短い暗号化鍵を用いる必要がある[2]。一方、デジタル著作物の価値が高い場合には、輸出上の制約やパフォーマンスの低下を引き換えにしても、十分に長い鍵を用いて暗号化を行うべきである。

データ保護において要求される実施様態の多様性は、単に暗号アルゴリズムや鍵の選択に止まらず、システムの実装方法にも及ぶ。例えば、MPEGで符号化された映像データの保護には全データの十分の一程度を暗号化すれば十分安全であると言われているのに対し[2]、音声データについて同等の安全性を得るためには全データを暗号化する必要がある。また、利用者の利便を重視するならば、暗号化データの復号はソフトウェアで実行されるべきであるが、高価値のデジタル著作物の保護のためには、利便性を犠牲にしても、セットトップボックスやオーディオ/ビデオボード上などハードウェア上での復号も選択肢に加えられるべきである。

つまり、データの保護に関していえば、デジタル著作物の種別や価値、利用や流通の形態などの適用対象の特性や事情に応じて、コストとパフォーマンスの最適なトレードオフを選択できるよう、システムの設計に自由度が求められるのである。

3.2. 著作権管理

当然のことながら、デジタル著作物毎に著作権の設定は異なる。更に、デジタル著作物を固定したとしても、許諾されるアクセスの内容は利用者毎に異なる。このように、デジタル著作物の著作権やアクセス資格をシステム的に取り扱うためには、デジタル著作物に付随する著作権の設定や、利用者に許諾されるアクセスの内容を、自由度をもって記述する手段が必要となる。本稿では、この手段を提供するための技術を、**著作権管理**(rights management)技術と呼ぶこととする。

著作権管理のための機能は、著作権の設定やアクセス資格内容を記述するための言語仕様の規定と、この規定に従って記述された**アクセス資格記述データ**を解釈する解釈プログラム(interpreter)から構成される。米Xerox社のDigital Property Rights Language™ (DPRL) [9]は、著作権管理のための言語仕様の好個の例である。

著作権管理技術にとって最も重要な評価尺度は、現実世界をどれだけ忠実にモデリングしているかという点にある。前述のDPRLも、米国における出版物の流通形態と著作権に関する法制・商習慣

---

[1] InterRights™ Point では DigiBox、Cryptolope™ では Digital Container、ContentGuard™では Self-Protecting-Document、アクセスチケット™システムではカプセルと呼ばれる。

[2] 原則として、インターネットでダウンロード可能なプログラムには、輸出規制の対象となる暗号技術を使用することは許されない。Wassenaar 条約とそれに準拠する国内法（外為令・貨物等省令）に従えば、慣用暗号で DES56 ビット超、公開鍵暗号で RSA512 ビット相当超の強度を有する暗号技術は、輸出規制の対象とはなる。

の研究から得られたモデルに基づいて設計されている。即ち、データ保護と同様、著作権管理技術もまた、業態や国で異なる著作権の考え方・法制など、適用対象の特性に強く依存するのである。

3.3. アクセス資格の認証

アクセス資格の認証の機能は、デジタル著作物へのアクセス制御を実現する上で中核となる機能であり、次の二つの役割を果たす。

1. 悪意の攻撃者による成り済ましを防ぎ、アクセス資格を有する利用者を確実に認証する[1]。
2. アクセス資格によって許諾されるアクセスの内容の改竄を防ぎ、利用者に許諾されたアクセス資格の内容を確実に認証する。

アクセス資格の認証機能を考える上で最も重要なことは、同機能を具体的なビジネスやアプリケーションに依存しないプラットフォームの機能として構築可能であり、また、そうすることにコストメリットがあるということである。この点が、アクセス資格の認証機能と残りの二つの機能とを区別する本質的な相違点である。少しく具体的に考察してみよう。

その役割から考えて、アクセス資格の認証機能は、利用者を認証するための手段を内包する必要があり、従って、認証のために何らかのメカニズムを利用者に広く配布するコストを払わなければならない。このコストを考えると、アクセス資格の認証機能を個別のアプリケーション毎に構築することは現実的ではない。裏返していえば、アクセス資格の認証機能をプラットフォームとして実現し、複数のアプリケーションが共通に利用することにより、コストメリットが得られるのである。

本稿では、アクセス資格の認証機能をプラットフォームシステムとして実現することに焦点を当てて、以下の議論を進めることとする。

表 1:著作権保護のアプローチ

アプローチ/機能		狙い
不正アクセスの追跡		事後に不正なアクセス内容を追跡することによる抑止効果
デジタル著作物へのアクセス制御	データの保護	アクセス制御を迂回する不正アクセスの防止
	著作権管理	著作権の設定及びアクセス資格の内容の記述と解釈
	アクセス資格の認証	利用者のアクセス資格と許諾されるアクセス内容の認証

3.4. アクセス資格の認証システムのモデル

ここでは、アクセス資格認証機能と他の二つの機能とがどのように協調し、デジタル著作物へのアクセス制御を行うかについて、モデルを提示して説明する。

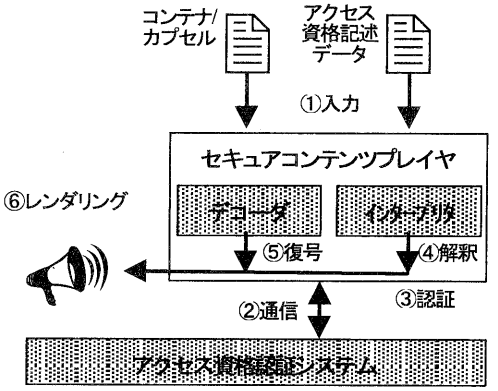
アクセス資格認証のためのシステム（以下、資格認証システム）は、例えば利用者の PC やセットトップボックスにインストールされ、利用者を識別するための情報を内蔵する[2]。一方、暗号化されたデジタル著作物データを復号するデコーダと、アクセス資格内容の記述を解釈するインタープリタとは、同じく利用者の PC やセットトップボックス上で動作するセキュアコンテンツプレイヤ中に設けられるものとする。セキュアコンテンツプレイヤは、デジタル著作物の種別など適用対象の特性を反映して、個別に実装される。

アクセス資格の認証に当たって、セキュアコンテンツプレイヤは、暗号化されたデジタル著作物データとアクセス資格記述データを入力として受け取ると（図 1①）、予め定められたインターフェースを介して資格認証システムと通信する（②）。次いで、資格認証システムとの通信内容から、利用者がアクセスを許諾されている本人であること、アクセス資格記述データが改竄されていないことを確認する（③）。その後、デジタル著作物データの復号をデコーダに、アクセス資格記述の解釈を

[1] ここでの認証では、利用者を「識別」する必要はなく、アクセス資格を有する利用者とそうでない利用者を「区別」できればよい。特に、利用者のプライバシを考える場合、利用者を、「識別することなく区別する」必要がある。

[2] 成り済ましを防ぐため、利用者の識別情報は改変や窃取が不可能となるように安全に保管されなければならない。例えば、同識別情報を、耐タンパー機能を備えたスマートカード中に記録する方法などが考えられる。

図 1:構成モデル



インタープリタに指示し（④⑤）、アクセス資格記述データにおいて許諾されているアクセス内容の範囲内で復号されたデータをレンダリングする（⑥）。

実際のシステムの実施様態は、このモデルと相違していても構わない。例えば、このモデルでは、資格認証システムとセキュアコンテンツプレイヤ間の通信は利用者のローカルな環境で実行されるが、インターネット上のサーバとの通信を含む構成としてもよい。ここでモデルを提示した目的は、あくまでも説明の便宜と読者の理解を図るためである。

4. アクセス資格認証のためのプラットフォームシステムが満たすべき要件と実現への手掛り

以下では、アクセス資格の認証を目的としたプラットフォームシステムについて考察する。特に、システムが満足すべき要件を、セキュリティ及びアーキテクチャの二つの観点から整理する。

4.1. セキュリティの観点からの要件

資格認証システムは、デジタル著作物の著作者、或いは、その利用者の利益を保護するため、以下の五項目のセキュリティ上の要件を満足している必要がある。

4.1.1. 譲渡不可能性 (Non-transferable)

利用者に対して発行されたアクセス資格を、（正当な手続きを踏むことなく）他の利用者に譲渡することが不可能であること。

4.1.2. 偽造不可能性 (Non-forgeable)

アクセス資格の偽造や成り済ましによる不正アクセスが不可能であること。特に、許容されるアクセスの内容を規定するアクセス資格記述データに関して、その偽造や改竄が不可能であること。

譲渡不可能性と偽造不可能性は、著作者の権利、即ち、著作権を保護するために必須の条件となる。一方、次に述べる三項目の要件は、デジタル著作物の利用者の権利を保護することを狙いとする。

4.1.3. 公開検証性 (Open-verifiable)

公開された手続きのみに従って、利用者（或いは、その利益代表者）が発行されたアクセス資格の正当性を検証できること。

著作者（或いは、その代理人）によるアクセス資格の発行と、利用者によるデジタル著作物への実際のアクセスの間には、時間的な隔たりがあるケースがある[1]。そのような場合でも、公開検証性により、利用者（或いは、その利益代表者）は、アクセス資格が正しく発行されたことを任意に確認することが可能となる。特に、アクセス資格記述データの内容を検証できることは重要である。

4.1.4. 否認拒否性 (Non-deniable)

アクセス資格の発行者が発行の事実を否認できないこと。

著作者により発行されたアクセス資格は、前述の公開検証性によって、その正当性を検証することが可能である。更に進んで、否認拒否性は、公開検証性に基づく検証に証拠性を付与することで、著作者との係争において利用者が不当に不利益を蒙ることを防止する。

[1] 利用者がデジタル著作権の定期購読権を購入した場合など。

4.1.5. 匿名性 (Anonymous)

利用者のプライバシの保護が要求される場合、アクセス資格の発行及び認証の過程において、利用者の匿名性が保証されること[1]。

表 2：セキュリティの観点からの要件

要件	内容
譲渡不可能性 (non-transferable)	アクセス資格を他の利用者に不正に譲渡できないこと
偽造不可能性 (non-forgeable)	アクセス資格の偽造や成り済ましができないこと
公開検証性 (open-verifiable)	アクセス資格を公開の手続きに従って検証できること
否認拒否性 (non-deniable)	アクセス資格の発行の事実を否認できないこと
匿名性 (anonymous)	アクセス資格の認証に当たって、利用者の匿名性が守られること

4.2. アーキテクチャの観点からの要件

セキュリティの観点からの要件に加えて、資格認証システムがプラットフォームとして機能するためには、アーキテクチャの観点から以下の二つの要件を満足することが求められる。

4.2.1. 接続性 (Connectivity)

資格認証システムは、複数のセキュアコンテンツプレイヤに対して、共通のインターフェースを介して機能を提供すること。

前述のように、セキュアコンテンツプレイヤは、デジタル著作物の種別など適用対象の特性を反映して個別に実装される。従って、資格認証システムが多様な適用対象において利用されるプラットフォームとなるためには、多様なセキュアコンテンツプレイヤとの接続は必須の要件となる。

接続性の考え方を更に進めて、次のオープンアーキテクチャ性を満足することで、サードパーティデベロッパによるセキュアコンテンツプレイヤの自由な開発が促進され、プラットフォームとして真価を発揮することとなる。

4.2.2. オープンアーキテクチャ性 (Open-architecture design)

セキュアコンテンツプレイヤが資格認証システムと通信する際のインターフェースが、安全性を損なうことなく公開可能であること。

表 3：アーキテクチャの観点からの要件

要件	内容
接続性(connectivity)	セキュアコンテンツプレイヤに対し共通のインターフェースを提供すること
オープンアーキテクチャ性(open-architecture design)	安全性を損なうことなく、インターフェースが公開可能であること

4.3. 公開鍵暗号技術の利用

資格認証システムに求められる上記の要件、特にオープンアーキテクチャ性の要件は、資格認証システムの構築方法に関してある示唆を与える。以下にそれを述べる。

セキュアコンテンツプレイヤは、資格認証システムとの通信内容を判断の材料として、利用者が正当なアクセス資格を有しているか否かを判断し、その後の処理を決定する。この時、資格認証システムがセキュアコンテンツプレイヤに対して判断材料として提供するデータは、資格認証システムのみが知り得る秘密情報を用いて生成されなければならない。そうでなければ、インターフェースが公開されている（オープンアーキテクチャ性）ことから、攻撃者が資格認証システムのエミュレータを任意に作成し、セキュアコンテンツプレイヤをだましてデジタル著作物に自由にアクセスすることが可能となってしまうからである。

更に、資格認証システムとセキュアコンテンツプレイヤとの通信内容から、秘密情報が漏洩することがあってはならない。オープンアーキテクチャ性により、攻撃者は資格認証システムと通信を行う「トロイの木馬」を自由に作成することが可能である。この時、資格認証システムとの通信内容

[1] 著作者側の要求として利用者を特定する必要がある場合もある。

から同システムの秘密情報が漏洩する可能性があると、トロイの木馬で収集した情報をもとに秘密情報を取り出し、資格認証システムのエミュレータが作成される危険があるからである。

このように、**資格認証システムは自分だけが知り得る秘密情報を用いてセキュアコンテンツプレイヤと通信する**が、この時、その**通信内容からは秘密情報を知るための手掛かりが一切得られない**ことが要求される。

この要求は、資格認証システムとセキュアコンテンツプレイヤとの通信プロトコルが、**公開鍵暗号に基づいて設計されるべきである**ことを示唆している。更に、公開検証性や否認拒否性など、その他の要件も同様に、公開鍵暗号が利用されるべきであることを示唆している。公開鍵暗号では、秘密鍵を用いて生成されたデータや公開鍵から秘密鍵を算出することが実質的に不可能であることが保証されている上、自ずと公開検証性や否認拒否性などの性質を備えているからである。

次節では、デジタル著作物毎に固有の公開鍵ペアを割り当て、同公開鍵ペアに属する公開鍵を用いてアクセス資格の認証を行うことを特徴とする、実際のシステムについて説明する。

5. 富士ゼロックスのアクセスチケットシステム

この節では、プラットフォームとして実現された資格認証システムの例として、富士ゼロックスが開発した**アクセスチケット™システム**[6,7,8]を概説する。

アクセスチケットシステムの最も大きな特徴は、**個々のデジタル著作物に固有の公開鍵ペアが割り当てられ、利用者に授与されたアクセス資格の認証は、同鍵ペアの公開鍵を用いて実行される**点にある。これは、公開鍵暗号をデジタル著作物のアクセス資格認証に用いる方法としては、最も直截的な方法である。また、アクセス資格の認証に必要な情報が公開鍵であることから公開検証性を、認証に用いられる公開鍵が利用者にではなくデジタル著作物に帰属することから匿名性の要件を満足することが、直ちに導かれる。実際には、アクセスチケットシステムは、前節で述べた全ての要件を満足する。加えて、アクセスチケットシステムは次の特長を有する。

1. 利用者のアクセス資格は、アクセスチケットと呼ばれるデータとして利用者に対して明示的に発行される。利用者は、発行されたアクセスチケットのコピー・削除を自由に行うことが可能であり、利便性に優れる[1]。
2. アクセスチケットの発行はインターネットを経由して行われるが、アクセスチケットによるアクセス資格の認証は利用者の環境（PC やセットトップボックスなど）でローカルに実行され、ネットワークへの接続を必要としない。
3. 大きな計算量を必要とする公開鍵暗号の計算は必要最小限に止められており、慣用暗号とハッシュ関数を利用することで良好な実行効率を実現している。
4. 認証のためのプロトコルが Ticket Authentication Protocols [7]として規定されていることに加えて、インターネット上でアクセスチケットを発行・受領するためのプロトコルも Ticket Granting Protocols [8]として明確に規定されている。

最後に、図 2 に示す例を用いて、アクセスチケットシステムにおける認証プロトコルについて、技術的な観点から若干詳細な説明を加える。

アクセスチケットシステムの特徴として、与えられたデジタル著作物に対して、固有の公開鍵ペアを割り当てる。この例では、RSA 公開鍵ペア(e, d, n)が割り当てられる。このデジタル著作物へのアクセス資格の認証は、公開鍵(e, n)を用いて実行される一方、後述するように、秘密鍵(d, n)はアクセス資格を表現するアクセスチケットの生成に利用される。また、利用者の環境にインストールされたアクセスチケットシステムは、利用者固有の非衝突性（ハッシュ）関数 $F(x, y, z)$を含む。更に、L

[1] 利用者の識別手段を、携帯性を有するスマートカードなどに実装すれば、なんらかの記憶媒体にアクセスチケットをコピーしてスマートカードとともに携行すれば、利用者は場所を選ばずデジタル著作物を利用することが可能となる。

を利用者に許諾されたアクセス内容を記述するアクセス資格記述データであるとする時、アクセス資格を表現するアクセスチケット *tckt* は次の式で定義される。

$tckt = d - \mathrm{F}(e, n, L) \bmod \lambda(n)$[1]

セキュアコンテンツプレイヤは、リプレイ攻撃を避けるべく、乱数チャレンジ C をアクセスチケットシステムに送り、レスポンス R を受け取る。この時、アクセスチケットシステムが利用者の識別関数である $\mathrm{F}(x, y, z)$を用いて R を計算している場合に限り、次の検査式が成立する[2]。

$(C^{tckt} R)^e = (C^{d-\mathrm{F}(e,n,L,)} C^{\mathrm{F}(e,n,L,)})^e = C^{de} = C \mod n$

ここで、アクセス資格記述データ L が改竄されていたり、差し替えられていると、R が正しい値とはなり得ず、検査式は成立しないことに注意されたい。

セキュアコンテンツプレイヤ		*アクセスチケットシステム*
乱数チャレンジ C を生成	$L, C, (e, n)$ →	
		乱数 k を生成
		DES **鍵** K = **SHA1**(k, L)**を生成**
k を復号		
DES **鍵** K = **SHA1**(k, L)**を計算**		
レスポンス R **を復号**	← k^{π}, **DES**(K, R)	**レスポンス** $R = C^{F(e,n,L)} \bmod n$ **を計算**
		k をプレイヤの公開鍵πで暗号化 k^{π}
$(C^{tckt} R)^e = C \bmod n$ **を検査**		**R を K で暗号化 DES**(K, R)

図 2：アクセスチケットシステムにおける認証プロトコルの一例

6. まとめ

デジタル著作物の著作権を保護する目的で利用者のアクセス資格を認証するシステムは、セキュリティの観点から、**譲渡不可能性・偽造不可能性・公開検証性・否認拒否性・匿名性**の性質を満たしている必要がある。また、資格認証システムをプラットフォームとして実現することで、コストの観点からデジタル著作物の流通を促進することが期待されるが、その実現のためには、**接続性・オープンアーキテクチャ性**の二つの要求を満足しなければならない。富士ゼロックスのアクセスチケットシステムは、これらの要求を満足しつつ、更に、利用者の利便性やパフォーマンスの点においても特長を有している。

参考文献

1. InterTrust Technology Corp.; *A Piece of Tick*; http://www.intertrust.com/media/pdf/tick.pdf
2. O.Sibert, D.Bernstein, D.Wie; *Securing the Content, Not the Wire, for Information Commerce*; http://www.star-lab.com/secure-the-content.html
3. IBM Corp.; *Cryptolope*™; http://www-4.idm.com/software/security/cryptolope
4. Xerox Corp.; *ContentGuard*™, http://www.contentguard.com
5. K.Shin, M.Kyojima; *Secure and efficient schemes to entrust the use of private keys*; IEEE WETICE '99
6. M.Kyojima, K.Shin; *Ticket Authentication Protocols v1.0*, Fuji Xerox technical report, 1999
7. M.Kyojima; *Ticket Granting Protocols v1.0*, Fuji Xerox technical report, 1999
8. T.Dierks, C.Allen; *Transport Layer Security*; RFC 2246
9. Xerox Corp.; *Digital Property Rights Language*™; http://www.contentguard.com/overview/tech_dprl.htm

[1] $\lambda(n)$は剰余環 $\mathbb{Z}/n\mathbb{Z}$ の元の位数の最大値を表す。

[2] この例では、セキュアコンテンツプレイヤを認証する機能も併せて提供している。具体的には、セキュアコンテンツプレイヤの公開鍵πが L 中に記述されており、アクセスチケットシステムはチャレンジ k をこのπで暗号化して、プレイヤに送付する。但し、チャレンジ k に対するレスポンスについては、本稿では記述を省略している。