社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＳＬＤＭ－129／2007－ＥＭＢ－4 (10)
2007／3／16

FPGAの自己動的部分再構成を利用したセキュアなコンテンツ配信システムの構築

堀　洋平† 横山 浩之†† 坂根 広史† 戸田 賢二†

† 独立行政法人 産業技術総合研究所 〒305–8568 茨城県つくば市梅園 1–1–1 中央第 2
†† 株式会社 KDDI 研究所 〒356–8502 埼玉県ふじみ野市大原 2–1–15
E-mail: †{hori.y,hirofumi.sakane,k-toda}@aist.go.jp, ††yokoyama@kddilabs.jp

あらまし FPGAの自己動的部分再構成機能を利用し，ネットワーク上において安全にコンテンツを配信するシステムを構築した．本システムでは，コンテンツ固有の再生回路をサーバからダウンロードし，端末側の回路と組み合わせることで，コンテンツの不正利用を防ぐことができる．また，端末回路の入出力ポートの構成を端末に固有とすることで，回路のインタフェースそのものを認証として利用した．今回，実際にFPGAを部分的に再構成して動画の再生実験を行い，システムの有効性について検証した．

キーワード FPGA，リコンフィギャラブル・コンピューティング，動的部分再構成，コンテンツ保護，デジタル著作権保護 (DRM)

Secure Content Distribution System with Self Run-Time Partial Reconfiguration of an FPGA

Yohei HORI†, Hiroyuki YOKOYAMA††, Hirofumi SAKANE†, and Kenji TODA†

† National Institute of Advanced Industrial Science and Technology (AIST)
Tsukuba Central 2, 1–1–1 Umezono, Tsukuba-shi, Ibaraki 305–8568, Japan
†† KDDI R& D Laboratories, Inc. 2–1–15 Ohara, Fujimino-shi, Saitama 356–8502, Japan
E-mail: †{hori.y,hirofumi.sakane,k-toda}@aist.go.jp, ††yokoyama@kddilabs.jp

Abstract We developed a secure content distribution system exploiting run-time partial reconfigurability of an FPGA. In the system, a user downloads both content and the content-specific circuit from a server to the client terminal. The content is properly played only when the downloaded circuit is correctly combined with the terminal. Since each terminal has unique I/O configuration, the interface of the terminal itself provides a novel authentication mechanism. This paper explains the content protection mechanism of the system, and then demonstrates its feasibility.

Key words FPGA, Reconfigurable Computing, Run-time Partial Reconfiguration, Content Protection, Digital Rights Management (DRM)

1 はじめに

携帯端末やデスクトップコンピュータの高機能化・高性能化と，ネットワークの高速化により，デジタルコンテンツ市場が急速に拡大している．特に，音楽や映像の配信事業の成長は目覚ましい[1],[2]．このような背景から，デジタルコンテンツをインターネット上で安全に配信する必要性が増している．

一方，携帯電話やセット・トップ・ボックスのように，プロセス性能や消費電力に関する制約が厳しい端末においては，リッチコンテンツを再生するために，カスタム化されたハードウェアを用いてシステムを構築する場合が多い．しかし，専用ハードウェアの機能は出荷後に変更することができないため，不具合を修正することや，新たに出現した攻撃手法に対処することなどが難しい．そのため，一度システムに対する攻撃方法が明らかになると，出荷された端末を使用することができなくなる可能性が高い．

このような問題を解決するため，筆者らはField-Programmable Gate Array (FPGA) の部分再構成を利用することで，安全にコンテンツを配信し，かつ新しいネットワーク攻撃の脅威に柔軟に対応できるシステムを構築する方法を提案してきた[3]～[7]．このシステムでは，コンテンツを再生する際に，再生回路の一部をサーバからダウンロードする．ダウンロードされる回路の

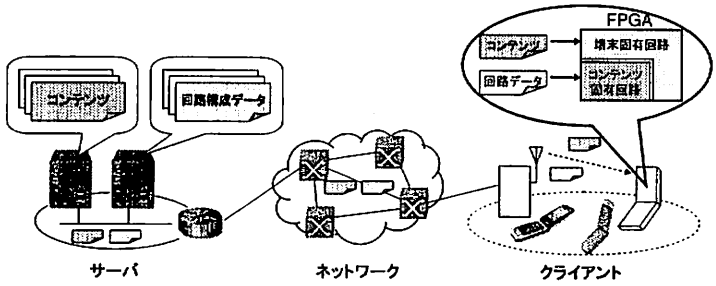

図 1　コンテンツ配信システムの構成

論理や入出力ポートの構成をコンテンツや端末に応じて変えることで，コンテンツが特定の端末上で再生されるようコントロールし，かつ回路機能をアップデートすることができるようになる．今回，FPGA を用いてシステム全体を実装し，実際に自己動的部分再構成を行ってシステムの有効性について検証を行った．

本稿では，まず第 2 章でザイリンクス FPGA における部分再構成の特徴について述べる．第 3 章では，部分再構成を利用したコンテンツ配信システムの概要について説明する．第 4 章では，実際に FPGA 上に実装されたシステムの構成について説明し，第 5 章でこれを用いた動画再生実験の結果について述べる．第 6 章では，実験結果をもとに将来の課題について検討し，第 7 章で本稿についてまとめる．

2　FPGA の動的部分再構成

2.1　動的部分再構成の概要

現在市販されている FPGA の中には，他の部分の演算を止めることなく，特定の部分のみを再構成することのできるものがある．このような再構成を，**動的部分再構成 (Dynamic Partial Reconfiguration, DPR)** と呼ぶ．現在，DPR の機能を有する FPGA には，ザイリンクスの Spartan シリーズ，Virtex シリーズや，アトメルの FPSLIC [8] がある．この中の一部デバイスは，外部回路を使用することなく，自分自身で部分再構成の制御を行う**自己動的部分再構成 (Self DPR)** の機能を有する．本研究はこの Self DPR を利用し，セキュアなコンテンツ配信システムを構築する手法を提案する．本章では，ザイリンクス FPGA における部分再構成の特徴について述べる．

2.2　部分再構成モジュール

ザイリンクス FPGA では，長方形のモジュール単位で部分再構成を行う．このとき，部分再構成の対象となるモジュールを **Partially Reconfigurable Module (PRM)** と呼び，そのモジュールが配置されるデバイス上の領域を **Partially Reconfigurable Region (PRR)** と呼ぶ．PRR は任意の大きさの長方形とすることができる．Virtex-II Pro 以前と Virtex-4 以降のデバイスでは，部分再構成されるフレームが異なる (図 2)．部分再構成フレームについての詳細は，文献 [7] を参照されたい．

2.3　バスマクロ

DPR では，部分再構成後の配線が正しく結線されることを保証する必要がある．ザイリンクス FPGA では，**バスマクロ**と呼ばれるハードマクロを用いてこれを実現する．PRM と固定モジュール，あるいは 2 つの PRM の間の信号は，必ずバスマクロを通らなければならない．バスマクロは，縦 4 個，横 4 個の合計 16 個の Look-up Table (LUT) から構成される配線済みハードマクロである．バスマクロは，左から右，あるいは右から左のどちらか一方向に 8 bit 幅の信号を通過させる．また Virtex-4 に限り，上から下，および下から上方向のバスマクロも存在する．さらに，信号の向きの違いのほか，同期/非同期，イネーブル付き/イネーブルなし，narrow/wide の区別がある (図 3)．

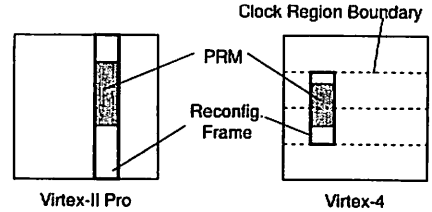

図 2　Xilinx FPGA の部分再構成フレーム

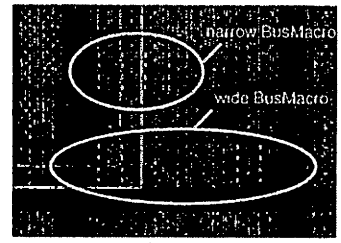

図 3　Xilinx FPGA のバスマクロ

2.4　Internal Configuration Access Port

Virtex II 以降の FPGA には，内部ロジックからコンフィギュレーションメモリにアクセスするための **Internal Configuration Access Port (ICAP)** と呼ばれるプリミティブがある．ICAP を通じてコンフィギュレーションメモリを読み書きすることで，外部制御を必要としない自己部分再構成を行うことができる．

3　コンテンツ配信システムの概要

3.1　システムの構成

図 1 に本システムの構成を示す．システムは，サーバ，クライアント端末，およびそれらを接続するネットワークから構成されている．本システムの特徴は，コンテンツと共に，コンテ

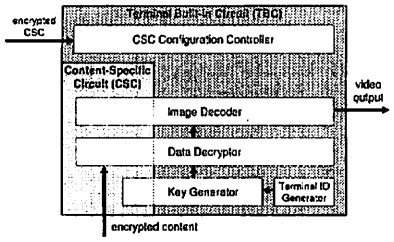

図4 CSC と TBC の実装例

ンツを再生するために必要な回路構成データをダウンロードし，これを端末上で構築することによって，初めてコンテンツを再生することができる点にある．

端末からサーバに対してデジタルコンテンツのダウンロードが要求されると，サーバは，暗号化されたコンテンツを端末が処理するために必要な回路の一部を作成する．この回路を，**コンテンツ固有回路 (Content-Specific Circuit, CSC)** と呼ぶ．CSC の回路情報は暗号化され，コンテンツと共にネットワーク経由で端末に送信される．

CSC は，要求元の端末に用意されている回路と結合することで初めて正しく動作する．この端末上の回路を，**端末固有回路 (Terminal Built-in Circuit, TBC)** と呼ぶ．また，CSC と TBC が正しく結合し，システム全体が意図した通りに動作することを，**インターロックする**という．本システムでは，CSC-TBC のインターロックのメカニズムをコンテンツ保護に利用し，FPGA の動的部分再構成を用いてこれを実現した．

3.1.1 コンテンツ固有回路 (CSC)

CSC には，鍵生成回路，復号回路，デコーダなどの一部分を実装する (図 4)．そのため，正しい CSC が構築されなければ，TBC 側の鍵生成や復号等の機能は正常に動作しない．CSC の内部構造はコンテンツに合わせてカスタマイズ可能であり，復号方式や符合化方式の更新に柔軟に対応できる．

CSC は回路全体のごく一部であるため，回路データのサイズは小さく，再構築にかかる時間を大幅に短縮することができる．そのため，再生途中に頻繁に復号鍵が変わるようなコンテンツでも，FPGA の動的再構成機能を用いることによって，鍵生成回路のみを再構成するような使い方が可能である．

CSC の回路構成データは，認証済の特定端末でのみ復号できるように暗号化して送信されるため，ネットワーク上で盗聴されても，第三者が使用することはできない．また，仮に回路構成データが解読されたとしても，コンテンツの復号鍵そのものを推測するための情報は得られない上，特定の端末と組み合わせないと正常に動作しないため，不正利用や回路の解析が困難である．

3.1.2 端末固有回路 (TBC)

TBC は，鍵生成，復号，デコード等のコンテンツの再生に必要な機能を提供するほか，CSC の再構成の制御を行う．TBC の鍵生成などの機能は，CSC が正しく結合されなければ動作しない．TBC は CSC とのインタフェースを備えているが，その構成は端末ごとに異なる．そのため，他のユーザ向けの CSC を使ってコンテンツを再生することはできない．このように，回路のインタフェースそのものが端末認証の役割を果たしている．

TBC はコンテンツの再生のたびに再構成されることはないが，FPGA 上に実装されているため，必要が生じれば回路構成を変更することは可能である．例えば，コンテンツ保護のフレームワークの更新に追随するために，日，週，月の単位で TBC を変更することで，よりセキュアにシステムを運用することができる．

3.2 インターロックによる保護メカニズム

コンテンツ再生時に CSC を動的に構成し，TBC と結合させる CSC-TBC アーキテクチャは，セキュアな認証のメカニズムを回路的に提供することができる．CSC-TBC がインターロックするには，CSC-TBC 間で以下の条件が全て成立する必要がある．これらの条件を CSC-TBC 間に固有とすることにより，インターロックを認証の手段として利用することができる．

a) 空間的条件

空間的条件とは，CSC-TBC 間の入出力ポートの位置に関する条件である．例えばザイリンクス社の FPGA では，部分再構成モジュールとの通信は，すべてバスマクロを経由しなければならない．もし，バスマクロが正しい場所に配置されていなければ，CSC が再構成された際に，回路全体が正常に動作することはない．

b) 時間的条件

時間的条件とは，送受信される信号のタイミングに関する条件である．例えば，CSC からダミーデータを含む信号が送信され，これを特定のタイミングでサンプリングすることによって正しい情報を取り出すことができるような方法が考えられる．このタイミングを端末に固有とすることで，第三者によって CSC が不正利用される可能性が大幅に減少する．

c) 電気的条件

電気的条件とは，CSC や TBC における信号の電圧や電流等の条件である．CSC と TBS においてこれらが一致するかどうかを，認証の手段として用いることができる．

d) 論理的条件

論理的条件とは，CSC-TBC 間のプロトコルに関する条件である．CSC-TBC 間におけるデータ送受信の手順を端末に固有とすることで，CSC が不正に利用される可能性が大幅に減少する．

これらの条件が成立した上で，さらに既存のチャレンジレスポンス方式などの認証を行い，CSC や端末が正規のものであるか確認することも可能である．

4 システムの実装

CSC-TBC のメカニズムを，ハイビジョン動画像の再生システムに応用した場合を想定してシステムの実装を行った．FPGA の部分書換えを利用することで，専用ハードウェアによる高速な画像処理と，コンテンツに応じた柔軟で粒度の細かな保護機能をセキュアに提供することが可能である．CSC のインタフェースはユーザ端末ごとに異なり，CSC-TBC メカニズムによる端末認証が行われる．CSC の機能は動画像ごとにカスタマ

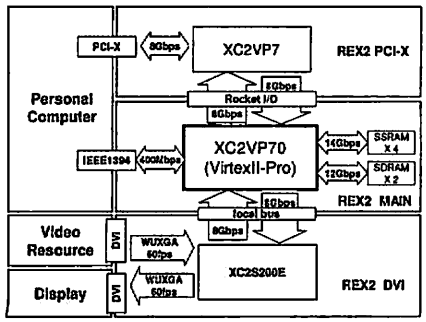

図5 システムのボード構成

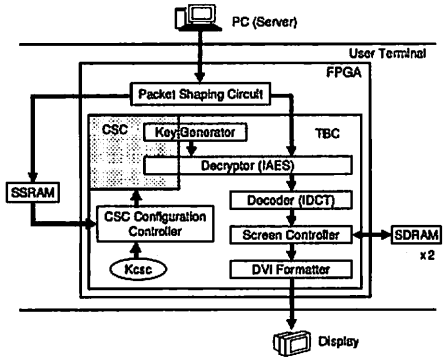

図6 システムの内部構成

イズされ，コンテンツの特性に応じた保護機能を提供する．

4.1 システムのハードウェア構成

DRM システムを，レクセオン・テクノロジー社(注1) の REX2 (REconfigurable EXperimental equipment 2) を用いて構築した．REX2 は，Virtex-II Pro XC2VP70 を搭載した FPGA 開発ボードである．REX2 を用いたシステムのハードウェア構成を図 5 に示す．システムは，CSC-TBC や動画再生回路が実装される主ボード (REX2 MAIN)，PC から映像ソースを供給するための PCI-X ボード (REX2 PCI-X)，および DVI 入出力ボード (REX2 DVI) から構成される．

回路の作成には，ザイリンクス社の統合開発環境 ISE 8.1i [9] と，同社の PlanAhead 8.2.3 [10] を使用した．PlanAhead は，部分再構成に特有の制約の設定やフロアプランができるほか，モジュールベースのインクリメンタルデザイン環境を提供し，部分再構成回路の開発プラットフォームとして利用することができる [11]．

4.2 システムの内部構成

図 6 にシステムの内部構成を示す．AES (CBC mode, 128-bit block size, 128-bit key) によって暗号化された動画像コンテンツは，CSC-TBC の結合回路によって生成された復号鍵を用いて TBC 内の復号回路で復号され，映像処理回路を経由してビデオ映像として外部モニタに出力される．

(注1)：レクセオン・テクノロジー (株) は，(独) 産業技術総合研究所の技術移転により設立されたベンチャー企業である．http://www.rexeon.com/

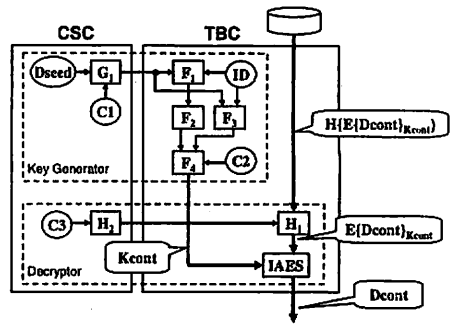

図7 CSC の内部構成の詳細

本システムでは，TBC のバスマクロの配置は，あらかじめ固定されている．ゆえに，動的に再構成される CSC のバスマクロの配置が TBC と完全に一致することがインターロックするための空間的条件となる．

4.3 CSC の詳細

図 7 に CSC-TBC のインターロック部のより詳細なブロック図を示す．ここで，CSC は固定値 D_{seed} の生成と機能ブロック G_1 および H_2 を担当し，TBC は機能ブロック $F_1 \sim F_4$，H_1，および IAES(AES の復号) を担当する．コンテンツを再生するには，AES を復号するための鍵 K_{cont} の生成と，バイナリ変換 H を行う必要があり，それぞれに対して，TBC および CSC の回路に固有の情報や機能が必要となっている．

本システムを構築する目的は，CSC-TBC メカニズムのコンセプトを実証することにある．特に，今回の実装では，インターロックの成否を利用したコンテンツ保護が正しく機能するかどうかを確認することを重視している．そのため，CSC-TBC で実行するデータ処理としては，以下に示す簡易な関数を用いた．これはデータの難読化を実現するよりむしろ，典型的な演算を組合せることによって実際の回路規模を大まかに模擬することを目的としているためである．

$$F_1 = (ID \oplus G_1) \gg 64$$
$$F_2 = TABLE(F_1)$$
$$F_3 = ((ID \gg 16) \oplus G_1) \gg 32$$
$$F_4 = F_2 \oplus F_3 \oplus C_2$$
$$G_1 = (Dseed \gg 96) \oplus C_1$$
$$H_1 = H\{E\{D_{cont}\}K_{cont}\} \oplus H_2$$
$$H_2 = C_3$$

ここで，ID は端末に固有な 128bit の値，D_{seed} はコンテンツに固有の 128bit の値，K_{cont} は暗号コンテンツを復号化するための鍵，D_{cont} はコンテンツデータである．D を暗号化する操作を $E\{D\}$ と表し，鍵 K を使って暗号化したことを明示する場合は $E\{D\}K$ と表す．また，データ $C_1 \sim C_3$ は定数である．演算子 $\oplus$ は排他的論理和を表し，$\gg$ は右循環シフトを表す．$TABLE(i)$ は，アドレス長 8 ビット，データ長 128 ビットのテーブルを，アドレス i で参照する関数を表す．

表1 端末固有回路(TBC)のリソース使用率

Resource	Utilization		(%)
Slice	11,881	/ 33,088	36%
Block RAM	235	/ 328	72%
MULT18x18	53	/ 328	16%
BUFGMUX	7	/ 16	43%
DCM	7	/ 8	88%
ICAP	1	/ 1	100%

表2 コンテンツ固有回路(CSC)のリソース使用率

Resource	Utilization		(%)
Slice	311	/ 33,088	1%

4.4 実装結果

TBCおよびCSCのハードウェアリソースの使用量を，それぞれ表1，表2に示す．CSCの大きさは，縦176 Slice，横4 Slice分である．これらの表が示すように，CSCが使用するSlice数はTBCと比較して極めて少なく，回路のごく一部分のみを変えることで，セキュアで粒度の細かな保護システムを提供可能であることがわかる．FPGA全体の回路構成データが約3.6 MBであるのに対し，CSCの暗号化ビットストリームは約75 KBと，およそ1/50の大きさである．CSCの再構成データはネットワークを経由して送信されるが，ネットワーク負荷は小さく，ダウンロード時間も短いと言える．

5 動画再生実験

実際に部分再構成を行ってCSCを構築し，システムが動作するか検証した．システムに対して暗号化された1080pハイビジョン(1920 × 1080ピクセルのプログレッシブモード)の動画像を送信し，正しく再生されるかどうか実験を行った．

5.1 実験手順

暗号化されたコンテンツを，以下の手順に従って再生する．ここで，暗号化されたCSCの再構成データ D_{csc} を復号するための秘密鍵を K_{csc} とする．

(1) システムを起動し，FPGA上にTBCを構築する．
(2) $E\{D_{csc}\}K_{csc}$ をPCから検証システムに送信する．$E\{D_{csc}\}K_{csc}$ はSSRAMに蓄積される．
(3) SSRAM内の $E\{D_{csc}\}K_{csc}$ を，CSC復号回路によって復号する．$E\{D_{csc}\}K_{csc}$ を復号するための秘密鍵 K_{csc} は，TBC内に埋め込まれている．
(4) K_{csc} で復号された D_{csc} を用いて部分書換えを実行し，CSCを構成する．
(5) CSC-TBCでコンテンツ復号鍵 K_{cont} を生成する．CSCが正規のTBCと正しく結合(インターロック)されると，コンテンツ復号鍵 K_{cont} が正しく生成される．CSCがインターロックされない場合，誤った鍵が生成される．
(6) 生成された復号鍵 K_{cont} が正しければ，暗号化されたコンテンツデータ $E\{D_{cont}\}K_{cont}$ は正しく復号され，再生される．

上記の手順を，CSCが以下の状態である場合においてそれぞれ実行し，動画の再生実験を行った．

A) CSCが構築されていない(システム初期状態)．
B) コンテンツに対応したCSCが，正規の端末上に構築される．
C) コンテンツに対応したCSCが，不正な端末上に構築される．
D) コンテンツに対応していないCSCが，正規の端末上に構築される．
E) コンテンツに対応していないCSCが，不正な端末上に構築される．

なお，正規の端末とは，認証されたユーザが所有する，コンテンツが再生されるべき端末である．不正な端末とは，コンテンツが再生されてはならない端末であり，攻撃者によって作成された端末のほか，他のユーザが所有する端末も含まれる．コンテンツに対応していないCSCとしては，図6における G_1 の演算結果を反転して出力する回路を与えた．

5.2 実験結果

前節で述べたA)からE)の場合について，暗号化された1080pハイビジョン動画の再生実験を行った．

A)のCSCが構築されていない状態では，図8に示すように映像が砂嵐状に再生された．これは，CSCが構築されなければ正しい鍵が生成されず，コンテンツの復号に失敗することを表している．よって，端末が第三者によって入手された場合でも，正規のCSCを入手できなければコンテンツの再生は不可能である．正規CSCの入手をPIN (Personal Identification Number)等で制限していれば，端末の盗難・紛失時にも，コンテンツが不正ユーザに利用されることを防ぐことが可能である．

B)はCSCとTBCがインターロックされた状態であり，ユーザによってシステムが正しく利用された場合に相当する．このとき，コンテンツは図9に示すように正しく再生された．これは，部分書換えを利用したCSCの構築，CSC-TBCのインターロック，CSC-TBCによる鍵の生成，およびコンテンツの復号に成功したことを表している．

C)は，コンテンツとCSCの対応はとれているが，不正な端末でCSCが構築された場合に相当する．このときシステムはフリーズし，コンテンツは正常に再生されなかった．ネットワーク経由で配信される回路情報 $E\{D_{csc}\}$ は暗号化されており，盗聴されても不正な端末でCSCが構築される可能性は低い．しかし，何らかの手段で $E\{D_{csc}\}$ が盗聴・解読され，D_{csc} が流出した場合でも，不正な端末ではインターロックが成立せず，コンテンツを正常に再生することはできないことが示された．しかし，システムがフリーズすると運用上の問題が生じるため，異常を検知して正常動作に復帰する仕組みが必要である．

D)は，正規の端末において，異なるコンテンツ用のCSCがTBC上に構築された場合に相当する．このとき，コンテンツはA)の場合と同様に砂嵐状に再生された．

E)は，他のコンテンツ用CSCまたは攻撃者が作成したCSCが，不正な端末で構築された場合に相当する．このときシステムはC)の場合と同様にフリーズし，コンテンツは正常に再生されなかった．

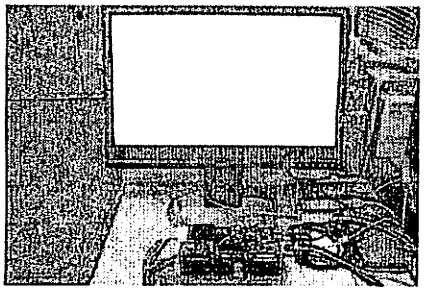

図 8　動画再生実験の結果 (インターロック失敗時)

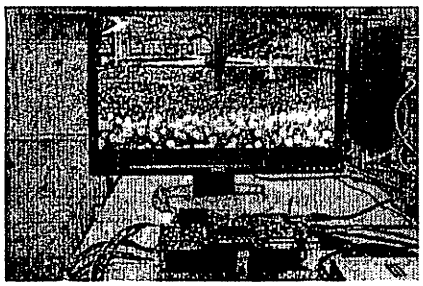

図 9　動画再生実験の結果 (インターロック成功時)

6 考　　察

ネットワーク経由で回路をダウンロードし，これを用いて FPGA を部分的に再構成するようなシステムでは，これまでにないエラー対策や攻撃への防御が必要になる．本章では，部分再構成を利用するシステムの保護について考える．

不正な CSC からの保護

ネットワーク経由で部分再構成を行うシステムでは，悪意のある第三者から不正な回路データが送られてくる可能性がある．CSC の回路データは暗号化されて送信されるため，暗号鍵がわからなければ端末上で動作する CSC を作成することはできないが，意味のないデータ列をシステムに与えることによって不具合を引き起こす攻撃が考えられる．今回の実験では，バスマクロの位置が不正であった場合に，システムがフリーズしてしまった．部分再構成を行うシステムでは，データによって回路そのものが変わってしまうため，単にリセットをかけても元の状態に復帰することができない．

このような不具合への対策として，異常状態から復帰する仕組みとともに，CSC を構築する前にそれが不正であるかどうか検証する仕組みを導入することが考えられる．

CSC の設計ミスへの対策

システムの不具合は，悪意のあるユーザによってのみ引き起こされるとは限らない．CSC の設計ミスにより，システムが破壊される可能性がある．例えば，予想を超えた温度上昇の発生，出力信号の衝突などによりシステムが破壊される可能性がある．この場合，サーバからは「正しい」CSC が送られてくるため，インターロックのメカニズムやチャレンジレスポンス方式等の認証を用いてエラーを防ぐことができない．そのため，CSC 構築後に回路の動作や信号を監視し，異常な状態が検出された場合に CSC を停止・再構築する仕組みが必要となる．

7 おわりに

FPGA の自己動的部分再構成を利用し，安全にデジタルコンテンツを配信するシステムについて説明した．また，産総研ベンチャーであるレクセオンテクノロジ社製の FPGA ボードを使用してシステムを実装し，実際に自己動的部分再構成を行ってシステムの有効性を検証した．

本システムでは，コンテンツに固有な再生回路の一部 (コンテンツ固有回路, CSC) をコンテンツとともにダウンロードし，端末側の回路 (端末固有回路, TBC) と結合することで，強力なコンテンツ保護の仕組みを提供する．CSC と TBC が正しく結合されなければコンテンツは再生されないため，回路のインタフェースの構成を認証の手段として利用することができる．また，急速に進歩する攻撃手法に，柔軟に対応して回路を更新することができる．

実際に構築した実験システムでは，暗号化された CSC の回路データの復号と，部分再構成機能を利用した CSC の構築に成功した．CSC は TBC と回路的に結合し，CSC が正規のものであった場合はコンテンツが正しく再生され，CSC が不正であった場合はコンテンツは再生されないことを確認した．これにより，部分再構成を利用した CSC-TBC の回路結合メカニズムをコンテンツ保護に利用できることを確認した．

今後の課題としては，不正な CSC が送られてきた場合の，システムのエラー対策が挙げられる．CSC を構築する前にそれが不正であるか確認する手段や，CSC 構築後の異常な動作を検出する手段について検討していく．

文　　献

[1] 財団法人デジタルコンテンツ協会 (編)，デジタルコンテンツ白書 2006，財団法人デジタルコンテンツ協会，2006.

[2] 財団法人インターネット協会 (編)，インターネット白書 2006，インプレス R&D，2006.

[3] 横山浩之，戸田賢二，"FPGA を用いたコンテンツ保護システムの開発，" 信学技報 CPSY2004-114，pp.55–60，2004.

[4] H. Yokoyama, and K. Toda, "FPGA-based content protection system for embedded consumer electronics," RTCSA, pp.502-7, 2005.

[5] 横山浩之，堀洋平，戸田賢二，"FPGA の部分書換方式を用いたコンテンツ保護システムの検討，" 信学技報 RECONF2006-34，2006.

[6] Y. Hori, H. Yokoyama, and K. Toda, "Secure content distributing system based on run-time partial reconfiguration," FPL, pp.637–640, 2006.

[7] 堀洋平，横山浩之，坂根広史，戸田賢二，"FPGA の自己動的部分再構成利用したシステムの設計と開発，" 信学技報 RECONF2006-75，pp.61–68，2006.

[8] Atmel Corporation, San Jose, CA, FPSLIC on-chip Partial Reconfiguration of the Embedded AT40K FPGA, , 2002.

[9] Xilinx, Development System Reference Guide, , for ISE8.1i edition, 2005.

[10] Xilinx, PlanAhead User Guide, Release 8.2, , 2006.

[11] N. Dorairaj, E. Shiflet, and M. Goosman, "PlanAhead Software as a platform for partial reconfiguration," Xcell Journal, vol.55, pp.68–71, 2005.