すれちがい通信を用いた分散型アクティベーションの提案

本部栄成† 高橋健太††,‡ 米山裕太† 西垣正勝†††

†静岡大学大学院情報学研究科，〒432-8011 静岡県浜松市中区城北 3-5-1
††(株)日立製作所横浜研究所，〒244-0817 神奈川県横浜市戸塚区吉田町 292
‡東京大学大学院情報理工学系研究科，〒113-8656 東京都文京区本郷 7-3-1
†††静岡大学創造科学技術大学院，〒432-8011 静岡県浜松市中区城北 3-5-1

あらまし ゲームソフトのコンテンツ保護を達成するには，ユーザ認証のコストやプライバシなどに起因する技術的課題と，ユーザのモラルの問題に起因する運用的課題の解決が必要となる．本稿では，これらの要求を満たすコンテンツ保護方式の一つとして，携帯ゲーム機のすれちがい通信を用いた分散型アクティベーション機構を提案する．提案方式では，秘密分散によってゲームソフトのID情報をゲーム機の個体識別番号に紐付けた形で分割し，そのシェアをゲームプレイ中に発生するすれちがい通信によってユーザ間で交換する．その際，過去に受信したシェアと通信相手のシェアから相手が不正ユーザであることを暴き，ユーザ間で注意を促すことによって，不正コピーに根付くユーザのモラル低下の問題の改善を図る．

A distributed product activation using direct communication on portable game machines

Eisei Honbu† Kenta Takahashi††,‡ Yuta Yoneyama† Masakatsu Nishigaki†††

†Graduate school of Informatics, Shizuoka University
3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan
††Hitachi, Ltd., Yokohama Research Laboratory
292 Yoshida, Tozuka, Yokohama, Kanagawa, 244-0817 Japan
‡Graduate School of Information Science and Technology, The Universe of Tokyo
7-3-1 Hongo, bunkyo, Tokyo, 113-8656, JAPAN
†††Graduate School of Science and Technology, Shizuoka University
3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan

Abstract Software protection has problems regarding privacy, cost, user's moral and so on. To cope with these problems, this paper proposes a distributed product activation scheme using direct communication on portable game machines. In the proposed scheme, a software ID is split into shares associated with a machine ID by secret sharing, and each shares are exchanged with other users using the direct communication channel as they are passing each other. At the moment, the shares are checked by using secret reconstruction, and illegal copy users will be disclosed. The game users can recognize who are illegal users, and thereby we expect illegal users to halt using illegal copy because they feel a sense of guilt.

1　はじめに

インターネットの普及により Web 上に違法アップロードされたデジタルコンテンツの違法ダウンロードやファイル共有ソフトによるコンテンツの不正コピーによる被害が増加している．特に，携帯ゲーム機においては，近年，マジコンと呼ばれるアクセスコントロールを回避する機器が流通したことなどにより，ゲームソフトの不正コピーが深刻な状況となっており，調査によるとその被害額は 3500 億円にも上ると報告されている[1].

不正コピーを防止する技術として，Windows®[1] OS などで用いられているオンラインアクティベーションがよく知られている[2]．しかしながら，我々が調べた限り，オンラインアクティベーションがゲームソフトの不正コピー防止技術として用いられている例は少ない．我々は，以下の 3 つの問題がその理由として挙げられると推測する．1 つ目が，アクティベーションとゲームが独立しており，アクティベーションさえ回避すれば支障なくそのゲームで遊べてしまうという，アクティベーションの単独性の問題である．2 つ目が，ゲームソフトメーカがオンラインアクティベーションのためのサーバを設置・管理・保守する必要があるという，販売者側のコストの問題である．3 つ目が，ユーザ（端末）情報をサーバに届け出ることが必要であるという，プライバシの問題である．また，マジコンが挿入された携帯ゲーム機を使って街中で堂々と遊んでいる人々がいる[1]ことに鑑みるに，ユーザのモラル低下も不正コピー蔓延の潜在的な要因であると考えられる．そこで，ゲームソフトの不正コピー防止策には不正者にモラルを取り戻してもらうための工夫も必要であると考える．

そこで本稿では，携帯ゲーム機のすれちがい通信を用いた分散型アクティベーションを提案する．提案方式では，秘密分散によってゲームソフトの ID 情報をゲーム機の個体識別番号に紐付けた形で分割し，そのシェアをゲームプレイ中に発生するすれちがい通信によってユーザ間で交換する．その際，過去に受信したシェアと通信相手のシェアから相手が不正ユーザであることが暴かれる．提案方式では，すれちがい通信を利用することによってアクティベーションの単独性の問題を，サーバレスの分散型アクティベーションとすることによってコストの問題を，秘密分散によってプライバシの問題を，それぞれ解決する．また，不正者はすれちがい通信の相手に自分が不正者であることを知られてしまうことになるため，それが不正者の罪悪感を増長させ，ユーザのモラル改善につながるのではないかと期待される．

提案方式は，すれちがい通信によってイベントが発生する機能を含むゲームソフトに対して適用可能である．

2　アクティベーションの課題

現在，オンラインアクティベーション（以下，単に「アクティベーション」と記す）は Microsoft の OS [2]や Adobe Systems のソフトウェア[3]などに用いられており，コンテンツ保護技術の主流の一つとなっている．

しかし，我々が調べた限り，アクティベーションがゲームソフトの不正コピー防止技術として使用されている例は少ない．我々は，以下の 3 つの問題がその理由として挙げられると推測する．

1 つ目が，アクティベーションとゲームが独立しており，アクティベーションさえ回避すれば支障なくそのゲームで遊べてしまうという，アクティベーションの単独性の問題である．ゲームのプレイ中に定常的に，かつ，プレイの邪魔にならない形で不正コピーの検査が実施されることが理想的である．

2 つ目が，ゲームソフトメーカがアクティベーションのためのサーバを設置・管理・保守する必要があるという，販売者側のコストの問題で

[1] Windows は米国 Microsoft Corporation の登録商標．

ある．ゲームソフトのライフサイクルに鑑みると，アクティベーション用サーバの運用期間は比較的長期に及ぶため，運用コストが増大してしまう．また，アクティベーション情報（ユーザのシリアル番号と端末情報の紐付け情報）は個人情報に該当するため，これを適正に保守するためには相応の管理コストがかかることになり，メーカにとって大きな負担となり得る．

3 つ目が，アクティベーション情報をサーバに届け出ることが必要であるという，プライバシの問題である．ゲームソフトの購入履歴からユーザの嗜好がメーカ側に伝わることになるため，アクティベーション情報の登録は，ユーザにとって大きなプライバシ上の懸念を生じさせることになる．

また，1 つ目の問題に関連して，不正ユーザのモラルの低下についても考慮が必要であろう．「アクティベーションさえ回避すればゲームで遊べる」という状況は，不正ユーザをアクティベーション回避の行動に駆り立てる一因となっている恐れがあるのではないかと我々は考えている．マジコンが挿入された携帯ゲーム機を使って街中で堂々と遊んでいる人々がいる[1]ことに鑑みるに，ユーザのモラル低下も不正コピー蔓延の潜在的な要因であると考えられる．そこで，ゲームソフトの不正コピー防止策には不正者にモラルを取り戻してもらうための工夫も必要であると考える．

3　必要要件と対策技術

2 章にて分析した現行のアクティベーションの問題に基づき，ゲームソフトの不正コピー防止機構に求められる要件をまとめる．また，どのような技術であればそれらの要件を満たすことができるか検討する．

3.1　サーバレス分散型アクティベーション

ゲームソフトメーカのコストの問題に対する対策として，サーバを用いない分散型のアクティベーションが有効である．すなわち，アクティベーション情報をサーバに収集する現行の一極集中型アクティベーションではなく，ユーザ間でアクティベート情報を交換し合い，ユーザ同士で不正者を検知する P2P 型の分散アクティベーションとする．

3.2　すれちがい通信

分散型アクティベーションではユーザ間においてアクティベート情報を交換するための通信が必須となる．アクティベーションの単独性の問題に対処するためには，このアクティベート情報の通信手段としてすれちがい通信を用いることが有効である．

すれちがい通信とは，携帯ゲーム機に搭載されている通信技術であり，すれちがい通信に対応したゲームをプレイしているユーザ同士が通信範囲にいる場合に Wi-Fi を用いて P2P ネットワークを形成し，自動的かつ瞬時にメッセージ交換を行うことができる．

任天堂から販売されている Nintendo DS®[2] は独自プロトコルを採用しているため詳細は明らかになっていないが，SONY から販売されている PSP®[3]では，IEEE 802.11 無線 LAN のアドホックモードを用いて通信が行われており [4]，DSR (dynamic source routing protocol) [5]などを用いて周辺の携帯ゲーム機を探索する．DSR では，自身の IP アドレスを含んだパケットをブロードキャストし，そのパケットを受信した端末はその IP アドレスを辿ることで通信のセッションを確立し，データのやり取りを開始する．

すれちがい通信によって，ゲームの中で特別なイベントが発生したり，ゲームをより一層楽しむためのデータを得ることができ，プレイヤは周りの仲間と一緒にゲームを遊んでいるという共有感を体験できる．このため，不正者であってもゲームを十分に楽しもうとすると，すれちがい通信を行わざるを得ない．すなわち，すれちがい通信は不正者を含め全ユーザが行う通信

[2] Nintendo DS は任天堂(株)の登録商標．
[3] PSP は(株)ソニー・コンピュータエンタテインメントの登録商標．

であると考えられる.

ゲームプレイ中に発生するすれちがい通信を用いてユーザ間でアクティベート情報を交換することによって，定常的な不正コピーの検査が実現し，ゲームとアクティベーションがより密接に結合することになる．また，現状のすれちがい通信にピギーバックさせる形でアクティベート情報を送受信してやれば，プレイの邪魔にならない形での不正コピーの検査についても達成される.

すれちがい通信の発生時に不正コピーの検査が行われるということは，不正者はすれちがった相手に自分が不正者であることを知られてしまうことを意味する．このため，それが不正者の罪悪感を増長させ，ユーザのモラル改善にもつながるのではないかと考えられる.

3.3 秘密分散

分散型アクティベーションでは，ユーザは自身のアクティベート情報を他のユーザの端末に送信しなければならない．すなわち，アクティベーションのプライバシの問題は更に深刻となる．ユーザのプライバシを保護しながら不正コピーの検知を実現するためには，秘密分散によるアクティベート情報の秘匿が有効である.

秘密分散とは，情報を複数のシェアに分割することによって秘匿する暗号技術である[6]．2-out-of-2 秘密分散では，2 個に分割したシェアを 2 つとも集めた場合に秘密が復元される．例えば Lagrange 補間に基づく秘密分散では，秘密情報を y 切片とした x の 1 次多項式 $f(x)$を構成し，異なる 2 個のサンプルポイント x_1，x_2 における $f(x_1)$，$f(x_2)$をシェアとして生成する．2 個のシェア$(x_1,f(x_1))$，$(x_2,f(x_2))$が分かれば，Lagrange 補間によって $f(x)$を特定でき，$f(0)$を求めることによって秘密情報（y 切片）が逆算できる.

これを利用し，ゲームソフトのコンテンツ情報をパラメータと捉えて 1 次多項式 f(・)を構成し，それぞれのゲーム機が各自のゲームソフトに関するシェアを出力することを考える．詳細は次章で説明するが，異なるゲーム機にて同一のゲームソフト（不正コピー品）がプレイされている場合にのみ，2 つのシェアが揃って情報が復元されることによって，不正コピーが発覚する.

4 分散型アクティベーション

3 章で説明した技術を用いた分散型アクティベーション方式の詳細を説明する.

4.1 前提

携帯ゲーム機にはゲーム機ごとに異なる個体識別番号 MID が割り振られている．MID は n ビットの空間からランダムに生成される．工場出荷時にハードウェア的に記録され，不正者が変更できない.

ゲームソフトには（同じゲームであっても）それぞれ異なるコンテンツ ID が割り当てられている．提案方式では，1 つのゲームソフトに対して 3 種類のコンテンツ ID（CIDa，CIDb，CIDc）が割り当てられる．CIDa，CIDb，CIDc は，それぞれ n ビットの空間からランダムに生成される．CIDb には，その正当性を確認できるように，適切なビット数のチェックサム CS が別途付与される．ゲーム機にはチェックサム CS を検査する機構がハードウェア的に実装されている．なお，CS はすべてのコンテンツにおいて共通である.

「コンテンツ ID」と「ゲームソフトのプログラム」を連結したデータに対してコード署名が付されている．コード署名の検証のために必要な公開鍵および公開鍵証明書もゲームソフトに付随する．ゲーム機にはコード署名の検査機構がハードウェア的に実装されており，コード署名の検査に失敗したゲームソフトについてはその実行が許可されない.

ゲームソフトはコード署名によって保護されているため，不正者はゲームソフトを不正にコ

ピーすることは可能であるが，その内容を改ざんすることはできない．すなわち，不正コピー品と正規品は同じコンテンツ ID を持つ．このため，不正者が不正コピー品を使用していた場合には，同じコンテンツ ID を持つゲームソフトが複数のゲーム機の中に同時に存在するという状況が起こる．

また，携帯ゲーム機に搭載される OS についてもコード署名によって保護し，ゲーム機起動時に署名の検証を行う．コード署名を検証するためのトラストアンカーとなる署名鍵は携帯ゲーム機内の耐タンパーモジュール TPM (Trusted Platform Module)上で管理される．

提案方式による不正コピー検知のルーチンも OS あるいはゲームソフトの中にコーディングされており，それぞれ OS およびゲームソフトのコード署名によって保護されている．

4.2 ゲーム機からのシェアの発信

個体識別番号が MID のゲーム機において，コンテンツ ID が CIDa，CIDb，CIDc のゲームソフトをプレイする場合を例に，提案方式の流れを説明する(図 1)．なお，現時点では MID，CID のビット数 n として 256 ビットを想定している．

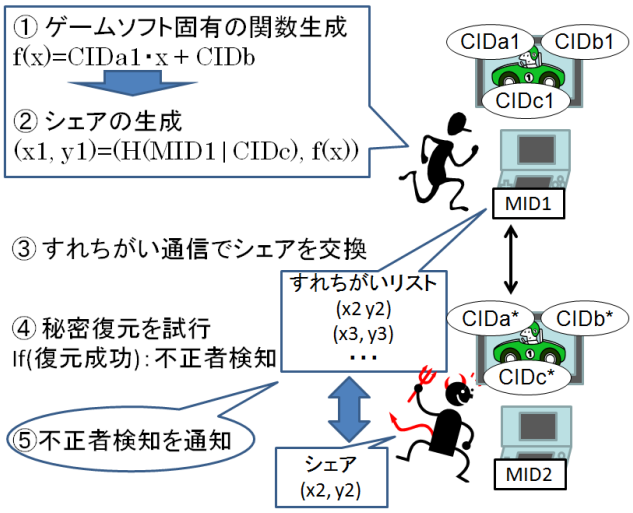

図1 提案方式の流れ

各ゲーム機は，1 次関数 f(x)=CIDa・x+CIDb | CS を生成し(図 1 における①)，その直線上の 1 点(x,y)=(h(MID | CIDc),f(h(MID | CIDc)))を算出する(図 1 における②)．ここで，h(w)は 2n ビットのメッセージ w を入力とし，n ビットのハッシュ値を出力するハッシュ関数を表し，n | m は n と m の連結を表す．コンテンツ ID (CIDa，CIDb，CIDc)はコード署名によって守られているため，不正コピー品を使用している不正者間では同一の 1 次関数が生成される点に注意されたい．また，異なるゲーム機を利用しているユーザ間においては，MID が異なるため，x=h(MID | CIDc)の値が一致することはない．

各ゲーム機は，他のゲーム機とすれ違う度に，すれちがい通信によって相手のゲーム機に自分のシェア(x,y)を送信する(図1における③)．同時に，相手のゲーム機のシェア(x,y)を受信する．また，各ゲーム機はすれちがい通信を行うたびに，それまでにすれちがい通信によって受信した他のゲーム機のシェア(x,y)も交換する．各ゲーム機には，それまでのすれちがい通信によって受信したシェアを保管する機構を有する．保管されている過去のシェアを「すれちがいリスト」と呼ぶ．

4.3 不正者の検知

各ゲーム機に集約されたシェア(x,y)を用いて，各ユーザが不正コピーを検査する手順を以下に示す．

ユーザ 1 のゲームソフトをユーザ 2 が不正コピーして使用しており，ユーザ 3 がその不正コピーを検知するという状況を仮定する．ユーザ 1 とユーザ 2 のゲーム機の MID をそれぞれ MID1，MID2 とし，両者が不正に共有しているゲームソフトの CID を CIDa*，CIDb*，CIDc* とする．ユーザ 1 とユーザ 2 の 1 次関数 f*(x)=CIDa*・x+CIDb* | CS は同一であり，それぞれのシェアは(x1,y1)=(h(MID1 | CIDc*), f*(h(MID1 | CIDc*))) ， (x2,y2)=(h(MID2 | CIDc*),f*(h(MID2 | CIDc*)))となる．ユーザ 3 のゲーム機の MID とゲームソフトの CID を，それぞれ MID3，CIDa3，CIDb3，CIDc3 とす

る. ユーザ 3 の 1 次関数は $f_3(x)$=CIDa3・x+CIDb3|CS，シェアは(x3,y3)=(h(MID3|CIDc*),f_3(h(MID3|CIDc3)))となる.

まず，ユーザ 3 がユーザ 1 とすれちがい通信を行ったとする. ユーザ 3 はユーザ 1 のシェア(x1,y1)を受信し，自身のゲーム機内のすれちがいリストにこれを追加し保管する. 同時に，ユーザ 3 も自身の(x3,y3)をユーザ 1 に送信し，ユーザ 1 はそれを自身のすれちがいリストに追加し保管する.

次に，ユーザ 3 がユーザ 2 とすれちがい通信を行ったとする. ユーザ 3 はユーザ 2 のシェア(x2,y2)を受信する. このとき，すれちがいリストに保管されている(x1,x1)と受信した(x2,y2)から 1 次関数 f(x)を復元できるかを試みる(図 1 における④). f(x)が正しく復元されたかどうかは，y 切片 CIDb のチェックサム CS によって確認できる. ここでは，(x1,x1)と(x2,y2)が同一の 1 次関数 f*(x)の上の異なるシェアとなっているため，秘密分散の性質から f*(x)が復元され，ユーザ 3 はその y 切片である CIDb*|CS を求めることができる. これによってユーザ 3 は，今すれちがった相手(ユーザ 2)が不正コピー品を使っていることが分かる.

ユーザ 3 のシェアに関しては，ゲームソフトが不正コピーされていない限り，1 つの 1 次関数 $f_3(x)$から 1 つのシェア(x3,y3)しか発生しないため，すれちがい通信によってシェアを発信してもその y 切片が正しく復元されることはない. このため，ユーザ 3 が不正者として判定されることはない.

ユーザ 3 がユーザ 1 とすれちがった時点においては，まだ 2 つのシェアが揃っておらず，ユーザ 3 はユーザ 1 の不正を発見することはできない. この問題を緩和するために，各ゲーム機はすれちがい通信を行う際に，自分自身のシェアだけでなく，自分が有するすれちがいリスト(自分がそれまでのすれちがい通信によって受信した他のゲーム機のシェア)も交換する. これによって各ゲーム機には，自分と実際にすれちがい通信をしていないゲーム機からのシェアも集まることになる.

また，すれちがった相手が不正者であることが判明した場合，その際の相手のシェアを「ブラックシェア」としてブラックリスト登録する. ブラックシェアリストもすれちがいリストと一緒に交換することによって，各ゲーム機には実際にすれちがい通信をしていない不正者のシェアが集まり，より効率的な不正者の検知が可能となる.

4.4 不正者に対する抑制

ゲームソフトの不正コピーにおいて，ユーザのモラルが低下していることが不正コピーの潜在的な要因であると考えられる. そこで，ユーザが不正者とすれ違った際には，すれちがい通信を用いて不正者のゲーム機に注意や警告などのメッセージを表示するとともに，正規ユーザのゲーム機にも「今，すれちがった人は不正コピーしたゲームを使用していますよ」というメッセージを表示する(図 1 における⑤). これによって，不正者には「周辺のユーザから白い目で見られている」という意識が生じ，人目を気にして不正コピー品の使用を躊躇するようになるのではないかと期待される.

5 考察

提案方式が十分に機能することを，すれちがいリストのサイズとプライバシの観点から考察する.

5.1 すれちがいリストのサイズ

不正コピー検知が十分に機能するために必要なすれちがいリストのサイズについて検討する. ここでは，「ユーザが不正者とすれちがった際に 50%以上の確率でこれを検知できる」という要件を満たすためのリストサイズを評価する.

携帯ゲーム機を所持する全ユーザ数を u，すれちがいリストのサイズを L とする. あるゲームソフトの不正コピー品がインターネット上の不正

サイトで違法公開されており，k 人の不正者(u>k)がこれを利用している(すなわち，コミュニティの中に同じコンテンツ ID を持つゲームソフトが k 個存在している)とする，

提案方式においては，「既に不正者のシェアを 1 つ以上有している状態にあるユーザ」が次の不正者とすれちがった場合に，不正者のシェアが2つ揃い，今すれちがった相手が不正者であることを発見することできる．よって，「あるユーザが，自身のすれちがいリストの中のシェアのみを用いて，今すれちがった相手が不正者であるか判定できる」という事象は，「すれちがいリストの中に不正者のシェアが含まれている」という事象と捉えることができる．すなわち，提案方式による不正者検知の確率は，「u 人のユーザから無作為に L 人を抽出した場合に，その中に不正者が 1 人以上存在する確率」という形で定式化が可能である．以上より，50%以上の確率で不正者を発見することができるか否かについては以下の不等式で評価できる．

$$\frac{1}{2} \leq \left(1 - \prod_{i=0}^{L-1} \frac{u-k-i}{u-i}\right) \quad (1)$$

式(1)中の$\prod_{i=0}^{L-1} \frac{u-k-i}{u-i}$は，リスト内の L 個のシェアが全て正規ユーザのものである場合の確率である．ここで，k，u が L よりも十分大きな値をとると仮定する(L << k, u)．この場合，式(1)を以下のように近似することができる．

$$\frac{1}{2} \leq \left(1 - \prod_{i=0}^{L-1} \frac{u-k}{u}\right) \quad (2)$$

右辺 $= 1 - \left(\frac{u-k}{u}\right)^L = 1 - \left(1 - \frac{k}{u}\right)^L$ より，式(2)は以下のように変形することができ，式(3)が得られる．

$$\left(1 - \frac{k}{u}\right)^L \geq \frac{1}{2}$$

$$\log\left(1 - \frac{k}{u}\right)^L \geq \log\frac{1}{2}$$

$$L \geq -\frac{\log 2}{\log(1 - \frac{k}{u})} \quad (3)$$

式(3)に基づいて，不正者とすれちがった際にそれを 50%以上の確率で検知するために必要なリストサイズ L を，$\frac{k}{u}$(全ユーザ数の内の不正者)に対して示したものが図 2 である．

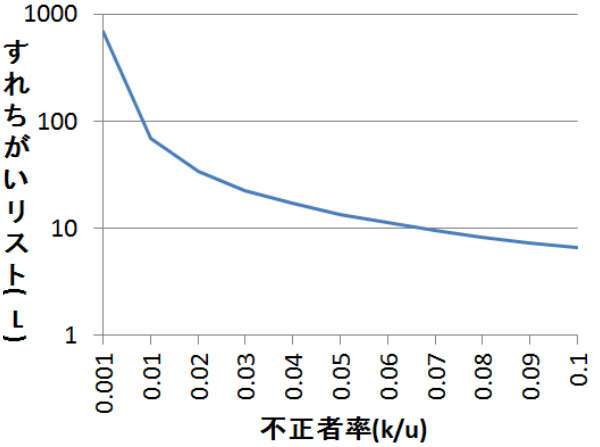

図 2 すれちがいリストサイズの推移グラフ

Nintendo DS の販売台数は 2012 年 1 月末の時点で 151,060,000 台である[7]．社団法人コンピュータエンターテインメント協会による違法複製ゲームソフトの使用実態調査報告書[8]によると，Nintendo DS のゲームソフトが違法にアップロードされている 22 サイトを調査した結果，2004~2009 年累計販売タイトルトップ 20 位のダウンロード総数は 19,347,668 回であると報告されている．すなわち，ゲームソフト 1 本当たりの平均違法ダウンロード数は 19,347,668 / 20≒967,383 と試算される．このすべての不正コピー品のコピー元が一つのゲームソフトであったと仮定すると，式(3)より，リストサイズは$L \geq -\frac{\log 2}{\log\left(1 - \frac{967,383}{151,060,000}\right)} \fallingdotseq 108$ となる．1 個当たりのシェア(x, y)のデータサイズと近年の携帯ゲーム機のストレージサイズに鑑み，過去にすれちがった相手から受信したすべてのシェアの内，最近受け取った 108 個程度のシェアをすれちがいリストの中に格納することは特に支障はないと考えてよいと思われる．

また，提案方式においては，すれちがい通信によって相手のシェアを受信する度に，すれちがいリストに含まれるシェアの各々と今受け取ったシェアを用いての不正コピーの検査(図 1 における④)が実行される．すなわち，不正コピーの検査に要する時間も，すれちがいリストの

サイズ L に比例することとなる. 現在の携帯ゲーム機の CPU の性能に鑑みるに, 108 回程度の秘密復元の操作はそれほど大きなオーバヘッドには至らないと考えてよいと思われる.

5.2 プライバシに関する検討

すれちがい通信によって交換されるシェア(x,y)から, ユーザのプライバシ情報が漏洩することがないか検討する. y は x に従属する情報(y=f(x))であるので, ここでは x に焦点を当て, x からユーザ(不正コピー品を使用していない正規ユーザ)のゲーム機に関する情報 MID が抽出されることがないか議論する.

説明を簡単にするため, ゲーム機 1(個体識別番号:MID1)を所有するユーザ 1 が, ゲームソフト 1(コンテンツ ID:CIDa1, CIDb1, CIDc1)とソフト 2(コンテンツ ID:CIDa2, CIDb2, CIDc2)をプレイした場合を想定する. ユーザ 1 がソフト 1 のプレイ中にゲーム機 1 から発信される x1 とソフト 2 のプレイ中にゲーム機 1 から発信される x2 は, それぞれ h(MID1|CIDc1)と h(MID1|CIDc2)となる.

x1 においては, MID1 が CIDc1 によってマスクされた上で, ハッシュ関数 h(・)によって撹拌されている状態であると見なせる. x2 においても同様である. したがって, ユーザ 1 以外の任意のユーザ i が x1 と x2 の両者を入手したとしても, x1 と x2 が同一の MID1 から生成されたものであることを判読することは不可能である. すなわち, ある日時にユーザ 1 がソフト 1 のプレイ中にユーザ i とすれちがい, その後, 別の日時にユーザ 1 がソフト 2 のプレイ中にユーザ i とすれちがったとしても, ユーザ i はその際に受信したシェア x1 と x2 からすれちがったユーザが同一人物であることを知ることはできない.

6 まとめと今後の課題

本稿では, 携帯ゲーム機のすれちがい通信を用いた分散型アクティベーションを提案し, その有効性をすれちがいリストのサイズとプライバシの問題の観点から考察した. 今後はプロトタイプシステムを実装して実環境でのパフォーマンス評価を行うとともに, プライバシ保護については安全性の証明を行っていきたい.

また, 提案方式は, 不正コピーを検知した場合は, その不正者に対して注意メッセージを送り, 不正ユーザの心理に訴えかけることによって不正者のモラル向上を促す. 今後, このような「ソーシャルな対応」が本当に不正コピーの抑止力になるのかについても検証を行っていく必要がある.

参考文献

[1] 読売新聞, 「マジコン」損害 3500 億円, 2010 年 11 月 20 日付夕刊

[2] マイクロソフト, Windows XP プロダクトアクティベーション, http://technet.microsoft.com/ja-jp/library/bb457054.aspx

[3] アドビ:アドビソフトウェアのライセンス認証, http://www.adobe.com/jp/products/activation/

[4] ソニー・コンピュータエンタテインメント, "PSP"のインフラストラクチャーモードとアドホックモードとは?, http://jp-playstation.custhelp.com/app/answers/detail/a_id/193

[5] D.B. Johnson, D.A. Maltz, Y.C. Hu, J.G. Jetcheva, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, Internet Draft, draft-ietf-manet-dsr-07.txt, Feb 2002, http://tools.ietf.org/html/draft-ietf-manet-dsr-07

[6] 尾形わかは, 黒沢馨, 秘密分散法とその応用, 電子情報通信学会誌, Vol.82, No.12, pp.1228-1236, Dec 1999.

[7] 任天堂株式会社, 2011 年度第 72 期(2012 年 3 月期)第 3 四半期決算短信, http://www.nintendo.co.jp/ir/pdf/2012/120126.pdf

[8] 馬場研究室, 違法複製ゲームソフトの使用実態調査報告書, 2010 年 5 月 17 日, http://www.cesa.or.jp/uploads/2010/ihoufukusei.pdf