情報処理学会論文誌 Vol.54 No.9 2188–2196 (Sep. 2013)

すれちがい通信を用いた分散型不正コピー検知の提案

西垣 正勝[1,a)] 本部 栄成[1] 米山 裕太[1] 高橋 健太[2,3]

受付日 2012年12月3日, 採録日 2013年6月14日

概要：ゲームソフトのコンテンツ保護を達成するには，不正コピー利用防止機構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．本論文では，これらの要求を満たすコンテンツ保護方式の 1 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不正コピー検知機構を提案する．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．

キーワード：不正コピー検知，すれちがい通信，秘密分散，携帯ゲーム機，罪悪感

A Distributed Software Protection Using Direct Communication on Portable Game Machines

Masakatsu Nishigaki[1,a)] Eisei Honbu[1] Yuta Yoneyama[1] Kenta Takahashi[2,3]

Received: December 3, 2012, Accepted: June 14, 2013

Abstract: Software protection has problems regarding privacy, cost, user's moral and so on. To cope with these problems, this paper proposes a distributed software protection 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 share is 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.

Keywords: software protection, direct communication, secret sharing, portable game machine, 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 3,500 億円にものぼ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，著者らが調べた限り，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．著者らは，以下の 3 つの問題がその理由としてあ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

[1] 静岡大学大学院情報学研究科
Graduate school of Informatics, Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[2] 株式会社日立製作所横浜研究所
Yokohama Research Laboratory, Hitachi, Ltd., Yokohama, Kanagawa 244–0817, Japan
[3] 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo, Bunkyo, Tokyo 113–8656, Japan
[a)] nisigaki@inf.shizuoka.ac.jp

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

遊べてしまうという，検査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] ことに鑑みると，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．

そこで本論文では，携帯ゲーム機のすれちがい通信を用いた分散型不正コピー検知を提案する．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検査の単独性の問題を，サーバレスの分散型不正コピー検知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．ここで，すれちがい通信がゲームの面白さに直結するソフトであるほど提案方式による不正コピー検知の効果が期待できる．

本論文の構成は以下のとおりである．2 章では既存のオンラインアクティベーションの概要と課題について述べ，3 章でその課題を解決するための要件とその技術をまとめる．4 章で提案方式の詳細について述べ，5 章で提案方式の可用性について考察する．最後に 6 章で本論文をまとめ，今後の課題を述べる．

2. オンラインアクティベーション

2.1 仕組み

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 1 つとなっている．

Microsoft の方式を例に採り，アクティベーションの流れについて述べる（図 1）．ソフトウェアメーカは販売するすべてのソフトウェアに固有なシリアル番号を付与した状態で出荷し，出荷されたシリアル番号のすべてを把握しておく．ソフトウェアを購入したユーザはソフトウェアのインストール時や実行時に，ソフトウェアのシリアル番号とハードウェアの構成情報（PC のプロセッサのシリアル番号などのハッシュ値）を 1 対 1 に対応させた紐付け情報を生成し，メーカが用意しているサーバにインターネットを介して登録する．メーカは，シリアル番号の正当性を確認するとともに，シリアル番号と端末情報の重複を検査することで，ソフトウェアの不正コピーを検知することができる．正規利用と判断された場合にのみ，メーカからユーザにアクティベートキーが送信され，ユーザはソフトウェアを実行することが可能となる．このように，メーカは登録情報を管理することで，どのユーザ（端末）がどのソフトウェア（シリアル番号）を所持しているのかを把握することができる．

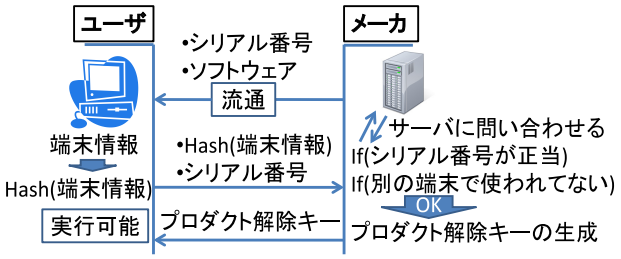

図 1 現行のアクティベーションの流れ
Fig. 1 Flow of existing online product activation.

2.2 問題点

著者らが調べた限り，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．著者らは，以下の 3 つの問題がその理由としてあ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，検査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うる．

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著者らは考えている．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] ことに鑑みると，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章で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検知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 サーバレス分散型不正コピー検知

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不正コピー検知機構が有効である．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の不正コピー検知ではなく，ユーザ間で不正コピー検査のための情報（以下，「不正コピー検査用情報」とする）を交換し合い，ユーザ同士で不正者を検知する P2P 型の分散不正コピー検知機構とする．

3.2 すれちがい通信

分散型不正コピー検知ではユーザ間において不正コピー検査用情報を交換するための通信が必須となる．ここで，検査の単独性の問題に対処するためには，この不正コピー検査用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 アドレスをたどることで通信のセッションを確立し，データのやりとりを開始する．

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，ゲームをよりいっそう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えない．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不正コピー検査用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，ゲームと不正コピー検知がより密接に結合することになる．ここで，不正コピー検査のための通信を新たに発生させるのではなく，ゲームの中で発生するすれちがい通信にピギーバックさせる形で不正コピー検査用情報を送受信することに注意されたい．すなわち，ゲームを遊ぶうえでのすれちがい通信の重要度（すれちがい通信がゲームの楽しさにどれくらい直結するか）が高いゲームソフトほど，提案方式の効果が期待される．

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

分散型不正コピー検知では，ユーザは自身の不正コピー検査用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，不正コピー検知におけるプライバシの問題はさらに深刻となる．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，秘密分散による不正コピー検査用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．たとえば 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 x1，x2 における f(x1)，f(x2) をシェアとして生成する．2個のシェア (x1, f(x1))，(x2, f(x2)) 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とらえて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

*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. 分散型不正コピー検知

3 章で説明した技術を用いた分散型不正コピー検知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（同じゲームタイトルであっても）それぞれ異なるコンテンツ識別番号 CID が割り当てられている．CID は α ビットの空間からランダムに選択される．CID には，その正当性を確認するための β ビットのチェックサム CS が連結され，CID|CS の形で n ビット（すなわち $\alpha+\beta=n$）のビット列を構成する．ここで，a|b は a と b の連結を表す．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．また，CID に紐付いた 2 つの乱数（以下，コンテンツ乱数）Ra と Rb が用意される．Ra と Rb は，それぞれ，n ビットの空間からランダムに選択される．

「CID および Ra と Rb」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．攻撃者によるハードウェアの改ざんはないものとする．すなわち，コード署名の検査機構を攻撃者が回避することはできないという前提をおく．

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識別番号を持つ．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，同じコンテンツ識別番号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となる署名鍵は携帯ゲーム機内の耐タンパモジュール 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（すれちがい通信の際に不正コピー検査用情報についても送受信する，受信した不正コピー検査用情報をチェックして通信相手が不正者であるか否かを判定する，などの一連のプログラム）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．

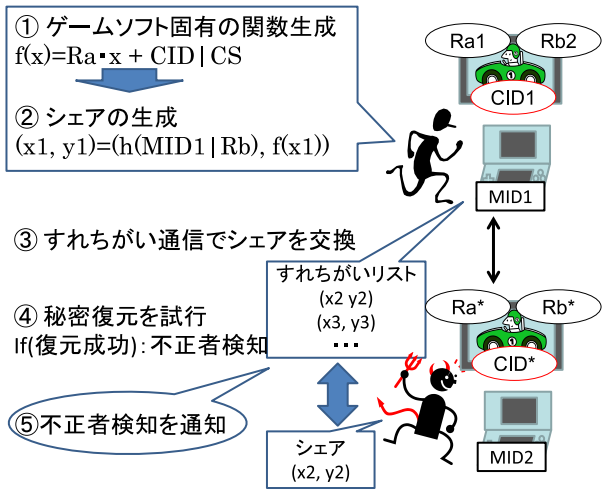

図 2 提案方式の流れ
Fig. 2 Flow of proposed scheme.

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，「コンテンツ識別番号が CID，コンテンツ乱数が Ra，Rb」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 2）．なお，現時点では MID，CID|CS，Ra，Rb のビット数 n として 256 ビットを想定している．

各ゲーム機は，1 次関数 $f(x) = Ra \cdot x + CID|CS$ を生成し（図 2 における ①），その直線上の 1 点 $(x, y) = (h(MID|Rb), f(h(MID|Rb)))$ を算出する（図 2 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，a|b は a と b の連結を表す．コンテンツ識別番号 CID およびコンテンツ乱数 Ra，Rb 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，個体識別番号 MID が異なるため，（不正コピー品を使用している不正者間であっても）$x = h(MID|Rb)$ 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たびに，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 2 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コンテンツ識別番号，チェックサム，コンテンツ乱数を CID*，CS*，Ra*，Rb*とする．ユーザ 1 とユーザ 2 の 1 次関数 f*(x) = Ra* · x + CID*|CS* は同一であり，それぞれのシェアは

$$(x1, y1) = (h(MID1|Rb^*), f^*(h(MID1|Rb^*))),$$
$$(x2, y2) = (h(MID2|Rb^*), f^*(h(MID2|Rb^*)))$$

となる．ユーザ 3 のゲーム機の個体識別番号とゲームソフトのコンテンツ識別番号，チェックサム，コンテンツ乱数を，それぞれ MID3，CID3，CS3，Ra3，Rb3 とする．ユーザ 3 の 1 次関数は $f_3(x) = Ra3 \cdot x + CID3|CS3$，シェアは $(x3, y3) = (h(MID3|Rb3), f_3(h(MID3|Rb3)))$ 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, y1) 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 2 における ④）．f(x) が正しく復元されたかどうかは，y 切片 CID|CS のチェックサム CS によって確認できる．ここでは，(x1, y1) 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 CID*|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) しか生成されないため，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．

4.4 シェアの管理

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．

すれちがいリストは携帯ゲーム機内に保管し，OS がリストの管理，送受信を行う．ここで，ユーザが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をプレイするにあたっては，ユーザはプレイ中にそのゲームに関するすれちがい通信が行われることを当然承知している．しかし，そのゲームとは関係のないすれちがい通信まで行われることはユーザも想定していないだろう．このため，すれちがいリストはゲームソフトごとにアイソレーションされることが望ましい．すなわち，あるゲームソフトのプレイ時に発生したすれちがい通信の際に行われるすれちがいリストの交換においては，そのゲームソフトに関するシェアのみが交換される．

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．

4.5 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 2 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，チェックサム CS のビット数，すれちがいリストのサイズ，オーバヘッド，プライバシの観点から考察する．

5.1 CS のビット数

すれちがい通信機能を搭載している代表的な携帯ゲーム機である Nintendo DS をモデルとしてチェックサム CS のビット数 β について考察する．

チェックサムは，CID が正しく復元されたか否かを確認するために CID に連結されるビット列である．例として，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 とユーザ 4 は正規ソフトを使用している場合を考えよう．この場合，提案方式においては，不正ユーザであるユーザ 1 のシェアとユーザ 2 のシェアから CID|CS を復元したときだけ CID と CS が整合し，正規ユーザであるユーザ 3 のシェアとユーザ 4 のシェアから CID|CS の復元を試みた際には CID と CS は整合しないようになっている．しかし，ここで，正規ユーザのシェアから CID|CS の復元を試みた場合にも，$\frac{1}{2^\beta}$ の確率で（2^β 回に 1 回の割合で）CID と CS が整合する，このような誤検知の発生を防ぐためには，β は十分な大きさでなければならない．

ここで，Nintendo DS 対応ソフトの販売本数は 2012 年 9 月末の時点で 917,610,000 本 [7] であることから．ゲームソフト 1 本あたりの総販売本数は 2^{30} 本程度と仮定する．すなわち，ある 1 つのゲームソフトに注目した場合，世の中に出現する正規ユーザのシェアの数は 2^{30} 個と見積もることができ，この中から 2 つの正規ユーザのシェアを選ぶにあたっての組合せ数は ${}_{2^{30}}C_2 \approx 2^{59}$ となる．

以上より，この 2^{59} 通りのいずれの組合せの場合であっても，CID と CS が整合することがないようにするためには，$2^\beta > 2^{59}$ である必要がある．よって，チェックサム CS は 60 ビットと設定する．

次に，コンテンツ識別番号 CID のビット数 α について考察する．今回は CID|CS を 256 ビットと想定しているため，CS を 60 ビットと設定した場合，CID は 196 ビットとなる．ここで，CID はコンテンツを識別するための ID であるので，すべてのゲームソフトで異なる数値となる必要がある．前述のとおり，Nintendo DS 対応ソフトの販売本数は 917,610,000 本であるため，CID の実質的なビット数 α は 30 ビットである．30 ビット分の情報量に対し，196 ビットの空間は十分に大きいため，コンテンツ識別番号が衝突する可能性は無視できるほど小さいと考えてよい．

5.2 すれちがいリストのサイズ

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識別番号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，「すで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ができる．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」という事象ととらえることができる．すなわち，提案方式を用いた際に，あるユーザによる不正者検知が成功する確率は，「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．

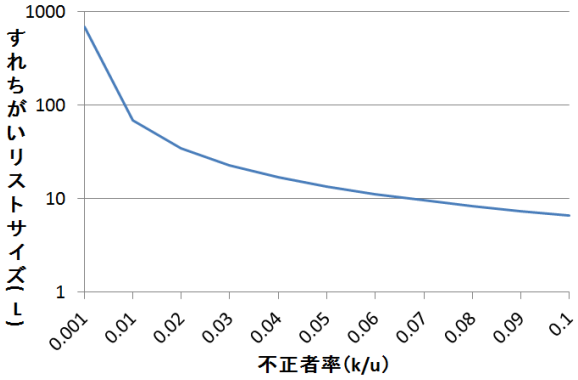

図 3 すれちがいリストのサイズ
Fig. 3 Size of share list.

今回は，不正者検知の確率が 50%を超える場合に「提案方式が十分に機能する」と考えることとする．上記の定式化により，50%以上の確率で不正者を発見することができるという状況は次の不等式で評価できる．

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

式 (1) 中の $\prod_{i=0}^{L-1} \frac{u-k-i}{u-i}$ は，リスト内の L 個のシェアがすべ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（$L \ll k, u$）と仮定した場合，式 (1) を以下のように近似することができる．

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

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．

$$\left(1 - \frac{k}{u}\right)^L \leq \frac{1}{2}$$
$$\log_2 \left(1 - \frac{k}{u}\right)^L \leq \log_2 \frac{1}{2}$$
$$L \geq -\frac{1}{\log_2\left(1 - \frac{k}{u}\right)} \tag{3}$$

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，不正者率 $\frac{k}{u}$（全ユーザ数のうちの不正者の割合）に対して示したものが**図 3** である．

Nintendo DS の販売台数は 2012 年 9 月末の時点で 152,500,000 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 本あ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 1 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 $L \geq -\frac{1}{\log_2(1-\frac{967,383}{152,500,000})} \fallingdotseq 108$ となる．ここで，x と y が各 256 ビットであるため，1 個あたりのシェア (x, y) のデータサイズは 512 ビットとなる．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うち，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．

5.3 オーバヘッド

すれちがい通信時に提案方式を実行する場合のオーバヘッドについて考察する．

5.3.1 通信コスト

提案方式においては，ユーザ自身のシェアとすれちがいリストに保管されている 108 個のシェアがすれちがい通信によって相手に送信される．すなわち，ユーザは合計 109 個のシェアを相手に送信することになるため，そのデータサイズは $512 \times 109 = 55,808$ ビットである．

Nintendo DS は無線通信規格として IEEE 802.11 を使用している [9]．IEEE 802.11 の通信速度の理論値は 2 Mbps であるが，通信速度の実測値を理論値の 5%であると仮定する．その場合，ユーザが送受信するのに要する時間は $\frac{55,808}{2,000,000 \times 0.05} \fallingdotseq 0.6$ 秒となる．以上より，提案方式の通信オーバヘッドは許容範囲内であると考えられる．

5.3.2 処理コスト

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たびに，「自身が所持するすれちがいリストに含まれる 108 個のシェアの各々」と「今受け取ったすれちがい相手のシェア」を用いての不正コピーの検査（図 2 における ④）が実行される．

256 ビットのシェア 2 個から Lagrange 補間によって y 切片を求め，そのチェックサムを検査するという手順を 108 回実行するプログラム[*4]を C 言語で作成し，これを 100 回実行した場合の平均所要時間を調べたところ，約 0.12 秒であった．使用したコンパイラは gcc（MinGW v4.7.2），測定に使用した PC の CPU は Intel Core® [*5] i5-3570（3.40 GHz）である．

Nintendo DS は ARM9 および ARM7 の CPU を搭載している [10] が，その詳細については開示されていない．ARM9 を例にとった場合，そのクロック周波数は速度最適実装において 470 MHz であり [11]，今回の測定に使用した PC の 1/10 である．以上より，現在の携帯ゲーム機において提案方式を実行する際のオーバヘッドは約 1.2 秒であると試算される．

携帯ゲーム機の CPU の高性能化は日進月歩であり，将来的には，提案方式のオーバヘッドは許容範囲内に収まってくると想定される（たとえば，携帯ゲーム機の CPU のクロック周波数が今回の測定に使用した PC の速度に達すれば，提案方式による不正コピー検査は約 0.12 秒で実施可能という見積りになる）．

5.4 プライバシ

分散型不正コピー検知では，ユーザは自身の不正コピー検査用情報を他のユーザの端末に送信することになる．すなわち，提案方式においては，不正コピー検査用情報のプライバシ保護に対して既存のアクティベーション方式以上に配慮が必要となる．本節では，提案方式におけるシェアの安全性について説明する．

5.4.1 シェアに関する情報理論的安全性

提案方式のシェアの x 座標の情報 x=h(MID|Rb) に対しては，2n ビット入力，n ビット出力のハッシュ関数 h(w) が用いられている．すなわち，定性的には，h(w) においては平均 2^n 個の入力が同じハッシュ値として出力されることになる．よって，h(w) の出力を観測した後の「MID と CID に関する事後エントロピ」は約 n ビットである．すなわち，プライバシ情報となる MID（n ビット）は，（おおよそ）情報理論的に安全であるといえる．

シェアの y 座標の情報 $y = Ra \cdot x + CID|CS$ に対しては，秘密分散によって y 切片である CID|CS が情報理論的に保護される．すなわち，プライバシ情報となる CID は情報理論的に安全であるといえる．

5.4.2 トレーサビリティに対する安全性

同一の正規ユーザからの複数のシェアに対して，名寄せが不可能であることを証明する．すなわち，攻撃者にとっての目的は，異なるシェアにおける MID の一致の判別である．攻撃者の知識はシェアのみであり，MID，CID は攻撃者にとっては未知である．また，MID と CID は独立である．同じく，MID と Ra，MID と Rb もそれぞれ独立である．

説明を簡単にするため，ゲーム機 1（個体識別番号：MID1）

[*4] C 言語の整数変数は 64 ビットまでであるため，実際には，64 ビットのシェア 2 個から Lagrange 補間によって y 切片を求め，そのチェックサムを検査するという手順のプログラムを作成した．乗算の計算オーダが $O(n^2)$ であることに鑑み，64 ビット版のプログラムの平均所要時間を 16 倍することによって，256 ビット版のプログラムの平均所要時間を見積もっている．なお，Lagrange 補間については文献 [9] を参考にした．

[*5] Core は Intel Corporation の登録商標．

を所有するユーザ 1 が，ゲームソフト 1（コンテンツ識別番号：CID1，コンテンツ乱数：Ra1，Rb1）とソフト 2（コンテンツ識別番号：CID2，コンテンツ乱数：Ra2，Rb2）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 から発信されるシェア $(x1, y1)$ とソフト 2 のプレイ中にゲーム機 1 から発信されるシェア $(x2, y2)$ は，それぞれ

$$(h(MID1|Rb1), Ra1 \cdot h(MID1|Rb1) + CID1|CS),$$
$$(h(MID1|Rb2), Ra2 \cdot h(MID1|Rb2) + CID2|CS)$$

となる．

ある日時 t1 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（ユーザ i は，ユーザ 1 からシェア $(x1, y1)$ を受信），その後，別の日時 t2 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（ユーザ i は，ユーザ 1 からシェア $(x2, y2)$ を受信）とする．その際に，もしユーザ i が，シェア $(x1, y1)$ と $(x2, y2)$ から「t1 ですれちがったユーザと t2 ですれちがったユーザが実は同一人物（ユーザ 1）である」ことを同定できてしまうと，トレーサビリティに関するプライバシ問題が発生することになる．

そこで，すれちがい通信によって交換されるシェア (x, y) から，ユーザを特定する情報 MID が漏洩することがないか検証する．

x1 においては，MID1 が Rb1 によってマスクされたうえで，ハッシュ関数 $h(\cdot)$ 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（攻撃者）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．

y は x に従属する情報（$y = Ra \cdot x + CID|CS$）であり，攻撃者が y を観測しても，x が有する「MID に関する情報量」以上の情報は得られない．よって，x1 と x2 から MID の情報が漏れないのであれば，y1 と y2 からも MID の情報が漏れることはない．

すなわち，t1 でユーザ 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，t2 でユーザ 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（攻撃者）はその際に受信したシェア $(x1, y1)$ と $(x2, y2)$ からすれちがったユーザが同一人物であったかどうかを知ることはできない．

6. まとめと今後の課題

本論文では，代表的な不正コピー検知技術である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検知に用いられない理由を考察し，その課題を解決する方式として，携帯ゲーム機のすれちがい通信を用いた分散型不正コピー検知方式を提案した．提案方式においては，各ゲーム端末がすれちがい通信によって不正コピー検査用情報をお互いに交換し，異なる個体識別番号（MID）を持つ複数の携帯ゲーム機上で，同一のコンテンツ識別番号（CID）を持つゲームソフトが起動していることが発覚した場合に，その不正コピーが暴かれる．提案方式の可用性をすれちがいリストのサイズ，通信コストと処理コストのオーバヘッド，プライバシの観点から考察した結果，その有用性を確認することができた．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っていきたい．

ゲームソフトの不正コピーにおいては，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が，現行のアクティベーションではその点について考慮されていない．そのため，提案方式では，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といった仕組みを採用した．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．また，法律で規制するなどの「従来の対応」を「ソーシャルな対応」と併用するようなアプローチについても検討していきたい．

提案方式は，すれちがい通信を用いて不正コピー検査用情報をユーザ間で交換することで不正コピーを検知する仕組みとなっている．そのため，不正者がすれちがい通信機能を使用しない場合には，提案方式は機能しない．このため，提案方式を実装する場合は，ゲームを遊ぶうえでのすれちがい通信の重要度（すれちがい通信がゲームの楽しさにどれくらい直結するか）を上げるなど，ユーザにすれちがい通信を利用してもらう工夫がゲームソフト開発者側に必要となる．

また，提案方式は，ある特定のゲームソフトを複数の携帯ゲーム機でプレイした場合に，それを不正コピーとして検出する仕組みとなっている．このため，ゲームソフトを友人から借りた場合，中古のゲームソフトを購入した場合，携帯ゲームを買い替えた場合などにおいては，不正コピーをしていないにもかかわらず，提案方式によって不正コピーとして誤検知されてしまう．この問題の解決法としては，「不正コピーの場合は同時刻に複数のユーザが不正コピー品を起動しうるが，ゲームソフトの貸借，中古売買，ゲーム機の買い替えの場合はそのゲームで遊んでいるユーザは 1 時刻で 1 人である」ことを利用し，提案方式に排他的制御を導入する方法が考えられる．

謝辞 本論文 5 章における評価プログラムの作成，実行にあたり，本学在籍の小林真也氏にご協力いただきました．心より感謝いたします．

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 (2010).

[2] マイクロソフト：Windows XP プロダクトアクティベーション，入手先 ⟨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，入手先 ⟨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？，入手先 ⟨http://jp-playstation.custhelp.com/app/answers/detail/a_id/193⟩.
[5] Johnson, D.B., Maltz, D.A., Hu, Y.C. and Jetcheva, J.G.: The DynamiCCource Routing Protocol for Mobile Ad Hoc Networks, Internet Draft，draft-ietf-manet-dsr-07.txt (Feb. 2002), available from ⟨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 (1999).
[7] 任天堂株式会社：平成 25 年 3 月期第 2 四半期決算短信，入手先 ⟨http://www.nintendo.co.jp/ir/pdf/2012/121024.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，入手先 ⟨http://www.cesa.or.jp/uploads/2010/ihoufukusei.pdf⟩.
[9] 土井 洋：秘密分散法とその応用について，情報セキュリティ総合科学，Vol.4, pp.137–149 (2012). 入手先 ⟨http://www.iisec.ac.jp/proc/vol0004/doi.pdf⟩.
[10] 任天堂株式会社：ニンテンドー DS：スペック，入手先 ⟨http://www.nintendo.co.jp/ds/spec/index.html⟩.
[11] ARM Holdings：ARM968 プロセッサ – ARM，入手先 ⟨http://www.arm.com/ja/products/processors/classic/arm9/arm968.php⟩.

西垣 正勝 （正会員）

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学院修士課程修了．1995 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．同講師，助教授の後，2006 年より同創造科学技術大学院助教授．2007 年同准教授，2010 年同教授，2013 年同大学院情報学研究科教授．博士（工学）．情報セキュリティ全般，特にヒューマニクスセキュリティ，メディアセキュリティ，ネットワークセキュリティ等に関する研究に従事．2013 年より情報処理学会コンピュータセキュリティ研究会主査．

本部 栄成

2011 年静岡大学情報学部情報科学科卒業．2013 年同大学大学院修士課程修了．在学中，情報セキュリティの研究に従事．

米山 裕太

2012 年静岡大学情報学部卒業．現在，同大学大学院修士課程．情報セキュリティに関する研究に従事．

高橋 健太

1998 年東京大学理学部情報科学科卒業．2000 年同大学大学院理学系研究科情報科学専攻修士課程修了．同年（株）日立製作所入社．以来，同横浜研究所（旧システム開発研究所）にて生体認証および情報セキュリティの研究開発に従事．2012 年東京大学大学院情報理工学系研究科博士後期課程修了．2008 年度情報処理学会論文賞受賞．電子情報通信学会会員．博士（情報理工学）．