携帯ゲーム機のすれちがい通信を用いた semi 分散型アクティベーションの提案

本部栄成† 高橋健太†† 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
††株式会社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
†††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 コンテンツ保護のためのオンラインアクティベーションには，ネットワーク環境下にないユーザがアクティベーションを実行することができないという可用性の問題や，ユーザの持つコンテンツと端末の情報をサーバに届け出させることによるプライバシの問題などが存在している．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 semi 分散型アクティベーションを提案する．提案方式では，ゲームソフトとゲーム機の紐付け情報を秘密分散によって分割し，そのシェアをすれちがい通信によってユーザ間で交換する．すべてのシェアはネットワーク環境下にあるゲーム機を経由してサーバに集約され，不正コピーを行ったユーザの情報のみがサーバ側で暴かれる．また，提案方式によって発見された不正者に対しては，すれちがい通信を用いて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の低下の問題に対する改善を図る．

A semi-distributed product activation using direct communication on portable game machines

Eisei Honbu† Kenta Takahashi†† 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 Science and Technology, Shizuoka University
3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan

Abstract Software protection by online product activation has problems regarding availability and privacy. To cope with the problems, this paper proposes a semi-distributed product activation scheme using direct communication on portable game machines. In the proposed scheme, the link information of a software ID and a machine ID is split into shares on every game machines by secret sharing, and each shares are exchanged with other users using the direct communication channel as they are passing each other. All shares are aggregated to a verification server through every game machines in online, and the link information only with respect to illegal copy users will be disclosed in the server. The illegal users' information is published so that all game users can recognize illegal game 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®[i] 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普及している[2]．しかし，オンラインアクティベーションには，インターネット環境下にないユーザがアクティベーションを実行することができないという可用性の問題と，ユーザの持つコンテンツと端末の情報をサーバに届けさせることによるプライバシの問題が存在する.

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 semi 分散型アクティベーションを提案する．提案方式では，ゲームソフトとゲーム機の紐付け情報を秘密分散によって分割し，そのシェアをすれちがい通信によってユーザ間で交換する．すべてのシェアはネットワーク環境下にあるゲーム機を経由してサーバに集約され，不正コピーを行ったユーザの情報のみがサーバ側で暴かれる.

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，ゲームソフトの不正コピー対策においては，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思われる．そこで提案方式では，発見された不正者の情報を公開し，すべて携帯ゲーム機において不正者とのすれ違いを検出可能とする．不正者を人目に晒すことによって，不正者の罪悪感を増長させ，ユーザのモラルの低下の問題に対する改善を図る.

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　要素技術

2.1　オンラインアクティベーション

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，現在のコンテンツ保護技術の主流の一つとなっている.

Microsoft の方式を例に採り，アクティベーションの実行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全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全てを把握しておく．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．メーカはこの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．メーカはこの登録の際に，使用されたシリアル番号が出荷したものに含まれるかを照合し，シリアル番号の正当性を確認する．また，シリアル番号と端末情報の組をすでにサーバに登録されているデータと比較することで，ソフトウェアの不正コピーを検知することができる．メーカが正規利用と判断した場合にのみ，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可能となる.

[i] Windows は米国 Microsoft Corporation の登録商標です

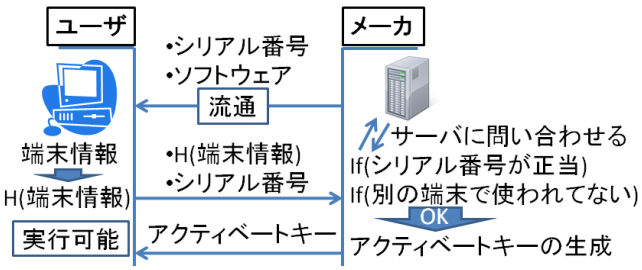

図 1　既存のアクティベーションの流れ

アクティベーションの実行には，サーバとユーザの情報のやり取りをネットワークを介して行う必要がある．しかしながら，全てのユーザの端末が常時ネットワーク環境下にあるとは限らない．そのような場合においては，アクティベーションを実行することができないという可用性の問題がある．また，サーバは不正者だけでなく，正規ユーザの端末情報とソフトウェアの紐付け情報も把握することができる．このため，トレーサビリティに関するプライバシの問題もあるといえる．

2.2　すれちがい通信

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どうし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通信技術である．

任天堂から販売されている Nintendo DS®[ii]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®[iii]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 (The 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，不正者が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ず，この結果，不正者自身の情報が他のゲーム機に送信されることとなる．

2.3　秘密分散

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]．n-out-of-m 秘密分散では，m 個に分割したシェアの内，n 個以上のシェアを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 n－1 次多項式 f(x)を構成し，互いに異なる m 個のサンプルポイント $x_1,\cdots,x_n$ における $f(x_1)$, $\cdots,f(x_n)$をシェアとして生成する．m 個のシェアの内，n 個のシェアが分かれば，Lagrange 補間によって f(x)を特定でき，秘密情報(y 切片)が求まる．

3　semi 分散型アクティベーション

現行のアクティベーションの有する可用性およびプライバシの問題を解決する semi 分散型アクティベーションを提案する．

3.1　前提

携帯ゲーム機がすれちがい通信の際に利用する IP アドレスは，ゲーム機ごとに異なる固定値であり，不正者が任意に変更できない．提案方式では，この IP アドレスをゲーム機の個体識別番号 MID として用いる．

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，各ゲームソフトに対して 2 種類のコンテンツ ID(CIDa と CIDb)が割り当てられ，CIDb をゲームソフトの個体識別番号とし

[ii] Nintendo DS は任天堂(株)の登録商標です
[iii] PSP は 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す

て，CIDa をゲームソフト固有の定数として用いる．CIDa，CIDb は 256bit の空間からランダムに生成される．

IP アドレス（ゲーム機の個体識別番号）とコンテンツ ID（ゲームソフトの個体識別番号）の重複を検査するためのサーバが用意される．次節以降で詳述する手順によって，この検査に必要となる情報が各ゲーム機からサーバに届けられる．各ゲームソフトの中にその手順を実行するためのルーチンもプログラミングされている．

「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．

提案方式では，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，その内容を改竄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．

3.2　ゲーム機からの紐付け情報の発信

提案方式においても，従来のアクティベーションと同様，「ゲーム機の個体識別番号 MID」と「ゲームソフトの個体識別番号 CIDb」を紐付けた情報（以下，「紐付け情報」と記す）をサーバに提出し，サーバ側でその重複を検査することによって不正コピーを検出する．

ただし，ユーザのプライバシを確保するために，提案方式ではこの紐付け情報を CIDb によって暗号化する．その上で，CIDb については 2-out-of-2 秘密分散を用いた秘匿化を行い，複数のゲーム機が同じゲームソフトを利用しているときのみ，サーバが CIDb を復元することを可能とする．また，ネットワーク環境下にないゲーム機からも紐付け情報を収集することを可能にするために，提案方式ではこの紐付け情報をすれちがい通信によってゲーム機間で交換する．交換された情報はネットワーク環境下にあるゲーム機を経由してサーバに集約され，不正コピーを行ったユーザの情報のみがサーバ側で暴かれる．

具体的な手順を以下に記す．

まず，各ゲーム機において，MID と CIDb の紐付け情報を $E_{CIDb}(MID)$という形で作成するとともに，一次関数 $f(x)=CIDa \cdot x+CIDb$ を生成し，その直線上の 1 点 $(x,y)=(h(MID), f(h(MID)))$を算出する．ここで，$E_k(w)$は共通鍵 k によるメッセージ w の暗号化を示し，h(w)はメッセージ w のハッシュ値を表す．コンテンツ ID（CIDa と CIDb）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一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，x=h(MID)の値が一致することはない．

次に，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$\{H(CIDb), (x,y), E_{CIDb}(MID)\}$の 3 つ組を送信する．同時に，相手のゲーム機の 3 つ組を受信する．また，各ゲーム機は，ネットワーク環境下にある場合には，自身の 3 つ組，および，今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 3 つ組をサーバに送信する．これによってサーバには，（すれちがい通信を行ってはいるが）ネットワーク環境下にないゲーム機からの情報も集約されることになる．なお，3 つ組情報は他のゲーム機とすれ違う度に発信されるため，1 つのゲーム機の 3 つ組情報が他のゲーム機を経由して何度もサーバに届き得る．1 つのゲーム機で同じゲームソフトを使用している限り，そのゲーム機から発信される 3 つ組情報は同一であるため，サーバ側で同一の 3 つ組情報が 2 通以上届いた場合には，2 通目以降の 3 つ組情報を削除してしまって構わな

い.

3.3　サーバによる紐付け情報の重複検査

サーバに集約された3つ組情報を用いて，サーバ側で紐付け情報の重複を検査する手順を以下に示す(図2).

前節で述べたように，不正コピー品と正規品は同じコンテンツ ID を持つことから，不正コピー品を各自のゲーム機で使用している不正者間においては H(CIDb)の値，および，一次関数 f(x)=CIDa・x+CIDb は同一であり，x=h(MID)の値のみが異なる.

簡単のために，ユーザ 1 のゲームソフトをユーザ 2 が不正コピーした状況を仮定する. ユーザ1と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*とすると，ユーザ1と2の3つ組情報はそれぞれ，
{H(CIDb*), (x1, y1), E_{CIDb*}(MID1)},
{H(CIDb*), (x2, y2), E_{CIDb*}(MID2)}
となる. ここで，x1=h(MID1)，x2=h(MID2)，
y1=f(x1)=CIDa*・x1+CIDb*,
y2=f(x2)=CIDa*・x2+CIDb*である.

よってサーバは，集約された3つ組情報の集合の中から等しい H(CIDb*)を持つものを抽出した上で，そこに含まれる(x1,y1)と(x2,y2)から一次関数 f(x)を復元し，その y 切片 CIDb*を得ることができる. これにより，サーバは E_{CIDb*}(MID1)および E_{CIDb*}(MID2)を復号することができ，不正者であるユーザ 1 と 2 の紐付け情報(MID1 も MID2 も CIDb*を使用しているという事実)を暴露することができる.

もしユーザ 1 と 2 が共に正規ユーザであり，使用しているコンテンツ ID が異なっていた場合には，それぞれのゲーム機において生成される一次関数は異なった関数となるため，(x1,y1)と(x2,y2)から一次関数(およびその y 切片)を復元することはできず，ユーザ 1 と 2 の紐付け情報は守られる.

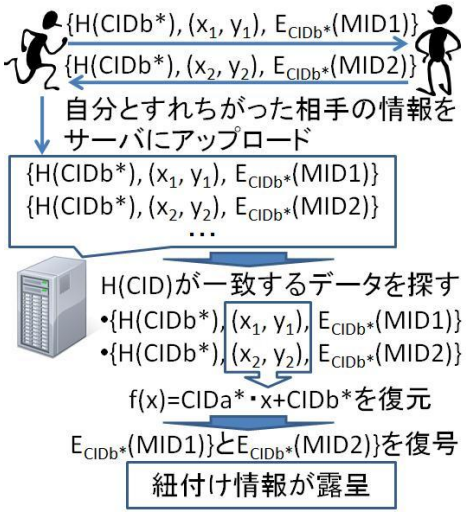

図 2　サーバでの紐付け情報の重複検査

3.4　不正者に対する抑制

サーバは明らかになった不正者の MID と CIDb をブラックリストとして登録する. 提案方式ではゲーム機の IP アドレスを MID として使用しているため，これ以降の時点で当該 IP アドレス(MID)を有するゲーム機がサーバにアクセスしてきた際にこれを検知し，当該ゲームソフトの実行をディスエイブルするためのフラグを当該ゲーム機に書き込むことができる.

さらにサーバは，サーバにアクセスしてきた正規ユーザの携帯ゲーム機にも不正者のブラックリスト(MID と CIDb の組)を送信する. このブラックリストはすれちがい通信の際に交換され，ネットワーク環境下にないゲーム機にも届けられる. この結果，すべてのゲーム機が，すれちがい通信を行う際に通信相手の IP アドレスがブラックリスト内に含まれているか否かを確認することによって，相手が不正者であるかどうかを検査することが可能になる.

正規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. 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と期待される．

4　提案方式の改良

提案方式においては，暗号化された紐付け情報 E_{CIDb}(MID)がゲーム機間で交換される．すなわち，紐付け情報のプライバシは計算量的にその安全性が確保されている．このため，悪意のあるゲーム機が E_{CIDb}(MID)の解読を試みた場合に，解読に成功する可能性がゼロではない．これに対し，紐付け情報を秘密分散によって分割することによって，情報理論的安全性に基づく形で紐付け情報を保護することができる．

紐付け情報(MID,CIDb)を 2-out-of-2 秘密分散で分割した場合を例に採って説明する．

紐付け情報を秘密分散によって分割した際のシェアを S1 と S2 とする．S1 と S2 のそれぞれに対して乱数 R1, R2 を割り振る．各ゲーム機において生成される 3 つ組を 3.2 節の形から{H(CIDb), (x,y), E_{CIDb}(R1,R2)}に変更する．そして，この 3 つ組の情報と共に，{R1,S1}および{R2,S2}という情報を生成する．

各ゲーム機は，他のゲーム機とすれ違う度に，({H(CIDb),(x,y),E_{CIDb}(R1,R2)},{R1,S1})，または，({H(CIDb),(x,y),E_{CIDb}(R1,R2)},{R2,S2})のいずれかを通信相手と交換する．

サーバにはすべてのゲーム機からの 3 つ組情報{H(CIDb),(x,y),E_{CIDb}(R1,R2)}とシェア情報{R1,S2}，{R2,S2}が集められる．3.3 節と同様の手法で不正者の 3 つ組情報から R1 と R2 が求まる．更にサーバは，この R1 と R2 をインデックス情報として，数多のシェア情報の中から不正者のシェア情報{R1,S2}，{R2,S2}を発見することができ，S1 と S2 から紐付け情報(MID,CIDb)を復元することが可能となる．

5　まとめと今後の課題

本稿では，現行のアクティベーションに対し，携帯ゲーム機のすれちがい通信を用いた semi 分散型アクティベーションを提案し，その基本形とその改良案を示した．提案方式では，ゲームソフトとゲーム機の紐付け情報を秘密分散によって分割し，そのシェアをすれちがい通信によってユーザ間で交換する．すべてのシェアはネットワーク環境下にあるゲーム機を経由してサーバに集約され，不正コピーを行ったユーザの情報のみがサーバ側で暴かれる．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方法となっている．

今後はシミュレーションなどによって提案方式の効果を評価していく予定である．また，提案方式では，ユーザ間の注意・警告などから生じる罪悪感によって不正者が不正コピーを躊躇するようになるという前提を置いている．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

[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.