Vol.2011-DPS-146 No.30
Vol.2011-CSEC-52 No.30
2011/3/11

携帯ゲーム機のすれちがい通信を用いたソーシャルな不正コピー対策

本部栄成[†]　渡邊幸聖[††]　小田 雅洋[††]　西垣正勝[†††]

近年，マジコンと呼ばれる機器の登場により，ゲームソフトの不正コピーの被害が増加している．ネットゲームであればサーバによる認証を用いて正規ユーザと不正ユーザを切り分けることが可能であるが，スタンドアロン型のゲームソフトに対しては不正コピーに対抗する有効な技術が存在しないというのが現状である．そこで本稿では，不正ユーザの心理に訴えかけるタイプのソーシャルな不正コピー対策を提案する．ゲームソフトが自身の真正性をコード署名を用いてセルフチェックし，その結果を携帯ゲーム機に搭載されているすれちがい通信を通じて他のゲーム機と共有することによって，不正者を一般ユーザの目にさらす．不正者は，罪悪感から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．本方式は，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コンテンツに適用可能である．本稿では本方式の有用性を統計的側面から評価する．

A social countermeasure to prevent illegal game software copies using direct communication on portable game machines

Eisei Honbu[†]　Yoshimasa Watanabe[††]　Masahiro Oda[††]
Masakatsu Nishigaki[†††]

In recent years, the damage from illegal copies of the game software increases due to the appearance of a device called “magic computer”. If the game software is an online game which connects into the internet, we can distinguish between normal users and illegal users with account authentication performed on a game server. However there is no way to block illegal copy of the stand-alone type software which doesn’t connect in the internet. In this paper, we propose a social countermeasure to illegal copies of a type that appeals to illegal user’s psychology. Game software checks itself with code signature, and they send these results to the other by directly communicating with each other. By sharing the information among game machines, all game users can recognize illegal game users. We expect illegal users halt to use illegal copy because they feel a sense of guilt. This scheme can be applied to contents which contain game events which appear in the exchange process. In this paper, we evaluate this scheme with a multi agent simulation.

1. はじめに

近年，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．調査によると不正コピーによるゲームソフトにおける被害額は 3500 億円にも上ると報告されている[1]．ゲームソフトの被害が増加している原因としてマジコンと呼ばれる機器の登場が挙げられている[1]．マジコンとはゲームソフトのコピーをニンテンドーDS などの携帯ゲーム機上で起動させる機器の総称である．本来，ニンテンドーDS にはコピーされたゲームの実行を防ぐアクセスコントロールが備えられている．しかしながら，マジコンを用いることで，このアクセスコントロールを回避し，コピーされたゲームを起動することができる．

携帯ゲーム機のゲームソフトの不正利用という問題に対し，様々な技術的対策が行われているが，上述のマジコンに代表されるように，不正と対策のいたちごっこが続く状態となっている．もちろん法的な対策も講じられており，2010 年 1 月 1 日には著作権法が改正され不正ダウンロード違法化が施行された[2]．しかしながら，ファイル共有ソフトの不正ユーザ数は施行直後一時的に減少したものの，再度増加傾向に向かっており十分な効果は得られていない[3]．

オンラインゲームのようにネットワークに接続する形態のゲームであれば，サーバによるユーザ認証を行うことで不正ユーザの利用を防ぐことが可能である．しかし，ネットワークに接続しないスタンドアロン型のゲームには適用できない．

スタンドアロン型ゲームの保護技術としてはコード署名[4]が挙げられる．「ゲームソフトのプログラム」と「購入者のユーザ ID（購入者が所持する携帯ゲーム機のプロダクト ID）」を連結したデータに対する電子署名を生成しておくことにより，署名チェックに失敗したゲームソフトについては，その実行を許可しないようにすることができる．なお，署名を検査する機構がクラックされてしまうとこの対策は無効化され

[†]静岡大学情報学部，〒432-8011 浜松市中区城北 3-5-1，
Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan
[††]静岡大学大学院情報学研究科，〒432-8011 浜松市中区城北 3-5-1，
Graduate school of Informatics, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan
[†††]静岡大学創造科学技術大学院，〒432-8011 浜松市中区城北 3-5-1，
Graduate School of Science and Technology, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan

ⓒ 2011 Information Processing Society of Japan

Vol.2011-DPS-146 No.30
Vol.2011-CSEC-52 No.30
2011/3/11

てしまうため，署名検査機構は携帯ゲーム機内にハードウエア的に作り込む形で実装する必要がある．

しかしながら，スタンドアロン型ゲームの場合，一般的に，ゲームソフト購入時に購入者のユーザ ID をゲームソフトとバインドするような販売形態は採られていない．このため，ゲームを使用しているユーザが本当にそのゲームを購入した者であるかどうかをチェックする術がなく，コード署名による不正コピー防止を実効的に運用することは難しい．したがって，スタンドアロン型ゲームの不正コピー対策においては，ユーザ ID が埋め込まれていない状態のゲームソフトに対して，「どのユーザがどのゲームソフトを購入したのか」という情報を管理する仕組みをいかに構築するかが鍵となる．そこで本稿では，各ゲームソフトがゲーム実行中に自身のコンテンツ ID をすれちがい通信機能によって発信しあうことによって，携帯ゲーム機間でお互いのゲームソフトに関する情報を共有し，不正コピー品を利用しているユーザを発見する方法を提案する．

コンテンツ ID はゲームソフトごとに割り振られる固有番号であり，同じゲームであってもソフトウエアごとに異なる．ここでは，「ゲームソフトのプログラム」と「コンテンツ ID」を連結したデータに対してコード署名が付されるという運用を想定する．従来からゲームソフトにはソフトウエア一本一本にロット番号が割り振られた形で販売されているため，ソフトウエアごとに異なるコンテンツ ID を付与した上でコード署名を施して販売するという想定は非現実的ではないと考える．すれちがい通信は携帯ゲーム機に搭載されている短距離通信技術であり，すれちがい通信によって特別なイベントが発生したり，ユーザにとって有益な情報や共有感等がもたらされるように作られているゲームソフトが数多く存在する．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，不正者自身のゲームソフトのコンテンツ ID が他のゲーム機に送信されることとなる．

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．提案手法は，すれちがい通信を用いてゲーム機間でお互いが所持するゲームソフトのコンテンツ ID を共有し，コンテンツ ID の重複を検査することによって，不正コピー品を使用している不正者の存在を検知する．

提案方式を運用することによって，正規ユーザが不正者とすれちがった際に，不正コピー品の存在が検出されることになる．しかし，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，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．そこで本稿では，不正コピー品が検知された場合には，不正者（不正コピー品を使用している携帯ゲーム機のユーザ）に注意や警告などのメッセージを表示するとともに，正規ユーザの携帯ゲーム機にも「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という方法を提案する．自分と自分の周辺のユーザがお互いに不正に対して意識的に気をつけ合うことによって，不正者は罪悪感から（または，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期待している．なお，不正者の携帯ゲーム機にメッセージが表示される機構については，不正者にクラックされて無効化されてしまわないように，携帯ゲーム機内にハードウエア的に作り込む形で実装することが必要である．

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．本稿では，マルチエージェントシミュレーションを通じて，提案方式の有用性を統計的側面から評価する．

2. 既存方式：ユーザ ID を含むコード署名を用いた方式

ユーザがゲームソフトを購入する際に，販売者がゲームソフトに購入者のユーザ ID を埋め込んだ形でゲームソフトのコード署名を生成することができる場合は，この署名を検査することによってスタンドアロン型ゲームの不正コピーをチェック可能である．なお，署名検査機構は携帯ゲーム機内にハードウエア的に作り込む形で実装する必要がある．

まず，ゲームソフト購入時に行われる情報のやりとりについて述べる．ゲームソフト購入者は購入時に販売者に自身のユーザ ID（購入者が所持する携帯ゲーム機のプロダクト ID）を送る．販売者は，ゲームソフト（プログラム）と購入者のユーザ ID に対するコード署名を販売者の秘密鍵を用いて生成する．最後に，販売者はゲームソフトと共に，生成した署名とその署名を検証する公開鍵，公開鍵の証明書を購入者に送る．

ゲームソフトのプログラムを GS，購入者のユーザ ID を UID，GS と UID に対する販売者のコード署名を sign(UID, GS)，署名に用いる販売者の秘密鍵を Sk，署名を検証する公開鍵を Pk，Pk に対する証明書を CERT とし，既存方式のゲームソフト購入時の手順を以下で述べる（図 1）．

STEP1-1 購入者は UID を販売者に送る．
STEP1-2 販売者は Sk を用いて UID と GS から sign(UID, GS)を生成する
STEP1-3 販売者は GS，sign(UID, GS)，Pk，CERT を購入者に送る．

ⓒ 2011 Information Processing Society of Japan

Vol.2011-DPS-146 No.30
Vol.2011-CSEC-52 No.30
2011/3/11

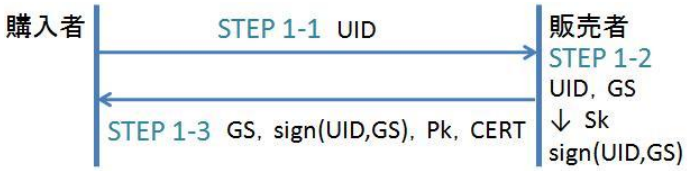

図 1　販売時の署名生成
Figure 1 Creation of code signing

次に，購入時に得た情報を用いることで，ユーザの正当性を確認する手法について述べる．購入時に販売者から送られてきたコード署名にはユーザ ID（購入者が所持する携帯ゲーム機のプロダクト ID）が含まれているため，ゲーム機内で署名をセルフチェックすることによりユーザの所有しているゲームソフトの正当性を検査することができる．このとき，公開鍵の正当性の検査も同時に行う必要がある．そのため，携帯ゲーム機にはゲーム機製造会社の公開鍵に対する証明書 $CERT_{ROOT}$ が出荷時に埋め込まれているとする．販売者の公開鍵 Pk の証明書 CERT は，ゲーム機製造会社によって発行された(ゲーム機製造会社の秘密鍵よって署名が付されている)ものであるか，または，$CERT_{ROOT}$ から CERT までの信頼の連鎖を辿るために必要となるすべての証明書を含むものでなければならない．

ゲームソフト GS を購入したユーザの携帯ゲーム機を GM とする．GS には，sign(UID, GS)，Pk，CERT が付随している．GM に割り振られているプロダクト ID は UID である．GM には，UID と $CERT_{ROOT}$ が備わっている．検証時の手順を以下に述べる（図 2）．

STEP 2-1 GM は CERT の正当性を $CERT_{ROOT}$ によって検証する．検証を通過しなかった場合，GS の実行を中止する．

STEP 2-2 GM は GS および Pk と自身の UID を用いて sign(UID, GS)の正当性を検証する．検証に失敗した場合，GS の実行を中止する．

あるユーザが正規に購入したゲームソフト（GS，sign(UID, GS)，Pk，CERT）を，不正者が何らかの方法で入手したとする．しかし，このゲームソフトは正規購入者の携帯ゲーム機（プロダクト ID が UID であるゲーム機）とバインドされてしまっているため，不正者は自分のゲーム機でこのゲームを実行することができない．

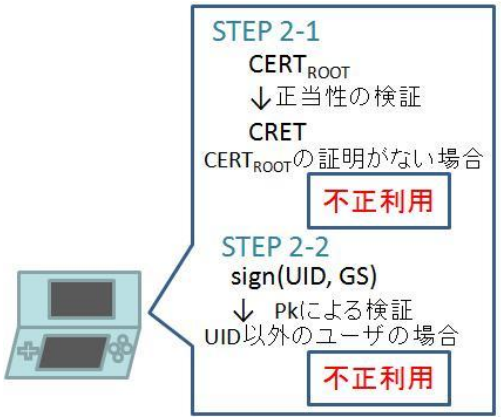

図 2　コード署名を用いた方式による不正利用検知
Figure 2 Detection of illegal copy with code signing

しかしながら，スタンドアロン型ゲームの場合，一般的に，ゲームソフト購入時に購入者のユーザ ID をゲームソフトとバインドするような販売形態は採られていない．また，この方式は正規購入者であっても，購入時に登録したゲーム機でしかゲームソフトを実行できない．このため，正規ユーザが他人のゲーム機を借りてゲームで遊ぶ場合や，ゲーム機を買い換えた場合に正規ユーザの利便性が担保できない．このため，この方式の運用は現実的には難しいといえる．

3. 提案方式：すれちがいリスト方式

スタンドアロン型ゲームの不正コピー対策においては，ユーザ ID が埋め込まれていない状態のゲームソフトに対して，「どのユーザがどのゲームソフトを購入したのか」という情報を管理する仕組みをいかに構築するかが鍵となる．本章では，各ゲームソフトがゲーム実行中に自身のコンテンツ ID をすれちがい通信機能によって発信しあうことによって，携帯ゲーム機間でお互いのゲームソフトに関する情報を共有し，不正コピー品を利用しているユーザを発見する方法を提案する．本方式を「すれちがいリスト方式」と呼ぶこととする．

3.1 ゲームソフトの販売形態と不正コピー

すれちがいリスト方式においては，すべてのゲームソフトには（同じゲームであっても）それぞれ異なるコンテンツ ID が割り当てられており，その上で，「ゲームソフトのプログラム」と「コンテンツ ID」を連結したデータに対してコード署名が付されるという運用を想定する．従来からゲームソフトにはソフトウエア一本一本にロット

ⓒ 2011 Information Processing Society of Japan

Vol.2011-DPS-146 No.30
Vol.2011-CSEC-52 No.30
2011/3/11

番号が割り振られた形で販売されているため，ソフトウエアごとに異なるコンテンツ ID を付与した上でコード署名を施して販売するという想定は非現実的ではないと考える．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．

更に本方式においては，すべての携帯ゲーム機にはコード署名の検査機構がハードウエ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を許可しないという仕様を定める．なお，ゲームソフトに付随する公開鍵証明書を検証するためのトラストアンカとなる公開鍵証明書も，携帯ゲーム機の中に書き換えられない状態で埋め込まれているものとする．

不正ユーザの多くは，ゲームソフトが違法にアップロードされているファイル共有サイトやファイル共有ソフトを用いてインターネット上からダウンロードするといった手段で不正ファイルを入手している．このため，ゲームソフトの不正ダウンロード数は不正アップロード数と比べ膨大であることが予想される．ゆえに，ある一人の不正者によってネットワーク上に不正アップロードされたゲームソフトのデータを，多数の不正者が所持するという状況となっていると考えられる．

提案方式のゲームソフト販売形態においては，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 すれちがい通信

すれちがいリスト方式においては，実際にゲーム機間でのすれちがい通信が発生した際に，お互いのユーザ ID（ゲーム機のプロダクト ID）とゲームソフトのコンテンツ ID の情報も自動的に交換されるように，ゲームソフトがコーディングされていることを想定する．なお，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改竄してユーザ ID およびコンテンツ ID を伏せた形ですれちがい通信を行うようにすることはできない．

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持つユーザどうしが通信範囲にいる場合に Wi-Fi を用いて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．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，プレー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，不正者自身のゲームソフトのコンテンツ ID が他のゲーム機に送信されることとなる．

3.3 すれちがいリストによる不正コピー検知

不正者が何らかの方法で，あるゲームソフトの不正コピー品を入手したとする．3.1 節で述べたように，ゲームソフトはコード署名によって保護されているが，このコード署名はゲームソフトのプログラムとコンテンツ ID の真正性を保証するものである（ゲームソフトの中にはユーザ ID の情報は含まれていない）．よって，正規のゲームソフトを 1 ビットも違わずに複製した不正コピー品はコード署名の検査を通過する．すなわち，不正者はゲームソフトの不正コピー品を自分のゲーム機にて実行することができる．

このため，不正者が他のユーザから隔離された場所にいる限り，不正者は自分が不正コピーしたゲームソフトで遊んでいるという事実を誰にも知られることはない．しかし，3.2 節で述べたように，不正者は他のユーザがいる場所に赴いてすれちがい通信を行わなければ，そのゲームを十分に楽しむことができない．そして，すれ違い通信の結果，不正者自身のユーザ ID（ゲーム機のプロダクト ID）とゲームソフトのコンテンツ ID が他のゲーム機に送信されることとなる．

3.1 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．よって，世の中に出まわっている不正コピー品の数を Ncp とすると，コピー元となった正規のゲームソフト 1 本と合わせて，同時に Ncp+1 個のゲーム機の中に「同じコンテンツ ID を持つゲームソフト」が存在することになる．したがって，すれちがい通信を用いてゲーム機間でお互いが所持するゲームソフトのコンテンツ ID を共有し，コンテンツ ID の重複を検査することによって，不正コピー品を使用している不正者の存在を検知することが可能となる．

ゲームソフトのコンテンツ ID の共有と不正コピー品の検知を行うために，各ゲーム機は，他のゲーム機が所持するゲームソフトの情報を「すれちがいリスト」として保持する．提案方式においては，3.2 節で述べたように，すれちがい通信が発生する度に，相手のゲーム機から「ユーザ ID とコンテンツ ID」が送られてくる．すれちがいリストは，今までにすれちがったゲーム機から受け取ったすべての「ユーザ ID とコンテンツ ID」の情報を羅列したリストである．

説明を分かりやすくするため，以下の具体例を用いて，提案方式によるゲームソフトの不正コピー検知の手順を記す．

1. ユーザ A，B，C，D，E が携帯ゲーム機を持っており，ユーザ A，B，C，D が同種のゲームソフトを購入している状況を想定する．各ユーザのユーザ ID（ゲーム機のプロダクト ID）を UID_A，UID_B，UID_C，UID_D，UID_E，各ユーザのゲームソフトのコンテンツ ID を CID_A，CID_B，CID_C，CID_D とする．
2. ユーザ C が自分のゲームソフトを不正コピーし，ユーザ E に渡したとする．ユーザ E のゲームソフトのコンテンツ ID は CID_C である．
3. ユーザ A は，ゲームのプレイ中に，B，C，D，E の順に他のユーザとすれちが

ⓒ 2011 Information Processing Society of Japan

Vol.2011-DPS-146 No.30
Vol.2011-CSEC-52 No.30
2011/3/11

うとする．

4. ユーザ A がユーザ B とすれちがった時点において，A と B の間でお互いのユーザ ID とコンテンツ ID が交換され，A は「UID_B:CID_B」という情報を受け取る．この時点では A のすれちがいリストは空集合であるため，不正コピー検知のための照合は行われない．A のゲーム機のすれちがいリストには「UID_B:CID_B」という情報が記録される．（同時に，B のゲーム機のすれちがいリストには「UID_A:CID_A」という情報が記録される．）
5. ユーザ A がユーザ C とすれちがった時点で，A が C から受け取る情報は「UID_C:CID_C」である．A のゲーム機は，不正コピー検知のために，自身のすれちがいリスト「UID_B:CID_B」との照合を行う．今回はコンテンツ ID の不正な重複はないため，正規コンテンツであると判定される．A のゲーム機のすれちがいリストに「UID_C:CID_C」が追記され，「UID_B:CID_B，UID_C:CID_C」となる．
6. ユーザ A がユーザ D とすれちがった時点で，A が D から受け取る情報は「UID_D:CID_D」である．A のゲーム機は，不正コピー検知のために，自身のすれちがいリスト「UID_B:CID_B，UID_C:CID_C」との照合を行う．今回も正規コンテンツであると判定される．A のゲーム機のすれちがいリストは「UID_B:CID_B, UID_C:CID_C, UID_D:CID_D」となる．
7. ユーザ A がユーザ E とすれちがった時点においては，E が使っているゲームソフトは C から入手したものであるため，A が受け取る E の情報は「UID_E:CID_C」である．A のゲーム機は，不正コピー検知のために，自身のすれちがいリスト「UID_B:CID_B，UID_C:CID_C，UID_D:CID_D」との照合を行う．UID_C:CID_C とのコンテンツ ID の不正な重複が発見され，今すれちがったユーザが不正コピー品を使用していることが検知される（図 3）．ユーザ A は，UID_C と UID_E のユーザ ID，および，CID_C のコンテンツ ID をブラックリストに登録する．ユーザ A はこれ以後，ユーザ ID が UID_C または UID_E であるゲーム機とすれちがった場合，および，CID_C のコンテンツ ID を持つゲームソフトを使用しているゲーム機とすれちがった場合に，相手のゲーム機を所持するユーザを不正者として検知する．

なお，上記では簡単のためにすれちがいの際に自身の「ユーザ ID とコンテンツ ID」のみが交換されるとして説明しているが，実際の運用では，すれちがいリストの共有率を高めるために，すれちがいの際にお互いの「すれちがいリスト」そのものを交換するという方法を採る．

提案方式は，ユーザ間の連携によって不正コピーを発見する分散協調型不正コピー検知方式となっており，ユーザが自身のユーザ情報を販売者側に登録する必要がなく，かつ，サーバ等と一切の接触を断った形で不正コピーの検知が可能である．

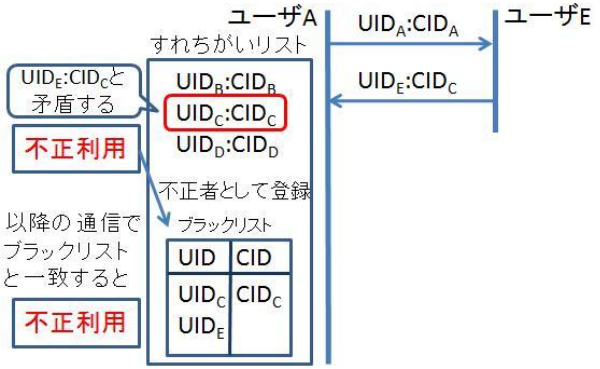

図 3　すれちがいリスト方式による不正者検知
Figure 3 Detection of illegal copy with passing list

3.4 不正者への注意

すれちがいリスト方式の運用によって，ユーザが不正者とすれちがった際に，不正コピー品の存在が検出されることになる．しかし，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，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，不正コピーを検知した場合には，不正者の存在を人目に晒すことによって，不正者の罪悪感を増長させることを狙う．

具体的には，不正コピーが検知された場合に，再度すれちがい通信を用いて，不正者（不正コピー品を使用している携帯ゲーム機のユーザ）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．なお，不正者の携帯ゲーム機にメッセージが表示される機構については，不正者にクラックされて無効化されてしまわないように，携帯ゲーム機内にハードウエア的に作り込む形で実装される．

4. すれちがい通信方式の評価

本節では提案方式の有用性を検証するためにマルチエージェントシミュレーションによる評価を行う．以下では，シミュレーションの目的について述べた後に，シミュレーションで用いるモデルやパラメータを説明し，最後にシミュレーションの結果

ⓒ 2011 Information Processing Society of Japan

Vol.2011-DPS-146 No.30
Vol.2011-CSEC-52 No.30
2011/3/11

について述べる．

4.1 シミュレーションの目的

提案方式では，すれちがい通信によってすれちがいリストの情報を交換し，不正者の検知を行う．ゆえに，提案方式の効果はすれちがい通信の発生頻度に大きく依存する．すれちがい通信の発生頻度は，シミュレーション空間の広さ，エージェント（ゲーム機を所持するユーザ）数，ゲームソフトの不正コピー品の数などのパラメータに相関があると考えられる．よって今回のシミュレーションでは，日本の都心における携帯ゲーム機の不正コピーの現状の数字に基づいて種々のパラメータを設定し，不正ユーザの検知数，すれちがい通信の発生回数，各ゲーム機が所持するすれちがいリストのサイズの観点から提案方式の可用性を評価する．また，すれちがい通信の発生頻度は，エージェントの行動パターンにも左右されるが，今回は簡単のためにランダムウォークモデルを採用した．このため，シミュレーションの結果はシミュレーションの度に異なり得る．よって，各パラメータ設定ごとに 10 回のシミュレーションを行い，その平均を評価結果とした．

4.2 シミュレーション空間とエージェントの動き

シミュレーション空間 Fsim を，x 軸方向の長さ Lx，y 軸方向の長さ Ly によって表される Lx×Ly 平面とする．Fsim は長さ GL 四方のグリッドに仕切られている．Fsim 上のグリッドの格子点に Na 人のエージェントをランダムに配置する（図 5）．各エージェントの動作はランダムウォークであり，ターン毎に上下左右どちらか一方に 1 グリッド移動するか，または，その場に留まる．上・下・左・右・停止の生起確率はすべて 0.2 である．現実世界での人間の行動範囲は限られていると考えられる．そのため，今回はそれぞれのエージェントに，初期位置から x 方向に p*Lx，y 方向に q*Ly の移動制限を設けた．例えば，移動制限の右境界に到達したエージェントは，次のターンで右への移動が生起された場合も，そこに留まることになる（上・下・左・停止の生起確率が 0.2・0.2・0.2・0.4 となることと等価）．ここで p と q はそれぞれ x と y 方向への移動制限変数であり，今回はシミュレーション開始時に各エージェントに対して $0.2 \leqq p \leqq 0.5$，$0.2 \leqq q \leqq 0.5$ の値がランダムに割り当てられる．

あるターンにおいて 2 体のエージェントが同じ格子点上に存在した場合にお互いのすれちがい通信が起きる．今回はすれちがい通信の無線到達距離およびユーザの歩行速度に鑑み，グリッドの大きさ GL は 30m に設定した．

Fsim の大きさは，今回のシミュレーションでは $1km^2$ を想定し，Lx=990m, Ly=1020m とした．グリッドの数は 33×34 となる．エージェント数 Na については，東京都の人口密度が 5,751 人/ km^2[5]であることから，Na=5,751 人とした．

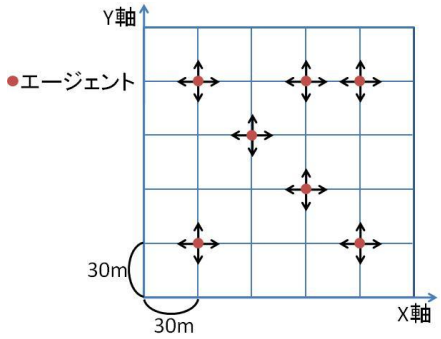

図 4　シミュレーション空間（Lx=150m，Ly=150m，Na=7 人の場合）
Figure 4 Simulation field (Lx=150m, Ly=150m, Na=7)

4.3 シミュレーションパラメータの設定

エージェントの携帯ゲーム機所有率を Rg, 携帯ゲーム機を所有しているエージェントの中で不正コピーを使用しているエージェントの割合を Ri とする．ここで，自身が購入したゲームソフトをファイル共有サイトに違法アップロードした不正者の人数を Ns とする．すなわち，ファイル共有サイトに違法アップロードされているゲームソフトは Ns 個である．他のすべての不正者は，不正コピー品を当該サイトからダウンロードして入手していると考える．よって，Fsim 内に存在するすべての不正コピー品のコンテンツ ID は, Ns 個のゲームソフトの内のいずれかのコンテンツ ID と同じである．また，今回は Ns 個のゲームソフトそれぞれが同じ数だけ不正にダウンロードされたとする．

以上より，Fsim 上に Na 体のエージェントが存在している環境では，Na*Rg 体のエージェントが携帯ゲーム機を所持し，その中の Na*Rg*Ri 体のエージェントがゲームソフトの不正コピーを使用している（すなわち，Fsim 上に存在する不正コピー品の数は Na*Rg*Ri 個）ことになる．Na*Rg*Ri 個の不正コピー品の内，同じコンテンツ ID を持つ不正コピー品はそれぞれ Na*Rg*Ri*1/Ns 個である．

今回のシミュレーションでは，実際に公表されている統計値からこれらのパラメータの値を設定することとした．

携帯ゲーム機所有率 Rg は，任天堂から発売されているニンテンドーDS の売上台数により算出する．平成 22 年 3 月 31 日までのニンテンドーDS の国内累計売上台数は 31,550,000 台であり[6]，日本の人口は 127,767,994 人である．このことから，ニンテンドーDS の所有率は 31,550,000 / 127,767,994≒0.25 となる．よって Rg=0.25 とする．

不正者率 Ri は，違法サイトからの不正ダウンロード件数から算出する．馬場らの報告[7]によると，違法複製ゲームソフトのアップロード・ダウンロードに対する禁止措

ⓒ 2011 Information Processing Society of Japan

Vol.2011-DPS-146 No.30
Vol.2011-CSEC-52 No.30
2011/3/11

置がとられていない 25 のファイル共有サイトを通じてのゲームソフト「ポケットモンスタープラチナ」の合計ダウンロード件数は 2,071,006 ダウンロードであった．したがって，携帯ゲーム機所有者と不正コピー使用者の比は 2,071,006 / 31,550,000≒0.066 となる．よって Ri = 0.066 となる．

ゲームソフトを違法アップロードした不正者の人数 Ns については，適正な統計情報が存在していないため，今回のシミュレーションでは Ns=5 と仮定した．

4.4 シミュレーション結果

今回のシミュレーション環境では，Na*Rg=1437 体のゲーム機（ゲーム機を所持するエージェント）が存在し，その中に Na*Rg*Ri=90 個の不正コピー品が存在する．すべての不正コピー品のコンテンツ ID は 5 種類の内のいずれかであり，同じコンテンツ ID を持つ不正コピー品はそれぞれ Na*Rg*Ri*1/Ns=18 個である．今回のシミュレーションでは，一つの不正コピー品のみに注目し，不正コピー品を所持するエージェント数を 18 とした．

時間（ターン数）とともに 18 個の同一コンテンツ ID を持つ不正コピーの検知数がどのように増加していくのかを図 5 に示した．横軸がターン数，縦軸がどこかで誰かによって 1 度でも検知された不正コピー品の数の累積である．ほとんどの不正コピー品がターン数の早い段階で発見されていることが確認できる．10 回のシミュレーションにおいて平均 30 ターンですべての不正者を（少なくとも誰かが 1 回）検知できており，エージェントの移動距離（エージェントは 1 ターンで 1 グリッド 30m 進むため，30 ターンで 900m 移動する）と日本人の一日あたりの歩数平均[8]から，すべての不正者は 1 日足らずで検知できるという計算となる．

時間（ターン数）ごとにどれくらいのすれちがい通信が発生しているかを図 6 に示した．横軸がターン数，縦軸がそのターンにおいて Fsim 内で発生しているすれちがい通信の総数である．また，不正者への注意のためのすれちがい通信（不正者とすれちがった際に不正者に対して送信される注意メッセージ）についても，時間（ターン数）ごとの発生頻度を図 7 に示した．図 7 より，全ターンを通じて Fsim 中で注意メッセージが発生していることがわかる．よって，不正者は自分の不正に対して複数回に渡って注意を受けているものと考えられる．

時間（ターン数）とともに各ゲーム機が所持するすれちがいリストのサイズがどのように増加していくのかを図 8 に示した．横軸がターン数，縦軸が全ゲーム機が所持するすれ違いリストのサイズの平均である．すれ違いリストのサイズは，リスト内に記録されている「ユーザ ID とコンテンツ ID のバインド情報」のエントリ数である．提案方式ではすれちがいリスト自体を交換するため，リストのサイズは指数関数的に増大するように思えるが，実際にはリストのエントリの数は Fsim 内に存在しているゲーム機の数以上にはならないため，それほど大きなリストサイズが必要となるわけではないことがわかる．また，図 7 と図 8 から，各ゲーム機が所持するすれちがいリストの増加に比例して，不正者の発見能力が向上し，不正者への注意メッセージの送信頻度が上昇していることが見てとれる．

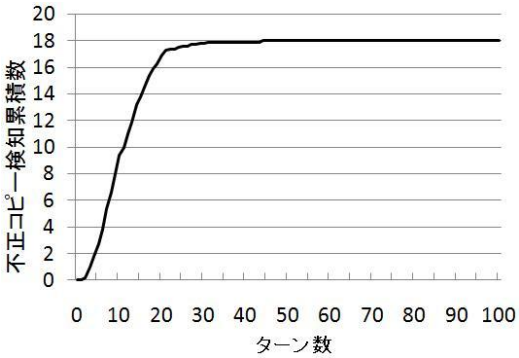

図 5　検知された不正コピーの累積数の遷移
Figure 5 The number of detections for illegal copy

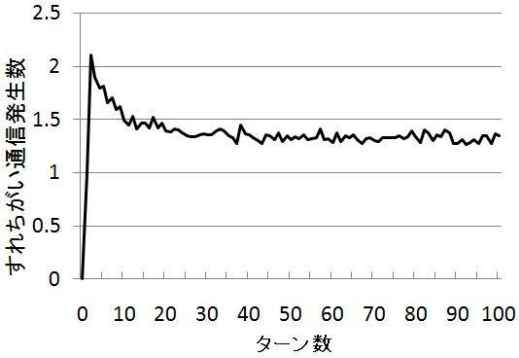

図 6　ターンごとの各ユーザのすれちがい通信の平均発生頻度
Figure 6 The number of direct communications

ⓒ 2011 Information Processing Society of Japan

Vol.2011-DPS-146 No.30
Vol.2011-CSEC-52 No.30
2011/3/11

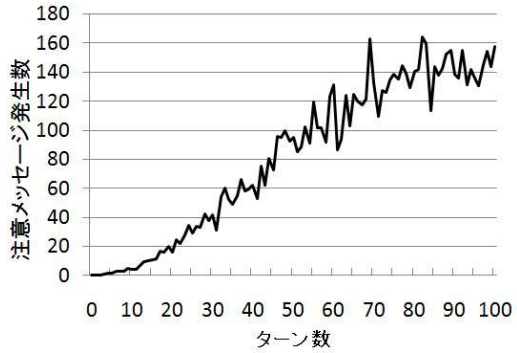

図 7　ターンごとの不正者への注意のためのすれちがい通信の発生総数
Figure 7 The number of direct communications to illegal agents

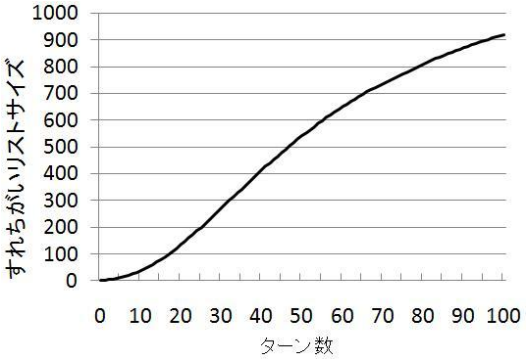

図 8　各ゲーム機が所持するすれちがいリストの平均サイズの遷移
Figure 8 The size of passing lists

5. まとめと今後の課題

本稿では，スタンドアロン型のゲームソフトに対し，携帯ゲーム機に搭載されているすれちがい通信を用いて，ユーザ同士がお互いのゲームソフトの真正性の検証を行うことで不正コピーを検知する方法を提案した. また, 不正コピーを検知した場合は，その不正者に対して不正コピー品の使用に対する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コピーを抑止する.

提案方式の可用性をマルチエージェントシミュレーションによって検証したところ，都市部であれば，提案方式によって比較的短い時間ですべての不正者を検知できることを示した.

今回は首都圏を想定してシミュレーションを行ったが，人口密度は都市の規模によって異なる. また, エージェントの移動はランダムウォークによってモデル化したが，実際のゲームのプレーヤの挙動は生活環境や交通手段などの制約を受ける．今後は，これらのパラメータやモデルを検討し，シミュレーションの精度を向上させて更なる評価を行う予定である．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（または，人目を気にして）不正者が不正コピーを躊躇するようになるという大前提を置いている．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] 文化庁：平成 21 年通常国会　著作権法改正等について，
http://www.bunka.go.jp/chosakuken/21_houkaisei.html
[3] ネットエージェント : Winny ノード数の推移分析, http://forensic.netagent.co.jp/winny_node.html
[4] Simson Garfinkel, Gene Spafford : Web security & commerce, O'Reilly, pp.123-133, 1997.
[5] 総務省 統計局統計調査部国勢統計課：平成 17 年国勢調査 最終報告書 「日本の人口」統計表 都道府県別面積，人口密度及び人口密度の指数（大正 9 年～平成 17 年），2010 年 2 月 26 日
[6] 任天堂株式会社：第 71 期中間報告書，http://www.nintendo.co.jp/ir/pdf/2010/breport_m1009.pdf
[7] 馬場章，藤原正仁：違法複製ゲームソフトの使用実態調査報告書，社団法人コンピュータエンターテインメント協会，2010 年 6 月 4 日
[8] 厚生労働省 健康局総務課生活習慣病対策室 : 平成 21 年国民健康・栄養調査結果の概要, 2010 年 12 月 7 日

ⓒ 2011 Information Processing Society of Japan