ICCS Journal of Modern Chinese Studies Vol.8 (2) 2015

論文

中国における RMT[1]　関連の事態とその問題点に関する研究

石　巍

要旨

中国においては、現時点で全国民の中に約半分がインターネットの利用者であることと、さらに発展していく見込みを踏まえて考えると、インターネット社会、特にネット上にあるユーザーの個人情報に対する管理は、中国社会の未来に深くかかわっている。

RMT に関して、需要と供給の関係が成立したため、インターネット上で盛んに発展している。RMT 市場での利益を狙い、RMT を生業にした者が現れて、さらに不正ツールの利用やアカウント窃盗事件が頻発している。RMT そのものは不正行為と見られていないが、犯罪を招くまで多くの問題を引き起こすことが無視できない。以上のような不正行為を規制するために、IP Geolocation[2]　や CAPTCHA[3]　、パスワード強化、多要素認証など管理方法が実行されているが、実際ユーザーに受け入れにくい点があり、効果がよくなかった。本稿では、中国における RMT 関連の不正行為の現状に対して研究し、RMT の存在する理由や引き起こした問題、及び管理方法の不足を明らかにする。

キーワード：RMT、不正ツール、アカウント窃盗、個人情報の流出、複数要素認証

[1] RMT（Real-Money Trading）とは、オンラインゲームにおいて、ゲーム内の通貨、アイテムまたはアカウントやキャラクターそのものを、現実社会で取り扱われている通貨と交換する行為のことを指す。

[2] アクセスユーザーの IP アドレスから位置を判定する技術である。

[3] CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart）とは、コンピューターと人間を区別するためのテストである。

はじめに

背景説明

2000 年以来、中国における IT 産業が急速に発展している。CNNIC[4] に発表された各年度の「中国インターネット発展状況統計報告」によれば、この調査が開始された 1997 年においては、インターネット利用者数は 62 万人であったが、2000 年 12 月には 2250 万人になり、2005 年 12 月には 1 億 1100 万人を超え、2010 年には 4 億 5730 万人に達した。2014 年に発表された最新データによると、2013 年 12 月段階で、中国のインターネット利用者数は 6.18 億人にのぼり、インターネットの普及率は 45.8%となっている[5] 。

ITU[6] は 2013 年 10 月 7 日、世界 157 カ国・地域の ICT（情報通信技術）普及度ランキングを公表した。人口に占めるインターネット利用者の割合は、韓国をはじめ、ヨーロッパ諸国、日本やアメリカなど先進国では平均で 77%を占めているという［1］。中国は、利用者数からみるとすでに世界一になったが、普及率からみれば第 78 位で、まだ潜在力がある。特に利用者全体の約 8 割は 10 代から 30 代の若者に集中していることによって、これから普及率も利用者数も増えていくことが予測できる。

たとえば 2013 年度、中国のインターネット旅行の市場規模は 2181.2 億元［2］、インターネット広告市場規模は 1100 億元に達し［3］、オンラインゲームの市場規模は 891.6 億元に達した［4］。特にインターネットショッピング市場取引規模は 1 兆 8409.5 億元を超え、社会全体の小売消費額の 7.9%を占めている。同年度アメリカのインターネットショッピング市場取引規模は 1 兆 5997.9 億元であった［5］。以上は中国における IT 産業の市場規模や利用者数、利用されている分野などのデータを用いた、IT 産業の中国社会に対する影響力と重要性、及びこれから発展していく潜在力などに対しての簡単なイメージである。

急成長とともに IT 産業をめぐる様々な問題が現れてきた。青少年のオンラインゲーム依存などの社会問題、業者のユーザー個人情報漏れなどの事件、政府のインターネットに対する政策は無力などとの指摘もある。いずれも中国 IT 産業の発展にとっては命にかかわる問題であるが、インターネット社会の主体としたユーザーによる不正行為の問題はもっとも深刻であると筆者は思っている。

現時点で全国民の約半分がインターネットの利用者であることと、さらに発展していく見込みを踏まえて考えると、インターネット社会特にユーザーに対する管理は、中国社会の未来のあり方に深くかかわっている。あいにく IT 産業は世界中でほぼ同時に発展し始めたものであるから、先進国も同じく様々な問題に対して対策を検討している。それに、各国の異なる現状によって、起こった問題も解決法も一致しない。従来のように先進国の経験を参考したり学んだりすることは無理である。

---

[4] 中国互联网络信息中心（China Internet Network Information Center，略称 CNNIC）とは、国別インターネットレジストリ（National Internet Registry）として、国家レベルでの IP アドレス管理、中国 IT 産業に関する学術研究・開発及びサービスを提供する組織である。
<http://www.cnnic.net.cn/gywm/CNNICjs/jj/> 2014.5.2

[5] CNNIC：各年度『中国互联网络发展状况统计报告』、2014 年現時点までに合計 33 回発表されている。

[6] 国際電気通信連合 （International Telecommunication Union）

1　RMT 研究の意義

1.1 定義

擬似的な経済システムが成立するMMORPG[7] や MORPG[8] 、レアアイテム[9]をプレーヤー間で取引できるソーシャルゲームなどで行われている。ゲーム内の経済バランスやモラルの崩壊の原因となりうるため、利用規約で禁止、規制している場合が多い。

RMT で現金と交換される仮想世界の財産は、仮想通貨だけではない。キャラクター、アイテムなど、仮想世界を構成する各種の財産が RMT の対象となる。本来のゲーム・プレイヤーに成り代わってゲームに参加し、キャラクターの育成を代行するサービスも RMT で販売されている。仮想通貨と交換される現実世界の財産も、現金以外に電子マネーなどが使われる場合もある。

1.2 RMT の違法性と問題点

RMT は電子データを売買する取引である。しかし、その電子データの著作権はオンラインゲームの運営会社にあることによって、運営会社が許可していない場合、RMT は著作権を侵害していること及び運営妨害することになる可能性がある。海外には RMT を許可しない運営会社が多いが、中国のほとんどの運営会社は RMT を黙認している。RMT の行為そのものを取締る法律そのものは存在しない。それに、RMT で法的制裁を受けた先例もない。

とはいえ、RMT は各種サイバー犯罪に非常に結びつきやすいことも事実である。RMT 業者がゲーム内通貨を取得する過程で、主に以下のような問題が発生する。ゲーム運営企業のサーバー群で不正稼動する BOT の大量発生により、サーバダウン・ラグを発生したり、ゲーム内経済のバランスを崩壊したりするほか、一般ユーザーのアカウント窃盗を目的としたコンピュータウィルス、不正アクセス等のサイバー犯罪の増加などがある。これらは直接的な原因となり、不満の蓄積したユーザー層が離散することにより、運営企業の収益低下リスクとなる。そのため、利用規約で RMT が禁止されているゲームにおいて RMT を利用することは、結果として運営企業に不要な負荷を強いることとなり、ゲームの魅力をユーザーが自ら破壊する行為となりかねない。

現実世界における国家間の経済格差によって、労働単価の安い発展途上国のゲーム・プレイヤーは、仮想通貨を獲得することで、現実世界で働くより高額の所得を得られるのである。中国系のゴールドファーマー[10] が欧米や日韓、台湾など各国・地域のオンラインゲームに足を入れて、そこで取得した外貨の不正な流出を危惧する声もある［6］。たとえば 2010 年頃から「Playerauctions.com」という

[7] MMORPG（Massively Multiplayer Online Role-Playing Game）とは、大規模多人数同時参加型オンライン RPG にと訳され、1 つのサーバーに多くのプレーヤーが共存するといった形態を取るオンラインゲームを指す。ちなみに RPG とは参加者が各自に割り当てられたキャラクターを操作し、架空の状況下において与えられる試練を乗り越えて目的の達成を目指すゲームの一種である。

[8] MORPG（Multiplayer Online Role-Playing Game）とは、複数プレーヤー参加型オンライン RPG と訳され、2～64 人といった、比較的少数のプレーヤーが同一のゲーム空間に集まりプレイするといった形態をとるオンラインゲームを指す。

[9] オンラインゲーム内で、入手困難もしくは不可能なアイテムを指す。

[10] ゲーム内で仮想資産を大量に稼ぎ、RMT によって現実の通貨に換金することを目的としたプレーヤー、すなわちバーチャル就労の者を指す。

サイトが、RMT の仲介業者として中国から米国に向けてRMT のサービスを提供している。それにオンラインゲーム先進国の韓国では 2006 年頃、オンラインギャンブルの仮想通貨が、暴力団の資金源になったことによって、RMT が社会問題になった［7］。

RMT は数多くの国において盛んに実在している。参与しているユーザーも多い。しかし仮想通貨・アイテムなどの取引は運営会社に提唱されていない個人行為であるから、売り手も買い手も保護しない。特に買い手にとっては、RMT を通じて買い取ったアカウントや仮想財産などが売り手に取り戻される可能性があるし、アカウントが運営会社に凍結される可能性もある。

図 1 のように、より多くの現実利益を得るために、RMT 商品の生産・収集の段階で、不正ツールの利用及びアカウント窃盗などのような不正行為が行われる。また RMT が存在することによって、ゲーム内及び現実社会に悪い影響を及ぼす。

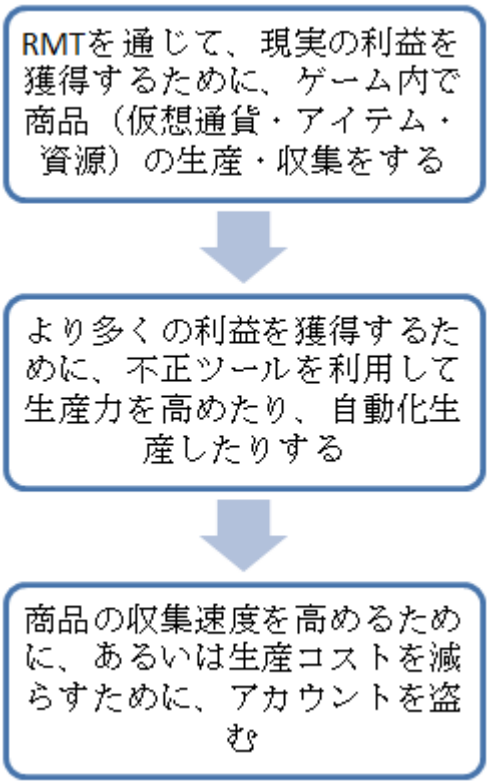


図 1　RMT と不正行為の関連

1.3　RMT の存在原因と現状

1.3.1　需要と供給の関係が実在

RMT はいったいどうして存在するか。一語とで言うとプレーヤーに必要されているからである。

ゲーム体験に対する要求によって、リアルマネーを投入し、速やかな成長を望むプレーヤーがいる。中国には好戦的なプレーヤーが多い。PK[11]　を有利にするために、強力な武器やアイテムが必要となる。けれども一般的なプレーヤーにとって、そのようなアイテムを入手するのは簡単ではない。それで RMT を利用して、よりいいゲーム体験を「買う」という考え方があった。アイテム課金のオンラインゲームには、運営業者もプレーヤーのこの特性を利用して、売り手の役を演じている。

[11] 他プレーヤーのキャラクターを攻撃、殺害することを指す。

また、MMORPG では Mob（ゲームの中でプレーヤーの敵と設定された AI）を狩って経験値を得る設定があり、一定量の経験値を貯めレベルアップすることによって、キャラクターの能力を上げる。プレーヤーにとってキャラクターの育成はゲームプレーの一つの目的である。ほとんどの韓国や中国製ゲームでは、レベルアップするために同じモンスターを何千回何万回以上狩らなければならない。とても時間がかかるし、つまらない作業である。普通どおりにキャラクター育成するのは時間の無駄であると思われ、それを避けるために強力な武器やアイテムを買って効率を上げるか、あるいは育成代行に頼むか、とにかくその分を RMT で短縮してもらえば、仲間との冒険や PvP[12] などのコンテンツをより多く楽しめると考えるプレーヤーがいる。これは育成代行を利用する原因の一つである。もう一つは、育成代行の関係者がゲームのプロであるから、レベルアップの効率が高いし、一般のプレーヤーより高難度の目標を達成できるのも重要な原因である。育成代行サービスの提供は内容も多様で、手段も多い。手作業で行うと宣伝される場合がほとんどであるが、実際は効率を上げるために不正ツールを開発・購入し利用する場合が多い。

一方、ゲームを通じて現実的な利益を獲得しようとしたプレーヤーもいる。一般的にはこのようなプレーヤーは、ゲームの達人だったり、時間をかけてたくさんのゲーム内の資源を生産するゴールドファーマーだったりして、ゲーム内の物々交換に興味がないという点は共通している。もちろん育成代行のような最初から現実利益目当ての個人や集団が含まれている。その他には、アイテムの入手難易度によって、一部のアイテムは現金でなければ取引できない。力で取れるアイテムより、運でしか得られないアイテムはもっと高価である。例えば「大話西遊Ⅱ」にある「神器」、「神獣」が出る確率は極めて低いから、ゲーム内の経済システムではとても評価できない。つまり、オンラインゲームの中には RMT に対する需要と供給の関係が成立しているわけである。

1.3.2 取引便利

RMT の実行については、現実社会で取引したり、銀行振り込みしたりして、1 対 1 で直接に取引する以外、よく利用される手段は、「淘宝網」や「5173」など第三者の取引プラットフォームを通じて売買することである。仮想通貨やアイテム、アカウントのほかにポイントカード、電子マネーや不正ツールまで売買できる。一部のオンラインゲームの運営会社もユーザーの取引をサポートしている。例えば「盛大網絡」には「盛大商城」という総合取引プラットフォームがあり、「網易」には「藏宝閣」という西遊シリーズの公式 RMT サイトがある。

1.3.3 取り締まりは困難

アカウントや仮想マネー、アイテムの販売については基本的に規則違反であるが、RMT 行為そのものを直接に犯罪行為とした法律も判例も無い。特にアイテム課金の場合は最初からリアルマネーが介入しているから RMT を否定する理由が見つからない。育成代行サービスの提供については、非法経営罪として裁いた判例があるが、それを支持する法律は微妙である。取引の手段も多様であり、運営業者の手の届かないことが多いから、取り締まりは困難である。それに、RMT を賛成するユーザーは多いし、ユーザーの離散を恐れる運営業者が目をつぶっていたことも普遍的である。

1.3.4 運営側の態度

そもそも RMT 行為に対して、運営側は曖昧な態度をとったことが根本的な問題である。

[12] Player vs Player の略称。オンラインゲームの人対人で行なう対戦のことである。

網易公司に運営されている MMORPG「World of Warcraft」を例にして説明する。アカウントや仮想通貨・アイテムなどに対する RMT 行為は、協議違反であるとはっきり禁止されている［8］。一方、実際はほとんどのサーバーに何年間も続けた有名で信用度の高い RMT 専門業者がいる。常にゲームの中で RMT 広告を散布するから、運営側は知らないはずがない。「淘宝網」や「5173」など第三者の取引プラットフォームには、このゲームの RMT 情報が数え切れないほど集まっている。RMT 行為を禁止する気があったら、買い手のアカウントをたまに凍結したり［9］時々無視したりするような曖昧な行動より、これらの取引情報の取り消しを要求すべきであると思う。もちろん RMT 行為に対して賛否両論の今では、同社が自主開発・運営している西遊シリーズのように RMT 行為をはっきり認めても構わない。禁止するか承認するか、いずれにしてもはっきりすべきであると思う。

2　RMT 関連の不正ツール

商品とする仮想通貨・アイテムを効率的に入手することを目指して、不正ツールを利用する行為が現れた。機能によって、主に「チート」と「ボット」の 2 種類に分けられる。オンラインゲームに使われることが多いが、近年「切符予約ツール」や「オークションボット」、何かのクライアント・サービスの「会員チート」などゲーム以外に使われるツールも現れた。このようなツールが利用されたら、運営会社あるいは一般ユーザーの正当利益が侵害される。

2.1 チート

2.1.1　チートとは

チート（cheat）とは、プログラム解析や専用のソフト、ツールなどを用いてゲーム内のプログラムデータを改造することである。不正に能力を上げたり、アイテムを入手したり、一撃必殺など、ゲームを非常に有利に進める条件を提供する機能の場合もある。通常利用規約等で禁止されている不正行為なので、運営側に見つかるとアカウントが剥奪される。よくあるのはスピードハック[13]、パケットハック[14]、ファイル改ざん[15]、メモリエディット[16]などである。基本的にキャラクターのデータと、オンライン側のサーバーを改ざんするため、技術的にもかなり高度な能力が要求される。

2.1.2　チートによる被害

チートという不正行為はいつも目立ちすぎで、一般プレーヤーに強く反発されているし、運営業者の取り締まりも厳しい。もっとも分かりやすい例としては、レースゲームでチート行為を行い、自分のレースカーの存在する座標を書き換えて、スタート直後にゴール直前に「置く」行為が挙げられる。このようになると他のレース参加者は、絶対的にチート行為を行ったプレーヤーを追い抜くことはできない。射撃類のゲームの場合は、壁など障害を透視したり、移動速度をアップしたり、さらに自動的で速やかにターゲットを狙い定めて正確に射撃することができるから、たとえ大人数の相手にしても全滅させられる。MMORPG 類のゲームの場合はスピードハック、アイテム改ざんを通じて戦闘力を大幅に強めて、一般プレーヤーのキャラクターを一

[13] たとえば移動や攻撃速度の操作など。
[14] パケット置き換え・転送による高レベルの操作。
[15] ゲームクライアント、ゲームデータファイルの分析・操作。
[16] メモリ内のゲームデータデバッグやメモリエディットなど。

撃で殺してしまうのも珍しくない。さらに普通はグループあるいはレイド[17]　でさえ簡単に倒せないモンスターを一人で倒してしまう。アイテムなどを容易に手に入れ、RMT で一般プレーヤーに販売し、結局ゲームの寿命が縮められる。

2.2 ボット

2.2.1 ボットとは

ボット（Bot）とは、ロボットの略称で、ボットツールやマクロ、自動操作プログラムを使って、キャラクターが一定のパターンの行動を行なえるようにしておき、ユーザーの操作無しに、キャラクターが自動で経験値やアイテムを得るようにする行為である。

たいていの場合において、本来プレーヤーの代わりにキャラクターをコントロールして、プレーヤーのやりたくない作業・行為[18]　を代行させることを目指す。

2.2.2 ボットによる被害

ボットの存在と被害はチートほど目立たない。もしチートがスーパーマンを作りだすものであると言うなら、ボットは絶えず働ける労働者を作りだすようなものである。クライアントプログラムには正常な動きと見えるので、なかなかシステム的には判断できない。それに、ゲームの内にボット通報仕組みをおく場合があるが、直接的な収益に配慮が払われて、ほとんどの運営業者はボットに対する取り締まりがあまい。

一般ユーザーは、いくら頑張っても毎日 24 時間で単純な操作を繰り返すことは考えられない。当然レベルや仮想財産など収益はボットに追いつけない。表面上からみると、ボットは個人行為で、一般ユーザーと同じく接続時間に応じて課金しているし、キャラクターの行動も基本的にゲームの設定されるルールから離れていない。しかしボットはサーバーに接続すれば飽きがこなく働き続けられる特性によって、ゲーム内の経済システムが影響され、生産力の低い一般ユーザーは貧しくなるのは当然である。不正行為で巨大な貧富の差が作り出され、一般ユーザーの積極性が挫かされた。この場合、一般ユーザーの反応は、RMT を通じて仮想通貨やアイテムを買うか、不正ツールを利用して生産力をアップするか、あるいは両方とも嫌なら止めるよりほかにない。

特に無料ゲームの場合には、1 台のパソコンで幾つかのボットプログラムを制御できるから、運営業者は収入が増えないのに、余計に回線とサーバーの負担を拡大される。プレイ時間による料金は一切発生しないから、超長時間ボットを利用することが可能である。それによって、レベルのより低いモンスターを狩れば、少々効率が悪いかもしれないが、消耗なしで済ませる。結局、アイテム課金の売上は減少するのも当然である。

3　RMT 関連のアカウント窃盗

3.1 現状

米国マカフィー社[19]　の研究機関によれば、オンラインゲームのパスワードを盗むコンピ

[17] RAID : MMORPG やソーシャルゲームにおいて複数の group を組んだ多数のプレーヤーが、強大な mob や zone に挑むこと。または、その集団。

[18] 経験値を溜めるための狩りや資源収集のような、単純で頻繁に繰り返し作業のこと。

[19] McAfee, Inc は、アメリカ合衆国カリフォルニア州サンタクララに本社があるコンピュータセキュリティ関連のソフトウェアとハードウェアを製作・販売する米インテルの子会社である。IT セキュリティの専業ベンダーとしては世界一の規模である。

ュータウィルスは 2003 年頃に出現し、2007 年の 1 年間で、パスワードを盗むウイルスが 8 万種類以上確認されたという。2011 年になると、パスワードを盗むウイルスは 30 万種類近くになって、その 40%から 50%は、オンラインゲームのパスワードを狙っているという。

米国では 2003 年ごろからフィッシングが流行し始めた。ユーザーを正規のサイトに見せかけた偽サイトへ誘導し、認証情報を入力させて盗む。2012 年、中国国内のサイトに見せかけた 22,308 個のフィッシング・Web ページが国家インターネット応急センターに探知された。これに関連する IP は 2,576 個があり、その中に米国の IP が 83.2%を占めているという［10］。

2004 年－2007 年、オンラインゲームの流行と共に、仮想財産が注目されるようになった。巨額の RMT 利益のもとで、攻撃者はユーザーのデータを目指して、オンラインゲーム・サーバーを標的にした。コンピュータウィルスやフィッシングなどより、効率も対応性も著しく高まった。2008 年－2009 年、攻撃対象は電子商取引サイトに移った。2010 年以来、ユーザー情報に対する収集・分析を通じて、いわゆる「社会工学」という攻撃手段の効果が、ハッカーたちに好評である。ユーザーの情報をより多く掌握できれば、攻撃の精度や効率を高められるから、確実で詳細なユーザー情報を大量に保有するソーシャルサイトとコミュニティサイトが標的になっている。地下で「人肉検査庫」[20] を作って、ユーザー常用のアカウントやメールアドレスを知れば、当ユーザー常用のパスワードを検索できるという［11］。

2011 年前半、コンピュータウィルスに攻撃されたユーザーは 2.17 億人いる、ユーザー全体の 44.7%を占める。アカウント盗難に遭ったユーザーは 1.21 億人いるという［12］。この 1.21 億人の中に、データベースハッキングによるアカウント情報の流出が 8 割以上を占める。その危害はコンピュータウィルスより遥かに大きいという［13］。2011 年 12 月下旬、中国でインターネット個人情報の流出事件が連続して発生した。2011 年 12 月 29 日まで、26 のデータベースが情報漏れの疑いがあり、かかわるアカウントとパスワードが 2.78 億組であるという［14］。

サイバースペースではアカウントとパスワードがユーザーそのものである。アカウントとパスワードが盗まれれば、他人が完全に盗まれたユーザーになりすますことができ、その行為の結果がすべて盗まれたユーザーの責任になる。最も重要でありながら、最も盗まれやすい。その原因の一つは RMT 市場が形成されて、これらをお金に換えることが可能になっているからである。

アカウント盗難によって、ユーザーの仮想財産やアカウントそのものが売られてしまうだけではなく、ネットバンクなど取引機能を持つアカウントが不正アクセスされたら、もっと現実的な被害になる。また、ユーザーの個人情報が現実社会で悪用される危険性が極めて高い［15］。

3.2 手段

3.2.1 コンピュータウィルス――盗む

「キー・ロガー」などのコンピュータウィルスが仕込まれたリンクを散布する場合もあるし、メールに添付して送りつける場合もあるし、一般プログラムに見せかけてダウンロードされる場合もある。実行すると、ユーザーのキー操作を記録し、ユーザーの認証情報などを自動的にハッカーに送る。

[20] ユーザーの個人情報を保存するデータベース。

3.2.2 フィッシング[21] ――騙す

実在する企業の Web サイトに見せかけたサイトへユーザーを誘導し、クレジット・カード番号などユーザーの認証情報を入力させて盗むことを指す。

3.2.3 パスワードクラック[22] ――破る

類推攻撃[23] ・辞書攻撃[24] ・総当り攻撃[25]のように何種類があるが、文字列を順に当てはめていくという基本的な特徴はみんな一緒である。パスワード候補のリストを順に試してゆくという点で、それらは似通っているという。実際に動作しているサーバーに ID とパスワードを送って認証に成功するかどうかを試すようなオンライン攻撃もあるし、サーバー以外でも動作中のサービスに認証情報を送って試すオンライン攻撃もある。

3.2.4 データベースハッキング――奪う

SQL[26] インジェクション攻撃[27] などの手段により、データベースを直接操作することができてしまう。それによって、データベースに格納していたクレジット・カード情報やアカウント情報など重要なデータが直接に盗む。あるいは、ウイルス感染を引き起こすようにサイト上にウイルスを埋め込めたり、公式サイトを攻撃者に都合の良い情報に書き換えたりして、間接的に情報を盗む。データベースのセキュリティを破って、アクセス権限を奪って、大量の確実で詳細なユーザー情報を取り出す。

3.2.5 内部関係者による情報流出――買う

情報漏れ事件については、外部からのデータベースハッキングより、内部関係者による情報流出の方が遥かに多い［16］。中国移動通信集団、中国工商銀行、中国招商銀行、中国農業銀行、多玩 YY[28] など内部関係者による情報流出も判明されている［17］、［18］、［19］。

表 1 のように、アカウント窃盗に関して、よく見られる手段は 5 つある。対象も危害も一致しないが、より遅く出現した手段は危害がより大きいと思われる。アカウント窃盗の手段が発展していて、対象も目的もだんだん明確になってきて、ターゲットの数も多くなっていることは明らかである。つまり、現状から見ると、現在一般的なサイトのセキュリティ水準では、インターネット上の個人情報を守りきれない。

表 1 アカウント窃盗手段と被害の比較

手段	対象	目的
コンピュータウィルス	不特定単一	不特定の情報あるいはパソコン制御の権限を取得
フィッシング	不特定単一	特定サイトの ID と PW をセットで取得
パスワードクラック	特定単一	特定 ID の PW を取得

[21] phishing が fishing（釣り）に基づいた造語され、オンライン詐欺の一種である。
[22] パスワードを見破ることを指す。
[23] ターゲットの個人情報に関する知識から、攻撃者自身がパスワードを類推し攻撃する。
[24] 人名や意味のある単語など、パスワードとして使われやすい文字列をデータベース（辞書）に登録し、それを順に当てはめていくという手法である。
[25] 理論的にありうるパターン全てを試す。
[26] SQL とは「Structured Query Language」の略で、データベースとやり取りをするためのものである。
[27] SQL インジェクションは、広く知られたハッキング手法で、この手法を用いると、正規の認証を通ることなく、データベースにアクセスすることが可能になる。
[28] 広州多玩信息技術有限公司に開発された即時通信ソフトウェアである。

データベースハッキング	不特定複数	特定サイトのIDやPWなど個人情報を取得
内部関係者による情報流出	特定 or 不特定 単一 or 複数	特定サイトのIDやPWなど個人情報を取得

3.3 小節

ユーザーはインターネットにおける通信・社交・ゲームなどソフトウェアやサービスを利用するために、当サイトに個人情報を提出して ID を申請する必要がある。場合によって、ユーザーの年齢などを確認する必要があるし、特に中国においては、インターネット実名制の全面実行により、インターネット上のサービスを利用するには個人情報の提出が前提条件になっている。そこでは、実名制の下でユーザーの個人情報を如何に守るかが重要なポイントとなる。

外部から侵入されるか、あるいは内部関係者による流出か、いずれにしてもユーザーの個人情報を守り切れない場合がある。会社によってセキュリティのレベルが違うが、ユーザーの個人情報の価値がかわらない。それ故、各サイトに大事な個人情報を提出することは、実にリスクが高いことである。今ユーザーは自分の個人情報がどのサイトから漏れたのかさえ分からない。この状態で、もちろん誰も責任を取ってもらえない。それに、インターネットと現実社会の繋がりがどんどん緊密になってきて、ネット上の個人情報流出により現実社会での被害が出てきてもおかしくない。

4 RMT 関連の不正に対応する対策

中国においては運営側からのアカウントに対する保護措置が多いが、ユーザーにとって不便なものも多いから、予想している効果が現実的に発揮できず、ユーザーの反発を招くことさえあった。それに運営側は RMT 行為に対して、実際に禁止も保護も一切しないことも問題であると思う。

ID 管理に関するユーザーの習慣やインターネット利用の体験などについて、56 人の 20 と 30 代のユーザーにアンケート調査を行った。こちらでは調査結果の概要をまとめる。インターネットにおいて、ほとんどのユーザーがたくさんの ID を持っている。覚えやすくするために、違うサイトで同じ ID と PW の組み合わせを利用する傾向がある。9 割以上のユーザーは ID が盗まれた経験があるが、安全性を高めるためによくパスワードを変更するのは 4%しかない。複数要素認証手段の中に携帯電話のメール認証が最もユーザーに愛用されている。その以外に USB トークン、E メール認証とセキュリティカードもよく利用されている。しかしすべての ID に複数認証を設定するわけではなく、携帯電話認証の場合は大体一人に 10 個以内を設定し、USB トークンは 5 個以内を持つ。身分を確認する道具を 10 個以上を持つと、また不便になると思われている。それに、IP Geolocation（即ちアクセス制御）を認めるのは多いが、CAPTCHA を認めるのはあまりいない。

4.1 IP Geolocation[29] ——アクセス制御

4.1.1 IP Geolocation とは

IP Geolocation については、国によって使い方が違う。

アメリカでは、海外のオンラインゲームやギャンブルサイトでの不正対策のひとつとし

[29] アクセスユーザーの IP アドレスから位置を判定する技術である。

て採用されているという［20］。

日本では、オンラインゲーム会社は規約違反の RMT を防止するため、中国からの接続を制限している場合がある。これに対して、中継用のサーバーを使うことで日本国内から接続するように見せかけていた中国からの接続の例があった。2006 年 11 月、熊本県で出入国管理法違反の疑いにより中国人留学生が逮捕された。この留学生は IP アドレスを擬装して中国からの大量アクセスを可能とするサーバーを熊本市内の自宅で稼働させていたとされる。

中国では、アカウント盗難が頻発しているから、主にアカウントを保護するためにアクセスを制御する。常用登録地・IP 以外の IP に接続された場合、アカウントが盗まれた可能性が高いと思われ、運営会社はユーザーのアカウントを保護するために臨時凍結することがある。

4.1.2 IP Geolocation の問題点

IP Geolocation によるアクセス制御はユーザーのアカウントを守るためのいい技術である。しかし実際的な応用で、細かい所で不足があると思う。

アカウント凍結のタイミングに関して、理論的にアクセスの瞬間で凍結するのはベストであるが、実際に被害が出た後で凍結される場合が多い。結局アカウント保護という役割を果たせず、かえってユーザーに不便をもたらす。仕事などの原因でよく出張するユーザーの場合、非常用 IP からのアクセスによって、アカウントの持ち主本人を不正アクセスと誤認されてしまうことがある。

他にも、RMT を利用し、売り手がアカウントを第三者の取引プラットフォームに預かる場合や、買い手がアカウントを育成代行に預かる場合などがある。確かにアクセスを実行する者はユーザー本人ではないが、あくまでもユーザーの意思による結果であるから、アカウントを凍結すべきかどうか、また検討する余地がある。

4.2 CAPTCHA[30] ——画像認証

4.2.1 CAPTCHA とは

CAPTCHA という画像認証システムは、主にパスワードクラックとボットを防ぐために使われる。アカウントの申請・登録・操作、BBS などでの書き込みの発表・転載あるいはゲーム活動の最中に、画像に応じて答えを入力することを要求し、応答者がコンピューターではないことを確認する。画像認証システムの発動するタイミングによって、阻止されたボットは大体 3 種類に分けられる。

1. アカウント申請用ボットを阻止

BBS などソーシャルで不正書き込み用（広告散布など）のアカウントを大量に申請する行為を阻止するためである。また、ID は数字で表現する場合がある。現実社会には電話番号や車のナンバープレートなどにかかわる人間がいることと同じく、インターネット世界には ID にかかわるユーザーがいる。気に入る ID を入手するために、あるいは RMT の商品として販売するために、不正ツールで ID を頻繁に申請することがある。

2. アカウント登録用ボットを阻止

特定なアカウントを登録するために頻繁にパスワードを試す行為、つまりパスワードクラックのことである。このような行為を阻止するために、アカウントを登録する時パスワードと画像確認が同時に要求される。

3. アカウント制御用ボットを阻止

最広範に利用されたのは、ユーザーの代わりにアカウントを制御するボットである。例えばオンラインゲームでの資源収集・キャラ

[30] 全称は completely automated public Turing test to tell computers and humans apart であり、コンピューターと人間を区別するためのテストである。

クター育成、ソーシャルサイトでの書き込みなどがある。アカウントの動きはユーザーによるものかボットによるのもかを確認するために、ゲームの最中や書き込みを発表する時に画像認証をする。

4.2.2 CAPTCHA の問題点

一般ユーザーにとって、あまり識別しにくい画像さえ出てこなければ、アカウントを申請・登録する時に画像認証が要求されても特に困ったとは思われない。しかもアカウントを登録する時、非常用の IP からのアクセスしか確認しない場合が多いから、不便を感じさせることは少ない。ユーザーに強く反発されたのは、アカウント操作中に出てきた画像認証である。例えばゲームの最中に画像認証が要求され、それを対処したせいで獲得したはずのものがなくなってしまうことであり、なかなか識別できない画像認証に頻繁に邪魔されたら尚更である。一方、システムの代わりにスタッフでボットを退治するのは、精度が高くなり一般ユーザーには影響を与えないが、運営側のコストを上げてしまう。総合的に考えると画像認証のタイミングと頻度を、できるだけユーザーの邪魔にならないようにすべきである。

もっと深く考えると、ひとつのゲームでたくさんのアカウントを持つユーザーが多い。それらのボットを利用する目的から分析すると、RMT の商品とする仮想財産を収集、及びメイン・アカウントを支持するために補助的なアカウントで仮想財産を収集する行為が考えられる。補充的なアカウントが凍結される覚悟ができている上で不正ツールを利用するという共通点がある。この場合は同一人物の身分証明書で申請したすべてのアカウントに連帯責任を負わさせなければ、不正ツールが消えないであろう。

ボットなど不正ツールの利用は、インターネット及びオンラインゲームの秩序を乱すことになるから、放任しておいてはいけない。CAPTCHA は一種の手段として、積極的に効果が発揮されているが、唯一の手段ではい。それにCAPTCHAの画像は読みにくいという特性があり、場合によって頻繁に出てくることもあるから､ユーザーに不便をもたらして、反発を招いた［21］、［22］。

4.3 パスワード強化

4.3.1 パスワード強化とは

パスワードクラックによるアカウント盗難事件を減少させるために、運営側はユーザーにパスワードの強化を求めている。安全性の高いパスワードの設定について、以下のようにアドバイスをしている。

1. ID と同じ、あるいは似るものを使わない。
2. 名前、誕生日、パスポート番号など個人情報を使わない。
3. 8 文字以上で設定する。
4. 大小英文字、数字、記号などを組み合わせて設定する。

場合によって、いずれの条件も強制的に要求されることがある。それに、Microsoft によると強力なパスワードの効果を保つために、違うサイトで同じパスワードと ID を使わなく、それにパスワードを頻繁に変更した方がいいという［23］。

4.3.2 パスワード強化の問題点

現実では、パスワードの安全性が高ければ高いほど忘れやすいという特性があるから、ユーザーはわざと安全性の低く覚えやすいパスワードを設定する傾向がある。それに、一般的には一人のユーザーが何十個もの ID を持っているから、同じものにしなかったら忘れてしまう恐れがある。パスワードを頻繁に変更するのはさらに現実的ではない。CSDN

によると、22.6%のユーザーが 100 個の常用パスワードを使っていて、60%以上のユーザーが数字だけで組んだパスワードを使っている。2011 年 12 月の大規模のインターネット個人情報流出事件以後、運営側が繰り返してパスワード変更の注意報を出た状況で、パスワードを変更したユーザーは 3 割しかない［24］。

今まで本人認証を一手に引き受けてきた ID・パスワードは非常に秀逸なアイデアである。けれどもコンピュータウィルスやフィッシング、パスワードクラック、データベースハッキング、内部関係者による情報流出などの他人のアカウントを窃盗・入手する手段が現れ、運営会社はユーザーの認証情報をなかなか守りきれない。このような状況が存在する限り、ID・PW だけでの認証は不十分である。パスワードの長さや複雑さはパスワードクラック以外の手段の前で、何の意味もないと言えるであろう。

4.4 複数要素認証

4.4.1 複数要素認証とは

中国においては、様々な原因でアカウント盗難が頻繁に発生し、さらに大規模のインターネット個人情報流出事件が連続的に起こっている。それで、ユーザー本人を認証する際、ID・PW だけでは十分ではないと認識されるようになった。パスワード提供の上、ほかの認証手段を通じて確認し、アカウント不正利用のリスクを軽減することを目指している。

認証方式が多様であるが、大きく 3 つの種類に分けられる［25］。

1. あなたが知っていること(What You Know)。パスワードや秘密の質問などを含む。
2. あなたが持っているもの（What You Have)。デジタル証明書、携帯電話認証サービス、USB トークンなどを含む。
3. あなた自身（What You Are)。指紋、声紋、虹彩などを含む生体認証である。

複数要素認証の問題点

秘密質問など第 1 種類の認証方法はパスワードと同じく、盗まれる可能性が高く、安全性が低い。大事な情報を流出しないように、偽情報を記入するユーザーが多く、結局答えを忘れてしまうケースがある。

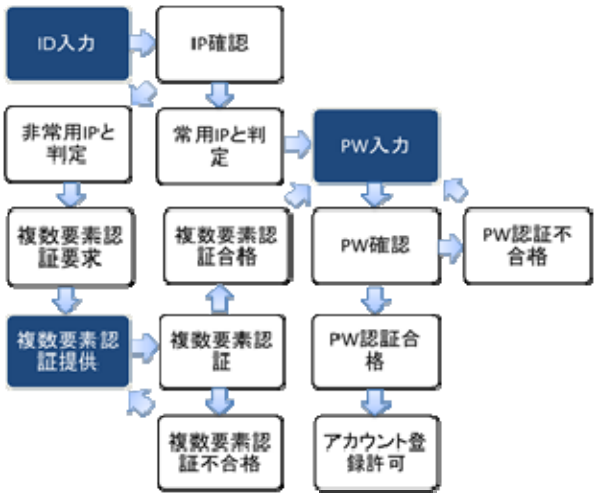
技術や設備、コストなどの関係で、インターネットにおいては生体認証が現時点でまだ普及されていない。

現在よく利用されいるのは第 2 種類の認証手段である。便利性からみると、デジタル証明書、携帯電話認証サービス、USB トークンの順であるが、安全性からみると逆である。現時点において USB トークンは各企業が独自発行するものである。複数要素認証が発展していくと、ユーザーは各社の認証設備を持たなければならない状況が予測できる。そうすると、不便を感じたユーザーが、安全性が低く覚えやすいパスワードを選んだように、USB トークンを利用しない恐れが考えられる。

4.5 小節

ユーザーの支持を欠いたら、予期される効果に達せないから、対応策を制定する時、安全性と便利性両方とも検討した方がいいと思う。例えば図 2 のように、まずユーザーに ID を入力させて、サーバー側は当 ID の非常用 IP からのアクセスを検出した場合、複数要素認証を要求し、アカウント凍結を実行するかどうかは認証結果の次第で決める。

図 2　IP Geolocation と多要素認証を活用したアカウント登録の流れ



パスワードの安全性に拘らなくて、IP Geolocation と多要素認証を活用し、ユーザーに与える不便を軽減する上で、アカウント窃盗事件を有効に防止できるはずである。

まとめ

中国においては、RMT そのものは不正行為と見られていない。需要と供給の関係が成立したため、インターネット上にはたくさんの RMT サイトができて、盛んに取引が行われている。オークションだけでなく、RMT 専門業者サイトや仲介サイト、個人間取引などを含め、形態は多様であり、利用者も多い。

しかし RMT によって、多くの不正行為が引き起こされたことは無視できない。RMT 市場での利益を狙い、ゴールドファーマーと呼ばれた RMT を生業にした者が現れて、商品とする仮想通貨・アイテムを効率的に入手することを目指して、不正ツールを利用する行為も現れた。さらに仮想商品を生産するには従量課金や時間などのコストがかかる。RMT の利益を最大限するために、「トロイの木馬」などコンピュータウィルスを不正ツールに仕掛けて、インターネットで散布し、感染したパソコンからユーザーの ID 情報を盗む。盗まれたものをまたユーザーに売り出して、通常は考えつかないほどの利潤が得られる。すなわち RMT は犯罪を招くまで、多くの問題を引き起こし、不正行為の源になっている。

RMT を全面禁止するか、不正行為の防止策を考えならが RMT を承認するか、いずれにしても運営側の意見ははっきりすべきであると思う。承認する場合、政府は取引税や関連する法律など RMT 市場を規範する政策を制定し、現実社会の市場のように管理・監督する。そして商品とした仮想通貨・アイテムなどの不正収集（不正ツールの利用とアカウント窃盗行為を含む）に対しても、厳しく対処すべきである。例えばユーザー本人が不正をしたと確定したら、証拠をホームページなどで公示する上、連帯責任として当ユーザー名義のすべてのアカウントを剥奪する。直接にボットの活動を阻止しようとする CAPTCHA に比べて、一般ユーザーに不便をかけずに、根源から不正行為で利益を得ようとする考え方を阻止した方が有効である。

現在利用されている複数要素認証手段は、第 2 種類の「ユーザーの持っているもの」が多い。便利性からみると、デジタル証明書、携帯電話認証サービス、USB トークンの順であるが、安全性からみると逆である。現時点において USB トークンは各企業が独自発行するものである。複数要素認証が発展していくと、ユーザーは各社の認証設備を持たなければならない状況が予測できる。そうすると、不便を感じたユーザーが、安全性が低く覚えやすいパスワードを選んだように、USB トークンを利用しない恐れがある。便利性と安全性のバランスを如何にとるかという点が今後

の課題になるであろう。

引用文献

[1] ITU『国际电联发布最新技术数据和全球排名』（図表 1、図表 5）
<http://www.itu.int/net/pressoffice/press_releases/2013/pdf/41-zh.pdf> 2014.5.2
[2] 艾瑞咨询集团『2014 年中国在线旅游度假市场研究报告』P5
[3] 艾瑞咨询集团『2014 年中国网络广告行业年度监测报告（简版）』P9
[4] 艾瑞咨询集团『2014 年中国网络游戏行业报告简版』P3
[5] 艾瑞咨询集团『2014 年中国电子商务行业年度监测报告（简版）』P13・14
[6] 日本経済新聞「RMT 総論：ゲームから生まれた仮想通貨の行方」
<http://itpro.nikkeibp.co.jp/article/COLUMN/20060907/247473/> 2014.5.10
[7] 日本経済新聞「ソーシャルゲーム「換金市場」の実態とは、競売サイトを温床に膨張」
<http://www.nikkei.com/article/DGXBZO39167360Y2A220C1000000/> 2014.5.13
[8] 「魔兽世界中文版使用条款」
<http://www.battlenet.com.cn/zh/legal-cn/wow-tou> 2014.5.13
[9] 「5173 买金币交易完成时号就被封」
<http://www.battlenet.com.cn/wow/zh/forum/topic/4217072464> 2014.5.13
[10] 国家互联网应急中心「2012 年中国互联网网络安全报告」P150
<http://www.cert.org.cn/publish/main/upload/File/2012Report.pdf> 2014.5.5
[11] 比特网「网络泄密背后脆弱的网站和法律防火墙」
<http://sec.chinabyte.com/176/12256176_7.shtml> 2014.5.18
[12] CNNIC「第 28 次中国互联网络发展状况统计报告」P36
[13] 东方网「中国黑客产业链浮出水面：规模价值达上百亿元」
<http://news.eastday.com/s/20111227/u1a6279125.html> 2014.5.18
[14] 国家互联网应急中心「2011 年中国互联网网络安全报告」
<http://www.cert.org.cn/publish/main/46/2012/2012052308553334121547 1_20120523085533341215471.html> 2014.5.18
[15] 「个人信息泄露后的六大后果」
<http://it.sohu.com/s2009/gerenxinxi/> 2014.5.21
[16] 「七成个人信息泄露是单位内部作案」
<http://news.sina.com.cn/o/2013-01-22/051926089902.shtml> 2014.5.18
[17] 央视 315 晚会「揭露个人信息泄露之谜」
<http://it.sohu.com/s2009/gerenxinxi/> 2014.5.18
[18] CCTV「招行工行农行泄露出售客户信息」
<http://jingji.cntv.cn/20120315/122436.shtml> 2014.5.18
[19] 南方日报「泄漏用户隐私屡查不绝 政企联手展开“严打”」 2012 年 1 月 12 日 星期四 B04 版
<http://epaper.nfdaily.cn/html/2012-01/12/content_7047942.htm> 2014.5.18
[20] News2u.net「オンラインゲーム人口の増加で表面化する RMT」
<http://www.news2u.net/releases/109849> 2014.5.21
[21] 「登録させる気のない Captcha」
<http://matome.naver.jp/odai/2125196064905045836> 2014.5.25

[22] 「無力感で心が折れそうなほどある意味ひどい認証用の CAPTCHA 画像まとめ」
<http://gigazine.net/news/20121218-captcha-fail/> 2014.5.25
[23] Microsoft「安全性の高いパスワードの作成」
<http://www.microsoft.com/ja-jp/security/online-privacy/passwords-create.aspx> 2014.5.25
[24] 「CSDN 高管泄漏密码续：泄密用户 7 成未改密码」
<http://sec.chinabyte.com/58/12243058.shtml> 2014.5.25
[25] 张丽・赵洋「身份认证技术的研究与安全性分析」，『计算机与现代化』2007 年第 5 期

参考文献

1. 土橋 喜「中国のインターネット利用者数と普及率の変化」『愛知大学情報メディアセンター』vol.23 <saturn.aichi-u.ac.jp/img/center/pdf/com38-4.pdf> 2014.5.3
2. CNNIC「中国互联网络发展状况统计报告」（2014 年現時点までに合計 33 回発表されている）
3. 李乐「MMORPGs 中的经济体系—探寻虚拟世界内部的经济现象」『佳木斯大学社会科学学报』2008.04
4. 李乐「虚拟世界的真钱交易分析」『重庆邮电大学学报(社会科学版)』2010.02
5. 李乐「基于商誉角度的虚拟物品真钱交易」『重庆邮电大学学报(社会科学版)』2010.05
6. 吴洪; 孙启明「国外网络货币虚转实交易研究述评」『经济理论与经济管理』2012.01
7. 李慧「简述互联网验证码技术与设计」『科技信息』
8. 谢波峰「虚拟游戏物品 RMT 交易的税收问题及其管理」『税务研究』2008 年 05 期
9. 黄家林； 李福芳； 廖俊平； 孙谦；「网络用户安全身份认证系统设计与实现」『电脑开发与应用』2003 年 04 期
10. 黄红兵「基于安全电子商务身份认证方法的研究」『商场现代化』2005 年 21 期
11. 张彩莱「网络安全与身份认证」『网络安全技术与应用』2001 年 04 期
12. 于志刚「论网络游戏中虚拟财产的法律性质及其刑法保护」『政法论坛：中国政法大学学报』2003 年 第 6 期
13. 仝磊「由 CSDN 信息泄露事件引发的思考」『网络安全技术与应用』2012 年 第 2 期
14. 褚建立 张洪星 李洪燕 马雪松「基于 Web 的多重身份认证的设计与实现」『电脑知识与技术：学术交流』2007 年 第 1 期
15. 李皓「网络环境下个人信息泄露的理论分析及防范探讨」『情报探索』2011 年 01 期
16. 简明「计算机网络信息安全及其防护策略的研究」『科技资讯』2006 年 第 28 期
17. 施荣华「一种多重密钥共享认证方案」『计算机学报』2003 年 第 5 期
18. 颜颖「网上银行身份认证技术分析」『哈尔滨职业技术学院学报』2012 年 第 6 期
19. 王泰文「多重身份认证引领企业信息安全新趋势」『A&S：安防工程商』2013 年 第 4 期
20. 五木宏,藤田篤,竹内飛鳥,松原仁「MMORPG ログデータを活用した RMT 被疑者の効率的な検出」『情報処理学会研究報告』2010 年 8 月
21. 五木宏,藤田篤,竹内飛鳥,松原仁「RMT に立ち向かう MMORPG 運営者の支援」『知能と情報』2010 年 12 月
22. 新清士「巨大化する RMT 市場 ： 仮想通貨「偽造」事件が突きつけるオンラインゲーム周辺市場の複雑さ」2006 年 7 月
23. Richard Heeks 「 Understanding "Gold Farming" and Real-Money Trading as the Intersection of Real and Virtual Economies」

<http://journals.tdl.org/jvwr/index.php/jvwr/article/viewArticle/868>2014.5.21

24. Jun-Sok Huhh「Effects of Real-Money Trading on MMOG Demand: A Network Externality Based Explanation」 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=943368>2014.5.21
25. Vili Lehdonvirta「REAL-MONEY TRADE OF VIRTUAL ASSETS: NEW STRATEGIES FOR VIRTUAL WORLD OPERATORS」 <http://www.hiit.fi/u/vlehdonv/documents/Lehdonvirta-2008-RMT-Strategies.pdf>2014.5.21
26. Vili Lehdonvirta「Real-Money Trade of Virtual Assets: Ten Different User Perceptions」 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1351772>2014.5.23
27. Ung-gi Yoon「Real Money Trading in MMORPG Items From a Legal and Policy Perspective」 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1113327>2014.5.23
28. Edward Castronova「A cost-benefit analysis of real-money trade in the products of synthetic economies」 <http://www.emeraldinsight.com/journals.htm?articleid=1576075&show=abstract>2014.5.23
29. Atsushi Fujita, Hiroshi Itsuki, Hitoshi Matsubara「Detecting Real Money Traders in MMORPG by Using Trading Network」 <http://www.aaai.org/ocs/index.php/AIIDE/AIIDE11/paper/viewFile/4057/4408>2014.5.24
30. Ioanna Constantiou, Morten Fosselius Legarth, Kasper Birch Olsen「What are users' intentions towards real money trading in massively multiplayer online games?」 <http://link.springer.com/article/10.1007/s12525-011-0076-9#page-1>2014.5.24