



German
Data
Security

G Data

Whitepaper 2010

ソーシャルゲームとオンラインゲームの危険度

G Dataセキュリティラボ

サブリーナ・バーケンコフ、ラルフ・ベンツミュラー、マーク・A・エスター、

瀧本往人(日本語版監修・翻訳)



Go safe. Go safer. G Data.

はじめに

パソコンで楽しむオンラインゲーム（もしくはネットゲーム）は、昨今のエンターテインメント産業のなかでも、類まれなる成功分野となっています。ヨーロッパでは、2009年の1年間で、延べ2億5300万ものゲームが販売され、80億ユーロ以上の売上を記録しています¹。

ヨーロッパインタラクティブソフトウェア連盟（ISFE）調べによれば、EUでは成人4人に1人がデジタルゲーム（パソコン、家庭用ゲーム機、ケータイを含む）を楽しんでいます²。また、日本でも、コムスコア調べによれば、約1,650万人が、パソコンでオンラインゲームを楽しんだことがあるとされています。

一方では、Xbox360やWii、PS3を例に出すまでもなく、ゲームに使用されるプラットフォームは多様化もしくは分化が進んでいます。しかし逆に、パソコンは今なお、もっとも一般的でもっとも多くの人に共通な「ゲーム機」であることに変わりはありません。実際のところ、パソコンは、ゲームプレーヤーのお気に入りのゲーム機（デバイス）の、二番目に選ばれています（ISFE調べ）。

また、米国での調査では、85%のオンラインゲームプレーヤーは、主なパソコンの用途をゲーム、と述べています³。さらに、最近発行された、プラットフォーム別に分類された新作ゲームの出荷に関する統計によれば、パソコンゲームは、まだまだ家庭用ゲーム機やモバイルゲームよりも好まれていることを示しています⁴。むしろ、スマートフォンなどのモバイル機器用のゲームが爆発的に利用者数を伸ばしている現状を考えると、多くのゲームプレーヤーにとって、デジタル機器はますます必要不可欠であり、ユーザー同士の情報交換や関連製品の購入などを含めて、その中心にパソコンが位置しているのが、現状です⁵。

しかも今、無料で利用可能なSNS上でのゲーム、つまり「ソーシャルゲーム」が急速に注目されはじめています。実際に、ゲーム開発者であるジンガ（Zynga）とSNS業界のリーダーであるFacebookも共同戦線をはり、戦略を共有しはじめたことによって、ゲームプレーヤー数が大きく増加しました。ところが残念なことに、この増加によって、ソーシャルゲームのユーザーは、サイバー犯罪者にとって格好の攻撃目標となってしまいました。

オンラインゲーム関連の犯罪は、これまですでに頻繁に出現してきました。ゲームプレーヤーは、アクセスデータや仮想通貨、および現金さえしばしば強奪されているのが現状です。ソーシャルゲームを含む「オンライン」のゲームが、この先しばらくの間は成長し続け、ゲーム市場の中心となるのは間違いのない、と専門家たちが表明している以上、今後ますます、営利を追求するネット犯罪者たちは、「オンライン」のゲームに攻撃を集中させるのは間違いありません。

特に、世界的には、World of Warcraftを代表とする、いわゆるMMORPG（不特定多数と対戦するロールプレイングゲーム）が、もっとも狙われており、奪われたアカウントやゲーム内のアイテムは、時には、数千ユーロの価格で取引されています。日本ではファイル共有ネットワークを通じて個人情報や盗取し暴露するという出来事も生じていますが、大部分のサイバー窃盗の最大の関心事は、効率よく利益が得られることなのです。

¹ ISFE Consumer Survey 2010 – <http://www.isfe.eu>

² ISFE Consumer Survey 2010 – <http://www.isfe.eu>

³ Study by The NPD Group, Inc. - http://www.npd.com/press/releases/press_100302.html

⁴ “New releases in 2010” diagram in GamesMarkt 14/10, page 27

⁵ Study by The NPD Group, Inc. - http://www.npd.com/press/releases/press_100721.html

目次

はじめに	2
攻撃手法	4
1 メール経由のフィッシング	4
2 ウェブサイトによるフィッシング	4
3 フォーラムやチャットルームにおけるフィッシング	5
4 その他のデータ窃盗	5
ゲーム関連マルウェア	7
危険なゲームサイト	9
ゲーム関連の裏取引価格	11
リアルマネーとの取引	13
日本版特別編	
ソーシャルゲームの危険度	14
ゲームとマルウェア	15
オンラインゲーム関連の出来事	16
安全対策	19

攻撃手法

サイバー犯罪者たちは、あらゆる種類の攻撃を試み、ゲーマーのアクセスデータを奪い取ろうとします。たとえば、いかにも公式のゲームの開発元やサポートから来たかのようにみせかける、誘い込みのためのメールを悪用します。ログインページは一見それらしく作られています。スパイウェアを仕掛けているものもあります。ここでは攻撃手法について、1)メール、2)ウェブページ、3)フォーラムやチャット、4)その他、から説明します。

1 メール経由のフィッシング

ネットで詐欺を働こうとする人間は、あらゆる可能性を探ります。そこには限界というものはありません。そのなかでも、もっともお気に入りの手法は、何百万ものスパムメールを潜在的なオンラインゲームプレイヤーと思わしき人びとに送りつけることです。

送信者は、ゲームメーカーを模倣するためにしばしば、送信者アドレスを偽造します。たとえば、ここに、非常に人気があるオンラインのロールプレイングゲームである World of Warcraft に関連する、偽のメール件名の例があります。

```
Blizzard Notification About World of Warcraft Account
FREE Games gold Warcraft
WorldofWarcraft mounts Trial notice
World of Warcraft Account Security Verification
World of Warcraft Account – Subscription Change Notice
World of Warcraft – Account Instructions
World of Warcraft – Account warning
```

犯罪者たちは、件名には、オリジナルとよく似たものを使用します。そのため、メールを受け取った側は、ついつい騙されて、自身のアクセスデータすべてをメールに記入して返送してしまいます。または、偽のサイトに連れてゆかれ、そこで、いつもと同じようにアクセスデータを入力してしまい、犯罪者側に情報を提供してしまいます。さらに別の手としては、ゲーマーにメールを送りつけ、その添付ファイル(実行ファイルである.exeやPDFなど)をクリックさせることで、マルウェアに感染させます。この不正ファイルは、表面上はいつも、パッチやアップグレード、請求書、登録フォームなどのふりをしています。

2 ウェブサイトによるフィッシング

スパムメールのなかには、URL が書かれておりクリックするとウェブサイトを表示させるものがあります。フィッシング詐欺師は、オリジナルのウェブサイトから、自分たちが用意したオンラインサーバにソースコードをそのままコピーして利用し、データをログインフィールドの中に入力させ、後にデータを転送させます。

また、メールから間接的に行うだけではなく、直接、ウェブサイト上で騙そうとするケースもあります。そのままページにアクセスデータを入力するのであれば、特に疑うこともなく、軽い気持ちで実行してしまいます。そこをつけこみネット犯罪者は、チップの追加やボーナスクレジットまたは特別なアイテムやツールの提供でユーザーを釣り上げようとします。この場合、ボーナスを受け取することを希望してアクセスデータを入力してしまえば、ほぼ確実にアカウントを詐欺師に与え



スクリーンショット1 アカウント情報を入力するとボーナスが提供されることを強調しフィッシングを行うポーカーサイト

てしまいます。

この詳しい情報に関しては、以下の「不正ゲームサイトの構成比」をご覧ください。

3 フォーラムやチャットルームにおけるフィッシング

犯罪者たちの仕掛ける罠の一つに、「偽サポートスタッフ」というものがあります。フォーラムやチャットに紛れこみ、ゲーム会社のサポートのふりをしてユーザーのアカウントを聞き出してしまうものです。勝手にパスワードを変えてしまえば、そのアカウントの乗っ取りはたやすくできてしまいます。特にビギナー（ニュービー）が狙われています。

4 その他のデータ窃盗

ゲームプレーヤーが重要なデータを失うには、さまざまな可能性があります。フィッシング攻撃についてはすでに説明しましたが、マルウェアもまた、ゲームプレーヤーのデータを狙って、しばしば用いられています。

マルウェアは、よく知られているゲームの（不法）コピーもしくは不正行為や特殊機能（＝チート）の提供を偽装するのに使用される傾向にあります。特に日本では、ファイル共有ソフト上に偽装ファイルが仕掛けられ、個人情報その他を盗もうとする行為がしばしば発生しています。

マルウェアは、ゲームをクラックしたりキージェネレーターを提供するようなファイル名を使ってファイル共有のネットワークに潜んでいるのみならず、関連サイトに見せかけたところにも配備されています。

また、ゲームプレーヤーのデータを狙うマルウェアのなかには、USBメモリが挿入されるときにWindowsで自動実行する機能を悪用して感染させようとするものもあります。

マルウェアは、データを狙って、以下の方法で取得しようとします。

ソフトウェアライセンスキー

ソフトウェアのライセンスキーは、コンピュータ内のさまざまな場所に保存されています。あるソフト

ウェアのキーは、レジストリに登録されていますが、多かれ少なかれ狙われる情報が含まれているファイルは、パソコン内のどこかに隠されます。

パスワード窃盗として知られているグループに属するマルウェアは、これらのデータがどこにあるのかわかっており、ゲームや他のソフトウェアのライセンスキーを探することができます。見つかったデータは、その後、データ窃盗グループによって制御されたサーバーに運ばれてしまいます。

ブラウザで保存されているパスワード

一般的に使用されているブラウザならば、いずれでも、パスワードやフォーム入力データを保存する機能を提供しています。この機能は、非常に役立つ便利なものであり、パスワードを使用する際に、はるかに簡便になります。しかし残念ながら、マイナスの側面もあります。データをコンピュータ上に保存しなければなりません。前記のように、パスワード等をコンピュータに保存してあった場合、そこからそれにアクセスしてキャプチャできるので、残念ながら、パスワードの保証は不十分になってしまいます。

ブラウザやブラウザのプラグインによっては、暗号化が十分長いパスワードで行われる限りは、このように得られたデータを役に立たなくするような暗号化機能を提供しているものもあります。しかし、いくつかのマルウェアプログラムによっては、適切ウェブサイトの入力フォームにおいて、それが解読されたところからデータを拾いだそうとする場合があります。そのような「フォームデータの横領」は、また、パスワード欄のコンテンツを読み込み、データ窃盗グループのサーバーにそれを送ることが可能です。

キーロガー

また、マルウェアはキーストロークを記録できるものもあり、キーロガーと呼ばれています。この名称は、機能に制限があるかのように思わせられますが、実は、もっと多くの記録が可能です。たとえば、クリップボードをモニターし、そこにコピーされるすべてのデータを奪い取ることができます。多くのキーロガーは、画面全体を一定の間隔を置いてスクリーンショットを撮るとか、マウスがクリックされる時、カーソルの周りの部分を保存できたりします。

多くの場合、記録保存は、特定のウェブサイトの訪問や入力フォームの出現、特定のゲームの実行のような条件と連動しています。しかしながら、インストールされたキーロガーはしばしば無制限な状態で動作し、ゲームのパスワードだけではなく、それ以外のものも盗みます。多くの場合、キーロガーの被害者は、それまで自分が使っていたメールアカウント、フォーラム、オンラインショップ、およびソーシャルネットワークにアクセスできなくなってしまいます。言い換えれば、オンライン上のアイデンティティすべてを奪うのが、キーロガーなのです。

辞書攻撃とランダム攻撃

ゲームフォーラムへのアクセスのためのデータもまた、試行錯誤を経て、窃取されてしまいます。この場合、攻撃者は、よく用いられるパスワードの一覧表(=辞書攻撃)を用いるか、または、手当たりしだいに特定の長さの英数字の組み合わせる(=ランダム攻撃)ことによって探り出そうとします。いずれにせよ、短いパスワードや「123456」「Admin」または「master」などのよく使用されるパスワードの場合には、すぐさま被害者となる可能性はきわめて高くなります。

ゲーム関連マルウェア

マルウェアプログラムは、コードの特質に基づいて区分が可能です。昨今では年間 200 万種ほどのマルウェアが活動していると言われますが、これらをプログラミングの類似性によって、ある程度まとめて、ファミリーとして分類できます。たとえば、ほとんどプログラムは同じように構成されている、ヘッダ情報の一部だけを変えたものは、亜種としてまとめます。近年は、ゲーム関連のマルウェアとしては、以下のファミリーの活動が盛んです。

オンラインゲームズ

オンラインゲームズ (OnlineGames) は、ゲーム関連でもっとも一般的なファミリーです。これらの亜種は、2010 年上半期に出現したマルウェア全体のうち、約 1.9% を占めました。これはファミリー別では、7 番目に多い数になります (詳細は「G Data マルウェアレポート 2010 年上半期」を参照)。

オンラインゲームズは、広く言うと、トロイの木馬型に含まれ、パスワード窃盗のグループに入ります。このファミリーは特定のゲームに制限されず、さまざまなゲームを狙うマルウェアが含まれます。攻撃可能なゲームは数多く、以下のものを含んでいます。

2moons	Fly for fun	Maple Story	Online
Age of Conan	Gash	Metin 2	Twelve Sky
Aion Online	Goodluck	Perfect World	Valhalla
Cabal Online	Knight Online	Seal Online	World of Warcraft
Dekaron	Last Chaos	Silk Road Online	
Dungeon Fighter	Lineage	The Lord of the Rings	

パスワード窃盗を特質とするファミリーに属するマルウェアは、偽装することによって、不正な機能をウィンドウズエクスプローラーに組み込みます。また、ファイルとレジストリのエントリを隠すために、ルートキットを使用する場合もあります。また、表面上はその動きを目立たなくさせることが可能なため、HackShield や nProtect 社の GameGuard など、ゲームメーカーが利用しているハッキング防止ツールも回避可能です。オンラインゲームズの亜種の大多数は、すべての共有ディレクトリに複製を組み込み、「autorun.inf」と呼ばれるファイル内に不正プログラムを組み込みます。すると、たとえば USB メモリやその他リムーバブル記憶媒体がパソコンに接続したときに自動的に不正プログラムが作動します。

マガニア

マガニア (Magania) は、主に、韓国や日本で活動しています。2010 年上半期のマルウェアの全体のうち、1.6% を占めました。マルウェアファミリーとしては 11 番目に多く出現しました

マガニアは、キーロガーのグループに属しています。名前の通り、リネージュやメープルストーリーで知られる、台湾のゲームメーカーであるガマニア (Gamania) に関連したものです。この事例の大多数では、マルウェアはメールを通じて拡散します。添付ファイルが実行されるとき、画像が隠蔽工作として出現し

ます。その際、マルウェアはバックグラウンドで動作します。マガニアのファミリーのマルウェアは、自身を隠しつつ、ウィンドウズのエクスプローラーと IE のプログラムに複製を送り込み、ユーザーには見えないところで活動し続けます。そのあと、ゲームのアクセスデータを盗み、インターネット上にある複数のサーバーにデータを送信します。一部の亜種は、さらに追加でマルウェアをダウンロードして別の活動を行う場合もあります。

WOW

WOW という名のマルウェアファミリーは、その名のとおり、World of Warcraft のアクセスデータを狙います。2010 年上半期のマルウェアのなかでは、0.3%を占め、その数は、49 番目となります。

特定のゲームを狙うものとしては、最大数です。データはキーロガーを使って盗み、インターネットを介してサーバーに送ります。盗まれたアクセスデータは、被害者のアカウントを略奪したのち、関連のフォーラムで仮想通貨やのキャラクターを販売するのに使用されます。

その他のマルウェア ファミリー

2010 年上半期に出現したマルウェアのなかで、リミア(Lmir)は、75 番目に多いマルウェアファミリーでした。プロキシは、中国や韓国で非常に人気のある Legend of Mir というゲームのアクセスデータを狙います。

103 番目には、ティバ(Tibia)という、ドイツのゲームのアクセスデータを狙うキーロガーのファミリーがランクインしています。

日本におけるゲーム関連マルウェア

ゲームに限定されるわけではありませんが、ファイル共有のネットワークを通じて感染するマルウェアが、日本では長期間にわたって活動しています。個人情報盗み出すものが主流ですが、アイコンを差し替えたり、パソコンを破壊するようなものもあります。

2004 年に Winny 使用者をターゲットにした、通称 Antinny が登場し、2005 年には Winny 以外のファイル共有ソフトでも感染した山田ウイルス、2006 年には山田オルタナティブ、そして原田ウイルスが登場します。そして、2010 年には原田ウイルスの作者が再び、タコイカウイルスをばらまきました。

また 2010 年 9 月には、DS ポケモンを違法に楽しむためのデータを装ったマルウェアが登場しましたが、これもまた、ファイル共有のネットワークに仕掛けられました。

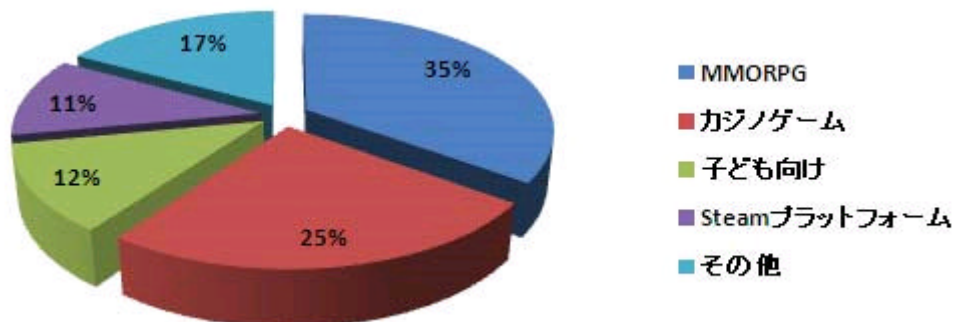
これらに共通しているのは、金銭目的でネット犯罪者が個人情報を盗むというよりも、ファイル共有のネットワークを利用している人びとをターゲットにし、かつ、彼らの個人情報をネット上にさらすことに主眼がある、という点です。その結果、直接的な金銭被害ではなく、周囲からの非難や知人からの信頼の失墜、職場に知られて失職、といった、社会的信頼に関して害を被っており、ここに、欧米圏との、決定的な文化的差異が見出されます。

ただし 2010 年 5 月には、アダルトゲームのデータを装った「KENZO」という名のマルウェアが、同様の手口で金銭目的で利用され、加害者が逮捕されました。したがって、日本では決して金銭目的のマルウェア利用はゲーム関連では起こらないというわけではありません。これは、金銭被害に加えて、社会的信頼を失墜させるような攻撃も同時に、注意せねばならないということです。

危険なゲームサイト

G Data のセキュリティラボでは、怪しいサイトを自動的に探し出したうえで、そのサイトの分析を行い、データとしてページ画像をスクリーンショットとして保存し、データベースを作成しています。2010年1月から6月のあいだで、66,534の危険なサイト（詐欺サイトやマルウェアを仕込んだサイトを含む）を採集しましたが、そのうち6.5%が、オンラインゲームにかかわる内容でした。

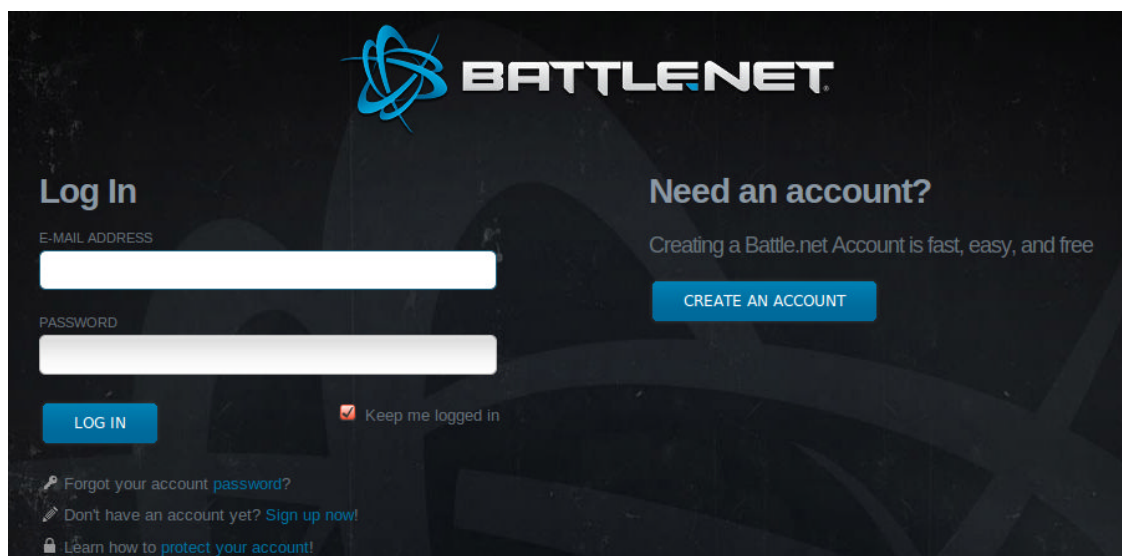
この6.5%のシェアは、さらに、以下のような項目に分類されます。



グラフ1 危険なゲーム関連サイトの分類

もっとも大きな割合を占めたのは、MMORPG（不特定多数と対戦を行うタイプ）で、35%でした。ここには、ワールド・オブ・ウォークラフト（WoW）やメティン2、ルネスケイプ、チビアなどが含まれています。次いで、カジノ（25%）、子供向け（12%）、Steamプラットフォーム（11%）、その他（17%）の順でした。

G Data が採集した不正サイトにおける、最も一般的な攻撃方法は、フィッシング詐欺でした。ユーザー数の多いゲームのオリジナルページを模倣したサイトを用意し、ネット上に公開し、この偽サイトにアクセスしたユーザーのアカウントを盗みとります。



スクリーンショット2 本物のページとほとんど見かけは違いが分からない偽ページの例

本物（アメリカ）の URL	https://us.battle.net/login/en/
偽物の URL	http://us.bvttie.net/login/login.htm http://us.bottlo.net/login/login.xmlref.html http://us-battlefusbattlenet.net http://us-battletests.net http://us.bbattlie.net http://us.balittlie.com http://www.account-battle.net/wow http://www.wowsupport.net

表1 battle.net の正しいアドレスとそれに似たフィッシングサイトのあいだのつづりは、とてもよく似ている

カジノゲーム(主としてポーカー)と子供向けゲーム(しばしばバーチャル・コミュニティ)においては、攻撃者は、アカウントを入力させようと、魅力的なボーナスページを使用するのが、よくある手口です。

Steam プラットフォームのアカウントも、攻撃者にとっては、狙う価値のあるものです。ゲームプレーヤーが、1つのアカウントを使用することで、複数のゲームをすることができるからです。したがって、ネット犯罪者にとっては、1つのアカウントで、1ゲームだけではなく多くのゲームにアクセスできるというメリットがあります。そのような Steam アクセスデータは、たとえば、裏市場で売りに出されます(表2を参照)。

「その他」のカテゴリーは、これまでの分類に入れることのできないものが含まれています。ここには、「warez」が主となっています。つまり、ゲームのためのクラック機能やキージェネレーターを持ったソフトのあるサイトや、URLに「game」や「gaming」を含む他のサイトが含まれます。

ゲーム関連の裏取引価格

ネットの裏市場では、カード情報、プログラムやゲームの登録キー、ID とパスワード、など、あらゆるものが取引されています。価格は、提供されるデータ量や知名度、ゲームのレベル上昇状況などで大きく変わります。

以下に示される価格は、不法な取引を行っている掲示板からの例です。

Steam、Battle.net のアカウント	価格
16 ゲームのアカウント: Counter-Strike 1.6, Counter-Strike: Source, Counter-Strike: Condition Zero, Day of Defeat, Day of Defeat: Source, Half-Life, Half-Life Deathmatch Classic, Half-Life Opposing Force, Half-Life Blue Shift, Half-Life 2, Half-Life 2 Deathmatch, Half-Life 2 Lost Coast, Red Orchestra: Ostfront 41-45, Ricochet, Saints Row 2, Speedball 2 Tournament, Team Fortress Classic	40 ユーロ
8 ゲームのアカウント: Counter-Strike: Source, Dark Messiah of Might & Magic, Day of Defeat: Source, Left 4 Dead, Left 4 Dead 2, Metro 2033, Saints Row 2, Supreme Commander	35 ユーロ
Call of Duty: Modern Warfare 2 Uncut	22 ユーロ
Counter-Strike: Source, Counter-Strike 1.6, Half-Life 2 Episodes 1 and 2, Team Fortress 2	20 ユーロ
Call of Duty: Modern Warfare 2, Order of War, Order of War Challenge	20 ユーロ
Counter-Strike: Source, Day of Defeat: Source, Half-Life 2 Lost Coast, Half-Life 2 Deathmatch	16 ユーロ
Alien vs. Predator Uncut	12 ユーロ
Starcraft II: Wings of Liberty, World of Warcraft	10 ユーロ
Empire: Total War, Warhammer 40,000 Dawn of War II, Warhammer 40,000: Dawn of War II Chaos Rising	10 ユーロ
GRID	5 ユーロ
Trackmania United Forever, Tombraider: Underworld	5 ユーロ
Counter-Strike 1.6	5 ユーロ

ゲームキー	価格
Battlefield: Bad Company 2 – Limited Edition	15 ユーロ
Assassin 's Creed – Special Edition	12 ユーロ
Command & Conquer 4: Tiberian Twilight	12 ユーロ
World of Warcraft Wrath of the Lich King – Collector 's Edition	12 ユーロ
World of Warcraft Wrath of the Lich King	10 ユーロ
Aion	10 ユーロ
Battlefield: Bad Company 2	10 ユーロ
FIFA 10	9 ユーロ
World of Warcraft Burning Crusade	6 ユーロ
World of Warcraft Classic	5 ユーロ

ゲーム時間とポイント	価格
PlayStation Network Card (50.00 ユーロ)	18 ユーロ
Xbox Live (12 ヶ月ゴールド)	12 ユーロ
World of Warcraft (60 日のゲーム時間)	10 ユーロ
NCSOFT (60 日のゲーム時間)	10 ユーロ
1,000 Sim ポイント	8 ユーロ
1,000 Wii ポイント	5 ユーロ

表2 さまざまな裏ショップにおけるゲーム関連の取引価格例

なお、ネット裏市場の全貌については、G Data のホワイトペーパー「アンダーグラウンド エコノミー」(2009 年 9 月)、「アンダーグラウンド エコノミー Part2」(2010 年 5 月)も参照してください。

リアルマネーとの取引




ゲーム用のアイテムやアカウントなどは、多かれ少なかれ合法的な場所で販売されています。世界中でよく知られているオンラインのオークションサイトは、なかでも非常に人気があります。また、ゲーム専用のオークションサイトが、ゲームにおけるアイテムとアクセスデータを販売するために設立されています。たとえば、playerauctions.com、mmobay.netまたはwowbay.netです。しかしながら、ほとんどのゲームメーカー(たとえば、ジンガやブリザードなど)では、ゲーム環境外でのゲーム製品やアカウントの売買を禁止しています。

3) In-Game currencies/goods
:
:
:
d) Transfers of Virtual Currencies and Virtual Goods are strictly prohibited except where explicitly authorized within the Service. Outside of the game, you may not buy or sell any Virtual Currency or Virtual Goods for "real world" money or otherwise exchange items for value. Any attempt to do so is in violation of these Terms and may result in a lifetime ban from Zynga Service and possible legal action.

スクリーンショット 3 禁止の例としてジンガの使用条件を抜粋

たとえば、playerauctions.comのオークションでは、すでに述べた「正規」ゲームアカウントと異なった価格で高値のアカウントを取り引きしています。

価格はキャラクターのレベル、スキル、利用可能な仮想通貨、そしてそのキャラクターがプレイしているサーバーによって大きく異なります。29のアカウントからは、現在の最も低い申し出は40USドルで来ています。しかしながら、スクリーンショット4におけるオファーは、かなり高い価格に達することができることを示します。

Offer	Price	Seller's Delivery Guarantee	Date	Secure Payment
 Superior WoW account - Offering: Mage + Rogue + DK tank/DPS 6420 GS ++ all of em and include SC2	\$2,550.00	24 Hours	Aug-06	View Details
Ashes of Al'ar mount and full t10 Tank/Kitty/Tree and pvp gear sets!	\$2,212.00	24 Hours	Jul-28	View Details
 Level 80 lock gnome alliance 3900 SP 6190 GS pve and 6075 GS pvp 11/12 ICC25 heroic + 5 lvl 80 toons	\$1,100.00	24 Hours	Aug-08	View Details
 2xLVL 80 Kingslayer Account + Everything you would ever want	\$800.00	20 Minutes	Aug-08	View Details
80 Orc hunter 6k gs & 80 Troll shaman 6k gs. 12/12 in both 10/25man and 11/12 HM achivement.	\$670.00	24 Hours	Jul-26	View Details

スクリーンショット4 現在のplayerauctions.comで最も高価なアカウント

これらの数字を見ると、なぜゲームプレイヤーがネット犯罪者に強く関心を抱かれているのかが、さらに明白になります。それはもうゲームを娯楽としてとらえているのではなく、また、仮想通貨を目的としているのでもありません。それは過小評価されるべきでない多量の現金に関するものなのです。

日本語版特別編

ソーシャルゲームの危険度

2002年以降、「ラグナロク」「ファイナルファンタジー」「リネージュ」などを筆頭に、日本では「オンラインゲーム」が多くのユーザーを集め、大きな市場を形成してきました。それまでスタンドアロンで行われていたゲーム（主にRPG）がオンライン化し、さまざまな人たちと一緒にプレイできるようになったことが、その成功の主な理由と言えます。今でも、一時期の興隆はないものの、安定した人気を誇っています。

それに対して今年2010年は、「ソーシャルゲーム」というカテゴリーが、じわりじわりと注目されつつあります。たとえば、7月にソフトバンクがソーシャルゲームの最大手であるジンガ（Zynga）に出資しジンガジャパンを設立、8月にはジンガがウノウを数十億円で買収、9月には20万人を集めた東京ゲームショウでも「3D」と並んでソーシャルゲームがキーワードになっていました。

さらに、10月1日からはヤフー（YAHOO）とディー・エヌ・エー（DeNA）がパソコン用のソーシャルゲーム「Yahoo!モバゲー」を開始するなど、各社が活発な動きを見せています。ゲーム会社やプラットフォーム提供会社、マスコミはもちろんユーザーも含めて、全体的に盛り上がっている感があります。

ところで、ソーシャルゲームは、フェイスブック（Facebook）やミクシィ（Mixi）など、SNSでのコミュニティを基盤にしつつ、そのコミュニケーションツールの一つとして導入されたゲームを指します。本格的なもの、高度なもの、というよりも、交友を深める機会として、誰もが気軽に楽しめるということに主眼があります。アイテム等への課金を行うものの、通常のプレイについては無料を基本とすることから、利用者数は爆発的に増加する傾向にあります。

すでに知られているところでは、ミクシィの「サンシャイン牧場」（中国製）がすでに、500万人以上の登録者をかかえているほどです。同じように、大規模なSNSの会員を擁しているグリー（GREE）やモバゲータウン（ディー・エヌ・エー）なども、急ピッチで市場拡大を狙っています。もちろん世界で2億人のユーザーをかかえるフェイスブックも、日本市場でももっと力を入れてくることでしょう。

ところで、日本のゲーム市場においては、パソコンを用いる層以外に、ケータイを用いる層と、Xbox360やPS3、Wiiといった、それぞれのゲームプラットフォームを用いる層と、三つの層があります。そのなかで、パソコンを用いる場合、ゲーム機やケータイと異なり、誰もが利用しやすく、仕事や友人づきあいの人間関係にも組み込んで違和感がないという意味で、もっとも多くのユーザーが利用するポテンシャルを秘めていると言えるでしょう。

しかしそれは同時に、パソコンを用いる以上、ソーシャルゲームのユーザーは、不可避免的にマルウェアによる猛威にさらされるということの意味します。すでにオンラインゲームにおいては、さまざまなネット犯罪が蔓延しています。これまでの手口はそのままソーシャルゲームにおいても応用されることでしょう。また、それに加えて新たな、ソーシャルゲームやSNSの特性を悪用した仕掛けも増えてくるはずですが、

巨大なネット犯罪組織は、しばしば英語、スペイン語、ロシア語など欧米語を基本に暗躍していますが、少なくともゲーム市場においては、中国、韓国、北朝鮮、台湾、日本といった極東諸地域においても、活発な動きがあります。このホワイトペーパーは欧米圏を中心とした事例を主に扱ってきましたが、その手法自体はそのまま日本でも応用される可能性があります。したがって本書の内容は、事前対策として役立つ部分もあります。是非しっかりとお読みいただき、オンラインゲームはもちろん、ソーシャルゲームまわりの安全対策にも活用してほしいと思います。

なお、日本語版特別編として、以下では、日本におけるゲームとマルウェアの課題と、2010年1月～9月における国内でのオンラインゲーム関連の主な出来事について、併載しました。こちらも併せてお読みください。マルウェアのない、安全で安心なパソコン環境でゲームを楽しめますよう、心から願っています。

日本におけるゲームとマルウェア

日本におけるゲームとマルウェアをめぐる課題は、以下の5点にまとめられるでしょう。

(1) USB ウイルス

ゲームユーザーは、アクセスデータやバックアップをUSBメモリもしくは外付ハードディスクに保存している場合が多く見られます。ネットに接続していないから大丈夫と思う人もいるかもしれませんが、逆です。それ専用のウイルスが蔓延しています。

一般には、USBウイルス、コンフィッカー、ダウンロード、キド等の名称で呼ばれています。2010年9月にバッファローのWi-Fiルータに混入してしまったのも、この亜種でした。

(2) ファイル共有経路による感染

改正著作権法が2010年1月1日に施行され、映像や楽曲などの不法ダウンロードに歯止めをかけようという動きがあり、ゲームソフトも、マジコンへの規制などが検討されており、厳しくチェックされつつあります。しかし同時に、ファイル共有ソフトを利用した違法ダウンロードは、決して減少していません。これまでの経緯からみても、ここを攻撃拠点とするネット犯罪者は、特に日本においては、決して少なくないでしょう。ロマンシング詐欺を仕掛けた人びとやタコイカウイルスの制作者が逮捕されたように、日本の警察はこの手の犯罪にかなり注目しているはずで

(3) SQL インジェクションとRMT

オンラインゲームのアカウントなどのデータを盗み出すのに、SQLインジェクションが頻繁に使用されました。この場合、そのアカウントを使って、ゲーム内の仮想通貨やキャラクター、アイテムなどをRMT(リアルマネートレーディング)にて売ってしまう場合もあれば、支払用のクレジットカードデータを探し出し、口座から勝手にお金を引き出すこともありえるかもしれません。

なお、RMTに関する規制をメーカー側も行っていますが、増加する一方であり、同時にトラブルも多発しています。次ページにある「出来事」は、氷山の一角にすぎません。

(4) ロマンシング詐欺

アダルトゲーム関連の情報と偽ってファイル共有ソフトに画像や動画ファイルに偽装したマルウェアをアップロードし、感染パソコンの情報を窃取、それをもとに恐喝し金銭を受け取るという被害が2009年から2010年にかけて発生し、マルウェア作成者と詐欺を働いた人物が逮捕されました。同様の手口はこれからも増える可能性があります。

(5) ソーシャルゲーム

ソーシャルゲームは、一見信頼できる人間同士がコミュニケーションをとりあっているように見えて、実は、ネット犯罪者が紛れ込んでも気づかない可能性があり、その盲点を突いて、マルウェアをしかけられたり、不正アクセスを試みられたりするおそれがあります。

また、社会的に注目されているせいもあって、ソーシャルゲーム関連の会社も、ネット犯罪者の攻撃の対象となりやすくなっています。

オンラインゲーム関連の出来事 2010年1月～9月

9月21日 TwitterにXSS攻撃

Twitterのクロスサイトスクリプティングの脆弱性を悪用、ツイートのURL内にJavaScriptコードを埋め込むことにより、ユーザーがリンクURLにカーソルを移動させただけで、フォロワーに自動的にツイートが送られてしまうというもの。ただしこの脆弱性は8月にすでに発見されていたものであり、しかも、一度は修正パッチで対応していた。しかしアップデートを行ったことで問題が再び発生し、ユーザーが悪用した。SNSの場合リアルタイムで爆発的に拡散するので、今後も要注意が必要。

9月21日 DSポケモン関連マルウェア

ニンテンドーDS専用ゲームソフト「ポケットモンスターブラック・ホワイト」を違法に使用するためのデータを偽装したマルウェアがファイル共有のネットワークに登場し、ゲームを違法コピーして使用できる機器である「マジコン」ユーザーの個人情報がネット上にさらされる。

9月6日 ワンタイムパスワードの利用

飛天ジャパンが「ラグナロク」をはじめとしたガンホーのオンラインゲームに対応した「ワンタイムパスワードトークン BRUCE KEY」を発売。

9月2日 不正アクセスは横ばい傾向

警察庁より「平成22年上半期のサイバー犯罪状況等について」が発表。不正アクセス禁止法違反については、85件で昨年の上半期の1,955件より大幅減(-95.7%)。ただし、昨年のデータには、15人の犯行グループによる組織的なオークション詐欺(1,813件)が含まれていたため、この数字を除けば、ほぼ同等の数になる。www.npa.go.jp/cyber/statics/h22/pdf01-1.pdf

8月27日 GREEを騙るフィッシング

「おめでとう御座います！」等のタイトルで、GREEの獲得ポイントが数万円分たまつたと偽の告知を行い、個人情報を盗み取るためのフィッシングサイトが出現。

<http://www.antiphishing.jp/alert/alert455.html>

8月12日 RMT行為の禁止のよびかけ

「リネージュ」をはじめとしたオンラインゲームを扱っているエヌ・シー・ジャパンは、RMT行為を利用規約で禁止しているにもかかわらず実際には増加している現状に対して、ゲーム環境に悪影響を及ぼすので禁止するようあらためて呼び掛ける特設サイトを公開。

<http://www.plaync.jp/event/stopRMT.htm>

7月23日 ガンホーへのアカウントハッキング

ガンホーで、アカウントハッキングが判明。ガンホーによれば、個人情報などの流出はないものの、盗まれたパスワードによるログインが行われた形跡があったという。

<http://raguweb.net/log/eid2464.html>

7月15日 高校生による不正アクセス

不正アクセス禁止法違反の疑いで、16歳の男子高校生を書類送検。2月9-11日に11回、自宅のノートパソコンから23歳の男性のID、パスワードを使ってオンラインゲームにアクセスし、7,800円分のゲームポイントを不正に使用。

7月14日 女性による不正アクセス

他人のパスワードを使って「アバター」を乗っ取ったとして、無職29歳の女性を不正アクセス行為の禁止等に関する法律違反の疑いで逮捕。2009年12月15日にインターネット上で知り合った40代の女性のパスワードを勝手に使って不正にアクセスし、アバターに着せる服や帽子などのアイテム42点を自分のアバターに渡す。被害総額は10数万円。どのようにパスワードを知ったのかは不明。

6月11日 モバゲーでフィッシング詐欺

DeNAが運営する携帯向けポータルサイト「モバゲータウン」を騙ったフィッシング詐欺が出現。モバゲーユーザーに対し、仮想通貨「モバコイン」が3倍になる「ポイント増量キャンペーン」を謳う偽メールを送付するというもの。メールの文中にあるURLにアクセスすると、「モバGAME」というサイトに飛ばされ、個人情報を入力するよう誘導される。

6月5日 FFへの不正アクセス

スクウェア・エニックスのFFXIに対して、不正アクセス攻撃が行われ、IDとパスワード、その他の登録情報が盗まれる。クレジットカード情報は流出していないとのこと。

6月2日 電気通信事業法違反

日本のオンラインゲームへのアクセスが規制されている中国からの通信を中継するため、総務省に届けることなくサーバーを4台設置したとして、中国籍の30歳の女性が電気通信事業法違反で逮捕。また、47歳の知人男性も同幫助で書類送検。この女性は、2009年3月から8月のあいだに中継手数料として、中国の利用者13人から、月に計約28万円を得ていた。また、2005年頃より中国でアルバイトを雇いゲームをさせ、得たアイテムをネット市場で現金化する不正行為もしていたという。

6月1日 ゲームボットがセキュリティ強化

ゲームボットはゲームコンテンツの公式サイトへのログインシステムに、セキュリティ強化を目的とした新システムとして「画像認証システム」および「アラートメールシステム」を導入。各ゲームコンテンツの公式サイトへのログイン時に画像認証が必要となり、連続で一定回数ログイン失敗があった場合、アカウント保護のため一時的にログインを行うことができなくなる。その際、登録メールアドレスに対して、ログインの一時停止に関するアラートメールが送信されるというもの。

5月27日 ロマンシング詐欺犯の逮捕

ネット関連会社「ロマンシング」社長を名乗る20歳の男性(事件当時19歳)とプログラマーの27歳の男性が、パソコンネットワーク上の詐欺の疑いで逮捕。2009年11月に、2人は、個人情報を盗む「暴露ウイルス」(=自称「Kenzo」)を、アダルトゲームに見せかけてファイル共有ネットワークを通じてばらまき、獲得した数名の個人情報を「著作権法違反者」としてインターネット上に公開し、情報削除料(当初は1,500円だったが後に値上げして5,800円)を架空団体「IC0国際著作権機構」に振り込むよう要求し合計数万円を詐取した疑い。

5月26日 ウェブマネーを使った詐欺

2009年8月中旬に、オンラインゲーム「レッドストーン」で使える仮想通貨を売ると掲示板に書き込み、購入を希望した16歳のアルバイト少年から3万4千円分のウェブマネーをだまし取った疑いで、無職の24歳の男性が逮捕。容疑者は少年とメールを数回やりとりし、価格などを決めたが、少年からウェブマネーを使うのに必要なプリペイド番号などをメールで知ると仮想通貨を渡さなかった。受け渡しはオンラインゲーム上の指定の場所で待ち合わせて渡すというものだったが、容疑者は現れなかった。

3月4日 増加傾向にある不正アクセス

警察庁が2009年における不正アクセス行為の発生状況の統計データを公表。不正アクセス行為の認知件

数は2,795件で、前年より506件増加、そのうち95.6%が国内からのアクセスだった。被害届を出した機関は、プロバイダが最も多く83%を占めた。不正アクセス後の行為内容は、ネットオークションへのなりすまし出品が77%、オンラインゲームにおけるアイテムの不正取得が12%だった。攻撃方法については、セキュリティホールへの攻撃が1%程度で、残りはすべてパスワード窃盗によるものだった。手口の詳細については、フィッシングサイトからの入手が82%、共犯者からの入手が7%、他人からの購入が4%、が上位であり、スパイウェア等のマルウェアによる入手は0.3%、ファイル共有ソフトや暴露ウイルスによる入手は0件だった。実際に利用した経路については、インターネットオークションが85%、メールが7%、オンラインゲームは3%だった。

http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_000011.html

2月18日 不正アクセス禁止法違反で小学生を補導

不正アクセス禁止法違反の疑いで15歳の男子中学生を検挙、12歳の女兒を補導。男子生徒は1月6,7日に18歳の男子高校生のIDとパスワードを用い12回にわたりオンラインゲーム「テイルズウィーバー」に不正アクセス。また女兒は2009年10月13日に同市内の15歳の女子中学生のIDとパスワードを用い1回、同「ハンゲーム」に不正アクセス。それぞれゲーム内のチャットで誘い、IDとパスワードを入手し、アイテムを奪い取る。

2月15日 オンラインゲーム関連の複雑な手口

中国籍の27歳の大学留学生が、自宅に無届けでサーバー2台を設置運営していたことにより、電気通信事業法違反の疑いで逮捕。容疑者はまず、日本の男性になりすましてインターネット銀行の口座を開設、アクセス数などに応じ報酬が支払われるポイントサイトに登録した。その後、容疑者のサーバーを経由して中国から日本のオンラインゲームを利用させる際に、アフィリエイトを活用し600万円ほどの報酬を得ていた。サーバーには2009年2~7月で約170万回のアクセスがあったという。2009年1月下旬に大学生から「オンラインゲームの仮想通貨が盗まれた」との相談を受け警察が調べた結果、全貌が判明。

1月21日 フィッシング詐欺

オンラインゲーム「ファンタシースターユニバース」をかたるフィッシング詐欺。IDとパスワードを盗むことが目的。攻撃者は、同ゲームのログインページに見せかけた偽サイトを用意。同ゲームのユーザーが集まるファンサイトの掲示板などに、その偽サイトのURLを書き込んで誘導。ユーザーをだまして、IDとパスワードを入力させようとした。

1月18日 電気通信事業法違反

無届けでインターネットのサーバーを運営し、本来は中国からは利用できない日本のオンラインゲームに不正アクセスさせたとして、電気通信事業法違反の疑いで中国籍の無職28歳の男性が逮捕。2009年6~9月に自宅に中国からのアクセスを中継するサーバーを設置し、無届けで運営した疑い。契約した日本のプロバイダのパスワードを中国の客に伝え月6千円の代金を受領、3カ月で160万円ほどの報酬を得ていた。

安全対策

ネット犯罪者による攻撃や詐欺から身を守り、アクセスデータを盗まれたり、パソコンを攻撃されることなく、安全にオンラインゲーム（ソーシャルゲーム等を含む）を楽しむには、以下の8項目をチェックし、対策を行ってください。

1) HTTP フィルタの使用

ウェブサイトに潜むマルウェアやフィッシングサイトしっかりとチェックする機能、たとえば、HTTP フィルタを機能として含む、高性能なインターネットセキュリティ製品を使いましょう。

2) ファイアウォールの使用

スパイウェアをはじめとしたさまざまな外部からの攻撃、もしくは内部からの勝手な通信を遮断するファイアウォール機能を利用しましょう。

3) スпамフィルタの使用

メールによる怪しい誘いや攻撃を避けるために、大量に拡散されるメールをリアルタイムにブロックできる機能や、スパムフィルタを含む製品をご利用ください。

4) パスワードの長さ

ゲームのパスワードには、数字、アルファベット、特殊記号を混ぜた、8文字以上のパスワードを使用してください。

5) パスワードの使い分け

用途に応じて、いくつかのパスワードを使い分けてください。同じパスワードを使用すると、盗まれてしまった際に、被害が大きくなるおそれがあります。

6) パスワードの保存

入力済のパスワードをブラウザに自動表示させないでください。

7) URL の確認

詐欺サイトに引っ掛からないように、表示されている URL を随時、確認しましょう。特に、ID やパスワードを入力する画面、オンラインバンキングを利用する際には、より注意が必要です。間違っても、ウェブやメールに表示されている URL をそのままクリックするのはやめましょう。短縮 URL も用心してください。

8) ファイル共有ソフト

ファイル共有ソフトを使用しないだけでも、かなり、感染や攻撃のリスクが軽減されます。