K-001

オンラインゲームのセキュリティのための学際的フレームワーク

Interdisciplinary Framework approaching Security in Massively Multiplayer Online Games

山根 信二 † Shinji R. Yamane
馬場 章 ‡ Akira Baba

1. はじめに

「オンラインゲーム」は，オンラインカジノ，モバイルゲーム，あるいは屋内で PC をつないで対戦する LAN ゲームなど，多くのゲームジャンルやネットワーク利用形態を含んでいる．本論文ではその中でも MMOG(Massively Multiplayer Online Game) のセキュリティについて検討する．これまで MMOG については，MMORPG (Massively Multiplayer Online Role-Playing Game) や MMOFPS (Massively Multiplayer Online First-Person Shooter)，MUD (Multi-User Dungeon)，カジュアル MMO といったサブジャンルごとに議論される一方で，*Second Life*®のように「ゲーム」を名乗っていない仮想空間サービスも含めた “Persistent Worlds”(継続する世界)[1] として総合的な把握も進められてきた．

仮想空間や分散コンピューティングの研究は長い歴史を持っているが [2][3]，その中でもオンラインゲームは過去の事例の中でも最大の参加者を集め，さらにリアルの世界への影響力を及ぼす仮想空間の代表的な事例として考えることができる．本論では仮想世界がリアル世界にどのように関わるかをオンラインゲームのセキュリティという観点から検討する．

1.1 概論

MMOG のセキュリティは，一般的なオンラインサービスとは異なる特徴を持っている．主な特徴を以下に示す．

1. ゲームデザインに対する依存性: ゲームデザインによって要求されるセキュリティレベルやサポートするユーザ層が異なる (類似のサービスを提供しても，セキュリティ破りが破滅的効果を持つものと損失にならないものがある [4])
2. 時間に対する依存性: MMOG タイトルが何年間提供されるか，セキュリティ投資の見積りが難しい．開発時点で許容できたリスクが数年後に大規模な攻撃を受ける場合もある．
3. ユーザコミュニティに対する依存性: 設計時に意図していない動作をユーザが試みる場合，時には大規模な共働体制によってシステムが解析され，技術力のない利用者でも利用できるツールが配布されうる．

こうした特徴が汎用的なセキュリティの構築を困難にしてきた．またこれまでセキュリティコミュニティとエンターテイメント産業の間には他の IT 関連産業と比べ密接な関係がなく [5]，MMOG の設計から運用におよぶプロセスにおいて開発者と研究者が問題を共有し，研究成果を応用するポイントを見出すためのフレームワークが必要とされている．

2. なぜオンラインゲームのセキュリティが問題なのか

2.1 社会的関心の高まり

リスク認知およびリスク評価の観点から，オンラインゲームのセキュリティは社会的な重要性を持つと考えられる．

オンラインゲームに関わるトラブルの報道が増加しているが，これは実際のセキュリティレベルをどのように反映しているのだろうか．筆者らは，報道だけでなく犯罪統計においてもオンラインゲームに関する認知件数が激増したことを示し，社会全体の IT セキュリティ対策が進む一方で，オンラインゲームを通じてユーザが抱く「体感治安」は改善されずむしろ悪化していることを示唆した [6]．

またオンラインゲームは娯楽目的以外の情報インフラとむすびつきつつある．2001 年の Castronova による報告以来，オンラインゲーム内の仮想世界の経済活動および市場の拡大は社会的にも注目を集め [7]，オンラインゲームの仮想世界に多くの企業が参入している．その一方で，オンラインゲームのセキュリティに対する取り組みが他業種に遅れをとっていることで，オンラインゲームをめぐるリスクは大きく変動した．いまやオンラインゲームは仮想世界とリアル世界とのプラットフォームを実現すると同時に，双方の世界のセキュリティにとって “the weakest link” にもなりうると考えられる．このような急激な産業の発展に対応できるセキュリティ研究の確立が必要とされている．

2.2 専門家にとっての課題は何か

オンラインゲームは多くの学問領域が関わっている総合領域であり，その知見の集積地も分散している．たとえば主要な国際的な会合として以下のものを挙げることができる．

- NetGames(ACM SIGCOMM Annual Workshop on Network and Systems Support for Games)
- ACM NOSSDAV (ACM SIGMM Network and Operating System Support for Digital Audio and Video Workshop)
- USENIX NSDI(Symposium on Networked Systems Design and Implementation)
- GDC(Game Developers Conference)

†東京大学大学院学際情報学府, Graduate School of Interdisciplinary InformationStudies, University of Tokyo
‡東京大学大学院情報学環, Interfaculty Initiative in Information Studies, University of Tokyo

この中で特にセキュリティに注目した場合，オンラインゲームのセキュリティについての専門知の集積は遅れている．セキュリティ分野に置ける共著論文調査 [8] によれば，近年において企業と大学とが少なくからぬ連携を進めてきたことが示されている．ところが同様に企業と大学がセクター間ですすめた研究をオンラインゲームでさがした場合，セクター間の共著論文は皆無といってよい (情報セキュリティ以外の分野では Feng らの共同研究 [9] がある)．

この要因として，ゲーム産業においては，他の成熟した産業に比べて技術公開や文献の整備がなされていないことが指摘されてきた．その一方で，たとえばゲーム AI の分野においては，研究開発の成熟がもたらす変化によって，これから数年で知識の体系化が進むことが期待されている [10]．オンラインゲームのセキュリティにおいても，同様にゲーム産業に関連する研究開発分野を巻き込んだ体系化が期待できる．本研究は，そうした今後の知の体系化に資することを目指すものである．

3. 必要とされるフレームワーク

3.1 集積の次に来るもの

現時点における個別のセキュリティ工学と体系的な知見の両者を備えたものとして，2007 年の Hoglund and McGraw による成果 [11][12] をあげることができる．しかし，対策技術および今後の課題を網羅した同研究成果においても，個別の手法を選択する基準については明らかではない．

選択基準の不在は技術論のみならず，現実のオンラインゲーム運用でも発生している．たとえば「それは運用ではなく設計で解決すべき問題」「それはカスタマーサポートの領分」「それはライセンス上問題ないゲームの遊び方の問題で，事業者のカバー範囲ではない」といった境界設定についてもはっきりとした判断基準が示されていない．このような判断基準としてリスクマネジメントのための上位のフレームワークが必要となる．

3.2 学際的フレームワークの構築に向けて

オンラインゲームのセキュリティの固有の問題に対応するためには手法の集積だけでは不十分である．この視点から，本研究では現在必要とされているのは個別の対策実施を社会の総合的コストの観点から評価するためのセキュリティのフレームワークの構築を提案する．

オンラインゲームのリスクおよび社会的なコストを扱うためには，どの業種がどのように取り組むべきかという産業構造の問題 [13]，(オンライン) ゲーム産業構造を規定するビジネスモデルの歴史経路依存性 [14]，そして展開する地域の地域文化論的な制約 [15, 16, 17] といったリスク／コスト要因に注意をはらい，これまで同一のものとして論じられなかった分野ごとのリスク評価を総合的に扱う必要がある．したがって，本フレームワークには学際的なアプローチが不可欠となる．

3.3 今後の課題

2007 年から，本研究では事例研究の収集と学際的なフレームワークの検討とを同時にすすめている．検討をすすめているオンラインゲームのセキュリティ対策の事例を以下に挙げる．

Senario 1: 中国からのアクセスを中継するサーバを設置し，ゲーム運営会社のサーバにアクセスを集中させ，画面の切替えが遅くなるなどの障害をあたえたとして訴追 (高松地裁 平成 18 年 1 月 13 日)

Senario 2: インターネット上のゲーム運営会社を装って「フィッシング行為」をしたなどとして、中国地方に住む中学 1 年生の女子生徒を不正アクセス禁止法違反の非行事実で補導 (宮城県警, 2006 年 7 月)

Senario 3: 既知の脆弱性を利用してショッピングサイトから個人情報およびクレジットカード番号とパスワードを取得．それを使ってクレジットカード情報を認証に用いているオンラインゲームサイトで金券、商品を購入．さらにサードパーティーのサイトで転売・換金した事例．クレジットカード会社と連携して顧客に周知 [18]

これらの検討をもとに，新たなリスクをどのように認知し，社会的コストをどのように考えるべきか，そのための学際的リスク評価のためのフレームワークはどのようなものになるかを明らかにしたい．

4. まとめ

本論では，オンラインゲームが特有の問題をもつこと，セキュリティについての専門的な知見を集積する必要があることを明らかにし，総合的なコストにもとづいて個別の対策を位置づけるフレームワークの必要性を示した．また，フレームワーク構築のためには学際的な取り組みが必要であること，そして現在検討中の事例研究についても言及した．

オンラインゲームが普及するにつれ，セキュリティについてのコストを誰が負担すべきかという問題は今後さらに大きくなり，今後のサイバーワールドの進展をはかる上で無視できない問題になると考えられる．今後もさらなる研究を進めたい．

参考文献

[1] Jamaes, D. and Walton, G.(eds.): *2004 Persistent Worlds White Paper*, IGDA Online Game SIG (2004). http://www.igda.org/online/IGDA_PSW_Whitepaper_2004.pdf (visited April 23, 2008).

[2] Vinge, V.: *True Names: And the Opening of the Cyberspace Frontier*, Tor Books (2001). Collection edited by James Frenkel. Contributed by James Frenkel, Danny Hillis, Timothy C. May, John M. Ford, Alan Wexelblat, Pattie Maes, Richard M.Stallman, Leonard N. Foner, Chip Morningstar and F. Randall Farmer, Mark Pesce, Vernor Vinge, and Marvin Minsky.

[3] Montfort, N.: *Twisty Little Passages: An Approach to Interactive Fiction*, MIT Press (2003).

[4] Bartle, R.: *Designing Virtual Worlds*, New Riders Games (2003).

[5] Felten, E.: Foreword, *Exploiting Online Games: Cheating Massively Distributed Systems* [12].

[6] 山根信二，　馬場章：オンラインゲームのセキュリティ: 傾向および課題，コンピュータセキュリティシンポジウム 2007(CSS 2007) 論文集，情報処理学会，pp. 331–336 (2007). October.

[7] Castronova, E.: *Synthetic Worlds: The Business and Culture of Online Games*, University of Chicago Press (2006).

[8] 江波戸謙，ケネス・ペクター，松浦幹太：SCIS における産学連携の状況，2003 年暗号と情報セキュリティ・シンポジウム (SCIS2003) 予稿集，Vol. 1, pp. 569–574 (2003).

[9] Feng, W., Brandt, D. and Saha, D.: A long-term study of a popular MMORPG, *NetGames '07: Proceedings of the 6th ACM SIGCOMM workshop on Network and System Support for Games*, New York, NY, USA, ACM, pp. 19–24 (2007).

[10] 三宅陽一郎：ディジタルゲームにおける人工知能技術の応用，人工知能学会誌，Vol. 23, No. 1, pp. 44–51 (2008).

[11] McGraw, G. and Hoglund, G.: Online Games and Security, *IEEE Security and Privacy*, Vol. 5, No. 5, pp. 76–79 (2007).

[12] Hoglund, G. and McGraw, G.: *Exploiting Online Games: Cheating Massively Distributed Systems*, Addison-Wesley (2007).

[13] 社団法人コンピュータエンターテインメント協会：オンラインゲーム不正事例報告書，Online document (2007). http://onlinegame.cesa.or.jp/20070726.html (visited April 23, 2008).

[14] 山根信二，　馬場章：アプリケーションソフトウェアのビジネスモデルの起源: 黎明期のホビイスト市場に注目して，電子情報通信学会 技術研究報告，Vol. 104, No. 343, pp. 7–12 (2004). SWIM2004–10.

[15] Chen, V. H., Duh, H. B.-L., Kolko, B., Whang, L. S. and Fu, M. C.: Games in Asia project, *CHI '06: CHI '06 extended abstracts on Human factors in computing systems*, ACM Press, pp. 291–294 (2006).

[16] Kabus, P., Terpstra, W. W., Cilia, M. and Buchmann, A. P.: Addressing cheating in distributed MMOGs, *NetGames '05: Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support for Games*, ACM Press, pp. 1–6 (2005).

[17] Consalvo, M.: *Cheating: Gaining Advantage in Videogames*, MIT Press (2007).

[18] サウンドハウス:不正アクセスに伴うお客様情報流出に関するお詫びとお知らせ，Press Release (2008). 2008 年 4 月 18 日付 http://www.soundhouse.co.jp/news/20080418.pdf (visited April 23, 2008).