



Title	Graph-structured Contents Delivery System Protecting Viewer's Privacy
Author(s)	岡村, 真吾
Citation	大阪大学, 2005, 博士論文
Version Type	
URL	<a href="https://hdl.handle.net/11094/45751">https://hdl.handle.net/11094/45751</a>
rights	
Note	著者からインターネット公開の許諾が得られていないため、論文の要旨のみを公開しています。全文のご利用をご希望の場合は、 <a href="https://www.library.osaka-u.ac.jp/thesis/#closed">https://www.library.osaka-u.ac.jp/thesis/#closed</a> 大阪大学の博士論文について

*The University of Osaka Institutional Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

氏 名	岡 村 真 善
博士の専攻分野の名称	博 士 (情報科学)
学 位 記 番 号	第 19617 号
学 位 授 与 年 月 日	平成 17 年 3 月 25 日
学 位 授 与 の 要 件	学位規則第 4 条第 1 項該当 情報科学研究科マルチメディア工学専攻
学 位 論 文 名	Graph-structured Contents Delivery System Protecting Viewer's Privacy (グラフ構造をもつコンテンツに対する視聴者のプライバシを保護した配信システム)
論 文 審 査 委 員	(主査) 教 授 藤原 融 (副査) 教 授 西尾章治郎 教 授 岸野 文郎 教 授 薦田 憲久 教 授 下條 真司 助教授 石原 靖哲

### 論 文 内 容 の 要 旨

インターネットや放送設備を利用したデジタルコンテンツ配信サービスにおいて、グラフ構造をもつコンテンツが登場してきている。グラフ構造をもつコンテンツでは、コンテンツ間に配信順序などの関係が定義されており、その構造に応じて配信を制御する必要がある。

本論文では、グラフ構造をもつコンテンツとしてインタラクティブドラマを対象とし、その配信システムを提案する。インタラクティブドラマでは複数のストーリーが用意されており、視聴者には各シーンの配信において選択肢が与えられ、選択した項目に応じたストーリーでドラマが配信される。コンテンツ提供者は、巧妙にストーリーを用意することにより、視聴者の好みに合わせたストーリーでドラマを提供することができる。一方で、視聴者の選択履歴からその視聴者の性格や思想に関する情報を得ることもできる。そのため、視聴者はコンテンツ提供者から選択履歴を秘匿したいと考える。一方でコンテンツ提供者は、用意したストーリーのいずれかに沿ってドラマを配信するためには選択履歴に関する情報を必要とする。本論文における配信システムの提案では、選択履歴の秘匿と正しい配信制御の実現を目的とする。

本論文は全 6 章で構成される。第 1 章において、研究の背景と目的を述べる。なお、対象とするインタラクティブドラマは二種類とする。一方は、視聴者は選択肢の中からどの項目でも選ぶことができるドラマ（基本インタラクティブドラマ）であり、他方は、視聴者が選ぶことができる項目が過去にその視聴者が選択した項目によって異なるドラマ（条件付き選択項目をもつインタラクティブドラマ）である。

第 2 章において基本インタラクティブドラマの配信システムを提案し、第 3 章において条件付き選択項目をもつインタラクティブドラマの配信システムを提案する。また、使用する暗号方式・署名方式が安全であること及び配信されるドラマが同一である（各シーンにおいて全視聴者に同じ選択肢が与えられ、かつ、同じシーンで同じ項目を選択した視聴者に対して次に配信されるシーンが同じである）ことを仮定したとき、各提案システムが安全性要件を満たすことを証明する。各提案システムにおいて、コンテンツ提供者に必要なメモリ量は配信回数に比例し、視聴者に必要なメモリ量、コンテンツ提供者と視聴者の計算量および通信量は配信回数やシーンの数に依存せず一定である。

第4章では、第2章および第3章で提案した配信システムを、携帯電話での配信サービス向けに拡張する。携帯電話事業者はコンテンツ提供者と視聴者との通信を仲介し、視聴者に対するコンテンツ利用料金の課金やコンテンツ提供者に対する分配金の支払いを行う。よって、新たに視聴者の選択履歴を携帯電話事業者に対しても秘匿し、請求する利用料金や分配金の金額が正しいことも保証する。

第5章では、安全性要件を満たすための重要な仮定である、配信されるドラマが同一であることを保証する放送型配信システムを提案する。

最後に第6章において、本論文の成果を要約すると共に今後の研究の展開について述べる。

### 論文審査の結果の要旨

ディジタルコンテンツ配信においては、コンテンツの構造や環境に応じて配信すべきである。また、セキュリティに関する様々な要求を、利便性を損なうことなく、いかに実現するかが重要となる。本論文では、グラフ構造をもつコンテンツとしてインタラクティブドラマを主たる対象とし、その配信システムを提案している。インタラクティブドラマでは視聴者が対話的にストーリーを選択できる。このため、視聴者は選択履歴を秘匿したいというセキュリティ要求がある。一方、配信者はドラマのいずれかのストーリーに沿った正しい配信や視聴動向調査のため、選択履歴の一部を知る必要があり、知った情報を秘匿したいという要求がある。本論文は、グラフ構造をもつコンテンツの配信に関して、次のような成果をまとめたものである。

まず、インタラクティブドラマとして、視聴者が各時点で次のシーンを作成者が準備した選択肢の中から自由に選択できる構造、及び過去の選択履歴の一部に依存して選択しなければならない構造を対象として、それぞれ配信システムを考案している。これらの配信システムでは、一回の配信における通信量が配信回数やシーンの数に依存しないなど、通信量や計算量をさほど犠牲にしていない。このようなシステムでは、その安全性を保証することも重要であるが、使用する暗号技術の安全性など妥当な仮定の下で、各提案システムがセキュリティに関する要求を満たすことを証明している。

また、最近、携帯電話における配信のように、(携帯電話)事業者がコンテンツ提供者と視聴者との通信を仲介し、視聴者に対するコンテンツ利用料金の課金やコンテンツ提供者に対する分配金の支払いを行う形態が行われている。このような環境で技術的に安全性が確保された配信システムは今後ますます重要になる。そこで、暗号や制限付きブラインド署名などの暗号技術を用いることにより、仲介者に対して必要な情報以外を秘匿できる配信システムを提案している。

さらに、配信される内容が視聴者毎に同一であることを保証することも、サービス内容が均等であることを示す上で重要である。一方、料金を払わない視聴者など配信を停止すべき視聴者もいる。これらを実現できる放送型配信システムも提案している。

以上のように、セキュリティの要求を満たすディジタルコンテンツ配信に関して重要な研究成果をあげており、本論文は情報科学に寄与するところが大きい。よって、博士(情報科学)の学位論文として価値あるものと認める。