【31】

氏名	中山弘二郎（なかやまこうじろう）
博士の専攻分野の名称	博士（情報科学）
学位記番号	第　２３０７４　号
学位授与年月日	平成21年３月24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	セキュリティを確保したマルチホップWebサービスにおけるスキーマ処理に関する研究
論文審査委員	（主査） 教授　薦田　憲久 （副査） 教授　藤原　融　　教授　西尾章治郎　　教授　岸野　文郎 准教授　原　隆浩

論文内容の要旨

近年，ビジネス環境の変化が激しく，企業における情報システムや企業をまたがる情報システムでは，この変化に迅速に対応するためWebサービスを用いたシステム連携を行うことが増えている。WebサービスはXML（Extensible Markup Language）ベースの標準技術を利用したシステム連携技術である。Webサービスでは中継者を経由してメッセージを転送することができる。このような中継者を経由したマルチホップWebサービスにおいて，最初のメッセージの送信者から最終的な受信者に渡るEnd-to-Endのセキュリティを確保するには，送受信するXMLデータに対して署名，暗号などのセキュリティ処理を行うメッセージレベルのセキュリティの確保が必要になる。メッセージレベルのセキュリティを実現するための標準技術として，XML署名，XML暗号，WS-Securityなどがある。一方，XMLを利用したシステムの構築ではスキーマが重要な役割を果たす。スキーマは，受信XMLデータの妥当性を検証するスキーマ検証や，XMLデータに容易にアクセスするための手段を提供するデータバインディングなどで利用される。しかし，メッセージレベルセキュリティ技術とスキーマ処理に関する技術とを組み合わせて使用する方法はまだ十分に検討されていない。

本研究では，セキュリティを確保したマルチホップWebサービスにおいて，中継者のシステムで必要となるスキーマ処理に関する課題について検討を行い，その解決方法を示す。まず，メッセージレベルセキュリティ技術とスキーマを始めとするXML関連技術を組み合わせて使用する方法について検証を行う。そして，XML暗号により部分暗号化されたXMLデータに対して，スキーマ検証やデータバインディングなどのスキーマ処理を行うための指針を提案する。さらに，中継者におけるスキーマ検証を実現するために必要となるポスト暗号化スキーマを自動生成する方法を提案する。

本論文では，全体を5章に分けて構成する。

第1章では，マルチホップWebサービスとそのセキュリティの重要性を述べ，関連する技術の概要を述べる。さらに，本研究で取り上げる課題について述べ，関連研究を概観すると共に，本論文の目的と位置付けを明らかにする。

第2章では，メッセージレベルセキュリティ技術とスキーマを始めとするXML関連技術を組み合わせて使用する方法を検証するために構築したマルチホップWebサービスのデモシステムについて述べる。実ビジネスを想定して実装したデモシステムに対し，XML署名，XML暗号，WS-Securityなどのメッセージレベルセキュリティや，スキーマ検証やデータバインディングなどのスキーマ処理を適用した結果について述べる。さらに，デモシステムの構築で明らかになった，中継者における部分暗号化データに対するスキーマ処理の課題を示す。

第3章では，マルチホップWebサービスの中継者における部分暗号化データの処理方法について検討を行う。部分暗号化データの処理として，予め暗号化を考慮したスキーマの設計，オリジナルスキーマの変換，受信XMLデータの変換，XMLプロセッサにおける部分暗号化対応処理の4つの処理方法を取り上げ，スキーマ検証及びデータバインディングに対する有効性の観点からこれらの処理方法の使い分けの指針を提案する。

第4章では，中継者における部分暗号化データのスキーマ検証を実現するため，スキーマを変換し暗号化後のXMLデータが妥当となるようなスキーマ（ポスト暗号化スキーマ）を自動生成する方法を提案する。さらに，業界標準のスキーマに対して提案方法を適用し，従来の手作業によるポスト暗号化スキーマの生成と作業工数の観点から評価を行なう。

第5章では，本研究で得られた成果を要約した後，今後の課題について述べる。

論文審査の結果の要旨

XML（Extensible Markup Language）を用いたシステム連携技術であるWebサービスが注目を集めている。中継者を経由してメッセージを送信するマルチホップWebサービスでは、セキュリティ確保のためにXML暗号、XML署名などのメッセージレベルのセキュリティ技術が必要になる。また、XMLを用いたシステムの構築ではスキーマが重要な役割を果たす。セキュリティを確保したマルチホップWebサービスを構築するには、これらのメッセージレベルセキュリティ技術やスキーマ処理に関する技術を組み合わせて使用する必要があるが、その組み合わせの方法はまだ十分に検討されていない。本論文では、このような背景を踏まえ、セキュリティを確保したマルチホップWebサービスにおけるスキーマ処理に関する研究成果を纏めたものである。その主要な成果を要約すると次の通りである。

(1) 大規模なマルチホップWebサービスのデモシステム構築を通し、メッセージレベルセキュリティ技術とスキーマ処理に関する技術を組み合わせて使用する方法を検証している。その結果、XML暗号を用いた部分暗号化により、XMLデータのスキーマに対する妥当性が保証されなくなり、スキーマ検証やデータバインディングなどのスキーマ処理に失敗する問題を指摘している。

(2) マルチホップWebサービスの中継者における部分暗号化データの処理方法として、予め暗号化を考慮したスキーマの設計、オリジナルスキーマの変換、受信XMLデータの変換、XMLプロセッサにおける部分暗号化対応処理の4つの方法を提示している。また、これらの処理方法について、スキーマ処理に対する有効性の観点から使い分けの指針を提案している。

(3) マルチホップWebサービスの中継者における部分暗号化データのスキーマ検証を実現するため、スキーマ変換により暗号化後のXMLデータが妥当となるスキーマ（ポスト暗号化スキーマ）を自動生成する方法を提案している。また、提案方法を業界標準のスキーマに適用した評価により、従来の手作業によるポスト暗号化スキーマの作成に比べ作業工数を低減できることを確認している。

以上のように、本論文はWebサービスのセキュリティ確保において必要となるスキーマ処理に関して成果を挙げた先駆的研究として、情報科学に寄与するところが大きい。よって本論文は博士（情報科学）の学位論文として価値あるものと認める。