長野県中信地域のユビキタスネットワークを活用した電子自治体実現のための情報セキュリティに関する研究（042304001）

Research for information security that realizes e-municipality using ubiquitous network in Central NAGANO

研究代表者

野瀬　裕昭　長野県工業技術総合センター

Hiroaki Nose　Nagano Prefecture General Industrial Technology Center

研究分担者

西田　崇[†]　清水　基弘[†]　不破　泰[††]　新村　正明[†††]　堀内　広水[††††]　瀬戸　雅章[††††]

洞澤　誠[††††]　前山　文行[††††]　野村　博文[††††]　井口　隆[††††]

Takashi Nishida[†]　Motohiro Shimizu[†]　Yasushi Fuwa[††]　Masaaki Niimura[†††]　Hiromi Horiuchi[††††]

Masaaki Seto[††††]　Makoto Horasawa[††††]　Fumiyuki Maeyama[††††]　Hirofumi Nomura[††††]

Takashi Iguchi[††††]

[†]長野県工業技術総合センター　[††]信州大学大学院工学系研究科　[†††]信州大学工学部

[††††]ソラン株式会社

[†]Nagano Prefecture General Industrial Technology Center

[††]Graduate School of Engineering Sciences, Shinshu University

[†††]Faculty of Engineering, Shinshu University　[††††]SORUN Corp.

研究期間　平成 16 年度～平成 18 年度

本研究開発の概要

本研究は、e-Japan 戦略に基づく高度情報化社会構築が進みつつあるなかで、ユビキタスネットワークを用いた利便性の高い行政サービスを実現するために必須となる、安全で信頼性の高いユビキタスネットワークシステムの実現を目指すものである。

このため、「たとえ障害が発生してもサービスを継続できる高い耐障害性の実現」と「高いセキュリティの確保」の２つが同時に実現できる、セキュリティ技術をベースとした新たな分散データベース技術の開発と、「操作者の権利に応じて限定されたサービスに対してのみアクセス可能な通信路を、いつでもどこでもその操作者の端末に提供する」ことを可能とする、個人認証によるバーチャルなネットワークを構成する動的経路制御技術と、ユビキタス環境下における個人認証をベースとしたサービス接続技術の開発を行った。

Abstract

In this study, our purpose is to realize a safety and trusted ubiquitous network system for the administrative services. To realize this network, we develop two new technologies. First is a new secured distributed database system. This database system is made with multiple subsystems, and provide a non-stop service even if some subsystem is broken. Second is a new dynamic routing system for a virtual network trusted by personal authentication, and service limitation system with personal authentication.

１．まえがき

松本市・塩尻市を中心とする長野県中信地域では、光ネットワークの整備が進み、広域的な高速ネットワークが実現されている。とりわけ塩尻市では、市内 72 ヶ所を結ぶ光ファイバー網を整備し、うち 41 ヶ所には無線ＬＡＮアクセスポイントを設置するなど、ユビキタスネットワーク環境が全国に先駆けて形成されつつある。今後は、これらのユビキタスネットワークを用いた様々な行政サービスを推進することになるが、そのためにはサービス自体の信頼性を高める必要がある。そこで、本研究では、「セキュリティ技術をベースとした新しい分散データベース技術」と「操作者の権利に応じたサービスにのみアクセスが可能な通信路を確保する技術」について研究開発を行った。

２．研究内容及び成果

2.1　電子自治体の実現

図 1 は研究開発した技術により実現する電子自治体の構成図である。地方自治体の情報システムは、きわめて高い秘匿性を要求する個人情報等を管理している。また、災害時等においても停止することなく行政サービスを提供することが要求される。このため、サイバー攻撃等に対する高いセキュリティと、地震等の災害による滅失から情報を守る高い耐障害性の両方が要求されることとなる。しかし、従来の技術によるデータベースシステムでは、この両

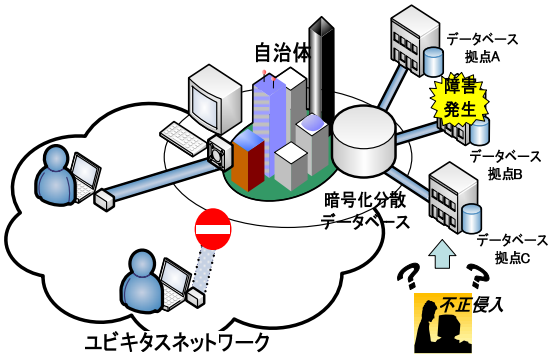

図1　電子自治体構成

方を同時に満足させることは難しく、トレードオフの関係にあった。そこで、本研究では暗号化分散データベースとセキュリティ通信の技術を利用することにより、高いセキュリティを維持したまま、高い耐障害性を実現した。

2.2 暗号化分散データベース

本研究で実現した暗号化分散データベースにおいては、暗号化したデータを冗長断片化して分散するという手法を採用している。このため、以下に挙げるような特徴を有する。

（1）冗長化技術をベースとしたデータの分散管理を行うため、地震等の災害により一部のデータベースノードに障害が発生しても、残りのデータベースノードでシステムの運用を継続することが可能である。

（2）分散データベースの各データベースノードには、暗号化され、さらに断片化されたデータしか存在しない。このため、1 つのデータベースノードをクラッキングしてデータを不正入手しても、まったく意味をなさないデータしか手に入れることができない。

これらの特長により、耐障害性を向上させつつ高いセキュリティを確保することが可能となった。特に、このシステムにおいては、正当な復号鍵とアクセス権の両方を同時に行使しないと元の情報を取り出すことができないため、たとえデータベースの管理者であっても、不正に元の情報にアクセスすることが出来ない。このため、近年問題となっている組織内部の人間による情報漏えいに対しても、有効な防止手段を有していると言える。

また、暗号化分散データベースの本体部分は、ミドルウェアである Hibernate をラッピングした形で実装している。これは、アプリケーションからは、通常の Hibernate と同じ使用方法で、暗号化分散機能が使用可能となる。つまり、暗号化分散環境をアプリケーションからは意識する必要がなくなり、導入が容易となる。また Hibernate を使用して作られたシステムであれば、その環境を維持したまま暗号化分散データベースに移行が可能となる。

2.3 個別暗号通信路

認証された個人のアクセス権に応じて、接続先とアクセス可能なサービスが個別に設定される暗号化通信路システム（Private Certificated Connection 以下、PCC と呼ぶ）を開発した。これにより、従来の VPN のように接続先の他のサービスが見えてしまうことはなく、権利のない他サービスへのクラッキングなどの攻撃を防ぐことが可能となる。また、柔軟にその経路を決定することが出来るため、災害時などネットワークに障害が発生している場合でも、その障害箇所を迂回させることにより接続経路を確保し、ネットワーク接続を維持することも可能である。

さらに、公開鍵暗号を用いた個人認証による操作者の特定を導入することにより、操作者の権利に応じたきめの細かいアクセス制御をかけることが可能となった。これにより、厳密な個人の特定が可能となり、自治体が展開する各種サービスにおける認証業務がより確実なものとなる。

また、PCC は機能ごとにモジュール化することで、機能の取り外しや追加、変更を容易に行うことができる。

2.4 実証実験

暗号化分散データベースと個別暗号通信路の各技術開発により得られた成果を統合し、行政アプリケーションの安全な運用が可能であることを確認するために実証実験を行った。長野県塩尻市の協力の下に、「介護予防システム」を Web アプリケーションとして実装し、平成１８年５月から９月にかけて実施した。

PCC システムに関しては、操作者の権利に応じたアクセス制御が可能であることと、介護予防システムを操作した塩尻市職員へのアンケート調査の結果、違和感なく操作できることが確認された。また、実施期間中に任意のデータベースノードの１台を停止する試験を行い、残りのデータベースノードによりサービスが継続されることと、ユーザはそのことに気づかずにアプリケーションを利用できることを確認した。

以上により、利用者から、高いセキュリティを維持しつつ、利便性を損なわないシステムとの評価を得た。

３．むすび

個人情報などを含む行政に関する情報は、その秘匿性を要する特性から管理を外部へ委託することが困難であった。しかし、本研究により開発されたシステムであれば、ユビキタスネットワーク上においても高いセキュリティを維持することができ、行政に関する情報システムの ASP 事業化によるアウトソーシングを促進することとなる。このことは、行政情報システムの効率的な運用の実現にとどまらず、慢性化している自治体における情報化に係る人材不足も解消することとなり一層の効率化が推進されることとなる。

【誌上発表リスト】

[1]Masaaki Niimura and Yasushi Fuwa, "A High-Speed Processing LSI for RSA Cryptograms Using an Improved Adder Circuit", IEEE Tencon 2004 paperID 0842（平成 16 年 11 月 24 日）

[2] Yasushi Fuwa, Yuka Maruyama, Hiromine Kanazawa, Kenichirou Komatsu, Tomoaki Goshima, and Masaaki Niimura "A Secure Printing System for Ubiquitous Network", IEEE Tencon 2005 paperID 0842（平成 17 年 11 月 24 日）

[3]松原幸祐、野瀬裕昭、西田崇、新村正明、不破泰、“個人認証をベースとした接続制限が可能な暗号化通信システムの開発”、電子情報通信学会技術研究報告 pp223-226（平成 19 年 3 月 9 日）

【申請特許リスト】

[1]ソラン株式会社（瀬戸雅章、野村博文、井口隆）、機密データの管理方法及び管理システム、日本国、平成 17 年 1 月 21 日

[2]不破泰、新村正明、松原幸祐、犬飼哲之、下瀬達也、中村智、個別暗号通信システム、日本、平成 18 年 4 月 7 日

[3]不破泰、新村正明、松原幸祐、犬飼哲之、下瀬達也、中村智、ネットワークセグメント間ローミング、日本、平成 18 年 4 月 7 日

【受賞リスト】

[1]瀬戸　雅章、日立 IT 論文賞　一般論文　優良賞、“セキュア分散データベースの研究開発”、平成 19 年 3 月 14 日

【報道発表リスト】

[1]“情報化新時代　変わる地域社会”、BUSINESS COMPUTER NEWS Vol1064、平成 16 年 11 月 15 日

[2]“電子自治体システム　ユビキタスでの情報保護　基礎研究終え成果期待”、松本市民タイムス、平成 17 年 1 月 19 日

[3]“災害に強いデータベース”、日経産業新聞、平成 17 年 2 月 15 日