氏名	奥田 剛（おくだ つよし）
博士の専攻分野の名称	博士（情報科学）
学位記番号	第 24812 号
学位授与年月日	平成23年3月25日
学位授与の要件	学位規則第4条第2項該当
学位論文名	Studies on Systems to Maintain Trustworthiness and Accuracy of Information Shared over the Internet （インターネット上で流通する情報の信頼性と確度を保つシステムに関する研究）
論文審査委員	（主査） 教授 村田 正幸 （副査） 教授 村上 孝三　教授 今瀬 真　教授 東野 輝夫 教授 中野 博隆

論文内容の要旨

Thanks to the pervasive connectivity to the Internet, information sharing through the Internet is in full bloom, production and consumption of information is active. A large number of the general public is enjoying information production and consumption because the advancement of the Internet technology and competition in the field of information technology reduced the cost of production and consumption. Though it is one of a good side of technical innovation, it leads to the degradation of the trustworthiness and accuracy of the information. On the other hand, as more information is produced and consumed, the trustworthiness and accuracy of information decline. In this dissertation, we divided the cause of this problem into four categories: modification of information, unintended information leak, rich information that contributes to user's context, and abuse of user's information. This dissertation presents four solutions to the problems to maintain trustworthiness and accuracy of information shared over the Internet.

Firstly, we propose a lightweight vulnerability management system (LWVMS) based on a self-enumeration approach. This LWVMS allows administrators to configure their own network security policy flexibly. It complies with existing standards, such as IEEE 802.1X and EAP-TLS, and can operate in existing corporate networks. Since LWVMS does not require IP reachability between the managed server and management servers, it can reduce the risk of invasion and infection in the quarantine phase. In addition, LWVMS can control the connectivity based on both the vulnerabilities of respective components and the network security policy.

Secondly, we propose an enhancement to role based access control, which can use OS identity as an element of subject. This model enables an

can use OS identity as an element of subject. This model enables an administrator to configure the access control policy, which allows specified users using specified OS to access the specific server. The prototype implementation of this model shows that the proposed model is effective to prevent information leak. This prototype implementation uses VM environment to authenticate a user, and filter network traffic based on the combinations of the OS running on VMs and user's identity using that OS.

Thirdly, we propose a method to detect the closest sensor node (CSN) based on the proximity and obtain sensed data directly from it. In identifying the CSN, the proposed method uses radio related index and reception time of packets as an index of distance between two nodes. The experiments using a prototype implementation show effectiveness of the proposed method. This prototype uses only the nodes surrounding the user to obtain sensed data. This method is effective to provide users' environmental information especially in an indoor environment.

Finally, we propose a profile control mechanism called Granularity Control Mechanism based on Identified Probability (GrIP) that controls the number and granularity of disclosing personal information while maintaining quality of personalized service. The GrIP generates a user profile from a combination of different kinds and granularities of personal information. The simulation experiments show that the proposed mechanism can balance the tradeoff between privacy and quality of personalized services.

論文審査の結果の要旨

不特定多数の一般的なユーザが情報の配信，利用を行うようになってきており，インターネット上で流通する情報の信頼性と確度をいかに保つかが問題となっている．本論文では，情報を配信する側と情報を消費する側の双方の側面から情報の信頼性と確度を保つシステムを提案している．

まず本論文では，情報が蓄積・配信されるサーバにおいて，情報の改ざんなどの信頼性を損ねる事象を防ぐ軽量でオープンな脆弱性管理システムを提案している．サーバファームにおいて，個々のサーバの脆弱性管理は重要であるが，本提案では，サイトごとのポリシとサービスの重要性，サービスの持つ脆弱性の深刻度を勘案し，サーバのネットワーク接続を制御する．提案を評価するため，このシステムに対する要件を整理し，オープンで標準的な規格に則って試作した．その結果，考えうる攻撃に対して耐性を持つことを確認し，本システムが効果的に脆弱性管理できることを示した．

情報の信頼性を保つためには，意図した情報のみ配信し意図しない情報を配信しないことが重要である．そこで，意図しない情報漏洩を防ぐために，既存のロールベースアクセス制御方式がOS環境の識別子をアクセス制御のサブジェクトの一つとして利用できるように拡張を行った．本提案では，OSとその上で動くアプリケーションのまとまりをOS環境としてとらえ，それを仮想計算機のインスタンスと結びつけることで，OS環境の識別を行う．さらに，ユーザの識別子とOS環境の識別子に対してロールを付加することにより，より詳細で柔軟なアクセス制御を可能にしている．論文では，試作を用いることで，考えうる攻撃やセキュリティ事案に対して本提案が効果的に情報漏洩を防ぐことを示した．

情報の確度を保つためにはユーザの周囲の情報が必要不可欠であるが，既存のワイヤレスセンサネットワーク（WSN）を用いてユーザの周囲の情報を収集するには位置特定機構が別途必要になる．そこで本論文では，WSNの機能のみを用いて，ユーザ端末自身が能動的に周囲の情報を取得可能にする手法の提案を行った．WSNのメッセージ交換のみを用いることで，他の機構を必要とせず，ユーザ端末が自身の周囲のセンサ情報を収集することが可能となる．論文中では，WSNとして広く使われているZigBeeセンサノードを用いて，WSNの機構だけでユーザの周辺情報を90%以上の精度で収集可能であることを示した．

最後に，サービス提供者にユーザに関する情報を多く開示することにより，情報の確度を高めることが可能であるが，同時にプライバシ侵害の危険性が高まる．そこで，プライバシ侵害の危険性をある一定の閾値以下に抑えながら提供される情報の確度を高く保つユーザプロファイル制御機構を提案した．ここでは，ユーザ個人が特定される確率を定義し，その確率を一定値以下に抑えるアルゴリズムを複数提案している．シミュレーションにより，本提案がより低い特定確率でより高いサービス品質を得られるようにユーザプロファイルを制御できることを示した．

以上のように，本論文ではインターネット上で流通する情報の信頼性と確度を保つための複数の研究成果をあげている．よって，博士（情報科学）の学位論文として価値のあるものと認める．