様式 C-19

科学研究費補助金研究成果報告書

平成２３年　５月２３日現在

機関番号：53901
研究種目：若手研究（Ｂ）
研究期間：2009～2010
課題番号：21700090
研究課題名（和文）　安全な機器間連携を実現するポリシ配布機構を備えたセキュアプロキシの開発
研究課題名（英文）　Development of a Secure Proxy System with a Policy Distribution Mechanism for Machine-to-Machine Networks
研究代表者
平野　学　（HIRANO MANABU）
豊田工業高等専門学校・情報工学科・講師
研究者番号：50390464

研究成果の概要（和文）：
Ubiquitous Computing や Internet of Things の概念を実現するために，従来のインターネットにおける人間対機械（Person-to-Machine）の通信に加えて，機械対機械（Machine-to-Machine, M2M）の通信によるサービスの提供が検討されている．本研究ではこのような機械対機械の通信に基づく連携動作を「トリガ」と「アクション」という単純なルールの組み合わせで表すモデルを提案し，そのような自律連携モデルにおけるセキュリティ機構を検証する．本研究では Machine-to-Machine ネットワークのためのセキュリティ機構の第一歩として，携帯端末のアイコン間にタップ動作で線をつなぐことで簡単に機器同士の連携動作を設定し，機器を制御するプロキシシステムへ設定情報を送信するシステムを開発した．

研究成果の概要（英文）：
Recently, many computer-embedded things that can connect to the Internet have been increased in our daily living environment. These computers provide useful functions to users naturally. However, such small and invisible computers are integrated into many daily things. Therefore, it will be difficult to grasp such small invisible computers surrounding them and to ensure their security mechanisms. In this study, I proposed federation model based on rules using triggers and actions for Machine-to-Machine networks. I developed a prototype implementation of the proposed inter-device federation model using an Android-based GUI application and Wi-Fi-based proxy systems with basic security functions.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	500,000	150,000	650,000
2010 年度	100,000	30,000	130,000
年度			
年度			
年度			
総　計	600,000	180,000	780,000

研究分野：システムセキュリティ
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：セキュアネットワーク，インターネット高度化，ネットワーク，情報システム，計算機システム

１．研究開始当初の背景

1991 年に Mark Weiser はユビキタスコンピューティングの概念を提案し，未来のコンピュータは環境に溶け込み，ユーザはその存在

を意識する必要が無くなることを示唆した．さらに MIT の AutoID センターの RFID の研究から生まれた Internet of Things (IoT) の概念によって,様々な身の回りのものをインターネットへ統合してユーザを支援する研究も進められている．その結果，従来の人間対機械の通信 (Person-to-Machine, P2M) だけではなくユビキタス環境に組み込まれたセンサやミドルレンジの機器等による機械対機械の通信 (Machine-to-Machine, M2M) のセキュリティ機構の研究が行われてきている．

２．研究の目的

本研究課題では広域エリアに分散配置され，ユーザ環境に自然に組み込まれたセンサゲートウェイや家電などの機器を安全に管理するセキュリティ機構を提案する．特に本研究課題では，板ガム大の組込み Linux ボードに独自開発を進めている機器の ID 管理と所有権に基づくアクセス制御を実現する IC チップを組み合わせたセキュアプロキシを開発する．セキュアプロキシは機器にセキュリティポリシを一斉配布して強制させる目的で使用する．本研究課題の推進と実証実験を通して，ユーザ環境に組み込まれ，自律的に連携する機器同士のネットワークを所有権ベースでアクセス制御する新しいセキュリティモデルを検証する．

３．研究の方法

(1) Machine-to-Machine ネットワークのセキュリティ機構を検討するための準備段階として，利用者が身の回りの機器に対して一度ルール設定を行ってしまえば，それ以降は機器同士が連携して自律連携をおこなうプロキシシステムを開発する．プロキシシステムは板ガム大の組込み Linux ボードを用いて開発する．

(2) Machine-to-Machine ネットワークのセキュリティ機構を検討するための準備段階として，(1) のプロキシシステムの連携動作設定をＧＵＩとタッチパネルで簡単におこなう管理アプリケーションを開発する．

(3) (1)(2)を用いて広域エリアに分散配置され，ユーザ環境に自然に組み込まれたセンサや家電機器を管理するためのデモシステムを構築する．

(4) 独自開発している機器の ID 管理と所有権に基づくアクセス制御を実現する IC チップを (1)～(3) の M2M 機器連携システムと組み合わせることでセキュリティ機構を実現する．

４．研究成果

(1) Machine-to-Machine ネットワークの連携モデルを新たに提案した．図 1 に提案した連携モデルを示す．提案方式では機器に存在するサービスをトリガとアクションに分けて表示し，それらを線でつなぐことで機器同士の連携動作を記述する．

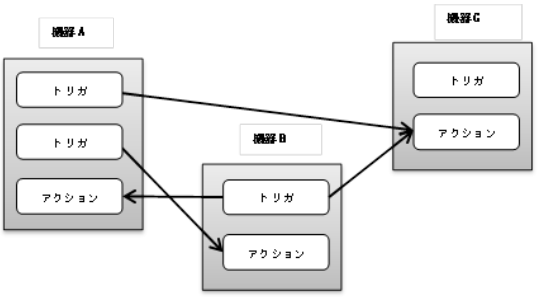

図 1　連携モデルの提案

(2) 機器間連携モデルのデモシステムを新たに構築した．デモシステムの全体構成を図 2 に示す. システムは Machine-to-Machine ネットワークを構築するための小型プロキシシステムと，それらの小型プロキシシステムの連携動作を管理するための Android 端末で動作する管理アプリケーションから構成される．本研究課題では上記２点の開発を実施した．

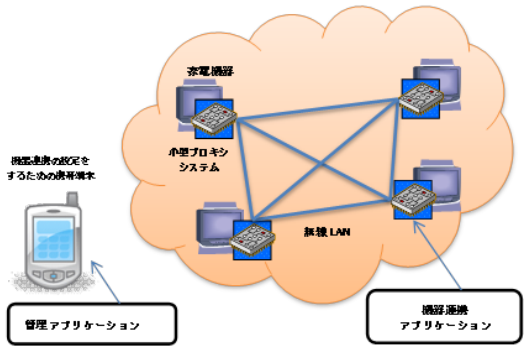

図 2　デモシステムの構成

(3) 小型プロキシシステムで動作する機器連携アプリケーションのユースケース図を図 3 に示す．機器連携アプリケーションは以下の４つの機能を持つ．①他の小型プロキシシステムの探索，②管理アプリケーションとの間の連携設定の処理，③トリガに基づく設定されたアクションの実行処理，④赤外線による家電機器の操作の処理．

小型プロキシシステムのハードウェアには Linux が動作する Gumstix 社の Overo ボードを使用した．開発した小型プロキシシステムの外観を図 4 に示す．小型プロキシシステムは家電機器を操作するために赤外線ユニ

ット（バッファロー社・PC-OP-RS1）を USB 接続している．プロトタイプ実装ではあらかじめ操作対象の家電機器の赤外線データを準備しておき家電機器の操作を実現した．小型プロキシシステムでは機器連携アプリケーションを動作させる．機器の探索，連携動作の設定，および他の機器のアクションの実行には UPnP を利用した．Linux での UPnP アプリケーションの開発にあたり CyberLinkForC を使用した．機器探索には UPnP の SSDP を利用し，連携動作の設定情報の受信と他の機器のアクション実行には SOAP を利用した．

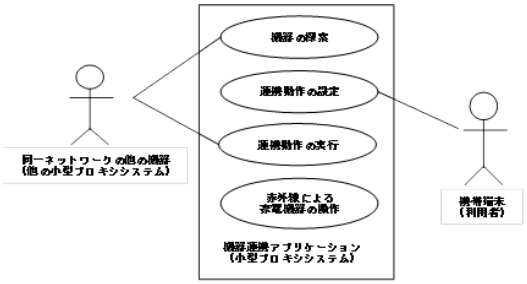

図 3 小型プロキシのユースケース図

図 4 小型プロキシシステムの実装
（上が Overo ボード，下は赤外線ユニット）

(4) 携帯端末で動作する管理アプリケーションのユースケース図を図 5 に示す．管理アプリケーションに必要とされる機能は，①ネットワーク内にある全ての小型プロキシシステムを探索する機能，②探索の結果見つかった小型プロキシシステムをアイコンで画面上へ可視化する機能，③可視化された機器同士の連携動作をグラフィカルユーザインターフェースで設定する機能,の 3 つである．利用者が管理端末をもってネットワークに参加した際に身の回りに存在する機器の一覧を画面に表示するために，小型プロキシシステムの探索（①の機能）を行う．利用者は探索の結果見つかった機器（小型プロキシシステム）を画面上にアイコンとして見ることができ，既に連携動作が設定されている場合はその関係をグラフで表示する．③の機能では画面上に表示された機器のトリガとアクションに線をつなぐ操作をすることで連携動作の設定を行う．設定内容はトリガを発生させる機器に接続された小型プロキシシステムへ送信する．

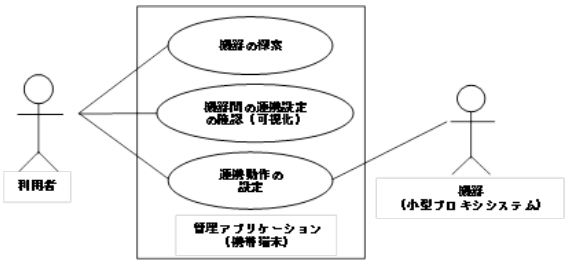

図 5 管理アプリケーションの
ユースケース図

携帯端末のハードウェアには NTT DoCoMo 社製 Xperia を採用した．この携帯端末は OS として Android が動作しており，管理アプリケーションを Android アプリケーションとして実装した．Xperia はタッチパネルを採用しており指で操作することができる．今回のプロトタイプ実装ではこのタッチパネルインターフェースを活用することで専門的な知識を持たない一般の利用者でも使いやすいユーザインターフェースを実現した．図 6 に Xperia 端末で周囲にあるプロキシシステムのアイコン一覧を表示させた画面を示す．なお，UPnP の実装には CyberLinkForJava を使用した．連携設定を機器の小型プロキシシステムへ転送するために SOAP を利用した．

図 6 周囲に存在するプロキシシステムの
アイコン表示

図 7 に各プロキシシステムのサービスの一覧を表示している画面を示す．ユーザはトリガとアクションを選択して，それらのアイコンを画面に追加していくことができる．

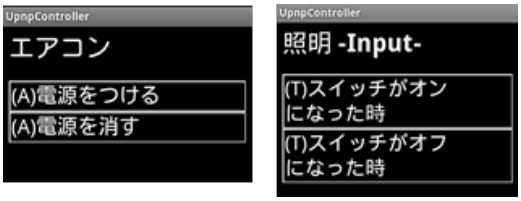

図 7 プロキシのサービス一覧の表示画面

図 8 にサービス（トリガとアクション）の

アイコン間をタッチパネル操作によって線で結び，連携動作を設定している画面を示す．

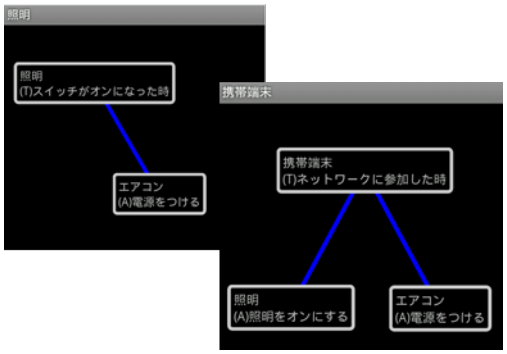

図 8 タッチパネル操作による
トリガとアクションの連携設定

(5) 研究成果(1)～(4)までのシステムを用いて，以下のシナリオのデモシステムを構築した．①「照明」のスイッチをオンにすると，それをトリガとして，「エアコン」の電源をオンにするアクションを実行する．②携帯端末がネットワークに参加するとトリガが発生し，「照明」と「エアコン」の電源をオンにするアクションを実行する．以上のデモシステムを実際の家電機器へ適用し，設計どおりに動作することを確認することができた．

(6) 本研究課題では研究成果 (1)～(5)までを開発したが，当初計画していた IC チップの連携部については開発が完了していない．しかしながら，本研究課題を推進することによってセキュリティ機構の主要部分（セキュリティポリシの配布機構）の開発を行うことができた．更に Android 端末で動作する管理アプリケーションから連携動作の設定情報を送信する機能までを開発することができた．本研究課題の推進によって Machine-to-Machine ネットワークの可視化とタッチパネル操作による連携の設定，そしてセキュリティ機構の基盤技術を開発できた．

本研究課題を通してのまとめと今後の展望を以下に述べる．まず，機械対機械の通信におけるセキュリティ機構の研究は，機械対機械のネットワーク構築が実現できたうえで初めて可能となるテーマである．ゆえに本研究課題の推進によって，機械対機械の自律的な連携動作のシステムを実現できたことの意義は大きく，本研究課題の成果に基づき，本格的にセキュリティ機構の研究に取り組む土台が出来たといえる．今後は，我々の研究グループが開発を進めてきた Machine-to-Machine セキュリティのための IC チップを，本課題で開発したプロキシシステムに組み込み，更に本課題で開発した管理アプリケーションを用いてセキュリティの設定情報を視覚的に確認できるシステムの研究を推進していく計画である．セキュリティの設定は一般の利用者にとって理解が困難なもののひとつである．ユビキタスコンピューティング時代のセキュリティの可視化と誰にでも設定できるユーザインターフェースの実現を目指して，本研究課題の成果をもとに研究を継続していく計画である．

本研究課題の推進にあたりお世話になりました関係者各位に感謝申し上げます．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計２件）

① Manabu Hirano, et al., A Two-step Execution Mechanism for Thin Secure Hypervisors, Proceedings of the 3rd International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2009), 査読有, 2009, pp.129-135 （共著者11名，第一著者）

② Manabu Hirano, et al., T-PIM: Trusted Password Input Method against Data Stealing Malware, Proceedings of 6th International Conference on Information Technology : New Generations (ITNG 2009), 査読有,2009, pp.429-434 （共著者4名，第一著者）

〔学会発表〕（計２件）

① 松川朋樹，平野学，機器間の自律的な連携動作モデルと管理システムの提案，情報処理学会マルチメディア通信と分散処理研究会，2011 年 3 月 10 日，関西大学（大阪府）

② 幾世知範，平野学，他，仮想マシンモニタ BitVisor のためのロールヘースアクセス制御機構の設計と実装，情報処理学会 コンピュータセキュリティ研究会，2010 年 3 月 4 日，東北大学（宮城県）（他に共著者 5 名，第二著者）

〔図書〕（計１件）

① Manabu Hirano, et al., IN-TECH, Engineering the Computer Science and IT (Chapter 24: Portable ID Management Framework for Security Enhancement of Virtual Machine Monitors) , 2009, pp.477-488, ISBN: 978- 953-307-012-4（共著者16名，第一著者）

６．研究組織

(1)研究代表者

平野　学（HIRANO MANABU）
豊田工業高等専門学校・情報工学科・講師
研究者番号：50390464