論 文 内 容 の 要 旨

博士論文題目

Secure Trans-organizational Role-Based Access Control for the Internet of Things（モノのインターネットにおける安全な多組織ロールベースアクセス制御の実現について）

氏 名 Ramon Francisco Mejia

（論文内容の要旨）

近年，通常の計算機のみならず，スマート機器やセンサ等，さまざまな物理的特性と機能をもつ端末がネットワークで相互接続され，日常生活の利便性向上等を目指した技術開発が行われている．これらの技術は Internet of Things (IoT, モノのインターネット) と総称されている．IoT では，個々の端末 (Thing) が他端末やそれを介した組織との間で安全なデータ送受信やサービスの相互提供を行える仕組みが必要である．本論文では，IoT におけるセキュリティ，特に多組織にわたるアクセス制御技術ならびに，端末が暗号鍵等を安全に保存・利用するための高密度２次元バーコード技術について論じられている．

第 2 章では，多組織にわたって利用可能な新しいアクセス制御モデル Trans-organizational role-based access control (ToRBAC) が提案されている．ToRBAC は，従来のロールベースアクセス制御 (RBAC) において，異なる組織のロール間の対応関係の記述を追加することにより，自組織内のユーザロール関係を互いに開示することなく，他組織のロールを自組織のアクセス制御に利用可能とするものである．ToRBAC では従来の RBAC と同様，ロール階層やロールに基づく制約も記述可能である．論文ではさらに，多組織がロールを共有するという環境では ToRBAC は RBAC よりも管理コストが小さいことが示されている．

第 3 章では，階層的 ID ベース暗号 (HIBE) を用いた ToRBAC の実現方式が提案されている．従来の RBAC と異なり ToRBAC では通常のユーザ認証ではなくユーザのもつロールの認証が必要になる．本論文では HIBE の鍵をロールに対応づけ，チャレンジレスポンス型プロトコルによってロールの認証を行う方式が提案されている．合わせて提案プロトコルの安全性，ならびに通常の PKI を実現に用いた場合と比較して本方式の優位性が示されている．

第 4 章では，新しい高密度 2 次元バーコード方式が提案され，その性能が実験的に示されている．このバーコード方式は，第 3 章で提案された ToRBAC の実現に用いられる暗号鍵等を保存・搬送するメディアとして有望なものである．誤り訂正符号として低密度パリティ検査符号（low-density parity check 符号，LDPC 符号）が採用され，大容量化・高密度化に適したバーコード設計（symbology）が提案されている．まず予備実験では，バーコードの印刷・紙媒体での保存・スキャナによる読み取りの過程は，ガウス雑音通信路でモデル化可能であることが示されている．次に，プリンタによる印刷・スキャナによる読み取りで得られた実データに基づく実験結果が示されている．具体的には，多くのパラメータ設定において，LDPC 符号は Reed-Solomon 符号よりも優れた誤り訂正特性を発揮すること，バーコードの印刷において約 11dB 以上の画質が確保できる場合，ビット誤り率を 0.05%以下に抑制できること，インターリーブ手法と併用することによりバースト誤り耐性が高まること等が示されている．

氏　名	Ramon Francisco Mejia

（論文審査結果の要旨）

本論文では，「モノのインターネット（Internet of Things, IoT)」におけるアクセス制御の実現に必要となる基礎技術について論じており，以下の知見を得ている．

（１）複数の組織にまたがってアクセス制御を実現するための理論的なモデルを構築している．IoT においては，ヒトやモノが組織の壁を超えて移動または流通し，様々な情報や資源にアクセスすることが想定される．単一の組織におけるアクセス制御については，行為主体のロール（役割）に基づいてアクセス制御を実現するロールベースアクセス制御（role-based access control, RBAC) が有効であるが，RBAC の仕組みを多組織にまたがって実現するにあたっては，RBAC を構成する種々の要素を拡張する必要がある．本論文では，異なる組織のロール間の対応関係の記述を追加することにより，他組織のロールを自組織のアクセス制御に利用可能とする拡張を提案している．この拡張モデル (Trans-organizational RBAC, ToRBAC) は，従来の RBAC と同様，ロール階層やロールに基づく制約も記述可能であり，従来のモデルを内包する拡張となっている．

（２）上記 ToRBAC を実現するための，ロール情報の安全な管理方法を提案している．ToRBAC の実現にあたっては，ある行為主体がどのようなロール情報を持つのか，誰でもが簡単・確実に確認できることが前提条件となる．オープンで自律的な IoT においては，行為主体となるヒトやモノが，自分の持つロール情報を自分で保持し，必要に応じて提示することが自然であると考えられる．本論文では，階層型 ID ベース暗号（HIBE）を利用することにより，ヒト・モノによるロール詐称を防ぎつつ，誰でもがユーザ・ロール情報を参照できる仕組みを提案している．具体的には，HIBE の鍵をロールに対応づけ，チャレンジレスポンス型プロトコルによってロールの認証を行う方式が提案されており，その安全性について議論されている．さらに，通常の PKI を実現に用いた場合と比較して本方式の優位性が示されている．

（３）モノにロール情報を保持させるための具体的な手段として，新しい高密度 2 次元バーコード方式を提案し，その性能を実験的に評価している．バーコードの密度を向上させるにあたっては，プリンタやスキャナの機械精度から生じる「誤り」の影響を慎重に取り除く必要がある．本提案方式においては，新しいバーコード設計や LDPC 符号の適用等が検討されており，これらの技術の導入が，従来型バーコードで一般的に使われている技術に対して優位であることが実験的に示されている．本バーコードを使って HIBE の鍵を印刷することにより，必ずしも情報処理機能を有しない簡便なモノであっても IoT に参加することが可能となり，IoT の適用範囲を大幅に広げる可能性が生まれる．

以上の通り，本論文で提案する手法は多様でオープンな IoT の実現に大きく貢献するものと期待される．とくに，各組織のアクセス制御に関する柔軟性や自律性を損なうことなく安全性を確保できる意義は大きく，博士（工学）の学位論文として価値あるものと認める．