論文審査の要旨及び担当者

報告番号	甲　乙　第　　号	氏　名	磯崎　宏

論文審査担当者	主　査	環境情報学部教授	兼政策・メディア研究科委員　武藤佳恭
	副　査	環境情報学部教授	兼政策・メディア研究科委員　清木　康
	副　査	環境情報学部教授	兼政策・メディア研究科委員　萩野　達也
	副　査	環境情報学部教授	兼政策・メディア研究科委員　武田　圭史
学力確認担当者：			

（論文審査の要旨）

磯崎宏君の学位請求論文は「Security Platform for Embedded End-point Devices in a Smart Grid」と題し，スマートグリッドで活用する組込み機器向けセキュリティソフトウェアプラットホームを提案している．

本論文で提案する手法では，組込みプロセッサのセキュリティ機能を活用し，オペレーティングシステムなどの汎用処理からセキュリティ処理を切り分け，ハードウェアウェアの高いロバストネスとソフトウェアのフレキシビリティ双方の利点を両立させた組込み機器向けソフトウェアアーキテクチャを実現した．これにより，従来技術では困難だった組込み機器に対する長期安全性の確保と，可用性の確保を実現した．さらに，提案手法をモバイルエージェントシステムに組み込み，エージェントの保護が可能なセキュアモバイルエージェントシステムを実現し，スマートグリッドの新たに実現可能なアプリケーションを示すことで，将来のスマートグリッドのあるべき姿を提案した．

本論文では，提案手法の有効性検証のために，提案手法を試作し，処理性能に与える影響を計測して評価した．その結果，現実的なユースケースにおいて，性能低下は許容範囲で小さいとの評価結果を得た．

スマートグリッドにおけるセキュリティ対策として，従来研究の成果として情報通信システムで培ってきた暗号技術や認証技術，ネットワークセキュリティ技術の活用が考えられる．しかしながら，スマートメータやコンセントレータ等のスマートグリッドで運用され

論 文 審 査 の 要 旨

る組込み機器は製品のライフサイクルが長い，電力計量など社会インフラに関連した処理を行う必要があるため高い可用性が求められる，各家庭に敷設されるため管理者による一括管理が困難であるといった特有の課題がある.

この課題に対し，本論文で提案する組込み機器向けソフトウェアプラットホームは次のように５つの機能を備える.

１．再起動不要なシステムの部分更新を実現するモジュールの動的ロード機能．モジュールを暗号化して配布することで鍵などの秘密情報を含めて配布できる.

２．保護対象モジュールに限定して，いつでもシステムが健全な状態か外部から確認するリモート検証機能.

３．監視方法と監視対象の隠ぺいが可能な攻撃耐性のあるシステム監視機能．オペレーティングシステムが攻撃によりクラッシュしたとしても監視機能を継続することができる.

４．汎用のＤＲＡＭを利用しつつも，オペレーティングシステムの改変を防止する仮想Read-Onlyメモリ機能

５．攻撃の試みを検出し，管理者にネットワークで知らせる通知機能

１，２の機能により，製品ライフサイクルの長い組込み機器を対象にソフトウェアモジュールをネットワーク経由で安全にアップデートするシステムを実現した．また，３，４，５の機能により，機器の停止時間を最小限に抑え，オペレーティングシステムのクラッシュを素早く検出し，管理者へのネットワークを介した通知と再起動が可能な高い可用性を備えたシステムを実現した.

従来手法では，上述のようなセキュリティ機能がオペレーティングシステム等の汎用機能と一体化していたため，汎用機能の実装に脆弱性が混入していると，その脆弱性を皮切りにセキュリティ機能が解析されたり改変されたりリスクがあった．提案手法では，セキュリティ機能を汎用機能から切り分け，独立に実行するプラットホームを実現することで，たとえ汎用機能の制御が攻撃者に奪われたとしてもセキュリティ機能が改変さ

論 文 審 査 の 要 旨

れることはなく，高いセキュリティを実現している．

さらに，提案手法をモバイルエージェントシステムに組込み，不正なホストからエージェントを保護するセキュアモバイルエージェントシステムを実現した．さらに，セキュア環境の時分割機能でオペレーティングシステムの長期停止を防止することができる．スマートグリッドにおけるスマートメータとコンセントレータから構成されるフィールドエリアネットワークに適用することで，インテリジェントな管理・運用が可能な次世代スマートグリッドアーキテクチャを実現した．このアーキテクチャではエージェントの実行処理を汎用処理から秘匿して実行することが可能であるため，プライバシ情報の漏えいや利用量に応じたアプリケーション課金といった，従来技術では困難であったアプリケーションが実現可能である．

従来のセキュリティ技術は，主として暗号アルゴリズムや暗号プロトコルといった暗号要素技術によって支えられてきた．暗号によりシステムの安全性を理論的に保証することができるが，情報通信システムにおける昨今のセキュリティ事故は暗号の脆弱性ではなく実装ミスに起因するものが大半であり，今後普及が見込まれるスマートグリッドも例外ではない．実装安全性を確保するために専用ハードウェアを利用したトラステッドコンピューティングと呼ばれる概念が情報通信システムでは浸透しつつある．本研究で提案する手法もトラステッドコンピューティングの概念を応用しているが，コスト制約の厳しい組込み機器への適用を考慮し，汎用でコモディティの組込みプロセッサで実現している点に特徴がある．

本論文は，８章から成り，第１章では，研究の動機と目的，成果について述べている．また，スマートグリッドの概要についても説明している．

第２章では，課題を定義している．セキュリティの観点から情報システムとスマートグリッドの違いを分析し，スマートグリッドで活用する組込み機器にとって長期安全性と可用性の確保が大きな課題であることを明らかにした．また，従来技術ではそれらの実現が

論 文 審 査 の 要 旨

困難である理由についても詳しく説明している．

第３章では，背景技術として組込みプロセッサの基本構成，プロセッサのセキュリティ機能である TrustZone と，セキュリティハードウェア TPM(Trusted Platform Module)について説明している．

第４章では，提案手法であるソフトウェアモジュールをネットワーク経由で安全にアップデートするシステムと，OS のクラッシュを素早く検出し，再起動が可能なシステムの構成を詳細に説明している．

第５章では，提案手法を要素技術とし，セキュアモバイルエージェントシステムを用いた自律分散型スマートグリッドアーキテクチャを説明している．従来手法では実現が困難であった３つのアプリケーションについても例示し，有用性を示している．

第６章では，関連研究の調査結果を述べている．

第７章では，今後の発展について言及し，第８章で，提案手法の結論をまとめている．

本論文で提案した手法により，スマートグリッドで活用する組込み機器単体で利用可能な基盤技術を確立した．また，セキュアモバイルエージェントシステムを実現し，次世代のスマートグリッドの姿を提案した．スマートメータは今後，国内で数千万台が敷設される計画となっており，それらスマートグリッドで活用する組込み機器のセキュリティを向上させることができるため，社会インフラに対して大きな貢献が期待できる．これらの貢献は，情報セキュリティ分野における実装安全性に関する一領域を切り開いたと言える．これらの成果は，著者が自立した一人の研究者として研究活動を行うために必要な高度な創造力，分析力およびその基礎となる豊かな学識を有することを示したものと言える．よって本論文の著者は博士（政策・メディア）の学位を受ける資格があるものと認める．