別紙様式第２号

学位論文及び審査結果の要旨

横浜国立大学

氏　　名　緒方 日佐男
学 位 の 種 類　博士（情報学）
学 位 記 番 号　環情博甲第 2136 号
学位授与年月日　令和 2 年 3 月 24 日
学位授与の根拠　学位規則（昭和 28 年 4 月 1 日文部省令第 9 号）第 4 条第 1 項及び横浜国立大学学位規則第 5 条第 1 項　（論博の場合は第２項）
学 府 ・専 攻 名　環境情報学府　情報メディア環境学専攻
学位論文題目　A Study on ATM Security Measures by Command Verification
（制御コマンド真正性検証を用いた ATM セキュリティ対策に関する研究）
論文審査委員　主査　横浜国立大学　教 授　松本 勉
横浜国立大学　教 授　森 辰則
横浜国立大学　教 授　四方順司
横浜国立大学　准教授　吉岡克成
横浜国立大学　講 師　白川真一

論文及び審査結果の要旨

海外では 30 か国以上の国・地域で、ATM（現金自動預け払い機）に対する様々な論理攻撃による不正出金が多発し、深刻な社会問題となっている。ATM の運用では ATM 内部への頻繁なアクセスが必要なので、ATM 内制御部である PC 上の実行ファイルの真正性を維持することを求める既存対策は、無効化される懸念がある。本論文は、PC の実行ファイルを厳密に保護する代わりに、PC から送られてきたコマンドの真正性を、PC から制御される周辺デバイス自身が検証する「Command Verification (コマンド真正性検証法)」の提案を核とする ATM セキュリティ対策に関する研究をまとめたものであり、全８章から構成されている。

第 1 章では、ATM に関する背景を述べ、本論文で解決を目指す課題を、社会インフラとしてのサービス安定性を維持しながら、金融機関や ATM 運用現場に大きな負担を掛けない、効果的な ATM セキュリティ対策手法を提供すること、および、ATM のシステム構成や処理の流れには複数の方法が存在するので、それらに適用できる汎用スキームを確立すること、と定めている。第 2 章 ATM System では、ATM システムと ATM 市場動向に関する予備知識を説明している。また、脆弱なポイントが解消されない背景についても説明する。キャッシュレス決済が世界的に広がりつつある中で、ATM 市場動向に関しては、新興国で経済規模の伸びに伴って、ATM の台数も増加していることを示し、ATM 分野のセキュリティ対策の重要性について説明している。第 3 章 Logical Attacks and Existing Measures では、ATM に対する典型的な不正出金攻撃と、それらに対する既存対策について説明している。ATM 内の制御用 PC にマルウェアをインストールする”Jackpotting”、 外部 PC を ATM 内現金処理モジュールに接続して不正出金コマンドを送る”Black boxing”、ATM－勘定系ホスト間通信を乗っ取る中間者攻撃と、既存対策の代表例として欧州刑事警察機構のガイドラインを紹介している。

第 4 章 Command verification by controlled devices では、Command Verification (制御コマンド真正性検証、以下 CV)が必要となる背景と、基本的なモデル、および、各種 ATM 取引への適用例を示している。物理的作用を伴う制御システムでは、コントローラ―アクチ

ュエータモデルでシステムが制御される。既存対策は、コントローラが不正コマンドを送信しないように、コントローラ内の実行ファイルの真正性を維持しようとする。一方、CV では、コントローラから送られてくる制御コマンドの真正性を、耐タンパー性を持つアクチュエータ側周辺デバイスが検証して実行する。耐タンパー周辺デバイスにより、ATM 内部アクセスを伴う ATM 運用の中でも、CV は高セキュリティを維持することが可能である。

第 5 章 Application of Command Verification to one transaction sub-process では、CV の適用が 1 か所である、IC カードを用いた出金取引を用いて、既存対策と CV の定性的効果比較行い、CV の優位性を示している。また、第 6 章 Application of Command Verification to two transaction sub-processes では、ひとつの ATM 取引処理内の複数個所に CV を適切に実装するために必要な実装モデル解析について記述している。本解析を用いて CV が適切に実装された ATM システムでは、運用コストは従来対策の 1 万分の 1 以下になることを示している。第 7 章 Application of Command Verification to all transaction sub-processes では、ATM 取引処理全体に CV を適切に実装するための ATM デバイス設計法について記述している。磁気カード出金取引では、提案設計手法により設計コストを大幅に節約できることを示している。最後の第 8 章は結言であり、上記の ATM に関する成果をまとめるとともに、CV は ATM だけでなく、スマートホーム、自動車、ロボット、産業制御機器等、物理的作用を伴う IoT システムへの適用が期待でき、それらのシステムへの適用が今後の課題であることを記述している。

以上のように、本論文は、ATM セキュリティにおける画期的な対策を提案するものである。なお、本論文を構成する主要な研究成果は、4 篇の査読付論文誌論文、1 篇の査読付国際会議論文、および 2 篇の国内会議論文により公表され、高く評価されている。

よって、本論文は博士（情報学）の学位論文として十分な価値を有すると論文審査委員全員一致で認め、令和 2 年 2 月 5 日（水）13 時から 14 時 20 分までの環境情報 1 号棟 305 号室における博士論文発表会終了後の 14 時 25 分から 14 時 50 分まで、同棟 3 階 304 室において審査委員全員出席のもとで、緒方日佐男氏の最終試験を行った。43 名の参加者を得て充実した質疑応答がなされた博士論文発表会を踏まえ、学力試験として情報セキュリティを中心とする専門分野および情報工学関連分野における口頭試問を行い、これらの分野の研究に関する深い専門知識と理解力、表現力、および質疑応答における適切な対応能力を同氏が有することを確認した。外国語は、英語論文執筆と国際会議において英語にて発表していることをもって、十分な学力を有すると判定した。また博士課程後期修了に必要な単位をすべて取得していることを確認した。これらから、緒方日佐男氏は最終試験に合格であると、審査委員全員一致で判定した。

以上の論文審査委員会の結論に基づき、令和 2 年 2 月 17 日（月）に開催の環境情報学府情報メディア環境学専攻会議にて審議し、全員一致で本論文を博士（情報学）の学位論文としての価値があるものとして環境情報学府教授会に付議することを決定した。その後、環境情報学府学務委員会での確認を経て、令和 2 年 3 月 2 日（月）に開催された環境情報学府教授会において審議を行い、無記名投票により、緒方日佐男氏に博士（情報学）の学位を授与することを決定した。