審査の結果の要旨

論文提出者氏名　　古原　和邦

本論文は「Provably-Secure Remote User Authentication Without Special Devices（特別な装置を持たない利用者の遠隔認証とその証明可能安全性に関する研究）」と題し，利用者の遠隔認証に関して①現実世界で行われる不正への対処②ネット上で行われる不正への対処③安全性の評価④特別な装置を必要としない方式の構成，といった4つの観点から検討している．従来から知られているパスワードと公開鍵暗号を利用する方式やスマートカードを利用する方式が，パスワードの入力操作を覗き見した上でスマートカードを窃取するなどの攻撃に脆弱であるのに対し，本論文ではこれらの攻撃に耐え得る方式を示している．しかも，バイオメトリクスを用いる方式とは異なり，認証に際し特別な装置を必要としない．どこからでも気軽にインターネットにアクセスできる基盤が整備されるに伴い，低コストかつ安全に利用者の遠隔認証を行う方法が求められている．本論文は，これらの要求に対し有効な解決策を示したものであり，「Introduction」を含め6章からなる．

第1章は「Introduction（序論）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している．

第2章は「Challenge-Response Human Identification（質問応答個人認証）」と題し，現実世界で行われる覗き見への対処方法とその改良方法を示している．質問応答個人認証方式とは，パスワードを従来のように直接端末に打ち込む方式とは異なり，サーバから送信された質問を利用者が自身で変換し，その結果を端末に打ち込む方式である．本章では，まず，質問応答個人認証方式の覗き見に対する耐性を評価し，そして，質問の出し方を制御することによる耐性の向上手法を示している．現実的な値を用いた場合，従来の質問応答個人認証方式は1回程度の覗き見にしか耐性がないのに対して，提案手法では数回程度の覗き見に耐性があることを示している．

第3章は「Application of Visual Secret Sharing（視覚復号型秘密分散方式の応用）」と題し，視覚復号型秘密分散方式を用いてパスワードの入力操作の覗き見を防止する手法を示している．視覚復号型秘密分散方式とは秘密情報を複数のスライドに分散し，それらを何枚か重ね合わせることにより秘密情報を視覚的に復号する方式である．本章では，スライドの間に隙間を入れた場合の復号情報の見え方を解析し，それを利用してある特定の場所にいる人物のみに復号情報を伝え得ることを示している．質問応答個人認証方式の質問をこの手法を用いて利用者に提示することで，攻撃者が質問を覗き見ることを防止できる．

第4章は「Provably-Secure Public-Key Cryptosystems（証明可能安全な公開鍵暗号方式）」と題し，原始的な公開鍵暗号から最強の安全性を持つ公開鍵暗号を構成する新しい一般的方法を示している．また，線形符号の復号問題に基

づく原始的な公開鍵暗号方式の安全性を評価し，それに基づく最強の安全性を持つ公開鍵暗号方式の構成方法を示している．ネットワーク上の攻撃は，最強の安全性を持つ公開鍵暗号を用いることで対処可能であるため，このような暗号方式を示すことの意義は大きい．

第5章は「Password-Authenticated Key-Exchange（パスワード認証された鍵交換方式）」と題し，パスワードで認証を行う鍵交換方式の改良方法を示している．ネットワーク上の攻撃は最強の安全性を持つ公開鍵暗号を持いて対処することが可能であるが，パスワードで認証を行う鍵交換方式を用いることも可能である．このパスワード認証・鍵交換方式を用いる場合，利用者は公開鍵を指定する情報を持つ必要が無くなるため，公開鍵暗号を用いる場合と比べ利便性は高まる．本章では，計算量および通信量の少ない方式を提案し，その方式の安全性が十分に高いことを証明している．

最後に第6章は「Conclusion（結言）」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文は，利用者の遠隔認証に関する基礎検討を行うとともに，その安全性向上とその評価に関して具体的な手法を明示したものであり，電子情報工学，特に情報セキュリティ工学上貢献するところが少なくない．

よって本論文は博士（工学）の学位請求論文として合格と認められる．