OUKA
Osaka University Knowledge Archive

Title	A Study on Confidentiality and Authenticity of Document using Public Key Cryptography
Author(s)	鮫島, 吉喜
Citation	大阪大学, 2008, 博士論文
Version Type	VoR
URL	https://hdl.handle.net/11094/399
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

氏名	鮫島吉喜（さめしまよしき）
博士の専攻分野の名称	博　士（情報科学）
学位記番号	第　２２１６３　号
学位授与年月日	平成 20 年 3 月 25 日
学位授与の要件	学位規則第４条第１項該当 情報科学研究科マルチメディア工学専攻
学位論文名	A Study on Confidentiality and Authenticity of Document using Public Key Cryptography （公開鍵暗号を利用した文書の機密性と真正性の確保に関する研究）
論文審査委員	（主査） 教　授　薦田　憲久 （副査） 教　授　藤原　　融　　教　授　下條　真司　　教　授　西尾章治郎 教　授　岸野　文郎　　准教授　秋吉　政徳

論文内容の要旨

本論文は筆者が 1992 年から現在まで日立ソフトウェアエンジニアリング（株）ならびに 2007 年から現在まで大阪大学大学院情報科学研究科マルチメディア工学専攻在学中に行ってきた、公開鍵暗号を利用した文書データの機密性と真正性確保に関する研究成果をまとめたものである。

インターネットの普及によりオフィス文書の機密性や真正性への脅威が顕在化、これに対して以下のような対策がある。第一に媒体紛失や盗聴、文書送信者の詐称の対策として、公開鍵暗号基盤（PKI）を用いた公開鍵暗号による文書の暗号化やデジタル署名による認証、改竄検知がある。PKI 自体は公開鍵管理のための仕組みであり、秘密鍵の保護、文書データの暗号化や署名など、さらに周辺の技術が必要である。第二にサーバ上にある文書への不正アクセスに対しては、サーバでの利用者認証と文書へのアクセス制御による対策がある。第三にウィルスによる文書の漏洩や改竄に対しては、一般にはウィルス対策ソフトウェアが利用されるが、仮想マシンを利用して一台の PC 上に二つの計算機環境を構築、一つを機密文書処理用、他方をウィルスを含む可能性のある一般文書処理用と使い分けるシステムもある。

しかし、これらの技術を現実に利用しようとすると、利用者の使い勝手や運用面から、幾つかの問題が生じる。PKI では認証局が発行する公開鍵証明書などの重要な署名の鍵について、署名鍵を分割、複数の署名者が協力しながら署名生成して署名者の不正防止対策とする例があるが、署名者の同時処理が必要であり、ワークフローが使えないなど業務上不便であった。また、所属異動や鍵紛失などの理由により公開鍵証明書を廃棄すると廃棄以前の署名検証が失敗、文書の真正性検証を行えなくなる。さらにグループ内で文書を作成、閲覧する場合では、章や頁などの文書部分に対する暗号化や署名が必要となる。文書サーバに関しては、サーバに登録済の利用者の認証やアクセス制御は行えるが、広域ネットワークで利用者がドメインごとに登録される環境での認証やアクセス制御は不十分である。仮想マシンを利用したウィルス対策では、二つの計算機環境を使い分けるため、特にネットワークアプリケーションで利用者に不便を強いる。

本論文は、７章から構成され、上記課題に対する解決策の提案と評価を行う。

第１章では、文書を対象に、セキュリティ上の脅威や既存研究の問題を述べ、本研究の背景と方針を述べる。

第２章では、署名アルゴリズムとして DSA をとりあげ、分割鍵保有者の同時署名処理不要なマルチパーティ DSA 署名を提案、スマートカードでの性能評価、安全性の評価、他の署名アルゴリズムへの適用可能性について述べる。

第３章では、PKI の証明書廃棄に関わる課題をとりあげ、解決策として有効期限付き公開鍵証明書情報とタイムスタンプサービスの組合せを提案、サービスの性能・規模性を評価する。

第４章では、二者間やグループ内で交換される文書のセキュリティ要求を洗い出し、交換用オフィス文書体系の標準である ODA のセキュリティを紹介、PKI 標準との不整合点を指摘、解決策を提案する。

第５章では、文書提供サービスのセキュリティ要求を洗い出し、利用者属性と文書付属属性によるアクセス制御方式及び利用者の所属するドメインが異なる場合や利用者のエージェントが文書にアクセスする場合の利用者属性の委譲方式を提案する。

第６章では、ウィルスによる文書の漏洩、破壊に対する仮想マシンを利用した解決策の利便性の問題点を指摘、添付文書暗号化によるメールクライアント統合を提案し、性能評価、安全性の評価を行う。

第７章では、結論として本研究で得られて成果を要約し、今後の課題を述べる。

論 文 審 査 の 結 果 の 要 旨

PC とインターネットを利用して文書を作成、交換、利用する上で、文書の機密性と真正性という安全性の確保は必須であり、同時に利用者に負担をかけないことが求められる。安全性確保のために公開鍵暗号を利用する際には、秘密鍵の保護と通信相手の正しい公開鍵の入手が前提となる。また、公開鍵適用先のシステムにおいては、利用者の利便性やシステムの規模性、標準の適合性などが求められる。本論文は、これらの課題を踏まえ、公開鍵暗号を利用した文書の機密性と真正性の確保に関する研究成果をまとめたものである。その主要な成果を要約すると次の通りである。

⑷ Digital Signature Algorithm（DSA）の秘密鍵保護のために、鍵を複数の鍵保有者に分割する手法があるが、鍵保有者が同時に署名処理する必要があり、利便性に問題があった。順次処理可能とするために、署名対象文書に依存しない乱数部分を事前計算することとし、これを四段階に分割、計算途中の結果をサーバを介して交換するようにして、事前計算の安全性を確保した。スマートカード上に実装して実用に耐え得る性能を確保していることを示し、さらに提案方式が元の DSA と同様に安全であることを証明した。

⑸ 正しい公開鍵入手の仕組みとして Public Key Infrastructure があるが、有効であった署名が、公開鍵証明書が廃棄されてしまうと無効になってしまうという問題があった。公開鍵証明書廃棄後も、廃棄以前には文書の署名が有効であったことを証明するために、署名検証時の公開鍵証明書の有効性と文書の存在を示すトークンを発行するサービスを提案した。本サービスを試作し、数十万規模の電子メール利用者に適用できるという規模性を確認するとともに、サービスの安全性の評価を行った。

⑹ 未知のウィルスに対する文書の安全性確保の手段として、機密文書とウィルスが含まれるかもしれないその他の文書を処理する計算機を分離、二つの計算機を仮想マシン技術と強制アクセス制御をもつセキュア OS を利用して一台の PC に統合するシステムがある。機密文書の安全性は確保しているが、電子メールを利用する際にはメールの相手により、二つの計算機のメールクライアントを使い分ける必要性があり、利便性に問題があった。ウィルスが含まれる可能性のある電子メールの添付ファイルを暗号化して機密文書用計算機のみで受信することで、使い分けを不要とするシステムを提案した。実用上問題のない時間で暗号処理ができることを示すとともに、処理系の安全性評価を行った。

以上のように、本論文は公開鍵暗号を利用した文書の機密性と真正の確保において成果をあげた先駆的研究として、情報科学に寄与するところが大きい。よって、本論文は博士（情報科学）の学位論文として価値あるものと認める。