論 文 の 内 容 の 要 旨

論文題目　Security of Cryptographic Protocols based on the Trusted Party

（和訳　信頼機関に基づく暗号プロトコルの安全性に関する研究）

氏　　名　　渡 邊 裕 治

近年のインターネットの普及に伴い、暗号技術及びそれらを利用した暗号プロトコルに対する様々な研究が行われている。安全な暗号プロトコルを構成する際には、必然的に何らかの形での信頼できる機関(TP)を必要とする。TP を全く利用せずに暗号プロトコルを構成することは非常に困難であり、例え可能であったとしても、そうしたプロトコルは多くの場合非常に非効率である。そのため、TP は前提として多くのプロトコルで利用されており、例として最重要な暗号基盤の一つである公開鍵暗号基盤(PKI)においても TP の存在は本質的である。だが一方で、攻撃者の不正侵入や内部犯罪などによりその前提、即ち TP に対する安全性の仮定が実現困難な場面も数多く存在する。

TP の安全性を評価することは、暗号システム全体を評価することを意味する。これまで、TP の安全性の評価・向上に関して数多くの研究がなされているものの、TP の安全性を評価する際の指標、即ち対象となる攻撃や不正の種類は無数にあり、未だ多くの解決すべき問題が存在する。そこで本研究では、TP の安全性に関して、(1)安全性の向上、(2)安全性の評価、(3)TP の安全性に対する信頼の低減、といった３つの観点から分析を行った。

本研究の結果は以下の３点である。

(1)　PKI における TP として機能する認証局(CA)の署名鍵は、非常に長い期間高度な安全性を維持することが必要な情報の代表例である。この署名鍵が漏洩すれば公開鍵暗号のインフラはその根底から安全性が覆されてしまう。従って、CA の署名鍵は不正により利益を得ようとする攻撃者にとって最も魅力的な攻撃対象の一つであるといえる。本研究においては、この署名鍵が攻撃者に漏洩した際の対応を可能にする方式を提案した。CA のような

非常に負荷の高い対象に対しても適用可能なように署名発行のアルゴリズムを効率化している。

(2)　不正侵入に対してTPを安全にするための手法として近年Proactive Securityが提案されている。このセキュリティは情報を一定期間ごとに更新することにより攻撃者の侵入などに対する耐性を向上しようとするものである。本研究では、このProactive Securityの侵入潜伏に対する安全性の確率モデルを用いた評価を行った。Proactive Securityに対して侵入検知の立場から評価を行った最初の結果である。

(3)　TPの安全性に大きく依存せずに暗号プロトコルを構成することは、TPの実現を容易にするため極めて重要である。本研究では具体的に次に挙げる3つの暗号プロトコルのアプリケーションにおいてTPを排除、もしくは仮定を弱めるための具体的な構成法を示した。

(a)　署名を添付した文書が特定の受信者から漏洩した場合に、それが誰から漏れた情報であるかを検出できるようにすることは署名文書の流れをコントロールするために極めて有効なアプローチと考えられている。ところが、通常の電子署名を用いてこれを行った場合、不正の検証が可能なのは署名者本人のみであり、公開検証可能性がない。本研究では、公開検証を可能とする効率的な署名文書の生成法を示した。従来方式に比べ、メモリ量・通信量ともに数十倍程度の効率化を実現した。

(b)　電子入札は暗号プロトコルの代表的な応用例であり、実際にインターネット上では多くの電子オークションサービスが提供されている。ところが、現在実用化されているサービスの殆どはオークション管理者が信頼できるという前提のもとに構成されている。本研究ではオークション管理者に対する信頼を仮定せずに、また同時に利用者のプライバシーを保護する電子入札プロトコルを提案した。

(c)　PayPerView等の放送型デジタルコンテンツ配信システムの著作権保護方式として有力視されているのが不正者追跡法(Traitor Tracing)と呼ばれている暗号プロトコルである。コンテンツ配布者が利用権限のある利用者に対してコンテンツの復号鍵を配布するとともに、その復号鍵が複製されて他所で発見された場合に誰がその鍵を漏洩したかを特定することを可能にする手法である。近年、この性質を有する極めて効率的なプロトコルが提案されたが、コンテンツ配布者側の不正も考慮した場合に対して示されたプロトコルは信頼できる第3者(TP)の存在を仮定する必要があった。TPの存在を仮定せずにこれを実現する手法は未解決の問題であったが、我々は、TPの存在を前提としない効率的な手法を示し、この問題に対する肯定的な解答を示した。