ヒューマンクリプトに基づく
超ディペンダブル暗号系に関する研究
～人間・社会と調和したディペンダブル情報セキュリティ技術～

今井秀樹　　松浦幹太
（生産技術研究所）

1. はじめに

ネットワーク社会では,電子申請・届出，電子投票，電子商取引，コンテンツ流通など，政治，経済，文化の多くの局面でネットワークを介してサービスが提供されるようになってくる.このようなサービスを支える重要な要素は暗号技術を基盤とする情報セキュリティ技術である.しかし，人が安心してこれらのサービスを利用できるようにするためには，ネットワークの情報セキュリティが確保されているだけでは十分ではない．人とネットワークやコンピュータとの接点が問題なのである．この部分に焦点をあてて総合的な情報セキュリティを達成し，人が真に安心してネットワーク社会の利便性を享受できるようにする技術が急務である．

本プロジェクトでは，このような安心して利用できる情報ネットワーク構築のためのディペンダブル高度情報セキュリティ技術をテーマとして，ヒューマンクリプトの研究に取り組んできた．今年度は，ヒューマンクリプトの視点で暗号理論，量子暗号，モバイル／ユビキタスセキュリティ，匿名認証と匿名通信，暗号技術の評価・認証，ネットワークセキュリティなどを捉え直して研究対象を拡大すると共に，新たに社会的視点も導入してソーシャルクリプトに関する先駆的な研究成果をあげた．本報告書ではそれらの成果の概要を示す．

2. 研究成果

2.1 ヒューマンクリプトとソーシャルクリプト

ヒューマンクリプトとは，端的に言えば人的要素を含めた情報セキュリティ技術のことである．昨年度までに本プロジェクトでは，少ない記憶情報でも安全性を保ち，かつ，サーバやクライアントからの情報漏洩にも強い個人認証方式や認証機能付き鍵共有方式を世界に先駆けて提案した[1],[2]．今年度は，さらにその効率を高め，しかもより現実的なモデルで安全性証明可能な方式を提案した[i]．この成果により，提案方式を暗号コプロセッサ非搭載端末でも利用できる可能性が高まった．

一方，ソーシャルクリプトとは，端的に言えば社会的要素を含めた情報セキュリティ技術や評価手法のことであり，我々は「いかに成果を社会に還元するか」「いかに理論を実証するか」に重点を置いた研究を行っている．前者に関しては，海外居住者向け在外投票システムのリスク分析等に関する研究を行い[xx]，成果はフィリピン国会で公式に紹介された．また，社会的に公正さが論点となる研究として，大規模な Peer-to-Peer オンラインゲームを公正に行うための研究も行い，信頼できる第三者を必要としない新たな方式を提案した[v]．後者に関しては，我が国の地方自治体が電子政府関連システムへ投資したデータを分析し，情報セキュリティ最適投資理論の実証分析に世界で初めて成功した[xx].

2.2 暗号理論

我々は，暗号理論について多角的な視野を持って取り組んできた．特に，ディペンダビリティをもたらすために，証明可能安全性，情報理論的安全性といった安全性解析を主なキーワードとしている．

証明可能安全性に関わる成果のひとつとして，最近提案された新たな機能をもつさまざまな暗号方式を一般的に取り扱うためのフレームワークをまとめ，要望に応じて任意の機能をもった暗号を，証明可能安全性を備えた状態で提供することを可能とした[iii]．さらに，従来の公開鍵暗号の証明可能安全性についても，他の暗号方式と組み合わせた場合の All-or-Nothing　Transform の厳密な安全性評価や，証明可能安全性を持ち冗長性がほぼ理論的限界まで削減された暗号方式の提案を行っている[iv]．情報理論的安全性に基づく暗号系に関わる研究については，これまで提案してきた具体的な構成方法をフォローし，安全性解析の完成度を高めた．

2.3 量子暗号

計算量的安全性のみに頼らず将来にわたって依存できる量子暗号の研究として，「鍵配送」「暗号プリミティブ」の２つの側面で実装可能性したがってディペンダビリティを高める成果を挙げている．

著名な量子鍵配送プロトコル BB84 では，現在実装されている量子通信路で長距離通信を行えば，安全性が崩壊することが知られている．そこで，量子通信実装技術をそのままとし，公開通信路を介して行われる古典的な通信のプロトコルを改良するだけで，従来の BB84 プロトコルと比較し，約 2.5 倍長の安全な通信を可能とする提案を行った[vi]．また，近年その実装の簡便性から注目を集めていた Y00 プロトコルと呼ばれる鍵配送方式が，一般には量子暗号として要求される安全性を保証できないことを厳密に証明した[vii].

プリミティブとしては，量子ビット列コミットメントに関し，実装可能なプロトコルの提案を行った[viii]．これは，従来のプロトコルと比較し，量子ビット列コミットメントの直感的な理解を与えるものであって，実用上の意義が大きい．

2.4 モバイル/ユビキタスセキュリティ

モバイル/ユビキタスセキュリティでは，人が実際に求めるもの，例えばプライバシー保護の観点で優位性のある技術や，少ない資源で安全性および利便性を高める方法を研究している．例えば，ワンタイム代理署名及び信頼できる第三者機関を応用することにより，モバイルエージェント自身がその所有者の署名鍵を危険にさらすことなく，自律的に決裁する機能の実現に成功した[ix]．また，RFID（Radio Frequency Identification）の機能を，１）書換え可能なメモリを持っている場合，２）持っていない場合，３）一度のみ書換え可能なメモリを持っている場合等に分類し，それぞれの条件において達成可能なプライバシーのレベルを明らかにし，その実現方法を提案した[x].

2.5 匿名認証と匿名通信

匿名性確保の基盤技術についても，フレームワーク[xi]だけでなく，匿名認証技術と匿名通信技術で様々な成果を得ている．具体的には，匿名認証技術の新たな基盤技術として我々が基礎を築いてきた"Refreshable Tokens Scheme"という方式に関して，譲渡可能性と権利の無効化について検討を行い，実運用の利便性を高めた[xii]．また匿名通信技術では，無線 LAN 環境の匿名通信路構築に着目し，既存手法の匿名性を劣化させることなく柔軟性を大幅に向上した手法を提案してき

た[xiii][xiv]．また，更に能動的な攻撃モデルに対処した改良手法の提案を行った[xv].

2.6 暗号技術の評価・認証

社会が安心して暗号技術を受容するためには，暗号技術の評価・認証が重要である．そのために我々は，暗号プリミティブの安全性評価，暗号プリミティブを組み合わせたプロトコルの安全性評価と暗号プリミティブを実装した場合の安全性評価という各視点から研究を行っている．

例えば，暗号プロトコルの安全性評価の分野では，無線 LAN での鍵交換プロトコルである WEP の脆弱性に関する研究がある．すなわち WEP に関しては脆弱性が指摘されており，より安全性の高い鍵交換プロトコルも提案されている．しかし，現実には既に WEP を実装した製品が普及しており，その製品がすべて代替されるまでいかに安全性を保つかという問題が残っている．そこで，我々は, WEP に関する脆弱な鍵を探索する手法や脆弱な鍵の存在確率を明らかにすることで，鍵の交換周期に対する提案を行った[xvi].

また，暗号プロトコルに関する安全性証明の分野では，形式的な安全性検証に関する研究を実施している．今年度は，CSP/Casper を用いた暗号鍵交換プロトコル EKE を対象に形式的な安全性評価手法の研究を行った[xvii].

2.7 ネットワークセキュリティ

今年度は，脅威を早期に検知して安心感を向上させる攻撃検知システムとその応用に関する研究を主に推進した．攻撃検知として現在最も問題にされているのが，インターネット上で各種サービスを提供するサーバへ多数の通信が送信されることでサービス機能を低下・停止させられるサービス妨害攻撃への対応である．本研究室では，各通信パケットの情報理論的複雑度（コルモゴロフコンプレキシティ）の変動を監視することで，任意のサービス妨害攻撃を検知可能な検知システムを新たに開発した[xviii].

また，検知システムの応用研究として，インターネットに広く配置されたネットワーク定点観測システムによって収集されたデータを用い，ネットワークの早期異常検知を試みた．その結果，新たにインターネット空間補完手法を提案し，これを応用することで，広域監視システムを持たない系でもその収集データのみを利用して自サーバに対する早期異常検知が可能であることが示された[xix].

3. むすび

以上のように，安全なネットワーク社会構築のためのディペンダブルセキュリティ技術およびプロトコル研究で，前年度までよりも範囲を拡大して成果を上げた．今後は更に，一般ユーザにとってより理解しやすく，安心して使用できる形でこれらの技術を提供できる方法まで含めて研究を発展させたい．また，安心感をもたらすための評価に関する研究をより充実させたい.

参考文献

[1] K. Kobara and H. Imai. “Pretty-simple password-authenticated key-exchange protocol proven to be secure in the standard model”. IEICE Trans., E85-A(10):2229--2237, October 2002.

[2] 山中晋爾, 花岡悟一郎, 赤尾雅人, 花岡裕都子, 今井秀樹, “バイオメトリックスを用いた鍵更新方式ーバイオメトリックスの効果的利用法ー,” 暗号と情報セキュリティシンポジウム (SCIS2003), pages 375--380, 2003.

2004 年度の主要な発表文献

[i] SeongHan Shin, Kazukuni Kobara, Hideki Imai,"The Lower-bound of Complexity in RSA-based Password-Authenticated Key Exchange," Proceedings of the Computer Security Symposium 2004 (CSS2004), pages295-300, October 2004.

[ii] 吉本晴洋, 繁富利恵, 今井秀樹, ``ネットワークゲームのチート防止策の実装,'' 暗号と情報セキュリティシンポジウム(SCIS2005), pages 1879-1884, 2005.
[iii] 花岡悟一郎,張鋭,Nuttapong Attrapadung, 今井秀樹, ``キメラ暗号,'' 暗号と情報セキュリティシンポジウム(SCIS2005), pages 475-480, 2005.
[iv] Rui Zhang, Goichiro Hanaoka, Hideki Imai, "On the Security of Cryptosystems with All-or-Nothing Transform," LNCS3089, Applied Cryptography and Network Security (ACNS 2004), June 2004.
[v] Jose Luis Lacson and Kanta Matsuura, "The Challenge of Providing a Voter Registration System for Millions of Filipinos Living Overseas," Lecture Notes in Computer Science 3183, Springer-Verlag, Berlin, pp.547-548, August 2004.
[vi] 江口 誠, 萩原 学, 今井秀樹, "量子鍵配送プロトコルの光子数分割攻撃に対する頑強性に関する評価," コンピュータセキュリティシンポジウム(CSS2004)予稿集, pages 541-546, October 2004.
[vii] 江口 誠, 萩原 学,今井秀樹, ``キメラ暗号,'' 暗号と情報セキュリティシンポジウム(SCIS2005), pages 655-660, 2005.
[viii] 今福健太郎, 今井秀樹, "量子論的に実装されたノイズィチャンネルへの簡単な能動的攻撃についての考察," 暗号と情報セキュリティシンポジウム(SCIS2005), pages 505-510, 2005.
[ix] 盛, "量子論的に実装されたノイズィチャンネルへの簡単な能動的攻撃についての考察," 暗号と情報セキュリティシンポジウム(SCIS2005), pages 1231-123 6, 2005.
[x] DingZhe Liu, Kazukuni Kobara, Hideki Imai, "How to provide a solution of RFID privacy protection without recordable memory in relatively low cost", 暗号と情報セキュリティシンポジウム(SCIS2005), pages 1399-1404, 2005.
[xi] 黄 楽平, 松浦幹太, 山根 弘, 瀬崎 薫, ``無線環境における位置情報プライバシー問題の評価基準に関する提案,'' コンピュータセキュリティシンポジウム(CSS2004)予稿集, pages 793-798, October 2004.
[xii] 繁富利恵, 大塚玲, 今井秀樹, " Bilinier Map を利用した Refreshable Tokens Scheme, " 暗号と情報セキュリティシンポジウム(SCIS2005), pages 109-114, 2005.
[xiii] J. Tamura, K. Kobara and H. Imai. "Application of Trust-Metrics for Evaluating Performance System in Ad-hoc Networks with Privacy", IEEE Wireless Communications and Networking Conference(WCNC), 2004.
[xiv] Shinji Yamanaka, Kazukuni Kobara, Hideki Imai, "Valkyrie - Anonymous Routing Scheme on Unstable Network," International Symposium on on Information Theory and its Applications(ISITA2004), pages 480-485, 2004.
[xv] 山中晋爾,古原和邦,今井秀樹,"能動攻撃に耐性のある Valkyrie," 暗号と情報セキュリティシンポジウム(SCIS2005), pages 1309-1314, 2005.
[xvi] 吉田雅徳,古原和邦,今井秀樹,"WEP の鍵回復攻撃をかわすための鍵更新タイミングに関する考察," 暗号と情報セキュリティシンポジウム(SCIS2005), pages 253-258, 2005.
[xvii] SeongHan Shin, Kazukuni Kobara, Hideki Imai, "A Lightweight Leakage-Resilient Authenticated Key Exchange Protocol for Wireless Security," Proceedings of the Seventh International Symposium on WPMC, 2004.
[xviii] 古谷隆行, 松浦幹太, アンダーソン・ナシメント, 今井秀樹, "コルモゴロフ・コンプレキシティによる複数のサービス妨害攻撃の検知," コンピュータセキュリティシンポジウム(CSS2004)予稿集, pages361-366, October 2004.
[xix] 田村研輔,松浦幹太,今井秀樹,"定点観測システム収集データを利用したインターネット空間補間手法の提案と早期以上検知への適用," 暗号と情報セキュリティシンポジウム(SCIS2005), pages 1381-1386, 2005.
[xx] Hideyuki Tanaka, Kanta Matsuura, and Osamu Sudo, "Vulnerability and Information Security Investment: An Empirical Analysis of E-Local Government in Japan," the Journal of Accounting and Public Policy, Vol.24, Issue.1, pp.37-59, January/February 2005.

受賞

[vi] 江口 誠, 萩原 学, 今井秀樹： コンピュータセキュリティシンポジウム(CSS)2004 学生論文賞. "量子鍵配送プロトコルの光子数分割攻撃に対する頑強性に関する評価," 情報処理学会. 2004 年 10 月 21 日.