# 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.このようなサービスの安心感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.そして, 真の安心感を得るためには，人とネットワークやコンピュータとの接点が問題となる．人的要素への取り組みではヒューリスティクスに頼りがちだが，情報セキュリティでは注意が必要である．すなわち，ディペンダビリティを獲得するための安全性等の評価は，理論や実証に基づかねばならない．

評価を重視したディペンダブル情報セキュリティを研究する本プロジェクトでは，ヒューマンクリプトのアプローチをとっている．具体的には，今年度は，セキュリティ技術の根幹の一つである暗号理論において，ID ベース暗号に重点的に取り組んだ．基盤がユーザに理解しやすいため，ヒューマンクリプトによる総合的な研究の意義が大きい分野である．もう一つの根幹であるネットワークセキュリティにおいても，プライバシー保護や管理者支援などヒューマンクリプトの視点を積極的に取り入れて研究を推進した．さらに，セキュリティマネジメントにおいても，公的な実態調査のデータに基づいた実証分析等を行った．関係する人々の間で認知度の高い数値データに基づく実証の方が，定性的な意見の積み重ねでしかない指針と比べて，ディペンダビリティが高いからである．本報告書では，プライバシー保護や暗号の評価・認証に特化した研究も含めて，研究成果の概要を示す.

## 2. 研究成果

### 2.1 ヒューマンクリプトとネットワークセキュリティ

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総合的な情報セキュリティ技術のことである．我々はネットワークセキュリティの重要項目の一つである侵入検知システム（IDS）に対してもヒューマンクリプトの視点から取り組み，プライバシー保護を取り入れた検知システム[i][ii]を提案した．IDS の分析根拠となる通信記録や実行記録等にプライバシー侵害につながりかねない情報が含まれている場合に，相対的に優位性が高くなる技術である．また，ネットワークセキュリティに関わる人的要素は，ユーザだけではない．管理者も考える必要がある．我々は，管理者の負担軽減とそれによるシステム全体としてのパフォーマンス向上及びネットワーク全体のディペンダビリティの改善を狙い，攻撃予測の研究を行った．すなわち，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によって収集された膨大なデータに対してネットワークアドレス間の距離を考慮した補間やデータマイニングによる解析を行うことで，ネットワークの早期異常検知として有効な結果を得た[iii]．時間的にも人手だけではまかなえないレンジを扱えることが特徴である.

## 2.2 セキュリティマネジメントとソーシャルクリプト

現実のネットワーク社会では，情報セキュリティ技術開発の進度に見合って実際のセキュリティ水準が向上しているかというと，残念ながらそうではない．情報セキュリティの確保には，技術だけではなく，情報セキュリティへの投資や対策導入に対する経済的動機づけの問題が重要になっている．

こうした問題を背景として，近年，情報セキュリティ投資に関する理論的研究が世界的に着手されている．そのうちの一つとして，情報ネットワーク・システムの脆弱性に着目した最適投資のための理論的枠組みが示されている．具体的には，脆弱性が高くなるほど，情報セキュリティ投資が必ずしも増えるわけではなく，高い脆弱性に対するセキュリティ投資は法外な額となるために，むしろ，中程度の脆弱性に対して投資を行うことが合理的であることを示している．情報セキュリティ投資に関する理論的枠組みはある程度示されつつあるが，それらを実証データに基づいて検証する研究は世界的にみても数が少なく，その取り組みが求められている．

我々は昨年度，地方公共団体を対象とした実証データに基づいた分析を行うことで，上述の情報セキュリティ投資に関する理論的枠組みを検証した．その結果，中程度の脆弱性のシステムの場合に，低程度又は高程度の脆弱性のシステムの場合よりも情報セキュリティ投資が多く行われていることが確認され，既存の理論的枠組みをサポートすることができた．

上記研究で我々が確立した脆弱性指標を用いて，今年度はさらに，ファイアーウォールなど情報セキュリティ技術への投資がセキュリティ・ポリシーの策定や従業員の教育・啓蒙と同時に実施されて初めて効果を発揮することを，民間企業を対象とした公的調査（経済産業省による情報処理実態調査）のデータを用いて実証した[xvi]．理論的には計量経済学を応用しており，ヒューマンクリプトと関連深いソーシャルクリプトという新たな学際分野を開拓する研究である．今後は，継続的な投資の有効性などを示すべく，実証分析を深める予定である．

## 2.3 暗号理論とその応用

現在一般的である公開鍵基盤に基づく暗号では，ランダムなビット列に過ぎない公開鍵を所有者と正しく結びつけるための鍵管理方式が煩雑である．安全性評価の結果に納得して安心するためには前提条件などにも納得しなければならないが，公開鍵基盤に基づく方式ではそもそも公開鍵の生成と割り当て自体が一般ユーザにとって難解である．それに対し，任意の文字列したがって ID 情報を直接的に公開鍵とすることができる ID ベース暗号は, ユーザが納得しやすいという性格を有している．そこで我々は，ヒューマンクリプトの視点から ID ベース暗号を重視し，その安全性評価（等価関係の厳密な定義と証明等）において世界でもっとも完成度の高い理論体系を構築した[v][vi].

ID ベース暗号では近年, 安全性が証明された様々な方式が発表されているが，それらの安全性は仮定する問題の難しさにタイトに帰着されていない.タイトに帰着されていない場合, 実用段階で鍵長等に不都合が生じてしまう．そこで我々は, 昨年, [1] において, Katz-Wang のテクニックを応用することで, 最強の安全性である IND-ID-CCA 安全がタイトに帰着できる ID ベース暗号を提案した．しかし，この方式は Boneh-Franklin の方式[2]よりも暗号文サイズが 2 倍以上になるという欠点を持っていた．そこで本年度は，安全性の帰

着効率をタイトに保ったまま，暗号文サイズがBoneh-Franklin の方式とほぼ同じとなる ID ベース暗号方式の提案を行った[iv].

### 2.4 プライバシー保護

プライバシー保護の基盤技術については，アプリケーションレイヤーとしての匿名認証技術やトラストメトリックス，また通信路レイヤーとしての匿名通信技術で様々な成果を得ている．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加え，更に方式の効率化をはかった[vii][viii].

また，動的ネットワークにおける双方向通信では，送信時に利用していた経路が返信時には利用できないケースは当然考慮されるべきである．しかしながら，とりわけ，返信先を知ることができない匿名通信のようなケースでは，問題はそう単純ではない．例えば，匿名掲示板によるカウンセリング活動など，返信までのタイムラグがあるアプリケーションほど，その様な問題に陥る可能性は高い．しかし，こうした点について従来の匿名通信方式では十分に考慮されているとは言い難かった．そこで我々は，主な既存方式の特徴や問題点を整理した上で，新たに高いデータ可用性を備えた方式の提案を行った[viv]. また，我々は近年増えつつあるこれらプライバシー保護技術の評価フレームワークに関する検討も行った[x][xi][xii].

トラストメトリックス（信頼度の定量化）とは，直接信頼することができない対象に対して，信頼することのできる第三者の判断をもとに信頼の度合いを定量化する研究であり，例えば公開鍵の本人性を確認したいときなどに用いることができる. アプリケーションとして PGP などが有名であるが，実際的には使いづらいいくつかの問題点が挙げられ，またその他のスキームにおいても，ユーザ同士が割り当てる信頼度が秘匿されないというプライバシー問題があった．そこで我々は，各信頼度を秘匿したまま目的対象の信頼度を定量化する手法を世界に先駆けて提案した[xiii].

### 2.5 暗号技術の評価・認証

人したがって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 で標準となっている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，最新の製品における WEP 実装の安全性検証を行った[xiv][xv]. 併せて，脆弱性の残存しているデバイスが混在した環境における最善の利用法等を検討し，ディペンダビリティの向上を達成した.

## 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マネジメントの研究で，前年度までよりも理論的完成度を高めて成果を上げた．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（すなわち，実感できるセキュリティ）まで含めて研究を

進展させたい．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．例えば，方式秘匿に頼ることは暗号研究者の間では望ましくないとされているが，実際の製品などでは多かれ少なかれ根強く行われている．そのような安全性のディペンダビリティが低いことを実際の生体認証装置の評価で検証するなど，よりユーザに近い視点でも研究を発展させたい．

## 参考文献


[1] T. Gomi, N. Attrapadung, J. Furukawa, R. Zhang, G.Hanaoka H. Imai, “CCA-secure IBE Scheme with Tight Security Reduction based on the Gap BDH Assumption,”Proc. of SITA’05, pp.159-162, 2005.
[2] J. Katz, N. Wang, “Efficiency Improvements for Signature Schemes with Tight Security Reductions,”In ACM-CCS’03, pp.155-164, 2003.


## 2005 年度の主要な発表文献


[i] Abdulrahman Alharby, Hideki Imai,” Privacy Protocols Attacks Detection Based on Bayesian Network”, IEICE Transactions, VolE89-D, 2006.
[ii]Abdulrahman Alharby, Hideki Imai,” Security Protocols Protection Based on Anomaly Behaviour of Selected Features”, Proceedings of Symposium on Cryptography and Information Security(SCIS)2006, Hiroshima, Japan, 2006.
[iii] Kensuke Tamura, Kanta Matsuura, Hideki Imai, “Various viewpoints analysis of the actual and large-scale data by using the data mining technique”, Proceedings of 2005 IEEE International Carnahan Conference on Security Technology, pages 283-286, 2005.
[iv] 五味 剛, ナッタポン アッタラパドゥン, 古川 潤, 張 鋭, 花岡 悟一郎, 今井 秀樹,” タイト安全かつ効率的な暗号文サイズの ID ベース暗号”, SCIS2006 予稿集,広島,2006.
[v] Peng Yang, Takashi Kitagawa, Goichiro Hanaoka, Rui Zhang, Kanta Matsuura and Hideki Imai: ``Applying Fujisaki-Okamoto to Identity-Based Encryption'', Lecture Notes in Computer Science 3857, pp.183-192, Springer-Verlag, 2006.
[vi] Nuttapong Attrapadung, Yang Cui, David Galindo, Goichiro Hanaoka, Ichiro Hasuo, Hideki Imai, Kanta Matsuura, Peng Yang and Rui Zhang: ``Relations Among Notions of Security for Identity Based Encryption Schemes'', Lecture Notes in Computer Science 3887, pp.130-141, Springer-Verlag, 2006.
[vii] 繁富 利恵, 山口 文彦, 大塚 玲, 今井 秀樹,” 匿名貸し出しプロトコルの効率に関する検討”, コンピュータセキュリティシンポジウム (CSS2005)予稿集,pages 25-30,愛媛,2005.
[viii]Rie Shigetomi, Akira Otsuka, Jun Furukawa, Keith Martin, “A Provably Secure Refreshable Partially Anonymous Token and its Applications”, Proceedings of SCIS2006, Hiroshima, Japan, 2006.
[viv] 田村仁, 古原和邦, 今井秀樹,” 動的ネットワークにおける双方向匿名通信路構築手法の提案”, SCIS2006 予稿集,広島,2006.
[x] 鈴木雅貴, 山根弘, 黄楽平, 古原和邦, 松浦幹太, 今井秀樹,” プライバシ保護技術の評価フレームワークに関する検討”, 第 28 回情報理論とその応用シンポジウム(SITA2005)予稿集,pages 821-824,沖縄県,2005.
[xi]鈴木雅貴, 野島良, 古原和邦, 今井秀樹,” サーバ側における ID の全数探索を必要とせず同期ずれに強い RFID システムの実現に関する一考察”, SCIS2006 予稿集,広島,2006.
[xii]野島良, 鈴木雅貴, 古原和邦, 今井秀樹, “チャレンジ・レスポンス型 RFID 認証方式の考察”, SCIS2006 予稿集,広島,2006.
[xiii] J. Tamura, K. Kobara and H. Imai, "Application of Trust-Metrics for Evaluating Performance System in Ad-hoc Networks with Privacy", The International Journal of Wireless and Mobile Computing, vol.1, no.3, 2005.
[xiv] 吉田雅徳, 古原和邦, 今井秀樹,” 最新の製品における WEP 実装の検証”, 第 28 回情報理論とその応用シンポジウム (SITA2005)予稿集,pages 805-808, 沖縄県, 2005.
[xv]吉田雅徳, 古原和邦, 今井秀樹, ” 弱 IV に基づく鍵回復攻撃に対して安全な WEP の実装”, SCIS2006 予稿集,広島,2006.
[xvi] Wei Liu, Hideyuki Tanaka, and Kanta Matsuura: ``Information Security Incidents and Countermeasures: An Empirical Analysis Based on an Enterprise Survey in Japan'', Proceedings of SCIS2006, 2006.