# 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

今井秀樹 松浦幹太
生産技術研究所

**概要**

人とコンピュータシステムをセキュリティの面から総合的に最適化するヒューマンクリプトの手法によって、安心感を飛躍的に高めた暗号系を構築すること。とりわけその際、人の立場から見た安全性の検証可能性を重視して、ディペンダビリティのブレークスルーを達成することが本研究の目的である。

## 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、電子決済、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ヒューマンクリプトである。

すなわち、ヒューマンクリプトとは、狭義には、人とコンピュータやネットワークとの関わりの部分における暗号技術、広義には、このような部分と密接に関連したプロトコルも含めた情報セキュリティ技術全般を言い、人とコンピュータネットワークを情報セキュリティの面から総合的に最適化するアプローチである。したがって、特に人とコンピュータシステムとのインターフェースが重要となってくる。新たな要素技術も必要となってくるが、既存の技術もヒューマンクリプトの観点から見直すことにより、人を含めたシステムの中における位置付けが明確となり、取組むべき課題が浮き上がってくる。

また、ヒューマンクリプトには、人を積極的に利用して、情報セキュリティを確保しようという面も含まれている。人とは、誤り率が高く、記憶力や計算力が低く、環境の影響が大きくて安定性に欠ける面もあるが、適応力はあり、コンピュータシステムの中で考えれば、その寿命は比較的長い。このような要素を有効に利用することによって、高い情報セキュリティを達成することもヒューマンクリプトの課題である。

## 2. 研究成果および考察

### 2.1 Password-Authenticated Key Exchange

安全なネットワークアプリケーションを使うためのまさに入り口となるオンライン認証技術に関して、システム（すなわち計算機）が人を認証する個人認証技術に関する研究は活発に行われてきた。しかしながら、これとは逆に人がシステムを認証する手段については、十分な研究がなされているとはいえない。本研究ではこの分野において、エントロピーの小さな秘密情報（パスワード）からエントロピーの大きな秘密情報（鍵長の長い秘密鍵）を人とシステムとの間で共有するための研究を行った。人が IC カードや PDA のような道具を何も持たない場合、ネットワークにおける個人認証や端末認証はパスワードなどの記憶情報を用いるか、個体あるいは端末固有の情報（バイオメトリックスや物理的なランダムパターンなど）を用いることとなる。最も簡単でかつ基本的なのはパスワードを用いる方法であるが、これには様々な攻撃が可能である。例えば、全数

攻撃や辞書攻撃などの方法で、パスワードが窃取されることも多い。中でも専門家の間でとりわけ脅威とされているオフライン辞書攻撃を実際上不可能とするように工夫された暗号学的なプロトコルとして、Password-Authenticated Key Exchange(PAKE)がある（図 1 参照）。これにより、オフライン辞書攻撃だけでなく、偽サーバによるパスワード採取も防ぐことができる。われわれの先駆的研究[1]では、既存の手法を改良し、より簡便に実装する手法を提案したが、評価方法が未成熟であった。今年度は、より完成度の高い評価を伴った成果[i],[ii]を発表し、次年度への布石とした。

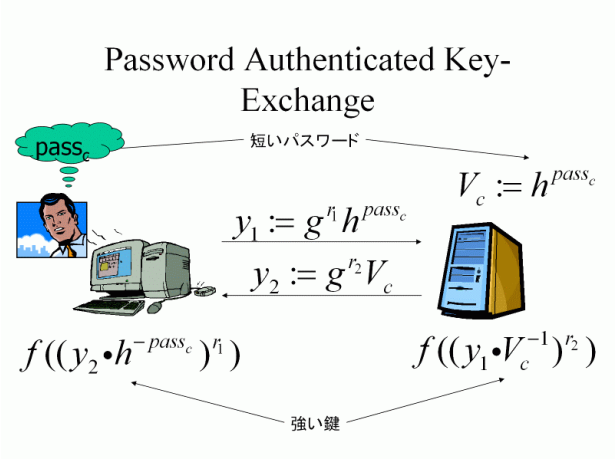


図 1：PAKE の概観

## 2.2 バイオメトリクス情報を利用した鍵生成

バイオメトリクス(Biometrics)技術を、暗号技術を中心とした情報セキュリティ分野に適用することも、ヒューマンクリプトにおける大きな課題の一つである。バイオメトリクスとは、「行動的あるいは身体的な特徴を用い、個人を自動的に同定する技術」のことである。これまでに、バイオメトリクスを利用した研究報告は多数なされているが、その大部分はバイオメトリクスを個人認証に応用したものである。これに対して近年、バイオメトリクス情報から公開鍵暗号系における秘密鍵を生成する方法がいくつか提案されている[2]。これは、バイオメトリクスの利用法としては画期的なものである。しかし、（１）バイオメトリクス情報から得られる秘密鍵のビット長が短い（40bit 程度）、（２）指紋のように変化することの無い固定的なバイオメトリクス情報を利用すると運用が難しい、といった問題点が存在し、結局適当な長さの乱数がさらに必要になっていた。本研究では、この問題を解決するために、動的な手書き文字情報を利用する方法を考案した[iii,iv]。われわれの提案手法[iv]では、動的な手書き文字情報を採取できる機器を用いて、利用者にある決まったパターンの文字・記号などを入力してもらう。そして、入力された文字の筆跡情報に加えて、筆圧情報、さらにはペンの傾き情報をも基にして、長いビット長(190bit 程度)の秘密鍵を生成することに成功した。この結果は、次に示す「新しい秘密鍵更新手法」や、長いビット長を必要とするその他のアプリケーションに、バイオメトリクス情報を基にした秘密情報（秘密鍵）を利用する手法を提供することになる。また、従来の個人認証技術で広く用いられてきたテンプレート情報（認証フェーズにおいて照合＝マッチングに利用する）は、その漏洩がプライバシ問題にも直結している。しかしながら、提案手法[iv]ではテンプレート情報を一切作成しないので、このような問題点も考慮する必要が無いことも利点の一つである。そして、自分のバイオメトリクス情報を利用して秘密鍵を生成しているので、既存の公開鍵基盤（PKI：Public Key Infrastructure）と比較しても、本人と秘密鍵とのつながりがより緊密であると言える。さらにまた、本技術を利用するなどして PKI 用 IC カードの対面取引における本人確認の安全性が保証されれば、PKI の秘密鍵漏洩後も本来の所有者が経済的不利益を被らないようなセキュリティプロトコルと運用方式を構成することができる[v]。このように、本プロジェクトでは、開発した技術の有効な応用方式まで含めて、幅広く研究を実施している。

## 2.3 バイオメトリクス情報を利用した鍵更新方式

次に、バイオメトリクス(Biometrics)技術を、暗号技術を中心とした情報セキュリティ分野に適用する新たな手法[vivii]を提案した。現在の公開鍵暗号系において、復号用秘密鍵の漏洩は、その秘密鍵の所有者（正当なユーザ）にとっては、もっとも重大な脅威の一つである。そのような鍵漏洩問題に対処するために、以前から復号用秘密鍵を更新する、という手法について、いくつかの報告があった[3], [4]。しかし、そのいずれの提案においても、信頼できるストレージ機器の存在を仮定していた。そのようなデバイスが攻撃を受けて秘密情報が漏洩すると安全性が低下してしまうこ

とは明らかである。われわれはこの様な問題点を排除した新しい鍵更新スキーム「バイオメトリクス情報を利用した鍵更新方式」を開発した。われわれの提案方式[vii]においては、いわゆる他の鍵更新方式と同様に、公開鍵の更新は行う必要が無く、秘密鍵のみ更新すればよい。そして、ある期間における復号用秘密鍵は、他の期間には利用することができない。このような仕組みによりある期間の復号用秘密鍵が漏洩しても復号用秘密鍵を更新することによって他の期間の安全性に影響を与えないようなシステムを達成できる。そして、実際の鍵更新時には、利用者は自分のバイオメトリクス情報から生成した秘密鍵と、古い復号用秘密鍵を基にして、新しい復号用秘密鍵を入手できるようになっている。

### 2.4 トラストメトリックに関わる研究

公開鍵を利用したインフラが広がるにつれ、相手や相手の鍵に対する信頼の問題はますます重要になってきている。公開鍵インフラには、信頼の形態の応じて大きく PKI モデルと PGP メールに代表される Web of Trust モデルに二分される。トラストメトリックスとは、特に Web of Trust モデルにおける、ユーザにとって信頼情報が分散された中での相手や、相手の鍵の正当性に対する信頼度の指標ともなる信頼の定量化方法についての研究である。我々は近年、とりわけ人の協力が必要な Web of Trust モデルにおいて、協力者の信頼性が必ずしも高くない場合に頑健な信頼度計算方式を研究している[5]。本プロジェクトでは、その方式に協力者のプライバシー保護の概念を導入し[viii]、協力を得やすくするという社会心理学的にも有効なシステムを考案した。さらに、最新の発表論文[ix]では、協力内容に関する検算機能を加えるという拡張を行った。これにより、個人情報を保護しながらもより確かな計算結果を得られることが可能となった。このように、セキュリティに関わる人の協力という視点まで研究対象を見出したことは、本プロジェクトの特徴的な成果の一つである。

### 2.4 署名の一人歩き問題に関わる研究

電子文書に対して、その文書の内容に確かに同意したことを保証する技術として、デジタル署名は非常に有用なツールとなっている。デジタル署名は署名者の秘密情報を使い、個々の電子文書に関連付けた形で署名が作られるため、他人による偽造は難しく、通常の紙媒体における署名よりも厳密な本人確認が可能である。また、署名の検証は誰でも参照できる公開情報を用いて行うので、誰でも容易に検証することができる。こうして作られた署名つき文書が署名者の意図に反して不当に流通すると、その本人性を強い意味で誰でも確認できる性質により署名の存在を否定できないため、署名者に対し甚大な被害をおよぼす恐れがある。このような署名つき文書の不正流出問題への対策として、署名検証を行えるエンティティを制限する方法が考えられる。このアプローチに基づく方式には否認不可署名や検証者指定署名がある。否認不可署名では署名者、検証者指定署名では指定された検証者と通信することによってはじめて、署名の正当性を確認できる。つまり、限られたエンティティの介在によってのみ署名検証を可能にすることによって、署名つき文書の不正流出を原理的に禁止する方式となっている。しかしこれらの方式では、特定のエンティティと通信をしなければ署名検証を行えないため、署名検証者が多数存在する場合や署名検証を頻繁に行う場合には効率的とはいえない。また、検証者指定署名において Confirmer（確認者）と呼ばれるエンティティは通信なしで署名検証を行うことができるが、Confirmer を複数指定すると署名長が Confirmer の数に従って大きくなってしまう。

一方、われわれらは、それらの問題点を解決または改善した方式[x]を考案した。これを可能としたポイントは、署名つき文書の不正流出を禁止するという先入観を捨て去り、署名つき文書に受信者を追跡できる機能を埋め込み署名つき文書が流出したときにその最初の受信者を特定できるようにしたという点にある。この機能によって不正者追跡署名は署名つき文書の不正流出問題に対する抑止策となっている。不正流出を完全に禁止できないが、誰でも公開情報のみで署名検証を行えることや、署名長が一定であるなどの利点を持つため、署名検証者が多数の場合には効率的な手法が達成された。

このように、電子署名を利用する人の心理的な保護に役立つ暗号技術開発も、我々のプロジェクトの特徴的な成果である。この視点は、ある暗号処理を施す際に必ず所望の必須処理を施す（例えば、あるデータベースの暗号化データを更新すると、暗号化だけでなく必ず証明書付きの署名を付し、かつ、セキュア・タイムスタンプサーバに送信する等）ことを保証するシステムの開発にも反

映させた[xi]。すなわち、一連のセキュリティ処理の連続性の保証が、社会心理学的な面からも高度なディペンダビリティにつながるわけである。

## 3. むすび

以上のように、ヒューマンクリプトの視点で高度なディペンダビリティを達成するための要素技術およびプロトコル研究で、一定の成果を上げた。重要なことは、その成果を得る過程で人の協力を得るための技術的なブレークスルーや社会心理学的に有効なシステム設計を行う着想を得たことである。これらをさらに活用して、引き続きプロジェクト研究を発展させていくことが期待できる。

参考文献


[1] K. Kobara and H. Imai, ``Pretty simple password authenticated key exchange protocol,'' In 24th Symp. Inform. Theory and Its Applications, (SITA '01), pages 561—563, December 2001.

[2] F. Monrose, M.K.Reiter, Q.Li and S.Wetzel, ``Cryptographic key generation from voice,'' In Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.

[3] Boneh and M. Franklin, ``Identity-based encryption from the weil pairing, '' CRYPTO'01, LNCS vol. 2139, Springer-Verlag, 2001.

[4] Y. Dodis, J. Katz, S. Xu and M. Yung. ``Key-insulated public key cryptosystems,'' EUROCRYPT'02, LNCS vol. 2332, Springer-Verlag, 2002.

[5] 田村 仁, 松浦幹太, 今井秀樹: ``審査能力について考慮した多次元トラストメトリックに関する考察'', 2002 年暗号と情報セキュリティシンポジウム(SCIS2002)予稿集, Vol.I, pp.103-108, Jan. 2002.


発表文献


[i] 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.

[ii] K. Kobara and H. Imai. ``PAKE vs. password-based authentications in wireless standards''. In Proc. of The 3rd International Workshop on ITS Telecommunications, pp.135--138, 2002.

[iii] 赤尾雅人, 今井秀樹, ``バイオメトリックスを用いた暗号鍵生成,'' 第 25 回情報理論とその応用シンポジウム, (SITA '02), pages 339—342, December, 2002.

[iv] 赤尾雅人, 山中晋爾, 花岡悟一郎, 今井秀樹, ``ペン入力を用いた暗号鍵生成手法,'' 2003 年 暗号と情報セキュリティシンポジウム(SCIS2003), pages 299—304, January, 2003

[v]小森旭, 花岡悟一郎, 松浦幹太, 須藤修: ``署名鍵漏洩問題における電子証拠生成技術について'', 2003 年暗号と情報セキュリティシンポジウム(SCIS2003)予稿集, Vol.II, pp.983-988, 2003.

[vi] 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,'' 2003 年 暗号と情報セキュリティシンポジウム(SCIS2003), pages 375--380, 2003.

[vii] Akao Masato, Shinji Yamanaka, Goichiro HanaokaYumiko Hanaoka and Hideki Imai, ``Key-Regenesis Encryption Scheme with Biometric Key,'' The Eighth Australasian Conference on Information Security and Privacy, (ACISP '03), (submitted).

[viii] J. Tamura, K. Kobara and H. Imai, ``A Proposal of Trust-Metrics considering Privacy,'' 第 25 回情報理論とその応用シンポジウム, (SITA '02), pages 135—138, December, 2002.

[ix] 田村仁, 古原和邦, 今井秀樹, ``個人情報の保護を考慮したトラストメトリックスの拡張および考察,'' 2003 年 暗号と情報セキュリティシンポジウム(SCIS2003), pages 995—1000, 2003.

[x] 米澤祥子, 花岡悟一郎, 今井秀樹, ``検証者が多数の場合に適した検証者指定署名,'' 2003 年暗号と情報セキュリティシンポジウム(SCIS2003), pages 67—70, 2003.

[xi] 安東 学, 松浦幹太, 馬場 章: ``分散環境で保存されるログファイルにおける各ログエントリー間の順序関係保証方法に関する考察'', コンピュータセキュリティシンポジウム(CSS)2002 論文集, 情報処理学会シンポジウムシリーズ, Vol.2002, No.16, pp.1-6, Oct. 2002.