2018 年度 委託研究

課題 202

超長期セキュア秘密分散保管システム技術の研究開発

研究計画書

国立研究開発法人
情報通信研究機構

１．研究開発課題

『超長期セキュア秘密分散保管システム技術の研究開発』

２．本課題が含まれる研究開発プロジェクトの全体像

はじめに

国立研究開発法人情報通信研究機構（以下「機構」という。）は、機構自ら行う研究や委託研究などを効果的に連携させながら、機構に与えられた中長期目標の達成を目指している。本課題はこのような連携の一部となる研究であるため、研究開発プロジェクト（以下、「プロジェクト」という。）の全体像について十分に理解したうえでの研究提案や実施が求められる。プロジェクトは、プロジェクトオフィサー及び機構職員で構成されるプロジェクトチームによりマネジメントされる。

２．１　プロジェクトの目的・ビジョン

個人の生命に関わる機密性の高い医療情報や国家機密など重要な情報は、世紀単位の超長期間にわたって機密性（情報が第３者に漏洩しないこと）と完全性（データが不正に改竄されないこと）を保証する必要がある。ところが、従来の計算量に基づく暗号技術のみでは、将来の安全性の危殆化を完全に防ぐことができないため超長期の機密性・完全性の確保は不可能である。

これに対して、物理乱数源によって生成される真性乱数と秘密分散法、及び適切な秘匿通信技術を組み合わせることにより、 高度な計算機でも解読が困難で、かつ災害等で一部エリアのサーバが破損しても原本データを正しく復元できる秘密分散保管システムを実現することができる。さらに、サーバ間通信を量子暗号により秘匿化すれば、将来にわたり機密漏えいのない分散保管を実現することができる。

そのために必要となる物理乱数源及び秘密分散ソフトウェアの研究開発を実施し、潜在ユーザとの共同実証を行いながら性能の検証を行い、プロトタイプを開発することにより、当該システムの社会実装を加速する。

２．２　社会的な背景・国内外の状況

重要情報のプライバシー・セキュリティ確保の機運は各国で高まっており、プライバシー保護データマイニングや高度な暗号技術の開発が進められているが、まだ本格的な実用化には至っていない。特に、近年、生命に関わる重要な医療情報やビジネス価値の高い機密情報などが急速に増えており、世紀単位の超長期間にわたって機密性と完全性を確保する必要性が増している。

このような重要情報は災害やサイバー攻撃があった場合でも減失や棄損があってはならず、必要なとき常に利用できる必要がある（可用性の保証）。そのためには、重要な原本データを一箇所のデータセンタに保管しておくだけでは不十分で、複数の遠隔地にあるデータセンタにバックアップ保管する必要がある。その際、データの機密性を確保する手法が秘密分散であり、原本デ

ータからシェアと呼ばれる、それ自体では意味をなさない情報を複数生成し、それぞれを物理的に離れたデータストレージ（シェアホルダ）に保管する手法である。シェアホルダ間は、安全な秘匿回線で接続する必要がある。これにより、一部のシェアホルダに被災やサイバー攻撃による障害がでた場合でも、残ったシェアホルダから原本データを安全に復元することができるようになる。

秘密分散処理の際には大量の乱数が必要となり、現在は、一定の数学アルゴリズムを実行するフィードバックレジスタ回路などによって生成される乱数を用いることが多い。しかし、数学アルゴリズムに基づいて生成された乱数は擬似乱数と呼ばれ、同じ初期値に対して同じ乱数列を作り出す再現性があり、同じビット列を繰り返す周期性もあるため、高い情報セキュリティが要求される用途では推奨されない。情報セキュリティシステムに要求される乱数は、乱数源の設計者ですら出力を予想できず、再現性の無い、いわゆる真性乱数であることが望まれる。物理乱数源は、ランダムな物理現象に基づき、真性乱数に極めて近い乱数を生成することができ、情報セキュリティ分野でのニーズが高まっている。

秘密分散は２０１７年に ISO で標準化が行われ（参考[1]）、近年、国内外のデータセンタや IT 端末での実用化が始まっているが（参考[2], [3], [4], [5], [6], [7]）、現実的な導入コストの問題や現時点で入手可能な技術に限界があるなどのために、超長期間にわたって機密性、完全性、及び可用性を総合的に実現するレベルには至っていない。特に、どのような乱数源を使っているかを明示している例は少なく、セキュリティの起点を明確化するうえで問題が残るのが現状である。セキュリティの起点としては、物理乱数源を用いるのが理想であり、その場合、一度使った乱数は使いまわすことなくワンタイムパッドで運用し、かつ非可逆性を保った乱数管理が必要となる。この点も従来技術では十分対応できていないという問題があった。基礎研究のレベルでは、機構が 2016 年に、超長期間の機密性、完全性、及び可用性を保証できる秘密分散保管技術を敷設環境に構築した量子暗号ネットワーク上で実証している（４．参考[8], [9]）。そこでは、量子暗号によるワンタイムパッド暗号通信と非可逆的鍵管理が実装されている。

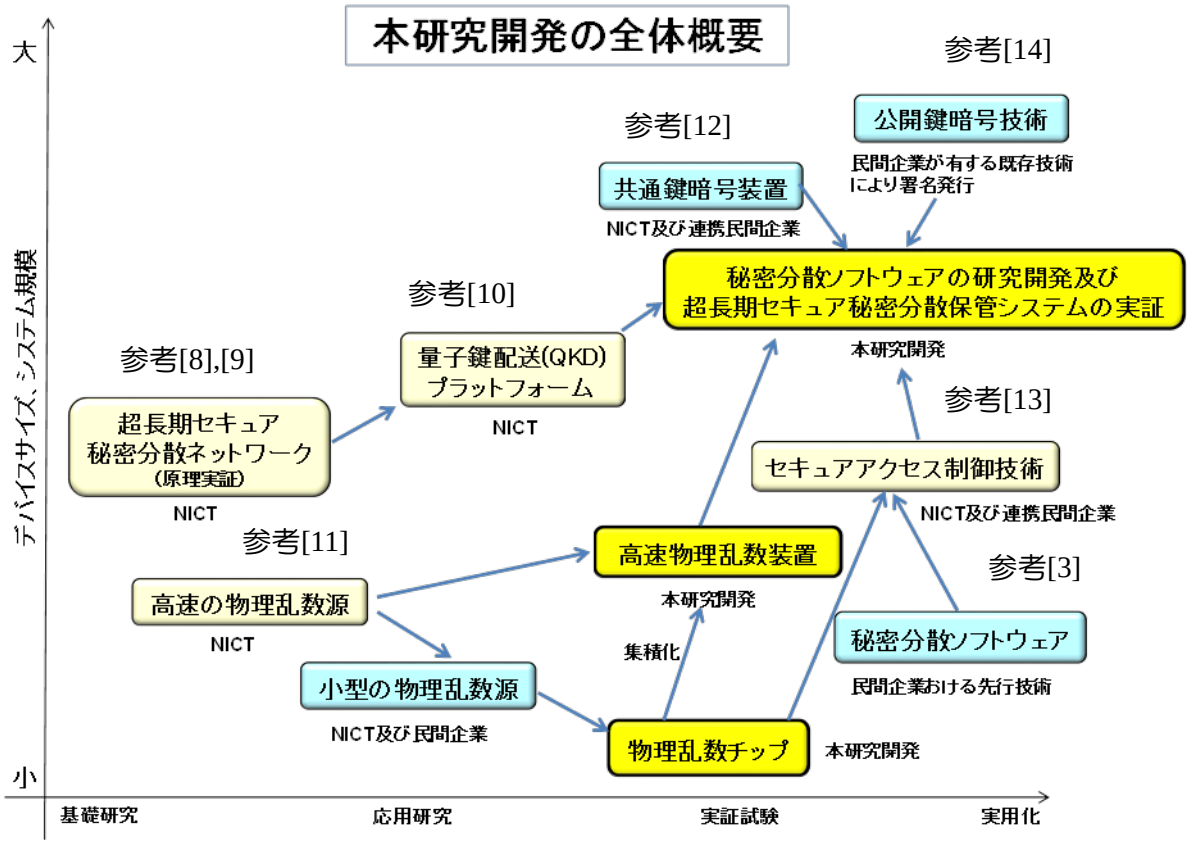
秘密分散やその基盤となる物理乱数源などに関する技術の普及と運用に関しては、まだ我が国には制度的な裏付けが不足しているほか、研究者、技術者側からの政府の制度・政策検討に必要な情報提供も不足している。本研究開発により、物理乱数源の小型化や高速化を実現するとともに、秘密分散アプリケーションの基本ソフトウェア群を開発して、適切な秘匿通信技術を統合し製品化に向けたプロトタイプが開発できれば、前述の問題を解消し、近い将来、重要データの流通、保管、利用における抜本的なセキュリティ強化が可能となる。

２．３　プロジェクトの概要

ランダムな物理現象に基づき、真性乱数に極めて近い乱数（以下、単に真性乱数と呼称）を生成する物理乱数源の小型化や高速化に向けた研究開発を機構の研究チームと連携して進める。小型化に関しては、USB などのインターフェースを介して携帯端末や PC に真性乱数を供給するための携帯性に優れた小型の物理乱数源（いわゆる物理乱数ドングル）を開発し製品プロトタイプを作製する。高速化に関しては、ネットワーク上のサーバ等に大量の真性乱数を供給し、データの秘密分散等を行うための高速物理乱数装置を開発する。

開発されたこれらの物理乱数源から真性乱数を受給し、秘密分散処理を行う基本ソフトウェア群を開発する。秘密分散を行う機器は、ネットワーク上のサーバのほか、PC や携帯端末も想定し、それぞれの用途に適した秘密分散ソフトウェアを開発する。

機構の研究チームやその協力機関と連携することにより、上記の物理乱数源と秘密分散ソフトウェアを、機構が構築した秘匿回線システムとインテグレートして、超長期セキュア秘密分散保管システム技術を開発し、潜在ユーザとの共同実証により評価・検証を行う。秘匿回線とサーバには、機構のネットワークテストベッド上に実装したシステムを活用する。すなわち、第１世代として、量子コンピュータへの耐性を持つセキュリティ確保のために共通鍵暗号システムを、第２世代として、将来にわたり危殆化しないセキュリティ確保のために 100 ㎞圏の量子暗号システム（参考[3]）を活用する。



２．４　プロジェクトオフィサー

未来 ICT 研究所　　佐々木 雅英

３．本委託研究

３．１　概要及び位置付け

本プロジェクトを実施するため、機構が行う研究委託では、物理乱数源及び秘密分散ソフトウェアの研究開発を行う。

その際、受託者は、高速物理乱数装置について、機構の研究チームと連携し研究開発を行う。また、携帯端末、PC、サーバなど、想定される利用機器と用途に適したインターフェース、及び

アプリケーションプログラムインターフェースを開発し、機構やその協力機関と共同で実施するネットワークテストベッド上でのフィールド試験に提供する。また、物理乱数源の評価法や秘密分散ソフトウェアの標準化に向けたドキュメント作成を機構の研究チーム及びコンソーシアム（量子 ICT フォーラム・QKD 技術推進委員会）と連携しながら進め、ガイドライン等を提言する。

３．２　到達目標

2022 年度末までに以下の到達目標を達成する。

課題 A 物理乱数源の研究開発

⑴実装環境依存性の極力少ないランダムな物理現象に基づき、真性乱数を安定的に生成できる小型の物理乱数チップを開発する。ランダムな物理現象の方式と物理乱数チップ単体自体の乱数生成速度に関して特段の指定はしないが、少なくとも次に述べる目標⑵を実現できるものとすること。

⑵様々な携帯端末や PC に安全にかつ容易に真性乱数を供給し、機器認証やアクセス制御、テキストデータなどの秘密分散を実現するための物理乱数ドングル（外形寸法を 12.5 cm×12.5 cm×2.54 cm 以下とする。）を開発し、製品化に向けたプロトタイプを作製する。その際、物理乱数ドングルには 10 Gbits 以上の乱数をバッファするためのメモリを内蔵し、そのインターフェース規格は USB 3.0 以降のものとする。また、データフォーマットはバイナリ、整数、浮動小数点が選択できるものを作製する。

⑶大量の真性乱数を必要とするサーバ、PC 等での秘密分散処理や暗号化のために、1 Gbps 級の速度で真性乱数を生成できる物理乱数装置を開発する。サイズは 19 インチラックの２ユニットに収まるものとすること。当目標の達成には、機構の提供する量子乱数発生回路を用いても良い。その場合、高速のアナログ/デジタル変換処理回路を開発し、当該量子乱数発生回路と組合せ、物理乱数装置として統合実装する。あるいは、目標 a を実現できる物理乱数チップを集積化して高速の物理乱数生成回路を実現し、高速アナログ/デジタル変換処理回路と統合実装して物理乱数装置を実現しても良い。

外部出力インターフェースとして SMA コネクタを用意し、LVDS 信号にて乱数データを出力し、別ポートの SMA コネクタに乱数出力周波数の 1/4 の周波数のクロックも LVDS 信号にて出力すること。

課題 B 秘密分散ソフトウェアの研究開発

⑴課題 A の物理乱数ドングルから真性乱数を受給するためのプログラムインターフェースと、供給された真性乱数を用いて秘密分散処理を行うためのソフトウェアを開発する。秘密分散されたシェアを保存する端末（シェアホルダ）の数（分散数）は３以上とする。また復元に必要なシェアの数（閾値）は任意に設定できるものとする。開発する秘密分散ソフトウェアには、真性乱数を一度使ったら消去し、また再度使用されることがないよう、一方向性を保ったまま管理運用するための機能を備えること。

また、最初の適用例として、課題 A の物理乱数ドングルと秘密分散ソフトウェア（例え

ば、分散数３、閾値２の秘密分散法に基づくシステム）を用いた外部持出し用ノート型 PC のセキュリティ管理・運用手法について検討し、製品化に向けたプロトタイプを作製し、機能評価を実施すること。

⑵機構の研究チームと連携することにより、課題 A の物理乱数ドングル、高速物理乱数装置、秘密分散ソフトウェアを秘匿回線システムとインテグレートして、超長期セキュア秘密分散保管システム技術を開発し、潜在ユーザとの共同実証により評価・検証を行う。

⑶上記⑵の結果に基づき、秘密分散ソフトウェアの標準化に向けたドキュメント作成を機構の研究チーム及びコンソーシアム（量子 ICT フォーラム・QKD 技術推進委員会）と連携しながら進めガイドライン等を提言する。

３．３　マイルストーン

課題 A　物理乱数源の研究開発

⑴物理乱数チップの開発

2020 年度　試作と機能、信頼性評価の完了
2021 年度　多重化等による高速化
2022 年度　製造要領、評価法のドキュメント化
2023 年度～2028 年度：
物理乱数チップの製品化及びセキュリティ市場への浸透

⑵物理乱数ドングルの開発

2020 年度　試作と機能評価の完了
2021 年度　超長期セキュア秘密分散保管システムへの組込みと総合評価
2022 年度　製造要領、評価法のドキュメント化
2023 年度～2030 年度：
物理乱数ドングルの製品化及びセキュリティ市場への浸透

⑶高速物理乱数装置の開発

2020 年度　試作と機能評価の完了
2021 年度　超長期セキュア秘密分散保管システムへの組込みと総合評価
2022 年度　製造要領、評価法のドキュメント化
2023 年度～2032 年度：
高速物理乱数装置の製品化及び分散ストレージ環境での実装の拡大

課題 B　秘密分散ソフトウェアの研究開発

⑴乱数受給のプログラムインターフェースと秘密分散処理ソフトウェアの開発

2020 年度　プロトタイプの開発と機能評価の完了
2021 年度　潜在ユーザとの共同実証と総合評価
2022 年度　物理乱数ドングルと統合化した製品プロトタイプの開発
2023 年度～2032 年度：
エンドポイントで個人情報を保持する必要のある様々なビジネスシーン

における本研究開発技術の適用および実際の運用を促進

⑵超長期セキュア秘密分散保管システムへのインテグレーションと評価・検証

2020 年度　インターフェースの開発と基本評価の完了

2021 年度　インテグレーション、潜在ユーザとの共同実証と総合評価

2022 年度　改修と試験運用

2023 年度～2032 年度：

上記ユーザとの試験運用を経て広域ネットワークにて運用できるよう社会実装を拡大させる。

⑶標準化に向けたドキュメント作成とガイドライン等の提言

2020 年度　評価法や標準化項目に関するドラフト化

2021 年度　検定制度、ビジネスモデルに関する調査とまとめ

2022 年度　標準化に向けたドキュメント作成とガイドライン等の提言

2023 年度～2032 年度：

秘密分散ソフトウェアの標準化を実現し、このソフトウェアを利活用、運用するためのガイドラインを作成

３．４　採択件数、期間及び予算等

採択件数　　：課題Ａ　物理乱数源の研究開発　１件

課題Ｂ　秘密分散ソフトウェアの研究開発　１件

研究開発期間：契約締結日から 2020 年度までの３年間（第１期）

なお、2021 年度から 2022 年度までの２年間（第２期）については、次期中長期目標の状況等も踏まえ、継続について検討する。

研究開発予算：課題Ａ　物理乱数源の研究開発

各年度、総額 15 百万円（税込）を上限とする。

課題Ｂ　秘密分散ソフトウェアの研究開発

各年度、総額 25 百万円（税込）を上限とする。

（提案の予算額の調整を行った上で採択する提案を決定する場合がある。）

研究開発体制：単独の提案も可能であるが、産学官連携等による複数の実施主体からなる体制とすることを推奨する。その際、社会実装を考慮した体制とすること。

３．５　提案に当たっての留意点

- 「課題Ａ　物理乱数源の研究開発」、「課題Ｂ　秘密分散ソフトウェアの研究開発」の受託者は相互に密接に連携しながら課題Ｂ　ａの目標を達成するとともに、機構の研究チーム及びその連携民間企業と連携しながら、２．３で述べた機構のネットワークテストベッド上での共同実証を行うこと。なお、各課題を進めるにあたって必要な情報は、秘密保持契約締結後、機構が各受託者に対して提供するものとする。
- 各受託者は、自身の到達目標のみならず、他の受託者の到達目標を意識したうえで提案を行うこと。

- ３．２の到達目標を踏まえ、第２期までの研究計画を記載した上で、第１期における目標設定を明確に記載すること。採択評価は、それらの記載内容全体を対象に実施する。
- 具体的目標に関しては、定量的に提案書を記載すること。
- 本研究開発成果の情報発信を積極的に行うこと。
- 本研究開発成果の社会実装に向けて、３．３に記載したマイルストーンを意識しつつ、具体的な時期（目標）、方策等を記載すること。
- 本研究開発の遂行過程で得られる科学的なデータがあれば、広くオープンにするのが望ましい。公開できるであろう科学的なデータの有無、および、もし有る場合には公開計画（例：公開するデータの種類、公開先、公開方法）を提案書に記載すること。

３．６　運営管理

- 機構と受託者の連携を図るため、代表提案者は、プロジェクトオフィサーの指示に基づき定期的に連絡調整会議を開催すること。
- 複数の機関が共同で受託する場合には、代表提案者が受託者間の連携等の運営管理を行い、受託者間調整会議を定期的に開催すること。
- 社会情勢や研究環境の変化等、必要に応じて、プロジェクトオフィサーが研究計画書を変更する場合があるので、留意すること。

３．７　評価

- 機構は、2020 年度に評価を実施する。また、本委託研究終了後に追跡評価（成果展開等状況調査を含む）を行う場合がある。
- 機構は、上記以外にも本委託研究の進捗状況等を踏まえて、臨時にヒアリングを実施することがある。

３．８　成果の社会実装に向けた取組

委託研究で得られた成果のオープン化を行う等、成果の社会実装に向けて必要な取組を行うこと。

４．　参考

［1］「秘密分散技術の初の国際標準に NTT の秘密分散技術が採択」（2017 年 10 月 23 日 NTT 持株会社ニュースリリース）
http://www.ntt.co.jp/news2017/1710/171023a.html

［2］五十嵐 大，露崎 浩太，川原 祐人「SHSS：オブジェクトストレージ向けの超高速秘密分散ライブラリ」情報処理学会研究報告，Vol.2015-CSEC-70 No.26（2015 年７月３日）

［3］松尾 正克，武藤 浩二「排他的論理和を用いた（k，n）しきい値秘密分散法」Panasonic Technical Journal, 59(2): 115-120, 2013

[4] Dan Bogdanov, Sven Laur, and Jan Willemson, “Sharemind: A Framework for Fast Privacy-Preserving Computations”, S. Jajodia, and J. Lopez (Eds.): ESORICS 2008, LNCS 5283, pp. 192-206, 2008

[5] 保坂 範和, 多田 美奈子, 加藤 岳久「秘密分散法とその応用」東芝レビュー, 62(7): 23-26, 2007

[6] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, “On a fast (k, n)-threshold secret sharing scheme”, IEICE Transactions, 91-A(9): 2365-2378, 2008

[7] 黒田 知宏, 木村 映善, 松村 泰志, 山下 芳範, 平松 治彦, 粂 直人「秘密分散技術を用いた HIS バックアップクラウド環境の実現性評価」, 医療情報学, 33(4): 225-233（2013 年 9 月 24 日）

[8] M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, W. Ogata, and M. Sasaki, ″Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing,” Scientific Reports 6, pp. 28988(1)--28988(8), July (2016).

[9] J. Braun, J. Buchmann, D. Demirel, M. Geihs, M. Fujiwara, S. Moriai, M. Sasaki, A. Waseda, ″LINCOS: a storage system providing long-term integrity, authenticity, and confidentiality,” in Proc. of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIACCS), pp.461--468, Apr. (2017). ePrint report 2016/742.

[10] The Tokyo QKD Network, Leading-edge field network of quantum cryptography and communications (The Project UQCC)
http://www.uqcc.org/QKDnetwork/

[11] 特願 2017-39437 藤原幹生、武岡正裕、佐々木雅英「物理乱数蒸留装置及び方法」

[12] 「NEC、量子暗号システムの実用化に向けた評価実験をサイバー・セキュリティ・ファクトリーで開始」（2015 年 9 月 28 日 日本電気株式会社）
https://jpn.nec.com/press/201509/20150928_03.html

[13] M. Fujiwara, T. Domeki, S. Moriai and M. Sasaki, “Highly Secure Switches with Quantum Key Distribution Systems,” International Journal of Network Security, Vol.17, No.1, PP.34-39, Jan. 2015

[14] 公開鍵暗号技術（PKI 関連技術情報：情報処理推進機構（IPA））
https://www.ipa.go.jp/security/pki/index.html