グローバルスタンダード最前線

ISO/IEC JTC1 SC27 WG2標準化動向

くさがわ　けいた　きくち　りょう　いちかわ　あつのり　みうら　たかゆき
草川　恵太　/菊池　亮　/市川　敦謙　/三浦　尭之
NTTセキュアプラットフォーム研究所

ISO（International Organization for Standardization）/IEC（International Electrotechnical Commission）JTC（Joint Technical Committee）1 SC（Subcommittee）27では，セキュリティやプライバシに関する方法・技術・ガイドライン等の開発・標準化が行われています．その中でもWG（Working Group）2は暗号およびその他のセキュリティメカニズムの開発・標準化を担っています．ここではWG2での暗号アルゴリズム・プロトコルに関する最新の標準化動向を紹介します．

全体の紹介ISO/IEC JTC1 SC27 WG2:

ISO（International Organization for Standardization）/IEC（International Electrotechnical Commission）JTC（Joint Technical Committee）1 SC（Subcommittee）27はセキュリティやプライバシに関する方法・技術・ガイドライン等を取り扱う標準化団体です．その中でもWG（Working Group）2は暗号およびその他のセキュリティメカニズムを扱うワーキンググループです．基本的な暗号方式（ブロック暗号やハッシュ関数）から匿名認証や秘密計算といった高度なプロトコルまでさまざまな方式を議論しています．

■軽量暗号（ISO/IEC 29192）

暗号方式の性能は，演算にかかる時間や遅延，消費する電力，ハードウェア実装した際の面積，演算に用いるメモリサイズといったさまざまな指標で測ることができます．デバイスがバッテリや電源で動くのであれば消費電力が低い暗号が必要ですし，伝送量が多い環境では演算にかかる時間が小さいことが求められます．また車載機器や工場でのセンサといったリアルタイム性が重要な環境では低遅延な暗号が必要でしょう．このような環境で用いられるような，なんらかの指標で既存の標準化された暗号よりも「軽い」暗号方式を，軽量暗号と呼んでいます．2000年代に研究が始まり，近年の機器に対する安全性要件やIoT（Internet of Things）の流れもあり現在も活発に研究・開発が行われています．

ISO/IECでも軽量暗号を分野ごとにまとめたISO/IEC 29192やRFID向けの暗号技術を定めたISO/IEC 29167が策定されています．米国NIST（National Institute of Standards and Technology）は2014年から軽量暗号の標準化を検討し，2018年に公募を行い，2021年1月現在，候補を絞りつつ選定プロセス（Round2）が進んでいます．日本のCRYPTREC（Cryptography Research and Evaluation Committees）でも検討が行われており，2017年には「CRYPTREC 暗号技術ガイドライン（軽量暗号）」(1)として検討内容がまとめられています．

WG2ではさまざまな軽量暗号に関する標準であるISO/IEC 29192を担当しています．この標準は，軽量ブロック暗号（Part2），軽量ストリーム暗号（Part3），軽量ハッシュ関数（Part 5），軽量メッセージ認証符号（Part6）などに分かれています．その中でもメッセージ認証符号（ISO/IEC 29192-6）に，Chasky-12やNTTがかかわっているLightMACが日本から提案され，2019年に標準化されました．

ほかにも調整可能ブロック暗号（Tweakable BlockCipher，TBC）を扱う規格としてISO/IEC 18033-7が2020年に立ち上げられました．こちらには軽量暗号コンペティションCAESARで選定された軽量暗号の1つDeoxysの基本要素であるDeoxys-BCやNTTがかかわっている軽量暗号SKINNYが掲載される予定です(2)．

■匿名署名（ISO/IEC 20008）

デジタル署名はさまざまな分野で用いられる基本技術です．署名者は署名鍵と検証鍵を生成し，検証鍵を公開します．署名者は署名鍵を用いて文書に署名を行い，検証者は検証鍵・文書・署名をそろえて検証を行います．

この場合，ある文書と署名を見たときに，どの検証鍵の持ち主が署名を行ったかということが分かります．デジタル署名を認証として用いる場合には，どの検証鍵の持ち主がその認証を行ったかが分かることになります．

アプリケーションによっては署名者の匿名性を守りたいという要求があり

ます．そのために匿名署名と呼ばれる技術が研究されてきました．ISO/IEC 20008シリーズでは匿名署名を扱っています（**図1**）．

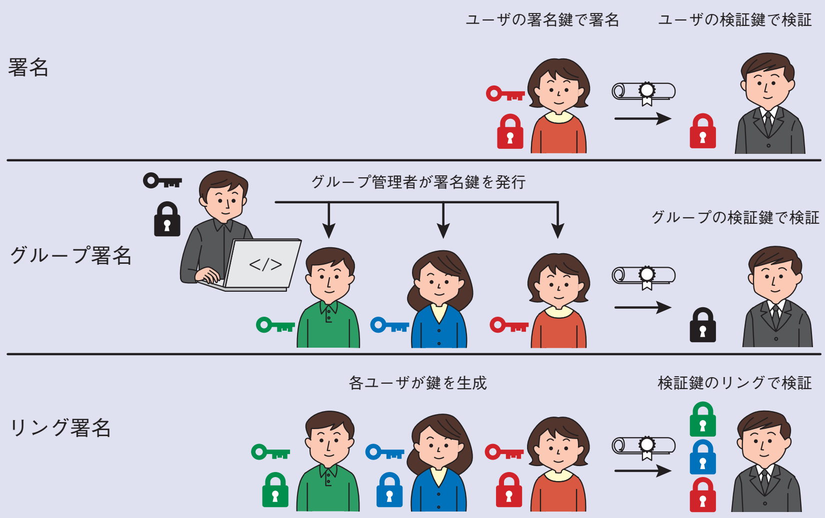


図1　匿名署名

■グループ署名（ISO/IEC 20008-2）

1991年に提唱されたグループ署名では，グループ管理者が各ユーザに署名鍵を発行します．ユーザは署名鍵を用いて文書に署名を行い，検証者はグループの検証鍵と文書と署名をそろえて検証を行います，この場合，検証者には相手がグループに所属しているという情報しか分かりません．そのため，ユーザの匿名性が守られることになります．

2010年ごろからISO/IEC 20008-2としてグループ署名の規格化が始まり，2013年には標準規格として出版に至っています．

■リング署名（ISO/IEC 20008-3）

2001年に提唱されたリング署名では，ユーザは各々通常の署名の署名鍵・検証鍵を持っています．ユーザは署名鍵を用いて文書に署名を行うのですが，そのときに他の検証鍵も一緒に用います．検証者は検証鍵の組（リングと呼ばれる）と文書と署名をそろえて検証を行います．

この場合，検証者には相手がリングの中のどれか1つの検証鍵の持ち主であるということしか分かりません．そのため，ユーザの匿名性が守られることになります．グループ署名と比べるとグループ管理者を必要としないため，非中央集権的であるといえます．

非中央集権的であることや，電子現金の匿名性を達成するための技術としてブロックチェーンに組み込まれる事例などを受けて，2020年にISO/IEC 20008-3としてリング署名の規格化が始まりました．NTTでもリング署名の黎明期から研究開発を行っており，提案やフィードバックを積極的に行っています．

ペアリング用楕円曲線（ISO/IEC 15946-5）

公開鍵暗号は，数学的な問題を基にしてつくられることが基本になっています．例えば，公開鍵暗号を提唱したDiffieとHellmanの論文(3)では離散対数問題に基づく鍵交換方式が載っています．その後，1985年ごろに楕円曲線上の離散対数問題に基づく公開鍵暗号の構成が提唱されました．通常の離散対数問題よりも鍵や暗号文のサイズを小さくできることが分かり，研究開発が進みました．2000年ごろには，楕円曲線上で定義されるペアリング関数をうまく使うことで，これまでにできなかった暗号方式（IDベース暗号，効率の良いしきい値暗号等）が，構成できることが分かりました．

WG2では楕円曲線暗号の標準化を行っており，1999〜2004年にかけてISO/IEC 15946シリーズとしてまとめていました．のちに暗号方式の標準は技術の内容ごとに分類され直しました．そのため，現在では楕円曲線暗号の用語を定義するISO/IEC 15946-1と，楕円曲線やペアリング関数と相性の良い楕円曲線の構成方法をまとめたISO/IEC 15946-5が残っています．

Kim（当時NTT）とBarbulescu

は2016年にペアリング関数と相性の良い楕円曲線上の離散対数問題を解く新たなアルゴリズムを提案しました(4)．このアルゴリズムは既存のアルゴリズムよりも高速に問題を解いてしまうため，これまでの楕円曲線の安全性レベルが低下してしまいます．このアルゴリズムの登場を受けて，新しい楕円曲線の安全性評価・選定が研究者・開発者の間で行われてきました．

WG2でも，ISO/IEC 15946-5に掲載されている楕円曲線の安全性レベルが低下してしまったことから，2018年より，安全性レベルの向上のために規格の改定の検討が始まりました．ペアリング関数と相性の良い楕円曲線の見直し・選定・パラメータ設定が議論され，最終的には2021～2022年ごろの標準化をめざしています．NTTもこの解析アルゴリズムの提案を受けて，新たな楕円曲線の研究を行っており(5)，WG2での議論においても積極的な貢献を行っています．

秘密分散 (ISO/IEC 19592-1, 2)

秘密分散は，秘密としたいデータを適切な符号化の下，複数の断片に分割します．断片からは元のデータの情報が洩れず，また，いくつかの断片が消失しても復元が可能であるという点が特徴です（**図2**）．

断片からは元の秘密情報が漏れないという点から，機微情報の漏洩対策に用いることができます．普段は断片のかたちで複数人が分散して保持しておき，秘密を復元する際には断片を持ち寄って復元を行います．また，後述する秘密計算の基幹技術でもあります．

さらに，いくつかの断片が消失してもデータが復元可能であるという点から，データの分散保存技術や災害時にデータ消失した場合のデータ復元技術としても用いることができます．

1979年にShamirとBlakleyによって独立に提案されて以降，非常に多くの方式が提案されています．安全性や分割の仕方・復元の仕方などさまざまな違いがあり，使い方によって適切な秘密分散を選定する必要があります．また学術的には同じ方式であっても，実装方法によって違いがあることも考えられます．

2014年からISO/IEC 19592シリーズとして秘密分散の標準化が始まりました．NTTはISO/IECでの秘密分散の標準化において活発に活動し，19592-2のエディタとして規格の作成を主導し，2017年の出版に大きく貢献しました．NTTの秘密分散・秘密

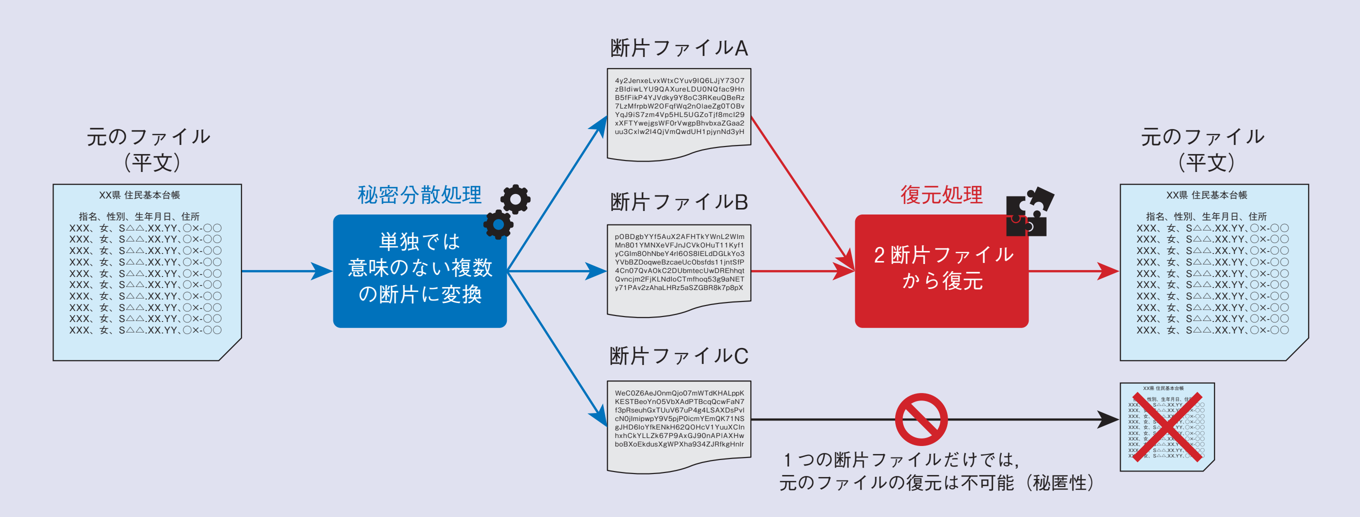
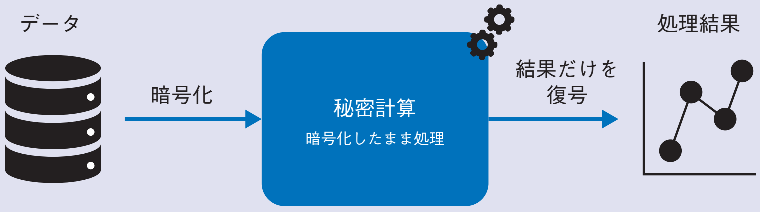


図2　秘密分散



	暗号化したまま行える範囲	
一般的な暗号	データの通信・保存	―
秘密計算		データの処理

図３　秘密計算

計算そのものの研究や，秘密分散を用いたさまざまなプロダクト（秘密分散技術trust-ss，分散ストレージSHSS，秘密計算技術「算師®」）の開発で得た知見をフィードバックし，扱いやすい秘密分散の選定に貢献しています．

NTTのプロダクトでは，３つの秘密分散方式を適切に使い分けて利用しています．2017年出版のISO/IEC 19592-２ではそれら３つの秘密分散方式を含む，５つの秘密分散方式が規定されています(6)．

さらに，最近ではこの秘密分散を基盤技術とした秘密計算の標準化も始まりました．

秘密計算の紹介（ISO/IEC 4922-1，２）

秘密計算は，データを暗号化したまま計算を行うための技術です．一般的な暗号はデータの通信・保存を保護します．秘密計算は，さらにデータの計算過程も保護することができます．秘密計算を使うことにより，個人のパーソナルデータや企業の営業秘密を用いる分析業務で，データを漏らさないだけでなく「データの中身を見ない」運用が可能になります（**図３**）．

これにより，より安全なデータ処理はもちろんのこと，今まで他組織に開示することが難しかったデータを持ち寄って，企業や業界の枠を越えた新しい統合分析が可能になると考えられています．

NTTでは暗号化の部分に秘密分散技術を利用した秘密計算の研究・開発を行っています．すなわち，データを秘密分散で断片に変換してからサーバに渡し，サーバはその断片を元データに戻すことなく計算を行います．新たなデータ流通・活用を可能にする技術として注目されており，NTT以外にもさまざまな企業・大学・研究機関で秘密計算の研究・開発が行われ，切磋琢磨している状況です．

2020年からISO/IEC 4922シリーズとして秘密計算の標準化が始まりました．ISO/IEC 4922-１は秘密計算全般に関する標準，ISO/IEC 4922-２は秘密分散に基づく秘密計算に関する標準になる予定です．NTTは両方のエディタとして積極的に規格作成を主導しています．

今後の展開

NTTの研究・開発の知見に基づき，暗号技術・プロトコルの国際標準の整備に貢献していきます．

■参考文献

⑴ https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf
⑵ https://standardsdevelopment.bsigroup.com/projects/9020-03695#/section
⑶ W. Diffie and M. Hellman: “New directions in cryptography,” In IEEE Transactions on Information Theory, Vol. 22, No. 6, pp. 644-654, Nov. 1976.
⑷ T. Kim and R. Barbulescu: “Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case,” Proc. of CRYPTO 2016 Part I, Vol. 9814, pp. 543-571, Santa Barbara, U.S.A., August 2016.
⑸ Y. Kiyomura, A. Inoue, Y. Kawahara, M. Yasuda, T. Takagi, and T. Kobayashi: “Secure and Efficient Pairing at 256-Bit Security Level,” Proc. of ACNS 2017, pp. 59-79, Kanazawa, Japan, July 2017.
⑹ https://www.ntt.co.jp/news2017/1710/171023a.html