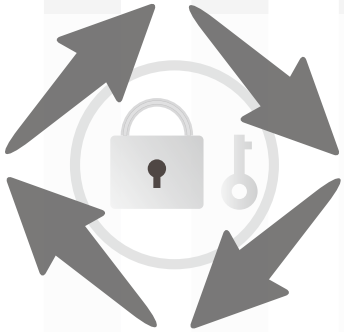

解説

基般

暗号を解かずにデータ処理
―準同型暗号の仕組みと産業応用―

下山武司（富士通研究所 データ・プライバシー保護プロジェクト）

「準同型暗号」とは

最近，準同型暗号（Homomorphic Encryption）と呼ばれる暗号方式が注目を集めている．準同型暗号を使うと，暗号を解かなくてもデータ処理ができるらしい，文字列検索もできるらしい，ということから，たとえば個人情報や金融情報等，機密データ・プライバシーデータの保護と利活用の両立を実現する切り札として期待されている．その一方，ここ数年で急速に進歩した新しい技術のため難解で，敷居が高いと思われている方も少なくないと思われる．本稿では，この準同型暗号を解説するとともに，広くデータ保護と利活用に向けた暗号技術について述べる．

準同型暗号の「準同型（Homomorphic）」とは数学用語で，数学的構造が同じ集合どうしを結びつける対応関係を意味する．この数学的構造とは，加算や乗算といった演算，あるいはその組合せで算出された要素の集まり全体のことである．この準同型という考え方を暗号に当てはめた場合，要するに準同型暗号とは，暗号化する前の平文の世界で演算できることは暗号文の世界でもでき，その結果は算術の意味において本質的には変わらない，という性質を持つことを意味している．この性質から，統計処理などのデータに対する処理内容を準同型暗号に対応する処理に変換し，それにより得られた結果を復号することで，平文に対する処理と同じ結果を得るという仕組みが実現できる．

準同型暗号には，加算あるいは乗算の一方のみができる単演算準同型暗号，加算と乗算の両方が可能であるが，その回数が制限される複演算準同型暗号，任意の処理が可能な完全準同型暗号（Fully Homomorphic Encryption）の3種類がある（**表-1**）．単演算方式は，RSA暗号やElGamal暗号等，比較的古くから知られていたが，複演算方式は，2005年にペアリング暗号を用い，加算に加え乗算が1回のみできるBGN方式を始め，2009年にGentryによって開発された完全準同型暗号を契機に，効率的に解くことが難しいとされる数学上の問題の1つである格子問題をベースとしたさまざまなバリエーションの準同型暗号が開発され，現在に至っている．

種類	暗号操作	処理性能	応用	代表的な方式
単演算準同型暗号	加算または乗算	高速	加算集計，電子投票，電子現金など	additive ElGamal, Pailler, RSA, 岡本-内山暗号
複演算準同型暗号	加算+乗算（回数制限）	回数が増えるに従い遅くなる	標準偏差，行列計算，文字列一致判定	BGN（乗算1回のみ），ideal格子ベース，整数ベース，Ring-LWEベース
完全準同型暗号	任意	かなり遅い	任意の演算，AES回路，ハッシュ関数	

表-1　準同型暗号の種類

準同型暗号は，ここがすごい

準同型暗号は，加算処理や乗算処理が暗号化したままで実施できるが，この性質によりさまざまな応用が可能になる．実際，これらの処理をビット単位で考えた場合，加算は論理回路で言うXOR回路，乗算はAND回路と考えられる．任意の論理回路はAND回路とXOR回路の組合せで表現することが可能であること

が知られている．よって何回でも演算できるような完全準同型暗号を使うと，理論的にはどのような演算でも暗号化したまま処理可能となる．しかし，完全準同型暗号は処理性能の面で課題が多く，実用的レベルには至っていないため，上記のようなどんな演算でも暗号化したまま処理を実用的な処理時間で行うというのは，現時点では難しいと言わざるを得ない．一方で演算回数を限定したSHE準同型暗号（Somewhat Homomorphic Encryption）は，完全準同型暗号よりも処理コスト・暗号データサイズともにかなり小さく，幅広い適用先に対し実用的に利用できると考えられる．この章では，これら準同型暗号でできる応用について述べる．

➡生体情報を使った安全な認証システム

モバイル端末やタブレットPC等が広く普及し，いつでもどこでも，メールアクセスや，検索などができるようになった．この背景には，ユーザからの要求を大規模に処理するクラウド技術やビッグデータの存在が大きいことが知られている．これらのサービスをビジネスとして捉える際には，誰にどのようなサービスを提供するか，どのように課金するかといったことを適切に管理するために，精度の高い個人認証技術が必須である．従来のIDやパスワードといった認証方式では，なりすましの危険があり，実際の被害事例も多く聞かれる．そこでユーザを特定する際に，指紋や静脈，光彩といった個人が持つ生体情報をユーザ認証に利用する生体認証技術が注目されている．生体情報は，個々人ごとに異なる性質を持つことから，なりすましを防止することが期待でき，個人を特定し，適切なサービスを提供することに役立つ．その一方で，生体情報は生まれながらにして持つ唯一の情報であるため，万が一，その情報が流出してしまった場合，一生取り返しがつかない恐れがある．よって，その扱いは慎重にならざるを得ない．通常の暗号化を用いることで，データを秘匿化し安全性を高めることは現在の技術でも十分可能であり，実際利用されている．その反面，生体情報は入力のたびに値が揺らぐという性質があり，従来暗号では，認証の際暗号データをいったん復号しない限り照合が難しい．従来の暗号化されたデータでは，外部からの攻撃に対し強固にしたシステムで守る必要があるなど，安全性を高めるためのコストがかかるため必ずしも導入が容易ではなかった．特にクラウドを利用した生体認証を考えた場合，クラウド上で生体情報が復号され，生の状態に戻されることには，ユーザの立場からすれば抵抗があり，セキュリティ管理等に課題も多いことから，従来の暗号技術では，生体情報を安全に守りつつ認証に利用することは難しい．そこで，データを暗号化したままで加算や乗算といったデータの演算処理が可能な，SHE準同型暗号を用いることで上記の問題を解決できる．準同型暗号を用いると，ハミング距離[☆1]を暗号化したままで計算することが可能なため，与えられた2つの生体情報（画像情報等）から抽出された，比較的短い特徴データのハミング距離を安全に計算することで，生体情報の安全性を保ったまま個人認証を行うことが可能となる．

➡購買履歴を用いた安全なデータマイニング

プライバシー情報の保護とその利活用のバランスを適切に管理しながら，利用価値の高い情報を安全かつ有効に活用するプライバシー保護データマイニングの研究が各方面で盛んに行われている．現在知られているプライバシー保護データマイニング手法には，大きく分けて匿名化・ランダム化・マルチパーティ計算・準同型暗号の4つのアプローチがある．購買履歴データ分析において，顧客データを劣化させることなく，大域的な統計・分析を含むより詳細な情報を得ることで，商品間の類似度指標を正確に求めたいような場合には，準同型暗号のアプローチが有効となる．以下に類似度指標計算の例を示す．

X,Y企業における2企業間の購買履歴データ分析を考える．その前提として2企業間の購買履歴データ分析において，まずX企業とY企業の間で共通の顧客IDが作成されX企業A商品とY企業B商

☆1 等しいビット数を持つ2つのバイナリデータで，対応する位置に対する値が異なるビットの個数．

顧客ID	企業X商品A
123	1（購入）
124	1（購入）
126	0（未購入）
129	1（購入）
130	0（未購入）
131	1（購入）
132	0（未購入）
135	1（購入）
136	0（未購入）
137	1（購入）

顧客ID	企業Y商品B
123	0（未購入）
124	1（購入）
126	0（未購入）
129	1（購入）
130	0（未購入）
131	0（未購入）
132	0（未購入）
135	1（購入）
136	0（未購入）
137	0（未購入）

表 -2　企業 X, Y の購買履歴データ

品との購買履歴データが，各企業で個別に管理されていたとする（**表 -2**）．購買履歴データ分析において，A 商品と B 商品の関連性を分析するためには，購買履歴集計データ（**表 -3**）を求める必要がある．この数値データを各種類似度指標の計算式に代入することで，A 商品と B 商品の間のさまざまな類似度（たとえば Jaccard 類似度 ＝a/(a＋b＋c) 等）を計算することが可能である．準同型暗号を利用すると，X 企業と Y 企業が持つ購買履歴データをお互いに公開することなくこの購買履歴集計データを計算できる．

➡遺伝子情報の安全な検索

近年，遺伝子を読み取る技術が急速に進歩し，特定の病気や身体的特徴等のさまざまな診断を，遺伝子情報を通じて特定することが可能となってきた．このようにしてさまざまな病院から集めた病歴や患者の遺伝子が持つ塩基配列情報を解析することで，新しい分析結果を得て，たとえば新薬の研究開発の効率化が期待できると考えられる．さらにクラウド環境やビッグデータ分析などの進展を背景に，健康管理などの個人に特化した新しい情報サービスが登場している．

その一方，病院の受診による病歴や，定期健康診

		商品B		合計
		購入	未購入	
商品A	購入	a=3	b=3	R1=6
	未購入	c=0	d=4	R2=4
合計		C1=3	C2=7	n=10

名称	類似度 s_{ij}	非類似度 d_{ij}
M1 交互作用統計量	$\frac{ad-bc}{\sqrt{R_1R_2C_1C_2/n}}$	$\max_{i,j}\{s_{ij}\}-s_{ij}$
M2 Cohen's Kappa	$\frac{2(ad-bc)}{2(ad-bc)+n(b+c)}$	$\frac{n(b+c)}{2(ad-bc)+n(b+c)}$
M3 Psi	$\frac{\lvert ad-bc\rvert}{\sqrt{R_1R_2C_1C_2}}$	$\max_{i,j}\{s_{ij}\}-s_{ij}$
M4 Sokal and Sneath 2	$a/(a+2b+2c)$	$(2b+2c)/(a+2b+2c)$
M5 Jaccard	$a/(a+b+c)$	$(b+c)/(a+b+c)$
M6 Czesanowski	$2a/(2a+b+c)$	$(b+c)/(2a+b+c)$
M7 Kulczynski	$a/(b+c)$	$\max_{i,j}\{s_{ij}\}-s_{ij}$
M8 Ochiai	$a/\sqrt{(a+b)(a+c)}$	$1-a/\sqrt{(a+b)(a+c)}$
M9 Yule's Q	$(ad-bc)/(ad+bc)$	$2bc/(ad+bc)$
M10 Russel and Rao	a/n	$(b+c+d)/n$
M11 カイ二乗距離	未定義	$\sum_{k=1}^{n}\frac{n}{n_{k\bullet}}(\frac{n_{ki}}{n_{\bullet i}}-\frac{n_{kj}}{n_{\bullet j}})^2$
M12 Rogers and Tanimoto	$(a+d)/(a+b+2c+2d)$	$(b+2c+d)/(a+b+2c+2d)$
M13 Sokal and Sneath 1	$2(a+d)/(2a+2d+b+c)$	$(b+c)/(2a+2d+b+c)$
M14 Simple matching	$(a+d)/n$	$(b+c)/n$
M15 Hamann	$(a+d-b-c)/n$	$(2b+2c)/n$
M16 主効果の相乗平均	$\sqrt{(a+b)(a+c)}/n$	$1-\sqrt{(a+b)(a+c)}/n$

表 -3　集計データと主な類似度指標 [1)]

断等で得られる健康情報などはプライバシーに深くかかわるデータであり，さらにそれに紐づけられた，遺伝子情報は究極の個人情報であり，特に厳重に守られるべき情報である．

データを秘匿しながら処理する技術である準同型暗号は，文字列の一致判定にも応用できることからこの技術を，医療情報の検索や，遺伝子に含まれる塩基配列の検索に応用することで，患者の遺伝子情報を暗号化で秘匿したまま，特定の配列パターンが含まれているかどうかを調べることが可能である（**図 -1**）．

このような性質を受けて，安全な遺伝子情報解析技術開発を促進させる動きとして，米国のサンディエゴ大学では，国際的なコンペを開催している．ちなみにサンディエゴ大学は DNA の発見者の 1 人として知られている Francis Crick 教授が在籍していたことで知られている大学である．2015 年 3 月に行

図 -1
遺伝子配列の文字列検索

われたコンペでは，与えられたVCFフォーマット（遺伝子情報圧縮形式の1つ）で記述された10万カ所の遺伝子情報を含むデータファイル2個から，それらのハミング距離ならびに編集距離（文字の挿入や削除，置換による2つの文字列の変形に必要な手順の最小回数）を，準同型暗号を利用して，暗号化したまま計算する課題が与えられ，複数の組織が各々解いた結果が公表されている．最も高い性能では，準同型暗号を用いてハミング距離を計算するのに約8分，1カ所当たり4.7ミリ秒であったとされ，実用的な処理速度に近づいていると報告された．

このように準同型暗号は，プライバシー情報・機密情報を安全に守りつつ利活用するための重要な技術の1つであることが示される．さらに準同型暗号は本章で取り上げた分野以外にも，教育や放送分野等に適用可能であり，応用の幅はさらに広がっている．

秘匿データ処理アラカルト

前章で述べた通り，準同型暗号を使うと，データを秘匿したままで加算や乗算といった統計量の算出や文字列検索などの処理，いわゆる秘匿データ処理を行うことができるが，このような機能を持つ暗号技術は，過去さまざまな方法が提案されてきた．ここでは，本稿で取り上げている準同型暗号以外の秘匿データ処理基盤技術として，ペアリング暗号とマルチパーティ計算，さらに共通鍵暗号を利用した秘匿検索技術などについて解説する．

➡ペアリング暗号

ペアリング（pairing）とは，数字の組（pair）をうまく1個の値にする数式であり，これを暗号に応用したものがペアリング暗号と呼ばれるものである．ペアリング暗号を利用すると，加算に加え，乗算が1回だけ可能という準同型性を持つBGN暗号が構成できる．ほかにもデータを秘匿しながら検索できる秘匿検索暗号や，暗号化の仕組みを使って，ユーザの属性に基づくアクセス制御情報をデータそのものに埋め込むことが可能な，関数型暗号等を構成できることが知られている．さらに最近では，このペアリングをベースとして，2つのデータが近い・遠いといった関係性を，異なる暗号鍵で秘匿化したデータに対しても判定することができるRelational Hash技術も提案され，従来の公開鍵暗号では面倒とされた鍵管理が容易となる技術が登場するなど，応用が広がりつつある．

➡マルチパーティ計算

マルチパーティ計算とは，複数の計算機（マルチパーティ）に分散された秘密情報に対し，安全な手順に従って，データを秘匿したまま協調して計算処理を行う技術である．個々の計算機上にある秘密情報からは，何の情報も得ることができないという情報論的安全性を有し，また分散されたデータを集めることで，元のデータを復元することができる機能を持っている．マルチパーティ計算を用いると，データを秘匿分散したままで，加減算や乗算といった算術演算とそれを利用した論理演算が任意回可能となる．この点でマルチパーティ計算は完全準同型暗号と似た特徴を持っているが，秘密分散技術をベースにしていることから，復号鍵の管理が不要である一方で，処理を行う際に複数の計算機間の通信が必要となる点に違いがある．

➡秘匿検索（キーワード登録型）

秘匿データ処理の一分野として，データを秘匿したままデータ検索を行う，秘匿検索技術がある．秘匿検索技術には，キーワードを暗号化して登録し，検索時に登録データとの照合判定を行うキーワード事前登録方式と，準同型暗号やペアリング暗号，マルチパーティ計算を用いることで，キーワードを事前に登録することなく，秘匿化した全文に対して検索を行う方式がある．ここではキーワード事前登録方式に基づく秘匿検索を実現する方法を紹介する．

キーワード登録方式は，事前に登録した暗号化キーワードと検索時に暗号化した検索キーワードが同一かどうかを判定することで，該当文書に検索キーワードがふくまれているかどうかを判定する方式で

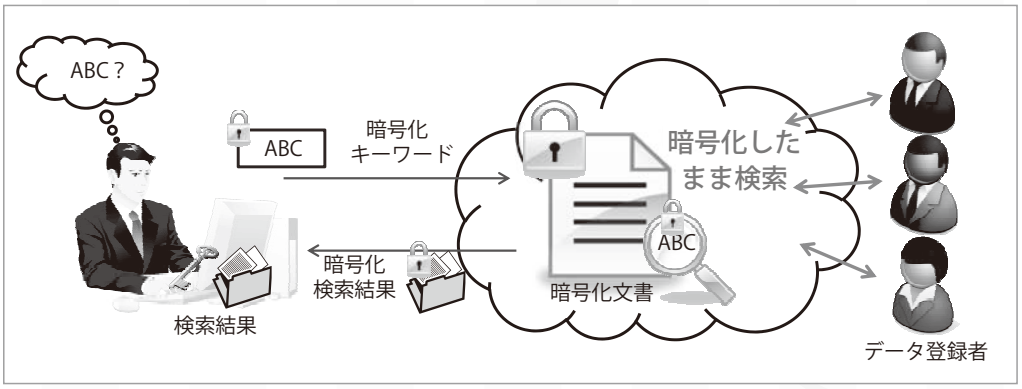

図 -2　秘匿検索

ある．複数のキーワードを指定できる方式や，規定個数以下の連続する文字列を暗号化する方式，あるいは類似文字列を検索できる方式も提案されている．使用する暗号により，共通鍵暗号型と公開鍵暗号型の 2 つのタイプがある．

共通鍵暗号型の秘匿検索技術として，2000 年の Song らによる方法[2] 等，いくつかの方法が提案されている．共通鍵暗号型の秘匿検索方式は，高い処理性能を持つ一方，キーワードの登録者と検索者で同じ秘密鍵を持つ必要があり，ユースケースを考える際，秘密鍵を登録者・検索者でどう安全に共有するかを別途検討する必要がある．

公開鍵暗号型の秘匿検索技術の例として，2004 年の Boneh らによる方法がある[3]．公開鍵暗号を用いて登録キーワードを暗号化して登録し，検索時には公開鍵に対応する秘密鍵によってのみ作ることが可能な検索キーワードを利用して，登録キーワードに一致しているかどうかを判定している．公開鍵暗号型では，登録時の暗号化鍵を公開することができるため，任意のユーザがキーワードを暗号化しておくことができる．よって，たとえば暗号メールにおけるキーワード検索をメールサーバで行うことができる等の用途が考えられる（**図 -2**）．

もうちょっとだけ詳しい話 ―仕組みと安全性・処理性能

ここでは準同型暗号が動く仕組みや安全性について解説する．

➡Ring-LWE ベース準同型暗号

一口に準同型暗号といってもさまざまな種類があることをすでに述べているが，ここでは加算と乗算が複数回実施可能な方式として 2011 年に Brakerski らによって提案された Ring-LWE ベースの準同型暗号を例に解説する[4]．本節はやや専門的な内容になるが，お付き合いいただきたい．

鍵生成

ガウス分布からサンプリングされた N 個の要素の集合（N 次元ガウス分布）からランダムな値 s を抽出し秘密鍵として固定する．同様にランダムに選ばれた要素 e を取り，さらにランダムな多項式の要素 p_1 と，平文の大きさを表すパラメータ t から $p_0 = -(p_1 \cdot s + t \cdot e)$ を計算し，公開鍵 $\mathrm{PK} = (p_0, p_1)$ を準備する．

暗号化

平文 m と公開鍵 PK に対し，N 次元ガウス分布のランダムな要素 u, f, g から暗号文 $Enc(m) = (p_0 u + tg + m, p_1 u + tf)$ を生成する．

暗号操作

暗号文 C_0, C_1 に対して，準同型加算は $C_0 + C_1$，準同型乗算は $C_0 \times C_1$ として定める．ただし演算 $+\times$ は，暗号化で生成された 2 要素の暗号文を変数 z の 1 次多項式 $C_0 + C_1 z$ として演算されたものとする．演算結果は 2 次多項式 $C'_0 + C'_1 z + C'_2 z^2$ となるため，3 要素 C'_0, C'_1, C'_2 となる．

復号

暗号文 C に対して，$\mathrm{DEC}(C) = [\sum_{i=0}^{n} C_i s^i]_q \bmod t$ を復号文と定める．ただし C_i は C の i 番目の要素，s は秘密鍵，$[a]_q$ は暗号文の空間の大きさ q に対して，

a を$\left[-\frac{q}{2},\frac{q}{2}\right)$の範囲に入るように剰余演算した値である．

➡準同型暗号が動く仕組み

本節では，前節で述べた Ring-LWE ベースの準同型暗号について，その動く仕組みと，処理性能について解説する．Ring-LWE ベースの準同型暗号は多項式の要素として処理されている．この多項式というのは加算と乗算の両方の演算が可能な数学的集合としての代表格と言ってよく，準同型暗号の性質である，暗号化したまま加算と乗算の処理が可能であるという性質を成り立たせる上で，非常に重要な役割を果たしている．

準同型暗号が正しく復号できる仕組みは，公開鍵の要素 p_0 の作り方がポイントになっている．$p_0=-(p_1 \cdot s+t \cdot e)$ より $p_0+p_1 \cdot s=t \cdot e$，つまり秘密鍵 s を使って変換すると暗号化の際に付加したランダムな要素に関する部分が綺麗に消え t の倍数にすることができるのである．もし平文が t 未満の値であれば先の値を t で割った余りを求めることで平文を取り出すことができることになる．これを m の暗号文 $Enc(m)=C$ を使って数式で示すと，次の通りである．

$C(s)=C_0+sC_1=(p_0u+tg+m)+s(p_1u+tf)=(-eu+g+sf)\,t+m$，より

$\mathrm{DEC}\,(C)=(-eu+g+sf)\,t+m \bmod t=m$

となり正しく復号できることが確かめられる．

ただし，秘匿データ処理を実施するたびに，暗号化の際に挿入したランダムな要素に対しても同様に演算処理が加えられてしまうために，結果的に暗号文のランダム要素の誤差が演算により大きくなっていく．秘匿データ処理を繰り返すと，この累積誤差が秘密鍵 s による復号可能範囲を超えてしまうため，正しく復号することができなくなってしまう．よって SHE 準同型暗号の秘匿データ処理の回数には制約がある．処理回数の制約をなくすためには，ブートストラップ[☆2] と呼ばれる処理が必要となるが，この処理には非常に大きな計算時間がかかるため，実用レベルには至っていない．

☆2 準同型暗号の復号処理を暗号化した状態で実施することで，暗号化処理の繰り返しによって生じたノイズをある程度小さくする方法．

➡準同型暗号の安全性

前節で解説した Ring-LWE ベース準同型暗号の“Ring-LWE”とは，固定された秘密鍵 s と多項式の要素 a，さらにガウス分布からサンプリングされた要素 e に対し計算された $a \cdot s+e$ の値を，要素 a，e を変えてたくさん集めたとして，S の値を求めるという数学的な問題である．Ring-LWE ベースの準同型暗号の安全性は，Ring-LWE 問題を解くことが非常に難しいことに由来している．ちなみに SHE 準同型暗号としては，この Ring-LWE 問題のほかにも，IDEAL 格子問題と呼ばれるものや，整数の近似 GCD 問題をベースとしたものが提案されており，各々特徴のある暗号アルゴリズムとなっている．これらの問題は，いずれも格子空間上の最短ベクトル問題（Shortest Vector Problem, SVP，効率的に解くことが難しいと考えられている数学的問題の 1 つ）と関係があるとされている．

なお，SVP 問題は NP 困難という，解くことが難しい問題の一種として知られていることから，もし将来，量子計算機が実用的なレベルにまで到達したとしても，その安全性が SVP 問題に帰着できる暗号については，破られることはないと言われており，耐量子計算暗号アルゴリズムとしても期待されている．

準同型暗号の課題と今後について

これまで紹介してきた通り，準同型暗号は，クラウドや IoT（Internet of Things）をはじめとする新しい情報環境への大きな流れの上で，さまざまなプライバシー情報・秘密情報を守りつつ利活用することが可能となる重要な技術の 1 つであると期待されている．その一方で，本格的な実用化に至るまでには，いくつかの課題があると考えられている．

まず，処理性能と暗号文サイズの肥大化の問題がある．SHE 準同型暗号を Intel Xeon X3480 3.07GHz 上で，2048 次元パラメータの場合で実装

し，処理性能を測定した結果，2048 ビット長の平文に対する暗号化，秘匿乗算，復号にかかる処理時間は，それぞれ，3.65 ミリ秒，5.31 ミリ秒，3.47 ミリ秒であり，RSA 暗号の処理時間と同程度である．ちなみにこの次元パラメータは，準同型暗号の安全性と演算の回数に関係がある．2048 次元は安全性を確保しつつ乗算 1 回が可能で処理性能がある程度高い範囲として設定されるが，秘匿処理が何度も実施されるような応用，たとえば秘匿データの集計結果を集め，さらに秘匿統計演算を行うような処理等については，さらに大きな次元パラメータが必要となり，より多くの処理時間がかかる．また暗号文サイズの肥大化も課題である．Ring-LWE ベース準同型暗号の暗号文は，上記のパラメータに対し，約 32 キロバイトであり，平文の約 120 倍となるため，容量に制約がある場合には問題となる場合がある．完全準同型暗号の処理性能については徐々に進化しており，最初に提案された 2009 年頃は，ブートストラップ処理（暗号処理によってたまった誤差を取り除く処理）に約 30 分程度かかっていたが，現在は 1 秒程度とされている．

準同型暗号は，任意の処理が行えると述べたが，条件分岐処理については，現状の準同型暗号では，安全性の理由から実現が難しい．計算された値によって処理を変える場合，本来秘匿処理中に漏れてはいけないはずの情報が，処理を分岐させることで，閾値を超えたという情報が計算サーバ側に漏れることを意味するためである．たとえば異常値の頻度を集計し一定以上になったらアラームを挙げるといった利用には，準同型暗号の秘匿演算処理のみで行うことは難しく，集計結果の復号処理をある程度の頻度で行う必要が出てくる．結果として，復号された各集計結果の値から秘匿データの各値が外部に漏れる可能性や，システムが複雑になってしまう恐れなど，新たな課題が見られることから，準同型暗号はあまり向かない．

さらにもう一点，秘密鍵の管理に関する課題を挙げておく．準同型暗号によって演算された結果は，秘密鍵を用いて復号することで得られる．この秘密鍵を使うと，処理結果だけでなく同じ鍵で暗号化されたすべての暗号文を復号することができてしまうことから，厳重な管理が必要になるが，誰がその役を担うか，秘密鍵を持つ者は誰なのか，という暗号システムを構築する上で避けて通れない課題がある．信頼できる鍵管理組織を運営することは，システム全体を複雑にし，コストを高めてしまう恐れがあり，簡単に解決されるものではない．秘匿検索技術に限れば，「秘匿データ処理アラカルト」の章で紹介した異なる鍵で暗号化した暗号文に対しても検索可能な Relational Hash 等の技術がある．

暗号技術は日々進歩し続けており，今後，これらの課題についてもいずれ解決され，次世代の暗号技術である準同型暗号がごく日常的に使われるようになる日も近いかもしれない．

参考文献

1) 石田　実，西尾チヅル，佐藤忠彦：交互作用距離による音楽 CD の購買予測，日本マーケティング・サイエンス学会第 84 回研究大会 (2008).
2) Song, D., Wagner, D. and Perrig, A. : Practical Techniques for Searching on Encrypted Data, S & P 2000, pp.44-55, IEEE (2000).
3) Boneh, D., Goh, E. -J. and Nissim, K. : Evaluating 2-DNF Formulas on Ciphertexts, In Theory of Cryptography, TCC2005, Springer LNCS 3378, pp.325-341 (2005).
4) Brakerski, Z. and Vaikuntanathan, V. : Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Message, In Advances in Cryptology, CRYPTO 2011, Springer LNCS 6841, pp.505-524 (2011).

(2015 年 10 月 7 日受付)

下山武司　shimo-shimo@jp.fujitsu.com

富士通研究所主管研究員．博士（工学）．1991 年富士通研究所入社．暗号研究に従事．本会喜安記念業績賞（2008, 2012），電子情報通信学会業績賞（2013），ドコモモバイルサイエンス賞（2013），各受賞．著書：気付力が夢をかなえる（日刊工業新聞社）．