URL https://journal.ntt.co.jp/article/37466
DOI https://doi.org/10.60249/25121201

NTTデータグループ　技術革新統括本部
グローバルアーキテクト推進部　シニア・スペシャリスト

中村泰治　Taiji Nakamura

世界最先端の国産暗号鍵管理システムの開発により，安心で使いやすいハイブリッドクラウド環境を提供

近年，経済安全保障の観点から，重要な情報を取り扱うシステムを海外資本のパブリッククラウドに頼ることなく，国内で自律的に運用していく気運が高まっています．しかし，パブリッククラウドの利便性は高く，当面はプライベートクラウドやオンプレミスにパブリッククラウドを組み合わせた，ハイブリッドクラウドの利用を促進することで，「自律性」と「利便性」を両立させていくことが現実的です．一般的に，パブリッククラウドの鍵管理はブラックボックス化されていることが多いため，利用者が主体的にこれを管理することは難しく，データを安全に利用するには，暗号鍵の管理技術が極めて重要となります．今回，この技術開発分野の一人者で，国が推進する「ハイブリッドクラウド利用基盤技術の開発」に取り組まれている，NTTデータグループ　技術革新統括本部の中村泰治氏に，強固な鍵管理によるデータセキュリティ技術の最新の研究開発状況と，技術者として大切にしている心構えを伺いました．

最新の国際標準規格に準拠する，世界でいまだ実現されていない鍵暗号モジュールの開発に挑戦

現在，手掛けている研究開発業務について教えてください．

現在，私たちのプロジェクトでは，2022年の経済安全保障推進法の制定に基づき，内閣府と経済産業省が構想を策定し，国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）が研究を推進する，経済安全保障重要技術育成プログラムの１テーマ，「ハイブリッドクラウド利用基盤技術の開発」へ全面的に取り組んでいます．

ハイブリットクラウドでは，各々が構築するシステムにおいて，利便性の高いパブリッククラウドの利用と，自律性を念頭にしたプライベートクラウド等の利用という，セキュリティポリシーの異なる領域を，データを行き来させて処理や利活用ができるような，データ中心のセキュリティを確保していくことが重要となります．

昨今，海外発のパブリッククラウドが普及する中，データセキュリティの「最後の砦」は暗号鍵にあることから，国内における暗号鍵分野の戦略的自立性が強く求められており，私たちは暗号鍵を正確に安全に使える，これまでにないシステムの実現に挑んでいます．

現状，暗号鍵管理システムは残念ながら外国製のシェアが非常に高いところですが，オールNTTで所有しているデータセンタ，クラウド，セキュリティ，暗号，ソフトウェアなどの優良な技術を結集させれば高性能な国産システムが完成できるはずだ，との思いで研究開発を進めています．

NTTデータとしては，この技術を活用することにより，クラウド基盤でのサービス提供をめざすとともに，将来のハイブリッドクラウドを構築する布石としても期待しています（**図１**）．

その技術開発は大きく３つに分かれています．

■暗号鍵管理システムベース開発（図２）

パブリッククラウドのサービスプロバイダ側で内部不正や人的ミス，安全管理処置の不備が生じると，データセキュリティが破られるリスクが存在します．よって，利用者が内部仕様を知るとともに，暗号鍵の生成やローテーション等の管理を高セキュリティに実施できる必要があります．本検討では，事実上の世界標準となっている米国NISTが定める鍵管理要件仕様を満たすべく，クラウド上でも技術的に機密が保たれる仕組みTEE（Trusted

Execution Environment：高信頼性環境）*1ベースの暗号モジュールをプラグインしたシステムを開発しています．TEEはメモリが暗号化されており，OpenSSL*2に代表される暗号ライブラリと比較しても，アクセスが難しく，鍵を生成，暗号化・複合化するうえで，セキュリティ的に極めて安全で理想的な環境といえます．

■クラウド統合暗号鍵管理モニタリング・監視技術

現在，暗号鍵の利用状態を統合的にモニタリング・監視する機能を提供する暗号鍵管理サービスはほとんど存在せず，利用者の負担が増加しています．そのため，ハイブリッドクラウドやマルチクラウド環境において，クラウド統合暗号鍵管理のモニタリングや監視技術を新規に開発しています．

■PQC（耐量子計算機暗号）*3実装技術

暗号アルゴリズムに関しては，現在のアルゴリズムが量子計算機によって現実的な時間で解読されてしまう危殆化が懸念されて

＊1 TEE：通常のOSから独立した，CPU内に設けられた特別（安全）な領域．CPUのハードウェア機能により保護され，たとえOSに不正アクセスがあっても，データやコードの完全性・秘匿性が保証されます．
＊2 OpenSSL：TLS/SSLプロトコルを実装したオープンソースの暗号ライブラリで，Webサーバやメールサーバなどさまざまなシステムでセキュアな通信を実現するために広く利用されています．

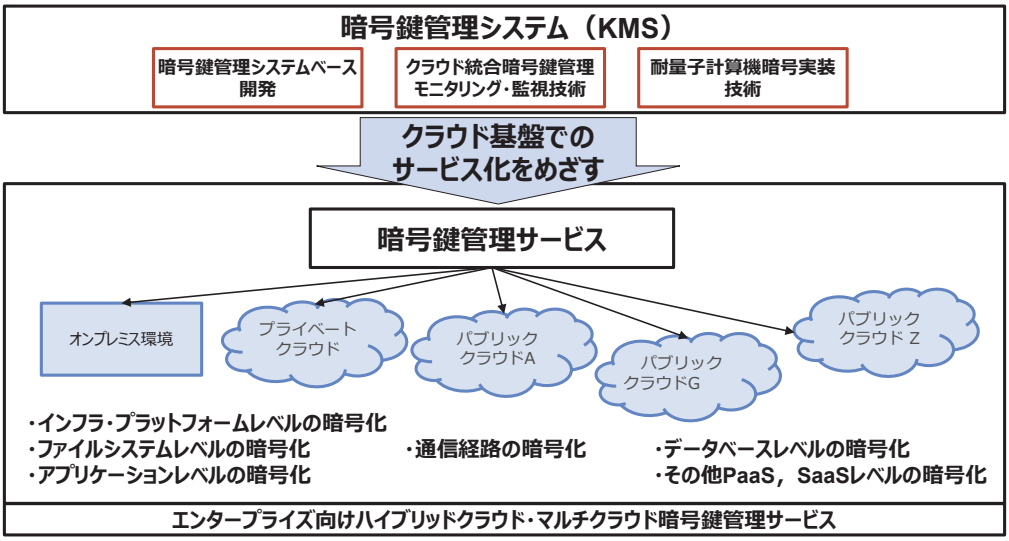

図1　暗号鍵管理システムの実施項目とめざす姿

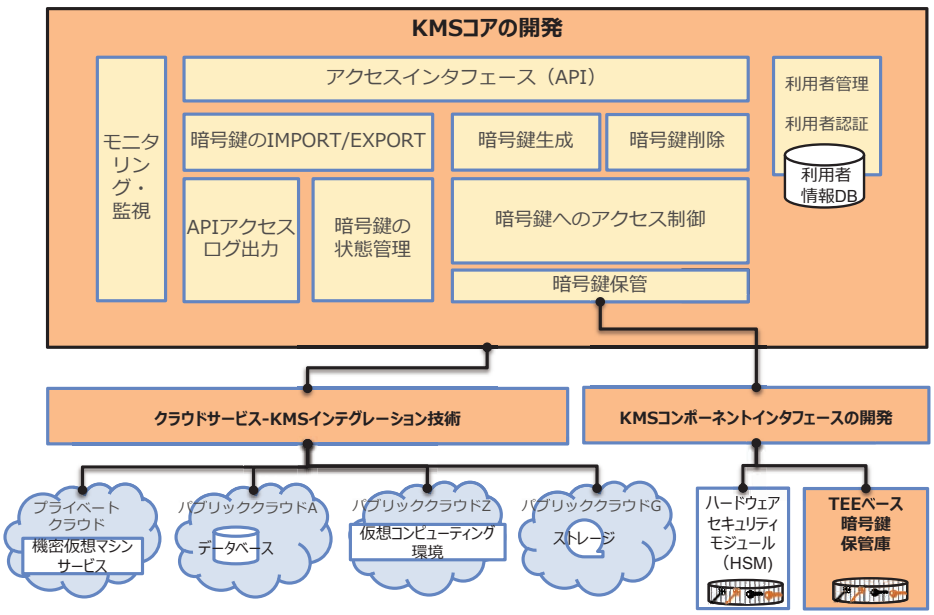

図2　暗号鍵管理システムベース開発の構成

おり，鍵管理システムベースにNTTグループオリジナルの耐量子計算機暗号アルゴリズムQR-UOV[*4]を独自に実装しています．

これら一連の開発を通じて，技術的にハードルが高く，現在，挑戦的に取り組んでいるのが，TEEに基づく鍵管理暗号モジュールの実装になります．私たちは，TEEベースで高性能なモジュールを開発する際に，もっとも理想的とされるインテルSGX[*5]のチップを活用することで，NIST（National Institute of Standards and Technology：米国国立標準技術研究所）が定める国際標準規格FIPS140-3による暗号モジュール規格に準拠するモジュールの実現を目標に掲げています．同時に，このシステムとAWS，Azure，Google Cloudなどのパブリッククラウドとの連携も実現しているところです（**図3**）．

ところで，このインテルSGXを使用したTEEを実装し，FIPS140-3の最新規格を取得したモジュールは世界的にもまだ実在していません．これは，SGXを組み込んだTEEの中でソフトウェアを作成するプロセスが，通常のOSにLinuxのアプリケーションを作成するときとでは大きく異なり，独自のプログラミングが求められるため，開発のハードルがかなり高くなることが理由の1つです．

また，図3右の黄色で囲まれた個所に認証テストにパスする要件が列挙されていますが，self-testsについては規格が旧から新へと改変される中，要求されるセキュリティ条件が時代の要請により増えてきたこと，そしてself-tests自体，その方法を各社が権利化しているため，それを侵害せずに実施していく必要があることなど，認証取得の技術的ハードルを一層高めている理由でもあります．

よって，現在，私たちが取り組んでいる，インテルSGXを使用するTEE内において，既存のアルゴリズムやPQCのアルゴリズムを実装し，さらにFIPS140-3の認証を取得することは，技術的に決して簡単なことではないのです．

私たちは，こうした課題を現在乗り越えようとしている最中で，システムの新規性や性能性ともに，世界でもっとも先行しているプロジェクトの1つと認識しています．新規格の認証テストが通った暁には，安心して使えるFIPS140-3国産モジュールソフトウェア第1号となります．

現在，実施されている総合システム検証のポイントや来年度の社会実装化に向けた展開についてお聞かせください．

現在開発している，暗号鍵管理システムの各要素技術は今年度上期でほぼ完成し，市場のニーズを考慮しながら，下期から総合的な検証を開始しているところです．ここでは，来年度の社会実装に向けて，各クラウド利用者が暗号鍵を制御する度合い（セキュリティの度合い）に応じて提案されている，3段階のモデルをスコープに，その実行性について検証していきます（**図4**）．

＊3 PQC：将来実用化される可能性のある強力な量子コンピュータでも解読できないように設計された暗号技術の総称．
＊4 QR-UOV：NTT社会情報研究所が開発したデジタル署名方式．多変数多項式問題の難しさを安全性の根拠としており，署名および公開鍵のデータサイズが小さいことが特徴．NISTの耐量子暗号標準化プロジェクトの第2ラウンドに進出した有力候補．
＊5 インテルSGX：Intel製CPUに搭載されたハードウェアベースのセキュリティ機能．プログラムの実行中にメモリ上に暗号化された保護領域を作成し，OSやハイパーバイザ，さらには物理的な攻撃からも機密データとコードを保護できます．

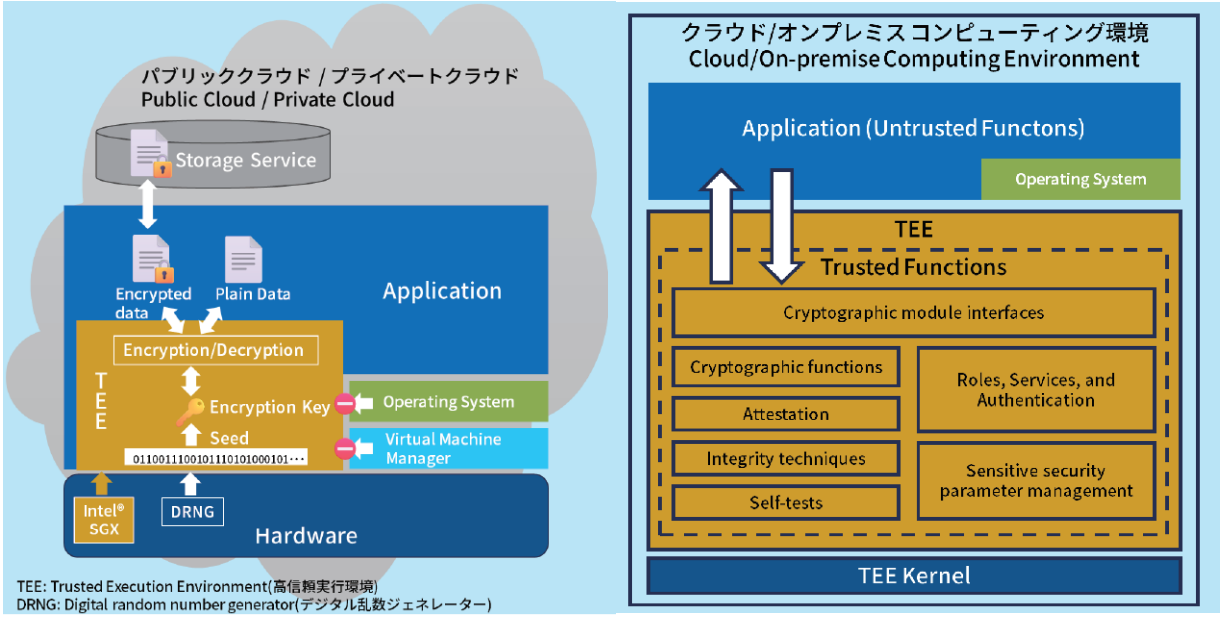

図3　Intel SGXを活用したTEEとその周辺の構成

■BYOK（Bring Your Own Key）

鍵の生成を利用者側で行い，生成した鍵をクラウド事業者側に持ち込み，持ち込まれた後の鍵はクラウド事業者側で管理されるモデルです．市場動向調査によると，マルチクラウド・複数リージョンにまたがる鍵の一括管理を目的とし，BYOKはグローバルメーカなどで需要があるとのことです．よって総合検証では，社内でトライアルプロジェクトを募集し，AWS，Azure，Google Cloud，OracleCloudなどのパブリッククラウドへの暗号鍵配送や鍵の一括管理について，実サービスに近い環境で評価していきます．社会実装に向けては，NTTデータのクラウドサービスのラインアップに加えるとともに，他社クラウドサービスにも採用されるよう，ソフトウェアを提供していきます．

■HYOK（Hold Your Own Key）

クラウド事業者が利用者の鍵管理システムを利用し，クラウド事業者側は利用者の管理下で鍵を扱うことになり，利用者が常に鍵管理を行うことが可能なモデルです．NTTデータによる市場動向では，2024年度に世界で話題になったものの，国内では浸透しておらず，暗号鍵は自国・自社の設備で保管する必要がある要件への対応に提起しているところです．よって，総合検証では，有望なユースケースの１つであるデータローカリゼーション要件への対応が十分であるか，想定利用者に評価していただく予定です．具体例として，重要技術を取り扱う製造業は開発・製造データのローカリゼーション管理が求められるケースがあり，データを特定の国や地域の物理的なサーバに保存・処理することを要求する法的・規制上の義務を遵守するために，暗号鍵を鍵管理システムに保管し，その所在が可視化されていることを検証する予定です．

■BYOE（Bring Your Own Encryption）

利用者が鍵の管理ならびに利用を一人称で行うモデルで，クラウド事業者が全く鍵にアクセスできないようにすることが可能です．社内の市場調査によると，国内や国外における新規の金融サービスを企画・開発する際に，この方式は必要とされるケースがあるとされています．したがって，総合検証では，ブロックチェーンの取引所ウォレットの秘密鍵を保管するシステムなどを検証します．例えば，イーサリアム基盤を用いたB2B金融サービスの場合は，イーサリアムの秘密鍵を，バリデータ（検証者）ノードから分離して，安全な環境として鍵管理システムに保管し，トランザクションデータにデジタル署名を実行するなど検証していきます．検証後はこれら機能を鍵管理システムに追加実装し，新規金融サービスに対応していくこととします．

利用者側の鍵管理のセキュリティレベルは向上していきますが，どの制御レベルの機能を利用するかは，利用者が求めるセキュリティの要件に依存します．いずれの制御レベルにおいても，暗号鍵に必要な保護および保証が提供され，暗号鍵のライフサイクル管理に必要な機能が提供されることが求められます．

2026年度以降の実用化では，経済安全保障重要技術育成プログラムの趣旨である「研究成果は，民生利用だけでなく，公的利用につなげていくことをめざす」を実現するため，NTTデータのハイブリッドクラウドは国内実績No.1の鍵管理システムをめざすことや，最強の暗号や認証技術の投入で長期安心して使える鍵管理システムをめざすことを方針とし，NTTデータによる鍵管理サービスの提供や他社への製品販売などを検討していく予定です．

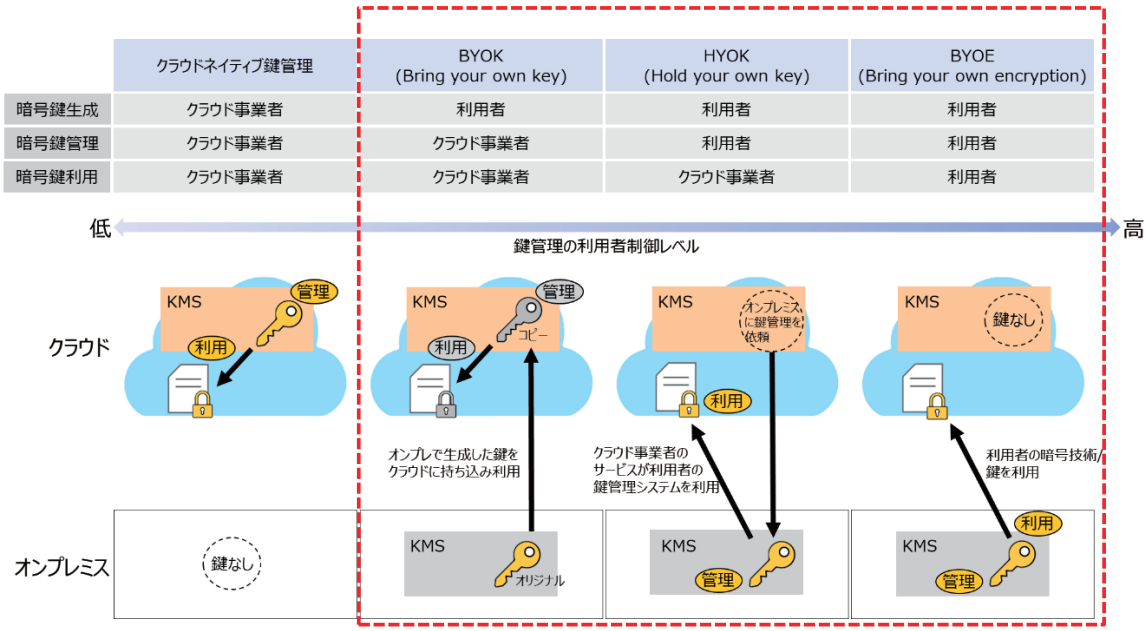

図４　パブリッククラウドにおける鍵管理の利用者制御モデル

海上自衛隊との共同システム開発で得たセキュリティ技術の知見や経験を，強固な暗号鍵システムの開発に活かす

今回の研究開発の進め方を教えてください．また，これを実行するうえで役に立ったご自身の経験などありますでしょうか．

本研究開発は，いわゆる「システム開発」と異なり，あらゆる面で不確実性が高く，調査，要件定義，事前検証（PoC），開発，テストというステップを組み，段階的に管理しながら進めていく必要がありました．その中でもっともコアな分野であるセキュリティにおいては，暗号のアルゴリズムに加え，暗号に関連した標準類の作成やベストプラクティスに関する知識が重要になります．

私自身，防衛省の海上自衛隊と共同で，長期間にわたりシステム開発をしてきた経験が，セキュリティの知見を高めるうえで，極めて大きかったといえます．装備品を開発するうえで，日米同盟として米国とのつながりが強い中，米国流のプロトコルに関する知識が必要となると，米国のエンジニアと仕事をする機会も多くありました．これらを通じて，米海軍の暗号鍵管理技術に接することができたのです．

かつては，米国等とやり取りする通信ネットワークは完全に隔離された専用線で運用されていましたが，インターネットの普及で，ある時期からバックアップ回線はインターネットも選択可能になり，私もこのテストプロジェクトに携わることとなりました．そこでは，インターネットでフォローする暗号アルゴリズムは，一般的に私たちが知っているものではなく，米海軍オリジナルのアルゴリズムを必要とされていましたので，暗号鍵を同盟国と米国の間でどう扱うかの取り決めや，鍵のローテーション期間をどうしていくのかなど，安全を守りながらデータ通信を実行するうえで，必要なプロセスを一通り学習できたのは大きな収穫でした．

また本研究の鍵管理システムをつくるうえで，暗号を取り扱う観点から必要となるのが，パブリッククラウドの知識と，それを使ったソフトウェア開発スキルとなります．例えばクラウド統合暗号鍵管理モニタリング・監視技術の場合，クラウドごとに仕様が異なるストレージやDBMSなど数多くのクラウドサービスの挙動に関する知見，シンプルで後々のメンテナンスも楽になるモニタリング手法やログデータ分析手法を考案するスキルが求められます．パブリッククラウドの知見は，個人というよりはNTTデータとして蓄えていますので，ここはNTTデータならではの強みであるといって良いと思います．昨今はクラウド環境のIaC（Infrastructure as Code）スキルが強く求められるなど，多様な人材が必要であり，いわゆるチームビルディングにも力を入れているところです．

さまざまな研究者，開発者，技術者と交わり，思いもしなかった概念や解決方法に接することを心掛けよう

自社のチーム内で，あるいは他社と共同で研究開発を進めていく中，日頃から心掛けていることはありますか．また，後進に向けたメッセージをお願いします．

現在，私たちのチームは20名ほどで構成されていますが，良い達成目標を与えると同時に，最大限の裁量も与え，取り組んでもらっています．これは若い人でもベテランでも通用するやり方だと思います．最終ゴールを示し，その過程については各メンバーが考え，試行錯誤してもらうと，皆その最終アウトプットに向けて，かなり良いロジックを考えてくれます．その際，目標を常に合わせていくことは非常に重要です．

特に若い人は，技術の習得が早く，古いタイプのC言語も，新しいクラウドのスクリプトも，熱心に学習して，実装に向けて高速に進める力があるので，明確な目標と，現在困っている課題の解決方法，方針を与えるだけで，コミュニケーションがとりやすいと感じています．

また，他社や他分野の技術者と共同でプロジェクトを進めていく際にも，目標を合わせることは重要です．例えば私の経験で思い出すのは，一緒に組み上げたシステムでトラブルが発生したときのことです．米国と日本との間で通信トラブルが発生し，これを解決するときに，各社が出したアイデアはさまざまで面白かったです．ある会社はハードウェア面で通信基盤回路の電圧電流値をチェックしました．また，ある会社は通信ケーブルの電圧や電流値を測定しました．NTTデータはその信号を受け取ったドライバーソフトや通信アプリケーションが期待どおり作動しているのかを確認しました．

私たちNTTデータにとって，電圧電流まで測定する発想は思いもよらないことでした．このように，各社が“ここが怪しい”と思うところを広く持ち寄り，一緒に調査，対策を打ち，解決したという経験は貴重でした．ですから，目標は1つに合わせて，そのアプローチは自由であるべき，ソフトウェア的な視点とハードウェア的な視点それぞれで観察していかないと，良いものはできないですね．

私自身，NTTデータ関係者はもとより，海上自衛隊の業務を通じて交流のあった米海軍エンジニアの方との交流，そして5年間在籍したNTT研究所で得た人脈は大きな糧となりました．ある意味特殊な分野である「暗号鍵管理システム」を企画できたのも，このおかげと思っています．さまざまな研究者，開発者，技術者と交わって，新しい視点を得て，自分では思いもしなかった概念や問題解決方法に接するよう心掛けてください．