

2026 年 10 月 22 日
株式会社データクレシス

***国産初、量子コンピュータ時代に備える PQC 対応 IRM「DataClasys PQC」を 12 月発売**
— 今盗まれたデータの将来の解読リスクに備える、次世代データ保護基盤 —



株式会社データクレシス（本社：東京都千代田区、代表取締役：曾我 祐二郎、以下「データクレシス」）は、量子コンピュータ時代を見据え、耐量子計算機暗号（PQC：Post-Quantum Cryptography）に対応した耐量子データセキュリティソリューション「DataClasys PQC」を開発し、2026 年 12 月より発売いたします。

量子コンピュータによる暗号解読が将来現実化した場合、すでに窃取・保存された機密情報は、その時点から保護し直すことができません。こうした将来の情報漏えいリスクに今から備えるため、データクレシスはファイル暗号化と鍵保護を組み合わせた、国産初の PQC 対応 IRM 製品「DataClasys PQC」を開発しました。

DataClasys PQC は、従来の DataClasys が備えるファイル単位の暗号化と利用権限管理を継承しながら、将来の量子コンピュータによる暗号解読リスクに備え、暗号鍵の保護や鍵確立などに関わる暗号技術を PQC 対応とした次世代の IRM（Information Rights Management）製品です。

昨今、企業や組織における不正アクセスや情報漏えいインシデントが相次ぐなか、自民党からは政府の重要システムへの PQC 導入の加速や移行時期の前倒しを求める提言案が示されるなど、量子コンピュータ時代に備えた早期対応の重要性が高まっています。

データクレシスは、量子コンピュータ時代を見据えたデータ保護技術をいち早く社会に提供することで、企業や組織が保有する重要情報の長期的な保護と、暗号解読リスクによる被害リスクの低減に貢献してまいります。

*国産初の PQC 対応 IRM「DataClasys PQC」

- 日本製 IRM の 40 商品を調査した結果。2026 年 10 月時点、ステラアソシエ株式会社調べ

DataClasys PQC 開発の背景

量子コンピュータの進展と AI による技術革新

現在、インターネット通信の安全性の確保や電子署名、企業の重要情報の保護など、デジタル社会のさまざまな場面で、RSA や楕円曲線暗号（ECC）などの公開鍵暗号技術が広く利用されており、この暗号技術は、従来のコンピュータでは解くことが極めて難しい数学的問題を安全性の基盤としています。

一方、量子コンピュータは、量子力学の原理を利用して計算を行い、特定の問題について、従来のコンピュータでは解くことが難しい計算を高速に処理できるとされています。

そのため、将来、十分な暗号解読能力を持つ量子コンピュータが実現すると、RSA や ECC など、現在広く利用されている公開鍵暗号の安全性が失われることが明らかになっています。

量子コンピュータの研究開発が世界各国で進むなか、AI（人工知能）の活用による技術革新も進んでいます。2026 年 10 月には、米国 Anthropic が、AI を用いて従来の研究成果を上回る効率的な量子回路を設計したと発表しました。

この成果には、楕円曲線暗号の量子解読にも関係する計算処理の効率化が含まれており、AI が量子コンピュータの実用化に向けた技術開発を加速させる可能性を示しています。

世界で進む耐量子計算機暗号（PQC）への移行

こうしたリスクに備える暗号技術が、耐量子計算機暗号（PQC：Post-Quantum Cryptography）です。

PQC は、将来の量子コンピュータによる攻撃に対しても安全性の確保を目指す暗号技術です。

米国国立標準技術研究所（NIST）は 2024 年 8 月、鍵確立に用いる ML-KEM などの PQC 標準規格を正式に発行しました。世界各国で移行に向けた取り組みが進められています。

日本政府も、政府機関等における PQC への移行について、原則 2035 年までに行うことを目指す方針を示しており、移行に向けたロードマップの策定を進めています。

さらに、日本経済新聞の報道によると、自民党が取りまとめたサイバー防御に関する提言案では、政府の重要システムへの PQC 導入を加速し、2035 年ごろを目標とする移行の前倒しを後押しする考えが示されています。これは政府による前倒し決定ではありませんが、PQC への早期移行の必要性が政策面でも重視されていることを示す動きです。

※出典

内閣官房 国家サイバー統括室「政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）」（2025 年 11 月 20 日）

日本経済新聞「『サイバー緊急事態』本部」（2026 年 10 月 20 日、記事利用許諾番号：004961）

将来の暗号解読リスクは、すでに現在の課題

量子コンピュータによる暗号解読の脅威は、将来だけの問題ではありません。

その理由が、「Harvest Now, Decrypt Later（HNDL）」と呼ばれる攻撃です。

HNDL は、現在は解読できない暗号化データをあらかじめ窃取・保存し、将来、量子コンピュータによって解読することを狙うものです。

一度窃取された暗号化データは、その後、企業が暗号方式を変更しても、攻撃者の手元にある過去のデータを保護し直すことはできません。

つまり、現在窃取された情報が、5年後、10年後の情報漏えいリスクにつながる可能性があります。

企業や組織内に存在する、設計情報、研究開発情報、製造技術、知的財産、個人情報、医療情報、経営情報など、長期間にわたり機密性を維持する必要がある情報の保護には、今から必要な対策を進めることが重要です。

不正アクセスが相次ぐ今、求められる「データそのものを守る」という考え方

近年、AIを活用したサイバー攻撃の高度化・自動化が進み、不正アクセスや情報窃取のリスクが高まっています。こうした状況において、企業には侵入防止だけでなく、情報が持ち出された場合にも、権限のない第三者が利用できない形でデータそのものを保護する対策が求められています。

また、ファイル本体を強固な暗号技術で保護していても、それだけでシステム全体の将来の安全性を判断することはできません。暗号化されたファイルを正規利用者が利用するためには、暗号鍵を安全に保護・確立する仕組みが必要であり、その過程でRSAやECCなどが使用されている場合、将来の量子コンピュータによる影響も考慮する必要があります。

これからは、ファイル本体の暗号化だけでなく、そのファイルを利用するための「鍵を守る仕組み」まで考えることが重要です。

独自調査から見た、長期機密情報とPQC対応の課題

データクレシスが実施した、経営層500人と情報セキュリティ・IT関係者500人の計1,000人を対象とする調査では、耐量子計算機暗号（PQC）について「知らない」と回答した人が50.0%に上りました。特に経営層では72.4%となり、PQCに関する認知の低さが明らかになりました。一方、勤務先が保有する機密情報について、最も長い機密保持期間が「5年以上10年未満」「10年以上」「期限を定めず」と回答した人は合計66.8%でした。

勤務先のPQC対応状況については、45.0%が「具体的な取り組みは行っていない」と回答しています。

これらの結果は、長期間にわたり保護すべき情報が存在する一方、PQCの認知や対応には課題が残されていることを示しています。

※調査概要

- 調査主体：株式会社データクレシス
- 調査対象：全国の企業経営層（20～79歳）および情報セキュリティ・IT関係者（20～64歳）の男女
- サンプルサイズ：1,000人（経営層500人、情報セキュリティ・IT関係者500人）
- 調査年月：2026年10月
- 調査手法：インターネット調査
- 実査委託先：楽天インサイト株式会社

DataClasys PQC の開発：現在と将来、双方の情報保護リスクに対応

こうした背景から、データクレシスは、従来の IRM によるファイル暗号化と利用権限制御に PQC を組み合わせた「DataClasys PQC」を開発しました。

ファイル本体には AES-256 を使用し、暗号鍵の保護には ML-KEM-1024 と ECDH P-521 を組み合わせたハイブリッド方式を採用しています。

これにより、現在の情報漏えい・不正利用リスクと、将来の量子コンピュータによる暗号解読リスクの双方に備える、データ保護・利用統制基盤を提供します。

DataClasys PQC の主な特長

耐量子計算機暗号（PQC）への対応

ファイル本体の AES-256 による暗号化を維持しながら、鍵の保護や鍵確立など、ファイル利用を支える暗号技術を PQC 対応としています。

ファイル単位の暗号化と業務上の利便性を両立

暗号化後もファイルの拡張子やアイコンを変更することなく、Microsoft Office や CAD など、対応するさまざまな Windows アプリケーションで、通常の操作感で利用できます。

組織外へ持ち出された後も利用権限を制御

利用者ごとに閲覧・編集等の権限を設定できます。暗号化されたファイルが組織外へ持ち出された場合にも、権限のない第三者が利用できない形で情報を保護します。

暗号鍵・利用権限の一元管理と操作ログの取得

暗号鍵や利用権限をサーバで一元管理するとともに、操作ログを取得し、企業のデータガバナンスや証跡管理を支援します。

従来の DataClasys からの PQC 移行にも対応

既存の DataClasys V5.x をご利用のお客様についても、DataClasys PQC への移行を可能とする構成を用意します。

従来方式で暗号化された既存ファイルについては、暗号鍵の更新や必要に応じた再暗号化など、利用環境に応じた移行設計を行うことで、段階的に PQC 対応環境への移行を進めます。

※既存ファイルが自動的に PQC 対応へ変換されるものではありません。移行方法・提供条件については個別にご案内します。

DataClasys PQC 製品体系

導入形態・規模に応じた製品

DataClasys PQC では、企業規模や導入方針に応じて選択できるよう、製品・ライセンス体系を刷新します。

従来からの永続ライセンスに加え、新たに 2 種類のサブスクリプションライセンスを提供します。

製品・ライセンス	概要
Subscription License Standard Edition	1 ユーザから導入可能。中小・中堅企業向けの基本構成
Subscription License Enterprise Edition	100 ユーザ分のライセンスと、冗長化・AD 連携等の主要機能を含む構成
Perpetual License (永続ライセンス)	1 ユーザから導入可能。必要な製品・オプションを組み合わせる永続利用型

※いずれの体系も、オンプレミス環境やプライベートクラウド環境でのクライアント・サーバ型です。

※サブスクリプションライセンスには、契約期間中の製品保守が含まれます。

※永続ライセンスについては、初年度の製品保守を無償提供します。

全社の PQC 対応を加速する、「DataClasys PQC Unlimited Program」

量子コンピュータ時代を見据えた PQC 対応の推進と、全社的なデータ保護・利用統制基盤の整備を支援するため、先着 100 社限定の「DataClasys PQC Unlimited Program」を提供します。

本プログラムは、5 年間の契約で年額 1,200 万円（税別）とし、対象となる DataClasys PQC のサーバライセンス、ユーザライセンスおよびデータクレンジング指定オプションを、数量制限なく利用できる特別プログラムです。

これにより、ライセンス数の増加に伴う追加購入を意識することなく、部門単位での導入から全社・グループ規模への段階的な展開を支援します。

※適用には所定の条件があります。導入支援、設計、構築、移行、運用支援等の役務は含まれません。

DataClasys PQC 希望小売価格公表について

DataClasys PQC の希望小売価格は、2026 年 11 月 6 日に公表する予定です。

お客様の DataClasys PQC 事前導入相談について

DataClasys PQC の事前導入相談は、2026 年 10 月 26 日より受け付けます。

ご相談は、末尾の「お客様からのお問い合わせ先」へご連絡ください。

盗まれたデータが、5 年後、10 年後に解読された場合。そのとき、説明できますか？

企業が長期間保護すべき重要情報は、現在の安全性だけでなく、将来の暗号解読リスクも見据える必要があります。

一度窃取された暗号化データは、後から暗号方式を変更しても保護し直すことはできません。

データクレシスは、ファイルそのものと暗号鍵を守る DataClasys PQC を通じて、PQC 対応をこれからのデータ保護における新たな選定基準として提唱し、その普及に取り組んでまいります。

DataClasys について

DataClasys は、累計導入社数 1,000 社以上の実績を持つ国産 IRM 製品です。2003 年から培ってきたファイル暗号化・利用権限管理技術を基盤に、さまざまな Windows アプリケーションに対応しています。ファイルの拡張子を変更することなく暗号化し、利用者ごとの権限制御や操作ログの取得などにより、重要情報の保護を支援しています。

株式会社データクレシス 会社概要

会社名：株式会社データクレシス

代表者：代表取締役 曾我 祐二郎

所在地：東京都千代田区

事業内容：ファイル暗号化製品 DataClasys の開発・販売

コーポレート Web サイト：<https://www.dataclasys.co.jp/>

DataClasys Web サイト：<https://www.dataclasys.com/>

【お客様からのお問い合わせ先】

DataClasys PQC の導入のご相談については、以下よりお問い合わせください。

株式会社データクレシス 営業本部

電話番号：03-3861-2348 電子メール：product@dataclasys.co.jp

※受付時間：平日 9 時 00 分～18 時 00 分（土日祝日および年末年始弊社休業日を除く）

【本件に関する報道関係者からのお問合せ先】

株式会社データクレシス マーケティング本部

電話番号：03-3861-2348 電子メール：pr@dataclasys.co.jp

※受付時間：平日 9 時 30 分～17 時 30 分（土日祝日および年末年始弊社休業日を除く）