金融庁「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」

耐量子計算機暗号（PQC）に関する概況等について

2024/09/20

株式会社NTTデータ
テクノロジーコンサルティング事業本部
テクノロジーコンサルティング事業部
小黒　博昭

※本資料は9月20日の検討会資料に編集上の修正を加えている場合があります。

目次

1. PQCに関する概況、現状認識

2. PQC移行に向けたサービス提供に関する状況

1

PQCに関する概況、現状認識

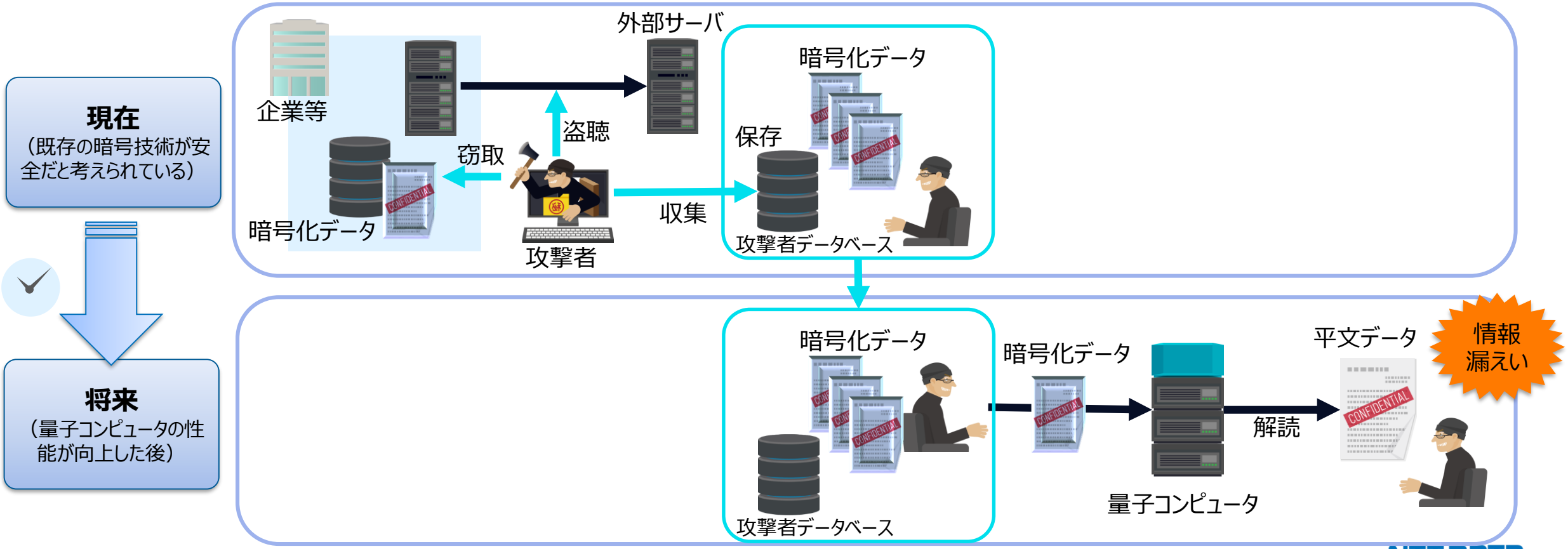
※「Capture now, decrypt later 攻撃」または「Harvest now, decrypt later 攻撃」とも呼ばれる。

Store now, decrypt later 攻撃

攻撃者は長期的な視点から暗号解読を成功させようとします。現在は量子コンピュータの性能が十分でないため暗号を破ることができなくても、将来量子コンピュータの性能が向上した時点で解読を試みる攻撃が脅威と捉えられ始めています。

Store now, decrypt later攻撃※とは？

既存の暗号技術が安全だと考えられている間に、攻撃者が暗号化データを収集しておき、量子コンピュータの性能が向上した将来に解読を試みる攻撃。



新たな脅威： 量子コンピュータと、暗号解読のための量子アルゴリズム

- 量子コンピュータ上で暗号を破るための**量子アルゴリズム**は既に提案されています。
- 量子コンピュータの性能が向上した後に、それらの量子アルゴリズムが悪用されることが新しい脅威になりつつあります。

暗号の種類	現在主流の暗号方式	暗号解読のための量子アルゴリズム	量子アルゴリズムが解こうとする問題	暗号への脅威	望ましい対策
共通鍵暗号	AES	グローバーのアルゴリズム	データ探索問題	大きいが限定的	「鍵長の伸長」および「安全な暗号利用モードへの変更」
		サイモンのアルゴリズム	周期探索問題	大きいが限定的	
公開鍵暗号	RSA暗号	ショアのアルゴリズム	素因数分解	非常に大きい	PQCへの移行
	楕円曲線暗号	ショアのアルゴリズム	離散対数問題	非常に大きい	PQCへの移行
	耐量子計算機暗号 (PQC)	**現在、発見されていない**	-	現在無し	-

（参考）暗号アルゴリズムに対する量子コンピュータの影響

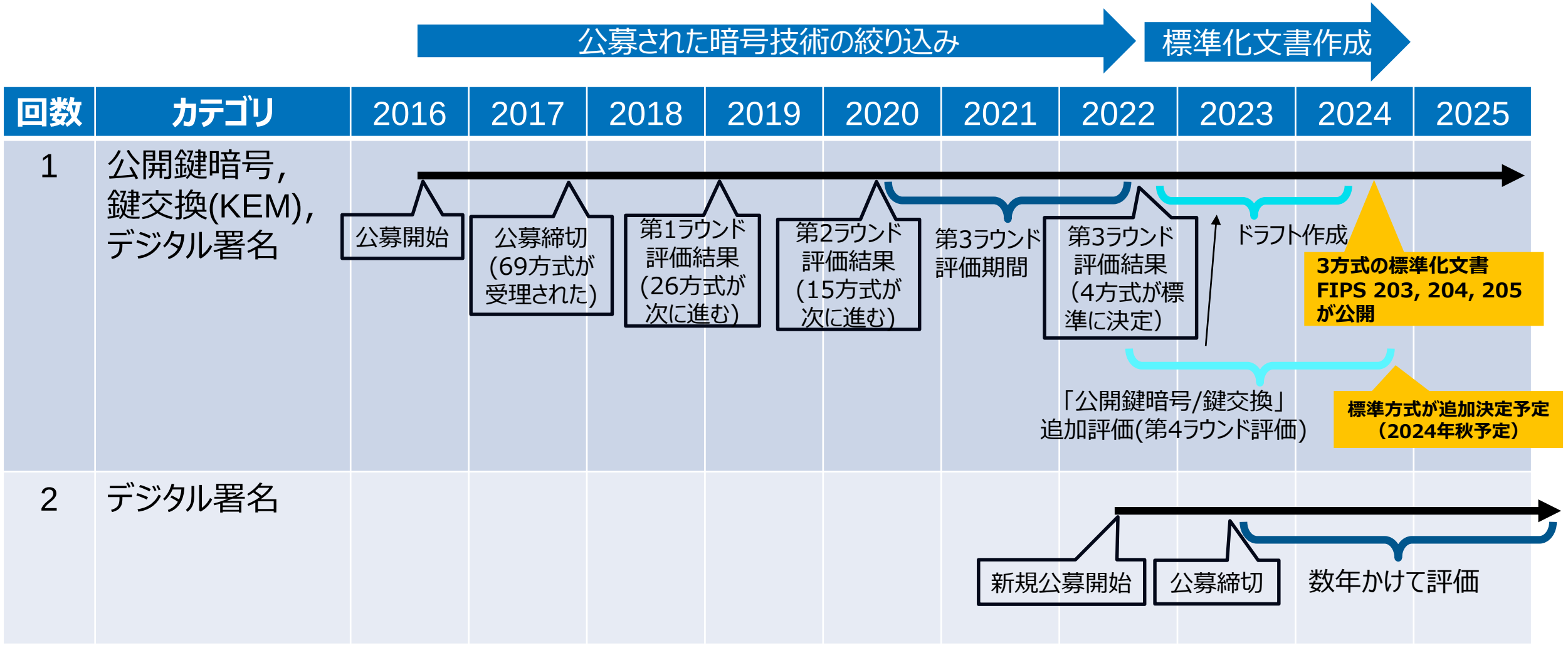
一般的なセキュリティ強度	安全性の分類	暗号系のタイプ	共通鍵暗号のタイプ	暗号アルゴリズム	ベースとなる数学上の困難な問題	用途	鍵長（公開鍵暗号では公開鍵長を記載）	ビットセキュリティ（古典コンピュータ上）	ビットセキュリティ（量子コンピュータ上）	暗号解析のための量子アルゴリズム	大規模量子コンピュータによる影響	量子耐性（またはPQC）
より高い	情報理論的安全性	共通鍵暗号	ストリーム暗号	ワンタイムパッド (OTP)	N/A	暗号化	N/A	N/A	N/A	N/A	影響なし	Yes
		N/A	N/A	(k, n)-閾値秘密分散	N/A	秘密分散	N/A	N/A	N/A	N/A	影響なし	Yes
より低い	計算量的安全性	共通鍵暗号	ブロック暗号	AES	N/A	暗号化	128, 192 bits	128, 192 bits	64, 96 bits	Groverのアルゴリズム、Simonのアルゴリズム	より長い鍵サイズが必要	No
							256 bits	256 bits	128 bits	Groverのアルゴリズム、Simonのアルゴリズム	安全	Yes
		公開鍵暗号	N/A	RSA	素因数分解	暗号化、鍵交換、署名	1024 bits	80 bits	~0 bits	Shorのアルゴリズム	もはや安全ではない	No
							2048 bits	112 bits	~0 bits	Shorのアルゴリズム	もはや安全ではない	No
				ECDSA, ECDH	楕円曲線上の離散対数問題	署名、鍵交換	256 bits	128 bits	~0 bits	Shorのアルゴリズム	もはや安全ではない	No
				DSA	有限体上の離散対数問題	署名	2048 bits	112 bits	~0 bits	Shorのアルゴリズム	もはや安全ではない	No
				CRYSTALS-KYBER	Module-LWE問題	暗号化、鍵交換	800, 1184, 1568 Bytes	128, 192, 256 bits	128, 192, 256 bits	まだ発見されていない	安全	Yes (PQC)
				CRYSTALS-Dilithium	Module-LWE問題	署名	1312, 1952, 2592 Bytes	128, 192, 256 bits	128, 192, 256 bits	まだ発見されていない	安全	Yes (PQC)
				FALCON	Learning with Errors (LWE) 問題	署名	897, 1793 Bytes	128, 256 bits	128, 256 bits	まだ発見されていない	安全	Yes (PQC)
				SPHINCS+	ハッシュ関数	署名	32, 48, 64 Bytes	128, 192, 256 bits	128, 192, 256 bits	まだ発見されていない	安全	Yes (PQC)

NISTレポート「NISTIR 8105, Report on Post-Quantum Cryptography」を基に株式会社NTTデータが加筆し作成。https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

赤字は128より小さい数字を表しており、128を量子耐性の閾値とする。

NISTの耐量子計算機暗号標準化タイムライン

米国NIST（国立標準技術研究所）は2016年からPQCの標準化活動を開始し、現在も標準化を継続しています。



PQC標準方式の選出

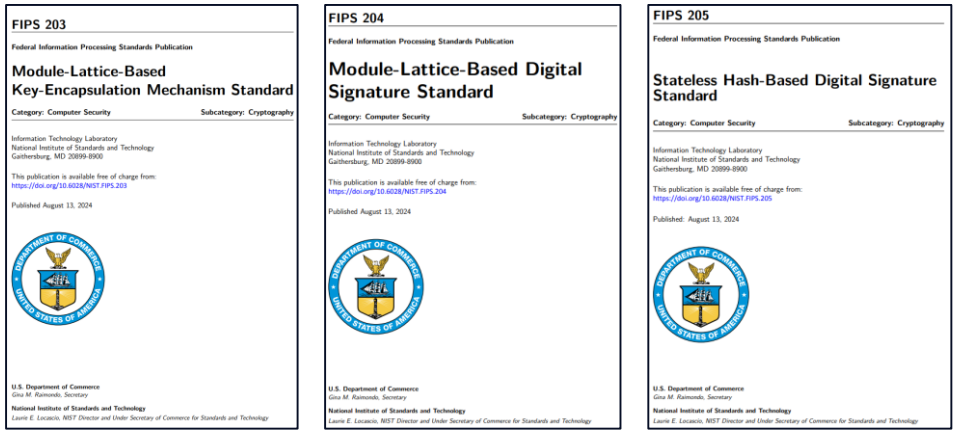
2022年7月、第3ラウンド評価の結果、公開鍵暗号または鍵交換(KEM)のカテゴリにおいて1方式、デジタル署名のカテゴリにおいて3方式、計4方式がPQC標準に選出されました。

	公開鍵暗号 / 鍵交換(KEM)	デジタル署名
標準方式として決定	CRYSTALS-KYBER	CRYSTALS-Dilithium FALCON SPHINCS+
第4ラウンド評価中	BIKE Classic McEliece HQC （※1）	-
追加公募による第1ラウンド評価中	-	**（符号ベース署名）** CROSS, Enhanced pqsigRM, FuLeeca, LESS, MEDS, Wave **（同種写像署名）** SQIsign **（格子ベース署名）** EagleSign, EHTv3 and EHTv4, HAETAE, HAWK, HuFu, Raccoon, SQUIRRELS **（MPC-in-the-Head署名）** Biscuit, MIRA, MiRitH, MQOM, PERK, RYDE, SDitH **（多変数署名）** 3WISE, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX **（対称ベース署名）** AIMer, Ascon-Sign, FAEST, SPHINCS-alpha **（その他の署名）** ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon, Xifrat1-Sign.I

（※1）公開鍵暗号 / 鍵交換(KEM) のカテゴリで「SIKE」も選定されたが、その直後の2022年7月、SIKEに攻撃が発見されたという論文が発表されたため、SIKEはPQC標準候補から外れた。

PQCの標準化ドキュメント

2024年8月13日、PQCに選出された4方式のうちの3方式に対し、
FIPS 203, 204, 205の標準化ドキュメントが公開されました。



カテゴリ	PQC標準選出時の名称	FIPS標準化時の名称	FIPS標準化ドキュメント
公開鍵暗号 / 鍵交換(KEM)	CRYSTALS-KYBER	**ML-KEM**	FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard https://csrc.nist.gov/pubs/fips/203/final
デジタル署名	CRYSTALS-Dilithium	**ML-DSA**	FIPS 204 Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/final
	SPHINCS+	**SLH-DSA**	FIPS 205 Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/final
	FALCON	FN-DSA（予定）	策定中

参考：
NIST, Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography
https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

WHITE HOUSE Report

2024年8月13日、White House からPQCに関するReportが公開されました。


THE WHITE HOUSE

MENU

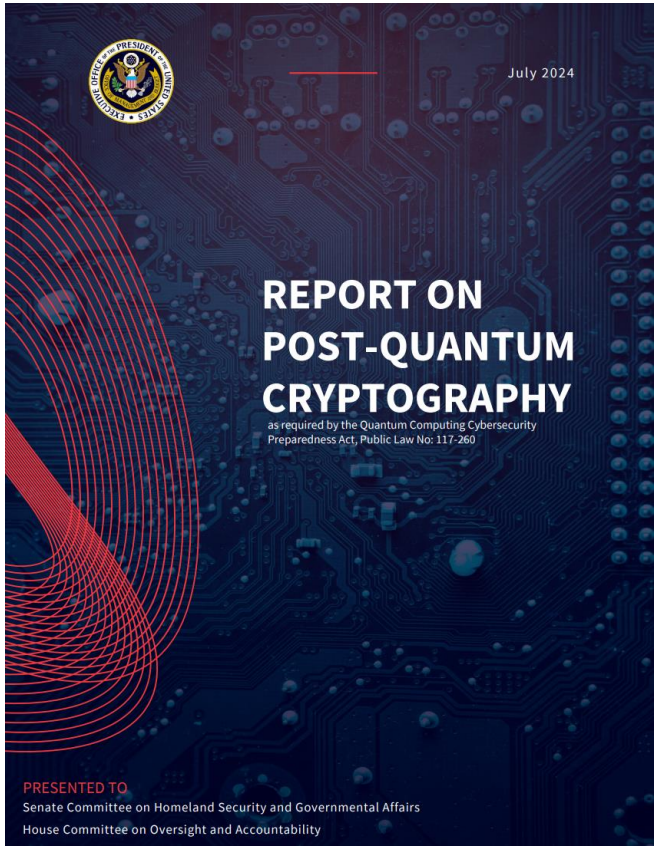
AUGUST 13, 2024

Fact Sheet: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future

ONCD ▸ BRIEFING ROOM ▸ PRESS RELEASE

August 13, 2024

The Biden-Harris Administration is committed to investing in science and technology innovation to solve future problems for our nation, generate jobs and new economic engines, and advance U.S. leadership around the world. While quantum information science (QIS) holds the potential to drive innovations across the American economy, from fields as diverse as materials science and



- Fact Sheet: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future (2024/08/13)
  - REPORT ON POST-QUANTUM CRYPTOGRAPHY

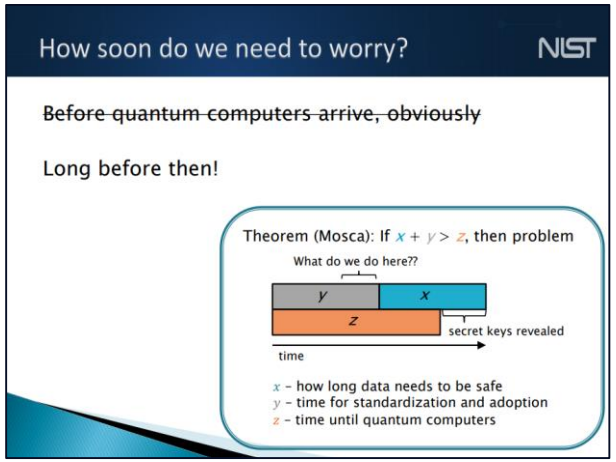
耐量子計算機暗号（PQC）への移行の緊急性の確認方法

米国NISTは、PQCへの移行の緊急性を直観的に理解するための「Moscaの定理」を紹介しています。

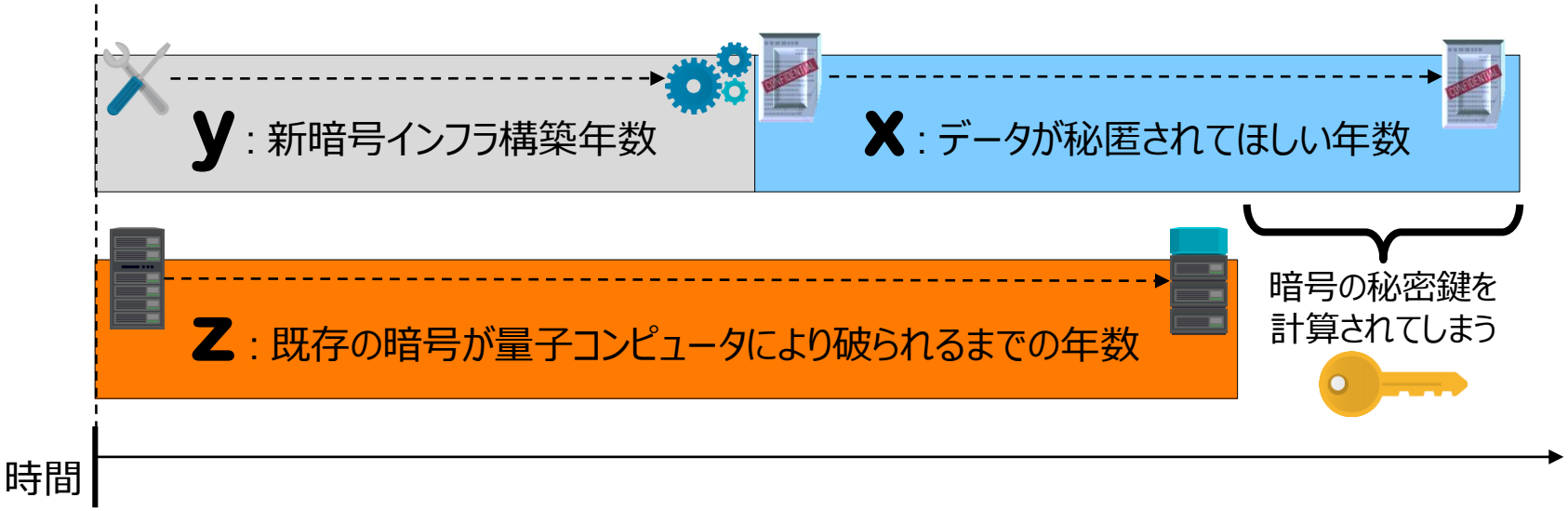
Moscaの定理：

x	その時点の暗号技術により、データが秘匿されていてほしい年数
y	量子コンピュータの攻撃に対し安全な暗号インフラの構築に必要な年数
z	既存の暗号を破る量子コンピュータの出現にかかる年数

のとき、**x＋y ＞ z** ならば、問題である。



https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

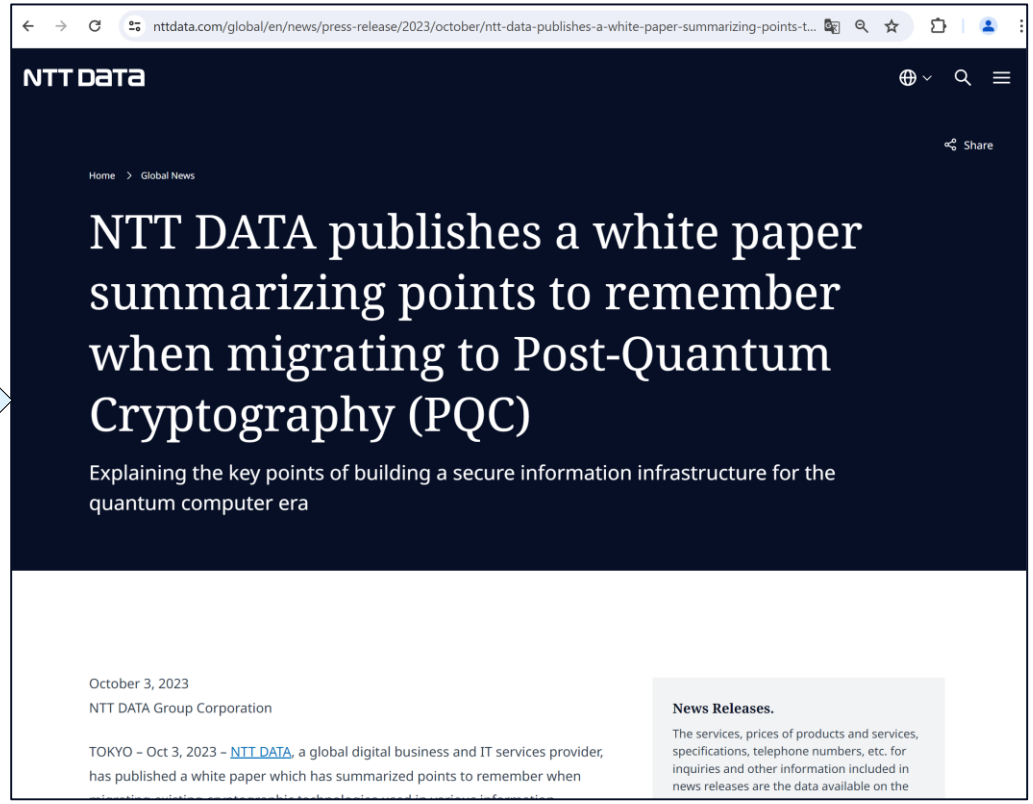


（例）
これまでのインフラ開発の経験から**y=20**年はかかると予測。行政の電子データ保存期間の制約から**x=50**年は秘匿されてほしい。RSA暗号を破る量子コンピュータは**z=30**年後に出現し普及すると予測。

すると、x+y = 50+20 > 30 (z) より問題！

PQCへの移行に関するホワイトペーパー

2023年10月、NTT DATAは、PQCへの移行に関するホワイトペーパー（日本語版および英語版）を公開しました。

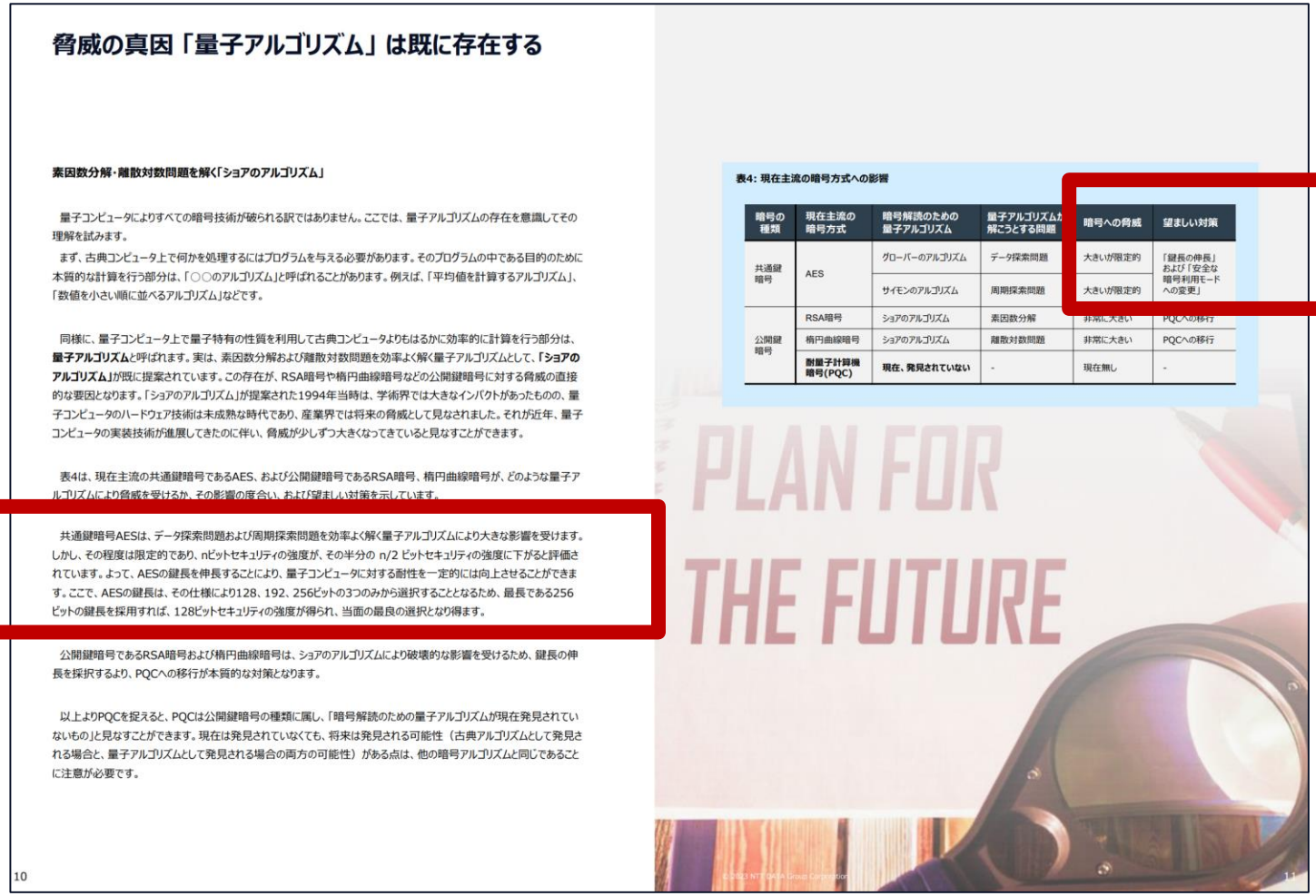


日本サイト
https://www.nttdata.com/global/ja/news/topics/2023/100301/

グローバルサイト
https://www.nttdata.com/global/en/news/press-release/2023/october/ntt-data-publishes-a-white-paper-summarizing-points-to-remember-when-migrating-to-pqc

ホワイトペーパーの特徴1：　共通鍵暗号の量子耐性に言及

共通鍵暗号では量子コンピュータによる脅威が公開鍵暗号ほどには大きくないことに関し、AESの例を用いて解説しております。



脅威の真因「量子アルゴリズム」は既に存在する

素因数分解・離散対数問題を解く「ショアのアルゴリズム」

量子コンピュータによりすべての暗号技術が破られる訳ではありません。ここでは、量子アルゴリズムの存在を意識してその理解を試みます。

まず、古典コンピュータ上で何かを処理するにはプログラムを与える必要があります。そのプログラムの中である目的のために本質的な計算を行う部分は、「○○のアルゴリズム」と呼ばれることがあります。例えば、「平均値を計算するアルゴリズム」、「数値を小さい順に並べるアルゴリズム」などです。

同様に、量子コンピュータ上で量子特有の性質を利用して古典コンピュータよりもはるかに効率的に計算を行う部分は、**量子アルゴリズム**と呼ばれます。実は、素因数分解および離散対数問題を効率よく解く量子アルゴリズムとして、**「ショアのアルゴリズム」**が既に提案されています。この存在が、RSA暗号や楕円曲線暗号などの公開鍵暗号に対する脅威の直接的な要因となります。「ショアのアルゴリズム」が提案された1994年当時は、学術界では大きなインパクトがあったものの、量子コンピュータのハードウェア技術は未成熟な時代であり、産業界では将来の脅威として見なされました。それが近年、量子コンピュータの実装技術が進展してきたのに伴い、脅威が少しずつ大きくなってきていると見なすことができます。

表4は、現在主流の共通鍵暗号であるAES、および公開鍵暗号であるRSA暗号、楕円曲線暗号が、どのような量子アルゴリズムにより脅威を受けるか、その影響の度合い、および望ましい対策を示しています。

共通鍵暗号AESは、データ探索問題および周期探索問題を効率よく解く量子アルゴリズムにより大きな影響を受けます。しかし、その程度は限定的であり、nビットセキュリティの強度が、その半分の n/2 ビットセキュリティの強度に下がると評価されています。よって、AESの鍵長を伸長することにより、量子コンピュータに対する耐性を一定的には向上させることができます。ここで、AESの鍵長は、その仕様により128、192、256ビットの3つのみから選択することとなるため、最長である256ビットの鍵長を採用すれば、128ビットセキュリティの強度が得られ、当面の最良の選択となり得ます。

公開鍵暗号であるRSA暗号および楕円曲線暗号は、ショアのアルゴリズムにより破壊的な影響を受けるため、鍵長の伸長を採択するより、PQCへの移行が本質的な対策となります。

以上よりPQCを捉えると、PQCは公開鍵暗号の種類に属し、「暗号解読のための量子アルゴリズムが現在発見されていないもの」と見なすことができます。現在は発見されていなくても、将来は発見される可能性（古典アルゴリズムとして発見される場合と、量子アルゴリズムとして発見される場合の両方の可能性）がある点は、他の暗号アルゴリズムと同じであることに注意が必要です。

10

表4: 現在主流の暗号方式への影響

暗号の種類	現在主流の暗号方式	暗号解読のための量子アルゴリズム	量子アルゴリズムが解こうとする問題	暗号への脅威	望ましい対策
共通鍵暗号	AES	グローバーのアルゴリズム	データ探索問題	大きいが限定的	「鍵長の伸長」および「安全な暗号利用モードへの変更」
		サイモンのアルゴリズム	周期探索問題	大きいが限定的	
公開鍵暗号	RSA暗号	ショアのアルゴリズム	素因数分解	非常に大きい	PQCへの移行
	楕円曲線暗号	ショアのアルゴリズム	離散対数問題	非常に大きい	PQCへの移行
	耐量子計算機暗号(PQC)	**現在、発見されていない**	-	現在無し	-

https://www.nttdata.com/global/ja/-/media/nttdataglobal-ja/files/news/topics/2023/100301/100301-01.pdf?rev=b614a1eba07f4544981c45ce0065a78e

ホワイトペーパーの特徴2：　望ましいPQCアルゴリズム選定指針に言及

今後PQCに移行する際に暗号アルゴリズムを決定する場面では、安全性の側面から、**格子暗号に属する暗号アルゴリズムを選択肢の一つに挙げておくことは望ましい**という意見を含めさせていただいております。

PQC標準の候補では格子暗号が多数

PQC公募暗号で多数を占める格子暗号

PQC標準化公募に受理された69個の暗号方式の分布を分析すると、数学における「格子（lattice）」に関連する様々な困難な問題（本書ではそれらを総称して「格子問題」と呼びます）を安全性の根拠とする方式が25個あり、最も多数でした（図10）。実際に、PQC標準方式に決定された4方式の内、「CRYSTALS-KYBER」、「CRYSTALS-Dilithium」、および「FALCON」の3方式は、格子問題を安全性の根拠とする**格子暗号**に属します。

図10: PQC標準化の第1ラウンド評価に進んだ69方式

● 応募された暗号方式

16

第2、第3ラウンドの各評価に進んだ方式においても、格子暗号が多い傾向は変わりませんでした（図11）。

この事象から、世界における格子暗号の研究者が多数存在することを読み取ることができます。ある特定の領域の研究者が多いことは、その領域から様々な暗号技術が考案されると同時に、それらの安全性を評価する研究者も多数存在することを期待できるため、その安全性に一定の安心感があると言えます。実際に、素因数分解・離散対数問題は多くの研究者により長年研究され、解くことが困難であることが証明されてきたため、それらを安全性の根拠とするRSA暗号・楕円曲線暗号などの安全性が信頼されてきたと言えます。

したがって、今後PQCに移行する際に暗号アルゴリズムを決定する場面では、安全性の側面から、格子暗号に属する暗号アルゴリズムを選択肢の一つに挙げておくことは望ましいと考えることができます。

図11: NIST PQC標準化第2ラウンド評価の結果（第3ラウンド評価に進んだ15方式）

括弧内は個数を表す

		格子暗号（7件）	符号暗号（3件）	多変数多項式暗号（2件）	ハッシュ関数署名（1件）	同種写像暗号（1件）	その他（1件）
公開鍵暗号および鍵交換（KEM）	最終候補	(3): CRYSTALS-KYBER, NTRU (NTRU-HRSS-KEM + NTRUEncrypt), SABER	(1): Classic McEliece	-	-	-	-
	代替候補	(2): Frodo-KEM, NTRU Prime	(2): BIKE, HQC	-	-	(1): SIKE	-
デジタル署名	最終候補	(2): CRYSTALS-Dilithium, FALCON	-	(1): Rainbow	-	-	-
	代替候補	-	-	(1): GeMSS	(1): SPHINCS+	-	(1): Picnic

17

https://www.nttdata.com/global/ja/-/media/nttdataglobal-ja/files/news/topics/2023/100301/100301-01.pdf?rev=b614a1eba07f4544981c45ce0065a78e

ホワイトペーパーの特徴3： PQC移行時の7つの留意点

PQCへの移行時の留意点を７つ示しています。これらはPQCへの移行計画を策定する際に考慮すべき点となります。

#	PQCへの移行時の留意点
1	鍵データ・暗号化データ・署名データのサイズが大きくなる可能性
2	処理速度が遅くなる可能性
3	暗号アジリティ（暗号の俊敏性）を高める設計・実装を取り入れる
4	暗号化データをシステムに保存している場合、再暗号化の検討が必要
5	TLSのハードウェアを使用している場合、調達は間に合うか？
6	NIST, SOG-IS, CRYPTREC等が公開する情報の継続的な収集
7	クラウドサービスプロバイダが提供するPQC機能を把握する

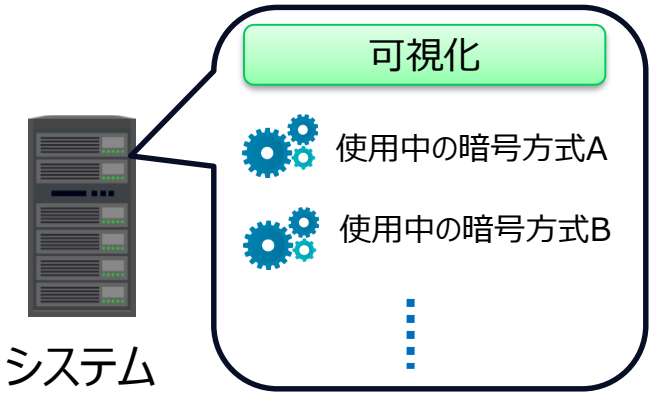
https://www.nttdata.com/global/ja/-/media/nttdataglobal-ja/files/news/topics/2023/100301/100301-01.pdf?rev=b614a1eba07f4544981c45ce0065a78e

（参考）留意点3: Crypto-Agility（暗号の俊敏性）を高める設計・実装を取り入れる

- PQCの各アルゴリズムは、従来のRSA暗号等に比べ**安全性評価の歴史が浅く、将来、攻撃が発見される可能性**がある。
  - 【対策例1】 システムで使用されている暗号方式を可視化し、**別の暗号方式に容易に移行できるように設計・実装する**
  - 【対策例2】 TLSでは**ハイブリッドモード**の採用を検討する。

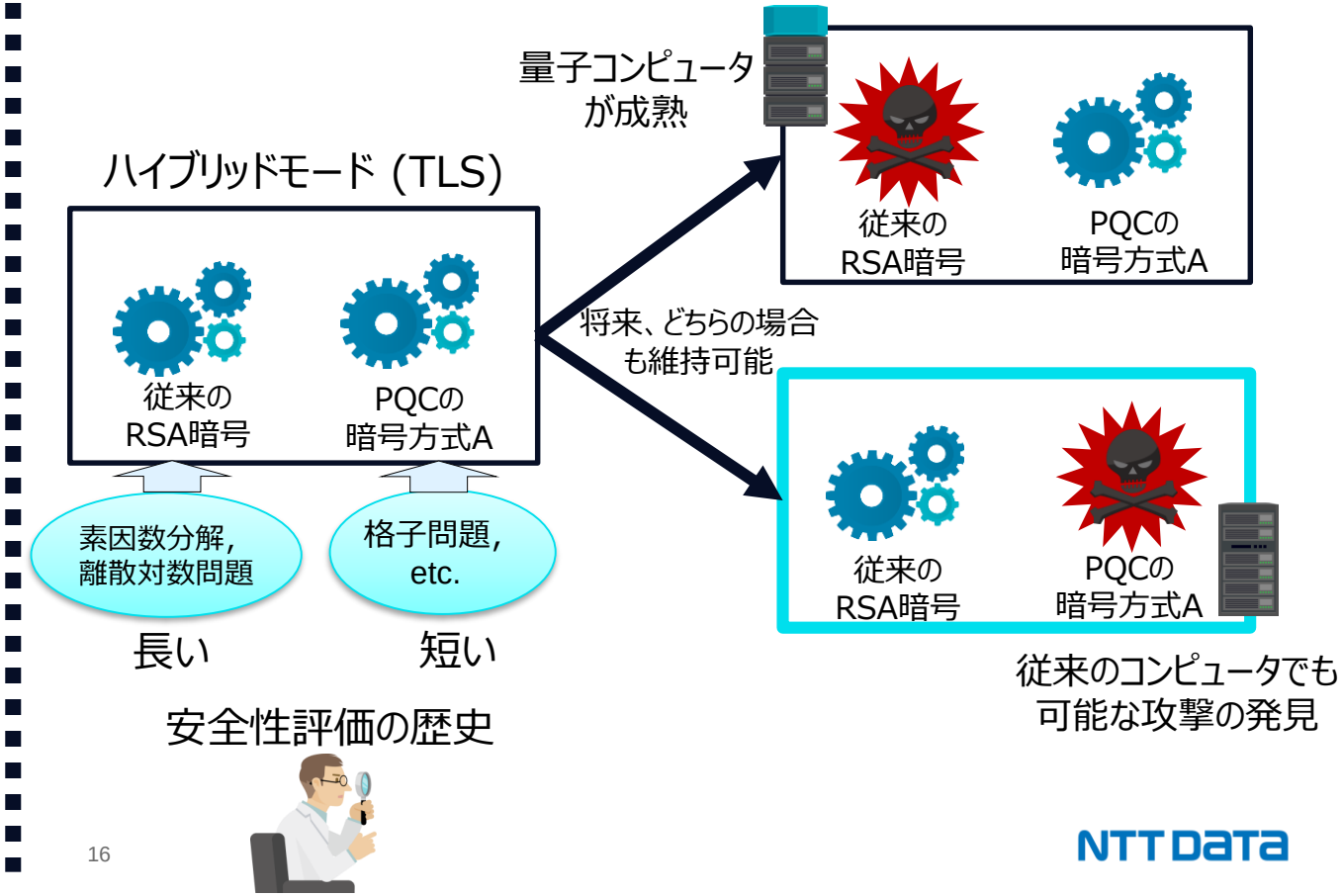
対策例1

A) システム内で使用されている暗号方式の目録（暗号インベントリ）を作成・管理



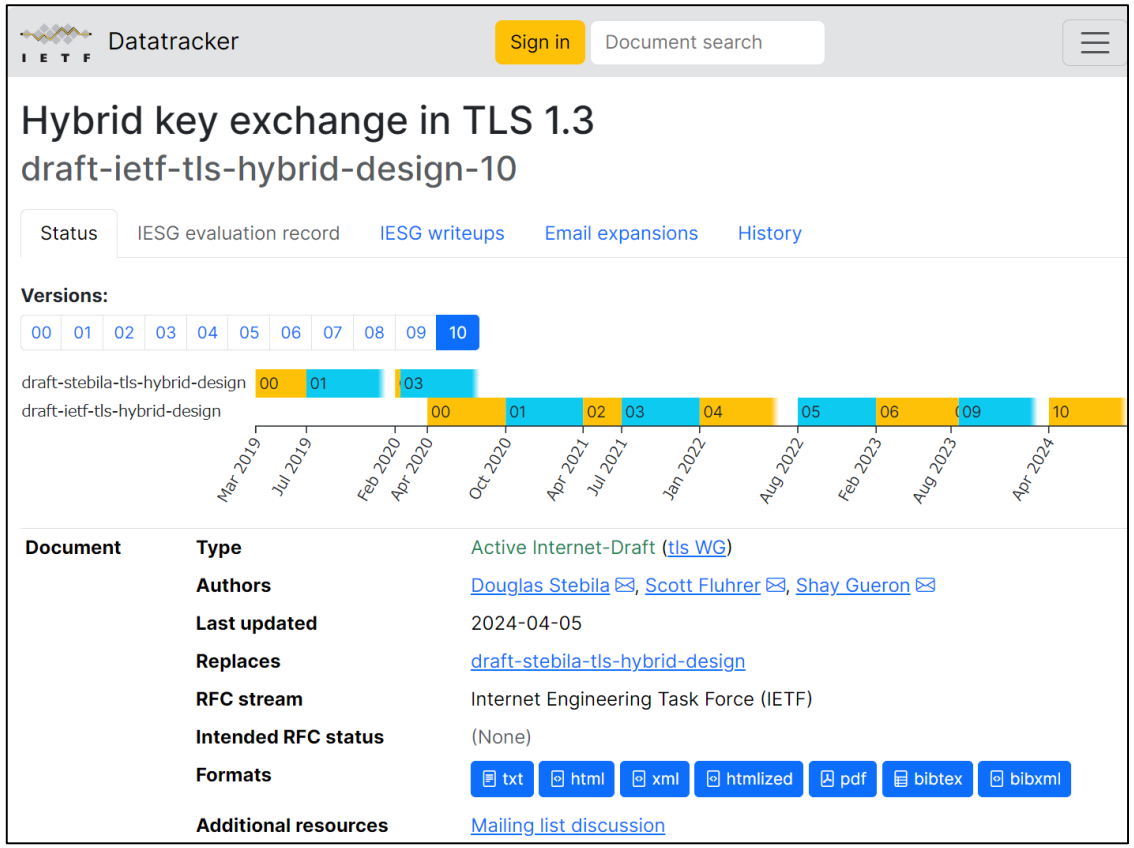
B) 設定の変更のみで自動的に移行できるように実装

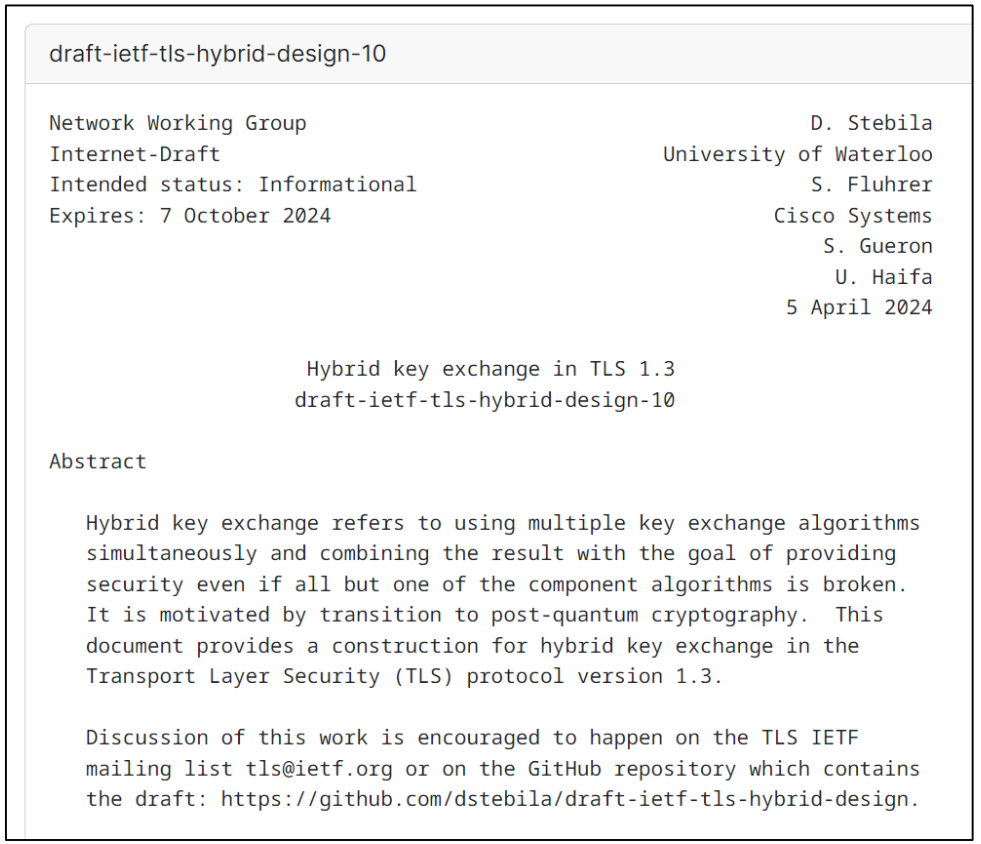
対策例2



IETFによる標準化： TLS 1.3 の鍵交換にハイブリッドモードを適用

- **ハイブリッドモード**とは、「既存の暗号」と「PQC」の両方を使用できるように情報システムを整備し、どちらか一方が危殆化しても、もう一方で維持させることができるようにする考え方
- IETFは既存のTLS 1.3の鍵交換の仕様に対しハイブリッドモードを追加することを検討しており、そのドラフトを公開している。





draft-ietf-tls-hybrid-design-10

Network Working Group — D. Stebila
Internet-Draft — University of Waterloo
Intended status: Informational — S. Fluhrer
Expires: 7 October 2024 — Cisco Systems
S. Gueron
U. Haifa
5 April 2024

Hybrid key exchange in TLS 1.3
draft-ietf-tls-hybrid-design-10

Abstract

Hybrid key exchange refers to using multiple key exchange algorithms simultaneously and combining the result with the goal of providing security even if all but one of the component algorithms is broken. It is motivated by transition to post-quantum cryptography. This document provides a construction for hybrid key exchange in the Transport Layer Security (TLS) protocol version 1.3.

Discussion of this work is encouraged to happen on the TLS IETF mailing list tls@ietf.org or on the GitHub repository which contains the draft: https://github.com/dstebila/draft-ietf-tls-hybrid-design.

Hybrid key exchange in TLS 1.3, draft-ietf-tls-hybrid-design-10
https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

2

PQC移行に向けたサービス提供に関する状況

1. PQC移行コンサルティング

2. クリプト・アジリティ

3. クライアント証明書(PQC)

4. PQC勉強会、人材育成

PQCへの移行プロセスに沿ったコンサルティング

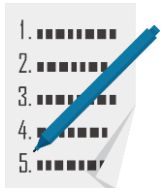
NTT DATAでは、**PQCへの移行プロセス**を定義し、同プロセスに沿ったコンサルティングサービスを検討しております。

1 現状把握

暗号化された情報や場所の特定

- 通信路上の暗号化終端箇所
- 情報の保存場所
- 外部通信の有無
- 暗号アルゴリズムと鍵長
- 共通鍵暗号の利用モード
- 移行に伴う影響の調査
  - ✓ データサイズ
  - ✓ スピード　等
- その他

2 優先順位付け



移行の優先順位付けを実施

- 優先順位付けを行う際は以下を念頭に検討する。
  - ✓ 情報の重要性
  - ✓ 暗号化された情報を保存すべき期間
  - ✓ 法令、基準

3 移行開始時期の検討

ステップ1, 2の結果から移行要否、移行を開始する時期を検討

- 移行要否
- Store Now, Decrypt Later攻撃の影響評価
- TLS通信に用いる暗号アルゴリズムの切り替え時期
- ロードバランサーの調達時期
- ガントチャートの作成
- 移行イメージのすり合わせ

4 移行方法の検討

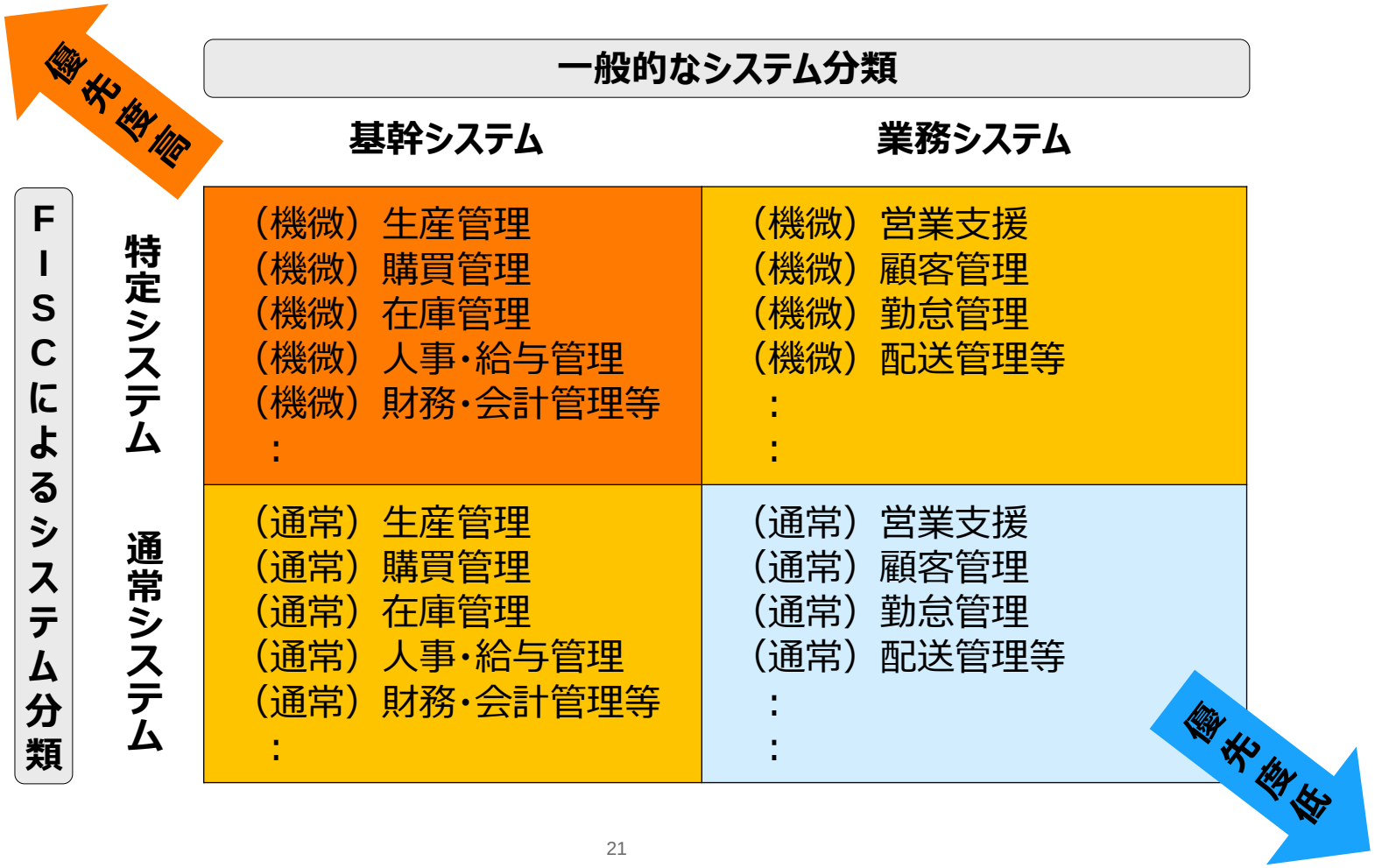
耐量子計算機暗号への移行方法を検討

- ハイブリットモード (TLS)
  - ✓ 従来のRSA暗号と耐量子計算機暗号の両方を維持する。どちらかの暗号に攻撃があっても安全を保証できる。
- 耐量子計算機暗号への完全移行

例：　PQCへの移行プロセス「①現状把握」の進め方

- PQCへの移行要否を検討すべき対象システムを抽出するには、**お客様ごとに様々な抽出方法が考えられます。**
- 一例として、金融分野では、「基幹／業務」のような一般的なシステムの分類、およびFISC安全対策基準における「リスクベースアプローチ」において定義された「特定／通常」のシステム分類を掛け合わせた4象限で優先度を検討する方法が考えられます。

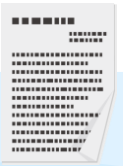
例：



PQC移行プロセス「①現状把握」の成果物イメージ

「システム管理者へのインタビュー」、「設計書の確認」、「NW機器の設定の確認」、「サーバ証明書の確認」、「クライアント証明書の確認」等の調査（ツールを利用できる部分に対してはツールを利用）により、暗号インベントリを完成させます。

1 現状把握



2 優先順位付け

暗号インベントリ

システム名	暗号化対象データ	暗号使用箇所	機密性	保存期限	暗号アルゴリズム種別	暗号アルゴリズム	鍵長	暗号利用モード	PQC移行の必要性
システム1	認証情報	サーバA、ストレージ	高	N1年	共通鍵暗号	AES	256ビット	GCM	不要
システム1	決済情報	サーバB、TLS	高	N2年	公開鍵暗号	RSA	1024ビット	ー	必要
システム2	セッション鍵	ロードバランサ、TLS	高	N3年	公開鍵暗号	RSA	2048ビット	ー	必要
システム3	:	:	中		:	:	:	:	:
:	:	:			:	:	:	:	:
:	:	:			:	:	:	:	:

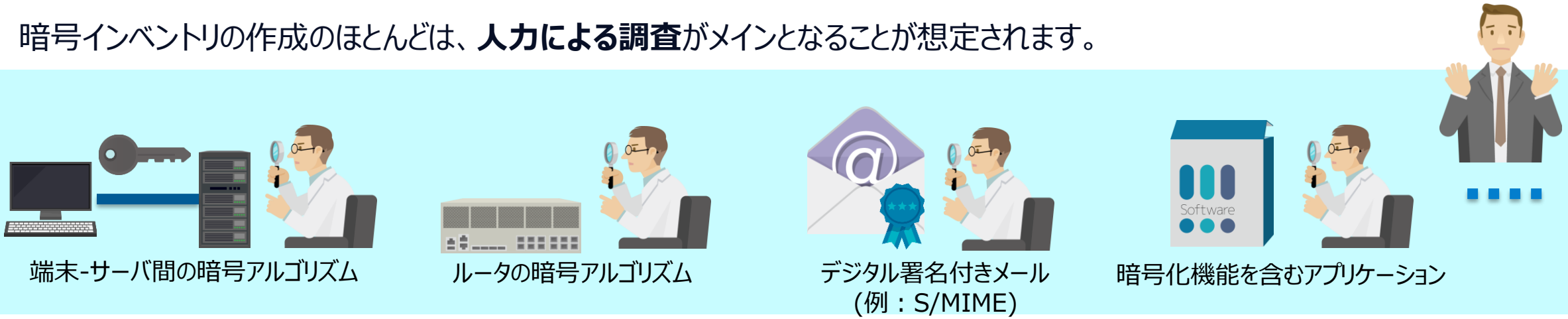
○○システムでは、共通鍵暗号AESの鍵長を256ビットに伸長することにより対処しましょう。

○○システムは、次期更改のタイミングでPQCに移行すべきでは？

機密性が高いデータを扱うシステムでは、優先度を上げよう。

暗号インベントリ作成・維持の自動化可能性

- 暗号インベントリの作成のほとんどは、**人力による調査**がメインとなることが想定されます。



- しかし、**サーバ証明書・クライアント証明書に用いられるデジタル署名アルゴリズムの調査**においては、ツールによるネットワークスキャンまたは証明書発行履歴管理ツールにより、自動化できる可能性があります。

Crypto-Agilityに関する支援提供の検討状況

- NEDO様の研究開発事業「経済安全保障重要技術育成プログラム（略称：K Program）／ハイブリッドクラウド利用基盤技術の開発／強固な鍵管理によるデータセキュリティ技術（鍵管理ソフトウェア技術）」（期間：2023年6月～2026年3月）において、「耐量子計算機暗号（PQC）実装技術」に関する研究開発を実施しております。

- その中で、暗号アジリティの一つの実現形態である**「TLS 1.3 ハイブリッドモード」**（※1）の機能を具備する暗号ライブラリを開発する予定でおります。

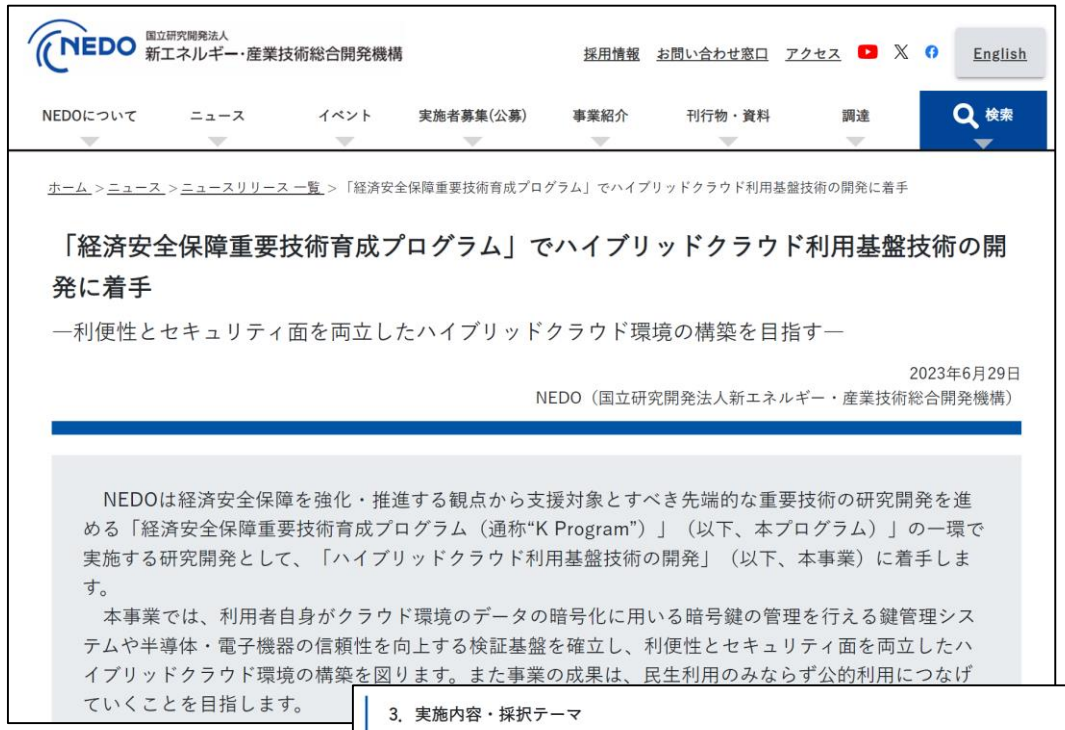
- ３か年の研究開発終了後、同暗号ライブラリは、弊社が提供するクラウドサービスにおける鍵管理サービスにおいて、セキュアな鍵配送機能に活用される予定でおります。

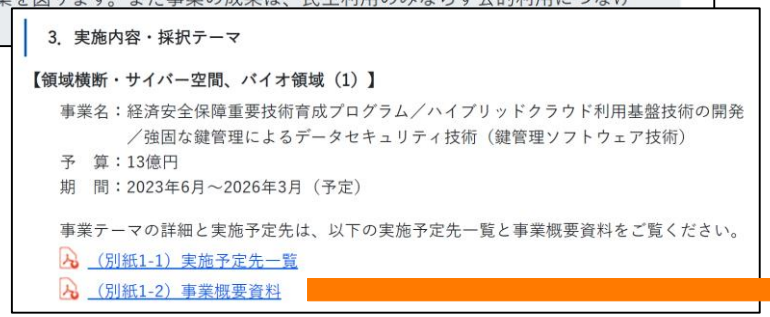
- 本研究開発で得られるノウハウを、様々なお客様案件に適用していくことを検討しております。

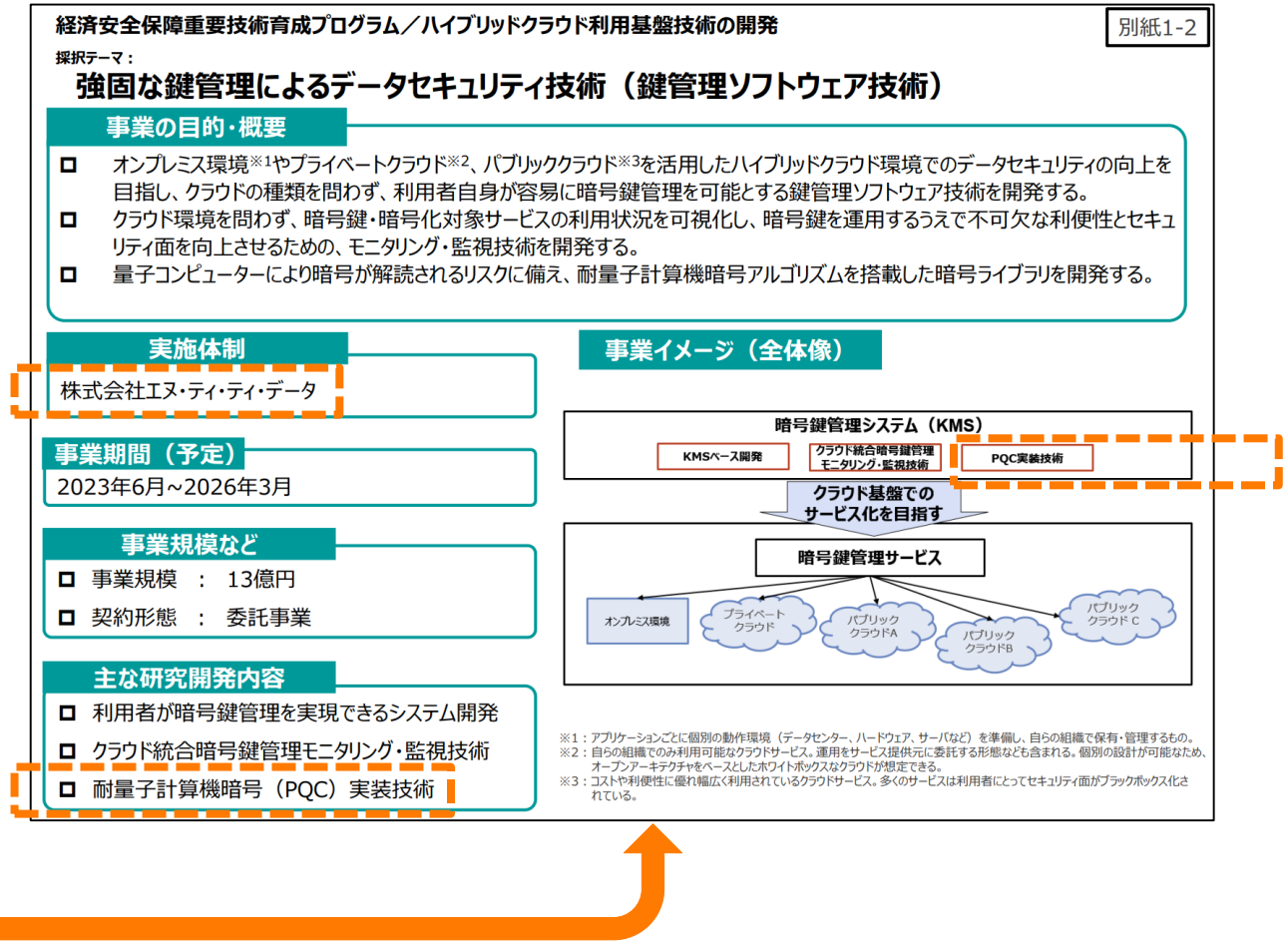
※1 参考記事：NTTデータ 技術ブログ DATA INSIGHT:「クラウドでの鍵管理の課題と耐量子計算機暗号の導入」
https://www.nttdata.com/jp/ja/trends/data-insight/2024/0619/

Crypto-Agility: NEDO様研究開発

NEDO様の研究開発事業において、「耐量子計算機暗号（PQC）実装技術」に関する研究開発を実施しております。



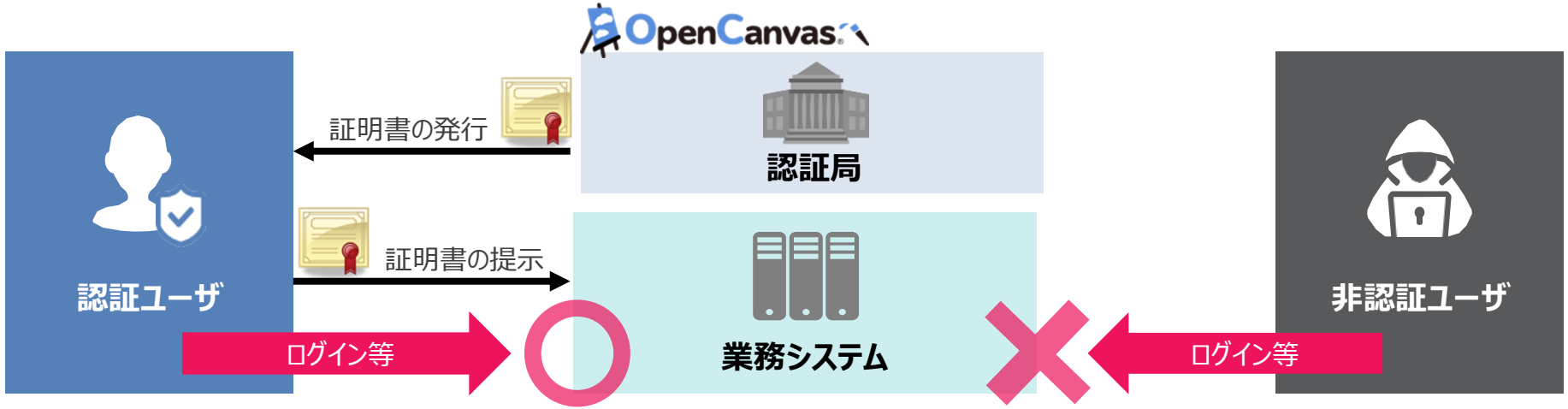




- 図の出典：NEDO,「経済安全保障重要技術育成プログラム」でハイブリッドクラウド利用基盤技術の開発に着手 https://www.nedo.go.jp/news/press/AA5_101668.html
- 参考記事：NTTデータ 技術ブログ DATA INSIGHT:「クラウドでの鍵管理の課題と耐量子計算機暗号の導入」https://www.nttdata.com/jp/ja/trends/data-insight/2024/0619/

（将来予定）　クライアント証明書サービスのPQC対応

NTTデータ　e-ビジネス事業部では、クライアント証明書サービス（※1）を提供しており、将来的にPQCアルゴリズムに対応するクライアント証明書をご提供できるよう、社内検証を計画しております。

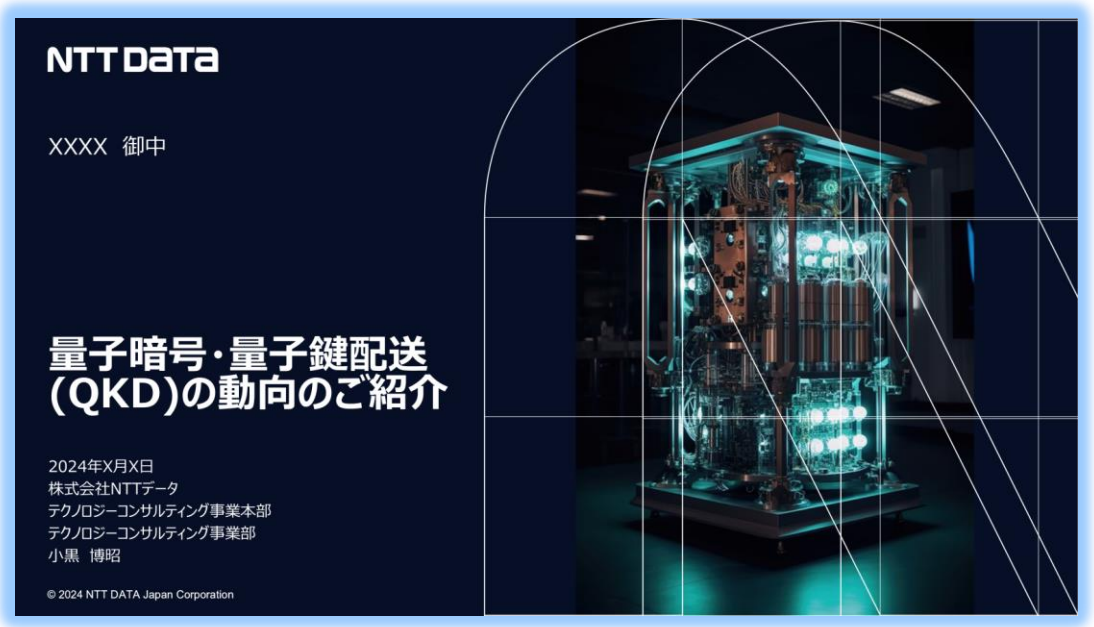


PQC対応認証局によるクライアント証明書の製品化に向けた技術検証等の計画を現在策定中で、2025年度着手予定。
金融機関をはじめとした様々なお客様の事業及び各業界のプラットフォームを支えるべく、
最先端のセキュリティに素早く追従する認証局サービスの提供を目指しております。

※1 参考：
・NTTデータ　ニュース「OpenCanvas クライアント証明書」を2022年3月から提供開始
https://www.nttdata.com/global/ja/news/services_info/2021/071900/
・NTT DATA PR,「外部アクセスからのセキュリティ強化！「OpenCanvas クライアント証明書」」
https://www.youtube.com/watch?v=PWtH4clkgHo

PQC勉強会、人材育成

NTT DATAでは、お客様向けに「耐量子計算機暗号（PQC）の動向」に関する勉強会を開催させていただいております。
PQCとは異なる概念「量子暗号/量子鍵配送（QKD）の動向」に関する勉強会もご要望に応じてセットで開催しております。



ディスクレーマー

本資料は信頼できると考えられる各種データに基づいて作成されていますが、当社はその正確性、完全性を保証するものではありません。ここに示したすべての内容は、当社の現時点での判断を示しているに過ぎません。また、本資料に関連して生じた一切の損害については、当社は責任を負いません。