第397回　NRIメディアフォーラム

耐量子計算機暗号（PQC）の現状と今後

～標準化ならびに国内外の動向と、企業が取るべき対応方針～

NRIセキュアテクノロジーズ株式会社
マネジメントコンサルティング事業本部
決済セキュリティコンサルティング部

エキスパートセキュリティコンサルタント　高木 裕紀
シニアセキュリティコンサルタント　平山 裕貴

2025年9月9日

NRIセキュアテクノロジーズ
NRI SecureTechnologies

Envision the value,
Empower the change

01 量子コンピュータの脅威と耐量子計算機暗号（PQC）

02 PQCへの移行に向けた国内外のタイムライン

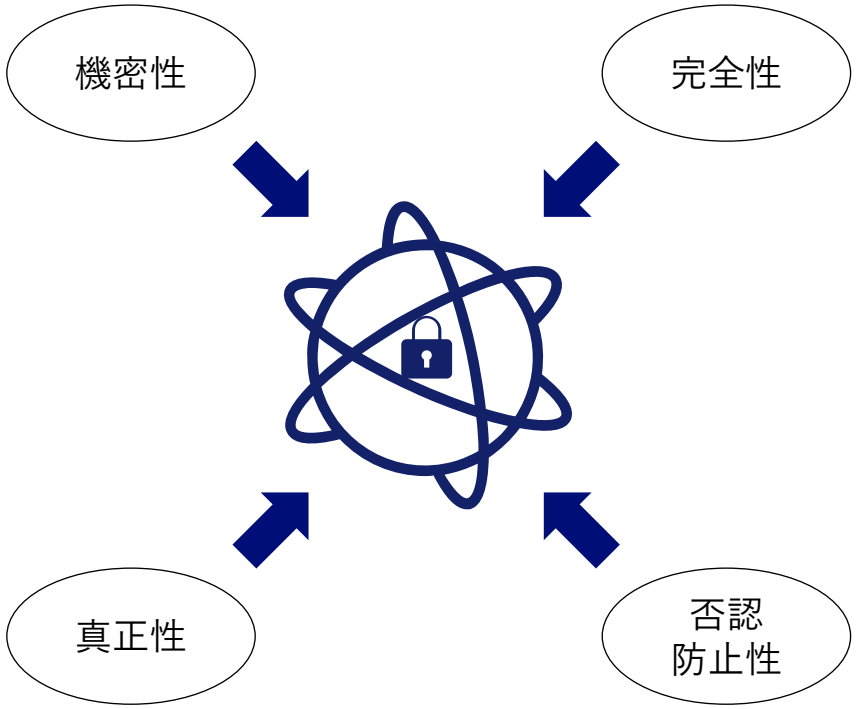
03 PQC移行の進め方と留意事項

1. 量子コンピュータの脅威と耐量子計算機暗号（PQC）

デジタル社会を支える暗号技術

安全安心なデジタル社会を実現するために、暗号技術が重要な役割を果たしている。

暗号技術の役割の例

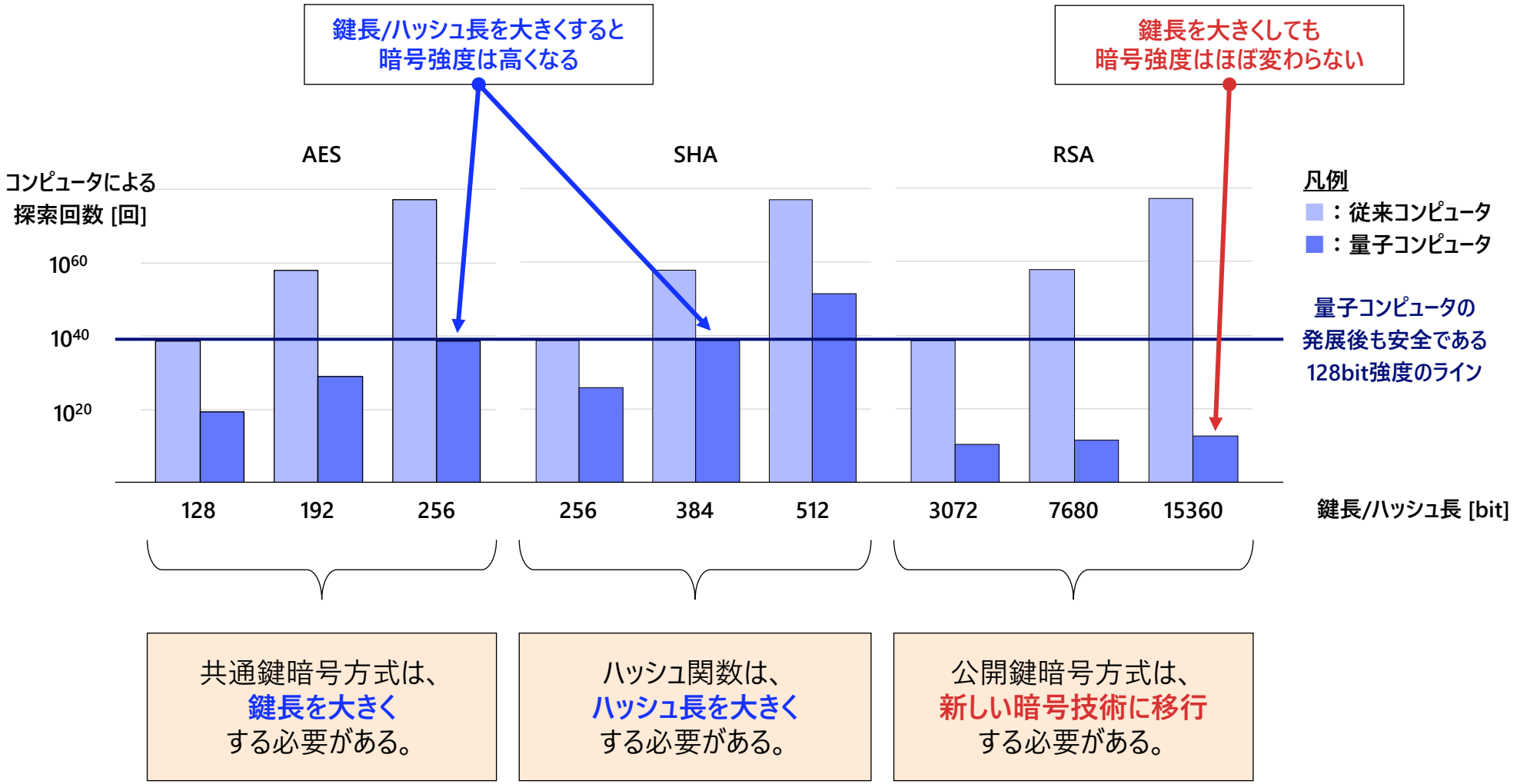


暗号技術の種類

種類	用途例	具体例
共通鍵暗号方式	• 通信やデータの秘匿	• AES • 3DES
公開鍵暗号方式	• 共通鍵の配送 • デジタル署名	• RSA • ECDSA
ハッシュ関数	• メッセージ認証（改ざん検知） • デジタル署名	• SHA

量子コンピュータ（Cryptographically relevant quantum computer｜CRQC）が及ぼす従来の暗号技術への影響

量子コンピュータの実用化により、従来の暗号技術が将来的に容易に破られる可能性がある。特に公開鍵暗号方式は、新しい暗号技術に移行することが求められる。



耐量子計算機暗号（Post-Quantum Cryptography｜PQC）とは

量子コンピュータによって暗号が解読されるリスクに対抗するための暗号技術。2025年8月時点では、新たに5種類のアルゴリズムがFIPS標準※となることが確定。

(※) Federal Information Processing Standardsの略称で、米国の国立標準技術研究所（NIST）が策定する情報処理に関する標準規格。

目的	名称	方式	FIPS標準
鍵交換	ML-KEM （CRYSTALS-Kyber）	格子	FIPS 203
	HQC	符号	未定
デジタル署名	ML-DSA （CRYSTALS-Dilithium）	格子	FIPS 204
	SLH-DSA （Sphincs+）	ハッシュ	FIPS 205
	FN-DSA （FALCON）	格子	FIPS 206 （策定中）

※現在も、さらなる軽量化や実装効率の向上などを目的として、追加第1ラウンドおよび第2ラウンドにおける候補アルゴリズムの評価が継続的に行われている。

量子コンピュータによる脅威シナリオ

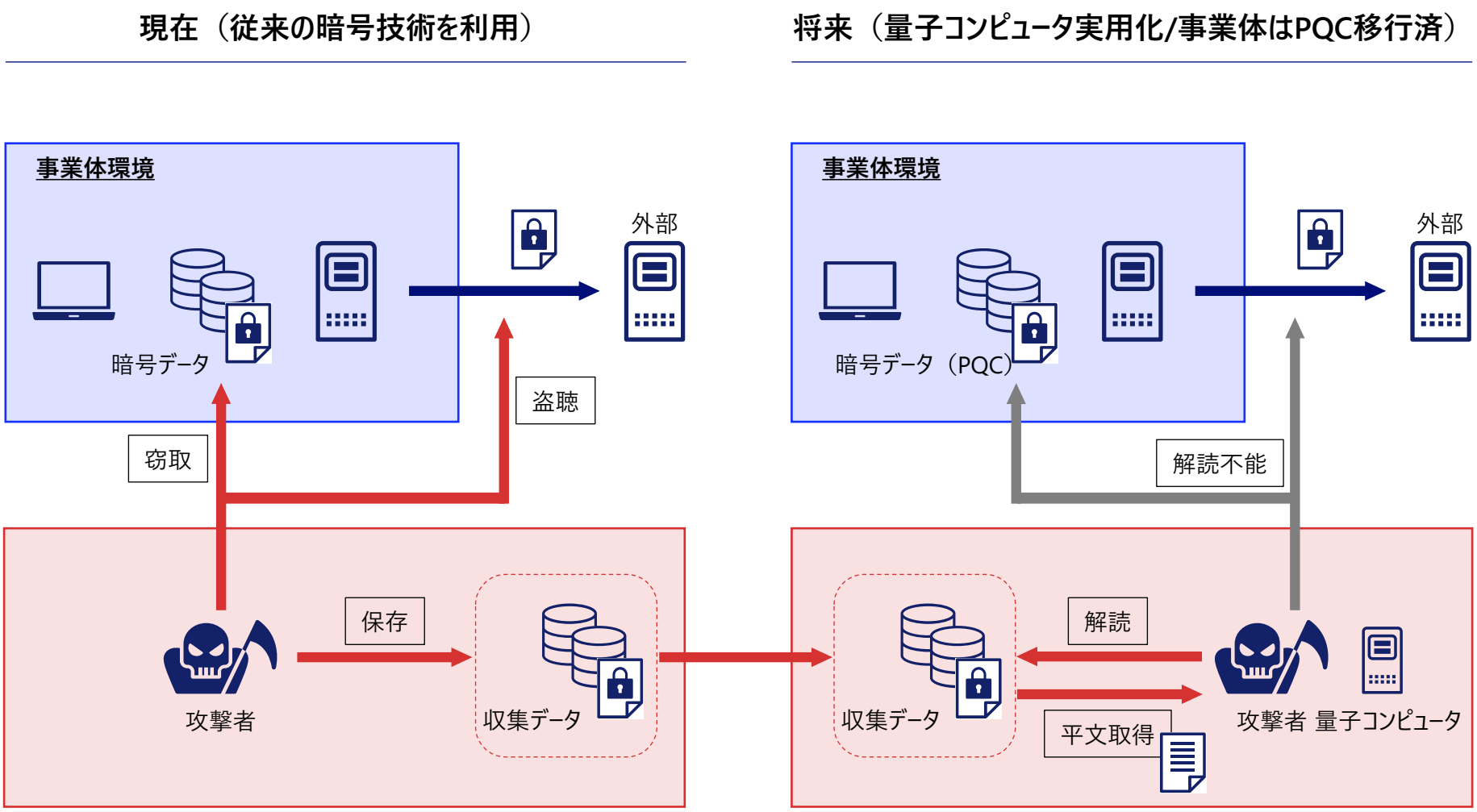
機密情報への不正アクセスや、データ・ソフトウェアの改ざんが発生する可能性がある。

リスク名称	リスク概要
ホールセール決済システムの認証の脆弱化（Risk 2）	ホールセール決済システムの認証は、公開鍵暗号に強く依存しているため、CRQCの攻撃で**合法的な取引を模倣した不正決済を実行される可能性**がある。
銀行間システムのインターフェースの侵害（Risk 3）	CRQCによる攻撃と同時にインターフェースの脆弱性が悪用される対象になる可能性が高まっており、複数銀行の機密性の高い**金融データや顧客情報、取引記録に不正アクセスされる可能性**がある。
分散型台帳技術（DLT）を基にした金融商品の侵害（Risk 4）	CRQCによって、基盤である初期のブロック（ジェネシスブロック）の内容が後から変更されると、その後のブロックの完全性が崩れ、**DLTの不変性と透明性を損なう可能性**がある。
ソフトウェアの完全性における脆弱化（Risk 7）	デジタル署名はソフトウェアとファームウェアの正当性の検証の基盤となっている。これらの署名は、公開鍵暗号アルゴリズムに依存しており、脆弱性を突いた攻撃により**ソフトウェアやファームウェアが改変され、それが組み込まれた重要なシステムに混乱をもたらす可能性**がある。
金融取引記録の改ざん（Risk 8 企業固有の台帳）	企業の内部情報システムに保存されているデジタル署名付与済の金融取引記録は、CRQCによるデータの改ざんにより、**資産所有権の書き換え、不正な取引の実行、取引履歴の変更等、取引記録（台帳）が保証する正確性と透明性を損なう可能性**がある。
金融取引記録の改ざん（Risk 9 公的な台帳）	土地登記などの台帳に保存される公共資産記録は、不動産の所有権、住宅ローン、及び関連する証券の基礎として機能しており改ざんのリスクをもち、**所有権や法的権利、公開企業の記録、規制当局への提出書類、及びその他のデータソースも改ざんされる可能性**がある。

（出所）UK Finance「Minimising the Risks: Quantum Technology and Financial Services」よりNRIセキュア作成

ハーベスト（Harvest Now Decrypt Later：HNDL）攻撃

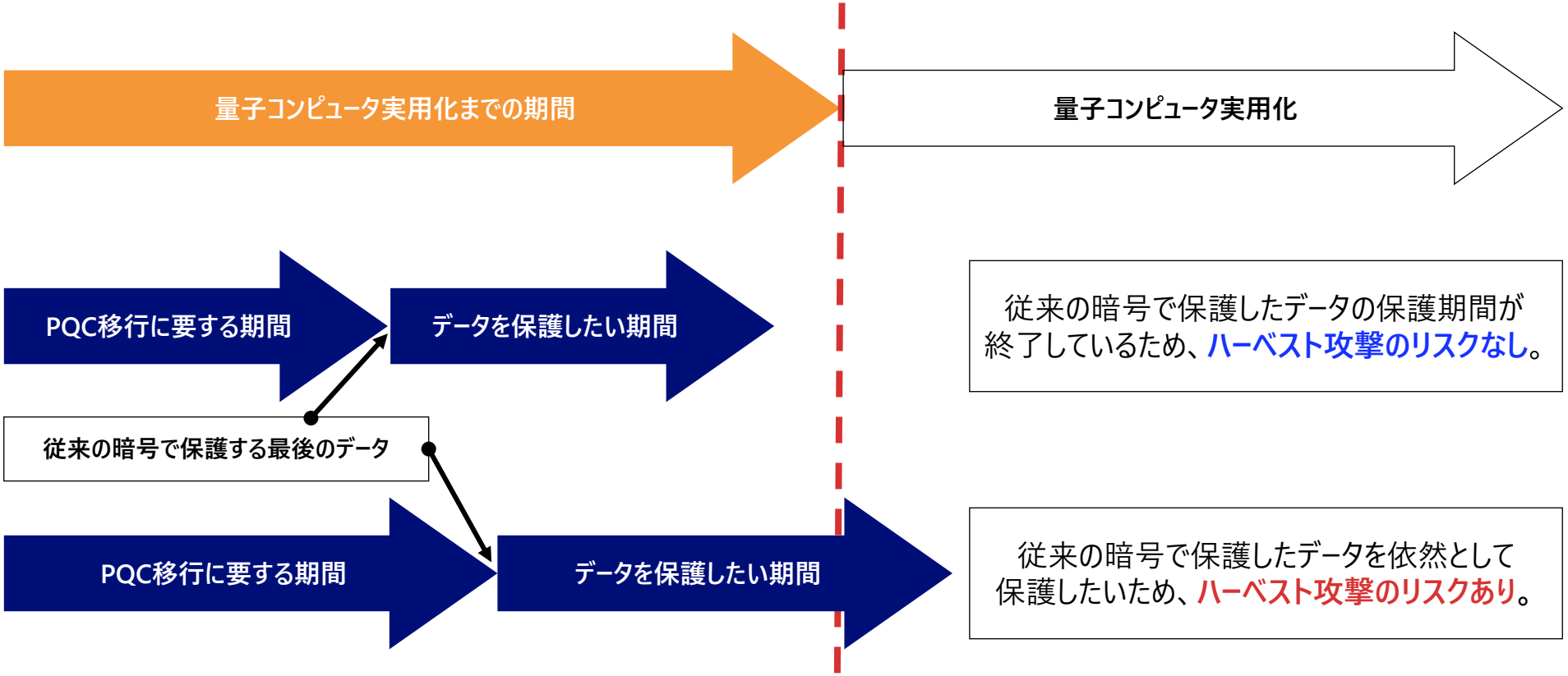
従来の暗号技術で保護されたデータを「現在」収集しておき、量子コンピュータ実用化後の「将来」解読するHNDL攻撃にも留意が必要。



2. PQCへの移行に向けた国内外のタイムライン

量子コンピュータが実用化するまでに移行すれば問題ないか？

法的要件やビジネスニーズなどを理由に長期間保護する必要があるデータについては、潜在的にハーベスト攻撃のリスクが発生している可能性があるため、早急に着手が必要。



「PQC移行に要する期間」と「データを保護したい期間」から逆算して、PQC移行を検討する必要がある。（Moscaの定理）

PQC移行に向けた米国のタイムライン（1/2）

米国は2035年までの量子リスクの軽減を目指し、NSA※1は2033年までに国家安全保障関連システムで使用する機器へのPQC実装を求めている。

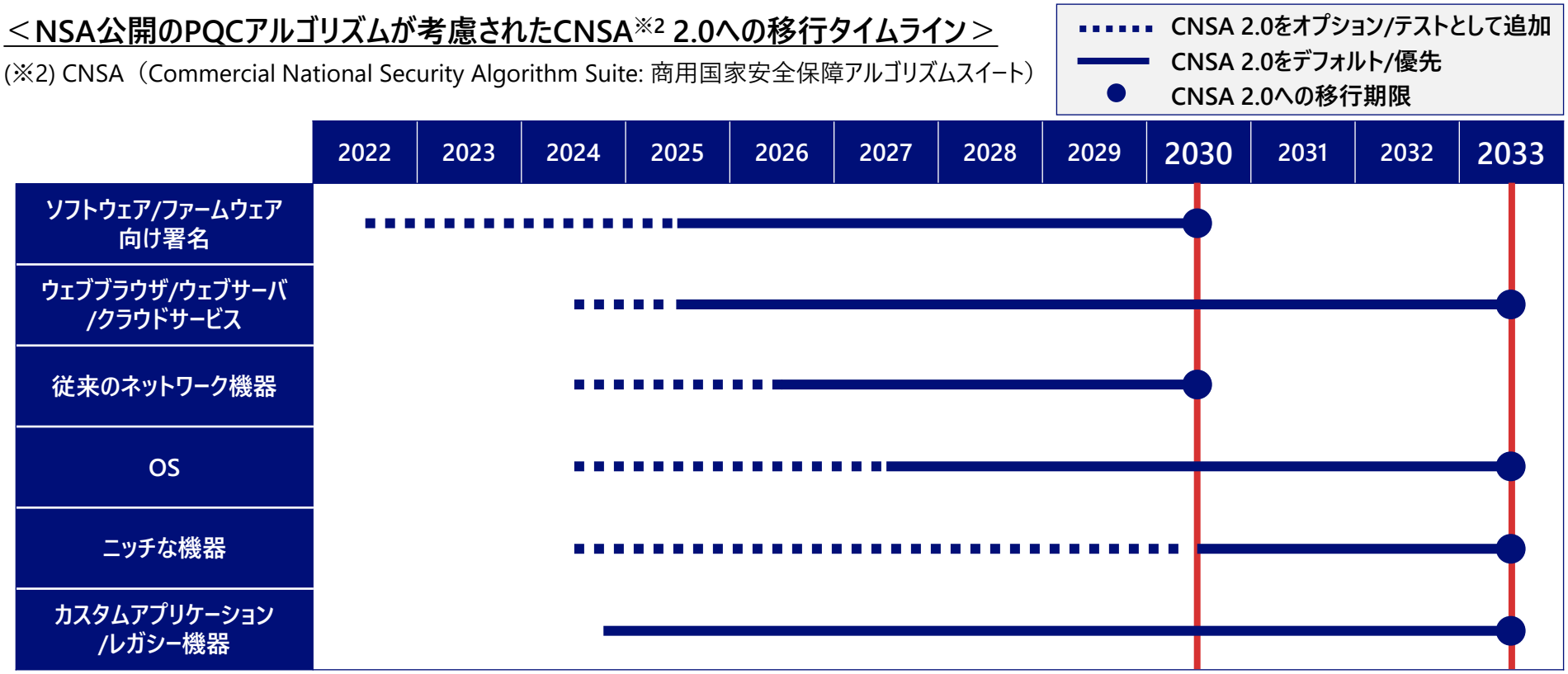
(※1) NSA（National Security Agency: 国家安全保障局）

＜ホワイトハウスからの公開原文（NSM-10）＞

To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, **with the goal of mitigating as much of the quantum risk as is feasible by 2035.**

＜NSA公開のPQCアルゴリズムが考慮されたCNSA※2 2.0への移行タイムライン＞

(※2) CNSA（Commercial National Security Algorithm Suite: 商用国家安全保障アルゴリズムスイート）



（出所）The White House「National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems（NSM-10）」(太字強調はNRIセキュア)

（出所）National Security Agency「Announcing the Commercial National Security Algorithm Suite 2.0」よりNRIセキュア作成

PQC移行に向けた米国のタイムライン（2/2）

NIST※では、公開鍵暗号方式の使用を2035年以降禁止とする方針。

（※）NIST（National Institute of Standards and Technology: 米国国立標準技術研究所）

鍵交換/デジタル署名アルゴリズム	強度	移行
ECDSA	112bit強度	2030年以降非推奨 **2035年以降禁止**
	≧128bit強度	**2035年以降禁止**
EdDSA	≧128bit強度	**2035年以降禁止**
RSA	112bit強度	2030年以降非推奨 **2035年以降禁止**
	≧128bit強度	**2035年以降禁止**

（出所） NIST「Transition to Post-Quantum Cryptography Standards (NIST Internal Report 8547, Initial Public Draft)」よりNRIセキュア作成

PQC移行に向けた日本のタイムライン（1/2）

内閣官房は、2025年6月より、内閣官房副長官補を議長に、「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」を開催中。

移行には、技術的課題のみならず、安全保障、産業政策、サービス安定供給、対応支援策、国際連携など多岐にわたる課題があるが、**まずは、政府機関等における耐量子計算機暗号（PQC） 利用に関し、関係府省庁の緊密な連携の下に必要な施策を検討・推進する**ため、政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（以下「連絡会議」という。） を開催する。

議　長	内閣官房副長官補（内政担当）
副議長	内閣官房内閣審議官（国家安全保障局）
	内閣官房内閣審議官（内閣サイバーセキュリティセンター）
主　査	デジタル庁統括官（デジタル社会共通機能担当）
	総務省サイバーセキュリティ統括官
	経済産業省商務情報政策局長
構成員	内閣官房内閣審議官（内閣官房副長官補付）
	内閣府科学技術・イノベーション推進事務局統括官
	警察庁長官官房技術総括審議官
	デジタル庁統括官（戦略・組織担当）
	外務省大臣官房サイバーセキュリティ・情報化参事官
	文部科学省研究振興局長
	経済産業省イノベーション・環境局長
	防衛省大臣官房サイバーセキュリティ・情報化審議官

今後のスケジュール（案）

令和７年６月	第１回関係府省庁連絡会議の開催
	（議事内容） ・ 連絡会議及び幹事会の設置 ・ 検討すべき論点の設定 ・ 今後のスケジュールの確認
令和７年７月 ～１１月	連絡会議幹事会の開催（随時）
	（議事内容） ・ 工程表（ロードマップ）の骨子の検討 〈主な検討内容（例）〉 ・ 危殆化する公開鍵暗号の特定とその時期 ・ PQC の安全性等の評価・確認とその時期 ・ PQC への移行期限及び危殆化した公開鍵暗号の利用停止の時期 ・ 移行への対応に必要な支援策等
令和７年１１月頃	第２回関係府省庁連絡会議の開催
	（議事内容（案）） ・ 工程表（ロードマップ）の骨子のとりまとめ
令和８年度中	第３回関係府省庁連絡会議の開催
	（議事内容（案）） ・ 工程表（ロードマップ）の策定について

（出所）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）利用に関する関係府省庁連絡会議」
（青枠及び太字強調はNRIセキュア）

PQC移行に向けた日本のタイムライン（2/2）

2025年8月時点では、日本における対応期限は明確化されていないが、諸外国の動向を踏まえ、2030年～2030年代半ばに設定される可能性がある。

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

- 対応時期目安について
  - 暗号解読可能な量子コンピュータの登場時期予測は、専門家内でも意見が分かれており時間軸に幅がある一方で、アメリカ政府では 2035 年目途に移行推進している状況から、預金取扱金融機関を対象にした各種法令や海外規制動向に耐量子計算機暗号への移行対応が盛り込まれる可能性がある。(p.16, p.41)
  - 各組織内の優先度の高いシステムは、技術進展や海外規制動向を注視しつつ、2030 年代半ばを目安に耐量子計算機暗号のアルゴリズムを利用可能な状態にすることが望ましい。(p.9, p.48)

衆議院 会議録 第217回第11号

○政府参考人（柳瀬護君）　お答え申し上げます。

委員御指摘のとおり、金融庁では、昨年検討会を金融業界と開催しまして、金融機関がＰＱＣへの移行を検討する際の推奨事項や課題等について議論し、昨年十一月に報告書を公表してございます。

この報告書も踏まえまして、当庁といたしましては、金融機関に対して、自社の各システムで使用している暗号の台帳を整備し、それに基づくリスク評価の上、ＰＱＣへの移行対応の優先順位を検討することや、ＰＱＣへの移行に関するロードマップの作成を含め、二〇三〇年代半ばまでの移行を目標とする準備などに直ちに着手することを求めておるところでございます。

（出所）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報告書」（青枠はNRIセキュア）
（出所）国会会議録「衆議院 会議録 第217回第11号」（令和7年）（青枠はNRIセキュア）

サイバーセキュリティ対策の更なる強化に向けた提言

○提言

民間セクターを含む我が国の重要な情報システムの耐量子計算機暗号技術の対応を、政府が責任を持って推進するため、以下５項目を含む「耐量子計算機暗号対応のための行動計画（仮称）」を策定の上、「サイバーセキュリティ戦略」にも明確に位置付けるべきである。

① 我が国全体を視野に入れた「移行計画（ロードマップ）」の策定と公表

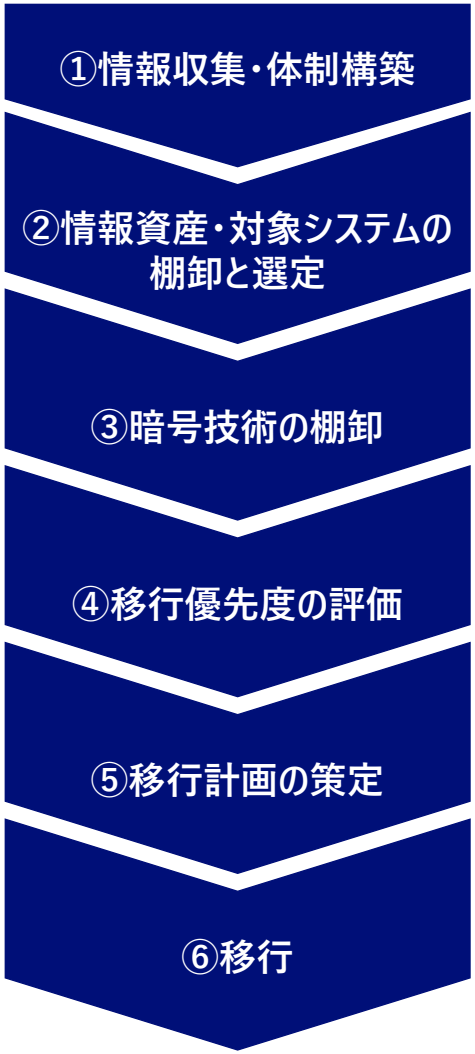
- 既に活用されている暗号技術については、現在の計算機の性能向上による解読リスクも考慮した必要なセキュリティ強度を有するアルゴリズムを活用することが重要であり、2030年を目途に強度がより強い暗号アルゴリズムへの移行を目指すこと（例えば、128 ビットセキュリティ強度を有するアルゴリズムの活用等）
- その上で、量子計算機技術の進展等も踏まえて必要な対応を行うべく、耐量子計算機暗号対応の影響調査や評価を速やかに実施し、公共領域、金融領域、通信領域、エネルギー領域等の重要領域において最優先対応システムを具体化するなど、対応の範囲・優先順位を明確化すること
- 優先順位に応じた対応年限を設定すること。そのうち、重要領域における最優先対応システムについては、2030 年を目途に対応を完了するよう設定すること。

（出所）自由民主党政務調査会 デジタル社会推進本部「サイバーセキュリティ対策の更なる強化に向けた提言」（青枠はNRIセキュア）

3. PQC移行の進め方と留意事項

PQC移行の進め方の概要

情報資産や対象システム、暗号技術の棚卸、移行優先度の評価をしたうえで、PQC移行計画を策定することが重要である。



①PQCに関する最新動向の情報収集を行い、移行に向けた目的や方針を明確化する。また、移行を推進する体制を構築する。

②PQC移行に向けた基礎として情報資産の棚卸を実施し、各システムが扱う情報の重要度、保護期間、外部公開の有無などの複数の観点から、移行の要否および優先度を分類する。

③アーキテクチャ設計書や構成管理資料、現場担当者へのヒアリングなどにより暗号技術の利用状況の全体像を把握する。自動収集ツールの利用も検討し、使用されているプロトコル、暗号アルゴリズム、証明書、鍵長などを整理していく。

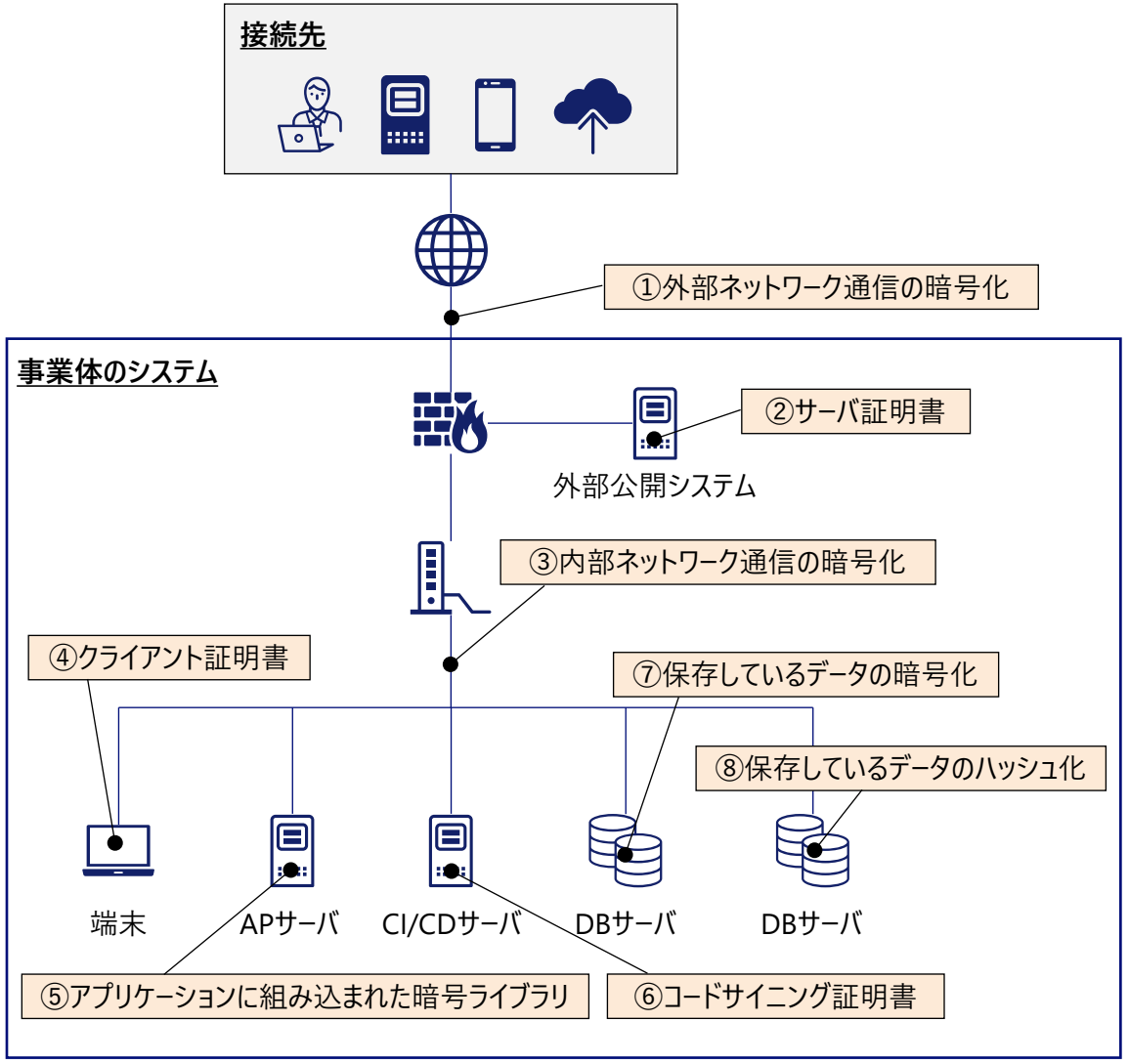
④情報の重要度、保護期間、現在の暗号方式の量子耐性、移行コストなどの複数の観点から、移行対象システムの暗号使用箇所におけるPQCへの移行の必要性と優先度を評価する。

⑤評価結果をもとに、各システムや暗号技術に対するPQCへの対応方針を定め、移行計画を策定する。

⑥自社内の関係者に加え、外部ベンダや他社など様々なステークホルダーと連携・協力し、PQC移行を推進する。

PQC移行に必要な対応は、PQCに対応したサーバ証明書に切り替えるだけで十分か？

サーバ証明書などに使用される公開鍵暗号方式だけでなく、共通鍵暗号方式およびハッシュ関数を含む事業体で使用する全ての暗号技術について考慮が必要。



No.	使用している暗号技術の例
①	公開鍵
②	公開鍵・ハッシュ
③	公開鍵
④	公開鍵・ハッシュ
⑤	共通鍵・公開鍵・ハッシュ
⑥	公開鍵・ハッシュ
⑦	共通鍵
⑧	ハッシュ
・・・	・・・

様々なステークホルダーとの連携・協力の必要性

経営層がリスクや移行期限などを正しく認識し、自社内の関係者に加え、外部ベンダや他社など様々なステークホルダーと連携・協力し、移行を推進することが重要。

・・・その対応には 長期にわたり多大なリソースを要するため、**経営層がリスクや移行の期限などを正しく認識する必要がある。**

経営層が全社（または全組織的施策）としてリーダーシップを発揮し、各システムで利用されている暗号状況や自組織データの重要性及び保存期間等を把握し、適切なリスク評価や優先順位付けした上で、移行方針を決定することが望ましい。

PQC対応においては、・・・**計画的にリソース（ヒト・カネ）を確保して推進することが肝要**である。特に、初期の活動として定義される**グランドデザインロードマップの策定やクリプト・インベントリの作成といった活動により施策全体として必要となるリソースが見積れるようになり、ライフサイクルに合わせた対応等を検討することにより効率的に実施できることから、早めに取り組むことが肝要**である。

・・・暗号に特化した部門・人材が十分に確保されていないことも想定され、既存のサイバー部門の役割・機能・体制の延長ではPQC対応の企画・管理・推進ができないことも視野にいれることが重要である。**暗号領域は専門人材が不足しており、外部パートナーを含めてリソース確保に取り組む等の検討が期待される。**

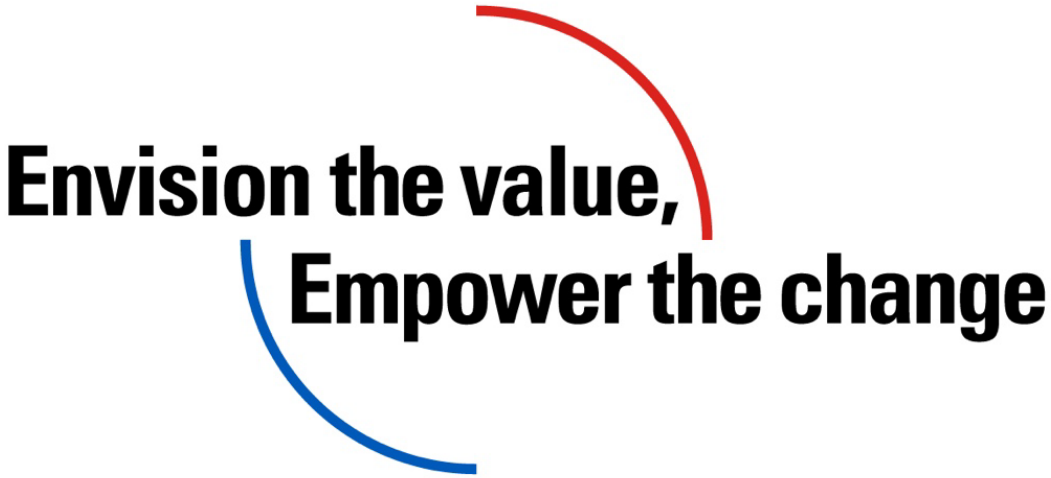
（出所）金融庁「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書」よりNRIセキュア作成

PQC移行にあたる課題・留意事項

PQC移行は長期間を要し、システムリソースの増大や脆弱性対応の遅延、移行後のPQC自身の危殆化など複合的なリスクが伴う。

課題・留意事項	説明
システムの暗号移行には長い期間を要する	• 大規模システムにおける暗号移行は、一般的に時間が掛かり、移行に要するコストも増加する傾向にある。 • ソフトウェアやシステム間に複雑な依存関係が存在する場合にはさらに長い時間を要する可能性がある。 • 関連するステークホルダーが多い場合や、特定の国際標準等に準拠することが必要な場合は、それらの調整にも時間を要する可能性がある。
PQCは従来の暗号アルゴリズムに比べて、より多くのリソースを要求しうる	• **PQCは従来の暗号アルゴリズムに比べて、通信量や計算量が増加する。**PQCは、暗号鍵のデータ量、デジタル署名のデータ量、必要とする計算量のうち、少なくとも1つ以上で、既存の公開鍵暗号アルゴリズムに比べて多くのリソースを消費する。 • 現状のTLS通信のServer Helloにおいては、PQC用のサーバ認証用証明書を単一のペイロードに格納できない。 • 単一のWeb サーバが同時に処理可能なコネクション数が減少する可能性がある。
PQC移行中は、脆弱性等への対応が遅れる可能性がある	• PQCへの移行中に、何らかのセキュリティホールが発見されることが考えられる。PQCへの移行が完了しない限りセキュリティパッチが適用できない状況であったとすると、PQCへの移行が完了するまでは当該セキュリティホールを放置することを余儀なくされる。
PQC移行後または移行実施中にPQC自身に問題が発生する可能性がある	• PQCへの移行完了後または移行実施中に、PQCアルゴリズムが危殆化するおそれがある。PQCアルゴリズムが、RSAやECDSA等の既存暗号アルゴリズムよりも早く危殆化する可能性は否定できない。 • PQC導入後の数年間は、いつでも既存のアルゴリズムに戻せる体制で運用を行うアプローチも考えられる。

（出所）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報告書」よりNRIセキュア作成


Envision the value,
Empower the change