資料2-4

量子セキュリティ・量子ネットワークの実用化戦略

国立研究開発法人 **情報通信研究機構**
量子ICT協創センター
研究センター長 佐々木　雅英

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

量子セキュリティ分野の現状と課題

これまでの問題点

- セキュリティ対策は、**強制力がなければ、後回しになりがち**
  ⇒企業は投資しづらく、ユーザは導入しづらい
  ⇒利用インセンティブを高めるガイドラインや法整備が必要
- 標準化や認定制度、ビジネスでは、これまで**欧米が先行**
- 耐量子-公開鍵暗号の標準化でも**日本は大きく出遅れた**

我が国の現状

- 量子暗号では、日本が技術性能、アプリケーション、標準化で世界をリード
- 量子暗号と現代暗号の統合による量子セキュリティ分野の開拓を先導

しかし、本格普及には、これだけでは不十分！

そもそも暗号ビジネスは、いつの時代も容易ではない

Thalesが約5000人のビジネスユーザーを対象に2017年に実施した調査レポートより引用

・組織全体で一貫した暗号化戦略を導入している企業は41%

＜導入の理由＞
1位：規制遵守
2位：知的所有権の保護
2位：「特定の識別できる脅威」に対する保護
4位：顧客の個人情報の保護

＜クラウドを活用する企業＞
①3分の2は、クラウドに送る前に暗号化（鍵を自社で管理）
②3分の1は、暗号鍵と暗号化プロセスをクラウド事業者に任せている

・暗号化について計画はないという企業は15%　（8社に1社）

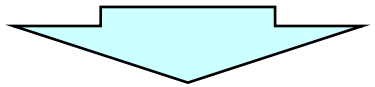
＜暗号化の利用が低い理由＞
1位：機密データが組織のどこに存在するのかを見つけることが困難
2位：暗号化技術の実装が容易でない。コストもかかる。
3位：暗号化するべきデータの判断が難しい

セキュリティ分野のみを舞台に考えていても、
ユーザ獲得、市場拡大は難しいだろう

守るべき秘密を創り出す

重要データを次々と生み出す新技術と組み合わせビジネス化する

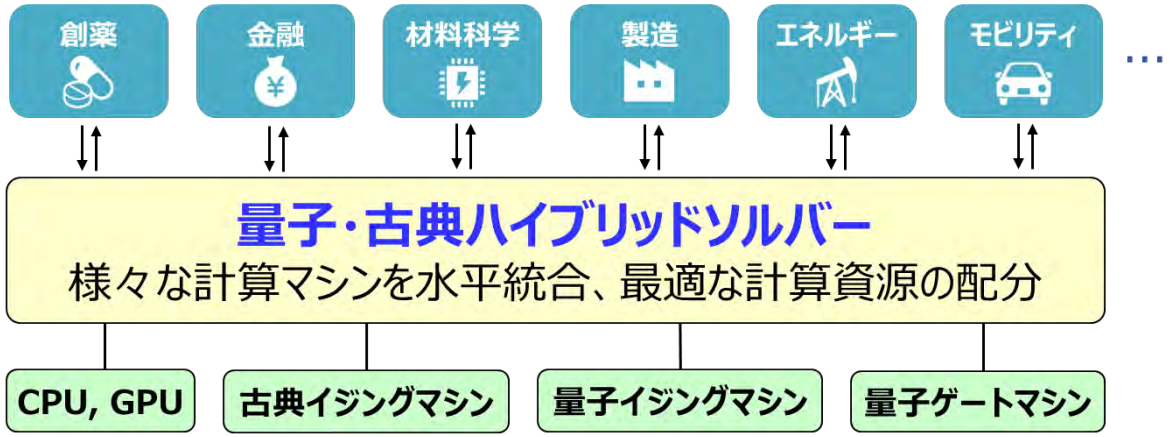
特に、**高度なコンピューティング技術**と組み合わせる
（あらゆる産業分野から投資が得られる）



コンピューティングサービスでユーザを獲得し、
セキュリティ対策コストを上回る付加価値を提供する

量子セキュアクラウド

次世代コンピューティング基盤 X **次世代暗号基盤**



- 耐量子ー公開鍵暗号 → 署名、認証、鍵交換
- 共通鍵暗号 → 秘匿通信
- 量子暗号 → 秘匿通信
- 秘密分散 → データ保管

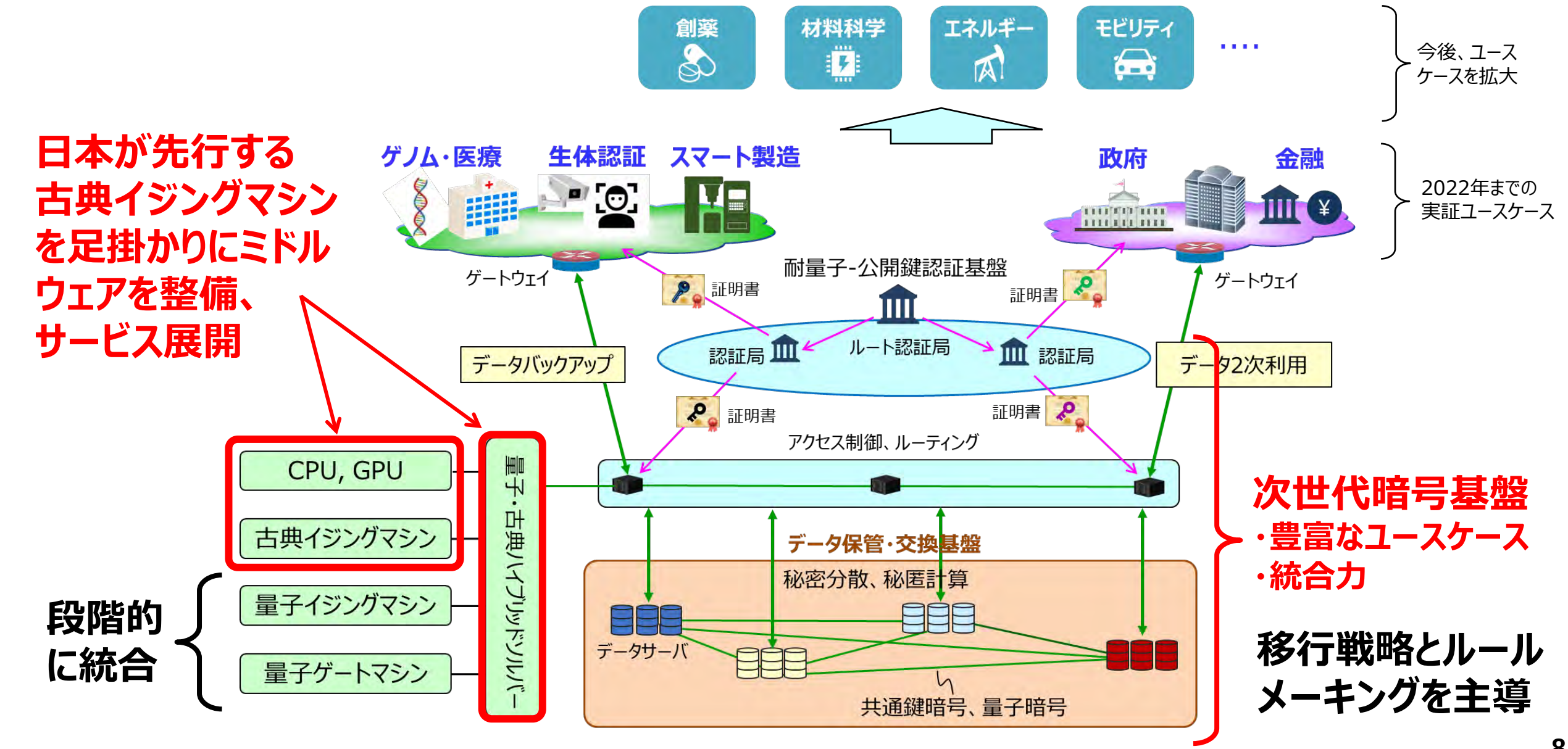
様々な分野の重要データ

クラウドビジネスの現状と課題

・現在、**クラウドサービスでは、GAFAMによる寡占化が進んでいる。**
インターネット事業の儲けをデータセンターの建設費に回してクラウド事業を席巻。
・データセンターは老朽化が進み、今後、建て替えの時期に入るが、
今の日本企業にデータセンターを建てる余力がないのが実情。

量子技術で日本が巻き返す戦略はどうあるべきか？

日本の強みを活かす


創薬
材料科学
エネルギー
モビリティ
....
今後、ユースケースを拡大
日本が先行する古典イジングマシンを足掛かりにミドルウェアを整備、サービス展開
ゲノム・医療
生体認証
スマート製造
政府
金融
2022年までの実証ユースケース
ゲートウェイ
証明書
耐量子-公開鍵認証基盤
証明書
ゲートウェイ
データバックアップ
認証局
ルート認証局
認証局
データ2次利用
証明書
証明書
アクセス制御、ルーティング
CPU, GPU
古典イジングマシン
量子イジングマシン
量子ゲートマシン
量子・古典ハイブリッドソルバー
段階的に統合
データ保管・交換基盤
秘密分散、秘匿計算
データサーバ
共通鍵暗号、量子暗号
次世代暗号基盤
・豊富なユースケース
・統合力
移行戦略とルールメーキングを主導

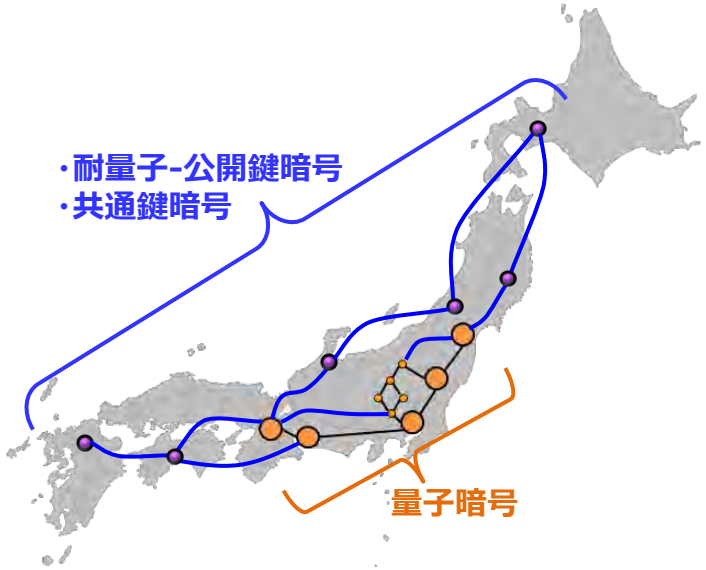
移行戦略

2023年頃

・都市圏-量子暗号網の拡充
・都市間-耐量子-暗号網の
テストベッドの設計開始

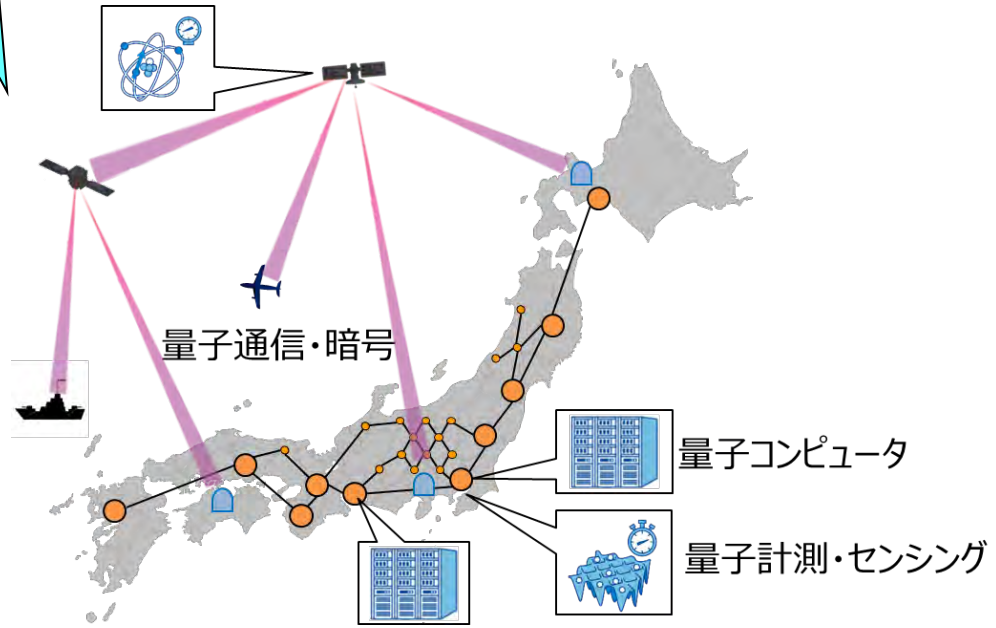
2025年頃

・都市間-量子暗号通信網
の構築開始
・広域-耐量子-暗号網の運用試験
・量子・古典ハイブリッドソルバー
ネットワークの構築
・QKD評価・認証制度の整備



2030年頃

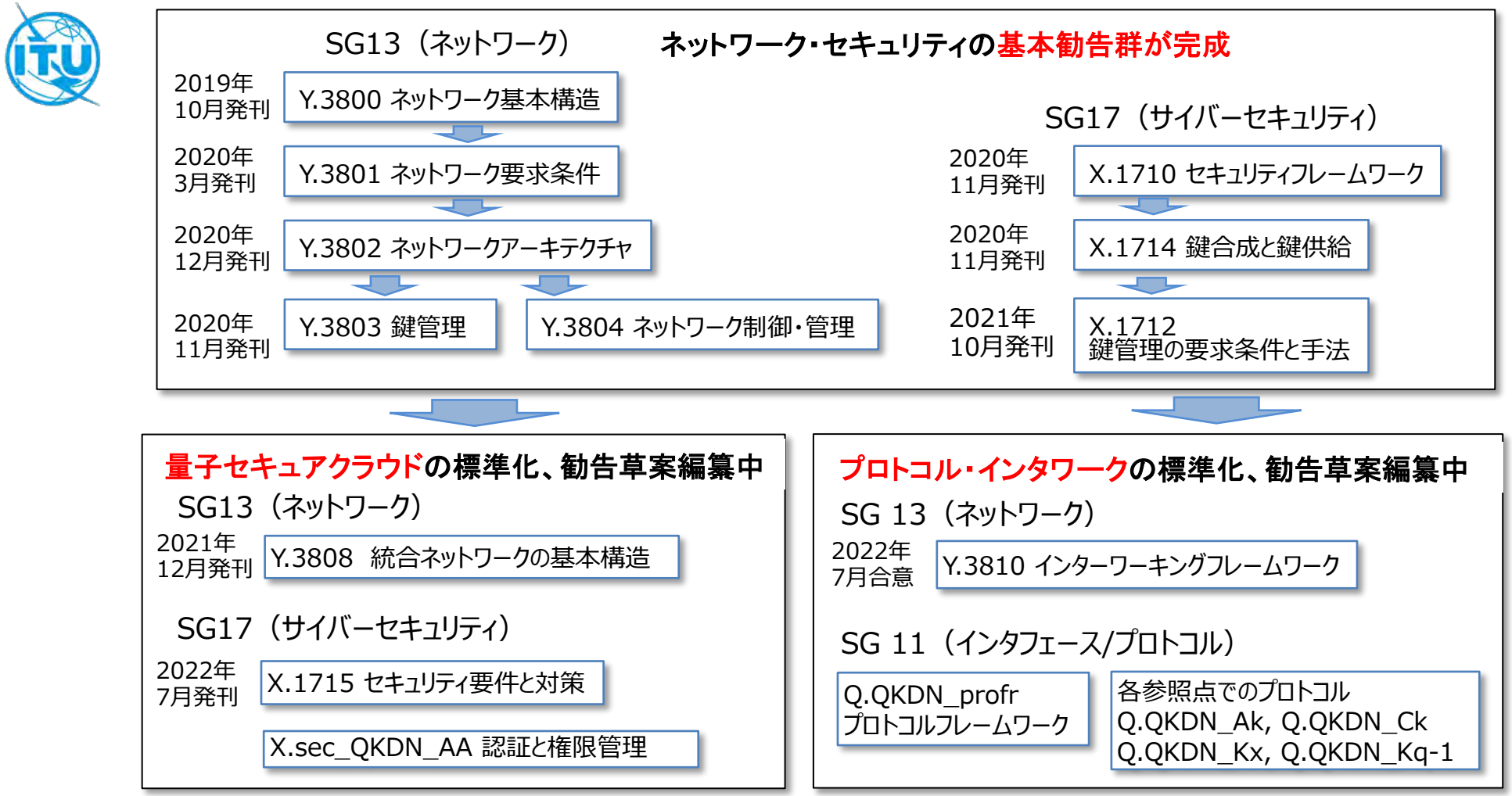
衛星・地上網の統合
様々な量子技術を融合、既存インフラと
統合、量子技術プラットフォームの構築



ルールメーキング

QKDネットワークの研究と並行して標準化を主導、日本仕様に基づく基本勧告体系を短期間で整備

⇒ 現在、通信事業者とのテストベッド設計、アプリ開発の指針となっており、開発作業を大いに効率化



QKD装置の評価・認証制度の整備

国際規格準拠の認証を取得した量子暗号装置を世界に先駆けて市場投入する

2025年
~2026年頃

・技術支援、規格の改定などを行う業界団体を設立する
・通信機器・計測機器メーカなどから評価者・認証者を育成する

国際規格

ISO JTC1 IEC INFORMATION TECHNOLOGY STANDARDS

コモンクライテリア(CC)
ISO/IEC23837、2023年上期発刊予定

ETSI World Class Standards

プロテクションプロファイル(PP) レベル4+ （政府用途等）
2023年8月発刊予定

まとめ

量子セキュリティ技術と量子・古典ハイブリッドソルバー技術を融合し、
共通基盤のテストベッドを構築する

様々な分野のユーザと共同PoCを推進し、体験者を増やす

段階的な『移行戦略』と『ルールメーキング』を主導する

2025年
~2026年頃

量子技術を融合し既存インフラと統合した量子技術プラットフォームを構築する

2030年頃

新たなサービスを創出し、市場を拡大する