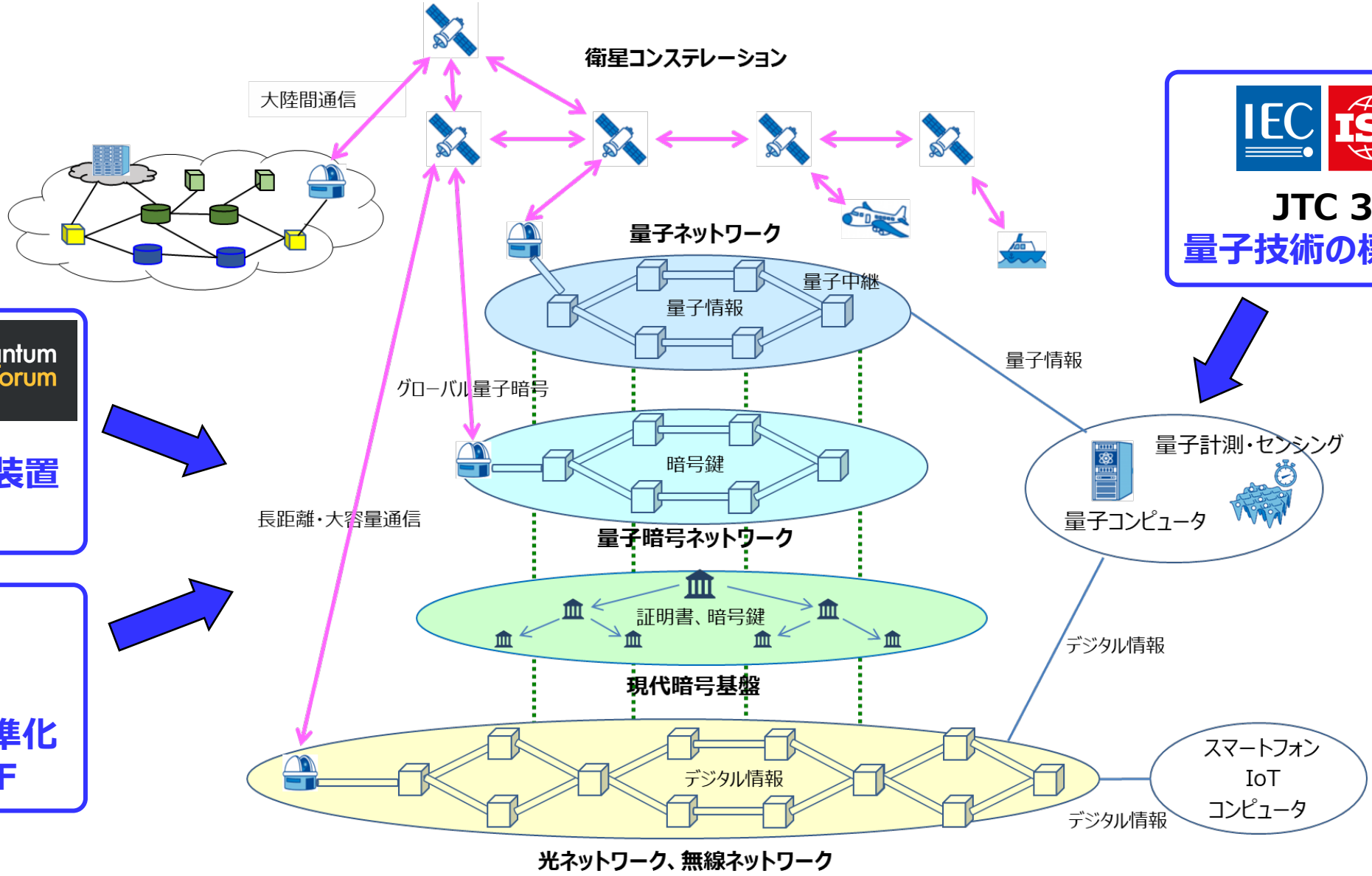
資料1-2

量子時代の通信インフラ構築に向けた国際標準化

国立研究開発法人 **情報通信研究機構**
オープンイノベーション推進本部
主管研究員　佐々木　雅英

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

量子時代の通信インフラのイメージと国際標準化の動向



ETSI World Class Standards

Quantum Forum

量子鍵配送（QKD）装置の評価・認証

ITU

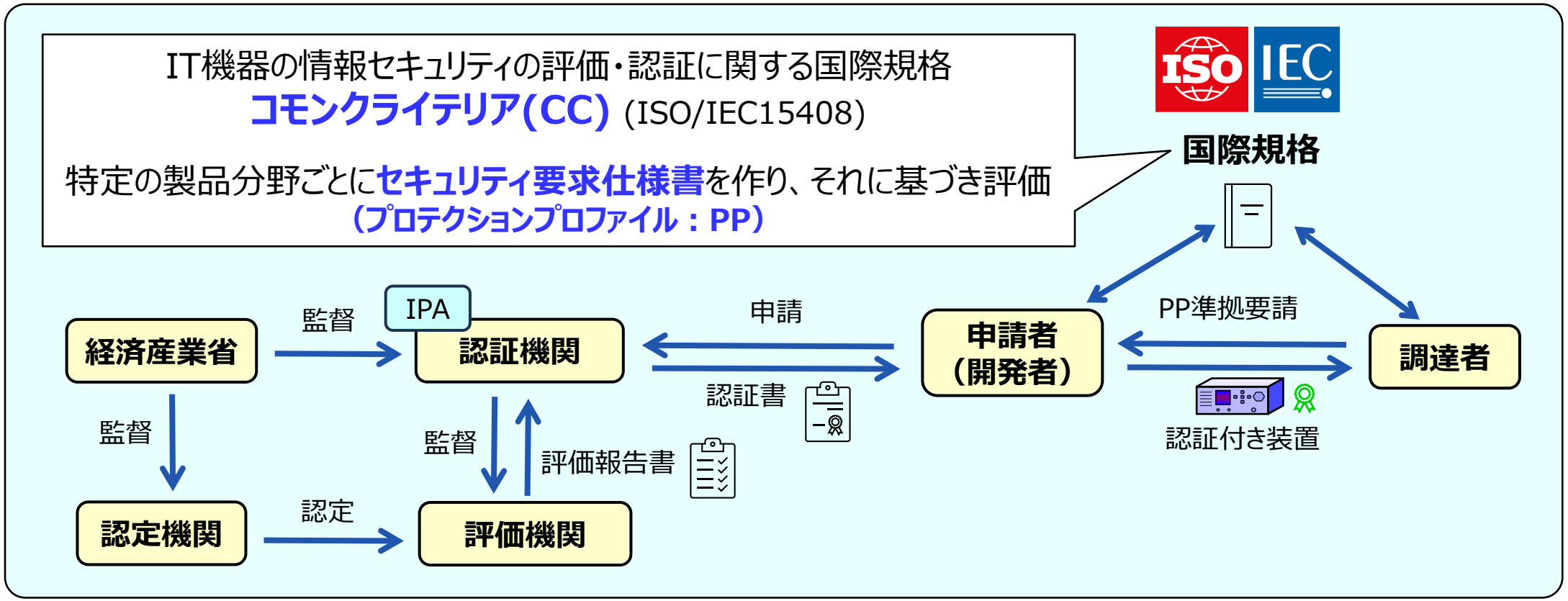
・QKDネットワークの標準化
・既存インフラとの統合IF

IEC ISO

JTC 3
量子技術の標準化

QKD装置の評価・認証制度の整備

国際規格『コモンクライテリア』に基づく認証制度の枠組みで、QKD装置の評価・認証を行う仕組みを整備中



CC認証制度には、**国際承認アレンジメント（CCRA）協定**があり、一度、日本で認証を取れば
CCRA加盟国（現在、31か国）で**相互承認が可能**で、国際市場展開を強化しやすい。
ただし、プロテクションプロファイルの**評価保証レベル（EAL）が2以下であることが条件**。

CC認証取得に向けた工程案

総務省プロジェクト
グローバル量子暗号通信網の研究開発

CC/PP会議

1．準備段階

✓ 2023年4月、QKD分野初の**PP (EAL4)**を発刊
⇒ CCRAの適用外。欧州の政府調達等で利用されると予想。

✓ 2024年1月、独の認証機関BSIが承認

✓ 2024年9月、**PP (EAL2)**ドラフト作成、ほぼ完了
⇒ ETSI-PP (EAL4) との共通事項を多く含むため、ETSIへ著作権許諾を申請中。

2024年

・付属文書の作成
・プロトコル・安全性証明文書
・評価手法文書

・付属文書の作成
・プロトコル・安全性証明文書
・評価手法文書

QKD分野として統一された規格化の推進が重要

2．製品開発段階

2025年

・ベンダーによる製品ごとの文書群の作成（セキュリティ設計仕様書など）
・評価・認証の実務人材育成
・評価環境の整備

3．製品のCC認証取得

2026年

・ハイエンドの政府調達向けへの製品展開

・CCRAの枠組みで国際市場へ製品展開

QKDネットワーク（QKDN）の標準化

- ✓ **ITU-Tにおける国際標準化を主導、日本の技術が世界標準に**
- ✓ QKDネットワークの基本仕様として活用され、通信事業者とのテストベッドの構築、アプリ開発を大いに効率化

基本勧告群

SG13（ネットワーク）

Y.3800 ネットワーク基本構造	(2019年10月発刊)
Y.3801 ネットワーク要求条件	(2020年4月発刊)
Y.3802 ネットワークアーキテクチャ	(2020年12月発刊)
Y.3803 ネットワーク鍵管理	(2020年12月発刊)
Y.3804 ネットワーク制御・管理	(2020年9月発刊)

SG17（サイバーセキュリティ）

X.1710 セキュリティフレームワーク	(2020年10月発刊)
X.1714 鍵合成と鍵供給	(2021年10月発刊)
X.1712 鍵管理の要求条件と手法	(2021年10月発刊)

異種QKDNインターワーキング SG 13（ネットワーク）

2022年9月発刊	Y.3810 インターワーキングフレームワーク
2023年9月発刊	Y.3818 インタワーキングアーキテクチャ

QKDNプロトコル・インタフェース SG 11（インタフェース/プロトコル）

2023年12月発刊	Q.4160 QKDNプロトコルフレームワーク
2023年12月発刊	各参照点でのプロトコル Q.4161(Ak), Q.4162(Kq-1), Q.4163(Kx), Q.4164(Ck)
勧告草案編纂中 2025年3月 以降、承認予定	Q.QKDNi_profr インタワークプロトコルフレームワーク Q.QKDN_Mk Mk参照点のプロトコル Q.QKDNi_KM KM間インタワークプロトコル

量子セキュアクラウド SG13（ネットワーク）

2022年2月発刊	Y.3808 SSN統合ネットワークの基本構造
2024年8月承認	Y.3808 Rev SSN統合ネットワーク

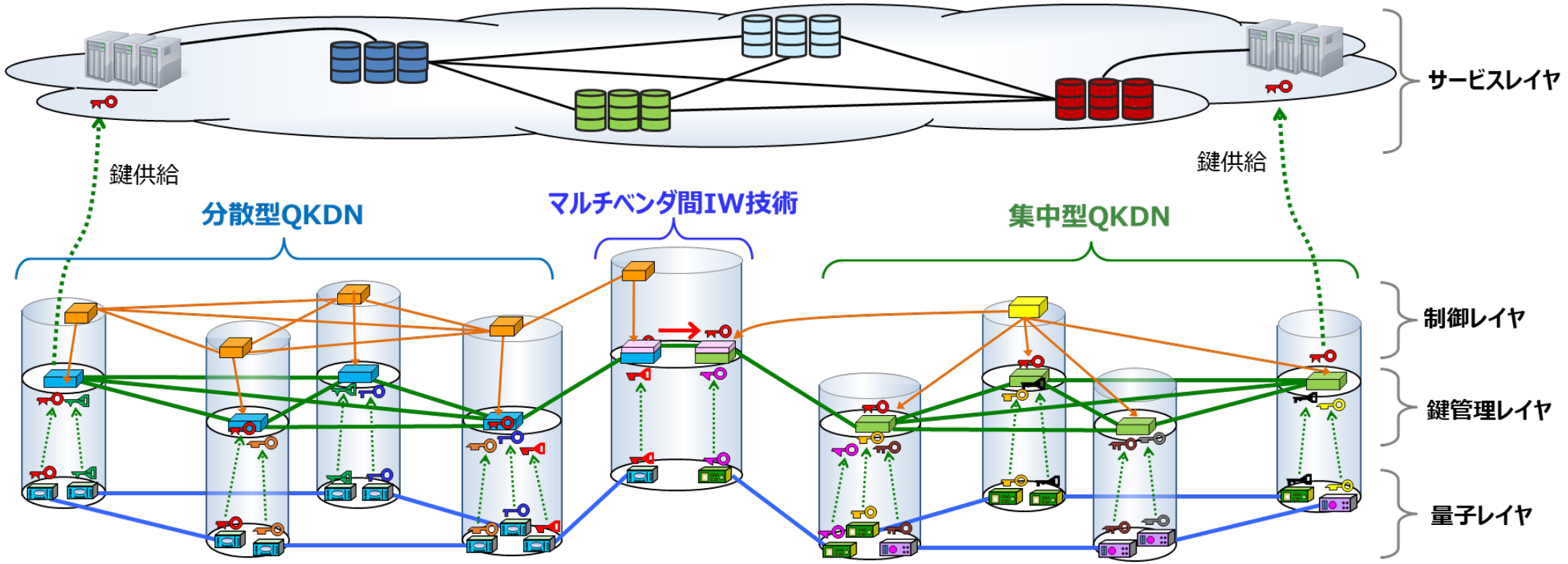
QKDNセキュリティ・認証・QKDプロトコル

SG17（サイバーセキュリティ）

2022年7月発刊	X.1715 SSN統合ネットワークのセキュリティ要件
2024年4月発刊	X.1713 トラステッドノードのセキュリティ
2024年9月承認	X.1716 QKDNの認可・認証 X.1717 QKDNの制御・管理
勧告草案編纂中 2025年4月 以降、承認予定	X.sec_QKD_profr QKDプロトコルフレームワーク

QKDネットワーク（QKDN）の標準化

現在、広域インフラ化に向けて、多様なベンダーの装置を相互接続するためのマルチベンダ間インターワーキング（IW）技術の標準化に重点が移っており、日本、中国、韓国、シンガポール、欧州などで標準化が進められている。



まとめと展望

・標準化や認証制度は、先手必勝

・一度先行されると、挽回は容易ではない。
・技術の成熟を待ってから取り掛かるのでは遅い。研究開発と並行しながら進める。

・人材育成の一環としても意義が高い

＜課題＞
・アジア諸国や欧州では、若手や中堅のリーダーが急成長。日本は、高齢化が進み、若手・中堅人材が続かない。
（企業から評価機関、認証機関へ出向者を出せない状況が続いている）。

＜若手・中堅にとってのメリット＞
・文章力、交渉力を磨く最高の場（論文執筆にも大いに役立つ）
技術の本質をつかみ普遍的な勧告文を書くためのスキルを様々な分野のエキスパートが教えてくれる
・熾烈な交渉の後の合意形成は、大きな達成感、一体感を生み出す
⇒ **このような経験を積んだ人材は、国際市場開拓のキーパーソンになる。**

＜要件＞
・出向コストの回収や制度維持には分野横断的な評価業務をこなせる人材が必要。
・計測機器、半導体分野の若手・中堅から量子技術の評価・認証人材をリクルート・育成し、量子エコシステム構築のトリガーにする。

若者よ、来たれ