様式１

経済安全保障重要技術育成プログラム／先進的サイバー防御機能・分析能力強化／セキュアな量子情報通信技術の開発

（中間評価）2024年度～2027年度　3年間

プロジェクト報告資料（公開版）

2026年1月26日

https://www.nedo.go.jp/activities/ZZJP_100334.html
2025年度実施一覧｜事業｜NEDO
NEDO:2025年度実施一覧

日立製作所

先進的サイバー防御機能・分析能力強化　（４）セキュアな量子情報通信技術の開発

（３０億円を超えない範囲／３年）

背景

近年実用化が進む量子計算機に対しても高い安全性を備えた暗号技術に対するニーズが増えている。従来安全であった暗号技術が、量子計算機の活用で破られることが知られており、量子計算機にも耐性のある安全な 暗号技術（耐量子計算機暗号）の研究開発等が実施されている。

一方で我が国が目指す Society 5.0 の技術発展とともに、様々な産業や社会活動において、情報通信で扱う情報は増大し、かつ非常に重要で機密性の高いものへと変化している。これらは、高速・大容量、低遅延を要求され、更にデータセンタ間の接続から IoT に至るまで、広範にセキュリティも要求されており、その対策が急務となっている。

QNSC の Y-00 プロトコルは、物理的な観測の複雑性（物理測定量的安全性）を量子雑音で実現しており、物理レイヤでの信号変調と同時に暗号化するため高速・低遅延であり、安全性が計算機の能力に影響されないため耐量子計算の安全性を実現できるなど、様々な特長を備える。また、様々な変調方式に対応可能と考えられており、伝送効率の高い変調方式への適用や光ワイヤレス通信への適用も期待できる。

本プロジェクトでは、経済安全保障重要技術育成プログラムの主旨を踏まえ、民生および公的利用の通信ネットワークの耐量子計算機の安全性を確保するためQNSC技術の早期社会実装を目指し研究開発を実施する。

想定されるニーズ

本プロジェクトの最大の目標は、現在の日本のネットワークセキュリティ対策において、物理レイヤの安全性を確保するため、成果であるQNSC(Y-00)装置を早期実装させることである。想定する最初のフィールドとしては、防衛（防衛情報通信基盤等）を中心に、政府関連施設を含め、アクセス系を中心とした環境への適用が考えられる。さらに、重要なデータセンター間通信にも適用可能と考え、実装提案を進める。

光ワイヤレス通信においては、指向性の特長も活かし、空港施設内の滑走路の横断通信や拠点内のビル間通信等への適用を検討していく。更に将来的には、衛星通信、移動体通信への適用も考える。

電力、金融、交通などの民生系への幅広い適用を考えると、更なるコスト低減、小型化および光通信の標準規格への対応、追従等を進める必要があるため、QNSC(Y-00)のASIC（LSI）化等の開発が必須となる。このため、今回の成果から民生系への適用の見通しを得ることができれば、新たな大型の国家プロジェクトの展開へ繋げることも必要と考える。

研究開発内容

〔1〕Y-00 のデジタルコヒーレントの開発

QNSC（Y-00）では、基本となる変調方式を多値化しデータを埋め込む処理を行うため、一般的なデジタルコヒーレント技術とは異なることから、専用のデジタルコヒーレント方式を新たに開発する。

① デジタル変復調技術　② リアルタイム処理　③ デジタル歪補正　④ 論理検証機（FPGA）の作成

〔2〕Y-00 の高速光ファイバ通信の開発

開発するY-00 プロトコル用のDSPは、目標の 20 Gbit/s 以上の高速・大容量通信と精度の高い制御を実現するための専用の同期方式や制御方式の開発が必要となる。また、リアルタイム制御実現のためにプロトコルの最適化を開発し、それに適したセキュア管理システムの開発も実施する。

① 光デバイス構成　② セキュア管理システムの開発　③ 光ファイバ伝送 20 Gbit/s 試作機の開発

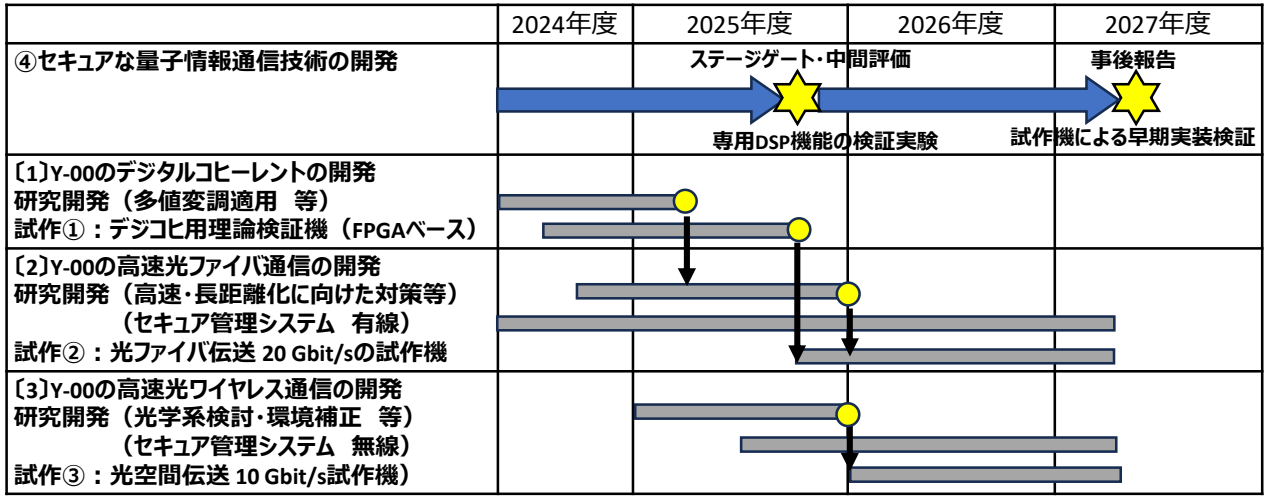
〔3〕Y-00 の高速光ワイヤレス通信の開発

QNSC（Y-00）を適用した光ワイヤレス伝送を実現するための光アンテナを開発する。光ワイヤレス伝送においては光ファイバ伝送とは異なり、不安定な通信媒体での正確で安全な通信が求められ、以下の項目で実施する。

① 光ワイヤレス通信専用のDSPの開発　② 光アンテナとの結合を想定した専用光モジュール開発

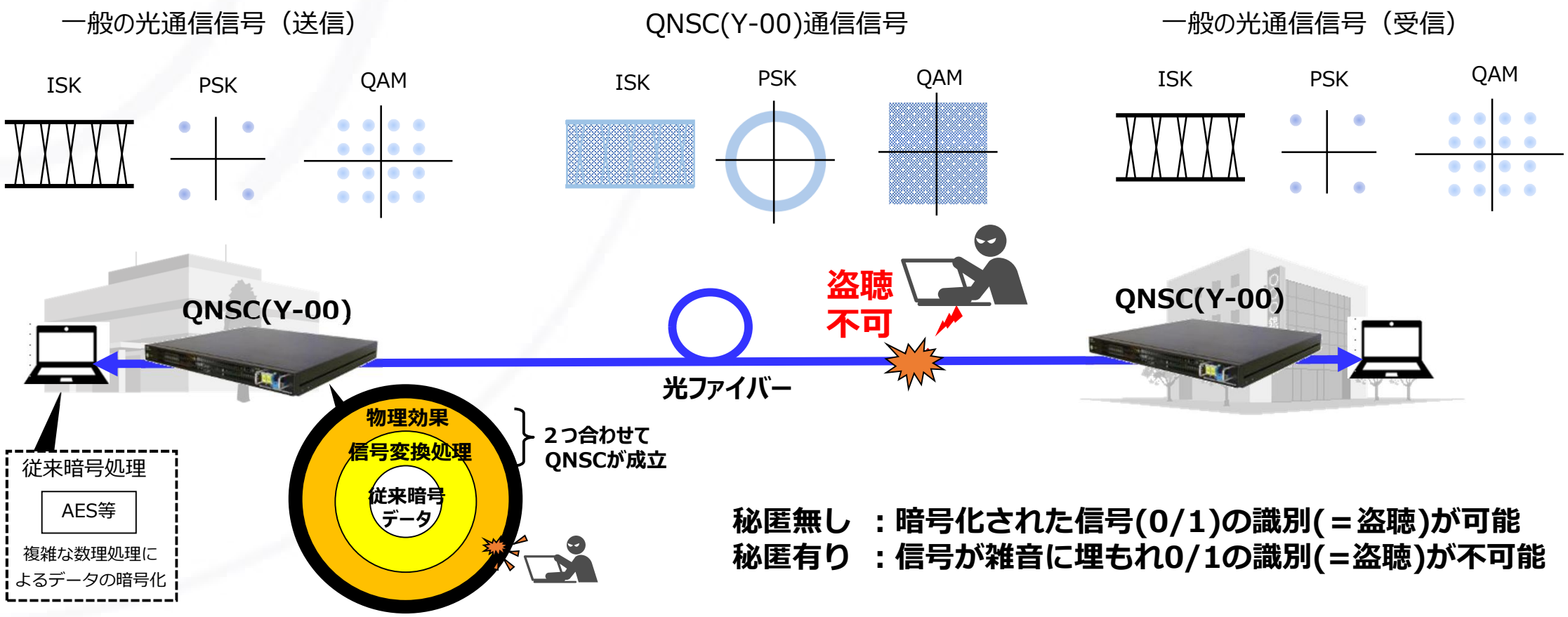
③ 光ワイヤレス伝送に適したセキュア管理システムの開発　④ 光空間伝送 QNSC 試作機の開発

想定スケジュール



QNSC（Y-00）の概要

Y-00（Yuen 2000）プロトコルとは、光通信に利用するデジタル信号（「0」、「1」）の情報を信号の振幅または位相の１次元方向に量子雑音に隠れるほどの多値数で変調させ、その中に「0」「1」の２値の組合せをランダムに埋め込み秘匿通信をおこなうプロトコルであり、ノースウェスタン大学のH.P.Yuen教授により2000年に米国DARPAプロジェクトで提唱された技術である。
QNSC（Quantum Noise Stream Cipher）は、このプロトコルを拡張し、位相と振幅の２次元方向に同時に多値変調することでQAM方式にも対応できるようにした技術であり、現在では、その言葉通り全体を包括する呼称となっている。



秘匿無し　：暗号化された信号(0/1)の識別(＝盗聴)が可能
秘匿有り　：信号が雑音に埋もれ0/1の識別(＝盗聴)が不可能

＜評価項目１＞研究開発ビジョン及び研究開発構想の実現に向けた研究開発課題の達成目標や内容の妥当性

(1) 達成目標の妥当性

(2) 知的財産・標準化戦略

QNSC(Y-00）の最新技術動向

近年（2024年～2025年）の国内外のQNSC（Y-00）技術動向の調査の結果、本プロジェクトの当初目標を変更するような公開情報は無く、目標設定として妥当と考える。
しかし想定ユーザの社会実装に対する要求時期は当初より早まっており、このタイミングに合わせた目標の達成、研究開発の加速が必要である。

本件に関わる最新の技術動向

調査可能な範囲および公開情報では、中国から６件の論文が出ているが、いずれもQNSCの基本技術の理論的理解が浅いため、我々の進める研究を脅かす技術的な脅威はなく、本プロジェクトの達成目標を影響を及ぼすほどのインパクトのある研究開発ではない。また、特に社会実装を考慮した実用化研究の報告等は皆無（殆どが方式の基礎検討報告）であり、本プロジェクトで進める社会実装におけるための同期方式の開発や通信の安全性や安定性を実現するプロトコルに対する研究も見当たらない。しかし、論文数からもわかるように中国の意識は高く、本プロジェクトの開発を加速し、早期社会実装を実現する方向で進める必要がある。一方で特に実装に関わる研究開発の成果の情報公開においては慎重に進める必要がある。

本プロジェクトでの研究開発目標は、社会実装する上での実使用に耐えられる目標設定になっており、またプロジェクト自体も指定基金協議会に参加されている府省庁等を中心に、想定ユーザとの情報交換を積極的に実施し、具体的な実施要件や計画等も議論できていることなどを踏まえると的確な目標をとらえている。しかし、その活動の中で想定ユーザ内で情報通信におけるセキュリティ意識が想定以上に向上してきており、本プロジェクトの成果の早期社会実装に向けた取組を加速させる必要がある。現在、当初想定していた社会実装開始時期が２～3年早まる見通しであり、本プロジェクトもこの需要とタイミングに対応できるよう25年度で終了予定の研究開発項目〔1〕をプロジェクト終了時期まで延長し早期社会実装を実現する準備を開始している。

本プロジェクトでの知財の取り扱い（方針）

基本方針

アイディア毎に是々非々ではあるが、大きくは「権利化」「秘匿化」の何れかを選択することを想定。「非公開特許化」の扱いについては、本QNSC技術が国の定める特定分野には当て嵌まらない点を重視し、「非公開特許」制度を利用した「秘匿化」は実施せず、関係者外に全く情報を出さない企業内等で「秘匿化」を実施する方向で検討している。以上、「権利化」「秘匿化」の方針を纏めると以下のようになる。

「権利化」：コンセプトレベルのアイディアや顕現性のある技術については権利化を進める方針。ただし、これに該当するものであっても、出願（公開）することで、本技術の安全性(情報の難読性)が損なわれるようであれば、「秘匿化」する。

「秘匿化」：本技術で扱う技術の実装ノウハウ内容やアルゴリズム、また実装に向けた新たな方式等に関しては秘匿化する方針。これらは基本的に出願することで、安全性が損なわれる類の情報であると想定。例外的なアイディアにおいては、関係者・関係機関(※)との慎重な議論の上、権利化を図ることも考慮。　※関係者：PD/SPD、プロジェクトメンバ　※関係機関：内閣府、経済産業省、NEDO、防衛省等の関係省庁

本プロジェクトでの知財の取り扱い（活動状況）

知財運営委員会　体制

役割	所属	担当
委員長	日立製作所	研究代表者
委員	日立製作所	研究員
再委託先代表	東北大学	再委託先研究代表者
	慶應義塾大学	再委託先研究代表者
	富士通	再委託先研究代表者

実施内容

項番	実施日	内容
1	2024/9/4	第1回４者全体定例会議で予告
2	2024/10/15	会則決定(各機関合意)
3	2025/1/30	第2回４者全体定例会議で知財戦略において方針案を説明、決定
4	2025/11/28	第9回PD/SPD定例会議にて秘匿特許化について報告

知財運営委員会 2024年10月15日発足 (「知財・データ取り扱い合意書」締結および「知財運営委員会運営規則」合意)

なお知財マネジメント活動の状況は以下のとおりである。

① 国内外の技術動向においては、常に調査を継続し、関係する論文投稿等があった際にはいち早く情報の入手および内容の解析を行い、本プロジェクトの目標の影響度を確認し、対策し、プロジェクトの推進を遅滞することなく早期に対応を図ることができている。特に、各再委託先研究機関や各ステークホルダーとも単に定例だけでなく、想定以上に密にかつ柔軟に良好な連携（対面やリモートなど必要に応じたタイムリーかつ率直で組織間の壁を感じさせない本質的な打ち合わせ）がとれてきており、その内容は、情報共有だけでなく、拠点に集合し、集中的にアイディア出しや技術レビューを実施している。

② 早期社会実装を進める上で、想定するユーザとも密に情報交換を開始している。ユーザの機密事項になるので詳しい情報は開示できないが、実現場の環境および将来計画を踏まえ要件等の整理を始めている。いまのところ本テーマの計画を大きく乖離するところは無いが、それらの要件が出てくれば迅速に対応していきたいと考えている。このような活動を積極的に進めていることは、大きく評価することができると考えられ、今後も継続して進めていきたいと考えている。

＜評価項目２＞研究開発課題の達成目標に向けた進捗状況

(1) 研究開発課題の達成目標に向けた進捗状況（国内外との比較を含む）
(2) 今後の見通し（多様な分野における実現可能性含む）
(3) 指定基金協議会において合意された内容の進捗状況　※該当無し

研究開発項目〔1〕サマリ

〔1〕Y-00のデジタルコヒーレントの開発 における目標達成状況　　達成：○　未達成：×

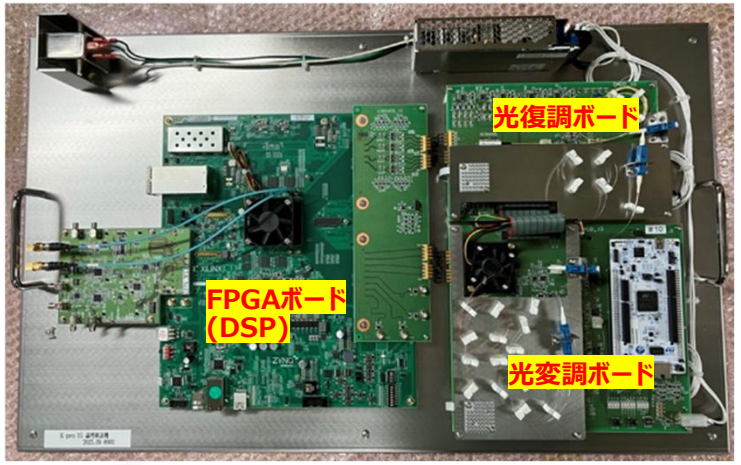
2024~25年度目標(実施計画書に基づく)	達成度	成果サマリ
PSK,QAMを基本とし1 Gbit/s程度の速度でのQNSCデジタル変復調技術を開発し、各方式の適用性について検討する。	○	ASK，PSK，QAMの各変調方式に対応したQNSCデジタル変復調方式を検討した。
QNSCの波形歪み等の補償処理を開発し1,000 km以上の長距離伝送を実現する。	○	光ファイバ伝送における主要な波形歪み要因である波長分散，偏波モード分散に対するデジタル補償技術を検討し、QNSC変調された信号に対しても有効であることを確認した。シミュレータによりアルゴリズム検討およびオフライン検証を行った後、FPGAによるリアルタイム実機検証により実現性を確認した。
FPGAによる論理検証用試作機を完成させ、実機による検証を実施、QNSCデジタルコヒーレント方式の基盤技術確立を目標とする。	○	従来にない、フルデジタル処理によるイントラダイン検波を適用したリアルタイム動作QNSC送受信技術を実現した。長距離伝送に適した方式としてQNSCデジタル変復調技術を適用したQPSK方式を採用し、リアルタイムで動作するレーザオフセット除去、光ファイバ起因の歪み補正処理を実装した論理検証用試作機を開発し、1GbEのQNSC伝送を検証した。

研究開発項目〔1〕 成果詳細

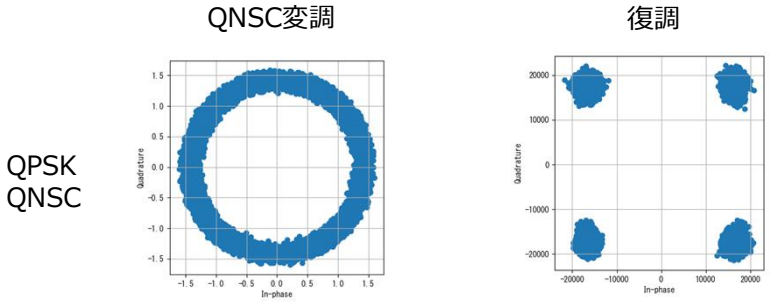
FPGAによる論理検証用試作機①

外観図①

外観図②



実機動作 (レーザ周波数オフセット：あり)

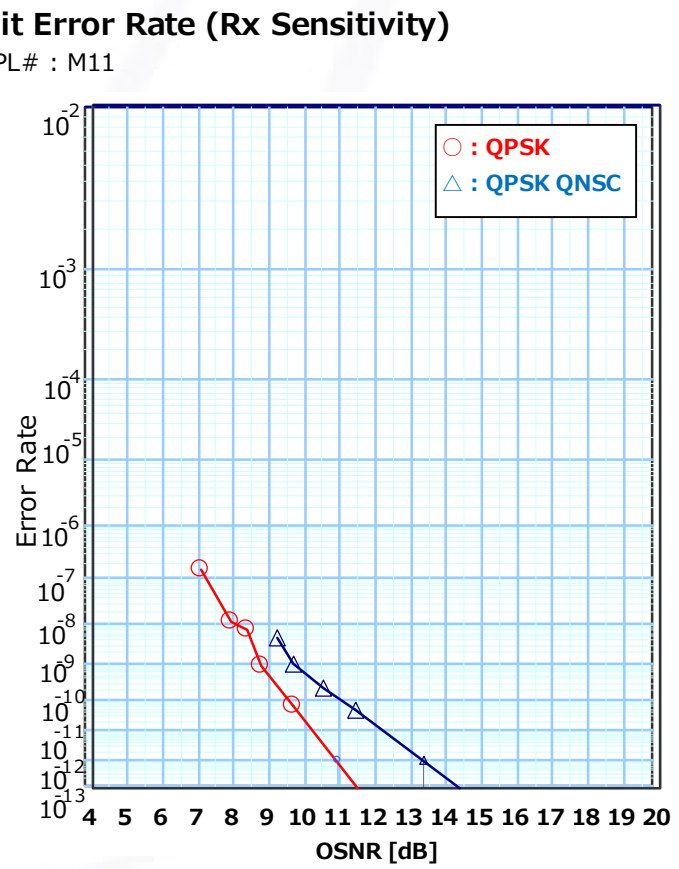


・コヒーレント光変復調機能
・フルデジタル処理によるイントラダイン検波技術
・適応等化 (波長分散補償、偏波分離) 技術
・QNSC信号処理技術

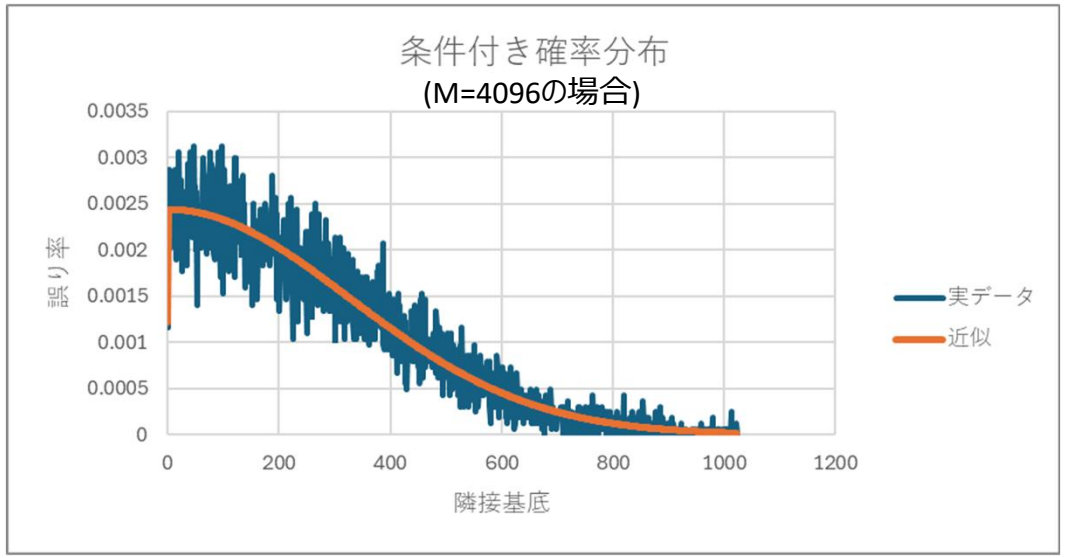
研究開発項目〔1〕 成果詳細

FPGAによる論理検証用試作機②

BER特性



QNSC性能
(条件付き誤り確率)



条件付き誤り確率 (真値に対して隣接基底レベルを検出する確率)
0.99878

マスキング効果
655

目標達成見込み　研究開発項目〔1〕サマリ

〔1〕Y-00のデジタルコヒーレントの開発 における目標達成見込み　　達成：○　未達成：×

最終目標(実施計画書に基づく)	達成見込み	状況サマリ
PSK,QAMを基本とし1 Gbit/s程度の速度でのQNSCデジタル変復調技術を開発し、各方式の適用性について検討する。	○	ASK，PSK，QAMの各変調方式に対応したQNSCデジタル変復調方式を検討した。
QNSCの波形歪み等の補償処理を開発し1,000 km以上の長距離伝送を実現する。	○	光ファイバ伝送における主要な波形歪み要因である波長分散，偏波モード分散に対するデジタル補償技術を検討し、QNSC変調された信号に対しても有効であることを確認した。シミュレータによりアルゴリズム検討およびオフライン検証を行った後、FPGAによるリアルタイム実機検証により実現性を確認した。
FPGAによる論理検証用試作機を完成させ、実機による検証を実施、QNSCデジタルコヒーレント方式の基盤技術確立を目標とする。	○	従来にない、フルデジタル処理によるイントラダイン検波を適用したリアルタイム動作QNSC送受信技術を実現した。長距離伝送に適した方式としてQNSCデジタル変復調技術を適用したQPSK方式を採用し、リアルタイムで動作するレーザオフセット除去、光ファイバ起因の歪み補正処理を実装した論理検証用試作機を開発し、1GbEのQNSC伝送を検証した。

研究開発項目〔2〕サマリ

〔2〕Y-00の高速光ファイバ通信の開発　における目標達成状況　　達成：○　未達成：×

2024~25年度目標(実施計画書に基づく)	達成度	成果サマリ
伝送速度20 Gbit/s以上、μsオーダーの低遅延、4,000値以上のQNSC多値変調の実現を目指し、主要デバイスの選定と入手を図る。選定結果と高速QNSC方式の設計結果を報告する。	○	高速な20 GS/s，16 bit-DA変換／12 bit-AD変換デバイスを選定し、複数のFPGAとの組み合わせにより暗号化多値度が4,000値以上のQNSC伝送装置を実現できる見通しを得た。 100 Gbit/sシステム用光学素子を選定し、これらの光学素子を用いたオフライン変復調試験を通じて復調信号に30 dB以上の高いS/Nが得られることを検証した。 システムを構成するFPGA送受信機および100 Gbit/s光学筐体の設計を終え、それらの1次試作を進めている。
光デバイスの小型化・可搬化および一次試作機の作製を2025年度内に完了させる。また、高速送受信機の一次試作を完了させる。	○	19インチラックサイズのユニットに収納した可搬型100 Gbit/s光学筐体の一次試作を完了した。 FPGA送受信機は高速ADC、DACチップの入手に時間を要したものの、年度内にこれらチップをFPGA装置内へ実装する目途が立った。

研究開発項目〔2〕 成果詳細

本開発での開発品の特徴

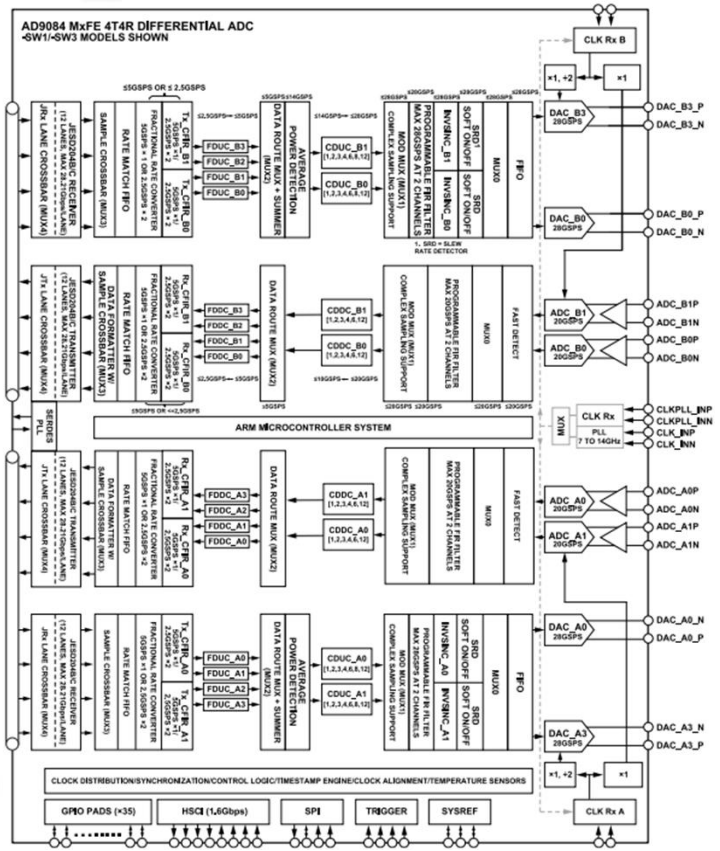
項目	20G試作機	100G試作機
研究主体	日立製作所	東北大学
検波方式	イントラダイン検波	ホモダイン検波
送受信波長同期	デジタル 周波数オフセット補償	アナログ 光注入同期によるレーザ波長同期
主眼	商用利用されているデジタルコヒーレント技術の発展型となるQNSC伝送技術の開発。 シンプルな光学系による将来的な装置の小型化。	高多値QAM変調をベースとする大容量伝送を見据えた高精度QNSC伝送技術の開発。 電気系の負荷低減による総合的な消費電力の削減。

研究開発項目〔2〕成果詳細（20G/100G共通）

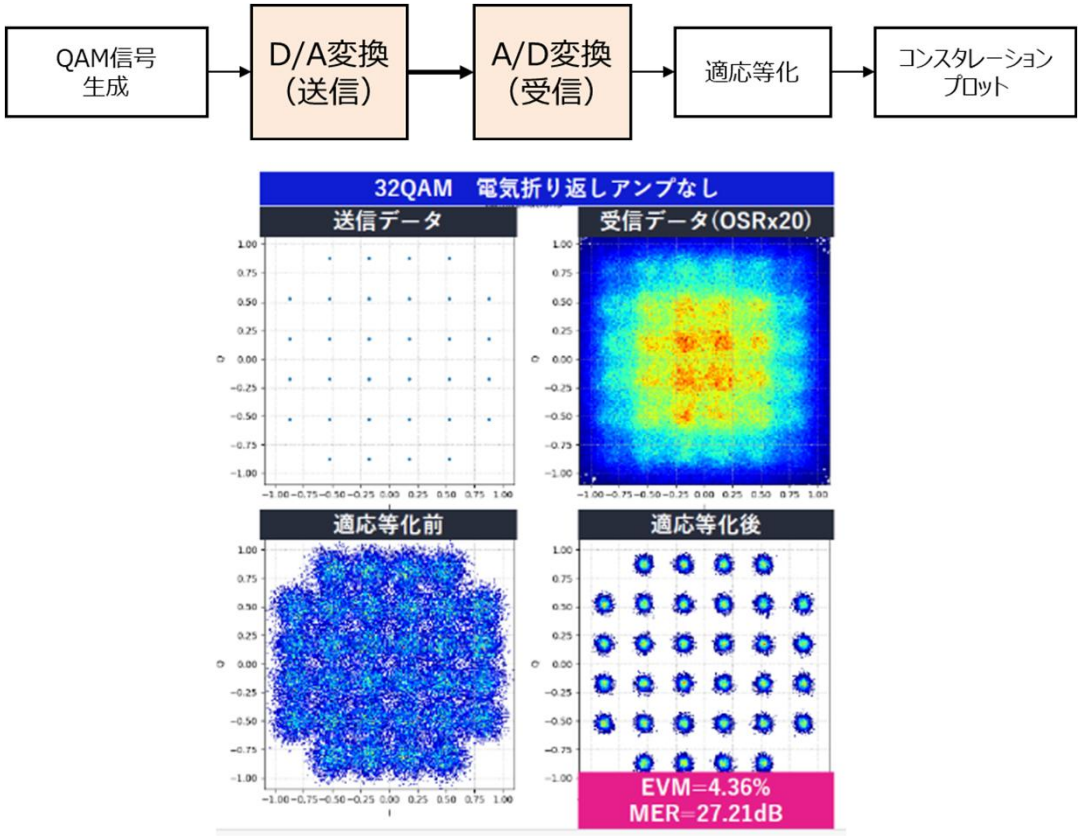
高速AD/DA (20G/100G共通)

デバイス概要

項目	仕様
ADC	チャネル数：4ch ビット幅：12 bit サンプリング速度：20 GS/s 帯域幅：18 GHz
DAC	チャネル数：4ch ビット幅：16 bit サンプリング速度：28 GS/s 帯域幅：18 GHz
パッケージ	24mm × 26mm、 0.8mmピッチ899ボールBGA

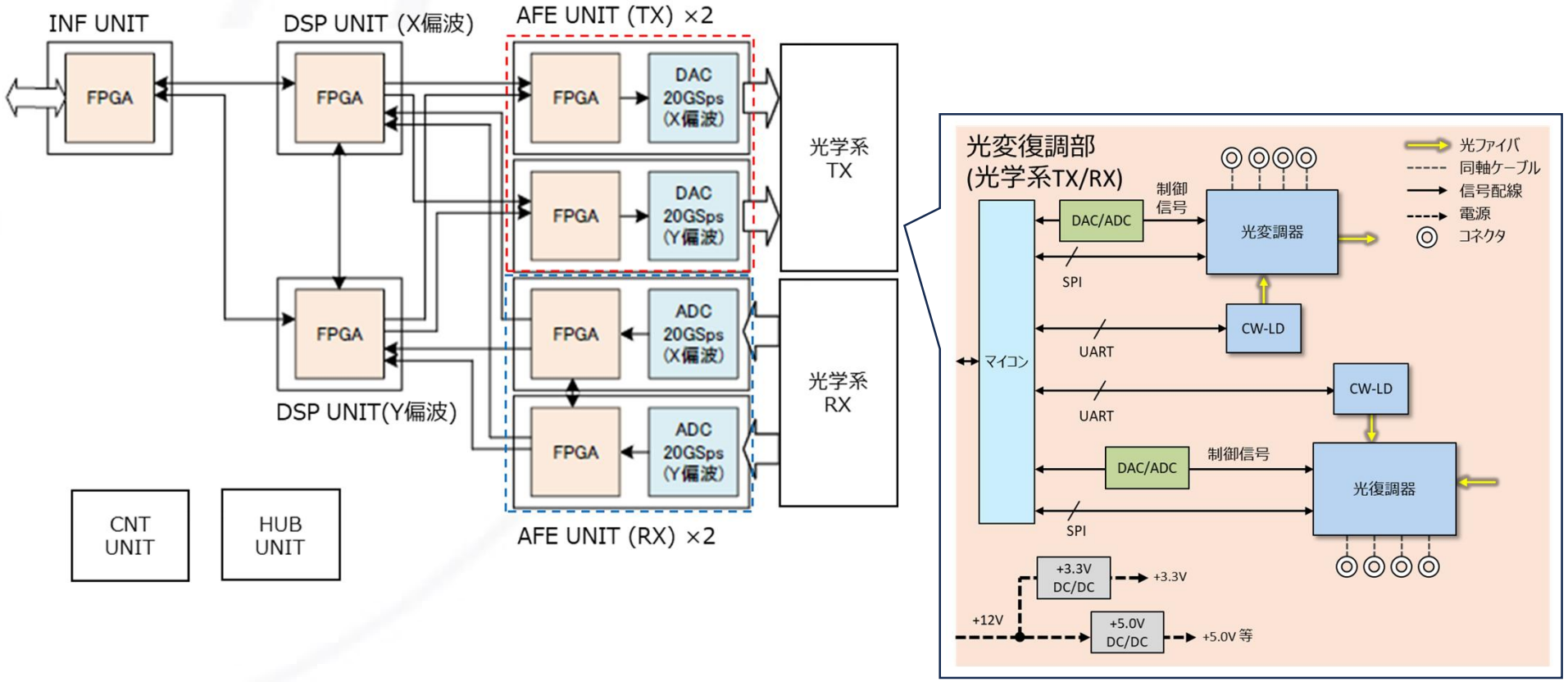


オフライン評価結果



研究開発項目〔2〕 成果詳細（20Gシステム）

装置構成 (20G)



目標達成見込み　研究開発項目〔2〕サマリ

〔2〕Y-00の高速光ファイバ通信の開発　における目標達成見込み　　達成：○　未達成：×

最終目標(実施計画書に基づく)	達成見込み	状況サマリ
20 Gbit/s試作機を完成し、報告に必要な検証実験を全て終了させる。	○	2025年度に完了予定の20 Gbit/s送受信機の1次試作機を改良し、双方向伝送可能な20 Gbit/sトランシーバを完成する。また、これを用いて1,000 kmを超える高秘匿光伝送の実証試験を達成する見込みである。
高速光デバイスの 1 次試作機の評価および改良試作を実施の上、長距離伝送・WDM伝送実験を実施する。そして1 Tbit/s 以上の大容量化に向けた WDMシステムの設計指針を立てる。	○	2025年度に完了予定の100 Gbit/s送受信機の1次試作機を改良し、これとWDM伝送系とを組み合わせ、1 Tbit/s以上の大容量光秘匿伝送の実証試験を達成する。具体的には、1台のCW光源と光変調器（コムジェネレータ）を組み合わせた安価な構成の10 ch以上のWDM光源、ならびに80 km×7スパンの560 km長距離伝送系の準備が既に整っており、これらを用いて最終目標を達成する見込みである。

研究開発項目〔3〕サマリ

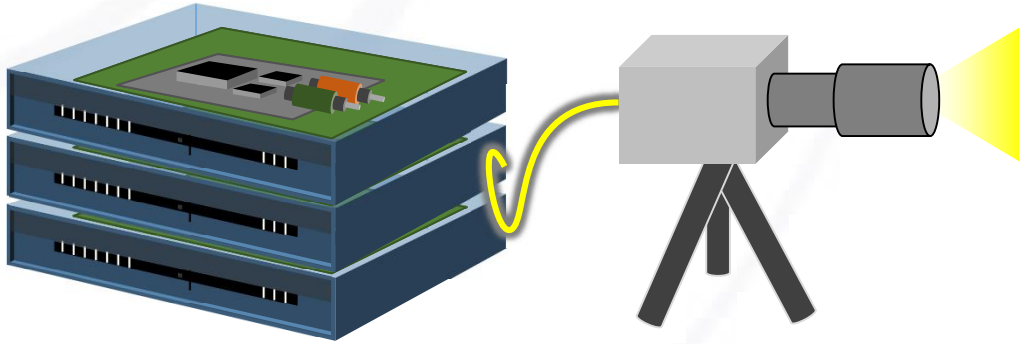
〔3〕Y-00の高速光ワイヤレス通信の開発　における目標達成状況　　達成：○　未達成：×

2024~25年度目標(実施計画書に基づく)	達成度	成果サマリ
〔1〕〔2〕の成果を利用し、QNSCを適用した光ワイヤレス伝送を実現することを目標とし、高速なQNSC再同期方式の確立を図る。当該機能を盛り込んだ光ワイヤレス通信用DSPの開発結果を報告する。	○	再同期処理の高速化に対し以下の方針に沿って詳細設計を行う方針とし、開発結果を報告した。 ①歪み補正処理の最適化 ②光遅延検波方式の採用 ③光信号瞬断後のQNSCパラメータ共有方式の見直し
〔1〕〔2〕で検討した変調方式を光ワイヤレス通信へ適用展開するための基本設計を完了し、光アンテナの詳細設計を完了させることを目標とする。光ワイヤレス通信用光モジュールの開発結果を報告する。	○	集積コヒーレントレシーバを利用した光遅延検波方式を考案し基本設計を完了した。光ファイバインタフェースの光アンテナの詳細設計を完了し、開発結果を報告した。また、製造に着手した。

研究開発項目〔3〕 成果詳細

光ワイヤレスQNSC検証機の構成

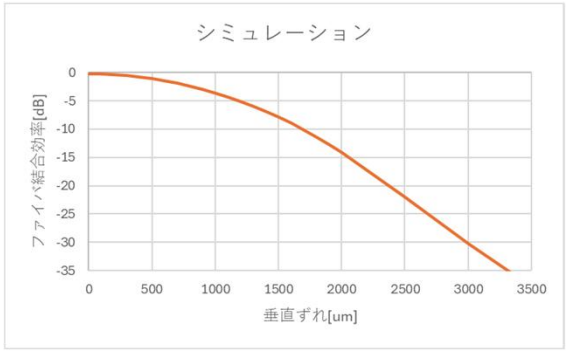
光ファイバQNSC伝送装置をベースとして光ワイヤレス用に復調方式等を最適化(遅延検波)、光軸合わせなどの光アンテナ部を新規設計

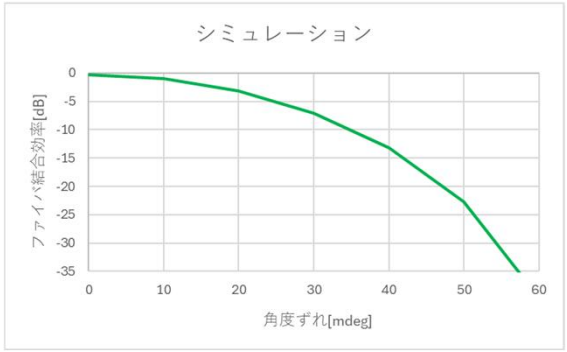


光ワイヤレス対応QNSC伝送装置

研究要素：
・検波方式の最適化(遅延検波方式)
・リンク高速化(暗号同期、他)
・ビームトラッキング技術

光軸ずれの検討





研究開発項目〔3〕 成果詳細

高速化のアプローチ

アプローチ	成果サマリ
歪み補正処理の最適化	光ファイバ伝送とは異なる光ワイヤレス伝送特有の歪み要因を特定し、歪み補正処理を最適化することによりDSP処理時間を短縮する。
光遅延検波方式の採用	受信光を分岐、遅延したのち光干渉する光遅延検波方式を採用し、送受間のレーザ周波数差に起因する周波数同期処理に要する時間を削減する。
光信号瞬断後のQNSCパラメータ共有方式の見直し	光信号瞬断後のQNSCパラメータ共有方式を見直し、再同期に要する時間を短縮する。

目標達成見込み　研究開発項目〔3〕サマリ

〔3〕Y-00の高速光ワイヤレス通信の開発　における目標達成見込み　　達成：○　未達成：×

最終目標(実施計画書に基づく)	達成見込み	状況サマリ
光ワイヤレス通信を実現する光アンテナと〔2〕で開発したQNSC（Y-00）装置を改造し結合させたQNSC（Y-00）光ワイヤレス通信装置を完成させる。この装置を用いて自由空間での伝送実験を実施し、各機能の有効性を確認する。	○	2025年度に完了予定の光アンテナと、2026年度に完了予定の20 Gbit/s送受信機を一部改造したQNSC伝送装置を結合し、光ワイヤレス伝送可能な10 Gbit/sトランシーバを完成する。また、これを用いて100 m程度の高秘匿光ワイヤレス伝送の実証試験を行い、目標を達成する見込みである。

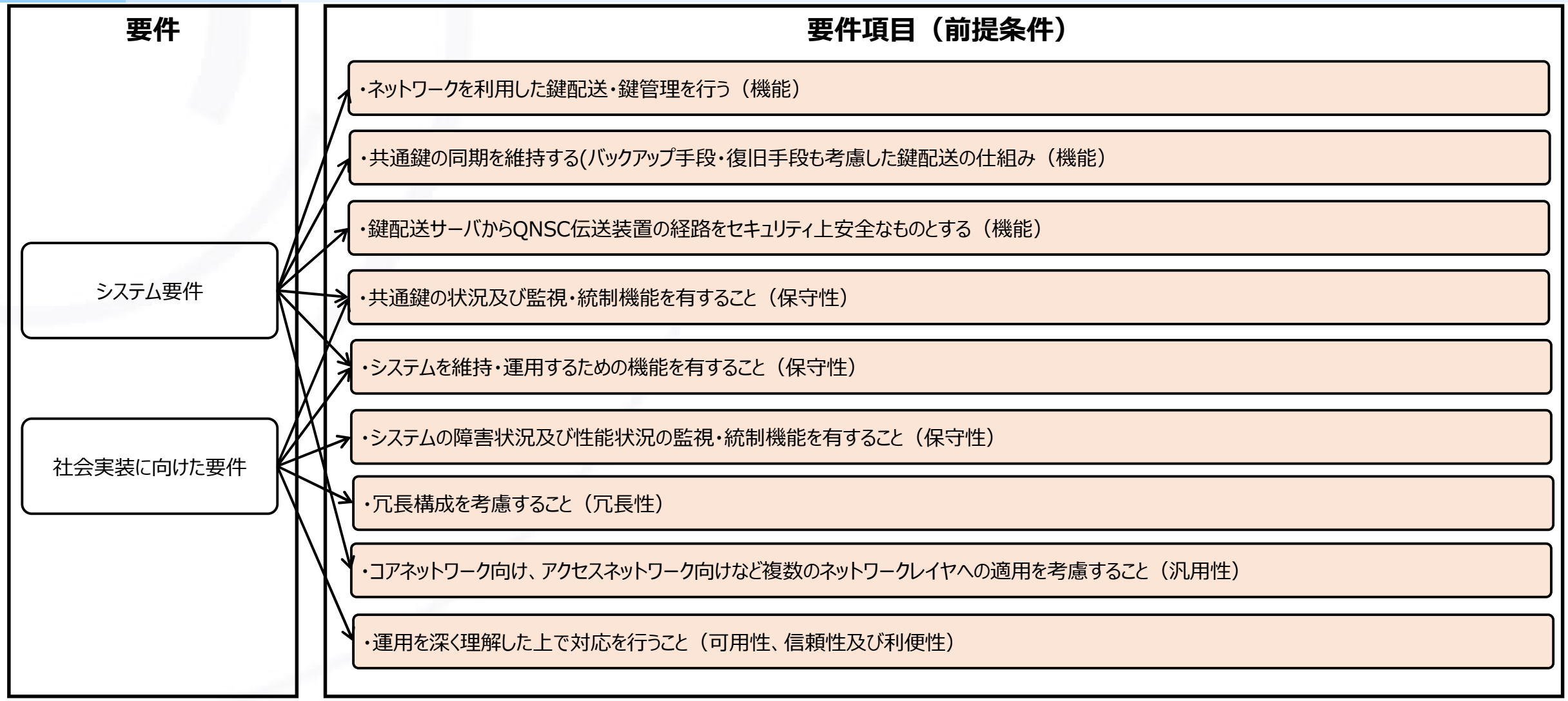
研究開発項目〔2〕〔3〕セキュア管理システム　サマリ

〔2〕〔3〕セキュア管理システム　における目標達成状況

2024~25年度目標(実施計画書に基づく)	達成度	成果サマリ
テストベッド構築に向け、セキュア管理システムの基本~詳細設計を完了させ、当該システム及びテストベッドの構成案をまとめる。	○	・社会実装を想定したQNSC伝送装置で構成するネットワーク形態とシステムのライフサイクルについて検討した。 ・セキュア管理システムの基本構成について整理し、システムに求められる機能の基本設計と詳細設計を完了した。 ・制御PCをQNSCの鍵管理を想定にテストベッド構成案をまとめた。
セキュア管理システムの安全性検証構想を完了させ、リモートアテステーション機能の基本構成検討と、その安全性検証結果をまとめる。	○	セキュア管理システムの安全性検証として、評価対象のモデル化、情報資産の抽出、脅威分析等を実施した。通信路のリスクに加えて、通信路を流れるデータ自身へのリスクが高いことを明らかにし、エンドツーエンドでの認証・署名・暗号処理によるリスク低減を図ることを構想とした。 リモートアテステーション機能について、証明書の連鎖構造、検証側での実行手順を定義した。また、安全性検証が可能な環境を構築し、適切に動作することを確認中である。

研究開発項目〔2〕〔3〕セキュア管理システム　研究開発内容

要件抽出（機能要件）



研究開発項目〔2〕〔3〕セキュア管理システム　研究開発内容

要件抽出（脅威分析）

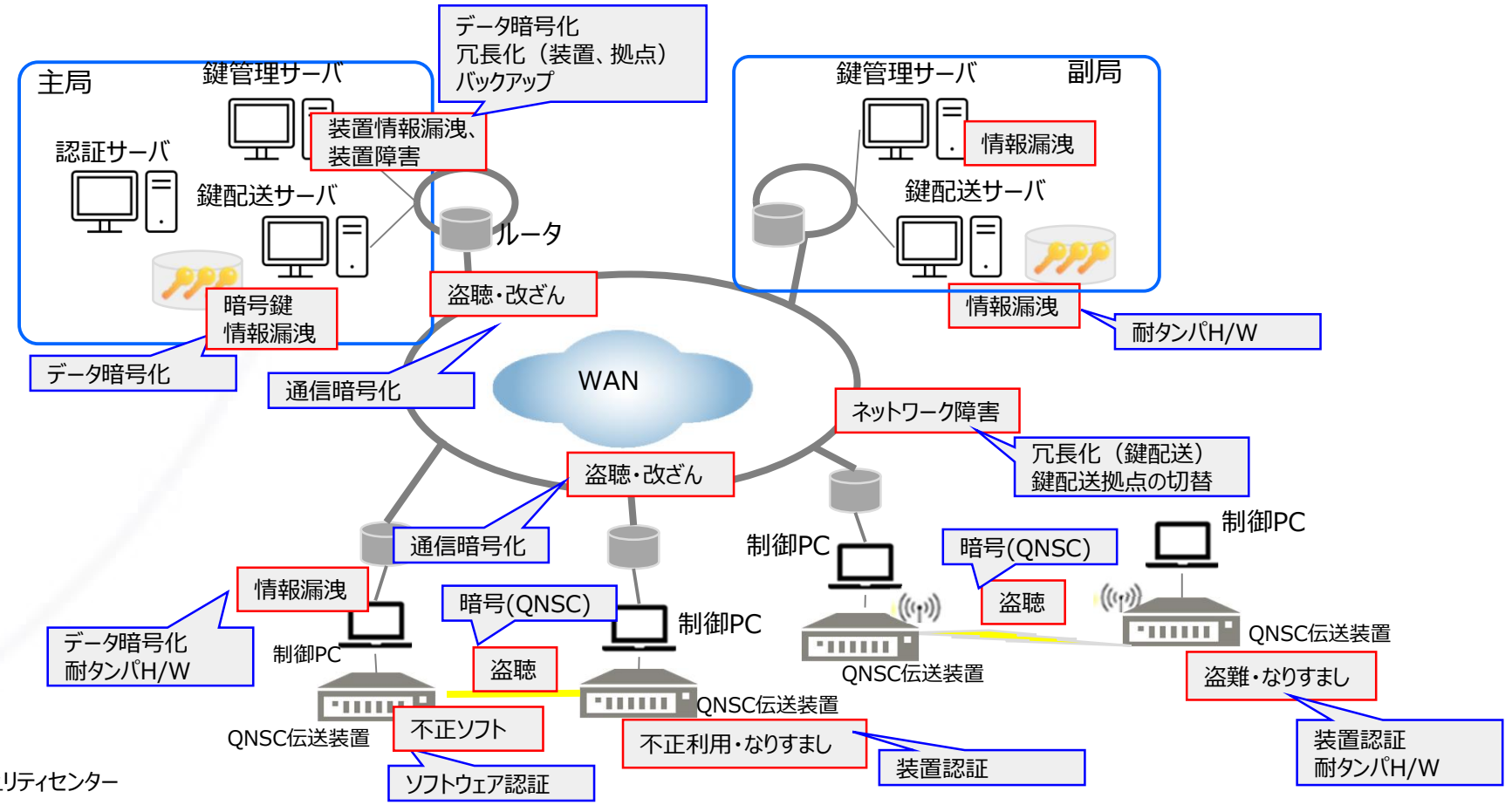
社会実装のネットワーク構成における脅威と対策

トラステッド領域を基本に社会重要インフラの可用性を考慮した対策（社会実装のネットワーク構成（接続）モデルを対象に検討）

・鍵配送をサービス提供をポイント
　ー装置障害への対応（冗長化）
　ー鍵配送拠点（主局／副局等）

・ネットワーク回線の障害
　ー拠点冗長化
　ー鍵配送拠点の切替（主局／副局等）

・制御PC＋QNSC伝送装置のソフトウェア
　ー不正ソフトウェアへの対応
　ーデータ管理への対応



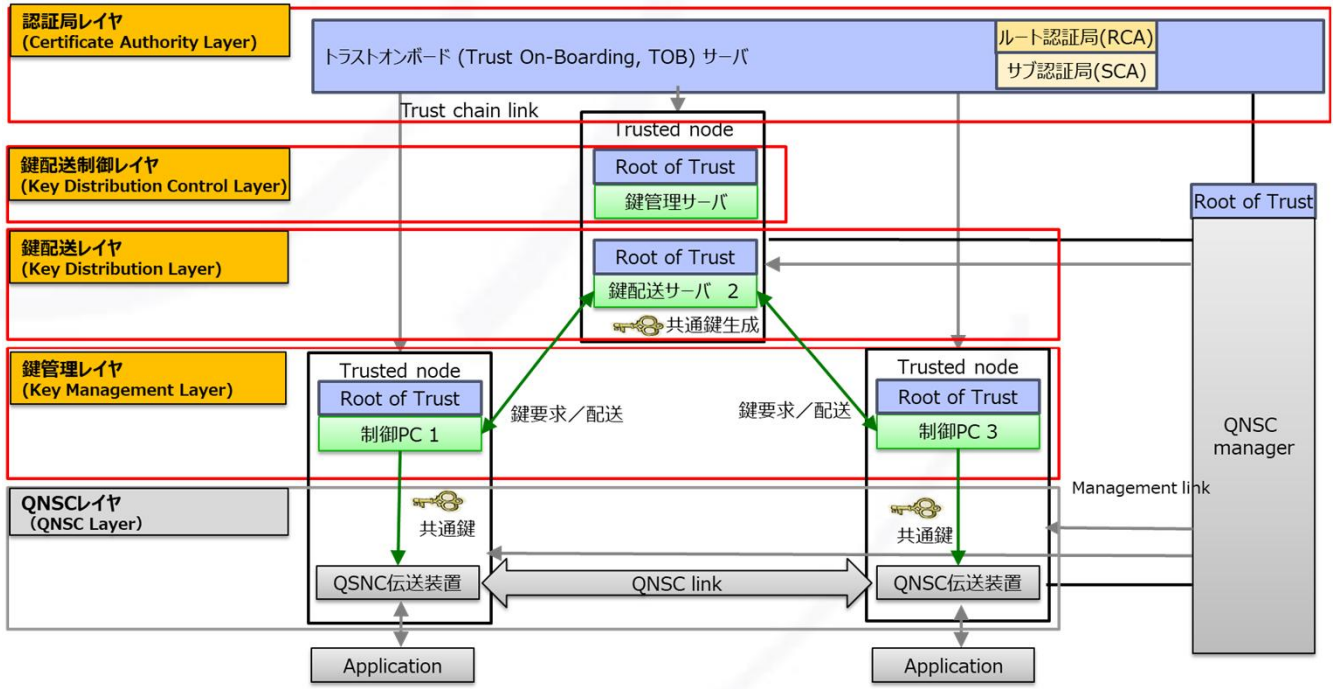
参考文献:独立行政法人　情報処理推進機構　セキュリティセンター
IoT開発におけるセキュリティ設計の手引き

研究開発項目〔2〕〔3〕セキュア管理システム　研究開発内容

システム構成（鍵管理モデル）

QNSC鍵管理モデル

QNSC伝送装置を構成するネットワークにおける鍵管理のアーキテクチャーを４つのレイヤを定義し、役割を定義した。

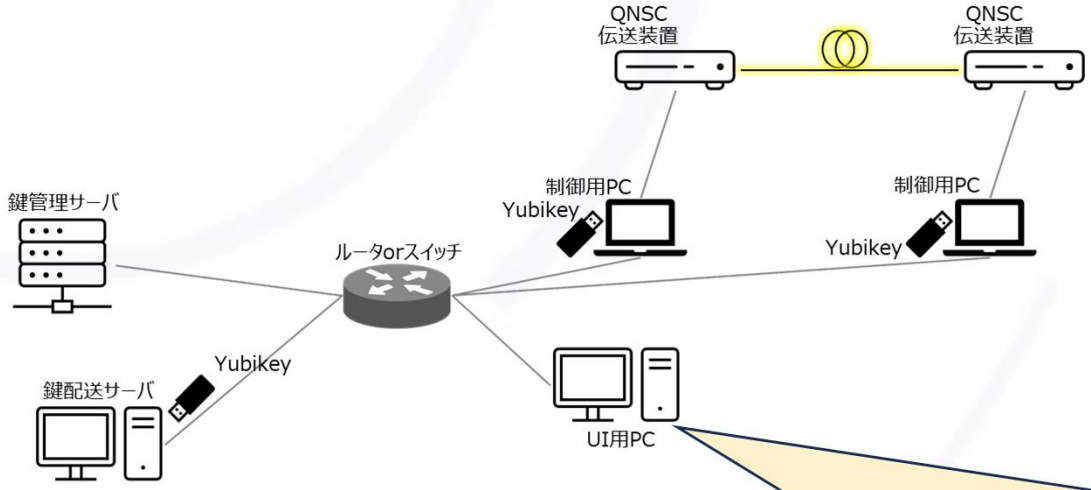


No	レイヤ	役割
1	認証局レイヤ	ルート認証局・サブ認証局の証明書を格納では、証明書チェーン検証を実現するため、装置のRoT（Root of Trust）内に信頼の基点となるルート認証局・サブ認証局の証明書を格納する。
2	鍵配送制御レイヤ	暗号通信を行うQNSCレイヤを管理する鍵管理レイヤの制御PC情報および保管されている鍵情報／運用している鍵情報を管理する。
3	鍵配送レイヤ	鍵管理レイヤ（制御PC）から共通鍵の要求に対して登録された装置およびQNSC伝送装置で通信可能な状態（ペア）を確認を行い、配送可能な状態のみ共通鍵を配送する。また、配送された鍵の状態取得および失効／破棄を通知する機能が含まれる。
4	鍵管理レイヤ	制御PCに実装されるQNSCコントローラから鍵配送レイヤへの共通鍵の要求および受領した鍵を管理する。またQNSC伝送装置への鍵の供給／破棄を制御する。
5	QNSCレイヤ	QNSC伝送装置がこのレイヤに位置し、鍵管理レイヤから鍵の供給を受けて暗号通信を行う。

研究開発項目〔2〕〔3〕セキュア管理システム　研究開発内容

検証（機能試験・セキュリティ機能）

右下図は、QNSC伝送装置の鍵状態などを示す、検証用に開発したUI画面。
本UIにて装置の共通鍵が正常に更新されていくこと、共通鍵配送にあたっての認証・署名・暗号処理が正常に動作することなどを検証する。



伝送装置

QNSC伝送装置　(S)[002]　通信中　閉じる

鍵更新ステータス：　手動鍵更新トリガ　実行

項目名	送信側	受信側
鍵番号	12	12
鍵状態	利用	利用
復号乱数列	000102030405060708090A0B0C0D0E0F10111213141516171819 1A1B1C1D1E1F202122232425262728292A2B2C2D2E2F30313 233343536373839 3A3B3C3D3E3F404142434445464748494A4B 4C4D4E4F505152535455565758595A5B5C5D5E5F6061626364 65666768696A6B6C6D6E6F707172737475767778797A7B7C7D 7E7F	000102030405060708090A0B0C0D0E0F10111213141516171819 1A1B1C1D1E1F202122232425262728292A2B2C2D2E2F30313 233343536373839 3A3B3C3D3E3F404142434445464748494A4B 4C4D4E4F505152535455565758595A5B5C5D5E5F6061626364 65666768696A6B6C6D6E6F707172737475767778797A7B7C7D 7E7F
生成共通鍵	000102030405060708090A0B0C0D0E0F	10111213141516171819 1A1B1C1D1E1F

装置ステータス：

警報名	状態	警報名	状態	警報名	状態
サーバ間認証失敗		送信側 鍵情報喪失		Line-LOS	
署名検証失敗		送信側 鍵情報不足		Line-LOF	
乱数列復号失敗		受信側 鍵情報喪失		Line-LOM	
サーバ間通信異常		受信側 鍵情報不足		Line-RDI	
鍵更新失敗		GCC-Tx-FAIL		QNSC-OOS	

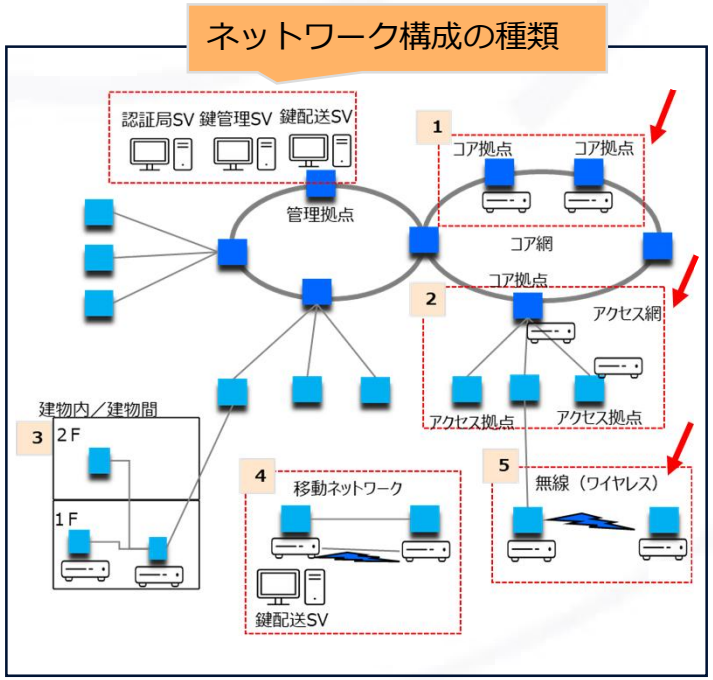
研究開発項目〔2〕〔3〕セキュア管理システム　研究開発内容

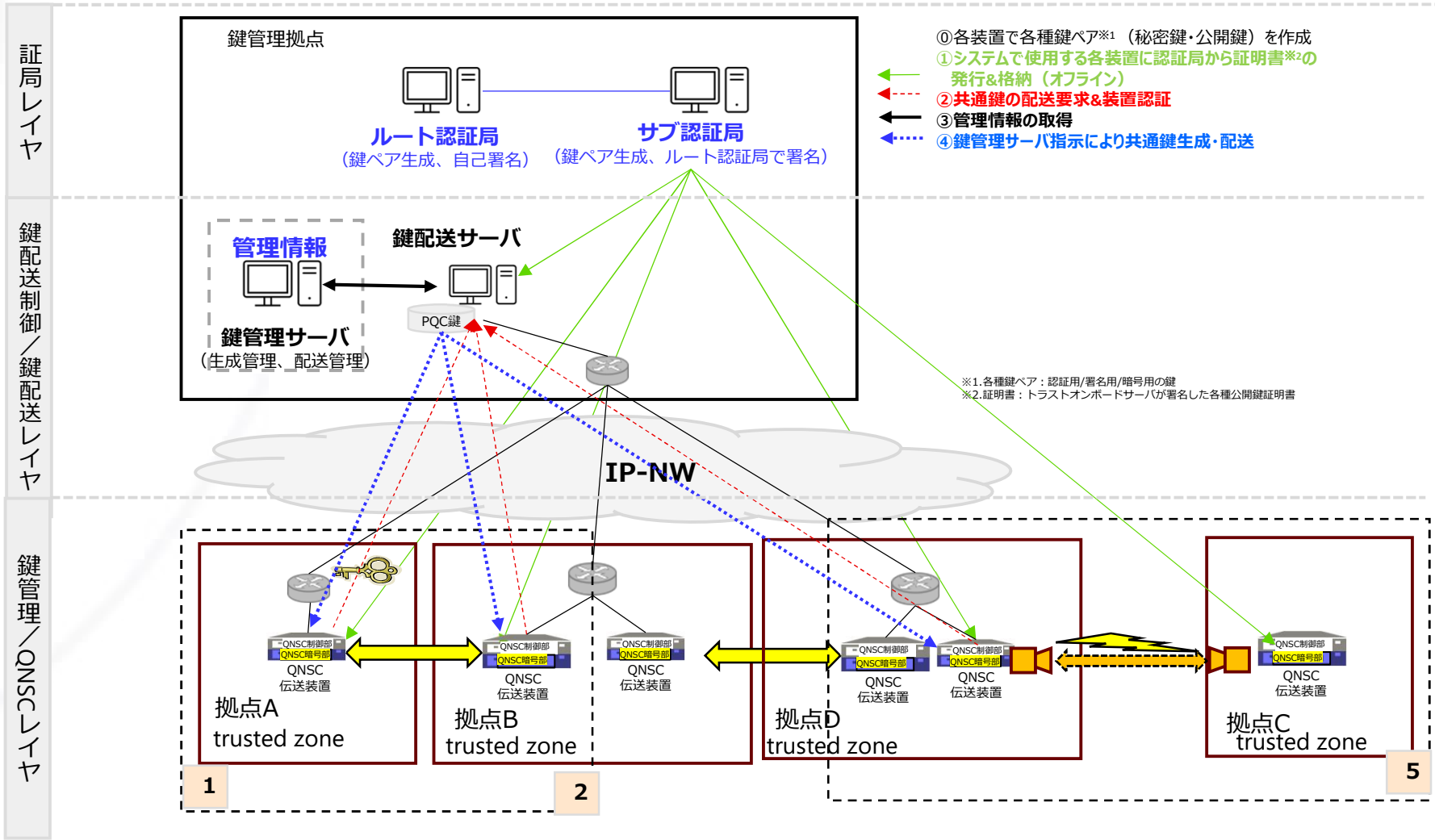
検証（テストベッド構成案）

テストベッド構成案

ネットワーク構成の種類のモデルと右図に記載している拠点Ａ／Ｂ／Ｃ／Ｄの関係は以下に示す。

- 「１」：コア拠点(拠点Ａ)ーコア拠点(拠点Ｂ)
- 「２」：コア拠点(拠点Ａ)ーアクセス拠点(拠点Ｂ)
- 「５」：アクセス拠点(拠点Ｄ)ー無線（拠点Ｃ）





目標達成見込み　研究開発項目〔2〕〔3〕セキュア管理システム　サマリ

〔2〕〔3〕セキュア管理システム　における目標達成見込み

最終目標(実施計画書に基づく)	達成見込み	状況サマリ
実運用形態を想定したセキュア管理システムのテストベッドを構築し、有効性・適用性を確認する。	○	認証レイヤ～鍵管理レイヤまでの動作確認完了。 一次検証による制御PC－QNSC伝送装置のICD設計で定義した正常／異常状態の確認が完了。
光ワイヤレス通信装置にセキュア管理システムを統合	○	光ワイヤレス構成の想定はスレーブ側装置への共通鍵をマスタ側装置から中継する仕組み基本構想を社会システム実装モデルで検討した。装置認証を含めた配送設計を制御PC内部のQNSCコントロール部で実現ができる見込みである。

研究継続による想定効果

- Cryptographic agilityへの対応（遠隔監視による鍵管理）
- 社会（特に想定ユーザ）の重要インフラ適用に必要な「可用性」「拡張性」「事案への対応方法」の確立

研究成果の社会実装に向けた活動

(1) 想定市場

省庁内/間ネットワークにQNSC（Y-00）光伝送装置およびシステムを提供する事業を想定。また、次ステップとして、重要社会インフラの通信網や金融などの高セキュア専用線サービスをターゲットに、通信事業者を中心にQNSC（Y-00）光伝送装置およびシステムの普及を目指す。

(2) 実用化・事業化に向けた計画等

2025年度までの成果により、QNSC（Y-00）光伝送の高速化・伝送距離延伸の見通しが得られた。本プロジェクトの成果は、その後の製品化開発を経て2031年以降の社会実装を想定していた。しかし想定市場におけるニーズの高まりを踏まえ、伝送速度要求に応えつつ2年程度の社会実装の前倒しが見込める10 Gbit/s QNSC光伝送装置の開発を本プロジェクトの枠内で実施することを検討・提案している。

＜評価項目３＞マネジメント

(1) 実施体制
(2) 研究資金の効果的、効率的な活用
(3) 国民との科学・技術対話に関する取組

実施体制

日立製作所

研究開発〔1〕Y-00のデジタルコヒーレントの開発
研究開発〔2〕Y-00の高速光ファイバ通信の開発
研究開発〔3〕Y-00の高速光ワイヤレス通信の開発
・全体纏め・方針策定
・デジタルコヒーレント適用Y-00
・システム・基本設計
・検証（性能、安全性、実環境）

Y-00コアを活用した装置開発実績

再委託(高速光ファイバ通信装置)

東北大学

研究開発〔2〕Y-00の高速光ファイバ通信の開発
・光ファイバ通信の高速化技術
・光デバイス構成
・100G高速光ファイバ通信装置の基本設計

超高速QNSC(70 Gbit/s/波長)の実績活用

再委託(セキュア管理システム)

慶應義塾大学

研究開発〔2〕Y-00の高速光ファイバ通信の開発
研究開発〔3〕Y-00の高速光ワイヤレス通信の開発
・セキュア管理システムの方式設計、基本設計
・セキュア管理(認証)システムの実装

サイバーセキュリティ研究の実績活用

再委託(セキュア管理システム)

富士通

研究開発〔2〕Y-00の高速光ファイバ通信の開発
研究開発〔3〕Y-00の高速光ワイヤレス通信の開発
・セキュア管理(鍵配送)システムの実装
・セキュア管理システムのネットワーク検証

省庁間NW、防衛基幹NWの実績活用

実施体制(補足説明)

- 事業遂行にあたっての技術力・事業能力について、下表に記す。
- 研究開発体制としては、委託先である日立製作所から再委託先の東北大学・慶應義塾大学・富士通への指示/業務委託を行う形態で統一し、責任分担等についても文書（プロジェクト管理基準）に規定・合意の上、業務を遂行している。
- 日立製作所主催で各再委託先機関とは**テーマ毎に毎週の技術定例会議**にて連携するとともに**四者合同の定例会議を1回/四半期**の頻度で開催し、全体的な方向性の共有と機関間の連携強化を図っている。（その他逐次対面、リモート会議を実施）

機関名	事業遂行にあたる技術力・事業能力
日立製作所	日立グループ内で、QNSCであるY-00プロトコルの研究開発黎明期(2002年頃)より当該プロトコルの実装技術を中心に装置開発を実施。現在は当該技術を日立製作所内に集約し研究開発及び事業化を推進中である。2.5 Gbit/s IMDD方式Y-00試作機の開発の他、RF無線通信や光ワイヤレス通信への応用の基礎研究等を進めている。
東北大学	超多値QAM光伝送技術の研究開発に従事しており、当該技術の物理レイヤ暗号への親和性に着眼し暗号技術としてQNSCを提唱。QKD/QNSC融合技術の提案や、DWDMとの組み合わせによるQNSCの10 Tbit/s伝送を世界で初めて実現。QNSC技術を世界に先駆け開発しており、FPGAを用いたリアルタイム伝送技術も有する。
慶應義塾大学	令和3,4年度「我が国が戦略的に育てるべき安全・安心の確保に係る重要技術等の検討業務」等の研究において、サイバーセキュリティ領域を個別調査分析し、報告書のとりまとめを行うなど、サイバーセキュリティ領域における研究・分析に実績を有しており、セキュア管理システムのリモートアテステーション機能の研究に最適である。
富士通	セキュリティ脅威・リスク分析に基づき、想定ユーザにおけるサイバーセキュリティに対応したインフラ基盤構築、及び、ネットワークにおける鍵管理システムの設計・開発・運用実績を有する。また、QNSC技術の実用化研究にも取り組んでおり、導入から運用まで考慮した耐量子コンピュータ性能に対応したセキュア管理システムの研究に最適である。

研究資金の活用状況

- 研究資金の活用状況について、下表に記す。
- 技術推進委員会については2025/9/2に実施、各委員のご指摘への対応状況は本資料にて記載済み。

項目	2024年度(実績)	2025年度(予定)	2026年度(想定額)	2027年度(想定額)
研究開発費 (単位: 百万円, 税込)	593	1,007	692 266(当初想定額からの増額)	70 60(当初想定額からの増額)
項目〔1〕概況	QNSCコヒーレント伝送に関わるデジタル処理方式及び光学系の検討、それに連なる検証用部材費、機能分割・実装作業に活用	24年度に引き続き機能分割・実装作業、および論理検証機の初期設計費・製造費用に活用中	【当初予定】当初計画上は、当年度での資金活用は無し 【追加予定】25年度までの成果を応用し、早期社会実装のため10 Gbit/sへの拡張を予定 諸検討及び検証用部材費への活用を想定	【当初予定】当初計画上は、当年度での資金活用は無し 【追加予定】10 Gbit/sへの拡張にあたり、検証機の評価や報告書作成に係る研究員費を想定
項目〔2〕概況	QNSCコヒーレント伝送に関わるデジタル処理方式の検討、当該方式の高速/並列化を考慮した機能分割検討作業に活用	24年度に引き続き機能分割作業、機能実装作業、および機能分割した各構成要素の初期設計費・製造費用に活用中	25年度に製作した高速伝送装置に対する検証および機能改善などへの活用を想定	主に機能改善に関わる動作確認・検証や報告書作成に係る研究員費を想定
項目〔3〕概況	光学系の机上検討に要する基本的な環境構築に活用	光アンテナなどの構成・機能検討、それに連なる実装作業、初期設計費・製造費用に活用中	25年度に製作した光アンテナおよび高速伝送装置に対する検証および機能改善などへの活用を想定	主に報告書作成に係る研究員費を想定
セキュア管理システム概況	セキュア管理システムの基本となる構成の検討、それに連なるソフトウェア機能の検討作業や構成要素の機材購入に活用	24年度に引き続きソフトウェア機能の検討作業・コーディング・検証等に活用中	25年度に製作したセキュア管理システムの機能拡張、ワイヤレス装置対応などの機能追加への活用を想定	主に報告書作成に係る研究員費を想定

対外的な成果発表

現在各テーマにおいて開発進行中であり、最短期間で進めている研究開発項目〔１〕においても評価中であり公開できる資料は纏まっていない。

但し、想定ユーザ内で開催される展示会等において、Kプロ事業紹介としての出展は行っている。