「量子鍵配送技術（QKD）、耐量子暗号技術（PQC）の課題と将来展望」

- 量子鍵配送技術（QKD）の技術と商業化の課題
- 耐量子暗号技術（PQC）システム実現に向けた取り組み
- 量子暗号通信技術の実社会での活用事例とその影響

講師（講演順）

（座長 —— 総合司会） 東京大学 名誉教授 **齊藤忠夫氏**

東芝デジタルソリューションズ株式会社
ICTソリューション事業部ビジネスユニットマネジャー **花井克之氏**

日本銀行金融研究所 参事役 **宇根正志氏**

NTTコミュニケーションズ株式会社 イノベーションセンター
技術戦略部門/IOWN推進室 主査 **森岡康高氏**

事務局 ハイテクノロジー推進研究所 〒150-00036 渋谷区南平台町15-12 南平台アイアイビル2F TEL 03(6416)0190㈹ FAX 03(6416)5351

「マルチメディア推進フォーラム」のご案内

明日の社会発展をリードする情報通信を目指して

情報通信技術が人類の新しい生き方を作り出し、新しい社会を作り出していることは、21 世紀に入ってから一般の人々を含め広く認識されるようになった。歴史的にも、人間は近くにいる人々との対話によって協力関係を構築し、グループで力を発揮することによって世界を変化させてきた。通信技術は対話の範囲を広げその能力を強化している。

マルチメディア推進フォーラムは日本の情報通信の発展のために、新しい技術とサービス、その社会的対応と法制度などを多角的に議論するフォーラムである。1990 年ころから準備を進め、1994 年からは現在の名称となって多くの方々の支援を得て、独占から競争へ、電話からインターネットへ、固定から携帯への変化をとらえ様々に論じてきた。特に情報通信ネットワークのサービスが競争環境で行われるようになった今日、競争状況のなかでなお、ネットワーク事業者は接続されるネットワークについて相互に理解し協力しなければサービスは成立しない。そのためには多くの事業者が相互に理解するチャンネルをオープンに持つことが不可欠であり、本フォーラムでの議論はネットワークサービスの円滑な発展のためにも貢献していると考えている。

通信技術はその発生以来、人と人が交信する技術として発展してきたが、21 世紀に入り世界のすべての人が端末を持つようになり、市場は飽和してきた。また通信端末は長く固定端末であったが、携帯端末が主流を占めるようになってきた。このような展開は 20 世紀には見られなかったことで、21 世紀に入ってからの変化は急激である。コンピュータに代表される情報技術は 70 年前に実現したが、ムーアの法則による超小型化の進展によって社会の隅々に情報処理技術を広げてきている。コンピュータの能力は高まり、大量情報の取り扱いによって、過去においては取り扱いが困難であった巨大な情報に適用することにより、いままで気が付かなかった現象を分析し、われわれの知識を増やしつつある。このような技術は、すべての社会活動の基礎として広く産業化され、社会化されるようになっている。

多くの情報は社会の様々な場面で発生する。それぞれの場面には多様な産業がある。家庭では家庭用の機器産業がある。鉄道では交通サービス産業がある。エネルギーを供給する電力産業、医療事業、自動車産業など多様な産業も情報処理と通信の技術を活用しながらサービスを展開しつつある。このような技術における通信は M2M 通信（機械と機械の通信）と呼ばれるが、多様な背景を持つ技術の M2M 通信について、その初期には産業分野ごとに通信ネットワークを構築する議論も稀ではない。しかし、各分野が独自に情報通信設備を構築することは現実的でない。M2M ネットワークの本質を理解しつつ、共通の通信インフラストラクチャを構成することは情報通信産業に課せられた課題である。同時に情報通信産業は個々のアプリケーションを形成する活用技術について、その特質を理解しなければならない。そのためには、技術を技術としてだけ論ずるのでは不充分である。技術を国際的視野から、社会的な側面を含めて分析し、関連する産業、法制度との整合性を含めて理解することが重要である。時には産業構造の変革、法制度の見直しを考えることも話題になろう。

マルチメディア推進フォーラムは、情報通信技術の多様な発展について論じつつ、新しい市場の特性を理解した幅広い問題を考慮しながら、情報通信事業とサービスの将来を論じたいと考えている。

ICT はますます多様化し、産業としても社会としても重要性を増している。社会の ICT 化はその社会が国際的に競争力を維持するための基本的要素となっている。マルチメディア推進フォーラムはそのための技術、社会、普及の条件等を幅広く討議し、競争力のある社会を形成する方策について議論を進めている。今日に至る情報通信技術の変革期の中で、その適切な発展のために当フォーラムの果たして来た役割は大きい。このような役割は今後共ますます大きくなると考えている。皆様のそれぞれの活動の発展のためにもマルチメディア推進フォーラムに対する御支援をお願いする次第である。

本フォーラムに関連する部門 あるいはご関心をおもちの部門にご回覧下さいますようお願い申し上げます。

■「マルチメディア推進フォーラム　　―― ＰＡＲＴ 978 ―― 」開催内容

(主催)マルチメディア推進フォーラム

テーマ　「量子鍵配送技術（QKD）、耐量子暗号技術（PQC）の課題と将来展望」

日　時　2025年　6月　13日　（金）　13時00分～16時50分

時間	講　演　内　容	講　師

(本フォーラムの趣旨・論点)

●量子鍵配送技術（QKD）の技術と商業化の課題
●耐量子暗号技術（PQC）システム実現に向けた取り組み
●量子暗号通信技術の実社会での活用事例とその影響

現在、量子鍵配送技術（QKD）、耐量子暗号技術（PQC）は、情報通信のセキュリティ強化において革新的な役割を果たすと期待されています。特に、量子コンピュータの発展により、従来の暗号技術が突破されるリスクが高まる中で、これら技術の重要性が増しています。これらの技術は、セキュリティの強化だけでなく、次世代通信ネットワークの基盤としても重要な要素です。

量子暗号通信は、量子鍵配送（QKD）を利用することで、従来の暗号方式に比べて圧倒的に高い安全性を提供します。量子インターネットの実現に向けた技術的な挑戦や、量子暗号通信の商業化への道のりは、研究者や業界関係者によって鋭意進められています。しかし、商業化に向けたハードルとしては、インフラ整備、コスト問題、そして規制の整備が挙げられます。

一方、耐量子暗号技術（PQC）は、量子コンピュータによる攻撃に耐性を持つ新しい暗号技術として注目されています。現在、NIST（アメリカ国立標準技術研究所）の標準化プロセスが進行中ですが、PQCの実用化には、性能やスケーラビリティ、既存システムとの互換性といった課題があります。

本フォーラムでは、これら量子鍵配送技術（QKD）、耐量子暗号技術（PQC）の最前線を、専門家が解説し、今後の通信インフラの革新をどのように実現するかを議論します。また、商業化に向けた課題や、これらの技術が社会に与える影響についても深掘りつつ、これらが未来の通信インフラを支え、より安全で効率的な社会を作り上げるのかについて、参加者に深い洞察を提供します。

(座長-総合司会)

東京大学　名誉教授　齊　藤　　忠　夫

13:00 ～ 13:20	**（基調講演）** **「量子暗号通信技術の最前線と未来の通信インフラ」** ●量子暗号通信技術の基礎と最新動向 ●量子暗号通信が通信インフラにもたらす影響 ●量子暗号通信技術の商業化に向けた道のりと課題	質疑応答	**齊　藤　忠　夫 氏** 東京大学 名誉教授
13:20 ～ 14:25	**「量子鍵配送（QKD）の技術と商業化の課題」** ●量子暗号通信の基礎と最新研究成果 ●量子鍵配送（QKD）の商業化に向けた取り組み ●量子暗号通信ネットワークの国際的展望	質疑応答	**花　井　克　之 氏** 東芝デジタルソリューションズ株式会社 ICTソリューション事業部ビジネスユニットマネジャー
（休憩）　（14:25 ～14:35）			
14:35 ～ 15:40	**「金融機関における耐量子計算機暗号への移行に向けた取組み：現状と課題」** ●量子コンピュータの実現による公開鍵暗号のセキュリティ低下の懸念 ●耐量子暗号（PQC）への早期移行（既存暗号アルゴリズムとの併用も含め） ●暗号アルゴリズムの柔軟な切替可能な暗号アジリティの高いシステム構築 ●業界全体での協調体制：リスク低減計画、情報共有、人材育成の推進	質疑応答	**宇　根　正　志 氏** 日本銀行金融研究所 参事役
（休憩）　（15:40 ～15:45）			
15:45 ～ 16:50	**「NTT Comが取り組むQuantum-safeなシステムの実証」** ●Quantum-safeに関する動向 ●IOWN PETsの概要 ●耐量子セキュアトランスポートについて ●NTT Com特許技術を活用したQuantum-safeなシステムの実証実験について ●今後の展開やビジネスの方向性について	質疑応答	**森　岡　康　高 氏** NTTコミュニケーションズ株式会社 イノベーションセンター 技術戦略部門/IOWN推進室 主査

●当日、講師の都合により、代理講師による講演あるいは講演順序を変更する場合があります。
●受講者交替可。

本フォーラムに関連する部門 あるいはご関心をおもちの部門にご回覧下さいますようお願い申し上げます。

「マルチメディア推進フォーラム」委員会

（順不同　敬称略）

委員長

齊藤　忠夫	東京大学	名誉教授

（運営諮問委員会幹事）

代表幹事

齊藤　忠夫	東京大学	名誉教授

副代表幹事

服部　　武	上智大学	理工学部　客員教授
森川　博之	東京大学	大学院工学系研究科電気系工学専攻　教授
成宮　憲一	一般社団法人 科学技術と経済の会	専務理事

幹　事

尾上　誠三	国際電気通信連合（ITU）	電気通信標準化局長
川野　真稔	総務省	国際戦略局　技術政策課長
間宮　淑夫	内閣官房	内閣審議官
渡邊　昇治	経済産業省	商務情報政策局　総務課長
西尾　　崇	国立研究開発法人 土木研究所	戦略的イノベーション研究推進事務局 次長
立川　敬二	㈱ﾊｲﾃｸﾉﾛｼﾞｰ推進研究所	取締役・特別顧問 （宇宙航空研究開発機構 元 理事長）
伊藤　寿浩	日本放送協会	技術局長
川添　雄彦	日本電信電話㈱	代表取締役副社長
星野　理彰	東日本電信電話㈱	代表取締役副社長
桂　　一詞	西日本電信電話㈱	代表取締役副社長
池田　　敬	日本電信電話㈱	常務執行役員　技術企画部門長
佐藤　隆明	㈱NTTドコモ	代表取締役副社長　CTO、CAIO、CPO
伊東　　匡	NTTアドバンステクノロジ㈱	代表取締役社長
稲葉　陽子	㈱NTTデータグループ	技術革新統括本部 イノベーション技術部長
吉村　和幸	ＫＤＤＩ㈱	取締役執行役員専務
宮川　潤一	ソフトバンク㈱	代表取締役 副社長執行役員 兼 CTO
石原　　直	東京大学大学院	工学系研究科 特任教授
浅見　　徹	㈱国際電気通信基礎技術研究所	代表取締役社長
遠藤　信博	日本電気㈱	特別顧問
新野　　隆	日本電気㈱	取締役　会長
木内　道男	日本電気㈱	執行役 Corporate EVP 兼 テレコムサービスビジネスユニット長
高木　康志	富士通（株）SVP　システムプラットフォームBG　エグゼディレクター	
石田　貴一	㈱日立製作所	事業部長
伊藤　明男	㈱日立国際電気	副社長執行役員
加茂下哲夫	ﾉｷｱｿﾘｭｰｼｮﾝｽﾞ&ﾈｯﾄﾜｰｸｽ㈱	代表執行役員社長

（主な設立発起人）

齊藤　忠夫	東京大学	名誉教授
吉川　弘之	東京大学	元 総長
立川　敬二	㈱ﾊｲﾃｸﾉﾛｼﾞｰ推進研究所	取締役・特別顧問 （宇宙航空研究開発機構 元 理事長）
杉本　榮一	自由民主党	元 政務調査会 調査役

（最高顧問）

甘利　　明	元･経済産業大臣
金子　一義	元･国土交通大臣
林　　芳正	元･防衛大臣

マルチメディア推進フォーラム ― ＰＡＲＴ978 ― 開催

●日時　2025年 6月 13日（金）13時00分～16時50分

●本フォーラムは会員様限定Zoomでのオンラインフォーラムとなります。
オンラインのみの開催となりますのでご了承の上お申込み下さい。
（一部、一般受講も受付ておりますのでご希望の方はお問合せ下さい。）

●参加申込要領

●**受 講 料**　￥53,570.－（消費税を含む）

●**申 込 先**　**事務局 ハイテクノロジー推進研究所**　ＴＥＬ(03)-6416-0190
〒150-0036 渋谷区南平台町15-12　南平台アイアイビル2F　ＦＡＸ(03)-6416-5351
E-mail fm@ahri.co.jp

●**申込方法**　申込書に所定の事項をご記入の上、ＦＡＸ又は、Ｗｅｂ上(http://www.ahri.co.jp)にてお申し込み下さい。

●**送金方法**　銀行振込 **みずほ銀行 渋谷中央支店　1554932(普)**
三菱ＵＦＪ銀行 渋谷明治通支店　3504194(普)
※領収書のご必要な方は、通信欄にご記入下さい。

●**キャンセル**　フォーラム開催前、6月6日までのキャンセルは可能ですが、お電話にてご連絡お願い申し上げます。その後のキャンセルについては、お申し受けできませんのでご了承下さい。その場合は代理の方の出席か当日配布の「資料」の送付をもって出席とさせていただきます。

●**申込書について**　ご記入頂いたご連絡先は本フォーラムの事後連絡として使用させて頂きます。尚、今後開催されるフォーラム等のご案内を配信(又は送付)させて頂きますが、今後 弊社からのご案内を停止される方は、事務局までご連絡いただけますようお願い申し上げます。

きりとり線

「マルチメディア推進フォーラム ― ＰＡＲＴ978 ― 申込書

（申込日）　月　日

会社名		ＴＥＬ（　）　－ ＦＡＸ（　）　－ E-mail:	
会社住所	〒		
ＮＯ	受講者・所属・役職		受 講 者 氏 名（ふりがな）
支　払 方　法	●銀行振込（　　）銀行 ●　　年　　月　　日振込予定	通信欄 請求書－要・不要	