CIPHER-CORE Co., Ltd.
Area Shinagawa 13th Floor,
1-9-36 Konan, Minato-ku,
Tokyo-to, Japan
info@cipher-core.com
https://www.cipher-core.co.jp/

九州大学 特別講演
「量子耐性・完全暗号技術」 中村 宇利

日時: 2025年11月11日 | 13:00 – 14:30 JST

作成者: Md. Shahjahan Islam、Cipher Core Co., Ltd. エグゼクティブ

学術とイノベーションをつなぐ、刺激的な講演

サイファ・コア株式会社の技術開発者である中村宇利代表取締役が、九州大学大学院システム情報科学研究院 情報学部門 サイバーセキュリティセンターにおいて、「量子プルーフ・完全暗号技術（Quantum-Proof Complete Cipher Technology）」をテーマとした特別講演を行いました。この講演では、博士課程の研究者、技術者、暗号専門家が一堂に会し、ポスト量子時代の情報セキュリティの最前線について活発な議論が交わされました。

CIPHER-CORE Co., Ltd.
Area Shinagawa 13th Floor,
1-9-36 Konan, Minato-ku,
Tokyo-to, Japan
info@cipher-core.com
https://www.cipher-core.co.jp/

参加者と関係者

- 暗号理論、AI、通信セキュリティを専門とする博士課程および研究生10名
- 遠隔医療データの安全化を研究する「ポータブル・ヘルスクリニック」プロジェクトの研究者5名
- 量子耐性通信や情報セキュリティ分野での連携を模索する企業関係者2名（原代表を含む）

中村代表の講演は、先端理論と実践的応用を結びつける内容として高く評価され、参加者に深い印象を残しました。

講演会の主要テーマ

AIと暗号技術の進化

中村代表は、MITにおける初期の情報理論研究を振り返り、AI発展の3つの時代を次のように整理しました。

- **第１次ブーム（1950～60年代）：**
  知能を人工的に構築する殆どすべての理論・概念を創造した時代。記号主義(Symbolism)とコネクショニズム (Connectionism)の２大潮流が生まれた。
- **第２次ブーム（1980～90年代）：**
  計算能力が限られた中で、第１次ブームの殆どの理論を実現した時代。
- **第３次ブーム（2010年代～現在）：**
  第2次ブームで実現したものを、圧倒的計算パワーで高速化した時代。

CIPHER-CORE Co., Ltd.
Area Shinagawa 13th Floor,
1-9-36 Konan, Minato-ku,
Tokyo-to, Japan
info@cipher-core.com
https://www.cipher-core.co.jp/

迫り来る量子の脅威

中村代表は、RSAやAESなど従来の暗号化方式は、今後10年以内に量子コンピュータによって解読される可能性が高いと言われていると指摘。「**Store Now, Decrypt Later** attacks（**SNDL／今保存し、後で解読する**攻撃、別名 **Harvest Now, Decrypt Later (HNDL)** attacks とも呼ばれる）」という脅威概念を紹介し、次のように強調しました。

「量子コンピュータはアルゴリズムを破るだけでなく、デジタル社会の信頼そのものを崩壊させる。」

現行サイバーセキュリティの限界

現在主流のネットワーク重視型セキュリティシステムでは、ゲート防御を突破された瞬間に内部データが無防備となる構造的弱点を持っています。真の防御は「情報そのものの保護」から始まると説きました。

AIによる情報汚染

AIが生成するデータ量が、歴史的に人間が生み出す情報量を近年中に**上回る勢いで増加**しており、AIが他のAIの生成した情報を学習に利用するようになることで、情報の真正性と正確性が失われました。AIは**情報セキュリティインシデントを人間以上に巧妙に偽装・捏造する能力**を獲得しつつあり、**何が本物で何が偽物なのかを見分けることがますます困難になっている**と警告しました。

「完全暗号」パラダイムの紹介

中村代表は、無限の計算能力をもってしても解読不可能な**Quantum-Proof** 次世代暗号基盤「**Complete Cipher（完全暗号）**」を紹介し、真の情報セキュリティは、ネットワークやシステムの堅牢性ではなく、**情報理論的安全性に基づく暗号**で情報そのものを守ることに尽きると強調しました。

「たとえ、機密情報が盗まれたとしても、完全暗号で暗号化された情報は最早情報ではない」

CIPHER-CORE Co., Ltd.
Area Shinagawa 13th Floor,
1-9-36 Konan, Minato-ku,
Tokyo-to, Japan
info@cipher-core.com
https://www.cipher-core.co.jp/

国際的文脈

中村代表は、米国、日本、EUがすでにポスト量子暗号（PQC）の採用を進めている現状を紹介し、中国の量子コンピュータ「九章二号」を例に挙げて、**量子コンピュータ時代の到来が目前に迫っている**ことを強調しました。

連携への道

中村代表は、今後のサイバーセキュリティには、学術界と産業界の緊密な連携が不可欠であると強調しました。

今回の講演は、九州大学および関連機関との共同研究協定（JRA）締結に向けた道を開くものであり、その焦点は以下の分野に置かれています。

- 量子耐性通信システムの構築
- AIによる情報汚染への対策
- 安全な医療データアーキテクチャの設計
- ポスト量子暗号技術の統合研究

振り返りと閉会の辞

九州大学の櫻井幸一教授（Prof. Dr. Koichi Sakurai）は、中村代表の貴重な貢献に深い感謝の意を表し、講演がポスト量子時代の情報セキュリティの未来に対して極めて示唆に富む内容であったと述べました。

参加者からは、「目が開かれるような内容だった」「従来の考え方の革新を促される講演だった」との声が多く寄せられ、理論研究と実践的イノベーションの双方に通じる意義が強調されました。