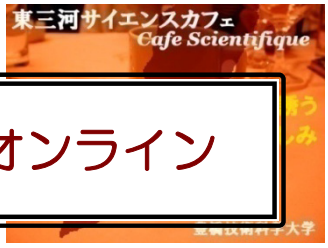
第２９５回東三河サイエンスカフェ
２０２２年８月１８日（木）
午後６時３０分～８時００分
~~豊橋駅前サテライトオフィス~~



オンライン

東三河サイエンスカフェ　検索

http://www.ita.cs.tut.ac.jp/~kawai/cs/

サイエンスカフェは、講演会や体験講座とは違い、ゲストスピーカーやほかの参加者とのフランクな語らいを楽しむ場です。どうぞ、サイエンスについて語らう楽しみを満喫してください。

ゼロ知識証明（Zero-Knowledge Proof）
― 情報Ａ－Ｚ「Ｚ」の巻 ―

ゼロ知識証明

ある人があることを知っているとします。そして、その「あることを知っている」ということを、ほかの人に示したい（証明したい）なら、その「あること」そのものを、相手に示せばよいでしょう。ただ、その「あること」が、例えば、パスワード（暗証番号）のような「大事なもの」なら、それを示すわけにはいきません。そこで、その「あること」に関するなんらの情報も示すことなく、本当に、自分がそれを知っている、ということを証明する方法を、ゼロ知識証明といいます。例えば、誰でも、自分の使っているパスワードは、当然知っていますが、そのパスワード自体を明かすことなく、そのパスワードを知っている、（すなわち、自分は自分である、）ということを証明しよう、というお話しです。

今宵は、ゼロ知識証明についてサイエンスしてみましょう。

★ゲストスピーカー：
河合 和久 先生
豊橋技術科学大学
情報・知能工学系
★先生のご専門：
コンピュータ・サイエンス
★先生からの一言：
ゼロ知識証明は、ユーザ認証や暗号に用いられています。ゼロ知識証明自体は、比較的古いもので、1985年に最初の論文が発表されました。近年のWeb3やNFTに関連して、あらためて注目されている技術のひとつです。

★対象：高校生以上どなたでも。参加費無料。
定員２０名。定員に達し次第しめきります。
事前に参加申込をしてください。
★申込：「第２９５参加希望」と明記し「氏名」「年齢」「連絡先（電話番号またはメイルアドレス）」~~「対面・オンラインのいずれで参加されるか」~~をお書きの上、下記のメイルアドレスあてお申込みください。
東三河サイエンスカフェ事務局
メイル：**cs@ita.cs.tut.ac.jp**
申込〆切：８月１７日（水）正午

★ご連絡いただいた個人情報は、申込受付等の連絡業務にのみ使用します。

オンライン

★オンライン（**Google Meet** 使用）：ＵＲＬ等詳細は申込者あて別途連絡。