

<b>研究室名</b> <b>岩本・渡邊研究室</b>	<b>場所</b> 東3号館 924号室 (岩本) 東3号館 928号室 (渡邊)
<b>連絡先(email等)</b> <a href="mailto:mitsugu@uec.ac.jp">mitsugu@uec.ac.jp</a> , <a href="mailto:watanabe@uec.ac.jp">watanabe@uec.ac.jp</a>	
<p><b>I. 研究概要</b></p> <p>多くの情報セキュリティシステムは、暗号理論を安全性の基盤としています。岩本研究室では、情報セキュリティシステムの安全性と実装方法を主たる研究テーマとして、安全性が厳密に証明でき、かつ現実的にも効率のよい暗号システムの提案を目指しています。同時に暗号システムへの攻撃手法も研究しています（敵を知り、己を知らば、百戦危うからず）。</p> <p>研究にあたっては、離散数学を基本的な道具として計算量的アプローチと情報理論的アプローチを駆使し、暗号実装を軸に研究を進めている崎山研究室、李研究室、菅原研究室と協力しつつ、情報セキュリティシステムについて多角的に考察することを目指しています。</p> <p><b>II. 研究分野（卒研テーマ）</b></p> <ul style="list-style-type: none"> <li>・ 暗号・署名などの基本的な構成要素の提案と安全性評価</li> <li>・ 情報理論的に安全なプロトコルの設計, 効率と安全性の関係に関する検討</li> <li>・ 情報理論的暗号に対する不正検出手法とその対策</li> <li>・ カードなどの身近な題材に関する暗号理論的な検討</li> <li>・ 鍵漏洩に耐性のある暗号技術の提案</li> <li>・ 暗号化したまま検索を可能とする暗号方式の設計と安全性解析</li> <li>・ 先端情報技術と組み合わせ可能な暗号技術の検討</li> </ul> <p>※上記以外のテーマでも相談に応じます。</p> <p><b>III. 卒研生の要件</b></p> <p>離散数学・暗号理論を履修していることが望ましいです。最低限、離散数学の履修内容がある程度理解できた上で、興味もてる内容であったこと（知識不足はフォローしますが、論理的な話題に苦手意識があると苦労します）。</p> <p>詳細は研究室WEBサイト <a href="https://iw-lab.jp/messages/">https://iw-lab.jp/messages/</a> を参照してください。</p> <p><b>IV. 研究室説明会日時・場所</b></p> <p>日時：11月23日（月・祝）13:00～13:30</p> <p>場所：Zoom（UECクラウドアカウントでのログイン必須）</p> <p>※ 詳細・URLは研究室WEBサイト <a href="https://iw-lab.jp">https://iw-lab.jp</a> に掲載する予定です。</p>	

