

情報学 情報学基礎

情報学基礎理論

暗号技術・耐タンパー技術
ネットワーク / ハードウェア
/ ソフトウェアセキュリティ
バイオメトリクス・偽造防止
自動車セキュリティ

教授
松本 勉
マツモト ツトム



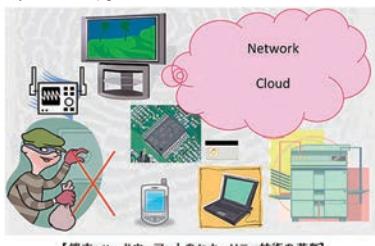
大学院環境情報研究院 社会環境と情報部門
情報メディア学分野 大学院環境情報学府
情報メディア環境学専攻 情報メディア学コース
先端科学高等研究院 理工学部 教育・電子情報系学科
情報工学教育プログラム 工学部 電子情報工学科
情報工学コース 未来情報通信医療社会基盤センター
tsutomo@ynu.ac.jp
http://ipsr.ynu.ac.jp/
http://ias.ynu.ac.jp/research/matsumoto.html

【研究概要】

情報・物理セキュリティ技術分野の探求を究め、社会への展開を志向した研究教育を実践しています。これまで、暗号理論、バイオメトリクス（生体認証）、人工物メトリクス、耐タンパー・ハードウェア・ソフトウェア、組込みシステムセキュリティ、ネットワークセキュリティ、マルウェア解析などのテーマ群で実績がありますが、新たな課題の探求も日常的に進めています。

【アドバンテージ】

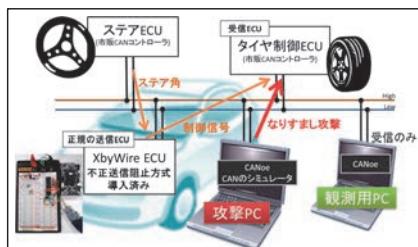
今日、「情報セキュリティ」という概念とその重要性は広く認知されていますが、現実の問題や技術を合理的に捉えるには、セキュリティの論理的側面に目を向けるだけでなく、論理を支える物理面をも総合的に考えることが必要であると考え、「情報・物理セキュリティ」分野を開拓しています。この分野は、少なくとも、論理的セキュリティ、物理的セキュリティ、物理と論理のはざま、論理と実装・実際、ソフトウェアとハードウェア、コンポーネントとシステムとネットワーク、組込みと汎用、といったキーワードで示される分野を包含するものと考えています。



【端末・ハードウェア・人のセキュリティ技術の革新】

【事例紹介】

自動車:



■ 相談に応じられるテーマ

セキュリティ技術全般
暗号技術
バイオメトリクス技術
耐タンパーソフトウェア技術
耐タンパー・ハードウェア技術
偽造防止技術
組込みシステムのセキュリティ
車載ネットワークのセキュリティ
マルウェア解析

■ 主な所属学会

電子情報通信学会
情報処理学会
国際暗号学会 (IACR)
米国電気電子学会 (IEEE)

■ 主な論文

- T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, K. Oishi 『A Method of Preventing Unauthorized Data Transmission in Controller Area Network』 [The 2012 IEEE 75th Vehicular Technology Conference, pp.1-5] 2012
- Y. Takahashi and T. Matsumoto 『A Proper Security Analysis Method for CMOS Cryptographic Circuits』 [IEICE Electronics Express Vol.9, No.6, pp.458-463] 2012
- 松本 勉, 青柳真紀子 『人工物メトリクスによってICカードのセキュリティを高める方法』 [情報処理学会論文誌 Vol.46, No.8, 2098-2106] 2005
- T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino 『Impact of Artificial "Gummy Fingers" on Fingerprint Systems』 [Proceedings of SPIE Vol.4677, pp.275-289] 2002
- T. Matsumoto 『Human-Computer Cryptography: An Attempt』 [Journal of Computer Security, Vol.6, No.3, pp.129-150] 1998