所　　属　：情報科学研究科　システム工学専攻　組込みデザイン研究室
職・氏名　：准教授　双紙　正和
ＵＲＬ　　：http://www.sos.info.hiroshima-cu.ac.jp/~soshi/
研究キーワード　：情報セキュリティ、ネットワーク、分散システム

■研究テーマ

① テーマ：ハッシュ関数を用いた効率的な認証法

概要：ハッシュ関数を用いることで，公開鍵暗号を必要としない，効率的な認証法について研究します.

② テーマ：センサーネットワーク，VANET 等の認証法

概要：センサーネットワーク，VANET など，近年注目を浴びている先進的ネットワークにおける効率的な認証法について研究します.

③ テーマ：DoS 攻撃対策

概要：近年急務となっている，DoS 攻撃（サービス拒否攻撃）への対策方法を研究します.

■研究テーマの応用例

・セキュアなセンサーネットワーク，VANET の構築
・センサーネットワーク，VANET における，効率の良いセキュアプロトコル
・効率の良い認証プロトコル
・DoS 攻撃対策システム

■主な著書、発表論文

（共著論文）Y. Kurihara and M. Soshi. A Novel Hash Chain Construction for Simple and Efficient Authentication. In 14th Annual Conference on Privacy, Security and Trust, PST 2016, December 2016.

（共著論文）K. Iwamoto, M. Soshi, and Takashi Satoh. An efficient and adaptive IP traceback scheme. In IEEE International Workshop on Internet of Things Services (IoTS), pp. 235-240, November 2014.

（共著論文）T. Karasawa, M. Soshi, and A. Miyaji. “A novel hybrid IP traceback scheme with packet counters”. In DCS 2012, vol. 7646 of LNCS, pp.71-84. Springer-Verlag, 2012.

（共著論文）A. Waseda and M. Soshi. “Consideration for multi-threshold multi-secret sharing schemes”. In ISITA 2012, pp. 265-269, August 2012.

（共著論文）K. Emura, A. Miyaji, A. Nomura, M. S. Rahman, and M. Soshi. “Ideal secret sharing schemes with share selectability”. In ICICS 2011, vol. 7043 of LNCS pp. 143-157. Springer-Verlag, 2011.

■主な特許、芸術作品等

■想定される連携先

・情報関連企業
・地域団体
・地方自治体
・公的研究機関
・教育機関
・ＮＰＯ／ＮＧＯ