# DHCP を用いたグループ鍵共有プロトコルに関する研究

# The study of the group key agreement protocol using DHCP

情報セキュリティ大学院大学
増山　一光

＜要旨＞

グループを単位として同一の鍵を共有するというグループ鍵共有プロトコルでは，グループ内のセキュリティを重視した鍵管理を実現することが可能になる．本研究においては，グループ鍵共有プロトコルの先行研究を踏まえて，LAN におけるグループ鍵共有プロトコルの提案を行うものとする．具体的には，DHCP を利用してホストの動的設定とグループ鍵共有を同時に実現するプロトコルの実装を行なうものである．本提案によれば，比較的安全な鍵長をもったグループ鍵を共有することでき、従来のグループ鍵共有プロトコルに比べ端末管理やユーザ認証がより効率的に行うことができる．

＜Abstract＞

For sharing a secret key commonly available among members of a group, a secure group key agreement protocol should be established. Referring preceding research focusing key sharing security, this study proposes a new protocol, especially assuming to be applied on LAN, and implements it along with the dynamic host configuration function of DHCP. The proposed protocol makes it possible to share the group key with sufficient length in terms of security, and to improve efficiency on both terminal management and user authentication, compared to conventional group key agreement protocols.