要 旨

RFID を用いた
セキュアな児童防犯支援システムの研究

秋本 菜緒

近年，児童が被害となる事件が多数起きており，学校や通学路における安全確保が大きな社会的課題となっている [1]．RFID(Radio Frequency IDentification) システムは，無線通信を用いた自動識別技術であるため，児童を守る児童防犯支援システムに利用することを考える．RFID システムは，物流分野だけでなく，医療分野，公共交通機関，書籍や商品管理等，様々な分野で普及している技術である [4]．しかし，RFID システムは，無線通信を用いているため，RFID タグに保存されている情報はリーダ/ライタを用いることで第三者が読み取ることが可能である．そのため，特定の RFID タグの情報からプライバシ問題が懸念されている [5]．既存方式としてハッシュ関数を用いて，RFID タグの ID 情報を毎回変化させる方式が提案されているが，RFID タグの個数が増えるほど，認証にかかる処理に時間がかかる問題がある．また，児童防犯支援システムに用いた場合，RFID タグを解析され，プライバシ問題が起きる危険がある．本論文では，ワンタイムパスワード認証方式 SAS-X を応用して，RFID タグの個数が増えたとしても認証にかかる処理速度は変わらず，RFID タグのみでは認証情報を生成することができない児童防犯支援システムに適している方式を提案する．また，現状の RFID システムを調査し，適用可能であるか検証する．

キーワード　RFID，プライバシ，認証，セキュア，児童

Abstract

Secure child security support system using RFID

Nao Akimoto

Recently, there have been many incidents that cause children to be damaged, ensuring safety at schools and school roads has become a major social issue[1]. Since the RFID (Radio Frequency IDentification) system is an automatic identification technology using wireless communication, we consider to use it for a child security support system that protects children. RFID systems are technologies that are popular not only in the field of logistics but also in various fields such as medical field, public transportation, books and product management [4]. However, since the RFID system uses wireless communication, information stored in the RFID tag can be read by a third party by using a reader / writer. Therefore, there is concern about privacy problem from information of specific RFID tags [5]. A method of changing the ID information of the RFID tag every time by using a hash function as an existing method has been proposed, but as the number of RFID tags increases, there is a problem that it takes time to process the authentication. Also, when used in a child security support system, RFID tags are analyzed and there is a danger of privacy problems occurring. In this paper, application of the one-time password authentication method SAS-X, processing speed for authentication does not change even if the number of RFID tags increases, and child identification information can not be generated with only RFID tags We propose a method suitable for the system. Also investigate the current RFID system and verify it is applicable.

key words RFID, privacy, authentication, secure, child