部屋の概念に基づく 誰でも使えるアクセス制御の実現に向けて

高橋 駿太朗[1]　趙 水鈺[1]　新城 靖[1]

1. 研究背景

多数の利用者がファイルやメッセージなどの資源を共有するシステムにおいて，資源やサービスに対するアクセス制御は不可欠である．例えば Microsoft Teams や Google Workspace では，グループの共有フォルダにアップロードされたファイルに対して同じグループのメンバのみ編集可能にしたり，教員やティーチングアシスタントのみが投稿できる掲示板を設けることが可能なアクセス制御の仕組みを備えている．

現在広く利用されている，クラウドで実装されたシステムではアクセス制御リスト（ACL, Access Control List）に基づくアクセス制御が採用されている．ACL に基づくアクセス制御では，利用者や資源が増加するにつれて誰が何にアクセスできるかを把握しきれなくなるという問題がある [1] ．特に，ディレクトリに対する ACL は，他の資源のアクセス制御に影響するので専門家であっても設定には苦痛を伴う．

一方，我々は日常生活で少人数で物理的な部屋を利用し，部屋の鍵によって室内の資源へのアクセス制御を行っている．これは誰にも馴染みやすく管理も容易である．そこで我々は，少人数のグループを対象とし，部屋の概念に基づくアクセス制御を計算機ネットワーク上で実装し，誰でも使えるアクセス制御の実現を目指す．

2. 提案手法

我々は，日常生活で使う物理的な部屋の特性を計算機上で再現することで，誰でも使えるアクセス制御を設計する．以後簡単のために，日常生活で使う物理的な部屋を**物理部屋**，計算機上で表現された部屋を**仮想部屋**とそれぞれ呼ぶ．それぞれの大まかな対照を**表 1** に示す．

2.1 物理部屋のアクセス制御

物理部屋は内部に書類や実験装置などのアクセス制御されるべき**資源**を設置することができる．それらを管理する人間を**室長**と呼ぶことにする．室長は，部屋の出入り口に**錠**を整備して，入室を許可する利用者に**鍵**を配布する．このため，室内の資源へアクセスできる主体を鍵を配布した人に限定できる．室長は鍵の配布や錠・鍵交換によって権限の付与と剥奪を行える．鍵の配布状況を記録すれば，アクセス権を容易に点検できる．

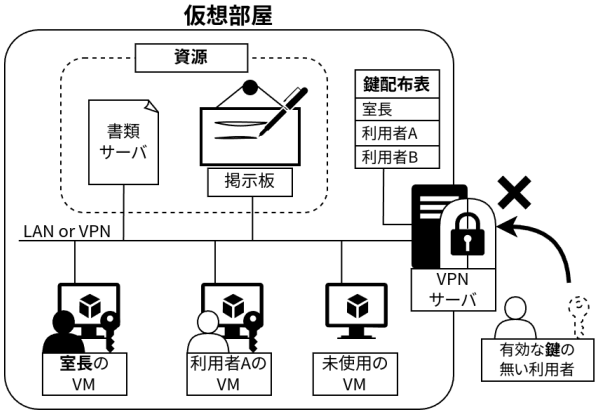

図 1　VM と VPN による部屋の概念に基づくアクセス制御

入室可能な利用者は，室内のすべての資源にいかなる操作も行うことができる．しかし，室長は信頼できる利用者のみへ鍵を配るため，普通問題にはならない．また資源の利用は原則部屋の中のみに制限され，持ち出しは制限されている．しかし研究室内で作成した論文を学会へ提出するなど，資源を別室へ持ち出したいという要求も存在するため，一定の制約のもと**持ち出し**が認められる．

2.2 仮想計算機と仮想専用通信網を使った実装

仮想計算機（VM, Virtual Machine）と仮想専用線（VPN, Virtual Private Network）とを使った仮想部屋の実装を提案する（**図 1**）．仮想部屋は，主に物理部屋と対応させて作成する．物理部屋内部に，外部のネットワークから隔離された LAN（Local Area Network）を用意して，室外からの接続を待ち受ける VPN サーバを稼働させる．利用者が仮想部屋に入室するとは，自分の PC で VM を起動し，それを仮想部屋の VPN に接続することである．資源は LAN または VPN で接続されたサーバ上のファイルおよび掲示板などのサービスとし，これらを LAN または VPN 内でのみ利用可能とする．物理部屋同様に室長が設定され，仮

[1] 筑波大学
University of Tsukuba

表 1　物理部屋と仮想部屋の対照

	物理部屋	仮想部屋（VM/VPN）	仮想部屋（Web ブラウザ）
主体	利用者自身（人間）	利用者の PC で動く VM	リモートデスクトップでアクセス可能な Web ブラウザ
資源	書類，実験装置など	ファイル，掲示板など	ファイル，掲示板など
鍵	鍵	クライアント証明書	クライアント証明書
入室	解錠	VM を起動し VPN に接続	自分のブラウザを WebRTC で部屋内ブラウザに接続
持出制約	規則制定，ラベル付け	VM 内に隔離	リモートデスクトップ

想部屋つまり LAN または VPN へのアクセス権を管理する．アクセスの主体は利用者の使う VM とする．仮想部屋の鍵は室長が発行するクライアント証明書とし，VPN 接続の際の認証に用いる．室長は証明書の発行・失効によって入室権を管理する．持ち出しを制約するために，1 つの VM は 1 つの仮想部屋の LAN のみに接続可能とする．利用者の PC に保存する VM はイメージを暗号化する．持ち出しが行われる際は，持ち出し元と持ち出し先の双方の仮想部屋で持ち出し（持ち込み）記録を残し，室長が監査可能とする．

2.3 Web ブラウザと WebRTC オーバレイネットワークを使った実装

Web ブラウザと，その上で利用できる WebRTC（Web Real-Time Communication）接続によるオーバレイネットワークを使った仮想部屋の実装を提案する．この方法では，VM と VPN ではなく Web ブラウザの WebRTC 接続によるオーバレイネットワークを用いる．資源は WebDAV などの Web ブラウザから利用可能なファイルや，掲示板などのサービスとし，これらをオーバレイネットワーク内でのみ利用可能とする．アクセスの主体は，利用者が使うオーバレイネットワーク内の Web サーバにのみ接続可能な Web ブラウザとする．この Web ブラウザを，**部屋内ブラウザ**と呼ぶこととする．利用者が仮想部屋に入室するとは，自分の PC で通常の Web ブラウザを実行し，それを通じて部屋内ブラウザを利用可能な状態にすることとする．これには，部屋内ブラウザをリモートデスクトップと同様に利用する手法を採用する．仮想部屋の鍵は室長の発行するクライアント証明書とし，通常の Web ブラウザと部屋内ブラウザとの間の WebRTC 接続時の認証に用いる．室長は証明書の発行・失効によってアクセス権を管理する．この方法では内部のファイルを仮想部屋外に持ち出すことはできない．特別に持ち出しを許すために，持ち出し元・持ち出し先双方の仮想部屋内のサーバ間で，データを複製・移動する機能を実装する．持ち出しの際は，VM と VPN による実装と同じく，双方の仮想部屋で記録を残す．

3. 関連研究

Penumbra は，誰でも使えるアクセス制御を目指す分散ファイルシステムである [2]．Penumbra では，ファイルは木構造に基づくパス名ではなく，「家族が写っている写真」，「会社の書類」などの属性によって組織化される．ファイルに付されたタグによって利用者にポリシーを定めさせ，アクセス制御を行う．また Chhetri らは，スマートホーム機器を対象とした類似のアクセス制御の方法を提案している [3]．

これらの研究は，誰でも使えるアクセス制御を目指す点で，本研究と目標を共有している．本研究の特徴は，資源を物理的な部屋と鍵の概念に関連付けて，部屋と鍵管理といった実世界の概念を用いてポリシーを記述でき，持ち出し記録を監査できることである．

4. まとめ

本研究は，ACL によるアクセス制御に代えて，部屋の概念に基づいた誰でも使えるアクセス制御を提案する．現在，WebRTC によるリモートデスクトップ機能の実装に取り組んでいる．今後，仮想部屋間の資源持出機能，および部屋・鍵管理機能の実装を進め，評価を行う．

参考文献

[1] Wang, Q. and Jin, H.: Data leakage mitigation for discretionary access control in collaboration clouds, *Proceedings of the 16th ACM Symposium on Access Control Models and Technologies*, SACMAT '11, pp. 103–112 (2011).
[2] Mazurek, M. L., Liang, Y., Melicher, W., Sleeper, M., Bauer, L., Ganger, G. R., Gupta, N. and Reiter, M. K.: Toward Strong, Usable Access Control for Shared Distributed Data, *12th USENIX Conference on File and Storage Technologies (FAST 14)*, pp. 89–103 (2014).
[3] Chhetri, C. and Genaro Motti, V.: User-Centric Privacy Controls for Smart Homes, *The 25th ACM Conference on Computer-Supported Cooperative Work and Social Computing*, pp. 1–36 (2022).