北海道科学大学研究紀要
第48号（2020年）
研究報告

Bulletin of Hokkaido University
of Science, No.48(2020)
Research Reports

スマートロックシステムの開発における IoT デバイスの導入検討

Consideration of Introduction of IoT Devices in Development of Smart Lock Systems

深井裕二*

Yuji Fukai

概要

既存のドアの錠開閉操作を自動化するスマートロック（Smart Lock）は，Wi-Fi や Bluetooth によって PC などの機器と通信する IoT（Internet of Things）デバイスのひとつである．本研究では，入退出管理などに用いられてきた既存の認証手段である指紋リーダーや非接触 IC カードの他，IoT デバイスとして BLE（Bluetooth Low Energy）機能を有するスマートウォッチなどを認証デバイスとし，大学の研究室やゼミ室の錠開閉を電子化するために利便性と安全な運用管理を重視したスマートロックシステムを開発した．本稿では，これらデバイスの特徴，開発コスト，運用法，性能およびセキュリティなどについて述べる．

1. はじめに

IoT（Internet of Things）はパソコンやスマートフォンなど従来のインターネット接続端末に加え，様々なものがインターネットに接続され相互の情報交換や制御を行う仕組みである．世界における IoT デバイスの普及数は 2020 年で 400 億個に達すると予測されており，その用途として通信，産業，コンシューマ，コンピュータ，自動車，医療など様々な活用場面がある[(1)]．このうちコンシューマ用途には家電，オーディオ，玩具，スポーツ・フィットネスなどがあり，IoT は情報化および自動化の技術を活用して我々の生活に恩恵をもたらすものである．スマートロック（Smart Lock）は，錠を開閉・管理する機器およびシステムの総称であり，一般的なドアの内側にある錠開閉操作部（サムターン）に設置することで電子制御による錠開閉ができる．近年のスマートロックは，IoT デバイスとしてインターネットに接続することでスマートフォン等から容易に錠開閉操作が行えるものもある（図 1）．

図 1　スマートロックデバイスとその設置状態

本研究では，大学の研究室・ゼミ室の施錠管理を対象として IoT を用いたスマートロックシステムを開発し，その設計および評価にあたり，利便性，性能，セキュリティ等の観点からデバイスの導入について検討した．

2. システム構成

2.1 システムの基本要件

スマートロックシステムの設計にあたり，本システムの基本要件を以下のように設定した．

(1) 入退室管理システムとしての発展性を考慮し，データベースへの記録や Web による状態・履歴の確認等の機能拡張のために制御や管理の処理システムを PC プログラムとして開発する．
(2) 簡素なプログラムで低開発コストを実現する．
(3) ドアや壁に対する工事や破壊的加工を避ける．
(4) ドア等の可動部分に設置するデバイスは有線

＊北海道科学大学工学部情報工学科

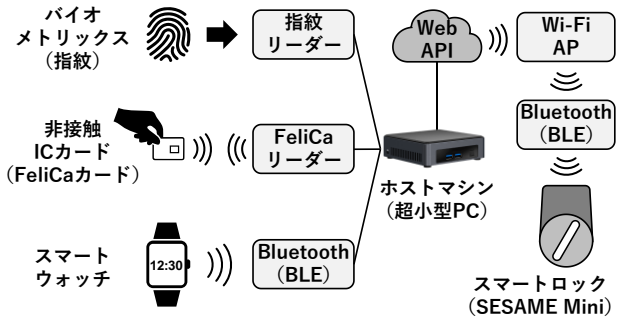

図 2　スマートロックシステムの構成

配線するタイプを避ける.

(5) 錠開閉操作のユーザインタフェースとして，指紋リーダー，身分証・学生証(FeliCa カード)，スマートウォッチ等を用い，それらの動作の比較や組み合わせによる活用を試す.

図 2 に本システムの構成を示す．プログラムを稼働させるホストマシンには超小型 PC の NUC8i5BEK（intel 社製，CPU：Core i5-8259U，メモリ：8GB，OS：Windows10）を用いた．開発には Visual Studio 2019 Community（Microsoft 社製）を用い開発言語に C#，データベースに SQLite を採用した．これらのソフトウェアはすべて無償である．錠開閉には IoT スマートロックデバイスを用い，開閉手段として，指紋によるバイオメトリックス認証，非接触 IC カードとして教員・学生が所持する身分証・学生証，IoT デバイスとしてスマートウォッチを用いた．以下に本システムに用いた各デバイスについて説明する.

2.2 スマートロック

本システムにおける錠開閉装置として，スマートロックデバイスには SESAME Mini（CANDY HOUSE 社製）[2] を用いた．これは様々なドアのサムターンに取り付け可能であり，両面テープを用いた簡易な施工ができる（図 1）．また電池で駆動し Wi-Fi および BLE（Bluetooth Low Energy）による通信方法を採用した IoT デバイスであり，有線配線が一切不要である．錠開閉方法として，スマートフォンを用いるほか，プログラム開発用に Web API（Application Programming Interface）が公開されている[3]．API コールでは表 1 のような REST(REpresentational State Transfer)形式を用いインターネット経由でデバイスを制御する．ここで device_id はデバイス固有の ID であり，api_key は事前に Web から入手した認証キーである．これらの情報通信では HTTPS における暗号化によってセキュリティが確保されている．SESAME Mini の選択理由として，本システムの基本要件を満たすことに加えて以下の理由が挙げられる．(1)同種の各社製品の中では最も小型であり，人の入退室動作に対しストレスを与えにくいこと．(2)公開 API がプログラミング言語に依存せずシステム開発において汎用性が高いこと.

表 1　スマートロックデバイスの Web API

エンドポイント
　https://api.candyhouse.co/public/

リクエスト，ヘッダ
　POST　/sesame/<device_id>
　Content-Type：　application/json
　Authorization：　<api_key>

ボディ（JSON 形式）
　{ "command" : "lock" }　… 施錠
　{ "command" : "unlock" }　… 解錠

2.3 指紋認証

指紋認証はバイオメトリックス認証の代表的手段であり実績も多い．本システムでは指紋リーダーに VeriMark 指紋認証キー K67977JP（Kensington 社製）[4] を用いた．本デバイスの認証精度は本人拒否率（False Rejection Rate，FRR）が 3%，他人受入率（False Acceptance Rate，FAR）が 0.002%である．また PC と USB で接続し Windows Hello[5] 機能を使用することで容易に利用でき安価であるのが特徴である．Windows Hello は Windows10 標準の生体認証機能であり，指紋や顔認証を用いてサインイン処理やユーザ認証を可能にするものである．指紋データの登録・管理や認証処理が Windows 側で行われるため信頼性が高く指紋登録・管理操作が容易である．またプログラム中での認証処理も数行程度で実装でき開発コストも非常に低い．なお，Windows Hello の本来の用途はサインイン時およびサインイン中ユーザの各場面でのパスワード入力の代わりとなるものであり，登録可能な指紋数は 1 ユーザに対し最大 10 件となる．ゆえに複数ユーザに対応した認証処理は難しく，シングルユーザを共有する形で 10 人までの指紋登録をする運用形態となる．デバイスの選択においては，Windows Hello に対応した同等製品が数多くあり，コストや性能は同程度であると思われる．指紋リーダーの設置位置は，図 3

図 3　指紋リーダーとその設置状態

図 4　FeliCa リーダーとその設置状態

のように室外のドア周辺となるが，指を接触させやすいような位置と角度を考慮する必要がある．

2.4 非接触 IC カード

入退出管理において IC カードは広く用いられている手段であり，近年では非接触型の IC カードが主流である．本学において教員・学生が学内で携行する身分証・学生証には，FeliCa（ISO/IEC18092）方式の非接触 IC カードを採用している．カード情報を読み取る FeliCa リーダーには PaSoRi RC-S380（Sony 社製）[6]を用いた．FeliCa リーダーの設置位置は一般的に室外のドア周辺となるが，非接触 IC カードの基本技術に用いられる電磁誘導は非金属を通過しやすいため，図 4 のようにガラス窓の室内側の設置位置でも作動可能である．リーダーは USB 接続した PC 側で制御する．FeliCa カードから読み取れる情報として，IDm（Manufacture ID）は IC チップ製造時に記録され書き換えできない 8 バイトの情報である．IDm を個人識別に利用した入退室管理等のシステムは多い．また本学の身分証・学生証には個別識別符号も含まれており，それらと IDm を合わせたものを認証キーに用いれば十分なビット長のパスワード強度が得られる．しかしこれらは非暗号化情報であり，カードの複製・偽造といったセキュリティ脅威が懸念される．これに対し簡易認証機能を持つ FeliCa Lite を用いることで容易にセキュリティを高めることができる．FeliCa Lite のカード側では，あらかじめ書き込まれた読み出し不可の個別化カード鍵とリーダーが生成した乱数から MAC（Message Authentication Code）を生成し，リーダー側で生成した MAC と照合することでカードを認証する[7]．これによってカードの複製・偽造による攻撃を防ぐことが可能である．FeliCa Lite カードは 1 枚数百円程度で購入でき，ドア鍵のように 1 個を複製するといった管理上の問題がなく，鍵の個別化とデータによる登録管理という点で優れており ゼミ室の鍵管理に活用できる．

図 5　スマートウォッチ

2.5 スマートウォッチ

スマートウォッチは多機能な腕時計デバイスであり，代表的な IoT ウェアラブル端末である．その多くは Bluetooth 通信によってスマートフォンと連携し，メールの着信通知，心拍数のモニタリングによる健康管理，GPS 機能を用いた運動管理など様々な活用ができる．本システムでは Mi Band 3（Xiaomi 社製）[8]（図 5）を用いた．これは Bluetooth4.2 規格に準拠し BLE 機能を持つ．BLE は低消費電力の通信方法であり，数メートル程度の近距離の情報通信に向いている[9]．また BLE デバイスはビーコン信号であるアドバタイズメントパケット（ADV パケッ

ト）を定期的に送出する．ADV パケットには一意な BD アドレス（Bluetooth Device Address）や受信信号強度（Received Signal Strength Indication, RSSI）が含まれ，この値からおおよその物理距離が推定できる.RSSI を利用すればスマートウォッチ装着者が数メートル範囲に近づいたらスマートロックを解錠するなどの手法が可能である．その際，セキュリティに関して BD アドレスのなりすまし等が懸念される．これに対し Bluetooth では PC とデバイス間でペアリングをすることで，暗号鍵を用いてデバイスを信頼する．よって事前に PC で BLE デバイスをペアリングしておき，ADV パケット受信時に BD アドレスとともにペアリング状態を調べることで登録済みデバイスであるかを判断できる.

3. システムの運用

本システムの運用では，表 2 に示す 3 種類の認証手段を用いた.各手段は 2.で挙げた各デバイスを使用している.認証およびスマートロックの制御は PC のプログラムによって集中的に行い，各操作および制御状況をイベント情報として PC 上のデータベースに記録する．各認証手段について，指紋認証および非接触 IC カードは同じ操作で施錠と解錠を行うトグル方式とした．その理由としては操作の単一化によるストレスの低減が挙げられる．またスマートウォッチでは 5 分以上施錠状態であるときに ADV パケットを受信した場合,RSSI から距離を推定し部屋のドア付近約 10m 以内に入ると解錠するようにした.反対に施錠時を考えた場合，距離が遠ざかるか ADV パケット無受信時間が一定値を超えるかで制御可能である．しかし RSSI の精度が低いことや在室時に長い無受信時間があり得ることを考えると，安定動作のために部屋からかなり離れてから施錠動作が行われることになる．これはセキュリティ上の不安要素となるため，スマートウォッチでは解錠のみとし施錠は行わない方針とした.

表 2　システムの認証手段

	施錠方法	解錠方法
指紋認証	指の接触	指の接触
非接触 IC カード	カードをかざす	カードをかざす
スマートウォッチ	なし	約 10m 以内に入る

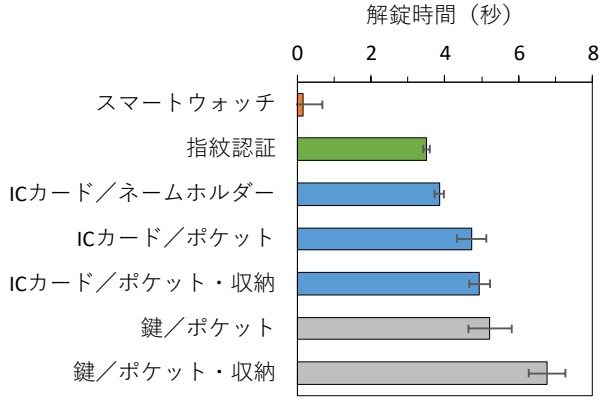

図 6　解錠時間の比較

図 6 は各デバイスによる平均解錠時間を比較したものでエラーバーは標準偏差である．測定方法は，ドア前で両手をおろした直立姿勢をとった状態を測定開始とし，それぞれのデバイスによる解錠操作を行いドアの鍵の解錠を完了するまでの時間を 10 回測定して平均した．スマートウォッチでは 0.17±0.52s と短く，その理由は 10m 以上離れた位置からドアに向かって歩行したとき，ドア前到着時には既に解錠済み状態がほとんどであったためである.ADV パケットの送出間隔は不定期であるが,もし 10m の歩行時間である約 9s 以内の送出間隔ならば解錠時間の測定値は 0s となる．指紋認証では 3.50±0.09s であり，指の接触動作が単純であるため解錠時間のばらつきは小さい．非接触 IC カードでは，首から吊るすネームホルダーに収納した場合と上着の胸ポケットに収納した場合を測定した．ネームホルダーをかざす動作も単純であるため 3.85±0.13s と指紋認証に近くばらつきも小さい．ポケットから出す場合は 4.74±0.39s とやや長い．従来の鍵での場合は，胸ポケットから出して解錠する際は 5.22±0.58s であった．ばらつきが大きい理由は，鍵がスムーズに入らないことや，鍵の挿入時に表裏の方向合わせに手間取ったり間違ったりすることで生ずる時間のロスによるものである．対して非接触 IC カードでは表裏は関係なく動作するのでこのような余計な行動が生じることなく心的ストレスも少ない．また非接触 IC カードと鍵において，胸ポケットへの収納も含めた解錠時間も比較した．鍵の場合は鍵を挿入・回転させ，鍵を抜き取ってポケットに収納するまでの合計時間は長くなる．一方，非接触 IC カードはかざしてすぐに認証が終了し，サウンドによる利用者への合図とともに解錠処理を開始するため，解錠終了を待たずにポケットへ収納でき収納完了時までの合計時間は短くなる.

表 3　各デバイスの比較

	鍵	非接触 IC カード	非接触 IC カード（認証機能付き）	指紋認証	スマートウォッチ
必要となるデバイスや機能・状態	−	FeliCa カードリーダー	FeliCa Lite カードリーダー	指紋リーダー	Bluetooth 機能ウォッチの充電
解錠操作時間	やや長い	やや短い		かなり短い	ほぼゼロ
解錠操作労力	やや多い	やや少ない		少ない	ほぼなし
デバイスの携帯について	容易	曲げに弱い		−	容易
デバイス紛失時の脅威度	とても高い	やや高い		−	やや高い
デバイスの偽造コスト	鍵の入手と複製	非暗号情報の入手と複製・偽装	暗号情報の解読と複製・偽装	形状情報の入手と模造	暗号情報の解読と複製・偽装
鍵の共通／個別	共通	個別			
鍵紛失時の対応	全鍵とドア鍵交換	データベースの個別鍵情報を抹消			
プログラミングコスト	−	数百行		数十行	

本システムによる錠開閉の処理時間には約 3s を要するが，これはスマートロックの通信制御時間の占める割合が大きい．今後 Web API の他に直接 Bluetooth 制御できる API が公開されれば，さらに時間短縮できるものと思われる．

4. デバイスの評価とシステムの発展性

表 3 に各デバイスによる比較をまとめた．管理上の危険性で見ると鍵は紛失に対する脅威度が高い．鍵の紛失があった際はドアノブの鍵交換および利用者への鍵の複製・配付に長い時間を要する．これに対し鍵以外の電子デバイスでは認証情報が個別化されているため，紛失時は当該個体のみのデータ抹消により迅速に安全性を保持できる．システムを Web で管理できるようにしておけば遠隔地から迅速なデータ抹消も可能である．解錠操作の時間短縮や労力軽減に関しては指紋認証やスマートウォッチが良好であると感じた．スマートウォッチは PC とペアリング可能な BLE デバイスであればウォッチ以外のデバイスでも代用が可能である．システムの開発面では，スマートロック制御やデータベース処理などの共通部分を除く認証デバイス特有の処理部分のみに着目すると，非接触 IC カードの処理に対し指紋認証やスマートウォッチの処理はプログラム行数で 1/10 程度と短いため，実装および改良・発展が容易であると考えられる．

本システムでは認証情報をデータベースに保存しておくが，ID 等のそのままの形ではなく，安全性を考慮し SHA-256 によるハッシュメッセージ認証コード（HMAC）でハッシュ化した値として保存している．もしホスト PC あるいはデータベースファイルが悪意の第三者に取得されても，ハッシュ値から元の ID を復元することは困難である．同様に指紋認証においても Windows Hello で使用する生体認証データは，取得できたとしても生体認証センサーによって認識される形式に変換することは容易でないとされている．

本システムの発展形を考えてみた場合，データベースに記録された施錠・解錠情報から研究室やゼミ室の在室状況や利用状況を Web 等によって遠隔的に把握することや，施錠・解錠をイベントとしてメール送信したり，他のアプリへ通知したりするなど，IoT システムとしての連携活用が可能である．また，未登録のデバイスによる解錠の試行を検出することで部外者による侵入を警戒できる予防的セキュリティシステムも考えられる．ゼミ室の鍵管理においては，電子化によって鍵の配布・回収が不要となり，データの登録・削除による管理法に変わる．こうした利便性や応用性が考えられる一方で電子的セキュリティについても検討する必要がある．これについては常日頃から認証に対する新たな脅威となる攻撃手法を知り，状況の変化に応じて本システムの危険性を再評価すべきであろう．

5. 複数認証デバイスによるシステムの有利性

本システムのように認証手段を複数実装する利点を述べる．セキュリティを強化する場合，本システムでは多要素認証(Multi-Factor Authentication)

の方式をとることが可能である．複数の認証デバイスを併用することで各手段の脆弱性をカバーし，認証攻略の難度を上げることができる．例えば，本システムの場合，施錠時は任意の認証デバイスを１つ使えば施錠できるようにしておき，利用者は自分にとって最も楽な手段を使えばよい．そして解錠時はセキュリティを高め，一定時間の中で 3 つの認証デバイスのうち2つまで認証成功すれば解錠するなどの手法が考えられる．

また複数の認証デバイスで構成される本システムでは，障害耐性を高めるフォールトトレランス設計が導入できる．一般に並列システムの全体故障率はデバイス単体故障率よりも低いため本システムの信頼性は高い．また 3 つのうち 2 つの手段で認証する場合（2-out-of-3 系），2 つのデバイスが故障すると稼働できなくなる．しかし故障状況に応じて一時的に 1-out-of-3 系で稼働させる運用法も考えられる．これは稼働を優先してシステム信頼度を動的に変更するものであり，システム障害によって入室できなくなるなどの事態発生を少なくすることができる．このような機能を実現するためには，個々のデバイスの動作不能を感知する仕組みやプログラムに動作異常時の例外処理を実装するほか，登録ユーザへはスマートフォンなどによるシステム信頼度の一時的変更を許可するといった手法が考えられる．

6. まとめ

本研究では，ドアの錠開閉操作を自動化するスマートロックシステムを開発した．これには既存の認証手段である指紋リーダーや非接触 IC カードの他，スマートウォッチ等の IoT デバイスを用い，利便性を高めている．IoT デバイスは情報通信によって他のシステムと連携を想定した道具や装置として，生活の様々な場面で活用されていくものと思われる．BLE は IoT における主力技術のひとつとされており，本システムで用いたスマートロックやスマートウォッチ等の IoT デバイスでは通信方法に BLE が用いられている．これら IoT デバイスの安全性については，BLE におけるペアリング処理やスマートロック制御の Wi-Fi 通信におけるサーバの認証処理によりセキュリティが確保されている．さらに本システムでは認証デバイスを複数用いた多要素認証によってセキュリティが高められる．本システムの開発においては，汎用プログラミング言語やデータベース処理の採用により，Web 経由で管理・活用するシステムへの発展形も比較的容易で自由度が高い．

一般の鍵は紛失時の危険度，運用管理の非柔軟性，操作・所持における高ストレスといった欠点がある．これらのことは複数人が部屋を共有する研究施設や職場において重大な事柄であろう．昔ながらの鍵に対し欠点が改善され先端的技術を利用した各種デバイスの活用は，IT 化されていく設備・施設や教育環境において，われわれの活動モチベーションを高める基盤のひとつとなるであろう．

参考文献

(1) 総務省：平成 30 年版 情報通信白書 IoT デバイスの急速な普及，2019-8-11 参照，http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd111200.html.

(2) CANDY HOUSE：SESAME Mini，2019-8-11 参照，https://jp.candyhouse.co/pages/sesame-mini-qrio-lock-comparison.

(3) CANDY HOUSE：Developer Reference，2019-8-11 参照，https://docs.candyhouse.co/.

(4) Kensington：VeriMark Fingerprint Key，2019-8-11 参照，https://www.kensington.com/p/products/security/biometric/kensington-verimark-fingerprint-key-supporting-windows-hello-fido-u2f-for-universal-2nd-factor-/.

(5) Microsoft：Windows Hello - Windows UWP applications，2019-8-11 参照，https://docs.microsoft.com/ja-jp/windows/uwp/security/microsoft-passport.

(6) Sony Japan：FeliCa 非接触 IC カード技術，2019-8-11 参照，https://www.sony.co.jp/Products/felica/consumer/products/index.html.

(7) Sony Japan：FeliCa Lite スターターマニュアル，2019-8-11 参照，https://www.sony.co.jp/Products/felica/business/tech-support/st_flsstarter_manual.html.

(8) Xiaomi：Mi Band 3，2019-8-11 参照，https://www.mi.com/global/mi-band-3/.

(9) Kebin Townsend，Carles Cufi，Akiba，Robert Davidson. 水原文(訳)：Bluetooth Low Energy をはじめよう，オライリー・ジャパン，2015.