C. D. 結果と考察

運用の概要については上図の様に、①ユーザーはまずキーターミナルを開ける権限が設定されている事が必要である。②ターミナルを開けてからは、ユーザー毎に持ち出せる鍵を設定することで、二重の制限をもうける。また南京錠側でも鍵の固有番号を判別できるので、開ける鍵を特定する事ができる。最終的には病原体管理システム（ICBS システム）内でログを一元的に管理するため、キーターミナル、南京錠それぞれが USB を経由して開錠履歴データをパソコンにつなぎ込みが可能な仕様とした。

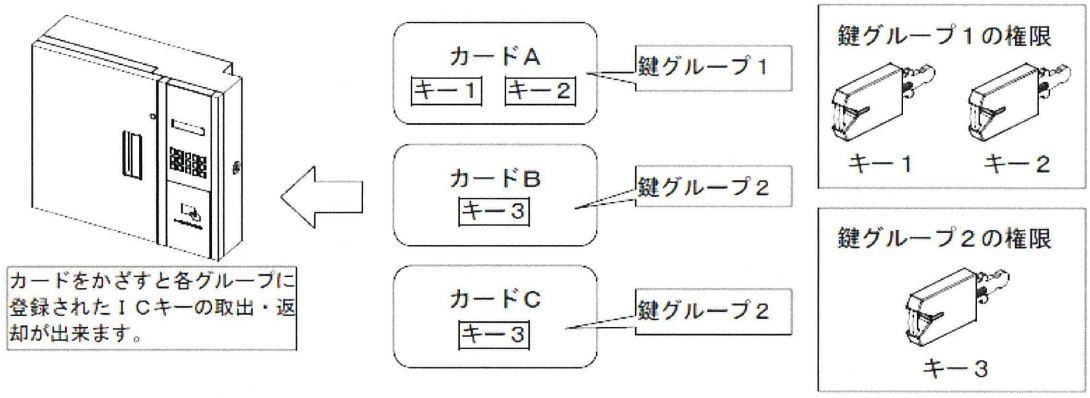
1．設定の手順について

（1）アクセス制限　の設定

まず、南京錠側にどの鍵に開錠権限が有るか否かの設定を行なうことで、利用可能な鍵を特定できる。今回は、さらにその鍵を利用できる人間を ID フェリカの固有番号で限定することにより、病原体へのアクセスができるメンバーをより厳密に特定できる。下図は組合せの例。

①フェリカと IC キーの紐付け、キーターミナルの開箱権限設定

管理アプリにて、ユーザー登録時に取出・返却権限を登録したグループ設定を行なう。



②IC キーとデジタル南京錠の紐付け

デジタル南京錠と管理 PC を USB ケーブルで接続して、登録する IC キーを差し込む。

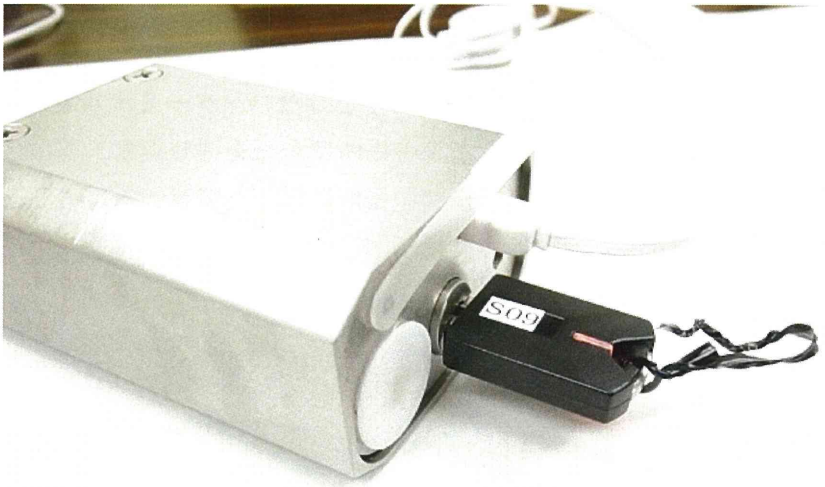


図 1　USB 接続 と IC キーの差し込み

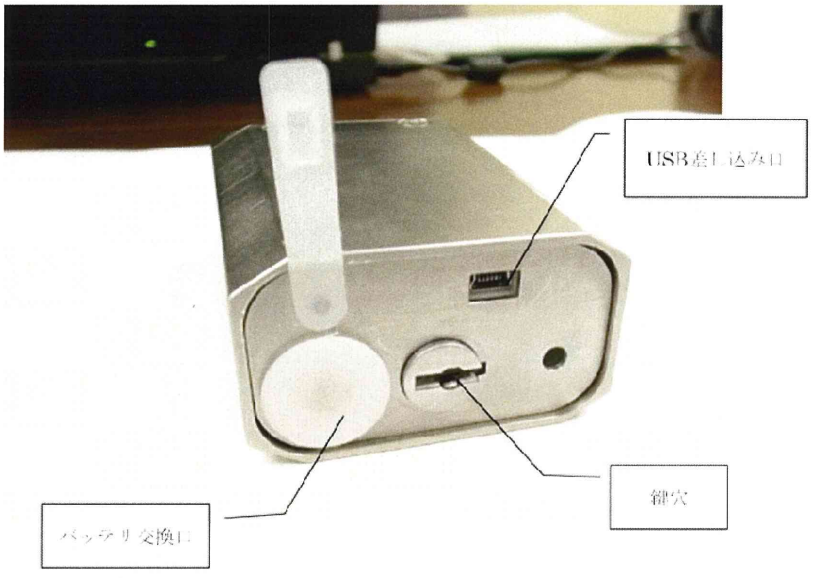


図 2　南京錠底面

③パソコンの管理アプリから ID 情報を送信し、登録完了。

（2）IC キーの取出し

①フェリカをかざす。

②フェリカがキーターミナルに認証されると、前面扉の LED が点灯し、扉を開けることができる。

③LED が点灯している IC キーのみ、取り出す事ができる。

※LED が点灯していない IC キーは権限設定がないので抜くことができない。

④IC キーの使用が終わったら、①②同様の動作を行ない、ターミナルを開け、本来の場所にキーを挿し戻す。

※別の場所に挿すとアラームが鳴り、返却間違いを知らせる。

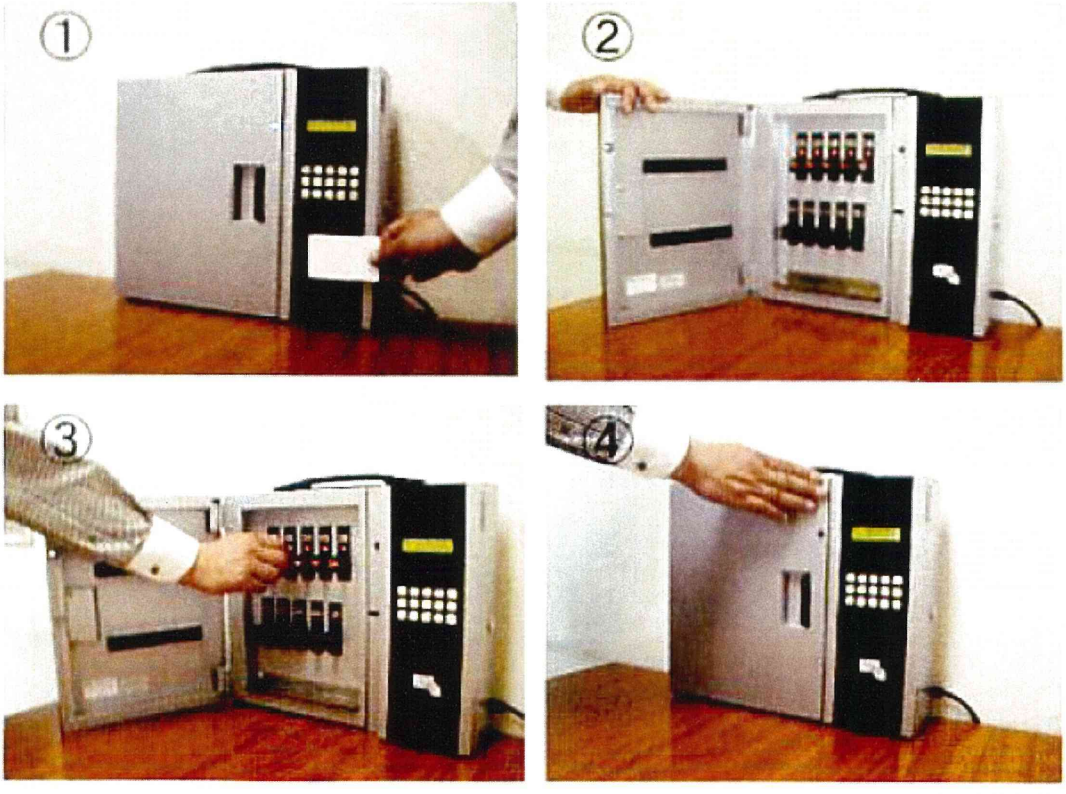


図 3　キーターミナルの開閉

（3）　冷凍庫を（南京錠を）開錠。

①南京錠に IC キーを差し込む（図 1 を参照）

②IC キーが南京錠に認証されると IC キーが点灯し開錠。（南京錠に設定のない IC キーでは開錠不可。

（4）　ログの取得

①管理者キーを挿し、USB ケーブルを管理 PC と接続し、手動でボタンを押下し、ログを取得する。

②キーターミナルのログは管理アプリから常時取得可能である。（図 3、図 4 を参照）

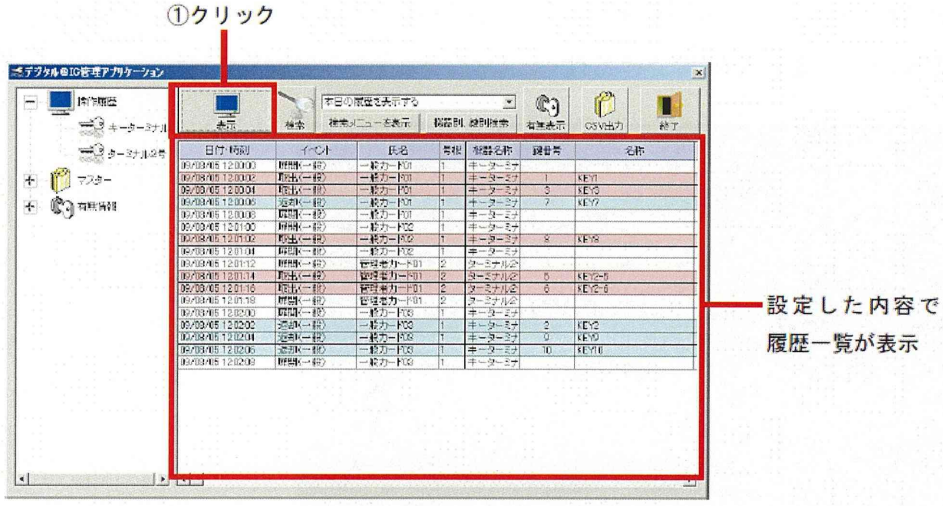


図４　キーターミナル　ログ閲覧画面

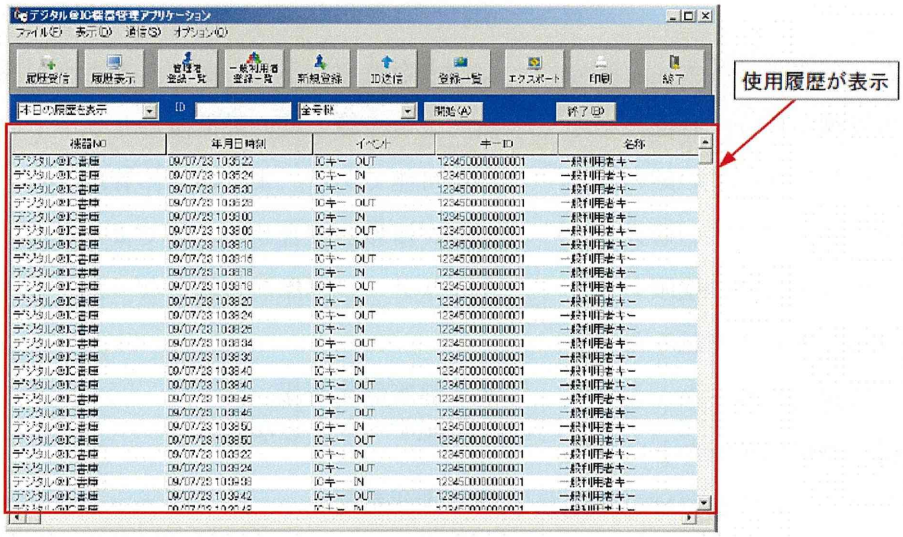


図５　南京錠　開閉ログ閲覧が面

４．非常時の開錠について

非常時の開錠方法については次のやり方を検討した。①どの南京錠でも開錠ができるマスターキーを１本用意する　②物理的に鍵を破壊する。　①についてはマスターキーが新たなセキュリティホールとなり、マスターキーを一般の鍵とは別に管理しなければならないという矛盾が発生する。②は鍵が通常の南京錠に比べると高価な物になるため、胴体部分ではなく鍵の輪の部分をきる事に成ると思われる。そのため後に修理がメーカーでのみ可能とし部品の取り付けで対応ができる用にした（図５）。さらに、ワイヤーを切った際に、異常な開錠である履歴を取得する事も検討中である。現在の想定では 10,000 回の開閉程度バッテリが持続可能と考えているが、電池が切

れた場合の開錠方法についても検討した。その結果 USB 経由で電源を供給できる仕様とし、バッテリの交換も可能とした。

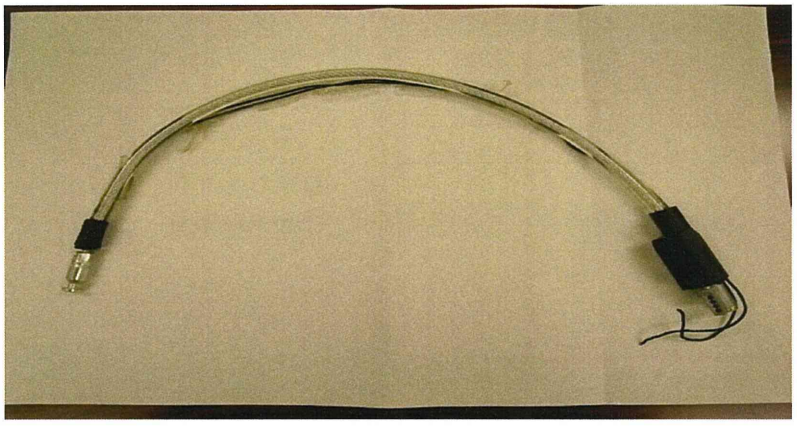


図 6　ワイヤーの例

E. 結論

保管庫に施錠をしてセキュリティを高める場合、必ず鍵の管理が伴う。利便性を追求すれば、ひとつの鍵ですべての錠の開錠が可能であればよいが、すべての研究者にすべての保管庫へのアクセスの権限を与えてしまうことになる。本研究で試みたアクセスコントロールは鍵をユニークなものとし、錠側にどの鍵で開錠が可能かという権限設定を可能とした。この仕様では、開錠権限を設定すると同時にどの鍵で何時開錠がなされたかといったログの情報採取も実現可能とした。また、キーターミナルへのアクセスはフェリカなどの個人に紐づく ID カードで鍵の取り出しログの取得が可能であるため、誰がアクセスしたかまで判明させること可能となった。また実用化に際してはなるべく安価である必要がある。今回の仕様では、錠側に権限設定を可能としているため、個人が 1 つずつの鍵を保持すれば、キーターミナルを利用することなく個人を特定することができるよう配慮した。よって鍵と錠の最低限のセットでの運用が可能である。また病原体管理システムのログ情報と突合せることでより有用なセキュリティの確保が可能となった。

F. 健康危険情報
特記すべきことなし。

G. 研究発表
なし

H. 知的所有権の出願・取得状況（予定を含む）
1. 特許取得
なし
2. 実用新案登録
なし
3. その他
なし

30. 病原体保管庫の施錠、鍵管理、開閉ログシステムの検証（平成22年度）

研究分担者：篠原　克明　国立感染症研究所　バイオセーフティ管理室　主任研究官
山本　明彦　国立感染症研究所　細菌第二部　主任研究官
研究協力者：小松　亮一　ヤマトシステム開発　㈱
神林　敬吾　ヤマトシステム開発　㈱

研究要旨　バイオセーフティ・バイオセキュリティの観点から、病原体管理を行なう上でフリーザーの施錠管理は重要である。平成20年度までは電子錠付きのフリーザーを開発しFelicaにてユーザー認証を行ない、開閉ログを取得するものを検討したが、新規導入には非常に高価であり、既存フリーザーへの取り付け工事も容易ではなく、汎用性には欠けている面も指摘された。平成21年度は開閉ログを取得できる南京錠タイプの電子錠を開発して既存フリーザーにも取り付けが容易な汎用性のあるものを考案した。この南京錠タイプの電子錠で「誰が」「いつ」「どの南京錠」を開閉したか管理することで、どのフリーザーが開閉されたかを判別する方式を採用した。現状では、研究員がログ管理と台帳管理を手作業にて行なっているが、本ログ管理システムを用いることにより、作業の効率化と簡便化が行えることが好評価された。また、キー1本1本に開閉権限を与える(アクセス権限)ことにより、研究員の扱うことができる病原体に特化した設定を行なえば、自動的にフリーザーへのアクセス権限も確立する。また課題として、アクセス制限を行っても、キーを他人に「貸与した」あるいは「盗難にあった」場合の「なりすまし」というセキュリティの脆弱性が懸念されており、本年度は「なりすまし」を防止するセキュリティ強化について検討を行った。

A．研究目的

前年度開発した南京錠タイプの電子錠の脆弱性である他人への貸与、盗難によるなりすましを防止するセキュリティ向上について検討を行なった。

B．研究方法

前年度までは、ユーザーはまずキーターミナルを開ける権限が設定されていることが必要であった。ターミナルを開けてからはユーザー毎に持ち出せるキーを制限することで、二重のセキュリティを設けていた。

また、南京錠側でキーの固有番号を判別し、キーを特定することが出来た。さらに、病原体管理システム(ICBSシステム)内で病原体へのアクセスログを一元管理するためには、キーターミナルと南京錠それぞれから開閉履歴を取得できることが必須であった。

本年度は、上記の条件に加え、「なりすまし」防止を追加するために、必要な技術調査を行った。さらに、上記の脆弱性を低減できることが可能かどうか検証するために、ボツリヌス毒素、ジフテリア、関連試薬などを管理している施設において、実運用試験を行なった。

1．なりすましの考え方

「なりすまし」防止の基本は、個人を特定できることにある。個人を特定する方法として、生体認証や暗証番号などがある。生体認証には静脈認証や指紋認証、虹彩認証などがあるが、どれも高価であり常に電源を必要とするため、南京錠に合わせて組み込むには現実的ではない。また、既存のフリーザーへの取り付けも容易ではなく、現実的ではない。暗証番号については、ＡＴＭやクレジットカードの認証にも採用されており、比較的容易に利用可能である。

2．暗証番号の決定

固定番号では他人に教えてしまえばキーの貸し借りと全く変わらない。しかしながら、番号を容易に変更することが可能であり、頻繁に番号変更を行えば、暗証番号を変更した本人あるいは変更に立ち会った人間のみが暗証番号情報を認識することができるのみであり、個人認証の強化につながると考えられる。

3．製品の選定

前年度に検討を行ったアクセス権限設定機能があり、開閉ログの取得可能であるものについて、上記1.2.の考え方を加味したものについて調査、選出を行った。具体的には、「フリーザーロックシステム(型番:RPWH-Y0001)」を選出して検証を行なった。

・フリーザーロックシステム
(型番:RPWH-Y0001)
内容物：
・モバイル封印錠(図1参照)(型番：RPWH-Y00PL)
機能／南京錠タイプ、開閉ログ取得、解錠権限設定、パスワードとの二重ロック、ローバッテリーLED。
・キーターミナル(図2参照)(型番：RPWH-Y00KT)
機能／解錠権限設定、キーへのパスワード書き込み、キーの取り出しログ取得機能。

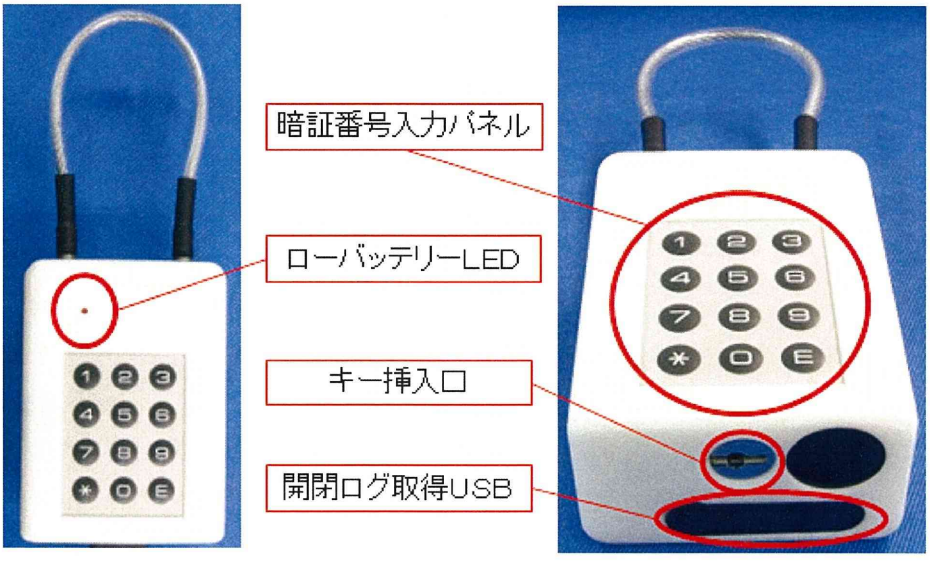


図１．モバイル封印錠

図２．キーターミナル

４．運用開始への条件を検討

モバイル封印錠(型番：RPWH-YOOPL)自体に二重ロック機能を持たせたものを使用した。この二重ロックは「解錠権限にて設定された専用のキー」と「キーターミナル(型番：RPWH-YOOKT)からキーに発行(書き込み)されたパスワード」が一致しなければ解錠できない。この機能により、キーを他人に貸与、盗難による「なりすまし」のリスクを低減できた。また、キーターミナルは個人のFelicaカードにて扉の開閉が可能であるため、モバイル封印錠と合わせて3重のロックを設けたこととなる。

また、ローバッテリーについても検討した。この仕様はキーを挿入した時点でバッテリーが少なければLEDを点滅させて知らせてくれる。よって、フリーザーを開ける際にバッテリー消耗にて開けることが出来ないというリスクも低減できた。

さらに、キーターミナル(型番：RPWH-Y00KT)のパスワード発行にも脆弱性がないか検討した。このキーターミナルは下記のパスワード発行設定が可能である。

(1)パスワード発行方法がランダム発行か任意設定か固定発行を選択可能

(2)パスワード桁数が2桁～12桁で選択可能。

まず(1)の固定発行については、パスワード変更が容易でない、運用上周知徹底が容易でない、内部犯行が容易、人の判別がしにくい、モバイル封印錠の二重ロックの意味が薄い、など多数の不安要素がある為不採用とした。

任意設定については、使用者が覚えやすい暗証番号を2桁～12桁で設定可能であるが、使用者の生年月日や個人番号、いつも同じ番号など他人にも解読されてしまうリスクも考えられるため不採用とした。

以上より、常に違う番号を書き込むランダム発行を採用して運用することにした。

次にランダム発行という条件かつ、(2)のパスワード桁数は2桁、3桁ではあまりにも短すぎる為不採用とし、人間が簡単に覚えられ、かつ機密性もある範囲での4～6桁が適切であると考え、今回は4桁にて検討を行なった。

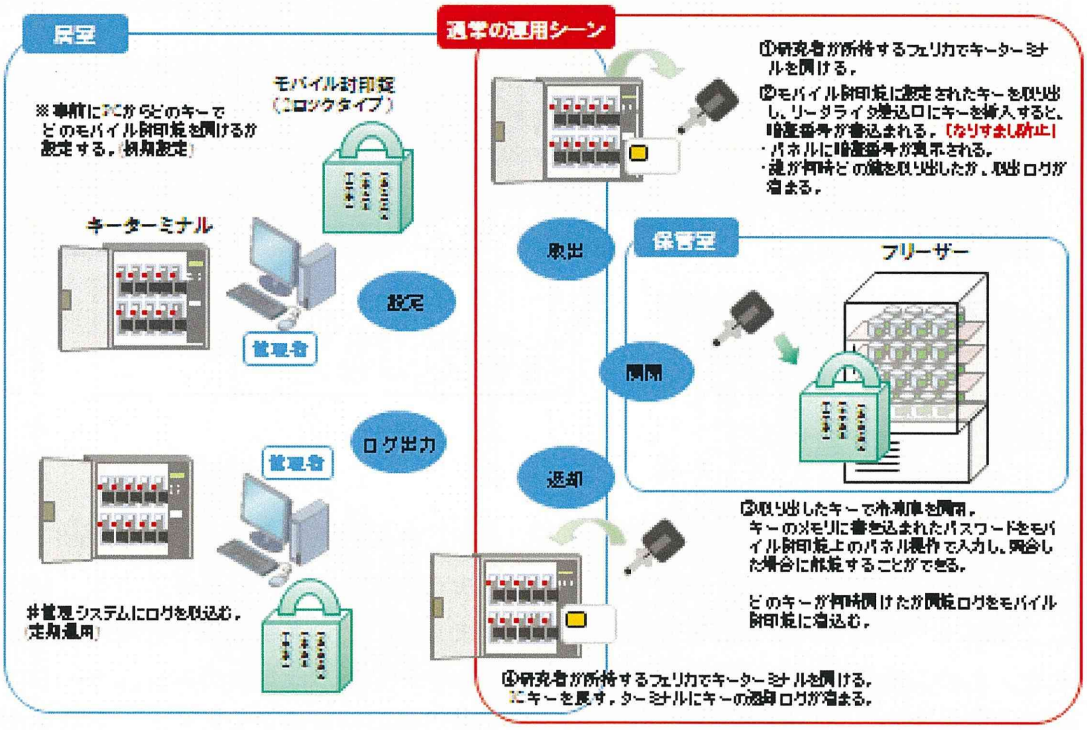


図３．運用イメージ

C．結果

結果として下記の様な①～④の操作をすることでなりすまし防止の考え方が成立し、セキュリティの脆弱性を低減させることが可能となった。(図3参照)

① 研究者が所持するフェリカカードでキーターミナルを開ける。

② モバイル封印錠に設定されたキーを取り出し、リーダライタ差し込み口にキーを挿入すると暗証番号が書き込まれる。(この時点でなりすまし防止の考え方が成立する)

・パネルに暗証番号が表示される。

・誰が何時どの鍵を取り出したか、取出ログを取得する。

③ 取り出したキーでモバイル封印錠を開閉。(同時にフリーザーを開閉)

・キーのメモリに書き込まれたパスワードをモバイル封印錠上のパネル操作で入力し、照合した場合に解錠することができる。

・どのキーが何時開けたか開錠ログをモバイル封印錠に溜込む。(誰が使用したキーなのかがわかる)

④ 研究者が所持するフェリカでキーターミナルを開け、IC キーを戻す。

・ターミナルにキーの返却ログが　取得される。

このシステムを利用する前に必ず初期設定を行なう必要があり、この時点でアクセス権限が成立する。

※ 初期設定：事前に PC から誰がどのキーを使用出来て、どのキーでどのモバイル封印錠を開けるか設定する。(図 3 参照)

また、ログ情報を定期的に取得することも行なえば、台帳管理のサポート及び運用方法の監視・管理・確立により効果的である。

＃ 定期運用：管理システムにログを取得。(図 4 参照)

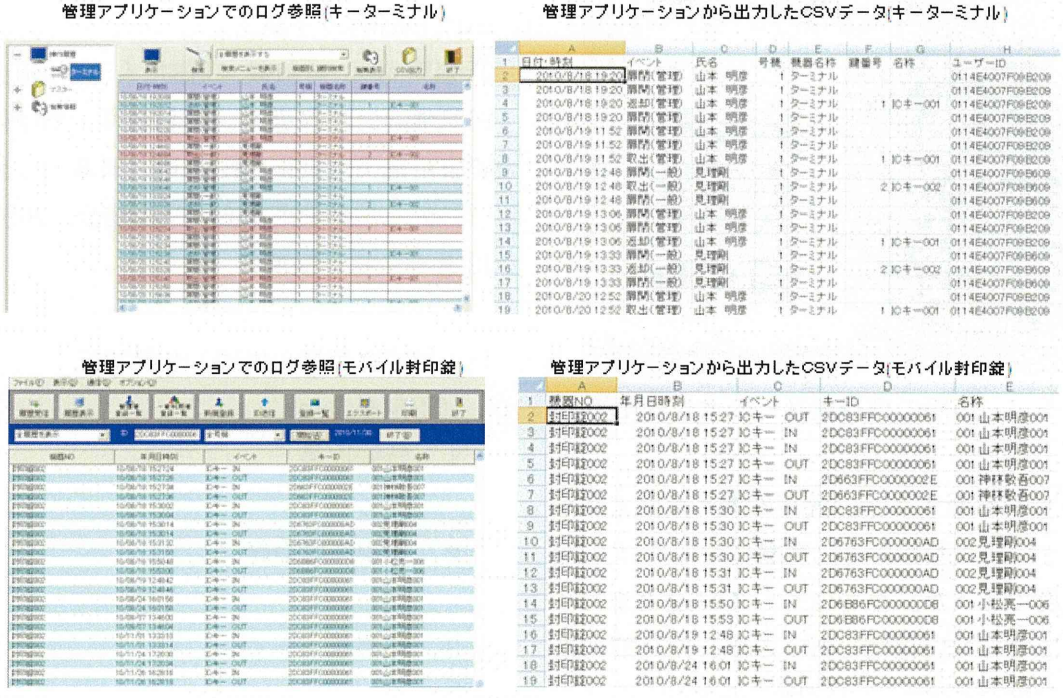


図４．　ログ参照画面、ＣＳＶデータ

D，E．考察及び結論

前年度から引き続き既存のフリーザーには容易に取り付けが可能な南京錠タイプの電子錠が有用であることが確認されている。なぜなら既存のチューブの入っているフリーザーに電子錠の取り付け工事を行なうとなれば、チューブをどこか別のフリーザーへ移し替えしなければならず、サンプルのダメージを伴うことが免れない。保存されているチューブに影響を与えずに取り付けることが必須の条件となる。また、バイオセーフティ及びバイオセキュリティの観点上、「いつ」「誰が」というアクセス管理が重要であり、今回検討したモバイル封印錠の二重ロックは個人特定の必須条件となり得ると思われる。ただし、課題として、モバイル封印錠の大きさが指摘された。

図５．　市販の携帯電話との大きさ比較

図５を参照すると、既存の携帯電話よりも大きいことがわかる。重量については450g程度であった。重さについては運用上特に気にならない程度であったが、南京錠の世間一般のイメージは安価で小さいものある。今回のものは、暗証番号入力用のタッチパネルがあるため、必然的に図５程の大きさになってしまう。運用上この大きさには問題は生じないが、より小さくなることが望ましいとの要求もある。また、ワイヤー部分に脆弱性がある。

今回の検討では、本「施錠、鍵管理、開閉ログシステム」は、「なりすまし」防止の解決には有効性が確立できたが、今後ワイヤー部分の脆弱性の改善について検討を行い、実用配備を可能とする。

Ｆ．健康危険情報

特になし。

Ｇ．研究発表

1）Shinohara, K., Kurata, T., Takada, A., Komatsu, R., Hayakawa, N., Development of a security padlock. American Biological Safety Association, 53rd Annual Biological safety Conference, October 4-6, 2010. Denver, USA.

2）篠原克明、倉田毅、高田礼人、早川成人、梶原唯之、小松亮一、神林敬吾：病原体保管庫用電子南京錠。第10回　日本バイオセーフティ学会学術総会・学術集会、2010年12月6-7日、横浜。

Ｈ．知的財産権の出願・登録状況

（予定を含む）

１．特許取得

なし

２．実用新案登録

なし

３．その他

なし

31. 病原体保管庫の施錠、鍵管理、開閉ログシステムの検証（平成 23 年度）

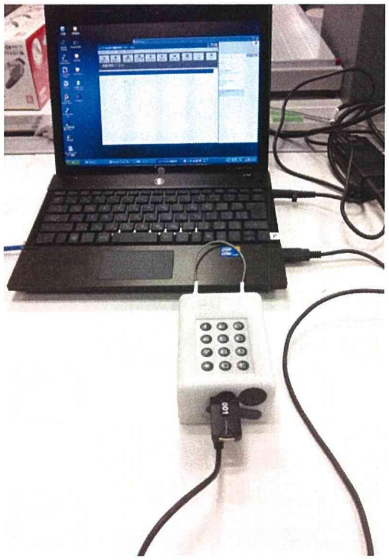
研究分担者：篠原　克明　国立感染症研究所　バイオセーフティ管理室　主任研究官
山本　明彦　国立感染症研究所　細菌第二部　主任研究官
研究協力者：小松　亮一　ヤマトシステム開発　株式会社

研究要旨　バイオセーフティ・バイオセキュリティの観点から、病原体管理を行なう上でフリーザーの施錠管理は重要である。昨年度までの研究にて、既存のフリーザーへの取付けが簡単な南京錠タイプの電子錠を検討してきた。キー1 本 1 本に開閉権限を与え(アクセス権限)、研究員の扱うことができる病原体に合わせて設定を行ない、「誰が」「いつ」「どの南京錠」を開閉したかを履歴を取ることで、自己申告制で記録している管理台帳のサポートと物理的なセキュリティを強化してきた。さらに、前年はなりすまし防止(暗証番号との 2 重ロック)をすることによりセキュリティレベルの向上を確立してきた。しかし、今までセキュリティ向上にポイントを当ててきた反面、本年度は実際の実験室での履歴の吸い上げをする操作性の悪さが声として上がった。

A．研究目的

今までの既存のフリーザーに後付できる南京錠タイプをもとめてきたが、開閉履歴を吸い上げる際に図 1 のように管理ＰＣの近くに鍵を持ってくる運用が必須であり、操作性の悪さがあった。

図 1



この操作をしないと、履歴の吸い上げができない。

鍵を常にフリーザーにつけて運用しているが、履歴を吸い上げるときだけフリーザーからはずして管理ＰＣの近くに持ってくる操作は非常に手間であり、そもそも実験室にＰＣを設置しておかなければならない。全ての実験室にＰＣが設置されていないため、ＰＣがない実験室では、わざわざ実験室外への持ち出しをしなければならなくなる。これは現実的ではないので、フリーザーから外さずに履歴を吸い上げる方法を検討する。

B．研究方法

フリーザーから鍵を外さずに履歴を吸い上げる方法を解決できる可能性のある、無線(ZigBee)通信を搭載した開閉ログを取れる製品を採用して検証を行った。この製品は昨年度の製品の後継機に価するもので、平

成 24 年度以降に正式にリリースされるものである。
製品名：フリーザーロックシステム(ZigBee 通信タイプ)
型番：SKC-Y3000-ZB

図２ー３内容物
図 2
製品名：デジタル@IC ロック
型番：SKC-Y3000-LC

この製品は南京錠タイプではなくフリーザーへの外付け工事が必要なタイプ。
(ZigBee 通信子機内蔵)

図 3
製品名：Zi g Bee 受信機
型番：SKC-Y3000-RC

親機：子機＝1：n の通信が可能。

図 4
製品名：デジタル@IC ターミナル
型番：SKC-Y1020-KT

キーを 10 本保有。

この製品の特徴
1. アクセス権設定
昨年度までの製品の後継機であるため、今まで必要とされてきたアクセス権限設定機能は有している。(キー1 本 1 本に開閉権限を与え、研究員の扱うことができる病原体に合わせて設定を行なう機能)今回は 2 重ロック機能を有していない。

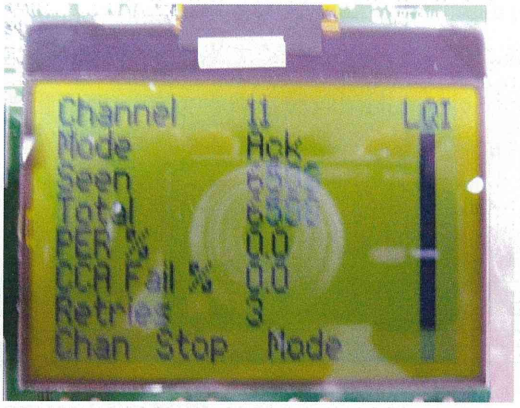
2. 無線(ZigBee)通信機能
無線(ZigBee)通信は「開閉アクション時(ロックの開閉がされた時)」に管理ＰＣへ履歴を飛ばす。また、管理ＰＣ側のソフトウェアで「開錠放置(開けたステータスのまま一定時間放置された時)」と「通信遮断時」に異常開放の通知がされる。この無線(ZigBee)通信機能は双方向の通信が可能で、アクセス権設定をロック側に送信できることと、ロック側の時刻同期ができる。また、中継器を使うことでより遠方にかつ壁が厚い部分でも回避して通信ができる。
この無線(ZigBee)機能で開閉履歴を手間な

く取得できるかを実際の実験室で通信テストを行なった。RI 実験室(P3)にて無線(ZigBee)通信の通信状態を把握できる図 4のようなアンテナを使って実証実験をした。

図 5

左：子機(ルータ)
右：親機(コーディネータ)

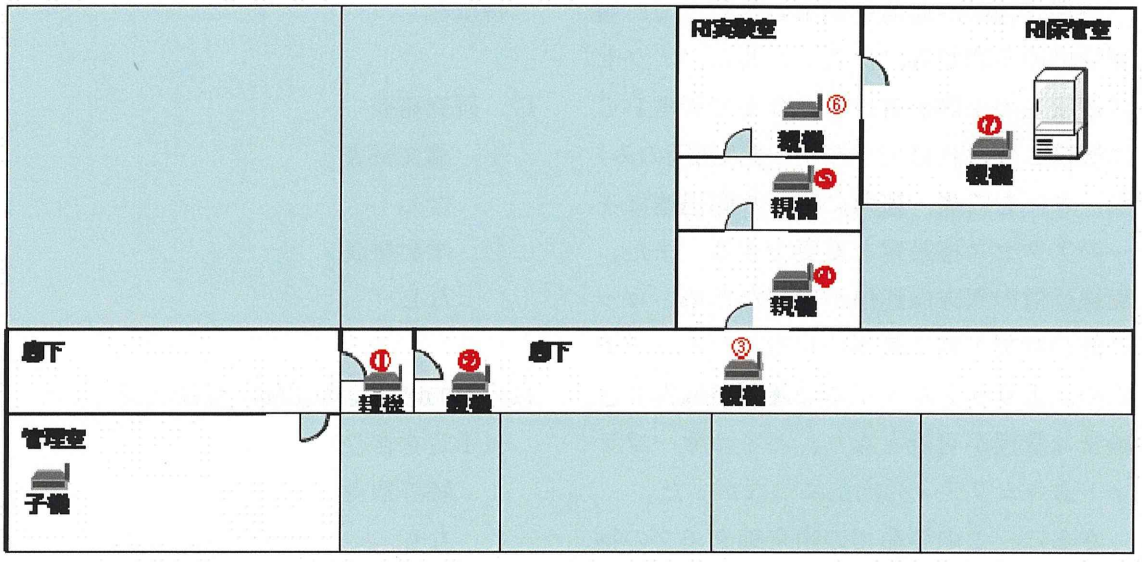
図 6



親機(コーディネータ)の計測画面／右側のゲージが通信状態を表わす。

子機を固定させ、親機を各扉や各部屋がある図 7：計測ポイントイメージの①～⑦の様なポイント(通信が遮断される可能性のある場所)で通信計測した。

図 7：計測ポイントイメージ



C．研究結果

管理室からRI保管室(図 7：計測ポイントイメージの⑦)までは子機・親機の 1to1 では通信不可であった。管理室から図 7：計測ポイントイメージでの④までは通信可能であった。図 7：計測ポイントイメージ④から⑦までも通信可能であったので、図 7：計測ポイントイメージの④のポイントに中

継器を置けば管理室からRI保管室まで通信可能であることが判明した。これで、実験室にＰＣを設置しなくても管理室側からフリーザーの開閉履歴を取得でき、施錠管理が可能となることがわかった。

図８：通信テスト結果

No	エンドデバイス子機(発信機) 固定ポイント	ケースNo	コーディネーター親機(受信機) チェックポイント	扉数	扉厚(mm)	部屋数 (間の部屋)	距離(mm)	チェック 結果	受信機の感度 (メーター値)	備考
1	バイオセーフティ管理室	1-1	廊下(2)	1	600	0	3000	○	90%	
		1-2	前室(1)扉1閉める	2	1200	1	6700	○	70%	
		1-3	前室(1)扉2閉める	3	1800	2	8000	○	50%	
		1-4	RI汚染検査室前	3	1800	2	33700	○	30%	
		1-5	前室(2)扉1手前	3	1800	2	42000	○	30%	
		1-6	前室(2)扉1閉める	4	2400	3	43100	○	20%	
		1-7	屋外(前室(2)から出る)	5	3000	4	44200	×	通信エラー	
		1-8	RI汚染検査室　扉閉める	4	2400	3	33700	×	通信エラー	防火扉の為
2	廊下(3)(前室(1)の手前)	2-1	RI汚染検査室前	0	0	0	25600	○	90%	
		2-2	RI汚染検査室	1	600	0	25600	○	50%	
		2-3	RI更衣室	2	1200	1	28100	○	20%	
3	RI汚染検査室前	3-1	屋外(前室(2)から出る)	2	1200	1	10500	○	10%	
		3-2	屋外(前室(2)から出て5m程離れた場所)	2	1200	1	15500	×	通信エラー	
4	RI汚染検査室	4-1	RI汚染検査室	0	0	0	0	○	100%	
		4-2	RI更衣室	1	600	0	2500	○	90%	
		4-3	RI測定室	2	1200	1	4500	○	80%	
		4-4	RI実験室(1)	3	1800	2	6000	○	60%	
		4-5	RI実験室(2)	3	1800	2	6000	○	60%	
		4-6	RI保管庫	3	1800	2	7000	○	40%	

No	エンドデバイス子機(発信機) 固定ポイント	ケースNo	コーディネーター親機(受信機) チェックポイント	扉数	扉厚(mm)	部屋数 (間の部屋)	距離(mm)	チェック 結果	受信機の感度 (メーター値)	備考
5	RI汚染検査室前	5-1	RI汚染検査室	1	600	0	500	○	70%	
		5-2	RI更衣室	2	1200	1	3000	○	50%	
		5-3	RI測定室	3	1800	2	5000	○	30%	
		5-4	RI保管庫	4	2400	3	7500	×	通信エラー	防火扉の為

Ｄ，Ｅ．考察及び結論

無線(ZigBee)通信を採用したことで、履歴受信の手間が省けたことと共に、アクセス権設定の手間が省けた。今まで管理ＰＣに接続しなければできなかった(初回のみ)が、キーを紛失・盗難にあった際迅速にキーのアクセス権設定を変更できる。また、無線通信の双方向通信が可能なため、ロック側の時刻が常に最新の状態となる。そのため、よりリアルタイムな履歴が取得でき、厳密な管理が可能となり、バイオセーフティ・セキュリティの向上につながった。

さらに、この製品での南京錠タイプの物であれば工事が必要なくなり、なりすまし防止の考え方(暗証番号による２重ロック)を取り入れることができれば、よりレベルの高いバイオセーフティ・セキュリティが確立されると考える。

Ｆ．健康危険情報

特になし

Ｇ．研究発表

１．論文発表

なし

２．学会発表

なし

Ｈ．知的財産権の出願・登録状況

(予定を含む)

１．特許取得

なし

２．実用新案登録

なし

３．その他

なし

32. 研究機関間の病原体輸送に関する位置情報測定機器の検証

研究分担者：篠原　克明　国立感染症研究所　バイオセーフティ管理室　主任研究官
倉田　　毅　富山県衛生研究所　所長、国立感染症研究所　名誉所員
高田　礼人　北海道大学　人獣共通感染症リサーチセンター　副センター長、国際疫学部門　教授
駒野　　淳　国立感染症研究所　エイズ研究センター　第三室　主任研究官
研究協力者：綿引　正則　富山県衛生研究所　細菌部　副主幹研究員
滝澤　剛則　富山県衛生研究所　ウイルス部　部長
小松　亮一　ヤマトシステム開発　㈱

研究要旨　平成 18 年度から平成 20 年度の研究で行われた輸送実験では、鍵付き搬送器具、GPS 端末などの検証を行ってきた。これまでの研究目的は、煩雑な事務手続きの簡素化、輸送中のセキュリテリの厳格化であった。平成 21 年度からの研究目的は実用化である。これまで開発をしてきた機器類の有用性はすでに検証できているが、新規開発品のためコスト高は否めない。そこで、機能は制限されるものの、より簡便且つ各機器本体及び通信費のコスト減を目的に、一般に流通している機器の応用とその有用性、実現性について検討を行なった。

A．研究目的

これまでの開発の基本的な要旨は踏襲しながらも、誰もが利用可能な市販携帯電話の GPS 機能、GPS ロガーなど一般的な機器を活用した場合の測位情報、通信費用についてデータを収集した。特に総務省は、「2007 年 4 月以降、携帯電話事業者が新規に提供する第 3 世代携帯電話端末については、原則として GPS 測位方式による位置情報通知機能に対応する」としており、普及率などからして、今後活用が期待できる機器である。今回は乗用車、鉄道、混載トラックの３つの輸送手段で携帯電話を使った測位方法を検証した。

B．研究方法

（１）乗用車での輸送

「病原体輸送の取扱要領」に定める第 1 種から第３種の病原体を輸送する想定で検証を行った。乗用車で国立感染症研究所の戸山庁舎を出発し、富山県衛生研究所までの間を携帯電話（AU）、GPS ロガーで測位を行った。携帯電話は約 1 分間隔で位置を測位し、サーバーと通信を行い WEB 上の地図に現在地をプロットする。今回は汎用性に重点を置いているので、携帯電話側に特別なアプリケーションを持たず、基本機能で URL を特定しサーバーとの通信を行うことにした。また、携帯電話がエリアの電波状況の問題などで通信できず、位置情報が取得できない場合のバックアップ手段として GPS ロガーを携帯し、後に実験と同時間帯

のログを取得することにした。携帯電話が１分毎に GPS 測位、サーバーとの通信を行った場合、相当な電池消費量が想定されるが、今回は別途小型の携帯バッテリーに接続し、東京から富山県までの移動時間である約５時間以上の電源供給を継続的に確保した。(図１機器の構成) 精度の検証に付いては、地図上に示されるプロットにカーソル番号を表記し、その精度が状況によってどのように変化するか、明らかになるようにした。(表１プロットカーソルとその意味)。輸送手段に付いては第一～第三種までを想定した専用車（今回は乗用車）輸送、参考として鉄道、混載トラックも検証を行った。

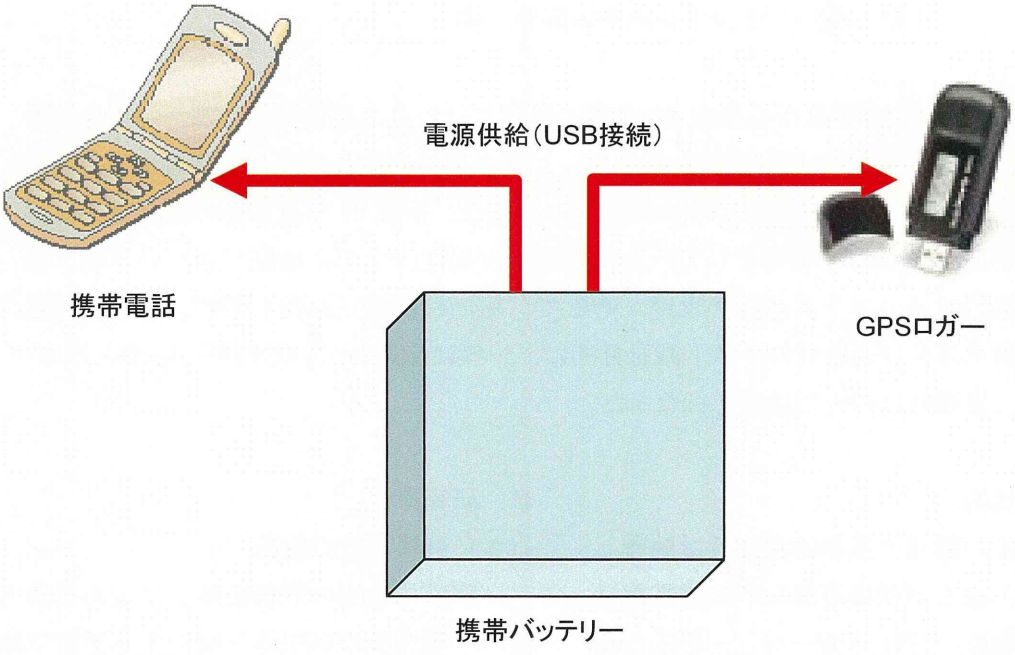


図１．機器の構成

表１．プロットカーソル番号とその意味（参考・推測）

番号	意味
0	GPS_ FIX:GPS のみ
1	HYBRID_FIX: GPS と基地局を利用した測位
2	AFLT_FIX: 複数基地局からの位置で測位
3	測位不可能 (プロットされません)
4	SECTOR_CENTER: セクタセンタ(指向性アンテナがカバーしている区域)単一基地局による測位
5	PREFIX_AFLT: BTS(単一基地局)による測位

（2）鉄道での輸送

鉄道については JR 小杉駅ー富山ー越後湯沢ー大宮ー東京ー早稲田の経路で情報の採取をした。越後湯沢ー大宮間は上越新幹線、東京（大手町）ー早稲田間では地下鉄東西線を利用した。

（3）混載トラックでの輸送

混載輸送では、宅配会社を利用しトラック内、中継基地の精度を検証した。東京都江東区東陽での集荷から有明の仕分け拠点までをトラックで輸送した。

C．研究結果

位置情報の精度については状況に応じて下記のような結果となった。

（1）結果概要

往路、復路を通して見ると、往路の乗用車での輸送経路ではトンネルや山間部ではやや精度がばらつく部分があるものの、比較的正確な測位ができていた。しかしながら、復路の鉄道で移動をした際は、上越新幹線の越後湯沢、高崎間での測位はプロットがほぼすべて抜け落ちており、測位が不可能であった。また、混載輸送も想定して、宅配業者のトラックでの測位も行ったが、バッテリーの問題、トラック内での測位に課題が見られた。また建物内の一箇所にとどまった場合の測位結果も非常にばらつきがあることがわかった。

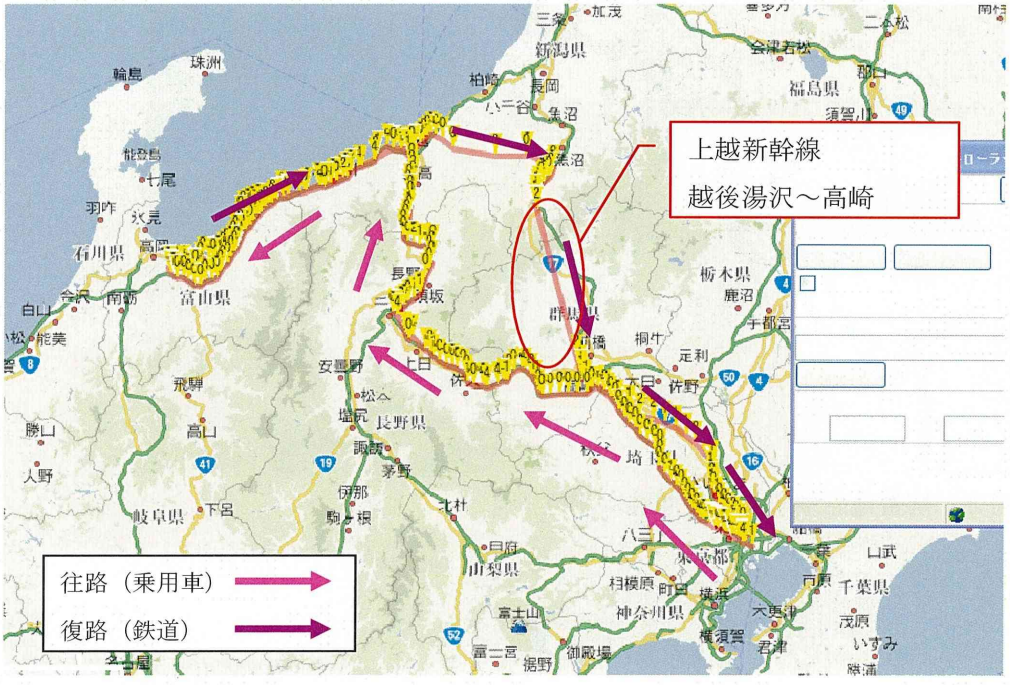


図２　往路、復路の測位情報のプロット状況

（２）乗用車での輸送

新宿戸山を出発してから富山県射水までの間、山間部を除いてほぼ正確な位置を把握できる状況であった。山間部のトンネルでの測位は携帯、GPS ロガーでもほぼ測位は不可能であるが、GPS、基地局を捕らえることが出来れば一応、地図上にはプロットされるが（図３，図４）、精度に付いては大きな誤差がみられた。図３ではトンネル部分を携帯で測位したもの、図４では GPS ロガーで測位したものである。携帯で測位したプロットカーソルが４、５と単一基地局を示しているため基地局の位置を示していると思われる。そのため実際の高速道路の位置からかなり離れた位置にプロットされている事がわかる（図３参照）。一方 GPS ロガーの場合は基地局での補足はできないものの、トンネルを出たところではほぼ正確な位置を補足している。対象物が動いている場合、1 分単位ではあるが連続で測位をしていれば、方向性などの予測がつきやすく、特に高速道路を進んでいる場合は道沿いに位置がプロットされるためどの道路上をどの方角に進んでいるか判断が比較的容易である（図４参照）。

図３　携帯電話端末で１分間隔に測位

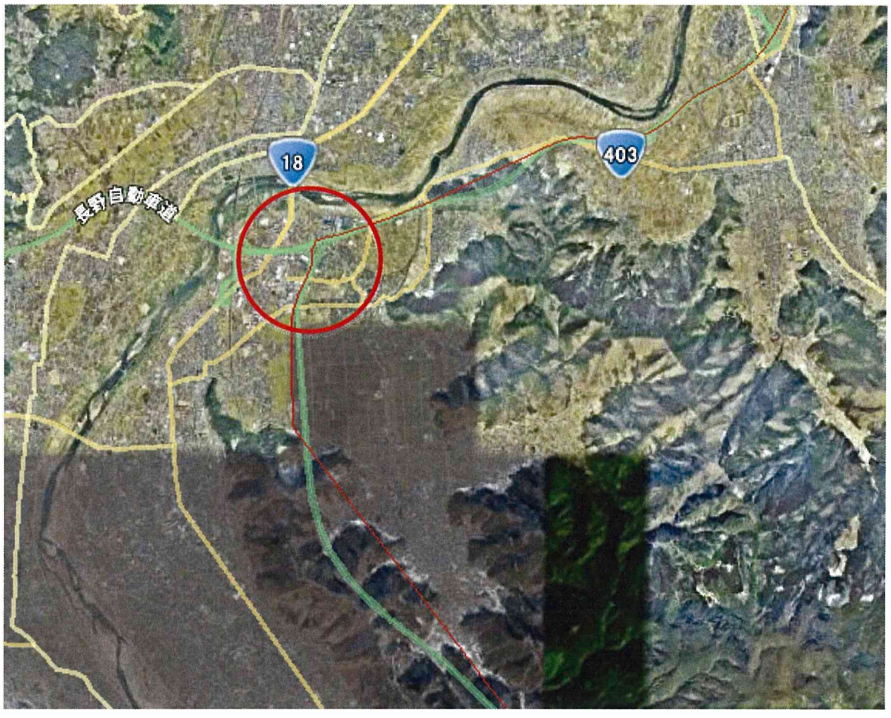


図４　GPS ロガーで一秒間隔に測位