Vol.2015-DPS-165 No.13
2015/12/11

インフラ維持管理業務におけるスマートデバイスの利用に関する考察

長橋和哉[†1]　後藤厚宏[†1]

概要：インフラ維持管理には，点検業務がある．点検業務は安全なインフラを維持するために必須である．点検業務はロボット技術などを活用した自動測定もあるが，現状，作業員が現地に赴き点検対象物を確認する巡視・巡回による点検が主である．そのため，作業員は，現地に点検対象物の設計仕様や設計図を持ち出し，確認する必要がある．現在，このような点検業務を支援する目的としてスマートデバイスの利用が考えられる．本稿では，点検業務と情報システムのフローを整理し，その上でスマートデバイス活用に関するセキュリティ上の課題を挙げる．また，それらを解決するために現状のスマートデバイス活用事例を分析し，考察する．

キーワード：点検業務，オフライン環境，スマートデバイス，セキュリティ

A study about use of the smart devices in infrastructure maintenance

KAZUYA NAGAHASHI[†1]　ATSUHIRO GOTO[†1]

Abstract: Infrastructure maintenance includes inspection work. Inspection work is indispensable in order to maintain a safe infrastructure. Although inspection work is partly done by the automatic measurement which robot technology is applied to, it is mainly done by human workers who go to the field and inspect the various items using their eyes and hands. Therefore, workers bring out specifications and the design chart of inspection subjects there. The application of smart devices is increasing as a purpose of supporting such inspection work now. In this paper, I confirm the flow of inspection work and an information system. I look up the problem on the security about smart devices for inspection work. And, in order to solve them, I analyze and consider the present smart devices practical uses.

Keywords: inspection work, offline environment, smart devices, security

1. はじめに

社会を支えるインフラ事業(道路，鉄道，港湾，航空，水道，通信など)には維持管理業務が必要である．内閣府が進める SIP(戦略的イノベーション創造プログラム)においてもインフラ維持管理・更新・マネジメント技術がテーマとして取り上げられている[1]．SIP により進められているインフラの維持管理フローを図 1 に示す．

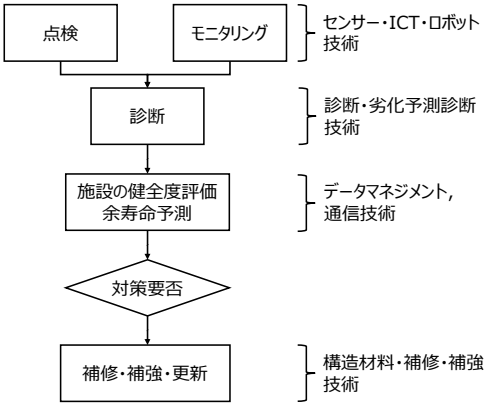

図 1 インフラ維持管理フローと基盤技術([1]を基に修正)

膨大なインフラの維持管理に対処するためには，維持管理フローの高効率化が必要であるため，SIP では，センサーやロボット技術を活用した点検・モニタリング業務の改善について研究開発が実施されている．SIP で検討されているようなセンサー・ロボット技術を駆使した自動点検もあるが，現状，インフラの維持管理における点検業務は，点検作業者が現場を巡回し目視，測定，打診等による作業も多い．

このような点検業務には，持ち運びが容易であり，点検対象の機器，施設をカメラで撮影可能なスマートデバイスの適用が考えられる．この際，スマートデバイスに点検時の判断基準となる情報を組込み，事業所から点検業務の現場へ情報を持ち出す必要性がある．しかし，持ち出す情報は設計情報や図面の情報など企業等にとって重大な情報であり，スマートデバイスの盗難・紛失により格納されている情報が漏えいした場合，設計情報，図面から物理的な脆弱性が分析され，弱点をさらけ出すことになってしまう．また，ICT の技術的観点から点検業務を分析すると，地下や山間部，高電圧を取り扱う箇所などで実施されることもあり，常に安定したネットワークの接続性を享受できるとは限らないという特徴もある．

本研究では，インフラ維持管理業務の一例として，点検業務を挙げ，セキュリティ上の課題を挙げる．また，課題に対する改善策を提案する．

†1 情報セキュリティ大学院大学

2. インフラ維持管理業務と情報システムの構成

インフラ事業(道路，鉄道，港湾，航空，水道，通信など)の維持管理業務には点検業務がある．点検業務は建物，通信路，管路といった対象物が，構築時の仕様から経年劣化や気温，湿度，天候などの影響により大幅にずれていないか，ずれが安全の範囲であるかを把握する業務である．安全ではないと判断した場合，点検業務から補修・補強業務に移行し，適切な処置を行う．

2.1 本研究の目的

点検業務でスマートデバイスを活用する場合に必要となるセキュリティ上の要件を整理する．点検業務以外の事例も含め，スマートデバイスを活用している先行事例を分析し，点検業務との共通点等を見出す．これらの結果から，課題の解決法，技術的取り組みを見出し，机上による評価を行う．

2.2 点検業務の特徴

水道局の業務を例に考察する．東京都水道局は，約 15 の支所等があり，技術・技能職には約 2,000 人が属している．定期点検要領等に定められた内容に基づき点検等の維持管理を行うため，点検業務には多くの人が携わっている．

点検業務の特性を図 2 に示す．点検業務では，水道管の敷設状況を確認するために図面や，管路の仕様，設置時期，点検履歴などの重要な情報を持ち出す必要がある．また，水道の管路は地上だけではなく，山間部やマンホール内の地下空間に配備されている．そのため，点検業務時，安定したネットワーク環境を利用できるとは限らず，システムはオフライン環境を前提とする要件がある．また，点検業務完了後は，次回以降の点検時に利用するため，点検結果を台帳へ更新する必要がある．

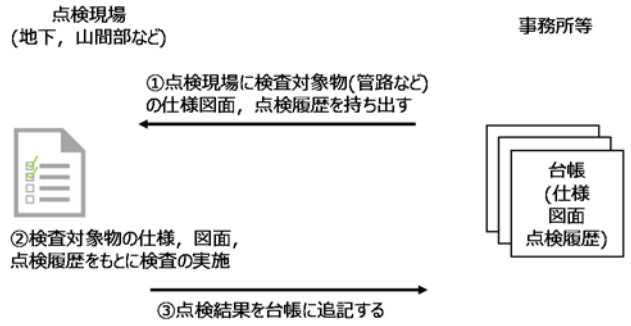

図 2 点検業務の特徴

2.3 点検業務における情報システムの構成

点検業務は，巡視・目視などにより構築時の仕様と現時点の測定値がどれだけ乖離しているかを確認する業務である．よって，点検業務では，確認の指標となる仕様や安全係数を考慮した値と比較する必要がある．そのため，業種や点検を必要とする機器の数にもよるが，図 3 に示すような仕様を管理する情報システムが存在するものと想定する．インフラ事業者は，点検対象となる機器の増設，撤去があった場合，仕様管理システムに対し，追加登録，削除を行う．

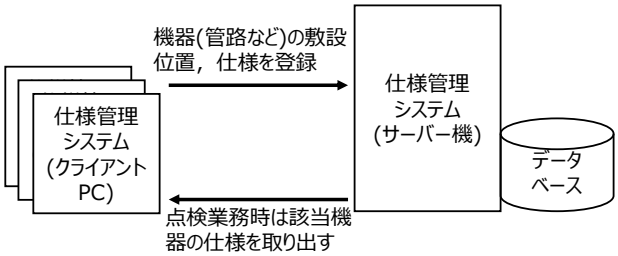

図 3 仕様管理システムの構成例

仕様管理システムを利用した点検作業時の業務フローを図 4 に示す．点検作業時，作業者は仕様管理システムから点検に必要な仕様を取り出し(図中①)，紙などに印字して持ち出す(図中②)．作業者は機器が設置してある場所に赴き点検作業を行い(図中③)，点検結果を紙に記載する(図中④)．作業者は事務所等に戻り，点検結果を仕様管理システムに反映する(図中⑤) [2].

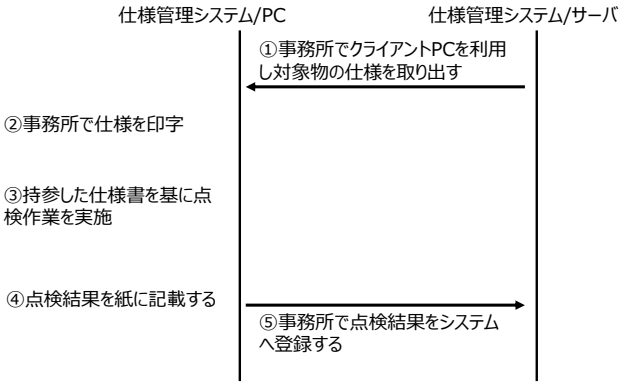

図 4 仕様管理システムを利用した点検時の業務フロー

2.4 点検業務へのスマートデバイス導入の目的

紙を利用した点検業務では，作業者が点検対象物の仕様，図面，点検履歴を点検現場で参照しつつ，点検結果をあらかじめ決められた様式に従い紙に記録する．よって，点検後，事務所等で記録用紙から仕様管理サーバへの登録作業が発生する．このような転記が発生することにより，情報システムへの登録遅延，転記時の誤りが発生する可能性がある[2]．スマートデバイスを導入することにより，作業者が点検現場で点検結果をデジタルデータとして記録し，点検業務完了後，事務所等において，作業者が仕様管理サーバへ点検結果を反映させるという仕組みを実現できる．よって，点検業務にスマートデバイスを導入することにより転記作業削減による業務効率の向上と転記時の入力ミスを防止することが可能となる．

また，点検業務では，作業者が点検対象をデジタルカメラにより撮影することがある．記録用紙にて点検業務を行う場合，作業者が事務所等に帰着後，点検対象物と撮影した写真の紐づけを行う必要がある．スマートデバイスを利用することにより，点検対象物の点検結果とスマートデバイスのカメラにより撮影した写真を関連づけて記録するこ

とが可能となり，作業者の業務量を減らしかつ，点検対象物に対する情報の一元管理を実現できる．

2.5 点検業務へのスマートデバイスの適用

点検業務にスマートデバイスを適用した場合，図 3 で示したクライアント PC の役割をスマートデバイスに変更させる方式がある．業務フローを図 5 に示す．図 4 と異なるのは仕様の印字，仕様書を基にした点検の実施，点検結果を紙に記載する部分である．図 5 では，これらの作業を直接，スマートデバイス上で行う想定である．

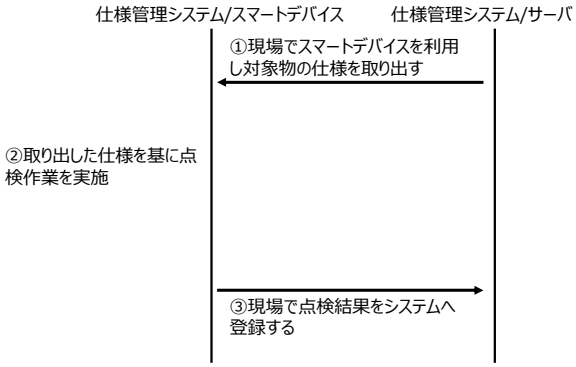

図 5 スマートデバイスを利用した点検時の業務フロー

しかし，この場合，スマートデバイスと仕様管理システム/サーバが常に通信可能な環境下にある必要がある．本研究では，スマートデバイスと仕様管理システム/サーバとの通信が不可能である環境(オフライン環境)を想定する．これは，道路・水道・電力などの点検業務の環境において，山間部や地下，または高電圧を取り扱う箇所などが存在し，安定した通信が常に可能だとは限らないためである．

オフライン環境を想定した業務フローを図 6 に示す．図 6 において，オフライン環境下で利用するのは③，④の業務である．

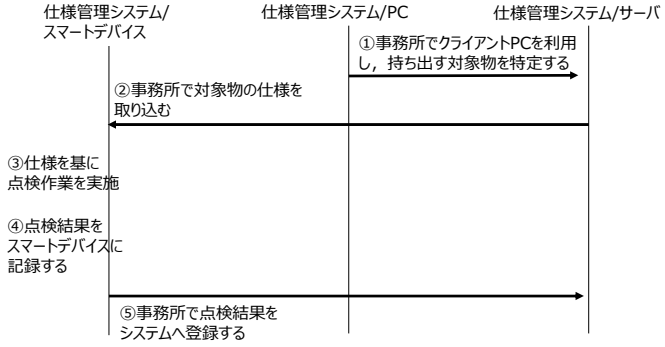

図 6 スマートデバイスを利用した点検時の業務フロー(オフライン)

3. 点検業務におけるスマートデバイス利用のリスク分析

点検業務でスマートデバイスを利用しようとした場合，オフライン環境を前提としたシステム構成を考える必要がある．

水道点検業務における情報資産を挙げ，情報資産の利用タイミングを 3 つ(事務所等における準備時，現場における点検作業時，点検作業終了後事務所等にてサーバへの登録完了時)に分け，リスク分析を行った．結果の一部を表 1 に示す．なお，表内の C,I,A の定義を表 2 に示す． 点検結果の測定値は，点検業務後からサーバ登録まで改ざん等が行われないデータの一貫性が求められる．点検履歴情報は読み取りのみであればスマートデバイス上のデータ改ざんが行われたとしても仕様管理サーバ上のデータが書き換わることはない．

表 1 水道点検業務における情報資産のリスク分析(一部)

項番	情報資産	準備時	作業時	完了時
1-1	管路の配管図	C	C,A	C
1-2	管路仕様			
1-2-1	管種(材質)	C	C,A	C
1-2-2	口径	C	C,A	C
1-2-3	布設時期	C	C,A	C
1-3	点検結果			
1-3-1	測定値	-	C,I	C,I
1-4	点検履歴情報	C	C,A	C

表 2 本研究における C,I,A の定義

性質	定義内容
Confidentiality	機密性が求められ，社外の者に渡ってはならない資産
Integrity	正常に業務を完了させるため，入力から仕様管理サーバ登録完了まで一貫性が求められる資産
Availability	点検業務を行うために利用が必須となる資産

また，水道業務の点検業務を時系列で分類し，従来の記録用紙を中心とした業務とスマートデバイスを利用した業務について，業務データを対象とした攻撃への対応策を比較した．比較結果の一部を表 3 に示す．記録用紙の場合，一部のデータを改ざん，または抜き取られてしまった事象を検知することは難しい．スマートデバイスの場合，一部データの改ざん，削除に対し技術的な対策により，検知することができる．一方で，スマートデバイスはデジタルデータを扱うため，データを容易にコピーされてしまう危険性がある．なお，攻撃者がスマートデバイス内のデータをコピーするためには物理的に攻撃対象のスマートデバイスを抑え，ケーブルを接続する必要があり，スマートデバイスの紛失・盗難対策が重要である．

水道点検業務の分析から，オフライン環境を前提としたスマートデバイス利用に対し，①点検対象物の仕様，図面，点検履歴情報といった業務データの持ち出し対策，②端末の盗難・紛失時に備えた対策，③点検結果の改ざん対策が必要であると考える．

表 3 記録用紙とスマートデバイスの対応策比較(一部)

項番	フェーズ	業務内容	想定する攻撃	記録用紙時の対応	スマートデバイス導入時の対応
4	現場業務(移動中)	作業員がファイリングしたデータを持ち，点検対象がある施設・場所に移動する	①一部データを書き換える ②ファイリングしたデータを盗む(一部または全部)	一部データを改ざん，削除することは容易である． 紙面上の情報は解読可能である．	一部データを改ざん，削除した場合，技術的に不整合であることを検出することも可能 一部データを盗む(複写)することは容易である 暗号技術により難読化することも可能である
6	現場業務(点検箇所)	図面から点検対象を特定し，点検業務を行う．この際，点検履歴のデータを確認する	①点検履歴データを一部書き換える ②ファイリングしたデータを盗む ③盗み見る	一部データを改ざん，削除することは容易である． 紙面上の情報は解読可能である． 「盗み見」は回避できない	一部データを改ざん，削除した場合，技術的に不整合であることを検出することも可能 一部データを盗む(複写)することは容易である 暗号技術により難読化することも可能である 「盗み見」はのぞき見防止フィルム(偏光フィルム)などを利用し，達成し辛くすることも可能
7	現場業務(点検箇所)	点検用紙に点検結果を記録する	①点検用紙に記録したデータを書き換える(改ざん) ②点検用紙を盗む	筆跡などが残るため改ざんは難しい 紙の点検結果は第3者が解読可能である	証跡を残さずに改ざんすることも可能である． 一部データを盗む(複写)することは容易である 暗号技術により難読化することも可能である
11	終了(事務所)	点検用紙から点検結果を仕様管理システムに登録する	①一部データを書き換える ②ファイリングしたデータを盗む(一部または全部)	一部データを改ざん，削除することは容易である．	一部データを改ざん，削除した場合，技術的に不整合であることを検出することも可能 一部データを盗む(複写)することは容易である 暗号技術により難読化することも可能である

3.1 業務データの持ち出し

オフライン環境を前提とするため，事務所等でスマートデバイスへ業務データを組込み，点検現場ではスマートデバイス内に組み込んでいるデータを利用する必要がある．点検業務に必要となる業務データを予めスマートデバイス内に組み込んでおく必要があるため，オンライン環境前提と比較し，スマートデバイスに保有する業務データは増える．よって，オフライン環境前提は，悪意のある第 3 者にスマートデバイスを盗まれた場合，流出する業務データが膨大となり，セキュリティリスクが高い状況となる．

3.2 端末の盗難・紛失

スマートデバイスの盗難，紛失対策として MDM によるリモートワイプやスマートデバイスの位置特定機能を利用することが多い．しかし，オフライン環境を前提とした場合，MDM の機能を期待することはできない．オフライン環境を前提としたスマートデバイスの盗難，紛失対策を検討する必要がある．

3.3 点検結果の改ざん

スマートデバイスに業務データを組み込んでおくため，悪意のある第 3 者にデータを汚れたデータに差し替えられてしまう可能性がある．オンライン環境前提であれば，データ更新の都度，スマートデバイスからサーバへの問い合わせが発生するため，サーバ側で通信頻度を測定することにより異常を検知することも可能であると考える．しかし，オフライン環境前提とした場合，悪意のある第 3 者がスマートデバイス内のデータを差し替えることでサーバ上のデータに汚れたデータを組み入れることができてしまうリスクがある．

4. 事例分析

4.1 先行事例の分析観点

スマートデバイスを利用した業務システムの先行事例について調査する．分析観点を表 4 に示す．

表 4 先行事例の分析観点

観点	目的
オフライン利用	点検業務では，オフライン環境における利用が必須と考えるため
取り扱う情報	点検業務では，図面や仕様情報など企業等にとって機密情報となるため
情報の格納方法	スマートデバイス内に情報を格納する際に暗号化等セキュリティの確保をしているかを確認するため
更新業務の有無	点検業務では，点検結果を仕様管理サーバへ登録・更新する必要があるため
端末管理	MDM の導入など端末管理の技術的な方法について整理するため
端末利用者	社内の特定された人が利用するのか，不特定の人が利用するのかを識別するため

4.2 分析結果

スマートデバイス利用目的の変化を図 7 に示す．企業においてスマートデバイスを利用する目的はコミュニケーションの促進が初期段階であり，その次の段階として，電

子カタログや電子会議といった他者への説明，プレゼンテーションツールとして利用されている. 既存の IT 資産を利用する段階では, スマートデバイスを既存の IT システムの一部として取り入れ，データ参照や入力として利用している. 点検業務によるスマートデバイスの活用は図 7 における「既存の IT 資産の活用」に相当すると考える.

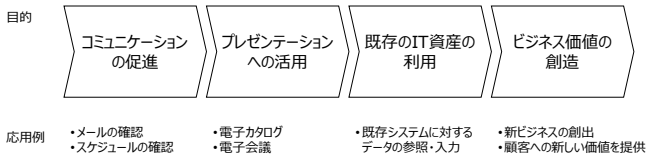

図 7 スマートデバイス利用目的の変遷

日本航空の事例では，用途として①客室乗務員向け業務・保安マニュアル, ②客室乗務員向け乗務後の業務報告, ③機内アナウンス練習，④コミュニケーションツールなどが挙げられていた．その際のセキュリティ上の特徴としては，①端末利用時にはパスコードを利用，②システム利用時にはイントラネットと共通のパスワードを要求する仕組み，③端末紛失時は，オンライン回復後，リモートワイプを実施することを対策としている．全日空の事例では，用途として①客室乗務員向け業務マニュアル，②アナウンスマニュアル・外国語学習, ③運航乗務員向けフライトマニュアル，④決裁，⑤コミュニケーションツールが挙げられていた．公開されている情報からセキュリティに関する事項は確認できなかった.

4.3 関連研究

スマートデバイスのセキュリティレベルを維持する主な技術として MDM がある．MDM はスマートデバイスを業務システムの一要素として利用するうえで必須と考えるが，多くの製品がオンライン環境を前提とした機能構成となっている．よって，点検業務で前提としているオフライン環境では，その効果を期待できない.

リモートワイプについては, 江口らの研究で, Android 環境において，完全にデータ削除が行えず，情報が復元されてしまう課題が提起されている[3]．対応策としては，ただ削除を行うだけではなく，削除したファイル領域に対し，乱数等の別データで上書きする方法が安全性の高い防止策であると結論づけている.

また，マカフィー社はモバイル端末において新たな攻撃手法，マルウェアが登場することを予測しており，より多面によるセキュリティ確保が求められている[4]．Android 環境では 2011 年から 2013 年の間にウイルスが混入した Android の不正アプリが 388%増加し，iOS 環境でもウイルス感染の被害が報告されている[5].

森田らは，オフライン利用を想定したデータの持ち出しについて手法を提案し，渉外業務を想定したシナリオで評価をしている[6]. 森田らの研究は, 提案と評価までであり，実装やシステム全体としての評価まで至っていない.

5. 点検業務への提案

5.1 提案内容

5.1.1 業務データの持ち出し

日本航空の事例では，客室乗務員向け業務・保安マニュアルを紙文書からスマートデバイスへ置き換えた．これからの変化に対し日本航空はペーパーレス化でリモートワイプが可能になった分，紙の場合に比べセキュリティレベルは上がったと評価している．紙文書による業務遂行によっても，紙を紛失するリスクはあったがリモートワイプにより遠隔操作で消し去ることを加点評価している.

点検業務においても，スマートデバイスを導入しない場合，紙資料を持参し，点検業務を行う．よって，スマートデバイス導入によりリスクが上がるわけではない. しかし，デジタルデータは紙資料とはことなり簡易な操作で多くの業務データを持ち出すことが可能である．よって，森田らの提案[6]のように事業所から現場に持ち出すデータ量を適切に制限する工夫により業務データ持ち出しに対するリスクは低減できると考える.

5.1.2 端末の盗難・紛失

日本航空では，オフラインの利用を考慮した設計となっており，端末紛失対策としてはオンライン回復後にリモートワイプを実施するという仕組みを採用している．日本航空の場合，主に客室乗務員が利用するスマートデバイスであり，航空機の離発着時，飛行時にオフライン環境に一時的になり，空港に到着すれば，オンライン回復が望める環境下であると想定する．つまり，日本航空の事例では，時間経過によりネットワーク環境が変わり，オンラインになるという期待がある．しかし，点検業務の場合，時間経過によるオンライン環境への復帰は期待できない．よって，紛失対策については，物理的に点検作業員とスマートデバイスをワイヤーなどで固定する方法や，スマートデバイスに対し，一定時間操作がなければ，警告音や光を点滅させるなどして, 紛失前に作業者へ知らせる方法が考えられる. また，業務データの保有期間を設定し，ある期間を超過した場合は業務データを削除する方法も考えられる.

盗難対策については，スマートデバイス内に組み込んでおいた仕様や設計図といった業務データを守る仕組みが必要となる．江口らの研究[3]で示されている通りリモートワイプ，ローカルワイプだけではデータを復元される課題があるため, 暗号を利用した難読化を取り入れる必要がある.

5.1.3 点検結果の改ざん

点検結果のデータが変更される可能性は，ワームなどのような悪性プログラムによるデータの改ざんと人間の意図的な操作によるデータ改ざん，または誤操作によるデータ修正がありうる．この中で，人間の誤操作によるデータ変更は悪意がないため改ざんの範囲外とする．また，人間の意図的な操作によるデータ改ざんを内部不正と考える.

本研究では, MAC(Message Authentication Code)を利用し，点検結果の改ざんへの対応を考察する．MAC はデータ D に対し，鍵 K によりタグ t を算出する関数である． MAC に利用する関数 H_k は事前にサーバ側, スマートデバイス側で共有されているものとする．更新データに対するハッシュを h_1 とし，タグの算出を下記のように定義する．

$$t_1=H_k(h_1,t_0)$$

この定義によるデータの更新フローを図 8 に示す．

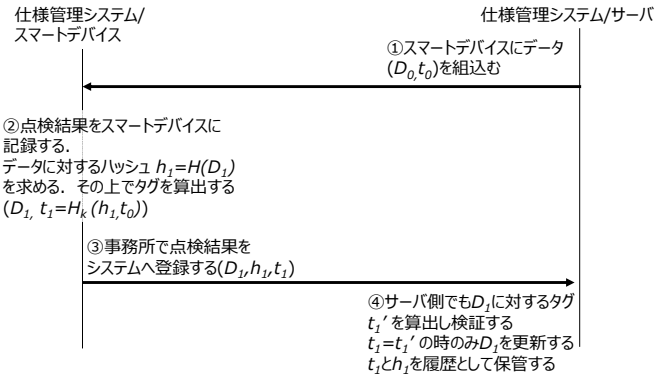

図 8 MAC を利用した更新フロー

サーバからスマートデバイスにデータを組込む際に，データ D_0 に対するタグ t_0 をスマートデバイスに組込む．点検作業員が点検結果をスマートデバイスに記録する際，スマートデバイスのアプリは更新データ D_1 に対するタグ t_1 を算出する．点検作業員が事務所等に戻り，スマートデバイスからデータを仕様管理システムサーバにアップロードした後，仕様管理システムサーバは D_1 に対するタグ t_1' を算出する．サーバは t_1 と t_1'が等しい場合，D_1 でデータを更新する．

タグを算出する際にデータのハッシュだけではなく以前のタグ情報(t_0)を利用する．この場合，悪意のある第 3 者がデータ D_x に対するタグ t_x を求めようとした場合，鍵 K 以外に以前のタグ情報(t_0 の情報)も必要となり, 容易に算出することはできない．また，サーバ側への更新が成功する t_x の値は t_0 の値によって変わるため常に一定とは限らず，データを改ざんすることは難しいと考える．

なお，タグ t については履歴を記録しておくべきと考える．直前の世代のみしか保持していなかった場合，作業のミスやプログラムのミスでタグ t が汚染されてしまった場合，再計算できないためである．タグ t が正しいものであるということを保証するためにある一定の期間は保持しておくことが望ましいと考える．

5.2 評価

業務データの持ち出しについては，記録用紙からスマートデバイスで切り替えることでリモートワイプによるデータの削除ができるなど加点評価をすることができる. また，用紙の場合，人間が解読可能な情報であるが，スマートデバイスに電子情報として記録するのであれば，暗号技術を利用することで難読化が可能である．

端末の盗難・紛失については，本研究で前提とした点検業務の場合，先行事例のように環境が変化することによりオンラインが回復することは望めない．そのため，点検作業者とスマートデバイスを物理的に固定するワイヤーロックや，一定時間操作がない場合は音や光で警告をする仕組みなどが有効だと考える．

データの改ざんについては，MAC を利用することにより，悪意のある第 3 が改ざんデータを容易に作成することはできない．また，内部不正については IPA が内部不正防止ガイドライン[8]にて基本原則として挙げている 5 項目(①犯行を難しくする，②捕まるリスクを高める，③犯行の見返りを減らす，④犯行の誘因を減らす，⑤犯罪の弁明をさせない)のうち，MAC を利用することにより，2 項目(①②)は対応可能になると判断する．

6. まとめと今後の課題

本研究では，インフラ維持管理に必要である点検業務に対しスマートデバイスを適用した際の問題点を情報セキュリティの C,I,A 観点を中心に分析し課題を示した．それらの課題に対し，先行事例の調査・分析，MAC を利用した技術的な解決策を提案し，評価を行った．

今後，解決策の一部を実験環境にて実装し，性能比較等を行う．

参考文献

[1] 内閣府: SIP(戦略的イノベーション創造プログラム)インフラ維持管理・更新・マネジメント技術研究開発計画, http://www8.cao.go.jp/cstp/gaiyo/sip/keikaku/7_infura.pdf, 2015/11/04 参照
[2] 嶋田善多, 矢吹信喜, 坂田智己:土木設備の維持管理体系における巡視点検と IC タグの活用,土木学会論文集 No. 777/VI-65, 161-173,2004
[3] 江口雅人, 岡田泰輔, 佐々木良一: Android スマートデバイスにおける情報漏洩防止策の安全性評価, 情報処理学会 Dicomo2014, pp1735-1740
[4] マカフィーLabs:McAfee 脅威レポート 2014 年 11 月－2015 年の脅威予測－, http://www.mcafee.com/jp/resources/reports/rp-quarterly-threat-q3-2014.pdf , 2015/11/04 参照
[5] Mac から iPhone／iPad をも狙う「WireLurker」、その危険性と行うべき対策は？, http://blog.trendmicro.co.jp/archives/10258, 2015/11/04 参照
[6] 森田伸義 ,礒川弘実,萱島信,梅澤克之:モバイル端末向けオフラインアプリケーション統制システムの提案, 情報処理学会第 74 回全国大会,2012
[7] 佐川浩彦,秋良直人,木村宣隆,栗原恒弥,関峰伸,竹内隆,藤本敬介: 拡張現実感による遠隔作業支援システムの開発,電子情報通信学会論文誌 D Vol.J98-D No.1 pp.258-268,2015
[8] 独立行政法人 情報処理推進機構:組織における内部不正防止ガイドライン, https://www.ipa.go.jp/security/fy24/reports/insider/, 2015/10/19 参照