Vol.2011-MBL-57 No.14
Vol.2011-UBI-29 No.14
2011/3/7

携帯端末での署名履歴交差を用いた証拠保全手法の提案と評価

三科貴[†]　白石陽[††]　高橋修[††]

携帯端末は現在，住所や電話番号，メールアドレスや通話履歴などの個人情報を多く含む重要な情報端末である．携帯端末が法人利用されることが増加している中で，安易に情報を取り扱ってしまう「無知」や，携帯端末の誤操作や紛失・盗難をされてしまう「過失」，情報の横流しなどを行うための意図的な持ち出しをする「故意」などの人的要因のインシデントを減少させるため，それらを後々に証明できる必要がある．
我々は，人的要因のインシデントを証明すること，また自身の振る舞いを証明することを目的とし，携帯端末へフォレンジックを適用した際の証拠の信頼性，CPUやメモリなどの計算資源が少ないという問題点を考慮し，携帯端末内の証拠保全手法の提案を行う．
提案する証拠保全手法では，保全データの優先順位付けとヒステリシス署名を用いて携帯端末にフォレンジックを適用した際の問題点を解決する．

Proposal and evaluation of evidence preservation method using signature history intercrossing for portable terminal

Takashi Mishina[†] Yoh Shiraishi[††] and Osamu Takahashi[††]

The portable terminal is an important information terminal that contains a lot of individual information such as addresses, telephone numbers, e-mail addresses, telephone call history, etc. As corporate use of the portable terminal increases, it will be necessary to prove the cause of computer security incidents to decrease information leaks due to human factors. These factors include "ignorance" (unwittingly losing information), "fault" (performing the wrong operation or losing / stealing the portable terminal), and "intention" (intentionally selling information illegally).
We propose a technique to preserve information in the portable terminal to prove the terminal's behavior and how information has leaked. In the proposal, we consider two problems. One is the reliability of the evidence when we applied digital forensics to the portable terminal and the other is the few calculation resources of CPU and memory, etc. Our proposal method solves these two problems by using the hysteresis signature and priority level of the evidence preservation.

1. はじめに

現在，携帯端末（本稿では PDA などの携帯情報端末，及び携帯電話やスマートフォンなどの携帯電話端末の両方を意味する）は多くの人が持ち，様々な状況で利用される重要な情報端末となっている．利用される状況は，個人利用における音声での連絡手段としてだけではなく，法人利用におけるデータ通信での情報共有，外部から社内のシステムへのアクセスなどがある．これらの状況では住所や電話番号，メールアドレスや通話履歴,操作ログやファイル情報などの多くの重要な個人情報が利用される．特に法人利用を想定した場合，個人情報が利用される際には情報セキュリティ対策を施す必要がある．これまでの情報セキュリティ対策は主に外部からの侵入や操作を防ぐという観点で捉えられてきた．しかし，現在，内部から外部へ情報が漏洩することが問題となっている．内部から外部へ情報が漏洩する情報セキュリティインシデントの 9 割以上が「人的要因」であり，バグやセキュリティホール，マルウェアといった「外的要因」は非常に少ない[1]. 人的要因の情報セキュリティインシデントは, 無知，過失，故意の 3 つに大きく分類することができる．それぞれ，安易に情報を取り扱ってしまう「無知」，携帯端末の誤操作や紛失・盗難をされてしまう「過失」，情報の横流しなどを行うための意図的な持ち出しをする「故意」である．

人的要因の情報セキュリティインシデントを減少させる方法として，人に対する直接的な教育を継続的に施す方法と，携帯端末に物理的な対策を施して人のミスをカバーする方法がある．人に対する直接的な教育を施す場合，未然に被害を防ぐことが可能だが，効果が現れるまでに時間がかかりそれに伴い人的・金銭的コストが多くかかってしまう．そのため，我々は物理的な対策の一つであるデジタルフォレンジックに着目し，携帯端末へ適用することで人的要因の情報セキュリティインシデントを減少させる方法を提案する．

デジタルフォレンジック[2]は不正侵入や情報漏洩などの情報セキュリティインシデントを証明することを目的とし，コンピュータ内のハードディスクやネットワーク内を流れる全通信を対象として証拠を収集・保全・解析する技術である．デジタルフォレンジックには「情報の取りこぼし」「性能低下，システムの停止」「検知遅れ」「調査活動が証拠破壊に繋がる」といった課題がある[3]．また，携帯端末へデジタルフォレンジックを適用させる際の課題として「通信機能の充実による不正操作」「データ記憶の仕組みの違い」「証拠の信頼性」といった課題がある[2]．携帯端末にフォレンジックを適用する場合にこれらの課題を考慮すると，日常的な使用をしつつも証

† 公立はこだて未来大学大学院
Graduate School of Future University Hakodate
†† 公立はこだて未来大学
Future University Hakodate

Vol.2011-MBL-57 No.14
Vol.2011-UBI-29 No.14
2011/3/7

拠を収集し，保全できる必要がある．それと同時に携帯端末内の証拠を収集・保全した場合の証拠の信頼性を確保する必要がある．しかし，携帯端末は計算資源が限られており，常に全ての情報を取得し続けることが難しく，また端末のみでの証拠の信頼性確保は難しい．

そこで本稿では携帯端末を用いた人的要因の情報セキュリティインシデントを減少すること，また自身の振る舞いを証明することを目的とし，携帯端末へデジタルフォレンジックを適用した際の CPU やメモリなどの計算資源が限られているという制約と，証拠の信頼性確保が難しいという問題点を考慮した携帯端末内の証拠保全手法の提案を行う．

2. 関連研究

本章では既存の携帯端末を対象としたフォレンジックツール，携帯端末を用いたデジタルフォレンジックの実現手法，及び証拠の信頼性を確保するための署名技術であるヒステリシス署名と署名履歴交差について示す．

2.1 モバイルフォレンジック

2.1.1 Device Seizure

Device Seizure[4]は RIM BlackBerry や Palm，Symbian や Microsoft Windows Mobile などの携帯端末を対象としたフォレンジックツールである．その特徴として，携帯端末の全てのファイルをオリジナルデータのままで保存できること，データの収集から解析までを Device Seizure のみで行えることが挙げられる．データは論理コピーや物理コピーで保存でき，Bluetooth や IrDA，Cable で接続してデータを保存する．データ保存する際には常にデータ保存を行う機器との接続が必要である．

2.1.2 SIMIS

SIMIS[5]は SIM カードを対象としたフォレンジックツールである．その特徴として，SIM カードのデータの取得と分析に対応していること，制御カード，データ保存カード，分析アプリケーション，カードリーダーから構成されていること，それぞれのプロセスが独立して動作していることが挙げられる．データは SIM カードの物理コピーを保存できる．データ保存には専用の機器との接続が必要である．

2.1.3 SIMIS

國井ら[6]は小規模なコンピュータ環境において，デジタルフォレンジックを実現しつつファイルを管理するシステムを提案している．このシステムでは携帯端末を署名生成デバイスとして使用しているが，携帯端末内の情報収集・保全は行わないため，携帯端末の情報セキュリティインシデントを証明することが難しい．

2.2 ヒステリシス署名

2.2.1 概要

ヒステリシス署名[7]は，電子文書の長期運用の際に問題となる署名生成鍵の漏洩や推定による被害を最小限にするための対策技術の一つである．

この技術では，電子文書を登録する際に署名情報を履歴に残す．電子文書に署名をする際には履歴に残された署名情報を取り込んで新たな署名を生成する．そのため，電子文書間に時系列的な連鎖構造が生まれる．具体的には，署名対象となる電子文書と，直前の署名記録のハッシュ値を結合し，自己の秘密鍵を用いて従来の署名生成処理を行ってヒステリシス署名付きメッセージを生成する．また同時に署名情報を履歴に残す(図 1).

ヒステリシス署名の検査をする場合，ヒステリシス署名付きメッセージに対して公開鍵による通常の署名検証を行う．また，検査の際に署名生成履歴の整合性検証として，ヒステリシス署名付きメッセージに過去の署名に関する情報があるかどうかを確認し，署名記録の連鎖性を確認できる．そのため，不正者がある文書や署名を偽造するためには，文書自体の偽造や電子文書作成者の秘密鍵を用いて署名を偽造するだけでなく，過去の署名生成履歴を反映した電子文書間の時系列的な連鎖構造を反映させて偽造しなければならない．以上のことから，ヒステリシス署名を利用することで署名の偽造は困難であると考えられる．

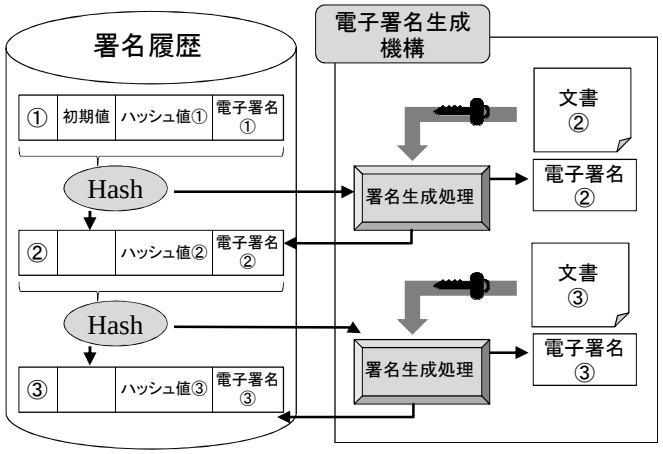

図 1　ヒステリシス署名の処理

2.2.2 署名履歴交差

署名履歴交差とは，署名生成履歴の証明力を向上させる手段であり，各利用者の署名履歴を交差させることで署名の改ざんをより困難にすることができる．署名履歴交

Vol.2011-MBL-57 No.14
Vol.2011-UBI-29 No.14
2011/3/7

差により，不正者が署名を偽造する際に，署名履歴の中に他の利用者と履歴交差を行った部分があれば，交差相手の署名履歴をも偽造する必要があり，署名の偽造がよりいっそう困難になる(図 2).

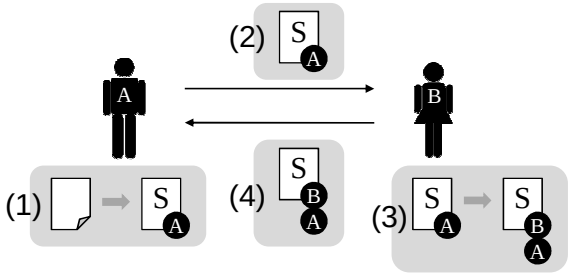

図 2　署名履歴交差

3. 提案する証拠保全手法

3.1 要求条件

コンピュータを対象としたデジタルフォレンジックでは通常，何か問題を確認した後に，電源を切ることで消えてしまうデータを収集するかを判断し，その後電源を切りシステム上のデータが変化しない状態にしてデータの収集を行う．このようにデジタルフォレンジックを適用させるのは，電源を切ることで消えてしまうデータは重要であるが，収集活動がファイルやシステム上のデータに変更を加えてしまう可能性があるためである．

しかし，携帯端末に対してデジタルフォレンジックを適用する際に前述した方法と同じ方法を適用するには様々な問題がある．越智ら[3]が挙げたデジタルフォレンジックの課題，辻井ら[2]が挙げた携帯端末へデジタルフォレンジックを適用する際の課題を参考に，本稿で必要となる携帯端末にデジタルフォレンジックを適用する際に必要となる要求条件を定める．以下に示す携帯端末内の証拠収集・保全の問題を防ぐことを本稿での要求条件とする．

(1) 証拠の取りこぼしが起き，情報漏洩の痕跡が取得できない

携帯端末は，データ記憶媒体にフラッシュメモリを使用しており，ハードウェアリセットにより全ての情報を消去することが容易である．そのため，証拠の消去をされてしまい適切な情報漏洩の痕跡が取得できない可能性がある．また携帯端末は基本的に持ち歩いて利用するため，専用の機器が必要な場合にはその場で証拠を取得することが難しく，証拠を取りこぼす可能性がある．

(2) データ収集や証拠保全が携帯端末の性能を低下させ，システムを停止してしまう

データ収集時に,外部から機器を接続する方法ではシステムを停止する必要があり，また持ち歩いて使用する携帯端末には不向きである．物理コピーの取得を頻繁に行う方法では，携帯端末の計算資源を多く必要とするため，システムの性能低下やシステム停止により緊急時の連絡が不可能となってしまう．

(3) 携帯端末のみで証拠収集・保全を行った際，証拠の信頼性が確保されていない

収集・保全を行った際に自身だけで電子署名を行った場合，秘密鍵が漏洩することで電子署名の偽造が可能となり，また署名の時間的順序性も保てない．

また，携帯端末は通信機能が充実しているため，収集活動が証拠に与える影響以上に，悪意ある操作により証拠が改ざんされる可能性がある．

これらの要求条件を解決するため，携帯端末内の情報を優先順位によって収集頻度を変更することにより全ての証拠を収集しながら携帯端末への負担を軽減し，署名履歴交差の利用により証拠の信頼性を確保する方式を提案する．

3.2 前提条件

提案する証拠保全手法は証拠の収集を行う携帯端末，及び証拠の保全と信頼性確保を行うサーバで構成される．サーバは認証局のような十分に信頼でき，サーバ内へのアクセスは厳格に制限されているものとする．サーバの例は以下の通りである．

(1) 認証局

認証局と他の当事者にデジタル公開鍵証明書を発行する機関である．公開鍵証明書には公開鍵とその持ち主の記載があり，個人，組織，サーバその他がその公開鍵に対応した秘密鍵の持ち主だと証言する．認証局は運用実績や知名度などのデジタル公開鍵証明書以外の方法で信頼性が示されることや，アクセスが厳格に制限されていることから信頼できる第三者と言える．

(2) ISP

ISP とは Internet Service Provider 略であり，インターネットに接続する際のユーザ毎の ID やパスワードの管理，アクセス制限などを行っている．日本では電気通信事業者の一つとして位置づけされており，国から認可されて業務を行っているため信頼性が高いと言える．

提案する証拠保全手法ではこれらのサーバを利用できるものとする．また提案する証拠保全手法を利用する際には無線ネットワーク（IEEE 802.11g 以上の速度が出るもの）に常に接続しているものとする．

3.3 情報の優先順位と収集頻度

3.3.1 情報の優先順位

PC や携帯端末のデータは，揮発性の状態と不揮発性の状態の両方で存在する．揮発性データとは，稼働中のシステム上に存在し，コンピュータの電源を切ると消失するデータ（システムの現在のネットワーク接続など）を指す．不揮発性データとは，コ

Vol.2011-MBL-57 No.14
Vol.2011-UBI-29 No.14
2011/3/7

ンピュータの電源を切ったあとも存続するデータ（ハードディスクドライブに格納されたファイルシステムなど）を指す．一般的に推奨されるデータ収集時の優先順位[8][9]を参考にした，携帯端末の揮発性データ，不揮発性データの一覧及びその優先順位を表 1 に示す．

表 1　揮発性データ及び不揮発性データの優先順位

		揮発性データ	不揮発性データ
優先順位	1	ネットワーク接続	通話履歴
	2	ログインセッション	SMS / MMS 履歴
	3	実行中のプロセス	電話帳
	4	開かれているファイル	カレンダー情報
	5	ネットワーク構成	設定ファイル
	6	OS 時間	ログファイル
	7	メモリの内容	データファイル
	8		アプリケーションファイル

この優先順位に決定した理由として，携帯端末に与える負荷が挙げられる．揮発性データの中で「メモリの内容」が最も優先順位が低い理由は，メモリの物理コピーを取得する必要があるためである．物理コピーを取得する作業は，元の媒体の空き領域などを含むコピーを生成できるが，論理ボリュームのディレクトリやファイルをコピーする論理コピーよりも多くの実行時間，端末への負荷を必要とする．

また不揮発性データの優先順位について，携帯端末独自の情報は携帯端末を利用した際の人的要因のインシデントを証明する場合に重要であると考えた．またデータファイル，アプリケーションファイルの保全には物理コピーの取得を必要とするため，優先順位が低い．

3.3.2　優先順位による収集頻度の変更

3.3.1 節で示した優先順位を用いて，3 段階の証拠の収集・保全を行う．表 2 に収集頻度と収集する証拠の範囲を示す．

表 2　収集頻度と収集範囲

収集頻度	収集範囲
高	揮発性データ：優先順位 1~6
中	揮発性データ：優先順位 7 不揮発性データ：優先順位 1~6
低	不揮発性データ：優先順位 7~8

収集頻度（高）の場合，揮発性データ優先順位 1~6 の情報に対して論理コピーを行う．収集頻度（中）の場合，メモリの物理コピーを取得し，不揮発性データ 1~6 の論理コピーを取得する．収集頻度（低）の場合，データファイルとアプリケーションファイル全体を保全するため，ROM の物理コピーを取得する．

情報の優先順位により収集頻度と収集範囲を変更することで，端末へ与える負荷を押さえてシステムの性能低下やシステム停止を防ぐことが可能となる．また，収集頻度に差はあるが全ての情報を収集するため，証拠の取りこぼしを防ぐことができる．

3.4　証拠保全手法

3.4.1　全体の流れ

提案する証拠保全手法の全体の流れを図 3 に示す．

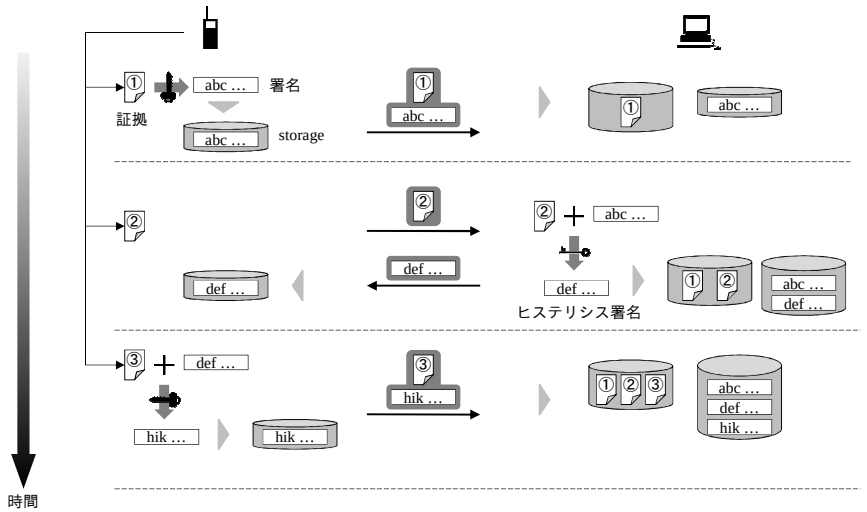

図 3　提案手法の流れ

3.4.2　携帯端末側の動作

携帯端末側では，

(1)　証拠の定期的な取得

(2)　ヒステリシス署名の生成，証拠と署名履歴の送信

を行う．

(1)証拠の定期的な取得では，3.3.2 節で示した証拠の収集頻度と収集範囲を利用して

Vol.2011-MBL-57 No.14
Vol.2011-UBI-29 No.14
2011/3/7

それぞれの証拠を定期的に取得する．証拠を収集するプログラムは，システムへの影響を最小限にとどめるため，耐タンパ性を持つ SD メモリカードなどのシステムとは別の保存領域から実行する．また，収集した証拠の完全性を証明するため，元のデータとのハッシュ値の比較を行う．収集した証拠は SD メモリカード内に保存する．

次に，取得した証拠と署名履歴を利用して，ヒステリシス署名の生成を行う．その後，サーバに対して証拠とヒステリシス署名を送信する．サーバに証拠とヒステリシス署名を送信した後，証拠の削除を行い，ヒステリシス署名を署名履歴として保存する．証拠を削除することにより，SD メモリカードの保存領域を確保し，情報漏洩を防止する．署名履歴は SD メモリカード内に保存する．サーバからヒステリシス署名を受信した場合，同様に署名履歴として保存する．ヒステリシス署名の生成，および署名履歴の保存は，収集頻度によって変化する収集範囲毎に別々の処理として行う．

(2)証拠と署名履歴の送信について，携帯端末で証拠と署名の暗号化を行った後，奇数回は証拠と署名履歴を送信する．偶数回では証拠のみを送信する．ヒステリシス署名の生成，および署名履歴の保存は，収集頻度によって変化する収集範囲毎に別々の処理として行う．

証拠とヒステリシス署名の送信について，奇数回は証拠とヒステリシス署名を送信する．偶数回では証拠のみを送信する．この動作により，携帯端末のみで証拠を収集し，信頼できるサーバとの署名履歴交差を行う．本来署名履歴交差は二者がそれぞれの持っているデータに対して署名を交差させる．しかし本提案手法では携帯端末のみがデータを収集するため，証拠と署名履歴の両方を送る場合と証拠のみを送る場合を交互に繰り返すことで署名履歴交差を実現する（図 4）．

3.4.3 サーバ側の動作

サーバ側では，

(1) 携帯端末から送られてくる証拠と署名履歴の受信
(2) ヒステリシス署名の生成と送信

を行う．

サーバ側では，携帯端末から送られてくる証拠と署名履歴を全て保存する．携帯端末側と同様に，ヒステリシス署名の生成，および証拠と署名履歴の保存は，収集頻度によって変化する収集範囲毎に別々の処理として行う．

(2)ヒステリシス署名の生成と送信について，奇数回は処理を行わない．偶数回では署名の生成と送信を行う．サーバ側でのみ証拠の保存を行うことにより，携帯端末の証拠を第三者による改ざんを防ぐことができる．また携帯端末のデータ保存領域はサーバ側と比べて非常に小さいため，多くの証拠を保存することができないという問題を解決することができる．

携帯端末とサーバで通信を行った結果，携帯端末は署名履歴交差実現のための最新の署名だけを保持し，保全データ自体は保持しない．サーバ側では全ての署名と全ての保全データを保持する．

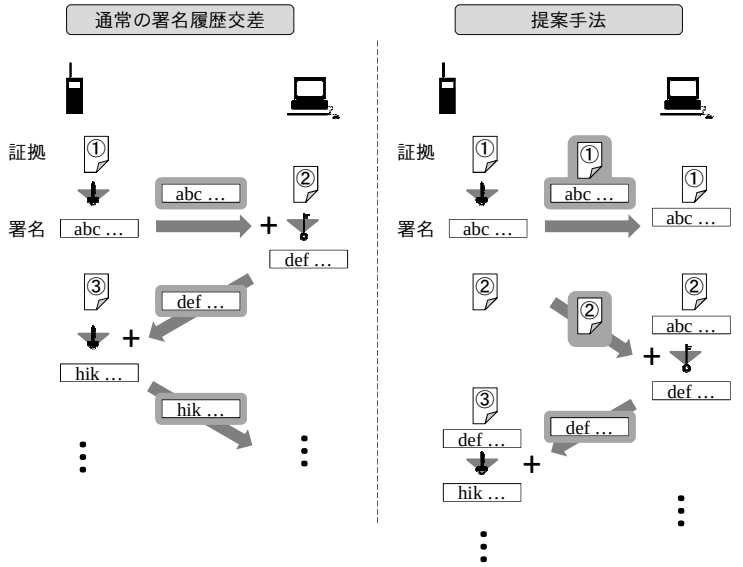

図 4 携帯端末の動作

4. 実験と評価

提案手法の有用性を確認するため，関連研究との定性的な比較を行い評価した．また実際に提案手法が携帯端末に与える負荷を調査するため，携帯端末に提案手法をアプリケーションとして実装し，定量的な評価を行った．

4.1 定性評価

定性評価の指標は以下の 4 点である．

(1) 証拠の取りこぼし
(2) 性能低下
(3) 証拠の信頼性
(4) 利便性

(1)から(3)までは 3.2 節で挙げた要求条件を満たしているかどうか，(4)は提案手法を利用する上での利便性を確保できるかを指標とした．定性評価の結果を表 3 に示す．

Vol.2011-MBL-57 No.14
Vol.2011-UBI-29 No.14
2011/3/7

表 3　定性評価の結果 (○:good, △: poor, ×: no good)

	Device Seizure	SIMIS	**提案手法**
証拠の取りこぼし	○	○	**△**
性能低下	×	×	**○**
証拠の信頼性	○	○	**○**
利便性	○	△	**○**

(1) 証拠の取りこぼし

Device Seizure や SIMIS では，ROM と RAM のデータを物理コピーとして収集・保全する．そのため収集・保全を定期的に行うことが可能であれば情報の取りこぼしは限りなく少なくすることが可能である．提案手法では，ROM や RAM の物理コピーを取得するが，頻繁に取得する内容は主に揮発性データの論理コピーなので，不揮発性データの取りこぼしが発生する可能性がある．

(2) システムの性能低下

Device Seizure や SIMIS では携帯端末のシステムを停止する必要があり，専用の機器も必要とするため携帯端末に緊急時の連絡などがあった場合に対処できない．提案手法では情報の優先順位を利用して収集頻度と収集範囲を変更する．そのためシステムへの負担が少なく，またシステムを停止することがない．

(3) 証拠の信頼性

Device Seizure や SIMIS では信頼できる PC と接続して証拠の収集・保全を行った場合，その証拠の信頼性は十分に確保されている．提案手法では収集・保全した証拠は一度携帯端末に保存するが，信頼できるサーバとの間で署名履歴交差を行い，証拠の長期保存はサーバが行うため，証拠の信頼性は十分に確保されている．

(4) 利便性

Device Seizure は様々な種類の証拠収集方法, 解析方法などが用意されており利便性が高い．SIMIS は SIM カードの情報のみを取得可能であり，専用の機器との接続方法の面からも Device Seizure と比較して利便性が低い．提案手法では設定によって様々な証拠の種類を収集し，専用の機器は不必要なため利便性は高い．

以上の定性評価の結果，提案手法は「証拠の取りこぼし」では関連研究に劣るものの，携帯端末では最も重要である「システムの性能低下」を減少させ,「証拠の信頼性」や「利便性」が高いことがわかった．

4.2 定量評価

定量評価の指標は以下の 3 点である．

(1)　CPU 使用率

(2)　メモリ消費量

(3)　実行時間

CPU 使用率とメモリ消費量は提案手法を利用する際の携帯端末に与える負荷である．実行時間は提案手法により証拠を収集し署名を施して保全が終わるまでの時間である．定量評価の実験環境を表 4 に示す．

表 3　実験環境

OS	Android 1.6
携帯端末の性能	HT-03A [10] CPU : 528MHz　Storage : 512 MB　RAM : 192MB
ネットワーク	IEEE 802.11g
共通鍵	AES 128bit key
公開鍵	DSA 1024 bit key
実験対象	高頻度取得データ 低頻度取得データ

定量評価の測定方法は以下の通りである．

(1) 端末から証拠の収集・署名・送信いずれか 1 つのプロセスを動作させる

(2) 動作中の負荷を vmstat(端末情報を表示するコマンド)を用いて測定

(3) 測定を 5 回行い，平均値を算出

実験では提案方式のアプリケーション以外を終了し，システムの CPU 負荷が 0-3% 程の定常状態で実験を行うことを前提条件とする．表 4 に高頻度取得データの実験結果を示す．

表 4　高頻度取得データの結果

	CPU 使用率 (%)	**メモリ消費量 (MB)**	**実行時間 (s)**
収集	16.7	0.09	2.8
署名	98	0	0.03
送信	71.4	0.96	9.3
平均	58.83	0.76	(合計時間) 12.13

提案手法を利用した場合，証拠の収集部分の CPU 負荷は低く処理時間も短い．署名部分の CPU 負荷が最も高く，処理時間が最も短い．証拠の暗号化と送信部分は CPU 負荷が高く処理時間が最も長いため，継続的に端末に対して負荷がかかる．

署名と暗号化の処理時間の違いについて，これは処理対象のデータ量の違いが原因だと考えられる．署名では元のデータのハッシュ値に対して処理をする．暗号化では

Vol.2011-MBL-57 No.14
Vol.2011-UBI-29 No.14
2011/3/7

元のデータ自体に処理をするため処理時間が長くなった．また収集，署名，送信のどの処理でもメモリ負荷は低いことが確認できた．

表 5 に低頻度取得データの実験結果を示す．

表 5　低頻度取得データの結果

	CPU 使用率 (%)	メモリ消費量 (MB)	実行時間 (s)
収集	55.57	1.13	70.2
署名	97.6	0	17.45
送信	63.15	0.11	2217.24
平均	63.19	0.14	(合計時間) 2304.89

提案手法を利用した場合,高頻度取得データの実験結果とほぼ同じ傾向が見られた．しかし低頻度取得データの送信プロセス時の実行時間が高頻度取得データと比較して非常に長いことがわかった．これはデータ量が非常に多く，暗号化やデータ送信に時間がかかるためである．メモリ消費量には両方の場合で大差がなかった．また CPU 使用率に関して，低頻度取得データの結果が 5%ほど高いことがわかった．これは提案手法の収集・署名・送信の 3 つのプロセスの中で最も CPU 負荷が高い送信プロセスの実行時間が長いため，結果としてその平均 CPU 使用率が上がったと考えられる．

4.1 実験と評価のまとめ

定性評価の結果，提案手法では 3.1 節で挙げた要求条件を全て満たしていることがわかった．定量評価の結果，高頻度で取得するデータが与える負荷は低く，低頻度で取得するデータが与える負荷は高かった．定量評価の結果から，証拠の収集頻度をユーザの携帯端末使用時間帯や利用状況によって変動させることで，利便性を下げることなく証拠を収集できる．

5. 考察

5.1 対処できる情報セキュリティインシデント

一般的に，情報セキュリティインシデントは，電子メールの誤送信などによる誤操作が最も多い．次に多いのは誤って重要な情報を他の情報と一緒に廃棄してしまう管理ミスである．また情報な情報が含まれる媒体の紛失・置き忘れ，盗難，不正な情報持ち出し，設定ミスなどが原因となっている[1]．提案手法によって，携帯端末を利用したこれらの人的要因によるインシデントを証明することが可能となる．

(1)　無知

無知には「管理ミス」「設定ミス」が含まれる．

重要な情報を誤って廃棄してしまった場合，実行中のプロセスや OS 時間，またデータファイルなどからいつ，どのようにしてどんなデータが廃棄されてしまったのかを証明することができる．

アプリケーションの設定ミスなどにより情報漏洩が発生した場合，設定ファイルやアプリケーションファイルにより，何をどのように設定したことが原因なのかを証明することができる．

(2)　過失

過失には「誤操作」「紛失・置き忘れ」「盗難」が含まれる．

携帯端末の誤操作により誤って電子メールを送信してしまった場合，ネットワーク構成やネットワーク接続，またログファイルなどからどのネットワークでいつ誰に対してメールが送信されてしまったのかを証明することができる．

携帯端末を紛失・置き忘れしてしまった場合や盗難されてしまった場合，ログインセッションや実行中のプロセス，開かれているファイルなどを利用して，携帯端末を操作していなかったことを証明することができる．この際，自身が携帯端末をある期間所持していなかったことを証明することが求められる．

(3)　故意

故意には「不正な情報持ち出し」が含まれる．

重要な個人情報である住所や電話番号などを携帯端末に入力したまま不正に持ち出した場合，データファイルやメモリの内容などからどのような情報を持ち出したのかを証明することができる．

これらの代表的な情報漏洩のインシデントでは収集頻度の高い揮発性データが多く求められる．上記以外のインシデントが発生した場合でも，提案する証拠保全手法では多くの揮発性データ，不揮発性データを収集しているため対処できると考えられる．インシデントを証明する際，情報の定期的な取得と署名履歴交差により時間的順序性を保った証明が可能である．

5.2 データ圧縮による処理負荷軽減

提案する証拠保全手法におけるそれぞれにプロセスでは「送信」に一番時間がかかり，CPU 負荷も高い．そのため，携帯端末からサーバへデータを送信する際に保全データにデータ圧縮を施すことによって「送信」プロセスの負荷を減少できるのではないかと考えた．データ圧縮は次の 2 つに大きく分けることが出来る[11].

・可逆圧縮：圧縮に伴って情報が欠落しないが圧縮率は低い
・非可逆圧縮：圧縮に伴って情報が欠落するが圧縮率が高い

原稿やプログラムなどの重要なデータは圧縮に伴って情報が欠落すると問題が発生するため可逆圧縮が利用される．本稿では自身の行動を証明するためのデータを圧縮対象とするため，情報が欠落しない可逆圧縮を考察対象とする．

Vol.2011-MBL-57 No.14
Vol.2011-UBI-29 No.14
2011/3/7

代表的な可逆圧縮法を利用した様々な圧縮ソフトが開発されている．その中から指標として代表的な，端末の CPU 使用率，圧縮に要する時間，圧縮率（圧縮後のファイルサイズ / 圧縮前のファイルサイズ）を計測しデータ圧縮による携帯端末への処理負荷軽減の可能性を追加実験する．追加実験の環境を表 6 に示す．

表 6　追加実験の環境

OS	Ubuntu 10.04
CPU	AMD Athlon 64 X2 6000+ 3.00 GHz
Memory	1024MB
圧縮対象のファイルサイズ	112MB
圧縮ソフト	・gzip - 1.3.12 (default, fast) ・bzip2 - 1.0.5 (default, fast) ・lzma - 4.43 (default, fast)

実験をする際には他の負荷がないことを確認し，3 回の試行の平均を求めた．またそれぞれの圧縮ソフトで標準の状態と高速処理オプションを利用した場合の 2 パターンでの実験を行った．追加実験結果を表 7 に示す．

表 7　追加実験の結果

	CPU 使用率 (%)	圧縮時間 (s)	圧縮率 (%)
gzip default	76.58	10.67	58.30
gzip fast	71.38	6.66	60.02
bzip2 default	95.95	41.66	58.57
bzip2 fast	87.94	34.67	58.39
lzma default	96.49	92.0	49.01
lzma fast	93.28	22.33	53.03

端末に与える負荷は lzma が最も高く，gzip が最も低かった．処理時間は gzip の fast オプションを利用した場合が最も短く，lzma の標準状態が最も長かった．圧縮率は lzma の標準状態が最も高く，gzip の fast オプションを利用した場合が最も低かった．

今回の追加実験環境と実際の携帯端末の性能は大きく異なっているものの，携帯端末でこれらの圧縮ソフトが利用できる場合，gzip の fast オプションを利用することで短時間に元のデータを 60%程に圧縮できることがわかった．データサイズと処理時間が比例するならば「送信」プロセスにかかる時間を 60%超に短縮できるため，圧縮は「送信」プロセスの負荷を減少できるために有効であると考えられる．

6. おわりに

本稿では，携帯端末においてデジタルフォレンジックを適用させる際，情報の優先順位を利用して収集頻度と収集範囲を変更する証拠の保全手法の提案を行った．

PC や携帯端末のデータで重要とされる揮発性データを頻度を高く収集することで，携帯端末への負担を少なく多くの情報セキュリティインシデントに対応できる．

提案手法の評価として定性評価及び定量評価を行った．定性評価では，関連研究との比較を行い提案手法の有用性を確認できた．定量評価では提案手法をアプリケーションとして実装し，携帯端末に与える負荷を計測した．その結果，適切な収集間隔やプロセス毎の時間帯変更を取り入れることで携帯端末への負荷を低減できることが確認できた．

今後の課題として携帯端末への負荷低減が挙げられる．本稿ではデータ圧縮により負荷を低減させる手法を考察したが，証拠収集や署名，送信にかかるそれ自体の負荷をより低減させることで提案手法の利便性を向上させることができる．またネットワーク非接続時の動作を検討する必要がある．携帯端末を利用する際に電波が存在しない状況で，ネットワークに再接続された場合の処理の検討する必要がある．

参考文献

1) Hisamichi Ohtani (Working Group Leader): Information Security Incident Survey Report, NPO Japan Network Security Association Security Incident Investigation Working Group (2008).
2) Shigeo Tsujii (editorial supervisor): Digital forensics dictionary, Digital forensics society (2006).
3) Takao Ochi, Takao Kojima, Masao Togawa, Yukio Itakura: The Proposal of Incident detection Method using the Hot Digital Forensic, Proc. IPSJ SIG Notes 2008, pp.267–272, Information Processing Society of Japan (2008).
4) Paraben Corporation – Device Seizure http://www.paraben.com/device-seizure.html
5) 3g Forensics smart forensic solutions – SIMIS http://www.crownhillmobile.com/simis.htm.
6) Svein Willassen: Forensic Analysis of Mobile Phone Internal Memory, Proc. International Federation for Information Processing (IFIP), Vol.104, pp.191–204 (2005)..
7) Seiichi Susaki, Tsutomu Matsumoto: Alibi Establishment for Electronic Signatures, Proc. IPSJ Journal, Vol.43, No.8, pp.2381–2394 (2002).
8) Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang: Guide to Integrating Forensic Techniques into Incident Response, Proc. NIST Special Publication 800–886 (2006).
9) D. Brezinski, T. Killalea: Guidelines for Evidence Collection and Archiving, RFC3227 (Best Current Practice) (2002)
10) htc ‐ HT-03A，http://www.htc.com/jp/product/ht03a/overview.html
11) 奥村晴彦，山崎敏：LHA と ZIP，ソフトバンクパブリッシング株式会社(2003).