情報処理学会論文誌 Vol.56 No.9 1889–1899 (Sep. 2015)

デジタル・フォレンジックのための ガイドライン総合支援システムの提案と開発

天野 貴通[1] 上原 哲太郎[2] 佐々木 良一[1,a)]

受付日 2014年11月28日, 採録日 2015年6月5日

概要：コンピュータの電磁的記録に関する紛争の増加にともない，デジタルデータの保全・調査・分析を行うデジタル・フォレンジックの需要がある．セキュリティインシデントが発生した場合，デジタル・フォレンジックの観点からインシデントの関連機器を適切に証拠保全する必要がある．特定非営利活動法人デジタル・フォレンジック研究会は証拠保全作業の手順を解説した証拠保全ガイドラインを発行しているが，緊急時に紙のガイドラインを参照しながら正確に作業を行うことは容易ではない．そこで著者らは証拠保全ガイドラインをベースに Android 端末と PC を使用して，インシデント発生現場で初動対応者の証拠保全作業を支援するシステムを開発した．作業終了後は作業の実施記録をレポートに出力することで，関係者間で証拠の情報を共有することができる．本稿ではガイドライン作成・実行・レポート出力を行う各アプリケーションの概要を説明し，その機能と疑似シナリオに適用した評価結果を報告する．

キーワード：フォレンジック，ガイドライン，支援システム，インシデント，セキュリティ

Proposal and Development of Guideline Total Support System for Digital Forensics

Takamichi Amano[1] Tetsutaro Uehara[2] Ryoichi Sasaki[1,a)]

Received: November 28, 2014, Accepted: June 5, 2015

Abstract: The recent rise in disputes relating to electromagnetic computer records has prompted the demand for digital forensic tools that can be used to preserve, investigate, and analyze digital evidence. Among a series of digital forensic work, “Guidelines for Preservation of Evidence” which showed the procedure for work of preserving evidence was established by “The Institute of Digital Forensics”, a non-profit organization. However, in the field of digital evidence preservation, speed and accuracy are fundamental requirements. Under such circumstances, working with guidelines in paper media form is difficult for first responders. Therefore, we have developed application programs that support evidence preservation work based on the Guidelines for Preservation of Evidence on the Android operating system and PC. The system consists of three components: a creation part of guideline, an execution part, and a report output part. In this paper, the authors report the developed applications and the evaluation results applying a small trial scenario based on an actual incident.

Keywords: forensic, guideline, support system, incident, security

1. はじめに

情報社会の進展によりコンピュータの電磁的記録に関する紛争の発生件数が年々増加している．警視庁が平成 25 年に発表した警察白書によると，サイバー犯罪の検挙件数は平成 24 年には 7,334 件となり 14 年の 1,606 件から約 4.6 倍に増加している [1]．サイバー犯罪の増加にともなって，インシデント発生時にそれぞれの立場における行動の正当性を主張するために，「デジタル・フォレンジック」の需要がある [2]．デジタル・フォレンジックはデジタルデータの

[1] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[2] 立命館大学
Ritsumeikan University, Kusano, Shiga 525–8577, Japan
[a)] sasaki@im.dendai.ac.jp

証拠保全・調査・分析を行う体系を指すが，利害関係者において最も重要な作業は証拠保全作業である．証拠保全作業では対象機器の物理および論理的な状態を法的に有効な証拠となりうる方式で確保することが求められるが，デジタル・フォレンジックの歴史が浅い日本においてその標準的な指標はこれまで存在していなかった．

そのような中，証拠保全作業の標準化を目的に「証拠保全ガイドライン」が特定非営利活動法人「デジタル・フォレンジック研究会」（以下，IDF と呼ぶ）により作成された [3]．証拠保全ガイドラインは IDF の Web サイトで配布されており自由に活用できる．しかし証拠保全のための初期対応者の作業は即時性と正確性が求められる作業であり，間違った操作を行うと証拠を消してしまう危険性がある．したがって，紙のガイドラインを参照しながら作業を行うことは容易ではない．またインシデントへの対応内容はフェーズや機器の状態によって様々であるため，状況に応じた適切な作業の実施が求められる．さらに証拠保全後は実施した作業や証拠の状態を関係者間で共有するために，作業レポートを作成する必要がある．

これらを実現するためには，コンピュータによる支援システムが不可欠であり，その開発目的は次の 2 点に整理することができる．

（目的 1）デジタル・フォレンジックの専門知識のある技術者は限られ現場にいるとは限らないので，できるだけ多くの人が証拠保全のための初期対応ができるようにする．

（目的 2）現場の技術者は，他にもいろいろな仕事を持っているので，証拠保全のための初期対応に要する作業工数を可能な限り低減できるようにする．

これらの目的を達成するために，著者らは Android 端末と PC を用いて証拠保全作業を総合的にサポートする「ガイドライン総合支援システム」（Guideline Total Support System: GSS）の開発を行ってきた [4]．システムが現場の作業を支援することで迅速に証拠保全でき，証拠に関するドキュメント作成の負担が軽減される．本稿では GSS の概要とインシデントの疑似シナリオに適用した評価を述べる．

類似研究としてデジタル・フォレンジック以外の看護手順の分野ではあるが，医療ガイドラインをベースに医療行為や達成方式のプロセスをモデル化し，看護師の学習支援を目的としたスマートデバイス向けアプリケーションの開発が行われている [5]．またガイドラインのシステム化については，医療分野において診療ガイドラインからフローチャートを生成する GLIF（GuideLine Interchange Format）[6] の開発が行われている．しかし，こちらは医療機関どうしの意思決定支援を目的としており，専門家以外を対象に作業手順のガイドを行いレポートの出力を行う GSS とは利用目的が異なる．さらに GSS においては，Android アプリケーションで作業の属性に応じたユーザインタフェースを提供するためにも，独自ツールでガイドラインを記述する必要があった．

デジタル・フォレンジックの分野においては多くの論文があるが（たとえば文献 [7], [8], [9]），ガイドラインの実行をサポートするシステムについては著者らが調査した範囲においては存在していなかった．

2. セキュリティインシデントへの対応状況

2014 年 1 月に情報処理推進機構が発行した「2013 年度情報セキュリティ事象被害状況調査—報告書—」によると，一般企業の情報セキュリティに関するインシデントへの対応体制についての調査において，25.4%の企業が「コンピュータセキュリティインシデントに対応する部門や人が定まっていない」と回答している．また情報セキュリティ業務担当者のスキル面での充足度について，全体の 52.9%の企業が「やや不足している」と回答している [10]．

教育機関においては，普通科高校の教員への意識調査で「情報漏洩等の可能性がある事故に遭遇した場合の連絡体制や対処を理解しているか」との問いに対して，72.3%が「いいえ」と回答している [11]．また昨今大学の研究室において独自にサーバを導入しネットワークの運営と管理を行う団体が増えてきている．研究室に所属する人間の属性は指導教員の研究領域に依存することが多いと考えられるため，ネットワークやフォレンジックの知識が不足している研究室でもセキュリティインシデントが発生することも考えられる．このことから，幅広い分野の組織でインシデントレスポンスに対する需要があることが考えられる．

3. 証拠保全ガイドラインとドキュメント作成

3.1 証拠保全ガイドライン

証拠保全ガイドラインは IDF が作成した電磁的証拠保全手続きの標準的なガイドラインであり，現場で最初に証拠保全にあたる「ファーストレスポンダ」が対象である．デジタル・フォレンジックの運用者にとって最も重要なことは，インシデントに関わるデジタル機器に残されたデータの中から電磁的証拠となりうるものを，確実に，そのまま（As-is）で，収集（Collection）・取得（Acquisition）し，保全（Preservation）することであるとされる．この手続きに不備があると，証拠を消してしまったり，証拠の原本同一性に疑義が生じることとなったりするため，これを行う者は非常に神経を使うことになる．

証拠保全ガイドライン第 3 版は全 67 ページから構成されており，「インシデント発生（又は発覚，以下同じ）直後の対応」や「対象物の収集・取得・保全」等目的とフェーズに応じて 5 つの章に分かれている．事前に行う準備や作業に必要な資機材も書かれており，作業実施時の手順書として用いることができる．


一貫性(Chain of Custody)追跡記録

インシデントの概要			
件名		インシデント番号	
作業者		作業日	

証拠リスト		
証拠番号	容量	証拠の内容

一貫性			
作業日	作業内容	作業確認者 (Sign & Print Name)	作業受取者 (Sign & Print Name)

* Picuture(s) may require to show an identity of the evidence

図 1 一貫性追跡記録シート
Fig. 1 Chain of Custody Sheet.

3.2 ドキュメント作成の重要性と負担

デジタル・フォレンジックにおいては証拠保全後に作業記録を管理することも重要である．Tanner らはインシデント調査の担当者が複数の案件を管理する困難さを指摘しており，各証拠の情報を可視化して整理するツールを提案している [12]．IDF の証拠保全ガイドラインにおいては付録として**図 1** に示す「一貫性（Chain of Custody）追跡記録」シートが添付されており，対象機器の概要をドキュメントにまとめることを推奨している．証拠保全作業を行う場合に，いつ，どのような作業をどの順番で行ったのかというログを残すことは証拠を確保することと同様に重要であり，これらの記録はこれまで手作業で行う必要があった．

4. ガイドライン総合支援システム

4.1 システムの要件

GSS を開発するにあたり，作業をサポートする対象と実現すべき要件を検討した．2 章の調査よりシステムの想定利用者は「一般企業または教育機関に所属する，デジタル・フォレンジックの深い知識を保有していない人物」とした．証拠保全作業を行う場合は基本的には IDF のガイドラインに沿って作業を行えばよいが，日本ではデジタル・フォレンジックに対する従業者の意識が低く，IDF のガイドラインの内容を事前に理解してもらうことは現実的ではない．そのために突然のインシデントの際にも，IDF のガイドラインを参照せずに手順を踏んで証拠保全作業を実施できるシステムの需要があると考えた．また現場の技術者は，他にもいろいろな仕事を持っているので，証拠保全のための初期対応に要する作業工数を可能な限り低減できることが望ましい．証拠保全作業をサポートする手段としては次の理由で Android アプリケーションを採用した．

(1) PC に比べ，インシデント発生時に持ち運びをしやすい．

(2) iPhone の iOS アプリケーションの開発には Mac OS を必要とするのに対し，Android アプリケーションの開発は Windows に対応している．

(3) Android アプリケーションは Java 言語で開発できるため，Java のプラットフォーム向けに提供されている多くのライブラリを利用することができる．

続いて，著者らは証拠保全ガイドラインの発行元である IDF の技術分科会ワーキンググループの協力のもとシステム化要件の検討を行った．まず，GSS においては一連の手続きのまとまりをガイドラインのファイルとして定義することにした．これは，ガイドラインの内容が議論によって変更されていくことを考慮したためである．ガイドラインをファイル単位で内容の差し換え可能にし，Android アプリケーションとガイドラインを疎の関係にすることで，内容の変更に柔軟に対応することができる．そのためはガイドライン作成を行う環境を用意し，Android アプリケーションで読み込むガイドラインを構造化された状態で保管する必要があった．

証拠保全作業の実施においては，現場にファーストレスポンダが 1 人しかいないという状況も考えられるため，ファーストレスポンダの知識の深さにかかわらず，手順に沿って証拠保全作業を実行できる必要がある．GSS では 6.3.1 項で記述する用語集機能と作業スキップ機能を実装し，フォレンジックについての深い知識を有していない人物の作業を支援することにした．用語集機能は証拠保全作業とリンクさせてガイドラインの作業に出てくる専門用語を解説する機能である．作業スキップ機能は，作業を実施できない場合にその作業を飛ばして次の作業に行くことができる機能である．作業をスキップする場合はその理由を選択させることで，フォレンジックの深い知識を有していない人物が，ガイドラインのどの項目においてどのような理由で作業を実施できなかったのかを判定することができる．これにより証拠保全作業で初心者が躓きやすい項目を後から洗い出すことができ，今後の証拠保全作業手順の見直しに生かすことができると考えた．作業スキップの理由は次の選択肢から選べるようにする．

- 状況的に実施できない．
- 対象物に関する情報不足．
- 作業者の知識不足．
- この作業を行うことに不安がある．

証拠保全作業においては，作業自体に証拠性を確保することも重要である．紙の証拠保全ガイドラインを参照しながら作業を行う場合は作業自体の証拠性を主張することは困難であるが，Android アプリケーションを使用することで時間や位置情報等の客観的な証拠性を確保することができると考えた．また Android 端末で利用できるカメラや音声録音をはじめとした入力インタフェースを利用することで作業者の情報入力の負担を軽減し，現場の詳細な状況を残すことができる．さらに作業終了後は 3.2 節の一貫性追跡記録シートに準じた形式の作業レポートが出力できると別途作業レポートを作成する手間が生じないため便利であ

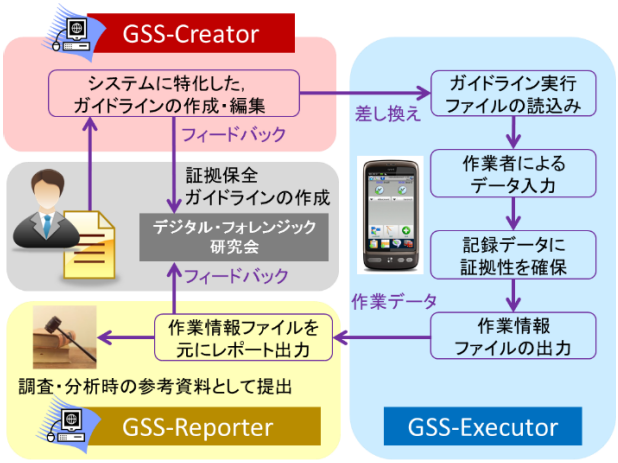


図 2 ガイドライン総合支援システムの概要
Fig. 2 Overview of the Guideline Total Support System (GSS).

る．これらの検討に基づき，次のようなシステム化要件を決定した．

(1)システム用のガイドラインファイルの作成を行う．
(2)構造化された手順に基づく作業のガイドを実施する．
(3)作業の証拠性を確保する情報を付与する．
(4)Android 端末の複数の入力インタフェースを利用する．
(5)行った作業についてのレポートを出力する．

5 つの要件のうち，(2)，(3)，(4) は Android アプリケーションで対応できるが，(1) のガイドラインの作成と (5) の作業レポートの出力は PC 環境で行う必要があることが分かった．そのため (1)，(5) を実現するために PC 上のツールを開発し，Android と PC の統合システムを開発することにした．これらの要件により，システム用のガイドラインファイルが正しいという前提条件の下で，(目的 1) および (目的 2) を達成することができるシステムを構築することができると考えた．

4.2 システムの概要

著者らが開発した GSS は 3 種類のアプリケーションから構成される．システムの概要を**図 2** に，各アプリケーションの概要を**表 1** に，動作・開発環境を**表 2**，**表 3** にそれぞれ示す．事故・犯罪等によってふだんと異なる機器の状態を察知したファーストレスポンダは，証拠保全作業手順のガイドを実行するために Android アプリケーション「GSS-Executor」を使用する．実施可能なひととおりの作業が終了したら PC 上にデータを展開し，「GSS-Reporter」を使用して作業レポートを出力する．

GSS-Executor で読み込むガイドライン実行ファイル（以下，実行ファイルと呼ぶ）は，専用の PC 上のアプリケーション「GSS-Creator」によって作成・編集する．実行ファイルは IDF の証拠保全ガイドラインをベースに作成するが，GSS-Creator の編集機能を利用して改良過程で検討を加えていくことを想定している．完成した実行ファイルは GSS-Executor にパッケージして配信し，アプリケーションのアップデートによって差し換えることができる．

表 1 アプリケーションの概要
Table 1 Application programs overview.

ツール名	概要
GSS-Creator	PC 上のアプリケーション． GSS-Executor で使用する XML 形式のガイドライン実行ファイルを生成する
GSS-Executor	Android アプリケーション． 保全現場で起動して作業を行う
GSS-Reporter	PC 上のアプリケーション． GSS-Executor で行った作業の記録を出力する

表 2 GSS-Creator，GSS-Reporter の動作・開発環境
Table 2 Operating and development environment for GSS-Creator and GSS-Reporter.

動作環境	Windows Vista/7/8/8.1
開発環境	Microsoft Windows 8 Enterprise Microsoft Visual Studio 2010 .NET Framework Version 4.0.30319 RTMRel
開発言語	C#
開発ステップ	約 6,000 ステップ（GSS-Creator） 約 500 ステップ（GSS-Reporter）

表 3 GSS-Executor の動作・開発環境
Table 3 Operating and development environment for GSS-Executor.

動作環境	API 10: Android 2.3.3（最小 SDK）
開発環境	Microsoft Windows 8 Enterprise Eclipse 4.2 Juno
開発言語	Java 1.6.0_43
開発ステップ	約 13,000 ステップ

5. GSS-Creator

5.1 ガイドライン作成ツールと作成手法

Android アプリケーション GSS-Executor で証拠保全作業のガイドを実行するには，作業手順や内容についての体系化された情報が必要である．著者らは GSS-Executor で読み込む実行ファイルを作成・編集する PC 上のアプリケーションとして GSS-Creator を開発した．GSS-Creator では時系列による作業手順を表現するために，フローチャートとブロックによってガイドラインの構築を行う．フローチャートはシステム設計において処理の流れを表現するために使用される図である．

デジタル・フォレンジックの研究においては，モバイルフォレンジックにおける証拠保全作業手順の視覚化にフ

表 4 証拠保全ガイドライン第 2 章の抜粋
Table 4 A part of Chapter 2 of the Guidelines for preservation of Evidence.

2.2.3 対応に過不足が確認された場合の対処
● 収集した情報・項目内に，不足している箇所が確認された場合，その情報を補充するためのインタビュー又は情報収集．
● 収集した情報・項目内に，余分な箇所が確認された場合，その情報を収集した基準及び理由を 聴取し，不必要と判断された場合は削除．

ローチャートが使用されている [13]．さらに GSS-Creator ではフローチャートを格納するブロックを定義することで，実行ファイル編集時の操作性向上を図る．

5.2 ガイドラインのデータ構造

GSS において実行ファイルをどのようなデータ構造で定義するべきか検討を行った．証拠保全ガイドラインの内容の一部を**表 4** に示す．証拠保全ガイドラインは現場の状況によって行うべき作業が分類されているので，証拠保全ガイドラインをベースに実行ファイルを作成する場合，作業の開始から終了までを 1 本のフローで定義することが難しい．そこで著者らは現場の状況に応じた作業を定義するために，条件分岐の階層構造を表現できる XML 形式のファイルを実行ファイルとして採用した．XML は単一の情報に複数の属性を記述できるため，作業の内容に応じた異なる振舞いを定義するために有効である．

5.3 証拠保全ガイドラインとの互換性と信頼性の評価

著者らは証拠保全ガイドラインをベースに実行ファイルを作成することにしたため，実行ファイルの信頼性を評価する必要があった．証拠保全ガイドラインそのものに問題があることが分かった場合に IDF へ報告することも考慮したため，GSS のフローチャートを共有する必要がある．本研究では Web 上でダイアグラムを作成し共有することができるサービス「Cacoo（カクー）」を利用する [14]．Cacoo を利用して作成したフローチャートを公開することで，作業の順序や内容について関係者やツールの使用者に対して意見を求めることができる．Cacoo を使用して作成・共有するフローチャートの一例を**図 3** に示す．

5.4 GSS-Creator の機能

図 4 は開発したアプリケーション GSS-Creator のメイン画面である．アプリケーションの右側の部分がフローチャートによる作業手順の作成部であり，1 つのブロックに相当する．画面左側にはブロックの一覧とフローチャートの全体図が表示されており，フローチャート上に作業項目を配置していくことで実行ファイルを作成していく．ブロックを利用することで複数の箇所で同一の作業フローを定義する必要がある場合にも，一度だけ中身のフローチャートを定義したブロックを作成するだけでよい．例として保全対象物がデスクトップ型かノート型のパソコンのとき，前者と後者で異なる作業フローを実行した後，電源を OFF にする手順を共通化したい場合に，電源 OFF 手順のブロックを両者の共通フローにすることができる．

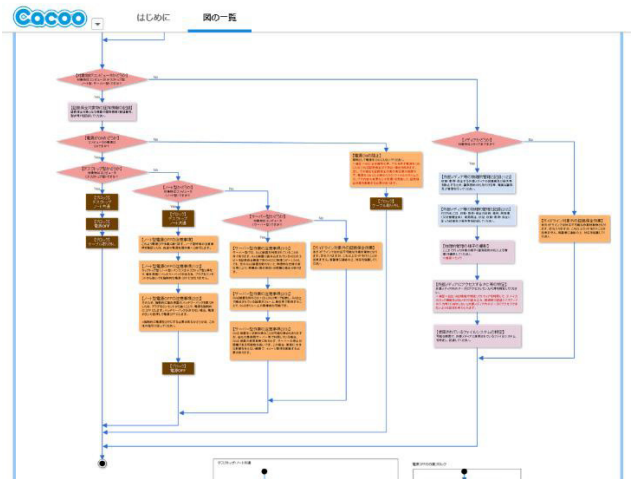


図 3 Cacoo を使用して作成したフローチャートの一例
Fig. 3 An example of flowchart created using Cacoo.

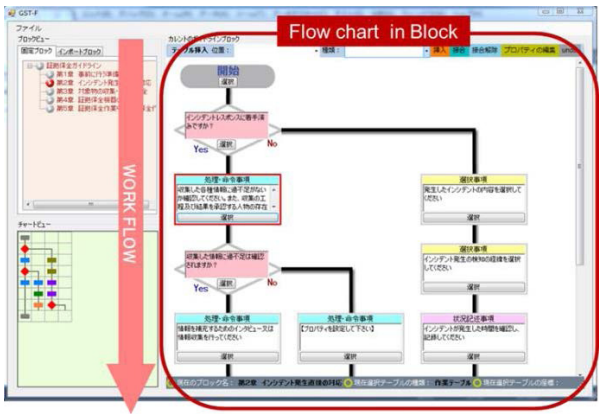


図 4 GSS-Creator のガイド作成画面
Fig. 4 Guideline creation screen of GSS-Creator.

IDF の証拠保全ガイドラインではインシデント発生時に作業者に様々な作業を行うことを要求しているが，著者らの調査の結果，**表 5** に示す 5 種類の作業項目に分類できることが分かった．このうち「記録」項目は Android 端末の入力インタフェースから適切な機能を呼び出す必要があるため，**表 6** のとおり設定可能なインタフェースを定義した．これにより現場の作業の種類に応じた適切なインタフェースを利用することができる．「条件分岐」項目はフローを Yes 側と No 側の 2 通りに分岐させることで，現場の状況によって作業が異なる場合を定義することができる．作業項目をフローチャートへ挿入した後，項目に応じたプロパティを設定する必要がある．

表 5 作業項目の一覧
Table 5 GSS-Creator Work items.

項目名	内容
注意	作業上の注意を促す
選択	複数の選択肢から当てはまるものを選ぶ
処理	具体的な行動を伴う作業を指示する
記録	現場の状況などについて記録を求める
条件分岐	選択内容に応じて作業フローを分岐する

表 6 設定可能な入力インタフェースの詳細
Table 6 Details of settable input interfaces.

インタフェース	Android 端末での動作
テキストボックス	ソフトウェアキーボードを表示し，テキストによって入力を行う
日時選択	年月日及び時刻を選択するインタフェースを利用する
数値入力	画面のスワイプ操作により数値を選択する機能を利用する
音声録音	Android のメディアレコーダー機能を呼び出して音声を録音する
カメラ	Android のカメラ機能を呼び出して写真を撮影する

6. GSS-Executor

6.1 GSS-Executor の機能

ファーストレスポンダは GSS-Executor を使用して証拠保全作業のガイドを実行する．インシデントの発生が疑われたら現場で GSS-Executor を立ち上げ「新規インシデント」を作成する．GSS-Executor はインシデント単位で証拠の情報を管理することができる．新規インシデント作成後はインシデント別のトップ画面に遷移し，実行したいガイドを選択するとガイドが開始される．**図 5** に GSS-Executor のメイン画面とインシデント別のトップ画面を示す．

ガイドが開始されると GSS-Executor は実行ファイルに記述されたフローに従い，作業内容と属性が定義されたタグを読み込んで作業項目の画面を生成する．GSS-Executor によるガイドの実行画面を**図 6** に示す．アプリケーションの画面上部には作業のタイトルや作業の種類を表示するラベルが配置されている．画面下部には次の作業へ遷移するためのボタンが配置され，画面の中央部分に入出力インタフェースを動的に更新して配置する．条件分岐項目の画面では質問文に対して Yes を選択するか No を選択するかによって，遷移する作業の項目が変化する．これにより現場の状況に特化した処理を行うことができる．

図 6 の左側の画面は選択事項の例である．この例では「発生したインシデントに関する対象物の種類を選択してください」という内容について，チェックボックスで該当する項目を選択して記録できるようになっている．図 6 の右側の画面はカメラ機能を利用している場面である．カメラ機能を利用することで作業者は保全対象物の状況を写真に撮ることができる．複数枚の撮影にも対応しており，メモも付与できる．また音声録音機能では，作業者が口頭で現場の状況を説明して録音できる．本稿の「はじめに」で述べたとおり証拠保全作業は迅速な対応が求められるので，著者らは Android 端末のソフトウェアキーボードによって入力を行うよりも口頭で録音する方法が有効だと考えている．本節で記述した以外のインタフェースとして 5.4 節の表 4 のインタフェースを利用できるが，説明は割愛する．

図 5 GSS-Executor の実行画面 1
Fig. 5 GSS-Executor execution screens 1.

図 6 GSS-Executor の実行画面 2
Fig. 6 GSS-Executor execution screens 2.

6.2 証拠性を確保するための機能

6.2.1 NTP サーバ接続による端末時刻の誤差の確認

GSS-Executor では各作業を行った時刻を記録するが，Android 端末のシステム時計依存では標準時との誤差が生

じる恐れがある．そのため Network Time Protocol（NTP）を使用した標準時刻とシステム時計の誤差を確認する仕組みを実装した．Android においては Apache Commons Net によって NTP 接続のライブラリが提供されており，本研究では同ライブラリを使用することで誤差の確認機能を実現した．時刻の同期が確実に行われたかどうかの情報も端末のデータベースに記録するようにする．

6.2.2 端末の通信状態の孤立

無線ネットワーク接続を行う機器が保全対象物となる可能性があるため，対象物への影響を最小限にするために Android 端末をネットワークから孤立状態にする．Android では「機内モード」に設定することで 3G 回線と Wi-Fi をともに遮断することができるため，本機能を実装した．機内モードになっていても作業中に意図的に Wi-Fi 接続を行うことが可能なため，作業項目が遷移するたびに通信状況を確認しその状態を記録するようにした．

6.2.3 GPS による位置情報の取得

証拠保全作業中に現場で確実に作業を行っているという情報を確保するために，端末の GPS 機能を利用して位置情報を記録する．GPS は屋外での使用が前提とされるが，屋内でも窓側で作業を行う場合や天候状態の変化等で GPS 衛星の信号を捕捉できるタイミングがあることが分かった．GSS-Executor ではガイド開始時に端末の GPS 機能を有効にし，作業中は GPS 信号の探索を継続することで現場の緯度と経度をデータベースに連続して記録する．

スマートデバイスにおける位置情報の取得方法としては iOS7 の iBeacon を用いる方法もある．iBeacon は屋内でも使用することができ，GPS と比較してより正確な位置情報を取得することができる．GSS-Executor ではプラットフォームに Android を採用したためこの機能の実装を行うことはできなかったが，iBeacon は現場に専用機器の設置が必要であるうえ，通信方式に Bluetooth を使用する．前節で述べたように GSS では端末の通信を孤立状態にする必要があるため，すべての通信が孤立状態でも使用可能な GPS による位置情報の取得はシステムの要件に合致していると考える．

6.3 付録機能

6.3.1 フォレンジック用語集

ガイド実施時に表示された文章中に赤文字で強調表示された単語がある場合，その単語の解説をポップアップで確認することができる．用語と解説はアプリケーション内のデータベースに登録されており，用語集単体で使用することもできる．本機能により情報セキュリティの専門知識を持たないファーストレスポンダの作業を支援する．

6.3.2 操作ログの確認

GSS-Executor で行われた各作業の操作履歴を記録し，アプリケーションが起動された日時や，意図せずに作業の実施情報が削除されていないかどうかを確認できる．証拠性確保の仕組みの一環として実装した．

7. GSS-Reporter

7.1 作業実施情報の抽出

GSS-Reporter は PC 上で動作するアプリケーションであり，GSS-Executor から出力された CSV 形式の作業情報ファイル（以下，情報ファイルと呼ぶ）を読み込んで内容を表示する．作業時に入力された情報を確認することができ，表示する項目の種類を絞り込むことができる．抽出できる項目の例を**表 7** に示す．情報ファイルとともに写真や音声のデータが出力されている場合は，そのファイルを読み込み確認することができる．作業中に意図的に行った不正がある場合や端末の設定ミス等で正しく作業が行われなかった場合は，その状況の変化を時系列で確認することができる．

7.2 作業レポートファイルの出力

GSS-Reporter を使用して作業レポートファイルを出力することができる．作業項目を抽出するチェックボックスで選択された項目のみを出力できるため，作業者自身や提携先のフォレンジック（調査・解析）チームの要望に応じて，カスタマイズした作業レポートを出力することが可能である．レポートは HTML ファイルの形式で出力されるため，インターネットブラウザが扱える環境であれば内容を確認したり印刷したりすることができる．GSS-Reporter によって出力されたレポートファイルのサンプルを**図 7** に示す．撮影された写真も時系列で出力されるため，詳細な作業状況を確認することができる．

表 7 主な抽出可能項目
Table 7 Main extractable Items.

項目	内容
インシデント番号	インシデント別に付与される番号
ガイド番号	ガイドライン別に付与される番号
シーケンス番号	作業の通し番号
日時	作業を行った日時
時刻精度	NTP サーバ接続による時刻同期が正常に行われたかどうか
GPS 経度・緯度	GPS 衛星から取得した位置情報
通信遮断	作業中に 3G 回線と Wi-Fi が共に OFF になっていたかどうか
タイトル	作業のタイトル
本文	作業の本文
入力	入力された内容（テキスト・音声・画像へのリンク）
作業スキップ	作業をスキップしたかどうか
登録タグ	作業時に登録されたタグ

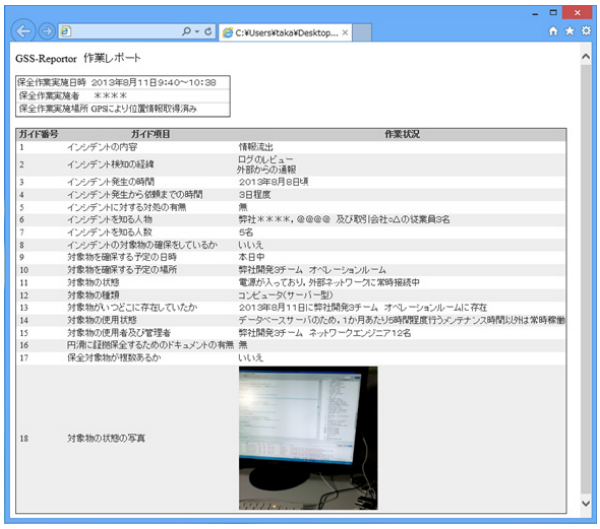


図 7 GSS-Reporter によって出力された作業レポート
Fig. 7 Work report generated in HTML format from GSS-Reporter.

3.2 節で示した IDF の「一貫性（Chain of Custody）追跡記録」シートでは，共通の記入項目としてインシデントの件名や作業者名，証拠の概要を記録し，その後に対象物に対して行った各作業について作業日時と作業内容を記録するようになっている．GSS-Reporter で出力する作業レポートファイルにおいても，GSS-Executor で入力されたインシデント名や作業者等の情報をレポートの先頭に出力し，そのあとに各作業の記録項目が作業日時等とともに出力される．このため GSS-Reporter で出力する作業レポートファイルは「一貫性（Chain of Custody）追跡記録」シートで求められる情報と同様の内容を出力することができる．

8. 疑似シナリオによる GSS 利用の評価

著者らは GSS を証拠保全作業に適用することを想定し，疑似シナリオによる適用の評価を行った．証拠保全作業のみでなく作業レポートの作成までを含めて，GSS が従来の作業と比べてどの程度負担が軽減されるかをユーザビリティのアンケート，作業時間，自由記述コメントにより総合的に評価した．なお疑似にあたっては実際に起こった電磁的記録に関するインシデント事例を調査し，疑似シナリオを作成して評価を行った．

8.1 疑似シナリオの選定

実験の事前準備として疑似シナリオの設定を行った．NPO 法人日本ネットワークセキュリティ協会が発表した資料によると，2012 年における情報漏えいにおける原因として管理ミスが最も多いため，管理ミスによる情報漏洩事件を題材とした [15]．今回の被験者は東京電機大学の情報系分野を専攻する大学生・大学院生 10 名とした．いずれの学生もデジタル・フォレンジックに関わる実務経験はなかった．

表 8 疑似シナリオ
Table 8 Artificial scenario.

ABC 大学の XYZ 研究室では研究に使用するために，提携先の企業から機密情報のデータ提供を受けている．XYZ 研究室とその企業の間では「データは絶対に専用の HDD から移動してはならず，データを使用している間は研究室のネットワークを遮断しなければならない」という契約になっていた．しかし長期間に及ぶデータ貸与の中で，関係者間で契約内容の引き継ぎが正しく行われず，外部ネットワークに接続された PC の共有フォルダに機密データがアップされていた．ある日，その事実を知った指導教員は【被験者】に対して企業との機密契約の事実を知らせ，すぐに該当データに対して外部からアクセスがなかったか確認するように指示した．【被験者】が通信ログを調べたところ，1 週間前に外部から当該データへ不正アクセスがあったことが確認された．【被験者】はすぐさま現時点の状況を証拠保全することにした．

表 9 共通の評価項目に対する評価結果
Table 9 Evaluation results against common questions.

	評価項目	平均値 (n=10)
1	実験のストーリー設定は適切だと思うか	4.4
2	実験用メモで提示された情報は，作業をするうえで必要十分なものだったか	3.7
3	システムは全体的に使いやすかったか	4.2

現場として大学の研究室を設定した．NPO 法人情報セキュリティフォーラムではセキュリティインシデントの事例を公開しており [16]，実例に基づいた疑似シナリオを**表 8** のとおり設定した．

この疑似シナリオを被験者 10 名に対して説明した後，作業に必要な情報を記した疑似用メモを渡して作業を行ってもらった．疑似は GSS を使用して作業レポートを出力するまでの一連の作業を行ってもらった．また同様の内容について紙の証拠保全ガイドラインでも作業を行ってもらい，両者の差異について検討を行った．5 名ごとに 2 つのグループに分け GSS と紙の実施順序を逆にすることで，先入観による評価結果への影響を最小限にした．

8.2 評価項目と結果

8.2.1 ユーザビリティのアンケート

共通の評価項目に対する評価結果を**表 9** に，GSS-Executor と GSS-Reporter のユーザビリティの評価結果を**表 10**，**表 11** に示す．それぞれの評価は各質問に対して 1 点から 5 点までの 5 段階で評価をしてもらう方式で行った．

疑似用に準備した環境が適切であったと確認できたほか，システム全体を通して使いやすいという評価を得ることができた．GSS-Executor の評価ではアプリケーション

表 10 GSS-Executor についての評価項目と評価結果
Table 10 Evaluation results against questions for GSS-Executor.

	評価項目	平均値 (n=10)
1	説明を受けなくても直感的に使えるか	3.6
2	各機能のレイアウト配置は適切か	3.6
3	作業の色分け表示はわかりやすかったか	4.5
4	タグの付与機能は良いと思うか	3.6
5	関連情報の表示機能は良いと思うか	4.1
6	証拠保全作業は即時性と正確性が求められるが，本ツールを使うことで素早く且つ正確にガイドを実行することができると思うか	4.2

表 11 GSS-Reporter についての評価項目と評価結果
Table 11 Evaluation results against questions for GSS-Reporter.

	評価項目	平均値 (n=10)
1	説明を受けなくても直感的に使えるか	4.0
2	表による出力は適当か	4.7
3	抽出できる項目の内容は適切か	4.7
4	レポートの出力機能は便利か	4.8

のルックフィールと提案手法について尋ねた項目で高評価を得た．一方で使用する前にアプリケーションの操作方法の説明が不十分であることが分かった．実際のインシデント発生時は作業者に心理的な余裕がないと考えられるので，そのような状況下でも確実に操作が行えるインタフェースを検討する必要がある．GSS-Reporter の評価では全体的に高スコアを得ることができたが，著者らはより細かい条件を指定してデータ抽出する機能の実装を検討している．

8.2.2 作業レポートの有効性

IDF の証拠保全ガイドラインの第 2 章「インシデント発生（または発覚，以下同じ）直後の対応」において，証拠保全の最初期に作業実施を要求している 9 項目の作業における，GSS を使用した場合の回答の割合を**表 12** に示す．判定は出力された作業レポートファイルをもとに行った．実施された作業の正確性や品質についての評価を行うのは困難なため，作業単位でその作業が実施されたか否かによって回答の割合を出した．

一部の被験者において回答を得られなかった項目があったが，全体として良好な回答の割合を得ることができた．このことから GSS を使用してインシデント発生直後における最初期の状況の入力を適切に行えることが分かった．これにより，少なくとも情報系の学生であればデジタル・フォレンジックに関する専門知識がなくても対応が可能であり，（目的 1）を達成できることが明らかになった．

表 12 作業項目別の回答の割合
Table 12 Response rate according to each work item.

項目	作業	回答
選択	発生したインシデントの内容	10/10
選択	発生したインシデント検知の経緯	9/10
記録	発生したインシデント発生の時間	10/10
記録	発生したインシデントを知る人物	10/10
分岐	対象物の確保の有無	10/10
記録	対象物を確保した日時	10/10
記録	対象物を確保した場所	9/10
選択	対象物の絞り込み	10/10
記録	対象物の状態	10/10

表 13 紙のガイドと GSS の作業時間の評価
Table 13 Evaluation result using GSS-Executor compared with paper media.

	紙のガイドライン	GSS-Executor
作業に要した平均時間	29 分 41 秒	24 分 12 秒

表 14 作業レポート作成の所要時間についての評価
Table 14 Evaluation result of the time required for working report generation.

被験者	証拠保全作業の所要時間（紙のガイドライン）	作業レポート作成の所要時間
1	34 分 14 秒	28 分 16 秒
2	22 分 49 秒	17 分 51 秒
3	17 分 04 秒	22 分 29 秒
平均	24 分 42 秒	22 分 52 秒

8.2.3 作業時間の比較

紙の証拠保全ガイドラインを参照しながら作業を行った場合と GSS-Executor を使用した場合で，作業時間にどの程度差が生じるかについて時間計測を行った．GSS-Executor と紙のガイドラインで，それぞれインシデント発生直後の対応内容を示す箇所についての作業を行ってもらい実施状況を比較した．**表 13** に示すとおり，結果は GSS-Executor が紙のガイドラインより約 5 分短いという結果になった．GSS-Executor はインシデントの状況に応じて必要な情報を自動的に読み込むため，作業者自身が情報を探す手間をかけなくてよいことが有効であったと考えられる．

一方レポートの作成においては GSS-Reporter を使用することで大きなメリットがあると考えられる．今回の被験者のうち 3 名に，紙の証拠保全ガイドラインで実施した作業内容を 3.2 節の一貫性追跡記録シートに準じた形式に手作業（PC 上）でレポートにまとめてもらったところ，**表 14** に示すとおり，作業にかかった時間の平均は約 23 分

となった．対象物の写真等を挿入したレポートを作成・編集する場合はさらに時間がかかると予想される．この点において，GSS を使用した場合はドキュメントを作成するための時間や負担は生じない．したがって，GSS は（目的 2）を達成できることが明らかになった．また，GSS-Reporter のユーザビリティ評価で高スコアを得ることができたことからも，レポート作成の面での GSS の有効性を確認できた．

8.3 その他の考察

自由記述コメントの回答では，GSS-Executor において「作業の実施順序が適切でないのではないか」や，「何度も同じ情報を入力していた気がする」等の意見を得た．今回実験用に準備した実行ファイルは IDF の証拠保全ガイドラインをベースにしたため，これらの指摘は証拠保全ガイドラインそのものに存在する問題だといえる．逆にいうと GSS を導入することにより証拠保全作業の事前検討が容易になり，より良いガイドラインを作成するために役立つことが分かる．今回の適用結果は IDF の技術分科会ワーキンググループにフィードバックすることで，ガイドラインの見直しに反映させていきたいと考えている．

9. おわりに

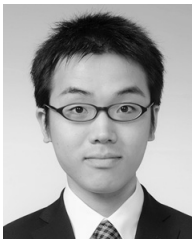
著者らは Android 端末と PC を使用してインシデント発生現場で初動対応者の証拠保全作業を支援するシステムを開発した．フローチャートの手順どおりに作業の内容をガイドする Android アプリケーションを利用することで，迅速かつ正確に証拠保全作業を行うことができると考える．さらに証拠保全作業のレポートを出力することで，関係者間で作業の実施状況を共有することができる．

今後は 1 つのシミュレーションだけでなく，マルウェア感染やクラウド上の証拠保全等の様々な種類のインシデント事例に対応できるかどうか検討を行っていく必要がある．また GSS-Reporter によって出力される作業レポート自体の証拠性も重要であるため，作業実施時に Android 端末で電子署名を付与する仕組みの実装が望まれる．一般に幅広く使ってもらうためにも，評価実験をふまえてシステム全体をより良いインタフェースにしていく予定である．

謝辞 GSS の開発にあたり種々の有益なご意見をたまわったデジタル・フォレンジック研究会技術分科会ワーキンググループの皆様，ならびに実験にご協力いただいた東京電機大学の皆様に感謝申し上げる．

参考文献

[1] 警視庁：平成 25 年警察白書 サイバー空間の脅威への対処，入手先 ⟨http://www.npa.go.jp/hakusyo/h25/pdf/pdf/04_tokusyu.pdf⟩
[2] デジタル・フォレンジック研究会：デジタル・フォレンジックとは，入手先 ⟨https://digitalforensic.jp/home/what-df/⟩
[3] デジタル・フォレンジック研究会 技術分科会 ワーキンググループ：「証拠保全ガイドライン 第 3 版」，入手先 ⟨https://digitalforensic.jp/wp-content/uploads/2014/06/5b0f6b0e93f42b5b3fd27a290d977a681.pdf⟩（参照 2013-09-30）．
[4] 天野貴通，高橋 涉，上原哲太郎，佐々木良一：証拠保全作業のためのガイドライン総合支援システムの開発と評価，マルチメディア，分散協調とモバイルシンポジウム 2013 論文集，pp.838–845 (2013).
[5] 笹嶋宗彦，西村悟史，來村徳信，ウイリアムソン彰子，木下智香子，服部兼敏，溝口理一郎：看護手順知識の習得を支援するタブレット型ツール CHARM Pad の試作，第 27 回セマンティックウェブとオントロジー研究会 SIG-SWO-A1201-06 (2012.5.9).
[6] Boxwala, A.A. et al.: GLIF3: A representation format for sharable computer-interpretable clinical practice guidelines, *Journal of Biomedical Informatics*, Vol.37, pp.147–161 (May 2004).
[7] Ashino, Y., Fujita, K., Furusawa, M., Uehara, T. and Sasaki, R.: Extension and Evaluation of Boot Control for a Digital Forensic System, *Advances in Digital Forensics V*, Peterson, G. and Shenoi, S. (Eds.), pp.133–141 (2009).
[8] Kuntze, N., Rudolph, C., Alva, A. and Endicott-Popovsky, B. (Eds.): On the Creation of Reliable Digital Evidence, *Advances in Digital Forensics VIII*, Peterson, G. and Shenoi, S. (Eds.), pp.3–17 (2012).
[9] Osborne, G., Thinyane, H. and Slay, J.: Visualizing Information in Digital Forensics, *Advances in Digital Forensics VIII*, Peterson, G. and Shenoi, S. (Eds.), pp.35–47 (2012).
[10] 独立行政法人情報処理推進機構：2013 年度情報セキュリティ事象被害状況調査—報告書—，入手先 ⟨http://www.ipa.go.jp/files/000036465.pdf⟩（参照 2014-01）．
[11] 財団法人 コンピュータ教育開発センター：学校情報セキュリティポリシー策定・運用のための学校情報セキュリティ・ハンドブック解説書，入手先 ⟨http://www.cec.or.jp/seculib/handbook/gjskai.pdf⟩
[12] Tanner, A., Dampier, D. and Thompson, J.: On developing a conceptual modeling report management tool for digital forensic investigations, pp.445–450 (2012).
[13] Raghav, S. and Saxena, A.K.: Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition, *Proc. 2009 IEEE Student Conference on Research and Development*, pp.5–8 (2009).
[14] Cacoo, available from ⟨https://cacoo.com/diagrams/⟩
[15] NPO ネットワークセキュリティ協会：2012 年 情報セキュリティインシデントに関する調査報告書—個人情報漏えい編，入手先 ⟨http://www.jnsa.org/result/incident/2012.html⟩
[16] NPO 情報セキュリティフォーラム：教育現場における情報セキュリティ事故・対応事例の研究事例集，入手先 ⟨http://www.isef.or.jp/rd/jirei.pdf⟩（参照 2014-04）．



天野 貴通

2013 年東京電機大学未来科学部情報メディア学科卒業．2015 年同大学大学院修士課程修了．現在，三菱電機インフォメーションシステムズ株式会社に所属．

上原 哲太郎 （正会員）

1990 年京都大学工学部情報工学科卒業．1995 年同大学大学院工学研究科情報工学専攻博士後期課程研究指導認定退学．同年同研究科助手．1996 年和歌山大学システム工学部講師．2003 年京都大学工学研究科付属情報センター助教授．2006 年同大学学術情報メディアセンター助教授．2011 年総務省情報通信国際戦略局通信規格課標準化推進官．2013 年より立命館大学情報理工学部教授．京都大学博士（工学）．システムセキュリティ，デジタルフォレンジック等の研究に従事．IEEE，電気学会，電子情報通信学会，日本ソフトウェア科学会，システム制御情報学会，社会情報学会，情報ネットワーク法学会，CIEC 各会員．

佐々木 良一 （フェロー）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001 年 4 月より東京電機大学工学部教授，2007 年 4 月より未来科学部教授．工学博士（東京大学）．1998 年電気学会著作賞受賞．2002 年情報処理学会論文賞受賞．2007 年総務大臣表彰等．著書に，「IT リスクの考え方」岩波新書 2008 年等．日本セキュリティ・マネジメント学会会長，内閣官房サイバーセキュリティ補佐官．