Android 携帯を用いた証拠保全作業支援アプリケーションの開発

高橋渉†
佐々木良一†　　上原哲太郎††

社会が情報通信技術に深く依存するとともに，個人や組織の間で様々なレベルの紛争が発生する中で，電磁的記録の証拠保全及び調査・分析を適切に行うための技術であるデジタルフォレンジックの必要性が高まっている．そのデジタルフォレンジックに関連した作業として，コンピュータセンターの担当者などによる初動時の電磁的証拠の保全の手続きがあるが正しく行動するのは容易ではない．そのため，デジタルフォレンジック研究会では，「証拠保全ガイドライン」を作成した．しかし，このガイドラインは量が多いため，緊急時に証拠保全を必要とする作業者が適切に対応するのは容易ではない．そこで，証拠保全作業者の実施すべき項目を Android 端末を用いてガイドできるようにするプログラムを開発することとした．その際，プログラム作成の手間を低減するとともに，ガイドライン作成者のガイド作成作業を容易にするため，PC 上で指定の様式に従ってガイドラインを記述すると Android 端末上のプログラムが自動的に作成できる機能もあわせて開発した．

Development of Application Program to Help Evidence Preservation Using Android Type Mobile Phone

WATARU TAKAHASHI†
RYOICHI SASAKI†　TETSUTARO UEHARA††

The need of digital forensics which is the technique to keep the evidence and perform investigation and analysis of the electromagnetic record has been increasing, while society depends on the information and communication technology deeply, and the dispute of various levels occurs between individuals and organizations. The operation for digital forensics performed by people in charge of the computer center to keep the evidence at the time of the first action is not easy. To cope with the problem, the Digital Forensic Institute developed the guideline to keep the evidence of the electromagnetic record. However, it is not easy for workers to keep evidence without computer aid, because the volume of the guideline is much quantity. Therefore, we decided to develop the program of the guidance system with android terminal. At that time, we also developed the support system to produce the guideline easily, and function to transform the data from the support system to the program for android terminal automatically.

†東京電機大学大学院未来科学研究科
††京都大学学術情報メディアセンター

1. はじめに

社会が情報通信技術に深く依存するとともに，個人や企業・組織間で様々なレベルの紛争が発生する中で，電磁的記録の証拠保全及び調査・分析を適切に行うための技術であるデジタルフォレンジックの必要性が高まっている[1]．このデジタルフォレンジックに関連した技術としてコンピュータセンターの担当者などによるインシデント対応のための初動時における電磁的証拠の保全の手続きがある．この電磁的証拠の保全の手続きには以下の2つの課題がある．

- 取得の対象となるデータはどの範囲であるべきか

⇒技術的，時間の制約から，全ての関連したデータの複製を取得することが現実的でない場合がある．

- 保全した証拠の原本同一性の保証はどの程度確実にするべきか

⇒取得したデータが変更や改ざんがなく，複製データは原本と同じものであると思っていても，データ複製の際，副作用でデータの一部が破損または紛失する可能性がある．

この課題に対し，デジタルフォレンジックの歴史が浅い日本では，未だに広く認識された標準的な取得手続きのガイドラインが存在しない．そこでデジタルフォレンジック研究会では，このような状況に対処するため，本論文の著者の一人である上原が中心になり「証拠保全ガイドライン」を作成した[4]．しかし，このガイドラインは A4 用紙 20 枚程度で記させているため，緊急時に証拠保全を必要とする作業者が適切に対応するのは容易ではない．またガイドを今後拡張するとガイドライン作成者に負担となる．

そこで，本研究では証拠保全作業者の実施すべき項目を Android 端末を用いてガイドできるようにするプログラムを開発することとした．その際，プログラム作成の手間を低減するとともに，ガイドライン作成者のガイド作成作業を容易にするため，PC 上で指定の様式に従ってガイドラインを記述すると Android 端末上のプログラムが自

動的に作成できる機能も実現することとした．

現在，デジタルフォレンジック研究として，ワーム感染経路特定手法[2]や機密のデータの伝搬経路の可視化[3]など種々の研究がなされてきているが，デジタルフォレンジックに関するガイドを支援するプログラムについては，著者らが調査した範囲においては従来なかったものである．

2. 電磁的証拠保全の手続き

電磁的証拠の保全の手続きとは事故・不正行為・犯罪などの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，電磁的証拠となるものを取り出すといった作業のことである．ここでデジタルフォレンジック運用者として最も重要なことは，確実に，そのままで(As-is)で，収集(Collection)・取得(Acquisition)し，保全(Preservation)することである．この手続きに不備があり，証拠の原本同一性に疑義が生じると，後の電磁的証拠の分析結果の信頼性を失うため，これを行う者は，非常に神経を使うことになる．特に，デジタルフォレンジックの専門家でないコンピュータセンターの担当者などがこれらの作業を正しく行うのは容易でなかった．

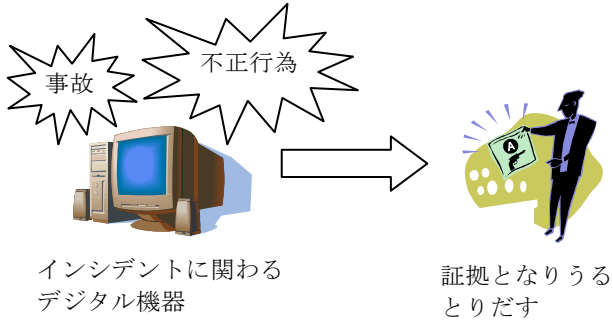

図１　電磁的証拠の保全の手続き

3. 証拠保全ガイドラインについて

3.1 証拠保全ガイドラインとは

「証拠保全ガイドライン」とはデジタルフォレンジック研究会が作成した電磁的証拠の保全手続きを行う標準的ガイドラインである．このガイドラインは，実際にデジタルフォレンジック関連技術の実運用している企業から意見を得ながら作成されたため，現時点での我が国における同関連技術の運用と大きく違いがないガイドラインとなっている．また，海外のガイドラインを参考にしながら作成されたこともあり，グローバルに活動する企業や組織にも利用可能なものとなっている．このガイドライン内容は以下のことが書かれている．

- 事前に行う準備
  証拠保全作業をする前に事前行う作業についてかかれている．例えば，インシデント発生の検出・判断方法，資機材の準備などが書かれている．
- インシデント発生直後の対応
  証拠保全作業を先方が行っている場合といない場合での対応の仕方，引き継ぎ作業方法が書かれている．
- 対象物の収集・取得・保全
  実際に行われる証拠保全作業方法が書かれている．
- 証拠保全機器の準備
  証拠取得機器の確認事項や必要な機能などが書かれている．
- 証拠保全作業中・証拠保全作業後
  証拠保全作業中また作業後に行うことが書かれている．例えば，作業中にビデオ撮影を行うなどが書かれている．

3.2 証拠保全ガイドラインの現状

証拠保全ガイドラインを参照し，電磁的証拠の保全手続きを行っている．しかし，まだまだ広く使われているわけではないのが現状である．今後，各現場において活用して頂けるようにしていく必要がある．

3.3 証拠保全ガイドラインの問題点

使っていただく上で次のような問題があると考えられる．

(1). 電磁的証拠の保全手続きを行う作業者は，A4用紙20枚程度の紙を見ながらの作業なので非常に面倒で即時の対応が困難である．また，作業ミスなど起こる可能性がある．

(2). 証拠保全ガイドライン作成者は，作業者が正しく動けるように必要十分な記述ができているかどうかの確認が容易ではなく，ガイドの拡張や新しい分野のガイドの作成に時間がかかる．

4. 提案方式

証拠保全ガイドライン内容をわかりやすくかつ作業ミスをなくすために携帯端末で表示することで，作業者の作業ミスや作業効率があがるのではないかと考えた．また，証拠保全ガイドライン作成者に対しては，編集作業を行いやすいガイドライン作成を支援するツールがあると非常に便利であると考えこれら 2 つを統合的に実現するツールを開発することにした．

4.1 提案方式概要

作業者に対して，証拠保全ガイドライン内容をわかりやすく，作業ミスをなくすために， 表１に各媒体における持ち運び，作業のしやすさ，開発のしやすさの観点から検討を行った． その結果，次の理由で証拠保全作業をAndroid携帯に表示するアプリケーションの開発を行うことにした．

(1). PCに比べ，インシデント発生時に持ち運びが容易である
(2). Android携帯は証拠性を保全する上で必要となる動画や静止画の撮影機能が標準で用意されている
(3). iPhoneアプリ開発はMacOSを必要とするのに対し，Androidアプリ開発はWindowsにも対応している．
(4). iPhoneアプリ開発にはObjectCといった独自の開発言語での開発に対し，Androidアプリ開発はJava言語で開発できる．

ガイドライン作成者に対しては，ガイドラインを作成するだけで，プログラムの熟練者がいなくても，誰でもAndroid画面を構築できると非常に便利である．そこで，ガイドラインを作成するだけで誰でもAndroid画面を構築できるプログラムの自動生成を行うアプリケーションの開発を行うことにした．現在，紙媒体のガイドラインがあるなかで，ガイドラインをまとめたマインドマップが作成されている[5]．このマインドマップをもとにした開発を行うことができないかと検討を行った．そこで，マインドマップを自動的にプログラムにする研究・アプリケーションを探した．しかし，UMLを入力するとソースコードを自動生成ツールの研究[6]や表形式UIモデル記述からのWeb画面プログラム自動生成[7]などのプログラムの自動化の研究がなされているが，マインドマップからAndroid画面を構築できる自動プログラムは存在しない．

また，マインドマップを作成できるFreeMindという既存のソフトを改良する方法も考えた．しかし，インターフェースなどがわからず容易にプログラムの開発を行うことができなかった．このことから，マインドマップを基にし，Android画面を構築できる自動生成プログラムを独自に開発することとした．

この2つのアプリケーションの使用の流れを図２に示す． ガイドライン作成者は紙媒体のガイドラインとガイドライン作成サポートツールを使いながら議論と入力を行い，ガイドラインを作成し，ガイドライン作成サポートツールからXML形式のガイドラインが出力される．次に，Android携帯に証拠保全ガイドライン内容を表示するアプリケーションで自動的にXML形式のガイドラインを読み込み，Android携帯に表示するといった流れになっている．以下に2つのアプリケーションについて説明していく．また，2つのアプリケーションの開発環境について表２，表３に示す．

図２　アプリケーションの使用の流れ

表１　各媒体の検討

媒体	持ち運び	作業しやすさ	開発のしやすさ
紙媒体ガイドライン	○	×	△
PC	△	△	○
Android携帯	○	○	○
iPhone	○	○	△

表２　Android携帯に証拠保全ガイドラインを表示する アプリケーション開発環境

言語	Java 1．6．0_21
SDK	Android SDK 1．6
開発OS	Windows Vista Business

表３　ガイドライン作成サポートツール開発環境

言語	C#
SDK	．net Framework3．5 SP1
開発OS	Windows Vista Business

4.2 Android 携帯に証拠保全ガイドライン表示アプリケーション

証拠保全ガイドライン内容を事前に閲覧せず，その場に応じた最適な作業を行うことが出来るよう，作業しやすい画面の検討を行った．その結果次のような2つの画面を繰り返し利用することで実現できると考えた．

① 状況を容易に入力させるための選択画面（図３左参照）

② 状況に応じ，作業を支持するとともに，その作業が終了したかどうかをチェックする機能を持つ画面（図３右参照）

また，証拠保全作業者が作業中，不正を行っていないという証拠を残したいといった要望がある．そこで2つの機能を付け加えることにより作業者が不正を行えないようにした．以下に2つの機能を示す．

I. カメラ機能

証拠保全作業中にガイドライン上で証拠保全作業物をカメラで撮ってもらうよう指示を行う．カメラ機能のAndroid画面を図４に示す． こうすることで，証拠提出時に写真データを提出してもらうことで，証拠保全作業を行った機器の証拠が確保される．

II. GPS機能

証拠保全作業中にGPS機能を使い位置データを取得する．こうすることで，証拠提出時に位置データを提出してもらうことで，実際に現場で証拠保全作業を行った証拠が確保される．

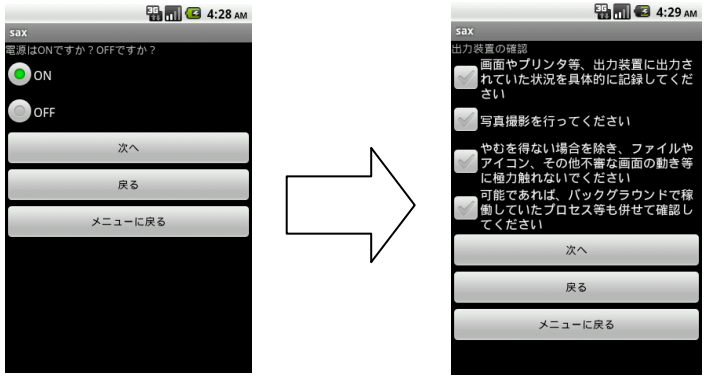

図３　証拠保全ガイドライン内容を表示した Android 画面

4.3 ガイドライン作成サポートツール

表４にガイドライン作成に適しているツールについて検討を行った．ガイドラインは質問に対し回答があり，また質問対し回答があるという構造からツリー構造になっていると言える．そのことからマインドマップを使うことでガイドラインの作成・編集作業が容易に行え，また視覚的に表現されることで作業の流れがわかりやすく抜けがなく議論を行いやすいと考えられる[5].

しかし，ガイドラインをマインドマップで作成しただけでは自動的にAndroid画面を構築できない．その理由として，ガイドラインをAndroid画面に表示するには３つの画面が必要になるからである．その必要な画面は以下の３つのである．

➢分岐画面

図３の左の画面である．この画面は質問文に対し，１つの回答を選択する画面である．これはラジオボタンで表現すこととした．

➢ 条件画面

図３の右の画面である．この画面は質問文に対し，すべての回答に対し選択する画面である．これはチェックボックスで表現することとした．

➢ メニュー画面

アプリケーション起動時の始めの画面である．

これらの画面情報を入力できないマインドマップでは自動的にガイドラインを

Android画面に表示することはできない．そこで，画面情報が入力できるマインドマップを基にしたアプリケーション開発を行った．

図４にアプリケーションのメイン画面を示し，表にそれぞれのボタンについて説明する．アプリケーションに表示される手順にしたがいガイドラインを作成する．まず，プロジェクトの作成ボタンもしくはガイドライン読み込みボタンを押す．次にメニュー作成，ツリービュー作成，プレビュー，Android サーバにアップするといった手順でガイドラインを作成していく．手順に従い作成していくことで，抜けのないガイドラインを作成することができる．

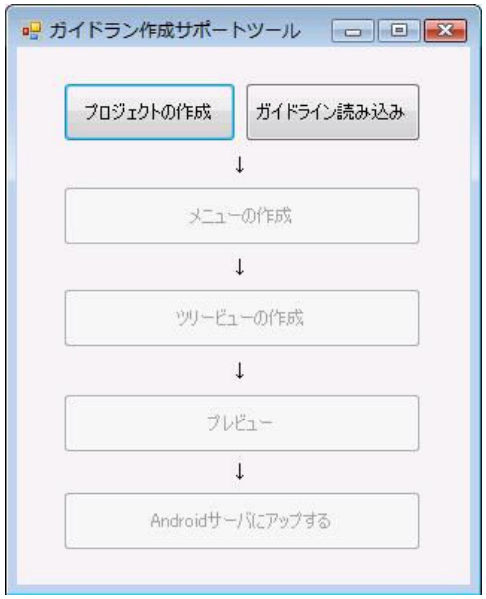

図４　ガイドライン作成サポートツールメイン画面

表４　ガイドライン作成サポートツールメイン画面のボタンの説明

ボタン	説明
プロジェクトの作成	ガイドラインのプロジェクトの名前を入力し，保存先を指定する．
ガイドラインの読み込み	以前にガイドライン作成サポートツールで作成したプロジェクトがある場合，読み込むことができる
メニューの作成	作成するガイドラインのメニュー内容を入力する
ツリービューの作成	ガイドラインの詳細を作成する
プレビュー	作成したガイドラインが Android 画面でどのように表示されるのか，簡単なデモ画面が表示される（現在実装中）
Android サーバにアップする	作成したガイドラインを Android Store にアップする（現在実装中）

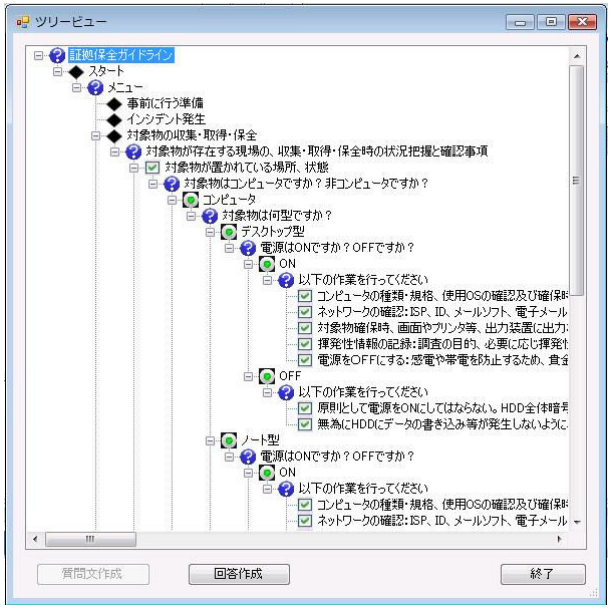

図５　ツリービュー画面

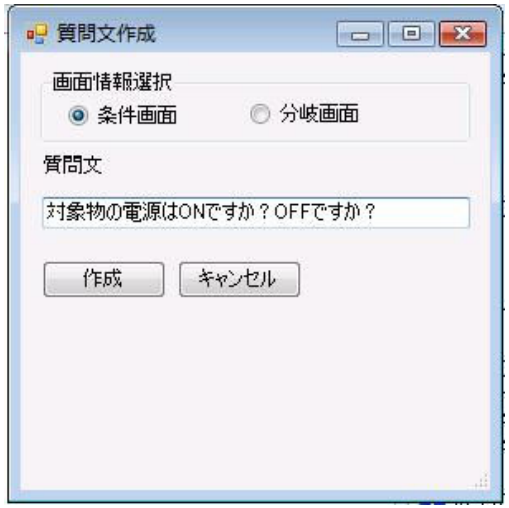

図６　質問分作成画面

図７　回答作成画面

ノードの作成・削除・編集，ノードの入れ替えといった基本的なマインドマップの機能を実現している．また，質問文の下には解答を入力できないよう，解答ノードが選択されている場合，解答作成ボタンは選択できず，質問文作成ボタンが選択できるようになっている．解答の入力は以上の逆である．こうすることで，ガイドライン作成の入力ミスをなくすことが出来るようになっている．さらに，質問文ノードの左側にクエスチョンマークのアイコンを表示し，また，解答の左側には選択した画面情報のアイコン（例えば，条件画面が選択された場合，チェックボタンアイコン）が表示される．こうすることで視覚的にわかりやすく，ガイドライン作成をサポートし，議論を行いやすいものとなっている．ガイドライン作成サポートツールの使い方について説明する．

質問文を作成する場合

解答ノードの選択し，画面下の質問文作成ボタンを押す．そうすると，図６の質問文入力画面が表示される．そこで，画面情報と質問文を入力し，作成ボタンを選択すると，選択した解答ノードの下に質問文ノードが作成される．

解答を作成する場合

質問文の作成と同様，質問文ノードを選択し，画面下の解答作成ボタンを押す．そうすると，図７の解答作成画面が表示される．そこで，解答を入力し，作成ボタンを選択すると，選択した質問文の下に解答ノードが作成される．

ノードの削除をする場合

削除したいノードを選択し，右クリックを押す．するとコンテキストメニューが表示され，削除を選択すると選択したノードが削除される．

ノードの編集をする場合

編集したいノードを選択し，右クリックを押す． するとコンテキストメニューが表示され，編集を選択すると編集画面が表示され，編集が可能となる．

作成したガイドラインを保存する場合

ツリービュー画面右下の終了ボタンを押すと，指定した保存先のファイルにXML形式ガイドランが保存される．

作成されたガイドラインを読み込む場合

メイン画面のガイドライン読み込みボタンから読み込むガイドラインを選択することで読み込むことができる．

ガイドライン作成サポートツールで出力されるXML形式のガイドラインを図８に示す．また，表５にタグの属性について説明する．

これにより，議論をしやすく，抜けがないガイドラインを作成でき，また Android 画面を構築する上での情報を入力できるようになっていると考えている．

```
<?xml version="1．0" encoding="UTF-8"?>

<root no="1" key="対象物の電源は ON ですか？OFF ですか？" type="質問文" pattern="ラジオボタン" nextno="0" />
  <item no="1" key="ON" type="解答" pattern="" nextno="3">
    <item no="2" key="以下の作業を行っていください" type="質問文" pattern="ラジオボタン" nextno="100">
      <item no="2" key="電源を OFF にしてはならない" type="解答" pattern="" nextno="100" />

                                  ・
                                  ・
                                  ・

    </item>
  </item>
  <item no="1" key="OFF" type="解答" pattern="" nextno="3">
    <item no="3" key="以下の作業を行ってください" type="質問文" pattern="ラジオボタン" nextno="100">
      <item no="3" key="周りの人をよぶ" type="解答" pattern="null" nextno="100" />
    </item>
  </item>
</root>
```

図８　XML 形式ガイドライン

表５　タグの属性

属性	説明
No	画面番号を表す
Key	画面に表示する文字を表す
Type	質問文，解答のいずれかが示される
Pattern	ラジオボタン，チェックボックス，メニューのいずれかが示される
Nextno	遷移番号を表す

4.4　XML 形式ガイドラインを読み込み画面

ガイドライン作成サポートツールで出力されるXML形式ガイドラインを読みこみAndroid画面を構築する手順について説明していく．図９に例からAndroid画面の構築について説明する．

１つのタグが１つのノードとなっている．まず，タグのnoは画面の番号になっている．質問フィールドにtypeが質問文タグのkeyを表示し，解答フィールドにtypeが解答タグのkeyを表示する．次へボタンが押されたら，選択された解答のnextnoを読み込み，読み込んだ画面番号の画面を表示する．

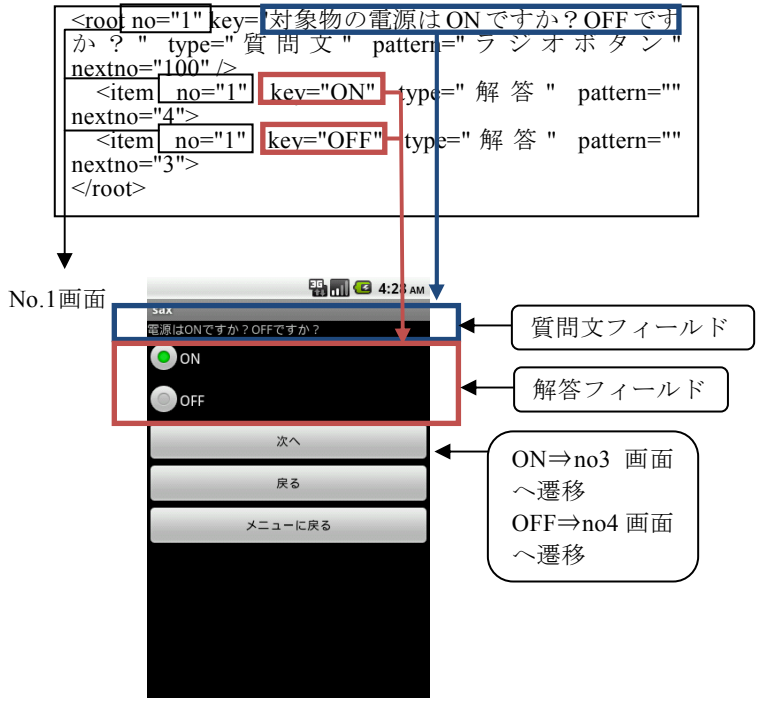

図９　XML 形式ガイドラインから Android 画面構築の流れ

5　おわりに

本稿では，デジタルフォレンジック研究会が作成した証拠保全ガイドラインの問題点を解決するため，Android携帯アプリケーション開発とガイドライン作成を支援するガイドライン作成サポートツールの2つのアプリケーション開発を行った．Androidアプリケーションは証拠保全作業者の作業効率と作業ミスをなくすため，使いやすい画面の検討を行い，Android画面構築の開発を行った．また，ガイドライン作成サポートツールは編集・作成のしにくさを解決するため，マインドマップを基にしたガイドライン作成ツールを作成することで視覚的に作業の流れがわかりやすくなると検討し，開発を行った．これらのアプリケーションを統合的に使うことにより，証拠保全作業，またガイドライン編集作業を容易に行えるようになると考えられる．

今後の課題として，これらのアプリケーションが本当に使いやすいものであるのか一般の方々に使っていただき評価する必要がある．具体的には，Androidアプリケーションは表示の仕方が正しく使いやすいものとなっているのか，またガイドライン作成サポートツールは本当にガイドラインを作成しやすいか，また議論を行いながら作成できるのかなど実験を行い評価する予定である．

参考文献

1) 佐々木良一：ディジタルフォレンジックの最新動向，電子情報通信学会誌 Vol.91, No.8, pp.744-745 (2008).
2) 稲場太郎，田原慎也，川口信隆，塩澤秀和，重野寛，岡田謙一：デジタルフォレンジックのためのワーム感染経路特定手法，情報処理学会論文誌　Vol.80，No.3, pp.1002-1011 (2009).
3) 中山佑輝，稲場太郎，芝口誠仁，岡田謙一：機密データの伝搬経路可視化手法(セッション安全/アイデンティティ)，情報処理学会研究報告. GN, [グループウェアとネットワークサービス] 2009(3), pp.31-36, (2009).
4) デジタルフォレンジック研究会理事（「技術」分科会主査）上原哲太郎：証拠保全ガイドライン　第一般，2010 年 4 月 5 日公開，http://www.digitalforensic.jp/eximgs/100405gijutsu.pdf
5) デジタルフォレンジック調査　サンプルマインドマップ，http://www.ji2.co.jp/forensics/map/index.html
6) 河村美嗣，土屋隆，浅見可津志，5B-1 UML を入力とするソースコード自動生成ツールの試作(プログラム設計支援,一般セッション,ソフトウェア科学・工学)，全国大会講演論文集　第 71 回平成 21 年(1), pp.279-280, (2009).
7) 渡邉圭輔，天沼敏幸，浅見可津志，今村誠，岡田康裕：D-13-1 表形式UIモデル記述からのWeb画面プログラム自動生成方式(D-13. 知能ソフトウェア工学,一般セッション)，電子情報通信学会総合大会講演論文集 2008年_情報・システム(2), pp.265, (2008).