「マルチメディア，分散，協調とモバイル
(DICOMO2014) シンポジウム」 平成26年7月

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

江口雅人[†1]　岡田泰輔[†2]　佐々木良一[†3]

近年，スマートフォンやタブレット型端末が普及しており，スマートデバイスからの情報漏洩に関する話題も多い．企業においても業務にスマートデバイスを導入する事例が増えてきた．これに伴い，スマートデバイス内に秘密情報や個人情報を保存するようになり，そうした情報を守る手段が必要となった．

主に廃棄時や盗難・紛失に情報漏洩が発生するため，現在では，情報漏洩防止策が用意されており，これらを導入することで情報漏洩を防止できるとされている．しかし，情報漏洩防止策は本当に安全であるのかを検証した研究は行われていない．そこで，著者らは既存手法を施した端末に復元ツールを用いて攻撃する実験を行うことで，情報保護の安全性検証を行った．その結果，暗号をかけていたとしても削除したはずの平文ファイルから容易にデータを復元できてしまうことを明確にするとともに，その対応策を示した．

Evaluation of security for information leakage preservation in Android smart device

MASATO EGUCHI[†1]　TAISUKE OKADA[†2]　RYOICHI SASAKI[†3]

1. はじめに

近年，スマートフォンやタブレット端末（以下，スマートデバイス）の普及に伴い，企業や組織でもそれらを業務に利用する事例が増加傾向にある．スマートデバイスを導入する事でペーパーレス化や業務効率の向上が期待される反面，スマートデバイス内に顧客情報等の秘密情報を保持するリスクも持ち合わせている．スマートデバイスの特徴として持ち運びが容易である反面，紛失・盗難の危険性が高いことが挙げられる．実際，スマートデバイスを業務に導入している，もしくは検討している企業を調査したところ，端末の紛失・盗難を懸念する企業は約 75%いることが判明している[1]．つまり，情報漏洩防止策においては PC 以上のものが求められる[2].

日本では，2005年4月1日に個人情報保護法が施行され，企業における個人情報保護は法律上の義務となった．

最近では，情報漏洩への危機意識も高まり，スマートデバイスからの情報漏洩に関する話題も多い．例えば，独立行政機関情報処理推進機構は 2013 年 4 月 26 日に「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル」を公開した[3].

企業にとって情報漏洩事故は企業イメージの低下や信用の損失に繋がるだけでなく，二次被害の発生も起こりうる．企業がスマートデバイスを導入する場合は，扱う情報や脅威を考慮し，情報漏洩防止策を導入する必要がある．

スマートデバイスでの情報漏洩に関連する資料やセキュリティ関連，業務へのスマートデバイス利用関連等の論文・記事は既に何件か存在する[4][5][6][7][8]．しかし，実験によって消去データの復元を行うことで，情報漏洩防止策の安全性検証を行った研究はない．

そこで，本研究ではスマートデバイスにおける情報漏洩防止策に焦点を当て，その防止策が本当に安全であるかを評価するために実験を行った．具体的には，2 章で説明する既存防止策を施した端末に対し，復元ツールを用いてデータを復元する実験を行った，そして，その結果を元に対象とした情報漏洩防止策の安全性を評価した．なお，本研究は Android OS のスマートデバイスを対象としている．

2. 既存対策手法

本章では 3 章で説明する実験 1･2 の対象となる情報漏洩防止策について説明する．各防止策がどのタイミングで使用できるか，また何ができるかを簡潔にまとめたものを表 1 に表す．各防止策の詳細は 2.1 章～2.3 章で説明する．

実験 1･2 を行い，ファイル暗号化ではデータが平文のまま残っていないか，リモートワイプとデータ抹消ではデータが復元できないかどうかを確かめる．

表 1　実験対象の情報漏洩防止策

Table 1　Information leakage prevention of experimental subject.

	データの不可視化	データの消去
インシデント発生時に使用		リモートワイプ
事前に使用	ファイル暗号化	データ抹消

†1 東京電機大学大学院
†2 東京電機大学（現在，ニフティ株式会社）
†3 東京電機大学

2.1 リモートワイプ

リモートワイプとは，スマートデバイスを Web コンソール上から操作し，端末内のデータを消去することができる機能である．これを使用するためには，予め端末にリモートワイプ機能を持ったアプリケーションをインストールし，アカウントを設定する必要がある．これにより，スマートデバイスの紛失などのインシデント発生時に遠隔地から秘密情報の削除が可能となる．

ただし，Web コンソールから送られた命令は幾つかのサーバを介して端末に送られるため，端末の電源が入っており，尚且つネットワークに接続可能状態でなければならない．また，リモートワイプ実行後は，端末が工場出荷前の状態になるので，リモートワイプに付随する位置情報の特定やアラームを鳴らす等の機能も実行不可能になる．

2.2 ファイル暗号化

ファイル暗号化とは，アプリケーションで実装可能な機能である．暗号化はファイル単位で実行され，SD メモリなどの外部ストレージにも有効である．そのため，暗号化したファイルを第三者が閲覧することはできない．

2.3 データ抹消

通常のデータ削除（端末上での主動作での削除）では，ファイル領域を開放するだけであり実データは消えない．データ抹消（以下，抹消）とはファイルが存在していた領域を乱数等の別データで上書きすることで復元を困難とする機能である．

3. 情報漏洩防止策の安全性検証実験

3.1 実験 1 概要

情報漏洩防止策を施した端末に復元ツールを用いてデータの取得を試みることで，情報保護の安全性の検証を行う．これは所有者が秘密情報の入った端末の盗難に気づき，直ちに情報漏洩防止策を実行したという状況の下，犯人が復元ツールを用いて情報の搾取を試みるという事を想定した．前提条件として端末には予め情報漏洩防止策を導入済みであるとする．

使用するデータは Word・Excel・PPT・PDF・JPG の 5 種類，容量 100KB・500KB・1MB の計 15 個のファイルを用意した．実験に用いたツールを表 2 に示す．Recuva と DiskDigger には復元でディスク内を検索する際に詳細に検索する機能がある．利用した端末の情報を表 3 に示す．

実験 1 の手順を図 1 に示す．「②事前準備」では端末内と SD メモリへのデータの保存，アプリのインストールなどの処理である．「③・⑤フォレンジックツールで解析」とはツールで他のファイルが無いか確認することである．「④対策の実行」でリモートワイプ，ファイル暗号化，抹消を実行する．

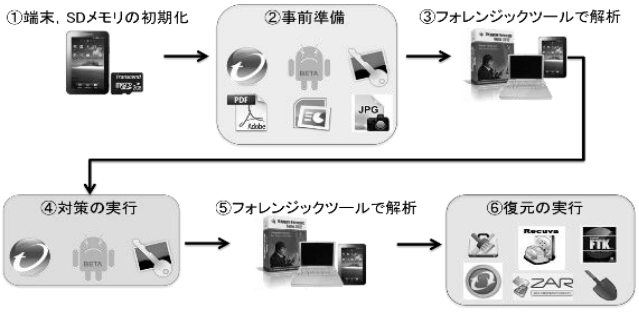

図 1　実験手順

Figure 1　Experimental procedure.

表 2　実験で使用したツール

Table 2　Tools used in the experiments.

復元ツール	Recuva Glary Utilities DiskDigger
スマートデバイス用フォレンジックツール	Oxygen Forensic Suite 2013

表3　端末情報

Table 3　Terminal information.

	OSバージョン	外部ストレージ	外部ストレージ容量
端末A	Android 2.3.5	あり	1.86GB
端末B	Android 4.0.4	あり	29.71GB

3.2 実験 1 結果

リモートワイプの端末 A・データ容量 100KB の場合の復元結果を図 2 に示す．また，端末 A・データ容量 500KB の場合の復元結果を図 3 に，データ容量 1MB の場合の復元結果を図 4 に示す．図 2 と図 4 を比較すると，ファイルサイズの大きい方が，復元率が高いことが分かる．端末 B の方では全ての容量のデータが完全に復元できた．

Recuva と DiskDigger で復元でき，Glary Utilities で復元ができなかった理由は，3.1 章で説明した詳細検索機能の有無によるものだと考えられる．また，100KB のデータ復元率が悪い理由だが，フラッシュメモリの性質に関係があると考えられる．データが存在していた領域を書き換えるためにはデータを消去してから書き込みを行う必要がある．100KB のデータだと存在していた領域が小さく，すぐに他のデータ（一時ファイル等）で上書きされてしまうため，復元率が悪くなる可能性が考えられる．

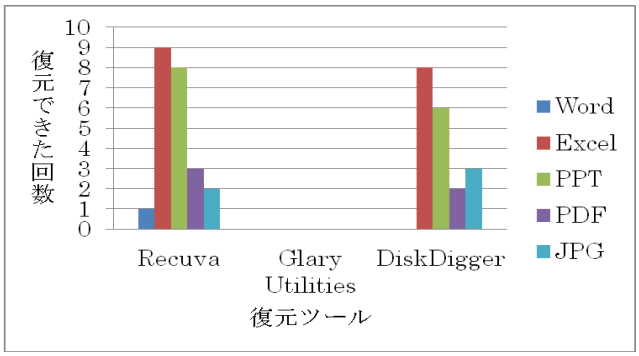

図 2 リモートワイプの復元結果（端末 A，100KB）

Figure 2 Restoring the results of remote wipe.(TerminalA, 100KB)

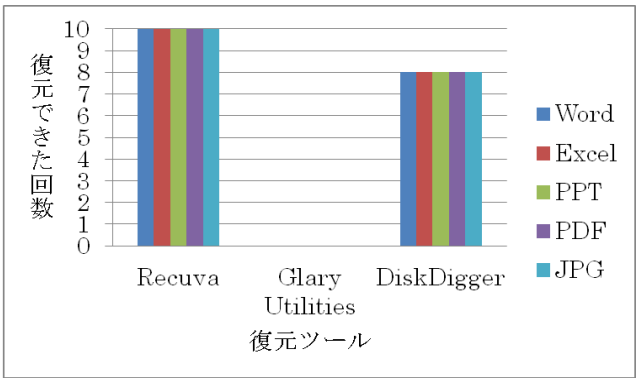

図 3 リモートワイプの復元結果（端末 A，500KB）

Figure 3 Restoring the results of remote wipe.(TerminalA, 500KB)

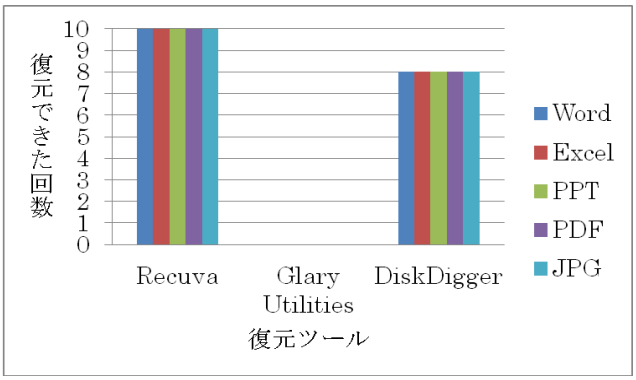

図 4 リモートワイプの復元結果（端末 A，1MB）

Figure 4 Restoring the results of remote wipe.(TerminalA, 1MB)

ファイル暗号化の端末 A・データ容量 100KB の場合の復元結果を図 5 に示す．端末 A での他のファイルサイズ，および端末 B でも同様の結果となり，ファイル暗号化では端末 A・B 共に全ての元ファイル（平文）が完全に復元できてしまった．今回使用した暗号化アプリは暗号化ファイルを作成する時に元ファイルを削除する機能があるが，元ファイルを完全に抹消することができなかったため，容易に暗号化前の元データを復元できてしまったと推測される．

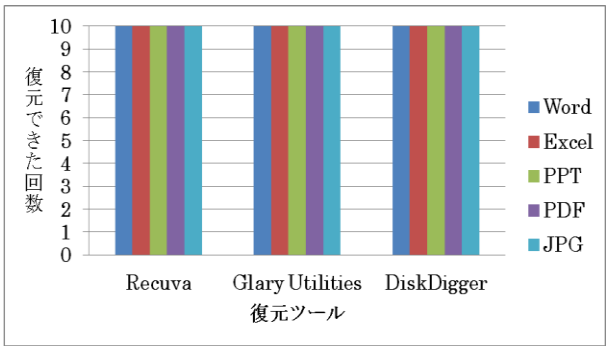

図 5 ファイル暗号化の復元結果（端末 A，100KB）

Figure 5 Restoring the results of file encryption.(TerminalA, 100KB)

ファイル暗号化とリモートワイプを組み合わせた実験も行った．端末 A・データ容量 100KB の場合の復元結果を図 6 に示す．また，端末 A・データ容量 500KB の場合の復元結果を図 7 に，データ容量 1MB の場合の復元結果を図 8 に示す．端末 B の方では全ての容量のデータが完全に復元できた．

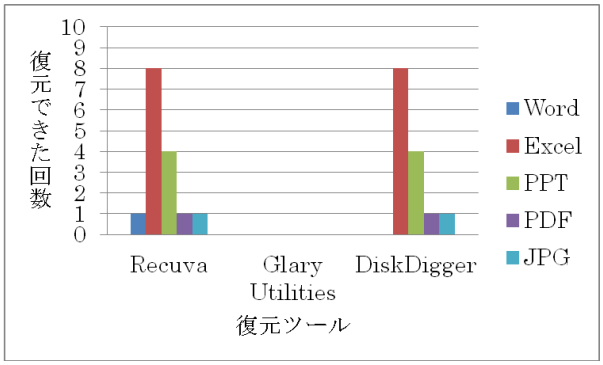

図6 リモートワイプ+ファイル暗号化の復元結果（端末 A，100KB）

Figure 6 Restoring the results of remote wipe and file encryption.(TerminalA, 100KB)

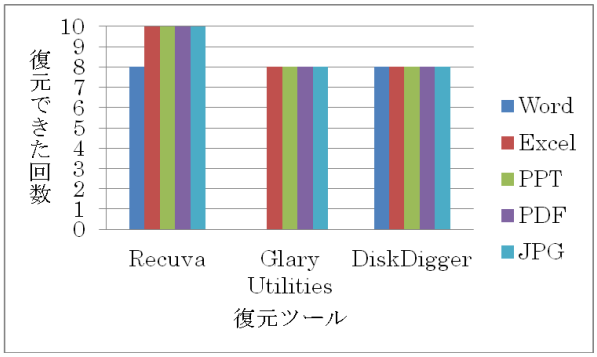

図7 リモートワイプ+ファイル暗号化の復元結果（端末 A，500KB）

Figure 7 Restoring the results of remote wipe and file encryption.(TerminalA, 500KB)

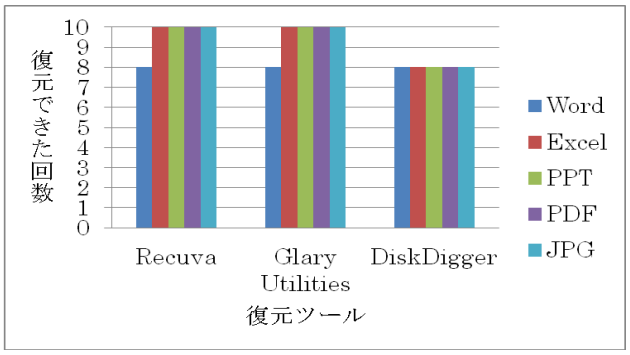

図8　リモートワイプ+ファイル暗号化の復元結果（端末 A，1MB）

Figure 8　Restoring the results of remote wipe and file encryption.(TerminalA, 1MB)

リモートワイプ単体とほぼ同じ結果となったが，500KB・1MBのデータがGlary Utilitiesでも復元できた点がリモートワイプ単体での復元結果と異なった．これも暗号化アプリの仕様による原因であると推測される．

最後に抹消の実験を行ったが，端末 A・B 共にデータが全く復元できなかった．図 9 に結果を示す．

図 9　抹消の復元結果

Figure 9　Restoring the results of erasure.

3.3　実験 2 概要

実験1ではデータを削除してからすぐに復元することで，復元の容易さを調べた. 実験2では削除後に時間を経過させた後に復元を試みることで，どの程度時間が経過してもデータが残ってしまうか調査する. 実験環境は実験1と同様である．復元を行う時間は，削除してから3・6・12・24・48時間後の6通り設定した．

これは端末のバッテリー稼働時間を考慮したためである．実験結果になるべく影響を与えないために，データ削除から復元までの間，端末は基本的に放置する．

対象とする防止策手法はリモートワイプとファイル暗号化とする．

3.4　実験 2 結果

リモートワイプ後の端末Aでの復元結果を図10～図12に，端末Bでの復元結果を図13～図14に示す．図中の「△」は復元できたデータの一部に破損がある場合を表している．

端末 A では端末 A では復元ツール Glary Utilities では削除直後から復元できなかったが，その他の復元ツールでの復元にて，データが 48 時間後も最低 3 回残った．端末 B ではデータが 48 時間後も最低 4 回残った．

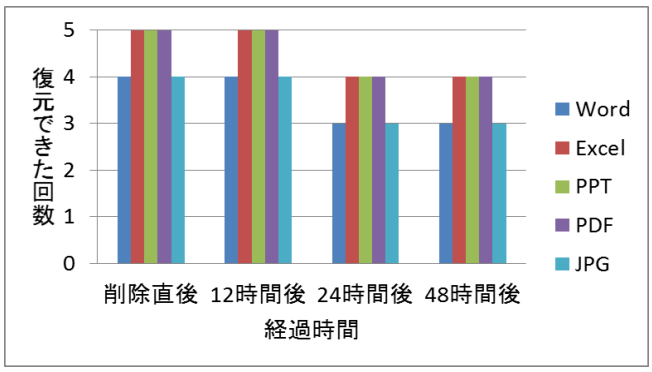

図10　リモートワイプの復元結果（端末A，100KB）

Figure 10　Restoring the results of remote wipe.(TerminalA, 100KB)

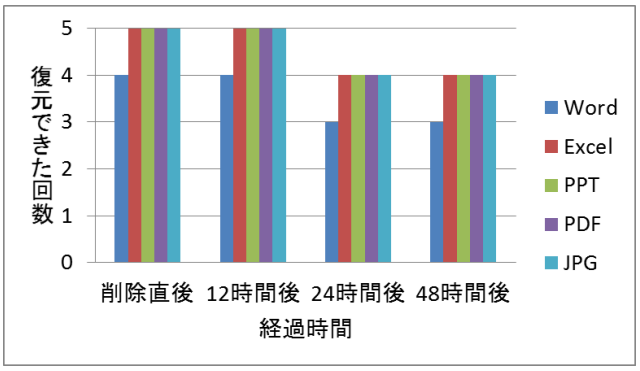

図11　リモートワイプの復元結果（端末A，500KB）

Figure 11　Restoring the results of remote wipe.(TerminalA, 500KB)

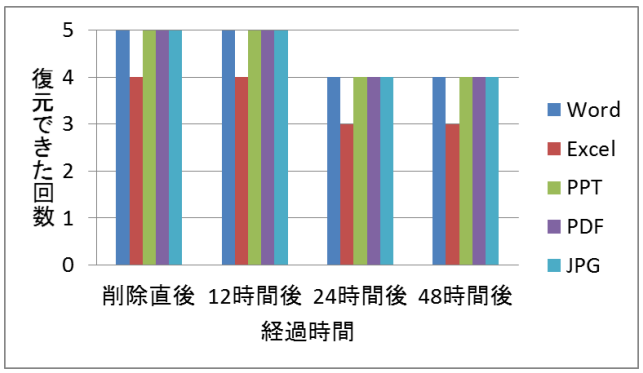

図12　リモートワイプの復元結果（端末A，1MB）

Figure 12　Restoring the results of remote wipe.(TerminalA, 1MB)

図 10～図 12 より，リモートワイプでデータを削除したとしても，48 時間でもデータが残存しており，復元できてしまう可能性が高いことがわかった．

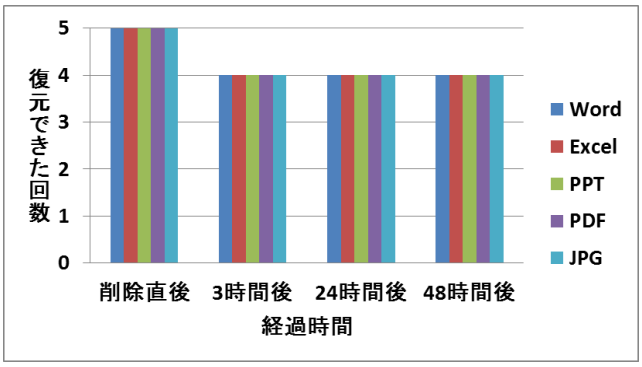

図13　リモートワイプの復元結果（端末B，500KB）
Figure 13　Restoring the results of remote wipe.(TerminalB, 500KB)

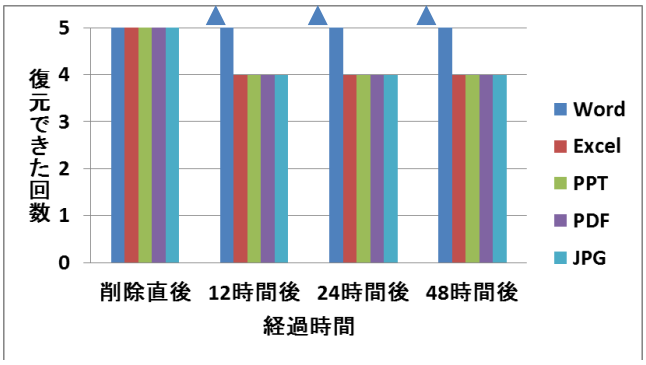

図14　リモートワイプの復元結果（端末B，1MB）
Figure 14　Restoring the results of remote wipe.(TerminalB, 1MB)

図 13～図 14 より，端末 B でもリモートワイプでデータを削除した後でもデータを復元できる可能性が高いことが分かった．なお，端末 B の方で，100KB のデータは 48 時間経過後も全て 5 回残った．

ファイル暗号化後の端末 A での復元結果を図 15～図 16 に，端末 B での復元結果を図 17～図 19 に示す．

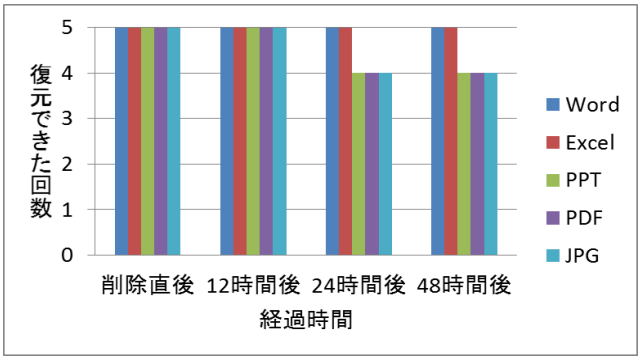

図15　ファイル暗号化の復元結果（端末A，100KB）
Figure 15　Restoring the results of file encryption.(TerminalA, 100KB)

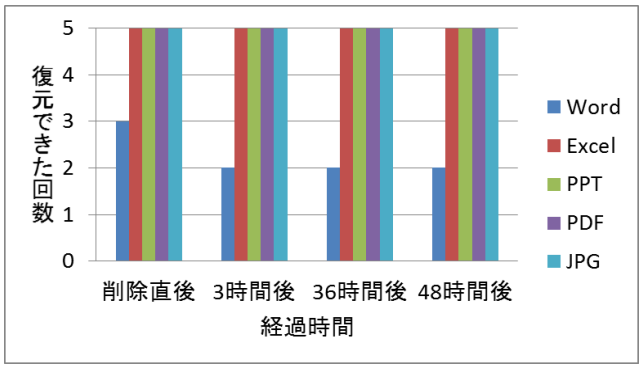

図16　ファイル暗号化の復元結果（端末A，500KB）
Figure 16　Restoring the results of file encryption.(TerminalA, 500KB)

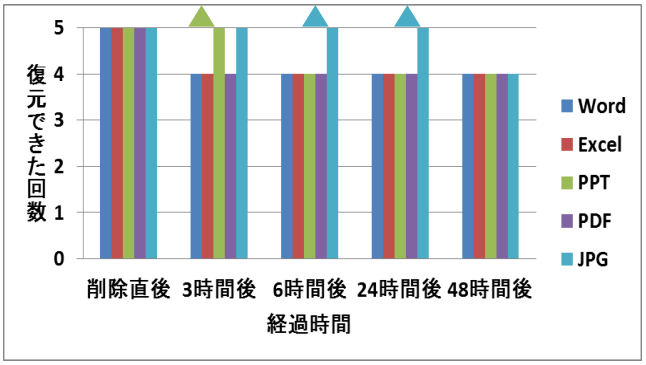

図17　ファイル暗号化の復元結果（端末B，100KB）
Figure 17　Restoring the results of file encryption.(TerminalB, 100KB)

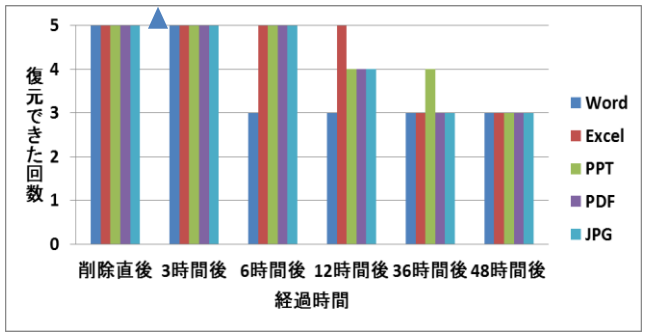

図18　ファイル暗号化の復元結果（端末B，500KB）
Figure 18　Restoring the results of file encryption.(TerminalB, 500KB)

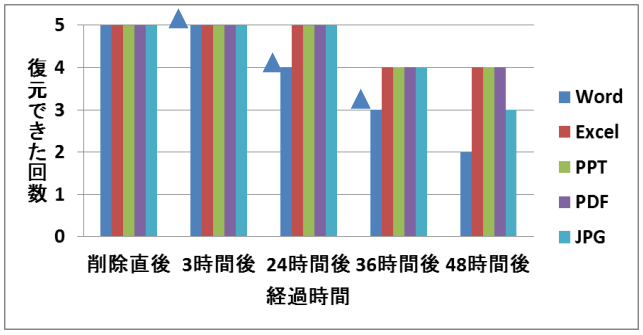

図19　ファイル暗号化の復元結果（端末B，1MB）
Figure 19　Restoring the results of file encryption.(TerminalB, 1MB)

図 15～図 19 より，ファイル暗号化を行った後でも高確率でデータが復元できてしまうことがわかった．なお，端

末 A の方で 1MB のデータは 48 時間経過後も全て 5 回残った．

ファイル暗号化とリモートワイプを組み合わせた実験も行った．端末 A で 500KB のデータの復元結果を図 20 に示す．

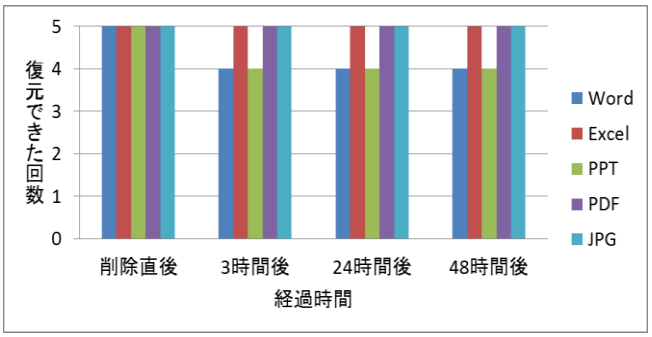

図20　ファイル暗号化+リモートワイプの復元結果（端末A，500KB）

Figure 20　Restoring the results of remote wipe and file encryption.(TerminalA, 500KB)

端末 A では復元ツール Glary Utilities では削除直後から復元できなかったが，その他の復元ツールでの復元にて 48 時間後も 8 割データが残った．なお，端末 A の方で 100KB と 1MB のデータは 48 時間経過後も全て 5 回残った．端末 B では 3 種類の容量の全データが 48 時間経過後も全て 5 回残った（1MB のデータに一部破損があった場合を含む）．

4. 情報漏洩防止策の安全性評価

実験 1・2 を踏まえて，秘密情報の入った端末に情報漏洩防止策を施すことで技術を持った（復元ツールを所持しており，それが使用できる）者から，データ復元による情報漏洩が防げるかという点から評価を行う．

実験 1 の結果より，以下のようなことが分かった．

(1)暗号をかけていたとしても削除したはずの平文ファイルから容易にデータを復元できてしまう．ファイル暗号化はアプリの実装次第で安全性が低下すると言える．

(2) リモートワイプはデータ容量が小さい場合はある程度安全性を保証できるが，通信可能状態でないと使用できない欠点がある．また，単純な消去では復元されてしまい，それを防ぐには上書き抹消が必要となる．

また，実験 2 の結果より，抹消以外のどの防止策手法でも 48 時間以内ではデータが残ってしまう可能性があることを確認した．

当研究室の別の研究より，PC ではデータが 24 時間経過するとデータが復元できなくなることが判明している[9]．スマートデバイスは PC と比較してデータが残りやすいことも判明した．従って，抹消が最も安全性の高い防止策であると言える．

5. おわりに

本研究では，2 種類の実験でスマートデバイスに対する既存の情報漏洩防止策の安全性を検証した．結果として，先行研究で安全性が高いと思われていた，ファイル暗号化+リモートワイプでも復元できる可能性があることを発見した．

この結果，抹消が最も安全性が高い防止策であると判断できる．しかし，抹消には 2 点課題点がある．

1 点目は，PC ソフトウェアの機能としては既に存在するが，スマートデバイス上では抹消を行うことができない点である．

2 点目は，データが復元できなくなるため，抹消はデータや端末の廃棄時以外で運用することが難しい点である．

このため，暗号化ファイル作成時の元ファイルの処理に抹消を用いることで，運用性と安全性の高い防止策として効果を発揮できると考えられる．

今後は，上記のことが Android スマートデバイス上で行えるアプリケーションの開発を行っていきたい．

参考文献

1) TechTargetジャパン：企業のスマートデバイス利用に関するアンケート調査，TechTargetジャパン（オンライン），入手先 <http://techtarget.itmedia.co.jp/tt/news/1106/29/news03.html>（参照2014-04-30）

2) 吉田　晋：スマートデバイスの業務利用におけるセキュリティ対策，pp66-95，ソフトバンククリエイティブ（2012）

3) 独立行政法人　情報処理推進機構：情報漏えいを防ぐためのモバイルデバイス等設定マニュアル，独立行政法人　情報処理推進機構（オンライン），入手先 <https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html>（参照 2014-04-30）

4) 奥田　健嗣，中務　亮，山内　利宏：Android における情報伝搬の追跡と漏洩防止手法の提案：電子情報通信学会技術研究報告（ICSS），Vol.111，No.495，pp5-10（2012）

5) 遠藤　英幸：スマートフォンの業務利用に関する留意点，ユニシス技報，Vol.31，No.110，pp93-101（2011）

6) 栗原　優樹，市原　尚久：マルチユーザ利用を考慮したスマートデバイス向けデータ保護方式の提案，情報処理学会研究報告（CESC），Vol.60，No.58，pp1-6（2013）

7) 竹森　敬祐，磯原　隆将，窪田　歩，高野　智秋：Android 携帯電話上での情報漏洩検知，暗号と情報セキュリティシンポジウム（2011.1）

8) 石黒　司：情報漏えいを防ぎ高速な暗号処理が可能なクラウド向け暗号方式を開発―安全な暗号処理分担技術によって，スマートフォンでも利用可能に―，電子情報通信学会誌，Vol.96，No.4，pp286-287（2013）

9) 林　健，佐々木　良一：時間経過に着目した HDD のデータ復元に関する実験と解析，研究報告マルチメディア通信と分散処理（DPS），Vol.154，No.14，　pp1-6（2013）．