APPENDIX-2
スマートフォン・タブレット型端末のデータ消去

はじめに

スマートフォン/タブレット型端末のデータ消去に関しては、業界団体である「リユースモバイル ジャパン（RMJ）http://rm-j.jp/」内の、リユースモバイル関連ガイドライン検討会が、2019 年 3 月 8 日に発表した「リユースモバイルガイドライン初版（http://rm-j.jp/pdf/RMJ_Guidelines.pdf）」内の「利用者情報の消去について」で、国内法である個人情報保護法に基づいた要求事項等を公表しており、その中で今後の方向として

EU における GDPR（General Data Protection Regulation：一般データ保護規則）の施行等、個人情報の保護に関しては、世界的にも関心が高まっている。また、米国では、国防総省や国立標準技術研究所が、情報機器の処分・消去に関して基準を設けている。ガイドラインは、将来的にそのような国際情勢や国際基準も勘案して行くべきである。

と、記載されています。

本 APPENDIX は、このような状況下で、米国の国立標準技術研究所（NIST）が発表している、情報機器の情報漏えい防止対策の基準である文書 SP800-88Rev.1 を基に、消去技術認証基準委員会が検討を行い策定した、「スマートフォン/タブレット型端末（iOS 及び Android）の情報漏えいの予防を目的とするデータ抹消のためのガイドライン」です。

本 APPENDIX で用いる「抹消」とは、データ消去技術ガイドライン第 5 章と同様に、情報を消し去り、何もない状態にする「消去」だけではなく、暗号化等で内容を判別・復旧することが不可能にする行為全般を指します。

iOS 端末（iPhone / iPad）

１．データ抹消のランクと方式（NIST SP800-88Rev.1）

Apple 社製の iPhone 及び iPad においては、ハードウェア暗号化が動作するように初期状態で設定されているため、端末上の機能を利用したオールリセット（全ての設定の初期化）を行うことで、端末を使用するうえで書き込まれた情報の暗号化消去によるデータ抹消が完了します。

※暗号化消去についての詳細は、データ消去技術ガイドライン第 2.2.1 版、
第 5 章 記憶媒体のデータ抹消（NIST SP800-88Rev.1）
４．Cryptographic Erase（暗号化消去：CE）を参照してください。

１）「Clear(消去)」、「Purge(除去)」

本体上で、設定>一般>リセット>「すべてのコンテンツと設定を消去」を実行する。

２）「Destroy(破壊)」

焼却炉で機器を焼いて細断、解砕、粉砕、または焼却する。

注意：データ抹消操作の後、マニュアル操作にて、端末の複数の領域（ブラウザの履歴、ファイル、写真など）に移動して、操作が間違いなく実行され、情報が保持されていないことを確認してください。

Android 端末

１．データ抹消のランクと方式（NIST SP800-88Rev.1）

Android 端末は、機器の製造元とキャリアによる機器の仕様に依存します。そのため、工場出荷時データリセットオプションによって得ることのできる消去のレベルは、特定の機器の設計や、記憶媒体の基本的なファームウェアなどの詳細設計に依存し、iOS 端末と同様に暗号化消去機能が有効なものも存在しますが、有効な方法を一律に規定することは困難です。

１）「Clear(消去)」、

米国で販売されている Android 4.4.2 を搭載している Samsung Galaxy S5 では、工場出荷状態に戻すためのコマンドが用意されているので、設定＞ユーザーとバックアップ＞バックアップとリセット＞工場出荷時に戻す、を実行します。 他のバージョンの Android および他の機器については、製造・販売元の発行するユーザーマニュアルを参照してください。

２）「Purge(除去)」

「パージ（除去）」に工場出荷時のデータリセットを利用しようとするデバイスであれば、機器に使用されている記憶媒体の eMMC Secure Erase または Secure Trim コマンド、またはその他の同等の記憶媒体に対して直接動作するコマンドによる消去方法が使用されていることが必要です。

３）「Destroy(破壊)」

認可された焼却炉でデバイスを焼却して、細断、粉砕、粉砕、または焼却します。

２．ADEC の推奨するデータ抹消方法（Clear）

Android 端末に対するデータ抹消について、NIST では製造元やキャリアに各端末の詳細な仕様について確認し、最も有効なデータ抹消の方法を選択することを求めていますが、NIST が対象としている米国の官公庁においては、情報の所有者・管理者である個別の官公庁が、NIST の指導に従って選択した手段を用いることが最適であると言えるのであろうが、それと同等の作業を、日本国内の民間企業における標準的なデータ抹消の方法と規定することには無理があるので、ADEC では Android 端末に使用されている記憶媒体が

eMMC であるため、同様の機能を持ち、同様に NAND 型フラッシュメモリーを使用している MMC や SSD に対応するデータ抹消手法を採用することが適当であると考えます。

※eMMC とは、embedded MMC の略で、MMC のコンポーネントを BGA パッケージに入れ、電子回路基板に直接実装して用いるものです。

1）「Clear(消去)」、（NIST SP800-88Rev1. による MMC に対する記述）
組織的に承認され、その有効性が確認されている上書き技術/方法/ツールを使って媒体を複数回上書きする。

注意：データ抹消操作の後、マニュアル操作にて、端末の複数の領域（ブラウザの履歴、ファイル、写真など）に移動して、操作が間違いなく実行され、情報が保持されていないことを確認してください。

※この方法（複数回の上書き）は、ADEC における SSD を対象としたデータ抹消ソフトウェアの消去動作検証を目的とした検体の作成時に、LBA の付与されていない余剰領域（オーバプロビジョニング）上に消去検証用のダミーデータを書き込む際に用いることでも有効性が確認されています。それにも関わらず Purge として認めない理由は、スマートフォンやタブレット型機器の場合、上書きの対象が eMMC 全体であるか、一部に留まっているかについては、データ抹消の対象となる機器の仕様に依存していることによります。

3．スマートフォン/タブレット型端末に関する注意点
1）NFC（Near Field Communication）および FeliCa などによる近距離通信や非接触型 IC カード機能は国内特有の物であり、NIST SP800-88 にデータ抹消の規定は存在しません。また、これら機能を付加する目的で、機器の内部に専用のメモリーIC を搭載している例が多く、消去ソフトウェア等を利用してデータの抹消を行うことが困難であるため、端末の所有者が事前にその機能の消去（初期化）を実行していることを確認することが必要です。

2）「LINE」に代表されるクラウド上にデータを保存する Web アプリのデータの抹消は、端末本体上に残されるキャッシュを除いて、端末本体を利用したデータの抹消は不可能であることの理解を得ることが必要です。

2019 年 7 月
ADEC（データ適正消去実行証明協議会）
消去技術認証基準委員会