Ecstra-APPENDIX-2
パブリッククラウド（データセンター）の暗号化消去を有効とする、システム認証の検証方法

はじめに

本 APPENDIX は、PC に搭載されている記憶媒体のデータ消去を対象に、消去技術認証基準委員会が作成した「データ消去技術ガイドブック」に、パブリッククラウドサービス等を利用した場合のデータ抹消手段として最も有効である「暗号化消去」の成立を保証するために必要な、システム構成の認証を目的とする検証方法を追補するためのものです。

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。

１．NIST SP800-88 上の取り扱い

ADEC が基準として取り扱っている NIST SP800-88Rev.1 では、暗号化消去を成立させるための条件として、

1）．媒体に保存する前に、対象となるすべてのデータ（データ及び仮想化されたコピーを含む）が暗号化されている場合。

2）．暗号化鍵が保存されている媒体上の場所がわかり、当該鍵が保存されている媒体上の実際の場所に対処することが保証され、適切な媒体固有のデータ抹消処理技術を使用してそれらの領域のデータ抹消処理が実行できる場合。

3）．対象データの暗号化に使用された暗号化鍵のすべてのコピーについてデータ抹消処理が行われたことを確認できる場合。

の 3 点を挙げ、また暗号化及び暗号化消去を行うに当たっては FIPS 140 の認証を受けた手段を用いることを推奨し、これらの条件を満たす状況による暗号化消去が成立した場合のデータ消去のレベルは、最先端の技術を持つ研究所によっても、情報の断片すら検出することの出来ない「Purge（除去）」レベルであるとしています。

２．暗号化消去が有効なシステム構成に求められる要件

日本に於ける暗号化/暗号化消去に関連する記載の存在する、ISMAP（Information system Security Management and Assessment Program：政府情報システムのためのセキュリティ評価制度）の管理基準に於いても、上記に準じて以下の点を求めています。

1）．対象となる情報（データ）が媒体への書き込み以前に全て暗号化されていること。
・暗号アルゴリズムは「電子政府推奨暗号リスト」に記載されていること。

2）．復号に用いる鍵が、バックアップ等も含め確実に保護・抹消されること。
・暗号鍵は物理的に保護されていること。（FIPS140-2/3 認証を受けた HSM の使用）

３．暗号化消去が成立するための動作要件

クラウド上に存在する情報の暗号化消去は以下の条件により成立します。

１）．対象となるデータは、媒体に書き込まれる以前に適切なアルゴリズムにより、暗号化されていること。

２）．暗号化されたデータは、暗号鍵の削除又は鍵管理サーバ（HSM）の切断等による無効化が行われた場合、① ユーザのアクセスが不可能となること、② ユーザのアクセスが不可能な状態においても、暗号化が維持されていること。

４．検証方法

１）．前提条件

マルチクライアント（複数の独立したボリューム/ディスク（以下領域と記す）構成）で運用される RAID 構成のサーバシステムであり、下記の検体番号によって示す各作業ステップに於いてシステム動作を停止し、検体（検証対象となる電磁記憶媒体）の取得が可能であること。各検体は、指定された作業段階に於いて、RAID 上の任意番号の電磁記憶媒体を選択し、クローン媒体（物理的複製）の作成により取得、或いは未使用の電磁記憶媒体との交換により取得することとし、当該システムにリビルト（再構築）などの適切な処置を施すことにより、継続的に使用する。

２）．検証方法詳細

①．暗号化実装の確認

・検証対象電磁記憶媒体

検体１：検証対象領域の存在しない状態

検体２：検証対象領域を設定した状態（仮想サーバのフォーマット完了等）

検体３：検証対象領域に、検証用ファイルを書きこんだ状態

注１：検証は、暗号化領域と非暗号化領域に収納されているファイルのバイナリレベルでの比較により実施するため、検証対象領域数は ”2” となる。

注２：検証用ファイルは、既知のファイルヘッダ（シグネチャー）を持ち、既知のバイナリデータで構成され、RAID を構成する全ての電磁記憶媒体に対して同一・同容量の（RAID ブロック/ストライプサイズを占有する）バイナリデータを分散書込みすることが可能な容量とする。

注３：検証用ファイルの数は、RAID を構成する全ての（電磁記憶媒体）に対し、複数のファイルヘッダを同数書きこむことが可能な数量とする。

注４：当該システムが、重複排除や自己データ圧縮を含むデータ削減機能を持つ場合はこれを不動作状態とし、電磁記憶媒体上に記録されるバイナリデータに影響を与えることの無い様にしておくこと。

注：前記、注 1～4 は、①NIST SP800-88Rev.1 に定められる暗号化の検証方法として、「既知のファイルヘッダの探索」が例示されていること、②検証対象領域内に存在するファイル一覧表示（スクリーンショットも含む）の取得を可能にすること、③各検証対象のドライブを RAID 上の特定の 1 台（同一媒体番号）とせず、各作業段階に於いて任意に選択した場合においても、NIST SP800-88Rev.1 の暗号化の検証方法として例示される、部分的なサンプリング方法によるバイナリデータの比較検証を可能とすることが目的。

・検証内容：

検体 1 and/or 2 と 3 及び書き込まれた（暗号化以前の）検証用ファイルとのバイナリデータの比較・検証による暗号化の確認、及び各検体上で検証対象領域の占有する LBA 範囲の特定。

②. 暗号化消去の確認

・検証対象電磁記憶媒体

検体 3 ：検証用ファイルを書きこんだ状態

検体 4 ：暗号鍵の削除（無効化）後の状態

・検証内容：

検体 3 と検体 4 のバイナリデータ比較・検証により、暗号鍵を無効化した場合においても、各検証対象領域の占有する LBA 範囲のバイナリデータに影響は無く、データの暗号化が継続的に有効であることの検証・確認。

5．検体以外に必要な証跡

・暗号化の実行、暗号鍵消去等に係る作業ログ又はスクリーンショット等。

注：FIPS140-2/3 認証を取得した HSM おいては、暗号鍵の操作に関わる内部のデータの取得は困難であるため、検体の作成に関わる記録として当該機器のログ又はそれに代わる証跡の取得が必須となる。

・上記、各検証対象領域内に存在するファイル一覧表示（スクリーンショット等）

・検証用ファイルの書き込み後に、当該ファイルの存在を示すもの。

・暗号化消去（暗号鍵抹消等による無効化）実行後に、システム上から当該領域/ファイルへのアクセスが不能であること（論理的に存在しないこと）を示すもの。

（詳細は、APPNDIX- ：「クラウド上の論理ボリューム等に対する、暗合化消去の成立確認に必要な証跡について」を参照のこと。）

2024 年 3 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