Ecstra-APPENDIX-1
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

はじめに

本 APPENDIX は、今までの 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ライン」に、クラウドサービスを利用した場合に必要な、データ抹消の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となる証跡などの追補を行うためのものです。

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。

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事の出来ない「Purge（除去）」レベルとしています。

２．暗号化消去に求められる証跡

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。
・サービス利用開始時点から暗号化が有効になっていること。
２). 復号に用いる鍵が、バックアップ等も含め確実に保護・抹消されていること。
・暗号鍵は物理的に保護されていること。（⇒HSM の使用）

Ecstra-APPENDIX-1
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

これにより、クラウド上に存在する情報の暗号化消去を認証するために必要な証跡（Log 又はスクリーンショット）を、以下の表に示します。

	要素	対象		必須項目
1	時刻合わせ	鍵管理サーバ	Result	
		情報収納サーバ	Result	
2	暗合化対象 Volume 作成	情報収納サーバ	Request	Volume Name/ID OS Name
			Result	
3	暗合鍵生成（※１）	情報収納サーバ	Request	暗合化方式 暗号鍵 ID
			Result	
4	鍵管理サーバ（HSM）接続（※２）	鍵管理サーバ	Request	HSM 型式等情報 管理 ID 接続先情報
			Result	
5	EVENT	情報収納サーバ	Request	
			Result	
		鍵管理サーバ	Request	
			Result	
6	暗号化 Volume 削除	情報収納サーバ	Request	Volume Name/ID OS Name
			Result	
7	暗号鍵削除（※１）	情報収納サーバ	Request	暗号鍵 ID
			Result	
8	鍵管理サーバ（HSM）接続断（※２）	鍵管理サーバ	Request	HSM 型式等情報 管理 ID （接続先情報）
			Result	
9	暗号鍵抹消（※２）	鍵管理サーバ	Request	暗号鍵 ID
			Result	

※１：暗号鍵の生成/抹消が情報収納サーバで行われる場合

※２：暗号鍵の生成/抹消が鍵管理サーバ等で行われる場合には、それも含む

Ecstra-APPENDIX-1
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

注１．：本表は、事前に当該システムの構成に対する技術認証を取得している場合に、暗号化消去の実行可能な論理ボリュームを新規に生成する場合を想定したものである。

注２．：本表に示す番号（順序）は一例であり、実際のシステム構成に影響される。

注３．：各要素に於いて Request/Result の双方を要求している理由は、Result のみでは事前に実行されたことの疑義を排除することができない事例の発生を防止する事による。

2024 年 1 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