ADEC 暗号化消去システム認証 for Cloud での CSP および CSC 審査の実施手順案　Ver 1.0

2024.12.17

はじめに

本基準は，クラウドストレージ使用時のデータ消去について、「政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）」に規定されている、遵守事項 4.2.2(5)「クラウ ドサービスを利用した情報システムの更改・廃棄時の対策」を満たすためのクラウドストレージの暗号化消去の消去証明書発行を実施するための基準である。

対象組織はクラウドサービスを提供する Cloud Service Provider（CSP）とクライドサービスを利用する Cloud Service Customer（CSC）となる。

クラウドサービスの暗号化消去は情報セキュリティマネジメントシステムの一部であり、審査の実施基準の前提として、対象組織が自身の活動，サービスのマネジメントのためのシステムを，組織の方針及び各マネジメントシステム規格の要求事項に従って実施していることが前提となる。

本基準は，対象組織 CSP および CSC に対する審査の手順と要求事項（チェックリスト）を規定している。

審査活動は，申請書のレビューから審査終了までのプロセス全体を構成する個別の活動をまとめたものである。

1　適用範囲

この基準は，CSP および CSC の審査の実施手順について規定する。本審査は ADEC（データ適正消去実行証明協議会）より任命された審査員が行う。

2　引用規格

次に掲げる規格は，本基準に引用されることによって，本基準の規定の一部を構成する。これらの引用規格は，その最新版（追補を含む。）を適用する。

2.1　政府情報システムのためのセキュリティ評価制度（ISMAP）

（Information system Security Management and Assessment Program）

2.2　ISMAP 管理基準が参考にしている規格

JIS Q 27001	マネジメント基準
JIS Q 27002	セキュリティ管理策
JIS Q 27017	クラウドサービスに関わる管理策
JIS Q 27014	ガバナンス基準（目標とプロセス）
統一基準	政府機関等のサイバーセキュリティ対策のための統一基準群
NIST SP800-53	アメリカ合衆国連邦政府の情報システムおよび組織のための

3　用語及び定義

3.1　CSC(Cloud Service Customer)

クラウド暗号化消去証明書利用目的で審査を受けるクラウドサービスを利用する組織

3.2　CSP(Cloud Service Provider)

クラウド暗号化消去証明書発行目的で審査を受けるクラウドサービスを提供する組織

3.3　ADEC（Association Data Erase Certification）

データ適正消去実行証明協議会

3.4　依頼者（client）　審査を依頼する人

3.5　審査員（auditor）　ADEC が任命した審査を行う人

3.6　仕様書ヒアリング　審査員が CSP と対面等でサービス仕様を確認するヒアリング会議

3.7　予備判定　審査員が仕様書ヒアリング、チェックリスト、ログデータ等からサービス認定を判断

3.8　最終承認会議　審査員の予備判定結果から ADEC での最終承認する会議

3.9　データ保管システム　インターネット経由でデータやファイルを保存・管理できるサービス

3.10 暗号化システム　クラウドに保存するデータを暗号化して、不正アクセスや悪用から保護する技術

3.11 鍵管理システム　クラウド上で暗号化鍵の生成から消去までを一元的に管理するシステム

3.12 ログデータ　上記システムの利用状況やデータ通信などの履歴や情報が記録されたデータ

3.13 不適合（nonconformity）要求事項を満たしていないこと

3.14 重大な不適合（major nonconformity）

意図した結果を達成するシステム能力に影響を与える不適合

3.15 軽微な不適合（minor nonconformity）

意図した結果を達成するシステム能力に影響を与えない不適合

4　CSP サービス認定の手順

4.1 全体フロー

CSP の依頼により、ADEC が CSP のサービスがクラウドストレージの暗号化消去の消去証明書発行の要件を満たしているか審査する。審査の結果、不適合が発見された場合、ADEC は CSP に対して一定期間内での是正を依頼する。審査結果が適合

となった場合、ADEC は CSP のサービスを認定サービスと認定する。

4.2 認定期間

認定の有効期間は 3 年とする。

4.3 CSP サービス認定の詳細手順

4.3.1 CSP の申請書記入

CSP は ADEC の Web サイトより申請書をダウンロードし、記入後、ADEC に返却する。データオーナーや保存期間などの CSC 情報についても、CPS にて取りまとめを行い、申請書類を完成する。

申請書類一覧

・サービス認証申請書

サービス概要・サービス組織関係図・システム構成図・システム構成詳細一覧・ログデータ構成

4.3.2 ADEC による申請書の確認

ADEC は申請書を受領後、本審査の審査員を選定する。審査員は入手した申請書を確認し、審査計画書の作成、および審査工数見積りをするとともに、サービス内容に応じたチェックリストを抽出し、CSP に送付する。工数は、標準審査工数表に基づいて、申請書から差分を追加する。仕様確認ヒアリング日程は CSP と協議して決める。

使用する書類一覧

・サービス認定申請書

・チェックリスト

・審査計画書（審査工数を含む）

4.3.3 CSP のチェックリスト回答

CSP は ADEC から送付されたチェックリストを確認・回答し、ADEC に送付する。

使用する書類一覧

・チェックリスト

4.3.3 仕様確認ヒアリング

審査員は入手した申請書・チェックリストを確認し、質疑がある場合は、CSP に対してメールなどで確認を行う。事前確認後、審

査員は CSP と対面等で申請書および運用チェックリストを用いて仕様確認ヒアリングを行う。ヒアリング時には実環境での動作確認を行い、実環境でのログ入手を行う。

使用する書類一覧

・サービス認定申請書

・チェックリスト

・実環境でのログデータ

4.3.4 予備判定

審査員は仕様確認ヒアリング結果およびチェックリスト・実環境でのログデータを確認し、認証サービスの要件を満たしているが予備審査で、認証の適合判定を行い、審査報告書を作成する。不適合が発見された場合は、4.3.4.1 に移行し、適合するまで予備審査を行う。

使用する書類一覧

・審査報告書

4.3.4.1 不適合が発見された場合

審査員の予備判定で、不適合が発見された場合、審査員は指摘事項報告書を作成し、CSP に一定期間での是正を依頼する。CPS が不適合を是正した後、審査員は指摘事項報告書の是正内容を確認し、再度予備審査を行う。

使用する書類一覧

・指摘事項報告書

4.3.4.2 不適合が是正されない場合

CPS により所定期間内に不適合が是正されない場合は、審査員での予備判定は完了できない。審査員から ADEC に CSP の是正処置がされるようにエスカレーションを行い、ADEC が CSP の是正処置の支援を継続して行う。是正処置が完了した場合、審査員による予備審査が再開される。

使用する書類一覧

・指摘事項報告書

4.3.5 最終承認

審査員により CSP のサービスが認証サービスの要件を満たしていると判定されると、審査員は審査報告書および指摘事項が発見された場合は是正処置が記入された指摘事項報告書を作成し、ADEC 内での最終承認会議にこれら報告書を提出し、最

終承認会議にて最終判断を行う。最終承認会議にて判定が合格ならば、 ADEC よりサービス認定書を CSP に送付する。同時に、ADEC より審査工数に応じた費用請求を CSP に行う。

使用する書類一覧

・サービス認定申請書

・審査報告書

・サービス認定書

4.4 認定の更新

認定期間終了の 3 か月前に、CSP は ADEC に対して更新申請を行う。

4.4.1 サービスシステムに重大な変更がある場合

サービスシステムのメジャーアップデートなどサービスシステムに重大な変更がある場合、またはチェックリストが大幅に改訂された場合は、CSP は変更箇所における、サービス変更認定審査を受けなくてはならない。

4.4.2 サービスシステムに変更がない、または軽微な変更がある場合

サービスシステムに変更がない、またはマイナーバージョンアップなど軽微な変更がある場合、チェックリストにアップデートがない場合は、CSP は更新申請を行わなくてはならない。

----- End of File -----