

別添 1 更改・廃棄時のセキュリティ対策

情報システムセキュリティ責任者は、クラウドサービスを利用した情報システムの更改・廃棄にあたり、以下の各項目に従い必要なセキュリティ対策を講じること。

(1) 利用終了手順に係る対策

情報システムセキュリティ責任者は、以下を含む利用終了手順に係る対策を講じること。

イ クラウドサービスの利用終了に伴う影響を考慮した移行計画書又は終了計画書の作成

ロ 移行計画書又は終了計画書について、クラウドサービス利用者に対し十分な期間をもって事前通知すること

(2) 情報の廃棄に係る対策

情報システムセキュリティ責任者は、以下を含む情報の廃棄に係る対策を講じること。

イ 取り扱った全ての情報がクラウドサービス基盤上から確実に抹消されていることを確認すること

- ・ 暗号化消去を目的として使用した暗号鍵について、バックアップを含めて完全に抹消すること
- ・ クラウドサービス提供者に対し、契約時に合意した情報廃棄手順の実施報告書を求め、内容を確認すること

ロ 暗号化消去が実施できない場合、基盤となる物理機器について、セキュリティを確保したうえで廃棄又は再利用されるための方針及び手順が確実に実施されていることを確認すること

(3) アカウント廃棄に係る対策

情報システムセキュリティ責任者は、以下を含むアカウント廃棄に係る対策を講じること。

イ 利用に伴い作成された全てのクラウドサービス利用者アカウントを削除すること

ロ 管理者アカウントについて削除又は返却を行い、再利用されないことを確認すること

（クラウドサービス提供者への問い合わせ又は公式ドキュメント等により確

認)

ハ 利用者アカウント以外の特権アカウント（ストレージアカウント等）を削除し、当該アカウントを用いて作成された情報が廃棄されていることを確認すること

(4) クラウドサービス管理者による対応

クラウドサービス管理者は、以下の情報セキュリティ対策を実施すること。

イ クラウドサービス上で取り扱った情報の廃棄

ロ 暗号化消去が行えない場合の物理機器の適切な廃棄

ハ 利用者アカウントの削除

ニ 管理者アカウントの削除又は返却

ホ 特権アカウントの削除および関連情報の廃棄

（ドメインの移行・廃止）

ドメインの移行または廃止については、「[Web サイト等の整備及び廃止に係るドメイン管理ガイドライン](#)」に基づき、契約期間中に委託者と協議の上、適切に対応すること。

以上