クラウドサービス
セキュリティガイドライン

更新 2024 年 07 月 17 日

株式会社網屋

改訂履歴

版数	改訂内容	改訂日
1.0	新規作成	2023 年 9 月 30 日
1.1	3-2.関係当局との連絡 ・バックアップデータの所在を追記	2024 年 07 月 17 日
	4-1.クラウドサービスカスタマの資産の除去 ・データの除去に関する詳細情報を追記	
	7-2.情報のバックアップ ・バックアップに関する詳細情報を追記	
	10-1.責任及び手順 ・目標時間を追記	
	11-1.記録の保護 ・データ削除に関する記述の修正	
	11-2.暗号化機能に対する規則 ・TLS のバージョンを追記	
	7-2.情報のバックアップ ・保存期間の表現を修正(保存期間に変更なし)	

目次

はじめに

本クラウドサービスセキュリティガイドライン（以下、「本ガイドライン」といいます）は、

株式会社網屋（以下、「弊社」といいます）がお客様に提供するクラウドサービス「ALog Cloud」におけるセキュリティに関する取り組みを記述した文書であり、JIS Q 27017 (ISO/IEC27017)の規格（以下「ISO27017」といいます）に依拠して作成されたものです。

なお、本ガイドラインの内容は冒頭記載の時点での取り組みに基づくものです。内容は予告なく変更される場合があります。

1. お客様との責任分界点

「責任分界点」とはお客様と弊社のそれぞれがクラウド基盤のどこからどこまでを担当するかを定めた境界をいいます。「クラウドサービスの管理範囲」と捉えていただければと存じ上げます。

ALog Cloud は、SaaS 型のクラウドサービスです。

本ガイドラインの対象となるサービス（以下「本サービス」といいます）は、その機能によってあらゆるシステム・クラウドサービスのログデータを自動で収集・分析・保管するログマネジメントサービスであり、サイバー攻撃や内部不正の検知をはじめ、有事の際の調査、監査対応まで、マルチなシーンで活用することができるようになっています。

上記の関係性、及びお客様と弊社の管理範囲については、以下へ図示します。

1-1. ALog Cloud の責任範囲

本サービスにおけるサービス基盤部分・各種設定情報・サービスで生成されたデータの管理責任は弊社にあるものとします。また、上記に記した管理責任の詳細につきましては、下図を参照ください。
一方、本サービスの利用環境やユーザーのアクセス制御および運用ポリシーを策定および管理することは、お客様の責任範囲となります。また、Web コンソールにてお客様により操作された結果の事象につきましても、不具合を除いてはお客様の責任範囲となります。

2. 情報セキュリティのための方針群

（以下の「項番」は、本ガイドラインの項目に対応する ISO27017 の規格の項目番号を意味しています。）

2-1. 情報セキュリティのための方針群

（項番：5.1.1）

ALog Cloud では、弊社の情報セキュリティ基本方針に従い、セキュリティに関する極めて重要な事項として取り扱い、サービス運営を実施します。

詳細は、弊社のセキュリティポリシー(https://www.amiya.co.jp/corporate/security_policy.html)をご確認ください。

3. 情報セキュリティのための組織

3-1. 情報セキュリティの役割及び責任

（項番：6.1.1）

弊社は、サービスに関する約款及びサービス仕様書にて契約条件及びサービス内容を定義した上で、サービスを提供しております。

ALog Cloud は SaaS 型のクラウドサービスであり、アプリケーション、設備などサービス基盤の運用は弊社の責任範囲としてサービスの提供範囲に含まれております。

3-2.　関係当局との連絡

(項番：6.1.3)

弊社の本社所在地は、東京都中央区日本橋浜町 3-3-2 トルナーレ日本橋浜町 11F です。
なお、クラウドセキュリティサービスに関するお問い合わせ窓口はサービス仕様書に記載しております。

お客様からお預かりしたデータ(バックアップを含む)は、下記に示すクラウドプロバイダーのデータセンターに保管されます。

サービス名	データ保管場所
ALog Cloud	AWS(アジアパシフィック (東京) リージョン)

3-3 クラウドコンピューティング環境における役割及び責任の共有及び分担

(項番：CLD.6.3.1)

約款やサービス仕様書にてサービス内容を定義し、サービス提供を実施しております。
また、責任分界点の詳細は、本ガイドラインの“1. お客様との責任分界点”をご参照ください。

4. 資産の管理

4-1.　クラウドサービスカスタマの資産の除去

(項番：CLD.8.1.5)

サービス解約の際、弊社サービス設備にて保有するデータの除去に関しましては、以下の通りです。

お客様専用アカウント	・本契約終了後 30 日間は保持 （トライアル終了時は 30 日間保持せず解約） ・削除可能日から 14 日以内に解約 （利用するプラットフォームの定めにより解約後 90 日経過で完全削除）
アクセスログ/集計データ	アカウント解約時に削除
アクセスログ/集計データのバックアップ	上記データ削除から 1 日後に削除
その他お客様データ	アカウント解約時に削除
その他お客様データのバックアップ	アカウント解約から 35 日後に削除
派生データ	永年保管

5. 利用者アクセスの管理

5-1. 利用者登録及び登録削除

（項番：9.2.1）

サービス提供開始時においてはご提供いただく申請書を元に、当社にて初期登録ログインユーザーの登録を行います。また、サービス提供開始後に関しましては、お客様専用管理画面よりアカウント登録及び削除が可能です。

5-2. 利用者アクセスの提供

(項番：9.2.2)

ALog Cloud にてお客様専用管理画面が提供されます。専用管理画面にて確認できる項目は、ユーザーガイドに記載しております。

5-3. 特権的アクセス権の管理

(項番：9.2.3)

特権的アクセス権を有するアカウントへは以下の機能を提供しております。

- ログインユーザー毎の権限付与
- 多要素認証機能等のセキュリティ機能

5-4. 利用者の秘密認証情報の管理

(項番：9.2.4)

ALog Cloud を利用される際のパスワードは、メールを受信したユーザーが個別にパスワード設定を行う仕組みとなっております。

5-5. 特権的なユーティリティプログラムの使用

(項番：9.4.4)

お客様専用管理画面にて、管理メニューの使用が可能です。
これによりログインユーザーの権限管理やセキュリティ設定等を含む全ての設定が制御できます。

6. 暗号

6-1. 暗号による管理策の利用方針

(項番：10.1.1)

ALog Cloud への通信及びメール送信では暗号化プロトコルを使用しています。
また、サービス基盤内における各種データの保存に関しても暗号化を実施しております。
なお、データ暗号化における詳細は、「11-2.暗号化機能に対する規則」をご参照ください。

7. 運用セキュリティ

7-1. 変更管理

(項番：12.1.2)

弊社にて本サービスの内容を変更する場合、お客様に対して専用管理画面上及びサポートサイト、メールのいずれかにてメンテナンス日時とその影響を掲載します。また、メンテナンスの完了及び修正内容については、メンテナンス完了後にサポートサイトにて掲載を行っております。

7-2. 情報のバックアップ

(項番：12.3.1)

本サービスに何らかの問題が発生した場合の復旧を目的としたバックアップを弊社で実施しております。リストアは弊社で必要な際に行いますが、バックアップからのリストアをお客様から承ることはできません。お客様にて保存データを直接バックアップする機能は付帯していません。

アクセスログデータ バックアップ	タイミング：世代管理(変更の都度) 保持期間：1 世代目は永年保存、2 世代目は 1 日保存 リストア所要時間：1 日
その他お客様データ バックアップ	タイミング：複数回/複数世代 保持期間：35 日 リストア所要時間：1 日

7-3. クロックの同期

(項番：12.4.4)

ALog Cloud のサービス基盤間は NTP を使用し、システムのクロックを同期しています。

7-4. 技術的ぜい弱性の管理

(項番：12.6.1)

弊社では本サービスに関するシステムについて、最新のセキュリティ情報を常に収集し、ぜい弱性のチェックを行います。また、新たな脆弱性が検知された場合には、ぜい弱性への対応を行い、サポートサイトにて公開しております。

8. システムの取得、開発及び保守

8-1. 情報セキュリティ要求事項の分析及び仕様化

(項番：14.1.1)

本ガイドライン及びサービス仕様書に定めております。

8-2. セキュリティに配慮した開発のための方針

(項番：14.2.1)

外部公開サービス基準に定めております。

9. 供給関係者

9-1. 供給関係者のための情報セキュリティ方針

(項番：15.1.1)

お客様から事前にご了承をいただいている場合を除き、弊社運用担当者がお客様の情報にアクセスすることはありません。(障害対応で可及的速やかな対応が必要となる場合は、この限りではありませんが、その場合でも情報へのアクセスは最低限とするように努めます。)

9-2. 供給者との合意におけるセキュリティの取り扱い

(項番：15.1.2)

ALog Cloud は SaaS 型のクラウドサービスです。責任分界点の詳細は、本ガイドラインの“1. お客様との責任分界点”を参照ください。

10. 情報セキュリティインシンデントの管理

10-1. 責任及び手順

(項番：16.1.1)

弊社の責任範囲である契約者情報やお客様に影響のあるサービス運営上の派生データ等に関する情報セキュリティインシデントが発生した場合には、1 営業日以内にお客様専用管理画面上及び サイトへの掲載を行います。

10-2. 証拠の収集

(項番：16.1.7)

お客様責任範囲における情報セキュリティインシデントに関するログ等の証拠の収集は、お客様にて実施いただく範囲となります。弊社責任範囲でのログ等の証拠が必要な場合は、お客様の要望に応じて個別に対応しております。都度、ご相談ください。

11. 法令及び契約上の要求事項の順守

11-1. 記録の保護

(項番：18.1.3)

ログデータを含む利用者データは、不正なアクセスや改ざんを防ぐため、弊社のサービス開発及び運用チームの一部の人間しかアクセスできないよう設定されたアクセス権のもとで保管されます。また、本データは”4-1.クラウドサービスカスタマの資産の除去”の定めに従い削除します。

11-2. 暗号化機能に対する規則

(項番：18.1.5)

ALog Cloud では下記の通りの暗号化を使用しております。なお、輸出規制の対象となる暗号化の利用はありません。

- クライアント-Web サービス間の通信は HTTPS を提供しております。
- メール送信には TLS 1.2 を使用しております。
- クラウド上に保存されるデータは AES-256 を使用しております。

11-3. 情報セキュリティの独立したレビュー

(項番：18.2.1)

弊社では、お客様が大切な情報を安心してお取り扱いいただけるよう、クラウドサービス事業者として情報セキュリティ対策に積極的に取り組み、それらの情報セキュリティ活動については、定期的に内部監査によるレビューを実施しております。なお、レビュー結果情報の開示については、セキュリティ保持の観点から特定の契約条件及び法令順守等の開示要求についてのみ開示されます。

以上