

# ALog MDRサービス仕様書

第2.2版

株式会社網屋

AMIYA

# 改訂履歴

版数	更新日付	更新内容【概要】
1.0	2023/03/01	新規作成
2.0	2024/07/24	サービス名称/サービス内容の修正
2.1	2024/10/01	1.1.3.提供サービス内容の修正
2.2	2024/12/16	1.1.3.提供サービス内容の修正



# 目次

<u>0. はじめに</u>	<u>3</u>
<u>1. サービス概要</u>	<u>4</u>
<u>1.1. サービス内容</u>	<u>4</u>
<u>1.1.1. サービス名称</u>	<u>4</u>
<u>1.1.2. サービス概要</u>	<u>4</u>
<u>1.1.3. 提供サービス</u>	<u>4</u>
<u>1.1.4. サービス提供の前提条件</u>	<u>4</u>
<u>1.1.5. サポート対象</u>	<u>5</u>
<u>1.2. サービス料金</u>	<u>5</u>
<u>1.2.1. サービス体系・金額</u>	<u>5</u>
<u>1.2.2. サービス契約期間</u>	<u>5</u>
<u>1.3. サポート窓口</u>	<u>5</u>
<u>2. サービスレベル</u>	<u>6</u>
<u>2.1. サービス品質</u>	<u>6</u>
<u>2.2. サービス対応範囲</u>	<u>7</u>
別紙	
<u>対応可能システム一覧</u>	<u>9</u>

# 0.はじめに

ALog MDRサービスは、株式会社網屋（以下、当社）が提供するサービスです。

本サービス仕様書は、ALog MDRサービスを、契約者に対し提供するにあたりサービスの仕様を明示した資料です。

- ・本サービス仕様書は、本契約に基づく当社の秘密情報とします。
- ・本サービス仕様書の内容については、予告なく変更する場合があります。
- ・本書で使用される用語は、本書において特に定める場合を除き、利用規約に定める意味を有するものとします。

# 1. サービス概要

## 1.1. サービス内容

### 1.1.1. サービス名称

## ALog MDRサービス Basic/Advanced

### 1.1.2. サービス概要

ALog MDRサービス（以下、本サービス）は、ALogおよびALog Cloud（以下、ALogサービス）を当社が運用することで、セキュリティインシデントの検知/分析を代行するサービスです。

### 1.1.3. 提供サービス

<MDR Basic/Advanced 共通>

- ・ ALog 設定/チューニング
- ・ セキュリティイベント監視/分析/報告
- ・ 定期レポート（1回/月）
- ・ 定期ミーティング（1回/月）
- ・ 相談窓口（ログに関する事項）
- ・ インシデント対応（メール/電話）
  - ※ログ転送フォワーダー、お客様保有システムの設定/チューニングは除く
  - ※セキュリティイベント監視/分析/報告およびインシデント対応については、ALogが取得しているログから判明できる内容に限る
  - ※ALogマネージャーサーバ/テナントは1つとする
  - ※一法人単独での利用、環境を前提とする

<ALog MDR サービス Advanced のみ>

- ・ 脆弱性診断  
（対象範囲はインターネットエリア [公開セグメント] とし、次号の契約年度1年間あたり4回実施）  
（診断1回あたり最大5IPアドレス迄。診断ごとの対象変更可）
- ・ アタックサーフェス調査  
（次号の契約年度1年間あたり4回実施）  
（調査一回あたり1ドメイン迄対象。調査ごとの対象変更可）
- ・ インシデント初動対応アドバイス
- ・ 相談窓口（セキュリティ全般）
- ・ セキュリティ情報連携

### 1.1.4. サービス提供の前提条件

- ・ ALogサービスを契約していること
- ・ 監視対象システムのログがALogサービスで取得できていること

### 1.1.5.サポート対象

以下のログ種別をサポート対象とします。ログ種別ごとの対応可能システムは、別紙「対応可能システム一覧」をご確認ください。

<サポート対象ログ種別>

- ファイルアクセスログ
- 認証ログ
- ネットワークログ（通信ログ）
- PCログ
- メールログ
- Proxyログ
- VPNログ

## 1.2. サービス料金

### 1.2.1 サービス体系・金額

料金表に記載の通り

### 1.2.2 サービス契約期間

- 年間契約
- サービス開始日は、当社が環境設定した日の翌月 1 日
- 契約期間満了日の2か月前までに解約の意思がない場合、1年間の自動延長契約

## 1.3. サポート窓口

No.	項目	内容	備考
1	問い合わせ窓口	ALog MDR サポートセンター メール： <a href="mailto:alog-mdr@amiya.co.jp">alog-mdr@amiya.co.jp</a> 電話：03-6822-9996	サービス内容に関する事項に限る 両方で事前に取り決めた管理責任者及び運用担当者からの問い合わせに限る
2	営業日	土日祝日及び年末年始の休業期間並びに当社の指定休業日を除く営業日	
3	営業時間	9：00～17：00	

## 2. サービスレベル

### 2.1. サービス品質

	サービス項目	サービス内容	提供 サイクル	サービス品質
1	ALog 設定/チューニング	ALog 全般の設定/設定変更	都度	ベストエフォート 対応範囲：ALogサービス ※ログ転送フォワーダ、お客様保有システムは除く
2	セキュリティイベント監視/ 分析/報告 (緊急度：低)	発生したアラート/レポート (緊急度：低)の常時監視、 脅威度判定、詳細分析、報 告	都度	ベストエフォート 報告タイミング：翌月の報告会
3	セキュリティイベント監視/ 分析/報告 (緊急度：高)	発生したアラート/レポート の常時監視（緊急度：高）、 脅威度判定、詳細分析、報 告	都度	ベストエフォート 対応開始目標：1時間以内（営業時間内） 最終報告目標：4時間以内 ※営業時間外のイベントは翌営業日対応
4	インシデント対応（相談窓 口）	お客様からの問い合わせに 対し、ログの調査、分析、 報告	都度	ベストエフォート 対応開始目標：1時間以内（営業時間内） 最終報告目標：4時間以内 ※営業時間外の問い合わせは翌営業日対応
5	定期レポート	前月発生したイベントや注 意事項についての報告書を 提供	月次	報告書の書式：当社書式
6	定期ミーティング	定期レポートをベースに、 発生したインシデント等 について説明	月次	Web会議
7	脆弱性診断	インターネットに公開して いるシステムへ脆弱性診断 を実施、報告 (ALog MDR サービス Advanced のみ)	四半期に1回	報告書の書式：当社書式
8	アタックサーフェス診断	サイバー攻撃の糸口となり うるインターネットに公開 しているシステムを調査、 リスクを報告 (ALog MDR サービス Advanced のみ)	四半期に1回	報告書の書式：当社書式
9	セキュリティ相談窓口	不審なメール/事象の安全確 認やセキュリティ製品の検 討など、セキュリティ運用 に関する相談受付 (ALog MDR サービス Advanced のみ)	都度	ベストエフォート ※質問の内容によっては回答できない場合があります。

## 2.2. サービス対応範囲

- セキュリティイベント監視/分析/報告、インシデント対応、定期レポート、定期ミーティングの対応範囲は、ALog に取得しているログから判明する範囲に限ります。
- 本サービスは、インシデント被害を完全に防止することを保証するものではありません。

---

ALog MDRサービス  
サービス仕様書  
第2.2版

株式会社網屋

〒103-0007 東京都中央区日本橋浜町3-3-2トルナーレ日本橋浜町 11階

TEL : 03-6822-9999(代表) / FAX : 03-6822-9998

Copyright© AMIYA Corporation

株式会社網屋の許可無く、複製・改変などを行うことはできません

# 別紙「対応可能システム一覧」

- ファイルアクセスログ  
Windowsファイルサーバ / SharePoint / OneDrive / Box / Google ドライブ
- 認証ログ  
Active Directory / Microsoft Entra ID
- トラフィックログ  
FortiGate / Palo Alto / SonicWall
- PCログ  
SKYSEA / LANSCOPE
- メールログ  
Exchange Online / Gmail ( GoogleWorkspace )
- Proxyログ  
i-Filter
- VPNログ  
Verona / FortiGate

- Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- その他、記載されている会社名、製品名は各社の登録商標です。