AMIYA

低コストで**カンタン**に
セキュリティを自動監視

カンタンSIEM

ALog

サービス概要資料

国産SIEM※1 1位

契約数※2 6,200以上

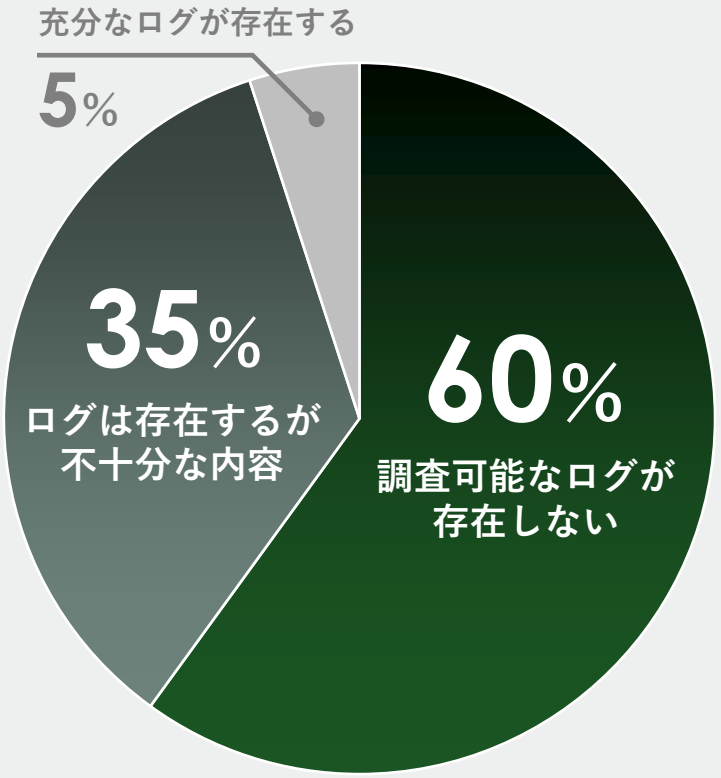
継続率※3 99%

導入業界※4 20以上

※1：セキュリティ情報イベント管理ツール出荷金額 国産メーカーとして（2023年度） https://mic-r.co.jp/mr/03370/ デロイト トーマツ ミック経済研究所 「内部脅威対策ソリューション市場の現状と将来展望 2024年度」2025年03月 発刊
※2,3,4：2025年1月時点による自社調査

ログの重要性

9割以上のお客様では、十分なログ管理ができていないため、**「攻撃された証拠」**が得られない



車なら、
ドライブレコーダー

会社なら、
会計帳簿

船なら、
航海日誌

医療なら、
カルテ

ITなら ▶▶▶ LOG ログ

引用：グローバルセキュリティエキスパート株式会社が対応する年間300件のサイバーセキュリティ被害対応相談より
【引用プレスリリース】網屋とGSXは戦略的業務提携を結び、全国約400万社の準大手・中堅・中小企業に対しログ管理ツール「ALog」の販売とセキュリティ人材の育成を強力に推進

セキュリティ強化の指針、ガイドラインでも

AMIYA

総務省

（６）ログの取得等
「①統括情報セキュリティ責任者及び情報システム管理者は、**各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存**しなければならない。」

「地方公共団体における情報セキュリティポリシーに関するガイドライン(令和４年３月版)」

経済産業省

指示５
サイバーセキュリティリスクに対応するための仕組みの構築
「**アクセスログや通信ログ等からサイバー攻撃を監視・検知する仕組み**を構築する。」

「サイバーセキュリティ経営ガイドライン Ver 2.0」

金融
金融機関等コンピュータシステムの安全対策基準・解説書

官公庁
政府機関の情報セキュリティ対策のための統一基準

水道
水道分野における情報セキュリティ確保に係るガイドライン

交通
国土交通省所管重要インフラにおける情報セキュリティ確保に係るガイドライン

重要インフラ
重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針

地方自治体
地方公共団体における情報セキュリティポリシーに関するガイドライン

中小企業
中小企業の情報セキュリティ対策ガイドライン

教育
教育情報セキュリティポリシーに関するガイドライン

SIEM製品をはじめとするツールを用いたログ管理・運用が必要不可欠

SIEM製品の課題

AMIYA

もしもの時、調査が難航

- ログは難しい
（多種多様、膨大、複雑難解）
- 求められるツール活用スキル

人材不足
活用には“専門家”が必要

- サイバー攻撃とログの関係性の理解
- 大量アラート通知から本当の異常を発見
- 情報システム部門すら足りていない

全体的にコストが膨らみがち

- 高機能かつ高額な海外製品
- 専門家は高額
- ログ以外の従量課金で費用が見えない

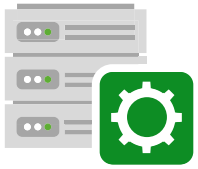
ALog

複雑でむずかしいログデータをカンタンに管理するSIEM製品。
あらゆる履歴を収集し、幅広いセキュリティ対策をひとつにして活用します。

AMIYA


ファイルサーバ


データベース


APサーバ


AD サーバ


PC


Web プロキシ


ネットワーク機器


クラウドサービス

ALog


監査対応


サイバー攻撃対策


内部不正対策


インシデント調査


利用状況の把握

ログデータ管理でNo.1

AMIYA

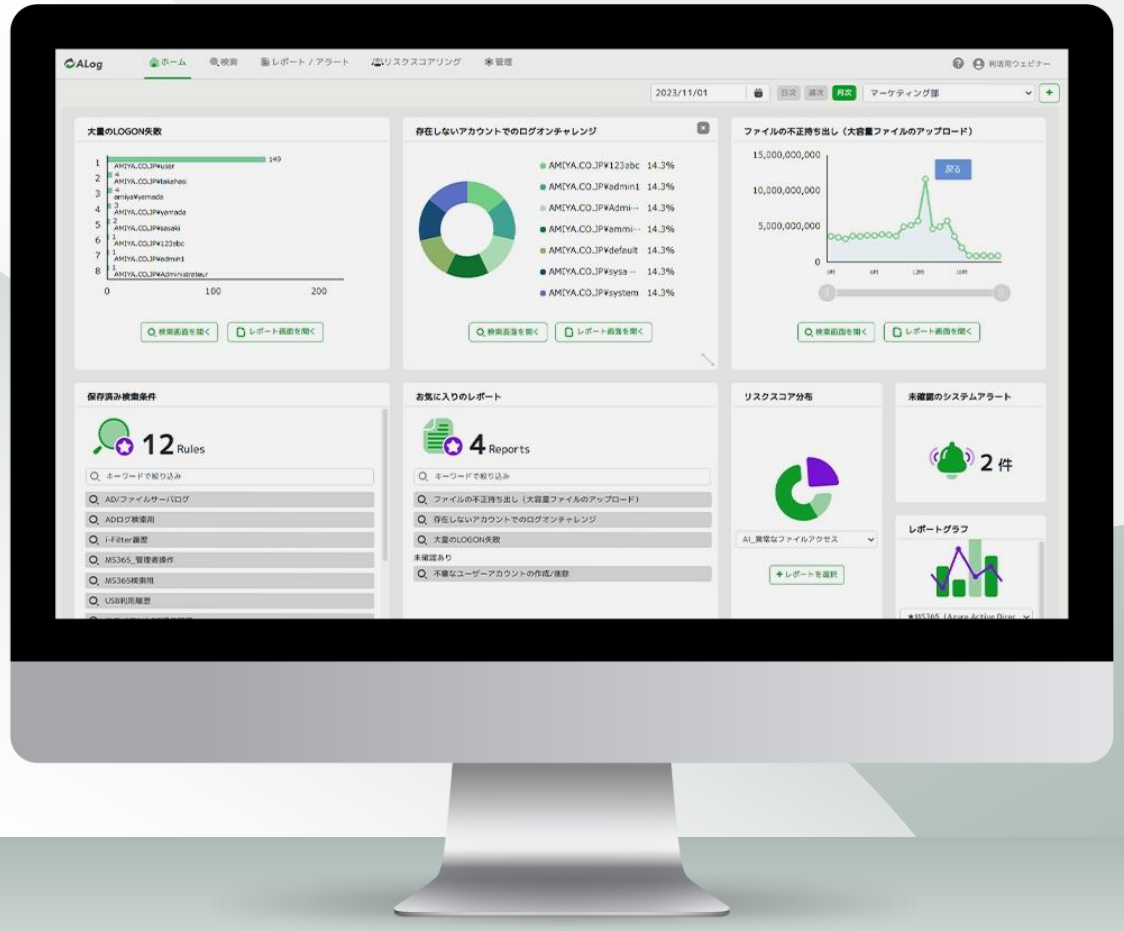
国産SIEM ※1	契約数 ※2	継続率 ※3	導入業界 ※4
1位	6,200以上	99%	20以上

※1：セキュリティ情報イベント管理ツール出荷金額 国産メーカーとして（2023年度） https://mic-r.co.jp/mr/03370/ デロイト トーマツ ミック経済研究所 「内部脅威対策ソリューション市場の現状と将来展望 2024年度」2025年03月 発刊
※2,3,4：2025年1月時点による自社調査

こんな企業様にご利用いただいています

Panasonic
NISSHINBO
NTT Communications
JTEKT
帝京平成大学
Designing The Future KDDI
トレイダーズ証券
明治安田アセットマネジメント
SBI GROUP SBI証券
SUBARU
mixi GROUP
品川区
LANDNET
SEKISUI HOUSE
LINEヤフー株式会社

SIEMのむずかしいをカンタンに



01 ノウハウ不要！
ログ分析をカンタンに

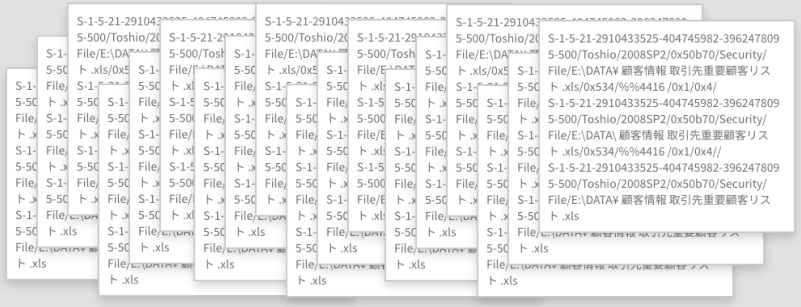
02 人材不足を解消！
専門家によるログ活用

03 国内ニーズに合った
シンプルな価格体系

ノウハウ不要でログ分析

特許取得（特許第6501159号）の翻訳変換技術で複雑なイベントログを“わかりやすく”変換してコンパクトに保管します。

複雑なログを



見やすいログに

日時	ユーザー	ファイル	操作
2024/03/29 15:44	K.Sato	\営業部\重要顧客リスト.xls	READ
2024/03/28 10:12	A.Yamada	\企画部\FY13事業計画.doc	WRITE
2024/03/25 05:08	Y.Tamachi	\経理部\給与明細_田中.xls	DELETE

システム的な内容も

正確なユーザー操作に

READ — ファイルを開いて

WRITE — 保存した

大容量のログを

※軽減率は、環境/フォルダパスの長さ/OSなどによって変化します。

元のログ 1GB

変換後 1MB

超コンパクトに

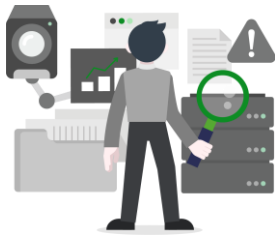
さらに圧縮 25KB

運用をもっとカンタンに、MDRという選択肢

長年、ログと向き合ってきたメーカーによるMDRサービス。
サイバー攻撃や内部不正の監視から、インシデント分析/報告/監視項目の最適化までサポートします。

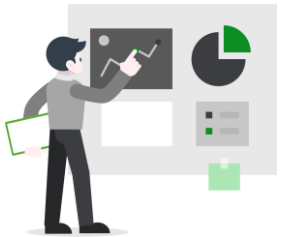
収集したさまざまな
ログデータを活用

ALog



監視

サイバー攻撃や
内部不正を監視



分析

インシデントを分析

報告

結果を
わかりやすく報告

最適化

監視項目の最適化

セキュリティスペシャリスト対応保有資格　情報システム監査人（CISA）/ 情報処理安全確保支援士

監視対象を意識しないライセンス体系

ALogはデータ量によるライセンス課金。監視対象を意識する必要がなく、スケーラブルなログ収集を実現します。

ALog

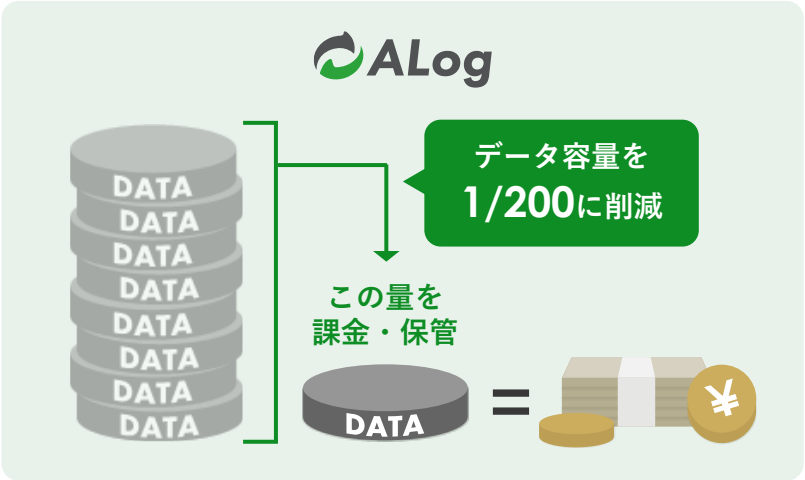
基本料金とログデータ容量のみ

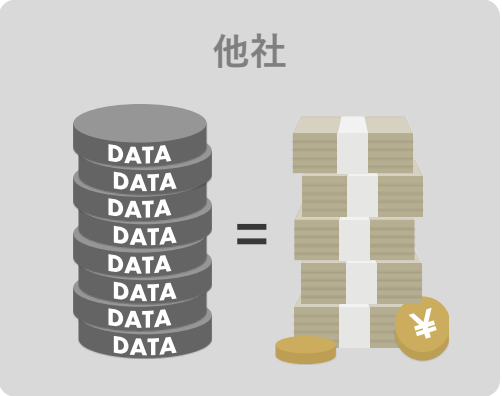
圧倒的コストパフォーマンスはココにあり！

ALogだけの“コンパクト術”

翻訳変換後のデータ容量で課金。
最大1/200*に削減したログ容量で課金するため、
コストを圧倒的に抑えられます。

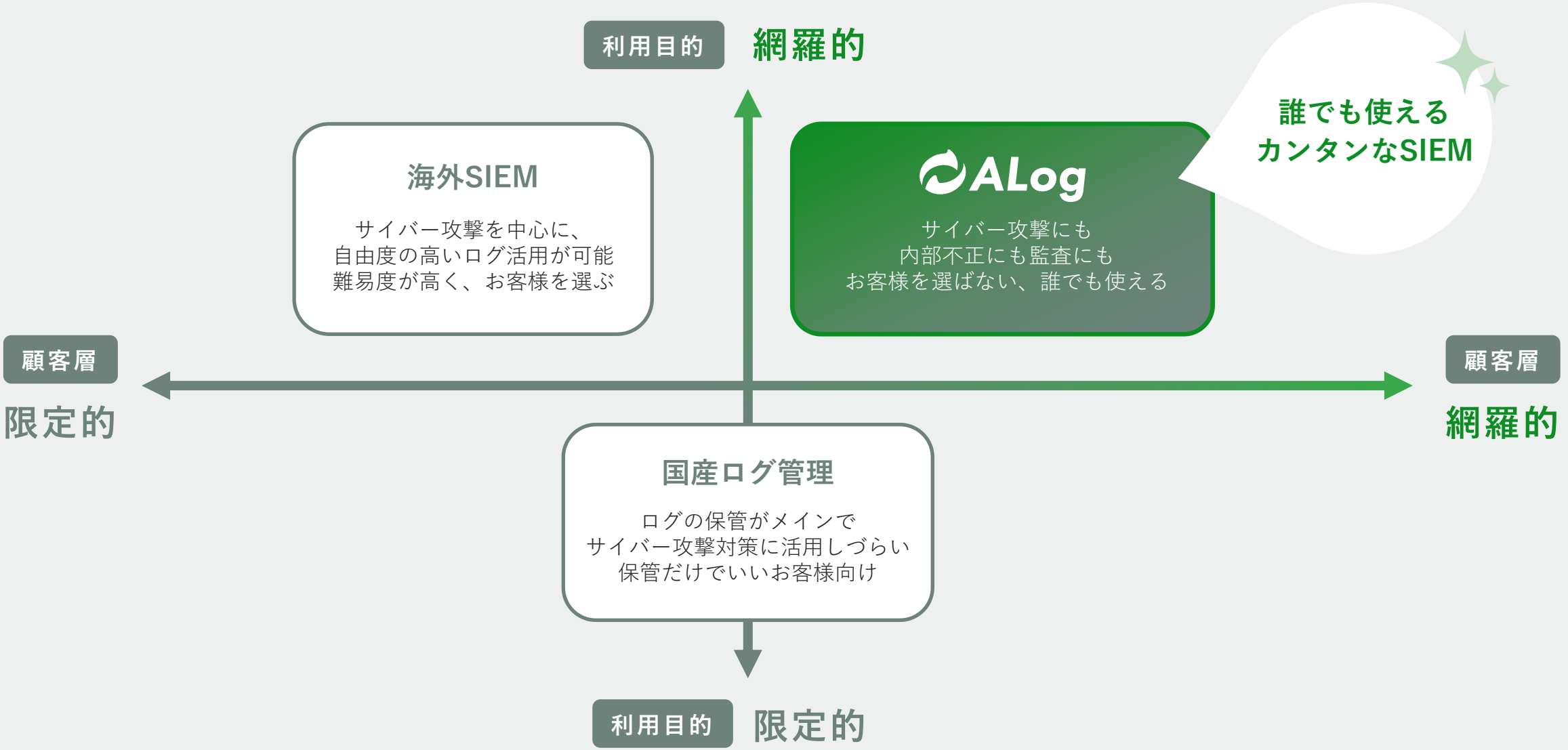
*取り込むOSやログ種別で異なります。





だから ALog

AMIYA

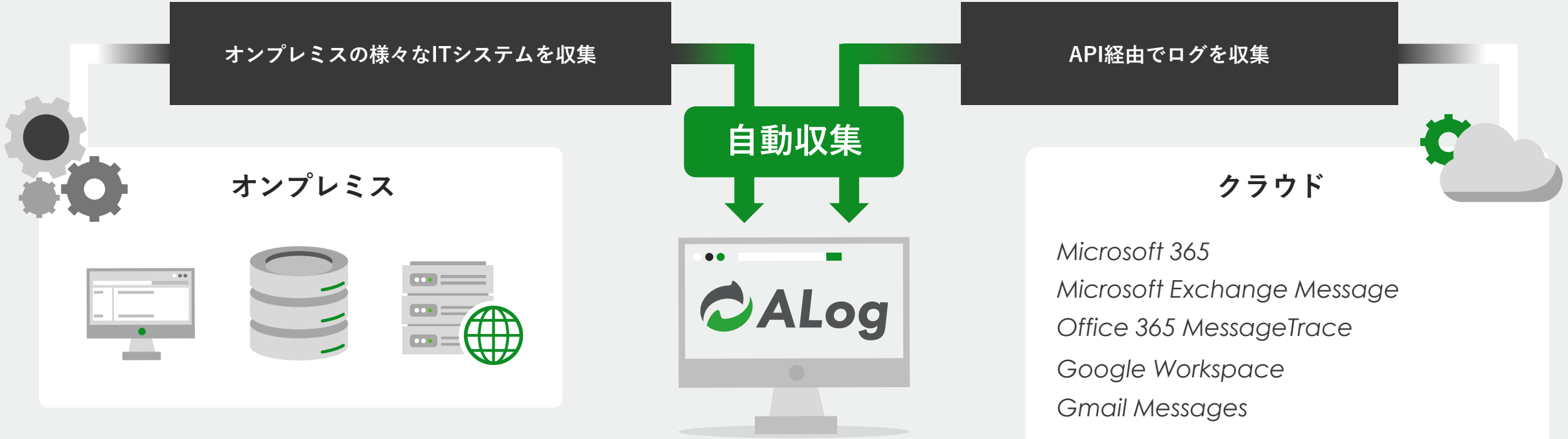


機能紹介

01	収集	オンプレもクラウドも、すぐにデータ取込み
02	アラート/レポート	最適化された監視テンプレート
03	ダッシュボード	異常に気付くダッシュボード
04	検索	Webブラウザのような検索窓
05	保管	選べるシステム構成

オンプレもクラウドも、すぐにデータ取込み

オンプレミスからクラウドまで、カンタンにログを自動収集します。
またクラウドサービスのAPI仕様が変更にあわせてアップデートするので運用もカンタンに。

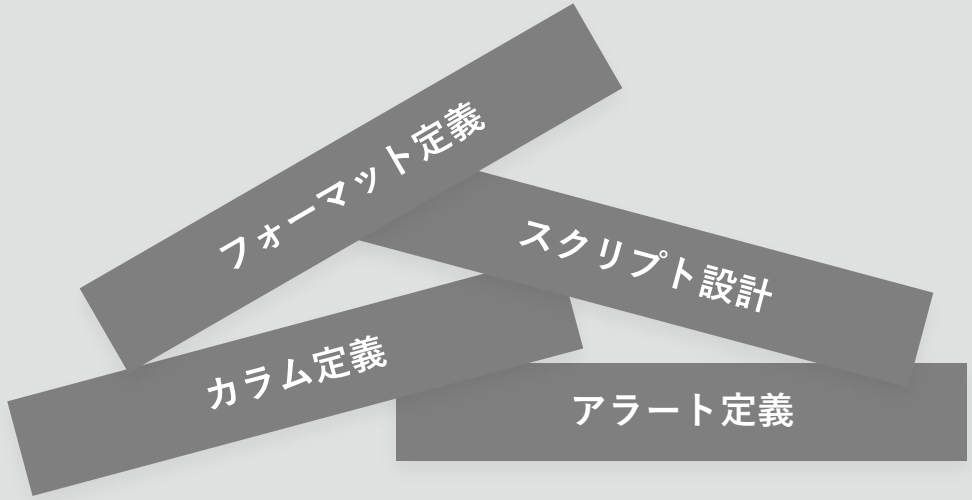


ALogクラウド版の場合は、ログ転送フォワーダーより収集

データの自動マッピングと再変換

時刻フォーマットの定義のみでログデータの取り込み設定が完了。すぐにログ管理を開始できます。
運用に応じて、フォーマットを再変換し、より詳細分析することも可能です。

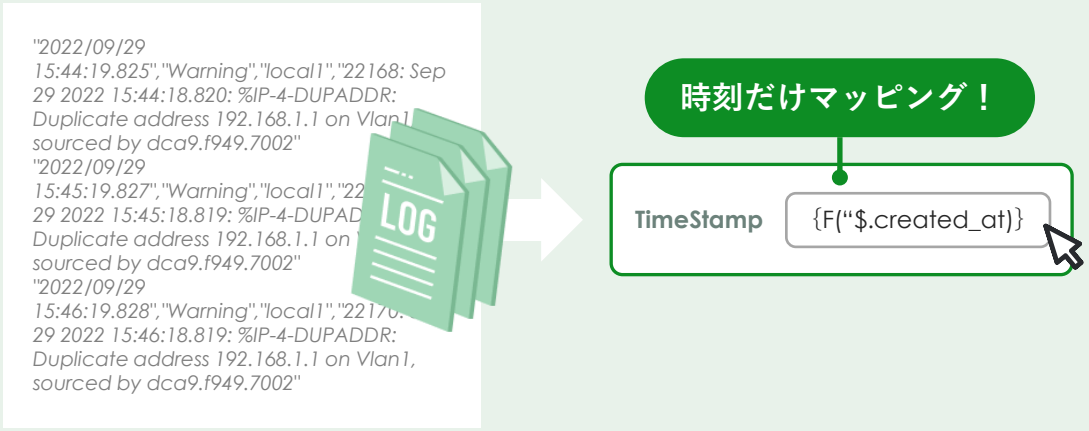
他社製品



細かな要件定義/設定が必要

後から変えにくいことが障壁に…

ALog



すぐに取り込んですぐに確認！

後から何度でもフォーマットの再変換もできる

最適化された監視テンプレート

テンプレートから選ぶだけのカンタン設定でセキュリティリスクを自動アラート/レポーティングします。
有事の際はメールやWebhookによるアラート通知、外部システムとの連携通知も。

- サイバー攻撃対策
- 内部不正対策
- クラウドサービス監視

アラート/レポートサンプル

IPAやJPCERTガイドラインに対応

- 不審なユーザアカウントの作成/削除
- 無効なアカウントによるログオンチャレンジ
- 特権ユーザのログオン
- ランサムウェアによる被害範囲の特定
- 不正アクセスの把握

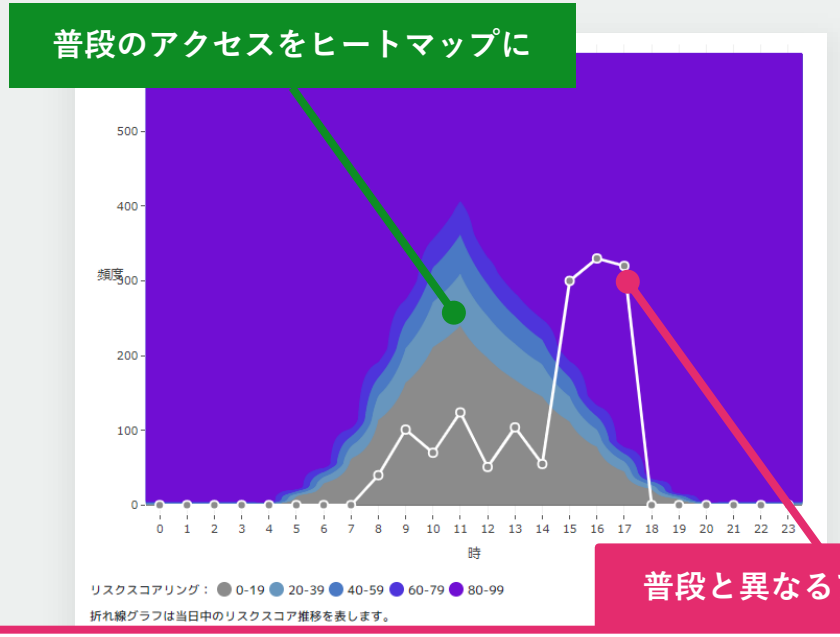
対象システム

- Windowsサーバ
- ファイルサーバ
- データベースサーバ
- Active Directory
- Firewall - UTM
  - FortiGate
- Microsoft365
  - Microsoft Entra ID
  - Exchange Online
  - SharePoint
  - OneDrive
  - Teams
- Box
- i-Filter

And more…

AIが脅威・不正を事前検知

AIによるリスクスコアリング機能でデータの特徴を自動分析。
「普段」との違いを、不正アクセスやサイバー攻撃の予兆としてリスクの度合いをスコアリングします。



いつもと違う時間のアクセス

9月

1	2	3	4	5	6	
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
				28	29	30

09:00 - 18:30

23:30 - 25:15

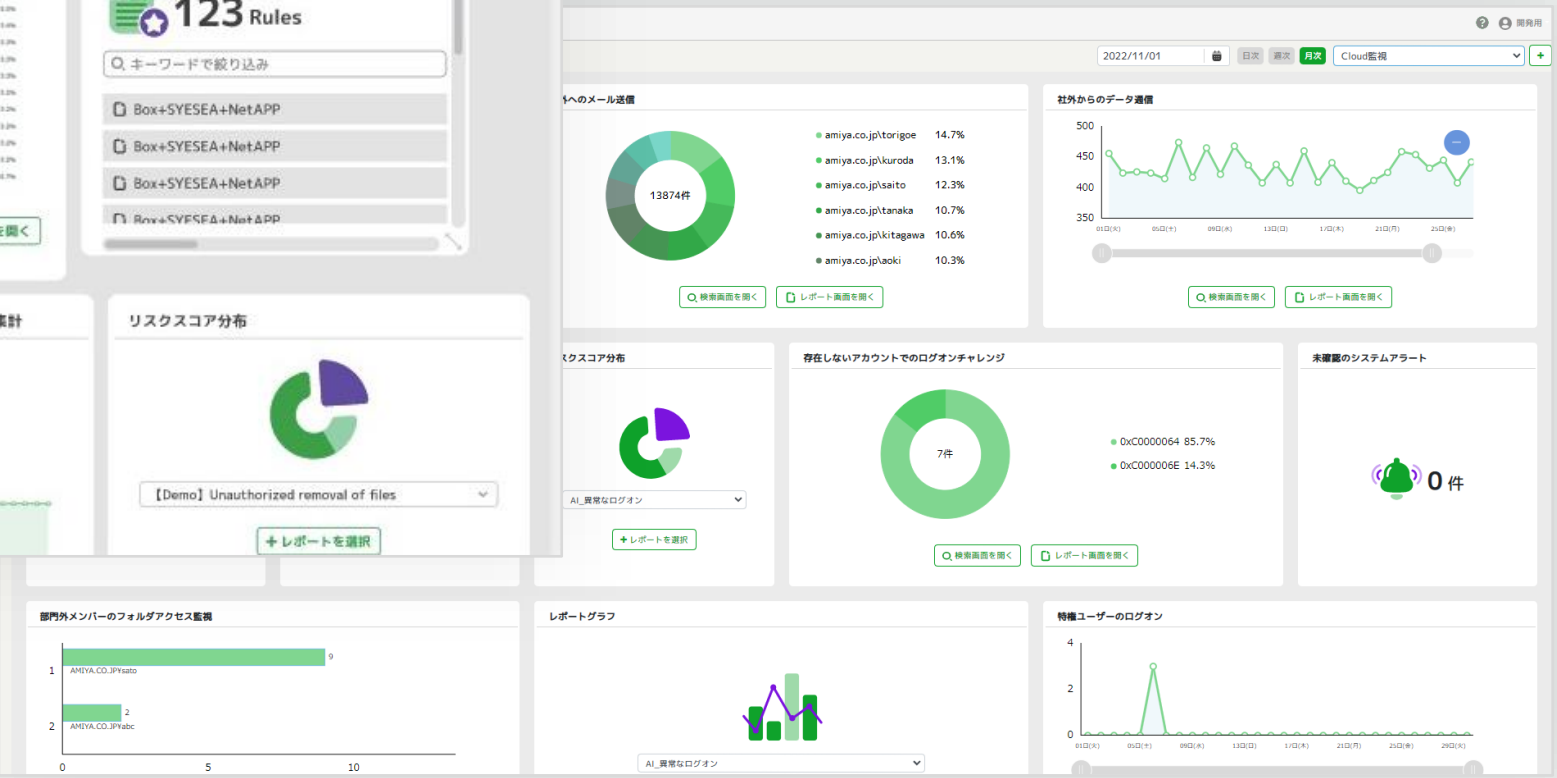
- いつもと違うIPアドレスからのアクセス
- いつもと違うトラフィック量
- いつもと違うファイルパスへのアクセス

And more

異常に気付くダッシュボード

すぐに確認したいレポートやアラート情報はダッシュボードに表示。ログイン後、一目で状態把握、異常に気づけます。

目的や担当者、機器サービスごとなど、
複数のダッシュボードを設定可能



見たいパネルを選択、
好きな場所に設置

Webブラウザのような検索窓

Webブラウザのような検索窓で任意のキーワード検索を。
大量データも高速にインポートして、複雑な検索条件でも高速検索と高度な分析を実現します。

選べるシステム構成

システム構成としてオンプレミス版、クラウド版を準備しています。

ALog クラウド版

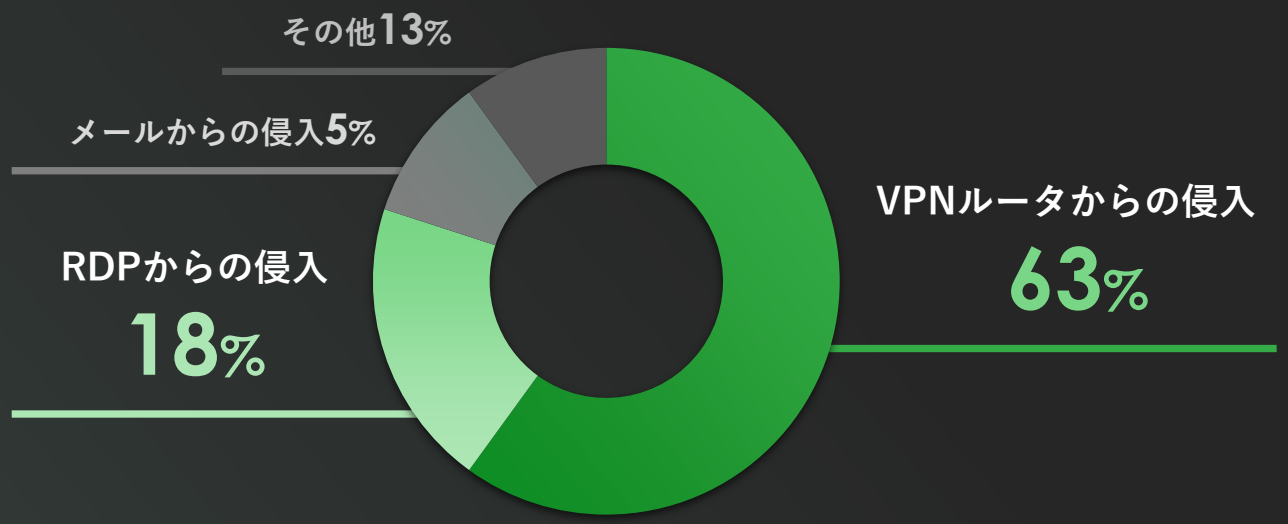
- サーバーレスで導入コストの削減
- 運用管理の負担軽減
- サポート情報の連携が容易

ALog オンプレミス版

- ネットワーク回線負荷の軽減
- クローズド環境のログ収集
- インフラの独自管理

MDR

ランサムウェア侵入経路の8割がVPNかRDP



引用：警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等」

最低限の絶対必要な対策！

検知するには 3 つの認証ログ監視が重要

VPN　RDP　Active Directory

注：図中の割合は小数点第一位以下を四捨五入しているため、統計が必ずしも100にならない。

サービスフロー

セキュリティスペシャリストがお客様環境のセキュリティインシデントを監視/対応。
不正侵入されても早期に検知し、被害を最小限に留める体制を整備します。

ALog

①アラート

②調査

ALog MDRセンター

③対応

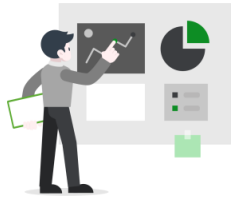
- 監視/トリアージ
- 脅威度判定
- 影響範囲調査
- 原因調査

サイバー攻撃・内部不正を監視

④報告

- 解析報告
- 推奨対策
- 月次レポート
- 改善提案

お客様



⑤決定

- インシデント対応
- 脅威度確認
- 対策

セキュリティスペシャリスト対応保有資格

- 情報システム監査人（CISA）
- 情報処理安全確保支援士

インシデント対応

※別途費用となります。

- インシデント対応コンサルティング
- フォレンジック
- 再発防止策

網羅的だから死角を最小に

網羅的な監視を任せられるからこそ、単一では気付けないサイバー攻撃を検知/分析。
何から始めて何を監視すべきかを専門に委託することでリスクを最小化します。

サービス範囲（対応システム一覧）

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）

ネットワークログ（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）

※状況に応じて、解析に必要なログ（DHCP、DNS、システムログなど）を取得します。
※順次監視対象を拡大中。記載がないシステムについてもご相談ください。

例えばサイバー攻撃

「侵入されても被害を最小化」するために網羅的に挙動を監視。
どれだけ素早く検知、特定、対処をするかで影響範囲が大きく変わります。

攻撃者の手口

侵入されない前提の
出入口対策

- Firewall　• Webフィルタ
- IPS/IDS　• アンチウイルス
- メールフィルタ

不正侵入

メールから侵入

脆弱VPNに侵入

感染

PowerShell
実行

遠隔操作

水平展開

他PCへ浸食

AD権限昇格

AD履歴削除

情報窃取

不正DB
アクセス

不正ファイル
アクセス

ファイル
外部送信

破壊

ファイル
暗号化

データベース
削除

ALog MDRセンター

爪痕 を網羅的に挙動監視

ログデータを監視することで侵入を先回り出来る

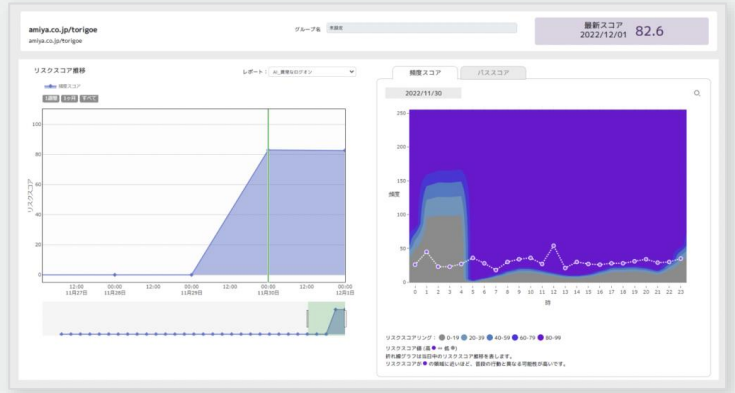
監視項目サンプル

ポリシー違反

- 業務時間外のログイン・ファイル操作
- 許可されていないWebサイトへのアクセス
- 許可されていない外部へのファイル共有
- 退職予定者のファイルアクセス/メール送信
- 重要フォルダへのアクセス

ITシステム監査

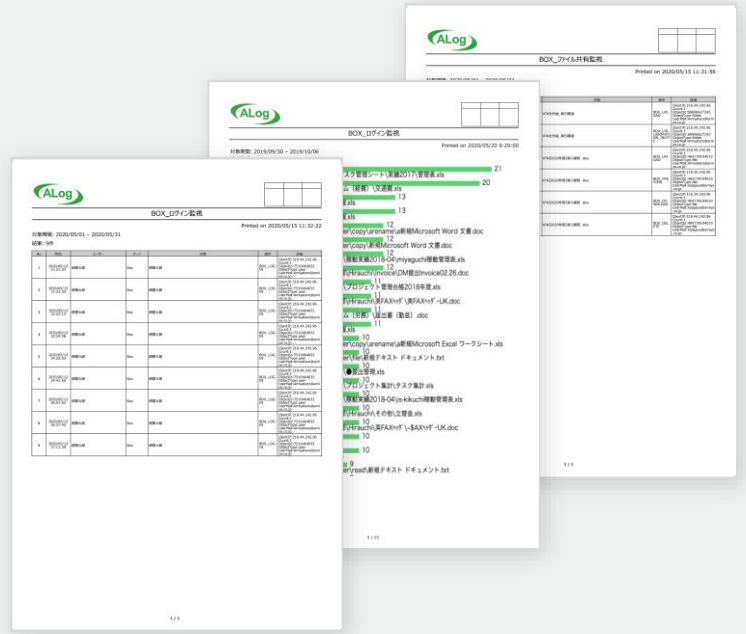
- 管理者権限ユーザのログオン
- 管理者権限ユーザの操作履歴
- 管理者権限ユーザのDB操作履歴
- ファイル/フォルダのアクセス権変更
- ユーザアカウントの追加/削除（消し忘れ）



不正アクセス

- VPNルータへの大量ログイン失敗
- 社員全員のWindows大量ログイン失敗
- ファイルサーバへの不正行為
  - ・PWファイルのREAD
  - ・組織図ファイルのREAD
  - ・ファイルへの大量RENAME
- UTM_マルウェア検知
- VPN_アクセス検知
- ドメインサーバへの不正行為
  - ・不審な権限昇格
  - ・不審なログ削除
  - ・不審なサービス起動
- クラウドサービスへの不正行為
  - ・MS365へのログオン失敗
  - ・MS365のアカウント作成/削除

等々



ALog MDRと他社の違い

	ALog MDRサービス	B社 ＳＯＣサービス（ミドルレベル）	C社 ＳＯＣサービス（ハイレベル）
脆弱性診断	○	△オプション	△オプション
相談窓口	○	△オプション	△オプション
監視対象	○網羅的	△限定的（EDR、UTMのみ）	△限定的（EDR、UTMのみ）
ログ管理製品	○ALog	×別途購入必要	×初期費用で購入
ログ運用代行	○	×お客様が運用	△オプション
外部攻撃監視代行	○アラート＋ログ分析	○アラート	○アラート＋ログ分析
内部不正監視代行	○レポート+AI分析	×	×
監査対応レポート	○	×	×
24365検知	○自動メール通知	○メール通知・電話	○メール通知・電話
24365対応	×	△電話でお客様をサポート	○SOWに従い実施
インシデント対応支援	○	○	○
イニシャルコスト	ALog導入 0円（サービス条件内）	製品導入 300万円～	製品導入 800万円～
ランニングコスト	20～45万円/月	30～40万円/月	80万円/月～

選べるMDRの運用レベル

AMIYA

		ログ運用をお任せしたい ALog MDR Basic	包括的なサイバーセキュリティ運用をお任せしたい ALog MDR Advanced
アタックサーフェス調査	予防	–	○
脆弱性診断		–	○
セキュリティ情報連携		–	○
SOC構築	検知	○	○
SOC運用（攻撃検知）		○	○
SOC運用（内部不正）		○	○
インシデント時のログ分析（原因/影響範囲）	対応	○	○
インシデント対応		○	○
インシデント初動対応アドバイス		–	○
レポート	その他	○	○
報告会		○	○
相談窓口		△（ログに関する事項）	○（セキュリティ全般）

戦略的ログ活用のために

ログは溜めているだけではその効力を発揮しません。
サイバー攻撃や内部不正などの脅威をアクティブに検知して対処するためにはログ活用が重要です。

攻撃の検出と通知

不審・異常アクセスのログを検知して通知。攻撃を初期フェーズのうちに検出し対応するためにログを活用。

解析

攻撃手法、侵略されたシステムやデータへのアクセス履歴より影響範囲の特定、攻撃の詳細な分析にログを活用。

証拠提供

セキュリティイベントとインシデントに関する法的要件への対応や証拠としてログを活用。必要情報としてログの提供、調査、報告、監査に活用。

再発防止

攻撃の痕跡をログで確認し、セキュリティプロセスやポリシーの改善等に活用。

価格・必要スペック

ALog クラウド版

ALog オンプレミス版

ALog MDRサービス

価格 ALog クラウド版

AMIYA

『基本利用料』に加え、『1日に取得するログデータ容量』で課金します。この料金内に1年間分のログ保管を含んでおります。
1年を超える期間ログを保管したい場合は、『ログ保管延長』をご契約ください。

基本利用料金

月額 ￥100,000

【型番：AC-BAS-1】

＋

ログデータ容量料金

月額 ￥50,000/5GB*

***1日に取得するログデータ容量**

【型番：AC-LOG-5】

＋

1年ログ保管料

￥0

保管1年延長オプション

月額 ￥10,000/5GB*

***1日に取得するログデータ容量**

【型番：AC-EXT-1】

- 年間での契約となります。（自動更新）
- 1日に取得するログデータ容量に応じて「ログデータ容量」をご契約ください。
  例：1日の取得するログデータ容量が10GBの場合は、(AC-LOG-5)×2で算出します。
- ALogイベントログ翻訳変換機能に対応しているOSは、翻訳変換後のログデータ容量で課金します。
- 取得したログデータ容量の月間平均値が契約の上限を2か月続けて超過した場合、ログの収集機能が停止します。
- 契約している容量の1000倍までデータスキャン（検索やレポート作成時のクエリ実行量）できます。（月合計）
  超過した場合には検索機能およびレポート/AIリスクスコアリングタスクが停止します。
  （ログデータ容量の追加契約または翌月タスクで解消します。）

ローカル変換システムフロー ALog クラウド版

AMIYA

対象システム

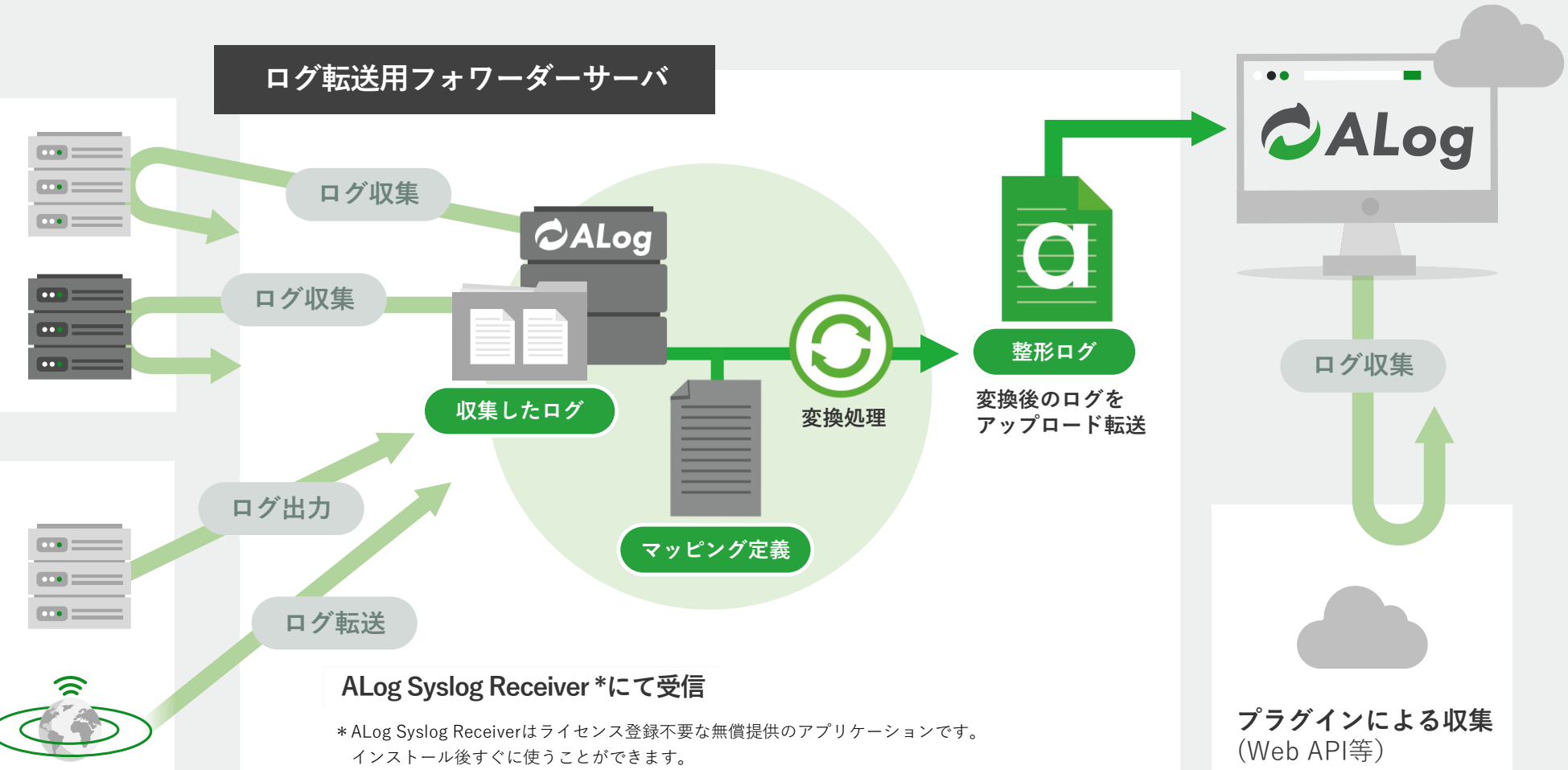
Windowsファイル共有
(NASサーバ等)

sshdによるSCP転送
(Linuxサーバ等)

ログ転送用
フォワーダーサーバの
ローカルフォルダに出力
(出力または転送)

Syslogを転送
(ネットワーク機器等)

ログ転送用フォワーダーサーバ



ALog Syslog Receiver *にて受信

＊ALog Syslog Receiverはライセンス登録不要な無償提供のアプリケーションです。
インストール後すぐに使うことができます。

プラグインによる収集
(Web API等)

クラウド変換システムフロー ALog クラウド版

AMIYA

対象システム

Windowsファイル共有
(NASサーバ等)

sshdによるSCP転送
(Linuxサーバ等)

ログ転送用
フォワーダーサーバの
ローカルフォルダに出力
(出力または転送)

Syslogを転送
(ネットワーク機器等)

ログ転送用フォワーダーサーバ

ログ収集

ログ収集

ログ出力

ログ転送

ALog

収集したログ

変換前のログを
アップロード転送

ALog Syslog Receiver *にて受信

＊ALog Syslog Receiverはライセンス登録不要な
無償提供のアプリケーションです。
インストール後すぐに使うことができます。

整形ログ

変換処理

マッピング定義

ALog

ログ収集

プラグインによる収集
(Web API等)

ローカルログ転送用フォワーダー必要スペック

ALog クラウド版

AMIYA

ローカル変換

対応OS	Windows Server 2016 / 2019 / 2022 / 2025
CPU	Quad Core以上
メモリ	16GB 以上
ディスク	500GB以上の空き容量

以下のいずれかのWebブラウザ

Google Chrome
Microsoft Edge

取得可能ログ形式

イベントログ、Syslog、テキストファイル（CSVなど）、
プレーンテキスト

クラウド変換

対応OS	Windows Server 2016 / 2019 / 2022 / 2025
CPU	Dual Core以上
メモリ	8GB 以上
ディスク	500GB以上の空き容量

以下のいずれかのWebブラウザ

Google Chrome
Microsoft Edge

取得可能ログ形式

Windowsイベントログ、Syslog、
テキストファイル（CSVなど）、プレーンテキスト

価格 ALog オンプレミス版

AMIYA

『基本利用料』に加え、『1日に取得するログデータ容量』で課金します。

基本利用料金

月額 ￥70,000

【型番：AL-BAS-1】

＋

ログデータ容量（5GB/Day）

月額 ￥50,000/5GB*

*1日に取得するログデータ容量

【型番：AL-LOG-5】

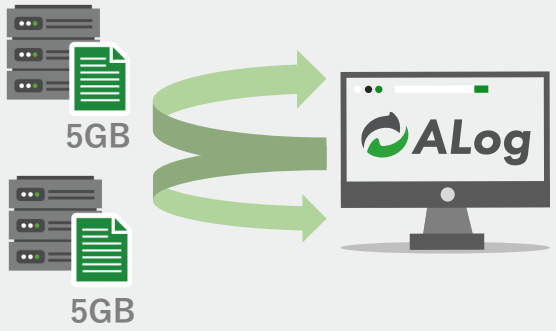
- 年間での契約となります。（自動更新）
- 1日に取得するログデータ容量に応じて「ログデータ容量」をご契約ください。
  例：1日の取得ログ容量が10GBの場合は、(AL-LOG-5)×2で算出します。
- ALogイベントログ翻訳変換機能に対応しているOSは、翻訳変換後のログデータ容量で課金します。
- 取得したログデータ容量の月間平均値が契約の上限を2か月続けて超過した場合、ログの収集機能が停止します。

冗長構成の考え方 ALog オンプレミス版

AMIYA

対象システムが冗長構成の場合

1台のマネージャサーバより
複数台のシステムからログを取得する



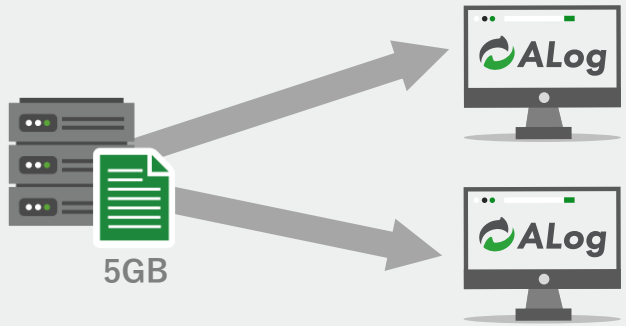
取得するログデータ容量：
各システム5GB/Day以内の場合

必要な契約

基本利用料金
（AL-BAS-1）× 1
＋
ログデータ容量
（ AL-LOG-5 ）×2

マネージャサーバが冗長構成の場合

2台のマネージャサーバにログを転送する



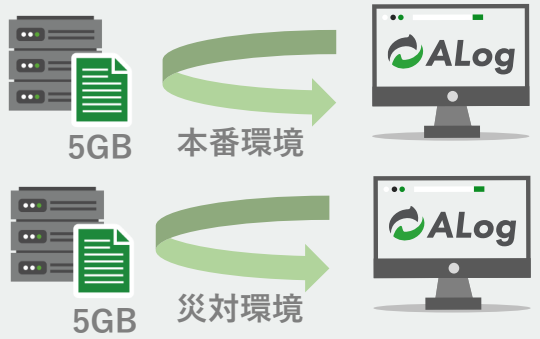
取得するログデータ容量：
5GB/Day以内の場合

必要な契約

基本利用料金
（AL-BAS-1）×2
＋
ログデータ容量
（ AL-LOG-5 ）×1

環境が冗長構成の場合

異なる環境ごとにマネージャサーバ設置、
システムのログを取得する



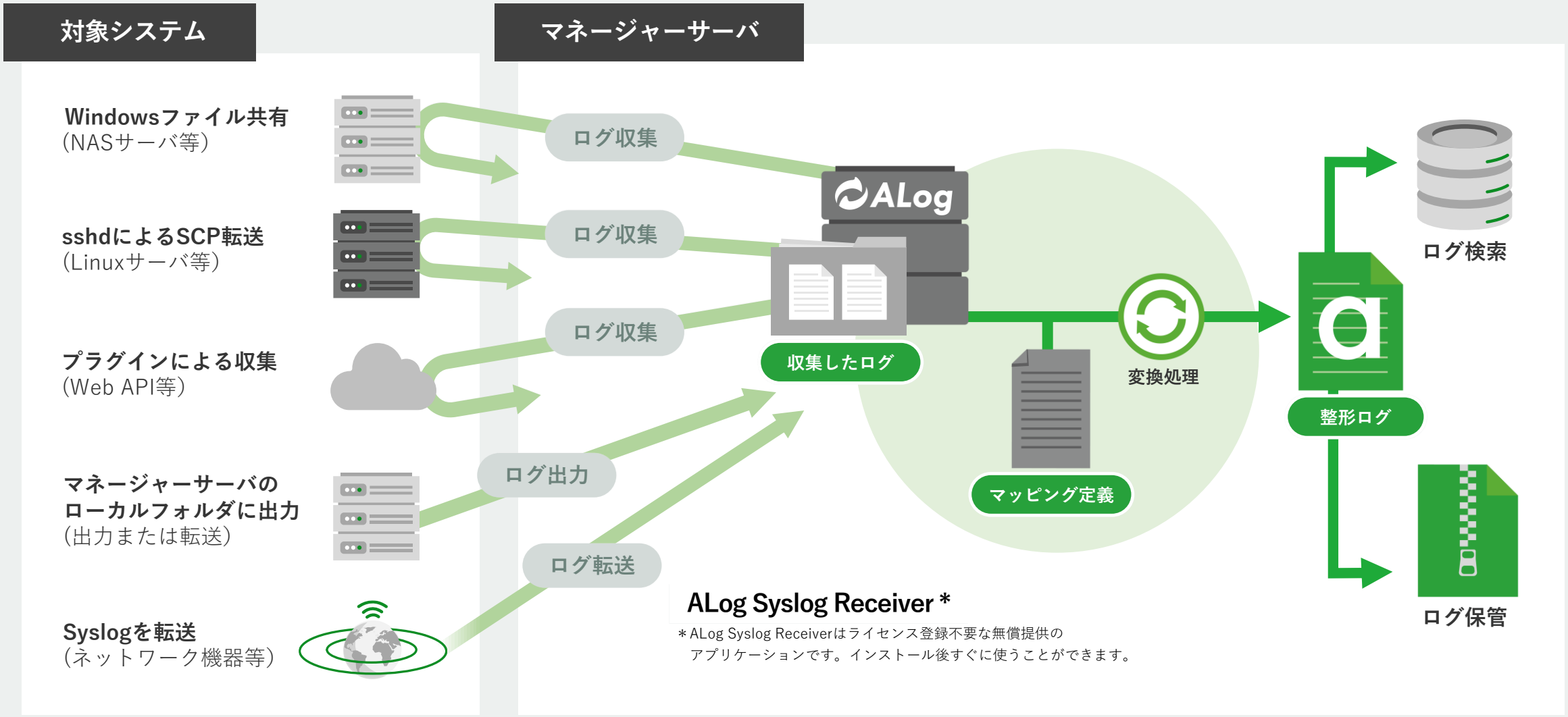
取得するログデータ容量：
各環境5GB/Day以内の場合

必要な契約

基本利用料金
（AL-BAS-1）×2
＋
ログデータ容量
（ AL-LOG-5 ）×2

システムフロー ALog オンプレミス版

AMIYA



マネージャーサーバ必要スペック ALog オンプレミス版

AMIYA

対応OS	Windows Server 2016 / 2019 / 2022 / 2025
CPU	2.7GHz 8コア 以上
メモリ	32GB 以上
ディスク	500GB以上の空き容量

以下のいずれかのWebブラウザ

Google Chrome
Microsoft Edge

取得可能ログ形式

イベントログ、Syslog、テキストファイル（CSVなど）、
プレーンテキスト

価格 ALog MDRサービス

AMIYA

アカウント数	MDR Basic （月額）	MDR Advanced （月額）
～1,000アカウント	¥200,000	¥300,000
～2,000アカウント	¥300,000	¥400,000
～5,000アカウント	¥500,000	¥600,000

サービス条件

【共通】
・サービスは年間契約、および自動更新でのご案内となります。
・上記にALogの基本利用料金/ログデータ容量のライセンスは含みません。
・契約は、Active Directory のアカウント数で課金します。
（Active Directoryをご利用でない場合は、Active Directoryに準ずるシステムのユーザアカウント数で課金します。）
・当サービスは、祝日年末年始を除く平日9－17時、リモート（遠隔）での対応となります。
※時間外のアラート対応は、翌営業日となります。
・サービス提供にあたり、ALogの構築環境（「オンプレミス」または「クラウド」）に応じてサービス条件が異なります。
・ALogマネージャーサーバ/テナントは1つ迄となります。
・一法人単独での利用、環境を前提となります。
・網屋からのリモート接続に専用端末が必要な場合、別途費用が発生します。

【MDR Advanced】
• 脆弱性診断：4半期に一回（年4回）、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、報告します。
• アタックサーフェス調査：4半期に一回（年4回）、インターネットに公開しているシステムを調査、リスクを報告します（1ドメインまで）

オンプレミス環境でALogを利用する場合
以下がサービス費用に含まれます。
・ALogインストール作業
・ALog設定作業
※ログ取得対象の登録は10システム迄

クラウド環境でALogを利用する場合
以下がサービス費用に含まれます。
・ALog Cloudの設定作業
※ログ取得対象の登録は10システム迄

運用形態の違い

	ALog クラウド版	ALog オンプレミス版
イニシャルコスト	・初期費用がかからない ・低コストでスタートができる	・マネージャーサーバの準備が必要
ランニングコスト	・月額利用料金＋ログデータ容量の費用が必要	・月額利用料金＋ログデータ容量の費用が必要 ・人件費やサーバの電気代などが必要
インフラ調達	・アカウント登録後すぐに利用できる	・機器調達がある場合、約数週間後からの利用
カスタマイズ性	・管理機能に制限あり	・自社で構築するため、構成上のカスタマイズが自由
処理性能	・クラウド上の豊富なリソースが利用できる	・マネージャーサーバのスペックに依存
セキュリティ	・ISO27017に乗っ取ったセキュリティ機能を提供 （ISO/IEC 27017：CLOUD 794817）	・自社ルールによるセキュリティ対策ができる
障害/災害リスク	・クラウド事業者が復旧作業を行うため、ユーザーはインターネット経由で復旧を確認	・自社で復旧を行うため、常にシステムに精通した従業員が必要
バックアップ	・クラウド側で全てのデータを自動バックアップ	・ログデータのバックアップ機能を提供 ・環境バックアップは任意で実施
運用負担	・自動メンテナンス/アップデート	・任意でメンテナンス/アップデート

サポートサービス

テクニカルサポート

メール・電話での回答

* 土日祝祭日・弊社指定休日および年末年始を除く平日9：00~17：00での対応
* メールは24時間365日受付

ALogシリーズサポートサイト

お問い合わせ機能、各種お役立ち情報を掲載

掲載情報

- メンテナンス・アップデート情報
- よくあるご質問・ご利用ガイド
- ユーザーマニュアル
- 各種ダウンロードコンテンツ

ALogシリーズサポートサイト

プレミアムサポート

プレミアムサポートは、通常のサポートサービスに加え、設定代行やレポートチューニング、稼働状況チェック、
さらに個別ログ調査・分析など、より深い技術支援をリモートでご提供するオプションサービスです。

プレミアムサポート料金

月額 ￥50,000

【型番： AL-PS】

- 年間での契約となります。（自動更新）
- サービスの提供回数：１ヶ月あたり２回付与
- サービスの提供時間：１回あたり２時間まで
  （提供回数を使用して連続での提供可能）

サポート範囲	サポート概要
ALogの設定代行	ログ取得対象や取得条件を見直し、 必要なログを確実に収集できる状態に整備します。
バージョンアップ代行	重要なパッチを漏れなく適用。運用の手間を軽減しつつ、 ALogを最新状態に保ちます。
稼働状況チェック	ログ取得状況、監査設定などを定期的に確認し、 安定かつ最適化された環境に保ちます。
レポートチューニング	お客様の要望に基づき、目的別にあわせた 監視・レポート設計を行います。
個別チューニング	AIリスクスコアリングや検索条件の設定を、 環境や要件に合わせて個別に最適化します。
個別ログ調査／分析	不正アクセスの兆候や疑いのあるログを、 専門スタッフが個別に調査・分析し、対応を支援します。

30日間無料トライアル

ALogなら最短3STEPでログ管理をスタート！

1
お申し込み

2
取得するログセット

3
レポート設定

Finish!

トライアルを申し込む

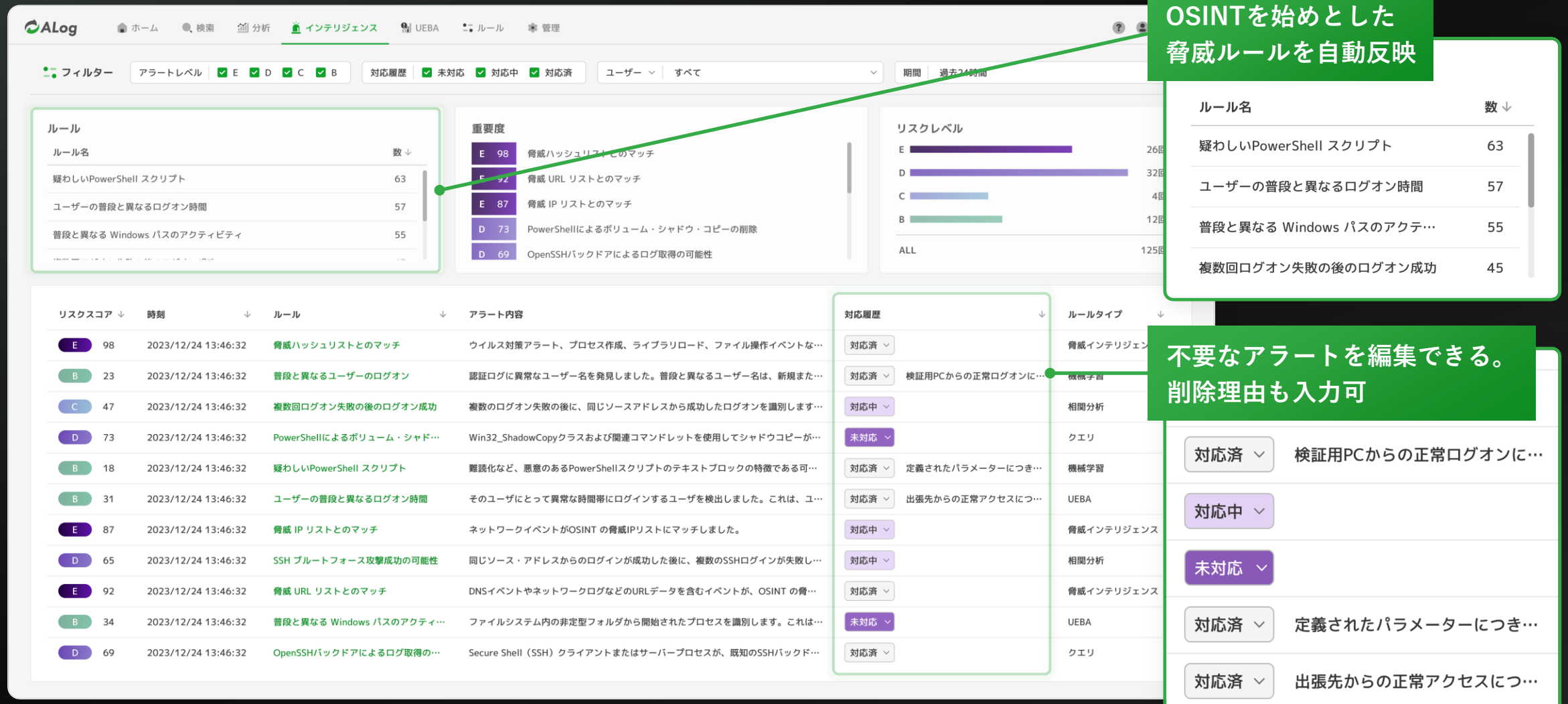
ALog

今後の機能拡充

- インテリジェンス連携
- Sigmaルール
  標準搭載
- AIの拡張分析
- UEBA強化
  AI振る舞い検知

今後の機能拡充

インテリジェンス連携



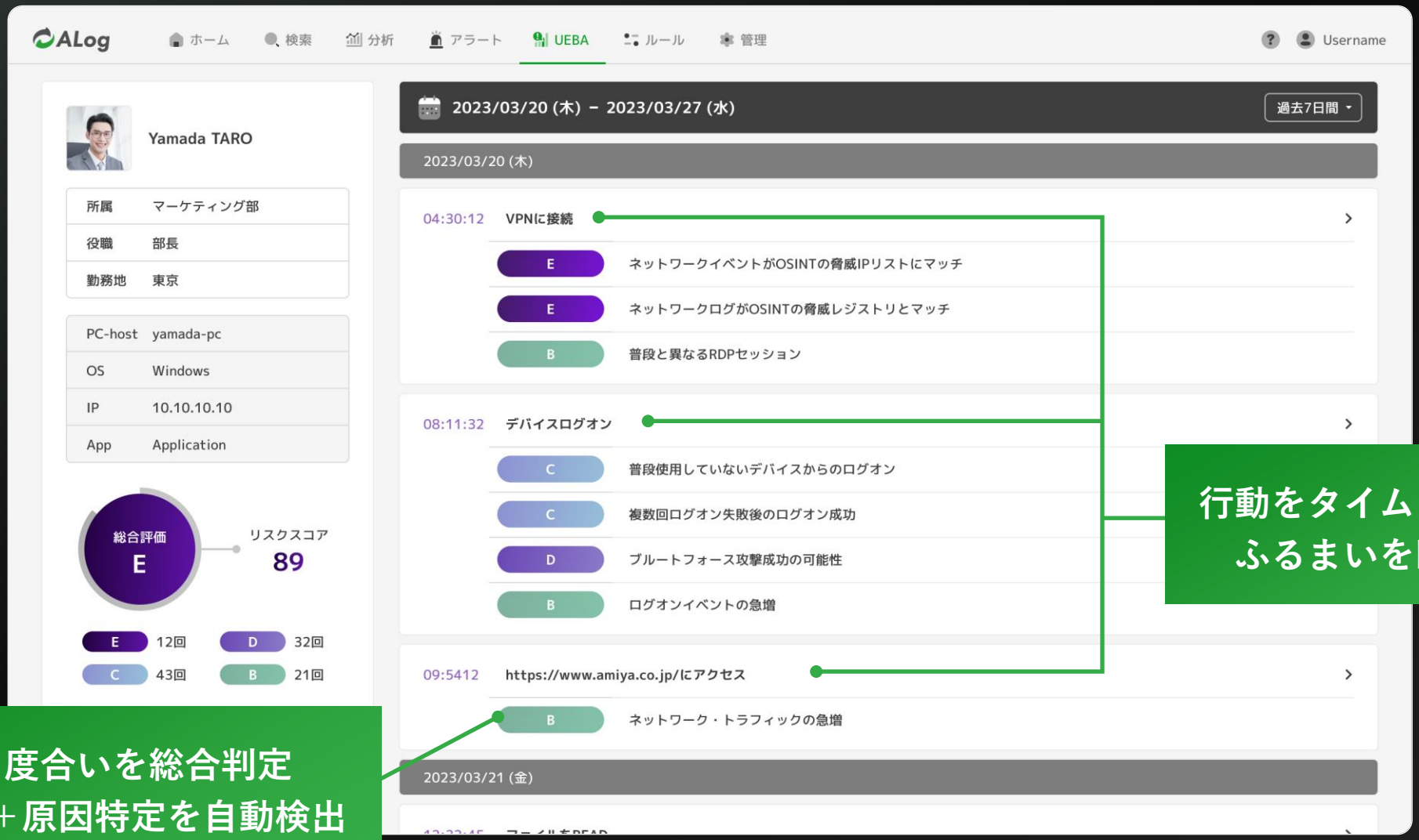
OSINTを始めとした脅威ルールを自動反映

ルール名	数
疑わしいPowerShell スクリプト	63
ユーザーの普段と異なるログオン時間	57
普段と異なる Windows パスのアクテ…	55
複数回ログオン失敗の後のログオン成功	45

不要なアラートを編集できる。削除理由も入力可

対応済	検証用PCからの正常ログオンに…
対応中	
未対応	
対応済	定義されたパラメーターにつき…
対応済	出張先からの正常アクセスにつ…

今後の機能拡充　UEBA強化



行動をタイムライン化。
ふるまいを時系列に

リスク度合いを総合判定
攻撃検知＋原因特定を自動検出

V8をご利用のお客様

2024/3/31に機能拡充を、2029/3/31に全てのサポート対応が終了します。

製品移行も“カンタン”に

購入製品機能のみのご利用	全ての製品機能を搭載
現行環境を引き継ぎたい	移行ガイド・ツールを提供

移行に関するご相談はこちら

AMIYA

網屋はセキュリティの製品やサービスを開発・製造・販売する総合セキュリティプロバイダとして、お客様のセキュリティの課題を幅広くワンストップでご支援致します。

ログ管理

ALog

複雑なログをわかりやすく管理。
AIと高度な分析機能で効果の見えるログ管理を実現。

クラウドCSIRTサービス

セキュサポ

当社のセキュリティ専門チームがお客様の環境全体を監視し、ランサムウェア攻撃をはじめとした一連のサイバー攻撃への対策を包括代行。

脆弱性診断サービス

セキュリティ監査サービス

クラウドネットワークインフラ

Network All Cloud®

煩わしいネットワーク構築や、導入後の運用や障害対応までをクラウド上のサポートセンターが代行。

サイバーセキュリティトレーニング

経営層から一般社員、エンジニアまで網羅的なサイバーセキュリティトレーニングで組織のセキュリティレベル向上をサポート。

AMIYA 株式会社網屋

https://www.amiya.co.jp/