ログ管理

zcrLog

ログを保存。
必要な証跡を検索。

zcrLogは、IT管理者とコンプライアンス担当者のために、セキュリティログの収集・保管・検索・レポート作成を行います。承認済みのチャネルパートナーを通じて、Cloud、専用VM、ハードウェアアプライアンスを検討できます。

導入形態

- Cloud / SaaS
- 専用 VM
- ハードウェアアプライアンス

1 — 2 — 3 ▶

収集

対応する Syslog UDP/TCP と API からログを収集。

保存

プラン、ログ量、利用可能な容量に応じて保持期間を設定。

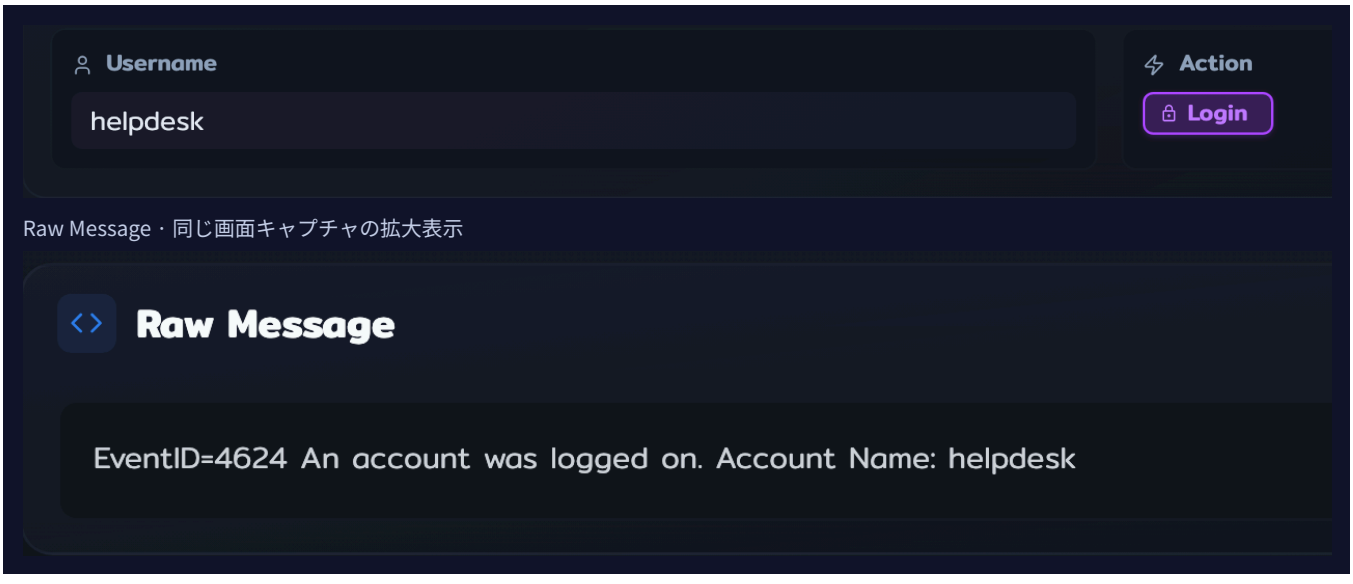
検索・レポート

時刻、収集元、ユーザー、Event ID で絞り込み。

利用の流れを示す概念図です。実際の導入構成ではありません。

イベントから、調査に使える証跡へ

DEMO / 4624



Raw Message・同じ画面キャプチャの拡大表示

実際のデモ画面です。イベントは説明用で、顧客データや性能測定値ではありません。

収集元システム: **Windows Server**　ユーザー: **helpdesk**　操作: **Login**

ログの収集元と導入形態をパートナーと検討

デモを確認 ↗　パートナーに相談 ↗

製品の詳細

収集と保管

02

サイジングは、ログの種類、転送方法、必要な保持期間によって決まります。画面の件数は利用状況を示すもので、性能測定の結果ではありません。

項目	範囲と条件
ログソース	ファイアウォール、Active Directory、Endpoint Security（CrowdStrike Falconなど）、Microsoft 365、Microsoft Entra ID、AWS CloudTrail、Google Cloud監査ログ、Syslog対応ネットワーク機器。各ソースのパーサーとAPI権限は、ソリューション設計の段階で確認します。
取り込み・転送	対応するSyslog UDP/TCPとAPIで収集。ソース、宛先、ポートを指定してSyslogサーバーやログ受信機へ転送できます。
時刻基準	複数システムのイベントを比較する前に、NTPとタイムゾーンを統一します。
保持期間	コンピュータ犯罪法第26条に基づくコンピュータトラフィックデータの保持：90日〜2年。実際の保持期間はプラン、取り込み量、利用可能ストレージに依存し、すべてのプランに2年の保持が含まれるわけではありません。
データ完全性	MD5、SHA-1、SHA-256による完全性検証と、AES-128によるログ暗号化。
アーカイブと出力	アーカイブ、JSON・CSV・Parquet出力、増分・フルバックアップ。
復旧	アーカイブやバックアップから復元。ディスク使用量を確認し、ポリシーに従ってアーカイブとクリーンアップを設定します。
バックアップ先	Cloud/SaaSはHTTPS経由でクラウドサービスへバックアップします。ハードウェアアプライアンスと専用VMでは、外部ディスク、FTP/TFTP、手動ダウンロードも利用できます。保存先と保護方法はソリューション設計で決めます。
冗長ストレージ	設計した構成に応じて対応します。冗長化はバックアップや復元テストとは異なります。

Microsoft 365、Entra ID、クラウドのログソース

zcrLogは、Microsoft Entra IDのサインインログと監査ログ、およびOffice 365 Management API経由でMicrosoft 365のワークロード監査ログ（Exchange・SharePoint・Teams）を収集します。AWS CloudTrail、Google Cloud監査ログ、CrowdStrike Falconのログも収集できます。

製品の詳細

検索と運用

03

ログが届いているか、いつ発生したイベントか、担当者が証跡を取得できるか。運用上の問いから確認を始めます。

項目	範囲と条件
検索と絞り込み	保存したログを、期間、ソース・デバイス、IP、ユーザー、イベント、アプリケーション、プロトコル、重要度で絞り込み。
ダッシュボード	ログ件数、ソースのTop-N、EPS、ストレージ、保持期間、直近のイベント、監査証跡を対応する画面で確認。
調査支援	インシデントのグループ化、MITRE ATT&CK対応付け、リスクスコア、攻撃マップ、IP情報が調査を支援します。すべての攻撃の検知を保証しません。
検知ルール	カスタム、AI支援、Sigma、テンプレートによるルール。運用前に、実環境のデータで各ルールを確認・テストしてください。
レポート	対象期間と証跡を選んで、エグゼクティブサマリーレポートを作成できます。MDRレポート（重要度の要約、攻撃の傾向、フォローアップが必要なインシデント、技術的な詳細、AIによる推奨事項）はzcrMDRサービスの一部として提供され、zcrLog単体の権利ではありません。本格的なSIEM運用は別製品のzcrSIEMが担います。
通知	検知・通知ルールと送信先の権限設定に基づくEmail、Microsoft Teams、LINE。
権限と監査	多要素認証（MFA）、役割ベースのアクセス制御（RBAC）、マルチテナント管理。ログイン・ログアウト、アクセス、設定変更、システムエラーの記録。
システム健全性	導入形態に応じたCPU、メモリー、ディスク、ネットワーク、ファイルシステム、サービス監視。ホストレベルのCPU・RAM・ストレージ閾値は、オンプレミス導入が対象です。

製品機能とサービス
インシデント画面やレポートは製品機能です。アナリストによる監視、インシデント対応、SLAはサービスで、契約に明記した場合にのみ含まれます。

モデル選定

ハードウェアアプライアンス

04

ICTモデルの公開仕様です。EPS（1秒あたりのイベント数）は各モデルの公表値です。発注前に、パートナーがワークロードに合うモデルを選び、構成部品表を確認します。

仕様	ICT1	ICT2	ICT3
CPU	8 Core	8 Core	16 Core
メモリー	16 GB	32 GB	64 GB
SSD	1 TB	2 × 480 GB	2 × 480 GB
HDD	—	2 × 4 TB	2 × 8 TB
ネットワーク	1 × 1 GE RJ45	2 × 1 GE RJ45	2 × 1 GE RJ45
形状	Mini PC	1 RU	1 RU
公開EPS	1,000	7,000	20,000
推奨デバイス数	3–5	6–15	16–30
基本保持期間	90日[1]	90日[1]	90日[1]

保持期間

[1] 実際の保持期間は取り込み量と使用可能容量に依存します。RAIDと予約領域を含めて計算してください。

RAID / 構成部品表

構成に応じてRAID 0/1/5/10に対応し、対応モデルの既定値はRAID 1です。納入構成をパートナーにご確認ください。

電源

電源定格は記載していません。発注前に、パートナーが納入モデルの電源要件と構成部品表を確認します。

すべてのプランに含まれるもの

zcrLogの各プランには、Syslog取り込み、ダッシュボード、MITRE ATT&CK対応付け、AI支援ルール、経営向け要約、通知、バックアップとアーカイブ、アカウント保護、マルチテナント管理が含まれます。導入支援、HA/DR、SLAは、提案書に明記した場合にのみ含まれます。MDRレポートはzcrMDRサービスの一部として提供され、zcrLogプランの権利ではありません。

→ **ログの収集元と導入形態をパートナーと検討**

発注前に、ログ量、保持期間、利用可能な容量、構成部品表をパートナーとご確認ください。 · パートナーに相談 ↗

モデル選定

専用VMとCloud

05

専用VMのプランは最小リソースとストレージで、Cloudのプランは日次取り込み量（GB/日）で決まります。EPSやデバイス数は参考値で、互いに置き換えられる容量上限ではありません。

専用VM・ICTC

仕様	ICTC1	ICTC2	ICTC3
最小CPU	4 vCore	4 vCore	4 vCore
最小RAM	4 GB	4 GB	4 GB
ストレージ	1 TB	2 TB	3 TB
参考デバイス数	3	5	10
基本保持期間	90日	90日	90日

専用VMのプランはEPSを上限にしていません。実際の処理量はVMに割り当てたリソースに依存します。上記は最小要件で、負荷が高い場合はリソースを追加してください。

Cloud / SaaS・日次取り込み量

プラン	Cloud1	Cloud2	Cloud3	Cloud4
GB / 日	1	3	5	10
基本保持期間	90日	90日	90日	90日
デバイス数	無制限	無制限	無制限	無制限

SaaSの課金基準はGB/日で、デバイス数やEPSを課金上限にしていません。表はCloud1〜4を示します。基本取り込みプランは50 GB/日まであります。180日・365日・2年の保持期間延長オプションは10 GB/日以下にのみ提供し、10 GB/日を超えるプランには提供していません。

製品の対象範囲：本書の対象はzcrLogのログ保管と証跡運用で、包括的なSIEMやMDRサービスではありません。zcrSIEMは独立した製品で、zcrLogを前提としません。

製品の詳細

パートナーと進める評価

06

設計と見積もりの段階で、パートナーがお客様と以下の項目を確認し、データと運用体制に合った構成にします。

評価項目	確認する内容
入力データ	ログソース、プロトコル、パーサー、API権限、GB/日、ピーク時間帯。
データポリシー	保持期間、保管場所、アクセス権、NTP、アーカイブ・バックアップ計画。
受け入れ確認	ソースイベントと時刻の照合、ログ検索、通知テスト、復元テスト。
責任分担	ソース、プラットフォーム、パートナーの担当者とエスカレーション経路。
サービス範囲	連携、導入支援、HA/DR、サポート、SLA、対象外の作業を書面で確認。

規格と調達時の確認資料

通信データ保持の参考規格としてタイ規格 มศอ. 4003.1-2560 を参照します。提案するソフトウェアのバージョンと導入形態に製品の認証書が適用されるか、承認済みパートナーと確認してください。

NECTEC のリンクは規格本文です。調達時は認証書の原本、認証番号、発行機関、発行日・有効期限、対象プロジェクトに適用される範囲を確認してください。

認証済みシステムを利用しても、法令上の組織の責任を代替するものではありません。

NECTEC の規格本文 ↗　パートナーに確認資料を依頼 ↗

zcrパートナーと評価を計画する

提案、契約、顧客への導入・提供は、承認済みのディストリビューター、リセラー・SI、MSP・MSSPを通じて行います。

パートナーに相談 ↗　現行プランを見る ↗　デモページを開く ↗

仕様とプランは変更される場合があります。最新の内容はパートナーにご確認ください。

7 · 設計時に確認する技術詳細

製品の詳細

設計時に確認する技術詳細

07

ソリューション設計の際にパートナーと確認する技術詳細です。SLAを約束するものではありません。

項目	範囲と条件
ログ転送	ログ転送では元データを変更せず、送信元・宛先・ポート・期間を指定できます。受け入れテスト時にペイロードの完全性と宛先側のタイムスタンプを確認してください。
アーカイブ圧縮	アーカイブ圧縮は内容により最大15倍まで到達します。実際の比率はご自身のログで測定してください。最大値をそのまま容量削減の保証として扱わないでください。
バックアップと復元	バックアップ先は提供形態によって異なります（2ページ参照）。受け入れテストでは、選んだバックアップ先からの復元を確認してください。
容量ポリシー	設定した使用量の閾値とポリシーに応じ、アーカイブ・クリーンアップ・削除を設定します。VMの容量拡張は選択するプランと提案内容によります。
オンプレミス監視	CPU・メモリー・ディスク・ネットワーク・ファイルシステム・サービスのホストレベル監視は、オンプレミス導入に適用されます。これらの閾値はすべてのSaaSテナントに保証される権利ではありません。
ネットワーク閾値	ネットワーク使用率、エラーパケット、破棄パケットの閾値に対応しています。監視対象のインターフェースと取得可能なテレメトリは、実際の環境で確認してください。
役割と監査	役割・権限の追加、ログイン・ログアウト、アクセス記録、システム状態変更、障害・エラー、構成変更を扱います。
レポートと取り込み	レポート期間は1・3・5・7・30・60・90日または任意指定です。取り込みはSyslog UDP/TCP、Microsoft 365向けのOffice 365 Management API、EDR APIキー、カスタム連携、機器別分析に対応します。各ソースのコネクターはソリューション設計で確認します。
MSSPとサービス範囲	マルチテナント管理だけでMSSPの再販権やMDRサービスが付くわけではありません。利用権、責任、サポート範囲はパートナーとの契約で明示します。