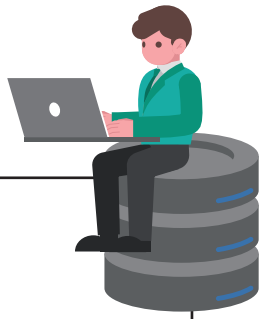
これさえ見ればわかる!

ログ管理スターターガイド

AMIYA

目次



本書の対象

本書は、

- これからログ管理を始める人
- 収集しているログを有効活用できていない人
- ログの活用で何ができるのか知りたい人

などのログ管理初心者向けに、ログの有用性を分かりやすく紹介するものです。ログは、インシデント発生時の事後調査や監査報告に利用できるのみならず、サイバー攻撃対策や内部不正対策、テレワークへの対応など、様々な場面で活用できます。本書がログ活用への第一歩となれば幸いです。

はじめに

活用して欲しい、ログという資産

企業の抱える課題は様々です。
セキュリティ脅威への対応は喫緊の課題です。
年々増加するサイバー攻撃は多様化・巧妙化しており、従来のセキュリティソフト対策だけでは太刀打ちできなくなってきています。
さらには、内部不正による情報漏えいも後を断たず、長年に渡って外部攻撃と並ぶセキュリティ脅威となっています。
また、近年の働き方改革や新型コロナウイルスの流行の影響でテレワークが普及し、多くの企業が勤怠管理上の課題を抱えるようになりました。

これらの課題解決に活用して欲しいのがログという資産。
ログはさまざまなシステムから出力される重要なデータです。
ログは、サイバー攻撃や内部不正の検知、分析を行い、被害を最小限に抑える対策に利用できることはもちろん、テレワーク中の勤務実態の把握など、幅広いシーンで活用し、企業の抱える様々な課題を解決することができます。
本書では、ログがどのように活用できるのかを紹介していきます。

「情報セキュリティ10大脅威 2022」

順位	脅威の内容	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
5位	内部不正による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

出典:IPA「情報セキュリティ10大脅威 2022」
https://www.ipa.go.jp/security/vuln/10threats2022.html

ログ管理の5つの目的

「ログ管理」とは、パソコンやシステム、アプリケーションなどで起こった様々な出来事の記録であるログを収集・保管し、一元管理することを指します。

ログ管理は、明確な目的を持って取り組むことで、ログを活用し、その効果を最大限に引き出すことができます。ここでは、ログ管理の主な目的を5つ紹介します。

1 サイバー攻撃対策

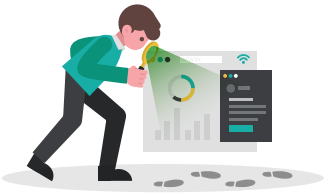
サイバー攻撃などによる不正アクセスを監視することができます。
ログ管理により、パソコンやサーバ、システムにいつだれがアクセスしたかを把握できるため、情報漏えいが発生した際に原因究明や被害範囲の調査が可能になります。

2 内部不正対策

情報漏えいは、外部からの攻撃によるものだけでなく、ヒューマンエラーによるものや、内部不正によるものもあります。ログ管理により社員の業務を把握することは、これらの情報漏えいの抑止や、原因調査にも有効です。

3 監査報告

ログを管理することで、証跡管理やログデータの長期保管が可能になります。
それにより、各種監査報告や、業種別のセキュリティガイドラインへの準拠ができるようになります。

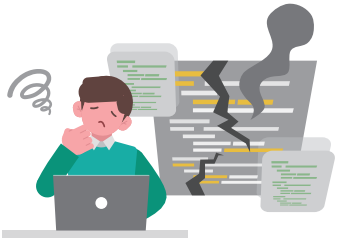


4 勤務実態の把握

パソコンのログオン/ログオフの記録やアプリケーションの利用状況から勤怠状況を可視化することに役立ちます。ログ管理をすることで、サービス残業や怠慢勤務などを可視化したり、より正確な勤怠管理を行ったりすることができるのです。

5 障害原因調査

利用状況を把握し、システム障害が発生した時にその原因を突き止められます。
障害が発生した前後にどのような通信が行われたのかを確認することで、障害からの復旧に役立てたり、同じ障害が起きないように対策を立てたりできます。



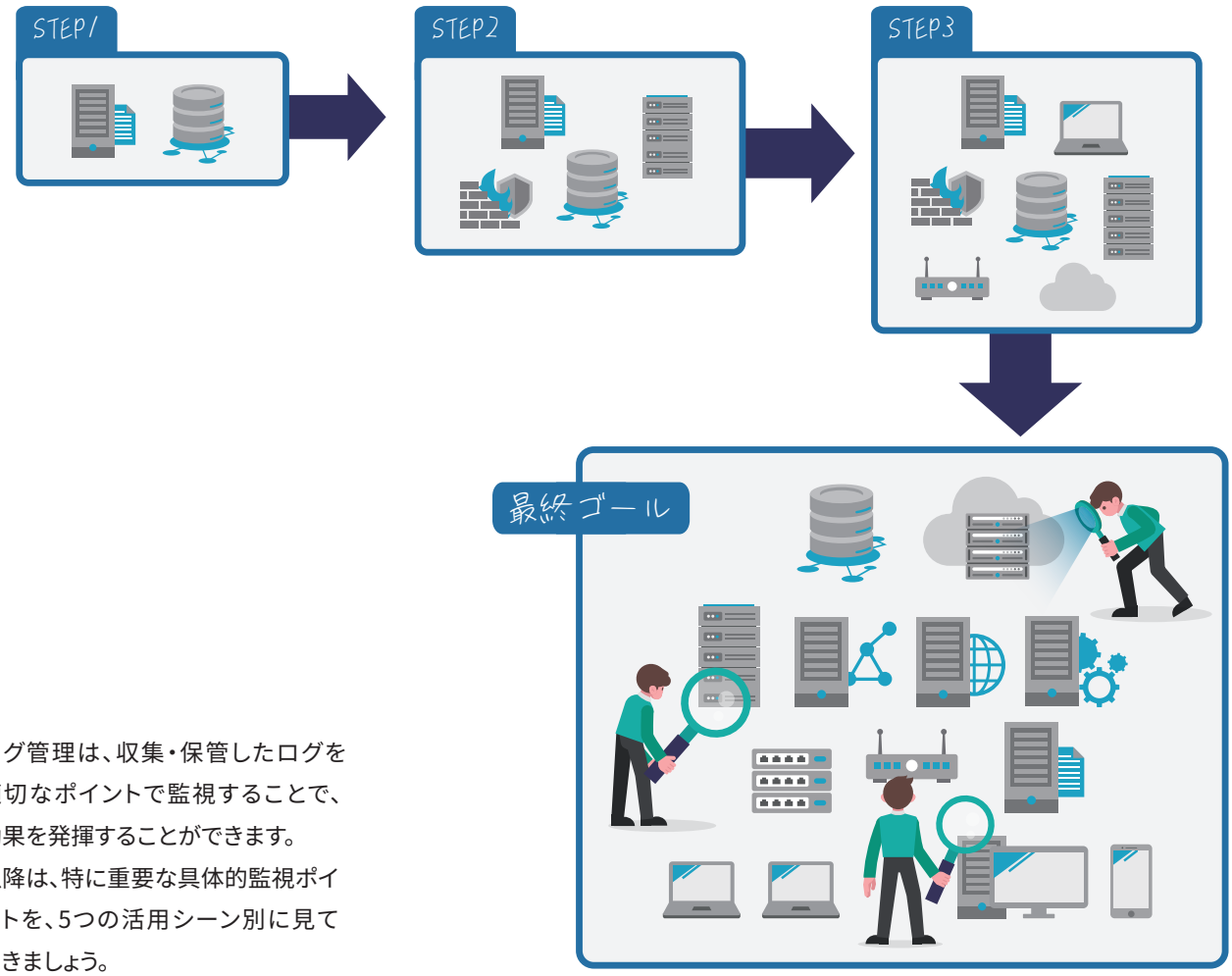
目的に応じたログ管理

企業を支えるシステムは、DX、クラウド化、テレワーク導入など多種多様な目的に応じて年々増加しています。
そのため、ログ管理をはじめるにあたって、様々なシステムの中の何のログを取得すべきか？という悩みがつきものです。

効果的なログ管理には、目的に応じたログ取得が必要です。
まずはログ管理の目的を明確にし、必要十分なログを取得しましょう。

* P17以降の『付録』に、ログ種別とシステム別のログ活用シーンをまとめているので、参考にしてみてください。

一方で、特定システムのログを取得していない状態では、万が一インシデントが発生した際に、その検知に漏れが生じたり、詳細な原因究明が行えない場合があります。
そのため、より正確に検知や原因特定を行うためには、全てのシステムのログを収集しておくことが理想的です。
最終ゴールとしては、全システムのログ管理体制を目指してみてください。

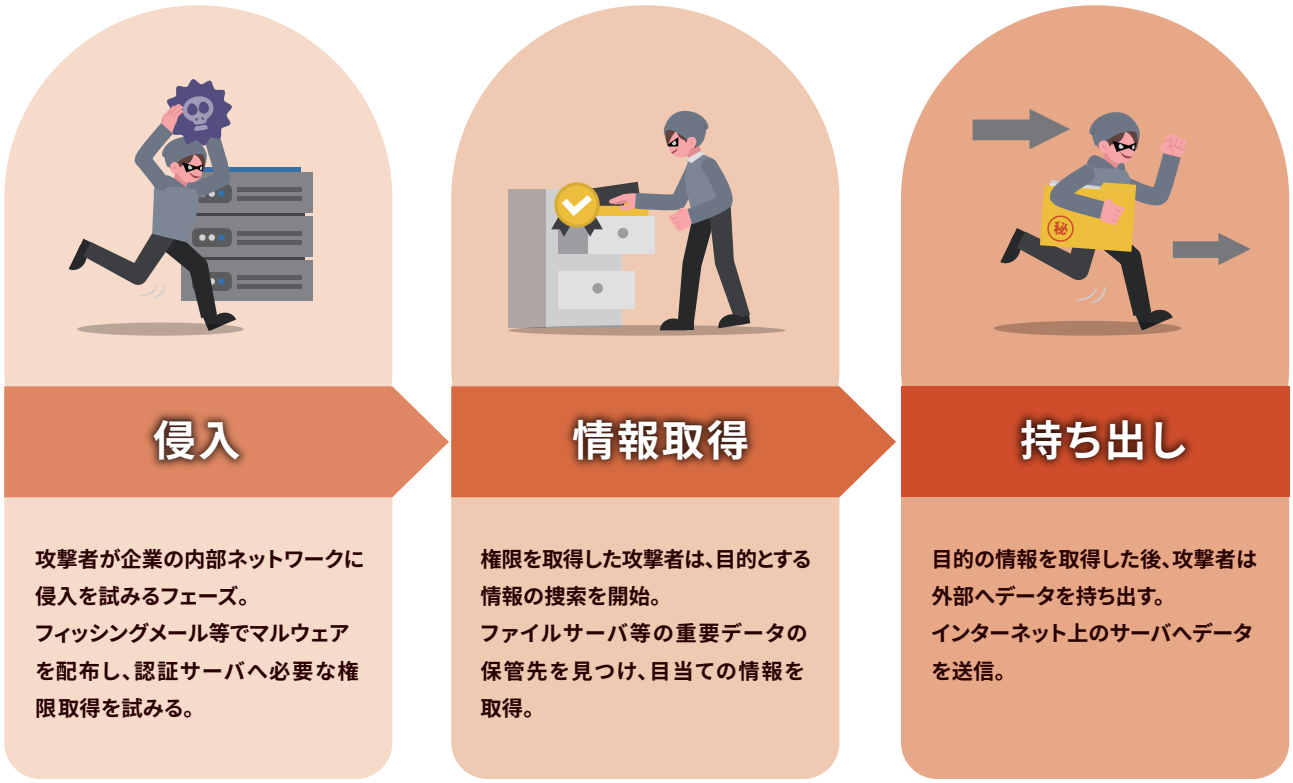


ログ管理は、収集・保管したログを適切なポイントで監視することで、効果を発揮することができます。
以降は、特に重要な具体的監視ポイントを、5つの活用シーン別に見ていきましょう。

ログ監視ポイント

サイバー攻撃対策

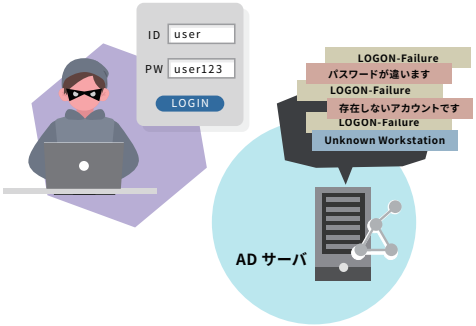
サイバー攻撃を受けた際、被害状況や影響範囲の調査などの事後対応にログが有用であることはもちろん、ログを監視することで、攻撃を受けた事実にいち早く気づき、被害を最小限に抑えるための早期対応を行うことが可能になります。
サイバー攻撃には以下のような攻撃段階があります。



攻撃段階に応じてポイントを絞ってログを監視することで、効果的対策を施すことができます。次のページで具体的な監視ポイントをご紹介します。

ログ監視ポイント

侵入

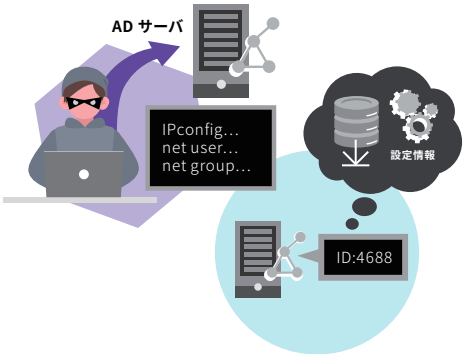


不審なログオン試行や、不正な特権利用を監視することで、侵入の初期段階での対応を可能にし、被害を最小化する効果が見込めます。

重要な監視ポイント

- ☑ 大量のログオン失敗
- ☑ 管理権限への昇格
- ☑ アカウントの作成
- ☑ ポリシーの変更

情報取得



通常は起こりえないファイルアクセスやPowerShellの実行があった場合、不正アクセスを疑います。
これらを監視することで情報漏えいを検知します。

重要な監視ポイント

- ☑ 大量のファイルの読み込み
- ☑ 大量のファイル名変更
- ☑ PoweShellの実行
- ☑ 深夜休日のファイルアクセス

持ち出し

サイバー攻撃は、手に入れた情報を外部サーバに送信する場合があるため、インターネット出入口の通信ログを監視することがポイントです。

重要な監視ポイント

- ☑ 未許可ポートの利用
- ☑ IP別の大量アップロード/ダウンロード
- ☑ WEB利用状況の監視

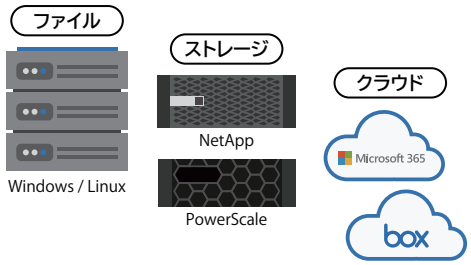
ログ監視ポイント

内部不正対策

内部不正による情報漏えいが生じてしまった場合、該当者の特定や流出情報の確認に時間を要してしまうと、社会的な信用失墜にも繋がりかねません。
素早い原因究明には、ログ管理が必要不可欠です。

また、ログによる監視は内部不正の抑止力ともなります。
下記の三視点での監視が有効です。

1 サーバ

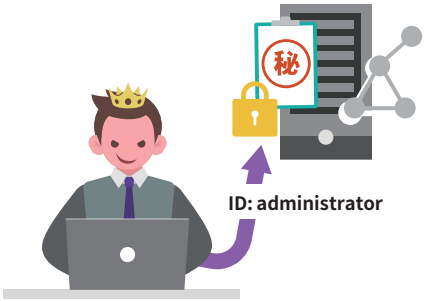


どんな流出経路であっても起点となるのは重要データが保管されている「サーバ」です。
サーバ内の「重要データへのアクセス履歴」を監視することは、内部不正の防止策として最も効果的でベーシックな手段です。

重要な監視ポイント

- ☑ 重要フォルダへのアクセス状況
- ☑ 大量のファイル読み込み
- ☑ 大量のデータコピー
- ☑ ファイル/フォルダのアクセス権変更

2 特権使用



特権ユーザーは、一般ユーザーでは本来見ることができないファイルを閲覧することができるため、特権が悪用されて いないかのログ監視をすることが重要となります。

重要な監視ポイント

- ☑ 特権管理者のファイルアクセス
- ☑ 特権管理者のデータベース操作

3 退職予定者

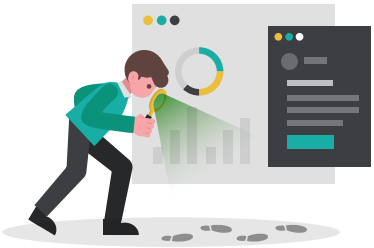
退職予定者が在籍中に不正行為をしていないかを監視 します。
重要データのコピー、クラウドストレージへのアップロード/ダウンロード、共有先の履歴、大量のプリント履歴など、時系列で行動を追跡することが有効です。

重要な監視ポイント

- ☑ 転職サイトの閲覧
- ☑ 退職予定者のファイルアクセス
- ☑ 外部デバイスへのファイルコピー
- ☑ 退職予定者のメール送信

ログ監視ポイント

監査報告



監査は、業務が決められた手順に従って適正に行われているかを確認できる有効な手段であるだけではなく、第三者への安全性のアピールにもなります。
ログにより、システムが不当に変更されていないこと、システムの変更を実施した際の過程が適切に記録・保存されていること、特権管理者操作の正当性、を証明することが求められます。

重要な監視ポイント

- 重要フォルダへのアクセス状況
- ファイル/フォルダのアクセス権変更
- 特権管理者操作
- ユーザアカウントの追加/削除

勤務実態の把握

社内PCの認証履歴や電源ON・OFFのログを勤怠管理に活用することで勤怠管理システムに手入力する手間もなく、客観的に業務実態を把握することができます。
さらには、従業員が業務に関係のない作業をしていないかどうか、業務の偏りがないかどうかも判断でき、業務効率化をも推進することもできます。

重要な監視ポイント

- PCログオン/ログオフ
- SNS/動画サイトの閲覧
- メール送受信履歴
- 深夜休日のPC操作

障害原因調査

社内で稼働しているシステム・ハードウェアなどのシステム/エラーログを集約することで、プログラムのどの部分で障害が起きたのか、原因調査や復旧に活躍します。

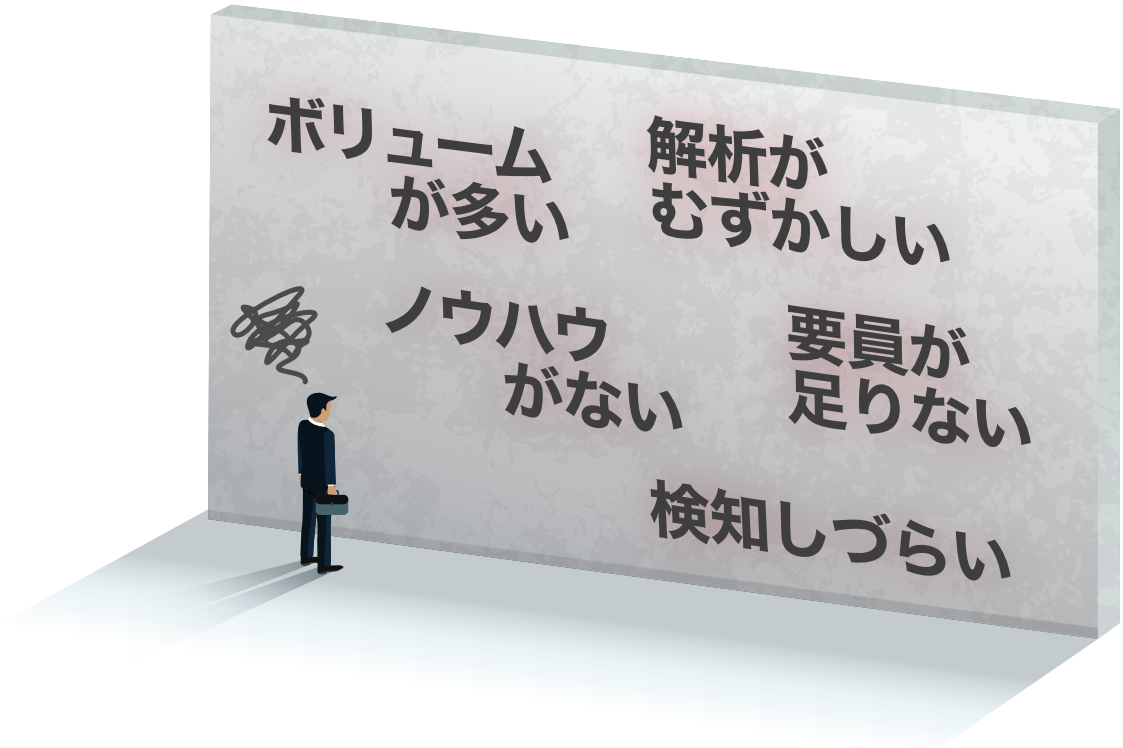
重要な監視ポイント

- ネットワーク機器のエラー
- アクセスポイント機器のエラー

ログ管理はむずかしい？

「ログ管理はむずかしい」という声をよく聞きます。
ここまで、ログ管理における重要な監視ポイントを紹介してきましたが、いざ各ITシステムのログを取得し監視してみても、その管理は簡単なものではありません。
監査やグループ企業からの指摘によりログ取得が急務となり、目的を整理できないままログを「とりあえず保管」しているケースも多く見られます。
もちろん、有事の際の「証拠」としてログを保管しておくことは必要不可欠です。しかし、ログ管理の本来の目的は「ITシステムで何が起きたのかを把握する」こと、すなわち、ログとして記録されているさまざまな事象から、「いつ」「何が」発生したのか、を理解することです。
そのため、理解するためのログの分析が、ログ管理の要であると言えます。

しかし、ログはシステムごとにフォーマットや取得できる情報が異なり、取得すると莫大なデータ量にもなるため、たとえ監視ポイントがわかっていたとしても、手作業で分散したログを収集し膨大なデータを分析することは困難を極めます。
また、システムから吐き出される生のログは複雑で、解析には専門知識やノウハウが必要となります。
さらには、異常の迅速な検知には常時ログを監視し分析し続けることが必要ですが、それも人的リソースを考えると非現実的です。
つまり、ログ管理における分析の難しさが、「ログ管理はむずかしい」と言われる所以なのです。



ログ管理ツールの活用を

前述の通り、収集した様々なシステムのログを分析することは極めて困難であり、システム担当者にとっても高負荷です。そこで役立つのが、ログを一括で収集・保管し、簡単に分析することができるログ管理ツールです。

ログ管理ツールを活用することで、ログ管理による効果を得られるようになります。
以下が、ログ管理ツールに求められる重要機能です。

ログ取得

様々な種類のログを収集し、見やすい形に整形して出力、指定されたサイズやファイル数に分けて保管する機能は、ログ管理のメイン機能です。

レポート分析

収集したログは、目的に応じて加工・分析することで、セキュリティインシデントやシステム障害の調査、業務改善等に役立てることができます。

アラート監視

ログを常時監視し、異常を検知した際にはアラート通知を行います。
それにより、外部からの攻撃や内部不正、障害などのトラブルを早期に発見できます。

安全な保管

重要データであるログは、暗号化等を用いて改ざんから守る必要があります。
また、保管期間はセキュリティーポリシーに沿って任意で設定できることが大切です。

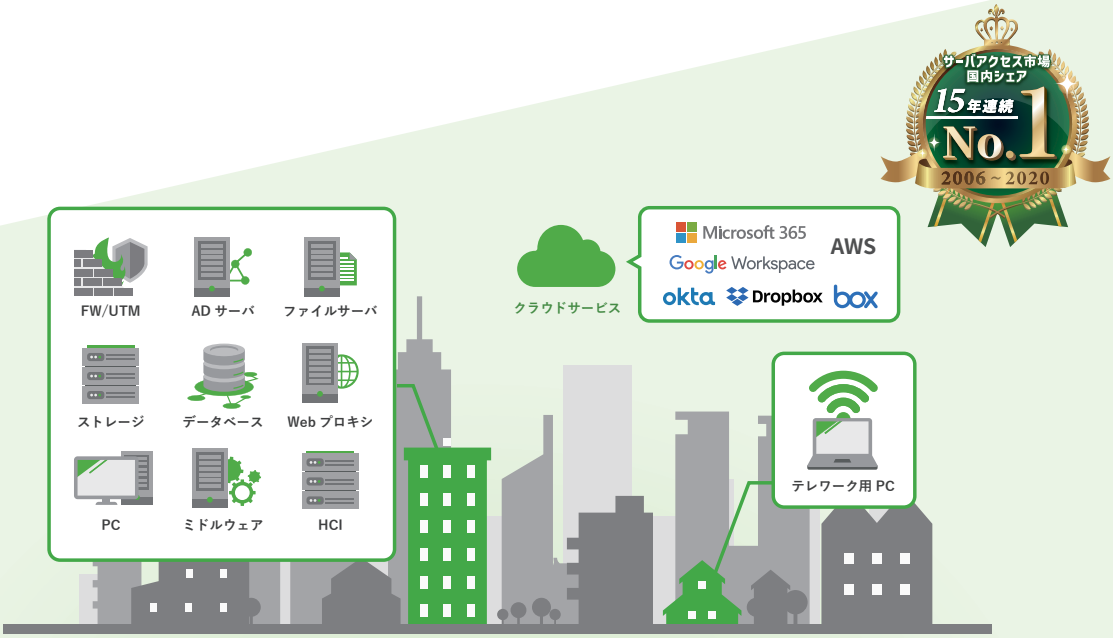
しかしながら、これらの機能を備えていても、あらゆるログ管理の目的に網羅的に対応できるツールでなければ、無駄な分散投資となってしまいます。

ログ管理のむずかしいをカンタンに！

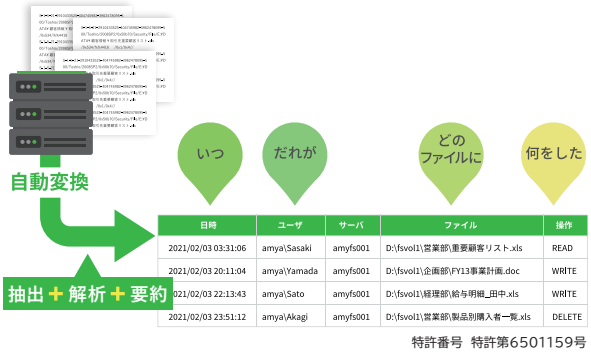
網屋のALog

網屋のALogシリーズなら、あらゆるログを活用して、サイバー攻撃対策/内部不正対策/監査報告/勤務実態の把握/障害原因調査、全てに網羅的に対応することができます。
ALogは、多様なITシステムのログをエージェントレスで自動集約・運用監視するログマネジメントソリューション。

前述のログ管理ツールに求められる機能はもちろん、特許を取得した独自のログ翻訳変換・整形技術をはじめとした、ログ管理の「むずかしいをカンタンに」する技術により、専門知識やノウハウがなくとも、高度なログ活用を実現できます。



むずかしいをカンタンにする 4つのポイント

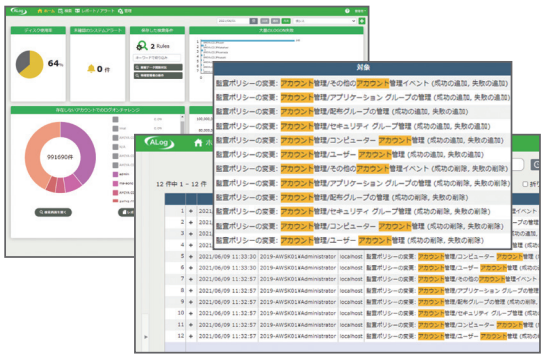


日時	ユーザ	サーバ	ファイル	操作
2021/02/03 03:31:06	amya\Sasaki	amyfs001	D:\fsvol1\営業部\重要顧客リスト.xls	READ
2021/02/03 20:11:04	amya\Yamada	amyfs001	D:\fsvol1\企画部\FY13事業計画.doc	WRITE
2021/02/03 22:13:43	amya\Sato	amyfs001	D:\fsvol1\経理部\給与明細_田中.xls	WRITE
2021/02/03 23:51:12	amya\Akagi	amyfs001	D:\fsvol1\営業部\製品別購入者一覧.xls	DELETE

特許番号 特許第6501159号

特許取得の翻訳変換技術

データアクセスの記録を複雑で膨大なシステムログから抽出し、特許(第6501159号)取得のログの翻訳変換技術を使って、見やすい「アクセスログ」にまとめます。



直感的に操作できるGUI

検索、レポート、管理機能全てをまとめて直感的に運用可能。
検索項目を意識せずにフォーマットの異なるログを横断的に検索できます。

目的別自動検知パック

目的別に“異常”を自動検知するレポート/アラートテンプレート集。
複雑な要件定義不要で、導入したその日からログ活用をスタートできます。

AIが異常を自動検知

ユーザーごとの行動傾向をAIが自動学習。
いつもと違う行動を危険度に応じてスコアリングし、不正や攻撃の予兆を検知します。

ALog活用術

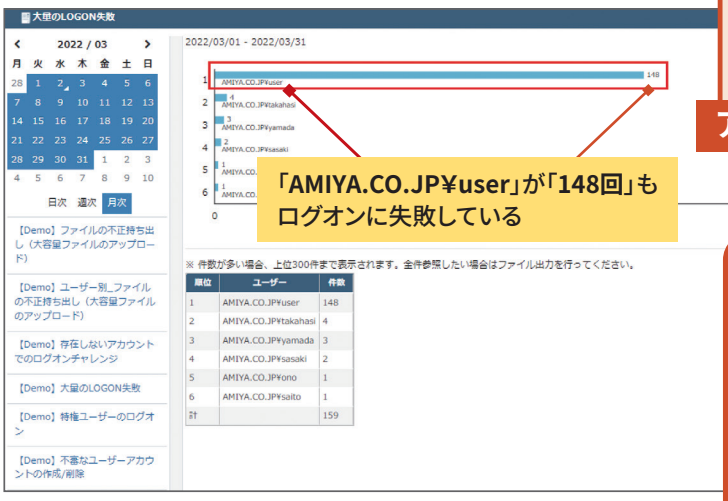
サイバー攻撃対策

ex. 不審なログオン試行からサイバー攻撃を検知

短時間で大量にログオン失敗ログが出力される場合、該当端末がマルウェアに侵入されていたり、攻撃者に乗っ取られようとしていたりすることを意味し、機械的なログオンチャレンジが行われていることが分かります。

ログオンに成功しない限りドメインへの侵入は完了していませんが、該当端末の調査を早期に行う必要があります。

レポート



アラート

- メールサービス
- Syslog通知
- API連携

slack
Chatwork
TEAMS
など

＝TIPS＝

API連携機能を利用すれば、チャットツールに即時アラート通知。
また、Syslog通知機能では、EDRをはじめとするエンドポイントツールやネットワーク機器にアラート情報を連携することで、不審な端末をネットワークから遮断することも可能！

サイバー攻撃自動検知パック

IPAやJPCERTガイドラインに対応。
典型的な攻撃パターンの証跡内容と最も効果的な監視項目を分析してパック化。

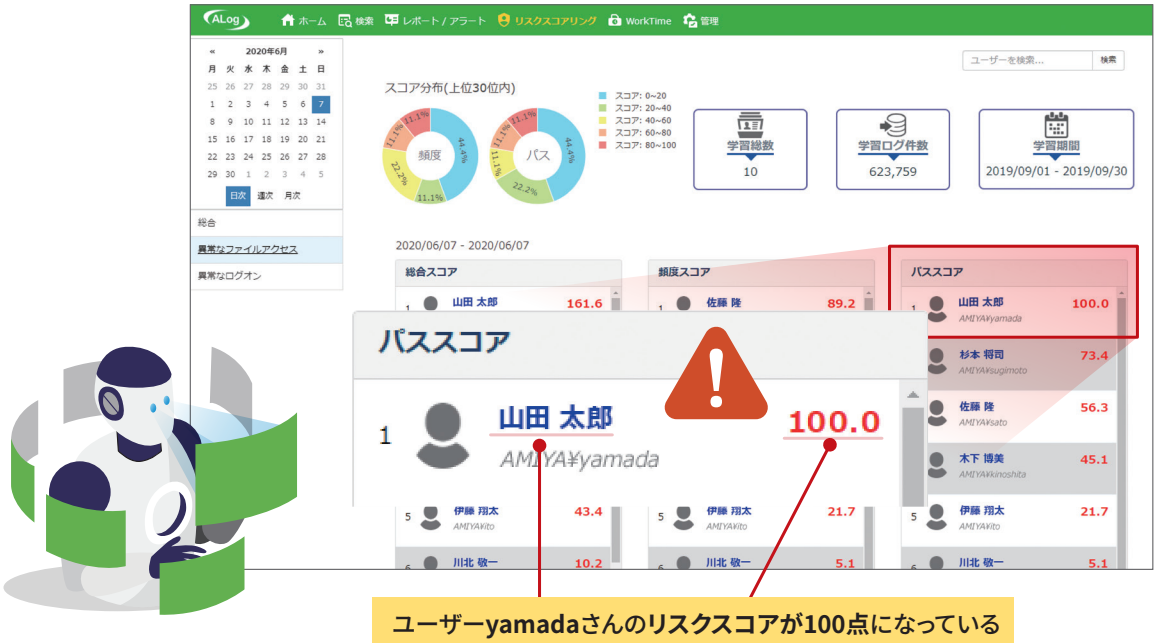
ALog活用術

内部不正対策

ex. 普段と異なるファイルアクセスから内部不正を検知

営業部の山田太郎さんが、普段アクセスしない開発部のフォルダにアクセスしている、といった普段と異なる不審な行動をAIが自動でリスクスコアリングし、内部不正の予兆を可視化します。

営業部の山田太郎さんの
フォルダアクセス



ユーザーyamadaさんのリスクスコアが100点になっている

内部不正AIパック

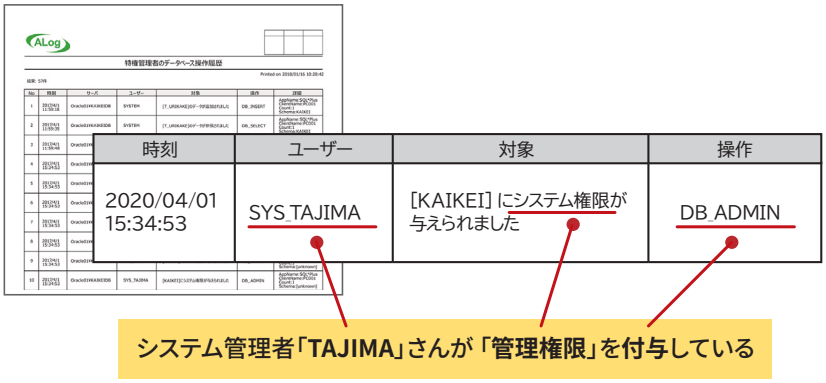
内部不正対策に特化したレポート内容を標準搭載。
事前にセットするだけで、AIが自動的に異常を検知。

ALog活用術

監査報告

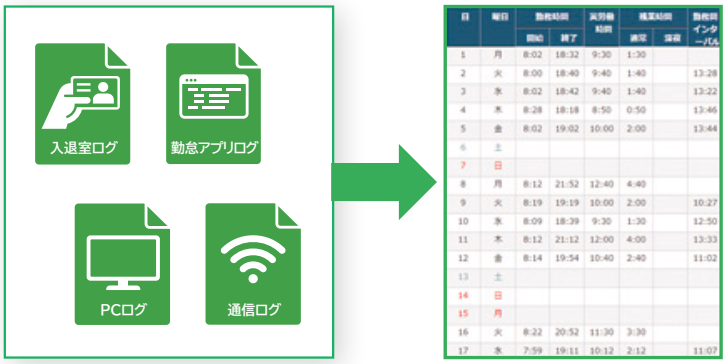
ex. 管理者操作の正当性を証明

ドメインコントローラやファイルサーバの操作履歴を取得して自動レポートを作成します。
中でも、管理者の操作履歴を監視することは、特権の不正利用や悪用を疑われた場合に、必要な作業であったことの証明にも繋がります。



勤務実態の把握

ex. 勤務実態に即した勤怠表を作成

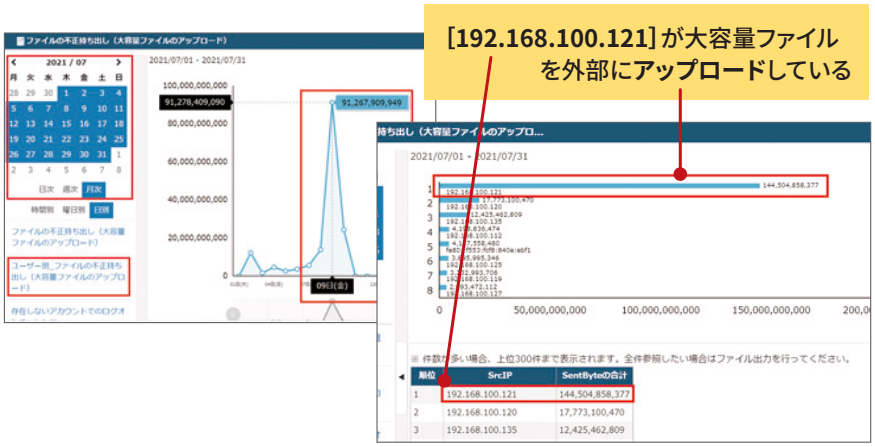


オプションツールWork Timeによりあらゆるログから勤怠表を自動作成します。
また、残業が多い社員をランキング化したり、業務インターバルが短い社員を確認したりすることもできます。

障害原因調査

ex. 通信のボトルネックを特定

ネットワーク機器の通信ログを確認することで、特定ユーザーが大容量データをダウンロードしている（ネットワーク回線が重くなる要因のひとつ）などのアクセス実態を把握することができます。



導入事例

テレワークの情報漏えい対策に。「いつもと違う」リスクをAIが自動判定

株式会社ミュゼプラチナム 様

課題

① ログ監査のリソース不足

② 不審な挙動を検知したい

③ 特権IDの正当性証明

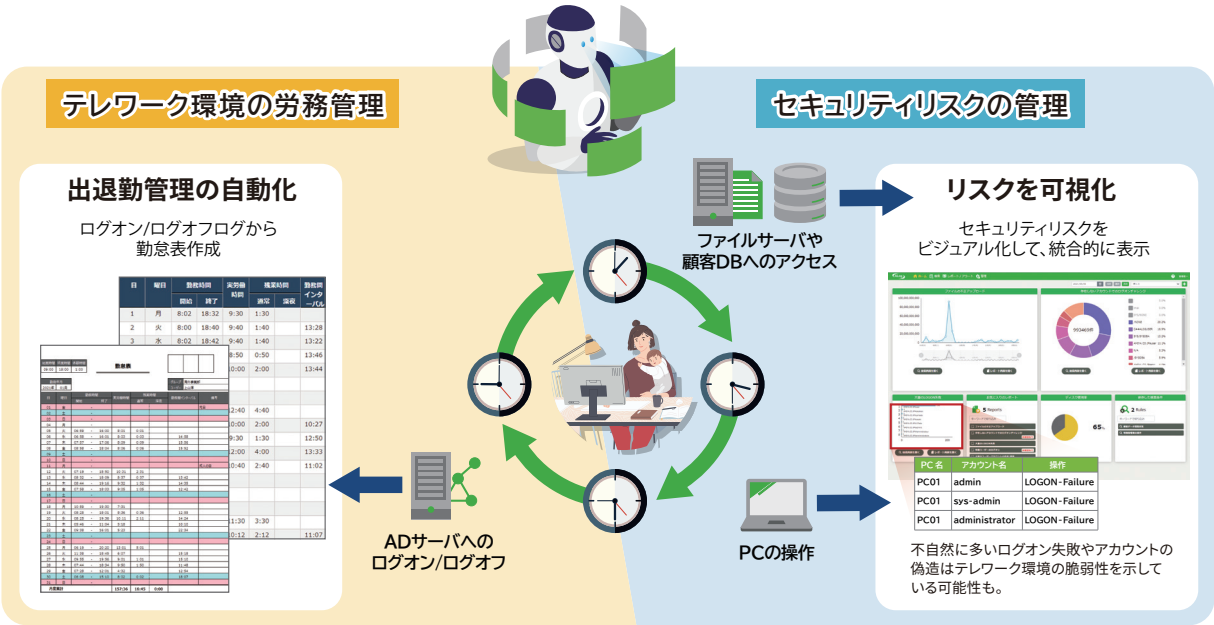
効果

① ログを集約しログ監査対応業務を自動化

② AIによるリスクの可視化で不審な挙動を検知

③ 特権IDの操作ログ取得、レポート化で潔白証明

ALog ワークライフバランスとセキュリティの両立をサポート



おわりに

はじめよう、効果の見えるログ管理

本書では、ログという資産がどのように活用できるのかを紹介してきました。
ログは収集・保存するだけでは意味を成しません。適切に管理し、いつでも分析ができる基盤を整えておくことではじめて効果を発揮し、サイバー攻撃対策/内部不正対策/監査報告/勤務実態の把握/障害原因調査など、幅広いシーンで活用し、様々な企業の課題を解決することができます。
効果の見えるログ管理を、はじめてみませんか？

本書のまとめ

- ログはあらゆるシーンで活用できる
- 目的に応じたログ管理が必要
- ログは適切なポイントで監視をすることで活用できる
- ログ管理の要は「分析」
- ログ管理にはログ管理ツールの活用を

付録1 ログ種別と活用シーン

種類	記録される内容	活用シーン
操作ログ	パソコンやスマートフォン等デバイス内の操作履歴です。基本的なログの一つで、アプリケーションの操作、ファイルやフォルダの作成、移動、閲覧などもこの操作ログに含まれます。操作ログは、操作ミスや不審操作のチェック、エラー調査や性能測定などで有用です。	サイバー攻撃対策 勤務実態の把握 障害原因調査
認証ログ	パソコンからシステムやネットワークへログインした履歴です。認証ログでは、認証失敗の記録もされ、ログイン失敗が多いユーザーや業務時間外のログインが多いユーザーなどを要注意リストに入れ、動向を注視できます。ブルートフォースアタック（総当たり攻撃）等のサイバー攻撃が行われた痕跡なども発見できます。	サイバー攻撃対策 勤務実態の把握 内部不正対策 監査報告 障害原因調査
アクセスログ	パソコン・業務システム・Webサイトなどへのアクセスに関する情報のログです。誰がいつどこでアクセスし、データの送受信サイズはどのようなものだったかを記録します。	サイバー攻撃対策 内部不正対策 監査報告 障害原因調査
イベントログ	システムやアプリケーションで生じた現象・動作を記録したログです。異常なイベント、ファイルへのアクセス、ログオン・ログオフなどの情報が各システムやアプリケーションごとに記録されます。	サイバー攻撃対策 障害原因調査
通信ログ	パソコンとサーバ間の通信の履歴です。どのような通信内容だったか、いつ開始され終了したか、どのパソコンとサーバ間で通信が行われたかといった内容を確認できます。端末とサーバーのマシン名やIPアドレス、通信時間などが記録されます。	サイバー攻撃対策
エラーログ	パソコンのシステムやアプリケーション内で発生したエラーを記録するログです。 エラーの内容、エラーが発生した日時や発生原因などが記録されています。	障害原因調査
設定変更ログ	権限を持つ担当者がシステムやファイル・ファルダの設定を変更した際に記録されるログです。Googleドライブの共有範囲の権限変更などの際に記録されるログも、この設定変更ログに含まれます。機密ファイルの持ち出しや改ざんなどの特定・追跡に活用されます。	サイバー攻撃対策 内部不正対策 監査報告
印刷ログ	複合機などの使用履歴です。印刷枚数、印刷したファイル名、印刷した日時などが詳細に記録されます。社外持ち出しなど、社内からの情報漏えいなどの原因究明などに活用されます。	内部不正対策
入退室ログ	特定の部屋への入室・退出記録です。扉上部に設置されたセンサー、またはICカードなどからログを収集し、不正侵入や従業員の不審な動向などをチェックします。	内部不正対策 勤務実態の把握

付録2 システム別のログ活用

システム	活用シーン	記録内容例
Firewall	サイバー攻撃対策	- HTTP、HTTPS等のプロトコルによる外部への通信 - ぜい弱なPCや内部サーバの探索 - 通過した通信、または拒否された通信
	障害原因調査	- ネットワーク障害検知 - 通信ボトルネックの特定
IDS/IPS	サイバー攻撃対策	-IDS/IPSが検知した、また検知から漏れた通信
プロキシサーバ	サイバー攻撃対策	- Webプロキシサーバを介さない外部への通信 - HTTP、HTTPS等のプロトコルによる外部への通信 - Webサーバが利用者から受け取った入力内容
	内部不正対策	- 転職サイトの閲覧
	勤務実態の把握	- SNSサイトの閲覧
DHCPサーバ	サイバー攻撃対策	- 被害範囲の特定
DNSサーバ	サイバー攻撃対策 内部不正対策	- HTTP、HTTPS等のプロトコルによる外部への通信 - データの異常アップロードサイズ/回数
メールサーバ	サイバー攻撃対策	- なりすましメール - 実行ファイル添付メール
Active Directory	サイバー攻撃対策	- ファイルサーバなどへのアクセスや権限の奪取 - 情報システムへのログイン、ログアウトなど認証の成功や失敗の記録 - 特権管理権限の利用 - 大量のログイン失敗 - ユーザアカウントの作成/削除
	勤務実態の把握	- ログオン/ログオフ
	監査報告	- 特権管理権限の利用
ファイルサーバ	サイバー攻撃対策	- ランサムウェアによる被害範囲の特定 - ファイルの参照や、編集などの成功や失敗の記録
	内部不正対策	- ファイルの参照や、編集などの成功や失敗の記録 - 退職予定者のファイルアクセス
データベースサーバ	サイバー攻撃対策 内部不正対策	- 規定外ツールによるDB操作 - アクセス失敗したユーザー - 発行されたSQLクエリ - アクセス頻度 - DBスキーマの変更・削除 - アカウント変更・削除
アプリケーション	サイバー攻撃対策	-発生したエラーの記録 -ユーザーによる予期しない操作の成功や失敗の記録
	内部不正対策	-禁止サイトへのアクセス試行・履歴 -外部デバイスへのコピー履歴
PC	勤務実態の把握	-PCの作動状況

サーバアクセスログ
ALog ConVerter®

ALog ConVerter は、重要データへのアクセス記録をエージェントレスで取得する製品です。重要データが格納されるサーバ側からログを取得することにより、ストレスのない効率的なログ管理を実現します。

統合ログ
ALog EVA

ALog EVA は、ALog シリーズの守備範囲を飛躍的に拡張します。
高度な専門技術を要求する従来の統合ログ製品から一線を画した手軽さと柔軟さを備えた新しい統合データマネジメントツールです。

詳しい製品のご紹介、評価版のご依頼は以下にお問い合わせください。

お問い合わせ先

株式会社網屋
データセキュリティ事業部

TEL：03-6822-9996　E-mail： bv-sales@amiya.co.jp

詳しい製品概要資料はこちら ›

開発元

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 11F
TEL: 03-6822-9999 FAX: 03-6822-9998
https://www.amiya.co.jp/