ALog

AIが防ぐ未来の情報漏えい

内部不正対策の新常識とは

AMIYA

目次

内部不正による情報漏えいの脅威 3P
内部不正はなぜ起こるのか 4P
元従業員による不正持ち出し
ケース1. 遠隔ソフトにより営業情報を取得 5P
ケース2. 営業管理ツールから顧客情報を不正閲覧 6P
内部不正をログで防ぐ3つのポイント 7P
時代の変化とともに広がる監視対象 8P
ALogで重要データのアクセス履歴を監視 9P
専門知識不要
わずか3ステップで内部不正対策を自動化 10P
AIが過去の行動から未来の不正を自動検知 11P
ALog × Microsoft 365のログで退職予定者の行動を監視 12P
その他内部不正に有効なログの活用例 アクセスを監視 13P
その他内部不正に有効なログの活用例 流出を監視 14P
内部不正・外部攻撃の両方に対応できるのはALogだけ 15P

ハッカー? 産業スパイ?
いいえ、情報漏えいリスクは常にあなたの足元に。

「組織の機密情報が盗まれた」と聞くと、一般的にイメージしやすいのは第三者（ハッカー）による外部攻撃や、産業スパイの潜入による盗難ではないでしょうか。まるで映画のような話ですが、こうした情報漏えいは、日々世界中で発生しています。

しかし、情報漏えいの原因は外部攻撃だけではありません。
「退職予定者が社内の技術情報を盗み、ライバル企業に転職した」
世間を騒がせた内部不正はなぜ起こったのか。
そして、どうすれば防ぐことができたのか。

次に狙われるのは、あなたの組織かもしれません。

内部不正による情報漏えいの脅威

内部不正による情報漏えいとは、私怨や金銭目的で組織内部の人間が機密情報を持ち出し、外部に流出してしまうことを言います。中には、うっかりミスなどの「ヒューマンエラー」や、ルール違反と知りながら「業務上やむを得ず行う違反」など、悪意のない漏えい事件も含みます。
在宅勤務が急速に浸透した2020年は、監視の目が届きにくいことから、オフィス勤務と比べて「内部不正による情報漏えい」インシデントが発生しやすいと言われています。

情報セキュリティ 10 大脅威 2020 「組織」向けの脅威の順位

順位	「組織」向け脅威
1	標的型攻撃による機密情報の窃取
2	内部不正による情報漏えい
3	ビジネスメール詐欺による金銭被害
4	サプライチェーンの弱点を悪用した攻撃
5	ランサムウェアによる被害
6	予期せぬ IT 基盤の障害に伴う業務停止
7	不注意による情報漏えい
8	インターネット上のサービスからの個人情報の窃取
9	IoT 機器の不正利用
10	サービス妨害攻撃によるサービスの停止

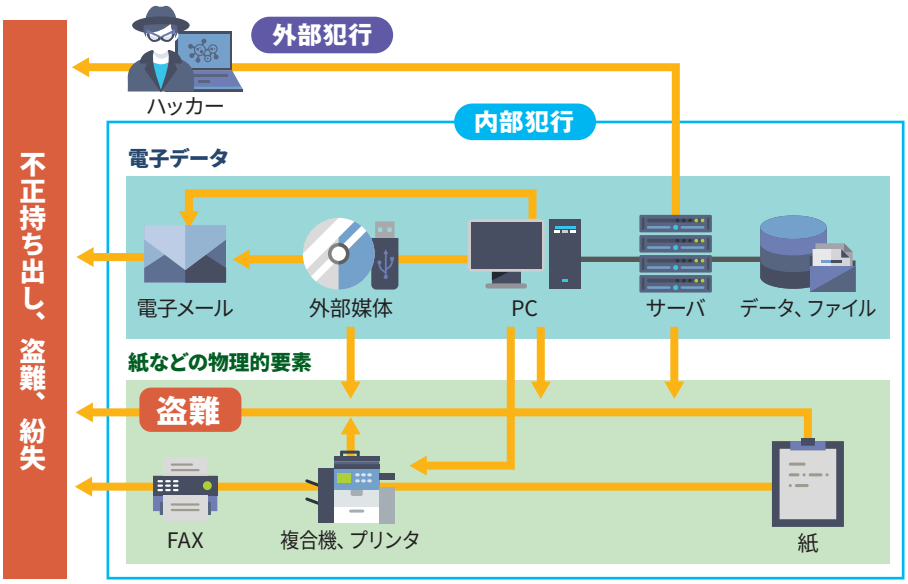
出典：IPA「情報セキュリティ10大脅威2020」P22より一部抜粋
https://www.ipa.go.jp/security/vuln/10threats2020.html

「損害賠償による経済的損失」、「社会的信用の失墜」など、情報漏えいが起こると組織はその根幹を揺るがしかねないほど甚大な被害を受けます。

内部不正はなぜ起こるのか

「重要情報のない組織」は存在しません。情報漏えいは、どの組織にも日常的に起こりうるリスクです。その流出経路は多岐にわたるものの、手口（要因）として大半を占めるのが「元従業員による不正持ち出し」「誤動作・紛失などのヒューマンエラー」と言われています。

情報の流出経路



元従業員による不正持ち出し

競合他社への転職（ヘッドハンティングなど）や、組織に不満があった故の退職など、故意に情報を取得し悪用。この場合、転職先への手土産、報復や売買による金銭取得などが動機にあたります。

誤動作・紛失などのヒューマンエラー

「顧客情報を誤って外部にメール添付」、「酩酊しパソコンやUSBを紛失」など、悪意なく発生するインシデント。もっとも身近な情報漏えいと言えます。

次章では、元従業員による具体的な被害事例を紹介します。

元従業員による不正持ち出し

ケース1. 遠隔ソフトにより営業情報を取得

流出経路 遠隔操作、メール送付

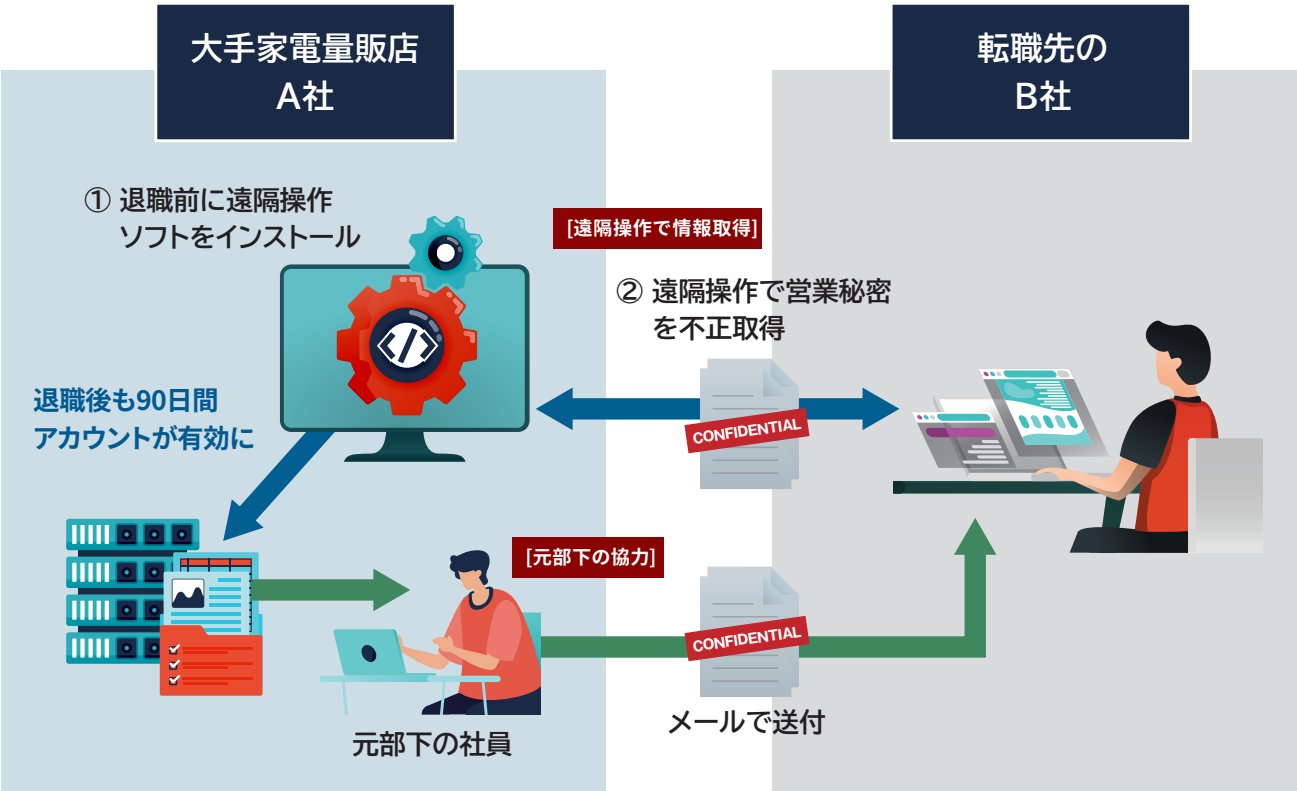
概　要 大手家電量販店A社の元社員が退職後に二通りのルートから不正に機密情報を取得し、転職先のB社で利用していた。

[遠隔操作で情報取得]

退職前に遠隔操作ソフトを無断でインストール。
退職後、転職先のPCから遠隔で不正ログインし、機密情報を取得。通常、ログインにはアカウントが必要だが、A社は事務手続きの都合で退職後も90日間アカウントを有効にさせていた。

[元部下の協力]

かつての部下である現役社員に依頼し、重要データをメール送付。



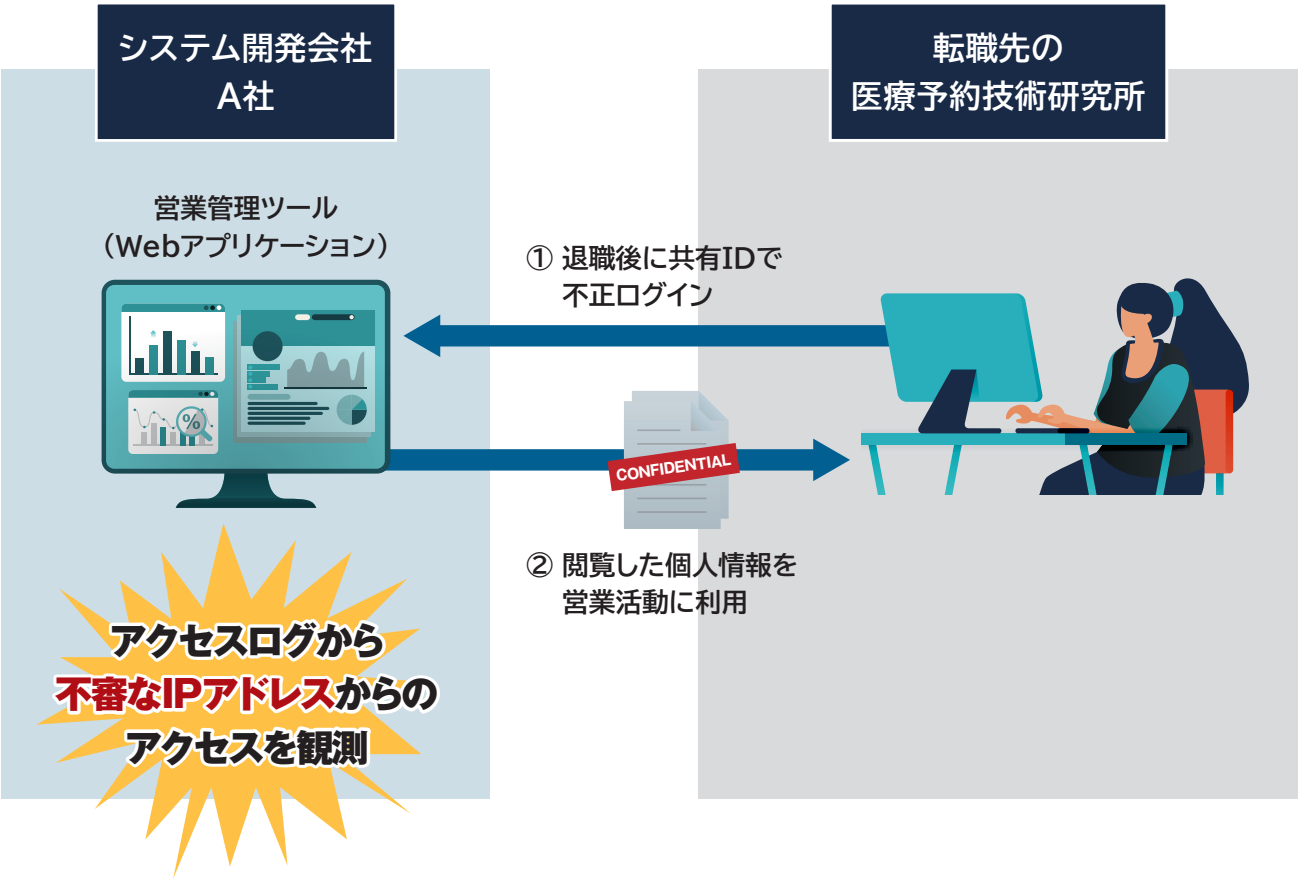
元従業員による不正持ち出し

ケース2. 営業管理ツールから顧客情報を不正閲覧

流出経路　Webアプリケーション（営業管理ツール）

概　要　システム開発会社、A社の元従業員が退職後に営業管理ツールに不正ログインし、顧客情報を閲覧。転職先である医療予約技術研究所の営業活動に利用していた。

発　覚　A社の取引先から「不審な営業活動があった」との指摘があり問題が発覚。
調査を行ったところ、製品の問い合わせ情報を管理している営業管理ツールのアクセスログに、不審なIPアドレスを発見。共用IDによりログインされていたことが判明。



内部不正をログで防ぐ3つのポイント

内部不正対策をするうえで従業員各人の行動を把握する必要がありますが、なにも監視カメラを設置する必要はありません。

システムの操作履歴、つまり「ログ」の取得・監視が有効です。

1. アクセスログの取得および監視

アクセスログの監視とは、重要データに対し「いつ、誰が、何をしたのか」を把握すること。
データの入出力やユーザーの行動をログ監視することで情報漏えいを未然に防ぐことができる他、有事の際には証跡となります。

2. 特権IDの管理・監視

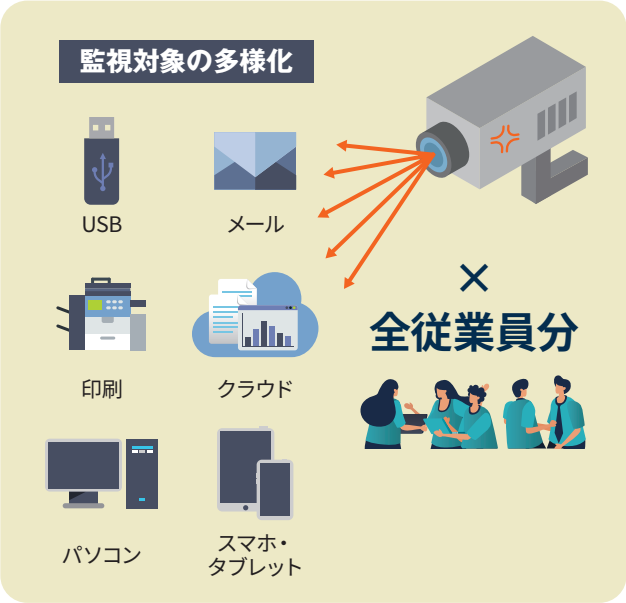
特権IDとは、システムの運用・構成の変更など、特別な権限を有するID、いわゆるスーパーユーザーです。一般ユーザーでは本来見ることができないファイルを閲覧することができるため、特権IDが悪用されていないかのログ監視をすることが重要となります。

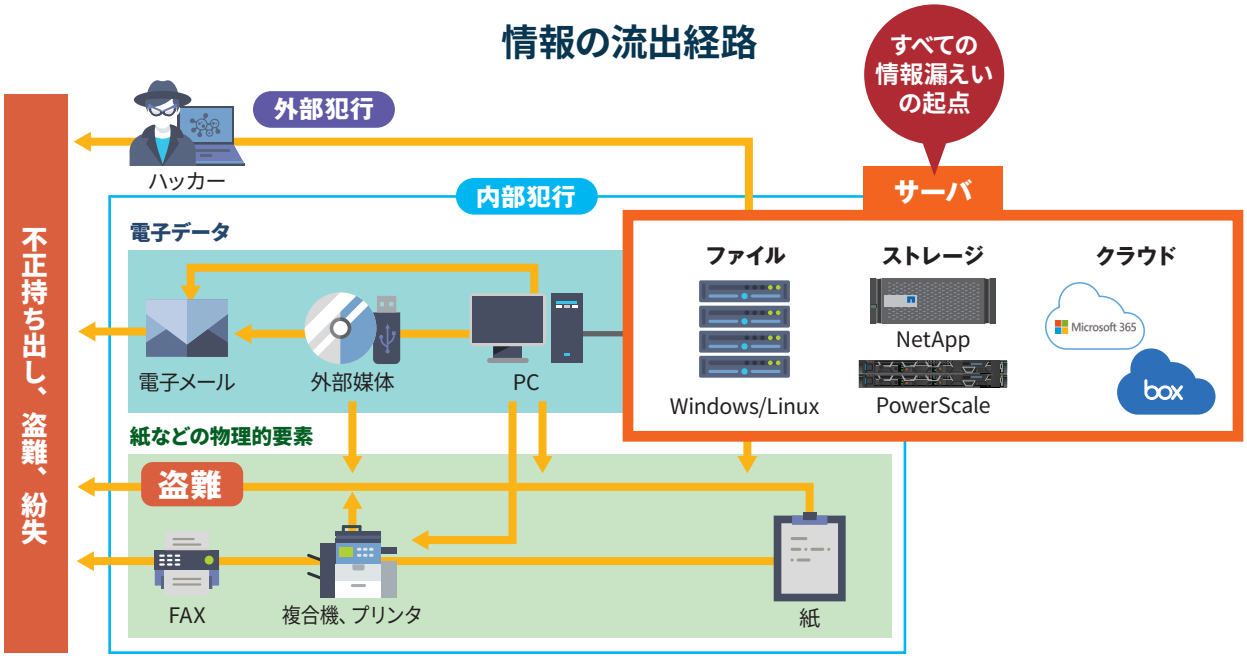
3. 退職者予定者の監視

退職予定者が在籍中に不正行為をしていないかを監視・検知します。重要データのコピー、クラウドストレージの履歴、大量のプリント履歴など、時系列でレポート化することが有効です。

時代の変化とともに広がる監視対象

デスクトップPC、ノートPCやスマートフォンなどのデバイスから、メール、クラウドストレージ、アプリケーション……テレワークが普及しつつある今、働く場所やデバイスを問わない勤務状況は今後ますます増加します。
ログ監視は非常に有効ですが、その一つ一つに目を光らせるのは、膨大な手間と費用がかかり、現実的ではありません。





「すべての流出はサーバに通ず」

しかし図の通り、流出経路がいずれであっても起点となるのはすべて、重要データが保管されている「サーバ」です。重要なのは効率的で効果的な監視。

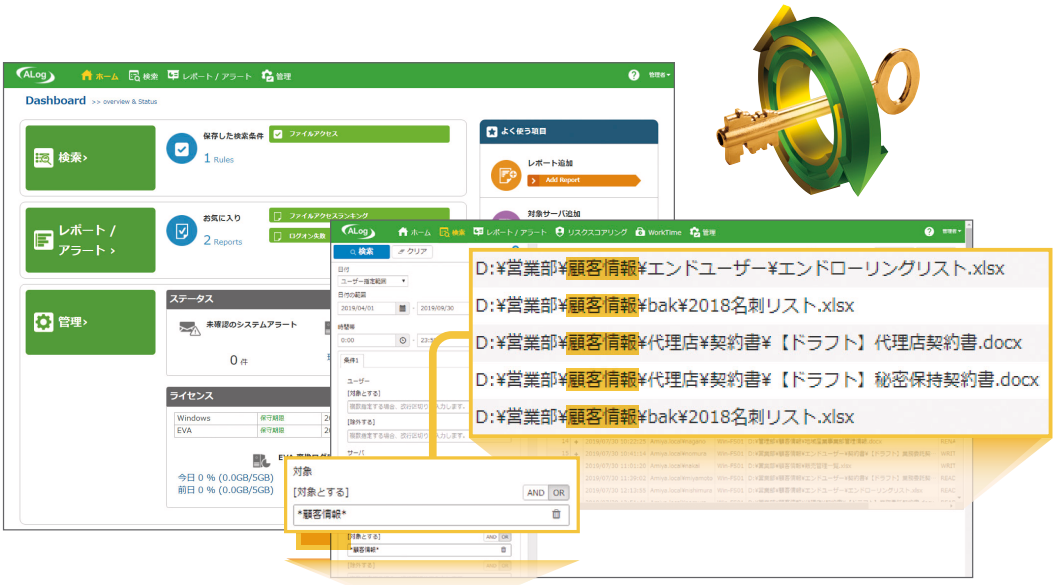
オンプレミス、クラウド問わず、サーバ内の「重要データへのアクセス履歴」を監視することは、内部不正の防止策としてもっとも効果的でベーシックな手段です。

ALogで重要データのアクセス履歴を監視

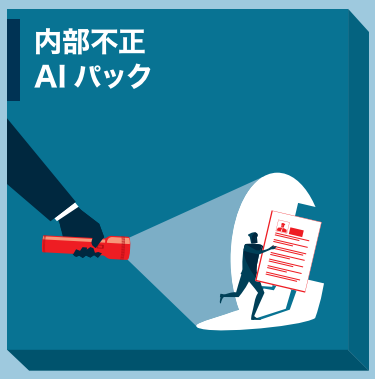
ALogは国産のログマネージメントソリューション。独自の変換技術により、複雑難解なログをエージェントレスで取得し、「いつ／誰が／何をしたか」が一目でわかる形式に翻訳変換します。直感的に操作できるGUIのため、専門知識は必要ありません。

複雑なログデータを実際の行動に翻訳変換

直感的なGUIで誰でも簡単操作



専門知識不要
わずか3ステップで内部不正対策を自動化

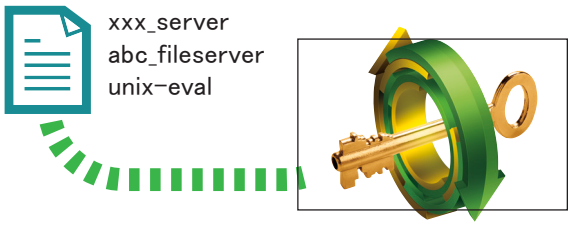


内部不正AIパック

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。
要件定義/設計/構築作業の必要がありません。

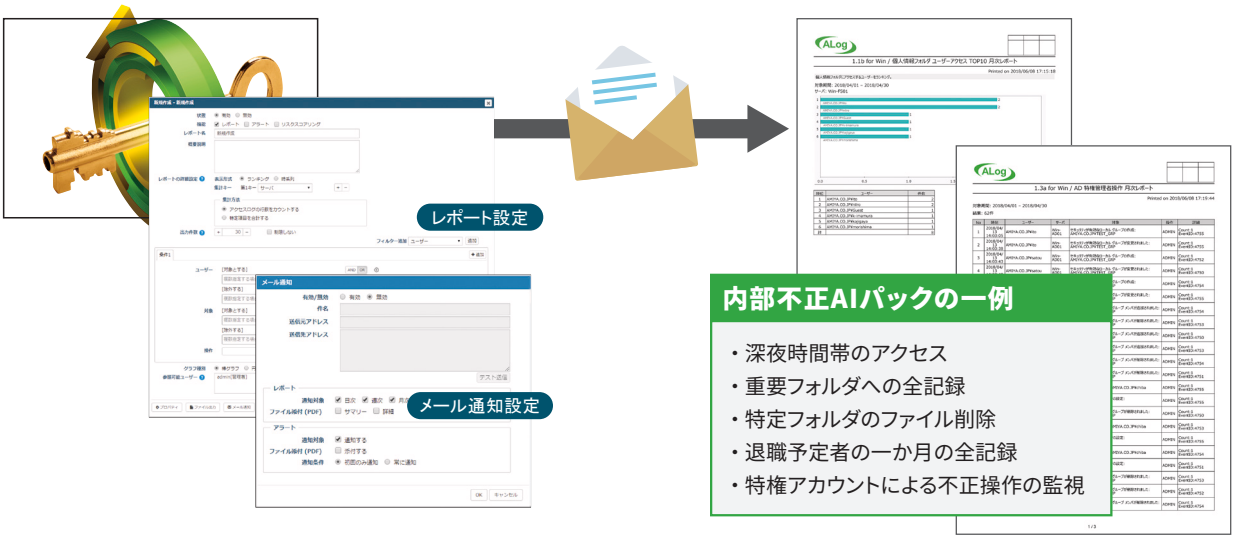
①テンプレートをインポート

②機器名を登録



③ 事前セットでレポート/アラートを自動通知

パックの中から必要なレポートを選んで設定するだけでOK。
自動でレポートが作成され、定期的に運用者にメール送信。異常時にはアラートも。



内部不正AIパックの一例

- 深夜時間帯のアクセス
- 重要フォルダへの全記録
- 特定フォルダのファイル削除
- 退職予定者の一か月の全記録
- 特権アカウントによる不正操作の監視

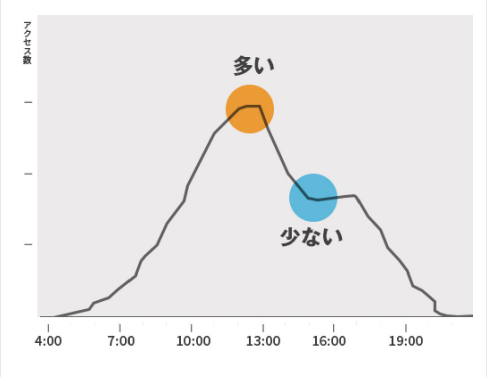
AIが過去の行動から未来の不正を自動検知

ユーザーの不審な行動（普段との差異）をAIが自動検知。人の目では気づきにくい内部不正の兆候を見逃しません。

従来

数値で不審を把握

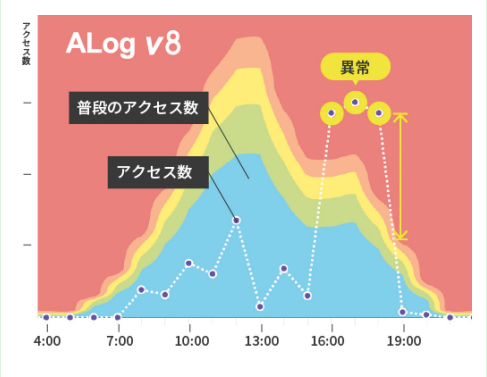
「多い」「少ない」だけでは、不審とみなす
数量のしきい値の設定が必要になる。

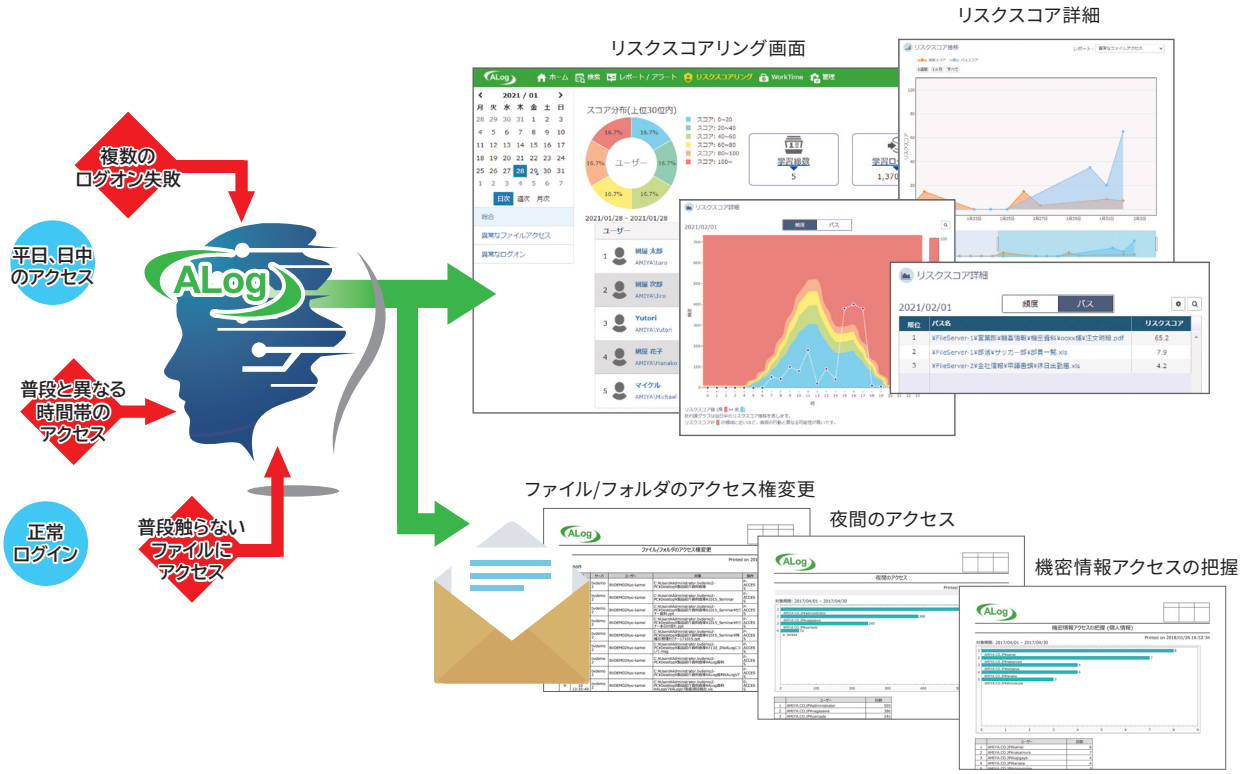


ALog

「普段」との差異をAIが過去データから分析

しきい値を設けなくても
普段との差異で異常を発見できる。

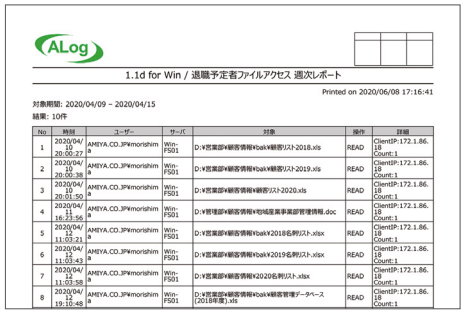




ALog × Microsoft 365のログで退職予定者の行動を監視

退職予定者がどのようなファイルにアクセスしているかを監視することで、未然に漏えい事件を防止することができます。Microsoft 365からのインシデントを例に、監視ポイントを見ていきましょう。

レポート例



ALog

1.1d for Win / 退職予定者ファイルアクセス 週次レポート

Printed on 2020/06/08 17:16:41

対象期間: 2020/04/09 – 2020/04/15

結果: 10件

No	時刻	ユーザー	サーバ	対象	操作	詳細
1	2020/04/10 20:00:27	AMIYA.CO.JP¥morishima	Win-FS01	D:¥営業部¥顧客情報¥bak¥顧客リスト-2018.xls	READ	ClientIP:172.1.86.18 Count:1
2	2020/04/10 20:00:38	AMIYA.CO.JP¥morishima	Win-FS01	D:¥営業部¥顧客情報¥bak¥顧客リスト-2019.xls	READ	ClientIP:172.1.86.18 Count:1
3	2020/04/10 20:01:50	AMIYA.CO.JP¥morishima	Win-FS01	D:¥営業部¥顧客情報¥顧客リスト-2020.xls	READ	ClientIP:172.1.86.18 Count:1
4	2020/04/11 16:23:56	AMIYA.CO.JP¥morishima	Win-FS01	D:¥管理部¥顧客情報¥包括業務事業部管理情報.doc	READ	ClientIP:172.1.86.18 Count:1
5	2020/04/12 11:03:21	AMIYA.CO.JP¥morishima	Win-FS01	D:¥営業部¥顧客情報¥bak¥2018名例リスト.xlsx	READ	ClientIP:172.1.86.18 Count:1
6	2020/04/12 11:03:43	AMIYA.CO.JP¥morishima	Win-FS01	D:¥営業部¥顧客情報¥bak¥2019名例リスト.xlsx	READ	ClientIP:172.1.86.18 Count:1
7	2020/04/12 11:03:58	AMIYA.CO.JP¥morishima	Win-FS01	D:¥営業部¥顧客情報¥2020名例リスト.xlsx	READ	ClientIP:172.1.86.18 Count:1
8	2020/04/12 19:10:48	AMIYA.CO.JP¥morishima	Win-FS01	D:¥営業部¥顧客情報¥bak¥顧客管理データベース(2018年度).xls	READ	ClientIP:172.1.86.18 Count:1

Microsoft 365対応パック

OneDrive、SharePointのファイルアクセスログやTeamsへのサインインログ、Exchangeのメールログなど、Microsoft 365で取得しておくべき監査ログをパッケージ。

SharePoint

SharePointより、顧客情報ファイルをダウンロード

「顧客情報」関連のファイルをダウンロード/アップロードした時にアラート通知

時刻	ユーザー	URL	対象	操作
2021/2/14 10:11:47	User A	https://abccorporation.sharepoint.com/confidential/	顧客情報 .xlsx	File-Downloarded

「Sharepoint」から**「顧客情報 .xlsx」**を**ダウンロード**している

Exchange

Exchangeで顧客情報ファイルを添付ファイル付きで外部送信

「顧客情報」関連のファイルを外部送信したらアラート通知
ファイル名と送信先をチェック

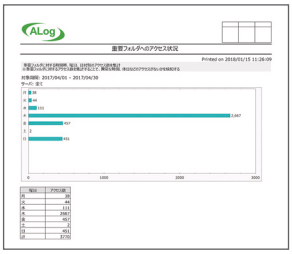
時刻	ユーザー	メールアドレス	対象	操作
2021/2/14 20:30:12	User A	xxx@e-mail.microsoft.com	顧客情報 .xlsx	365_MSG_Delivered

「xxx@e-mail.microsoft.com」あてに**「顧客情報 .xlsx」**を送信している

その他内部不正に有効なログの活用例
アクセスを監視

重要フォルダへのアクセス状況を監視

重要データにアクセスされていないかを監視

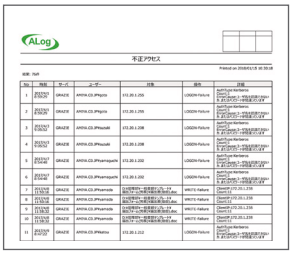


時刻	ユーザー	対象	操作
2020/07/18 15:12.0	AMIYA.CO.JP¥kamei	D:¥ 経理部 ¥ 給与計算 ¥2019 年度 ¥ 給与台帳 .xls	READ

ユーザー**「kamei」**さんが**「給与台帳 .xls」**に**アクセス**している

不正アクセスを監視

ログオンの失敗を繰り返すユーザ、ファイル削除の失敗を繰り返すユーザなど、
さまざまな観点から不審な行動を監視

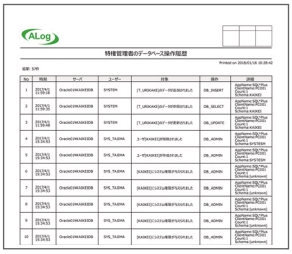


時刻	ユーザー	対象	操作
2020/04/07 8:54:48	AMIYA.CO.JP¥yamaguchi	172.20.1.202	LOGON-Failure

ユーザー**「yamaguchi」**さんが**「ログオン」に失敗**している

特権管理者のデータベース操作履歴

ドメインコントローラやファイルサーバの管理者の操作履歴を監視



時刻	ユーザー	対象	操作
2020/04/01 15:34:53	SYS_TAJIMA	[KAIKEI] にシステム権限が与えられました	DB_ADMIN

システム管理者**「TAJIMA」**さんが**「管理権限」**を**付与**している

その他内部不正に有効なログの活用例
流出を監視

不正アップロード/ダウンロードの監視

重要ファイルのアップロード/ダウンロードや、外部共有の履歴を一覧化

時刻	ユーザー	対象	操作
2020/3/24 20:24:47	takashima@amiyasap.onmicrosoft.com	https://amiyasap.sharepoint.com/sites/AmiyaX/Lists/List/顧客リスト.xlsx	FileUploaded

ユーザー**「takashima」**さんが**「顧客リスト.xlsx」**を**アップロード**している

外部共有の監視

機密情報が不正に持ち出されていないかの監視に

時刻	ユーザー	対象	操作
2020/03/26 22:40:14	watanabe@amiyasap.onmicrosoft.com	https://amiyasap.sharepoint.com/sites/Shared Documents/財務・会計【社外秘】.xlsx	SharingSet

ユーザー**「watanabe」**さんが**「財務・会計【社外秘】.xlsx」**を**共有**している

印刷の監視

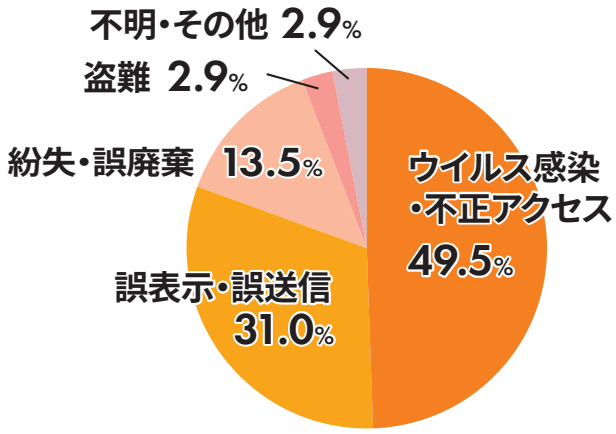
重要データが印刷されていないかを監視

時刻	ユーザー	対象	操作
2020/09/04 15:40:33	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース.xlsx	PRINT

ユーザー**「s-morishima」**さんが**「顧客管理データベース.xlsx」**を**印刷**している

内部不正・外部攻撃の両方に対応できるのはALogだけ

情報漏えいといえばこれまで約80%を内部不正が占めていました。しかし東京商工リサーチが発表した「上場企業の個人情報漏えい・紛失事故」によると、2020年に上場企業で公表された情報漏えいの約50%が外部要因によるものです。
これはテレワークの浸透により、「デバイスの紛失・置き忘れ」が減少し、標的型攻撃をはじめとした「サイバー攻撃」が増えたため。これからは、内部、外部、両方からの攻撃を警戒する必要があります。



東京商工リサーチ調べ

出典：東京商工リサーチ「上場企業の個人情報漏えい・紛失事故」調査（2020年）
https://www.tsr-net.co.jp/news/analysis/20210115_01.html

外部攻撃（サイバー攻撃）の対策に関する詳細はぜひこちらの資料をご覧ください。

ホワイトペーパーダウンロード ›

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

AMIYA 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/

販売元

ALog ConVerterは株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、著作権の侵害になります。