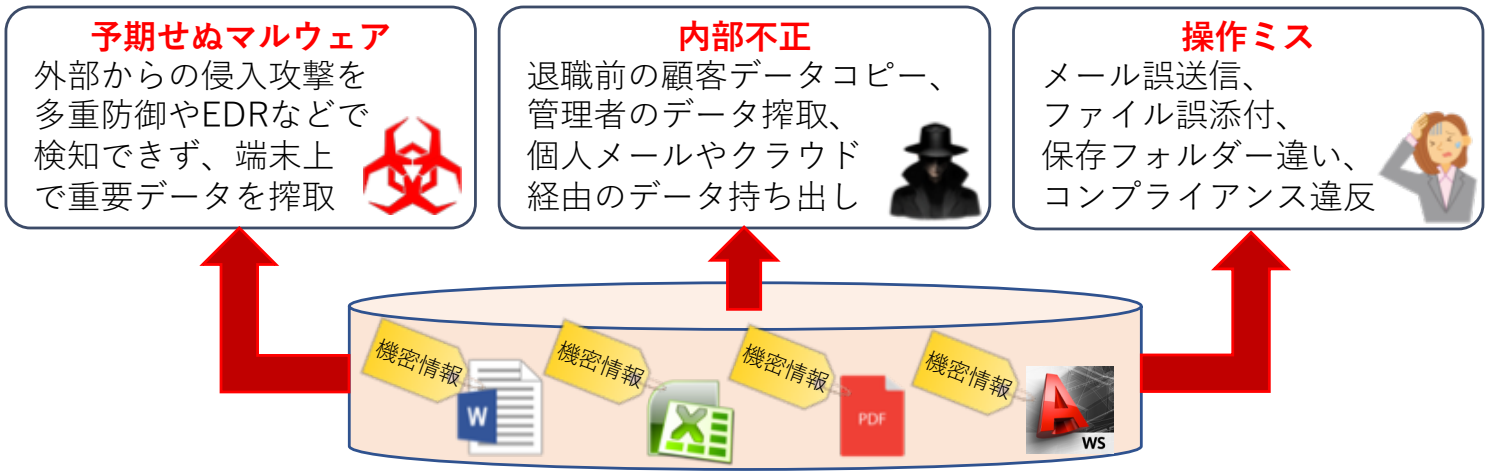
情報漏洩に直結するふるまいをリアルタイムに監視・ブロック・分析、レポート

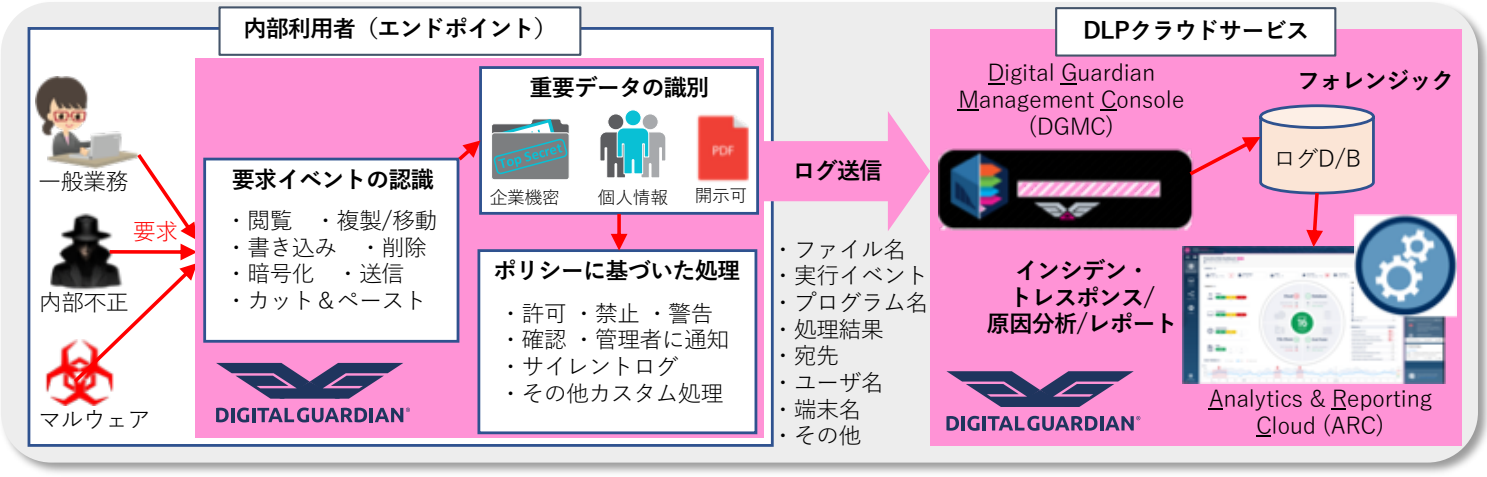
# デジタルガーディアンの新世代情報漏洩対策(DLP)

**電子化による業務効率が向上する一方、情報漏洩事故は増加の傾向にあります。
高度化する暗号化やアクセス権管理などの技術の導入は、漏洩事故の原因を削減する効果は図れても根本的な撲滅までには至っていません。
情報漏洩事故を撲滅するためには外部からの侵入を防ぐだけでなく、内部不正にも対応した対策が必須です。デジタルガーディアンの新世代DLPは、データの重要性を識別しリアルタイムに監視することで、外部への流出や誤送信、またランサムウェアによるデータ破壊などから重要データを守ることができる画期的なソリューションです。**

## 情報漏洩事故の原因




## ソリューションの特長



## DLPクラウドサービスを用いたスレットハンティング

**スレットハンティング**とは、情報漏洩事故につながる可能性の高い利用者やイベントなどをいち早く検出し事故発生前の気づきや、万一の漏洩被害の影響や原因分析などの調査のことです。
デジタルガーディアンのDLPクラウドを利用することで、次の例のような詳細調査を即時に行うことが可能となります。

### ■ EDRなどで検知できず端末に入り込んだ不正プログラムの活動調査

- 影響を受けたファイル（送信、改ざん、破壊など）
- 送信先アドレスや名前
- 感染した端末とユーザ名
- プロセスツリー
- システムファイルへの影響

### ■ 内部不正の早期発見、および実害調査

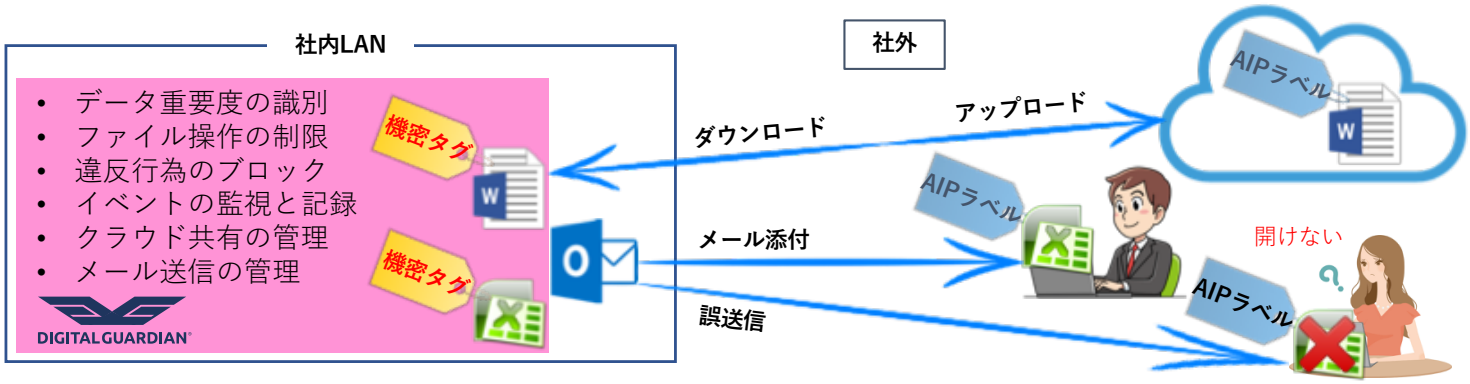
- 管理者権限を持つユーザの行動分析（データ復号後、サーバログイン後のイベント）
- 退職前のデータ持ち去り（ コピーファイル数やサイズの突然の増加）
- 不審なユーザの行動分析（早朝深夜、休日出勤回数の増加）
- 反社会的、または復讐活動（機密データの破壊や証拠ファイルの削除など）
- コンプライアンス違反者の監視（常習犯、突然変貌、うっかり）

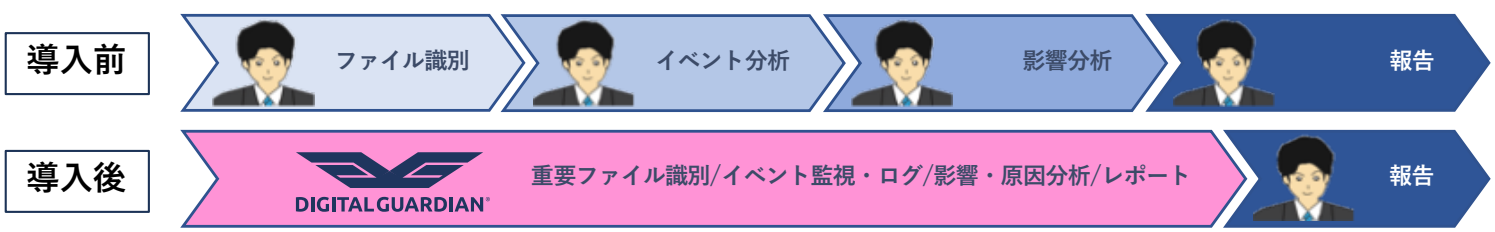
### ■ 漏洩事故、または未遂の詳細追跡調査

- イベントログ（ファイルの複製、移動、名前の変更、拡張子変更、カット＆ペーストなど）
- アプリケーション（ファイルを操作したプロセス）
- リアクション（ブロック、警告、許可など）
- イベントの時間と場所（ファイル操作の日時と端末、およびユーザ名）
- ブロックの理由（未遂に終わったファイル操作のブロックルールの表示）

## 二次情報漏洩対策（Microsoft AIPとシームレスな連携）

デジタルガーディアンのファイルタグはマイクロソフト社のAIPラベルと連携できるので、クラウドやメール添付で共有された重要ファイルも、AIPのアクセス権で保護されるため二次漏洩防止にも対応できます。




## 導入効果

デジタルガーディアンの新世代DLPを導入することで、業務負荷が大幅に削減されます。特に、重要なファイルに直結したイベントや内部不正の早期発見や外部から潜入した不正なプログラムの影響などを即座に分析・レポートできるので、担当者の日常業務の負荷が大幅に軽減されます。