

内部不正・サイバー攻撃から「データ」を守る

DIGITAL GUARDIAN®

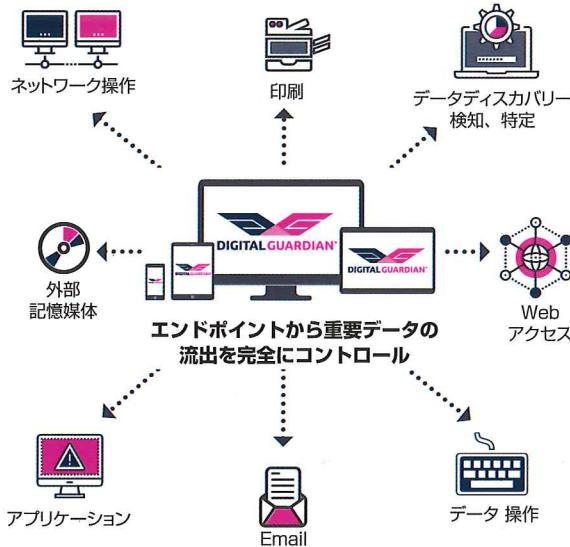
データに関わるあらゆるイベント(コピー、移動、修正、削除など)を監視

Digital Guardian は、エンドポイント型情報漏えい対策ソフトウェアです。PCやサーバなどのエンドポイントにエージェントをインストールし、データに関わるあらゆるイベント(コピー、移動、修正、削除など)を監視し、管理コンソールで可視化します。さらに、ポリシーによりエンドポイントごとのイベントを管理し、USBメモリ、プリンタなどのデバイスを制御します。これからの究極のセキュリティは、データ保護です。

退職者ダッシュボード



退職前数か月間における退職者個人のすべてのデータイベントを可視化します。企業の機密データが、メール送信、オンラインストレージへのアップロード、USBメモリへのコピーなどにより漏えいしていないことを確認できます。



機密情報ダッシュボード



過去1か月間における企業の機密データに関するイベントを集計します。機密データへのアクセス件数、移動・コピーされたデータ量、移動・コピーの手段などを詳細に分析できます。また、標的型攻撃などによる機密情報への異常なプロセスも検知します。

2016 EDITION



2016年Gartnerでリーダーを獲得

デジタルガーディアンは、ガートナーレポートにおいて、3つの重要なユースケースにトップ10のDLPプロバイダーとしてランク付けされております。

- 知的財産保護 - 第1位
- 法規制遵守 - 第3位
- データの可視性と監視 - 第3位

Gartner®

2016 Gartner Magic Quadrant for Enterprise Data Loss Prevention  
Released January 2016

## 活用事例「退職者など内部社員による情報漏洩への対策」

### データの持ち出しを監視・管理

2016年から施行される改正不正競争防止法で機密データの不正持ち出しへの罰則が強化されますが、同時に不正持ち出しを実証する証拠が求められます。今やエンドポイントの外へのデータの持ち出しを検知・記録することは、知的財産を守るためには不可欠になってきています。この対策の1つとしてデジタルガーディアンは従業員毎にデータに関わるイベントの履歴を正確に記録し、さらに、容易にデータの持ち出し状況を監視・管理できる専用ダッシュボードを用意しています。



退職者が使用するエンドポイント



退職者に知られることなく行動履歴を取得



退職者の重要データの取り扱い履歴をダッシュボード化

## VISIBILITY STUDY「機密情報の利用状況クイックアセスメント」

### 機密データのコピー、移動、保存を可視化

デジタルガーディアンでは、機密データの利用状況を可視化するVisibility Studyというツールを無償で提供しています。このツールを使うことで、日常業務での機密データの利用状況を可視化して、機密データの外部漏洩のリスクを評価することができます。



※ファイル名(及びパス)とデータの重要性が格納されます。データの内容がサーバに格納されることはありません。

世界で特許など知的財産を多く保有する企業の上位10社のうち7社、  
上位10社の自動車メーカーのうち5社が、デジタルガーディアンのユーザーです



#### セキュリティガバナンスの向上

セキュリティポリシーを強制適用するため、意識の低い利用者が機密データにアクセスしてもセキュリティレベルは低下しません。



#### 密かな攻撃を表面化

不正アクセスを検知した時点でユーザー画面上にポップアップメッセージを表示し、侵入した攻撃者の存在を表面化させます。



#### コピーファイルも追跡

自動探索機能によりデータを探索して、タグを付与し、コピーや、パスワードロックがかけられても機密ファイルの追跡を続けます。

主な機能	ご利用例
デバイス制御	特定のシリアルナンバーのUSBデバイスだけを使用可能とする。
印刷制御	機密資料は印刷不可とする。業務時間外はプリンタを使わせない。
ネットワーク制御	社内のすべてのファイルは、Facebook、Dropboxにアップロードさせない。機密ファイルは、FTP経由でアップロードさせない。
アプリ制御	Skypeなどブラックリストのアプリケーションを起動させない。
データ操作制御	特定データのコピー&ペースト、削除、移動をさせない。ソースコードのファイル名/拡張子の変更をさせない。プリントスクリーンを実行させない。
Eメール制御	マイナンバーの含まれたファイルはメールに添付させない。
暗号化	CADデータを外部デバイスに移動させる際には暗号化する。
通知 - 制御	定のファイルを添付してメールする際には、警告を通知、理由を要求、または送信をブロックする。
データ分類	クレジットカード番号が含まれるファイルは全て、機密扱いのタグを自動的に付与する。
レポート	退職者が、退職までの期間に、社内ポリシーに反する機密ファイルへのアクセスなど異常がないかダッシュボードで分析する。
サイバー攻撃対策	サイバーポリシーバックにより、各エンドポイントが未知のマルウェアによる異常なプロセスを起こしていないか分析し、検知する。

< 開発元 >  
デジタルガーディアン株式会社

〒105-0021 東京都港区東新橋2-11-4 汐留プラザビル9F  
Tel. 03-6435-6207 Fax. 03-6435-6204

contact-jp@digitalguardian.com  
https://www.digitalguardian.com/ja/

< お問い合わせ先 >  
AOSリーガルテック株式会社

〒105-0001 東京都港区虎ノ門5-1-5 メトロシティ神谷町5F  
Tel. 03-5733-5790 Fax. 03-5733-7011

✉ law@aos.com  
www.aos.com