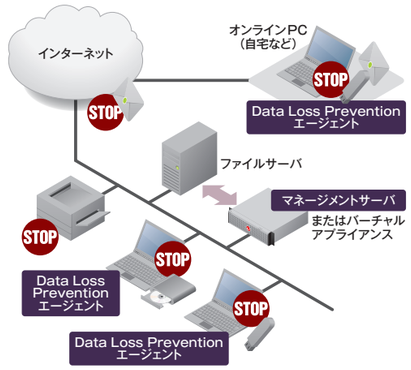
Trend Micro Data Loss Prevention™ システム構成／動作イメージ

Trend Micro Data Loss Prevention は既存のネットワーク環境を大きく変えることなく、ファイルサーバと連携して機密文書管理を実施します。クライアント・エージェント型なので、外部に持ち出したPCであっても機密文書をブロックします。



●構成コンポーネント

クライアントPC：Data Loss Prevention エージェント

サーバ：マネージメントサーバ（アプライアンス版またはバーチャルアプライアンス版）

主な特徴

●簡単な機密情報の定義

4種類の定義方法：キーワードマッチング、パターンマッチング、ファイル属性、独自のフィンガープリント技術による機密情報の定義が可能です。

各種テンプレート：個人情報やソフトウェア資産など目的に応じたテンプレートを備えており、導入したその日から情報漏えい防止に役立ちます。

データディスカバリ機能：社内に散在しているデータをチェックして機密情報の在り処をスムーズに把握できます。情報資産の棚卸しにも効果的です。

違反行為時に表示されるダイアログ画面はメッセージやロゴのカスタマイズが可能です。管理者への申告もできます。

●柔軟な運用ルール／ポリシーの設定

持ち出し制御：持ち出しの全面禁止、制限付きでの持ち出し許可、持ち出し時の申請・管理など、情報の機密レベルに応じた運用ルール、ポリシーを柔軟に設定できます。

USBメモリ ホワイトリスト機能：特定のベンダー、モデル、シリアル番号などを基に、ポリシーに合致するUSBメモリだけを使用可能にすることができるので、業務効率を下げずに運用できます。
※Trend Micro USB Security™ for Biz との連携による、より堅固な情報資産管理を実現

Active Directory 対応：ログインしているユーザごと、役職、グループ単位でポリシーを設定できます。1台のPCを共有している環境でも、個別の設定による柔軟な運用が可能です。

●高い教育効果／意識向上の促進

警告ダイアログ：ポリシー違反時のリアルタイム警告によって“気付き”を促し、情報漏えい対策への意識向上と教育効果を促します。

製品に関する詳細はこちらから ▶ http://www.trendmicro.co.jp/TMDLP/

安心を、ひとつ上のステージへ。
TREND MICRO トレンドマイクロ株式会社

東京本社
〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
TEL.03-5334-3601（法人営業代表）FAX.03-5334-3639

大阪営業所
〒532-0003 大阪市淀川区宮原3-4-30 ニッセイ新大阪ビル13階
TEL.06-6350-0330　FAX.06-6350-0591

名古屋営業所
〒460-0003 愛知県名古屋市中区錦3-5-27 錦中央ビル10階
TEL.052-955-1221　FAX.052-963-6332

福岡営業所
〒812-0011 福岡県福岡市博多区博多駅前2-3-7 サンエフビル7階
TEL.092-471-0562　FAX.092-471-0563

www.trendmicro.co.jp

お問い合わせ先

C30-DLP4P-SCTV-C001

安心を、ひとつ上のステージへ。
TREND MICRO™

Trend Micro Data Loss Prevention™

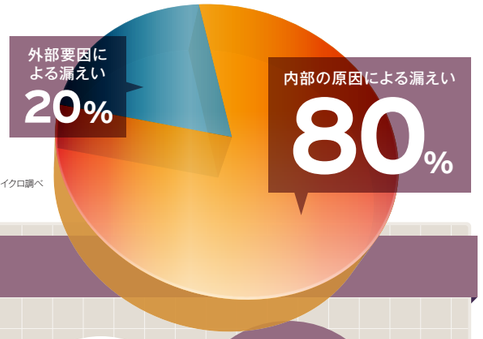
守るべき機密情報を漏えいさせないDLPソリューション

トレンドマイクロ株式会社

“重要な情報を守っている”と思っていても、

情報の漏えいは起きている

個人情報や開発中のソフトウェア資産をはじめ、守るべき情報はさまざまです。多くの企業・団体が、暗号化やログ取得、アクセス制御といった対策によって、漏えいの防止に努めています。
しかし、情報は日々漏れ続けています。
そして、その原因のほとんどは内部にあるのです。



※2009年トレンドマイクロ調べ

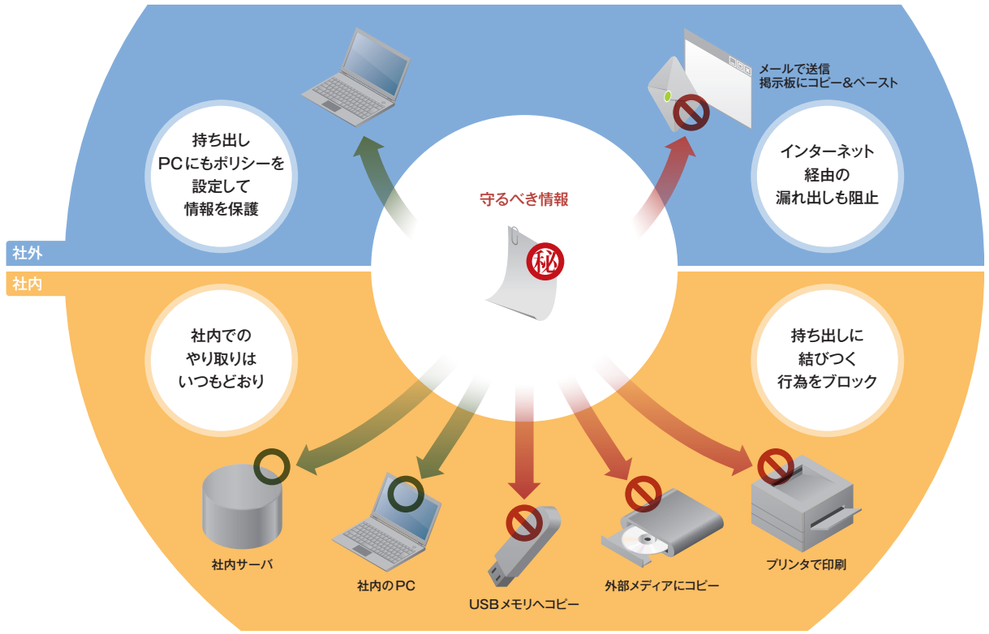
従来の情報漏えい対策は何をしているのか？

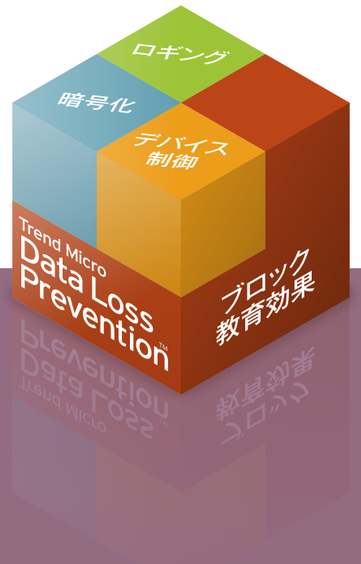
- **アクセスログ取得**：PCの操作内容を記録する
- **暗号化**：データを容易に読めなくする
- 情報の持ち出しそのものは誰でもできてしまう
- **デバイスコントロール**：USBメモリやプリンタ、外部記憶装置の利用を制限する
- 厳密すぎると利便性が損なわれ、緩いと効果が得られない

利便性、業務効率を下げずに、情報の持ち出しそのものを防ぐ対策が必要

シンプルな運用で、情報漏えい対策とビジネスの利便性を両立

Trend Micro Data Loss Prevention™





エンドポイントからの機密情報の“持ち出しを防ぐ”それが「DLP」ソリューション

DLP（Data Loss Prevention）は、エンドポイントにおける情報漏えい対策を包括的に支援するソリューションです。PCやサーバに蓄積されている情報の内容をチェックし、機密情報に該当するものは外部へ持ち出せなくすることで、うっかりミスはもとより、意図的な漏えいも防ぎます。業務効率を損なわずに情報資産を利用でき、メリハリのある運用を実現できることが大きな特徴です。
既存の情報漏えい対策と相互に補完させることで、より効果的な対策が可能になります。

業務効率を落とさず情報を活用

- 機密情報に該当するものでも、社内のやり取りは普段どおり行えます。情報のコピー&ペーストなど一部の行為は制限を設けることもできます。
- あらかじめ登録したUSBメモリなどのデバイスは通常どおり利用できます。
- 機密情報に該当しないものは、コピーやプリントアウトをはじめ、普段と変わらない利用が可能です。

守りたい情報を簡単登録

- テンプレートやキーワード、特定の文字列パターンなどを基に、機密情報を簡単に登録できます。
- 登録した機密情報が持ち出されそうになったときの対処法（ポリシー）を設定できます。

ルール違反をすぐに警告

- 禁止行為をするとすぐに警告ダイアログを表示して、ユーザの意識向上を促します。

リアルタイムに持ち出しを防止

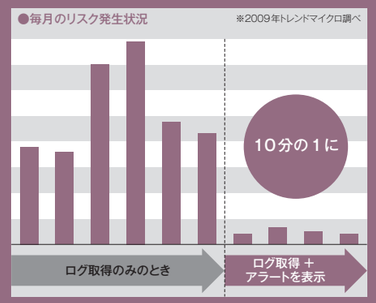
- USBメモリやCD/DVD、プリントアウトなど、持ち出し可能な機器や媒体への出力を制限できます。
- eメール、Webメールでの送信や、掲示板へのコピー&ペーストなどによる、インターネットへの流出を防ぎます。

社外からの漏えいも防止

- 持ち出しPCからのメール送信やUSBメモリなどへのコピー、印刷も社内と同じレベルで禁止できます。

「気付き」がもたらす大きなリスク削減効果

これまでの情報漏えい対策では、システム面の対策が注目されてきました。より確実な効果を上げるには、「うっかりミス」や「ちょっとしたルール違反」をはじめとする人的要因への対策を行い、意識を向上させることが非常に重要です。
Trend Micro Data Loss Prevention™は、禁止行為をダイアログで警告し、ポリシー違反に関するメッセージを表示。“気付き”を施すことにより、教育効果を高めます。



業務中の違反行為をリアルタイムに“気付かせる”ことでリスクの発生が大幅に減少