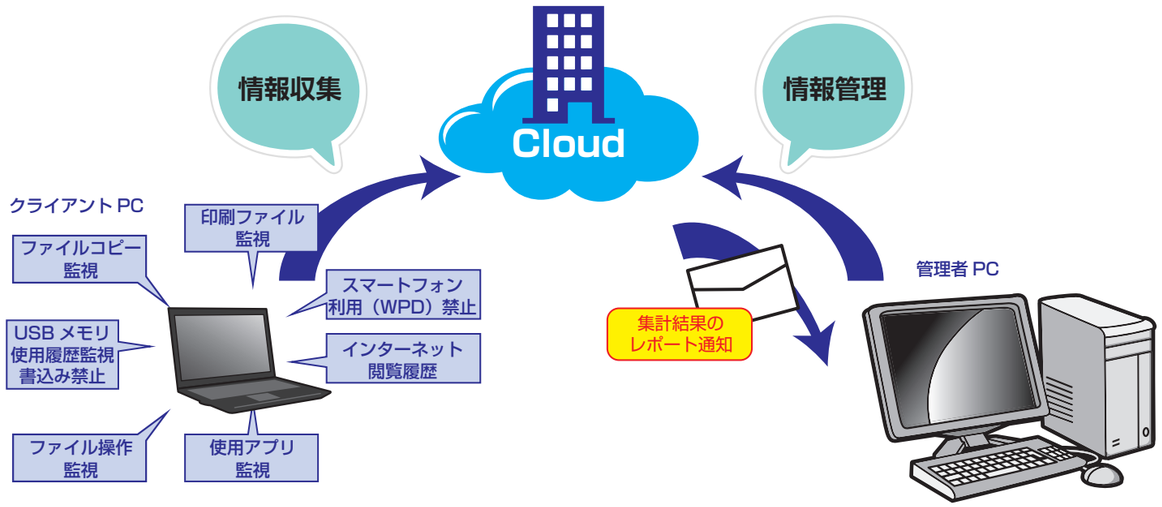
ご利用イメージ



仕様	SAP200α
内部統制ソフト Watch主な機能	■PCを監視して、稼働状況･作業内容を記録 ●個人情報ファイルをPCに保存していないか等の確認(トリガーカスタマイズ可) ●USBメモリ利用履歴　●印刷ファイル名の記録 ●PC作業内容管理　●ファイル操作履歴 ●PC操作時間管理　●利用アプリケーション統計 ●インターネット閲覧履歴　●デスクトップ画面保存 ■USBメモリ/WPD(スマートフォン)利用制限:書込禁止･使用 禁止 ■利用禁止アプリ設定 ■日報･週報･月報メール送信 ■クライアントアプリアンインストパスワード設定 ■タスクトレイ/スタートメニュー/コントロールパネルでのアプリ非表示
ライセンス数/期間	20CL　/　ご利用開始から7年間※
OS	Windows 10 (32bit/64bit)/11
CPU	各使用OSの仕様条件に準ずる
メモリ	8GB以上
ストレージ	10GB以上の空き容量
必須ソフトウェア	.NET Framework 4.8以降
構成品	プログラムCD､取扱説明書　等

●内部統制ソフト「Watch」は、PC 操作履歴を管理することで、不要な情報利用や持ち出しによる情報漏えいを抑止するシステムです。Watch を利用することで情報持ち出しによる情報漏えいを完全に防止するものではありません。情報利用に関する社内ルールの徹底等を必ず確認して下さい。●本紙掲載の会社名および商品名等は、一般に各社の商標または登録商標です。●本紙に掲載している商品の価格には配送設置・工事・接続調整などの費用は含まれておりません。●パソコンの操作方法、ご質問及びトラブルに関しては、各メーカーへお問い合わせ下さい。●本製品の誤動作･不具合･通信障害あるいは停電などの要因によってデータの損失が発生した場合や、通信などの機会を逃した為に生じた純粋経済損失およびメール誤送信による如何なる損失や損害につきましては、補償いたしかねます。予めご了承下さい。●本資料は 2024 年 1 月現在のものです。製品改良等により仕様およびデザインは予告なく変更する場合があります。　※ご利用期間経過後はサポートを終了し、サービスを停止いたします。

株式会社 アレクソン

IS 680370 / ISO 27001
対象範囲：本社・東京支社

ISO14001
対象範囲：本社・東京支社・伊丹工場

ビジネスパートナー部 営業一課
〒103-0013 東京都中央区日本橋人形町2-25-13 リンレイ日本橋ビル5F
TEL 03-3667-2276　FAX 03-3667-5329

ビジネスパートナー部 営業二課
〒541-0052 大阪府大阪市中央区安土町1-8-6 大永ビル4F
TEL 06-6121-6048　FAX 06-6121-6049

ビジネスパートナー部 営業二課 福岡営業所
〒819-0025 福岡県福岡市西区石丸2丁目40番8号
TEL 092-892-9677 FAX 092-892-9678

ホームページ　https://www.alexon.co.jp/

お問い合わせ

情報漏えい対策パック

SAP200α

IT資産の「見える化」対策

情報資産を守り安全に管理

情報漏えい対策

PCの管理・監視

内部不正防止

個人情報の取り扱い厳格化、漏洩時の通知の完全義務化など欧米並みに

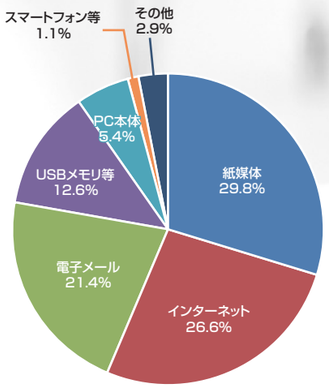
2022年4月1日に施行された「改正個人情報保護法」では、個人情報の取り扱い厳格化、漏洩時の通知の完全義務化など欧米並みに厳格化されました。
報告義務違反などの法令違反に対する罰則・罰金も強化されており、不備が発覚したときの訴訟リスクも高まるため、企業は厳密な対応を求められます。

しかしながら、企業にとって重要な情報は、マイナンバーや個人情報だけではありません。

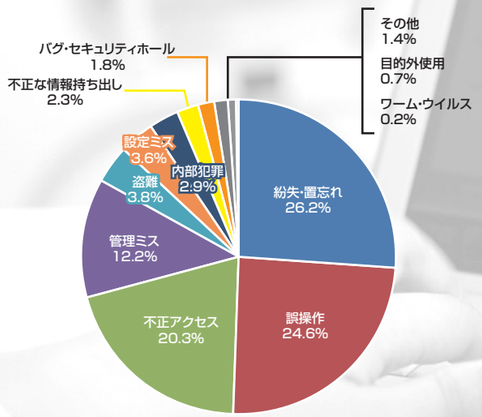
●顧客情報
●価格情報
●技術情報

「自宅で仕事をしようと、USBメモリにコピーして、紛失してしまった。」
「自社社員あてに送るつもりが、間違って取引先に原価の入った価格情報を送ってしまった。」
「退職社員が、顧客情報や技術情報を持ち出しして、ライバル企業に転職した。」

これらの情報漏えいは、個人情報および特定個人情報（マイナンバー）の情報漏えいと違い、刑事罰こそありませんが、直接企業の信用や競争力を低下させるため、経営者にとって頭の痛い問題です。



媒体及び経路別 情報漏えい件数



情報漏えいの主な原因

参考:特定非営利活動法人日本ネットワークセキュリティ協会　「2018情報セキュリティインシデントに関する調査報告」より

上記グラフで示しているように、情報漏えい件数は、「紙媒体」に次いで「インターネット」「電子メール」「USBメモリ」等が多くなっています。
また、原因としては「誤操作」「管理ミス」「紛失・置忘れ」が過半数を占めています。

セキュリティパッケージ SAP200αは、ユーザーの「プリントアウト」「USBメモリ」「ファイル操作」等のPC操作を管理し、さらに、USBメモリへの書き込み禁止やスマートフォン等デバイス（WPD）の禁止も行うことができます。
監視と利用禁止、2つの手段で社内重要情報の不正な情報漏えいを抑止、防止するシステムです。

PC作業を可視化・内部統制し、情報漏洩リスクを軽減 SAP200α

SAP200αは、内部統制ソフト「Watch」にて構成されています。
本システムを利用することによって、情報漏えいの抑止に効果を発揮します。

PC管理・監視

PCの利用状況（利用アプリ・ファイル）を集計して、管理者にメール通知します。
利用状況を管理することで、情報漏えいリスクを軽減し、生産性を向上させます。

収集するおもなPC利用状況は下記のとおりです。
- ■PC作業時間及び時間帯
- ■使用アプリおよび使用時間
- ■PC作業内容
- ■インターネット利用履歴
- ■USBメモリ利用履歴

個々の作業内容を時系列で記録・通知します。
通知メールは［日報］［週報］［月報］の形で送信します。

☑ 日報　☑ 週報　☑ 月報

また、特に情報漏えいの原因となりやすい「USBメモリ」やスマートフォンデバイス（WPD）への書込禁止を行うことで、情報漏えいのリスクを低減します。

USBメモリ使用禁止

- ◉ USBメモリを使用禁止しない
- ○ USBメモリを使用禁止にする
- ○ USBメモリへの書込のみ禁止する

※注）設定変更後はクライアントPCでUSBメモリを抜いた後に再起動が必要です。

Android等のWPD(PortableDevice)を使用禁止

- ◉ WPDを使用禁止しない
- ○ WPDを使用禁止にする
- ○ WPDへの書込のみ禁止する

※注）設定変更後はクライアントPCでWPDを抜いた後に再起動が必要です。

PCを監視することによりPC利用者がストレスを感じないように常駐状態を非表示にすることも可能です。