◆パソコン対応機能

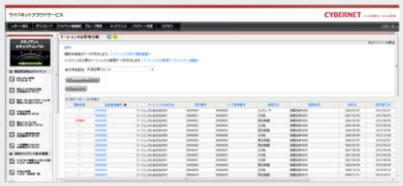
■資産管理

ハードウェア/ソフトウェア情報収集、台帳作成

管理対象パソコン（Windows/Mac）やスマートデバイス（Android/iOS）ごとにハードウェアの構成情報やソフトウェアのインストール情報をリアルタイムに自動取得し、資産管理番号や社員番号、利用用途などの資産情報を入力可能で、それらの情報を元に台帳を作成することで、企業が保有するIT資産の現状把握が行えます。
インターネット環境に接続できないWindows端末の管理も可能です。スタンドアロンパソコンのインベントリ情報もUSBメモリ経由で収集できます。

ライセンス管理台帳/レポート

Microsoft Office製品、Adobe製品専用の管理台帳機能を搭載。インストール状況などの詳細を確認することができます。残りのライセンス数に関しては、色別でわかりやすく表示します。



リース/レンタル管理

クライアント情報にリース/レンタル契約情報を紐付けて管理することで、どの契約でリース・レンタルしている機材が、いつどれだけの数、期限切れになるのかを把握でき、契約の延長や返却等の確認を正確に行えます。リース会社が発行する契約データ(CSV)の取り込みも可能です。リース/レンタル契約管理機能として、月次での棚卸やリースアップ前にユーザー/管理者への事前通知も可能です。

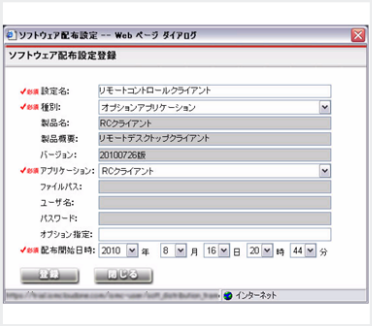
グループ管理

グループ全体の各企業を管理するグループ企業管理者や企業の各部門を管理するグループ管理者など4階層の管理者の設定ができます。社内の各部門のグループ管理者に管理者コンソールと権限を与え、そのグループ単位でのIT資産管理、セキュリティ管理が可能です。

アンケート収集

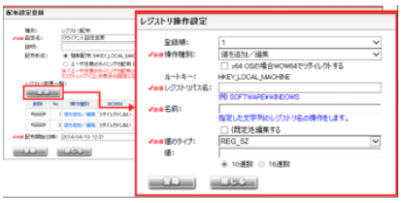
ユーザーからアンケート形式で任意の情報を収集できます。収集した情報は各クライアントのインベントリ情報に登録されます。

■遠隔管理



ソフトウェア配布/ファイル配布

社内ネットワーク経由でのソフトウェア配布が可能です。Windowsではファイルやフォルダの配布も可能です。



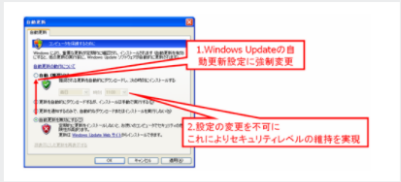
レジストリ配布

指定したレジストリ値の追加/編集、エントリの削除、キーの削除などのレジストリ設定をリモートで行うことができます。

リモートコントロール [オプション][Windows]

企業内でLAN接続されているパソコンはもちろん、外出中や海外の端末までインターネットに接続されているすべてのパソコンをリモート操作することができます。本機能を活用することで、自席の端末から対象パソコンをリモート操作できるため、作業の効率化やサポート工数/負荷軽減が図れます。

■セキュリティ管理

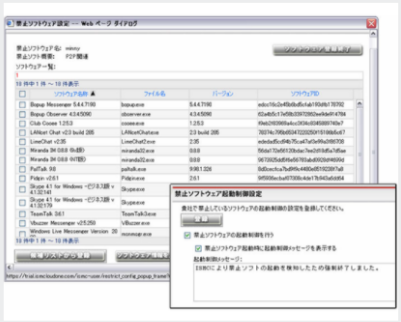


Windows Update更新支援

WindowsやOffice製品などのセキュリティパッチの更新設定を常に自動に保ち、各パソコンの適応状況を確認できます。また、管理者側でWindows Updateを実行することも可能です。

セキュリティレベル診断

毎日自動更新される「セキュリティ辞書」と実際の状況を突き合わせて、社内のセキュリティパッチの適用状況、ウイルス対策ソフトのパターンファイル更新、禁止ソフトのインストール状況などから、パソコンのセキュリティレベルを日次で診断します。インベントリ情報を条件にした診断項目の作成や辞書による診断の除外設定も可能ですので、社内の運用に合わせた独自の脆弱性診断を行うことができます。



利用禁止ソフトウェアの検出＆起動制御

社内ポリシーで認めていないソフトウェアのインストール状況の把握と、利用禁止ソフトウェアをユーザーが起動させた場合の起動制御が可能です。

ウイルス対策ソフトウェア/セキュリティパッチ適用状況把握

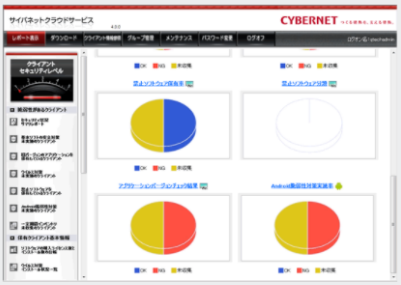
Windowsセキュリティパッチ未適用のパソコンや、各パソコンの未適用パッチの種類を自動でレポートします。また、ウイルス対策ソフトのインストール状況や、パターンファイルの更新状況の診断が可能です。

セキュリティアラートメール

1日1回、登録メールアドレス宛てに社内パソコンのセキュリティ概要アラートメールを自動送信できます。

外部記憶メディア制御 [オプション][Windows]

パソコンからUSBメモリ等の外部記憶メディア、USB接続したスマートフォン・デジタルカメラ等に対してデータの書き出しと読み込みを制御できます。管理者側で個人やグループ別に利用権限を設定できるほか、社員からの申請～管理者の承認、承認結果の通知、外部メディア接続/取出し履歴の取得までの一連の作業を単体で実現しており、情報漏えい対策としての外部メディアの利用制限の導入と運用を簡単に実施できます。（※申請・承認フローはポータブルデバイス対象外）



ソフトウェアのバージョンチェック機能による脆弱性対策

各クライアントパソコンの情報を収集し、旧バージョンがインストールされている(脆弱性のある)パソコンを特定、レポートとして出力できます。また脆弱性のあるパソコンへの対策として、ソフトウェアをリモートインストールしたり、デスクトップメッセージからユーザーにアップデートを指示する等のアクションも可能です。このほか自動アップデート機能を搭載したソフトウェアに対しては、常にその機能が有効になるよう設定を維持することもできます。

ユーザー操作ログ取得 [オプション][Windows]

・操作ログに関するシステムアラート情報を収集できます。
・外部メディアの挿入/取り出し、ファイル書き出し操作を収集できます。
・ドキュメントファイルへのアクセス、操作内容、外部メディアへの書き出しなどのファイル操作を収集できます。
・アクセスしたWebサイトのURL、サイト名や、SNS サイト（Ameba/Facebook/Google+/mixi/Twitter）への書き込み情報を収集できます。
・Webメール（Gmail/Outlook.com/Yahoo!メール）を送信した際の送信元/送信先のメールアドレス、メール内容、添付ファイル名を収集できます。
・パソコンの稼働状況を収集できます。

ハードディスク暗号化 [オプション][Windows]

OSなどのシステム領域やデスクトップまで含めハードディスクを丸ごと暗号化します。ハードディスク暗号化の基盤は、Common Criteria EAL4など世界最高レベルの認証を多数取得し、全世界で6300万ライセンスの出荷実績を持つハードディスク暗号化製品「Check Point Full Disk Encryption」を使用しており、オンプレミスの製品と同様の暗号化機能をクラウドで提供します。

【暗号化適用状況の可視化】
PC&モバイル管理サービスの管理コンソールよりクライアントパソコンの暗号化状態の確認を行います。また、アラートメールによる自動検知により、暗号化未適用パソコンを素早く発見することが可能です。

【リカバリファイルの集約管理】
データ復旧時に必要な復号キーファイル（リカバリファイル）は自動的に管理コンソールで集約・管理され、必要な際に簡単に入手することができます。

◆モバイル対応機能

■資産管理

端末情報/利用アプリ情報の取得 [Android/iOS]

電話番号や端末のバージョン、機種番号といったスマートデバイスのハードウェア情報や、インストールされているソフトウェア情報を日次で収集。登録した資産情報との紐付けにより、パソコンとスマートデバイスの一元的な資産管理が可能です。

アプリケーション配布 [Android/iOS]

Android端末およびiPhone/iPadへ任意のアプリケーションを配布することが出来ます。
ISM CloudOneのクライアントモジュールも配布する事が出来ますので、GooglePlayを通さずクライアントのバージョンアップが可能です。
※iOSはApp Storeから指定したアプリケーションをダウンロードします

アプリケーションポータル [Android/iOS]

企業やグループで利用を許可されたアプリケーションを公開し、ユーザーが必要に応じてアプリケーションポータルからダウンロードすることができます。
業務上必須のアプリケーションは配布機能でインストールし、その他のアプリについてはユーザーが必要に応じてアプリケーションポータルからインストールするといった運用が可能です。

■セキュリティ

ポリシー違反の検知

【Root化、JailBreak検知】
Android端末のRoot化、iOS端末のJailBreakを検知し、管理者へメールで通知します。
該当端末は、「スマートデバイス脆弱性対策未実施のクライアント」としてレポートに表示されます。
【パスワードポリシー強制変更】 [Androidのみ]
管理者が設定したパスワードポリシーに則っているかチェックします。
脆弱性診断レポートでチェック結果を確認することができるほか、
ポリシー違反の端末に対して警告メッセージを表示し、パスワード変更を促すことが可能です。
【禁止アプリのインストール検知】 [iOSのみ]
端末に禁止アプリがインストールされているかどうか検知することが可能です。
禁止アプリのリストはポリシーに対して設定することができます。
【ポリシー構成プロファイルの削除検知】 [iOSのみ]
ポリシー構成プロファイルの削除を検知することができます。
削除検知はユーザーコンソールの脆弱性診断レポートで確認することができます。

ネットワーク接続設定・制御 [Android/iOS]

管理コンソールから各端末に対してWi-FiとVPNの設定を一斉に実施する機能を搭載しています。これにより、1台1台設定する手間やユーザーに任せてパスワードが広まってしまう危険性をなくすことができます。

違反時ポリシーの適用 [Android/iOS]

ポリシー違反がある端末に対して、「違反時用ポリシー」を適用させることができます。あらかじめ違反時用のポリシーを設定しておくことで、ポリシー違反がある端末に対して速やかに違反時のポリシーを適用させ、ユーザーの不正利用を抑止することができます。

アプリケーションの起動制御 [Android/iOS]

業務とは無関係なアプリケーションの利用を制限できます。Android端末ではアプリケーションの起動を制限、iPhone / iPad ではアプリ入手元となるApp Storeを含むプリインストールアプリの利用を禁止することができます。また、Androidでは緊急時にあらかじめポリシーで設定したアプリをリモートでロックする機能が搭載されています。端末ロックと合わせて企業情報へアクセス可能なアプリを使用できなくすることで情報漏えいを確実に防ぎます。

自動セキュリティ診断 [Android/iOS]

ウイルス対策ソフトのインストール状況やエンジンバージョンチェック、ウイルス対策ソフトが停止していないか、端末のパスワードロックの設定実施、「提供元不明のアプリ」設定が無効になっているか、デバイス管理者の指定先がPC&モバイル管理サービスになっているかという項目を確認。未実施の端末をレポート表示することで、セキュリティ設定の変化をチェックできます。

PC&モバイル管理サービスのクライアント自動再起動 [Androidのみ]

Androidクライアントのサービスを監視プログラムが監視し、停止を検知すると10秒以内に自動起動します。サービスをユーザー操作により不正に停止されても、自動でサービスを起動するため、常にPC&モバイル管理サービスの管理下に置くことができます。

URLフィルタリング [オプション] [Windows/Android/iOS]

社内外すべての端末に対し、SNS書き込みのブロックや外部の不審なサーバーとの通信を禁止し、内部からの情報漏洩を未然に防ぎます。

SDカード/Bluetooth制御 [Androidのみ]

ポリシー設定により、SDカードやBluetoothの使用を制限することができます。これによりSDカードやBluetoothを経由した情報漏洩・ウイルス感染を未然に防ぐことができます。

リモートロック/リモートワイプ [Android/iOS]

スマートデバイス紛失・盗難の際、遠隔から端末ロックやリモートワイプ（端末初期化）、パスワードの変更等の対策を実施することで、端末内に保存された住所録等の個人情報や業務データ等の漏えいを防ぎます。ワイプの実行結果も確認できます。また、Windows 8タブレットにも対応しており、リモートによるフォルダの削除やBitLockerパスワードの変更が可能です。

位置情報の取得 [Android/iOS]

位置情報を収集し、コンソールから地図で確認できます。紛失した端末やRoot化された端末の位置情報を収集することで端末回収に役立ちます。位置情報取得が無効になっている端末には1日1回有効化を促すメッセージを通知します。なお、iOSはiOS Enterprise developer契約が別途必要となります。

24時間・365日サポート [オプション][Android/iOS]

スマートフォンやタブレット端末の盗難・紛失にあった時、深夜や週末など管理者が不在時にも情報漏えい対策を実施できる24時間365日サポートをご用意しております。

【オペレータリモートワイプ】
オペレータリモートワイプは、リモートワイプなどの遠隔操作をオペレータが24時間365日代行するサービスです。
深夜や週末など管理者が不在のときに、端末利用者からオペレータに直接連絡することで、
リモートワイプなどの情報漏えい対策を講じることができます。