ISM CloudOne

Vol.7.1.4

ISM LogAnalytics

ログ管理 ノウハウ溜めて 20年

サクサク検索!! ログ検索!

長期保存もできるよ

2022.2.8
ISM LogAnalytics Debuted!!

最新情報は **https://ismcloudone.com/**

クオリティソフト株式会社　e-mail : sales@qualitysoft.com

本　社	〒649-2333 和歌山県西牟婁郡白浜町中1701番 3
東京本部	〒102-0083 東京都千代田区麹町3-3-4 KDX麹町ビル6F
大阪オフィス	〒541-0051 大阪府大阪市中央区備後町1-7-10 ニッセイ備後町ビル 8F
名古屋オフィス	〒460-0008 愛知県名古屋市中区栄3-2-3 名古屋日興證券ビル 4 階

※記載されている会社名及び製品名は、各社の商標または登録商標です。
※このカタログは、2022年10月現在の内容です。
※各製品の価格はオープンプライスとなっております。
　価格につきましては、販売パートナーにお問い合わせ下さい。

■販売パートナー

2022s10-a

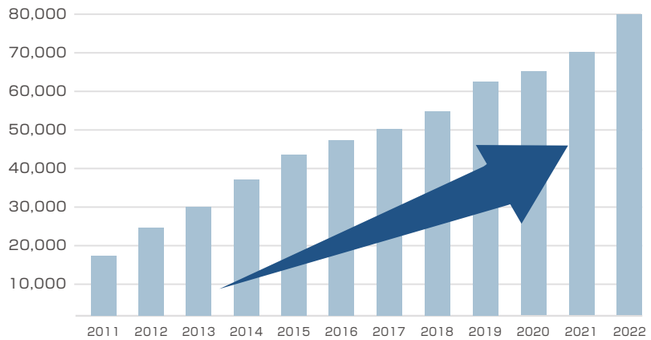
QualitySoft

全ての企業に「トランスペアレントな安全」を

トランスペアレント（transparent）とは、
「透明な、透き通った」といった意味を持つ英単語です。
IT技術に置き換えると、内部での処理などがユーザーからは見えず
「意識する必要がない」といった意味を指します。
ISM CloudOneは企業の持つ情報が「意識することなく」
「安全」に守られる状態を実現するためのプラットフォームです。

ISM CloudOneは、多様化するIT環境に対応できるソリューションとして多くの企業様に導入いただいております。

2007年リリースからの導入実績

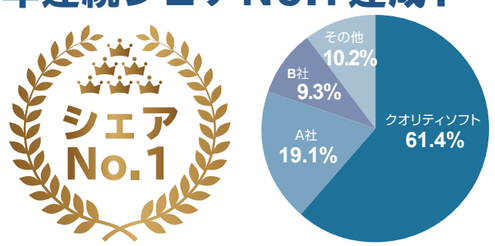


80,000社突破

2022年10月時点

クラウド型資産管理サービス市場

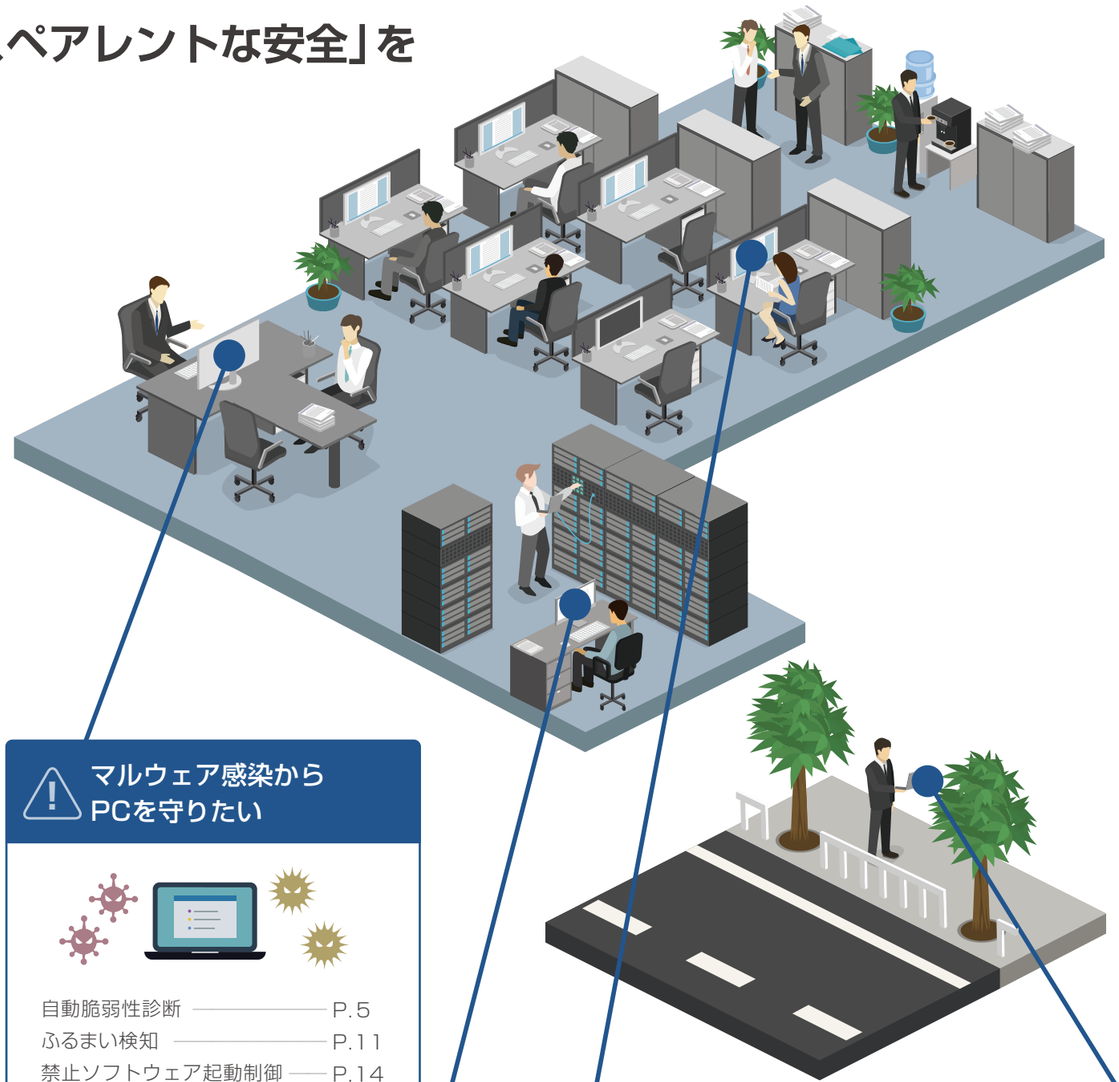
6年連続シェアNo.1達成！



デロイト トーマツ ミック経済研究所株式会社
「情報セキュリティマネージド型・クラウド型サービス市場の現状と展望 2021年度版」
https://mic-r.co.jp/mr/02100/

日本国内のみならず、
世界 **55ヶ国以上** で導入。

国内に本社があり海外に進出している企業は
端末管理に多くの課題があります。
ISM CloudOneは導入いただいた多くの
企業様よりご満足いただいております。



マルウェア感染から PCを守りたい

自動脆弱性診断 P.5
ふるまい検知 P.11
禁止ソフトウェア起動制御 P.14

サイバーリスクから 企業の情報を守りたい

LogAnalytics P.7
ふるまい検知 P.11

企業内のPCを確実に管理したい

ハードウェア・ソフトウェア管理 P.23
Windows 10管理運用支援 P.15
ファイル・ソフトウェア配布 P.17

テレワーク端末を管理したい

外部デバイス制御 P.21
LogAnalytics P.7
リモートコントロール P.13

目次

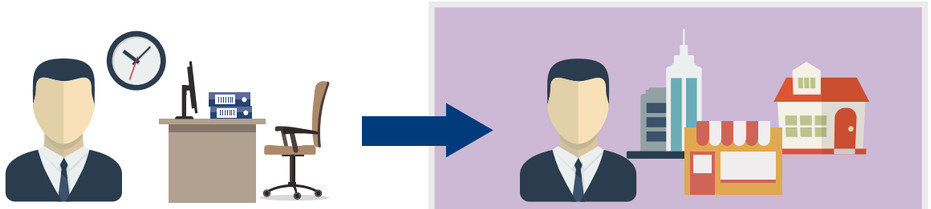
セキュリティ対策

IT資産管理

私たちを取り巻く環境

アフターコロナで続くテレワーク

コロナ禍で広がったテレワークは常態化し、どこでも働く事ができる様に…



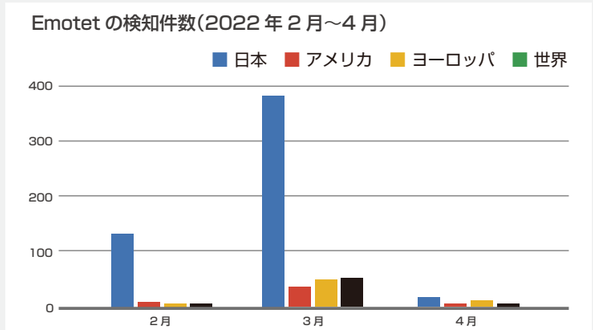
＜以前＞ 社内が基本

＜現在＞ いろいろな場所

ランサムウェア・標的型攻撃の激化

サイバー攻撃は巧妙かつ激化。
その上グローバルと比較しても日本は
最も狙われる国のひとつに…

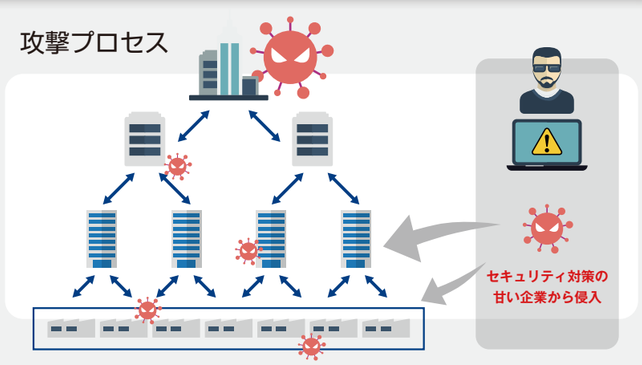
コロナ禍で猛威を振るったEmotetは、全世界の8割以上が日本に着弾しているという調査結果も。
攻撃者にとって、日本は狙いやすい国として認識されている様です。



サプライチェーン内の海外企業や中小企業を標的にしたサイバー攻撃

セキュリティ対策の甘い海外の
取引先や国内の中小企業から侵入。
大企業・グローバル企業を
狙い撃ち…

グローバル企業は、セキュリティ対策にも多額の投資を行いサイバー攻撃から身を守っています。
サプライヤーの中には中小企業も数多く存在していますが、その全ての企業がセキュリティ対策に投資できるわけではありません。
企業規模に関係なく、攻撃者はサプライチェーンの弱いところを突いて攻撃します。



様々な要因から企業を守るためのポイント

最低限行うべきこと

取引先・サプライヤーも含めた **全ての PC の脆弱性管理**

その次に行うべきこと

事業継続に必要な最低限守るべき情報を・・・

特定する

外部に流出した場合に取引先からの信用をなくす様な重要な情報や、競合他社に知られてしまうことで企業活動に支障を来す情報などが誰の端末にどのくらい保存されているかを把握します。

監視する

・USBに書き出されていないか
・大量に印刷されていないか
・メールに添付して送っていないか
・クラウドストレージにアップしていないか

検知 / 防御する

マルウェア感染防ぐためには、エンドポイントで多重の防御をする必要があります。また、感染や外部流出を素早く検知することもとても重要です。

分析する

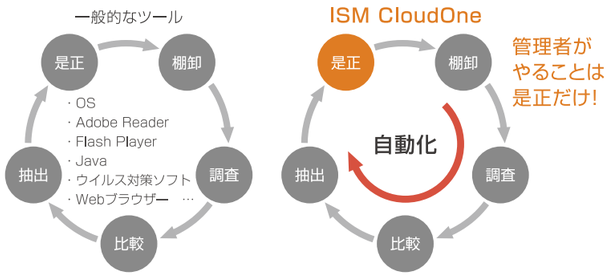
今までの様に操作ログを取得して溜めておくだけでなく、通常と違うふるまいをしているエンドポイントがないかを分析し、可視化することが大切です。

自動脆弱性診断

サイバー攻撃で狙われやすい「PCの脆弱性」を自動で診断!
レポート結果から必要な是正操作をシームレスに行うことができます

ソフトウェアのバージョン管理工数を大幅に削減

システムが端末の状態と「セキュリティ辞書」を1日1回突合させることで、どのPCに脆弱性があるか自動でレポート化します。
これにより、管理者はスムーズに対処を行うことが可能です。



セキュリティ辞書とは?

Windows更新プログラム、Adobe製品、Java、ウイルス対策ソフト、Webブラウザなどのあるべき姿(最新状態)が登録されたデータベース。
辞書が毎日更新されます。

セキュリティレベル診断

STEP1 企業全体のセキュリティレベルをひと目で把握

ダッシュボード(管理画面)

企業全体のセキュリティレベルを5段階で評価
OSのパッチ、ソフトウェアのアップデート状況、
ウイルス対策ソフトの導入状況などから全体を評価しています。

Windows更新
プログラムの適用状況

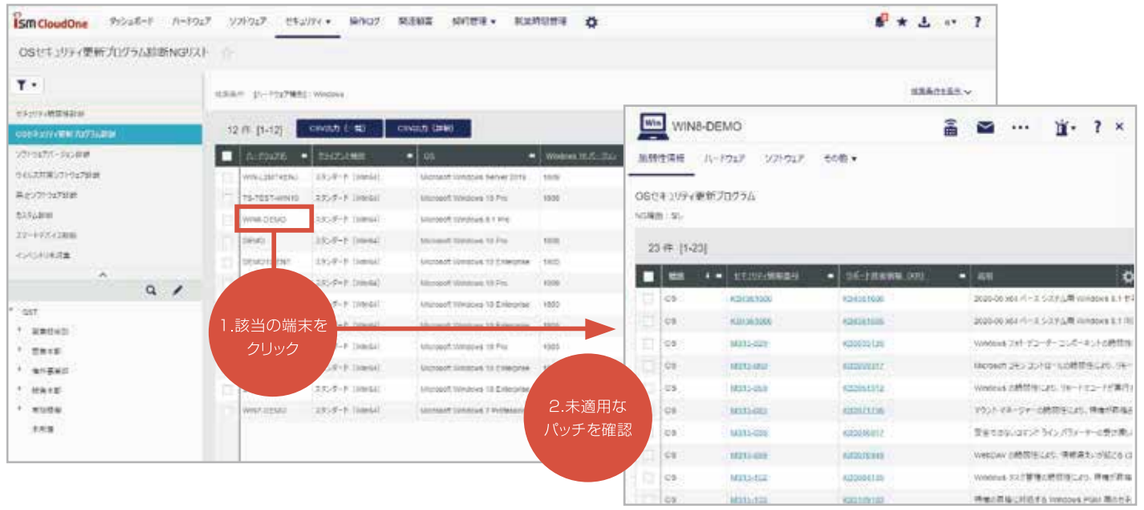
ソフトウェアの
アップデート状況

ウイルス対策ソフトの
導入・アップデート状況

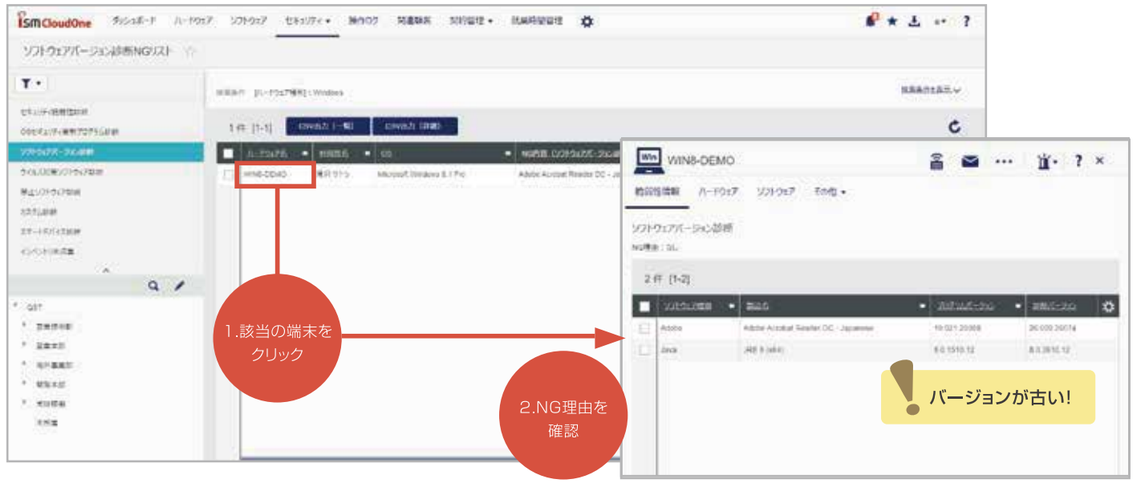
社内利用禁止ソフトウェアの
インストール状況

STEP2 NGリストから、各端末の詳細を確認

OSセキュリティ更新プログラム診断NGリスト



ソフトウェアバージョン診断NGリスト



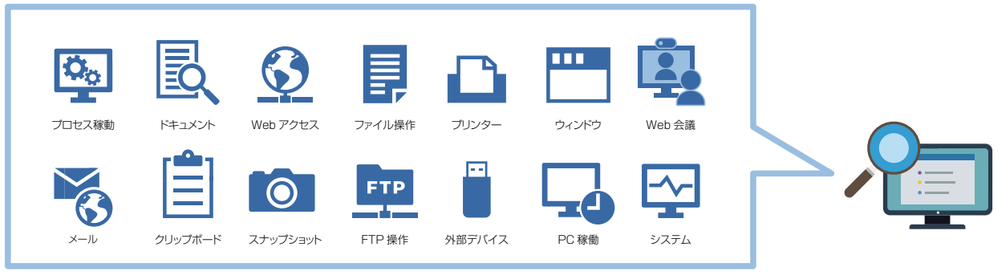
最新パッチの配布はファイル・ソフトウェア配布をご参照ください。

管理者側でソフトウェア自動更新を一括設定!

ソフトウェア自動更新機能を使えば、セキュリティ更新プログラムの自動適用を行えます。
ISM CloudOneではWindows Update、Adobe製品、Webブラウザーの更新設定を管理者側で一括に変更することが可能です。

豊富なログ取得機能で稼働状況確認に加え、長期保管でサーバー負荷の心配やメンテナンスが不要です

いつ/誰が/どのような操作を行っていたかの記録を取得するPC操作ログ収集。長期保管で過去起こったインシデントに対してもすぐに原因特定が可能です。 見やすいレポート・アラートで情報漏洩や不正インシデントの防止を簡単に実現します。



ログの長期保存が可能

サイバー攻撃の被害にあった際、企業はどこからどのように侵入してきたのかを追跡する必要があります。
ISM LogAnalyticsは最大7年間分の操作ログをコンソールから直接確認可能です。サイバー攻撃の被害にあったり、過去に発生したインシデントをアーカイブデータの掘り起こしといった作業時間を要せず確認することが可能で、オンプレミス製品と比較して物理的なストレージが不要なため、管理工数の削減を実現しております。

視認性を高める操作ログレポート

レポート画面から確認された異常値をクリックすることで、詳細情報の確認が可能です。
またスライダー操作によって期間内の異常値をスムーズに確認することができ 平常時と異なるPC操作の確認をスピーディーに行うことができます。

セキュリティレポート

■ファイル持ち出しレポート
外部デバイスへの書き出し回数を集計
■印刷レポート
印刷回数を集計
■メール添付送信レポート
ファイルを添付したメールの送信回数を集計
■Webアップロードレポート
クラウドストレージへのファイルアップロード回数

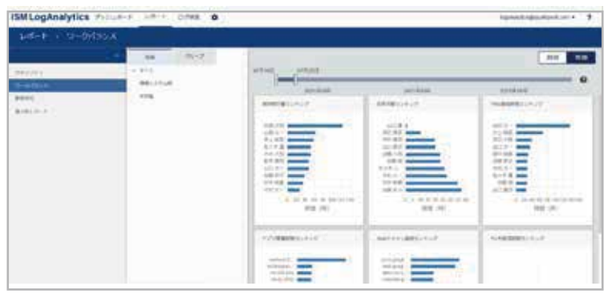
個人情報ファイルレポート

PC内の個人情報探査を行いリスクの洗い出しが行えます。
また個人情報が含まれているファイルの操作をレポートで容易に確認でき、個人情報漏えいにつながるユーザー操作の監視が行えます。
以下の個人情報を対象として監査可能です。

氏名 / 住所 / 電話番号 / メールアドレス / マイナンバー / 住民票コード / 免許証番号 / クレジットカード番号

ワークバランスレポート

■長時間労働ランキング
PCの稼働時間の多い順に集計
■効率労働ランキング
PCの稼働時間の少ない順に集計
■Webドメイン接続ランキング
アクセス数の多いWebドメインを集計
■Web接続時間ランキング
アクセス時間の長い順に集計
■PC未使用時間ランキング
PCの使用時間を集計
■アプリ稼働時間ランキング
全ユーザーが使用したアプリケーションのアクティブ時間を集計



勤怠状況レポート

「勤怠状況レポート」を提供します。 勤怠管理ツール※と連携し、当月・前月の残業時間や過去6ヶ月までの平均残業時間、また当年度・前年度の残業時間が一定時間を超えている社員の確認を容易に行うことができます。

個人別レポート

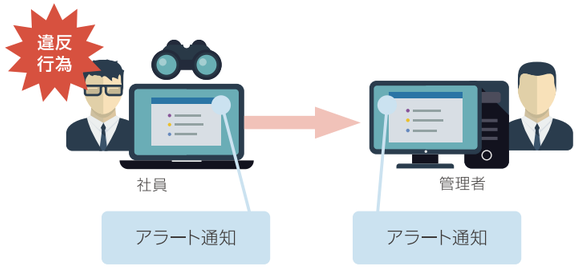
個人別にクライアントの利用状況が把握できます。業務時間外や休日時でのPC稼働状況が把握できるため、過度な残業やPCの私物利用をしていないかどうかといったことを確認することができます。

※連携している勤怠管理ツールの詳細は、当社営業へご確認ください。

操作ログ

オプション

クライアントPCの操作をログとして管理
問題発生時の早期発見や不正操作の抑止に役立ちます



取得可能なログ

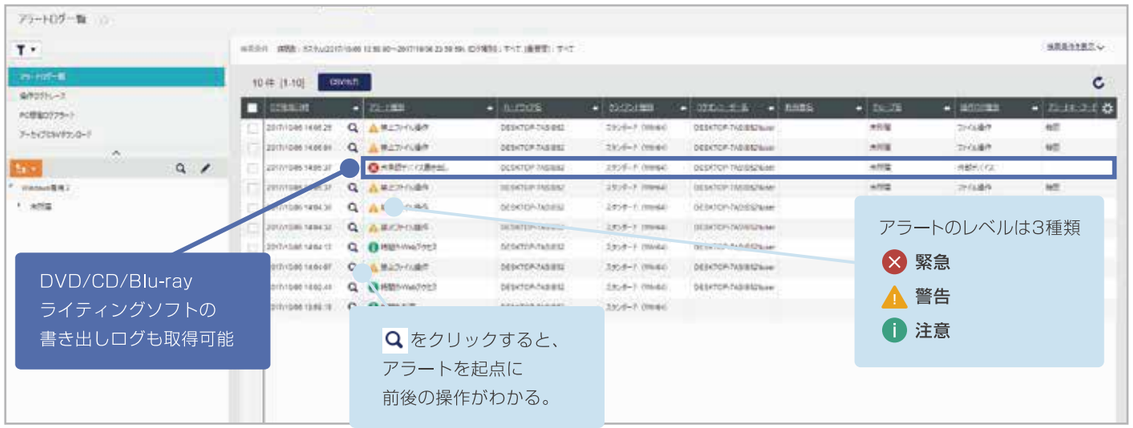
システム　外部デバイス　ドキュメントアクセス　ファイル操作　Webアクセス　クラウドストレージ

Webメール送信　PC稼働　プリンター

※Mac OSの操作ログ収集は一部制限事項がございます。

クライアントPCの操作を見える化

ポリシー違反を行っている端末の操作ログをアラートとして一覧化します。また、アラートが上がっている操作ログを起点に、該当端末の直近の操作も確認することができ、端末の操作を可視化します。



柔軟な検索機能で必要なログを追跡

管理者が全てのログを確認するのは膨大な工数がかかり、現実的ではありません。

柔軟な検索設定やアラートログだけを表示することで、無理なく不正な操作を発見することができます。

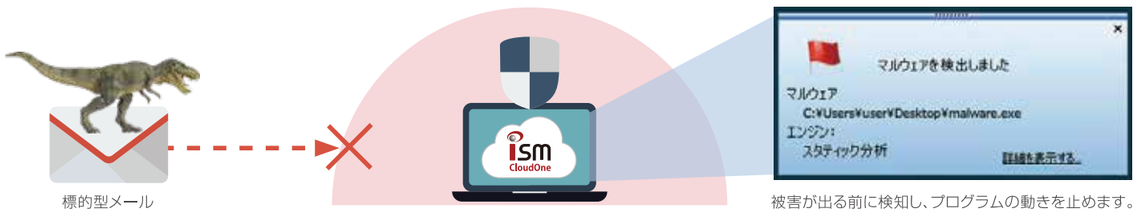
○ … 標準対応　- … 非対応　★ … オプション製品導入または個別サービスご契約の場合利用可

		操作ログ情報取得機能	ISM LogAnalytics	操作ログオプション	備考
操作ログ情報取得機能	操作ログレポート表示	セキュリティレポート / ワークバランスレポート	★	ー	
	PC 稼働ログ	電源 ON・OFF	★	★	
	OS ログイン・ログオフ	ログイン・ログオフ / スタンバイ（スリープ）	★	★	
	ドキュメントアクセスログ	ファイル参照	★	ー	
		ファイル参照（拡張子指定）	★	★	
	ファイル操作ログ	書き込み / コピー / 移動 / 削除	★	★	
	プロセス稼働ログ	アプリケーションの起動 / 終了	★	ー	
		プロセスログ	★	ー	
		アクティブウィンドウタイトル	★	ー	
	クリップボード操作	コピー	★	ー	
	スナップショット		★	ー	
	ウィンドウタイトルログ	アクティブウィンドウタイトル	★	ー	
		ウィンドウアクティブ時間取得	★	ー	
	システム日時変更		★	★	
	印刷	印刷ログ	★	★	
	外部デバイス接続	デバイス挿抜	★	★	
	メール送受信 (POP3 / SMTP)	メール送信	★	ー	
		メール受信	★	ー	
		メール送信時の本文	★	ー	
		添付ファイル名	★	ー	
	Web メール送信	メール宛先	★	★	
		メール本文	★	★	
		添付ファイル名	★	★	
	Web アクセス	Web アクセス	★	★	
		SNS 書き込み	★	★	
		ファイルアップロード	★	★	
	FTP	FTP コマンド	★	ー	
	アラート設定	アラート設定ログ	★	★	
	管理者操作ログ	コンソール操作ログ	★	★	
	操作ログトレース		★	★	
	操作ログ詳細		★	★	
	ポリシー	基本ポリシー設定	★	★	
		個別ポリシー設定	★	★	
	コンソール閲覧権限	管理者	★	★	
		グループ管理者	★	★	
		部分表示（ログのみ / 勤怠のみ）	★	★	
	勤怠	CSV データ取り込み	ー	★	
		残業時間集計	★	★	
		個人別レポート（PC 稼働ログ）	★	★	
		個人別レポート（PC 稼働 + 勤怠）	ー	★	
		クライアント通知 / 制御	ー	★	
	OS 等	Mac ログ	★	★	
		Windows 7 以降	★	★	
		Windows Server 2008 以降	★	★	
		リンククローン	ー	★	
	API 連携ツール		ー	★	
	他社ログ取り込み		★	ー	
	ポリシー反映タイミング	定期反映	4H	4H	
		PUSH 要求（設定同期）	ー	★	
	ログ取得タイミング	指定サイズ超過時	ー	★	
		定期送信	★（最大 40 分）	★（最大 30 分）	
		アラート発生時	★	★	
		起動	★	★	
	通知タイミング	管理者メール	★	★	アラート発生時
	GDPR		ー	★	

ふるまい検知

オプション

プログラムの特徴や動きを監視し、標的型攻撃などの未知の脅威からPCを守ります



被害が出る前に検知し、プログラムの動きを止めます。

静的＋動的分析で未知の脅威をブロック

ふるまい検知機能は、5つのエンジンを使ってマルウェアを検知します。静的＋動的と多層で防御することでゼロデイ攻撃や高度な標的型攻撃をエンドポイントで防御します。

脆弱性対策	自動脆弱性診断	ZDP
静的分析	Sandbox	Static
動的分析	HIPS	機械学習

マルウェア検知情報を一覧で把握！

マルウェアが検知された端末を一覧で確認できます。
また、検知された際は管理者にアラートを送信することができます。一覧から端末をクリックすることで、検知されたファイルのパスや駆除ステータスなどを確認することができます。

検知実績（ピックアップ）

マルウェアの種類	未知の脅威および標的型攻撃	発生報道時期	防御エンジンリリース時期
Emotet	「Emotet」（2022 年 3 月版） 「Emotet Downloader」（2021 年 11 月版） 「Emotet」（2020 年 2 月版）	2022/3 2021/11 2020/12	2019/1 2019/1 2018/2
ランサムウェア	「Conti」（2022 年 2 月版） log4j の脆弱性攻撃に使用されたランサムウェア「NightSky」	2022/2 2022/1	2019/1 2019/1
特定のイベントや事象に関連する攻撃	ワクチン予約を装うフィッシングサイトに関するマルウェア 東京オリンピックに関係する日本語のファイル名をもつマルウェア	2021/9 2021/7	2021/5 2019/1
標的型攻撃	国内防衛産業を標的としたマルウェア 日本年金貿易を狙ったマルウェア「Emdivi」	2017/8 2015/6	2016/10 2014/8

URLフィルタリング（Web接続制御）

オプション

不審なサイトの閲覧やストレージサービスへのアクセスを制限し内部からの情報漏えいを未然に防止します

柔軟で容易な設定

カテゴリ別ルール登録
部署·グループ毎にポリシー設定が可能です。

スケジュール設定
曜日や時間帯に応じて柔軟にルールを適用できます。

社内外問わず端末に同じポリシーが適用できます。

国内最高水準のURLデータベース

カテゴリ数 148、登録数 57 億件以上（2022年10月時点）

通信業者や公的機関など、さまざまなルートからURLを収集し、カテゴリ毎に分類したものをURLデータベースとして登録しています。
国内シェアNo.1を誇る、URLデータベースにより柔軟なフィルタリングとセキュアなインターネット環境を実現します。

URLデータベースカテゴリ			
不法	セキュリティ	出会い	金融
ギャンブル	ショッピング	ITサービス	コミュニケーション
ビジネス·経済	過激な表現	青年・成人向け	趣味と娯楽
生活と暮らし	医療と健康	学術・教育	政治・行政
広告	迷惑メール	ニュース	各種サービス
各種産業	システムコンテンツ	アダルト・フェティシズム	
プロバイダ・ポータル・ホスティング			

リモートコントロール

インターネット経由のリモート操作で、業務の効率化を実現します

簡単操作でリモートコントロール

クライアントを選択してリモコンボタンをクリックするだけで簡単にリモート操作を開始することができます。

リモート操作時にはクライアント側にも通知がされます。

ファイル転送

管理者端末からリモコン先にファイルを転送することができます。

インターネット経由でリモートコントロール　（個別サービス「クイックリモコン」）

社内ネットワーク内の端末はもちろん、インターネット経由でのリモート操作も可能です。
海外を含む遠隔拠点のトラブル対応にも役立ちます。
またクライアント･管理者双方向のファイル転送も可能なため、離れている拠点のヘルプデスク対応などにも役立ちます。

クイックリモコン とは？

クイックリモコン

クイックリモコンは安定した環境で素早くトラブルが発生している端末のリモート操作が可能です。そのため、管理者は現地に向かう必要がなく、工数を大幅に削減できます。

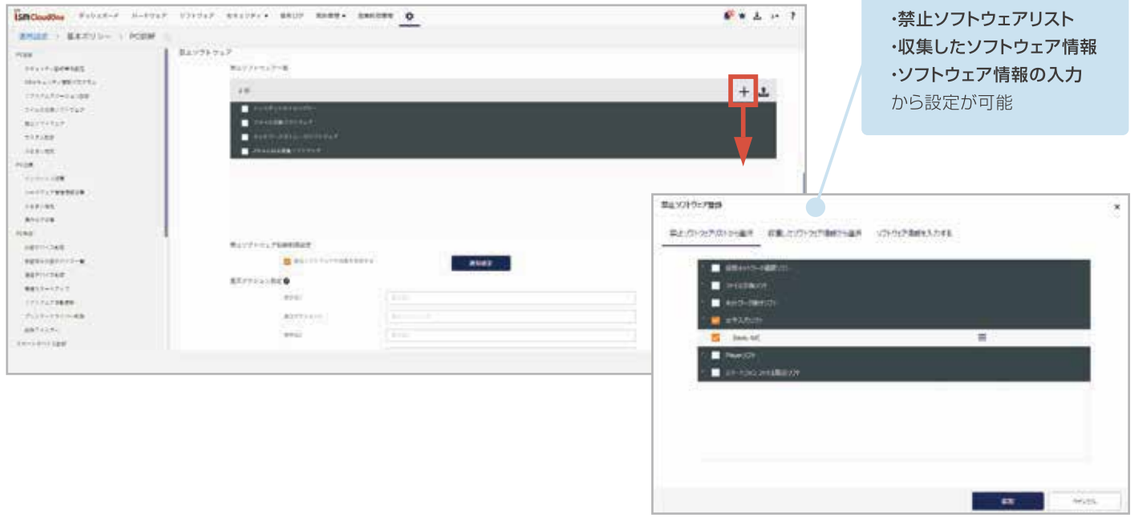
社内LANに接続しているPCはもちろん、インターネットを経由して海外拠点などの遠隔地にあるPCに対してもリモート操作が可能。社内LANにアクセスできない端末の運用管理も支援します。

※個別サービスとなります。

禁止ソフトウェア起動制御

用意されたブラックリストから、企業にリスクのあるソフトウェアの利用制御を簡単に行えます

管理者設定画面



・禁止ソフトウェアリスト
・収集したソフトウェア情報
・ソフトウェア情報の入力
から設定が可能

ハッシュ値から制限できます。

クライアント画面

起動制御と共に、
ユーザーにはポップアップで通知

ブラックリスト=禁止ソフトウェアリストで簡単制御！

情報漏えいに繋がる恐れのあるソフトウェアをリストアップしたデータベースを搭載！
定期更新を行っており、現在では10,000種以上が登録されています。管理者はこのリストから禁止したいソフトウェアを選択することで簡単に起動制御をかけることができます。

※2021年8月現在

Windows 10管理運用支援

WindowsOSの定期的なアップデートなどの制御が可能
管理者の管理効率向上に役立ちます

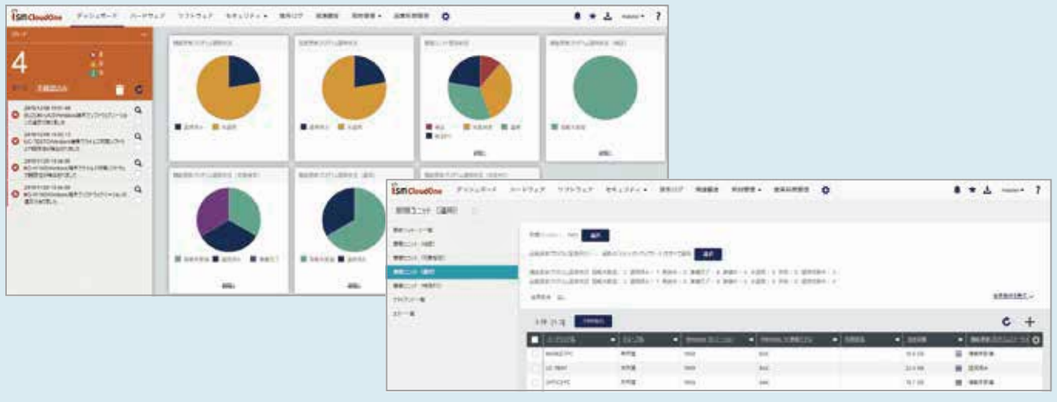
Windows 10アップデート制御

Windows 10の大型アップデートである、機能更新プログラム(Feature Update、FU)のインストールの時期を決定するブランチ準備レベル(SAC、SACT)の指定や、機能更新プログラムや品質更新プログラム(Quality Update、QU)の適用を延長する日数を指定できます。
大型アップデートが適用される時期をコントロールすることで、配信されてから十分な準備期間を設けることと、同時期にアップデートされることを防ぎ、負荷分散することが可能となります。

Windows 10アップデート支援

オプション

社内にアプライアンスサーバーを設置することで、社内ネットワーク経由でWindows 10の機能更新プログラムと品質更新プログラムが配布できます。
Windows 10のFUとQUを分散配布し、Windows 10の運用負荷とネットワーク負荷を軽減します。
ISM CloudOneがFUやQUのアップデートの有無を毎日確認し、更新がある場合は更新プログラムを適用するためのパッケージ生成を自動で行います。
ダッシュボードでユニットごとの適応状況を確認することができます。対象のユニットをクリックすると、PCごとの詳細を確認できます。また、適用に失敗したPCのエラー内容も確認できます。



高速スタートアップ制御

高速スタートアップの設定ON/OFFができます。
アプリケーションのインストール後に必要な再起動が行われず、長期間インストールが完了しないといった、管理者による管理が行き届かないケースを解決することが可能になります。

※一部機能に制限がございます。
※ISM CloudOneによる制御設定よりも、Windowsグループポリシーでのアップデート制御設定が優先されます。
※高速スタートアップ制御はWindows 10のみ対象となります。

Windows Defender制御機能　（個別サービス「 DefenderControl 」）

Windows 10の端末に標準搭載されているWindows Defenderの設定を制御し、端末ごとの設定状況やマルウェアの検知状況を可視化します。Windows Defenderの設定をコンソールで遠隔操作や一括管理ができ、クライアントPCのセキュリティを担保できます。
また、レポートからスキャン結果の確認も可能です。

DefenderControl とは？

DefenderControl

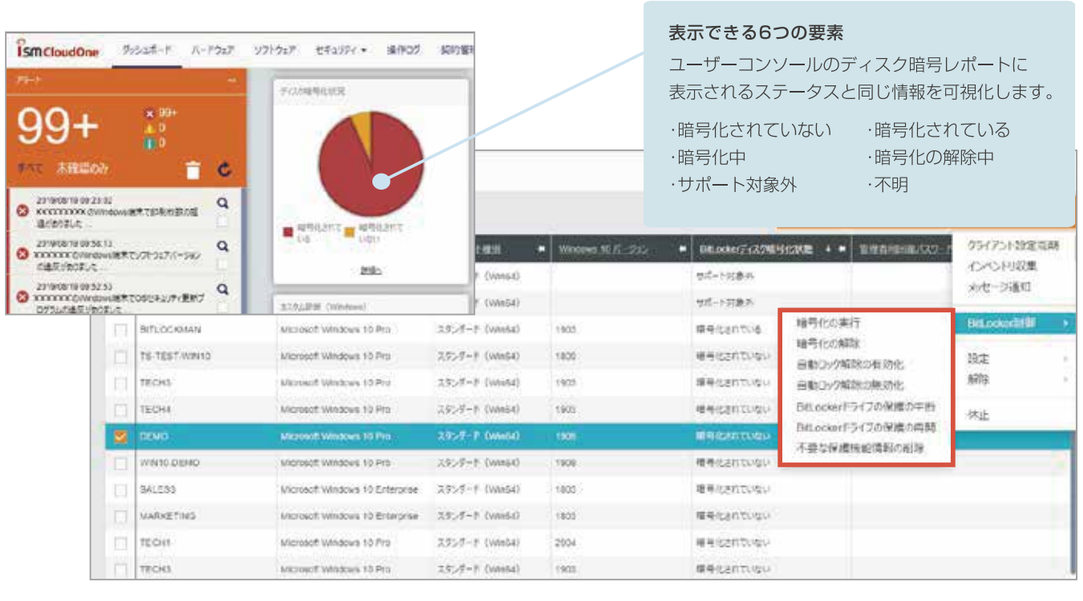
「 DefenderControl 」は、Windows に標準で搭載されている「Windows Defender」の設定情報管理や制御ができます。

※個別サービスとなります。

紛失した時こそ必要なクラウド管理

BitLocker管理・制御

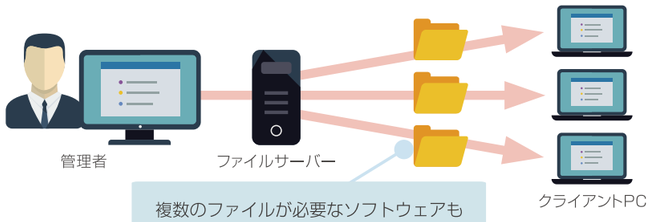
BitLockerの保護情報をダッシュボード上に可視化し、クライアント毎のハードディスク暗号化状況がわかりやすく表現されています。
クラウドだからこそ、いざというときも、持ち出し端末の暗号化の確認やコントロールが可能です。



ファイル・ソフトウェア配布

セキュリティパッチの適用や、管理者が任意に設定したファイルなど、クライアント端末への一斉配布が行えます

社内ネットワーク経由でソフトウェア、
ファイル・フォルダ、レジストリなどの
配布・実行が可能です。
レジストリ値については、追加・編集、
エントリーの削除、キーの削除を行う
ことができます。

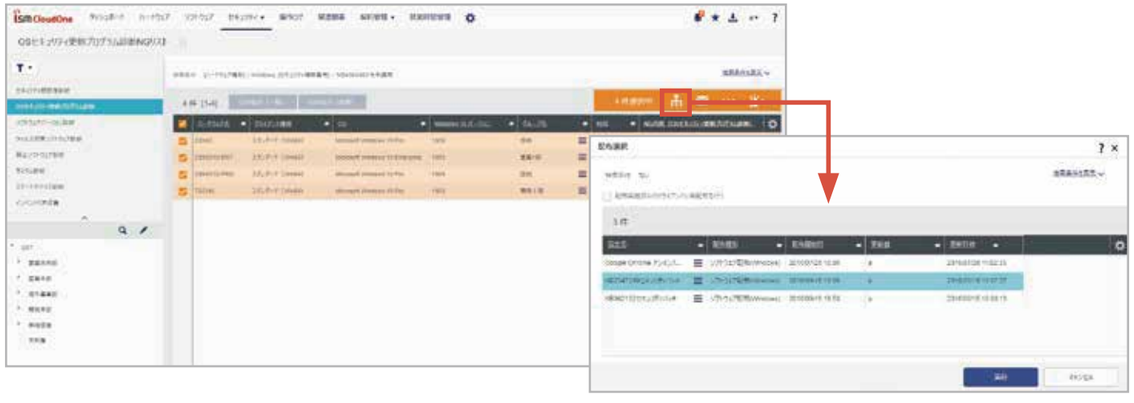


複数のファイルが必要なソフトウェアも
配布後実行が可能です。

STEP1 配布したいソフトウェアを登録

配布方式を選択できるので、
柔軟な運用を行えます。
＜配布方式＞
・ユーザー任意のタイミングで配布
・強制配布

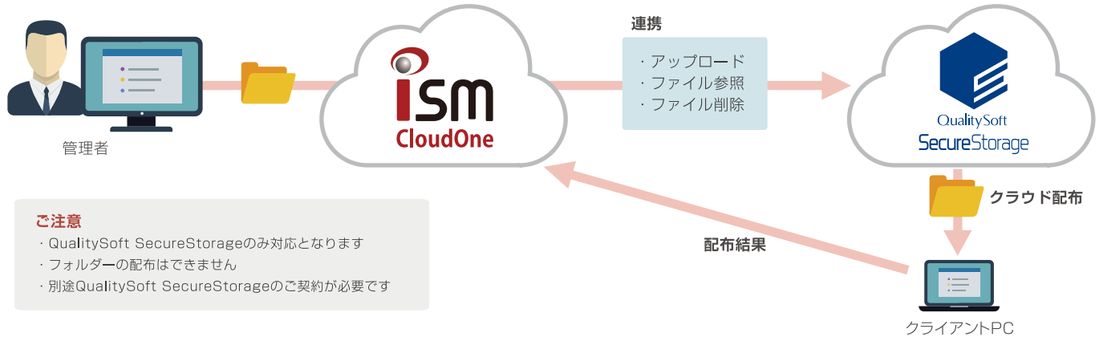
STEP2 対象者を選択し実行



オンラインストレージと連携することで、ファイルやソフトウェアをクラウド経由(インターネット)で配布できます

クラウド配布

QualitySoft SecureStorage（※別途ご契約）と連携することでクラウド経由でファイルやソフトウェアを配布することができます。
クラウド配布ができるため、社内ネットワークに繋がっていない端末に対してパッチ配布や脆弱性対策が可能です。
ISM CloudOneコンソールからファイルのアップロード、削除、参照やアップロード先のストレージ残容量の確認もできます。



ご注意
・QualitySoft SecureStorageのみ対応となります
・フォルダーの配布はできません
・別途QualitySoft SecureStorageのご契約が必要です

QualitySoft SecureStorageとは？

オプション

QualitySoft SecureStorage

「QualitySoft SecureStorage(QSS)」は、高セキュリティかつ低コストで
社内外のファイル共有を実現できる企業向けオンラインストレージです。

高度なセキュリティ

最新の暗号化アルゴリズムを採用し
様々な脅威からデータを守ります。
ウイルスチェックや、デバイス認証、IP
アドレス制限、ワンタイムパスワード
などの必須機能もあります。

ユーザー数無制限

他社の企業向けクラウドストレージとは違いユーザー数に制限はありません。
必要分のストレージ容量をお求めください。

他社比較

	QSS	A社	B社
ストレージ容量	**500GB**	無制限	ユーザーあたり1TB
ユーザー数	**無制限**	ユーザー従量課金	ユーザー従量課金

※QSS スタンダードプランの場合

就業時間管理

※画面はイメージです。実際の画面と異なる場合がございます。

時間外労働の超過をデバイス側から抑制します

従業員の勤務時間を把握し、時間外労働の超過をパソコンなどのデバイス側から抑制することができます。
ISM CloudOneは、働き方関連法案の中でも右記の4つの改正内容に対応します。

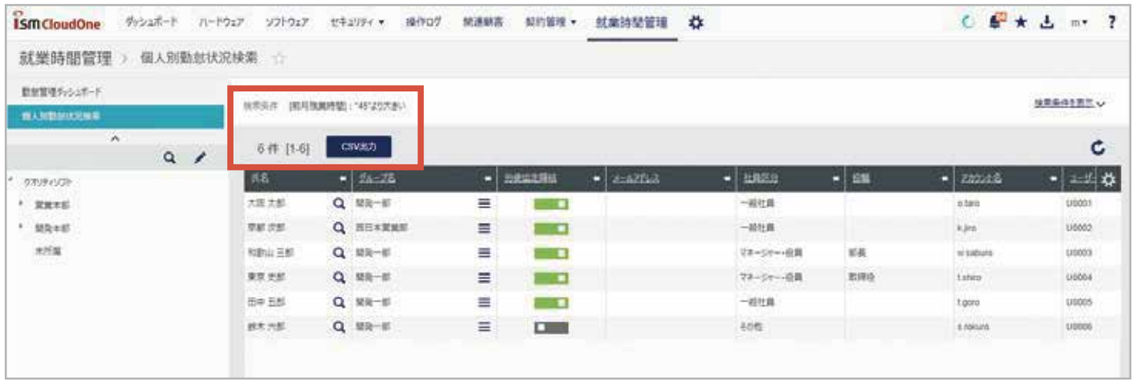
- 時間外労働の上限抑制
- 産業医との連携による保健機能の強化
- 「労働時間の適正把握」の義務化
- 勤務間インターバル制度の普及促進

時間外労働の上限規制

勤怠管理ダッシュボードから、時間外労働時間が上限を超えている従業員の人数や、月間・年間を通して時間外労働が多い従業員を把握し、残業抑制などのアクションにつなげることができます。
時間外労働が上限に達したときや定時退社日には、パソコンをシャットダウンして残業をさせないようにすることが可能です。
また、上限に近づいた従業員に注意を促し、上限を超えてしまうことを事前に予防することもできます。

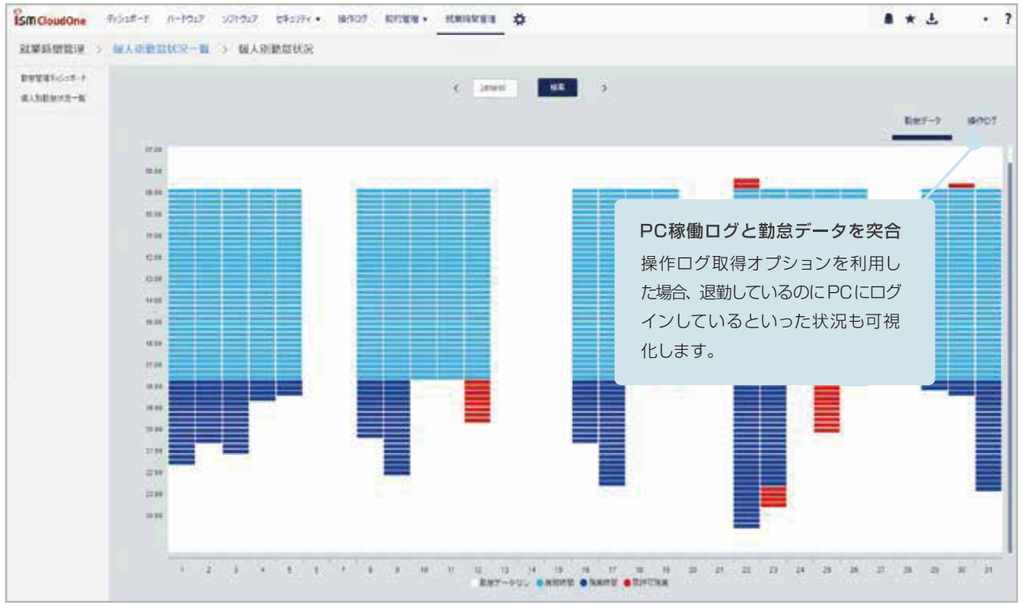
産業医との連携による保健機能の強化

長時間労働を行っている従業員の勤務状況を産業医に提出する場合があります。
必要な情報を検索し、CSVファイル形式で出力することができます。



「労働時間の適正把握」の義務化

実働労時間をグラフで可視化します。
従業員の労働時間を適切に把握することができます。



PC稼働ログと勤怠データを突合
操作ログ取得オプションを利用した場合、退勤しているのにPCにログインしているといった状況も可視化します。

勤務間インターバル制度の普及促進

業務終了後、設定した勤務間インターバル内に業務を開始しようとした従業員に対して、メッセージを表示させたりパソコンを強制的にシャットダウンすることで、十分な休息時間を設けるよう促すことができます。

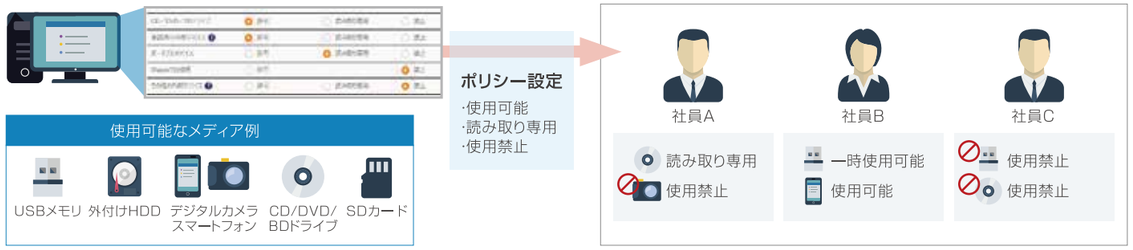
外部デバイス制御

オプション

USBメモリやCD、スマートデバイスなどの外部デバイス利用を制御し、ファイル持ち出しによる情報漏えいを防ぎます

用途に合わせて様々なメディアの利用を制限

USBメモリやCD、スマートデバイスなどの外部デバイス利用を制限することができます。
デバイスの種類ごとに制御方法を設定。個人別、グループ別にポリシーを設定することもできます。



デバイス毎の設定で柔軟な運用が可能

デバイスの種類毎に制御方法が
設定可能です。
個人別、グループ別にポリシーを
設定することもできます。

予め登録した
デバイスのみ
許可することも可能!

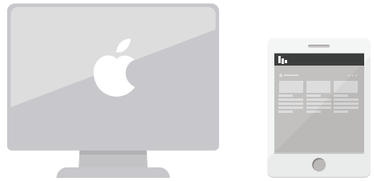
ワークフロー機能で申請・承認作業を効率化

一時的に利用が必要な場合、ユーザー側から管理者に
期限を設けて利用許可申請を送信することもできます。

ユーザー画面　　管理者画面

Macクライアントに対応

Macクライアントに接続されたUSBメモリやCD/DVDドライブを制御することが出来ます。接続されたデバイス情報はISMサーバーに収集され、使用履歴として保存されます。
Macクライアントから利用申請を提出することもできます。
※一部制限事項がございます。



許可していないWi-FiやBluetoothの利用を制限し、通信デバイス経由のセキュリティリスクに対応

通信デバイスの使用を制御

社内ポリシーで許可したWi-Fiにのみ接続させることが可能です。
盗聴や悪意のアクセスポイントなどの危険性がある公共のフリーWi-Fiには接続させない運用や、
特定のWi-Fiには接続させる運用、自由な機器接続によるデータ転送を禁止することができます。

※SSIDの制限はTCP/UDPプロトコルの通信が対象
※Bluetooth通信制御はMicrosoft製のBluetoothドライバのみ対象
※Windowsのみ対象

SSID登録ではワイルドカードが使用可能

ハードウェア・ソフトウェア管理

ハードウェア・ソフトウェアの情報を自動で収集
手間を掛けず端末の利用状況を把握することができます

ハードウェア・ソフトウェア情報を自動で収集

社内で利用されているクライアント端末のハードウェア情報やソフトウェア情報を自動的に収集し、レポート化します。

柔軟なフィルター、検索機能で
棚卸しにかかる工数を
大幅に削減します。

取得可能な項目							
クライアント情報	OS情報	BIOS情報	TCP/IP情報	Windows Update情報	外部デバイス制御	Windows10バージョン	高速スタートアップの状態
利用者情報	IE情報	メモリ情報	ディスプレイ情報	自動アップデート情報	リモートロック状態	Windows10更新モデル	
PC情報	CPU情報	HDD情報	デバイス情報	操作ログ	ディスク暗号	Windows10アップデート適用延長日数	

アンケート収集機能も搭載　資産管理に必要な情報に対して、アンケート形式でユーザーから情報収集することもできます。

オフライン機器管理／ハードウェア契約管理

ネットワークに接続されていないオフライン端末を登録、管理することができます。オフライン端末は管理画面からの登録またはCSV形式で一括登録が可能です。登録された端末は、ハードウェア一覧より確認できます。
リース・レンタル端末の契約先や開始日・終了日といった契約情報を登録・管理できます。また、契約情報と紐付けて棚卸端末を一覧で表示します。

契約情報の登録

登録できる情報
契約種別：リース/レンタル/購入
機器種別：PC/スマートデバイス/プリンター/
　　サーバー機/その他
契約責任者、保管場所、契約数、契約開始・終了日　など

棚卸機能

ワンクリックで棚卸状態の
切り替えができます。

ソフトウェアライセンス管理

ソフトウェアの購入状況と使用状況を可視化し、
ライセンス利用状況をレポートします

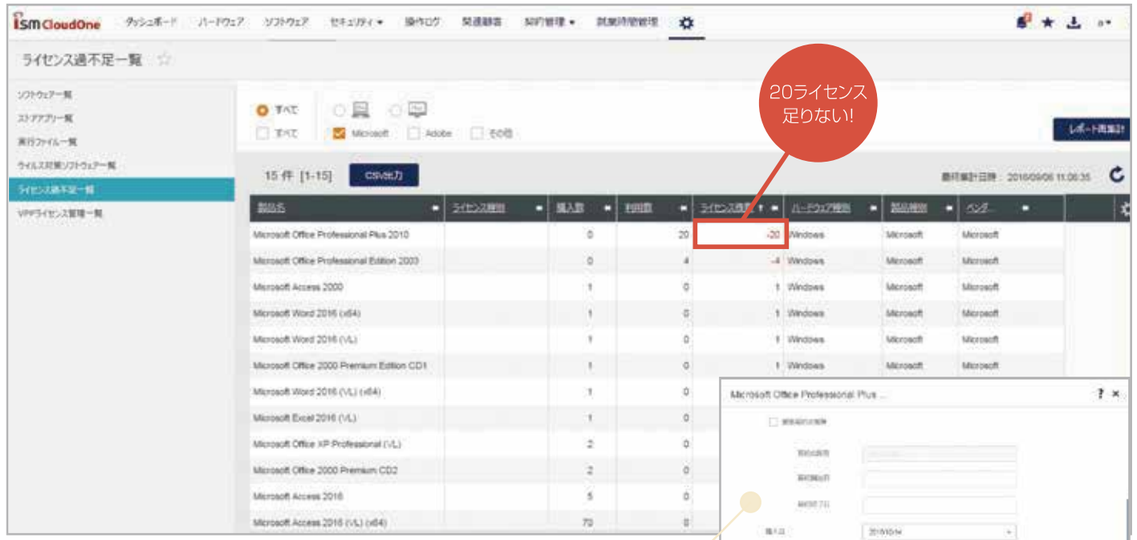
Microsoft Office製品やAdobe製品などを管理できる、管理台帳機能を搭載しています。
ライセンス種別や形態、インストール状況などの詳細を表示します。
保有ライセンス数と突き合わせることで、ライセンス数の過不足状況を可視化し、適切なライセンス管理の運用を支援します。

STEP1　購入したソフトウェアを登録

STEP2　端末から情報を収集

STEP3　過不足状況をレポーティング

ライセンス過不足一覧



購入状況に合わせてソフトウェアを登録！
契約期限の情報や、ライセンス種別・形態・管理番号などの
購入情報を入力。適切なライセンス管理を行えます。

スマートデバイス管理

PCだけでなく、スマートフォンやタブレットもまとめて1コンソールで管理することができます

PCとスマートデバイスを一元管理

ISM CloudOneは、PCもスマートデバイスも同一のコンソールで一元管理します。
管理ツールを別々に用意する必要がないので、管理の無駄を省くことができます。

ハードウェア名	クライアント種別	利用者名	グループ名	OS
DEMO10-ENT	スタンダード（Win64）	安藤 サブロー	営業1部	Microsoft Windov
+819000000000	iOS（クライアントプログラム）		未所属	iOS 13.3
SALES3	スタンダード（Win64）	伊藤 マサキ	営業	Microsoft Windov
MARKETING	スタンダード（Win64）	赤井 ショウ	マーケティング	Microsoft Windov
07000000000	スタンダード（Android）		未所属	Android 5.1.1
SALES2	スタンダード（Win64）	福田 ミライ	営業	Microsoft Windov
SALES1	スタンダード（Win64）	前田 ハルナ	営業	Microsoft Windov
TS-Mac mini	スタンダード（Mac）		未所属	macOS 10.15.1
WIN-L2MTKENJV15	スタンダード（Win64）		未所属	Microsoft Windov

アプリケーション管理

管理者側からアプリケーションの配布や
配布したアプリケーションの削除を
行うことができます。

また、社内で利用を許可している
アプリケーションをダウンロードできる
アプリケーションポータルを
作成することができます。

アプリケーションポータルは
企業･グループ毎に設定可能。

その他スマートデバイス管理に役立つ機能が多数

JailBreak･
Root化検知

アプリケーション
起動制御

SDカード

Wi-Fi
ネットワーク設定/
Bluetooth制御

※スマートデバイス管理機能は、OSにより一部機能差および制限があります。

盗難・紛失時における第三者の不正利用や重要データの漏えいリスクを軽減することができます

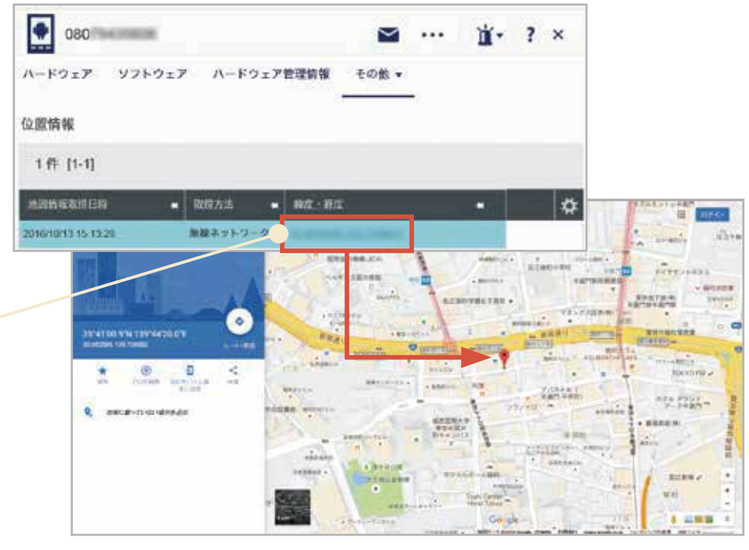
紛失時の緊急操作

持ち歩いて利用するスマートデバイスは、紛失や盗難などのリスクを避けられません。
ISM CloudOneは、紛失･盗難などの緊急時にリモートロック･ワイプといった操作を遠隔で実行することができます。

位置情報の取得

GPSで位置情報を取得し、現在地を確認することができます。
紛失した端末の発見や、社員の行動管理に役立ちます。

クリックすれば
ブラウザで地図を開きます。



グローバル対応

海外の拠点にあるデバイスもまとめて管理！
世界中55ヶ国以上で利用されています

導入国

·シンガポール	·香港
·マレーシア	·スイス
·タイ	·アメリカ
·インドネシア	·カナダ
·ベトナム	·ブラジル
·フィリピン	·オーストラリア
·台湾	など

グローバル対応

端末環境·管理者環境とも日·中·英の3ヶ国語に対応！国内のみならず、海外拠点の端末管理が可能です。
エージェントがOSの言語設定を自動で判断し、表示言語が選択されます。

日本語　中国語　英語

導入事例

グローバルで300社を超えるグループ会社
エンドポイントセキュリティのリスクを見える化してセキュリティ強化に取り組む

豊田通商株式会社

トヨタグループの総合商社としてグローバルに事業を展開している豊田通商株式会社（以下、豊田通商）は、300社を超える事業会社すべてでグローバルITガバナンスを強化するため、ネットワークの標準化とOffice 365によるメールの標準化を推進。同時に、エンドポイントセキュリティの強化を行うため、グローバル対応のISM CloudOneを導入している。

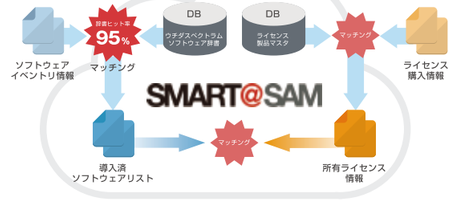
※詳細は当社Webページにて公開中！

お客様のさまざまなご要望にお応えするため、ISM CloudOneは、アライアンスを推進しています。

ソフトウェアライセンス管理
ウチダスペクトラム社：SMART@SAM

ISM CloudOneで収集したソフトウェアのインベントリ情報と、SMART@SAMが保有するソフトウェア辞書を突合し使用許諾に基づいてライセンス情報を紐付け、ソフトウェア導入状況を可視化しメーカーごとの使用許諾に沿った管理を行います。
専門家の支援のもと、ソフトウェア資産管理運用（SAM）で必要な4台帳（導入ソフトウェア／所有ライセンス／ライセンス関連資産／ハードウェア）を作成しSAMを行うベースラインを作成、維持します。

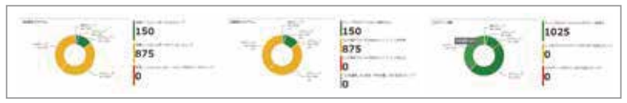
「API 連携」
インポート可能な
形式で自動出力！



専門家による辞書更新、
ライセンス管理を
トータルでサポート

Windows 10アップデート支援
横河レンタ・リース社：Unifier Cast

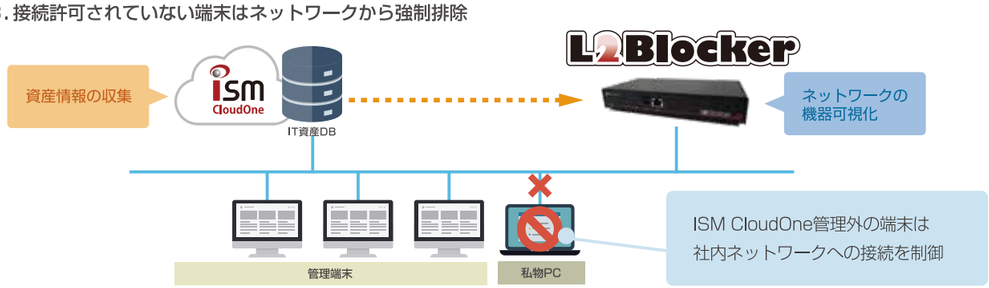
Unifier Castは、Windows 10のアップデート運用を支援するソリューションです。ネットワークの負荷を考えたアップデートの分散配布（分割配信機能、キャスト配信機能）や、アップデートの適用進捗や運用、結果がひと目でわかるダッシュボード機能などがあります。これにより、情報システム部門の運用工数増加や配布によるネットワーク負荷、アップデート対応など、Windows 10の運用に関する課題の解決をサポートします。



不正PC検知・排除
ソフトクリエイト社：L2Blocker

ISM CloudOneで管理している機器などのインベントリ情報をL2Blockerと共有し、 管理されていない端末を検出、また、利用を認めていない端末やWi-Fiルーター等を社内ネットワークに接続させない環境を構築します。

1. 管理端末の情報を収集、接続されている機器を把握
2. IT資産管理データと突き合わせ、管理されていない端末を検出
3. 接続許可されていない端末はネットワークから強制排除



機能一覧

※2021年10月現在の情報です。
※制限事項や機能詳細は当社Webサイトをご確認ください。
※動作環境はクオリティソフト社のWebサイトをご確認ください。

○…標準機能　—…非対応　★…オプション製品導入の場合利用可

		機能	ISM CloudOne Win	ISM CloudOne Mac	備考
セキュリティ対策	脆弱性診断・レポート	OSセキュリティ更新プログラム診断	○	—	
		禁止ソフトウェア診断	○	—	
		ソフトウェアバージョン診断	○	—	Adobe社製品 / Java / Webブラウザ
		ウィルス対策ソフト診断	○	—	
		カスタム診断	○	—	
		インベントリ未収集	○	○	
		外部メディア挿入・取り出し履歴一覧	★	★	
		操作ログ	★	—	Webアクセス / メディア書き込み / 稼働状況 等
		マルウェア検知率・駆除状況	★	—	
		ディスク暗号化状態	○	—	
		診断辞書提供サービス	○	—	
	PC制御	ソフトウェア自動更新	○	—	Windows Update / Adobe社製品 / Webブラウザ
		禁止ソフトウェア起動制御	○	—	
	操作ログ	「操作ログオプション」及び「ISM LogAnalytics」は操作ログの表をご確認ください。			
	外部デバイス制御	USBメモリ / SDカード	★	★	
		ポータブルデバイス（デジタルカメラ、携帯電話、スマートフォンなど）	★	—	
		CD / DVD / Blu-ray / FD	★	★	Macの場合、CD / DVDはドライブによって制御できない場合があります
		iTunes経由の接続	★	—	
		通信デバイス（有線LAN、Wi-Fi、Bluetooth）	★	—	
	ふるまい検知	マルウェア検知・隔離	★	—	
	URL フィルタリング（Web接続制御）	フィルタリングデータベースによる書き込み規制	★	—	
		フィルタリングデータベースによる接続規制	★	—	
	紛失対策	HDD暗号・復号	★	—	クラウド版のみ提供。BitLocker管理・制御は標準機能です
		ファイル / フォルダ削除	○	—	Windows 8 以降対応機能
	Windows Defender制御	Windows Defender 設定一括管理	★	—	個別サービス「Defender制御Control」
		マルウェア検知状況の可視化	★	—	個別サービス「Defender制御Control」
		スキャン実行結果の確認	★	—	個別サービス「Defender制御Control」
IT資産管理	診断・レポート	ハードウェア一覧	○	○	
		ソフトウェア一覧 / ストアアプリ一覧	○	○	ストアアプリ一覧は Windows のみです
		ソフトウェアライセンス過不足一覧	○	○	
	ソフトウェアライセンス管理	契約情報管理	○	○	
		販売種別判定	○	—	Adobe社製品 / Microsoft Office
	ハードウェア管理	棚卸一覧	○	○	
		ハードウェア契約	○	○	
		ファイル / フォルダ配布	○	—	
	配布	ソフトウェアリモートインストール	○	—	
		レジストリ変更（文字列型）	○	—	
		プリンタドライバ（設定変更）	○	—	キヤノン製プリンタドライバ対応
		Windows 10アップデート支援	★	—	Feature Update / Quality Update対応
		フォルダ配布指定（複数ファイル一括配布）	○	—	
	オフライン機器管理	USBメモリによるオフライン収集	○	—	
		オフラインPC / 任意デバイスのCSVインポート	○	○	
	リモートコントロール	LAN対応	○	—	
		インターネット対応	★	—	サービスプロバイダー提供状況による

		機能	ISM CloudOne Win	ISM CloudOne Mac	備考
	Active Directory連携	組織情報のAD連携	○	—	
	メッセージ通知	メッセージ通知	○	—	
システム	関連顧客管理	関連顧客セキュリティ状況	○	○	
		セキュリティ状況一覧	○	○	
	運用セキュリティ	コンソール操作ログ記録・閲覧	○	○	
	アラート	不正運用・不正操作各種管理者アラート	○	—	
		不正運用・不正操作各種ユーザーアラート	○	—	
	多言語対応	取得インベントリ情報の多言語表記（日・中 ※・英）	○	○	
		サーバ、管理コンソール、管理対象クライアントの多言語OS対応（日・中 ※・英）	○	○	

※ 簡体中国語

○…標準機能　—…非対応　★…オプション製品導入または個別サービス契約の場合利用可

			機能	勤怠データと操作ログ	勤怠データのみ	操作ログオプションのみ	ISM LogAnalytics ※4
就業時間管理 ※1	勤怠管理ダッシュボード			○	○	—	○
	個人別勤怠状況一覧			○	○	— ※2	○
	個人別勤怠グラフ	勤怠データ	業務時間	○	○	—	○
			残業時間	○	○	—	○
			無許可残業	○	○	—	○
		操作ログ	業務時間	○	○	○	○
			残業時間	○	○	○	○
			無許可残業	○	○	—	○
			退勤中のPC利用	○	—	—	○
	残業超過事前メッセージ			○	○	—	—
	残業超過時アクション			○	○	—	—
	残業抑制用アクション			○	○	○	—
	インターバルアクション			○	○	—	—
	勤怠システム連携 ※3			—	—	—	○

※1 Windowsのみ対応しています。
※2 個人別勤怠状況一覧は表示されますが、残業時間や診断総評の値は表示されません。
※3 連携サービスについては、当社担当営業へご確認ください。
※4 個別サービス「ISM LogAnalytics」はP.13 をご確認ください。

○…標準機能　—…非対応　★…オプション製品導入の場合利用可

		機能	ISM CloudOne Android	ISM CloudOne iOS	備考
スマートデバイス管理	運用・制御	各種脆弱性診断レポート	○	○	
		アプリケーション配布（アプリケーションポータル対応）	○	○	
		VPP（Volume Purchase Program）管理	—	○	
		アプリケーション起動制御	○	○	iOSでのアプリケーション起動制御はApple StoreとiTunesのみ
		Root化・Jailbreak検知	○	○	
		Bluetooth制御	○	—	
		SDカードアクセス制御	○	—	
		Wi-Fi接続先制御	○	—	
		違反時ポリシー適用	○	○	
		フィルタリングデータベースによる書き込み規制	★	★	専用ブラウザのみ対応
		フィルタリングデータベースによる接続規制	★	★	専用ブラウザのみ対応
	紛失対策	パスワード変更	○	—	
		位置情報取得	○	○	
		リモートロック・ワイプ	○	○	Android7～10はリモートワイプのみ対応