ism CloudOne
Vol.4

QualitySoft

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 TEL : 0739-45-1001　FAX : 0739-45-1008
東京本部	〒102-0083 東京都千代田区麹町3-3-4 KDX麹町ビル6F TEL : 03-5275-6123　FAX : 03-5275-6130
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 TEL : 06-6125-2161　FAX : 06-6125-2170
名古屋オフィス	〒460-0002 愛知県名古屋市中区丸の内 1-16-8 C-8ビル9F TEL : 052-684-7158　FAX : 052-684-7157
松本研究開発センター	〒390-0815 長野県松本市深志 2-8-6 OTKビル2F TEL : 0263-87-5413　FAX : 0263-87-5418

※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、2019年1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

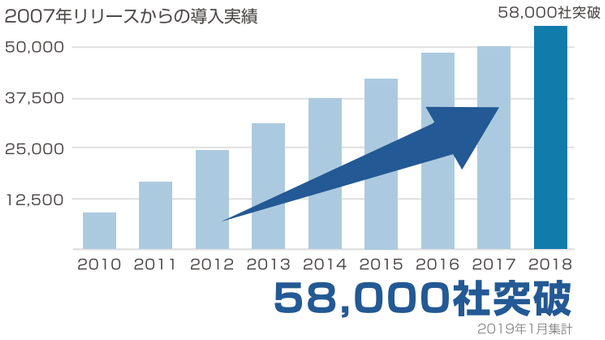
Canon
キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南2-16-6 CANON S TOWER
canon.jp/it-sec

201901-K

全ての企業に「トランスペアレントな安全」を

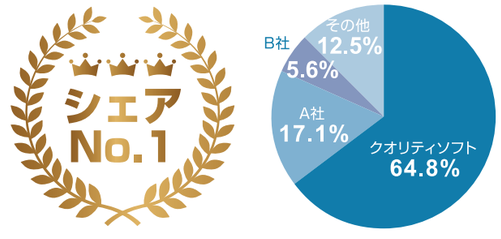
トランスペアレント（transparent）とは、
「透明な、透き通った」といった意味を持つ英単語です。
IT技術に置き換えると、内部での処理などがユーザーからは見えず
「意識する必要がない」といった意味を指します。
ISM CloudOneは企業の持つ情報が「意識することなく」
「安全」に守られる状態を実現するためのプラットフォームです。

**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。**



58,000社突破
2019年1月集計

クラウド型資産管理サービス市場
3年連続シェアNo.1達成！



株式会社ミック経済研究所
「情報セキュリティマネジメント型・クラウドサービス市場と展望2018年度版」

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。

サイバー攻撃による ウイルス感染を防ぎたい

自動脆弱性診断 —— P.7
ふるまい検知 —— P.9
URLフィルタリング —— P.10

顧客情報を不正に 持ち出していないか心配

操作ログ取得 —— P.11
外部デバイス制御 —— P.13
禁止ソフトウェア起動制御 —— P.15

社内のPC管理を行いたい

ハードウェア·ソフトウェア管理 —— P.17
Windows10管理運用支援 —— P.18
ファイル·ソフトウェア配布 —— P.19
ソフトウェアライセンス管理 —— P.21
グローバル対応 —— P.22

持ち出し端末の盗難·紛失による 情報漏えいが心配

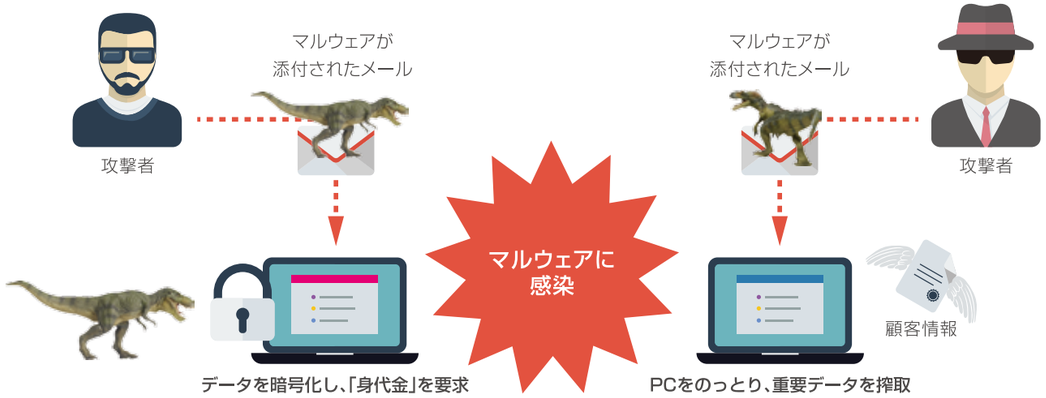
PC
ディスク暗号化 —— P.16
スマートフォン
スマートデバイス管理 —— P.23

目次

深刻化するサイバー攻撃による情報漏えい

サイバー攻撃の脅威

2大脅威：標的型攻撃とランサムウェア



未知のマルウェアや脆弱性を狙った攻撃は、ゲートウェイ製品やウイルス対策ソフトをすり抜けるケースがあります。

改正個人情報保護法や働き方改革におけるセキュリティ対策も必要

ストレージサービスの
不正利用

顧客情報の
不正持ち出し

禁止アプリの
インストール

不正アクセス等の外部脅威だけではなく、USBメモリやストレージサービスからの機密・顧客情報の不正持ち出しへの対策も必要です。

参考：2017年に発生した個人情報漏えい被害

インシデント件数	漏えい人数	想定損害賠償総額
386件	約520万人	約1,914億円

出典：JNSA「2017年　情報セキュリティインシデントに関する調査報告」

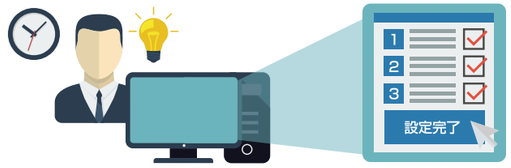
情報漏えいを防ぐためには、年々変化する流出経路に対応しなければなりません。

ISM CloudOneはトランスペアレントな安全で企業の情報を守ります

特徴1　シンプルマネジメント

ウィザードで簡単に初期設定

ウィザードに沿って設定を進めるだけで、
必要なポリシー設定が簡単に完了し、運用準備が整います。



自動診断による運用工数の削減

対処が必要な端末が自動でレポート化されるため、
管理工数を抑えたセキュリティ対策を実現します。

管理者はアラートやグラフを確認するだけでOK

特徴2　ロケーションフリー

社内ネットワークだけでなく、外出先や海外など利用環境を問わず管理することが可能です。
いつでも･どこでも管理対象全てにポリシー適用･脅威対策などを行うことができます。

特徴3　エンドポイント多層防御

外部からの脅威

自動脆弱性診断とふるまい検知で既知+未知の脅威を
多層防御します。

ゲートウェイをすり抜けてきた攻撃をエンドポイントで防御

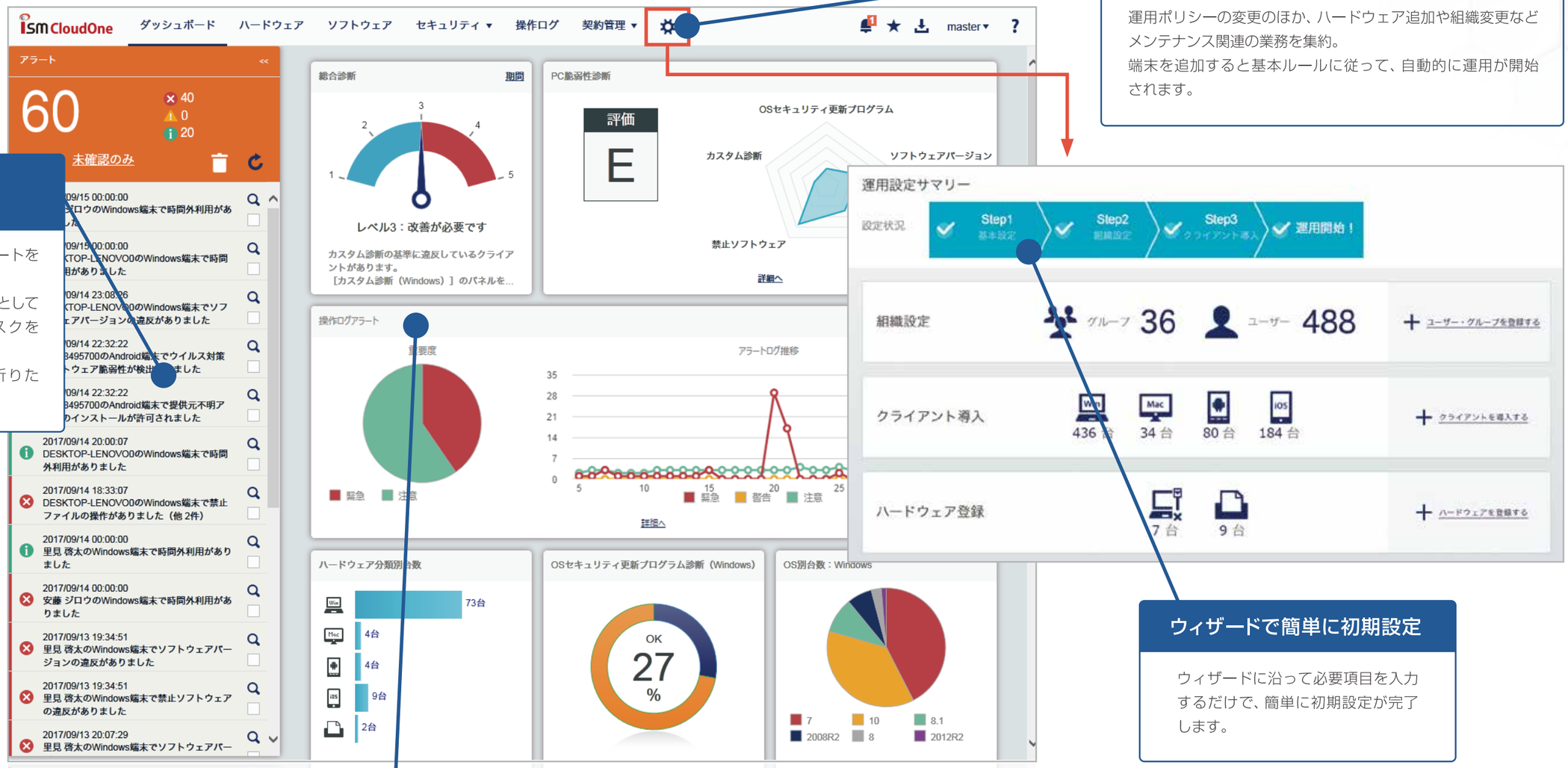
内部関係者による不正行為

操作ログ取得や外部デバイス利用制御で、企業が保有している
機密情報、顧客情報などの不正な外部流出を防ぎます。

従業員の不正行為や情報の持ち出しを防ぐ

直感的に操作できる管理画面で日々の運 用を効率化します

ISM CloudOneの管理画面は、どなたでも迷わず利用できることを目指して設計されています。
クライアント管理業務の運用導線を意識したインターフェイスとなっているため、
必要な操作を自然に行うことができます。



メンテナンス作業を集約

運用ポリシーの変更のほか、ハードウェア追加や組織変更などメンテナンス関連の業務を集約。
端末を追加すると基本ルールに従って、自動的に運用が開始されます。

問題点を見逃さない アラート確認リスト

閲覧時点までに発生したアラートを一覧表示します。
アラートを簡易チェックタスクとして扱うことができ、社内のリスクを見逃しません。
画面のサイズに合わせて、折りたたむこともできます。

ウィザードで簡単に初期設定

ウィザードに沿って必要項目を入力するだけで、簡単に初期設定が完了します。

必要な情報・問題点がひと目でわかるダッシュボード

ISM CloudOneのダッシュボードは、クライアントPC一覧から端末を選んで情報を見るのではなく、レポートを起点に、「今見るべき情報」にすぐアクセスできる設計にこだわりました。
ダッシュボードは運用に合わせてレポートパネルをカスタマイズできます。
また、レポートから対策が必要な端末一覧を表示し、そのまま是正操作を実行することができます。

お気に入り機能で管理効率向上！

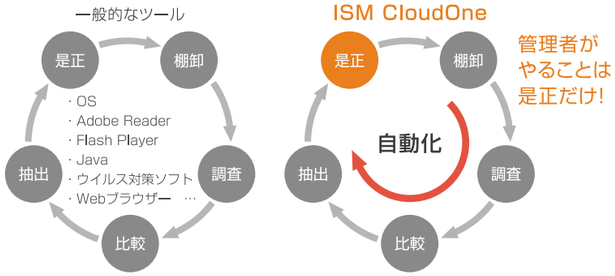
運用上よく使うページをお気に入り登録できます。
頻繁に変更・追加が必要な設定を登録することで運用を効率化できます。

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。

『詳細へ』をクリック

Windows更新
プログラムの適用状況

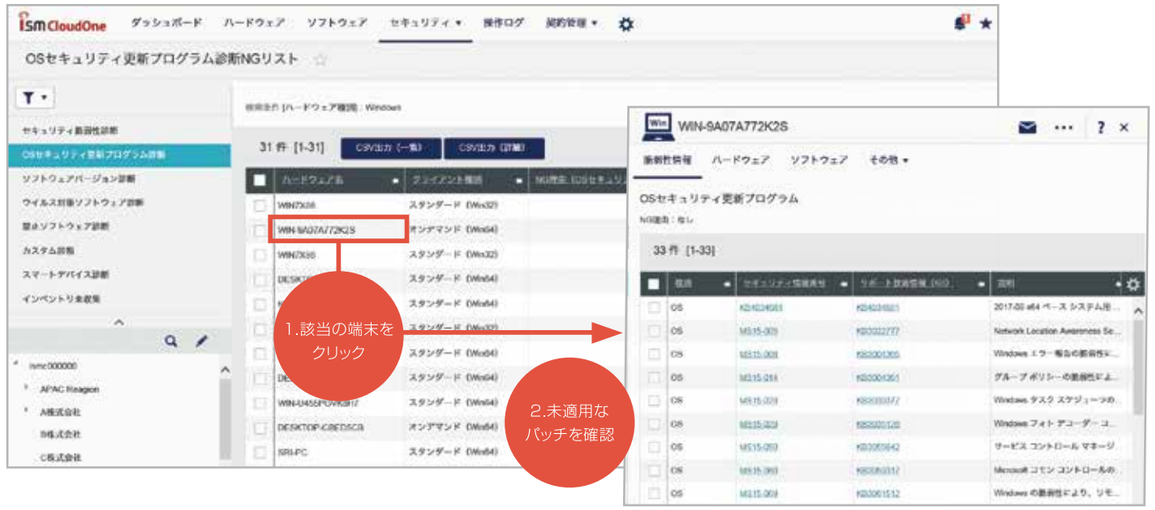
ソフトウェアの
アップデート状況

ウイルス対策ソフトの
導入・アップデート状況

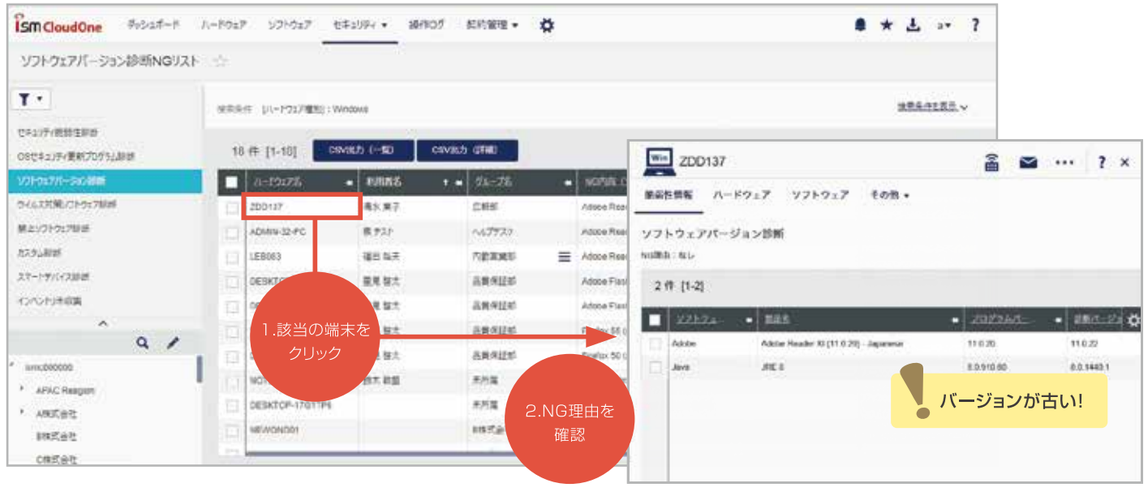
社内利用禁止ソフトウェアの
インストール状況

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(P.19)をご参照ください。

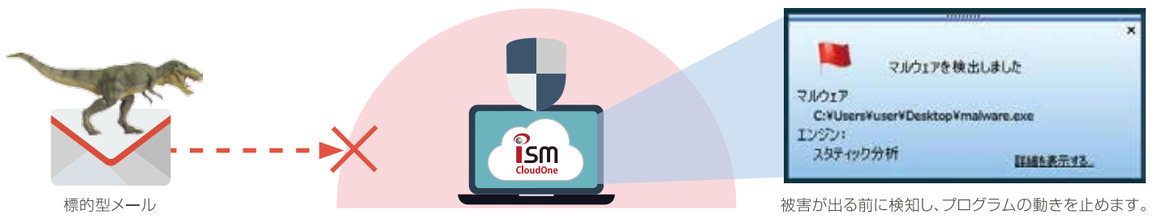
管理者側でソフトウェア自動更新を一括設定!

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。

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



標的型メール

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）

発生・報道時期	当時の未知脅威及び標的型攻撃	検知&防御エンジン
2018年7月	Clipboard Hijacker マルウェア	Static分析エンジン
2018年5月	Adobe Acrobatの脆弱性(CVE-2018-4990)	ZDP（脆弱性攻撃検出）
2017年5月	仮想通貨採掘マルウェア「Adylkuzz」	Static分析エンジン
2017年5月	ランサムウェア「WannaCry/WannaCrypt」	Static分析エンジン
2017年1月	IoTマルウェア「Mirai」	Static分析エンジン
2016年5月	不正送金マルウェア「Gozi/Ursnif」	HIPSエンジン
2016年3月	ランサムウェア「PETYA」	Static分析エンジン
2016年2月	ランサムウェア「Locky」	HIPSエンジン
2015年12月	不正送金マルウェア「URLZone」	Sandboxエンジン
2015年6月	日本年金機構を狙ったマルウェア「Emdivi」	（非公開）

（2018年10月末時点）

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

社内外問わず端末に同じポリシーが適用できます。

国内シェアNo.1のURLデータベース※

32億1672万コンテンツ

（2018年10月15日現在）

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。

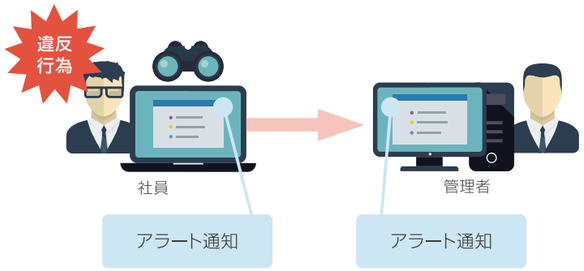
URLデータベースカテゴリ			
不法	職探し	広告	ゲーム
コミュニケーション	宗教	金融	ライフスタイル
旅行	セキュリティ・プロキシ	成人嗜好	ユーザー設定
主張	グロテスク	未承認広告	ショッピング
ダウンロード	政治活動・政党	ギャンブル	スポーツ
趣味	出会い	オカルト	
アダルト	話題	ニュース	

※出典：IDC Japan, 2017年7月「国内情報セキュリティ製品市場シェア、2016年：外部脅威対策および内部脅威対策」(Report# JPJ41780817)

操作ログ取得

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

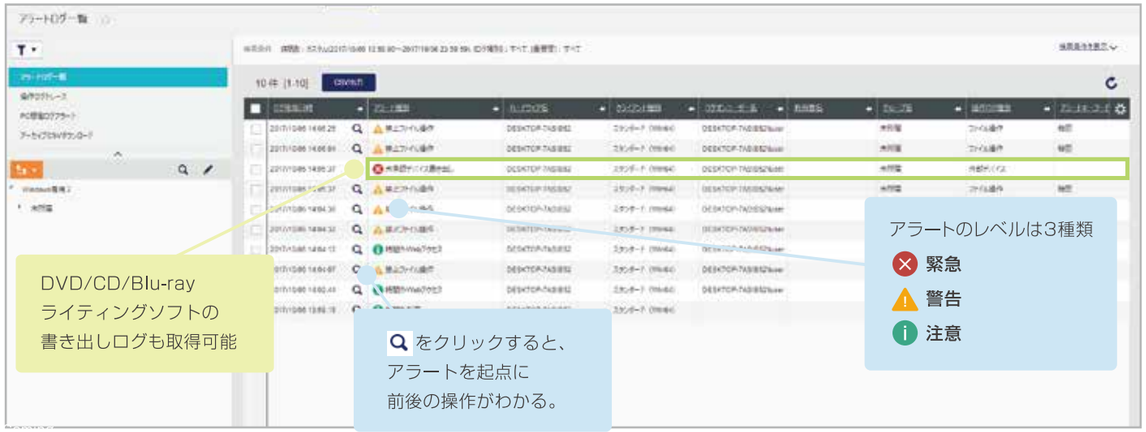
システム　外部デバイス　ドキュメントアクセス　ファイル操作　Webアクセス　クラウドストレージ

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。

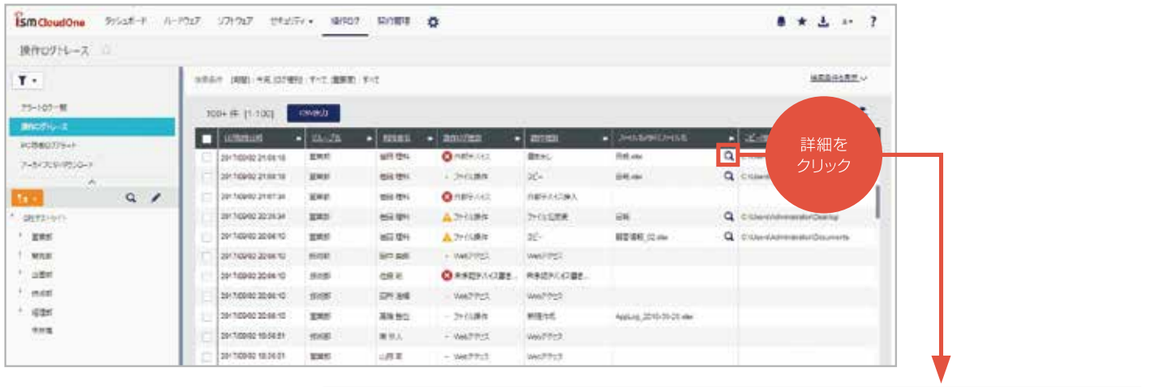


柔軟な検索機能で必要なログを追跡

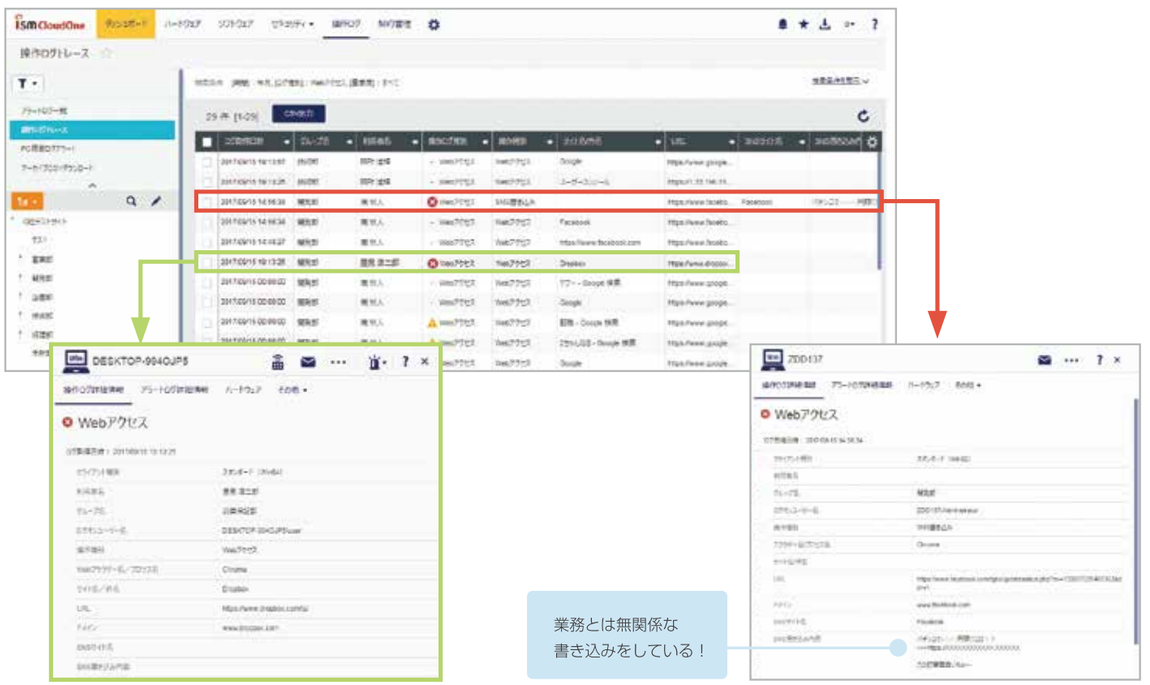
管理者が全てのログを確認するのは膨大な工数がかかり、現実的ではありません。

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。

操作ログトレース＞外部デバイス



操作ログトレース＞Webアクセス

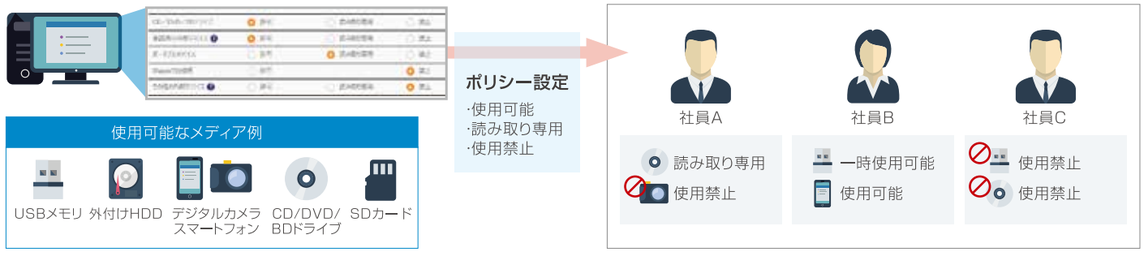


外部デバイス制御

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。



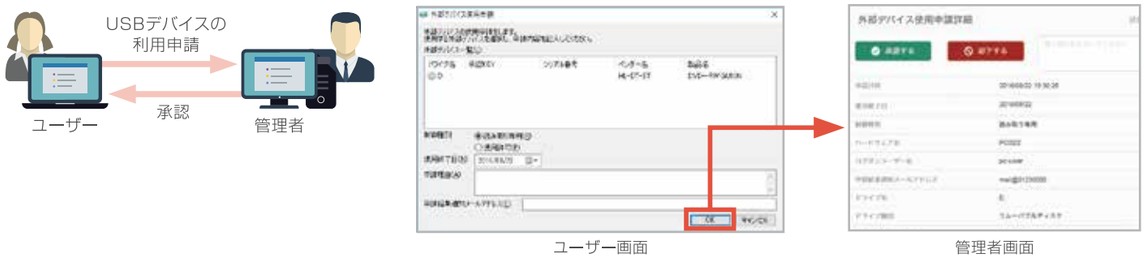
デバイス毎の設定で柔軟な運用が可能

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にのみ接続を許可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。

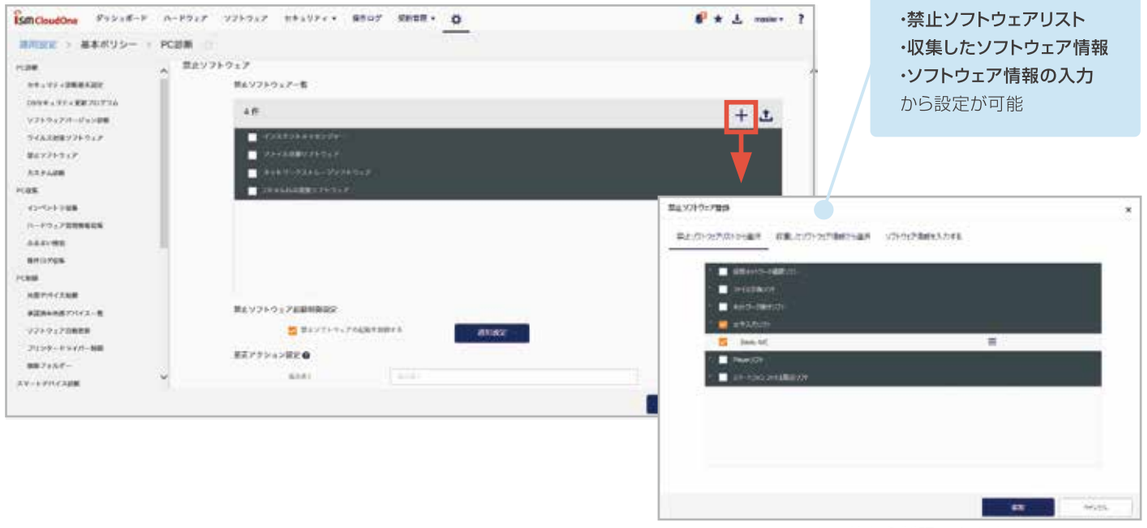
※SSIDの制限はTCP/UDPプロトコルの通信が対象
※Bluetooth通信制御はMicrosoft製のBluetoothドライバのみ対象
※Windowのみ対象

SSID登録ではワイルドカードが使用可能

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5,500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。

※2018年10月現在

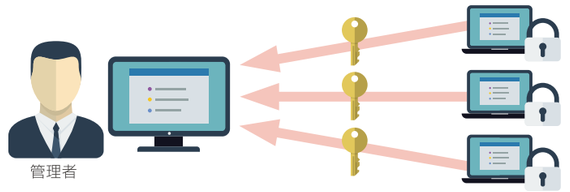
ディスク暗号化

オプション

システム領域も含めハードディスク全体をまるごと暗号化
持ち出しPCの盗難や紛失による情報漏えいを防ぎます

ハードディスク暗号化で端末内のファイルを守る！

復号化のためのリカバリファイルはISM CloudOneが管理！



暗号化状態をひと目で把握！

ハードウェア名	クライアント種別	OS	利用者名	グループ名	ディスク暗号化状態	リカバリファイ
DESKTOP-GM5MHPI	スタンダード（Win64）	Microsoft Windows 8.1 Enterprise	斎藤 真司	開発部	暗号化完了	あり
YAMASAKIS2	スタンダード（Win64）	Microsoft Windows 7 Professional	山崎 誠	営業部	未インストール	-
INO-WIN8	スタンダード（Win32）	Microsoft Windows 8 Enterprise	田所 活輝	開発部	暗号化完了	あり
NEWQND01	スタンダード（Win32）	Microsoft Windows 7 Professional	田中 由郎	営業部	未インストール	-
PC	スタンダード（Win32）	Microsoft Windows 7 Professional	安内 智史	営業部	暗号化完了	あり
WIN-PAVADR5HG2L	スタンダード（Win32）	Microsoft Windows 7 Professional	田辺 いづみ	営業部	暗号化完了	あり
ISMC-TEST7	スタンダード（Win32）	Microsoft Windows 7 Professional	山田 司	営業部	暗号化完了	あり

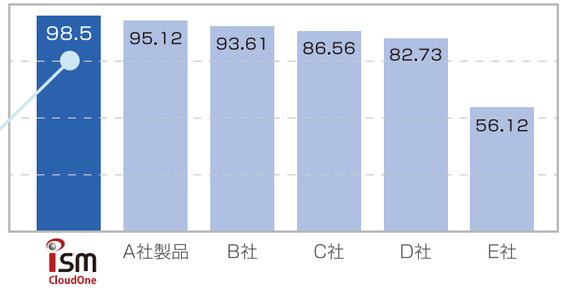
管理端末の暗号化状態を一覧で把握することができ、暗号化されていない端末を即座に特定します。

暗号化されていない！

高いパフォーマンス維持率

ISM CloudOneのハードディスク暗号化は、ファイル操作時にリアルタイムで暗号化・複合化を実行しますが、利用者がパフォーマンスの低下を体感することはほとんどありません。

パフォーマンス
維持率98.5%



Windowsのログオンと連携可能！

ディスク暗号化の認証とWindowsのログオンを連携することで、パスワード入力の回数を増やすことなくOSの起動が可能です。

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。

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
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。

Windows10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

Windows10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。

高速スタートアップ制御

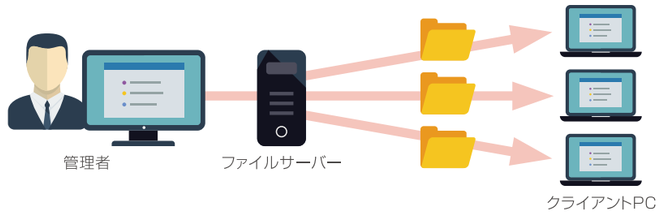
高速スタートアップの設定ON/OFFができます。
アプリケーションのインストール後に必要な再起動が行われず、長期間インストールが完了しないといった、管理者による管理が行き届かないケースを解決することが可能になります。

※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。

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

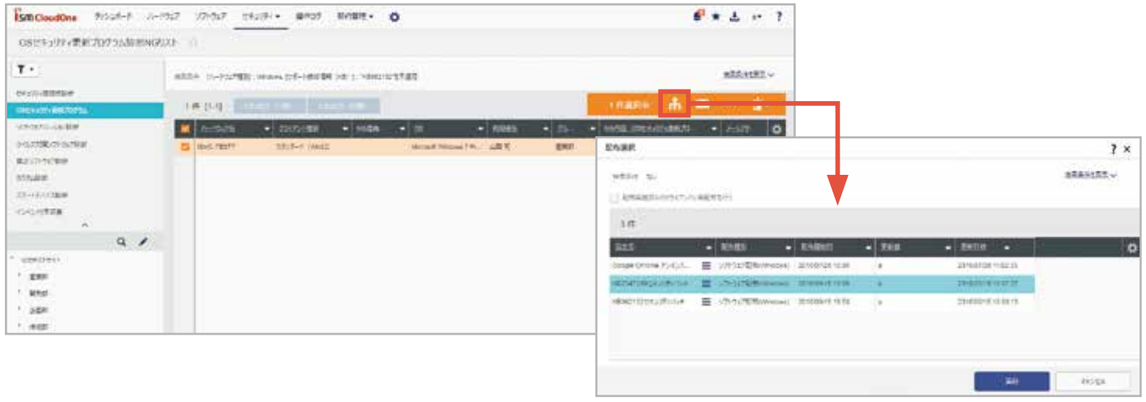
社内ネットワーク経由でソフトウェア、ファイル・フォルダ、レジストリなどの配布・実行が可能です。
レジストリ値については、追加・編集、エントリーの削除、キーの削除を行うことができます。



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

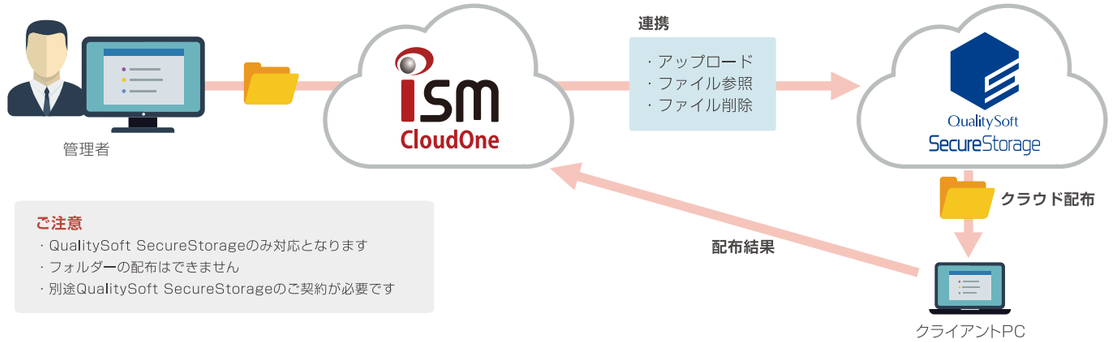
STEP2 対象者を選択し実行



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から、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

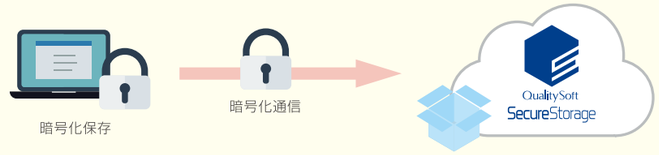
QualitySoft SecureStorageとは？

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	300GB	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

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

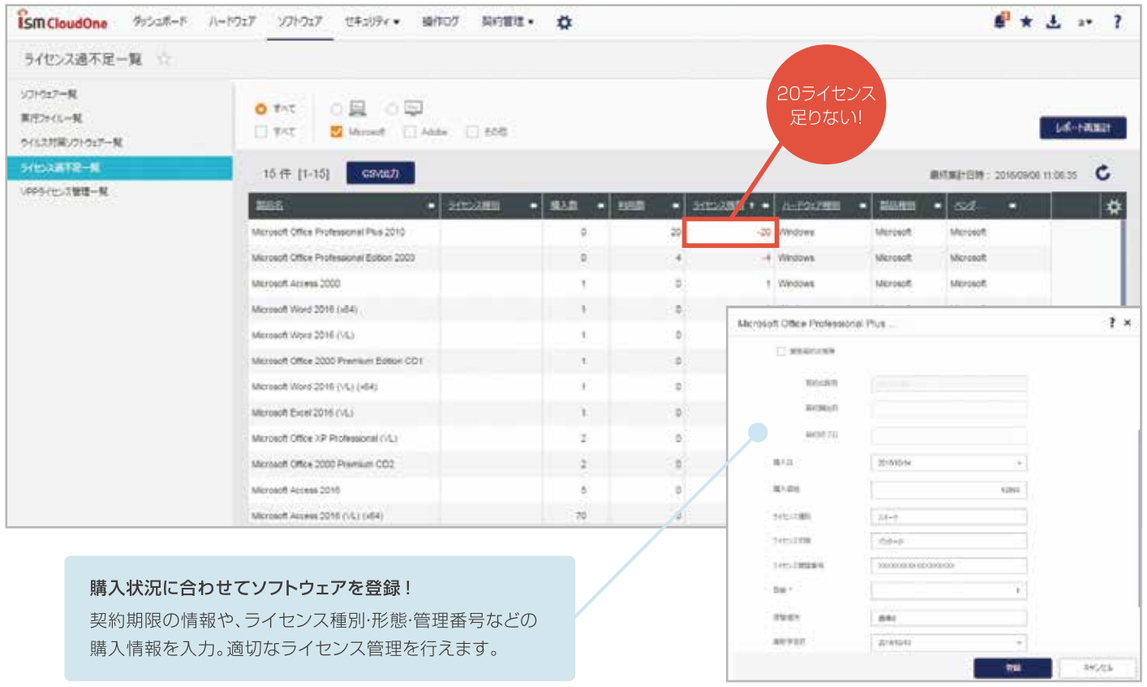
Microsoft Office製品やAdobe製品などを管理できる、管理台帳機能を搭載しています。
ライセンス種別や形態、インストール状況などの詳細を表示します。
保有ライセンス数と突き合わせることで、
ライセンス数の過不足状況を可視化し、
適切なライセンス管理の運用を支援します。

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。

今の管理で大丈夫?ソフトウェアライセンス管理 運用支援サポート

クオリティソフトでは、適切なソフトウェアライセンス管理を行えるよう、運用支援サポートを行っております。
現状のリスクを可視化する診断サービスを始め、SAMに関する教育やライセンス監査時の対応支援など、SAMコンサルタントが企業のライセンス管理を徹底サポートいたします。

※詳細は弊社営業までお問い合わせください。

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

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！

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
DESKTOP-PG95QHK	スタンダード（Win64）		営業部	Microsoft Windows 10 Education
83b9defa5cf600e1	iOS（クライアントプログラム）		グローバル	iOS 7.1.2
HD-SMP-10P-X64	スタンダード（Win64）		未所属	Microsoft Windows 10 Pro
DESKTOP-RK0BDGM	スタンダード（Win64）		未所属	Microsoft Windows 10 Enterprise 201
WIN81V	スタンダード（Win32）		APAC Reagion	Microsoft Windows 8.1 Pro
DESKTOP-GAVK65O	スタンダード（Win64）		東京	Microsoft Windows 10 Enterprise
IBB099	スタンダード（Win32）		未所属	Microsoft Windows 7 Enterprise
08000000000	iOS		未所属	iOS 10.2.1
WIN-LF48RK8VB0N	スタンダード（Win64）		本社	Microsoft Windows 7 Professional
ladmin の Mac mini (3)	スタンダード（Mac）		営業部	Mac OS X 10.8.5
VMHTWIN740-PC	スタンダード（Win32）		営業部	Microsoft Windows 7 Professional

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/
Bluetooth制御

Wi-Fi
ネットワーク設定

※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。

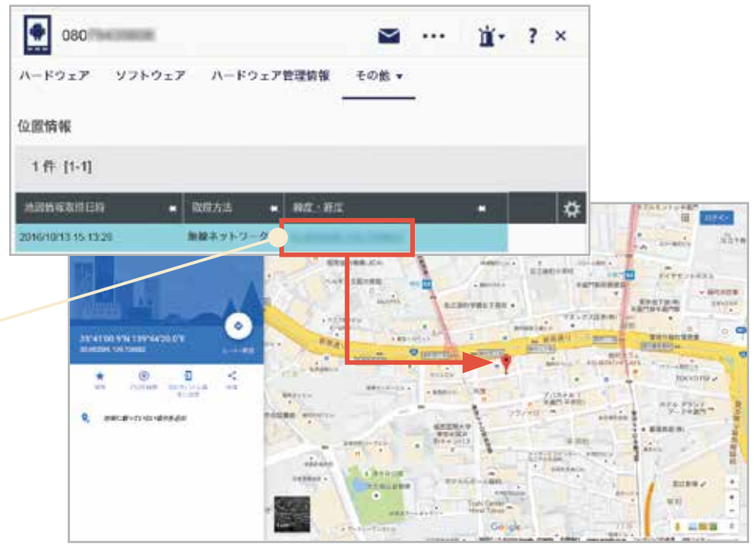
操作を実行したい端末を
選択して…

実行する操作を
選択するだけ！

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。



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。

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。

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。

インターネット経由でリモートコントロール（オプション）

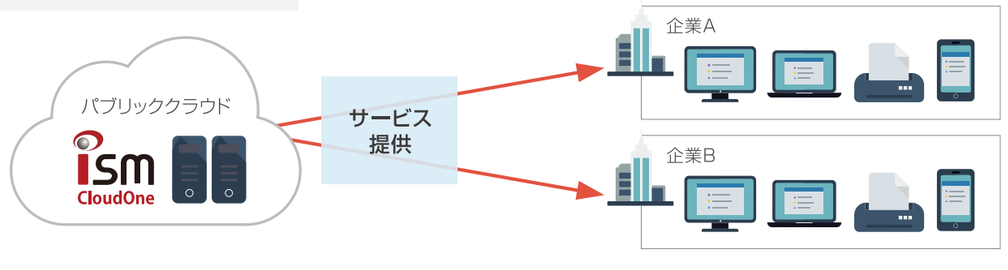
社内ネットワーク内の端末はもちろん、インターネット経由でのリモート操作も可能です。
海外を含む遠隔拠点のトラブル対応にも役立ちます。
またクライアント・管理者双方向のファイル転送も可能なため、離れている拠点のヘルプデスク対応などにも役立ちます。

会社規模や運用ニーズに合わせてさまざまな利用形態をご用意しています

ISM CloudOne（クラウド版）

クラウド提供のため、日々の運用やサーバーの管理・設置にかかる工数を大幅削減！
簡単・低コスト・短期間にセキュリティ対策やIT資産管理を実現したい場合に適しています。

オススメの環境
- ☑ すぐに運用を始めたい
- ☑ 専任のシステム管理担当者が不在
- ☑ サーバーを社内に持ちたくない
- ☑ サーバー設置・管理工数を削減したい



ISM CloudOne（パッケージ版）

大規模環境やパブリックなクラウドに不安があり、クローズド環境で利用したい場合に適しています。
管理コンソールをグループ毎に切り分けて提供することができるため、日々の管理と運用は各グループ担当者、サーバーや全体的な統制は親会社で行うなど、柔軟な対応ができます。

プライベートクラウドで利用する場合

オススメの環境
- ☑ 大規模環境で利用
- ☑ 複数拠点を一元管理したい

社内設置のサーバーを利用する場合

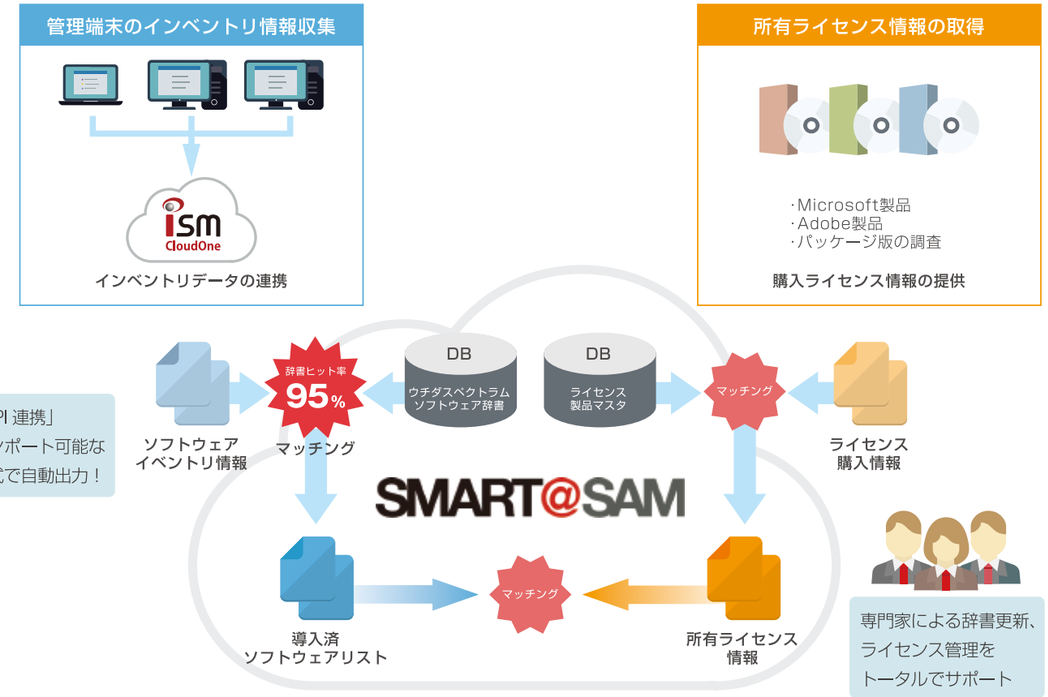
オススメの環境
- ☑ クローズド環境で利用したい
- ☑ 月々のコストを抑えたい

アライアンス製品

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。様々な製品とAPI連携を行うことで、より強固なセキュリティとパフォーマンスの高い管理を行う事ができるようになります。

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製品連携を推進しております

セキュリティ対策は１つのツールを導入すれば対策が完了できるといったような簡単なものではありません。
サイバー攻撃や内部不正など、懸念要素に合わせて複数の対策が必要です。
ISM CloudOneでは、企業のセキュリティ環境を守るべく、様々なアライアンス製品との連携を推進しております。
他社製品とAPI連携を行うことにより、より強固なセキュリティ対策をクラウド上で実現して参ります。

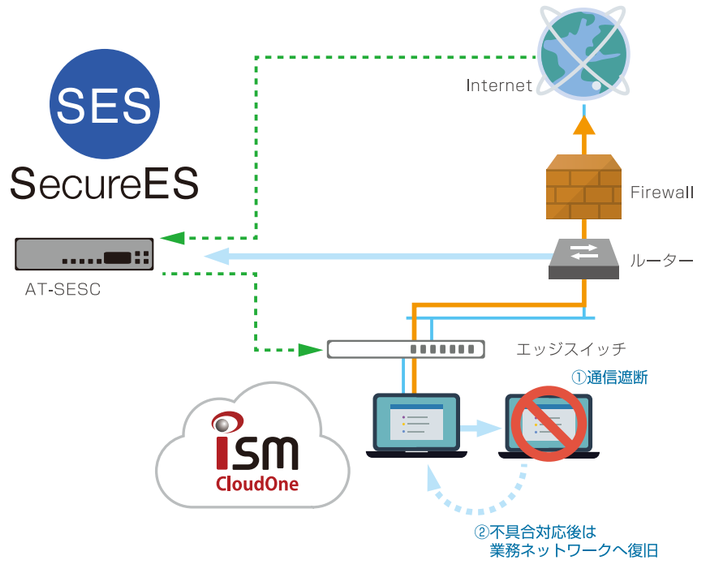
SDN
アライドテレシス社：Secure Enterprise SDN（SES）

脆弱性のある端末を検知し、問題がある端末は検疫ネットワークに隔離することでセキュリティを統制し、ネットワークの運用を効率化します。

1.ホワイトリストの自動登録
ISM CloudOne 管理下にない端末からのネットワーク接続を防止します。また、MACアドレスや部署名情報の自動登録が可能。管理端末のアクセス制御設定を自動化します。

2.セキュリティ統制
自動脆弱性診断で NG端末を判定、問題がある端末は自動で検疫ネットワークへ隔離し業務ネットワークのセキュリティを守ります。また、不具合対応後は自動的に業務ネットワークへ復旧させることが可能です。

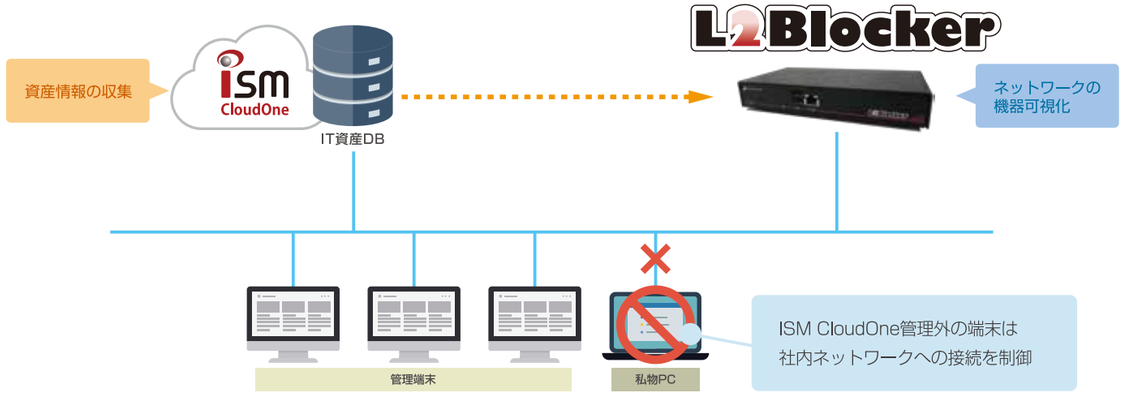
3.ふるまい検知
ランサムウェア / マルウェア感染端末を検知、被疑端末の通信をエッジスイッチにて遮断し、被害の拡散を防止します。



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

※2019年1月現在の情報です。最新情報は弊社営業までお問い合わせください。

○…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		制限事項
			Win	Mac	
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 製品 /WEB ブラウザ）	○	—	
		禁止ソフトウェア起動制御	○	—	
	操作ログ	印刷（プリンタ名 / ドキュメント名）	★	—	
		ファイル操作（各種ファイル作成 / 削除 / 名前の変更 / 移動 / コピー / 保存、ライティングソフトウェアによる書き出し）	★	—	
		外部デバイスの挿入・取出・書き込み	★	—	
		スナップショット（アラート発生時）	★	—	
		Web アクセス（HTTP/HTTPS/SNS 書き込み / クラウドストレージへのアップロード）	★	—	InternetExplorer/Chrome/FireFox/Edge対応 Twitter/Facebook/mixi/Google+/Ameba対応
		Web メール送信	★	—	Gmail/Yahoo!メール/Outlook.com対応
		PC 稼働（電源 on/off、ログオン / ログオフ、スリープ / 休止 on と復帰タイミング）	★	—	
		ファイルアクセス	★	—	
		クラウドストレージ	★	—	Googleドライブ/One Drive/Dropbox/QualitySoft SecureStorage
	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	★	★	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
		FD	★	★	
		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
		ファイル／フォルダー削除	○	—	Windows8以降対応機能
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	○	○	
		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）	○	—	
		約款情報辞書・自動引き当て	★	—	パッケージ版のみ対応

機能			ISM CloudOne		制限事項
			Win	Mac	
IT 資産管理	ハードウェア管理	棚卸一覧	○	○	
		ハードウェア契約	○	○	
	配布	ファイル／フォルダ配布	○	—	
		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）	○	—	
		プリンタードライバー (設定変更)	○	—	キヤノン製プリンタードライバー対応
	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
	メッセージ通知	メッセージ通知	○	—	
システム	顧客関連管理	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）	○	○	
		サーバー、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）	○	○	

機能			ISM CloudOne		制限事項
			Android	iOS	
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	○	○	

動作環境

※2019年1月現在の情報です。最新情報は弊社Webサイトをご確認ください。

ISM CloudOne Ver.6.5i 動作環境

●…対応　空欄…非対応

OS		エディション	サービスパック／バージョン	サーバー			クライアント	RCコンソール	URL Filteringエージェント ※7 ※8	ディスク暗号エージェント ※7 ※8 ※10 ※11	ふるまい検知エージェント ※7 ※8 ※11
				システムサーバー	ログサーバー	RCサーバー					
Linux(x86)	Red Hat Enterprise Linux 6			●							
	CentOS 6			●							
Linux(x64)	Red Hat Enterprise Linux 6～7			●	●	●					
	CentOS 6～7			●	●	●					
Android (ARM系CPU / IntelCPU)	3.0 ～ 6.0 ※1						●				
	4.0 ～ 6.0								●		
iOS	5.0 ～ 12 ※1 ※2 ※3						●				
	10 ～ 12								●		
Mac OS X (macOS) (IntelCPU)	10.6 ～ 10.13						●				
Windows(x86)	XP	Home / Professional	SP3				●※16	●			
	Vista	Home Basic / Home Premium / Business / Enterprise / Ultimate	未適用 / SP1 / SP2				●※16	●	●※9	●※12	
	7	Home Premium / Professional / Enterprise / Ultimate	未適用 / SP1				●	●	●※9	●※12	●
	8	エディションなし / Pro / Enterprise	未適用				●※16	●	●	●※12	
	8.1 ※4	エディションなし / Pro / Enterprise	未適用				●	●	●	●※12	●
	10 ※17	Home / Pro / Enterprise / Education	1507～1809				●	●	●	●※12※13	●※18
	Server 2003	Standard / Enterprise	SP1 / SP2				●※6※16	●			
	Server 2003 R2	Standard / Enterprise	SP1 / SP2				●※6※16	●			
	Server 2008 ※5	Standard / Enterprise	SP1 / SP2				●※6	●			●
Windows(x64)	XP	Professional	SP2				●※16	●			
	Vista	Home Basic / Home Premium / Business / Enterprise / Ultimate	未適用 / SP1 / SP2				●※16	●		●※12	
	7	Home Premium / Professional / Enterprise / Ultimate	未適用 / SP1				●	●	●※9	●※12	●
	8	エディションなし / Pro / Enterprise	未適用				●※16	●	●	●※12	
	8.1 ※4	エディションなし / Pro / Enterprise	未適用				●	●	●	●※12	●
	10 ※17	Home / Pro / Enterprise / Education	1507～1809				●	●	●	●※12※13	●※18
	Server 2003	Standard / Enterprise	SP1 / SP2				●※6※16	●			
	Server 2003 R2	Standard / Enterprise	SP1 / SP2				●※6※16	●			
	Server 2008 ※5	Standard / Enterprise	SP1 / SP2				●※6	●			●
	Server 2008 R2 ※5	Standard / Enterprise	未適用 / SP1				●※6	●			●
	Server 2012 ※5	Essentials / Standard / Datacenter	未適用				●※6	●			●
	Server 2012 R2 ※5	Essentials / Standard / Datacenter	未適用				●※6	●			●
	Server 2016 ※5	Essentials / Standard / Datacenter	未適用				●※6	●			●
	Server 2019 ※5	Essentials / Standard / Datacenter	未適用				●※6	●			

※1 スマートデバイス検証済み機種一覧については、以下URLをご確認ください。https://ismcloudone.com/requirements/　※2 iOS 7に対応しているクライアントプログラムは、Ver.4.5.4以降となります。
※3 iOS 8、iOS9に対応しているクライアントプログラムは、Ver.4.9.1以降となります。　※4 Windows 8.1 update1対応済み。　※5 Server Coreインストールで利用している場合は、動作保証対象外です。
※6 外部デバイス制御機能およびライティングソフトによる書き出しログは、Server系OSには対応していません。　※7 VDI上での動作には対応していません。　※8 日本語OSにのみ対応しています。
※9 OSのサービスパックは最新版にのみ対応しています。　※10 ISP版にのみ対応しています。　※11 詳細なシステム要件については、別途弊社営業までお問い合わせください。
※12 各OSのエディション「Home Basic」「Home Premium」「エディションなし」には対応していません。　※13 Windows 10 April 2018 Update (Ver.1803)以降には対応していません。
※14 Essentialsには対応していません。　※15 CMCサーバーには対応していません。　※16 Ver.6.0.2以前よりインストール済みのWindowsクライアントは引き続きご利用できますが、Ver.6.1以降の新機能は動作しません。
※17 LTSB(2015/2016) 対応済み。　※18 Windows 10 October 2018 Update (Ver.1809)以降には対応していません。
・日本語・簡体中国語・英語OSに対応しています。　・ISM CloudOne パッケージモデルの場合は、お客様にてサーバーを構築する必要があります。　・サービス事業者によっては、サポート範囲が異なる場合があります。
・各OSについては、最新のサービスパックを適用することを推奨します。万が一、旧サービスパックにて動作上の問題が発生した場合は、最新サービスパックの適用をお願いします。

必要CPU・メモリ・ディスク容量

システムサーバー・クライアント

		CPU	メモリ	ディスク
システムサーバー	管理対象PC：クライアント数1,000	Core2Duo E4300以上	2GB以上	128GB以上
	管理対象PC：クライアント数3,000	Core2Duo E4300以上	4GB以上	256GB以上
クライアント(Android)		ARM系CPU Intelプロセッサ	256MB以上(512MB以上を推奨)	-
クライアント(iPhone/iPad)		-	-	-
クライアント(Mac)		Intelプロセッサ	512MB以上	100MB以上(500MB以上を推奨)
クライアント(Windows)		Pentium4 1GHz以上 ※1	1GB以上 ※2	120MB以上(650MB以上を推奨)

※1 Windows XP/Windows Server 2003/Windows Server 2003 R2の場合は、Pentium3 1GHz以上
※2 Windows XP/Windows Server 2003/Windows Server 2003 R2の場合は、128MB以上（256MB以上を推奨）

操作ログ

		CPU	メモリ	ディスク
ログサーバー (ログ保持期間：30日)	管理対象PC：クライアント数1,000	Core2Duo E6400以上	8GB以上	305GB以上
	管理対象PC：クライアント数3,000	Core2Duo E6400以上	12GB以上	428GB以上
クライアント (Windows) ※1		ISM CloudOneのクライアント(Windows)に同じ		

※1 ISM CloudOneのWindowsクライアントをインストールすることで、操作ログ収集機能が利用できます。

ディスク暗号

	CPU	メモリ	ディスク
エージェント (Windows)	Pentium4 1GHz以上	1GB以上	1GB以上

リモートコントロール

	CPU	メモリ	ディスク	ネットワーク帯域
RCサーバー ※1　管理対象PC：クライアント数3,000	Core2Duo E4300以上	1GB以上(2GB以上を推奨)	20GB以上	200Mbps 以上 ※5
RCコンソール・RCクライアント	Pentium4 1GHz以上 ※2	1GB以上 ※3	200MB以上(500MB以上を推奨)	2.2Mbps 以上 ※4 ※5

※1 3,000台収容、RCクライアントからの通信間隔30秒、同時リモコン上限100接続とした場合の動作要件です。
※2 Windows XP/Windows Server 2003/Windows Server 2003 R2 の場合は、Pentium3 1GHz以上
※3 Windows XP/Windows Server 2003/Windows Server 2003 R2 の場合は、128MB以上（256MB以上を推奨）
※4 RCコンソール、RCクライアントそれぞれの利用環境で2.2Mbps以上の帯域が確保されている必要があります。
※5 ファイル転送機能を利用する場合は、転送するファイルサイズに合わせた帯域が追加で必要です。利用できる帯域と実際の通信量によって、リモコン操作、ファイル転送に遅延が発生する可能性があります。

ふるまい検知

	CPU	メモリ	ディスク
EMCサーバー	Intel Pentium 4以上	2GB以上	100GB以上
CMCサーバー	Xeonシリーズ 4Core以上	8GB以上	100GB以上
クライアント	Intel Core2Duo以上	2GB以上	1GB以上

・推奨するシステム要件です。管理台数に合わせた詳細なシステム要件については、別途弊社営業までお問い合わせください。

サービスコンソール・ユーザーコンソール対応 Webブラウザバージョン

Webブラウザ	対応バージョン
Internet Explorer	10 ～ 11
Microsoft Edge	20 ～ 42
Google Chrome	53 ～ 70
Safari	9 ～ 11

・解像度はXGA（1024×768）以上、WXGA (1366×768)を推奨。
・Internet Explorerの互換モードには非対応です。

RC管理コンソール対応 Webブラウザバージョン

Webブラウザ	対応バージョン
Internet Explorer	10 ～ 11

・Internet Explorer10・11は、Internet Explorer9互換モードで、デスクトップ版のみ対応です。

ご案内

選べる無料トライアル

疑似体験サイト

ダッシュボードでの管理作業のシミュレーションを無料で1日体験できます。すでに登録されている端末情報を元にレポーティングされたグラフや、とるべき措置をお知らせするアラートなど、ISM CloudOne のダッシュボードの操作感をお試しいただけます。

有効期限：お申し込み後翌日 4 時まで

30日間無料トライアル

ご自身のクライアントPCにエージェントをインストールしていただき、実際の情報を元にセキュリティ状況を診断、レポート化します。実データを元にセキュリティ状況の把握や処置を行う事が可能です。

有効期限：お申込み後 30 日間

各種セミナー

eラーニング

ISM CloudOne の導入・運用に必要な基本操作を、トライアルサイトの操作を行いながら習得できます。

ハンズオン形式

ハンズオンを交えながら基本的な操作説明を学ぶセミナーです。導入直後で操作方法がわからない方にオススメです。

運用サービスのご支援

「ウイルス対策ソフトで見逃しているマルウェアはないのか？」「標的型攻撃のリスクはどれくらいあるのか？」「セキュリティ対策における運用工数を削減できないか？」など、忙しい管理者様に代わり、サイバー攻撃対策の導入前から導入後までをご支援する、さまざまなサービスをご用意しております。

MEMO