機能もサービスも、オーダーメイド感覚。

IT統合管理ソフトウェア

AssetView®

アセットビュー

HAMMOCK

HAMMOCK

製品の最新情報やお問い合わせはこちら

https://www.hammock.jp/assetview/

0120-922786　海外・携帯電話・PHSからは 03-5291-6121
平日 9:00～12:00、13:00～17:00（弊社休業日を除く）

※本カタログに使用している製品画像は開発中の内容も含まれており、実際のものとは異なる場合があります。
※サービス内容・製品の仕様は予告なしに変更する場合があります。最新情報は Web サイトをご覧ください。
※AssetView は（株）ハンモックの登録商標です。記載された社名および商品名は、一般に各社の商標または登録商標です。

PRINTED WITH SOY INK
このカタログは大豆油インキで印刷しています

開発・総販売元

株式会社 ハンモック

本　　社　〒169-0072　東京都新宿区大久保1-3-21 ルーシッドスクエア新宿イースト3F
TEL 03-5291-6121　FAX 03-5291-6122

名古屋営業所　〒460-0008　愛知県名古屋市中区栄2-9-26 ポーラ名古屋ビル A館11F
TEL 052-209-7877　FAX 052-209-7855

大阪営業所　〒550-0002　大阪府大阪市西区江戸堀1-3-3 肥後橋レックスビル5F
TEL 06-6446-2230　FAX 06-6446-2232

福岡営業所　〒812-0013　福岡県福岡市博多区博多駅東2-5-19 サンライフ第3ビル6F
TEL 092-433-2020　FAX 092-433-2021

E-mail nws_hp@hammock.co.jp　URL https://www.hammock.jp

お問い合わせ

プライバシーマーク 10823085

※このカタログは 2024 年 4 月現在のものです。

組織の情報守るなら

AssetView（アセットビュー）

AssetView は組織内のクライアント PC 情報を収集する機能に加え、
Windows Update の更新管理や各種制御・警告・マルウェア対策など

選ばれる理由

AssetViewの特長

低コストで
最大限の効果を発揮！

企業が抱える PC 管理の課題をまとめて解決。管理に必要なサーバーの統合、管理ツールやサポート窓口の一本化により、高効率な運用とコスト削減を実現いたします。

ニーズに合わせて
クラウドとオンプレミスが
選択可能！

導入コストがかからないクラウド、必要な機能を必要なライセンス分だけ購入できるオンプレミス、どちらも低コスト運用を実現いたします。

導入から運用まで
サポートが充実！

構築、導入、運用アウトソーシング、サポートまで、弊社のカスタマーサクセスが幅広くご支援いたします。

AssetView 導入実績

業種、業務、規模を問わず多くのお客様にご導入いただいております。

製造
Panasonic
Kawasaki

食品
Coca-Cola BOTTLERS JAPAN INC
寿心
旭松

サービス
NIPPON Rent-A-Car
NEXCO
ニトリ NITORI

金融
日本カストディ銀行 Custody Bank of Japan
きらぼし銀行
神奈川銀行

情報通信
ID Holdings
crops
日経HR NIKKEI HUMAN RESOURCES

小売
Keio

不動産
小田急不動産 odakyu
奥村組 OKUMURA CORPORATION

医療
富士薬品
美容皮膚科クリニック REGINA CLINIC レジーナクリニック

教育
獨協大学 DOKKYO UNIVERSITY
拓殖大学 Takushoku University

官公庁
山形県 山形市役所
香川県 善通寺市役所

ユーザー様の声

業種	組合・団体・協会
従業員規模	300-1000 人未満

個人情報取り扱い台帳を整備する際、これまでは各部署より手書きにクライアントへ保存しているデータを報告してもらっていたが、**AssetView の導入により劇的な作業負荷の軽減と効率化**が図られた。

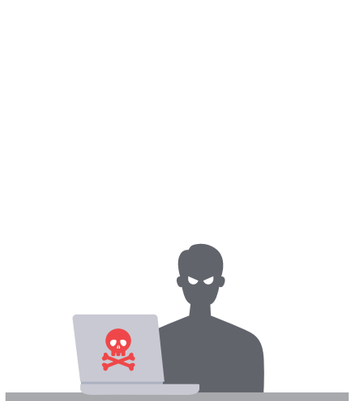
業種	不動産売買
従業員規模	300-1000 人未満

海外メーカーも含めていくつか比較したが、AssetView が一番親切で画面がわかりやすく感じた。価格面でも機能ごとに分かれていたので、**必要な機能だけを契約**することで安く抑えることができた。アップデートも頻繁に行われており、導入後のサポートも丁寧で安心して使用

PCの管理・セキュリティ対策を包括的に実現

AssetViewでは目的に応じた機能の段階導入ができるため、**必要最小限のコスト**　から**かんたんに機能拡張**ができ、統合管理・コスト削減を実現できます。

オンプレミス、クラウドサービスのどちらかをお選びいただけます！※



外部からのさまざまな脅威

- ウイルス・マルウェア混入メール
- ウイルス感染不正サイト
- ウイルス混入デバイス
- 不正持ち込みPC

入口対策

- **AssetView Vplus エンドポイントセキュリティ**：マルウェア対策
- **AssetView F Webフィルタリング**：不正サイトアクセス禁止
- **AssetView G デバイス制御**：未許可デバイス使用禁止
- **AssetView S 不正PC遮断**：不正PC遮断

組織内

クライアントPC

内部対策

ログ監査

- **AssetView M PC操作ログ管理**：PC操作ログ取得、実行制御
- **AssetView I 個人情報検索**：重要情報ファイルの利用監査
- **AssetView Mail 電子メール監視**：電子メールログ取得
- **AssetView REC 画面操作録画**：重要操作の録画保存

PC状態把握・適正化

- **AssetView A IT資産管理**：該当端末の把握、危険アプリ発見
- **AssetView D アプリケーション配布**：業務アプリ配信・設定変更
- **AssetView RC リモートコンソール**：遠隔での設定変更・ヘルプデスク

Windows アップデート管理・脆弱性対策

AssetView P PC更新管理

- 更新状態の可視化
- 低帯域でも更新展開
- 実行コントロール

■FU/QU対応
■Microsoft 365、Office2019/2021対応
■サードパーティー製パッチ対応

出口対策

- **AssetView K ファイル制御・暗号化**：ファイル暗号化
- **AssetView F Webフィルタリング**：SNS / Web メール / オンラインストレージ等禁止
- **AssetView G デバイス制御**：デバイス制御・申請
- **AssetView MDM スマートデバイス管理**：スマートデバイスデータの初期化

外部への持ち出し

- 流出データの削除
- Web経由の流出禁止
- USBメモリ保存時の自動暗号化 ※暗号化機能と連携
- 紛失時のデータ削除

※クラウドサービスではご提供していない機能もございます。詳しくは営業担当までお問い合わせください。

利用環境に合わせて自由にカスタマイズ！

パッケージソフトウェアの導入だけではクリアできない課題を包括的に解決します。

		オンプレ	クラウド
AssetView 共通 共通機能	・基本インベントリ取得 ・基本アンケート配信 ・メッセージ配信 ・コマンド送信(vPro /WOL) ・電源管理、スクリーンセーバー設定 ・自動レポート(20 帳票)	単機能でも導入可能	標準提供
macOS 対応 AssetView A IT資産管理	・ハードウェア情報取得・管理 ・インストールアプリ情報取得・管理 ・ソフトウェアライセンス管理 ・任意のアンケート配信 / デスクトップへの付箋 ・任意のファイル検索 ・ソフトウェア辞書(オプション) P.12	スタンダードパッケージ	
macOS 対応 AssetView D アプリケーション配布	・ファイル自動配布 ・プログラム自動実行 ・設定自動変更(INI ファイル / レジストリ編集) ・OS シャットダウン / 再起動自動実行 ・PC 操作自動実行(マクロメーション) P.16		
macOS 対応 AssetView M PC操作ログ管理	・PC の各種操作ログ収集 ・ファイル操作の追跡 ・プログラム起動 / ファイル操作 警告 / 禁止 ・稼働状況グラフ表示 ・シャドウイング / 簡易 Web フィルタリング P.20		
AssetView I 個人情報検索	・個人 / 機密 / 特定個人情報ファイル検索 ・検出ファイルの結果確認(内訳取得) ・検出ファイルの隔離 / 完全削除 ・個人 / 機密 / 特定個人情報ファイル操作時のリアルタイムアラート(M/I 連携) ・検出ファイルの自動暗号化(I/K 連携) P.24		セキュリティパッケージ
macOS 対応 AssetView G デバイス制御	・USB デバイス個別制御 ・光ディスク・SD/FD/MO 制御 ・デバイス利用申請 ・Wi-fi アクセスポイント制御 Bluetooth 機器 個別制御 P.26		
AssetView S 不正PC遮断	・不正 PC 検知 (ARP リクエストによる MAC アドレス確認) ・不正 PC 遮断(未許可 MAC アドレスの NW 接続遮断) ・ネットワーク機器の自動登録 ・IP アドレス範囲別の制御指定 P.28		
AssetView RC リモートコンソール	・クライアント PC のリモート操作(画面共有) ・ファイル転送 ・ペイントモード ・リモート接続許可要求 ・インターネットリモコン P.29		

		オンプレ	クラウド
AssetView P PC更新管理	・配信用プログラム自動ダウンロード ・FU/QU の計画配信、配信詳細把握 ・WindowsUpdate 制御(勝手アップデート無効化) ・Microsoft365/Office2019 アップデート ・3rd パーティ製アプリの脆弱性管理 P.30	単機能でも導入可能	
AssetView Vplus エンドポイントセキュリティ	・パターンファイルマッチング ・振る舞い検知 ・リアルタイムモニタリング ・パターンファイル取得先変更 P.34	●	●
AssetView F Webフィルタリング	・インターネットアクセスコントロール (アクセス可、アクセス不可、閲覧のみ可 / 書き込み NG) ・高精度データベース自動更新 ・プログラム利用規制 ・Web 書き込みサイズ指定制御 ・社内 NW 以外時のみフィルタリング実施設定 P.36	●	●
AssetView K ファイル制御・暗号化	・ファイル暗号化(AES 256bit) ・ファイルへのアクセス権設定 ・ファイルへの各種規制設定(回数 / 期限 / 印刷禁止等) ・ファイル追跡、削除 ・自動暗号化 P.38	●	●
AssetView Mail 電子メール監視	・送信メールログ取得 ・添付ファイルの保存 P.40	●	●
AssetView MDM スマートデバイス管理	・iOS/Android/Windows の管理 ・位置情報取得 ・リモートロック / リモートワイプ ・ハードウェア / インストールアプリ情報取得 ・プロファイルの適用 P.42	●	●
AssetView REC 画面操作録画	・画面操作録画 ・不正操作画面キャプチャ取得 ・スケジュール録画 / タイムシフト録画 P.44	●	
AssetView アーカイブ 高速ログ検索/長期保存	・高速ログ検索 ・長期保存 P.46	●	

※macOS 対応：一部機能制限があります。詳細は営業へお問い合わせください。 ※選べるオプション・・・●

ニーズに合わせて選べる利用環境

クラウド

AssetViewクラウド版の特長

オンプレミス版と遜色ない充実な機能構成

標準機能をベースにオプションで必要な機能を選択できます。

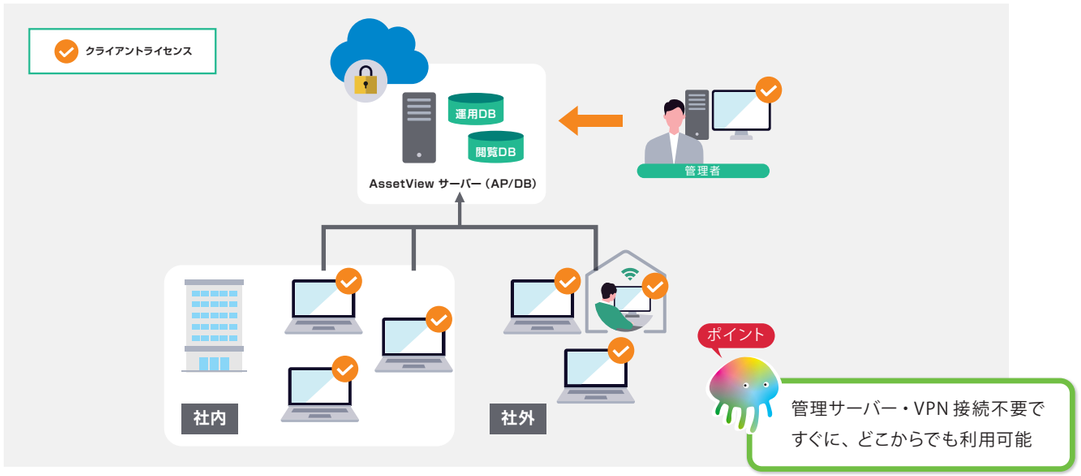
運用コストの負荷軽減

運用で必要なサーバー死活監視、WindowsUpdate 運用、製品バージョンアップ作業も弊社にて対応いたします。
日々の運用管理の負担を軽減いただけます。

ロケーションフリーですぐに利用可能

社内 LAN や VPN 接続しないテレワーク端末も統合して管理できます。

システム構成・運用イメージ



提供プラン

		機能		最低購入数
		A D RC S M I G	オプション機能 P Vplus F K Mail MDM	
クラウド	AssetView CLOUD	標準機能	ー ※標準機能に加えて単機能で追加購入可能	100 ライセンス～

オンプレミス

AssetViewオンプレミス版の特長

単機能からオーダーメイド感覚で導入可能

全 15 機能を1機能からご導入いただくことができます。

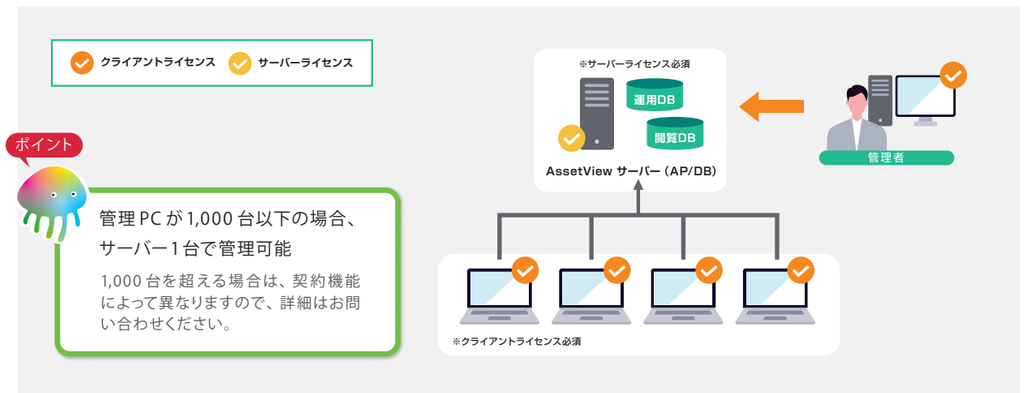
導入する機能を選べるからコスト削減

必要な機能やサービスを必要な数だけ導入することができるので、最小限のコストでご利用いただけます。

インターネットに接続できない環境でも利用可能

インターネットに接続できないネットワークが分離した環境でも端末管理からセキュリティ対策の実現ができます。

システム構成・運用イメージ



提供プラン

		機能				最低購入数
		A RC D	S	M I G	オプション機能 P Vplus F K Mail REC MDM アーカイブ	
オンプレミス	単機能	組み合わせ自由。1機能からOK！				50 ライセンス～
	スタンダードパッケージ	○			ー ※単機能で追加購入可能	
	セキュリティパッケージ	ー ※単機能で追加購入可能		○		

使いやすい

多彩な機能をひとつの画面で操作・管理することができます。

業界初！ Web ブラウザのような高い操作性

一つ前の画面にワンクリックで戻れる
効率の良い操作を実現しました。

目的がすぐ分かる使いやすいメニュー

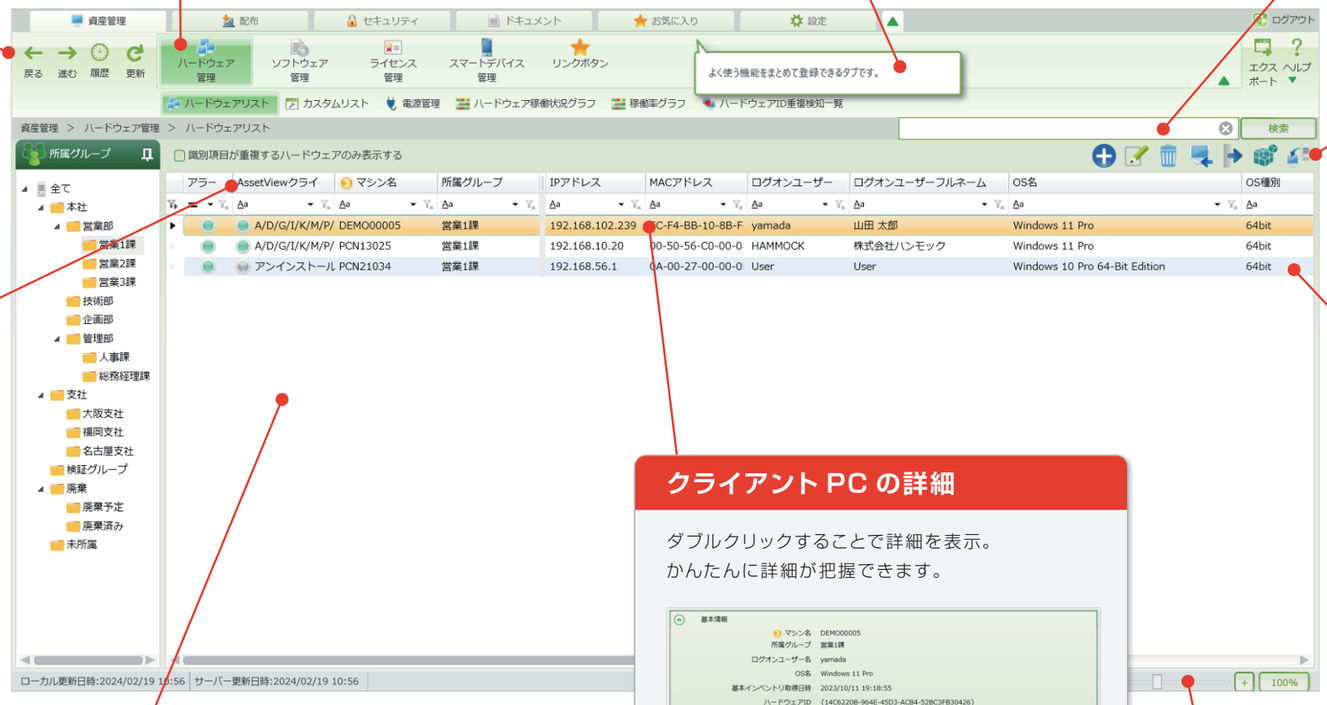
ワンクリックで、目的の画面を開くことができるため
操作に迷いません。

ヒント表示で、操作に迷いません

機能ボタンに、カーソルをあわせることで、
どんな機能で何ができるのかが表示されます。

表示したい情報をキーワードですばやく検索

キーワード検索が行えるので、大量のデータが表示され
ていても、確認したい情報をすばやく抽出できます。

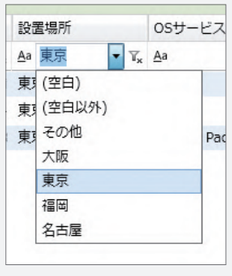


頻度の高い操作は アイコンからワンクリック

追加や削除、編集など使用頻度
の高い操作機能をアイコン表示。
ワンクリックで効率よく作業がで
きます。

必要な情報を、 フィルターですばやく抽出

必要な条件で絞り込んだ情報を CSV、Excel で
加工することなく表示ができるため、情報把握が
短時間で可能です。



コピー＆ペースト、 直接編集が可能

エクスポートはもちろん、表示
項目をそのままコピーして、
Excel に貼り付けることもで
きます。
項目によって、直接値を変更す
ることも可能です。

クライアント PC の詳細

ダブルクリックすることで詳細を表示。
かんたんに詳細が把握できます。

表示領域が広くなったリスト画面

従来の画面より、表示領域が広くなり、
1 画面で表示できる情報量がアップしました。

画面に応じて文字サイズを変更可能

表示倍率の変更が可能になり、
文字サイズの拡大や縮小ができます。

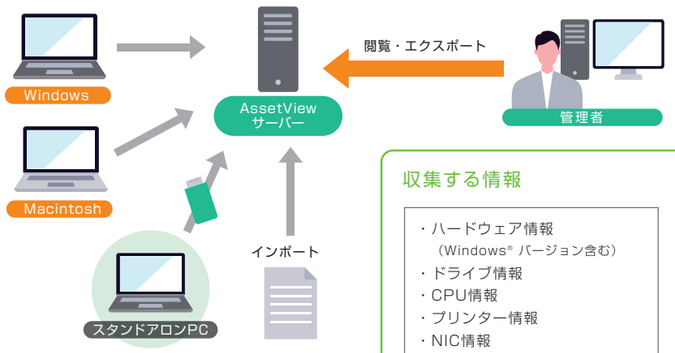
IT資産管理

管理業務を効率化しコスト削減。
コンプライアンス対策を強化。

IT資産管理の基本は企業内のハードウェア、アプリケーション、ドキュメントに関する情報を把握することです。
AssetView は、さまざまなIT資産情報を効率よく管理し、有効活用するための仕組みを多数搭載しています。

70種類以上ものインベントリ情報を手間をかけずに自動収集

社内で稼働するハードウェア、アプリケーションの情報を収集、閲覧できます。収集するタイミングは任意に設定可能です。



収集する情報

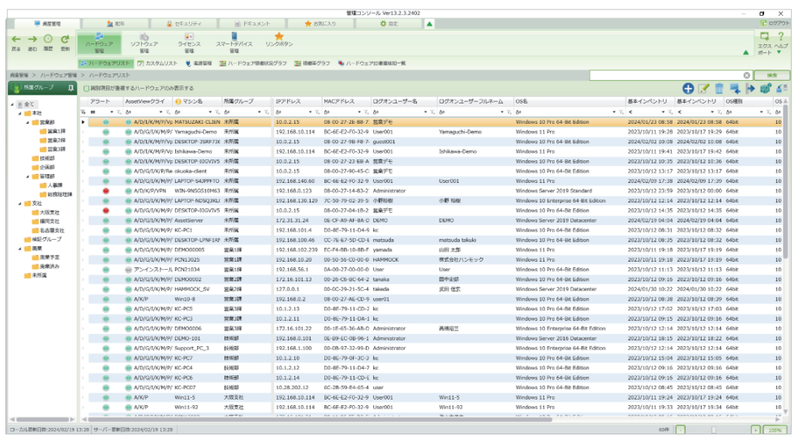
- ハードウェア情報
  （Windows® バージョン含む）
- ドライブ情報
- CPU情報
- プリンター情報
- NIC情報
- INIファイル情報
- レジストリ情報
- MIB情報取得
- 電話番号
- ICCID
  など

- アプリケーションの追加と削除の情報
- Microsoft® Officeの情報
- Adobe® の情報
- JustSystems® の情報
- Autodesk® の情報
- ウイルス対策ソフトの情報
- Hotfixの情報
- 任意の実行ファイル（exe）の情報
  など

- 任意のドキュメントファイルの
  検索情報　など

※上記は Windows® の場合となります。Mac OS® では取得する情報が異なります。

自動収集したハードウェア情報、ユーザーからのアンケート結果、インポートした機器情報を一元的に管理。
IT 資産の管理状況の把握ができる台帳作成がかんたんにできます。

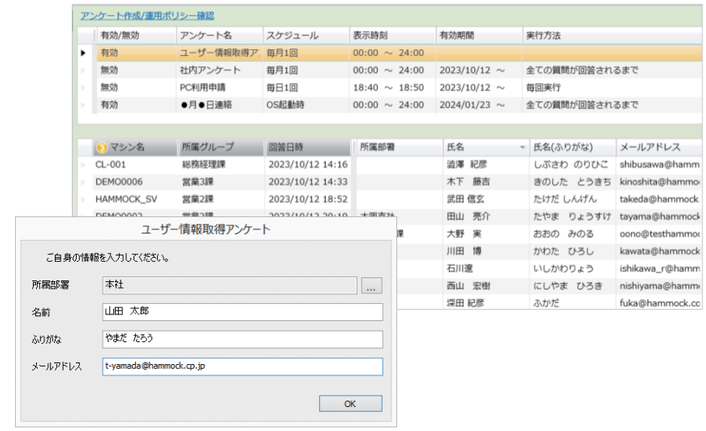


AssetView A
IT資産管理

アンケートを使ってユーザーから情報収集

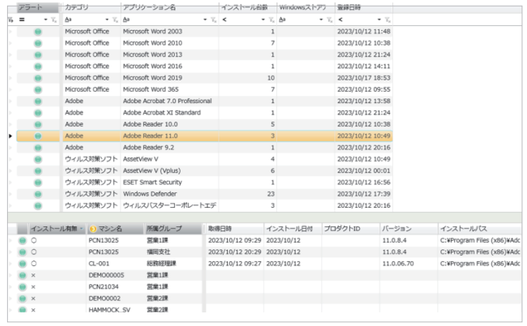
アンケート収集

PC から取得できない情報（資産管理 No、利用者の社員番号等）を、利用者の PC 上に表示させアンケートを行って集めます。スケジュール機能で月に1度実施するなど計画的な情報収集が可能です。



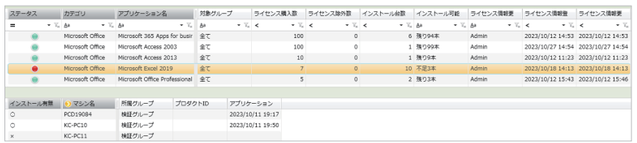
アプリケーションのインストール状況を把握。不正なアプリを発見

クライアント PC にインストールされているアプリケーションを把握できます。
ソフトウェアごとにインストール台数、プロダクト ID やバージョンを一覧で把握できます。
また事前にアラートに指定したアプリケーションのインストールを発見すると、管理者へ通知を送信します。



ライセンス購入数とインストール台数の差分からライセンス超過を発見

ライセンスの購入数に対してインストール台数を自動で突合、不足があるとアラートが上がります。



ソフトウェアライセンス管理

AssetView A IT資産管理

ソフトウェアライセンス管理実現に向けた現状把握や情報の突合作業を効率化。

複雑化したソフトウェアのライセンス形態や、オープンソース、フリーウェアの利用が拡大する現代において、
適切な実態調査や資産情報の管理は組織や担当者にとって大きな負担となります。
AssetView は、現状把握や煩雑な情報の突合作業を大幅に効率化し、
ソフトウェアライセンス管理実現を支援します。

4つの管理台帳を効率よく作成

自動収集したインベントリ情報と、実際に保有しているライセンスの情報は必ずしも一致しているとは言えません。
ソフトウェアライセンス管理実現においては、よく現状把握を行った上で、ハードウェアを含めた情報の突合作業が必要になります。手順に沿って登録することで、ソフトウェア資産管理（SAM）実現に向けて必要とされている4つの管理台帳を効率よく作成できます。

煩雑な現状把握、棚卸の突合作業を効率化

多彩なライセンス/管理形態に対応したソフトウェア管理

ソフトウェアのグループ管理により、サービスパック適用などで不揃いになりがちな情報を一元化できます。
ダウングレード使用権やセカンドライセンスなど、様々かつ複雑なライセンス種別や付帯条件に対応していますので、煩雑なソフトウェアライセンスの管理を効率化します。

例 ダウングレード使用権をふまえた管理の例

ソフトウェア	ライセンス所有数	ライセンス割当 正規	ライセンス割当 ダウングレード権行使	ライセンス割当 合計	過不足
〇〇オフィス2024	5	2		4	1
〇〇オフィス2022	0		2		

ライセンスを適切に管理するため、利用における割当管理や割当予約も可能です。ユーザーからの利用申請機能を活用すると、管理者が承認した時点で割当も完了するため作業負荷を最小限に、効果的なフローで運用プロセスをまわすことができます。

ポイント
承認後、自動割当されるため手間なく適切な管理を実現。
手作業の登録作業でありがちな、ソフトウェア名の差異による管理ミスも防止します。

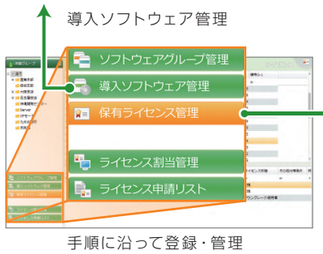
管理対象とするソフトウェアの分類や関連情報の管理もかんたん

取得したインベントリデータやソフトウェア辞書による情報をもとに、ソフトウェアを分類し、管理対象とするソフトウェアを決定します。
ソフトウェアのベンダー名や、インベントリ情報の有無を条件に、管理対象とするソフトウェアをかんたんに抽出・分類することができます。

ソフトウェア辞書（オプション）

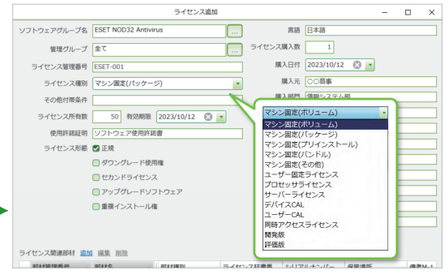
- 23万種類以上のソフトウェア情報を収録
- 辞書データは定期的に更新

ソフトウェア辞書により、そのソフトウェアが製品版なのか、フリーウェアなのか、といった分類を自動的に行うことができます。



手順に沿って登録・管理

保有ライセンス管理



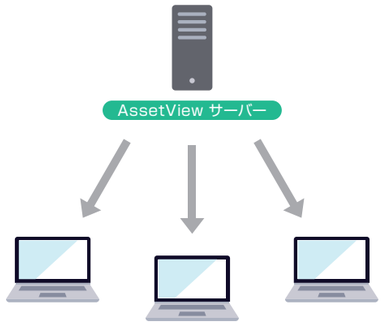
ポイント
保有しているソフトウェアのライセンス情報は、
ライセンス種別や形態、また関連部材を紐づけた管理が可能です。

アプリケーション配布

アプリケーションインストールと
設定変更も自動化して効率アップ。

Windows® 上で動作するほとんどのアプリケーションの自動インストールや環境設定の変更が可能です。
クライアントPCを回らずに管理者の設定だけで実現できるため、作業効率アップにつながります。
マクロメーションでサイレントインストール未対応ソフトの自動展開も可能です。
成功率を向上させるための細やかな条件設定ができます。

さまざまなインストール・環境設定を実現



- ファイル配布
- ソフトウェアインストール
- 環境設定変更
- セキュリティパッチ適用
- OSシャットダウン、再起動
- プリンタドライバーインストール

社内の業務用アプリケーションのバージョンを統一したり、緊急性が高いセキュリティパッチなどのプログラムを定期的にインストールすることでクライアント PC のトラブルを未然に防ぐことができます。また、アプリケーションの自動インストールだけでなく、各クライアント PC の環境設定の変更も可能です。管理者は、クライアント PC を回らずに一括したポリシーを適用させることができます。

アラート	有効/無効	優先順位	タスク名	タスク種別	対象グループ
	無効	1	情報システムの利用案内を配布	ファイル配布	全て
	有効	2	アンインストール：百度（アンインストーラーを起動）	プログラム実行	全て
	有効	3	アンインストール：旧ウイルス対策ソフト	プログラム実行	全て
	有効	4	アンインストール：旧フィルタリング対策ソフト	プログラム実行	全て
	有効	5	アンインストール：旧IT資産管理ソフト	プログラム実行	全て
	有効	6	設定変更：スクリーンセーバーの起動時間（1分）	レジストリ編集	全て
	有効	7	インストール：Officeソフト	プログラム実行	全て
	有効	8	インストール：PDF閲覧ソフト	プログラム実行	全て
	有効	9	インストール：プリンタドライバ（*****）	プログラム実行	全て
	有効	10	インストール：セキュリティパッチ（MS14-**）	プログラム実行	全て
	有効	11	インストール：リマインダー	プログラム実行	全て
	有効	12	インストール：圧縮・解凍ツール	プログラム実行	全て

ウィザード形式でインストール・環境設定変更が可能

専門的な知識や操作は不要のウィザード形式で
インストールや環境設定のタスクが作成できます。

ステップ1

配布対象PCを確定します。
インベントリから条件指定で端末を抽出したり、配布専用のグループを予め作成することで、適切な対象PCに対して実施ができます。

ステップ2

実施内容や、実施条件を設定します。実施タイミングも、OS起動時や、毎日、曜日指定など柔軟な選択肢の中から画面に従って入力できます。

また、大容量のデータの配布を行う際に、対象のPCが無線LANやVPNに接続している場合には実行しないなど、PCの状態に配慮して実行回避できるため、環境に負荷をかけずに配信業務を実施できます。

ステップ3

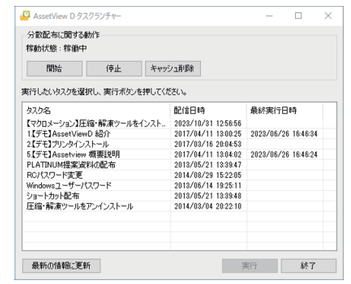
配布対象ファイルの指定や、実行コマンド等を指定します。成功条件も指定できるため、配信業務を円滑に進められます。

ポイント
スクリプトの作成不要、
GUI で簡単に設定できます。

利用者の任意タイミングでの実行が可能

タスクランチャー

インストールや環境設定を強制的に実行するだけではなく、クライアントPCを使うユーザーの、任意のタイミングでインストールを実行することが可能です。



ポイント
利用者は選択して実行する
だけの簡単操作。

アプリケーション配布

ネットワークに負荷を与えない、
通信機能「マルチキャスト配布」を標準搭載

ネットワークの負荷を軽減する、配信効率と運用性の高いアプリケーション配布を行うための
分散通信方式を標準搭載しています。

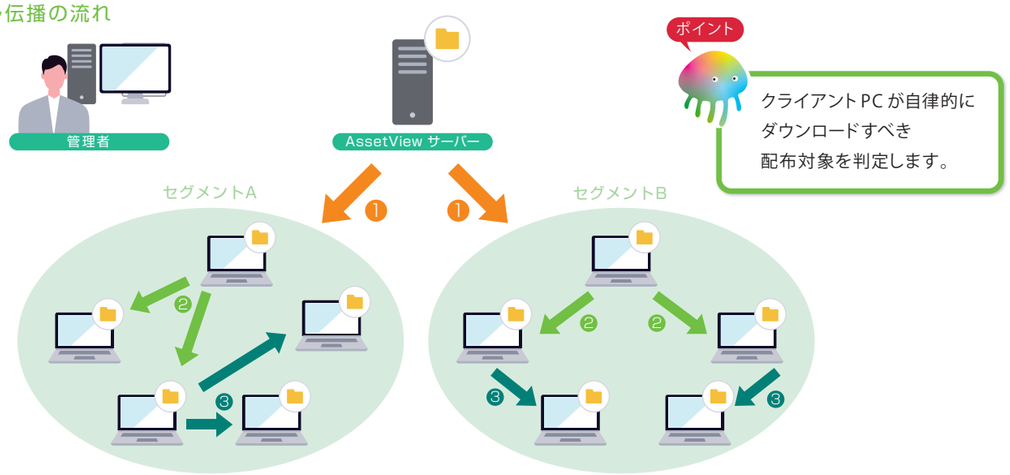
AssetView D アプリケーション配布

低負荷（ネットワーク）を実現したマルチキャスト配布を支える仕組み

ネットワーク回線が細い環境でもネットワーク負荷を抑えたクライアント PC へのファイルやアプリケーション配布が可能です。

- ネットワーク負荷を分散したファイル配布
- キャッシュによる上流ネットワークの負荷軽減
- 重複ダウンロード自動判別機能
- グルーピングによる帯域制御

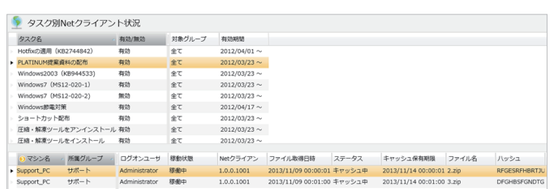
ファイル伝播の流れ



1. セグメント内のクライアント PC いずれか1台が、サーバーからファイルをダウンロード。
2. サーバーからファイルをダウンロードしたクライアント PC から、他のクライアント PC がファイルをダウンロード。
3. セグメント内のクライアント PC に次々にファイルが伝播していきます。

ファイル伝播状況の把握

クライアントごとの視点、ファイルごとの視点で状況把握可能です。



ポイント

グルーピングによる帯域制御が可能。

グループごとに利用帯域の上限を設けることが可能です。帯域幅の上限は、パーセンテージで設定できます。システム管理者は、通信速度の詳細まで把握することなく設定を実施できます。

システム管理者の運用負担を軽減

ダウンロード自動再開（レジューム）機能

クライアント PC の省電力設定が適用されるなど、ダウンロード中に何らかの原因で通信が中断しても、次回通信時にはダウンロードの途中から再開します。しかもレジューム機能は、クライアント間の通信でも有効ですのでセグメント内のネットワーク負荷をあげることなく、システム管理者の手を煩わせることもなく確実にファイル配布が行えます。

管理コンソール上にてファイルの伝播やキャッシュ状況の把握

クライアントごとの視点、ファイルごとの視点で状況把握が可能です。状況にあわせてシステム管理者側から該当クライアントに対してマルチキャスト機能だけを停止、キャッシュ削除等の操作が可能です。

さまざまな対障害性能

ハッシュキー チェックによるファイルの正常性対応

ダウンロード後、キャッシュしたファイルとサーバーにある配布ファイルのハッシュ値を比較。違っている場合は、ダウンロードを再開し正常なファイル入手を行います。ダウンロード中にファイル破損した場合の対策や、システム管理者の誤操作によりファイル対象を設定後すぐに変更した場合等、ファイルの正常性を担保するのに有効です。

管理コンソールでの集中管理

クライアント側の動作ログはサーバーで一元管理。システム管理者はログから状況を把握し、アクションを行うことができます。

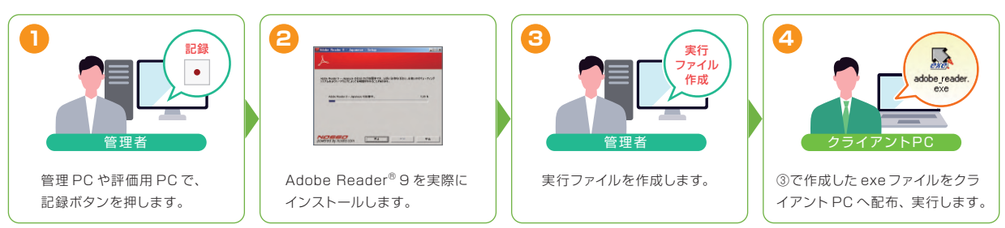
拠点間の通信障害時にも対応可能

回線が細い拠点や拠点間障害時等に対して、大容量のファイルを配布したい場合、サーバー・クライアント間の通信をメディア等で代用する運用が可能です。

自動展開に便利な自動化プログラム（EXE）をGUI操作で作成可能

マクロメーションは、アプリケーションのインストールや環境設定変更実行を管理者の画面で操作するだけで、条件を記録し、クライアント PC 側で再現できる機能です。クライアント PC の環境設定にも活用できます。マクロメーションを使えば、ほとんどのアプリケーションのインストールを自動化できます。

例 Adobe Reader® 9をマクロメーションを使ってクライアントPCに配布



PC操作ログ管理

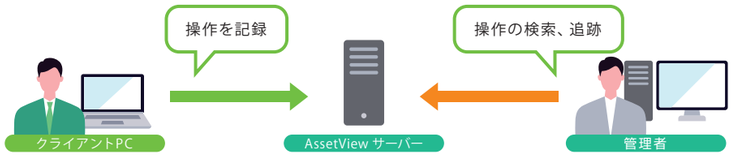
日立ソリューションズの「秘文」シリーズにOEMとして提供を行っている、
高品質で確かな技術のPC操作ログ取得機能です。

AssetView M PC操作ログ管理

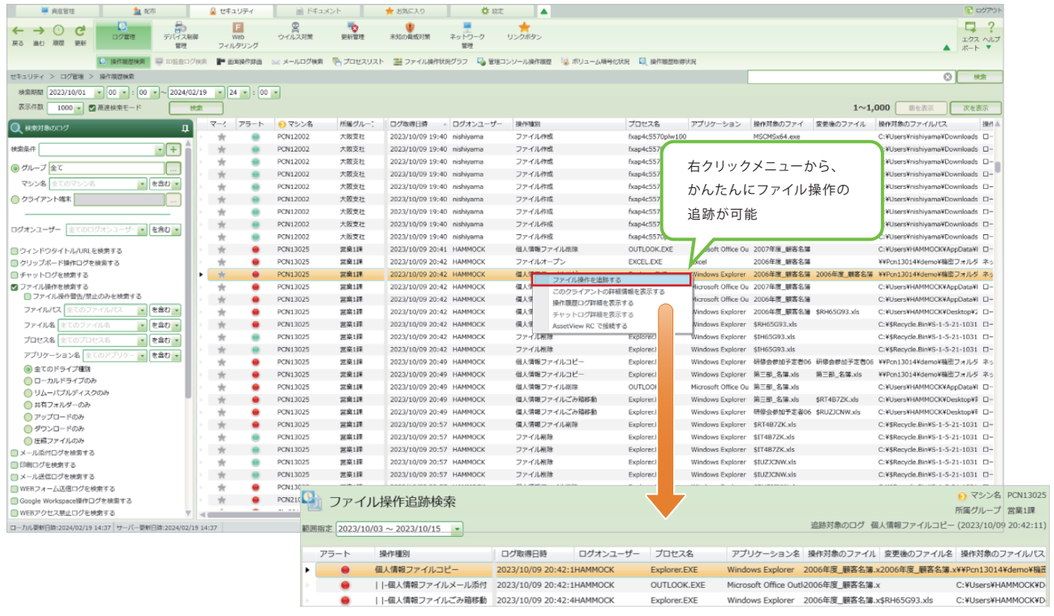
PC操作ログを取得し、効率的に把握、検索、追跡。

クライアントPC操作に関するさまざまなログを取得できます。
AssetView はこれらのログを効率的に把握することができます。問題のある操作は操作ログの一覧上でアラートを出し、クリックで詳細な情報を表示。膨大なログの中から、すばやく絞り込める機能を搭載し、特定操作の前後の操作を追跡することも可能です。
情報漏洩対策に効果を発揮します。

PC操作ログを自動取得、効率的な操作の把握が可能



目的に応じて複数の検索条件を保存しておくことで効率的な検索ができます。
また、ファイル流出経路が追跡できるようにファイル操作の追跡も可能です。



クライアントPCで行われるさまざまな操作を記録

クライアント PC に関するさまざまな操作ログを取得、監視します。
取得の可否も細やかに設定することができ、ポリシーや運用環境に合わせた監視体制を構築することができます。

取得項目	内容
PC 起動	クライアント PC の稼働状況を確認するための情報を取得。 ・AssetView クライアント起動（PC 起動） ・OS ログオン ・スリープ解除 ・ロック ・アンロック ・OS ログオフ ・スクリーンセーバー ・OS シャットダウン要求 ・スリープ ・スクリーンセーバー解除 ・OS シャットダウン
ファイル操作	クライアント PC で行われた、ファイル操作の情報を取得。 ・操作対象のファイル名 ・コピー / 移動先のドライブ種別 ・操作対象のファイルパス ・スマートフォンへのファイル操作ログ ・操作元のドライブ種別 ・コピー / 移動先のファイルパス ・変更後のファイル名 ・プロセス名
Microsoft365®のファイル操作	Web ブラウザ上で行った Microsoft365® の以下のファイル操作の情報を取得。 ・新規作成 ・ファイルオープン ・名前を付けて保存 ・コピーを保存 ・名前の変更 ・ローカルへのダウンロード
インターネットへのファイルアップロード	クライアント PC から Web サイトに HTTP-POST でアップロードされたファイルの情報を取得 ・操作対象のファイル名 ・操作対象のファイルパス ・アップロード先の URL ・HTTP（S）ファイルアップロードログ ▼対象サービス ・Dropbox ・GoogleDrive ・FilePost ・汎用サイト ・OneDrive（個人用） ・Box ・NetFolder ※content-type として「multipart/form-data」が指定 ・OneDrive for Business ・EverNote ・アップローダー ・SharePoint ・おくりん ・汎用サイト ※Firefox /Chrome /Edge(Chromium) で取得可能
ファイルダウンロード	Webブラウザで行ったダウンロード元のURL情報を取得。
メール添付	メール作成時に指定した添付ファイルの情報を取得。 ・操作対象のファイル名 ・操作対象のファイルパス ・プロセス名 ・操作元のドライブ種別
メール送信	メール送信ログを取得します。 ・件名 ・送信元メールアドレス ・添付ファイル名 ・送信日時 ・送信先メールアドレス ※SMTP／ESMTP で送信されたメールが取得対象。 ※AssetView Mail を追加することで本文、添付ファイル実体も取得可能。
印刷	クライアント PC で印刷された、ドキュメントの情報を取得。 ・ドキュメント名 ・プリンター名 ・印刷データタイプ ・ファイル名 ・印刷枚数
ドライブの追加と削除	ドライブの追加と削除を検知して、以下の情報を取得。 ・ドライブ種別（ローカルディスク、リムーバブルディスク、ネットワークドライブ、FD、CD/DVD、ポータブルデバイス） ・ドライブ名 ・UNC パス（ネットワークドライブの場合） ・デバイス名（USB デバイス / ポータブルデバイスの場合） ・ベンダー（USB デバイス / ポータブルデバイスの場合） ・プロダクト ID（USB デバイス / ポータブルデバイスの場合） ・シリアルナンバー（USB デバイス / ポータブルデバイスの場合）

	内容
クリップボード操作 ※オンプレ版のみ	クライアント PC で行われた、以下のクリップボード操作を取得。 ・文字列のコピー ・画像のコピー / プリントスクリーン ・ファイルのコピー
ウィンドウタイトル	クライアント PC でアクティブになっているウィンドウの情報を取得。 ・プロセス名 ・ウィンドウタイトル ・URL
プロセス	クライアント PC で起動している、プロセスの情報を取得。 ・プロセス名 ・バージョン ・起動していた時間 ・アカウント名 ・起動日時 ・Windows ストアアプリ 対応
Web フォーム送信 ※オンプレ版のみ	クライアント PC から Web サイトへの書き込みを検知して情報を取得。 ・接続先 IP アドレス ・ポート番号 ・URL ・本文（送信データ）
FTP ファイルアップロード	FTP サーバーへのアップロードされたファイルの情報を取得。 ・ファイル名 ・ファイルパス ・送信先 IP アドレス
Google Workspace	Google Chrome で操作した Google Workspace の情報を取得。 ・Google ドライブ ・Google カレンダー ・Gmail ・Google グループ
Wi-Fi 接続	Wi-Fi 接続、切断した情報を取得。 ・Wi-Fi アクセスポイント接続 ・Wi-Fi アクセスポイント切断 ・Wi-Fi アクセスポイント接続禁止 ※AssetView G（デバイス制御）ライセンスが必要です。
Bluetooth ペアリング	Bluetooth 機器とペアリングした情報を取得。 ・Bluetooth 機器ペアリング ・Bluetooth 機器ペアリング解除 ・Bluetooth 機器使用禁止 ※AssetView G（デバイス制御）ライセンスが必要です。
システムログ監視	システムログの取得、レジストリやファイルの更新があった場合にその情報を取得。 ・Windows イベントログの取得 ・指定したレジストリエントリの更新 ・指定したファイルの更新

※アプリケーションや環境によって制限事項がございます。
詳細は営業担当までご確認ください。

PC操作ログ管理

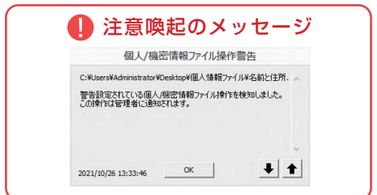
不正な操作には警告。
ユーザーのセキュリティ・コンプライアンス
意識向上を促進。

さまざまな情報の取得･管理は証跡管理としての活用にとどまりません。
不正な操作が行われた際には警告や操作の禁止をすることで、適切なIT資産利用が保たれ、
社内ポリシーや情報漏洩に対するユーザーの意識向上にも高い効果を発揮します。

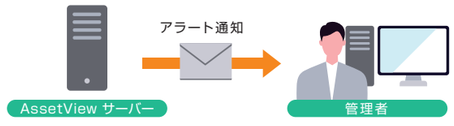
AssetView 個人情報検索

個人情報ファイルの証跡管理、利用者への注意喚起からセキュリティ意識を向上

クライアントPCでファイル操作があるたびにリアルタイムで中身をチェックし、個人情報、機密情報を含む操作であった場合には、管理者はアラート通知を受け取ったり、管理画面上で操作ログとして確認できます。またクライアントPC利用者には操作の際に注意喚起のメッセージを表示させることで、不正操作への抑止効果が期待できます。



1、ファイル操作を検知
2、ファイルの中身をチェック
3、個人情報や機密情報の場合には注意メッセージを表示
4、管理者へアラート通知を発報
5、ログ画面でも証跡確認



ポイント

PCN13025	営業1課	2023/10/09 20:49	HAMMOCK	個人情報ファイルごみ箱移動	Explorer.EXE	Windows Explo	第三部_名簿.xls
PCN13025	営業1課	2023/10/09 20:49	HAMMOCK	個人情報ファイルごみ箱移動	Explorer.EXE	Windows Explo	研修会参加予定者0610
PCN13025	営業1課	2023/10/09 20:57	HAMMOCK	個人情報ファイル削除	Explorer.EXE	Windows Explo	$RT4B7ZK.xls
PCN13025	営業1課	2023/10/09 20:57	HAMMOCK	個人情報ファイル削除	Explorer.EXE	Windows Explo	$RUZJCNW.xls
PCN21034	営業1課	2023/10/10 13:59	Administrator	ファイル作成(実行ファイルの不正操作)	OneDrive.exe	OneDrive	OneDriveSetup.exe
CL-001	総務経理課	2023/10/10 14:14	Administrator	特定個人および個人情報ファイルコピー	Explorer.EXE	Windows Explo	デモデータについて.txt

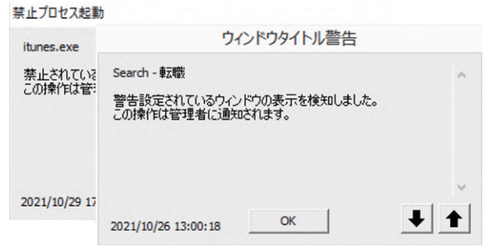
ファイル名では判断せずに、中身の情報をチェックしているため、一見すると個人情報に見えないファイル名でも、
実は「個人情報をコピーした」という操作を証跡として追うことが可能です。

AssetView M PC操作ログ管理

不正アプリケーション操作・不正WEB閲覧に対して警告・禁止で問題を未然に解決

クライアントPC上の様々な不正操作を禁止したり、警告メッセージを表示し注意喚起することが可能です。警告メッセージが表示されることでユーザーへの抑止効果も働きます。

例：特定プロセスの起動禁止/警告
　　特定文字列をタイトルに含むウィンドウオープンへの警告



PCの起動ログから隠れ残業を発見

クライアントPCのログオン、ログオフ、シャットダウンのログと勤怠システムの情報をもとに隠れ残業を発見できます。

◀取得ログ（時系列で端末の起動状況を確認できます。）

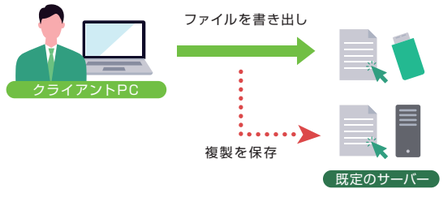
マシン名	所属グループ	ログ取得日時	ログオンユーザー	操作種別
PCN12002	大阪支社	2023/10/09 15:20	Administrator	スリープ
PCN13025	営業1課	2023/10/09 15:31	SYSTEM	スリープ解除
LAPTOP-S4JPPF	未所属	2023/10/09 16:04	SYSTEM	OSシャットダウン
AssetServer	未所属	2023/10/09 16:16	DEMO	OSログオフ
AssetServer	未所属	2023/10/09 16:16	SYSTEM	OSシャットダウン
AssetServer	未所属	2023/10/09 16:17	SYSTEM	AssetViewクライアント起動
AssetServer	未所属	2023/10/09 16:17	DEMO	OSログオン
CL-001	総務経理課	2023/10/09 16:19	Administrator	スリープ
AssetServer	未所属	2023/10/09 16:40	SYSTEM	AssetViewクライアント起動
AssetServer	未所属	2023/10/09 16:40	DEMO	OSログオン
PCN12002	大阪支社	2023/10/09 16:52	Administrator	スリープ解除
DEMO00005	営業1課	2023/10/09 17:02	SYSTEM	AssetViewクライアント起動
DEMO00005	営業1課	2023/10/09 17:02	Administrator	OSログオン

▼標準レポート
（1日の最初のログオン、最後のシャットダウンから稼働時間を割り出します。）

マシン名	2017年 6月 1 木			2 金		
	ログオン	シャットダウン	稼働時間	ログオン	シャットダウン	稼働時間
HOSTNAME-0001	8:43:49	17:50:35	9:06:46	8:42:30	18:14:47	9:32:17
HOSTNAME-0002	8:39:09	17:49:45	9:10:36	8:43:49	17:50:35	9:06:46
HOSTNAME-0003	8:43:49	17:50:35	9:06:46	8:39:09	17:49:45	9:10:36

書き出したファイルを自動で複製保存（シャドウイング）

USB デバイス、CD/DVD、ポータブルデバイスへコピー / 移動を行ったファイルをサーバー上に複製保存（シャドウイング）します。これにより、万が一不正な持ち出しがあった場合に、対象ファイルの原本を確認することができます。



デバイス制御も併せて運用が効果的

AssetView G デバイス制御

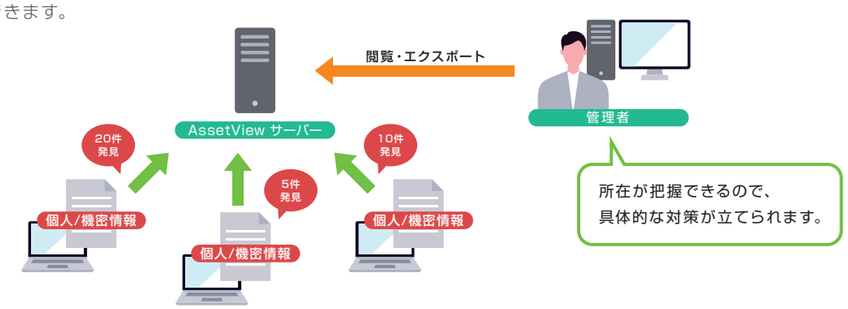
個人情報検索

個人情報の棚卸で
情報漏洩リスクを把握。

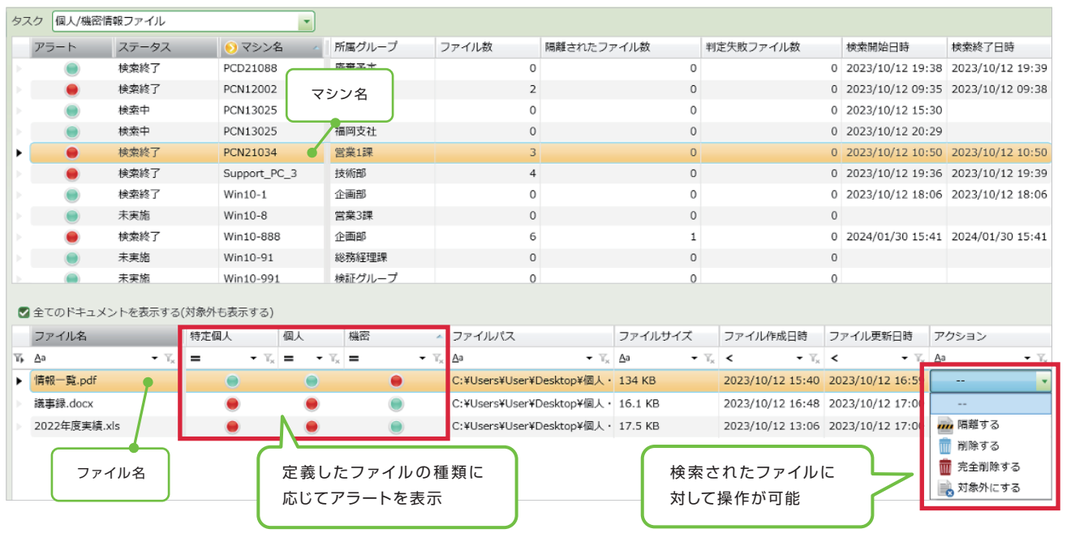
個人情報保護法が施行されてから、企業における個人情報の扱いにはさらに慎重さを要するようになりました。
AssetView は、社内のクライアントPC内に放置されている個人情報をファイル内まで検索し、洗い出しを行うことができます。
企業・組織として大きな情報漏洩リスクとなる情報資産の棚卸を実現し、
個人情報や機密情報取り扱いに対する意識向上を図ることができます。
マイナンバーを含むファイルを特定個人情報ファイルとして検索することも可能です。

ファイルの中身をチェックして個人、機密情報が含まれるファイルを棚卸

所在を把握することで、拡散している重要ファイルを把握して、適切な管理・運用をすることで情報漏洩リスクを大幅にさげることができます。



社内のクライアントPCに存在する個人情報、機密情報が含まれるファイルをファイル内までチェックして検索します。
個人情報だけでなく、重要なキーワードを含むファイルを機密情報ファイルとして定義できます。
さらに、検索されたファイルに対して、隔離、削除、完全削除、対象外の操作が可能です。



AssetView I 個人情報検索

スケジュール実行による定期監査、検出時の自動暗号化も対応

毎月1回 12:00 ～ 13:00 に実施するなど個人情報検索のスケジュール実行が可能です。
また、クライアント PC から個人 / 機密情報が検出された際にメールによるアラート通知をだすなど定期的な自動監査に役立ちます。

ポイント
リアルタイムでアラート通知が送信されるため、タイムリーにセキュリティ上の懸念に対応できます!

検出と同時に検出されたファイルに対して、ファイル暗号化（AssetView K との連携機能）や、隔離を行う設定も可能です。

ファイル検出時に自動暗号化
万が一の情報漏洩対策に役立ちます。
＋ AssetView K ファイル制御・暗号化

利用環境にあわせて個人、機密、特定個人情報の定義が可能

条件に一致する文字列が設定数以上検出された場合に、そのファイルを個人、機密、特定個人情報ファイルとして検出します。
「or」条件だけでなく、「and」条件による検出が可能なので検出設定を細かく設定できます。

個人情報ファイルの定義

- 人名
- 住所
- 生年月日
- 電話番号
- メールアドレス
- 免許証番号
- パスポート番号
- クレジットカード番号
- 口座番号
- ユーザー辞書（任意の文字列）

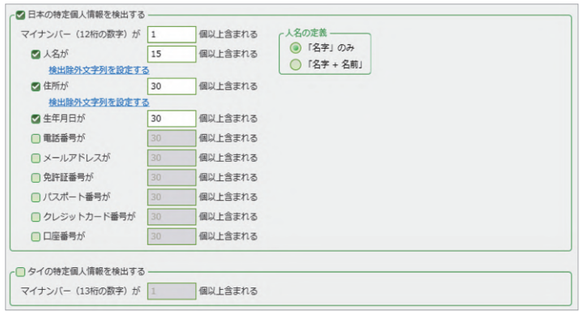
特定個人情報ファイルの定義

- マイナンバー
- 人名
- 住所
- 生年月日
- 電話番号
- メールアドレス
- 免許証番号
- パスポート番号
- クレジットカード番号
- 口座番号

機密情報ファイルの定義

任意の文字列を自由に追加

特定個人情報ファイル



ポイント
検出対象から除外したい文字列を設定することが可能です。

デバイス制御

USBデバイスを管理し、制御する。
セキュリティ対策の必須機能。

小型で大容量データの持ち運びができるUSBデバイスは、個人情報や機密情報などの重要情報を大量に持ち出すことが可能です。
また、管理ミスによる情報漏洩リスクもあり、今後その対策は必須と言えます。
対策には、社内のUSBデバイスを把握し、ユーザーに適切に使用させるための制御が必要です。

情報漏洩リスクの高いUSBメモリ、SDカードなどデバイスを制御

全体、グループ、ユーザーごとにデバイス制御（書込み許可、読取り専用、使用禁止）の設定が可能です。

ステップ１ デバイス制御のポリシー設定

大きなアイコンと、分かりやすい設定画面でかんたんに設定。
クリック操作だけでお好みの設定にできます。

ポイント

グループ単位でのデバイス制御ポリシーの設定も可能です。

ステップ２ デバイス制御を個別に設定

グループごとのデバイス制御設定

グループごとにデバイス制御（書込み許可、読取り専用、使用禁止）の設定が可能です。

例

ユーザーごとのデバイス制御設定（Active Directory 連携）

Active Directory 上のユーザー単位でデバイス制御が可能です。きめ細かな設定までサポートしています。

例

メディアを識別した制御を実現

個々のメディアを識別して個別に制御することができます。

AssetView G デバイス制御

デバイス制御の影響を受けない特権ユーザーの定義が可能

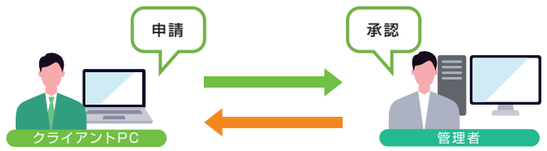
Active Directory 上の「役職」情報からデバイス制御の影響を受けない特別な権利を持ったユーザー（特権ユーザー）の定義が可能です。システム管理者、部門の USB デバイス管理者はデバイス制御をしない柔軟性の高い運用が可能です。

通信デバイス制御

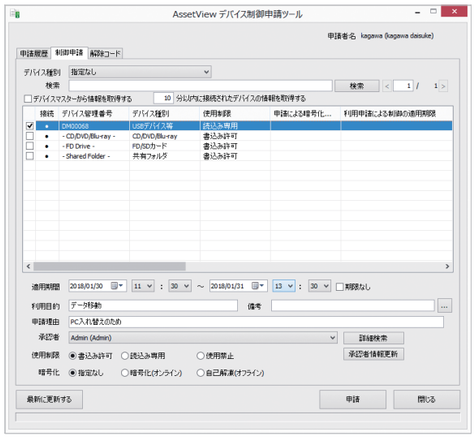
Wi-Fi や Bluetooth の使用制限をかけられます。
Wi-Fi では、SSID と BSSID の組み合わせで個体識別を行います。社内の Wi-Fi 以外は利用を制限するなど持ち出し端末が不要に公衆 Wi-Fi に接続し、通信を盗聴されるリスクを防ぎます。Bluetooth は、デバイス検知に MAC アドレスを取得することで個体制御を実施します。スマートフォンと PC 間の Bluetooth によるデータ通信も PC 側で会社貸与機器以外のスマートフォン利用制限することで、不正な情報の持ち出しなどを制御します。

デバイス利用申請で柔軟でよりセキュアな運用を実現

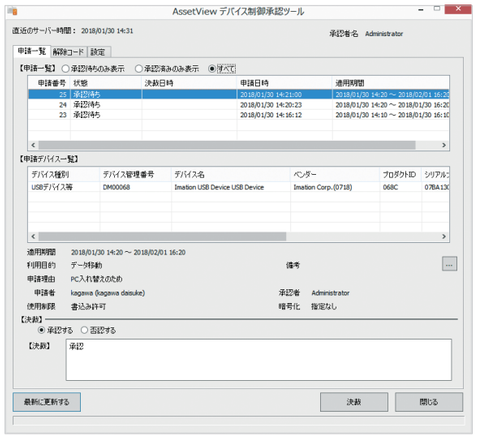
デバイス制御ポリシーで利用が禁止されているデバイスも申請機能で利用することができます。
ユーザーごとに利用するデバイスを管理者に申請することで期間や制御内容、さらには利用時の『自動暗号化』までを指定した利用申請、承認が可能です。



▼利用申請画面



▼申請承認画面



不正PC遮断

AssetView S 不正PC遮断

管理されていないIT機器を検知。
不正なPCは社内ネットワークから遮断。

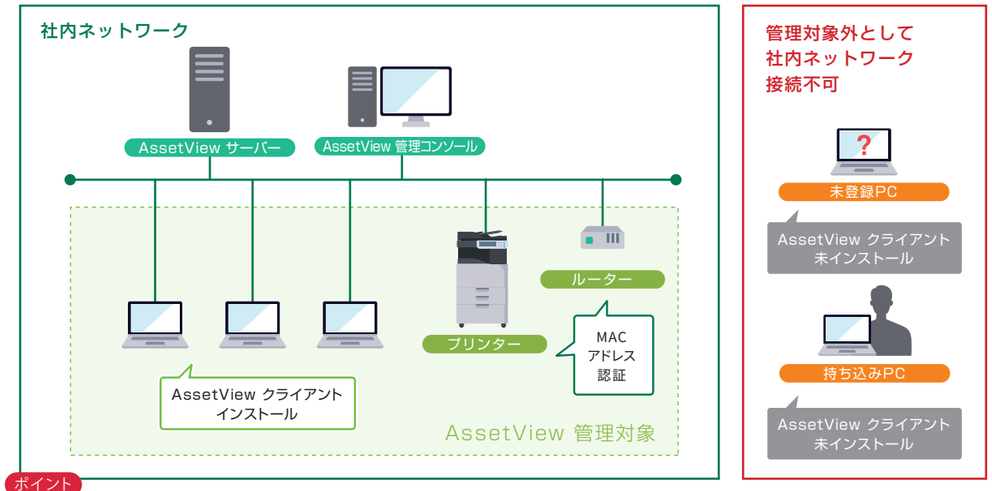
AssetView は、ネットワークに新しい機器を導入せずにソフトウェアによる遮断を実現しました。
管理されていないPCがネットワークに接続されたら検知、遮断し、情報漏洩やウイルス感染などのリスクを防ぎます。

ソフトウェアによる遮断を実現

AssetView クライアントのインストール認証、MAC アドレス認証により、社内ネットワークへの接続を管理します。
不正利用や未許可 PC の接続を排除できるため、P2P ツールの対策にもつながります。
遮断・検知が不必要なセグメントには AssetView S を有効にしない運用も可能なため、フレキシブルに活用できます。

運用イメージ

1. 管理対象のPCに、AssetView クライアントをインストール
2. ハードウェアの検知機能を有効にする
3. プリンター、ルーターなどのMACアドレスを接続許可に設定
4. 許可されていないハードウェアを遮断する運用に移行



ポイント

指定した IP アドレスの範囲のみのネットワーク制御（検知・遮断）が可能です。

ネットワーク機器の自動追加が可能

AssetView クライアントがインストールできない PC（対象外 OS など）や MAC アドレスを持つネットワークプリンターなどのネットワーク機器を検知し、自動的に追加します。これらの機器はハードウェアリスト上で、AssetView クライアントがインストールされた PC や手動で追加したネットワーク機器以外のハードウェアと一緒に表示できるため、効率的な把握・管理を行うことができます。

リモートコンソール

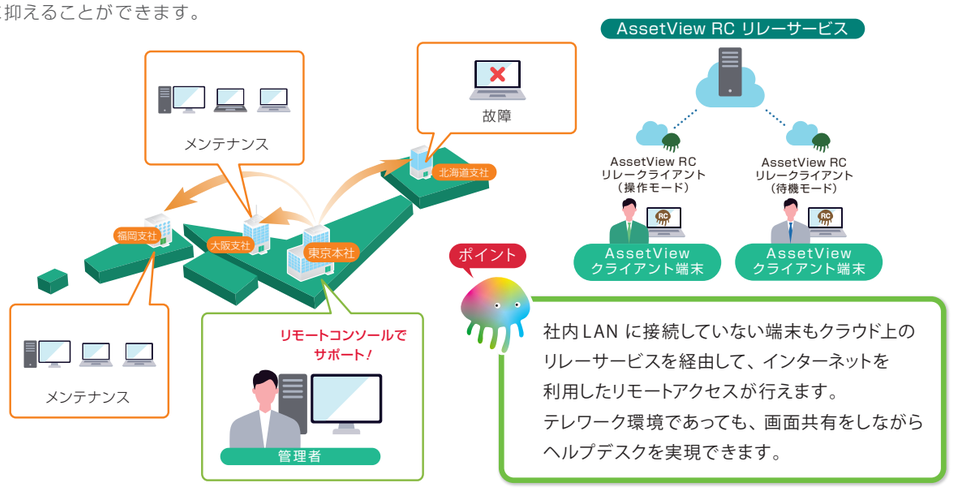
AssetView RC リモートコンソール

遠隔地のクライアント PC をリモート操作。
ヘルプデスク業務の効率化を支援。

管理 PC からリモート操作で遠隔地のクライアント PC を複数台同時に操作できる機能です。
管理者主導のさまざまなアクションが実行可能です。管理工数の大幅削減を実現し、メンテナンスをサポートします。

リモート接続で遠隔地への現地サポートコストを削減

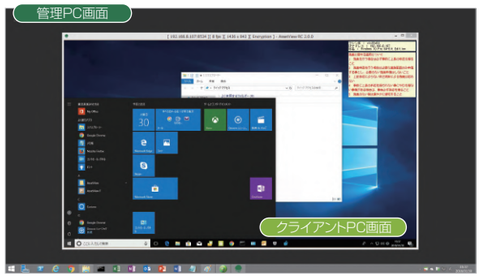
故障やメンテナンスの対応も、リモートコンソールを活用すれば、わざわざ現地に出向かなくても、スピーディーに対応できます。これまで出張していたコストを削減できるだけでなく、ユーザーの業務に支障がでる時間を最小限に抑えることができます。



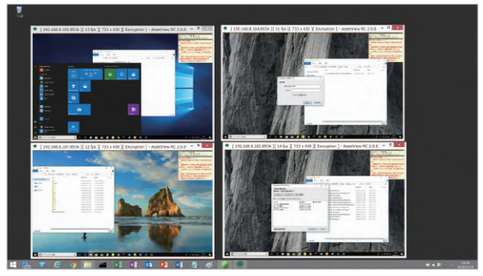
ポイント

社内 LAN に接続していない端末もクラウド上のリレーサービスを経由して、インターネットを利用したリモートアクセスが行えます。
テレワーク環境であっても、画面共有をしながらヘルプデスクを実現できます。

管理画面から右クリックでかんたんにリモート操作が可能



▲操作画面



▲複数台同時接続・監視画面

セキュアで利便性の高いリモート操作を実現

AssetView RC は、「暗号化通信」に対応し、ホストとゲスト間の通信をセキュアに保つことが可能です。
また、操作時に「圧縮方式」「画像品質」「ビデオレート」等を変更することができるので、通信環境に影響を受けやすいリモート操作にも柔軟に対応できます。

PC更新管理

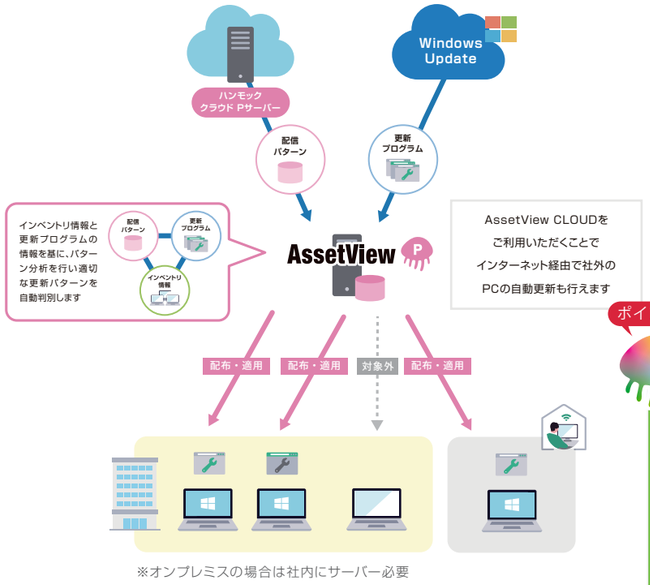
Windows
更新管理対応

AssetView P
PC更新管理

「可視化」「ネットワーク負荷軽減」の視点で、Windows 更新プログラムの配信・管理業務を支援。

Windows を業務利用するうえで定期的なアップデート管理体制を整えない場合、「未検証での更新適用による端末不具合」「大容量更新プログラムによるネットワークの負荷」等 業務へ大きな影響を与えます。
「AssetView P」は、わかりやすい管理画面と分散配布機能によって、PCの更新管理業務の課題解決を支援します。

PC更新管理機能でできること



※オンプレミスの場合は社内にサーバー必要

◀PC更新管理「AssetView P」の全体像

社内の Windows 端末の状態を可視化し、個々のクライアント PC ごとに Windows Update がかからないように制限をかけ、AssetView サーバーから FU、QU、Defender の定義ファイル、Microsoft365 /Office2019/2021 等を負荷分散しながら柔軟なタイミング指定のもと配信・実行を行います。

ポイント

その1　WindowsUpdate の制御
その2　端末の状態の可視化
その3　配信時のネットワーク負荷分散
その4　FU/QU/Defender の定義ファイル、Microsoft365、Office2019/2021 等の配信・実行
　　配信・実行時の柔軟な条件指定
その5　実行エラーの際の原因究明と対策

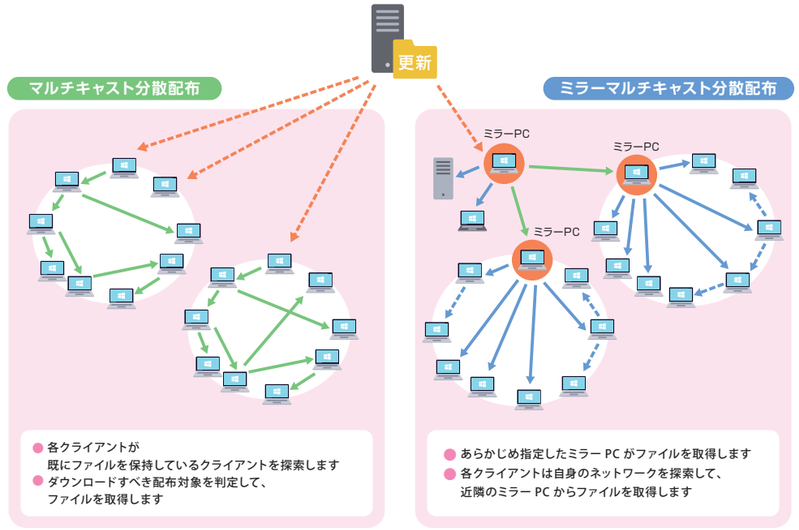
Windows 端末設定状況を可視化

各 PC の FU、QU の状態を一覧で確認出来ます。
現状、社内 PC がどのような設定なのかを可視化することで、展開計画を立てやすくなります。

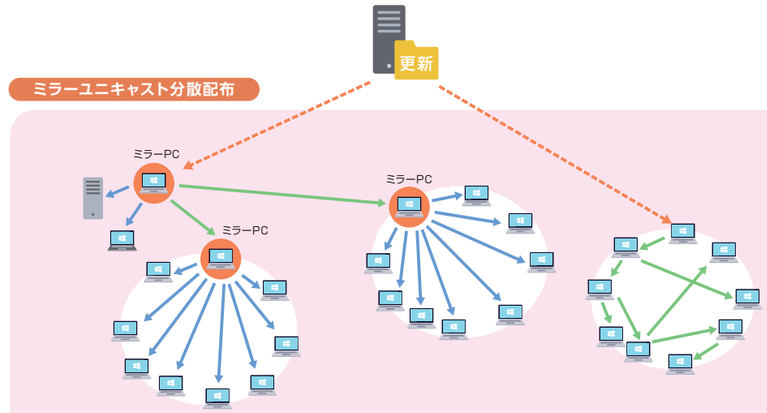
マシン名	所属グループ	OS名	Windowsバージョン	品質更新
Win11-997	購買支社	Windows 10 Pro 64-Bit Edition	不明	2023-10
PCD19084	検証グループ	Windows 11 Pro	22H2	2023-10
Win11-5	大阪支社	Windows 11 Pro	不明	2023-10
Ishikawa-Demo	未所属	Windows 11 Pro	不明	2023-10
assetview-test02	廃棄済み	Windows 11 Pro	22H2	2023-05
assetview-test01	廃棄済み	Windows 11 Pro	22H2	2023-04
KC-PC01	検証グループ	Windows 10 Pro 64-Bit Edition	22H2	2023-03
KC-PC03	企画部	Windows 10 Pro 64-Bit Edition	22H2	2023-03
KC-PC07	技術部	Windows 10 Pro 64-Bit Edition	21H2	2023-03
KC-PC11	大阪支社	Windows 10 Pro 64-Bit Edition	21H2	2023-03
KC-PC1	未所属	Windows 10 Pro 64-Bit Edition	21H2	2022-09

さまざまなネットワーク環境に合わせた柔軟な分散配布

「マルチキャスト分散配布」・「ミラーマルチキャスト分散配布」の 2 種類の機能を利用し、更新時のネットワーク負荷を軽減します。



- 各クライアントが既にファイルを保持しているクライアントを探索します
- ダウンロードすべき配布対象を判定して、ファイルを取得します
- あらかじめ指定したミラー PC がファイルを取得します
- 各クライアントは自身のネットワークを探索して、近隣のミラー PC からファイルを取得します



- あらかじめ指定したミラー PC がファイルを取得します
- 各クライアントは自身のネットワークを探索して、近隣のミラー PC からファイルを取得します
- 移動先でも近隣を探索します
- ミラー PC が近隣に居ない場合はサーバーから取得して、マルチキャスト分散配布が行います（設定にて無効可）

ポイント

2つの手法は、拠点の環境に合わせて、混合運用が可能です。また、ミラーコンピューターはクライアント OS で動作が可能です。PC がインターネットに接続している必要もありません。

PC更新管理

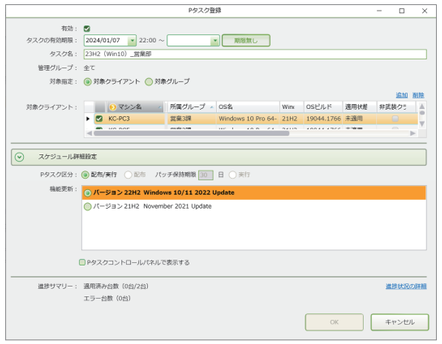
Windows
更新管理対応

「更新プログラムの自動ダウンロード」「実行コントロール」
「Microsoft365®・Office2019/2021」で
更新プログラムの配信・適用を支援。

Windows、Microsoft365®、Office2019/2021の定期的なアップデートの「更新プログラムの自動ダウンロード」を行うために運用作業を大幅に削減します。
「実行コントロール」を柔軟に設定することで、様々なシチュエーションに対応し、業務への影響を最小限に抑えます。

アップデート実行の即時コントロール

適用する更新プログラムは自動で取得し、どのプログラムを適用すべきか自動で判定します。
端末ごとに、どのようなタイミングで適用させるのかも、GUIの画面で簡単に設定が可能です。

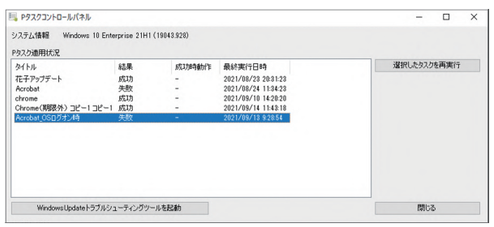


ポイント

適用中に端末をスリープに移行させない設定や、
Wi-Fi 接続時、VPN 接続時には適用をさせない設定なども可能です。

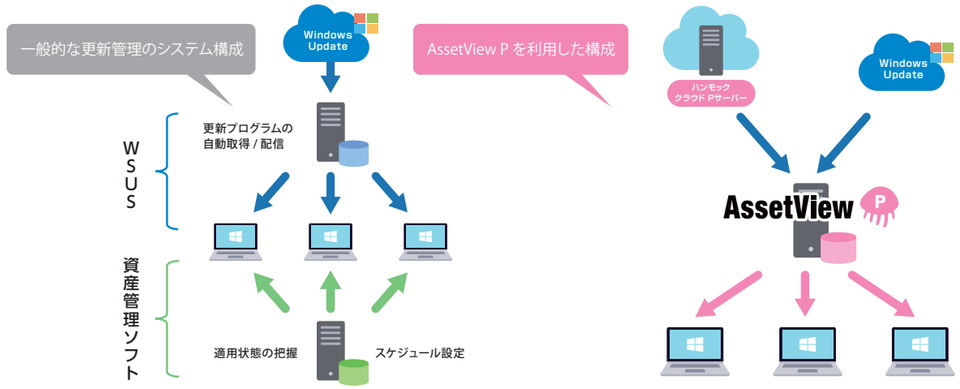
実行エラーの場合にはユーザー自身で課題解決が可能

端末側で失敗原因の究明や再アクションを実施でき素早く対応を進めることが可能です。
また、通常 Microsoft から提供されるトラブルシューティングツールは管理者権限での実行が必要になりますが、AssetViewでは、AssetView が権限を代行して実行しますので、ユーザー権限でログインしている環境下でもWindowsUpdate エラーの対策を打つことが可能です。



AssetView P
PC更新管理

WSUSとの違い



年2回の Future Update・毎月のQuality Update の配信を、負荷なく安全に行います。

対象プログラム

重要な更新 / 定義更新プログラム / Feature Packs / セキュリティ問題の修正プログラム/ Service Packs / 修正プログラム集 / 更新 / Upgrades / その他ベンダーパッチ / Microsoft 365、Office2019/2021

比較表

	WSUS	AssetView P
管理方法	△ プログラム(KB)の管理のため管理がしづらい	○ プログラム(KB)ではなく更新タスクの管理のため管理がしやすい
端末状況の可視化	△ どの端末にいつの機能更新(FU)が適用されているか一覧にできない	○ 機能更新(FU)の適用状態が一覧で表示されるため端末の状況が一目でわかる
実行スケジュール	△ おおよそのスケジュールは組めるが、具体的にいつ適用されるか分からないまたすぐには実行できない	○ 実行方法、時間、成功後の再起動まで詳細なスケジュール管理を行える今すぐ実行することも可能
ネットワーク負荷分散	△ 中継機をサーバー OSで用意する必要があるためコストがかかる	○ 中継機を既存のクライアントOSにて行えるので、コストを抑えて負荷分散が可能
実行エラーの対策	✕ できない	○ 管理者権限不要でWindowsUpdateトラブルシューティングツールの実行が可能
Microsoft 365、Office2019/2021の更新 ※1	✕ できない	○ 現在インストールされているバージョン情報の把握、更新プログラムの適用まで実現可能
サードパーティ製品パッチの管理	✕ できない	○ Adobe®・Autodesk®・Oracle®・Mozilla® Google®・JustSystems®のパッチも自動取得し、MSのパッチ同様、かんたん操作で適用できる
管理サーバー	△ IT資産管理ソフトとWSUSを別々のサーバーで管理する必要がある	○ サーバー 1台でWindows 更新業務の統合管理が可能
管理コンソール	△ IT資産管理ソフトとWSUSを別々の管理画面で管理する必要がある	○ 1つの管理コンソールでスムーズな管理が可能
問い合わせ窓口	△ IT資産管理ソフトとWSUSで別々の窓口に問い合わせが必要	○ 問い合わせ先を一本化できる
運用コスト	△ 複数のサーバーの維持管理費が必要	○ 単一サーバーの維持管理費のみ

※1：ClickToRun 型の Office2019/2021 のみが管理対象となります。

エンドポイントセキュリティ

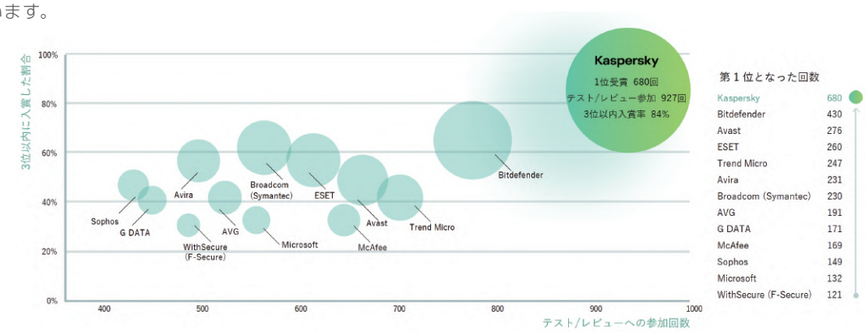
Powered by kaspersky

パターンファイルマッチングと振る舞い検知で既知、新種のマルウェアを防御

IPAの情報セキュリティ10大脅威で例年上位に入り、増加の一途をたどる「標的型攻撃」や「ランサムウェア」。
特定の企業・団体を狙い撃ちで攻撃してくるため、一見しただけでは不審なメールと気が付かないような、業務連絡や顧客とのやり取りを装ったメールが送られてくるのが特徴です。
またニューノーマルな働き方が広がり、社外での業務を行う際に、公衆Wi-Fiへの接続や、気の緩みから業務外のWEB閲覧によるマルウェア感染等きっかけは広がっています。どれだけセキュリティ教育を徹底しても、エンドポイントで最後の砦として既知、未知を問わずにマルウェア検知・駆除できるセキュリティ強化が重要です。

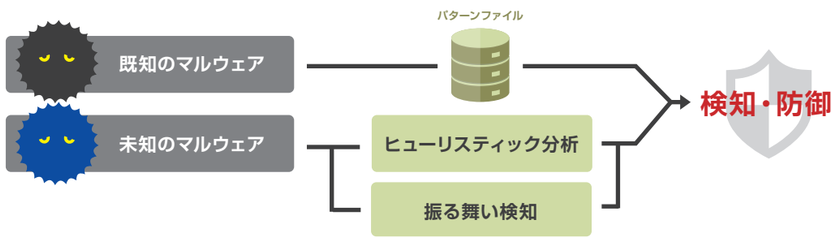
高精度なカスペルスキーエンジン採用

『AV-Comparatives』や『Virus Bulletin』など様々な評価機関から高評価を受けているカスペルスキー製品と同じエンジンをOEMで組み込んでいます。カスペルスキーは3年連続で「Gartner Peer Insights」エンドポイントプロテクションプラットフォーム部門において、「Customer's Choice」に選出されています。5点満点中4.6点という高い顧客満足度を獲得しています。



既知のマルウェアだけではなく、未知、亜種のマルウェアにも対応

パターンファイルマッチングだけでは防ぎきれない未知、亜種のマルウェアにもヒューリスティック分析と振る舞い検知で対応します。



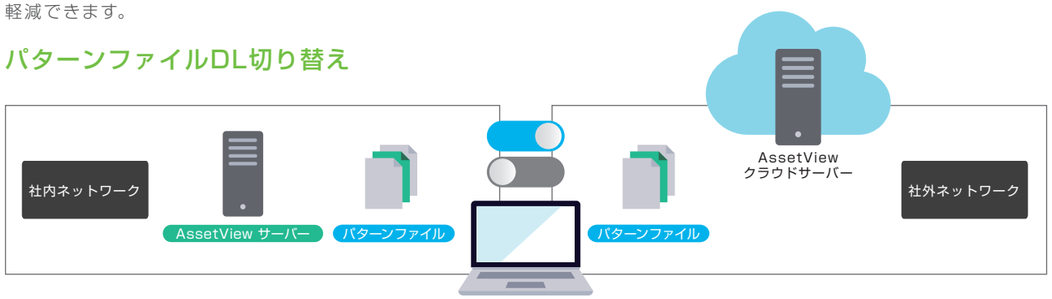
※ヒューリスティック分析とは：仮想的な環境（サンドボックス）で挙動を確認する
振る舞い検知とは：実際のプロセスの振る舞いから怪しい動きを検知する

AssetView Vplus エンドポイントセキュリティ

テレワーク、クラウド化時代への対応

パターンファイルの取得先を社内、社外で変更することが可能です。
テレワーク時はクラウドサーバーからパターンファイルをダウンロードすることで、パターンファイルの適用が遅れるリスクを軽減できます。

パターンファイルDL切り替え



over SSL、httpsなど暗号化通信が主流に

Vplus SSL 通信に対応したWeb モニター、メールモニターでクラウドサービス利用時の不審な動きも検知します。

統合管理による運用効率の向上

万が一の感染時にも感染経路の特定、原因究明、対策をワンストップで実現します。

AssetView M PC操作ログ管理
PC操作ログからマルウェア感染の前後にクライアント端末上でどういった操作が実施されていたのか確認できます。

AssetView P PC更新管理
脆弱性をついた攻撃を受けないためOS、ソフトのアップデートを支援します。

AssetView G デバイス制御
USBの利用制限をかけることでテレワーク時、私物のUSBからのマルウェア感染を防止します。

AssetView A IT資産管理
メッセージ配信やデスクトップへの付箋機能で注意喚起を行います。

AssetView K ファイル制御・暗号化
重要ファイルを暗号化しておくことで万が一のファイル流出時も情報漏洩を防ぎます。

Webフィルタリング

Powered by ALSI

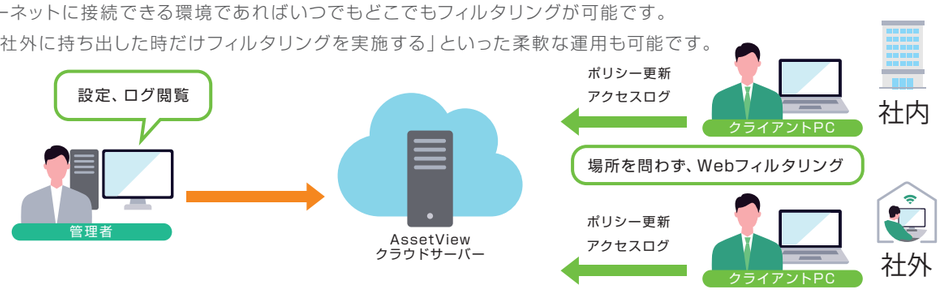
AssetView F Webフィルタリング

不正サイトへのアクセスを制御する。
高精度なフィルタリングを実現。

業務に欠かす事ができないインターネット利用。しかし、Webメールを使ったファイル持ち出しやSNS、ブログへの書き込み、フィッシングサイトへのアクセスを経由した不正アクセスなどインターネット利用には、さまざまな脅威と課題があります。
その対策のためには業務への影響を最小限にしながら、不正サイトへのアクセスまたは書き込み制御が有効です。
社内のPCだけでなく、在宅勤務や外出・出張先など社外への持ち出しPCの情報漏洩・ウイルス感染や私的利用も防止します。

管理外のネットワークに接続しているPCもフィルタリングが可能

インターネットに接続できる環境であればいつでもどこでもフィルタリングが可能です。
「PC を社外に持ち出した時だけフィルタリングを実施する」といった柔軟な運用も可能です。



高精度データベースによる安心の国産Webフィルタリング

国内主要携帯キャリア３社にも採用された高精度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。AssetView F は国産製品、日本の利用ニーズに応じたデータベース・カテゴリを保有しています。

Webフィルタリングデータベース

特長
- 豊富な経験を持つ専任リサーチャー 40 名による目視確認
- データベース収集後、90 日後に再度内容を確認し、修正・削除
- 社会情勢に応じた収集体制
- 独自のアルゴリズムにより、発生直後のサイトも迅速に収集

データベース登録数　79 億 8644 万コンテンツ

カテゴリ数　148（ユーザー設定：5）　（2024 年 4 月 1 日現在）

携帯電話事業者採用率100%、実績が証明するデータベース品質

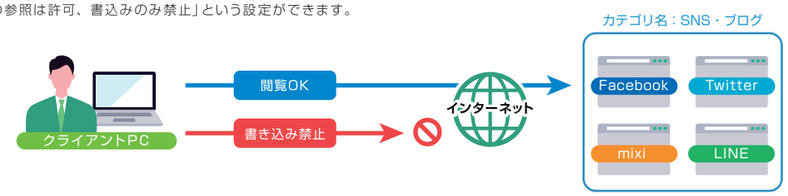
国内大手携帯キャリア３社が採用、実績が証明するデータベース品質
以下の携帯電話のフィルタリングサービスでも同社のデータベースが利用されています。

- 「キッズ i モードフィルタ」「i モードフィルタ」「あんしんウェブフィルター」（株式会社エヌ・ティ・ティ・ドコモ）
- 「安心アクセスサービス 特定カテゴリ制限コース」（KDDI 株式会社）
- 「ウェブ利用制限機能」「有害サイトアクセス制限サービス」「Web アクセス制限」（ソフトバンク株式会社）

ソーシャルメディアや掲示板への対策を実現

カテゴリごとに設定が可能なため、例えば SNS・ブログの閲覧は許可、書込みは禁止、という設定ができます。
HTTPS サイトであっても、対策が可能です。

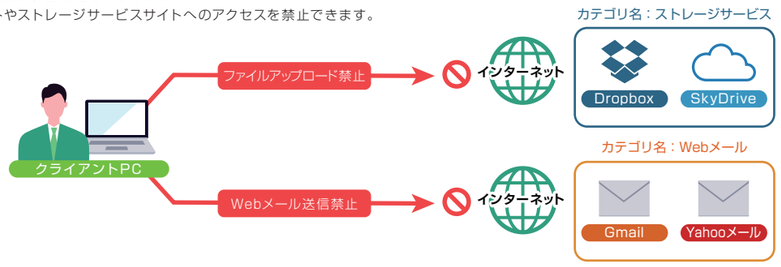
対象のカテゴリに書込み禁止設定をすることで
「SNS・ブログの参照は許可、書込みのみ禁止」という設定ができます。



Webメール・ストレージサービスを利用したファイル流出リスク対策を実現

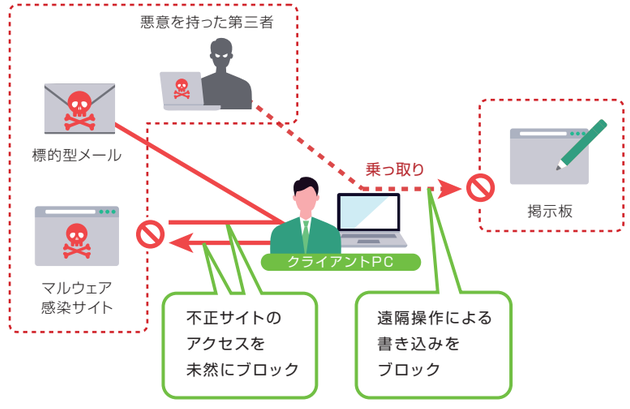
Web メールサイトやストレージサービスサイトへのアクセスを禁止することで、情報流出リスクの回避を実現できます。
HTTPS サイトであっても対策が可能です。

対象のカテゴリに閲覧禁止設定をすることで
Web メールサイトやストレージサービスサイトへのアクセスを禁止できます。



マルウェア対策の補助的な利用にも効果的

不正なプログラムが組み込まれたサイトにアクセスし、マルウェアに感染してしまうという被害が拡大しています。
これらのサイトは、無料でソフトウェアをダウンロードすることができるサイトや、スパムメールに記載された URL から誘引されてしまうケースもあり、マルウェア対策ソフトを導入していても、検知されない場合があるため、注意が必要です。
AssetView F の活用は不正サイトへのアクセスを未然にブロックするだけでなく、掲示板や SNS などのサイトへの書き込みもブロックできるため、マルウェア感染予防になります。



ファイル制御・暗号化

特許技術
特許番号
第6242019号

AssetView K
ファイル制御・暗号化

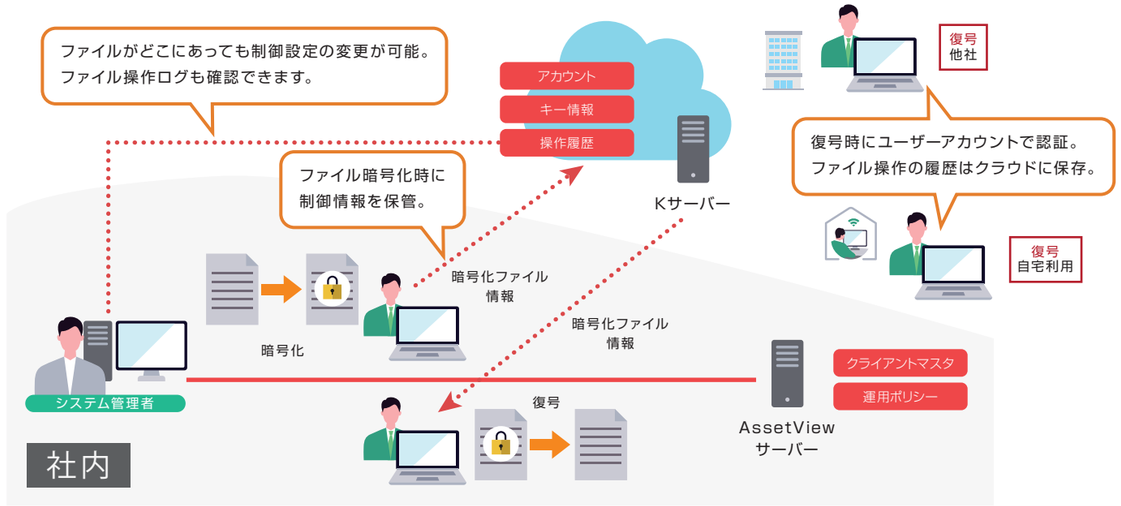
社内、社外問わず、どんな環境でも重要ファイルを暗号化し保護。社外にあるファイルでも証跡を追ったり、削除可能。

テレワークの定着により、従来の「境界型セキュリティ」が限界を迎える中、全てのネットワークを危険とみなし、
守るべき対象を「ネットワーク」から「アプリ」「端末」「データ」に変える「ゼロトラスト」が普及し始めています。
社内であっても、社外であっても、許可された人しかファイルの中の情報を閲覧できないようにする
ファイル暗号化を活用することでこれからの時代に即したセキュリティ対策を実現できます。

パスワード保護ではない暗号化

ファイルを守る	追跡する	削除する
ファイルを暗号化して制御	どこで開いても追跡	渡したファイルをあとから削除
制御内容 ・閲覧回数 / 閲覧の期限 ・保存禁止 ・印刷禁止 ・文字列や画像のコピー ・プリントスクリーン禁止	**アクセスログの確認** ・いつ？ ・どのファイルに？ ・誰が？ ・何をした？	**リモート制御** ・ファイルの消去 ・制御内容の変更 ・アクセス権限の変更

ファイルがどこにあっても許可された人のみが復号出来る仕組み

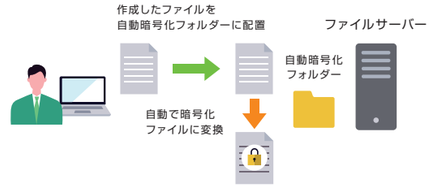


従業員の負担にならない暗号化

ファイル暗号化の運用を定着させるには、日々の業務の中で従業員の負担にならない暗号化の仕組みが必要不可欠です。
AssetView では3つの暗号化の手法をご提案いたします。

1、自動暗号化フォルダー

AssetViewが順次フォルダーを監視し、
中のファイルに対して暗号化を施します。
ファイルサーバーに自動暗号化フォルダーを配置し、通常通り
ファイルを配置すれば暗号ファイルに変換できるため、従業
員に暗号化処理を意識させず、負担なく運用が可能です。



2、重要ファイルの自動暗号化 + AssetView Iライセンス

AssetView I（個人情報検索）にて、個人情報、機密情報を
含むファイルを見つけ次第、自動で暗号化を施します。
従業員の作業負担なく重要ファイルを保護することが可能です。

3、デバイス書き出し時の自動暗号化 + AssetView Mライセンス

USBデバイスにファイルを書き出した際に
ファイルを自動で暗号化します。
社内では平文の状態で、社外に持ち出す際のセキュリティ保
護として暗号化するという運用の際に、負担なくご利用いた
だけます。

BitLockerドライブ暗号化状況の監視 共通

Windows OS に搭載のBitLocker ドライブ暗号化機能に
よるドライブ暗号化状況の監視を行います。

機能
・ドライブ暗号化状況取得
・ドライブ暗号化解除監視
・回復キー取得

暗号化されたファイルの操作ログ取得、制御設定変更

暗号化されたファイルに対してどのユーザーアカウントでどの
ような操作がされたのかログを確認できます。
また、手元にファイルが無くても、制御設定を変更することで、
ファイルの自動削除も可能です。

証跡管理

・いつ、誰が、どのファイルを操作したか
・権限のないアカウントでのアクセス
・パスワード入力ミス等のログインの失敗
・閲覧可能な残り回数
・閲覧回数を超えたことでのファイルの自動削除

ポイント
拡散したファイルまで
削除できる。

電子メール監視

さまざまな環境のメール送信ログ取得を実現。

企業や組織での電子メール利用は、現在なくてはならないものになっています。
利便性が高い反面、情報漏洩のリスク、私的利用による業務生産性の低下などの課題もでてきました。
電子メール監視を行うことを組織内で周知し、適切な責任者が万が一の有事の際や情報漏洩リスクがあった際に確認できる仕組みを構築しておくことで課題解決が可能です。

メール送信ログ

以下のメール送信情報を取得します。

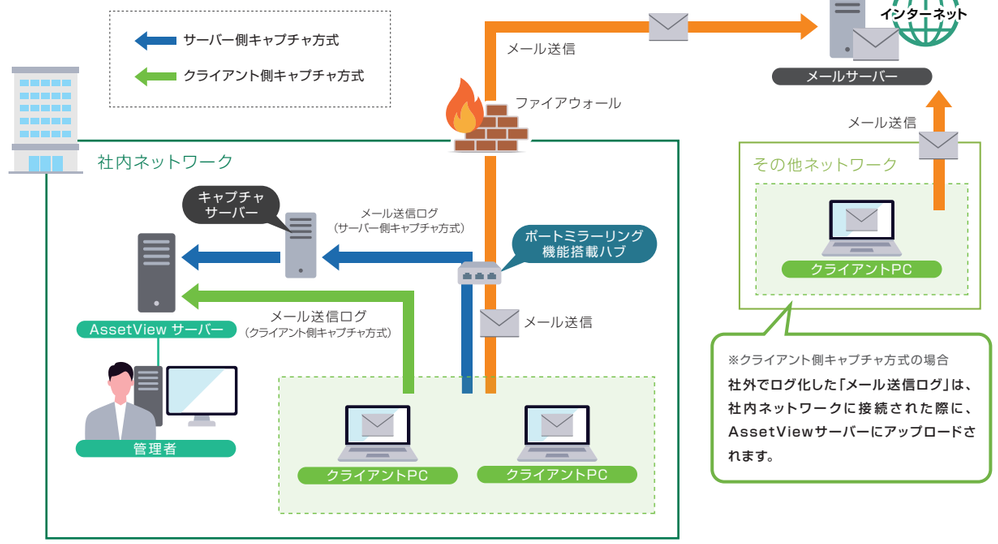
・件名	・送信日時	・送信先メールアドレス	・添付ファイル実体 ※1
・本文	・送信元メールアドレス	・添付ファイル名	

※取得可能な項目は、クライアント側キャプチャ方式、サーバー側キャプチャ方式共に共通です。
※1：クラウド版では取得対象外です。

取得方式を選んで運用が可能

クライアントPC上でログを取得するクライアント側キャプチャ方式と、サーバー上でログを取得するサーバー側キャプチャ方式の2種類からログする方式を選択することができます。

システム構成図



※サーバー側キャプチャ方式はオンプレミス版のみ対応しています。

AssetView Mail 電子メール監視

件名や本文をキーワードにログ検索、添付ファイルの中身も確認

AssetView M では取得対象外の「本文」「添付ファイル実体」が取得可能です。
操作履歴検索ウィンドウからPC操作ログとあわせてログを確認することで利用者の行動把握が容易に行えます。

操作履歴検索画面で表示

メール送信情報は操作履歴検索画面で表示できるので、AssetView M の機能と連携してメール送信前後のファイル操作やウィンドウタイトルの遷移を確認できます。

▼管理コンソール画面

ログ取得日時	ログオンユーザー	操作種別	プロセス名	アプリケーシ	操作対象のファイル名/ウィンド
2023/10/09 20:42	HAMMOCK	個人情報ファイル削除	OUTLOOK.EXE	Microsoft Office	2006年度_顧客名簿.xls
2023/10/09 20:42	HAMMOCK	個人情報ファイルごみ箱移動	Explorer.EXE	Windows Explo	2006年度_顧客名簿.xls
2023/10/09 20:42	HAMMOCK	個人情報ファイル削除	Explorer.EXE	Windows Explo	$RH65G93.xls
2023/10/09 20:42	HAMMOCK	ファイル削除	Explorer.EXE	Windows Explo	$IH65G93.xls
2023/10/09 20:42	HAMMOCK	ファイル削除	Explorer.EXE	Windows Explo	$IH65G93.xls
2023/10/09 20:43	HAMMOCK	メール送信			個人情報

さまざまな環境に対応（クライアント側キャプチャ方式）

クライアント側キャプチャ方式の場合、専用プラグインを追加することで、下記のメール送信ログを取得することができます。

■ Edge（Chromium）のアドイン
・OWA（Outlook Web App）

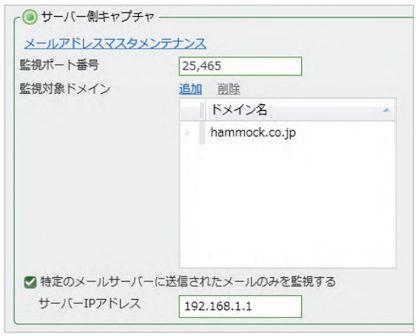
■ Becky! Internet Mail のプラグイン
・Becky! Internet Mail Ver.2.55 ～ Ver.2.70

■ Microsoft Outlook のアドイン
・Microsoft Outlook 2016
・Microsoft Outlook 2019
・Microsoft Outlook 2021
・Microsoft 365(Exchange Online）デスクトップ版

※OWAでのメール送信情報の取得は
Edge（Chromium）／Chrome／Firefoxのアドインで
対応しています。
※OWAではファイル名、添付ファイルのログは取得出来ません。

取得に関する詳細な設定が可能（サーバー側キャプチャ方式）

サーバー側キャプチャ方式の場合、取得に関するさまざまな機能や設定が利用できます。



※オンプレミス版のみ対応しています。

主な機能

監視対象ドメインによるメール送信ログ取得
設定されたドメインから送信されたメールをメール送信ログとして取得します。

特定のメールサーバーに送信されたログのみ取得
特定のメールサーバーに送信されたメール送信ログのみ取得します。

監視対象外とするメールアドレスの設定
設定したメールアドレスのメール送信ログを監視対象外と設定することができます。CSVファイルでのインポートによる一括登録も可能です。

スマートデバイス管理

スマートデバイスの安全かつ効率的なビジネス利用を支援。

民間企業、官公庁、教育現場まで普及しているスマートデバイスのセキュリティを強化します。
iOS、iPadOS、Windows、Android™ を一元的に管理できます。
Windowsはクローズドネットワーク（閉域網環境）内に管理サーバーを構築し管理することもできます。

スマートデバイス管理機能について

企業におけるモバイルデバイスの管理において従業員による私的利用をさせず、セキュリティ基準やコンプライアンスに準拠した利用をさせることが重要です。

対象OS

iOS/iPadOS（ADE）
※前提条件：ABM アカウント取得
管理デバイスが ADE 対応

Android
※前提条件：Android EMM 対応
管理デバイスがEMM 対応デバイスリスト

Windows
※前提条件：MDMv4 専用エージェントの
インストールが必要

※ADE（Automated Device Enrollment）：Apple が提供する企業向け iOS/iPadOS 端末導入支援サービスです。

できること

・デバイスのキッティング、アプリ/ポリシーの適用を簡略化
・紛失時の位置情報取得や遠隔でのワイプ　・ポリシーの適用による私的利用の制限

※ワイプの定義は、OS により異なります。

iOS、iPadOSの管理

ABM（ASM）に対応した IOS、iPadOS を以下の流れで管理いただけます。

1、デバイスのキッティングの簡略化（ADE（旧：DEP））
2、業務アプリの配信（旧：VPP）
3、プロファイルの適用（ポリシーの作成と適用）
4、端末情報の取得、位置情報の取得
5、紛失時のリモートロック、リモートワイプ

ポイント

私的利用制限のために、各種機能（設定・アプリ）に対して利用制限をかけることが可能です。
また、一括で Wi-Fi、VPN の接続設定、メール設定やメッセージ配信など、
便利にご利用いただけます。教育現場では、ホーム画面のレイアウトを変更できたり、
授業で用いるWEB サイトをホーム画面上に表示させるといった運用も可能です。

AssetView MDM スマートデバイス管理

Android™の管理

Android Enterprise の機能により Android デバイスを管理します。

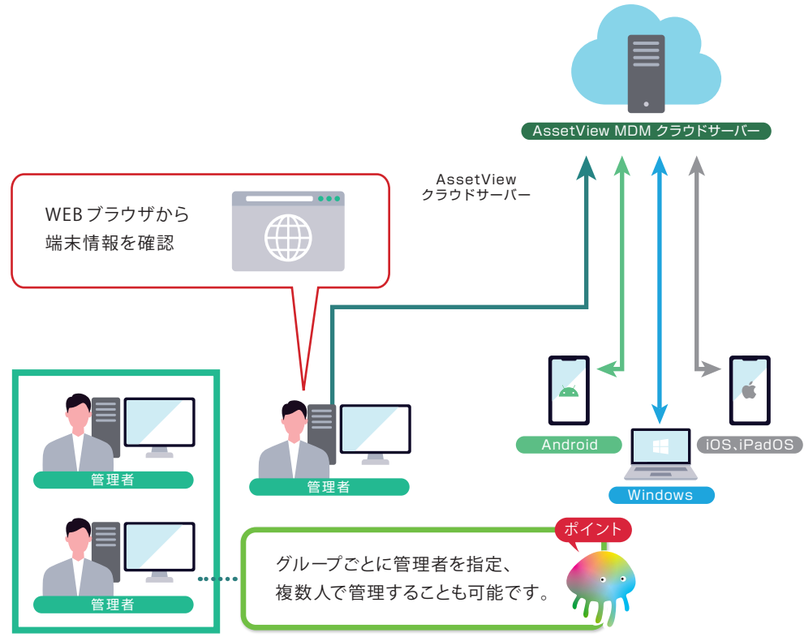
1、デバイスのキッティング簡略化
2、業務利用に限定した managed Google Play の構成と
　オリジナルアプリケーションの配布
3、端末情報の取得、位置情報の取得
4、紛失時のリモートロック、リモートワイプ

ポイント

デバイス初期設定時には2次元バーコードを読み取らせることで簡潔にキッティングを行えます。
ポリシーを適用することにより、ユーザーによって設定が変更されたり、アプリをインストールおよび
アンインストールされることを防ぎます。

SaaSでのご提供

サーバーレスで簡単に始められます。



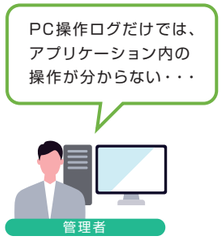
画面操作録画

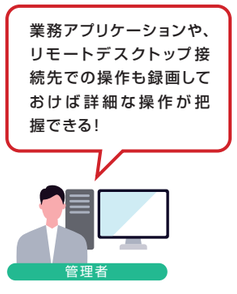
利用者のPC操作を録画して保存。
PC操作ログだけでは分からない
アプリケーション内の操作まで把握可能。

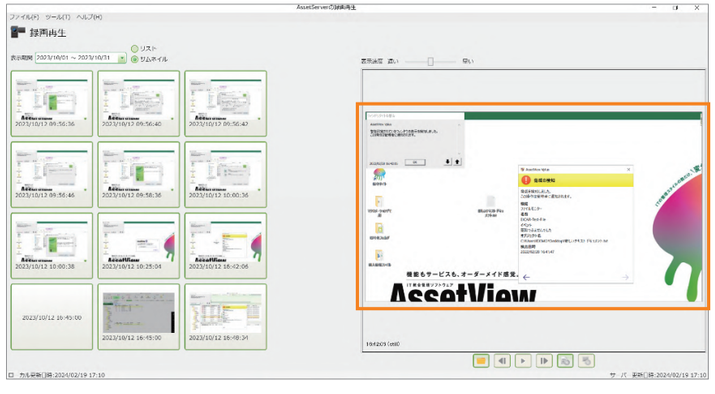
PC操作ログ管理ソフトは、個々のアプリケーション内の利用者の操作まではログとして取得することができず
不正な操作を検知しても詳細の把握は難しいことが課題でした。
AssetView では操作ログと画面操作録画の両方のログによって、誰が、いつ、どのようなアプリケーションを起動して
「どのような操作をアプリケーション内でおこなったか？」ということまで監視が可能です。

利用者のPC操作を録画、実際の操作を再生して確認

ウィンドウタイトルだけでは分からないアプリケーション内の操作 (入力、変更、削除、設定変更等) も、録画することで確実に証跡を残します。録画したデータは、管理コンソールのインストール有無に関わらず、再生することが出来ます。
管理コンソールがインストールされていない端末で再生する場合は AVI 形式での再生方法に加えて、MP4 形式で録画データを出力することで長時間の録画データの確認ができます。



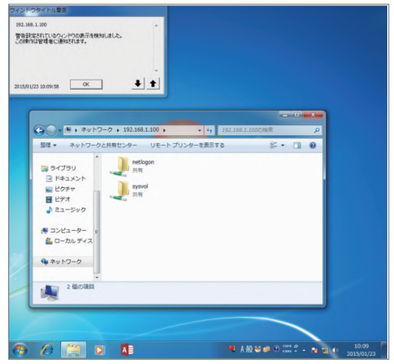




AssetView REC
画面操作録画

利用者が不正操作を行った際にスクリーンショットを取得

ウィンドウタイトルにアラート対象となるキーワードが含まれていた場合だけ、利用者のデスクトップのスクリーンショットを取得します。



アラートをきっかけに
スクリーンショットを取得
・ウィンドウタイトルアラート

＋ AssetView M PC操作ログ管理

※AssetView や、OS、アプリケーションで表示されるウィンドウタイトル名を登録しておくことでさまざまなタイミングでスクリーンショットを取得します。

スケジュール録画

録画のスケジュール化により常時監視が可能です。
クライアント PC ごとに毎月、毎週、毎日、指定した時間の録画ができます。
監視が必要な PC だけ常時録画する、といった運用が可能です。

ポイント

録画データを最小限のサイズで保管できます。
・運用を考慮したデータ量を抑えた録画
・重要な箇所だけの録画を可能にした『タイムシフト録画』
従来型の画面操作録画機能と比べて、
動画の記録に必要なディスク容量を大幅に削減できます。

1 時間録画した場合の
録画データのサイズの目安

画質	サイズ（目安）
4bit モノクロ (4色)	17MB
8bit モノクロ (256色)	26MB
3bit カラー (8色)	7MB
6bit カラー (64色)	14MB
15bit カラー (32768色)	45MB

タイムシフト録画

不正操作を検知したら、過去にさかのぼって録画データを保管。不正操作が起きる直前の操作や行動が把握できます。

高速ログ検索/長期保存

AssetView アーカイブ
高速ログ検索/長期保存

長期間保存された大容量ログデータから目的の情報をすばやく入手。

万が一の情報漏洩時の事後調査、内部統制やコンプライアンスへの対応が求められる昨今、
PC操作ログ管理、電子メール送信ログの長期保存が求められています。
AssetView アーカイブ は、非常に大きなデータになる傾向のあるログを数年に渡って保存し、大容量データの高速検索を実現します。

AssetView アーカイブ 3つのメリット

AssetView 製品ログの高速検索、長期保存が可能

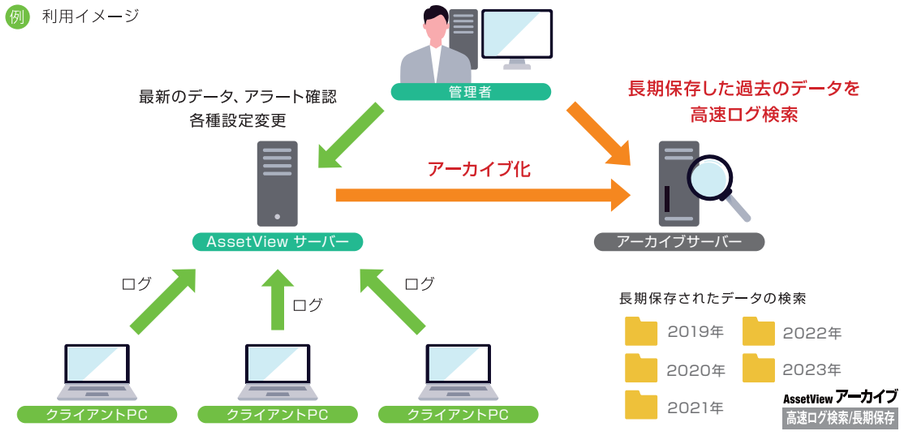
データの取り扱いがかんたん

ログのインデックス化によりアーカイブしたデータは日付単位でフォルダーで管理します。
バックアップ、復元、移動などデータの取り扱いが非常にかんたんに行えます。

シンプルなシステム構成

独自のインデックス方式により SQL Server は不要。
専用プログラムをインストールすることでアーカイブしたデータの閲覧が可能です。

例 利用イメージ



対象製品	アーカイブ項目
AssetView M PC操作ログ管理	ウィンドウタイトル、クリップボード操作、ファイル操作、メール添付、印刷、メール送信、Web フォーム送信、GoogleWorkspace 操作、Web アクセス禁止、アラートプロセスの起動警告 / 禁止、停止監視プロセスの停止、使用禁止デバイスの接続、ドライブの追加 / 削除、ウイルス対策結果、ログオン / ログオフ / スリープ / シャットダウン、特定操作抑止機能、Windows ファイアウォールでの接続禁止、Wi-Fi 接続ログ、Bluetooth ログ
AssetView Mail 電子メール監視	送信日時、件名、本文、送信元メールアドレス、送信先メールアドレス

レポート

データ活用レポート　有償

データを自動で加工・出力し、すばやく可視化・分析！

✓ 作業時間の削減

AssetViewでデータ収集

ファイル操作　デバイス利用
ログオンログオフ　メール送付
アプリケーション利用 etc...

✓ 迅速な異常検知、意思決定

多種多様な業務システムと連携

用途に応じてデータを
加工出力し可視化・分析

✓ ノウハウ属人化の解消

多角的に業務実態を把握

意思決定　異常検知
レポートの自動化　時間の削減

ポイント

用途別にレポーティングされ、あらゆるシステムと連携ができるので、データ活用業務が楽になります！

AssetView で取得したデータを活用する目的（例）

勤怠管理

パソコンの利用実態の確認
働き方改革の実現をサポート

必要なデータ

・PC ログオン、ログアウト ・PC 平均稼働時間
・WEB 閲覧履歴 ・アプリケーション操作履歴

内部不正対策

不正操作による情報漏洩の予防
インシデント発生時の迅速な対応

必要なデータ

・デバイス使用状況 ・デバイス使用履歴
・ファイル操作履歴 ・印刷履歴
・メール送信履歴 ・WEB フォーム送信履歴

脆弱性対策

情報漏洩に繋がる
危険なソフトウェア利用を可視化

必要なデータ

・アプリケーション利用状況
・アプリケーション操作履歴

自動レポート　無償

AssetView は csv で出力可能な以下のデータを標準機能で提供しています。

・アラート集計
・USB デバイスリスト
・ライセンス管理リスト
・パソコンの起動・終了状況の可視化レポート
・ハードウェアカスタマイズ状況可視化レポート
・業務外ソフトウェア可視化レポート
・不正サイト閲覧状況の可視化レポート
・外部記憶媒体利用状況の可視化レポート
・企業標準ソフトウェア普及状況／企業標準ソフトウェア以外のインストール状況の可視化レポート
・外部記憶媒体紛失／盗難リスク可視化レポート

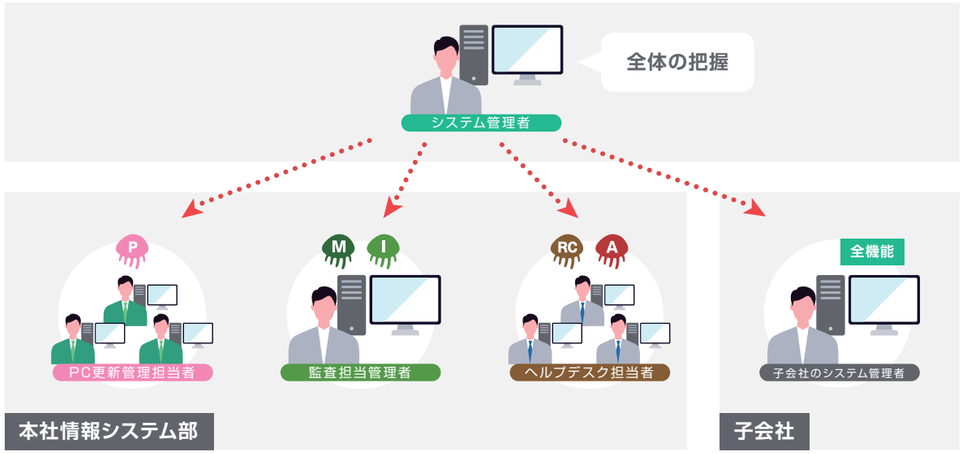
※オンプレミス版のみ対応しております。

多様化する環境や 運用に対応

権限委譲で分散管理

運用に合わせた柔軟な設定が可能

利用できる機能、対応グループ、アクセス権を限定して権限の分散ができます。
全社的な管理者の他に、拠点や部署ごとの管理者に運用の一部を任せたいという場合には、その機能と関連する情報だけを表示させ、見せたくない情報を非表示にできます。これにより、管理者の負担を適切に分散させることができます。



グローバル対応

英語・中国語（簡体）での運用が可能

■ 管理コンソール

対応製品 A D RC S M I G

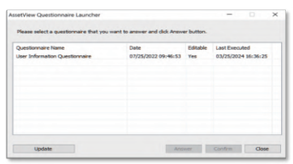
管理コンソールの表示と管理者宛ての
各種通知メールの言語を選択できるので、
海外拠点の外国の方による管理を実現します。

対応製品 M G

クライアント PC の言語設定に合わせて、
警告メッセージを変更可能

■ クライアント

▼アンケートランチャー



▼警告メッセージ

対応製品 A D M G

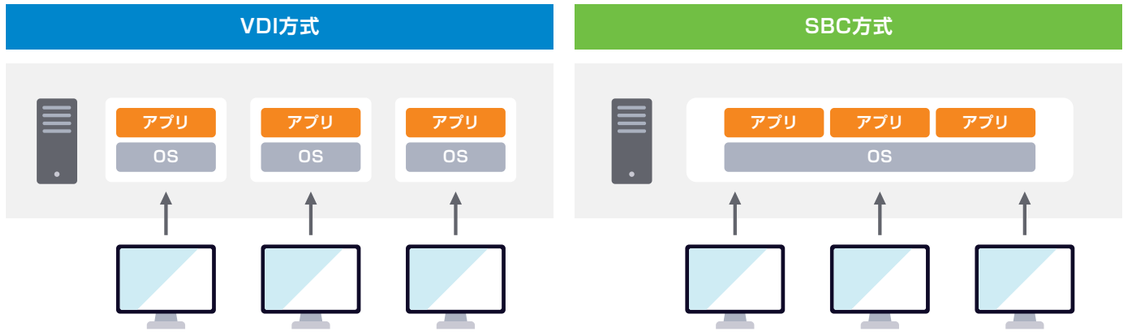
- 警告メッセージ
- アンケートランチャー
- タスクランチャー
- USB デバイス申請ツール
- デバイス制御申請ツール
- ライセンス申請ツール
- デスクトップの付箋表示

クライアント PC の言語設定に合わせて、各種機能で表示する言語が日本語・英語・中国語（簡体）のいずれかに切り替わります。

シンクライアント対応

さまざまな方式が存在する新クラインアント PC の管理が可能

働き方の多様化により、より利用が促進したシンクライアントシステム。
AssetView ではさまざまなシンクライアント環境に対応しています。



VMware や Hyper-V、AVD などに対応しています。
クライアントモジュールをインストールし、管理対象としたい仮想マシンの数分通常ライセンスが必要となります。

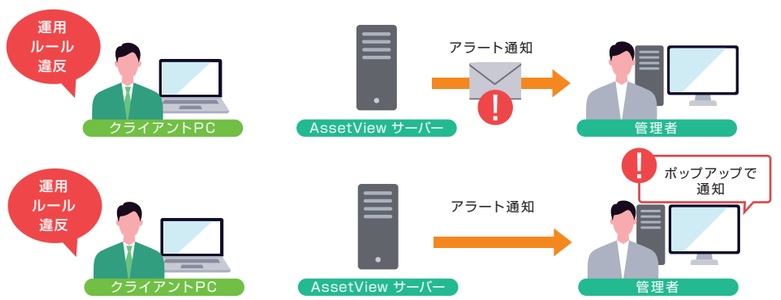
RDS、RDSH、公開アプリケーション方式に対応しています。
最大同時接続する端末数分の SBC ライセンスが必要になります。

※接続方式によって利用できる機能が異なります。詳細はお問い合わせください。

アラート通知

設定された運用ルールに違反する動きがあった際に、アラートとして管理者に通知

予め指定された管理者へメールでの通知や端末上のポップアップでの表示により、管理コンソールにログインすることなくアラートに気づくことが可能です。



ポイント

利用機能に応じて多様なルール設定が可能

重要情報ファイル操作・使用禁止デバイス接続・閲覧警告・禁止ウィンドウオープン・起動警告・禁止プロセス・不正機器のネットワーク接続・重要情報保持・ソフトウェアライセンス不足　など

充実したサポート

保守サービス内容

ライセンス保守契約、サービス利用契約の中で以下をご利用いただけます。

製品サポート対応（ヘルプデスク）

技術的なご質問は、Web/ メール /TEL にて
お受けいたします。

保守ユーザー様専用サイトのご利用

よくあるご質問やトラブルシューティングなどの技術情報を
ご提供いたします。最新モジュールもこちらからご提供して
おります。

バージョンアップモジュール提供

機能強化や修正等の最新のモジュールと手順書を
ご提供いたします。

最新情報のメール配信「AssetView Express」

製品のアップデートやメンテナンス、その他緊急性が高い
情報などをメール配信にてご案内いたします。

AssetViewをご利用いただくために

「せっかく導入したけれど使いこなせない、他の会社はどう使っているのか？」など
導入時のから運用開始後の不安解消や製品活用を弊社カスタマーサクセス部がご支援しております。
保守サービス以外での種々のサービス、コンテンツをご用意しておりますので、お気軽にご利用ください。

詳細はこちら
https://bit.ly/3JcNiKp

AssetView 活用セミナー（無償）

初めて AssetView を使い始める、機能別の利用方法など、
日々の製品活用のヒントをご提供いたします。

詳細はこちら
https://bit.ly/3yrmQ0V

技術支援メニュー（有償）

導入時のサーバー構築や、機能別の設定や操作など
弊社の技術者がお伺いしてご支援いたします。

多くのお客様・さまざまな用途でご利用いただいています

https://goo.gl/vafyF9

製造業

オンプレミス

Panasonic

パナソニックグループの
DLP対策を担う、AssetView
※DLP（Data Loss Prevention/情報漏洩防止）

内部不正対策

詳細はこちら ➡ https://bit.ly/48TqQ4q

オンプレミス

AGC
Your Dreams, Our Challenge

PCにインストールされたアプリケーションの
効率的な把握・配布を実現

IT資産管理の効率化

詳細はこちら ➡ https://bit.ly/3FgJKoo

サービス

クラウド

NIPPON Rent-A-Car

「統合管理」「クラウド化」により、
システム運用の業務効率が大幅に向上

WindowsUpdate含めた統合管理

詳細はこちら ➡ https://bit.ly/3S0hvSD

金融

クラウド

日本カストディ銀行
Custody Bank of Japan

テレワーク時、持ち出し端末の管理に
「AssetView CLOUD」を導入

テレワーク端末のセキュリティ対策

詳細はこちら ➡ https://bit.ly/3PVrIIT

人材

クラウド

Japan Create Group
株式会社ジャパンクリエイトグループ

変化するIT環境で求められるセキュリティ要件に
対応し、レジリエンス向上を支援

テレワーク端末のセキュリティ対策

詳細はこちら ➡ https://bit.ly/3M79lE3

小売

オンプレミス

Keio

20年間の継続利用
百貨店の情報インフラを支える AssetView

パッチ自動化

詳細はこちら ➡ https://bit.ly/46xqoqY

不動産

クラウド

小田急不動産
odakyu

オンプレミス型のセキュリティ対策をクラウドシフト
働く場所を問わず、効率的なIT資産管理が可能に

情報漏洩対策

詳細はこちら ➡ https://bit.ly/3tyVy2G

医療

クラウド

富士薬品

IT資産や業務の可視化、傾向分析から業務生産性向上への
新たなチャレンジを推進するプロジェクトがスタート

テレワーク端末のセキュリティ対策

詳細はこちら ➡ https://bit.ly/4aH61cs

教育

オンプレミス

拓殖大学
Takushoku University

学内のIT資産を守ることで、大学の信頼を守る
名門国際大学のIT統制、資産管理業務の効率化に貢献

情報漏洩対策

詳細はこちら ➡ https://bit.ly/3PVuORG

官公庁

オンプレミス

山形市役所

IT資産の最適化、業務効率の向上に貢献
山形市役所が製品指定で導入した AssetView

情報漏洩対策

詳細はこちら ➡ https://bit.ly/3RX6MrR

AssetView 機能詳細一覧表

ライセンス	機能名	説明
すべてのライセンス 共通	基本インベントリ情報の取得	クライアントPCから、OSとネットワークに関連する基本的な情報を取得します。 ・マシン名　・IPアドレス　・MACアドレス　・サブネットマスク　・ドメイン/ワークグループ名　・Active Directory ドメイン名　・ログオンユーザー名 ・ログオンユーザーフルネーム　・OS名　・OSサービスパック　・OS種別　・OSバージョン　・OSビルド番号　・OSプロダクトID　・タイムゾーン ・地域と言語（システムロケール）　・AssetView クライアントバージョン
	アンケートによるユーザー情報取得 mac	クライアントPCから、アンケートにより以下の情報収集を行います。 ・所属部署　・氏名　・氏名(ふりがな)　・メールアドレス
	クライアントPCで、アンケートを選択して実行する（アンケートランチャー）	クライアントPCのスタートメニューに登録されている[アンケートランチャー]で、自身を対象に登録されているアンケートを選択して、任意のタイミングで実行することができます。
	メッセージ配信	指定したスケジュールで、クライアントPCに任意のメッセージを表示します。
	電源管理機能	クライアントPCの電源オプションの設定を変更することができます。
	スクリーンセーバー管理機能	クライアントPCのスクリーンセーバーの設定を変更することができます。
	スタートメニュー登録有無の選択	AssetView クライアントインストール時に、スタートメニュー、プログラムの追加と削除への登録有無を選択することができます。 クライアントPCを使用しているユーザーに、AssetView がインストールされていることを意識させない運用が可能です。
	クライアントアンインストールパスワード	アンインストール時にパスワードを要求することで、ユーザーが故意に AssetView クライアントをアンインストールすることを防止します。
	ハードウェアの手動追加	AssetView クライアント以外のハードウェアを、手動で登録して管理することができます。
	ハードウェア情報のインポート	CSVファイルからハードウェア情報をインポートして、AssetView クライアント以外のハードウェアの一括登録、ユーザー追加列の一括編集、所属グループの変更を行うことができます。
	管理アカウントの登録	管理コンソールにログオンするアカウントを複数登録することができます。各管理者に適切な権限を設定することで、円滑な管理を行うことができます。
	管理アカウントの権限設定	管理アカウントごとに、権限と管理対象とするグループを設定することができます。
	管理アカウントの個別機能設定	管理アカウントごとに、管理コンソールで有効にする機能を個別設定することができます。
	グループの自動振り分け	アンケートの回答結果と、インベントリ情報の値を条件として、クライアントPCの所属グループを自動的に振り分けることができます。
	Active Directory の組織単位（OU）をグループ情報にインポートする	Active Directoryの組織単位（OU）を、所属グループにインポートすることができます。 組織単位（OU）と同名のグループにクライアントPCを移動することも可能です。
	Active Directory からのユーザー情報取得	Active Directory から、クライアントPCにログオンしているドメイン ユーザーの情報をインポートすることができます。 ・表示名　・電子メール　・部署　・役職　・上司　・事業所　・電話番号　・Webページ　・携帯電話　・IP電話　・組織名
	グループの表示順変更	グループツリーで同じ階層に表示されるグループの並び順を、任意に変更することができます。
	任意の列追加（ユーザー追加列）	ハードウェアのインベントリ情報として任意の列（ユーザー追加列）を追加することができます。
	カスタムビュー	管理者ごとに、任意の条件でハードウェアの情報をカテゴリ分けして表示するビューを作成することができます。
	リモートインストーラー	管理コンソールから、ネットワーク上のPCに対して AssetView クライアントのリモートインストールを行うことができます。 インストール対象のPCを、CSVファイルで指定することも可能です。
	帯域調整	AssetView クライアントと、アプリケーションサーバー間の通信速度を調整することができます。
	クライアントPCの自動削除	指定期間更新のないクライアントPCを、自動的にマスター情報から削除することができます。
	AssetView クライアントの自動更新	各クライアントPCにインストールされている AssetView クライアントを、自動的に最新バージョンに更新することができます。
	分散配布（マルチキャスト配信）	クライアントPC同士で配布対象ファイルを共有することで、拠点間のネットワーク負荷を軽減します。 ・ファイル配布タスクのキャッシュデータ管理　・各クライアントPCの分散配布機能動作状況の取得　・レジューム機能による通信再開 ・通信速度の制御　・ハッシュ値による整合性チェック　・スリープ抑止　・ミラーコンピューター（ユニキャスト）
	自動レポート	ログデータを自動的に集計し、管理者にメール通知する機能です。 ・アラート集計　・ライセンス管理リスト（A）・USBデバイスリスト（G）・パソコンの起動　・終了状況の可視化レポート(M) ・時間外就労状況統計レポート(M)　・ハードウェアカスタマイズ状況可視化レポート(A)　・ハードウェアカスタマイズ状況統計レポート(A) ・業務外ソフトウェアの可視化レポート(M)　・業務外ソフトウェアの統計レポート(M)　・業務外ソフトウェアの起動ランキング(M) ・企業標準ソフトウェア普及状況／企業標準ソフトウェア以外のインストール状況の可視化レポート(A) ・企業標準ソフトウェア(外)インストール状況統計レポート(A)　・不正サイト閲覧状況の可視化レポート(M) ・不正サイト閲覧状況統計レポート(M)　・不正サイト閲覧状況統計ランキング(M)　・外部記憶媒体利用状況の可視化レポート(G/M) ・外部記憶媒体利用状況統計レポート(G/M)　・外部記憶媒体紛失／盗難リスク可視化レポート(I/M) ・外部記憶媒体紛失／盗難リスク統計レポート(I/M)　・外部記憶媒体紛失／盗難リスクランキング(I/M)
	アラートメール	アラートログを出力したクライアントPCの情報を、管理者にメール通知します。
	通知アプリ（アラートクライアント）	アラート通知をメールで受け取るのではなく、特定の端末にポップアップで表示します。
	WOLでOS起動コマンドを送信する	Wake On LAN に対応したPCに対して、管理コンソールから電源を起動するコマンドを送信します。
	vPro でコマンドを送信する	インテル vPro テクノロジーに対応したPCに対して、管理コンソールからコマンドを送信します。　・電源ON　・電源OFF　・再起動
	vPro KVM（キーボード/ビデオ/マウス）リモート コントロール機能のオン/オフ	インテル vPro テクノロジーに対応したPCに対して、管理コンソールからKVMリダイレクションの有効/無効を制御します。
	スタンドアロンPCからのログデータ収集/運用ポリシー反映（スタンドアロン対応ツール）	サーバーにネットワーク接続できないクライアントPCであっても、USBメモリなどを経由してログデータの収集と運用ポリシーの反映を行うことができます。
	データベースのバックアップ	設定したスケジュールに従って、データベースを自動的にバックアップします。
	バックアップデータの閲覧	バックアップデータを『閲覧用データベース』に指定することで、現在の運用データに影響を与えることなくバックアップデータを閲覧することができます。
	バックアップデータのリストア	リストアツールを使用することで、データベース破損の場合に運用データベースをバックアップ時点まで復旧することができます。
	運用ポリシー/システム設定のエクスポート	現在データベースに登録されている、運用ポリシーとシステム設定の情報をエクスポートします。 運用データベースに問題が発生した場合、このデータをインポートすることで復旧することができます。
	サーバー稼働状況報告	AssetView のデータベース、アプリケーションサーバーのディスク使用量、クライアント数等の情報をシステム管理者にメールで通知します。
	サーバーディスク容量警告	AssetView のデータベースサーバー、アプリケーションサーバーのディスク使用量が、しきい値を下回ると、システム管理者にメールで通知します。
	ナビゲーション	組織全体に適用するセキュリティとコンプライアンスのレベルに応じて、関連する運用ポリシーの設定を最適化します。
	管理コンソール操作履歴	AssetView の管理コンソールで、誰が、いつ、どのような操作を行ったかを検索することができます。
	IPアドレス管理	マスター情報に登録されているハードウェアに対して、IPアドレスの割当管理を行うことができます。
	フィルター	管理コンソールに表示されているログデータの、任意の値を含む行だけをフィルター表示することができます。
	CSVファイルへのエクスポート	現在管理コンソールに表示されているログデータを、CSVファイルにエクスポートすることができます。
	管理コンソール表示履歴	管理コンソールの画面表示の履歴から、「戻る」、「進む」などの操作で画面遷移することができます。
	管理コンソールの文字列コピー	管理コンソールに表示しているログデータ等の文字列を、コピーすることができます。
	L2Blocker連携	L2Blockerが保持するハードウェア情報、検知ログ、アラート情報、制御設定をAssetViewに連携し、ログの閲覧、制御設定の変更を行うことができます。
	ハードウェアID重複検知	AssetViewが使用する個体識別番号である『ハードウェアID』の重複を検知します。 ※設定により、重複した端末それぞれに新規ハードウェアIDを自動的に割り当てることもできます。
	ボリューム暗号化の監視	Windows BitLocker ドライブ暗号化によるドライブ暗号化状況を監視します。
	ServiceNow連携	ServiceNow連携ツールの利用により、ハードウェアとアプリケーションの情報をServiceNowに同期できます。

ライセンス	機能名	説明
AssetView A （IT資産管理） A	ハードウェア情報の取得	クライアントPCから、ハードウェアに関連するインベントリ情報を取得します。 ・ベンダー名　・モデル名　・BIOS バージョン　・BIOS シリアル 番号　・キーボード種別　・メモリ容量　・ハードウェア情報取得時の空きメモリ ・ハードウェア情報取得時の 仮想メモリ　・システムドライブ 容量　・システムドライブ空き領域　・Windows フォルダー　・PCの説明 ・ディスプレイデバイス名　・MDAC バージョン　・Outlook Express バージョン　・Windows Media Player バージョン　・Direct Xバージョン ・.Net Frameworkバージョン　・画面の解像度　・ICCID　・電話番号
	ドライブ情報の取得 mac	ハードウェア情報として、クライアントPCのドライブごとに以下の情報を取得します。 ・ローカルディスクドライブの、空き容量/ディスク容量　・ネットワークドライブの接続先共有フォルダーのUNCパス ・ドライブの種別（FD/SD、CD/DVD、リムーバブル、Secure Drive）
	CPU情報の取得	ハードウェア情報として、クライアントPCのCPUから以下の情報を、最大32CPU分取得します。 ・ベンダー名　・モデル名　・クロック数
	プリンター情報の取得 mac	ハードウェア情報として、クライアントPCに登録されているプリンタードライバーから以下の情報を、最大20件分取得します。 ・プリンターの名前　・プリンターのポート番号
	NIC情報の取得 mac	ハードウェア情報として、クライアントPCのNICごとに設定されている以下の情報を、最大10件分取得します。 ・デバイス名　・MACアドレス　・DHCP設定　・IPアドレス　・サブネットマスク　・デフォルトゲートウェイ　・優先DNSサーバー ・代替DNSサーバー　・優先WINSサーバー　・代替WINSサーバー
	任意のINIファイルの値の取得	任意のINIファイルの値を、ハードウェア情報の取得対象に追加します。
	任意のレジストリの値の取得	任意のレジストリの値を、ハードウェア情報の取得対象に追加します。
	任意のアンケートによる情報取得	クライアントPCから、任意のアンケートによる情報収集を行います。
	アンケートの回答結果表示	クライアントPCから収集したアンケートの回答結果を、表示対象列に追加することができます。
	アンケートの回答結果コピー	クライアントPCから収集したアンケートの回答結果を、ユーザー追加列にコピーすることができます。
	デスクトップの付箋表示	クライアントPCのデスクトップにハードウェア情報または任意の文字列を表示します。
	プログラムの追加と削除からの情報取得 mac	クライアントPCの『プログラムの追加と削除』に登録されているアプリケーションの、以下の情報を収集します。 ・アプリケーション名　・インストール日付　・バージョン　・会社名
	Microsoft Office の情報取得	クライアントPCにインストールされている Microsoft Office の、以下の情報を収集します。 ・アプリケーション名　・インストール日付　・サービスパック　・製品バージョン　・プロダクトID　・インストールパス　・GUID
	Adobe社アプリケーションの情報取得 mac	クライアントPCにインストールされている、以下のアプリケーションの情報を収集します。 ・Adobe Reader（Adobe Acrobat Reader）　・Adobe Acrobat　・Adobe Illustrator　・Adobe Photoshop　・Adobe Creative Suite 各アプリケーションからは、以下の情報を取得します。 ・アプリケーション名　・インストール日付　・製品バージョン　・プロダクトID　・インストールパス
	JustSystems社アプリケーションの情報取得	クライアントPCにインストールされている、以下のアプリケーションの情報を収集します。 ・一太郎　・花子 各アプリケーションからは、以下の情報を取得します。 ・アプリケーション名　・製品バージョン　・プロダクトID　・インストールパス
	Autodesk社アプリケーションの情報取得	クライアントPCにインストールされている、以下のアプリケーションの情報を収集します。 ・AutoCAD　・AutoCAD Electrical　・AutoCAD Mechanical　・AutoCAD Civil　・AutoCAD LT　・AutoCAD MAP 3D ・AutoCAD Architecture　・AutoCAD Inventor　・AutoCAD Inventor LT 各アプリケーションからは、以下の情報を取得します。 ・アプリケーション名　・製品バージョン　・プロダクトID　・インストールパス
	ウイルス対策ソフトの情報取得	クライアントPCにインストールされている、以下のウイルス対策ソフトの情報を取得します。 ・トレンドマイクロ社（TrendMicro ウイルスバスター）　・マカフィー社（McAfee VirusScan/Total Protection）・シマンテック社（Norton AntiVirus /Symantec Endpoint Protection）・キヤノンITソリューションズ社（ESET Smart Security/ESET NOD32アンチウイルス） ・カスペルスキー社（Kaspersky End）・Microsoft社（Windows Defender）
	Hotfixの情報取得	各クライアントPCに適用されている、Hotfixの情報を取得します。　・表示 名　・KB番号　・適用日時
	任意の実行ファイルの情報取得 mac	全てのユーザーアカウントのスタートメニュー、デスクトップ、クイック起動に登録されているショートカットから実行ファイルを検索し、以下の情報を取得します。 ・実行ファイル名　・ファイルバージョン　・会社名　・製品名　・著作権　・ファイル作成日時　・ファイル更新日時　・ファイルパス 任意のファイルパスと、ファイル名を検索対象に追加することもできます。
	Windowsストアアプリの情報取得	ショートカットの情報として、Windows ストアアプリの情報を取得します。 ・実行ファイル名（パッケージ名）　・ファイルバージョン　・会社名　・製品名　・ファイル作成日時　・ファイル更新日時　・ファイルパス
	任意のドキュメントファイルの検索	クライアントPCから、任意のファイル名を検索します。 ・ファイル名　・ファイルサイズ　・ファイル 作成日時　・ファイル 更新日時　・ファイルパス
	OS/アプリケーションのライセンス管理	クライアントPCから収集した情報をもとに、アプリケーションの購入数と実際にインストールされている件数の差分を確認することができます。
	ライセンス形態別のライセンス情報登録	ライセンス種別、ライセンス形態に応じたライセンス情報を登録することができます。AssetView クライアント以外のハードウェアを、管理対象にすることも可能です。
	ソフトウェア辞書のインポート	保守ユーザーページからダウンロードしたソフトウェア辞書（有償）を、管理対象ソフトウェアにインポートすることが可能です。
	ソフトウェアグループ	エディションやバージョンにより、『ソフトウェア名』が異なるソフトウェアを、まとめて管理することができます。
	ライセンス割当て管理	ライセンスごとに、該当のソフトウェアの利用を許可するクライアントPCを割当てることができます。
	ライセンス利用申請	クライアントPCから、ライセンス登録されているソフトウェアの利用許可（割当て）を申請することができます。
	ソフトウェア資産管理台帳	以下のソフトウェア資産管理台帳を作成することができます。 ・利用ソフトウェア台帳　・ライセンス台帳　・ライセンス関連部材台帳
	ハードウェア情報のアラート通知	以下の条件に該当するハードウェア情報を取得したら、管理者にアラートメールを送信します。 ・システムドライブの空き容量不足　・IPアドレス重複　・MACアドレス重複
	アプリケーション情報のアラート通知	指定した文字列を含むアプリケーション情報を取得したら、管理者にアラートメールを送信します。
	死活監視	指定したIPアドレスに対して、pingによる死活監視とSNMPによる情報の取得を行います。
AssetView D （アプリケーション配布） D	ファイル 自動配布	クライアントPCに対して、任意のファイルを配布するタスクを登録することができます。
	プログラム 自動実行	クライアントPCに対して、任意のコマンドを実行するタスクを登録することができます。
	INIファイル 自動編集	クライアントPC上の、任意のINIファイルを編集するタスクを登録することができます。
	レジストリ 自動編集	クライアントPC上の、任意のレジストリ値を編集するタスクを登録することができます。
	OSシャットダウン/再起動の自動実行	クライアントPCの、OSシャットダウン/再起動を実行するタスクを登録することができます。
	OS起動時に実行	OS起動時に自動実行するタスクを、登録することができます。
	OSログオン時に実行	OSログオン時に自動実行するタスクを、登録することができます。
	指定時間にランダムに開始	指定した時間帯の範囲で、ランダムに開始するタスクを登録することができます。クライアントPCごとに、異なるタイミングでタスクを実行することで、ネットワークの負荷を分散することができます。
	クライアントPCで、タスクを選択して実行する（タスクランチャー）	クライアントPCのスタートメニューに登録されている[タスクランチャー]で、自身を対象に登録されているタスクを選択して、任意のタイミングで実行させることもできます。
	タスクの先送り	タスクの先送りが必要な場合は先送りする時間を設定できます。

※クラウド不可　mac ※macOS 対応（一部対応していない機能があります）

AssetView 機能詳細一覧表

ライセンス	機能名	説明
AssetView D (アプリケーション配布)	ファイル配布/プログラム実行タスクのアラート通知	タスクが失敗したら、管理者にアラートメールを送信します。
	Macromation（マクロメーション）	Windows 上で行った操作を記録し、実行ファイルに保存して再現することができます。マウスやキーボードの操作に条件判断を設定することで、あらゆる処理を自動化することが可能です。
	WSUS連携	WSUS環境における更新プログラムの適用を行うタスクを登録することができます。
	スクリプト連携	弊社から提供したスクリプトを配布/実行するタスクを登録することができます。
	メッセージ配信	クライアントPCに対して、任意のメッセージを配信するタスクを登録することができます。
AssetView M (PC操作ログ管理)	プロセスログの取得 (mac)	クライアントPCで起動している、プロセスの情報を取得します。 ・プロセス名 ・アカウント名 ・バージョン ・起動日時 ・起動していた時間
	ホワイトリストプロセス登録機能	プロセス名もしくはフォルダーパスを登録し、対象となるプロセス以外のプロセス起動に対し、警告メッセージ表示または強制終了処理を行います。
	アラートプロセス起動警告 (mac)	任意の実行ファイルの起動を検知して、クライアントPCに警告メッセージを表示します。
	アラートプロセス起動禁止 (mac)	任意の実行ファイルの起動を検知して、自動的に強制終了します。
	プロセス停止監視	任意のプロセスの停止を検知して、クライアントPCに警告メッセージを表示します。
	ウィンドウタイトルログの取得	クライアントPCでアクティブになっているウィンドウの情報を取得します。 ・プロセス名 ・ウィンドウタイトル ・URL
	ウィンドウタイトル警告 (mac)	任意の文字列を含むウィンドウタイトルがアクティブになった際に、クライアントPCに警告メッセージを表示します。
	ウィンドウタイトル警告時のスクリーンショット取得（AssetView REC ライセンス連携機能）	ウィンドウタイトル警告時に、デスクトップのスクリーンショットを取得することができます。
	ウィンドウタイトル警告時の強制終了	ウィンドウタイトル警告時に、プロセスを強制終了することができます。
	クリップボード操作ログの取得	クライアントPCで行われた、以下のクリップボード操作を取得します。 ・文字列のコピー ・ファイルのコピー ・画像のコピー/プリントスクリーン
	プリントスクリーン操作ログの取得	クライアントPCで行われたクリップボードを経由したプリントスクリーン操作ログを画像データ付きで取得します。
	QQチャットログの取得	テンセントQQ(インスタントメッセンジャー)でチャットした際に送受信された文字列を取得します。
	メール送信ログの取得	クライアントPCのメール送信を検知して、以下の情報を取得します。 ・件名 ・送信日時 ・送信元メールアドレス ・送信先メールアドレス ・添付ファイル名
	Webフォーム送信ログの取得	クライアントPCからWebサイトへの書き込みを検知して、以下の情報を取得します。 ・接続先IPアドレス ・ポート番号 ・URL ・本文(送信データ)
	Google Workspace操作ログの取得	Google Chrome/Microsoft Edge(Chromium)で操作した、以下のGoogle Workspaceの情報を取得します。 ・Googleドライブ ・Gmail ・Google カレンダー ・Google グループ
	Webアクセスログ取得	クライアントPCのWebアクセス(HTTP GET)を検知して、接続先URLの情報を取得します。
	Webアクセス禁止	指定したURLへのアクセスを禁止します。
	ファイル操作ログの取得 (mac)	クライアントPCで行われた、ファイル操作の情報を取得します。 ・操作対象のファイル名 ・操作対象のファイルパス ・操作元のドライブ種別 ・変更後のファイル名 ・プロセス名 ・コピー/移動先のファイルパス ・コピー/移動先のデバイス情報
	メール添付ログの取得	メール作成時に指定した添付ファイルの情報を取得します。 ・操作対象のファイル名 ・操作対象のファイルパス ・プロセス名 ・操作元のドライブ種別
	印刷ログの取得 (mac)	クライアントPCで印刷された、ドキュメントの情報を取得します。 ・ドキュメント名 ・ファイル名 ・プリンター名 ・印刷枚数 ・印刷データタイプ
	HTTPでのファイルアップロードログの取得	クライアントPCからWebサイトにHTTP-POSTでアップロードされたファイルの情報を取得します。 ・操作対象のファイル名 ・操作対象のファイルパス ・アップロード先のURL
	FTPでのファイルアップロードログの取得	クライアントPCから、FTPサーバーにアップロードされたファイルの情報を取得します。 ・操作対象のファイル名 ・アップロード先のIPアドレス
	ダウンロードログの取得	クライアントPCから、Webブラウザーで行ったダウンロード元のURL情報を取得します
	ファイル操作警告	指定したファイル名、またはファイルパスを含むファイルの操作を検知した際に、クライアントPCに警告メッセージを表示します。
	ファイル操作禁止	指定したファイル名、またはファイルパスを含むファイルの操作を禁止します。
	個人情報/機密情報のファイル操作時検出（AssetView I ライセンス連携機能）	個人/機密情報が含まれる可能性のあるファイル操作を検知して、クライアントPCに警告メッセージを表示します。
	個人情報/機密情報ファイル自動暗号化（AssetView K ライセンス連携機能）	個人/機密情報が含まれる可能性のあるファイル操作を検知して、自動的に暗号化します。
	外部デバイスにコピー・移動したファイルの自動暗号化（AssetView K ライセンス連携機能）	リムーバブルディスク、共有フォルダーおよびCD/DVD/Blurayにコピー・移動したファイルを自動的に暗号化します。
	HTTPでアップロードしたファイルの自動暗号化（AssetView K ライセンス連携機能）	Webブラウザーからアップロードされたファイルを自動的に暗号化またはアップロードを遮断します。
	WEBからダウンロードした個人/機密情報ファイルの自動暗号化（AssetView I/K ライセンス連携機能）	Webブラウザーからダウンロードされた個人/機密情報ファイルを自動的に暗号化します。
	日本語環境以外での警告メッセージ	クライアントPCの環境に応じて、以下の言語で警告メッセージを表示することができます。 ・日本語 ・中国語(簡体字) ・英語(日本語/中国語以外)
	ドライブの追加と削除の情報取得 (mac)	ドライブの追加と削除を検知して、以下の情報を取得します。 ・ドライブ種別（ローカルディスク、リムーバブルディスク、ネットワークドライブ、FD、CD/DVD、ポータブルデバイス） ・ドライブ名 ・UNCパス（ネットワークドライブの場合） ・デバイス名（USBデバイス/ポータブルデバイスの場合） ・ベンダー（USBデバイス/ポータブルデバイスの場合） ・プロダクトID（USBデバイス/ポータブルデバイスの場合） ・シリアルナンバー（USBデバイス/ポータブルデバイスの場合）
	稼働状況の取得 (mac)	以下のイベントを検知して、情報を取得します。 ・AssetView クライアント起動 ・OSログオン ・OSログオフ ・スリープ ・スリープ解除 ・スクリーンセーバー ・スクリーンセーバー解除 ・OSシャットダウン要求 ・OSシャットダウン ・ロック ・アンロック
	Windows ファイアウォール管理	クライアントPCの Windows ファイアウォールに、アクセスを禁止するIPアドレスの設定を登録することができます。
	右クリック/Ctrl+Pの禁止	指定したウィンドウタイトルがアクティブになると、コンテキストメニューの表示またはCtrl+P/Ctrl+Shift+Pキー(印刷ダイアログ表示)を禁止します。
	クリップボード禁止	指定したプロセスが起動している間、クリップボードへの文字列または画像のコピーを禁止します。
	プリントスクリーン禁止	プリントスクリーン操作を禁止します。
	操作履歴検索	条件を指定して、クライアントPCの操作履歴ログを検索します。
	検索条件の保存	操作履歴の検索条件に名前をつけて保存することができます。
	操作履歴のマーキング	任意の操作履歴ログをマーキングすることができます。
	ファイル操作の追跡	クライアントPCから取得したファイル操作ログから、特定のファイルの操作履歴を追跡することができます。
	不正操作検出のアラート通知	以下の条件に該当する操作を検知したら、管理者にアラートメール又は通知アプリにて通知します。 ・警告プロセスの起動 ・禁止プロセスの起動 ・停止監視プロセスの停止 ・ウィンドウタイトル警告 ・ファイル操作警告 ・ファイル操作禁止 ・ドライブ追加 ・特定フォルダアクセス ・ローカル共有フォルダ作成 ・ローカル共有フォルダアクセス ・指定アプリケーションの名前変更 ・レジストリ変更 ・システム構成変更 ・Windowsストアの利用 ・不許可ファイル検索 ・CSVファイル出力 ・規定時間外端末機操作 ・ローカル共有フォルダ作成 ・ローカル共有フォルダアクセス ・カスタマイズ(運用ポリシー設定の変更など) ・禁止ファイル持ち込み ・実行ファイルの不正操作

ライセンス	機能名	説明
AssetView M (PC操作ログ管理)	USBデバイス使用状況のエクスポート	指定した期間に、各クライアントPCに接続されたUSBデバイスの情報を、CSVファイルに出力します。
	稼働状況グラフ表示	ハードウェア、アプリケーション、ドキュメントそれぞれの視点で、クライアントPCの24時間の稼働状況をグラフ表示し、アラートを検知した時間を赤で表示します。
	シャドウイング	外部デバイスへコピー/移動を行ったファイルをサーバー上に複製保存(シャドウイング)します。
	システムログの監視	システムログから特定のイベント/レジストリ/ファイルの更新を監視してログを取得します。
AssetView I (個人情報検索)	特定個人情報ファイルの検索	クライアントPCから、特定個人情報(マイナンバーを含む個人情報)に該当する可能性のあるファイルを検索します。 ※マイナンバーは日本版/タイ版に対応しています。 ※日本の特定個人情報はマイナンバーのほか以下の個人情報を検出対象とすることができます。 ・ファイル名 ・ファイルサイズ ・ファイル作成日時 ・ファイル更新日時 ・ファイルパス ・人名 ・住所 ・生年月日 ・電話番号 ・メールアドレス ・免許証番号 ・パスポート番号 ・クレジットカード番号 ・口座番号
	個人情報ファイルの検索	クライアントPCから、個人情報を含む可能性のあるファイルを検索します。 ※以下の個人情報を検出対象とすることができます。 ・ファイル名 ・ファイルサイズ ・ファイル作成日時 ・ファイル更新日時 ・ファイルパス ・人名 ・住所 ・生年月日 ・電話番号 ・メールアドレス ・免許証番号 ・パスポート番号 ・クレジットカード番号 ・口座番号 ・ユーザー辞書(任意の文字列)
	機密情報ファイルの検索	クライアントPCから、任意の文字列を含むファイルを検索します。・ファイル名 ・ファイルサイズ ・ファイル作成日時 ・ファイル更新日時 ・ファイルパス
	圧縮ファイルからの個人/機密情報検出	ZIP、またはLZH形式で圧縮されたファイルから、個人/機密情報を検索することができます。
	個人情報/機密情報ファイル自動暗号化（AssetView K ライセンス連携機能）	個人/機密情報ファイルを検出した際に、自動的に暗号化します。
	個人/機密情報ファイルの隔離	管理コンソールから指定した個人/機密情報ファイルを、ユーザーからアクセスできない場所に隔離します。検出時に自動的に隔離することも可能です。
	個人/機密情報ファイルの削除	管理コンソールから指定した個人/機密情報ファイルを削除します。
	個人/機密情報ファイルの完全削除	管理コンソールから指定した個人/機密情報ファイルを削除すると同時に、ディスク上からデータの痕跡を消し去ることで、復元ツールなどを利用しても該当のファイルを復旧できないようにします。
	対象外ファイルの指定	次回検索時から、個人/機密情報として扱わないようにするファイルを指定することができます。
	個人/機密情報検出のアラート通知	個人/機密情報ファイルが検出されたら、管理者にアラートメールを送信します。
AssetView G (デバイス制御)	USBデバイスの情報取得 (mac)	クライアントPCに接続したUSBデバイスの情報を取得します。 ・デバイス名 ・ベンダー ・プロダクトID ・シリアルナンバー
	USBデバイスの個別制御 (mac)	USBデバイスを個体識別して、使用を制御します。 ・書込み許可 ・読込み専用 ・使用禁止
	未定義のUSBデバイスの設定	新規に検知したUSBデバイスの初期設定を変更することができます。 ・書込み許可 ・読込み専用 ・使用禁止
	USBデバイス制御時の警告メッセージ	使用を禁止しているUSBデバイスの接続、読込み専用に設定したUSBデバイスへの書き込みを検知して、クライアントPCに警告メッセージを表示します。
	USBデバイス接続警告	USBデバイスの接続を検知して、クライアントPCに警告メッセージを表示します。
	指定期間更新されていないUSBデバイスの使用禁止	指定した日数接続されていないUSBデバイスを、自動的に使用禁止にすることができます。
	USBデバイスの実行ファイル存在警告（AssetView M ライセンス連携機能）	USBデバイスの接続を検知した際に、該当のUSBデバイスに実行ファイルが存在する場合に警告メッセージを表示します。
	USBデバイスに格納されているファイル情報の取得(AssetView M ライセンス連携機能)	USBデバイスの接続を検知した際に、該当のUSBデバイスに格納されているファイルの情報を取得します。
	FD/SDカードの制御	FD/SDカードドライブの使用を制御します。 ・書込み許可 ・読込み専用 ・使用禁止
	FD/SDカード制御時の警告メッセージ	FD/SDカードへの書き込み禁止時に、クライアントPCに警告メッセージを表示します。
	メディア識別	以下のデバイスを対象に、個々のメディアを識別して個別制御することができます。 ・USBデバイス ・SDカード ・MO
	CD/DVD/Brue-rayの制御	CD/DVD/Blu-rayドライブの使用を制御します。 ・書込み許可 ・読込み専用 ・使用禁止
	ライティングソフトの起動禁止	CD/DVD/Blu-rayを読込み専用、または使用禁止にした際に、以下のライティングソフトの起動を禁止します。 ・B's Recorder GOLD 16 ・Easy Media Creator 10 ・Nero 9 StartSmart Essentials ・Nero BurnExpless 2019 ・Nero Burning ROM 2020 ・CyberLink Power2Go 8/CyberLink Power2Go 13
	CD/DVD/Blue-ray制御時の警告メッセージ	CD/DVD/Blu-rayへの書き込み禁止時に、クライアントPCに警告メッセージを表示します。
	共有フォルダーの制御	共有フォルダーでのファイル操作を制御します。 ・書込み許可 ・読込み専用 ・使用禁止
	共有フォルダー制御時の警告メッセージ	共有フォルダーへの書き込み禁止時に、クライアントPCに警告メッセージを表示します。
	ポータブルデバイスの情報取得	スマートフォン、オーディオプレーヤー、デジタルカメラ等、Windows ポータブルデバイスとして認識されるデバイスが接続された際に、以下の情報を取得します。 ・デバイス名 ・ベンダー ・プロダクトID ・シリアルナンバー
	ポータブルデバイスの個別制御	ポータブルデバイスを個体識別して、使用を制御します。 ・使用許可 ・読込み専用 ・使用禁止
	未定義のポータブルデバイスの設定	新規に検知したポータブルデバイスの初期設定を変更することができます。 ・書込み許可 ・読込み専用 ・使用禁止
	ポータブルデバイス制御時の警告メッセージ	使用禁止ポータブルデバイスの接続、警告対象とするファイルの書き込みを検知した際に、クライアントPCに警告メッセージを表示します。
	デジタルカメラの個別制御	USBデバイス、ポータブルデバイスのうちデジタルカメラとして設定されたものを個体識別して、使用を制御します。 ・書込み許可 ・読込み専用 ・使用禁止
	未定義のデジタルカメラの設定	新規に検知したデジタルカメラの初期設定を変更することができます。 ・書込み許可 ・読込み専用 ・使用禁止
	MOの個別制御	MOドライブを個体識別して、使用を制御します。 ・書込み許可 ・読込み専用 ・使用禁止
	未定義のMOの設定	新規に検知したMOの初期設定を変更することができます。 ・書込み許可 ・読込み専用 ・使用禁止
	Wi-Fiの制御	Wi-Fiアクセスポイントに対し個別に接続を制御します。 ・接続許可 ・接続禁止
	Bluetoothの制御	Bluetoothデバイスを無効にすることができます。
	Bluetoothの個別制御	Bluetoothデバイスを個体識別して、使用を制御します。 ・接続許可 ・接続禁止
	未定義のBluetoothの制御	新規に検知したBluetoothデバイスの初期設定を変更することができます。 ・接続許可 ・接続禁止 ・無効にする

※クラウド不可　(mac) ※macOS 対応(一部対応していない機能があります)

AssetView 機能詳細一覧表

ライセンス	機能名	説明
AssetView G（デバイス制御）	日本語環境以外での警告メッセージ	クライアントPCの環境に応じて、以下の言語で警告メッセージを表示することができます。 ・日本語 ・中国語（簡体字） ・英語（日本語/中国語以外）
	USB接続のNICの制御	USB接続のNICに対し個別に使用を制御します。・使用許可 ・使用禁止
	未定義のUSB接続のNICの設定	新規に検知したUSB接続のNICの初期設定を変更することができます。 ・使用許可 ・使用禁止
	デバイス管理番号	クライアントPCから検知した個々のデバイスに対して、自動的にデバイス管理番号を発行します。
	デバイス種別の変更	管理コンソールで、デバイス種別を任意に変更することができます。 ・USBデバイス ・FD/SDカード ・ポータブルデバイス ・MO ・デジタルカメラ
	デバイス種別の自動判定	クライアントPCから検知したUSBデバイス、またはポータブルデバイスのデバイス名を条件として、デバイス種別を自動的に変更することができます。
	特権ユーザー	Active Directory ユーザーを対象に、デバイス制御の適用対象から除外する『特権ユーザー』を設定することができます。
	特権ユーザーの自動判定	組織単位（OU）の『役職』を条件として、自動的に特権ユーザーを設定することができます。
	特権クライアント	デバイス制御の対象から除外する、『特権クライアント』を設定することができます。
	USBデバイス利用申請	クライアントPCから、特定のUSBデバイスの制御設定変更の申請を行うことができます。 指定した申請書のファイル（Excel）を起動し、シリアルナンバー等の値を自動的に転記します。
	USBデバイス制御申請 (mac)	クライアントPCから、特定のUSBデバイスの制御設定を一時的に変更する申請を行うことができます。 管理者は、申請を承認/否認するだけでなく、申請された内容を変更することも可能です。
	デバイス制御の申請	クライアントPCから、右記のデバイスの制御設定を一時的に変更する申請を行うことができます。 ・FD/SDカード ・CD/DVD/Blu-rayドライブ ・共有フォルダー 管理者は、申請を承認/否認するだけでなく、申請された内容を変更することも可能です。
	クライアントPCでの承認	管理アカウントにクライアントPCを割当てることで、管理コンソールだけでなくクライアントPCでもUSBデバイス申請/デバイス制御申請を承認することができます。
	デバイス利用申請時の自動暗号化設定（AssetView K ライセンス連携機能）	デバイス制御申請で申請したデバイスにファイルを保存する際に、自動的に暗号化することができます。
	デバイス利用申請対象の事前登録	事前に登録されたデバイスのみを申請対象とすることができます。
	USBデバイスの一時ポリシー設定	管理コンソールから、クライアントPC、またはグループに対して、特定のUSBデバイスの制御設定を一時的に変更することができます。（クライアント型のみ）
	デバイス制御の一時ポリシー設定（クライアント型）	管理コンソールから、クライアントPCに対して、以下のデバイス制御設定を一時的に変更することができます。 ・FD/SDカード ・CD/DVD/Blue-rayドライブ ・共有フォルダー
	デバイス制御の一時ポリシー設定（サーバー型）	管理コンソールから、クライアントPCまたはユーザーに対して、デバイス制御設定を一時的に変更することができます。
	解除コード	管理コンソールで発行した解除コードを入力することで、サーバーにネットワーク接続できないクライアントPCのデバイス制御設定を一時的に変更することができます。
	デバイス制御状態のグラフ表示	クライアントPCに現在登録されている、デバイス制御の運用ポリシーと一時設定をもとに、将来適用されるデバイス制御の状態をグラフ表示します。
	USBデバイスの棚卸	各機器に貼られている管理番号と該当の機器を利用している職員番号の組合せをキーとして、利用者からの申請、または管理コンソールで登録したUSBデバイスをリスト化します。
	申請情報の通知	管理対象のクライアントPCから、USBデバイス申請/デバイス制御申請が登録されたことを、管理者にメールで通知します。 管理アカウントにクライアントPCが割当てられていた場合は、バルーンでも通知します。
	デバイス制御申請ユーザー情報のインポート	CSVファイルからデバイス制御申請ユーザー情報をインポートして、一括設定することができます。
	デバイス設定のインポート	CSVファイルからデバイスの設定情報をインポートして、一括設定することができます。
	デバイス制御のアラート通知	以下の条件に該当する操作を検知したら、管理者にアラートメールを送信します。 ・使用禁止USBデバイスの接続 ・使用禁止デバイスの接続 ・使用禁止ポータブルデバイスの接続 ・使用禁止Bluetoothデバイスの接続 ・読込み専用USBデバイスへの書込み ・読込み専用デバイスへの書込み ・USBデバイス内に実行ファイルを検知した場合（クライアント型のみ）
	セーフモード時のデバイス制御	『セーフモードとネットワーク』または、『セーフモードとコマンドプロンプト』でOSが起動された場合は、スクリーンロックをかけ、OSの操作を制御します。 また、『セーフモード』で起動された場合は、接続されたデバイスを使用禁止で制御します。
	Wi-Fiの状況の取得	以下のイベントを検知して、情報を取得します。 ・Wi-Fi接続 ・Wi-Fi切断
	自動実行の無効化	クライアント端末に接続されたデバイスの自動実行を無効にします。
AssetView S（不正PC遮断）	ハードウェアの検知	ネットワーク上から、AssetView クライアント以外のハードウェアを自動的に検知します。
	ハードウェア情報の自動登録	ネットワーク上から検知した、AssetView クライアント以外のハードウェアを、マスター情報に自動的に登録します。
	許可されていないハードウェアの遮断	許可されているハードウェア以外を、ネットワークから遮断します。
	IPアドレスごとの制御設定	検知したハードウェアから要求されたIPアドレスの範囲によって、制御設定を変更することができます。 ・遮断する ・検知する ・何もしない
	ネットワーク検知/遮断のアラート通知	ネットワークからハードウェアを検知、遮断したら、管理者にアラートメールを送信します。
	ランダムMACアドレスの制御	ランダムMACアドレスに対してネットワーク制御を設定できます。 ・遮断する ・遮断しない ・無視する
	遮断/検知端末の設定	遮断/検知端末について設定できます。 ・同一ネットワーク（セグメント）内で稼働させる台数を指定する ・特定のIPアドレスの範囲で稼働させない
AssetView RC 2.0.0（リモートコンソール）	リモートデスクトップ	クライアントPCのデスクトップをリモート操作します。 使用するポート番号、パスワードは変更できます。ホストとゲスト間の通信は暗号化されています。
	ユーザー操作制限	リモート接続中にユーザーのキーボードおよびマウス操作を制限することができます。
	接続確認	リモート操作開始時にクライアントに接続許可を求めることができます。
	ビデオレート変更	リモート接続中にビデオレートを変更することができます。
	ファイル転送	ホストとゲスト間でファイルを送受信することができます。
	ファイルコピー	ホストとゲスト間でクリップボードやドラッグアンドドロップによるファイルコピーができます。
	ペイントモード	リモート操作中のクライアントPCのデスクトップ上に描画します。
	リレークライアント	相互接続できない場合もインターネットを介してリモート操作ができます。
AssetView F（Webフィルタリング）	内部/外部のPCに対するインターネットアクセス制御	クラウド上のサーバーを参照してフィルタリングを行うため、クライアントPCが外部にあってもWebアクセスを制御することができます。
	プログラム利用規制	ファイル共有ソフトやメッセンジャーなど、指定したプログラムの通信を規制することができます。
	高精度データベース	日本国内の携帯電話キャリア5社にも採用された、高品質のURLデータベースを保有しています。
	カテゴリフィルタリング	149種類のカテゴリでフィルタリングを行います。※ユーザー設定カテゴリを含みます。
	フィルタリング設定	カテゴリごとに利用状況に応じたフィルタリング設定が可能です。・許可・書込み規制・規制・一時解除 ※カテゴリ未分類のURLに対しても設定可能です。

ライセンス	機能名	説明
AssetView F（Webフィルタリング）	書き込み規制のサイズ指定	書込み規制を規制する際にサイズを指定することができます。
	HTTPSサイトのフィルタリング	HTTPSサイトへのアクセスもフィルタリングすることができます。
AssetView K（ファイル制御・暗号化）	暗号ファイル作成	指定したファイルを暗号化（AES 256bit）することができます。
	ActiveDirectory連携	ActiveDirectoryからユーザー情報をインポートすることができます。 許可されたアカウントでOSにログオンしていれば、パスワードを入力せずに暗号化ツールを起動することができます。
	アカウント指定でのアクセス権設定	暗号ファイルを閲覧する権限を、アカウント単位で設定することができます。
	グループ指定でのアクセス権設定	暗号ファイルを閲覧する権限を、グループ単位で設定することができます。
	パスワード指定でのアクセス権設定	パスワードのみで暗号ファイルを閲覧する権限を設定することができます。
	暗号ファイルの制御	暗号化したファイルを閲覧する際の制限を設定することができます。 ・閲覧回数 ・閲覧期限 ・保存禁止 ・印刷禁止 ・文字列や画像のコピー、Print screenの禁止
	閲覧制限を越えたファイルの削除	閲覧回数、閲覧期限を超過した暗号ファイルを閲覧しようとした際に、該当のファイルを削除することができます。
	暗号化ファイルのパスワード変更	すでに暗号化されたファイルの場合でも、管理者は復号に必要なパスワードを変更することができます。 また、パスワードモードで暗号化されたファイルを暗号化ツールを使用することで、一括でパスワードを変更することができます。
	クラウドストレージ自動暗号化	クラウドストレージ（Dropbox/OneDrive/OneDrive for Business）のアプリケーションをクライアントにインストールしている場合、 クラウドストレージとの同期に使用されるローカルのフォルダに配置されたファイルを自動暗号化することができます。
	メール添付ファイルの自動暗号化	Microsoft Outlookで送信したメールの添付ファイルを、管理者が指定した設定で自動的に暗号化することができます。
	メール添付ファイルの自動ZIP形式圧縮化	Microsoft Outlookで送信したメールの添付ファイルを、管理者が指定した設定で自動的にパスワード付きZIP形式で圧縮することができます。
	復号ツール	復号ツール単体のインストーラーを提供することができます。 インターネットに接続可能な環境であれば、AssetView がインストールされていない環境でも暗号ファイルの閲覧が可能です。
	自己復号形式での暗号化	自己復号形式（EXE）で、暗号ファイルを作成することができます。 インターネットに接続可能な環境であれば、復号ツールがインストールされていない環境でも暗号ファイルを閲覧することができます。
	クライアントPCでのアカウント作成	暗号ファイルを外部に提供する場合などに、クライアントPCの暗号化ツールで閲覧専用のアカウントを作成することができます。
	暗号ファイルの操作履歴	管理コンソールで、暗号ファイル作成、閲覧の履歴を表示することができます。
	暗号ファイルの設定変更	管理コンソールで、暗号ファイルのアクセス権や制御設定を変更することができます。
	個人/機密情報の検出（AssetView I ライセンス連携機能）	暗号ファイル作成時に、該当のファイルに個人/機密情報が含まれているかどうかを判定することができます。 管理者は、個人/機密情報が含まれる可能性があるファイルを暗号化する際に適用する制御設定の初期値を設定することができます。
	フォルダーに配置したファイルの自動暗号化/パスワード付きZIP化	指定したフォルダーに配置されたファイルを自動的に暗号化、もしくは、パスワード付きZIP形式で圧縮することができます。
	アラート通知	以下の制限を越えた暗号ファイルがあれば、管理者にアラートメールを送信します。 ・制限時間内に指定回数以上復号された ・業務時間以外に復号された ・指定したドメイン以外で復号された
AssetView Vplus（エンドポイントセキュリティ）	ファイルモニター	クライアントPC上で行われたファイルI/Oを監視し、リアルタイムにウイルス等の脅威を検知します。
	メールモニター	クライアントPC上で行われるメール送受信（SMTP/ESMTP/POP3/IMAP）を監視し、リアルタイムにウイルス等の脅威を検知します。
	Webモニター	クライアントPCのWebアクセスを監視し、リアルタイムにウイルス等の脅威を検知します。
	ウイルススキャン	指定したスケジュールでクライアントPCのドライブをスキャンし、ウイルス等の検知を行います。
	オンデマンドスキャン	管理コンソールからクライアントを指定して、またはクライアントPC自身で任意のファイルやフォルダーを右クリックして、 ウイルススキャンを即実行することができます。
	セキュリティレベル	セキュリティレベルを選択することで簡単に設定できます。選択後にカスタム可能です。
	ヒューリスティック分析	過去に発見された脅威の分析結果をもとにウイルス等に特徴的な挙動を判定して、脅威の可能性のあるプログラム（疑わしいオブジェクト）を検知することができ、分析レベルが選択できます。
	ふるまい検知	実行段階のふるまいをもとに脅威の可能性のあるプログラム（疑わしいオブジェクト）を検知することができます。
	USBデバイス接続時の自動スキャン	USBデバイスの接続を検知して、該当のデバイスのウイルススキャンを実行することができます。
	警告メッセージの表示	ウイルス等の脅威を検知した際に、クライアントPCに警告メッセージを表示します。
	脅威検知レポート	管理コンソール、またはクライアントPC自身で、検知された脅威のログを確認できます。
	パターンファイルの即時更新	管理コンソール、またはクライアントPC自身で、パターンファイルのダウンロードを即時実行することができます。
	隔離されたファイルの復元/削除	クライアントPC自身で、隔離されたファイルを復元または削除できます。
	パターンファイルのエクスポート/インポート	オフラインで運用しているPCに、他のクライアントPCからエクスポートしたパターンファイルをインポートすることができます。
	脅威が検知されたPCのアラート通知	クライアントPCからウイルス等の脅威を検知した際に、管理者にアラートメールを送信します。
	特別な駆除	検出された脅威を通常の駆除では削除できない場合に特別な駆除を実行することができます。
	クラウド接続	クライアントPCでパターンファイルの取得元およびログの送信先としてクラウドを選択できます。
AssetView P（PC更新管理）	自動更新	インターネット接続環境下のPサーバーは、週次更新データに更新がある場合、クラウドから自動的にダウンロードします。
	週次更新データの同期	インターネット接続ができない環境下のPサーバーに、他のPサーバーからエクスポートした週次更新データをインポートすることができます。
	ヘルスビュー	Pサーバーおよびpタスク、ミラーコンピューター、WSUS連携などの状況を表示します。また、Pサーバーの再起動や定期処理の即時実行を要求できます。
	機能更新の確認と設定	WindowsUpdateの機能更新プログラムの情報取得と設定、適用タスクの作成ができます。
	品質更新の確認	WindowsUpdateの品質更新プログラムの情報取得、適用タスクの作成ができます。
	更新プログラムのアンインストール要求	Windowsの更新プログラムのインストール情報を取得し、管理コンソールからアンインストール要求ができます。
	WindowsUpdateの実行	管理コンソールからクライアントを指定してWindowsUpdateのスケジュール実行または即時実行を要求できます。
	新着脆弱性情報の確認	弊社配信の脆弱性情報の内、より重要な情報を表示します。
	脆弱性検出数の確認	脆弱性検出数を深刻度別に表示します。
	脆弱性検索	以下の条件を指定して、脆弱性情報検索することができます。 ・公開日 ・更新日 ・キーワード ・ベンダー名 ・製品名 ・組織内検出 ・対策あり ・深刻度
	脆弱性対策の実行	対策が「あり」となっている脆弱性について該当端末に対し適用タスクを作成し、実行することができます。
	パッチ適用	ダウンロード済みのパッチについて任意の端末に対し適用タスクを作成し、実行することができます。
	Defender定義ファイル適用	Defender定義ファイルの配布について専用タスクを作成し、任意の時間帯に実行することができます。
	分散配布（マルチキャスト配信）	パッチの配布について分散配布を利用できます。

※クラウド不可 (mac) ※macOS 対応（一部対応していない機能があります）

AssetView 機能詳細一覧表

ライセンス	機能名	説明
AssetView P （PC更新管理）	ミラーコンピューター（ユニキャスト）	パッチの配布についてミラーコンピューターを利用できます。ユニキャストを指定することでブロードキャストを行わず直接通信を行うこともできます。
	ミラーコンピューターリスト	ミラーコンピューターの同期状況やドライブ空き状況を表示します。また、同期の即時実行を要求できます。
	WSUS連携	パッチ配布時にWSUSサーバーで保持するパッチを参照することができます。
	Microsoft 365利用	Microsoft 365/Officeの更新プログラムをPタスクで配布できます。 事前にMicrosoft社の提供するOffice展開ツールを使用した更新プログラムのダウンロードが必要です
	Office更新管理	Microsoft 365/Officeの更新プログラムを配布できます。 Office管理画面からOffice管理サーバーに対し任意のチャネルを追加できます。配布には以下のいずれかの方法を選択できます。 ・Officeセルフアップデート参照先を任意のOffice管理サーバーに設定 ・任意のOffice管理サーバーから更新プログラムを取得し、ファイル配布タスクで配布（分散配布を利用できます） インターネット接続環境下のOffice管理サーバーに、事前にMicrosoft社の提供するOffice展開ツールのインストールが必要です。 インターネット接続ができない環境下のOffice管理サーバーには、ファイル共有サーバー等からスクリプトを利用して更新プログラムをダウンロードできます。
	非武装クライアントの指定	脆弱性チェック対象から除外するクライアントを設定することができます。
	脆弱性の除外	特定の脆弱性を対策から除外することができます。
AssetView Mail （電子メール監視）	メール送信ログの取得 （クライアント側キャプチャモード）	クライアントPCのメーラーおよびブラウザーにメール送信を検知するアドオンを登録し、以下の情報を取得します。 ・件名　・本文　・送信日時　・送信元メールアドレス　・送信先メールアドレス　・添付ファイル
	メール送信ログの取得 （サーバ側キャプチャモード）	サーバーにてSMTPパケットをキャプチャし、、以下の情報を取得します。 ・件名　・本文　・送信日時　・送信元メールアドレス　・送信先メールアドレス　・添付ファイル
	Becky! Internet Mailでの SMTPSメール送信取得 （クライアント側キャプチャモード）	Becky! Internet Mailで、SMTPS（SMTP over SSL）で送信したメールの情報を取得することができます。
	OutlookでのExchange サーバーメール送信取得 （クライアント側キャプチャモード）	Microsoft Outlook で、Exchangeサーバーに送信したメールの情報を取得することができます。
	メールログ検索	指定した期間のメール送信ログを検索します。
AssetView REC （画面操作録画）	スケジュール録画	指定したスケジュールで、クライアントPCのデスクトップを録画することができます。
	タイムシフト録画	バックグラウンドで常に録画を行うことで、即時録画を行った場合に現時点よりも過去に遡って録画を開始することができます。
	マルチディスプレイ対応	複数のディスプレイを利用している環境では、最大4画面まで録画することができます。
	録画データのエクスポート	録画データを、動画（AVI／MP4）または静止画（JPEG）で出力することができます。
AssetView MDM （スマートデバイス管理）	ダッシュボード	お知らせやサマリを表示します。
	ユーザーの管理	デバイスを紐づけるユーザーの作成、編集、削除ができます。 グループ作成、移動、削除、グループ名変更、ユーザーとグループの紐づけができます。
	デバイスの管理	アプリケーション情報、ハードウェア情報、コマンド送信等のアクティビティを確認できます。 任意情報の更新、デバイスとユーザーの紐づけ、デバイス情報の削除、グループの作成／移動／削除、グループ名変更、デバイスとグループの紐づけができます。 以下の各デバイスを管理できます。 ・iOS/iPadOS端末（iPhone、iPad）・Android 端末（スマートフォンやタブレット）・Windows端末（ノートPCやタブレット）
	iOS/iPadOS端末の アプリケーション情報の取得	iOS/iPadOS端末にインストールされているアプリケーションの情報を取得します。 ・アプリ名　・iTunesストアID　・予定外　・不足
	Android 端末の アプリケーション情報の取得	Android 端末にインストールされているアプリケーションの情報を取得します。 ・アプリ名　・アプリID　・予定外　・不足
	Windows端末の アプリケーション情報の取得	Windows端末にインストールされているアプリケーションの情報を取得します。 ・アプリ名　・ストアID
	iOS/iPadOS端末情報の取得	iOS/iPadOS端末のハードウェア情報を取得します。 ・デバイス名　・電話番号　・IMEI　・IPアドレス　・カレントキャリア　・サブスクライバーキャリア　・ベンダー名　・モデル　・OSバージョン ・ビルドバージョン　・UDIS　・製品名　・製品番号　・シリアル番号　・Wi-FiのMACアドレス　・ICCID　・BluetoothのMACアドレス　・OS種別 ・名前　・最終アクセス日時　・デバイスコード
	Android 端末情報の取得	Android 端末のハードウェア情報を取得します。 ・MACアドレス　・IMEI　・製造メーカー　・モデル　・ネットワークキャリア　・電話番号　・OSバージョン　・OS種別　・名前 ・最終アクセス日時　・デバイスコード
	Windows端末情報の取得	Windows端末のハードウェア情報を取得します。 ・ハードウェアID　・デバイス種別　・マシン名　・最終アクセス日時　・MACアドレス　・IPアドレス　・サブネットマスク　・OS名 ・OSバージョン　・ドメイン名　・ログインユーザー　・MDMクライアントのバージョン情報
	コマンド実行-リモートロック	管理対象の端末のOSをリモートロックします。Windows端末では、解除可否について選択できます。
	コマンド実行-パスコードリセット	iOS/iPadOS端末のパスコードをリセットすることができます。
	コマンド実行-パスワード変更	Android 端末のパスワードを変更することができます。
	コマンド実行-リモートワイプ	iOS/iPadOS端末、Android 端末のOSを初期化します。Windows端末では、以下が実行されます。 ・システム以外のドライブをフォーマット（設定でON/OFF可能） ・指定フォルダの削除（設定で対象を指定可能） ・リモートロック（解除不可）
	コマンド実行-位置情報取得	位置情報を取得します。
	コマンド実行-デバイス情報の取得	デバイスのハードウェア情報を取得します。
	コマンド実行-紛失モードON/OFF	iOS/iPadOS端末の紛失モードをON/OFFに設定できます。
	コマンド実行-サウンドを鳴らす	iOS/iPadOS端末の紛失モードON時にサウンドを鳴らすことができます。
	コマンド実行-アプリ不足の配布	iOS/iPadOS端末にプロビジョニングで指定したアプリケーションを配布できます。
	コマンド実行 -プロファイルセットの適用	iOS/iPadOS端末、Android 端末にプロファイルセットを適用することができます。
	メッセージ送信	iOS/iPadOS端末、Android 端末にメッセージを送信します。
	プロファイル設定（iOS/iPadOS）制限	iOS/iPadOS端末の機能制限の簡易/詳細設定を登録することができます。
	プロファイル設定（iOS/iPadOS） -Wi-Fi	iOS/iPadOS端末のWi-Fi接続に関する設定を登録することができます。
	プロファイル設定（iOS/iPadOS） -VPN	iOS/iPadOS端末のVPN接続に関する設定を登録することができます。
	プロファイル設定（iOS/iPadOS） -メール	iOS/iPadOS端末のメール送受信に関する設定を登録することができます。
	プロファイル設定（iOS/iPadOS） -Webクリップ	iOS/iPadOS端末にWebクリップを配信することができます。

※クラウド不可　※macOS 対応（一部対応していない機能があります）

ライセンス	機能名	説明
AssetView MDM （スマートデバイス管理）	プロファイル設定（iOS/iPadOS） -証明書	iOS/iPadOS端末に証明書を配信することができます。
	プロファイル設定（iOS/iPadOS） -パスコード	iOS/iPadOS端末のパスコードポリシーを変更することができます。
	プロファイル設定（iOS/iPadOS） -Webコンテンツフィルタ	iOS/iPadOS端末で接続を許可/制限するURLを登録することができます。
	プロファイル設定（iOS/iPadOS） -ホーム画面レイアウト	iOS/iPadOS端末でホーム画面レイアウトを登録することができます。
	プロファイル設定（iOS/iPadOS） -カスタムプロファイル	iOS/iPadOS端末にApple Configuratorで作成した設定(mobileconfigファイル)を配信することができます。
	プロファイル設定（iOS/iPadOS）-ADE	iOS/iPadOS端末（ADE対応端末）の導入支援としてADE定義プロファイルを作成、端末割当を行います。
	プロファイル設定（ Android ） -システム設定	Android 端末のシステムの簡易/詳細設定を登録することができます。
	プロファイル設定（ Android ） -セキュリティ	Android 端末のセキュリティに関する設定を登録することができます。
	プロファイル設定（ Android ） -機能制御	Android 端末の機能制御を設定できます。
	プロファイル設定（ Android ）-アプリ	Android 端末のアプリの権限やインストール/アンインストールについて設定できます。
	プロファイル設定（ Android ）-Wi-Fi	Android 端末のWi-Fi接続に関する設定を登録することができます。
	アプリケーション管理	iOS/iPadOS端末、Android 端末のアプリケーションについて、ストアの購入アプリ一覧を表示できます。 サイドローディングでアプリケーションファイルを登録できます。
	プロビジョニング	プロファイルセットを作成し、iOS/iPadOS端末、Android 端末に適用することができます。
	データ入出力	ユーザー、デバイスについてインポート/エクスポートを行い、そのログを表示できます。 また、ASM SFTPのアップロードログを表示し、対象のファイルをダウンロードできます。
	設定-ユーザー種別	ユーザー管理に使用する種別を追加、編集、削除できます。種別ごとにユーザー数、紐づくデバイス数を確認できます。
	設定-任意項目	任意項目の追加、編集、削除ができます。
	設定-位置情報取得	位置情報の定期取得間隔について設定できます。
	設定-証明書・トークン	iOS/iPadOS端末の管理に使用するAPNs証明書、ADEトークン、VPPトークンのアップロードと有効期限の確認ができます。
	設定-紛失モード	iOS/iPadOS端末が紛失モードの場合の表示について設定できます。
	設定-ASM SFTP	iOS/iPadOS端末のASM SFTP接続情報を設定できます。
	設定-自動ロック	Windows端末の自動ロックON/OFFと間隔を設定することができます。
	設定-OS自動更新	Windows端末のOS自動更新ON/OFFを設定できます。
	設定-SmartScreen利用	Windows端末のSmartScreen機能ON/OFFを設定できます。
	設定-USBデバイス利用制御	Windows端末がUSBデバイスとして認識するデバイスへのアクセスポリシーを設定できます。
	設定-クライアントアプリ	Windows端末からアプリ（AssetView MDM v4）をアンインストールする際にパスワードを要求することで、 ユーザーが故意にアプリをアンインストールすることを防止します。
	設定-削除対象フォルダ設定	Windows端末のワイプ操作時に指定されたフォルダーを削除することができます。
	設定-管理者	管理対象の端末についてWeb管理画面から表示、操作できる管理者を設定できます。操作できる画面の権限セット設定や監査情報の表示も行います。

AssetView 稼働環境　下記システム要件を満たすPC/AT互換機で動作します。

※アプリケーションや環境によって制限事項がございます。詳細は営業担当までご確認ください。

データベースサーバー

OS	Microsoft Windows Server 2025 Standard/Datacenter Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※NET Framework 4.7.2 以降がインストールされている必要があります。 ※Visual Studio 2015、2017、2019、および 2022 用 Visual C++ 再頒布可能パッケージがインストール されている必要があります。
CPU	OS推奨値以上　最小：クアッドコア Intel Xeon 2.33GHz同等以上 ソケット数：1～4（5ソケット以上の場合も4ソケットまでのみ使用します）
メモリ	OS推奨値以上　最小：4GB以上
ディスク容量	データベースサーバーのインストールには、システムドライブに 20GB 以上の空き容量が必要です。また、バージョンアップ時にも十分な空き容量があることを確認してください。 データベースファイルの配置先となるドライブと、バックアップデータの配置先となるドライブは、十分な空き容量のあるシステムドライブ以外のローカルドライブを指定してください。
Microsoft Office	自動レポート機能を利用する場合は、データベースサーバーに Microsoft Excel 2016 以降または Microsft365 がインストールされ、ライセンスが認証されている必要があります。
その他	インストール時に専用データベースが導入されます。 AssetView 専用サーバーとすることを推奨します。 AssetView ではバージョンアップや今後の機能追加等の理由によりサーバー OS の再起動が必要となる場合があります。 他のシステム等と同居して運用する場合、処理速度や性能が低下する可能性があり、更に問題発生時には他のシステムと切り離した専用環境のご用意をお願いする場合があります。

アプリケーションサーバー

OS	Microsoft Windows Server 2025 Standard/Datacenter Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※.NET Framework 4.7.2 以降がインストールされている必要があります。 ※Visual Studio 2015、2017、2019、および 2022 用 Visual C++ 再頒布可能パッケージがインストール されている必要があります。
CPU	OS推奨値以上　最小：クアッドコア Intel Xeon 2.33GHz同等以上
メモリ	OS推奨値以上　最小：4GB以上
ディスク容量	アプリケーションサーバーのインストールには、システムドライブに 70MB 以上の空き容量が必要です。 AssetView Vplus ライセンスを有効にする場合は、システムドライブに 2GB 以上の空き容量が必要です。 ルートフォルダーの配置先となるドライブは、システムドライブ以外の十分な空き容量のあるローカルドライブを指定してください。
その他	AssetView専用サーバーとすることを推奨します。 AssetViewではバージョンアップや今後の機能追加等の理由によりサーバーOSの 再起動が必要となる場合があります。 他のシステム等と同居して運用する場合、処理速度や性能が低下する可能性があり、 更に問題発生時には他のシステムと切り離した専用環境のご用意をお願いする場合があります。

AssetView 稼働環境　下記システム要件を満たすPC/AT互換機で動作します。

※アプリケーションや環境によって制限事項がございます。詳細は営業担当までご確認ください。

AssetView クライアント

OS	Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows 11 Enterprise（21H2/22H2/23H2/24H2） Microsoft Windows 11 Home/Pro（22H2/23H2/24H2） Microsoft Windows 11 Enterprise LTSC（2024） Microsoft Windows 10 Home/Pro/Enterprise（22H2） Microsoft Windows 10 Enterprise LTSB/LTSC（2016/2019/2021） ※Windows Server Azure Edition はサポート対象外です。 ※Windows Installer 3.1 以上がインストールされている必要があります。 ※.NET Framework 4.7.2 以降がインストールされている必要があります。 ※Windows Server OS では以下の機能はサポート対象外です。 AssetView ボリューム暗号化機能 ※Windows 11（23H2/24H2/LTSC 2024）では以下の機能はサポート対象外です。 AssetView P WSUS 連携機能 ※Windows 10（1909/2004/20H2/21H1/21H2）は以下の機能についてのみサポート対象とします。 AssetView P ライセンス機能による 22H2 機能更新プログラムの適用 ※Windows 11 Home/Pro（21H2）は以下の機能についてのみサポート対象とします。 AssetView P ライセンス機能による 22H2/23H2/24H2 機能更新プログラムの適用 ※『Windows キオスクモード』を設定したクライアント端末はサポート対象外です。
CPU	OS 推奨値以上 ※Surface Arm 版（Microsoft SQ 搭載品）はサポート対象外です。 ※Copilot+ PC Arm 版（Snapdragon X 搭載品）はサポート対象外です。
メモリ	OS 推奨値以上 ※ AssetView クライアントが動作するに十分なメモリ容量が必要です。 メモリの空き容量が極端に少ない場合、OS の動作が極端に遅くなる可能性があります。
ディスク容量	AssetView クライアントのインストールには、システムドライブに 300MB 以上の空き容量が必要です。 AssetView Vplus ライセンスを有効にする場合は、システムドライブに 800MB 以上の空き容量が必要です。 AssetView P 更新管理機能を利用して機能更新プログラムを適用する場合は、システムドライブに 50GB 程度の空き容量を確保してください。内容は以下の通りです。 ・Windows の機能更新自体に必要な空き容量 ・ダウンロードした機能更新プログラムのファイル ・機能更新プログラムと同等のサイズの実行ファイル ・分散配布を利用している場合のキャッシュ
ディスプレイ	1024×768 以上の画面解像度で運用してください。

管理コンソール

OS	Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows 11 Enterprise（21H2/22H2/23H2/24H2） Microsoft Windows 11 Home/Pro（22H2/23H2/24H2） Microsoft Windows 10 Home/Pro/Enterprise（22H2） ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※.NET Framework 4.7.2 以降がインストールされている必要があります。 ※Visual Studio 2013 の Visual C++ 再頒布可能パッケージがインストールされている必要があります。 32bit 端末用と 64bit 端末用がありますので、管理コンソールをインストールするコンピューターに合った パッケージをインストールしてください。
CPU	OS推奨値以上　最小：2GHz 以上
メモリ	OS推奨値以上　最小：4GB以上
ディスク容量	管理コンソールのインストールには、システムドライブに 200MB 以上の空き容量が必要です。
ディスプレイ	1024×768 以上の画面解像度で運用してください。
Microsoft Office	Excel形式のエクスポート機能を利用する場合は、Microsoft Excel 2016以降または Microsft365がインストールされ、ライセンスが認証されている必要があります。

AssetView リモートデスクトップアドイン

OS	Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows 11 Enterprise（21H2/22H2/23H2/24H2） Microsoft Windows 11 Home/Pro（22H2/23H2/24H2） Microsoft Windows 10 Home/Pro/Enterprise（22H2） ※Windows Server Azure Edition はサポート対象外です。 ※Windows Installer 3.1 以上がインストールされている必要があります。 ※AssetView クライアントが起動している端末ではリモートデスクトップアドインは動作しません。
CPU	OS推奨値以上
メモリ	OS推奨値以上
ディスク容量	1MB 以上の空き容量が必要です。

ファイル転送Webサービス（Mac OS / Linux OS を管理する場合）

OS	Microsoft Windows Server 2025 Standard/Datacenter Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。
CPU	OS 推奨値以上　最小：クアッドコア Intel Xeon 2.33GHz 同等以上
メモリ	OS 推奨値以上　最小：4GB 以上
ディスク容量	システムドライブに 5MB 以上の空き容量が必要です。
IIS	IIS 7.0 以降

AssetView Mailサーバー

OS	Microsoft Windows Server 2025 Standard/Datacenter Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※.NET Framework 4.7.2 以降がインストールされている必要があります。 ※Visual Studio 2015、2017、2019、および 2022 用 Visual C++ 再頒布可能パッケージがインストール されている必要があります。
CPU	OS 推奨値以上　最小：クアッドコア Intel Xeon 2.33GHz 同等以上
メモリ	OS 推奨値以上　最小：4GB 以上
ディスク容量	Mail サーバーのインストールには、システムドライブに 70MB 以上の空き容量が必要です。 SPOOL フォルダー、PARTS フォルダーの配置先となるドライブは、 システムドライブ以外の十分な空き容量のあるローカルドライブを指定してください。
その他	Mail サーバー（サーバー側キャプチャ）を導入する場合、 導入するサーバーの TSO(TCP Segmentation Offload) を無効化してください。

AssetView F 管理コンソール

OS	Microsoft Windows 11 Enterprise（21H2/22H2/23H2/24H2） Microsoft Windows 11 Home/Pro（22H2/23H2/24H2） Microsoft Windows 10 Home/Pro/Enterprise（22H2） ※日本語版のみ対応 ※アップグレードした OS では、動作保証しておりません。 ※ARM 製や ARM ベースの CPU はご利用いただけません。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
Web ブラウザー	Microsoft Edge Google Chrome

AssetView F クライアント

OS	Microsoft Windows 11 Enterprise/Education（21H2/22H2/23H2/24H2） Microsoft Windows 11 Home/Pro（22H2/23H2/24H2） Microsoft Windows 10 Home/Pro/Pro for Workstations/Enterprise/Education（22H2） ※日本語版のみ対応 ※ARM 製や ARM ベースの CPU はご利用いただけません。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
ディスク容量	システムドライブに 120MB 以上の空き領域（エラーログ使用領域を除く）
Web ブラウザー	Microsoft Edge Mozilla Firefox /Firefox ESR Google Chrome
その他	クライアントモジュールをインストールする PC では、 インターネットに接続可能な環境、かつ DNS による名前解決ができる必要があります。

フィルタリングキャンセラ（Windows版）

OS	Windows 32 on Windows 64 (WOW64), 64bit アーキテクチャ ・Windows Server 2016 Standard ・Windows Server 2019 Standard ※日本語版のみ対応
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
Web ブラウザー	200MB 以上の空き領域（ログ使用領域を除く）

AssetView MDM クライアント（Windows）

OS	Microsoft Windows 11 Pro/Enterprise/Education（21H2/22H2/23H2） Microsoft Windows 10 Enterprise（21H2/22H2） Microsoft Windows 10 Pro（22H2） ※S モードでは本機能を利用できません。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
ディスク容量	システムドライブに 200MB 以上の空き領域 (エラーログ使用領域を除く)
ポート番号	TCP/443

AssetView MDM クライアント（iOS/iPadOS）

OS	iOS/iPadOS 13.6 以降（ADE）
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
ストレージ容量	9.5MB 以上の空き領域
ネットワーク要件	以下に準拠 https://support.apple.com/HT210060

AssetView MDM クライアント (AndroidTM)

OS	Android 8.0 OreoTM 以降 ※Oreo は Mondelez International, Inc. group の商標です。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
ストレージ容量	25MB 以上の空き領域
ネットワーク要件	以下に準拠 https://support.google.com/work/android/answer/10513641?hl=en

AssetView MDM Web管理画面

OS	Microsoft Windows 11 Pro/Enterprise/Education（21H2/22H2/23H2） Microsoft Windows 10 Enterprise（21H2/22H2） Microsoft Windows 10 Pro（22H2）
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
Web ブラウザー	Microsoft Edge（Chromium 版） Google Chrome

※Google 、Android 、Gmail 、Google Chrome 、およびその他のマークは Google LLC の商標です。

※Oreo は Mondelez International, Inc. group の商標です。

AssetView P サーバー

OS	Microsoft Windows Server 2025 Standard/Datacenter Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※ .NET Framework 4.7.2 以降がインストールされている必要があります。
CPU	OS 推奨値以上　最小：クアッドコア Intel Xeon 2.33GHz 同等以上
メモリ	OS 推奨値以上　最小：8GB 以上
ディスク容量	P サーバーのインストールには、システムドライブに1GB 以上の空き容量が必要です。 パッチ格納用フォルダーの配置先となるドライブは、システムドライブ以外に充分な空き容量（ユーザー P サーバーのダウンロード処理の設定で期間を最大値とし、すべての分類を選択の場合は 1TB 以上）のあるローカルドライブ（外付けドライブを除く）を指定してください。
その他	インストール時に AssetDB とは異なる AssetView P 専用データベースが導入されます。 AssetView 専用サーバーとすることを推奨します。AssetView ではバージョンアップや今後の機能追加等の理由によりサーバー OS の再起動が必要となる場合があります。他のシステム等と同居して運用する場合、処理速度や性能が低下する可能性があり、更に問題発生時には他のシステムと切り離した専用環境のご用意をお願いする場合があります。

AssetView P ミラーコンピューター

OS	Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows 11 Enterprise（21H2/22H2/23H2/24H2） Microsoft Windows 11 Home/Pro（22H2/23H2/24H2） Microsoft Windows 10 Home/Pro/Enterprise（22H2） ※Windows Server Azure Edition はサポート対象外です。 ※.NET Framework 4.7.2 以降がインストールされている必要があります。 ※バッテリー駆動時は動作保証していません。 ※AssetView クライアントとして A/D/P 機能が有効になっている必要があります。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上 最小：4GB 以上
ディスク容量	パッチ格納用フォルダーの配置先となるドライブは、対象となるパッチの分類により必要な空き容量（すべての分類を選択の場合は 1TB 以上）のあるローカルドライブ（外付けドライブを除く）を指定してください。

AssetView P WSUS連携ツール

OS	Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※Windows Installer 3.1 以上がインストールされている必要があります。 ※WSUS サーバー 6.3 以上がインストールされている必要があります。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
ディスク容量	20MB 以上の空き容量が必要です。
その他	WSUS データベースに連携用のログインユーザー (admin 権限) を作成します。

AssetView P Office 更新管理サービス

OS	Microsoft Windows Server 2022 Standard/Datacente Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※.NET Framework 4.7.2 以降がインストールされている必要があります。 ※データベースサーバー、管理コンソール、クライアント端末と通信できる必要があります。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
ディスク容量	インストール先に 100MB 以上の空き容量が必要です。また、ダウンロードする ({製品・種別 (32bit/64bit)・チャネル・世代} +1) ごとに 3GB 程度の容量が必要です。

AssetView 稼働環境　下記システム要件を満たすPC/AT互換機で動作します。

※アプリケーションや環境によって制限事項がございます。詳細は営業担当までご確認ください。

Mac OS 稼働環境

AssetView クライアント（Mac OS版）

OS	macOS 15 Sonoma(64bit) macOS 14 Sonoma(64bit) macOS 13 Ventura (64bit) macOS 12 Monterey (64bit) macOS 11 Big Sur (64bit)
HDD 容量	10MB 以上の空き容量が必要です。

Linux 稼働環境

AssetView クライアント（Linux OS版）

OS	Redhat Enterprise Linux 6(i386) Cent OS 6(i386) Red Hat Enterprise Linux 6(x86_64) Red Hat Enterprise Linux 7(x86_64) Red Hat Enterprise Linux 8(x86_64) Red Hat Enterprise Linux 9(x86_64) Cent OS 6(x86_64) Cent OS 7(x86_64) Cent OS 8(x86_64)
HDD 容量	5MB 以上の空き容量が必要です。

AssetView アーカイブ 稼動環境

サーバー

OS	Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※.NET Framework 4.7.2 以上がインストールされている必要があります。 ※32bit 版 OS には対応しておりません。
CPU	Intel Core i5 2.4GHz 以上　推奨：クアッドコア Intel Xeon 2.33GHz 以上
メモリ	推奨：16GB 以上
HDD 容量	アーカイブサーバーのインストールには、システムドライブに 40MB 以上の空き容量が必要です。 アーカイブデータの出力先がローカルディスクを指定している場合、作成されるアーカイブデータの容量に従い空き容量が必要になります。
AssetView データベース	AssetView Ver.13.2.0 以降 ※その他バージョンは動作保証外です。
AssetView	アプリケーションサーバー（メンテナンス処理を実行するサーバー）がインストールされている必要があります。 ログデータ保存期間の設定で［クライアント端末でログデータを取得した日時を基準にする］をオンにする必要があります。

管理コンソール

OS	Microsoft Windows Server 2022 Standard/Datacenter Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows 11 Enterprise（21H2/22H2/23H2） Microsoft Windows 11 Pro（22H2/23H2） Microsoft Windows 10 Pro/Enterprise（22H2） ※Windows Server Azure Edition はサポート対象外です。 ※アップグレードした OS ではサポート対象外です。 ※.NET Framework 4.7.2 以上がインストールされている必要があります。
CPU	OS推奨値以上　推奨：2GHz 以上
メモリ	OS推奨値以上　推奨：4GB 以上
HDD 容量	アーカイブ管理コンソールのインストールには、システムドライブに 20MB 以上の空き容量が必要です。
ディスプレイ	960×720 以上の画面解像度で運用してください。

Memo