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。

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 新宿TXビル3F
TEL 03-5291-6121　FAX 03-5291-6122

札幌営業所 〒060-0052 北海道札幌市中央区南2条東2-16 昭尾ビル3F
TEL 011-211-0957

名古屋営業所 〒460-0008 愛知県名古屋市中区栄2-9-5 アーク栄東海ビル5F
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 n_sales@hammock.co.jp　URL https://www.hammock.jp

お問い合わせ

RIAGROUP 株式会社リアテック

大阪府大阪市北区天神橋１－９－５　山西屋西孫ビル7、8階

☎ 06-6356-9250 （9：00～17：30）

riatec@riatec.co.jp

https://www.riatec.co.jp

※このカタログは 2019 年 4 月現在のものです。

04152019

製品のご販売、お問合せは

HAMMOCK

ITの管理スタイルの数だけ、変幻自在！

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

機能もサービスも、オーダーメイド感覚

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。

共通機能

AssetView 共通 共通機能

- IT統合管理
- 自動レポート
- 自動バックアップ
- 自動バージョンアップ
- ナビゲーション
- メッセージ配信
- 電源管理（vPro / WOL）

単体導入が可能 / スタンダードパッケージ

AssetView A IT資産管理

- ハードウェア情報取得・管理
- アプリケーション情報取得・管理
- ライセンス管理
- アンケート実施
- ソフトウェア資産管理台帳
- ライセンス利用申請
- 死活監視

オプション
- ソフトウェア辞書

P.16

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
- 設定変更
- シャットダウン / 再起動の自動実行
- PC 操作自動実行（マクロメーション機能）
- マルチキャスト配信

P.20

セキュリティパッケージ

AssetView M PC操作ログ管理

- PC 操作ログ収集
- ファイル操作追跡
- プログラム起動警告／禁止
- ファイル操作警告／禁止
- 稼働状況グラフ表示
- 簡易 Web フィルタリング

P.24

AssetView I 個人情報検索

- 個人情報ファイル検索
- 機密情報ファイル検索
- 特定個人情報ファイル検索

P.28

AssetView G デバイス制御

- USB デバイス情報取得・管理
- USB デバイス接続警告
- デバイス制御
- デバイス使用申請

P.30

AssetView S 不正PC遮断

- 不正 PC 検知
- 不正 PC 遮断
- ネットワーク機器自動登録

P.32

AssetView RC リモートコンソール

- リモート操作
- ファイル転送
- ペイントモード

P.33

単体導入が可能

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
- 高精度データベース自動更新
- プログラム通信制御
- 書き込みサイズ指定制御

P.34

AssetView K ファイル制御・暗号化

- 社外ファイル制御
- 社外ファイル削除
- 社外ファイル操作追跡
- ファイル暗号化

P.36

AssetView V ウイルス対策

- ウイルススキャン
- リアルタイムモニタリング
- USB デバイス自動スキャン

P.38

AssetView W 未知の脅威対策

- ふるまい検知
- ランサムウェア対策
- アンチスパム対策
- フィッシング対策
- 未知の脅威対策ダッシュボード

P.40

AssetView P PC更新管理

- Windows 10 展開リング管理
- Windows Update 設定 /DO 設定の可視化・コントロール
- Windows 10 プログラム管理・配信・即時実行
- 複数方式のネットワーク負荷分散配布
- 他ベンダーアプリケーションのアップデート

P.42

AssetView Mail 電子メール監視

- 送信メールログ収集
- 添付ファイルの保存

P.44

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

P.46

AssetView MDM スマートデバイス管理

- iOS / Android デバイス情報管理
- リモートロック / リモートワイプ
- アプリ制御 / 設定
- パスコード制限 / 消去

P.48

オプション

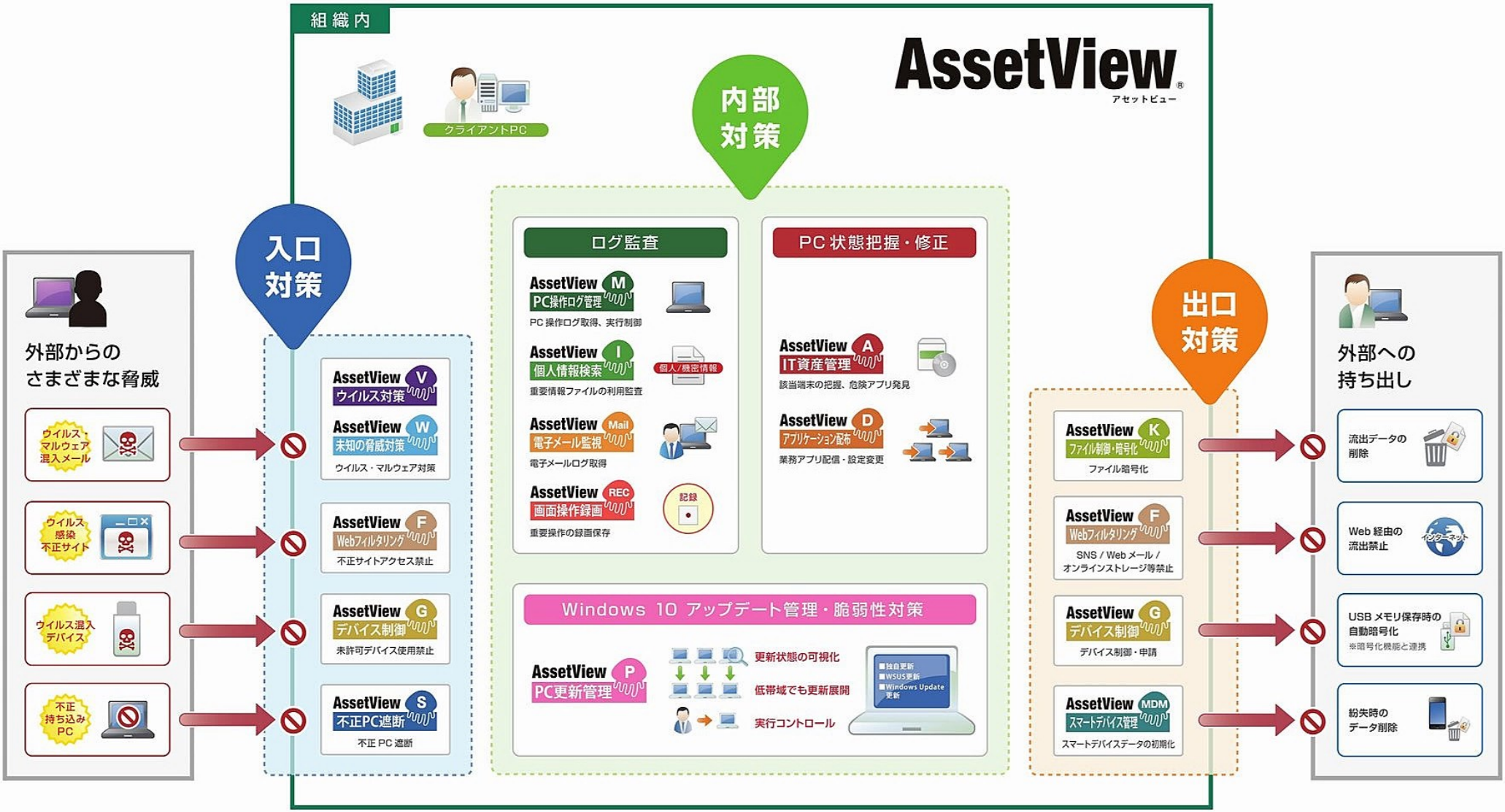
AssetView アーカイブ 高速ログ検索/長期保存

- 高速ログ検索
- 長期保管

P.50

PCの管理・セキュリティ対策を包括的に実現

PCを使った業務が標準になったこの時代において、情報システム部門のPC対応業務の幅は日々広がり続けています。
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。



低コスト&トータルサポート

必要最小限のコストで最大限の効果を発揮

導入する機能を選べるから、コストも削減

必要な機能やサービスのみを、必要なライセンス数だけ購入できるので、コストを最小限に抑えられます。

AssetView A IT資産管理 ＋ AssetView M PC操作ログ管理

一般的なオールインワンパッケージソフトウェア　選択型パッケージソフトウェアとサービスの組み合わせ

まとめて導入しても低コスト

特別価格のパッケージとしてIT統合管理のためにお客様ニーズが特に高い7機能、ソフトウェア辞書オプションをまとめた『AssetView スタンダードパッケージ』、情報漏洩対策に特化した『セキュリティパッケージ』をご用意しています。

AssetView スタンダードパッケージ

- AssetView A IT資産管理
- A オプション ●ソフトウェア辞書
- AssetView D アプリケーション配布
- AssetView G デバイス制御
- AssetView M PC操作ログ管理
- AssetView S 不正PC遮断
- AssetView I 個人情報検索
- AssetView RC リモートコンソール

AssetView セキュリティパッケージ

- AssetView M PC操作ログ管理
- AssetView I 個人情報検索
- AssetView G デバイス制御

段階導入で着実なステップアップをサポート

課題に応じたパッケージソフトウェアやサービスを段階的に導入可能 ライセンス数の追加も柔軟

社内の管理状況や計画に応じた段階導入を実現できるため、着実なステップアップが可能です。

STEP 1　IT資産管理をスタート

STEP 2　セキュリティ対策を強化　追加機能を導入

※機能の追加導入展開はライセンスキーの登録のみでOK。詳しくはP.11をご覧ください。

ポイント

ライセンスを数回に分けて追加購入する場合も、常に保有するトータルのライセンス数のレンジ価格が適用される（ライセンスが増えるほど安価になる）ため、段階的な導入において無駄な投資をすることはありません。

※例えば、初年度150ライセンス、次年度50ライセンス購入した場合は、次年度の導入時に200（150+50）ライセンスの価格が適用されます。

構築、導入、運用アウトソーシング、サポートまで、幅広く支援

検討

資料ダウンロード / 資料請求、ご購入前のお問い合わせ

資料請求、資料ダウンロードを各専用フォームより、ご購入前のお問い合わせをお電話・お問い合わせフォームで受け付けています。

評価版 / 評価機貸し出しサービス

製品をお試しいただけます。ご希望の運用をヒアリングして、使い方や活用例のご案内もあわせてご提示します。

技術セミナー開催（検討 / 運用段階の方向け）

AssetView 各機能や、テーマにわけた活用実例などを盛り込んだ、実技操作体験型のセミナーを開催しています。ぜひご参加ください。

導入

導入支援訪問サービス（導入・操作説明）

ご利用の準備が丸ごと詰まったスターターサービス。お客様ご自身でも導入は可能ですが、効果的なご利用にはこちらがおすすめです。

運用

技術的なお問い合わせ（ヘルプデスクサービス）

ご購入後の技術的なお問い合わせは、お電話・お問い合わせフォームからのメールサポートで受け付いたします。

保守契約ユーザー様専用 Web サイト

製品バージョンアップ用プログラムのご提供や、FAQ、トラブルシューティング等をまとめた専用 Web サイトをご提供します。

最新情報ご提供サービス（Express）

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

リモートサポートサービス

お客様の PC をリモート操作して、操作の案内、トラブル解決します。保守ユーザ様専用 Web サイトから受け付けします。

オンサイトサポートサービス

バージョンアップ方法、活用方法、ご担当者様の変更によるスタート支援などをご相談ください。ご要望に応じた運用支援をご提案いたします。

製品の価格、ライセンス、保守内容に関するお問い合わせ
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）

製品の機能、使い方に関する技術的なお問い合わせ
0120-994577
海外・携帯電話・PHS からは 03-5291-6137
平日 9:00 ～ 12:00、13:00 ～ 17:00（弊社休業日を除く）

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。

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

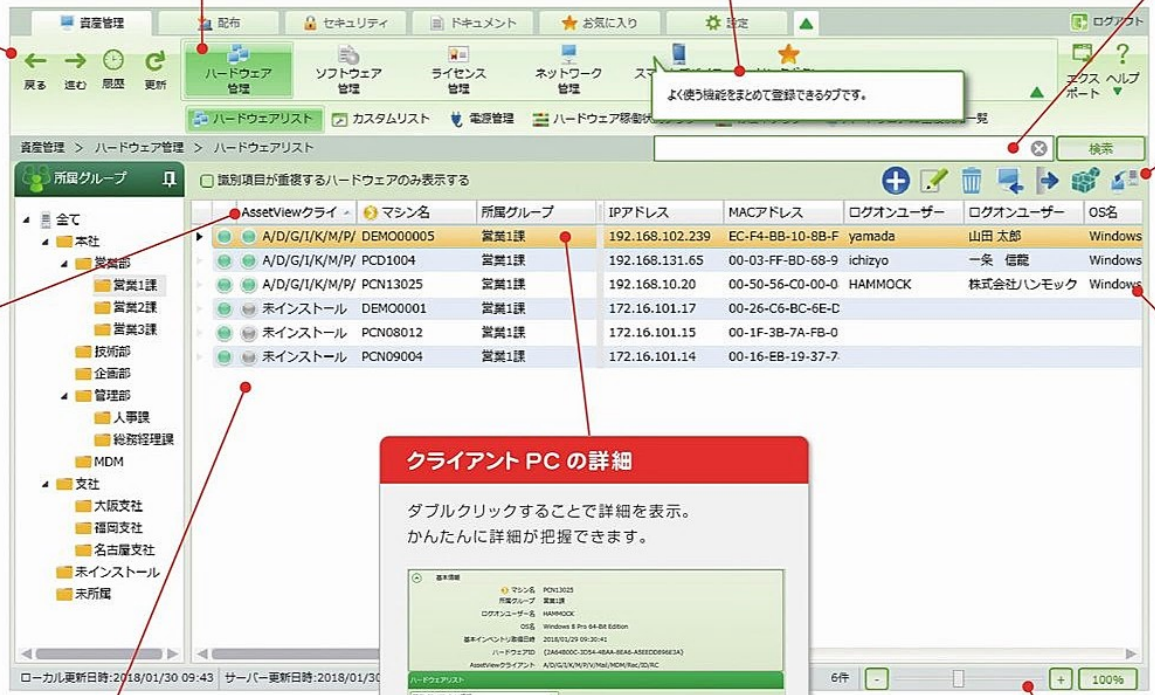
機能ボタンに、カーソルをあわせることで、
どんな機能で何ができるのかが表示されます。

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。

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。

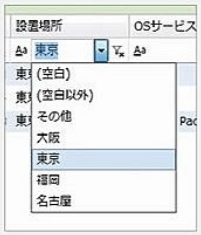


頻度の高い操作は
アイコンからワンクリック

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。

使いやすい

権限委譲することで分散管理が可能

利用できる機能、対象グループ、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可能です。

所属グループの PC やソフトウェア
ライセンスの管理を担当

PC 情報の閲覧とリモート接続で
社内問い合わせ対応を担当

社員の PC 操作状況の把握と
個人情報の取り扱い管理を担当

所属グループのクライアント PC のみ
情報閲覧・管理が可能

社内にあるすべてのクライアント PC の
情報閲覧・管理が可能

必要な機能だけを表示、操作に迷いません

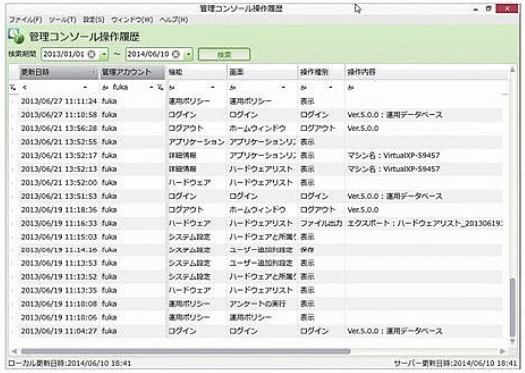
IT の管理スタイルに合わせて表示させる機能を変更可能です。
利用者に応じた管理スタイルで不要な画面、機能を表示しないことで迷うことなく目的達成ができます。

例 設定例
- ソフトウェアのライセンス管理だけを管理するシステム担当者
- 営業部の PC 操作ログだけを管理したい営業部のマネージャー
- ウイルス対策、不正 PC 遮断だけを管理したいセキュリティ管理者　　など

▼例：ソフトウェアのライセンス管理だけを管理するシステム担当者向けに設定した管理画面

アカウント別の管理コンソール操作履歴

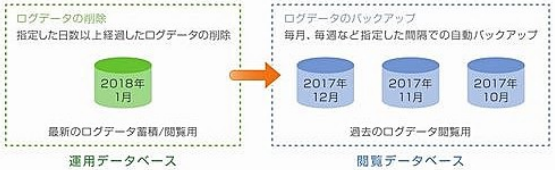
権限委譲したユーザーがどのような操作をしたのかを記録できます。監査への対応、不正操作の有無の把握に役立ちます。



さらに運用の負担を削減する自動化の仕組み

自動ログローテーション

運用データベース・閲覧データベースという2つのデータベース構造によりレスポンスの高い運用を実現。ログデータのバックアップと、ログデータの削除をあらかじめ設定したスケジュールで自動実行します。高価な専用ツールの追加購入は不要です。



自動バージョンアップ

AssetView クライアントのバージョンアップや機能追加は、管理コンソールから行なえます。「自動更新する」項目にチェックしておけば、クライアント PC の起動状況によって自動でバージョンアップされます。

ここにチェックがあれば、クライアントのインストーラーを登録するだけで自動的にバージョンアップ

機能追加もかんたん

ライセンスキーを登録する

ライセンスキーを登録するだけで追加した機能が有効になります。

通信負荷を軽減する帯域調整機能＆通信圧縮機能を搭載

「ネットワークの帯域を○○%しか使わない」、「通信の圧縮レベル」を設定できます。ネットワークに与える影響を最小限にした運用が可能です。

購入ライセンス数やバージョン、有効にしている機能も一目でわかります。

すぐに使える

わずかなステップで導入完了

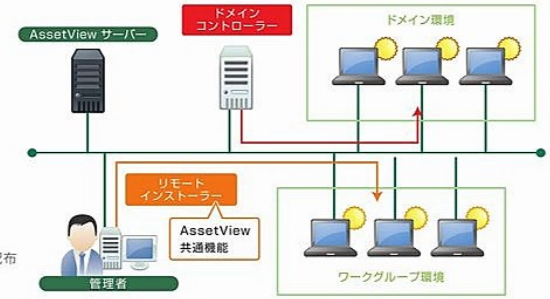
ステップ１　環境構築

サーバーの準備
Assetview 専用データベース、
AssetView サーバープログラムの導入

管理 PC の準備
管理コンソールの導入

クライアント PC の準備
管理したい PC に AssetView クライアントプログラムの導入

- リモートインストール
- Active Directory によるアプリケーション配布
- 手動でのインストール



ステップ２　クライアントPCを管理するグループ作成

グループ管理

クライアント PC を、グループに分けて管理することができます。営業部、技術部といった組織単位で管理者を置いて管理するなど柔軟な運用が可能です。

Active Directory 連携

AssetView でクライアント PC を管理するためのグループ情報に、Active Directory の「組織単位（OU）」情報をインポートすることができます。新規導入時だけでなく、組織変更の際に必要な設定変更の作業を効率化します。

グループを自動で振り分け

クライアント PC から自動収集したマシン名や IP アドレス等のインベントリ情報をもとに、拠点や部署ごとに自動でグループを振り分けます。ユーザーからのアンケート回答結果を振り分けに活用することも可能です。

ポイント

クライアント PC 側でアンケートに答えるだけで、自動的に所属グループに振り分けられます。

アンケート機能

以下の情報をユーザーから収集できます。

- 所属部署
- 氏名
- 氏名（ふりがな）
- メールアドレス

※AssetView A があれば、任意で項目を設定することも可能

ステップ３　IT機器管理台帳の作成

さまざまな機器をまとめて AssetView で台帳管理。

ネットワーク機器
プリンターやルーター等、ネットワーク参加している機器は台帳に自動追加します。

スタンドアロンPC
ネットワーク接続できないクライアント PC は、USB デバイスを経由したログデータ収集＆運用ポリシー適用で運用できます。

その他の機器
資産管理台帳として管理したい項目は手動での機器追加できます。

クライアント PC はもちろん、
それ以外のさまざまな機器の一元管理が可能です。

※手動追加した機器の情報は自動収取できないため、個別に情報を追加・更新する必要があります。

運用のための設定もかんたん

ナビゲーション

さまざまな機能を『コンプライアンス』と『セキュリティ』のカテゴリに分類し、それぞれ「通常設定」と「厳重設定」といった運用レベルの設定を、専門的な知識がなくてもかんたんに適用することができます。

インベントリ情報や操作ログの収集などの基本的な内容のほかに、１つ１つ設定していくには面倒なセキュリティ対策の細かい設定も選択した運用レベルに合わせて自動で行います。ナビゲーションは運用スタート時だけではなく、任意のタイミングで実行することができます。

ポイント

ナビゲーションを実行することで約 100 種類の注意プログラムを自動登録。

例 ナビゲーションを利用して運用スタート

運用レベルを選ぶだけで設定が適用されます。

セキュリティ設定画面　　コンプライアンス設定画面

不正プログラム対策	**セキュリティ「通常設定」では主に警告のみ「厳重設定」では主に起動禁止の設定を行います。** 下記 10 カテゴリで約 100 種類を自動的に登録。 ファイル共有(Winny等のP2Pツール)・5ちゃんねるビューア・ソフトウェア転送(FTP通信ツール等)・メッセンジャー・skype・音楽/映像・GAME(Windows標準)・GAME(オンラインゲーム)・ブラウザー・インストーラー（プログラムの設定アップを監視可能）
インターネットの私的利用対策	**私的利用と想定できる文字列約 50 種類を自動的に登録します。** 例：5 ちゃんねる、5ch、blog　など

※詳細設定後にナビゲーションを実行すると、ナビゲーションの設定内容で設定が上書きされるものもあります。

運用ポリシー設定

目的別に統合された設定画面は、操作に迷うことはありません。
わかりやすい表現で、専門知識がなくてもかんたんに運用ができます。

導入支援サービス

ご利用の準備が丸ごと詰まったスターターサービス。お客様ご自身でも導入は可能ですが、効果的なご利用にはこちらがおすすめです。お客様のご運用をヒアリングさせていただき、最適な利用 / 設定 / 運用方法をご提案します。

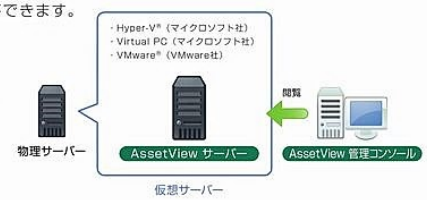
多様化するIT環境に対応

サーバー仮想環境に対応

AssetView はサーバー仮想環境をサポートしています。AssetView サーバーモジュールを仮想環境に構築すれば、初期投資や維持コストの削減、メンテナンス時の作業工数を削減することができます。

ポイント

AssetView サーバーを仮想化すれば、サーバーのシステムクラッシュなどの際に、高速に過去のサーバー環境への復元ができます。



シンクライアント対応

さまざまな方式が存在するシンクライアントPCの管理が可能

情報漏洩防止・コスト削減・内部統制強化といった多くのメリットがあり、導入する企業も増えたシンクライアントシステム。AssetView はさまざまなシンクライアント環境に対応しています。

●VDI（仮想マシン）

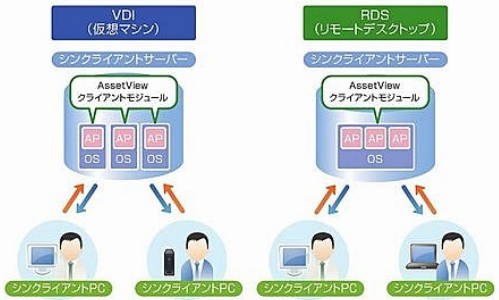
AssetView では、仮想マシンはサーバー（ホスト OS）とは独立したクライアント PC として認識されます。

●RDS（リモート デスクトップ）

クライアントからサーバーにリモートでログオンして操作します。シンクライアント PC がリモートデスクトップ環境で行った操作ログは、シンクライアントサーバーにインストールされた AssetView クライアントから取得されます。

●RemoteApp（公開アプリケーション）

公開アプリケーションのプロセスログ、ファイル操作ログは、シンクライアントサーバーにインストールされた AssetView クライアントから取得されます。ウィンドウタイトルログは、各シンクライアントにインストールされた AssetView クライアントが取得します。



ポイント

HYPER-V®やリモートデスクトップ接続など、クライアント側で起動しているシンクライアントアプリケーションのウィンドウタイトルログから、「どのPC」が「どんな仮想マシンを起動していたのか」「どのサーバーにリモート接続していたのか」を確認することができます。

※ブレード PC、ネットワークブート方式についてはご相談ください。

インテル® vPro™ テクノロジーとWOLに対応

自動インストール、ファイル配布等の機能を持った AssetView D や、リモート接続が可能な AssetView RC と組み合わせることにより、クライアント PC の効率的で、フレキシブルな管理を実現します。

インテル® リモートKVM 機能に対応

BIOS画面やブルースクリーン、電源OFF状態からのリモート接続が可能です。

ハードウェアリスト（クライアントPCの一覧）から、右クリックでかんたんに操作可能 ▶

グローバル対応

日本語以外の環境に対応

管理コンソール　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インストール時に日本語・英語・中国語（簡体）のいずれかから選択することができます。

英語、中国語（簡体）での運用が可能　対応製品 A D M I G S RC

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が実現できます。

※AssetView RC、マクロメーション機能は日本語か英語のいずれかになります。

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　対応製品 M G

クライアント PC のシステム設定内にある「地域と言語」に合わせて、警告メッセージを変更できるため、言語特有の表現方法やセキュリティレベルにあわせた運用が可能です。

クライアントPCの言語設定に合わせて、英語OS、日本語OS、中国語OS、それぞれのメッセージを設定することが可能です。

クライアントPC　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。

※通常はインストールした OS の言語が初期設定の形式となっています。日本語、中国語以外の環境では英語となります。

対応製品 A D M G

対応する機能

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

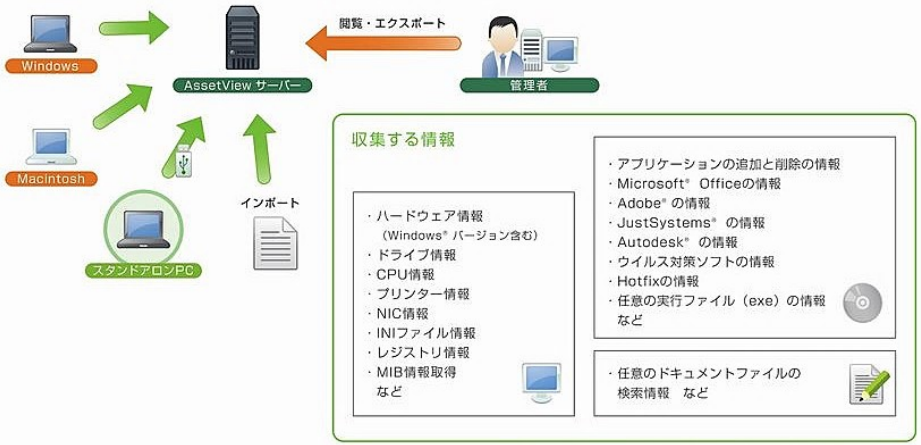
IT資産管理

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。

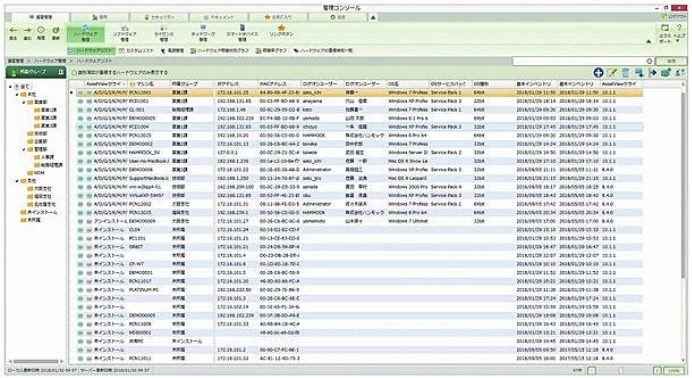
70種類以上ものインベントリ情報を手間をかけずに自動収集

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。



※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。

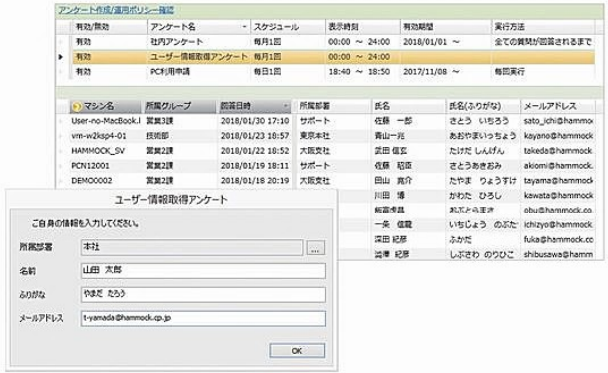


AssetView A IT資産管理

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。



ソフトウェアのインストール状況を把握、ライセンスの最適配置を実現

ソフトウェア情報収集

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。ソフトウェアごとのインストール台数、プロダクト ID やバージョンを一覧で把握。

ネットワーク機器の監視を行って一元管理を実現

IP アドレスの範囲を指定して、ネットワーク機器の死活監視、情報収集（SNMP）ができます。

例 運用例

死活監視の結果、応答がないプリンターを発見。
メッセージ配信機能、デスクトップ付箋機能を使って利用者に状況共有および利用できるプリンターの案内をすることで業務への影響を最小限にします。

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。

ハードウェア台帳

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

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
○○オフィス2014	5	2	2	4	1
○○オフィス2012	0				

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。

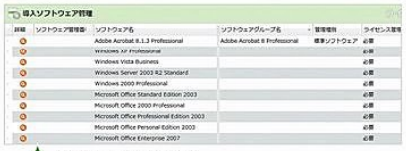
ポイント
承認後、自動割当されるため手間なく適切な管理を実現。
手作業の登録作業でありがちな、ソフトウェア名の差異による管理ミスも防止します。

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）
- 10万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

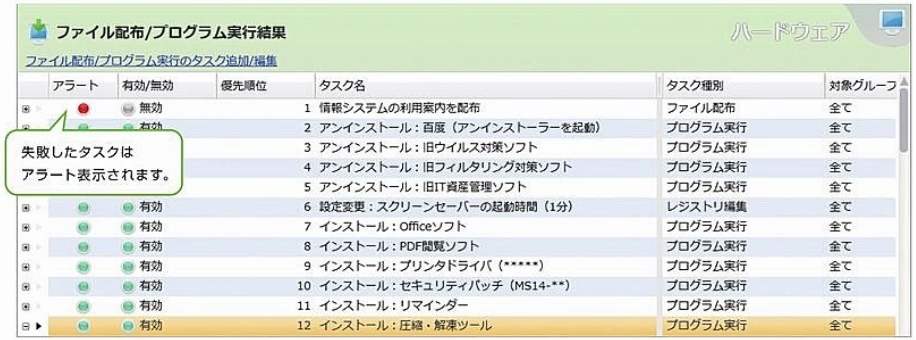
アプリケーションインストールと設定変更も自動化して効率アップ。

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
		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
		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
		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

AssetView D アプリケーション配布

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。実施の条件、実施内容をウィザードに従って進めるだけで誰でもかんたんに思い通りのプランを作成することができます。

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。

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

自動展開用スクリプトのご提供（保守ユーザー様専用ページ）

各種アプリケーションのインストール、アンインストールスクリプトをご提供。かんたんに自動化の設定をすることができます。

アプリケーション配布

AssetView D 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

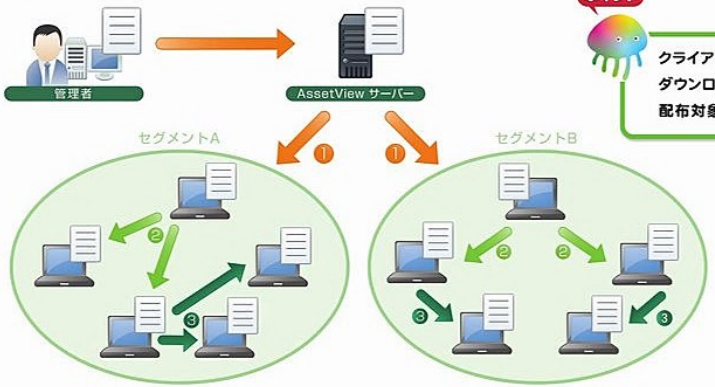
ネットワークに負荷を与えない、運用性と精度の高いアプリケーション配布を行うための通信インフラを標準搭載しています。
クライアント PC の設定変更が不可欠な Microsoft® Windows Server® Update Services (WSUS) も
AssetView D との連携でかんたんに設定コントロールが可能です。

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



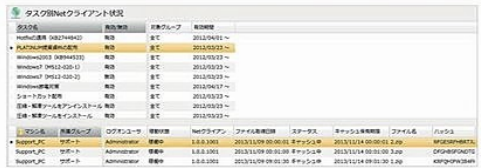
ポイント

クライアントPCが自律的にダウンロードすべき配布対象を判定します。

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。

WSUS連携でWindowsパッチ適用の実施タイミングを自在にコントロール

Microsoft® Windows Server® Update Services (WSUS) を利用するにはクライアント PC の設定変更が不可欠です。
AssetView D と連携してクライアントの設定コントロールがかんたんに行えます。

- **アクセスが集中しない時間帯に Windows Update を実施する分散運用**
  Windows Update の定期実行設定をグループ、クライアント単位で設定できます。多彩な実行タイミング設定が可能です。
  OS 起動時 / ログオン時 / タスクランチャーで実行(ユーザー任意のタイミング) / 指定時間でランダムに開始(毎日、毎週、毎月といったスケジュール化)
- **Windows Update の即時実行**
  クライアント PC やグループを指定した Windows Update の即時実行が可能です。

ファイル配布 / プログラム実行結果と一元的に把握可能

WSUS 連携機能

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。

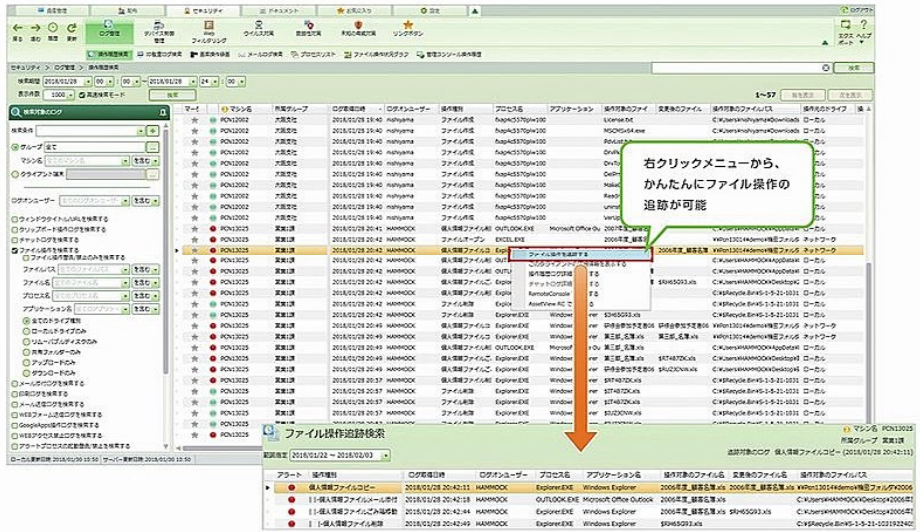
AssetView M
PC操作ログ管理

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。問題のある操作はグラフ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します。 ・AssetView クライアント起動（PC 起動）　・スリープ解除　・OS シャットダウン ・OS ログオン　・スクリーンセーバー　・ロック ・OS ログオフ　・スクリーンセーバー解除　・アンロック ・スリープ　・OS シャットダウン要求
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します。 ・操作対象のファイル名　・変更後のファイル名　・コピー / 移動先のドライブ種別 ・操作対象のファイルパス　・プロセス名　・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
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　・HTTP（S）ファイルアップロードログ（Internet Explorer の場合）
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
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 ※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します。 ・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）
クリップボード操作	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
チャットメッセージ	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。
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します。 ・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します。 ・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	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します。 ・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
Google Apps 操作	Google Chrome で操作した Google Apps の情報を取得します。 ・Google ドライブ　・Google カレンダー ・Gmail　・Google グループ

※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

AssetView M
PC操作ログ管理

不正な操作には警告。
ユーザーの意識向上を促します。

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時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。

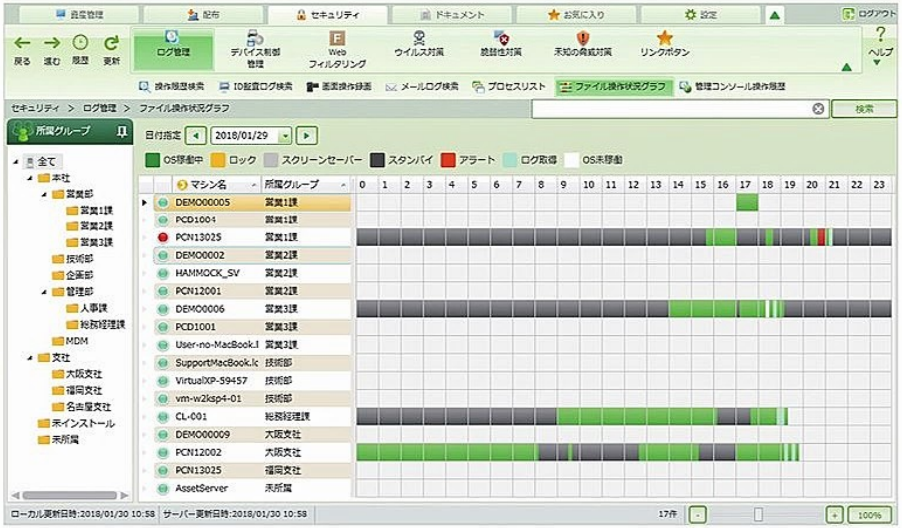
不正な操作の禁止、警告、抑止により利用者のセキュリティ意識を向上

不正な操作の禁止
- アプリケーションの起動
- Webサイトへのアクセス
- ファイル操作の検知

不正な操作への警告
- アプリケーションの起動
- アプリケーションの停止
- ウィンドウタイトルの検知
- ファイル操作の検知

特定操作の抑止
- 右クリック禁止
- キー操作禁止
- クリップボード禁止（画像）
- クリップボード禁止（文字列）

ファイル操作状況をグラフィカルに表示

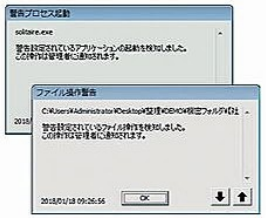


不正操作禁止・警告で問題を未然に解決

クライアントPC上のさまざまな不正操作を禁止したり、クライアントPCに警告メッセージを表示することが可能です。
問題がある不正操作はアラートとして管理者へ通知（メール）します。
また、クライアントPCに警告メッセージを表示させることで抑止力を効果的に発揮することができます。

例 警告メッセージ

例 禁止メッセージ



ユーザーの不正なアプリケーション利用を阻止します。
起動しようとして止められた、というログも反映します。

ポイント
約100種類の注意アプリを自動で登録して警告、禁止

不正なWebサイトへのアクセスを禁止

簡易Webフィルタリング

事前に登録したURLへのアクセスを禁止します。
リダイレクト先を指定できるため、組織でのWeb閲覧ポリシーを表示するポータルサイトへリダイレクトさせてセキュリティ意識を高める、といった使い方が可能です。

禁止URL
- SNS: Facebook, Twitter, mixi, LINE
- オンラインストレージ: Dropbox, SkyDrive
- Webメール: Gmail, Yahooメール

高精細なフィルタリングは、AssetView F で対応可能。
- 柔軟なフィルタリング設定（許可、書き込み規制、規制）
- 高精度なURLデータベース
- カテゴリ別のフィルタリング

AssetView F Webフィルタリング

個人情報検索

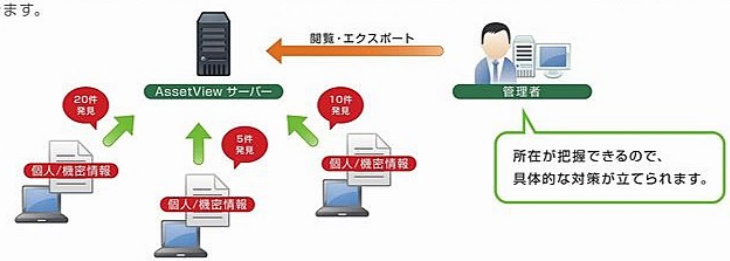
AssetView I 個人情報検索

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。



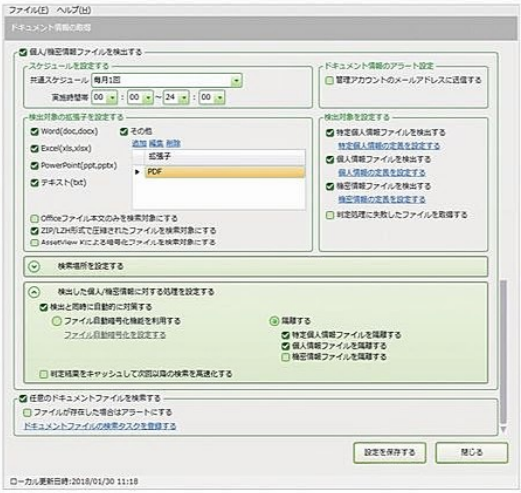
社内のクライアントPCに存在する個人情報、機密情報が含まれるファイルをファイル内までチェックして検索します。
個人情報だけでなく、重要なキーワードを含むファイルを機密情報ファイルとして定義できます。
さらに、検索されたファイルに対して、隔離、削除、完全削除、対象外の操作が可能です。

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。

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。



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

- 名前
- 住所
- 電話番号
- メールアドレス
- ユーザー辞書（個人情報として扱う文字列を追加）

機密情報ファイル

ユーザー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

AssetView G 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。

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（Bluetooth接続）

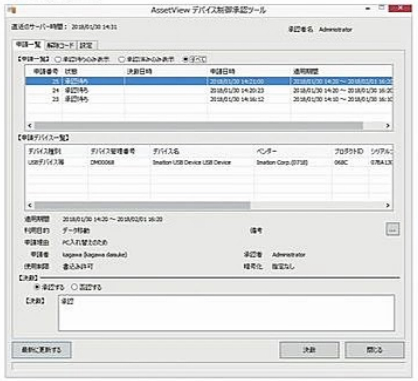
スマートフォンと PC 間のデータ通信に使われる Bluetooth 接続も PC 側で利用を制御することができます。

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PCは ネットワークに接続できません。

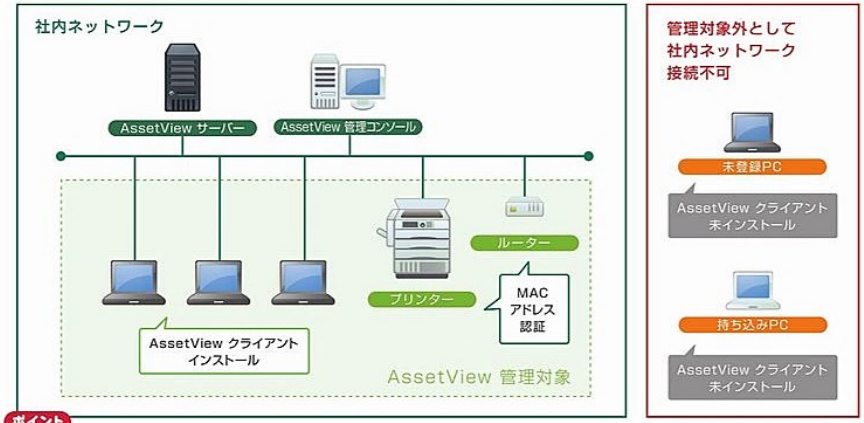
AssetView は、ネットワークに新しい機器を導入せずにソフトウェアによる遮断を実現しました。
管理されていないPCがネットワークに接続されたら検知、遮断し、情報漏洩やウイルス感染などのリスクを防ぎます。

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

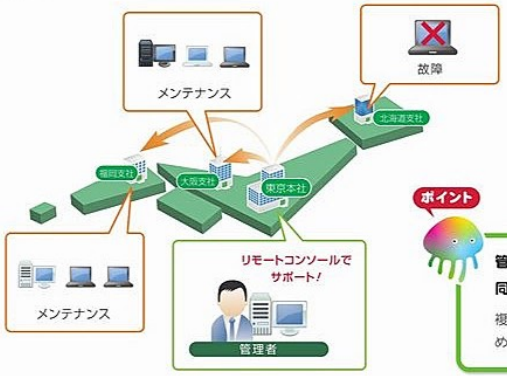
AssetView RC リモートコンソール

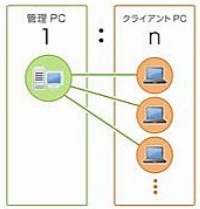
遠隔地のクライアント PC をリモート操作。 メンテナンスをサポートします。

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

管理 PC から複数台のクライアント PC への同時接続・監視を実現。

複数台同時選択の場合、表示順に連続処理を行うため、ネットワーク負荷も最小限に抑えられます。

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。

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 32 億 9888 万コンテンツ

カテゴリ数 82（ユーザー設定：5）　（2018 年 7 月 2 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

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。

- 「Kid ´s i モードフィルタ」「i モードフィルタ」「sp モードフィルタ」（株式会社エヌ・ティ・ティ・ドコモ）
- 「EZ 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」（ソフトバンク株式会社）
- 「有害サイトアクセス制限サービス」（ソフトバンク株式会社）
- 「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

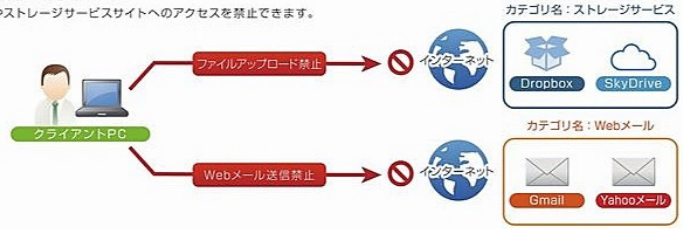
カテゴリごとに設定が可能なため、例えば SNS・ブログの閲覧は許可、書込みは禁止、という設定ができます。
HTTPS サイトであっても、対策が可能です。

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

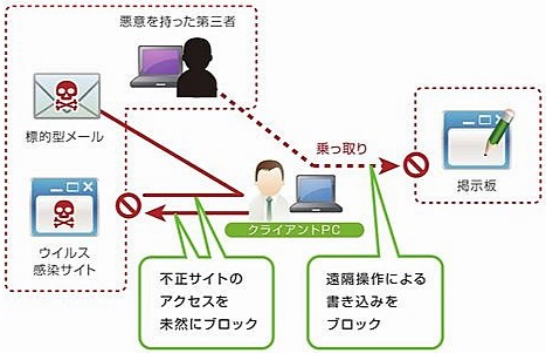
Web メールサイトやストレージサービスサイトへのアクセスを禁止することで、情報流出リスクの回避を実現できます。
HTTPS サイトであっても対策が可能です。

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。



ウイルス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、ウイルス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、ウイルス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、ウイルス感染予防になります。



ファイル制御・暗号化

AssetView K
ファイル制御・暗号化

ファイルの受け渡しリスクを解消。
ファイルが外部に流出しても『追跡』して『削除』。

インターネット上に公開された情報漏洩インシデントは、管理ミス、誤操作、紛失などによる、
「人」が原因の情報漏洩が約９割を占めると言われています。
ファイルが流出しても、中身が読めないようにする暗号化を活用することで、十分な対策をとることができます。

まったく新しい仕組みの暗号化

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

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

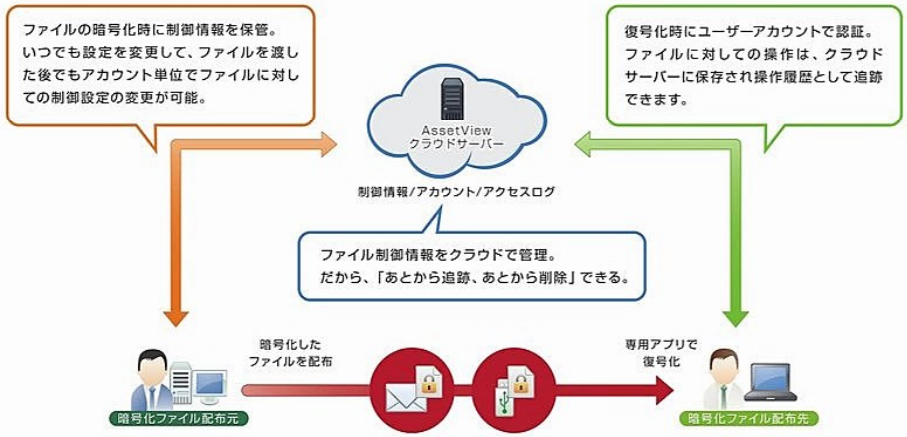
どこで開いても追跡

アクセスログの確認
- いつ？
- どのファイルに？
- 誰が？
- 何をした？

渡したファイルをあとから削除

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

ファイルが外部に流出しても「追跡」して「削除」できる仕組み



渡したファイルを『守る』

重要ファイルを持ち出す際、ファイル単位で暗号化。
ファイルに制御設定を行うことで重要ファイルの情報漏洩を防止します。

ファイルへの制御
- アカウント指定でのアクセス制御
- 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

渡したファイルを後から『追跡』

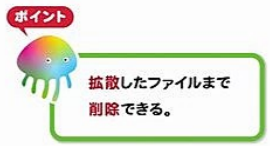
制御･暗号化したファイルへのアクセスは、操作履歴情報としてクラウドサーバーに保存。
管理コンソールを利用して操作履歴情報を把握し証跡管理を実現します。

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

ファイルアクセス時のユーザーアカウント / 接続元IPアドレス が判明

渡したファイルを後から『削除』

ファイルが社外の人物に渡った後でも、
管理コンソールから削除したいファイルを指定すれば、
クラウドサーバー経由で該当するファイルを削除できます。



ウイルス対策

POWERED BY KASPERSKY

vb 100 VIRUS virusbtn.com

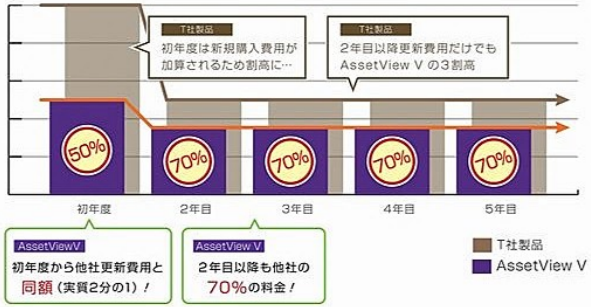
既存のウイルス対策ソフトを乗り換え。高い検知力のカスペルスキーエンジン。

近年、標的型攻撃に代表される新しい手法によるウイルス混入で重要情報(知的財産、顧客情報等)が狙われる事件が多発しています。標的型攻撃によるサイバー攻撃対策には多層の防御が必要ですが、その対策の基本はウイルス対策です。ウイルス対策は高検知力、高パフォーマンスな製品導入と最新情報の維持が重要です。

既存製品維持コストより安価に乗り換え、運用が可能

安価なライセンス形態

初期導入費が他社更新費用と同額なため、既存のウイルス対策ソフトよりもコストを抑えた乗り換えを実現しました。



統合管理によるコスト削減

目的別に存在していたサーバーを統合。ハードウェアコスト削減、管理工数の削減に役立ちます。

他社ウイルス対策ソフトからの移行作業もかんたん

メジャーなウイルス対策ソフトウェアをアンインストールするスクリプトを保守ユーザー様専用ページでご提供。AssetView D アプリケーション配布機能を使ってかんたんに移行作業の自動化ができます。

＋ AssetView D アプリケーション配布

アプリケーション配布機能『AssetView D』を利用した移行作業イメージ

他社ウイルス対策ソフトから「AssetView V」への乗り換え作業も手間がかからずダウンタイムも発生しません。

1. 他社ウイルス対策ソフト導入環境に「AssetView V」を追加して共存させる
2. 他社製品のアンインストールタスクを「AssetView D」で実行
3. 「AssetView V」動作開始

※機能追加は管理コンソールの設定のみ
※この時点では AssetView V は動作しません

※他社製品のアンインストールを自動検知して動作を開始します

AssetView V ウイルス対策

統合管理による運用効率の向上

統合された管理コンソールでクライアント管理ができます。

- ウイルス検知状況の把握
- AssetView V クライアントの起動
- リアルタイムモニターの各種設定
- ウイルススキャンのスケジュール設定
- スキャン除外設定

ウイルス対策リストから、ドリルダウンしてPC操作ログ管理の稼働状況グラフを把握。
ウイルス検知の直前の操作を把握し、原因特定に役立てます。

連携してより高セキュリティな運用を実現

USBメモリのセキュア運用を実現。ウイルスの侵入を防止します。
自宅等に持ち帰ったUSBメモリへのデータ保存を禁止できます。

＋ AssetView G デバイス制御 ＋ セキュリティ USB メモリ ソリューション

ウイルス検知直前の操作を把握します。原因の特定に活用できます。

＋ AssetView M PC操作ログ管理

リアルタイムモニタリング

リアルタイムで脅威を検知。
最適な除去、削除を高い検知力で実施します。

オフラインPCの管理も可能

オフラインのPCは、パターンファイル更新がされない危険な状態です。オフラインPCのウイルス対策として、オンラインPCからパターンファイルをエクスポートし、オフラインPCにインポートできる柔軟な運用が可能です。

USBデバイスの自動スキャン

クライアント PC に USB デバイス等が接続されたことを検知した際に、該当のデバイスに対して自動でウイルスキャンを行うことができます。

未知の脅威対策

POWERED BY KASPERSKY

AssetView W 未知の脅威対策

パターンファイルマッチングでは対処しきれない亜種のマルウェアの脅威に「ふるまい検知」で対応。

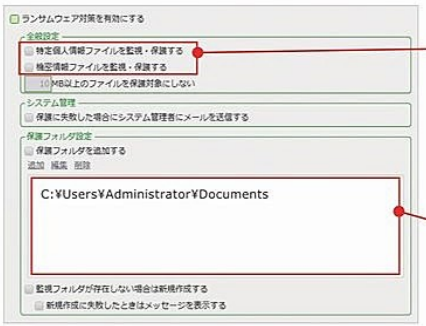
従来のパターンファイル型製品だけでは、日々増加する未知の脅威への対策は不十分です。
世界中で確認される検体を分析、学習し亜種のマルウェアの構造や不正な動き（振る舞い）を自動判断して検知できる仕組みが未知の脅威に対する回避策となります。

1日約30万件のマルウェア解析と機械学習

AssetView W では、機械学習を用いてマルウェアの解析を行い、エンドポイントでふるまい検知により未知のウイルスを防御します。
他社メーカーでは１日に約数万件のマルウェアを解析しているのに対してカスペルスキーでは１日に約 30 万件のマルウェア解析を行っています。解析数の差は検知能力の高さに比例します。

万が一、ランサムウェアに感染しても安心のバックアップ機能

ランサムウェア対策として最も有効な「バックアップ機能」を実装。高いマルウェア検知能力に加え、万が一の際にも安心です。



重要ファイルの自動保護

個人情報や機密情報など重要なファイルが見つかった場合に、該当のファイルを監視・保護します。ファイルをバックアップするのでランサムウェアに備えることが可能です。

保護フォルダ設定

ランサムウェアに感染し、更新を検知すると設定したフォルダを AssetView がバックアップします。

選べるセキュリティモード

ユーザーが求めるセキュリティレベルに合わせたテンプレートを選択するだけで、誰でもかんたんに設定が完了します。
カスタム設定ももちろん可能です。

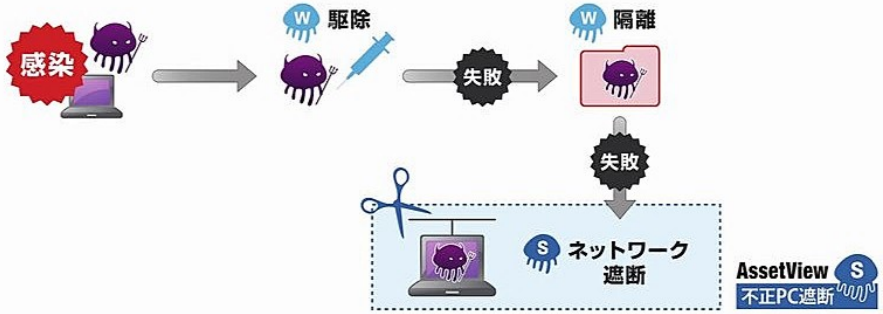
「ハイパフォーマンス」モード

「推奨」モード

「高セキュリティ」モード

ウイルスの駆除～隔離～ネットワーク遮断までをトータルで実現

AssetView S 機能と連携し、隔離に失敗した場合にネットワークを遮断できます。



検知実績のあるマルウェア一覧（powered by Kaspersky）

AssetView W で、検知できる代表的なマルウェアは以下の通りです。

マルウェア名	内容
Emdivi	Emdivi は、標的型メールに添付されたファイルをユーザ自身が開封することや、改ざんされた Web サイトを閲覧し、不正なファイルをダウンロードするドライブバイダウンロード攻撃によって感染します。Emdivi に感染した端末が外部の C&C サーバに接続することで、攻撃者が感染端末をリモートから操作することが可能となります。
Locky	Locky ウイルスは、感染すると PC 内のファイルを勝手に暗号化してしまうランサムウェアと言われる種類のウイルスです。暗号化されたファイルは、拡張子が「Locky」となってしまうことから通称「Locky」と呼ばれています。感染経路としては、メール添付ファイルと脆弱性を攻撃するWebサイトの大きく２つがあります。
Petya	Petya は 2016 年 3 月後半にかけて猛威を振るうようになったランサムウェア。ファイルシステム上のファイルを暗号化する従来のランサムウェアと比べ、ブートコードとファイルシステムのメタデータそのものを暗号化してデータへのアクセスを困難にするという特徴があります。主にビジネスユーザーが狙われ、仕事の応募書類などをよそおったスパムメールで感染することが多く、暗号化が完了すると、ASCII 文字で描かれたドクロのような絵が映しだされます。
その他のマルウェア：URLZone 別名：Shiotob / Bebloh、**TeslaCrypt**(vvv ウイルス)、**Gozi** 別名：Ursnif /Snifula / Papras	

検体については https://virustotal.com/ にて「Kaspersky」の検知名で検知実績があることを確認しております。

PC更新管理 Windows 10 対応

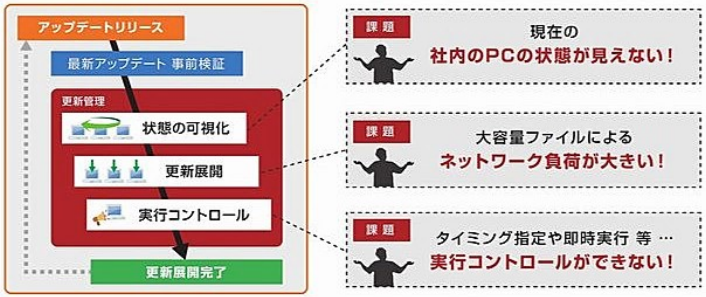
AssetView P
PC更新管理

「可視化」「ネットワーク負荷軽減」「実行コントロール」の視点で、
Windows 10 更新プログラムの
配信・管理業務を支援します。

Windows 10 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。

Windows 10 更新管理の課題は大きく3つ

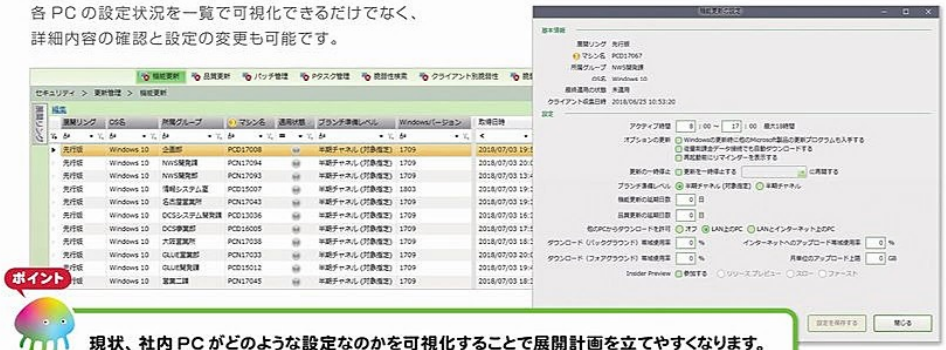
新たなアップデートが公開されてから、社内 PC への更新展開が完了するまでの課題を解決します。



Windows 10 端末設定状況を可視化

WSUS支援　Windows Update 支援

各 PC の設定状況を一覧で可視化できるだけでなく、
詳細内容の確認と設定の変更も可能です。



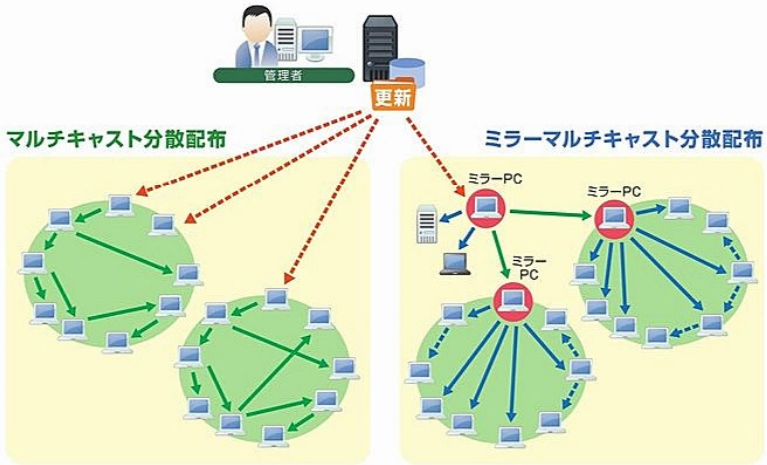
ポイント

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。
また、可視化だけでなく設定の変更もそのまま行えます。

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

独自更新管理

「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。



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。

アップデート実行の即時コントロール

独自更新管理　WSUS支援　Windows Update 支援

端末へアップデート実行の即時コントロールが可能です。
「AssetView P で独自で作成したタスク毎の即時実行」「Windows Update を即時実行」と実行手法は 2 種類あります。

電子メール監視

AssetView Mail 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。Webメール送信ログも取得可能。

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

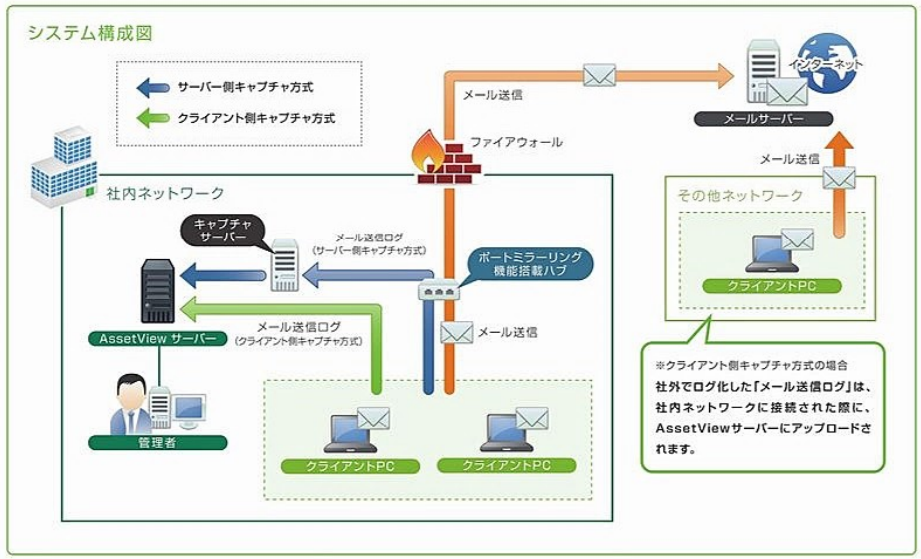
以下のメール送信情報を取得します。

- 件名
- 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
- 添付ファイル名
- 添付ファイル実体

※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。

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。



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	操作対象のファイル名/ウィンド
2018/01/28 20:41	HAMMOCK	個人情報ファイルメール添付	2017年度_顧客名簿.xls
2018/01/28 20:41	HAMMOCK	個人情報ファイルメール添付	2017年度_顧客名簿.xls
2018/01/28 20:42	HAMMOCK	ファイルオープン	2018年度_顧客名簿.xls
2018/01/28 20:42	HAMMOCK	個人情報ファイルコピー	2018年度_顧客名簿.xls
2018/01/28 20:42	HAMMOCK	個人情報ファイルメール添付	2018年度_顧客名簿.xls
2018/01/28 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。

■ Internet Explorer（9以降）のアドイン
- Yahoo!メール
- Gmail
- Office365（Exchange Online）

※Webメールからは、添付ファイル本体を取得できません。
※Internet Explorer 以外のブラウザからは取得できません。

■ 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 2007
- Microsoft Outlook 2010
- Microsoft Outlook 2013

※Outlook Web App でのメール送信情報の取得は非対応です。

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。

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。

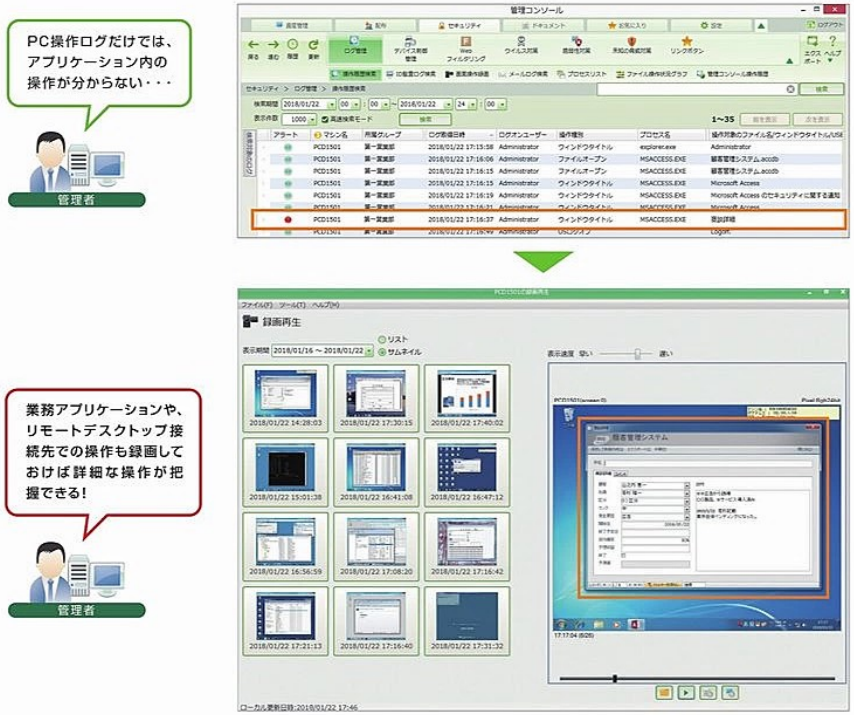
画面操作録画

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。



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。

スマートデバイス管理

AssetView MDM 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。

ビジネス利用が進む iPad®やiPhone®、またAndroid™ 端末の一元管理を実現し、
ビジネス用途での安全かつ効果的な利用促進に貢献します。

情報漏洩リスクの高い盗難・紛失対策、位置情報まで把握可能

紛失時に対処したい端末のロック、データ削除、位置情報の把握ができます。
端末を紛失した際の基本的な情報漏洩対策の実施が可能です。

スマートデバイス管理機能

スマートデバイス管理に必要なセキュリティ、運用管理に関する機能を標準搭載しています。

iOS

- リモートワイプ
- リモートロック
- ポリシー設定
- 機能制限
- インベントリ取得
- インハウスアプリ配信
- 位置情報取得
- アプリ利用ログ ※iOS9.0以降は不可
- パスコード削除

Android

- リモートワイプ
- インベントリ取得
- 位置情報取得
- アプリ利用ログ
- アプリ起動制限
- カメラ制御
- パスワード変更

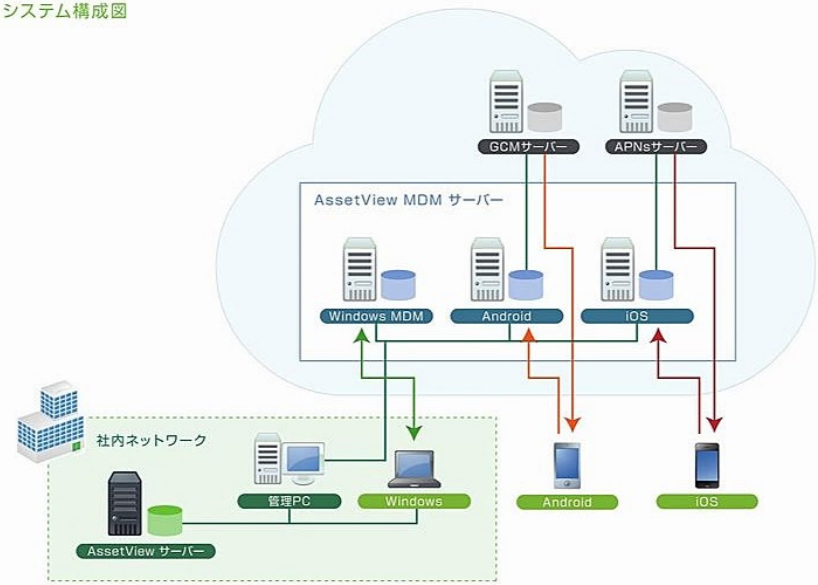
Windows

- リモートロック
- リモートワイプ ※OS起動不可
- 位置情報取得

AssetView で一元管理

スマートデバイス用に新たなサーバー構築は不要です。
すでにお持ちの AssetView サーバー上にスマートデバイスの管理も統合管理できます。
ハンモックが提供するクラウドサーバーを介して、スマートデバイスへの各種設定変更、各種ログのアップロードを行います。

システム構成図



ポイント

管理コンソールの権限設定機能を使うことで運用の分散、権限委譲が可能です。

すべてのIT資産を管理するユーザーはもちろんのこと、営業部門のIT資産を管理するユーザーや、
一部の機能だけを有効にした管理範囲を限定したユーザーなど運用にあわせた柔軟な設定が可能です。

24時間365日 リモートオペレーションサービス（オプション）

スマートデバイス紛失・盗難時の緊急対策を、お客様のIT管理者に代わり、ヘルプデスクが行います。スマートデバイス利用者からのヘルプデスクへの電話連絡により、スマートデバイスのリモートロック、解除、リモートワイプ（データ消去）を行います。

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

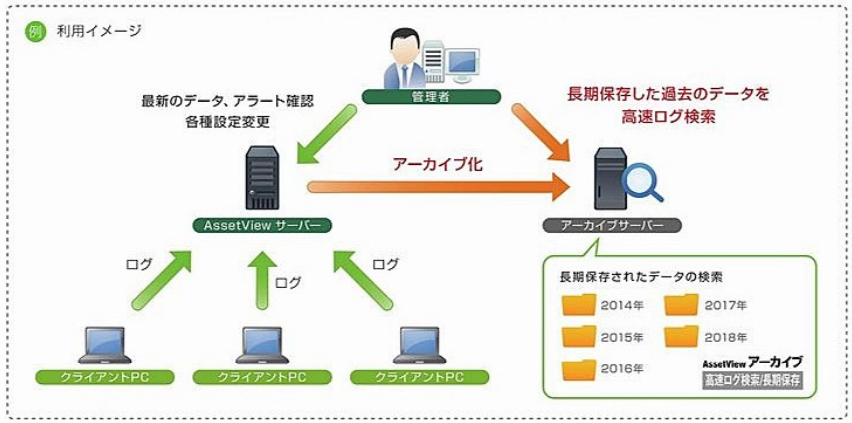
AssetView 製品ログの高速検索、長期保存が可能

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。



対象製品	アーカイブ項目
AssetView M PC操作ログ管理	登録日時、マシン名、ユーザー名、操作種別、アラート、プロセス名、ファイル名 / ウィンドウタイトル、コピー / 移動先のファイルパス、ファイルサイズ、URL、ドライブ種別、ローカル / リムーバブル / ネットワーク、コピー移動先、プリンター名、印刷枚数、ログ種別
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、添付ファイル名

ライセンス	機能名	説明
すべてのライセンス M	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 ・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　・タイムゾーン
	アンケートによるユーザー情報取得	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悪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　・会社名
	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(%)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。
	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。
	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。
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　・Internet Explorer バージョン　・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
	ドライブ情報の取得	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

ライセンス	機能名	説明
AssetView A (IT資産管理)	プリンター情報の取得	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	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	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	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	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)	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。
	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。

ライセンス	機能名	説明
AssetView M (PC操作ログ管理)	プロセスログの取得	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	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	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	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
	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 Apps 操作ログの取得	Google Chrome で操作した、以下の Google Apps 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	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	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サイトにアップロードされたファイルの情報を取得します。 Internet Explorer での操作であれば、HTTP(S)でのファイルアップロードも取得することができます。 ・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/Bluayにコピー・移動した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	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	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。
	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。
	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。
	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を送信します。 ・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
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。 ・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
	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。 ・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
	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。

ライセンス	機能名	説明
AssetView I（個人情報検索）	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	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	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 11 ・Nero 9 StartSmart Essentials ・Roxio Easy Media Creator 10
	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。 ・使用許可 ・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。
	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。
	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）
	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	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。
	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。
	デバイス制御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
	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社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。

ライセンス	機能名	説明
AssetView G（デバイス制御）	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 ・使用禁止ポータブルデバイスの接続 ・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
	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
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。
AssetView RC（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。
	メッセージ送信	クライアントPCに、任意のメッセージを送信します。
	プログラム実行	クライアントPCに、任意のコマンドを送信します。
	シャットダウン	クライアントPCに、OSシャットダウン、ログオフ、再起動等のコマンドを送信します。
	インストール	ネットワーク上のPCに、RCクライアントをリモートインストールします。
	アンインストール	クライアントPCから、RCクライアントをリモートアンインストールします。
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。
	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。
	ポート変更	リモート接続に使用するポート番号を変更することができます。
	パスワード変更	リモート接続時に求められるパスワードを変更することができます。
	暗号化通信	ホストとゲスト間の通信を暗号化します。
	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）	社内/社外の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が社外にあっても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	82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
	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	暗号ファイルを社外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 機能詳細一覧表

ライセンス	機能名	説明
AssetView V （ウイルス対策）	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	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。
	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。
	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	管理コンソール、またはクライアント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。
AssetView W （未知の脅威対策）	ファイルモニター	クライアント端末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。アンチウイルス機能に対応しています。
	メールモニター	クライアント端末上で行われるメール送受信（POP3/SMTP/ESMTP/NNTP/IMAP）を監視します。アンチウイルス機能とアンチスパム機能に対応しています。
	Webモニター	クライアント端末のWebアクセスを監視し、以下を検知してブロックします。アンチウイルス機能に対応しています。
	スケジュールスキャン	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端末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時実行することができます。 ウイルス等の脅威を検知すると、該当のファイルから危険なコードの除去を行い、コードのみを除去できなかった場合は感染ファイルの削除を行います。
	オンデマンドスキャン	クライアント端末でウイルススキャンを即時実行することができます。 ウイルス等の脅威を検知すると、該当のファイルから危険なコードの除去を行い、コードのみを除去できなかった場合は感染ファイルの削除を行います。
	ヒューリスティック検知	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）を検知します。
	隔離ファイルの管理	各種検知により隔離されたファイルについて、実行される処理を選択できます。隔離されたファイルを復元することも可能です。
	連携機能（S連携）	AssetView S ライセンス機能と連携し、隔離に失敗した場合にネットワークを遮断できます。
	パターンファイルの更新	管理コンソール、またはクライアント端末の未知の脅威対策設定ツールから、任意のタイミングでパターンファイルの更新を行うことができます。
	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。
	ランサムウェア対策	PC 内のファイルを使用できない状態にし、身代金を要求するマルウェアへの対策として、あらかじめ重要データを自動的にバックアップする機能です。
	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。
	連携機能（I連携）	AssetView I ライセンス機能と連携し、個人情報/特定個人情報および機密情報を監視・保護対象に含めることができます。
AssetView P （PC更新管理）	ヘルスビュー	Pサーバーの状況が表示できます。
	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。
	脆弱性社内該当件数の確認	脆弱性社内該当端末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　・社内該当あり　・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。
	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。
	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。
	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。
	OfficeProPlus利用	OfficeProPlusの配布ができます。
	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Internet Explorer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。
	Webメールの取得 （クライアント側キャプチャモード）	Internet Explorerで送信した、以下のWebメールの情報を取得することができます。 ・Yahoo Mail　・Gmail　・Office 365
	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）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）	Android端末の管理	スマートフォンやタブレットなどのAndroid端末を管理対象とすることができます。
	iOS端末の管理	iPhone、iPad を管理対象とすることができます。
	Windows MDM の管理	ノートPCや Windows タブレットなどを管理対象とすることができます。
	MDMインストールメール送信	指定したメールアドレスに、Android/iOSアプリのインストールを案内するメールを送信することができます。
	位置情報取得	位置情報を定期的に取得します。
	リモートロック	Android/Windows端末のOSをリモートロックします。
	リモートワイプ	Android/iOS端末のOSを初期化します。Windows MDM では、OSを起動できないようにします。

ライセンス	機能名	説明
AssetView MDM （スマートデバイス管理）	端末情報の取得	Android/iOS端末のハードウェア情報を取得します。 ・電話番号　・IMEI　・IMSI　・SIMシリアル　・MACアドレス（iOS端末のみ）　・IPアドレス　・キャリア　・ベンダー　・モデル名 ・OSバージョン　・UDIS　・デバイス名　・ビルドバージョン　・製品名　・製品番号　・シリアル番号　・ICCID
	アプリ情報の取得	Android/iOS端末にインストールされているアプリの情報を取得します。 ・アプリ名　・パッケージ名　・バージョン　・アプリのサイズ（iOSのみ）　・書類とデータ（iOSのみ）
	アプリの起動/終了ログの取得	Android/iOS端末のアプリ起動/終了日時を取得します。
	パスワードの変更	Android端末のパスワードポリシーと、パスワードの値を変更することができます。
	カメラ制御	Android端末に搭載されているカメラの有効/無効を制御します。
	アプリ制御	Android端末にインストールされているアプリの起動を禁止することができます。
	iOSの機能制限	iOS端末の機能制限を設定することができます。
	Wifiの設定	iOSのWifi接続に関する設定を登録することができます。
	VPNの設定	iOSのVPN接続に関する設定を登録することができます。
	メールの設定	iOS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。
	Webクリップの配信	iOSにWebクリップを配信することができます。
	インハウスアプリの配信	iOSにインハウスアプリを配信することができます。
	パスコードポリシーの変更	iOS端末のパスコードポリシーを変更することができます。
	パスコードのリセット	iOS端末のパスコードをリセットすることができます。
	iPhone構成ユーティリティで作成した設定の配信	iPhone構成ユーティリティで作成した設定（mobileconfigファイル）を配信することができます。
	ハードウェア情報に追加	Android/iOS端末の情報を AssetView のマスタ情報に登録し、クライアント端末と同様に管理することができます。

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 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 ※ アップグレードした OS では動作保証していません。 ※ NET Framework 3.5 および .NET Framework 4.5 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　推奨：クアッドコア Intel Xeon 2.33GHz同等以上
メモリ	OS推奨値以上　推奨： 4GB以上
HDD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 5MB 以上の空き容量が必要です。 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されることを推奨します。
Microsoft Office	自動レポート機能を利用する場合は、Microsoft Excel 2003 以降がインストール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。 通信にポート番号 2943(可変)/3307 を使用します。

管理コンソール

OS	Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SPなし/SP1 Microsoft Windows Server 2008 Standard/Enterprise SP1/SP2 (32bit版のみ) Microsoft Windows 10 Pro/Enterprise Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 8 Pro/Enterprise Microsoft Windows 7 Professional/Ultimate/Enterprise SPなし/SP1 Microsoft Windows Vista Business/Ultimate/Enterprise SP1/SP2 (32bit版のみ) Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 (32bit版のみ) Microsoft Windows Server 2003 Standard/Enterprise SP2 (32bit版のみ) Microsoft Windows XP Professional SP3 (32bit版のみ) ※ .NET Framework 4 または .NET Framework 4.5 以降がインストールされている必要があります。 .NET Framework 4 の環境では、更新プログラム KB2468871v2 を適用してください。 ※ アップグレードした OS では動作保証していません。
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	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	Microsoft Excel 2003 SP3以降 Microsoft Excel 2007 Microsoft Excel 2010 Microsoft Excel 2013 Microsoft Excel 2016 Microsoft Excel 2019 ※ Microsoft Excel 2003/2007 で、CSV ファイルを展開した際に文字化けして表示される場合は、以下のセキュリティ更新プログラムを適用してください。 Microsoft Office 2003 の場合 KB2344693 Microsoft Office 2007 の場合 KB965470

AssetView リモートデスクトップアドイン

OS	Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SPなし/SP1 Microsoft Windows Server 2008 Standard/Enterprise SP1/SP2 (32bit版のみ) Microsoft Windows 10 Pro/Enterprise Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 8 Pro/Enterprise Microsoft Windows 7 Professional/Ultimate/Enterprise SPなし/SP1 Microsoft Windows Vista Business/Ultimate/Enterprise SP1/SP2 (32bit版のみ) ※ 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。 ※ リモートデスクトップ接続を行うクライアントの OS が以下の場合はリモートデスクトップ接続によるウィンドウタイトル取得を行えない場合があります。 Microsoft Windows Embedded Standard 7 SP1 Microsoft Windows Vista Business/Ultimate/Enterprise SP1/SP2 (32bit 版のみ) Microsoft Windows Server 2003 R2 Standard/Enterprise SP1/SP2 Microsoft Windows Server 2003 Standard/Enterprise SP2
CPU	OS推奨値以上
メモリ	OS推奨値以上
HDD容量	1MB 以上の空き容量が必要です。

AssetView RC RelayClient

OS	Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SP なし /SP1 Microsoft Windows Server 2008 Standard/Enterprise SP1/SP2 (32bit 版のみ) Microsoft Windows 10 Pro/Enterprise Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 8 Pro/Enterprise Microsoft Windows 7 Professional/Ultimate/Enterprise SP なし /SP1 Microsoft Windows Embedded Standard 7 SP1 Microsoft Windows Vista Business/Ultimate/Enterprise SP1/SP2 (32bit 版のみ) Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 Microsoft Windows Server 2003 Standard/Enterprise SP1/SP2 (SP1 は 32bit 版のみ) Microsoft Windows XP Professional SP3 ※アップグレードした OS では動作保証していません。 ※ .Net Framework 4 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
メモリ	OS 推奨値以上
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。
その他	RelayService との通信にポート 80 を使用します。 またリモート接続用にポート 20000 ～ 30000 を動的に取得します。

アプリケーションサーバー

OS	Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 ※ アップグレードした OS では動作保証していません。 ※ NET Framework 3.5 および .NET Framework 4.5 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　推奨：クアッドコア Intel Xeon 2.33GHz同等以上
メモリ	OS推奨値以上　推奨： 4GB以上
HDD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 V ライセンスを有効にする場合は、システムドライブに 700MB 以上の空き容量が必要です。 AssetView W ライセンスを有効にする場合は、システムドライブに 900MB 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されることを推奨します。

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 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SP なし /SP1 Microsoft Windows Server 2008 Standard/Enterprise SP1/SP2 (32bit 版のみ) ※ アップグレードした OS では、動作保証しておりません。
CPU	OS 推奨値以上　推奨：クアッドコア Intel Xeon 2.33GHz 同等以上
メモリ	OS 推奨値以上　推奨：4GB 以上
HDD 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	Mac OS を管理する場合は Ver.4.2.0 以降のアプリケーションサーバーがインストールされている必要があります。 Linux OS を管理する場合は Ver10.2.0 以降のアプリケーションサーバー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

OS	Microsoft Windows Server 2019 Standard/Datacenter Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SPなし/SP1 Microsoft Windows Server 2008 Standard/Enterprise SP1/SP2 (32bit版のみ) Microsoft Windows 10 Pro/Enterprise Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 8 Pro/Enterprise Microsoft Windows 7 Professional/Ultimate/Enterprise SPなし/SP1 Microsoft Windows Embedded Standard 7 SP1 Microsoft Windows Vista Business/Ultimate/Enterprise SP1/SP2 (32bit版のみ) Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 Microsoft Windows Server 2003 Standard/Enterprise SP1/SP2(SP1は32bit版のみ) Microsoft Windows XP Professional SP3 ※ 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。 ※ クライアント端末に .Net Framework 3.5 SP1 がインストールされていなければ、 下記機能が正常に動作しません。 AssetView Mail (Web メールの取得機能を使用する場合) AssetView Rec AssetView ID (ブラウザタイプを使用する場合) ※ クライアント端末に .Net Framework 4.0 以上 がインストールされていなければ、 下記機能が正常に動作しません。 AssetView W (未知の脅威対策設定ツールの使用) ※ Windows Embedded では以下の機能が動作しません。 AssetView V/W ライセンス機能 ※ Windows XP では以下の機能はサポート対象外となります。 AssetView V ライセンス機能 ※ Windows7 SP1 未満では以下の機能はサポート対象外となります。 AssetView P 更新管理機能 AssetView M/K 自動暗号化機能 ※ AssetView ID/MDM/REC ライセンス機能は、Windows Vista 以前の OS では動作しません。
CPU	OS推奨値以上
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。
HDD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 V 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 W ライセンスを有効にする場合は、システムドライブに 1GB 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。

AssetView Mail キャプチャサーバー

OS	Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SP なし /SP1 Microsoft Windows Server 2008 Standard/Enterprise SP1/SP2 (32bit 版のみ) ※ アップグレードした OS では動作保証していません。 ※ NET Framework 3.5 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：クアッドコア Intel Xeon 2.33GHz 同等以上
メモリ	OS 推奨値以上　推奨：4GB 以上
HDD 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されることを推奨します。
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) を無効化することを推奨します。

AssetView F 管理コンソール

OS	Microsoft Windows 10 Pro/Enterprise Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 8 Pro/Enterprise Microsoft Windows 7 Enterprise/Ultimate/Professional SP1 Microsoft Windows Vista Business SP2 (32bit 版のみ) ※ アップグレードした OS では、動作保証しておりません。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
Web ブラウザー	Microsoft Internet Explorer 7.0/8.0/9.0/10.0 (互換表示のみ) /11.0

AssetView P サーバー

OS	Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 ※ アップグレードした OS では動作保証していません。 ※.NET Framework 4.5 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　推奨：クアッドコア Intel Xeon 2.33GHz 同等以上
メモリ	8GB 以上
HDD 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 1 GB 以上の空き容量が必要です。脆弱性対策データ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 600GB 以上を推奨）のあるローカルドライブ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。クラウド P サーバーおよび HvnDB (脆弱性情報 DB) との通信にポート番号 3306 を使用します。1 クライアント当たり 5Mbps 程度のネットワーク帯域確保を推奨します。

AssetView P ミラーコンピューター

OS	Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter Microsoft Windows Server 2012 Standard/Datacenter Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 Microsoft Windows 10 Pro/Enterprise Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 7 Professional/Ultimate/Enterprise SP1 ※ アップグレードした OS では動作保証していません。 ※ NET Framework 4 Client Profile 以降がインストールされている必要があります。 ※AssetView P クライアント Ver.10.3.1 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　※Windows 7 SP1 の推奨：マルチコアで 2GHz
HDD 容量	バッチ格納用フォルダーの配置先となるドライブは、対象となるバ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 600GB 以上を推奨）のあるローカルドライブを指定してください。
その他	ミラーコンピューター間の通信にポート番号 40000 を使用します。 接続側は Any になります。 ミラーユニキャスト用の待機ポートとして、40001 ポートをミラーコンピューター側が待機します。

AssetView F クライアント

OS	Microsoft Windows 10 Home/Pro/Enterprise/Education Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 8 Pro/Enterprise Microsoft Windows 7 Enterprise/Ultimate/Professional SP1 Microsoft Windows Vista Business SP2 (32bit 版のみ) ※ Microsoft Windows 8 Pro/Enterprise は、日本語版のみ対応 ※ Microsoft 社による サポート方針の改訂に伴い、Windows 8 および Internet Explorer 7.0/8.0/10.0 については以下の対応とさせていただきます。 • 日本語版 Microsoft Windows 8 のみに発生する問題については動作保障外となります。 • Internet Explorer 7.0/8.0/10.0 のみに発生する問題については動作保障外となります。 ※ アップグレードした OS では、動作保証しておりません。
CPU	OS 推奨値以上
メモリ	OS 推奨値以上
HDD 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 Internet Explorer 7.0/8.0/9.0/10.0/11.0/ Microsoft Edge Mozilla Firefox ESR Google Chrome ※ 管理設定を行う場合は、Internet Explorer 7.0/8.0/9.0/ 10.0 (互換表示のみ) /11.0 を使用してください。

AssetView P WSUS連携ツール

OS	Microsoft Windows Server 2016 Standard/Datacenter Microsoft Windows Server 2012 R2 Standard/Datacenter ※アップグレードした OS では動作保証していません。 ※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
HDD 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 MDM スマートデバイス管理

Android	Android 4.0 以降
iOS	iOS 7.0 以降
Windows	Windows 7 以降 ※位置情報取得機能は、Windows 8 以降のクライアント OS を対象としています。 ※その他の条件は、AssetView クライアントの稼働条件に準拠します。

Mac OS 稼働環境

AssetView クライアント (Mac OS版)

OS	Mac OS X 10.14 Mojave (64bit) Mac OS X 10.13 High Sierra (64bit) Mac OS X 10.12 Sierra (64bit) Mac OS X 10.11 El Capitan (64bit) Mac OS X 10.10 Yosemite (64bit) Mac OS X 10.9 Mavericks (64bit) Mac OS X 10.8 Mountain Lion (64bit) Mac OS X 10.7 Lion (64bit) Mac OS X 10.6 Snow Leopard (32bit) Mac OS X 10.5 Leopard (32bit) Mac OS X 10.4 Tiger (32bit) ※32bit 版では下記機能が動作しません。 OS シャットダウンタスクの実行　OS 再起動タスクの実行　ウィンドウタイトルログの取得 ローカルドライブのファイル操作ログ取得　外部デバイスのファイル操作ログ取得
HDD 容量	5MB 以上の空き容量

Linux 稼働環境

AssetView クライアント (Linux OS版)

OS	Redhat Enterprise Linux 5(i386) Redhat Enterprise Linux 6(i386) Cent OS 4(i386) Cent OS 5(i386) Cent OS 6(i386) Redhat Enterprise Linux 5(x86_64) Redhat Enterprise Linux 6(x86_64) Redhat Enterprise Linux 7(x86_64) CentOS4(x86_64) CentOS5(x86_64) CentOS6(x86_64) CentOS7(x86_64)
HDD 容量	5MB 以上の空き容量

AssetView アーカイブ 稼働環境

サーバー

OS	Microsoft Windows Server 2012 R2 Standard/Enterprise Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 ※ アップグレードした OS では、動作保証しておりません。 ※ .NET Framework 4 または .NET Framework 4.5 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	AssetView Ver.8.1.0 AssetView Ver.8.3.0 AssetView Ver.8.3.1 ※ その他バージョンは動作保障外です。

管理コンソール

OS	Microsoft Windows Server 2012 R2 Standard/Enterprise Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 8 Pro/Enterprise Microsoft Windows 7 Professional/Ultimate/Enterprise SP1 ※ アップグレードした OS では、動作保証しておりません。 ※ .NET Framework 4.5.2 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	1280×1024 以上の画面解像度で運用してください。