本ウェビナーの流れ

1

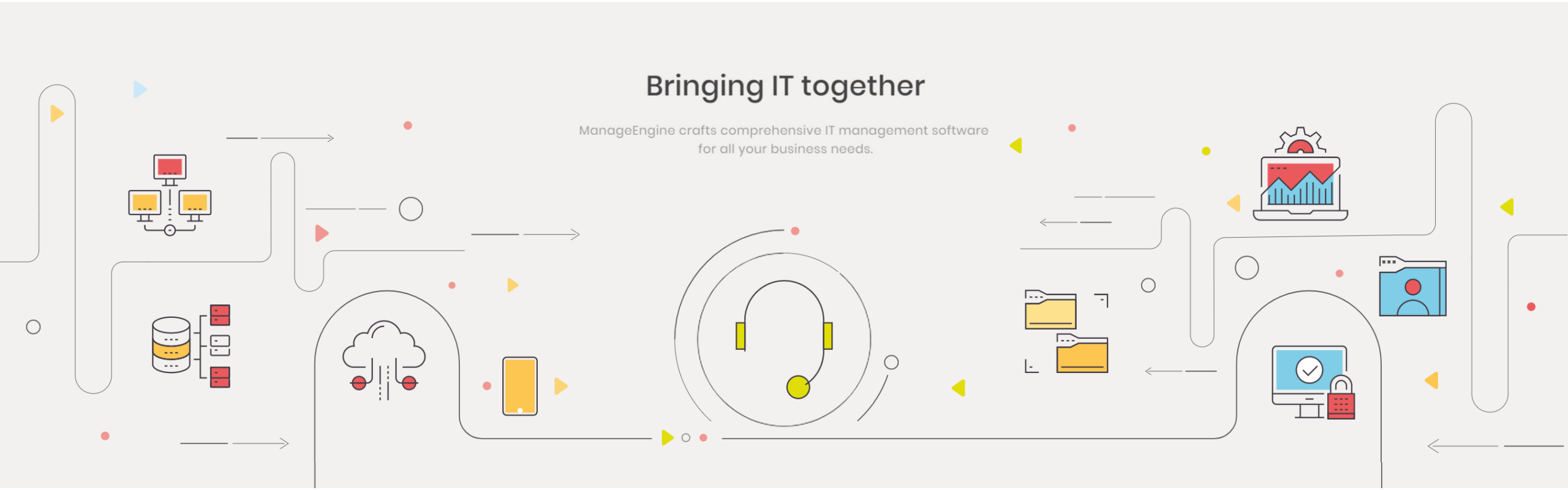
企業のエンドポイントを守る
～テレワーク導入/継続のための資産管理とパッチ管理術～

株式会社DXコンサルティング

2

テレワーク中の資産管理/セキュリティ対策に役立つ製品のご紹介

ゾーホージャパン株式会社



～テレワーク導入/継続のための資産管理とパッチ管理術～

企業のエンドポイントを守る

ゾーホージャパン株式会社　　株式会社DXコンサルティング

プロフィール　鈴木 浩一

2002年、現在所属する株式会社DXコンサルティングの前身である、株式会社フェスに入社。

多数の企業/組織のシステムにおいて、オペレーション、システム移行、運用設計、運用管理、運用サービス企画など、システム運用関連業務にたずさわる。

その後、大手物流系システム会社におけるITSMをベースとしたシステム運用の品質管理/業務改善など、顧客内におけるシステム運用/保守にかかわる品質改善にかかわる業務を担当し、現在に至る。

現在は、上席サービスマネジメント・アーキテクトとして、ITサービスマネジメントプロセス設計、顧客業務分析/改善、システム運用/セキュリティ運用関連製品の導入支援などに従事。

【主な業務実績】

・統合監視システム（監視/自動切り分け/チケット管理）の導入

・ITサービスマネジメントプロセスの設計・運用

・システム運用業務のプロセス改善/システム監査

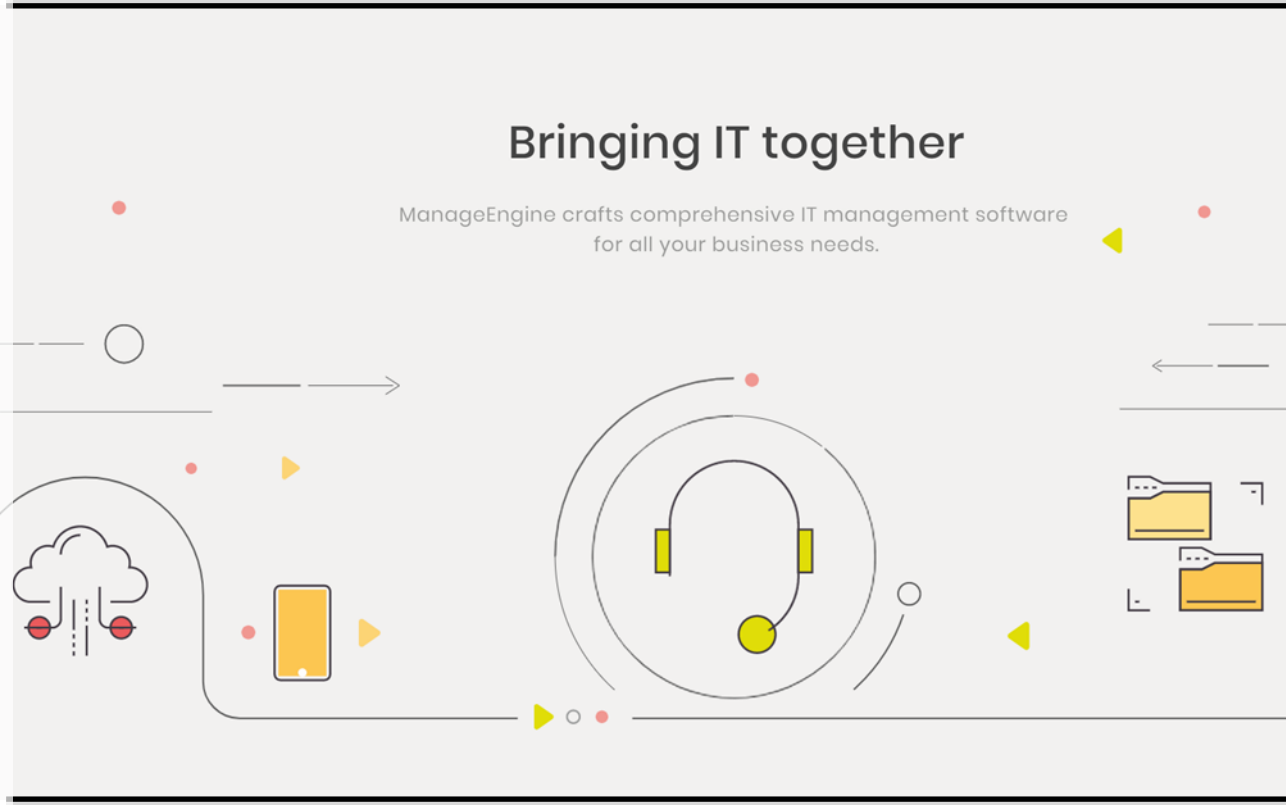
・ITSM、セキュリティ関連のパッケージ製品導入支援

・そのほか、ITサービスマネジメントに関連する各種支援全般

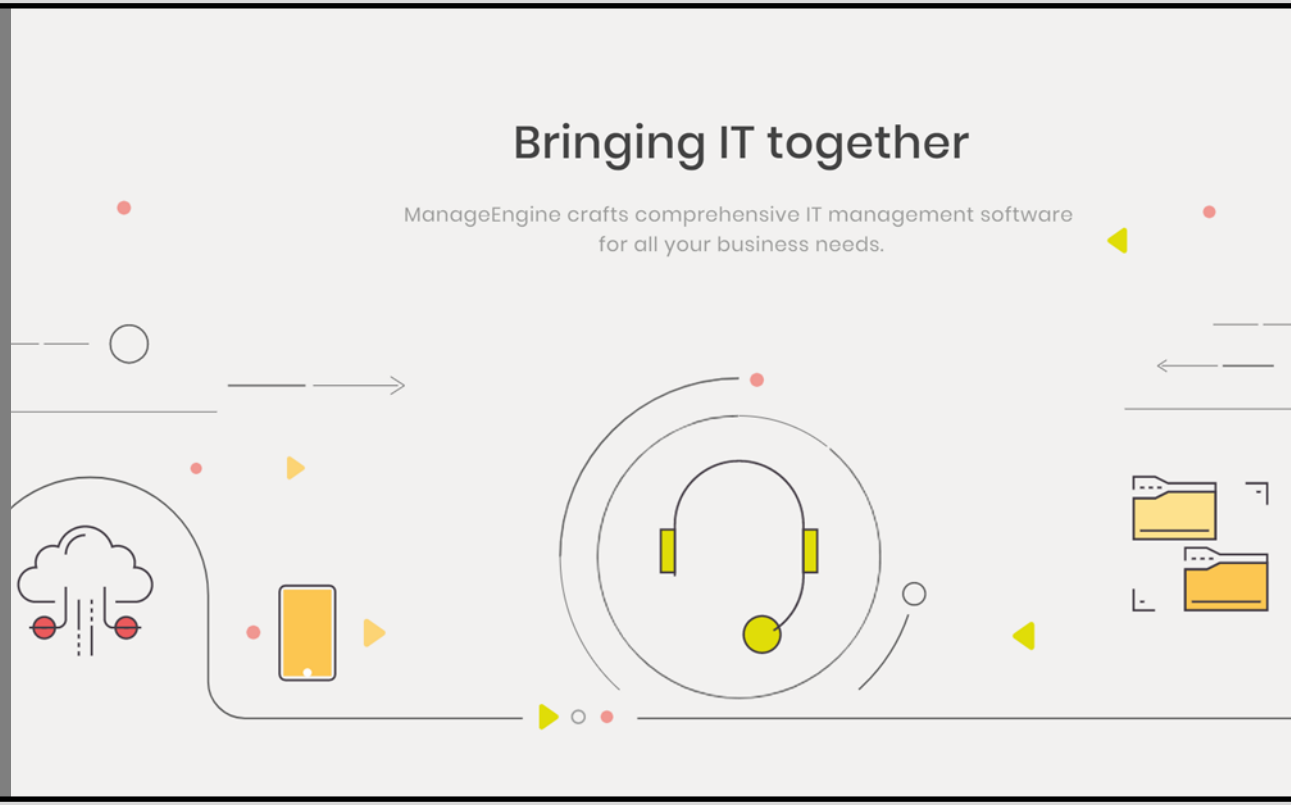
株式会社DXコンサルティング

目次

- はじめに
- テレワークがもたらした変化
- 必要なセキュリティ対策
- さいごに



はじめに


Bringing IT together
ManageEngine crafts comprehensive IT management software
for all your business needs.

はじめに

テレワークが普及し、企業のPCやモバイルデバイスなど、あらゆる端末が在宅ワークで利用されるようになりました。

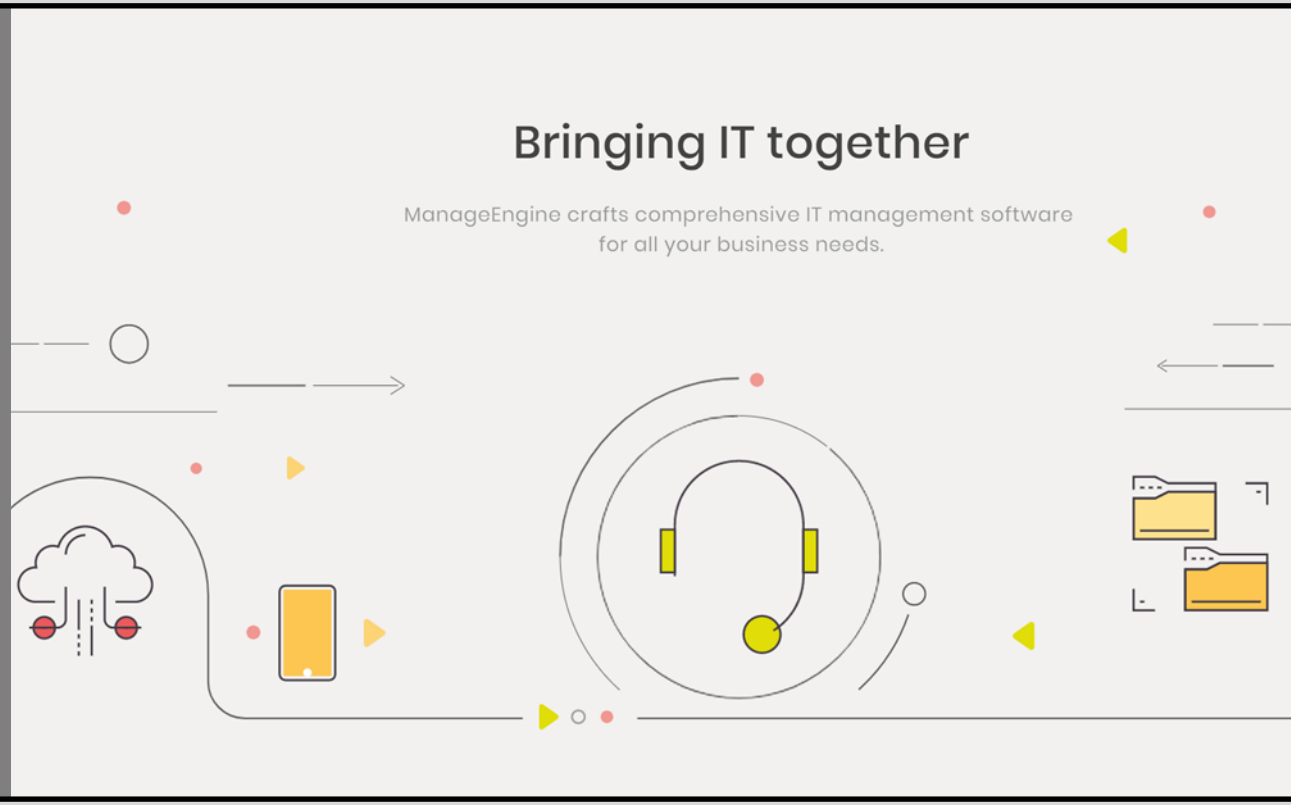
しかし、社員の自宅から情報システムへのアクセスを許可することは、サイバー攻撃を受けるリスクとなります。

本セミナーでは、テレワークを安全に導入/継続するために重要な

- ✓ マルチOSに対応した脆弱性対策
- ✓ モバイル端末の管理
- ✓ テレワーク環境での効率的な資産管理

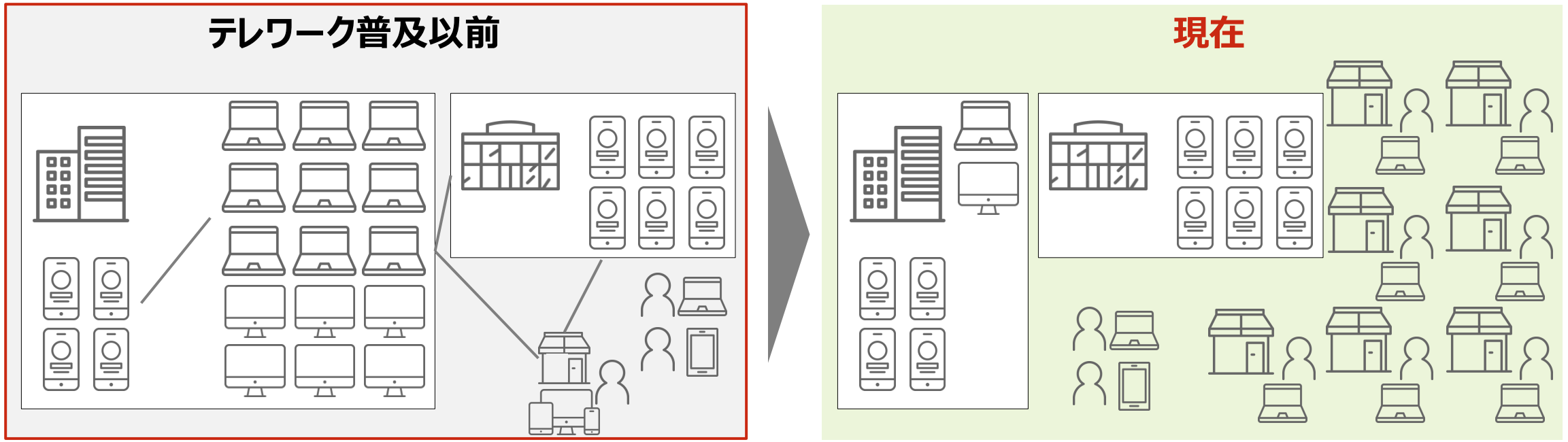
を踏まえた、セキュリティ対策についての解説・ソリューションの紹介をします。

テレワークがもたらした変化



テレワークによる、情報システム利用の変化

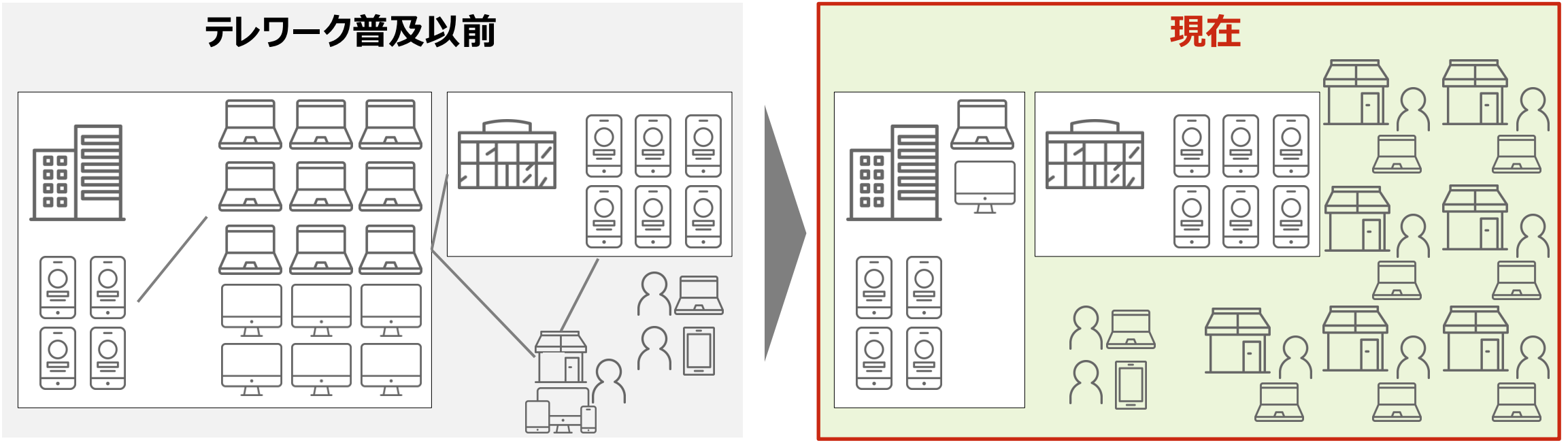
テレワーク普及前と現在



外部からのアクセスが劇的に増加

テレワークによる、情報システム利用の変化

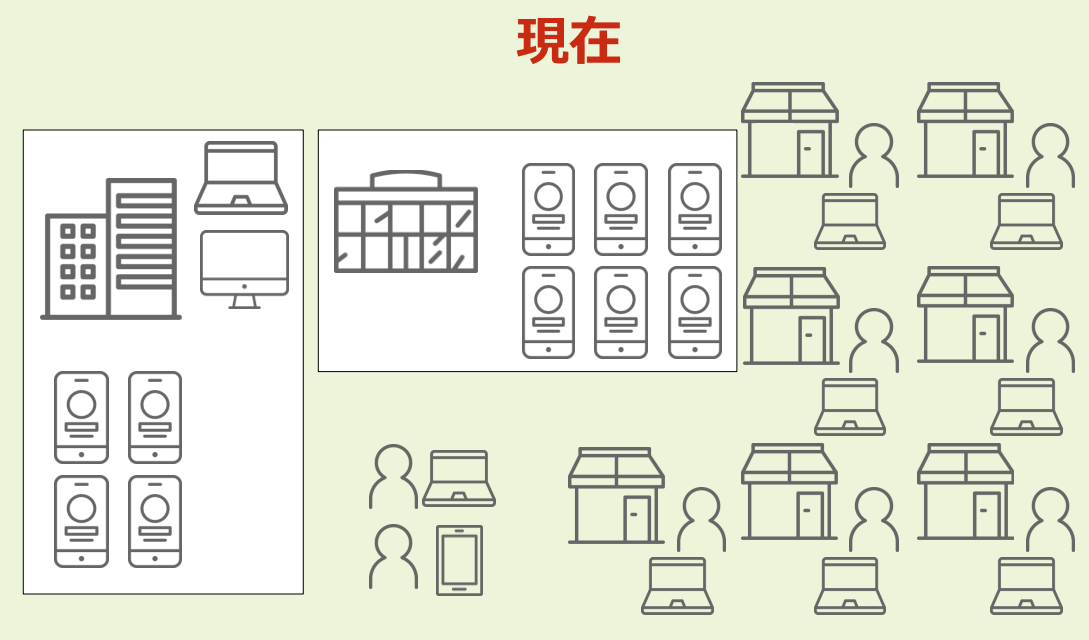
テレワーク普及前と現在



外部からのアクセスが劇的に増加

テレワークによる、情報システム利用の変化

テレワークにより情報システムの利用形態は変化



- 社員はテレワークを中心とした業務に
- 社員が利用する、大量の端末が情報システム部門より貸し出される
- シンクライアントの整備により、個人端末からのアクセス（BYOD）を許可する組織も増加
- 顧客先訪問や支社への出張は激減
- 会議やミーティングはWeb会議/電話会議が中心
- **情報システム部門もテレワーク化の対象となってきている**

本業をおこなう社員にくわえて、情報システム部門にもテレワークは拡大

情報システム利用の変化による課題

システム運用負荷

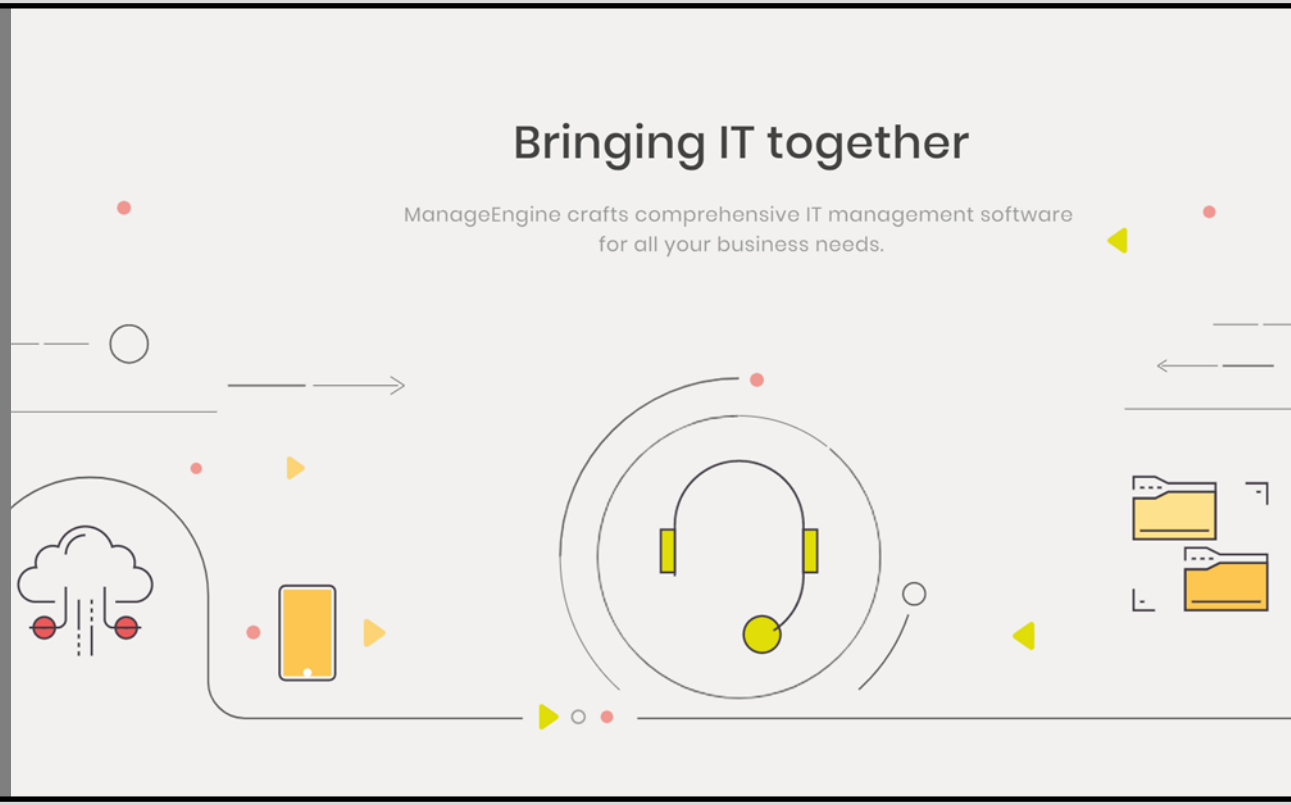
- 社員に貸し出した端末の管理負荷が増大
  - 貸し出し手続き
  - 購入
  - 棚卸し　・・・・

セキュリティリスクの増大

- セキュリティ対策が急務
  - セキュリティパッチ
  - 不正アクセス防止
  - 端末紛失対策　・・・

負荷低減を踏まえたセキュリティ対策が必須

必要なセキュリティ対策



必要なセキュリティ対策

テレワークが普及した現在では、貸し出した端末に対するセキュリティ対策が重要です。これまでも外部へ持ち出す端末への対策としてうたわれてきたものばかりですが、**その対象が劇的に増加**したことを考慮する必要があります。

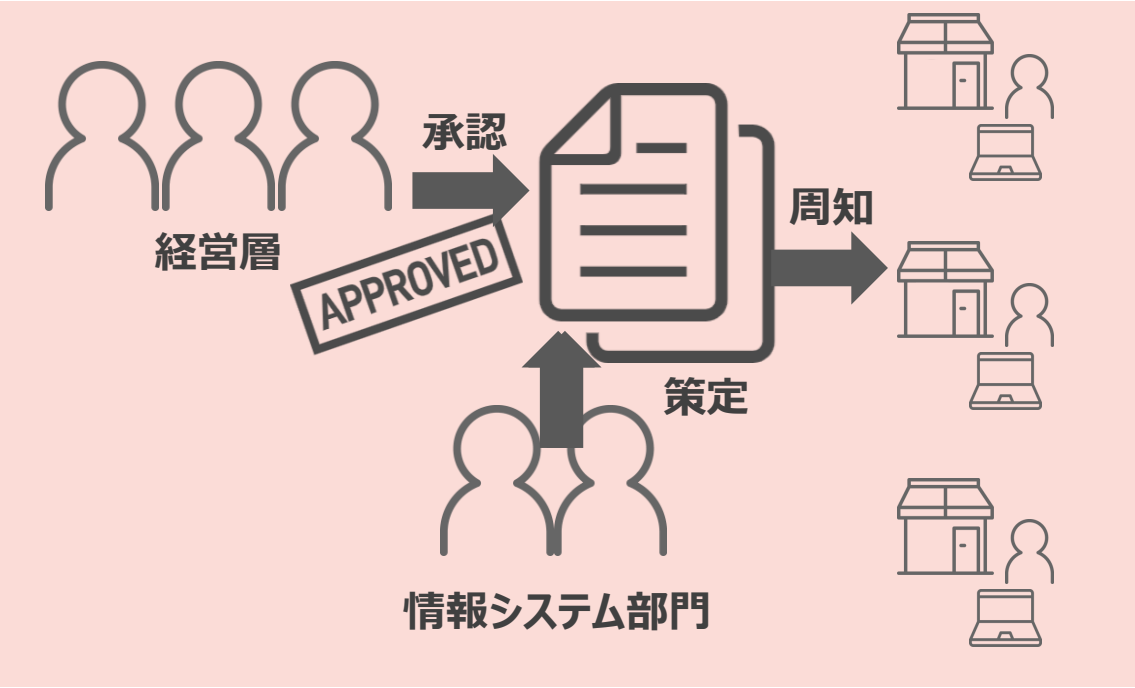
端末に関するセキュリティ対策

- 規定/ガイドラインの整備
- 端末管理
- データの保護
- ネットワークの安全性確保
- 端末の識別と認証
- 脆弱性対策/パッチ管理
- USBデバイスの接続制御
- アプリケーションの利用制限
- 証跡の保存と監査
- 不正利用時のアラート通知

膨大な端末へのセキュリティ対策が必要

規定/ガイドラインの整備

規定/ガイドラインの整備

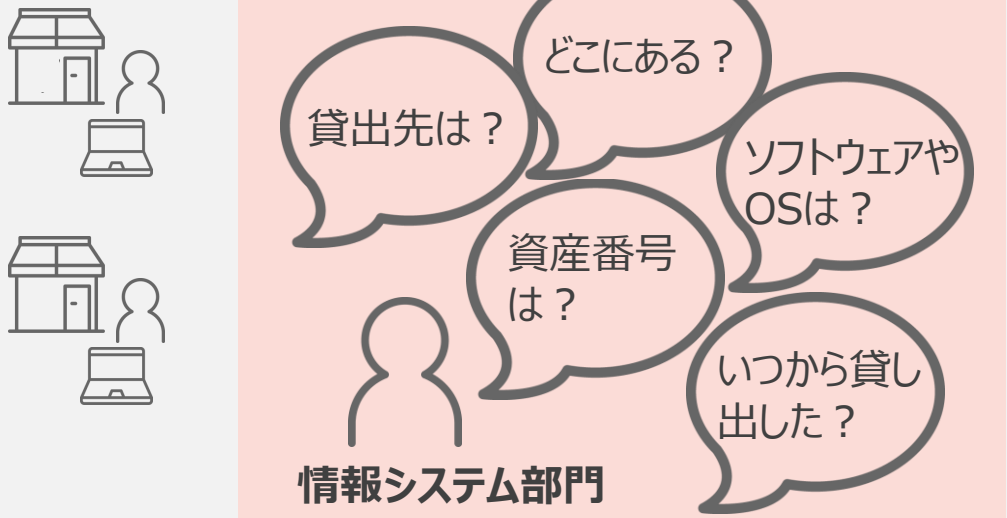


- テレワークに関する規定/ガイドラインの策定
  - 基準となるフレームワーク　※後述
  - テレワーク時の社員向け業務ルール
  - 端末貸し出し/持ち出しフロー
  - 持ち出し/貸し出し端末設定に関するルール（ウイルス対策ソフトの必須化など）
  - セキュリティ対策の実施内容　など

公開されている各種規定やガイドラインをベースとすると抜け漏れが防止できる

端末管理

端末を管理する際に必要な項目

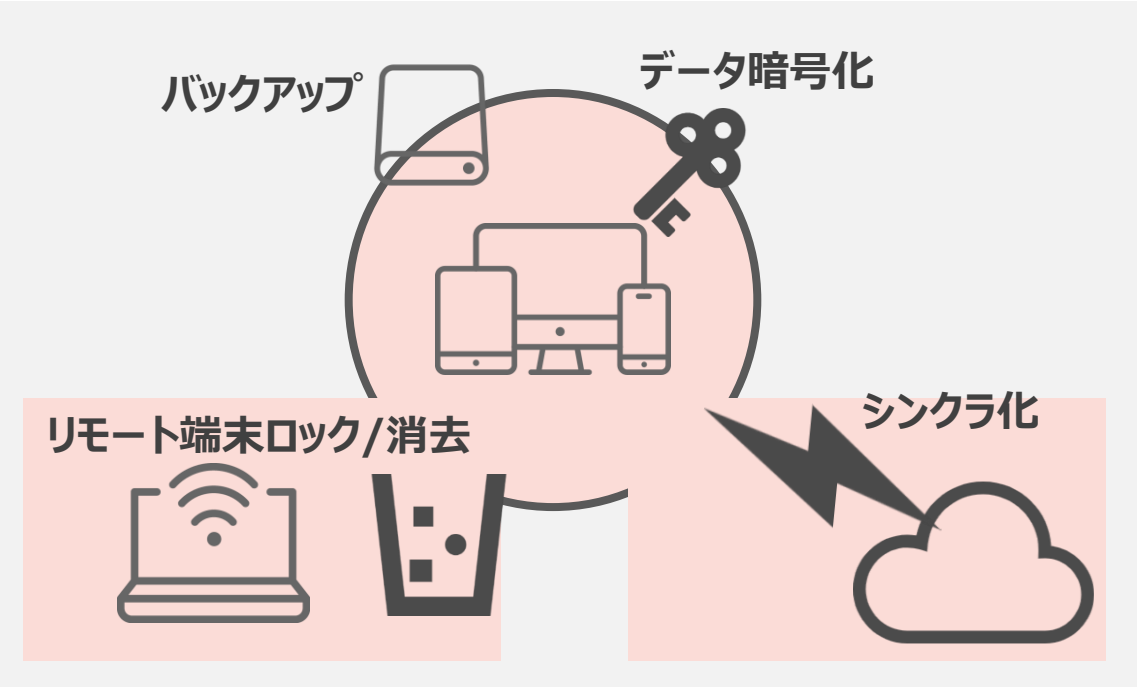


- 端末の貸出先である所有者の特定
- システムアカウントの把握
- 端末位置情報の取得
- 資産情報の管理（機種、搭載OS、アプリケーションなど）
- 貸出期間
- そのほか、リース契約なのか/購入したものであるか、など資産としての管理も必要となります

外部に持ち出すことにより、端末管理の重要性はより高まる

データの保護

データを保護するための対策

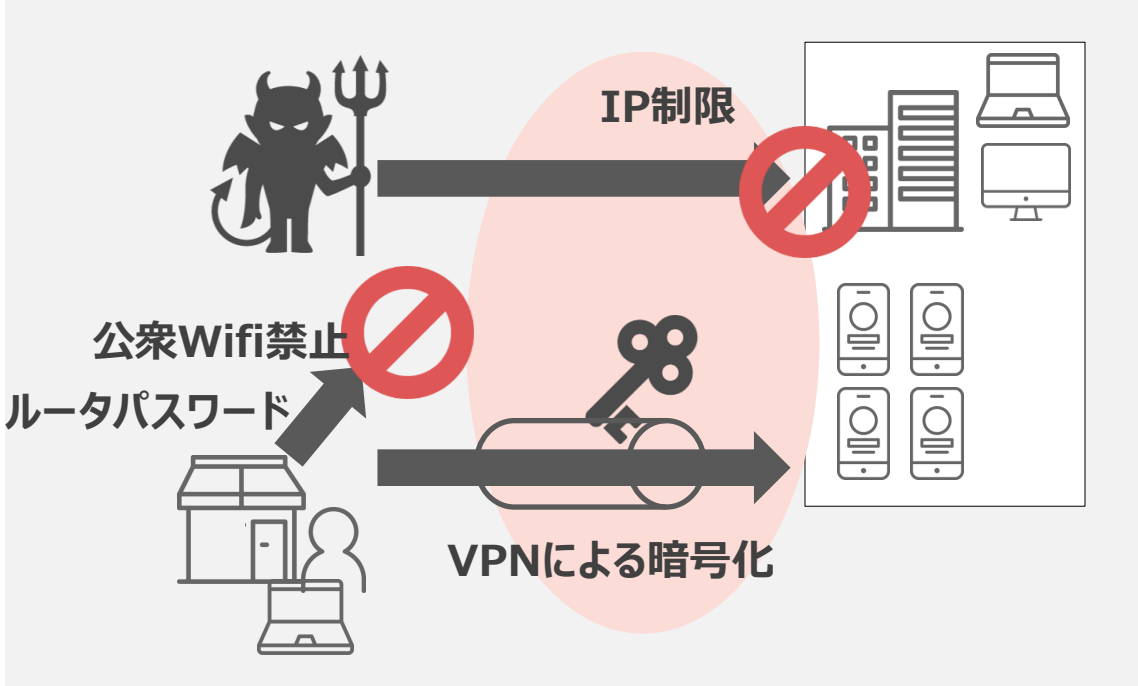


- 端末に保管されているデータの暗号化
- 盗難時の遠隔制御による端末ロック
- 盗難時のデータ消去（リモートデータワイプ）
- 端末データのバックアップ
- シンクライアント化による、データのローカル保存禁止

盗難時の情報漏洩を防止する

ネットワークの安全性確保

外部からのアクセスに対するネットワーク安全性確保

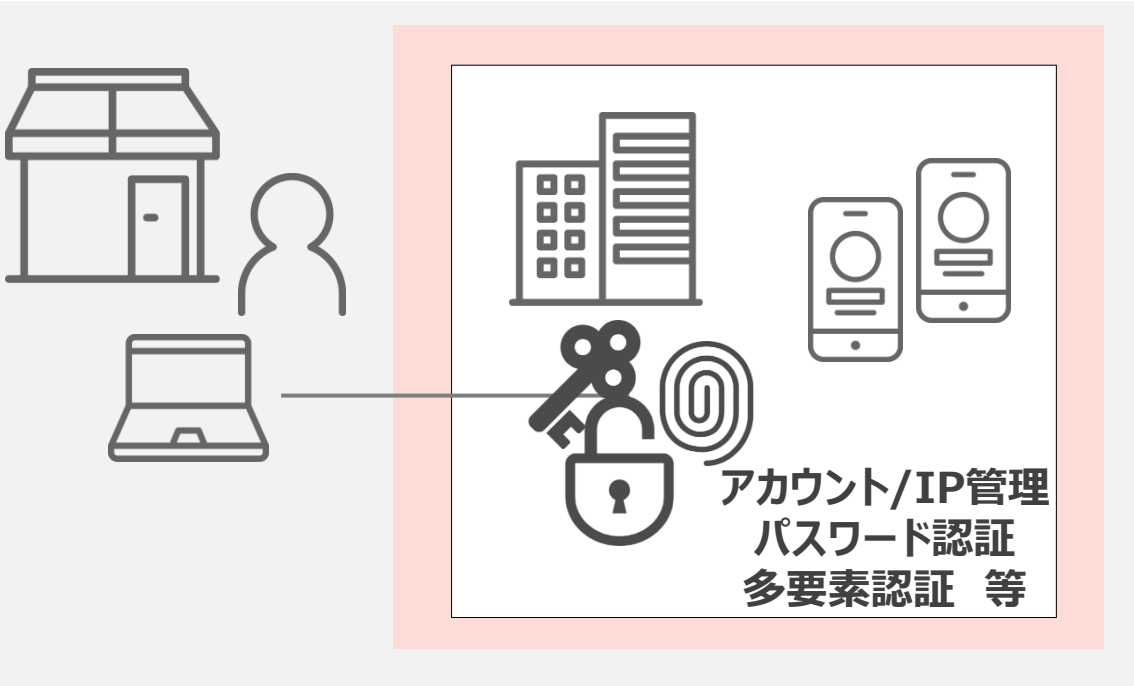


- SSL、VPNなどによる通信暗号化
- 情報システムへの接続元IP制限
- 公衆回線（公衆Wifi）使用の禁止
- Wifiルータの認証パスワード設定
- オープンなスペースでの業務禁止

通信経路上の盗聴や漏洩を防止する

端末の識別と認証

端末の識別と認証による不正アクセス防止



- 接続元IPの把握
- システムアカウントの特定
- パスワード複雑性のルール順守
- ソーシャルエンジニアリングからの保護（バイオメトリクス認証や多要素認証の導入）

接続元の端末やアカウントを管理することにより、不正アクセスを防止する

脆弱性対策/パッチ管理

端末の脆弱性対策

- OSのセキュリティパッチ適用
- ブラウザ/Acrobatなど、汎用的に利用されるサードパーティのパッチ適用
- 情シス担当もテレワークとなったため、リモートによるパッチ適用の仕組みが必要
- 端末ごとのパッチ適用状況把握

システムの脆弱性をねらった攻撃からシステムを保護

参考　～NISTが提唱するパッチ管理のポイント～

広範囲のコンピュータに手作業でパッチを適用する方法は、インストールする必要があるパッチの数が増え、また攻撃者による脆弱性実証コードの開発期間が短くなるにつれて、有効でなくなりつつある。

パッチ適用や脆弱性の監視は気の遠くなるような作業に思えることもあるが、組織内の脆弱性を一貫して軽減することは、自動化されたパッチ技術を有効利用した、テスト済みの統合されたパッチ適用プロセスによって実現できる。

エンタープライズ向けパッチ管理ツールを使用することにより、PVG（またはPVGと緊密に連携するグループ）は、パッチを多数のコンピュータに自動かつ短時間で適用することができる。

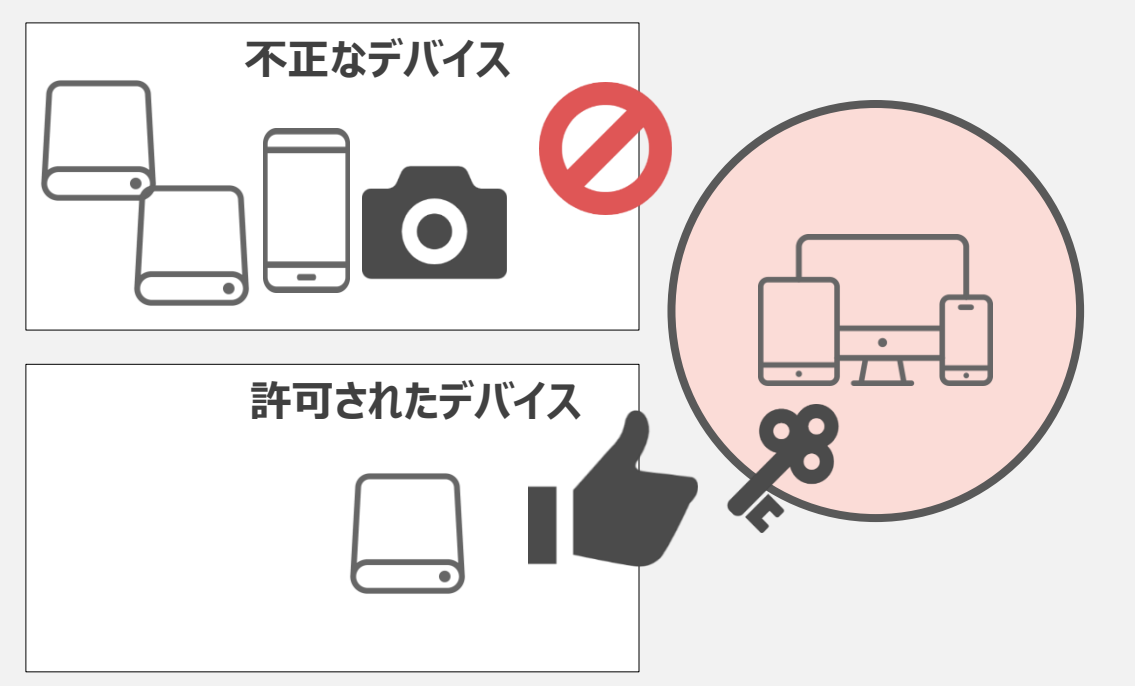
すべての中～大規模組織は、所有する大部分のコンピュータに対してエンタープライズ向けパッチ管理ツールを使用すべきである。**たとえ小規模な組織であっても、何らかの自動化されたパッチ適用ツールに移行すべきである**。

出典　パッチおよび脆弱性管理プログラムの策定　NIST
https://www.ipa.go.jp/files/000025330.pdf

散在する膨大な端末のパッチ適用には自動化が必須

USBデバイスの接続制御

端末へのUSBデバイス接続制限

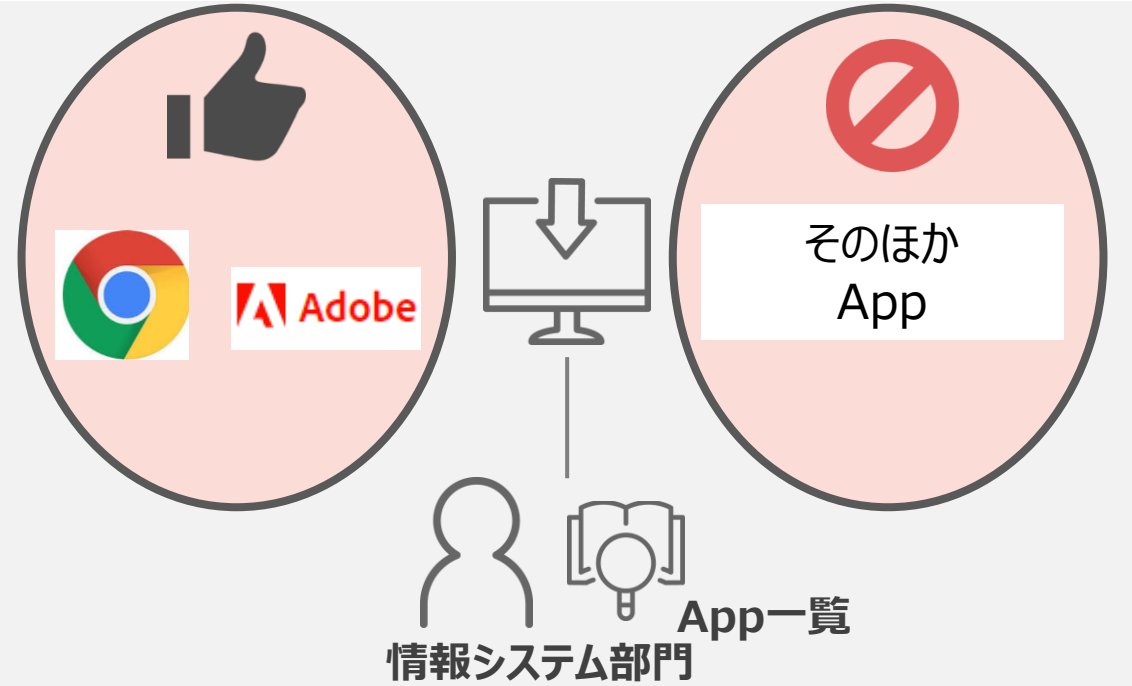


- 許可されたデバイスのみが接続可能
- 接続されているデバイスを把握
- 不正なデバイスが接続されたらアラート通知

許可されたデバイスは許可、それ以外は不正接続として拒否/検知する

アプリケーションの利用制限

不要なアプリのインストールや、Webアクセスを制限

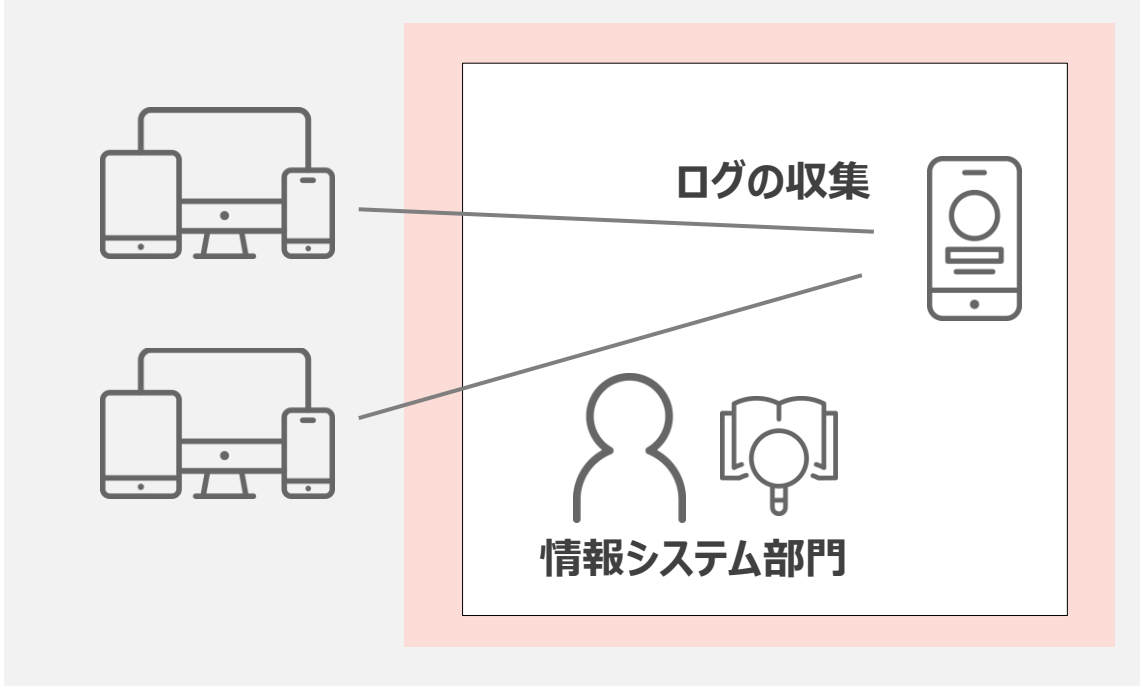


- 不要なプログラムのインストール防止
- 利用しているアプリケーションの把握
- ウェブフィルタ/メールフィルタ

不要なアプリの動作による、サイバー攻撃（バックドアなど）を防止する

証跡の保存と監査

証跡の保存

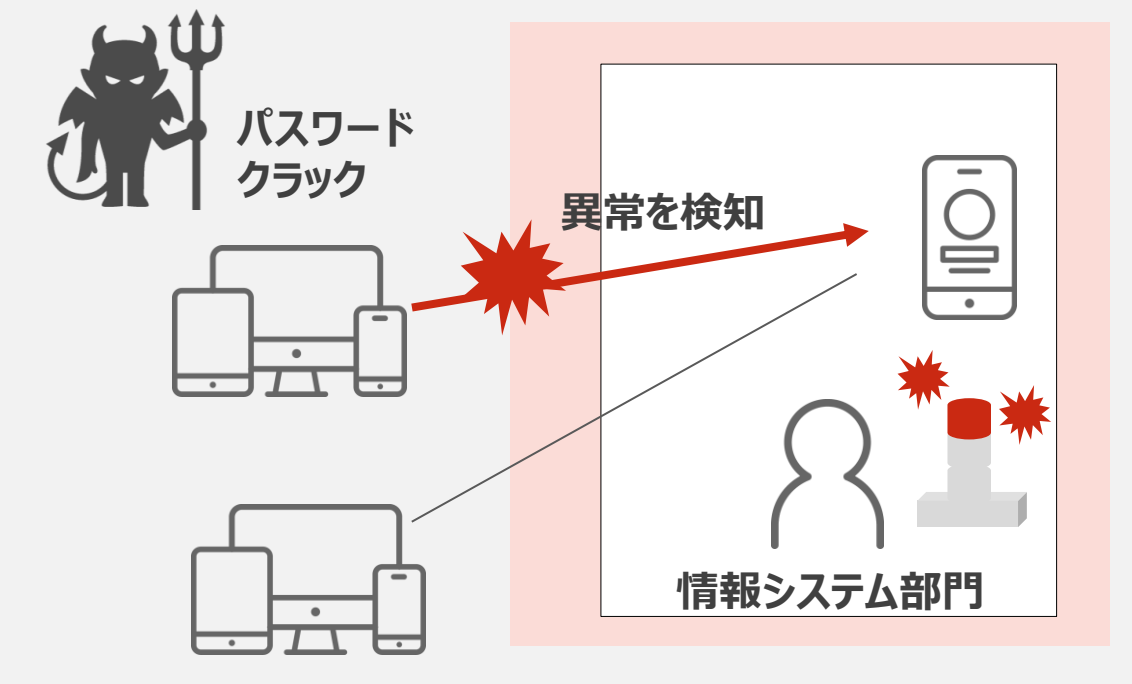


- 端末からのログ収集
- ログの一元管理
- ログの可視化（レポーティング機能）
- 検索性の確保（期間指定、キーワード指定などによる条件検索）
- ログのアーカイブと保管
- 監査対応（日々のチェック、内部監査対応　など）

日々のチェックなどにより、不正な行動/挙動を抑止する

不正利用時のアラート通知

異常な挙動をアラート通知



- 異常な挙動の例
  - 通常ではありえない時間の利用（夜間帯など）
  - パスワードクラック（パスワードを変えての連続ログイン試行）
  - 不正な端末の接続
- 通知方法/タイミング
  - メール
  - パトライト
- 異常時のアクション
  - エスカレーション先、一次調査手順　など

通知方法、タイミング、アクションをすべてきめておく

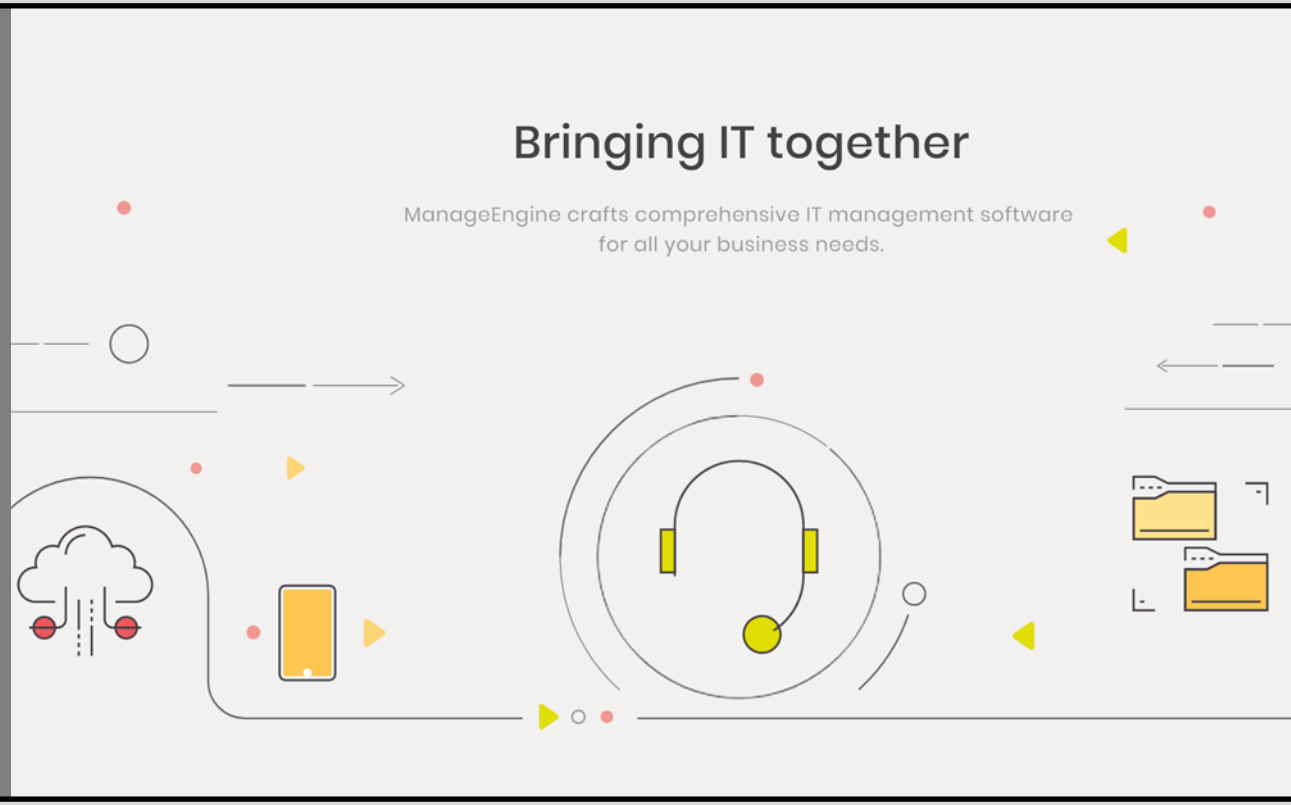
参考　～セキュリティ対策に関連するガイドやフレームワーク～

セキュリティ対策を検討、実施するにあたっては、ガイドラインやフレームワークを参考にすると抜け・漏れを防止することができます。すべてを実施するのではなく、**自組織で重要視される項目が何か、優先度づけをして**の対策を検討するのがセオリーです。

No	文書名	発行元	説明
1	スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書	内閣サイバーセキュリティセンター	「政府機関の情報セキュリティ対策のための統一基準」に準拠した、情報セキュリティ対策の考え方や対策例等を整理したもの。
2	テレワークセキュリティガイドライン	総務省	企業等がテレワークを導入・活用していただくための指針をまとめたもの。
3	パッチおよび脆弱性管理プログラムの策定（SP 800-40）	NIST	NIST（米国国立標準技術研究所）が公開しているコンピューターセキュリティに関する文書、SPシリーズのうちのひとつであり、脆弱性とパッチの管理についてのガイドライン。

情報システム全体に対する対策を検討する場合は、ISMSやPCI-DSSといった、必要に応じた規格やガイドラインをベースに検討とみなおしをおこないます。

さいごに


Bringing IT together
ManageEngine crafts comprehensive IT management software
for all your business needs.

さいごに

テレワークを導入/継続するにあたっては、すべての対策を一度におこなうのは現実的ではありません。

最初は対象とする部署を限定するなど、セキュリティを担保しつつ、運用負荷をみながら導入していることを推奨します。

コロナ終息後も、テレワークは「ニュー・ノーマル」として推進されていくことはまちがいないと思います。

テレワークへの対策がおくれることが、ビジネスへ影響する可能性も十分に考えられます。自組織にできる範囲で早めの対策をとるとよいでしょう。

- ご清聴ありがとうございました -

お問い合わせ先

ゾーホージャパン株式会社

ManageEngine　営業担当

神奈川県横浜市西区みなとみらい三丁目6番1号
みなとみらいセンタービル13階
TEL：045-319-4612
E-MAIL：jp-mesales@zohocorp.com
https://www.manageengine.jp/

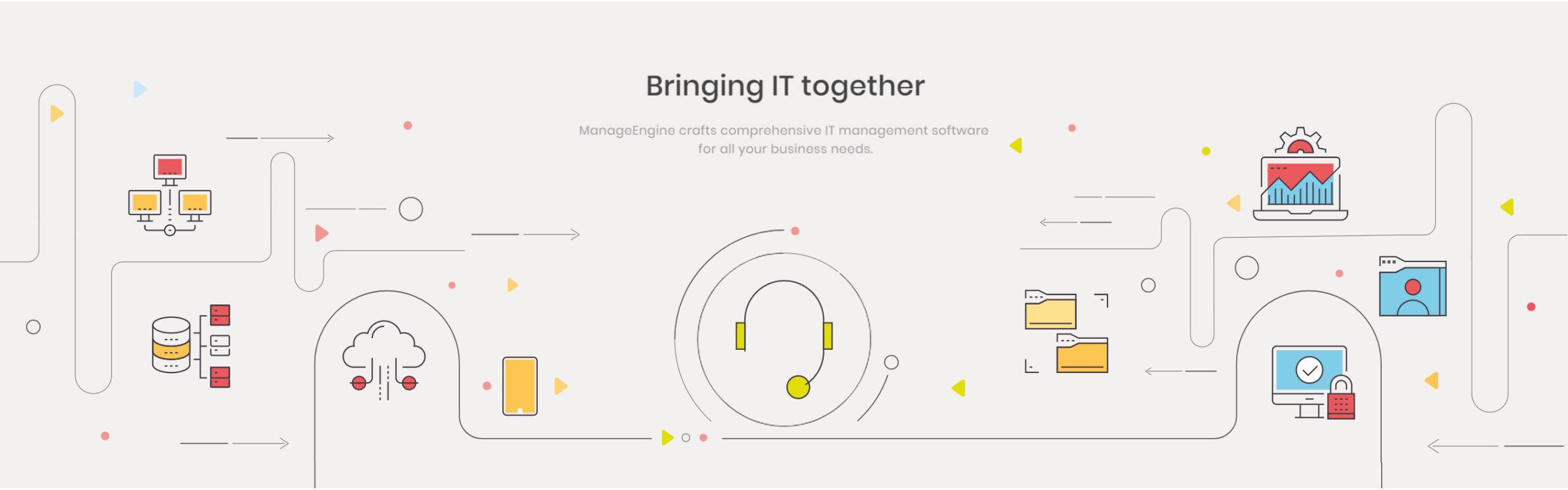
株式会社DXコンサルティング

DXコンサルティング　営業担当

東京都千代田五番町 12-1　番町会館
TEL：03-5211-0812
E-MAIL　itsm@dx-consul.co.jp
http://www.dx-consul.co.jp/business/consulting.html

お気軽にお問い合わせください

ManageEngine



企業のエンドポイントを守る

テレワーク中の資産管理・セキュリティ対策に役立つ製品のご紹介

ゾーホージャパン株式会社

会社紹介

社名

ゾーホージャパン株式会社
（英文名： ZOHO Japan Corporation）

神奈川県 横浜市 西区みなとみらい3-6-1
みなとみらいセンタービル13階

（サテライトオフィス） 静岡県榛原郡川根本町東藤川1013-1

グローバル本社

ZOHO Corporation Pvt. Ltd

Chennai, Tamil Nadu, India

クラウド型ソリューション

企業のIT化・業務効率の向上をサポート
全世界で**3,000万ユーザー**が利用

(Est. 2005)

ManageEngine

IT運用管理ツール

コストパフォーマンスの高いソフトウェア群
全世界で**18万社**以上の導入実績

(Est. 2002)

ManageEngine（マネージエンジン）紹介

ITインフラ

- ネットワーク管理ソリューション
- サーバー・アプリケーション管理ソリューション

ID・ログ・セキュリティ

- Active Directory管理ソリューション
- ログ管理＆セキュリティソリューション

ヘルプデスク

- ヘルプデスクソリューション
- クライアント管理ソリューション

必要機能を詰め込んだパッケージ

あらゆる企業や組織で共通して必要とされる機能を、パッケージ化して標準搭載

費用と工数を最小化

自社に必要なものだけを選択し導入することで、導入や運用にかかわる費用と工数を最小化

グローバル対応

グローバルで必要とされる機能と多言語へ対応

IT運用管理とセキュリティ対策に必要な製品を幅広く提供しています

アジェンダ

1. 企業のエンドポイントを守る！製品の概要紹介
2. テレワーク中のエンドポイント管理に役立つ 製品の機能紹介
3. 参考情報

ManageEngine

アジェンダ

1. 企業のエンドポイントを守る！製品の概要紹介
2. テレワーク中のエンドポイント管理に役立つ 製品の機能紹介
3. 参考情報

ManageEngine

企業のエンドポイントを守る！製品の概要紹介

ManageEngine
Desktop Central

統合エンドポイント管理ツール

- パッチ管理、ソフトウェア配布、インベントリ管理など、豊富な機能を搭載
- オプションライセンスを追加することで、モバイルデバイスもまとめて管理可能

ManageEngine
Patch Manager Plus

パッチ管理ツール

- Desktop Centralのパッチ管理機能のみを切り出した製品
- WSUSや、他社製資産管理ツールとの併用も可能

ご要件に応じて、必要な製品をご選択いただけます

Desktop Central　主な機能一覧

パッチ管理

社内の脆弱性パッチ管理を
一元管理し、脆弱性を低減

ソフトウェア配布

リモートからソフトウェアのインストール、
アンインストールを実施し、工数を削減

インベントリ管理

自動的にハードウェア・ソフトウェアの最
新情報を収集
その他ソフトウェアの禁止や実行ファイル
の制御なども可能

モバイルデバイス管理

プロファイル設定の一括適用や、
盗難・紛失時のロック/ワイプなどに
より安全にモバイルデバイスを管理

電源管理

電源設定の適用、スクリーンセーバー
の停止、Wake On LANによる電源
ONおよび未使用コンピューターの
シャットダウン

システムマネージャー

コマンド実行やサービス、プロセスの
開始/停止、レジストリの変更など
きめ細かいシステム設定

リモートコントロール

画面表示、ファイル転送、操作録画
などにより、エンドユーザーに対する円
滑なトラブルシューティングをサポート

USB制御

USBデバイスの利用を制限し、データ
流出の脅威とデバイスによるウイルス
やスパイウェアの感染の懸念を低減

スクリプト配布

作成したスクリプトを実行し、端末に
同一の設定を適用する等が可能

クラウド版・オンプレミス版からご選択いただけます

Patch Manager Plus　主な機能一覧

パッチ管理

社内の脆弱性パッチ管理を
一元管理し、脆弱性を低減

リモートシャットダウン・再起動

リモートおよびスケジューリングによるシャットダウン・再起動によりエンドユーザーに対する円滑なトラブルシューティングをサポート

パッチの拒否

アプリ単位・パッチ単位で
拒否の設定が可能

ソフトウェア自動更新の無効化

ソフトウェアの自動更新を無効化する
スクリプトを配布可能

レポート

標準で用意されている様々な
レポートにより、状況を正確に把握

- パッチレポート
- システムレポート
- 設定レポート

Desktop Centralのパッチ管理機能を切り出した製品です

対応しているOS一覧

管理対象にはエージェント（モバイルデバイスの場合はアプリ）のインストールが必須

エージェントをインストール可能なOS

Windows：7 / 8 / 8.1 / 10

Windows Server：2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019

Mac OS：10.11 / 10.12 / 10.13 / 10.14 / 10.15 / 11.1

Linux：Red Hat Enterprise Linux 7以降 / CentOS 7以降 / Fedora 30以降 /
Ubuntu 14.04 LTS以降 / Debian 8以降 / OpenSUSE 15.1以降 /
Linux Mint 18以降 / SUSE Enterprise Linux 11以降

※エージェントをインストール可能なすべてのOSがパッチ管理に対応しているわけではございません。

モバイルデバイス管理のサポート対象OS

iOS：4.0以上

Android：4.0以上

iPadOS：13.0以上

Windows Phone：8.1 / 10

ChromeOS：57.0以上

macOS：10.7以上

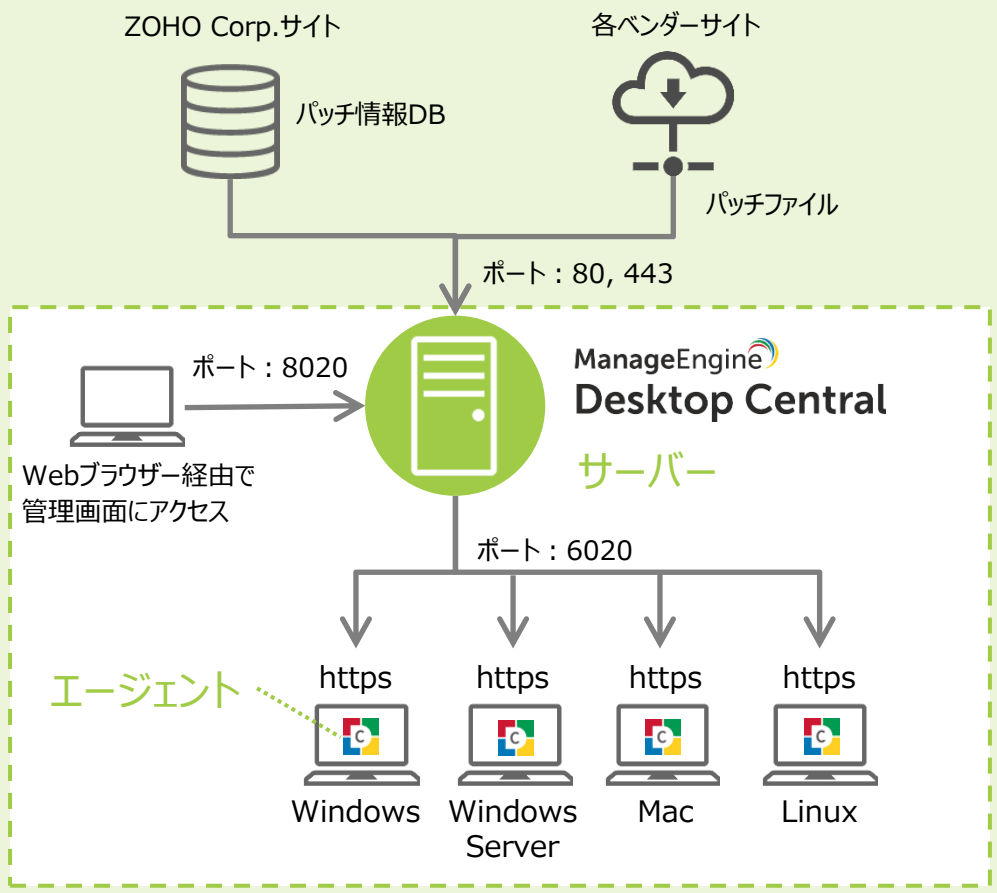
tvOS：7.0以上

システム要件を見る：https://www.manageengine.jp/products/Desktop_Central/system-requirements.html

最新情報は、Webページまたは営業窓口にてご確認ください

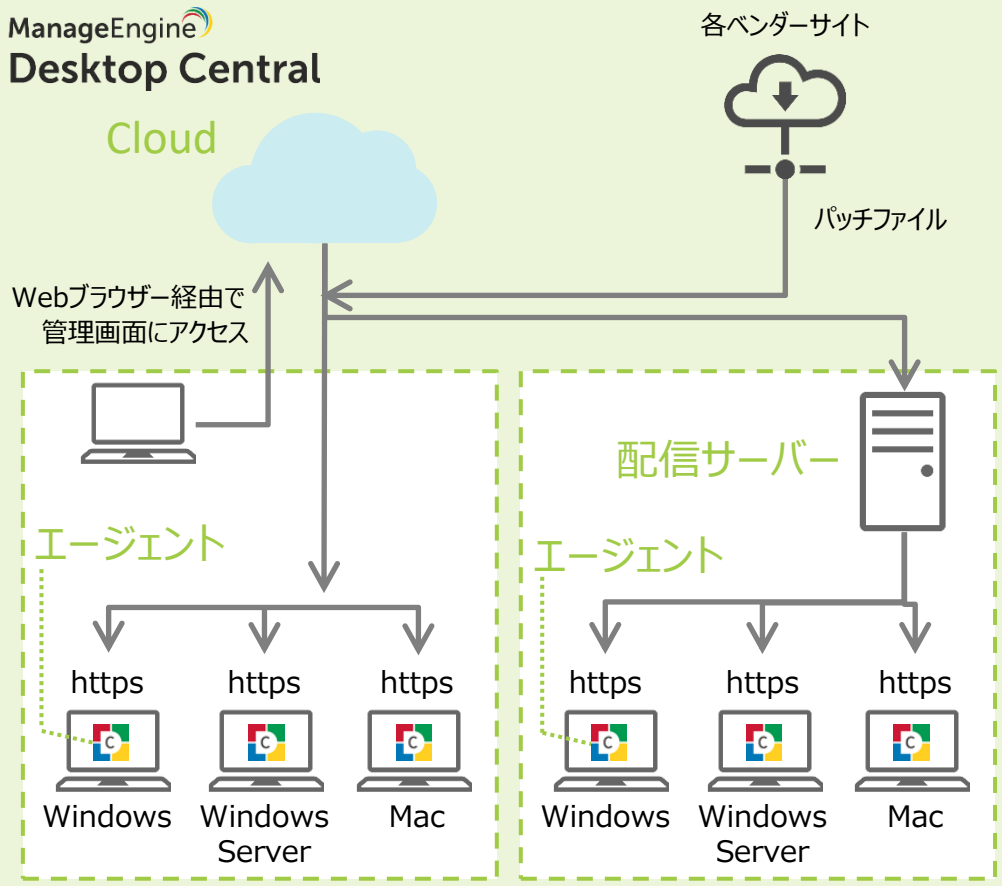
利用形態ごとのシステムアーキテクチャー

オンプレミス版



Desktop Central オンプレミス版利用イメージ

クラウド版



Desktop Central クラウド版利用イメージ

アジェンダ

1. 企業のエンドポイントを守る！製品の概要紹介
2. テレワーク中のエンドポイント管理に役立つ 製品の機能紹介
3. 参考情報

ManageEngine

本日ご紹介する機能一覧

1 パッチ管理

管理対象に自動でパッチを当てる

2 インベントリ管理

社内のIT資産情報を棚卸しする

3 USB制御

USBの使用を禁止する

4 その他おすすめ機能

テレワーク中に活用したい便利機能

Desktop Centralの画面を用いて、デモンストレーション形式で紹介します

本日ご紹介する機能一覧

1 パッチ管理

管理対象に自動でパッチを当てる

2 インベントリ管理

社内のIT資産情報を棚卸しする

3 USB制御

USBの使用を禁止する

4 その他おすすめ機能

テレワーク中に活用したい便利機能

Desktop Centralの画面を用いて、デモンストレーション形式で紹介します

1 - 1　パッチ管理　対応OS・アプリケーション紹介

対応OS

Windows： 7 / 8 / 8.1 / 10（Windows 7はESUのみ）

Windows Server： 2008 / 2008 R2 / 2012 / 2012R2 / 2016 / 2019

Mac： 11-Big Sur / X–Catalina / X-El Capitan / X–Mojave / X–Sierra / X-High Sierra

Linux： Red Hat Enterprise Linux/ SUSE Linux / CentOS / Ubuntu / Debian

対応アプリケーションの一例

Microsoft Office：2019 / 2016 / 2013 / Microsoft 365 / Office 2016 for Mac など

Webブラウザー：Google Chrome / Mozilla Firefox / Internet Explorer　など

その他：Adobe Acrobat Reader DC / Adobe Flash Player / Java SE Development Kit　など

サーバー系：Apache / Bind / MySQL / OpenSSH / PostgreSQL / SQLite / Ruby / Python など

対応OS・アプリケーション一覧：https://www.manageengine.jp/products/Desktop_Central/patch_management_supported_application.html

Windows、Mac、Linuxに加え、350種類を超えるサードパーティ製品のパッチに対応

1 -2　パッチ管理　管理対象に自動でパッチを当てる方法

1

パッチDBを設定

管理したいパッチを選び、
最新の脆弱性・パッチ情報を
自動で集める

2

自動配布のルールを作成

適用したいパッチを選び、
管理対象・配布日時を
設定する

3

適用状況を確認

すべての管理対象への
パッチ配布が成功しているか、
結果を確かめる

簡単な設定で、パッチを自動的に配布できます

1 -2　パッチ管理　管理対象に自動でパッチを当てる方法

1

パッチDBを設定

管理したいパッチを選び、
最新の脆弱性・パッチ情報を
自動で集める

2

自動配布のルールを作成

適用したいパッチを選び、
管理対象・配布日時を
設定する

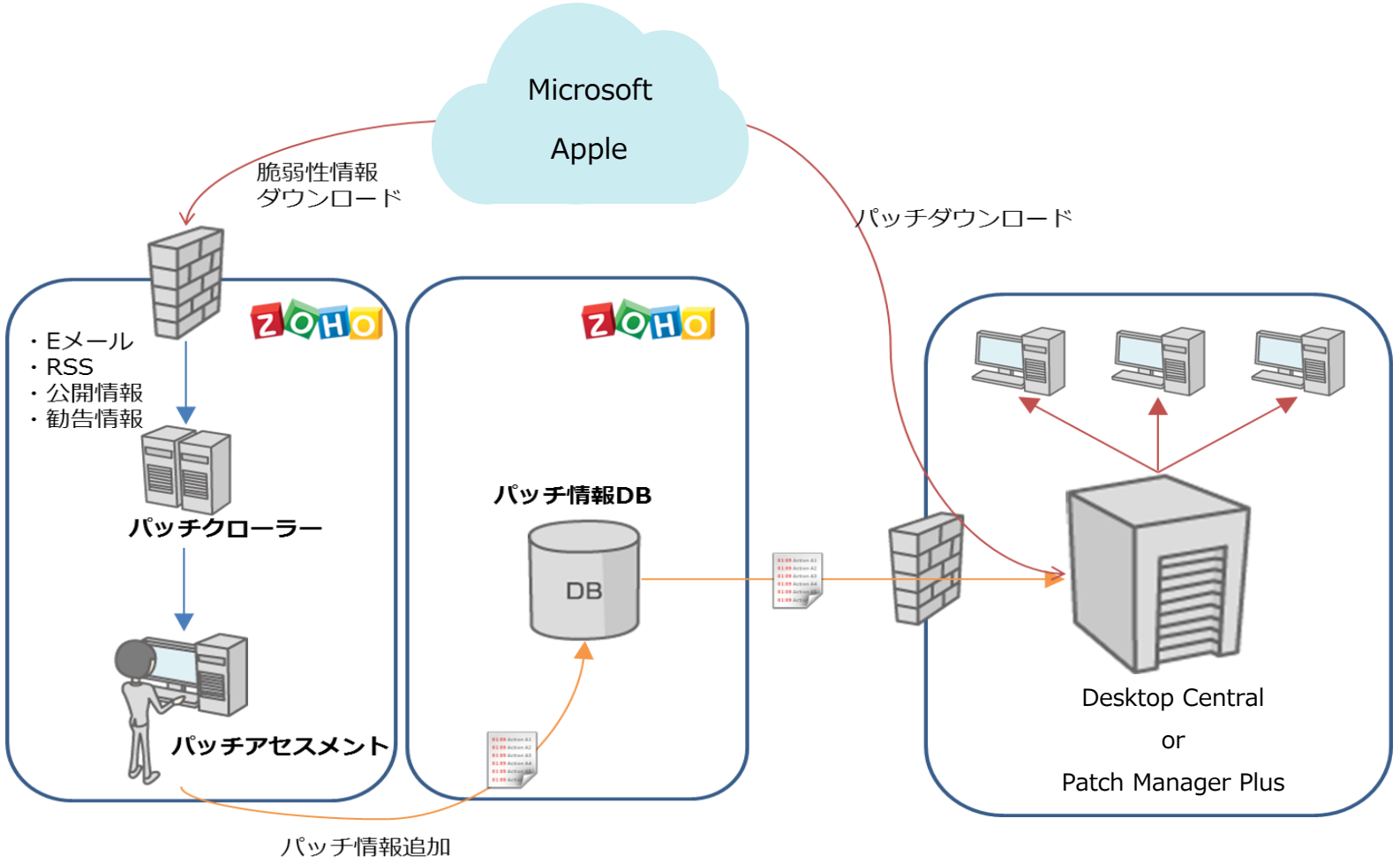
3

適用状況を確認

すべての管理対象への
パッチ配布が成功しているか、
結果を確かめる

簡単な設定で、パッチを自動的に配布できます

参考情報　パッチ情報の取得と適用の仕組み



1 -2　パッチ管理　管理対象に自動でパッチを当てる方法

1

パッチDBを設定

管理したいパッチを選び、
最新の脆弱性・パッチ情報を
自動で集める

2

自動配布のルールを作成

適用したいパッチを選び、
管理対象・配布日時を
設定する

3

適用状況を確認

すべての管理対象への
パッチ配布が成功しているか、
結果を確かめる

簡単な設定で、パッチを自動的に配布できます

ManageEngine
Desktop Central 10

SDPへジャンプ　ライセンス　ビルドバージョン:10.0.587

ホーム　構成　パッチ管理　ソフトウェア配布　インベントリ　OS配備　モバイルデバイス管理　ツール　レポート　エージェント　管理　サポート

アラート　(1)　情報　(1)　トレーニングビデオ

メールサーバーが未設定です
メールサーバーに接続できません。Telnetコマンドを用いて、メールサーバーへの接続が可能か確認してください。設定

デモンストレーション形式での機能紹介

概要　リン

ntralの利用状況を把握する機能の要望

最近追加/変更した構成

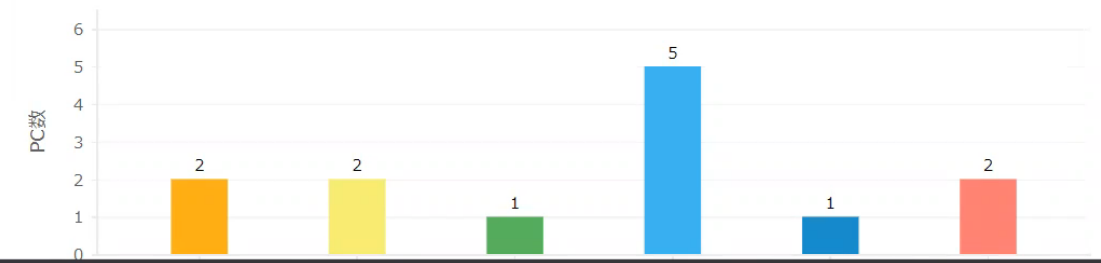
構成名

test4
appblock_test_on_M1Mac
セルフサービスポータルの不具合修正
MyConfiguration2032
Macアップグレード禁止

再試行中　期限切れ

構成ステータス

OSごとのPC一覧



ソフトウェアの概要

すべてのソフトウェア	: 3664
ライセンス準拠	: 1
ライセンス過剰	: 7
ライセンス不足	: 0
ライセンスの有効期限切れ	: 2

javascript:openWindowFromTab('/upgradeLicense.do?actionToCall=loadDetails','UpgradeLicense','scrollbars=yes,resizable=yes,','700','600')

1-4　パッチ管理　管理対象に自動でパッチを当てる方法

1

パッチDBを設定

管理したいパッチを選び、
最新の脆弱性・パッチ情報を
自動で集める

2

自動配布のルールを作成

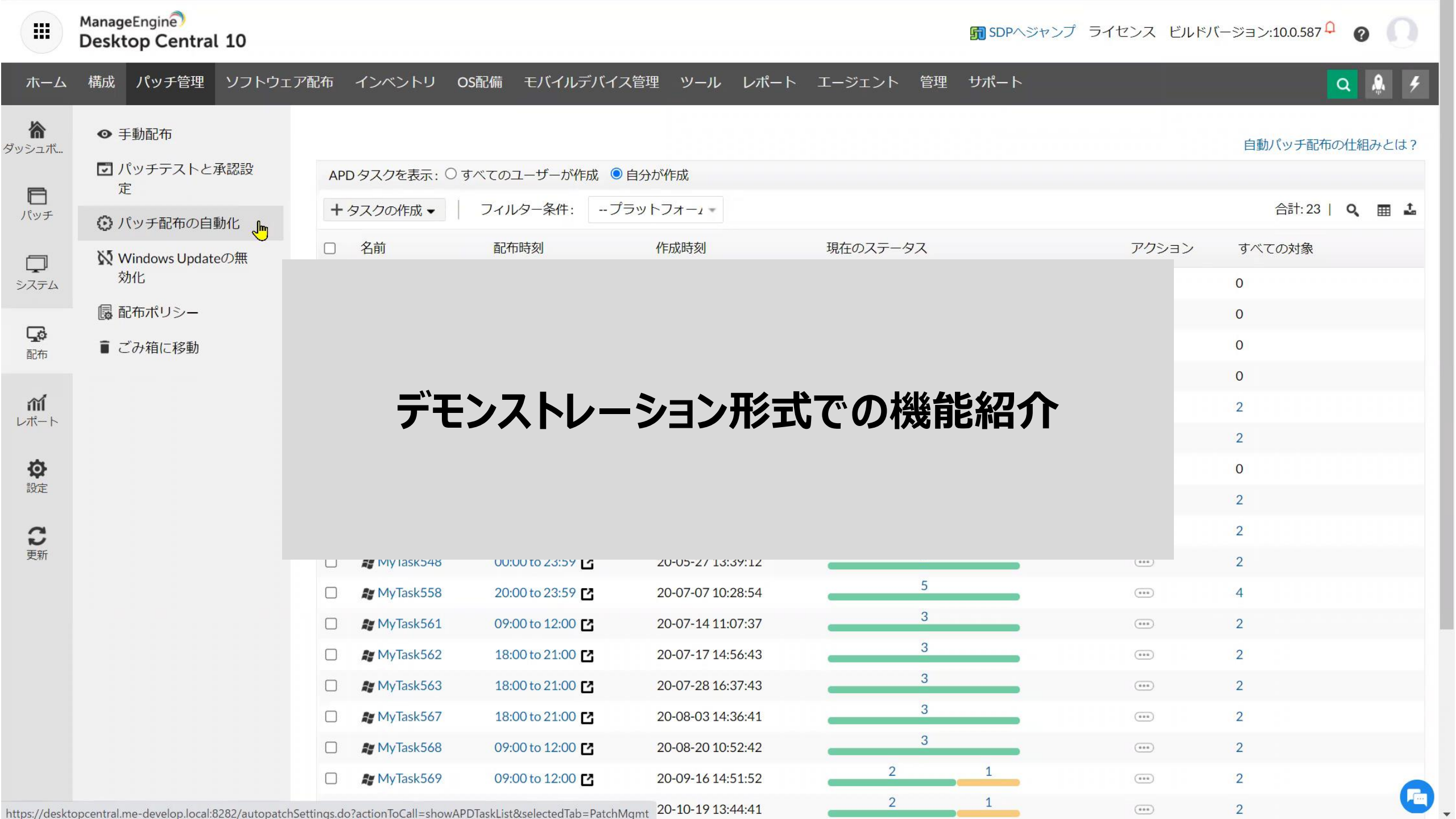
適用したいパッチを選び、
管理対象・配布日時を
設定する

3

適用状況を確認

すべての管理対象への
パッチ配布が成功しているか、
結果を確かめる

簡単な設定で、パッチを自動的に配布できます


ManageEngine
Desktop Central 10
SDPへジャンプ
ライセンス
ビルドバージョン:10.0.587
ホーム
構成
パッチ管理
ソフトウェア配布
インベントリ
OS配備
モバイルデバイス管理
ツール
レポート
エージェント
管理
サポート
ダッシュボ...
パッチ
システム
配布
レポート
設定
更新
手動配布
パッチテストと承認設定
パッチ配布の自動化
Windows Updateの無効化
配布ポリシー
ごみ箱に移動
自動パッチ配布の仕組みとは？
APD タスクを表示：すべてのユーザーが作成 自分が作成
タスクの作成
フィルター条件：
合計: 23
名前
配布時刻
作成時刻
現在のステータス
アクション
すべての対象
デモンストレーション形式での機能紹介
MyTask558 20:00 to 23:59 20-07-07 10:28:54 5 4
MyTask561 09:00 to 12:00 20-07-14 11:07:37 3 2
MyTask562 18:00 to 21:00 20-07-17 14:56:43 3 2
MyTask563 18:00 to 21:00 20-07-28 16:37:43 3 2
MyTask567 18:00 to 21:00 20-08-03 14:36:41 3 2
MyTask568 09:00 to 12:00 20-08-20 10:52:42 3 2
MyTask569 09:00 to 12:00 20-09-16 14:51:52 2 1 2
20-10-19 13:44:41 2 1 2
https://desktopcentral.me-develop.local:8282/autopatchSettings.do?actionToCall=showAPDTaskList&selectedTab=PatchMgmt

1-5　パッチ管理　管理対象に自動でパッチを当てる方法

1

パッチDBを設定

管理したいパッチを選び、
最新の脆弱性・パッチ情報を
自動で集める

2

自動配布のルールを作成

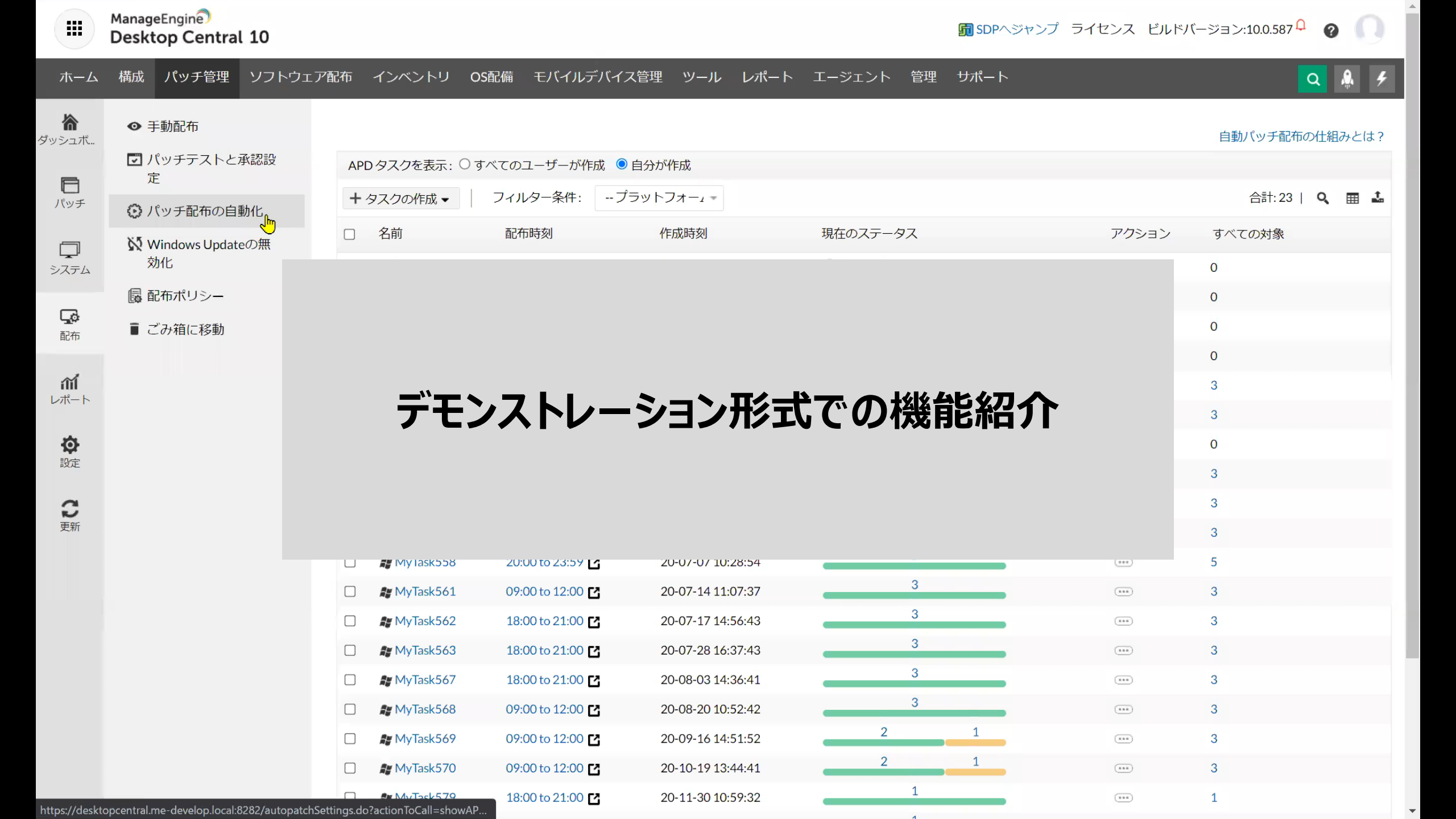
適用したいパッチを選び、
管理対象・配布日時を
設定する

3

適用状況を確認

すべての管理対象への
パッチ配布が成功しているか、
結果を確かめる

簡単な設定で、パッチを自動的に配布できます


ManageEngine
Desktop Central 10
SDPへジャンプ
ライセンス
ビルドバージョン:10.0.587
ホーム
構成
パッチ管理
ソフトウェア配布
インベントリ
OS配備
モバイルデバイス管理
ツール
レポート
エージェント
管理
サポート
ダッシュボ...
パッチ
システム
配布
レポート
設定
更新
手動配布
パッチテストと承認設定
パッチ配布の自動化
Windows Updateの無効化
配布ポリシー
ごみ箱に移動
自動パッチ配布の仕組みとは？
APD タスクを表示：
すべてのユーザーが作成
自分が作成
タスクの作成
フィルター条件：
--プラットフォー
合計: 23
名前
配布時刻
作成時刻
現在のステータス
アクション
すべての対象
デモンストレーション形式での機能紹介
MyTask561 09:00 to 12:00 20-07-14 11:07:37
MyTask562 18:00 to 21:00 20-07-17 14:56:43
MyTask563 18:00 to 21:00 20-07-28 16:37:43
MyTask567 18:00 to 21:00 20-08-03 14:36:41
MyTask568 09:00 to 12:00 20-08-20 10:52:42
MyTask569 09:00 to 12:00 20-09-16 14:51:52
MyTask570 09:00 to 12:00 20-10-19 13:44:41
18:00 to 21:00 20-11-30 10:59:32
https://desktopcentral.me-develop.local:8282/autopatchSettings.do?actionToCall=showAP...

1 -2　パッチ管理　管理対象に自動でパッチを当てる方法

1

パッチDBを設定

管理したいパッチを選び、
最新の脆弱性・パッチ情報を
自動で集める

2

自動配布のルールを作成

適用したいパッチを選び、
管理対象・配布日時を
設定する

3

適用状況を確認

すべての管理対象への
パッチ配布が成功しているか、
結果を確かめる

簡単な設定で、パッチを自動的に配布できます

本日ご紹介する機能一覧

1 パッチ管理

管理対象に自動でパッチを当てる

2 インベントリ管理

社内のIT資産情報を棚卸しする

3 USB制御

USBの使用を禁止する

4 その他おすすめ機能

テレワーク中に活用したい便利機能

Desktop Centralの画面を用いて、デモンストレーション形式で紹介します

2 インベントリ管理

1

IT資産情報を棚卸し

コンピューターのハードウェア情報や、
インストールされているソフトウェア情報を
自動的に把握する

2

禁止ソフトウェアを設定

特定のアプリケーションの使用を禁止し、
使用が検出された場合は
アンインストールを実行する

社内のIT資産情報を、自動的に収集します

2 インベントリ管理

1

IT資産情報を棚卸し

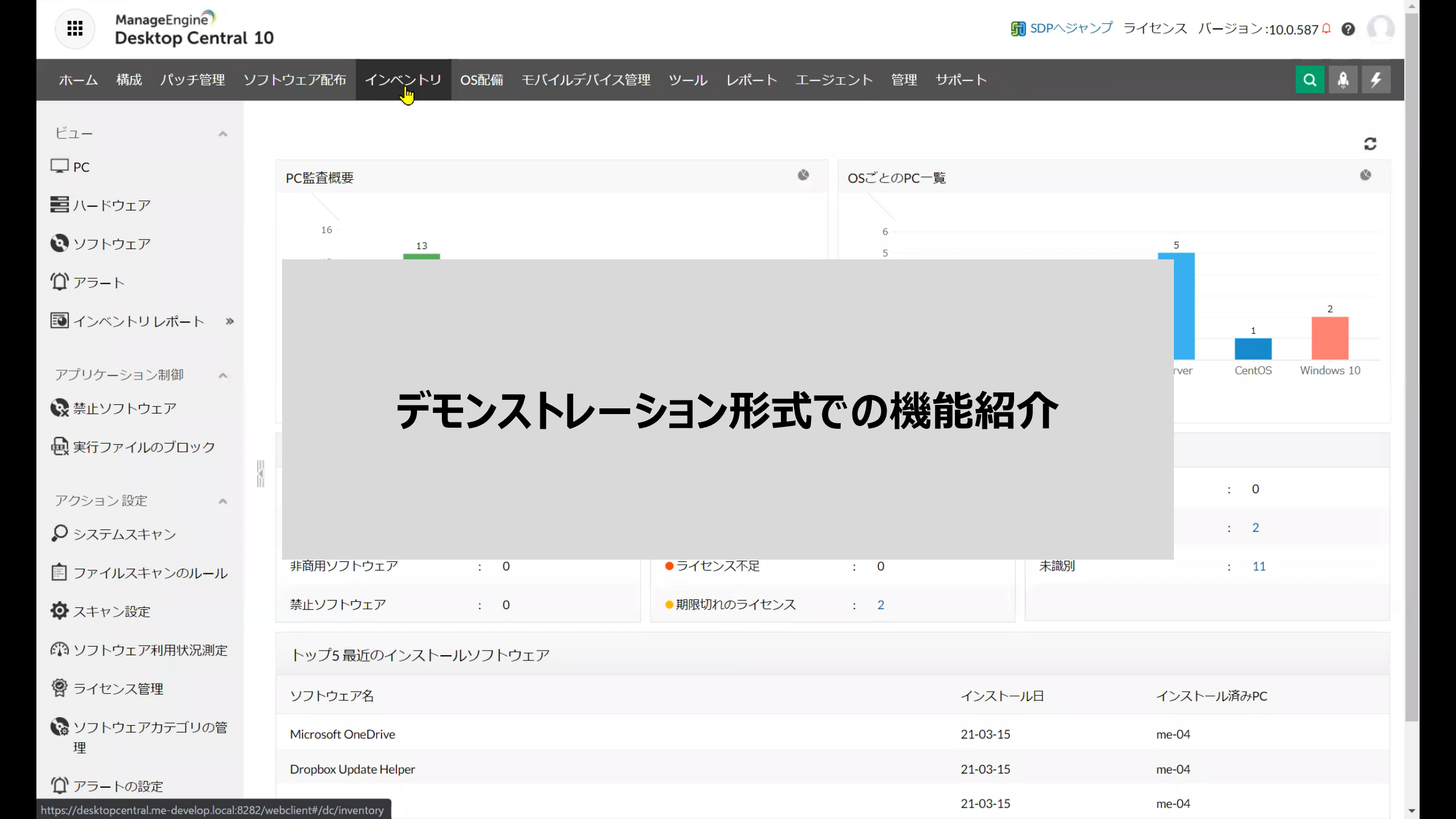
コンピューターのハードウェア情報や、
インストールされているソフトウェア情報を
自動的に把握する

2

禁止ソフトウェアを設定

特定のアプリケーションの使用を禁止し、
使用が検出された場合は
アンインストールを実行する

社内のIT資産情報を、自動的に収集します


ManageEngine
Desktop Central 10
SDPへジャンプ
ライセンス
バージョン:10.0.587
ホーム
構成
パッチ管理
ソフトウェア配布
インベントリ
OS配備
モバイルデバイス管理
ツール
レポート
エージェント
管理
サポート
ビュー
PC
ハードウェア
ソフトウェア
アラート
インベントリ レポート
アプリケーション制御
禁止ソフトウェア
実行ファイルのブロック
アクション設定
システムスキャン
ファイルスキャンのルール
スキャン設定
ソフトウェア利用状況測定
ライセンス管理
ソフトウェアカテゴリの管理
アラートの設定
PC監査概要
16
13
OSごとのPC一覧
6
5
5
2
1
CentOS
Windows 10
デモンストレーション形式での機能紹介
非商用ソフトウェア : 0
禁止ソフトウェア : 0
ライセンス不足 : 0
期限切れのライセンス : 2
未識別 : 11
トップ5 最近のインストールソフトウェア
ソフトウェア名
インストール日
インストール済みPC
Microsoft OneDrive
21-03-15
me-04
Dropbox Update Helper
21-03-15
me-04
21-03-15
me-04
https://desktopcentral.me-develop.local:8282/webclient#/dc/inventory

2 インベントリ管理

1

IT資産情報を棚卸し

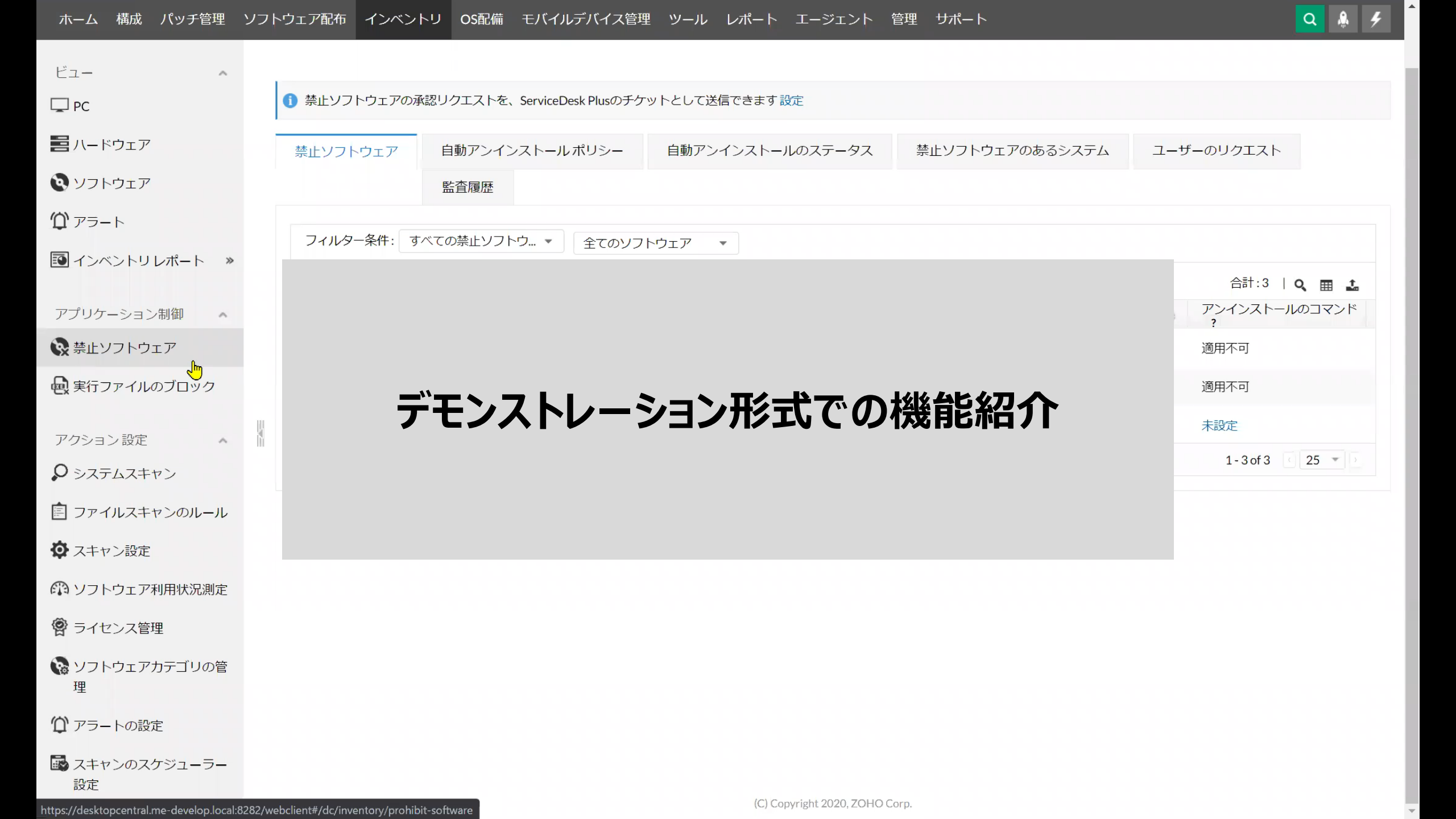
コンピューターのハードウェア情報や、
インストールされているソフトウェア情報を
自動的に把握する

2

禁止ソフトウェアを設定

特定のアプリケーションの使用を禁止し、
使用が検出された場合は
アンインストールを実行する

社内のIT資産情報を、自動的に収集します


ホーム 構成 パッチ管理 ソフトウェア配布 インベントリ OS配備 モバイルデバイス管理 ツール レポート エージェント 管理 サポート
ビュー
PC
ハードウェア
ソフトウェア
アラート
インベントリ レポート
アプリケーション制御
禁止ソフトウェア
実行ファイルのブロック
アクション 設定
システムスキャン
ファイルスキャンのルール
スキャン設定
ソフトウェア利用状況測定
ライセンス管理
ソフトウェアカテゴリの管理
アラートの設定
スキャンのスケジューラー設定
禁止ソフトウェアの承認リクエストを、ServiceDesk Plusのチケットとして送信できます 設定
禁止ソフトウェア
自動アンインストール ポリシー
自動アンインストールのステータス
禁止ソフトウェアのあるシステム
ユーザーのリクエスト
監査履歴
フィルター条件:
すべての禁止ソフトウ...
全てのソフトウェア
合計:3
アンインストールのコマンド
適用不可
適用不可
未設定
1 - 3 of 3
25
デモンストレーション形式での機能紹介
(C) Copyright 2020, ZOHO Corp.
https://desktopcentral.me-develop.local:8282/webclient#/dc/inventory/prohibit-software

2 インベントリ管理

1

IT資産情報を棚卸し

コンピューターのハードウェア情報や、
インストールされているソフトウェア情報を
自動的に把握する

2

禁止ソフトウェアを設定

特定のアプリケーションの使用を禁止し、
使用が検出された場合は
アンインストールを実行する

社内のIT資産情報を、自動的に収集します

本日ご紹介する機能一覧

1 パッチ管理

管理対象に自動でパッチを当てる

2 インベントリ管理

社内のIT資産情報を棚卸しする

3 USB制御

USBの使用を禁止する

4 その他おすすめ機能

テレワーク中に活用したい便利機能

Desktop Centralの画面を用いて、デモンストレーション形式で紹介します

3 USB制御

1

ユーザーのUSB使用を禁止

デバイスの種類ごとに使用許可を設定し、

ウイルス感染・情報漏洩を防ぐ

特定のUSBのみ使用を許すことも可能

2

USB使用状況を監査

レポート機能を活用し、

各コンピューターごとのUSB使用履歴を

まとめて表示・確認する

USBの使用を禁止し、セキュリティを強化します

3 USB制御

1

ユーザーのUSB使用を禁止

デバイスの種類ごとに使用許可を設定し、

ウイルス感染・情報漏洩を防ぐ

特定のUSBのみ使用を許すことも可能

2

USB使用状況を監査

レポート機能を活用し、

各コンピューターごとのUSB使用履歴を

まとめて表示・確認する

USBの使用を禁止し、セキュリティを強化します

ManageEngine
Desktop Central 10

SDPへジャンプ　ライセンス　バージョン:10.0.587

ホーム　構成　パッチ管理　ソフトウェア配布　インベントリ　OS配備　モバイルデバイス管理　ツール　レポート　エージェント　管理　サポート

構成の追加
- 構成
- テンプレート
- コレクション

ビュー
- ごみ箱に移動

レポート
- USBレポート
- 構成レポート

設定
- 構成の設定
- スクリプトリポジトリ

Need more Configurations?

構成の追加

ユーザー構成はユーザーのログイン/リフレッシュサイクル時に適用され、コンピューター構成はコンピューター起動/リフレッシュサイクル時に適用されます。

Windows　Mac　Linux

ネットワークプリンター　ショートカット　ユーザー管理　WiFi

クイックリンク　表示

デモンストレーション形式での機能紹介

3 USB制御

1

ユーザーのUSB使用を禁止

デバイスの種類ごとに使用許可を設定し、

ウイルス感染・情報漏洩を防ぐ

特定のUSBのみ使用を許すことも可能

2

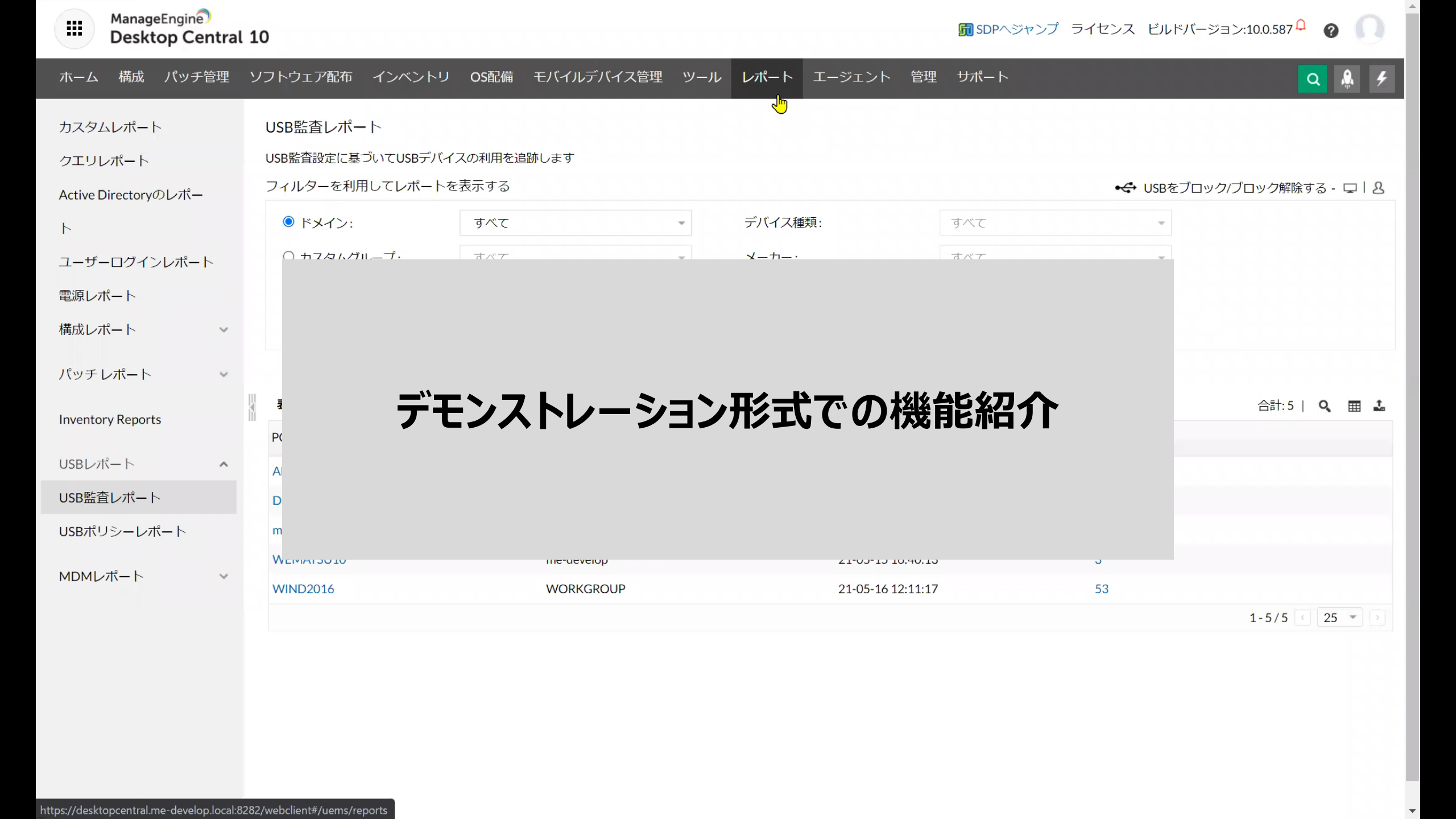
USB使用状況を監査

レポート機能を活用し、

各コンピューターごとのUSB使用履歴を

まとめて表示・確認する

USBの使用を禁止し、セキュリティを強化します


ManageEngine
Desktop Central 10
SDPへジャンプ
ライセンス
ビルドバージョン:10.0.587
ホーム
構成
パッチ管理
ソフトウェア配布
インベントリ
OS配備
モバイルデバイス管理
ツール
レポート
エージェント
管理
サポート
カスタムレポート
クエリレポート
Active Directoryのレポート
ユーザーログインレポート
電源レポート
構成レポート
パッチレポート
Inventory Reports
USBレポート
USB監査レポート
USBポリシーレポート
MDMレポート
USB監査レポート
USB監査設定に基づいてUSBデバイスの利用を追跡します
フィルターを利用してレポートを表示する
USBをブロック/ブロック解除する -
ドメイン:
すべて
デバイス種類:
すべて
カスタムグループ:
メーカー:
デモンストレーション形式での機能紹介
合計: 5
WIND2016
WORKGROUP
21-05-16 12:11:17
53
1 - 5 / 5
25
https://desktopcentral.me-develop.local:8282/webclient#/uems/reports

3 USB制御

1

ユーザーのUSB使用を禁止

デバイスの種類ごとに使用許可を設定し、

ウイルス感染・情報漏洩を防ぐ

特定のUSBのみ使用を許すことも可能

2

USB使用状況を監査

レポート機能を活用し、

各コンピューターごとのUSB使用履歴を

まとめて表示・確認する

USBの使用を禁止し、セキュリティを強化します

本日ご紹介する機能一覧

1 パッチ管理

管理対象に自動でパッチを当てる

2 インベントリ管理

社内のIT資産情報を棚卸しする

3 USB制御

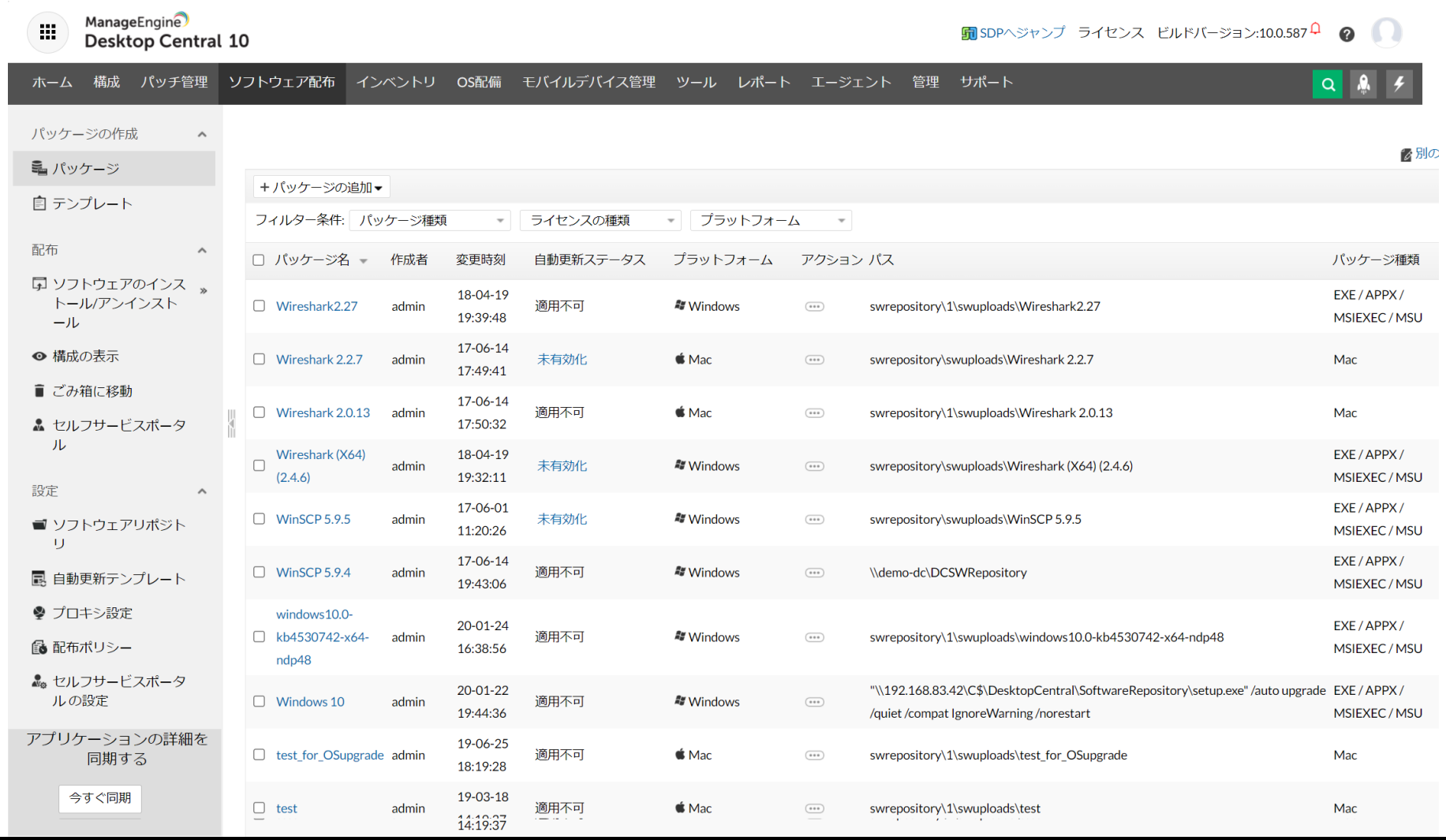
USBの使用を禁止する

4 その他おすすめ機能

テレワーク中に活用したい便利機能

Desktop Centralの画面を用いて、デモンストレーション形式で紹介します

4 テレワーク中に活用したい便利機能　ソフトウェア配布

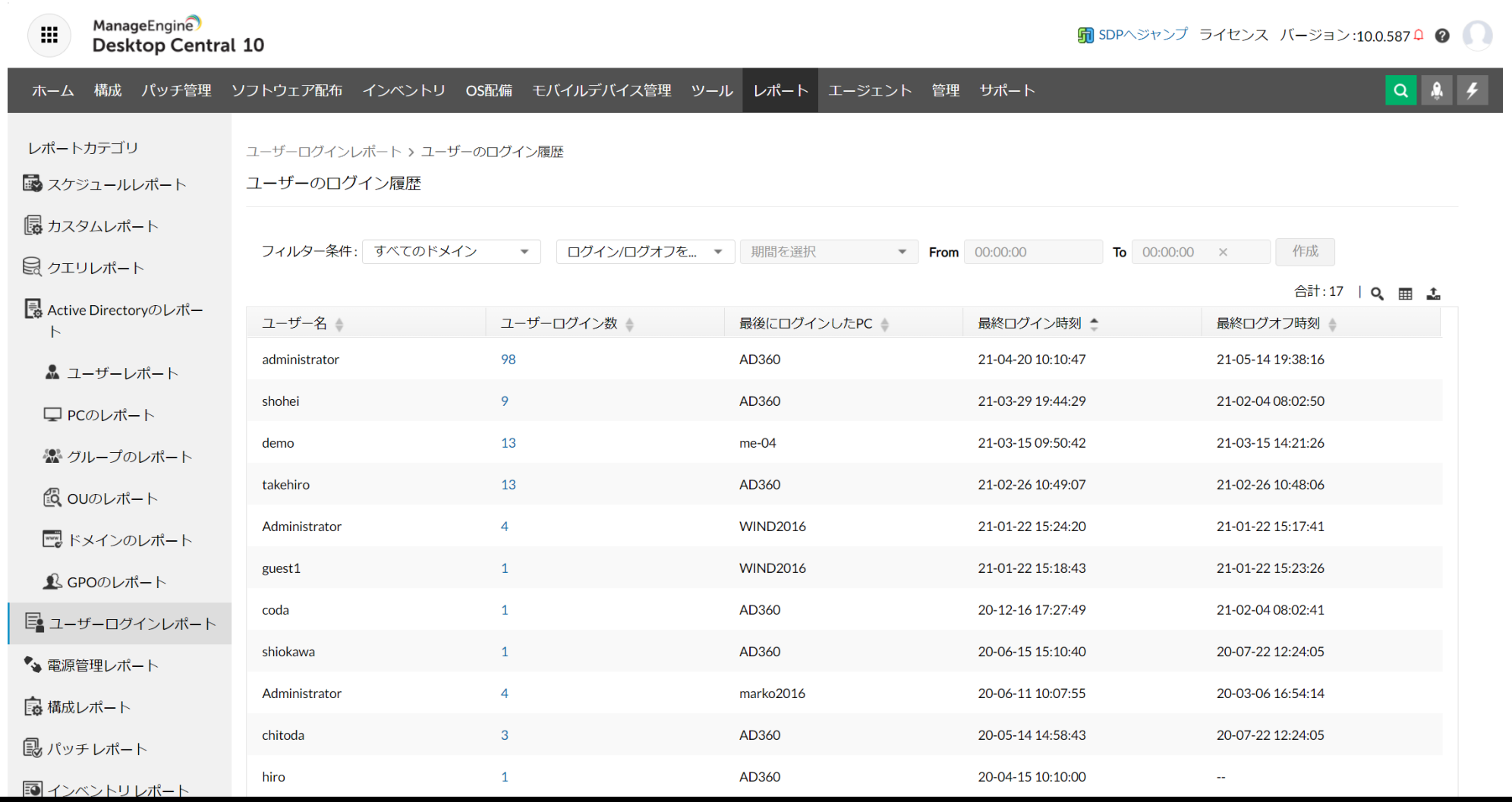


ソフトウェアのインストール、アンインストール、アップデートを一括で実施します

4 テレワーク中に活用したい便利機能　リモートコントロール

リモート端末にも、迅速にトラブルシューティング可能です

4 テレワーク中に活用したい便利機能　ユーザーログインレポート



ユーザー名	ユーザーログイン数	最後にログインしたPC	最終ログイン時刻	最終ログオフ時刻
administrator	98	AD360	21-04-20 10:10:47	21-05-14 19:38:16
shohei	9	AD360	21-03-29 19:44:29	21-02-04 08:02:50
demo	13	me-04	21-03-15 09:50:42	21-03-15 14:21:26
takehiro	13	AD360	21-02-26 10:49:07	21-02-26 10:48:06
Administrator	4	WIND2016	21-01-22 15:24:20	21-01-22 15:17:41
guest1	1	WIND2016	21-01-22 15:18:43	21-01-22 15:23:26
coda	1	AD360	20-12-16 17:27:49	21-02-04 08:02:41
shiokawa	1	AD360	20-06-15 15:10:40	20-07-22 12:24:05
Administrator	4	marko2016	20-06-11 10:07:55	20-03-06 16:54:14
chitoda	3	AD360	20-05-14 14:58:43	20-07-22 12:24:05
hiro	1	AD360	20-04-15 10:10:00	--

ユーザーのログイン、ログオフ履歴をまとめて確認できます

本日ご紹介する機能一覧

1 パッチ管理

管理対象に自動でパッチを当てる

2 インベントリ管理

社内のIT資産情報を棚卸しする

3 USB制御

USBの使用を禁止する

4 その他おすすめ機能

テレワーク中に活用したい便利機能

Desktop Centralの画面を用いて、デモンストレーション形式で紹介します

導入実績について

導入の決め手

- Windowsだけでなく、
  Mac、Linuxも管理可能なマルチOS対応
- 柔軟に設定可能なUSBデバイス制御機能
- Adobeなど各種アプリケーションのパッチ管理に対応
- 使いやすいユーザーインターフェース
- 必要十分な機能と、コストパフォーマンス

導入事例を見る： https://www.manageengine.jp/products/Desktop_Central/case-studies.html

詳しい導入事例は、Webページでご覧いただけます

アジェンダ

1. 企業のエンドポイントを守る！製品の概要紹介
2. テレワーク中のエンドポイント管理に役立つ 製品の機能紹介
3. 参考情報

ManageEngine

Desktop Central　ライセンスについて

クラウド版/オンプレミス版
年間ライセンス
Annual Subscription

19.8万円/年～

サポート付

- 1年間利用可能な製品ライセンスで、年間保守サポートサービスが含まれています。
- 1年ごとに一定額の年間ライセンス契約を更新します。
- クラウド版は年間ライセンスのみとなります。

オンプレミス版
通常ライセンス
Perpetual License + Annual Maintenance Support

44.1万円～

初年度サポート付

- 無期限の製品ライセンスに、初年度のみの年間保守サポートサービスが含まれています。
- 2年目以降は、1年ごとに年間保守サポートサービス契約を更新する必要があります。

価格表を見る：https://www.manageengine.jp/products/Desktop_Central/pricing.html

ご要件に応じて、お好きなライセンス体系を選択可能です

Patch Manager Plus　ライセンスについて

クラウド版/オンプレミス版

年間ライセンス

Annual Subscription

14.2万円/年～

サポート付

- 1年間利用可能な製品ライセンスで、年間保守サポートサービスが含まれています。
- 1年ごとに一定額の年間ライセンス契約を更新します。
- クラウド版は年間ライセンスのみとなります。

オンプレミス版

通常ライセンス

Perpetual License + Annual Maintenance Support

34.7万円～

初年度サポート付

- 無期限の製品ライセンスに、初年度のみの年間保守サポートサービスが含まれています。
- 2年目以降は、1年ごとに年間保守サポートサービス契約を更新する必要があります。

価格表を見る：https://www.manageengine.jp/products/Patch_Manager_Plus/pricing.html

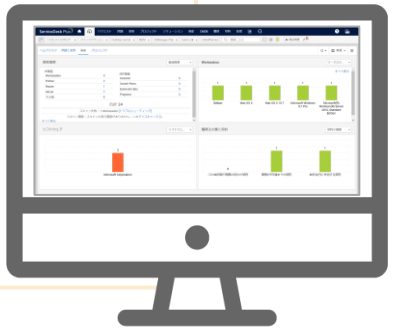
ご要件に応じて、お好きなライセンス体系を選択可能です

今すぐ使える評価版のご案内

無料ですべての機能が試用できます

https://www.manageengine.jp/products/Desktop_Central/download.html

- **クラウド版／オンプレミス版**どちらもご試用可能
- 評価版ご利用期間中に限り、**技術サポートを無料**で提供
- 試用開始後**30日**経過すると無料版に自動的に切り替わります



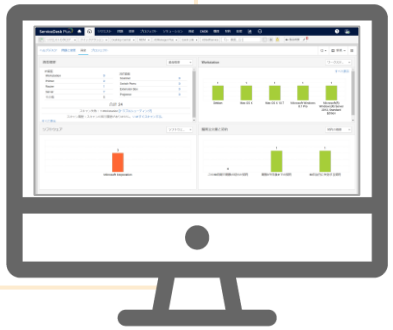
製品の機能・操作感をぜひお試しください

個別オンライン相談のご案内

貴社のご要件に沿った説明を受けられます

https://www.manageengine.jp/online_meeting/

- 製品担当者による相談会を**無料**で実施いたします
- パソコン画面を共有するため、**実際の画面や使用感**が分かります
- 気になる点やご不明点について、**その場で解消**いたします



申し込みフォームより、まずはお気軽にお申込みください

個別オンライン相談のご案内

オンライン相談に申し込む：https://www.manageengine.jp/online_meeting/

テレワーク中のIT資産管理・セキュリティ対策を強化し、
企業のエンドポイントを守り抜きましょう。

ご清聴ありがとうございました。

ManageEngine

製品の概要資料・評価版をダウンロードする

各製品の特徴を分かりやすく説明する概要資料をご用意しています。製品導入の検討・提案時にご活用ください。
また各製品の評価版は、すべての機能を30日間無料でご利用いただけます。製品の機能・操作感をぜひお試しください。

ManageEngine
Desktop Central

統合エンドポイント管理ツール

クリックして
概要資料を
ダウンロード

クリックして
評価版を
ダウンロード

ManageEngine
Patch Manager Plus

パッチ管理ツール

クリックして
概要資料を
ダウンロード

クリックして
評価版を
ダウンロード

テレワーク中のセキュリティ対策に、ManageEngine製品をぜひご活用ください