TOSHIBA

TSCMでオフィス内のPCやタブレットを統合管理。

「TSCM V2」および「TSCM for MDM」は、ソフトウェアライセンスによる販売となります。
TSCMのご使用には、ソフトウェアライセンスと年間保守のご購入が必要となります。
TSCMが内包している IBM® Endpoint Managerの機能により、
他社製品を含むマルチベンダー環境においても、オフィス内のPCやタブレットを統合管理することが可能です。

本カタログ記載の内容など詳細に関しましては、当社営業担当までお問い合わせください。

TOSHIBA
株式会社 東芝 デジタルプロダクツ & サービス社
国内営業統括部
〒105-8001 東京都港区芝浦1-1-1（東芝ビルディング）

安全に関するご注意
正しく安全にお使いいただくために、ご使用前に必ずソフトウェアに添付のオンラインマニュアルなどをよくお読みください。

このカタログの記載内容は2014年2月現在のものです。

管理番号 PC-973

東芝がお勧めする Windows 8.

TOSHIBA
Leading Innovation

2014.2

IBM® Endpoint Manager（IEM）連携 クライアント管理ソリューション
東芝スマートクライアントマネージャー（TSCM）

東芝自社開発BIOS技術の応用により、エンドポイントを統合管理し、クライアント環境で起こりうるリスクから、ビジネスを守ります。

TSCMは、東芝自社開発BIOSに搭載した「センサーマネージメント技術」と「セキュア通信技術」を応用したクライアント管理ソリューションです。IBM®のエンドポイント統合管理ソリューション IEMと組み合わせ、起動制御やセキュリティパッチ配布、インベントリ収集など、高度なクライアント運用管理をWindows® PCやAndroid™ タブレットで実現します。

Windows® PC 向け
TSCM V2

BIOSがセンシングしたデータを活用し、PCが自らの利用環境を監視できる機能を搭載。BIOSのセンシングとサーバー通信機能による「OSすら起動させずにPC本体の電源を遮断する機能」、BIOSが収集したHDDの状態を東芝独自のビッグデータ解析アルゴリズムを駆使して「HDDの故障予兆を検知する機能」、BIOSが実測する消費電力による「消費電力管理機能／省エネ効果の可視化」でクライアントの高度な運用管理を実現します。

Android™ タブレット向け
TSCM for MDM

「センサーマネージメント技術」で培ったノウハウを生かして独自に改良したAndroid™ を活用し、高度なセキュリティ管理機能を搭載。運用面やセキュリティ面の配慮から導入を懸念されがちだったAndroid™ タブレットに、システムレベルで「ストレージ利用制限」「インストール／アンインストール制限」「アプリケーション起動制御」といった機能で強固なセキュリティを実現します。

東芝自社開発BIOSによる「センサーマネージメント技術」と、「独自改良したAndroid™」で、さまざまなリスクからクライアントを守り、より高度な運用管理を可能にしました。

Windows® PC 向け TSCM V2

東芝独自のBIOS制御で、セキュリティ、HDD故障リスク、節電への最適な 対策を実現します。

●IBM® Endpoint Manager for Patch Management とIBM® Endpoint Manager for Power Managementの機能を含みます。

パッチ管理ソリューション

IBM® Endpoint Manager（IEM） for Patch Management

IBM® ではWindows OSやアプリケーション（Microsoft Office、Java、Flashなど）に対する最新パッチのいち早い適用を可能にしています。IEMのパッチ配布機能は、自律型エージェントにより対象PCを自動抽出し、OS環境なども自動識別して迅速かつ正確にパッチ配布を実行。これにより、従来よりも大幅にIT管理者の負荷を軽減でき、さらにパッチのアナウンスから適用までの脆弱な時間が短縮されることで、セキュリティリスクを軽減できます。

- PCの構成情報をリアルタイムに収集・管理。
  端末情報インベントリ収集
- 最新のセキュリティ情報をお客様のサーバーへ配信。
  セキュリティ情報監視
- パッチの配布スクリプトをお客様サーバーへ配信。
  配布スクリプト自動生成
- 自律型エージェントによる最新のPC状況を把握。
  配布対象PC自動抽出
- OSパッチに加え、広範囲なアプリケーションに対応。
  パッチ／アプリケーション配布

PC電源管理ソリューション

IBM® Endpoint Manager（IEM） for Power Management

リアルタイム追跡機能により、各エンドポイントがアイドル、アクティブ、スタンバイ、電源オフになった時間を正確に把握できるため、全PCクライアントの現在の電力使用量やコストなどを可視化できます。また、個別にポリシーの配布が行えるため、業務への影響を最小限に抑えながら省電力化できます。

dynabook と組み合わせることで、さらに高度な運用管理が可能に。

東芝自社開発BIOSによる「センサーマネージメント技術」は、リスクがあるとき、OSを起動すらさせません。

セキュリティ運用管理機能

TSCMでは、社内ネットワークに有線LANで接続されていないPCの起動はBIOS制御により“不正起動”とみなし、OS起動もさせることなくPC本体の電源を遮断できます。これは、東芝 自社開発BIOSによる「センサーマネージメント技術」と「OSに依存しないセキュアな通信技術」によって実現した、他社にはない独自機能です。紛失・盗難時には強制的に起動禁止にすることで、データ漏えいのリスクからPCを守ります。また、指定回数以上の不正アクセスが続いた場合、HDDデータの遠隔消去ができます。さらにモバイル環境では、有線LANの代わりにUSBトークンを用いた起動制御による運用も可能です。

●不正起動遮断までのプロセス　TSCMはセキュリティリスクを最小化

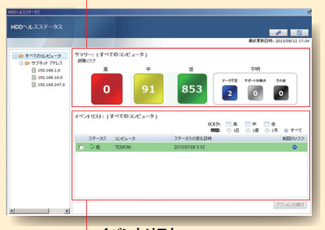
S.M.A.R.T.データを定期的に収集・蓄積。さらに、過去のHDD稼働データを独自アルゴリズムでビッグデータ解析することで、故障リスクを自動検知。迅速な予防措置を可能にします。

HDD故障予兆検知機能（HDDヘルスステータス）

HDDには自己診断機能S.M.A.R.T.が搭載されています。一般的な故障予測アプリケーションではS.M.A.R.T.をもとに、エラー発生の頻発といった不具合が発生してからアラートを発するため、データ退避などの予防措置が間に合わない可能性があります。TSCMでは、管理下にあるHDDのリードエラー発生率、ディスクヘッドに衝撃が与えられた回数、代替処理されたセクタ数などのS.M.A.R.T.データを定期的に収集・蓄積し、東芝独自の故障予兆アルゴリズムで解析を加え、故障リスクのあるPCをいち早く自動検知してIT管理者に通知します。これにより、高い精度でHDD故障を予兆し、ユーザーにバックアップを促すなど迅速な予防措置が可能になります。東芝独自のアルゴリズムは、東芝が世界に出荷したPCのHDDや、東芝の修理センターに持ち込まれたHDD修理データなどのビックデータを解析し、故障予兆の精度を高めています。

※PCに内蔵されたHDDのみが対象です。また、SSDやハイブリッドHDD、外付けのHDDは対象外です。

故障リスクアイコン
HDDのリスク状態別に台数が表示された管理画面を確認し、リスクの高いPCユーザーにバックアップ実行を指示。



イベントリスト
ステータスが変わったPCリスト、故障リスク別に該当するPCリストを表示。

省エネ効果の可視化により、PCごとの消費電力をより正確に把握・制限できます。

消費電力管理機能（節電管理）

TSCMでは、東芝 自社開発BIOSによる「センサーマネージメント技術」でPCの消費電力をリアルタイム監視。PC単体やユーザーグループごとの実使用電力を時系列でグラフ化して表示できます。IT管理者は、消費電力管理の設定前後を比較することで、手間をかけずに削減量を可視化。従来、判定しにくかった削減効果も金額ベースで管理することが可能になります。また、グループごとの消費電力設定ポリシーの配信・実行、ユーザーによる設定変更の禁止も可能なので、省エネ対策を徹底させることができます。

対象製品

対象OS: Windows® 7
Windows 8
Windows 8.1には、2014年4月対応予定。

サーバー側OS: Windows Server 2008 R2
Windows Server 2012
（セキュリティ運用管理機能は、Windows Server 2008 R2をご使用ください。）

Android™ タブレット向け TSCM for MDM

東芝独自のAndroid™ 改良により、強固なセキュリティ監視機能をタブレットに組み込んでいます。

●IBM® Endpoint Manager for Mobile Devicesの機能を含みます。

モバイルデバイス管理ソリューション

IBM® Endpoint Manager（IEM） for Mobile Devices

スマートフォンやタブレットの急速な普及にともない、PCクライアントに加えてモバイル端末の運用管理が重要な課題に。IEM for Mobile Devicesは、端末側のエージェントとサーバー上の管理コンソールで、すべてのモバイル端末のインベントリ情報を自動的に収集し一元的に管理。これによりAndroid™ タブレットのクライアント管理ツールとして「インベントリ管理」「セキュリティ管理」「ポリシー管理」「アプリケーション配布」が行えるため、IT管理者の負荷軽減に役立ちます。

- モバイル端末の情報をまとめて収集・管理。
  端末情報インベントリ収集
- モバイル端末の位置をリアルタイムに把握。
  位置情報（GPS）取得
- モバイル端末へのインストール内容をひとめで把握。
  アプリケーション一覧
- モバイル端末のパスワード改ざん・なりすましを防止。
  パスワードルール設定
- サーバーからモバイル端末にアプリケーションやパッチのインストール。
  パッチ／アプリケーション配布
- 遠隔操作で画面をロックして不正操作を防止。
  端末画面ロック
- 遠隔操作でデータを消去して情報漏えいを防止。
  端末データ消去
- 不正にルート権限を取得したモバイル端末を検知。
  ルート化端末検出
- モバイル端末のカメラからの情報漏えいを防止。
  カメラ禁止

REGZA Tabletと組み合わせることで、さらに高度な情報漏えい対策が可能に。

TSCM for MDM　5つの機能

外部メモリの使用禁止で、書き出し・読み込みによる情報漏えいを防げます。

ストレージ利用制限

USBやBluetooth® など拡張インターフェースの利用をシステムレベルで制御。USBメモリやSDメモリカードなどの外部ストレージを接続してもデータの書き出し・読み込みが自由に行えないように制限したり、USBやBluetooth® で接続するキーボードやマウスも使用禁止にすることができます。これにより個人情報の漏えいなどのセキュリティリスクを回避できます。

安全なアプリケーションのみ受けつけ、スパイウェアやウイルスの侵入を許しません。

インストール制限

IT管理者がアプリケーション単位でインストールの許可／拒否を指定可能。許可されたアプリケーション以外はインストールできないため、不正なアプリケーションに埋め込まれたスパイウェアやウイルス侵入のリスクを回避できます。

許可したアプリケーションのみ起動し、セキュリティの抜け穴をつくらせません。

アプリケーション起動制御

インストールと起動を許可したアプリケーション以外は起動できないようにシステムレベルで制御されているため、不正なアプリケーションの起動による情報漏えいのリスクを回避できます。

安全なアクセスポイントへの接続で、ネットワーク経由での情報漏えいリスクを回避できます。

ネットワーク利用制限

IT管理者によって許可された接続可能なネットワークをシステムレベルで自動判別し、それ以外のネットワークへの接続を制限。不正なWi-Fiアクセスポイントを介した情報漏えいのリスクを回避できます。

削除してはいけないアプリケーションが誤って削除されるのを防止できます。

アンインストール制限

IT管理者がアプリケーション単位でアンインストールの許可／拒否を指定可能。正規にインストールされている業務アプリケーションや、ウイルス対策アプリケーションなどの削除を制限できるため、業務への支障やウイルス感染による情報漏えいリスクが生じるのを防止できます。

対象製品

対象：Android™ 4.1 以上

サーバー側OS: Windows Server 2008 R2
Windows Server 2012