IBM Security
Thought Leadership White Paper

Enterprise Mobility Management

ビッグバン理論 - モバイル機器管理が膨張して、デバイス、アプリ、コンテンツをのみ込むまで

IBM

はじめに

スマートフォン、タブレット、その他のポータブル機器のパワーが解き放たれたことで、「オフィス内」、「出先」、または「家庭」での仕事の境界が曖昧になっています。従業員は、自分が選んだデバイスで柔軟に仕事をすることを期待しているし、経営者は常時オンの可用性を期待するようになりました。このビジネス要件はほとんどの場合、企業ネットワークとデータを保護する人員たちと不協和音を生じさせます。企業によっては、無慈悲にも「ノー」という答えが返ってくる結果となります。しかし今日では、そのような反応はめったに見られなくなりました。今では、「状況によります」という答えが標準です。また、企業内には各種部門からなる小宇宙が存在することを忘れてはなりません。この小宇宙により、機密データの保護方法との均衡を取りながら、必要なアクセスをどのように決めたらいいのか、再び大きな議論が巻き起こります。

モビリティを最大化するため、今日では微妙なさじ加減の戦略が一般的です。モビリティの変革力を実現するには、IT はビジネス推進要因を理解した上で、皆の目標をサポートする技術ロードマップを考案するビジネス・パートナーになる必要があります。

モビリティの世界は複雑な世界であり、常に広がり続けています - まるで本物の宇宙のようです。常に広がり続ける私たちの宇宙とモビリティのもう 1 つの類似点は、合理的、分析的な幅広い理解を通じて実現できる可能性を秘めている点です。

モビリティの爆発的な広がり: ビッグバンによって拡大中

最初は真っ暗闇でした。特に、出先や自宅で仕事を終える必要のある人たちにはそうでした。従業員は、データや生産性プログラムを融通の利かないデスクトップに残したまま退社したものです。ノートパソコンはオフィス外での作業を可能にしましたが、接続にコストがかかり不安定でした。また、ノートパソコンの電源を切った瞬間に、情報が何もないブラックホールが広がるばかりでした。

BlackBerry が登場すると、企業の指導層はオフィスにつながることができるようになりました。明かりがさしましたが、光り輝く灯台というよりは、暗い夜空の遠い星のようなものでした。

それから、白熱したイノベーションが燃え上がり、最初のスマートフォンが登場しました。

光はデバイスと同様に、実質的にあらゆる場所の人々に広がりました。幹部には BlackBerry がありましたが、突然、iOS と Android オペレーティング・システムを搭載した新しいタッチベースのデバイスが人々のポケットと職場に入り込み始めました。

それから、またしても爆発が起こり、タブレットの登場です。画面が大きかったので仕事も遊びも多くこなせるようになりました。その大型サイズとインテリジェンスの強化により、ついに出先でデータの取得と操作を行うことが現実になったのです。従業員は啓蒙されましたが、IT は納得できずに、どことなく影を背負ったままでした。どのデバイスを企業リソースにつなぐべきか?つながないデバイスはどれにする?どれが安全なのか?

モビリティのビッグバン管理

モビリティのビッグバンはどのように管理できるのでしょうか?

デバイスの管理

可視化を実現し、いくつかのコントロールを適用できる IT のビッグバン・ポイント・ソリューションの核、モバイル機器管理 (MDM) の幕開けです。この宇宙の広がりの中で、MDM はパスコードの実行、電子メールや Wi-Fi ネットワークなどの企業リソースへの接続、デバイスの監視を行う機能を IT にもたらしました。

オペレーティング・システムに組み込まれた API により、IT は設定を構成し、機能を有効または無効にすることができるようになりました。また、デバイスをリモートで発見、ロックし、必要に応じてデータを部分的または完全にワイプすることも可能になりました。

外部サービス・プロバイダーが管理されるデバイス数は、2015 年には 50 パーセント以上成長する見込み[1]

IT はこれを良しとし、皆も大筋で同意しました。しかし、ユーザーとアプリがより先進的になり、スプレッドシートや Word 文書などのドキュメントがモバイル機器で操作可能になると、多くの企業が MDM 以上のものが必要なことに気付きました。

この願いに応えるために、また爆発が起こりました。それは、アプリとコンテンツ管理用のソリューションの出現、コンテナーという形の仕事と個人の分離でした。

アプリの管理

モバイル・アプリケーション管理 (MAM) は名前が示すように、配布、更新、エンタープライズ・アプリ・カタログ、ブラックリスト/ホワイトリスト、およびセキュリティーなど、ライフサイクル面に焦点を置いており、パブリック・アプリとカスタム・アプリの広がり続ける宇宙を管理するために必要とされていました。

しかし、アプリケーションは万能ではありません。企業によって開発または所有されていないアプリもあるため、これらを制御する能力は常に限られたものになります。MAM に理想的なアプリケーションは、1 つのアプリの専用デバイスを管理するもので、これは「キオスク・モード」と呼ばれることもありました。小売店とホテルでこのモードを利用した結果、チェックイン・プロセス、在庫検索、食材と飲み物の注文を効率よく処理することができました。

コンテンツの管理

宇宙は再び爆発しました。まばゆい光の中で、モバイル・コンテンツ管理 (MCM) が人々に提供されました。その結果、ファイルとドキュメントをチームのしかるべきメンバーと選択的に共有することが可能になりました。一部のドキュメントを閲覧し、転送する権限を持つ人もいますが、そうでない人もいます。一部の人はドキュメントを編集し、変更を保存した後、全員が閲覧できるようにファイル共有に戻し、変更を複数のデバイスと同期することができます。MCM はこの種の機能とコントロールをエンタープライズ・モビリティにもたらしました。将来は希望と約束にも満ちています。パブリック・ファイル共有サービスにありがちなゴツゴツしたセキュリティー小惑星との衝突を心配することなく、モバイル機器上で共有ドキュメントを個人で、そして同時共同作業でセキュアに編集することが可能になるかもしれません。

「でも、私たちは同僚に家族とペットの写真を見せたいし、朝、仕事をする前に業務メールをチェックしたいんです!」と人々は言いました。「1 台のデバイスで両方できませんか?」

非常に短期間で起こったこれらの爆発により、企業にはモビリティ管理のための目眩のするような数々の選択肢が残されてしまったため、IT は、利用可能になったエンドポイント管理オプションを理解しようなどと試みたくないので、ほとんど自主的に再び暗闇の中に入ってしまいました。

IT マネージャーの 66 パーセントが抱いている最大のセキュリティー問題は、企業ネットワークへの個人デバイスの接続に端を発しています[2]

仕事と人生の境界

また閃光が走りました - 多くの人はすでにこの大きな光への準備ができていて、サングラスを買っていました。空からはコンテナーが落ちてきて、MAM と MCM により強い焦点を当て、デュアル・ペルソナ・エクスペリエンスを作りました。

コンテナーは、コンテキストと ID をベースに、社内の誰なのか、どこに所属しているのか、何を担当しているのかなど、アプリとコンテンツの両方をよりきめ細かく管理するアプローチを提供します。また、エンタープライズ・アプリを個人アプリからシールドし、業務のメールまたはドキュメントをサンドボックス化することで、個人データと企業データを分離します。

コンテナーは従業員のプライバシーを保護し、ネットワーク・アクセスやセキュアな会社認可の Web ブラウジングなど、業務で使うコントロールを個別に提供します。これらのコンテナーは、デバイスの「片側」からもう一方の側へのコピーを防止できます。会社所有コンテナーの場合、不正なアクティビティが発生したときには、デバイスのもう一方の「側」に影響を及ぼすことなく、ワイプまたはロックが可能です。典型的な使用事例は、規制の厳しい業界の従業員に企業の機密情報が託される場合です。

エンタープライズ・モビリティ管理:
今日のモバイルの宇宙のため、そして次に起こること

IT は大喜びです。これで、ユーザーは会社のシステムを侵害することなく、商用アプリ・ストアからアプリをダウンロードできるようになりました。コンテナーによって柔軟性も広がりました。コンテナーの「作業側」は、デバイス上の残りのデータやアプリに影響することなく、簡単に削除できます。

多くの企業は複数のソフトウェア・プラットフォームを使用し、デスクトップ・コンピューターとローカル・ネットワーク上で様々な種類のドキュメントを絶えず交換しています。「これと同じことがモバイル機器上でできないものでしょうか?」と人々は尋ねました。

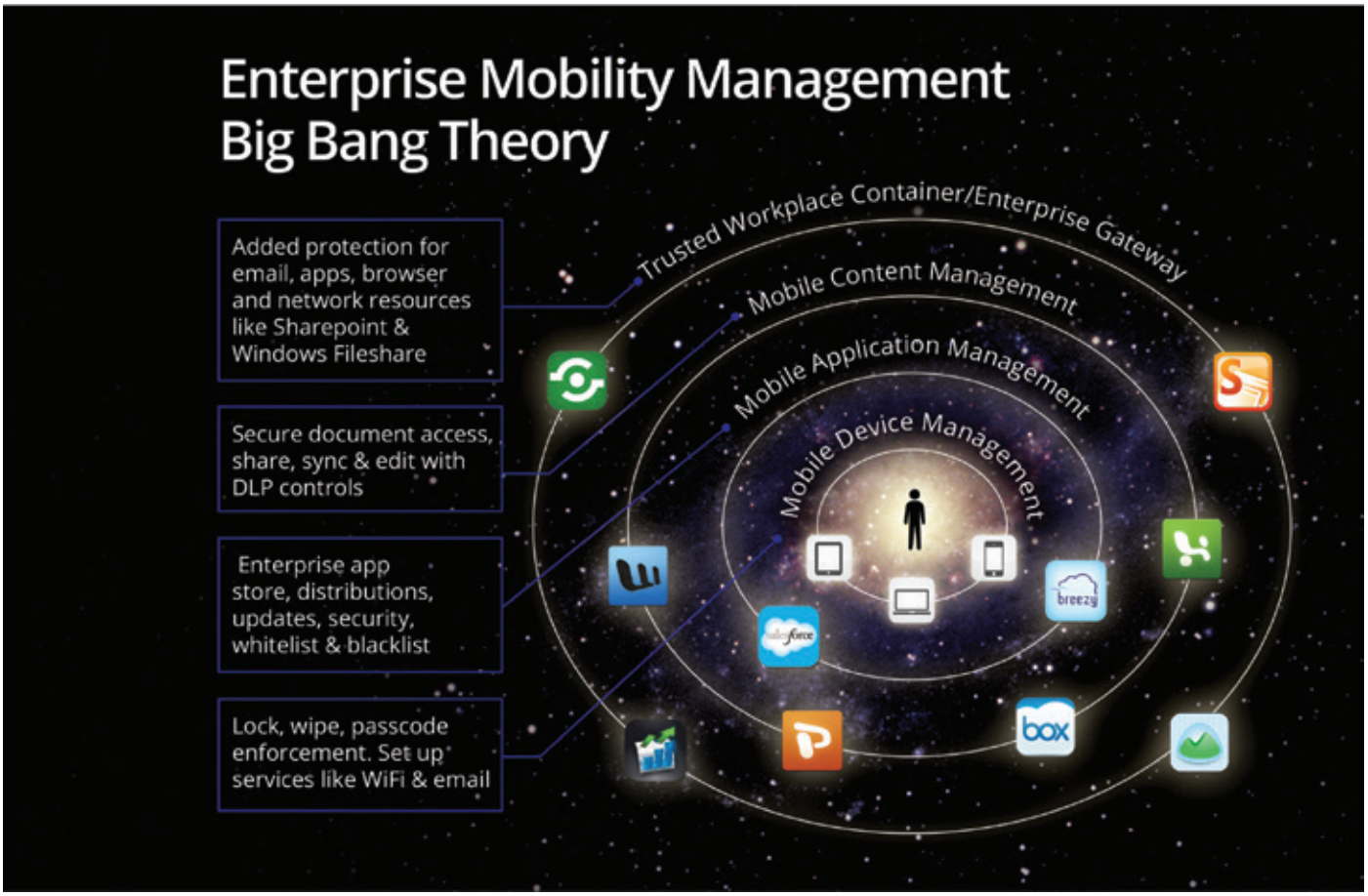

*図 1:*エンタープライズ・モビリティ管理のビッグバン理論

28 パーセントの CIO が、会社にはモバイル・テクノロジー戦略がないと回答しました[3]

企業は再び大変動を経験していますが、今回は、外の世界の爆発というより内部爆発という感じです。モバイル・ビジネスの問題点を解決したポイント・ソリューションの多くは、エンタープライズ・モビリティ管理 (EMM) の元に統合されており、そのおかげで IT は、モバイル宇宙における全データとセキュリティーの課題を容易に把握することができます。今日の画期的な時代は、暗黒時代からルネッサンス期を迎えたかのようであり、大小の企業に多くの選択肢を約束します。そのため、企業は真のビジネス要件を満たす構成要素を極めて柔軟に選ぶことができます。

IT は EMM により、モバイル宇宙における全データとセキュリティーの課題を容易に把握することができます。

では、啓蒙の状態に入るにはどうしたらいいのでしょうか?企業が真の可能性を発揮して、モバイル戦略からビジネス価値をもぎ取ることができないのは、これらのソリューション、ソリューション間の統合について考えが整理できていないことが原因かもしれません。ベンダーの数が多すぎることがその一因ですが、IT の目が届かないところで活動する事業部門や従業員という不確定要素が原因でもあります。その場合、企業にとっての課題は、ビジネスにぴったり合い、ユーザーが簡単に採用、使用できるモバイル管理への体制を整えて、それを効果的に実施することになります。

組織の 51 パーセントには、明確に定義したイニシアチブとともに全社的なモバイル戦略がありますが、49 パーセントの組織にはそのような戦略はありません[4]

企業が真の可能性を発揮して、モバイル戦略からビジネス価値をもぎ取ることができないのはなぜでしょうか? それは、これらのソリューション、ソリューション間の統合について考えが整理できていないからかもしれません。

最後のフロンティア

宇宙は選択肢と豊富の時代に入りましたが、カオスの時代でもあります。今日、人々のモバイル・ソリューションへの要求は、これらの要求を満たし、保護する IT の能力を大きく超えることがあります。従業員は出先でモバイル機器からビジネス情報にアクセスすることを望んでいます。

事業部門は、アクセスを管理下で許可することで得られる価値をますます強く認識しています。柔軟性がどれほど生産性を高め、企業システムに出先からアクセスできないことで生じる遅延を防ぎ、貴重な企業情報を危険にさらすセキュリティー・ホールを塞げるかを見ているからです。そのため、会社所有の個人対応デバイスと BYOD (個人所有機器の持ち込み可) 戦略が急速に根を下ろしつつあります。

アプリを従業員にプッシュする企業の38パーセントが、カスタマイズしたアプリを使っています

通常、ほとんどの人は、異なる使用プロトコル、データ・プラン、決済スキーム、電話番号の入った2台のデバイスを持ち歩きたいとは思いません。一部の企業では、個人デバイスから企業システムへのアクセスをあまねく許可していますが、完全にブロックしている企業もあります。アプリとデバイスのライフサイクル (導入、更新、セキュリティー保護、処分) をどのように管理するかについてまったく考えもせずに、アプリの開発と配布を許可している企業もあります。このようなアプローチは危険な不備があります。

企業データをしっかり保護するには、より大規模で包括的な管理システム、および関連する戦略の両方が必要です。

広がり続ける宇宙を簡単に管理

EMMがなければ、ITは広がり続けるモバイル宇宙を課題として捉え、多くのITが、使用中のアプリの数、アプリの使用者を正確に把握しなければならず、大変な思いをしていたことでしょう。アプリの開発サイクルは速く、あっという間に普及させることができます。少なくとも、iOS、Windows、Androidの3つのOS、それから数十社ものメーカーのモバイル機器に広まります。

さらに悪いことに、クラウドベースのサービスによって、アプリのダウンロード、新しいアプリの開発、ファイルの転送などが容易になり、場合によっては、企業ネットワークから完全に離れたところでこれらが行われることがあります。

アプリ開発もまた、分散したために急増しています。たとえば、マーケティング部門は新しいアプリを2、3週間で開発して、会議の場でスタッフに、購入したタブレットに展開し、そしてアプリはバックエンド・システムにつながります。これがITの管理外で、またはITの知らないうちに起こったとしたら、セキュリティーと管理のリスクが発生します。また、このような状況は1日に何度も起こっています。

ハッブル望遠鏡のように、適切なEMMソリューションは、企業のデータ領域に入り込むすべてのデバイスを非常にわかりやすく可視化することができます。

ITマネージャーは、モバイルが戦略的に役立ち、モバイルの使用が不可避であることを知っており、会社の競争力を維持できるようにしたいと望んでいます。その一方で、ITは、標準化されていないプラットフォームとデバイスの多様性に対応し、企業データを保護する任務を負わなければなりません。

そこで次のような問いが浮かびます。

- ITがセキュリティーと生産性のバランスを図るにはどうすればよいのか?
- 企業のITのモバイル課題は、これら複数のベンダーとどう絡み合うのか?
- モバイル採用を増やしている企業が競争力とセキュリティーを強化するにはどうすればよいのか?
- エンタープライズ・モビリティへのITのアプローチを「ITによってデバイスをロックダウンして悪いことが起こらないようにする」から「ITによって、以前は不可能だったことを可能にし、良いことが起こるようにする」に変える方法は?
- 宇宙の均衡を再び取り戻すと同時に、光に浴するには?

エンタープライズ・モビリティ管理:ようやく宇宙が理解可能な状態に

EMM は、複数の用途でモバイル・ユーザー・コンピューティングを実現する上で必要な、幅広い領域のアクティビティとポリシーをカバーするソリューション・スイートです。EMM は包括的な手法であり、複数の OS 環境の管理を標準化し、既存の企業システムと統合できます。また、アプリからコンテンツに大量のデータをセキュアに拡張できます。

EMM はモバイル管理のあらゆる面を網羅することで、広がり続けるモバイル宇宙を IT で活用できるようにします。デバイス中心モデルから、社内外のアプリケーション、データ、コンテンツなどをデバイスに依存しない環境に組み込むアプリ/データ中心モデルへと話を広げます。MDM、MAM、MCM のすべての利点、およびコンテナー化をより柔軟な構造に組み込みます。また、EMM はモビリティに対して ROI を実現することで、エグゼクティブ・サマリーと詳細分析を提供して、モバイル接続の真の価値を確認できるように支援します。

EMM により、デバイス依存から脱却

EMM を使用すると、企業はいくつものデバイスと OS の中から 1 つだけを選んでサポートする必要がなくなり、大きなかぢあの一部しか解決しないポイント・ソリューションから遠ざかることができます。社内開発したアプリケーションと他社製アプリケーションの両方を組み込んで、データに埋め込まれた独自に知的財産に集中することができます。異種混在システム管理へのこの同種アプローチは、IT が初めて MS 認定試験を受けてから強く求めてきた監視の万能薬です。

回答者の 40 パーセントが、従業員による BYOD へのトップ・プライオリティとして「デバイスの選択肢」を挙げています[7]

EMM は、グローバルなビジネス環境に対応するソリューション

ビジネスがますますグローバルな命題になりつつあることは、疑いの余地がありません。企業はかつて競争にしのぎを削っていたものですが、今ではサプライチェーン全体がグローバルに協働、競争しなければなりません。つまり、従業員とパートナーは定期的に出張、取引を行い、複数の管轄と文化にまたがる企業資産を扱っています。

EMM は、どこにいても規制コンプライアンスに遵守できるように支援します。従業員は、元のモバイル機器、ノートパソコンなどデバイスに関係なく、出先から安全に企業データにアクセスできます。社内外での協働、ファイル交換、データ同期がはるかに容易になります。ネットワークへのアクセス方法が何であっても、適切なセキュリティーを適用できます。

人気の高いコンシューマー向けアプリケーションは、役に立つから人気があります。しかし、ERP や CRM など、システム・オブ・レコードとやり取りするようになっているとは限りません。EMM ソリューションは、データ中心アプローチを採用し、モバイル ROI という新しい可能性を生みだすことで、このようなギャップの橋渡し役になります。

EMM:垂直型 ROI の推進

多数のデバイスとアプリケーションが広がりつつありますが、企業の数と潜在的なモバイルの利用方法に比べればどうということはありません。EMM はそれぞれの企業、部門、従業員、パートナーのニーズに合わせてカスタマイズすることができます。いくつかの使用事例について考えてみましょう。

大手製造メーカーは、外部代理店と請負業者のネットワークを使って製品を売っていました。このサードパーティの営業部員に対し、アプリケーションを使って販売の効果を上げてほしいと考えていましたが、そのデバイスも管理することは現実的ではありませんでした。目標はただ、営業部員の個人デバイスにアプリを提供して、アプリ内のデータを保護することでした。EMM は必要とされる (MDM ではなく MAM) モビリティ管理の側面を整理できるように支援し、管理を容易にしながら、個人デバイスを所有する他社営業部員に煩わしい思いをさせません。

ある大手エンターテインメント企業は、食べ物と飲み物を出すまでの時間を平均 20 分から 4 分に短縮することで、顧客体験を強化することができました。タブレットでセキュアに管理される専用モバイル・アプリをスタッフに使わせることで、注文を迅速に処理しています。また、注文数の増加によって売上が伸びています。

モビリティの ROI 評価

ある消防署では、管轄区内の建物の間取図が入っていて、建物に取り付けた Web カメラからのライブ・フィードを得られる iPad で消防隊をパワーアップさせました。消防署を出て現場に着くまでの数分の間に、緊急要員が火災の広がり具合を調べて、建物のレイアウトをより的確に把握します。現場に到着する前に現場の様子をよく把握できたため、10 分速く消火できたということは、人命救助の成功という何よりも素晴らしい ROI になります。

EMM の過小評価されている側面に、モバイルに対する特定の投資の ROI 評価に使用できる分析機能が挙げられます。たとえば、保険会社はこれまでの間ずっと、大量の書類が作成されてきました。ある米国の大手保険会社は、モバイル機器から電子メールにアクセスすることを従業員に許可し、電子メールが送信された時間、送信元デバイスを追跡できるようにしました。すると、モバイル機器の使用率は退社後に大幅に上昇することに気付きました。また、それに呼応して紙の使用率も下がりました。なぜなら、従業員は毎晩、印刷した書類を家に持ち帰る必要がなくなったからです。その結果、モバイル・イニシアチブの ROI が明確に上がりました。

他の企業は、EMM を使って特定のアプリケーションやコンテンツのパフォーマンスと使用状況を分析しています。その結果、IT と事業部門マネージャーは、その投資を続けることが適切かどうかを判断する上ではるかに優れた知見を得ることができます。

まとめ

ほぼすべての企業が、2 年前ですら聞いたことがなかったレベルでモバイル機器に対処しなければなりません。様々なデバイス、OS、アプリケーション、潜在的な利用方法の選択肢は無限に広がり、めまいがするほどです。

デバイス、コンテンツ/アプリ管理機能、コンテナーのスタック全体が必要か、その一部のみが必要かを問わず、何らかの企業向けモバイル戦略が必要です。EMM を導入した企業は、今日の環境の課題の多くに打ち勝ち、従業員からのアクセス要求、企業データの保護に対処できており、モバイル戦略による生産性と ROI の新たな可能性で経営陣を喜ばせています。もちろん、他のツールと同様に、EMM は自律的に機能する「魔法の薬」ではありません。経営陣はモバイル採用ライフサイクル全体を考えて、モバイルが会社独自の運用条件にもたらす課題と機会を的確に理解した上で、EMM を導く必要があります。

モバイル宇宙が新たに「膨張」するたびに、自動的に対応するよりももっと多くの働きをする統合モバイル・ポリシーを組織で確立することをお勧めします。IT は、各種グループに様々な権限とコントロールを設定し、これらのコントロールを共通のシステムから管理する上で重要な役割を果たします。

モバイル宇宙は今後もさらにパワフルになりますが、ようやく理解と管理の及ぶ、理にかなった状態に落ち着くかもしれません。豊富な情報に裏打ちされたこの合理性をモビリティに適用すれば、光に背をそむけずに、モビリティの力を良いことに利用できるのだと自信を持って、ロケットのようにまっすぐ前進することができるでしょう。

本資料は CITO Research によって作成され、Fiberlink によって後援されました。

CITO Research

CITO Research は、CIO、CTO、他の IT とビジネスのプロフェッショナルによって利用されているニュース、分析、調査、知識の源です。CITO Research は、読者と対話しながらテクノロジーの動向を捉えて、それを高度な方法で収穫、分析、伝達し、実践者が難しいビジネス課題を解決できるように支援します。

次のサイトをご覧ください: http://www.citoresearch.com

IBM MaaS360 について

IBM MaaS360 は、業務のあり方に合わせて生産性とデータ保護を実現するエンタープライズ・モビリティ管理プラットフォームです。モバイル・イニシアチブの基盤として多数の組織から信頼されています。MaaS360 は包括的な管理機能を提供し、ユーザー、デバイス、アプリ、コンテンツへのセキュリティーを強力に制御することで、どのようなモバイル導入もサポートします。IBM MaaS360 の詳細と 30 日間の無料トライアルのご利用については、次の Web サイトをご覧ください。
www.ibm.com/maas360

IBM Security について

IBM のセキュリティー・プラットフォームはセキュリティー・インテリジェンスを提供して、組織が人々、データ、アプリケーション、インフラストラクチャーを包括的に保護できるように支援します。IBM は、ID およびアクセス管理、セキュリティー情報およびイベントの管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、次世代侵入保護などのためのソリューションを提供しています。IBM は、世界で最も幅広くセキュリティー研究開発を行い、セキュリティーを提供している組織の一つです。詳細は、以下をご覧ください。
www.ibm.com/security

注記

注記

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in Japan
March 2016

1 Gartner; http://blogs.gartner.com/eric_goodness/2014/07/30/magic-quadrant-for-managed-mobility-services/

2 Ponemon Institute® Research Report; *2014 年「State of Endpoint Risk」*、Lumension®による後援、第三者機関 Ponemon Institute LLD により実施、発行日:2013 年 12 月、https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of -the-endpoint/2014-State-of-the-Endpoint-Whitepaper- Lumension.pdf

3 Donavan, Fred;「*Wanted: Mobile tech strategy*」、Robert Half Technology による調査、FierceMobileIT、2014 年 3 月 26 日、http://www.fiercemobileit.com/story/wanted-mobile-tech-strategy/2014-03-26

4 Bernhart Walker, Molly、「*Only half of enterprises have a mobile strategy, security the biggest challenge, says report*」、Cisco/Illuminas Survey による委託調査、FierceMobileIT、2014 年 4 月 1 日、http://www.fiercemobileit.com/story/only-half-enterprises-have-mobile-strategy-security-biggest-challenge-says/2014-04-01

5 Fiberlink の「*MaaS360 Mobile Metrics*」2014 年 5 月 (現在、非掲載) から取得したデータ・ポイント

6 Cisco Study:「*IT Saying Yes to BYOD*」プレス・リリース、the network、Cisco's Technology News Site、2012 年 5 月 16 日、http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYODwww.maas360.com/maasters/blog security-information/is-your-device-security-policy-leaving-your-company-vulnerable

WGW03109-JPJA-01