企業におけるスマートフォンのセキュリティ管理

マカフィー株式会社
プロダクトマーケティング部
スペシャリスト　松久 育紀

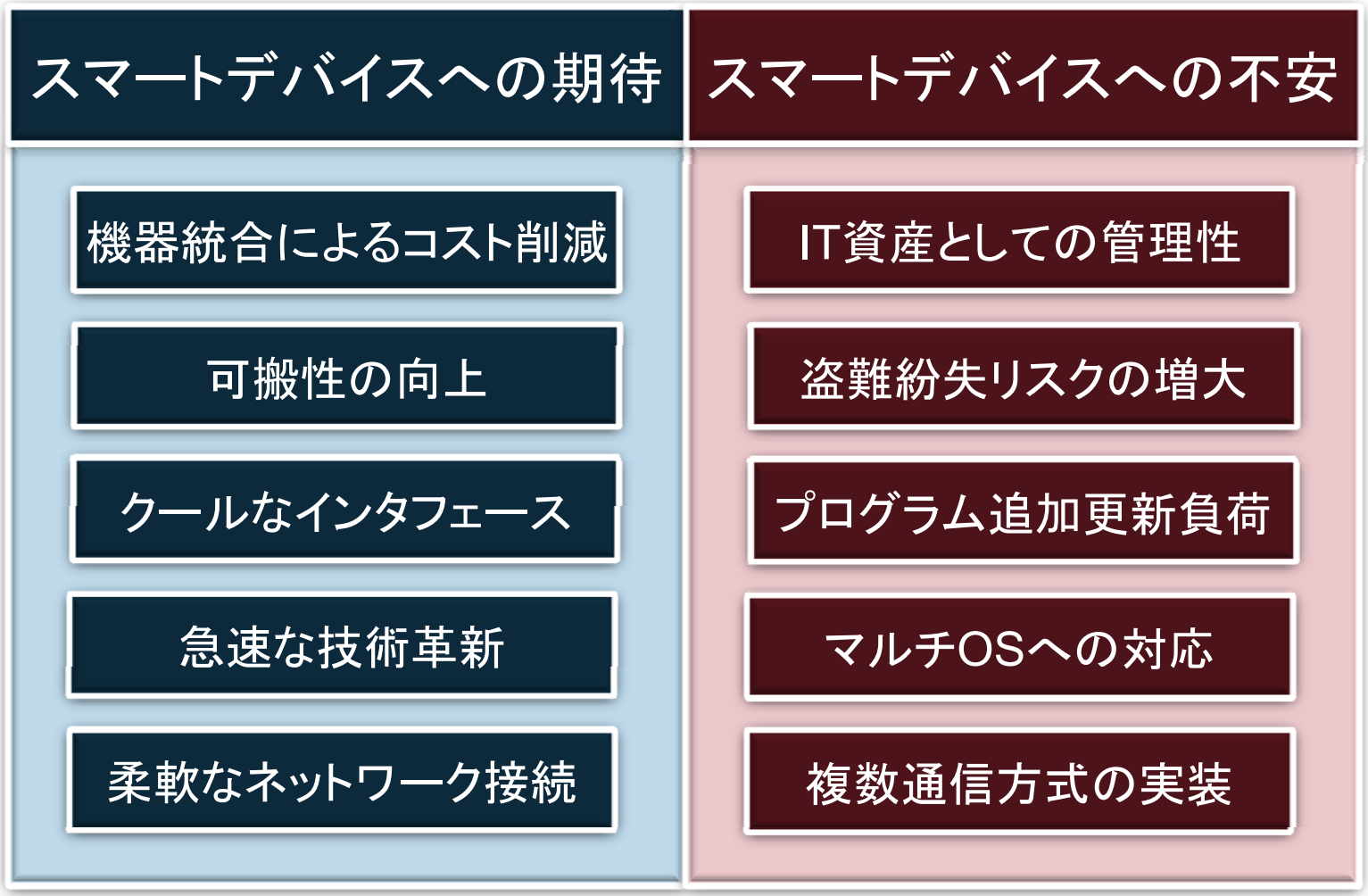
Securing Your Digital World™

What's New in Mobile?

- 2010年Q3携帯電話機出荷数は866万台（前年同期比18.9%増、内訳スマートフォン20%） 出典：IDC Japan
- スマートフォンの業務への急速な導入（日経コンピュータ 2010/12/8）
- 業務アプリケーションベンダーがスマートフォン対応アプリを投入
- 端末管理の要望の急速な高まり

＜予測＞出典：日経パソコン(2011年3月28日号)
年間出荷台数3700～3800万台の内、2011年度には4割、2012年度には5割に達する見通し。

企業が抱える期待と不安



Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

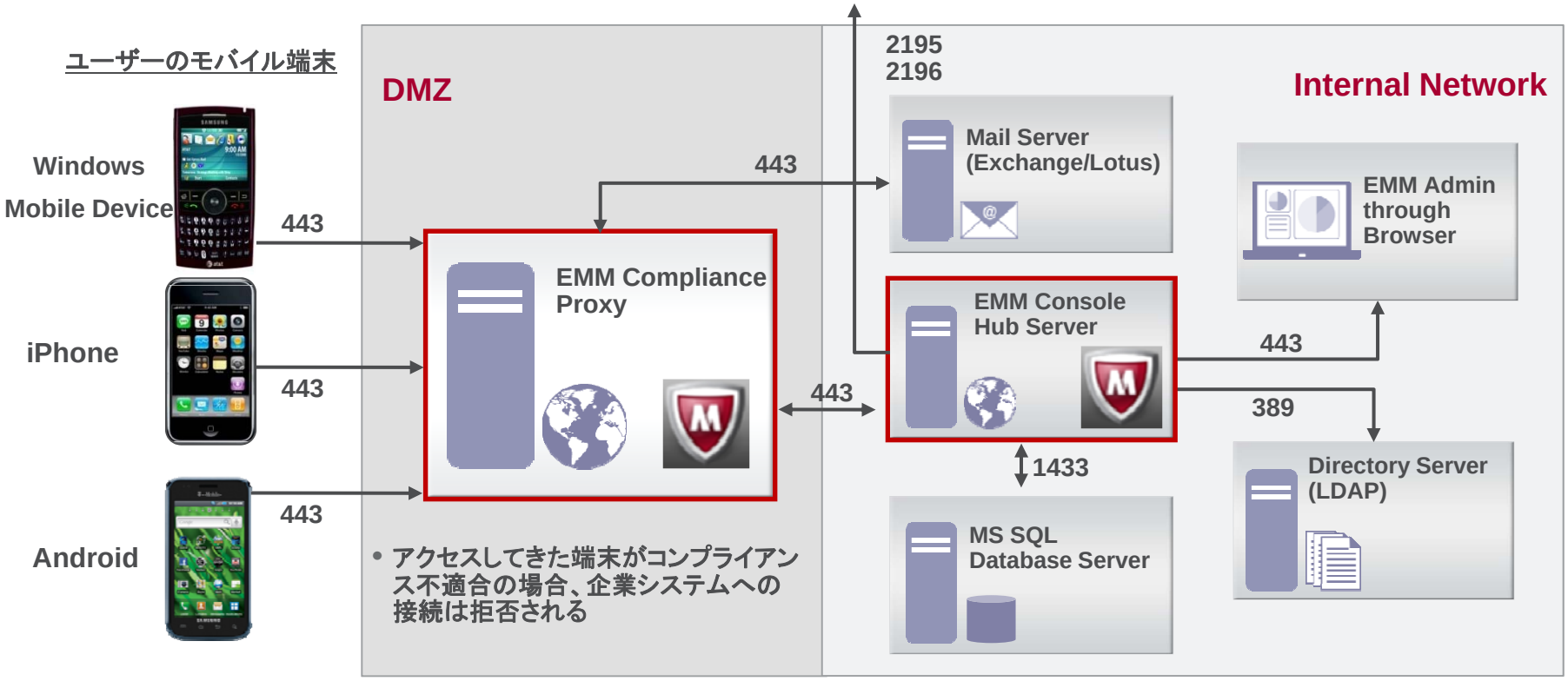
企業の求めるスマートデバイスへのセキュリティ

Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

モバイルデバイス管理（MDM）ソリューションとは？

- **情報漏洩対策に**
  - モバイル端末の紛失・盗難対策
- **よりセキュアに**
  - 企業ポリシー/コンプライアンスの遵守
  - セキュリティポリシーの作成と展開
  - セキュアに企業データにアクセス
- **より簡単に**
  - セルフ・プロビジョニング
  - 個々のニーズに対応する設定
- **大規模な展開にも**
  - モバイル端末の一元管理
  - 何千もの端末を運用管理出来る
    スケーラブルなシステム構成

MDMシステムの構成
（※McAfee Enterprise Mobility Managementの場合）



①MDMエージェントがインストールされたスマートフォンで、3G回線やWi-Fiなどを使用してインターネット経由で企業システムにアクセスする際、まず企業システムとインターネットの境界（DNZ）に設置されたコンプライアンス　プロキシのサーバーにアクセス。

②デバイスが企業が設定したコンプライアンスに適合しているかチェックされ、接続の可否が決定。

③コンプライアンス適合であれば、デバイスは社内のメールサーバーやその他のシステムリソースにアクセスする許可を得ることができ、企業システムの一部として動作することが可能。

Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

MDMによるセキュリティポリシーの適用

（※McAfee EMMでの設定項目になります）

デバイス紛失防止

- ▶デバイスPIN/パスコード強制
- ▶パスコード履歴とパスコードポリシー強制
- ▶パスコード失敗時のアクション設定
- ▶デバイス暗号化のチェック
- ▶完全/部分的デバイスのワイプ
  （データ消去）

セルフ・プロビジョニング

- ▶電子メールのリアルタイム同期
  (Exchange/Lotus Domino)
- ▶通信設定の自動設定
  - ■ VPN
  - ■ WiFi

デバイス制御

- ▶カメラ使用禁止
- ▶Webブラウザ禁止
- ▶アプリケーション制御

証明書に基づいた強力な認証

コンプライアンス管理とレポーティング

- ▶デバイスハードウェア情報
- ▶OS
- ▶脆弱なデバイスの状態
- ▶ポリシーと設定の状態
- ▶アクセス日時
- ▶導入アプリケーション一覧

セキュリティポリシー例

（※McAfee EMMでの設定項目になります）

項目	
コンプライアンス	暗号化されていない端末の接続制御
	Jailbreak/root化された端末の接続制御
	OSバージョンの制御（古いOSは接続不可）
メンバーシップ	ディレクトリグループごとのポリシー割り当て
パスワードポリシー	簡単なパスワード、長さ、英数字の組み合わせ、自動ロック、パスワード複数回失敗時のワイプ（ローカルワイプ）
	有効期間、履歴（過去パスワードの利用制御）
機能制御	iTunes, YouTube, Camera, FaceTime, Screen Capture, Active Sync Roaming, In-App Purchases, Multiplayer Gaming, Voice Dialing, Install Non-Enterprise App, Browser
プロビジョニング（設定配布）	VPNプロファイルの配布： L2TP, PPTP, IPSec(Cisco), Cisco AnyConnect, Juniper SSL
	WiFiプロファイルの配布： None(Open), WEP, WPA/WPA2, Any(Personal), WEP Enterprise, WPA/WPA2 Enterprise, Any(Enterprise)
PKI	証明書機関（Microsoft CA）と連携した証明書配布 (VPN/WiFiで利用)
メール同期	ActiveSync連携（Microsoft Exchange/ Lotus Domino）
ヘルプデスク（管理・運用）	デバイス情報の取得、導入アプリの情報取得
	ロック / ワイプ(完全/部分) / パスワードリセット
アプリケーション配布	推奨アプリケーションの表示

MDMによるiPhoneへの機能制限に伴う画面変更

機能制限適用前

ポリシー適用

- Restrict YouTube
- Restrict iTunes
- Restrict Camera
- Restrict Installing Non-Enterprise Applications
- Restrict Browser

機能制限適用後

ポリシーで制限されている機能が削除される

まとめ

- 強固なコンプライアンス運用を実現する，リアルタイムでのポリシーの設定・維持・確認
- デバイス，ポリシー，アプリケーション，接続設定を一元的に管理するとともに配布・適用を自動化
- 各端末への紛失・盗難時のデータ消去（ワイプ）やロックなどのセキュリティポリシーの適用
- 各端末のインベントリ情報の収集および確認

MDMによって、企業でのモバイルデバイス使用時のセキュリティを向上させ、安全にビジネスに利用することが可能になります。

Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

McAfee Enterprise Mobility Management
ご紹介

Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

モバイルデバイス管理のライフサイクル

Enterprise App Store
アプリケーションをセキュアかつロールに基づいて有効化し、ダウンロード可能もしくはAppStoreで入手可能、Webリンクから利用可能にする

Provisioning
セキュリティポリシー、ネットワーク接続、リソース（デバイスを自動的にパーソナライズ化するためのセルフサービス・プロビジョニング）の定義

IT Operations Support
McAfee ePOコンソールを利用することで接続しているデバイスを集中的に可視化して管理できます

Security and Authentication
2要素認証をサポートし、Microsoft CAよりもさらに強力な方式でデバイス認証します

Compliance
ネットワークに接続する前にデバイスを自動的にチェックします

Policy Management
OTA(Over the Air)によりセキュリティポリシー、コンフィグレーションをアップデートすることでヘルプデスク業務を効率化します

Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

EMMの特徴

- シングル・コンソールによる一元的な操作性を実現
  - 弊社統合管理ツール（McAfee ePolicy Orchestrator）との統合により、モバイル端末、ラップトップPC、サーバなどのセキュリティ管理を同じコンソールで一元管理
- マルチOS対応
  - Android, iOS, Symbian, Palm, Windows Mobileに対応
- 管理者を必要としないユーザ自身でのプロビジョニング
  - EMMエージェントをインストールした端末からメールアドレスとパスワードによる認証のみで端末のプロビジョニングが可能
  - 個人所有端末であっても、コンプライアンス適合すれば企業ネットワークへの接続が可能
- データワイプ時に、完全消去に加え、企業環境と個人環境との共存を実現する「部分消去」を実装
- 無線環境でのアプリケーションの配布・更新を提供する，Over-The-Air 技術を実装

Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

McAfee Mobile Security
ご紹介

マルウェア対策 / 端末紛失対策 / 安全なウェブ検索

Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

McAfee Mobile Security
マルウェア対策 / 端末紛失対策 / 安全なウェブ検索

■ モバイル端末の総合セキュリティソフトウェア

- マルウェア対策
- リモートロックとデータの消去
- デバイスの位置特定と追跡
- 自動バックアップとリストア
- 安全なウェブの閲覧と検索

Copyright © 2003-2011 McAfee, Inc. All Rights Reserved.

McAfee®