



Securing Your Journey
to the Cloud



クラウド時代に求められる スマートフォンの管理とセキュリティ対策

トレンドマイクロ株式会社 エンタープライズマーケティング
転法輪 浩昭, プロダクトマーケティングマネージャー

Agenda

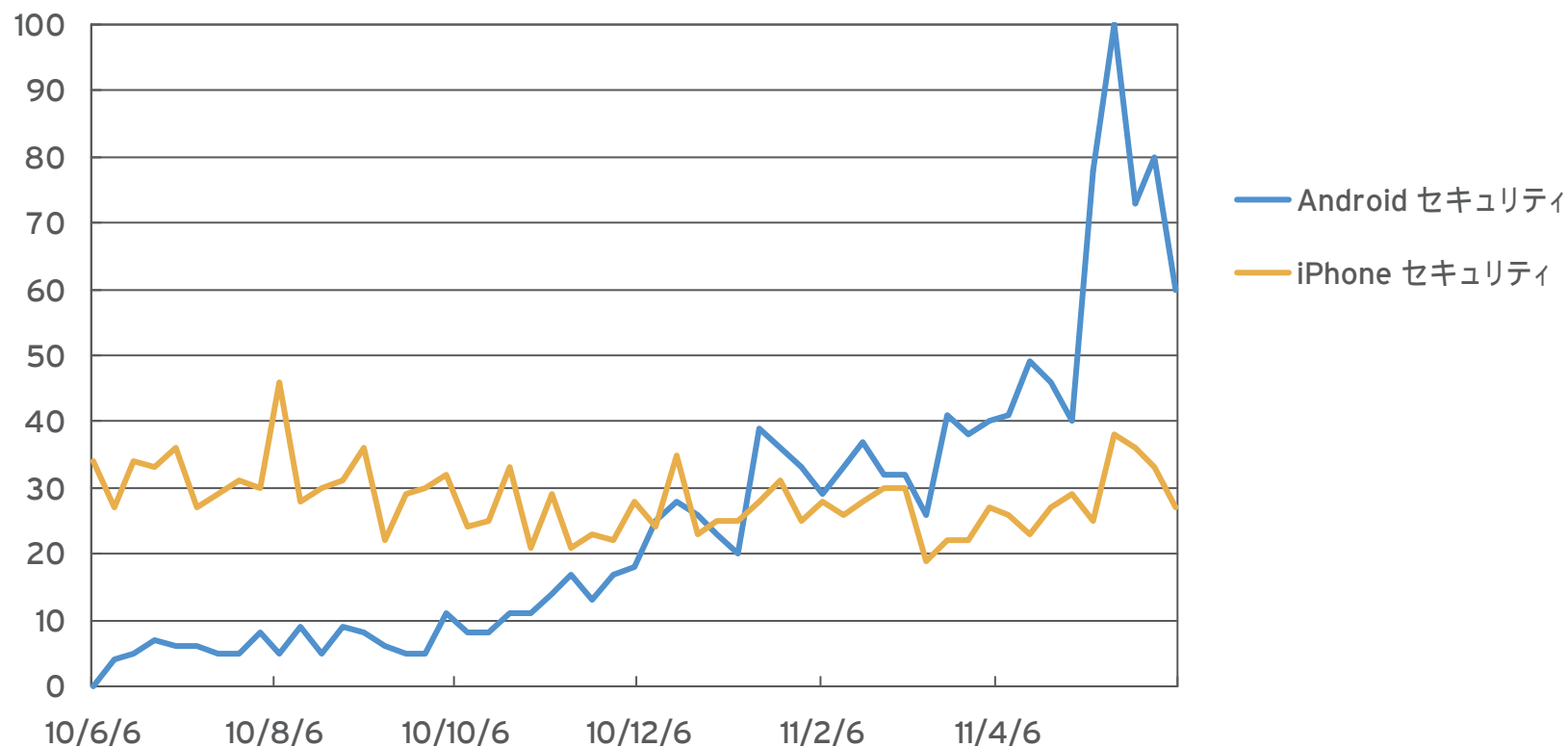
スマートフォンウィルスの現状

法人におけるスマートフォン活用の課題と

トレンドマイクロの取り組み

スマートフォンとセキュリティ

スマートフォンのセキュリティへの関心



Google Insights for Search

キーワード:

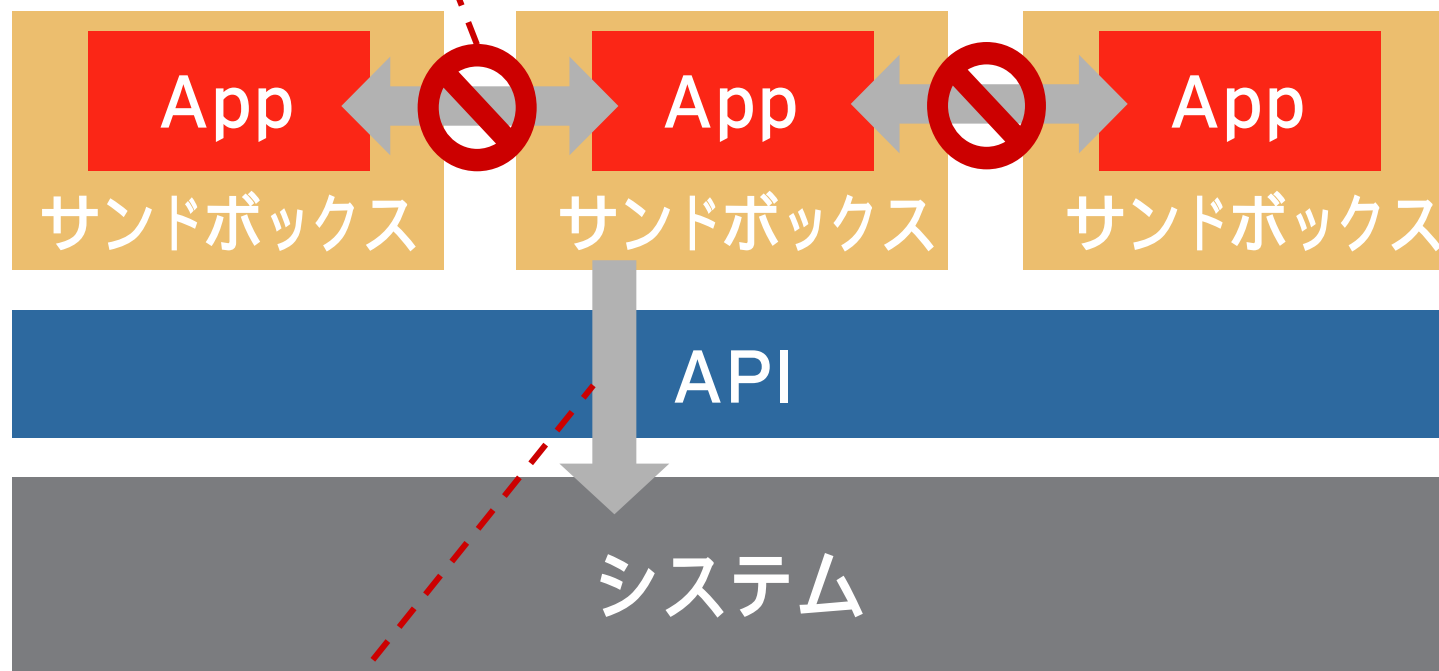
- Android セキュリティ + アンドロイド セキュリティ
- iPhone セキュリティ + iOS セキュリティ + iPad セキュリティ

地域: 日本

期間: 2010/6-2011/6

一般的なスマートフォンのシステムの構造

アプリケーションはお互いにアクセスできない



アプリケーションは限定的な API を通じてのみシステムの機能
やリソースへアクセスできる

ソフトウェアの配布と安全性

開発者の登録

- 開発者の登録費用
 - iOS: \$99/年, Android: \$25 (1回のみ)
- クレジットカードを利用
 - セキュリティコードの利用

マーケットへアプリケーションの登録

- Apple App Store : 審査
- Android マーケット: 無審査

マーケットにおける配布

- 利用者はインストール前に評価、ダウンロード数や、リソースのアクセス許可(Android)などを参照可
- デジタル証明書によるリリース後の不正プログラム感染からの保護 (特にIOS)

デバイスへのインストール



- IOS の場合は App Store からのみインストール
- Android マーケット以外からも自由にインストール

Jailbreak/ルート化とセキュリティ

- Jailbreak

- iOSの脆弱性を利用して、App Store以外で提供される非正規アプリケーション等のインストールが可能な環境を構築すること。Apple のサポート外。
- Ikee、Duh、Ikee.B など Jailbreak したデバイスで動作する不正アプリケーションが見つまっている

- Root化

- Androidではセキュリティ等の理由からユーザーやアプリケーションがある階層以上にしかアクセスできないように制限がなされている。その制限を解除し最低階層にアクセスできるようにすること

iOS の脆弱性を悪用するJailbreakツール

• 経緯

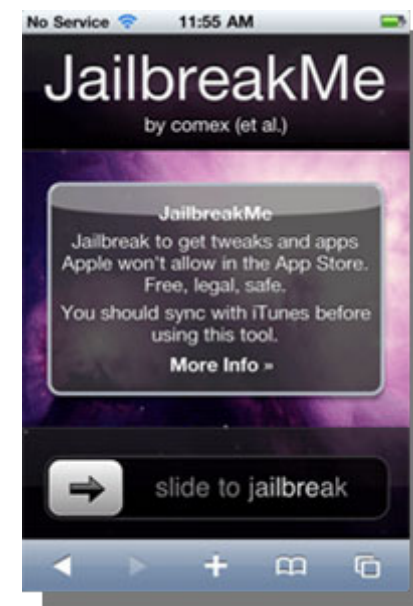
- 2010年8月、iPhone4対応のJailbreakツール "JailbreakMe"がインターネット上で公開されていることを確認。iOS の2つの脆弱性を悪用してJailbreakを簡単に可能とする。

• 悪用された脆弱性と流れ

- CVE-2010-1797 : SafariでPDFファイルを閲覧する際に生じる脆弱性。
- CVE-2010-2973 : iOS搭載の端末に侵入した攻撃者の権限を昇格させる脆弱性。

• 危険性

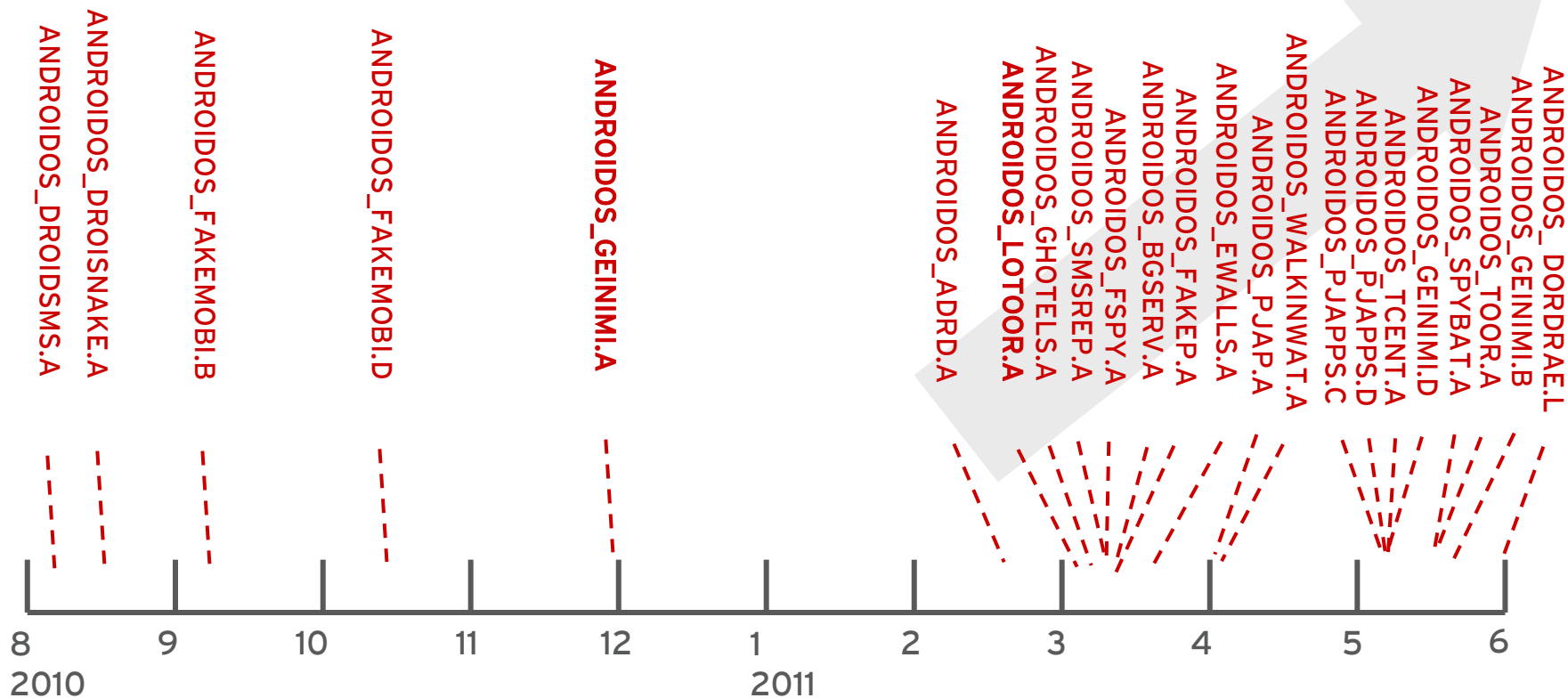
- 現在見つかっている不正アプリケーションはJailbreak したデバイスだけで動作が確認されている



増加する Android 向けマルウェア



Android端末に感染する不正プログラムは半年で約14倍に急増 *1



*1 2010年12月末と2011年6月末時点の当社のパターンファイル登録数を比較



Android不正プログラム例

アプリを装って侵入

- ANDROIDOS_GEINIMI.A

- ゲームアプリに混入、非公式サイトから配布。インストールしているアプリや、利用者情報、機種モデル名や端末のGPS情報を外部に送信。
- “世界初のAndroidボット”として注目。

- ユーザ自身が非公式な場所からアプリやゲームを手しインストールして初めて感染する。
- Android Market では今のところ配布されておらず、中国の非公式アプリ配布サイトからしか見つかっていない。

- 再パッケージされて配布されているアプリケーション

例

Aliens vs.
President



いっしょに
とれーにんぐ



Monkey
Jump 2



Baseball
Superstars 2010



ANDROIDOS_GEINIMI.A動作イメージ

悪意のあるユーザサイト
(C&Cサーバー)

私設のマーケット、web

ANDROIDOS_GEINIMI.A
感染済みアプリケーション
をダウンロード

サービスとして常駐し、以下の
コマンドを実行

- ・ パッケージ/アプリケーションの列挙
- ・ アプリケーションの実行
- ・ アプリケーションダウンロード/
インストール/アンインストール
- ・ 携帯電話のGPS座標情報の収集
- ・ 連絡先情報の解析 / 読み込み
- ・ 携帯電話の受信箱に保存されている
SMSやEメールなどのメッセージの解析
/読み込み

また、以下の情報を収集し
サーバへ送付

- ・ ダイアルイン番号/IMEI/IMSI番号など
- ・ システムプロパティ情報

5分毎にサーバにアク
セスし、コマンドの確認
と結果を送付

クライアント&サーバ
間の通信を暗号化

以下のポートをOpen。

- TCPポート4501番(IANA)
- TCPポート8791番(Unassigned)
- TCPポート6543番(Ids_distrib)
- TCPポート5432番(PostgreSQL Database)

Android端末

法人におけるスマートフォン活用の課題と トレンドマイクロの取り組み

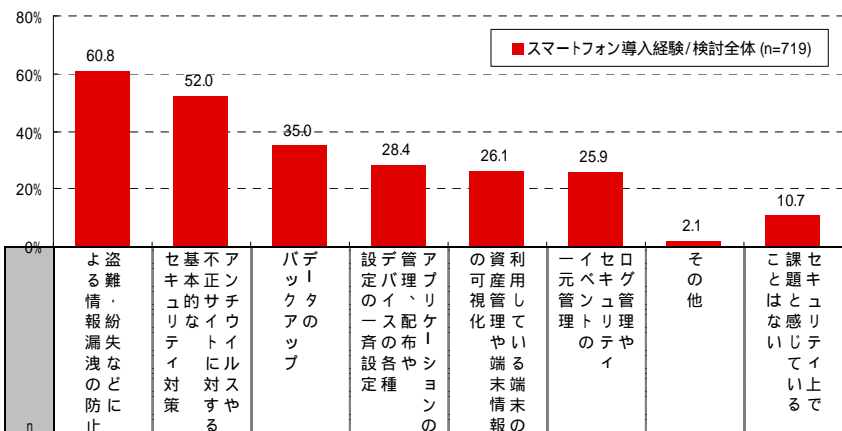


法人におけるスマートフォン導入の課題

スマートフォン管理・セキュリティの課題

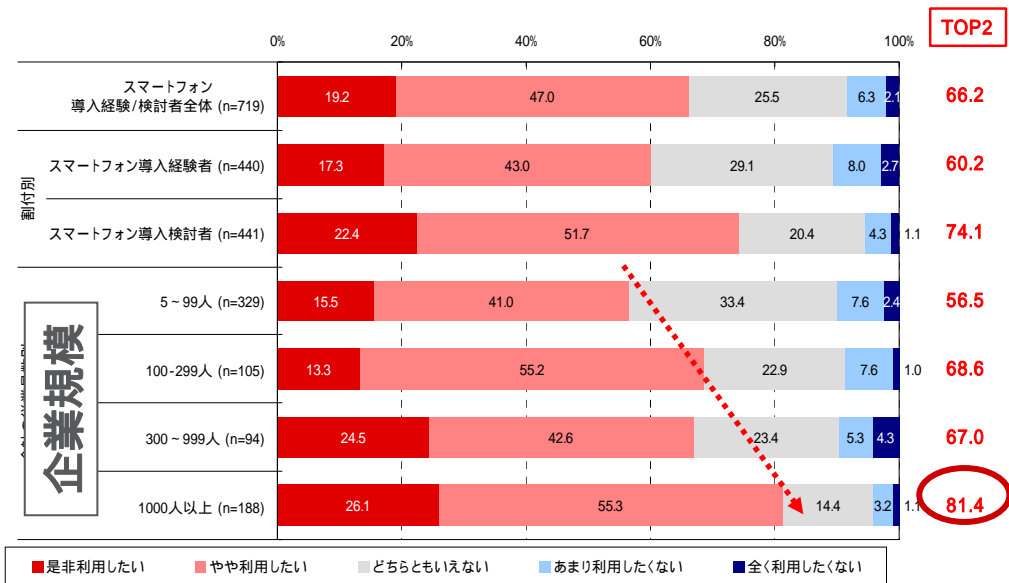
(Source: トレンドマイクロ, 03/2011)

1. 紛失・情報漏洩 61%
2. ウイルス、不正サイト 52%
3. データの保護 35%
4. 管理(資産、構成、変更) 25%ずつ



モバイル端末の管理、セキュリティ対策の導入意向

(Source: トレンドマイクロ, 03/2011)

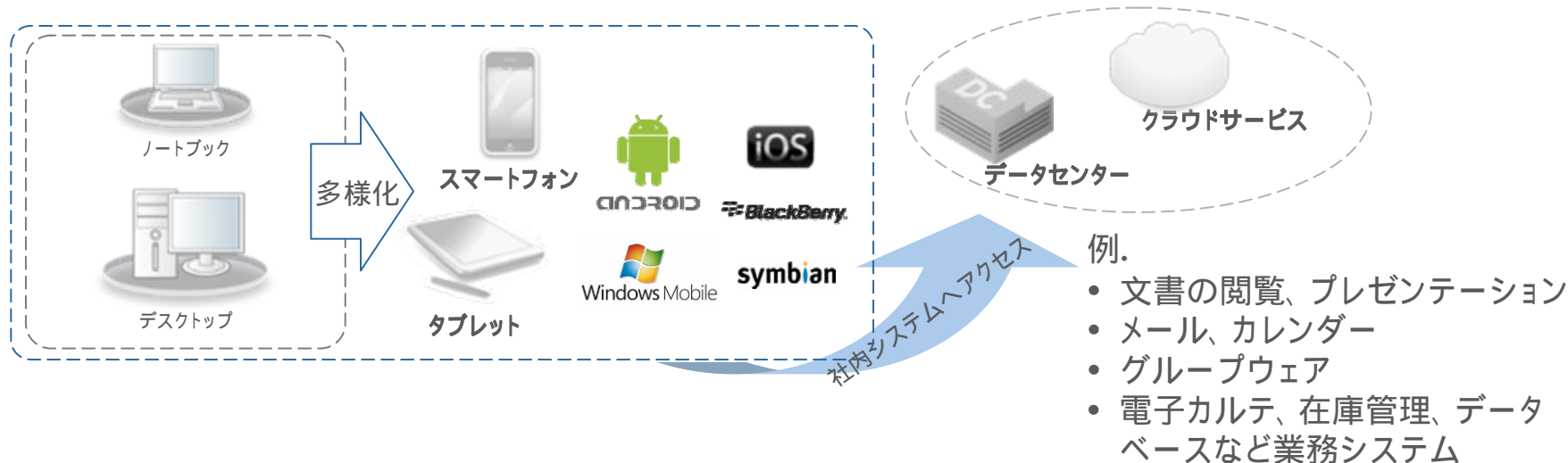


- 紛失対策、コンテンツセキュリティ対策などが大きな課題と認識
- 60% を超える法人がユーザーセキュリティ対策やデバイス管理の導入に積極的
- 企業規模の大きなほど、管理、セキュリティ対策両方の対策を求めている

エンドポイントの多様化と管理の必要性

ユーザの懸念

- Android 端末の増加をはじめエンドポイントが多様化でどう管理すればよいか分からない
- 端末の紛失などによる情報漏えいのリスク



- ガバナンスの強化で情報漏洩などのセキュリティリスクの低減
- 効率的なデバイスの管理

Trend Micro Mobile Security

● 主な特徴

- モバイルデバイス管理からコンテンツセキュリティまで、ひとつの管理基盤で集中管理
- 集中管理を備えたコンテンツセキュリティ対策

● 主な機能

- 不正プログラム対策
- Webからの脅威対策
 - Web レピュテーション
- 着信/SMSフィルタ
- リモートワイプ、リモートロック
- 一元的なポリシー管理
 - パスワード強制
 - カメラ、Bluetooth などの機能制限
- 端末情報やログの一元管理

● 対象デバイス



Trend Micro Mobile Security

セキュリティ対策からデバイス管理まで包括的なソリューション


コンテンツセキュリティ対策	モバイルデバイス管理
<ul style="list-style-type: none">不正プログラム対策不正サイトのブロック通話/SMS のフィルタリング	<ul style="list-style-type: none">リモートロック / リモートワイプGPSトラッキング機能制限 (カメラ、Bluetooth)パスワードの強制設定デバイスプロビジョニング(*)ソフトウェア管理(*)
<h3>集中管理</h3> <ul style="list-style-type: none">エージェント配布ポリシー管理レポートログ管理 (*)	

* 将来の機能追加、強化を予定しています。



その他のツール

無償
配布中

- ウイルスバスター モバイル for Android
 - 不正プログラム対策
 - 不正サイト、有害サイトへのアクセスをブロック
 - 不要な電話、SMSをブロック
 - ベータ版を無償配布中
 - <http://tmqa.jp/vbma/>
- Smart Surfing for iPhone OS
 - iOS 用のセキュアブラウザ
 - Webレピュテーション技術を使い、危険なサイトへのアクセスをブロック
 - 無償で配布中 
 - <http://jp.trendmicro.com/jp/products/personal/ssfi/>





TREND
M I C R O TM

Securing Your Journey
to the Cloud