

第43回 スクエアfreeセミナー

ビジネスの安全を守るセキュリティ基盤

～ スマートデバイスのセキュリティ対策 ～

株式会社OPENスクエア
田中 昭造

今どきのシステム構成



クライアント

ネットワーク

サーバ



PC

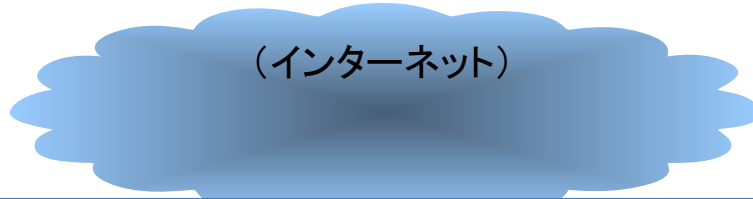


携帯電話



スマートデバイス

PCと携帯電話の利点を備えていることから、業務での利用が拡大



(インターネット)

VPN接続



Load Master



Webサーバ



DBサーバ



アプリケーションサーバ

セキュリティ
対策

SWANStor®

MOBILE CONVERT
for スマートフォン

ポストPC or PC+ (プラス)



クラウドの浸透、通信環境の整備によりスマートデバイスが急速に普及

場所を問わない

時間を問わない

簡単に使える

スマートデバイスの特徴



PCの代わりに利用

新たにモバイル端末として利用



アンチウイルス PCと同様のセキュリティ対策が必要



アンチセフト 更にデバイスの紛失、盗難(ひったくり)対策も必要

セキュリティ上の脅威 1



国内の携帯電話

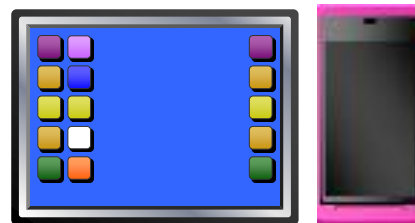


機種ごとに異なる仕様

利用者の自由度は低い

ウィルスを作りにくい／
ウィルスに感染しにくい

スマートデバイス



特徴が似ている

海外製を含む多くの機器で共通の仕様

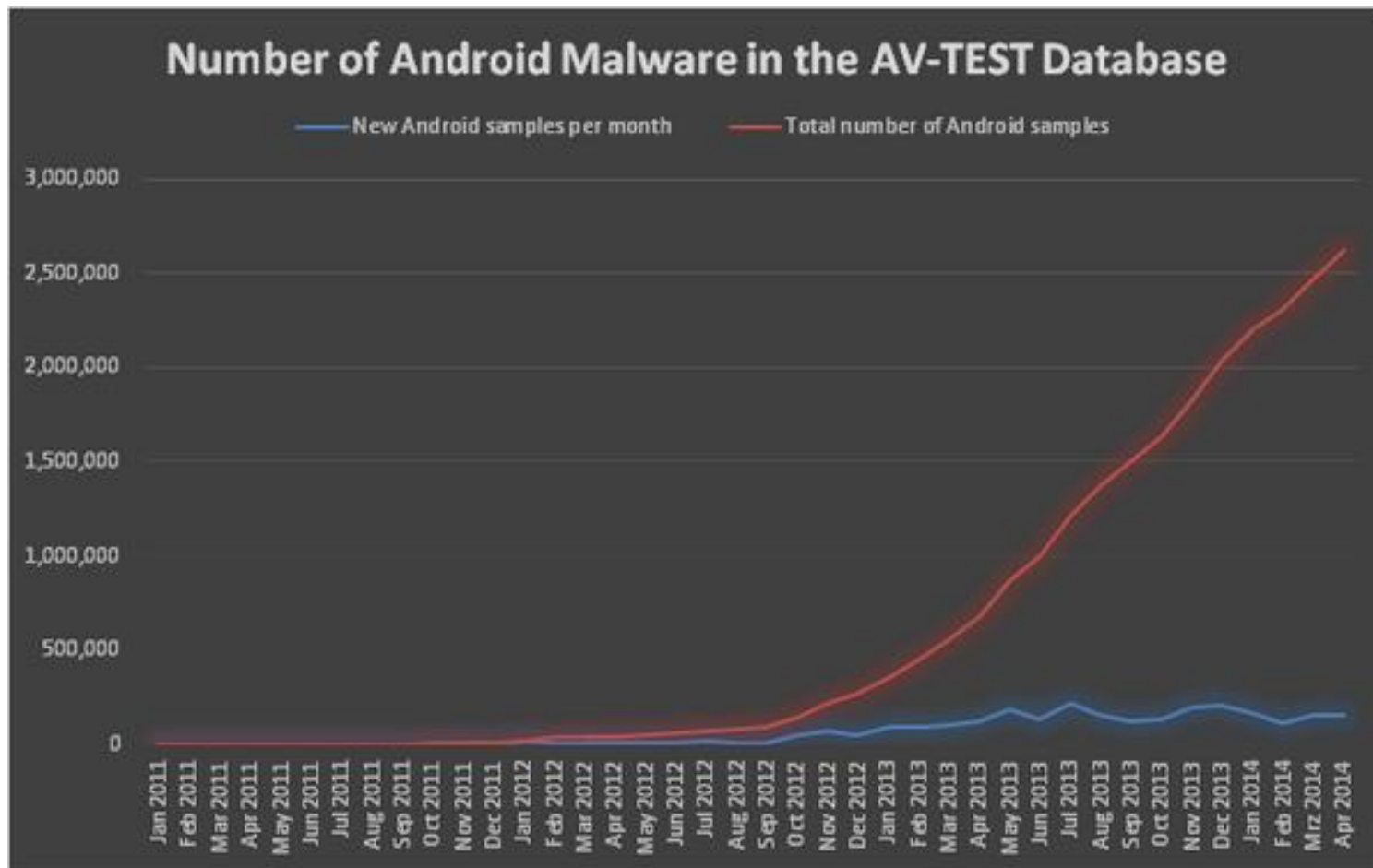
利用者が自由にアプリケーションを追加でき、
アプリケーションを開発することもできる

ウィルスの脅威は似た状況である

PC



急増するスマートデバイスのマルウェア



毎月、AV-TESTは約150,000の新しいユニークなAndroidのマルウェアの検体を登録。

これまでの合計は266万。

出展: AV-TEST

セキュリティ上の脅威 2



紛失

スマートフォンの紛失台数、1年間で142,706台

マカフィーとPonemon Institute社が439社を対象として調査した結果では、スマートフォンの紛失数は1年間142,706台。そのうち約62%は、従業員に業務用として支給している会社所有のスマートフォン。

(参照: マカフィーとPonemon Institute社は2012年7月17日に発表した「The Lost Smartphone Problem(スマートフォンの紛失問題: 英語)」調査結果)

盗難(ひったくり)

スマートフォンの盗難が多発、目的はブラックマーケットでの販売

- ・世界中でスマートフォンの盗難件数が急増している。一台何百ドルもする製品の旺盛な需要があり、何百万人もの人たちがこうしたデバイスを地下鉄や歩道で手に持った(通話中も含めて)ままなので狙われる。
- ・日本でも昨年11月に東京都台東区と千代田区の路上でのスマートフォン(スマホ)を狙ったひったくり事件が発生。13日からの7日間で少なくともスマホ12台(新しい機種「iPhone5」が9台、1世代前の「iPhone4」が3台)が被害。

OPENスクエアがお手伝いできること



現在、世界3位のシェアを誇るエンドポイントセキュリティー・スイート製品をご紹介します。

- 1. 検知力が凄く、運用が容易な製品お届けします。**
- 2. クライアント、サーバ、スマートデバイス、仮想環境の全てをサポートした製品をお届けします。**
- 3. アンチウィルス、アンチセフトの両方をサポートした製品をお届けします。**



KASPERSKY lab

Kaspersky製品ラインナップ



エンドポイントプロテクション

- 様々なOSに対応。社内ITを包括的に保護
- 管理サーバで一元管理
- セキュリティポリシーに応じて機能が選べる柔軟なライセンス体系



仮想環境のプロテクション

- VMwareの仮想環境を基盤から保護
- 仮想OSにアプリケーションをインストールしないエージェントレスタイプ
- 仮想OSに負荷を与えず、保護可能



メールセキュリティ

- スпамメール対策
- ウイルスメール対策
- 標的型メール攻撃(ゼロデイ)対策
- クラウドとの連携で即座に対応



ウェブセキュリティ

- Proxy(Squid)と連携したウェブコンテンツをスキャン
- 改ざんされたページから感染するマルウェアから保護



Kaspersky Security for Business



Advanced

ライセンス管理

イメージ管理

NAC

暗号化

脆弱性対策・パッチ管理

リリース予定

脆弱性対策・
パッチ管理

Select(クライアント-サーバタイプ)

Select(クライアントタイプ)

コントロール

デバイスコントロール
アプリケーションコントロール
コンテンツフィルタ

MDM

アンチウイルス

アンチウイルス

Core

アンチウイルス



Windows



Mac



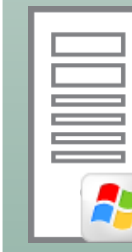
Linux



Android



iOS



Windows



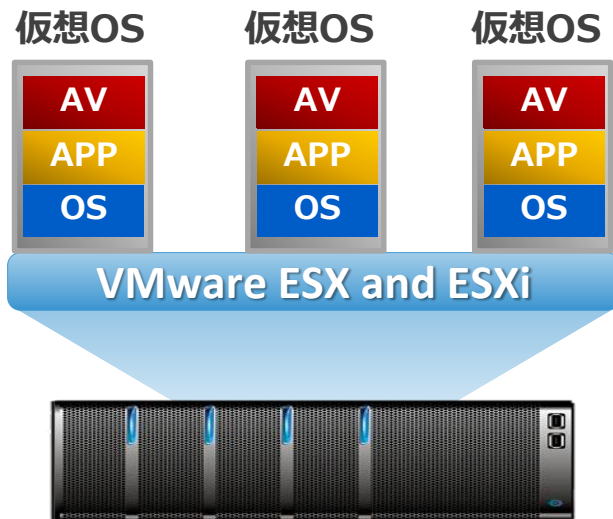
Linux

Kaspersky Security for Virtualization



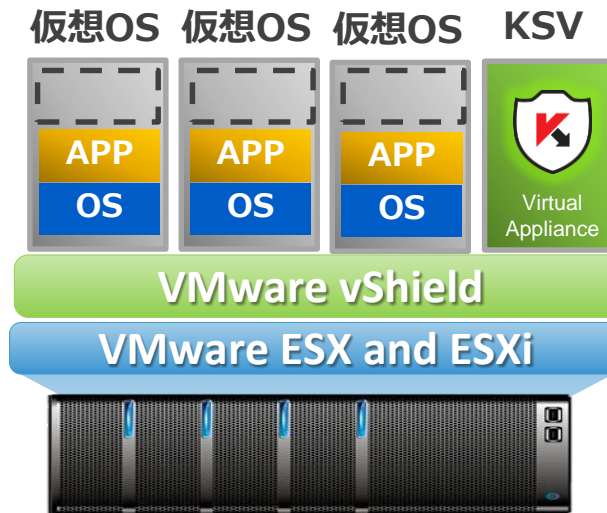
仮想環境における従来のセキュリティー対策
各仮想OSにそれぞれ、セキュリティーソフト
をインストール

仮想環境におけるカスペルスキーの
セキュリティーソリューション
各仮想OSはエージェントレス！
仮想環境の集積度向上



それぞれの仮想OSで・・・

- ・インストール作業
- ・CPU/メモリ/HD(定義DB)のリソースを消費
- ・定義データベース更新作業、フルスキャンタスク
- ・バージョンアップなどのメンテナンス作業
- ・運用管理、監視



Virtual Appliance(仮想アプライアンス)を導入するだけで・・・

- ・全仮想OSの保護が可能
- ・**KSV**だけが定義データベースを更新
- ・**KSV**だけが各仮想OSをスキャン
- ・**KSV**だけをメンテナンス
- ・**KSV**だけを運用、監視

Kasperskyの凄い1



▶ 検知力 = 防御力 がスゴイ！

- 第三者評価機関からの最高水準の評価
- 導入頂いたお客様先でも今まで潜んでいたウイルスが検知された事例など多数

A社、B社の製品を利用

レントゲン画像サーバへのアクセスが突然切断される

カスペルスキー製品導入

- ネットワーク攻撃型のマルウェアを多数検知→駆除・削除
- レントゲン画像サーバへの接続障害が解消

A社の製品を利用

特にマルウェアの検知は無かった

カスペルスキー製品導入

- 今まで見落としていたマルウェアを検知
- 他自治体が管理しているウェブサイトの改ざんも検知。

Kasperskyの凄い2



▶ ウイルス対策機能以外にもこんなことが出来る

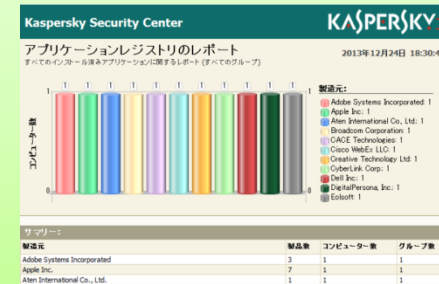
セキュリティーリスクのコントロール

- 外付けデバイス接続の制御
- アプリケーションの起動制御
- ウェブコンテンツのフィルタリング



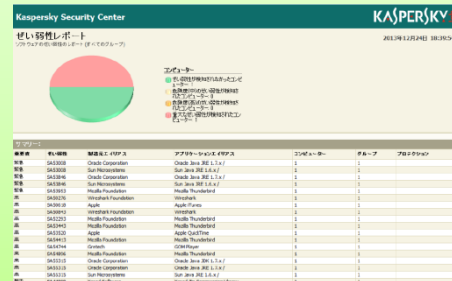
資産情報レポート(ソフト、ハード)

- ソフトウェアのインベントリレポート
- ハードウェアのインベントリレポート



ぜい弱性モニター

- アプリのぜい弱性をモニタリング
- ぜい弱性を発見次第、管理者にアラート

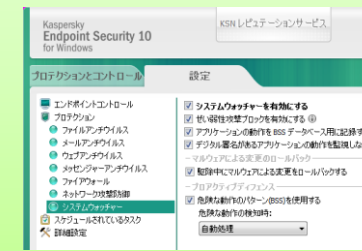


ゼロデイ攻撃対策

ゼロデイ対策機能として

- ヒューリスティックスキャン
- ウェブ、メールアンチウイルス
- 振舞い検知
- AEP

(Automatic Exploit Prevention)を搭載



Kasperskyの凄い3



▶ 管理がラク!、入れ替えもラク

一つの管理サーバですべてを管理

一つの管理サーバで管理が可能

- Windows
- Mac
- Linux
- Android
- iOS
- 仮想環境

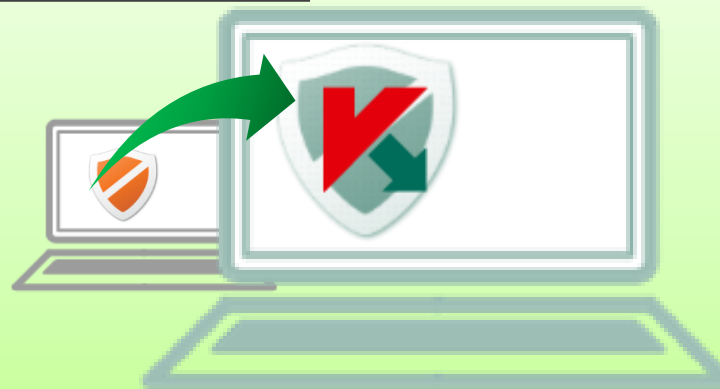


Kaspersky Security Centerでまとめて管理



管理サーバからリモートで導入

- 既存製品のリモートアンインストール
- カスペルスキー製品のリモートインストール



これからのシステム構成



クライアント

ネットワーク

サーバ



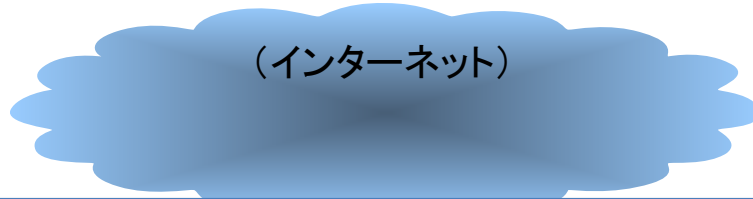
PC



携帯電話



スマートデバイス



(インターネット)

VPN接続



Load Master



Webサーバ



DBサーバ



アプリケーションサーバ



お問い合わせは



株式会社OPENスクエア

担当 : 田中昭造

電話 : 03-6413-1840

メールアドレス : salese_os@opensquare.cp.jp

ご清聴ありがとうございました。