IoT時代の
デジタルサイネージに求められるセキュリティ

2015年3月10日

マカフィー株式会社　セールスエンジニアリング本部　二宮秀一郎

本日のAgenda

❖IT環境を取り巻く現状
- ▶デバイスの多様化と巧妙化するサイバー攻撃

❖Internet of Things時代のセキュリティ
- ▶Intelの定義するInternet of Things
- ▶Internet of Thingsにおけるセキュリティ

❖IoT Deviceのセキュリティ
- ▶McAfee® Embedded Control

❖IoT時代のSecurity

IT環境を取り巻く現状

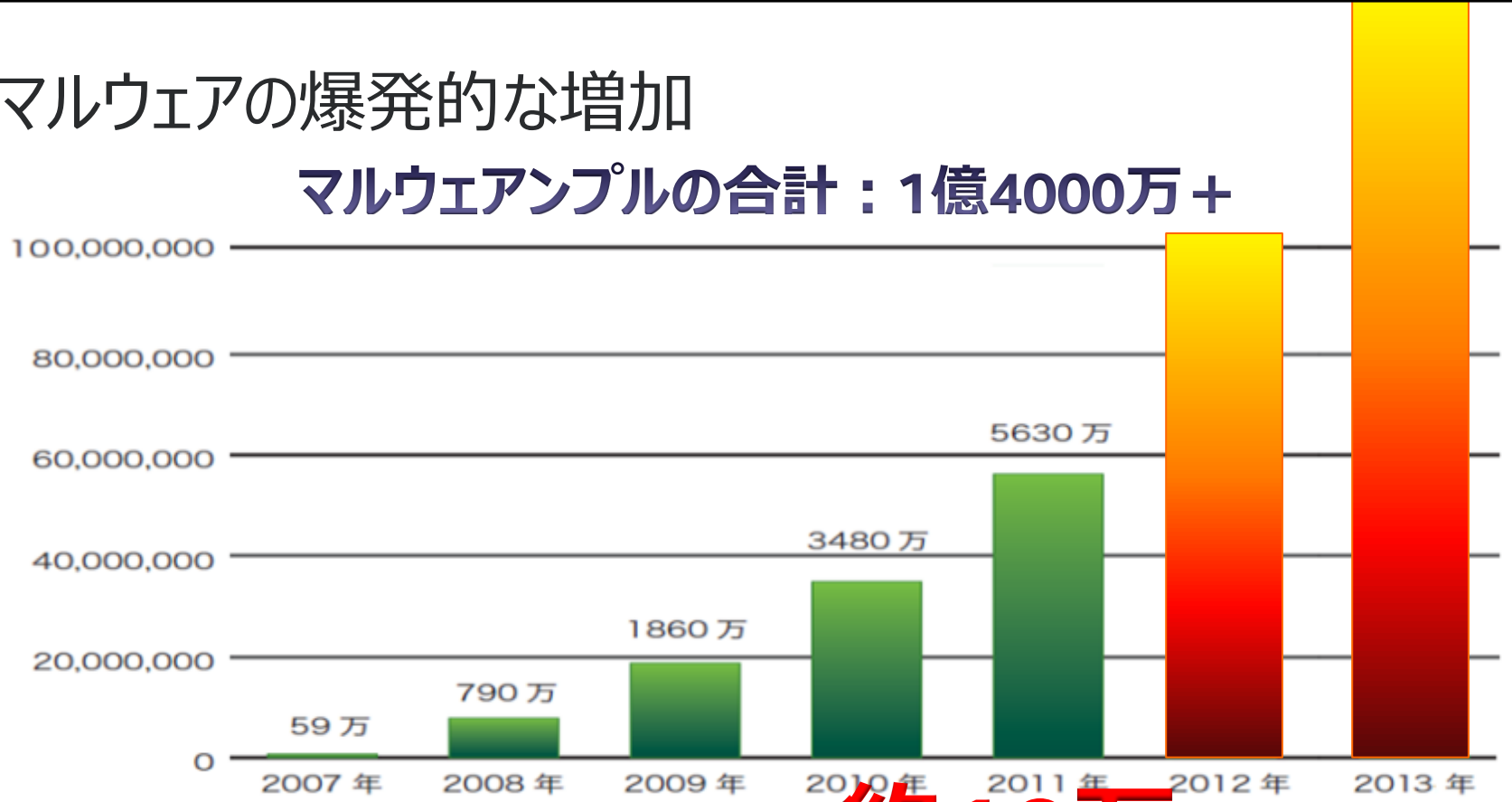
デバイスの多様化と巧妙化するサイバー攻撃

IT環境の変化 Anytime, Anywhere

デバイス・ネット環境の多様化，アプリケーションの氾濫

マルウェアの爆発的な増加

マルウェアンプルの合計：1億4000万＋



1日に発生するマルウェア 約10万 件以上

McAfee脅威レポート：2012年第3四半期 http://www.mcafee.com/japan/about/prelease/pr_12b.asp?pr=12/12/04-1

巧妙化するマルウェア

1分毎に出現するマルウェア数

*Source: McAfee Labs 脅威レポート 2013年第4四半期

200

マカフィーが保有するマルウェアのサンプル数

*Source: McAfee Labs 脅威レポート 2014年第1四半期

200,000,000+

難読化・パッキング（対策製品の検知を逃れるための巧妙な細工）されているマルウェアの割合

*Source: McAfee Labs

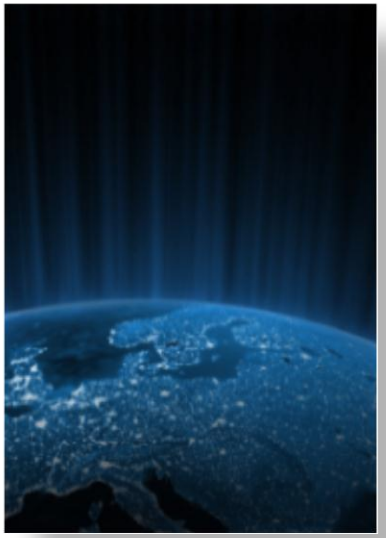
60%

セキュリティの脅威動向

Slammer

ZeuS

Aurora



Stuxnet

愉快犯 → 金銭目的の組織的犯罪 → 知的所有権奪取を目的 → 国家が操る犯罪

組込みシステムにおける事例

狙われるPOSシステム/カード情報

How RAM Scrapers Work: The Sneaky Tools Behind the Latest Credit Card Hacks | WIRED
http://www.wired.com/2014/09/ram-scrapers-how-they-work/

マルウエアの特徴

- 空調機器システムを提供していた業者のネットワークを経由し侵入

- 市販のマルウエア（BlackPOS）がベース
- Target社のシステム環境にあわせて
  マルウエアはカスタマイズされていた

アンダーグランドで販売されていたBlackPOS/Kaptox
(POS端末向けのマルウェア)は$1,800～$2,000程度

Remote Name	Resource Type	Local Resource to Map	Connect as User	Connection Password
\\10.116.240.31\c$\WINDOWS\twain_32	RESOURCETYPE_DISK	S:	ttcopscli3acs\Best1_user	BackupU$r

Targetの設定（ユーザIDやIPアドレスなど）がマルウエアにハードコーディング

- **不正侵入後に内部環境を詮索**
- **環境にあわせてマルウエアを作成**

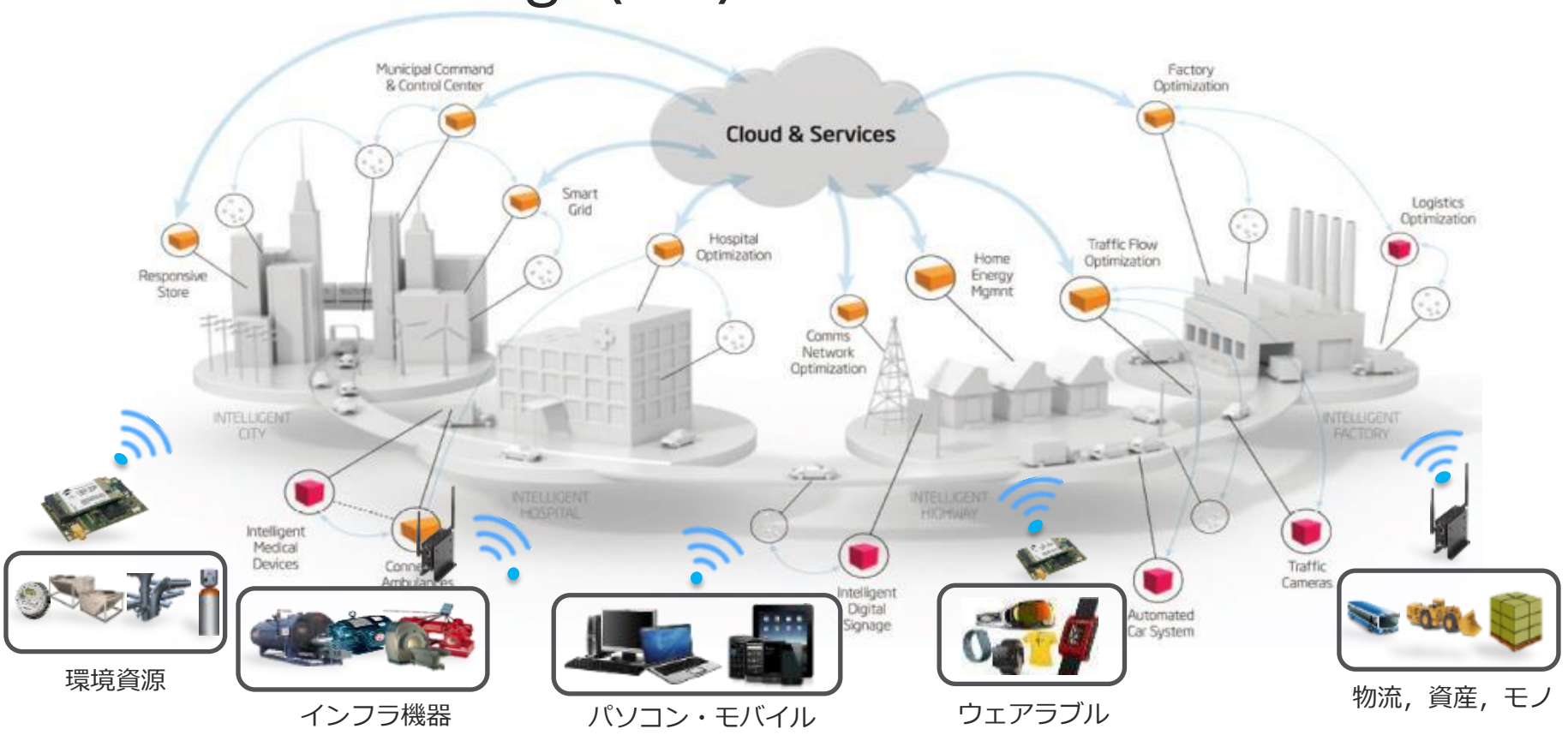
デジタルサイネージは安全でしょうか？

San Francisco Digital Traffic Sign Hacked, Warns of "Godzilla Attack"

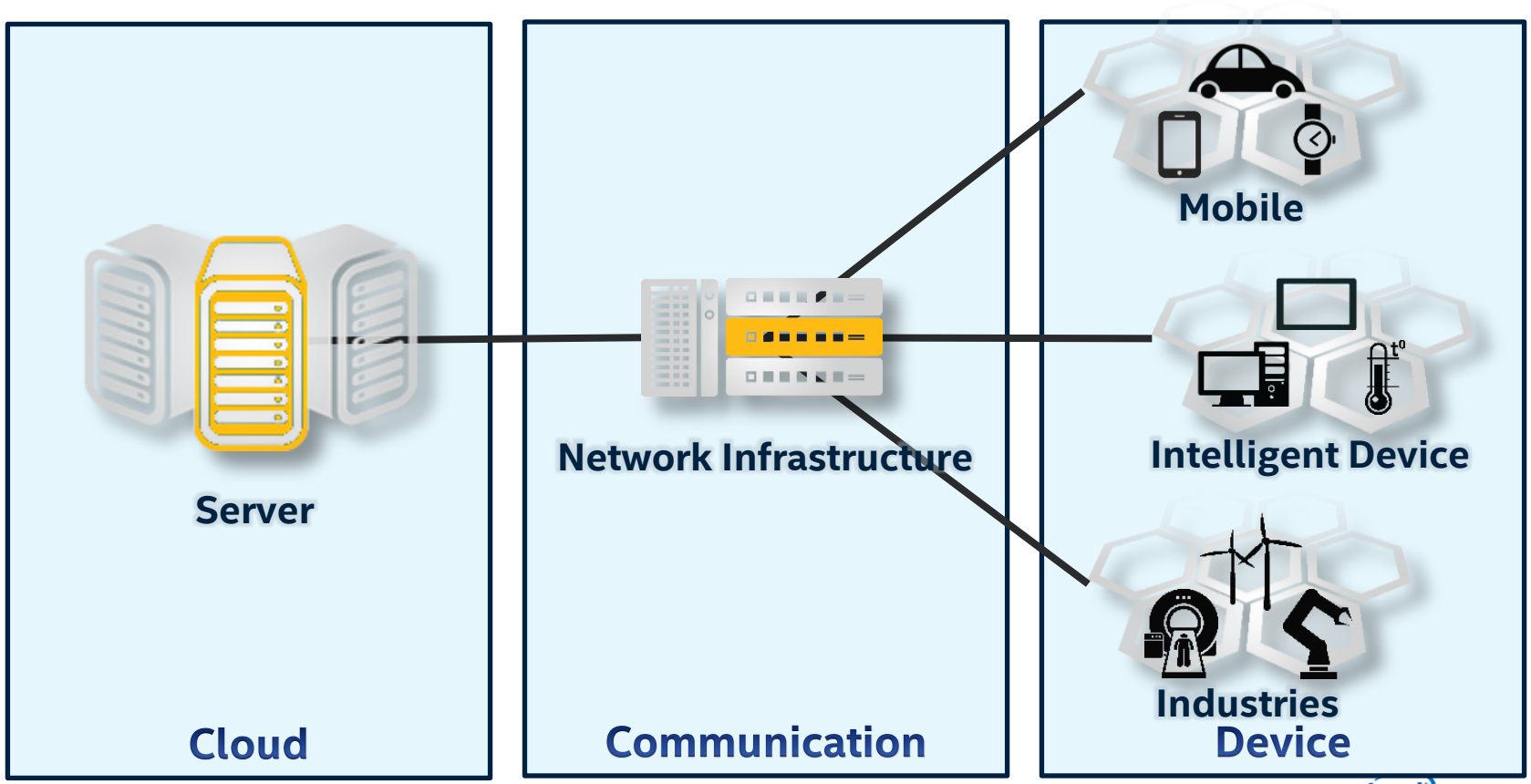
出展：http://www.nbcbayarea.com/news/local/Hacked-San-Francisco-Message-Board-Warns-About-Godzilla-Attack-259449961.html

Internet of Things時代のセキュリティ

Internet of Things (IoT) ～ モノのインターネット



Intelの定義するInternet of Things



Internet of Thingsにおけるセキュリティ

Device

- セキュリティに優れたID管理
- デバイスの完全性
- データ・プロテクション

Communication

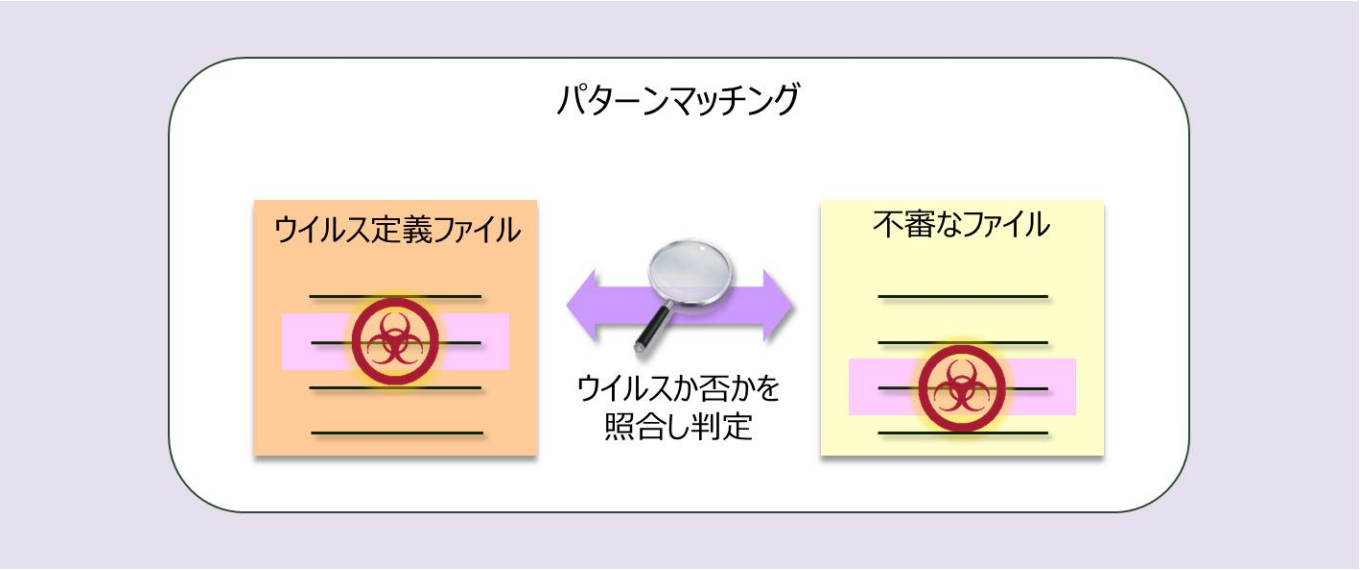
- アプリケーションのセキュリティ
- トラヒックの保証
- データの完全性

Cloud / Data Center

- IoTサービス，分析に要求される信頼性
- データの完全性
- システムの可用性・拡張性

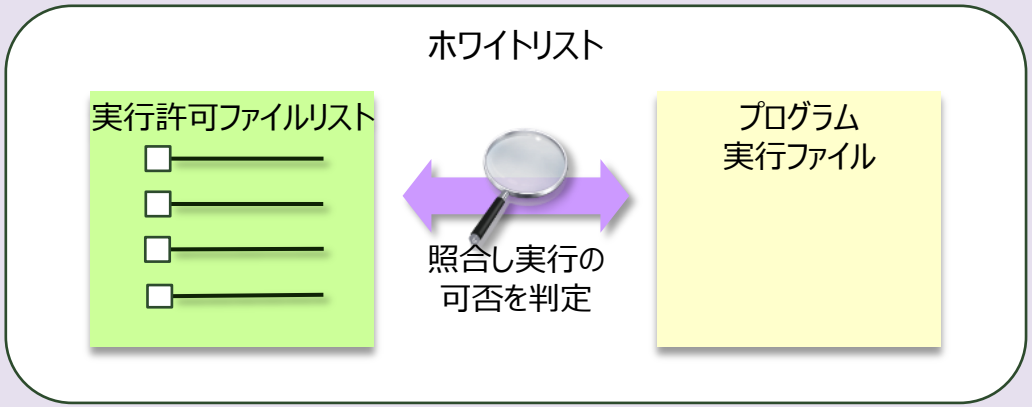
IoT Deviceの鉄壁の防御

ブラックリスト型セキュリティ



ホワイトリスト型セキュリティ対策

動かしても良いプログラム，スクリプトを定義することによって
怪しげなプログラムが入り込んでも動かせなくする技術
実行可能な全てのファイルを『漏らすことなく』制御することが重要



ウィルス対策のアプローチ
ブラックリスト方式とホワイトリスト方式

ブラックリスト方式

- ❖指名手配
- ❖動かしてはいけないプログラムをリスト

- ❖ウィルス定義ファイルの更新が必要
- ❖フルスキャンが必要

- ❖製品のサポート期間≒OSのサポート期間
- ❖大多数の製品が，Embedded OSはサポート外

ホワイトリスト方式

- ❖通行手形
- ❖動かしても良いプログラムをリスト

- ❖ウィルス定義ファイルの更新は不要
- ❖フルスキャンは不要

- ❖OSのサポート終了後も製品の利用が可能
- ❖Embedded OSもサポート対象

ホワイトリストによるセキュリティ
どんなファイルの実行を制御してくれるの？

**実行可能なファイルの『全て』をホワイトリストで管理できて
はじめてセキュリティを実装したと言えます**

実行可能なファイルって
.exeとか.dllファイルのことでしょ！？

ちょっと待った！

Windows環境ならバッチファイルとか
VBスクリプトとかも使うよね
.fonという拡張子のフォントファイルを
使うDuqeというマルウェアもあるんだ

拡張子だけの判断ではなく
実行可能な全てのファイルを
ホワイトリストで管理することが
重要なんだ

ホワイトリストによるセキュリティ

大事なファイルは勝手に変わらないように守ってくれるの？

ホワイトリストに登録されたファイルは
改ざん防止機能で守られていなければなりません

ホワイトリストに登録されると
セキュリティは万全ですよね！？

安心！安心！

とんでもない！

ホワイトリストに登録したファイルが
勝手に書き換えられないよう
保護してあげないと
大事なファイルが書き換えられたり
消去されてしまっていたりして
システムが壊れてしまうぞ！

改ざん防止機能が必須なんだ

ホワイトリストによるセキュリティ
ホワイトリストで守ったまま更新できるの？

ホワイトリストで保護したままプログラムの追加・変更・削除を可能とすることにより，業務継続と高いセキュリティとを両立できます

ホワイトリストで保護すると
プログラム追加・変更・削除の度に
ホワイトリストを作り直さなければ
ならないんでしょ！？

ちょっと面倒かも

McAfeeのホワイトリストは
ダイナミックホワイトリスティング！

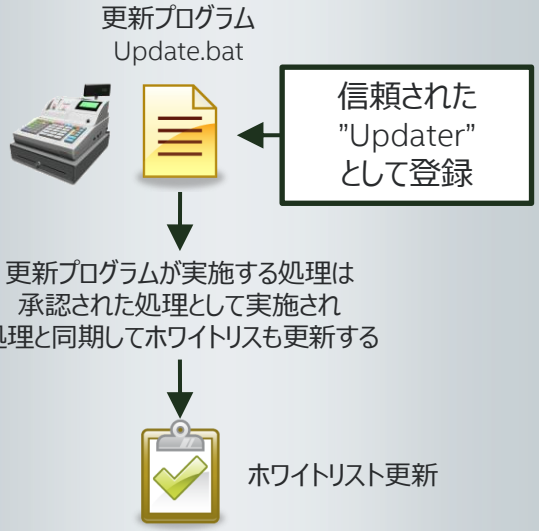
保護したままの状態でプログラムを
追加・変更・削除できるよ
だからセキュリティもバッチリ！

追加・変更・削除に合わせて
自動的にホワイトリストを
アップデートしてくれるので安心

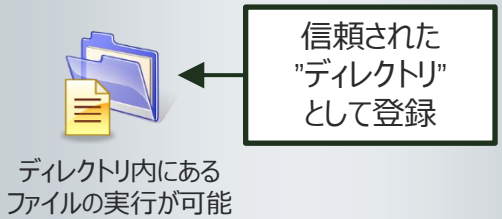
デバイス向けセキュリティ対策

ホワイトリスト型セキュリティ対策　アップデイト方法

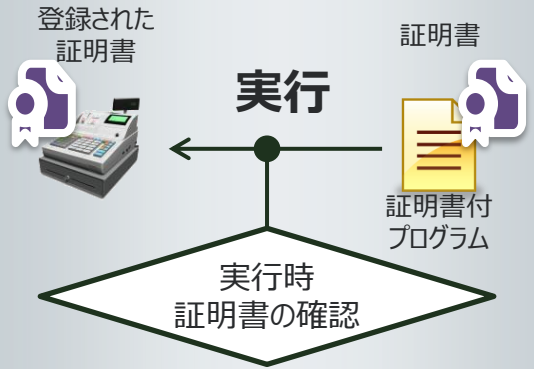
信頼されたアップデータ



信頼されたディレクトリ/ユーザ



信頼された証明書



管理者による会話型更新

ホワイトリストによるセキュリティ
システムの負荷は大きいの？

投資対効果を最大化するため
システム資源の消費は最小化されなければなりません

セキュリティソフトを導入すると
システムが重くなっちゃうじゃない？

できればインストールしたくないな

心配御無用！

McAfeeのホワイトリストはとっても
軽快に動作するんだ

CPU負荷は数%，メモリー使用量は
20MB前後とシステム負荷はとっても
小さくなっている

リソースの空きが少ない
システムへの導入も安心だね

ホワイトリスト方式でシステムを防御

McAfee® Embedded Control

アプリケーション・ホワイトリスティングによるセキュリティソリューション

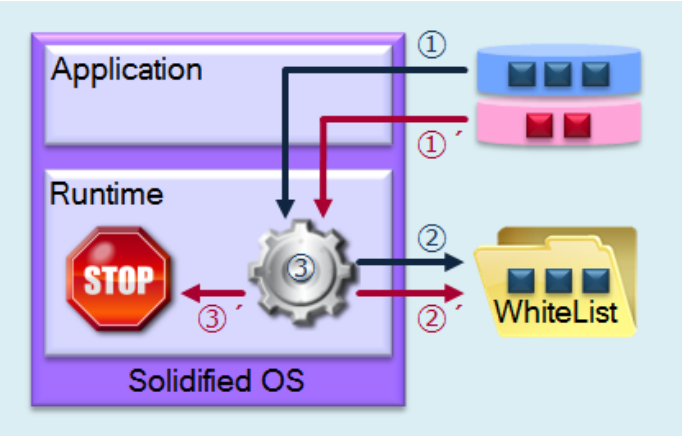
❖ホワイトリストに登録されたプログラムのみ動作を許可

- ▶ホワイトリストに登録されていない**プログラム，実行コード，スクリプトの実行**から防御
- ▶ホワイトリストに登録したプログラムは，**改ざん防止機能**により保護

32bit/64bitの双方の環境に対して**メモリー保護機能**も実装

国内で**300,000ライセンス以上の導入実績**

❖製造，医療，金融，流通など多くのインダストリで採用



デジタルサイネージでの導入事例

立教大学

セキュリティ上の課題

❖システムのリプレースに併せて，サイネージ装置のセキュリティとして導入

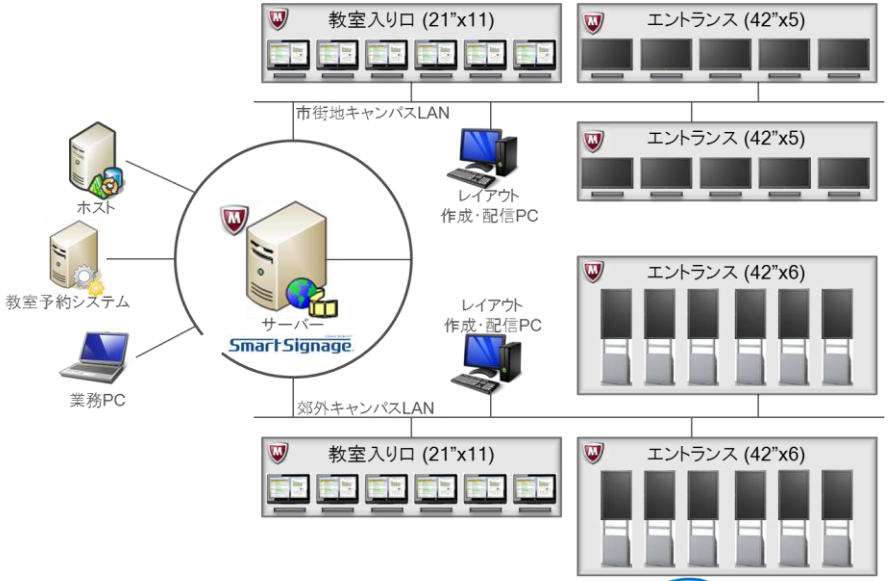
❖構内LANとの接続には，学内のセキュリティ・ポリシーを遵守しなければならない

求められるセキュリティ機能

❖稼働中のシステムで導入している，
アンチウィルス製品の運用制約を解決したい

❖セキュリティによるシステム負荷の低減

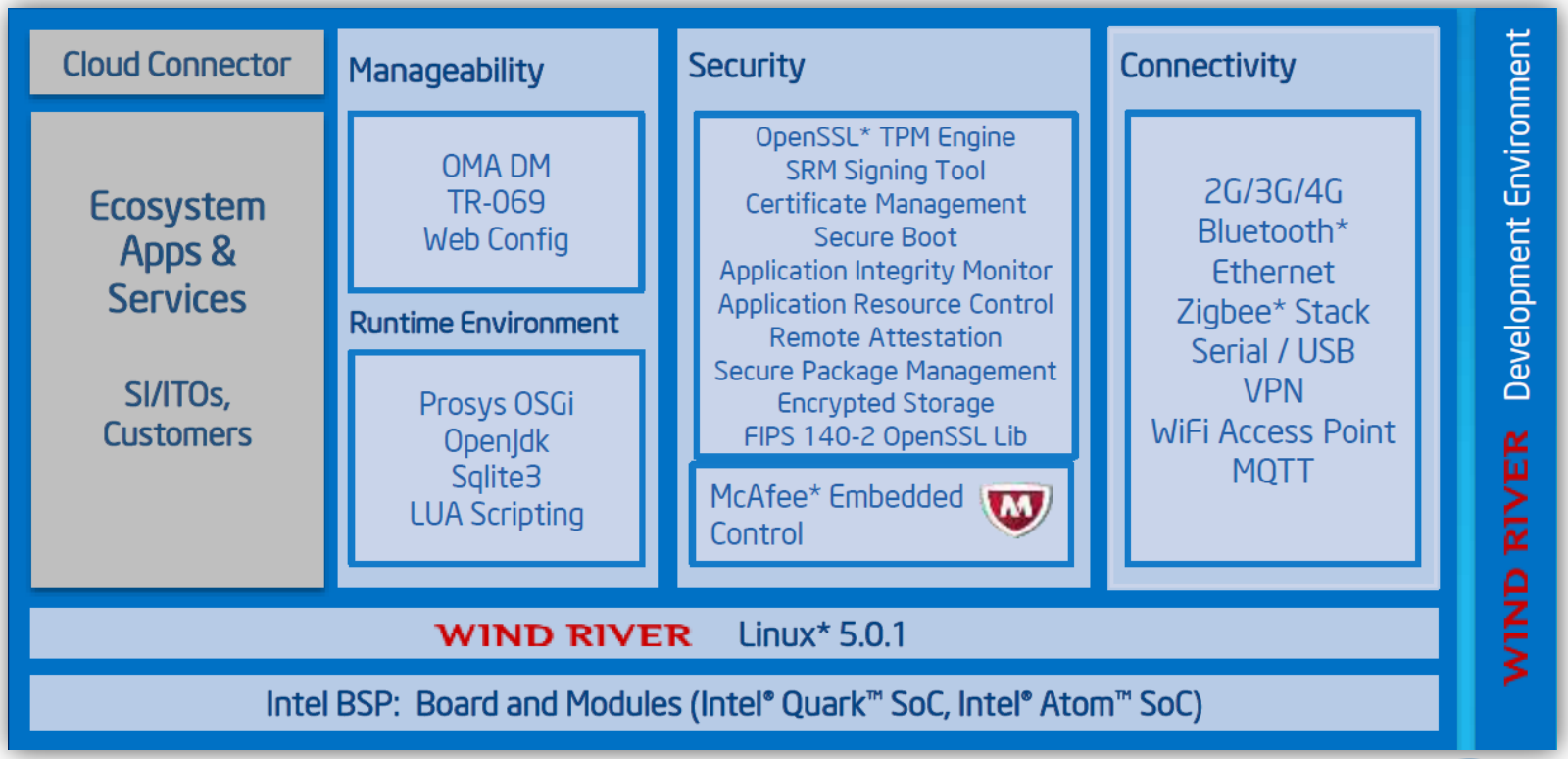
❖好奇心旺盛な学生によるディスプレイ
制御PCの操作から守りたい



IoT時代のSecurity
McAfeeだったらどう守れるのか

IoT Deviceのセキュリティ = IoT Gateway

McAfee® Embedded Control



McAfeeが実現するIoT時代のSecurity

End-to-Endでの状況認識とリアルタイム管理

Cloud / Data Center

Server

- サーバーセキュリティ
  Virus Scan Enterprise
  Application Control
  MOVE
  Host IPS
- セキュリティ状況認識
  SIEM
- 統合管理
  ePolicy Orchestrator

Communication

Network Infrastructure

- IPS/IDS
  Network Security
  Platform
- 次世代ファイアウォール
  Next Generation Firewall
- 次世代サンドボックス
  Advanced thread
  Defense

Edge Device

Gateway

- アプリケーション
  ホワイトリスト
  Embedded Control
- GTI連携
  Trustedsource SDK
- 暗号化
  Encryption

Sensor
Actuator

ご清聴ありがとうございました