資料２－３

日本スマートフォンセキュリティフォーラム ご紹介

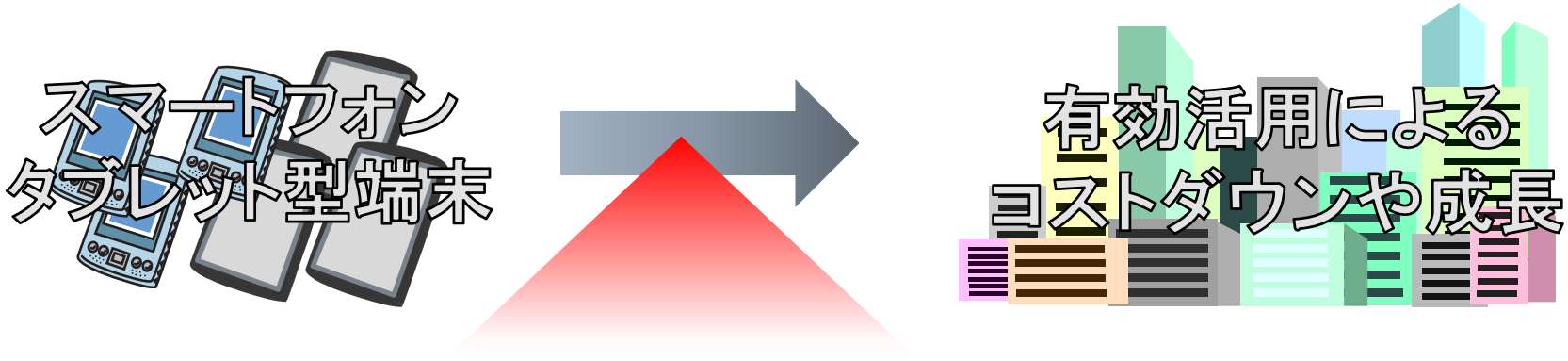
2011年11月4日

JAPAN SMARTPHONE SECURITY FORUM

http://www.jssec.org/

セキュリティを担保した運用の確保

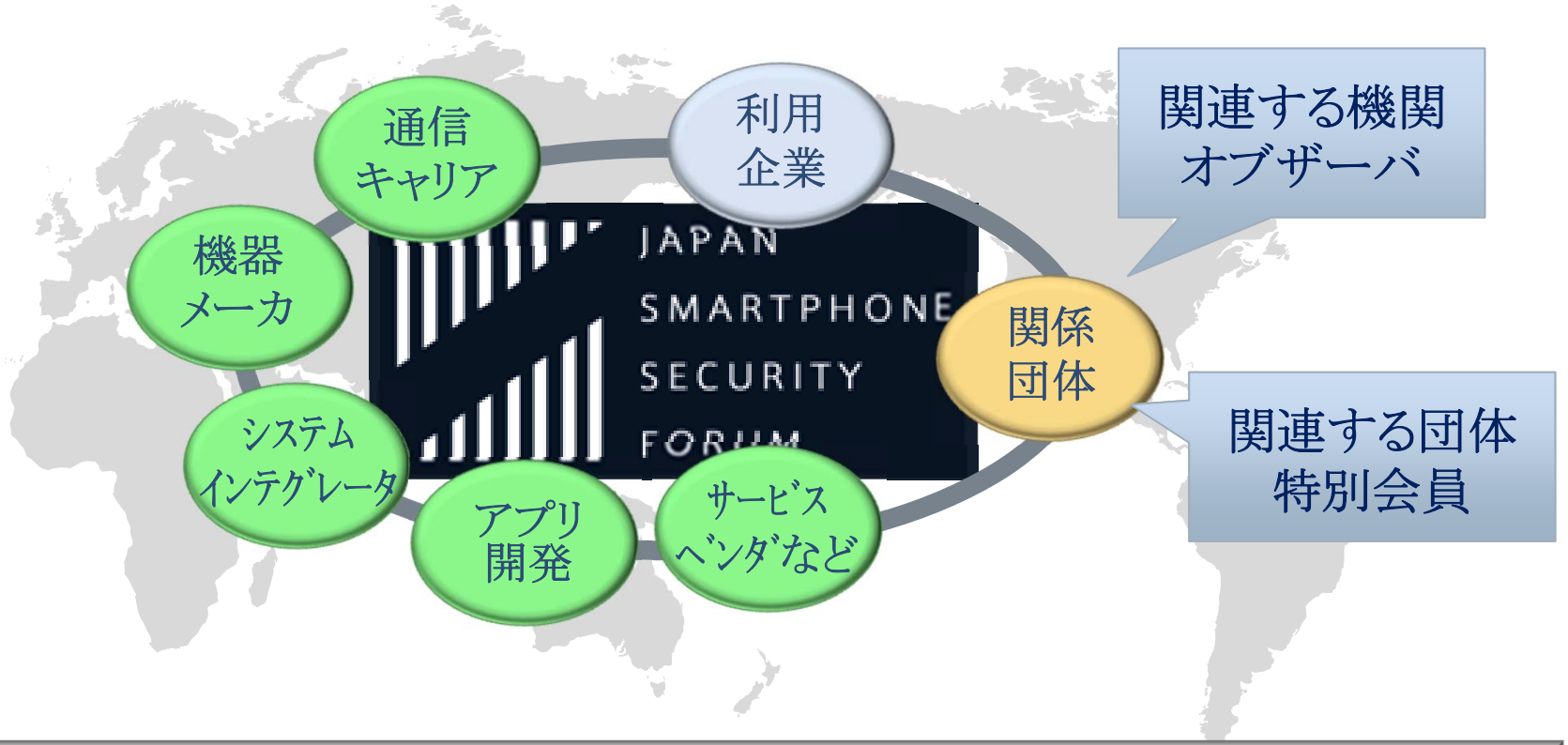
個人を中心に急激に普及するスマートフォンやタブレット型端末。（以降スマートフォン）企業や団体でも、業務効率化・生産性向上、ならびに新しい事業基盤の中核ツールとして、大きく期待されています。



ところが、不適切な利用やセキュリティ上の不備、悪意ある行為などにより利用者・事業者へ悪影響などを警戒するあまり、成長の機会を逸する危険性

解決には、業界を横断した協調が必要

急激に普及するスマートフォンの安全な利活用を図るため、関連する様々な分野の企業や団体が協調して取り組むことが重要



日本スマートフォン セキュリティ フォーラム（JSSEC）

目的・活動内容

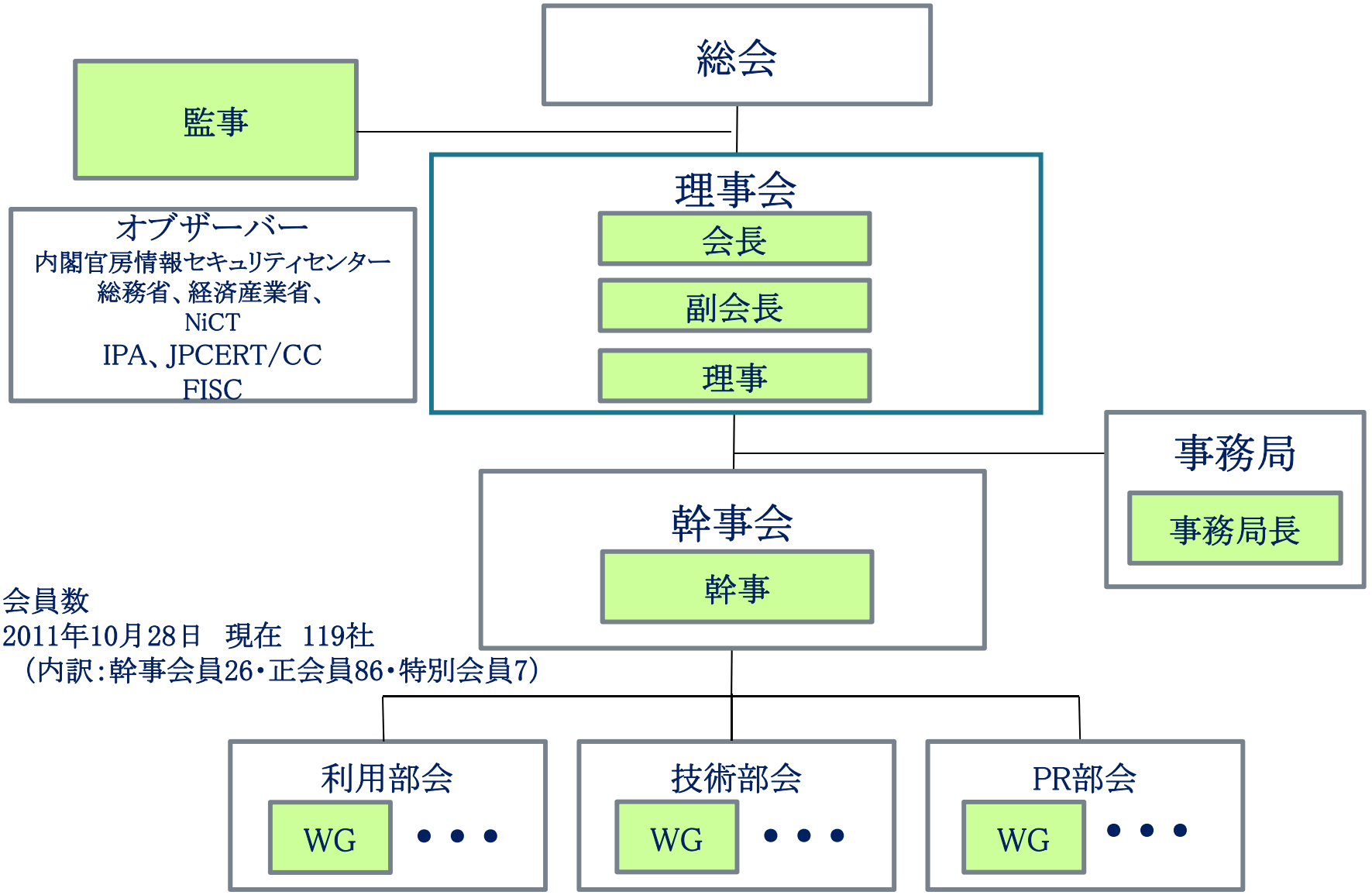
目的

1. 企業・団体における利用者が安心して高度なサービスを受けられるようにする。
2. 実装すべきセキュリティレベルの理解を社会に浸透させ、提供者が安心して事業推進を行えるようにする。
3. 利用者のセキュリティリテラシー向上のための活動も行い、さらに高度なサービスを受けられるようにする。
4. セキュリティを切り口とした「信頼できるニッポン！」を確立しグローバル市場へアピールする。

活動内容

参加メンバー間で、スマートフォンに関するセキュリティ上の課題を共有するとともに、解決策を検討、その結果および成果物を公開し、関係者の成長に寄与します。

体制



会員数
2011年10月28日　現在　119社
（内訳：幹事会員26・正会員86・特別会員7）

利用部会

目的:
スマートフォンの安全利用促進のための『事実』に基づいた情報の収集と、その共有のための情報発信を目的とする。

ワーキンググループ	目的	活動内容	成果物
利用ガイドライン WG	スマートフォンの利用状況に沿った安全利用のためのガイドラインを策定	・法人がスマートフォンを業務利用する際に必要なセキュリティガイドラインを策定する。 ・事例体系化を経て整理された事実に基づき、ユーザの利用シーンに合わせたガイドラインとする。 ・ガイドラインは、概要に加え、事例体系化から得た分析結果を踏まえて広い用途で実践的に利用できるものをめざす。	ガイドラインの作成 (8月にβ版、10月に第1版を発表)
利用シチュエーションと要求セキュリティの体系化WG	スマートフォンの利用状況についての体系化の検討	スマートフォン利用者の分類とその検討を行う。	「エンタープライズデプロイメントガイドブック(仮)」を執筆中 ・実際にスマートフォン導入を実施する際のガイド ・デプロイメントする際のセキュリティ体系の網羅～導入の仕方までを解説 (初版はビジネス市場占有率の高いiOSをターゲット)
事例研究WG	導入事例についての調査・研究を実施	・利用ガイドラインWG、及び体系化WGの成果を現実と比較確認のための事例の収集 ・参加企業から紹介のあった導入事例を事例講座として適宜紹介	情報交換を目的に「事例研究会」を開催 ・第1回:国内BYOD事例紹介 ・第2回:JPCERT/CCとの意見交換会

パブリックリレーションズ部会

目的:
JSSECで行われている活動を知って頂くための情報配信を行う。

年間計画(概要):

2011年6月～8月	部会内の各WGの活動ルールの確立
2011年8月～10月	年間イベントの確定、メディア対応/情報配信の開始
2011年10月～12月	イベントの実行、メディア対応/情報配信の継続
2011年12月～2012年3月	イベント実行/メディア対応/情報配信の継続、他団体コラボ

ワーキンググループ	目的	活動内容	成果物
コミュニケーションWG	JSSECの各部会/WGからの情報をタイムリーに配信し情報の展開を通じてJSSECの活動を啓発していく。	公式ホームページからの情報配信 TwitterによるJSSECの活動に関する情報、スマートフォンやセキュリティーのニュース案内 FacebookによるJSSECの活動内容に関する情報配信	JSSEC公式ページ、Twitter、Facebookに残る情報およびその配信
イベントWG	JSSEC、及び各部会(利用部会、技術部会)の様々な活動を、各種イベントや関連団体との協調を通じて啓発していく。	成果発表会の企画/運営 ・シンポジウムの企画/運営	各イベントの開催および運営ノウハウの蓄積
メディアリレーションズWG	JSSECの様々な活動をメディアを通じて、広く広報し多くの企業や個人の参加を促し、JSSECの社会的地位の向上を目指す。	プレスリリースによるJSSECのイベントや成果物の案内 各報道機関、メディアからの依頼対応(取材、執筆、講演など)	各イベント、成果物のプレスリリース 取材、執筆、講演などによる情報展開 成果物の著作権管理

技術部会

目的：スマートフォンを安全に利用するための技術的な調査・研究・議論を行う。

ワーキング グループ	目的	活動内容
脆弱性WG	主に、スマートフォンにおける脆弱性について情報収集、情報提供を通してスマートフォン利用の安全・安心に寄与する。	スマートフォン全般における「脆弱性情報」を収集・分析し、 JSSEC参加企業に周知することにより自主改修を促進する。 Google社、Adobe社、JSSECに参加していない企業に対しては、IPAを通じて周知する予定。また、JSSEC会員企業向けに、脆弱性チェックツールの提供も計画中。
アプリケーションWG	アプリケーションに関するセキュリティ側面の情報収集、対策検討、情報提供等を通じて、スマートフォン利用の安全・安心に寄与する。	スマートフォンのアプリケーションに関する諸問題について議論し、成果物として一般に提供することを目的としており、現在、「マルウエア」、「マーケット運用」、「アプリケーションの攻撃性検査」、「情報収集モジュール」、「セキュアコーディング」といった、スマートフォンにおけるアプリケーションの作成から配布に至る広範囲な問題について、それぞれタスクフォース化し活発な議論が行われている。
デバイスWG	主に、デバイス（端末）に関するセキュリティ側面の情報収集、対策検討、情報提供等を通じて、スマートフォン利用の安全・安心に寄与する。	スマートフォンの、主にデバイスに即した諸問題について議論し成果物として一般に提供することを目的としており、現在、「デバイスの堅牢化」及び「MDM」といったデバイス側からのセキュリティについてタスクフォースを作成し活発な議論が行われている。
ネットワークWG	主に、ネットワークに関するセキュリティ側面の情報収集、対策検討、情報提供等を通じて、スマートフォン利用の安全・安心に寄与する。	スマートフォンのネットワーク観点から、セキュリティ課題の検討を行い、実装するうえで有効となる情報をまとめ提供する。 現在「スマートフォンに関するネットワーク認証」及び「スマートフォン監視」について、活動課題としている。また、新しいタスクフォースとして「クラウド」についてのタスクフォースを計画している。

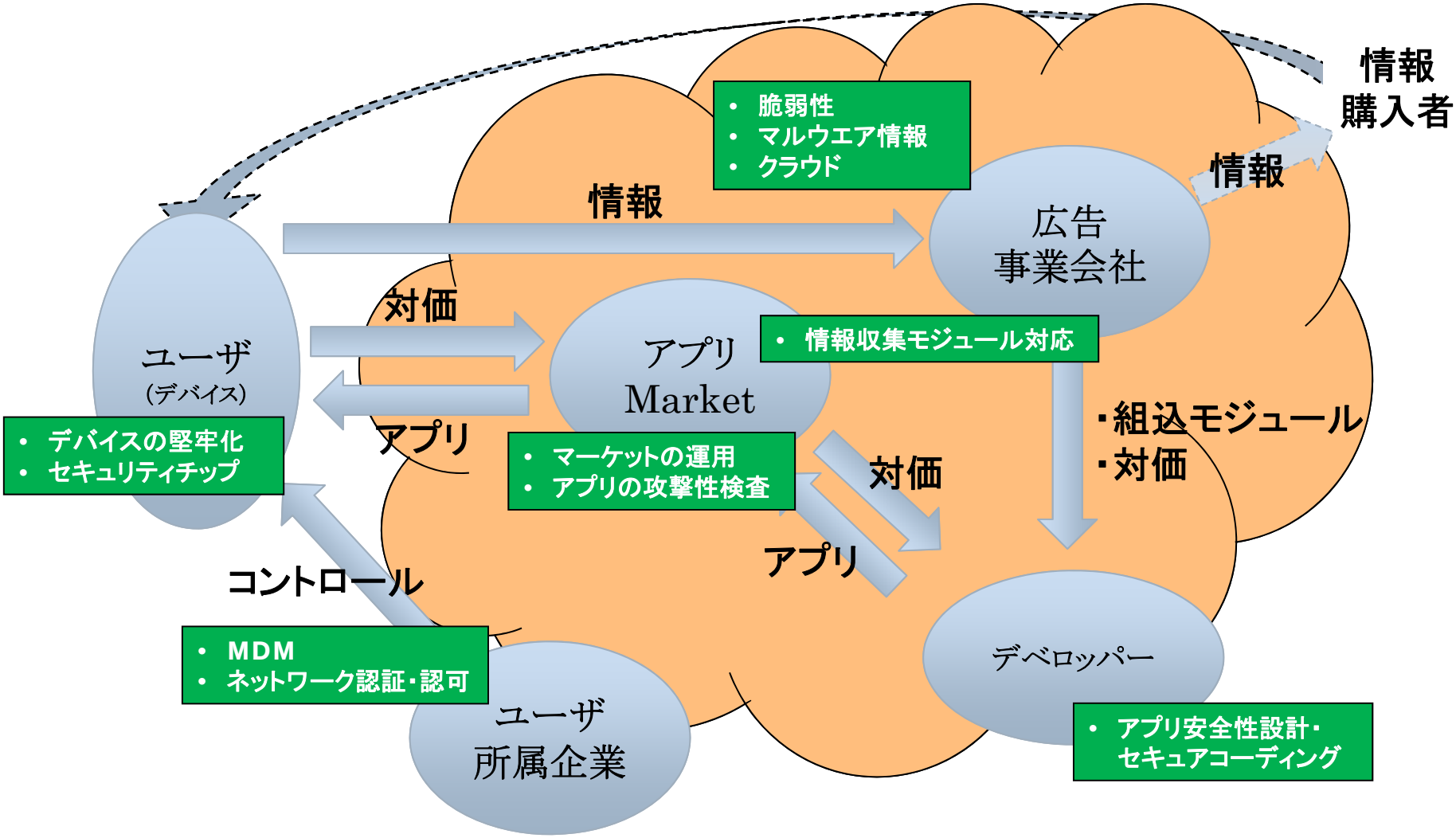
技術部会WG/TF一覧

脆弱性					
タスクフォース	ステータス	概要	成果物	予定	備考
脆弱性情報	Running	スマートフォン脆弱性情報の収集分析	JSSEC内企業への展開、及びIPAとの連携	2011/11（中旬～下旬）	
脆弱性検査アプリ	Pending	Android用脆弱性検査アプリの作成と公開	脆弱性検査アプリの提供	未定	
ネットワーク					
タスクフォース	ステータス	概要	成果物	予定	備考
ネットワーク	Running	端末認証・サービス（アプリケーション）認証として堅牢な認証方法を技術仕様書としてまとめる	スマートフォンセキュリティ実装ガイド（認証・認可編）	2011/12(アルファ版)	
セキュリティチップ	Planning	セキュリティーチップによるデバイスの紛失・盗難・置忘れの防止、第三者による不正利用防止の有効性と認証方法について検討する	・有効性についての報告書 ・認証方法に関する技術仕様書	未定	
クラウド（新）	Planning	スマートフォントとの通信が発生するインターネット上のサーバを対象とした各種セキュリティ調査および予測とガイドラインの作成	クラウド事業者向けガイドライン	2012/03末（ベータ版）	
アプリケーション					
タスクフォース	ステータス	概要	成果物	予定	備考
マルウエア	Running	・スマートフォン用マルウエア情報の提供 ・マルウエア対策アプリケーション選定ガイドラインの作成	・マルウエア情報の提供	未定	
	Planning	・セキュリティ対策サービス選定ガイドラインの作成	・セキュリティ対策サービス選定ガイドライン	未定	プラン作成中

技術部会WG/TF一覧

アプリケーション					
タスクフォース	ステータス	概要	成果物	予定	備考
Marketの運用	Running	独自マーケットの立ち上げを検討する企業に対して、選択するソフトウエアのセキュリティを担保するような形にするための、マーケット運用などに関する議論	マーケット運用ガイドライン	2011/12（ベータ版）	・ITU-T ・ユーザに適したアプリを提供する便利で安全・安心なMarketの認定制度を検討
アプリ攻撃性検査	Running	アプリケーションの安全性チェックに関する指針の策定	アプリの安全性を評価するチェックポイントのガイドライン	2011/12（ベータ版）	ガイドラインについては、Marketの運用でも使用（アプリの選定）
情報収集モジュールへの対応	Running	スマートフォンアプリにおける広告モジュール等をはじめとした情報収集モジュールに関する課題を整理して対応策を検討する	・実態調査報書 ・情報収集のあり方について指針	2011/12（ベータ版）	
アプリ安全設計・セキュアコーディング	Planning	スマートフォンアプリケーションの安全設計・セキュアコーディングに関する調査とまとめ	・Androidアプリのセキュア設計 ・セキュアコーディングガイド	未定	
デバイス					
タスクフォース	ステータス	概要	成果物	予定	備考
デバイスの堅牢化	Running	・MDMが搭載された端末を、デバイス自身の堅牢化で保護する ・ガラパゴス化しない程度で、効果の高い堅牢化について、ガイドラインの策定について検討する	端末堅牢化に関する指針	未定	
MDM	Running	・スマートデバイスのあるべき基本セキュリティ機能要件／仕様の策定 ・上記のサブセットとして、遠隔制御・管理を主な役割とするMDMについて、企業がMDM製品を選定・利用する際のガイドを策定	・スマートデバイスの基本セキュリティ設計 ・導入ガイド（仮） ・MDM利用ガイド（案）	未定	

WG/TFの位置



情報収集モジュール

- 広告事業者は、行動ターゲッティング広告、その他への利用目的等でユーザのスマートフォンから情報を収集する
- 情報を収集するためのモジュールは、デベロッパーなどに配布され、アプリケーションに組み込まれる
  - 利用に際して、デベロッパーには対価が支払われるため、ユーザに対して無償でのアプリケーション提供が可能となる等の利点がある
- 適切に運用されている情報収集モジュール
  - ユーザに対して、収集する情報の種類と取得する旨を開示し、ユーザから同意を得る
  - 収集された情報が適切に管理されている
  - 業界による自主規制等もあり、それらに準拠している
    - 総務省 「配慮原則」（2010年5月）
    - 一般社団法人インターネット広告推進協議会（JIAA）
      「行動ターゲティング広告ガイドライン」（2010年6月）

アプリの流通経路

【Androidアプリケーション配布におけるマーケットの重要性】

- Androidアプリケーションのほとんどは、アプリケーションマーケットを介して提供される
- Androidでは、Googleのマーケットとそれ以外の独自マーケットが存在する
  - docomoマーケット
  - au one マーケット
  - その他参入希望あり
- 独自マーケットにおいて、アプリケーションを取り扱う際に、安全な物のみを扱うことで、セキュリティが確保できるのでは？
  - アプリケーションに組み込まれている情報集数モジュールは適切な業者のものであるか
  - アプリケーションの攻撃性
    - アプリケーションの説明とパーミッションに食い違いはないか
  - デベロッパーの素性の確認
  - その他

マーケット認定基準

アプリケーション開発から配布（販売）、ユーザからの情報収集に関する部分で安全性確保が必要ではないのか？

- ひとつの案として、「独自マーケット」に対する認定基準を設ける
  - 常識的な一定の基準を示し、それを満たしたマーケットを「認定マーケット」とする
    - ここからダウンロードすれば、安全なアプリケーションであると言う、ユーザに対する指標
  - **JSSEC**として「マーケット運用ガイドライン」を作成
    - 開発元の確認 - 配信（販売）するアプリケーションの開発元責任を確認するため。匿名や出元が不明な物を安易に拡散しないため
    - アプリケーションの挙動に悪意がない – アプリの攻撃性検査にて議論
    - 安全な課金システムの使用
    - 著作権の適正な管理
  - 管理する、運用代行する、保障する、運用に責任を負うものなどではない