経済産業省
Ministry of Economy, Trade and Industry

スマートフォン時代の
リスクハンドリングの課題について

経　済　産　業　省
商 務 情 報 政 策 局
情報セキュリティ政策室
室長補佐　守谷　学

0．イントロダクション

スマートフォンの登場で変わる ビジネス・ライフスタイル

いつでも、どこでもインターネット上の情報資源にアクセスできるスマートデバイスの登場は、ビジネススタイル、ライフスタイルを大きく変えた。

- **ビジネススタイル・・・**BYOD（Bring Your Own Device）、**ノマドワーク**
- **ライフスタイル・・・様々な出自の情報を縦横に組み合わせて利用する様々なアプリケーションの登場**
  （ウェブは見るものから活用するものへ）
  →特にパーソナル情報利用サービスの急拡大

各自がリスクを「評価」することが これまで以上に重要に

- データを「かくまって」いたら、教授できるサービスも最小
  →データを出して活用することが生み出す価値と、
  セキュリティリスクのトレードオフの中で

  ・どこまでのサービスを利用したいのか
  ・どこまでデータの機密性を確保したいのか

  を各企業・個人がしっかりと評価して、その判断の中でセキュリティリスクを最小化することが必要。

リスクハンドリングのために求められる政策対応

①インターネット上に置かれるデータ
→クラウドサービスのセキュリティ評価

②アプリケーション脆弱性のハンドリング

③不正アプリケーションのハンドリング

＜横断的課題＞
・官民連携による意識啓発の更なる展開
・国際的な制度調和・・・データは国境を越える

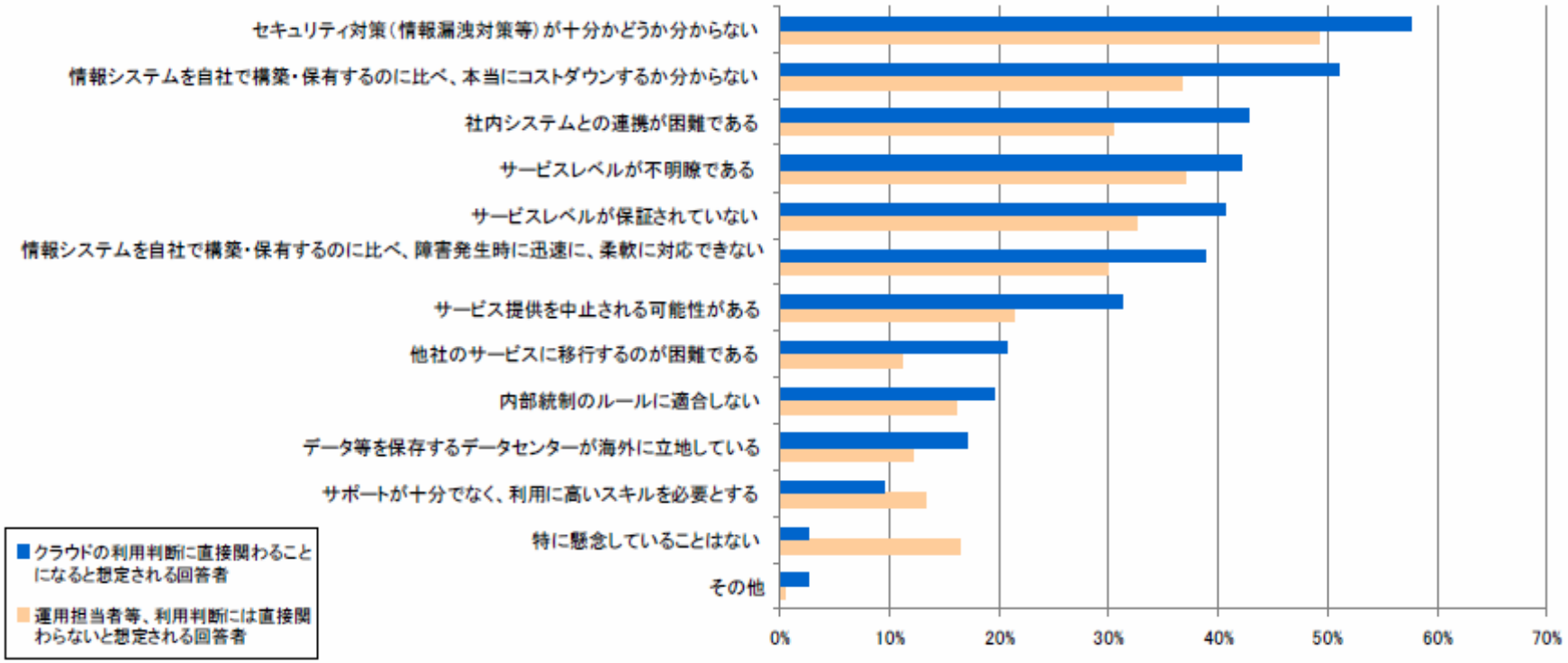
1. クラウドサービスのセキュリティ

クラウドサービス利用における懸念事項

経済産業省
Ministry of Economy, Trade and Industry

■Web アンケートにより500 人を対象に調査によると回答割合が最も高いのが，『セキュリティ対策（情報漏洩対策等）が十分かどうか分からない』であり，セキュリティに対する懸念については共通認識が形成されている

■情報セキュリティに関する情報を含め，クラウドサービスの利用を検討するために十分な情報がクラウド事業者から開示されていない状況



＊出典「高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会」（経済産業省2009年3月）

クラウドセキュリティガイドライン策定の背景

経済産業省
Ministry of Economy, Trade and Industry

クラウド利用者の不安

クラウド利用においてセキュリティ上の不安が払拭できていない

クラウド事業者への要求

クラウド利用者はクラウド事業者に、
情報セキュリティ監査及び
JIS Q 27001ベースのセキュリティ管理を
望んでいる。

「情報セキュリティ」および「事業者におけるシステム運用」が見えないことに関する不安を「見える化」する

クラウド利用者のための情報セキュリティマネジメントガイドラインの策定

- 利用者視点による セキュリティリスクの 共通認識の形成
- 事業者選択における 基準として利用できる 対策標準
- 情報セキュリティ監査による利用者と事業者の 信頼関係の構築

クラウド利用者のための情報セキュリティマネジメントガイドライン目次構成

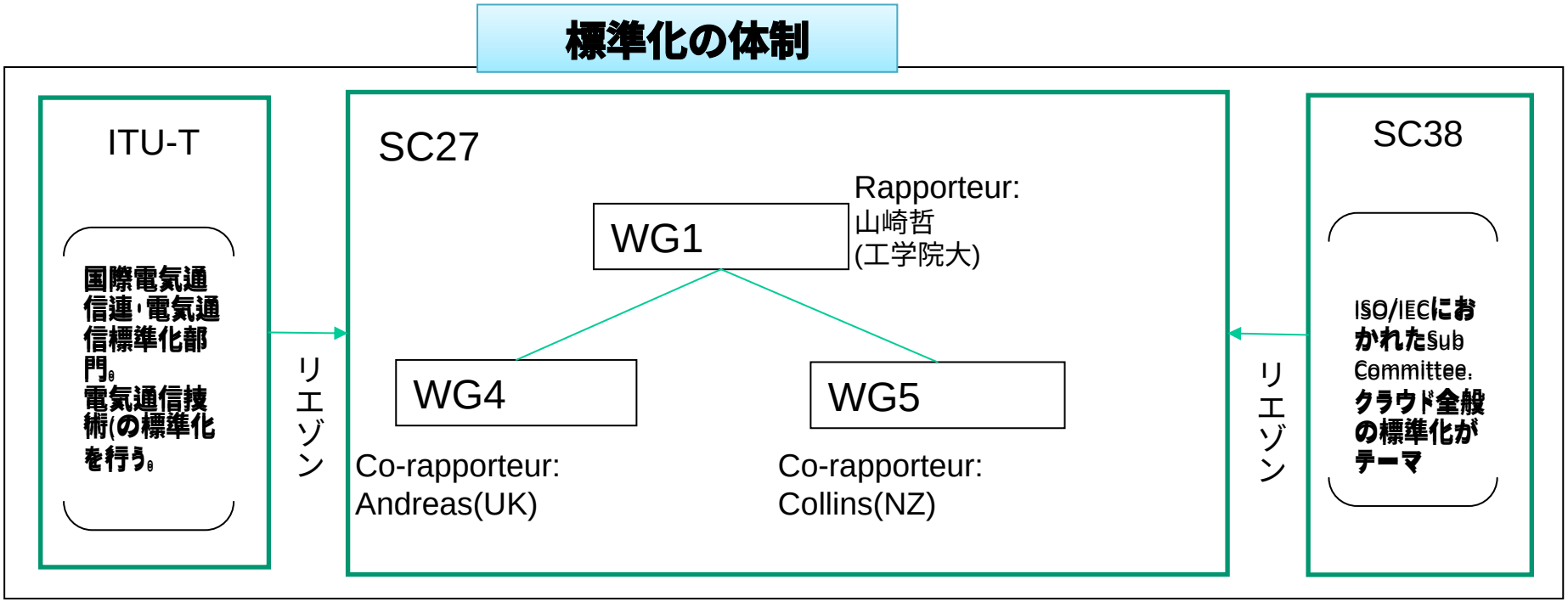
経済産業省
Ministry of Economy, Trade and Industry

•本ガイドラインの箇条5～15は，クラウド利用者がJIS Q 27002（実践のための規範）の箇条5～15の管理策を実施するための補足として活用できる。
•参考として附属書Aは，クラウドサービス利用に係るリスクを例示し，附属書Bは，クラウドサービス利用におけるリスクアセスメントの実施例の一つを示す。

国際標準化動向

経済産業省
Ministry of Economy, Trade and Industry

- 我が国として、国内ガイドラインをベースとした国際標準が策定されるよう、ISO／IECに提案を行い、現在、2014年度目途の国際標準策定に向け、議論が進められている。

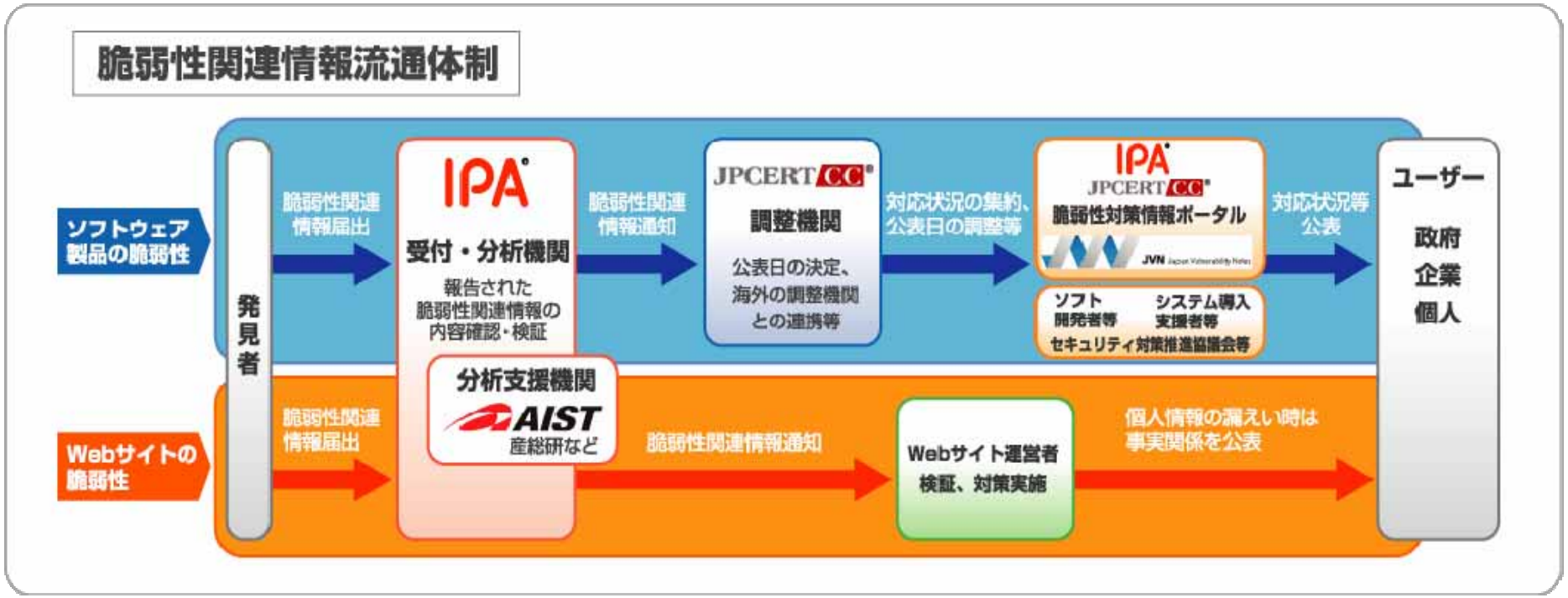


2．アプリケーション脆弱性のハンドリング

情報セキュリティ早期警戒パートナーシップ

経済産業省
Ministry of Economy, Trade and Industry

- 脆弱性情報、攻撃手法の収集･分析
- 脆弱性の軽減
- 脆弱性関連情報の届出受付･分析および脆弱性対策の普及促進
  - JPCERT/CC等関係機関/団体と連携、「情報セキュリティ早期警戒パートナーシップ」を運用（2004年7月8日～）
  - 脆弱性対策情報データベースJVN iPedia



スマートフォンの普及にともない、スマートフォン関連製品の届出がソフトウェア製品全体の3割前後にまで増加。

脆弱性対策情報DB「JVN iPedia」

経済産業省
Ministry of Economy, Trade and Industry

- 脆弱性対策情報を広く蓄積、公開。
- ２０１２年第3四半期までで累計３０，８４３件を公開（米国国立標準技術研究所の脆弱性データベース「ＮＶＤ」の情報を含む。）

スマートフォンの脆弱性対策情報

経済産業省
Ministry of Economy, Trade and Industry

JVN iPediaへの脆弱性対策情報登録件数は、Android系ソフトウェア（OSとアプリ）が2011年から2012年にかけて急増している（18件→95件）。

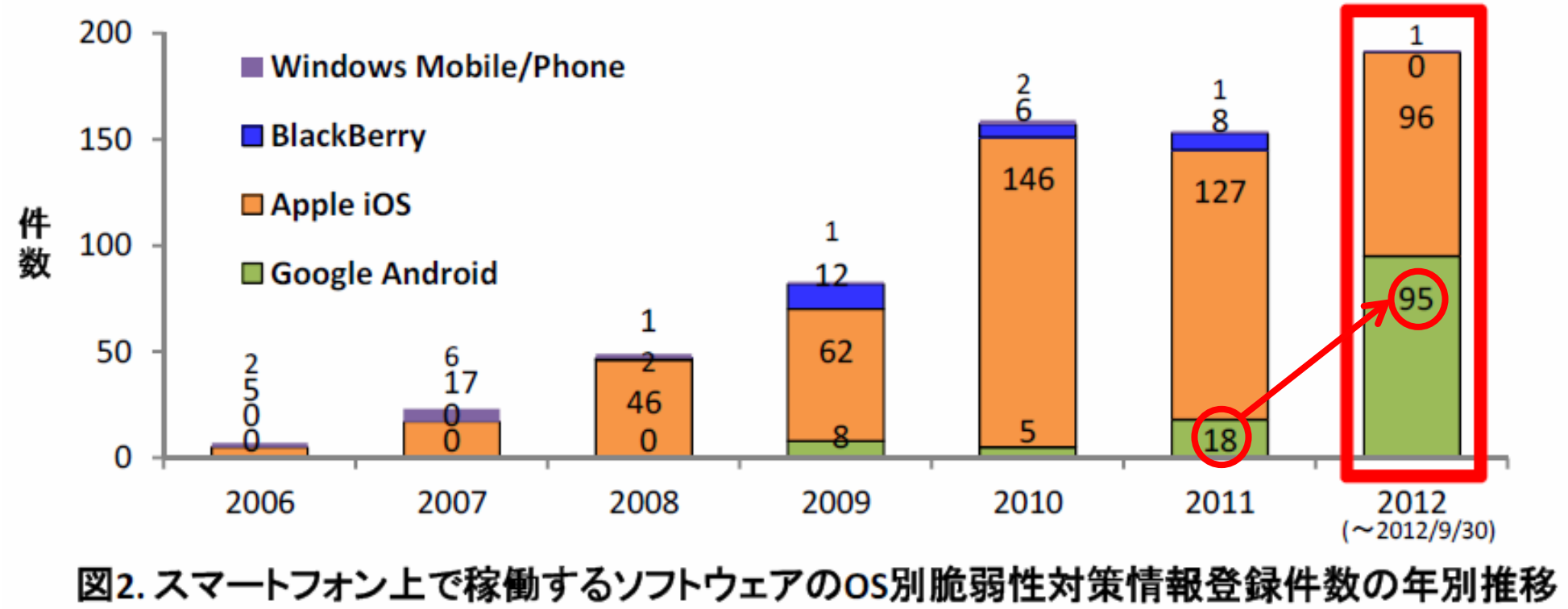


図2. スマートフォン上で稼働するソフトウェアのOS別脆弱性対策情報登録件数の年別推移

出典：独立行政法人情報処理推進機構（IPA）
脆弱性対策情報データベース JVN iPedia の登録状況［2012年第3四半期（7月～9月）］
（10月18日プレスリリース）

Android系スマートフォンの脆弱性対策情報

経済産業省
Ministry of Economy, Trade and Industry

Android系ソフトウェアでは、OSに比べアプリの脆弱性対策情報が2011年から2012年にかけて急増している（8件→90件）。

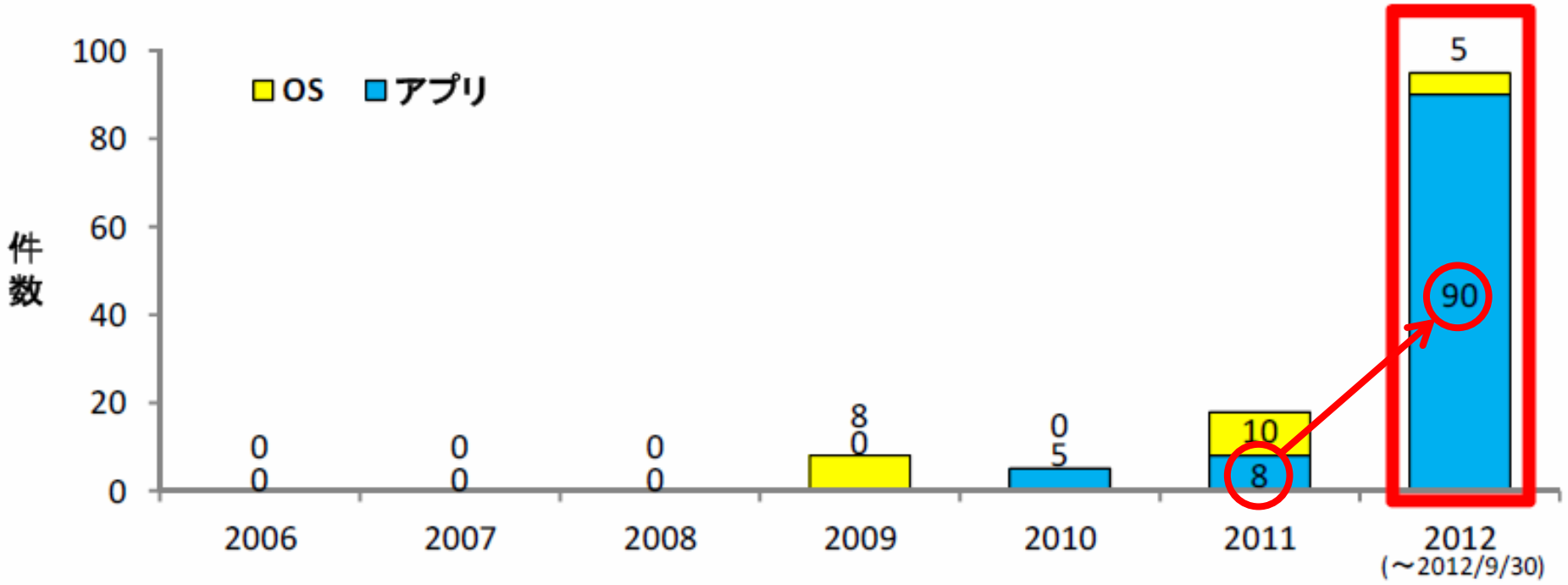


図3. Android OS系ソフトウェアの製品区分別脆弱性対策情報登録件数の年別推移

出典；独立行政法人情報処理推進機構（IPA）
脆弱性対策情報データベース JVN iPedia の登録状況［2012年第3四半期（7月～9月）］
（10月18日プレスリリース）

Android系アプリのカテゴリ別深刻度

経済産業省
Ministry of Economy, Trade and Industry

Android系アプリのカテゴリ別深刻度割合のうち、**ブラウザやメールなどの通信アプリ、ＳＮＳアプリが全体の５９％**を占めている。これらのアプリは個人情報を扱うものが多く、メッセージ内容、通信履歴、連絡先等の情報が漏えいする可能性あり。

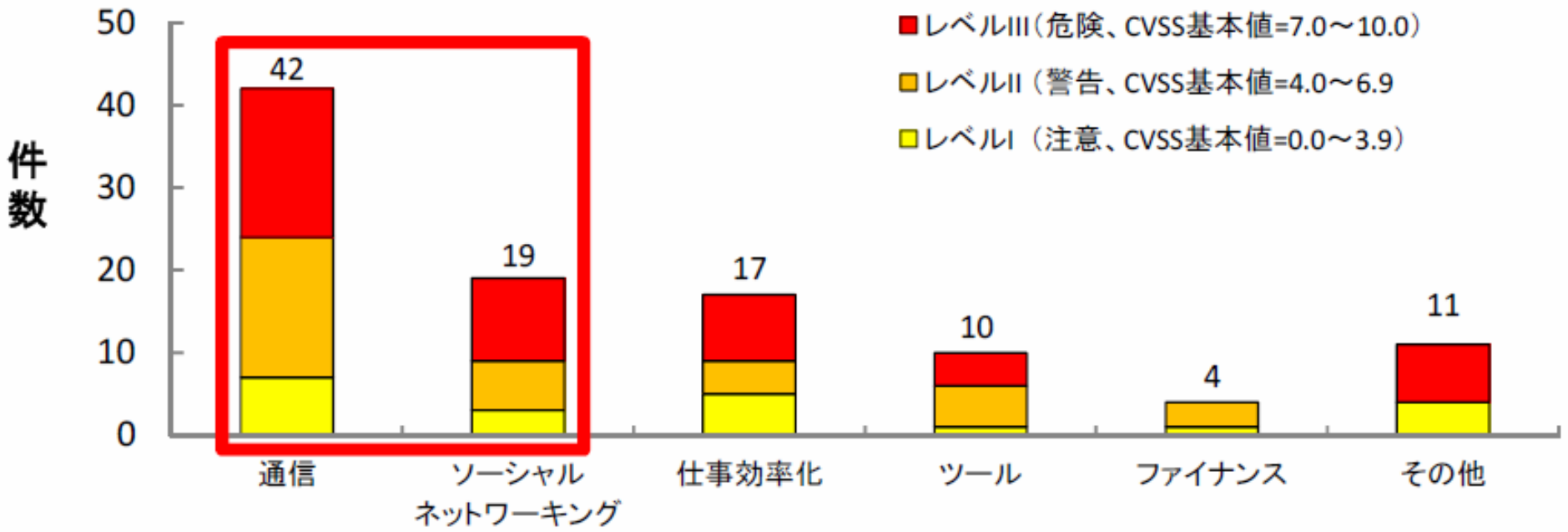


図4.Androidアプリのカテゴリ別深刻度割合

出典；独立行政法人情報処理推進機構（IPA）
脆弱性対策情報データベース JVN iPedia の登録状況［2012年第3四半期（7月～9月）］
（10月18日プレスリリース）

Androidアプリの脆弱性の傾向

経済産業省
Ministry of Economy, Trade and Industry

- ２０１２年5月末までにＩＰＡに届け出られたＡｎｄｒｏｉｄアプリは累計４２件。これらの脆弱性の傾向を分析すると、「アクセス制限の不備」に起因するものが多い。
- 届け出られた「アクセス制限の不備」の脆弱性は、ファイル作成時のアクセス許可の設定等のＡｎｄｒｏｉｄにおける基本的な設定の不備から生じている。
- Ａｎｄｒｏｉｄ特有の設定内容が開発者に周知できておらず、結果的に、アクセス制御の不備の脆弱性を作り込んでしまっているのではないかと推測される。

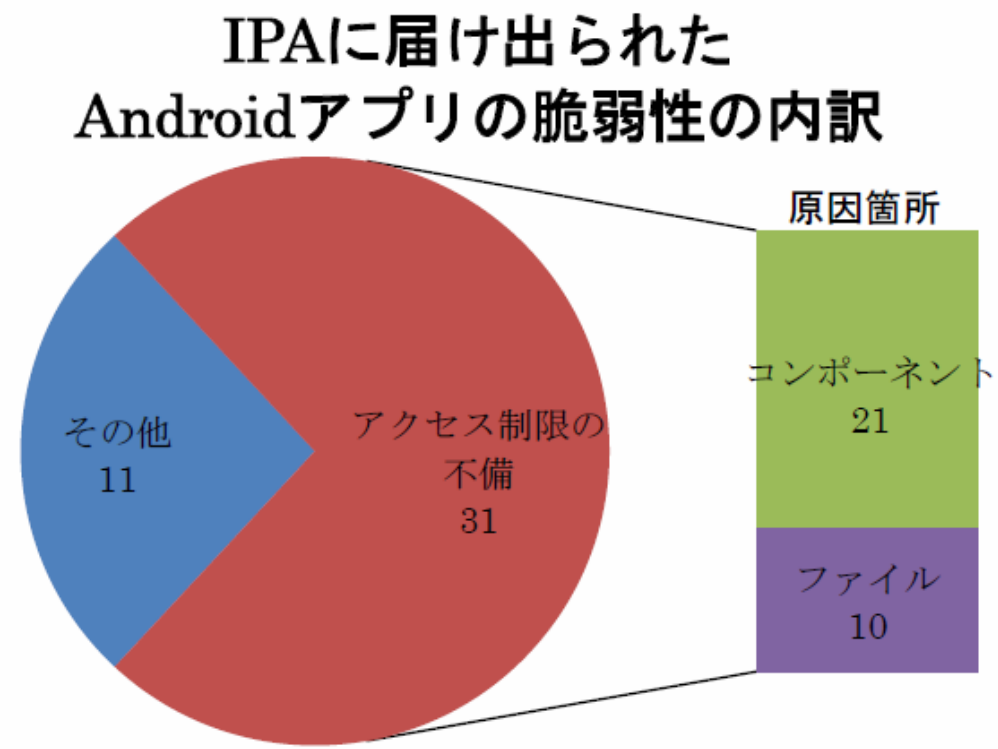


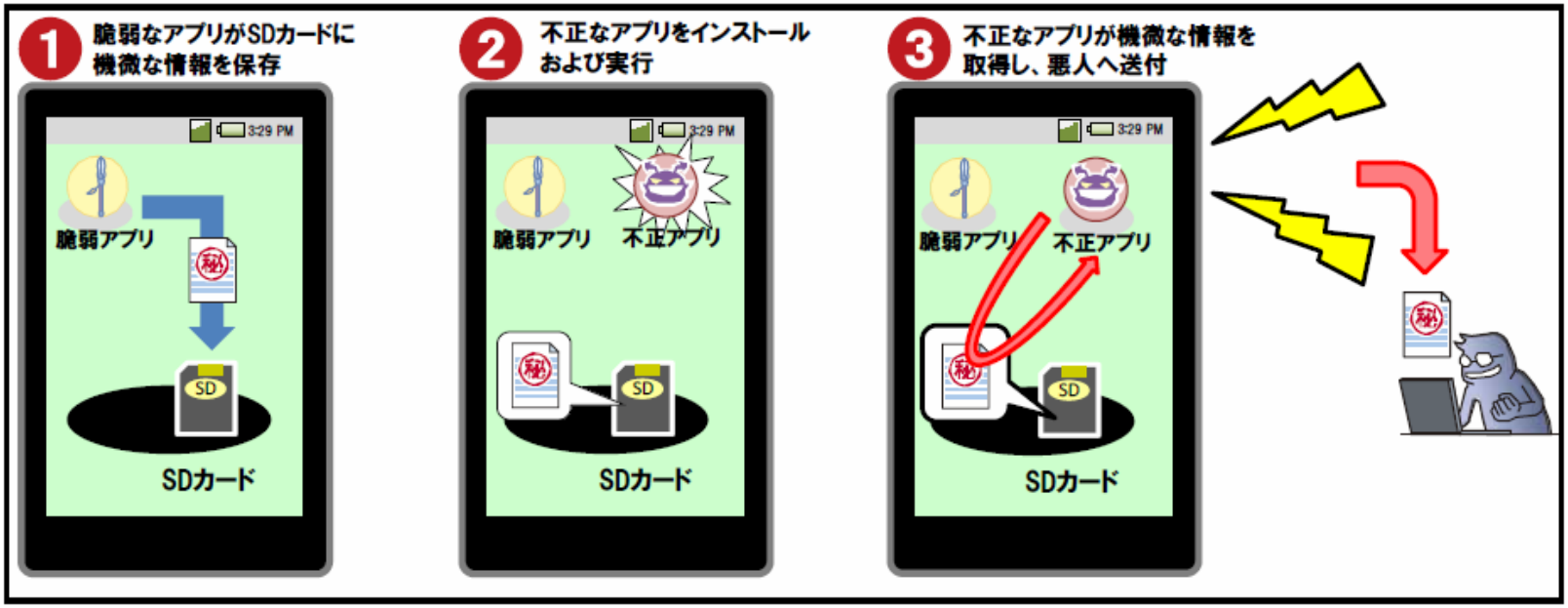
図 3-1 IPA に届け出られた Android アプリの脆弱性の内訳

出典；独立行政法人情報処理推進機構（IPA）
テクニカルウォッチ「Android アプリの脆弱性」に関するレポート

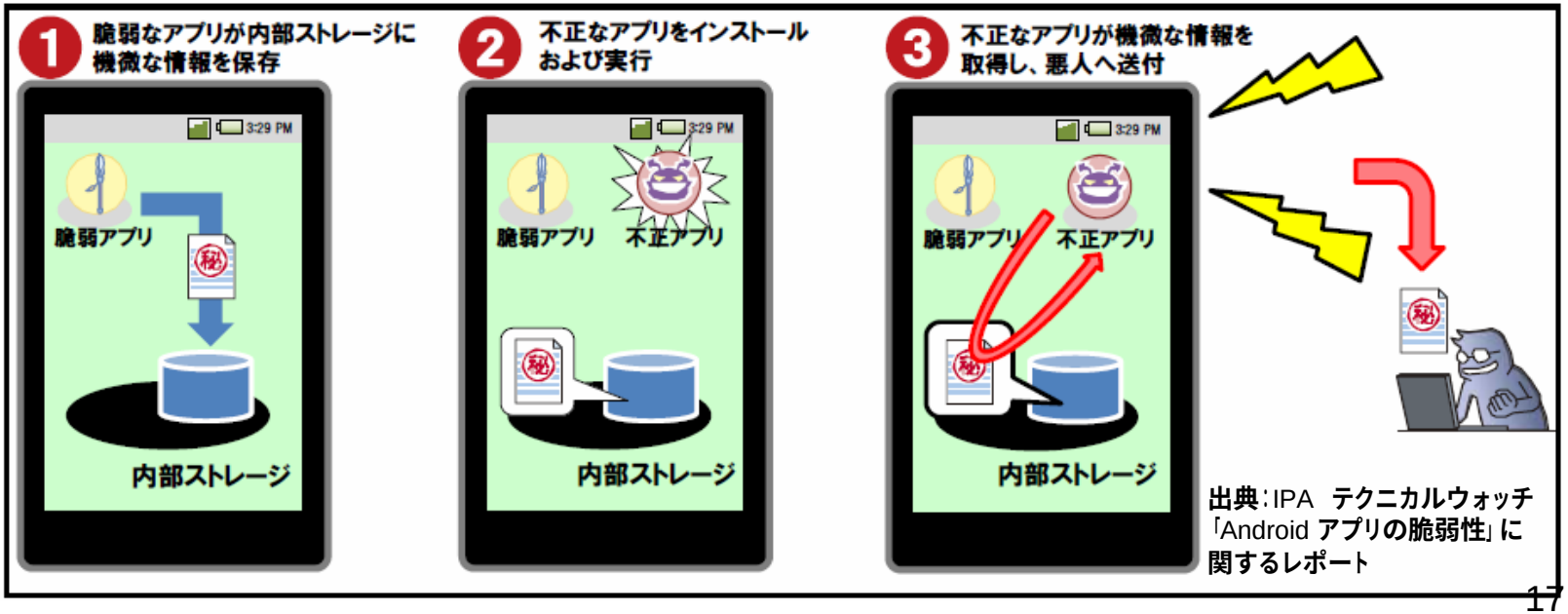
脆弱性例の紹介（1）

経済産業省
Ministry of Economy, Trade and Industry

①
ＳＤカードに機微な情報を保存



②
ファイルが不正なアプリからアクセス可能



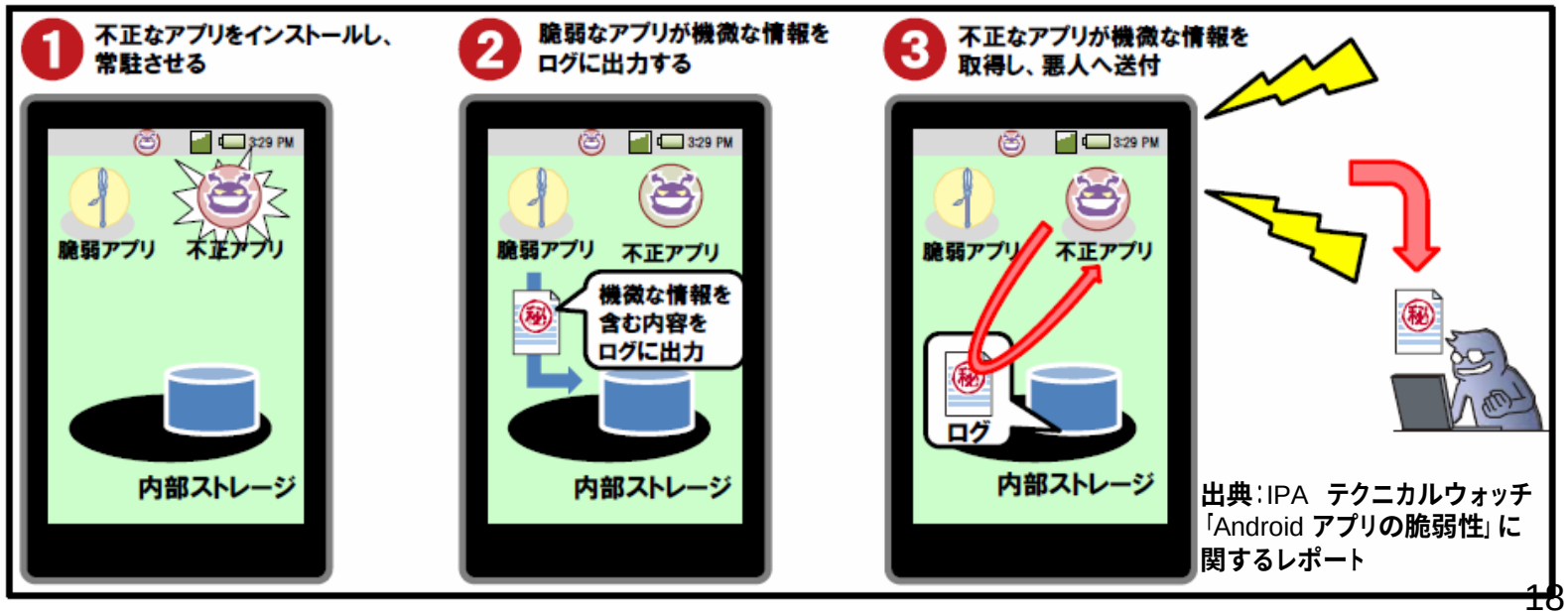
出典：IPA　テクニカルウォッチ「Android アプリの脆弱性」に関するレポート

脆弱性例の紹介（2）

経済産業省
Ministry of Economy, Trade and Industry

③
不正なアプリに機能を悪用される

④
機微な情報をログに出力する



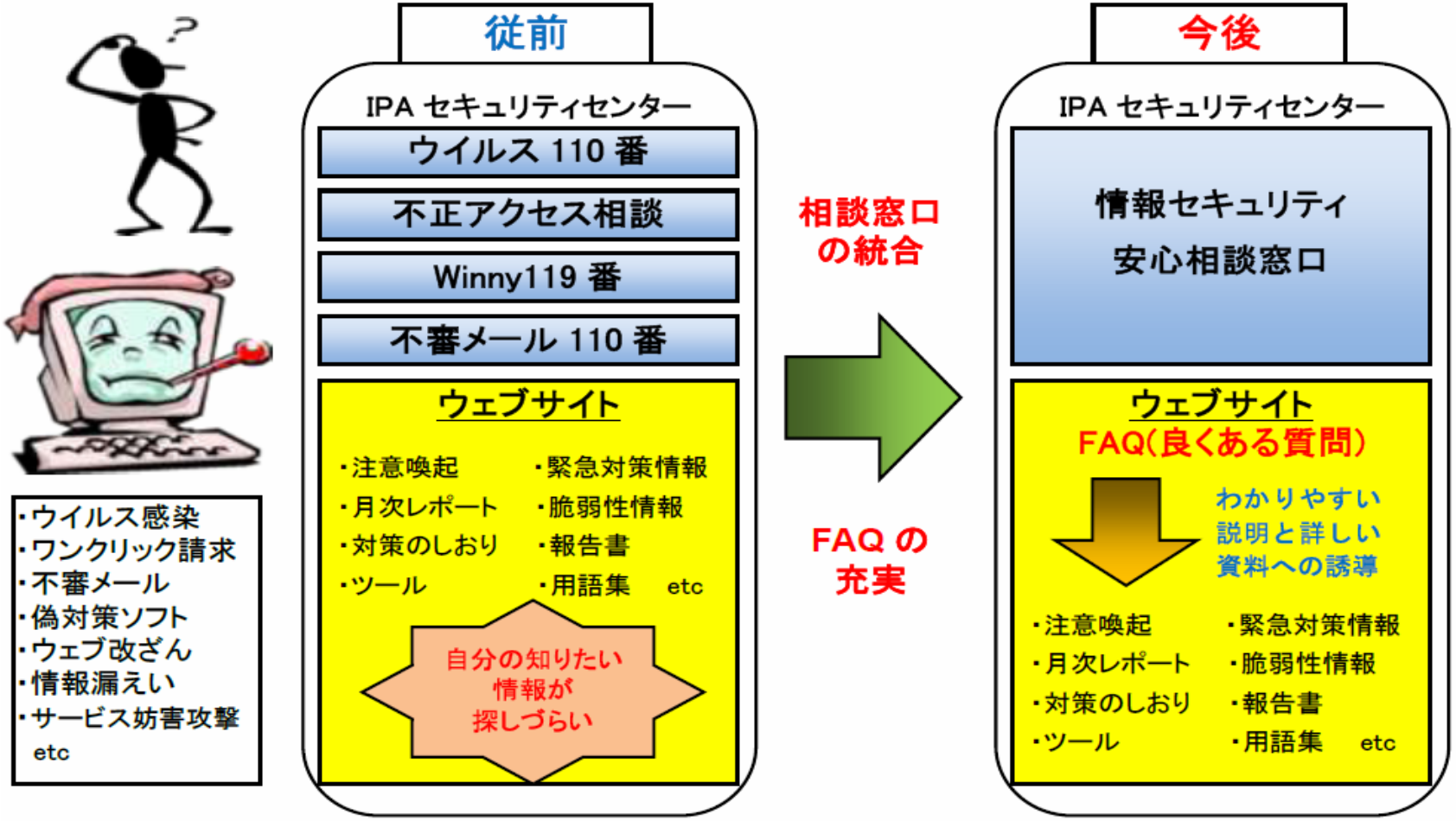
出典：IPA　テクニカルウォッチ「Android アプリの脆弱性」に関するレポート

3．不正アプリケーションのハンドリング

IPAに「情報セキュリティ安心相談窓口」を設置

経済産業省
Ministry of Economy, Trade and Industry

- 変化する相談内容に継続的に対応するとともに、相談窓口選択の必要を無くし、速やかに適切な情報を提供することを目的として、複数の相談窓口を一本化
- 時間外でも多くの問題を解決できるよう、ウェブサイトのFAQ（よくある質問と回答のリスト）を充実

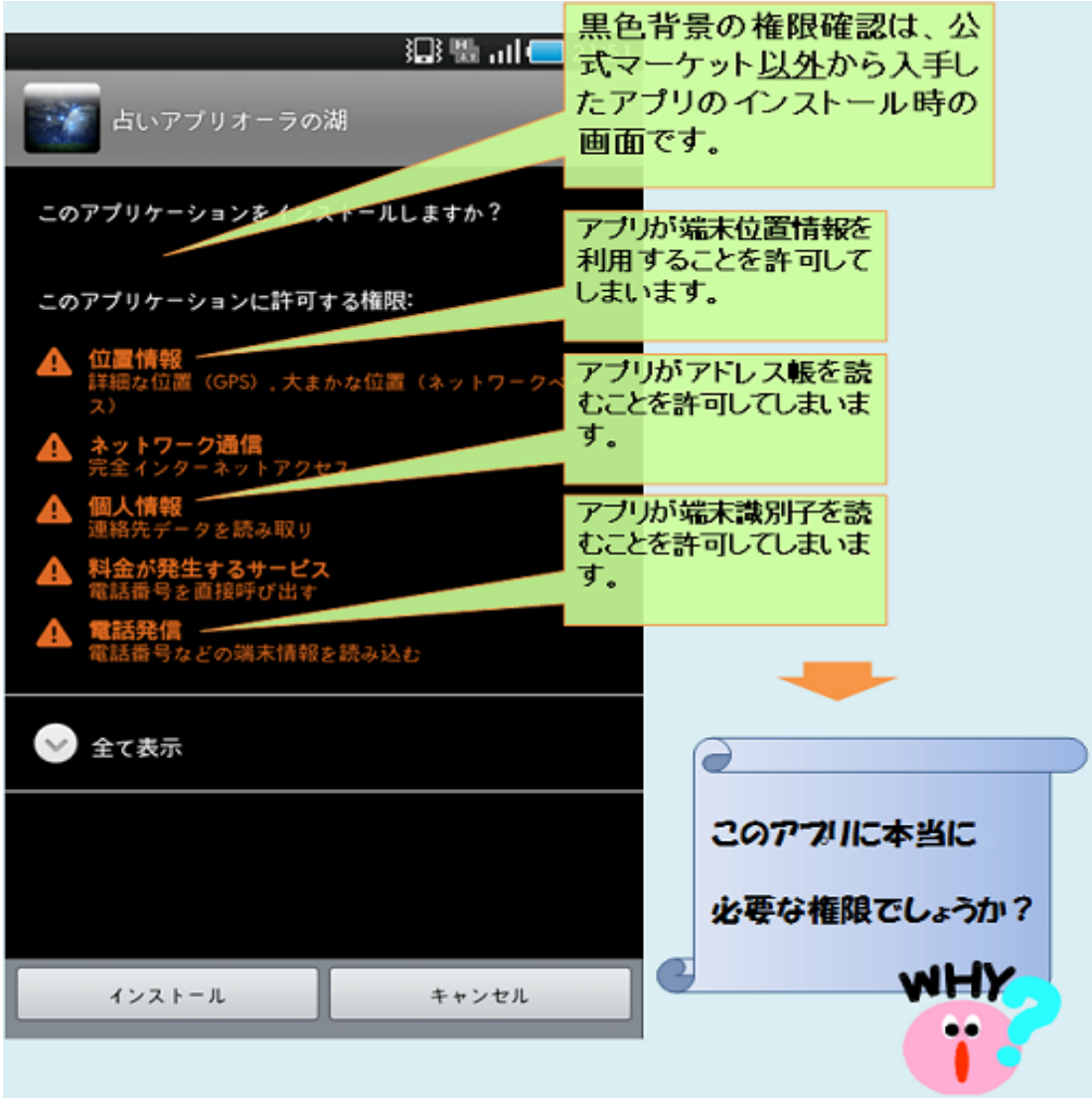


※2010年10月19日以降

公式外の場所に存在した不審アプリの事例（2012年5月）

経済産業省
Ministry of Economy, Trade and Industry

※Androidの事例



公式外の場所に存在した不審アプリの事例（2012年5月）

経済産業省
Ministry of Economy, Trade and Industry

※Androidの事例

アフィリエイトの仕組みを悪用し、ポイントサイトや個人ブログなどで広く紹介されていた！！

公式外の場所に存在した不審アプリの事例（2012年5月）

経済産業省 Ministry of Economy, Trade and Industry

※Androidの事例

SNSやメールで不正アプリサイトへ誘導する事例（2012年9月）

経済産業省
Ministry of Economy, Trade and Industry

Facebookの
某コミュニティに投稿されていた、不正アプリサイトへのリンクを含んだ投稿

SNSやメールで不正アプリサイトへ誘導する事例（2012年9月）

経済産業省 Ministry of Economy, Trade and Industry

※Androidの事例

Subject:スマホの電池切れを解消！便利アプリを紹介[APP マグ]
Date:2012/09/24 11:30
To:●●@i●.jp

今回はアプリを紹介します。

□ 電池バッテリー改善アプリ
---
http://●.net/●/◆◆.html

スマホの電池切れを解消する、画期的なアプリが出ました。
このアプリを入れるだけで、朝充電して帰宅まで充電が不要になりました。
有料版や無料版を数多く試してきましたが、
今のところこのアプリが「ベスト」です。
バージョンアップの期間中だけ、無料でダウンロードが可能です。
今すぐ試してみて下さい！

□ 安心スキャン
---
http://●.net/●/▼.html
一番最初に入れたいウイルス対策アプリ。
軽い動作と、常に最新のウイルス対策パターンをダウンロードします。
無料でさくっとスキャン出来るのは魅力的。
定期的に実行すれば安心ですね♪

* ==========* APPSマグ *
◆編集・発行：便利アプリを紹介！APPマグ
◇配信停止・配信先の変更 http://●.net/●/
◆Copyright(C) 2011-2012, APPSマグ
◇本メールマガジンの著作権はAPPSマグに帰属します。,
記事の無断転載は堅くお断りします

リンクをタッチすると、不正アプリが置かれているサイトに飛ばされる！

スマホ内から情報が送られている様子

経済産業省
Ministry of Economy, Trade and Industry

①：実際に悪意ある攻撃者に送られている情報

original:
test = 1%3A%E3%81%84%E3%81%B1 %E6%AC%A1%E9%83%8E%3A999-9999%3Ajiro.t01c%40virus.ipa.go.jp%2F2%3A%E5%B1%B1%E7%94%B0%E5%A4%AA%E9%83%8E%3A888-8888%3Ayamada.taro.t01c%40virus.ipa.go.jp%2F

decode:
test = 1:いぱ 次郎:999-9999:jiro.t01c@virus.ipa.go.jp/2:山田 太郎:888-8888:yamada.taro.t01c@virus.ipa.go.jp/

②：①をIPAが目で見てわかるように変換した内容

IPAによる「呼びかけ」と「注意喚起」

経済産業省
Ministry of Economy, Trade and Industry

届出や相談を発端として「呼びかけ」や「注意喚起」を実施した最近の事例

- Android OSを標的としたウイルスに関する注意喚起（2011年1月）
- 2011年2月の呼びかけ
  「スマートフォンのウイルスに注意！」
- 2011年8月の呼びかけ
  「スマートフォンを安全に使おう！」
- 2012年2月の呼びかけ
  「スマートフォンでもワンクリック請求に注意!」
- 2012年5月の呼びかけ
  「あなたを狙うスマホアプリに要注意！」
- Android OSを標的とした不審なアプリに関する注意喚起（2012年5月）
- 2012年9月の呼びかけ
  「情報を抜き取るスマートフォンアプリに注意!」
- 楽天BLOG　～　IPA情報セキュリティブログ
  「Androidを狙い、情報を抜き取る不正アプリに注意！」（2012年9月）

一般スマホユーザー向けの啓発資料

http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/

これからの課題

経済産業省
Ministry of Economy, Trade and Industry

スマートデバイスの登場は、パーソナルサービスを一気に身近なものに

- **一方で、利用者情報収集型のマルウェアが問題に**

どう対応していくべき？

1. **悪意のあるマルウェア**
2. **開発者に悪意はないが、プライバシーポリシーと実際の機能に乖離があるアプリケーション**
3. **開発者に悪意はなく、プライバシーポリシー通りの機能だが、利用者に分かりづらいアプリケーション**