スマートフォンとセキュリティ脅威

Internet Week 2011
S10 スマートフォンセキュリティ

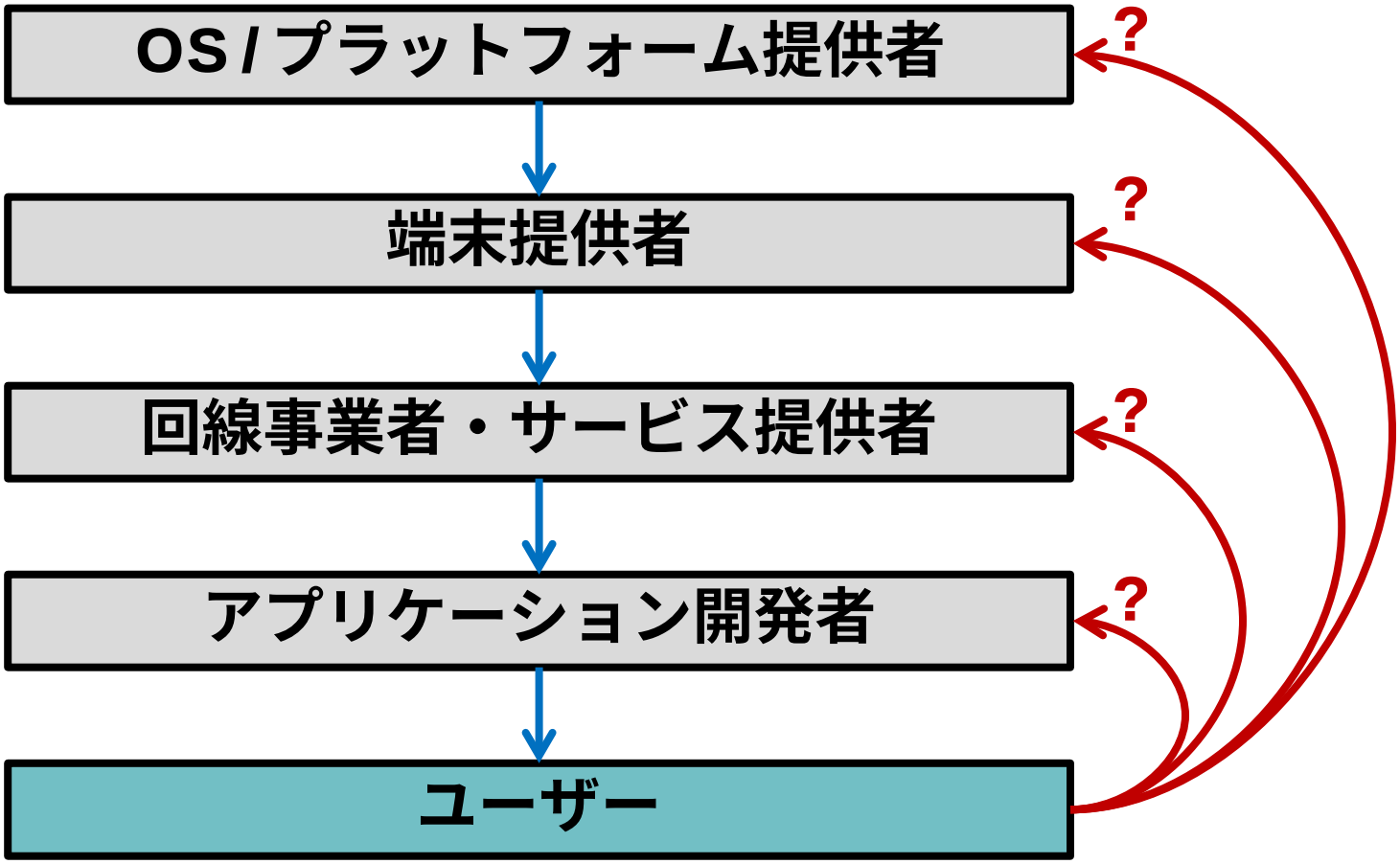
JPCERTコーディネーションセンター　分析センター
センター次長　椎木　孝斉

スマートフォンの特徴

スマートフォンの特徴(機能、運用面)

- PCとの類似性
  - Internet 接続性が高い
  - アプリケーションインストールの自由度が高い
  - 汎用OSが使用されている
- 従来型携帯電話との類似性
  - 可搬性が高い
  - 個人との結びつきが強い
  - 豊富なハードウエアデバイス
    - GPS、カメラ、通話、非接触型ICカードetc

スマートフォンの特徴(環境面)



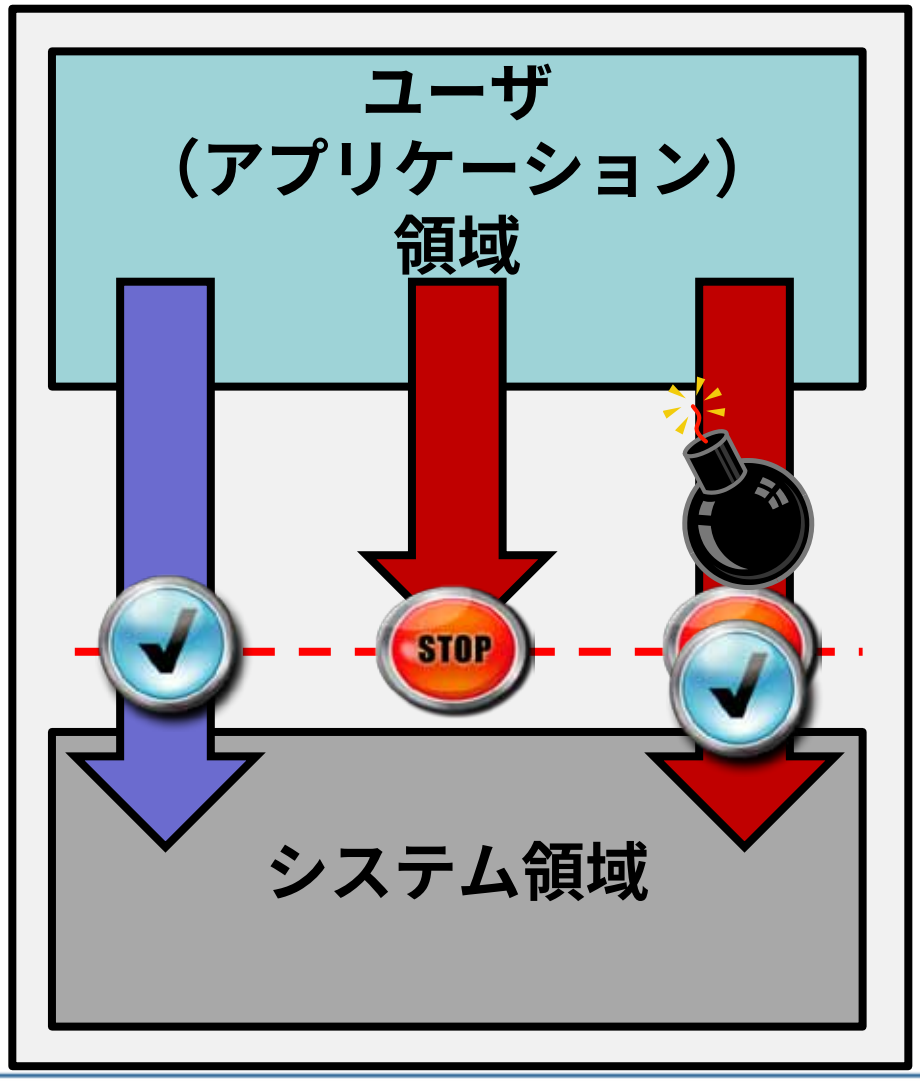
代表的なスマートフォンの比較

	iPhone(iOS)	Android
プラットフォーム 開発主体	Apple	Google
ライセンス	プロプラエタリ	オープンソース
フレームワーク	Mac OS X(BSD）ベース	Linux ベース
OS最新バージョン	5.01(*)	4.0(*)
端末	Appleのみが販売	多くのベンダが販売
アプリケーション	App Store経由での 公開、入手	制限なし
開発言語	Objective-C	Java, (C/C++)
アプリケーション審査	Apple社による審査	基本的に審査されない
電子署名	Apple ID にひもづく証明書	自己証明書
その他		インストール時のパーミッション確認 リモートからの端末内アプリケーション削除

(*)2011年11月18日現在

スマートフォンセキュリティの基本的な考え方

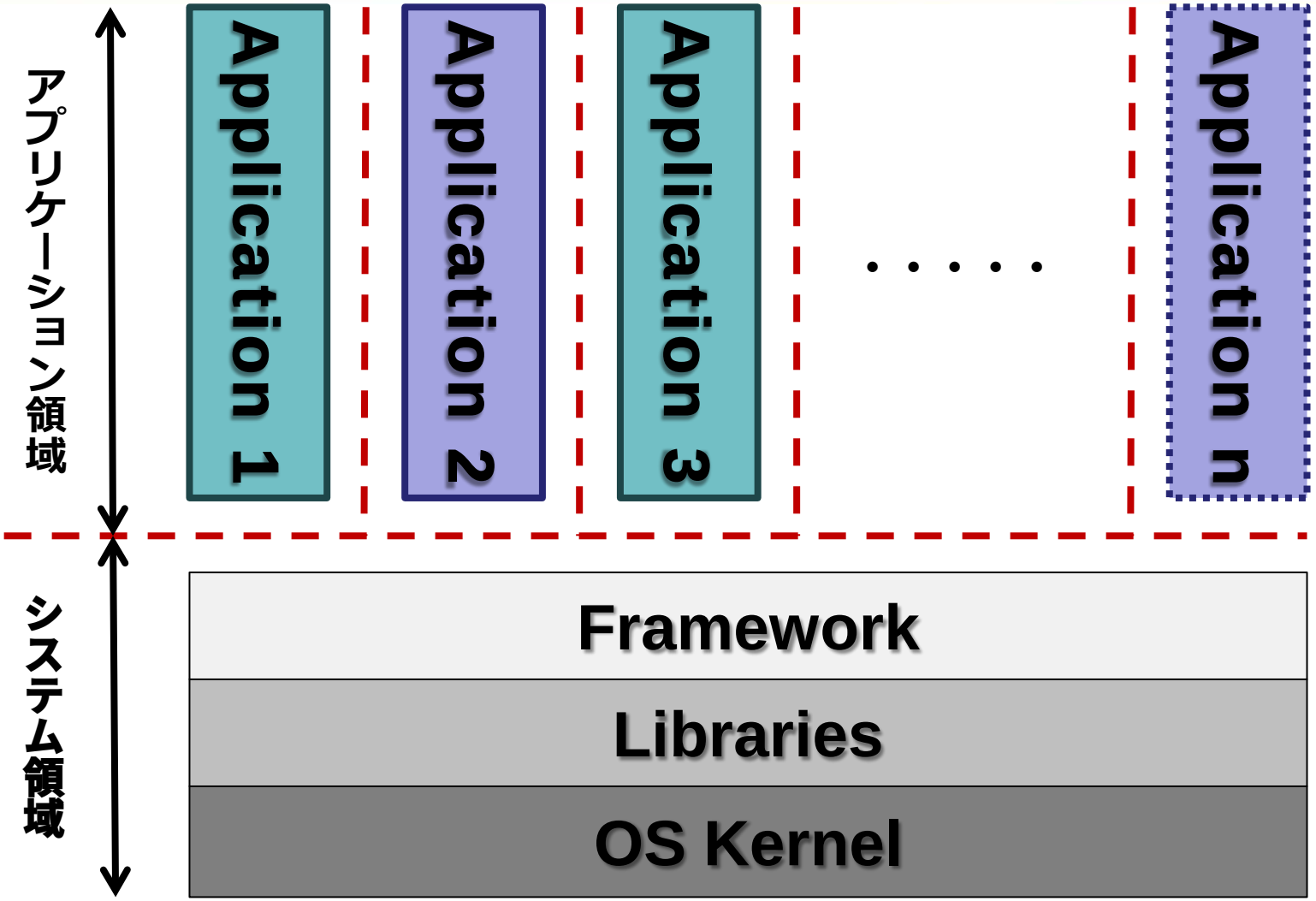
システム保護



- アプリケーション/ユーザに管理者権限は与えない
- システムで保護されている領域とアプリケーションが明確に分離されている
- 脆弱性の悪用(含むJailbreak/rooting)によってその前提が崩される

アプリケーションのサンドボックス化

JPCERT CC®



データ保護

- 可搬性の高さがもたらすリスク（端末の紛失、盗難）に対する対策

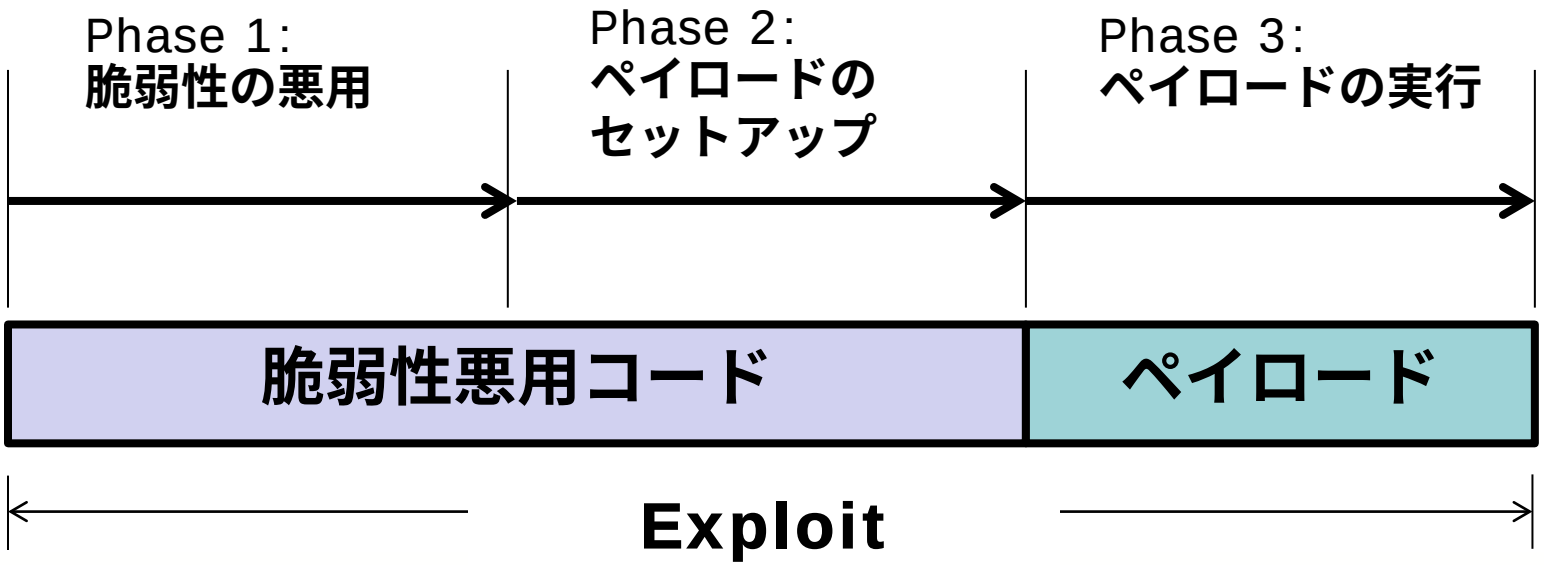
- データ暗号化
  - ディスク（ファイルシステム）レベルでの暗号化
  - アプリケーションレベルでの暗号化

- リモートからの端末操作
  - リモートロック
  - リモートワイプ

脆弱性悪用とExploit

- ソフトウエアがExploit可能とは、
  1. 脆弱性を悪用し、
  2. 自分の意図すること(通常はコード)を実行可能

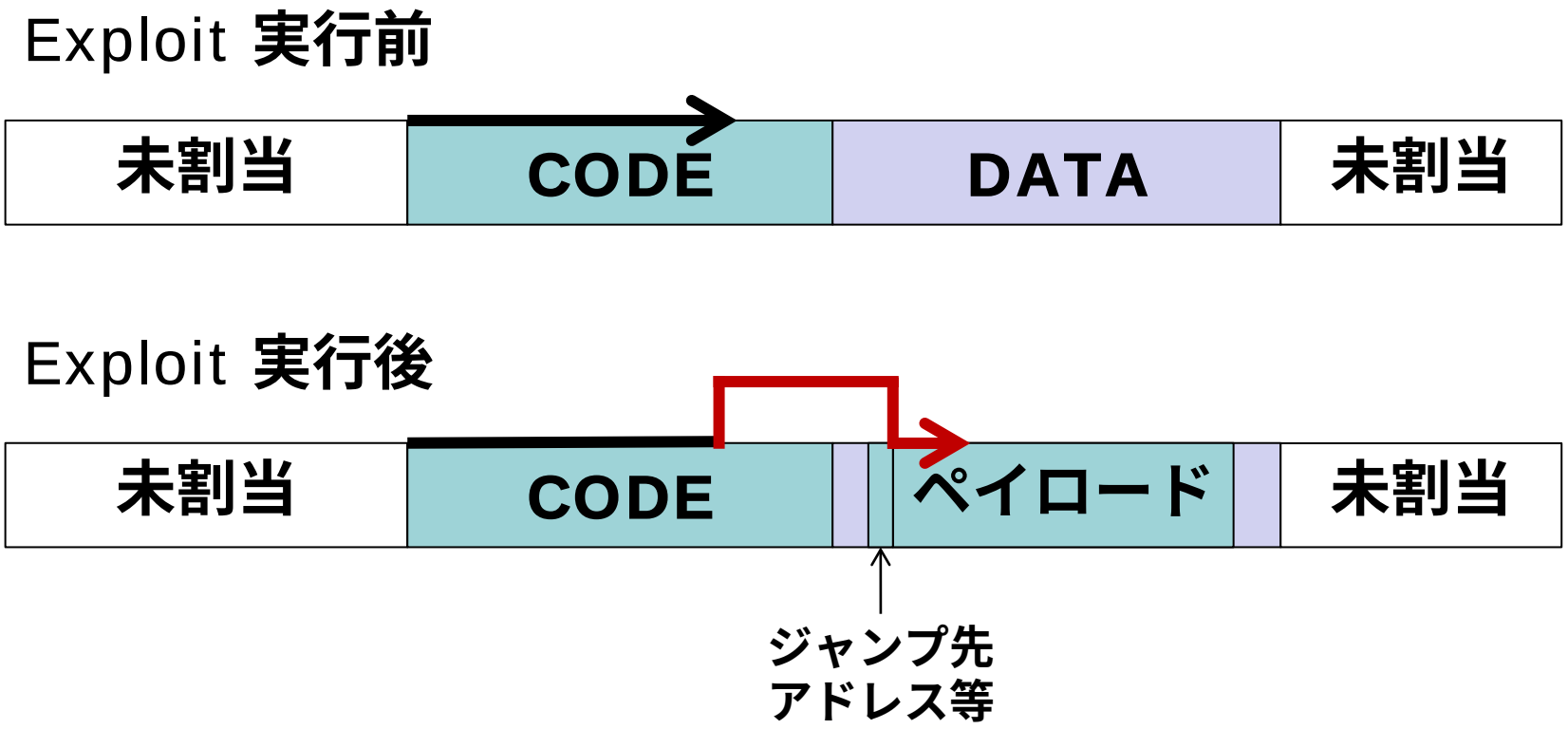
- Exploit実行のフェーズ



ペイロードセットアップの方針(１)

JPCERT CC®

- 方針:実行可能なペイロードをメモリ上に書き込んで、実行する



ペイロードセットアップ方針(1)に対する対策

- 対策A: マーカーを設定しておいてデータが上書きされたらわかるようにする

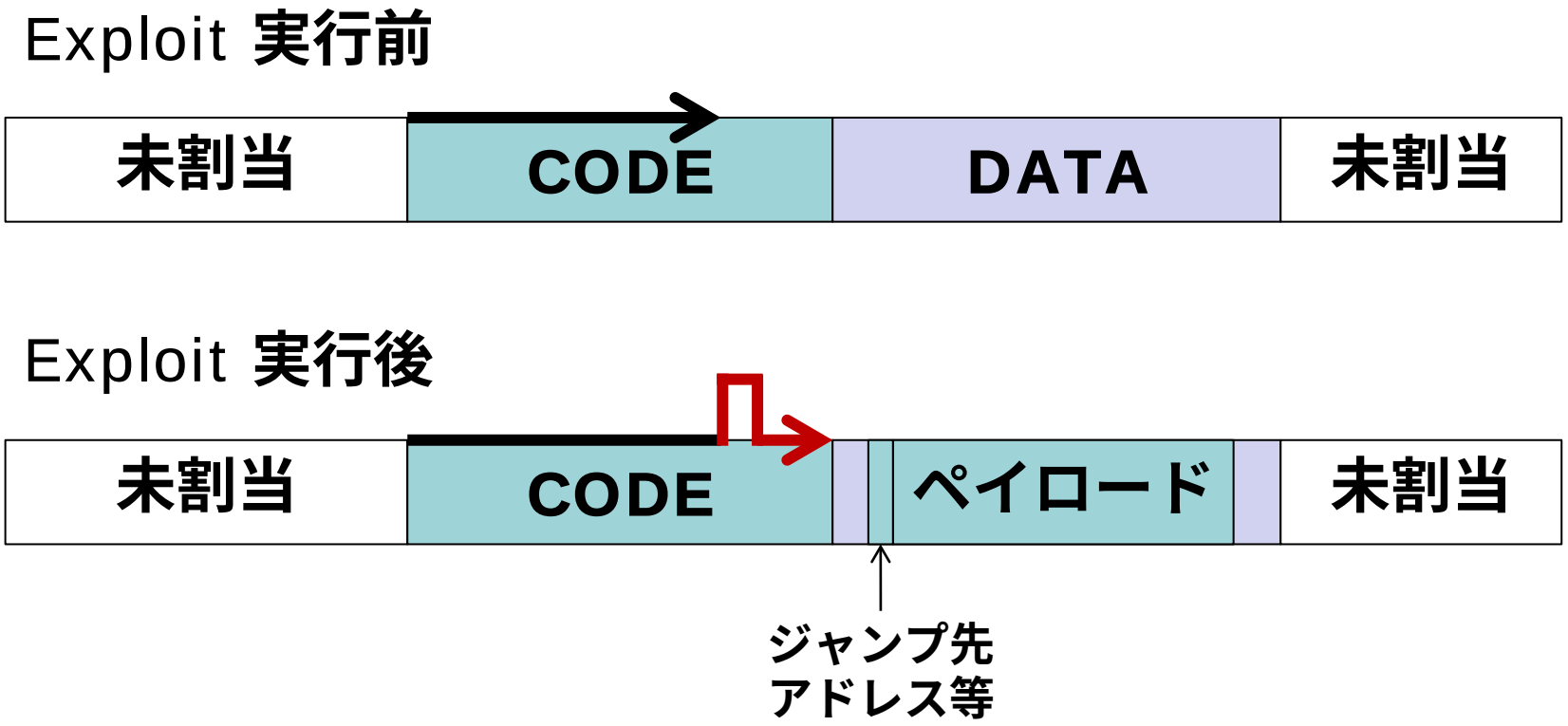
  - コンパイラの協力が必要:
    - Microsoft Visual Studio: Buffer Security Check(/GS)
    - GCC StackGuard(-fstack-protector)など

- 対策B: DATA領域は実行できないようにする
  - DEP(Data Execution Prevention)

  - ハードウエアの協力が必要:

ペイロードセットアップの方針(2)

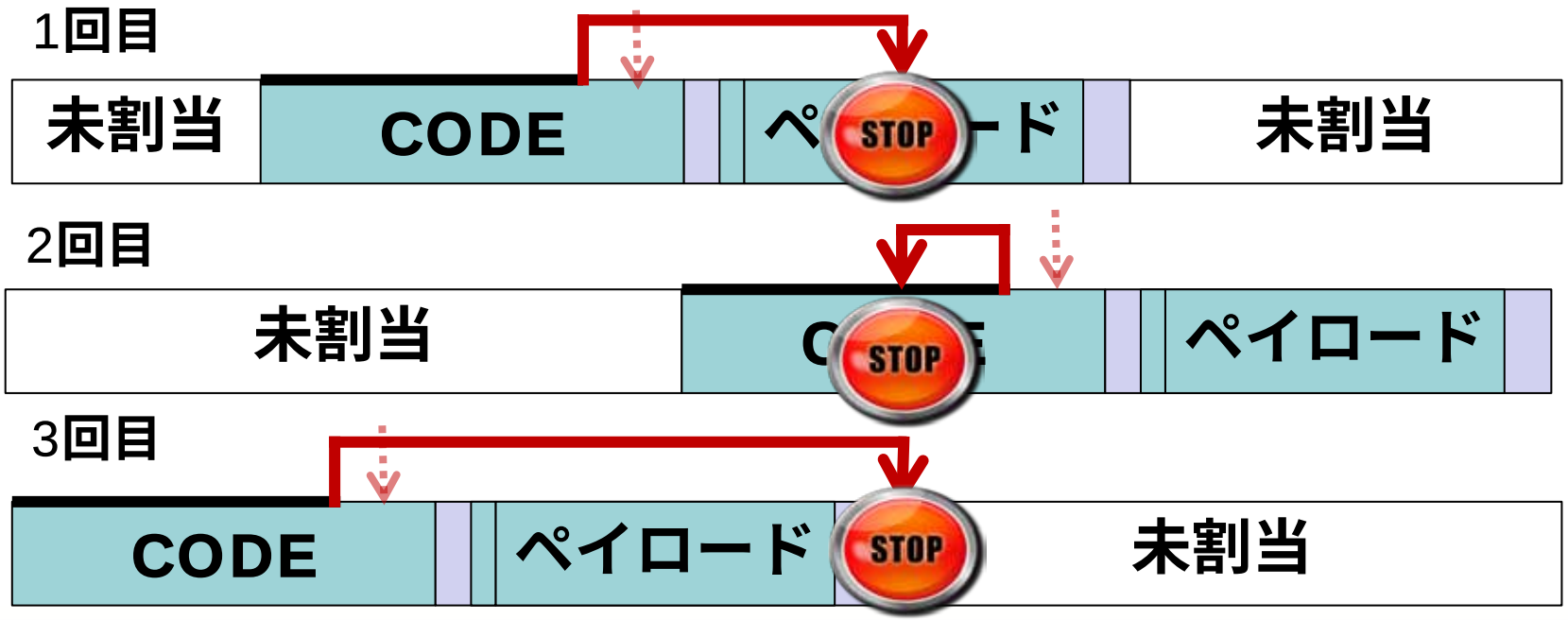
- 方針: 実行するコードは既存の動作可能なコードを利用し、挿入するペイロードはデータとして使用



ペイロードセットアップ方針(2)に対する対策

JPCERT CC®

- **対策**: Exploitが利用したいコードがあらかじめ分からないように（毎回違うアドレスにロードされるように）する。
  - ASLR(Address Space Layout Randomization)



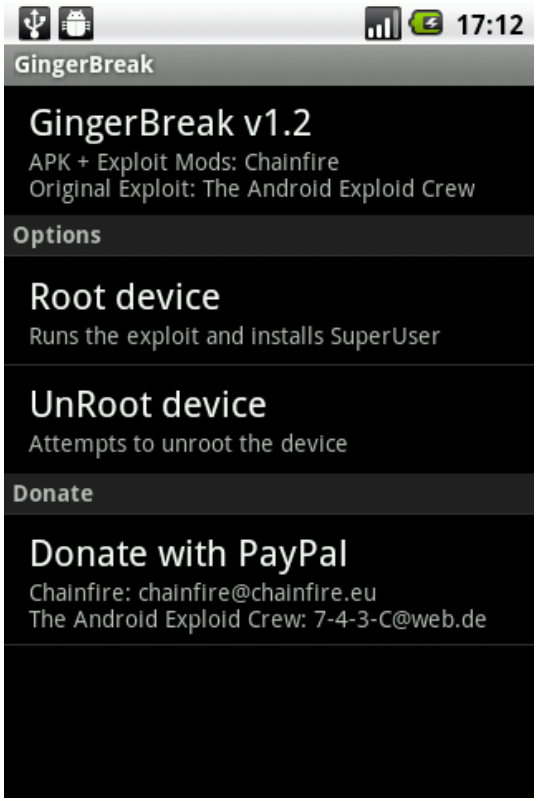
スマートフォンに関する
セキュリティ問題事例

セキュリティ問題事例(1)
～脆弱性問題～

JPCERT CC®

- Apple iOS関連脆弱性
- Jailbreak

- Android関連脆弱性
- Rooting



セキュリティ問題事例(2)
～マルウエア[1]～

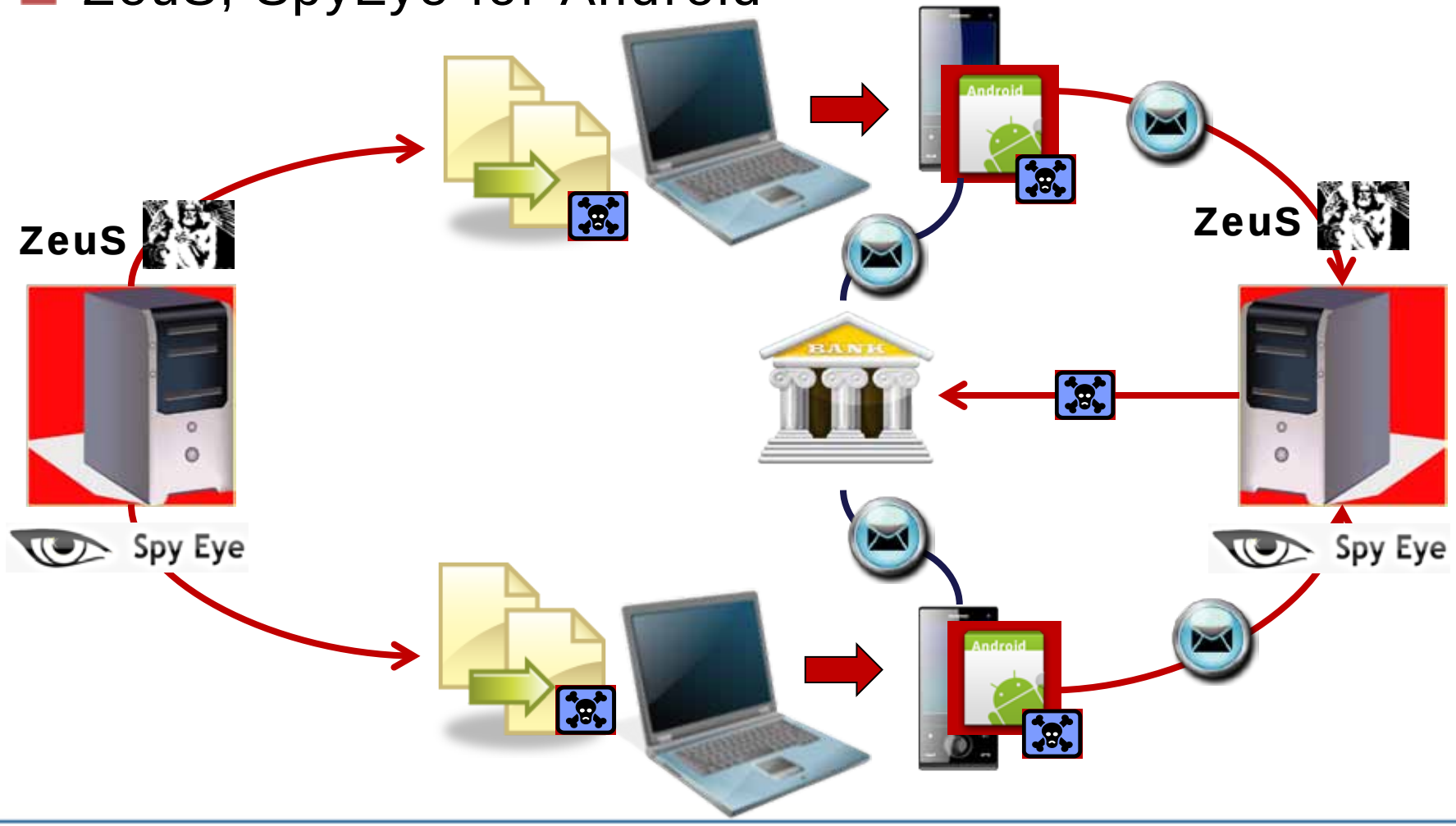
JPCERT CC®

- ikeeウイルス(2009年11月)
  - Jailbreak された iPhoneがターゲット
    - OpenSSHのデフォルトパスワード経由で感染
- Android.Geinimi(2010年12月)
  - 正規のAndroidアプリに不正なコードを挿入
  - 正規ではないサイトで配布
  - 端末情報を送信するほかbot機能を持つ
- DroidDream(2011年3月)
  - 正規の複数のAndroidアプリに不正なコードを挿入
  - 正規のAndroidMarketで配布
  - adbの脆弱性を悪用し管理者権限を取得するモジュール(rageagainstthecage)を含む

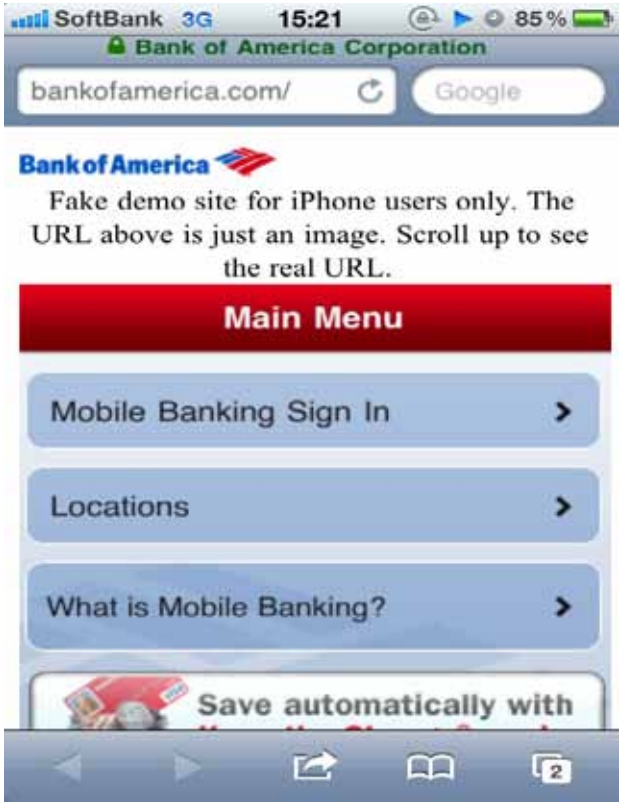
セキュリティ問題事例(2)
～マルウエア[2]～

JPCERT CC®

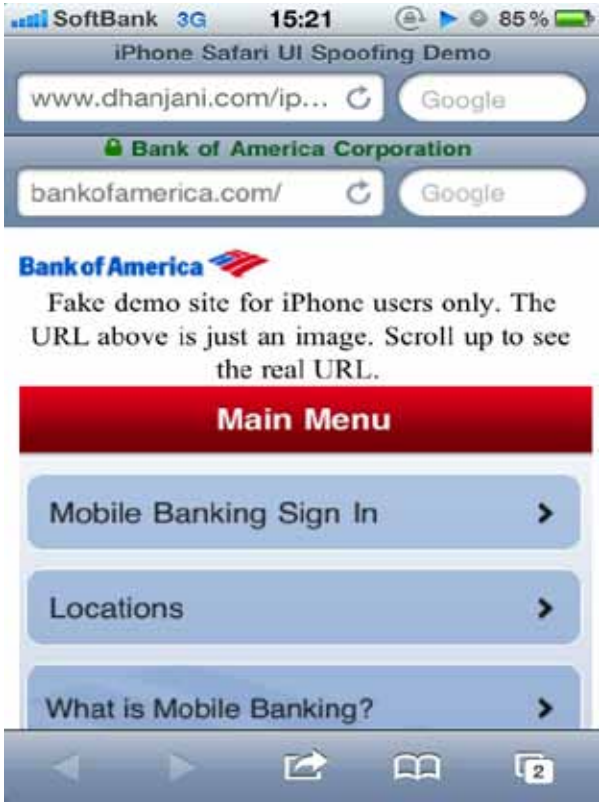
- ZeuS, SpyEye for Android



セキュリティ問題事例(3)
～フィッシングに関わる問題～



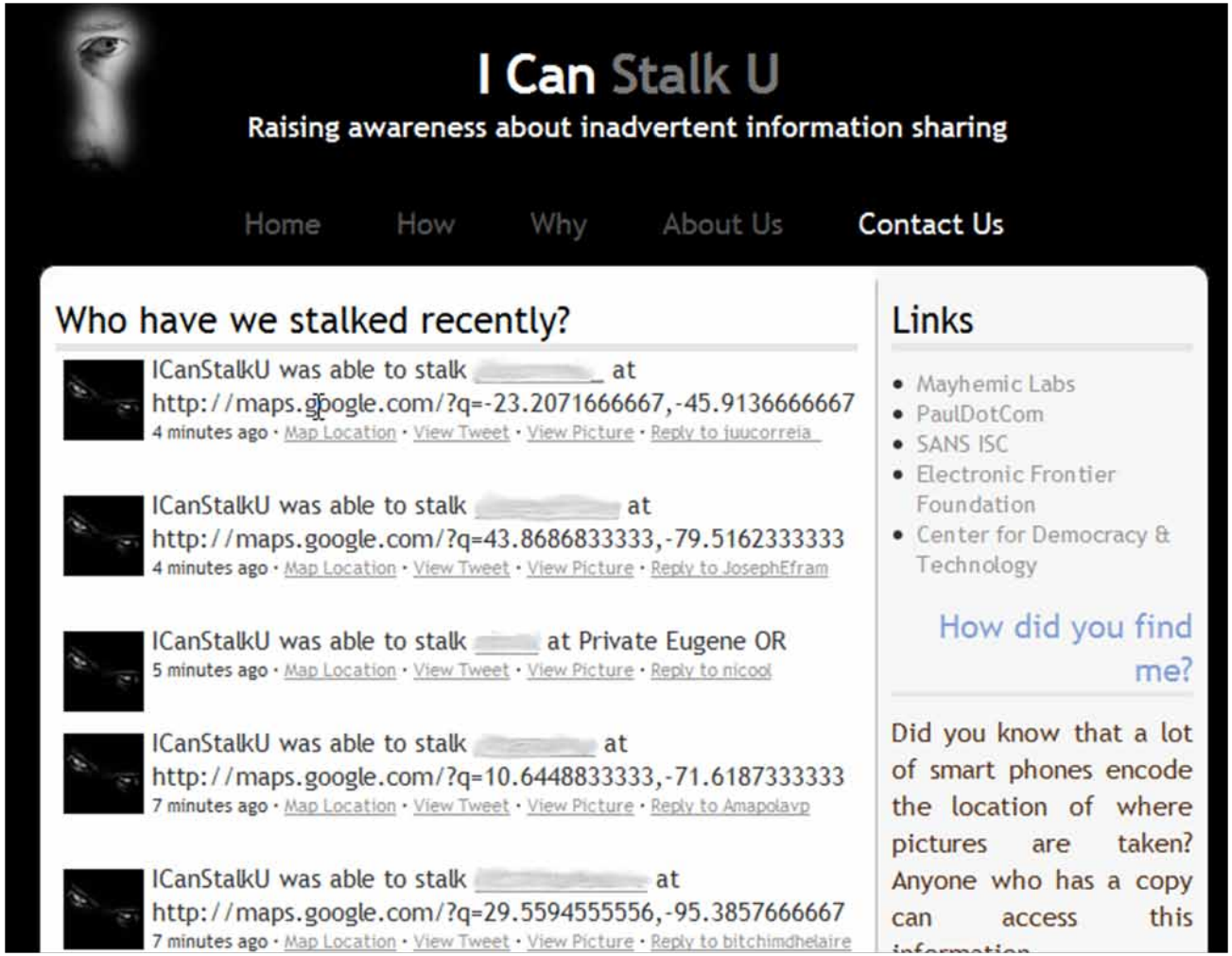
表示されるページ



実際のページ

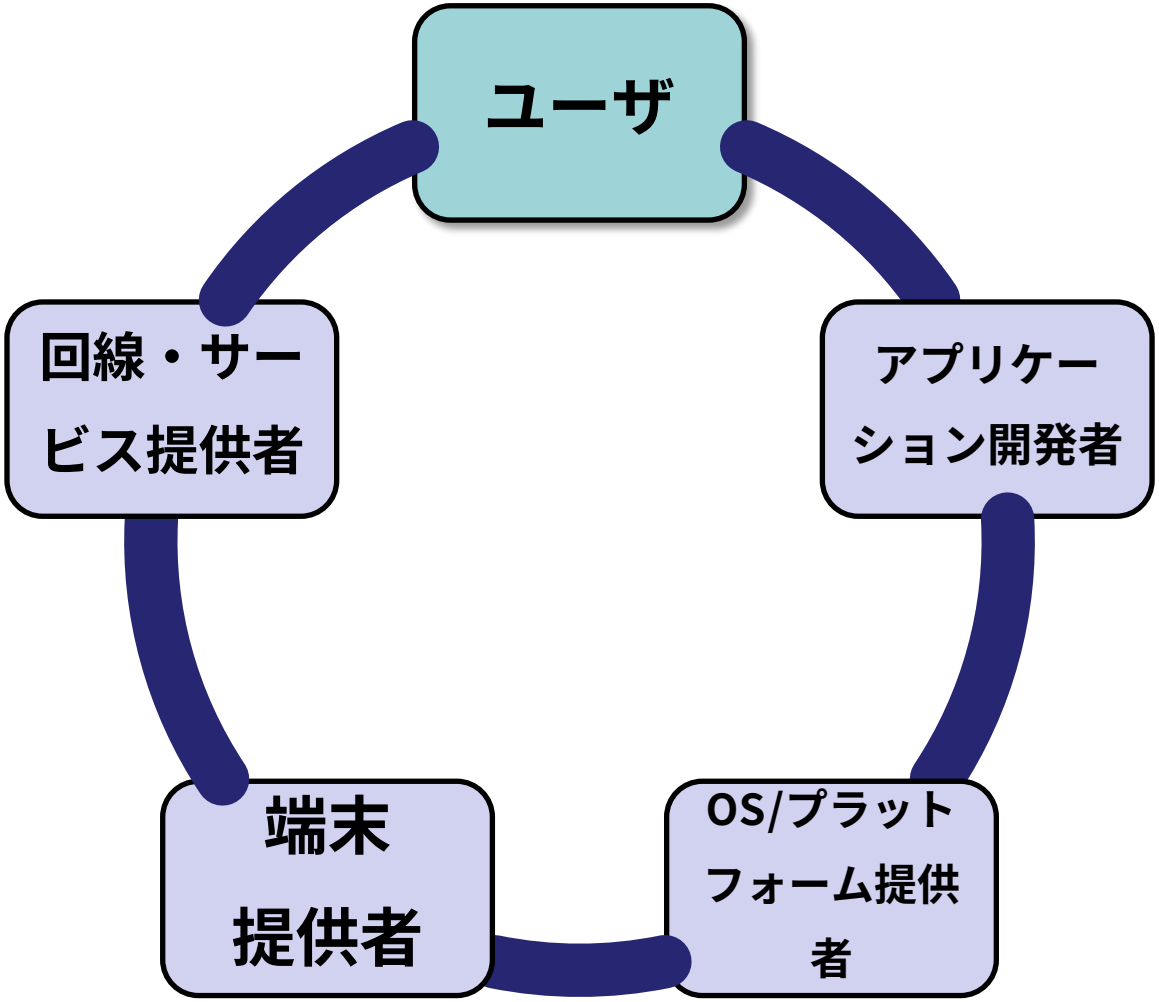
出典: http://www.dhanjani.com/ios-safari-ui-spoofing/

セキュリティ問題事例(4)
～プライバシー・情報漏えい問題～



出典: http://icanstalku.com/

よりよい対応を進めていくために



Contact Information

JPCERT Coordination Center

- Email: office@jpcert.or.jp
- Tel: +81-3-3518-4600
- Web: https://www.jpcert.or.jp/

Incident Reports

- Email: info@jpcert.or.jp
- Web: https://www.jpcert.or.jp/form/

Analysis Center

- Email: aa-info@jpcert.or.jp