

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

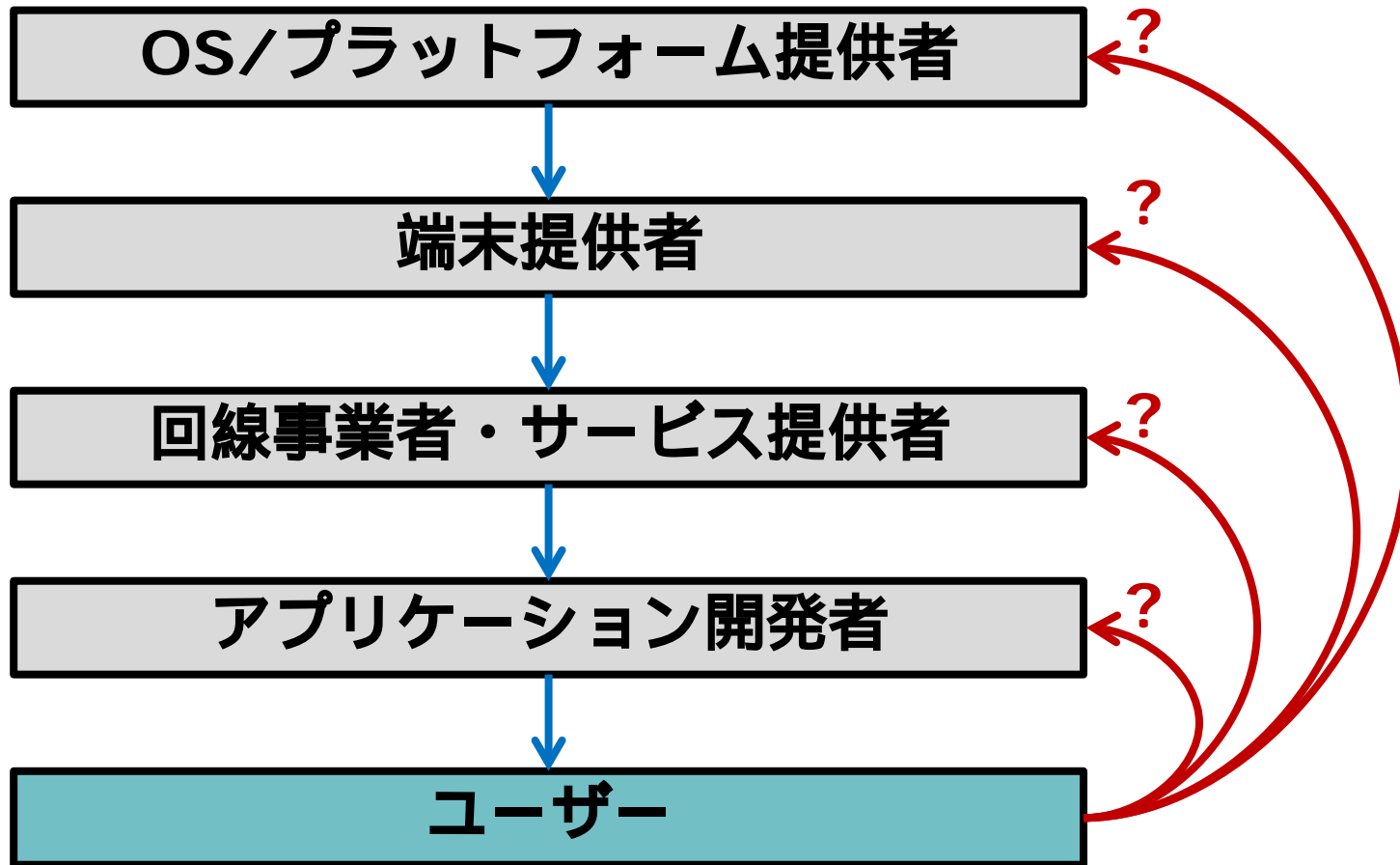
■ PCとの類似性

- ρ Internet 接続性が高い
- ρ アプリケーションインストールの自由度高い
- ρ 汎用OSが使用されている

■ 従来型携帯電話との類似性

- ρ 可搬性が高い
- ρ 個人との結びつきが強い
- ρ 豊富なハードウェアデバイス
 - GPS、カメラ、通話、非接触型ICカードetc

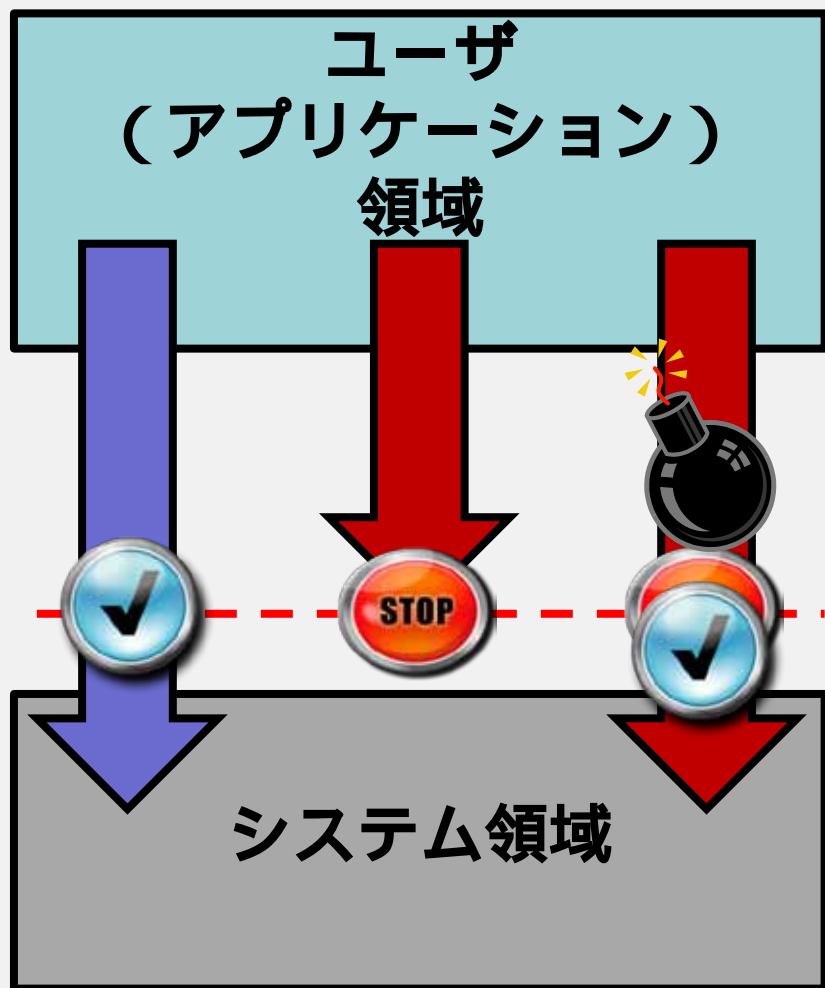
スマートフォンの特徴(環境面)



代表的なスマートフォンの比較

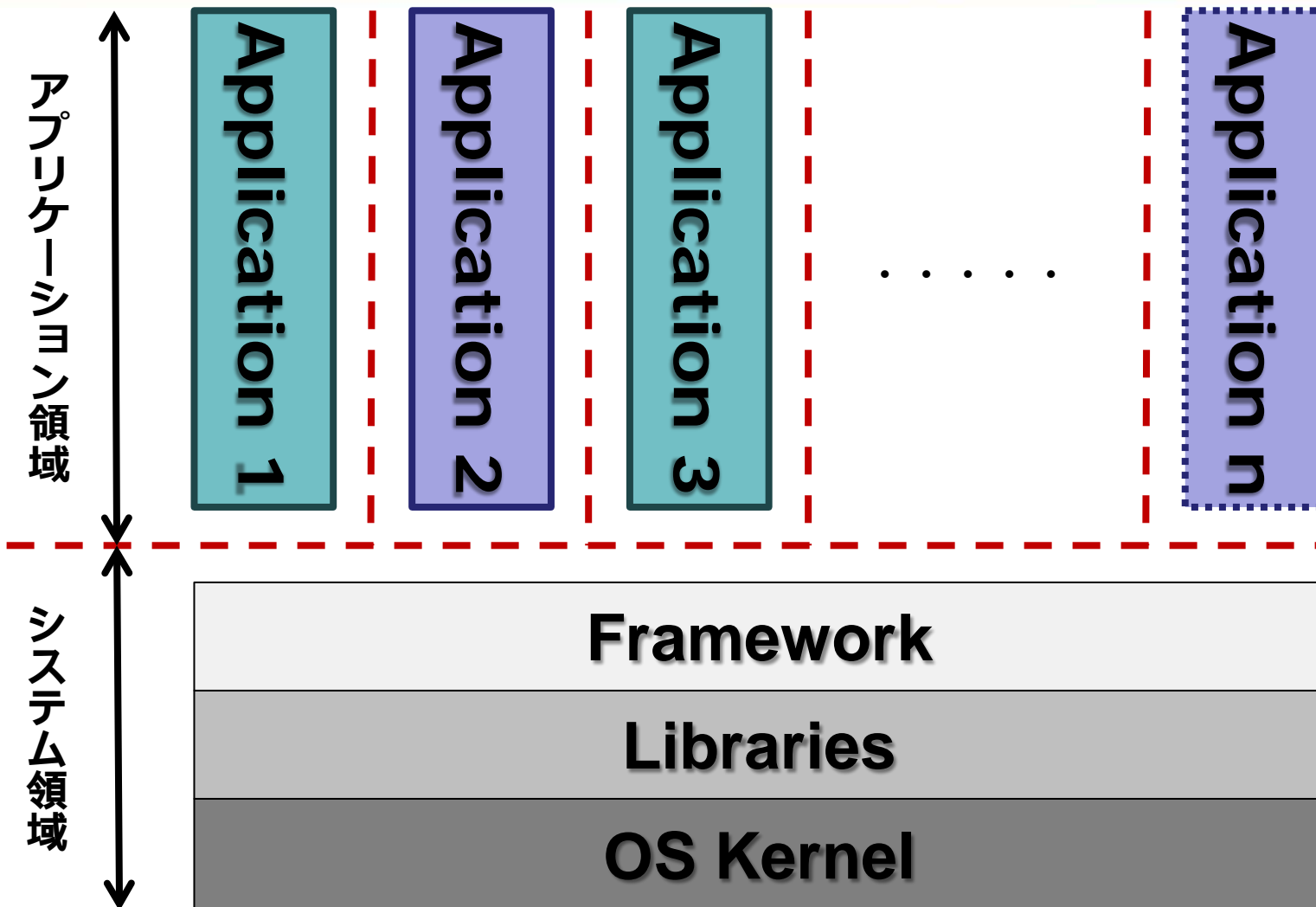
	iPhone(iOS)	Android
プラットフォーム 開発主体	Apple	Google
ライセンス	プロプラエタリ	オープンソース
フレームワーク	Mac OS X(BSD) ベース	Linux ベース
OS最新バージョン	5.01(*)	4.0(*)
端末	Appleのみが販売	多くのベンダが販売
アプリケーション	App Store経由での 公開、入手	制限なし
開発言語	Objective-C	Java, (C/C++)
アプリケーション審査	Apple社による審査	基本的に審査されない
電子署名	Apple ID にひもづく証明書	自己証明書
その他		インストール時のパーミッ 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

スマートフォンセキュリティの基本的な考え方



- 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



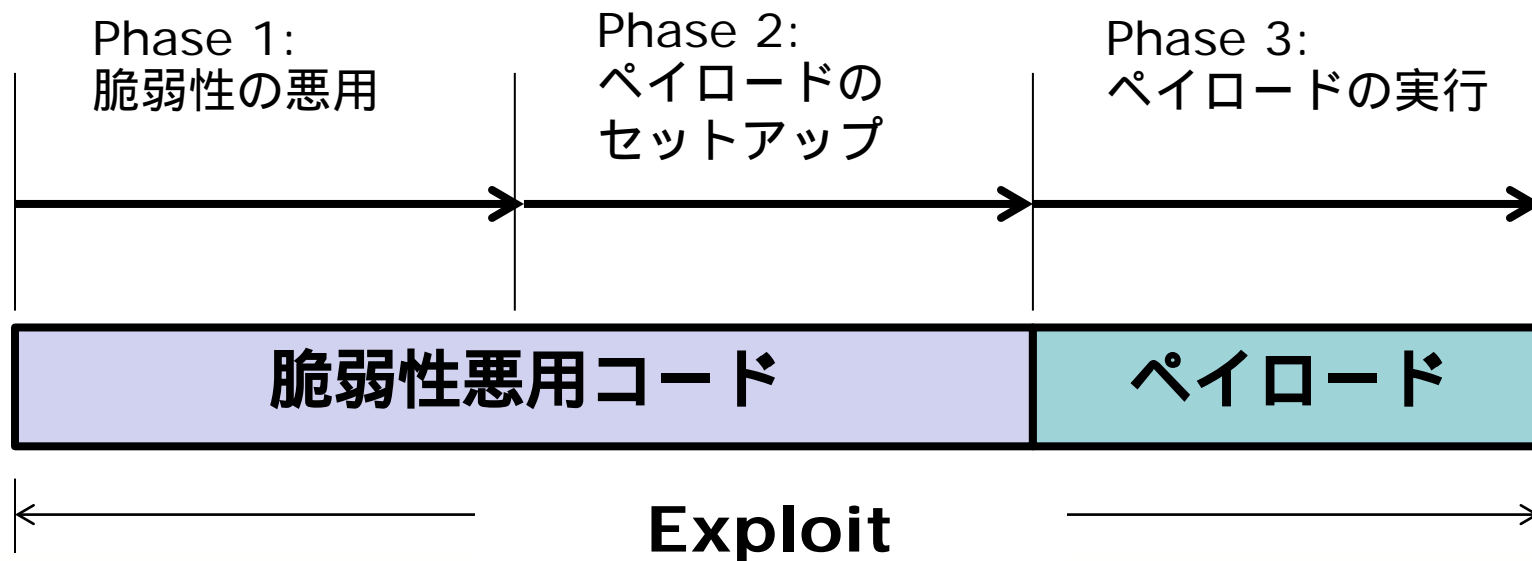
- 可搬性の高さがもたらすリスク（端末の紛失、盗難）に対する対策

- データ暗号化
 - ρ ディスク（ファイルシステム）レベルでの暗号化
 - ρ 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
 - ρ リモートロック
 - ρ リモートワイプ

- ソフトウェアが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

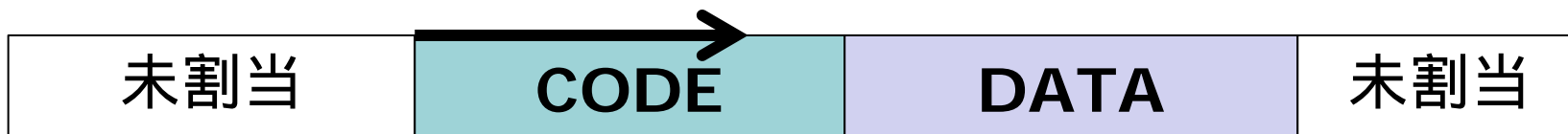
■ Exploit実行のフェーズ



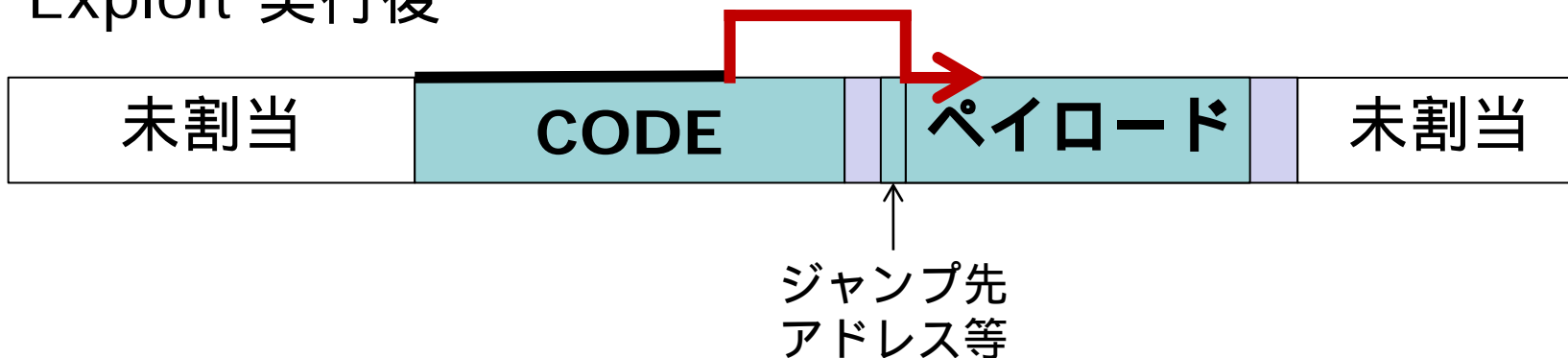
ペイロードセットアップの方針(1)

- 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

Exploit 実行前



Exploit 実行後



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:

↑ マーカー

- 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)

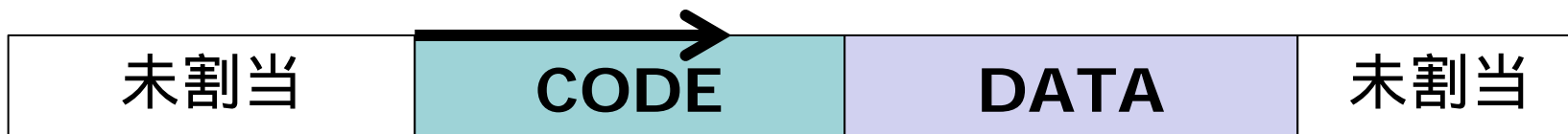


Ⓟ ハードウェアの協力が必要:

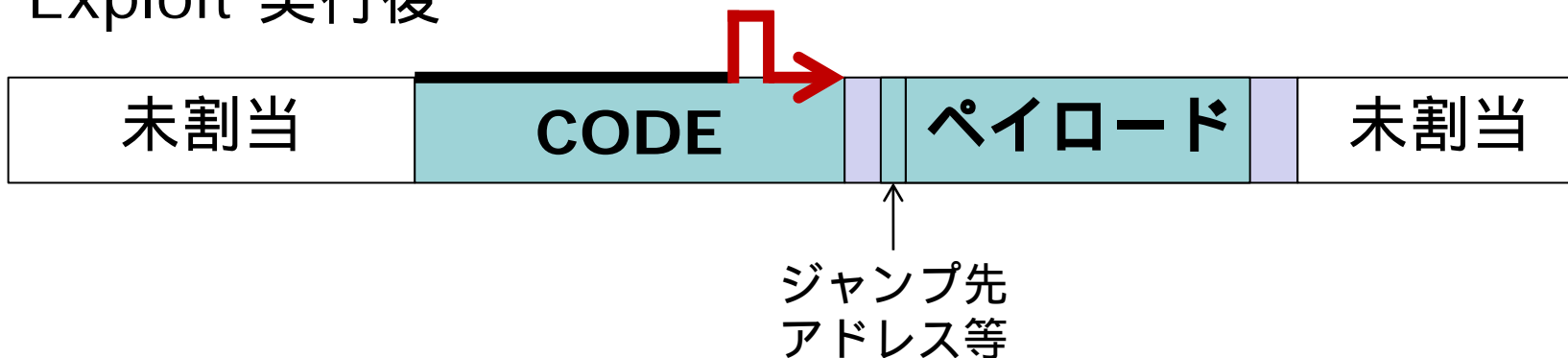
ペイロードセットアップの方針(2)

- 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

Exploit 実行前



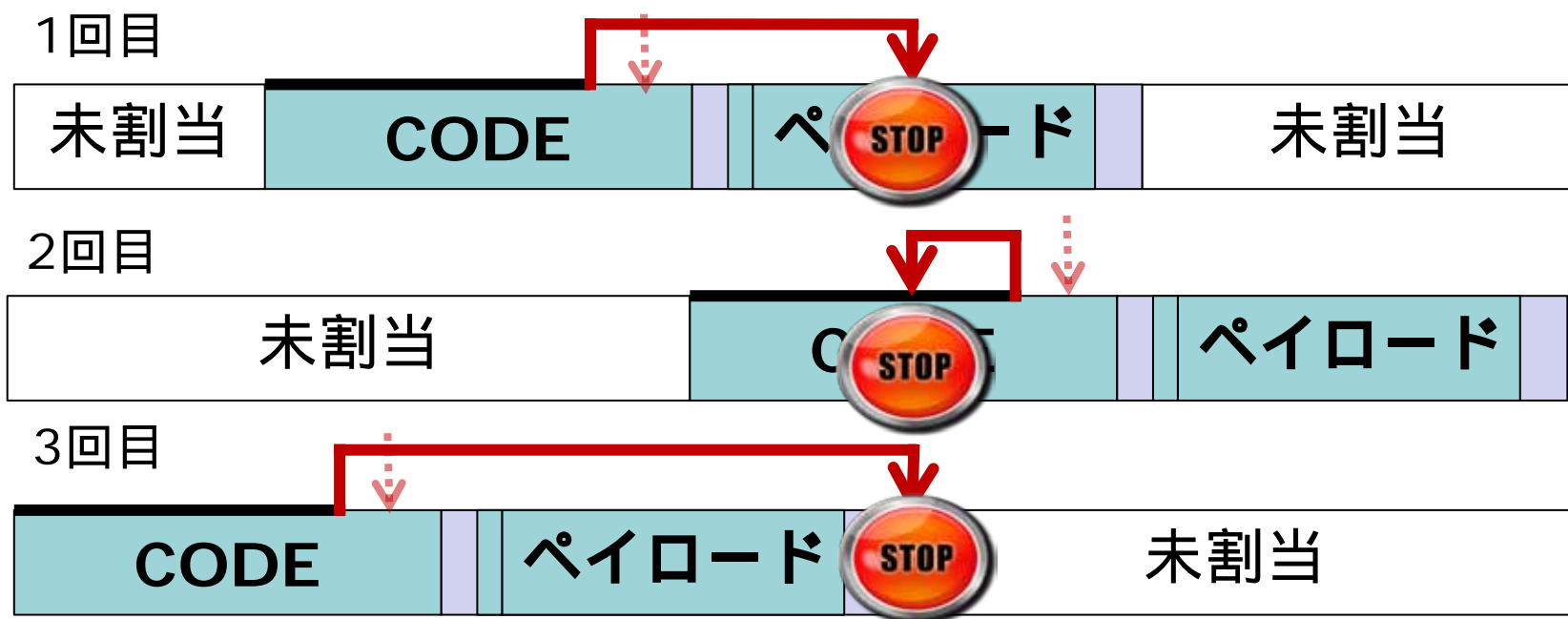
Exploit 実行後



ペイロードセットアップ方針(2) に対する対策

- 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～

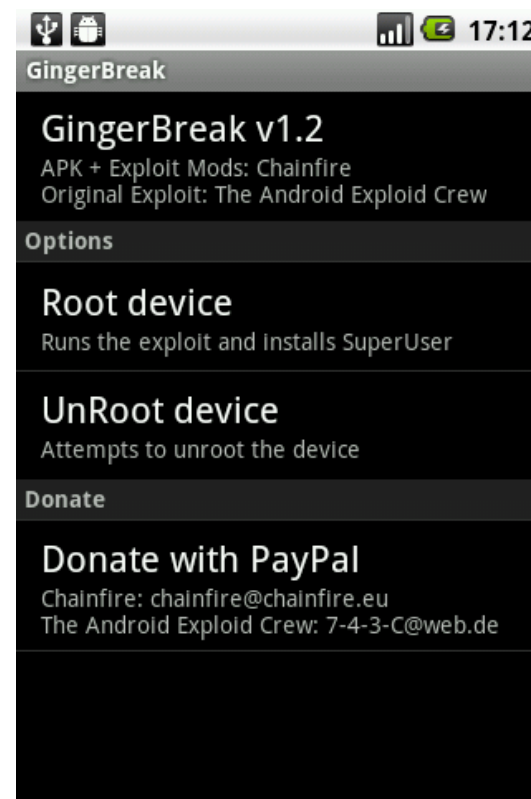
■ Apple iOS関連脆弱性

■ Jailbreak



■ Android関連脆弱性

■ Rooting



セキュリティ問題事例(2)

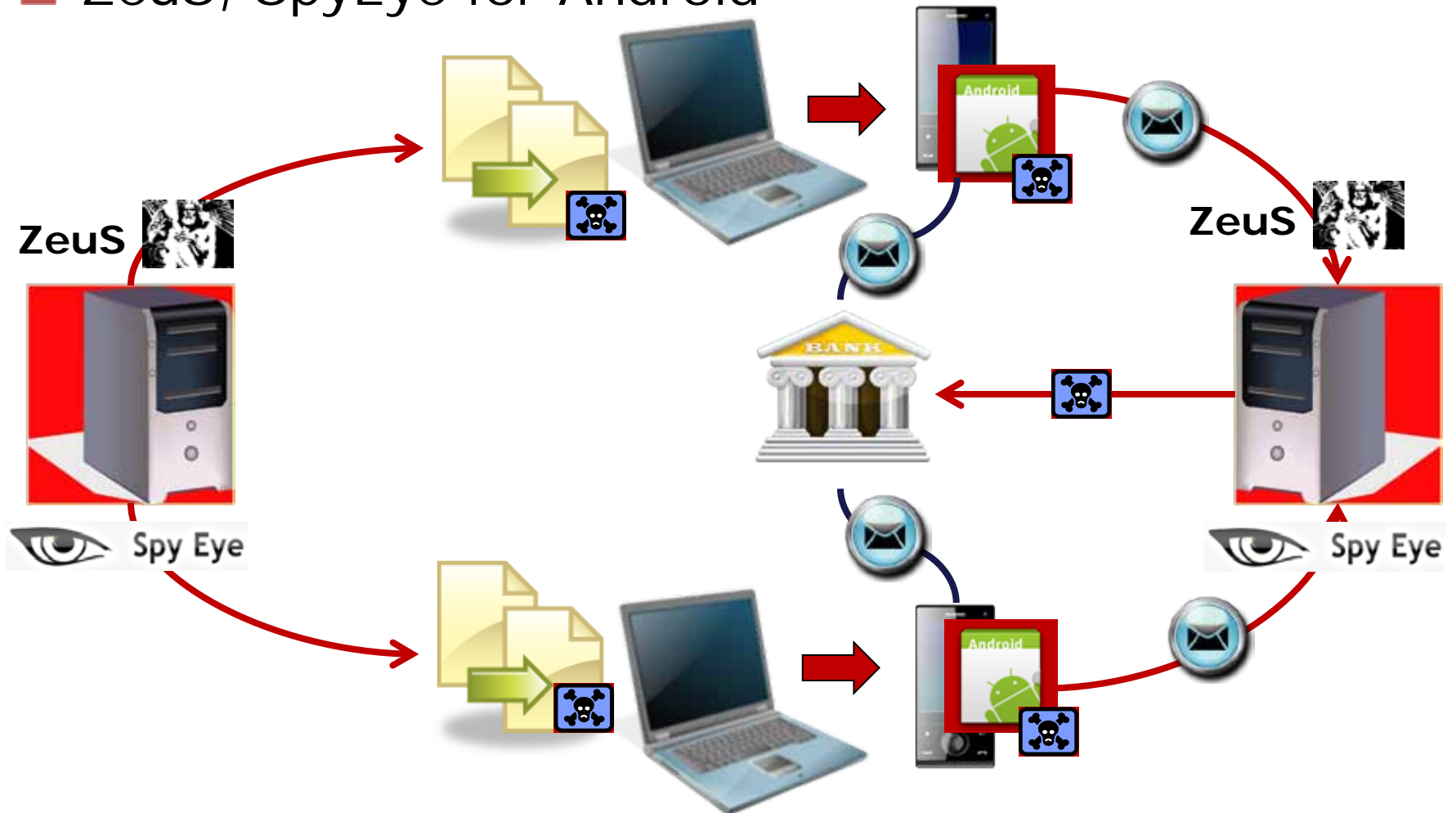
～マルウェア[1]～

- 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 Android Market 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) ~ マルウェア[2] ~

■ 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～



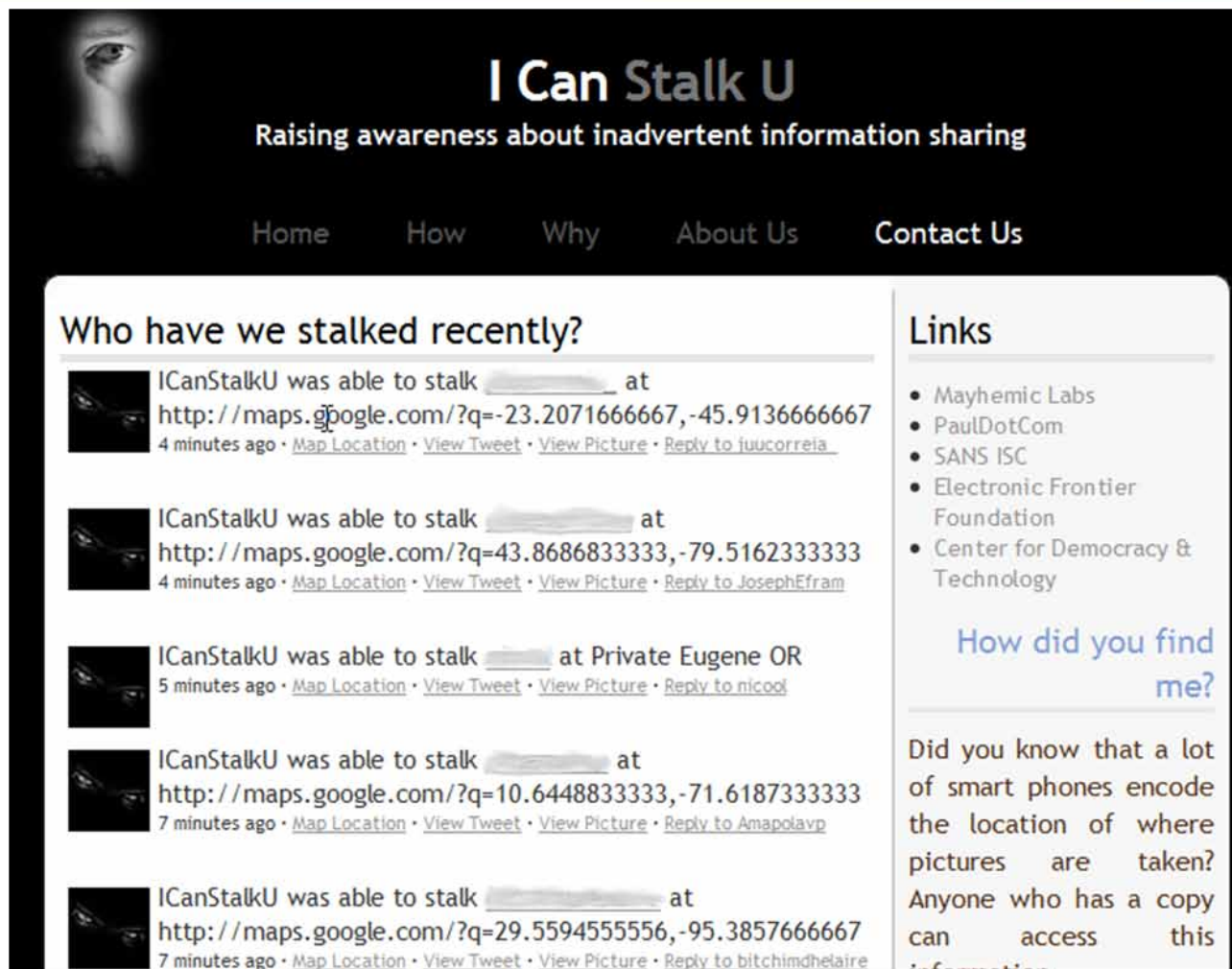
表示されるページ



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～



I Can Stalk U
Raising awareness about inadvertent information sharing

Home How Why About Us Contact Us

Who have we stalked recently?

-  ICanStalkU was able to stalk [redacted] at <http://maps.google.com/?q=-23.2071666667,-45.9136666667>
4 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [Reply to juucorreia](#)
-  ICanStalkU was able to stalk [redacted] at <http://maps.google.com/?q=43.8686833333,-79.5162333333>
4 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [Reply to JosephEfram](#)
-  ICanStalkU was able to stalk [redacted] at Private Eugene OR
5 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [Reply to nicool](#)
-  ICanStalkU was able to stalk [redacted] at <http://maps.google.com/?q=10.6448833333,-71.6187333333>
7 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [Reply to Amapolavp](#)
-  ICanStalkU was able to stalk [redacted] at <http://maps.google.com/?q=29.5594555556,-95.3857666667>
7 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [Reply to bitchindelaire](#)

Links

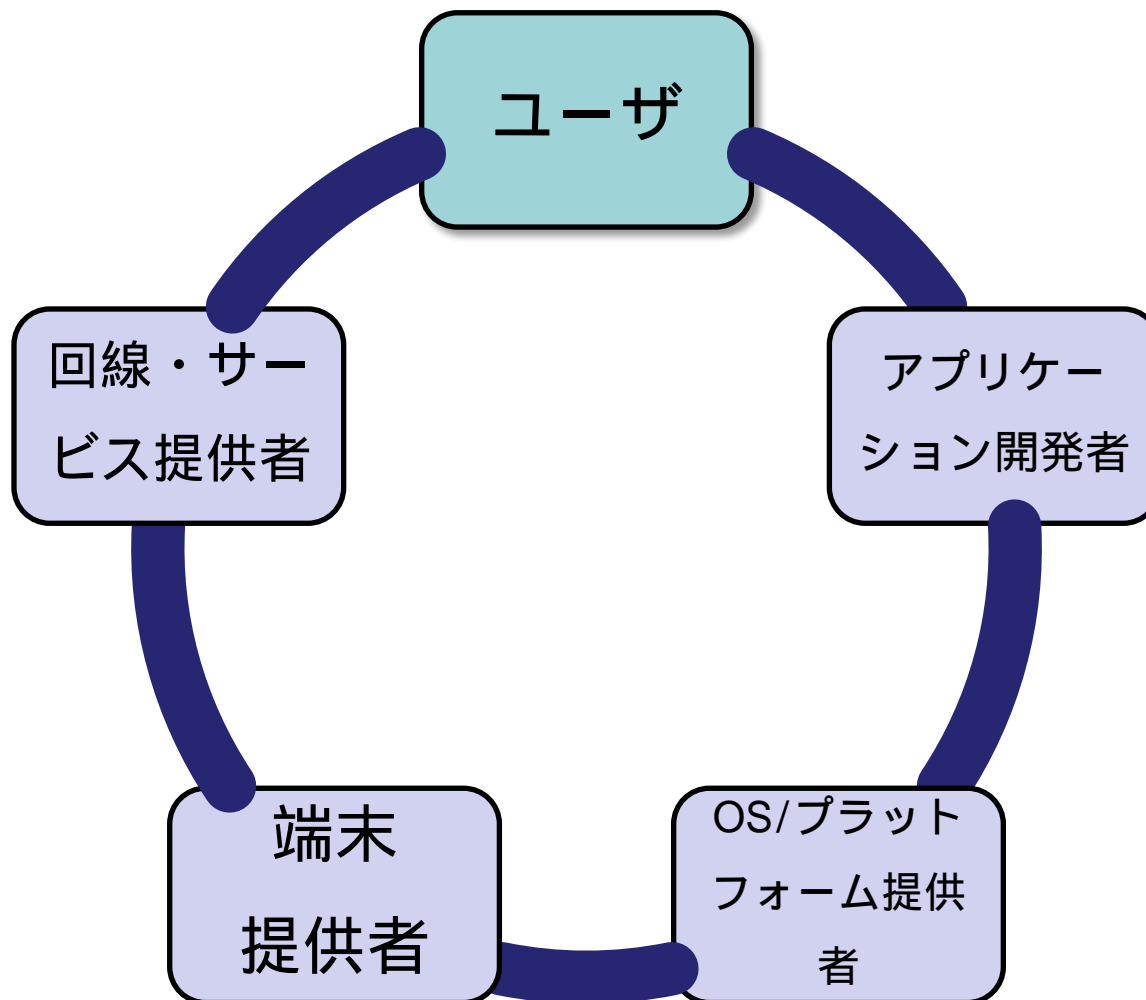
- Mayhemic Labs
- PaulDotCom
- SANS ISC
- Electronic Frontier Foundation
- Center for Democracy & Technology

[How did you find me?](#)

Did you know that a lot of smart phones encode the location of where pictures are taken? Anyone who has a copy can access this information.

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

HTTPS

セキュリティインシデント...
フィッシングガイド...
Webサイトの改ざん...
マルウェア...
不正アクセス...

発生元への「謝罪」を依頼したい
インシデントを「報告」したい

ISDAS
「インターネット安全検定」

インターネット上に配置したセ
ンサーにより、セキュリティ上の
脅威となるトラフィックを監視し
ています。

おすすめページ

セキュリティ
対策講座

被害被害者が便する、新入社
員などが身につけておくべきセ
キュリティ知識などを紹介して
います。

イベント

- 第20回 FIRST Annual
Conference 京都 参加申し込み受付中
- 「COH」セキュリティコーディネ
ィングハーフデイキャンプ参加申し込み