zMTD

モバイル・セキュリティ・リスク防衛ソリューション のご紹介

株式会社東陽テクニカ
情報通信システム営業部
Cyber Security Project Team

グローバル・モバイル・脅威の現在状況

- US, China, Russia, Brazilにたいしてもっとも頻繁に攻撃がなされている
- 最も危険なMITMイベントが全世界で観測されている。
  - これはグローバルな問題
- グローバルメジャーなWebサービスは大規模なユーザー情報を所有しているため狙われている
- 複数の地域・国では様々な手法で狙われている。(ネットワークやウェブサイト)
- モバイル端末のダイアグノスティック・サービスは、攻撃者に対して詳細なエンジニアリング情報を流出させている

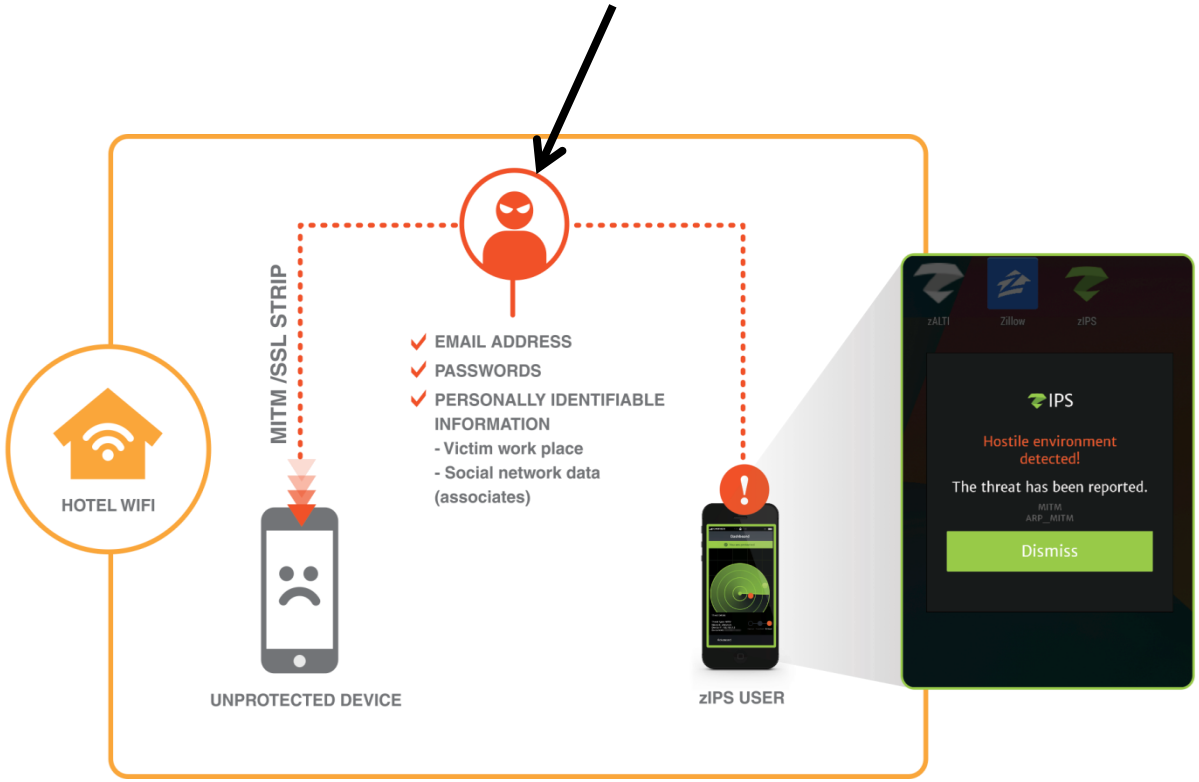
危険なMITMイベントの検出 Topカントリー

*MITM: 中間者攻撃(Man-In-The-Middle)

ARPポイゾニングとICMPリダイレクト技術が 用いられている

- **U.S.** 全攻撃に対する比率の **9.1%**
- **China** 全攻撃に対する比率の **5.15%**
- **Brazil** 全攻撃に対する比率の **5.19%**
- **France** 全攻撃に対する比率の **4.7%**
- **Mexico** 全攻撃に対する比率の **3.58%**

盗聴・なりすまし・詐称



（参考）携帯セルラー通信における脅威

・スマートフォンの普及率の向上およびモバイル金融取引の一般化に伴い、個人情報や金融情報を狙うマルウェアが急増している。

Tweet g+1 1 Share

Apple's Much-Maligned Malware 'Wire Lurker' Lurks And Hops Through Your OS, iPhones , MacBooks, USBs?

Nov 09, 2014 10:01 PM EST | By Adelyn Torralba

Tags **iOS, OSXを狙う新マルウェア**

Wire Lurker, Wire Lurker Updates, Wire Lurker Latest News, Wire Lurker News, Wire Lurker Latest Update

引用元：palalto network
http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

ここ1~2年で
急速な増加！

直近3年間の1月~9月に発見されたスマートフォンマルウェアの件数

引用元：Ahnlab
http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

（参考）Wi-Fi関係における脅威

・駅や飲食店など不特定多数が利用できるフリーWi-Fiなどは特に、悪意のある攻撃ツールによって簡単に情報が窃取されてしまう危険が非常に高い。

主な例：

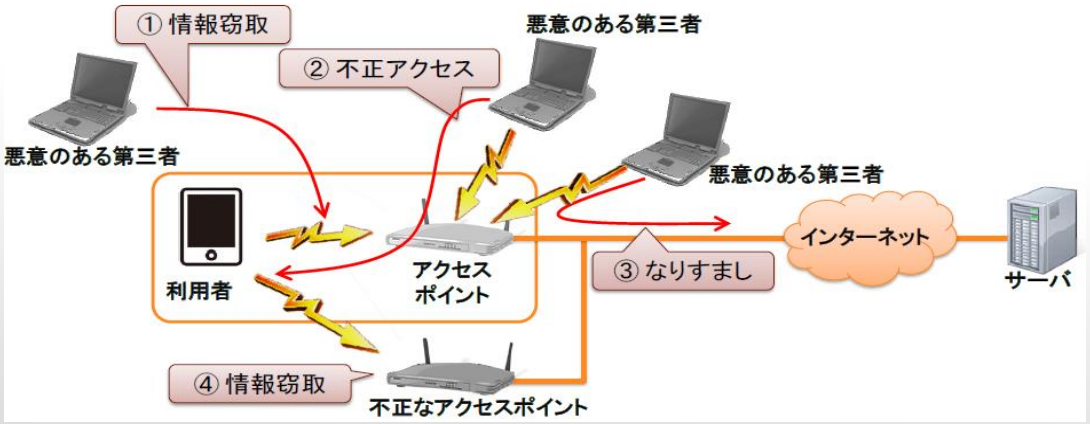
① 無線ＬＡＮ区間における情報窃取 **（ホテルの無線LANサービスから宿泊者情報窃取など）**

② 他端末からの不正アクセス

（LINEアカウントのっとり、POSマルウェアによるクレジットカード情報の窃取）

③ 利用者端末へのなりすまし **（ICMPリダイレクトによる侵入・なりすましによる盗聴）**

④ 不正なアクセスポイントにおける情報窃取 **（ウィルス感染や情報漏えいなど）**

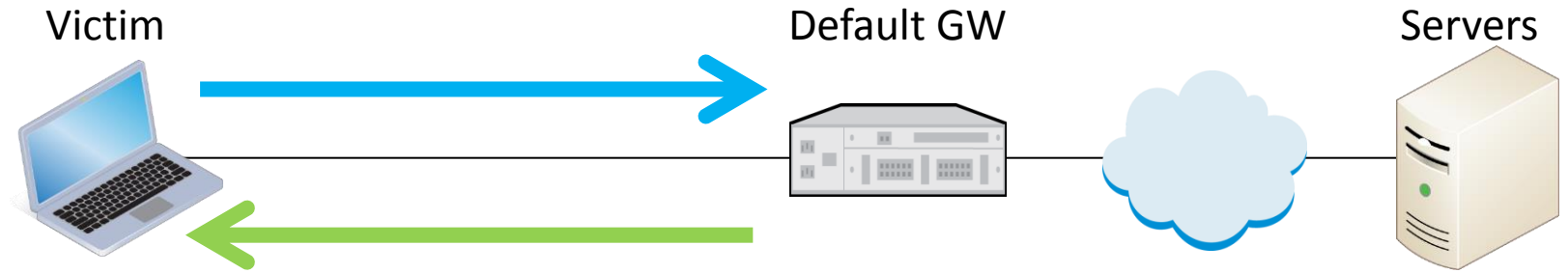


引用元：総務省
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf

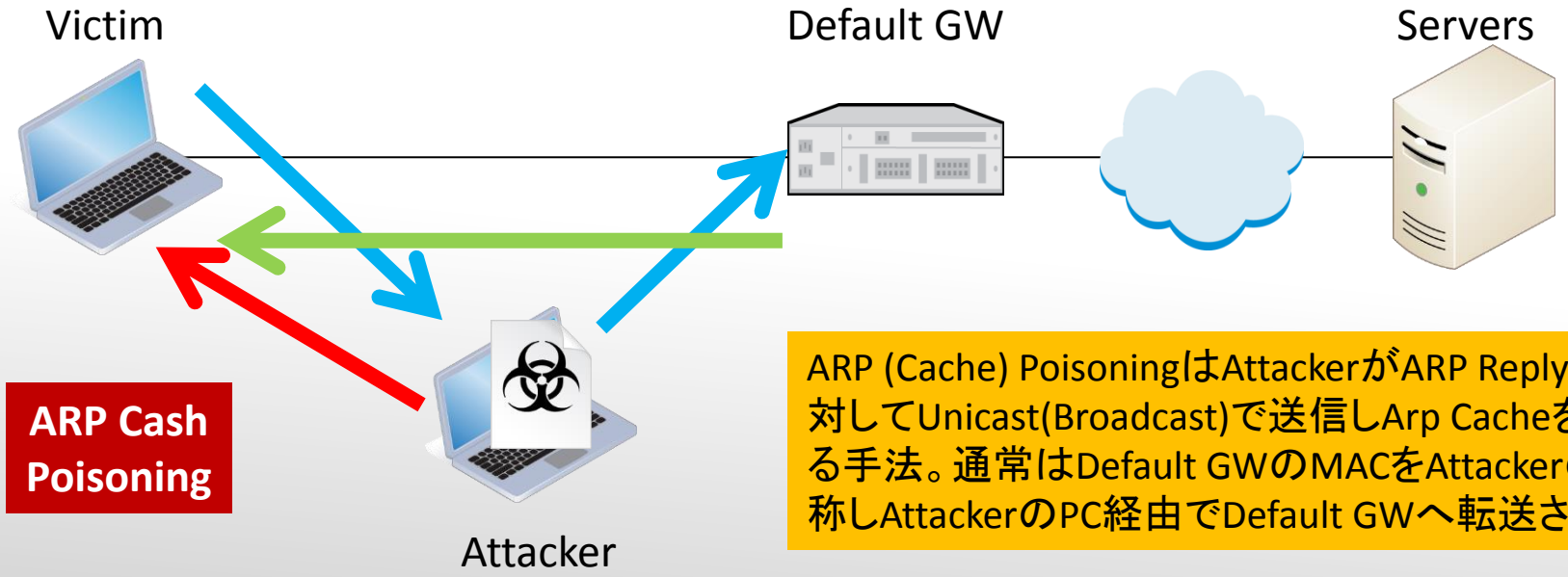
あなたを狙う脅威

- ネットワーク **MiTM** 攻撃
- クライアント側のスピア・フィッシング
- **SSL**ストリッピング・ネットワーク・アタック
- モバイル **RATs (**リモートアクセス・トロイ）
- マリシャス・アプリケーション

（参考）代表的な攻撃例: ARPポイゾニング



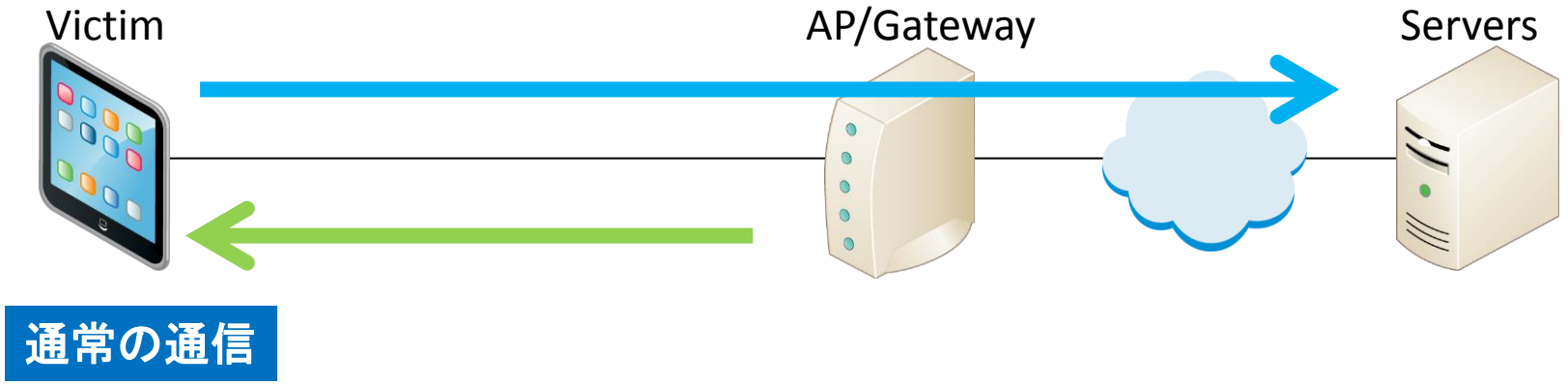
通常の通信



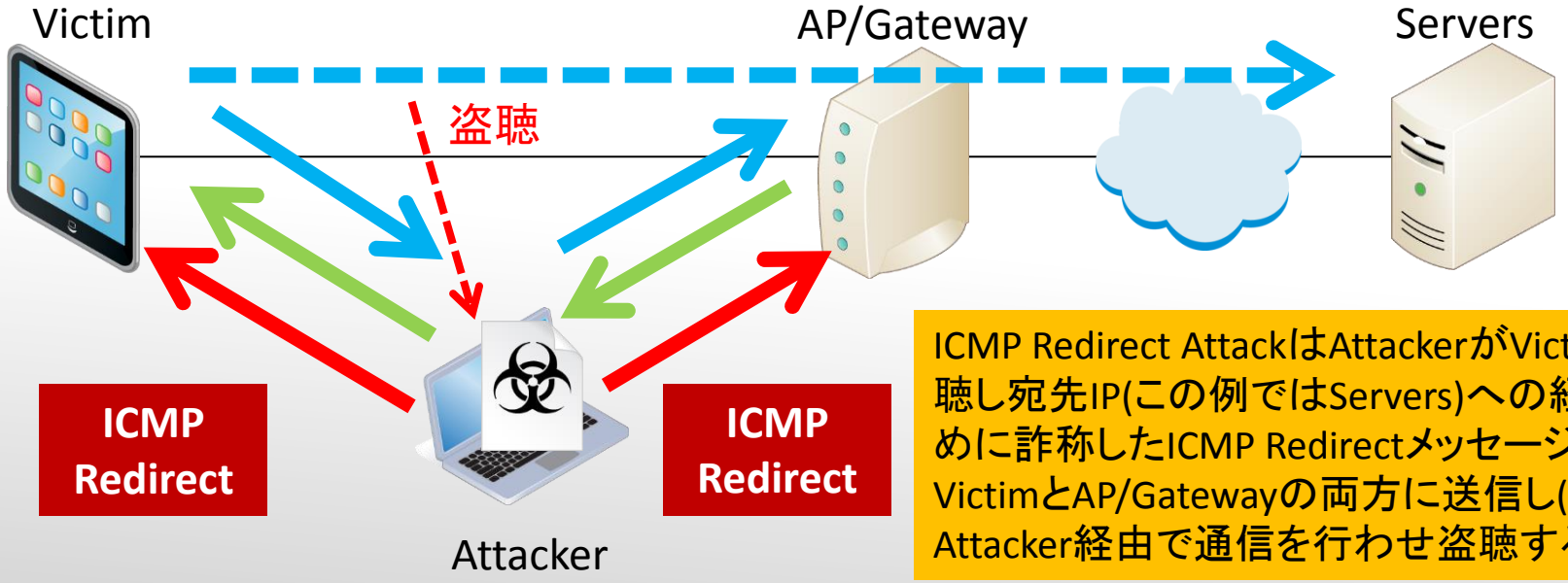
ARP Cash Poisoning

ARP (Cache) PoisoningはAttackerがARP ReplyをVictimに対してUnicast(Broadcast)で送信しArp Cacheを上書きする手法。通常はDefault GWのMACをAttackerのMACに詐称しAttackerのPC経由でDefault GWへ転送させる。

（参考）代表的な攻撃例: ICMPリダイレクト

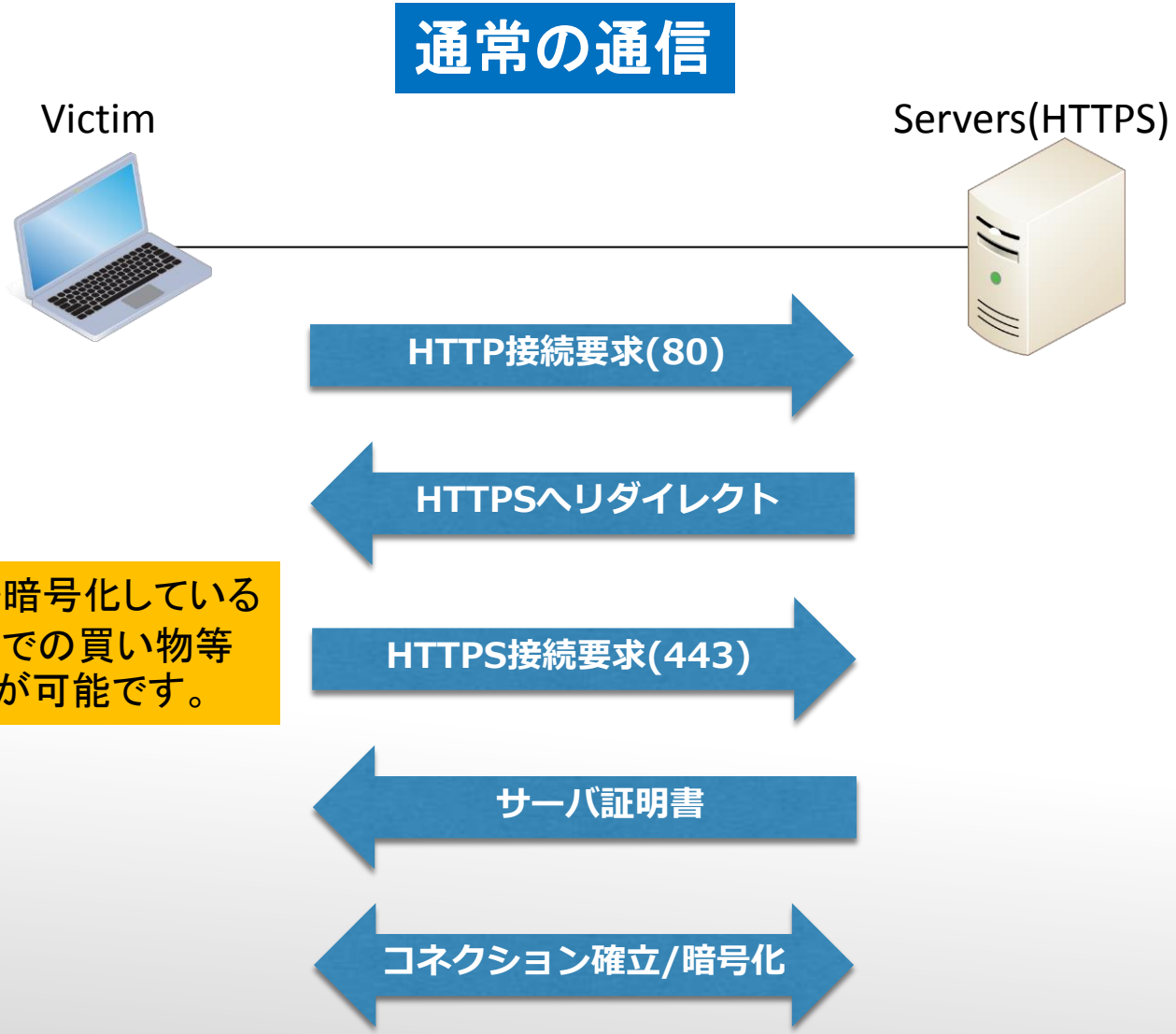


通常の通信



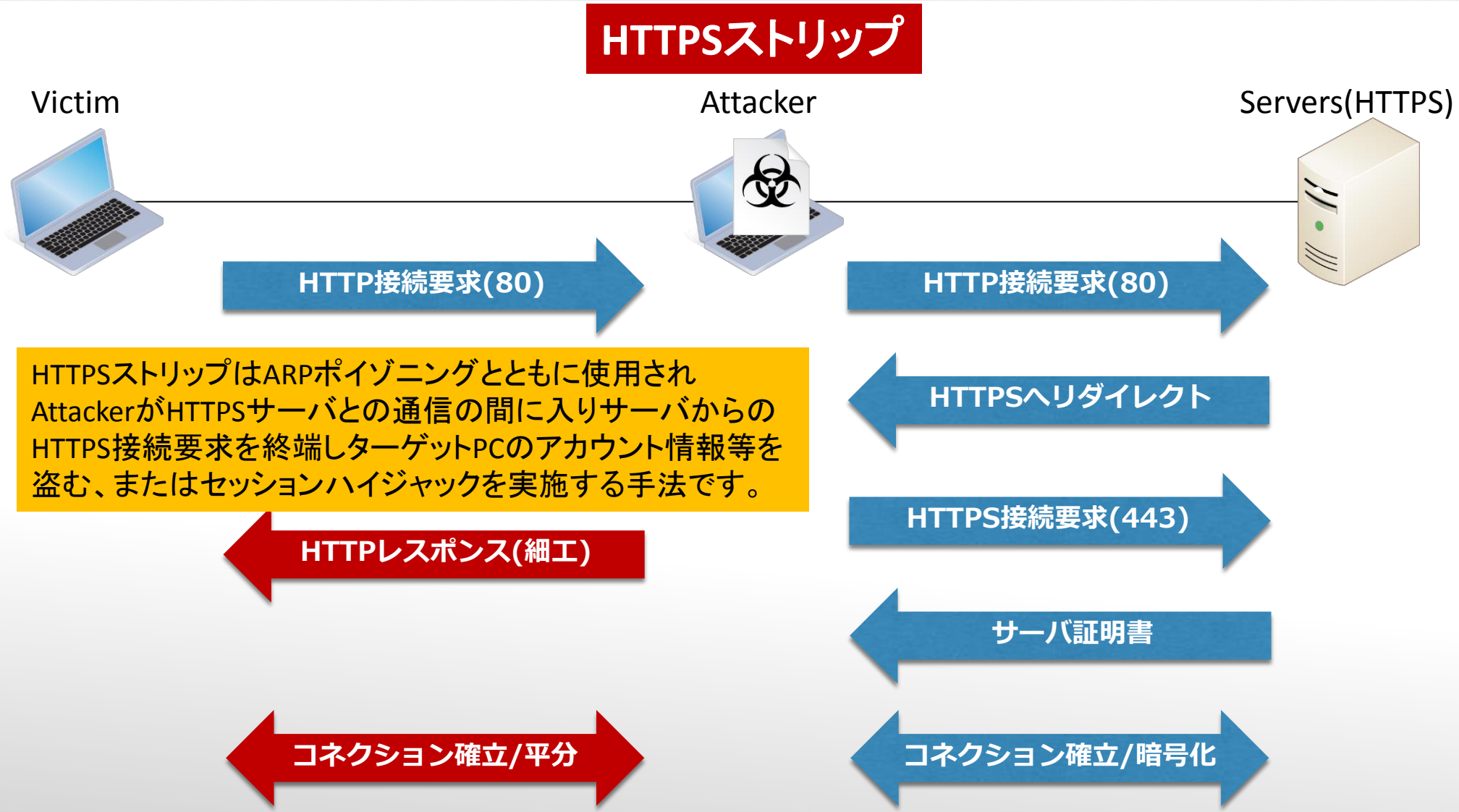
ICMP Redirect AttackはAttackerがVictimの通信を盗聴し宛先IP(この例ではServers)への経路を変えるために詐称したICMP Redirectメッセージ送信する手法。VictimとAP/Gatewayの両方に送信し(Double-Direct)、Attacker経由で通信を行わせ盗聴する。

（参考）代表的な攻撃例: HTTPSストリップ



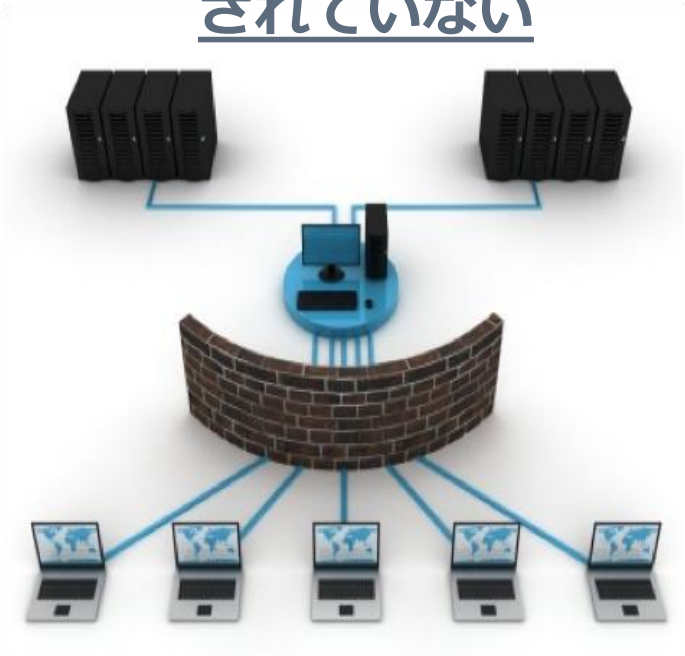
HTTPSでは通信内容を暗号化しているためショッピングサイトでの買い物等安全に通信を行うことが可能です。

（参考）代表的な攻撃例: HTTPS(SSL)ストリップ



従来のネットワーク向けセキュリティソリューションは あなたのモバイルユーザを完璧に防御できない

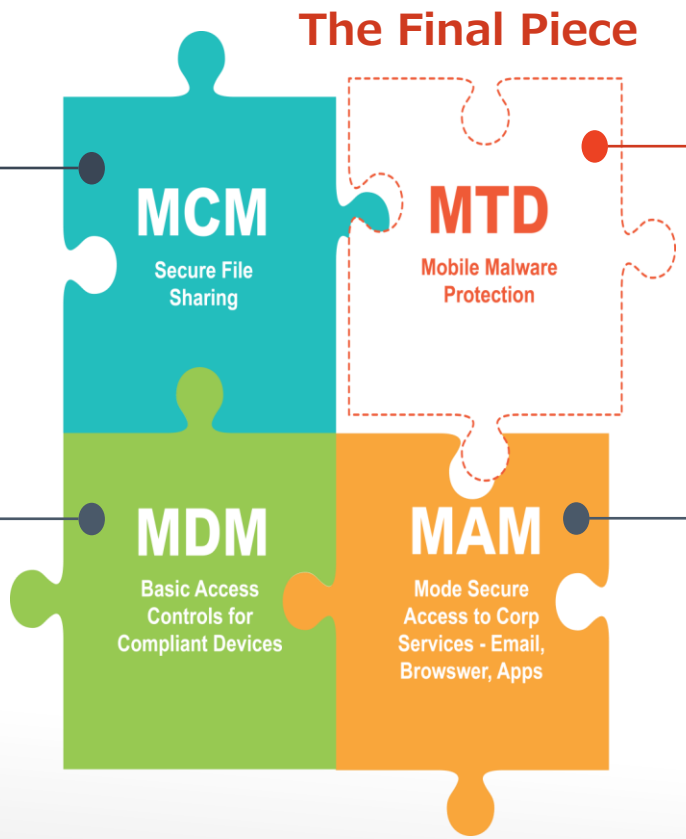
ネットワーク・セキュリティ ソリューション
モバイルに対してフォーカス されていない



MDM プロダクト
モバイルセキュリティ脅威を緩和 する為に、デザインされていない

まったく新しいコンセプトの セキュリティソリューションが必要

Zimperiumモバイル・セキュリティ・リスク防衛ソリューション
- モバイル・セキュリティ完成の為の最後の1ピース -



Mobile Content Management

文書の暗号化
Dropbox問題を解決

Mobile Device Management

許可、認可していないデバイスが業務ネットワークに接続されることを防止

ZIMPERIUM

Mobile Threat Defense

モバイルデバイスに当てられたMaliciousな攻撃を予見

Mobile App Management

業務アプリを包括制御（Wrap)する事で業務データがどこに送付されるかを制御

連携済みMDM製品の一例

CITRIX XenMobile　MobileIron　airwatch by vmware　Samsung Knox

Zimperium MTD
モバイル・セキュリティ・リスク防衛ソリューション

TOYO Corporation

Zimperium会社概要

本社：サンフランシスコ（米国）

開発拠点: テル・アビブ（イスラエル）

営業拠点：テキサス（米国）、バンガロー（インド）

社員: 約60名

<沿革>

2010　Zimperium創立

2012　イスラエルTOP５スタートアップカンパニーに選出される（Venture Beatによる）
　　イスラエルPrestigious スタートアップ2013に選出される

2013　World Mobile Congress 2013にて世界初のモバイル端末IPS「zIPS」を発表
　　Sierra VenturesとSamsungにより、＄8Mの投資

2014　iOSサポートの開始、Air WatchのMDMへのインテグレーションの実現
　　Shrider Mittalが新CEOに、Zuk AvrahamがChairmanに就任。.

2015　Telstraより＄12Mの投資。

SIERRA VENTURES

SAMSUNG

airwatch

Zimperiumモバイル・セキュリティ・リスク防衛ソリューション
iOSとAndoroidデバイスに対応

zIPS PROTECTION

モバイル端末をサイバーアタックから防御

ネットワークの脆弱性検証ツール

zCONSOLE MANAGEMENT

レポーティング
リスクベースのポリシマネージメント

ネットワークとホストベースの攻撃防御で特許取得。常に端末のバックグラウンドで動作

モバイル・セキュリティ・リスク防衛
業務ユーザ端末用Softwareアプリケーション

バックグラウンドで**常に**防御
強制終了はイベントとして検知

Known, Unknown
に依存しない検知アルゴリズム

端末に依存しない
iOSと **Android** 両方の
プラットフォームに対応

DPI技術を使わないため
消費電力やリソースの消費を低減

振る舞いベース検知はユーザモードで動作(root化の必要なし)

ホストベース、ネットワークベース、ブラウザからの攻撃を防御

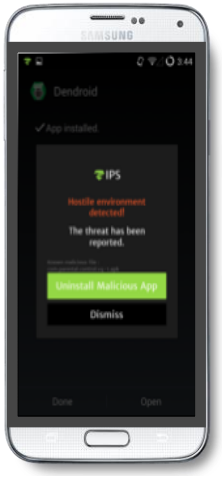
脅威検知・防御機能

iOS/Android端末共通

- Man-in-the-middle
(MITM／中間者攻撃)
- SSLストリップ
- Reconnaissanceスキャン
(ARP/TCPスキャンなど)
- 不正アクセスポイント
- 不正基地局／フェムトセル

Android端末のみ

- シグネチャ検知
(40社を超えるデータベース)
- ペイロードのダウンロード、実行
- マリシャス・アプリケーション
- 感染／マリシャス・ファイル
- 不正アプリケーション
- リモートアクセス・Trojans



Zimperiumモバイル・セキュリティ・リスク防衛ソリューション
iOSとAndoroidデバイスに対応

zIPS PROTECTION　モバイル端末をサイバーアタックから防御

ネットワークの脆弱性検証ツール

zCONSOLE MANAGEMENT

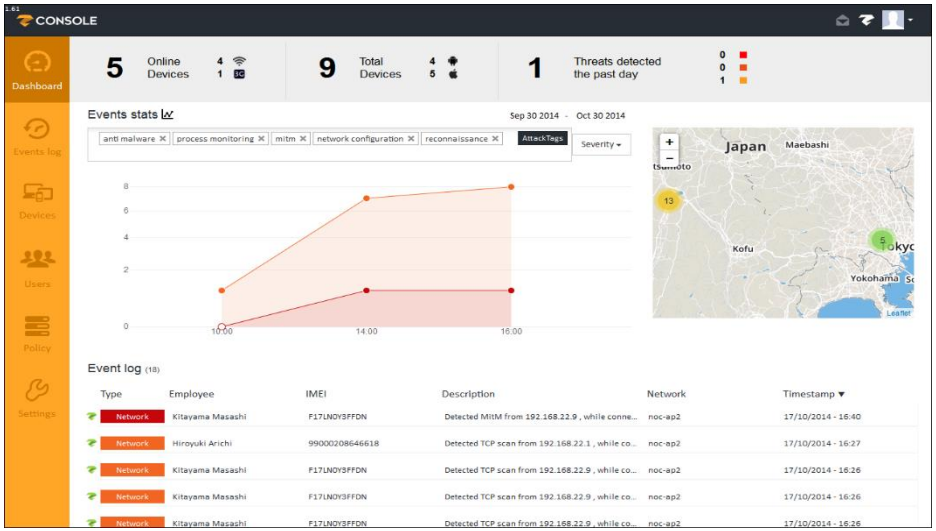
レポーティング
リスクベースのポリシマネージメント

ネットワークとホストベースの攻撃防御で特許取得。常に端末のバックグラウンドで動作

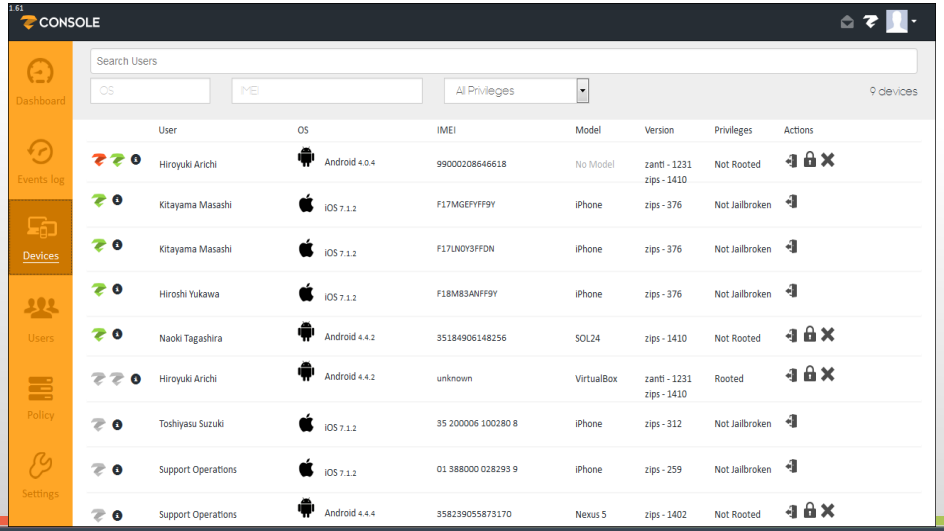
zCONSOLE MANAGEMENT

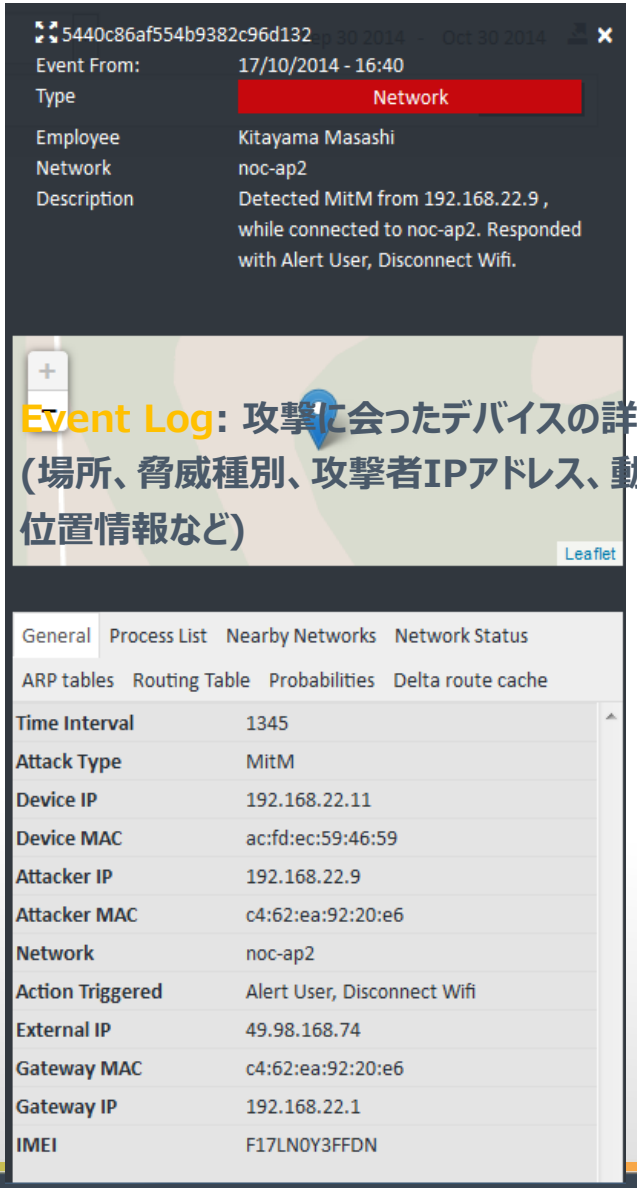
管理者用画面

Dashboard: 脅威のリストと詳細をデバイスごとに表示



Devices: 所有者とデバイス情報を表示(OS、バージョン)



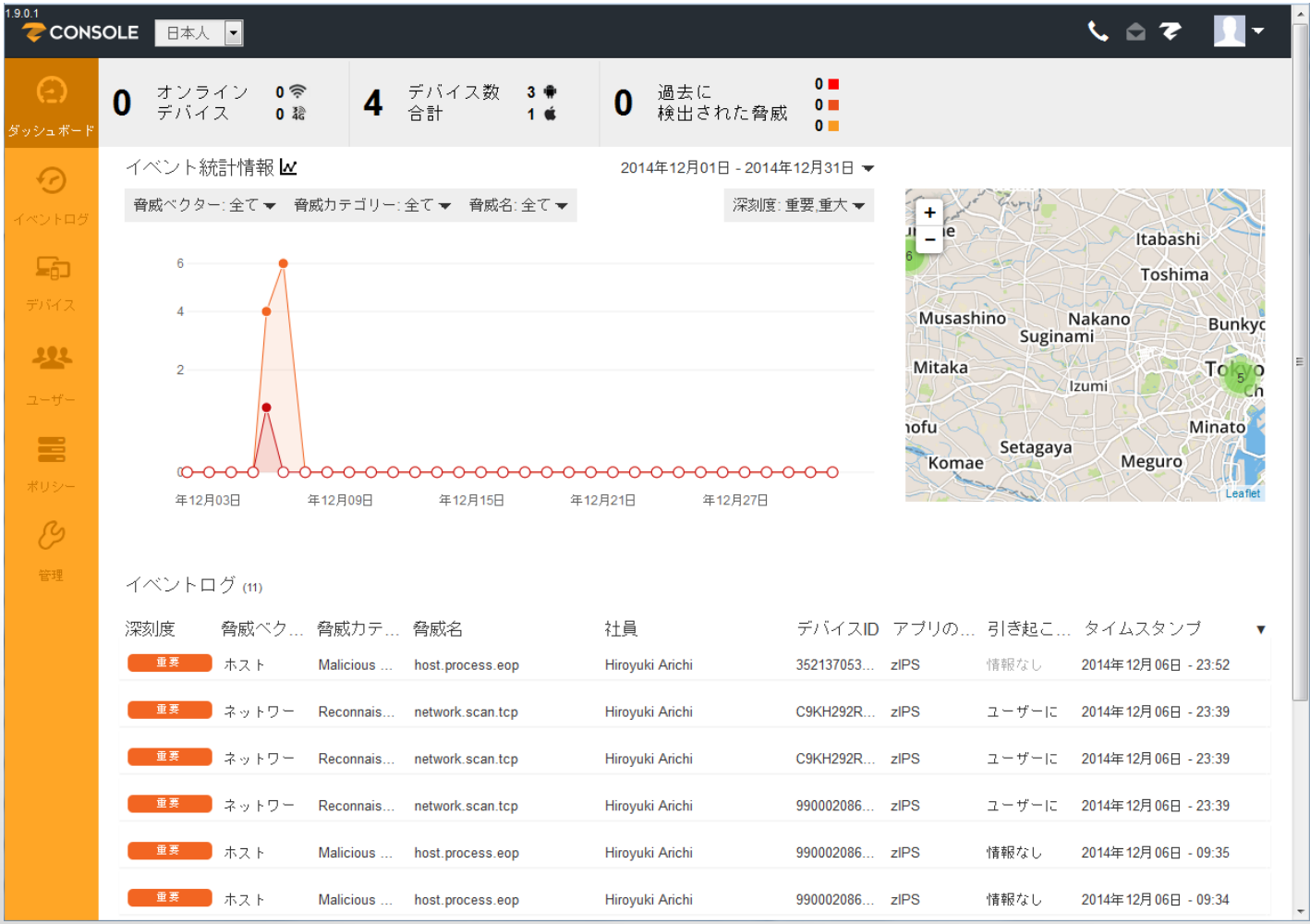


Event Log: 攻撃に会ったデバイスの詳細情報を表示(場所、脅威種別、攻撃者IPアドレス、動作プロセス一覧、位置情報など)

日本語化対応済み

zIPS PROTECTION

zCONSOLE MANAGEMENT



zIPSトライアルライセンス配布中

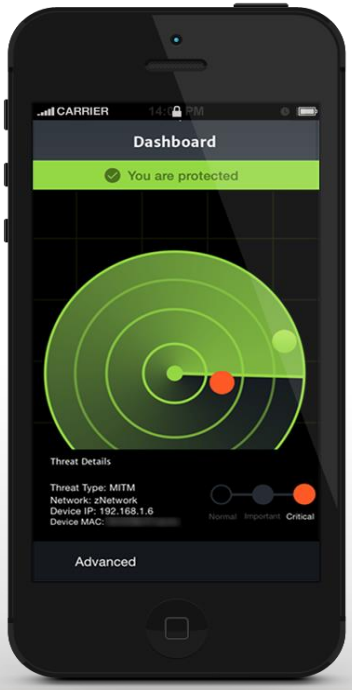
ただ今zIPSの2週間限定フリーライセンスの配布を実施中です。
ご希望の方はアカウント情報をお配りしますので下記「お問い合わせ先」までご連絡ください。

＜zIPS導入手順＞

1.右のＱＲコードより、Google playのzIPSをインストールしてください。
2.インストール後、アカウント入力画面にて、アカウントとパスワードを入力してください。
3.zIPSが開きましたら、アクティベート成功です。

＜zIPS操作・表示画面について＞

1.「詳細設定」タブより検出した脅威のインシデントログを確認することができます。
2.「重大/重要/普通」など、端末が受けた脅威の深刻度によって表示されるメッセージが異なります。
3.「重大/重要」レベルの脅威を受けた場合、接続しているWi-Fiを自動的に切断し、脅威から端末を守ります。再度Wi-Fiを利用される場合は、マニュアルで再接続をお願い致します。
※トライアルライセンスのデフォルト設定であり、設定変更をすることは出来ません。



＜ご注意事項＞

※トライアルライセンスは、Androidのみとさせて頂いております。
※本トライアルライセンスではプライバシを考慮し、端末の位置情報取得機能をオフとさせて頂きます。
※本トライアルライセンスは、2週間限定です。期間終了後は使用出来なくなります。
トライアル期間中、利用上のお問い合わせについては下記にて受付しております。
トライアル期間後の継続使用のご要望につきましても、下記までお問い合わせ下さい。

お問い合わせ先：東陽テクニカ　情報通信システム営業部　CyberSec_PJ@toyo.co.jp
直通電話番号：03-3245-1250(9:30～17:30)

モバイル・セキュリティ・リスク防衛ソリューション（MTD)
Zimperium, Inc

ありがとうございました

問い合わせ先： 03－3245－1245
CyberSec_PJ@toyo.co.jp