プレスリリース
2014 年 9 月 19 日
独立行政法人情報処理推進機構

注意喚起

# HTTPS で通信する Android アプリの開発者は SSL サーバー証明書の検証処理の実装を

～米国CERT/CC (*1) が脆弱性のある 617 のAndroidアプリを指摘 (*2)。今後さらに指摘される見込み～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）セキュリティセンターは、米国の CERT/CC が 2014 年 9 月 3 日、複数の Android アプリに「SSL 証明書を適切に検証しない脆弱性」を確認したとの発表を受け、Android アプリ開発者に対して注意喚起を発することとしました。

HTTPS（HTTP over SSL/TLS）でサーバーと通信する Android アプリは、HTTPS 通信の開始時に通信先から送信された SSL サーバー証明書が適切か検証する必要があります。本来、HTTPS 通信では、利用者とウェブサイトの通信経路上に攻撃者が割り込み、通信内容を盗聴したり改ざんしようとする攻撃（中間者攻撃）を防ぐことができます。しかし、開発者が提供する Android アプリが「SSL サーバー証明書を適切に検証」していない場合、中間者攻撃を防ぐことができず、攻撃者に HTTPS 通信の内容を盗聴または改ざんされる可能性があります。

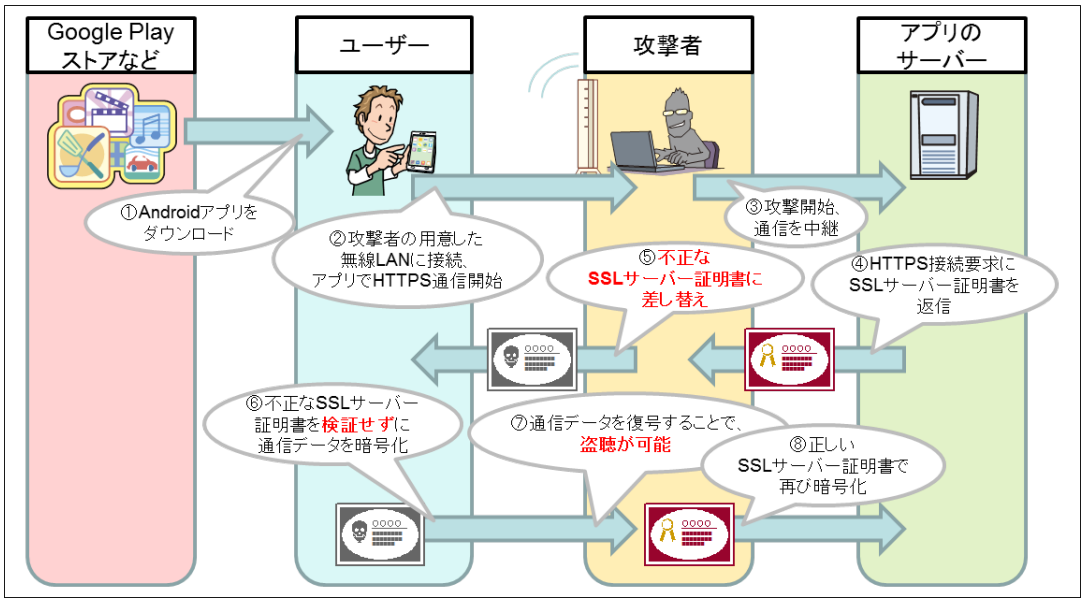

図 1：中間者攻撃により不正な SSL サーバー証明書を用いて盗聴されるイメージ

## CERT/CC は、大規模な調査を継続中。脆弱性のある Android アプリは速やかに修正を

米国のCERT/CCは 2014 年 9 月 3 日（米国時間）、複数のAndroidアプリに「SSL証明書を適切に検証しない脆弱性」があったとの調査結果を発表しました（注意喚起 VU#582497 (*3)、日本語版 JVNVU#90369988 (*4)）。CERT/CCは本脆弱性があるAndroidアプリ開発者への通知およびリストの公表を行っており、9 月 18 日時点でリストには複数の日本語名のアプリを含む 617 のアプリが記載されています。CERT/CCは自動化された大規模な調査を継続中であり、今後も公表されるアプリが増える見込みです。

(*1) CERT/CC (CERT Coordination Center) は、インターネットセキュリティの問題に対処するための機関
(*2) Android application SSL spreadsheet（米国時間 2014 年 9 月 18 日 0 時時点で 617 件公表あり）
https://docs.google.com/spreadsheets/d/1t5GXwjw82SyunALVJb2w0zi3FoLRIkfGPc7AMjRF0r4/edit?usp=sharing
(*3) VU#582497 Multiple Android applications fail to properly validate SSL certificates
http://www.kb.cert.org/vuls/id/582497
(*4) JVNVU#90369988 複数の Android アプリに SSL 証明書を適切に検証しない脆弱性（過去に修正され JVN で公表された 13 件のリストを記載あり）https://jvn.jp/vu/JVNVU90369988/

■**開発者向け対策：「SSL サーバー証明書を用いた検証を実装する」**

CERT/CC からの通知の有無にかかわらず、**HTTPS 通信を行う Android アプリの開発者は、提供する Android アプリに「SSL 証明書を適切に検証しない脆弱性」の有無について点検を行い、脆弱性があれば速やかに修正しアップデートを公開**してください。

なお、IPA では、Android アプリの脆弱性の学習・点検ツール「AnCoLe」を無償提供しています。AnCoLe を用いることで、ソースコードに「SSL 証明書を適切に検証しない脆弱性」（SSL 通信の実装不備）が無いか、点検が行えます。

Android アプリの脆弱性の学習・点検ツール AnCoLe
https://www.ipa.go.jp/security/vuln/ancole/index.html

具体的な実装方法については、以下の資料に解説されていますのでご参照ください。

JSSEC「Android アプリのセキュア設計・セキュアコーディングガイド」
http://www.jssec.org/report/securecoding.html

また、この脆弱性は Windows や iOS のアプリにも存在する可能性があります。Android アプリに限らず、サーバーとの HTTPS 通信を行うアプリケーションを提供する開発者は、アプリケーションの HTTPS 通信の開始時には SSL サーバー証明書の検証処理を実装してください。

■**利用者向け対策：「アップデートを適用した Android アプリを使用する」**

本脆弱性は Android アプリ開発者が対策する必要があります。Android アプリ利用者は、開発者から提供されるアップデートがあれば、速やかに適用して、常に最新の状態で Android アプリを使用してください。

また、一般的に本脆弱性を悪用した Android アプリへの中間者攻撃は、攻撃者が用意した無線 LAN 環境を介して行われます。以下の情報などをご参照いただき、無線 LAN の安全な利用を心がけてください。

総務省「Wi-Fi（無線 LAN）の安全な利用について」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html
総務省「Wi-Fi 利用者向け 簡易マニュアル」（PDF）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_Users.pdf

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター 中西／谷口
Tel： 03-5978-7527 Fax： 03-5978-7518 E-mail： vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ 横山／白石
Tel： 03-5978-7503 Fax： 03-5978-7510 E-mail： pr-inq@ipa.go.jp