NTT DATA
Global IT Innovator

【緊急レポート】
KRACKs <key reinstallation attacks：鍵再インストール攻撃> について

NTTデータ先端技術株式会社
（IL-CSIRT）

© 2017 NTT DATA INTELLILINK Corporation

はじめに

2017年10月16日、ベルギーの研究者であるMathy Vanhoef氏が、無線LAN(以下、Wi-Fi)の認証プロトコルに複数の脆弱性があることをWebサイト(https://www.krackattacks.com/)で公表しました。

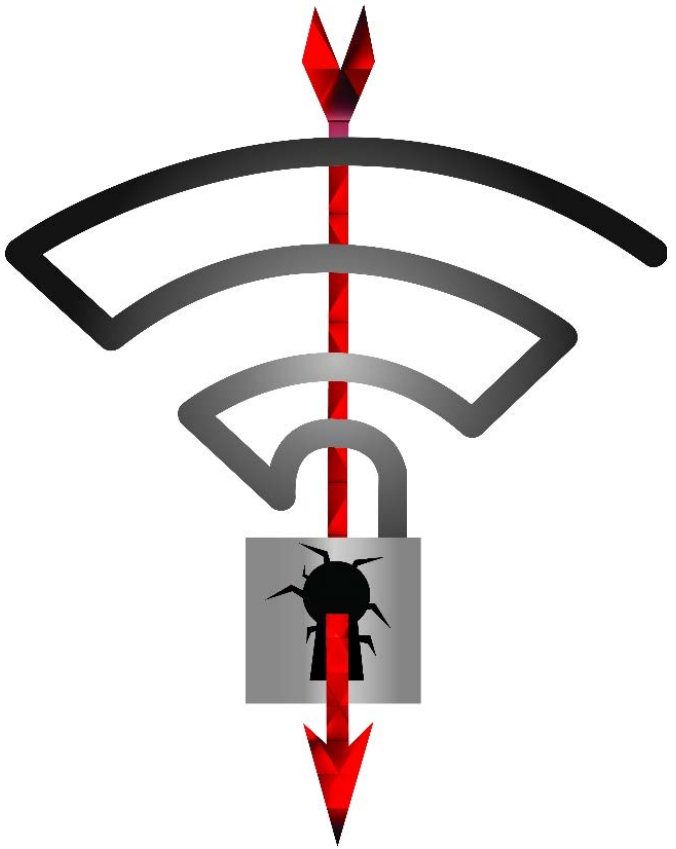
Vanhoef氏は、これら一連の脆弱性および攻撃手法の詳細を、2017年12月にイギリスで開催されるBlack Hat Europe 2017で明らかにするとしています。

本レポートは、2017年10月18日時点で明らかになっている情報に基づき、想定される脅威と現在考えられる対策について、IL-CSIRTの見解を示すものです。

© 2017 NTT DATA INTELLILINK Corporation

INDEX

1. KRACKs
2. 脆弱性概要
3. 対象CVE
4. 現状考えられる対策



"Key Reinstallation Attacks" by Mathy Vanhoef, licensed under CC BY 4.0.
https://creativecommons.org/licenses/by/4.0/

© 2017 NTT DATA INTELLILINK Corporation

NTT DATA
NTTデータ 先端技術株式会社

1. KRACKs

Mathy Vanhoef氏が公表した一連の脆弱性は、Wi-Fiの認証プロトコルであるWPA/WPA2の「4-way handshake」などの仕様に起因するものです。Mathy Vanhoef氏は、これらの脆弱性をつく攻撃手法を **KRACKs**（**K**ey **R**einstallation **A**tta**CKs**）と名付けました。

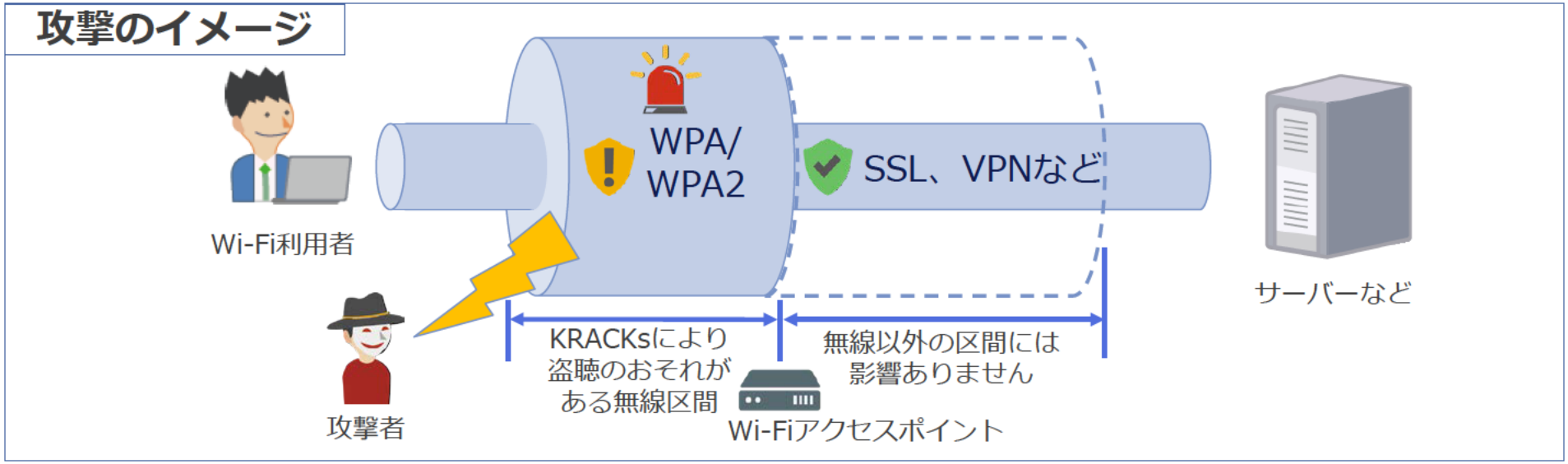
▽経緯

年月日	詳細
2017.5.19	Vanhoef氏より研究論文が提出される
2017.7頃	Vanhoef氏より米CERT/CCに脆弱性の情報が開示される
2017.8.28	米CERT/CCより複数の開発ベンダに通知が出される 開発ベンダによるセキュリティパッチの開発がスタート
2017.10.6	BlackhatのサイトにてWPA2の脆弱性に関する発表がある旨公開される
2017.10.16	WPA2の脆弱性(KRACKs)に関して情報が公開される
2017.12.4～7	Black Hat Europe 2017でKRACKsの詳細情報が公開される予定

© 2017 NTT DATA INTELLILINK Corporation

1. KRACKs

▽KRACKsがもたらす脅威
　攻撃者が、脆弱性のあるWi-Fiネットワークの電波を受信できる場合、KRACKsの攻撃手法を使ってWPA/WPA2プロトコルの暗号化を解読して**Wi-Fiの通信内容を復号・盗聴することが可能**となります。



※攻撃者が復号・盗聴できる通信はあくまで「暗号化されたWi-Fiの通信」です。利用者からサーバーまでの経路がSSLやVPNなどで暗号化されていれば、Webサイト閲覧などのデータがKRACKsによって直接盗み見られることはありません。

© 2017 NTT DATA INTELLILINK Corporation

1. KRACKs

【参考】WPA2、WPAとWEP

　WPA2は、IEEEが策定したWi-Fiの認証プロトコルの実装の一つで、Wi-Fiネットワークを設置する際に広く採用されています。 WPA2はWPAやWEPといった他の認証プロトコルよりも堅固なため、一般的にWPA2を採用することが推奨されています。
WEPはKRACKsの攻撃対象外ですが、WEPは既に破られ解読可能な認証プロトコルであるため、KRACKs対策としてWEPを採用すべきではありません。

※本レポートでは、一般家庭や小規模な企業などのWi-Fiネットワークで使用されるWPA2-Personal（WPA2-PSK）を想定して記述しています。

© 2017 NTT DATA INTELLILINK Corporation

NTT DATA
NTTデータ 先端技術株式会社

2. 脆弱性概要

▽対象機器

・WPA/WPA2をサポートするすべてのWi-Fi機器

- WPA/WPA2の仕様に関する脆弱性となり、特定の機器やOS・ソフトウェアに限らず広範囲に影響が及びます。
- 主に影響を受ける対象はクライアント側とされていますが、AP側も影響を受ける可能性があります。

▽盗み見られる情報

・クライアント⇔APで電波を使って通信する間の平文情報

- クライアント⇔AP間で電波を使って通信する間の暗号が解読されたことにより、HTTP通信など平文で情報を受け渡している場合、攻撃者に通信の内容を盗み見られる可能性があります。
- SSL通信やVPNを使用している場合、本脆弱性のみで通信の内容が盗み見られることはありません。

▽悪用のための条件

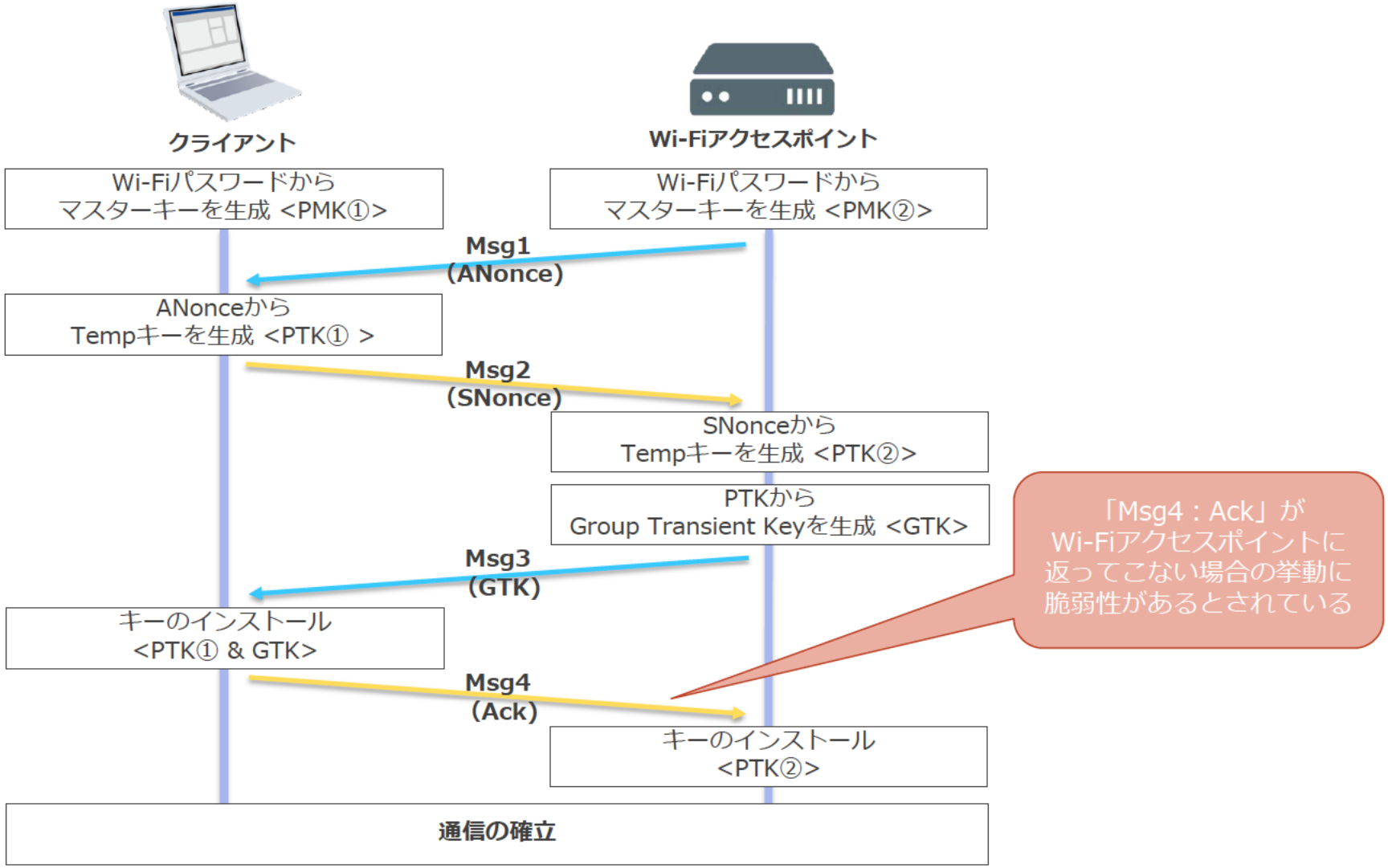
・攻撃者が電波の届く範囲にアクセス可能

- 電波の届く範囲でのみ利用可能な脆弱性となります。
  ※無線以外のネットワーク経由で攻撃されることはありません。
  ※現状明らかになっていませんが、中間者攻撃を行う場合はクライアント、AP両方の電波の届く範囲にいる必要があると推測されます。

© 2017 NTT DATA INTELLILINK Corporation

2. 脆弱性概要

▽脆弱性悪用フロー（4-Way HandShakeの場合の悪用）



© 2017 NTT DATA INTELLILINK Corporation

NTT DATA
NTTデータ 先端技術株式会社

3. 対象CVE

▽KRACKs関連の脆弱性一覧

CVE番号	CVSS (Ver3.0)		概要
	Base	Temp	
CVE-2017-13077	6.8	-	4way Handshakeにおけるペア暗号鍵(PTK-TK)の再インストール
CVE-2017-13078	-	-	4way Handshakeでのグループ鍵(GTK)の再インストール
CVE-2017-13079	-	-	4way Handshakeにおける整合性グループ鍵(IGTK)の再インストール
CVE-2017-13080	-	-	Group Key Handshakeにおけるグループ鍵(GTK)の再インストール
CVE-2017-13081	-	-	Group Key Handshakeにおける整合性グループ鍵(IGTK)の再インストール
CVE-2017-13082	-	-	再送されたFast BSS Transition Reassociation Requestの受け入れと、その処理におけるペア暗号鍵(PTK-TK)の再インストール
CVE-2017-13084	-	-	PeerKey HandshakeにおけるSTK鍵の再インストール
CVE-2017-13086	-	-	TDLS HandshakeにおけるTunneled Direct-Link Setup(TDLS) PeerKey(TPK)の再インストール
CVE-2017-13087	-	-	ワイヤレスネットワーク管理(WNM)スリープモードレスポンスフレームを処理する際のグループ鍵(GTK)の再インストール
CVE-2017-13088	-	-	ワイヤレスネットワーク管理(WNM)スリープモードレスポンスフレームを処理する際の整合性グループ鍵(IGTK)の再インストール

※「-」表記となっている箇所は2017.10.18現在非公開

© 2017 NTT DATA INTELLILINK Corporation

4. 現状考えられる対策

2017年５月頃から本脆弱性に関する情報が開示され、本レポート公開時点で開発ベンダー各社からパッチの作成や配信が開始されています。ただし本脆弱性はWPA/WPA2の仕様上の脆弱性であり、WPA/WPA2をサポートするすべての機器が影響を受けるため、対策が行き届くまでには相当の時間を要することが予想されます。

▽対策方法

・OS/機器ベンダー提供のパッチ適用/バージョンアップを行う
  - 主にクライアント側のパッチがリリースされています。
  - 一部のWi-Fi中継機器のようにAPであってもクライアントとしても動作するものやローミングのプロトコルである802.11rに対応している機器は、その機能の停止やパッチ適用が必要です。
  - OSやドライバーに依存せず、チップセットの機能だけで通信ができる機能を持つ製品についてはファームウェアの更新も必要な場合があります。

・VPNやSSLなど通信の暗号化を行い盗聴を防ぐ
  - 電波を使って通信している間の暗号が解読されただけで、その中身であるクライアント⇔サーバ間の暗号がすぐに解読できるわけではありません。
  - 一般的な公衆Wi-Fi利用時と同じレベルで情報セキュリティに気を配っておくことで、多くの危険を回避できます。

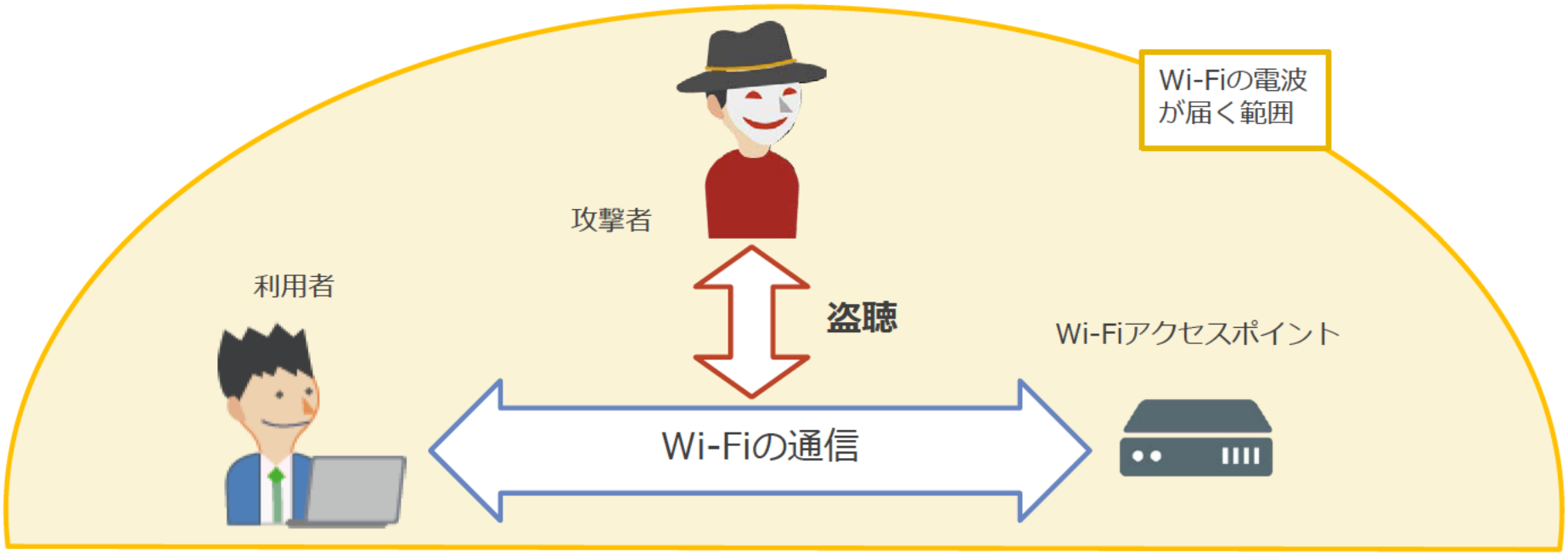
© 2017 NTT DATA INTELLILINK Corporation

4. 現状考えられる対策

▽対策方法(つづき)

・電波の届く範囲を最小限とする

- 電波の届く範囲でのみ利用可能な脆弱性のため、出力調整等が可能な機器では電波の到達範囲を「必要最小限にする」「物理的にアクセスが制限できる範囲に限る」などの手法も併用してリスクを低減してください。



© 2017 NTT DATA INTELLILINK Corporation

4. 現状考えられる対策

▽注意

- 脆弱性対策を行わない状態であってもWEPよりはセキュアであるため、WPA/WPA2の使用を継続することを推奨します。
- 詳細が公開された結果、中間者攻撃も想定される脆弱性であると判明した場合、接続先のAPが正しいことやサーバー類の証明書が正規のものである確認をしっかり行うことが重要となります。

▽主なベンダパッチ配布状況(2017.10.18現在)

ベンダ	状況
Windows	2017.10パッチ配布済み (CVE-2017-13080)
Linux(RHEL)	2017.10.18 パッチ配布済み (RHSA-2017:2907 - Security Advisory)
Apple(macOS, iOS)	macOS,iOS,tvOS,watchOSのベータ版では既に脆弱性が修正されており、数週間以内でのリリース待ち
Google(Android)※	問題を認識しており、影響を受けるデバイスに対するパッチを数週間のうちに発行する予定

※Googleのパッチ発行から、各メーカーの端末に適合したパッチ配布開始までは長期間掛かる可能性があります。提供元の通信キャリアやメーカーの情報をご確認ください。

© 2017 NTT DATA INTELLILINK Corporation

情報ソース

▽一次情報
・Key Reinstallation Attacks
<https://www.krackattacks.com/>
・KEY REINSTALLATION ATTACKS: BREAKING THE WPA2 PROTOCOL
<https://www.blackhat.com/eu-17/briefings/schedule/#key-reinstallation-attacks-breaking-the-wpa2-protocol-8861>

▽注意喚起
・Vulnerability Note VU#228519 Wi-Fi Protected Access II (WPA2) handshake traffic can be manipulated to induce nonce and session key reuse
<https://www.kb.cert.org/vuls/id/228519/>
・JVNVU#90609033　Wi-Fi Protected Access II (WPA2) ハンドシェイクにおいて Nonce およびセッション鍵が再利用される問題
<https://jvn.jp/vu/JVNVU90609033/>
・WPA2 における複数の脆弱性について
<https://www.ipa.go.jp/security/ciadr/vul/20171017_WPA2.html>
・無線LAN（Wi-Fi）暗号化における脆弱性について（注意喚起）
<http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000274.html>
・Wi-Fi Alliance® security update
<https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-security-update>

© 2017 NTT DATA INTELLILINK Corporation

NTT DATA

Global IT Innovator

© 2017 NTT DATA INTELLILINK Corporation