Wi-BiZ
無線LANビジネス推進連絡会

資料18-2

# 公衆無線LANのセキュリティに関して

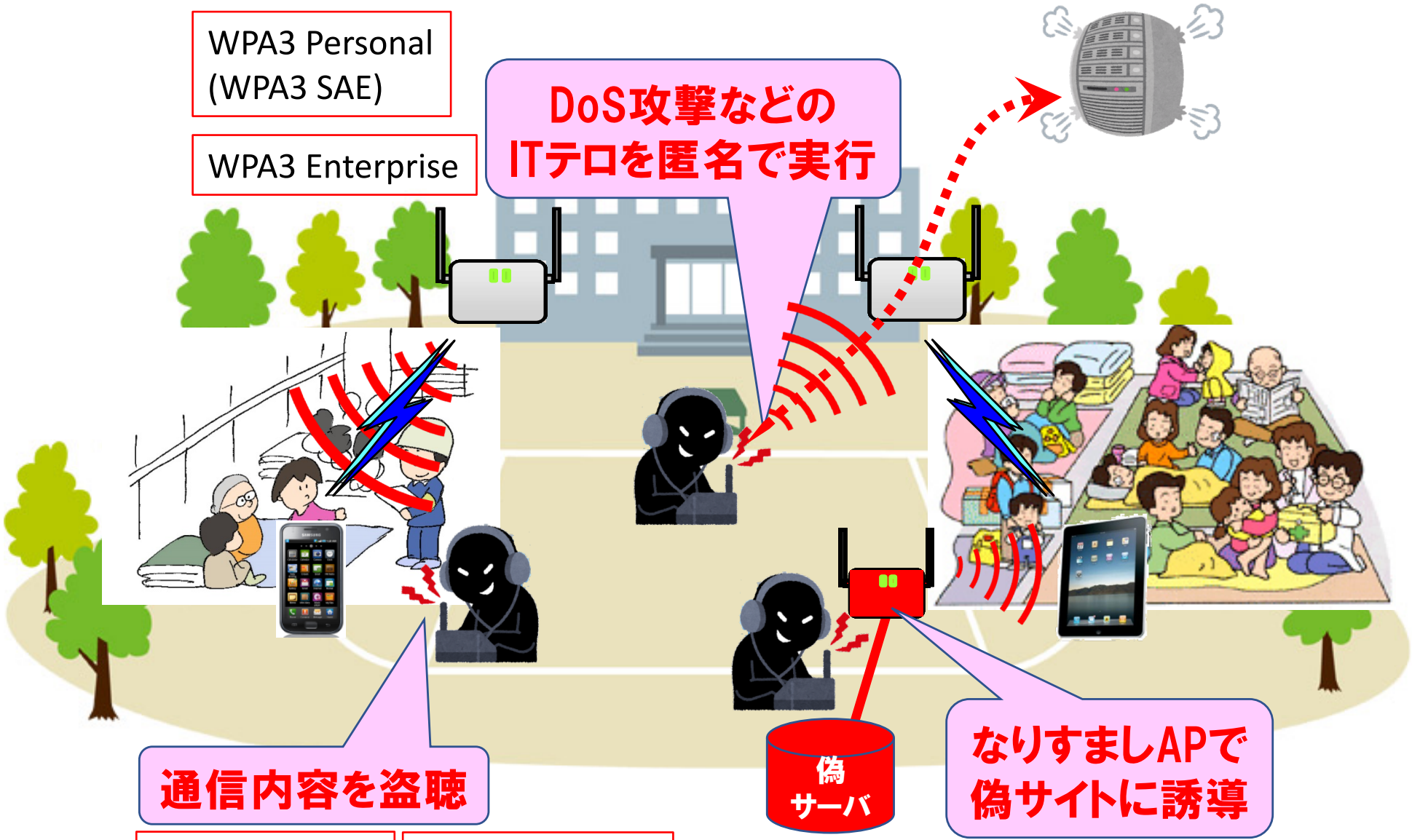
2019年12月5日
無線LANビジネス推進連絡会
技術・調査委員会

# Wi-Fiにおける最近のセキュリティ・トピック

- WPA3
- Enhanced Open

| 新しい認定 | 現在の認定 | 主な特徴 | 追加機能の扱い |
|---|---|---|---|
| WPA3 Personal (WPA3 SAE) | WPA2 Personal (WPA2 PSK) | PSKモードをSAEで強化しオフラインの辞書攻撃への耐性 | WPA3の必須要件 |
| WPA3 Enterprise | WPA2 Enterprise | 192ビットCNSAを導入し、暗号の組合せの一貫性 | CNSAはオプション |
| Enhanced Open | なし | オープンネットワークをOWEにより暗号化 | WPA3とは別認定でオプション |

# 公衆無線LANのセキュリティ・リスク




WPA3 Personal
(WPA3 SAE)

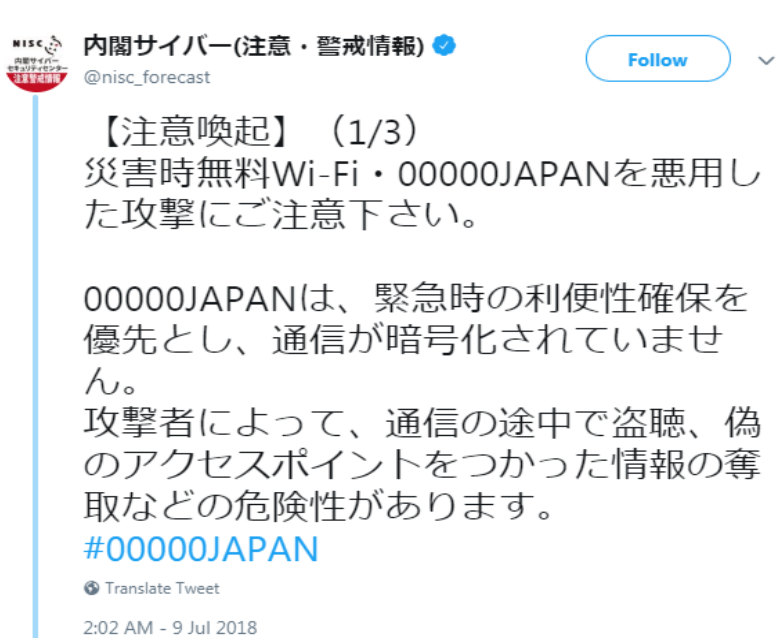
Enhanced Open

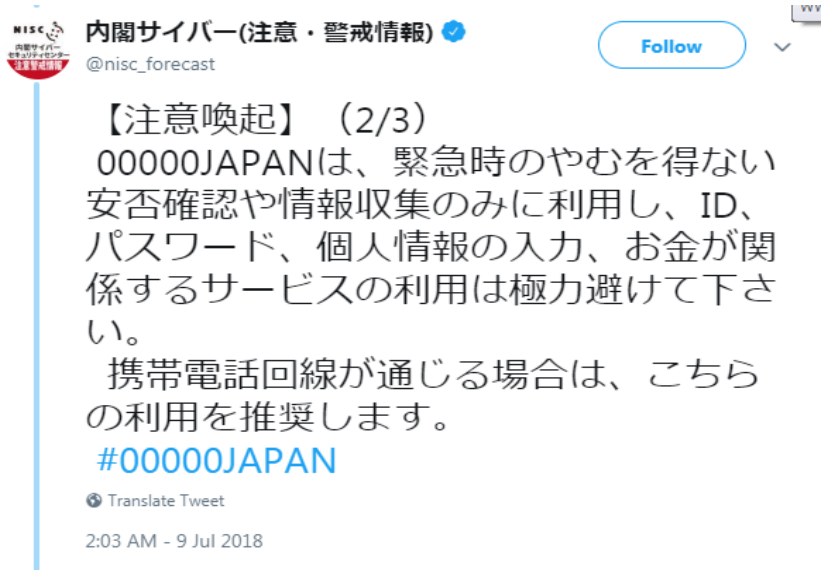
* APおよび端末の対応が必要になります

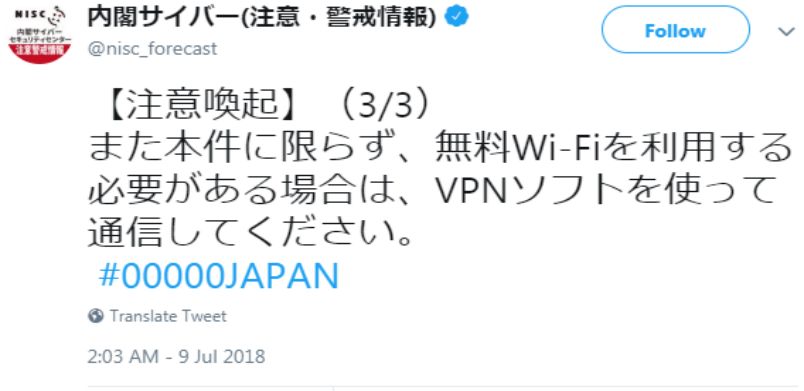
Wi-BiZ
無線LANビジネス推進連絡会

# セキュリティの課題

## 「00000JAPAN」に対する内閣サイバーセキュリティセンターのコメント



# ■公衆無線LANのリスク

- ➢通信を盗聴されるリスクがある
  - ①端末 – AP間が暗号化されていない
  - ②詐称されたAPで通信を抜かれる

# ■リスクに対する一般的な対処

| | 端末－AP間が暗号化されていない | 詐称されたAPで通信を抜かれる | 備考 |
|---|---|---|---|
| 暗号化されたWi-Fiを利用する(PSK) | △ | X | 公衆サービス等でPSKが開示されている場合はリスク |
| 暗号化されたWi-Fiを利用する(Enterprise) | ○ | ○ | 要認証 |
| 暗号化されたWi-Fiを利用する(Enhaced Open) | ○ | X | |
| HTTPS / TLSを利用する | ○ | ○ | 証明書とサイトの偽造には効果ない |
| VPNを利用する | ○ | ○ | VPNプロバダーの信頼性に依存 |

【表１】

■ リスクに対処した具体的な例（１）

- Secured Wi-Fi(NTT BP) [EAP-Enterprise]
- ギガぞう(Wi2) [EAP-Enterprise, VPN]

⇒ いずれも公衆Wi-Fiサービスであるが、
会員向けサービス

- LinkNYC(NYC) [Passpoint]

⇒初回利用時に端末にEAP-Enterpriseの設定を実施

⇒いずれも事業者側のコスト増またはユーザ側へのコスト負担の発生

# ■ コスト増の具体例

## □ AP・サービスを提供する側

- Enhanced Openに対応するにはAPファームのバージョンアップもしくは対応APへの交換が必要
- WPA-Enterpriseを提供するには認証設備が準備と運用が必要（一部APシステムに認証機能を含むケースもあり）

## □ 利用者側

- Enhanced Openに対応するには対応端末もしくはファームウエアのバージョンアップが必要
- WPA-Enterpriseを利用するには端末に認証情報の登録が必要
- VPNサービスの加入（有償・無償）

■ リスクに対処した具体的な例（２）

- 公衆無線LANの利用者に公衆無線LANのセキュリティ対策の状況や自ら講じるべきセキュリティ対策を理解してもらう

また、約7割の利用者が公衆無線 LAN のセキュリティに「不安を感じている」と回答しており、約5割の利用者は、「不安を感じているが、利用する」と回答している。（図1－10）

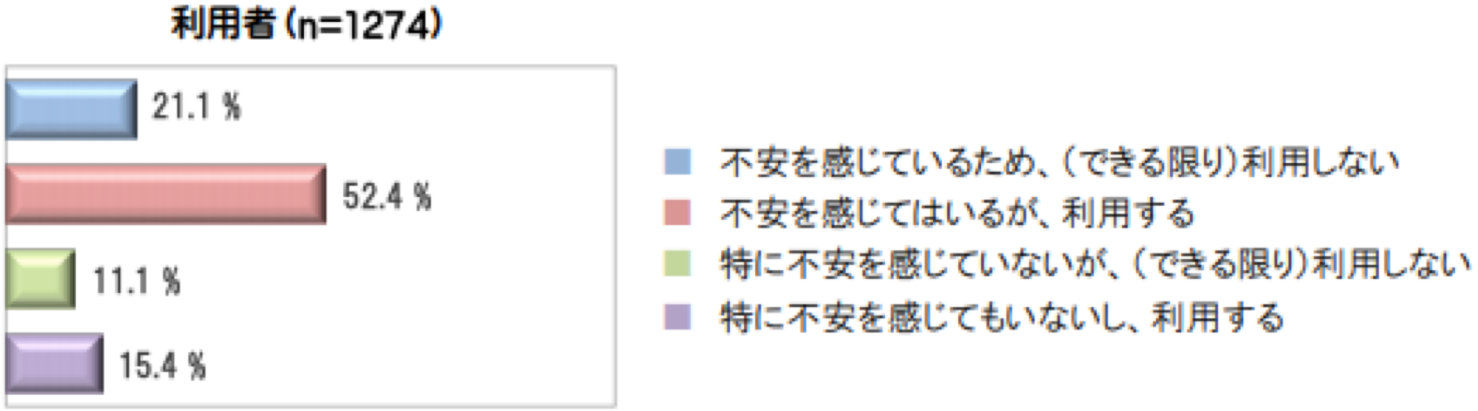



図1－10　利用者における公衆無線 LAN のセキュリティに関する意識

参考：公衆無線 LAN セキュリティ分科会報告書（2018/3） p13

# 各社の対応とユーザへの注意喚起

## 1. Wi-Bizホームページへの「ご利用上の注意点」の掲載

- 「00000JAPAN」は、大規模災害や深刻な災害等の緊急時に、被災地で誰でも使えるという利便性を確保するため、通信の暗号化等セキュリティへの対応は行っていません。
- 「00000JAPAN」のご利用は、緊急時の安否確認や情報収集にとどめるとともに、やむを得ずIDやパスワード等個人情報の入力、金融系のサービス等他の用途でご利用の場合は、HTTPSやVPN等自らセキュリティ対策を行って頂く必要があります。

## 2. 事業者による避難所ポスター、ホームページへの注意事項の掲載

- 総務省からの要請により、避難所掲示ポスターに注意事項を記載
（NTTドコモは当初より記載）
- 各社ホームページへ注意事項を掲載
（ソフトバンクは当初より掲載）

■ リスクに対処した具体的な例（再）
- 公衆無線LANの利用者に公衆無線LANのセキュリティ対策の状況や自ら講じるべきセキュリティ対策を理解してもらう

- リスクを伝えるだけではなく、便利につかってもらうユースケースの提供
- 利用時間、トラフィック量、利用者数の多いところでの周知（ポスター、テーブルサイン、キャプティブポータル等）[次項参考データ]
- httpsで正規のサイトにアクセスしていることの見分け方の周知

# ■ WiBizに頂いたご意見

【参考】

●Wi-Bizに問い合わせのあったご意見
・公衆サービスにおけるWPA2-PSKは、PSKが公開されているためリスクがあり結局httpsやVPNの対策が必要。
したがって、00000JAPANの記述について、「暗号化されていないので対策が必要」という表現は誤解を受ける。

・偽サーバへの誘導があった時には、httpsで正規のサイトにアクセスしていることが確認できないと意味がないので、見分け方の周知啓蒙が必要
（鍵マークとドメイン名など）