Orchestrating a brighter world

NEC

資料2－1

公衆無線LANを安全に使用する為の利用者の自衛手段について

2017年12月1日

日本電気株式会社

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

公衆無線LANにおける自衛可能な脅威

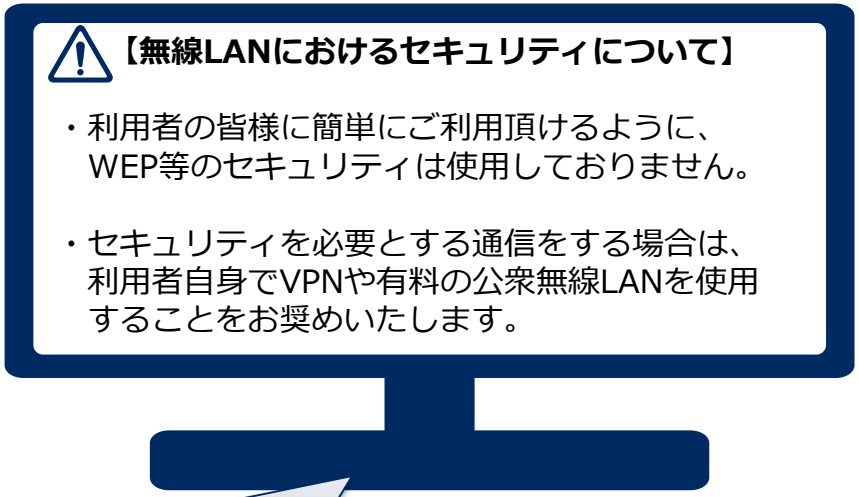
公衆無線LANは、セキュリティ対策を実装するより利用者の利便性を優先しているため、利用者はそのリスクを理解した上で自衛する必要がある

公衆無線LAN環境における一般的な脅威

盗聴 利用者間の通信を傍受し、窃用すること	**悪意のAP** 第三者が情報窃取など悪意のある目的で設置した、実在する正規のAPと同一のSSIDや暗号化キーを設定したAPのこと
不正目的でのインフラ利用 公衆無線LAN経由で掲示板への犯罪予告の書き込みや違法ダウンロードを実行すること	**なりすまし** 第三者が不正に情報入手し、正規の利用者や機器になりすまして不正にサービスを利用すること

利用者側で自衛可能

例）公衆無線LAN接続時の注意画面



利用者個人で対策を講じるよう注意喚起を実施

【参考】IPA 公衆無線 LAN 利用に係る脅威と対策
https://www.ipa.go.jp/files/000051453.pdf

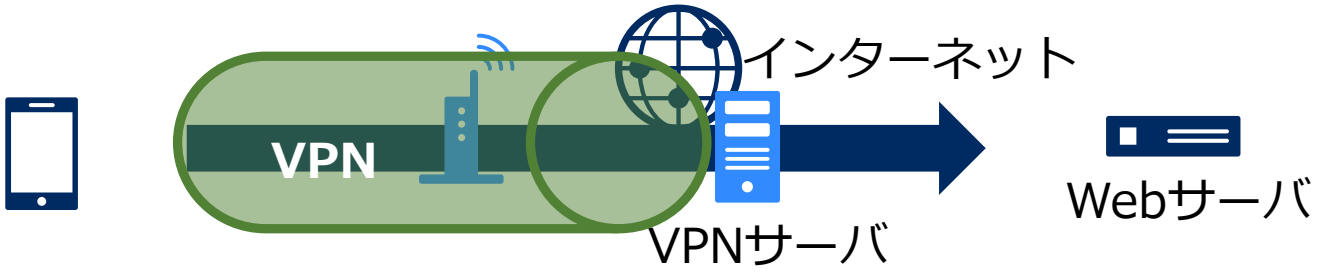
盗聴等の脅威に対するセキュリティ対策技術

公衆無線LANにおける、通信の盗聴、悪意のAP等の脅威への対処法として主に３つの手法が挙げられる

1. Passpoint™認定のアクセスポイント（AP）を使用

2. TLS/SSL通信を使用

3. VPNサービスを利用



Passpoint™認定のAPを用いる安全性確保の特徴

Passpoint™認定のAPを用いることで、端末・AP間の通信を安全にすることができる

- 端末がPasspoint™認定のAPが設置された公衆無線LANエリアに入ると、**ネットワークを自動で検知・認証し、接続が可能**
  - 認証はSIMカード等のユーザに紐づく情報をもとに行われる

- **Passpoint™認定APの設置が必要**

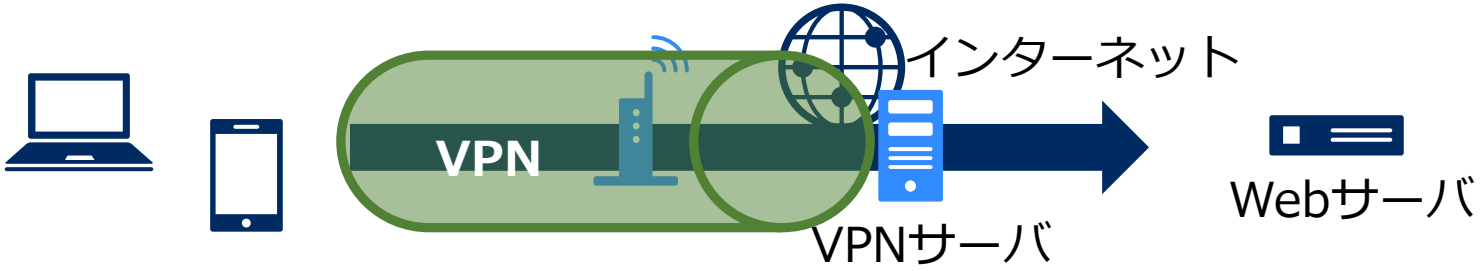
TLS/SSLプロトコルを用いる安全性確保の特徴

TLS/SSLプロトコルを用いることで、端末・Webサーバ間の通信を安全にすることができる

- 端末・Webサーバ区間の通信が全て暗号化されているため、
  暗号化されていないAPを利用した場合でも、安全な通信が可能
- 保護対象が**Web通信に限定される**
- **全てのWebサーバでTLS/SSLプロトコルが使われていない**

VPNサービスを用いる安全性確保の特徴

VPNサービスを利用することで、端末・VPNサーバ間の通信を安全にすることができる



- 無線区間を含む端末・VPNサーバ区間の通信は全て暗号化されているため、**暗号化されていないAPを利用した場合でも安全な通信が可能**

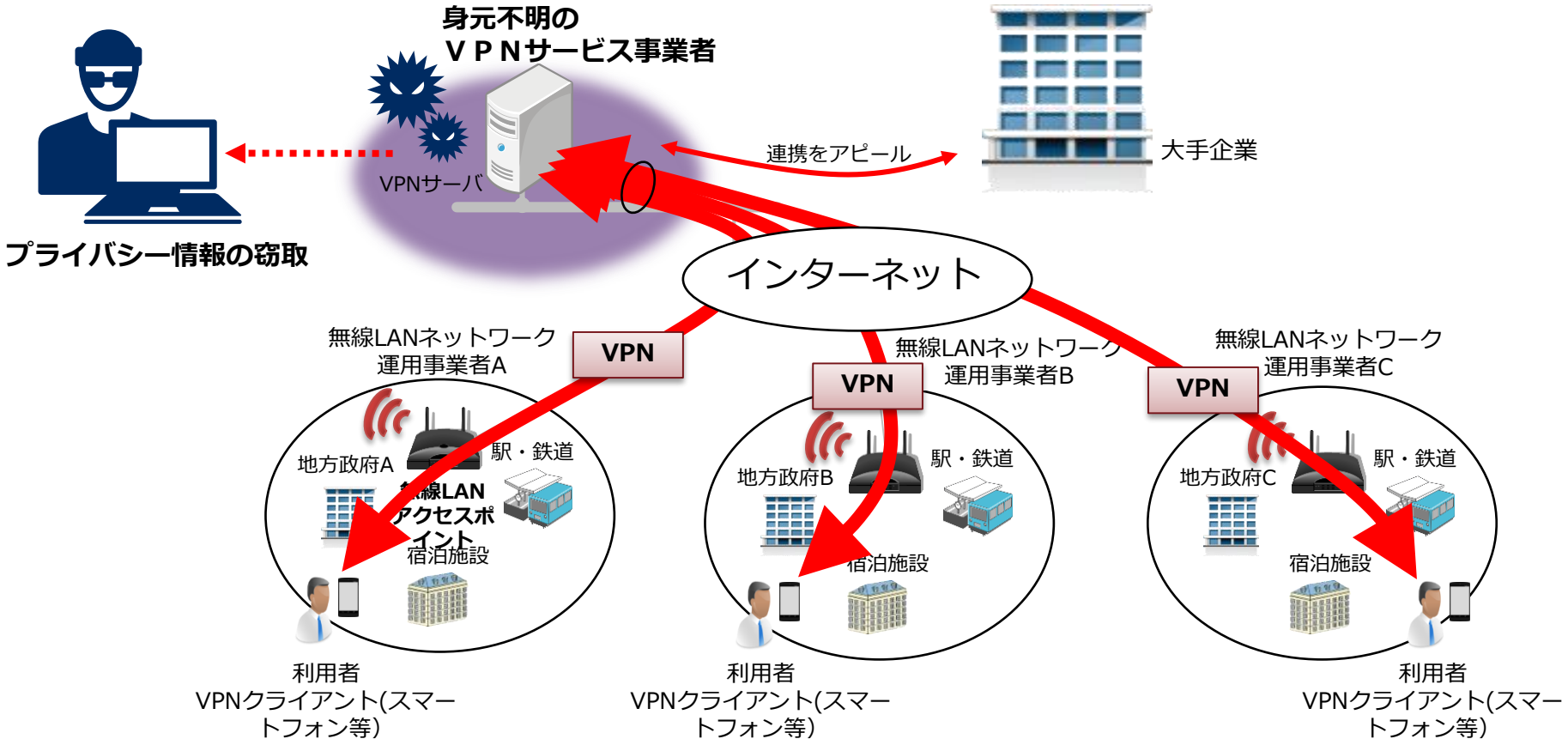
- **通信プロトコルによらず、安全な通信が可能**

- VPNサーバに全てのトラフィックが集まるため、**情報が健全に取り扱われない場合、重大なセキュリティリスク**になる
  - VPNサービス事業者が信頼できるか否か、現状は判断が難しい

身元不明のVPNサービスの使用で生じるリスク

ユーザのプライバシー情報窃取の危険性

- 2017年、米国大手企業との提携を謳うVPN業者が存在していることが判明
- 有名企業の知名度を利用して、ユーザのプライバシーを盗もうとしていた



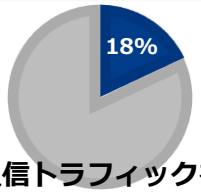
身元不明のVPNサービスに関する調査結果

実態調査結果：「Android端末向けのVPNアプリの大半は悪質なものである」

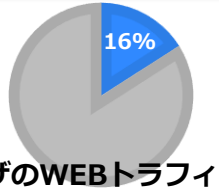
- 2016年11月に開催されたInternet Measurement Conference (IMC) 2016 で報告された
  【参考】M. Ikram, et al., “An Analysis of the Privacy and Security Risks of Android VPN permission-enbled Apps,” IMC 2016, pp. 349-364, 2016.

Google Playで提供されている283個のAndroid向けVPNアプリの分析結果

通信の盗聴、改ざんの危険性

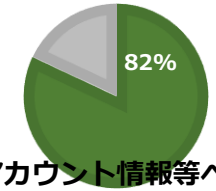


通信トラフィックを暗号化していない

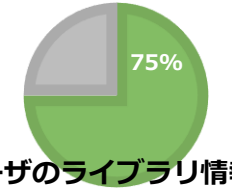


ユーザのWEBトラフィックにデータを挿入できる危険性

VPNサービスに不要な権限の許可

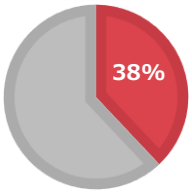


アカウント情報等へのアクセス許可



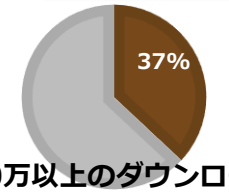
ユーザのライブラリ情報の取得を許可

マルウェアの組み込み

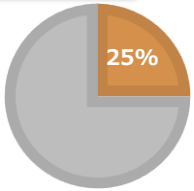


マルウェアが仕込まれている

VPNアプリの利用状況



50万以上のダウンロードがある



評価が★4以上である

- **現状では信頼できるVPNアプリかどうかを確認することが難しい**
- **危険なVPNアプリが存在することを理解せずに利用している可能性がある**

信頼のおけるVPNサービスを選定可能にするために

危険なVPN サービスが 存在…

Step1

- 利用者に注意を促す

何を対策して いるのか わからない…

Step2

- 対策内容やポリシー等を開示させる

本当に対策等を 実施しているの かわからない…

Step3

- 対策状況をチェックする仕組みを整備する

何を基準に 選べばいいのか わからない…

Step4

- 利用者が安全なアプリを選べる手段を整備する


Orchestrating a brighter world
NEC