資料２－３

すべてのステークホルダーから信頼され支持される企業へ
ADMIRED COMPANY

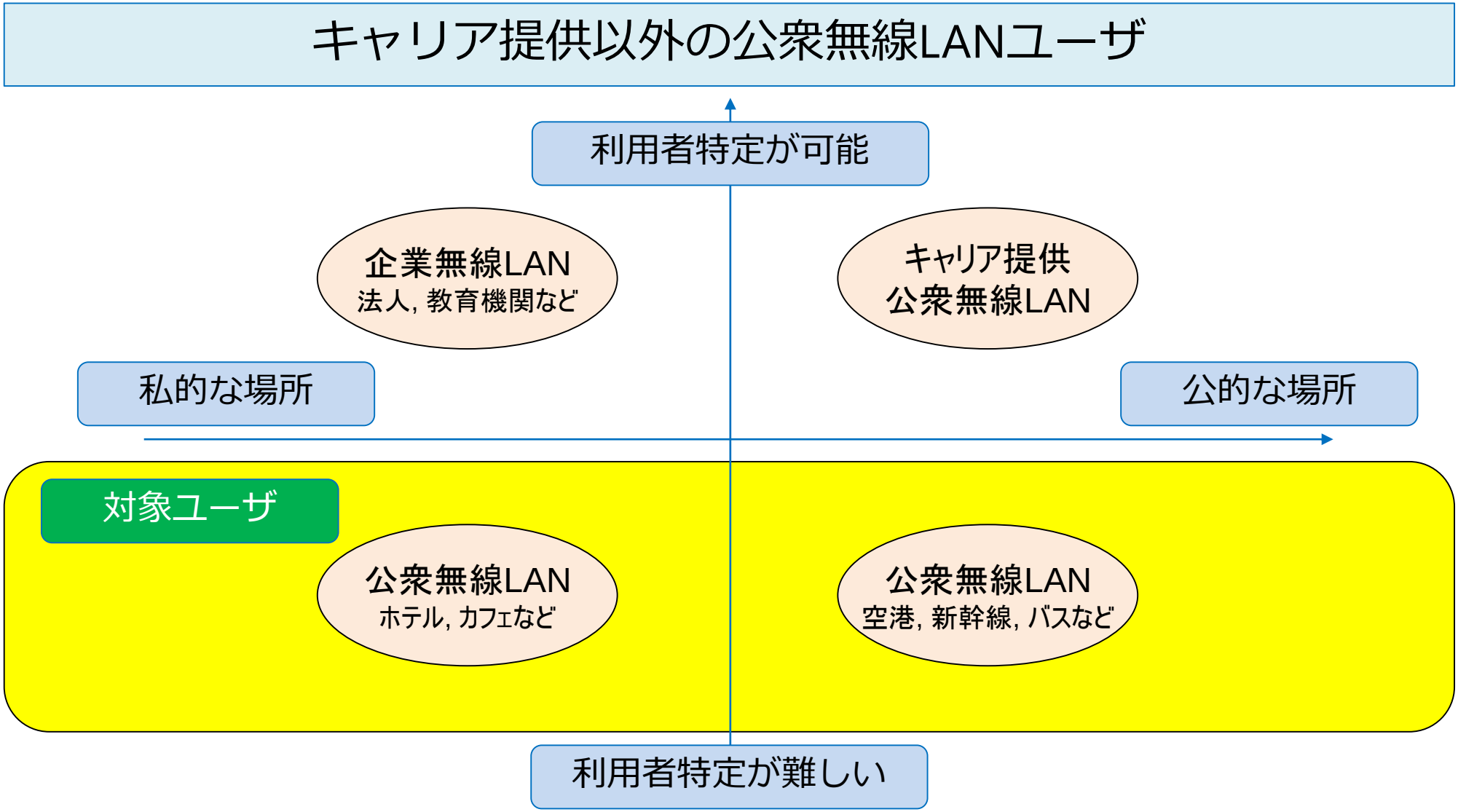
公衆無線LANセキュリティ分科会

セキュリティに配慮した公衆無線LANサービスの普及実現に向けて

平成29年（2017年）12月1日
ネットワンシステムズ 株式会社
ビジネス推進本部 応用技術部
中野 清隆

net one

本資料における対象ユーザ



© NetOneSystems Co., Ltd. All rights reserved.

・・・目　次・・・

- 公衆無線LANの現状と課題
- 対応策案
- まとめ

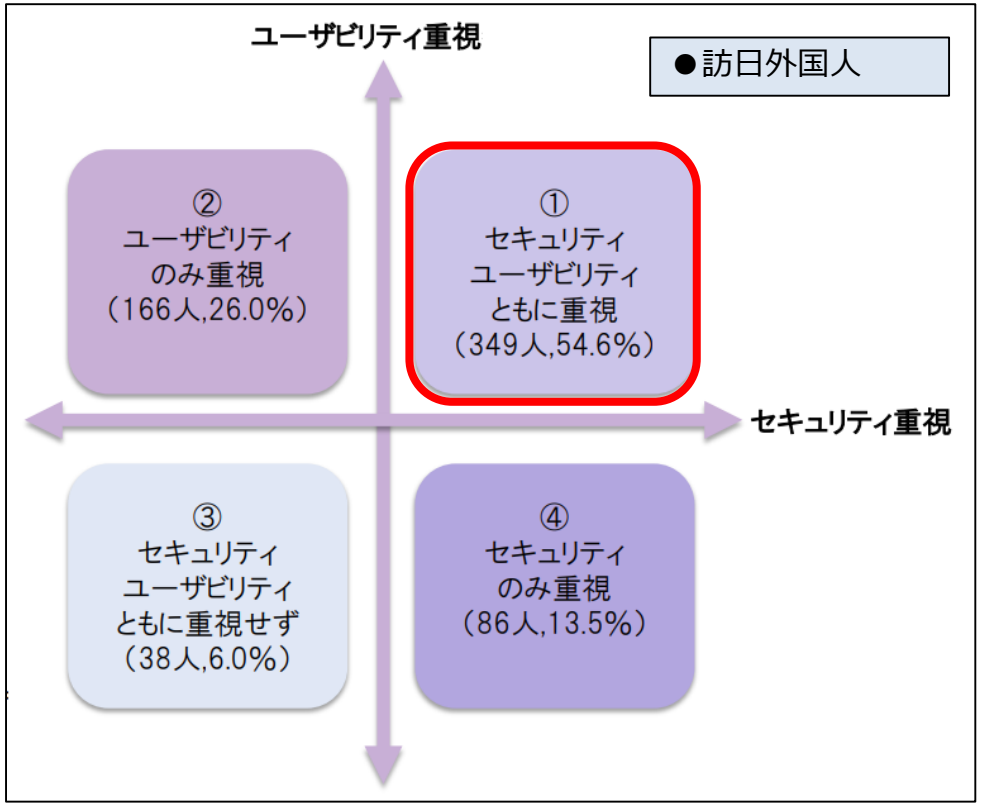
© NetOneSystems Co., Ltd. All rights reserved.

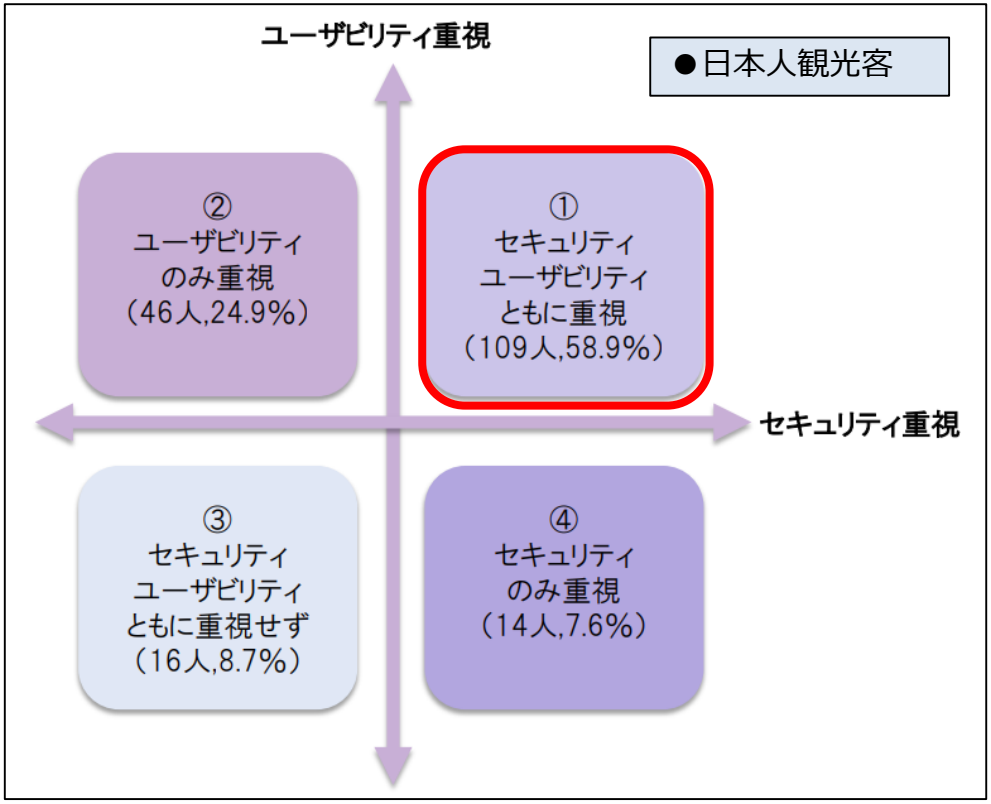
公衆無線LANの現状と課題

© NetOneSystems Co., Ltd. All rights reserved.

公衆無線LANに関する調査結果

平成27年 総務省「公衆無線LAN利用に関する情報セキュリティ意識調査結果」
便利で使いやすい公衆無線LANサービスの提供に向けて、改善が求められると感じる点



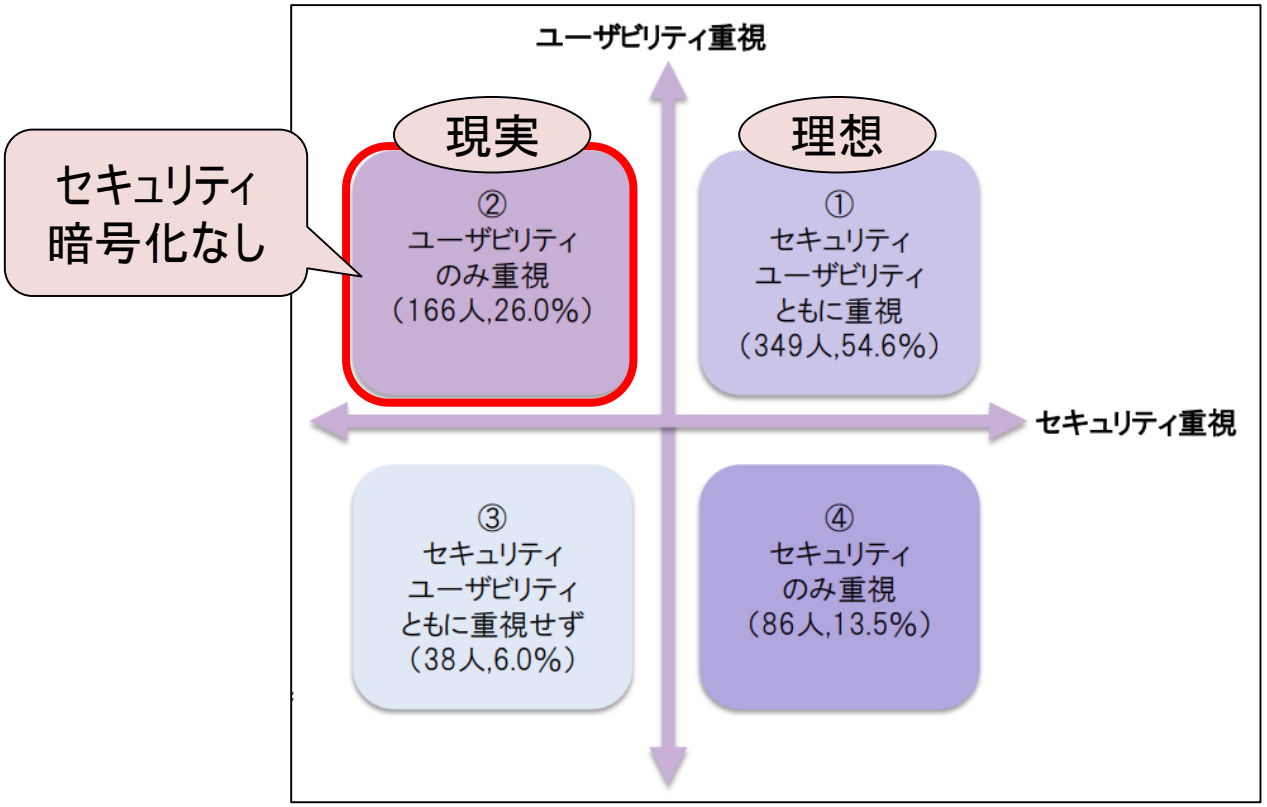


公衆無線LANにおいて「利便性」「セキュリティ」の両方が求められている

© NetOneSystems Co., Ltd. All rights reserved.

公衆無線LANの理想と現実

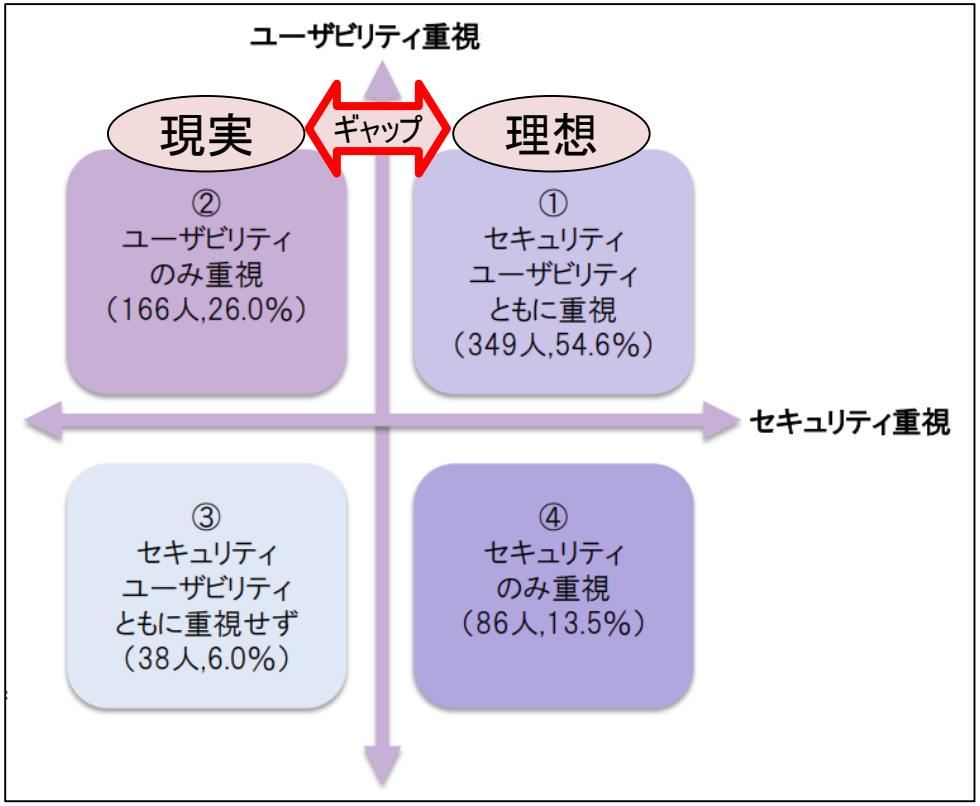
現状の公衆無線LANにおいては
利便性を優先してセキュリティ対策が十分ではない場合が多い



© NetOneSystems Co., Ltd. All rights reserved.

理想と現実のギャップを埋めるには

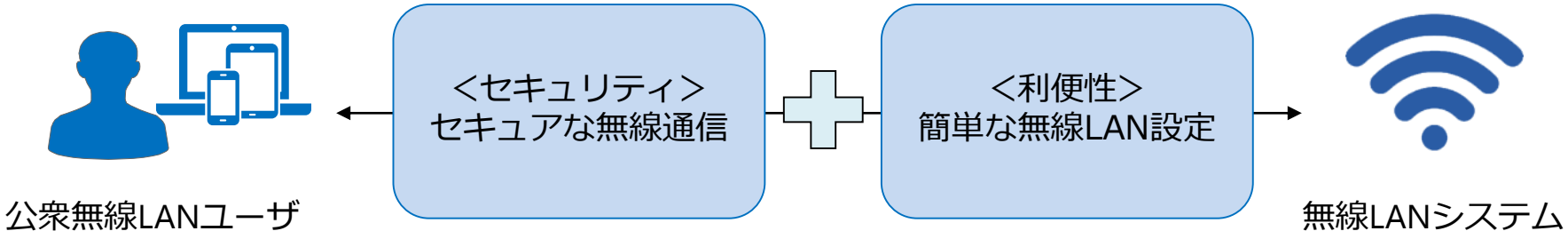
【課題】
『セキュリティ』を高めつついかに『利便性』を損なわない仕組みを作れるか



© NetOneSystems Co., Ltd. All rights reserved.

理想と現実のギャップを埋めるには

【課題】
『セキュリティ』を高めつついかに『利便性』を損なわない仕組みを作れるか



© NetOneSystems Co., Ltd. All rights reserved.

対応策案

© NetOneSystems Co., Ltd. All rights reserved.

セキュリティ：無線区間の暗号化

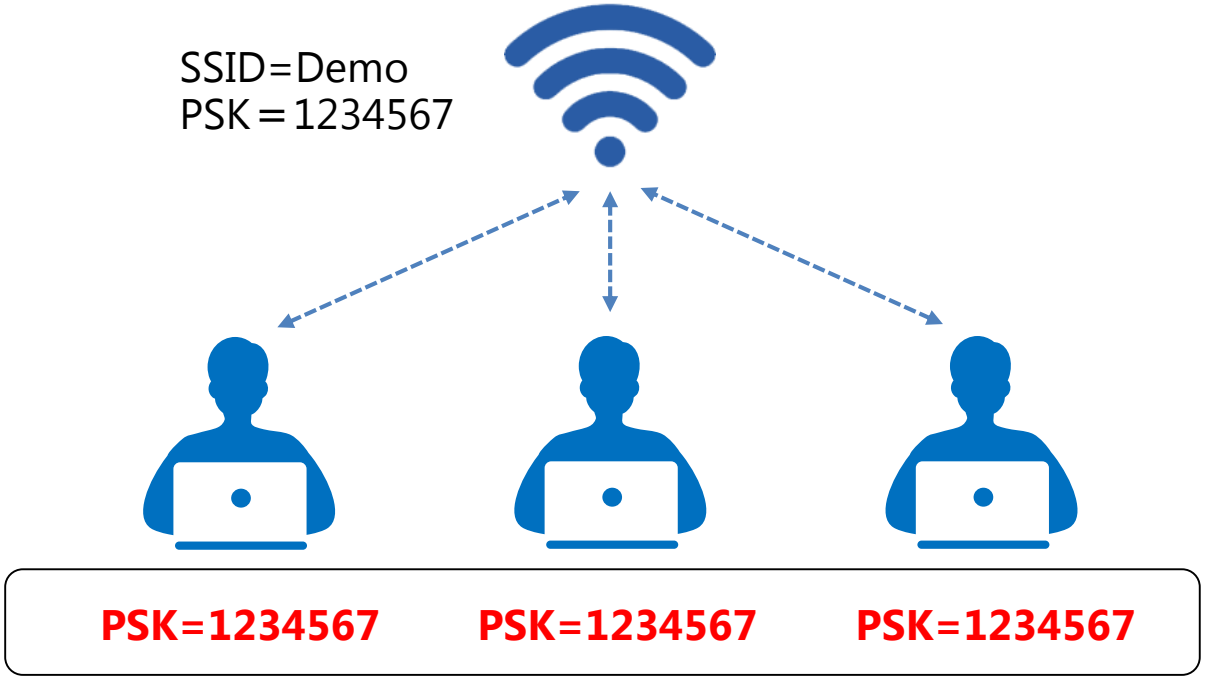
	利便性	セキュリティ強度
• 暗号化なし – 盗聴のリスク大	◎	×
• 暗号化あり：WPA2-PSK（Pre Shared Key） – **暗号鍵：全ユーザ共通** – 暗号化なしよりはセキュリティを確保可能 – ただし、全ユーザが共通の暗号鍵を利用するため、高いセキュリティを確保するためには定期的な暗号鍵の変更が必要 – 企業においても実際はなかなか頻繁な暗号鍵の変更は実施がされておらずPSK利用における課題	○	○ 暗号鍵の定期的な変更をしない場合は△に
• 暗号化あり：WPA2（IEEE802.1X/EAP：証明書ベース） – **暗号鍵：ユーザ個別** – 認証サーバと連携しユーザごとに異なる暗号鍵を生成可能なため高いセキュリティを確保可能 – ただし、IEEE802.1Xは証明書ベースのため、公衆無線LANにおいて証明書の運用が課題	△	◎

公衆無線LANにおいて
「利便性」と「セキュリティ」の両方を考えるとWPA2-PSKの利用がポイントに

© NetOneSystems Co., Ltd. All rights reserved.

PSKのセキュリティ面での課題

- WPA2-PSK（Pre Shared Key）
  - **暗号鍵：事前固定暗号鍵設定・全ユーザ共通**
  - 暗号化なしよりはセキュリティを確保可能
  - **ただし、全ユーザが共通の暗号鍵を利用するため、高いセキュリティを確保するためには定期的な暗号鍵の変更が必要（変更時には全ユーザへの通知が必要）**



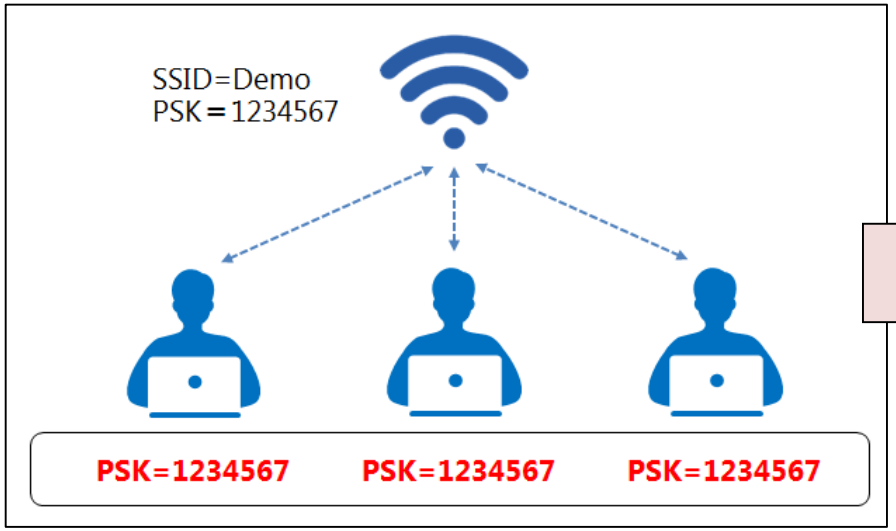
【理想】IEEE802.1X/EAP利用時のように
ユーザごとに個別の暗号鍵を生成して利用すること！

© NetOneSystems Co., Ltd. All rights reserved.

PSKにおける課題への対応策案

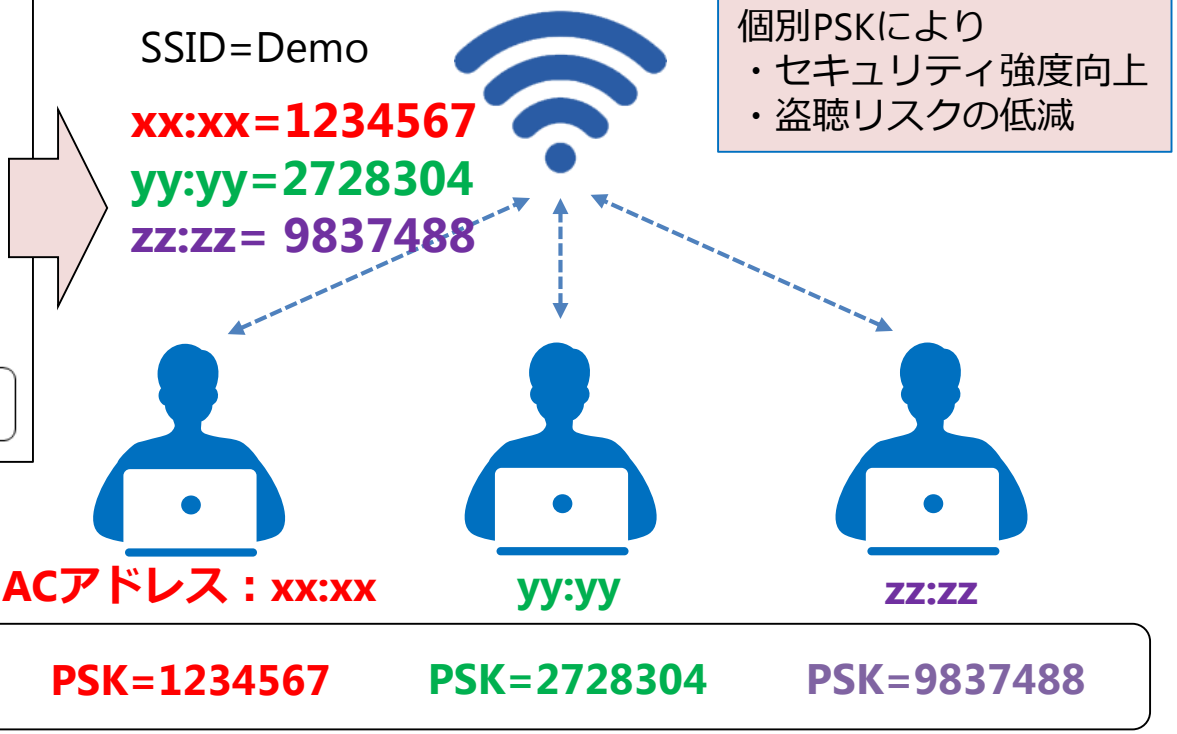
IEEE802.1X/EAP利用時のように
ユーザごとに個別の暗号鍵を利用可能な機能が実装された製品がリリース

これまでのPSK



個別PSK

同じSSID配下でユーザごとに異なるPSKの実現



© NetOneSystems Co., Ltd. All rights reserved.

個別PSK対応製品例

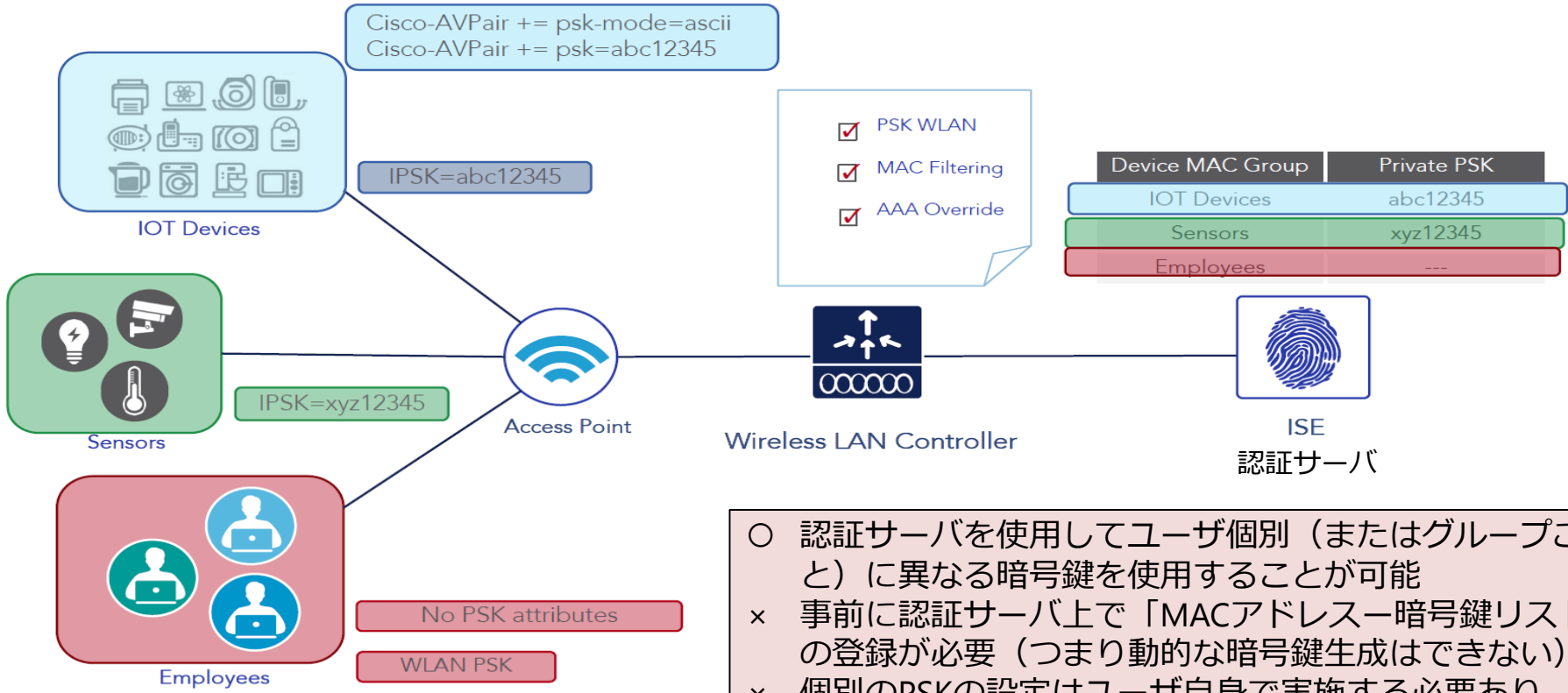
- Cisco Systems
- Ruckus Wireless

© NetOneSystems Co., Ltd. All rights reserved.

Cisco社による個別PSK

Identity PSK(Pre Shared Key)
認証サーバを利用した個別PSKの実現

https://www.cisco.com/c/ja_jp/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html

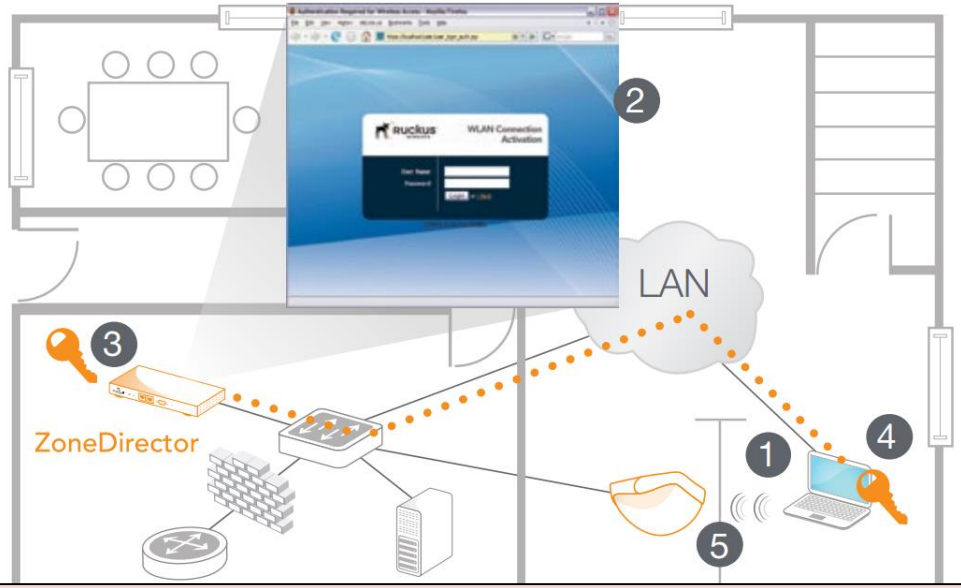


○ 認証サーバを使用してユーザ個別（またはグループごと）に異なる暗号鍵を使用することが可能
× 事前に認証サーバ上で「MACアドレスー暗号鍵リスト」の登録が必要（つまり動的な暗号鍵生成はできない）
× 個別のPSKの設定はユーザ自身で実施する必要あり

© NetOneSystems Co., Ltd. All rights reserved.

Ruckus社による個別PSK

Dynamic PSK(Pre Shared Key)
無線LANコントローラを利用した個別PSKの実現



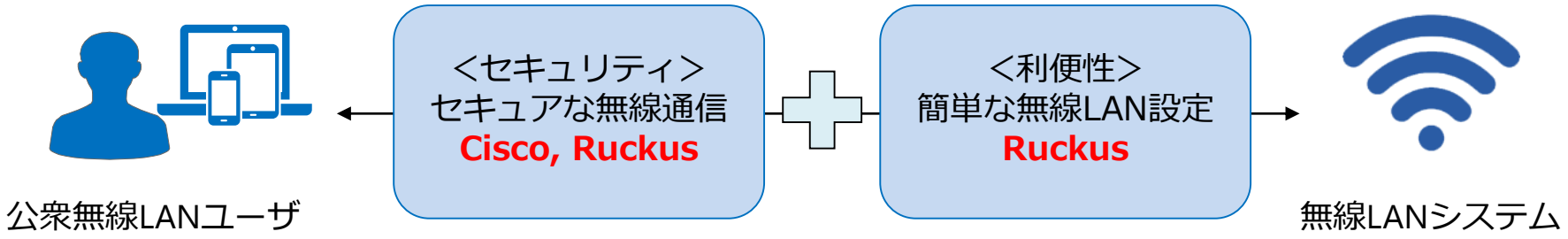
- ○ 無線LANコントローラを使用してユーザ個別に異なる暗号鍵を使用することが可能
- ○ 無線LANコントローラによって暗号鍵の自動生成が可能
- ○ 自動生成した暗号鍵情報含め、無線LAN設定情報をユーザのデバイスに対して簡単設定することが可能（右絵）
- × 個別PSKを生成するための設定ログイン画面（左絵）にユーザがアクセスするために、事前にユーザアカウント登録する必要あり

http://ruckus-www.s3.amazonaws.com/pdf/feature-sheets/fs-dynamic-psk.pdf（左）
http://www.netone-pa.co.jp/solution/ruckus-wireless/（右）

net one
© NetOneSystems Co., Ltd. All rights reserved.

PSK比較

	WPA2-PSK	Cisco Identity PSK	Ruckus Dynamic PSK
ユーザごとの暗号鍵	×（全ユーザ共通）	○（事前登録）	○（自動生成）
認証サーバ	不要	必要	不要
簡単な無線LAN設定	× 事前にアクセスポイント、ユーザデバイス側に暗号鍵設定が必要	× 事前に認証サーバ、ユーザデバイス側に暗号鍵設定が必要	○ 事前に無線LANコントローラ、ユーザデバイス側に暗号鍵設定は不要
まとめ	IEEE802.1Xに比べると使いやすいが、個別PSKに比べると暗号鍵が前ユーザ共通なので「セキュリティ」の点で劣る	ユーザごと異なる暗号鍵を使用可能なため「セキュリティ」を強化可能	「セキュリティ」「利便性」ともに強化可能 ただし、無線LAN設定において事前に**ユーザアカウント登録**が必要



© NetOneSystems Co., Ltd. All rights reserved.

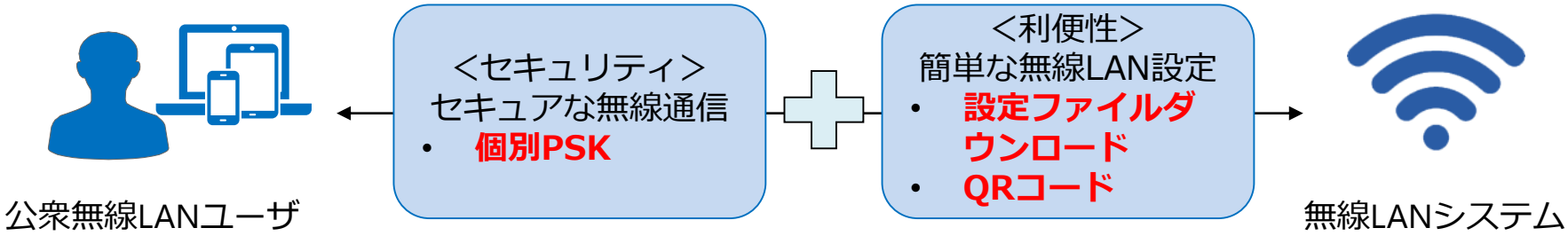
まとめ

© NetOneSystems Co., Ltd. All rights reserved.

まとめ

＜セキュリティ＞
- 個別PSKを利用することでWPA2-PSKのセキュリティを高めることが可能

＜利便性＞
- 設定ファイルのダウンロードや他製品ではQRコードなどでユーザのデバイスに対して簡単な無線LAN設定の実現が可能

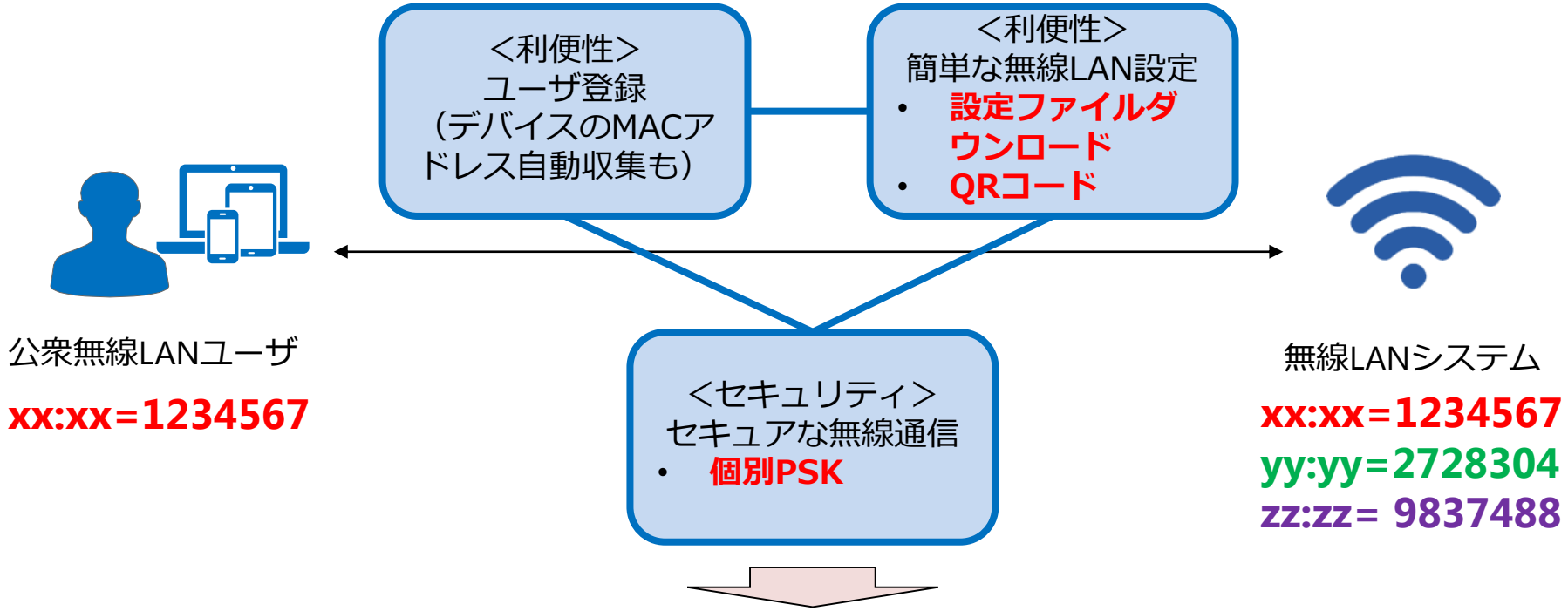


ただし既存製品の仕組みではユーザ登録との連携がうまく実現できていない
※個別PSKを実現するためにはユーザ（デバイス）とPSKの紐付けるために
ユーザ登録の実施が必要

© NetOneSystems Co., Ltd. All rights reserved.

まとめ

「ユーザ登録」「簡単な無線LAN設定」「セキュアな通信」
をうまく連携させることで
セキュリティを高めつつ利便性を大きく損なわない仕組みを実現可能



セキュリティに配慮した公衆無線LANサービスの普及！

© NetOneSystems Co., Ltd. All rights reserved.

課題として

提供形態によって連携が難しい場合あり

- ホテル
  - フロントにて「ユーザ登録」を実現することは可能なので「ユーザ登録」「簡単な無線LAN設定」「セキュアな通信」をうまく連携させることは可能

- 空港、新幹線、バスなどの公共性の高い場所
  - 訪れた人に対して、どのようにして「ユーザ登録」を実現させるかが課題

© NetOneSystems Co., Ltd. All rights reserved.

つなぐ ∠ むすぶ ∠ かわる

net one