NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

公衆無線LANをビジネスで使用するときの課題

新日鉄ソリューションズ(株)
松島 正明

2003 年 6月 4日

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

2003 spring
Network Security Forum

公衆無線LANサービスについて

ネットワークの安全を考える

公衆無線LANとは

- 駅構内、Hotel、各種会場、喫茶店、ファーストフード店など、多くの人が集まる場所で提供される、無線LANを用いた高速インターネット接続サービス
- 無線LANは、IEEE802.11aおよび、IEEE802.11bを使用し、現在主流となっている802.11bでは最大11Mbpsでの通信が可能

広がる無線スポットサービス

- 様々な事業者が無線スポットサービスを実施
  - FREESPOT（FREESPOT協議会）
  - HOTSPOT（NTTコミュニケーションズ(株)）
  - MZONE（(株)NTTドコモ）
  - @Mobile（アットマークベンチャー(株)）
  - Yahoo! BB モバイル（ヤフー(株)） など…
- エリアの拡大
  - 上記の事業者が行っているサービス以外にも、ホテル・施設などで独自にアクセスポイントを用意しているところもある
  - MapFanWeb 無線スポット検索ページ
    - http://www.mapfan.com/musen/

サービスの効果的な利用

- 忙しいビジネスマンにとってこれらのサービスを有効に利用できれば、時間とコストを削減できる
  - 出張や営業の空いた時間などに仕事ができる
  - PHSなどでの接続に比べて高速である
- 問題点
  - 無線LANのセキュリティ
    - 認証はどうなってるの？
    - WEPの64bit暗号で本当に大丈夫？
    - その他のセキュリティ上の問題は？
- 実現したいこと
  - 社内のリソースにセキュアにアクセスしたい

公衆無線LANのセキュリティ

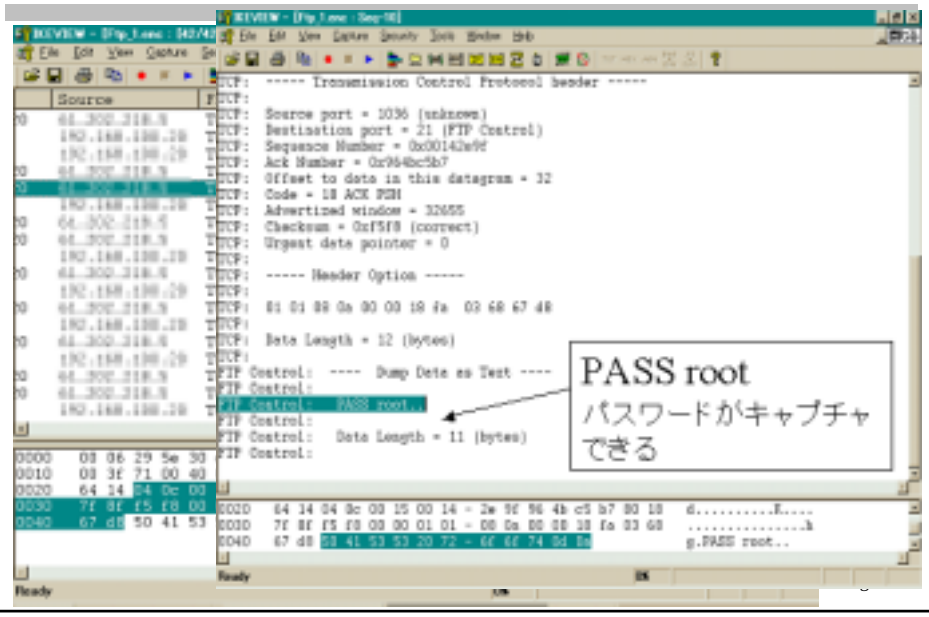
- 認証および暗号化
  - SSID (Service Set ID：管理ID)
    - 無線LANのグループ識別子
      - 一部のOSでは自動的に取得できてしまい、暗号化等はされていないため、通信を保護することはできない
  - MACアドレスフィルタリング
    - 無線に接続できる端末をMACアドレスでフィルタリングする
      - OS上で簡単に変更可能なため、セキュリティ保護には？？
  - WEP (Wired Equivalent Privacy：有線なみのプライバシー)
    - 有線LANと同等の機密性を保持するための仕様
      - RC4を利用した暗号通信。40bit版と104bit版がある。
  - 802.1xでの認証および暗号化
    - 実装している製品が少ない

WEPの脆弱性

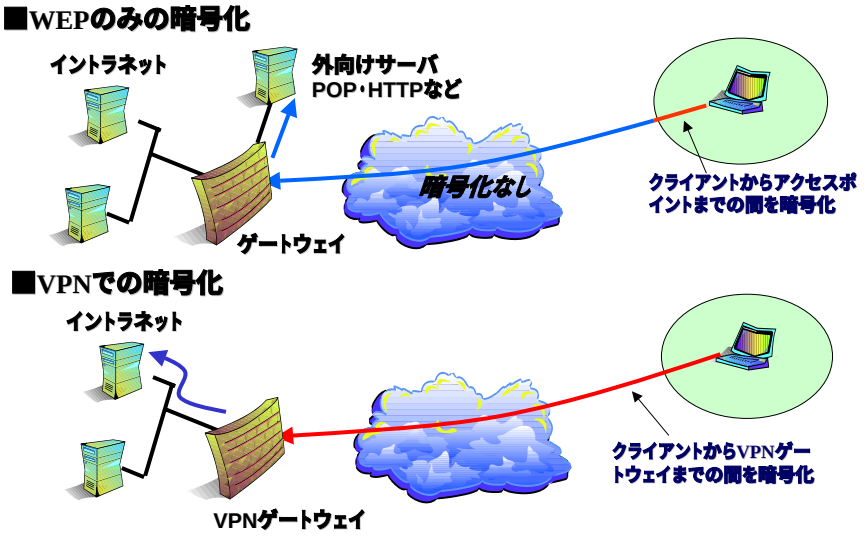
- WEP Keyの脆弱性
  - 40bit WEP Keyの解読は、最長2.7日程度可能
    - 英数字のみ使用の場合は、数秒～数十分程度で解読可能
      - 株式会社ラック 無線LANセキュリティ設定実態調査より
      - http://www.lac.co.jp/security/intelligence/SNSSpiffy/3.pdf
    - AirSnortなどのフリーのWEP 解読ツール

	WEP Keyに使用する文字列			
	0-9, a-z	0-9, a-z, A-Z	0-9, a-z, A-Z, 記号	16進
WEP 64 5桁 (Key：40bit)	13.1秒	3.3分	21.3分	2.7日
WEP128 13桁 (Key：104bit)	1.2×10^6年	1.4×10^9年	1.7×10^11年	1.4×10^17年

APで共通のWEP Key



VPNの利用



VPNの利用

- IPsecによるVPNで得られるメリット
  - クライアントPCよりVPNゲートウェイまでを暗号化
  - 社内リソースへアクセス可能
    - 外出先から、会社のPCへアクセスして資料をダウンロードしたり、社内のイントラネットWEBにアクセスして検索を行うなど・・・
  - サービスを選ばない
    - 基本的にはどんなサービスでも利用可
      (POP/SMTP/HTTPなどのプロトコル)
      サービス毎に暗号化する必要がない

公衆無線LAN調査

公衆無線LANとVPN

JNSA

- 無線スポットはWorkspaceとして利用できるか
  - Workspace：作業スペースがあり、社内リソースへのセキュアなアクセスが可能であること。
  - 物理的な問題
    - PCを使うために十分なスペースが確保できるか？
    - 無線スポット用の電源は確保されている？
  - 通信に関する問題
    - Wireless LAN NICとAccess Pointの接続性は？
    - VPNでの接続性
    - MTUの問題は無いの？
  - セキュリティの問題

調査内容

- 調査目的
  - 各キャリアが提供している無線スポットサービスがWorkspaceとして使えるかどうか
- 調査内容
  - 通信環境調査
    - IPアドレス（グローバル or プライベート）
    - 電波状況
  - VPN通信テスト
    - Ping
    - FTPでのGET／PUT

調査対象

- 調査参加企業（50音順）
  - SSHコミュニケーションズ・セキュリティ(株)
  - 工学院大学 LINCS
  - Cisco システムズ(株)
  - 新日鉄ソリューションズ(株)
  - セコムトラストネット(株)
  - ソフトバンクBB(株)
  - ソフトバンクテクノロジー(株)
  - (株)ディアイティ
  - (株)ヒューコム
  - 三菱電機(株)

調査対象

- 対象公衆無線LANサービス

サービス	有料/無料
Yahoo! BB／Yahoo!JAPAN	試験サービス中(無料)
JR東日本	試験サービス終了
Mzone／NTT DoCoMo	有料
HOTSPOT／NTTｺﾐｭﾆｹｰｼｮﾝｽﾞ	有料
ネオモバイル／NTT Me	有料
@Mobile／@ベンチャー	無料
FREESPOT／FREESPOT協議会	無料

調査対象

- 対象機器

メーカ	VPNゲートウェイ	クライアントソフト
Checkpoint	VPN-1	SecureClient
Cisco	VPN3000	VPN3000 Client
NetScreen	NS204	NetScreen Remote
SSH	IPSEC Express Toolkit	SSH Sentinel

- 各機器設定内容

ﾒｰｶ	Phase1	Phase2	圧縮	NAT対応	認証
Checkpoint	MM 3DES/SHA-1 DH-2	3DES/SHA-1 Tuunel DH-2	なし	独自(UDP2746)	ハイブリッド
Cisco	AM 3DES/SHA-1 DH2	3DES/SHA-1 Tuunel DH-2	あり	独自(UDP 10000)	PSK/Xauth
NetScreen	MM 3DES/SHA-1 DH-2	3DES/SHA-1 Tuunel DH-2	なし	NAT-T(UDP 500)	PSK/Xauth
SSH	MM AES/SHA-1 DH-2	3DES/SHA-1 Tuunel DH-2	なし	NAT-T(UDP 500)	PSH/Cert

試験結果

- 通信環境調査

サービス	相性	WEP	IPアドレス	認証方式
Yahoo! BB／Yahoo!JAPAN	○	64	Private	ブラウザ
JR東日本	○	64	Private	ブラウザ／MACアドレス
Mzone／NTT DoCoMo	○	64	Global	ブラウザ
HOTSPOT／NTTｺﾐｭﾆｹｰｼｮﾝｽﾞ	○	64	Global	ブラウザ
ネオモバイル／NTT Me	○	64※	Private	MACアドレス
@Mobile／@ベンチャー	○	なし	Private	なし
FREESPOT／FREESPOT協議会	○	なし	Private	なし

相性：○はCisco AIRONET350で接続可能
WEP：※はWEP無しを選択することも可能

試験結果

- VPN通信テスト

	Checkpoint			Cisco			NetScreen			SSH		
サービス	ping	put	get	ping	put	get	ping	put	get	ping	put	get
A社	○	○	○	○	○	○	○	○	○	○	○	○
B社	○	○	○	-	-	-	○	○	○	○	○	○
C社	○	○	○	○	○	○	○	○	○	○	○	○
D社	○	○	○	○	○	○	○	○	○	○	○	○
E社	○	○	○	-	-	-	○	○	○	○	○	X ※1
F社	○	○	○	○	○	○	-	-	-	○	○	○
G社	○	○	X	○	○	○	○	○	X	○	○	○

X：失敗　　※1：試験実施時の FTPサーバ設定不備のため
－：未調査

JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

2003 spring
Network Security Forum

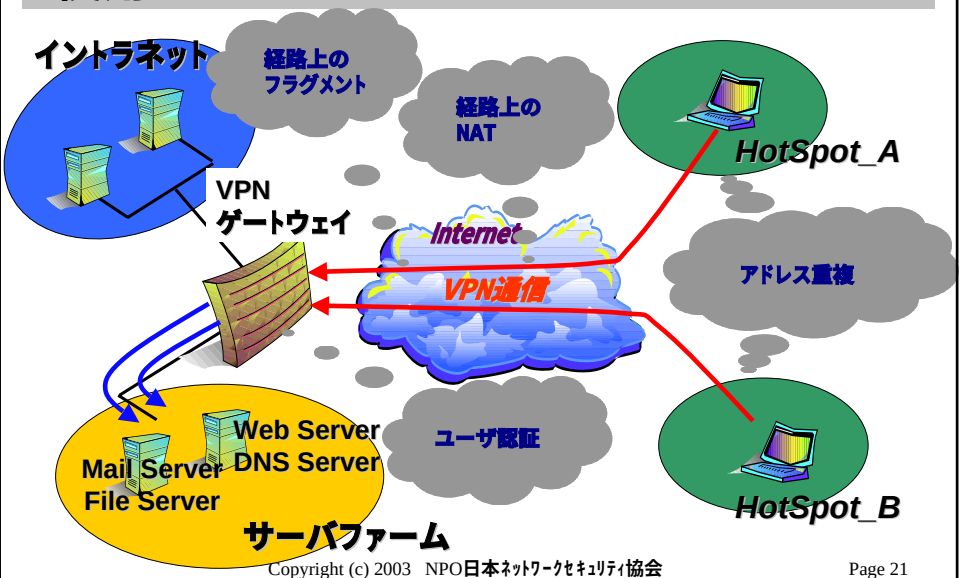
公衆無線LANを
ビジネスで使用する時の課題と対応

公衆無線LANでIPsecを使用するために

JNSA

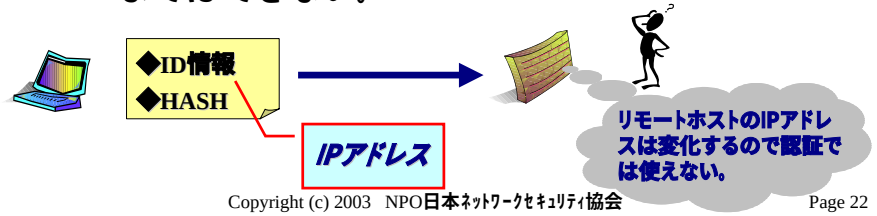
- 検討すべき問題点
  - 認証に関する問題
    - リモートユーザを認証するためのしくみ
  - NATに関する問題
    - ほとんどのキャリアが提供するサービスはPrivate IPアドレスのため、経路上にNAT機器が介在する
  - IPアドレスに関する問題
    - Private IPアドレスの重複
  - フラグメントに関する問題
    - VPNゲートウェイでフラグメント化されたパケットがVPNクライアントまで到達しない

公衆無線LANでIPsecを使用するために



認証に関する問題

- 認証に関する問題1
  - ゲートウェイ間のIPsec通信で最も使用されている、Mainモードで Pre-Shared認証を使用する方法はリモートクライアントでは使用できない。
- 原因
  - MainモードのPre-Sharedでは、ユーザの特定まではできない。

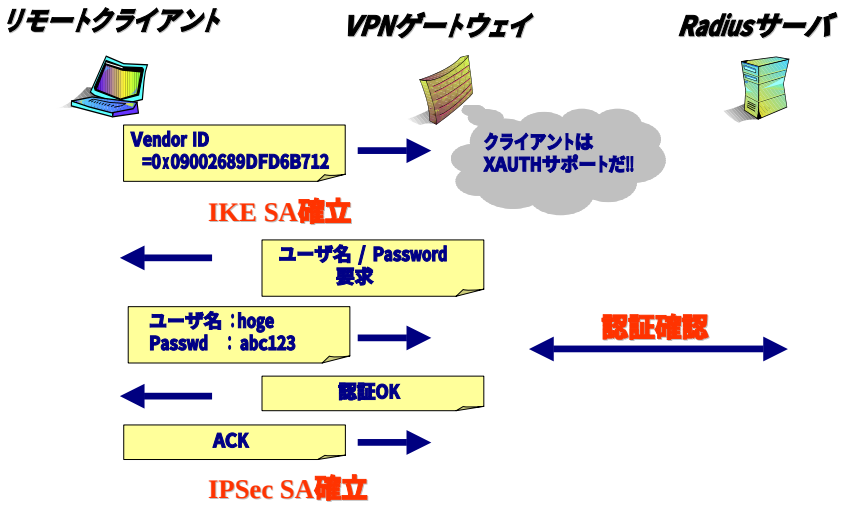


認証に関する問題

- XAUTH・Hybrid Auth・証明書
  - 対応策
    - XAUTHは、IKEにおいて認証方式を拡張する
      - パスワード、OTP、RADIUS、S/KEYなど
    - Hybrid Authは、VPN機器とクライアントでの認証方式を異なるものにできる
      - VPN機器は証明書、クライアントはパスワード認証など
      - VPNデバイス同士は証明書で認証させたいが、クライアントには従来のパスワードで認証させたい時などに
      - XAUTH，Hybrid AuthともInternet DraftからExpire
      - ただし、多くのIPsec機器およびClientソフトはXAUTHをサポートしている
      - Hybrid Authをサポートしている製品は少数
    - 証明書での認証を行う

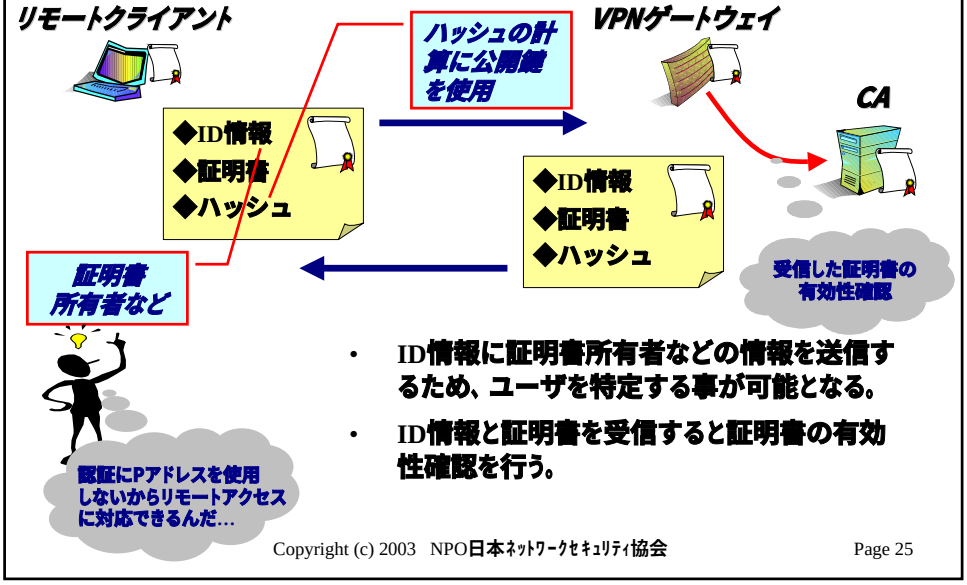
認証に関する問題

～ XAUTHを利用したIKE ～



認証に関する問題

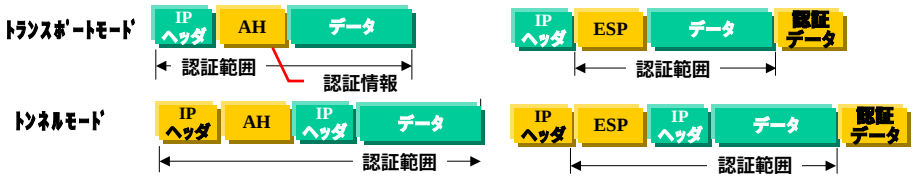
～ 証明書を利用したIKE ～



- ID情報に証明書所有者などの情報を送信するため、ユーザを特定する事が可能となる。
- ID情報と証明書を受信すると証明書の有効性確認を行う。

NATに関する問題

- **NATに関する問題点**
  - AHは、IPヘッダが認証範囲に入っているため、NATには対応できない。
  - ESPは、IPヘッダのすぐ後に、ESPヘッダがあるため、NAPT（Network Address Port Translation）に対応できない。（1対1のNATには対応可能）



NATに関する問題

- **解決策**
  - **NAT Traversal (NAT-T) をサポートする製品を使用する。**
    - **イニシエータはNAT-Dペイロードに始点IPアドレス/ポート番号・終点IPアドレス/ポート番号を埋め込んで送信する。レスポンダはNAT-Dペイロードの中のデータと実際のIPアドレス・ポートを比較してNATの有無を検知する**

    - IPsecパケットは、『UDP Encapsulation of IPsec Packet』でUDP Encapsulationされる。
    - NAT-Tのドラフトバージョンが異なると、NAT-T対応製品同士でも接続は不可能 (要注意!!)

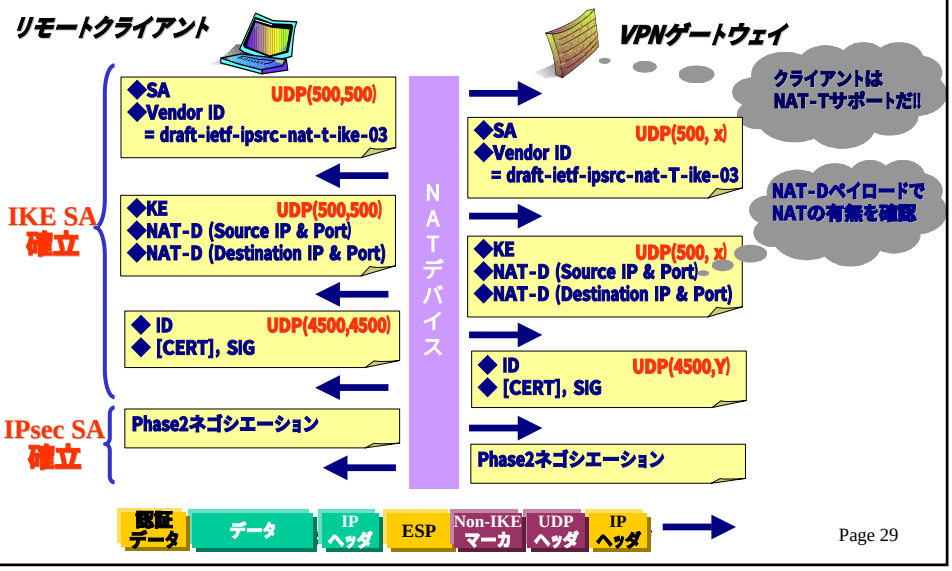
NATに関する問題

- NAT-Traversal 対応製品
  - Netscreen
  - SSH
- **メーカ独自機能によるNAT越え対応製品**
  - Checkpoint
    - **ネゴシエーション時のUDPポートでNAT有無を確認**
    - NAT有りと判断された場合は、IPsecパケットをUDP 2746でカプセリング。
  - Cisco
    - TCP high port(TCP encapsulation) TCP 10000ポート
    - UDP high port(UDP encapsulation) UDP 10000ポート (デフォルト)

製品名/メーカー名	鍵交換方式	カプセル化使用ポート
CheckPoint VPN-1	IKE または独自(TCP)	UDP 2746(または任意)
Cisco VPN3000	IKE または独自(TCP)	UDP 10000 / TCP 10000
SSH	IKE	UDP 500/4500(または任意)
Netscreen	IKE	UDP 500

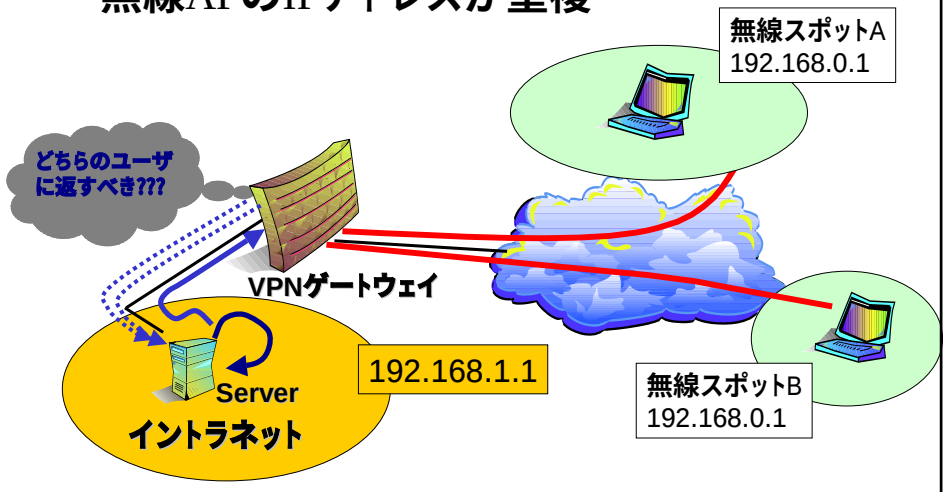
NATに関する問題

～ NAT Traversal (NAT-T) ～



IPアドレスに関する問題

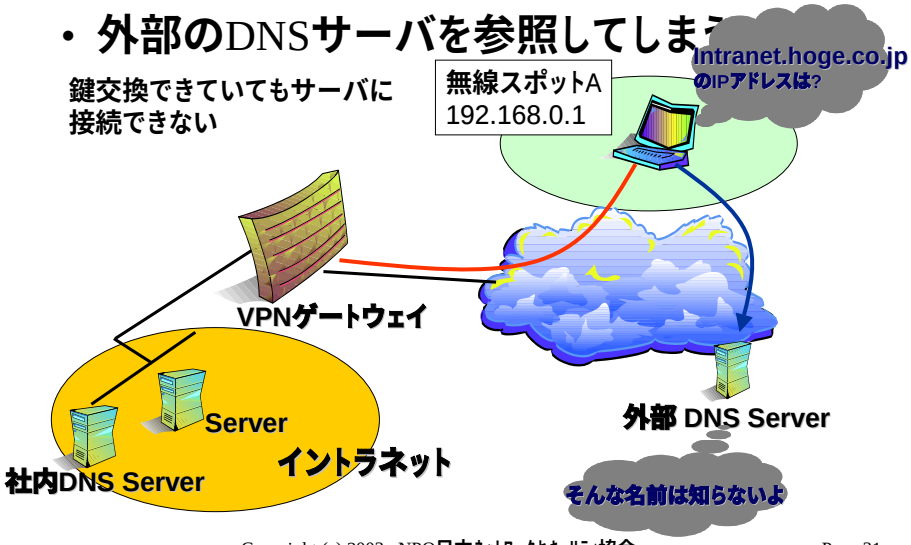
- 無線APのIPアドレスが重複



IPアドレスに関する問題

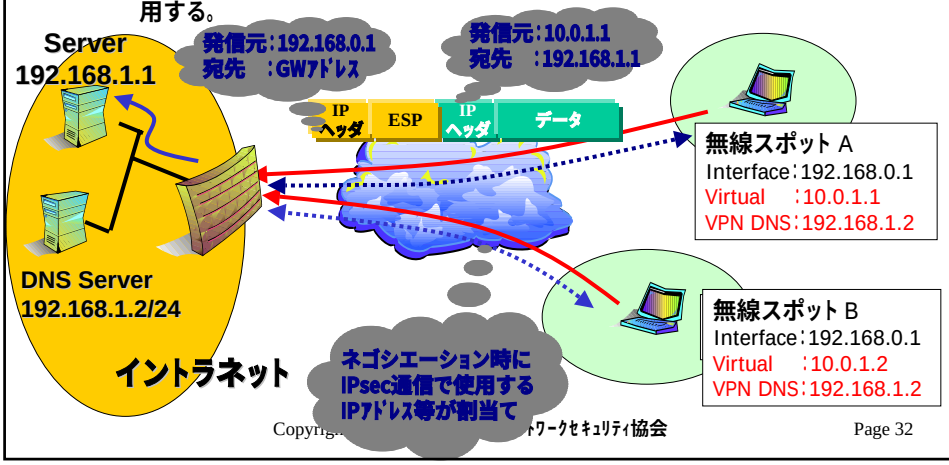
- 外部のDNSサーバを参照してしまう

鍵交換できていてもサーバに
接続できない



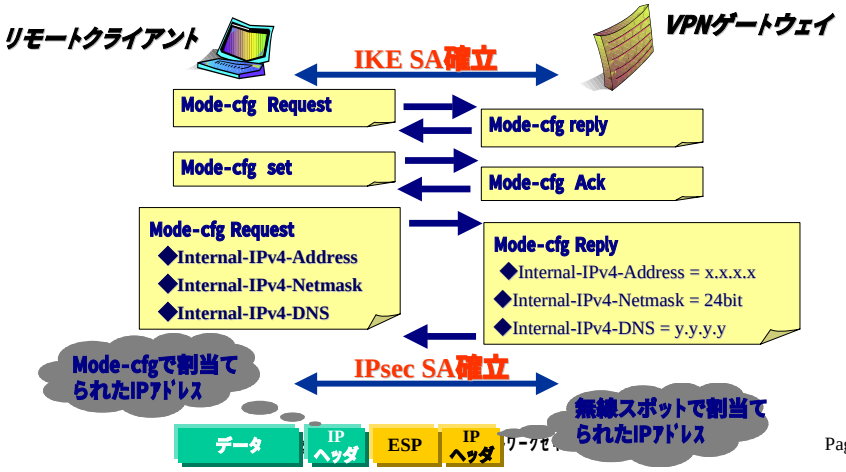
IPアドレスに関する問題

- 解決策
  - VPNゲートウェイから、VPN通信用のIPアドレスを割当てる。
  - IPsec-DHCPまたは、ISAKMP Configuration Methodをサポートする製品を使用する。



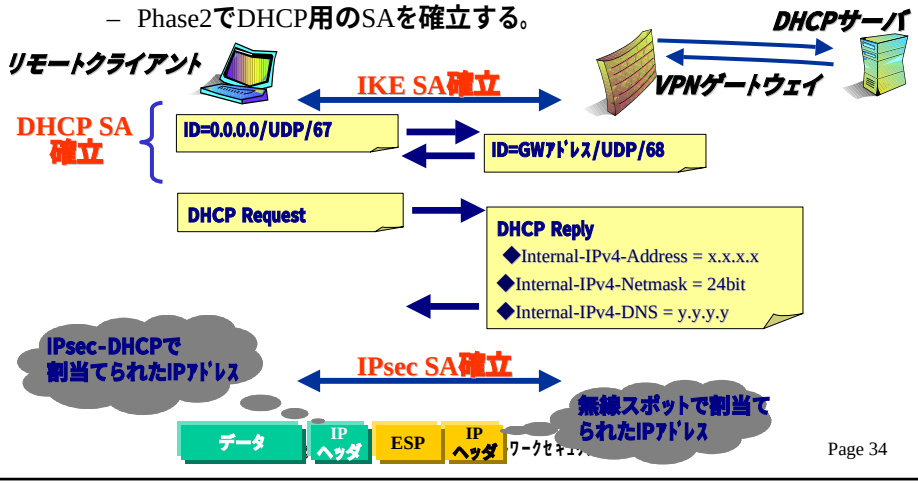
IPアドレスに関する問題
～ ISAKMP Configuration Method ～

- 解決策
  - ISAKMP Configuration Method(mode-cfg)
  - IKEを変更する必要があるため、DraftからExpire



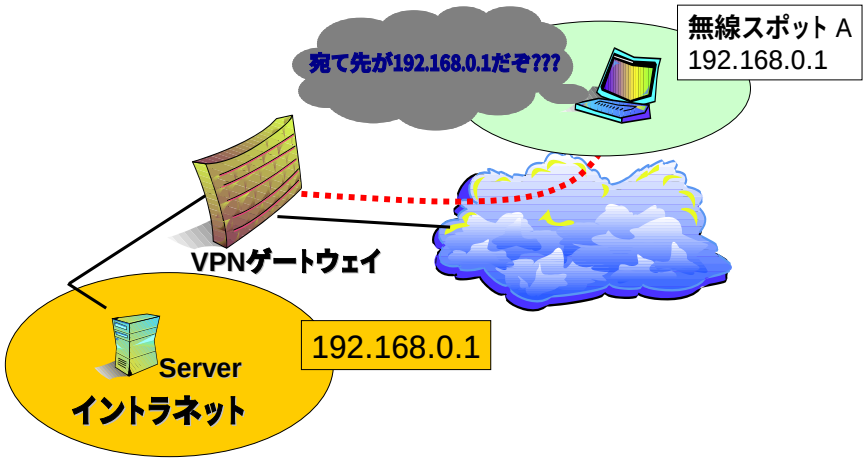
IPアドレスに関する問題
～ IPsec-DHCP ～

- 解決策
  - RFC3456 (Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode)
  - Phase2でDHCP用のSAを確立する。



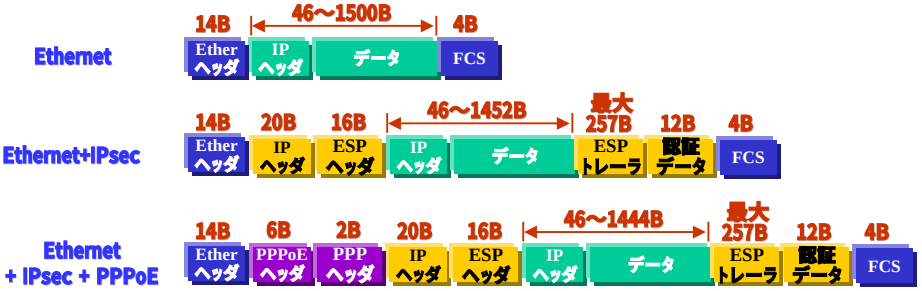
IPアドレスに関する問題

- 無線APと社内のIPアドレスが重複

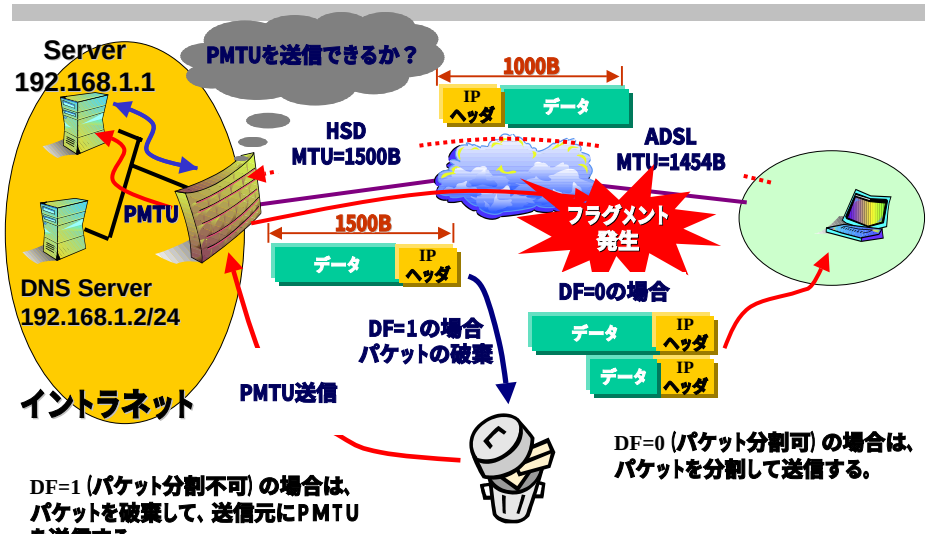


フラグメントに関する問題

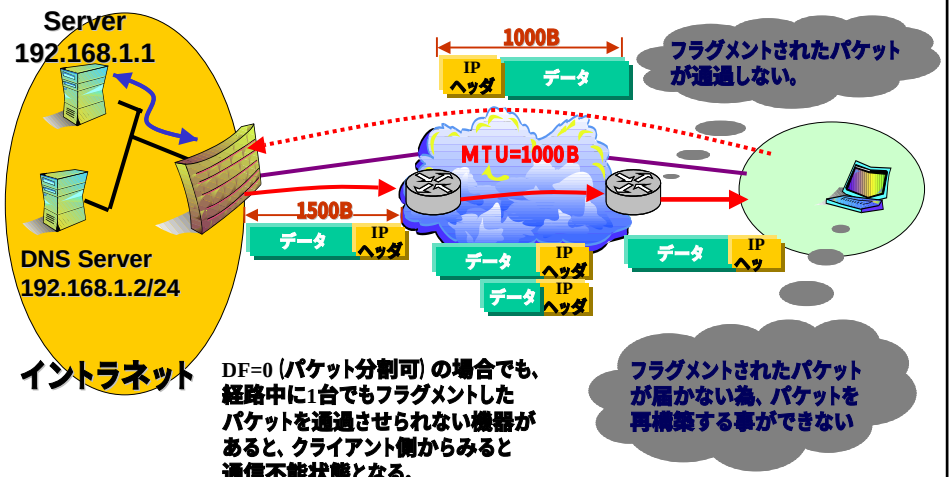
- フラグメントに関する問題
  - IPsec使用により、ヘッダ等の情報追加でMTUを越える可能性が高くなる。
  - HotSpotではADSLが多く使用されているので、PPPoEヘッダ等の追加もあるので、更にフラグメントが発生し易い状態になる。



フラグメントに関する問題

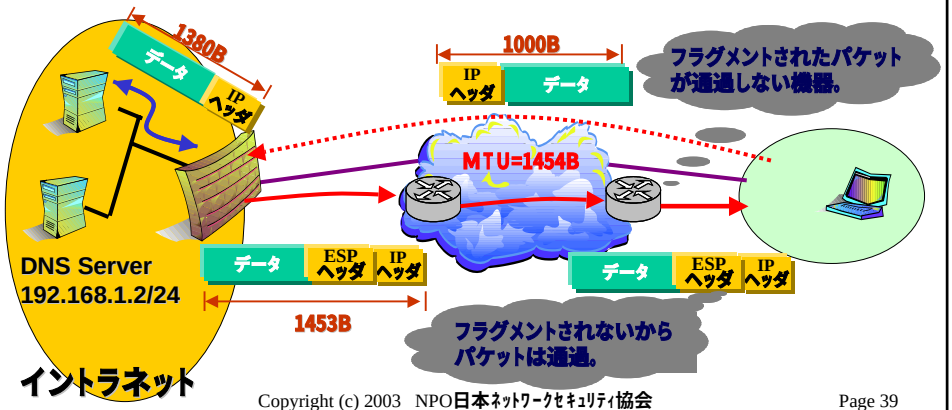


フラグメントに関する問題



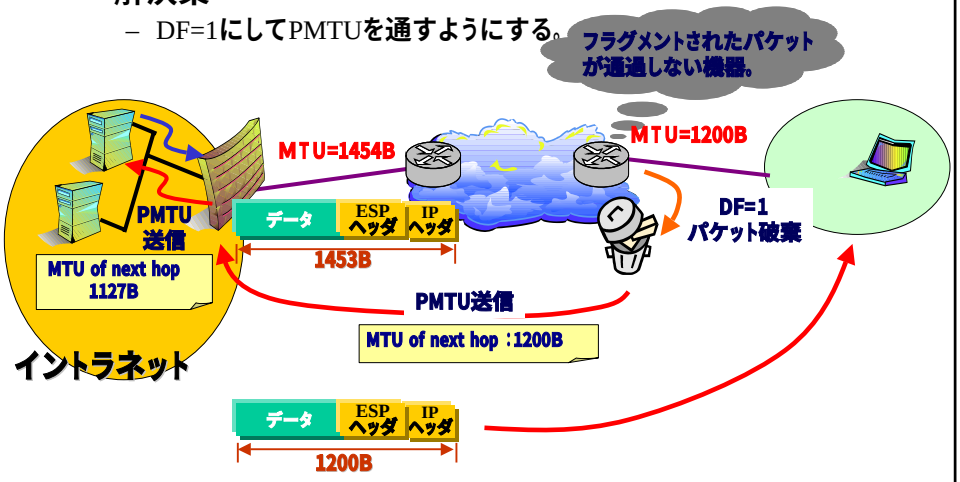
フラグメントに関する問題

- 解決策
  - サーバ側のMTUサイズを調整する。
  - 経験上、1380B程度に設定すればフラグメントによる通信障害の大半は回避できる。



フラグメントに関する問題

- 解決策
  - DF=1にしてPMTUを通すようにする。



その他の問題

- NICとアクセスポイントとの相性
  - テスト前に懸念していた無線LANカードと無線LANアクセスポイントの相性に拠るトラブルは発生しなかった。(IEEE802.11b使用時)
  - 今後、IEEE802.11aやIEEE802.11gによるサービスが一般化したときにも相性による問題が発生する可能性もある。
- ポートのフィルタリング
  - 今回の調査では、一部の公衆無線LANサービスでポートフィルタリングを行っている為、IKEおよびNAT-Tの通信が行えないスポットがあった。

今後の課題

- 調査して感じたこと
  - 環境について
    - 少なくとも作業のための机と椅子は必須
    - 店員に無線アクセスポイントのことがきちんと説明されているところは安心して利用できた
    - 電波が弱く、すぐに切れてしまって実用にならないところも
    - 「この辺りで使えます」などという表示があるとうれしい(実は表示があっても使えないところがあった)
    - 意外と環境は大事である
  - サービスの認証について
    - 複数のサービスを利用する場合、接続時の認証が面倒
    - 今後　事業者間でのローミングを期待

今後の課題

- 無線アクセスサービスの今後
  - 無線LAN自体は確実に広まってきている
  - 新たにサービスを開始する業者もあれば、サービスを停止する事業者も
  - まずはきちんと使える環境を
    - ただ単にアクセスポイントを置くだけではダメ。ユーザが使いやすい環境を
    - 利用できることを広く告知
      - 広い店内などでは目立ちやすい入り口に告知するなど
    - 設置側の店舗での理解･知識が必要
      - 店員に聞いてもよくわからないといったことをなくす

まとめ

- VPN構築において留意すべき点
  - 認証は何を使うか？XAUTHやHybrid Authに対応しているか？
  - NAT-Traversalに対応しているか？
  - ISAKMP-ConfigやIPsec-DHCPに対応しているとより便利
  - 経路上にIKEをふさぐようなデバイスがないか
  - フラグメントが起きて通信できないような場合は予めサーバ側のMTUを小さくしておく。またICMPのPMTUを通すようにしておく。
  - クライアントのデスクトップセキュリティ
    - ウイルスその他の攻撃に遭った場合、それをそのまま会社に持ち込む可能性も考えられる

JNSA

ありがとうございました。

商標について

・本文記載の会社名および製品名は、それぞれ各社の商標又は登録商標です。