

無線LANのセキュリティ ～最新事情と導入の基本方針～

(株)ファム セミナー事務局

<http://www.famm.jp>

根津 研介

nez@samba.gr.jp

Copyright 2003, © Kensuke Nezu,
All rights Reserved.

802.11bセキュリティの「現在」

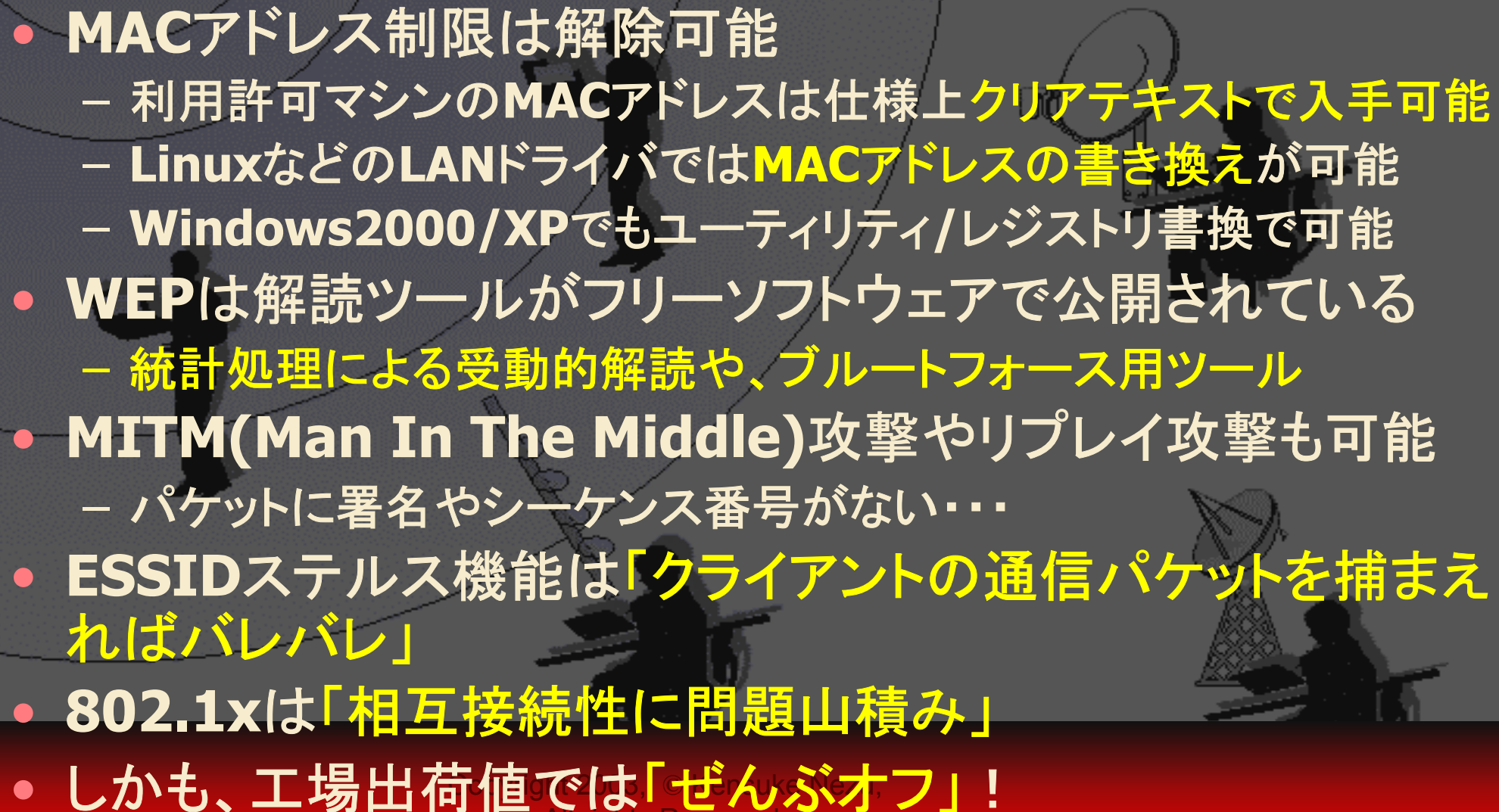
- コンシューマーモデルの機能
 - MACアドレスフィルタリング
 - WEP(40bit, 104bit)による暗号化
 - ESSIDステルス機能
 - ESSID=Any拒否機能
 - (モノによるけれど)ログ機能
- コーポレートモデルの機能
 - コンシューマーモデル機能は当然あって、さらに、
 - 802.1xによる認証と鍵交換の機能

1秒間に10回APが
だすビーコンに
ESSIDを載せない

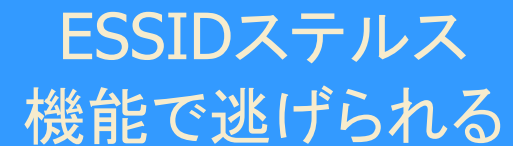
ESSID=Anyのプロ
ブリクエストに
ESSIDを返さない

ESSID=Any設定の
クライアントからの
接続を拒否

()

- 
- **MACアドレス制限は解除可能**
 - 利用許可マシンのMACアドレスは仕様上クリアテキストで入手可能
 - LinuxなどのLANドライバでは**MACアドレスの書き換え**が可能
 - Windows2000/XPでもユーティリティ/レジストリ書換で可能
 - **WEPは解読ツールがフリーソフトウェアで公開されている**
 - 統計処理による受動的解読や、ブルートフォース用ツール
 - **MITM(Man In The Middle)攻撃やリプレイ攻撃も可能**
 - パケットに署名やシーケンス番号がない...
 - **ESSIDステルス機能は「クライアントの通信パケットを捕まえばバレバレ」**
 - **802.1xは「相互接続性に問題山積み」**
 - **しかも、工場出荷値では「ぜんぶオフ」!**

APのMACアドレスから メーカーも分かる

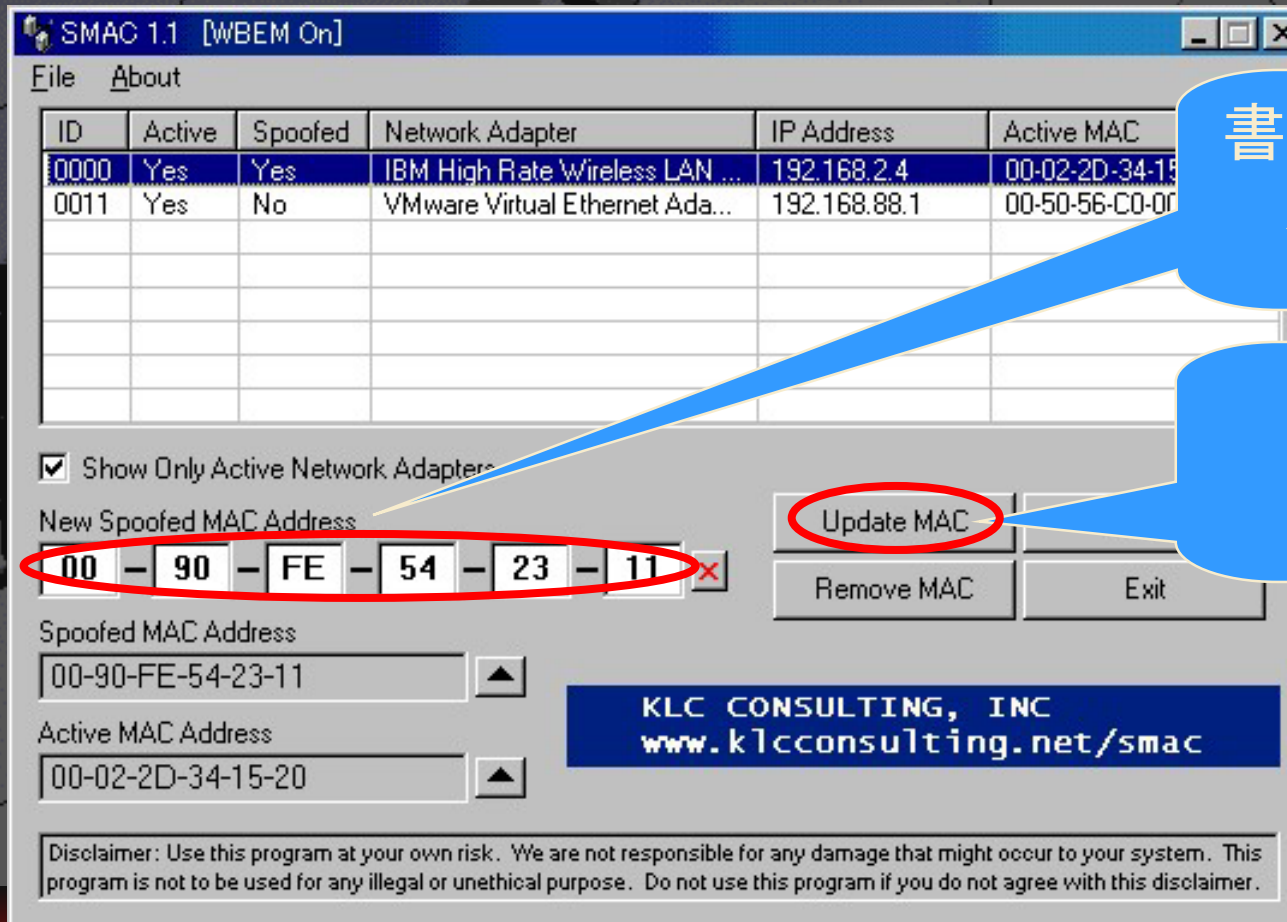


MACアドレス変更ソフト (Windows)

SMAC

2003/03/22 NT-Committee2

緊急対応コンピュータセキュリティ研究会



書き換えたいアドレスを入れて...

このボタンを押すだけ！

無線LANキャプチャ(Linux) Ethereal

No.	Time	Source	Destination	Protocol	Info
153	14.641749	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
154	14.744399	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
155	14.846510	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
156	14.876999	Agere_34:15:20	SUMITOMO_26:02:a2	IEEE 802.11	Data
157	14.877209		Agere_34:15:20 (RA)	IEEE 802.11	Acknowledgement
158	14.949151	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
159	15.051378	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
160	15.153735	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
161	15.256268	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
162	15.358790	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
163	15.461144	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
164	15.563112	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
165	15.622735	00:00:00_00:00:00	00:00:00_00:00:00	IEEE 802.11	Association request
166	15.665476	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
167	15.767917	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
168	15.870331	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame
169	15.972770	ELECOM_70:0b:8c	Broadcast	IEEE 802.11	Beacon frame

Duration: 258
BSS Id: 00:90:fe:70:0b:8c (ELECOM_70:0b:8c)
Source address: 00:02:2d:34:15:20 (Agere_34:15:20)
Destination address: 00:00:5f:26:02:a2 (SUMITOMO_26:02:a2)
Fragment number: 0
Sequence number: 1133
☒ WEP parameters
Data (108 bytes)

ESSIDステルス機能
を使っても端末側の
フレームにはESSID
が載っている

通信を許可された
クライアントのMAC
アドレスもばれ

WEP解析ソフトウェア(Linux) AirSnort

どれだけのパケット
が必要かは何とも
いえない

WEPの脆弱性で事
前共有鍵はばれる

The screenshot shows the AirSnort application window. The menu bar includes File, Edit, Settings, and Help. The interface has several input fields: 'scan' (checked), 'channel' (set to 1), 'Network device' (wlan0), and 'Card type' (Prism2 (wlan-ng)). On the right, there are settings for '40 bit cr...' and '128 bit cr...' with 'readth' and 'breadth' values of 2 and 3 respectively. Below these is a table with columns: C, BSSID, Name, WEP, Last Seen, Last IV, Chan, Packets, Encrypted, Interesting, PW: Hex, and PW:. The first row of data is highlighted with a blue background. The 'Encrypted' and 'PW: Hex' columns in this row are circled in red. At the bottom of the window are three buttons: Start, Stop, and Clear.

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW:
X	00:09:41:07:71:19	WirelessNetwork	Y		AF:B7:C4	1	5486764	5241927	3574	CA:FE:CA:FE:CA	
	00:90:FE:70:0B:8C	WirelessNetwork	Y		00:00:00	6	18	0	0		
	00:00:00:00:00:00				00:00:00	6	3428	0	0		
	FF:FF:FF:FF:FF:FF				00:00:00	6	1498	0	0		

WPA (Wi-Fi Protected Access) は 救世主になりうるか？

σ(--#)アタマイターツ~

- AirSnort等の解析よけにはなる
- WPA for Home/SOHOではTKIP採用
 - 事前共有鍵の管理が必要なのは802.11bと一緒に
 - 企業で導入する場合、鍵の管理がタイヘン
- WPA for EnterpriseではEAP+802.1x+RADIUS採用
 - 複雑な相互接続性の問題はそのまま残る...
 - CA局による証明書の管理、またはサポートする認証方式 (PEAP、LEAP、MD5等) の選択の問題 → 管理がタイヘン
 - CA局、RADIUSサーバの構築運用のコストもかかる
- しかも、工場出荷値では「ぜんぶオフ」なのは一緒！

802.11a,802.11g,802.11iは・・・？

- 802.11a製品は相互接続性認証(Wi-Fi Certified)が始まったばかり
- 802.11g製品は見切り発車で相互接続性認証(Wi-Fi Certified)は計画段階
- 802.11a/gはセキュリティ的には802.11bレベル
- 802.11i製品がでてくるのは2003年末～2004年？

(;_;)導入するのはまだ冒険？

じゃあ、どうすればいい？

SIerが相互接続確認したもので揃える

- 現段階では、どこかに見切りが必要
- 1メーカー製品で上から下まで揃えられるか？
 - 無線**LAN**内蔵ノート**PC**等が無視される場合も...
 - Windows**XP**のみ対応の場合も...
- 802.11bでできる限りのセキュリティを施す？
 - 無線**LAN**は小型のインターネットのようなもの、有線**LAN**はセキュリティポリシーのレベルが異なる
 - 異なるレベルのものを接続させるポイントは、インターネットの**DMZ**と一緒に＝ゲートウェイによる分離
- 「無線**LAN**は使わない」という選択肢もある

802.11bでできる限りのセキュリティを施す(1)

- ナーバスな情報(顧客情報等)を無線LANに流さない
- 無線LANはアクセスポイントもクライアントもミニ放送局だという意識を持つ
- 扱っている情報を類推されるので、意味のある(企業名等)ESSIDをつけない
- WEPは128ビットで16進数で指定する
- WEPキーは期間ごとに更新する←これがタイヘン
- WPA対応を表明しているメーカー製品を採用する

802.11bでできる限りの セキュリティを施す(2)-1 ～理想編～

- セキュリティポリシーの異なるもの同士の接続
インターネット

→ 外向き
← 内向き

有線LANエリア



ファイアーウォール



Private CA局

RADIUS

ファイアーウォール

無線LANエリア



802.1x対応
AP

理想

- ユーザ認証
- TKIPキー配布

802.11bでできる限りの セキュリティを施す(2)-2

～理想編～

- RADIUSサーバー＋802.1x
- メリット
 - － WEP鍵の管理が不必要
 - － 通信の初期段階からユーザ認証可能
- デメリット
 - － 相互接続性の問題がある
 - － 認証方式にEAP-TLSを利用した場合、別途CA局が必要
 - ※CA局をプライベートに立ちあげサーバー/クライアントに配布する管理が別途必要になる
 - ※EAP-TTLS, LEAP, PEAP等は相互接続性にまだ問題が...
 - － RADIUSサーバーの管理も必要

802.11bでできる限りの セキュリティを施す(2)-3 ～理想編～

- 実現方法1: 相互接続性が保証されているメーカー製品での統一
 - － 手間はかからないが金銭的な負担や、サポートできない端末も・・・
- 実現方法2: フリーのFreeRADIUS + HostAPドライバによるアクセスポイントの構築(マニア向け?)
 - － どちらもLinux/*BSD上でCVS版を使う必要がある
 - － 情報は英語ページがほとんど
 - － オウンスクでの利用が必要
 - － サプリカント(端末ソフト)は、無償ダウンロードできるものやWindowsXPの機能を利用する

802.11bでできる限りの セキュリティを施す(3)-1 ~現実編1~

- セキュリティポリシーの異なるもの同士の接続
インターネット

→ 外向き
← 内向き

有線LANエリア

ファイアーウォール



IPSec
PPTP

ファイアーウォール

無線LANエリア



ファイアーウォール

現実1

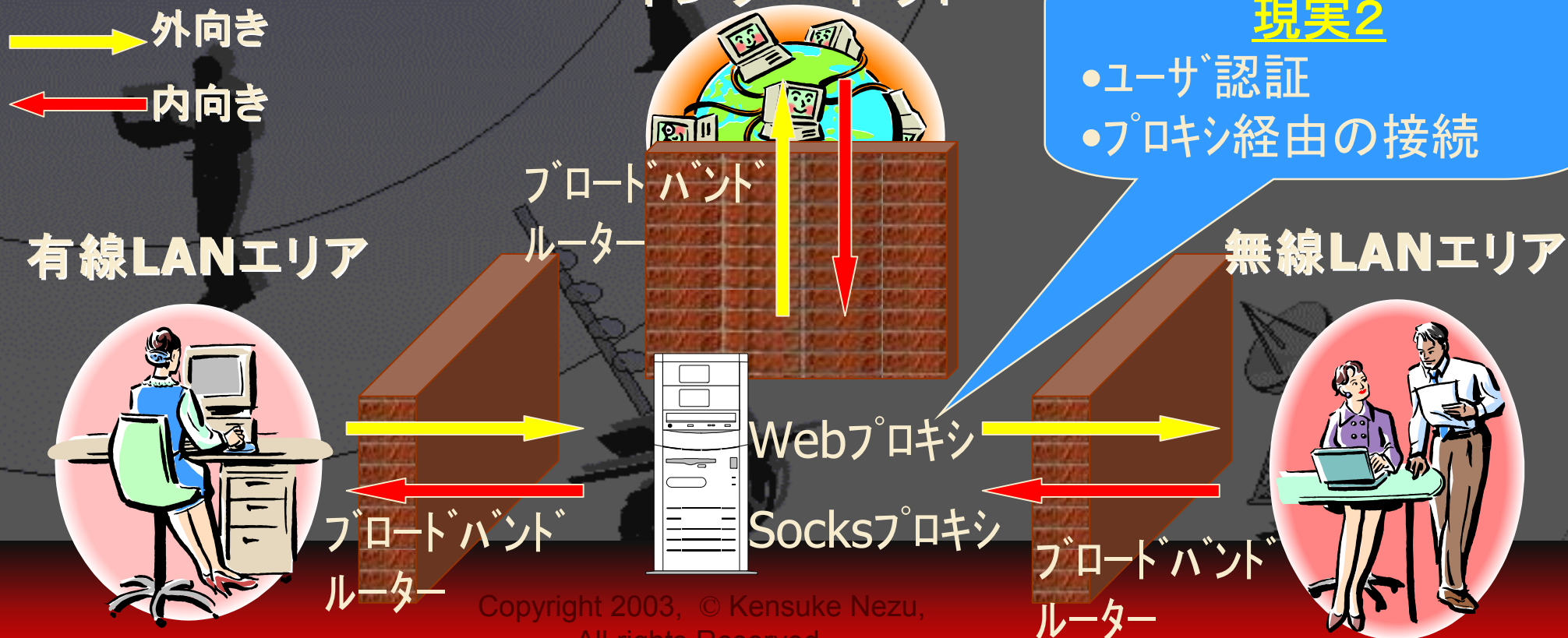
- ユーザ認証
- 通信の暗号化

802.11bでできる限りの セキュリティを施す(3)-2 ~現実編1~

- IPsecまたはPPTPによる接続
- メリット
 - ー 現時点では相互接続性が比較的ある
 - ー IPsecの暗号化は現在のところ安心(PPTPは……………)
- デメリット
 - ー WEP鍵の管理が必要(でもそう頻繁に変更しなくてもよい?)
 - ー 通信の初期段階で必ずしも暗号化通信が行われるわけではない
 - ー IPsecは初期設定のノウハウが充実していない
 - ー クライアントの防御が別途必要になる

802.11bでできる限りの セキュリティを施す(4)-1 ~現実編2~

- セキュリティポリシーの異なるもの同士の接続
インターネット



802.11bでできる限りの セキュリティを施す(4)-2 ~現実編2~

- Webプロキシ/Socksプロキシ等の利用
- メリット
 - 比較的簡単、手軽に実現可能
 - 有線LAN、インターネットからは隔離できる
 - コンシューマー機器で構築可能(ホームユーザでも実現可)
- デメリット
 - WEP鍵の管理(定期的な手動変更)が必要
 - 通信の内容は守れない可能性がある(ID/パスワードも...)
 - ※無線LANから有線LANには怖くて入れられない
 - クライアントの防御が別途必要になる

使わないという選択肢

- 前述のような管理や構築が不可能/できないという場合は、使わないという選択肢もある
- あと1年くらいすると、802.11iや802.11gも構築や相互接続のノウハウができている可能性もあるのでそれまで待つのも手
- **使わない場合も、定期的にNetStumblerなどを利用して勝手に設置されたアクセスポイントがないか監視する必要がある**
 - コンシューマー製品は手軽に買えてしまう
 - 有線LANから見たときに判別できないケースもある
 - ただし、社外のアクセスポイントである可能性も考慮すること
- セキュリティポリシーを設定して、「設置許可願い」を作っておくことで、潜在的な「設置予定者」を炙り出す手もある

まとめ

- 現状では、利用用途と管理コストを考慮した運用が必要
- 基本的に脆弱であることを認識することが必要
 - － ユーザにも周知が必要
 - － えらい人にも周知が必要
- 過渡期の製品なので製品寿命をあまり長く見てはいけない
 - － 無理に高価なものを導入するのは考えもの
- 最悪でも、社内の「機密情報」や「顧客情報」にアクセスする手段は排除しておくことが必要
- コンシューマー製品は、「企業向け」ではないことをえらい人に周知することが必要
 - － 「こんなに安く売っているものを何故使わないんだ！」が成り立たないことを場合によっては実証する必要がある

参考文献(1)

いちおし！

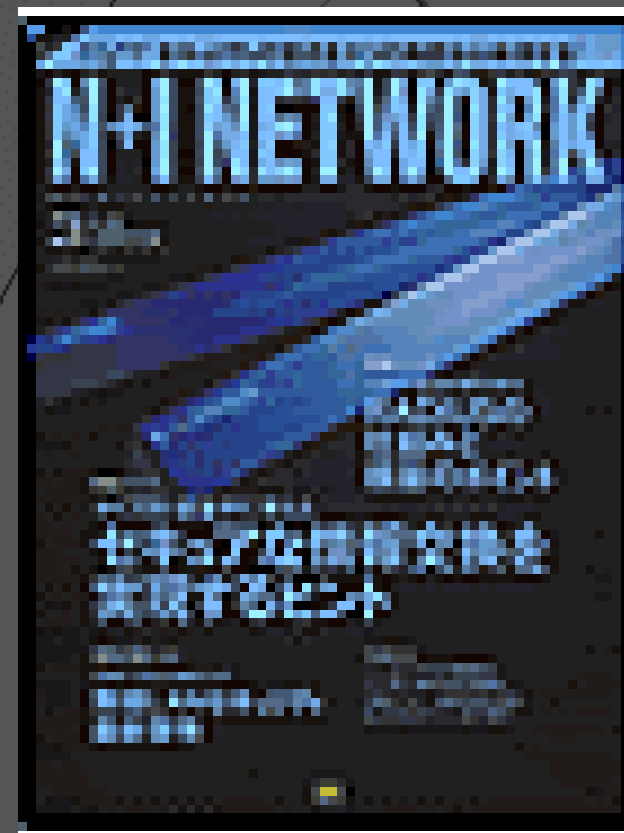
- 日経ネットワークセキュリティ
～無線LANパニック～
 - － 法律的な面や関係省庁の見解、
弁護士の見解もある
 - － WPAに対する各メーカーの
アップグレード方針もわかる
 - － 無線LANに関する最強の1冊
 - － 流通業界での顧客情報漏洩事
例も紹介されている



参考文献(2)

おすすめ！

- N+I NETWORKガイド
2003/03号
 - ー Sierからみた無線LANの解説記事がある
 - ー RADIUSの仕組みと構築のポイントに関する記事がよい



参考文献(3)

待ちきれない
人、英語に自
信のある人は
頑張って英語
版を読もう！

日本語版を待て！

- 802.11 Security
 - O'Reilly本
 - FreeBSD/NetBSD/Linux/Mac OS Xのクライアント設定例がある
 - hostAPドライバ(*BSD/Linuxをアクセスポイントにするドライバ)の解説がある
 - ゲートウェイの構築についてのヒントも...
 - トータルな無線LANセキュリティの解説本としてオススメ



参考URL

- Host AP driver for Intersil Prism2/2.5/3
<http://hostap.epitest.fi/>
- FreeRADIUS -- building the perfect RADIUS server --
<http://www.freeradius.org/>
- WPAに関する一次情報
<http://www.wi-fi.org/OpenSection/secure.asp#resources>
- 無線LAN ML“ドット・イレブン”
<http://www.freeml.com/info/dot-eleven>