

外出先からでも業務がしたい！ その時のセキュリティ対策は?? (リコーにおけるモバイル事例)

2003年1月28日

業務革新

IT活用

IT/S: Information Technology
& Solution

RGO platform



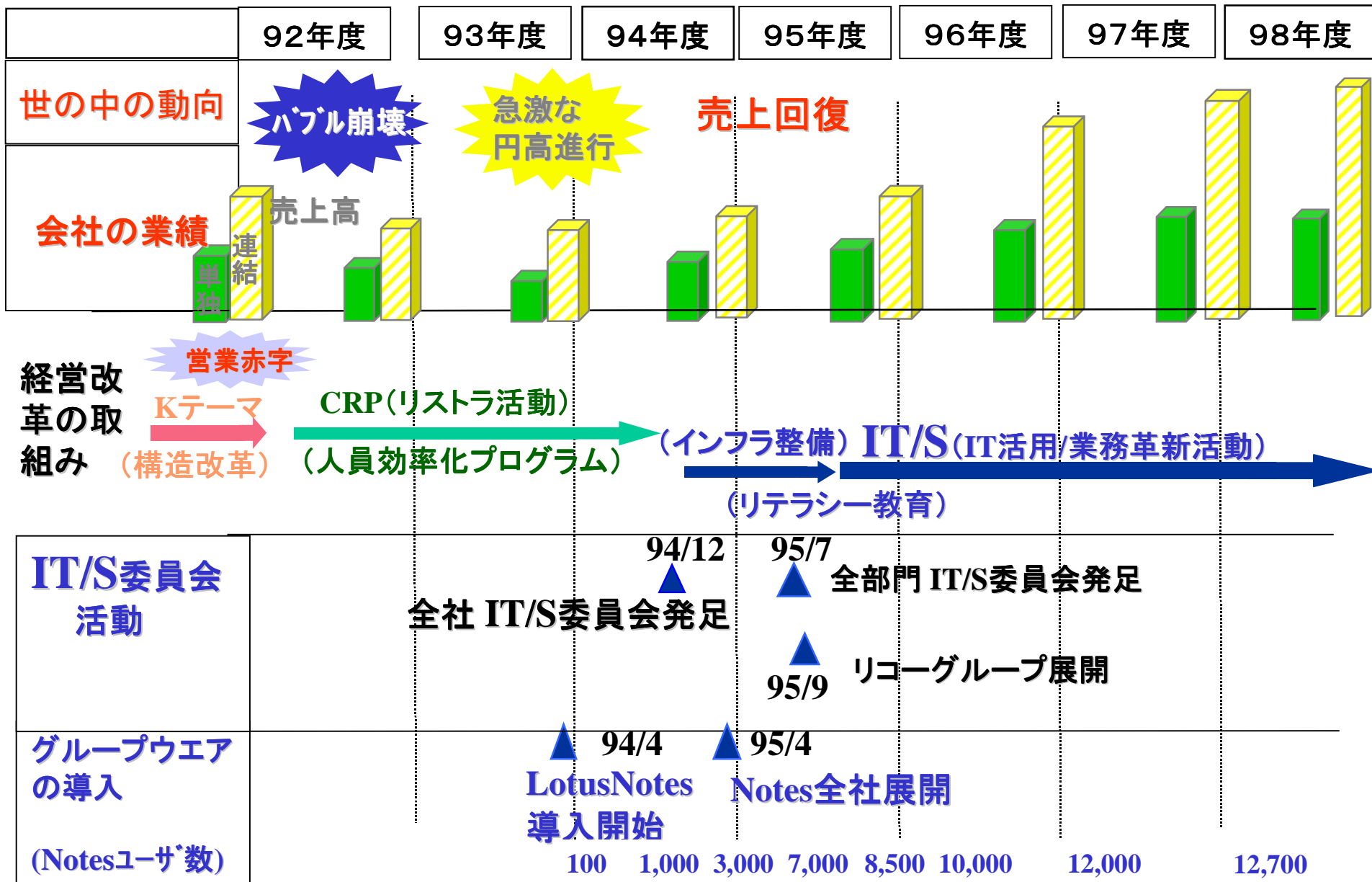
株式会社リコー IT/S本部

IT/S推進センター IT/S技術グループ

宮腰 寿之

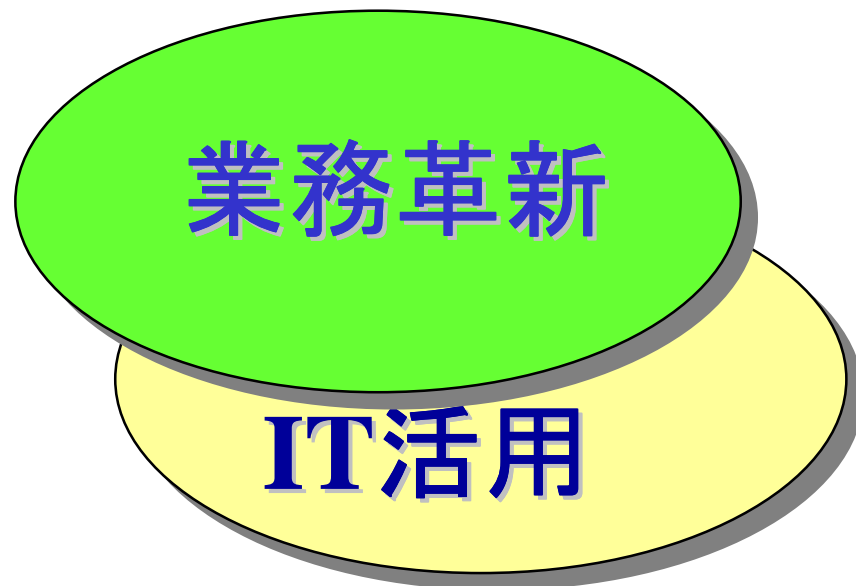
miya@isd.ricoh.co.jp

リコーにおけるIT/S活動の歴史



『業務革新が主役』

業務革新とIT活用の同時進行

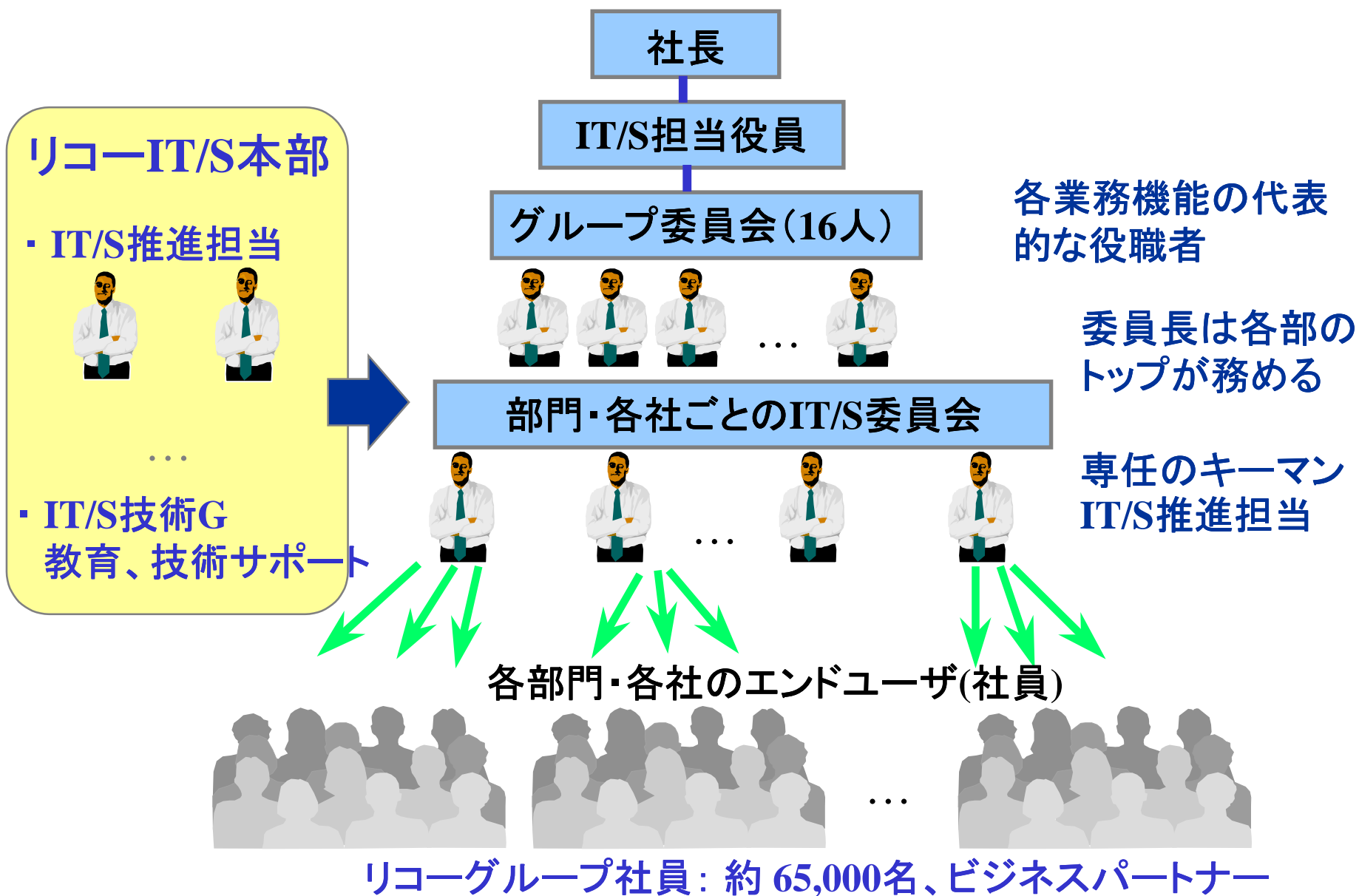


止められないか

プロセスの中抜きが出来ないか

今迄出来なかった業務が出来る様にならないか

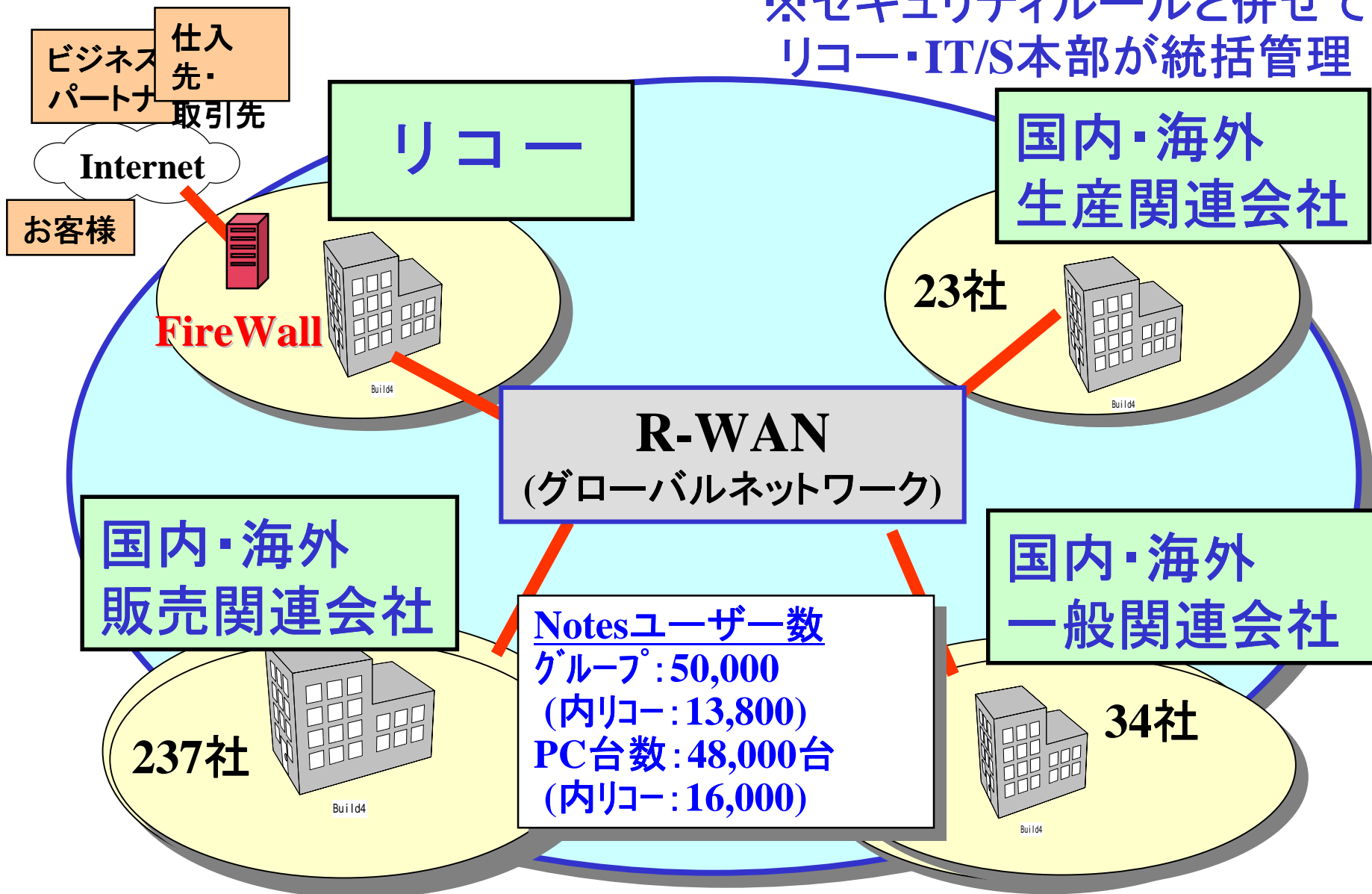
グループIT/S活動の推進組織



グローバル・ネットワークの構築

= 全世界を結ぶネットワーク作り =

※セキュリティルールと併せて
リコー・IT/S本部が統括管理



リコーグループのWAN構成について

当初は、CAD用のデータ交換のためのネットワークとして利用を開始。

1987年から構築を開始し、1995年に大規模再構築を実施。随時、増速を実施中。

名称:R-WAN (Ricoh Widearea Network)

- ・現在は、主にIP-VPN網を利用
- ・対象は、リコーグループ関連会社

a. 国内部分及び国際部分

現在のネットワークは、3つの系統で構成されており、それぞれ別々の会社に出注している
また、トータルな運用をリコーテクノシステムズ(RTS)に業務委託

- 1) 社内・開発・生産系
(リコー及び開発・生産関連会社を接続)
- 2) 総合販売会社系
(国内販売系関連会社を接続)
- 3) 国際系
(海外関連会社を接続)

b. ネットワークのアウトソーシングの考え方

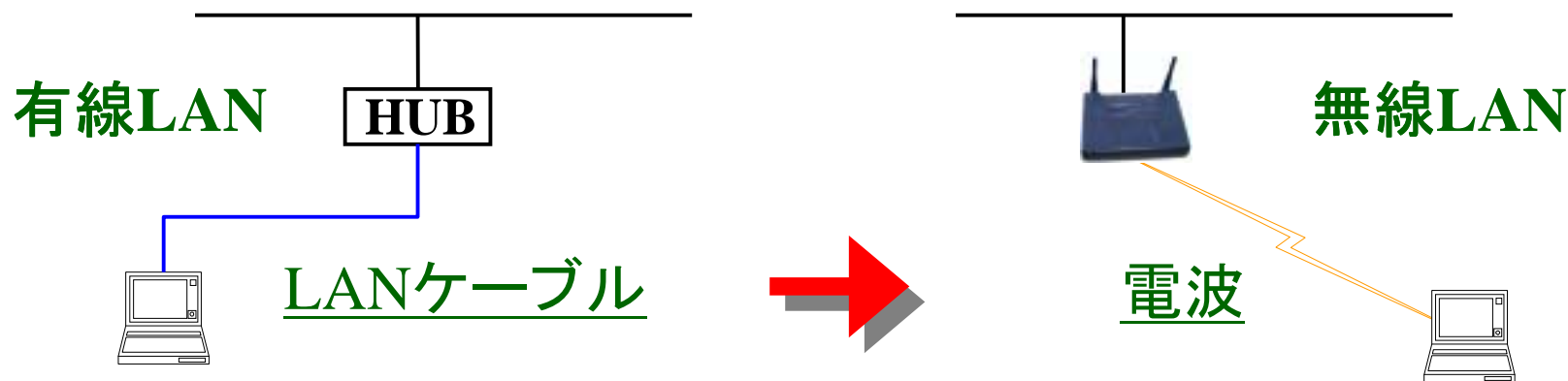
1995年の大規模再構築からアウトソーシングを実施

<方針>

- 1) 日常運用を委託する
- 2) 技術はリコーに残す
- 3) ワンストップショッピングが基本
 - ・通信費
 - ・ルーター費用(レンタル・保守)
 - ・監視／運用費用

社内でのモバイル (無線LANの利用)

無線LANとは



PCなどを無線でLANに接続

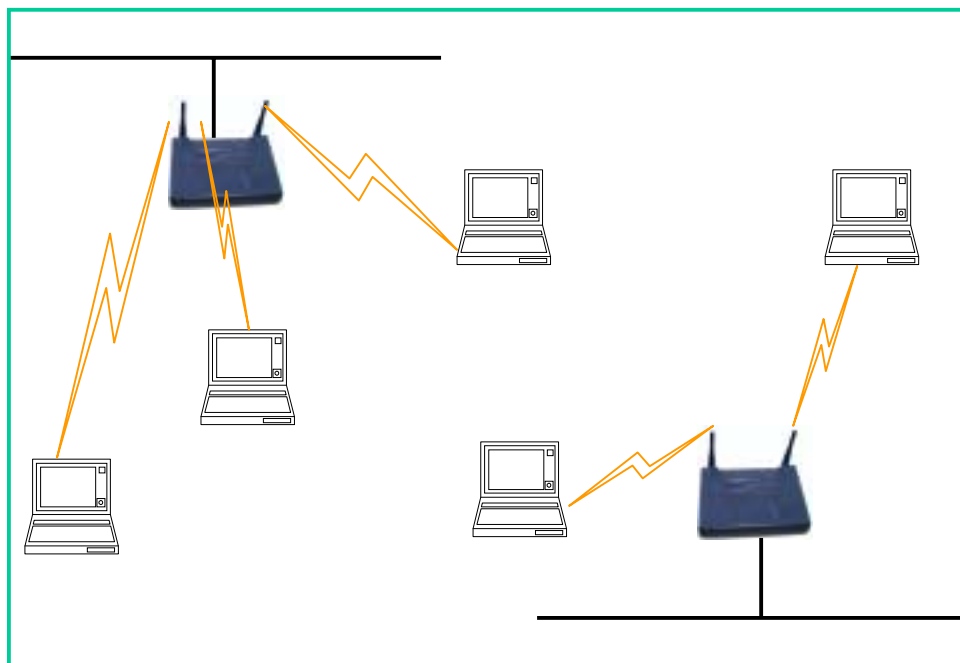
電波の届く範囲ならばLANアクセス可能

方式として、電波と赤外線の2種存在

電波と赤外線のリコーでの利用例

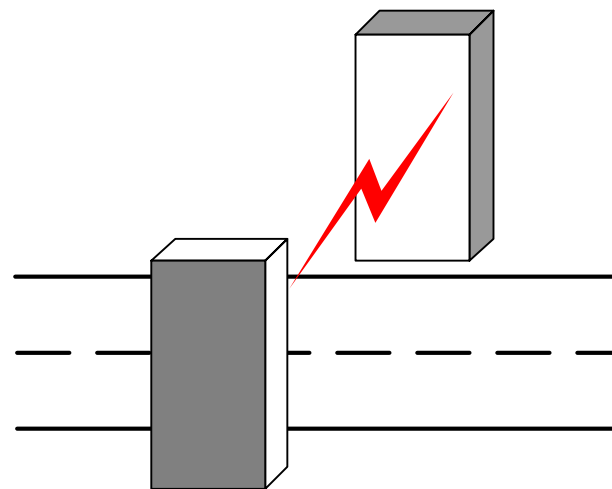
電波

- オフィス内
- 隣接した建て屋間



赤外線

- 距離のある建て屋間



無線LANの規格

現在の規格

方式	IEEE802.11b	IEEE802.11g	PBCC	IEEE802.11a	HiSWANa
電波	2.4GHz帯	2.4GHz帯	2.4GHz帯	5GHz帯	5GHz帯
最大伝送速度	11Mbps	54Mbps	22Mbps	54Mbps	54Mbps
備考	IEEE802.11と互換	IEEE802.11bと互換	IEEE802.11bと互換		

• IEEE802.11b

- 2.4Ghz帯を利用
 - 最大伝送速度11Mbps
 - 異メーカー同士の相互接続性の保証あり
- **Wi-Fi**

無線LANの特徴

メリット

LAN配線が不要となり、初期導入費が安価
→レイアウト変更柔軟に対応

内蔵バッテリーを併用することでケーブル不要

デメリット

設置環境や使用環境等により
通信が不安定となることがある

電波によるため、不正侵入や
通信内容が傍受される危険性がある

11Mbpsの帯域共有のため、通信速度に限界

(株)リコー導入の背景

Step1:会議のペーパーレス化・効率化を推進

- Notesサーバに資料を置き、各自のPCで資料を見ながら会議を実施したい
→LAN環境が必要

Step2:会議室で気軽にLAN環境を利用したい

- 事前に、HUBの設置やLANケーブルの敷設といったLAN敷設工事が必要となり大変
- 移動の都度IPアドレス等の設定変更がPC側で必要となり、手間がかかる

東品川事業所への導入

1999年9月：当時最新の2Mbps機による試行

2000年7月：11Mbps機の全館設置（B1～6F）

事業所全体で、AP8台・カード約200枚
（1フロア約1,000m²）

DHCP(IPアドレス自動配布)を併用

→IPアドレスの設定が不要

全館にわたり、1つの専用サブネットを敷設

→どのフロアでも同じアドレス利用可

他事業所への展開(2002年12月現在)

24事業所・研究所・工場の全てにて導入

AP約300台、無線LANカード約3,000枚

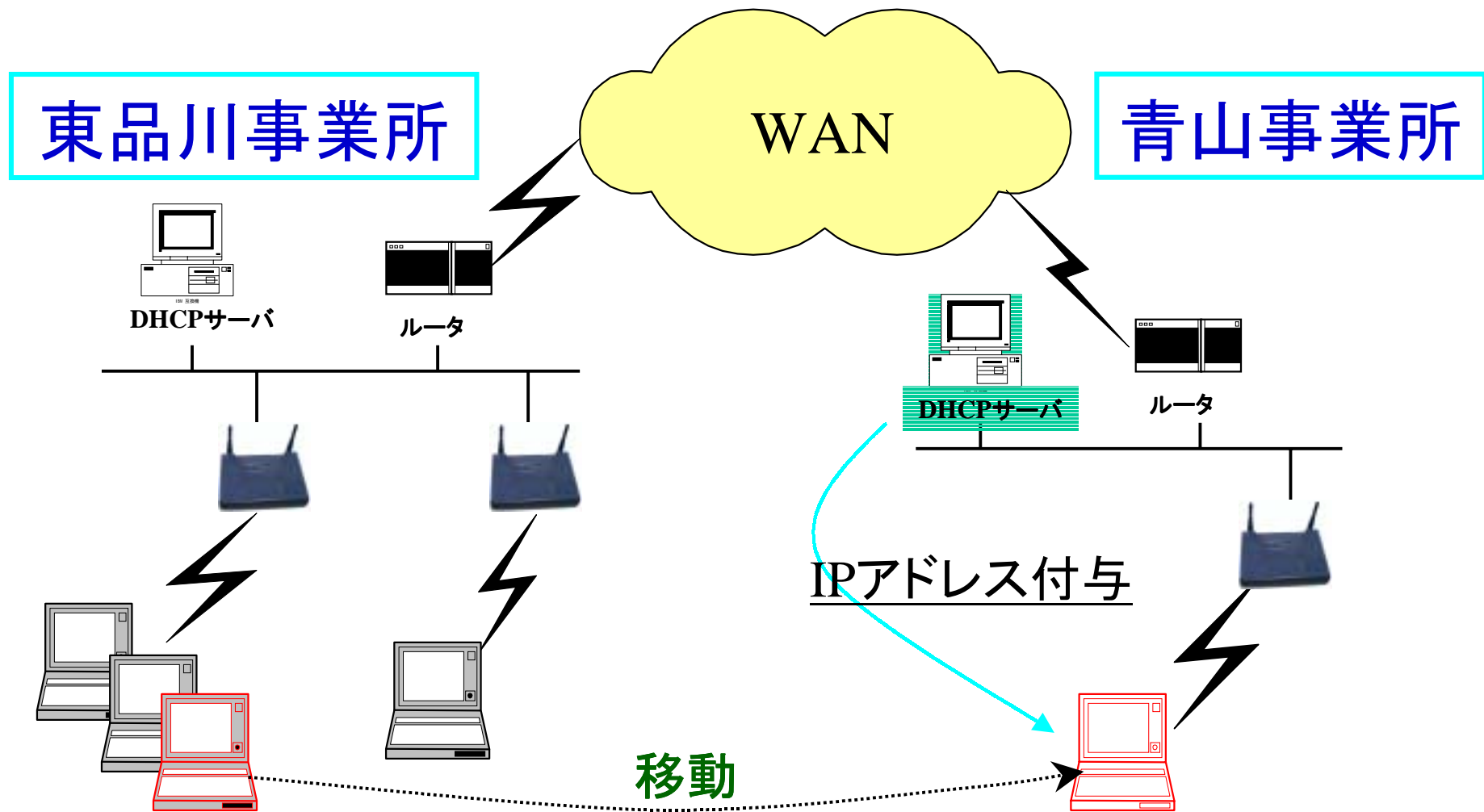
DHCPを利用して、事業所間の利用も可

干渉問題や技術的な問題がある為、
IT/S本部主体で計画的に展開

業務効率化につながる場所で優先的に導入
(共通会議室・工場・実験室等)

無線LAN接続イメージ図

※MACアドレス登録済みの無線LANカード利用が前提



→設定変更無く移動先でネットワークに接続可能

セキュリティ上の留意点

電波の**不正侵入**や**盗聴**を防ぐ必要がある

不正侵入対策

ESSID(SSID)設定

MACアドレス制限

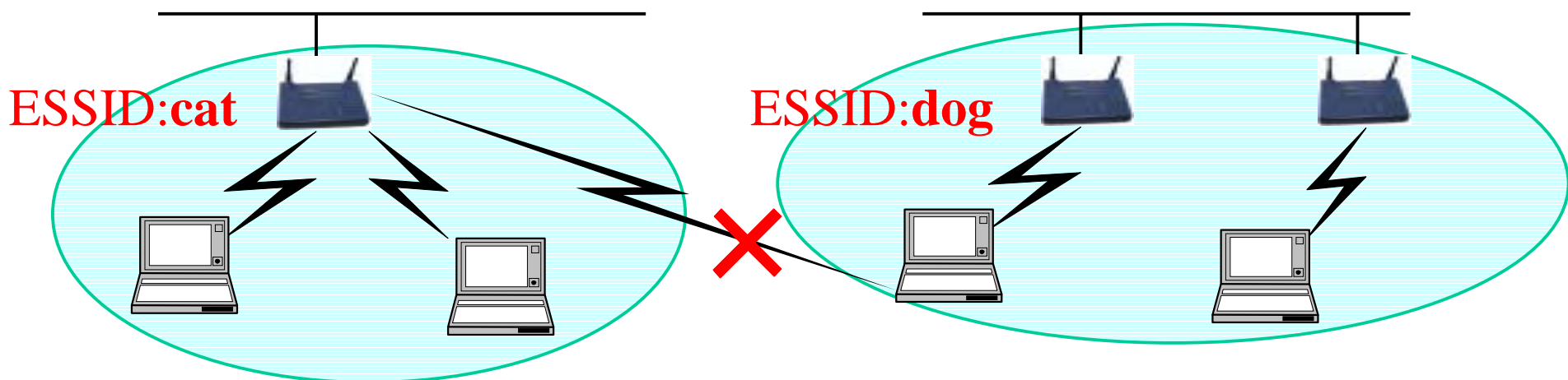
盗聴対策

暗号化 (WEP)設定

セキュリティ(ESSID)

PC-AP間で同じKEYを設定することで、無線通信部分を論理的にグループ分け

ESSIDが同じ機器同士でしか通信ができないため、不正接続を防止



→ESSIDが判明しない限り接続不可能

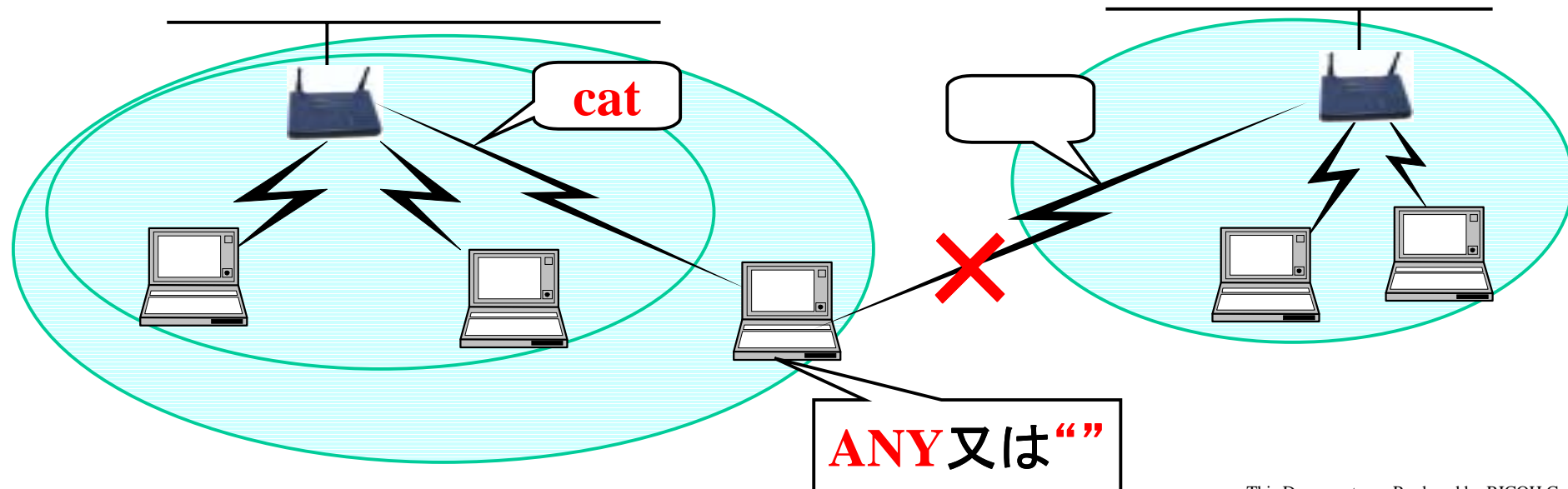
セキュリティ(ESSID)

ESSIDを電波で配信してしまうAPでは、
ESSID未設定又は“ANY”で不正侵入可能！

CISCO AironetはESSIDの配信を止められる

ESSID:cat

ESSID:dog



セキュリティ(MACアドレス制限)

通信できる端末を、MACアドレスにより
制限を行うしくみ



あらかじめ登録された機器しか
通信できないため、不正侵入を防止

MACアドレスリストの管理が必須

すべてのAPに設定する必要あり

セキュリティ(WEP)

無線部分を暗号化して通信を行うしくみ




電波を傍受されても、通信内容は漏れない
盗聴防止

暗号化キーが合わないと通信できない

- Static WEP Keys(固定)
64bitと128bit、128bit非対応の機種もある
- Dynamic WEP Keys(変動)
通信毎に暗号化キーを変え、高セキュリティ

データベースのマニュアル例

無線LAN管理データベースより抜粋

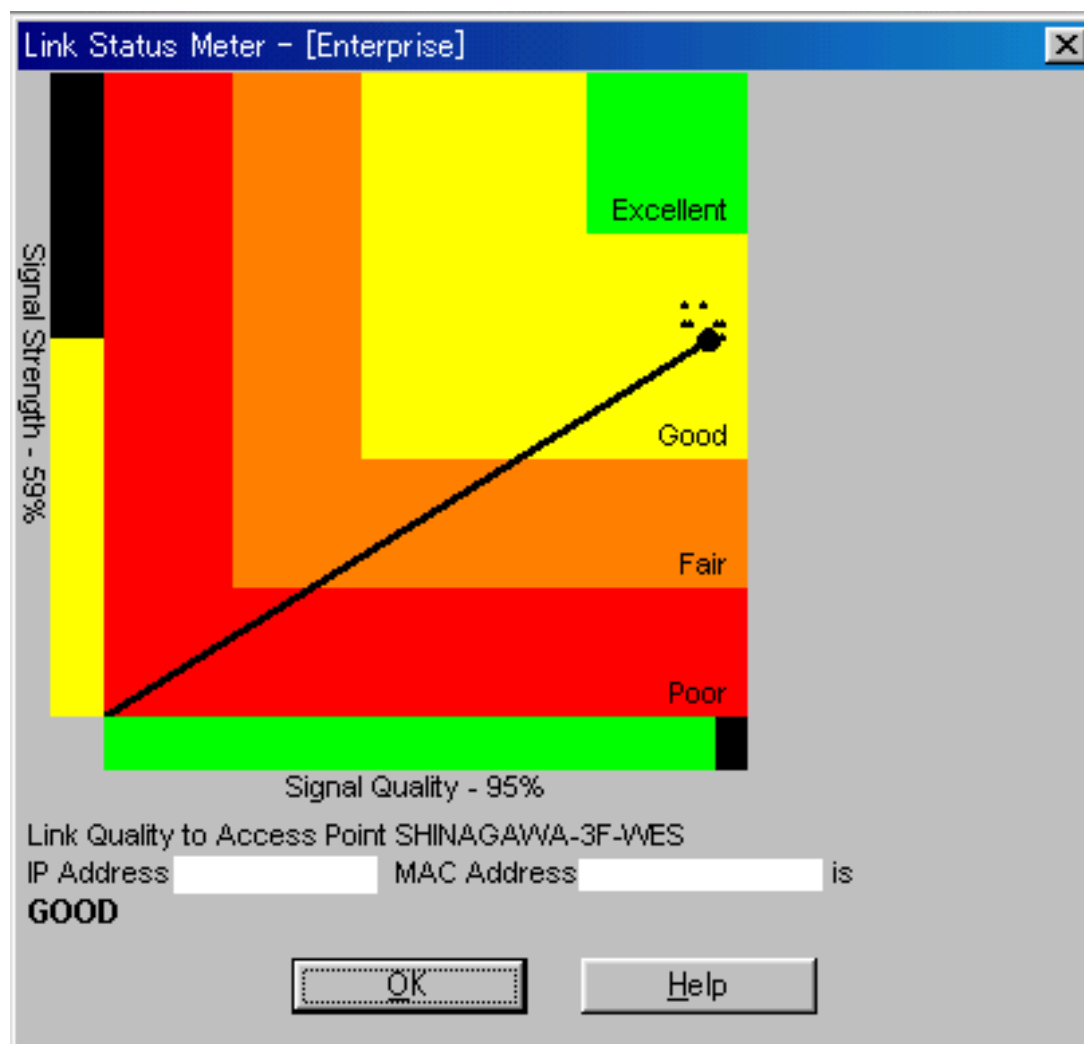
無線LAN管理	 閉じる  文書の編集  マニュアル文書作成	
<ul style="list-style-type: none"> ▶ AP情報 ▶ カード管理 ▶ マニュアル ▶ 拠点情報 ▶ 受信メール ▶ 登録申請文書 ▶ 廃止カード 	区分	タイトル
	▼ 1. 必ずお読みください	
		はじめに
	▼ 2. カードの購入と登録	
		無線LANカードの購入方法
		無線LANカードの登録申請方法
	▼ 3. 設定	
		【CISCO製】無線LANカード設定方法
		【CISCO製以外】無線LANカードの設定について
		【メルコ製】無線LANカード(WLI-PCM-L11)設定簡易マニュアル
	▼ 4. 利用可能場所	
		導入拠点一覧
	▼ 5. トラブルシューティング	
		Cisco LANカード 350を認識しない
		建物をまたいで移動したら通信できなくなった
		無線LAN系以外の系と通信ができない
	▼ 6. Tips	
		Windowsファイル共有の設定方法
		【重要】IPアドレスが取得できているかの確認方法
	▼ 7. 問い合わせ先	
		問い合わせ先

設置事例



ツールを用いた電波調査例

利用対象場所で常に“Good”以上であること



今後の技術動向(通信速度)

現在、通信速度11Mbpsの製品が主流

2.4GHz帯を利用 (IEEE802.11b)

最大54Mbpsの規格が制定

5.2GHz帯を利用 (IEEE802.11a)

APのカバーエリアが比較的狭い

IEEE802.11bとの互換性は無いが共存可

→評価後、技術動向を見て、展開を検討

今後の技術動向(認証方法)

IEEE802.1xの認証方法

RADIUSサーバによるユーザー認証システム

ユーザー毎に個別のWEPKey利用可能

通信中にWEPKeyを変えることが可能

WEP2により暗号化機能の強化

→認証方法と複数メーカー共存環境で利用可能性を検証した上で導入の方向

社外でのモバイル
(リモートLANアクセスの利用)

リモートLANアクセスサービスの背景

外出先・自宅からNotesを使いたい!!
(メールの送受信を含めた業務全般の実施要望)

当初はNotesサーバへダイヤルアップ

問題点・要望:

- ・Notes用モデムファイルのメンテナンスが大変
- ・Notes以外の業務も行いたい。

1998/4～『リモートLANアクセスサービス』を開始

システムのアウトソーシング

システムは三菱電機情報ネットワーク(MIND)に
アウトソーシング

- ①運用管理負荷の軽減
 - ・ユーザ管理(新規登録・変更・削除)
 - ・アクセスサーバ管理
 - ・ルータ設定管理
 - ・回線監視
- ②24時間365日の運用体制

セキュリティルールに添ったID体系

ワンタイムパスワード(OTP)、固定パスワード、
発信者番号認証の併用

- ・異なるセキュリティレベルを利用し、アクセスを制限
＜使用アプリケーション制限＞
 - OTP、発信者番号認証：制限無し
 - 固定：Notes,スケジュール管理ツールのみ
- ＜ユーザIDに対するセキュリティ制限＞
 - OTP:5回連続入力ミスでロックアウト
 - 固定、発信者番号認証:9回,3ヶ月の有効期限

ワンタイムパスワード(OTP)とは

一分毎に異なる6桁の数字を表示し、接続時刻毎に異なる認証を行う。

表示されているその時だけ有効な、使い捨てのパスワード



※個人コード4桁+OTP6桁の、10桁のパスワードにて認証

MINDを選択した理由

着信課金による距離に関係ない全国一律の通信料金

全国同一番号のため、場所を移動するごとに一番近い
アクセスポイントを探す必要がない

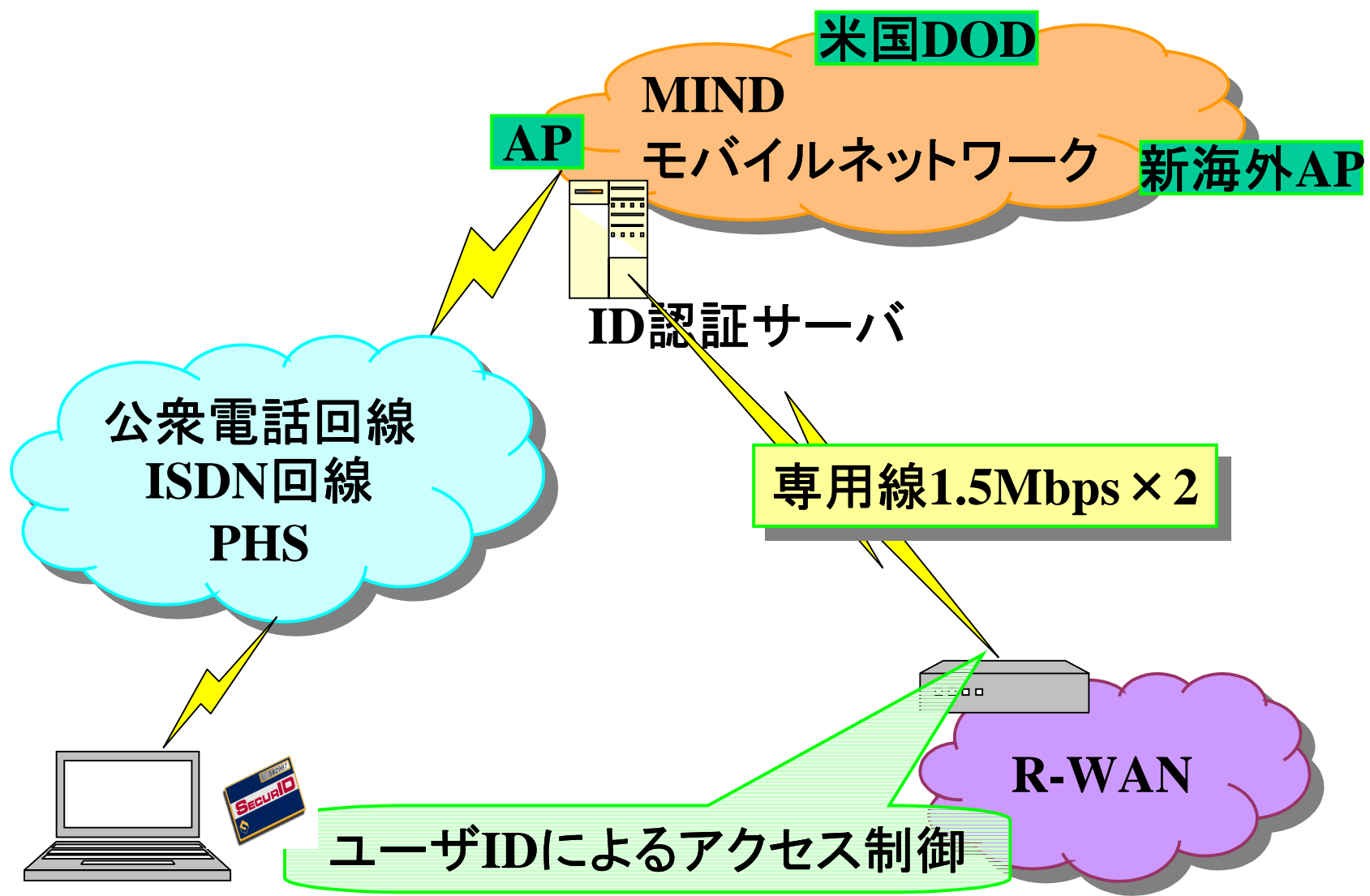
海外にも着信課金のアクセスポイントを設置

ユーザ認証方式として、ワンタイムパスワードを
標準サービスで提供

リコーが指定するプライベートアドレスが利用可能
同時アクセス人数の拡張性

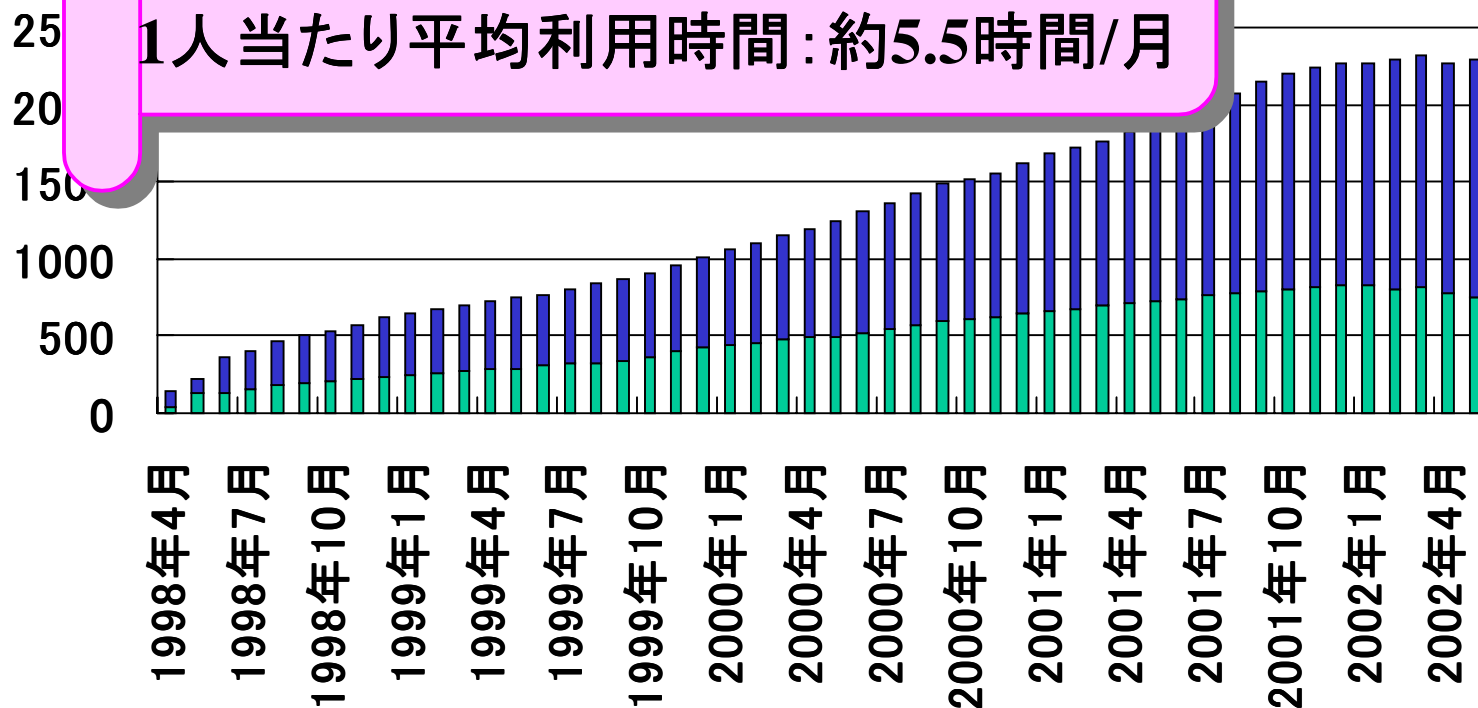
アナログ回線、ISDN、携帯電話、PHSの
各通信方式が利用可能

ネットワーク構成図 [~2002.6]



利用者数の推移

2002年12月現在
 ワンタイムパスワードユーザ: 1,985人
 固定パスワードユーザ: 679人
 関連会社61社: 1,586人
 1人当たり平均利用時間: 約5.5時間/月



ヘルプデスクの設置

利用者の増加に伴い、問い合わせ件数も増加

担当者3人だけでは対応しきれない!!

2001/1～ ヘルプデスクの設置
→リコーテクノシステムズ(株)にアウトソーシング

ユーザに均一したサービスを提供
担当者の負荷軽減

よくある問い合わせ

ワンタイムパスワードカードに
ロックがかかってしまったのですが？

固定パスワードの有効期限が切れてしまったのですが？

DLIC

12

問い合わせ数
約50件/月

MINDに接続できません。

固定パスワードからワンタイムパスワードに変更したい。

通信費用について

着信課金による距離に関係ない全国一律の通信料金

KDDIのMALサービスを利用することにより実現

日本

DDIポケット,一般公衆回線: 通話料約10円/分+接続料5円/分

その他の携帯端末: 通話料: 各通信会社による+ 接続料5円/分

InternetVPN: 通話料: ISPによる+ 500円/月-ID

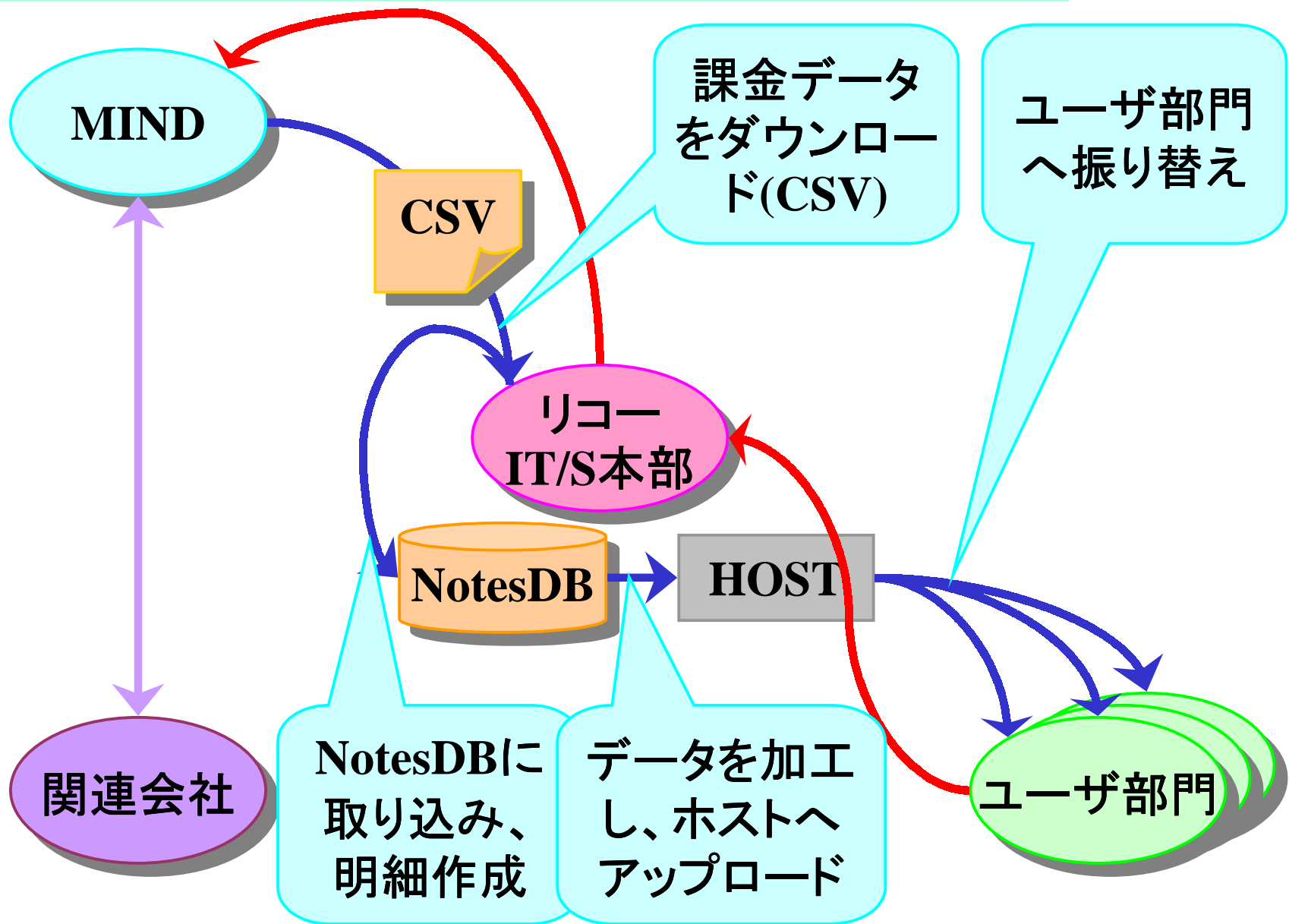
海外

MIND提供AP: 通話料60円/分

プロバイダ経由: 通話料: 各通信会社による+ 接続料60円/分

MINDよりリコーへの請求部分

利用部門への課金の流れ



利用明細提供画面

リモートLAN申請 - 8.通話明細(T)*b.利用者別(N) - Lotus Notes

ファイル(F) 編集(E) 表示(V) 作成(C) アクション(A) ヘルプ(H)

Workspace リモートLAN申請 - 8.通話明細(T)*b.利用者別(N) notes

利用月	所属	請求額
▶ 多田 武		¥96,223
▶ 多田 聡		
▶ 多和田 紀久		
▶ 太田 謙治		
▶ 太田 俊郎		
▶ 太田 純		
▶ 太田 善久		
▶ 太田 泰		
▶ 太田 直樹		¥67,392
▶ 太田 哲夫		¥153,013
▼ 太田 篤宏		¥74,986
2001/08	IT/S I推C I技G	¥1,930
2001/05	IT/S I推C I技G	¥14,459
2001/04	IT/S ITC I技G	¥1,636
2001/03	IT/S ITC I技G	¥2,606
2001/02	IT/S ITC I技G	¥1,547
2001/01	IT/S ITC I技G	¥1,920
2000/12	IT/S ITC I技G	¥3,359
2000/11	IT/S ITC I技G	¥2,365
2000/10	IT/S ITC I技G	¥1,500
2000/09	IT/S ITC I技G	¥5,413
2000/08	IT/S ITC I技G	¥7,110
2000/07	IT/S ITC I技G	¥8,827
2000/06	IT/S ITC I技G	¥1,967
2000/05	IT/S ITC I技G	¥5,477
2000/04	IT/S ITC I技G	¥1,754

明細は全社員が参照可能

オフィス

インターネットからの利用について

インターネット経由でリモートLANを使用したい!!

- ・インターネットへの常時接続サービスの普及
ダイヤルアップの通話料の削減要望
- ・高速なインターネット接続環境の普及
速度Upへの要望(64Kbps超)

安全にインターネットから利用するための技術を検討

インターネットに対応したセキュリティの強化

インターネットVPN技術

→ IPsecを利用した暗号化によりデータの不正解読を防止

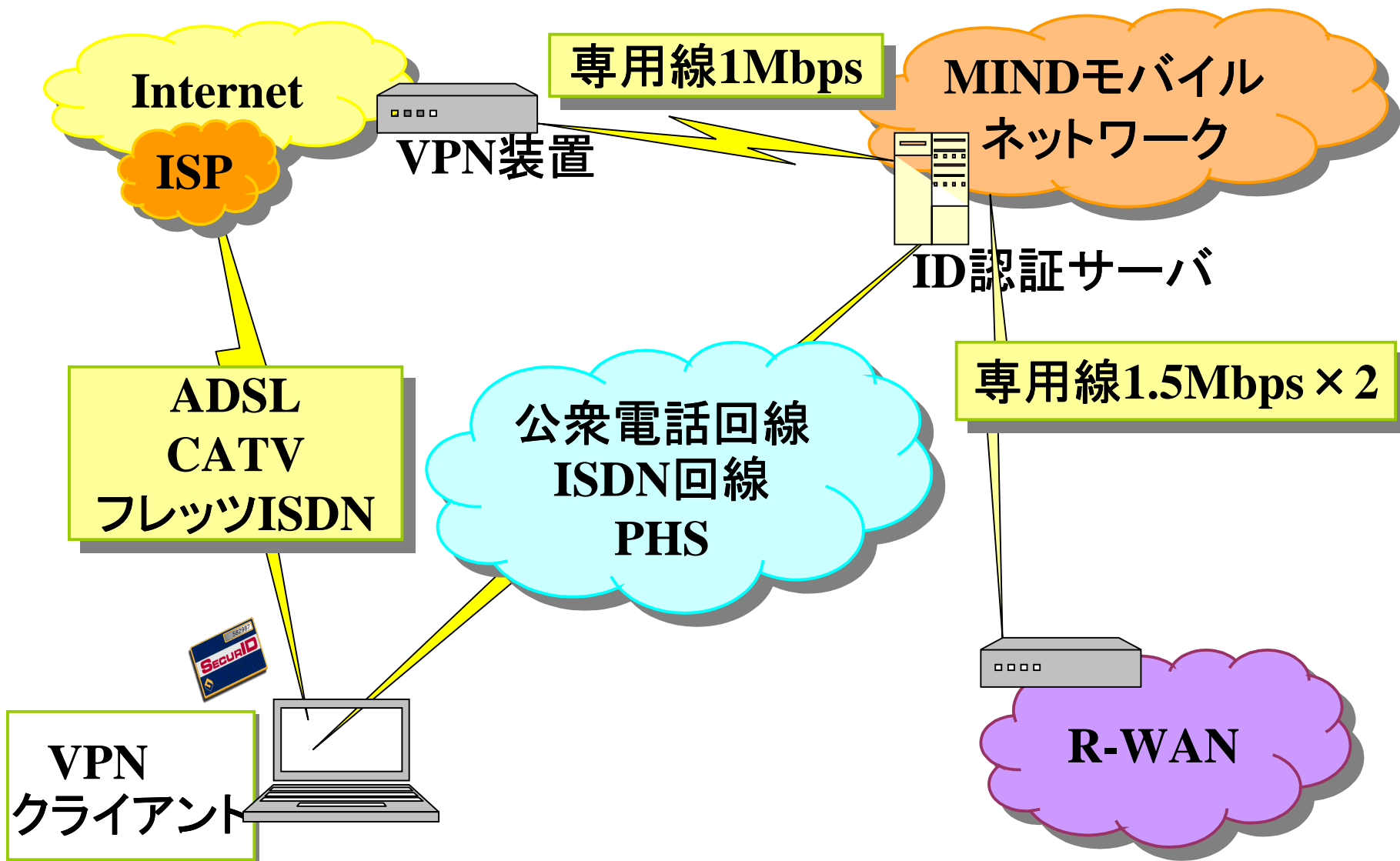
パーソナルファイアウォール

→ 悪質ウィルスの感染などから使用するPCを防御

ワンタイムパスワード

→ 使い捨てパスワードの利用で不正ユーザ(なりすまし)を防止

ネットワーク構成図 [2002.7~]

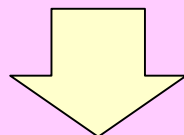


今後の展開(1)

インターネットからのリモートアクセスの活用

①ホットスポットの活用

無線LANカードを利用し、外出先からインターネットVPN経由で会社へリモートアクセス



社内でも外出先でも、社内の自席にいる時と同様に快適なアクセスで業務を行うことが可能!!

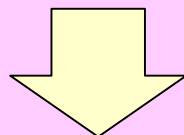
モバイルの利便性向上 → 更なる業務効率の向上

今後の展開(1)

インターネットからのリモートアクセスの活用

②SOHOへの活用

小規模オフィスにてADSLを利用し、インターネットVPN経由でWANにリモートアクセス



専用線でWANに接続した場合と変わらない環境を低コストで実現可能

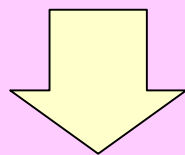
WAN構築の低コスト化→

より柔軟なWANの構築が可能

今後の展開(2)

専用アクセスサービスの充実化

128Kbps/パケットサービスの適用

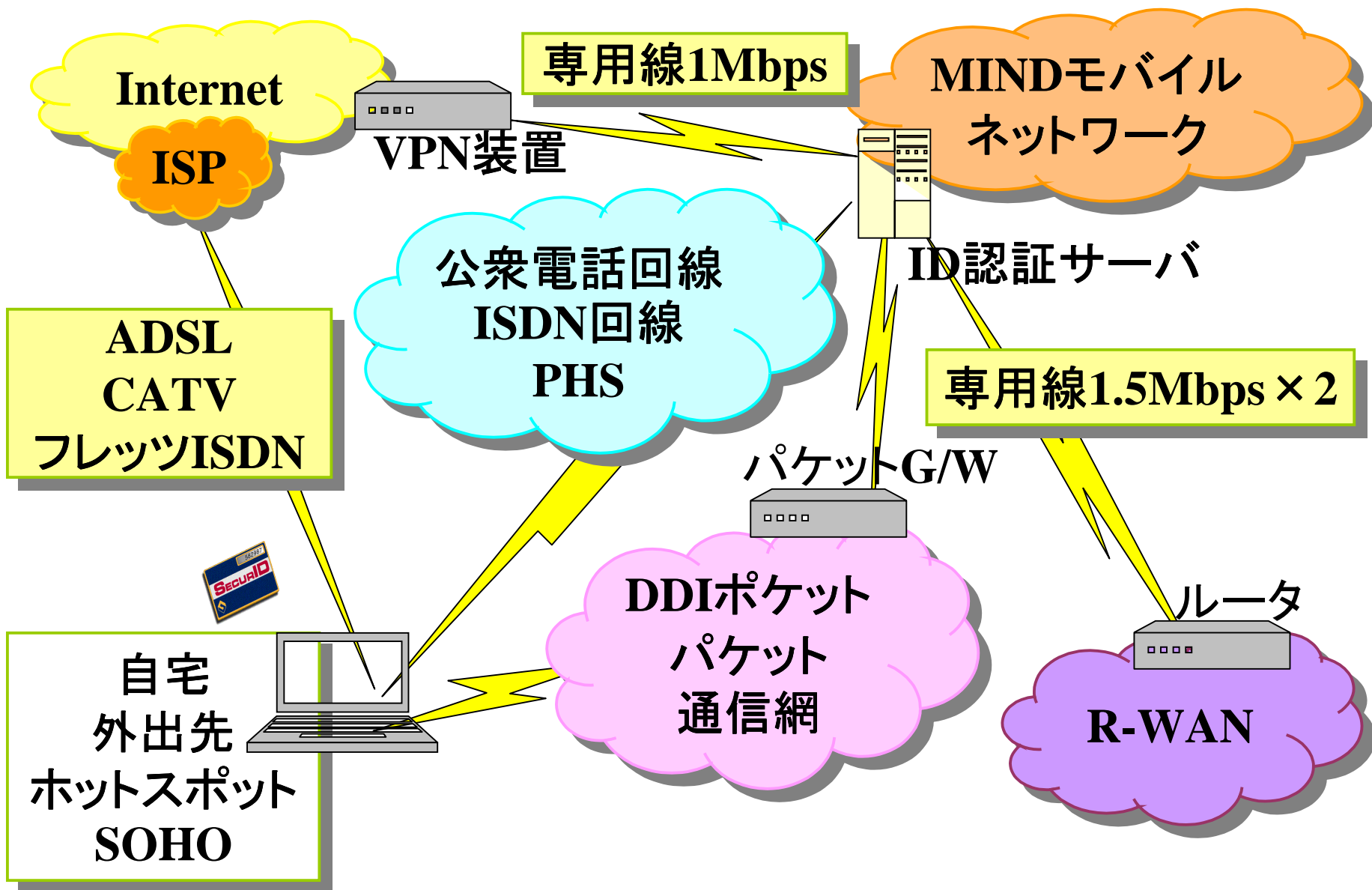


定額料金(6,800円/月)のため通信コスト削減が可能
従来のPHSでの接続より、切れにくく安定した品質

モバイルの低コスト化・品質の安定化

→ ユーザサービスレベルの向上

ネットワーク構成図[2003.3予定～]



無線LAN及びリモートLANアクセスを展開することにより「ユビキタス・ネットワーク」を目指します。

御清聴、誠にありがとうございました。