移動通信とセキュリティ

名城大学
渡邊晃

内容

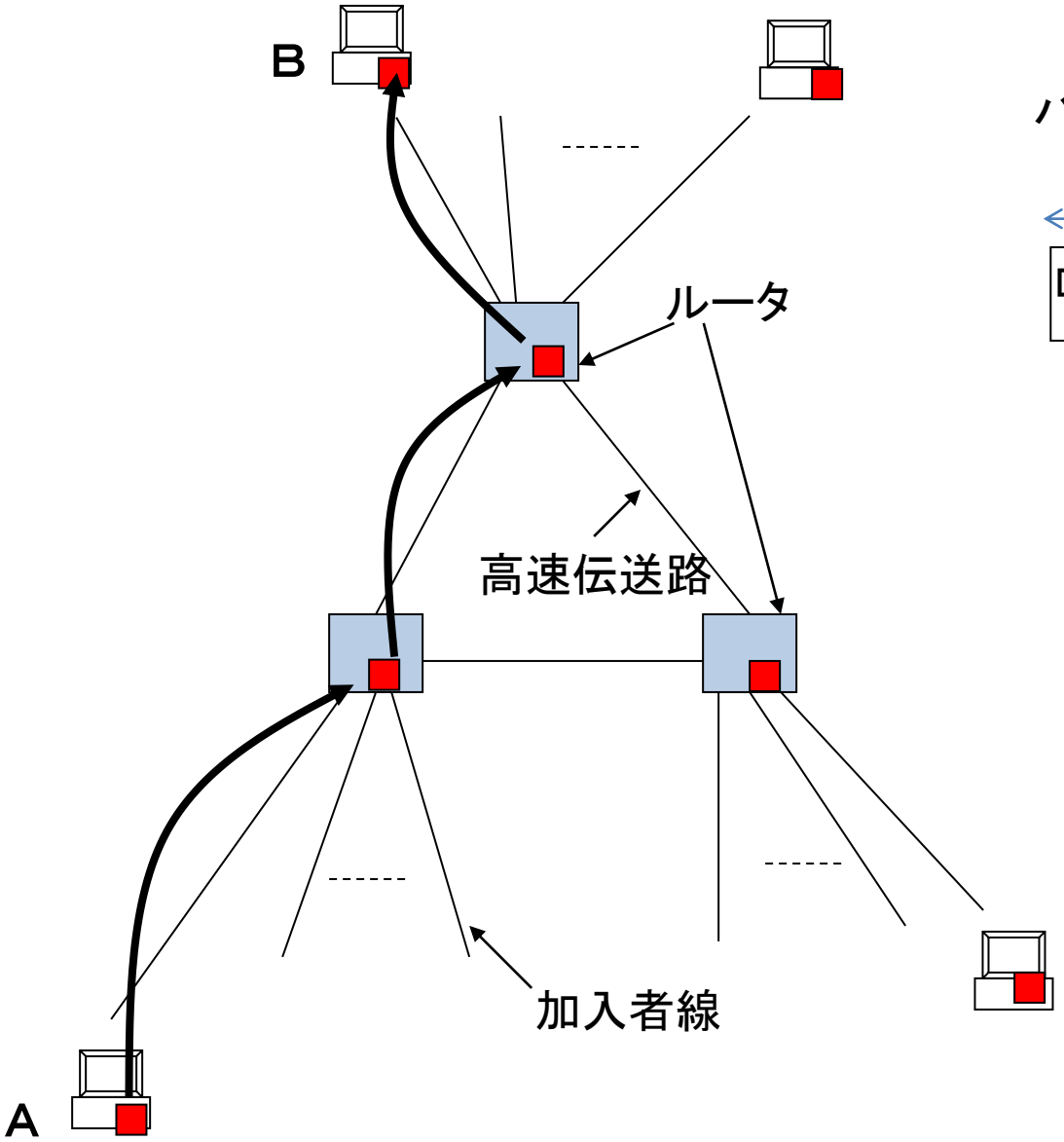
①パケット交換方式

②移動通信
- IPアドレスの枯渇　→　NAT越え問題
- 移動透過性

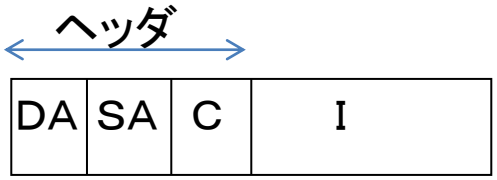
③セキュリティ
- ウイルス
- 暗号技術

データ通信網の構成　---　パケット交換方式（蓄積交換方式）

情報をパケットの形にして中継装置をバケツリレーして行く



パケットの構造



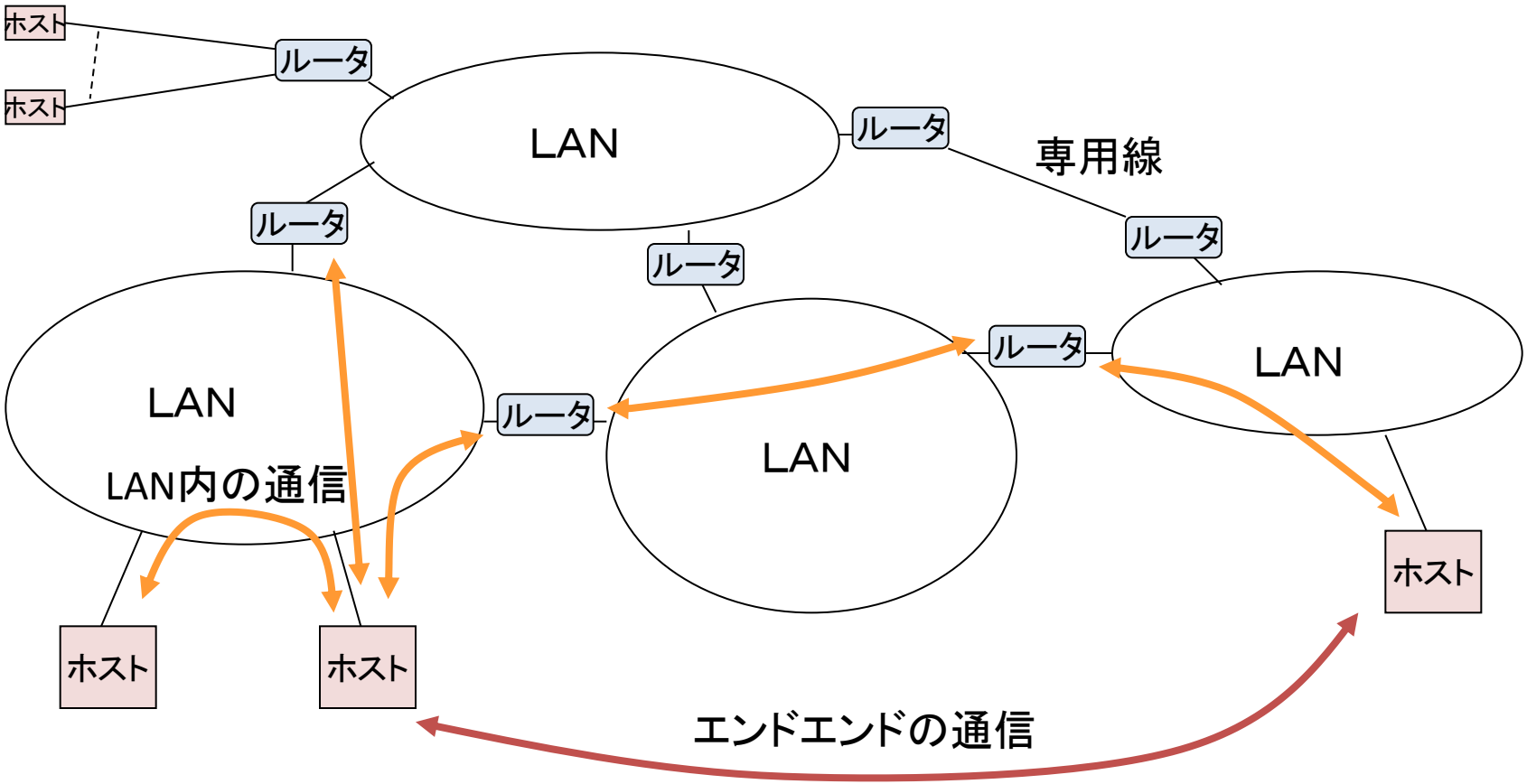
DA；宛先アドレス

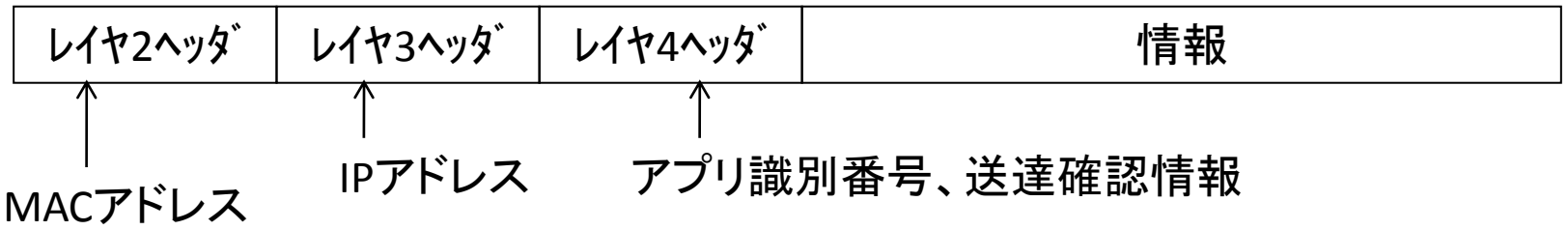
SA；送信元アドレス

C　；制御情報

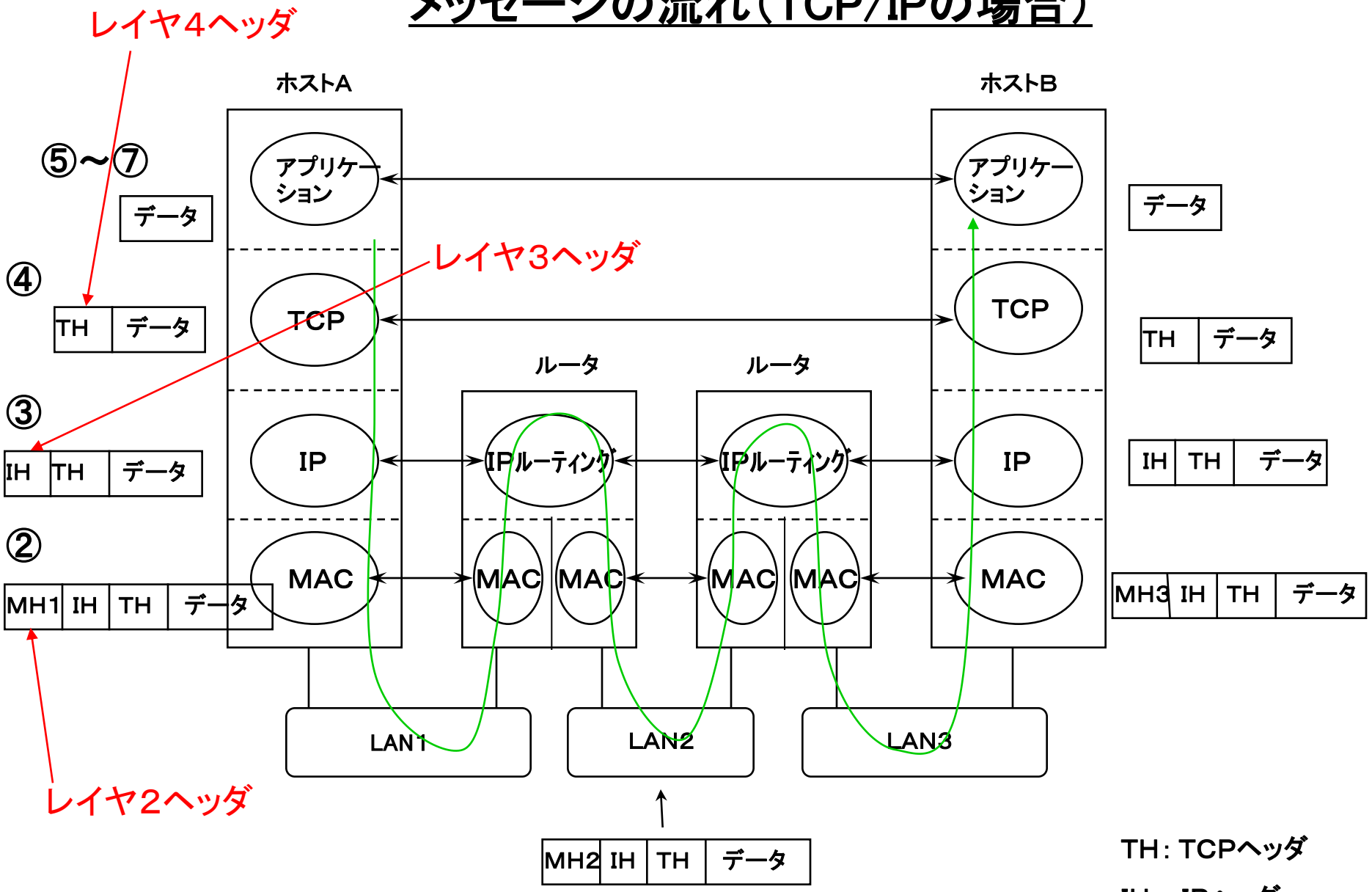
I　；ユーザデータ

パケットフォーマット


ホスト
ホスト
ルータ
LAN
ルータ
専用線
ルータ
ルータ
ルータ
ルータ
LAN
LAN内の通信
ルータ
LAN
ルータ
LAN
ホスト
ホスト
ホスト
エンドエンドの通信


レイヤ2ヘッダ
レイヤ3ヘッダ
レイヤ4ヘッダ
情報
MACアドレス
IPアドレス
アプリ識別番号、送達確認情報

メッセージの流れ（TCP/IPの場合）

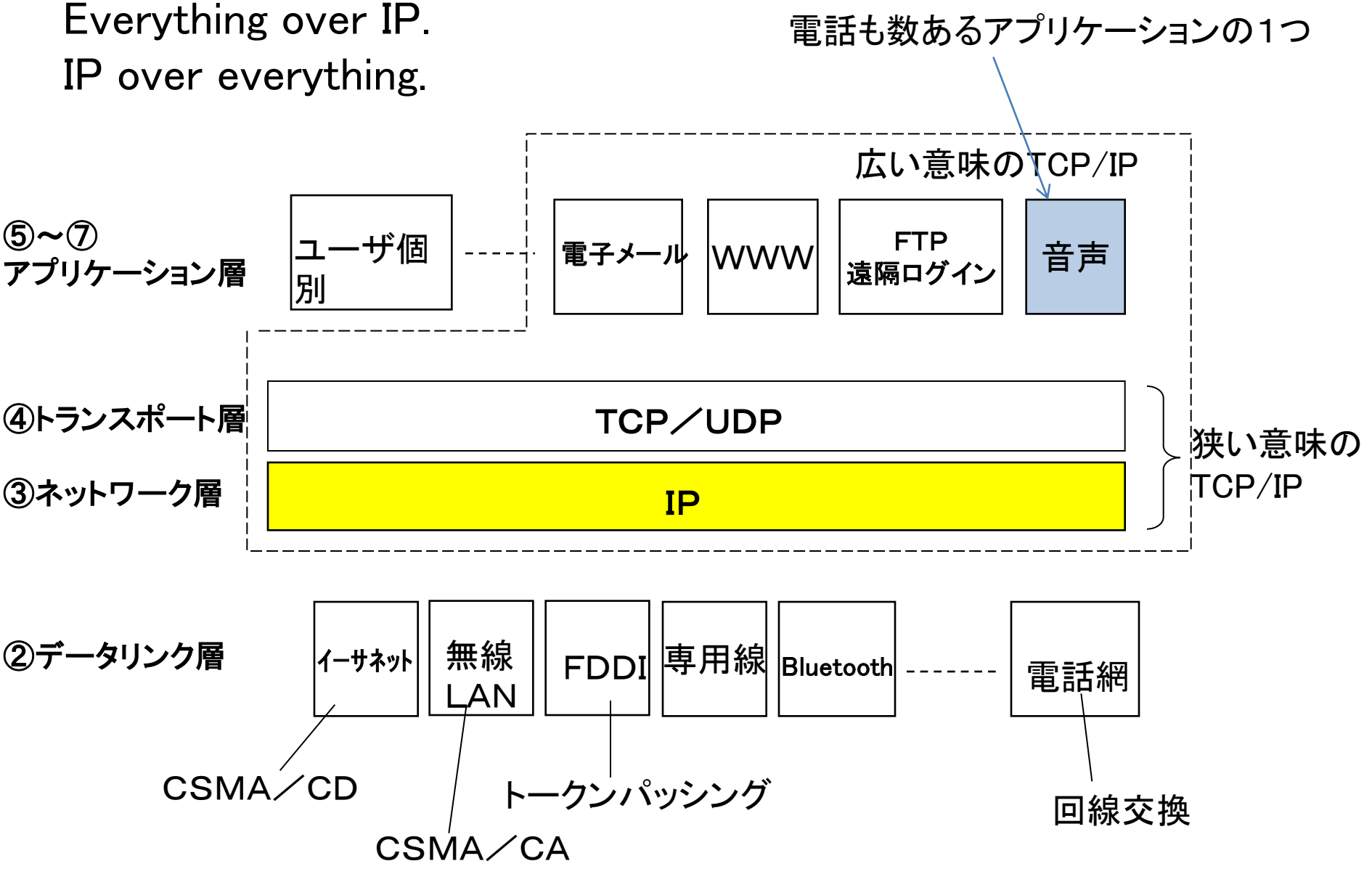


MAC（Media Access Control）；ネットワークのアクセス方式

インターネット（代表的なデータ通信網）

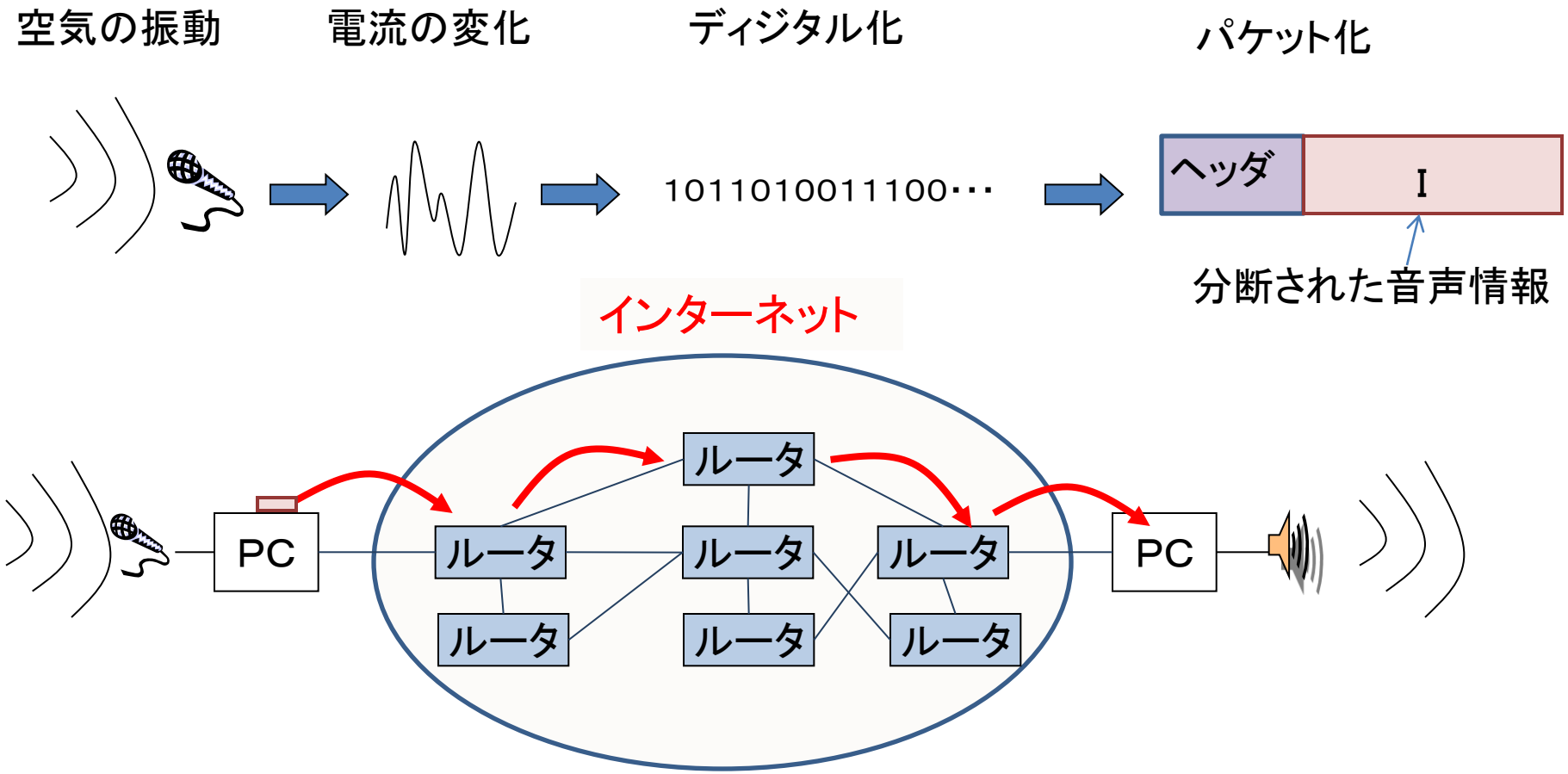
- 世界中に広がるデータ通信網
- 格段に安い通信価格
- パケット交換方式
- ベストエフォート型サービス
- 核戦争に耐えられる耐障害性
- 共通の通信プロトコルTCP/IP

Everything over IP.
IP over everything.



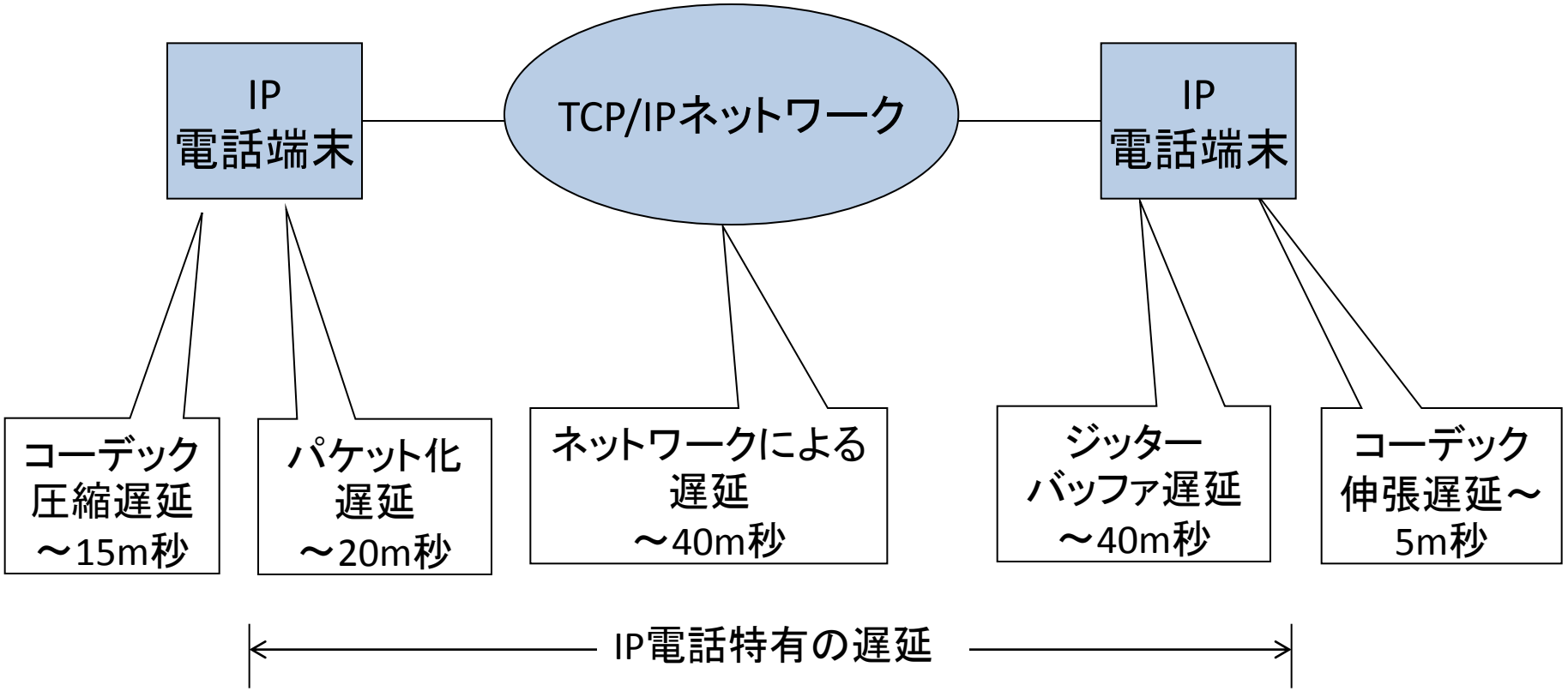
アプリケーションとデータリンクは独立して発展

IP電話のしくみ



音声情報は、20ミリ秒に1回、パケット化されて送信される
200mS以内の遅延であれば会話可能

遅延の要因（遅延の合計が200m秒以下が望ましい）



コーデック；符号化方式

ジッター；揺らぎ
（この場合はパケット受信間隔）

携帯電話の世代推移

・携帯電話も、3.9G以降はIP電話となる（All IP化の流れ）

世代	通信方式	速度	事業者	互換性
1G(アナログ) 1985～1998	Hicap (FDMA)		NTT IDO	
2G(デジタル) 1993～	PDC (TDMA)	28.8k 64k	NTTドコモ（mova） ソフトバンク ツーカー	日本独自 （欧米はGSM）
2.5G 1998～	cdmaOne (CDMA)	14.4k 2M	au	日、米
3G 2001～	W-CDMA (CDMA)	384k 2M	NTTドコモ（FOMA） ソフトバンク（3G）	日、米、欧
	CDMA2000 (CDMA)	144K 2.4M	au	日、米、欧
3.9G 2010～	LTE(*)	86.4M 325.1M	NTTドコモ	日本が標準化を 主導

↓

All IP化

(*)2010年12/24サービス開始（東京、大阪、名古屋）

TCP/IP最大の課題：IPアドレスの枯渇

・IPアドレスは32ビット・・・・約40億個

・IPアドレスの構造は階層・・・・アドレス空間の無駄が多い

⇩

アドレスが足りない

短期解決策；

1．アドレス取得が可能な範囲を細切れにして、アドレス空間を有効利用

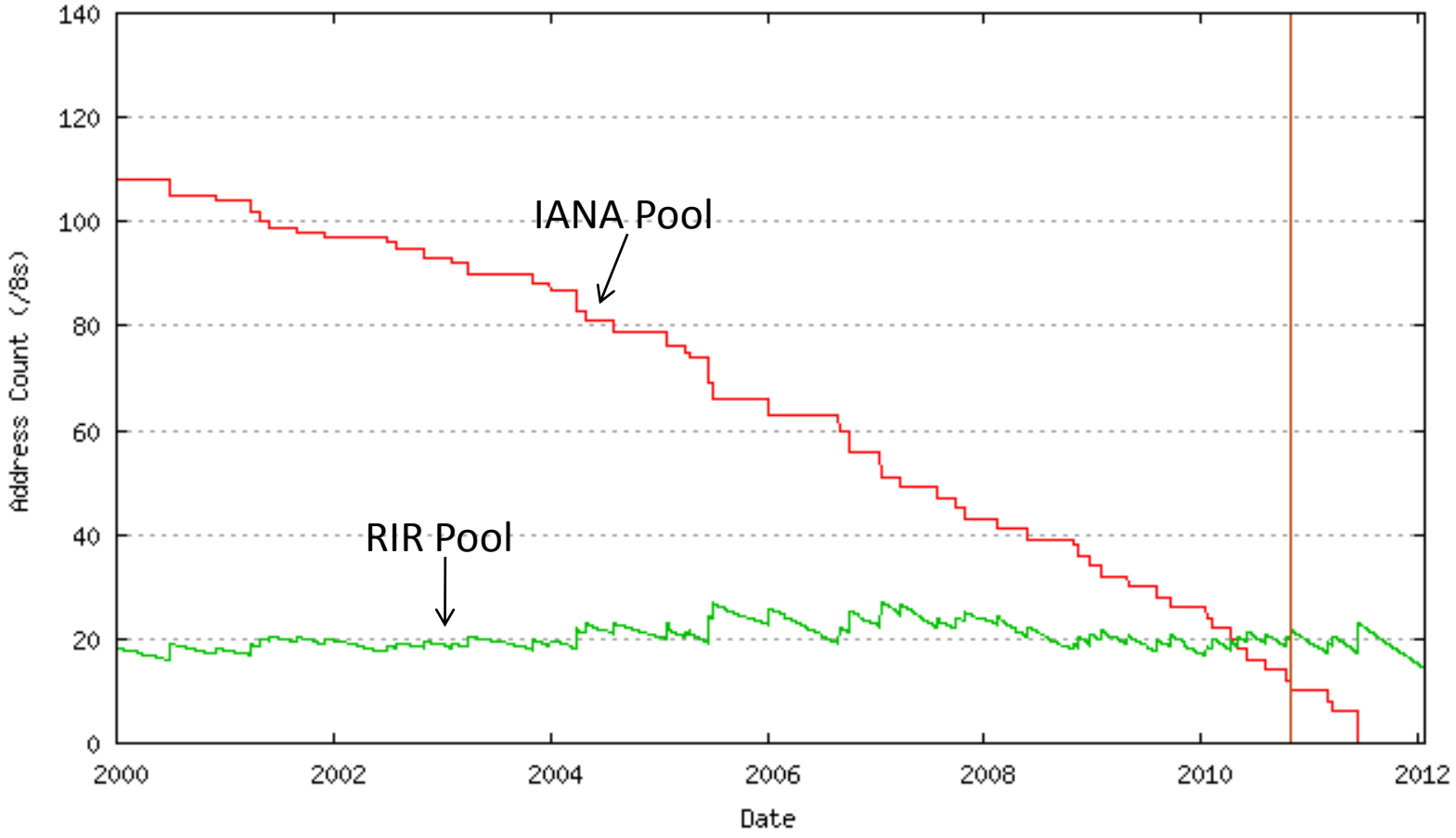
2．組織内で自由に使えるアドレスを定義－－＞プライベートアドレス

長期解決策；

IPv6　→アドレス長128ビット

IPv4グローバルアドレスのプール状況

出展:
http://ipv4.potaroo.net/
(2010/7).



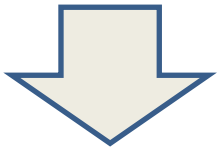
末端のISPへの影響が出るのは2014年ごろ
アドレス枯渇後の新規ユーザはIPv6アドレスしか取得できなくなる

IPv6

・128ビットのアドレス空間を持つ新しいプロトコル
・IPv4とIPv6の互換性はない

IPv6は普及するか

・IPv4が広く普及済み
・IPv6でなければいけないアプリケーションが今のところ存在しない
・2011年にIANAの持つIPv4グローバルアドレスが枯渇する



・IPv6はやむを得ず徐々に導入されていく。
・旧来のユーザはIPv4のまま残る（積極的に移行する理由がない）
　－IPv4で蓄積したノーハウがある
　－IPv4にもよい点がある（アドレスの隠蔽）
・IPv4/v6混在環境が今後長く続く

プライベートアドレス

IPv4の延命に寄与

私的なネットワーク内でのみ利用できるアドレス空間

・アドレス取得機関への申請は不要

・外部との通信に使用してはいけない

・外部との通信はNAT(Network Address Translator)を介して実現

プライベートアドレス用として予約されているアドレス空間

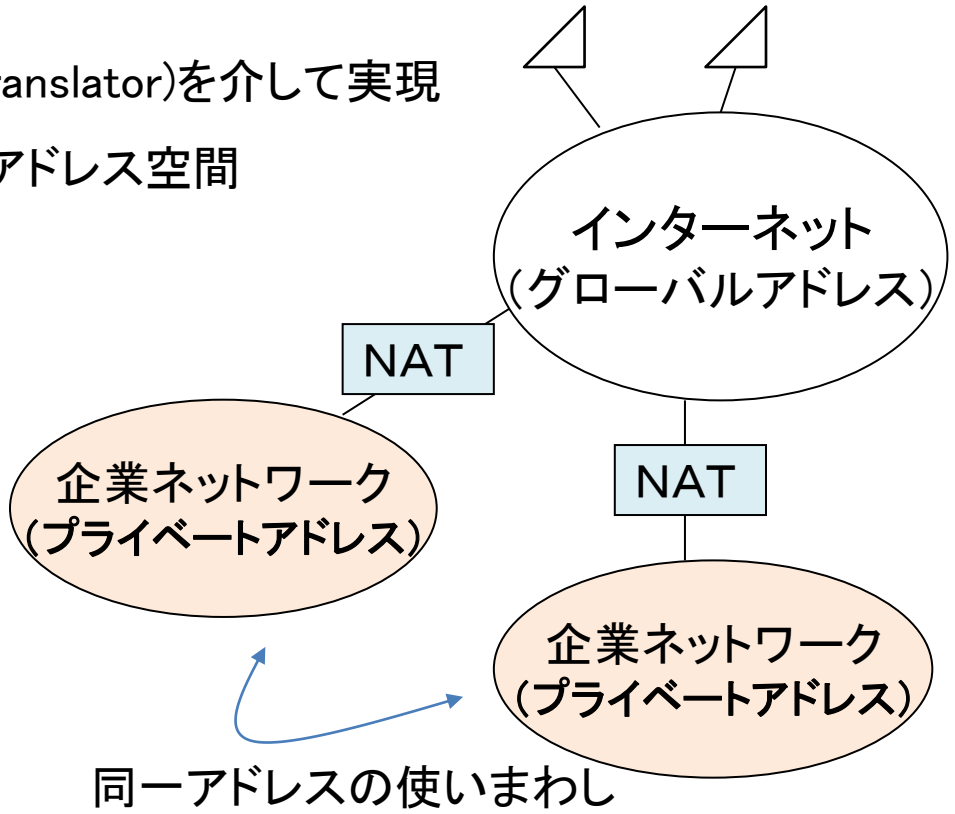
10.　0.　0.　0 ～　10.255.255.255

172. 16.　0.　 0 ～ 172. 31.255.255

192.168.　0.　 0 ～ 192.168.255.255

⇩

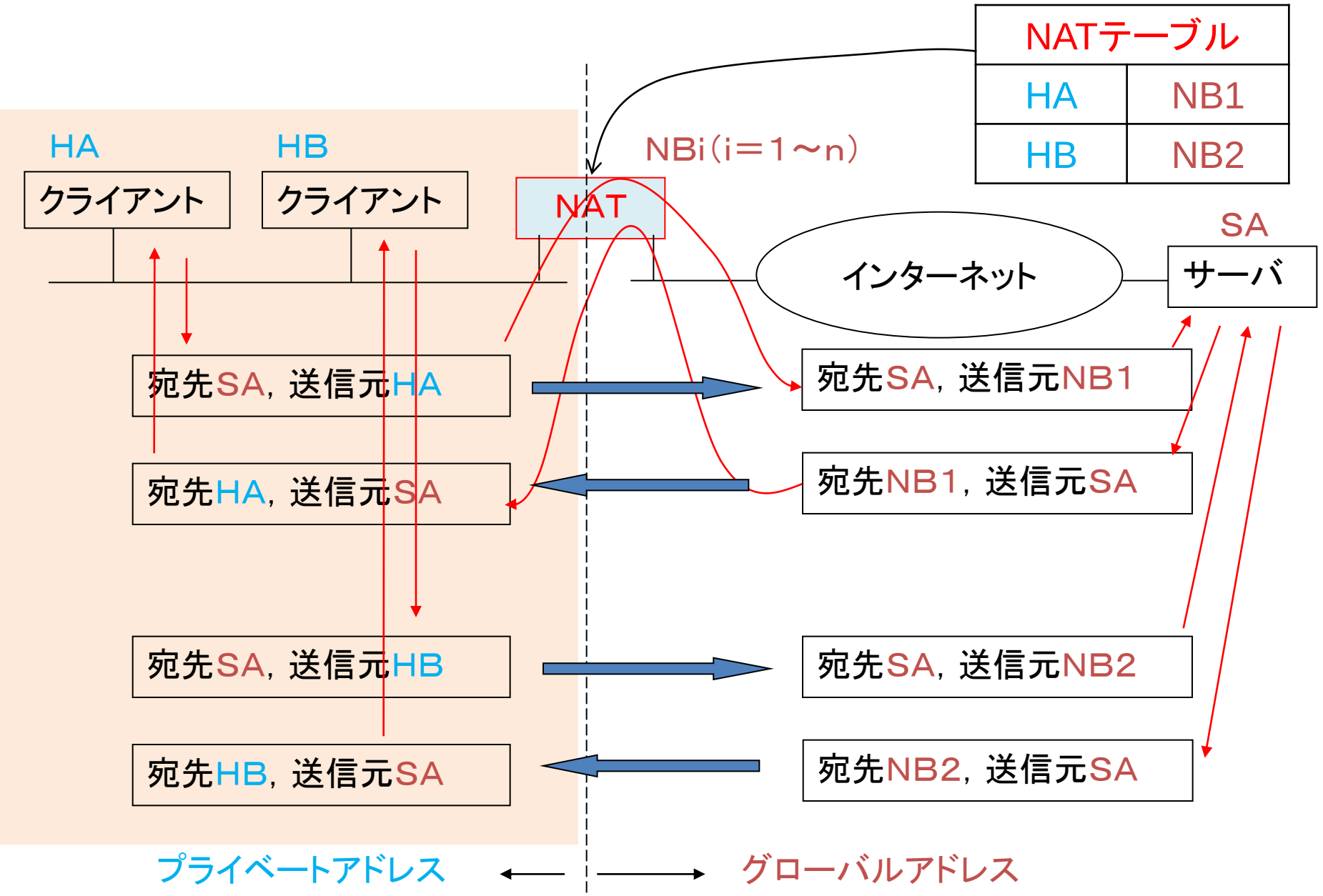
組織は少数のグローバルアドレスを
確保すればよい



同一アドレスの使いまわし

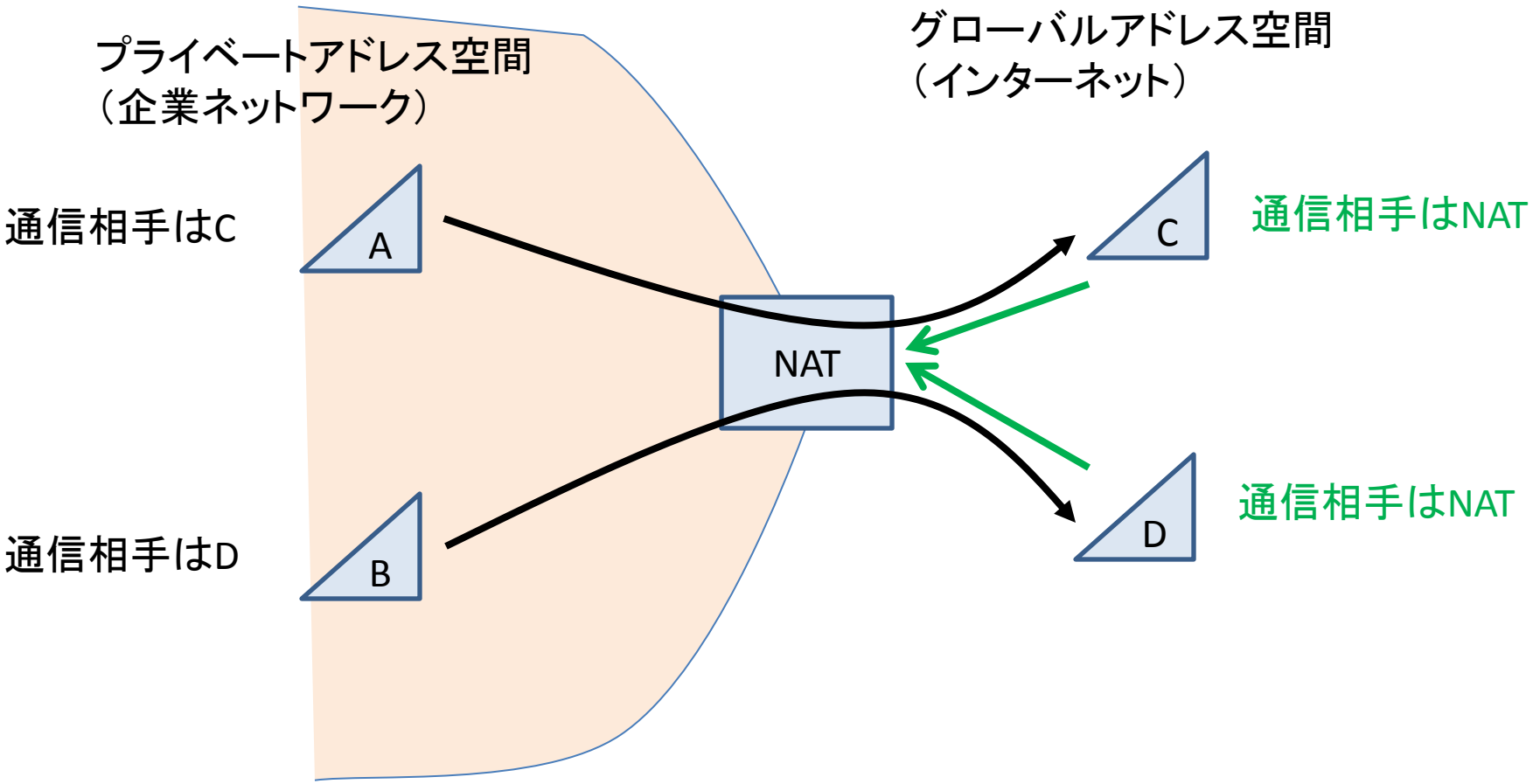
NATのしくみ

クライアントからサーバへの最初のアクセス時にプライベートアドレスとグローバルアドレスを変換するNATテーブルを作成する



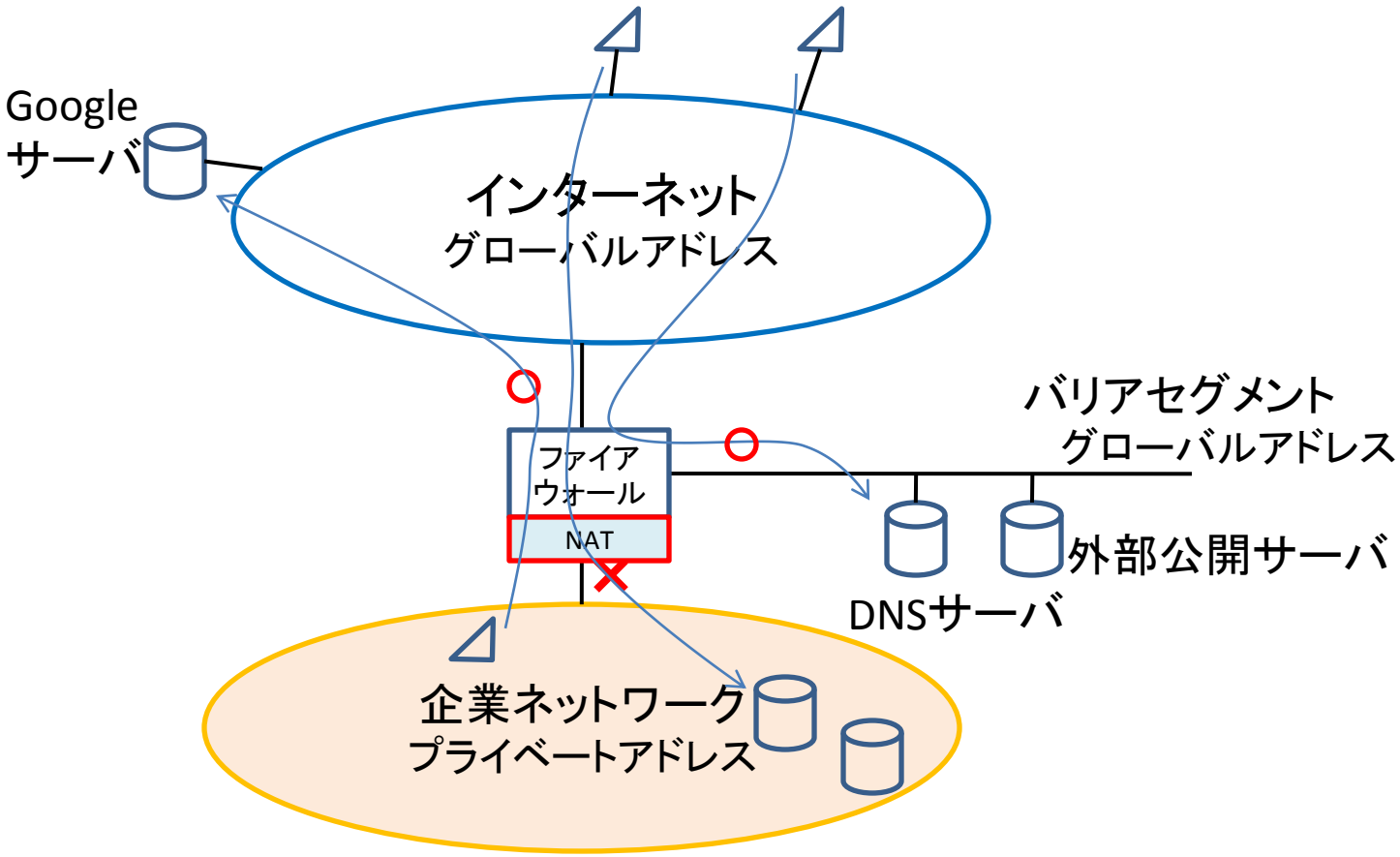
NAT越え問題

インターネット側（グローバルアドレス側）からの通信開始ができない



NATの利点：組織のネットワーク構造が外部から隠蔽される

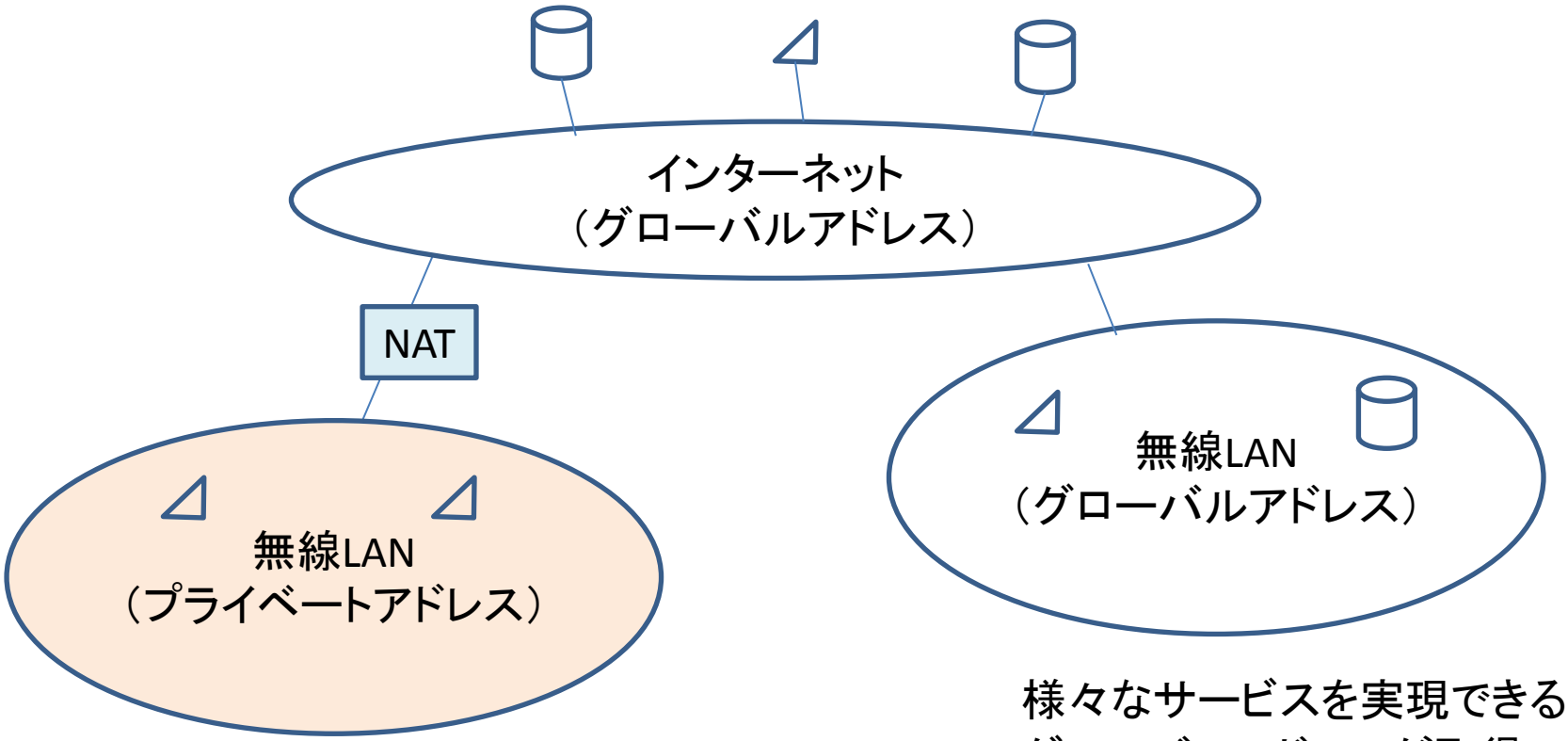
一般的な企業ネットワークの構成



NATはファイアウォールの影に隠れていた

NAT; Network Address Translation

無線LANサービスを行う場合の考慮



グローバルアドレスの取得不要
NAT越え問題による通信の制約
サーバを設置したサービスが難しい

様々なサービスを実現できる
グローバルアドレスが取得できなくなる可能性

サーバ

クライアント

移動透過性

IPアドレスはノードを識別する情報であるとともに、ノードの位置を示す情報である。

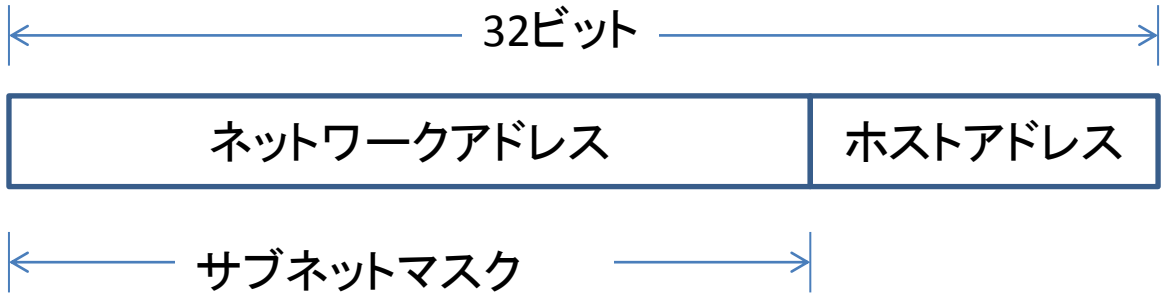
・ネットワークアドレス部によりノードの位置が決まる

・IPアドレスは通信識別子として使われている

⇒移動してIPアドレスが変わると、通信を継続できない

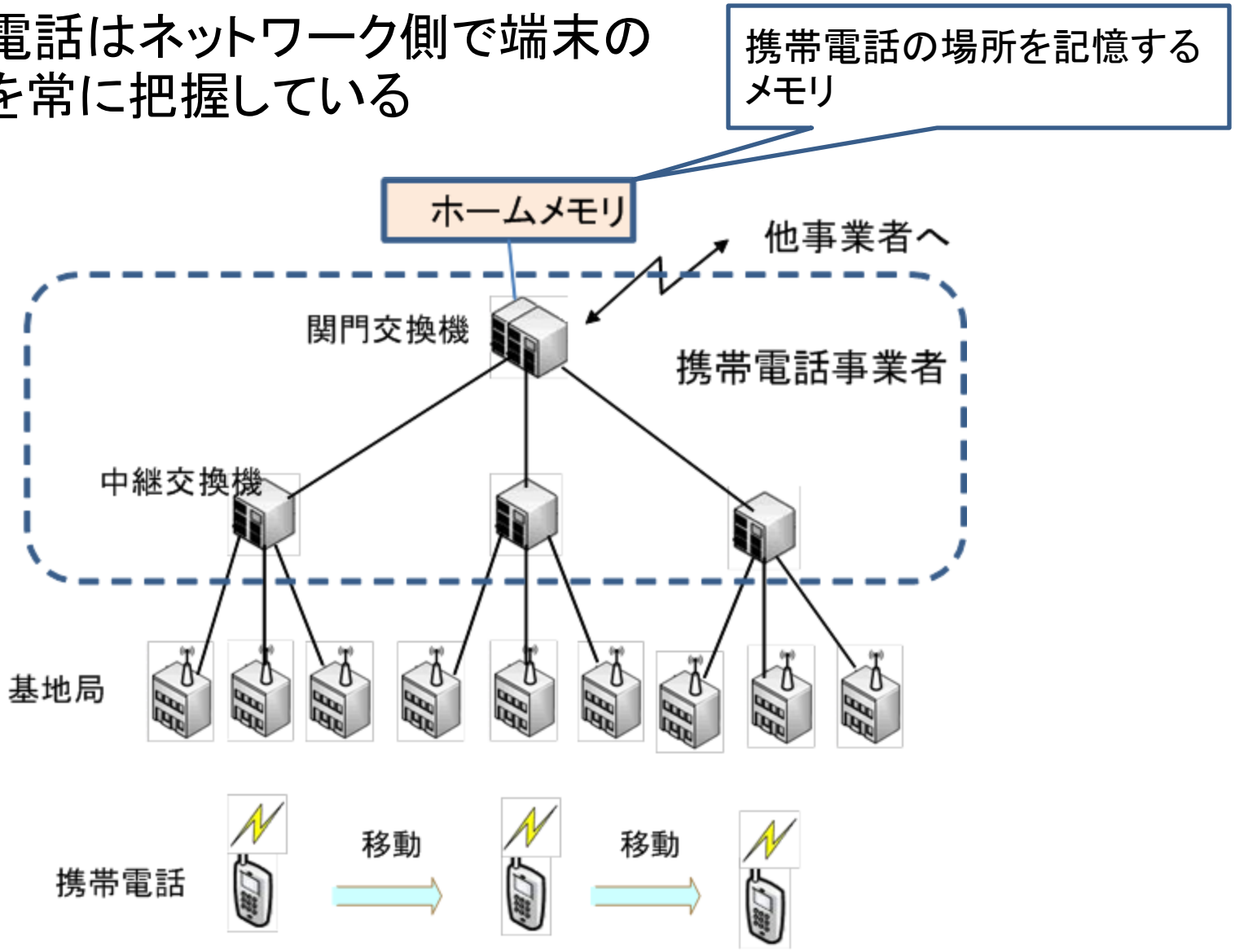
インターネット上の通信において、端末がどのように移動しても通信が可能であることを移動透過性があると言う。

IPアドレスの形式



ルータはネットワークアドレスを判別してパケットの経路を決定する

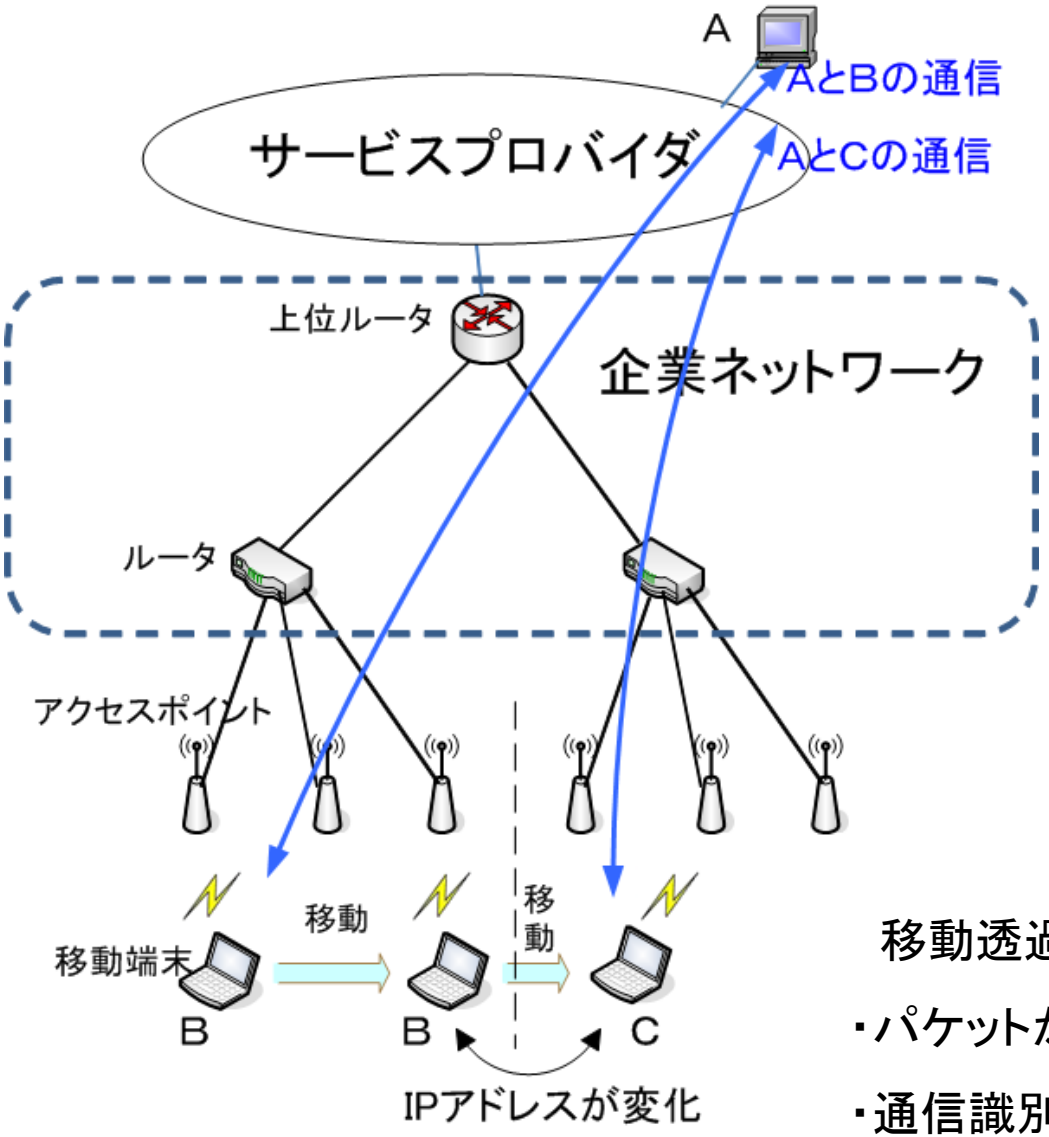
携帯電話はネットワーク側で端末の位置を常に把握している



電話番号とIPアドレスをリンクさせるため、
移動してもIPアドレスが変わらない

・ネットワークの頑張り
・事業者ごとに異なる方式

インターネットでは、ネットワーク側では何もしてくれない（エンドエンドの原則）



IPアドレスは通信の識別子

↓

アドレスが異なると違う通信とみなされる

移動透過性を実現するには

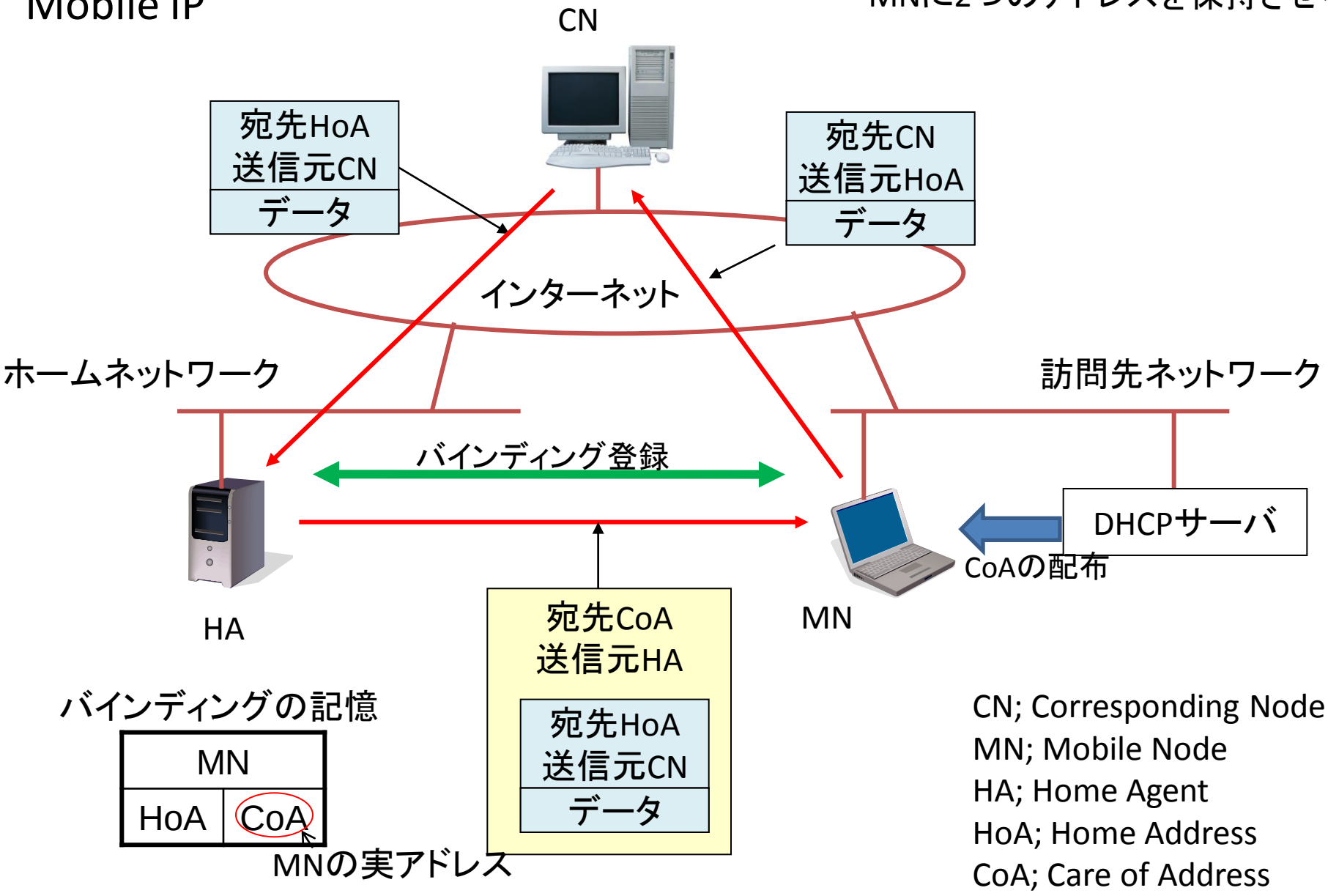
・パケットがうまくルーティングできる

・通信識別子が変わらない

IPv4における移動透過性プロトコル

Mobile IP

・第3の装置HAを導入
・MNに2つのアドレスを保持させる



バインディングの記憶

MN	
HoA	CoA

MNの実アドレス

CN; Corresponding Node
MN; Mobile Node
HA; Home Agent
HoA; Home Address
CoA; Care of Address

Mobile IPの課題

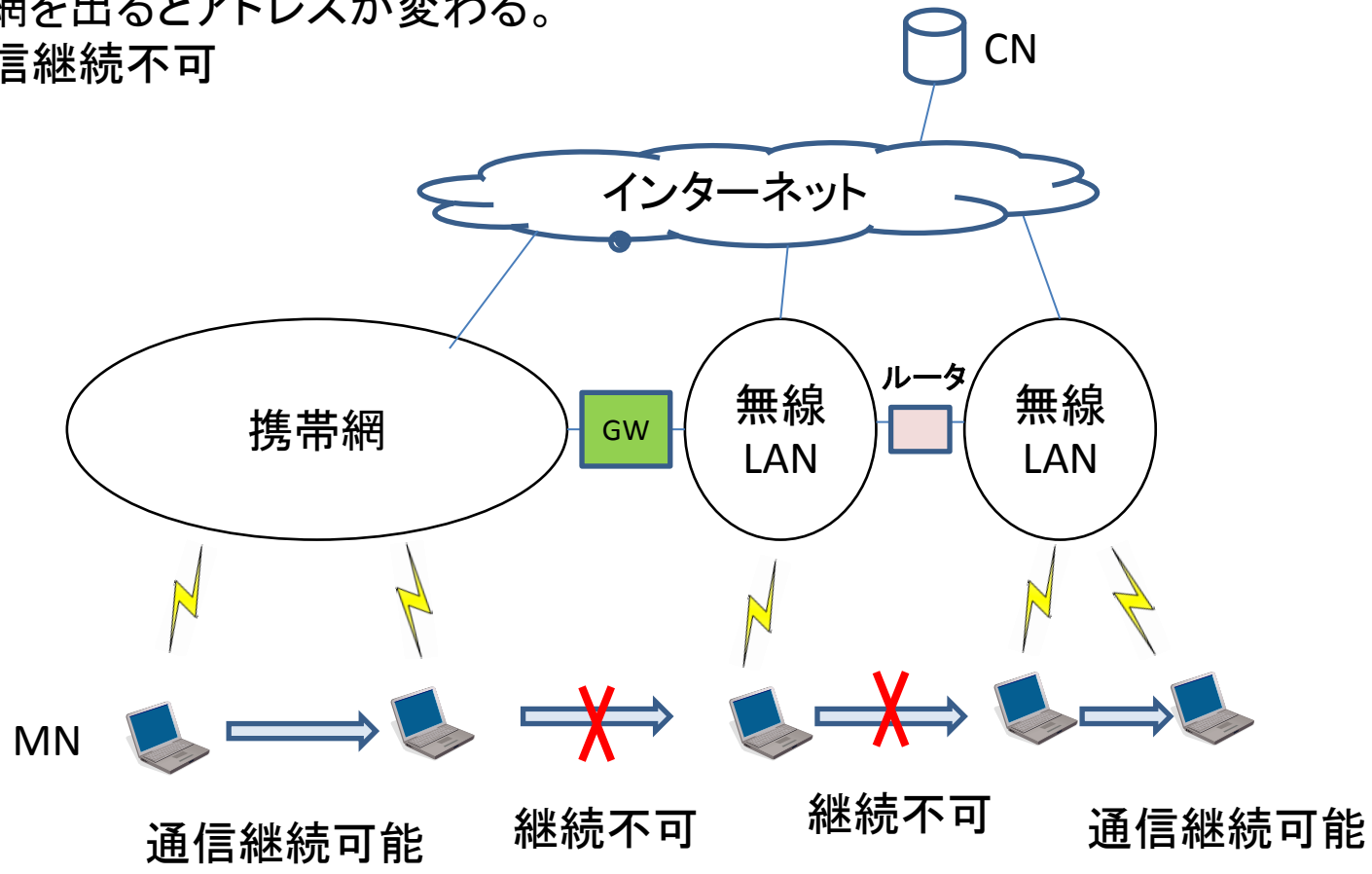
- 特殊な装置(HA)が必要となる
  導入の敷居が高い
  HAの障害に弱い
- 通信経路が三角経路となる
  通信経路が冗長
- HAとMN間はトンネル転送（カプセル化）となる
  カプセル化によるオーバーヘッド
- パケットの送信元アドレスが正しい位置を示していない
  途中のルータで廃棄される可能性あり

IPv4の環境で適切な標準移動透過プロトコルは
現状存在しない

移動通信の現状

・携帯網内では通信しながら移動が可能

・携帯網を出るとアドレスが変わる。
→通信継続不可



有力なモバイル端末

携帯電話
　携帯網を利用
　屋外で高速移動中でも安定した通話・通信が可能
　電話機能が中心。小トラフィックのインターネット利用

ノートPC
　無線LANを利用
　オフィスのPC環境をそのまま社外に持ち出して利用できる
　大トラフィックへの対応可
　通信中にルータを跨る移動ができない

スマートフォン
　携帯電話とノートPCのよい点を融合（携帯網＋無線LAN）
　ネットワーク中心の多種多様な機能（クラウドとの連携）

スマートフォンの定義
　仕様が公開された汎用的なOSを搭載し、利用者が自由にアプリケーションを追加して機能拡張やカスタマイズができる携帯端末
　　iPhone
　　Android

セキュリティ

セキュリティの定義、分類

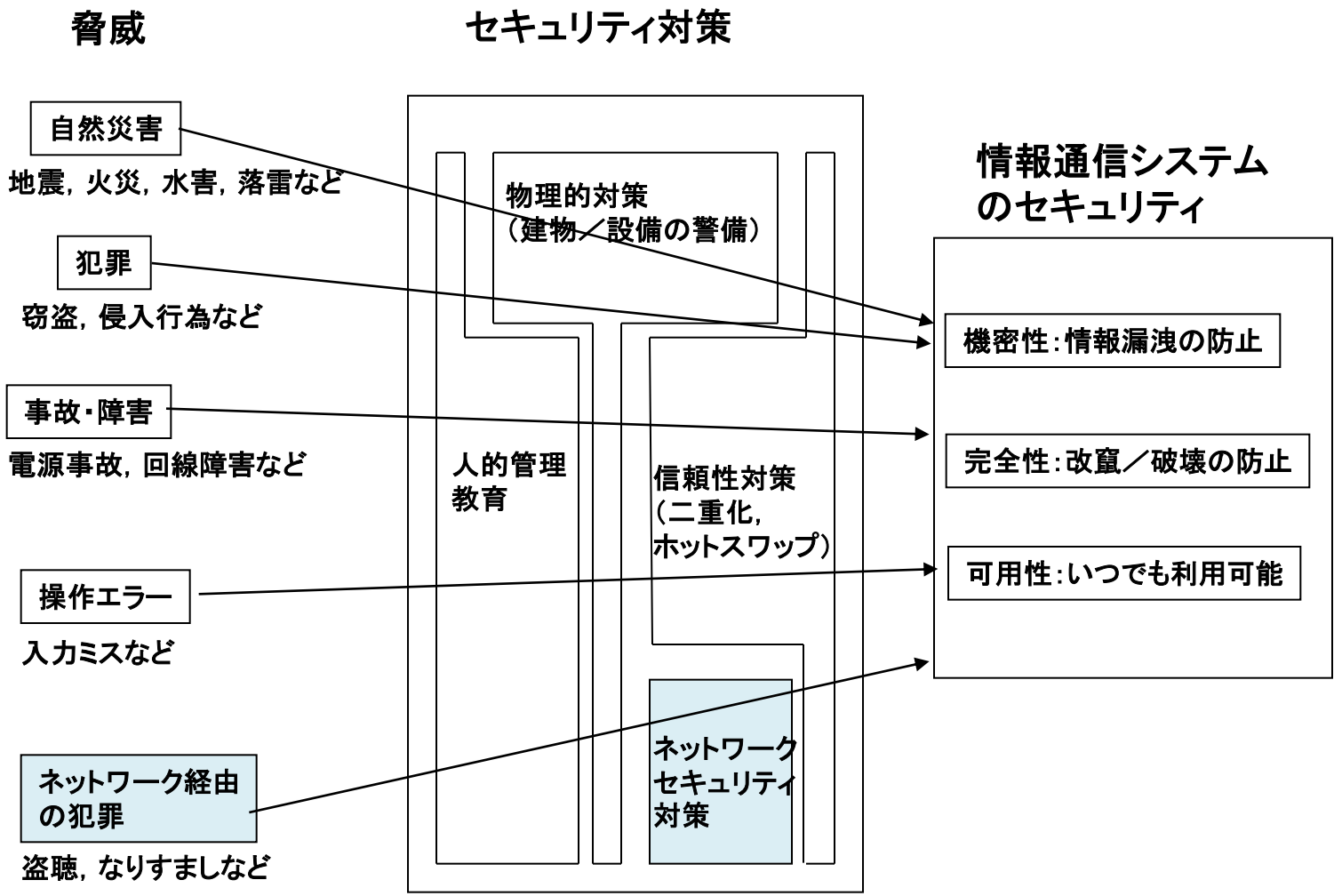
ネットワークセキュリティ対策
- ウイスル、ボット
- 暗号技術（公開鍵と共通鍵）

無線LANのセキュリティ

モバイル端末のセキュリティ

ネットワークセキュリティの位置づけ

ネットワークの普及により発生した新たな脅威



ホットスワップ；コンピュータの電源を入れたまま、パーツやケーブルを交換すること。

ネットワークセキュリティ対策

・ファイアウォール

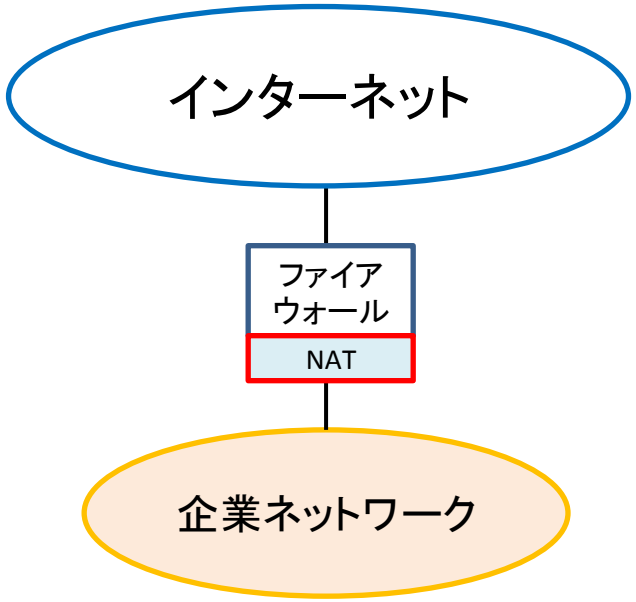
組織内のネットワークを外部の脅威から守るしくみ

・ウィルス対策ソフト

コンピュータウィルスの感染を検出、除去するソフトウェア

・暗号技術

情報の隠蔽、認証のために必須の技術



認証；正当性を検証する作業（相手認証，パケットの正当性確認など）

ウイルスの感染タイプ

①ファイル感染型ウイルス
　古典的なウイルス（狭義のウイルスに相当）

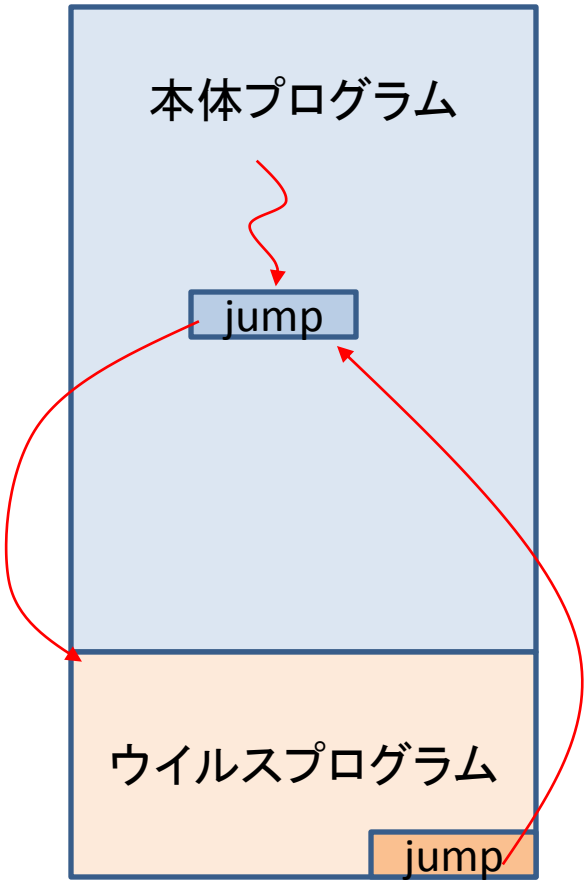
②インタプリタ型ウイルス
　インタプリタ型言語(注1)またはスクリプト言語(注2)で記述されたウイルス
　最近のほとんどのウイルスはこのタイプ
　ウイルス自体が独立したプログラムとなっている（ワームに相当）
　　・マクロウイルス
　　・スクリプトウイルス

(注1)インタプリタ型言語；逐次命令を解釈しながら実行させるタイプの言語。
　機能に制限があるがコンパイルが不要
　ソースコードを記述してすぐに実行できる

(注2)スクリプト言語；比較的単純なプログラムを記述するための簡易的なプログラミング言語全般
　インタプリタ型であることが多い（スクリプト言語≒インタプリタ言語）
　Java Script，VBA(注3)，MS-DOSのコマンドで記述した命令列

(注3)VBA (Visual Basic for Application)；MSオフィス用のスクリプト言語
　VBAを用いたオフィスの機能をマクロ機能と呼ぶ

ファイル感染型ウイルス



原理

・パッチと同じ手法

プログラムのバグを除去する修正プログラム

・本体プログラムを実行するとウイルスプログラムが呼び出される

・発病条件を満たさなければ本体プログラムに戻る

感染方法

・ウイルスプログラムによる感染処理

・人間が外部メモリを介してファイルコピー（初期のウイルス）

・ネットワーク経由のDLL

インタプリタ型ウイルス

マクロウイルス

MS オフィス（ワード、エクセルなど）のマクロ機能を利用したウイルス
メールの添付ファイルを実行することにより感染する。

マクロ機能；
VBA により、ワード/エクセルを使用した定型業務を自動化できる機能
キーボードやマウスの操作を記録し、プログラムとして利用できる機能もある

マクロ機能を利用して文書を作成すると、記述内容がオフィス文書の一部として格納される
このファイルを閲覧するとVBAの書式ファイルが最初に実行される
⇑これがマクロウイルスの元凶
オフィスを利用するすべてのOS（Mac、LINUXなど）に感染する

オフィスファイルは単なる文書ファイルではない。
マクロ機能を有効にしたオフィスファイルを開くと、実行ファイルが実行される。

スクリプトウイルス

スクリプト言語を利用したウイルス。

感染方法：
メーラやブラウザのバグをつく方法
　対策のとられていないメーラでHTMLメールを閲覧すると感染
　対策のとられていないブラウザでWEBサーバをアクセスすると感染
メールの添付ファイルを実行させる
　ソーシャルエンジニアリング的手法（注１）

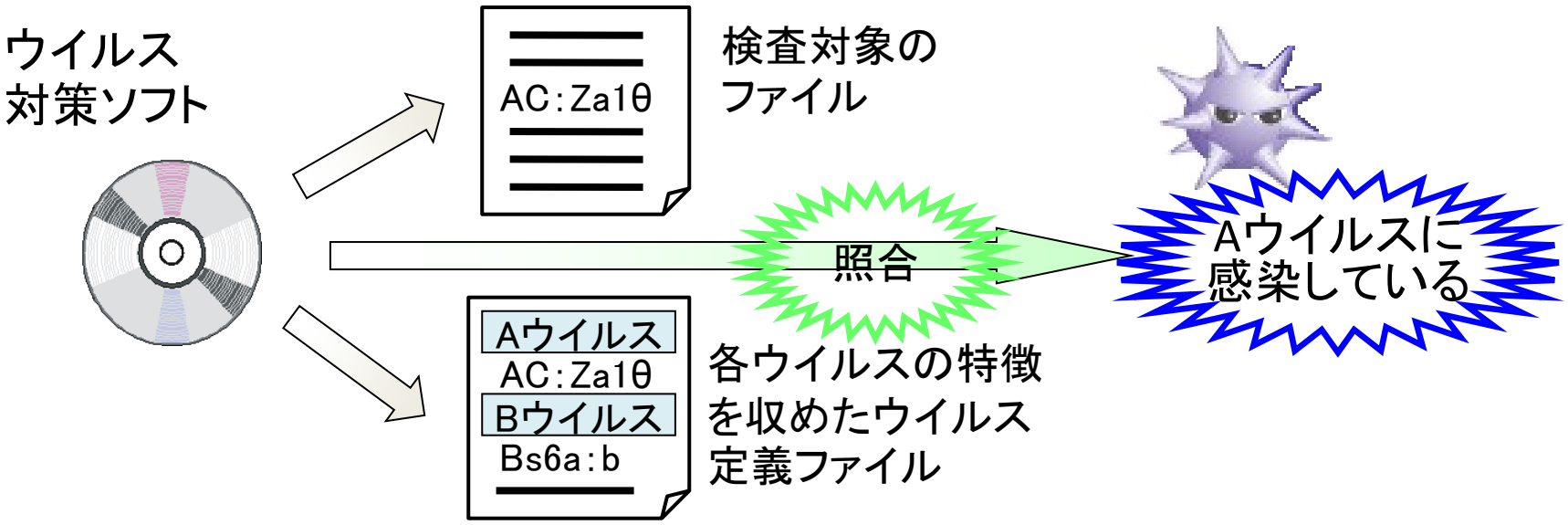
　添付ファイルの名前の例
　　〇〇〇.vbs
　　□□□.txt　　.vbs　　←一見テキストファイルに見える
　　メールに添付すると.vbsが表示されない

（注１）ソーシャルエンジニアリング：人間の心理的な隙や行動のミスにつけこむ手法
　　・肩越しにパスワードを盗み見る（ショルダーサーフィン）
　　・管理者を装ってパスワードを聞きだす
（注２）vbs：Visual Basicで書かれたスクリプトファイルの拡張子

ウイルス対策ソフト

（またはアンチウイルスソフト、ワクチンソフト）

ウイルスの特徴（ビット列）を収めた「ウイルス定義ファイル」と対象ファイルを照合し、特徴が対象ファイルに含まれていれば、ウイルスに感染していると判断する

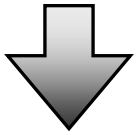


ウイルスバスター（トレンドマイクロ）
ノートンアンチウイルス（シマンテック）
インターネットセキュリティ（マカフィー）

ウイルスの進化

- ボット（bot）
  - 2004年頃から活発化している（広義の）ウィルス
  - 対策無しでネットに繋ぐと約4分でボット化
  - 国内で40万台～50万台がボット化

- ボットネット（botnet）
  - ボットに感染したPCにより構築されたネットワーク



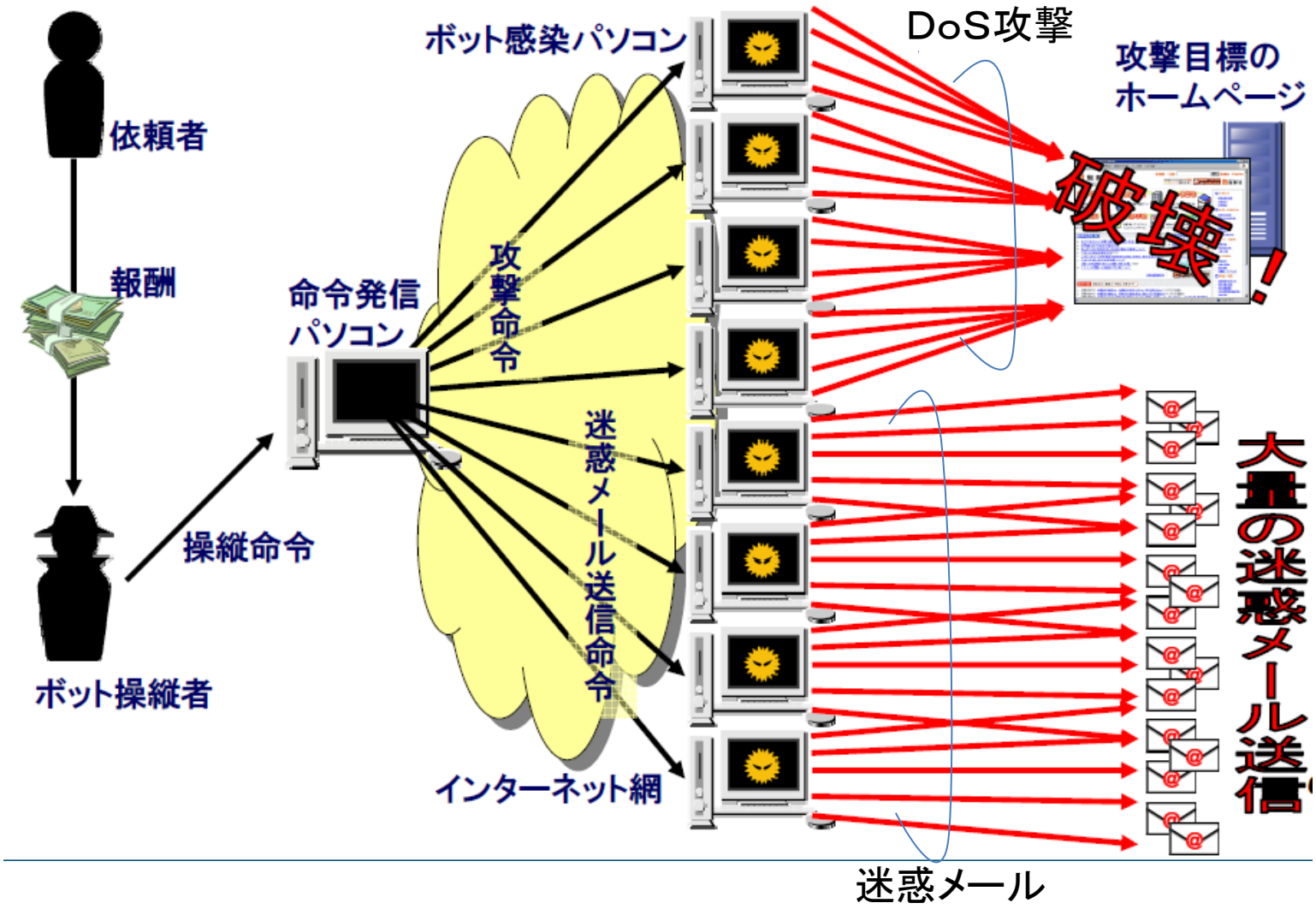
アンダーグラウンドビジネスに利用

語源はロボット（Robot）
　　ロボット：人間の指示に従って行動を起こす

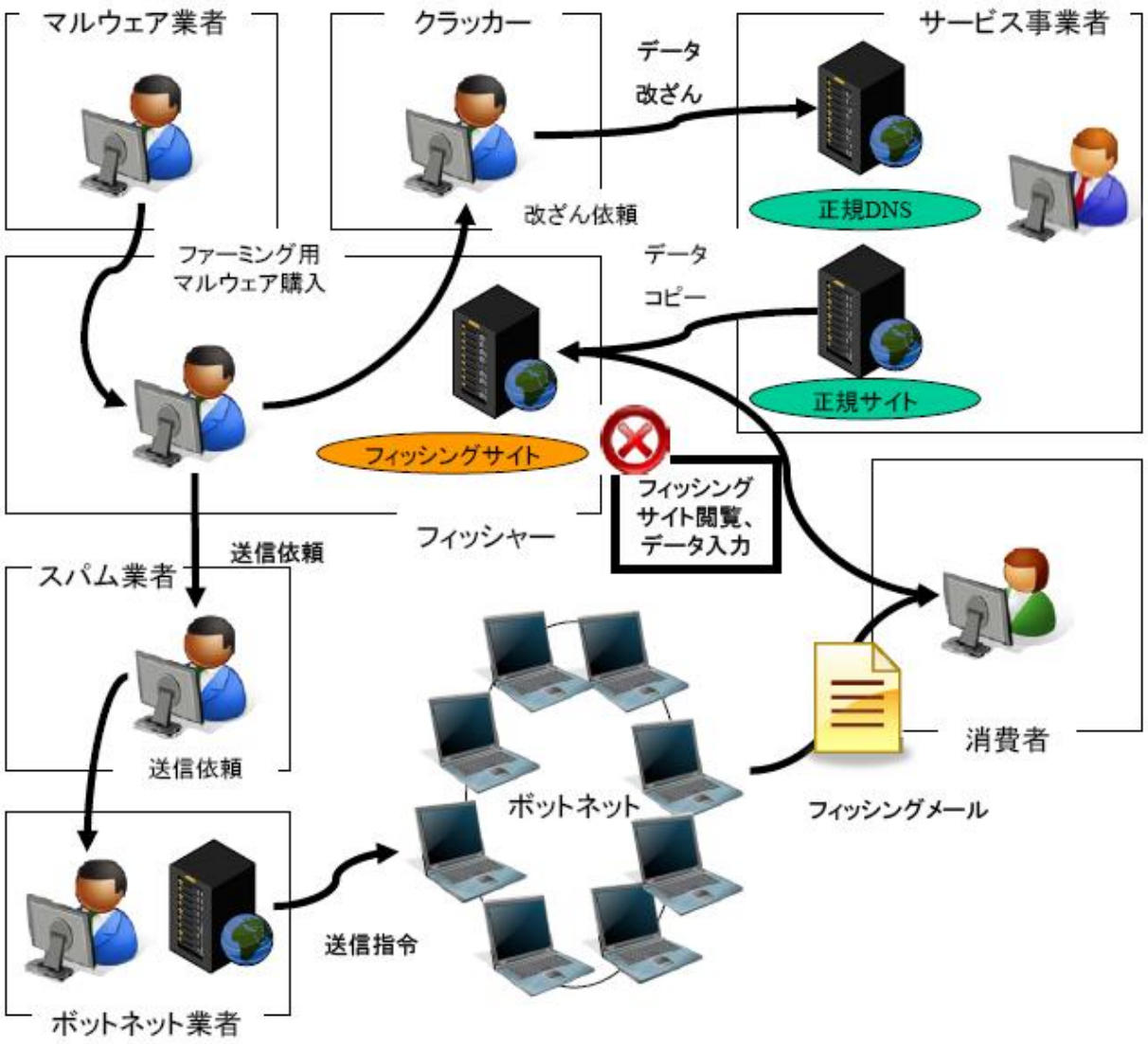
攻撃者の命令を受けて，その命令に従って感染や攻撃をするプログラム

出典；Telecom ISAC Japan

ボットを利用した迷惑行為



ボットネットとフィッシング詐欺



フィッシング詐欺；WWWやメールを用いた詐欺の一種

実際の偽メール

Subject:【重要なお知らせです】
To:xxxxx@yahoo.co.jp

Yahoo! Auctionsよりご案内です

いつもYahoo! Auctionをご利用頂きありがとうございます。
http://prlamiemrimenbersid.●●●●●●●●.com/yahoo-actions.co.jp/ir
よりお客様の会員情報の更新をお願いします。
更新を行われない場合、出品制限等の不具合を起こす場合も
ありますのでご協力お願い致します。

※こちらのメールは自動送信メールとなっておりますので、そのままご返信い

Thanks 10 years! Yahoo! Shopping and Yahoo! Auctions

実際の偽サイト

YAHOO! JAPAN プレミアム こんにちは [ログアウト]

YAHOO! JAPAN - ヘルプ

Yahoo!プレミアム

重要なお知らせ Yahoo! JAPANを装ったメール、偽の情報登録ページを用いて、お客様の個人情報を不正に聞き出す事例が報告されています。個人情報を入力する際には、アドレス欄がhttp通信であることを確認し、十分ご注意ください。

お客様情報とお支払い方法を入力して、画面下の「登録」ボタンを押してください。[必須] は入力必須項目です。
※Yahoo!JAPAN IDに登録されている情報は、下記のフォームに自動入力されています。内容が正しくない場合は、修正のうえ、ご登録ください。

登録手順

1. お支払い情報の登録
2. 登録内容の確認
3. 登録完了

お客様情報の登録

郵便物をお送りする場合がありますので、ビル、マンション名まで含め、正確に入力してください。

名前 [必須] 姓 名

フリガナ [必須] セイ メイ (全角)

郵便番号 [必須]

(半角数字) 例) 1110001、111-0001

都道府県 [必須] 以下より選択してください

住所1 [必須]

住所2 [必須]

ビル、マンション名等

電話番号 [必須] - - (半角数字)

ヒント

お客様情報の登録

- 海外在住の場合はこちらをご覧ください。
- 郵便番号から住所を検索できない方はこちらをご覧ください。
- 「住所2」には住所を検索した結果の続きを入力し

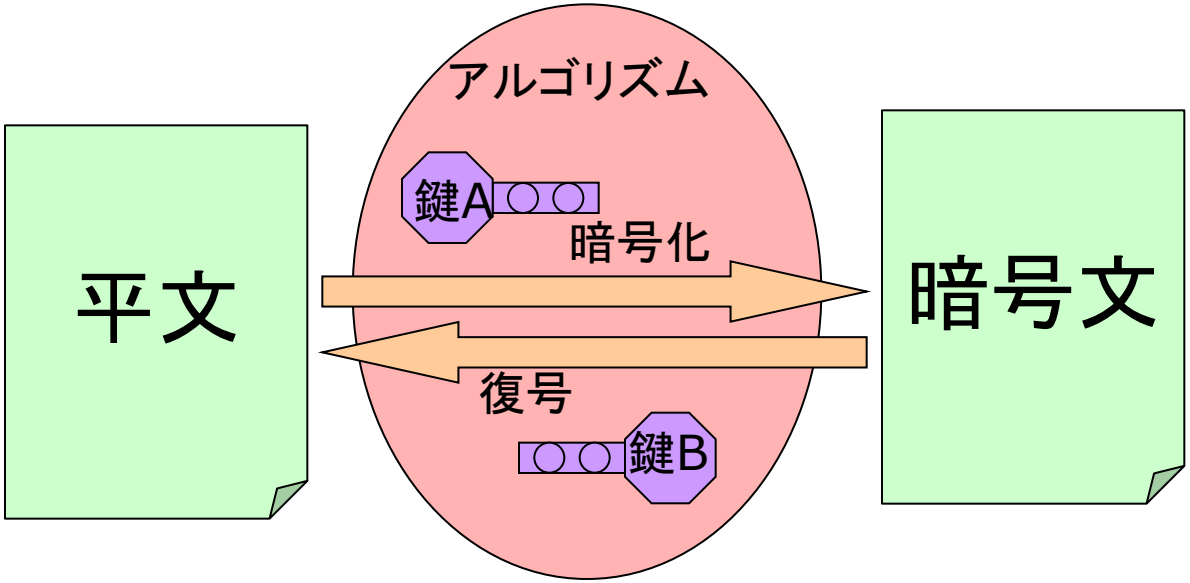
暗号化技術

暗号方式

- 共通鍵暗号 （慣用暗号，対称暗号）
  - 暗号化と復号に同じ暗号鍵を使う
  - DES（デス），3DES（トリプルデス），AESなど多数
  - 太古の歴史あり
  - 数字の列
- 公開鍵暗号 （非対称暗号）
  - 暗号化と復号に異なる暗号鍵を使う
  - RSA
  - 生まれて30年余り
  - 20世紀最大の発明と言う人も

現代暗号の仕組み

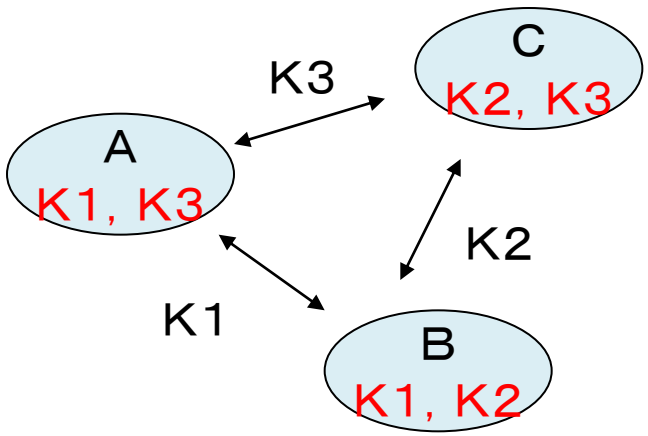
アルゴリズムは公開、暗号鍵を隠す



- 共通鍵暗号：暗号化と復号に同一の鍵を用いる方式
- 公開鍵暗号：暗号化と復号に異なる鍵を用いる方式

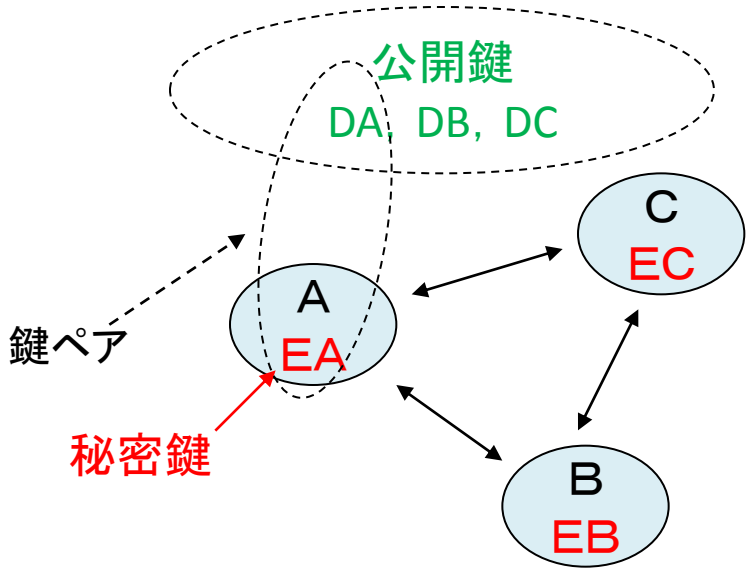
古代暗号（～1970年代）はアルゴリズムも秘匿
暗号の存在自体が秘密

共通鍵暗号による暗号通信



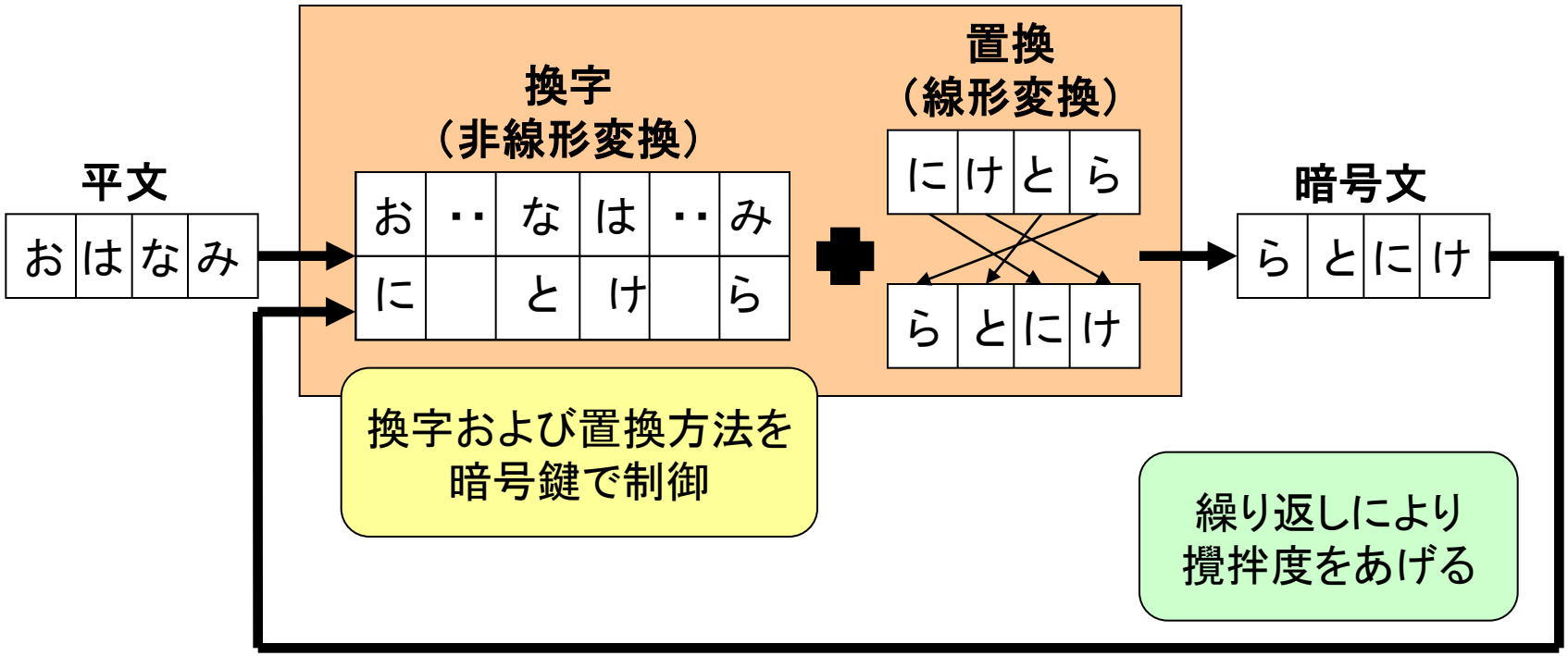
あらかじめ、共通鍵を共有しておく

公開鍵暗号による暗号通信



鍵ペアを生成し、一方の鍵を公開する

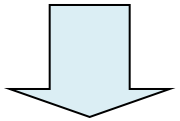
共通鍵暗号アルゴリズムの原理



暗号鍵により換字と置換のルールが変わる

共通鍵暗号の課題

1. 鍵の配送が難しい
   どうやって安全に鍵を相手に渡すのか？
   →事前に手渡しするなど
2. 鍵の管理が面倒
   すべての人と完全に安全な通信を行おうとした場合、通信相手の数だけ鍵が必要
   鍵の数＝ユーザ数×（ユーザ数－１）/2
   →ユーザ数を限定する必要性



公開鍵暗号方式の誕生（1976年）

公開鍵暗号

・公開鍵暗号では暗号鍵が2つある

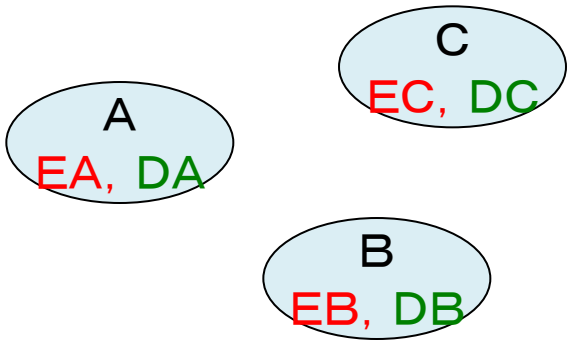
・2つの鍵には数学的関連性がある

・鍵1で暗号化したものは鍵2で復号、鍵2で暗号化したものは鍵1で復号できる

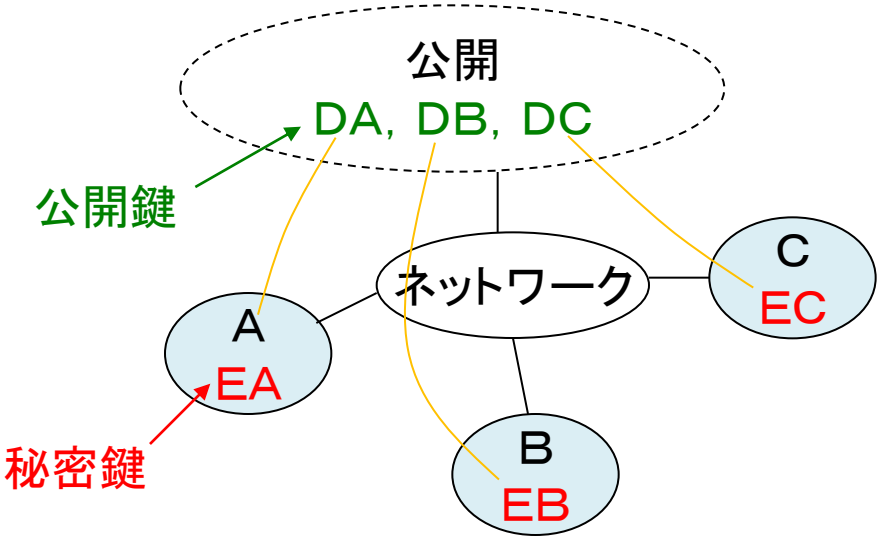
・どちらか一方の鍵を公開する

ノード	鍵1	鍵2
A	EA	DA
B	EB	DB
C	EC	DC

各ノードで鍵ペアを生成する



一方の鍵をネットワーク上に公開する



公開鍵から秘密鍵を類推することは数学的に困難

ペアの関係

公開鍵の代表：RSAの原理

暗号化　$C=M^e \bmod n$

復号　$M=C^d \bmod n$

M；平文

C；暗号文

(e, n)； 公開鍵

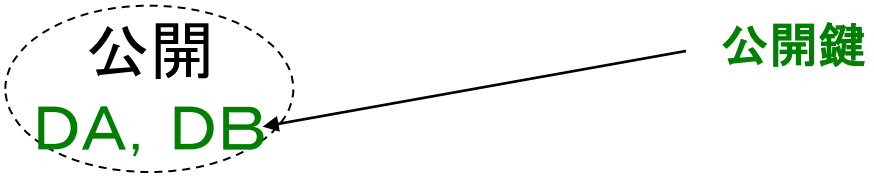
(d, n)； 秘密鍵

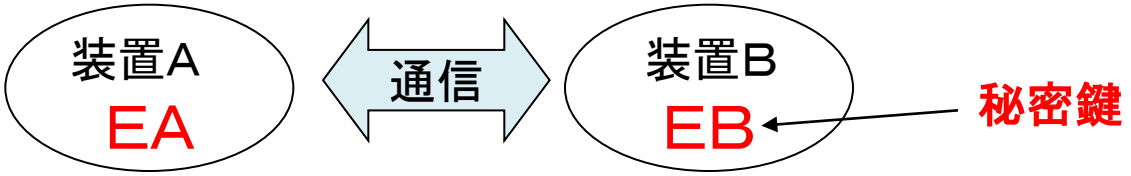
条件
n=pq
p,qは素数

非常に大きな数の素因数分解は困難であることを利用する。
n から p, q を計算することは困難。
p, q が分からないと、(d, n) を計算するのに膨大な時間を要する（事実上不可能）。

a mod n ; aをnで割ったあまり(例：2=17 mod 3)

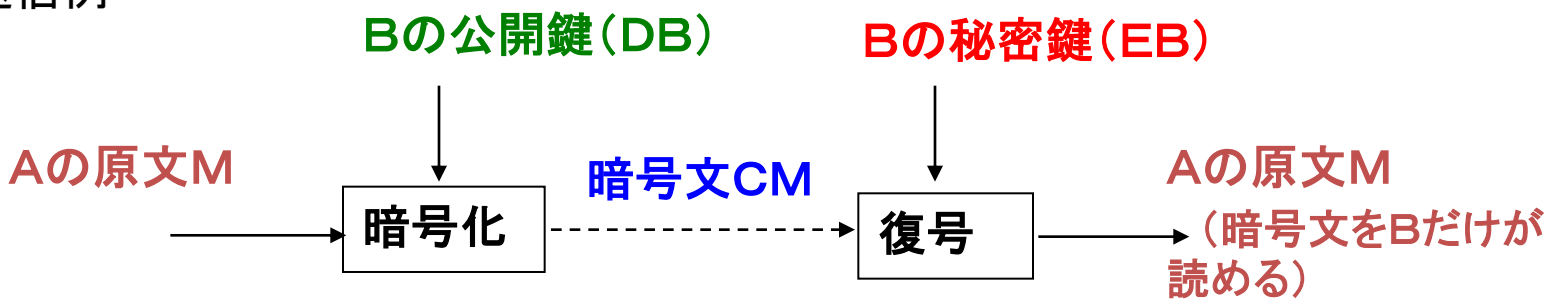
公開鍵の使用方法



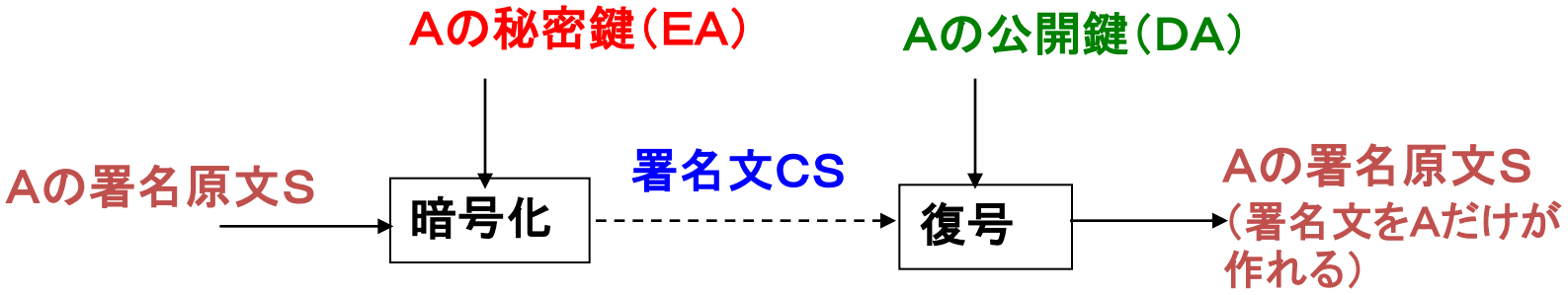


AからBへの送信例

暗号化



認証



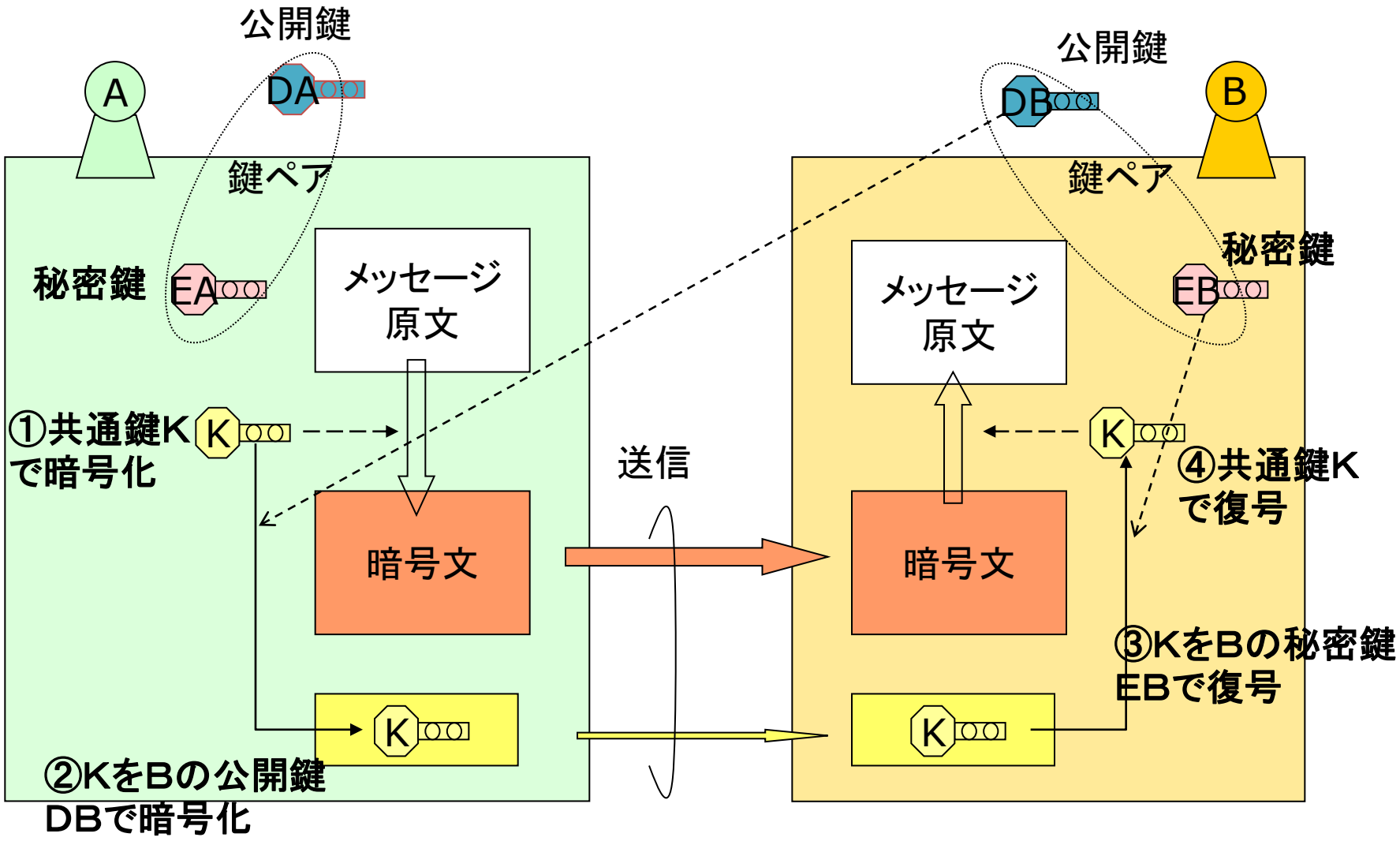
秘密鍵による暗号化を「署名」と呼ぶ

両暗号の比較

比較項目	共通鍵暗号	公開鍵暗号
処理速度	早い	遅い （共通鍵暗号より3桁遅い）
鍵の配送	要	不要

- 公開鍵暗号で共通鍵暗号用の鍵を配送し，情報の暗号化には共通鍵暗号を用いるハイブリッド方式がよく利用される.

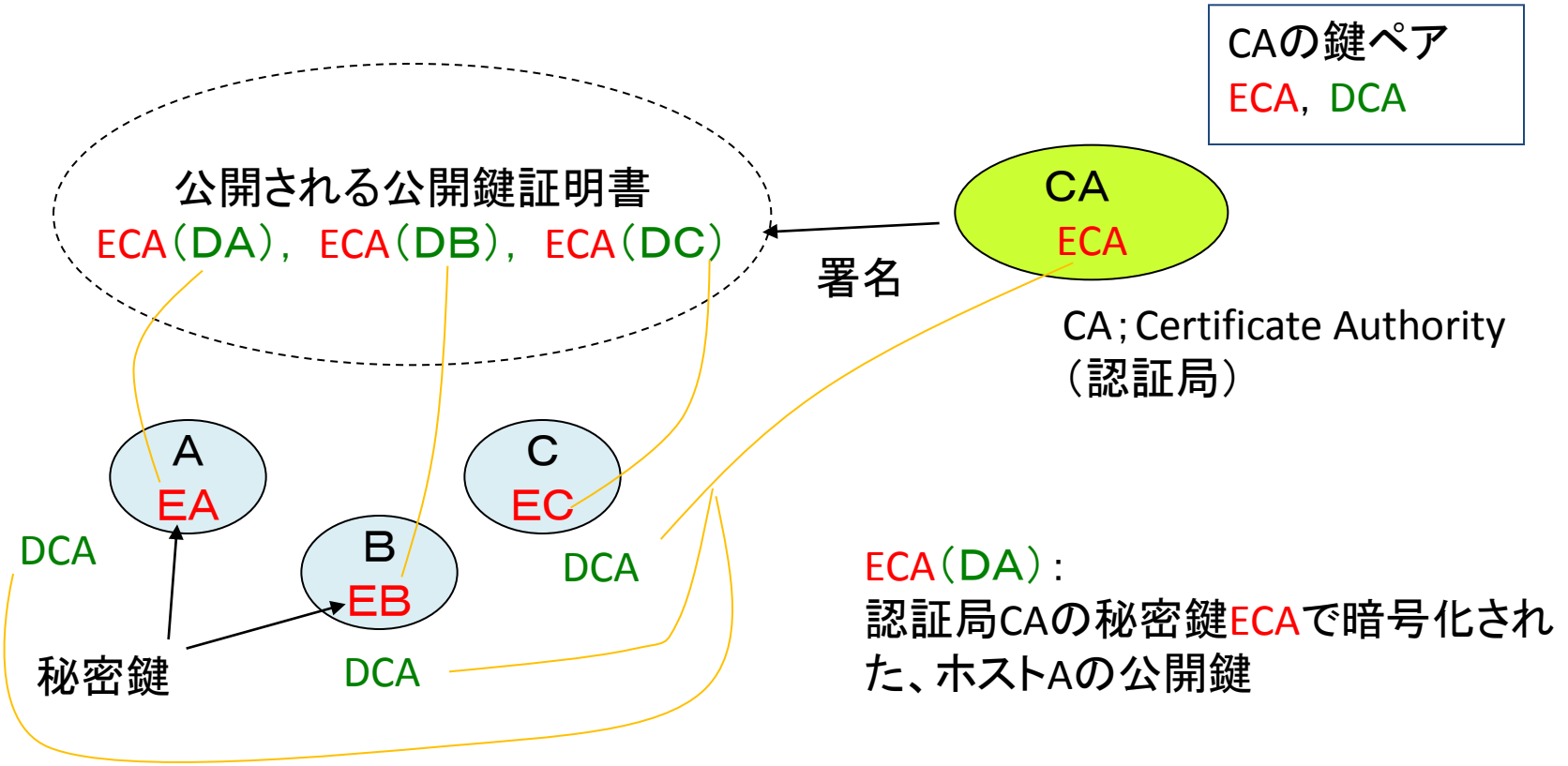
共通鍵と公開鍵の利点を組み合わせた暗号化通信（Bの公開鍵を使用）



公開鍵が正しいという前提が必要

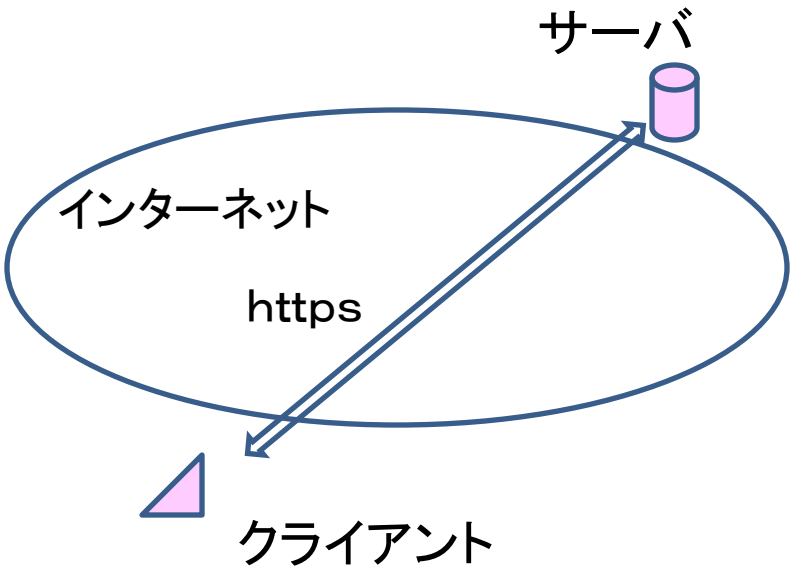
公開鍵認証基盤：PKI（Public Key Infrastructure)

公開鍵が正しいことを証明するしくみ
信頼できる第三者機関（CA）が公開鍵に署名して公開鍵証明書を発行
公開鍵証明書を公開する

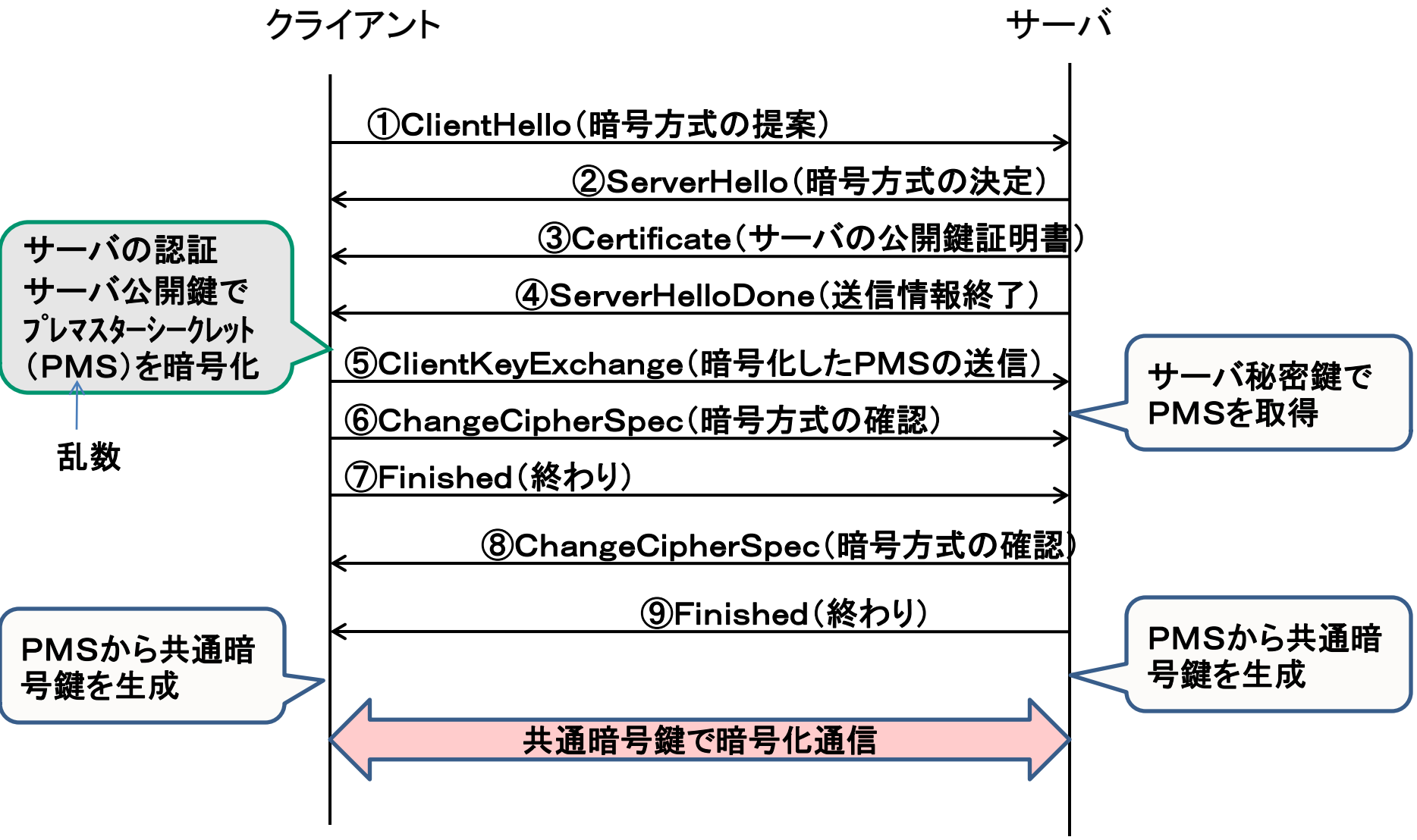


PKIの代表的な応用例
SSL(Secure　Socket　Layer)

インターネットショッピングに必須の機能
- サーバが正しいことを証明する
- サーバ/クライアント間通信を暗号化する
  （個人情報，クレジットカード番号など）



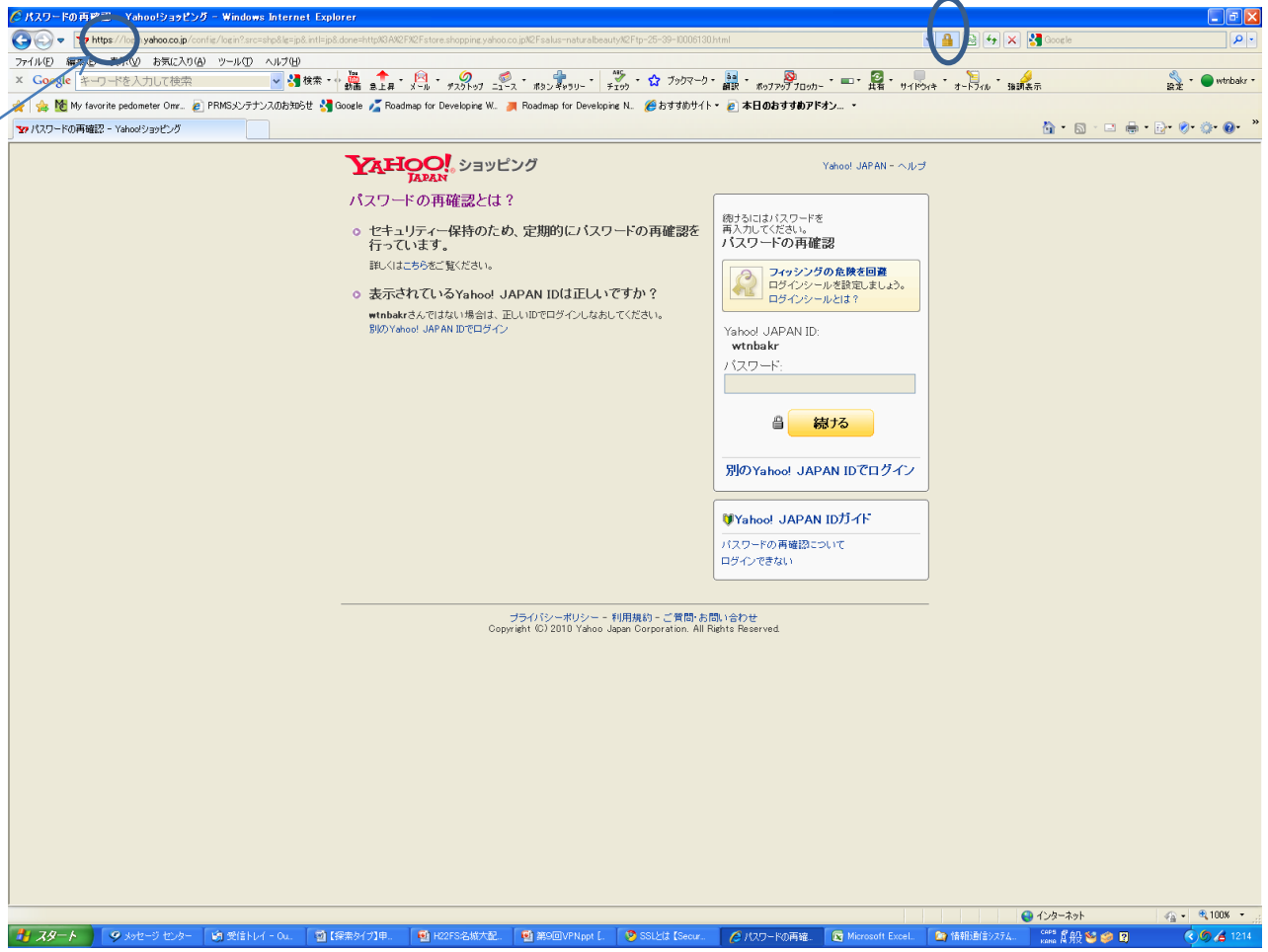
SSLのシーケンス


クライアント
サーバ
①ClientHello（暗号方式の提案）
②ServerHello（暗号方式の決定）
③Certificate（サーバの公開鍵証明書）
④ServerHelloDone（送信情報終了）
サーバの認証
サーバ公開鍵で
プレマスターシークレット
（PMS）を暗号化
乱数
⑤ClientKeyExchange（暗号化したPMSの送信）
⑥ChangeCipherSpec（暗号方式の確認）
サーバ秘密鍵で
PMSを取得
⑦Finished（終わり）
⑧ChangeCipherSpec（暗号方式の確認）
⑨Finished（終わり）
PMSから共通暗
号鍵を生成
PMSから共通暗
号鍵を生成
共通暗号鍵で暗号化通信

SSL通信中であることを確認する方法；
・ステータスバーに錠マークがある
・URL欄がhttps://で始まっている
　例　YAHOOショッピングのID登録画面

鍵マーク

URLがhttps
で始まっている



スマートフォンのセキュリティ

・ファームウエアをコンピュータのOSと同様に最新のものとする

・パスコードを設定する
　一定時間使用しないと自動的にロックがかかる
　誤ったパスコードが10回連続すると、ユーザ設定や保存されているすべてのデータが削除される

・ネットワークへの自動接続を解除
　WiFiに自動接続すると、ネットに接続されていることに気付かない
　WiFiを使用しないときは自動接続をオフにするとセキュリティを高めることができる

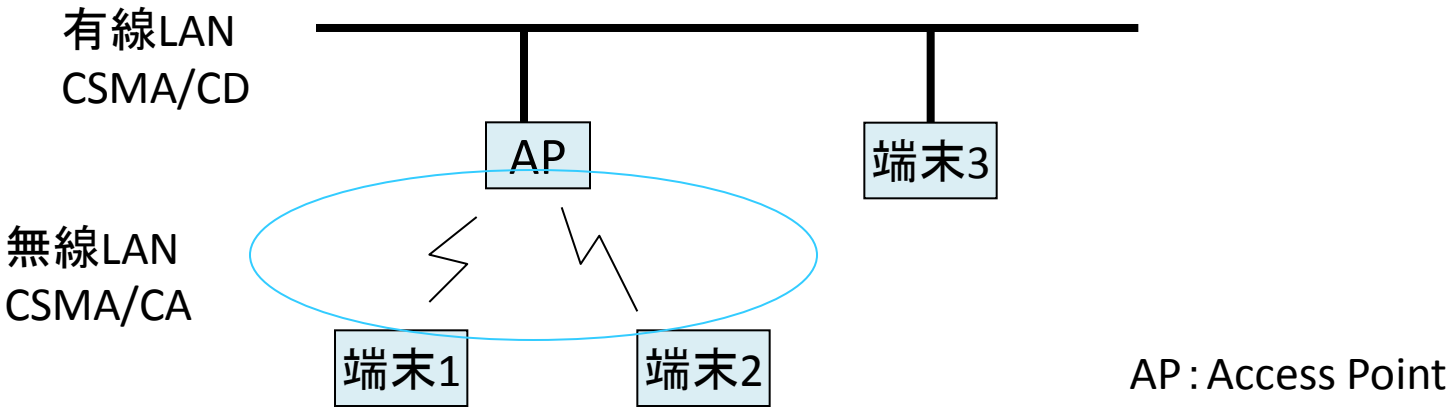
・端末を処分したり修理に出す際にはデータを消去する

・安全なブラウザを使用してWebサイトを閲覧する
　WEBアクセス時にレピュテーションデータベースに確認し、不正なファイルが置かれていた場合や不正なページへの接続であった場合はブロックする。フィッシン詐欺や個人情報詐取などの「Webからの脅威」から守ることができる。

レピュテーション；評判、世評

無線LANのセキュリティ

- SSIDの隠蔽
- MACアドレスフィルタリング
- WEP/WPA（暗号化）



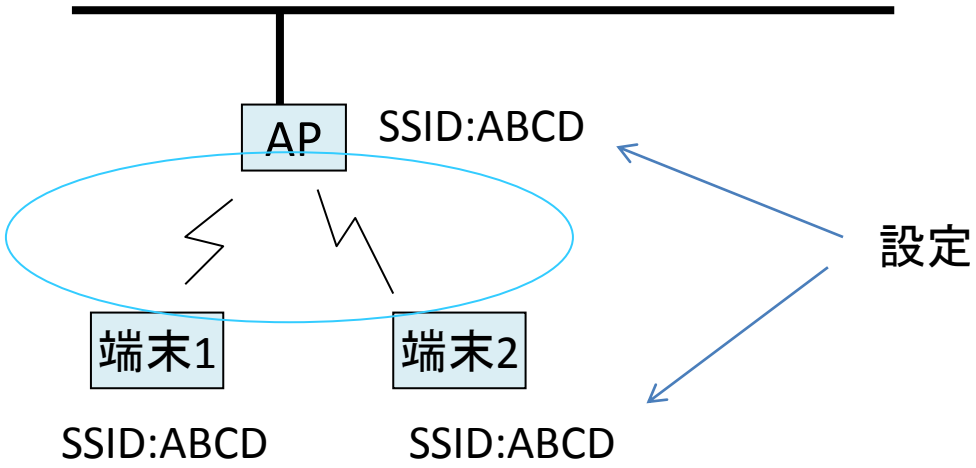
AP : Access Point

SSIDの隠蔽

（Service Set ID）

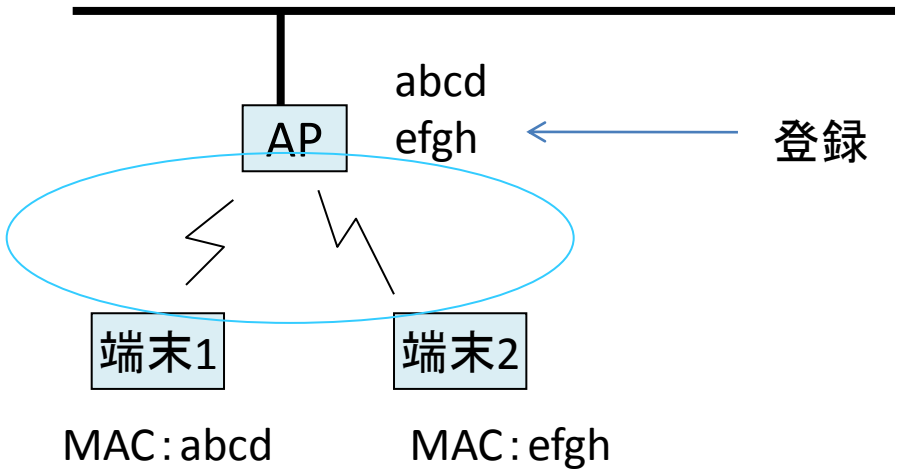
同じSSIDを設定した端末だけがAPに接続できる

→簡単なセキュリティ対策として利用可能



MACアドレスフィルタリング

APにMACアドレスを登録したノードだけがAPに接続できる



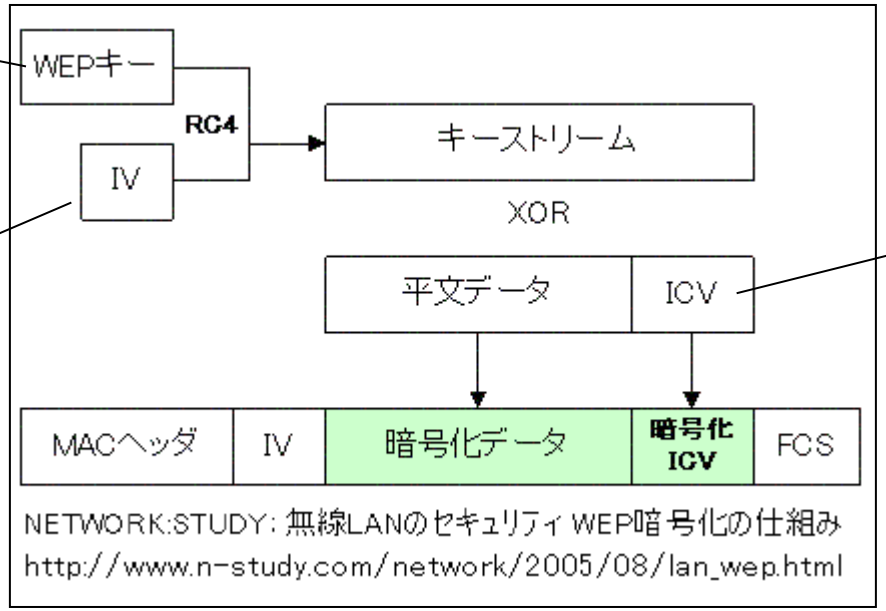
ネットワークをモニタすればMACアドレスがわかるため偽造される可能性がある

WEPによる暗号化

無線LANの世界で最初に登場した暗号化方式
（現在でも多く使われている）

パスワードから生成した暗号鍵
（5または13バイト）

パケットごとに生成した乱数
（3バイト）

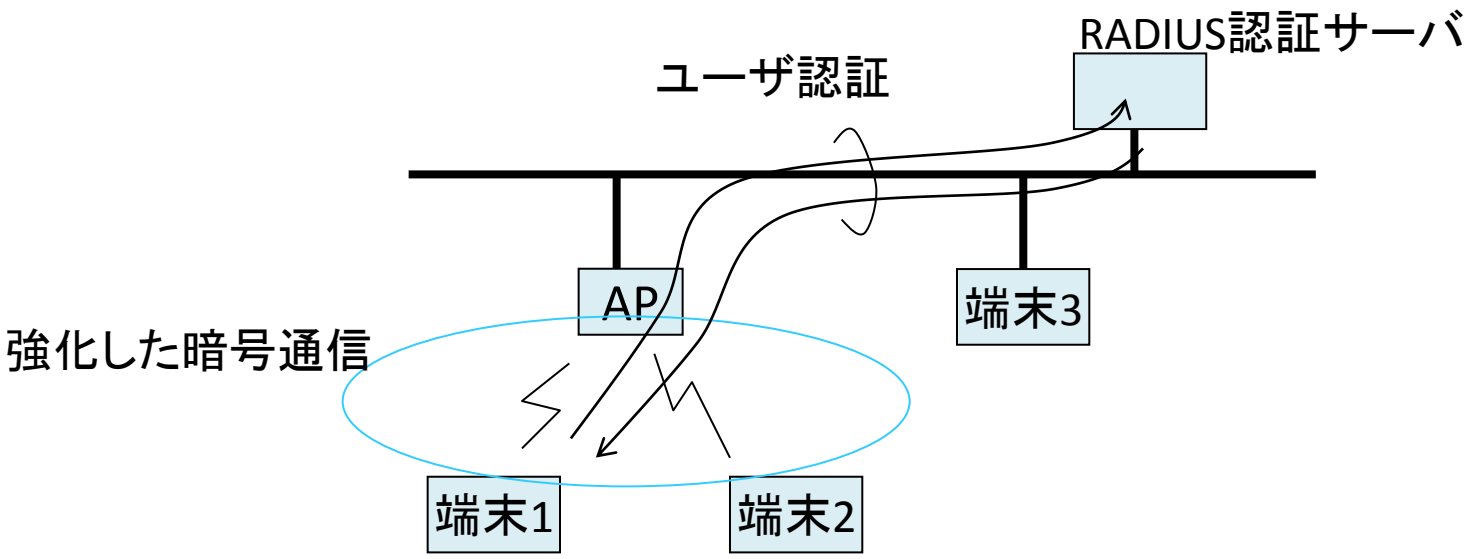


平文データのハッシュ値

WEPの脆弱性
暗号化に使う鍵データの生成方法が単純
同じ暗号鍵が使われ続ける

WPA（Wi-Fi Protected Access）

・アルゴリズムの強化
・暗号鍵を10,000パケットごとに更新
・ユーザ認証機能を追加（RADIUS）
　RADIUSを使う方法
　共通暗号鍵を保持させる方法



高齢者見守りシステムの提案

背景
・少子高齢化
・独居老人の増加
・高齢者ドライバの増加
↓

遠隔地から高齢者を見守るサービスが必要

遠隔監視に関する類似研究

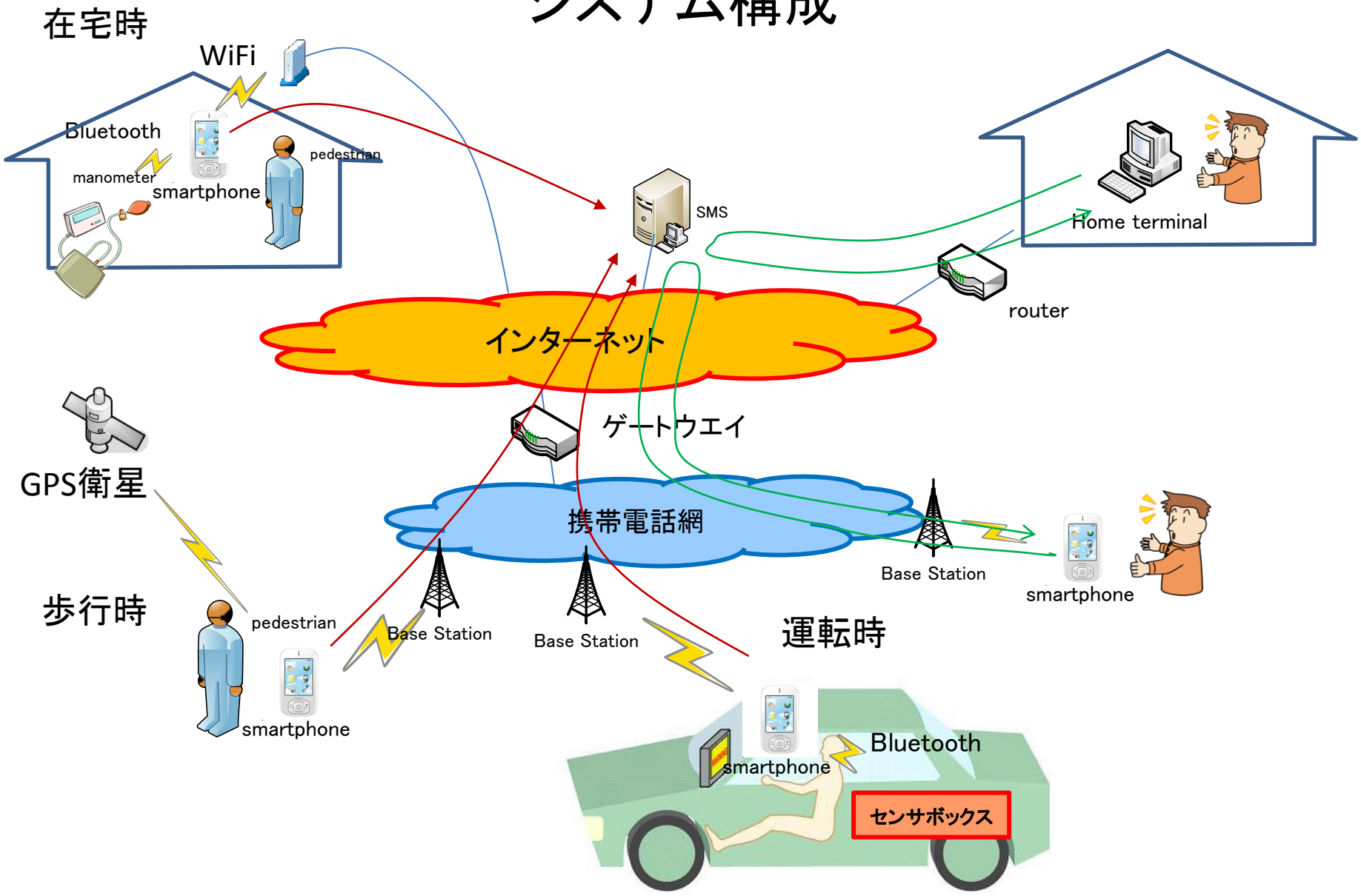
名称	組織	センサの対象	備考
ホームヘルスケア プロジェクト	NEDO 健康機器メーカ	健康機器からのセンサ情報 （脈拍、血圧、体温）	在宅時のみ
Cell Link	なし（国際会議発表）	車速度、エンジン回転数等	車が対象
見守り安心ネット 公田町プロジェクト	国交省 横浜市	人感センサ、TVリモコン、照明	在宅時のみ

提案システムの特徴：

見守る側の人を対象としたシステム
スマートフォンを利用

高齢者の安否を常に確認できる（いつでも、どこからでも）
運転時には車両の情報も取得する
取得情報
　位置情報、歩数、体組成、（脈拍、脳波）
　車速度、センターラインからの距離の分散
暗号化技術でプライバシーを確保

システム構成


在宅時
WiFi
Bluetooth
manometer
smartphone
pedestrian
SMS
Home terminal
router
インターネット
ゲートウエイ
GPS衛星
携帯電話網
Base Station
Base Station
Base Station
smartphone
歩行時
pedestrian
smartphone
運転時
smartphone
Bluetooth
センサボックス

表示例

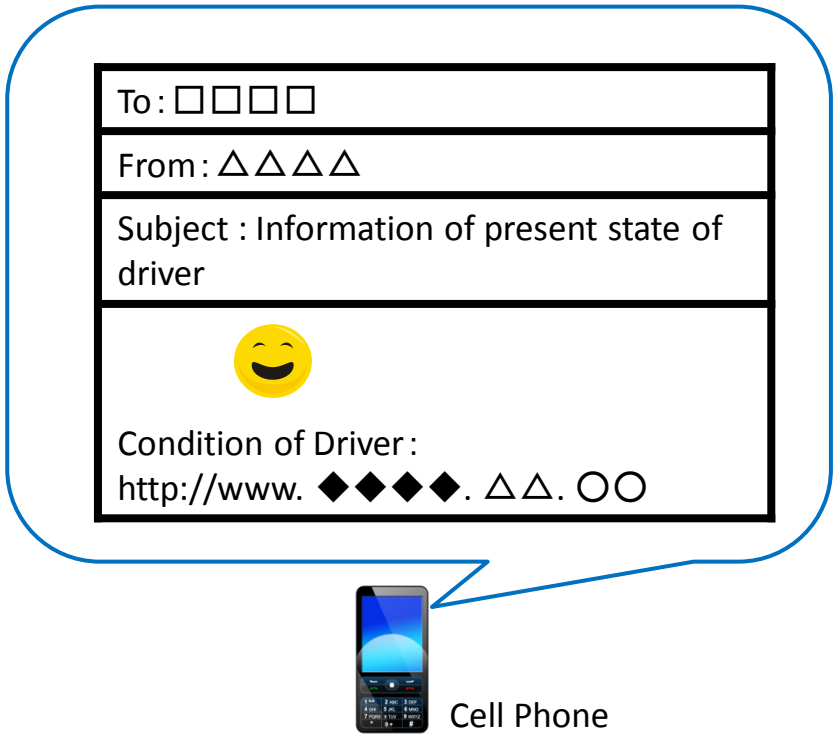
サーバに蓄積された情報を
ホーム端末より閲覧した例

位置トレース（GPSにより位置情報を取得）

歩数の履歴（加速度計の変化から歩数を計測）

現状
・GPSによる位置トレースの表示
・歩数計の表示

今後
・血圧計、体組成計からのデータ取得（Bluetooth）
・ドライビングシミュレータからの車両データ取得と表示
・扱いやすいGUIメニュー画面（観察者側）
・過去統計データとの比較画面
・メールによる定期報告サービス（1日1回）
・異常時のアラームメール
・異常時のワンタッチダイレクト会話



ご静聴ありがとうございました

なぜインターネットは急速に普及したのか

・圧倒的な安さ
・キラーアプリケーションの出現　　WWW（1994年）
・検索エンジンの技術　→　リアルタイムでの情報収集
・ホームページによる情報発信
・豊富なアプリケーション（メール、WWW、地図、ショッピング、ニュース、電話）
・TCP/IPがインターネットの普及に耐えられるものであったこと