インターネットインフラ特論
６．IPセキュリティ

太田昌孝

mohta@necom830.hpcl.titech.ac.jp

ftp://ftp.hpcl.titech.ac.jp/infra6j.ppt

セキュリティ

- IPv6ではIPSECを標準実装、、、
- セキュリティには鍵が必要
  - IPSECだけでは使えない

インターネットセキュリティの本質

- エンドツーエンドセキュリティ
  - インターネットの基本原理がエンドツーエンド原理
- すべてのエンド（アプリケーション）をセキュアーに
  - 王道はない
  - 魔法もない

ILOVEYOU

- マクロウィルス
  - 小賢しいアプリケーションの弱点を攻撃
    - アプリケーションが勝手にプログラムを実行
- ファイアーウォール、VPN等をすべて透過
- 対策
  - 小賢しいアプリケーションやOSは使わない
    - マイクロソフト製品は不用意に使わない
  - ウィルスチェッカーも事後には有用だが、、、

インターネットの原理

- エンドツーエンド原理
  - 端末でできることは網側ではやらない
- グローバルコネクティビティ
  - 全端末は直結
- スケーラビリティ
  - 超大規模になっても困らない

セキュリティとは？

- 秘匿
  - 情報を第三者の目から隠すこと
  - 暗号化
- 認証
  - 身分証明
- 相互に関連
  - 認証のための情報は秘匿しなければならない
  - 認証された人には情報を秘匿しなくていい

秘匿の方式

- 共有秘密鍵
  - 暗号文＝E(平文、秘密鍵)
  - 平文＝D(暗号文、秘密鍵)
- 公開鍵
  - 暗号文＝E(平文、公開鍵)
  - 平文＝D(暗号文、秘密鍵)

認証の方式

- ハッシュ関数（疑似乱数）を利用
- 共有秘密鍵
  - 認証情報＝H（平文、秘密鍵）
- 公開鍵
  - 認証情報＝A（H（平文）、秘密鍵）
  - D（認証情報、H（平文）、公開鍵）

WEAK SECURITY

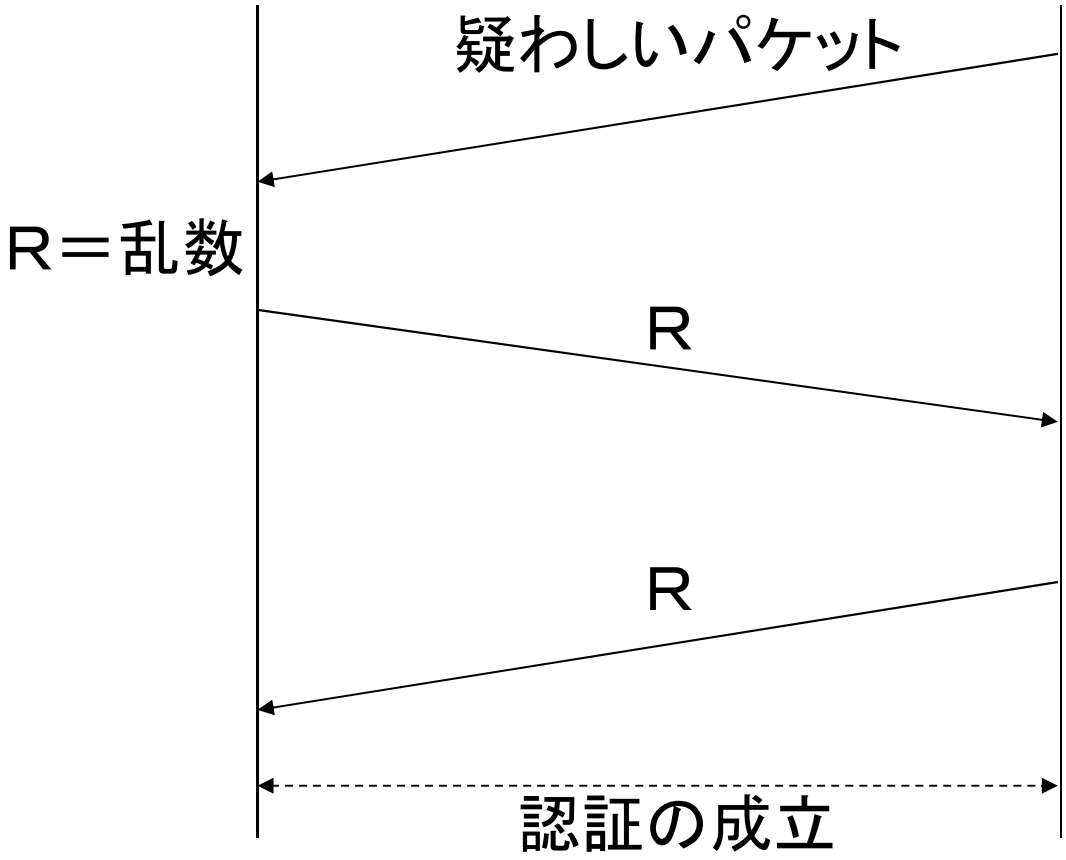
- 第三者の提供するインフラを無条件に信頼することに基づくセキュリティ
  - ISPが信頼できれば、指定したIPアドレスの相手と通信でき、パケットの盗聴も改変もない
  - ISPがパケットの盗聴や改変をすれば破綻
- 電話網のセキュリティも、この程度
  - 電話会社が通話の盗聴や改変をすれば破綻
- （実はPKIのセキュリティも、この程度）

電話網のセキュリティ

- 電話事業者は信頼できると仮定
  - ある電話番号にかければ、その電話番号の電話につながる
  - 途中で盗聴もない
  - 電話番号により相手を特定可能
    - 電話会社の通知する相手の番号は信用する
    - 相手の自称する電話番号は信用できない
      - 掛けなおしによる確認は必須
- あくまで仮定にすぎない

インターネットの WEAKセキュリティ

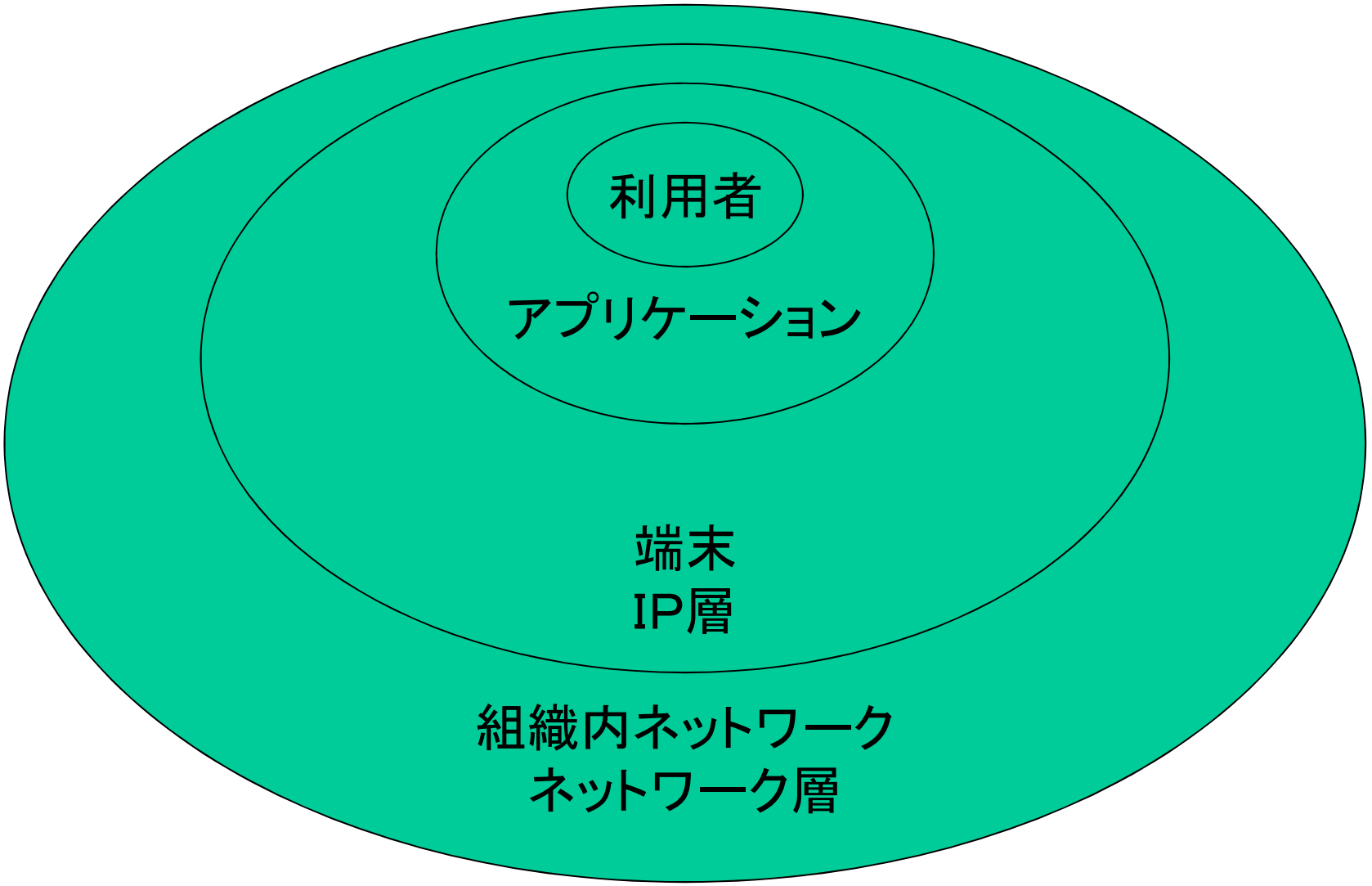
- インターネット事業者は信頼できると仮定
  - あるIPアドレスにパケットを送れば、そのIPアドレスの相手に届く
  - 途中で盗聴もない
  - IPアドレスにより相手を特定可能
    - ただし、あるパケットが届いても、そのソースIPアドレスからきたパケットとは限らない
      - ハンドシェークによる確認（自分の送った疑似乱数が相手から帰ってくる）は必須



WEAKセキュリティのための相手IPアドレスの認証

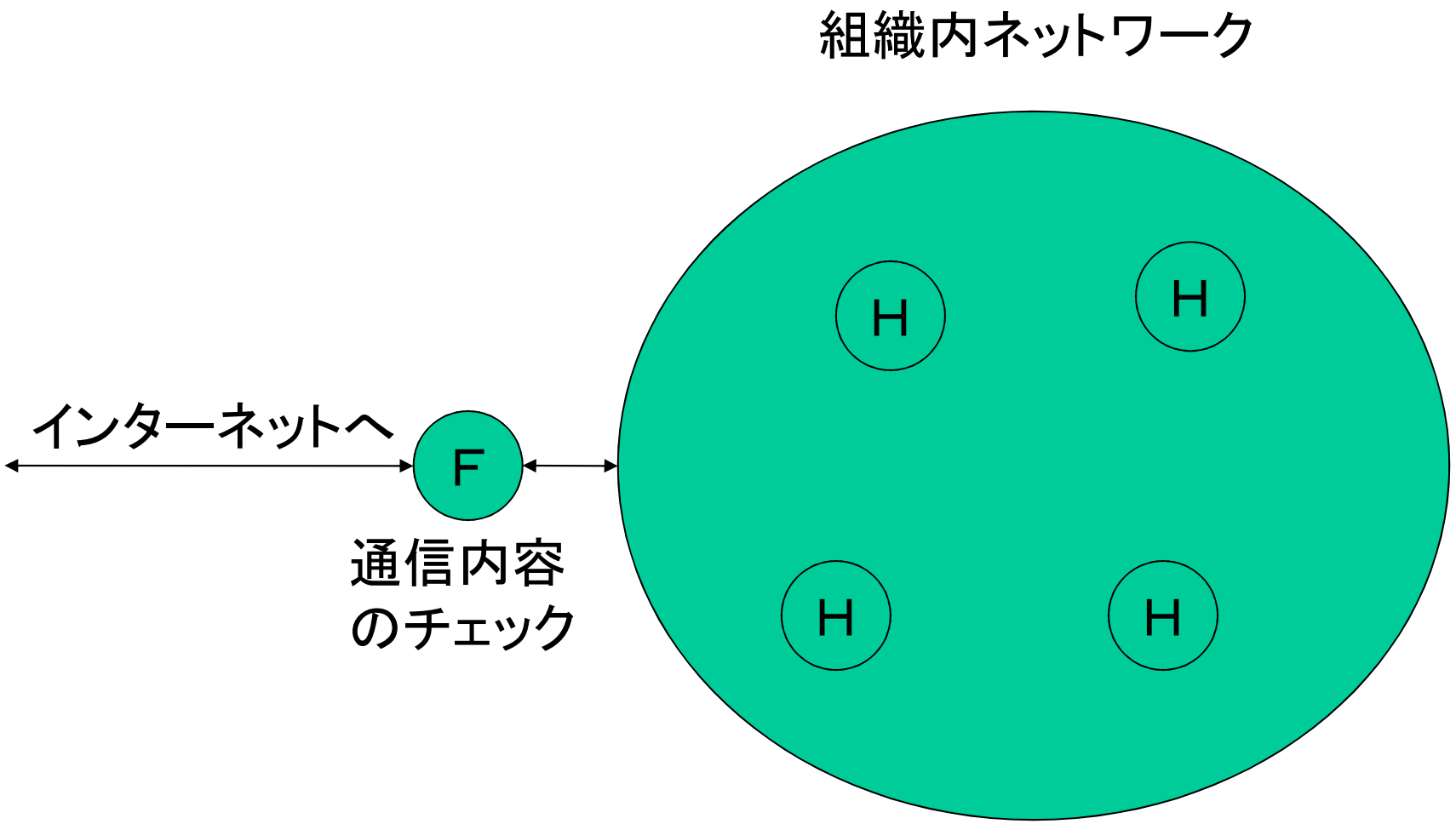
セキュリティの目的

- 個々のアプリケーションの個々の利用者にセキュリティを提供すること

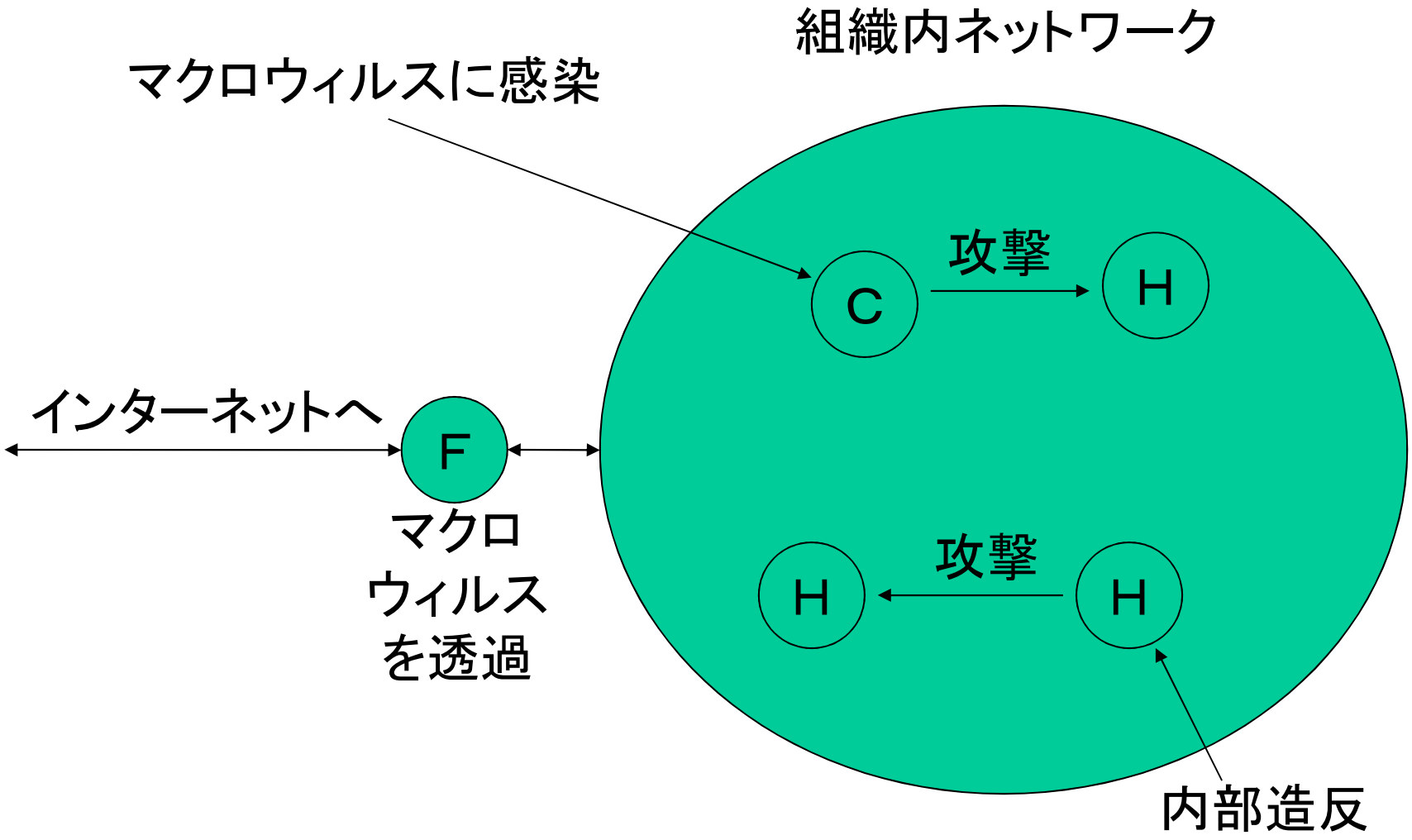

利用者
アプリケーション
端末
IP層
組織内ネットワーク
ネットワーク層

セキュリティの手段

- ファイヤーウォール？
  - ネットワークの一部を他の部分から隔離する
  - ネットワーク層でのセキュリティしかない
  - 気休めにしかならない（風邪薬と同じ）
    - 個々のホストにセキュリティがあれば、ファイヤーウォールは不要



ファイアーウォールの意味



ファイアーウォールの無意味

本当のセキュリティのためには

- 各ユーザーがセキュリティを意識
- 各アプリケーションをセキュアに
- 各ホストをセキュアに
  - 他人とホストを共有する場合は要注意

本当のセキュリティの実現

- 秘密鍵の共有
  - なんらかの方法で、通信の当事者間で秘密鍵を共有
  - N対NではN^2の鍵が必用に
- 公開鍵
  - 各自が秘密鍵をもち、それに対応する公開鍵を公開
  - N対NでもN個の鍵ですむ（Scalability！）？

公開鍵の原理

- 公開鍵から秘密鍵を計算するのは事実上不可能
  - 大きな整数の素因数分解や離散対数
- 秘密鍵から公開鍵を計算するのは比較的簡単
  - といっても、数百ビットの整数計算は大変
  - 実際の通信では、公開鍵を利用して共有秘密鍵（セッションキー）を交換（N^2より多い）

公開鍵と認証局

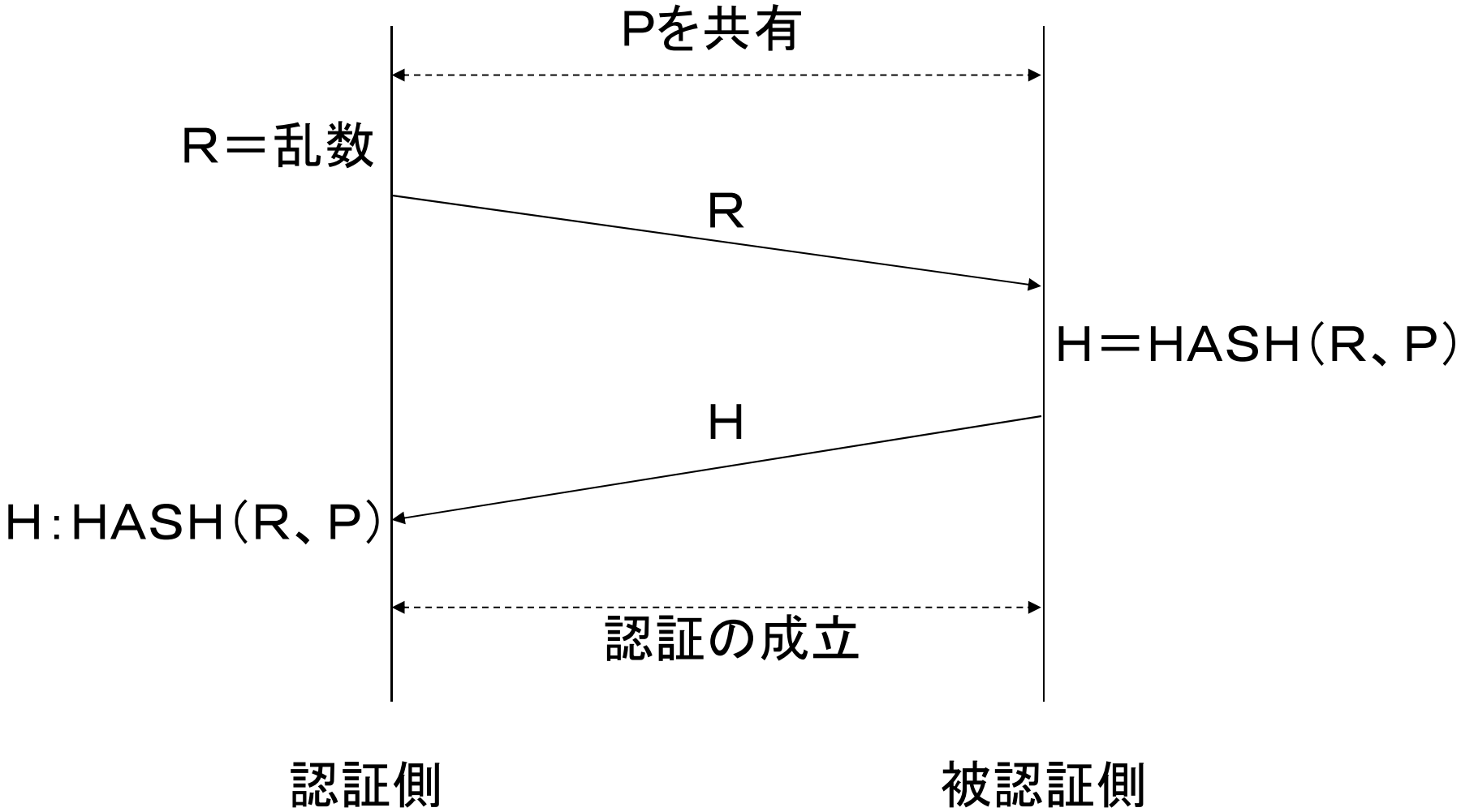
- 相手の公開鍵をどう知るか？
  - 公開鍵の認証が必用
- 認証局を置き、その公開鍵を共有
  - 認証局が他の組織の公開鍵を認証
  - さらに孫組織の認証も
    - 認証の階梯が社会構造を反映しないと無意味

認証のための秘匿の例

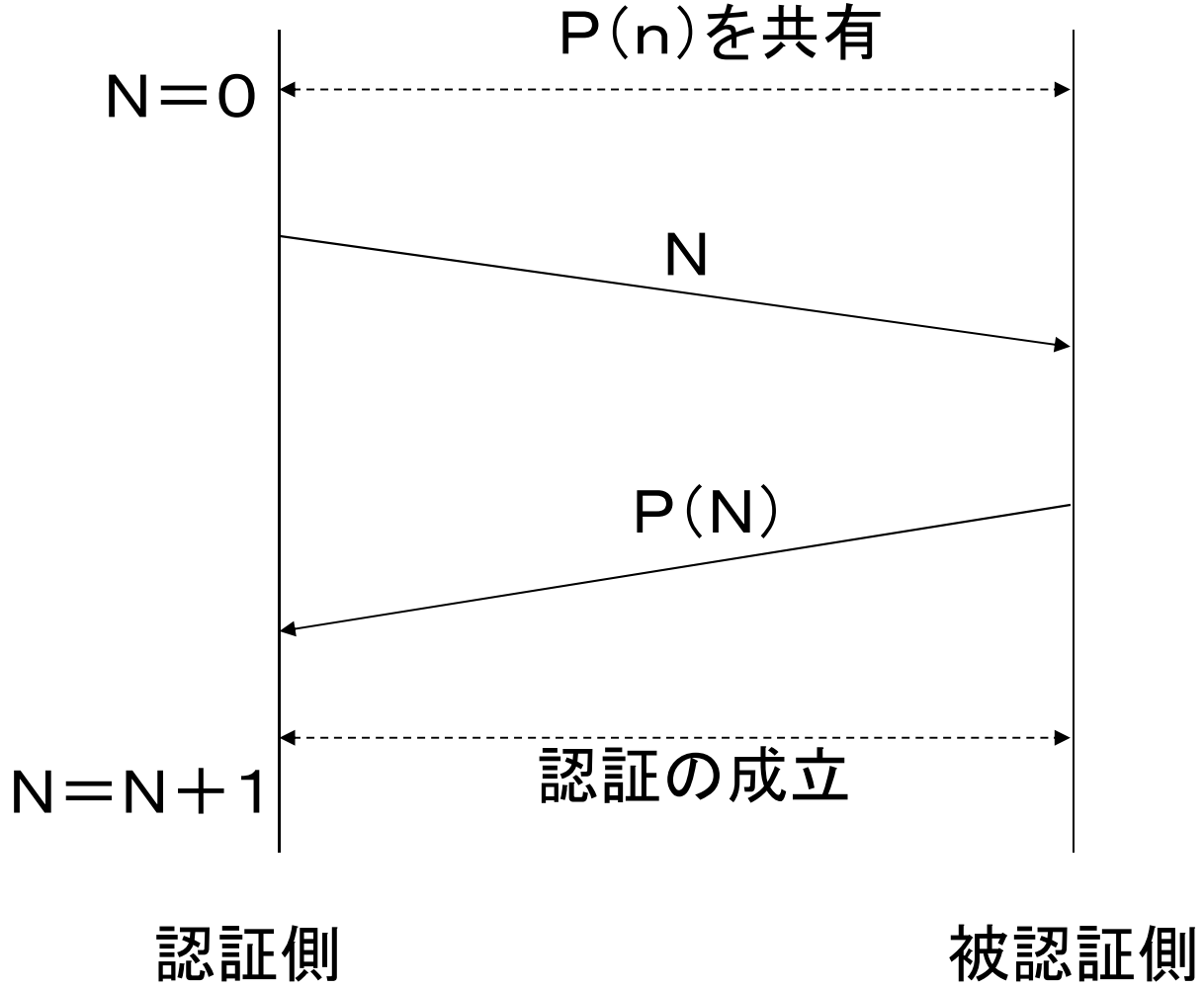
- 普通のパスワード
  - パスワードにより利用者を認証
  - 通信が傍受されると
    - パスワードが盗まれ、認証が成立しない
  - 傍受される通信路では普通のパスワードは使えない
    - ワンタイムパスワード等が必用に

安全なパスワード

- CHAP （Challeng Handshake Authentication Protocol）
  - 相手からの乱数（チャレンジ）と平文パスワードを組み合わせて疑似乱数を生成
  - 疑似乱数を送って照合
- ONE TIME PASSWORD
  - 同じパスワードは一度しか使わない
  - あらかじめ多数のパスワードを（携帯端末等に）記憶



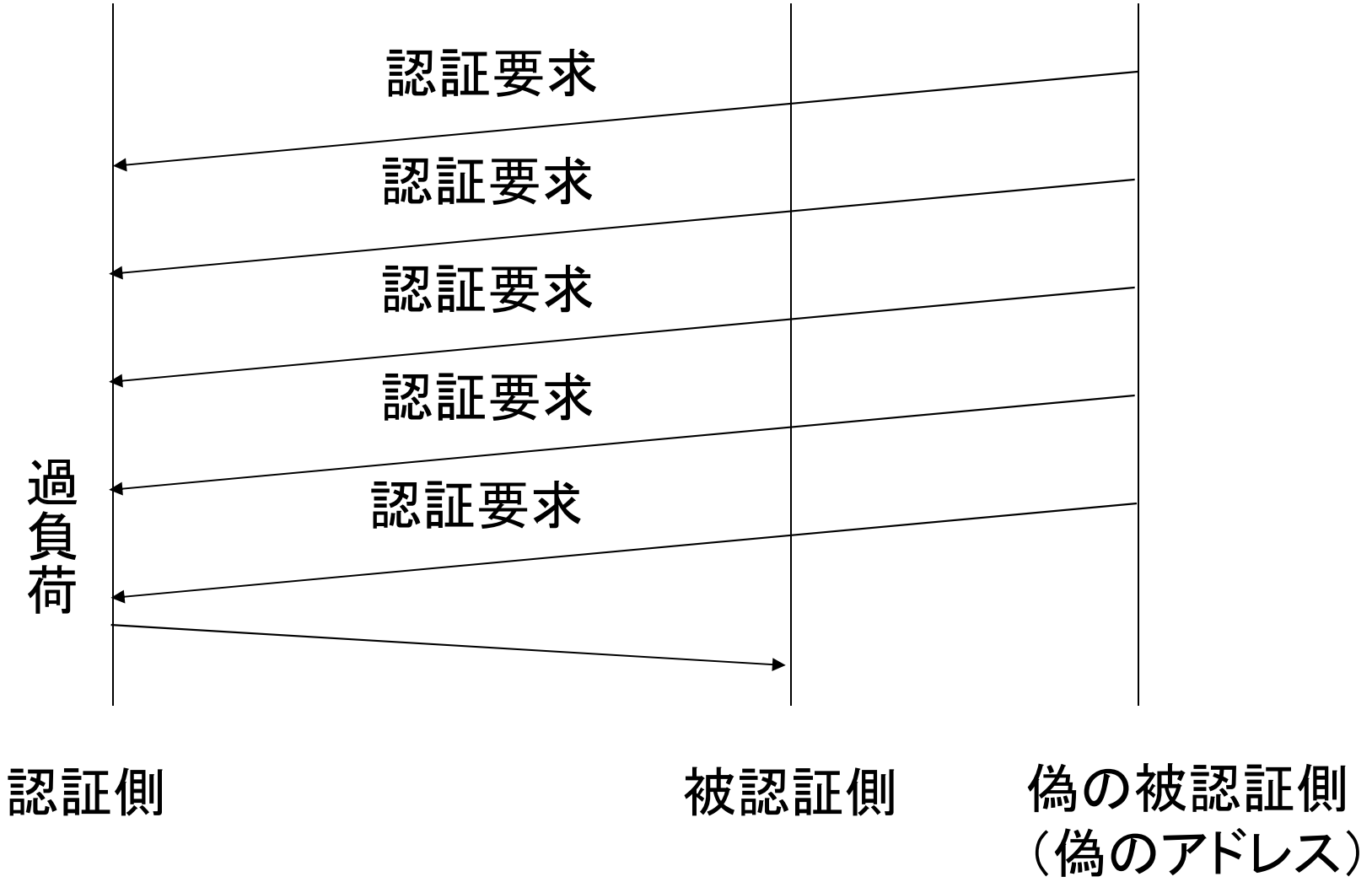
CHAPの仕組み（Pは通信路にあらわれない）



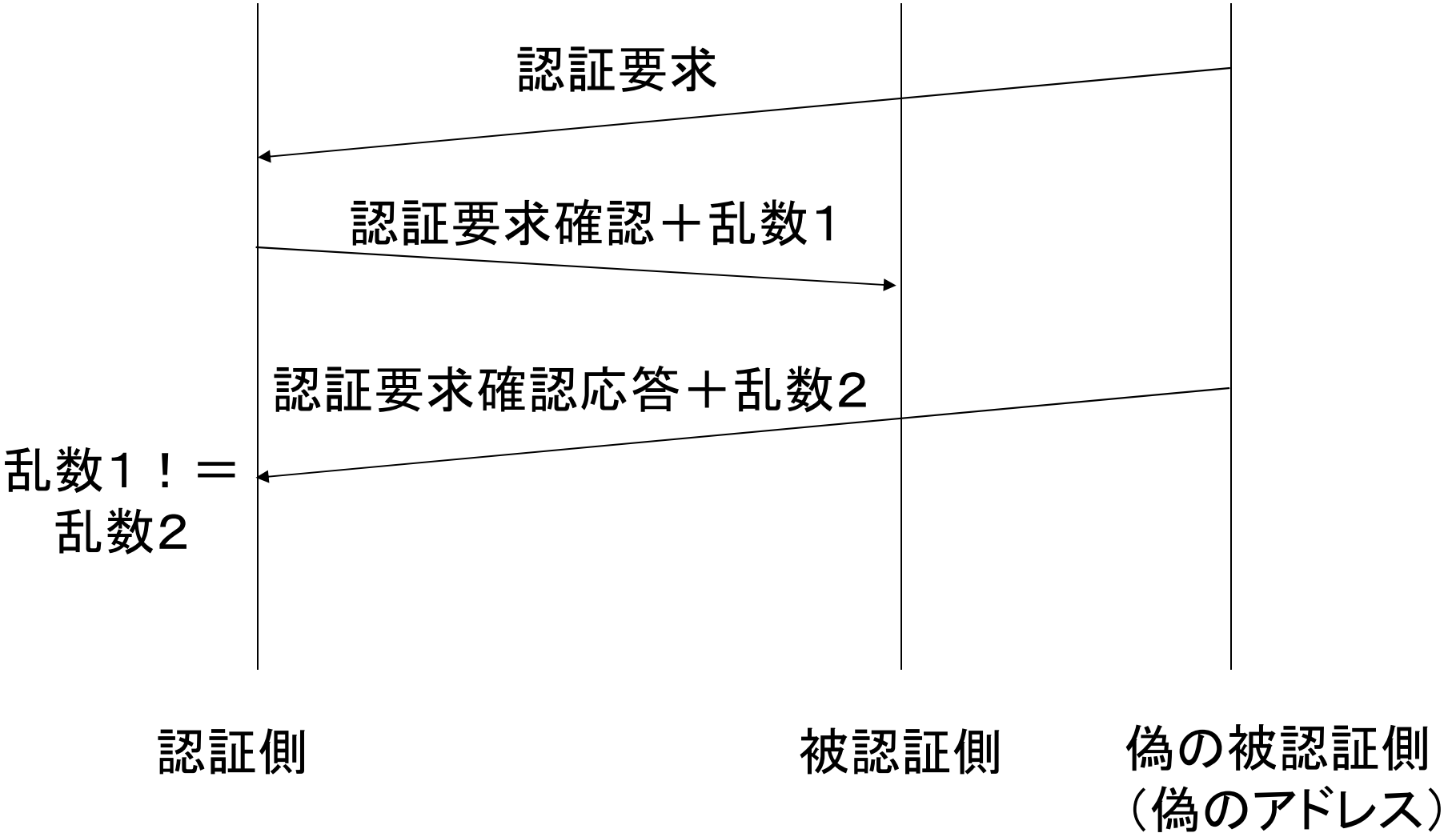
ONE　TIME　PASSWORDの仕組み
（同じP(n)は一度しか使わない）

DoS（Denial　of　Service）

- 無意味なデータにより無意味な負荷をかける攻撃
- 防ぐことは基本的に不可能
  - 高度（で高負荷）な認証はDoSの好餌
- 攻撃元を特定することは可能
  - 高度な認証をやるまえに、WEAKセキュリティによる3WAYハンドシェークを



DOS攻撃の例



DOS攻撃の被害の最小化

VPN （Virtual Private Network）

- インターネット上にプライベートネットワーク（インターネットではない）を構築する技術
- 完全なプライベートネットワークなら意味あり
  - 電話会社から専用線買うよりはまし（安い）
  - インターネットから電子メイルが到達するようではあまり意味がない

インターネットプロトコル群のセキュリティ

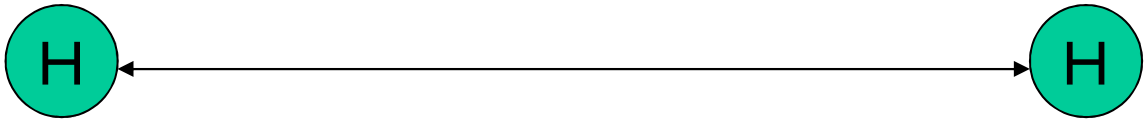
- 個々のプロトコルは個別のセキュリティを持つ
  - 例： FTPのパスワード
- 統一的な枠組みが必用？
  - IPSEC

IPSEC （RFC2401）

- トランスポート／アプリケーション層（SPIにより区別）のためのIPヘッダの標準フォーマット
- 秘密鍵を共有
- 認証（AH、ESP）と秘匿（ESP）を行う
- 鍵交換が問題（ISAKMP？IKE？DNSSEC？）
- トランスポートモードとトンネルモード

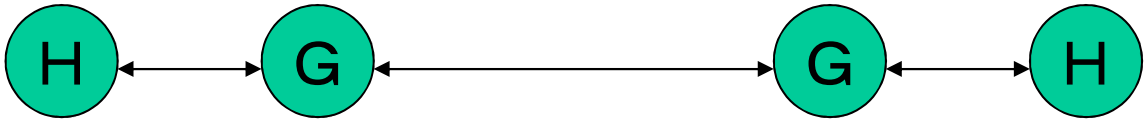
トランスポートモード

- ホスト間の通信で直接利用
- まっとうなエンドツーエンドセキュリティ



トンネルモード

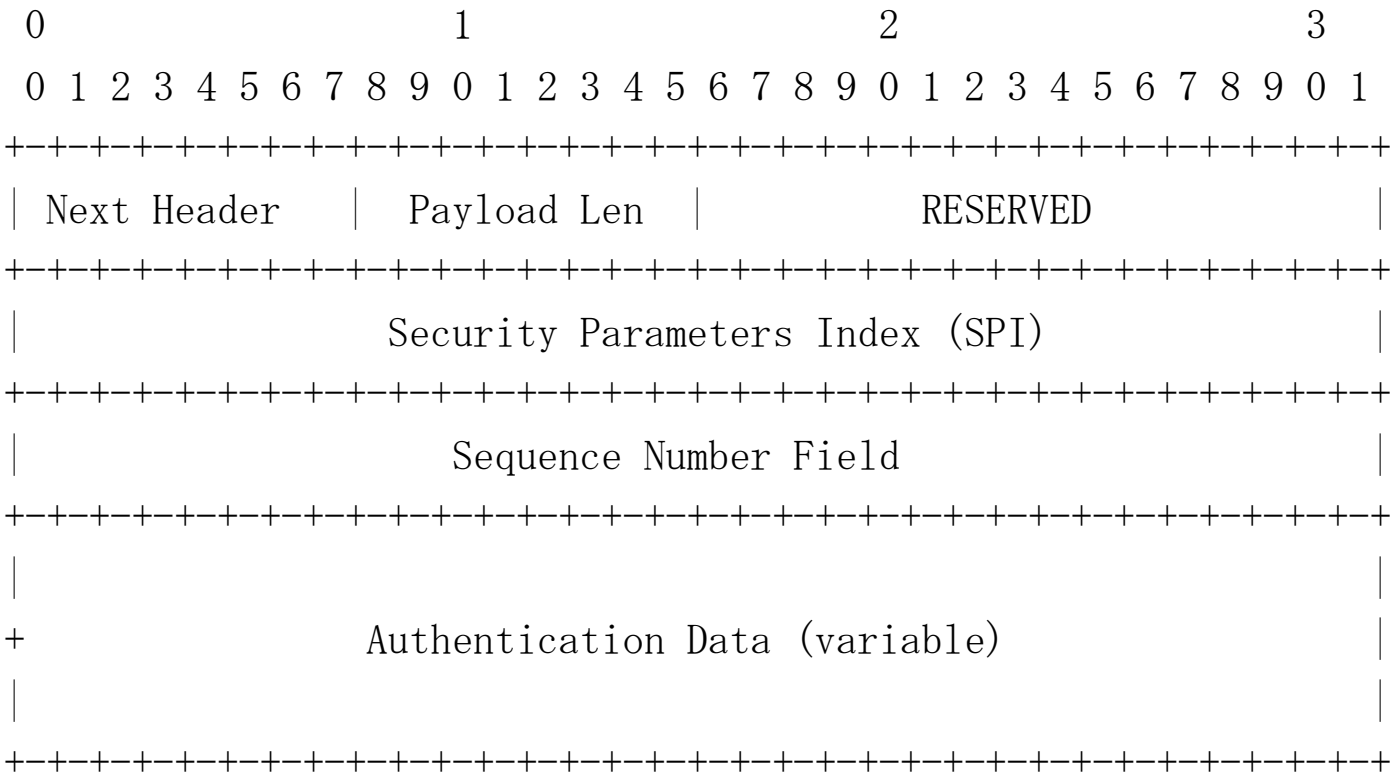
- セキュリティゲートウェイ間で利用
  - VPNでの利用？
- エンドツーエンド原理違反という以前にインターネットではない



SA （Security Association）

- セキュリティのコネクション
  - トランスポートコネクションと1対1に対応する必用はない
  - SAごとに認証や秘匿のアルゴリズムも異なる
- 単方向

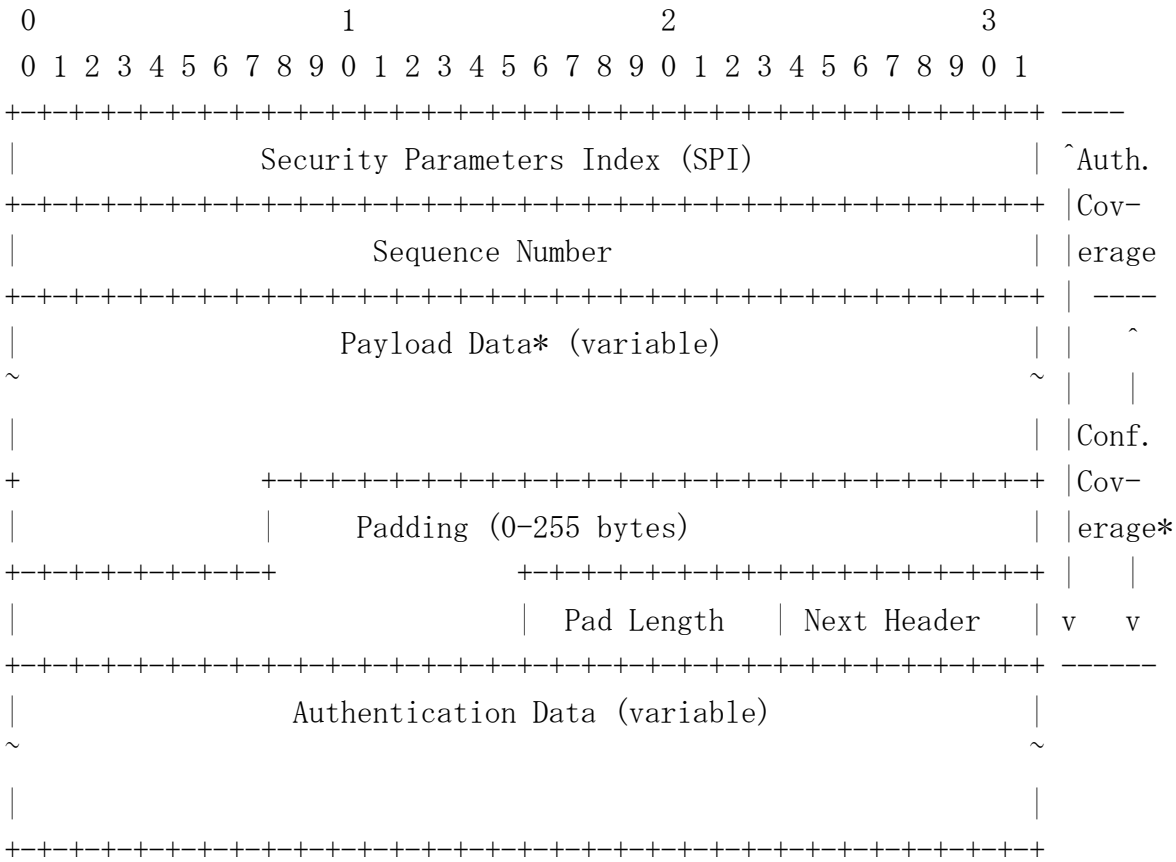
AH（Authentication Header）（RFC2402）



AHのフィールド

- SPI
  - 目的地IPアドレスとともにSAを識別
- SEQUENCE　NUMBER
  - リプレイ攻撃を防止
- AUTHENTICATION　DATA
  - パケット内容と共有秘密からのハッシュ

ESP（Encapsulating Security Payload）（RFC2406）



ISKAMP（Internet Security Association and Key Management Protocol）（RFC2408）

- 鍵交換の枠組み
- 公開鍵をベース
- SAの管理
- キーの生成
- DOS攻撃の防止
- リプレイ攻撃の防止

IKE（The Internet Key Exchange）（RFC2409）

- 実際の鍵交換方式
- 公開鍵をベース
- SAの管理
- キーの生成
- DOS攻撃の防止
- リプレイ攻撃の防止

SECURE DNS（RFC2535）

- DNSに本当のセキュリティ（認証）を
  - 通常のDNSは、WEAKLY SECURE
- 公開鍵暗号の木構造とゾーンの木構造を対応づけ
  - ルートゾーンの公開鍵を共有
  - 親のゾーンの公開鍵で、子のゾーンの公開鍵の認証を順次確認
    - DNSの階層と認証の階層が一致していれば有用

IPSECの実状

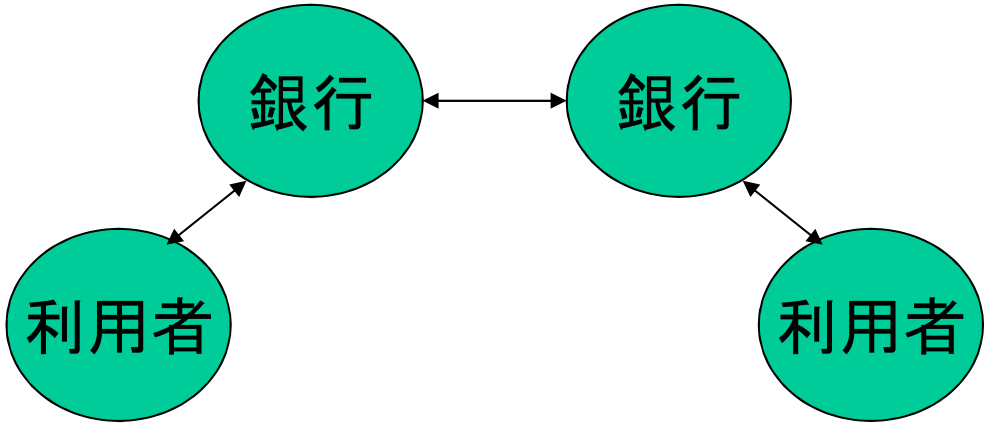
- ESPだけあれば十分で、AHは余計？
- 鍵交換は手作業
  - ISKAMPは複雑すぎ
    - あまりに汎用
  - DNSSECも複雑すぎ
    - DNSとの親和性が極端に悪い
- 個別プロトコルの個別セキュリティは根強く使われている

そもそも公開鍵暗号系は無意味では？

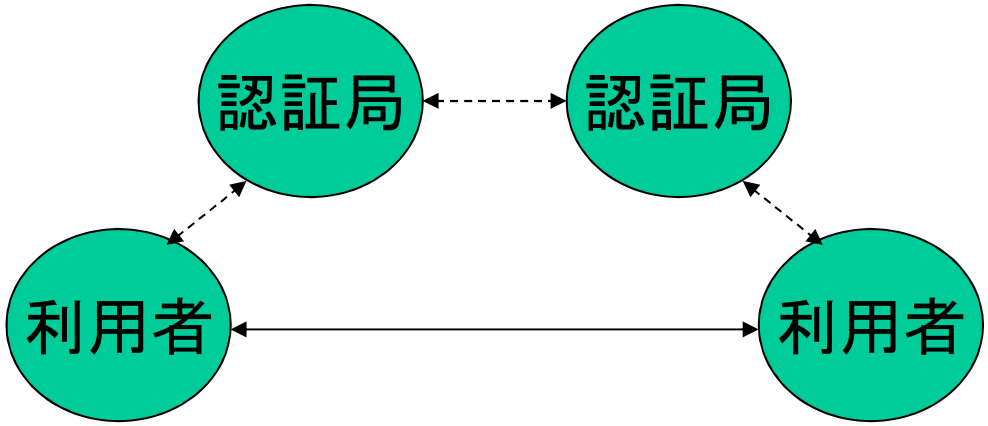
- 共有鍵の数（N^2）は問題ではない
- 共有鍵暗号系でも鍵配布局を利用すれば認証局と同様のことが可能
  - ただし、鍵配布のたびに通信は必要
    - インターネットでは通信は無料
    - どのみち何かやるには通信は必要
- 信頼できる認証局を誰が運用するのか？
  - ISPは信用できないのに、認証局は信用？

電子決済を考えてみると、、、

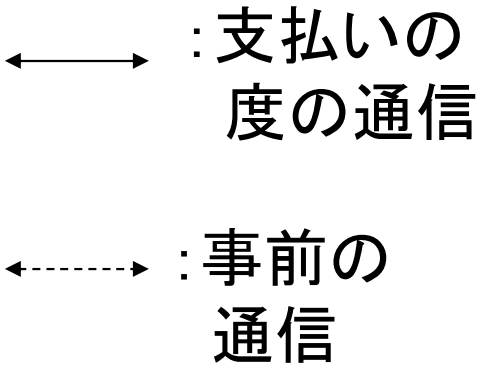
- 通信には遅れと誤りがつきもの
  - 分散システムでは「正確に1度」は保証できず
  - 不払い、二重払いの防止のためには、信頼できる仲介者（銀行）は必要
- 決済のたびに銀行と通信が必要
- 公開鍵暗号系で通信なしに決済すると
  - 事故がおきたとき誰も責任をとれない
  - 預金残高証明書で相手を安心させるのと同じ



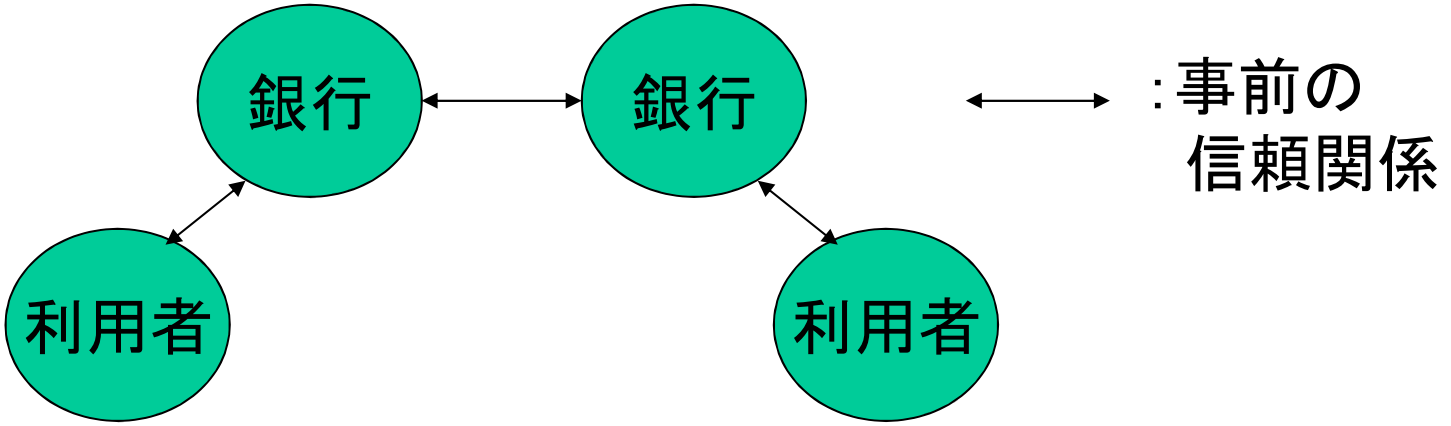
銀行を利用した決済



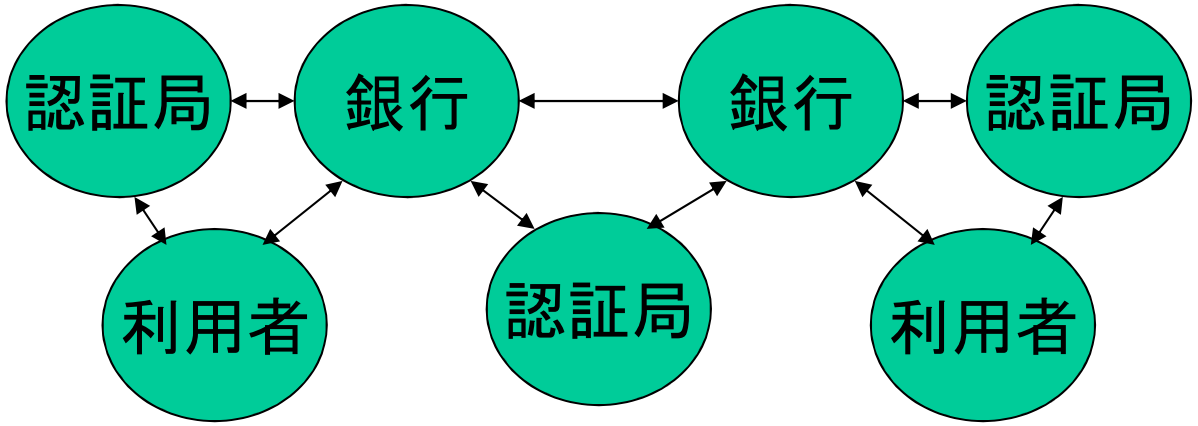
認証局を利用した決済



電子決済の様子



銀行を利用した決済（信頼関係にもとづき鍵を共有）



銀行と認証局を利用した決済（必要な信頼関係が増えるだけ）

銀行と認証局の併用？

消費される信用に関する認証への公開鍵暗号基盤の無意味性

太田昌孝
東京工業大学情報理工学研究科
mohta@necom830.hpcl.titech.ac.jp

PKIの三つの大きな問題点

- PKIは信用残の保証には使えない
  - 取引毎の信用残の確認と更新が必要
    - 共有鍵に比べての利点なし
- PKIは途中認証局に不正があれば危険
  - 通信は途中通信局に不正があれば危険
- たとえPK　Structureはありえても
  - PK　Structureは目的の信頼構造毎に必要
    - 汎用のPK　Infrastructureはありえない

小切手帳による古典的な詐欺

- 銀行に預金して小切手帳をもらう
- 小切手帳を利用して以下を繰り返す
  - （小額の）買い物を行う
  - 商品を古物商等に転売して換金
- ばれる前にどろん
- 換金合計金額が預金残高を超えたら成功

小切手帳による古典的な詐欺への防衛手段

- 気休め（犯罪のコストを増加）
  - 小切手帳をなかなか発行しない（日本）
  - 古物商での身分証明の要求
- 本質的（犯罪の利益、被害を限定）
  - 小切手帳の枚数は有限
  - 店にリスクを負わせる
    - （高額の買い物では）店が銀行に口座残高を問い合わせ

クレジットカードによる古典的な詐欺

- クレジットカードを入手
- クレジットカードを利用して以下を繰り返す
  - （小額の）買い物を行う
  - 商品を古物商等に転売して換金
- ばれる前にどろん
- 換金合計金額がクレジットカード入手コストを超えたら成功

クレジットカードによる古典的な詐欺への防衛手段

- 気休め（犯罪のコストを増加）
  - クレジットカード発行時の身分証明の要求
  - 古物商での身分証明の要求
  - クレジットカードは１枚だけ（偽造は困難）
- 本質的（犯罪の利益、被害を限定）
  - 店にリスクを負わせる
    - 店がカード会社に口座残高を問い合わせ
      - 小額の買い物はクレジットカード利用不可
      - 中額の換金困難な商品では問い合わせ省略可

共有鍵暗号

- 関係者が秘密鍵を「安全に」共有
- Ｎ人の間の直接的相互認証には
  - 事前にＮ＊（Ｎ－１）／２の「安全な」鍵共有が必要
  - Ｎが大きいと現実的ではない
- Ｎ人でKDC（鍵配布局）を共有すれば
  - 事前にはKDCとのＮの鍵共有しか必要でない
  - 取引の際にKDC経由でセッション鍵を共有
- KDCの階層化も可能

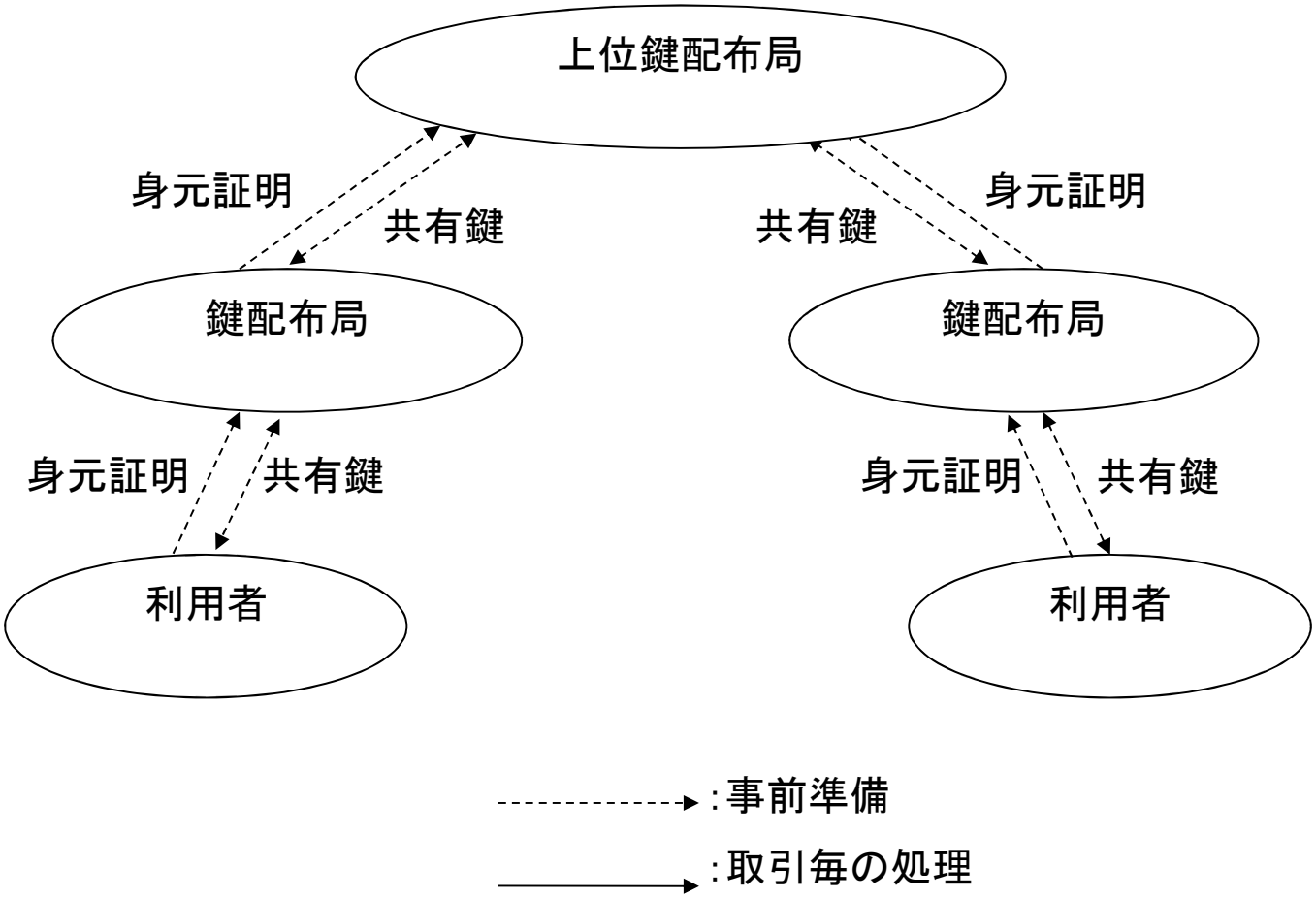


図2　共有鍵暗号と鍵配布局（事前準備）

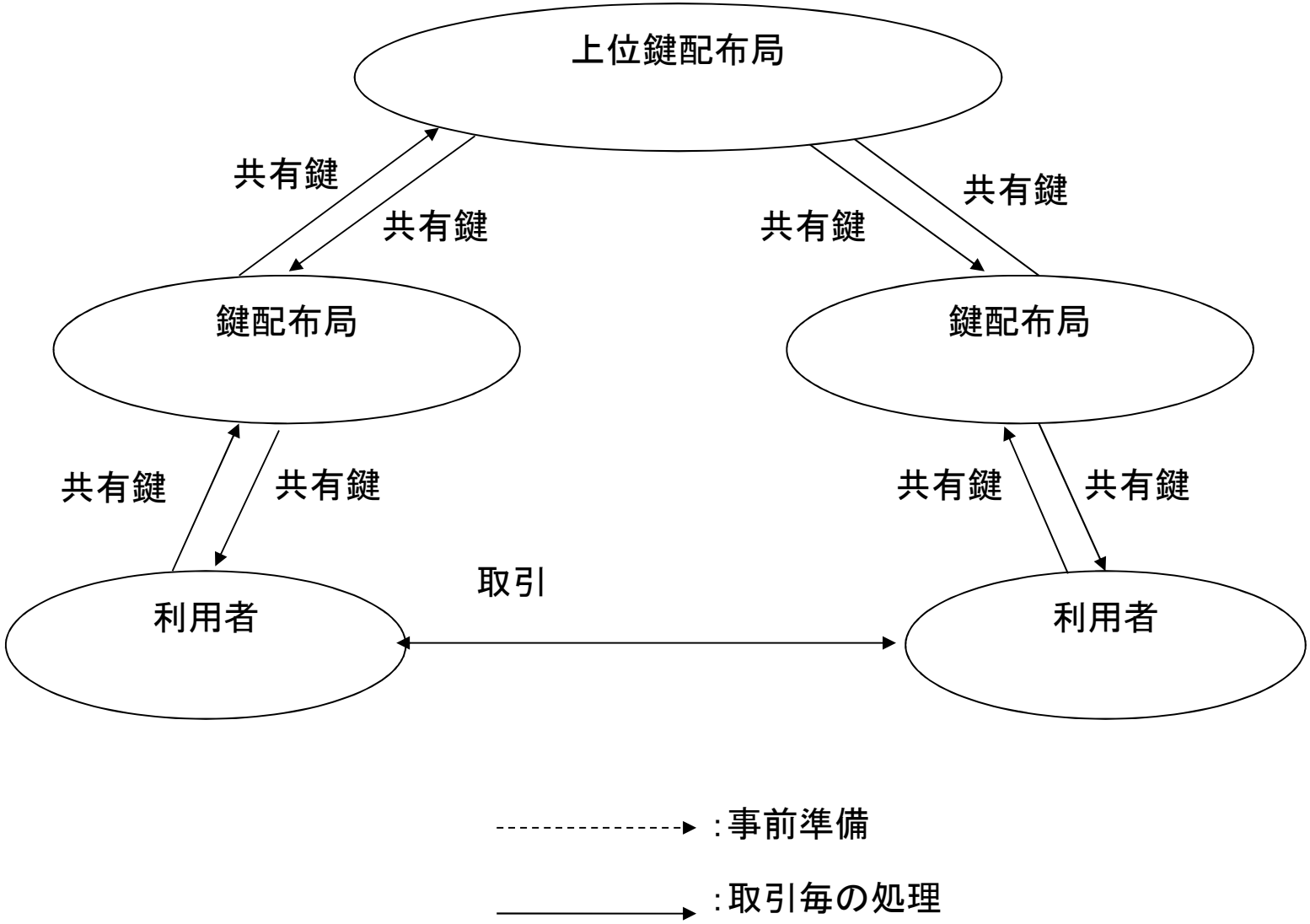


図3　共有鍵暗号と鍵配布局（取引毎）

公開鍵暗号（１）

- 関係者の一方は秘密鍵を保有
  - 公開鍵は全関係者で「安全に」共有
- Ｎ人の間の直接的相互認証には
  - 公開鍵、秘密鍵はN個でよい
  - 公開鍵の「安全な」共有には
    - 事前にＮ＊（Ｎ－１）回の「安全な」鍵配送が必要
    - 事前にN回の「安全な」鍵放送でもよい
  - Ｎが大きいと現実的ではない

公開鍵暗号（２）

- Ｎ人でCA（認証局）を共有すれば
  - 事前にはCAの公開鍵の共有と、CAによるNの鍵への署名しか必要でない
  - 取引の際にはCAの証明書によりセッション鍵を共有
    - CAの介在は不要
- CAの階層化も可能
- 効率的計算には共有セッション鍵を利用
  - セッション鍵の数は共有鍵の場合と同じ

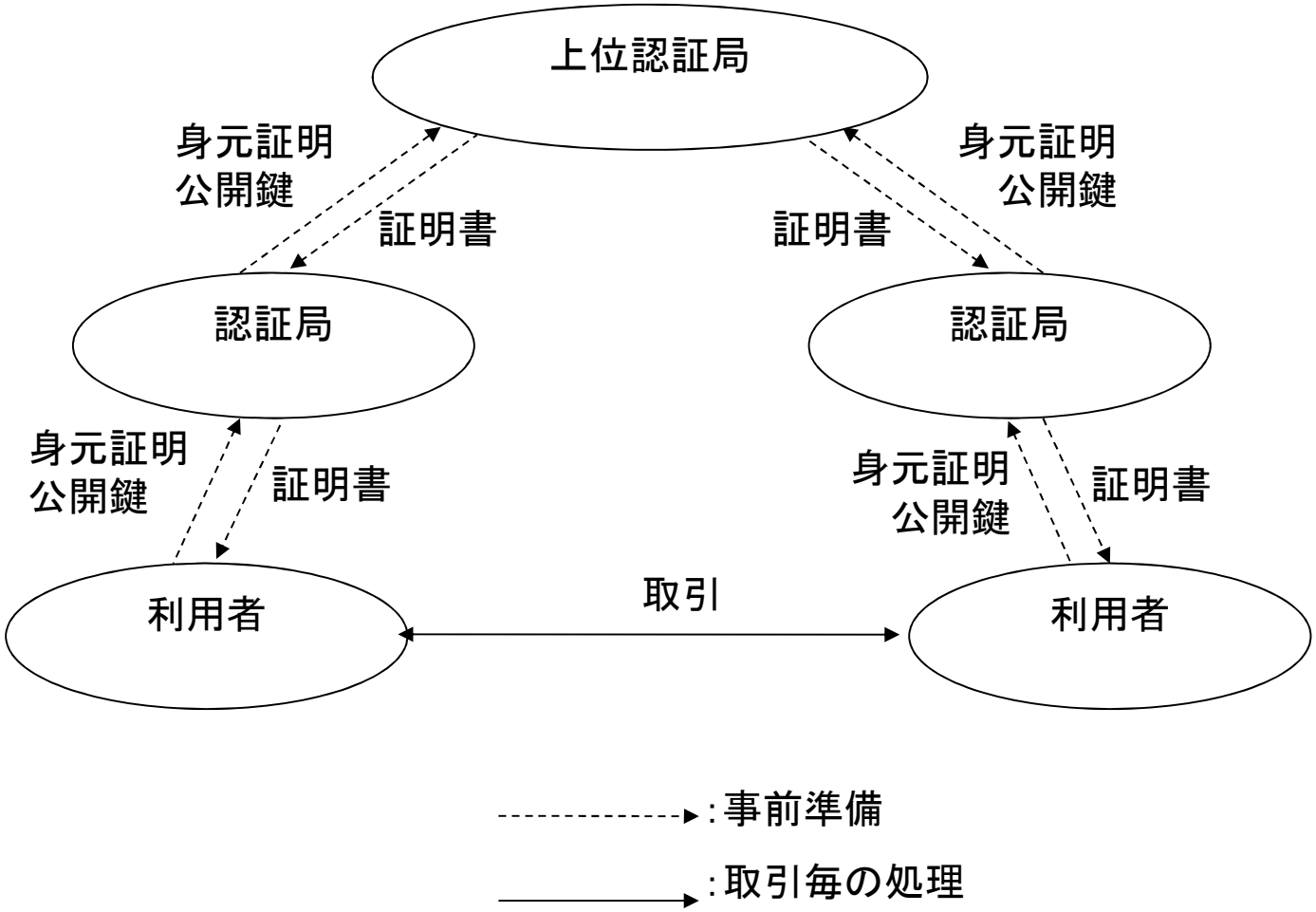


図1　公開鍵暗号と認証局

公開鍵による信用残への証明書を利用した詐欺

- 認証局から信用残の証明書をもらう
- 証明書を利用して以下を繰り返す
  - （小額の）買い物を（電子的に）を行う
  - 商品を古物商等に（電子的に）転売して換金
- ばれる前にどろん
- 換金合計金額が証明書取得コストを超えたら成功

公開鍵による信用残への証明書を利用した詐欺の特徴

- 証明書はいくらでもコピー可能
- 取引は電子的
- 取引回数には制約がほとんどない
- 千箇所から千秒間、秒千回の百万円の買い物をすると、取引総額は千兆円
  - 千箇所から千秒間、秒千回の千円の買い物をしても、取引総額は一兆円
    - CRLによる取消では手遅れ

公開鍵による信用残への証明書を利用した詐欺への防衛手段

- 気休め（犯罪のコストを増加）
  - 証明書発行時の身分証明の要求
  - 古物商での身分証明要求はPKIの自己否定
- 本質的（犯罪の利益を限定）
  - 店にリスクを負わせるだけでは無意味
  - 信用残を実時間で管理する信用局を導入
    - （いかに小額の取引でも）店が信用局に口座残高を問い合わせ
      - 換金が絶対に不可能な商品では問い合わせ省略可

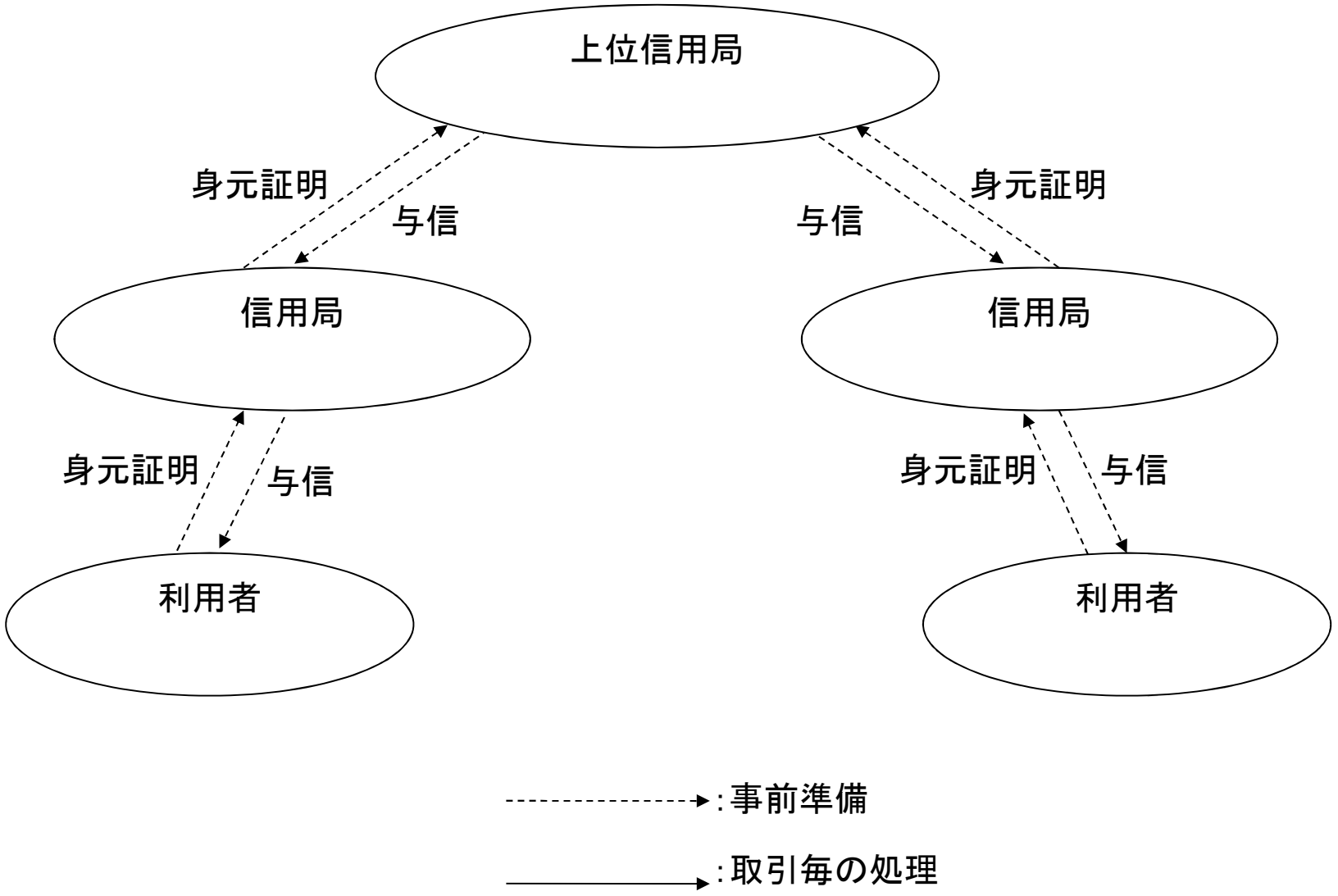


図4　信用残と信用局（事前準備）

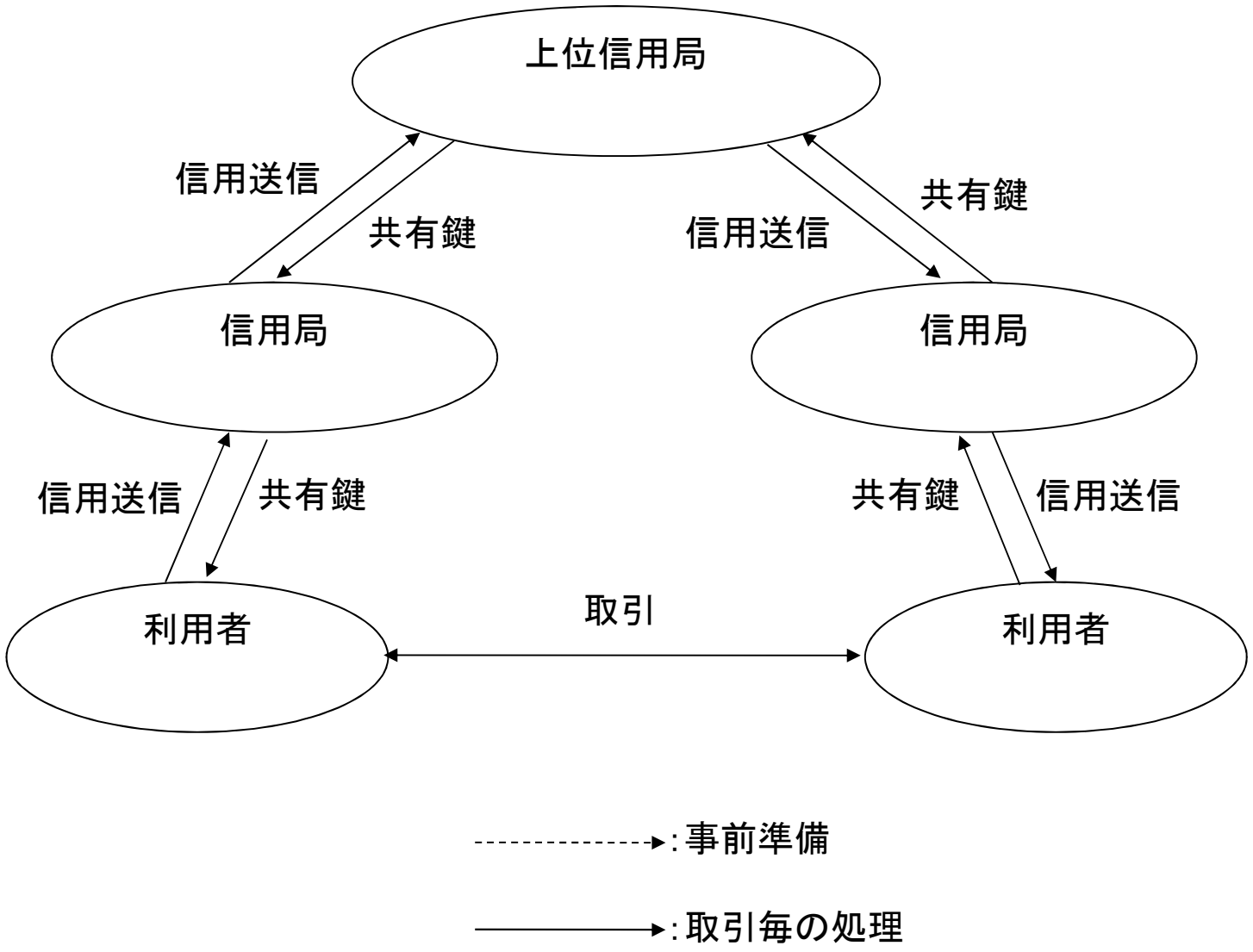


図5　信用残と信用局（取引毎）

信用局と暗号

- 信用局と信用局との通信が信頼できれば詐欺は不可能
  - 信用局は認証局、鍵配布局の役割を担う
    - 追加の認証局、鍵配布局は無意味
    - 信用局の秘密情報が漏れるとその信用局は破綻
- 信用局とは取引の都度通信が必須
  - 共有鍵暗号で十分
- 信用局の実体は銀行やカード会社
  - 消費される信用についてはPKIは無意味

WEAK SECURITY

- 第三者の提供するインフラを無条件に信頼することに基づくセキュリティ
  - ISPが信頼できれば、指定したIPアドレスの相手と通信でき、パケットの盗聴も改変もない
  - ISPがパケットの盗聴や改変をすれば破綻
- 電話網のセキュリティも、この程度
  - 電話会社が通話の盗聴や改変をすれば破綻
- （実はPKIのセキュリティも、この程度）

WEAK SECURITY

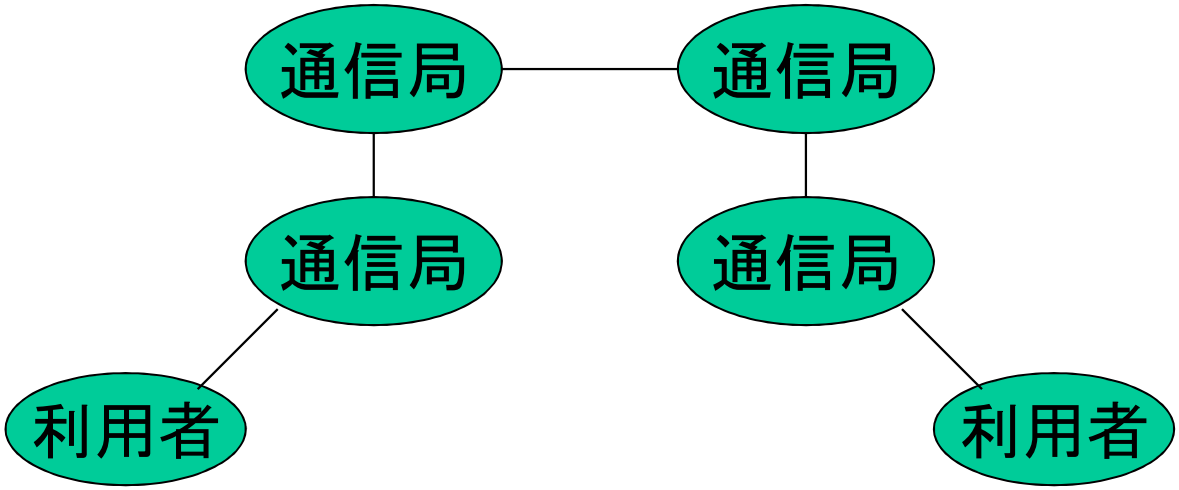
- 第三者の提供するインフラ（PKI）を無条件に信頼することに基づくセキュリティ
  - 認証局が信頼できれば、認証局に署名された相手の証明書も信頼でき、証明書の偽造もない
  - 認証局が証明書の偽造をすれば破綻
- PKIのセキュリティは、この程度

DH（Diffie-Hellman）鍵交換

- 大きな素数pを法として計算、通信相手が互いにmを共有し、乱数a、bを生成
- m^aとm^bを交換（盗聴可能）
  - m^aからaを求めるのは、至難（離散対数）
- （m^a）^b＝（m^b）^aが共有秘密鍵
- もちろん、完璧ではない
  - 能動的Man in the Middle攻撃に弱い

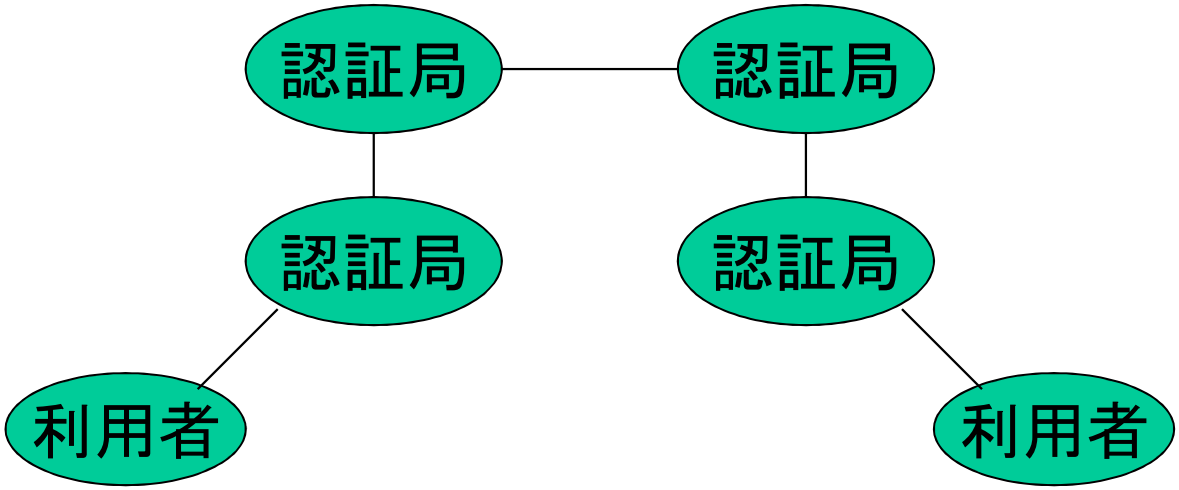
MitM（Man in the Middle）による攻撃

- 中間通信局等による通信の傍受、改変、捏造により、平文パスワード、DHは破綻
  - 通信が安全なら暗号技術によるセキュリティはそもそも不要



MitM（Man in the Middle）によるPKIへの攻撃

- 中間認証局等による証明書の改変、捏造
  - 認証局も通信局も同程度に信用すべきはず
  - 証明書が安全でないなら暗号技術によるセキュリティは無意味



MitM攻撃を防ぐために

- 第三者には頼らない
  - 第三者に頼るのは、エンドツーエンド原理違反
- 第一者もしくは第二者が運用する（ISP、認証局）のみを利用する
  - 認証局の場合、第一者と第二者の間で直接（エンドツーエンド）の鍵交換が必要
    - N:NならN^2の鍵交換が必要
    - 公開鍵暗号を利用する意味はない

公開鍵暗号は有用？

- PKIはあまり使いものにならない
- 公開鍵は計算が遅く、また不安
  - 秘密鍵から公開鍵が計算可能になるかも
- 消費されない信用への証明？
  - 消費される信用へ転換可能だと同じこと
    - そうできないはずの証明でも、電子的証明は危険
- 非対称性の利用？
  - 放送コンテンツの認証？

信用とエンドツーエンド原理

- 暗号は信用を運ぶための道具にすぎない
  - 信用とは、例えば与信限度額
- 信用は一対一で形成される
  - 同時に共有鍵の交換が可能
  - 認証局は信用を提供しない
  - 認証局は中間にある無用の長物
- 信用するエンド同士が直接秘密鍵を共有するのが、インターネットのあるべき姿

まとめ

- インターネットは既に電話網なみに安全
- エンドツーエンドセキュリティこそ肝要
  - ホストやアプリケーション単位のセキュリティ
- IPSEC（AH、ESP）
  - セキュリティの標準フォーマット？
- DNSSEC
  - DNSの認証は、それ自体は有用？
- PKIはエンドツーエンド原理違反