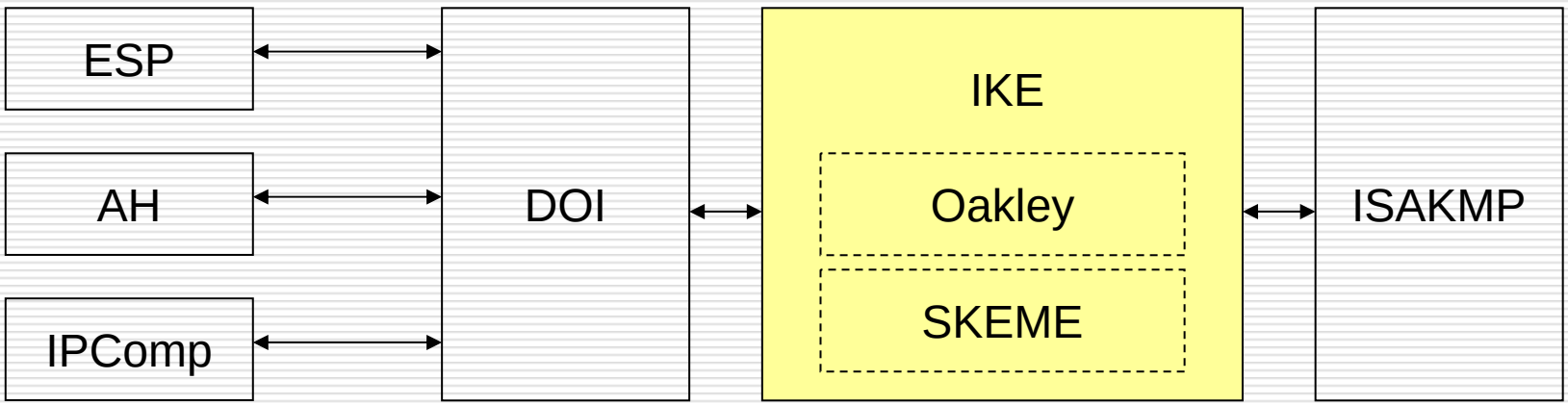
通信プロトコルの認証技術

- 「PKIを使用するプロトコルでのモデル紹介」
  - IPsec/SSLの現状、動向、および課題
  - IETFでの技術動向
- まとめ＆考察

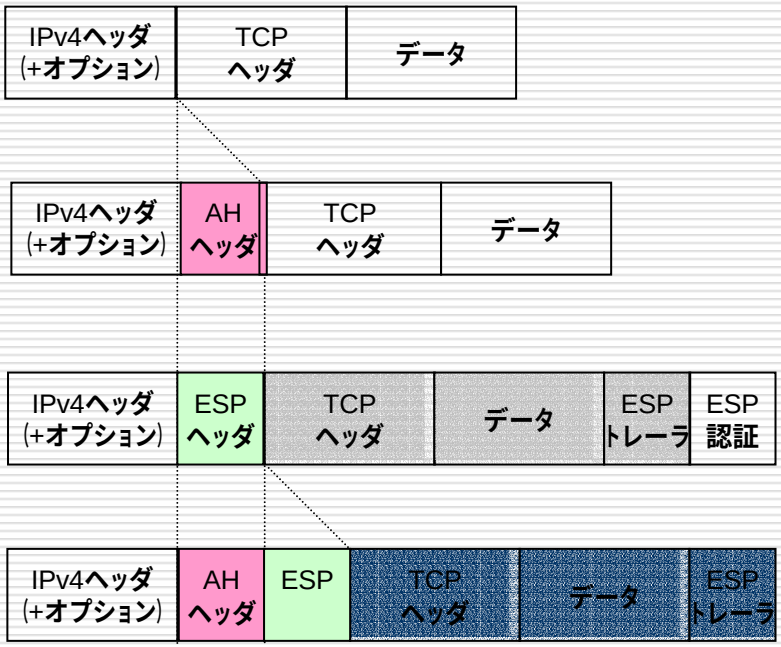
松下電工株式会社　新事業企画室
福田　尚弘　(http://www.netcocoon.com)
2004.12.9

IPsecの概要

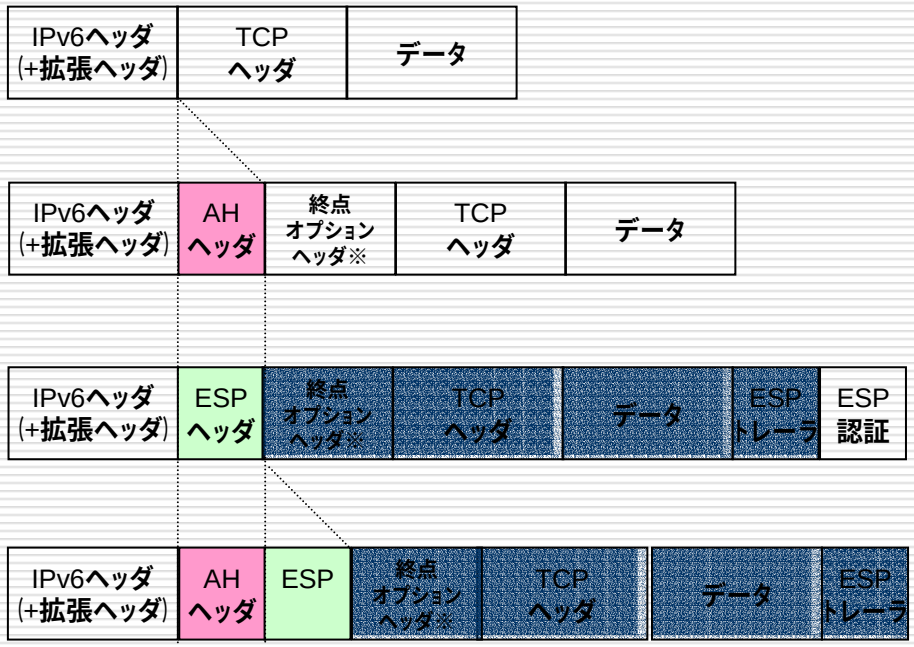
- ESP,AH,IPComp：暗号化、認証、圧縮のペイロード
- DOI：SAで使用されるパラメータの定義
- IKE：SAと鍵管理を行うためのプロトコル
- ISAKMP：IKEのプロトコル・フレームワーク



IPsecの概要
～トランスポートモードのヘッダ構成～



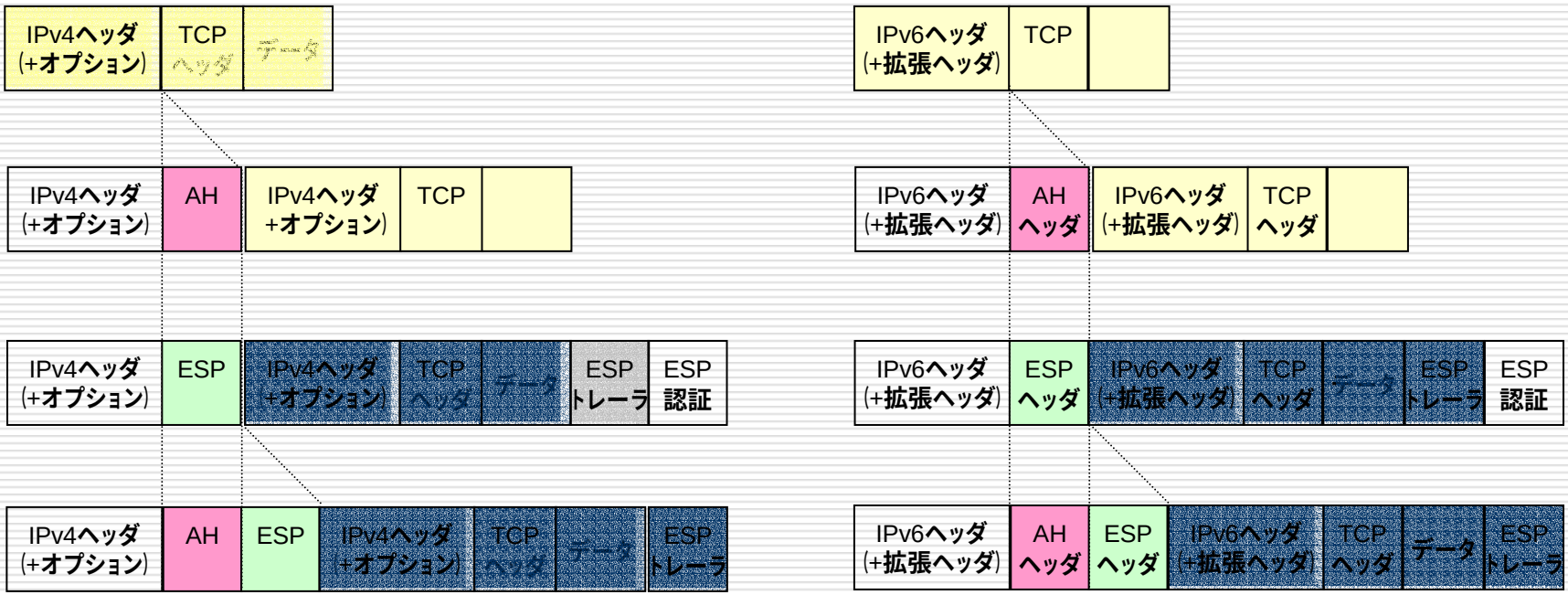
IPv4の場合



IPv6の場合

圧縮ヘッダ (IPComp) はAHのみではAHの後に、ESPがあればESPの後に位置する
※拡張ヘッダの終点オプションヘッダはセキュリティヘッダの内側または外側のどちらでもよいが、内側が推奨である。

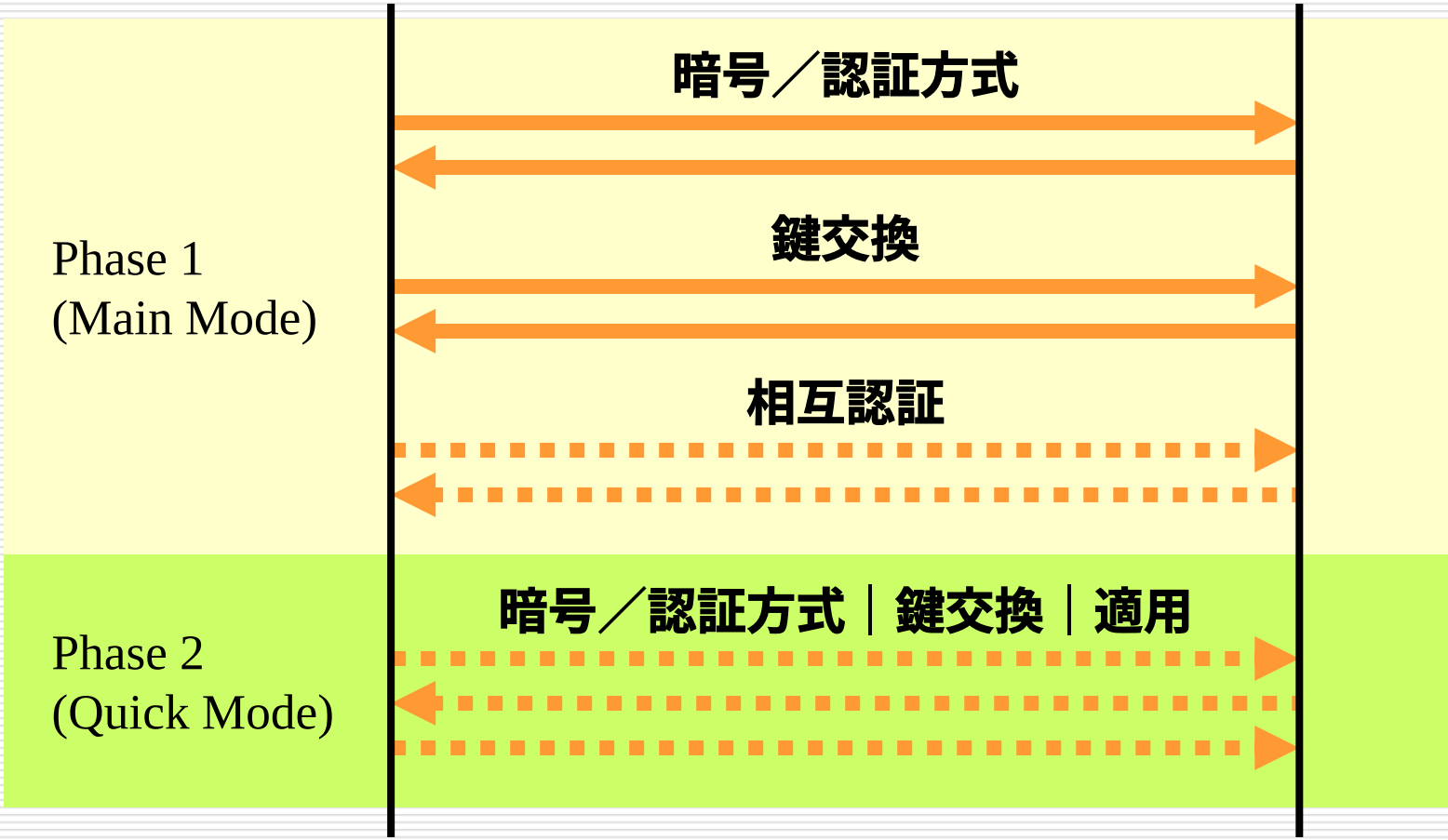
IPsecの概要
～トンネルポートモードのヘッダ構成～



IPv4の場合　　IPv6の場合

圧縮ヘッダ (IPComp) はAHのみではAHの後に、ESPがあればESPの後に位置する

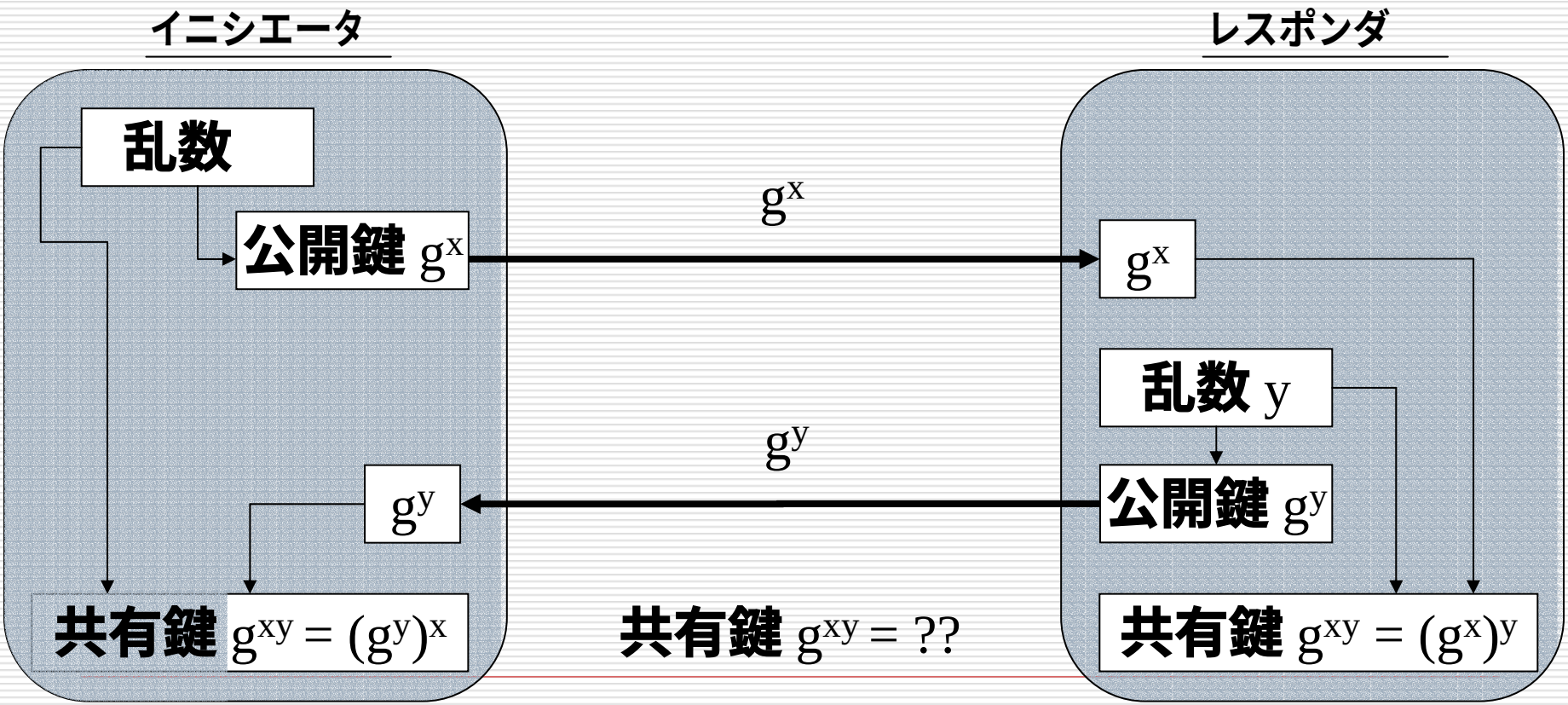
IPsecの概要
～IKEの手順～



注：実線は平文、点線は暗号化

IPsecの概要

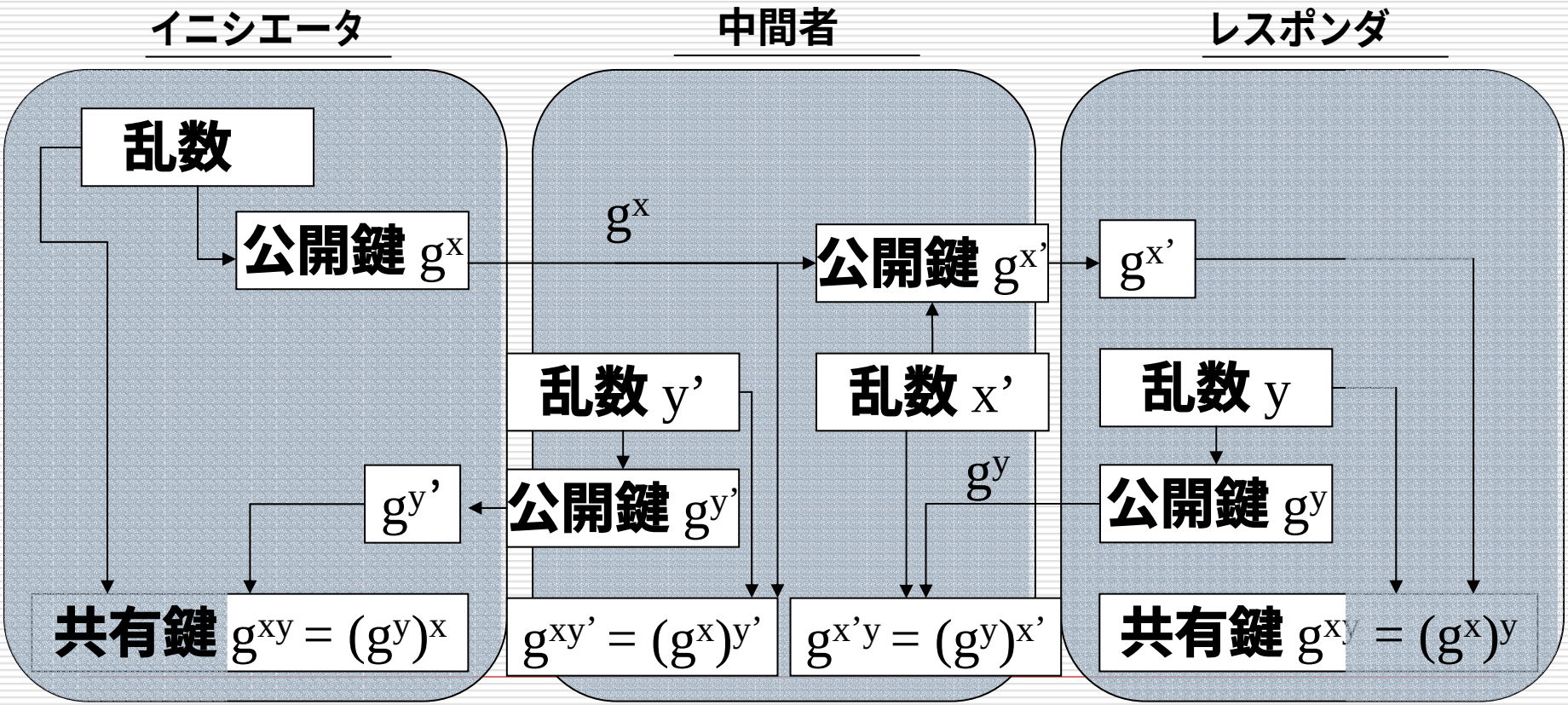
- DH(Diffie-Hellman)



注：ここでは「mod p」計算を省略

IPsecの概要

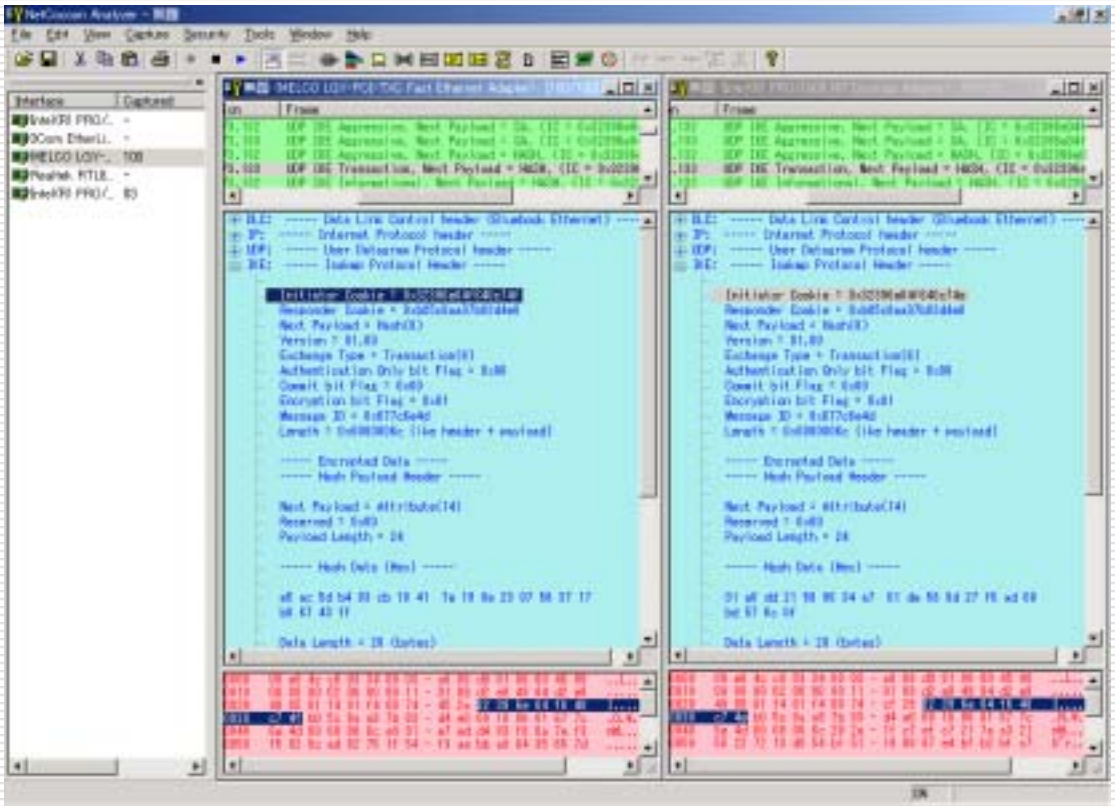
- Man-in-the-Middle for DH



注：ここでは「mod p」計算を省略

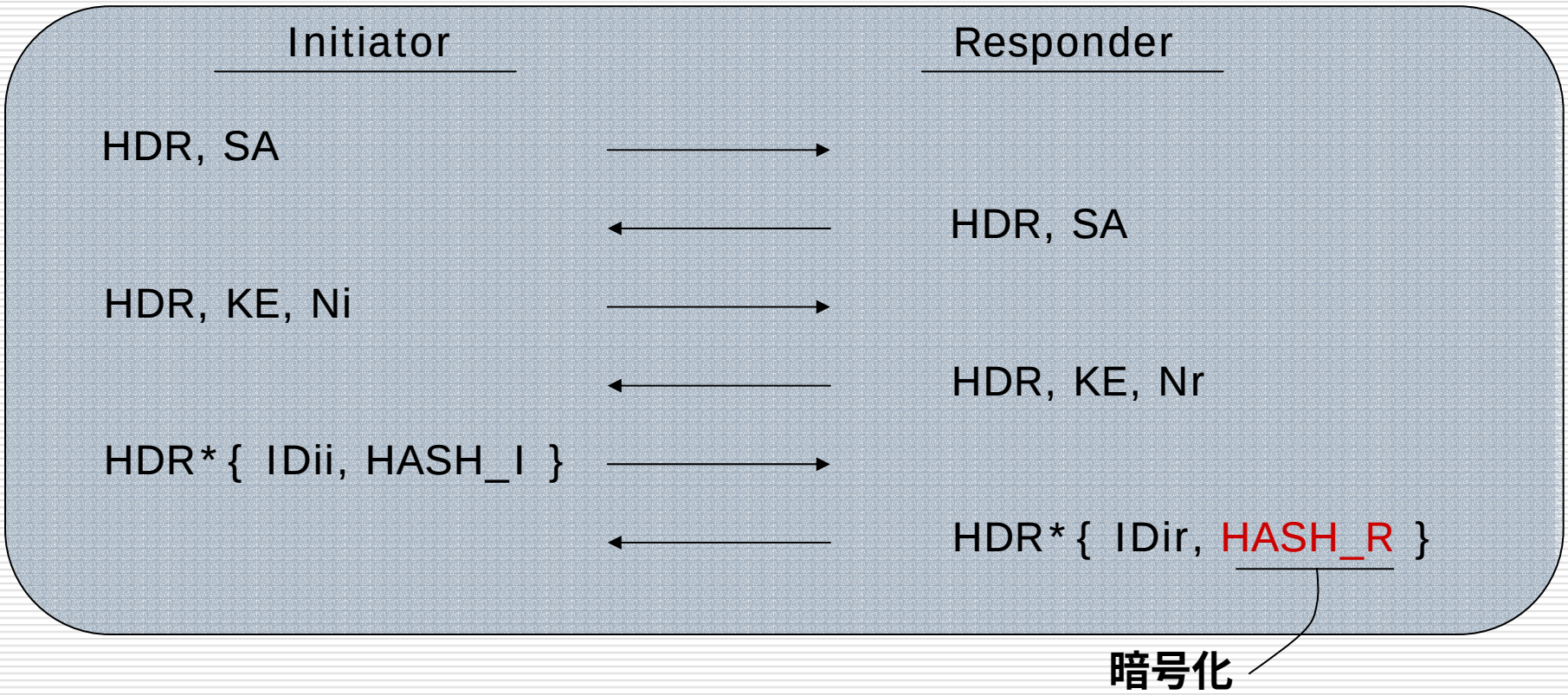
IPsecの解析例

- NetCocoon Analyzerの例



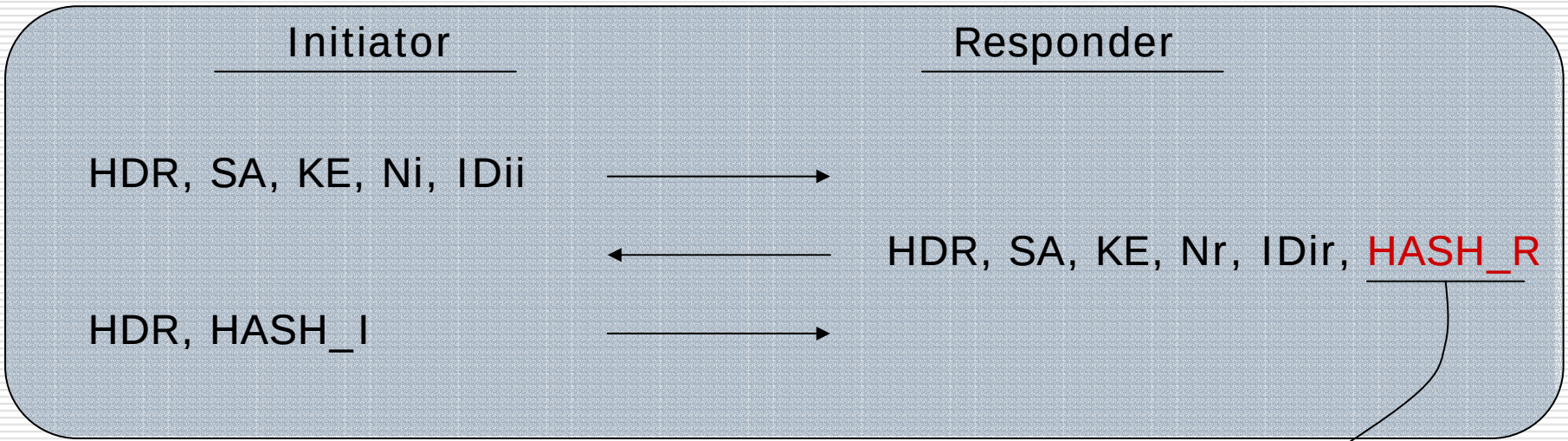
IPsecのMain Mode

Pre-shared keyのMain Mode:



IPsecのAggressive Modeの危険性

Pre-shared keyのAggressive Mode:



SKEYID = prf(*pre-shared-key*, Ni_b | Nr_b)

ハッカーが知りたいもの

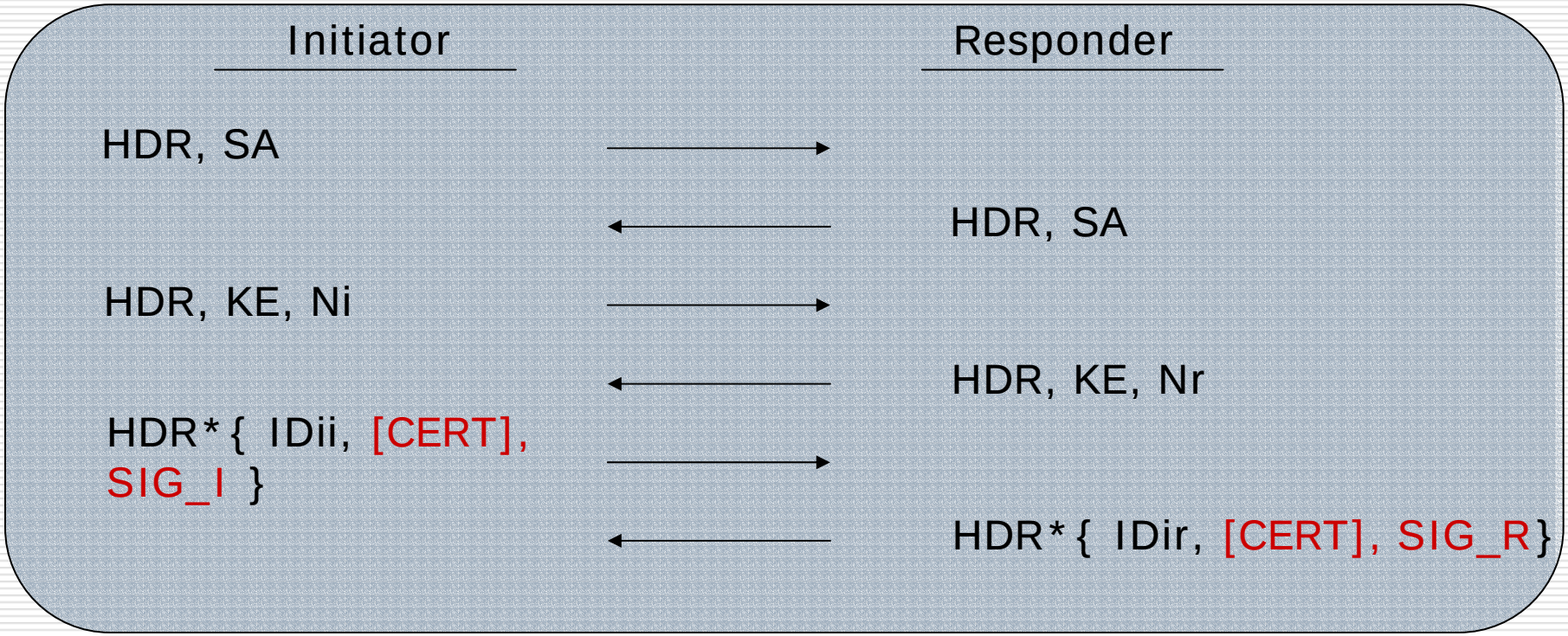
非暗号（機知）

HASH_R = prf(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b)

機知

IPsecのMain Mode (2)

SignatureのMain Mode:



注：SIG_x = Sign (HASH_x)

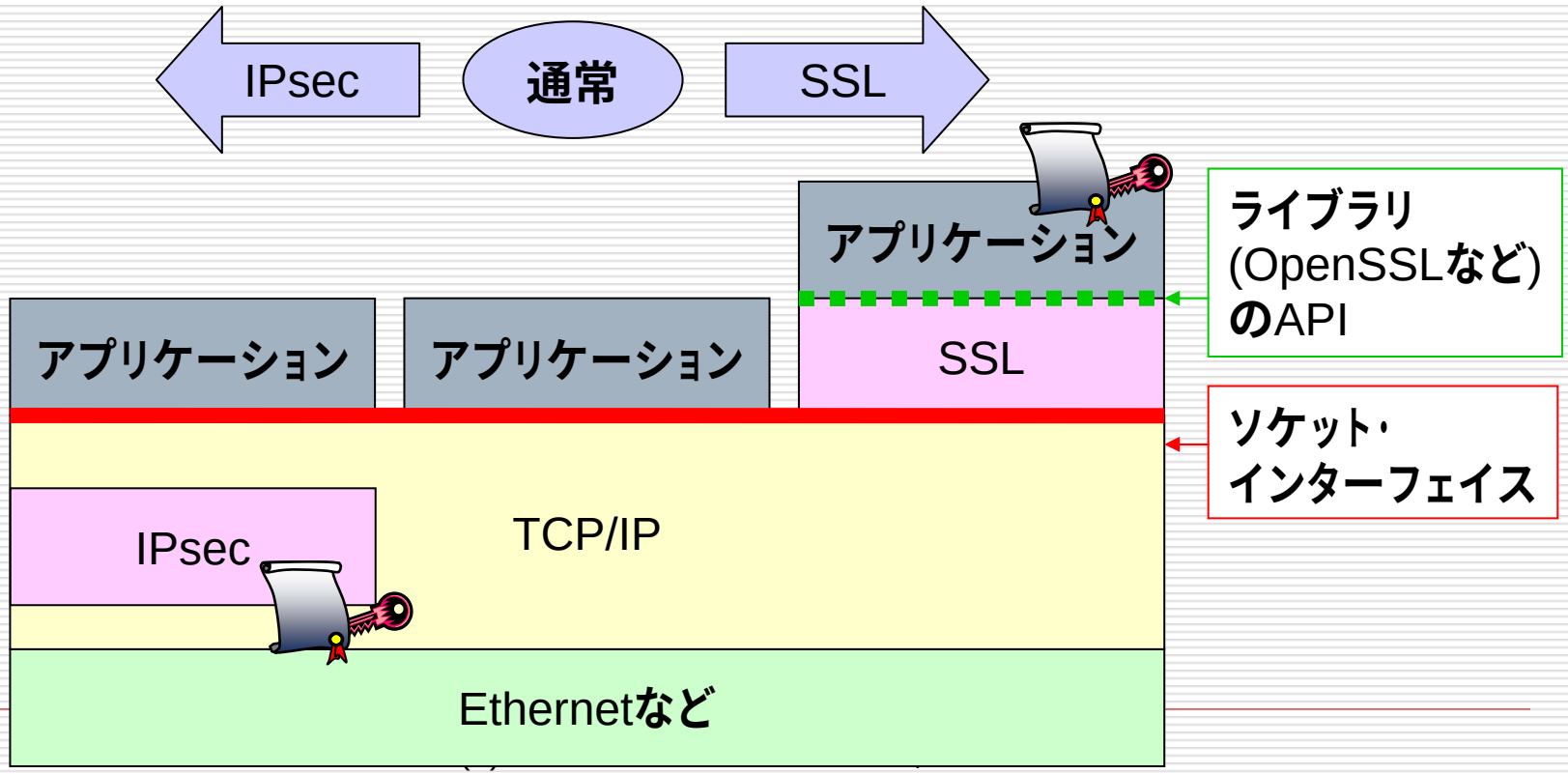
IPsecと認証

- 個人、小規模 (プリシェアード)
  - プリシェアードに対応した鍵管理
- 中規模・大規模 (証明書)
  - プライベートCAで費用を抑える？
  - 簡単な証明書のシステム？
- IPsec-VPN:拠点間
  - リモートアクセスにはX-auth、Mode-Configが必要
  - Aggressive Modeは避ける
- SSL-VPN:リモートアクセス
  - NAPT越えで有利。IPsecではNAT-Tが必要。

SSL/TLSの概要 ～IPsecとの比較～

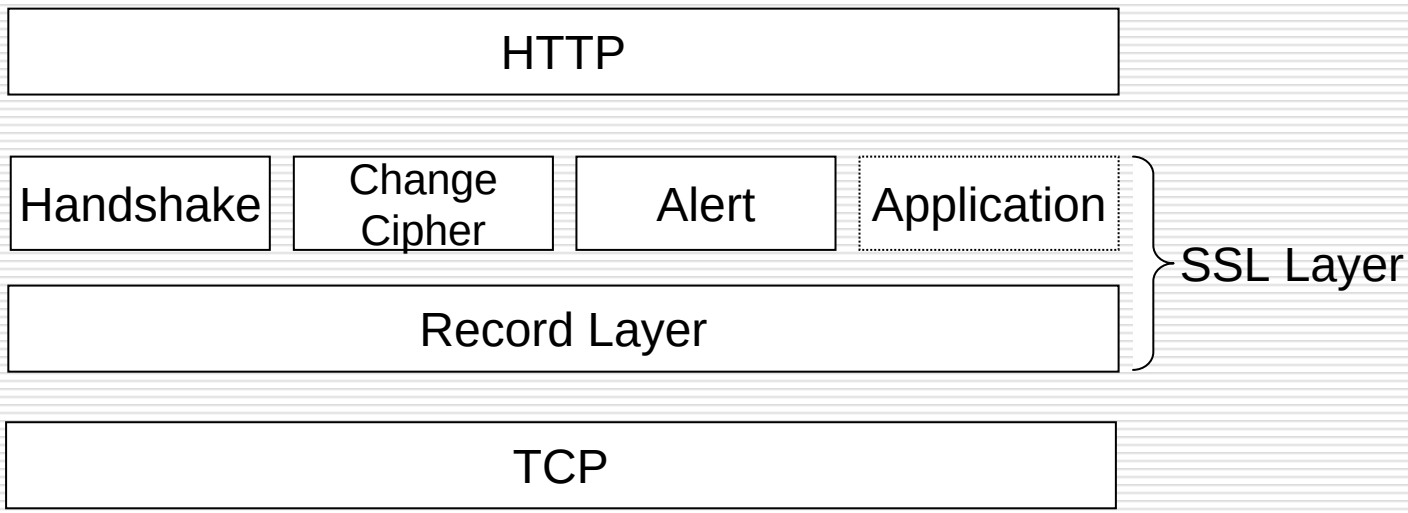
アプリケーションをそのまま使える
鍵や証明書はOSで一括管理

プログラムを書き換える必要がある
鍵や証明書はアプリケーションで管理

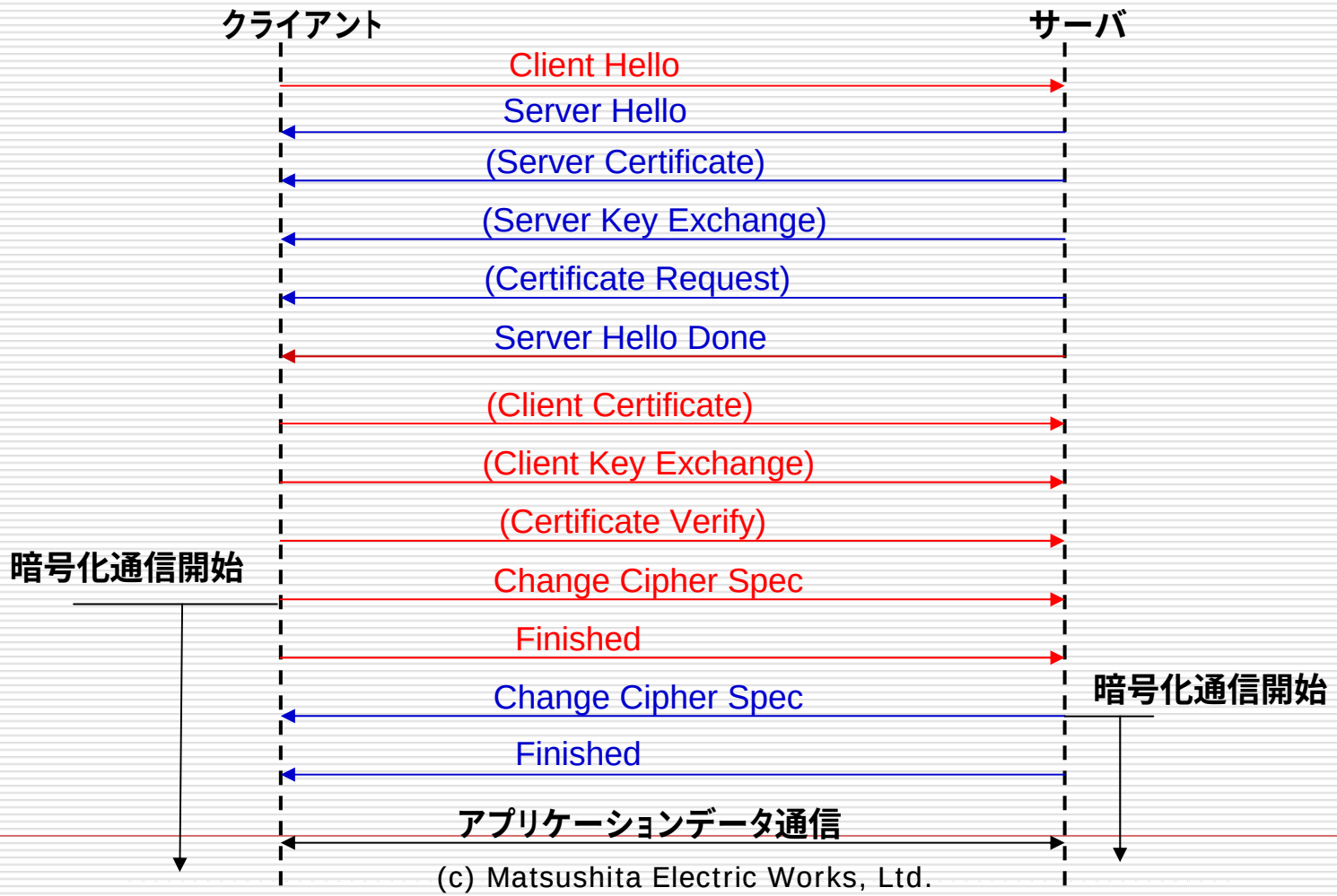


SSL/TLSの概要
～SSLのプロトコルコンポーネント～

- SSLハンドシェークプロトコル
  - 正当性確認（相互認証）、乱数の交換、暗号スイートの選択
- SSLチェンジサイファプロトコル
  - 暗号スイートの適用（暗号化アクティベート）
- SSLアラートプロトコル
  - 期待外のメッセージを受信した場合相手に送信する。
    （証明書がない場合、証明書が失効している場合などに送信する。）

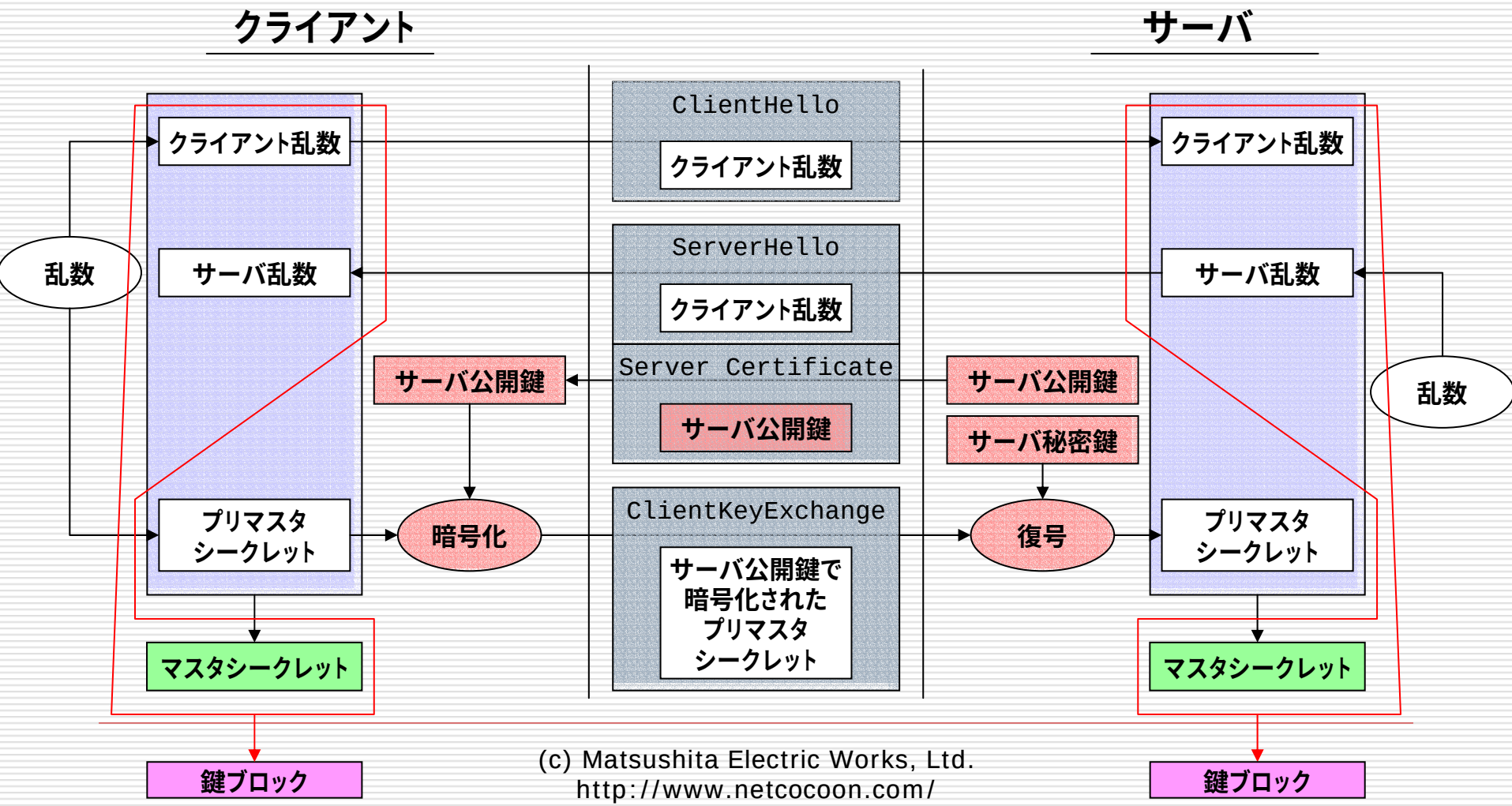


SSL/TLSの概要
～ メッセージ交換 (開始) ～



SSL/TLSの概要
～ メッセージ交換 (再開) ～

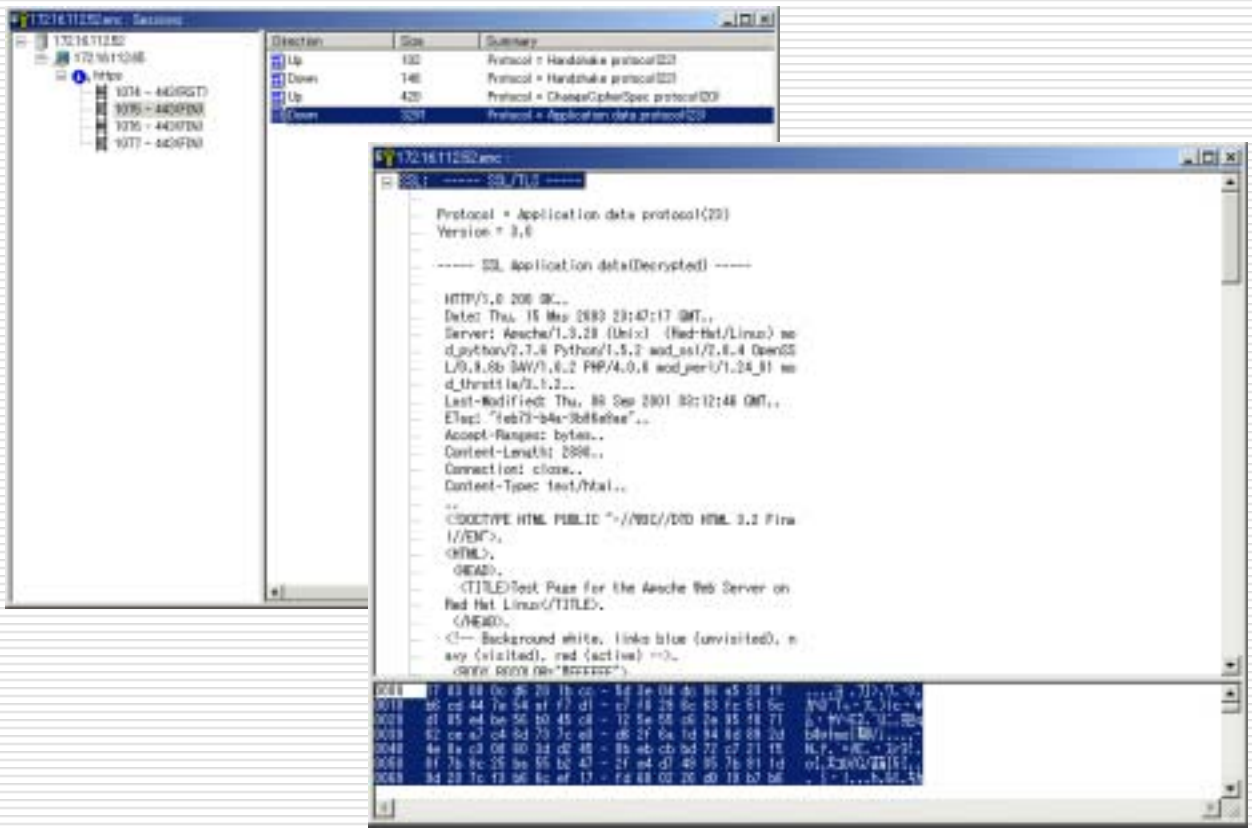
SSL/TLSの概要
～ メッセージ交換 (開始) ～



SSL/TLSの概要
～ メッセージ交換 (再開) ～

SSL/TLSの解析例

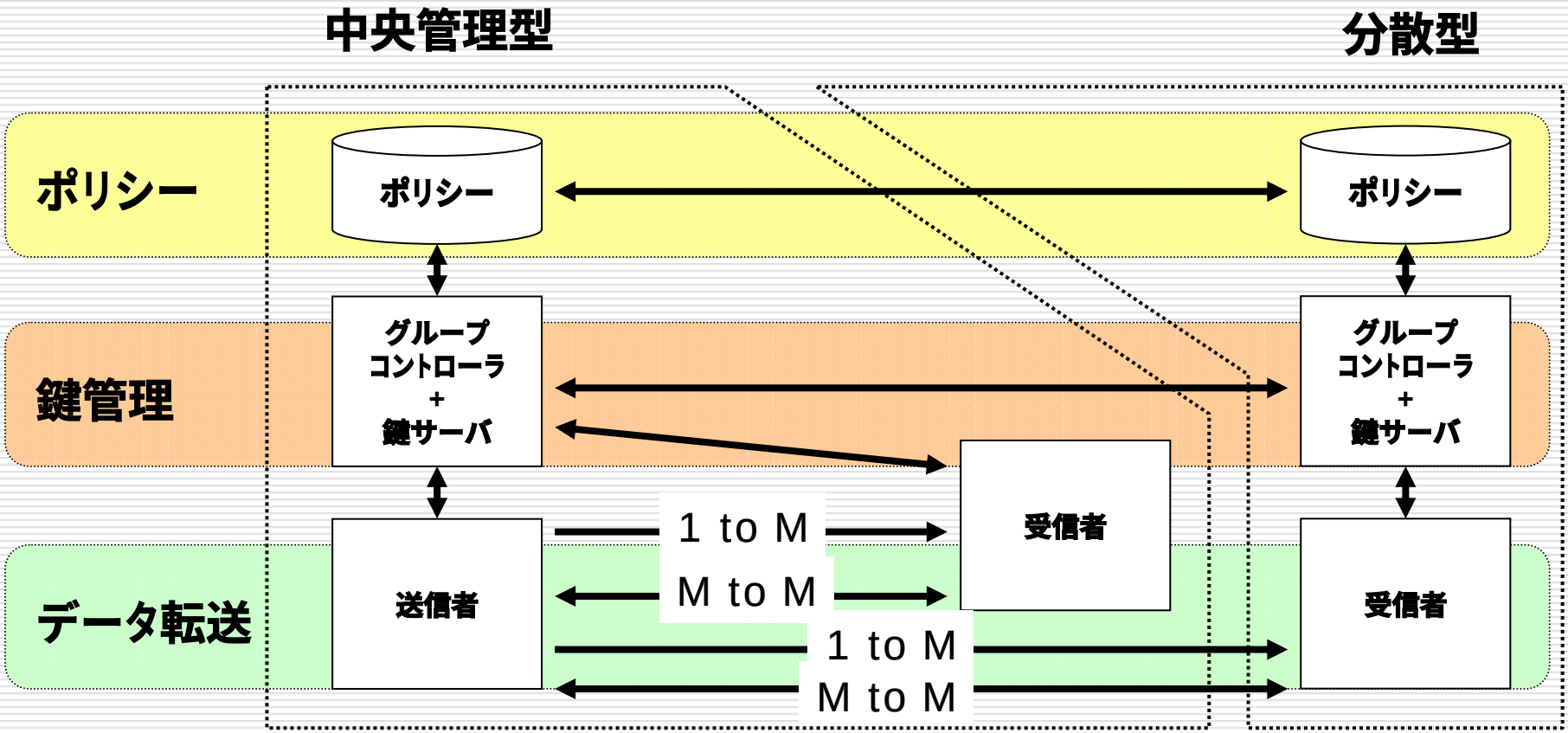
- NetCocoon Analyzerの例



SSL/TLSと認証

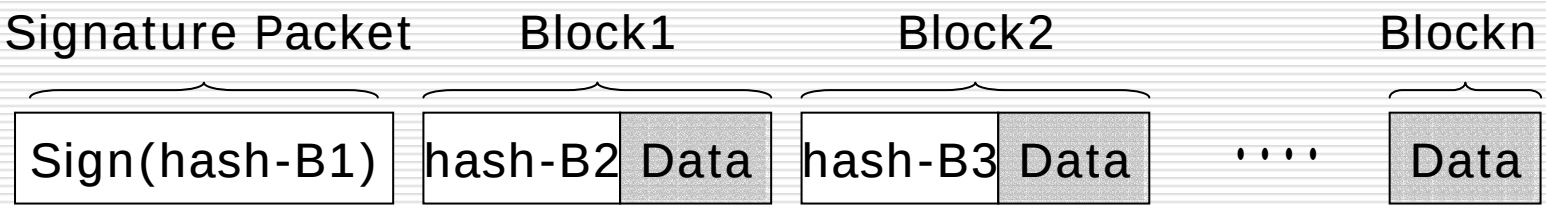
- IPsecは相互認証（EAPはクライアント認証）
- SSL/TLSはサーバ認証(基本)
- RSAを中心とした暗号プロトコル
  - ”ServerKeyExchange”メッセージで、DHやRSAのパラメターを交換する場合もある。
- ブラウザの設定が安全性の鍵
- フィッシング→サーバ証明書の確認が重要
  - 証明書の確認は慎重に行う。

[参考] MSEC
～マルチキャスト対応のセキュリティ～

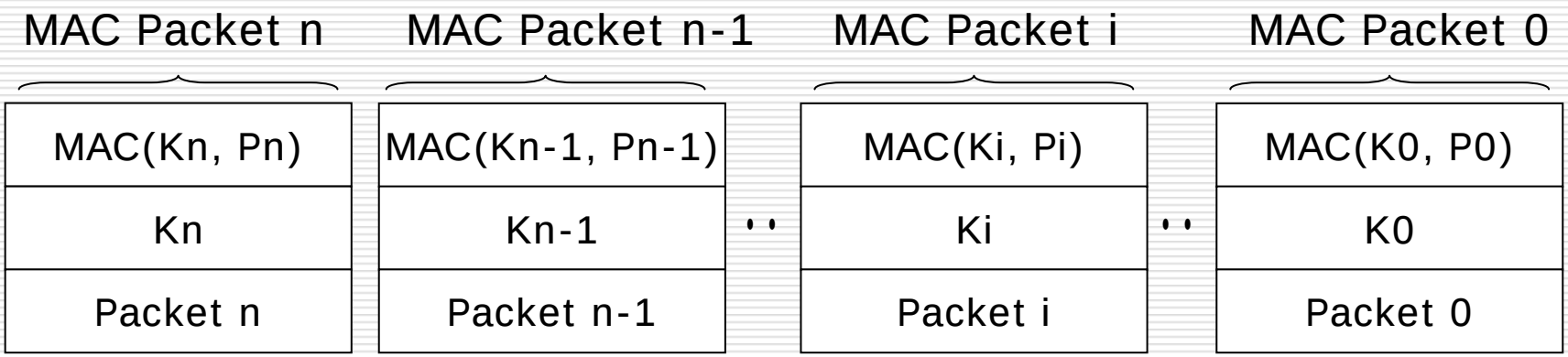


[参考] MSEC
～ストリームデータの認証とハッシュ連鎖～

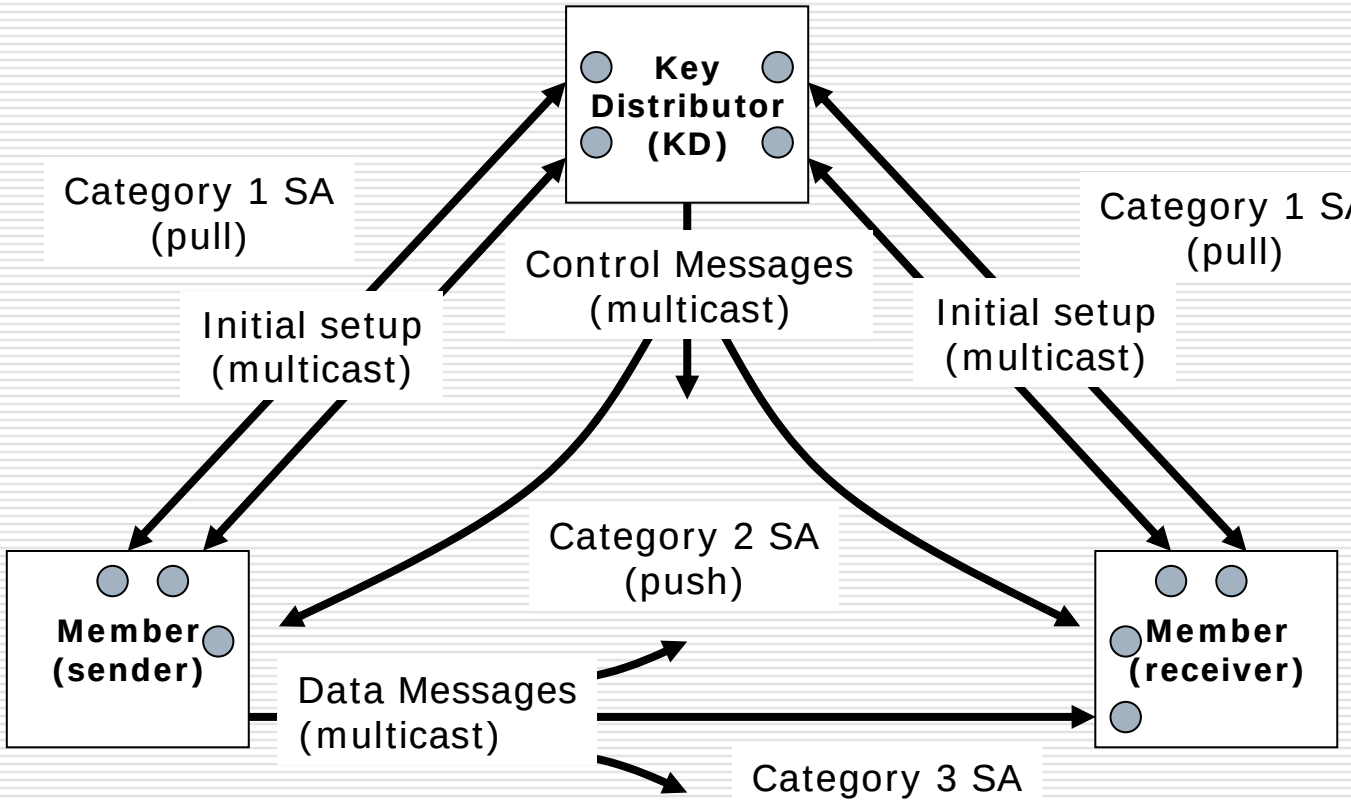
Hash Chainingによるストリームのソース認証



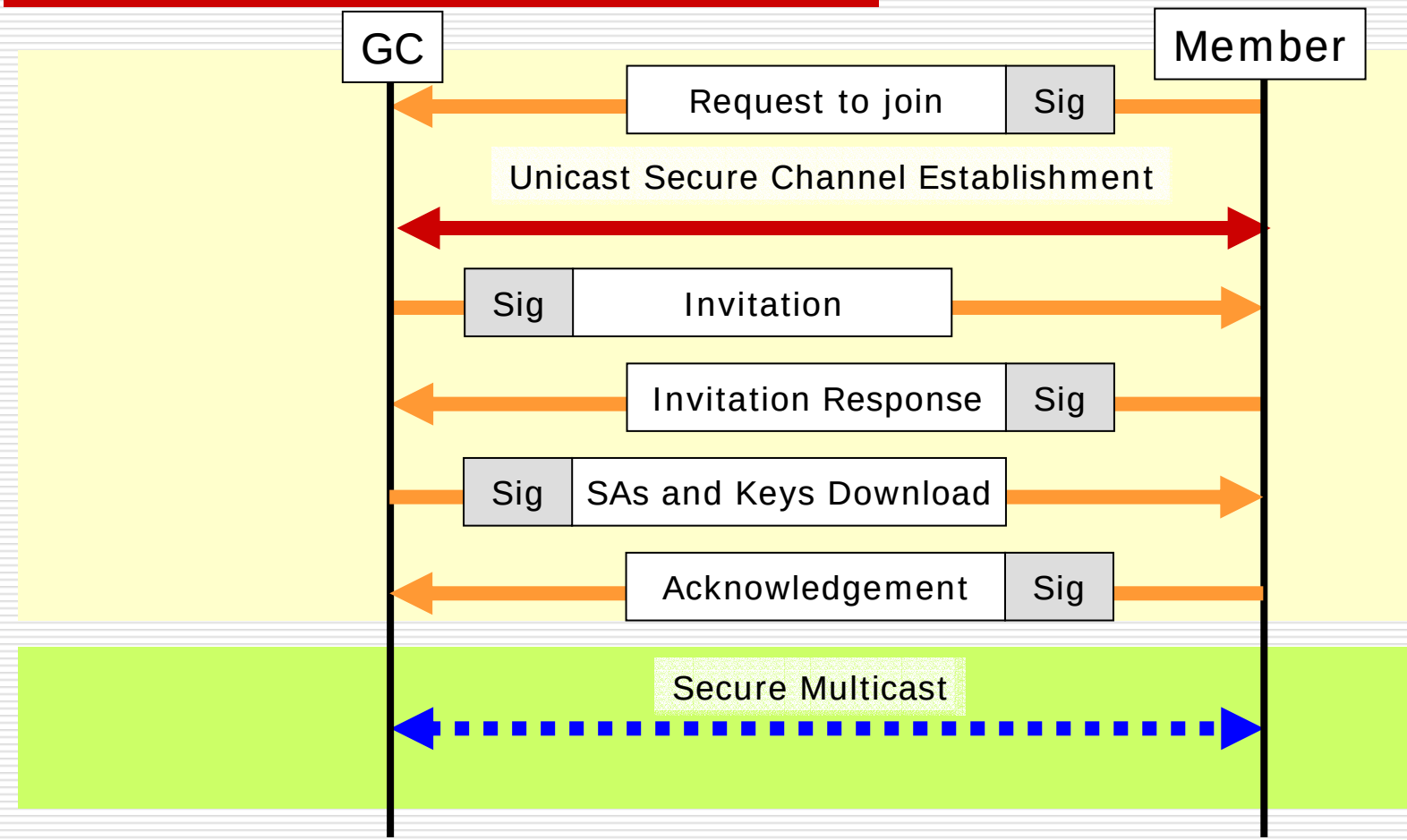
TESLAによるストリームのソース認証



[参考] MSEC ～SA～



[参考] MSEC ~GSAKMP~



GC:Group Controller

注:実線は平文、点線は暗号化

IETFでの動向

- IKEv2
- PKI4IPSEC
- MOBIKE
- NBTS
- EASYCERT
- INCH (RID)

IKEv1→IKEv2

- リモートアクセスVPN対応
  - EAP(RFC3748)認証によるユーザ認証
  - NAT-T(NAPT対応)
- DoS耐性 (Cookie)
- IKEv2のネゴシエーションの認証は証明書のみとなる (ただしオプション)
  - RSA、DSSの認証は使われない
- カウンターモード→ギガネットワーク対応
- OCSP in IKEv2

PKI4IPSEC

- IPsecで証明書をもっと使ってほしい(v1/v2)
- PKIとIPsec間の証明書のライフサイクルの取り扱い
- CMCがよい
- CRLsのInbound/Outbound問題
- IKEのUDPフラグメント問題
- CRLsのサイズ問題
- OCSPではInbound

MOBIKE

- IKEv2のモビリティとマルチホーミング実現
(IPアドレスが変わっても鍵交換と認証を省略したい)
  - Peer宛Notify PayloadでIPアドレスアップデート
  - DPDでPeerとのルーチング状態を確認
  - IKE-SA、IPsec-SAは新しいIPアドレスに変更

NBTS
~ Nothing Better Than Security BoF ~

- Nothing Better Than Security BoF
  - IETF61thでBoFが立ち上がったが求心力を得ているようである。BCPとする。
  - Pre-sharedやCAを使わず簡単にIPsecする
    - Off-path-Attackに対応
    - Man-in-the-middleは除く
  - BGPなどのプロトコルを防御する（ないよりまし）
  - 今後普及する可能性あり

EasyCert
~Easy to use Certificates BOF~

- **公開鍵、証明書の扱いを簡単にする**
  (楽に生活しようよ)
- **ペイパービューPKI (銀行,クレジットカード…)**
- **MITの学生用CAの運用**
  - **10年ほどの運用実績**
- **社員の証明書プロファイルの扱い**
- **SIPアーキテクト**

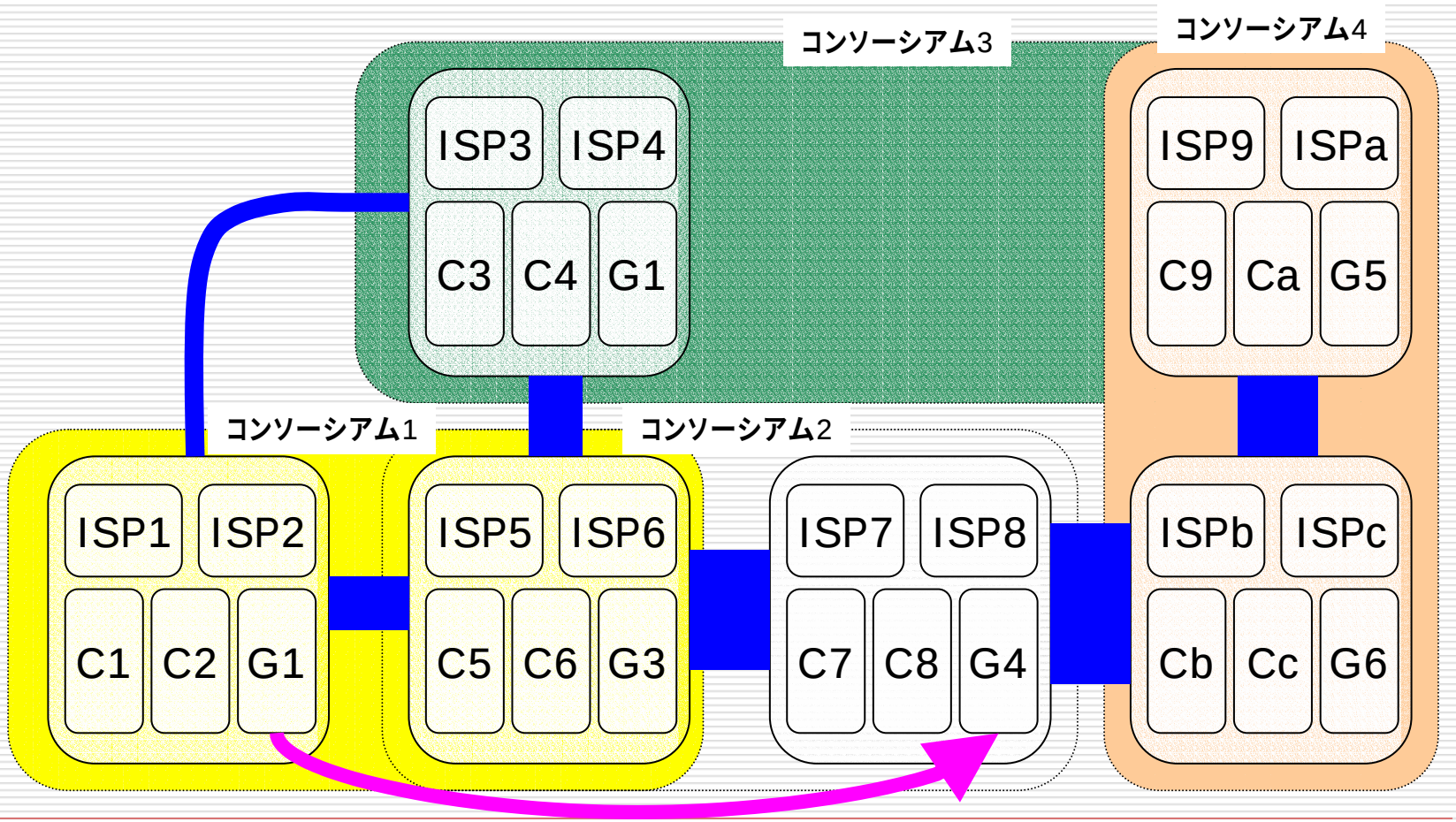
RID (Realtime Inter Defense)

- RIDの目的
  - DoS/DDoS、乗っ取り、ワーム、ウイルスなどのインシデント・ハンドリングを目的とする。
  - ネットワーク横断的なインシデントの検出と追跡の統合、およびその対策（防御）のための拡張性の提供。
- RIDの内容
  - ネットワークプロバイダ（NP）間の境界（バウンダリ）を横断して存在する追跡メカニズムを統合し、攻撃源の特定を行うための先進的相互通信手法のこと
- RIDの役割
  - ネットワーク横断的（バウンダリ横断）な攻撃源の追跡
  - インシデント検出と追跡実行の統合
  - インシデントハンドリングのための拡張（防御など）提供

RIDの課題

- 各国政府レベル、企業レベルでのポリシー策定
- 各国間の連携（コンソーシアム間の連携）
- NPの協力と推進
- インシデント検出、追跡装置の認知と普及
- 大規模なシステムによる実験

RID
～プライバシーへの配慮～



IETFでの動向 & まとめ

- 見直しの動き
  - 簡略化 (EasyCert, NBTS)
  - リバイス (IKEv2)
  - 性能向上 (MSEC, MOBIKE, カウンターモード)
- ポリシーとプライバシー問題
  - INCH (RID)

- まとめ

  様々なプロトコルでPKIは使われてきているが課題もある