~~SSL~~
TLSとDNSSEC

セコム(株)IS研究所
島岡　政基

TLSが実現するセキュリティ

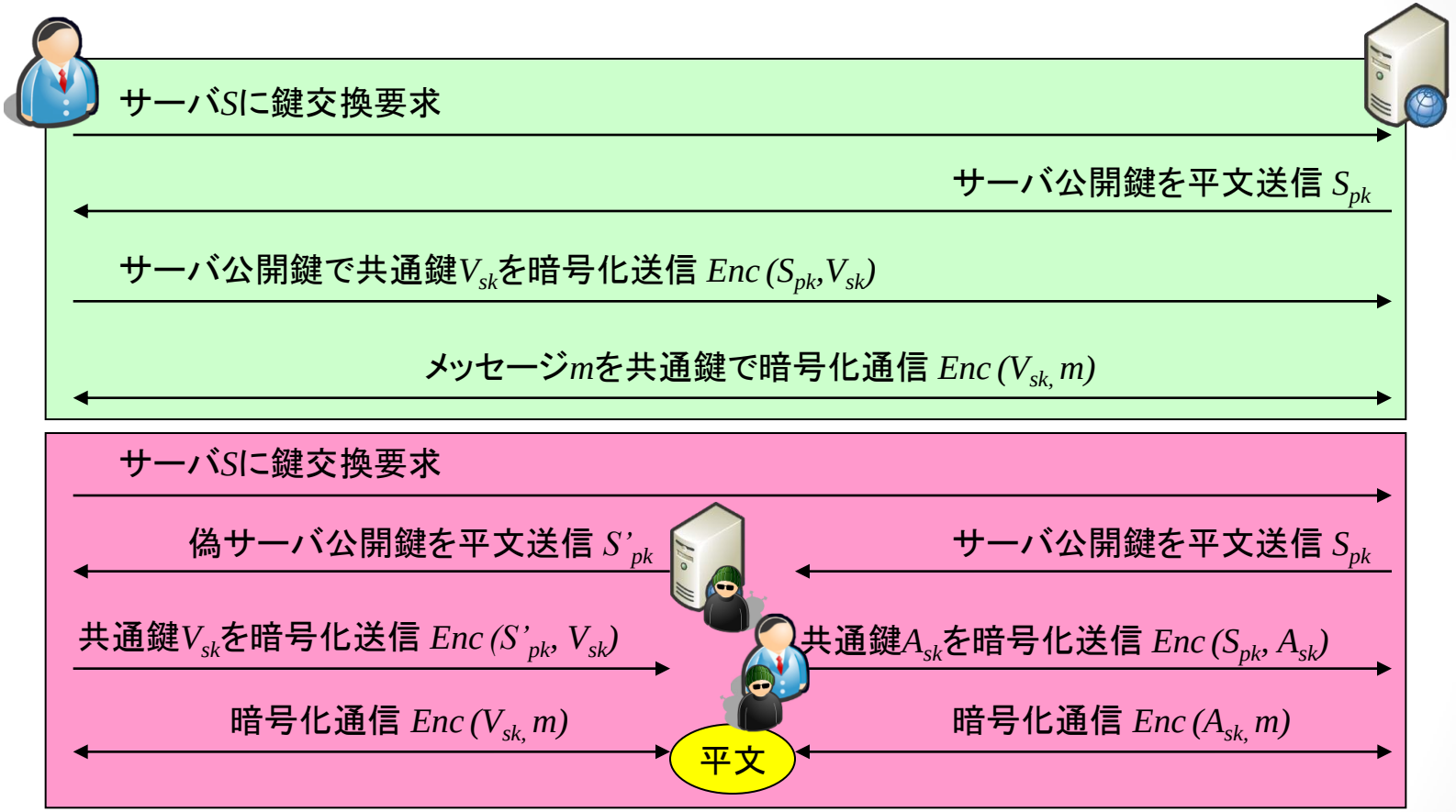
- サーバ認証、時々クライアント認証

- 暗号化通信が最終的な目的(サーバ認証)
  - 共通鍵の鍵配送問題→事前鍵共有 or 鍵交換プロトコル
  - DHの中間者攻撃問題→TTP(認証局)による署名

中間者攻撃がなければDHでOK
DANEすらいらなくなる、はず

- 商用認証局による付加価値
  - 実在性証明(EV証明書、OV証明書)
- プライベート認証局による信頼ドメイン
  - 組織内PKIなど

DHの中間者攻撃脆弱性

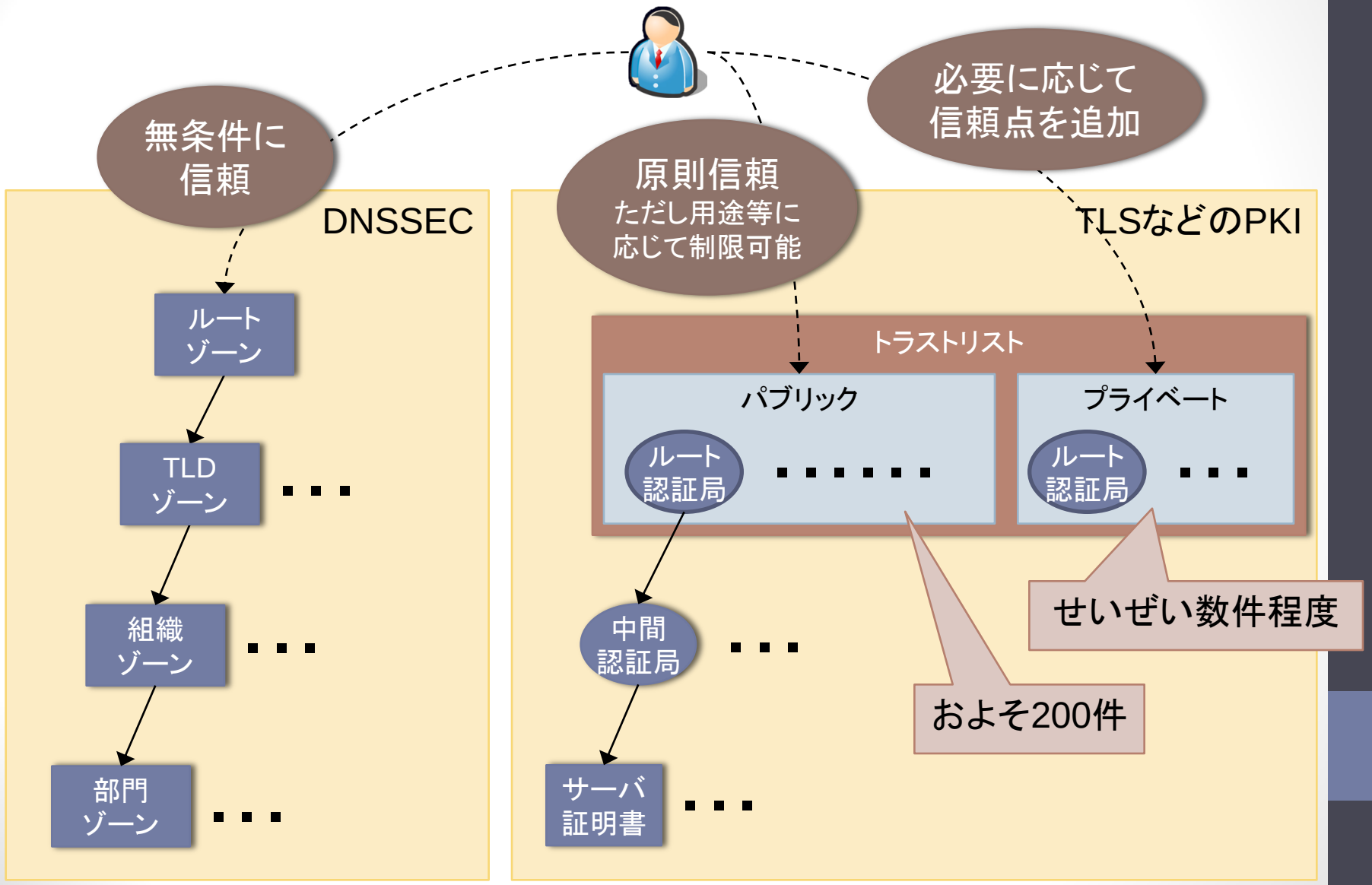


サーバSへの送信に偽サーバS'が応答できれば中間者攻撃成立
DNSポイズニング、IPスプーフィングなど方法は色々
偽サーバS'(の公開鍵)を看破できる技術としてのTLSやDNSSEC

TLSとDNSSECの違い

	DNSSEC	TLS
目的	DNS応答の真正性 (キャッシュ含む)	認証相手の本人性 (および暗号化)
保証するもの	ドメイン名と IPアドレスの紐付け	ドメイン名と 鍵ペア所有者の紐付け
信頼点	ルートゾーン一択	パブリック認証局 または プライベート認証局
信頼点の配布	安全な経路で配布	配布不要 (パブリック認証局)
導入単位	ゾーン毎 (かつ上位依存)	ホスト毎
信頼の範囲	DNSドメイン	信頼点を共有する エンティティ同士
クライアント	キャッシュDNS (DNSバリデータ)	エンドエンティティ (Webブラウザなど)

トラストモデルの違い


無条件に
信頼
DNSSEC
ルート
ゾーン
TLD
ゾーン
組織
ゾーン
部門
ゾーン
原則信頼
ただし用途等に
応じて制限可能
必要に応じて
信頼点を追加
TLSなどのPKI
トラストリスト
パブリック
プライベート
ルート
認証局
ルート
認証局
中間
認証局
サーバ
証明書
およそ200件
せいぜい数件程度

DANEとTLS

- 典型的な使い方
  - TLSAレコードに以下を登録
    1. サーバ証明書のフィンガープリント
    2. ルート証明書そのもの
  - TLSハンドシェイクで取得したサーバ証明書を1と照合
  - サーバ証明書のトラストアンカとして2を使用
- TLSサーバ認証をより安全に
  - トラストアンカの配布安全性がDNSSECというTTP?によって保証される
- DANEができること
  - オレオレ証明書の安全?な配布
- DANEができないこと
  - 証明書、認証局は不可欠

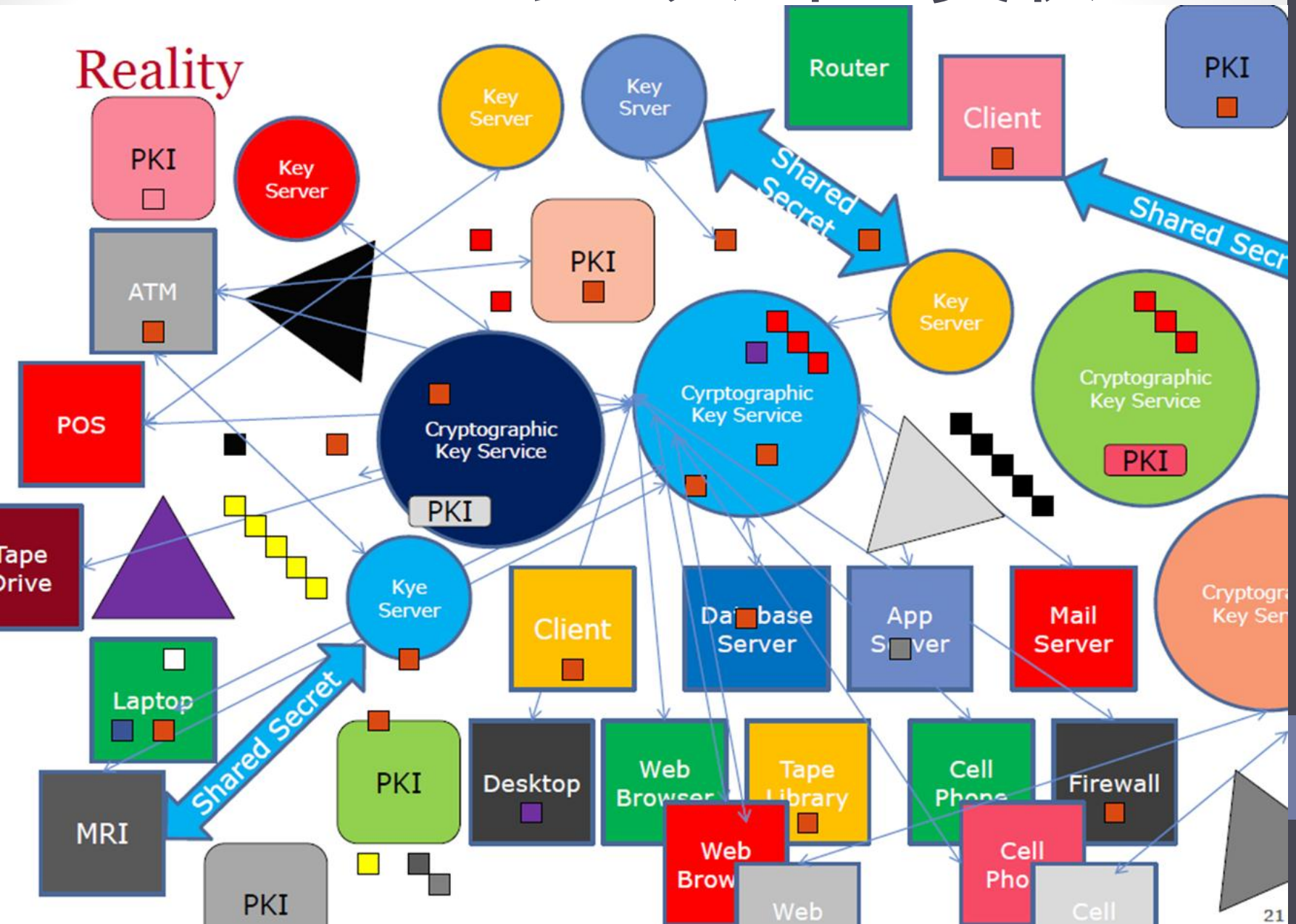
インターネットにおける Add-onセキュリティ

- 既存プロトコルに対するadd-onセキュリティの歴史
  - DKIM, SPF, DNSSEC, TLSもまた然り
  - 移行のインセンティブが弱い
  - あくまでもオプション
- DNSSEC導入の課題
  - 上位ゾーンによる導入を待つ必要がある
  - 限定的運用も勿論可能だろうけど。。。

- かと言って Security by Design なネットワークもまた非現実的
- 運用管理者はセキュリティ確保のために様々な代替技術を組み合わせて補完する
- 他の技術で一定のセキュリティが確保できればますます移行インセンティブは弱くなる

http://storageconference.org/2010/Presentations/KMS/9.Stieber.pdf#page=22 より

Add-onセキュリティの実状



DNSSECの守備範囲

- DNSSECは完全ではないし万能ではない
  - もちろん他の多くのセキュリティ技術も然り
  - インターネット上のすべてのDNSサーバが対応するわけでもない
  - リソースレコード応用への期待感
    - 価値付加によるDNSSEC普及のジレンマ
- 中間者攻撃対策を完全に防ぐことはできない
  - 本来はDNSキャッシュポイゾニング対策の技術
  - RPKIやTLSなどとの併用が大事
- 現状の運用モデルで困難なこともある
  - 管理レコードの肥大化、鍵更新、HSM運用、DPS準拠など
  - セキュアDNSホスティングサービスがあってもいいのでは?