

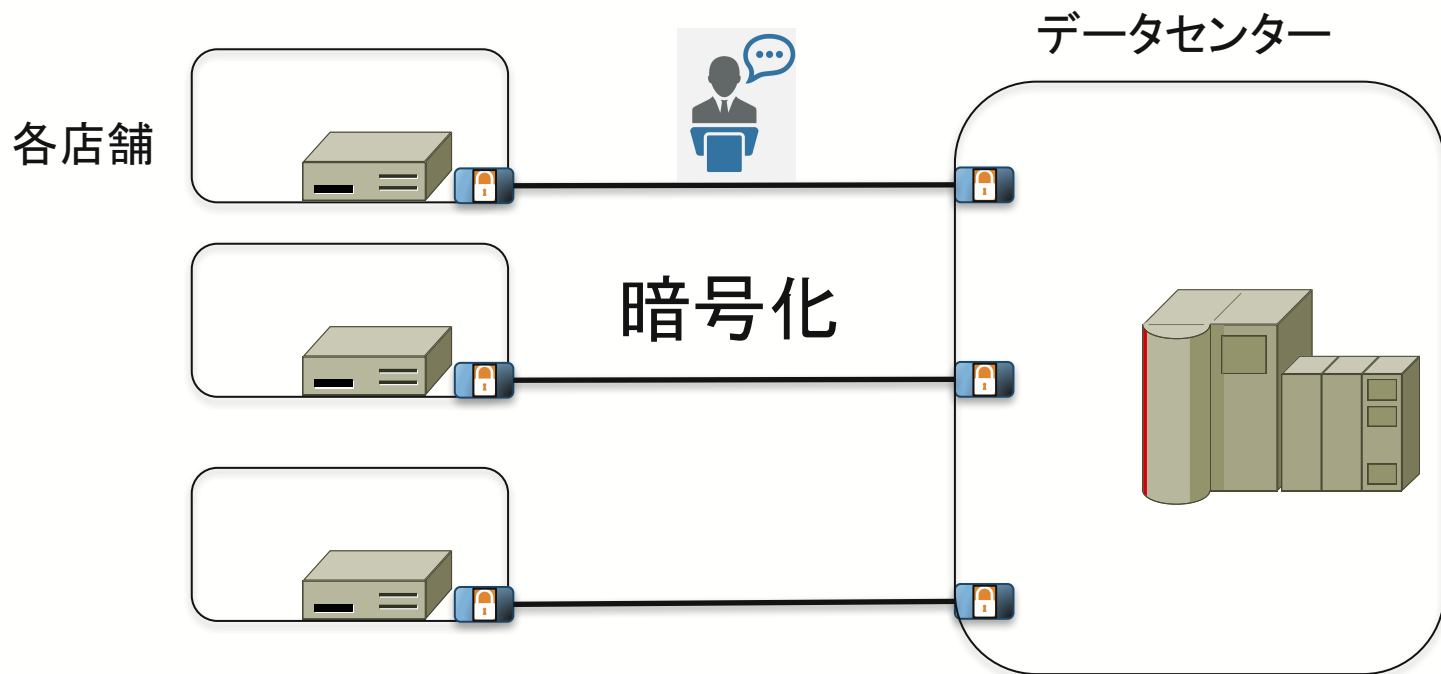
Encrypted データセンター -IEEE802.1AE(MAC Security)

Shishio Tsuchiya
shtsuchi@arista.com

FISCとは？

- 公益財団法人 金融情報システムセンター
 - FISC: The **C**enter for **F**inancial Industry **I**nformation **S**ystems
- 金融情報システムにおける様々なガイドラインを提示

昔の金融ネットワーク



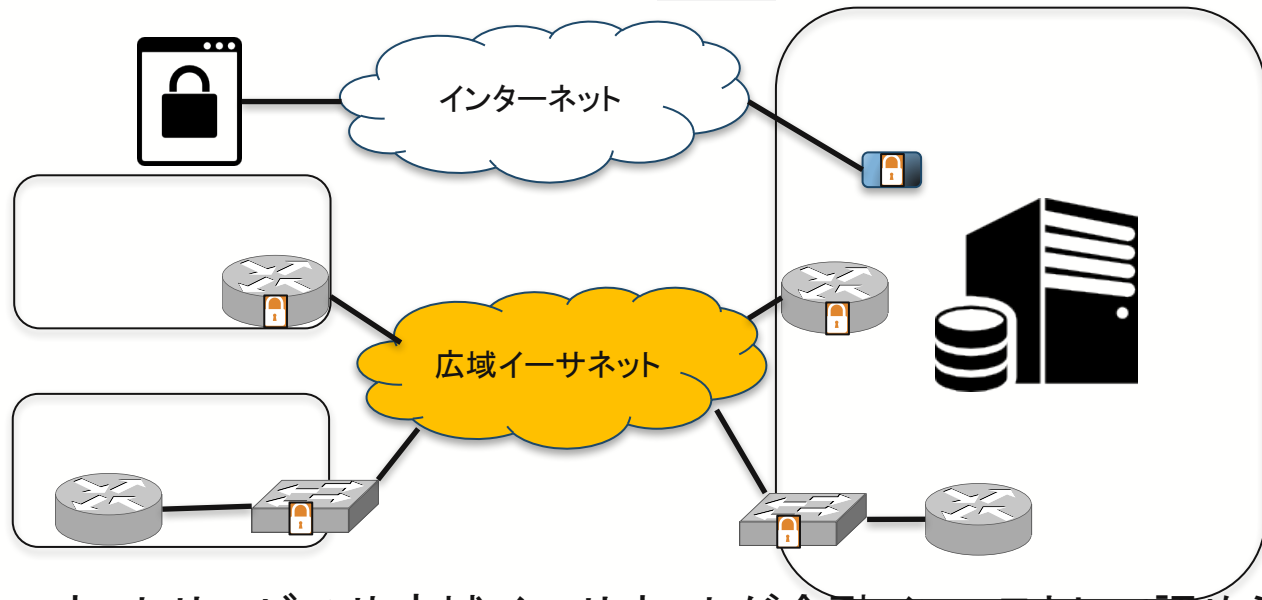
- T1回線などの間に暗号化装置を入れて、キャリアであったとしても通信を見る事が出来ない

昨今の金融ネットワーク



データセンター

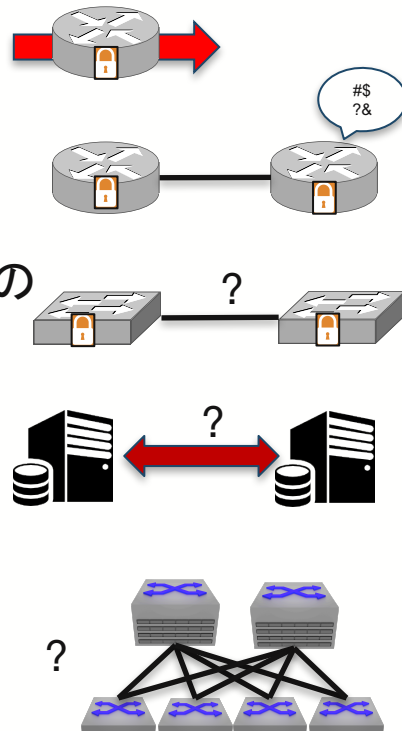
各店舗



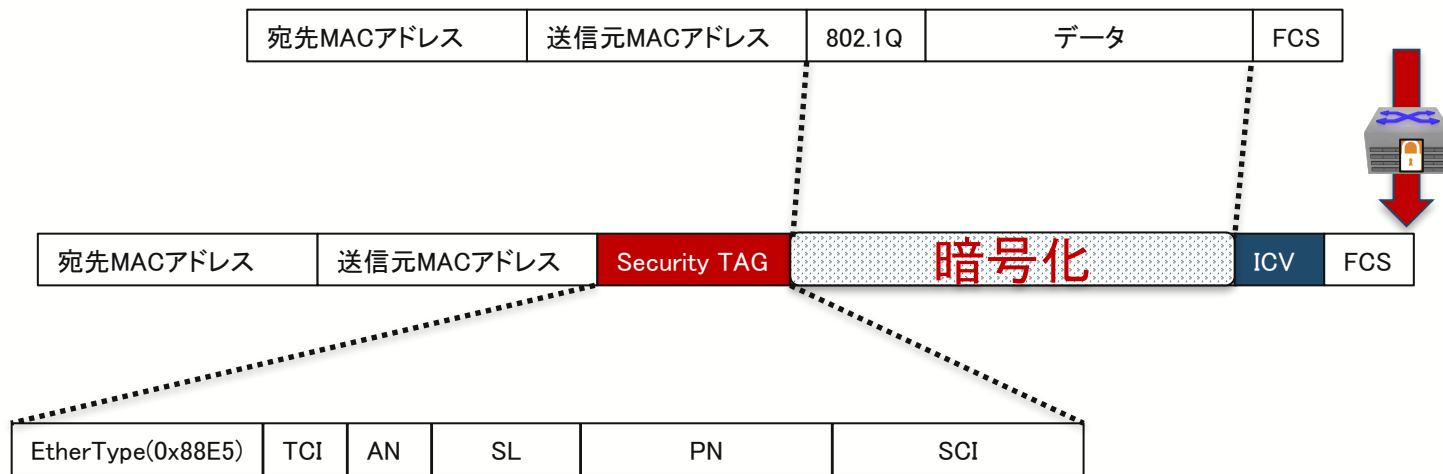
- インターネットサービスや広域イーサネットが金融インフラとして認められ、様々な暗号化プロトコルが使用されるようになった
- SSL インターネット
- IPSec / 独自イーサネット暗号化スイッチ

昨今の金融ネットワークでの暗号化の考慮点

- IPSecルータのパフォーマンス
- IPSecルータの異機種間での相互接続性:IKEv2?
- イーサネット・スイッチでの暗号化手法
- ディザスタリカバリーなど信頼性を高める為のDCIでの暗号化手法
- クラウド型データセンターでの暗号化方式
 - スケール型のネットワークでどのように暗号化を提供するか?
- プライベートクラウドでの展開

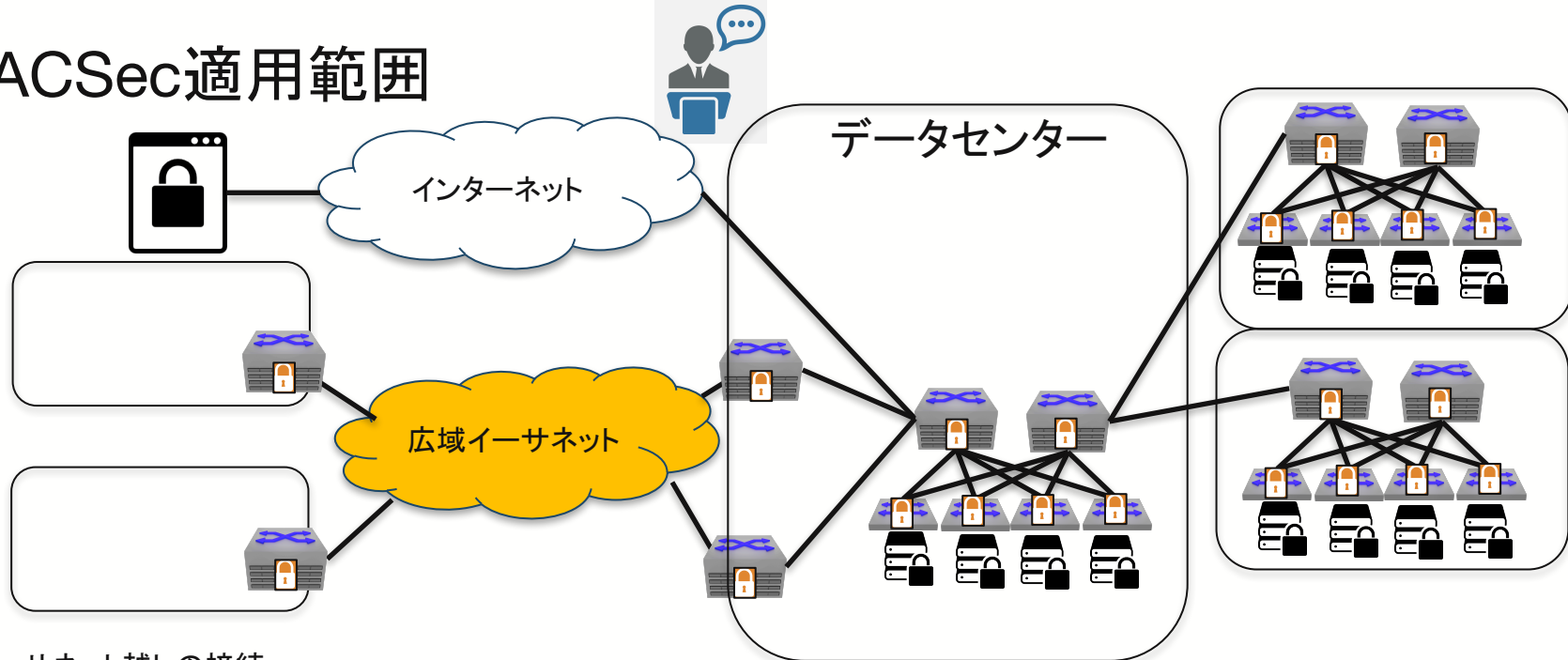


IEEE802.1AE(Mac Security)



- 2006年に標準化された方式: 2011年 802.1AEbn/2013年802.1AEbwと拡張
- IEEE802.1AE(MACSec)ではオリジナルフレームの802.1q情報以下のデータは全て暗号化される
- Security TAGおよびICV(Message Authentication Code)が付与される

MACSec適用範囲



- 広域イーサネット越しの接続:
 - IPSec相互接続問題やパフォーマンス問題を解消
 - 独自暗号化設備からの解放
- データセンター内
 - スケール型ネットワークデザインでアプリケーションレイヤーのみならずインフラでも暗号化
- データセンター間
 - パフォーマンス劣化/相互接続問題無しでセキュアな接続

まとめ

- 日本の金融ネットワークではFISCが様々なガイドラインを提供
- 最近では広域イーサネット/IP-VPNなどの利用やSSL/IPSecなどのプロトコルの利用が普及してきた
- 一方IPSec暗号化のパフォーマンスや相互接続性の問題は多く、また日本では独自暗号化装置も普及
- IEEE802.1AE(MAC Security)は標準化プロトコルであり、チップレベルでの実装となる為、パフォーマンス劣化および暗号化により遅延は最小で抑えられる



Thank You

www.arista.com