修士論文審査

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

階層化原理に基づくプロトコル スタックのモデル化と代表的ICSプロトコルとの比較分析

Modeling of a Protocol Stack Based on Hierarchical Principle and Comparative Analysis of Representative ICS Protocols

後藤研究室　博士前期課程2年
我妻　敏

2020/02/15

提案モデルの提供するもの

工場、プラントなどのICS通信プロトコルは多岐に渡り、オープン化した場合のリスク評価が十分ではない

- 種類が非常に多い
- ベンダー ユニークなものも多い
- 情報セキュリティにあまり関心がなかった

■提案した手法では、通信要件を階層に分割し（Divide）、分析・評価する（Conquer）ことで、システマチックに各プロトコルが持つ脆弱性を確認することができた

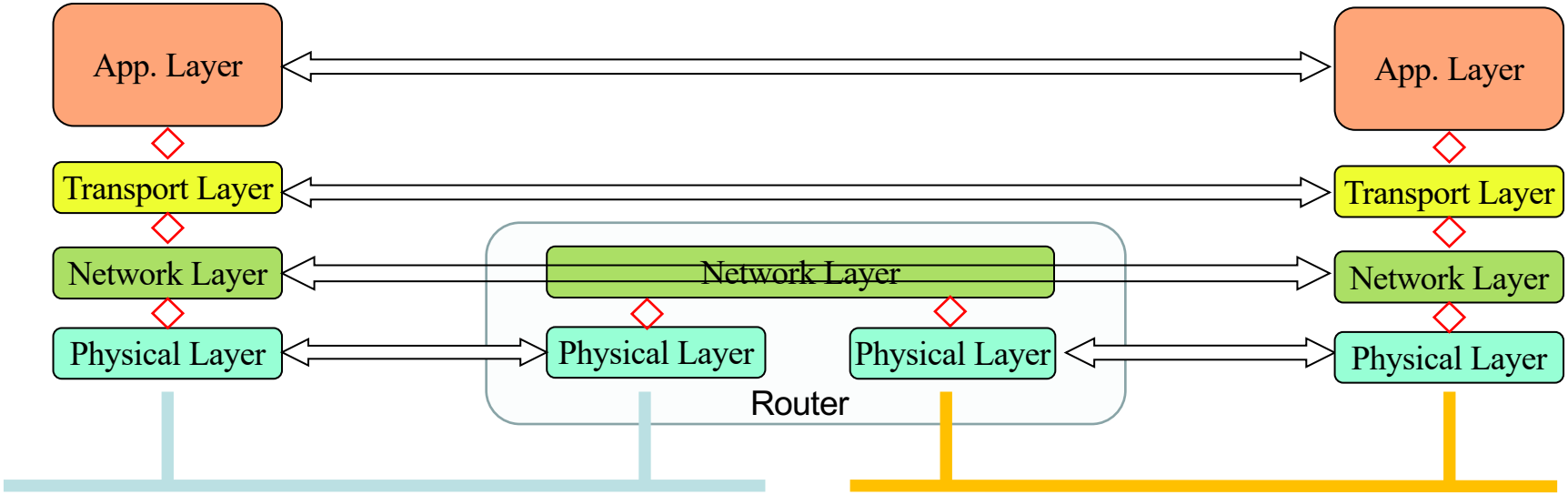
提案モデルの提供するもの　続き

- 階層に応じて脆弱性が整理されるため、取るべき対策はレゴ的に検討が可能となった

- 本手続きを利用し、代表的ICSプロトコルの特性を確認することができた
  - Modbus/TCP
  - EtherNet/IP_CIP
  - FL-net
  - OPC UA

手法の概要

4階層構造



階層	機能	エンティティ
アプリケーション層	メッセージ交換	アプリケーション プロセス
トランスポート層	Process-to-Process	ソケット インターフェイス
ネットワーク層	Host-to-Host	ホスト
物理層	NIC-to-NIC	NIC

上記のアプリケーション層は、OSI参照モデルのそれとはまったく定義を異にすることに注意

階層別： 通信要件

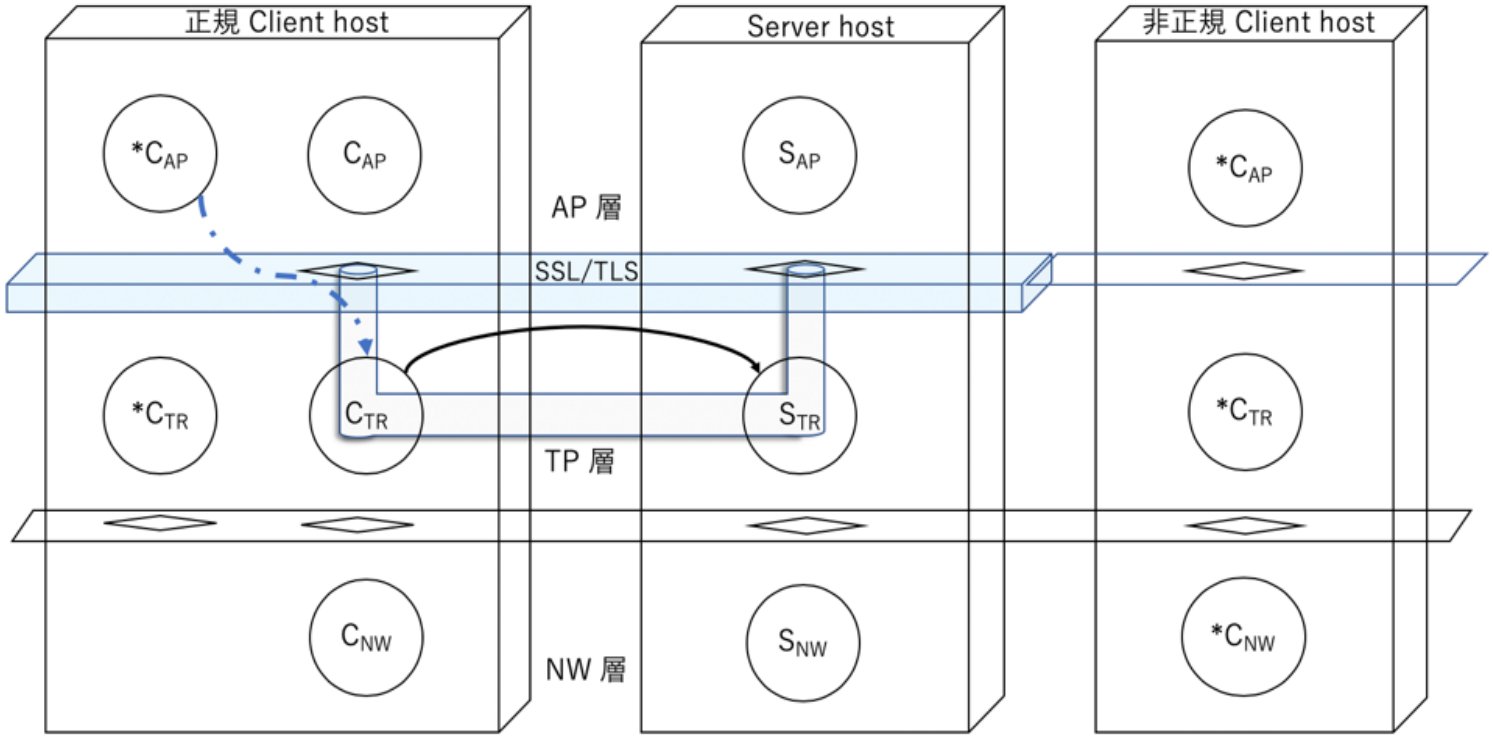
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■4階層構造に分割し、各階層ごとに下記の要件の充足度を評価する

レイヤ	コード	対象要素	要求仕様
アプリケーション	AP-const-1	インスタンス（プログラム）	エンティティ認証
アプリケーション	AP-const-2	インスタンス（プログラム）	（SEQ番号、メッセージ）の完全性
トランスポート	TP-const-1	インスタンス（サービス）	透過性の保護
トランスポート	TP-const-2	インスタンス（サービス）	コネクション型の使用
トランスポート	TP-const-3	インスタンス（サービス）	着信許可エンティティの指定
トランスポート	TP-const-4	インスタンス（サービス）	エンティティ認証
ネットワーク	NW-const-1	通信ノード	受信許可サブネットの指定
ネットワーク	NW-const-2	通信ノード	受信許可ノードの指定
ネットワーク	NW-extra	通信ノード	エンティティ認証

N層緩和策のカバレッジ

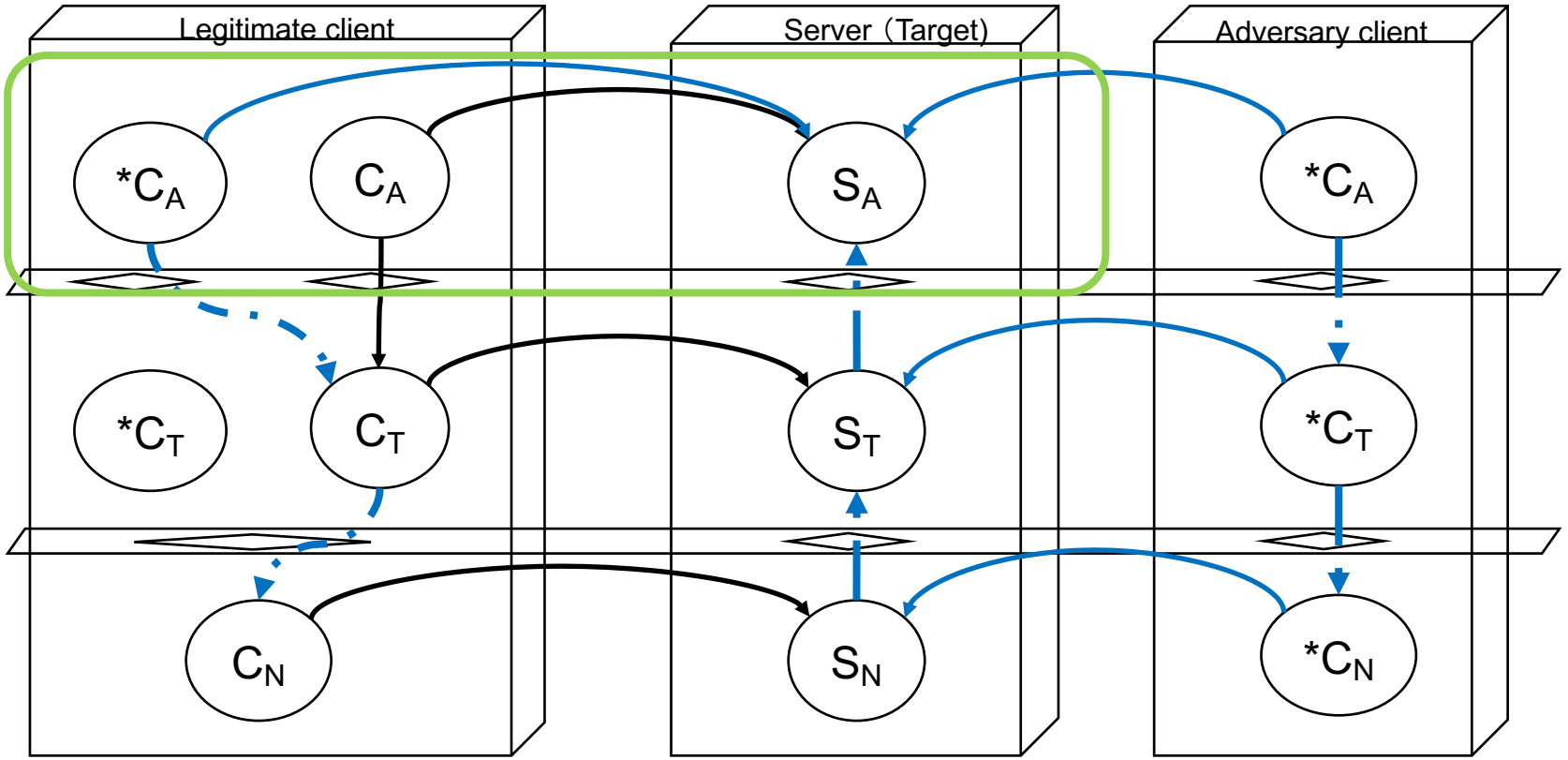
■N層緩和策は、N層以下の脅威エージェントに大して有効



アプリケーション層を対象に

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

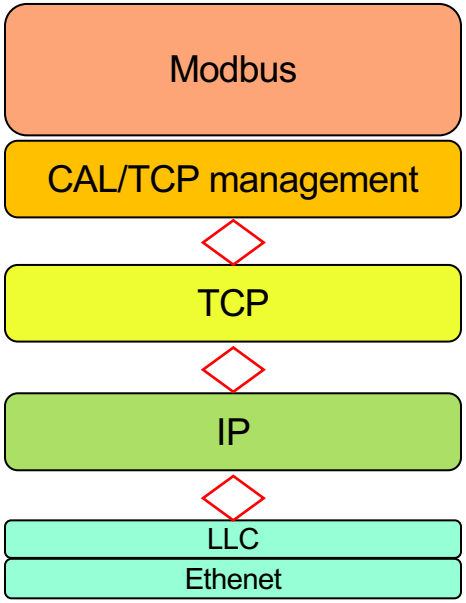
■アプリケーション層プロトコルを検討する



Legacy - Modbus/TCP

■4階層モデル

- Modbus、CAL/TCP management を分析
- ネットワーク層、トランスポート層は、TCP/IP一般における脆弱性を評価、その対策が利用可能



Legacy – Modbus/TCP

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

*C_A からのメッセージは検知可能か

アプリケーション	AP-const-2	インスタンス（プログラム）	（SEQ番号、メッセージ）の完全性

message = (code, data)

SDU:C->S = (message, Req#, UnitId#, Len, Proto#)

(Req# = Transaction Identifier)

第3のエンティティは、偽のメッセージを生成可能:

*SDU:C->S = *(message, Req#, UnitId#, Len, Proto#)

-> (*message, *Req#, *UnitId#, *Len, *Proto#)

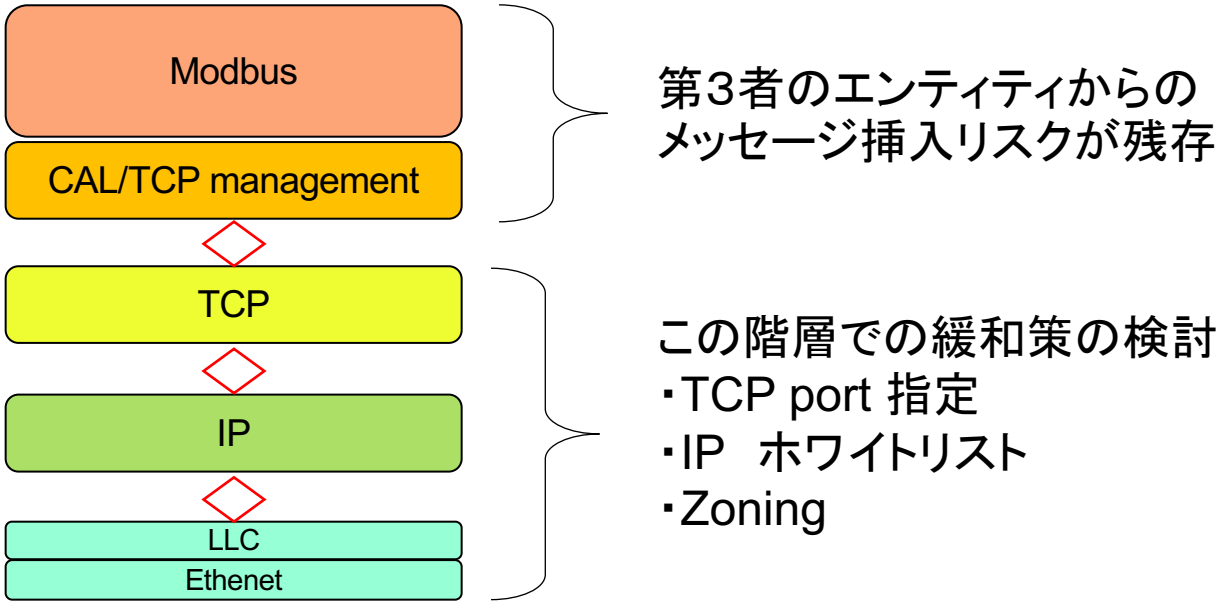
これら2項組の意味上の差が表現できない

(seq = i, command = a) then (seq = i+1, command = a)

(seq = i, command = a) then (seq = i, command = a)

Legacy – Modbus/TCP

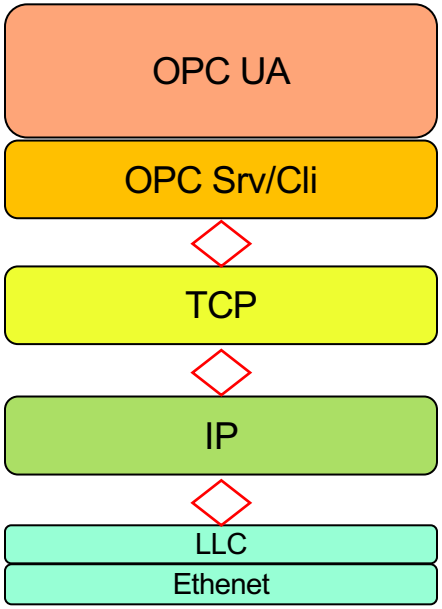
- エンティティ認証、コマンドとそのシーケンスの保護ができない
  - 第3のエンティティの検知はできない
- トランスポート層以下の緩和策のみが実装可能



Modern – OPC UA

■4階層モデル

- OPC UA / OPC Srv/Cli を分析
- ネットワーク層、トランスポート層は、TCP/IP一般における脆弱性を評価、その対策が利用可能



Modern – OPC UA

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

*C_A からのメッセージは検知可能か

アプリケーション	AP-const-2	インスタンス（プログラム）	（SEQ番号、メッセージ）の完全性

SecureChannel が確立：

req = (request, Sec_hdr, Seq_hdr)

SDU:C->S = (request, Sec_hdr, Seq_hdr, H(request, Sec_hdr, Seq_hdr, cliKsec))

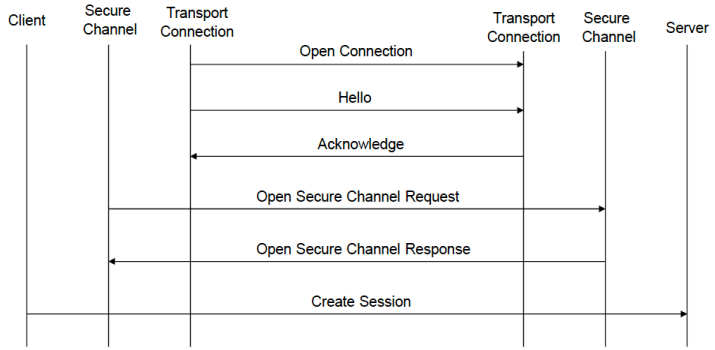
Sec_hdr は SenderCertificate 等を保持

Seq_hdr は SequenceNumber, RequestID を保持

第3のエンティティは、‘cliKeysec’ にアクセス不能：

*H(request, Sec_hdr, Seq_hdr, cliKsec) = ⊥

∴ *SDU:C->S = ⊥

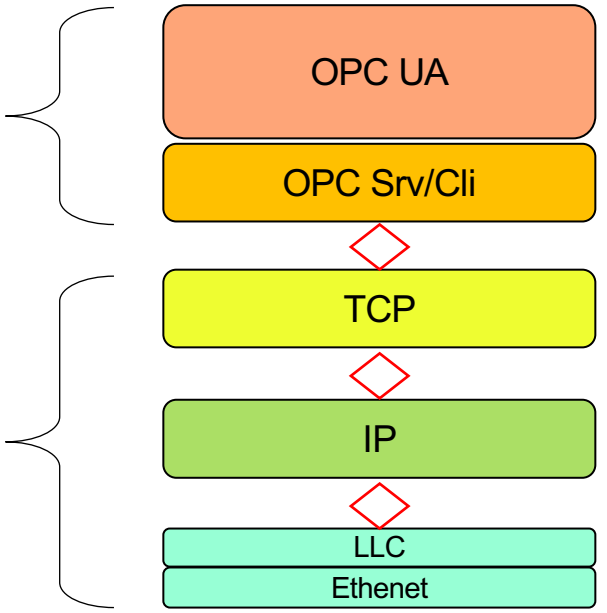


Modern – OPC UA

- エンティティ認証、コマンドとそのシーケンスの保護が可能
  - 適切な Profileの定義とその実装
- トランスポート層以下の緩和策は、上位層の負荷軽減に寄与

第3者のエンティティの検知可能
リプレイによるシーケンス破れの検知可能

この階層での緩和策
・TCP port 指定
・IP　ホワイトリスト
・Zoning
負荷の高い上位層の処理を軽減



提案モデルの提供するもの － 再掲

- 提案した手法では、通信要件を階層に分割し（Divide）、分析・評価する（Conquer）ことで、システマチックに各プロトコルが持つ脆弱性を確認することができた
- 階層に応じて脆弱性が整理されるため、取るべき対策はレゴ的に検討が可能となった
- 本手続きを利用し、代表的ICSプロトコルの特性を確認することができた

今後の課題
外部発表

今後の課題

- メッセージの持つ意味的なConstraints
  - 設定値などの変更によるリスクへの対応
    - メッセージをさらに構造化
    - 独立したリファレンス モニタ
- (関心事)マルウェアの感染モデル
  - 無数に設置されたセンサーがマルウェアに感染した場合、どの程度の感染率で影響があらわれるのか
    - 分散システムの合意形成
  - 多様性は有効か
    - 生物のような、ゆらぎがない
    - デジタル ツインだから、一つのVirusで全滅

外部発表：NCSS’10

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Nagasaki, Japan, November 26-29, 2019

CANDER ’19 併設 Workshop に参加

NCSS’10

The 10th International Workshop on Networking, Computing, Systems, and Software

■ 11月29日　発表

NCSS3

- Chair: Jacir L. Bordim (University of Brasilia)
- 132 Preliminary version: Attempt of modeling of connected Industorial Control System’s communication aiming information security risk extraction, Satoshi Agatsuma
- 136 PKI-enabled OSPFv3 for Reliable IP Traceback, Takahiro Oriishi, Kenji Matsuura and Kenji Ohira
- 201 Multi-agent Based Energy Balancing Management Algorithm for Smart Grid System, Malla Dinesh Bahadur, Katsuyoshi Sakamoto and Tomah Sogabe
- 192 Flower pollination optimization for the multi-objective knapsack problem, Yuta Hadachi and Akihiro Fujiwara

以上

ありがとうございました。