固定通信事業サービスを支える制御ネットワークのセキュリティ確保
Considerations for ensure security of control Network supporting telecom business services

長谷川　勇気・システム分科会・情報セキュリティ大学院大学

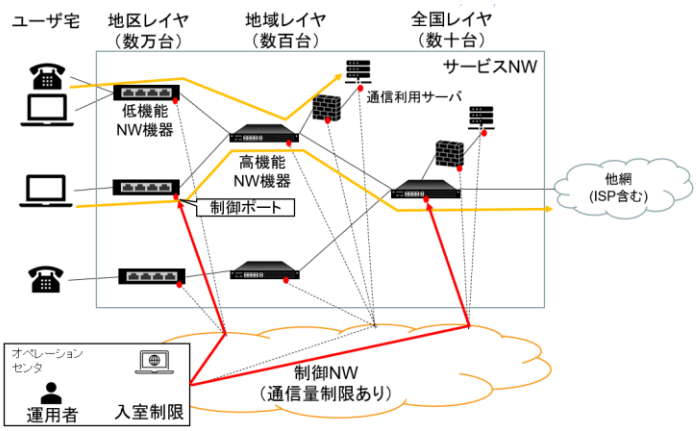
Telecommunication carriers provide control NWs separately from service NWs through which actual Internet communications and other traffic pass. Conventionally, the security of the control NW has been ensured by prohibiting mutual communication with the service NW. In this study, we examined the issues of control NWs and proposed a method to solve them. To confirm the validity of the proposed method, we created a simulation environment and verified.

1. 背景と概要

- 通信事業者では、実際のインターネット通信等が通過するサービスNWとは別に、制御NWが用意されている。
- 従来はサービスNWとの相互通信を禁じることで制御NWのセキュリティを確保してきた。
- 本研究では、制御NWの課題を検討した上で課題の解決手法を提案した。
- 提案手法の正当性を確認するため、シミュレーション環境を作成し、制御NWに適用可能か検証した。

2. 通信事業者のNW

サービス提供に必要なNW機器やサーバを、制御NWを通して日々制御を行っている。



■制御NWの特徴
- 全国規模の大規模に展開されている
- 制御NWの通信量は制限されている
- 制御NWはサービスNWと相互に通信を禁止し、インターネット等別NWへ通信できない

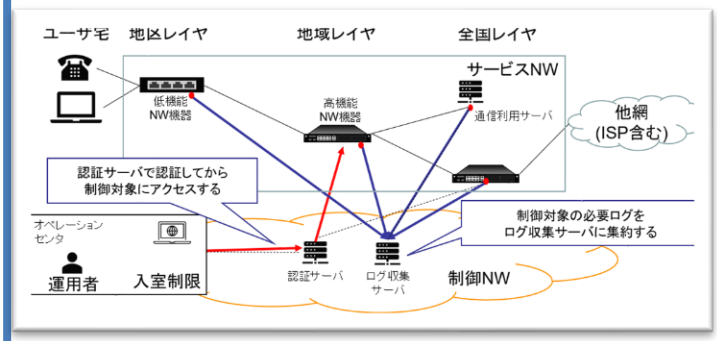
3. 制御NWの課題

通信事業者の制御NWに対してIPAの「制御システムのセキュリティリスク分析ガイド」に基づき、分析を行った

■分析結果による課題
- 誰がどの装置に適切な権限で制御を行ったか判断できない
- 各ルータ等の制御対象に対して、いつ、どこから制御されたのか判断できない

4. 提案手法

- 制御NWを通じたアクセスを全て認証サーバで認証を行い、アクセスを可能にする
- 制御NWを通じた制御対象への認証ログを全て収集する
上記情報を相関して検査することで攻撃検知



■提案手法による攻撃検知を実施

ログ分析基盤にて攻撃を検知可能！

5. シミュレーション検証

■GNS3によるシミュレーションを実施