一般社団法人レジリエンス協会
2024年 1月 30日

NTP トンネリングの脅威モデルの実証とその対策

2024年1月定例会 ～学生発表会～

定例会テーマ：「レジリエンスの未来を担う」

千葉工業大学
情報科学研究科 情報科学専攻
菅澤　真志

目次
Agenda

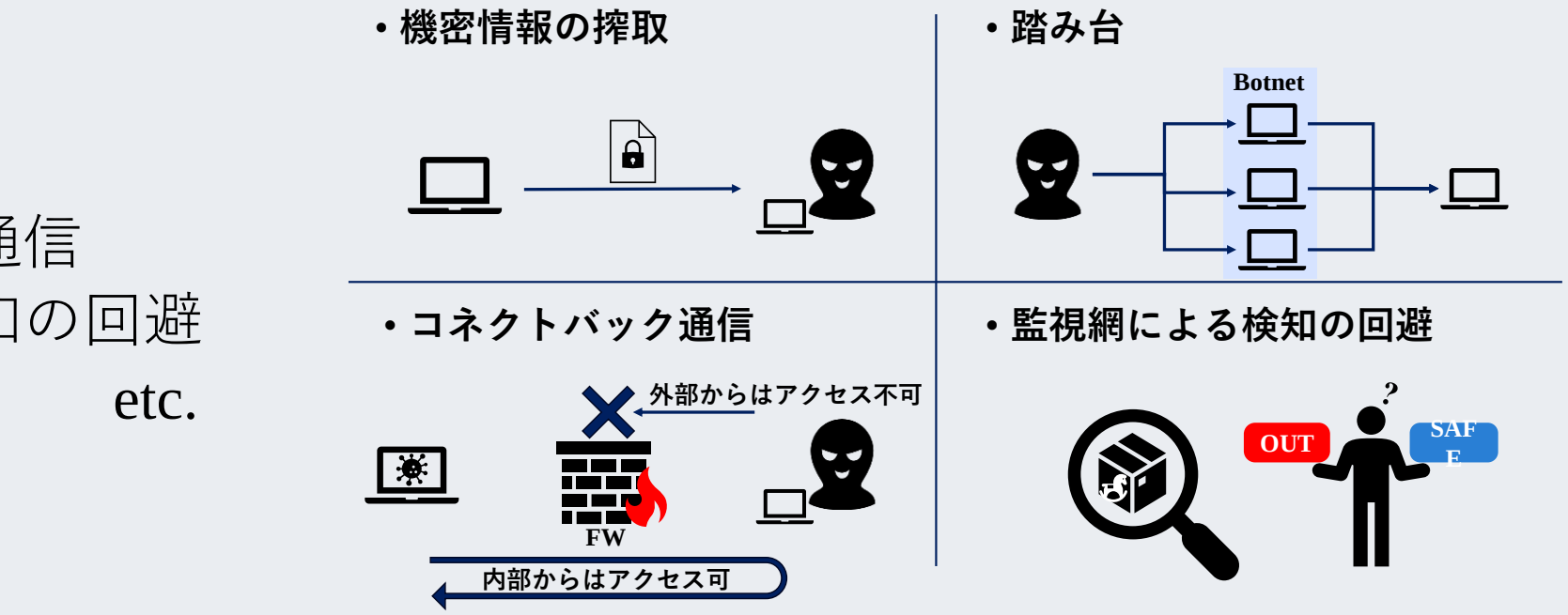
01　不正秘匿通信手法とは

Command & Controlの概要

- **Command & Control (C&C, C2)とは**
  - 攻撃者が制御化にあるシステムに対して，指令（コマンド）を送信し，通信による機器の遠隔操作（コントロール）をすること

- **C&C の利用目的**
  - 機密情報の奪取
  - 踏み台
  - コネクトバック通信
  - 監視網による検知の回避

etc.



※Googleカレンダーが C2チャネルとして悪用される恐れ：Googleが注意喚起
https://codebook.machinarecord.com/threatreport/30296/

不正秘匿通信手法の定義

- C&Cで使われる主な手段

既存ツール利用
- SSH
- RDP
- Web

プロトコル偽装
- DNSトンネリング
- HTTP(S)トンネリング
- ICMPトンネリング

Webサービス利用
- Dropbox
- Google
  - Drive
  - カレンダー*

不正秘匿通信手法

研究背景

- **不正秘匿通信手法の定義**

  C&Cを実現する通信手段の1つで，データやコマンドをプロトコルのクエリなどに挿入して，無害な通信に偽装する通信手法の総称

- **不正秘匿通信手法の特徴**
  - プロトコルの特性を悪用
  - ステルス性が高い
  - 正確な検知が難しい

不正秘匿通信手法の有用性から

- 攻撃者による悪用が続く
- 新たな手法が出現する

研究目的

- **目的**
  - 新たな不正秘匿通信手法の脅威モデルを考案・評価
  - 脅威モデルに対する対策案を提言
- **事前調査**
  - DNSトンネリング
  - HTTP(S)トンネリング
  - ICMPトンネリング　　etc.

  } 不正秘匿通信手法に悪用されるプロトコルの特性を分析
- **事前調査より**
  - Network Time Protocol (NTP)が不正秘匿通信手法に悪用されうる

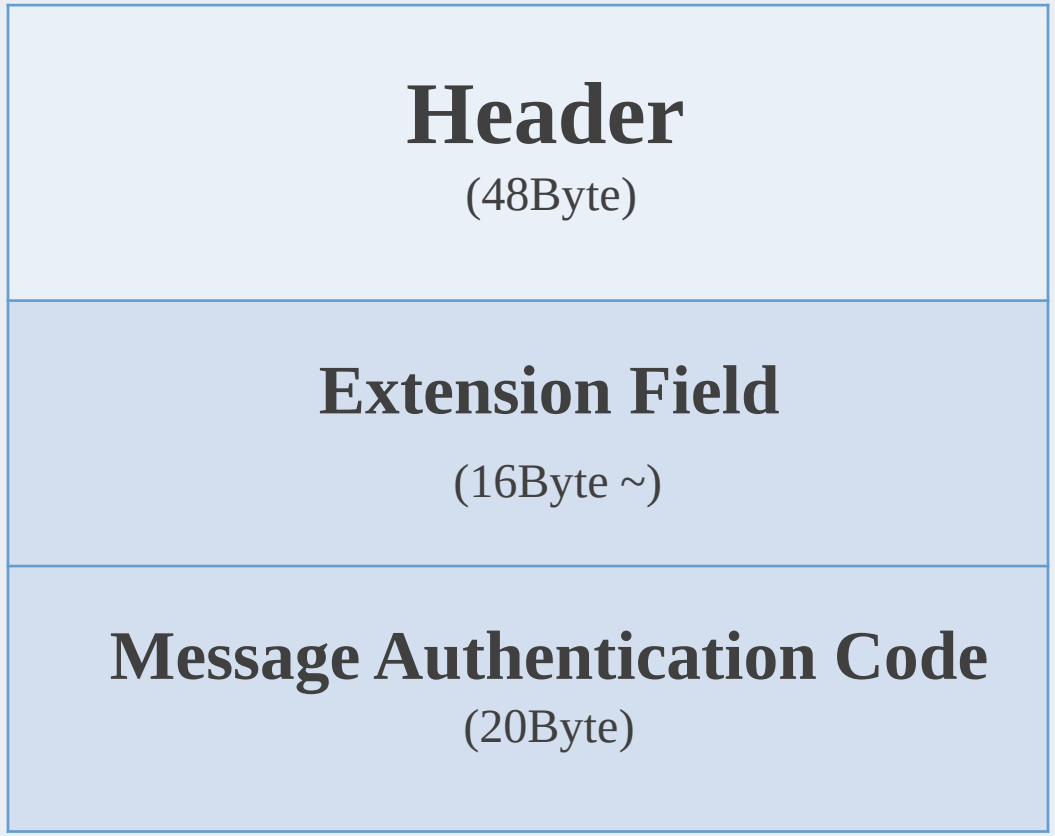
NTPを不正秘匿通信手法として悪用する脅威モデルを検討する

02　Network Time Protocol

Network Time Protocolの概要

- **NTP (Network Time Protocol)**
  - ネットワークに接続する機器の時刻を同期するプロトコル
  - 一般にUDPの123番ポートを使用する
  - Stratumを用いた階層構造をもつ
  - 複数のバージョンが存在するが，本研究においては
    現行バージョン（NTP version 4, RFC 5905）を使用する

NTPパケットフォーマット



- 3つのコンポーネントから構成
  - **Header**
    - NTPの標準ヘッダー
  - **Extension Field（拡張フィールド）**
    - RFC 7822
    - 標準ヘッダーでは伝達されない追加情報を提供できる
  - **Message Authentication Code（MAC）**
    - RFC 8573
    - NTP認証を行う際に利用される
      - RFC 7822に補足情報あり

03　NTPトンネリングの脅威モデル

NTPトンネリングの定義

- NTPトンネリング
  - NTPを不正秘匿通信手法として悪用する
    - 組織の監視網による検知の回避
    - NTPのパケットフィールドにコマンドやデータを挿入
    - NTPによる時刻同期の通信に偽装
  - **NTPの特性を悪用**
    - アーキテクチャ（クライアントサーバモデル）
    - パケットフォーマット（MACフィールド）
      - NTP認証のパケットに偽装して双方向通信を検討

NTP認証

- MACフィールドにNTPから求めたハッシュ値を挿入することで,パケットの改ざんや送信元を認証する

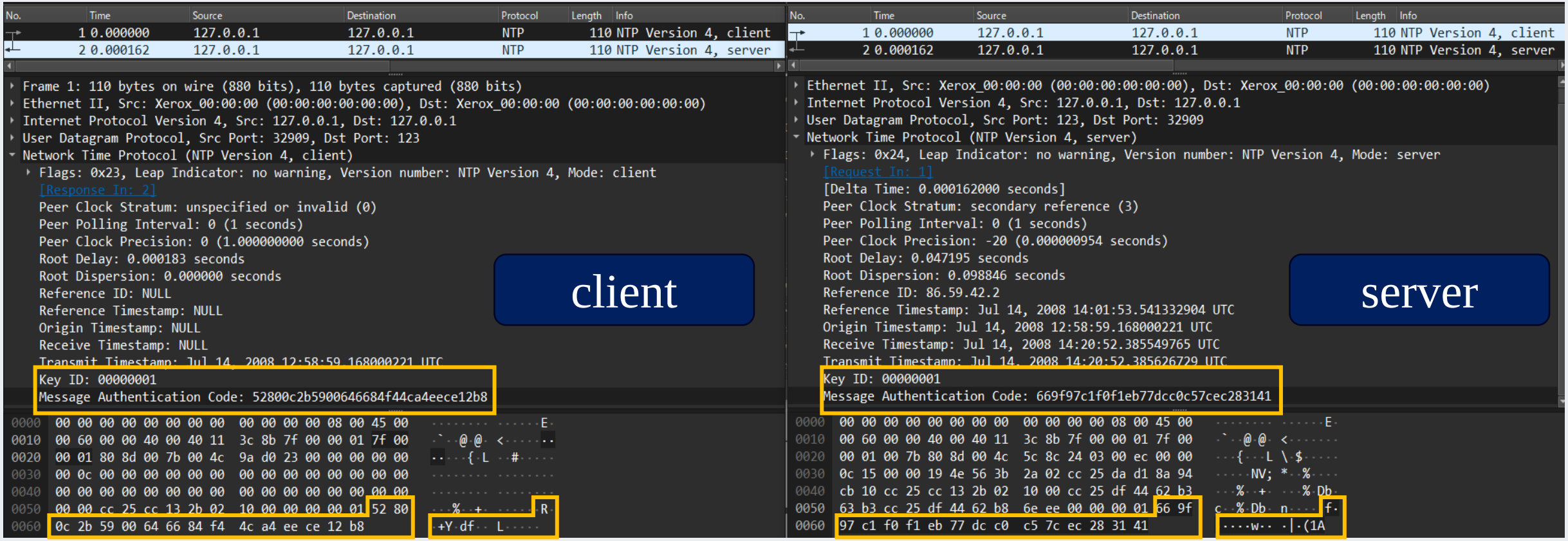
- MACフィールド
  - NTPパケットの最後の部分に位置するオプションフィールド
  - フィールドフォーマット
    - Key Identifier : 使用する鍵の指定（4桁の数字）
    - dgst : 鍵とNTPパケットから求めたハッシュ値を挿入

Key Identifier (32bit)
dgst (128bit*)

* 機器間で同意があれば128ビット以上を挿入可能

正常時のNTP認証パケット

両パケットのMACには，MD5暗号化キー「foobar」で求めたハッシュが挿入

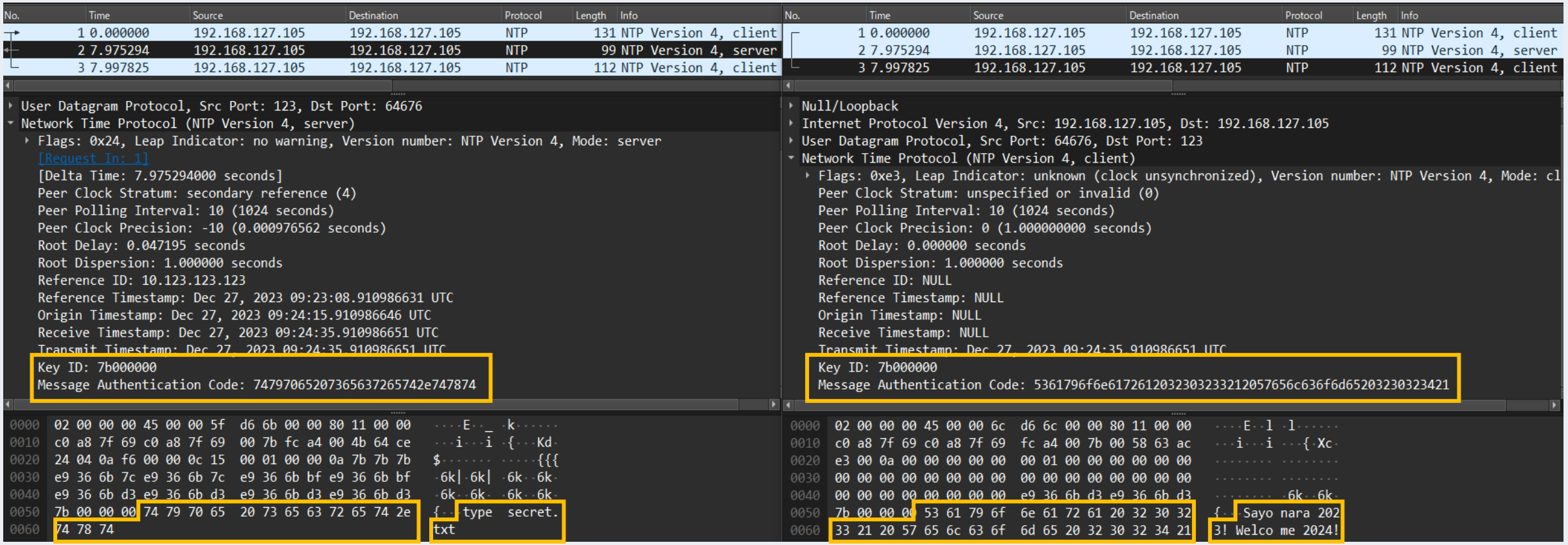


Wireshark (NTPパケット)
https://wiki.wireshark.org/NTP

NTPトンネリングによるC2パケット

C2 server

client



MACにコマンドを挿入してクライアントに送信
コマンド：type secret.txt

MACにコマンド出力を挿入してC2サーバに送信
コマンド出力：Sayonara 2023! Welcome 2024!

https://youtu.be/lrATb5BWoIE

04　NTPトンネリングへの対策

NTPトンネリング対策の提案

対策案）内部NTPサーバの必須化

- 以下の3つの要件を満たす
  - ① 内部にNTPサーバあるいはNTPサーバ機能をもつネットワーク機器を設置する
  - ② 外部のNTPサーバを参照できるのは内部NTPサーバのみとする
  - ③ 内部のNTPサーバを除くすべてのNTPパケット外部送信を拒否する

NTPトンネリング対策案の評価

対策案）内部NTPサーバの必須化

- 「検知できるか」ではなく「必要のない通信を遮断」する
- 実運用を加味した対策のため
  - 導入が容易でかつ迅速に行える
  - NTPの既存システムを変えず対策を導入できる
- NW機器でも代用できるため中小規模組織でも対策が可能

対策案は有効である

05　結論

まとめ

- 直接的に関係のないデータやコマンドをプロトコルに挿入して無害な通信に偽装する通信手法の総称不正秘匿通信手法と定義
- 不正秘匿通信手法の共通要素を分析し，Network Time Protocolが脅威になり得ることを明らかにした
- NTPを用いる不正秘匿通信手法，NTPトンネリングの脅威モデルを実装し，その脅威と有効性を確認した
- NTPトンネリングの対策案を提案
  - 内部NTPサーバの必須化
    ① 内部にNTPサーバあるいはNTPサーバ機能をもつネットワーク機器を設置する
    ② 外部のNTPサーバを参照できるのは内部NTPサーバのみとする
    ③ 内部のNTPサーバを除くすべてのNTPパケット外部送信を拒否する

Future Work

今後について

- 新たな不正秘匿通信手法の模索
  - QUIC (Quick UDP Internet Connection)
  - HTTP/3 (Hypertext Transfer Protocol version 3)
  - Transport Layer Security (TLS)

貢 献

- NTPに対するセキュリティ意識の認知向上
- 不正秘匿通信手法の認知度向上
- 攻撃者による不正秘匿通信手法の抑制

Thank you.