

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
- 02 Network Time Protocol
- 03 NTP トンネリングの脅威モデル
- 04 NTP トンネリングへの対策
- 05 結論

# 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

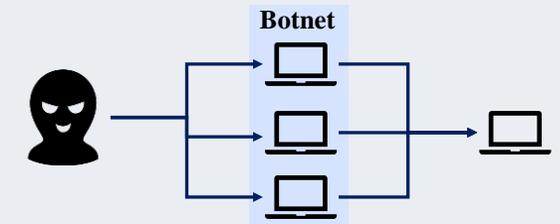
- 機密情報の奪取
- 踏み台
- コネクトバック通信
- 監視網による検知の回避

etc.

### • 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



# 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

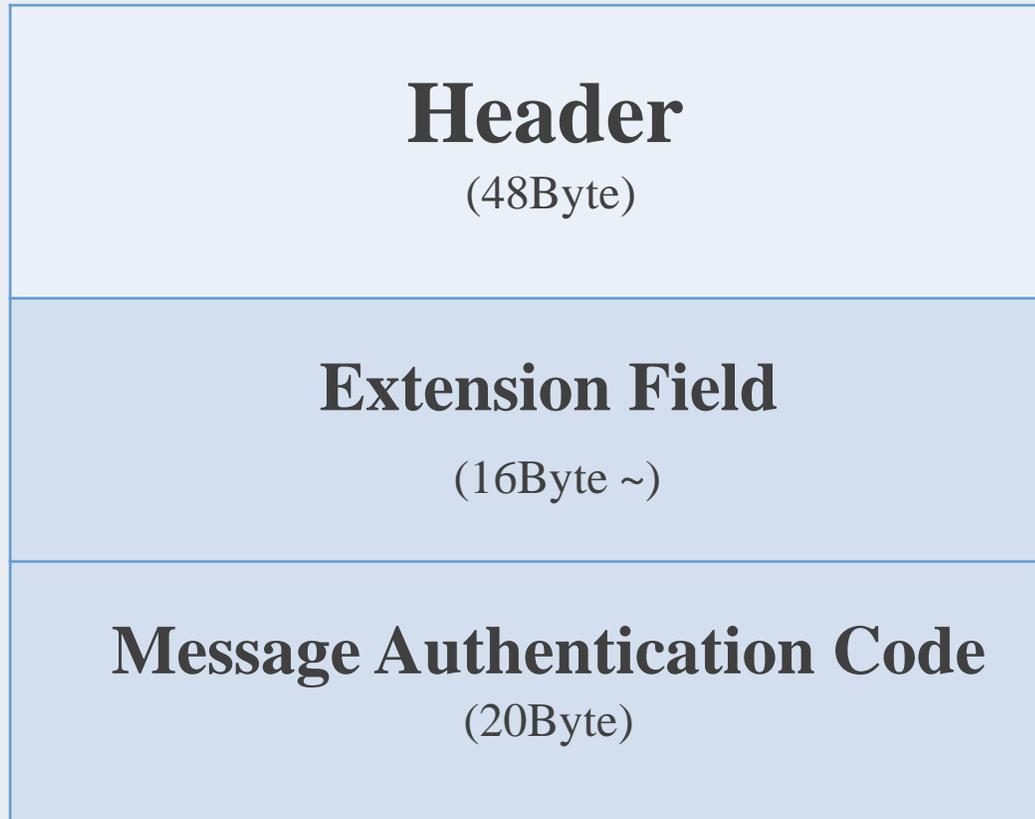
---

- **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

<b>Key Identifier (32bit)</b>
<b>dgst (128bit*)</b>

\* 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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	NTP	110	NTP Version 4, client
2	0.000162	127.0.0.1	127.0.0.1	NTP	110	NTP Version 4, server

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	NTP	110	NTP Version 4, client
2	0.000162	127.0.0.1	127.0.0.1	NTP	110	NTP Version 4, server

client

```

Network Time Protocol (NTP Version 4, client)
  Flags: 0x23, Leap Indicator: no warning, Version number: NTP Version 4, Mode: client
  [Response In: 2]
  Peer Clock Stratum: unspecified or invalid (0)
  Peer Polling Interval: 0 (1 seconds)
  Peer Clock Precision: 0 (1.000000000 seconds)
  Root Delay: 0.000183 seconds
  Root Dispersion: 0.000000 seconds
  Reference ID: NULL
  Reference Timestamp: NULL
  Origin Timestamp: NULL
  Receive Timestamp: NULL
  Transmit Timestamp: Jul 14, 2008 12:58:59.168000221 UTC
  Key ID: 00000001
  Message Authentication Code: 52800c2b5900646684f44ca4eece12b8
          
```

server

```

Network Time Protocol (NTP Version 4, server)
  Flags: 0x24, Leap Indicator: no warning, Version number: NTP Version 4, Mode: server
  [Request In: 1]
  [Delta Time: 0.000162000 seconds]
  Peer Clock Stratum: secondary reference (3)
  Peer Polling Interval: 0 (1 seconds)
  Peer Clock Precision: -20 (0.000000954 seconds)
  Root Delay: 0.047195 seconds
  Root Dispersion: 0.098846 seconds
  Reference ID: 86.59.42.2
  Reference Timestamp: Jul 14, 2008 14:01:53.541332904 UTC
  Origin Timestamp: Jul 14, 2008 12:58:59.168000221 UTC
  Receive Timestamp: Jul 14, 2008 14:20:52.385549765 UTC
  Transmit Timestamp: Jul 14, 2008 14:20:52.385626729 UTC
  Key ID: 00000001
  Message Authentication Code: 669f97c1f0f1eb77dcc0c57cec283141
          
```

# NTP トンネリングによるC2パッケージ

C2 server

client

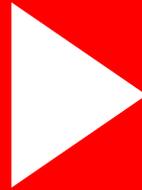
No.	Time	Source	Destination	Protocol	Length	Info	No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.127.105	192.168.127.105	NTP	131	NTP Version 4, client	1	0.000000	192.168.127.105	192.168.127.105	NTP	131	NTP Version 4, client
2	7.975294	192.168.127.105	192.168.127.105	NTP	99	NTP Version 4, server	2	7.975294	192.168.127.105	192.168.127.105	NTP	99	NTP Version 4, server
3	7.997825	192.168.127.105	192.168.127.105	NTP	112	NTP Version 4, client	3	7.997825	192.168.127.105	192.168.127.105	NTP	112	NTP Version 4, client

C2 server							client						
User Datagram Protocol, Src Port: 123, Dst Port: 64676 Network Time Protocol (NTP Version 4, server) Flags: 0x24, Leap Indicator: no warning, Version number: NTP Version 4, Mode: server [Request In: 1] [Delta Time: 7.975294000 seconds] Peer Clock Stratum: secondary reference (4) Peer Polling Interval: 10 (1024 seconds) Peer Clock Precision: -10 (0.000976562 seconds) Root Delay: 0.047195 seconds Root Dispersion: 1.000000 seconds Reference ID: 10.123.123.123 Reference Timestamp: Dec 27, 2023 09:23:08.910986631 UTC Origin Timestamp: Dec 27, 2023 09:24:15.910986646 UTC Receive Timestamp: Dec 27, 2023 09:24:35.910986651 UTC Transmit Timestamp: Dec 27, 2023 09:24:35.910986651 UTC Key ID: 7b000000 Message Authentication Code: 74797065207365637265742e747874							Null/Loopback Internet Protocol Version 4, Src: 192.168.127.105, Dst: 192.168.127.105 User Datagram Protocol, Src Port: 64676, Dst Port: 123 Network Time Protocol (NTP Version 4, client) Flags: 0xe3, Leap Indicator: unknown (clock unsynchronized), Version number: NTP Version 4, Mode: cl Peer Clock Stratum: unspecified or invalid (0) Peer Polling Interval: 10 (1024 seconds) Peer Clock Precision: 0 (1.000000000 seconds) Root Delay: 0.000000 seconds Root Dispersion: 1.000000 seconds Reference ID: NULL Reference Timestamp: NULL Origin Timestamp: NULL Receive Timestamp: NULL Transmit Timestamp: Dec 27, 2023 09:24:35.910986651 UTC Key ID: 7b000000 Message Authentication Code: 5361796f6e6172612032303233212057656c6366f6d65203230323421						
<pre> 0000 02 00 00 00 45 00 00 5f d6 6b 00 00 80 11 00 00  ....E.._k..... 0010  c0 a8 7f 69 c0 a8 7f 69 00 7b fc a4 00 4b 64 ce  ...i..i...{...Kd. 0020  24 04 0a f6 00 00 0c 15 00 01 00 00 0a 7b 7b 7b  \$.....{{ 0030  e9 36 6b 7c e9 36 6b 7c e9 36 6b bf e9 36 6b bf  6k 6k 6k6k 0040  e9 36 6b d3 e9 36 6b d3 e9 36 6b d3 e9 36 6b d3  6k6k6k6k 0050  7b 00 00 00 74 79 70 65 20 73 65 63 72 65 74 2e  {...type secret. 0060  74 78 74  txt                     </pre>							<pre> 0000 02 00 00 00 45 00 00 6c d6 6c 00 00 80 11 00 00  ....E..l.l..... 0010  c0 a8 7f 69 c0 a8 7f 69 fc a4 00 7b 00 58 63 ac  ...i..i...{Xc. 0020  e3 00 0a 00 00 00 00 00 00 01 00 00 00 00 00 00  ..... 0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..... 0040  00 00 00 00 00 00 00 00 e9 36 6b d3 e9 36 6b d3  .....6k6k 0050  7b 00 00 00 53 61 79 6f 6e 61 72 61 20 32 30 32  {...Sayo nara 202 0060  33 21 20 57 65 6c 63 6f 6d 65 20 32 30 32 34 21  }! Welco me 2024!                     </pre>						

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.