福岡大学におけるDNSセキュリティの取り組み

福岡大学 情報基盤センター
藤村 丞（ふじむら しょう）
fujimura@fukuoka-u.ac.jp

福岡大学情報基盤センターマスコットキャラクター ナナクマ君

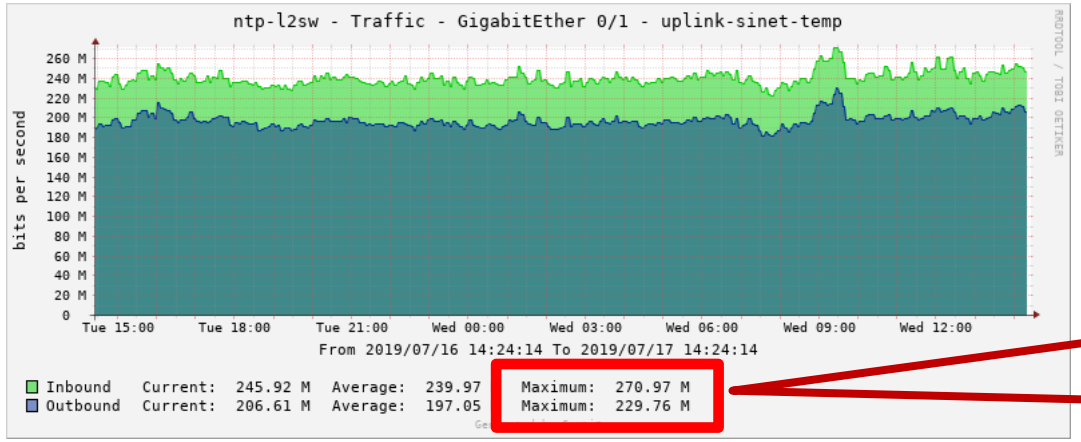
福岡大學
FUKUOKA UNIVERSITY

自己紹介

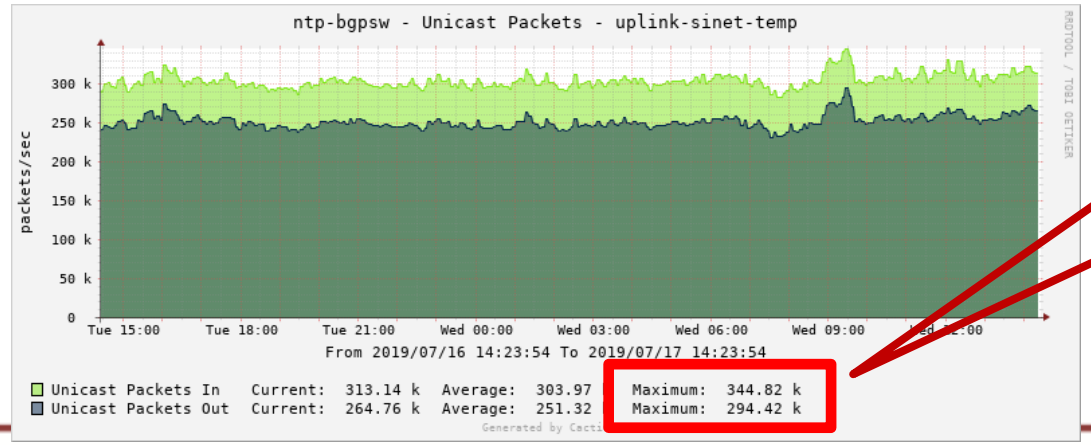
- 名前
  - 藤村 丞（ふじむら しょう）
  - 『丞』…人名用漢字、JIS第1水準
- 所属
  - **福岡大学 情報基盤センター 専任教員**
- 担当（各種サポート含む）
  - **キャンパスネットワーク、ネットワークセキュリティ、認証基盤など基盤系**
  - 学内情報システム全般（医療系オーダリング以外）
- 公開NTPサービス
  - https://www.itc.fukuoka-u.ac.jp/i/service/special/public_ntp

トラフィック量

- 2019年7月16日-17日

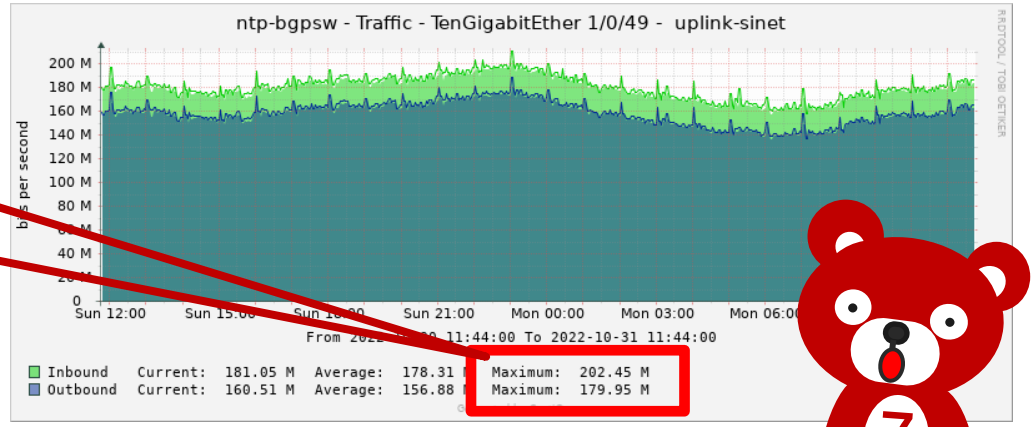


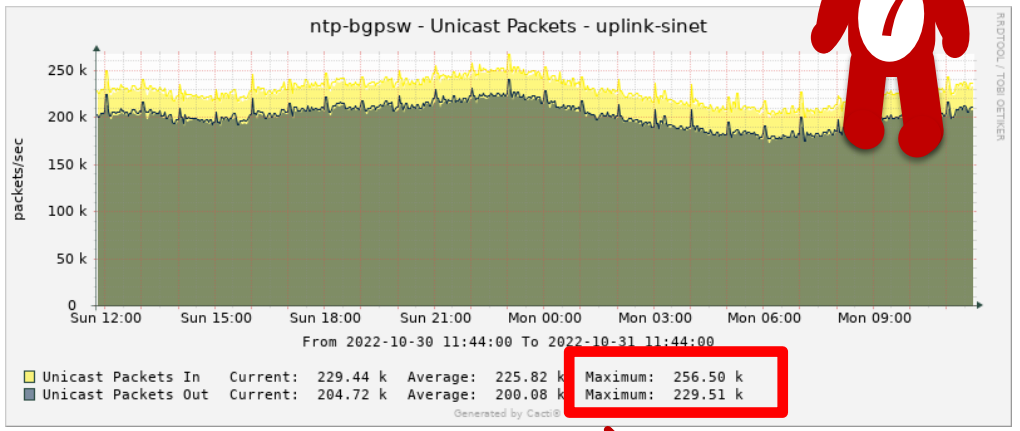
Inbound:
270.97 Mbps
Outbound:
229.76 Mbps



Inbound:
344,820 pps
Outbound:
229,760 pps

Inbound:
202.45 Mbps
Outbound:
179.95 Mbps





- 2022年10月30日-31日

Inbound:
256,500 pps
Outbound:
229,510 pps

本日の目次

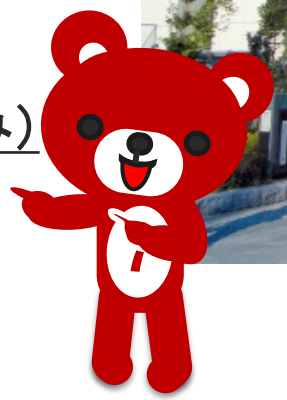
- ネットワーク構成やトラフィックなどの規模感
- DNSセキュリティの取り組み

- みなさまのご意見や状況などをお聞かせください！

福岡大学とは
（IPアドレスとAS）

福岡大学とは

- **私立大学**（創立88周年）
- **所在地：福岡県福岡市**
  - 地下鉄七隈線で都心から16分
- 学部数：9学部（31学科）
- 研究科数：10研究科（33専攻）
- **学生数：約19,200名（大学+大学院）**
- 大学病院 3病院
- 附属高等学校 2校、附属中学校 1校
- ネットワーク構成
  - **IPv4：133.100.0.0/16**
  - **IPv6：2405:be00::/32（全学に展開済み）**
- **AS18148（キャンパスネットワーク）**
  AS63785（公開NTPサービス）
  - SINETと10Gbps x2にて接続



ネットワーク構成

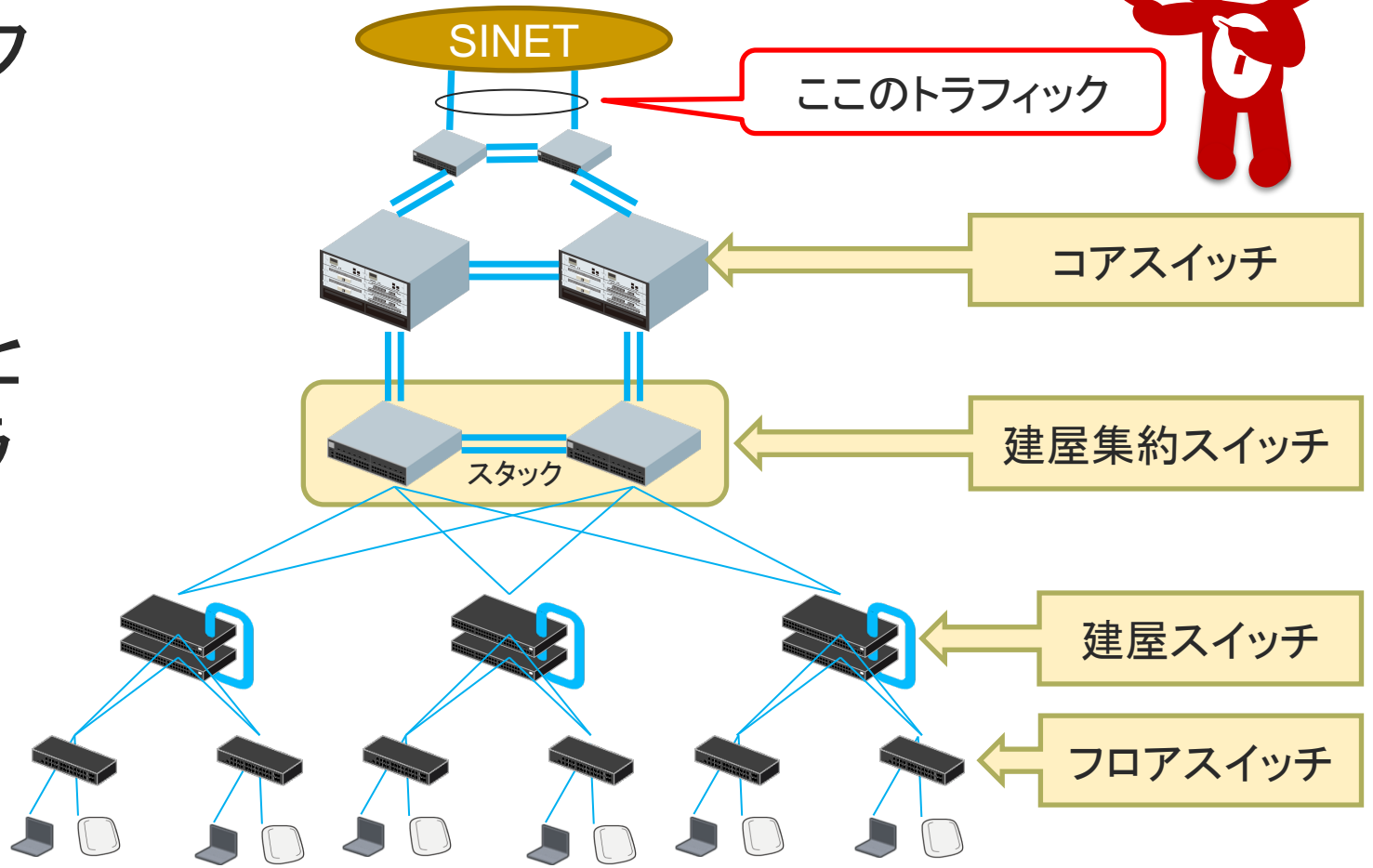
キャンパスネットワーク構成

- ネットワークスイッチ
  - **合計で約420台、無線LANは約630台**
- インターネット接続はSINETに10Gbps 2回線で接続
- SINET接続から建屋スイッチまでは冗長構成
  - 建屋集約まではマシン室も別々
- 各建屋スイッチと建屋集約スイッチは1Gbps x2（リンクアグリゲーション）
- **講義期間中は約2.5万台（推定）超のデバイスが接続**

トラフィック量について

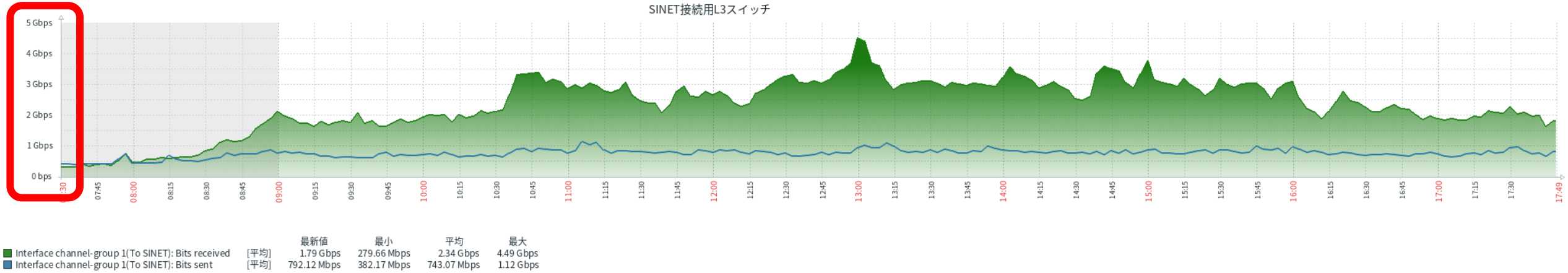
インターネット接続トラフィック量（1/2）

- SINET接続のトラフィック
  - SINET
    - 学術情報ネットワーク
- キャンパスネットワークとインターネット接続のトラフィック



インターネット接続トラフィック量（2/2）

- ピークはおおよそ4.5Gbpsから5Gbpsの間
  - 5分平均なので瞬間最大風速はまだ上の値（のはず）
- 時間帯は13:00頃



ネットワークセキュリティ
（DNSセキュリティ）

DNSSEC

- 2015年9月より
  - **DNSキャッシュサーバによるDNSSECの署名検証開始**
  - **DNSコンテンツサーバによるDNSSECの署名開始**
    - 情報基盤センター管理分のみ（マスターゾーンのみ）
  - ただし2015年には設定ミスにより鍵の更新に失敗し…
    - DNSSECを一時的にOFFにすることにより回避
  - **運用開始後1年間程度は数件の問い合わせ（接続できない）**
- 課題
  - **スレーブゾーンへの署名適用**
  - **逆引きゾーンへの署名適用**

OP53B（Outbound Port 53 Blocking）

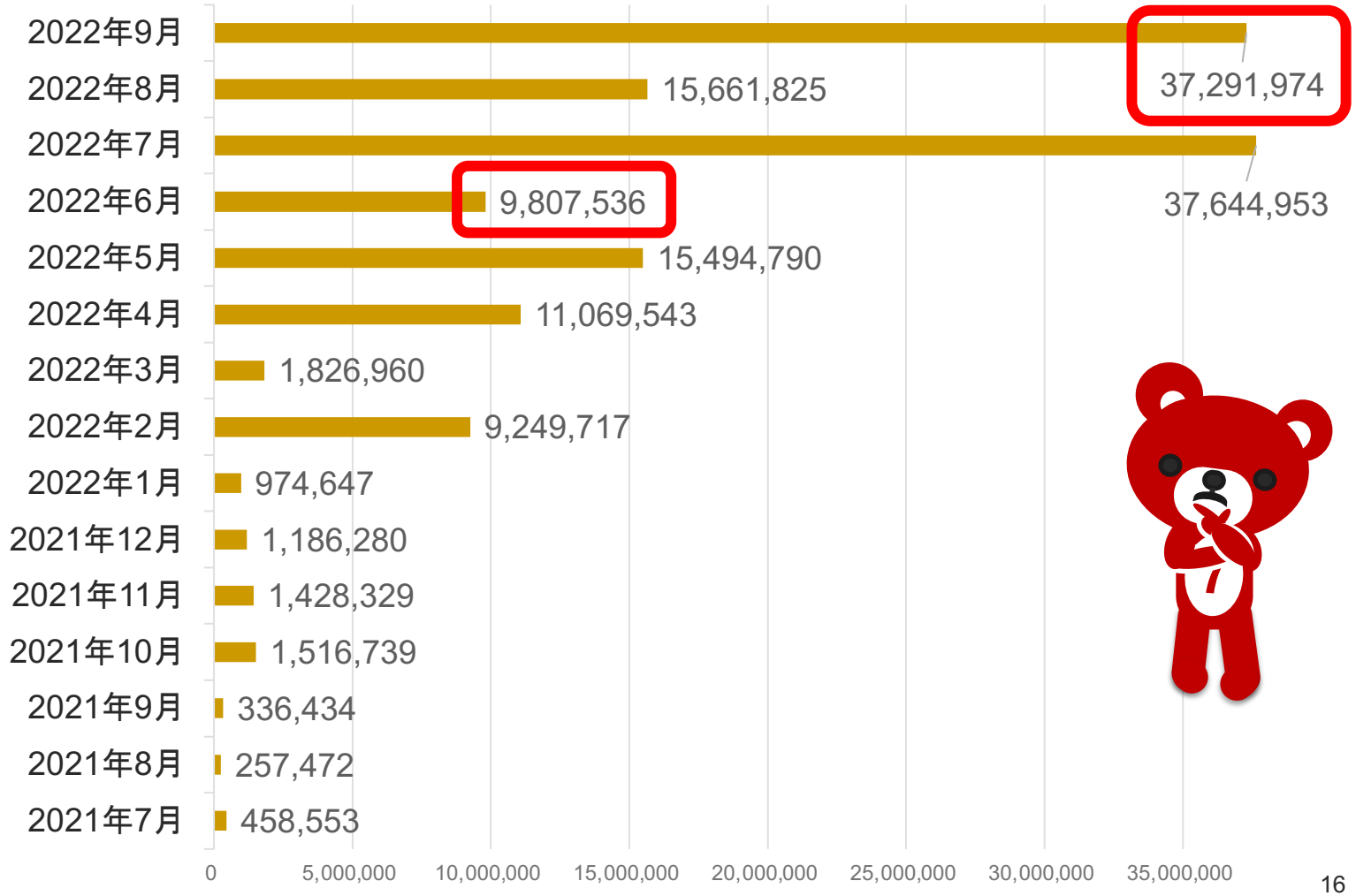
- 2020年9月より
  - **外向き（インターネット向け）TCP/UDP53番ポート（DNS）の遮断**
  - **マルウェアによる不正なサイトへの誘導や情報漏洩などから守るため**
  - **後述の DNS Firewall の導入効果を高めるため**
  - Public DNS サーバへは接続できない
  - DNS運用者へはforwardersの設定マニュアルを作成・配布
  - 回避手段として解除申請を設けている
    - 今のところ申請は1件のみ --> 今年度内に廃止予定
- 課題
  - 2022年9月現在
    特に問い合わせや運用課題になるような事象は起きていない

DNS Firewall

- 名前解決をするタイミングでフィッシングサイトや偽サイト、マルウェアをダウンロードさせるサイトなど、**悪意のあるサイトへのアクセス（名前解決）と検知した場合、自動的に通信を止め**（名前解決を行わず）、悪意ある攻撃の前段階で攻撃をブロックする仕組み
  - **C&C サイト**
  - **ウイルス、マルウェア配布サイト**
  - **DoS（Denial of Service attack）攻撃用サイト**
  - **Bogon space（割当てられていないアドレススペースの応答）**
  - **DoH（DNS over HTTPS）サイト**

DNS Firewall 利用分析

- DNS Firewallでのブロック数
  - 推定2.5万台が対象
  - 名前解決を行わなかったクエリ数
- DoHの遮断もこれで行っている
  - DNS over HTTPS
- 一定の効果を得ていると考えている



NSAが企業ネットワークでのDoHの利用に警告（1/2）

- 米国家安全保障局（NSA）は2021年1月14日、DNS-over-HTTPS（DNSプロトコルの暗号化）の持つリスクを説明するアドバイザリを公開
- NSAからの注意喚起
  - **DoHを使用しても攻撃者がユーザーのトラフィックを完全に見られなくなるわけではない**
  - ネットワークの内部で使用した場合、**従来の（平文の）DNSトラフィックを調べることで脅威を検知している多くのセキュリティツールの働きを阻害する恐れ**がある
  - **今日のDoHを使用可能なDNSサーバの多くは、**企業ネットワークの外部にホストされているため、企業の**制御下にはなく監査を行うこともできない**

https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF

NSAが企業ネットワークでのDoHの利用に警告(2/2)

- 米国家安全保障局(NSA)は2021年1月14日、DNS-over-HTTPS(DNSプロトコルの暗号化)の持つリスクを説明するアドバイザリを公開
- NSAからのアドバイス
  - 社内ネットワークでは**暗号化されたDNSを使用するのを避けるか、DoHを**使用可能なDNSサーバを使用する場合には、少なくとも社内でホストし、**自社の制御下に置く**べきである
  - **企業ネットワークのDNSトラフィックは暗号化されているかどうかに関わらず、指定された(信頼された)DNSリゾルバーだけに送信する**ようにすることを勧める
    - **他の全てのDNSサーバは無効化するか、ブロックすべきである**

https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF

DoHのブロック理由

- **DoHを悪用するマルウェアが存在**
  - C2とのトラフィックを隠すためにDoHを利用
  - とあるDoH経由でマルウェアを配布
    - 悪意のあるペイロードを含む「データ」フィールドが存在
- **学内の（正規の）DNSをバイパスすることで、セキュリティ機能の脆弱性が狙われる**
- **契約関係のない（誰が作ったかわからない）DNSサーバに名前解決を依頼することができるか…？**
  - NTPサービスも同じ
    - システムにとって大事な時刻を誰に任せるか？
- **信頼されたDNSキャッシュサーバへのみクエリを送信するべきである**

DNS Firewallの課題

- **悪意のあるサイトの名前解決を行おうとしたクライアントへの対応**
  - FU-CSIRTでは人手が圧倒的に足りない（検知の数が多すぎる…）
  - 運用に乗せられていない
- **IP指定のDoH と DoT（DNS over TLS）の取り扱い**
  - 今のところDoHのDNS Firewallでの（名前解決での）ブロックのみ
- 自前のDoHとDoTを提供する？
  - これはもう少し考えたい（様子を見たい）
- 2022年10月現在
  DoHに関係する問い合わせや運用課題になるような事象は起きていない

さいごに

- DNSセキュリティの導入効果を確認できた
- 運用課題はたくさんある
  - 一度には解決できないが、できるところから考えていきたい
- ネットワークセキュリティについては攻撃および防御手法の移り変わりが激しい
  - 最新の情報収集は怠らず
  - 組み込めるところやチューニングなどは随時行っていきたい
- **常に改善点を求めていきたい**
- **ぜひみなさまのご意見・情報交換をさせていただきたい**

人をつくり、時代を拓く。

福岡大学

ご清聴ありがとうございました！


7