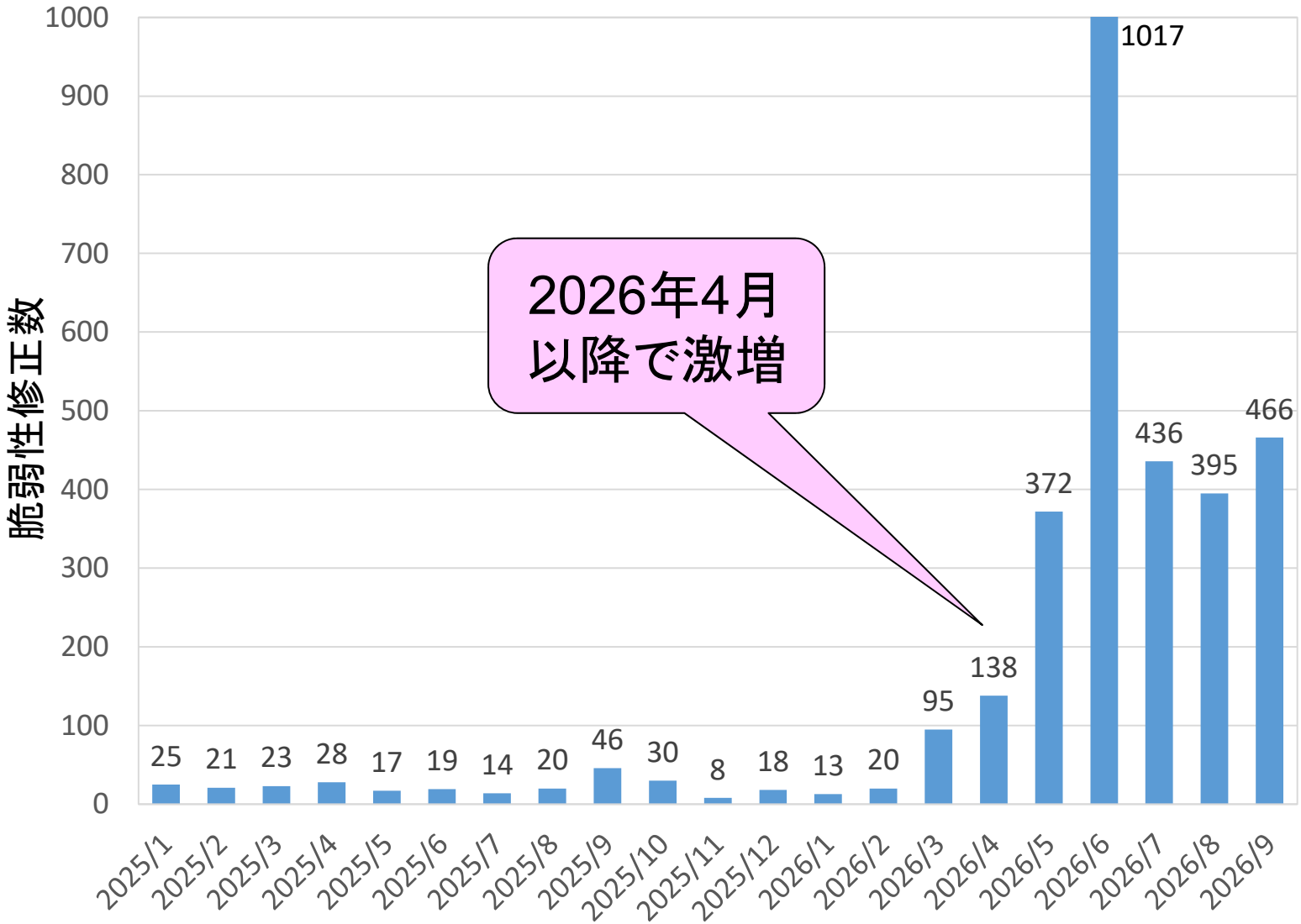
最近のサイバーセキュリティ事情

名古屋大学 情報基盤センター
情報基盤ネットワーク研究部門
基盤ネットワーク研究グループ
嶋田 創

概要

- Claude Mythosによる世界の変化
  - 直近の脆弱性発見祭りの起因
  - 他のLLMやLocal LLMなどによる模倣
  - 更新できないネット接続機器のセキュリティリスク激増
- いい加減なアプリが表面化
- プライバシーのための暗号化の推進
- アプリに入れられたResidential Proxyの悪用の増加

あるWebブラウザの脆弱性修正数の月別集計



脆弱性探査に特化したor強いAIモデルの出現

いわゆるAIによる脆弱性探査は昔から試みられていた

- Sync Deep Code AI (2020): コードレビューベースで脆弱性探査と分析
- Semgrep AppSec (2020): コード解析ベースの脆弱性探査と分析

その他、コーディングサポートAIの多くが脆弱性探査を備える

⋮

今年の春に非常に強力なAIモデルが登場

- **Anthropic Claude Mythos (2026/4)**: 汎用モデルながら当初から脆弱性探査に強いことをアピールしたAIモデル
  - 単純な脆弱性探査のみならず、攻撃の実現の検証までの、複数段階の手順を構築可能

世界を変えた

- 「AIを使ってあそこまでできるのか」「自分の手持ちもいろいろ組み合わせて模倣したい」という動きが出た
  - Artex, Cairn, Strixなどが夏ぐらいから同レベルになってきている
  - ArtexとCairnは実際に攻撃に使われた痕跡がある[1,2]
- なお、本家の商用LLMの方は夏あたりから安全装置(ガードレール)が相当厳しくなって来ている
  - /.well-known/security.txt(RFC 9116)に許可設定入れないと絶対に無理
- こいつらが頑張った結果の被害(の発覚)が9月末から続いている

[1] https://piyolog.hatenadiary.jp/entry/2026/10/23/065256
[2] https://piyolog.hatenadiary.jp/entry/2026/10/06/121225

いつまで続く?

- 各ソフトウェアに脆弱性が無限にあるわけではない
- 活発に更新されている物は、しばらくすれば脆弱性発見も昔のペースに落ちつくのでは
  - WindowsもiOSもLinuxカーネルも毎回すごい数の修正が入る
- ただし、更新されない(できない)物の脆弱性は発見されても修正されない
  - これを機会にお金をかけて新しく活発に更新されている物ベースにしないといけない
  - もっと言えば、余計な機能(脆弱性のもと)はありがたくない時代になる

更新できないネット接続機器のリスクが激増

- 古いソフトウェアや古いファームウェアな機器をだましだまし使うリスクが激増
  - 産業機器とか医療機器とかはクローズドネットワークでだましだまし使っている機器が多そう
- 古い機器とかは、「使っている人が少ないから脆弱性探してもなぁ…」で後回しになっていたのが無くなるのもきつい
  - AIペネトレーションは疲れ知らずかつ人手に比べて低コストで脆弱性探査できる
- 「便利機能で何々入れておきました」のリスクも激増
  - 後の話題で「右肩上がりで機能拡張」を批判している(ずっと批判してきた)が…
  - PHP2shellで「UIをPHPで作っておきました」なアプライアンスがすごく面倒なことに

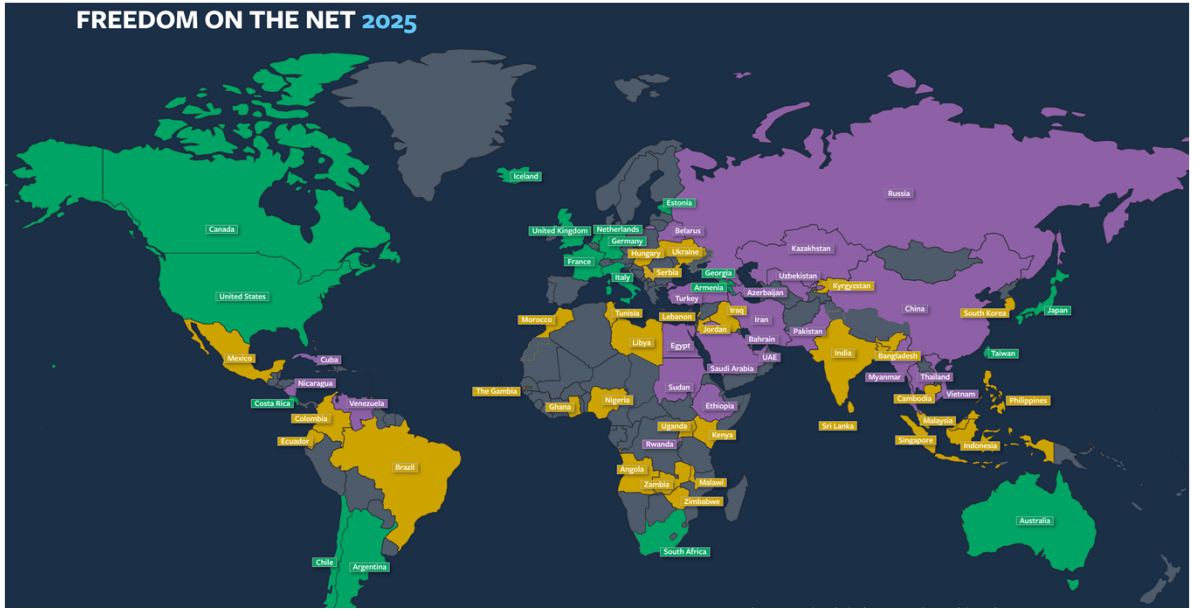
いい加減なアプリの表面化

- 10月冒頭に「いい加減に作られたアプリを解析してWebサービス攻撃の起点にしているのでは」という話[1,2]
  - アプリのバックエンドはRESTなどWeb APIベースが多い
  - APIキー、認証関係、検証環境接続先、旧API、バックドア(公式)、クラウド資源(DBなど)、の接続先(URI)をを含む情報が容易に見れたり
- 実際にセキュリティ技術者がAI使ってアプリ解析してみた報告(某シンポジウムのBoF)だと…
  - アプリ100件をダウンロードからレポートまで自動化して3.5時間で完了してしまう(4並列実行)
  - 認証とかAPIの鍵とか特にヤバそうなものが検出されたのが2割弱

[1] https://www.jpcert.or.jp/at/2026/at260030.html
[2] https://security.macnica.co.jp/blog/2026/10/web-incidents2026.html

世界には思ったよりもインターネットコンテンツを検閲をしている国は多い

- Freedom Houseによるレポート[1]によると
  - ソーシャルメディアに検閲が入る国数は22
  - 政治社会信仰コンテンツに検閲が入る国数は45
  - ネットワーク基盤に分離が入れられている国数は17
- もちろん、被害者の人権に影響が多大な違法コンテンツ等をブロックしている国は多い



- 日本のスコアは78で9位
- 緑(Free)でも米国、イギリス、イタリア、ドイツ、オーストラリア、フランスなどは日本より下

[1] Freedom House, "Freedom on the net 2025," 2025.

ということで、自由と安全の両立のための動きは続いている

…が、それをサイバー犯罪者が悪用するのも続く

- (暗号技術自体も悪用されているが、犯罪者追跡の観点から)
- 通信本体: TLS (HTTPS)
  - ただし、現在ではTLSでもSNI(Server Name Identifier)は見える
    →Encrypted SNIが2017年に策定されて徐々に普及中
  - 無料の認証局はサイバー犯罪者にも活用される
- DNS: DNS over TLS, DNS over HTTPS (+QUIC)
  - ESNIに必要なHTTPSレコードを信用のできるDNSから
- IPアドレス: CDN
  - 本来は負荷分散などの目的だが、サイバー犯罪者が(無料枠のある)CDNをオリジナルIPアドレス隠蔽に利用することが

[1] Freedom House, "Freedom on the net 2025," 2025.

ESNI(Encrypted Server Name Identifier)

- 最初の接続(Client Hello)時に接続先サーバ情報SNIは見えてしまう
  - サーバ側の公開鍵を入手するための通信

Time	Source	Destination	Protocol	Lengtl	Info
9.814016	192.168.0.66	133.6.90.81	TCP	54	60715 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
9.815522	192.168.0.66	133.6.90.81	TLSv1.3	2646	Client Hello (SNI=www.net.itc.nagoya-u.ac.jp)
9.830568	133.6.90.81	192.168.0.66	TLSv1.3	675	Application Data

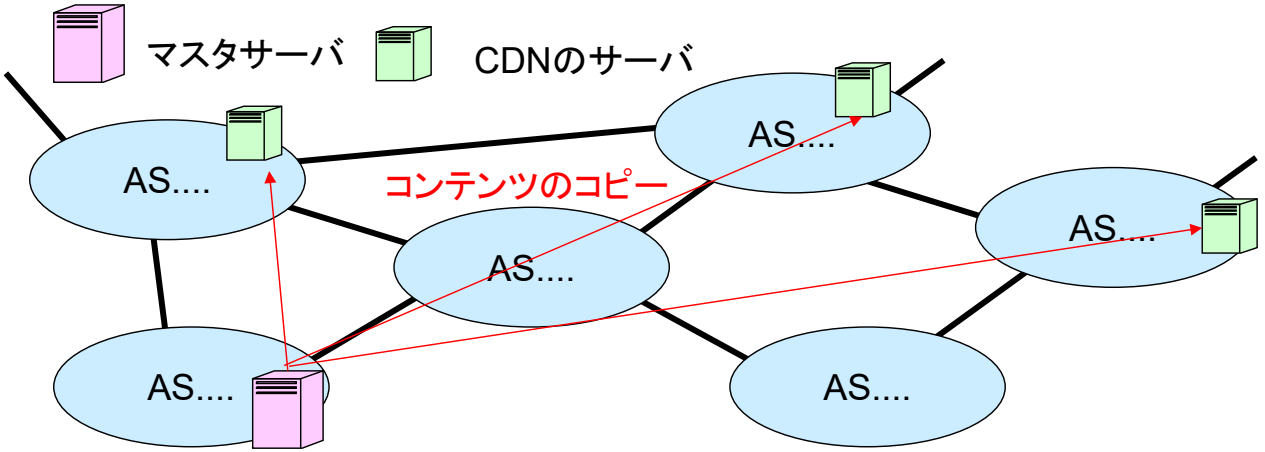
- これを暗号化するのがESNI (RFC 9849)
  - 2018年にドラフト、2026/3にRFC 9849に
- サーバの公開鍵はDNSのHTTPSレコードから入手
  - え? ネットワーク接続時に指定されたDNSを信用して大丈夫なの?
    (悪意のあるDNSの話は情報セキュリティとリテラシ1でやった通り)

DNS over TLS(DoT), DNS over HTTPS(DoH), DNS over QUIC(DoQ)

- 平文のDNSを暗号化するDOS over TLS = DoT(RFC 7858)がベース
  - それをHTTPSでやるのがDNS over HTTPS = DoH(RFC 8484)
  - それをQUICでやるのがDNS over QUIC = DoQ(RFC 9250)
- 提供されるDNSサーバが信頼できない場合、DoHで信頼できる外部DNSサーバを参照できる
  - 盗聴してもただのHTTPS通信にしか見えない
- DoHについては、「DoHを提供しているサーバがそもそも信頼できるか(プライバシー保護の面で)?」という問題がある
  - 私は特に理由が無い限り、日本国内では大学や自分の契約したISPのDNSを使っている
    - ホテル宿泊時は、基本的に大学や自宅にトンネルを掘っている(特に海外)

CDN

- CDNは大規模情報サービスには無くてはならない存在
  - SNSでバズったことによる急激なアクセス集中時の代理対応
  - DDoS攻撃を受けた時に代理被害対応
- 最寄りのCDNのサーバが代理対応(ネットワーク特論B)
- …が、これを攻撃者も悪用することも
  - マルウェアや司令(C&C通信)をCDN経由で配布することも
  - 無料枠のあるCDNが特に悪用されているという噂



何がセキュリティ的にきついか

- これまでネットワーク・フォレンジックで取っていた情報が取れなくなったり効果が
  - DNSクエリログは? →No
  - SNIからの接続先サーバ名は? →No
  - 接続先IPアドレスは? →CDNのIPアドレスで他とごっちゃに
- DoH(有名DoHサーバ)をブロックしたり対策は取れなくも無いが、独自で立てられたら厳しい
- もうクライアント上で暗号化されていない状態をEDRで記録するか無いのでは
  - 一応、UTM/IPSで暗号化をほどく(要全クライアントに追加証明書)手もあるが、経路上で暗号化をほどくと怒るクラウドサービスも多い

アプリに入れられたResidential Proxyの悪用の増加

- (悪性)アプリにProxy機能を設けて、proxy接続利用いくらな商売がブラックマーケットではある
  - AI育成データ集めのスクレイピング
  - サイバー犯罪の踏み台
- ポイ活とか「無料で何々できる」とか釣ってResidential Proxy入りの悪性アプリを配布
- 昨年あたりから話題になっていたが、問題がでかくなったのか対策アライアンスが発足[1]
- 家族とか昔の友人とかで怪しいアプリには注意させて
- 昔はブロードバンドルータなどのIoT機器に設置されることが多かったが、最近はアプリ型も多い

[1] レジデンシャルプロキシ対策アライアンス
https://www.npa.go.jp/bureau/cyber/what-we-do/alliance.html