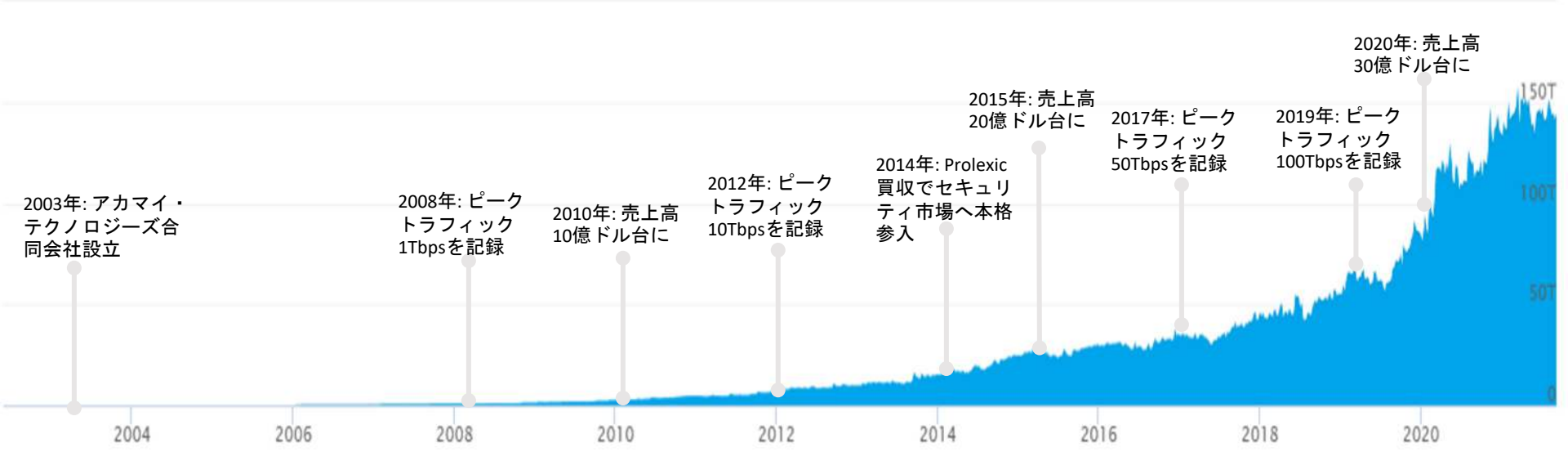
最近の Akamai Blog から

2022 年 6 月 24 日

アカマイ・テクノロジーズ合同会社
松本 陽一

Akamai、約20年の歩み



Akamai Intelligent Edge Platform

世界最大のスケールを有する超分散型のエッジプラットフォーム

いつでもどこでも、アカマイは最も近い場所=エッジから、
優れたセキュリティ、スピード、コンピューティング機能を提供します。

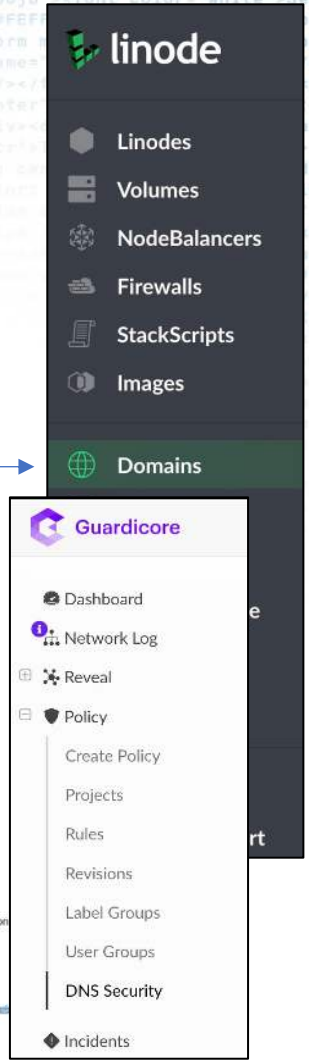
Akamai と DNS

- DNS ソフトウェア
  - DNSi CacheServe / DNSi AuthServe
- DNS サービス
  - Edge DNS / Global Traffic Management / Linode DNS Manager
- DNS によるセキュリティ
  - Secure Internet Access
  - Akamai Guardicore Segmentation
- DNS の応用
  - 各種配信製品や Web セキュリティ製品等におけるエンド・ユーザー・マッピング (他にも CNAME によるオンランプや ACME DNS-01 等 DNSとの関わりは多数..)
- クエリデータの解析による脅威情報分析

New!

New Brand!

New!



Akamai Blog から

Akamai Blog https://www.akamai.com/blog

日本語 https://www.akamai.com/ja/blog
(一部の記事の日本語訳や日本独自記事)

セキュリティを中心に、あらゆるトピックの記事を掲載

- Undetected Attacks on Anti-Malware Agents Using DNS Spoofing (2022/04/14)
  多くのアンチ・マルウェア製品が DNS でファイルの評価を問い合わせることの危険性
- Linode + Akamai が開発者のクラウドの使い方に変革をもたらす理由 (2022/04/12)
  Akamai CEO トム・レイトンの語る Linode 買収のもたらす相乗効果
- Conti のハッカーマニュアル - 読後レビューと分析 (2022/04/05)
  ランサム攻撃集団から流出した情報から読み解く攻撃手法
- TCP Middlebox Reflection: Coming to a DDoS Near You (2022/03/01)
  2021 年に発表された新しいリフレクション攻撃ベクターが現実化

Akamai Blog から – Cybersquatting

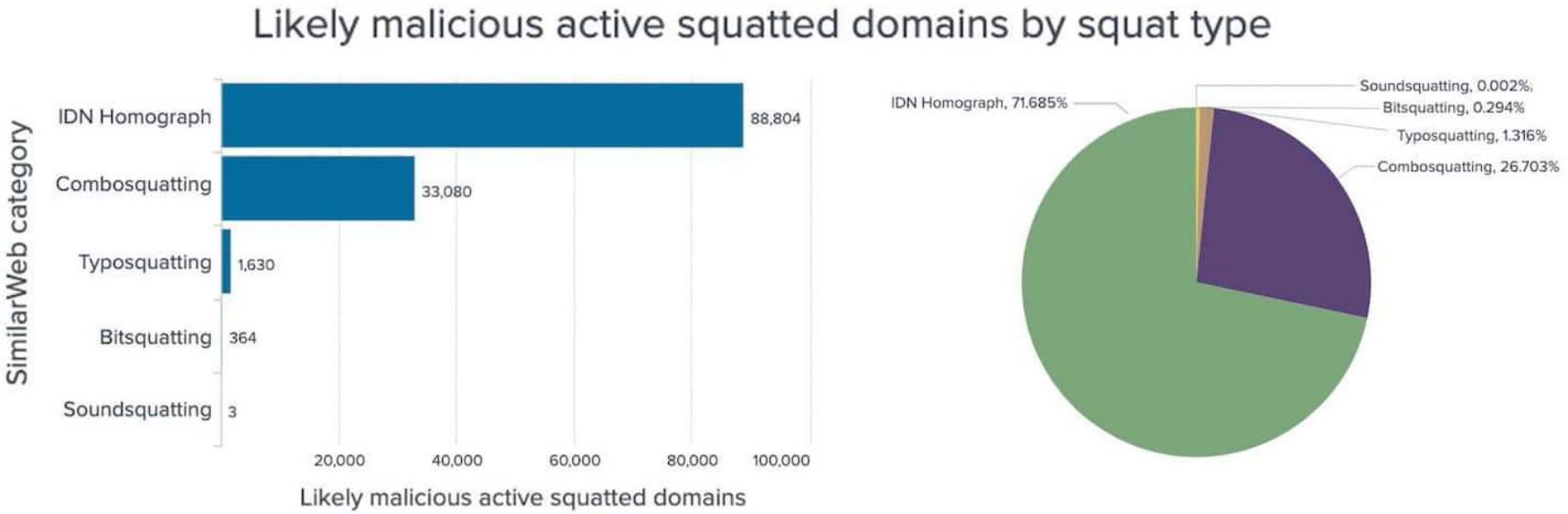
DNS Cybersquatting: The Case for Edge DNS Zone Protect (2022/03/21)

サイバースクワッティング(ドメインスクワッティング) – フィッシング等の不正で用いられる他者のブランドを模倣したドメイン名のバリエーション

- Typosquatting
  打ち間違いを狙う – domain[.]test → domein[.]test
- Combosquatting
  言葉を付け足す – domain[.]test → domainchangepassword[.]test
- Levelsquatting
  階層を付け足す – domain[.]test → domain[.]test[.]test[.]test
- Bitsquatting
  ビットを反転 – domain[.]test → doeain[.]test ("m":01101101 "e":01100101)
- IDN Homograph
  国際化ドメインにより他の言語の似た文字で置き換える – domain[.]test → domáin[.]test
- Soundsquatting
  同じ音の言葉・表現で置き換える – domainforus[.]test → domain4us[.]test

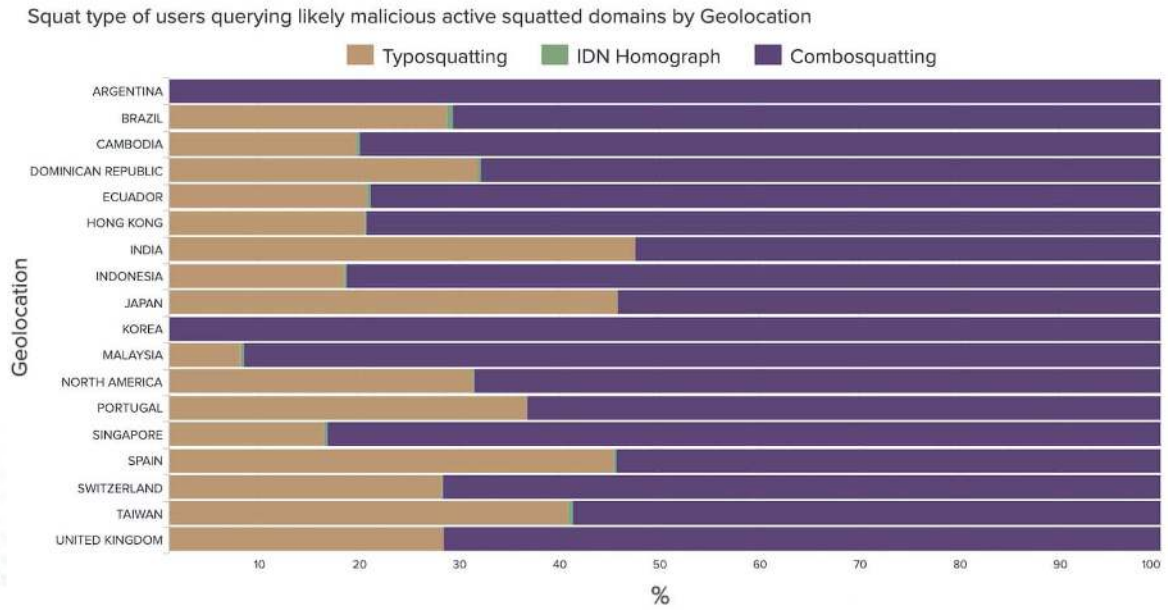
Akamai Blog から – Cybersquatting

実際の不正らしきスクワットドメインはドメイン数にすると
IDN Homograph が多いという調査結果



Akamai Blog から – Cybersquatting

クエリしたユーザーでは Combosquatting や Typosquatting が多い
日本は他の国と比較して Typosquatting が多い？



Akamai Blog から - iCloud Private Relay

Powering and Protecting Online Privacy: iCloud Private Relay and Information for Akamai Customers (2022/03/02)

iCloud Private Relay

Apple が iOS15、iPadOS15、macOS Monterey で iCloud+ ユーザーにベータとして提供する、ユーザーのプライバシーの保護するためのサービス

誰もエンド・ツー・エンドのトラフィックを可視化できないようにするため

- Multiplexed Application Substrate over QUIC Encryption（MASQUE)
- Oblivious DNS over HTTPS (ODoH)

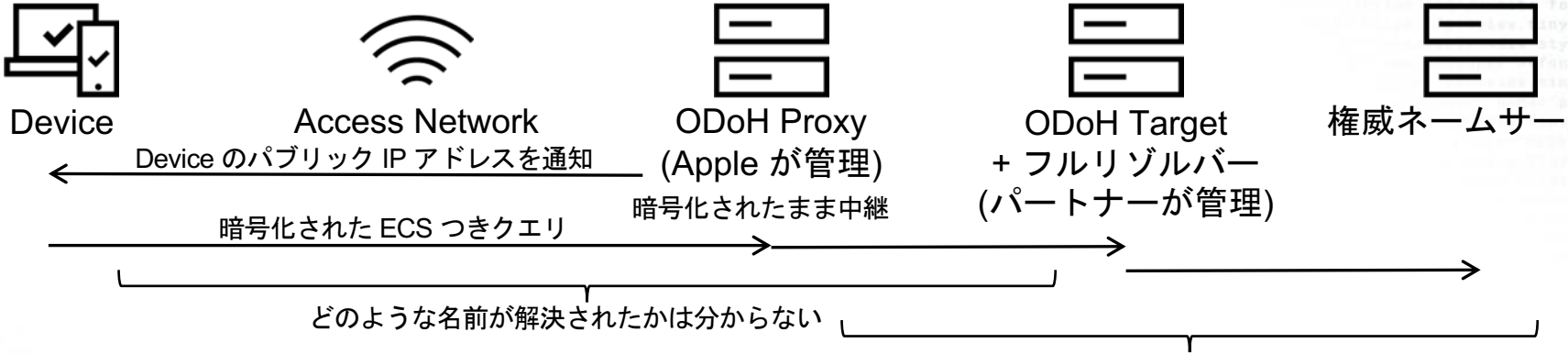
を用いる。詳細は
https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF

エンドユーザーが iCloud Private Relay を用いている場合に Akamai (CDN等) の利用者が意識すべきことを解説

Akamai Blog から - iCloud Private Relay

- 同じユーザーでも IP アドレスが変わるので認証トークンに IP アドレスを用いるのは(今まで以上に)避けるべき
- クライアント IP アドレスや宛先 IP アドレスに依存したサービス(ゼロレーティング等)に課題が生じる
- 各種ジオ IP を用いる場合は Apple 提供のリストが反映されていることを確認 (Akamai Edgescape は反映済)
- IPv6 の方が粒度が細かいのでデュアルスタックをおすすめ
- この仕組みは認証されたデバイスだけが用いることができるようになっており、既存のセキュリティソリューションは引き続き有効

iCloud Private Relay における DNS (ODoH)



Blog からリンクされた Apple の資料によると..

- API や ODoH Proxy の発見以外の名前解決に適用
  (ただし Safari, unencrypted HTTP, custom-encrypted DNS といった例外)
- ODoH Proxy は Apple が管理、ODoH Target はパートナーが管理
- 端末と ODoH Target との間で暗号化が行われる
- ODoH Proxy は暗号化されたクエリを ODoH Target に自分をクライアント IP アドレスとして中継
- ODoH Target がクエリを復号
- クライアントは ODoH Proxy から受け取ったパブリック IP アドレスの情報によりクエリに ECS をつけられる

権威ネームサーバー側で観測されるクエリにも ECS がついている様子(粒度の設定を問わず)


Akamai