JPAAWG 8th General Meeting

- TwoFive から提供する幕の内弁当セッション

マーケット分析とパブリック証明書関連の変更アップデート

DigiCert　林　正人

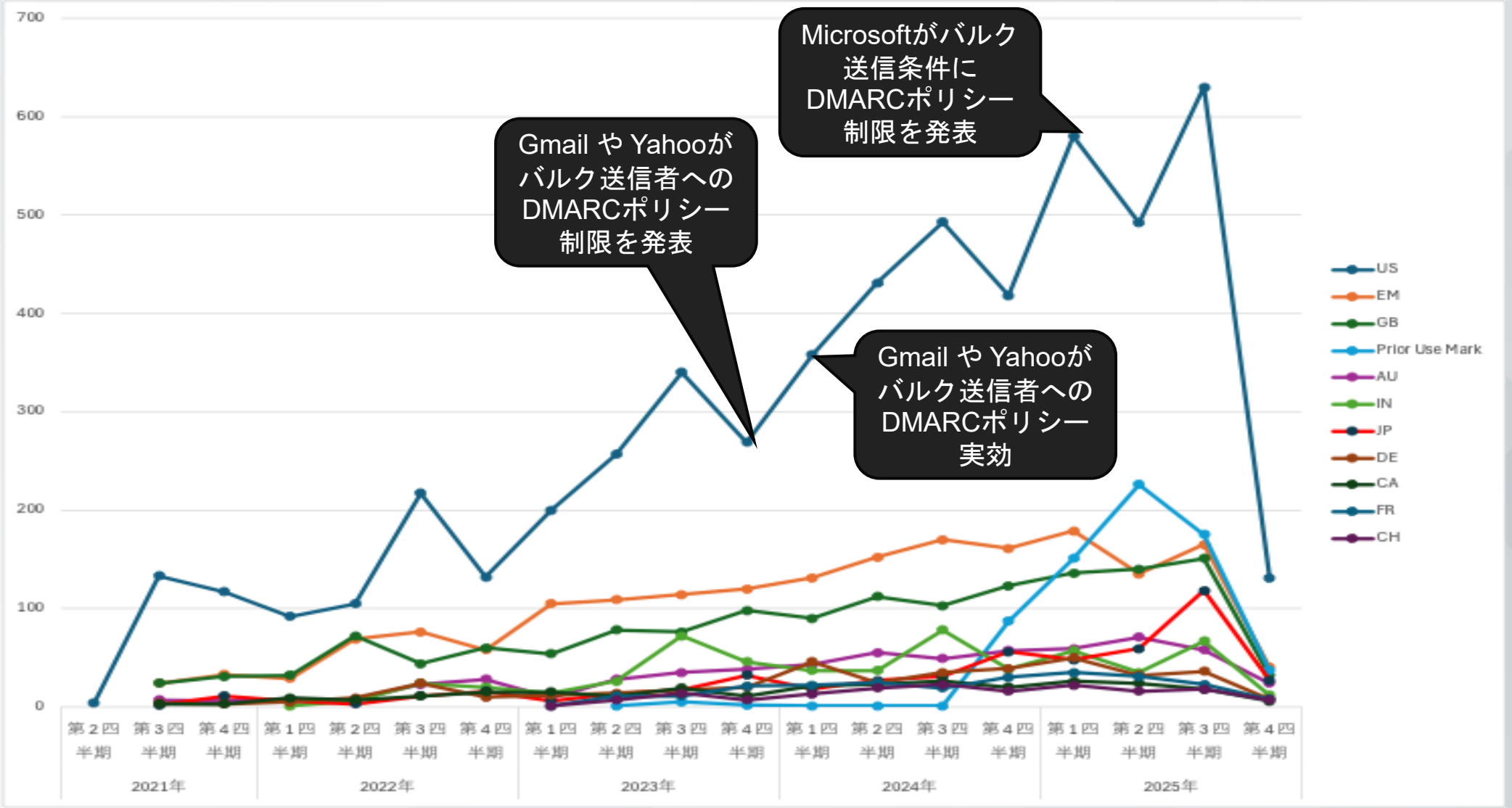
2025.11.4

Agenda

✓CTLOGから見るマーク証明書
✓TLS証明書の有効期限47日に関して
✓マーク証明書、 TLS証明書のDNSの利用トレンド

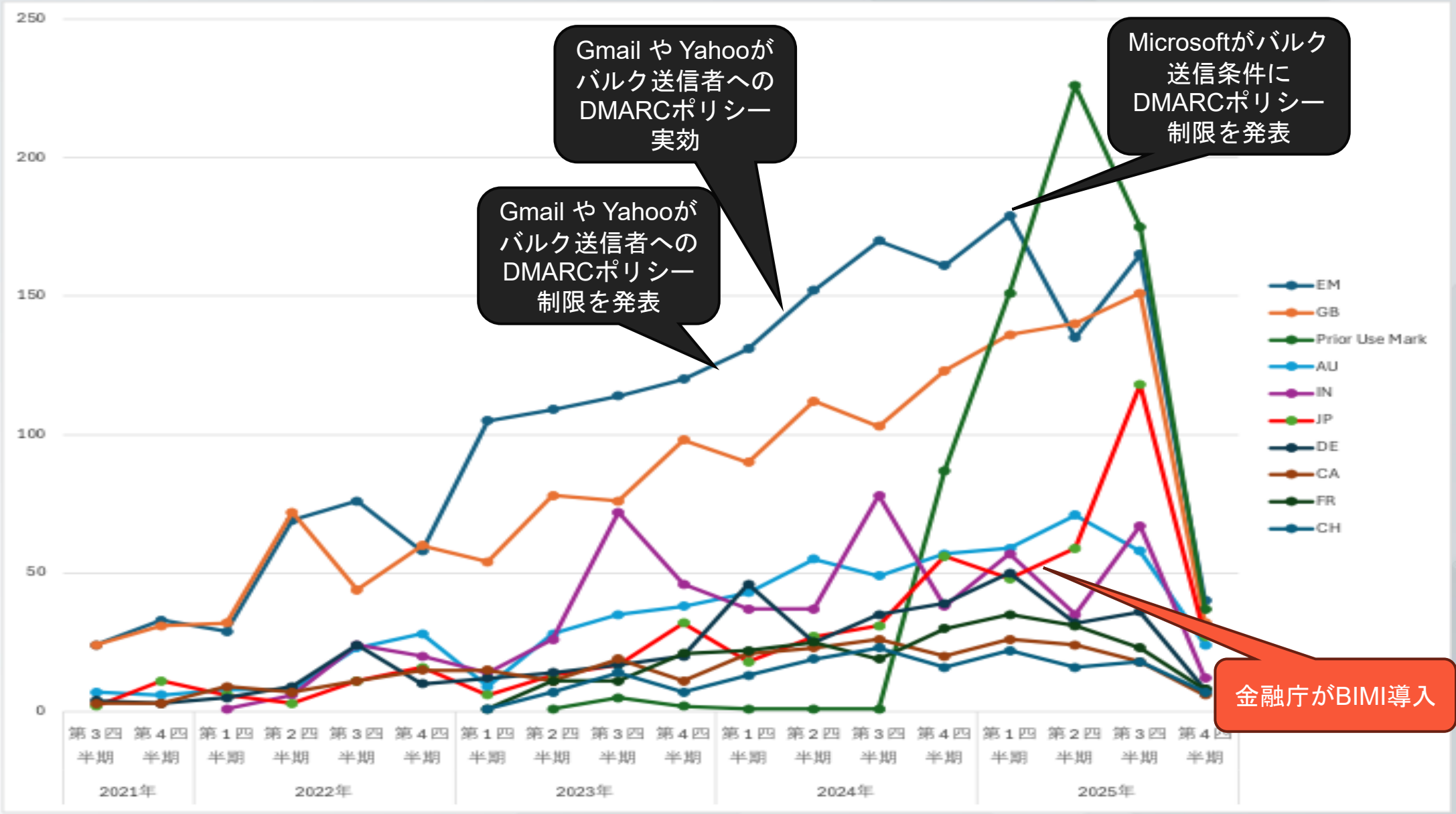
digicert®

CT logデータから読むマーク証明書



digicert®

USを除外すると


Gmail や Yahooがバルク送信者へのDMARCポリシー実効
Gmail や Yahooがバルク送信者へのDMARCポリシー制限を発表
Microsoftがバルク送信条件にDMARCポリシー制限を発表
金融庁がBIMI導入
EM
GB
Prior Use Mark
AU
IN
JP
DE
CA
FR
CH
250
200
150
100
50
0
第３四半期
第４四半期
第１四半期
第２四半期
第３四半期
第４四半期
2021年
2022年
2023年
2024年
2025年

成長要因

金融業界

- 金融庁の対応
- PriorUseによる対応
- 地方銀行への広がり

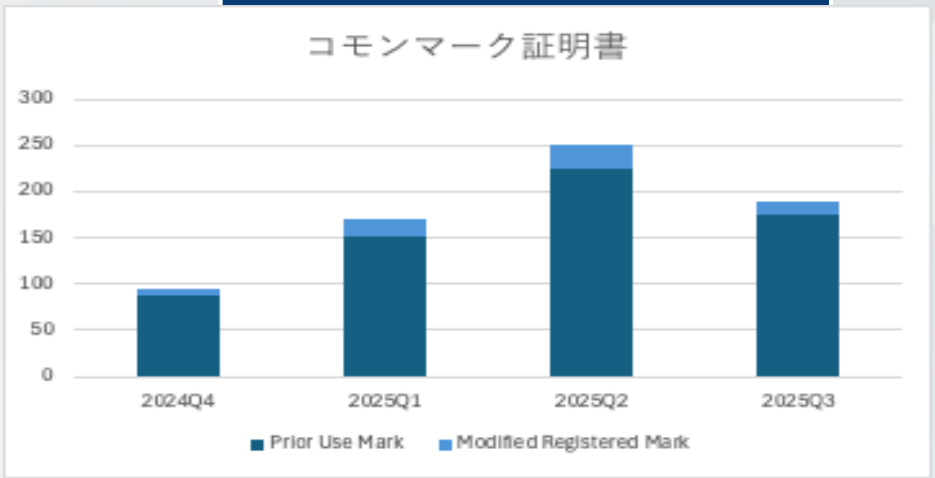
コモンマーク証明書

- PriorUseMark
- Modified Registered Mark

対消費者向け

- IT、小売が利用を牽引
- ヘルスケア、旅行、ゴルフ、スポーツに利用が

		VMC	CMC
5月	チューリッヒ,外為どっとコム	2	0
6月	横浜銀行, アフラック生命	3	0
7月	SBI証券,北國銀行、四国銀行、住信ＳＢＩネット銀行	5	0
8月	三井住友カード、豊橋信用金庫、みなと銀行	2	10
9 月	みずほ銀行、りそな銀行、マネックス証券、池田泉州銀行	3	2
10月	北國銀行、01銀行	2	0



組織別でマーク証明書を多く発行したのは？

申請組織	枚数
Conde Nast Holdings Limited	28
Rakuten Group, Inc.	15
株式会社エス・エム・エス	11
Halsted Financial Services, LLC	10
Lloyds Banking Group PLC Caleres, Inc	9

VOGUE GQ WIRED THE NEW YORKER

Rakuten Rakuten Mobile

VISSEL

TLS証明書の有効期間が47日に短縮

現在 2025年	3月15日 2026年	3月15日 2027年	3月15日 2029年
証明書有効期限 398日	最大有効期限： 200日	最大有効期限： 100日	最大有効期限： 47日
ドメイン/IPデータ期限 398日	データ再利用期限： 200日	データ再利用期限： 100日	データ再利用期限： 10日
組織情報再利用期限: 825日	組織情報再利用期限： 825日から398日に	組織情報再利用期限： 398日	組織情報再利用期限： 398日

なぜ有効期間を短くしようとするのか

ブラウザベンダーが指摘するパブリック証明書の課題

ブラウザ速度向上

- CRLやOCSPなどの証明書失効情報への参照トランザクションを減らす

セキュリティ向上

- OCSP/CRL取得時の発IPによるプライバシーの漏洩

有効期間の短縮化

- 常に新しい認証をもとに更新を行うことで、CRL/OCSPを利用しなくても安全な状態にする
- 現在の暗号が危殆化したときの新技術の適用を高速化する

手動での更新の限界

（サーバ10台の場合）	年間更新（398日）	月間更新（47日）
更新頻度	年に1～10回	年に8回～120回
作業時間（@3h）	30h	～360h
作業コスト	人的コストは少ない	外注している場合、手数料が大きい
ヒューマンエラー耐性	△	×

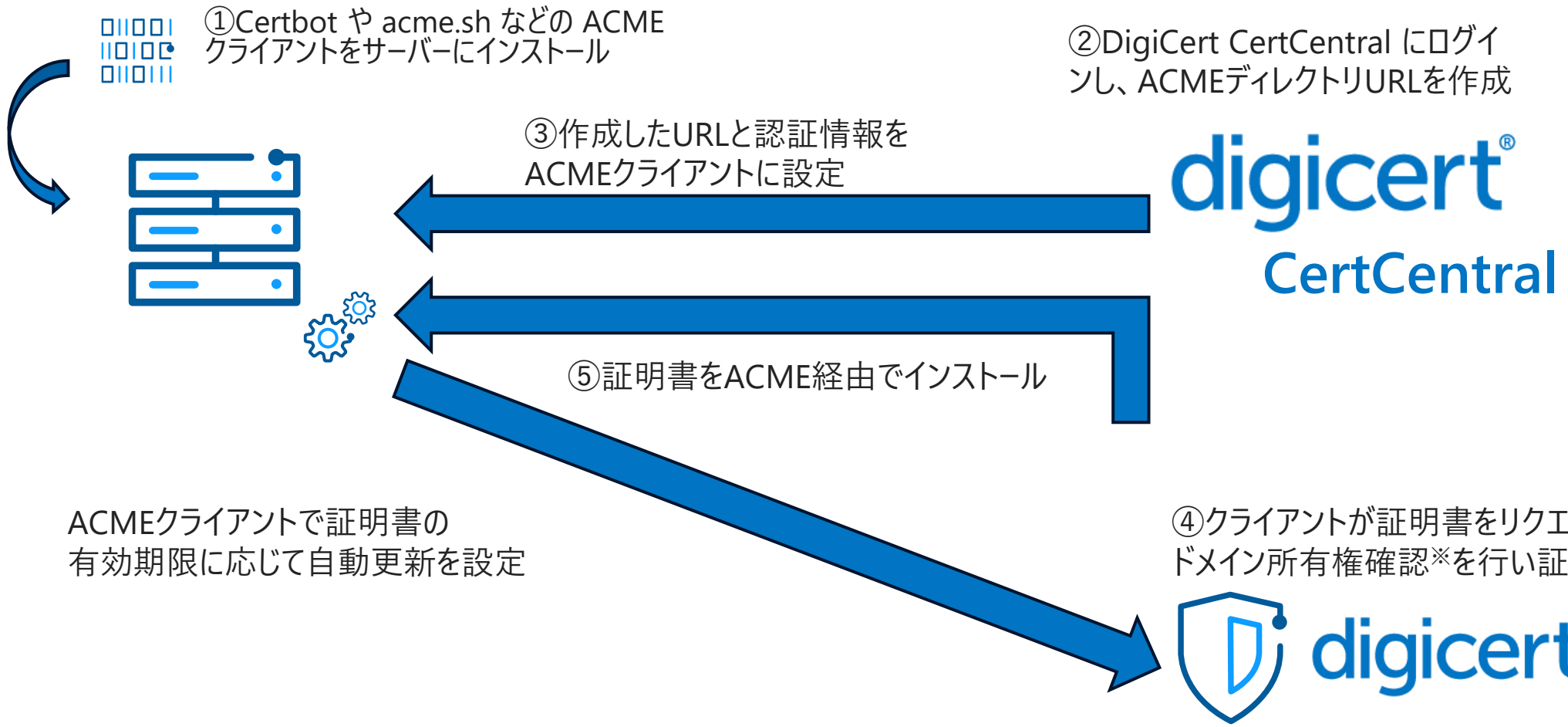
作業内容（3時間）：
- 関係者確認
- CSR作成
- 申請
- 認証対応
- DNS設定変更依頼
- インストール（サーバー、ロードバランサー、その他）

など

手作業が面倒だけど何とかなる・・・？

Excelで台帳管理だとミスも怖い

ACMEクライアントによる自動化



※ DNS -01チャレンジと呼ばれる文字列をDNSサーバーのレコードに書き込むことで、またはHTTPチャレンジで認証を行う方法です

顧客のペインポイント：現場からの洞察

- ドメイン利用権確認, 運用効率, 連携に対する主な課題

1. **ドメイン利用権確認 の課題**
   - ドメイン名利用権の確認 (DCV) のための長くて手動のプロセス
   - DNSと証明書ワークフロー間の同期の問題

2.健全な運用
   - 標準プロセスの欠如は非効率
   - 古いDNSレコードや誤ったDNSレコードは脆弱性を生む

3.ヒューマンエラーと後始末
   - うっかりや連絡ミスは、証明書の期限切れや検証の失敗
   - 不適切に管理されたレコードの後始末には、多大な時間とリソース

4.他チームとの調整
   - DNS、IT、セキュリティの各チーム間の連携が不十分なため、ボトルネック
   - スムーズな承認と変更管理のためのServiceNowのようなツールとの統合に関する課題

Webサーバ証明書の流用はリスク

パブリックPKI

不特定多数がアクセスする公開WebサイトやSMTPサーバでの利用

プライベートPKI

特定ネットワーク内利用（社内ゼロトラスト、BtoBネットワーク、業界用PKI、VPN、ATM、など）

パブリック証明書の制約

Chrome Root Program Policyが目指すこと *

- 自動化手段提供の義務化
- ルート証明書の有効期限の短縮化
- 多目的ルート証明書の段階的廃止
- clientAuthの段階的除外
- ドメイン認証の強化
- リーフ証明書の有効期間短縮（90日、47日）
- 失効期限：24時間および5日間

* https://cabforum.org/2024/10/08/minutes-of-the-f2f-63-meeting-in-seattle-wa-usa-october-8-10-2024/6-chrome-root-program-update.pdf

DNSとPKIワークフローの統合

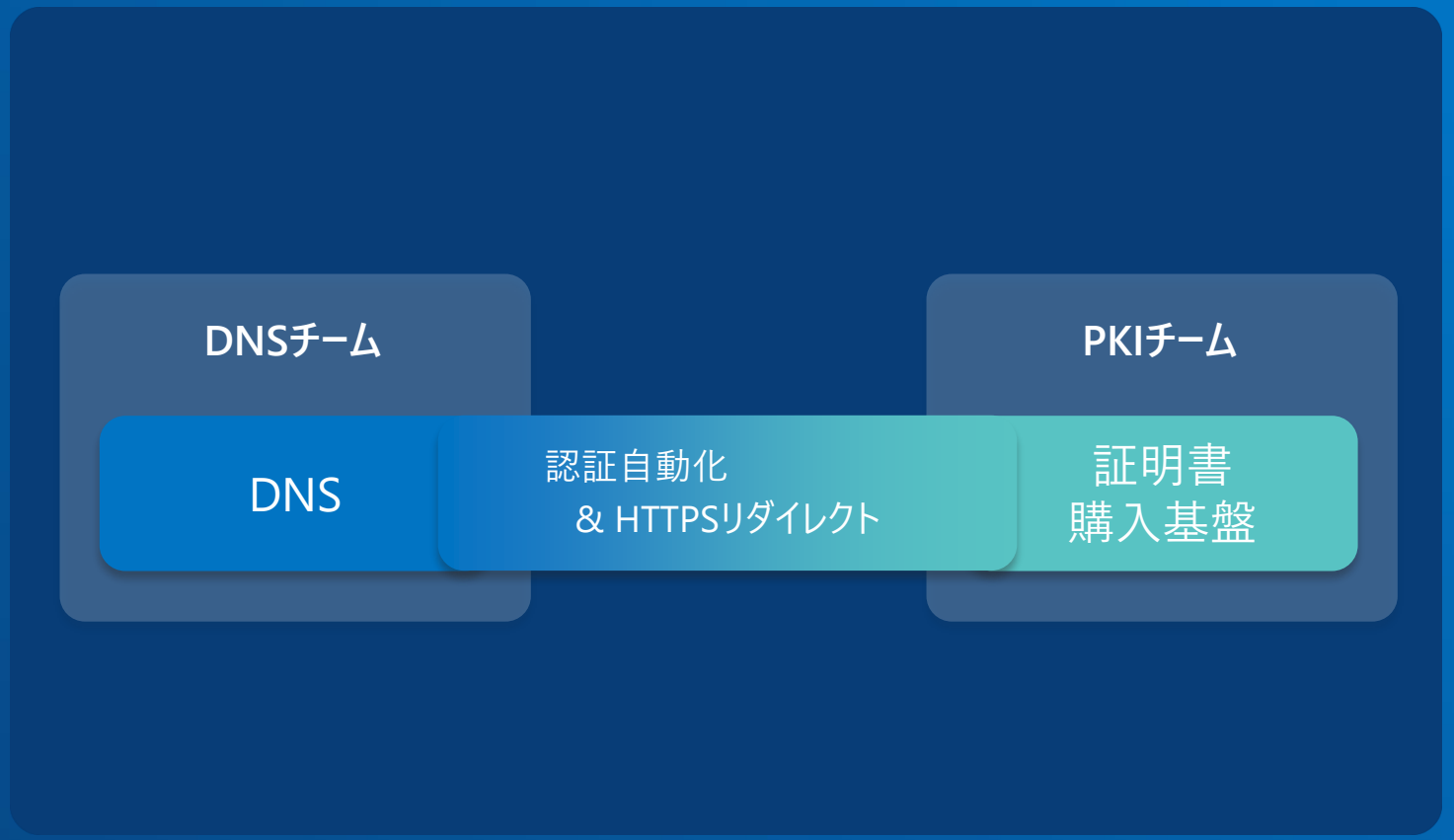
デジタルトラストを強化するため組織の壁を取り除く

業界の背景

ほとんどすべてのパブリック証明書でドメイン名利用権の確認（DCV）が必要

DNSは認証のためのほぼ唯一の有効な選択肢

証明書の有効期間が短縮



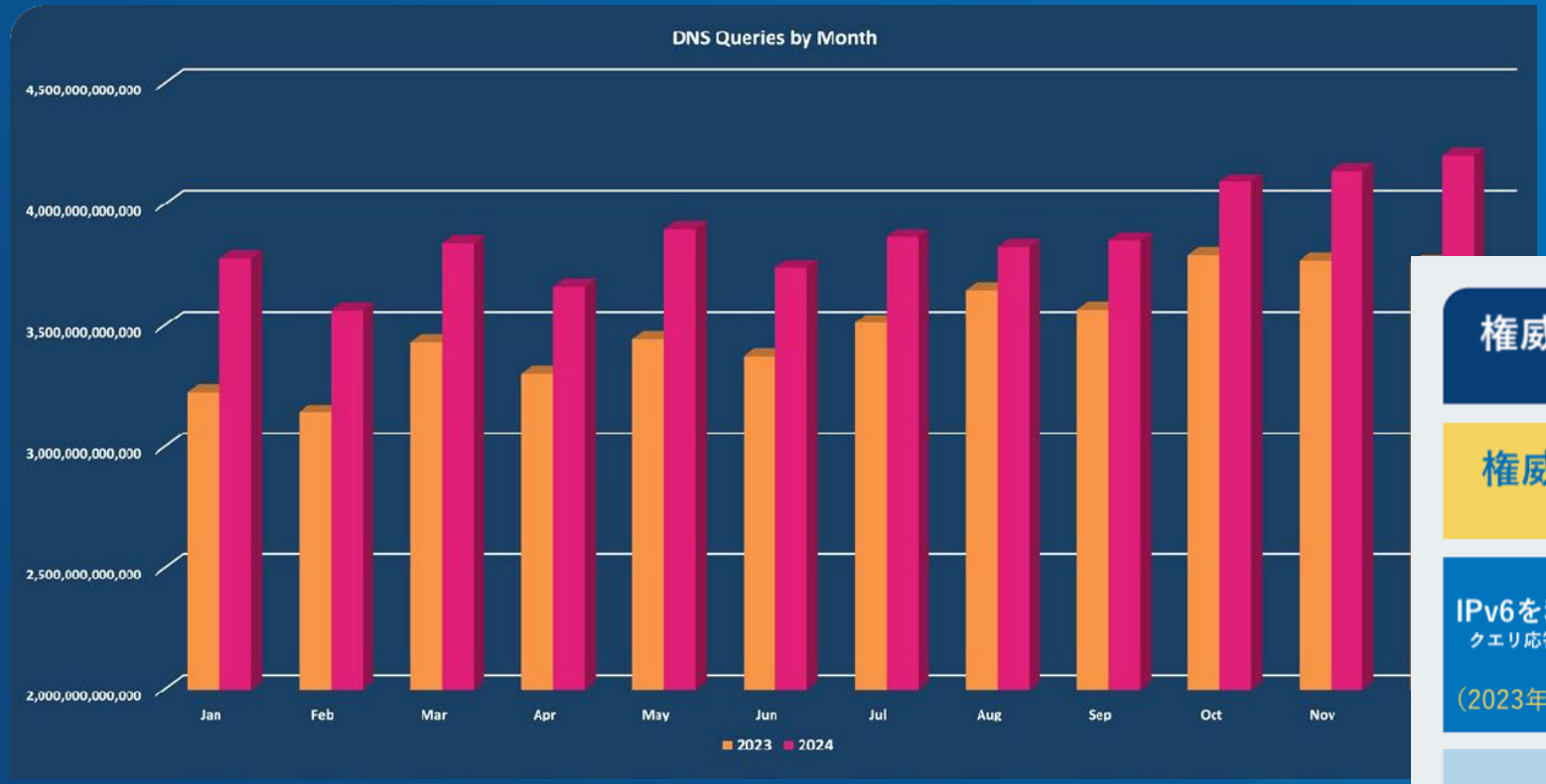
暗号アジリティの向上

コストと時間の削減

回復力を高める

DNSの現状

-この変化、複雑さ、増加に今後どう対応するか？



権威DNSへのクエリ年間総数：46.46兆
（2023年と比較して10.68%増加）

権威DNSへの日次クエリ数:　38.7億
（2023年から10.68%増加）

IPv6を利用 23.48%
クエリ応答の割合
（2023年から年率15.86%増加）

AAAA（IPv6） 18.44%
レコードの割合
（2023年から年率4.47%増加）

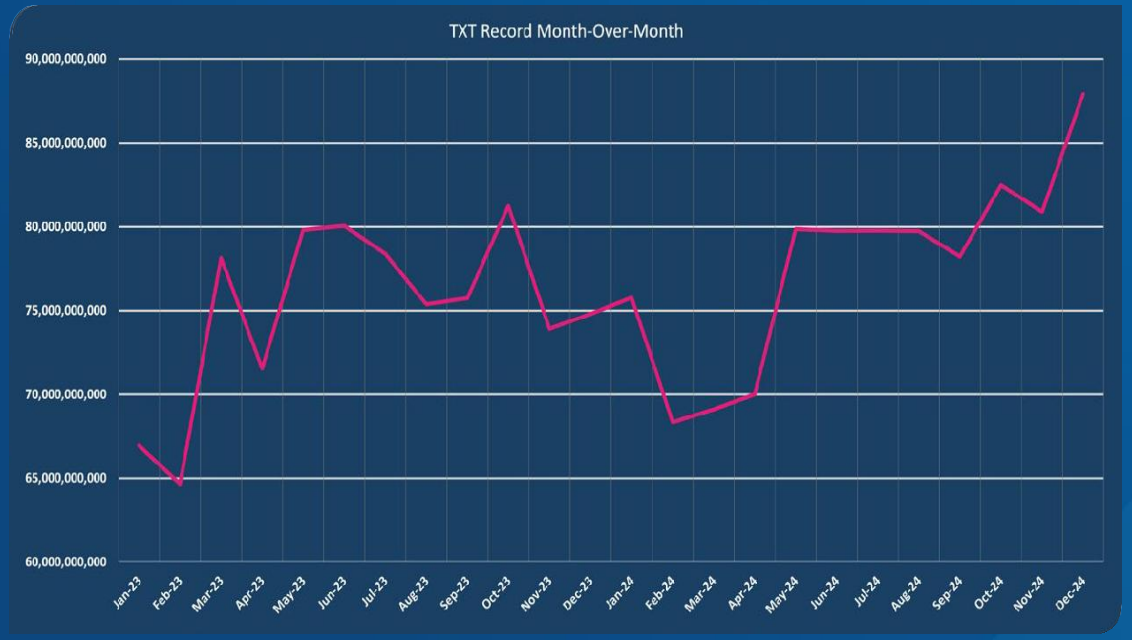
NOERR 78.22%
クエリ応答コードの割合
（2023年から年率8.73%増加）

NXDOMAIN 21.23%
クエリ応答の割合

UltraDNSに対するDDoS攻撃の割合　2,214
（2023年と比較して**29.70%の増加**）

増加するRecord types

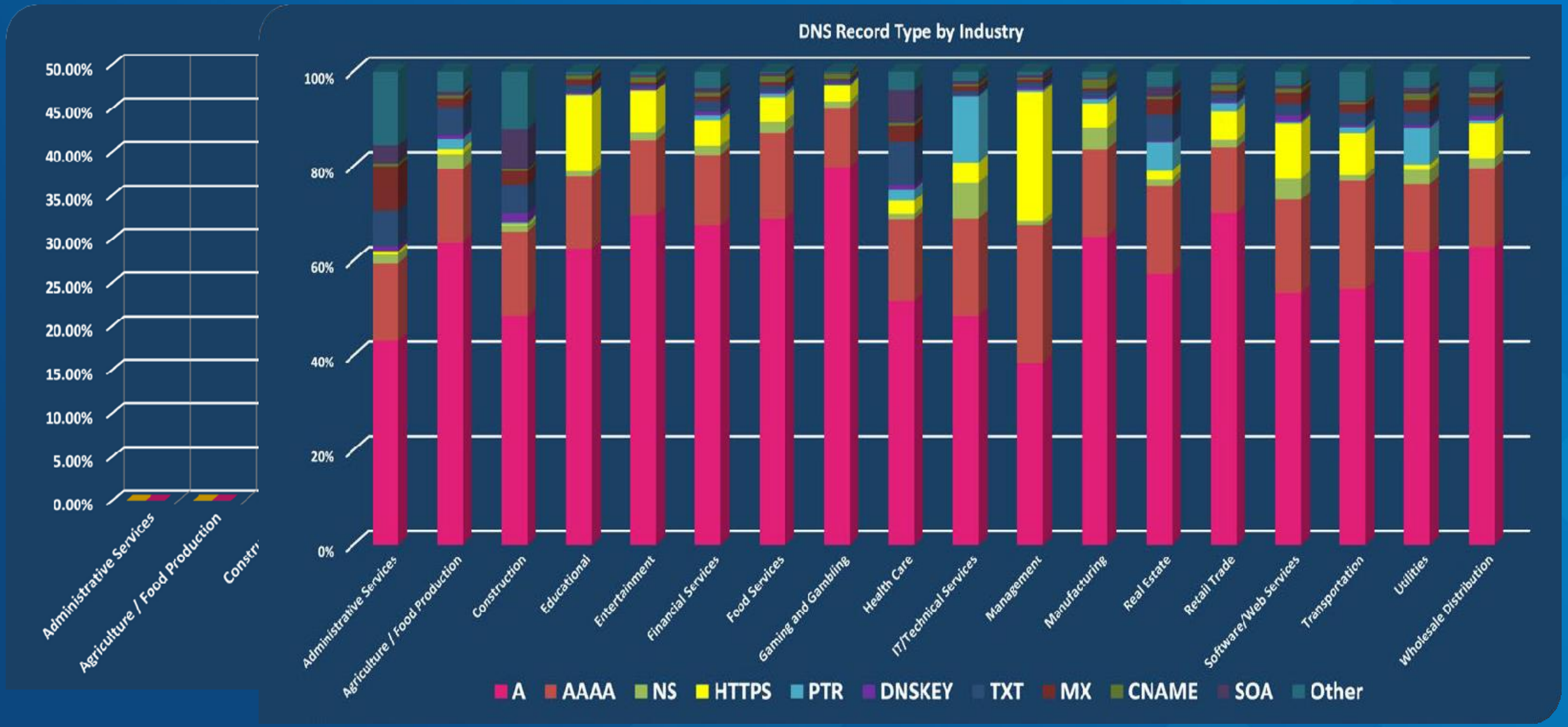
- A Record
- AAAA for IPv6
- CNAME –or cloud service
- MX for Email Security
-TXT for SPF,DKIM,DMARC,DCV….



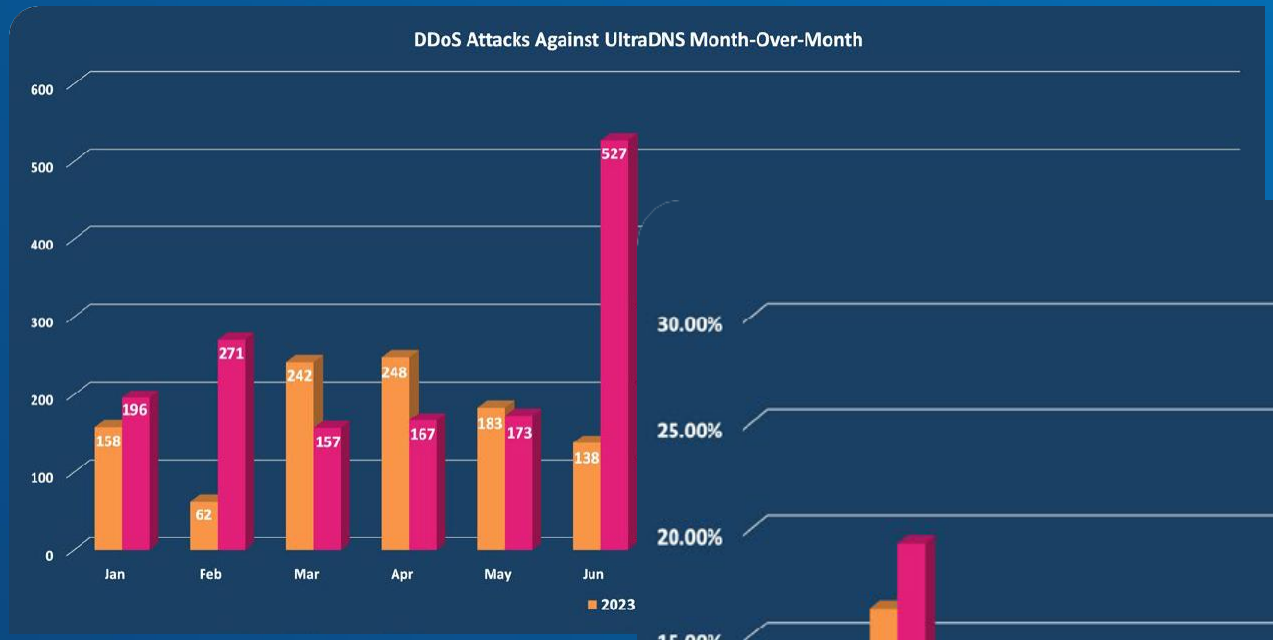
Record	Count	Percent	% Change
A	25,334,799,857,437	54.52%	▲ 8.90%
AAAA	8,572,100,391,456	18.45%	▲ 4.47%
NS	3,294,501,631,905	7.09%	▲ 45.57%
HTTPS	3,038,838,030,898	6.54%	▲ 61.31%
PTR	1,743,003,437,493	3.75%	▲ 18.57%
OTHER	1,150,347,403,826	2.48%	▼ -37.44%
TXT	931,909,792,233	2.01%	▲ 3.47%
MX	796,764,371,636	1.71%	▲ 7.98%
CNAME	469,009,003,196	1.01%	▲ 36.24%
DNSKEY	369,301,213,325	0.79%	▲ 17.70%
SOA	368,347,676,479	0.79%	▼ -2.96%
SRV	322,962,018,715	0.70%	▼ -1.33%
ANY	53,855,861,321	0.12%	▲ 59.16%
SPF	7,975,467,656	0.02%	▼ -20.16%
SVCB	6,523,806,932	0.01%	▲ 335.27%
NAPTR	1,623,376,595	0.00%	▼ -3.91%

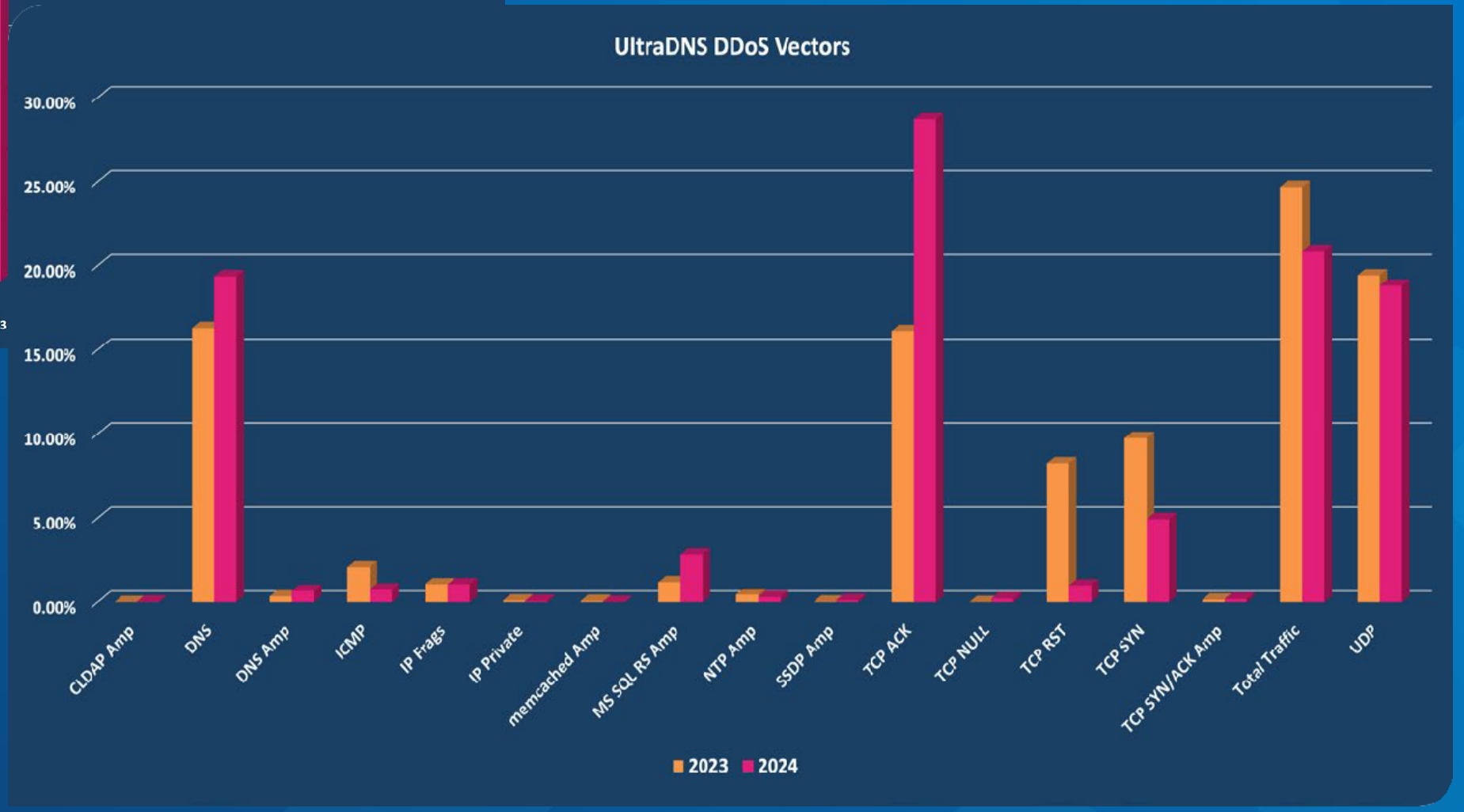
Record	Count	Percent	% Change
HINFO	1,427,603,408	0.00%	▲ 80.36%
NSEC	959,666,117	0.00%	▲ 189.85%
A6	893,039,393	0.00%	▼ -14.37%
RRSIG	343,691,750	0.00%	▲ 189.30%
SSHFP	199,947,588	0.00%	▲ 11.33%
NSEC3	184,625,428	0.00%	▲ 17.82%
CERT	181,551,122	0.00%	▲ 31.63%
LOC	145,571,174	0.00%	▲ 16.90%
NSEC3PARA	84,538,580	0.00%	▼ -5.33%
DLV	62,232,039	0.00%	▼ -48.20%
IPSECKEY	58,248,251	0.00%	▲ 1197.04%
RP	19,723,900	0.00%	▼ -86.16%
TA	4,499,276	0.00%	▲ 131.12%
TSIG	4,487,027	0.00%	▲ 359.26%
TKEY	4,394,634	0.00%	▲ 475.58%
MF	4,307,358	0.00%	▲ 85.56%

業界動向


DNS Record Type by Industry
100%
80%
60%
40%
20%
0%
Administrative Services
Agriculture / Food Production
Construction
Educational
Entertainment
Financial Services
Food Services
Gaming and Gambling
Health Care
IT/Technical Services
Management
Manufacturing
Real Estate
Retail Trade
Software/Web Services
Transportation
Utilities
Wholesale Distribution
A
AAAA
NS
HTTPS
PTR
DNSKEY
TXT
MX
CNAME
SOA
Other

DDoS 攻擊


DDoS Attacks Against UltraDNS Month-Over-Month
600
500
400
300
200
100
0
158
196
62
271
242
157
248
167
183
173
138
527
Jan
Feb
Mar
Apr
May
Jun
2023


UltraDNS DDoS Vectors
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
CLDAP Amp
DNS
DNS Amp
ICMP
IP Frags
IP Private
memcached Amp
MS SQL RS Amp
NTP Amp
SSDP Amp
TCP ACK
TCP NULL
TCP RST
TCP SYN
TCP SYN/ACK Amp
Total Traffic
UDP
2023
2024