JPAAWG Japan Anti-Abuse Working Group

JPAAWG Keynote #2

DMARC.org

Steven Jones

Topics

- DMARC and ARC
- DKIM Replay
- Statistics and Adoption

DMARC and ARC

JPAAWG

DMARCbis – Updates to DMARC

IETF DMARC Working Group has been working on revisions for 2 years

Most Significant Changes:

- Public Suffix Domain replaces Public Suffix List
- Policy Discovery and DNS Tree Walk
- Policy for non-existent domains

DMARC and Public Suffix List

PSL can be found at `https://publicsuffix.org`

Domains under which organizations register domains:

- `au, com, jp, uk, us`
- `co.jp, gov.uk, national.museum`
- `nsw.edu.au`
- `pvt.k12.ma.us`

From PSL: “A "public suffix" is one under which Internet users can (or historically could) directly register names.”

DMARC and Policy Discovery

DMARC uses PSL to find Organizational Domain by a right-to-left match:

`From: user@a.b.c.d.example.com`

- `a.b.c.d.example.com` – no DMARC policy found, lookup OD
- `com` – longest match on PSL (`example.com` not listed)
- Take next element left of `com` as Organizational Domain

The Organizational Domain is `example.com`

DMARC and Public Suffix List

Concerns with the PSL:

- A volunteer effort
- Not designed for email
- DMARC mail receivers must update their copy of the PSL regularly

DMARCbis and Public Suffixes

Public Suffix Domains and Public Suffix Operators

- Incorporates RFC9091
- Allow policies for Top Level Domains (TLDs), like `.bank` and `.jp`
- Allow policies for controlled domains like `gov.uk` included in the PSL
- Set default policy for non-existent child domains of TLDs and PSDs
  - New `np=` tag in DMARC record

DMARCbis and DNS Tree Walk

DNS Tree Walk is a general mechanism to find:

- Organizational Domain
- Public Suffix Domain

DMARCbis and DNS Tree Walk

DNS Tree Walk matches left-to-right, “with a skip”

`From: user@a.b.c.d.mail.example.com`

1. `a.b.c.d.mail.example.com` – more than 5 labels
2. Shorten to less than 5 labels
3. `d.mail.example.com` – check at 4-label level, no record
4. `mail.example.com` – check 3-label level, record found

The record at `_dmarc.mail.example.com` is used.

PSD and Organizational Domain

Public Suffix Domain (PSD) may include the `psd=y` tag in the DMARC DNS record

```
_dmarc.bank v=DMARC1; psd=y; p=reject; …
```

Organizational Domain (OD) is one label longer than a PSD, and may include the `psd=n` tag in the DMARC DNS record

```
_dmarc.sample.bank v=DMARC1; p=reject; …
_dmarc.example.com v=DMARC1; psd=n; p=reject; …
```

OD records with `psd=n` tag are for cases where PSD parent published DMARC record without `psd=y`

DMARCbis and Non-Existent Domains

New `np=` tag for Organizational Domains and Public Suffix Domains

Spammers invent non-existent subdomains, especially of PSDs like `gov.uk`

`np=` specifies a policy to use for subdomains that return an `NXDOMAIN` for DNS lookups

```
_dmarc.gov.uk  p=none; sp=quarantine; np=reject; …
```

JPAAWG

Which Policy To Apply?

- For `From:` domains that do <u>not</u> return `NXDOMAIN`:
  1. RFC5322.From domain (`p=` tag)
  2. Organizational Domain (`sp=` tag)
  3. Public Suffix Doman (`sp=` tag)

- For `From:` domains that <u>do</u> return `NXDOMAIN`:
  1. Organizational Domain (`np=` tag)
  2. Public Suffix Doman (`np=` tag)

`_dmarc.gov.uk  p=none; sp=quarantine;` **`np=reject;`** …

`From: user@Y9RE1BU.gov.uk` will have `np=reject` applied

ARC – Enabling DMARC Adoption

- Authenticated Received Chain, RFC8617
- Forwarded messages and mailing lists tend to fail DMARC checks
- ARC conveys authentication results across participating intermediaries (forwarders, list operators)
- ARC results from trusted intermediaries can validate messages that otherwise fail DMARC
- Who to trust is decided by the mail receiver

Microsoft Using ARC in Office 365

- 2019: Microsoft uses ARC internally, “but plan to add support for third-party ARC sealers in the future.”

Now Office 365 Admins can configure Trusted ARC Sealers

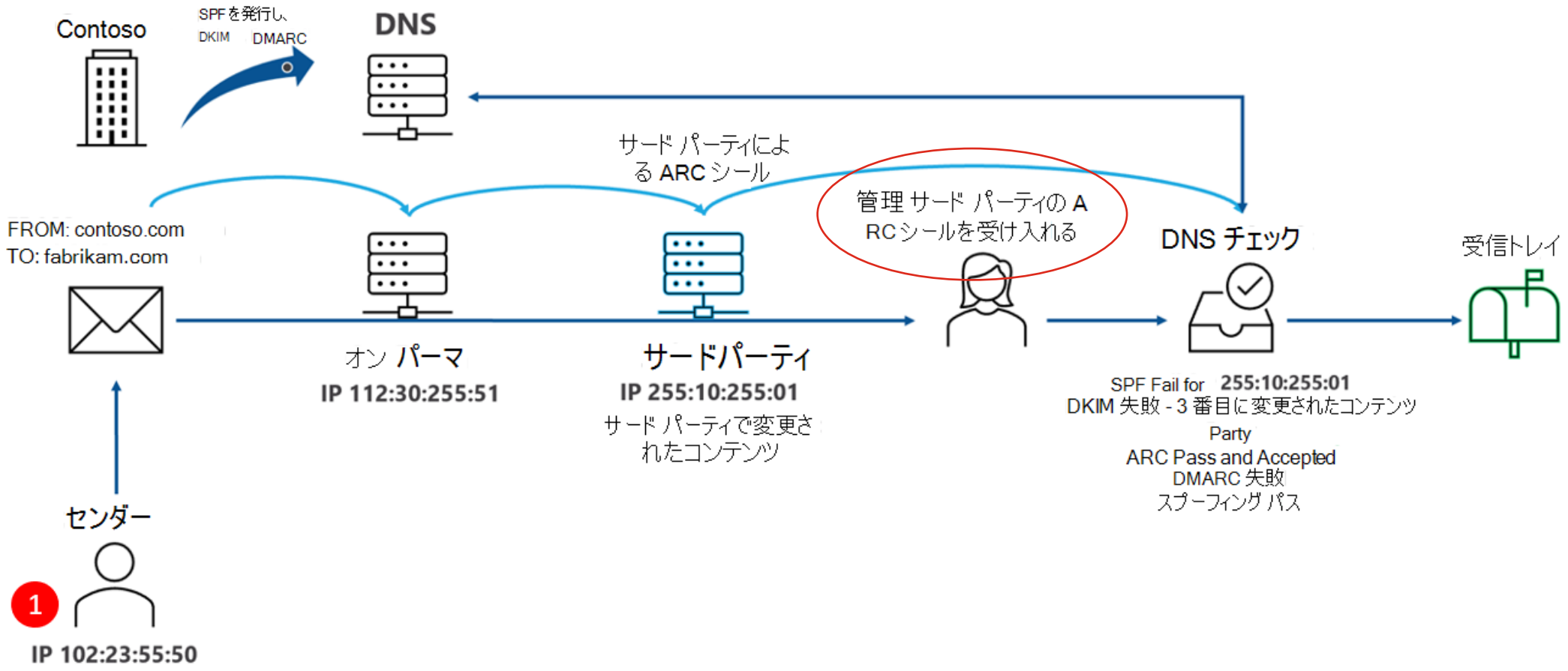
- 2022: “Trusted ARC sealers lets admins add a list of trusted intermediaries into the Microsoft 365 Defender portal. **Trusted ARC sealers allows Microsoft to honor ARC signatures from these trusted intermediaries**.”

JPAAWG

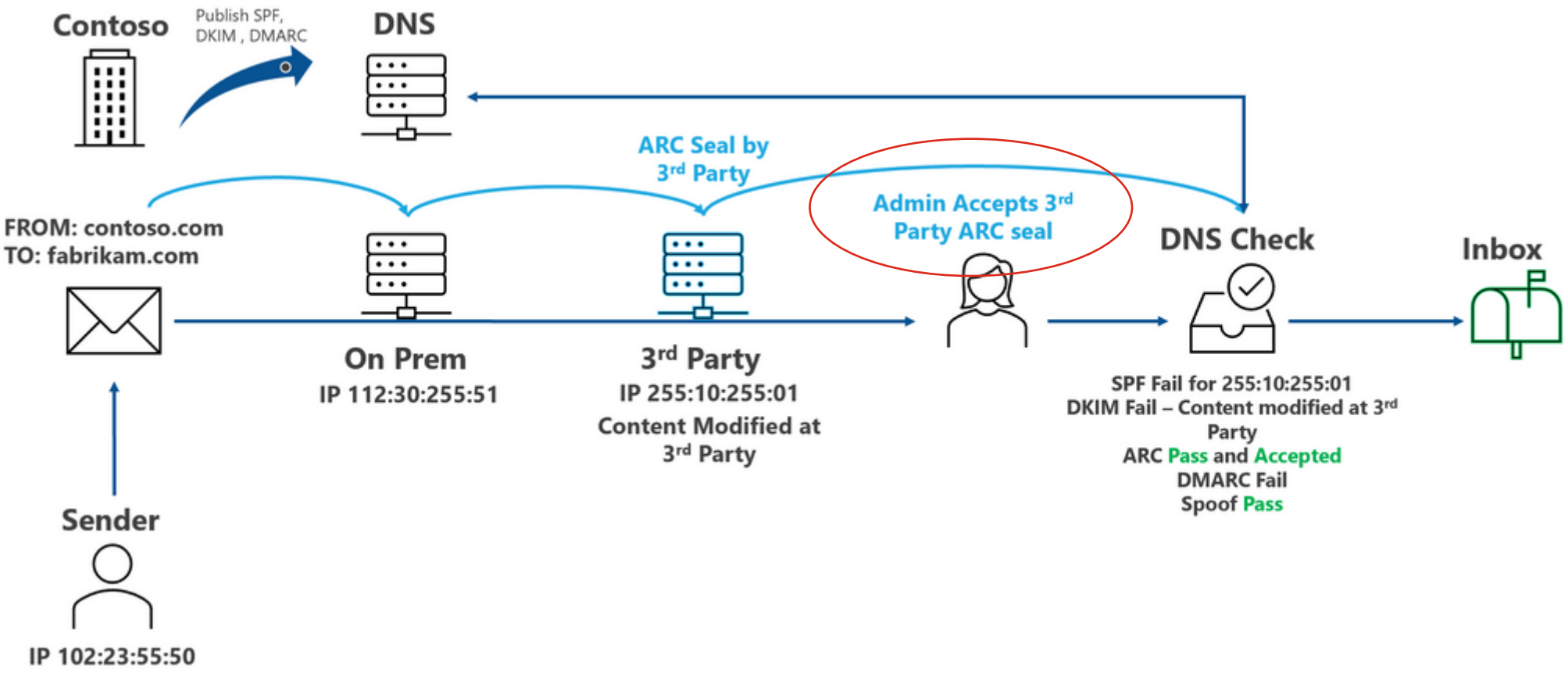
Microsoft

Microsoft Using ARC in Office 365

ARC シール付き:



Microsoft Using ARC in Office 365



Microsoft Using ARC in Office 365

Several articles published in 2022:

- 6月: Using ARC in Defender for Office 365
  - https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/improving-defense-in-depth-with-trusted-arc-sealers-for/ba-p/3440707
- 10月: 正当な間接メールフローを信頼する信頼された ARC 送信者の一覧を作成する
  - https://learn.microsoft.com/ja-jp/microsoft-365/security/office-365-security/use-arc-exceptions-to-mark-trusted-arc-senders?view=o365-worldwide
- 10月: DMARC を使用してメールを検証する
  - https://learn.microsoft.com/ja-jp/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide

Microsoft Using ARC in Office 365

Several articles published in 2022:

- 6月: Using ARC in Defender for Office 365
  - https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/improving-defense-in-depth-with-trusted-arc-sealers-for/ba-p/3440707
- 10月: Make a list of trusted ARC Senders to trust
  - https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-arc-exceptions-to-mark-trusted-arc-senders?view=o365-worldwide
- 10月: Use DMARC to validate email
  - https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide

Future of Mailing Lists?

SIGN IN / UP The Register

OSES 52

The GNOME Project is closing all its mailing lists

Everyone has to join Discourse… although you can still participate via email

Liam Proven Thu 27 Oct 2022 11:33 UTC

The GNOME Project is preparing to shut down its mailing lists due to problems maintaining the project's GNU Mailman instance - which relies on Python 2 - and a lack of moderators.

The community's leaders maintain a substantial selection of mailing lists, hosted via the GNU Project's Mailman tool. It also hosts its own instance of the Discourse web forum tool, notably also used by Canonical to host the official Ubuntu forums.

That's going to change, and very soon: at the end of this month. Announcements on several of the lists, such as here on the list for the Evolution email client, state that the lists are closing down, and discussions must move to Discourse.

DKIM Replay Attacks

JP AAWG

Real World DKIM Usage

- DKIM designed to help receivers track reputation of email-sending domains
- DKIM attaches a digital signature to an email message
- ESPs and mailing lists may use the same signature for all messages in a campaign
  - They may not sign some recommended fields to support this
- ESPs may sign with their domain (`d=esp.com`), and use their domain in the `From:` address

What Is DKIM Replay?

- A message sent to one recipient is DKIM signed by a domain with good reputation
- This message is extracted and re-sent to many recipients
- DKIM signature on these messages is still valid
- If DKIM `d=` domain and `From:` domain align, DMARC still passes
- Attacker can add unsigned/missing headers (`Cc:`)
- Good reputation of DKIM signer is sometimes enough to bypass spam filters

Why Is This Hard to Detect?

Replay attacks look like legitimate traffic:

- Forwarding breaks SPF, leaves DKIM intact (passing)
- Mailing lists break SPF but may leave DKIM intact
- ESPs and lists may use same DKIM signature on all messages in the same campaign
- ESPs and lists may use their own domain for RFC5321.MailFrom, but leave `From:` intact

Is DKIM Replay a New Attack?

Described in original DKIM spec (RFC 4871) and all updates

```
8.5 Replay Attacks

In this attack, a spammer sends a message to be spammed to an
accomplice, which results in the message being signed by the
originating MTA.  The accomplice resends the message, including
the original signature, to a large number of recipients, possibly
by sending the message to many compromised machines that act as
MTAs. The messages, not having been modified by the accomplice,
have valid signatures.
```

Some abuses of body length limits (“l=“ tag) also described

Rise in DKIM Replay Attacks

- ProtonMail reported problems due to DKIM Replay attacks starting in December 2021
  - https://proton.me/blog/dkim-replay-attack-breakdown
- Other reports emerged through early 2022
- Numerous industry blog posts during 2022

Industry Response to DKIM Replay

- Data sharing between MBP, ESPs, researchers
- Many informal channels
- Recent activity at M3AAWG:

2月	Discussed informally at M3AAWG 54
	DKIM Replay initiative created
6月	Several sessions at M3AAWG 55
10月	BoF session at M3AAWG 56

Discussion at IETF 115 on Monday (London time)

DKIM Replay Countermeasures

- Limit the time each DKIM key and/or signature is valid
  - More frequent DKIM key rotation
  - Use the `x=` tag (expiration time) in DKIM signatures
- Always sign `From:`, `To:` and `Cc:` headers even if empty
  - Sign as many headers as you reasonably can
  - Review all header signing – `Date:`, `Reply-To:`, `Subject:`, etc
- Content scan messages sent from new/trial accounts
- Disallow pre-shortened links in messages
- Limit `To:` addresses for trial accounts

Four Proposals at M3AAWG BoF

- Kucherawy: Include Envelope in DKIM Signature
  - https://datatracker.ietf.org/doc/draft-kucherawy-dkim-anti-replay/
- Chuang: Replay Resistant ARC
  - https://datatracker.ietf.org/doc/draft-chuang-replay-resistant-arc/
- Bradshaw: DKIM Envelope Validation Extension
  - https://www.ietf.org/id/draft-bradshaw-envelope-validation-extension-dkim-00.html
- Gondwana: Mailpath, an Email Chain of Custody
  - https://datatracker.ietf.org/doc/draft-gondwana-email-mailpath

Kucherawy: Sign the Envelope

- New tag for DKIM signatures: `e=y`
- Add all envelope recipients (RFC5321.RcptTo) in signature
- Signatures no longer valid if any changes made to envelope recipient address(es)

Kucherawy: Sign the Envelope

Pros

- Simple implementation
- Old signer/verifier works
- Can double-sign during transition

Cons

- Cannot validate post-delivery, need envelope data
- Looks like a failed signature
- No more envelope splitting
- Does not survive forwarding or mailing lists

Chuang: Replay Resistent ARC

Two elements:

- Declare All Recipients and Affirm (DARA)
  - Intermediaries record any RFC5321.RcptTo address changes in new `Forwarding-To:` header
  - Receiver confirms that RFC5321.RcptTo address is in a signed `To:`, `Cc:` or `Forwarding-To:` header
- Sender Receiver Co-Signing (SeRCi)
  - Extend SMTP transaction to include challenge-response
  - Includes next hop in each `ARC-Signature:`

Chuang: Replay Resistent ARC

Pros

- Replay limited to original recipients
- No changes to DKIM

Cons

- DARA requires changes to ARC + widespread adoption
- SeRCi requires SMTP extension
- Participants must publish DARA and SeRCi DNS records
- Mailing lists/forwarders asked to add new DARA header (`Forwarded-To:`)

Bradshaw: Envelope Validation

- Described as a DKIM extension
- New `DKIM-EVE:` headers created by Sender
- Hash of all header and envelope addresses, plus `Message-ID` and unique `EVE-ID`
  - Sender would include expected intermediaries
- DKIM signature would include `DKIM-EVE:` headers

Bradshaw: Envelope Validation

Pros

- Captures envelope details
- Allows envelope splitting
- No changes to DKIM
- DKIM still passes for forwarded messages
- Receivers can compile reputation of intermediary

Cons

- Requires intermediary reputation system
- Headers must never be re-ordered

Gondwana: Mailpath

- "A chain of custody for email"
- Record ingress, modification, and egress from an ADMD
- Ingress
  - Record `Mailpath-Authentication-Results:` and `Mailpath-Signature:`
  - Signature includes addresses used to check alignment
- Modification
  - Indicate changes to addresses, message content
- Egress
  - See if next hop supports Mailpath
  - Add `Mailpath-Disposition:`, indicate if next hop has Mailpath
  - Add `Mailpath-Transit-Signature:` that covers all other Mailpath, ARC, and DKIM headers

Gondwana: Mailpath

Pros

- Records address and content changes at each hop
- Includes expected next hop at each step

Cons

- Tries to capture all email state at each hop
- 4-5 headers and three signing operations per hop
- Check for Mailpath support at next hop is required
- New DNS TXT record for every MX server

Statistics and Adoption

JP AAWG

DMARC Activity in Japan

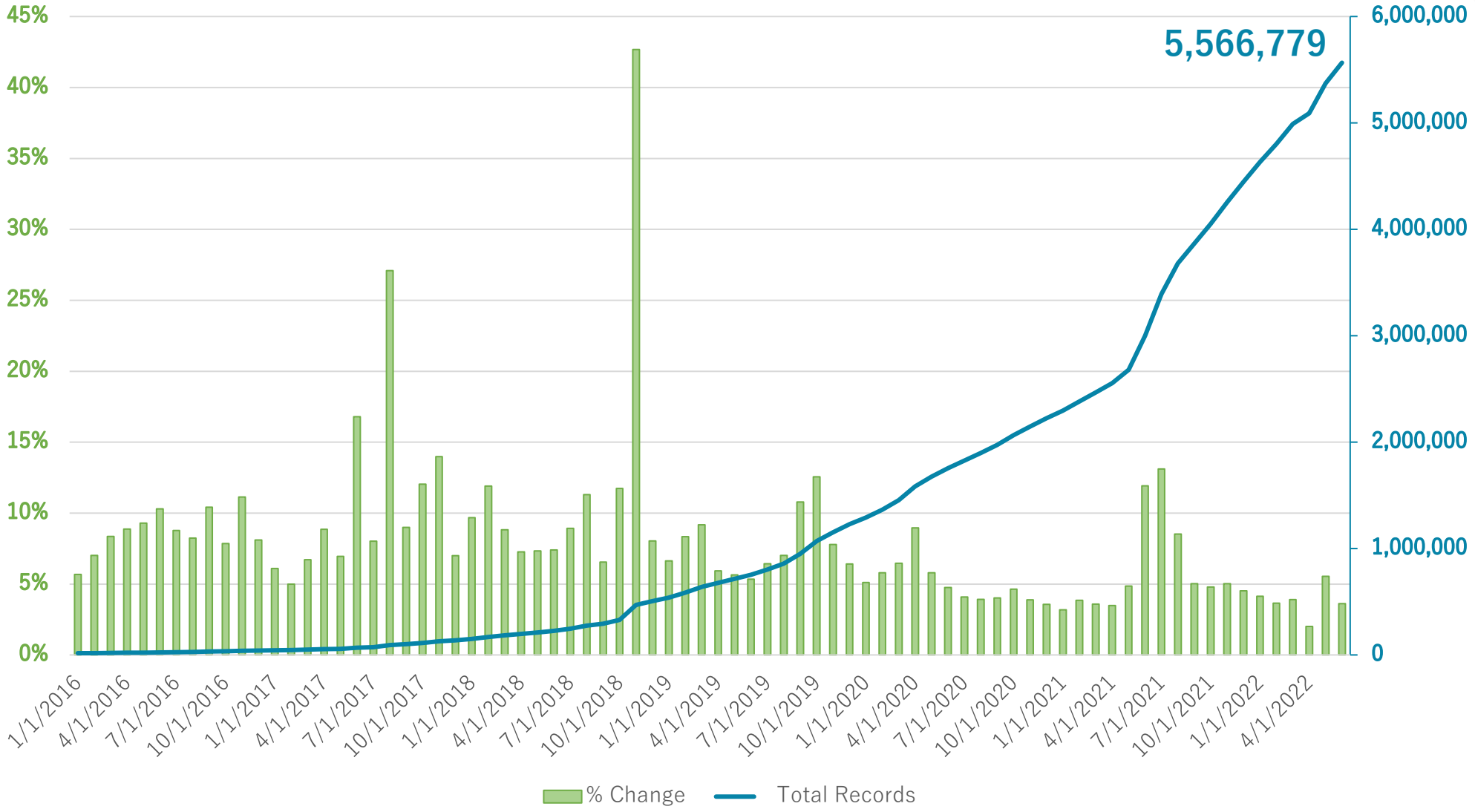
- Nifty sending aggregate reports (1月)
- NTT Docomo verifying DMARC (8月)
- 50% of Nikkei 225 companies have deployed DMARC

About This Data

- Raw data supplied by DomainTools
- DNS request/response data captured from sensors widely deployed across the Internet
- Not 100% coverage of Internet, but a stable sensor network useful for comparisons over time
- DMARC.org thanks DomainTools for their continuing support

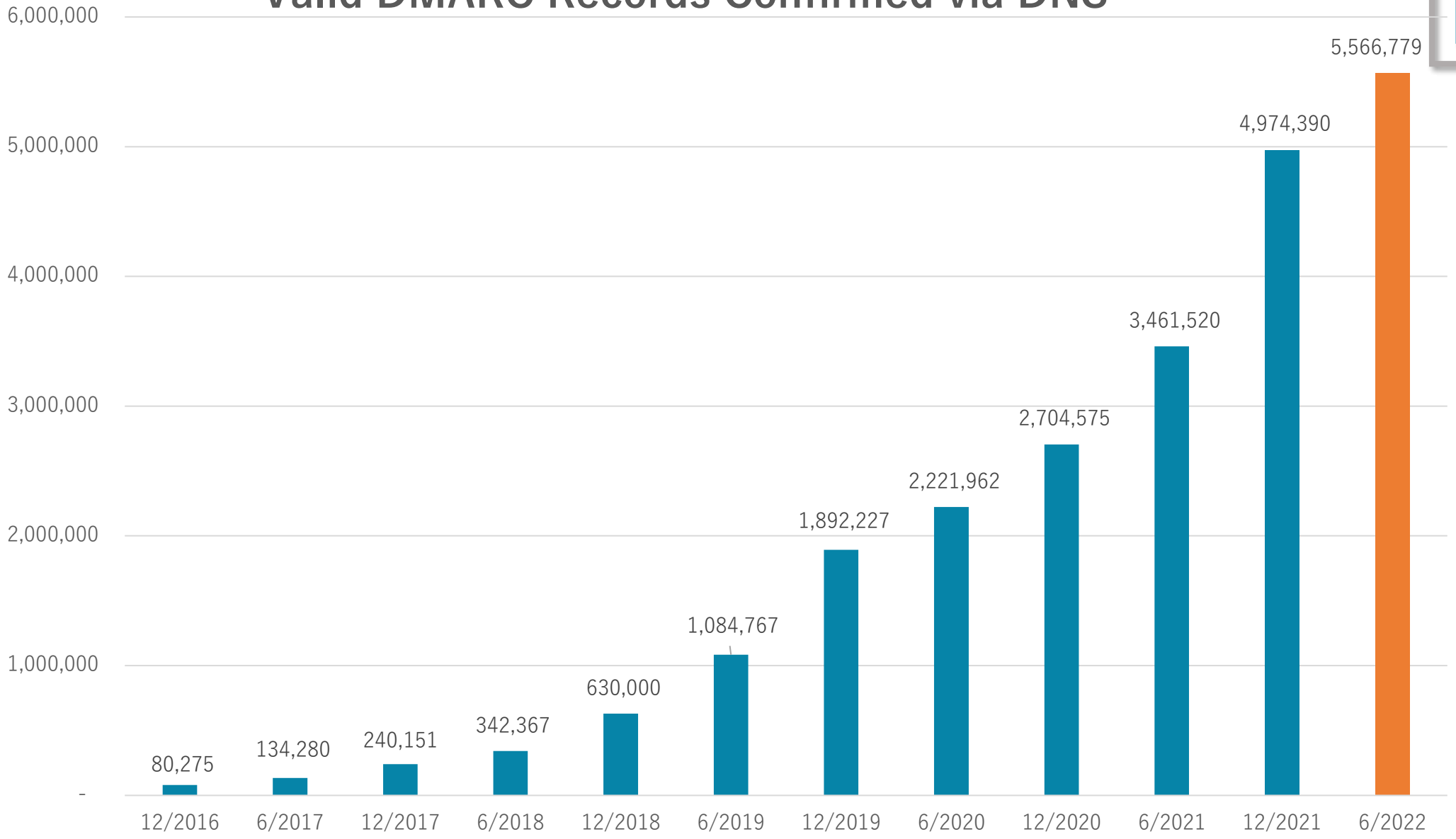
DOMAINTOOLS

Active DMARC Records and % Growth by Month



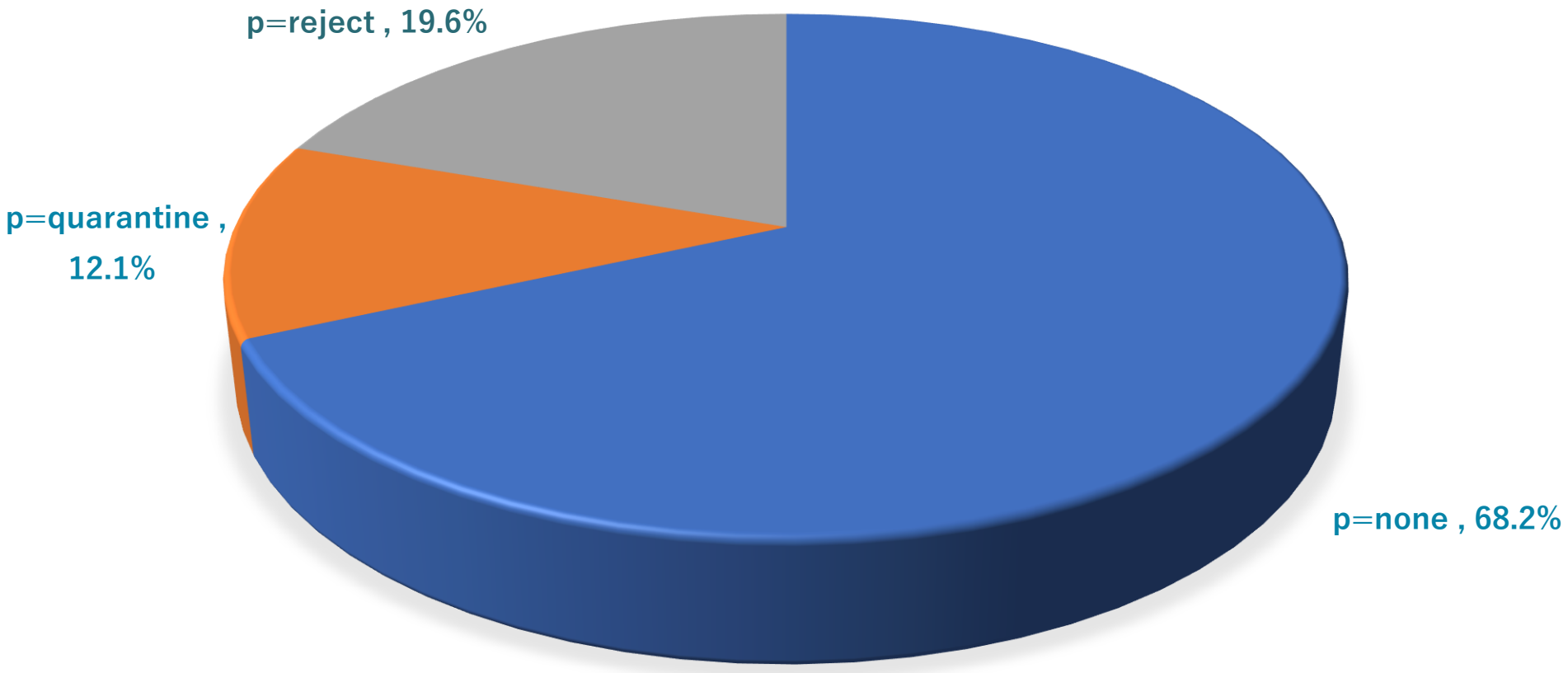
JPAAWG

Valid DMARC Records Confirmed via DNS

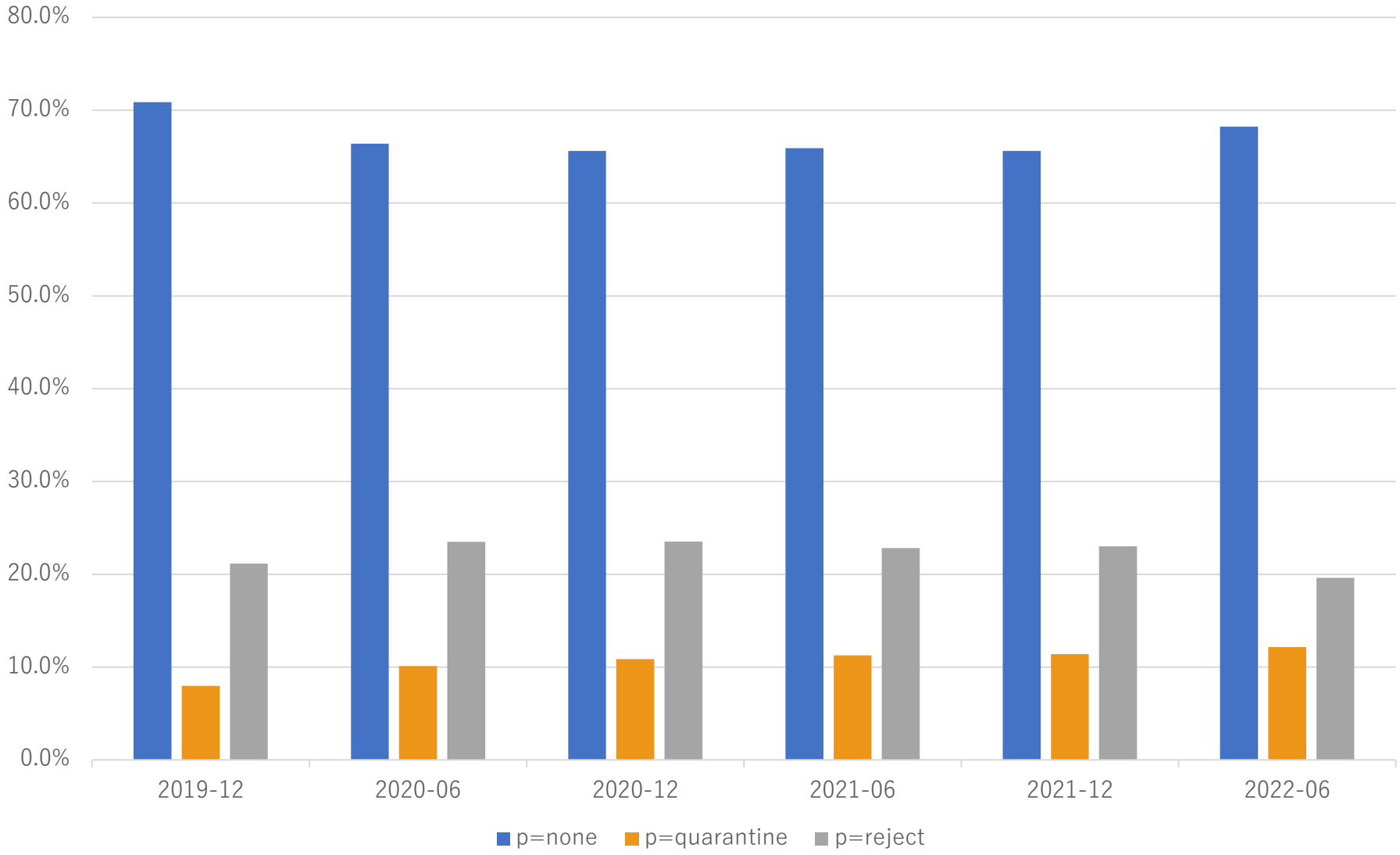


JPAAWG

DMARC Policies

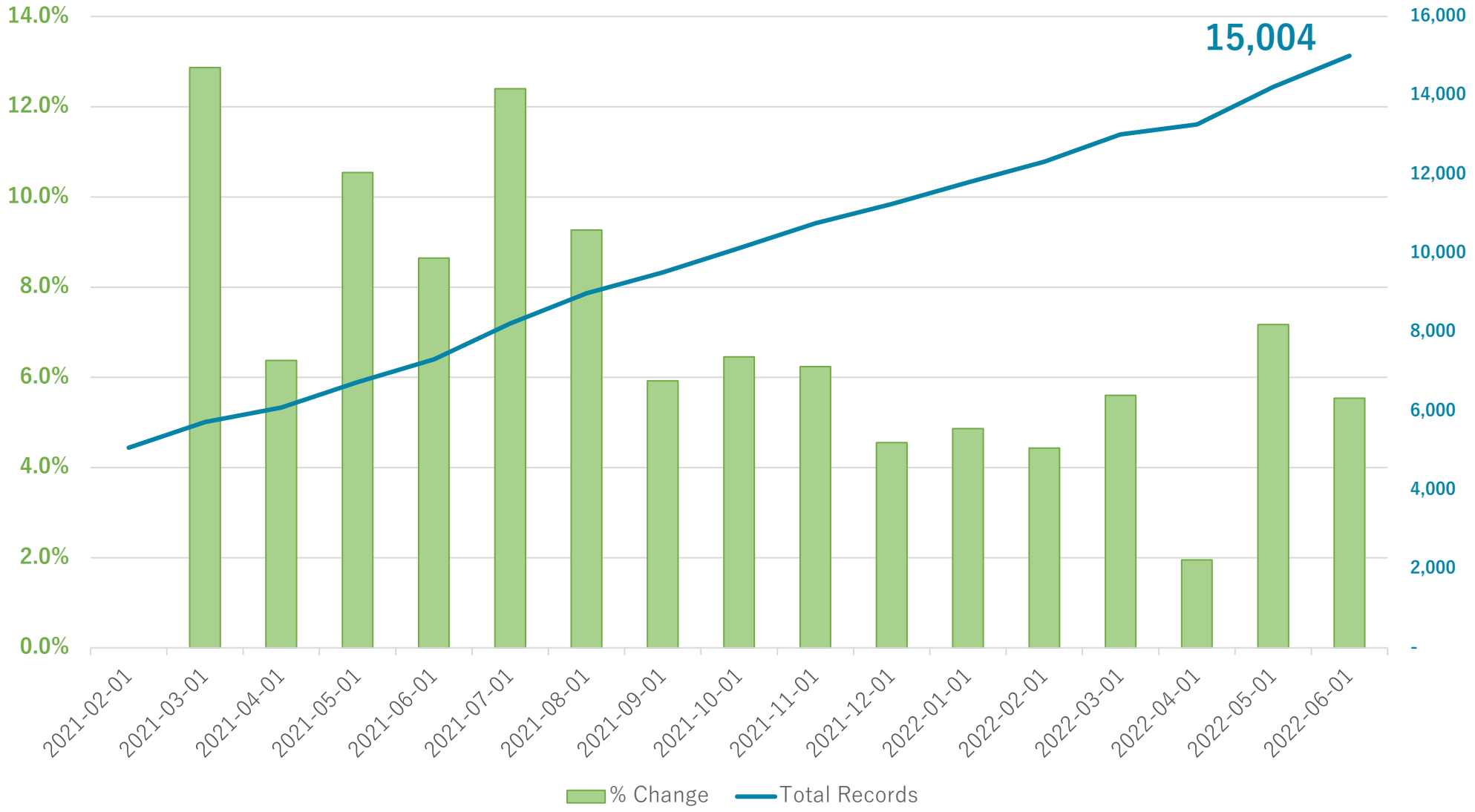


DMARC Policies Over Time



JPAAWG

Active BIMI Records and % Growth By Month



JPAAWG

BIMI Records

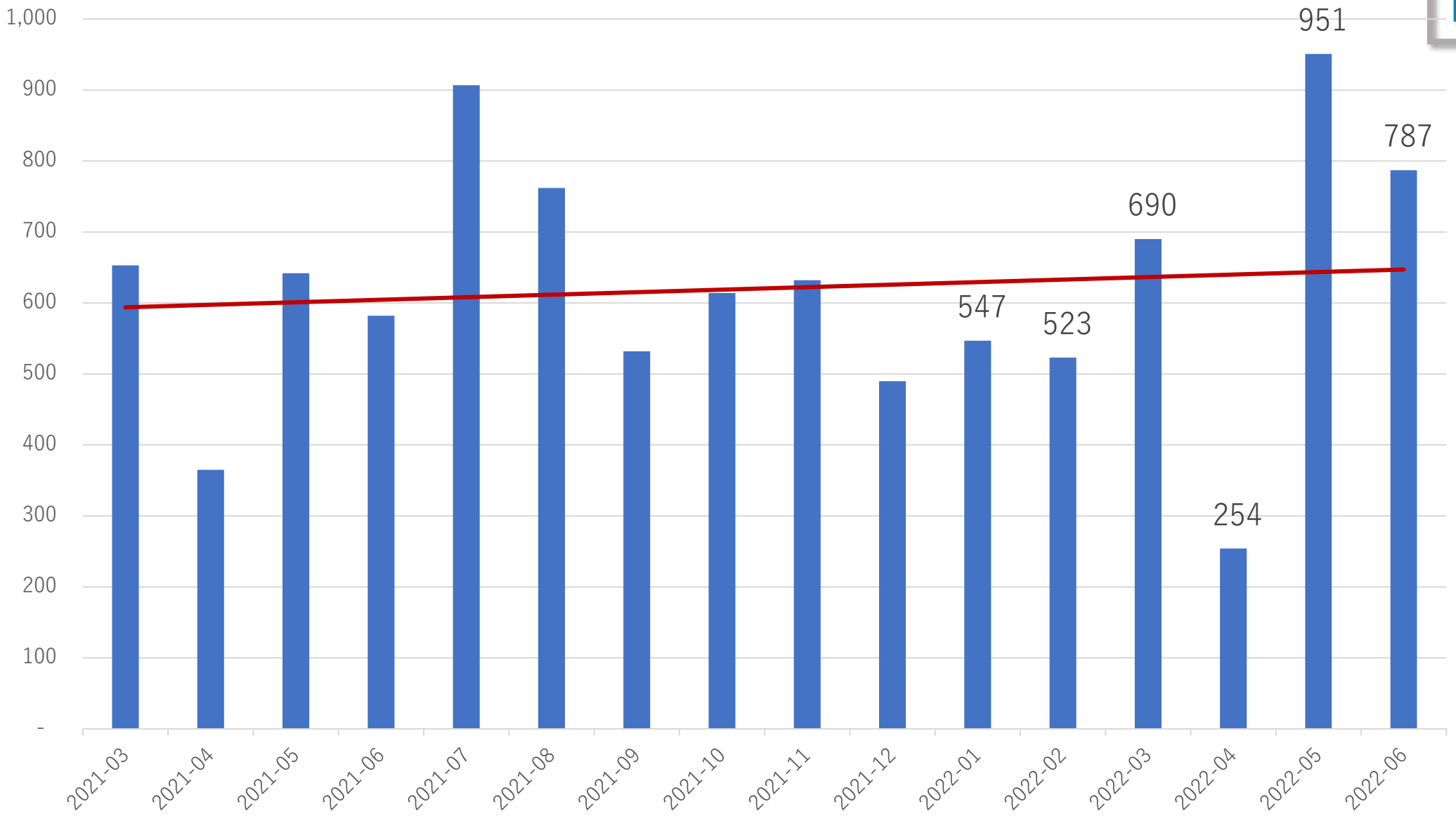
2021 Q3

- Total BIMI records observed: **9,860**
- Including link to a VMC: **179**

2022 Q2

- Total BIMI records observed: **15,004**
- Including link to VMC: **930**

New BIMI Records By Month



JPAAWG

Thank you