令和4年度 総務省事業 ISPにおけるネットワークセキュリティ技術の導入に関する調査より

DMARC技術 関連調査結果報告

2023.11.06

三菱総合研究所 先進技術・セキュリティ事業本部

目次

事業の背景

- 情報通信分野の急速な技術革新により、高度化・多様化した電気通信サービスが国民各層に広く普及・浸透し、国民生活に大きな利便性をもたらす一方、電子メールのなりすまし、迷惑メール等の被害は継続して発生している状況である。
- 総務省では、インターネットの安全性、信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境を実現するため、電子メールのなりすまし対策や迷惑メール対策、及び経路ハイジャックの抑止のための認証技術の普及促進を行っているが、国内ISPでの導入は一部にとどまっている。
- このため、昨年度はこれら各種の認証技術のうちDMARCの導入を促すこと目的とし、導入の課題を調査し、課題解決に向けた論点を整理した。

技術的課題の調査

- 本調査報告は、総務省事業である「令和4年度ISPにおけるネットワークセキュリティ技術の導入に関する調査」における技術的課題の調査内容をまとめたものである。
- 本調査では、以下の4点について調査した。

❶ メール環境 メール環境の調査、DNS権威サービスの調査

ホスティング・クラウドサービスについて、送信ドメイン認証関連の機能やDNSゾーン仕様を調査し、SPF/DKIM/DMARCレコードを自組織のドメインで設定する際の参考情報を取り纏める。

❷ 個人UX 個人UXの改善・情報共有に関する調査

DMARC検証結果をどのようにエンドユーザに対して可視化するか・体験してもらうかについて代表的な2つの実施方法を調査する。

❸ OSS調査 SPF/DKIM/DMARCのOSS調査・パフォーマンス調査

利用されている2つのOSSについて、利用可能な機能を整理し、メールシステムに導入した際のパフォーマンス計測し、DMARC検証機能の参考情報として取り纏める。

❹ チェックサイト DMARC設定等を外部からチェックできるサイトの開発・構築に関する調査

既存のチェックサイト等を参考に、対応状況や設定状況をチェックするために必要な項目・機能を調査する。

1. メール環境の調査、DNS権威サービスの調査

1.1. 調査概要

- 本調査では、まず、企業・組織がメール送信で利用するドメインに対してDMARCを導入する際にどのような設定が必要であるかを整理する。次に、利用が拡大しているクラウドサービスにおいて、企業・組織がDMARCを導入する際に必要な機能を有しているかについて調査を実施した。具体的には以下のとおりである。

  - **企業・組織がDMARCを導入する際に必要なDNS設定およびメール送信サーバの機能**
  - **権威DNSクラウドサービスに関する調査**
  - **メール送信クラウドサービスに関する調査**

1.2. 企業・組織がDMARCを導入する際に必要なDNS設定およびメール送信サーバの機能 1/3

- DMARCを適切に運用するためには、メール受信側である国内ISPのDMARC認証への対応だけではなく、メール送信側である企業・組織もDMARCの導入が必要である。第一に、利用しているメール送信システムを把握・整理して、それらの送信元IPアドレスをSPFレコードとして登録する。第二に、利用しているメール送信システムにDKIM署名付与の機能を実装する。第三にDMARCレコード（p=none）を設定して、DMARC集計レポートを分析する。そして、正当なメールが適切にDMARC認証で成功していることを確認したのち、DMARCレコードのポリシーを隔離（p=quarantine）あるいは拒否（p=reject）へ変更する（図1）。

図1 企業・組織のDMARC運用ワークフロー例

出所）三菱総合研究所

1.2. 企業・組織がDMARCを導入する際に必要なDNS設定およびメール送信サーバの機能 2/3

- これらの活動に際しては、SPFレコード、DKIMレコードおよびDMARCレコードの設定が当該ドメインの権威DNSの設定作業が必要である。そして、権威DNSクラウドサービスを利用している場合は、これらDMARCに関連するリソースレコードの設定に関する機能を有するか、あらかじめ確認する必要がある。ここでは、具体的に権威DNSクラウドサービスにおいて、どのような機能が必要であるかの調査項目を整理した（表1）。
- これら10の機能のうち、DMARCの導入に必須となる機能は1、3、4および8である。

表1 権威DNSクラウドサービス調査項目一覧

認証技術	必須	権威DNSクラウドサービスの機能
SPF	●	1.TXTリソースレコードが設定できるか
	任意	2.SPFレコードの構文チェック機能があるか
DKIM	●	3.ドメインに対してラベル”_domainkey”を設定できるか
	●	4.TXTリソースレコードの文字数が十分な文字列の長さを設定できるか
	任意	5.DKIMレコードの構文チェック機能があるか
	任意	6.DKIMセレクターのロールオーバー支援機能があるか
	任意	7.CNAMEリソースレコードが設定できるか
DMARC	●	8.ドメイン名に対してラベル”_dmarc”を設定できるか
	任意	9.DMARCレコードの構文チェック機能があるか
その他	任意	10.マニュアルにSPFレコード・DKIMレコード・DMARCレコードの設定について言及があるか

1.2. 企業・組織がDMARCを導入する際に必要なDNS設定およびメール送信サーバの機能 3/3

- 多くの企業・組織ではメール送信システム(の一部)をクラウドサービス(メール送信クラウドサービス)に移行しており、権威DNSだけではなくメール送信クラウドサービスについても、DMARCに対応しているかを把握する必要がある。ここでは、具体的にメール送信サービスにおいて、どのような機能が必要であるかを整理した(表2)。
- これら11の機能のうち、DMARCの導入に必須となる機能は1、3、4および8である。ただし、8においてエンベロープFromドメインを企業ドメインで設定できない(SPF認証においてアライメントできない)場合は、1は必須ではない。

表2 メール送信クラウドサービス調査項目一覧

認証技術	必須	メール送信クラウドサービスの機能
SPF	●	1.SPFレコードにincludeする送信元情報が用意されているか
	任意	2.SPFレコードの設定アシスタント機能があるか
DKIM	●	3.DKIM鍵生成ができるか、もしくはDKIM秘密鍵をアップロードする機能が用意されているか
	●	4.DKIM鍵長は1024ビット以上が設定できるか
	任意	5.DKIMレコードの設定アシスタント機能があるか
	任意	6.DKIM鍵の自動ローテーション機能があるか
	任意	7.DKIM鍵の手動廃止機能はあるか
DMARC	●	8.エンベロープFromドメインを企業ドメインで設定できるか、もしくはDKIM署名ドメインを企業ドメインで設定できるか
	任意	9.DMARCレコードの設定アシスタント機能があるか
	任意	10.DMARC集計レポートの分析機能があるか
その他	任意	11.マニュアルにSPF認証対応・DKIM署名対応・DMARC認証対応について言及があるか

1.3. 権威DNSクラウドサービスに関する調査

- 表1で挙げられた調査項目について、権威DNSに対応した代表的なクラウドサービスとして、Amazon Route 53、Cloud DNS、お名前.com、IIJ ドメイン管理サービス、さくらのクラウド、ニフクラ、QUALITIA DNSを調査した（表3）

表3 調査対象の権威DNSクラウドサービスに関する公開情報

サービス	公開情報URL	調査時期
❶ Amazon Route 53	https://aws.amazon.com/jp/route53/features/	2023年1月
❷ Cloud DNS	https://cloud.google.com/dns?hl=ja	2022年12月
❸ お名前.com	https://www.onamae.com/guide/p/70	2022年12月
❹ IIJ ドメイン管理サービス	https://www.iij.ad.jp/biz/dns-pfm/ https://manual.iij.jp/dpf/help/	2023年1月
❺ さくらのクラウド	https://manual.sakura.ad.jp/cloud/appliance/dns/index.html	2023年1月
❻ ニフクラ	https://pfs.nifcloud.com/spec/dns/	2023年1月
❼ QUALITIA DNS	https://product.qt-dns.com/functions.html	2023年2月

1.3.1. Amazon Route 53の機能仕様

- 2023年1月時点で、Amazon Route 53における権威DNSクラウドサービス調査項目一覧の対応状況は以下のとおりである（表4）。

表4 Amazon Route 53の「権威DNSクラウドサービス調査項目」結果一覧

調査項目	対応状況	補足情報
1. TXTリソースレコードが設定できるか	●	SPFのリソースレコードも非推奨と表示されているが登録可能
2. SPFレコードの構文チェック機能があるか	なし	
3. ドメインに対してラベル”_domainkey”を設定できるか	●	
4. TXTリソースレコードの文字数が十分な文字列の長さを設定できるか	●	最大4,000文字
5. DKIMレコードの構文チェック機能があるか	なし	
6. DKIMセレクターのロールオーバー支援機能があるか	なし	
7. CNAMEリソースレコードが設定できるか	●	
8. ドメイン名に対してラベル”_dmarc”を設定できるか	●	
9. DMARCレコードの構文チェック機能があるか	なし	
10. マニュアルにSPFレコード・DKIMレコード・DMARCレコードの設定について言及があるか	なし	

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- Amazon Route 53については、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.3.2. Cloud DNSの機能仕様 1/3

- 2022年12月時点で、Cloud DNSにおける権威DNSクラウドサービス調査項目の対応状況は以下のとおりである（表5）。なお、構文チェック機能に関連した情報を付記する（図2～図5）。

表5 Cloud DNSの「権威DNSクラウドサービス調査項目」結果一覧

調査項目	対応状況	補足情報
1. TXTリソースレコードが設定できるか	●	SPFのリソースレコードも非推奨と表示されているが登録可
2. SPFレコードの構文チェック機能があるか	△	部分的にチェック（図2、図3）
3. ドメインに対してラベル”_domainkey”を設定できるか	●	
4. TXTリソースレコードの文字数が十分な文字列の長さを設定できるか	●	最大255文字
5. DKIMレコードの構文チェック機能があるか	△	部分的にチェック（図4、図5）
6. DKIMセレクターのロールオーバー支援機能があるか	なし	
7. CNAMEリソースレコードが設定できるか	●	
8. ドメイン名に対してラベル”_dmarc”を設定できるか	●	
9. DMARCレコードの構文チェック機能があるか	△	部分的にチェック（図4、図5）
10. マニュアルにSPFレコード・DKIMレコード・DMARCレコードの設定について言及があるか	なし	

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- Could DNSについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.3.2. Cloud DNSの機能仕様 2/3

図2 Cloud DNSの警告文①（v=spf1の後方にスペースがない場合）

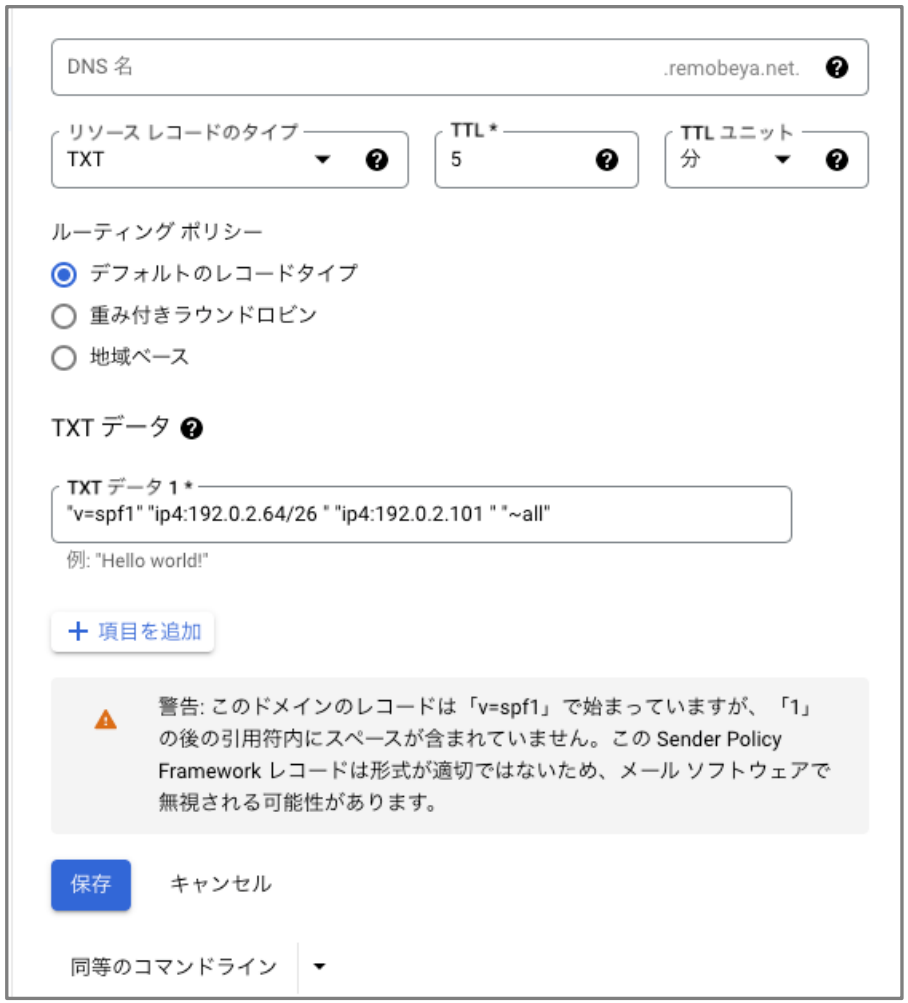


図3 Cloud DNSの警告文①の解消例

1.3.2. Cloud DNSの機能仕様 3/3

図4 Cloud DNSの警告文②（引用符で値が囲まれていない場合）

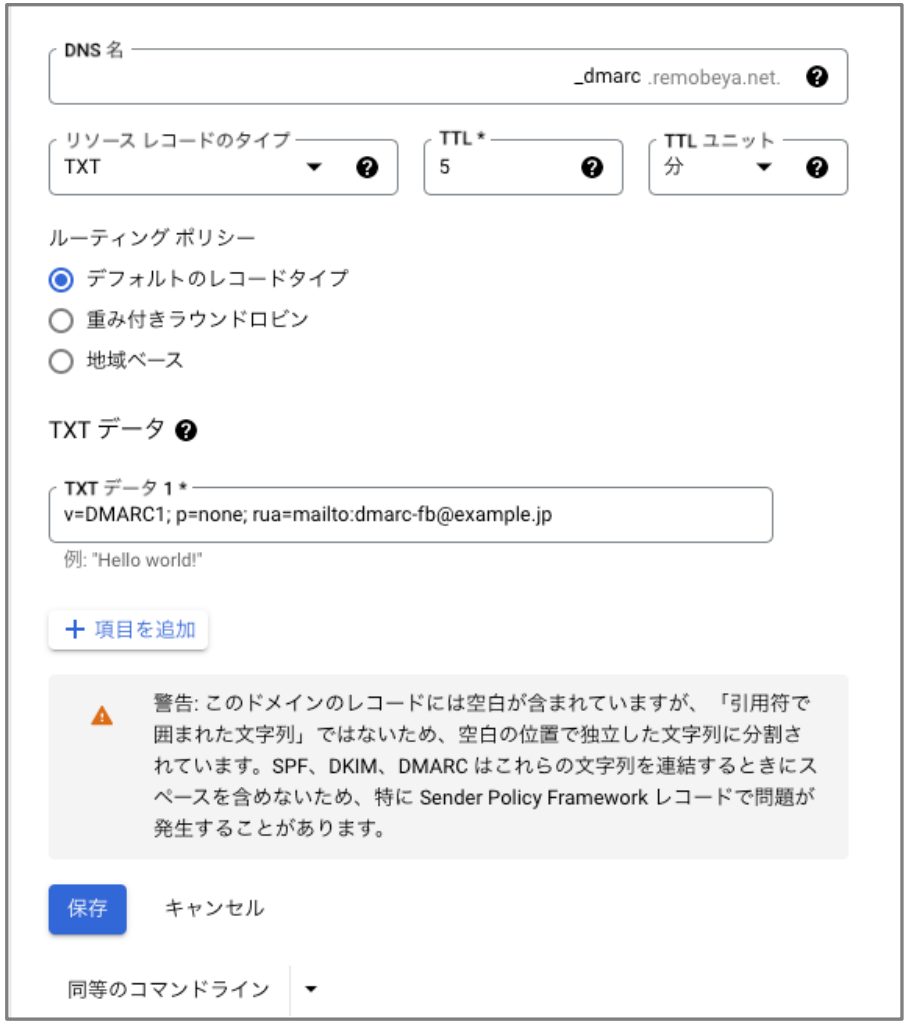


図5 Cloud DNSの警告文②の解消例

1.3.3. お名前.comの機能仕様

- 2022年12月時点で、お名前.comにおける権威DNSクラウドサービス調査項目の対応状況は以下のとおりである（表6）。

表6 お名前.comの「権威DNSクラウドサービス調査項目」結果一覧

調査項目	対応状況	補足情報
1. TXTリソースレコードが設定できるか	●	SPFのリソースレコードは設定不可
2. SPFレコードの構文チェック機能があるか	なし	ヘルプで設定例の記載あり
3. ドメインに対してラベル”_domainkey”を設定できるか	●	
4. TXTリソースレコードの文字数が十分な文字列の長さを設定できるか	●	最大510文字
5. DKIMレコードの構文チェック機能があるか	なし	
6. DKIMセレクターのロールオーバー支援機能があるか	なし	
7. CNAMEリソースレコードが設定できるか	●	
8. ドメイン名に対してラベル”_dmarc”を設定できるか	●	
9. DMARCレコードの構文チェック機能があるか	なし	
10. マニュアルにSPFレコード・DKIMレコード・DMARCレコードの設定について言及があるか	●	

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- お名前.comについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.3.4. IIJドメイン管理サービスの機能仕様

- 2023年1月時点で、IIJドメイン管理サービスにおける権威DNSクラウドサービス調査項目の対応状況は以下のとおりである（表7）。

表7 IIJドメイン管理サービスの「権威DNSクラウドサービス調査項目」結果一覧

調査項目	対応状況	補足情報
1. TXTリソースレコードが設定できるか	●	SPFのリソースレコードは設定不可
2. SPFレコードの構文チェック機能があるか	なし	
3. ドメインに対してラベル”_domainkey”を設定できるか	●	
4. TXTリソースレコードの文字数が十分な文字列の長さを設定できるか	●	詳細不明
5. DKIMレコードの構文チェック機能があるか	なし	
6. DKIMセレクターのロールオーバー支援機能があるか	なし	
7. CNAMEリソースレコードが設定できるか	●	
8. ドメイン名に対してラベル”_dmarc”を設定できるか	●	
9. DMARCレコードの構文チェック機能があるか	なし	
10. マニュアルにSPFレコード・DKIMレコード・DMARCレコードの設定について言及があるか	なし	

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- IIJドメイン管理サービスについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.3.5. さくらのクラウドの機能仕様

- 2023年1月時点で、さくらのクラウドにおける権威DNSクラウドサービス調査項目の対応状況は以下のとおりである（表8）。

表8 さくらのクラウドの「権威DNSクラウドサービス調査項目」結果一覧

調査項目	対応状況	補足情報
1. TXTリソースレコードが設定できるか	●	SPFのリソースレコードは設定不可
2. SPFレコードの構文チェック機能があるか	なし	
3. ドメインに対してラベル”_domainkey”を設定できるか	●	
4. TXTリソースレコードの文字数が十分な文字列の長さを設定できるか	●	最大500文字
5. DKIMレコードの構文チェック機能があるか	なし	
6. DKIMセレクターのロールオーバー支援機能があるか	なし	
7. CNAMEリソースレコードが設定できるか	●	
8. ドメイン名に対してラベル”_dmarc”を設定できるか	●	
9. DMARCレコードの構文チェック機能があるか	なし	
10. マニュアルにSPFレコード・DKIMレコード・DMARCレコードの設定について言及があるか	なし	

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- さくらのクラウドについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.3.6. ニフクラの機能仕様

- 2023年1月時点で、ニフクラにおける権威DNSクラウドサービス調査項目の対応状況は以下のとおりである（表9）。

表9 ニフクラの「権威DNSクラウドサービス調査項目」結果一覧

調査項目	対応状況	補足情報
1. TXTリソースレコードが設定できるか	●	SPFのリソースレコードは設定不可
2. SPFレコードの構文チェック機能があるか	なし	
3. ドメインに対してラベル”_domainkey”を設定できるか	●	
4. TXTリソースレコードの文字数が十分な文字列の長さを設定できるか	不明	記載なし
5. DKIMレコードの構文チェック機能があるか	なし	
6. DKIMセレクターのロールオーバー支援機能があるか	なし	
7. CNAMEリソースレコードが設定できるか	●	
8. ドメイン名に対してラベル”_dmarc”を設定できるか	●	
9. DMARCレコードの構文チェック機能があるか	なし	
10. マニュアルにSPFレコード・DKIMレコード・DMARCレコードの設定について言及があるか	なし	

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- ニフクラについては、調査項目のうち必須項目（1、3、4、8）は4以外で満たしている。4については確認できなかった。

1.3.7. QUALITIA DNSの機能仕様 1/5

- 2023年2月時点で、QUALITIA DNSにおける権威DNSクラウドサービス調査項目の対応状況は以下のとおりである（表10）。なお、構文チェック機能に関連した情報を付記する（図6～10）。加えて、BIMIに関連した構文チェック機能が確認できる（図11～13）。

表10 QUALITIA DNSの「権威DNSクラウドサービス調査項目」結果一覧

調査項目	対応状況	補足情報
1. TXTリソースレコードが設定できるか	●	
2. SPFレコードの構文チェック機能があるか	●	IPアドレスやCIDRの文法チェック（図6、図7）
3. ドメインに対してラベル”_domainkey”を設定できるか	●	
4. TXTリソースレコードの文字数が十分な文字列の長さを設定できるか	●	最大64,771文字
5. DKIMレコードの構文チェック機能があるか	●	不正な公開鍵、1024ビット未満の公開鍵のチェック （図8、図9）
6. DKIMセレクターのロールオーバー支援機能があるか	なし	
7. CNAMEリソースレコードが設定できるか	●	
8. ドメイン名に対してラベル”_dmarc”を設定できるか	●	
9. DMARCレコードの構文チェック機能があるか	●	レコードの構文チェック（図10）
10. マニュアルにSPFレコード・DKIMレコード・DMARCレコードの設定について言及があるか	△	設定ウィザードで対応

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- QUALITIA DNSについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.3.7. QUALITIA DNSの機能仕様 2/5

図6 SPFレコード設定アシスタント機能

図7 SPFレコード設定アシスタント機能の警告（不正な入力値の場合）

1.3.7. QUALITIA DNSの機能仕様 3/5

図8 DKIMレコード設定アシスタント機能

図9 DKIMレコード設定アシスタント機能の警告（不正な公開鍵の場合）

1.3.7. QUALITIA DNSの機能仕様 4/5

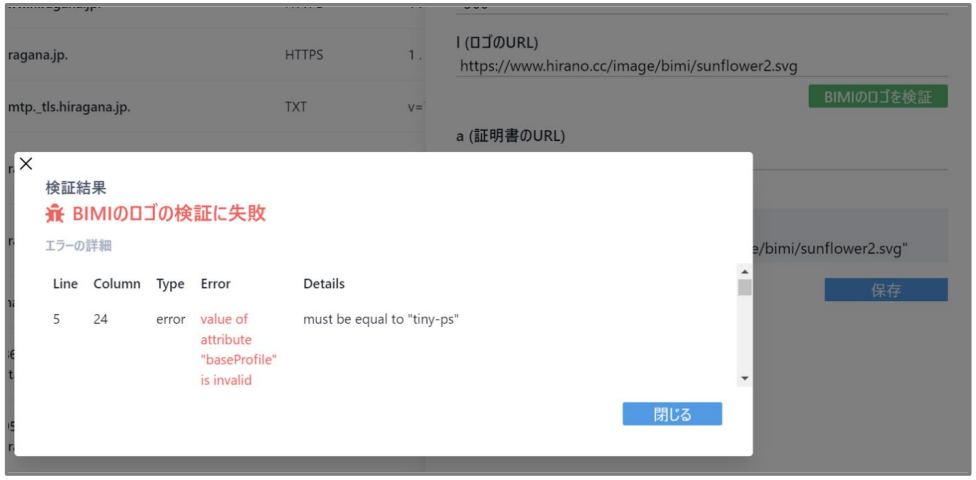
図10 DMARCレコード設定アシスタント機能

図11 BIMIレコード設定アシスタント機能

1.3.7. QUALITIA DNSの機能仕様 5/5

図12 BIMIレコード設定アシスタント機能
（正しいロゴ画像の場合）

図13 BIMIレコード設定アシスタント機能
（不正なロゴ画像の場合）



1.4. メール送信クラウドサービスに関する調査

- 表2で挙げられた調査項目について、代表的なメール送信クラウドサービスとして、Amazon SES、SendGrid、MailPublisher、ClickM@iler、SPIRAL、ニフクラESS、WEBCAS e-mailを調査した（表11）。

表11 調査対象のメール送信クラウドサービスに関する公開情報

サービス	公開情報URL	調査時期
❶ Amazon SES	https://docs.aws.amazon.com/ja_jp/ses/index.html	2022年12月
❷ SendGrid	https://sendgrid.kke.co.jp/docs/index.html	2022年12月
❸ MailPublisher	https://mp-portal.force.com/s/article/000004060	2022年12月
❹ ClickM@iler ASP	https://www.clickmailer.jp/func/	2023年1月
❺ SPIRAL	https://support.smp.ne.jp/faq/	2023年1月
❻ ニフクラESS	https://pfs.nifcloud.com/guide/ess/sender_auth.htm	2023年1月
❼ WEBCAS e-mail	https://www.webcas.jp/email/price/	2023年2月

1.4.1. Amazon SESの機能仕様 1/2

- 2022年12月時点で、Amazon SESにおけるDMARC関連機能の対応状況は以下のとおりである（表12）。なお、アシスタント機能に関連した情報及びマニュアル情報を付記する（図14～15）。

表12 Amazon SESのDMARC関連機能の対応状況

調査項目	対応状況	補足情報
1. SPFレコードにincludeする送信元情報が用意されているか	●	”v=spf1 include:amazonses.com ~all”
2. SPFレコードの設定アシスタント機能があるか	なし	ドキュメントに記載あり
3. DKIM鍵生成ができるか、もしくはDKIM秘密鍵をアップロードする機能が用意されているか	●	
4. DKIM鍵長は1024ビット以上が設定できるか	●	Amazon Route 53を利用中のドメイン場合は、CNAMEを自動で設定
5. DKIMレコードの設定アシスタント機能があるか	●	Easy DKIM機能 （図14、図15）
6. DKIM鍵の自動ローテーション機能があるか	●	
7. DKIM鍵の手動廃止機能はあるか	●	
8. エンベロープFromドメインを企業ドメインで設定できるか、もしくはDKIM署名ドメインを企業ドメインで設定できるか	●	
9. DMARCレコードの設定アシスタント機能があるか	なし	
10. DMARC集計レポートの分析機能があるか	なし	
11. マニュアルにSPF認証対応・DKIM署名対応・DMARC認証対応について言及があるか	●	※（次頁）

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- Amazon SESについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.4.1. Amazon SESの機能仕様 2/2

図14 Easy DKIMの設定画面

図15 Easy DKIMの設定後のDNSレコード表示

※Amazon SESが提供するマニュアルは以下のとおりである。

https://docs.aws.amazon.com/ja_jp/ses/latest/dg/send-email-authentication-spf.html
https://docs.aws.amazon.com/ja_jp/ses/latest/dg/send-email-authentication-dkim.html
https://docs.aws.amazon.com/ja_jp/ses/latest/dg/send-email-authentication-dmarc.html

1.4.2. SendGridの機能仕様 1/2

- 2022年12月時点で、SendGridにおけるDMARC関連機能の対応状況は以下のとおりである（表13）。なお、マニュアル情報を付記する。

表13 SendGridのDMARC関連機能の対応状況

調査項目	対応状況	補足情報
1. SPFレコードにincludeする送信元情報が用意されているか	△	includeが不要な運用。※1（次頁） 該当のサブドメインをエンベロープFromドメインとして送信。
2. SPFレコードの設定アシスタント機能があるか	なし	
3. DKIM鍵生成ができるか、もしくはDKIM秘密鍵をアップロードする機能が用意されているか	△	CNAMEでの指定のみ
4. DKIM鍵長は1024ビット以上が設定できるか		CNAMEでの指定のみ
5. DKIMレコードの設定アシスタント機能があるか	なし	
6. DKIM鍵の自動ローテーション機能があるか	●	
7. DKIM鍵の手動廃止機能はあるか	なし	
8. エンベロープFromドメインを企業ドメインで設定できるか、もしくはDKIM署名ドメインを企業ドメインで設定できるか	●	該当のサブドメインをエンベロープFromドメインとして送信
9. DMARCレコードの設定アシスタント機能があるか	なし	
10. DMARC集計レポートの分析機能があるか	なし	外部サービスの利用を推奨
11. マニュアルにSPF認証対応・DKIM署名対応・DMARC認証対応について言及があるか	●	※2（次頁）

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- SendGridについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.4.2. SendGridの機能仕様 2/2

- ただし、8において、エンベロープFromドメインが企業ドメインを設定できないため、1については必須ではない。なお、DKIM鍵生成機能の代わりにCNAMEでの設定のみである。

※1 サブドメインでCNAMEを指定し、そのCNAMEのTXTで送信元IPアドレスを設定しているため

※2 SendGridが提供するマニュアルは以下のとおりである

https://sendgrid.kke.co.jp/docs/User Manual JP/Settings/Sender authentication/How to set up domain authentication.html

https://sendgrid.kke.co.jp/docs/User Manual JP/Settings/Sender authentication/How to set up domain authentication.html

1.4.3. MailPublisherの機能仕様 1/2

- 2022年12月時点で、MailPublisherにおけるDMARC関連機能の対応状況は以下のとおりである（表14）。なお、アシスタント機能に関連した情報及びマニュアル情報を付記する（図16、図17）。

表14 MailPublisherのDMARC関連機能の対応状況

調査項目	対応状況	補足情報
1. SPFレコードにincludeする送信元情報が用意されているか	●	”v=spf1 include:spf-bma.mpme.jp ~all”
2. SPFレコードの設定アシスタント機能があるか	●	SPF検証結果確認 （図16）
3. DKIM鍵生成ができるか、もしくはDKIM秘密鍵をアップロードする機能が用意されているか	●	
4. DKIM鍵長は1024ビット以上が設定できるか	●	
5. DKIMレコードの設定アシスタント機能があるか	●	送信ドメイン認証 -署名設定 （図17）
6. DKIM鍵の自動ローテーション機能があるか	なし	利用者が管理画面で再設定する
7. DKIM鍵の手動廃止機能はあるか	●	
8. エンベロープFromドメインを企業ドメインで設定できるか、もしくはDKIM署名ドメインを企業ドメインで設定できるか	●	
9. DMARCレコードの設定アシスタント機能があるか	●	設定状況の確認 （図17）
10. DMARC集計レポートの分析機能があるか	なし	外部サービスの利用を推奨
11. マニュアルにSPF認証対応・DKIM署名対応・DMARC認証対応について言及があるか	●	※（次頁）

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- MailPublisherについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.4.3. MailPublisherの機能仕様 2/2

図16 SPF検証結果確認画面
（オンラインマニュアルより）

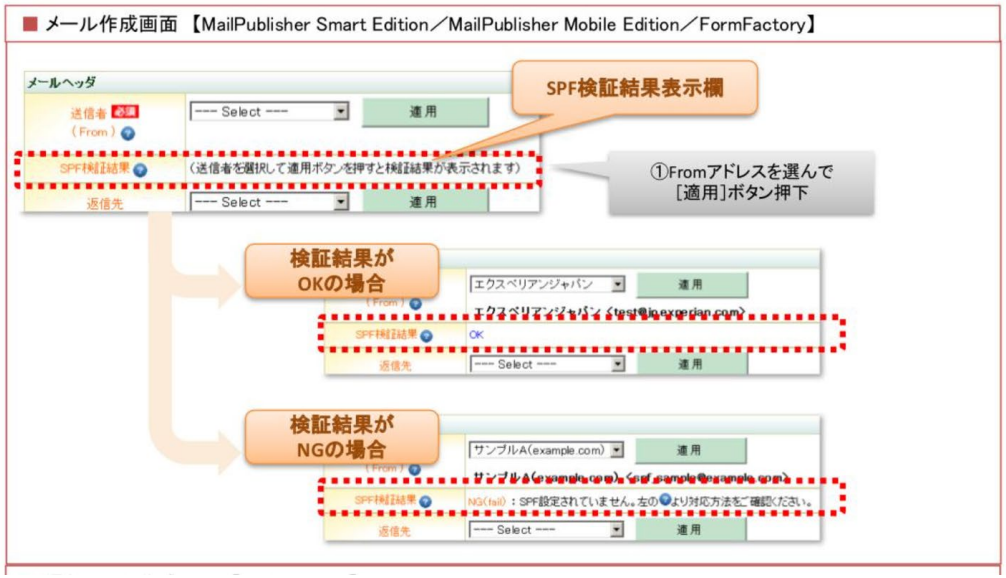


図17 DKIMの設定画面およびDMARCレコード
設定状況確認画面

※MailPublisherが提供するマニュアルは以下のとおりである。

https://mp-portal.force.com/s/manuals/mpse-manuals
https://mp-portal.force.com/s/article/S00043
https://mp-portal.force.com/s/article/000004060

1.4.4. ClickM@iler ASPの機能仕様 1/2

- 2023年1月時点で、ClickM@iler ASPにおけるDMARC関連機能の対応状況は以下のとおりである（表15）。

表15 ClickM@iler ASPのDMARC関連機能の対応状況

調査項目	対応状況	補足情報
1. SPFレコードにincludeする送信元情報が用意されているか	●	個別に案内
2. SPFレコードの設定アシスタント機能があるか	なし	利用者に資料で説明
3. DKIM鍵生成ができるか、もしくはDKIM秘密鍵をアップロードする機能が用意されているか	なし	利用者に資料で説明 また、運営会社にて設定作業も可能
4. DKIM鍵長は1024ビット以上が設定できるか	●	
5. DKIMレコードの設定アシスタント機能があるか	なし	利用者に資料で説明
6. DKIM鍵の自動ローテーション機能があるか	なし	利用者に資料で説明 また、運営会社にてローテーション作業も可能
7. DKIM鍵の手動廃止機能はあるか	なし	利用者に資料で説明 また、運営会社にて廃止作業も可能
8. エンベロープFromドメインを企業ドメインで設定できるか、もしくはDKIM署名ドメインを企業ドメインで設定できるか	●	
9. DMARCレコードの設定アシスタント機能があるか	なし	利用者に資料で説明
10. DMARC集計レポートの分析機能があるか	なし	外部サービスの利用を推奨
11. マニュアルにSPF認証対応・DKIM署名対応・DMARC認証対応について言及があるか	●	個別に案内

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

1.4.4. ClickM@iler ASPの機能仕様 2/2

- ClickM@iler ASPについては、調査項目のうち必須項目（1、3、4、8）のうち、1、4、8は満たしている。なお、3については、運営会社が個別で設定することも可能である。

1.4.5. SPIRALの機能仕様 1/2

- 2023年1月時点で、SPIRALにおけるDMARC関連機能の対応状況は以下のとおりである（表16）。

表16 SPIRALのDMARC関連機能の対応状況

調査項目	対応状況	補足情報
1. SPFレコードにincludeする送信元情報が用意されているか	●	※1（次頁）
2. SPFレコードの設定アシスタント機能があるか	なし	ドキュメントに記載あり
3. DKIM鍵生成ができるか、もしくはDKIM秘密鍵をアップロードする機能が用意されているか	なし	
4. DKIM鍵長は1024ビット以上が設定できるか	●	
5. DKIMレコードの設定アシスタント機能があるか	なし	
6. DKIM鍵の自動ローテーション機能があるか	なし	
7. DKIM鍵の手動廃止機能はあるか	なし	
8. エンベロープFromドメインを企業ドメインで設定できるか、もしくはDKIM署名ドメインを企業ドメインで設定できるか	●	
9. DMARCレコードの設定アシスタント機能があるか	なし	
10. DMARC集計レポートの分析機能があるか	なし	
11. マニュアルにSPF認証対応・DKIM署名対応・DMARC認証対応について言及があるか	●	※2（次頁）

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- SPIRALについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.4.5. SPIRALの機能仕様 2/2

※1 SPFレコードにincludeする送信元情報

Ver.1 https://support.smp.ne.jp/faq/mail-faq/f0043/

Ver.2 https://support.spiral-platform.com/etc/2740.html

※2 SPIRALが提供するマニュアルは以下のとおりである。

https://support.smp.ne.jp/manuals/mail/spf dkim dmarc/

https://support.smp.ne.jp/faq/mail-faq/f0043/

https://support.smp.ne.jp/manuals/mail/dkim domain list/

https://support.spiral-platform.com/function/193.html

https://support.spiral-platform.com/etc/2740.html

1.4.6. ニフクラESSの機能仕様 1/2

- 2023年1月時点で、ニフクラESSにおけるDMARC関連機能の対応状況は以下のとおりである（表17）。なお、マニュアル情報を付記する。

表17 ニフクラESSのDMARC関連機能の対応状況

調査項目	対応状況	補足情報
1. SPFレコードにincludeする送信元情報が用意されているか	●	”v=spf1 include:spf.ess.nifcloud.com -all”
2. SPFレコードの設定アシスタント機能があるか	なし	
3. DKIM鍵生成ができるか、もしくはDKIM秘密鍵をアップロードする機能が用意されているか	△	CNAMEでの指定のみ
4. DKIM鍵長は1024ビット以上が設定できるか	●	CNAMEでの指定のみ
5. DKIMレコードの設定アシスタント機能があるか	なし	
6. DKIM鍵の自動ローテーション機能があるか	●	
7. DKIM鍵の手動廃止機能はあるか	なし	
8. エンベロープFromドメインを企業ドメインで設定できるか、もしくはDKIM署名ドメインを企業ドメインで設定できるか	●	
9. DMARCレコードの設定アシスタント機能があるか	なし	
10. DMARC集計レポートの分析機能があるか	なし	
11. マニュアルにSPF認証対応・DKIM署名対応・DMARC認証対応について言及があるか	●	※（次頁）

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- ニフクラESSについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.4.6. ニフクラESSの機能仕様 2/2

- なお、DKIM鍵生成機能の代わりにCNAMEでの設定のみである。

  ※ニフクラESSが提供するマニュアルは以下のとおりである。

  https://pfs.nifcloud.com/guide/ess/sender auth.htm

1.4.7. WEBCAS e-mailの機能仕様 1/2

- 2023年2月時点で、WEBCAS e-mailにおけるDMARC関連機能の対応状況は以下のとおりである（表18）。なお、アシスタント機能に関連した情報を付記する（図18、図19）。

表18 WEBCAS e-mailのDMARC関連機能の対応状況

調査項目	対応状況	補足情報
1. SPFレコードにincludeする送信元情報が用意されているか	●	ASP型とSaaS型で異なる
2. SPFレコードの設定アシスタント機能があるか	●	passとならない状態の場合に警告
3. DKIM鍵生成ができるか、もしくはDKIM秘密鍵をアップロードする機能が用意されているか	●	
4. DKIM鍵長は1024ビット以上が設定できるか	●	
5. DKIMレコードの設定アシスタント機能があるか	●	DNSレコードに設定する内容を画面に表示。 なお、DNSレコード設定は利用者側で実施。 （図18、図19）
6. DKIM鍵の自動ローテーション機能があるか	なし	
7. DKIM鍵の手動廃止機能はあるか	なし	
8. エンベロープFromドメインを企業ドメインで設定できるか、もしくはDKIM署名ドメインを企業ドメインで設定できるか	●	※（次頁）
9. DMARCレコードの設定アシスタント機能があるか	なし	
10. DMARC集計レポートの分析機能があるか	なし	
11. マニュアルにSPF認証対応・DKIM署名対応・DMARC認証対応について言及があるか	●	利用者向けマニュアルに記載

●:対応、△:一部対応もしくは代替機能あり、なし:対応が確認できなかった

- WEBCAS e-mailについては、調査項目のうち必須項目（1、3、4、8）は全て満たしている。

1.4.7. WEBCAS e-mailの機能仕様 2/2

図18 WEBCAS e-mailのDKIM署名設定照会画面

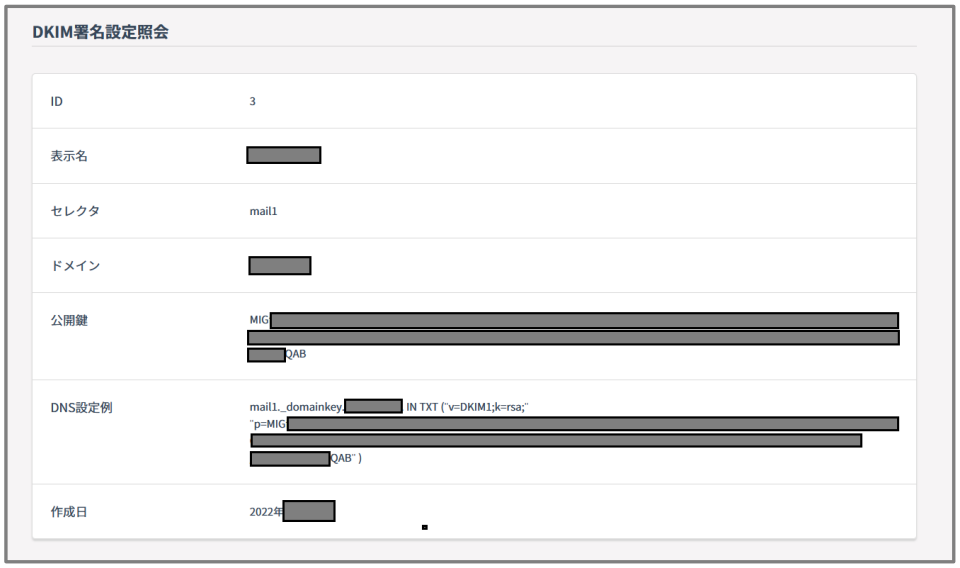


図19 WEBCAS e-mailのDKIM署名設定画面

※ ASP型とSaaS型で異なる。エンベロープFromドメインは、SaaS型のみ対応。DKIM署名ドメインは、両方対応。

1.5.1. 権威DNSサービス調査結果のまとめ

- 本調査の対象となる権威DNSサービスについては、いずれのサービスも必須項目は全て満たしていた（表19）。一方で、SPF、DKIMおよびDMARCレコードの構文チェック機能やそれに該当する支援機能は用意されていないサービスが大半であった（表20）。

表19 権威DNSサービスの調査項目（必須項目）のまとめ

サービス	1.TXTレコード設定	3."_domainkey"ラベル設定	4.TXT最大文字数	8."_dmarc"ラベル設定
Amazon Route 53	●	●	●	●
Cloud DNS	●	●	●	●
お名前.com	●	●	●	●
IIJ ドメイン管理サービス	●	●	●	●
さくらのクラウド	●	●	●	●
ニフクラ	●	●	不明	●
QUALITIA DNS	●	●	●	●

表20 権威DNSサービスの調査項目（構文チェック項目）のまとめ

サービス	2.SPF構文チェック	5.DKIM構文チェック	9.DMARC構文チェック
Amazon Route 53	なし	なし	なし
Cloud DNS	△	△	△
お名前.com	なし	なし	なし
IIJ ドメイン管理サービス	なし	なし	なし
さくらのクラウド	なし	なし	なし
ニフクラ	なし	なし	なし
QUALITIA DNS	●	●	●

1.5.2. メール送信クラウドサービス調査結果のまとめ

- 本調査の対象となるメール送信クラウドサービスについては、ほとんどのサービスで必須項目は全て満たしていた（表21）。また、一部のメール送信クラウドサービスでは、DKIMやDMARCを導入するためのアシスタント機能またはマニュアルが提供されていた（表22）。

表21 メール送信クラウドサービスの調査項目（必須項目）のまとめ

サービス	1.SPF include情報	3.DKIM秘密鍵設定機能	4.DKIM鍵長が1024ビット超	8.アライメント一致
Amazon SES	●	●	●	●
SendGrid	△	△	●	●
MailPublisher	●	●	●	●
ClickM@iler ASP	●	なし	●	●
SPIRAL	●	●	●	●
ニフクラESS	●	△	●	●
WEBCAS e-mail	●	●	●	●

表22 メール送信サービスの調査項目（構文チェック項目）のまとめ

サービス	1.SPF レコードアシスタント	5.DKIM レコードアシスタント	9.DMARC レコードアシスタント	11.マニュアル整備
Amazon SES	なし	●	なし	●
SendGrid	なし	なし	なし	●
MailPublisher	●	●	●	●
ClickM@iler ASP	なし	なし	なし	●
SPIRAL	なし	なし	なし	●
ニフクラESS	なし	なし	なし	●
WEBCAS e-mail	●	●	なし	●

1.6. 略称一覧

表23 略称一覧

本報告書でも表記	正式名称・意味など
DMARC	Domain-based Message Authentication, Reporting, and Conformance 送信ドメイン認証技術の一つ。SPFとDKIM両者を利用したメールのドメイン認証を補強する技術である。
DKIM	DomainKeys Identified Mail 送信ドメイン認証技術の一つ。送信元が付した電子署名により送信元情報の真偽及び電子メールの本文の改変を検知することができる。
SPF	Sender Policy Framework 送信ドメイン認証技術の一つ。エンベロープ情報の From メールアドレスのドメイン名をチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。
FQDN	Fully Qualified Domain Name TCP / IP ネットワーク上で、ドメイン名・サブドメイン名・ホスト名をすべて省略せずに指定した記述形式のことを指す。
OD	Organizational Domain 組織ドメインと呼ばれる、wwwなどのラベルを持たない登録ドメイン（ネイキッドドメイン）を指す。
BIMI	Brand Indicators for Message Identification Webメールやメールアプリで、DMARC認証が成功し、なりすまされていないメールに対して、その送信者ドメインに関連したロゴを表示する仕組み。
VMC	Verified Mark Certificate BIMIで表示するロゴが送信者ドメインの所有するロゴであることを証明する証明書。

2. 個人UXの改善・情報共有に関する調査

2.1. 調査概要

- 本調査では、すでにDMARC認証に対応したメールサービスおよびメールクライアントについて、認証結果をどのようにドメイン管理者や利用者に認知させているか、なりすましメールと正当なメールをどのように利用者に区別させるかの調査を実施した。具体的には以下のとおりである。

  - **既存メールサービスに関する調査**
  - **調査結果まとめ**

2.2. 調査対象メールサービスおよび調査項目 1/2

- DMARC認証に対応した代表的なメールサービスとして、海外サービスはGmail、Fastmail、Outlook on the web（以下、Outlook）を、国内サービスはYahoo!メール、So-net Webメール、Active! mailを調査した（表1）。

表1 調査対象のメールサービスのなりすましメールに関する公開情報

区分	メールサービス	公開情報URL
海外	❶ Gmail	https://support.google.com/a/answer/2466580?hl=ja
	❷ Fastmail	https://www.fastmail.help/hc/en-us/articles/1500000280461-Sender-authentication
	❸ Outlook	https://learn.microsoft.com/ja-jp/microsoft-365/security/office-365-security/message-headers-eop-mdo?view=o365-worldwide
国内	❹ Yahoo!メール	https://mail.yahoo.co.jp/antispam/dmarc.html
	❺ So-net Webメール	https://www.so-net.ne.jp/option/mail/basic/?page=tab domaincheck
	❻ Active! mail	https://www.qualitia.com/jp/product/am/function.html

2.2. 調査対象メールサービスおよび調査項目 2/2

- 前頁のメールサービスについて、以下の仕様および設定の調査をした（表2）。

表2 調査対象のメールサービスの調査項目

区分	仕様および設定	調査内容の詳細
基本仕様	宣言ポリシー	提供サービスのメールドメインにおいて、DMARCポリシー設定がnone、quarantine、rejectのいずれかであるか。
	DMARC認証	提供サービスで受信したメールにおいて、DMARC認証しているかどうか。
	ポリシー処理	提供サービスで受信したメールにおいて、DMARC認証に失敗したメールをポリシーに従った処理をするかどうか。
	集計レポート	提供サービスで受信したメールにおいて、DMARC集計レポートを提供しているかどうか。
	失敗レポート	提供サービスで受信したメールにおいて、DMARC失敗レポートを提供しているかどうか。
表示仕様	ヘッダー	提供サービスで受信したメールにおいて、ヘッダーにどのような認証結果を付与するか。 具体的には、Received-SPFヘッダーやAuthentication-Resultsヘッダーが想定される。
	ヘッダー以外	提供サービスで受信したメールにおいて、認証結果をヘッダー以外でどのように表示するか。
	アイコン	提供サービスで受信したメールにおいて、なりすましではないと判断されたメッセージに対して、正当性を示すアイコンを表示するかどうか。
ポリシー処理仕様	ポリシーなし	提供サービスで受信したメールにおいて、DMARC未対応ドメインからのメールをどのように取り扱うか。
	p=none	提供サービスで受信したメールにおいて、DMARCポリシーがnoneであるドメインからのメールをどのように取り扱うか。
	p=quarantine	提供サービスで受信したメールにおいて、DMARCポリシーがquarantineであるドメインからのメールをどのように取り扱うか。
	p=reject	提供サービスで受信したメールにおいて、DMARCポリシーがrejectであるドメインからのメールをどのように取り扱うか。
	警告表示	提供サービスで受信したメールにおいて、なりすましメールと判定された場合にどのような警告が表示されるか。

2.3.1.1. Gmailの調査結果

- Gmailは、Googleが運営するフリーメールサービスであり、ドメイン名はgmail.comである。2022年12月時点で、Gmailでは、宣言ポリシー、DMARC認証、ポリシー処理、集計レポート、失敗レポートの対応状況は以下のとおりである（表3）。

表3 GmailのDMARC基本仕様

宣言ポリシー	DMARC認証	ポリシー処理	集計レポート	失敗レポート
none	●	●	●	なし

2.3.1.2. Gmailのヘッダー認証結果表示 1/2

- Gmailでは、DMARC認証の結果および関連情報を以下のヘッダーへ付与する。具体的に付与されるヘッダーおよび記載内容は以下のとおりである（表4、次頁図1）。

表4 GmailのDMARC関連の認証結果表示仕様

ヘッダー名	認証技術	記載内容
Received-SPF	SPF	SPF認証結果
		エンベロープFromドメイン
		送信元IPアドレス（client-ip=タグ）
Authentication-Results	DMARC	DMARC認証結果
		ポリシー
		処理結果
		ヘッダーFromドメイン（header.from=タグ）
	SPF	SPF認証結果
		エンベロープFromドメイン
		送信元IPアドレス
	DKIM	DKIM認証結果
		署名ドメイン（header.i=タグ）
		署名セレクター名（header.s=タグ）
	その他	ARC認証結果

2.3.1.2. Gmailのヘッダー認証結果表示 2/2

- Gmailのヘッダーでは、Received-SPFヘッダーとAuthentication-Resultsヘッダーの2種類が付与されていた。Authentication-Resultsヘッダーではその他情報として、ARC認証結果が記述されていた。なお、Gmailでは、BIMIによるアイコン表示に対応しているものの、BIMIに関連した情報はこれらのヘッダーには確認できなかった。

図1 Gmailのヘッダー例

```
Received-SPF: pass (google.com: domain of kase@twofive25.com designates 160.16.234.226 as permitted sender) client-
ip=160.16.234.226;
Authentication-Results: mx.google.com;
      dkim=pass header.i=@twofive25.com header.s=tf0001 header.b=EhSvzazW;
      dkim=pass header.i=@twofive.onmicrosoft.com header.s=selector1-twofive-onmicrosoft-com header.b=q1XtjXiE;
      arc=pass (i=1 spf=pass spfdomain=twofive25.com dkim=pass dkdomain=twofive25.com dmarc=pass fromdomain=twofive25.com);
      spf=pass (google.com: domain of kase@twofive25.com designates 160.16.234.226 as permitted sender)
smtp.mailfrom=kase@twofive25.com;
      dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=twofive25.com
```

2.3.1.3. Gmailのヘッダー以外の認証結果表示

- Gmailでは、DMARC認証の結果をヘッダー以外の方法で確認できる。表示内容は以下のとおりである（図2、図3）。

図2「メッセージのソースを表示」で確認できるDMARC認証結果

図3 メッセージ表示で確認できるDMARC認証結果

2.3.1.4. Gmailのアイコン表示

- Gmailでは、以下のような仕様でDMARC認証の結果をアイコン表示で確認できる。アイコン表示の閲覧方法、表示画面およびその詳細については以下のとおりである（表5）。

表5 Gmailにおけるアイコン表示

閲覧方法	表示画面	表示機能の有無	表示条件・備考
Webメール	メッセージ一覧	なし	
	メッセージ表示	●	BIMI対応ドメインのみ。VMC認証が必須（図4）
専用アプリ	メッセージ一覧	●	BIMI対応ドメインのみ。VMC認証が必須（図5）
	メッセージ表示	●	BIMI対応ドメインのみ。VMC認証が必須（図6）

図4 Gmailアイコン表示例（Webメール・メッセージ表示）

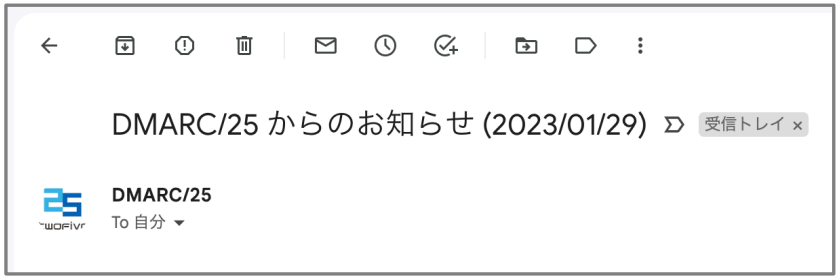


図5 Gmailアイコン表示例（専用アプリ・メッセージ一覧）

図6 Gmailアイコン表示例（専用アプリ・メッセージ表示）

2.3.1.5. Gmailの認証失敗メールの取り扱い 1/2

- Gmailでの、DMARC認証に失敗メールに対しての取り扱い仕様について整理する。公開情報に記載がない場合、テストアカウントでの動作から推定した。結果は以下のとおりである（表6）。

表6 GmailにおけるDMARC認証失敗したメールの取り扱い

ポリシー	取り扱い	備考
ポリシーなし	受信する	
none	受信しない場合がある。また、メッセージ表示の際に警告を表示する（次頁図7、図8）	SMTPプロトコルでのレスポンスは以下のとおり。 421-4.7.0 This message does not pass authentication checks (SPF and DKIM both do not pass).
quarantine	受信しない	SMTPプロトコルでのレスポンスは以下のとおり。 550-5.7.26 This message does not pass authentication checks (SPF and DKIM both do not pass).
reject	受信しない	SMTPプロトコルでのレスポンスは以下のとおり。 550-5.7.26 This message does not pass authentication checks (SPF and DKIM both do not pass).

2.3.1.5. Gmailの認証失敗メールの取り扱い 2/2

- DMARC認証結果を含めてなりすましメール（迷惑メール）と判定された場合に表示される警告メッセージは、以下のとおりである（図7、図8）。

図7 Gmailのなりすましメールに対する警告例（Webメール）

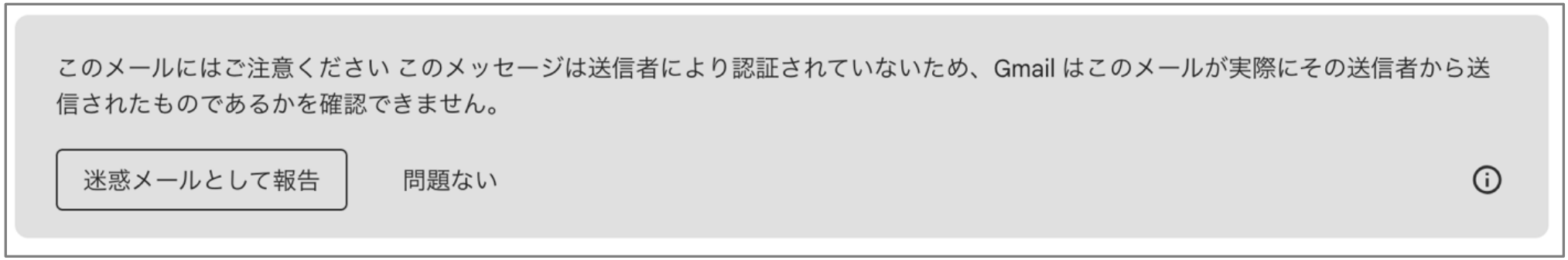
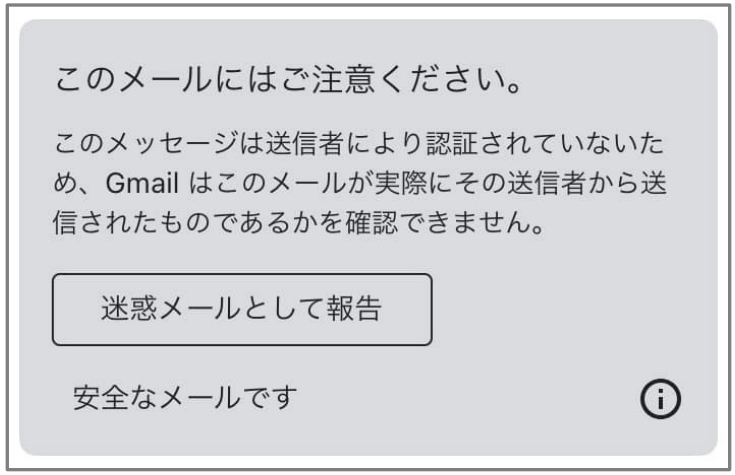


図8 Gmailのなりすましメールに対する警告例（専用アプリ）



2.3.2.1. Fastmailの調査結果

- Fastmailは、Fastmail Pty. Ltd.が運営するメールサービスであり、ドメイン名はfastmail.comである。2023年1月時点で、Fastmailでは、宣言ポリシー、DMARC認証、ポリシー処理、集計レポート、失敗レポートの対応状況は以下のとおりである（表7）。

表7 FastmailのDMARC基本仕様

宣言ポリシー	DMARC認証	ポリシー処理	集計レポート	失敗レポート
none	●	なし	●	なし

2.3.2.2. Fastmailのヘッダー認証結果表示 1/2

- Fastmailでは、DMARC認証の結果および関連情報を以下のヘッダーへ付与する。具体的に付与されるヘッダーおよび記載内容は以下のとおりである（表8、次頁図9）。

表8 FastmailのDMARC関連の認証結果表示仕様

ヘッダー名	認証技術	記載内容
Authentication-Results	DMARC	DMARC認証結果
		ポリシー（policy.published-domain-policy=タグ）
		処理結果（policy.applied-disposition=タグ）
		評価結果（policy.evaluated-disposition=タグ）
		ヘッダーFromドメイン（header.from=タグ）
	SPF	SPF認証結果
		エンベロープFromドメイン（smtp.mailfrom=タグ）
		HELOドメイン（smtp.helo=タグ）
	DKIM	DKIM認証結果
		署名ドメイン（header.i=タグ）
		署名セレクター名（header.s=タグ）
		署名の暗号アルゴリズム（header.a=タグ）
		署名鍵のサイズ（x-bit=タグ）
	その他	送信元IPアドレス（smtp.remote-ip=タグ）
		ARC認証結果
		BIMI認証結果
		BIMI対象ドメイン（header.d=タグ）
		BIMIセレクター名（header.selector=タグ）
		VMCの検証結果（policy.authority=タグ）
		VMCのURI（policy.authority-uri=タグ）

2.3.2.2. Fastmailのヘッダー認証結果表示 2/2

- Fastmailのヘッダーでは、Authentication-Resultsヘッダーのみが付与されていたが、単一のヘッダーではなく、複数ヘッダーに分かれていた。Authentication-Resultsヘッダーではその他情報として、ARC認証結果およびBIMIに関連した情報が記述されている。

図9 Fastmailのヘッダー例

```
Authentication-Results: mx1.messagingengine.com;
    x-csa=none;
    x-me-sender=none;
    x-ptr=pass smtp.helo=ik1-307-13640.vs.sakura.ne.jp
      policy.ptr=ik1-307-13640.vs.sakura.ne.jp
Authentication-Results: mx1.messagingengine.com;
    bimi=skipped (DMARC did not pass) policy.authority=pass
      policy.authority-uri=
      https://bimi.s3.twofive.rstorcloud.io/bimi-twofive25-6578326.pem
Authentication-Results: mx1.messagingengine.com;
    arc=none (no signatures found)
Authentication-Results: mx1.messagingengine.com;
    dkim=none (no signatures found);
    dmarc=fail policy.published-domain-policy=quarantine
      policy.applied-disposition=quarantine
      policy.evaluated-disposition=quarantine policy.arc-aware-result=fail
      (p=quarantine,d=quarantine,d.eval=quarantine,arc_aware_result=fail)
      policy.policy-from=p header.from=dmarc25.jp;
    iprev=pass smtp.remote-ip=153.126.142.144
      (ik1-307-13640.vs.sakura.ne.jp);
    spf=fail smtp.mailfrom=info@dmarc25.jp
      smtp.helo=ik1-307-13640.vs.sakura.ne.jp
```

2.3.2.3. Fastmailのヘッダー以外の認証結果表示

- Fastmailでは、DMARC認証の結果をヘッダー以外の方法で確認できる機能はなかった。

2.3.2.4. Fastmailのアイコン表示

- Fastmailでは、以下のような仕様でDMARC認証の結果をアイコン表示で確認できる。アイコン表示の閲覧方法、表示画面およびその詳細については以下のとおりである（表9）。

表9 Fastmailにおけるアイコン表示

閲覧方法	表示画面	表示機能の有無	表示条件・備考
Webメール	メッセージ一覧	なし	
	メッセージ表示	●	BIMI対応ドメインのみ VMC認証は不要 （図10）
専用アプリ	メッセージ一覧	なし	
	メッセージ表示	●	BIMI対応ドメインのみ VMC認証は不要 （図11）

図10 Fastmailアイコン表示例（Webメール・メッセージ表示）

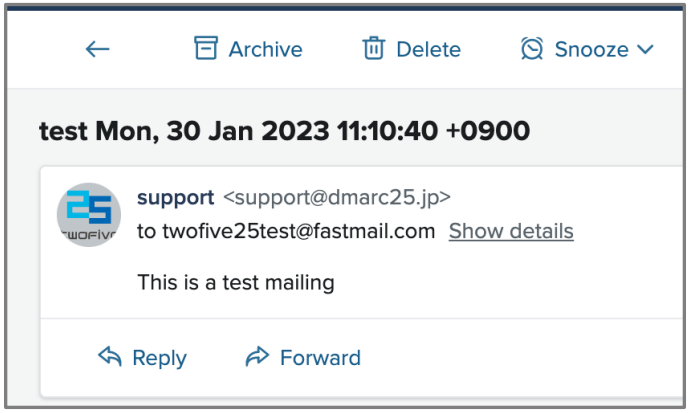
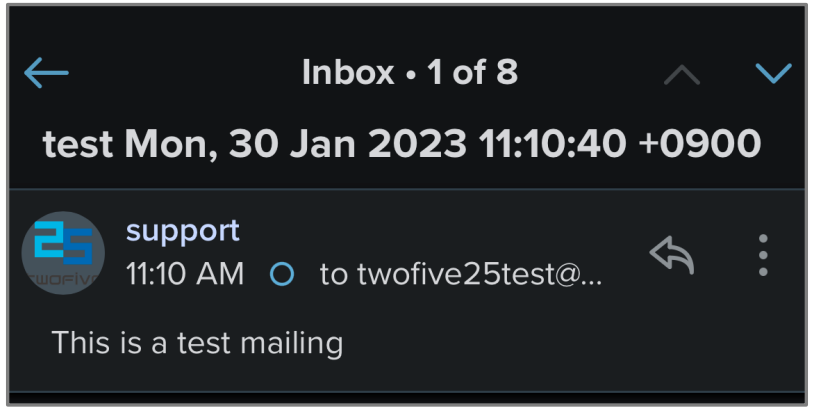


図11 Fastmailアイコン表示例（専用アプリ・メッセージ表示）



2.3.2.5. Fastmailの認証失敗メールの取り扱い

- Fastmailでは、DMARC認証に失敗メールに対しての取り扱い仕様について整理する。なお、公開情報に記載がない場合は、テストアカウントでの動作から推定した結果を記載する（表10）。

表10 FastmailにおけるDMARC認証失敗したメールの取り扱い

ポリシー	取り扱い	備考
ポリシーなし	受信する	Authentication-Results ヘッダーでは、”policy.applied-disposition=none”と記載。
none	受信する	Authentication-Results ヘッダーでは、”policy.applied-disposition=none”と記載。
quarantine	受信するが、迷惑メール扱いの場合がある	利用者の設定（Spam ProtectionのProtection Level）による。
reject	受信するが、迷惑メール扱いの場合がある	利用者の設定（Spam ProtectionのProtection Level）による。

2.3.3.1. Outlookの調査結果

- Outlookは、Microsoftが運営するメールサービスであり、ドメイン名はoutlook.comである。2023年1月時点で、Outlookでは、宣言ポリシー、DMARC認証、ポリシー処理、集計レポート、失敗レポートの対応状況は以下のとおりである（表11）。

表11 OutlookのDMARC基本仕様

宣言ポリシー	DMARC認証	ポリシー処理	集計レポート	失敗レポート
quarantine	●	●	●	なし

2.3.3.2. Outlookのヘッダー認証結果表示 1/2

- Outlookでは、DMARC認証の結果および関連情報を以下のヘッダーへ付与する。具体的に付与されるヘッダーおよび記載内容は以下のとおりである（表12、次頁図12）。

表8 OutlookのDMARC関連の認証結果表示仕様

ヘッダー名	認証技術	記載内容
Authentication-Results	DMARC	DMARC認証結果
		ヘッダーFromドメイン（header.from=タグ）
		処理結果
	DKIM	DKIM認証結果
		署名ドメイン（header.d=タグ）
Received-SPF	SPF	SPF認証結果
		エンベロープFromドメイン
		HELOドメイン（helo=タグ）
		送信元IPアドレス（client-ip=タグ）

2.3.3.2. Outlookのヘッダー認証結果表示 2/2

- Outlookのヘッダーでは、Received-SPFヘッダーとAuthentication-Resultsヘッダーの2種類が付与されていた。Authentication-ResultsヘッダーではSPF関連情報、DKIM署名のセレクター情報は記述されていなかった。

図12 Outlookのヘッダー例

```
Received: from DM3NAM02FT041.eop-nam02.prod.protection.outlook.com
 (2603:10b6:5:bc:cafe::58) by DM6PR13CA0015.outlook.office365.com
 (2603:10b6:5:bc::28) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6064.22 via Frontend
 Transport; Tue, 31 Jan 2023 09:16:26 +0000
Authentication-Results: spf=pass (sender IP is 27.133.154.48)
 smtp.mailfrom=dmarc25.jp; dkim=pass (signature was verified)
 header.d=dmarc25.jp;dmarc=pass action=none
 header.from=dmarc25.jp;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of dmarc25.jp designates
 27.133.154.48 as permitted sender) receiver=protection.outlook.com;
 client-ip=27.133.154.48; helo=dmarc25mail-01.dmarc25.jp; pr=C
Received: from dmarc25mail-01.dmarc25.jp (27.133.154.48) by
 DM3NAM02FT041.mail.protection.outlook.com (10.13.5.133) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.6043.22 via Frontend Transport; Tue, 31 Jan 2023 09:16:25 +0000
```

2.3.3.3. Outlookのヘッダー以外の認証結果表示

- Outlookでは、DMARC認証の結果をヘッダー以外の方法で確認できる機能はなかった。

2.3.3.4. Outlookのアイコン表示

- Outlookでは、以下のとおり、DMARC認証の結果はアイコン表示できない（表13）。

表13 Outlookにおけるアイコン表示

閲覧方法	表示画面	表示機能の有無	表示条件・備考
Webメール	メッセージ一覧	なし	
	メッセージ表示	なし	
専用アプリ	メッセージ一覧	なし	
	メッセージ表示	なし	

2.3.3.5. Outlookの認証失敗メールの取り扱い

- Outlookでは、DMARC認証に失敗メールに対しての取り扱い仕様について整理する。なお、公開情報に記載がない場合は、テストアカウントでの動作から推定した結果を記載する（表14）。

表14 OutlookにおけるDMARC認証失敗したメールの取り扱い

ポリシー	取り扱い	備考
ポリシーなし	受信する	Authentication-Results ヘッダーでは、”action=none” と記載 また、DMARC認証結果は”dmarc=bestguesspass”と記載
none	受信する	Authentication-Results ヘッダーでは、”action=none” と記載
quarantine	受信するが、迷惑メール扱いの場合がある	Authentication-Results ヘッダーでは、”action=quarantine” と記載
reject	受信するが、迷惑メール扱いの場合がある	Authentication-Results ヘッダーでは、”action=oreject” と記載

2.3.4.1. Yahoo!メールの調査結果

- Yahoo!メールは、Yahoo!JAPANが運営するメールサービスであり、ドメイン名はyahoo.co.jpである。2022年12月時点で、Yahoo!メールでは、宣言ポリシー、DMARC認証、ポリシー処理、集計レポート、失敗レポートの対応状況は以下のとおりである（表15）

表15 Yahoo!メールのDMARC基本仕様

宣言ポリシー	DMARC認証	ポリシー処理	集計レポート	失敗レポート
quarantine	●	●	なし	なし

2.3.4.2. Yahoo!メールのヘッダー認証結果表示 1/2

- Yahoo!メールでは、DMARC認証の結果および関連情報を以下のヘッダーへ付与する。具体的に付与されるヘッダーおよび記載内容は以下のとおりである（表16、次頁図13）。

表16 Yahoo!メールのDMARC関連の認証結果表示仕様

ヘッダー名	認証技術	記載内容
Received-SPF	SPF	SPF認証結果
		エンベロープFromドメイン
		送信元IPアドレス（client-ip=タグ）
		送信元IPアドレスの逆引きドメイン（receiver=タグ）
Authentication-Results	DMARC	DMARC認証結果
		ポリシー
		ポリシー適用率
		ポリシードメイン
		ヘッダーFromドメイン（header.from=タグ）
	DKIM	DKIM認証結果
		署名ドメイン（header.i=タグ）

2.3.4.2. Yahoo!メールのヘッダー認証結果表示 2/2

- Yahoo!メールのヘッダーでは、Received-SPFヘッダーとAuthentication-Resultsヘッダーの2種類が付与されていた。Authentication-Resultsヘッダーではその他情報として、DomainKeys認証結果が記述されていた。なお、Authentication-ResultsヘッダーではSPF関連情報、DKIM署名のセレクター情報は記述されていなかった。

図13 Yahoo!メールのヘッダー例

```
Received-SPF: pass (mail-yb1-f169.google.com: domain of kase.masaki@gmail.com d
esignates 209.85.219.169 as permitted sender) receiver=mail-yb1-f169.google.com; cli
ent-ip=209.85.219.169; envelope-from=kase.masaki@gmail.com;
Authentication-Results: mta7065.mail.djm.ynwp.yahoo.co.jp  from=gmail.com; domaink
eys=neutral (no sig); dkim=pass (ok); header.i=@gmail.com; dmarc=pass (p=NONE,sp
=QUARANTINE,pct=100,domain=gmail.com); header.from=gmail.com
```

2.3.4.3. Yahoo!メールのヘッダー以外の認証結果表示

- Yahoo!メールでは、DMARC認証の結果をヘッダー以外の方法で確認できる。表示内容は以下のとおりである（図14、図15）。

図14 メール表示画面で確認できるDMARC認証結果

図15「このメールの認証情報」で確認できるDMARC認証結果

2.3.4.4. Yahoo!メールのアイコン表示 1/2

- Yahoo!メールでは、以下のような仕様でDMARC認証の結果をアイコン表示で確認できる。アイコン表示の閲覧方法、表示画面およびその詳細については以下のとおりである（表17、次頁図16～19）。

表17 Yahoo!メールにおけるアイコン表示

閲覧方法	表示画面	表示機能の有無	表示条件・備考
Webメール	メッセージ一覧	●	独自で管理するドメインのみ
	メッセージ表示	●	独自で管理するドメインのみ
専用アプリ	メッセージ一覧	●	独自で管理するドメインのみ
	メッセージ表示	●	独自で管理するドメインのみ

2.3.4.4. Yahoo!メールのアイコン表示 2/2

図16 Yahoo!メールアイコン表示例
（Webメール・メッセージ一覧）

図17 Yahoo!アイコン表示例（Webメール・メッセージ表示）

図18 Yahoo!メールアイコン表示例
（専用アプリ・メッセージ一覧）

図19 Yahoo!メールアイコン表示例
（専用アプリ・メッセージ表示）

2.3.4.5. Yahoo!メールの認証失敗メールの取り扱い

- Yahoo!メールでは、DMARC認証に失敗メールに対しての取り扱い仕様について整理する。なお、公開情報に記載がない場合は、テストアカウントでの動作から推定した結果を記載する（表18）。

表18 Yahoo!メールにおけるDMARC認証失敗したメールの取り扱い

ポリシー	取り扱い	備考
ポリシーなし	受信する	
none	受信する	
quarantine	受信するが、迷惑メール扱いの場合がある	一部、例外のケースも見受けられる
reject	受信するが、拒否あるいは迷惑メール扱いの場合がある	一部、例外のケースも見受けられる

2.3.5.1. So-net Webメールの調査結果

- So-net Webメールは、ソニーネットワークコミュニケーションズが運営するメールサービスであり、ドメイン名は（※）.so-net.ne.jpである。2023年1月時点で、So-net Webメールでは、宣言ポリシー、DMARC認証、ポリシー処理、集計レポート、失敗レポートの対応状況は以下のとおりである（表19）

表19 So-net WebメールのDMARC基本仕様

宣言ポリシー	DMARC認証	ポリシー処理	集計レポート	失敗レポート
None ※	●	●	なし	なし

出所）組織ドメインso-net.ne.jpにおいてDMARCレコード（p=none）が設定されている。

2.3.5.2. So-net Webメールのヘッダー認証結果表示

- So-net Webメールでは、DMARC認証の結果および関連情報を以下のヘッダーへ付与する。具体的に付与されるヘッダーおよび記載内容は以下のとおりである（表20、図20）。

表20 So-net WebメールのDMARC関連の認証結果表示仕様

ヘッダー名	認証技術	記載内容
Authentication-Results	DMARC	DMARC認証結果
		ヘッダーFromドメイン（header.from=タグ）
	SPF	SPF認証結果
		エンベロープFromドメイン
	DKIM	DKIM認証結果
		署名ドメイン（header.d=タグ）

- So-net Webメールのヘッダーでは、Authentication-Resultsヘッダーのみが付与されていた。なお、Authentication-Resultsヘッダーでは送信元IPアドレス、DKIM署名のセレクター情報は記述されていなかった。

図20 So-net Webメールのヘッダー例

```
Authentication-results: ms-mxin04.so-net.ne.jp; spf=pass smtp.mailfrom=softest@nifty.com; dkim=pass header.d=nifty.com
header.b=1e1ecMoY; dmarc=pass header.from=nifty.com
```

2.3.5.3. So-net Webメールのヘッダー以外の認証結果表示

- So-net Webメールでは、DMARC認証の結果をヘッダー以外の方法で確認機能はなかった。

2.3.5.4. So-net Webメールのアイコン表示

- So-net Webメールでは、以下のような仕様でDMARC認証の結果をアイコン表示で確認できる。アイコン表示の閲覧方法、表示画面およびその詳細については以下のとおりである（表21、図21）。

表21 So-net Webメールにおけるアイコン表示

閲覧方法	表示画面	表示機能の有無	表示条件・備考
Webメール	メッセージ一覧	●	自社オフィシャルメールのみ （図21）
	メッセージ表示	●	
専用アプリ	メッセージ一覧	ー	
	メッセージ表示	ー	

図21 So-net Webメールアイコン表示例（Webメール・メッセージ一覧）

2.3.5.5. So-net Webメールの認証失敗メールの取り扱い

- So-net Webメールでは、DMARC認証に失敗メールに対しての取り扱い仕様について整理する。なお、公開情報に記載がない場合は、テストアカウントでの動作から推定した結果を記載する（表22）。

表22 So-net WebメールにおけるDMARC認証失敗したメールの取り扱い

ポリシー	取り扱い	備考
ポリシーなし	受信する	
none	受信する	
quarantine	受信する	
reject	受信する	

2.3.6.1. Active! mailの調査結果

- Active! mailは、QUALITIAが運営する法人向けメールサービスであり、ドメイン名は顧客の独自ドメインである。2023年2月時点で、Active! mailでは、宣言ポリシー、DMARC認証、ポリシー処理、集計レポート、失敗レポートの対応状況は以下のとおりである（表23）。

表23 Active! mailのDMARC基本仕様

宣言ポリシー	DMARC認証	ポリシー処理	集計レポート	失敗レポート
ドメインによる	●	●	●※	なし

※今後提供予定。

2.3.6.2. Active! mailのヘッダー認証結果表示

- Active! mailでは、DMARC認証の結果および関連情報を以下のヘッダーへ付与する。具体的に付与されるヘッダーおよび記載内容は以下のとおりである（表24、図22）。

表24 Active! mailのDMARC関連の認証結果表示仕様

ヘッダー名	認証技術	記載内容
Authentication-Results	DMARC	DMARC認証結果
		ヘッダーFromドメイン（header.from=タグ）
	SPF	SPF認証結果
		DKIM認証結果
	DKIM	署名ドメイン（header.d=タグ）
		DMARC認証結果

- Active! mailのヘッダーでは、Authentication-Resultsヘッダーのみが付与されていた。なお、Authentication-Resultsヘッダーでは送信元IPアドレス、DKIM署名のセレクター情報は記述されていなかった。

図22 Active! mailのヘッダー例

```
Authentication-Results: mail.example.jp; spf=pass; dkim=pass header.d=qualitia.co.jp; dmarc=pass header.from=qualitia.co.jp
```

2.3.6.3. Active! mailのヘッダー以外の認証結果表示

- Active! mailでは、DMARC認証の結果をヘッダー以外の方法で確認できる。表示内容は以下のとおりである（図23、図24、図25）。

図23 メール表示画面で確認できるDMARC認証結果

図24 メッセージ表示で確認できるDMARC認証結果表示

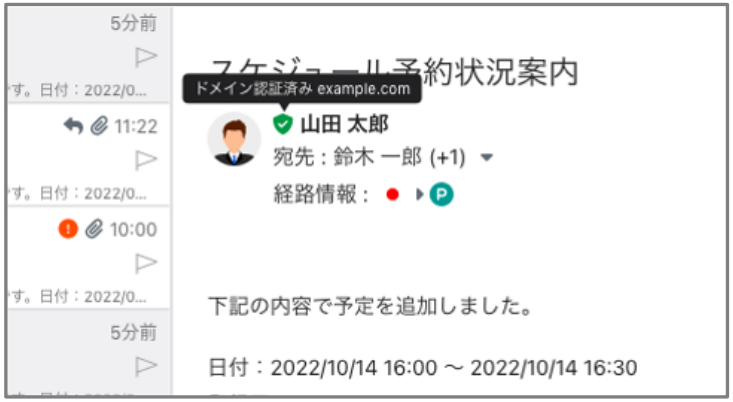
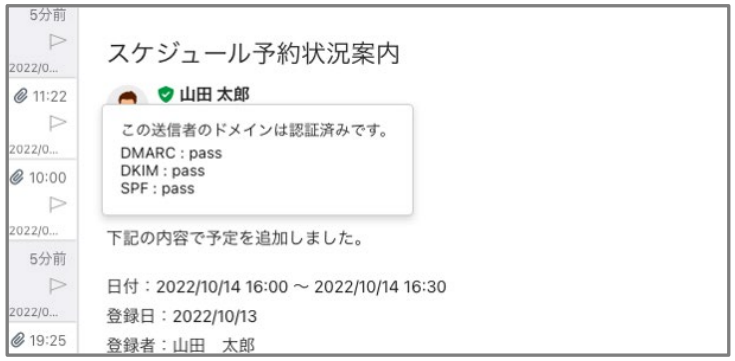


図25 メッセージ表示で確認できるSPFおよびDKIM認証結果表示



2.3.6.4. Active! mailのアイコン表示

- Active! mailでは、以下のような仕様でDMARC認証の結果をアイコン表示で確認できる。アイコン表示の閲覧方法、表示画面およびその詳細については以下のとおりである（表25、図26）。

表25 Active! mailにおけるアイコン表示

閲覧方法	表示画面	表示機能の有無	表示条件・備考
Webメール	メッセージ一覧	●	BIMI対応ドメインのみ。VMC認証が必須 （図26）
	メッセージ表示	なし	
専用アプリ	メッセージ一覧	ー	
	メッセージ表示	ー	

図26 Active! mailアイコン表示例（Webメール・メッセージ一覧）

2.3.6.5. Active! mailの認証失敗メールの取り扱い

- Active! mailでは、DMARC認証に失敗メールに対しての取り扱い仕様について整理する。なお、公開情報に記載がない場合は、テストアカウントでの動作から推定した結果を記載する（表26）。

表26 Active! mailにおけるDMARC認証失敗したメールの取り扱い

ポリシー	取り扱い	備考
ポリシーなし	受信する	
none	受信する	
quarantine	隔離フォルダへ振り分ける	
reject	受信しない	SMTPプロトコルでのレスポンスは以下のとおり 550 5.7.1 <Rejected by DMARC policy(fail)>... Access denied

- DMARC認証結果を含めてなりすましメールと判定された場合に表示されるアイコンや警告メッセージは、以下のとおりである（図27）。

図27 Active! mailのなりすましメールに対する警告例（Webメール）

2.4.1. 調査結果まとめ

- 本調査の既存メールサービスについては、いずれもDMARC認証に対応しているものの、ポリシーに従った処理を実装していないサービスも存在した（表27）。
- また、ポリシーに従った処理を実装しているサービスにおいても、サービス全体での処理結果の一貫性はなく、個別のメッセージや利用者の設定に左右される形で認証に失敗したメッセージが処理された。

表27 既存メールサービスのDMARC関連仕様のまとめ

メールサービス	宣言ポリシー	DMARC認証	ポリシー処理	集計レポート	失敗レポート
Gmail	none	●	●	●	なし
Fastmail	none	●	なし	●	なし
Outlook	quarantine	●	●	●	なし
Yahoo!メール	quarantine	●	●	なし	なし
So-net Webメール	none	●	なし	なし	なし
Active! mail	ドメインによる	●	●	△	なし

●: 実装あり、△: 実装予定

2.4.2. 調査結果まとめ 1/4

- DMARC認証結果をユーザーが確認する方法としては、大きく分類して「メッセージ一覧（フォルダ内のメール一覧）」「メッセージ表示（選択したメールの本文表示）」「ヘッダー表示（選択したメールの詳細ヘッダー表示）」「警告表示（なりすましであることの注意喚起）」の4つであった。
- 閲覧方法については、「Webメール」「専用アプリ」の2つ用意されているが、「専用アプリ」の場合は、表示エリアが大きくないことからヘッダー表示に対応しているメールサービスはなかった（表28）。また、表示する内容については、正当なメールに対してアイコン表示する方法もいくつかのメールサービスでは見られた（表28）。

表28 既存メールサービスの表示方法のまとめ

メールサービス	閲覧方法	メッセージ一覧	メッセージ表示	ヘッダー表示	警告表示
Gmail	Webメール	なし	◎	●	●
	専用アプリ	◎	◎	なし	●
Fastmail	Webメール	なし	◎	●	なし
	専用アプリ	なし	◎	なし	なし
Outlook	Webメール	なし	なし	●	なし
	専用アプリ	なし	なし	なし	なし
Yahoo!メール	Webメール	◎	◎	●	なし
	専用アプリ	◎	◎	なし	なし
So-net Webメール	Webメール	◎	なし	●	なし
	専用アプリ	—	—	—	—
Active! mail	Webメール	◎	なし	●	●
	専用アプリ	—	—	—	—

◎: アイコン表示あり、●: 表示あり

2.4.2. 調査結果まとめ 2/4

- 認証結果を記述したメールヘッダーとしては、「Received-SPF」「Authentication-Results」の2つを利用している傾向があり、前者はSPF認証結果に関する情報のみ、後者はDKIMやDMARCを含む多くの認証結果に関する情報を記述することができる。そのため、調査対象の全てのメールサービスでAuthentication-Resultsを採用していた（表29）。
- BIMIに対応しているメールサービスは、GmailとFastmailであるが、認証結果ヘッダーにBIMIに関連した情報を記述していたのはFastmailのみであった（表29）。

表29 既存メールサービスの認証結果ヘッダーのまとめ

メールサービス	Received-SPF	Authentication-Results
Gmail	●	●
Fastmail	なし	◎
Outlook	●	●
Yahoo!メール	●	●
So-net Webメール	なし	●
Active! mail	なし	●

◎: BIMI関連情報あり、●: DMARC関連情報あり、なし: ヘッダーなし

2.4.2. 調査結果まとめ 3/4

- SPF認証結果に関する情報としては、主に「認証結果」「エンベロープFromドメイン」「送信元IPアドレス」の3つが挙げられる。それぞれのメールサービスでの認証結果ヘッダーへの記載状況は以下のとおりである（表30）。

表30 既存メールサービスのSPF認証結果に関する記載情報のまとめ

メールサービス	認証結果	エンベロープFromドメイン	送信元IPアドレス	その他
Gmail	●	●	●	
Fastmail	●	●	●	HELOドメイン
Outlook	●	●	●	HELOドメイン
Yahoo!メール	●	●	●	送信元IPアドレスの逆引きドメイン
So-net Webメール	●	●	なし	
Active! mail	●	なし	なし	

●: 情報あり、なし: 情報なし

2.4.2. 調査結果まとめ 4/4

- DKIM認証結果に関する情報としては、主に「認証結果」「署名ドメイン」「署名セレクター名」の3つが挙げられる。それぞれのメールサービスでの認証結果ヘッダーへの記載状況は以下のとおりである（表31）。

表31 既存メールサービスのDKIM認証結果に関する記載情報のまとめ

メールサービス	認証結果	署名ドメイン	署名セレクター名	その他
Gmail	●	●	●	
Fastmail	●	●	●	署名アルゴリズム 署名鍵のサイズ
Outlook	●	●	なし	
Yahoo!メール	●	●	なし	
So-net Webメール	●	●	なし	
Active! mail	●	●	なし	

●: 情報あり、なし: 情報なし

2.5. 略称一覧

表32 略称一覧

本報告書でも表記	正式名称・意味など
DMARC	Domain-based Message Authentication, Reporting, and Conformance 送信ドメイン認証技術の一つ。SPFとDKIM両者を利用したメールのドメイン認証を補強する技術である。
DKIM	DomainKeys Identified Mail 送信ドメイン認証技術の一つ。送信元が付した電子署名により送信元情報の真偽及び電子メールの本文の改変を検知することができる。
SPF	Sender Policy Framework 送信ドメイン認証技術の一つ。エンベロープ情報の From メールアドレスのドメイン名をチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。
FQDN	Fully Qualified Domain Name TCP / IP ネットワーク上で、ドメイン名・サブドメイン名・ホスト名をすべて省略せずに指定した記述形式のことを指す。
OD	Organizational Domain 組織ドメインと呼ばれる、wwwなどのラベルを持たない登録ドメイン（ネイキッドドメイン）を指す。
BIMI	Brand Indicators for Message Identification Webメールやメールアプリで、DMARC認証が成功し、なりすまされていないメールに対して、その送信者ドメインに関連したロゴを表示する仕組み。
VMC	Verified Mark Certificate BIMIで表示するロゴが送信者ドメインの所有するロゴであることを証明する証明書。

3. SPF/DKIM/DMARCのOSS調査・パフォーマンス調査

3.1. 調査概要

3.2. 一般的なDMARC認証機能の導入方法

3.3. 調査実施概要

3.4. 性能調査

3.5. 機能調査

3.6. 略称一覧

3.1. 調査概要

- 本調査では、メールサーバ側でDMARC認証・DKIM署名機能を導入するために必要なオープンソースソフトウェアの性能および機能調査を実施した。具体的には以下のとおりである。
  - 一般的なDMARC認証機能の導入方法
  - 調査実施概要
  - 性能調査　OpenDMARC＋OpenDKIM
  - 性能調査　Fastmail Authentication Milter
  - 機能調査

3.2. 一般的なDMARC認証機能の導入方法 1/4

- 一般的な受信メールサーバとしてPostfix(https://www.postfix.org/)を例にして、DMARCに関連する認証方式であるSPF認証、DKIM認証およびDMARC認証を可能にするための導入方法を以下に示す。

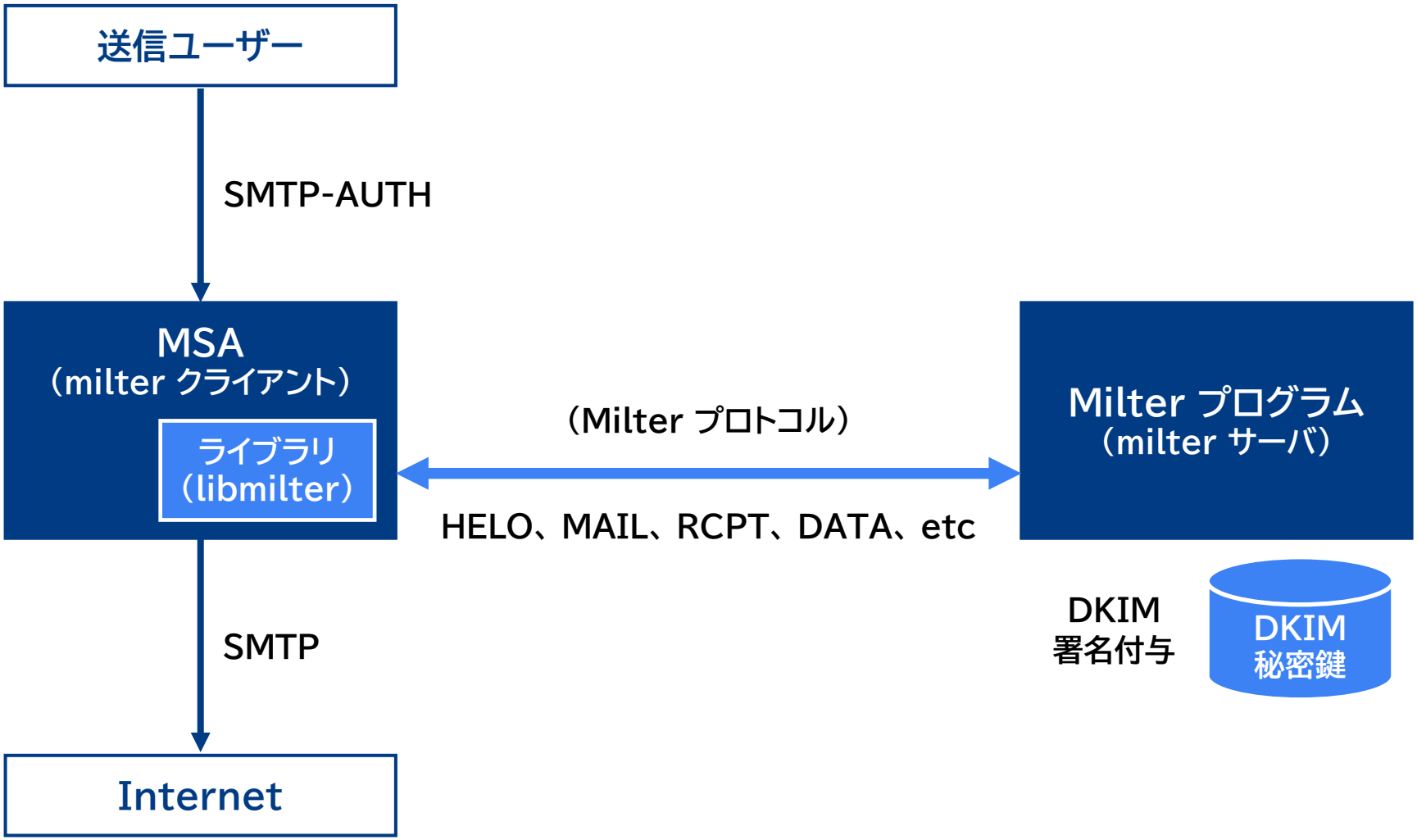
- Postfixではバージョン2.3以降、Sendmail8のMilter（mail filter）プロトコルをサポートしており、このプロトコルはMTAの外側のアプリケーションでメールの内容だけでなくSMTPのイベント（接続、切断）、SMTP コマンド（HELO、MAIL、RCPT、DATAなど）を検査するために利用する。Postfixを利用したメールサーバでは、一般的にこの機能を有効化することで、SPF認証、DKIM認証およびDMARC認証に対応できる。

- メール送信サーバの場合は、送信ユーザーから送信されたメッセージに対してDKIM署名を付与するため、Milterプロトコルを利用して、Milterプログラムにメッセージデータを転送する。Milterプログラムはあらかじめ管理するDKIM署名用の秘密鍵を用いてDKIM-Signatureヘッダーを生成・付与する(次頁 図1.a)。

- なお、DKIM署名は受信時にその正当性を検証するため、DKIM署名を付与してからInternetへ送出するまでにメッセージの書き換えをしないことが重要である。もし、何らかの理由によりメッセージの書き換えをする場合は、書き換え後にDKIM再署名をして、受信時のDKIM認証の失敗を防止する。

3.2. 一般的なDMARC認証機能の導入方法　2/4

図1.a



3.2. 一般的なDMARC認証機能の導入方法 3/4

- メール受信サーバの場合は、Internetから受信したメッセージに対してDKIM認証をするため、Milterプロトコルを利用して、Milterプログラムに SMTPコマンドやメッセージデータを転送する。Milterプログラムはそれらの情報から、必要に応じてDNSからSPFレコード、DKIMレコードおよびDMARCレコードを取得して、それぞれSPF認証、DKIM認証およびDMARC認証を実施する（次頁 図1.b）。

- なお、SPF認証は送信元IPアドレスとSPFレコードを突合して、送信元IPアドレスの正当性を検証するため、Internetから受信する前にセキュリティゲートウェイシステムが存在する場合は、認証に利用する送信元IPアドレスが本来のものとは異なるため、SPF認証が失敗する場合がある。

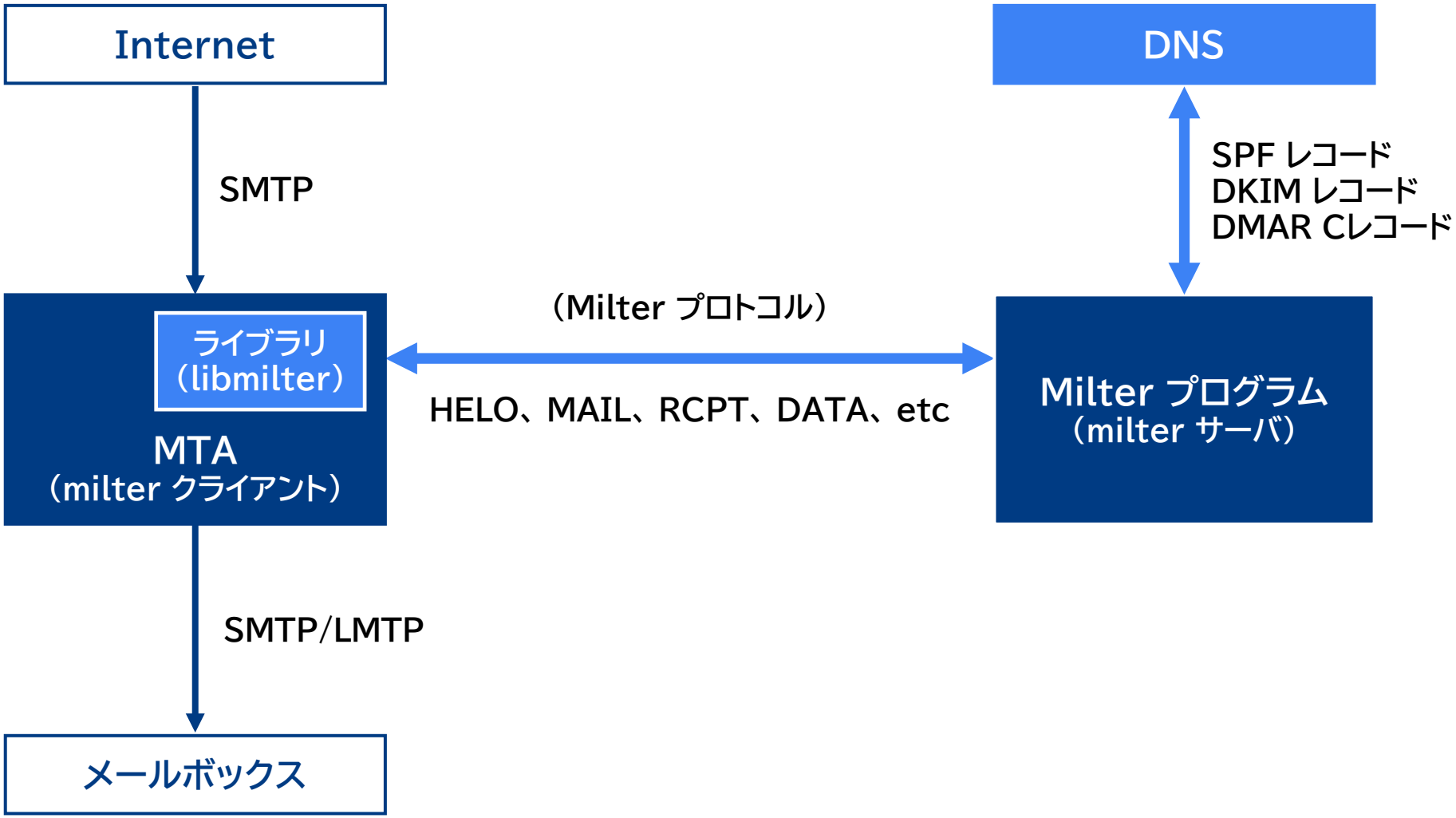
- 同様に、DKIM認証はDKIM署名の正当性を検証するため、セキュリティゲートウェイシステムがメッセージの書き換えをする場合は、DKIM認証が失敗する場合がある。

- これらの理由により、DMARC認証も失敗する場合がある。一般的には、メール受信サーバでMilterプログラムを利用する場合は、Internetに最も近い段階で連携する必要がある。

- なお、セキュリティゲートウェイシステムがこれらSPF認証、DKIM認証およびDMARC認証を実施できる場合は、それらの機能をセキュリティゲートウェイシステムで利用することができる。

3.2. 一般的なDMARC認証機能の導入方法　4/4

図1.b



3.3. 調査実施概要　1/5

- 本調査では、3つのオープンソースソフトウェアについて性能・機能を調査した。対象となるオープンソースソフトウェアの概要は以下のとおりである（表1）。

表1 対象オープンソースソフトウェア

	OpenDMARC	Fastmail Authentication Milter	OpenDKIM
調査時期	2022年12月		
開発元情報	The Trusted Domain Project	Fastmail Pty. Ltd.	The Trusted Domain Project
開発言語	C言語	Perl	C言語
SPF認証機能	●	●	—
DKIM認証機能	—	●	●
DMARC認証機能	●	●	—
DMARCレポート機能	●	—	—
DKIM署名機能	—	—	●
認証結果のヘッダー付与	●	●	●
その他関連機能		Sender ID認証 ADSP認証 ARC認証 BIMI認証	

3.3. 調査実施概要　2/5

- 受信側での性能調査では、SPF認証、DKIM認証およびDMARC認証を全て同一サーバで実行して性能比較をするため、「Postfix単体」「OpenDMARC＋OpenDKIM」「Fastmail Authentication Milter」の3パターンで調査を実施した。

- 機能調査では、SPF認証仕様およびDKIM認証仕様を確認するため、「OpenDMARC」「Fastmail Authentication Milter」「OpenDKIM」それぞれが提供する機能のみで調査した。

- その他調査では、異なる方式でDKIM署名付与を実行して性能比較をするため、「OpenDKIM（RSA 2048bit）」「OpenDKIM（RSA 3072bit）」「OpenDKIM（RSA 4096bit）」「OpenDKIM（ed25519 256bit）」の4パターンで調査を実施した。

- これら性能調査および機能調査においては、さくらのクラウドの環境をテスト環境として利用した。テスト環境のスペックおよび構成は以下のとおりである（次頁 表2、図2）。

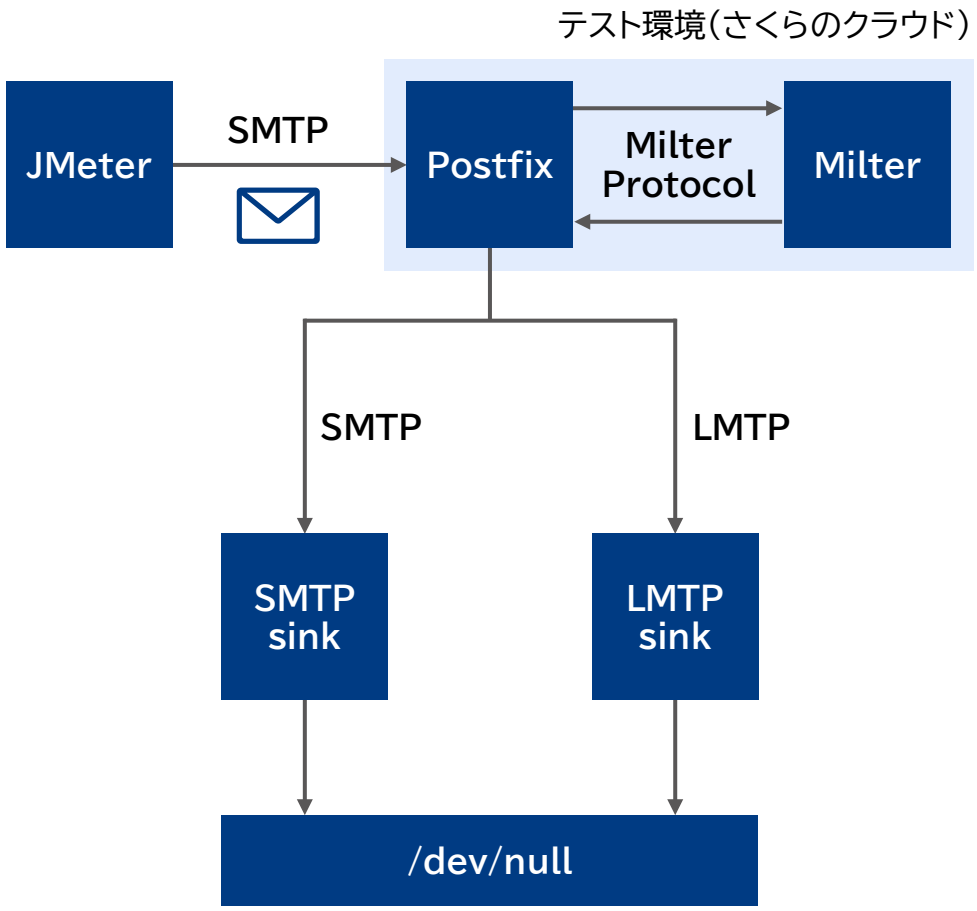
- 調査実施方法については、それぞれの調査対象を接続したPostfixサーバ（テスト環境）に対して、JMeterを実行して計測した。テスト環境の性能項目および機能項目については以下のとおりである（次々頁 表3）。

3.3. 調査実施概要 3/5

表2 テスト環境のスペック

項目	テスト環境の情報
利用インフラ	さくらのクラウド
サーバOS	Rocky Linux 8.6 64bit
CPU/コア数	3 vCPU
メモリ容量	6GB
ディスク	SSD 20GB
ネットワーク帯域	100Mbps
MTAソフトウェア	Postfix 3.5.8-4
└ OpenDMARC	OpenDMARC 1.4.1.1-3
└ Fastmail Authentication Milter	Fastmail Authentication Milter 3.20221121
└ OpenDKIM	OpenDKIM 2.11.0-0.28

図2 テスト環境の構成



3.3. 調査実施概要　4/5

表3 テスト環境の性能項目および機能項目

大項目	小項目	概要
性能項目	処理通数	単位時間あたりのメッセージ処理数の平均値。
	CPU使用率	テスト実行時間内のCPU使用率（system+user）の平均値。
	空きメモリ率	テスト実行時間内の空きメモリ率の平均値。
機能項目	SPFルックアップ数	検証対象ドメインのSPFレコード探索において、ルックアップ制限があるかどうか。
	DKIM検証数	検証対象メッセージのDKIM署名の検証処理において、処理数の制限があるかどうか。
	DKIM楕円曲線暗号	ed25519-sha256に対応しているかどうか。

3.3. 調査実施概要　5/5

- なお、比較のためPostfix単体でテスト実行した結果は以下の通りである（表4、図3、図4、図5）。

表4「Postfix単体」の性能調査結果

実行スレッド数	処理通数（通/秒）	CPU使用率（%）	空きメモリ率（%）	エラー率（%）
50	47.0	26.2	6.6	0.0
100	92.6	48.4	4.3	0.0
200	165.9	69.3	13.0	0.0
500	214.0	75.3	10.0	0.0
700	201.8	72.8	10.7	0.1
1,000	202.8	76.6	10.5	0.1

図4「Postfix単体」の性能調査結果（CPU使用率）

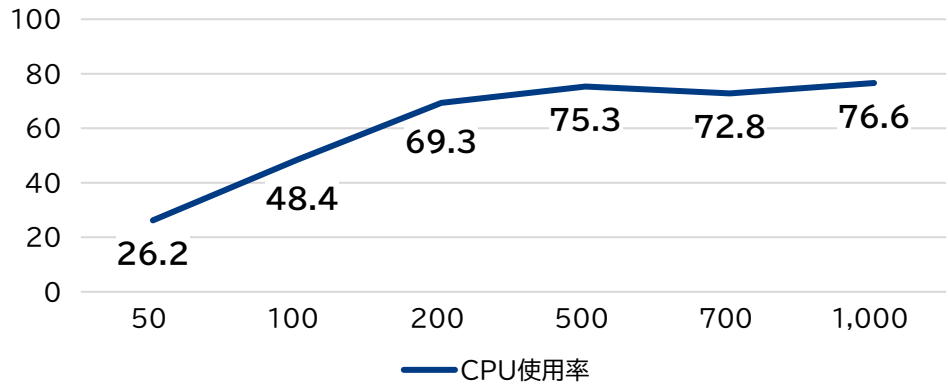


図3「Postfix単体」の性能調査結果（処理通数）

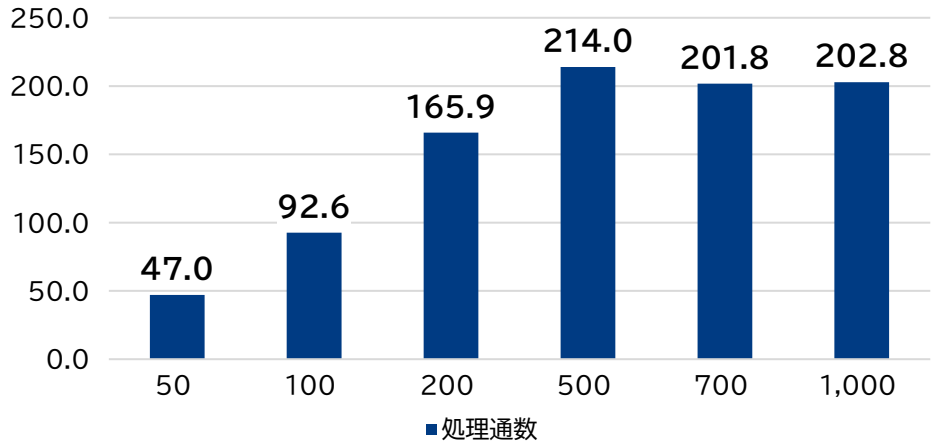
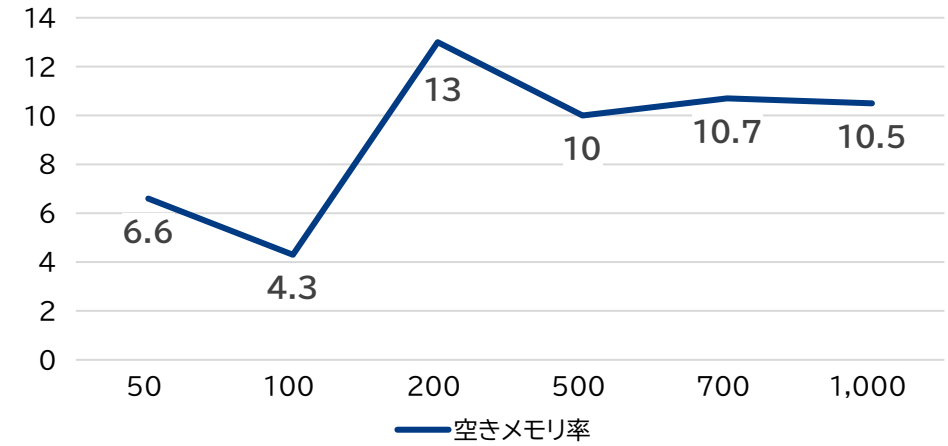


図5「Postfix単体」の性能調査結果（空きメモリ率）



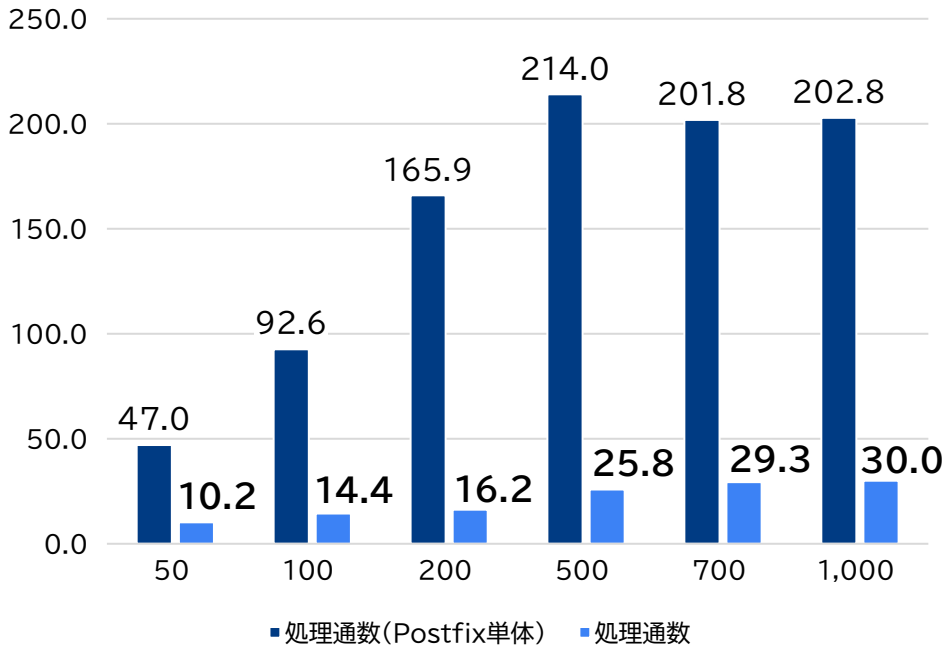
3.4.1. 性能調査 OpenDMARC＋OpenDKIM

- OpenDMARCおよびOpenDKIMはThe Trusted Domain Projectが開発したオープンソースソフトウェアで、前者はSPF認証およびDMARC認証機能を提供し、後者はDKIM認証機能を提供する。
- 以下、PostfixにOpenDMARC、OpenDKIMを接続した場合の性能調査結果を示す（表5、図6）。

表5 OpenDMARCおよびOpenDKIMを接続した場合の性能調査結果

実行スレッド数	処理通数（通/秒）	CPU使用率（%）	空きメモリ率（%）	エラー率（%）
50	10.2	10.6	35.9	0.0
100	14.4	13.9	30.5	0.0
200	16.2	15.6	30.6	0.0
500	25.8	23.2	17.2	0.0
700	29.3	25.2	18.5	3.5
1,000	30.0	49.9	13.1	10.1

図6「Postfix単体」との性能比較グラフ（処理通数）



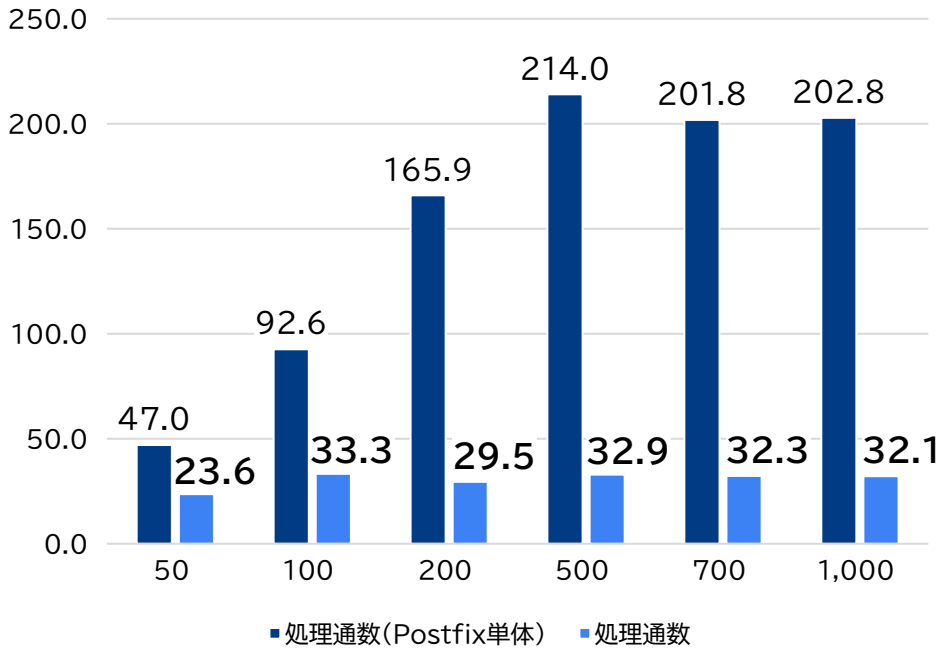
3.4.2. 性能調査 Fastmail Authentication Milter

- Fastmail Authentication MilterはFastmail Pty. Ltd.が開発したオープンソースソフトウェアで、SPF認証、DKIM認証およびDMARC認証機能を提供する。
- 以下、PostfixにFastmail Authentication Milterを接続した場合の性能調査結果を示す（表6、図7）。

表6 Fastmail Authentication Milterを接続した場合の性能調査結果

実行スレッド数	処理通数（通/秒）	CPU使用率（%）	空きメモリ率（%）	エラー率（%）
50	23.6	70.2	35.5	0.0
100	33.3	89.3	16.8	0.0
200	29.5	83.0	10.6	0.0
500	32.9	87.5	8.7	0.1
700	32.3	83.2	12.2	3.1
1,000	32.1	81.3	13.7	3.8

図7「Postfix単体」との性能比較グラフ（処理通数）



3.5.1. 機能調査 SPFルックアップ数

- SPFに関連するRFC7208（https://datatracker.ietf.org/doc/rfc7208/）では、DNS参照負荷を考慮してメカニズム・モディファイアのDNSルックアップ数に制限を設けている。具体的には、検証対象ドメインのSPFレコード探索時に、最大10回のDNSルックアップ数で実装するという記述がある。
- 3つのオープンソースソフトウェアのうち、SPF認証機能がある「OpenDMARC」「Fastmail Authentication Milter」についての動作は以下のとおりである（表7）。

表7 SPFルックアップ数制限の機能調査

	OpenDMARC	Fastmail Authentication Milter	OpenDKIM
SPFルックアップ数制限の有無	なし	あり	—
ルックアップ数が10を超えた場合のSPF認証結果	pass	permerror	—

3.5.2. 機能調査 DKIM検証数

- DKIMに関連するRFC6376（https://www.rfc-editor.org/rfc/rfc6376/）では、DKIM検証負荷を考慮して複数のDKIM-Signatureヘッダーが存在する場合にはどの署名を検証するかどうかを選択できるとしている。具体的には、DKIM署名の検証処理において、処理数の制限を設けることができる。
- 3つのオープンソースソフトウェアのうち、DKIM認証機能がある「Fastmail Authentication Milter」「OpenDKIM」についての動作は以下のとおりである（表8）。

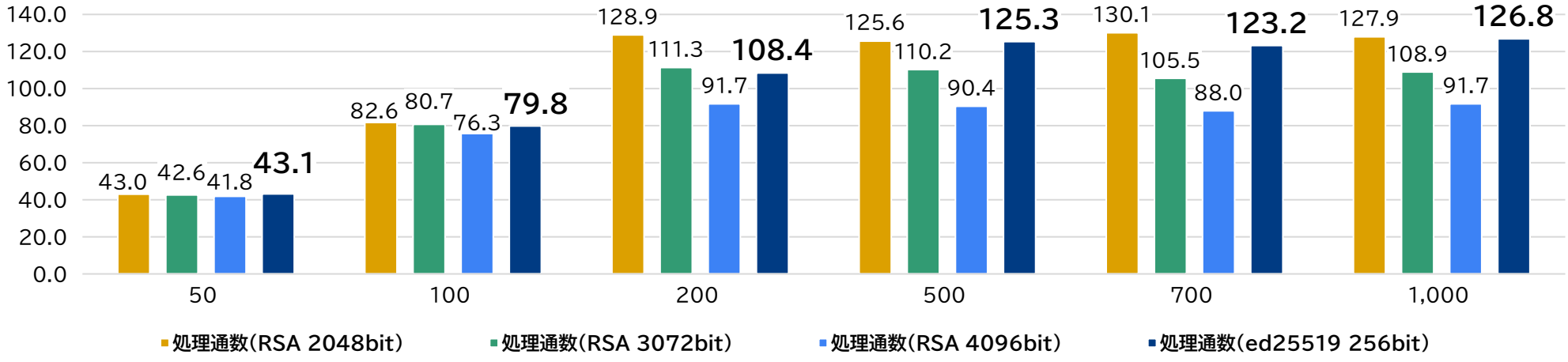
表8 DKIM検証数制限の機能調査

	OpenDMARC	Fastmail Authentication Milter	OpenDKIM
DKIM検証数数制限の有無	—	なし	あり
DKIM署名数が大量に存在する場合のDKIM認証結果	—	全てのDKIM署名を検証する	3つのDKIM署名を検証して、残りを無視する

3.5.3. 機能調査 その他の機能 1/2

- DKIMに関連するRFC8463（https://datatracker.ietf.org/doc/rfc8463/）では、既存の電子署名アルゴリズムあるrsa-sha256に加えて、ed25519-sha256を採用している。
- 後者の電子署名アルゴリズムで生成された鍵ペアの鍵長は256bitであるが、前者の鍵ペアの鍵長で比較した場合にはrsa-sha256の3072bitに相当する強度があると言われている。
- 一方で、公開鍵の文字列が非常に短く、計算量も小さく済む。
- OpenDKIMは、電子署名アルゴリズムとしてrsa-sha256およびed25519-sha256両方に対応しているため、rsa-sha256の場合は「2048bit」「3072bit」「4096bit」の3つの鍵のサイズで、ed26619-sha256では「256bit」の鍵サイズで、DKIM署名処理の性能を比較した（図8）。

図8 RSAとed25519のDKIM署名性能比較グラフ（処理通数）



3.5.3. 機能調査 その他の機能 1/2

- DKIM認証機能がある「Fastmail Authentication Milter」「OpenDKIM」についての対応状況は以下のとおりである（表9）。
- 現在のDKIMの電子署名アルゴリズムはrsa-sha256（2048bit）が主流であり、ed25519-sha256は限定的である。しかし、将来的にはrsa-sha256（3072bit）やed25519-sha256に対応した送信メールサーバが増えると考えられる。
- また、過渡期については、両方の電子署名アルゴリズムで認証が成功するように、両方のDKIM署名が2つ付与されることも考えられる。いずれについても、性能の悪化やDKIM認証の偽陽性が発生しないような実装・対応したソフトウェアを利用することが必要である。

表9 DKIMの電子署名アルゴリズムの対応状況調査

	OpenDMARC	Fastmail Authentication Milter	OpenDKIM
検証機能（rsa）	—	●	●
検証機能（ed25519）	—	未対応	未対応
検証機能（両方）	—	未対応	未対応
署名機能（rsa）	—	—	●
署名機能（ed25519）	—	—	●
署名機能（両方）	—	—	未対応

3.6. 略称一覧 1/3

表10 略称一覧

本報告書でも表記	正式名称・意味など
DMARC	Domain-based Message Authentication, Reporting, and Conformance 送信ドメイン認証技術の一つ。SPFとDKIM両者を利用したメールのドメイン認証を補強する技術である。
DKIM	DomainKeys Identified Mail 送信ドメイン認証技術の一つ。送信元が付した電子署名により送信元情報の真偽及び電子メールの本文の改変を検知することができる。
SPF	Sender Policy Framework 送信ドメイン認証技術の一つ。エンベロープ情報の From メールアドレスのドメイン名をチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。
Sender ID	SPFとCaller IDの両技術の仕様を統合した送信ドメイン認証技術の一つ。
ADSP	Author Domain Signing Practices 送信ドメイン認証技術の一つ。
ARC	Authenticated Received Chain 電子署名の技術を利用し、メールが再配送された場合でも認証結果を示す Authentication-Resultsヘッダーを辿れるようにすることで、認証の連鎖を帰納的に確認できるようにする技術。

3.6. 略称一覧　2/3

表10 略称一覧

本報告書でも表記	正式名称・意味など
FQDN	Fully Qualified Domain Name TCP / IP ネットワーク上で、ドメイン名・サブドメイン名・ホスト名をすべて省略せずに指定した記述形式のことを指す。
OD	Organizational Domain 組織ドメインと呼ばれる、wwwなどのラベルを持たない登録ドメイン（ネイキッドドメイン）を指す。
RUA	Reporting URI(s) for aggregate data DMARCを含む送信ドメイン認証結果について、ある程度の期間分をまとめて受信メールサーバからドメイン管理者にフィードバックされる統計情報。
RUF	Reporting URI(s) for failure data 送信されたメールがSPFまたはDKIMに一致せず、受信者側でDMARC認証に失敗した場合に生成されて、受信メールサーバからドメイン管理者にフィードバックされるフォレンジック情報。
BIMI	Brand Indicators for Message Identification Webメールやメールアプリで、DMARC認証が成功し、なりすまされていないメールに対して、その送信者ドメインに関連したロゴを表示する仕組み。
VMC	Verified Mark Certificate BIMIで表示するロゴが送信者ドメインの所有するロゴであることを証明する証明書。
Milter	mail filter Sendmailが開発したメー ルフィルタプラグインの仕組み。

3.6. 略称一覧　3/3

表10 略称一覧

本報告書でも表記	正式名称・意味など
RSA(暗号)	発明した3人の名前「R. L. Rivest、A. Shamir、L. Adleman」に由来する暗号方式で、大きな数字を素因数分解するのは困難であることを利用したアルゴリズム。
ed25519	エドワーズ曲線デジタル署名の実装の一つであり、ハッシュ関数としてSHA-512(SHA-2)を使い、曲線としてCurve25519を用いるアルゴリズム。

4. DMARC設定等のチェックサイトの開発・構築に関する調査

4.1. 調査概要
4.2. 調査対象一覧
4.3. DMARCチェックサイトの機能要件
4.4. 運用の課題および懸念点
4.5. 調査結果のまとめ
4.6. 略称一覧

4.1. 調査概要

- 本調査では、国内ISPでのDMARC導入を支援するための政府主導のDMARCチェックサイトの開発および運用に向けた調査を実施した。具体的には以下のとおりである。
  - **海外DMARCチェックサイト一覧**
  - **国内DMARCチェックサイト一覧**
  - **DMARCチェックサイトの機能要件**
- また、実際に本チェックサイトを運用する際の課題および懸念点を合わせて整理する。

4.2. 調査対象一覧

- 本調査における対象は、海外チェックサイト、国内チェックサイトから、以下を対象とした。

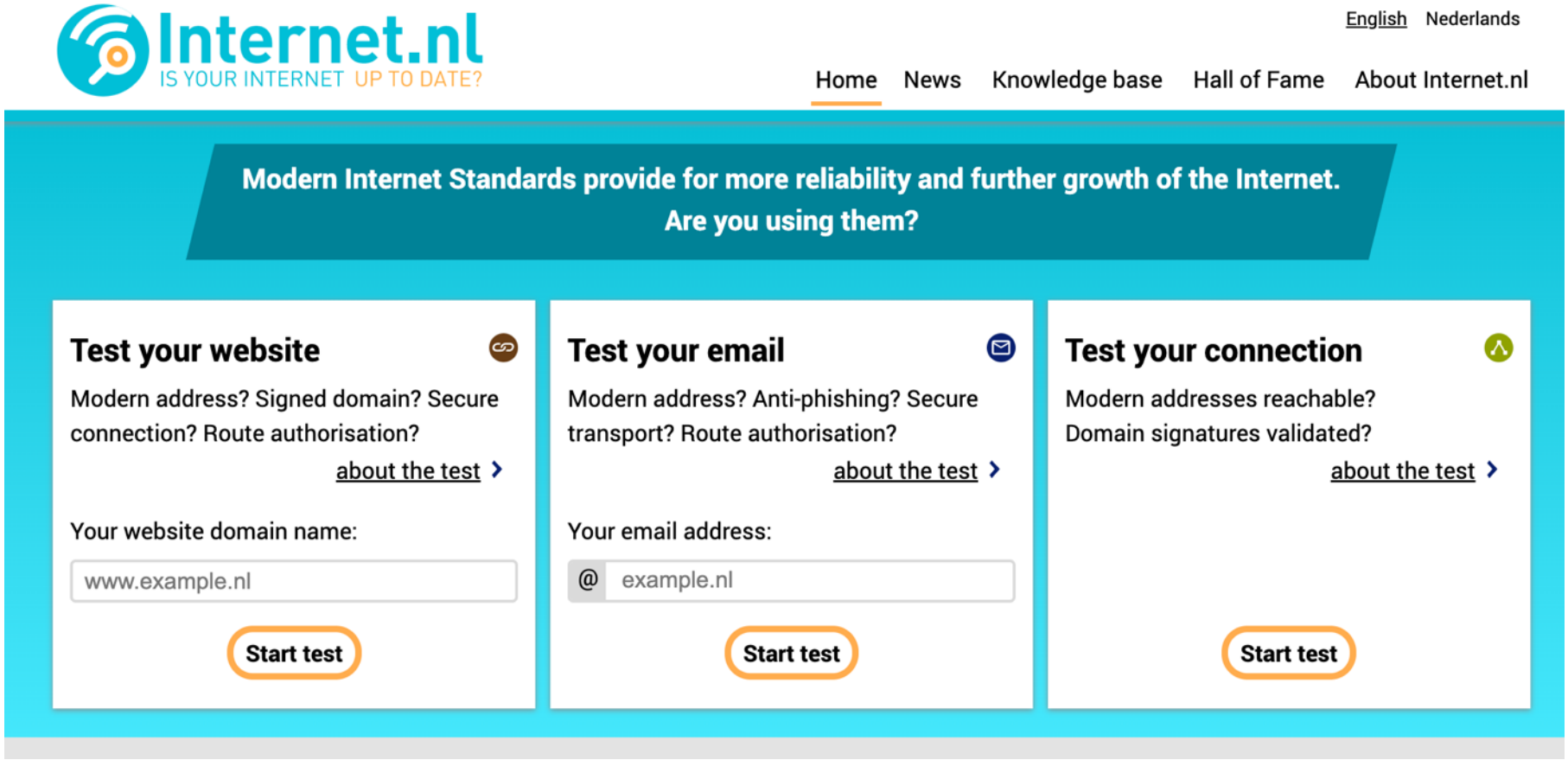
表1 調査対象のチェックサイト一覧

区分	チェックサイト	公開情報URL
海外	❶ Internet.nl	https://internet.nl/
	❷ MXToolBox	https://mxtoolbox.com/
	❸ DMARC Inspector	https://dmarcian.com/dmarc-inspector/
	❹ Domain Scanner	https://easydmarc.com/tools/domain-scanner
	❺ DMARC Validator	https://www.mailhardener.com/tools/dmarc-validator
	❻ MECSA	https://mecsa.jrc.ec.europa.eu/en/technical
国内	❼ ナリタイ	https://naritai.jp/notice check dmarc.html

4.2.1.1. Internet.nl【海外】

- Internet.nlは、オランダ政府およびインターネットコミュニティが運営するサイトで、DMARCを含む最新のインターネット標準に準拠しようとするサイトやドメイン管理者への貢献が目的である。

図1 Internet.nl ウェブサイト(https://internet.nl/)



4.2.1.2. Internet.nl 【海外】チェック項目と結果の通知

- Internet.nl では、入力した「ドメイン名」に対してDMARC関連設定を含めた以下の項目についてチェックができる（表2）。

表2 Internet.nl チェック項目とその概要

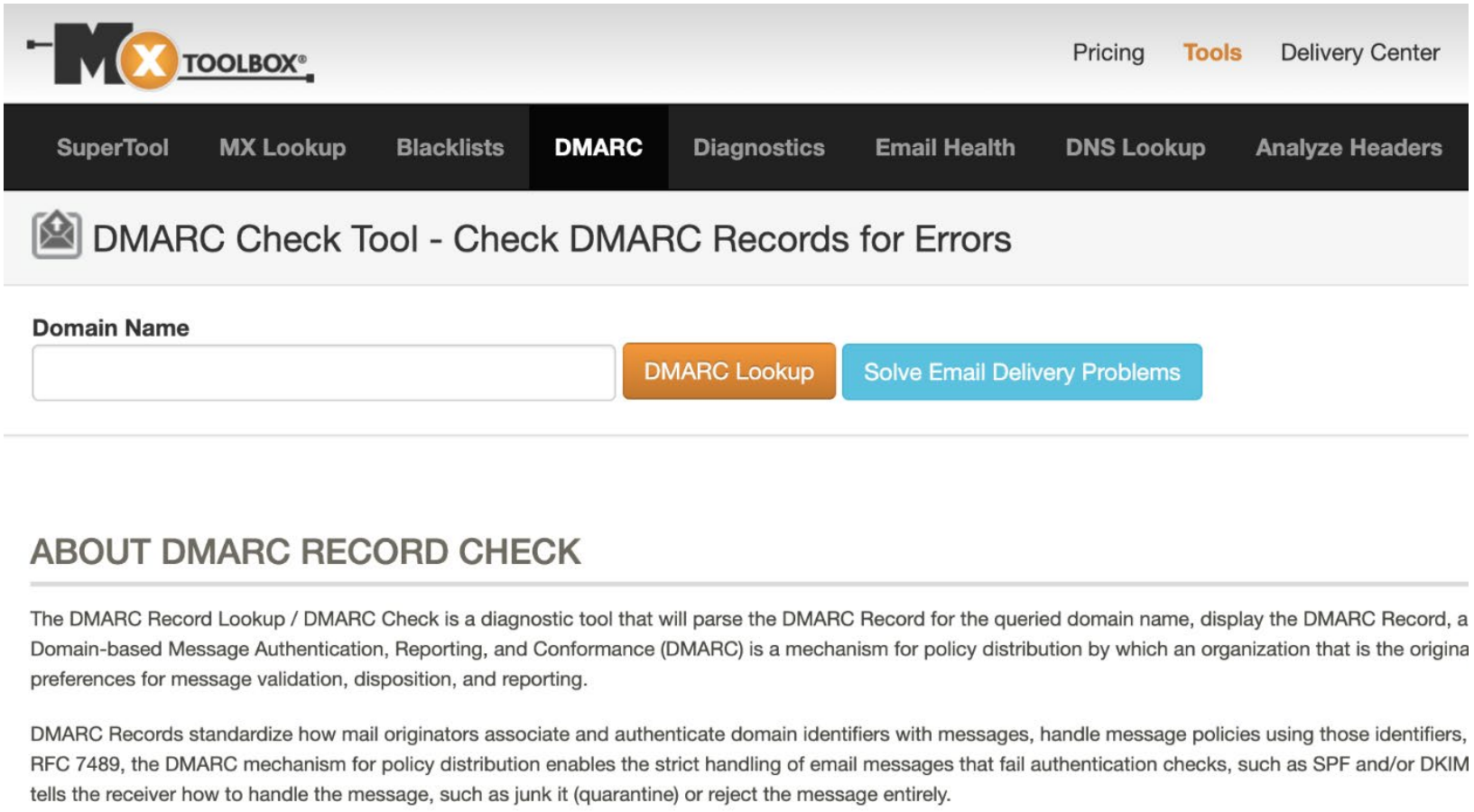
チェック項目	チェック内容	DMARCとの関連
IPv6	AAAAレコードの設定、到達性	
DNSSEC	DNSSECの対応状況	
DMARC, DKIM and SPF	DMARCレコードの存在、DMARCポリシー、 DKIMレコードの存在、SPFレコードの存在、SPFポリシー	●
STARTTLS and DANE	STARTTLS有効性、TLSバージョン、暗号強度、暗号スイート、 証明書、DANEの存在	
RPKI	ROAの存在、ROVの確認	

- Internet.nl では、チェック結果をWebブラウザに表示・レスポンスする（チェックに5～200秒）。

4.2.2.1. MXToolBox【海外】

- MXToolBoxは、MXToolBox, Inc.が運営するサイトで、DMARCを含むネットワーク診断や検索ツールを提供することで、さまざまなインフラの問題解決を支援することが目的である。

図2 MXToolBoxウェブサイト(https://mxtoolbox.com/DMARC.aspx)



4.2.2.2. MXToolBox【海外】チェック項目と結果の通知

- MXToolBox では、入力した「ドメイン名」に対してDMARC関連設定を含めた以下の項目についてチェックができる。なお、チェック項目「DKIM」については、「セレクター名」も合わせて入力する必要がある（表3）。

表3 MXToolBox チェック項目とその概要

チェック項目	チェック内容	DMARCとの関連
MX Lookup	MXレコードの存在、DMARCレコードの存在、DMARCポリシー	●
Blacklists	主要RBLのリストに含まれるか	
Diagnostics	逆引き設定状況、TLSサポート、SMTPコネクション/トランザクションタイム、オープンリレーチェック	
DMARC	DMARC レコードの存在、各タグの設定状況	●
SPF	SPFレコードの存在、各タグの設定状況、ルックアップ可否、ルックアップ数	●
DKIM	DKIMレコードの存在	●
DNS Lookup	Aレコードの存在	

- MXToolBoxでは、チェック結果をWebブラウザに表示・レスポンスする（チェックに数秒から30秒）。

4.2.3.1. DMARC Inspector【海外】

- DMARC Inspectorは、dmarcianが運営するサイトでDMARC設定状況を分析し、電子メールの制御となりすましメール対策の課題解決を促すことが目的である。

図3 dmarcianウェブサイト(https://dmarcian.com/dmarc-inspector/)

4.2.3.2. DMARC Inspector 【海外】チェック項目と結果の通知

- DMARC Inspectorでは、入力した「ドメイン名」に対してDMARC関連設定を含めた以下の項目についてチェックができる（表4）。

表4 DMARC Insperctor チェック項目とその概要

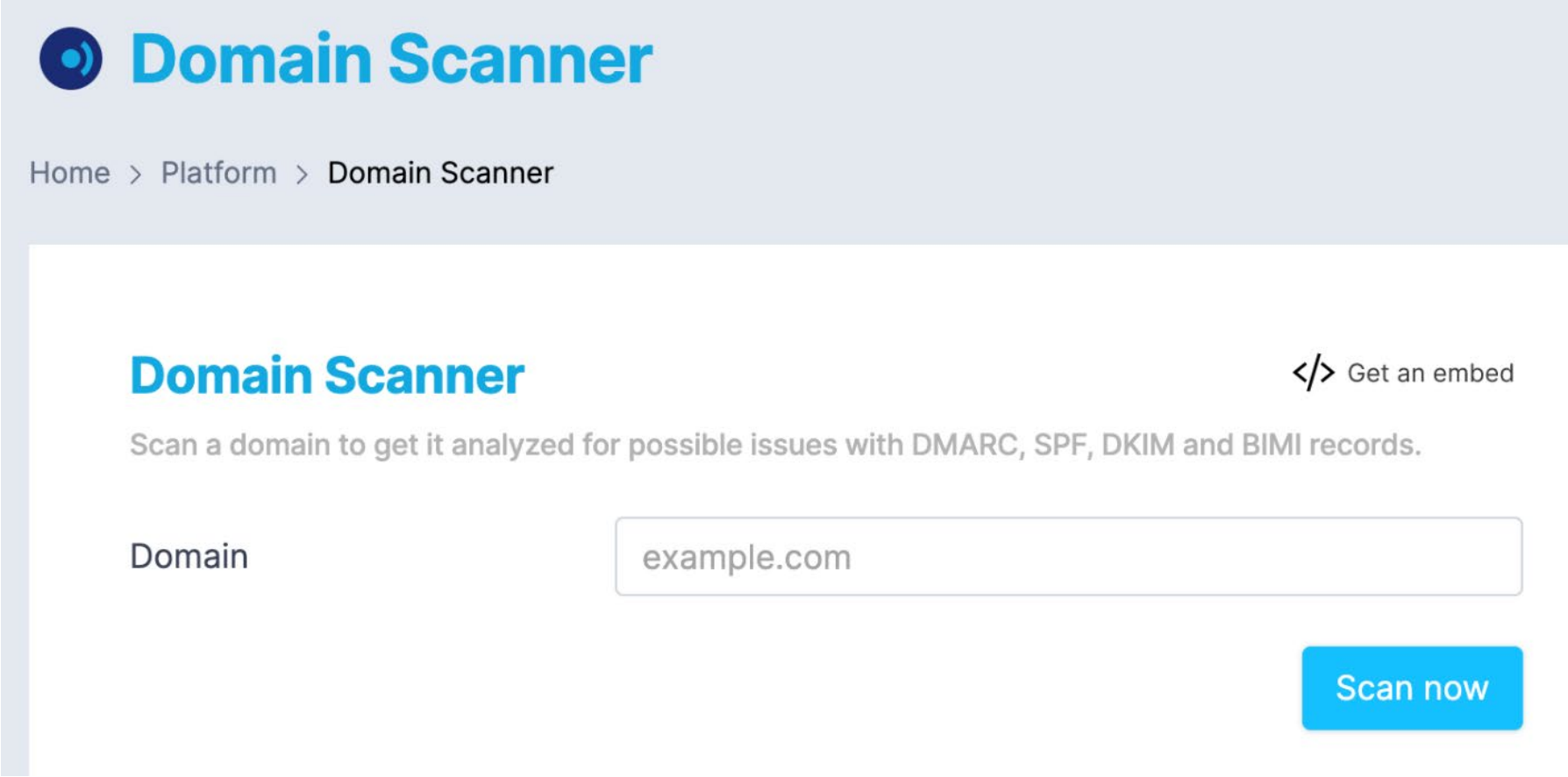
チェック項目	チェック内容	DMARCとの関連
DMARC	DMARC レコードの存在、各タグの設定状況	●

- DMARC Inspectorでは、チェック結果をWebブラウザに表示・レスポンスする（数秒）。

4.2.4.1. Domain Scanner【海外】

- Domain Scannerは、EasyDMARCが運営するサイトでDMARCを含む設定状況を分析することができる。

図4 Domain Scannerウェブサイト(https://easydmarc.com/tools/domain-scanner)



4.2.4.2. Domain Scanner【海外】チェック項目と結果の通知

- Domain Scannerでは、入力したドメイン名に対してDMARC関連設定を含めた以下の項目についてチェックができる（表5）。

表5 Domain Scanner チェック項目とその概要

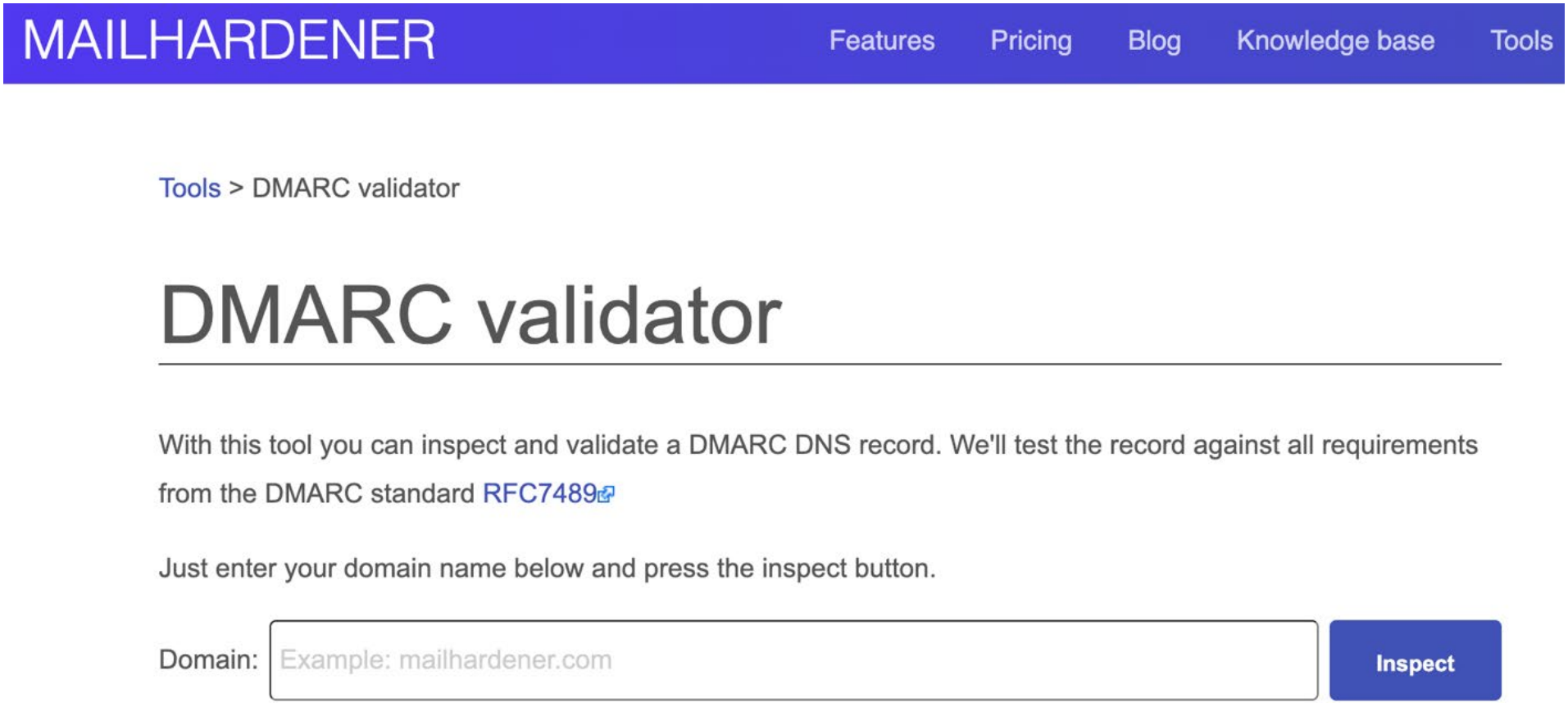
チェック項目	チェック内容	DMARCとの関連
DMARC	DMARC レコードの存在、各タグの設定状況	●
SPF	SPFレコードの存在、ルックアップ数、ネスト数、CIDRの範囲	●
DKIM	DKIMレコードの存在 （ただし、EasyDMARCシステムで管理するセレクター名のみ）	●
BIMI	BIMIレコードの存在、ロゴ画像形式、VMC妥当性、VMC付随情報（有効期限、組織名、商標番号など）、ロゴ画像ビュー	●

- Domain Scannerでは、チェック結果をWebブラウザに表示・レスポンスする（数秒）。

4.2.5.1. DMARC Validator【海外】

- DMARC Validatorは、MAILHARDENERが運営するサイトでRFC7489の全ての要件についてDMARCレコードの探索およびレコードの検証ができる。

図5 DMARC Validatorウェブサイト(https://www.mailhardener.com/tools/dmarc-validator)



4.2.5.2. DMARC Validator【海外】チェック項目と結果の通知

- DMARC Validatorでは、入力したドメイン名に対してDMARC関連設定を含めた以下の項目についてチェックができる（表6）。

表6 DMARC Validator チェック項目とその概要

チェック項目	チェック内容	DMARCとの関連
DMARC	DMARC レコードの存在、各タグの設定状況	●
RUA or RUF	レポート受信先	●

- DMARC Validatorでは、チェック結果をWebブラウザに表示・レスポンスする（数秒）。

4.2.6.1. MECSA【海外】

- MECSA（My Email Communications Security Assessment）は、JRC（Joint Research Centre）によって開発されたDMARCを含むプロバイダー間の電子メール通信のセキュリティを評価するための ツールである。

図6 MECSAのウェブサイト（https://mecsa.jrc.ec.europa.eu/en/technical）

4.2.6.2. MECSA 【海外】チェック項目と結果の通知

- MECSAでは、入力したドメイン名に対してDMARC関連設定を含めた以下の項目についてチェックができる（表7）。

表7 MECSA チェック項目とその概要

チェック項目	チェック内容	DMARCとの関連
STARTTLS	STARTTLS接続可否	
X.509 certificates	サーバ証明書確認	
SPF	SPFレコードの存在、SPFポリシー	●
DKIM	NSサーバからの応答確認	●
DMARC	DMARC レコードの存在、DMARCポリシー	●
DANE	DANEレコードの存在	
DNSSEC	DNSSECによる保護の有無、SPFレコードのDNSSECによる保護の有無、DMARCレコードのDNSSECによる保護の有無、MXレコードのDNSSECによる保護の有無、各MXドメインのDNSSECによる保護の有無、各MXドメインのTLSAレコードのDNSSECによる保護の有無	●
MTA-STS	MTA-STSレコードの存在、MTA-STSポリシーを取得、各MXドメインのMTA-STSポリシーの一致	

- MECSAでは、Pythonスクリプトを実行し、チェック結果をコンソールに出力・レスポンスする（数十秒）。

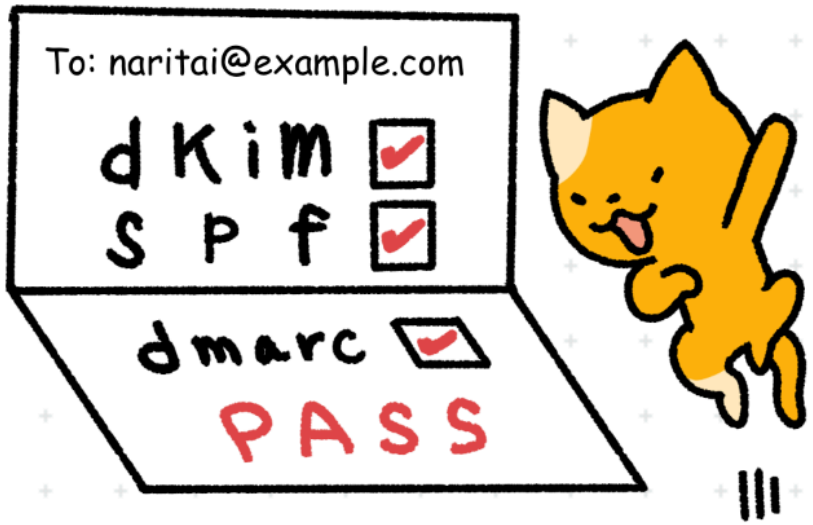
4.2.7.1. ナリタイ 【国内】

- ナリタイは、ナリタイ製作委員会により運営されるサイトで、指定されたメールアドレスにテストメールを送信することで、差出人ドメインのDMARC認証結果をメールで返答するサービスである。

図7 ナリタイのウェブサイト(https://naritai.jp/notice_check_dmarc.html)

DMARC DKIM CHECK について

DMARC DKIM CHECK では、あなたのドメインやメールサーバが正しく設定されているかを確認するツールです。
以下の内容をご一読していただき、
check@naritai.jp に空メールを送信すると、ナリタイから送信ドメイン認証の結果を返送します。
DKIM や DMARC の設定確認にご活用ください。



返送メール例

返送メールには以下のような情報が記載されています。

4.2.7.2. ナリタイ 【国内】チェック項目と結果の通知

- ナリタイでは、入力したドメイン名に対してDMARC関連設定を含めた以下の項目についてチェックができる（表8）。

表8 ナリタイ チェック項目とその概要

チェック項目	チェック内容	DMARCとの関連
DMARC	DMARC認証結果、認証ドメイン、ポリシー	●
SPF	SPF認証結果、接続元IPアドレス	●
DKIM	DKIM認証結果、署名ドメイン	●

- ナリタイでは、チェック結果を差出人メールアドレスに返信・レスポンスする（数秒から30秒）。

4.2.8. 個別調査結果まとめ 1/3

- 本調査の既存チェックサイトについては、DMARC設定だけではなくSPF設定やDKIM設定のチェックまで範囲を広げているサイトが多い（表9、表10、表11）。これは、DMARC認証を成功させるためには、必然的にSPF認証もしくはDKIM認証が求められるためである。

表9 既存チェックサイトのDMARC関連チェック項目のまとめ

チェックサイト	レコード有無	ポリシー設定	各タグ設定
Internet.nl	●	●	なし
MXToolBox	●	▲	●
DMARC Inspector	●	▲	●
Domain Scanner	●	▲	●
DMARC Validator	●	なし	なし
MECSA	●	●	なし
ナリタイ	—	—	—

●：チェック項目あり　▲：各タグのチェック項目がある

4.2.8. 調査結果まとめ 2/3

- SPF認証のチェック項目では、ルックアップ制限内であるかどうかを調査するサイトがいくつか見られており、これはSPF設定の失敗事例としてよく知られていることが理由と考えられる。

表10 既存チェックサイトのSPF関連チェック項目のまとめ

チェックサイト	レコード有無	ポリシー設定	各タグ設定	ルックアップ制限
Internet.nl	●	●	なし	なし
MXToolBox	●	▲	●	●
DMARC Inspector	なし	なし	なし	なし
Domain Scanner	●	▲	●	●
DMARC Validator	なし	なし	なし	なし
MECSA	●	●	なし	なし
ナリタイ	—	—	—	—

●：チェック項目あり　▲：各タグのチェック項目がある

4.2.8. 調査結果まとめ 3/3

- DKIM認証のチェック項目では、DMARC設定やSPF設定とは異なり、ドメイン名だけでは探索できないが、3サイトのうち2サイトは、公開鍵情報を探索する目的でセレクター名を入力する必要がある。他方1サイト（Domain Scanner）については、EasyDMARCを運営するサイトが顧客のDKIM設定管理を運用している場合、セレクター名を入力せずにチェックが可能である。

表11 既存チェックサイトのDKIM関連チェック項目のまとめ

チェックサイト	レコード有無
Internet.nl	●
MXToolBox	●
DMARC Inspector	なし
Domain Scanner	●
DMARC Validator	なし
MECSA	●
ナリタイ	

●：チェック項目あり　▲：各タグのチェック項目がある

4.3.1. DMARCチェックサイトの機能要件【DNS設定チェック】

- 既存チェックサイトの調査結果を踏まえ、チェックサイトに「ドメイン名」を入力するフォームを用意して、評価ボタンをクリックすることで、以下の項目を評価することが望ましい（表12）。また、評価結果はウェブサイトに表示することが望ましい。なお、チェック項目「DKIM」をチェックするためには、署名に利用する公開鍵情報を指定する目的で「セレクター名」も合わせて入力する必要がある。

表12　チェックサイトに必要と考えられるDNS設定評価項目一覧

評価項目	評価ポイント	評価方法・内容
DMARC	1.存在性（FQDN）	ラベル”_dmarc”を先頭に付与したドメイン名のTXTレコードが存在するかどうかを評価する
	2.存在性（OD）	ドメイン名の組織ドメインについて、ラベル”_dmarc”を先頭に付与したドメイン名のTXTレコードが存在するかどうかを評価する
	3.構文評価	1もしくは2で確認されたレコードがDMARCレコードとして有効であるかどうかを評価する
	4.ポリシー評価	3で有効と評価されたレコードのポリシーが”quarantine”あるいは”reject”であるかどうかを評価する
	5.タグ評価	3で有効と評価されたレコードの各タグが適切であるかどうかを評価する
	6.レポート先評価	3で有効と評価されたレコードのruaタグおよびrufタグで指定されたURIが適切であるかを評価する
SPF	7.存在性	ドメイン名のTXTレコードのうち、SPFレコードの構文として有効なものが唯一つ存在するかどうかを評価する
	8.ルックアップ可否	7で確認されたレコードのディレクティブ（a, mx, include, redirectなど）が有効であるかを評価する
	9.ルックアップ数	7で確認されたレコードのルックアップ数が制限以下であるかを評価する
DKIM	10.存在性	ドメイン名およびセレクター名で構成されたDKIMレコードが存在するかどうかを評価する
	11.構文評価	10で確認されたレコードがDKIMレコードとして有効であるかどうかを評価する
	12.強度	10で確認されたレコードの公開鍵の強度が十分であるかを評価する
BIMI	13.存在性	ドメイン名およびセレクター名で構成されたBIMIレコードが存在するかどうかを評価する
	14.ロゴ画像評価	13で確認されたレコードのlタグで指定されたロゴ画像が妥当であるかどうかを評価する
	15.VMC妥当性評価	13で確認されたレコードのaタグで指定されたVMCが妥当であるかどうかを評価する

4.3.2. DMARCチェックサイトの機能要件【送信メール判定チェック】

- チェックサイトに記載されたメールアドレスにテストメールを送信することで、以下の項目を評価する（表13）。評価結果は差出人メールアドレス（ヘッダーFromドメイン）に返送する。

表13　チェックサイトに必要と考えられる送信メール判定評価項目一覧

評価項目	評価ポイント	評価方法・内容
DMARC	1.認証結果	DMARCの認証結果を記載する。
	2.DKIMアライメント	DKIMイン・アライメントかどうかを評価する。DMARCが有効でない場合は推定する。
	3.SPFアライメント	SPFイン・アライメントかどうかを評価する。DMARCが有効でない場合は推定する。
	4.措定される処理結果	DMARCポリシーに従った処理結果を評価する。DMARCが有効でない場合は評価しない。
SPF	5.認証結果	SPFの認証結果を記載する。
	6.SPFドメイン	SPF評価に利用したドメイン名を記載する。
	7.スコープ	エンベロープFromドメインかEHLO/HELOドメインかを記載する。
	8.接続元IPアドレス	SPF評価に利用したIPアドレスを記載する。
DKIM	9.認証結果	DKIMの認証結果を記載する。
	10.署名ドメイン	DKIM評価に利用したドメイン名を記載する。
	11.セレクター名	DKIM評価に利用したセレクター名を記載する。
	12.失敗理由	DKIMの認証結果がpass出ない場合の理由を記載する。
BIMI	13.認証結果	BIMIの認証結果を記載する。
	14.ロゴ画像	表示するロゴ画像を記載する。
	15.VMC評価	VMCの有効期限、組織名、商標番号

4.4. 運用の課題および懸念点

- 上記に挙げた機能要件を有するDMARCチェックサイトを運用するにあたり、以下の課題や懸念があるため、これらを考慮して、設計することが望ましい。

1. 運用サイトのドメイン

調査したDMARCチェックサイトの多くは民間組織での運用である（6サイトのうち、4サイト）。サイト運用が民間ではなく政府の場合は、サイトドメインは政府ドメイン（.GO.JP）もしくはそのサブドメインで永続的に運営する必要がある。運用サイトのドメイン名が政府ドメイン以外にならざるを得ない場合は、ドロップキャッチによる悪用を防止する体制を整える。

2. 安定的な稼働のためのアクセス制限

調査したDMARCチェックサイトは原則として無料で利用なツールであるが、大量通信やサイバー攻撃への防御を想定した外部仕様・システム設計が必要である。具体的な例は以下の通りである。

- 接続元情報によるアクセス数制限の実施（大量通信対策）
- 評価結果表示のレスポンス遅延（大量通信対策、ボットアクセス対策）

3. 技術規格のアップデートへの対応

DMARC技術規格およびBIMI技術規格については将来的に更新される可能性があるため、定期的な見直しをする必要がある。また、DKIMに関しては、署名として利用が推奨される鍵ペアの強度や電子署名アルゴリズムを見直す必要がある。

4.5. 調査結果のまとめ

- 本調査では、海外の6つのDMARCチェックサイトおよび国内の1つのDMARCチェックツールを調査した。DMARCチェックサイトを開発・運用する場合には、それぞれの評価項目のうち、DMARCに関連する項目のみを網羅するような機能要件が望ましい。
- DNS設定に関する評価はウェブサイトで評価結果が表示されるインターフェースが主流である。
- さらに、実際に正規なメールシステムから送信されたメールの認証結果のフィードバックはメール返送するチェックサイトもあった。
- 利用者の利便性を考慮し、これらと同様の仕様で構築、運用することが望ましい。
- DKIMに関連する項目については、署名に利用する公開鍵情報を探索する目的で、ドメイン名と合わせてセレクター名も入力項目として用意することが望ましい。
- 本調査結果で整理した機能要件をもとにして、DMARCチェックサイトを開発・運用することが求められる。

4.6. 略称一覧 1/2

表14 略称一覧

本報告書でも表記	正式名称・意味など
DMARC	Domain-based Message Authentication, Reporting, and Conformance 送信ドメイン認証技術の一つ。SPFとDKIM両者を利用したメールのドメイン認証を補強する技術である。
DKIM	DomainKeys Identified Mail 送信ドメイン認証技術の一つ。送信元が付した電子署名により送信元情報の真偽及び電子メールの本文の改変を検知することができる。
SPF	Sender Policy Framework 送信ドメイン認証技術の一つ。エンベロープ情報の From メールアドレスのドメイン名をチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。
FQDN	Fully Qualified Domain Name TCP / IP ネットワーク上で、ドメイン名・サブドメイン名・ホスト名をすべて省略せずに指定した記述形式のことを指す。
OD	Organizational Domain 組織ドメインと呼ばれる、wwwなどのラベルを持たない登録ドメイン（ネイキッドドメイン）を指す。
RUA	Reporting URI(s) for aggregate data DMARCを含む送信ドメイン認証結果について、ある程度の期間分をまとめて受信メールサーバからドメイン管理者にフィードバックされる統計情報。

4.6. 略称一覧　2/2

表14 略称一覧

本報告書でも表記	正式名称・意味など
RUF	Reporting URI(s) for failure data 送信されたメールがSPFまたはDKIMに一致せず、受信者側でDMARC認証に失敗した場合に生成されて、受信メールサーバからドメイン管理者にフィードバックされるフォレンジック情報。
BIMI	Brand Indicators for Message Identification Webメールやメールアプリで、DMARC認証が成功し、なりすまされていないメールに対して、その送信者ドメインに関連したロゴを表示する仕組み。
VMC	Verified Mark Certificate BIMIで表示するロゴが送信者ドメインの所有するロゴであることを証明する証明書。
RBL	Real-time Block List 迷惑メール(スパムメール)の中継・発信元のIPアドレスをまとめたブロックリスト。
X.509 証明書	X.509は、公開鍵証明書の標準形式の一つ。
CIDR	Classless Inter-Domain Routing クラスを使わないIPアドレスの割り当てと、経路情報の集成を行う技術。
MTA-STS	SMTP MTA Strict Transport Security メールの配送経路上のメールサーバ間の暗号化を強制化する技術の一つ。

DMARC技術 関連調査結果報告

2023年11月6日 初版

株式会社 三菱総合研究所

先進技術・セキュリティ事業本部

本資料の記載は、「令和4年度総務省事業ISPにおけるネットワークセキュリティ技術の導入に関する調査」を基にしています。