DMARCご紹介資料

2024年1月

Messaging Business Division / HENNGE株式会社

Customers Mail Cloud
Produced by HENNGE

目次

DMARC とは？

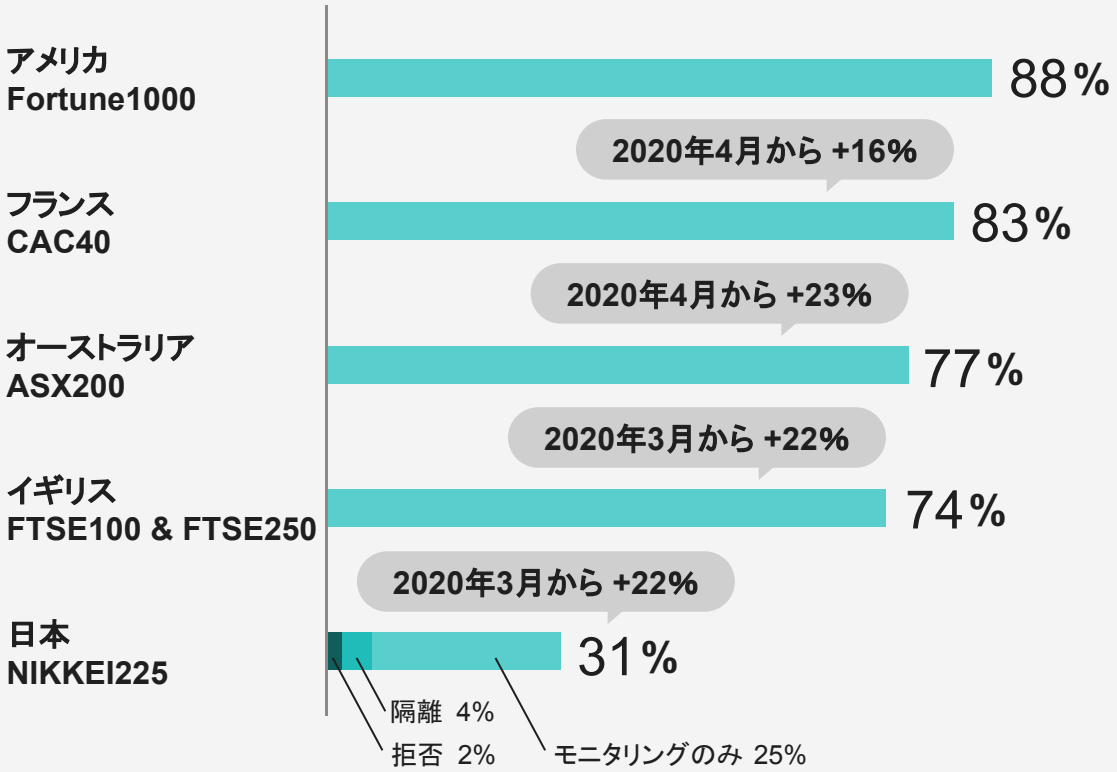
DMARCとは、Domain-based Message Authentication, Reporting & Conformanceの略。

巧妙な「なりすましメール」の増加にともない、メール受信者をフィッシング被害から守るために、世界で活用されている対策の1つ。

本資料では、DMARCの基本的な内容の確認から、導入の際はどのように進めればよいのか、つまづきやすいポイントなどをご説明いたします。お客さまのDMARC導入の際に、ご参考になれば幸甚です。

なぜ今なのか？DMARCへ取り組むべき理由

なぜ今なのか？DMARCへ取り組むべき理由



出典:Proofpoint

- 個人向けメールサービスにおいて**DMARCは世界標準**。
- アメリカでは約90%、ヨーロッパでは半数～約70%がDMARC認証を導入。
- 日本では約31%*1。**ビジネスメール詐欺の標的としてDMARC未導入企業が狙われている**状況。
- イギリス・アメリカでは**政府サービス・ドメインでDMARCを義務化**され*2、民間企業での導入も進む。
- **日本政府も一部民間企業などへDMARC導入を要請**しており、その有用性が注目されている。

＊1:Nikkei225企業内
＊2:イギリスは2016年、アメリカは2017年より義務化
＊3:2020年～

DMARCに関する行政の動き

経済産業省

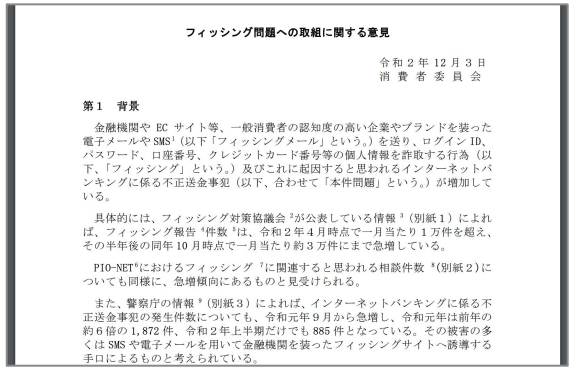
フィッシング詐欺の被害を未然に防ぐことを目的に、**「フィッシング対策協議会」**を設立

2005年4月

内閣府

送信ドメイン認証技術（SPF、DKIM、DMARC）の導入を普及促進

2020年12月



フィッシング問題への取組に関する意見

令和２年12月３日
消費者委員会

第１　背景

金融機関や EC サイト等、一般消費者の認知度の高い企業やブランドを装った電子メールや SMS[1]（以下「フィッシングメール」という。）を送り、ログイン ID、パスワード、口座番号、クレジットカード番号等の個人情報を詐取する行為（以下、「フィッシング」という。）及びこれに起因すると思われるインターネットバンキングに係る不正送金事犯（以下、合わせて「本件問題」という。）が増加している。

具体的には、フィッシング対策協議会[2]が公表している情報[3]（別紙１）によれば、フィッシング報告[4]件数[5]は、令和２年４月時点で一月当たり１万件を超え、その半年後の同年 10 月時点で一月当たり約３万件にまで急増している。

PIO-NET[6]におけるフィッシング[7]に関連すると思われる相談件数[8]（別紙２）についても同様に、急増傾向にあるものと見受けられる。

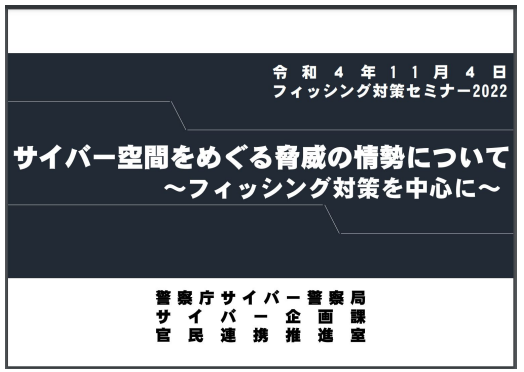
また、警察庁の情報[9]（別紙３）によれば、インターネットバンキングに係る不正送金事犯の発生件数についても、令和元年９月から急増し、令和元年は前年の約６倍の 1,872 件、令和２年上半期だけでも 885 件となっている。その被害の多くは SMS や電子メールを用いて金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられている。

※2020年12月3日「フィッシング問題への取組に関する意見」より（https://www.cao.go.jp/consumer/content/20201203_iken.pdf）

警察庁

サイバー警察局「フィッシング対策セミナー」にて**DMARC導入を推奨**

2022年11月



令和４年11月４日
フィッシング対策セミナー2022

サイバー空間をめぐる脅威の情勢について
～フィッシング対策を中心に～

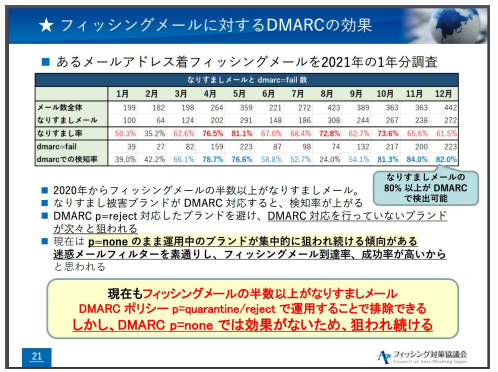
警察庁サイバー警察局
サイバー企画課
官民連携推進室

※「フィッシング対策セミナー2022」（2022年11月4日）より（https://www.antiphishing.jp/pdf/apcseminar2022npa.pdf）

経済産業省

第４回クレジットカード決済システムのセキュリティ対策強化検討会にて**DMARC導入を推奨**

2023年2月



★ フィッシングメールに対するDMARCの効果

■ あるメールアドレス着フィッシングメールを2021年の1年分調査

なりすましメールと dmarc=fail 数

	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
メール数全体	199	182	198	264	359	221	272	423	389	363	363	442
なりすましメール	100	64	124	202	291	148	186	308	244	267	238	272
なりすまし率	50.3%	35.2%	62.6%	76.5%	81.1%	67.0%	68.4%	72.8%	62.7%	73.6%	65.6%	61.5%
dmarc=fail	39	27	82	159	223	87	98	74	132	217	200	223
dmarcでの検知率	39.0%	42.2%	66.1%	78.7%	76.6%	58.8%	52.7%	24.0%	54.1%	81.3%	84.0%	82.0%

なりすましメールの80%以上がDMARCで検出可能

■ 2020年からフィッシングメールの半数以上がなりすましメール。
■ なりすまし被害ブランドが DMARC 対応すると、検知率が上がる
■ DMARC p=reject 対応したブランドを避け、DMARC 対応を行っていないブランドが次々と狙われる
■ 現在は **p=none のまま運用中のブランドが集中的に狙われ続ける傾向がある**
迷惑メールフィルターを素通りし、フィッシングメール到達率、成功率が高いからと思われる

現在もフィッシングメールの半数以上がなりすましメール
DMARC ポリシー p=quarantine/reject で運用することで排除できる
しかし、DMARC p=none では効果がないため、狙われ続ける

21

※第6回クレジットカード決済システムのセキュリティ対策強化検討会（2023年1月20日）（https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/004.html ）

正規のメールアドレスから送信される「なりすましメール」

- もっとも高度なものは、「ドメインのなりすまし」。
- メールソフトに表示されるメールアドレスは簡単に偽装することができる。
- 実際に送信したメールアドレスと、表示されるメールアドレス(head-from)が同じものか、受信者が見分けることは困難。
- **DMARCを実装することにより、なりすましメールに起因する犯罪被害から顧客を守ることが可能に。**

メールソフトで表示されるフィッシングメールの例

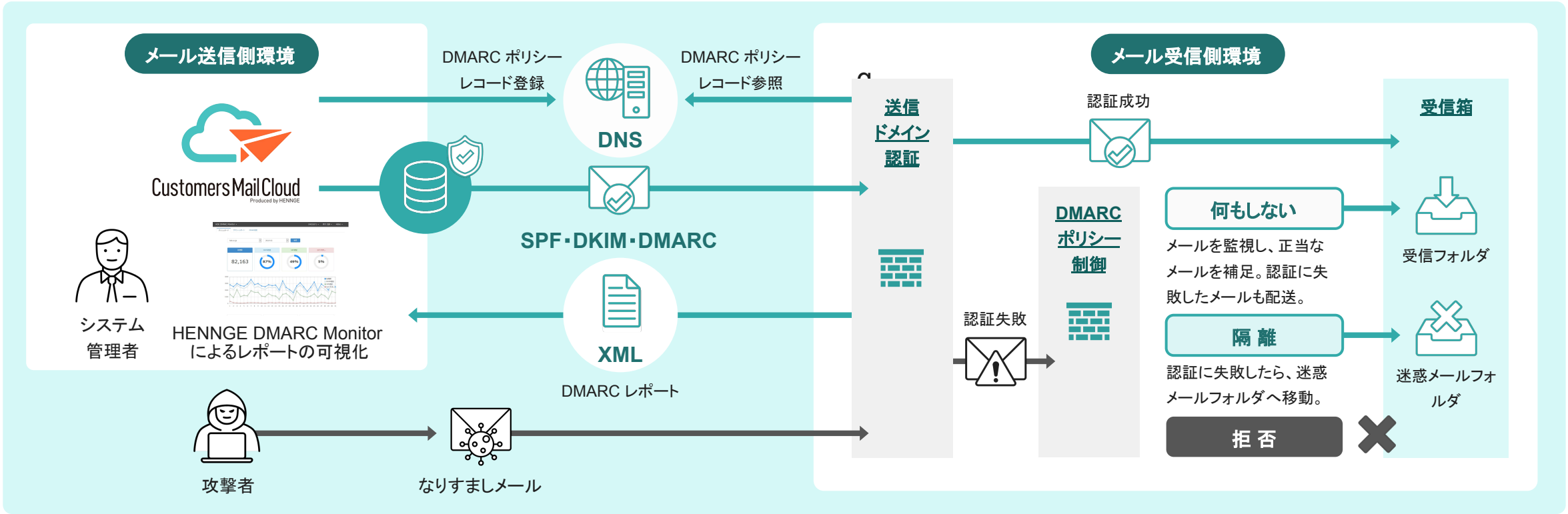
見かけ上の ❶ 送信元表示名・❷送信元メールアドレスが偽装されているケースは、なりすましの判別が困難。

出典：独立行政法人情報処理推進機構安心相談窓口だより2021年9月21日号
https://www.ipa.go.jp/security/anshin/mgdayori20210921.html

DMARCの仕組み・メリット

DMARCの仕組み

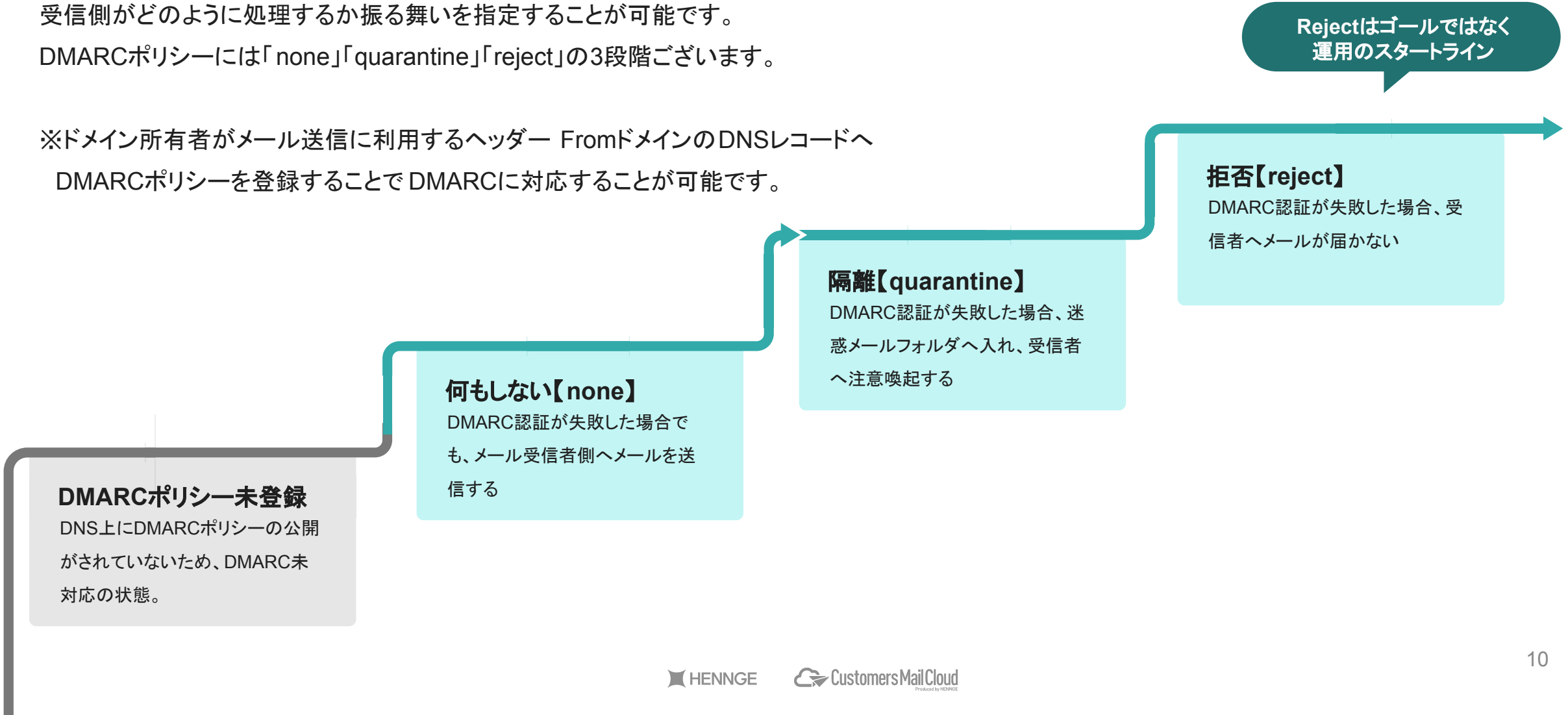
DMARCとは、メール送信側が「なりすましメール」の取り扱い方法（ポリシー）を宣言し、
既存の標準技術であるSPFとDKIMを用いて、メール受信側から認証状況についてレポートを受け取るなど、
送信ドメイン認証の結果を積極的に活用する仕組みです。



DMARCポリシーとは

DMARCではメール送信に利用するドメインの所有者が DMARC認証に失敗したメールを
受信側がどのように処理するか振る舞いを指定することが可能です。
DMARCポリシーには「none」「quarantine」「reject」の3段階ございます。

※ドメイン所有者がメール送信に利用するヘッダー Fromドメインの DNSレコードへ
DMARCポリシーを登録することで DMARCに対応することが可能です。



DMARC対応のメリット

DMARCレポートから以下の情報を取得し活用することで、社内のIT資産管理や投資計画に役立てることも可能です。

Report 1

疑わしいIPアドレス(送信元)

DMARCからなりすましメールの流通状況が把握でき、不正利用の通報、DMARCポリシーの強化に活用可能となる。

Report 2

DMARC認証が失敗する理由

認証結果を集計することで、DMARCの認証に失敗要因の確認、メール送信側がDMARC適応にあたり対応すべき内容が明確となる。

Report 3

把握していない正規のメールサーバ

認証結果を集計することで、送信元のメールサーバの一覧が確認できるため、社内の利用状況調査等に活用できる。

Report 4

メールサーバの設定不備の詳細

認証結果を集計することで、認証失敗の原因となりやすいSPFレコードの設定不備や把握していないサブドメインの確認ができる。

セキュリティ体制の証明

顧客に安全な企業のイメージを与え、メール到達率の向上も期待できます。

自社ドメインが狙われにくくなる

犯罪者は未対策のドメインを狙う傾向があり、ブランド保護に役立ちます。

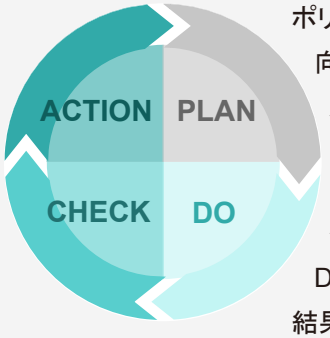
送信者側で受信者のアクションを制御

DMARCポリシー宣言により、認証失敗メールに対するアクションを指定できます。

DMARCの導入・運用に必要なものとは

Policy=Rejectへの道

Policy(p)=rejectまで到達するには、
各段階でPDCAを回し続けなければいけない。



SPF/DKIM設定の見直し、DMARC認証成功の確認

ポリシー引き上げに向けたタスクとスケジュール整理

DMARC認証失敗理由と不正送信元の洗い出し

タスクの実施
DMARC認証の結果確認

調査
DMARCを適応させるドメインの決定、メール送信元システムの洗い出しと、各システムのSPFとDKIMの設定状況を確認。

モニタリングの開始
DMARCポリシー「none」にてヘッダFromドメイン毎に送信元システム情報等の洗い出し。

設定の不備の修正
モニタリングの結果を元にDMARC認証が失敗しているメール送信元システムの改修。
改修後の結果確認。

DMARCポリシーの引き上げ
改修後のDMARC認証結果を基にポリシーを「quarantine」「reject」へ引き上げを実施。

さらなるPDCA
Rejectはゴールではなく運用のスタートライン

レポート評価とアクション設定の正解がわからない
受信したDMARCレポートを、どう見ていけば良いのか？専門家の力を借りたい..

初期設定の作業が重くて踏み出せない！
特に前半の段階は大変な道のり..
なかなか手がつけられていない。

自前でのDMARC導入が難しい理由

自前でDMARC導入に取り組み始めた担当者は、このようなことに悩み、先に進めなくなります。

大量のレポート解読に悩む

日々返却されてくる大量のDMARCレポート。
中身がXML形式だから解読できない…

DMARC導入の進め方に悩む

まずはp=noneでDMARCレコードを公開したものの、次に何をしたら良いのか、全くわからない…

関係者特定と、コンセンサス作りに悩む

自社ドメインを送信しているIPアドレスが分かっても、どの部署が何の業務で利用しているのか不明…

顧客や社内への影響に悩む

正規の送信メールが届かなくなることはないか？顧客や事業部門からクレームが来たら困る…

導入を断念

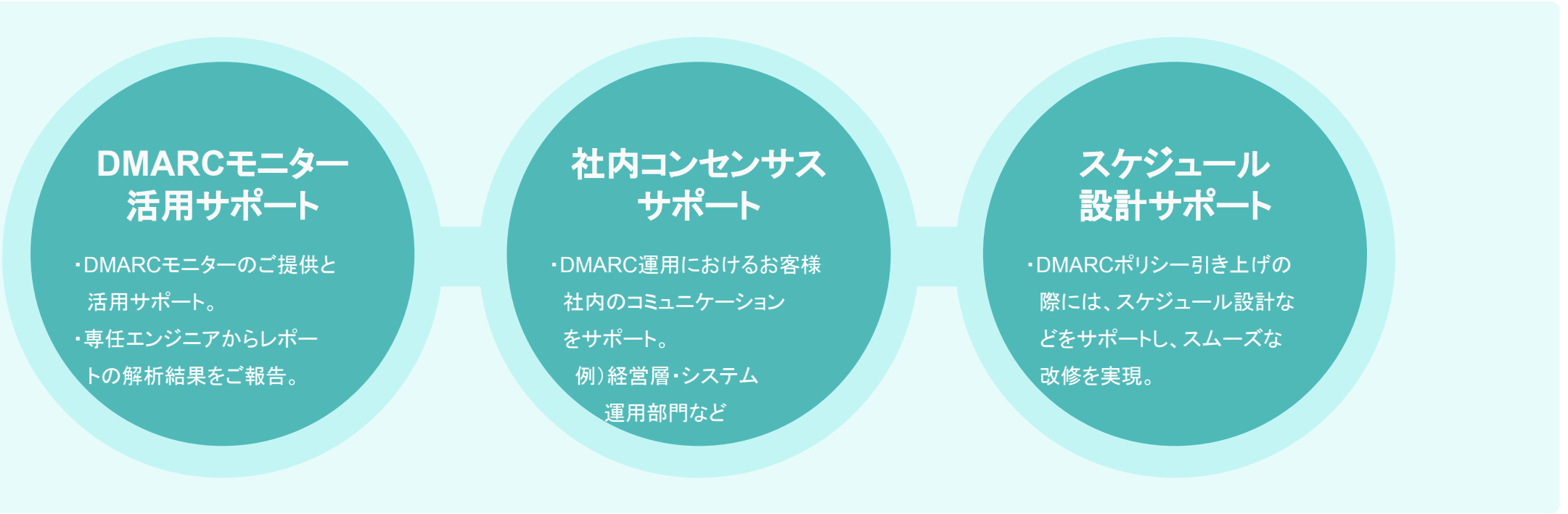
導入に膨大な時間と手間を要し、リソース不足に陥るケースが多い。導入したものの、活用できない例も。

専門家による支援を依頼

DMARC導入には、専門家のサポートが必要不可欠。
サポートを受けることでスムーズな導入と運用を！

p=rejectの状態に引き上げることができる！

HENNGEによるDMARC最適化支援

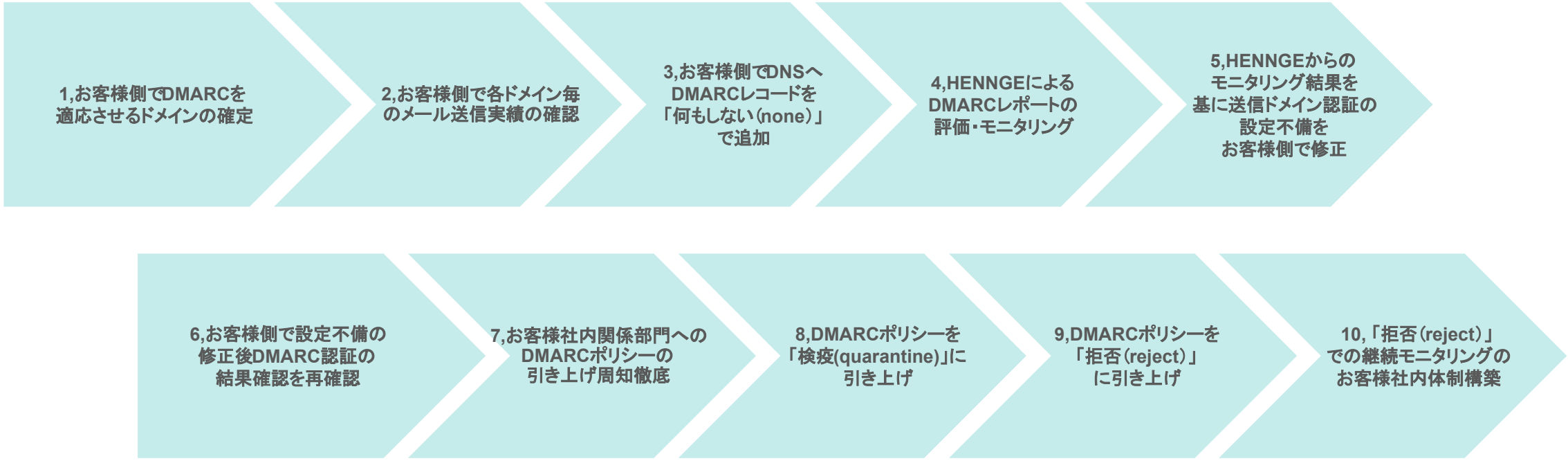


- DMARCの実装・運用にあたっては、多くの時間・工数・専門知識が必要。
- 導入後も活用できない企業様が増えている。
- 専門家がトータルでサポートすることによりスムーズな導入・運用を実現できる。

HENNGEの具体的な支援内容

DMARCの導入手順

DMARCを実装するにあたり多くの時間や工数・専門知識・社内でのコミュニケーションや合意形成が必要となるため、
導入後に継続的に活用できない企業が増えております。
HENNGEは、DMARCの導入からDMARCポリシーの「reject」引き上げまでトータルにご支援いたします。



HENNGEのDMARCコンサルティング支援

HENNGEではDMARCの導入前からポリシーの引き上げ完了までを 2つのphaseに分けてご支援させていただきます。

- Phase1：お客様側でメール送信に利用しているドメインの洗い出しをご支援
- Phase2：DMARCを適応させるドメイン毎のポリシーの引き上げをご支援

Phase1（p=noneの状態で現状のメール送信状況を整理）

内容	期間	支援・作業内容
▼確認作業 モニタリング（p=none）実施前の現状整理	約3ヵ月～半年	・DMRACモニターツールの利用方法レクチャー ・DMRACレコード登録支援 ・各親ドメインへ紐づくサブドメインのヘッダーFromドメインの確認 ・各ヘッダーFromドメイン毎のサービス名・IPアドレスの確認 ・各ヘッダーFromドメイン毎のDMARC認証不備情報の確認 ・QA支援

Phase2（p=noneの状態でのモニタリング～ p=rejectの完了）

内容	期間	支援・作業内容
▼ DMARCの実装 ポリシー引き上げ支援	約半年～1年	・各親ドメインへ紐づくサブドメインのヘッダーFromドメインの確認 ・各ヘッダーFromドメイン毎のサービス名・IPアドレスの確認 ・各ヘッダーFromドメイン毎のDMARC認証不備情報の確認 ・ドメイン毎のポリシー引き上げの計画支援・進行支援 ・DNSレコード（TXTレコード、MXレコード）設計支援 ・社内関係者向け説明会（必要に応じて最大回/月） ・QA支援

Apendix

先進企業の事例（BIMI）

＊BIMI(Brand Indicators for Message Identification)
ドメインから送信される認証済みメールにブランドのロゴを追加するためのメール標準で、BIMI に対応するメールクライアントの受信トレイでは、メールの横に送信者のブランドのロゴが表示される。

- DMARC 導入および reject へのポリシー変更の際には、ウェブサイトや広報誌などで受信者向けに周知を行い、送信者ドメインの確認を促すことが求められます。
- 弊社も事例の公開や連名でのプレスリリースなどにより広報活動をサポートいたします。

正規メールの視認性向上においては、GmailやApple iCloudメールで使えるBIMIやYahoo!メールブランドアイコンなどのサービスが有益です。これら視認性向上技術の導入に関しても弊社でサポート可能です。

出典：Yahoo! JAPANプレスリリース(2022.09.06)
https://about.yahoo.co.jp/pr/release/2022/09/06a/

楽天グループにおけるなりすまし・フィッシングメール対策について
https://corp.rakuten.co.jp/security/anti-fraud/

HENNGEが提供する価値

メール送信基盤整備の専門家

20年以上に渡り、政府・金融機関やエンタープライズ企業のメール送信基盤整備を手掛けてきた、メールのプロフェッショナル集団。S/MIME、SPF/DKIM、DMARCと多数の導入支援実績。

フィッシング対策へのコミット

フィッシング対策協議会の正会員企業として、関係する政府機関とも連携して、DMARCの普及促進に積極的に関わっています。

フィッシング対策協議会
Council of Anti-Phishing Japan

クラウドセキュリティのトータルソリューション

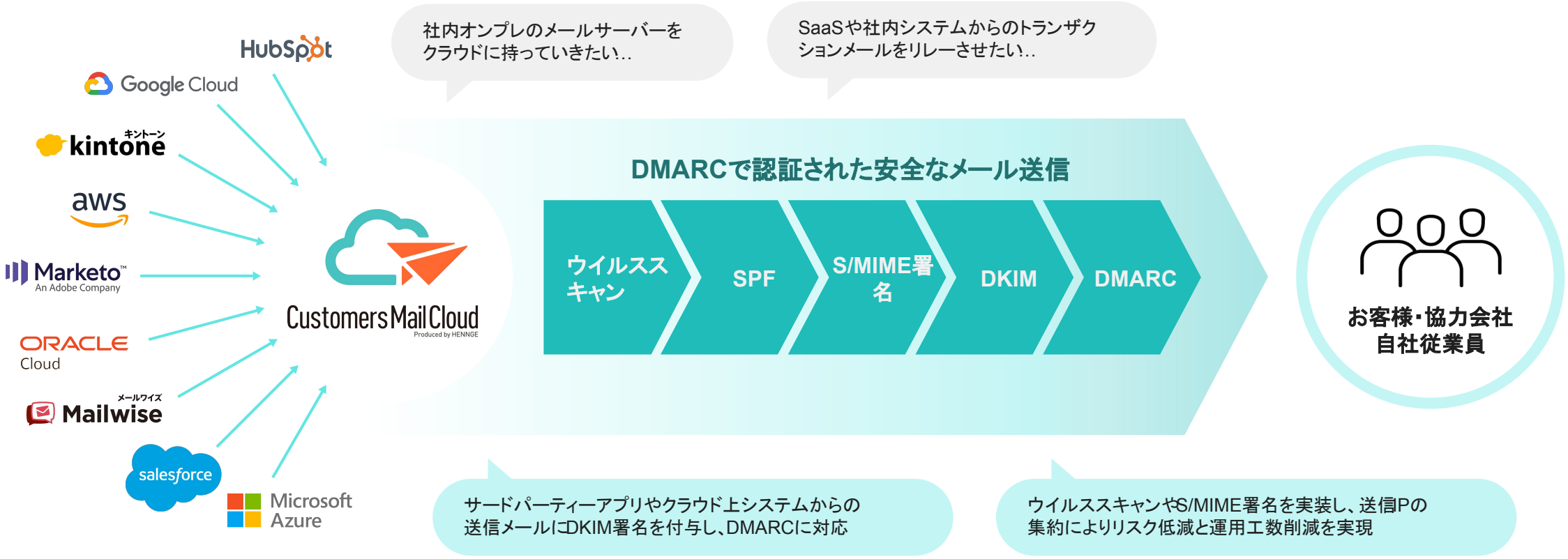
国内導入実績No.1のHENNGE One（アクセス制限・シングルサインオン・メールセキュリティ）などのプロダクトを提供。トータルで企業をサポートします。

HENNGE One

クラウドやSaaSからのメールも安全に

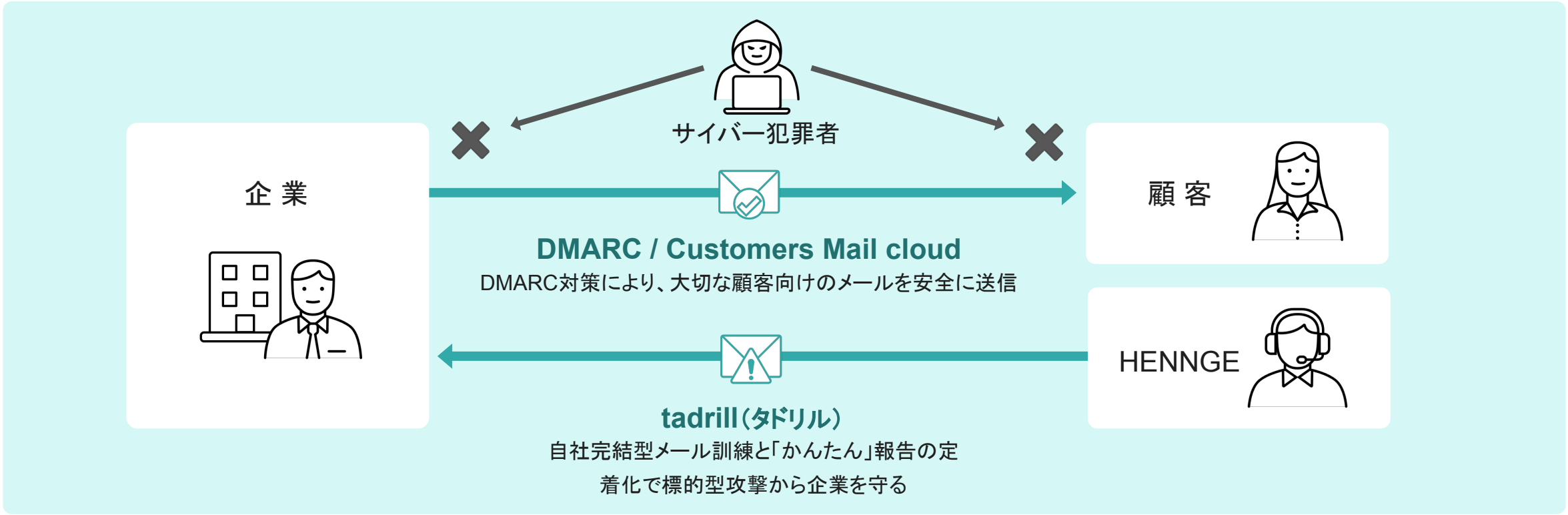
クラウド上のアプリケーションやSaaSからのメールもDMARC対応のスコープになります。

クラウド型のメールサービスを経由することでDMARC認証された安全なメール送信を実現します。



送信と受信の両面で企業と顧客を守る

企業はメール送信側でもあり、受信側でもあります。送信側の立場ではDMARC対応することにより、顧客へのメールを安全に送信し犯罪者から送信されるフィッシングメールから顧客を守ります。受信側の立場では標的型攻撃訓練サービスの利用により、自社および従業員に対するフィッシングメールのリスクを低減できます。




HENNGE