DMARC・DKIM設定支援のご提案書

2023年12月1日
株式会社システナ
DXデザイン本部

メール業界の動向

なりすましメール被害のリスク軽減に対する対策として、国内、海外の主要ISP、業界団体はDMARCの推進を強めており、送信ドメイン認証の対応を呼びかけています。
また、製造・物流・小売業界等でも**取引の条件でDMARCの対応**が呼びかけられたり、業界として対応するように呼びかけも強化されています。

2023年 7月 19日以降、 Microsoft社はDMARCポリシーを遵守するようになりました。

公式ページ：Announcing New DMARC Policy Handling Defaults for Enhanced Email Security

2024 年 4 月以降 (2月以降段階的に適用開始)、Google社、yahoo社がメール送信者のガイドラインに準拠しない場合、メールを受信しないようにすることを名言してしています。その中で**DMARC** や**迷惑メール率**などが定義されています。

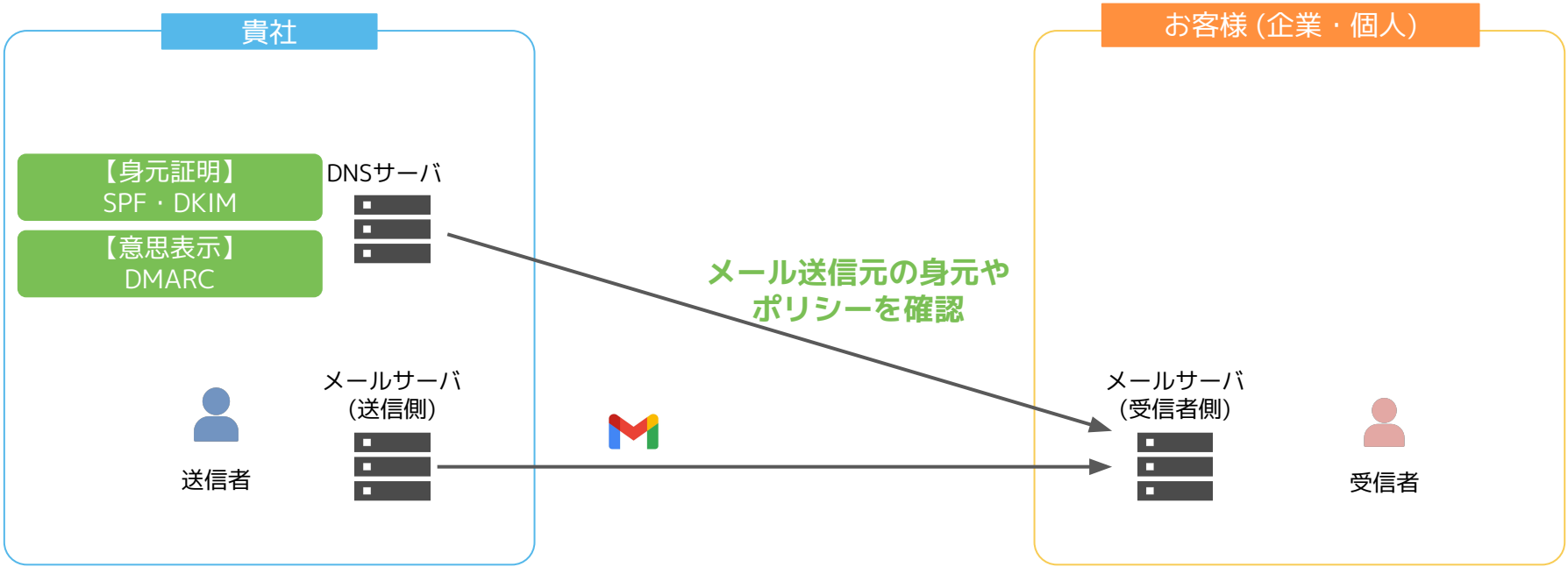
公式ページ：Google社メール送信者ガイドライン

重要

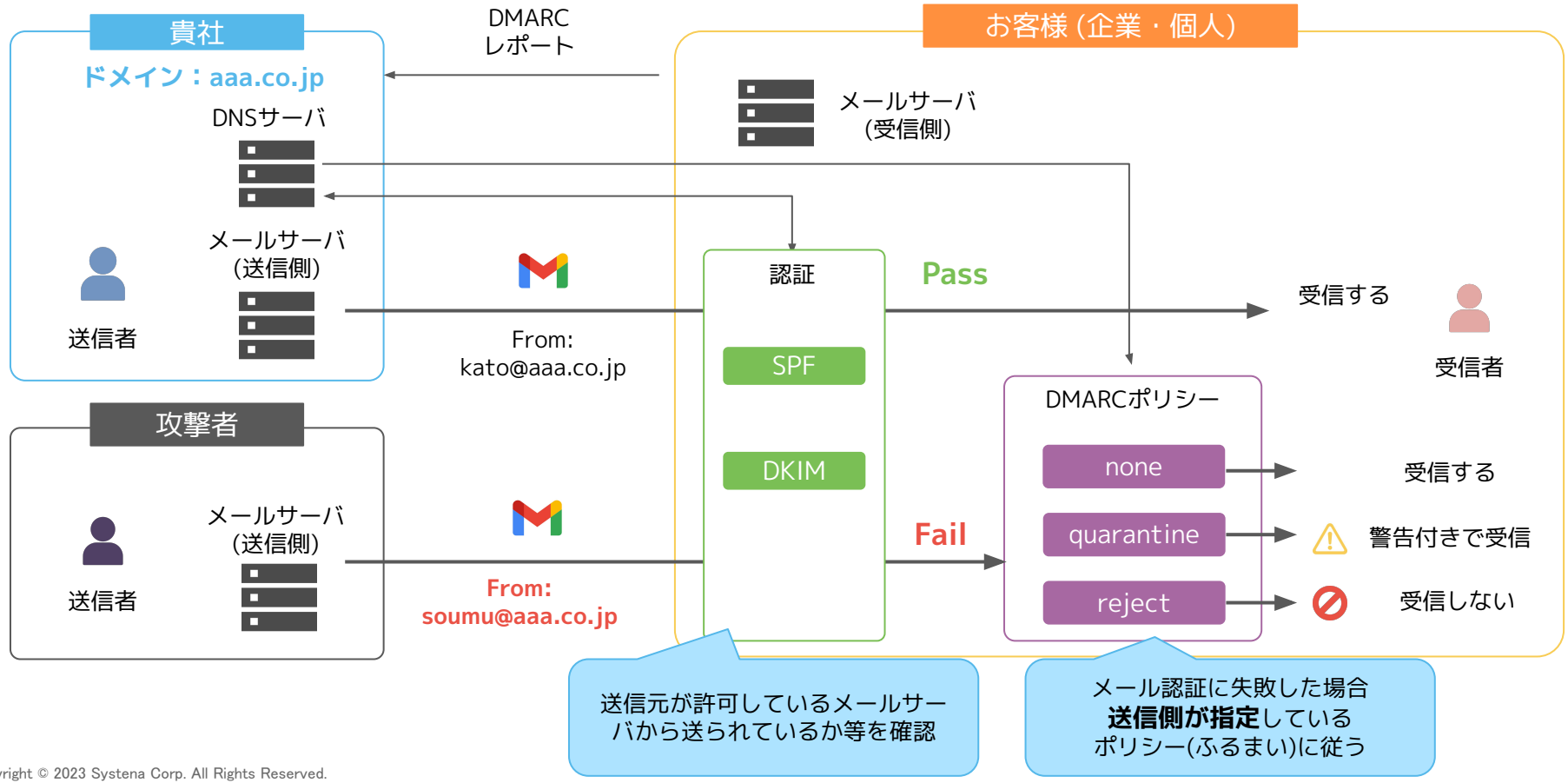
送信ドメイン認証に必要なSPF・DKIM・DMARCの設定が正しくされていないと2024年 4 月以降取引先、コンシューマーへのメールが届かなくなる可能性が高まります。

DMARC・DKIMとは

メール受信者がメール送信者の身元などを確認できる情報をDNSにて公開する仕組みの一つです。
GoogleWorkspaceの場合は導入時からDKIM(共通版) が設定されておりますが
今回ご提案するのは DKIM(専用版)・DMARC という仕組みの設定となります。



メールの仕組み



用語説明

会社メールのなりすましを防止するために会社ドメイン(メールで使用しているドメインすべて)に使用しているメールサーバー情報、メールサーバーの証明書等を記載することで、送信元メールアドレスの詐称やメール内容の改ざんを検知することが可能になります。下記は対象のDNSレコード情報の概要となります。

SPF（Sender Policy Framework）：

メールを送信することが承認されているサーバーとドメインを指定することで、指定外の送信元からのなりすましメールを検知する仕組みです。

DKIM（DomainKeys Identified Mail）：

すべての送信メールにデジタル署名を追加することで、受信サーバーはメールが実際に組織から送信されたものであることを確認できます。

DMARC（Domain-based Message Authentication, Reporting, and Conformance）：

組織からの送信メールが SPF または DKIM の検証に合格しなかった場合に、そうしたメールの処理方法を受信サーバーに指示する仕組みです。
指示パターンとして検証に合格しなかった場合、該当メールを受信サーバーが**「通す(受信する)（none）」・「隔離(迷惑メール扱い)（quarantine）」・「拒否(受信しない)（reject）」**を指定することができます。

よくあるご相談

Microsoft社、Google社の呼びかけが強まっており、DMARC設定に対するご相談が急増しております。

1位　DMARCの設定方法がわからない、ちゃんと設定されたかの確認方法がわからない

2位　DKIMの設定方法がわからない、ちゃんと設定されたかの確認方法がわからない

3位　DMARCポリシーの設定、そのリスク、運用方法がわからない

解決策

SPF・DKIM・DMARC設定支援からDMARCポリシー引き上げのための分析支援まで一連のご支援プランをご用意しております。
有識者をアサインしますので各設定時の注意すべきポイントをおさえたご支援、トラブルが発生した際も早期解決に向けた対応が可能です。

SPF・DMARC・DKIM設定支援内容

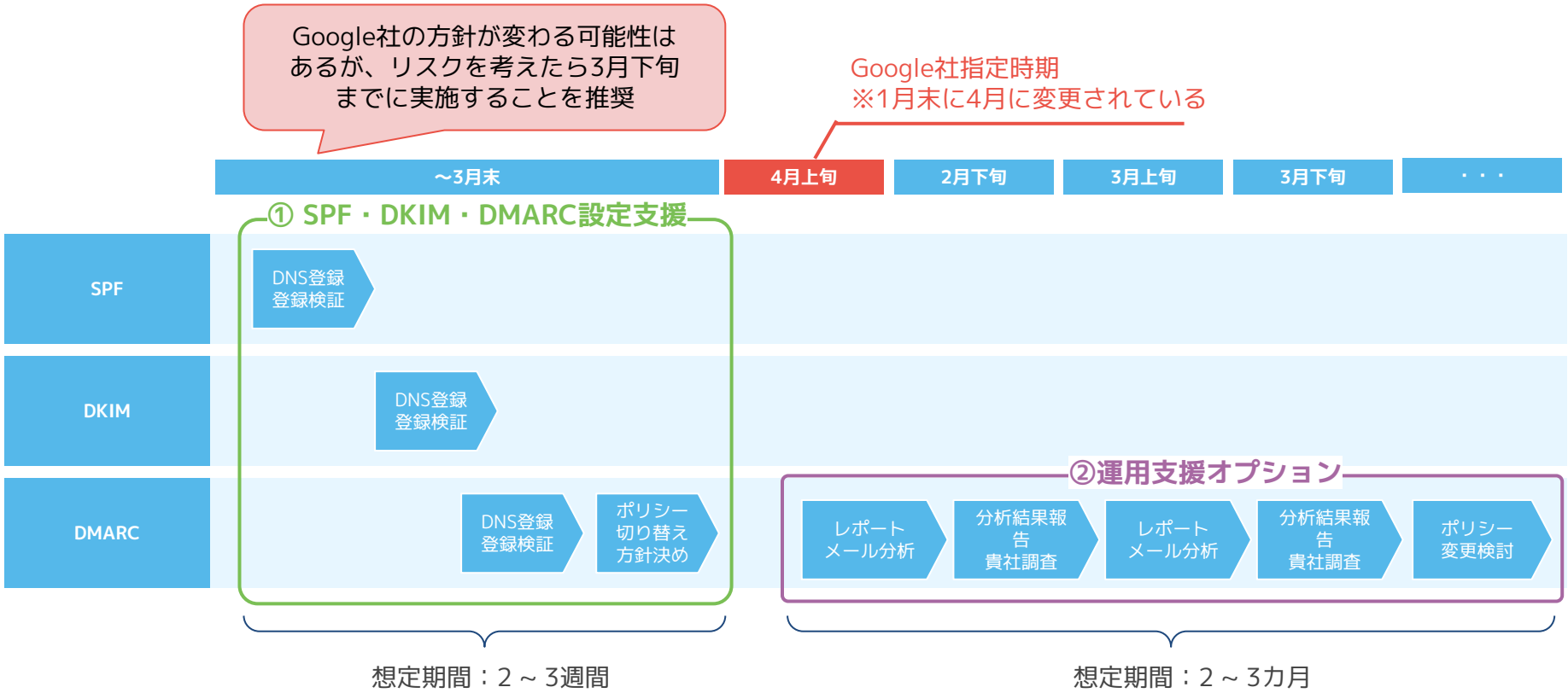
① SPF・DKIM・DMARC設定支援

STEP1	STEP2	STEP3
SPF・DKIM設定	DMARC設定	DMARCレベル切り替えの方針決め
・メインメールサービスのSPFレコードの登録確認 ・管理コンソールでDKIM鍵を取得支援 ・DNSレコードの登録支援 **・ツールによる検証** ・DNS反映確認 **・メール受信による確認** **・DNS参照回数確認**	・DNSレコードの登録情報支援 **・メール受信による確認** **・ツールによる検証**	ポイント **・DMARCポリシー切り替えまでの流れ、手順のドキュメント提供**

②運用支援オプション

STEP4
DMARCレポート監視 DMARCレベル切り替え
・DMARCレポートメール分析代行 **・分析結果、見解報告** **・セキュリティレベル切り替え支援**

設定支援想定スケジュール



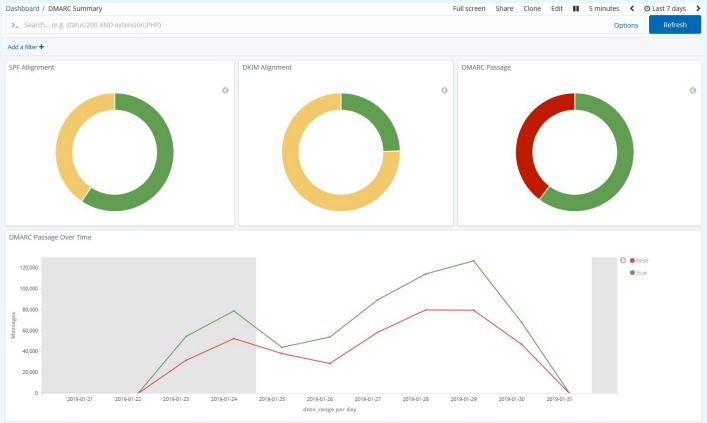
運用支援オプション　イメージ

1カ月目	2カ月目	3カ月目
分析環境構築 初回分析	**社内対応 対応後の状況分析**	**DMARC厳格化 厳格化後の最終分析**
・**DMARCレポート可視化、分析用ツールの環境構築** ・**Google Workspaceの場合、メールから添付ファイルを一斉出力するスクリプトの提供** ・1カ月相当のDMARCレポート可視化データ提供	・可視化データをもとにDNSの追加や社内調整の相談会 ・必要に応じてDNSの設定支援 ・2 週間 ~ 1カ月のDMARCレポート可視化データ提供	・**厳格化可否の相談会** ・厳格化に伴うDNSの設定支援 ・厳格化後の2 週間 ~ 1カ月のDMARCレポート可視化データ提供

DMARCレポート分析例

分析ツールを使った分析結果例となります。

送信元IPアドレスの所有者	送信元IPアドレスのDNS逆引き結果	送信元IPアドレス	送信元IPアドレス（国）	受信側の処理	SPF認証結果	DKIM認証結果	レポート送信元	SPF認証結果（詳細）	DKIM認証結果（詳細）	ヘッダーFromドメイン	件数
google.com	mail-sor-f69.google.com	209.85.220.69	US	none	TRUE	TRUE	google.com	pass	pass	貴社ドメイン	10000
kagoya.net	vms**.kagoya.net	153.127.230.**	JP	none	FALSE	FALSE	Enterprise Outlook	softfail	-	貴社ドメイン	100
kagoya.net	vms**.kagoya.net	153.127.230.**	JP	none	FALSE	FALSE	google.com	softfail	-	貴社ドメイン	200



分析ツールグラフイメージ

全体のメール送信総数に対してSPF/DKIMの認証失敗の割合を一目で見れるグラフでの出力も可能です。

最後に

Link People for Happiness

systena

DXデザイン本部

中村　芳将

nakamurayo@systena.co.jp
TEL 090-6046-6623

株式会社 システナ

本　　社　〒105-0022　東京都港区海岸1丁目2番20号　汐留ビルディング 16Ｆ
TEL 03-6367-3871　FAX 03-3578-3016

https://www.systena.co.jp　　https://canbus.com/

東京証券取引所プライム市場（証券コード：2317）

本書に含まれる情報は、貴社内部でのご検討、評価のために提供されるものです。貴社内でのご使用、複製、開示はこの目的の為に必要な範囲でのみお願いいたします。