Email Security Under Attack: What Hackers Exploit, and How to Stop Them

メールセキュリティの攻撃と対策：悪用される脆弱性と防御の仕組み

March 9, 2026 / 2026 年 3 月 9 日

English Version

See page 3 →

日本語版

27 ページへ →

eSolia

Email Security Under Attack: What Hackers Exploit, and How to Stop Them

March 9, 2026

Contents

A plain-language guide to email authentication: SPF, DKIM, and DMARC — and what breaks when they are missing.

The Call You Never Made

Your company's name appears in someone's inbox. The sender address looks legitimate. The subject line says there's a voicemail waiting. The recipient clicks, enters credentials, and hands an attacker the keys to their account.

Nobody at your company sent that email. Your domain was used without your permission — and without the right protections in place, there was nothing to stop it.

This guide explains how attackers exploit unprotected email domains, what the technical defenses do, and what happens when those defenses work as intended. Real-world attack patterns show the difference protection makes.

How Email Was Designed — and Why That's a Problem

Email was invented in the 1970s for a small network of trusted researchers. The original design has a fundamental flaw that was never fixed: **anyone can claim to be anyone**.

When you send an email, the "From" address is just a label. Nothing in the original protocol requires proof that the sender controls that domain. It's like sending a letter with any return address you choose — the postal system has no way to verify it's real.

This is why attackers can send email that appears to come from `yourcompany.com`, `yourbank.com`, or even government agencies. The address in the recipient's inbox is a claim, not a verified identity.

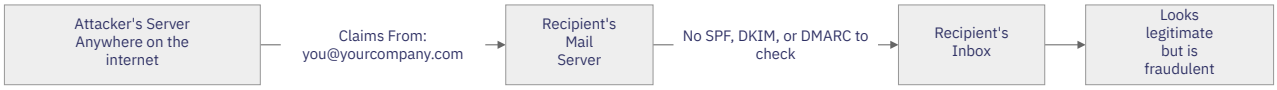
Three technologies were developed to fix this: SPF, DKIM, and DMARC. Together, they create a chain of proof that ties email to the domain it claims to come from.

The Attack Surface: What Happens Without Protection

Attackers have three main approaches when a domain has no protections.

Scenario 1: Direct Domain Spoofing

An attacker sends email claiming to be from `you@yourcompany.com`. Without SPF or DKIM, receiving mail servers have no basis to reject it. The email lands in the recipient's inbox looking completely legitimate.



Direct Domain Spoofing Diagram

An unprotected domain opens the door to executive impersonation for wire-transfer fraud, credential harvesting through fake login pages, and malware disguised as internal IT attachments.

Scenario 2: Lookalike Domain Attack

The attacker registers a domain that resembles yours: `yourcompany-jp.com`, `yourcompny.com`, or using Unicode characters that look identical to Latin letters. They set up proper SPF and DKIM on their domain, so email passes authentication — it just authenticates to the wrong domain.

Scenario 3: Third-Party Service Abuse

Attackers frequently use legitimate, reputable email delivery services — such as major cloud providers' bulk mail platforms — to send phishing email. Because these services have strong IP reputations, the messages bypass IP-based spam filters easily.

A common variant is **vishing** (voice phishing): an email formatted as a missed-voicemail notification, designed to create urgency and prompt the recipient to click a link to "retrieve their message." The familiar format lowers suspicion. The link leads to a credential-harvesting page.

The authentication headers in this kind of attack tell the story clearly:

Check	Result	Explanation
SPF	Pass	The cloud service is an authorized sender — but for its own domain, not the claimed domain
DKIM	Pass	The cloud service signed the message — with its own key, not the claimed domain's
DMARC	**Fail → Reject**	Neither SPF nor DKIM aligned with the `From:` domain

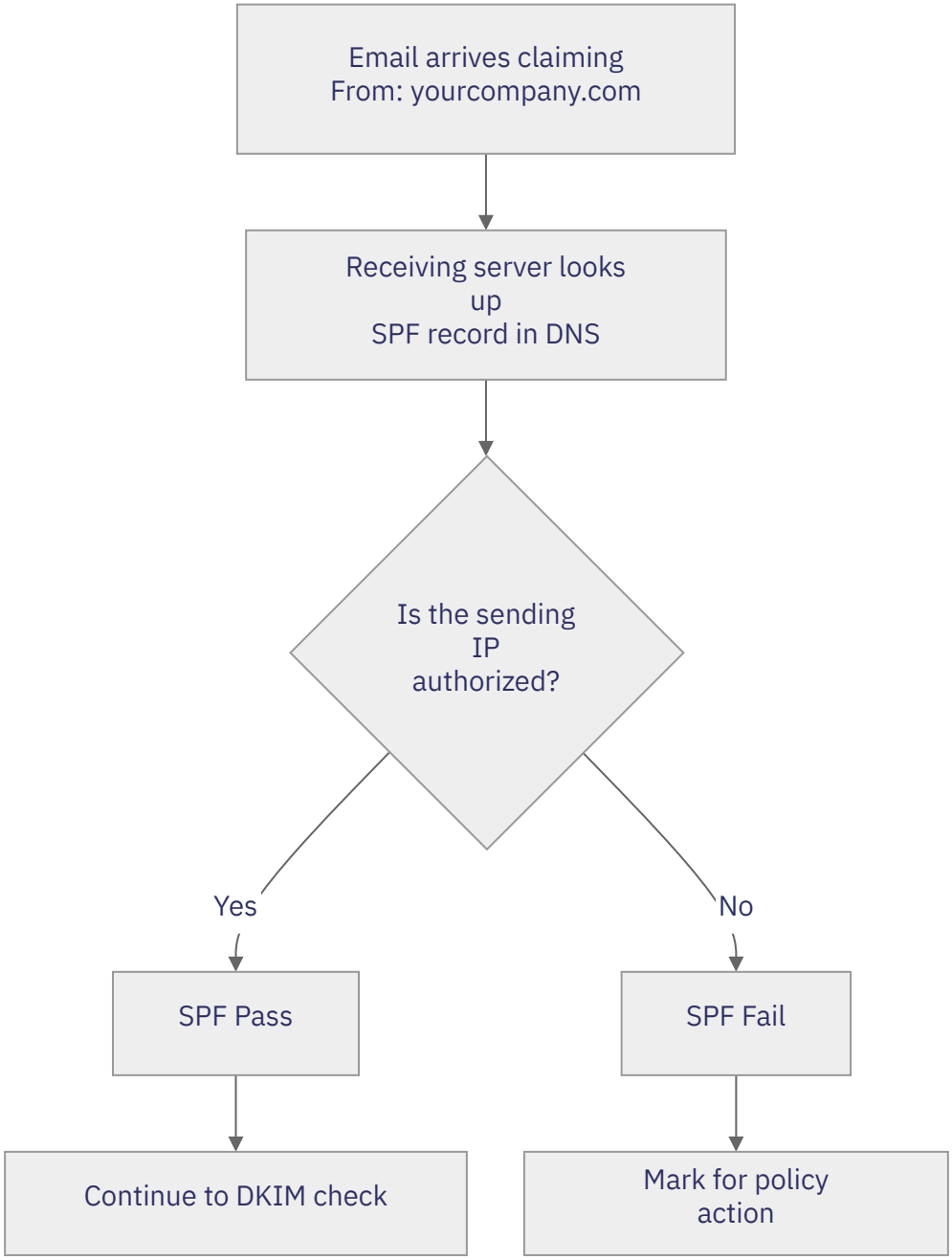
When DMARC is configured with a `reject` policy, this attack fails before reaching the recipient. Without DMARC, it delivers cleanly.

The Three Defenses Explained

SPF: Authorized Senders

SPF (Sender Policy Framework) is a DNS record that answers the question: “Which mail servers are allowed to send email for this domain?”

When a receiving server gets an email from `yourcompany.com`, it looks up the SPF record in DNS and checks whether the sending server’s IP address is on the approved list.



SPF Check Flow Diagram

SPF's limitation: It checks the envelope sender — the technical routing address — not the visible "From" address in the email client. An attacker can pass SPF with their own sending infrastructure while displaying your domain in the From field. SPF alone is not enough.

Example SPF record:

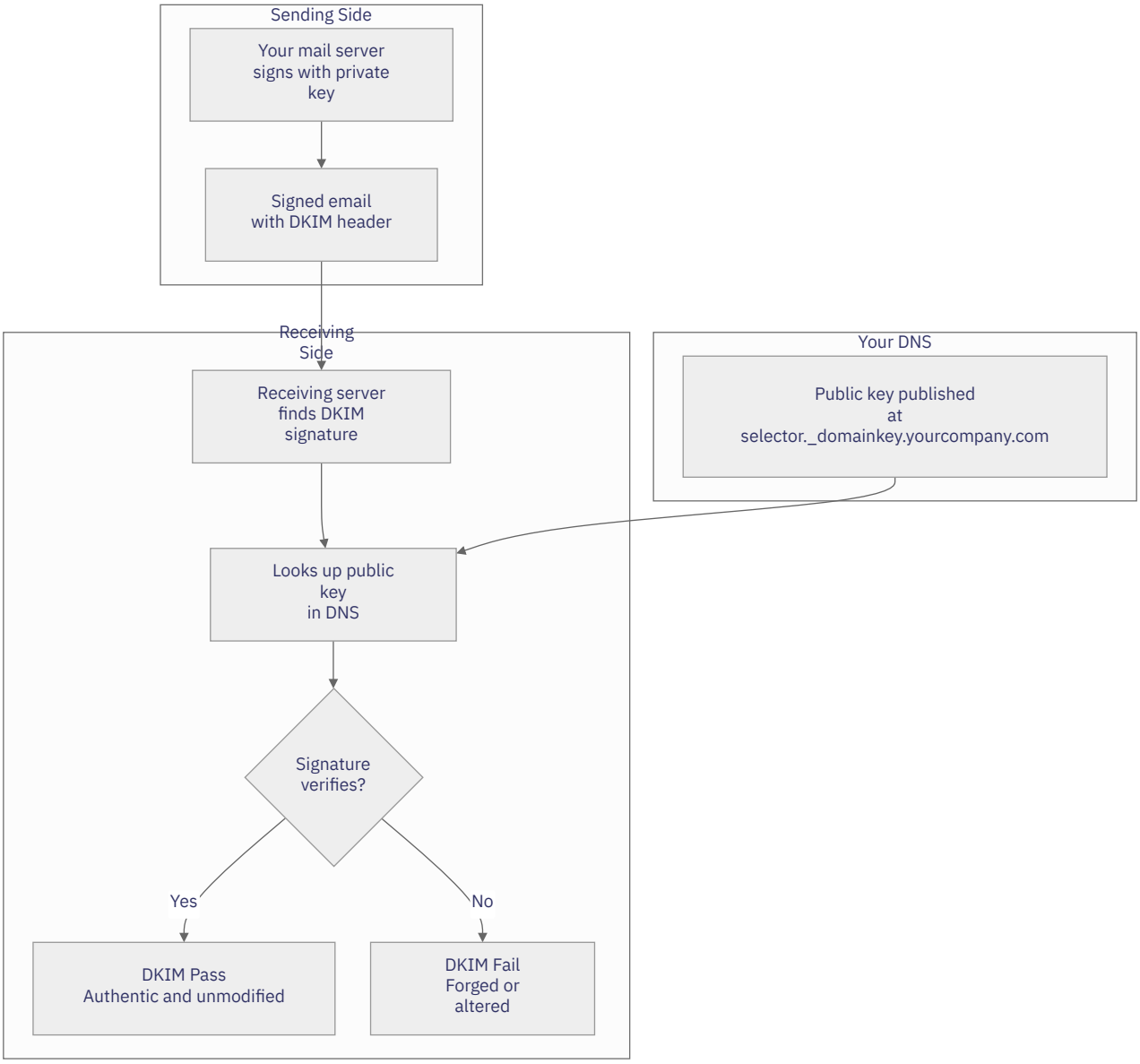
```
v=spf1 include:amazonses.com include:protection.outlook.com -all
```

This says: "Only these authorized services may send for this domain. Reject everything else."

DKIM: Tamper-Proof Signatures

DKIM (DomainKeys Identified Mail) works differently from SPF. Instead of checking where the email came from, it checks whether the email was signed by the domain it claims to represent — and whether that signature is still intact.

The domain owner generates a cryptographic key pair: a private key used to sign outgoing email, and a public key published in DNS. When a receiving server gets the email, it retrieves the public key and verifies the signature.



DKIM Verification Flow Diagram

DKIM proves two things: the email was sent by someone with access to the private key, and the message body has not been modified in transit.

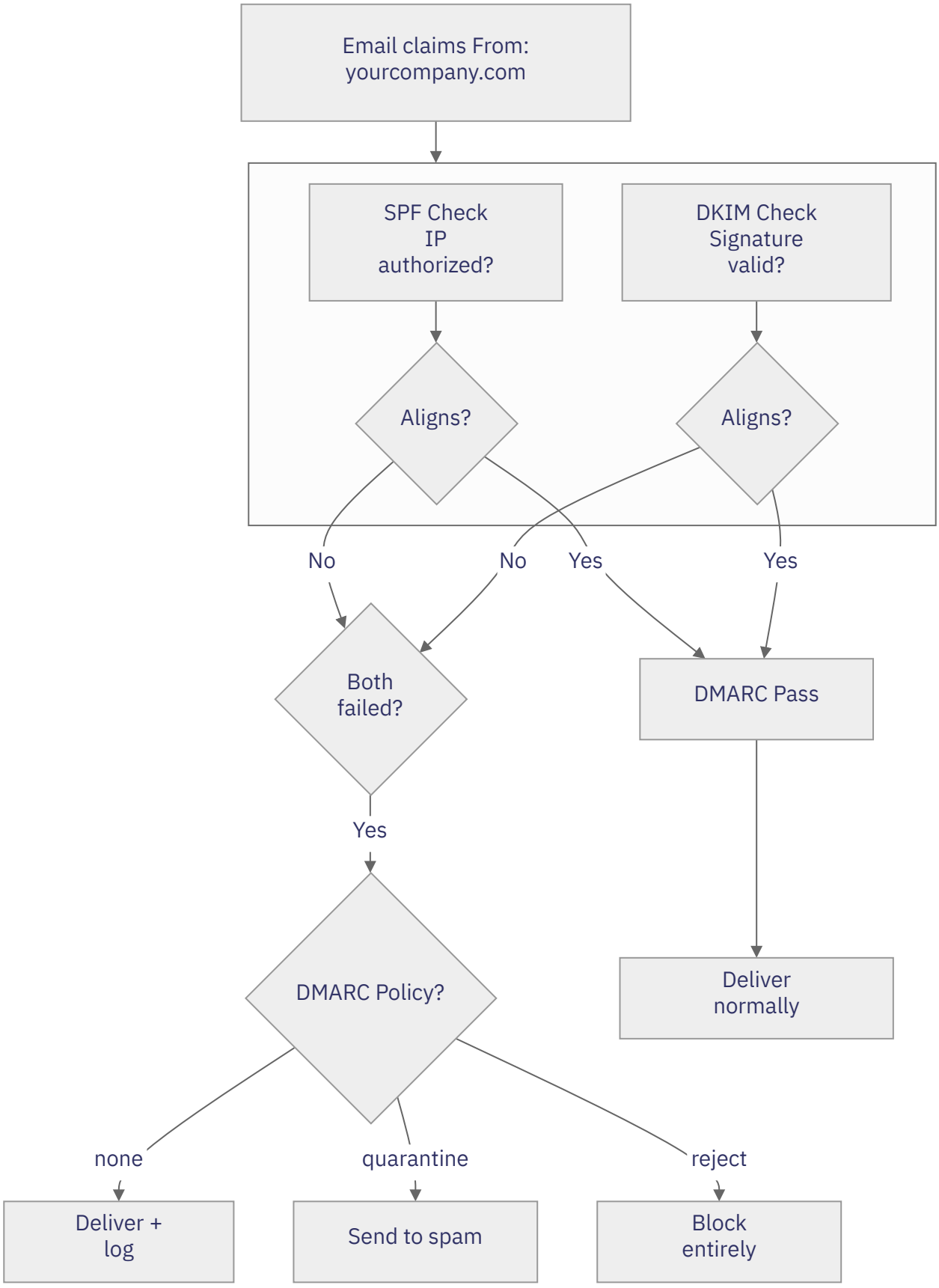
DKIM's limitation: Passing DKIM only means the signing domain is verified — which might be a third-party delivery service rather than `yourcompany.com`. This is the gap that DMARC closes.

DMARC: Alignment, Policy, and Reporting

DMARC (Domain-based Message Authentication, Reporting, and Conformance) solves the limitations of SPF and DKIM by adding two critical requirements:

1. **Alignment** — At least one of SPF or DKIM must authenticate a domain that matches the visible `From:` address. Not just any domain — that specific domain.
2. **Policy** — The domain owner declares what to do with email that fails: `none` (monitor only), `quarantine` (send to spam), or `reject` (block entirely).

This is why third-party service abuse fails when DMARC is configured correctly. The cloud provider passes SPF and DKIM — but for their own domain, not yours. DMARC alignment check fails. The `reject` policy is enforced.



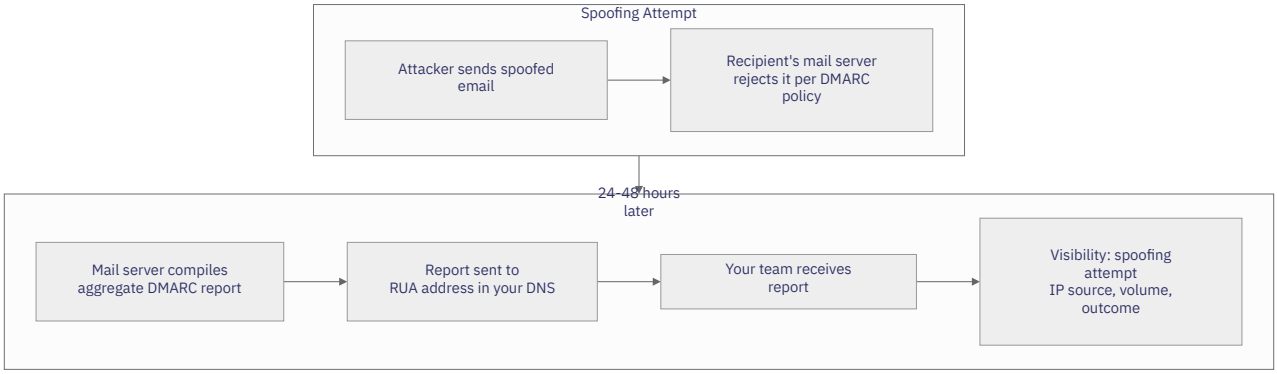
DMARC Alignment Check Diagram

DMARC also enables reporting. Receiving mail servers send aggregate reports back to the domain owner — showing every email that passed or failed DMARC, which servers sent it, and from which IP addresses. This is how a domain owner can see spoofing attempts even when the `reject` policy stops them from reaching anyone.

The DMARC Reporting Loop

When email fails DMARC and gets rejected, the domain owner — the organization whose name was spoofed — does not automatically know it happened. The email is silently blocked at the receiving end.

The mechanism for visibility is **DMARC aggregate reports (RUA)**. Receiving mail servers — Google, Microsoft, and others — compile daily summaries of all email they received claiming to be from your domain, including pass/fail results, and send those reports to an address specified in your DMARC record.



DMARC Reporting Loop Diagram

Without RUA configured: The domain owner never knows spoofing attempts are happening.

With RUA monitoring: Reports arrive daily and are parsed automatically. A new IP source appearing in reports, or a spike in DMARC failures, is a visible signal that active spoofing is underway.

These reports cover a date range and arrive after the fact — typically 24 to 48 hours after the period they cover. They are an audit trail, not a real-time alert. Real-time alerting requires a separate monitoring layer on top.

TLS Reporting: The Other Report Stream

Alongside DMARC aggregate reports, Periodic collects a second type: **TLS-RPT reports** (defined in RFC 8460). Where DMARC reports cover authentication — who is claiming to send as your domain — TLS-RPT reports cover encryption: whether mail servers delivering to your domain can establish a secure TLS connection successfully.

When a sending mail server attempts delivery to your domain and encounters a TLS problem — a certificate mismatch, a failed DANE validation, an MTA-STS policy violation, or a downgrade to unencrypted delivery — it logs the failure and sends a report to the address published in your `_smtp._tls` DNS record. Periodic collects and parses these.

A healthy domain shows near-zero TLS failures. When failures do appear, they fall into a few categories:

Certificate issues. The mail server's TLS certificate doesn't match what's expected — expired, wrong domain, or signed by an untrusted authority. If this appears on your own receiving infrastructure, it needs fixing. If it appears on third-party infrastructure delivering to you, it's their problem, but worth flagging to the sender.

DANE validation failures. If your domain publishes TLSA records (DANE), sending servers check that the certificate presented during delivery matches the hash in DNS. A mismatch — from a certificate renewal that wasn't reflected in DNS, for example — blocks delivery from DANE-validating senders. This is one of the most operationally important things TLS-RPT catches, because DANE failures are silent from the sender's perspective without reporting.

Policy failures. If your domain has an MTA-STS policy published, senders enforcing that policy will refuse to deliver over a connection that doesn't meet it. TLS-RPT shows when and where those enforcements are triggering.

DMARC protects your domain's identity — stopping spoofing. TLS-RPT protects your domain's mail channel — ensuring email in transit is encrypted and authenticated at the transport layer. Both arrive as daily reports that Periodic parses into a readable summary.

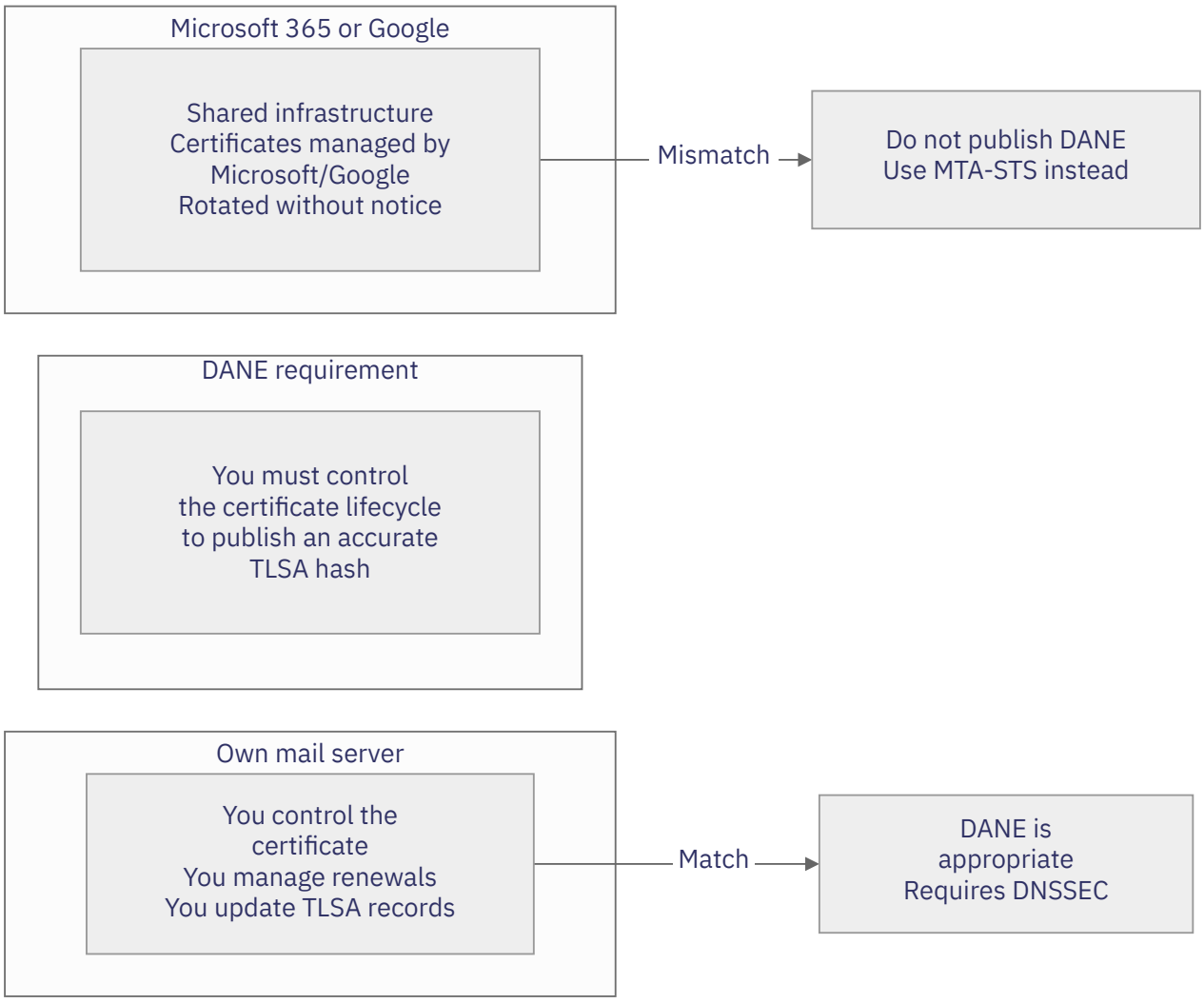
DANE and DNSSEC: Transport-Layer Hardening

DANE: Not for Most Organizations

DANE (DNS-based Authentication of Named Entities) lets a domain publish the hash of its mail server's TLS certificate directly in DNS as a TLSA record. When a DANE-validating sender delivers email, it checks that the certificate the server presents matches the hash on record — a hard cryptographic binding that goes beyond trusting any certificate signed by any commercial Certificate Authority.

It sounds compelling. For most organizations, it is not the right tool.

The reason is straightforward: DANE requires you to control the certificate on your mail server. If your inbound mail runs on Microsoft 365 or Google Workspace — which is true for the overwhelming majority of organizations — you do not control those certificates. Microsoft and Google manage them on shared infrastructure and rotate them without notice. Publishing a TLSA hash for a certificate you don't control means the hash will go stale on the next rotation, and DANE-validating senders will fail to deliver to you. The cure becomes the problem.



DANE Applicability Decision Diagram

DANE is appropriate when an organization runs its own mail server infrastructure — an on-premises MX, or a hosted MX where they manage the certificate directly. That scenario applies to a small fraction

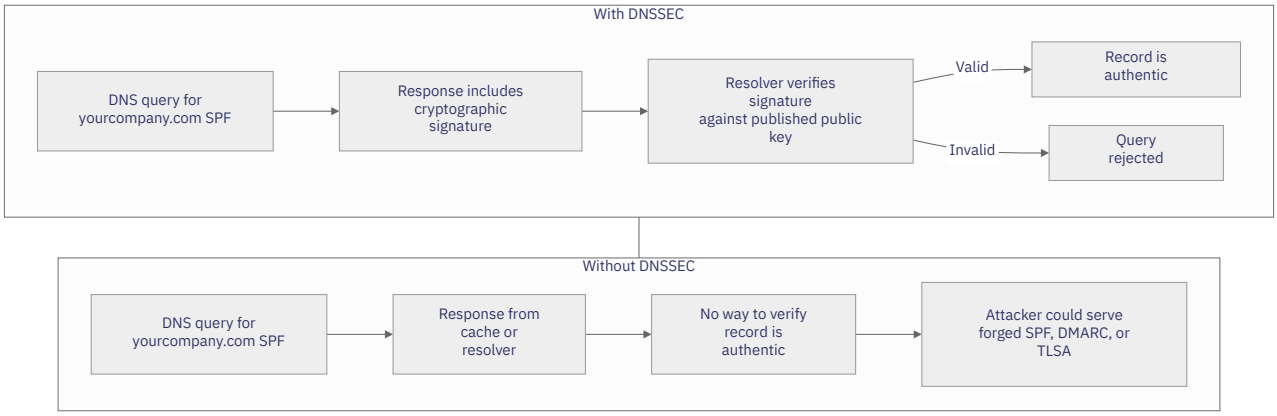
of organizations today, predominantly in sectors with the most stringent security requirements: government, academic institutions, financial infrastructure, and security-conscious technology companies.

For everyone on M365 or Google Workspace, **MTA-STS** is the right mechanism for enforcing inbound TLS. It publishes a policy file over HTTPS stating that your domain requires TLS for delivery, and senders enforcing MTA-STS will refuse to deliver over an unencrypted connection. No certificate hash pinning required.

DNSSEC: Protecting the DNS Records Themselves

Every email authentication mechanism described in this guide — SPF, DKIM, DMARC, TLS-RPT, MTA-STS, and DANE if applicable — is published as DNS records. That creates a dependency: if those records can be tampered with in transit, the protections they provide can be undermined.

DNSSEC addresses this directly. It adds cryptographic signatures to DNS records, so that resolvers can verify a record is authentic and has not been modified between the authoritative server and the query. Without DNSSEC, an attacker capable of DNS cache poisoning or a BGP route hijack could theoretically serve forged DNS responses — replacing your SPF record to authorize their own servers, or substituting a `none` DMARC policy for your `reject` one.



DNSSEC Comparison Diagram

For email security specifically, DNSSEC matters on two levels. For all domains, it protects SPF, DKIM selector, and DMARC records from being forged. For domains publishing DANE, it is a hard prerequisite — DANE validators will not act on TLSA records from an unsigned zone, because an unsigned TLSA record offers no stronger guarantee than the records it is trying to replace.

Operational considerations. DNSSEC requires support from both the DNS registrar (to publish DS records to the parent zone) and the DNS provider (to sign zone records). For `.co.jp` domains through registrars like JPDirect, this is supported. For `.com` and most other TLDs, registrar support is now widespread. The operational complexity is real: DNSSEC key rollovers require careful timing, and a misconfigured DNSSEC deployment can make an entire domain unreachable rather than just degraded. Monitoring tools — including Periodic — watch for DNSSEC validation errors as part of DNS health checks.

DNSSEC is worth enabling for any domain where email authentication records are critical assets. It does not replace SPF, DKIM, or DMARC — it protects them.

Reading the Numbers: What a 1% Failure Rate Means

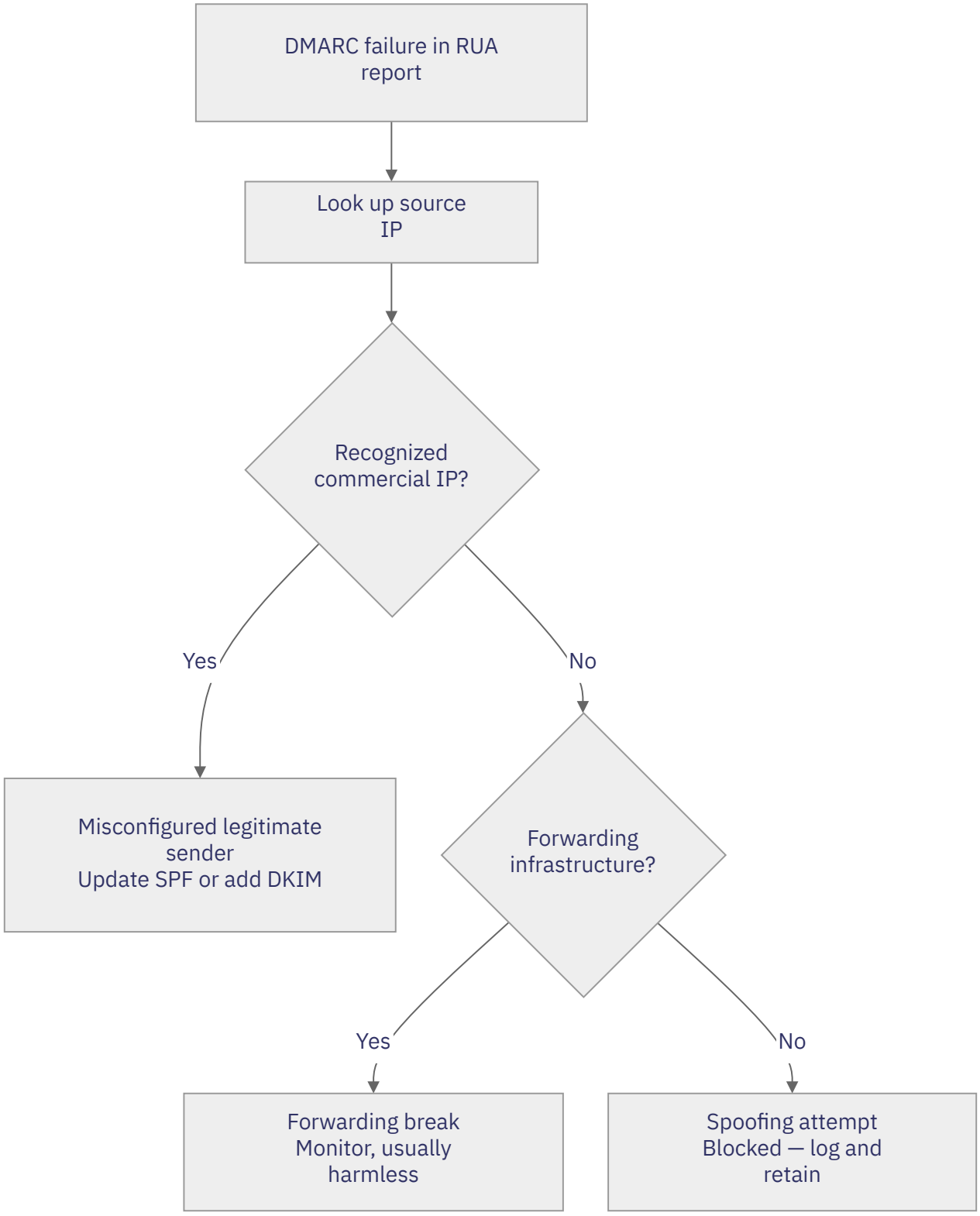
A well-configured domain monitored in Periodic typically shows a pass rate of 99–100%. Whether the remaining 1% warrants action depends entirely on which emails are failing.

Looking at the source IP of each failure row separates them into three distinct categories.

Legitimate but misconfigured senders. A SaaS platform that someone connected to your domain without updating the SPF record or configuring DKIM signing. The range of tools that send email on behalf of a company domain is wider than most IT teams realize. Business card scanning and contact management services like Sansan send connection notifications and meeting requests. CRM and sales platforms like Salesforce send deal updates, automated follow-ups, and customer-facing emails. Internal business systems — such as eSolia PROdb for operations management, or SecureNavi for security training and compliance workflows — send notifications, reports, and reminders to staff. Each of these platforms sends from its own mail infrastructure, and unless your SPF record lists them or DKIM signing is configured on the platform, every email they send will fail DMARC alignment. These failures show up as recognizable commercial IP ranges in the report. They represent a configuration gap, not an attack — but they underscore why maintaining a current sender inventory matters.

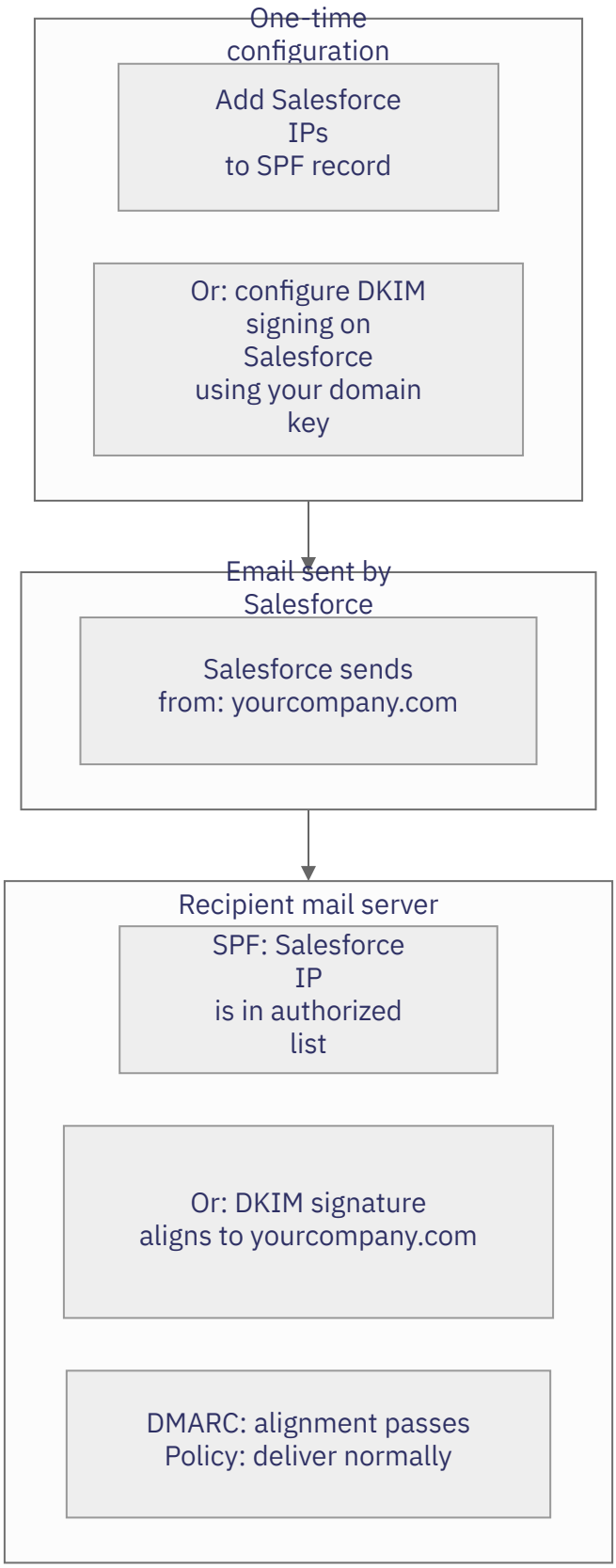
Forwarding. When email is forwarded through a third-party system — an alumni address, a partner's mail relay, a personal catch-all — SPF breaks because the forwarding server's IP is not on the authorized list. DKIM usually survives forwarding intact, so these often still pass DMARC overall through DKIM alignment. If they appear as full failures, the forwarding service is likely stripping DKIM signatures as well. Forwarding-related failures are common and generally harmless, but worth understanding so they don't obscure real signals.

Spoofing attempts. Failures from unfamiliar IP ranges — cloud infrastructure, known spam networks, residential proxies — indicate someone tried to send email claiming to be your domain. With a `reject` policy in place, none of those emails reached anyone. From a security perspective, this is the system working correctly. From an audit perspective, each instance is logged evidence of an attempted attack on your domain's identity.



DMARC Failure Triage Diagram

When a third-party platform is correctly configured, two things are in place before a single email is sent: the platform's sending IPs are listed in the domain's SPF record, or the platform is configured to sign outgoing email with a DKIM key tied to your domain. Either path produces DMARC alignment.



Third-Party Platform Configuration Diagram

Without either step, Salesforce's IPs are not authorized, its DKIM signature aligns to `salesforce.com` not your domain, and DMARC fails. The email either lands in spam or is rejected outright — silently, from the sender's perspective.

The right starting point is a sender inventory: a maintained list of every platform authorized to send email using your domain, with confirmation that each one is correctly listed in SPF or has DKIM signing active. This is not a one-time exercise. Staff add tools, vendors change their sending infrastructure, and marketing campaigns spin up new platforms. An inventory reviewed quarterly — and cross-checked against what Periodic sees in the RUA reports — is the difference between a configuration gap that gets caught early and one that quietly causes delivery failures for months. **If any team in your organization starts using a new third-party application that sends email on your behalf, contact eSolia before it goes live.** Adding the service to SPF or configuring DKIM signing takes minutes; diagnosing why legitimate email is failing DMARC weeks later does not.

The one scenario that warrants immediate attention: a recognized legitimate sending service appearing in the failure rows that your team didn't know was configured. This means someone in the organization connected a new tool to your domain — a marketing campaign, a new helpdesk, an automated notification system — without going through the proper configuration process. The service is sending real email, that email is failing DMARC, and depending on the recipient's mail server, some of it may be getting quarantined or rejected. Track down which tool, notify eSolia to get it authorized, and put controls in place to prevent undocumented sender additions in future.

Real-World Attack Patterns and How Protection Stops Each One

Pattern 1: Executive Impersonation (BEC)

Without protection: An attacker sends email appearing to be from your CFO, instructing finance staff to wire funds. The address is identical to the real CFO's. The email delivers and looks authentic.

With DMARC reject: The receiving server checks alignment. The attacker's sending infrastructure is not authorized by the CFO domain's DMARC policy. Email blocked before delivery.

Pattern 2: Vishing — Fake Voicemail Notification

The attack: An attacker uses a reputable cloud email platform to send a "missed voicemail" phishing email, with a subject line such as "Caller left VM — 3:45 sec duration." The format is immediately familiar, creates a sense of urgency, and prompts the recipient to click a link to retrieve the supposed message. The cloud platform passes SPF and DKIM for its own domain. Without DMARC, the email delivers cleanly under the spoofed company name.

With DMARC reject: DMARC alignment fails — SPF and DKIM authenticated the delivery platform, not the claimed sender domain. The email is rejected before it reaches the recipient.

Rejection as evidence: When a `reject` policy fires, the receiving server typically generates a Non-Delivery Report (NDR) back toward the apparent envelope sender. If the attacker used the victim organization's address as the return path, that NDR lands in their inbox — inadvertently revealing that spoofing was attempted, even though it failed. The failed attack becomes its own evidence.

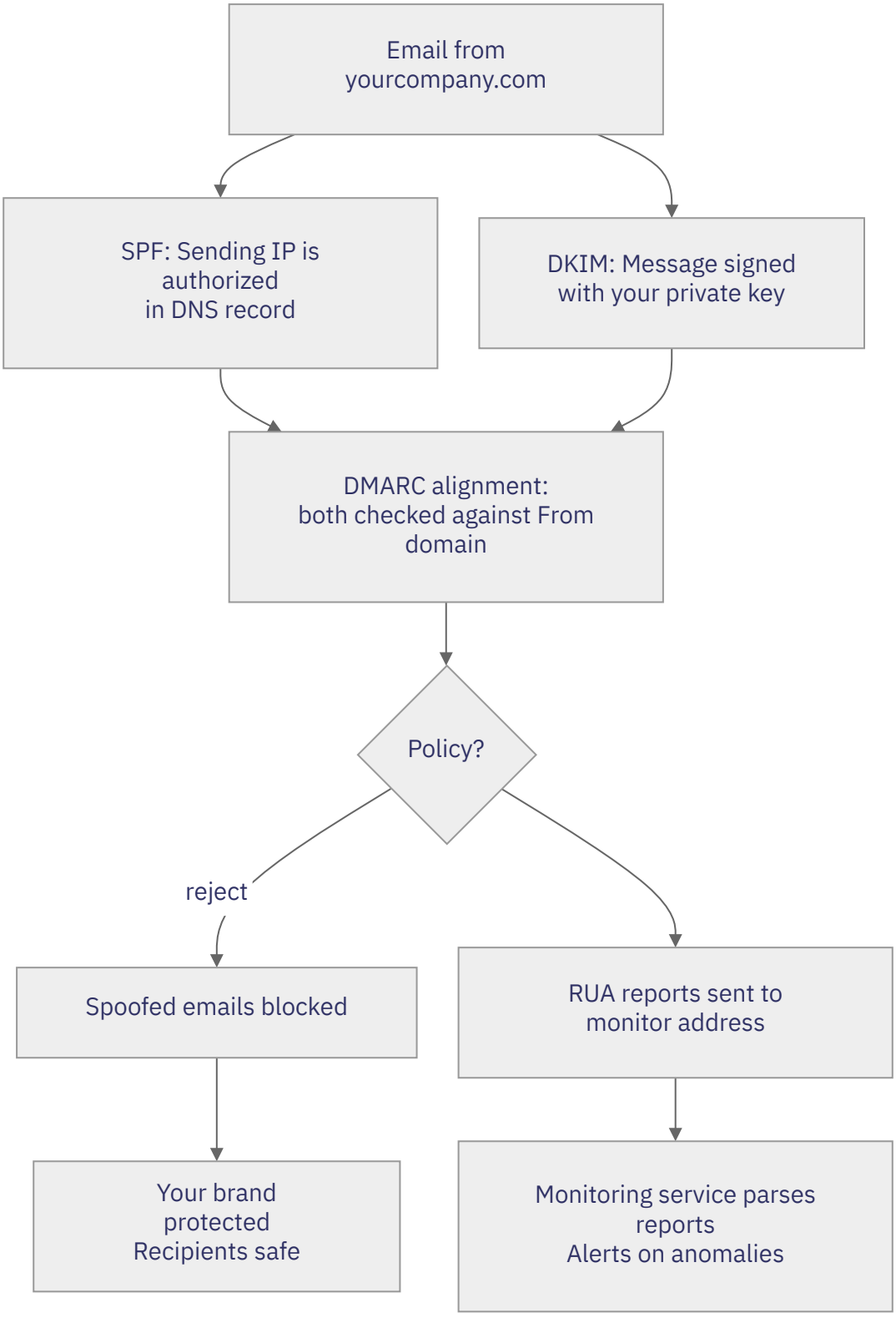
Pattern 3: Credential Harvesting via Lookalike Domain

The attack: An attacker registers `yourcompany-login.com`, builds a convincing login page mirroring your real site, configures valid SPF and DKIM for the lookalike, and sends phishing email from it. DMARC for the lookalike domain passes — it authenticates to the lookalike, not your real domain. Recipients may not notice the slight difference in the address bar.

With domain monitoring: The lookalike is detected during permutation scanning — when it first resolves (has DNS records pointing somewhere) or when a TLS certificate is issued for it (visible in Certificate Transparency logs). Evidence is collected automatically: screenshot, DNS records, registrar data. Monitoring begins from the moment the domain appears, before any recipients are targeted.

What a Protected Domain Looks Like

A well-configured domain has all three layers working together, with DMARC at `reject`:



Protected Domain Overview Diagram

SPF record: Lists every authorized sending service — your mail provider, CRM, ticketing system, marketing platform. Anything not listed is unauthorized.

DKIM: At least 2048-bit RSA keys, rotated periodically. Separate selectors for different sending services allow independent key management.

DMARC at `reject`: The destination for a mature, confident configuration. Getting there often requires a period at `none` or `quarantine` first, to confirm all legitimate sending services are properly authenticated before tightening the policy.

RUA reports: Directed to a monitored address or a parsing service, so the organization has ongoing visibility into how their domain is being used across the internet.

Web Protections: The Complementary Layer

Email authentication protects against spoofed email. A complementary layer protects the organization's web presence from unauthorized access attempts — the kind of probing that precedes many attacks.

A web application firewall (WAF) inspects incoming HTTP traffic and applies rules to block known attack patterns: SQL injection attempts, credential stuffing, bot traffic, and vulnerability scanning.

The volumes involved are larger than most organizations expect. Much of this traffic is automated scanning — bots probing every IP address on the internet looking for vulnerable services. Blocking it is routine, but the scale illustrates that internet-facing systems are under constant automated pressure. Unprotected systems absorb that exposure silently, with no visibility into what is being attempted.

A layered approach — email authentication, WAF rules, and domain monitoring — addresses different parts of the attack surface.

Staying Current: Configuration Drift Is the Real Risk

A protected domain is not a set-and-forget state. Configurations drift. New sending services get added without SPF updates. DKIM keys expire. Policies soften during mail migrations and don't get restored afterward.

Continuous monitoring covers four areas: DNS record changes (any modification to SPF, DKIM, or DMARC outside a maintenance window is anomalous by definition), DMARC aggregate report analysis (daily reports from major receivers show every server claiming to send as your domain), lookalike domain scanning (permutation-based checks that detect brand-abuse registrations before they target anyone), and dead man's switch validation (an external pulse check confirming the monitoring system itself hasn't failed silently).

Summary: The Layers at a Glance

Layer	What it does	What it stops
SPF	Authorizes specific sending IPs for a domain	Unauthorized servers sending on your behalf
DKIM	Cryptographic signature proving message origin and integrity	Message tampering; unauthorized signing
DMARC	Aligns SPF/DKIM to the visible From address; sets policy	Spoofed From addresses; unaligned third-party abuse
DMARC reporting (RUA)	Aggregate visibility into how your domain is being used	Invisible spoofing campaigns
WAF	Filters malicious web traffic before it reaches the application	Credential stuffing, scanning, injection attacks
Domain monitoring	Detects lookalike domains and configuration drift	Brand impersonation, policy weakening
DNSSEC	Cryptographically signs DNS records so resolvers can verify authenticity	Forged SPF, DKIM, DMARC, and TLSA records served via cache poisoning or BGP hijack
DANE	Pins a mail server's TLS certificate hash in DNS (own infrastructure only — not applicable to M365 or Google Workspace)	Certificate substitution during SMTP delivery

These protections need to be in place before an attack, not after. A `reject` policy configured the day after a successful phishing campaign is the right response — but it does not undo what already happened.

Contact Us

eSolia Inc. Shiodome City Center 5F (Workstyling) 1-5-2 Higashi-Shimbashi, Minato-ku Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	hello@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST

メールセキュリティの攻撃と対策：悪用される脆弱性と防御の仕組み

2026 年 3 月 9 日

目次

メール認証の基礎ガイド：SPF・DKIM・DMARC の仕組みと、設定が不十分な場合に何が起きるか。

身に覚えのない電話

取引先の受信トレイに、自社名を騙ったメールが届く。差出人アドレスは正規のものと見分けがつかない。件名には「ボイスメールが届いています」とある。受信者はリンクをクリックし、認証情報を入力し、攻撃者にアカウントへのアクセス権を渡してしまう。

そのメールは、自社の誰も送っていない。ドメインが無断で使われたのだ。適切な対策が講じられていなければ、これを防ぐ手段はない。

このガイドでは、保護されていないメールドメインが攻撃者にどう悪用されるか、技術的な防御の仕組み、そしてそれが正しく機能したときに何が起きるかを説明する。実際の攻撃パターンをもとに、対策の有無がどれほどの差を生むかを示す。

メールの設計上の欠陥

メールは 1970 年代、少数の信頼された研究者のネットワーク向けに設計された。当初の設計には、現在まで修正されていない根本的な欠陥がある。**誰でも誰かのふりができる**、ということだ。

メールを送信するとき、「From」アドレスはただのラベルにすぎない。送信者が実際にそのドメインを管理しているかどうかを、元のプロトコルは確認しない。任意の差出人住所を書いた手紙を郵便で送るようなもので、郵便局にはそれが本物かどうかを確かめる方法がない。

だからこそ、攻撃者は `yourcompany.com` や銀行、さらには政府機関を装ったメールを送れる。受信者の画面に表示されるアドレスは、主張にすぎず、検証された身元ではない。

この欠陥を補うために開発されたのが、SPF・DKIM・DMARC の 3 つの技術だ。これらを組み合わせることで、メールが実際に発信元として主張するドメインから送られたことを証明できる。

対策なしに何が起きるか

ドメインに保護がない場合、攻撃者が取る主なアプローチは 3 つある。

パターン 1：ドメイン直接なりすまし

攻撃者が `you@yourcompany.com` を名乗るメールを送る。SPF も DKIM もなければ、受信メールサーバーにはそれを拒否する根拠がない。メールは完全に正規のものに見える形で受信トレイに届く。

ドメイン直接なりすまし図

保護のないドメインは、役員なりすましによる振込詐欺、偽のログインページへの誘導、社内 IT 部門を装ったマルウェア添付などの入口になる。

パターン 2：類似ドメイン攻撃

攻撃者が `yourcompany-jp.com`、`yourcompny.com`、あるいはラテン文字と見た目が同じ Unicode 文字を使ったドメインを取得する。自分のドメインには正規の SPF と DKIM を設定するため、認証は通過する——ただし、認証されるのは偽ドメインだ。

パターン 3：正規サービスの悪用

攻撃者は、大手クラウドプロバイダーのメール配信サービスなど、信頼性の高い正規サービスをフィッシングメールの送信に使うことが多い。これらのサービスは IP レピュテーションが高く、IP ベースのスパムフィルターを容易に通過してしまう。

よく使われる手口が**ビッシング**（音声フィッシング）だ。「ボイスメールが届いています」という通知メールを模した形式で、受信者に「メッセージを聞く」リンクをクリックさせる。見慣れた形式が警戒心を下げ、リンク先は認証情報を盗むページだ。

この種の攻撃の認証ヘッダーは次のようになる：

確認項目	結果	説明
SPF	Pass	クラウドサービスは正規送信者——ただしそのサービス自身のドメイン向けであり、主張するドメインではない
DKIM	Pass	クラウドサービスが署名——ただしそのサービス自身の鍵であり、主張するドメインの鍵ではない
DMARC	**Fail → Reject**	SPF も DKIM も `From:` ドメインとアライメントしていない

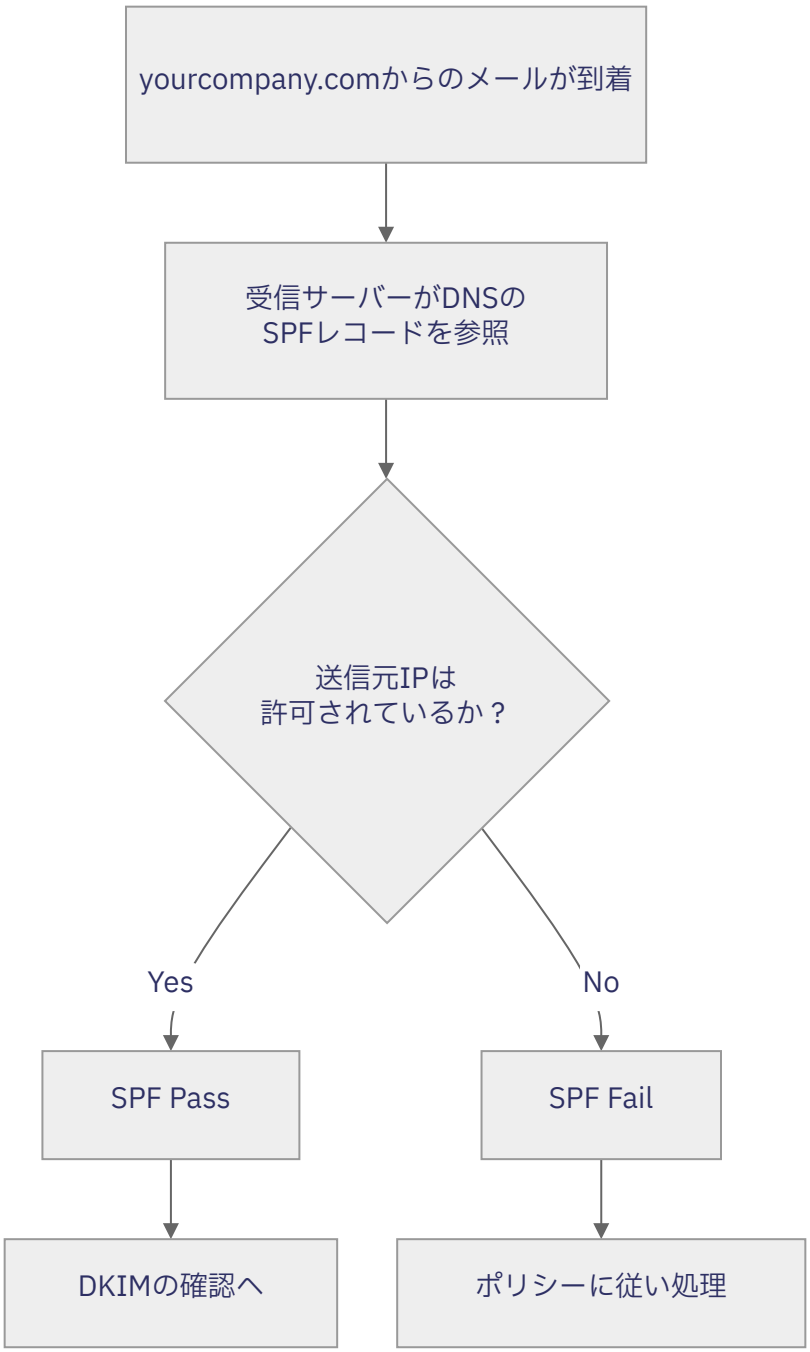
DMARC が `reject` ポリシーで設定されていれば、この攻撃は受信者に届く前に阻止される。DMARC がなければ、メールはそのまま配信される。

3 つの防御の仕組み

SPF：送信許可サーバーの定義

SPF（Sender Policy Framework）は「このドメインからメールを送信できるメールサーバーはどれか？」という問いに答える DNS レコードだ。

受信サーバーが `yourcompany.com` からのメールを受け取ると、DNS の SPF レコードを参照し、送信サーバーの IP アドレスが許可リストに含まれているか確認する。



SPF チェックフロー図

SPF の限界：SPF が確認するのはエンベロープ送信者——技術的な送信経路のアドレスであり、メールクライアントに表示される「From」アドレスではない。攻撃者は自身の送信インフラで SPF を通過させながら、From フィールドに任意のドメインを表示できる。SPF 単体では不十分だ。

SPF レコードの例：

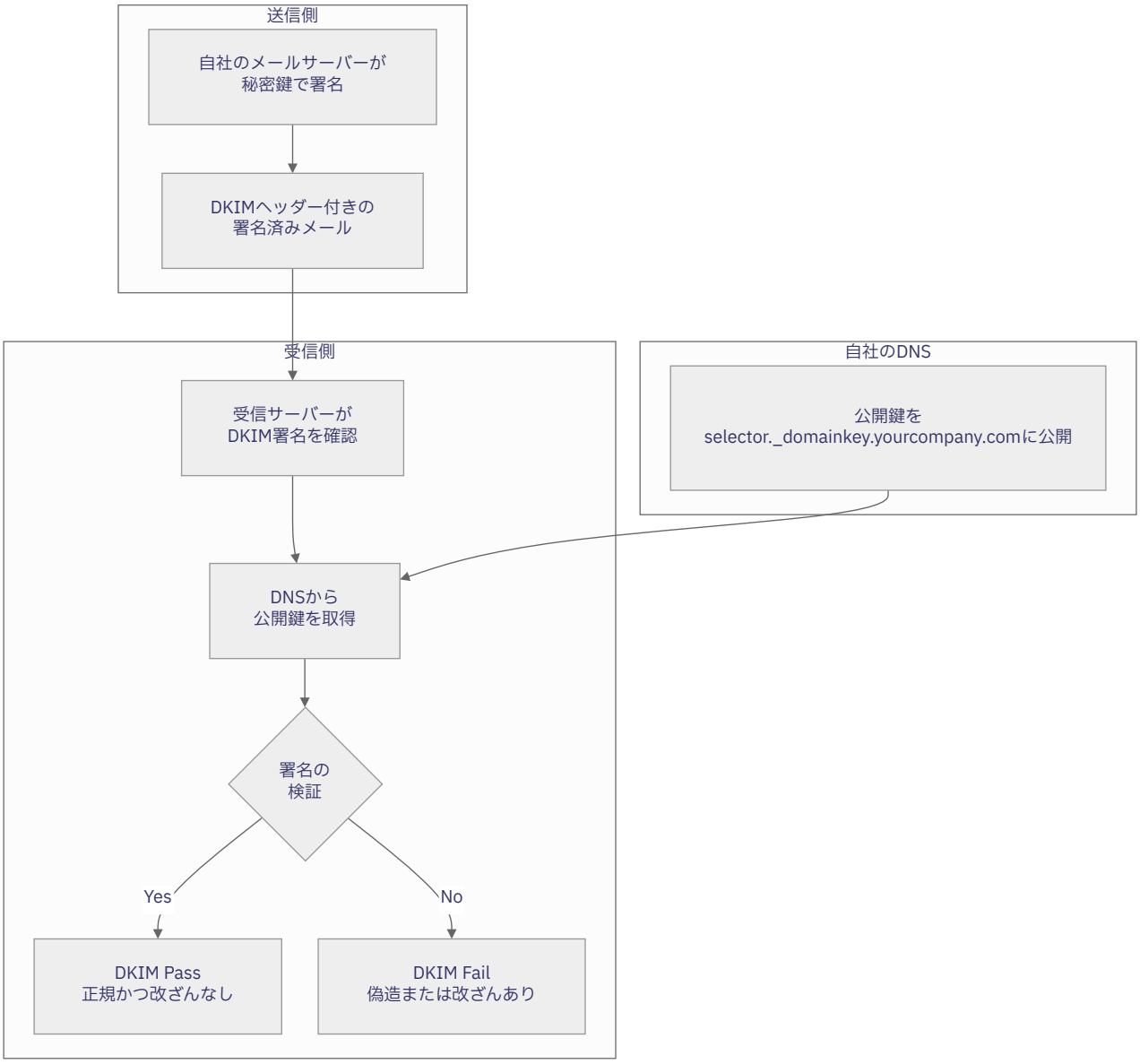
```
v=spf1 include:amazonses.com include:protection.outlook.com -all
```

「このドメインのメールを送信できるのは、これらの許可サービスのみ。それ以外は拒否。」という意味になる。

DKIM：改ざん検知のための電子署名

DKIM は SPF とは異なるアプローチを取る。メールがどこから来たかではなく、そのメールが主張するドメインによって署名されているか、そして署名が改ざんされていないかを確認する。

ドメイン所有者は暗号鍵ペアを生成する。秘密鍵は送信メールの署名に使い、公開鍵は DNS に公開する。受信サーバーはメールを受け取ると、公開鍵を取得して署名を検証する。



DKIM 検証フロー図

DKIM が証明するのは 2 つ :秘密鍵にアクセスできる者がメールを送ったこと、そして送信中にメール本文が改ざんされていないことだ。

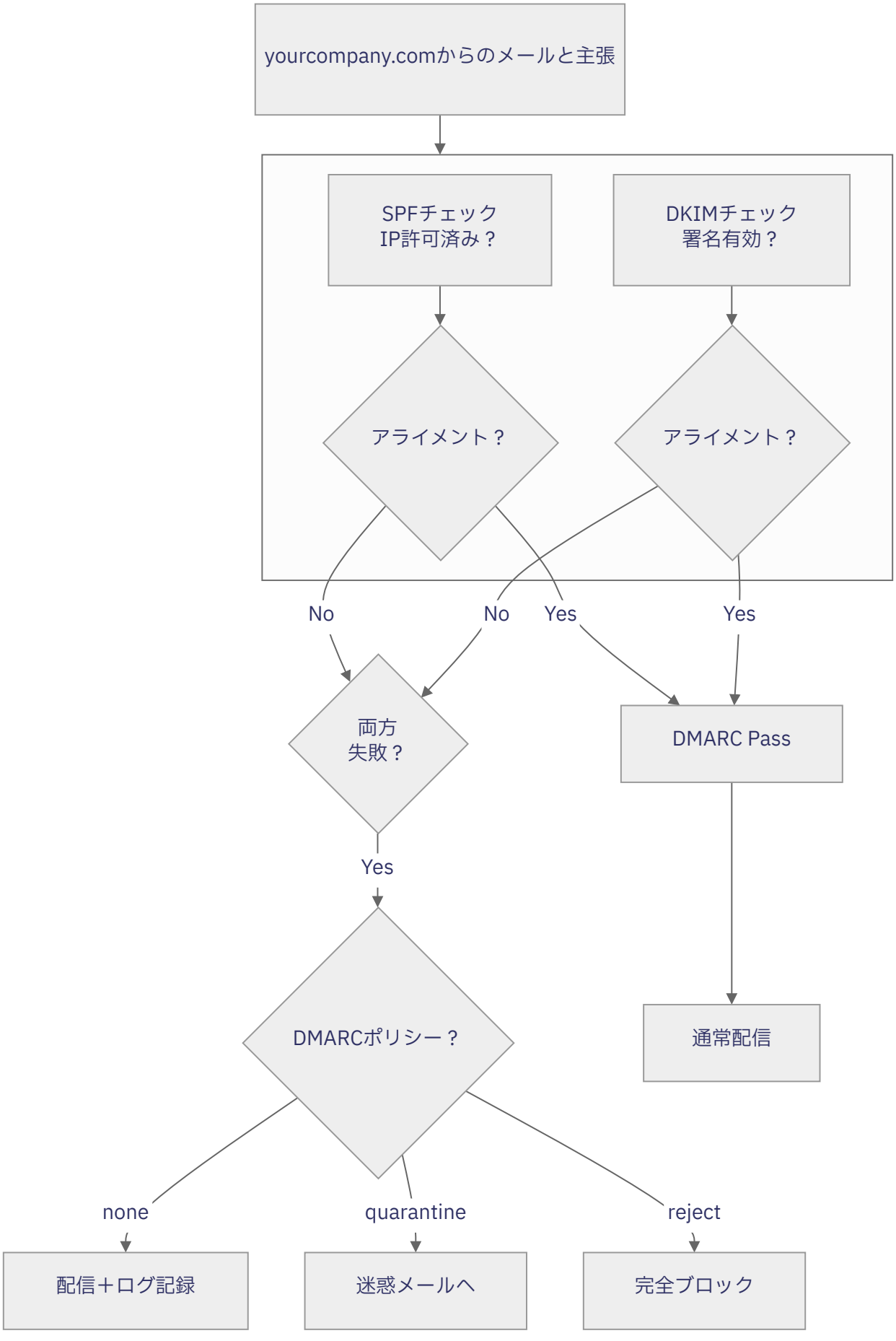
DKIM の限界： DKIM での認証は署名ドメインの正当性を証明するにすぎない。それは `yourcompany.com` ではなく、サードパーティの配信サービスのドメインである可能性がある。この穴を塞ぐのが DMARC だ。

DMARC：アライメント・ポリシー・レポーティング

DMARC（Domain-based Message Authentication, Reporting, and Conformance）は、SPF と DKIM の限界を補う 2 つの要件を加える：

1. **アライメント** — SPF または DKIM のいずれかが、表示される `From:` アドレスのドメインと一致するドメインを認証していること。どのドメインでもなく、そのドメインでなければならない。
2. **ポリシー** — ドメイン所有者が失敗時の処理を宣言する：`none`（監視のみ）、`quarantine`（迷惑メールへ振り分け）、`reject`（完全にブロック）。

サードパーティサービスの悪用がDMARCで阻止される理由がこれだ。クラウドプロバイダーはSPFとDKIMを通過するが、それは自社のドメインであり、送信者が主張するドメインではない。DMARCアライメントチェックで失敗し、`reject`ポリシーが執行される。



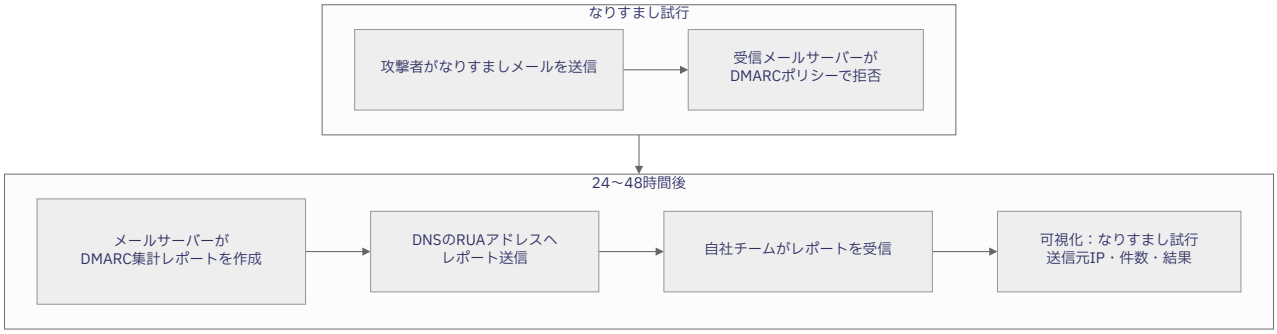
DMARC アライメントチェック図

DMARC はレポーティングも提供する。 受信メールサーバーはドメイン所有者に集計レポートを送信し、DMARC のパス・失敗、送信サーバー、IP アドレスなどを報告する。`reject` ポリシーで阻止された場合も、なりすまし試行の全貌を把握できる。

DMARC レポーティングの仕組み

DMARC によってメールが拒否されたとき、ドメイン所有者――なりすまされた組織――は自動的にそれを知ることができない。メールは受信側でサイレントにブロックされるだけだ。

可視性を確保する仕組みが **DMARC 集計レポート（RUA）** だ。Google・Microsoft などの受信メールサーバーは、自社ドメインを名乗るメールのパス・失敗結果を含む日次サマリーを集計し、DMARC レコードに指定されたアドレスに送信する。



DMARC レポーティングループ図

RUA が設定されていない場合： ドメイン所有者はなりすましが発生していることに気づかない。

RUA 監視がある場合： レポートは毎日自動で解析される。見慣れない送信元 IP の出現や DMARC 失敗件数の急増は、アクティブなスプーフィングが進行しているシグナルとなる。

レポートは対象期間分をまとめて、通常 24～48 時間後に届く。リアルタイムのアラートではなく、監査証跡だ。リアルタイム通知には、別途監視レイヤーが必要になる。

TLS レポートという第二の監視軸

Periodic が収集するのは DMARC 集計レポートだけではない。もう一種類、**TLS-RPT レポート**（RFC 8460 で定義）も収集している。DMARC レポートが認証――誰が自社ドメインを名乗っているか――を扱うのに対し、TLS-RPT レポートは暗号化を扱う：自社ドメインにメールを配信しようとするサーバーが、TLS 接続を正常に確立できているかどうかだ。

送信メールサーバーが自社ドメインへの配信を試みた際に TLS の問題が発生した場合――証明書の不一致、DANE バリデーションの失敗、MTA-STS ポリシー違反、非暗号化通信へのダウングレードなど――そのサーバーはエラーをログに記録し、DNS の `_smtp._tls` レコードに登録されたアドレスへレポートを送信する。Periodic はこれを収集・解析する。

正常なドメインでは TLS 失敗はほぼゼロだ。失敗が発生した場合、主に次の 3 種類に分類される：

証明書の問題。 メールサーバーの TLS 証明書が期待されるものと一致しない――期限切れ、ドメイン不一致、信頼されない認証局による発行など。自社の受信インフラで発生している場合は対処が必要だ。配信元の第三者インフラで発生している場合は先方の問題だが、送信元に連絡する価値はある。

DANE バリデーション失敗。 自社ドメインが TLSA レコード（DANE）を公開している場合、送信サーバーは配信時に提示された証明書のハッシュが DNS 上のものと一致するか確認する。不一致――証明書更新後に DNS が更新されていない場合など――は DANE 検証を行う送信者からの配信をブロックする。TLS-RPT が検知する中でも最も運用上重要なケースの一つだ。DANE の失敗はレポートがなければ送信者側からは見えないためだ。

ポリシー違反。 MTA-STS ポリシーを公開しているドメインの場合、そのポリシーを適用する送信者は要件を満たさない接続での配信を拒否する。TLS-RPT は、そのような適用がどこで発生しているかを可視化する。

DMARC は自社ドメインのアイデンティティを守り、なりすましを防ぐ。TLS-RPT は自社ドメインのメール経路を守り、送受信中のメールが暗号化・認証されていることを保証する。どちらも日次レポートとして Periodic が解析し、可読な形で提供する。

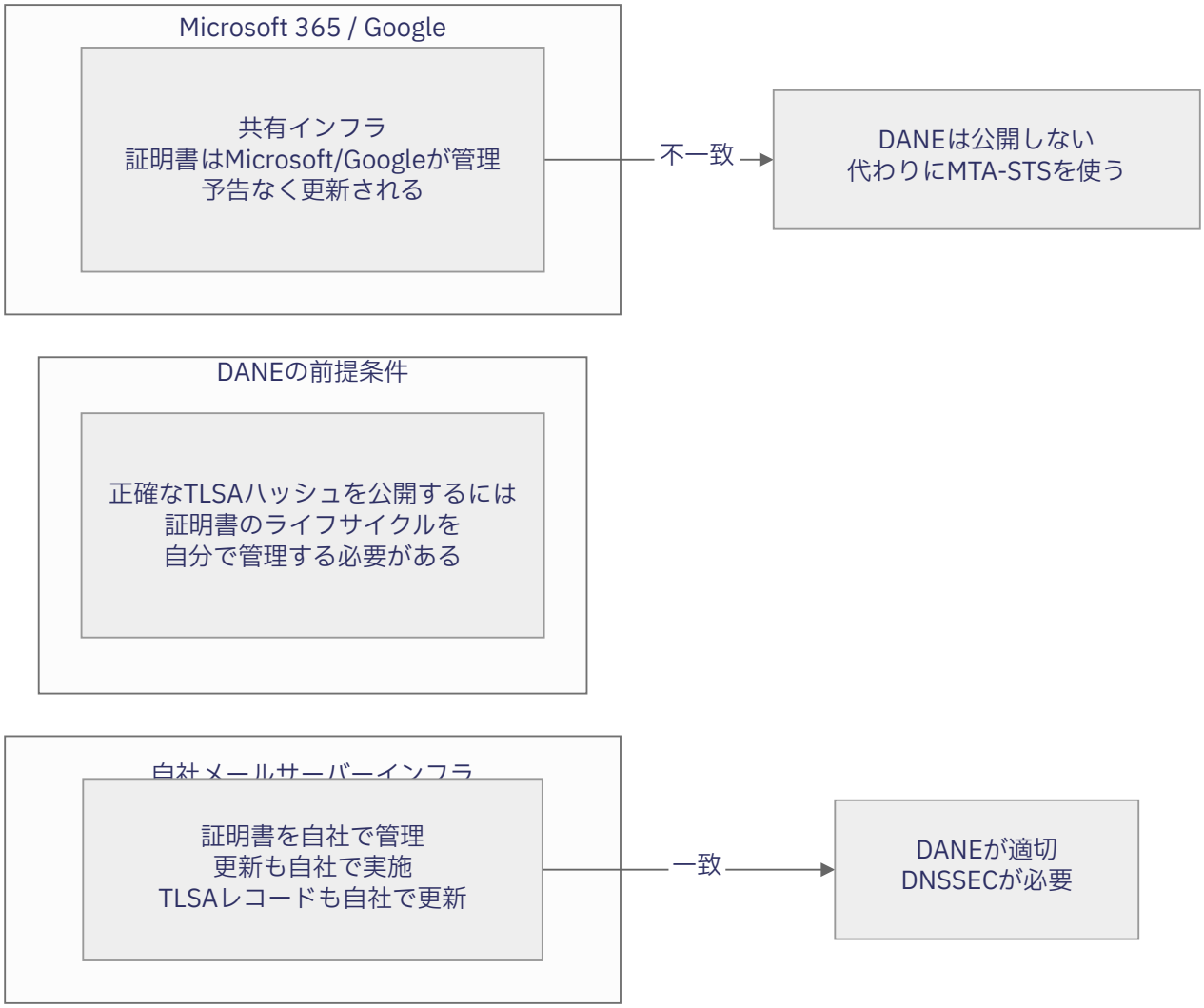
DANE と DNSSEC：トランスポート層の強化

DANE：ほとんどの組織には不要

DANE（DNS-based Authentication of Named Entities）は、メールサーバーの TLS 証明書ハッシュを TLSA レコードとして DNS に公開する仕組みだ。DANE 対応の送信サーバーは、配信時に提示された証明書が記録されたハッシュと一致するか確認する――商業認証局が署名したあらゆる証明書を信頼するのではなく、暗号的に特定の証明書に縛る、より強固な仕組みだ。

魅力的に聞こえる。しかしほとんどの組織にとって、適切なツールではない。

理由は明確だ。DANE はメールサーバーの証明書を自分でコントロールする必要がある。受信メールが Microsoft 365 または Google Workspace で運用されている場合――大多数の組織がそうだ――証明書は Microsoft や Google が管理する共有インフラ上にあり、予告なく更新される。コントロールできない証明書の TLSA ハッシュを公開することは、次の更新時にハッシュが古くなることを意味し、DANE 対応の送信者からの配信が失敗するようになる。防衛策が障害になるのだ。



DANE 適用判断図

DANE が適切なのは、自社でメールサーバーインフラを運用している場合――オンプレミスの MX、または証明書を自社で管理しているホスト型 MX だ。今日この状況に該当するのはわずかな組織に限られ、主に最も厳

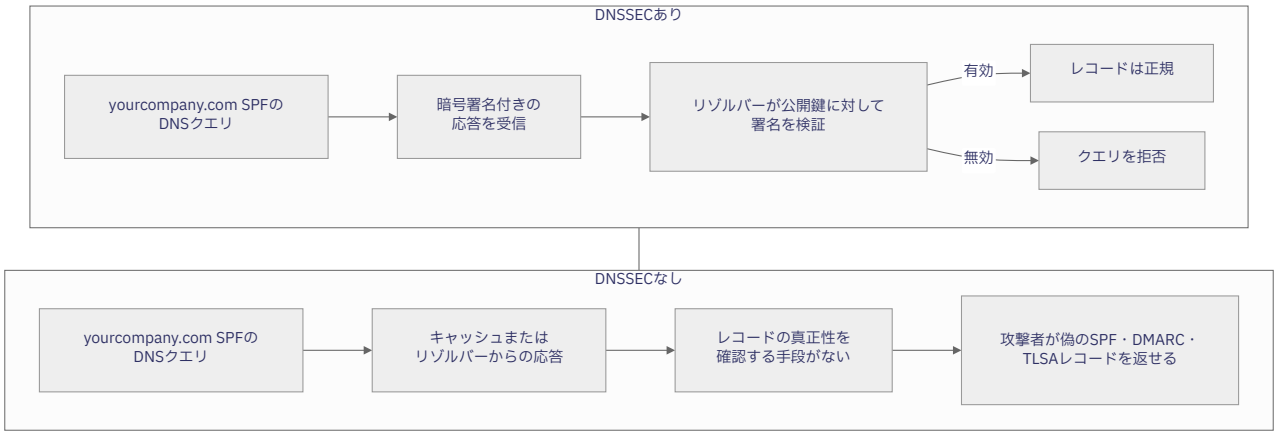
格なセキュリティ要件を持つ政府機関・学術機関・金融インフラ・セキュリティ意識の高いテクノロジー企業などだ。

M365 または Google Workspace を利用している組織には、**MTA-STS** が受信 TLS を強制する適切な仕組みだ。HTTPS 経由でドメインが TLS を要求するポリシーファイルを公開し、MTA-STS を適用する送信者は非暗号化接続での配信を拒否する。証明書ハッシュのピン留めは不要だ。

DNSSEC：DNS レコード自体を守る

このガイドで説明したすべてのメール認証の仕組み——SPF・DKIM・DMARC・TLS-RPT・MTA-STS、そして該当する場合は DANE——は DNS レコードとして公開される。つまり、これらのレコードが経路上で改ざんされた場合、それが提供する保護そのものが損なわれるという依存関係がある。

DNSSEC はこの問題に直接対処する。DNS レコードに暗号署名を付加することで、権威サーバーからクエリまでの間にレコードが改ざんされていないことをリゾルバーが検証できるようにする。DNSSEC がなければ、DNS キャッシュポイズニングや BGP ルートハイジャックが可能な攻撃者は、理論上、偽の DNS レスポンスを返すことができる——SPF レコードを書き換えて自社のサーバーを許可させたり、`reject` ポリシーを `none` に置き換えたりすることが可能になる。



DNSSEC 比較図

メールセキュリティの観点から、DNSSEC は 2 つのレベルで重要だ。すべてのドメインにおいて、SPF・DKIM セレクター・DMARC レコードの偽造を防ぐ。DANE を公開しているドメインでは、DNSSEC は絶対的な前提条件だ——署名されていないゾーンの TLSA レコードは DANE バリデーターが処理しない。署名のない TLSA レコードは、置き換えようとするレコードと同程度の保証しか提供しないためだ。

運用上の考慮点。 DNSSEC には、DNS レジストラ（親ゾーンへの DS レコード公開のため）と DNS プロバイダー（ゾーンレコードへの署名のため）の両方がサポートしている必要がある。JPDirect などのレジストラを通じた `.co.jp` ドメインはサポートされている。`.com` その他主要な TLD でも、レジストラサポートは広く普及している。運用上の複雑さは実際にある：DNSSEC の鍵ロールオーバーは慎重なタイミング管理が必要で、設定ミスはドメイン全体にアクセスできなくなる事態を招く可能性がある。Periodic を含む監視ツールは、DNS ヘルスチェックの一環として DNSSEC バリデーションエラーを監視する。

DNSSEC は、メール認証レコードが重要な資産であるすべてのドメインに対して有効化する価値がある。SPF・DKIM・DMARC を置き換えるものではなく、それらを守るものだ。

数字の読み方：失敗率 1% は問題か

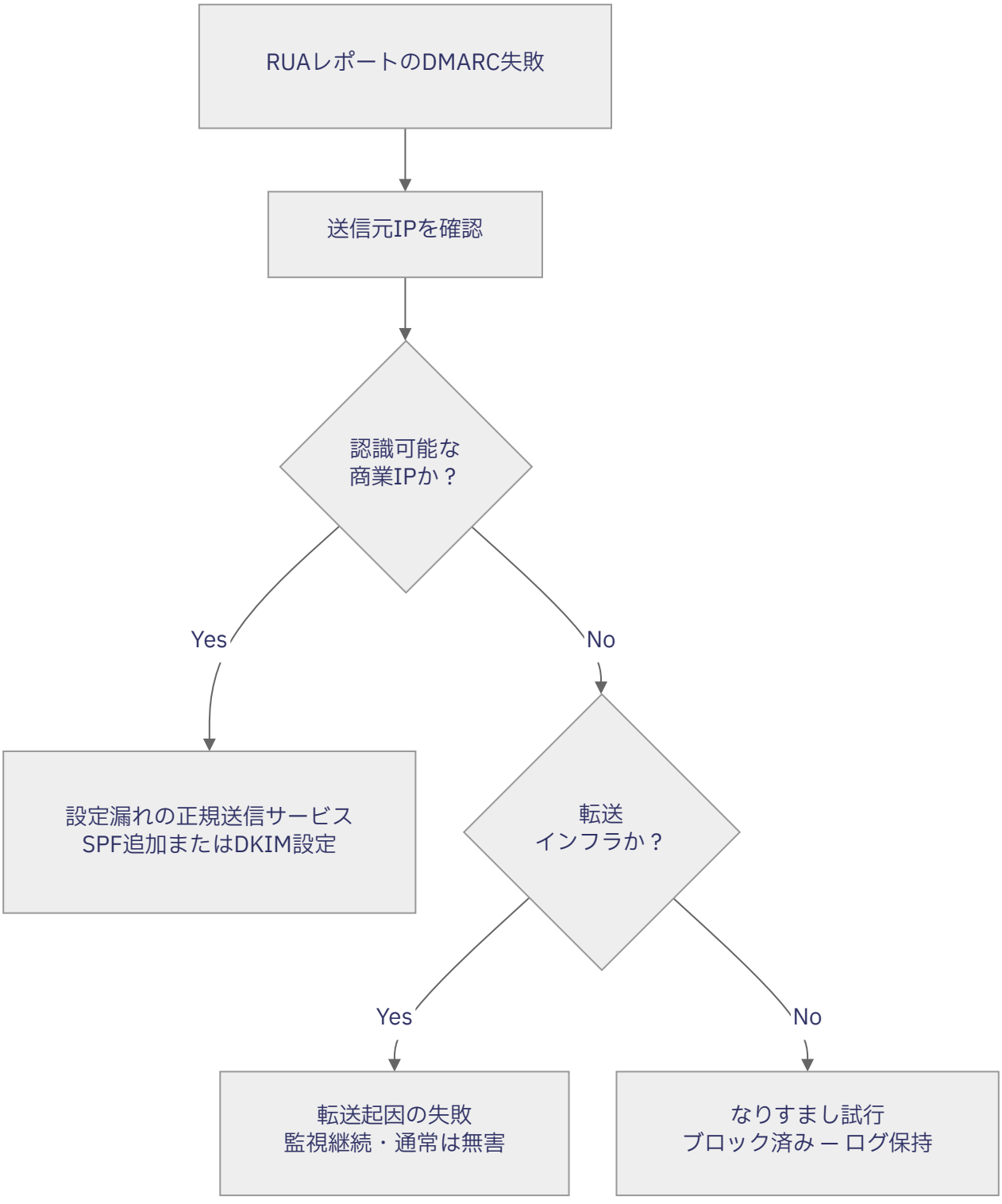
Periodic で監視している適切に設定されたドメインは、通常 99〜100% のパス率を示す。残り 1% への対応が必要かどうかは、どのメールが失敗しているかによって変わる。

失敗の送信元 IP を確認することで、3 つの類型に分類できる。

設定漏れの正規送信サービス。 SPF レコードの更新や DKIM 署名設定を行わないまま接続された SaaS プラットフォームだ。会社のドメインを使ってメールを送信するツールの範囲は、IT 担当者が想定するよりもはるかに広い。Sansan のような名刺管理・連絡先管理サービスはコネクション通知や会議リクエストを送信する。Salesforce のような CRM・営業支援プラットフォームは商談更新・自動フォローアップ・顧客向けメールを送信する。eSolia PROdb（業務管理）や SecureNavi（セキュリティ研修・コンプライアンス管理）といった社内業務システムは通知・レポート・リマインダーを送信する。これらのプラットフォームはすべて自社のメールインフラから送信しており、SPF レコードへの追加またはプラットフォーム側での DKIM 署名設定がなければ、すべてのメールが DMARC アライメントで失敗する。レポート上では認識可能な商業 IP レンジとして表示される。攻撃ではなく設定漏れだが、送信サービスの棚卸しがいかに重要かを示している。

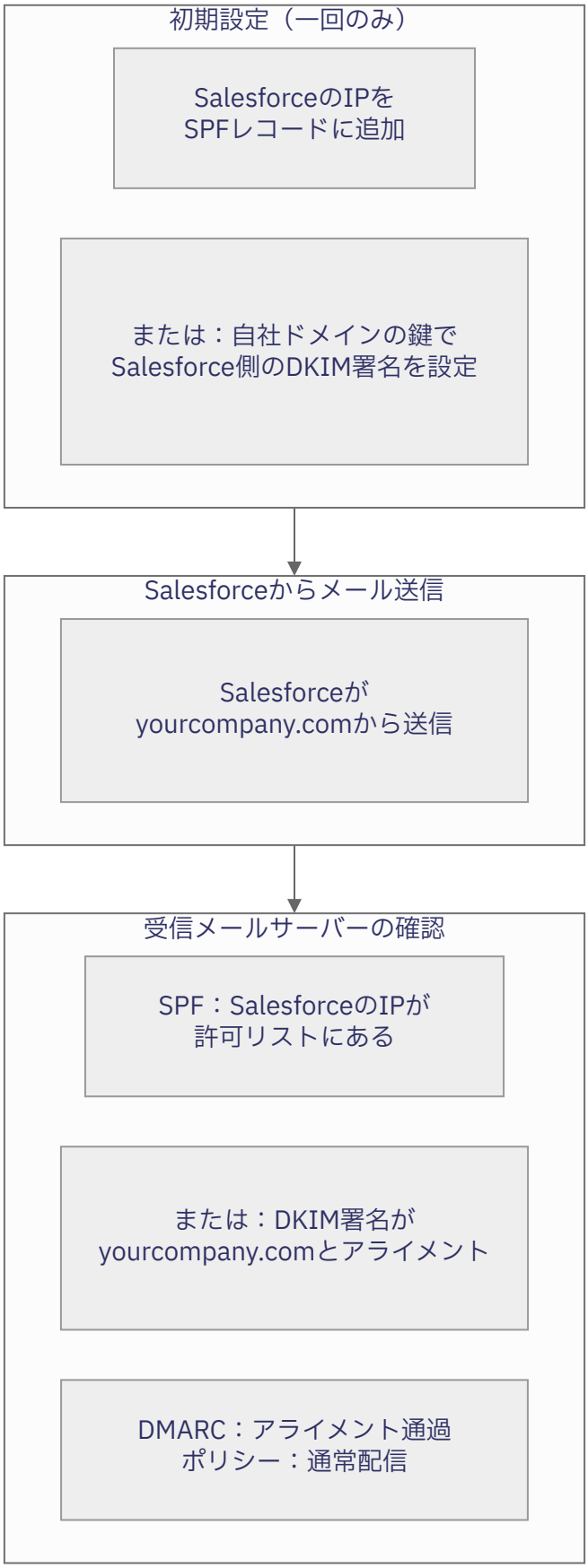
転送。 メールが第三者システム——OB 向けアドレス・パートナーのメールリレー・個人の集約アドレスなど——経由で転送される場合、転送サーバーの IP が許可リストにないため SPF が失敗する。DKIM は転送後も通常有効なため、DKIM アライメントで DMARC を通過することが多い。完全な失敗として表示されている場合、転送サービスが DKIM 署名を剥ぎ取っている可能性がある。転送に起因する失敗は一般的で通常は無害だが、本当のシグナルを埋もれさせないよう把握しておく価値がある。

なりすまし試行。 未知の IP レンジ——クラウドインフラ・既知のスパムネットワーク・住宅用プロキシ——からの失敗は、誰かが自社ドメインを名乗ってメールを送ろうとしたことを示す。`reject` ポリシーが適用されていれば、それらのメールは誰にも届いていない。セキュリティの観点からは、システムが正常に機能している証拠だ。監査の観点からは、自社ドメインのアイデンティティへの攻撃試行の記録証拠となる。



DMARC 失敗トリアージ図

サードパーティプラットフォームが正しく設定されている場合、1通のメールが送られる前に2つのことが確認されている：プラットフォームの送信 IP がドメインの SPF レコードに追加されているか、または自社ドメインの鍵を使った DKIM 署名がプラットフォーム側に設定されているか。どちらの経路でも DMARC アライメントは通過する。



サードパーティプラットフォーム設定図

どちらの設定もない場合、Salesforce の IP は許可されておらず、DKIM は `salesforce.com` に対して署名されているため自社ドメインとアライメントせず、DMARC は失敗する。メールは迷惑メールフォルダに入るか、完全に拒否される——送信側からは静かに、気づかれないまま。

送信サービスの棚卸しが出発点だ：自社ドメインを使用するすべてのプラットフォームを網羅し、それぞれが SPF に正しく追加されているか、DKIM 署名が有効かを確認した一覧を作成・維持する。これは一度限りの作業ではない。担当者がツールを追加し、ベンダーが送信インフラを変更し、マーケティングキャンペーンが新たなプラットフォームを使い始める。四半期ごとに棚卸しを見直し、Periodic が実際に RUA レポートで確認している内容と照合することで、設定漏れを早期に発見できる。**自社のどの部門でも、メール送信を行う新しいサードパーティアプリケーションの導入を検討している場合は、本番稼働前にイソリアへご連絡いただきたい。**SPF への追加または DKIM 署名の設定は数分で完了するが、数週間後に正規メールが DMARC で失敗している原因を調査するのは、そう簡単ではない。

すぐに対処が必要なケースが一つある：チームが把握していない正規の送信サービスが失敗行に現れた場合だ。これは組織内の誰かが、適切な設定プロセスを経ずに新しいツールをドメインに接続したことを意味する——マーケティングキャンペーン・新しいヘルプデスク・自動通知システムなど。そのサービスは実際のメールを送信しており、そのメールは DMARC で失敗しており、受信側のメールサーバーによっては迷惑メール扱いされているか拒否されている可能性がある。どのツールか特定し、イソリアに連絡して正規化の対応を依頼し、今後は未申告の送信サービス追加が発生しないよう管理体制を整えることが必要だ。

実際の攻撃パターンと対策

パターン 1：役員なりすまし（BEC）

対策なしの場合： 攻撃者が CFO を装ったメールを送り、経理担当者に送金を指示する。アドレスは本物と見分けがつかない。メールはそのまま届き、正規に見える。

DMARC の reject がある場合：受信サーバーがアライメントを確認する。攻撃者の送信インフラは CFO のドメインの DMARC ポリシーで許可されていない。配信前にブロックされる。

パターン 2：ビッシング――偽ボイスメール通知

攻撃の手口：攻撃者が信頼性の高いクラウドメールプラットフォームを使い、「ボイスメールが届いています――3 分 45 秒」といった件名の不在着信通知を模したフィッシングメールを送信する。見慣れた形式が緊迫感を生み、受信者にリンクをクリックさせる。クラウドプラットフォームは SPF と DKIM を自社ドメインで通過させる。DMARC がなければ、なりすまされた会社名でそのまま配信される。

DMARC の reject がある場合：DMARC アライメントで失敗――SPF と DKIM は配信プラットフォームを認証しているが、主張する送信者ドメインは認証していない。メールは受信者に届く前に拒否される。

拒否が証拠になる： `reject` ポリシーが発動すると、受信サーバーは通常、見かけ上のエンベロープ送信者に不達通知（NDR）を返す。攻撃者がリターンパスに被害組織のアドレスを使っていた場合、その NDR が受信トレイに届く――攻撃が失敗したにもかかわらず、なりすましが試みられたことが明らかになる。失敗した攻撃が、自らの証拠になるのだ。

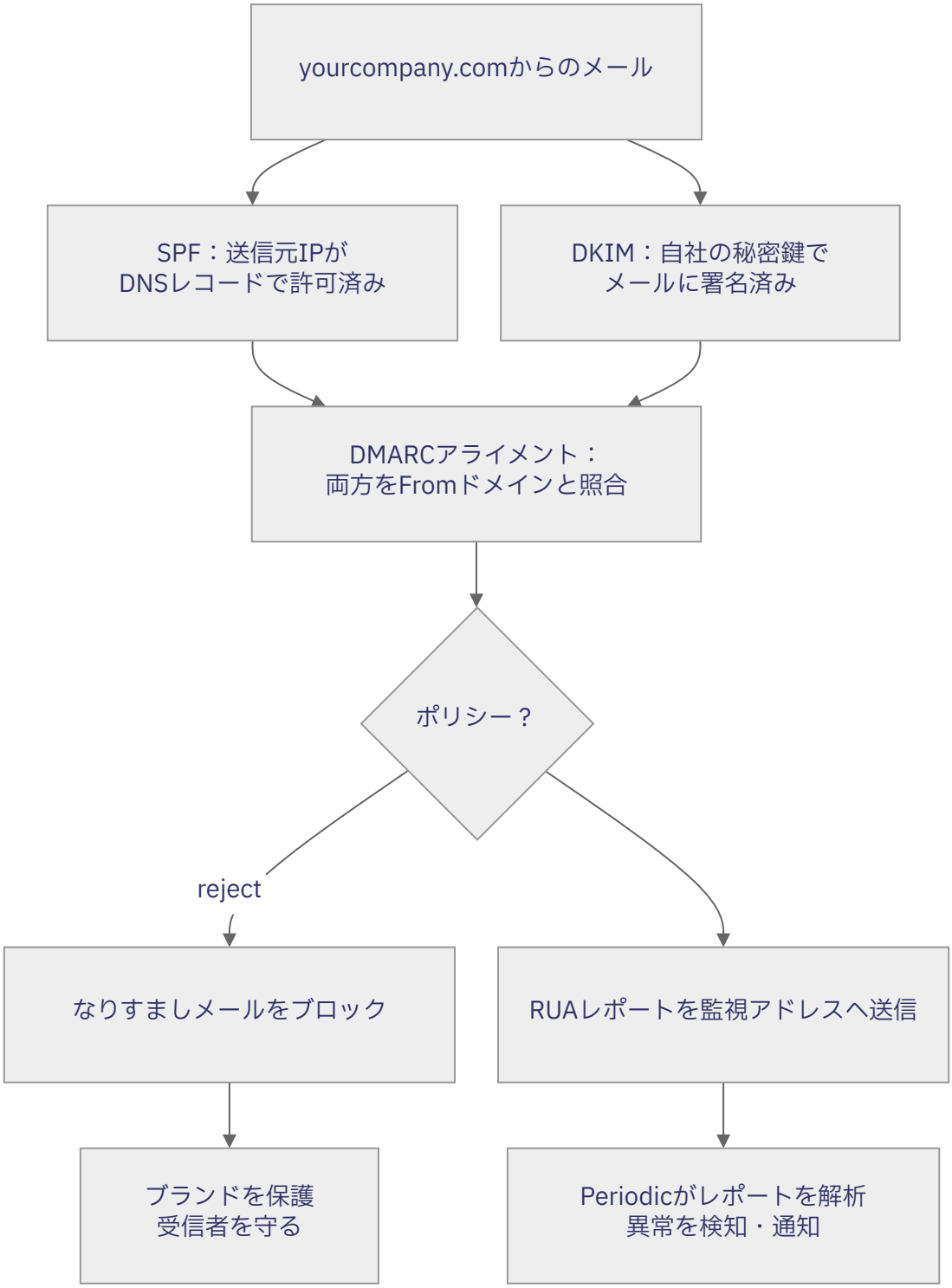
パターン 3：類似ドメインによる認証情報窃取

攻撃の手口： 攻撃者が `yourcompany-login.com` を取得し、本物のサイトを模した説得力のあるログインページを構築し、偽ドメインに正規の SPF と DKIM を設定してフィッシングメールを送信する。偽ドメインの DMARC はパスする――本物のドメインではなく偽ドメインに対して認証されているためだ。受信者はアドレスバーの微妙な差異に気づかないかもしれない。

ドメイン監視がある場合： パーミュテーション（変形パターン）スキャン中に偽ドメインが検知される――DNS レコードが初めて解決された時点（どこかを指すようになった時）、または TLS 証明書が発行された時点（証明書透明性ログで確認可能）のいずれかで。証明書のスクリーンショット・DNS レコード・登録者情報が自動収集される。誰も標的にされる前の、ドメインが出現した瞬間から監視が始まる。

適切に設定されたドメインの姿

適切に設定されたドメインは、3 つのレイヤーが連携し、DMARC が `reject` になっている：



保護されたドメインの全体像図

SPF レコード：すべての正規送信サービスをリスト化——メールプロバイダー・CRM・チケットシステム・マーケティングプラットフォーム。リストにないものはすべて未許可となる。

DKIM：最低 2048 ビットの RSA 鍵を定期的にローテーション。送信サービスごとにセレクターを分けることで、独立した鍵管理が可能になる。

DMARC の `reject`：成熟した確信のある設定の到達点。そこに至るまでには通常、まず `none` または `quarantine` の期間が必要で、ポリシーを厳しくする前にすべての正規送信サービスが適切に認証されていることを確認する。

RUA レポート：監視アドレスまたは解析サービスに向けることで、組織はインターネット上での自社ドメインの使われ方を継続的に把握できる。

Web への攻撃：もう一つの防御レイヤー

メール認証はなりすましメールを防ぐ。もう一つのレイヤーは、多くの攻撃に先行する Web への不正アクセス試行から組織の Web 環境を守る。

Web アプリケーションファイアウォール（WAF）は受信 HTTP トラフィックを検査し、SQL インジェクション試行・クレデンシャルスタッフィング・ボットトラフィック・脆弱性スキャンなど既知の攻撃パターンをブロックするルールを適用する。

実際の規模はほとんどの組織が想定するよりも大きい。このトラフィックの多くは自動スキャンだ――インターネット上のすべての IP アドレスを探索して脆弱なサービスを探すボットだ。ブロックすること自体はルーティンだが、この規模はインターネットに接続されたシステムが常に自動化された圧力にさらされていることを示している。保護のないシステムはそのリスクを静かに、可視化されないまま蓄積していく。

メール認証・WAF ルール・ドメイン監視を組み合わせた多層アプローチが、攻撃対象領域のそれぞれ異なる部分をカバーする。

設定の維持：ドリフトこそが本当のリスク

保護されたドメインは設定して終わりではない。設定はドリフトする。SPF を更新しないまま新しい送信サービスが追加される。DKIM 鍵が期限切れになる。メール移行中にポリシーが緩められ、その後復元されない。

継続監視がカバーする４つの領域：DNS レコードの変更（メンテナンスウィンドウ外での SPF・DKIM・DMARC への変更は定義上、異常だ）、DMARC レポート解析（主要受信サーバーからの日次レポートが自社ドメインを名乗るすべてのサーバーを可視化する）、類似ドメインスキャン（誰かを標的にする前にブランド悪用のドメイン登録を検知するパーミュテーションチェック）、そしてデッドマンズスイッチ検証（監視システム自体が無音で失敗していないことを確認する外部パルスチェック）。

各レイヤーの機能一覧

レイヤー	機能	防御対象
SPF	ドメインの送信許可 IP を定義	未許可サーバーによる送信
DKIM	メッセージの発信元と完全性を証明する暗号署名	メッセージ改ざん・未許可署名
DMARC	SPF/DKIM を表示 From アドレスとアライメント；ポリシーを設定	なりすましの From アドレス；アライメントしていないサードパーティによる悪用
DMARC レポーティング（RUA）	自社ドメインの使われ方の集計的可視化	気づかれないなりすましキャンペーン
WAF	悪意のある Web トラフィックをアプリケーション到達前にフィルタリング	クレデンシャルスタッフィング・スキャン・インジェクション攻撃
ドメイン監視	類似ドメインと設定ドリフトを検知	ブランドなりすまし・ポリシーの弱体化
DNSSEC	DNS レコードに暗号署名を付加し、リゾルバーが真正性を検証できるようにする	キャッシュポイズニングや BGP ハイジャックによる偽 SPF・DKIM・DMARC・TLSA レコード
DANE	メールサーバーの TLS 証明書ハッシュを DNS に固定（自社インフラのみ対象——M365 や Google Workspace には適用不可）	SMTP 配信時の証明書置換

これらの保護は攻撃の前に整備されていなければならない。`reject` ポリシーをフィッシング成功の翌日に設定するのは正しい対応だが、すでに起きたことは取り消せない。

お問い合わせ

株式会社イソリア 〒105-7105 東京都港区東新橋 1-5-2 汐留シティセンター 5 階 (Workstyling)

電話	**03-4577-3380**
メール	hello@esolia.co.jp
Web	https://esolia.co.jp
営業時間	月～金、9:00～18:00