CEO Display Name Impersonation: Analysis and Recommended Protections

CEO 表示名なりすまし：分析と推奨対策

Prepared for / 宛先

Mr. Yasushi Oyama, Japan Activation Capital

尾山 康 様, ジャパン・アクティベーション・キャピタル

March 17, 2026 / 2026 年 3 月 17 日

English Version

See page 9 →

日本語版

3 ページへ →

CEO 表示名なりすまし：分析と推奨対策

宛先

尾山 康 様, ジャパン・アクティベーション・キャピタル

2026 年 3 月 17 日

目次

作成： 株式会社イソリア
日付： 2026 年 3 月 17 日
サイト： japanactivationcapital.com
ステータス： アドバイザリー：推奨対策

発生している問題

外部の第三者が、貴社代表取締役（大塚 博行）の表示名を使用して、使い捨てのメールアドレス（例：`rtstyjvxw@hotmail.com`）から貴社宛にメールを送信しています。これらのメールは、受信者に個人の LINE 連絡先情報の共有を求め、監視されていないチャネルへのコミュニケーション移行を試みています。

これは**表示名なりすまし攻撃**（ビジネスメール詐欺の一形態）です。攻撃者は社内アカウントへのアクセスを持っていません。ほとんどのメールクライアントが実際のメールアドレスよりも送信者名を目立つように表示することを悪用しています。

既存の保護が機能しない理由

貴社ドメインの SPF、DKIM、DMARC レコードは正しく設定されており、`@japanactivationcapital.com` の直接なりすましからは保護されています。ただし、これらの保護は、差出人アドレスにドメインが偽装された場合にのみ適用されます。

今回の攻撃では、送信者は正規の外部アドレス（`@hotmail.com`）を使用しています。Hotmail 自体の SPF と DKIM は認証チェックに合格します。メールシステムの観点では、このメッセージは実在する Hotmail アカウントからの正当なメールであり、表示名フィールドに代表取締役の名前が設定されているだけです。デフォルトではこれをブロックする認証メカニズムはありません。

推奨対策

以下のすべての推奨事項は、Microsoft 365 E5 ライセンスに含まれている機能を使用します。追加費用は発生しません。

1. なりすまし防止保護の有効化（Defender for Office 365）

これが直接的な対策です。Microsoft Defender for Office 365（E5 に含まれる）は、受信メールの表示名が保護対象ユーザー（代表取締役やその他の役員など）に近似している場合を検出し、自動的に検疫またはフラグを付けることができます。

設定方法： - Microsoft Defender ポータル → **メールとコラボレーション** → **ポリシーとルール** → **脅威ポリシー** → **フィッシング対策** を開く - デフォルトポリシーを編集（または新規作成） - **なりすまし** → **保護するユーザー** で、代表取締役およびその他の主要役員を名前とメールアドレスで追加 - ユーザーなりすましのアクションを **メッセージを検疫** に設定 - **なりすましユーザーのヒントを表示** を有効化し、受信者に警告バナーを表示

想定されるデメリット：保護対象役員と同姓同名の外部関係者がいる場合、そのメールが検疫されます。IT 管理者が確認・解放する必要があります。珍しい名前であれば発生頻度は低いですが、取引先やパートナーの連絡先で発生する可能性があります。誤検知 1 件あたり数分の IT 確認作業が必要です。また、役員の異動時には保護対象リストの更新が必要です。

ユーザーへの影響： なし。検疫の確認は IT が対応します。エンドユーザーのワークフローに変更はありません（正当なメールが検疫審査で遅延する場合を除く）。

2. 優先アカウントの指定

Microsoft 365 E5 には **Priority Account Protection** が含まれており、指定された VIP に関わるメールに対して、強化されたメールフロー分析とより厳格なヒューリスティックを適用します。標準ポリシーでは検出が困難な巧妙ななりすまし試行も捕捉します。

設定方法： - Microsoft Defender ポータル → **設定** → **メールとコラボレーション** → **ユーザータグ** を開く - 代表取締役、CIO、その他の役員を **優先アカウント** タグに追加 - 優先アカウントには、強化された検出、専用レポート、追加のフィルタリングが適用される

想定されるデメリット： エンドユーザーへの影響はありません。完全にサーバー側の処理であり、ワークフローに変更は発生しません。IT が優先アカウント向けの詳細レポートを確認できるようになりますが、これは負担ではなく利点です。

ユーザーへの影響： なし。すべてのユーザーにとって透明。

3. 外部送信者識別の有効化

組織外からのメールを識別できるようにし、スタッフが内部メッセージと外部メッセージを一目で区別できるようにします。最も目立つものから最も控えめなものまで、3 つの実装オプションがあります：

オプション A：件名に［外部］を追加（トランスポートルール）

すべての外部メールの件名末尾に［外部］が追加されます。シンプルで、すべてのメールクライアントで機能します。

- Exchange 管理センター → **メールフロー** → **ルール** を開く
- ルールを作成：送信者が組織外の場合、件名に［外部］を追加

オプション B：Outlook 外部送信者バナー（推奨）

Outlook が外部メールの上部に控えめな情報バーを表示：「この送信者は組織外です。」件名は変更されません。Microsoft 365 版 Outlook（デスクトップアプリおよび Outlook on the web）で利用可能。

- Exchange Online PowerShell で以下を実行:
  `Set-ExternalInOutlook -Enabled $true`
- または Exchange 管理センター → **メールフロー** → **外部送信者識別** で設定

オプション C：HTML ディスクレーマーバナー（トランスポートルール）

メール本文の上部にカラー警告バナーを追加（件名ではなく本文）。すべてのクライアントで機能しますが、すべての外部メッセージに視覚的な要素が追加されます。

想定されるデメリット： オプション A はすべての外部メールの件名を変更するため、外部とのやり取りが多いユーザーには煩雑に感じられる場合があります。オプション B が最も控えめです。バナーはメール閲覧時にのみ表示され、件名は変更されません。オプション C は可視性がありますが、すべてのメッセージ本文に要素が追加されます。

ユーザーへの影響：選択するオプションに依存します。オプション B が最も摩擦が少ない選択肢です。すべてのオプションは、不審なメールだけでなくすべての外部メールに適用されます。なりすまし試行のみを選択的にタグ付けすることはこの層では不可能です。

4. 表示名トランスポートルールの作成

追加の保護として、主要役員の表示名と一致する外部メールを対象とするメールフロールールを作成します。対象を絞った対策であり、保護対象の名前に一致するメールのみに適用されます。

設定方法： - Exchange 管理センター → **メールフロー** → **ルール** を開く - 新しいルールを作成： - **条件：** 送信者が組織外であり、かつ From ヘッダーに「大塚 博行」が含まれる（必要に応じて変形を追加） - **アクション：** ディスクレーマーを追加：「このメールは組織外から送信されました。返信前に送信者のメールアドレスをご確認ください。」 / レビュー用に検疫にリダイレクト - 攻撃者がメールアドレスを変更しても、なりすましを捕捉する

想定されるデメリット： 対策 1 と同じ誤検知の可能性があります。役員と同姓同名の正当な外部連絡先がフラグされます。なりすまし防止ポリシーと併用することで、二重の保護を提供します。メンテナンス要件は同一で、役員異動時に名前リストの更新が必要です。

ユーザーへの影響： ほとんどのユーザーに影響なし。特定の役員名パターンに一致するメールのみに適用されます。

概要：保護範囲とトレードオフ

保護	検出対象	ユーザーへの影響	反発リスク
SPF/DKIM/DMARC（既存）	ドメイン直接偽装	なし	導入済み
なりすまし防止ポリシー（新規）	外部アドレスからの表示名なりすまし	なし（IT が検疫対応）	低
Priority Account Protection（新規）	VIP への巧妙ななりすまし	なし（透明）	なし
外部送信者タグ（新規）	すべての外部メールを明確化	すべての外部メールに表示	中（オプション A）、低（オプション B）
表示名トランスポートルール（新規）	役員表示名と一致する外部メール	なし（IT が検疫対応）	低

弊社の推奨

4 つの対策すべてを同時に導入するのが難しい場合は、以下の優先順位で実装を推奨します：

1. **なりすまし防止ポリシー** — 現在の攻撃への直接対策、ユーザーへの影響なし
2. **Priority Account Protection** — 透明、ユーザーへの影響なし、検出強化
3. **表示名トランスポートルール** — 対象を絞った保護、ユーザーへの影響なし
4. **外部送信者タグ（オプション B）** — 幅広い認識向上、最も摩擦の少ないアプローチ

対策 1～3 はエンドユーザーから見て透明であり、現在の CEO なりすまし攻撃に直接対応します。対策 4はすべての外部ソーシャルエンジニアリングに対する一般的な認識向上策ですが、ユーザーからのフィードバックが最も出やすい対策でもあります。

コスト

推奨されるすべての保護は Microsoft 365 E5 ライセンスに含まれています。追加のライセンスやサブスクリプションは不要です。

推奨スケジュール

対策	優先度	工数
なりすまし防止ポリシーの有効化	即時	30 分
優先アカウントの指定	即時	15 分
表示名トランスポートルールの作成	今週中	30 分
外部送信者タグの有効化（オプション B）	今週中	15 分

ユーザー向けガイダンス

これらの保護が導入されるまで、全スタッフに以下を周知してください：

- リクエストに応答する前に、表示名だけでなく実際のメールアドレスを必ず確認する
- 代表取締役がメールで個人の LINE QR コードやその他の個人連絡先情報を求めることはない
- 不審なメールは返信やリンクのクリックではなく、IT に転送してレビューを依頼する

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

eSolia

CEO Display Name Impersonation: Analysis and Recommended Protections

Prepared for

Mr. Yasushi Oyama, Japan Activation Capital

March 17, 2026

Contents

Prepared by: eSolia Inc.
Date: 17 March 2026
Site: japanactivationcapital.com
Status: Advisory — recommended actions

What Is Happening

External parties are sending emails to your organization using your CEO's display name (大塚 博行) as the sender name, but from throwaway email addresses (e.g., `rtstyjvxw@hotmail.com`). The emails request that recipients share personal LINE contact information, attempting to move communication to an unmonitored channel.

This is a **display-name impersonation attack** (a form of Business Email Compromise). The attacker does not have access to any internal account. They are exploiting the fact that most email clients prominently display the sender's name rather than the actual email address.

Why Existing Protections Do Not Help

Your domain's SPF, DKIM, and DMARC records are correctly configured and protect against direct spoofing of `@japanactivationcapital.com`. However, these protections only apply when someone forges your domain in the From address.

In this attack, the sender uses a legitimate external address (`@hotmail.com`). Hotmail's own SPF and DKIM pass authentication checks. From the email system's perspective, the message is a valid email from a real Hotmail account — it just happens to have the CEO's name in the display name field. No authentication mechanism blocks this by default.

Recommended Actions

All recommendations below use features included in your Microsoft 365 E5 licenses at no additional cost.

1. Enable Anti-Impersonation Protection (Defender for Office 365)

This is the direct fix. Microsoft Defender for Office 365 (included in E5) can detect when an incoming email's display name closely matches a protected user — such as the CEO or other executives — and automatically quarantine or flag the message.

Configuration: - Open the Microsoft Defender portal → **Email & collaboration** → **Policies & rules** → **Threat policies** → **Anti-phishing** - Edit the default policy (or create a new one) - Under **Impersonation** → **Users to protect**, add the CEO and other key executives by name and email address - Set the action to **Quarantine the message** for user impersonation - Enable **Show tip for impersonated users** so recipients see a warning banner

Potential downside: If anyone external legitimately shares the same name as a protected executive, their emails will be quarantined. An IT administrator must review and release them. For an uncommon name this is rare, but it can occur with vendors or partner contacts. Each false positive requires a few

minutes of IT review. New executives must also be added to the protected list manually — if someone joins or leaves, the list needs updating.

User impact: None. Quarantine review is handled entirely by IT. End users see no change to their workflow unless a legitimate email is delayed by quarantine review.

2. Designate Priority Accounts

Microsoft 365 E5 includes **Priority Account Protection**, which applies enhanced mail-flow analysis and stricter heuristics to emails involving designated VIPs. This catches sophisticated impersonation attempts that standard policies might miss.

Configuration: - Open the Microsoft Defender portal → **Settings** → **Email & collaboration** → **User tags** - Add the CEO, CIO, and other executives to the **Priority account** tag - Priority accounts receive enhanced detection, dedicated reports, and additional filtering

Potential downside: None for end users. This is entirely server-side — enhanced scanning with no change to anyone's workflow. IT receives more granular reports for priority accounts, which is a benefit rather than a burden.

User impact: None. Invisible to all users.

3. Enable External Sender Identification

Mark emails from outside the organization so staff can distinguish internal messages from external ones at a glance. Three implementation options are available, ranging from most visible to least intrusive:

Option A — Append `[External]` to subject line (transport rule)

Every external email gets `[External]` appended to the subject. Straightforward and works in all email clients.

- Open the Exchange admin center → **Mail flow** → **Rules**
- Create a rule: if the sender is outside the organization, append `[External]` to the subject line

Option B — Outlook external sender banner (recommended)

Outlook displays a subtle info bar at the top of external emails: "This sender is outside your organization." The subject line is not modified. Available in Outlook for Microsoft 365 (desktop app and Outlook on the web).

- Open Exchange Online PowerShell and run:
  `Set-ExternalInOutlook -Enabled $true`
- Or configure via the Exchange admin center → **Mail flow** → **External sender identification**

Option C — HTML disclaimer banner (transport rule)

Append a colored warning banner to the top of the email body (not the subject line). Works across all clients but adds visual clutter to every external message.

Potential downside: Option A modifies every external subject line, which some users find cluttered — especially staff whose communication is predominantly external. Option B is the least intrusive: the banner appears only when reading the email, and the subject line stays clean. Option C is visible but adds bulk to every message body.

User impact: Depends on option chosen. Option B has the lowest friction. All options affect every external email, not just suspicious ones — there is no way to selectively tag only impersonation attempts at this layer.

4. Create a Display-Name Transport Rule

For additional protection, create a mail-flow rule that specifically targets external emails whose display name matches key executives. This is narrowly targeted — it only fires for emails that match the protected names.

Configuration: - Open the Exchange admin center → **Mail flow** → **Rules** - Create a new rule: - **Condition:** The sender is located outside the organization AND the From header contains "大塚 博行" (add variations as needed) - **Action:** Append a disclaimer: "This email was sent from outside the organization. Verify the sender's email address before responding." / Redirect to quarantine for IT review - This catches impersonation even if the attacker changes the email address

Potential downside: Same false-positive scenario as Action 1 — a legitimate external contact who shares the executive's name will be flagged. Since this is layered on top of the anti-impersonation policy, it provides belt-and-suspenders coverage. The maintenance requirement is the same: update the name list when executives change.

User impact: None for most users. Only affects emails that match the specific executive name patterns.

Summary: Protection Coverage and Trade-offs

Protection	What It Catches	User Impact	Pushback Risk
SPF/DKIM/DMARC (existing)	Direct domain spoofing	None	Already in place
Anti-impersonation policy (new)	Display-name impersonation from external addresses	None (IT handles quarantine)	Low
Priority Account Protection (new)	Sophisticated impersonation of designated VIPs	None (invisible)	None
External sender tagging (new)	All external emails clearly labeled	Visible on every external email	Medium (Option A), Low (Option B)
Display-name transport rule (new)	External emails matching executive display names	None (IT handles quarantine)	Low

Our Recommendation

If adopting all four measures feels like too much change at once, we recommend implementing them in priority order:

1. **Anti-impersonation policy** — the direct fix for the current attack, no user impact
2. **Priority Account Protection** — invisible, no user impact, enhanced detection
3. **Display-name transport rule** — targeted protection, no user impact
4. **External sender tagging (Option B)** — broad awareness, lowest-friction approach

Actions 1–3 are invisible to end users and address the specific CEO impersonation attack. Action 4 is a general awareness measure that helps with all forms of external social engineering, but it is also the one most likely to generate user feedback.

Cost

All recommended protections are included in Microsoft 365 E5 licensing. No additional licenses or subscriptions are required.

Recommended Timeline

Action	Priority	Effort
Enable anti-impersonation policy	Immediate	30 minutes
Designate priority accounts	Immediate	15 minutes
Create display-name transport rule	This week	30 minutes
Enable external sender tagging (Option B)	This week	15 minutes

User Guidance

Until these protections are in place, advise all staff:

- Always check the actual email address (not just the display name) before responding to any request
- The CEO will never ask for personal LINE QR codes or other personal contact information via email
- Forward any suspicious emails to IT for review rather than replying or clicking links

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