

急増する「LINEグループ作成」要求 CEO詐欺の最新手口と対策

2025年末から日本全国の組織を襲う、巧妙な「権威」と「密室」の罠



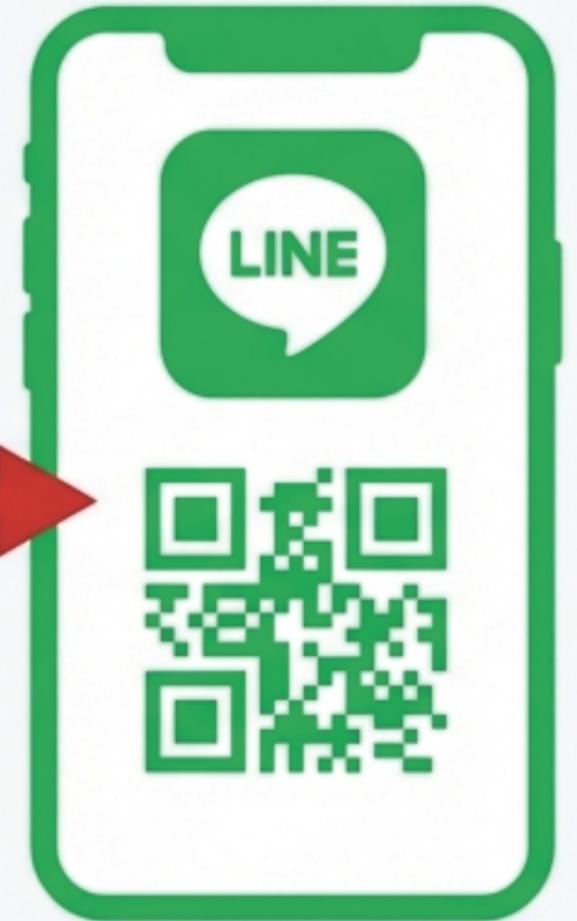
To employee@company.com>

From **CEO** <ceo.official.jp@gmail.com> ⚠

Subject **【至急】業務連絡**

山田様、
至急、機密案件についてLINEグループを作成してください。詳細はそちらで。

罠への誘導経路



「密室」への引き込み：
権威を悪用した巧妙な手口

2025年12月、潮目が変わった



通常、フィッシング詐欺の増加は緩やかですが、これは「爆発」でした。日本国内の組織を一斉に狙った、極めて組織的な攻撃キャンペーンです。

「数千万円」がスマホひとつで消える



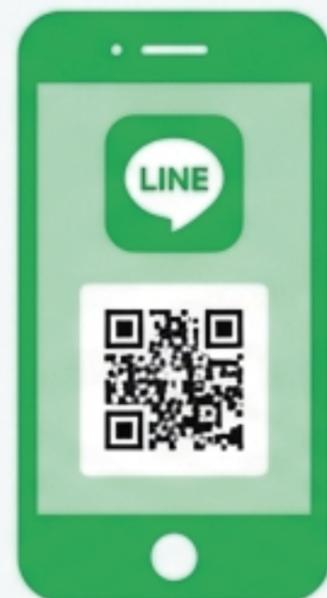
自治体から製造業まで。組織の規模や地域に関わらず、すべての企業が標的です。

攻撃の解剖図：3つのステップ



1. The Bait (導入)

偽の社長メール
「至急、LINEグループを作れ」



2. The Switch (隔離)

企業セキュリティの外へ
「QRコードを送れ」



3. The Sting (実行)

金銭の要求
「極秘案件のため送金せよ」

攻撃者の狙いは、監視された「企業のメール環境」から、セキュリティの目が届かない「個人のスマホ（密室）」へあなたを連れ出すことです。

心理的な罠：なぜ信じてしまうのか

件名：【重要】業務連絡

件名：【重要】業務連絡

社長です。業務上の都合により、**至急**LINEグループを作成してください。

【注意事項】

- ・他者招待の禁止：グループ内には**あなたと私の2名のみ**とします。
- ・他言無用：極秘プロジェクトに関わるため、誰にも相談してはいけません。

権威 (Authority)

緊急性 (Urgency)

密室性 (Secrecy)

「誰かに相談させない」ために、あえて『他者招待の禁止』や『極秘』という言葉を使い、心理的にも孤立させます。

なぜ「LINE」なのか？

Firewall
(企業セキュリティ)

個人のスマホ / LINE



⚠ 企業セキュリティ：不審なワードを検知してブロック

✓ 個人のスマホ：企業の監視システムは「不可視」

LINEや個人のスマホに移動した瞬間、企業のセキュリティフィルターは無効化されます。
攻撃者にとって、そこは無法地帯です。

見抜くポイント①：送信元アドレス



Red Flag Domains

- ⚠️ • gmail.com
- ⚠️ • outlook.com
- ⚠️ • hotmail.com
- ⚠️ • yahoo.com
- ⚠️ • aol.com

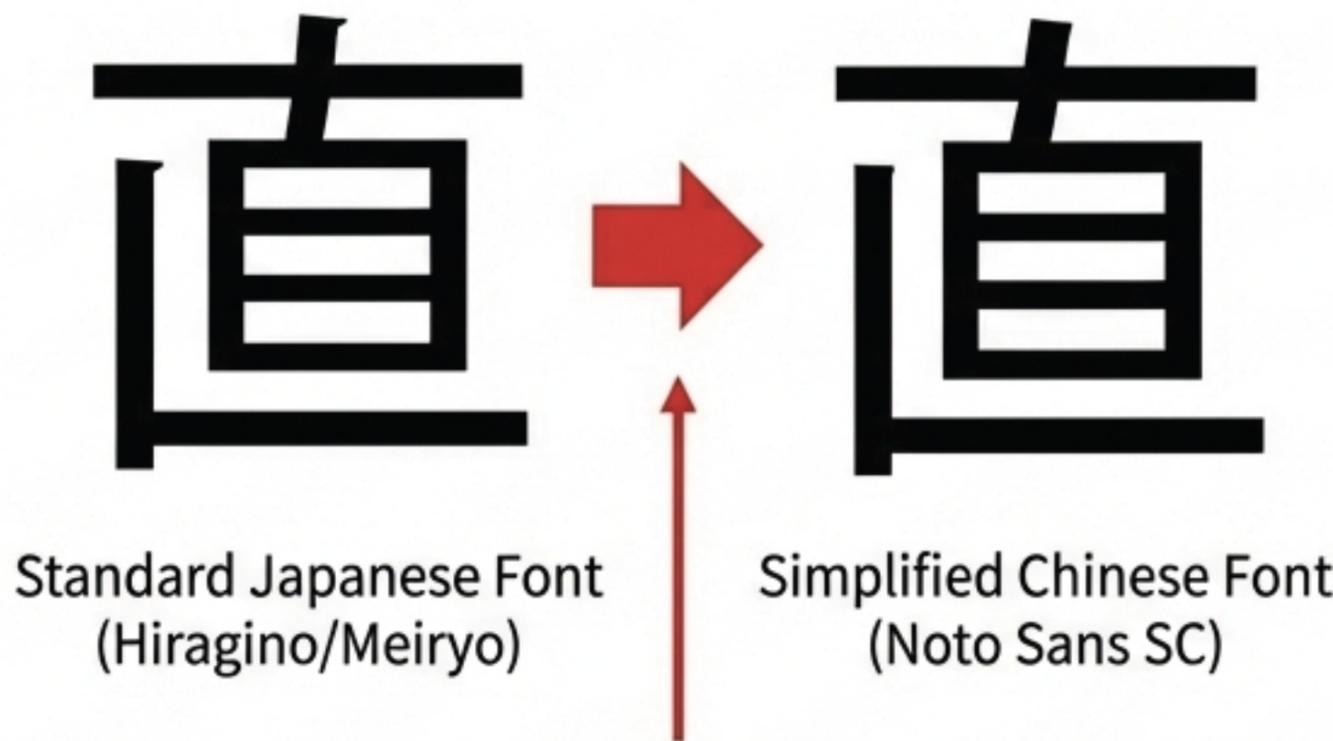
企業の代表者が、重要な業務指示にフリーメールを使うことはありません。
表示名が正しくても、アドレス（ドメイン）が嘘を吐いています。

見抜くポイント②：不自然な日本語とフォント



会社用のLINE **群組** を作成してください。
公司 管理を円滑にするため...
こんなお願いいたします。

中国語由来の単語
(群組=Group, 公司=Company)



直 → 直

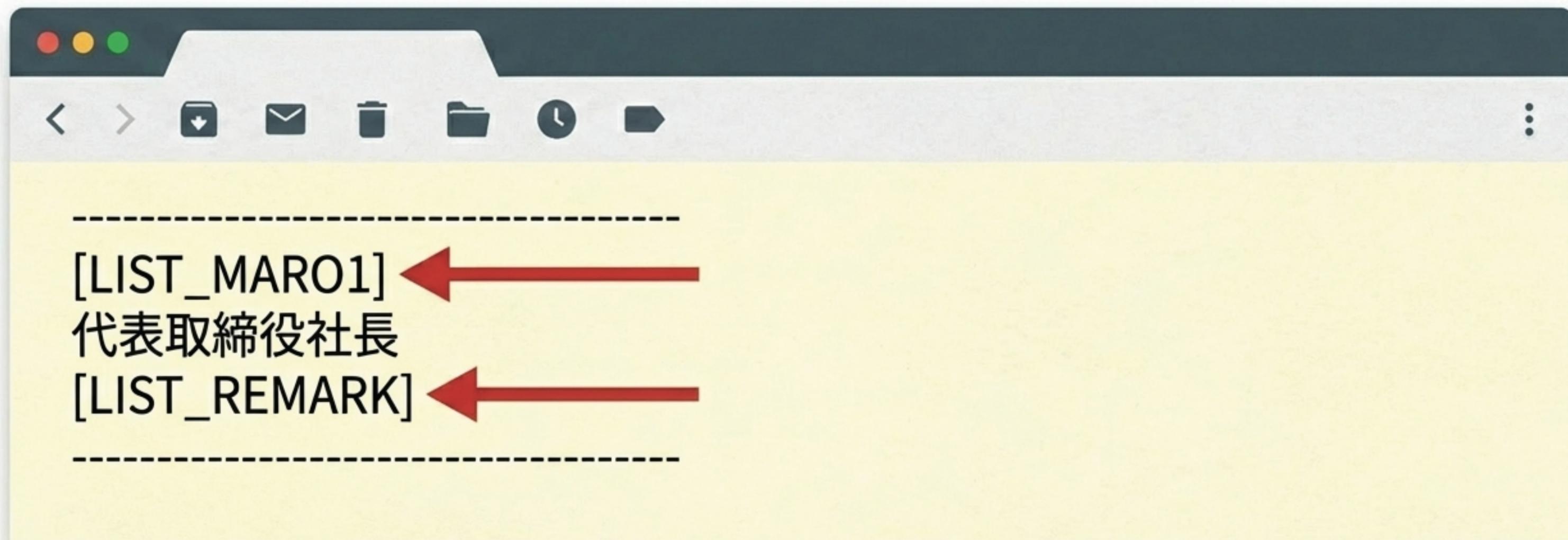
Standard Japanese Font
(Hiragino/Meiryo)

Simplified Chinese Font
(Noto Sans SC)

中国語フォント特有の字形（漢字の骨格が違う）

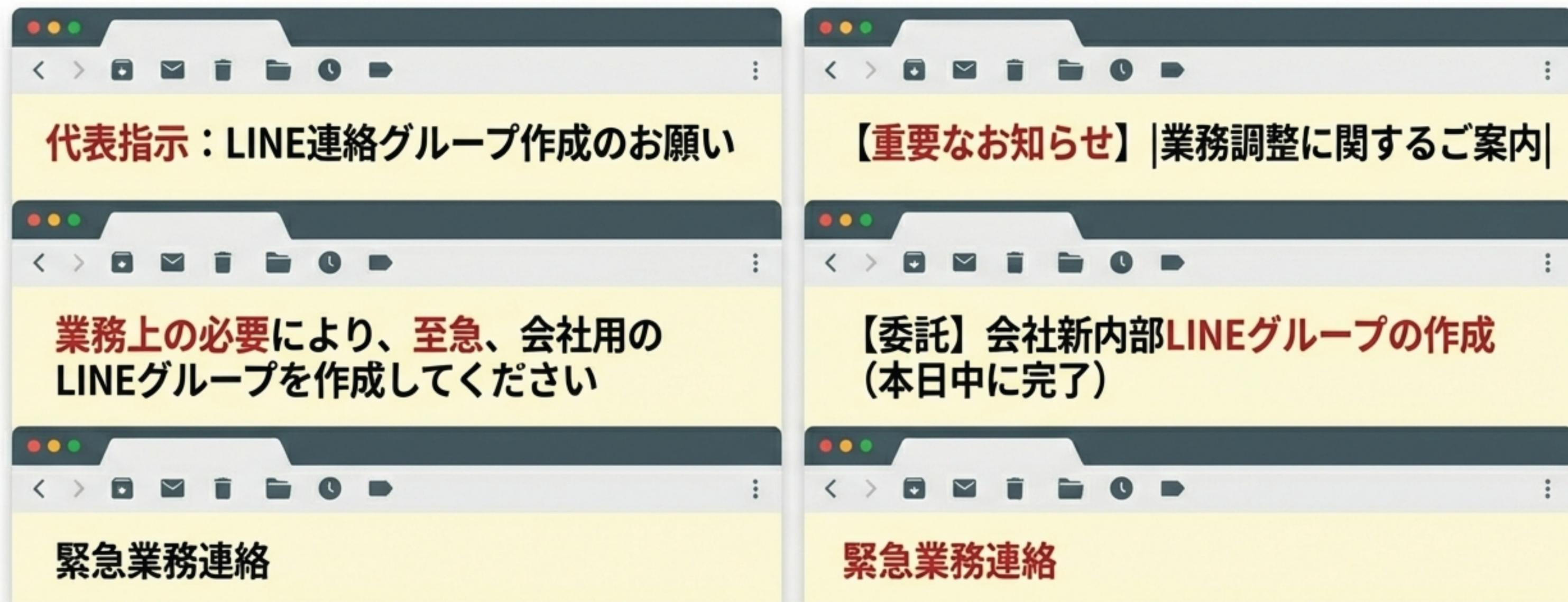
攻撃者の多くは翻訳ツールを使用しています。ビジネスメールにはあり得ない単語や、**違和感のある漢字フォント**が混ざっています。

見抜くポイント③：自動化の「ボロ」



これらは一斉送信ツールの「置き換えタグ（変数）」です。攻撃者が設定をミスして、そのまま送信されているケースが多発しています。個別のメールではなく、プログラムによる自動送信である証拠です。

実際の件名パターン



「業務上の都合」「作成のお願い」「本日中に」というフレーズが共通しています。これらを見たら、反射的に警戒してください。

もし、このメールが届いたら



1. 返信しない (Do Not Reply)

QRコードを作らない。リンクをクリックしない。



2. 別ルートで本人確認 (Verify Offline)

メールへの返信は厳禁です。
必ず「内線電話」や「知っている携帯番号」で
本人、または秘書に確認してください。



3. システム部門へ報告 (Report)

社内のIT担当者へメールを転送し、
周囲への注意喚起を行ってください。



組織として守る：社内ルールの策定



チャットでの 金銭指示禁止

LINE、SMS、個人チャットでの送金指示は「無効」とするルールを明文文化してください。すべての決済は正規のワークフローを経由する必要があります。



標的部署 への警告

攻撃者は「経理」「財務」「人事」を狙い撃ちします。これらの部署には、この手口の具体例を今すぐ共有してください。

すでにクリック/送金してしまった場合

Time 0 (Now)



通信遮断

詐欺師との連絡を絶つ。

Time +1min



銀行へ連絡

送金してしまった場合、直ちに銀行へ連絡し資金凍結を依頼する。

Time +5min



警察・IT部門へ連絡

サイバー犯罪対策課へ相談。社内被害の拡大を防ぐためIT部門へ報告。

⚠ 隠蔽是最悪の選択です。スピードが被害額を決定します。

CEO詐欺対策チェックシート

予兆 (The Signs)

- 件名：「LINEグループ作成のお願い」
- 送信元：Gmail / Outlook(フリーメール)
- 本文：「他者招待の禁止」「極秘」

アクション (Action)

- 返信しない / QRを送らない
- 内線電話で本人確認
- IT部門へメールを転送



確認 (Check)

- 日本語の不自然さ (「群組」「公司」)
- フォントの違和感
- 自動化タグ ([LIST_MARO])



鉄則 (Rule)

「チャットで金銭指示は詐欺」

セキュリティは、全員の仕事です。

攻撃手口は日々進化しています。昨日は請求書詐欺、今日はLINEグループ。
最高の防御策は、社員が躊躇なく「これは本物ですか？」
と確認できる組織文化です。

この資料を、今すぐあなたのチームに共有してください。