検知からテイクダウン、従業員保護まで、今必要なソーシャルエンジニアリング対策

河内 洋幸, CISSP
ドッペル株式会社　セールスエンジニアリング本部　Director of Sales Engineering
IDC IT Security Forum 2026, Japan｜2026年11月11日

© Doppel Inc. 2026. All Rights Reserved.

Doppelのご紹介及び自己紹介

Doppel, Inc.

統合型ソーシャルエンジニアリング対策プラットフォームを提供。マルチチャネルのソーシャルエンジニアリング攻撃を、検知・キャンペーン可視化・インフラ遮断まで統合的に防御

設　立：2022年2月

代　表：Kevin Tian

所在地：米国カリフォルニア州

拠　点：SF / NY / London / Austin / Toronto / Tokyo

従業員：300名～

資金調達：シリーズC 累計1億2,400万ドルを調達

日本法人：ドッペル株式会社

設立：2026年8月

代表：牛込秀樹

所在地：東京都千代田区丸の内2−7−2 JPタワー14F



河内 洋幸, CISSP
セールスエンジニアリング本部
Director of Sales Engineering

ISP系のSIerでキャリアをスタートし、大規模検索エンジンのインフラエンジニアとして従事。その後、大手クラウドベンダーでグローバルネットワーク基盤のエンジニア、CDNベンダーでウェブセキュリティのコンサルタント、エンドポイントセキュリティベンダーで金融・公共部門の技術責任者を歴任。
直近はコンサルティングファームのサイバーセキュリティ部門で技術責任者として脅威ハンティング等のプロジェクトをリードした後、Doppelに入社。

© Doppel Inc. 2026. All Rights Reserved.

本日お伝えしたいこと

①AIは攻撃コストを下げ、最後の標的を「人の判断」に移した

対策を重ねても、送金・承認・アカウント復旧等の判断は人に残る

②「見抜く力」を人に求めるだけでは限界がある

攻撃はキャンペーンとして組織の外側で準備され、人に届く前に元を断つという発想が必要

③組織外の脅威インフラ・メール・従業員の3つの観点を共通の脅威情報で接続する

脅威インフラに対する先回りのテイクダウンと、確認・報告できる仕組みの両輪で強化していく

Doppel

© Doppel Inc. 2026. All Rights Reserved.

AIが変えた攻撃の前提

AIは攻撃コストを下げ、量・質・速度を向上させている

AIによって容易になったこと

文面の作成
自然な日本語を相手や状況に合わせて大量に生成

偽サイトの構築
本物に酷似したログイン画面を短時間で複数用意する

なりすまし・ディープフェイク
SNSアカウント、音声、映像で実在の人物や企業を装う

標的の調査や偵察行動
公開情報から組織体制や担当者、取引関係を効率的に把握

攻撃者が準備・実施・改変・再試行するコストは圧倒的に下がった

そして、すり抜けた攻撃は「人の判断」に委ねられる

Doppel

© Doppel Inc. 2026. All Rights Reserved.

最後に残る標的は「人の判断」

技術的な対策を重ねても、業務上の判断は最後まで人に残る

技術的な対策領域(アタックサーフェス)

エンドポイント	ネットワーク
クラウド・SaaS	ID・アイデンティティ
Web・アプリ	コード・リポジトリ
サプライチェーン	AI・LLM基盤

カテゴリ化され、比較的守る対象が明確

最終的に人に残るもの(従業員と判断)

経理	実際の振込や送金先の変更
IT担当	アカウント作成・権限付与
従業員	ログインやMFA承認
管理職	至急の承認や情報共有のリクエスト

守るべき対象と認識されにくい

従業員を「対策できない領域」とするのではなく、企業の判断を支える「保護すべき対象」と捉える

Doppel

© Doppel Inc. 2026. All Rights Reserved.

参考：セキュリティインシデントにおける侵害の手法

直近の、システムやデータへのアクセスを阻害したランサムウェア被害で、最も重要な最初の侵害の起点は何でしたか

出典：IDC、From Infrastructure to Inbox: Defending the Full Social Engineering Attack Chain、US54799626、2026年7月

最初の侵害の起点	割合
インターネット閲覧中に攻撃者がアクセスを獲得する、各種のブラウザベースの攻撃	17.6%
サプライチェーン攻撃（例 SolarWinds、PC Cleaner、Kaseya）	13.0%
システムに接続された周辺機器やリムーバブルメディア内のマルウェア	12.7%
フィッシングメール内の悪意あるURLのクリック、または悪意ある添付ファイルの開封	12.4%
侵害された認証情報を利用した不正アクセス	11.8%
パッチが適用されていない脆弱性の悪用	9.2%
システムへのアクセスを許してしまう設定ミスの悪用	7.8%
内部脅威（悪意ある内部関係者）	6.4%
ゼロデイ脆弱性の悪用	5.7%
組織として最初の侵害の起点を特定できなかった	2.3%
わからない・最初の侵害の具体的な内容や詳細を知らされていない	1.1%

様々な侵害に「人の判断」が関係している

© Doppel Inc. 2026. All Rights Reserved.

ソーシャルエンジニアリングの構造

「信頼させ、判断を急がせ、行動させる」の3ステップ

①信頼関係を利用する

上司、取引先、社内IT、普段使うサービスを装い、警戒心を下げる

例：ロゴ、デザイン、類似ドメイン

②判断を急がせる

期限や例外対応を理由に、確認する時間と余裕を奪う

例：「本日中に」「アカウント停止」

③行動を促す

攻撃者が必要とする「一手」へ、自然な流れで誘導する

例：ログイン、情報入力、送金、MFA承認

経路：メール SMS 電話 SNS 広告 チャット

経路が変わっても、構造は変わらない

Doppel

© Doppel Inc. 2026. All Rights Reserved.

攻撃は「キャンペーン」で動く

被害が発生する前から、攻撃インフラは組織外で準備されている

組織外 — 企業の管理が及びにくい領域

組織内・従業員・顧客

準備	誘導	接触	実行	被害
ドメイン取得、偽サイト構築、偽アカウント作成、偽広告	メール、SMS、SNS、検索広告、電話	従業員や顧客が、本物と見分けにくい依頼を受け取る	認証情報の入力、送金、MFA承認、情報の提供	不正アクセス、金銭被害、情報漏えい、ブランド毀損

被害が起きる前から、攻撃インフラはすでに組織外に存在しており、
本来はそこに「先回り」できる余地がある

Doppel

© Doppel Inc. 2026. All Rights Reserved.

我々はどう対策を行うべきか

自社環境を守ることは従前から必須だが、では「相手(=攻撃者)」についてはどう考えるべきか？

自社環境を守る場合	組織外の攻撃準備を止める場合
エンドポイント ネットワーク ID クラウド メール Web	偽ドメイン 偽サイト 偽のSNSアカウント 偽広告 攻撃インフラ
侵入を防ぎ、被害を最小限に留める	攻撃に使われるインフラを早期発見し、停止・削除につなげる

攻撃を防ぐだけでなく、攻撃そのものを止めにいく

© Doppel Inc. 2026. All Rights Reserved.

従来の対策の4つのギャップ

人の注意力と個別対応に依存した運用には、構造的な限界がある

ギャップ 1

人に「見抜け」と求める教育

精巧になった攻撃を、個人の注意力だけで防ぎ続けることは難しい

ギャップ 2

URL単位の「点」の対処

1つを止めても、関連するドメインやアカウントから攻撃が再開される

ギャップ 3

申請して終わる運用

攻撃インフラの停止の確認や再出現の監視がなく、対処の実効性が見えない

ギャップ 4

部門ごとに分断された運用

攻撃インフラの検知・メール対策・トレーニング等が別々に管理され、1つのコンテキストとならない

Doppel

© Doppel Inc. 2026. All Rights Reserved.

発想の転換：3つの防御線を統合する

組織外・受信メール・人の防御線を、共通の脅威インテリジェンスでつなぐ

攻撃の流れ

第1の防御線｜組織外

届く前に断つ

偽サイト・偽アカウント・偽広告を継続的に把握し、関連する攻撃インフラごとテイクダウンする

第2の防御線｜受信メール

届いたら止める

実際のメールを分析し、検知・隔離で従業員から遠ざける

第3の防御線｜人

人の判断を支える

確認と報告が機能する手順を整え、実際の手口に即した訓練で従業員の判断力を向上させる

共通の脅威インテリジェンス
攻撃をキャンペーン単位で捉え、コンテキストを3つの防御線で共有する

Doppel

© Doppel Inc. 2026. All Rights Reserved.

攻撃者に「先回り」を行うこと

ドメイン等の単一の点ではなく攻撃インフラ全体を面で捉え、テイクダウン(運営事業者に通報して削除・閉鎖させること)を行っていく

	これまで	これから
検知	通報や被害の報告を受けてから把握する	偽ドメイン・SNS・広告など複数のチャネルを継続的に監視し、被害発生の前に把握する
調査	見つかったURLを1件ずつ確認する	ドメイン、IP、証明書などの共通点から関連する対象をたどり、全体像を把握する
対処	申請を送った時点で完了とする	停止・削除を確認し、未対応なら再申請やエスカレーションを行う
評価	申請件数を数える	実際に停止した割合と所要時間、再出現の有無を追う

© Doppel Inc. 2026. All Rights Reserved.

従業員保護で考えていくべきこと

確認と報告が機能する仕組みを作り、訓練を継続していく

確認の手順を決める

- 確認が必要な依頼を決めておく
- 正規の連絡先へ別経路で確認
- 確認のための業務停止を許容

報告しやすくする

- 確信がなくても報告できる窓口
- 受付責任者が結果を返す
- 早期報告や失敗の申告を評価

業務に即して訓練する

- 役割別のシナリオで訓練
- メール・SMS・音声で実施
- 実際に観測された手口を題材に

クリック率だけでなく、「報告率」と「報告までの時間」で組織の成熟度を測る

Doppel

© Doppel Inc. 2026. All Rights Reserved.

Doppelのアプローチ

3つの防御線を、1つの統一された環境で：ソーシャルエンジニアリング対策プラットフォーム

第1の防御線｜組織外

DRP

デジタルリスクプロテクション

・偽ドメイン、偽サイト、SNSなりすまし、偽広告を継続検知

・テイクダウンから停止確認、再出現の監視までAIと自社SOCを組み合わせ、量と質を担保する

第2の防御線｜受信メール

メールセキュリティ

Email Security / Email Triage

・既存のメール環境とAPI連携し、受信メールを分析、攻撃インフラのコンテキストを追加

・報告された不審メールを分析し、訓練に還流する

第3の防御線｜人

HRM

ヒューマンリスクマネジメント

・メール・SMS・音声による、業務に即した訓練

・訓練中の行動に応じた学習とフォロー

Threat Graph

脅威を関連付け、攻撃キャンペーン全体を可視化する共通基盤

Doppel

© Doppel Inc. 2026. All Rights Reserved.

Threat Graphで攻撃の全体像を可視化する

散在する脅威を関連付け、攻撃キャンペーン単位でテイクダウンする

①検知：偽サイト、偽アカウント、偽広告などをアラートとして提示

②関連付け：ドメイン、IP、証明書、リンクなどの共通点から脅威を関連付ける

③テイクダウン：適切な事業者へ申請し、停止・削除と再出現を確認する



Threat Graphの画面例

Doppel

© Doppel Inc. 2026. All Rights Reserved.

想定シナリオ例

1つのなりすまし攻撃を、3つの防御線で止める

例：社内IT担当を装い「本日中に認証方式の更新を」と偽ログイン画面へ誘導するメール

防御線	把握する	対処する	改善する
第1｜組織外 DRP	偽サイトと関連ドメインを調査	停止・削除を申請し完了を確認	再出現と関連対象を再評価
第2｜受信メール メールセキュリティ	受信メールと誘導先を分析	ポリシーに沿って隔離など	判定と報告対応を見直す
第3｜人 HRM・社内運用	不審な依頼に気づき報告	正規のIT窓口へ別経路で確認	同じ手口を訓練の題材に

Doppel

© Doppel Inc. 2026. All Rights Reserved.

明日から確認したい3つのポイント

①自社を装う偽サイト・偽アカウントを被害前に把握し、停止までできているか

②届いた不審メールと、その誘導先の攻撃インフラを結び付けて調査できているか

③確認・報告できる仕組みを整え、実践的な訓練を行っているか

攻撃者に先回りを行い、人の判断を支え、そして従業員と組織を保護する仕組みへ

© Doppel Inc. 2026. All Rights Reserved.



Thank You

© Doppel Inc. 2026. All Rights Reserved.