プレスリリース

報道関係者各位

2026 年 11 月 24 日

有限会社スーパーシーアールエム

本社：神奈川県川崎市多摩区菅稲田堤 2-1-8　代表：國信 正直

フィッシング被害と止まらない情報漏洩対策の為に Windows 用メールソフト「SuperCRM_Mail」、2026 年 12 月に無料で公開

未登録のリンク先は開かず偽サイトへの誘導を抑制。添付ファイルは開く前に検査しゼロディ攻撃、ゼロクリック攻撃、ウイルスによる情報漏洩のリスクを抑えます。メールアドレスやメールサーバーは今のまま使用可能。

有限会社スーパーシーアールエム（本社・神奈川県川崎市、代表・國信 正直）は、フィッシング被害と情報漏えいに備える日本製の Windows 用メールソフト「SuperCRM_Mail（スーパーシーアールエム メール）」を、2026 年 12 月に無料公開します。

偽のログイン画面に誘導されて ID やパスワードを入力する。取引先を装ったメールの添付ファイルを開き、ウイルスに感染する。こうした被害は、普段のメール操作をきっかけに起こります。

SuperCRM_Mail は、自身に独自のフィッシング対策や各種の攻撃対策機能を持つことで、許可リストにないリンク先を開かず、添付ファイルは利用前に検査します。さらに、メールを読み解く処理を PC 内の制限された環境で動かし、攻撃の影響がほかのファイルや機能に及ぶリスクを抑えます。

無料版は、今、お使いの対応メールアドレスとメールサーバーで利用でき、専用サーバーの追加は不要です。個人、企業・各種法人、官公庁・自治体、学校などで利用でき、広告やアプリ内課金もありません。子会社や委託先にも、ソフトの利用料なしで導入を広げられます。

組織で設定や更新を一括管理できる機能を持った有料版「SuperCRM_Mail Business」は、2027 年 1 月に提供予定です。

■開発の背景

・IPA（情報処理推進機構）の「情報セキュリティ 10 大脅威 2026」組織編では、「ランサム攻撃による被害」が 1 位、「AI の利用をめぐるサイバーリスク」が初選出で 3 位、「機密情報を狙った標的型攻撃」が 5 位、「ビジネスメール詐欺」が 10 位に挙げられています。[1]
・フィッシング対策協議会が受領した 2025 年のフィッシング報告件数は、過去最多の 2,454,297 件で、前年比約 1.43 倍でした。同協議会は、攻撃者が自分で用意したアドレスを使い、送信元の確認を通過して迷惑メールの振り分けを逃れる手口も報告しています。[2]
・Verizon の 2026 年の調査報告書では、調査対象の情報漏えいなどの事案の 48%に、取引先や外部サービス事業者などの関与があったと報告されています。メール経由に限った数字ではありませんが、自社だけでなく取引先・委託先にも対策を広げる重要性を示しています。[3]

こうした脅威に対し、メールを読む処理を分けて動かす、添付を検査・作り直す、開ける接続先を限定するなど、場面ごとに対策を重ねています。利用者が自分だけでメールの真偽を見抜く負担を減らし、誤った操作による被害リスクを抑えることを目指します。

[1] IPA「情報セキュリティ 10 大脅威 2026」
https://www.ipa.go.jp/security/10threats/10threats2026.html
[2] フィッシング対策協議会「フィッシングレポート 2026」
https://www.antiphishing.jp/report/report/phishing_report2026.html
[3] Verizon「2026 DBIR」公式発表（2026 年 5 月 19 日）
https://www.verizon.com/about/news/breach-industry-wide-dbir-finds

■SuperCRM_Mail の主な特長

1. 未登録のリンク先を開かず、偽サイトへの誘導を抑える
メール本文のリンクをクリックすると、開いてよい接続先を登録した許可リストと照合します。一覧にないリンク先は開きません。日本語などを含むウェブアドレスも確認対象です。メールに埋め込まれた外部画像も、表示条件を確かめてから読み込みます。

2. 添付を開く前に検査し、画像と PDF は見える内容から作り直す
開ける添付ファイルを、対応するテキスト、画像、PDF、Word・Excel・PowerPoint 形式に限定します。開く前や保存する前には、対応するウイルス対策ソフトで検査します。画像と PDF は表示される内容から作り直したファイルを開き、細工された元のファイルを直接開くことによるリスクを抑えます。

3. メールを読み解く処理を分離し、攻撃の影響が広がるリスクを抑える
添付やリンクをクリックしなくても、メールを読み込む処理が攻撃の入口になる場合があります。利用者の操作を必要としない攻撃は「ゼロクリック攻撃」、修正プログラムが提供される前の弱点を突く攻撃は「ゼロデイ攻撃」と呼ばれます。SuperCRM_Mail では、メールを読み解く処理を、ほかのファイルや機能へのアクセスが制限された環境で動かします。処理の弱点を突かれた場合にも、PC 内の情報に被害が及ぶリスクを抑えるための仕組みです。

4. 警告の理由が分かる
差出人やリンク先などの確認結果を緑・黄・赤で表示し、警告の理由も確認できます。信頼する差出人として登録した取引先のメールにも、リンク先の確認と添付ファイルの制限・検査を適用します。

5. 生成 AI にコピーするときは、隠れた文章を取り除く
メール本文や対応する添付から、画面に見えないように設定された文章や一部の不可視文字を除いたコピーを作ります。利用者は除いた内容を確認できます。コピーには、メール中の命令を利用者本人の指示として扱わないよう求める注意文も添えます。

■組織向け「SuperCRM_Mail Business」
2027 年 1 月に提供予定の有料版では、管理者が組織専用の許可リストとアプリの更新を各 PC にまとめて配布できます。PC ごとに設定や更新を行う手間を減らし、組織全体で共通の安全対策を運用しやすくします。
・組織専用の許可リストを作成し、各 PC に一括配布
・アプリと許可リストを、更新用のインターネット接続を使わず組織内ネットワークで更新
・利用状況と動作記録を収集し、管理者が確認
　これらの管理機能を利用するには、組織内に管理用サーバーが必要です。

■製品概要
・製品名
　SuperCRM_Mail（スーパーシーアールエム メール）
・公開予定
　2026 年 12 月
・無料版
　広告・アプリ内課金なし
・組織向け有料版

SuperCRM_Mail Business（2027 年 1 月提供予定）

・対応 OS

Windows 10・Windows 11（64 ビット）

・必要なソフト

.NET 10 Desktop Runtime、Microsoft Edge WebView2 Runtime

・メモリー

4GB 以上

・対応するメール

POP3・IMAP・SMTP、Microsoft 365／Outlook.com（OAuth 2.0 認証）、Gmail。
（Gmail は 2027 年 1 月対応予定）

・製品ページ

https://www.super-crm.co.jp/scmail.html

■今後の展開

初年度の売上目標は 5 億円です。上場企業や官公庁を中心に導入を進めます。
今後は、送信者から受信者までメールの内容を暗号化して保護する「エンドツーエンド暗号化（E2EE）」と、多言語対応を予定しています。

■会社概要

会社名　有限会社スーパーシーアールエム
代表　　國信 正直
設立　　2002 年 8 月
所在地　〒214-0003
神奈川県川崎市多摩区菅稲田堤 2-1-8
事業内容
　コンピュータ・ソフトウエア、ハードウエアの開発・製造・販売、コンピュータを用いた情報処理・情報提供サービス業
主な製品
　コールセンターシステム「SuperCRM」、電子メール配信システム、ヘルプデスク受け付け用電話自動応答システム
URL　　https://www.super-crm.co.jp/

■本件に関するお問い合わせ

有限会社スーパーシーアールエム　担当：国信
報道関係の方：pr@super-crm.co.jp

製品・導入について：sales@super-crm.co.jp
電話：044-945-8284
記載の会社名・製品名は、各社の商標または登録商標です。