第494号　2026年8月1日発行

ワンポイント通信

ワンストップで安心サポート
PARTNER'S PROJECT
(株)パートナーズプロジェクト®

E-mail pro@3d-m.jp　Web https://www.3d-m.jp/
TEL 0258-36-2685　FAX 0258-35-2820

＜コラム＞　次ページにて、💬についてより詳しくご紹介しています。

なぜ地方の中小企業が不正アクセスの脅威にさらされるのか?
それは、悪意ある第三者がセキュリティの強固な大企業などを狙う際の「踏み台」として利用しやすいからです。

※内容のご質問等については、TEL 0258-33-8836　担当　㈱ネオス　小野塚　まで
※配信中止等のお問い合わせは、ホームページ　https://www.3d-m.jp/contact/others/

開催セミナーのご案内　●無料セミナー●対面セミナー形式にて開催

令和8年8月28日（金）　時間：15：00～17：00　会場：パートナーズＰＬＡＺＡ

内容『「人を増やす」ことは難しい。だからこそ、今すべきこと！』　講師：株式会社ＧＦＮ 五味由紀子

少子高齢化による人材不足が深まる中、「採用」だけに頼るのではなく、今いる社員が安心して意見を交わし、主体的に力を発揮できる職場づくりが企業の成長には不可欠です。本セミナーでは、心理的安全性とハラスメント防止の観点から、社員の主体性を引き出し組織力を高める職場づくりについて、具体事例を交えながら一緒に考えていきます。

2026 年 6 月、KDDI が運営するレンタルサーバーサービスが不正アクセスを受け、計 1,700 万件以上の電子メール関連情報が漏えいする事案が発生しました。こうした不正アクセス事案は大企業だけが狙われるわけではありません。
中小企業も強固な大企業などを狙う際の「踏み台」として利用するために、悪意ある第三者に狙われています。

「踏み台」（サプライチェーン攻撃）とは？

「踏み台」とは、セキュリティが甘い企業を“中継地点”にして、本命である取引先の大企業などへ侵入する攻撃手法です。
自社が被害を受けるだけでなく、知らぬ間に「他社を攻撃する加害者」に仕立て上げられてしまうのが、この「踏み台」の恐ろしさです。

踏み台にされる原因 2 選

1. **巧妙なスパムメールによる「アカウント情報の盗取」や「マルウェア感染」**
   スパムメールの偽リンクや添付ファイルは、アカウント情報の盗取・マルウェア感染の原因になります。スパムメールは単なる迷惑メールではなく、「アカウントを盗むトラップ」「PC を遠隔操作するための侵入口」として悪用されます。
2. **アカウント管理の甘さやネットワーク機器の放置**
   パスワードの使い回しや、セキュリティが古くなったネットワーク機器（ルータや VPN）の放置が踏み台にされる大きな要因です。建物に例えると「鍵の管理が甘い」「勝手口の壊れたドアを放置している」ような状態です。

対策①　メールは名前ではなく「メールアドレス」をよく確認！

メールの送り主の名前は容易く偽装できます。しかし、メールアドレス自体を偽装するのは難しいです。
送り主のアドレス「例:〇〇〇〇@example.com」の部分をよく見て、正規のメールであることを確認しましょう。

対策②　パスワードや機器の定期的な更新

各種アカウントのパスワードは推測されにくい複雑なものへ定期的に変更し、VPN 機器やルーターは常に最新のソフトウェアへ更新しましょう。セキュリティの穴（脆弱性）を放置しないことが侵入を防ぐ基本です。

AI などの便利な技術が悪用され、サイバー攻撃の手口は日々進化しています。
「自社が攻撃の踏み台になるリスク」を他人事と捉えず、定期的なセキュリティの見直しで安全な IT 運用を徹底しましょう。