

企業を狙った不正アクセスが相次いでいます！

あなたの会社の「侵入口」、放置されていませんか？

1 最近の主な不正アクセス事案（国内）



通信・小売関連



外食関連



教育機関



サービス業・その他

不正アクセス等による情報漏えいは様々な業種で発生しており、今後も発生が懸念されます

2 狙われるのは、こんな「隙」です。



古い機器・ソフト

- ・OSやソフトウェアの更新が未実施
- ・VPN機器等の脆弱性



弱い認証

- ・パスワードの使い回し
- ・多要素認証の未導入
- ・不要アカウントの放置



公開システムの脆弱性

- ・Webサイト、ECサイトの脆弱性
- ・リモートアクセス機器の脆弱性
- ・クラウド設定の不備



取引先・委託先

- ・取引先との接続環境
- ・サプライチェーンを狙った攻撃

3 今すぐ確認をしてください。



OS・ソフトウェア・VPN機器などは最新の状態で



不要なアカウント・ポート・サービスを停止しているか



インターネット公開機器に既知の脆弱性が残っていないか



不審なログインや通信を確認できるようログを取得・監視しているか



管理者・VPN・クラウドサービスに多要素認証を設定しているか



バックアップを取り、ネットワークから切り離して保管しているか

どの企業でも「侵入される可能性がある」

ということを前提に各種対策をお願いします！

