2025 年 10 月 31 日

【最重要】ランサムウェア等サーバー攻撃の脅威増大と セキュリティ対策の再徹底について

平素より当協会の運営にご理解、ご協力いただきありがとうございます。

報道等でご存知のとおり、昨今、国内外でランサムウェア（身代金要求型ウイルス）によるサイバー攻撃の被害が急増しており、システム停止や機密情報・個人情報漏洩といった甚大な被害が現実のものとなっています。他社様が受けた攻撃事例は、決して対岸の火事ではありません。

特に業務で利用する PC やサーバがマルウェアに感染した場合、**被害は社内全体さらには会員会社や取引先にまで連鎖的に及ぶ可能性**があります。**各社情報セキュリティ部門等にて対応中とは思いますが、全従業員一人ひとりが「最後の砦」として危機感を持ち行動することが求められています。**

1 . 日常業務における情報セキュリティ徹底事項の再確認

特に以下の点について再確認と**厳守**をお願いいたします。

【最重要】不審なメールや Web サイトへの対処ルールの徹底

・**送信元が不明、件名の内容に不審**な点があるメールは、**絶対に開封しないでください。**

・業務上必要な場合を除き、添付ファイルやメール本文中の **URL は絶対にクリック・実行しない**でください。

・業務に関係のない**件名や内容、請求書・注文書などを装っていてもの、少しでも不審に感じた場合は、即座に自社の情報セキュリティ部門等へ報告・相談**してください。

【必須】パスワードの適正な設定と管理の徹底

・システムへのログインパスワードは、**定期的な変更**を行い、**使い回しをしない**でください。

・**複雑なパスワードを設定**してくさい（最低でも 10 文字以上、「@」、「%」、「“」などの記号やアルファベットに大文字と小文字も混ぜる等）

※政府広報：https://www.gov-online.go.jp/useful/article/202210/2.html

【情報資産の適切な管理の徹底】

・社外秘の情報や個人情報を含むデータは、**自社で指定された場所**で適切に管理し、**無断での持ち出しや私的な利用は禁物**です。

2.万が一、不審な事象を確認した場合の対応（インシデント発生時）

【緊急対応】不審な事象を確認したら、すぐに報告・連絡

・**不審なメール**を開いてしまった、「**ウイルス感染が疑われる**挙動（ＰＣの動作が異常遅い、見覚えのないファイルがあるなど)」、**不正アクセス**の兆候を発見した場合は、**決して自己判断せず、**直ちに自社の情報セキュリティ部門等にご報告ください。

・各社のセキュリティルールに応じて、**ネットワークケーブルを抜く**など、被害拡大を防ぐための**一時的な対策（隔離）**が求められる場合があります。

※警察庁：https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html

会員各社一人ひとりのセキュリティ意識と行動が、通建業界全体の情報資産を守る**最も重要な防壁**となります。

ご多忙とは存じますが、本注意喚起の内容を熟読・理解し、より一層の情報セキュリティ意識の向上にご協力いただきますよう重ねてお願い申し上げます。

令和７年１０月３１日

一般社団法人 情報通信エンジニアリング協会

専務理事 海老根　崇