FOL IT レター

2020-3 号

点検しましょう！
（有）フロンティア・オンライン
TEL:0242-37-0758

IT 脅威、 どこまで備えている？

近年、 IT の先進的な活用を誤り、 データを損失したり、 漏えいするケースが増えております～

～ 2019 年１０大脅威～

1 位	標的型攻撃による被害
2 位	**ビジネスメール詐欺による被害**
3 位	ランサムウェアによる被害
4 位	サプライチェーンの弱点を悪用した攻撃の高まり
5 位	内部不正による情報漏えい
6 位	サービス妨害攻撃によるサービスの停止
7 位	インターネットサービスからの個人情報の窃取
8 位	IoT 機器の脆弱性の顕在化
9 位	脆弱性対策情報の公開に伴う悪用増加
10 位	**不注意による情報漏えい**

どんな人にメール詐欺が多い？

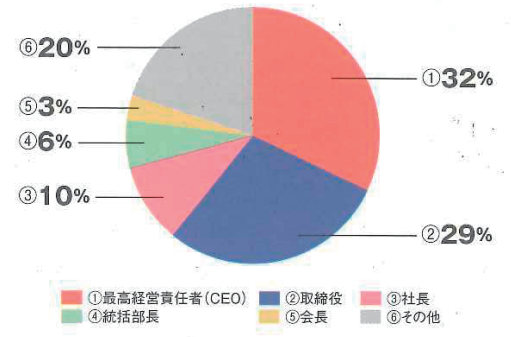

図 1-1-3 ビジネスメール詐欺関連のなりすましに利用された職位の割合
(出典)トレンドマイクロ社「2018 年年間セキュリティラウンドアップ」を基に IPA が作成

【被害者の８割】
経営者・上層幹部

【Tips】
特に中小企業は経営者がご自身で重要な情報を抱えることが多いことに注意。

情報漏えいの原因

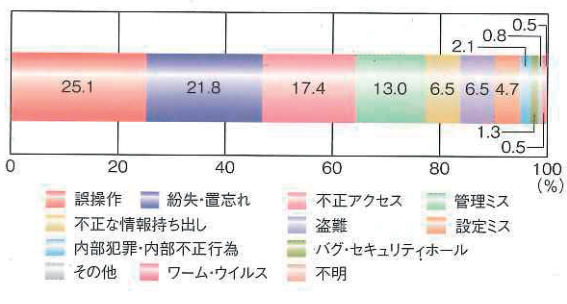

図 1-2-29 漏えい原因の比率(n=386)
(出典)JNSA 調査報告書を基に IPA が作成

【８割対策漏れ】
多くの原因が安全対策への取り組み・意識が要因

【Tips】
設備、 技術導入も大事だが、 リテラシーはもっと重要

多様化する IT 活用

・PC、 スマホ、 タブレット
・NAS、 サーバ、 データセンタ、 クラウド

～ IT 活用の利便性と安全性は相反傾向～

・利便性を早急に求め、 安全対策は後手
　⇒脆弱性を自身で広げる結果
　⇒重要データがどこまで広域化しているか分からない
・セキュリティへの意識は高、 データ保全性への意識は低
　⇒漏えい防止はできたが、 データを欠損

現状把握と運用ルール

～企業の個性、 現状を把握した上、 IT 活用ルールを決めましょう～

１）利便性
２）漏えい防止
３）情報損失対策

～ UTM（総合脅威管理）～
対策ソフトは導入済みだけど、 いるの？
　⇒推奨、 脅威対策は多重化

情報セキュリティ自己診断 - 診断のための 25 項目

～ IPA　中小企業の情報セキュリティ対策ガイドライン第３版より～

	実施済み	一部実施	未実施	不明
基本的対策 - 5 項目				
1）パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？				
2）パソコンやスマホなどにはウイルス対策ソフトを導入し、 ウイルス定義ファイルは最新の状態にしていますか？				
3）パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？				
4）重要情報※1 に対する適切なアクセス制限を行っていますか？				
5）新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？				
※1) 営業秘密など事業に必要で組織にとって価値のある情報や顧客や、 従業員の個人情報など管理責任を伴う情報のこと				
従業員としての対策 - 13 項目				
6）電子メールの添付別ルや本文中の URL を介したウイルス感染に気をつけていますか？				
7）電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？				
8）重要情報は電子メール本文に書くのではなく、 添付するファイルに書いてパスワードなどで保護していますか？				
9）無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？				
１０）インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？				
１１）パソコンやサーバのウイルスルス感染や誤操作による重要情報の消失に備えてバックアップを取得していますか？				
１２）紛失や盗難を防止するため、 重要情報が記載された書類や電子媒体は机上に放置せず、 書庫などに安全に保管していますか？				
１３）重要情報が記載された書類帽子媒体脱出す時は、 盗難や紛失の対策をしていますか？				
１４）離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？				
１５）関係者以外の事務所への立ち入りを制限していますか？				
１６）退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？				
１７）事務所が無人になる時の施錠忘れ対策を実施していますか？				
１８）重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、 復元できないようにしていますか？				
組織としての対策 - 7 項目				
１９）従業員に守秘義務を理解してもらい、 業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？				
２０）従業員にセキュリティに関する教育や注意喚起を行なっていますか？				
２１）個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？				
２２）重要情報の授受を伴う取引先との契約書には、 秘密保持条項を規定していますか？				
２３）クラウドサービスやウェブサイトの運用等で利用する外部サービスは、 安全・信頼性を把握して選定していますか？				