

サイバーセキュリティ関連情報（2月号）

鳥取県警察本部サイバー犯罪対策課



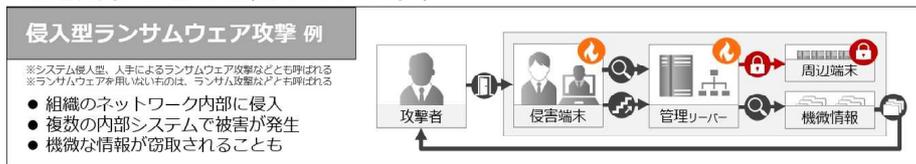
○ もしもランサムウェア攻撃を受けてしまったら？

世界各地でランサムウェア攻撃による被害が拡大しており、国内では医療機関などで一部業務の停止を余儀なくされる大規模な被害に至るケースも確認されています。

JPCERTコーディネーションセンターでは、ランサムウェア攻撃を受けてしまった場合の初動対応を支援する資料「侵入型ランサムウェア攻撃を受けたら読むFAQ」を公式HPで公開しています。

もしもランサムウェア攻撃を受けてしまった際、「復元できるのか?」「身代金を払ってもいいのか?」などの様々な疑問や初動対応の手順などについて解説された資料が少なくないことを受け、同センターが実際のインシデント対応を支援してきた知見を活用し、詳しく取りまとめたものです。

具体的には、被害発生への報告、状況把握、対応方針や原因の対処、システムの復旧などのポイントについて、FAQ (Frequently Asked Question: よくある質問) 形式で解説されており、企業や組織におけるインシデント対応を進める上での参考情報として活用することを促しています。



※ 侵入型ランサムウェア攻撃： 企業や組織の内部ネットワークに攻撃者が侵入した後、情報窃取やランサムウェアを用いたファイルの暗号化などを行う攻撃



引用 JPCERTコーディネーションセンター <https://www.jpcert.or.jp/magazine/security/ransom-faq.html>

○ 鳥取県警察におけるサイバー相談受案件数が過去最多！

鳥取県警察において、令和3年中に受理したサイバー犯罪に関する相談件数が、過去最も多かった平成29年中の1,703件を上回る1,793件で過去最多を更新しました。

新型コロナウイルス感染症に関連した相談の増加が、過去最多となった大きな要因となっており、特に、サポート詐欺や架空請求、偽通信販売サイト、新型コロナウイルス便乗などの詐欺・悪質商法に関する区分が967件で全体の半数以上を占めています。

また、コロナ禍における生活スタイルの変化等に伴うインターネットの利用が増加していることにより、名誉棄損・誹謗中傷等、不正アクセス・コンピュータウイルス、迷惑メール・スパムメールの3つの区分において、いずれも過去5年間で最も多い件数となっています。

今年に入ってから、鳥取県内では、パソコンのウイルス除去名目によるサポート詐欺、有料サイトの登録取り消しなどの名目による架空請求詐欺がそれぞれ発生しており、いずれも犯人からコンビニで電子マネーの購入を求められ、電話で番号を伝えて騙し取られる手口による被害となっています。

また、知らない間に第三者がインターネットバンキングを勝手に申し込み、預金を盗まれそうになったという相談も複数件受理しています。

いずれも金融機関の職員を名乗る者から、「保険料の払い戻しがあるが、コロナの影響で窓口対応ができないため、口座振込する。」などと電話があり、聞き出した口座情報を基にインターネットバンキングの申込みをして、相談者の預金を犯人の口座に送金するという新手の手口であり、今後も注意が必要です。

警察や役場、銀行などの職員が、口座情報や暗証番号を直接、聞くことはありません。

電子マネーや口座等の情報を伝える前に、一旦電話を切り、家族や警察にご相談下さい。

区分	H29	H30	H31(R1)	R2	R3
詐欺・悪質商法	1,363	1,017	694	729	967
インターネットオークション	45	31	23	10	17
名誉毀損・誹謗中傷等	129	127	112	150	166
不正アクセス・コンピュータウイルス	88	47	73	142	178
迷惑メール・スパムメール	33	53	87	60	174
その他	45	81	171	299	291
合計	1,703	1,356	1,160	1,390	1,793

参考 鳥取県警察HP <https://www.pref.tottori.lg.jp/270500.htm>