事　務　連　絡
平成 28 年４月 21 日

各府省庁情報セキュリティ担当課室長 殿

内閣官房 内閣サイバーセキュリティセンター
内閣参事官（政府機関総合対策担当）

ランサムウエアへの対処について（注意喚起）

最近、ランサムウエアと呼ばれる不正プログラムが、メールや不正サイト等によって広範に送り付けられているとの分析があります（※１）。

この不正プログラムに感染した場合の挙動としては、感染端末や接続されているサーバのファイルを暗号化して読み取れないようにしてしまい、その上で攻撃元からは情報を取り戻したければ身代金（ランサム）を払え、場合によっては身代金を払わなければ暗号化して人質に取った情報を勝手に公開する、などとして脅すのが主なものです。未知の脆弱性を利用し、セキュリティ製品等では検知・駆除不可なものも存在します。もちろん、身代金を払ったとしても攻撃元が情報を正常な状態に戻す、又は外部に公表しないといった行為をとる確証は全くありません。

これら不正プログラムによる被害を最小化するためには、

・ＯＳやソフトウェアを常に最新版に保つこと
・多量のデータが格納されているサーバ等の被害を抑えるために、定期的にバックアップをとり、バックアップデータはインターネットから隔離しておくこと

その他のいわゆる標的型攻撃への対策が有効です。

なお、政府機関等の端末がこの不正プログラムに感染する場合、業務継続が不能となる、内部情報が窃取される、攻撃を受けたことが外部に知られ容易に攻撃が成功する組織として認知されるといった悪影響が主に考えられます。

各府省庁におかれましては、職員にこうした脅威の顕在化についてお知らせの上、基本的な注意や動作（不審なメールの添付ファイルを開いたりリンクをクリックしたりしない、業務に関係ないサイトの閲覧をしない、不審に気づいた際は府省庁内連絡窓口に報告する）を改めて促していただくともに、最近のランサムウエアによる感染についても脅威として想定した上で対策を再検証し、不測の事態に備えるようお願いいたします。

＜参考＞

・独立行政法人情報処理推進機構(IPA)
　https://www.ipa.go.jp/security/txt/2016/01outline.html
※１　https://www.ipa.go.jp/security/topics/alert280413.html
・JPCERT コーディネーションセンター
　https://www.jpcert.or.jp/pr/2016/pr160002.html

問合せ先
内閣官房内閣サイバーセキュリティセンター
政府機関総合対策グループ　眞弓・久保山
03-3581-3959