かごしまサイバー通信

令和６年１月15日
鹿児島県警察本部
サイバー犯罪対策課
TEL　099-206-0110

Ransomware（ランサムウェア）高水準で推移中

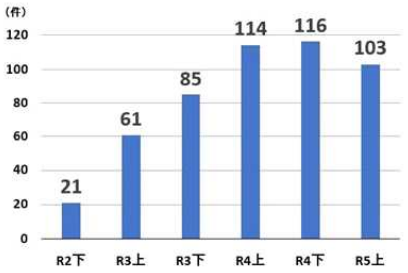
１．現状

◎　令和５年上半期中に警察庁に報告された国内のRansomwareによる被害件数は，103件となっています。

◎　サプライチェーン攻撃等により，企業，団体等の規模やその業種等を問わず，広範に及んでいます。

◎　「二重恐喝」という手口が全体の78%と主流となっています。
「二重恐喝」は，従来の「暗号化したデータに対する身代金の要求」に加えて，「盗んだデータの公表」を盾に脅迫し，金銭を要求する手口です。

◎　感染経路は，VPN機器等や強度の弱い認証情報等が設定されたリモートデスクトップサービスが多くを占めています。



企業・団体等におけるRansomware被害の警察に対する被害報告件数

出典：警察庁「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」

２．Ransomwareとは

◎　Ransomwareとは，「Ransom（身代金）」と「Software（プログラム）」を組み合わせた造語で，マルウェア（不正なプログラム）の一種

◎　Ransomwareは１年間だけでも数百種類確認されており，現在も新しい種類が作られています。

◎　対策が不十分な場合，復旧に長期間を要する場合があり，データを復元できない場合もあります。

出典：出典元:ﾋﾞｼﾞﾈｽ＋ IT(https://www.sbbit.jp/article/cont1/65631)

３．被害の未然防止対策

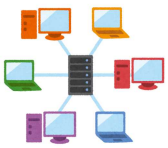
(1)　電子メール等への警戒

攻撃者は，受信者の関心を引くような内容や重要と思わせる内容のメールを用いて添付ファイル開かせる。

添付ファイルやURL付きのメールについては，送信元に確認をとる。

(2)　VPN機器等のぜい弱性対策

OSやソフトウェアにぜい弱性がある状態のままでは，電子メールの添付ファイルの実行やウェブサイトの閲覧により，マルウェアに感染するリスクがあるため，利用している機器やOS等の更新ファイル，パッチ等を適用してぜい弱性を残さないようにする。



(3)　ウイルス対策ソフト等の導入

ウイルス対策ソフトを導入し，定義ファイルを最新状態に更新する。

ネットワークへの侵入を許してしまった場合に，不審な動作を検知し，被害を最小限に食い止めるため，EDR（Endpoint Detection and Response）の導入も検討する。

(4)　認証情報の適切な管理

パスワードの場合は，大文字・小文字・数字・記号の組み合わせにより文字数が多く，推測されにくい文字列を設定するとともに，他のサービス等で使用していないものを設定し直すなど認証情報を適切に管理する。

また，２要素認証等による強固な認証手段の導入や，IPアドレス等によるアクセス制限と組み合わせるなどの対策も検討する。

4．感染に備えた被害軽減対策

⑴　データのバックアップ等の取得

不測の事態に備えて，バックアップをなるべくこまめに取得し，ネットワークから物理的に切り離して保管する。

また，日頃からバックアップデータによるシステムの復旧手順を確認しておく。

⑵　アクセス権等の権限の最小化

ネットワークに侵入された場合の被害を抑えるため，ユーザーアカウントに与える権限やアクセスできる範囲を各人の必要最小限にする。

⑶　ネットワークの監視

ランサムウェアを含め，マルウェア等に感染した端末では，外部のサーバーとの間で不審な通信が発生する場合がある。

EDR等を導入し，ネットワーク内の不審な挙動や外部との通信を監視することで，感染拡大や外部からの侵入の範囲拡大を阻止することにつながる。

5．感染時の対応方法

⑴　ネットワークから端末を切り離す。

端末を接続したままでは被害が拡大してしまうため，全ての端末機器のLANケーブルを外し，Wi-Fiをオフにする。

⑵　端末の電源は切らない。

電源を切ってしまうことで，メモリに記録されている情報が消えてしまい，データの復号（復元）が困難となる場合があるため，電源は切らない。

⑶　身代金の支払いをしてもデータ復元の保証は一切ない。

身代金を支払ったとしても，ランサムウェアが機能していると犯罪者に対して証明するだけであり，データが復元される保証は一切なく，将来的に再びターゲットにされる可能性がある。

⑷　システム関係者に報告，警察へ相談・通報する。

被害の拡大を防ぐためにも，システム担当者や委託先セキュリティベンダーに速やかに報告する。

最寄りの警察署やサイバー犯罪対策課に相談・通報することで，多くの情報が集約され，より効率的に犯罪組織の活動を阻止することができる。

6．専門サイトについて

◎　「No More Ransom（ノーモアランサム）」プロジェクト

「No More Ransom」プロジェクトは，欧州刑事警察機構，オランダ警察等により，2016年７月に設立された，Ransomwareの被害低減を目指す国際的なプロジェクトです。

同プロジェクトは，Ransomwareの危険性と対策に関する情報，無料復号ツールやQ&Aなど，Ransomwareの被害者に役立つ情報を公開しています。

事前対策としても有用なので，是非，ご活用ください。

出典元:No More Ransom(https://www.nomoreransom.org/ja/index.html)

アドレスは「https://www.nomoreransom.org/ja/index.html」です。