（公開資料）

資料２－１

不正アクセス事案に関する報告（最終報告）（概要）

令和３年９月８日
原 子 力 規 制 庁

１．経緯

令和２（２０２０）年１０月２６日、外部からの攻撃と思われる不正な通信を検知し、原子力規制委員会ネットワークシステム※（以下「システム」という。）の一部サーバに侵入された痕跡が認められたことから、速やかにシステムの外部とのアクセスを遮断した。

以降、内閣サイバーセキュリティセンター等の協力を得て、不正アクセスの状況等に関する調査を実施した。

※　原子力規制委員会全職員が利用する情報システムであり、電子メール、ファイル共有等のサーバ及びパソコン、複合機、プリンタで構成されている

２．調査結果

（１）不正アクセスの状況

令和元（２０１９）年８月から９月の間、ＶＰＮ装置の脆弱性を突く攻撃手法によりシステム内に侵入され、職員及び請負業者の認証情報を窃取された。

令和元年９月及び令和２年３月、窃取された認証情報を利用してシステム内に侵入し、偵察された。

令和２年１０月、窃取されたと思われる認証情報を利用してシステム内に侵入し、データを窃取された。（窃取されたデータは、システムを構成する一部サーバの設定ファイルや職員及び請負業者の認証情報の可能性があるが、特定できなかった。）

（２）データ漏えいの状況

不正アクセスに使われた職員及び請負業者の認証情報を除き、職員の作成した職務に係る文書等のデータが漏えいした痕跡は、遡っての調査が可能な範囲において確認されなかった。

なお、核物質防護に係る情報については、完全に分離された別のネットワークシステムで管理されているため、システムへの不正アクセスの影響を受けなかった。

（３）外部との不審な通信の状況

システムと外部とのアクセス遮断以降、利用者の操作を伴わない不審な外部への接続試行がないことを確認した。

３．今後の方針

必要なセキュリティを確保した上で職員用の一部サービス（１月１８日にテレワーク用のサービス、３月２３日に外部サーバを利用する暫定的なメールサービス）を再開した。調査が可能な範囲での解明に留まるため、全面的なサービスの復旧は次期システム（令和４（２０２２）年１月稼働予定）の稼働をもって行う。

今後の再発防止策として、次期システムにおいて本事案を踏まえたセキュリティ対策を強化するとともに、情報セキュリティ体制の充実を図ることとする。