

## 不正アクセス事案に関する報告（中間報告）（概要）

令和3年5月20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、現時点では確認されていない。

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. 今後の方針

引き続きデータ漏えいの有無に関する調査を実施する。

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）を再開したが、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。