原子力規制委員会了承文書
（2016FY-19）
平成28年5月18日
（議題1資料1-3）

公益財団法人核物質管理センターにおける情報セキュリティ対応の不備について

平成28年5月18日
原 子 力 規 制 庁

1．経緯

原子炉等規制法に基づく指定保障措置検査等実施機関及び指定情報処理機関である公益財団法人核物質管理センター（以下「センター」という。）において、平成27年8月及び9月、インターネットを通じた意図しない通信の発生又はその試みが確認されていた。当該事象は原子炉等規制法に基づき、指定機関としてセンターが認可を受けている「指定保障措置検査等実施機関業務規定」及び「指定情報処理機関業務規定」（以下「業務規定」という。）に規定する事項の詳細を定めた内部規程に従って、速やかに原子力規制庁に報告すべき事象であったが、センターはその報告を怠っていた。

本事案は、平成28年1月15日に原子力規制庁が外部からの指摘を受け、センターに事実関係を確認したところ判明した。原子力規制庁は、同年1月27日に、同25日にセンターから報告された事案の顛末、それまでの原因究明及び対応について評価した上で、センターへの対応について原子力規制委員会に諮った。原子力規制委員会は、センターが業務規定及び下位規定である内部規程に違反し、使用が許可されていないソフトウェアを情報ネットワークシステム内にインストールしたこと、情報流出が発生したこと、及び当該事象について原子力規制委員会に対する報告を怠ったことについて厳重注意を行うとともに、本事案に関して、

① センターの情報ネットワークシステムにおける他の情報流出及び意図しない外部通信が同システムに与えた影響の有無に対する調査・検証

② 本事案及び①の調査・検証の結果発覚した事案について、センターにおける情報ネットワークシステム及び情報セキュリティ管理体制の問題を含めた原因究明

③ 上記②の結果を踏まえた課題の抽出及び再発防止対策の策定・実施

を指示し、本年3月31日までに報告することを求めた。

センターからは本年3月31日に報告書が提出され、その後内容を追加・修正した補正版が本年5月12日に提出された。

本件は、これを受けてセンターから原子力規制庁に対して提出のあった報告に対する原子力規制庁としての評価を原子力規制委員会に報告するとともに、今後の対応について諮るものである。

２．センターの報告書の概要

（１）調査・検証

理事長を総括責任者として、センター内に対応体制を設け、意図しない外部通信の発生、情報システム内のマルウェアの存在及びシステム管理者権限の流出等の有無について、外部の情報セキュリティ専門会社の支援を受けて調査を実施した。

情報セキュリティ専門会社による常時監視、センター内に設置されていた統合脅威管理機器等の監視システムによる意図しない外部通信の検知結果をもとに、通信制御機器等の記録、当該通信の発生が確認された業務用端末の調査、情報セキュリティ専門会社が把握している脅威度の高い通信先との照合等及び同調査の過程で判明したその他の情報セキュリティ上の問題に係る検証を通じて、以下の調査結果を得た。

①情報流出について

常時監視及び統合脅威管理機器等による監視によって、ファイル共有ソフトに起因する可能性があると識別された通信のうち、通信制御機器等の記録による照合が可能な通信に対し調査・検証を行うとともに、職員への聞き取り等を行った。その結果、センターの情報ネットワーク内にインストールされたファイル共有ソフトによって発生したとの確定的な結論が得られた通信は、本年１月２７日に原子力規制委員会に報告を行った六ヶ所保障措置センターの業務用端末から発生した通信のみであった。ただし、事象確認後の調査において証拠保全に考慮が至らず、当該業務用端末を初期化してしまった等の影響から、当該通信により流出した可能性がある情報の特定には至らなかった。事象発生時のセンターの情報システム環境から判断して、追加的な調査によって新たな情報が得られる可能性は極めて低い。

識別されたその他の通信については、通信制御機器等の記録による照合では、通信内容の確定に至らないものも多く、現時点で情報流出の可能性が完全に否定できないものもあるが、情報セキュリティ専門会社からは、ウェブ閲覧やメール通信等、ファイル共有ソフトに起因するもの以外の通信を誤検知した可能性が高いとの報告を受けている。また、ファイル共有ソフトによるものとして検知された通信を発生させていた一部の業務用端末の通信記録や状態を詳細に調査した結果、調査可能な範囲においては、ファイル共有ソフト等不正なソフトウェアの存在や実行、情報流出の痕跡は認められなかった。

通信制御機器等の記録と情報セキュリティ専門会社が把握している脅威度の高い通信先との照合の結果、これらの通信先への通信が複数確認された。これらの中にはウェブ閲覧情報を外部に送信するソフトウェアからのものと思われる通信等が含まれるが、通信元として特定された業務用端末の通信記録や状態の詳細な調査や、ウイルス対策ソフトによるクロスチェックの結果、センターの保有する情報が流出した痕跡は認められなかった。

②情報システムの健全性について

ウイルス対策ソフトのスキャンで、新たにウイルスが検知／隔離されたが、悪意のある不正なソフトに感染したことを示す通信は検知されていない。また、情報セキュリティ専門会社からは、権限管理サーバの詳細調査の結果、管理者権限が流出した形跡はなく、代理サーバ設置後の通信記録の検証の結果等からも、現時点で情報ネットワークシステムは健全な状況にあるとの報告を受けている。

③その他の情報セキュリティ上の問題について

平成２７年１月、常時監視の開始以前から稼働していた監視システムでファイル共有ソフトによる通信の疑いのある通信が検知され、センター内で業務連絡書により対処を指示していた事案があった。また、平成２７年２月、計算機室のサーバが悪意のある外部のコンピュータにより、別の外部のコンピュータを標的とする攻撃の踏み台として使われていた事案もあった。これらは業務規定に基づく内部規程に従い、流出した可能性のある情報の把握や原子力規制庁への報告を行うなどの対応を要する事案であったが、これらの対応を怠っていた。

（２）原因究明

まず、一連の情報セキュリティの不備についての調査・検証の結果又はその過程で得られた情報から具体的に問題のあった点を抽出した。次に、それらの問題点から情報システムの技術的要因を抽出し、最後に情報システム上の問題の背景ともなっているセンターの組織的要因の側面から、本事案に至った原因を究明しており、その結果は以下のようにまとめられる。

① ソフトウェアの扱いや情報管理に関する規程の内容や運用に不備があるほか、不明確な指揮命令系統が存在しているなど、情報セキュリティ体制が不十分であった。

② 使用が認められていないソフトウェアのインストールや脅威度の高いウェブサイトへの通信を物理的に遮断するシステムを備えていないなど、情報セキュリティシステムそのものが脆弱であった。

③ 情報セキュリティ担当部局の能力不足、マネジメントによる資源配分や問題発生時の対応が不適切であり、組織としての情報管理の重要性の認識や情報セキュリティに対する意識や能力に不足があった。

その上で、これらの根源的な要因が、管理すべき情報に対する情報セキュリティ上のリスクに対応するという問題に真摯に向き合ってこなかったことと特定している。

（3）再発防止策

原因究明の過程で特定した技術的、組織的要因を踏まえ、以下の再発防止策を策定し、情報セキュリティ対策の強化に組み込むことで、新たな情報システムを構築し、厳格に運用する。

①情報セキュリティ体制の強化

- 抽出された組織上の問題、マネジメント上の課題に対応するため、外部有識者からなる第三者委員会を設置し、問題点の検証と再発防止策の実効性の評価を行うとともに、外部専門技術者を活用した情報セキュリティ運用・管理担当組織の設置や、理事長を最高責任者とした非常時対応体制の構築等、組織体制を整備する。
- 情報セキュリティマネジメントシステムを導入し、明確な規程、手順を整備するとともに、継続的な情報セキュリティ管理体制とセキュリティ対策の見直し・改善を図り、早期に情報セキュリティに係る国際的な認証を取得できるレベルに達するよう組織能力を高める。

②情報セキュリティシステムの強化

- 管理情報等の格付けと明確化を行うとともに、一般情報を取り扱うネットワークから物理的に隔離し、情報流出のリスクを低減する。
- 使用が認められていないソフトウェアのインストールや脅威度の高いウェブサイトへの通信を物理的に遮断するシステムの導入、端末やサーバへのアクセス権限や情報資産の集中管理化により、個人の判断や裁量による情報流出のリスクを低減する。

③ 情報セキュリティの意識改革と行動の徹底

- 最新のサイバー攻撃の情報収集を行い、情報セキュリティ専門会社から入手した対処方法等を組織内で速やかに周知徹底する。情報共有は理解しやすい内容とし、周知徹底事項の履行確認を行う。
- 体系的な教育訓練を通じて、情報セキュリティの重要性と情報管理に係る責任感への意識改革を図り、情報セキュリティに係る個々の対応能力を向上させる。
- 高い情報セキュリティ意識と知見を持ち、外部専門家の知見を組織内に展開・定着させる能力を備えた情報セキュリティ担当者を養成する。

３．報告書に対する原子力規制庁としての評価

（１）調査・検証

①調査方法について

情報セキュリティ専門会社の支援を受けて、センターに設置されていた統合脅威管理機器等の情報、並びに通信制御機器及び代理サーバに残された記録の分析及びその結果から意図しない通信の発生が検知された一部の端末について詳細な調査を実施し、確認が必要なものについては対象職員に聞き取りを実施している。また、情報セキュリティ専門会社の支援を受けて、センターに存在する端末の権限管理サーバについての詳細な調査を実施したとしており、これらの調査方法は妥当であると考える。

②調査結果

事象発生時のセンターの情報セキュリティ環境及び事象発生後の時間経過等を考慮すると、センターの情報セキュリティ機器に残された記録から得られる情報は限定的である上、事案が発生した端末の初期化を行うといった不適切な対応により情報を喪失してしまったため、調査によって明らかにできる内容に制約が生じているが、その制約下においては、調査・検証で得られた調査結果は妥当であると考える。

③その他の情報セキュリティ上の問題について

業務規定に基づくセンターの内部規程では、不正アクセスが確認された場合は、情報管理に関する異常として、速やかにその状況を国に報告するとしている。一方、平成２７年８月の常時監視の開始以前から稼働していた監視において、外部機関から不正アクセスの検知に関する報告を受けており、それに対して流出の可能性があった情報や原因の特定のための調査を行わず、業務連絡書のみによる対処を行っていた等の事実は平成２８年１月２７日の原子力規制委員会に対する報告以降に原子力規制庁に対して報告されている。また、平成２７年２月にセンターの計算機室のサーバが悪意のある外部のコンピュータにより、別の外部のコンピュータを攻撃する際の踏み台にされていたことは、平成２８年４月になり、初めて原子力規制庁に報告された。これらは本来事象確認後適切な手続きを経て、速やかに原子力規制庁に対して報告されるべきものであり、業務規定及びセンターの内部規程に違反するものであった。

（２）原因究明に対する評価

調査・検証の結果得られた情報をもとに問題点を抽出し、それらの問題を発生させる背景となった情報システムの技術的要因を分析した上で、これらの要因の根底にある組織要因の分析を行っている。これら各層で抽出された問題は認識された事実に基づいており、後段の再発防止策により改善を図る際に参照が可能な程度の具体性を備えているものと考える。

これらの様々な問題の背景にあった根源的な問題点としては、センターが指定保障措置検査等実施機関及び指定情報処理機関としての責務を遂行する上で必要となる、管理すべき情報に対する情報セキュリティ上のリスクに対応するという問題に真摯に向き合ってこなかったことが挙げられるとしている。これは、原子力規制庁に報告すべき情報セキュリティ上の事象を把握していたにもかかわらず、複数回に亘り報告を怠っていた例のみをもっても、組織としての意識の低さを示すものであり、妥当な自己評価であると考える。

（3）再発防止策に対する評価

①記載されている再発防止策は、抽出された問題と対応しており、具体的な工程も示されていることから、妥当であると考える。

②再発防止策が、センターの強固な情報セキュリティシステムの構築に着実に繋がっていることを原子力規制庁として継続的に確認する必要がある。

4．原子力規制庁の今後の対応

①再発防止策の進捗状況について、随時、原子力規制庁に対する報告を求め、必要な指導を行う。

②再発防止策の実施状況を踏まえ、原子炉等規制法に基づく立入検査を行い、情報セキュリティ対策の状況を厳格に確認する。なお、その後も同法に基づく立入検査を定期的に行い、業務状況を継続的に確認していく。

以　上