情報セキュリティ対応の不備に関する調査結果報告（概要）

平成 28 年 5 月 18 日
公益財団法人　核物質管理センター

1．　はじめに（報告書　1.）

(1)　核物質管理センターにおいて、平成 27 年 8 月及び 9 月に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、情報流出の可能性をもたらしました。また、内部規定に則り速やかに原子力規制庁に報告すべき事象であったにもかかわらず、その報告を怠っていました。

(2)　この件に関して、本年 1 月に公表を行い、原子力規制委員会に報告しました。原子力規制庁より厳重注意を受け、1)情報流出範囲の確定とその影響の調査、2)その結果に基づく問題発生の背景を含めた原因究明、3)その結果を反映した再発防止策の策定と実施を行い、その結果を本年 3 月 31 日までに報告するよう指示を受けました。

(3)　報告期限である3月末に原子力規制庁に報告書を提出しましたが、調査の過程で追加調査を必要とする事象が確認されたため、その調査・検証を行い、補正報告書を提出しました。

(4)　なお、本年 1 月に原子力規制委員会に報告した事案の他に、過去に検知された通信等について、報告すべきところ報告を怠っていた事案がありましたので、これらの事案も含めて報告しております。

2.　調査・検証結果（報告書　4.）

センター内に調査・検証の実施体制を設け、情報システム全体の包括的調査と関連する PC・サーバ等の網羅的な調査・検証を行うため、情報セキュリティ専門会社による支援を受け、FW 等ログの調査、ブラックリストとの通信先照合、フォレンジック調査等の技術的調査を実施し、その結果について職員に対するヒアリングにより事実確認、検証を行いました。情報流出及びその他の情報セキュリティ上の問題についての調査・検証により、概要以下のような結果を得ました。

(1)　本年 1 月に報告しました Xunlei として検知された通信については、平成 27 年 4 月 3 日に初めて Xunlei が UTM で検知される直前に、1 台の PC にフリーソフト Drive The Life がダウンロードされました。その後、Xunlei として検知された通信先等にファイル共有ソフト特有の通信（ネイティブポート通信）が発生していました。再現試験による検証と当該フリーソフト開発会社への問い合わせの結果、当該フリーソフトに製品として組み込まれたファイル共有ソフトである Thunder が原因で通信が発生したものと考えます。この通信によりセンターが保有する情報の一部が流出した可能性はありますが、当該 PC をクリーンインストールしてしまったことから、その情報の内容を特定することはできませんでした。

(2)　過去、統合脅威管理機器（UTM）がファイル共有ソフトによるものとして検知した通信が複数の PC から多数ありました。これら通信には、ネイティブポート通信が見られなかったこと、PC の Web ブラウザにファイル共有ソフトがアドオンされていないこと、聞き取り調査から Web 閲覧を行っていたこと、ファイル共有ソフトを使用していないとのこと等から、Web 閲覧を誤検知した可能性が高いと情報セキュリティ専門会社から報告を受けています。しかしながら、通信があった当時、Web ブラウザのアドオン機能によりネイティブポート通信を発生させずに通信した可能性を排除できないため、センターが保有する情報の一部が流出した可能性は残ります。なお、UTM によりファイル共有ソフトによるものとして本年2月に検知された通信は、誤検知の可能性が高いと UTM 運営会社から報告を受けています。また、常時監視では報告されていませんでした。

(3) 情報セキュリティ専門会社が保有するブラックリストとセンターの Proxy サーバ及び FW のログを照合した結果、緊急性の高いマルウェア感染による通信は確認されませんでしたが、上記(1)で言及した Xunlei によるものを含む不審な通信やマルウェアの存在が確認されました。フォレンジック調査等の結果、Web 閲覧履歴や PC 本体の情報（PC や HDD のメーカ名、シリアル No.等）が流出した可能性があるものの、業務データの流出につながる痕跡は確認されませんでした。また、Xunlei を除き、ファイル共有ソフトがインストールされた形跡はありませんでした。

(4) AD サーバのフォレンジック調査の結果、外部からの不正アクセス、マルウェア感染の痕跡、不審なファイル探査やデータ圧縮の痕跡は認められず、AD サーバの管理者権限が流失したことはないと考えられること、加えて、新 FW のログと Proxy サーバのログの調査結果、常時監視の結果に基づく限り 、情報セキュリティ専門会社の見解によれば、現時点では情報システムは健全な状態にあるとのことでした。

(5) 平成 27 年 1 月 19 日、センターは、UTM の監視結果としてファイル共有ソフト eDonkey によるものとして検知された通信が報告されました。これに対し、業務連絡書による指示等の対応を講じましたが、業務規定及び内部規定に従った措置は講じておらず、当該事象の発生について原子力規制庁に報告しておりませんでした。

(6) 平成 27 年 2 月 19 日、センターの DNS サーバが DDoS 攻撃の踏み台として使用されたとの通報が外部機関からあり、DNS サーバの設定を変更することで対処しました。本事象はセンターからの情報流出につながるものではないものの、外部からの不正アクセスであり、また他機関に対して被害を与えた情報セキュリティ上の重大な問題であったことからも、原子力規制庁への報告を要する事象でしたが、報告を怠っていました。

3. 原因究明（報告書 5.）

センターの情報セキュリティの不備をもたらしている原因を究明するため、まず調査の結果又はその過程で得られた情報から問題点を抽出しました。その上で、センターの情報システムの技術的要因を抽出し、最後にそれらの背景ともなっているセンターの組織要因の抽出を行いました。

(1) 情報セキュリティ体制上の問題

- マネジメント上の課題として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。
- 情報セキュリティの確保のための人的・資金的投資を行う必要性の理解が不十分であり、適切な情報システム上の防護策を講じてこなかったこと。
- 業務が分権的で指揮命令系統が並立しており、情報セキュリティを担当する部署がセンターを統括して情報セキュリティ対策を講じられる体制になかったこと。
- 情報セキュリティを担当する部署には専任の担当者がおらず、情報セキュリティの確保に必要な人材の確保を怠ってきたこと。
- 非常時対応体制を設けていなかったこと。
- 情報セキュリティの管理に必要なルールが十分整備されておらず、また不明確であったこと。

(2) 情報システム上の問題

- ネットワーク構成とそのセキュリティレベルの統一ができていなかったこと。
- 管理情報等を取扱う情報ネットワークシステムの情報セキュリティが不十分であったこと。
- 情報システムによる以下の仕組みを導入していなかったこと。
  - 許可されていない PC、外部記憶装置、記録媒体等の接続の監視・ブロック
  - 使用禁止ソフトのインストールや使用の監視・遮断

- リスクのある Web サイトへのアクセスの遮断
- ファイル共有ソフトに起因する意図しない外部通信等の遮断設定

(3) 情報セキュリティに関する意識や行動の問題

- 情報システム担当部署が必要な専門知識・技術を有しておらず、外部の専門家の活用などの必要性も十分に認識できていなかったこと。
- 問題を把握した際、経営陣が適切な情報共有と国への報告を含む必要となる対応を怠ったこと。

4. 再発防止策（報告書 6.）

特定した技術的要因及び組織要因を踏まえ、それらに対する再発防止策を策定し、平成 27 年度より進めてきた情報セキュリティ対策強化策に組み込み、新たな情報システムを構築し、厳格に運用していきます。

4.1 情報セキュリティ体制の強化

(1) 組織体制の整備

- 情報セキュリティマネジメントに関する役員によるリーダーシップの発揮とコミット。
- 外部有識者から構成される第三者委員会による客観的、専門的な見地から改善すべき問題点についての検証、再発防止策の実効性の評価。
- 情報セキュリティ専任組織の設置、常時監視会社との対処方策等に係る連携協力、情報セキュリティコンサルティングの有効活用、ライン機能の強化等。
- 非常事態体制の設置

(2) 情報セキュリティマネジメントの導入

- 国の情報セキュリティポリシー及び対策基準に適合した規程等の整備による対策レベルの向上。
- 情報セキュリティマネジメントシステムの取り入れ、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。

4.2 情報セキュリティシステムの強化

(1) 情報ネットワークの分離

- 情報流出のリスクを低減させるため、全ての管理情報等をインターネット接続環境から完全に遮断したクローズドネットワーク下に置き、一般業務情報を取り扱うネットワークと分離。
- 一般業務情報を取り扱うネットワークへの管理情報等の持込みを情報システムにより禁じるとともに、パスワードの適切な設定、USB 等リムーバブルメディアの接続・アクセス禁止等を含む情報システムによる一層の厳格な制限・管理の適用。

(2) 禁止ソフト等の使用やその影響を物理的に防止する対策の実施

- C&C サーバや脅威・悪性サイトへの通信のブロック。
- 許可した標準製品リストを設け、禁止事項とする無許可ソフトの使用や無許可ハードの接続を情報システムが自動遠隔遮断する等、できる限り個人の判断・裁量の余地を無くす情報技術の取り入れ。

(3) 情報セキュリティシステム全体の運用体系の改善

- 中央集中管理及びその責任境界と権限の明確化によって、情報ガバナンスの徹底、セキュリティ情報の集中管理をし、情報の流出リスクの低減化、インシデントへの迅速な対応。

(4) IT 製品のセキュリティチェック

- IT 製品のセキュリティ要件の実装状況、セキュリティ機能の確認・検査、初期設定の確認を含めたセキュリティチェック。

4.3 情報セキュリティの意識改革と行動の徹底

(1) 最新のサイバー攻撃の情報収集と備え

- 最新のサイバー攻撃の情報収集、常時監視会社からの対処対策方法の入手、速やかな組織内での情報共有、注意喚起、対処方法等の周知徹底。

(2) 情報共有の実効性向上

- 職員の理解と適確な対応のための具体的な解説を含めた業務連絡書、係る事案の重要性に応じた各情報管理責任者等による解説・説明。業務連絡書による指示、周知徹底により原課で執られた方策とその処置状況の報告とその確認。

(3) 教育訓練

- 情報セキュリティ基礎教育及びその反復学習、標的型メール訓練、重大インシデント発生を想定した訓練等を通じて、情報セキュリティの意識改革と行動の徹底。
- 発生インシデントの脅威の正しい理解・解釈、適切な対処のための専門知識と技術の習得。一段高い情報セキュリティ意識を持つ、必要な専門スキルを備えた技術者の養成。

4.4 今後の対応

- 上記の再発防止策を実施に移しつつ、情報セキュリティ対策の専門家の知見を十分に活用し情報システムを構築していきます。
- 移行までの間の情報セキュリティは、現行システムにて可能な対策を講じていくとともに、常時監視とそのアナリストによる分析報告を正確に理解し、各種セキュリティログの確認、インシデントへの適時・適切な対処を徹底していきます。

5. おわりに（報告書 7.）

- 情報システムによる情報流出の防御機能、情報セキュリティに係る組織体制、情報セキュリティマネジメント、原子力規制庁への報告等において重大な不備を生じさせていたことに、センターは深く反省いたします。
- センターは、この根底にある問題と重大な不備に対する改善・対策として、情報セキュリティに関する役職員の意識の改革、組織体制の整備、情報システムのセキュリティ強化、情報マネジメントシステムの導入等からなる再発防止策を実施していきます。
- さらに、外部有識者からなる第三者委員会を設置し、客観的、専門的な見地からセンターが改善すべき問題点の検証と再発防止策の実効性について評価していただき、一層効果的・効率的な対策の実施につなげます。
- センターは、指定機関の使命と責任を再認識するとともに、指定機関としての管理情報等の機密性・完全性・可用性を確保し、社会からの信頼回復に努めてまいります。

以上