環境防災Ｎネットにおける個人情報の不適切な取扱いに係る調査報告書

平成 25 年８月 30 日

公益財団法人原子力安全技術センター

環境防災Ｎネットにおける個人情報の
不適切な取扱いに係る調査検討委員会

目　次

第１章　はじめに

平成25年6月30日、公益財団法人原子力安全技術センター（以下、「センター」という。）は、センター（防災技術部）が運営する公開Webサイト「環境防災Ｎネット（以下、「Ｎネット」という。）」において個人情報を含んだテキストファイルが外部から閲覧可能になっているとの通報を受けた。

Ｎネットでは、原子力防災情報を広く一般に公開するとともに、同Web上でご質問・ご意見を受け付けている。閲覧可能となっていた個人情報は、Ｎネット上で質問・意見を受け付ける際、センターからの返信用に入力をしていただいたものだった。

センターは、当面の措置として事態の拡大を防ぐために必要な措置を取るとともに、影響を受ける可能性のある方へ連絡を行い、国等への報告を行った。また、個人情報の不適切な取扱いという事態の重要性を認識し、外部の専門家を含めた委員会により、原因究明及び再発防止策の検討を行い、この結果を受けて組織的な対応と改善を行うこととしている。

本報告書は、上記委員会にて検討いただいた原因究明及び再発防止策の調査検討結果を取りまとめたものである。

第２章　委員会の設置及び検討経緯

２．１　委員会の設置

今回発生したＮネットにおける個人情報の不適切な取扱いについて、原因の究明と再発防止策を検討するために「環境防災Ｎネットにおける個人情報の不適切な取扱いに係る調査検討委員会」（以下、「委員会」という。）を設置した。委員には、検討の万全を期すため外部専門家の参加を得た。

２．２　検討経緯

委員会では、本事案の発生原因及び再発防止策の調査について２回の会合及び書面による検討を行い、本報告書を取りまとめた。

以下に、委員会の開催概要を示す。

委員会　開催概要

第１回環境防災Ｎネットにおける個人情報の不適切な取扱いに係る調査検討委員会

開催日　平成 25 年 7 月 25 日（木）

議　　題

（１）委員会の設置について

（２）個人情報の不適切な取扱いに関する経緯及びこれまでの対応について

（３）発生原因の調査について

（４）再発防止策（案）について

（５）その他

配布資料

資料１－１　環境防災Ｎネットにおける個人情報の不適切な取扱いに係る調査検討委員会の設置について

資料１－２　委員名簿

資料１－３　個人情報の不適切な取扱いに関する経緯及びこれまでの対応について

資料１－４　発生原因の調査について

資料１－５　再発防止策（案）について

第２回環境防災Ｎネットにおける個人情報の不適切な取扱いに係る調査検討委員会

開催日　平成 25 年 8 月 5 日（月）

議　　題

（１）議事録（案）について

（２）第１回委員会における指摘事項の対応状況について

（３）環境防災Ｎネットの構成及び環境設定について

（４）アタックテストの結果について

（５）報告書（案）について

（６）その他

配布資料

資料２－１　議事録（案）

資料２－２　第１回委員会における指摘事項の対応状況

資料２－３　環境防災Ｎネットの構成及び環境設定について

資料２－４　アタックテストの結果について

資料２－５　環境防災Ｎネットにおける個人情報の不適切な取扱いに係る調査報告書（案）

第３章　個人情報の不適切な取扱いに関する経緯及びこれまでの対応について

３．１　経緯

平成 25 年 6 月 30 日に、一般の方からＮネットに情報登録した自身の個人情報が Web 上で閲覧可能であるとの指摘をメールで受けた。センターは７月１日にその事実を確認し、直ちに、閲覧可能となっていたファイルの削除、個人情報が閲覧可能な状態であった方々への連絡及び事実関係の報告・公表を行った。対応の時系列について表１にとりまとめた。

表１　対応の時系列

日にち	時間	対　応　内　容
6 月 30 日（日）	19:59	環境防災 N ネットに情報登録された方から個人情報を含む内容が第三者から閲覧可能であることを指摘するメールを受信
7 月 1 日（月）	9:40	上記メールを確認
	9:50	33 名の個人情報を含む 2 つのファイル（以下、当該ファイル）が Google から検索・閲覧可能な状態であることを確認
	10:30	当該ファイルを環境防災 N ネットのサーバ上から削除
	10:30	Google に当該ファイルのキャッシュ及び検索結果の削除を依頼
	10:40	Google 以外の 24 の検索サイトについて検索できるか確認開始､同日 18 時までに、検索可能であったサイトにキャッシュと検索結果の削除を依頼
	11:30	WEB サーバ内に個人情報が他にないかの確認開始（17：30 までに確認終了）
	17:30	本事案について、センター内に報告・周知
	19:39	最初に通報いただいた方に対し、お詫びと連絡をとりたい旨のメール発信
	19:59	原子力規制庁にメールで報告（後に電話連絡）
	23:58	当該ファイルに情報が含まれていた 32 名（通報者除く）に対し、お詫びと連絡希望する旨をメール発信
7 月 2 日（火）	10:21	当該ファイルに情報が含まれていた方々との連絡状況を原子力規制庁に報告
	18:00	原子力規制委員会記者クラブにおいてセンターから本件について記者発表
	20:00	センターのホームページに本件について報告及び謝罪の記事を掲載
7 月 3 日（水）	20:10	前々日メールをお送りした方々のうち、返信のない方 23 名に対し再度メール送信
7 月 4 日（木）	16:36	当該ファイルに情報が含まれていた方のうち、メール返信がなく、電話番号を登録されていた方 10 名に電話連絡
7 月 5 日（金）		内閣府公益認定等委員会に対し、状況説明（個人情報保護法に基づく所管官庁への報告について確認を依頼）
7 月 11 日（木）		当該ファイルに情報が含まれていて、電話及びメールが通じない方のうち、住所を登録いただいていた方 2 名に謝罪及び 2 次被害等確認依頼の文書を郵便で発送
7 月 22 日（月）		郵便連絡を試みた 2 名のうち 1 名の方について住所・氏名該当なしとして郵便が返送され到着

３．２　対応状況のまとめ

○閲覧可能となった情報内容の確認

閲覧可能となっていた個人情報を含むファイルを確認した結果、平成23年3月12日から3月24日の期間に意見等を頂いた33名の「氏名(ハンドルネームを含む)」、「電子メールアドレス」、「ご意見等の内容」及び一部の方の「住所」、「電話番号」、「所属」の情報が含まれており、その全てが閲覧可能な状況にあった。

○影響範囲の特定

・影響を受ける可能性のある方への連絡

影響を受ける可能性のある方へ7月1日から電話及びメールにて連絡対応を行い、電話及びメールでの連絡が取れなかった方には7月11日郵送にて状況報告を行った。8月30日現在の連絡状況について表2にとりまとめた。

・二次被害の確認

閲覧可能なファイルに記載されていた33名に対し、二次被害の有無について確認を試みた。その結果、平成25年8月30日現在、12名の方と連絡が取れ、二次被害等の連絡はなかった。

○所管官庁への報告

・原子力規制委員会原子力規制庁への報告

7月1日19:59に監視情報課へ内容及び対応状況についてメールにて報告を行い、その後電話にて報告を行った。

・内閣府公益認定等委員会事務局への報告

7月5日本事案について、これまでに確認した内容及び対応状況の説明を行った。

○事実関係の公表

・プレス発表

7月2日18:00にプレス発表を行い、個人情報の不適切な取扱いに関する事実関係の公表及び謝罪を行った。

・センターのホームページでの公表

7月2日20:00頃にセンターのホームページに「環境防災Ｎネットにおける個人情報の不適切な取扱いに関するお詫びとご報告」を掲載した。また、8月12日に経過報告を掲載した。

○原因究明及び再発防止策の検討

「環境防災Ｎネットにおける個人情報の不適切な取扱いに係る調査検討委員会」を設置し、原因及び再発防止策を検討することとした。

○再発防止策の実施

センターは、本委員会で検討した再発防止策を計画通りに実施することとする。

表２　影響を受ける可能性のある方へ連絡を試みた結果（8 月 30 日現在）

登録者	登録されていた項目					連絡を試みた結果			
	メールアドレス	氏名	住所	電話番号	所属	メール送信結果	電話連絡結果	郵便連絡結果	結果
1	▲	▲				×			×
2	○	○				○			○
3	○	○				○			○
4	▲	▲				×			×
5	○	○	○	○		×	×	×（該当者なしとして郵便物が返送された）	×
6	○	○				○			○
7	○	○		○		○	○		○
8	○	○	○	○		○	○		○
9	○	○		○		○（ご了解のメールを頂いた）			○
10	○	○		○		○	○		○
11	○	○				○			○
12	○	○	○	○	○	×	○		○
13	○	○				○			○
14	○	○				×			×
15	○	○	○	○		×	○		○
16	○	○				○			○
17	○	○				○			○
18	○	○	○	○		○	○		○
19	○	○		○	○	○（ご了解の電話を頂いた）			○
20	○	○				○			○
21	○	○				○			○
22	○	○				○			○
23	○	○	○	○		○	×	○	○
24	○	○				○			○
25	○	○				○			○
26	○	○				○			○
27	○	○	○	○		○	○		○
28	○	○				○			○
29	○	○				○			○
30 ※	○	○				○			○
31	○	○	○	○		○	○		○
32	○	○				○			○
33	○	○				○			○
○計	31	31	8	12	2	26	8	1	29

※：通報頂いた方

○：項目が登録されている、または連絡を試みた際にエラーとなっていない

▲：登録されているが実在のメールアドレスまたは氏名ではないと考えられるもの

×：連絡を試みた際にエラーまたは不通となった

第４章　発生原因の調査について

本事案の経緯及びこれまでの対応について整理することによって、事実の把握に努めた。これらの事実をもとに、原因究明については、以下に示す手順のとおり行った。

①本事案の発生状況の確認

・現状におけるＮネットでの個人情報の取扱いを整理

・個人情報が外部から閲覧可能となっていた状況を整理

②調査方法の検討

・発生原因の検討に漏れが生じないよう、複数の観点からそれぞれ調査を進めることとした。第一に発生原因者がセンター内部にある場合と外部にある場合に分けることとした。内部に原因があるとした場合については、記録類から発生原因の痕跡を探す「記録類の調査」と作業手順を分析して発生原因を演繹的に推測する「作業内容の調査」を行うこととした。また、外部に原因があるとした場合については「システムの脆弱性調査」を行うこととした。

③調査結果の考察

・各調査において、情報の収集と精査を行い発生原因の可能性を考察し、この結果を再発防止策の検討に活用する。

４．１　発生状況

（１）Ｎネットの概要

Ｎネットは、環境放射線及び原子力防災に関する国民の理解増進を目的としてインターネットに公開しているホームページである。平成 14 年度よりセンターが文部科学省の委託を受けて運用を開始し、平成 24 年度からは原子力規制委員会の委託により運用を継続している。

（２）Ｎネットにおける個人情報の取扱い

Ｎネットでは環境放射線等の情報を提供する他、利用者からのご質問・ご意見を Web 上で受け付けている。その際、氏名及びメールアドレスを必須の入力項目としており、さらに住所、電話番号、所属等についても入力欄を設けている。これらの情報とともにご質問・ご意見が登録されると、登録された全内容がＮネットの保守管理用端末に自動でメー

ルされ、公開サイトには情報が残らない仕組みとなっている。Ｎネットの保守管理用端末は、Ｎネット公開サイトと別のネットワークに設置して、外部から参照することはできない環境で個人情報を保管していた。

（３）個人情報が外部から閲覧可能となっていた状況

一般の方からメールで指摘を受け、本事案で問題となったファイルが第三者から閲覧可能であることを確認した際の状況は、以下のとおりであった。

・個人情報を含む２つのテキストファイルが、Ｎネット Web サーバの公開ディレクトリ配下に置かれており、Ｎネットのメニューからはリンクされていないが、インターネットで検索・閲覧が可能な状態であった。

・当該ファイルが置かれていたディレクトリはＮネットの「情報 box」コーナーのコンテンツが格納されている場所であった。同コーナーでは、原子力防災に関する Q&A、用語集等が掲載されている。

・当該ファイルの内容は、Ｎネットにご質問・ご意見が登録された際に保守管理用端末にメールで送信された全内容を結合したものであった。２つのファイルで合計 33 件の登録内容が含まれていた。それらがＮネットに登録されたのは、平成 23 年 3 月 12 日から 3 月 24 日までであった。

・当該ファイルのタイムスタンプは、２つとも平成 24 年 4 月 12 日 11:53 であった。ただし、公開コンテンツは一部を更新する際にディレクトリ全体を上書きすることがあるので、これらのファイルが最初に置かれた日時とは限らない。

・第三者から閲覧可能となっていた当該ファイルと全く同じものが、Ｎネットの保守管理用端末に保管されていた。これらのファイルのタイムスタンプは平成 23 年 3 月 23 日と 24 日であった。このことから、これらのファイルは平成 23 年 3 月 23 日と 24 日に作成されたものと考えられる。

４．２　調査の方法

原因の調査は、現在保存されている記録類から発生原因に関連する記録を抽出して精査する「記録類の調査」、作業内容を網羅的に整理し各作業が原因となる可能性を考察する「作業内容の調査」及びＮネットに

おけるシステムの脆弱性を精査する「システムの脆弱性調査」の３つの方法で実施することとした。

（１）記録類の調査

現在保存されている記録類としては、システムのバックアップデータと作業記録がある。本事案で問題となったファイルが作成されたと考えられる平成 23 年 3 月当時のバックアップデータはないが、当時の作業担当者に聞き取りを行い、収集した記録類から本事案に関連する記録を可能な限り抽出し精査した。

（２）作業内容の調査

作業内容を調査するにあたって、今回の事案を生じさせた可能性のある者を、Ｎネット関係業者及びセンター職員に分けて検討することとした。また、Ｎネットの保守管理作業項目を整理し、それぞれ原因を生じさせた可能性の有無を精査した。

（３）システムの脆弱性調査

Ｎネットのシステムにおいて、第三者によるシステム乗っ取りや機密情報の漏洩など、セキュリティ上の大きな問題となるような欠陥や仕様上の問題点を精査した。

４．３　調査内容

４．３．１　記録類の調査

（１）バックアップデータの確認

①保存状況の確認

Ｎネットは、毎週金曜日にバックアップを実施しており、１回のバックアップデータを１本の DAT（Digital Audio Tape：外部記憶媒体の一種）に格納している。本作業のためのバックアップ用 DAT は５本用意しており、それらをローテーションして使用することにより、５週間前までのバックアップデータを保管している。本作業により、平成 25 年 6 月～7 月にかけて作成したバックアップデータが保管されていることを確認した。

また、平成 24 年 4 月に５本のバックアップ用 DAT を、経年劣化を考慮して新しく入れ替えていたため、それまで使用していた DAT５本が残っており、平成 24 年 3 月～4 月にかけて作成した５週分のバックアップデータが得られることを確認した。

この他、平成 23 年 1 月 26 日に保守作業のために使用したバックアップデータと、平成 24 年 7 月に実施した機器更新作業に使用した平成 24 年 7 月 30 日のバックアップデータを確認した。

②バックアップデータに格納されていたファイルのタイムスタンプの確認

①で得られたバックアップデータ 12 本から、本事案で問題となったファイルが作成された時期を明らかにするため、当該ファイルのタイムスタンプを確認した。バックアップデータの確認結果を、表３に示す。

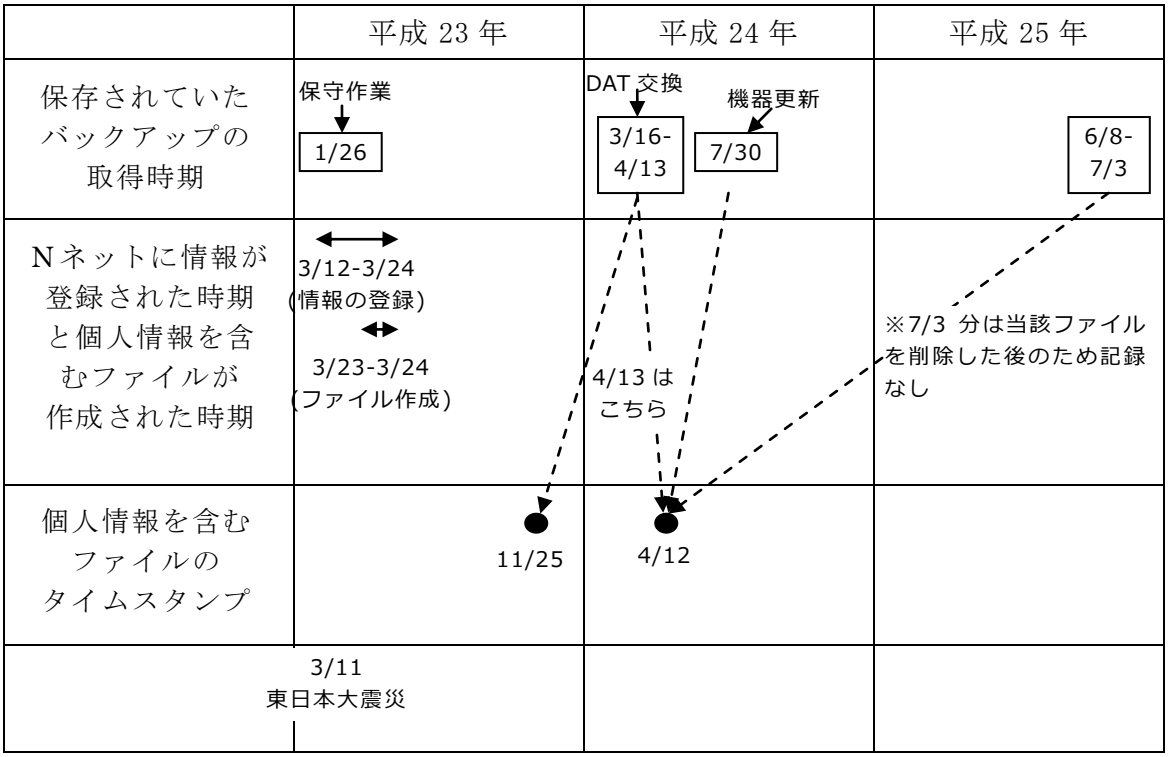
当該ファイルのタイムスタンプを確認した結果、平成 23 年 11 月 25 日から当該ファイルが第三者から閲覧可能な状態で置かれた可能性がある。しかしながら、他のコンテンツ変更があった際に当該ファイルのタイムスタンプが変わる場合があるため、平成 23 年 11 月 25 日以前から同ファイルが閲覧可能な状態で置かれていた可能性もある。

③バックアップデータに格納されていたログ類の確認

12 本のバックアップデータのうち、当該ファイルが最初に置かれた時期にもっとも近いと考えられる平成 24 年 3 月 16 日付のバックアップデータに、ログ類が格納されていることを確認した。これらのログは、ログの種類毎に保存期間を 7 日から３ヶ月の間で設定しており、HTTP のアクセスログについては、１ヶ月間の保存期間を設定していた。これらログ類全てについて、当該ファイルを取り扱った作業に関するログが残っていないか、同ファイルに対して第三者からアクセスされたことを示すログが残っていないかの観点で精査した。

精査の結果、いずれの観点についても参考となる情報は得られなかった。

表３　バックアップデータの確認結果



（２）作業担当者からの聞き取り及び作業記録の確認

本事案で問題となったファイルが作成されたと考えられる平成 23 年３月当時の作業担当者に聞き取りを行った。その結果は以下のとおりである。

①作業担当者からの聞き取り

・作業担当者１名は、当該ファイルを編集していた明確な記憶があるものの、ファイルのタイムスタンプの日時に実際に作業した記憶はなかった。他の１名は当該ファイルについて存在も認識していなかった。

・作業担当者２名とも当該ファイルを Web サーバに転送した記憶はなかった。また、Web サーバにそのような情報を置いてはならないことの認識は当時から持っていたため、意図的に転送することはない、とのことであった。

・Ｎネットのコンテンツ更新方法を確認したところ、Ｎネットのコンテンツを更新する際、公開されているファイルをファイル転送用端末に一旦ダウンロードし、同パソコンで編集作業した後、Web サーバのテスト環境にアップロードして編集結果を確認し、その後、公

開していた。公開されているファイルのアップロードとダウンロードはファイル単位またはディレクトリ単位で行っていた。

・ディレクトリ単位でアップロードを行う場合に、他のファイルが含まれる可能性を作業担当者に確認したところ、ディレクトリ単位で行う場合は編集作業中に他のファイルが含まれても気づかずにアップロードしてしまう可能性がある、との認識であった。

②作業記録の確認

当該ファイルが作成された当時の作業について、当時のメールやメモ及び運用報告等をもとに確認した。その結果を表４に整理した。なお、表４に示した以外の期間についても、記録及び作業担当者の記憶を確認したが、当該ファイルを Web サーバに転送することを含む作業が実施されたことは確認できなかった。

作業担当者からの聞き取り及び作業記録によると、当該ファイルが作成されたと考えられる平成 23 年 3 月 23 日及び 24 日以降、当該ファイルが置かれていたＮネットの「情報 box」ディレクトリ内のファイルを更新したのは平成 23 年 4 月 13 日であった。したがって、当該ファイルが第三者から閲覧可能となっていた可能性のある期間は最長で平成 23 年 4 月 13 日からと考えられる。ただし、平成 23 年 4 月 13 日はあくまで現在残っている記録をもとに検証した結果に過ぎず、実際には日にちが前後する可能性もある。

（３）記録類の調査のまとめ

保存していたバックアップデータ及び作業記録等から、コンテンツ更新作業を行う際に、コンテンツ更新作業と無関係のファイルが含まれていても気づかずにアップロードしてしまう可能性があることがわかった。

また、本事案で問題となったファイルが第三者から閲覧可能となっていた期間は、最も長い場合では平成 23 年 4 月 13 日頃以降、最も短い場合で平成 23 年 11 月 25 日頃以降である。

表４　個人情報を含むファイルが作成された当時の作業実施状況

作業の実施状況	実施時期と作業項目
◎Ｎネットの通信設定及び表示設定作業 （福島第一原発事故の影響で、インターネット上でＮネットに対してアクセス数が急増した。Ｎネットの表示レスポンスが遅い等、一般の方からの問合せが増加したこともあり、表示レスポンス改善のために種々設定変更等を行った。）	平成 23 年 3 月 16 日 ・トップページを簡易版に変更 ・DB のパラメータ変更 平成 23 年 3 月 18 日 ・テロップ表示速度変更 平成 23 年 3 月 23 日 ・OS、Apache、DB のパラメータ変更
◎Ｎネットのコンテンツ更新作業 （福島第一原発事故の影響で、Ｎネットの利用者が増大したこともあり、ライフライン情報の更新、表示内容を解説する注釈の追加等のコンテンツ更新作業を実施した。更新作業は従来からのルーチン作業として実施した。）	平成 23 年 3 月 22 日、27 日、29 日 ・注釈の追加、変更 平成 23 年 3 月 27 日 ・テロップ表示内容の追加 平成 23 年 4 月 1 日、4 日、5 日、6 日 ・関係自治体ページの情報追加 平成 23 年 4 月 13 日 ・「情報 box」ページの情報更新
◎ご意見・ご質問の登録情報整理 （文科省に報告するための整理作業。作業は保守管理用端末で実施。）	平成 23 年 3 月 23 日 ・3/12～3/22 日分ファイル作成 平成 23 年 3 月 24 日 ・3/23～3/24 日分ファイル作成 平成 23 年 3 月 31 日 ・3/29～3/30 日分ファイル作成 以後、5 月 30 日まで継続 （以上は記録、記憶ともないため、ファイルのタイムスタンプを作成日とした）

４．３．２　作業内容の調査

ここでは、本事案で問題となったファイルが第三者から閲覧可能となる状況を生じさせたことについて、作業内容から発生の可能性を考察する。

最初にこのような状況を生じさせた可能性のある者を、Ｎネット関係業者及びセンター担当者に分けて、それぞれ考察する。

（１）Ｎネット関係業者による場合

Ｎネット関係業者がＮネットのサーバを操作するのは、サーバ等の点検、環境設定、請け負った業務で整備した機能や改修ページをインストールするときのみである。

Ｎネット関係業者がサーバまたはファイル転送用端末を使用する場合には、センター担当者が管理している ID とパスワードでログインした後、端末の使用を許可している。Ｎネット関係業者が作業している間は、終始立会をしている。

Ｎネット関係業者がサーバ内のファイルについて更新等する際には、センター担当者立会のもとダウンロードするか、センター担当者がダウンロードしてファイルを渡している。

以上のことから、Ｎネット関係業者が今回の事案を生じさせた可能性はない。ただし、センター担当者がＮネット関係業者に貸与したデータの中に、問題となるファイルが含まれていた可能性は残る。

（２）センター担当者による場合

センター担当者がＮネットのコンテンツの改修等でサーバにファイルのアップロードが行われる作業項目は、以下のとおりである。

①Ｎネット利用者に対する新着情報等の更新

Ｎネットのトップページに一覧表示またはテロップ表示している新着情報または緊急のお知らせについて、表示内容を更新する。

②観測局情報の更新

Ｎネットで公開しているモニタリングデータの測定場所の追加や削除、またはその情報を変更する。

③避難所情報の更新

Ｎネットで公開している避難所の場所の追加や削除、またはその情報を変更する。

④モニタリングデータの補完登録

Ｎネットのサーバが点検等で停止した場合、その期間登録されなかったモニタリングデータを補完登録する。

⑤道府県が発刊している報告書と広報誌の更新

道府県で実施された環境放射線監視調査結果の年報と季報を入手次第掲載する。また、道府県で発刊した広報誌も掲載する。

⑥その他掲載情報の更新

外部リンクの URL が変更された場合、地域防災計画の改訂版を入手した場合、原子力防災用語集や研修資料などの資料が更新された場合の対応として、該当ページを更新する。

上記の作業におけるファイルのアップロードの操作は、以下の３通りに分類できる。

ⅰ．Ｎネット専用のコンテンツ管理機能による操作

①から③の作業において更新するデータは、Ｎネットのデータベースに登録されている。情報の更新作業は、Ｎネットに備わっているコンテンツ管理機能を用いて行う。

ⅱ．Ｎネット専用のモニタリングデータ登録機能による操作

④の作業は、Web サーバ内の非公開領域にある決められたディレクトリに登録するモニタリングデータを格納し、モニタリングデータ登録機能を用いて行う。

ⅲ．手動によるアップロード及びダウンロードの操作

⑤と⑥の作業は、センター担当者が処理するファイルを手動でアップロードまたはダウンロードする作業である。Ｎネットのコンテンツを更新するときの機器構成を図１に示す。Ｎネットのコンテンツ更新はファイル転送用端末または保守管理用端末で行う。ファイル転送用端末はアップロードとダウンロードの専用端末、保守管理用端末は「ご質問・ご意見」コーナーに寄せられた情報をメールで受信する専用端末である。

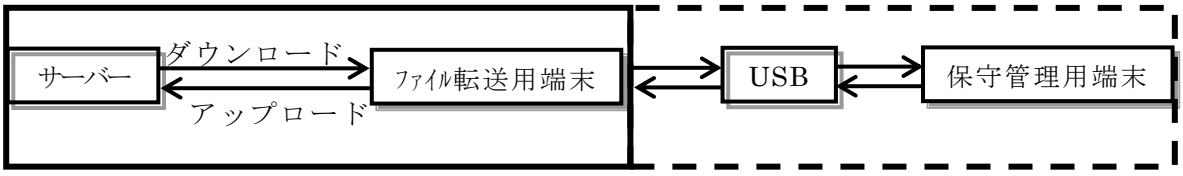


図１　Ｎネットのコンテンツを更新するときの機器

各作業について、本事案で問題となったファイルを閲覧可能な場所に置いた可能性を考察する。

ⅰ．及びⅱ．の方法によるファイルのアップロードが行われる作業、すなわち上記①から④の作業では、取り扱うファイル及びその格納場所

が使用する機能によって限定されているため、これら作業が本事案の発生原因となった可能性はない。

ⅲ．の方法によるファイルのアップロードが行われる作業は、図１のファイル転送用端末または保守管理用端末のいずれかで行われることから、それぞれの場合について考察する。

ａ．ファイル転送用端末のみで処理した場合（図中の実線枠）

ファイル転送用端末でダウンロードして、ファイルを改修し、アップロードする。サーバに個人情報を含むデータはないため、この作業単独で考えると個人情報を含むファイルをサーバにアップロードすることはない。

ただし、ディレクトリ単位でアップロードを行う場合に、ディレクトリ内のファイルを個々にチェックしていないことから、問題となったファイルが外部記憶媒体（USB メモリ等）を介して他の端末からファイル転送用端末に置かれ、アップロードされたディレクトリに混入していた可能性がある。

ｂ．保守管理用端末で処理した場合（図中の点線枠）

「ご質問・ご意見」コーナーに寄せられた情報は保守管理用端末にメールで送られ、そこに集約されることから、本事案で問題となったファイルの生成に保守管理用端末が関わっていると考えられる。

保守管理用端末とファイル転送用端末ではネットワークが異なるため、外部記憶媒体（USB メモリ等）を介してファイルの受け渡しが行われていたが、外部記憶媒体に格納されたデータのチェックは行われていなかった。

保守管理用端末ではコンテンツ更新作業も実施していたことから、問題となるファイルが外部記憶媒体を介して保守管理用端末からファイル転送用端末に移され、さらに Web サーバにアップロードされた可能性がある。

（３）作業内容の調査のまとめ

以上のことから、センター職員がＮネットの保守管理作業においてコンテンツの更新作業を行う際に、コンテンツと無関係のファイルをコンテンツの格納場所に誤って置いてしまった可能性がある。

４．３．３　システムの脆弱性調査

ここでは、本事案で問題となったファイルが外部からアクセス可能な場所に保存されたことについて、Ｎネットにおけるシステムの脆弱性を精査する。

第三者からの脅威に対する脆弱性を、技術的脆弱性及び物理的脆弱性の２つに分類して、Ｎネットにおけるシステムの脆弱性への耐性を調査する。具体的には、第三者がインターネットを通してＮネットに侵入し作業した可能性と、第三者がＮネットのシステムを設置した場所に侵入し作業した可能性について整理する。

（１）システムの脆弱性の検証

①第三者がインターネットを通してＮネットに侵入し作業した可能性

Ｎネットについては、脆弱性検出ソフト QualysGuard を用いたアタックテストを年１回実施している。今回問題となったファイルが作成された時期も含めて、これまでに要対処の脆弱性が抽出されたことはない。

なお、本年７月に原子力規制庁が所管するホームページに対するアタックテストが実施された。Ｎネットも対象となり、「脆弱性なし」の判定がなされたとの報告を得ている。

また、今回問題となったファイルは本来Ｎネットの保守管理用端末に格納されているものである。第三者が侵入して当該ファイルをインターネットで閲覧可能とするためには、一旦Ｎネットの保守管理用 LAN まで侵入し、端末の ID とパスワードの認証を受ける必要がある。ファイアウォール及び保守管理用端末のログを確認する限りにおいてネットワーク及び端末に対して侵入されるような事態が発生したことはない。

一方、当該ファイルが第三者から閲覧可能な状況が生じていたと考えられる平成 23 年３月からＮネットの機器更新が行われる平成 24 年７月にかけては Apache 等 Web サーバーソフトのバージョンが最新のものでなかったことが確認された。このため、適切にバージョンアップした場合に比較して脆弱性が高まっていた。

しかしながら、Ｎネットでは外部からのアクセス状況等について土日祝日を除き、毎日ログをチェックしており、これまでに不正な侵入は確認されていない。また、過去のバックアップデータのログについても精査しており、外部から不正な侵入があった痕跡はない。ログについても

絶対的な証拠とはならないものの、継続的にチェックが行われており、何ら検知されていないため、不正な侵入があった可能性は低い。

②第三者がＮネットのシステムを設置した場所に侵入し作業した可能性

Ｎネットのサーバ等の機器はセキュリティ管理された計算機室または操作室に設置されており、24 時間職員の監視下にあり、第三者が検知されずに侵入して作業することは物理的に不可能である。

（２）システムの脆弱性調査のまとめ

技術的脆弱性及び物理的脆弱性の観点から、脆弱性への耐性を調査した結果、第三者によるＮネットへのインターネットを通した侵入については、ログを精査することにより、その可能性が低いことは確認できたが、使用しているソフトウェアが最新でない時期があったなど、対策が万全ではなかった。

４．４　調査結果

以上の調査から、センター職員がＮネットの保守管理作業においてコンテンツの更新作業を行う際に、コンテンツと無関係のファイルをコンテンツの格納場所に誤って置いてしまった可能性が高く、本事案は、個人情報の管理に問題があった。

また、使用しているソフトウェアが最新でない時期があったなど、外部からの侵入対策に万全でないところがあった。しかし、第三者によるＮネットへの侵入については、ログを精査することなどにより、その可能性は低い。

第５章　再発防止策について

発生原因の調査結果を踏まえて以下の個人情報に係る再発防止策と今回確認された脆弱性についての対策を行う必要がある。

なお、これらの再発防止策については、すぐに実行可能なものとシステムの検討などの準備が必要となるものを仕分けし、防止策ごとに 1 週間以内から 3 ケ月以内に実施する。再発防止策の実施スケジュールを表 5 に示す。

５．１　個人情報の管理の強化

（１）取扱う個人情報の最少化

Ｎネットではこれまで、「ご質問・ご意見」コーナーで送信者の氏名、住所、電話番号、電子メールアドレス及び職業の個人情報を収集していた。本事案の再発防止のために、取扱う個人情報を少なくすることを検討し、「ご質問・ご意見」コーナーでは、入力できる項目をセンターからの返信のためのメールアドレスと、ご質問・ご意見の内容のみの必要最低限の情報とする。

（２）個人情報の保管方法

①個人情報の識別

「ご質問・ご意見」コーナーによって入力された情報は個人情報を含むことから、これらの情報は個人情報として識別し管理する。

②メールの暗号化

「ご質問・ご意見」コーナーからのメールは、セキュリティソフトを用いて暗号化して保管する。

③保管期間の設定

保管期間は１ヶ月とし、その後消去する。また、消去されたことを記録し、これを管理者が確認する。

④記録の作成

Ｎネット作業日報に、記録を残し管理する。

５．２　技術的な対策の強化

（１）システムの脆弱性への対策

①不正侵入からの保護

「IPS（Intrusion Prevention System：不正侵入防止システム)」を導入して、Ｎネットシステムを外部攻撃から保護する。

②不正侵入検知

「AIDE（Advanced Intrusion Detection Environment：高度な侵入検知環境)」を導入して、Web サーバにあるファイル及びディレクトリを確認し、予期せぬ設定ファイルの編集及びコンテンツ改ざん等の有無をコンテンツ更新の都度、更新がない場合は月１回確認する。

③パッチの適用

常に最新のパッチ情報を入手し、必要に応じてパッチを適用する。

④アタックテストの強化

これまで実施している年１回のアタックテストに加え、より効果的なアタックテストを実施し、脆弱性の有無確認の強化を図る。

５．３　人為的原因に対する対策の強化

原因となりうる可能性のある作業について、作業ミス防止のための対策を講じる。また、今回の事案のような事態が発生した場合、迅速に対応処理できるようセンターの情報セキュリティ基本方針に則り手順書の整備を実施し、教育を行う。

（１）作業ミス防止のための対策

①チェック体制の強化

コンテンツ更新作業において、コンテンツをダウンロード、編集及びアップロードする作業者とは別の者が更新されたコンテンツをアップロード前にチェックする。チェックは、アップロードする全てのファイルに対してチェックする。その結果をＮネット作業日報に記録する。

②使用媒体の限定

サーバからアップロードまたはダウンロードしたコンテンツファイルの格納に用いる電子媒体（USB メモリ）は専用のものとし、専用「アップロード・ダウンロード専用」とラベルを付して、他の使用を禁じる。

専用とする電子媒体は更新終了後、空にしたことを確認する。さらに電子媒体の使用・保管は管理表で管理する。

③手動アップロードの制限

コンテンツのファイルをアップロードする際は、ファイル転送のコマンド及び専用ソフトは使用しないこととする。コンテンツファイルのアップロード用にツールを作成し、ファイルを個々に指定してアップロードする。

④不要ファイルの有無の確認

Ｎネットでコンテンツ更新した際には、更新の都度、公開用ディレクトリ配下のファイル構造を確認して、更新予定以外のファイルの存在の有無をチェックする。チェックは前回のファイル構造と直近のものと比較する。

（２）今回の事案のような事態が発生した場合の対応策の策定

①インシデント対応手順の明確化

今回の事案のような事態が発生した場合や、システムログ、システムの稼働状況、他者からの情報提供等のインシデントが発生した場合の対応が迅速に処理できるよう、センターの情報セキュリティ基本方針に則り、手順の明確化を図る。

②インシデント発生時のログ等の評価

今後発生したインシデントについては、ログ等を評価し、その結果を具体的な対応手順としてインシデント対応手順に反映させる。

③システムログ等の保存期間の延長

インシデント発生時の原因究明のために、システムログ等のログ類の保存期間を現状の７日から３ヶ月程度から１年間を目途に延長する。このため、出力したログ類は定期的に外部記憶媒体に移行して保管することとする。

（３）手順書の整備及び教育

①手順書の整備

今回対策を実施する項目に対して手順書を整備する。本手順書は、センターの品質マネジメントシステムに則り、手順書の定期的なレビューを実施し継続的改善を行う。

②教育の実施

今回対策を実施する項目を含めたＮネットについての教育を定期的に実施し、Ｎネットの運用管理技術の向上を図る。

表５　再発防止策スケジュール

項　目	内　容	速やかに 実施 （１週間以内）	９月中に 実施予定 （１ヶ月以内）	11 月中に 実施予定 （３ヶ月以内）
個人情報の管理の強化	（１）取扱う個人情報の最小化	○		
	（２）個人情報の保管方法			
	①個人情報の識別	○		
	②メールの暗号化	○		
	③保管期間の設定	○		
	④記録の作成	○		
技術的な対策の強化	（１）システムの脆弱性への対策			
	①不正侵入からの保護		○	
	②不正侵入検知		○	
	③パッチの適用	○		
	④アタックテストの実施	○		
人為的原因への対策の強化	（１）作業ミス防止のための対策			
	①チェック体制の強化	○		
	②使用媒体の限定	○		
	③手動アップロードの制限		○	
	④不要ファイルの有無の確認		○	
	（２）今回の事案のような事態が発生した場合の対応策の策定			
	①インシデント対応手順の明確化		○	
	②インシデント発生時のログ等の評価		○	
	③システムログ等の保存期間の延長	○		
	（３）手順書の整備及び教育			
	①手順書の整備（定期的にレビュー）		○	○
	②教育の実施（定期的に実施）		○	○

第６章　おわりに

Ｎネットの運用管理においてセンターが個人情報を不適切に取扱ったことにより、そこに情報が含まれていた個人の方々、Ｎネット利用者並びに委託元の原子力規制庁に多大なご迷惑をおかけすることとなった。

本事案に対し、センターはこれまで影響の確認・拡大防止等に努めるとともに、原因調査と再発防止策の検討を本委員会に要望した。本委員会の原因調査の結果を踏まえて、センターは様々な状況を想定した再発防止策を設定し、再発防止策を速やかに実行するとともに影響確認については継続して実施することを本委員会は強く求める。

Ｎネットが環境放射線及び原子力防災の情報提供サイトとして今後も有効に利用されるよう、センターの情報セキュリティ基本方針に則り、情報及びシステムの適切な管理を実施して本事案のようなことを再び生じさせないように不断の努力が重要である。

環境防災Ｎネットにおける個人情報の不適切な取扱いに係る調査検討委員会
委員名簿

平成 25 年８月現在
（敬称略、順不同）

	氏　名	所　属
委員長	鈴木　富則	公益財団法人原子力安全技術センター　理事
委　員	鈴木　一明	独立行政法人科学技術振興機構
〃	村瀬　一郎	株式会社三菱総合研究所
〃	塩崎　哲夫	富士通株式会社
〃	梅山　信昭	公益財団法人原子力安全技術センター 企画課課長代理（情報セキュリティ統括補助者）
〃	熊本　文生	公益財団法人原子力安全技術センター 技術展開部長（情報セキュリティ推進責任者）
〃	土岐　邦彰	公益財団法人原子力安全技術センター 原子力防災事業部　研修訓練部長