

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

概要

1. 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

(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。

(2)対応状況のまとめ

対象者 33 名のうち、29 名の方に対し、電子メール、電話、郵便のいずれかで連絡を行った。4 名の方についてはメールアドレスが変更されている等により、連絡ができていない。連絡を行った 29 名のうち 12 名の方については連絡が届いていることを電子メールによる返信もしくは電話で確認をとることができた。

また、二次被害等の発生については 8 月 30 日時点で連絡はない。

2. 発生原因の調査について

(1)調査方法

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」
- ・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。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。

(2)調査結果

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、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、その可能性は低いと判断した。

3. 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。

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ヶ月以内に実施する。

(1)個人情報の管理の強化

1)取扱う個人情報の最少化

入力できる項目を当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個人情報を含むファイルを識別し管理する。
- ②「ご質問・ご意見」コーナーからのメールは暗号化して保管する
- ③保管期間は1ヵ月とし、その後消去する。
- ④Nネット作業日報に、記録を残し管理する。

(2)技術的な対策の強化

1)システムの脆弱性への対策

- ①不正侵入防止システムを導入する。
- ②不正侵入検知システムを導入する。
- ③常に最新のパッチ情報を入手し、必要に応じパッチの適用を行う。
- ④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。

(3)人為的な対策の強化

1)作業ミスの防止のための対策

- ①コンテンツ更新作業におけるチェック体制を強化する。
- ②コンテンツファイルの格納には専用の電子媒体を使用する。
- ③手動アップロードを制限する。
- ④更新予定以外のファイルの存在の有無をチェックする。

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インシデントが発生した場合の対応手順の明確化を図る。

②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、システムログ等の保存期間を延長し、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。

3)手順書の整備及び教育

①今回実施する項目に対する手順書の整備を行う。

②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実施し、Nネットの運用管理技術の向上を図る。

以下に再発防止策スケジュールを示す。

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 (定期的レビュー)		○	○
②教育の実施 (定期的実施)		○	○	

以上

環境防災Nネット個人情報の不適切な取扱いに係る調査検討委員会

1. 委員構成
- | | | | |
|-----|------|-------------------|-------------------------|
| 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 | (研修訓練部長) |

2. 委員会議事

(1)第1回検討委員会(平成25年7月25日(木))

- ・委員会の設置について
- ・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
- ・発生原因の調査について
- ・再発防止策(案)について

(2)第2回検討委員会(平成25年8月5日(月))

- ・議事録(案)について
- ・第1回委員会における指摘事項の対応状況について
- ・環境防災Nネットの構成及び環境設定について
- ・アタックテストの結果について
- ・報告書(案)について

以上