脆弱性診断情報保護規定

目次

作成・更新履歴

発行・改訂年月日	改訂版	改訂記録	作成	承認	備考
2015/06/29	1	初版	森	森	
2015/07/17	1.1	形式の修正（内容修正含まず）	森	森	

1 総則

1.1 目的

本規定は、特定非営利活動法人鹿児島インファーメーション（以下当NPO）の「情報セキュリティ方針」に基づいて、当NPOが保有する脆弱性診断情報について、適切な保護を実現することを目的とする。

1.2 対象者

脆弱性診断情報を扱う当NPOの職員。

1.3 適用範囲

当NPOが取得する全ての脆弱性診断情報(利用者から依頼された脆弱性診断の結果・診断レポート、利用者に関する情報)について適用される。なお、脆弱性診断情報の媒体については、電子媒体、紙面いずれも対象とする。

1.4 引用規格並びに順守法規

(1) 不正アクセス行為の禁止等に関する法律

(2) 不正競争防止法□（営業秘密関係）

1.5 定義

本規定において使用される用語は、次に定める。

(1) 脆弱性診断情報: 利用者から依頼された脆弱性診断の結果、および依頼元に通知するための診断レポート

(2) 依頼元情報: 脆弱性診断を依頼した利用者に関する情報

(3) 職員: 当NPOの指揮監督を受け、脆弱性診断情報の取扱いに従事する者(当NPO役職員、派遣社員、パート、アルバイト等)

2 脆弱性診断情報の取得

2.1取得の原則

脆弱性診断情報の取得は、利用者から依頼された場合に限り利用目的を明確に定めて、その目的達成のために必要な限度において行う。

2.2 取得の際の順守事項

(1) 利用者と合意された脆弱性情報のみを取得する

(2) 偽り・不正な手段により取得しない

(3) 利用者と合意された日時に限り脆弱性診断を実施し、脆弱性情報を取得する

3 脆弱性診断情報の利用、提供

3.1 利用の原則

脆弱性診断情報は、依頼元への提示と、業務の遂行上必要な限りにおいて利用できるものとする。業務には日本語以外の言語で記述された診断情報を日本語に翻訳するための業務を含む。

3.2 目的外の利用

利用目的の範囲を超えて脆弱性診断情報を利用しない。

3.3第三者提供について

あらかじめ本人の同意を得ずに脆弱性診断情報を第三者へは提供しない。ただし、下記の場合はこの限りでない。

(1) 法令に基づく場合。

(2) 生命、身体または財産の保護に必要がある場合であり、依頼元の同意を得ることが困難な場合。

(3) 使用する診断ツールのモジュールに紐付けされ当NPOにより日本語に翻訳された脆弱性診断情報。

3.4 委託について

脆弱性診断情報の取扱いを委託する場合は、関係法令及び当NPO内規定と同等の取扱い管理が行われることを確認の上、委託先を決定し、秘密保持に関する契約を締結することとする。また、委託先の安全管理が徹底するように、必要であれば監督を行う。

4 脆弱性診断情報の管理

4.1 正確性を確保

利用目的の範囲内で、脆弱性診断情報を正確に保つこと。

4.2 安全性の確保

(1) 脆弱性診断情報を格納したサーバは、安全な場所に隔離し、盗難対策をとること。

(2) 脆弱性診断情報を格納したサーバは、アクセス権設定を行い、必要最小限者のみがアクセス可能な状態を維持するようにすること。

(3) 文書ファイルの保管時は、鍵のかかるキャビネットに保管しておくこと。

(4) 脆弱性診断情報を破棄する際は、上書きソフトを使用するなど適切な処理を施すこと。

(5) 情報セキュリティ管理責任者は､脆弱性診断情報にアクセスする担当者が脆弱性診断情報の取扱いを適切に行うことに関する管理責任を負うこと。

(6) 情報セキュリティ管理責任者は、日常的に脆弱性診断情報の管理状況を確認し、問題を発見した際には、速やかに改善すること。

(7) 脆弱性診断情報を以下のような操作ミス等により漏洩することがないような考慮をすること(システムによる保護、複数人管理等)。

- メールによるアドレスの誤送信
- FAX による宛先間違いの誤送信
- ファイル転送による誤送信
- 媒体による住所間違いの誤配送
- 不適切な文書管理による流出

4.3消去・廃棄

脆弱性診断情報は、利用目的の終了後に速やかに廃棄・消去すべきであるが、外部流出等の危険防止のために、 廃棄責任者を決め、適切な方法(裁断、媒体破壊等)により実施し、廃棄記録を残すこと。

5 脆弱性診断情報の開示・訂正・利用停止・削除

5.1 透明性の確保

依頼元から自己の情報について開示・訂正・利用停止・削除の求めがあった際には、合理的な期間内にこれに応じるものとする。

5.2 依頼元の情報の利用又は提供の拒否

依頼元から自己の情報について利用又は第三者提供の拒否をされた場合は、これに応じるものとするが、法令に基づく場合は、この限りでない。

6 脆弱性診断情報の苦情及び相談

当NPOは、脆弱性診断情報に関する相談窓口を設置し、依頼元からの脆弱性診断情報に関する苦情及び相談を受付けて遅滞なく対応するものとする。

7 雑則

7.1 罰則事項

本規定の順守事項に違反した者は、当NPO就業規則に基づいて対処する。