情報セキュリティインシデント対策管理規程

株式会社三重県農協情報センター

改廃履歴

Rev	改 廃 内 容	実 施 日
1.0	初版	2020.03.01

目　　次

情報セキュリティインシデント対策管理規程

規程番号　５００８－０００－００－規
制 定 日　２０２０年　3月　1日

（目　的）
第　１条　本規程は、情報セキュリティに関するインシデント（以下、「インシデント」という）が発生した場合、ＣＳＩＲＴおよび情報利用者がおこなうべき対応内容を記載し、インシデント発生時から解決までの一連の処理が迅速におこなわれることを目的として定める。

（体　制）
第　２条　インシデント対策については、情報セキュリティ管理組織体制のもと、ＣＳＩＲＴ責任者が統括し、各部門の情報セキュリティ管理者へ具体的な対策を指示する。

（役割・責任）
第　３条　インシデント対策における各管理・責任者は主に以下の役割を担う。
（１）ＣＳＩＲＴ責任者
インシデント対策における全社的な責任を負う。
（２）情報セキュリティ責任者
ＣＳＩＲＴ責任者の指示のもと、部門におけるインシデント対策責任を負う。
（３）ＣＳＩＲＴ
ＣＳＩＲＴ責任者の指示のもと、インシデントの具体的な対策をおこなう。
①　インシデント内容の確認、発生前の通信状況や操作内容等の情報収集をおこなう。
②　インシデント発生時には速やかに対策を実施する。
③　インシデント発生要因の再発防止策を検討する。
（４）システム担当部門／運用担当部門
①　サーバやパソコンのウイルス最新パターンファイルの更新管理をおこなう。
②　システムのアクセス権やログ等を監視する。
③　インストールされているソフトウェアの管理をおこなう。

（定義）
第　４条　この規程で「不正アクセス」とは、Ｗｅｂの改ざんとＳＱＬインジェクションに代表されるＷｅｂアプリの脆弱性悪用と定義づける。

（インシデント対策の必要性）
第　５条　情報利用者は、ウイルス感染をはじめとしたセキュリティ事故の被害状況等の情報に注意をはらうとともに、以下のセキュリティ事故の被害を防止するために、セキュリティ対策の必要性を認識する。
（１）パソコン内のデータが改ざん・破壊される。
（２）パスワードやクレジット番号などの個人情報を搾取される。
（３）個人情報が搾取され外部へ流出した場合、組織の社会的信用問題や損害賠償の対象となる。
（４）サーバやパソコンのリカバリが必要となった場合は、復旧に膨大な時間がかかる。
（５）ウイルス付きメールの送信などにより、知人や他人に対しウイルス感染の危険性がある。

（6）大量のデータ送信によりネットワークに負荷をかけ、ネットワークの遅延、業務システムが利用できない等の事象が発生する。

（インシデント予防）

第　6条　ウイルス感染をはじめとしたセキュリティ事故を予防するために、以下のセキュリティ対策を実施する。

（1）ウイルスチェック

情報利用者は、次の場合にはウイルスチェックを実施する。なお、新規にＰＣを導入したときは、運用部門の担当者が実施する。

① 修理等でメーカー等外部の人が使用したとき。
② 修理又は作業等でＰＣを外部から持ち帰ったとき。
③ 新規ソフトウェアを導入（インストール）したとき。
④ 外部とのファイルの受渡しをおこなうとき。
⑤ 外部からＰＣを持ち込みしたとき。

（2）不正アクセス予防

運用部門の担当者は、不正アクセス予防として、以下の対策を実施する。

① 適切なアクセス権を設定する。
② 可能な限りアクセス制御管理規程に準拠したパスワードを設定する。
③ アクセスログを収集する。

（3）ＤＤｏＳ攻撃の予防

運用部門の担当者は、ＤＤｏＳ攻撃予防として、以下の対策を実施する。

① 必要な機器やネットワークはセキュリティ監視をおこなう。
② リスクの高いサイトからのアクセスを拒否する。
③ 可能な端末はＯＳやアプリケーションを最新にする。

（インシデント発見）

第　7条　情報利用者は以下に該当するような兆候については、常に注意をはらう。兆候を感じたり、問い合わせを受けたりした場合は、自部門の情報セキュリティ管理者へ連絡をおこなう。なお、ウイルス感染の兆候に関しては、情報利用者が一次対応もおこなう。

（1）ウイルス感染の兆候

以下に該当する場合は、ウイルス感染の疑いがあるものとして対応する。

① ウイルスチェックプログラムが検出した。
② 突然パソコンの動きが止まる、不安定になる。
③ 突然パソコンが立ち上がらない。
④ 突然パソコンがネットワークに繋がるのが遅くなる、または繋がらない。
⑤ 不審なメールが到着している。または異常にメールが多い。
⑥ 身に覚えのないファイルが生成されたり、ファイル名や拡張子が変更されたりする。
⑦ その他パソコンの動作がいつもと違う。

（2）ウイルス感染時の一次対応

前項の兆候があった場合、情報利用者は以下の一次対応を実施する。

① 該当機器（ＰＣ・サーバ）をネットワークから切り離す。

② 該当機器（ＰＣ・サーバ）の電源は極力切らず、操作等もおこなわない。
（サービスログ等の証跡が消える、二度と立ちあがらなくなる等の回避）

（3）不正アクセスの兆候
以下に該当する場合は、自部門の情報セキュリティ管理者へ連絡をおこなう。
① 情報センターのＷＥＢサイトから不審なサイトに誘導された。
② 情報センターのＷＥＢサイト閲覧時、マルウェアに感染した。
③ 情報センターのＷＥＢサイトに身に覚えのない情報が掲載されている。

（4）ＤＤｏＳ攻撃の兆候
以下に該当する場合は、自部門の情報セキュリティ管理者へ連絡をおこなう。
① 情報センター公開サーバを利用しているＷＥＢサイトが閲覧困難になる。
② インターネット接続が遅い、もしくは繋がらない。

（インシデント検知・通知）
第 8条 システム担当部門／運用担当部門は、ファイアウォールやウイルス対策ソフトマネージャ等で検知・通知されたインシデントについて、ＣＳＩＲＴへ連絡をおこなう。

（トリアージ）
第 9条 ＣＳＩＲＴおよびシステム担当部門／運用担当部門は、インシデントの重要度や深刻度に応じて対応要否や対応順序の判断をおこなう。
（1）情報収集・調査
インシデント内容の確認、発生前の通信状況や操作内容などの情報を収集し調査をおこなう。

① ウイルス感染
インシデント発見者およびシステムログ等を確認する。
② 不正アクセス
インシデント発見者およびシステムログ等を確認する。
③ ＤＤｏＳ攻撃
ファイアウォールの接続ログ等を確認する。

（2）対応要否判断
ＣＳＩＲＴは、調査結果から対応要否および対応順序の判断をおこない、対応が不要であればインシデント発見者へ対応終了の連絡をおこなう。なお、ウイルス感染に関しては、インシデント発見者へ対応終了の連絡とともに、ネットワークへの再接続許可などもおこなう。

（インシデント対応）
第１０条 ＣＳＩＲＴおよびシステム担当部門/運用担当部門はベンダーと連携し、インシデントの詳細分析と対応方法を決定する。
（1）事象の分析
① ウイルス感染
ア．対象端末の動作、ログ等の確認
イ．対象端末以外の動作、ログ等の確認
ウ．ウイルス対策マネージャーでのログ等の確認
エ．影響範囲の特定

② 不正アクセス
ア．ＷＥＢサイト閲覧端末の動作、ログ等の確認
イ．公開ＷＥＢサーバのＦＴＰログ等の確認
ウ．ファイアウォールでの接続ログ等の確認
エ．影響範囲の特定

③ ＤＤｏＳ攻撃
ア．ファイアウォールの接続ログ等の確認
イ．攻撃先ＩＰアドレスの確認
ウ．影響範囲の特定

（2）対応方法の決定
ＣＳＩＲＴは詳細分析の結果から対応方法を決定し、報告書にて情報セキュリティ委員会へ報告をおこなう。なお、報告書は「情報セキュリティインシデント対応報告書」を使用する。対応方法検討の結果、対応不要と判断した場合は、情報セキュリティ委員会への報告とともにインシデント発見者へ対応終了の連絡もおこなう。

（対応実施）
第１１条　ＣＳＩＲＴ、システム担当部門/運用担当部門およびベンダーは、以下のインシデント対応等を実施し、情報セキュリティ委員会へ報告をおこなう。なお、報告書は「情報セキュリティインシデント対応報告書」を使用する。

（1）ウイルス感染
① 端末のネットワーク遮断とウイルス検査
② インシデント発生の要因となっているシステムのシャットダウン
③ ウイルスの除去
④ システム、データの復旧

（2）不正アクセス
① ファイアウォールでの不正アクセス元ＩＰアドレスの遮断
② システム、データの復旧

（3）ＤＤｏＳ攻撃
① 情報センター公開サーバの利用団体、ＪＡへの連絡。
② 公開サーバのネットワークを切断する。
③ ＤＤｏＳ攻撃が止まることを確認。
④ 公開サーバのネットワークを復旧する。
⑤ 情報センター公開サーバの利用団体、ＪＡへの報告。

（再発防止）
第１２条　ＣＳＩＲＴ、システム担当部門/運用担当部門は、インシデント発生要因に対してどのような事前対策が可能であるか検討をおこなう。

（1）パッチ適用、ソフトウェア更新ルールの見直し
（2）監視体制の強化

（3）セキュリティポリシーの見直し

（記　録）

第１３条　情報セキュリティ委員会事務局は、情報セキュリティインシデント対応報告書の記録・保管をおこなう。