ＣＳＩＲＴ運営要領

株式会社三重県農協情報センター

改廃履歴

Ｒｅｖ	改 廃 内 容	制　定　日
1.0	初版	2016/09/01

ＣＳＩＲＴ運営要領

規程番号　０３０１－０００－０８－要
制 定 日　　２０１６年０９月０１日
改 正 日　　年　月　日

（目的）
第　１条　この要領は、情報セキュリティ対策規程第２条（情報セキュリティ管理組織および体制）および第３条（情報セキュリティ管理組織体制の役割）にて定められたＣＳＩＲＴ（Computer Security Incident Response Team)について、求められる役割を果たすため、その運営要領を定める。

（名称）
第　２条　この組織は、「ＣＳＩＲＴ」（シーサート）と称する。

（組織の位置づけ）
第　３条　ＣＳＩＲＴは、情報セキュリティ対策規程第２条（情報セキュリティ管理組織および体制）および第３条（情報セキュリティ管理組織体制の役割）の定めにより情報セキュリティ委員会の専門部会として設置する。
２　本要領第５条（任務）にて定められた任務の遂行にあたって、重要な事項は情報セキュリティ委員会へ報告する。
３　新たな情報セキュリティ対策や改善を実施する場合は、情報セキュリティ委員会の承認を得る。
４　インシデントの対応にあたって緊急性がある場合は、情報セキュリティ委員会の承認および指示を待つことなく、ＣＳＩＲＴ責任者のもと対応策を検討、実施、指示することができる。ただし、情報セキュリティ委員会の指示があった場合は、この限りではない。

（構成）
第　４条　ＣＳＩＲＴの構成は、情報セキュリティ対策規程第３条（８）「ＣＳＩＲＴ責任者およびＣＳＩＲＴ」の定めにより次のとおりとする。
（１）構成員は次のとおり。
①ＣＳＩＲＴ責任者は、運用部の部長とする。
②情報セキュリティにかかる技術者は、運用部から３名、開発部から２名を選任する。
③情報セキュリティ委員会との連絡・調整を図る事務局員は、情報セキュリティ委員会事務局員のなかから１名を選任する。
④構成員はいずれも所属部門の職務との兼務とする。
（２）上記の構成員②の指名にあたっては、ネットワーク管理、システム管理、システム開発のいずれかを１年以上経験し、会社が認めた情報セキュリティ関連資格を取得あるいはＣＳＩＲＴ責任者がその能力を有すると認めたものを対象とする。なお、会社が認めた情報セキュリティ関連資格とは、資格取得表彰細則__別表１（資格・検定一覧）に定めた資格のうち情報セキュリティをテーマとした資格とする。
（３）ＣＳＩＲＴ責任者は、任務遂行のため、選任された要員のほか必要な要員を随時招集することができる。

（任務）

第　５条　ＣＳＩＲＴの任務は、情報セキュリティ対策規程第３条（８）「ＣＳＩＲＴ責任者およびＣＳＩＲＴ」の定めにより、情報システムに対する「故意」や「攻撃」によるインシデントについて一元的に対応することとする。

２　ＣＳＩＲＴが対応するインシデントは、ウィルス感染、不正アクセス、不正使用、ＤＤｏＳ攻撃などの故意または攻撃により、情報システムの正常な運用または利用を阻害する事案、情報の漏洩、改竄、消失などを引き起こす事案およびそれらの疑いがある事案とする。

３　インシデントの発生を抑制する事前対策を実施する。

①通報・連絡にかかる体制・手段の整備、周知
②情報セキュリティ対策の検討および情報セキュリティ委員会への答申
③インシデント対応手順書の整備
④インシデント早期発見のためのモニタリング（ログ管理・分析等）
⑤システム評価（脆弱性分析）
⑥ＩＴセキュリティ最新情報収集（インシデント・セキュリティ対策技術など）
⑦従業員に向けたＩＴセキュリティ教育、訓練
⑧従業員に向けた注意喚起

４　インシデント発生時には被害を極限化する事中対策を実施する。

①通報受付窓口
②情報セキュリティ委員会ほか外部関係組織へ連絡(発見)
③状況把握
④証拠保全
⑤被害抑制のための方策の決定
⑥必要に応じて社内の要員招集、社外協力ベンダー等へ支援要請
⑦緊急対応実施（隔離、遮断など被害抑制）、各部への指示
⑧情報セキュリティ委員会ほか外部関係組織へ報告(中間・結果)

５　インシデント収束後はシステム利用環境を早期復旧させる事後対策を実施する。

①脆弱性対応
②システム復旧（全面利用）、各部への指示
③復旧後のモニタリング
④再発防止策の検討および情報セキュリティ委員会への答申
⑤情報セキュリティ委員会ほか外部関係組織へ報告(結果)
⑥従業員に対し、インシデントの攻撃手法と対策についての情報共有と注意喚起

（教育）

第　６条　ＣＳＩＲＴ責任者はＣＳＩＲＴ要員すべてが、任務を実施するために必要な力量をもてるように教育を計画し、実施する。

２　ＣＳＩＲＴ要員に必要な力量は、セキュリティ対策の現状評価、改善案の立案ができることに加えて、インシデント発生の早期発見、被害・影響の把握、原因究明、被害拡大防止、インシデントの収束、システムの回復、再発防止策の策定などの能力を有すること。

３　教育内容は、システム管理、ネットワーク管理等幅広いＩＴ技術に加えて、コンピュータ・ネットワークに対する脅威、攻撃手法、ウィルス対策、不正アクセス対策の知識およびサイバー攻撃や内部不正など最新インシデント情報等を対象とする。

４　情報セキュリティ関連資格の取得を推奨し、支援する。