湘南工科大学情報セキュリティインシデント対応チーム（SHONAN-CSIRT）設置要項

制定　令和４年７月13日

（趣旨）

１　この要項は、湘南工科大学情報セキュリティポリシー（以下「セキュリティポリシー」という。）と湘南工科大学情報セキュリティ対策基準（以下「対策基準」という。）に基づき、湘南工科大学情報セキュリティインシデント対応チーム（以下「SHONAN-CSIRT」（ショウナンシーサート）という。）の設置及び運用に関して必要な事項を定める。

（目的）

２　SHONAN-CSIRTは、湘南工科大学（以下「本学」という。）において情報セキュリティに係るインシデント発生時は、迅速に被害の拡大防止と再発防止策を計画立案し、実施することを目的とする。

（組織）

３　SHONAN-CSIRT は、本学のセキュリティポリシーと対策基準に基づき、次に掲げる者で組織する。

（１）最高情報セキュリティ責任者
（２）全学システム管理責任者
（３）部局システム管理責任者
（４）システム管理者
（５）学外機関への連絡担当部局の責任者
（６）情報セキュリティ担当部局の職員
（７）その他CISOが必要と認めた者

（SHONAN-CSIRTの統括）

４　最高情報セキュリティ責任者はChief Information Security Officer（以下「CISO」という。）とし、SHONAN-CSIRTの業務を統括する。なお、緊急を要する場合でCISOが職務を遂行できないときは、全学システム管理責任者がその職務を代行する。

（業務）

５　SHONAN-CSIRTは、情報セキュリティのインシデント対応に係る次に掲げる業務を行う。

（１）インシデント発生時の通報受付及び状況の把握と記録に関すること。
（２）学内及び学外への連絡調整と情報提供に関すること。
（３）インシデントの障害区分の切り分けと初期対応に関すること。
（４）被害の拡大防止と復旧に必要な技術的対応に関すること。
（５）インシデントの原因調査及び再発防止策の計画立案に関すること。
（６）その他インシデント防止に関わる部局等への助言及び指導に関すること。

6 SHONAN-CSIRTは、５に定めた業務を行うに当たり、必要に応じて次に掲げる措置を講じるものとする。

（１）インシデント検知のためのネットワーク監視

（２）インシデント調査のための通信パケットの収集と解析

（３）インシデント調査のためのサーバ及びパソコン、その他機器等のログの収集と解析

（４）マルウェアの検知及び駆除

（５）ファイアウォールの操作

ポート遮断等の設定変更が有効な措置として認められる場合は、全学システム管理責任者の判断で当該措置を実施する。ただし、設定変更の影響が大きいと判断され、時間的猶予がある場合には、関係者に連絡した上で実施するものとする。

（６）ネットワークの全面停止

ネットワークにおける被害が全学におよび、ネットワークの全面停止以外に適切な措置が認められない場合、CISOの指示に基づき当該措置を実施する。ただし、被害が拡大するおそれがあり、緊急を要する場合は、全学システム管理責任者の判断で当該措置を実施する。その場合、全学システム管理責任者は事後にCISOに報告し承認を得るものとする。

（７）ネットワークの一部停止

ネットワークの一部停止が有効な措置として認められる場合、その停止箇所を管理する全学システム管理責任者及び各部局システム管理責任者に連絡した上で当該措置を実施する。ただし、被害が拡大するおそれがあり、緊急を要する場合は、各部局の利用者やシステム管理者、または情報セキュリティ担当部局の職員が当該措置を実施し、事後に当該停止箇所の管理責任者に報告し承認を得るものとする。

（８）その他インシデント対応に関して必要な措置

7　SHONAN-CSIRTへの報告・相談の受付はメディア情報センターが行う。