椙山女学園電子情報リスク対応規程

平成１９年規程第３２号
平成１９年１０月２６日

（趣旨）

第１条　この規程は、椙山女学園電子情報セキュリティ規程（平成１９年規程第１８号）第９条の規定に基づき、意図的又は偶発的に生じる、本学園規程等又は法律に違反する情報セキュリティ上の事故又は事件等（以下「リスク」という。）に適切に対応するために必要な事項を定めるものとする。

（適用範囲）

第２条　この規程の適用範囲は、リスクの発生から対応、復旧及び報告までとする。なお、緊急を要するリスクの対応については、別に定める。

（リスク区分）

第３条　リスクは、次のとおり区分する。

(1)　情報破壊　　情報資産の破壊、破損又は喪失
(2)　情報改ざん　　情報資産の意図しない、悪影響のある修正又は変更
(3)　情報漏洩　　情報資産の不正複製、盗難、流出又は学外紛失
(4)　不正アクセス　　権限がない者の情報資産へのアクセス
(5)　ウイルス感染　　ウイルス、ワームなど悪意あるソフトウェアの侵入又は感染
(6)　サービス停止　　情報資産が必要なときに利用不可になること。

（被害レベル区分）

第４条　リスクによる被害の程度は、最終的に被害が及ぶ範囲により次のとおり区分する。

(1)　被害レベル１　　被害にまでは至らないが被害が発生する可能性があった事象又は将来において被害が発生する可能性がある事象若しくは兆候が発見されたとき。
(2)　被害レベル２　　職員等個人の業務遂行に被害が及ぶとき。
(3)　被害レベル３　　所属内の業務遂行に被害が及ぶとき。
(4)　被害レベル４　　学園全体の業務遂行に被害が及ぶとき。
(5)　被害レベル５　　外部に被害が及ぶとき。

（リスク発生時の報告）

第５条　構成員は、リスクの発生を発見したときは、被害の程度を判断し、次の各号に規定する報告先に報告しなければならない。

(1)　被害レベル１及び２　　学園情報センター
(2)　被害レベル３、４及び５　　当該所属の電子情報セキュリティ管理者（以下「管理者」という。）及び学園情報センター

２　前項の報告を受けた学園情報センターは、被害レベル４及び５の場合は、電子情報セキュリティ管理責任者に報告する。

（構成員のリスク対応）

第６条　構成員は、前条に定める報告先に報告するとともに、被害レベルに応じて次のとおり対応する。

(1)　被害レベル１

リスク区分によらず、リスクを発見し次第、被害可能性及び被害内容について学園情報センターに報告する。

(2)　被害レベル２

ア　情報破壊及び情報改ざんの場合は、リスクの原因の特定及び応急処置、バックアップによる復旧又は再作成並びに原因対策を実施する。原因が特定できない場合は、学園情報センターに相談する。

イ　情報漏洩及び不正アクセスの場合は、リスクの特定、応急処置及び今後の予防策を実行する。原因の特定、応急処置及び今後の予防策が不明の場合並びに個人で実行不可能な場合は、学園情報センターに相談する。

ウ　ウイルス感染の場合は、ネットワークケーブル又は無線LANカードを抜き、原因の特定、応急処置及び今後の予防策を実行する。原因の特定、応急処置及び今後の予防策が不明の場合並びに個人で実行不可能な場合は、学園情報センターに相談する。

エ　サービス停止の場合は、原因の特定、応急処置及び今後の予防策を実行する。原因の特定、応急処置及び今後の予防策が不明の場合並びに個人で実行不可能な場合は、学園情報センターに相談する。

(3)　被害レベル３及び４

ア　情報破壊、情報改ざん、情報漏洩及び不正アクセスの場合は、発見した事実をできるだけ速やかに第５条に規定する報告先に報告する。

イ　ウイルス感染の場合は、ネットワークケーブル又は無線LANカードを抜き、発見した事実をできるだけ速やかに第５条に規定する報告先に報告する。

ウ　サービス停止の場合は、発見した事実をできるだけ速やかに第５条に規定する報告先に報告する。

(4)　被害レベル５

ア　情報破壊、情報改ざん、情報漏洩及び不正アクセスの場合は、発見した事実を直ちに第５条に規定する報告先に報告する。

イ　ウイルス感染の場合は、ネットワークケーブル又は無線LANカードを抜き、発見した事実を直ちに第５条に規定する報告先に報告する。

ウ　サービス停止の場合は、発見した事実を直ちに第５条に規定する報告先に報告する。

（重要度の高いリスク対応）

第７条　学園情報センターは、リスクの重要度を第４条に規定する被害レベルから判断し、重要度の非常に高いリスクの場合、次のとおり対応する。

(1)　リスク対応チーム組織

ア　学園情報センターは、速やかに電子情報セキュリティリスク対応チームを招集するとともに、管理責任者に報告し、指示を受ける。

イ　リスク対応チームのリーダー及び構成員は、学園情報センター、総務部、企画広報部、財務管財部及び当該部門の中から、リスクの規模及び内容に応じて適宜学園情報センターが指名する。

(2)　原因解析

ア　リスク対応チームは、リスクの発生原因及び被害の程度を分析するため、当該システムの運用責任者及び開発責任者（以下「解析者」という。）に、リスクの原因解析を依頼する。

イ　リスク対応チームは、解析者からの解析報告に基づき、リスクの発生原因及び被害の具体的な程度を分析し、暫定策、恒久策及びそれに係る概略工数を立案する。

ウ　リスク対応チームは、被害レベルの重要度に応じて、発生原因及び脅威の識別、暫定策及び恒久策並びに概略工数（必要であればコストを含む。）を管理者に報告する。

(3)　対策実施

ア　リスク対応チームは、解析者からの解析報告を検討し、リスク対策を実施する場合、当該リスクに係る対策を実施する担当者（以下「実施者」という。）に依頼する。

イ　実施者は、リスク対応チームから指示された仕様に従い、暫定策及び恒久策を実施する。

ウ　実施者は、対策を実施後、評価結果を管理者に報告し、再稼動の可否を問う。

(4)　評価結果審査

ア　管理者は、実施者から報告を受けた評価結果及び効果の確認を行い、再稼動の可否を判断し、利用者に報告する。

イ　管理者は、改善及び予防処置につなげるために、発生原因から脅威を特定し、記録する。

(5)　電子情報セキュリティ委員会への報告

管理者は、リスクの発生及び解析結果の報告、対策案の実施可否、再稼動の可否など、必要に応じて電子情報セキュリティ委員会へ報告する。

(6)　改善・予防処置

リスク対応チームは、再発が予測されるリスクの場合は、別に定める改善・予防処置を実施する。

（重要度の低いリスク対応）

第８条　管理者は、リスク対応チームを組織しない場合のリスク対応を行い、学園情報センターが支援する。

２　リスクのうち、当該システム又はアプリケーションで別途対処方法が定められている場合は、その手順に従う。

３　管理責任者は、リスクの原因を特定し、再発防止に努める。

（リスクの届け出）

第９条　管理責任者は、発生したリスクが故意の犯罪に基づくと判断する場合、それぞれ必要な関係機関に届け出るものとする。

（訓練）

第１０条　電子情報セキュリティ管理者会議は、リスクに対し速やかに対応できるように必要な訓練を実施するものとする。

附　則

この規程は、平成１９年１０月２６日から施行する。

附　則（令和７年規程第３７号）

この規程は、令和７年４月１日から施行する。