椙山女学園電子情報セキュリティ緊急対応規程

平成１９年規程第３３号
平成１９年１０月２６日制定

（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１２条の規定に基づき、緊急性の非常に高い電子情報セキュリティ事故（以下「事故」という。）が発生した場合又は発生すると予測される場合、速やかな対応を図り、事故の拡大防止及び早期復旧又は被害の防止を行うために必要な事項を定めるものとする。

（権限）

第２条　学園情報センター長は、緊急対応のために必要と判断する場合には、構成員に対し被害の予防又は拡大防止のため、次のことを行うことができる。

(1) 情報機器の利用停止指示、サービス提供の中止又は禁止指示及び情報の開示要求
(2) 早期復旧のため応急処置及び処置後のサービス再開に関する決定
(3) 処置対応のために必要な関連する職員（必要であれば、職員以外の者も含む。）の招集
(4) 開示要求の対象とした構成員の情報への必要最小限の接触

（権限委譲）

第３条　次の各号に掲げる場合には、当該各号に定めるものに権限を委譲することができる。

(1) 学園情報センター長不在のときは、ネットワーク主幹がその職務を代行する。
(2) 学園情報センター長及びネットワーク主幹ともに不在のときは､情報支援課長がその職務を代行する。

（守秘義務）

第４条　学園情報センターの処置担当者は、構成員の情報を被害の予防及び拡大防止並びに早期復旧のためにのみ利用し、この目的以外に公開、利用してはならない。

（対応）

第５条　学園情報センターは、学園情報センター長の指示の下に、情報セキュリティ事故（情報破壊、情報改ざん、情報漏洩、不正アクセス、ウイルス感染、サービス停止等）に対して以下の対応を図らなければならない。

(1) 電子情報セキュリティ管理責任者（以下「管理責任者」という。)、管理者、ネットワーク管理責任者に緊急対応を行う旨の周知
(2) 学園内に重大な被害を及ぼす事態の防止又は進行・拡大阻止
　ア　原因（二次的な原因を含む。）となる、又は原因と疑われるサーバ、アカウント、ネットワーク機器、ＰＣ等の利用停止指示
　イ　情報資産保護のためのネットワーク遮断並びに各種ログ調査及び分析
　ウ　機密性レベル３以上の場合における漏洩の拡大阻止並びに漏洩ルートの追跡及び原因究明
　エ　サーバ等のバックアップデータからの復旧
　オ　完全性・可用性レベル３以上の場合における情報システムの早期復旧
(3) 学園の構成員又は情報機器を原因として学園外に被害を及ぼす事態の防止又は早期除去
　ア　原因（二次的な原因を含む）となる、又は原因と疑われるサーバ、アカウント、ネットワーク機器、ＰＣ等の利用停止指示
　イ　外部の情報資産保護のためのネットワーク遮断並びに各種ログ調査及び分析
(4) 状況及び対応処置等の内外への必要最小限の告知
(5) 事故原因の特定、応急処置の実行及び処置結果の確認並びに可能な範囲でのサービス再開

（報告）

第６条　学園情報センター長は、管理責任者及び該当する部門の管理者に、処置対処後の報告並びに恒久処置及び予防策の提案を行う。

附　則

この規程は、平成１９年１０月２６日から施行する。