○学校法人名古屋電気学園情報セキュリティ対策規程

（目的）

第１条　この規程は、学校法人名古屋電気学園（以下「学園」という。）のシステム・機器へのサイバー攻撃、電子媒体の盗難・紛失等による個人情報・学術情報等重要データの漏えい、不正アクセス、Webサイト改ざん、システム機能不全等の情報セキュリティインシデント発生を防止するため、学園事務局及び各設置校の情報セキュリティ対策水準の維持・向上を図るとともに、情報セキュリティインシデントが発生した場合の対処について定めるものとする。

（用語の定義）

第２条　この規程における用語の定義は、次の各号に定めるとおりとする。

⑴　情報セキュリティ　情報の機密性、完全性、可用性を維持することをいう。

⑵　機密性　情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保することをいう。

⑶　完全性　情報が破壊、改ざん又は消去されていない状態を確保することをいう。

⑷　可用性　情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。

⑸　情報セキュリティインシデント　以下の行為により情報セキュリティの確保が困難な事象、その恐れのある事象をいう。

ア　ネットワークや情報システムの稼働を妨害し、又は、データの搾取、改ざんや消失を起こす行為

イ　ネットワークの帯域やディスクやCPUの資源を浪費するなど、ネットワークやシステムの機能不全や障害又は利用者の迷惑となる行為

⑹　構成員　学園の学生、生徒、職員及び学園内において業務を行うことが認められている者をいう。

（情報セキュリティインシデントのレベル）

第３条　情報セキュリティインシデントはその事象により次の各号に定めるレベルに分ける。

⑴　レベル１　個人、単一部署に影響のある事象

⑵　レベル２　複数部署、複数ユーザに影響が及ぶ事象

⑶　レベル３　学園外に影響が及ぶ事象

（最高情報セキュリティ責任者）

第４条　学園に、最高情報セキュリティ責任者（Chief Information Security Officer）（以下「CISO」という。）を置く。

２　CISOは、学園事務局長をもって充てる。

３　学園事務局長は、学園事務局長が不在時、代わってCISOの責務を果たす者を予め指名しておく。

４　CISOは、学園全体の情報セキュリティ対策の維持・向上を推進するとともに必要な措置を講ずる。

５　CISOは、学園全体に影響をおよぼすインシデント発生時、解決に向けた対処を統括し、必要な措置を講ずる。

（構成員の責務）

第５条　構成員は、指針の定めるところにより情報セキュリティ対策への意識を持ち、学園の情報セキュリティ対策管理体制の下で、その職務の遂行にあたらなければならない。

２　所属長は、当該部署における情報セキュリティ対策の責任者であり、学園の情報セキュリティ対策

管理体制の下で、情報セキュリティ対策を推進するとともに、必要な措置を講じる。

（情報セキュリティ対策学園委員会）

第６条　学園及び設置校における情報セキュリティ対策に必要な事項を審議するため情報セキュリティ対策学園委員会（以下「学園委員会」という。）を置く。

２　学園委員会に委員長を置き、CISOをもって充てる。

３　委員は、学園事務局の各部次長及び委員長の指名する者とする。

４　設置校における情報セキュリティ対策に必要な事項を審議するため、設置校に委員会を置く。

５　学園委員会の庶務は、情報システム部情報システム課において行う。

（情報セキュリティ専門委員会）

第７条　学園委員会で審議する内容を企画し、決定した対策を実行するため情報セキュリティ専門委員会（以下「情報専門委員会」という。）を置く。

２　情報専門委員会に委員長を置き、情報システム部長をもって充てる。

３　委員は、委員長の指名する者とする。

４　情報専門委員会の庶務は、情報システム部情報システム課において行う。

（情報セキュリティ組織連絡協議会）

第８条　学園委員会で審議・決定した事項の各設置校への連絡、及び、各設置校での取組・発生したインシデントの報告を行うため､設置校の代表者で組織する情報セキュリティ組織連絡協議会（以下「情報組織連絡協議会」という。）を置く。

２　情報組織連絡協議会の庶務は、情報システム部情報システム課において行う。

（インシデント発生時の初期対応等）

第９条　構成員は、情報セキュリティインシデントの発生を発見、又は、情報を入手したら、直ちに所属長及び情報システム課に通報しなければならない。併せて、感染の拡大を防ぐため、該当パソコン等を物理的にネットワークから切断するなど必要な初動対策を行わなければならない。

２　通報を受けた所属長は、速やかに状況を確認し、該当システムの運用管理部署所属長及び情報システム課長へ報告するとともに必要な措置を講じなければならない。

（インシデント対策学園本部の設置）

第10条　CISOは、インシデントが発生した場合において、対策を講じる必要があると判断する場合は、速やかにインシデント対策学園本部（以下「対策学園本部」という。）を設置する。

２　対策学園本部は次の各号に掲げる者をもって組織する。

⑴　CISO

⑵　情報システム部長

⑶　総務部長

⑷　情報システム課長

⑸　総務課長

⑹　広報課長

⑺　CISOの指名する者

３　本部長はCISOをもって充てる。

４　第２項第７号の者は、発生したインシデントの事象ごとにCISOが指名する。

５　対策学園本部は、本部長が、該当インシデントの対策が終息したと判断し宣言したとき、解散するものとする。

6　対策学園本部の庶務は、情報システム部情報システム課において行う。

（インシデント対策学園本部の権限）

第11条　対策学園本部は、CISOの指揮の下に、速やかにインシデントの解決に向け対処しなければならない。

2　設置校、その構成員は、対策学園本部の指示に従わなければならない。

3　対策学園本部は、インシデントの対処にあたり、学園の定めるところにより必要とされる手続きを省略することができる。

4　CISOは、必要に応じ、設置校の情報セキュリティ責任者に対し、インシデント対策本部の設置を要請することができる。

（対策学園本部の業務）

第12条　対策学園本部は、次の各号に掲げる業務を行う。

⑴　発生したインシデントに係る情報収集及び分析

⑵　発生したインシデントの解決に向けた必要な対策の決定及び実施

⑶　発生したインシデントに係る構成員等への注意喚起

⑷　発生したインシデントに係る関係機関への報告

⑸　発生したインシデントに係る報道機関等、学外への対応

⑹　各設置校の「インシデント対策本部」との連携、必要事項の指示

⑺　その他発生したインシデントへの対応に関する必要な事項

（その他）

第13条　この規程に定めるもののほか必要な事項は、学園委員会の議を経て、理事長が別に定める。

附　則

この規程は、平成29年6月1日より施行する。