学校法人京都産業大学学内ネットワーク運用管理に関する対策基準

制　　定　平成22年10月１日

（趣旨）

第１条　この対策基準は，学校法人京都産業大学ネットワークセキュリティ規程第４条に基づき，学校法人京都産業大学の設置する学校（以下「学校」という。）において，ネットワークを安全に運用管理するための基本的な事項を定める。

（定義）

第２条　マルウェアとは，不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称である。

２　マルウェアの例としては，ウィルス，バックドア，キーロガー，トロイの木馬，スパイウェアなどがある。

３　ウィルスの例としては，WordやExcelのマクロウィルス，ブートセクタウィルス，スクリプトウィルスなどがある。

（対象）

第３条　この対策基準の対象者は以下のとおりとする。

(1)　サーバ管理者
(2)　サービス提供者
(3)　ネットワーク管理者

（脅威）

第４条　この対策基準で想定する脅威は以下のとおりである。

(1)　情報の漏洩
(2)　情報の改ざん
(3)　情報の破壊
(4)　意図しないソフトウェア等の停止
(5)　意図しないソフトウェア等の開始
(6)　他のコンピュータ等への不正アクセス
(7)　他のコンピュータ等からの不正アクセス
(8)　マルウェアの感染，又は送信

（対策基準）

第５条　学内ネットワークの運営にあたり，ネットワーク管理者の対策基準は以下のとおりとする。

(1)　通信が漏洩しないよう運用しなければならない。
(2)　ブロードキャスト（同報通信）等の全ノードに対する通信は最小限の範囲に行われるよう設定しなければならない。
(3)　不正にネットワークに接続できないよう運用しなければならない。
(4)　不要な通信を行わないよう，ネットワークとファイアウォールの適切な設定を図らなければならない。
(5)　ネットワーク管理者の不在時も含め，ネットワークが被害を受けた場合の対応を予め定めておかなければならない。
(6)　運用に関する方針及び操作手順を文書で定めることが望ましい。

(7)　脅威が発生した場合，迅速に対応しなければならない。
(8)　ネットワーク機器は，正しい時刻で運用しなければならない。
(9)　ネットワーク機器の遠隔管理を行う場合，通信の暗号化を実施しなければならない。
(10)　ネットワークやサーバへの侵入を検知するシステムや侵入を防御するシステム，並びにファイル更新監視ソフトなどを導入し，攻撃や不正アクセスを受けていないかを監視することが望ましい。
(11)　遠隔管理を行う場合，暗号化した通信で操作を行わなければならない。

第６条　学内ネットワーク運用における脅威が発生した場合の対策基準は以下のとおりとする。
(1)　ネットワーク管理者は，早急に対策を行わなければならない。
(2)　ネットワーク管理者は，脅威の発生を確認した場合，コンピュータ管理者及びネットワークセキュリティ所属管理責任者に報告しなければならない。
(3)　ネットワーク管理者は，コンピュータへのマルウェア等の感染の可能性が考えられる場合は，コンピュータ管理者と協議し，直ちに当該コンピュータをネットワークから切り離すなど，脅威の原因が排除されるまで，学内ネットワークの利用をさせてはならない。
(4)　コンピュータが目的外の動作をし，ネットワークセキュリティの損失が避けられないと判断される場合，ネットワーク管理者はネットワークセキュリティ所属管理責任者の許可の下にネットワークの切断など，暫定措置を講じることができる。

（制限）

第７条　ネットワーク管理者はネットワークセキュリティ学校管理責任者と協議のうえ，学内ネットワークの利用について，以下の制限を行うことができる。
(1)　DHCP等ネットワークの制御に影響ある機能を制限することができる。
(2)　IPアドレスの運用ルールを定め，安易な運用を制限することができる。
(3)　無線LANアクセスポイントの運用ルールを定め，ルール通りに設置することができる。
(4)　P2Pソフトウェアの利用を制限できる。ただし，教育研究上必要な場合であって，ネットワークセキュリティ学校管理責任者に申し出て許可を得た利用については，運用させる。
(5)　その他，ネットワークセキュリティ学校管理責任者が定めた制限を行うことができる。

（改廃）

第８条　この基準の改廃は，学校法人京都産業大学ネットワークセキュリティ委員会で決定する。

附　則

この基準は，平成22年10月１日から施行する。