学校法人京都産業大学学内ネットワーク接続利用に関する対策基準

制　　定　平成18年４月１日

最近改正　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，ネットワークにコンピュータ等を接続し安全に利用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)　学内ネットワークに接続するコンピュータ（持込の物を含む。）等の管理者（以下「コンピュータ管理者」という。）

(2)　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　学内ネットワークを接続利用するコンピュータの管理者は自らが管理者となるコンピュータに関して全責任を持ち，その対策基準は「インターネット及び学内ネットワーク利用に関する対策基準」に定めるものの他，以下の対策基準を行うものとする。

(1)　学内ネットワークを利用するコンピュータ等が，サービス機能を有する場合，サーバシステム運用における対策規準を遵守しなければならない。

(2)　意図しないサービスが開始していないことを定期的に確認しなければならない。

(3)　セキュリティホールに対する情報を定期的に入手し，セキュリティパッチを適切に適用しなければならない。

(4)　マルウェア等の対策ソフトウェアを運用しなければならない。

(5)　定期的にウィルススキャンを実行することが望ましい。
(6)　コンピュータは，正確な時間で運用することが好ましい。
(7)　コンピュータの運用には，安全性の高い文字数で，英大文字小文字，数字と記号のすべてを用いたパスワードを設定しなければならない。
(8)　定期的にパスワードを変更することが望ましい。

第６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あらかじ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)　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。

第７条　学内ネットワーク利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)　コンピュータ管理者は，早急に対策を行わなければならない。
(2)　コンピュータ管理者は，ネットワーク管理者又は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)　コンピュータ管理者は，マルウェア等の感染の可能性が考えられる場合は，直ちに当該コンピュータをネットワークから切り離し，脅威の原因が排除されるまで，学内ネットワークを利用してはならない。
(4)　マルウェア等の排除のためには，コンピュータ管理者は，必要な情報を当該コンピュータからバックアップのうえ，コンピュータの全情報をフォーマットし，基本ソフトの再インストールを行わなくてはならない。
(5)　サービス提供者又はサーバ管理者は，脅威からの回復のために暫定的にサービスの停止を行うことができる。
(6)　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８条　コンピュータ管理者は，学内ネットワークの接続利用について，以下のことを行

ってはならない。

(1)　ネットワーク管理者の許可無しに，DHCP等ネットワークの制御に影響ある機能を開始してはならない。

(2)　ネットワーク管理者から許可されていないIPアドレスを使用してはならない。

(3)　ネットワーク管理者との事前協議無しに，独自に無線LANアクセスポイントを運用してはならない。

(4)　P2Pソフトウェアを利用してはならない。ただし，教育研究上必要な場合は，ネットワークセキュリティ学校管理責任者に申し出て，許可を得て利用するものとする。

(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なってはならない。

（改廃）

第９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

この対策基準は，平成18年4月１日から施行する。

附　則

この基準は，平成22年10月１日から施行する。