学校法人京都産業大学サーバ運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，学校内外の不特定多数を利用者とするサーバシステム（以下「サーバ」という。）を安全に運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　この対策基準を適用する対象者は，以下のとおりとする。

(1)　サービス提供者

(2)　サーバ管理者

(3)　ネットワーク管理者

（脅威）

第４条　サーバ運用で想定する脅威は，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)　意図しないサービスの停止

(5)　意図しないサービスの開始

(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　サービス提供者の対策基準は，以下のとおりとする。

(1)　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を遵守しなければならない。

(2)　サービス提供者は，適切な利用基準を定め，サービス利用者に周知しなければならない。

(3)　提供している公開情報を監視し，意図したとおりの情報のみが公開されていることを把握しなければならない。

(4)　サービス提供者は，サービスの脆弱性を克服し，安全で適切な運用を行なわなけれ

ばならない。
(5)　新たなサービスを開始する場合は，サーバ管理者に届けなければならない。
2　サービス提供者及びサーバ管理者の対策基準は，以下のとおりとする。
(1)　運用しているサービスの動作について把握しなければならない。
(2)　サービス提供者及びサーバ管理者は，両者の不在時も含め，システム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。
(3)　公開制限情報を保存するサーバ及びネットワークシステムを設置する場所は，許可された者だけに出入を制限しなければならない。
(4)　サーバ及びネットワークシステムを円滑かつ安全に運用するため，システム障害，事故及び災害等による被害を最小限にするための対策を施さなければならない。
(5)　サービス及びサーバに対して不正アクセスがなされないよう，また不必要な通信を行わないよう，ネットワーク及びファイアウォール等の適切な対策を施さなければならない。
(6)　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。
(7)　サービス及びサーバの運用管理には，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)　運用に関わるパスワードは定期的に変更しなければならない。
(9)　運用に関する方針及び操作手順を文書で定めなければならない。
(10)　脅威が発生した場合に備えて，対策マニュアルを整備しなければならない。
(11)　保存しているデータの定期的なバックアップを行なわなければならない。
3　サーバ管理者の対策基準は，前項に加えて以下のとおりとする。
(1)　サーバは，正しい時刻で運用しなければならない。
(2)　サーバが意図しない通信を行っていないか，定期的に検査することが望ましい。
(3)　運用している全てのサーバを把握し，不必要なサーバは停止させなければならない。
(4)　新たにサーバを設置し運用開始する場合は，所属管理責任者に届けなければならない。
（サーバ設計）
第６条　サーバ運用にあたり，サーバ管理者は，以下について設計し実施しなければならない。
(1)　使用しないネットワークポートの遮断
(2)　使用しないサービスの停止
(3)　定期的なセキュリティパッチの適用
(4)　バックアップの計画的実施及びバックアップ媒体の保管
(5)　脅威の発見のためのログ保存と監視
(6)　脅威発見時の対応マニュアル整備
(7)　遠隔管理を行う場合，通信の暗号化を行わなければならない。
(8)　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。

(9)　その他，サーバ運用に関する必要な事項

２　サーバ管理者は，前項の設計を文書で保存し，ネットワークセキュリティ学校管理責任者の求めに応じ提出しなければならない。また，設計に変更があれば速やかに当該文書を更新しなければならない。

（脅威発生時対策基準）

第７条　サーバ及びサービス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)　サービス提供者及びサーバ管理者並びにネットワーク管理者は直ちに情報を共有し，早急に対策を行わなければならない。

(2)　サービス提供者及びサーバ管理者又はネットワーク管理者のうち，いずれが欠けた場合であっても，残るものが必要な対策にあたらなければならない。

(3)　サービス提供者又はサーバ管理者又は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に報告しなければならない。

(4)　マルウェアが発見された場合は，利用者に対処の方法を含めて通知しなければならない。

(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)　サーバ又はサービス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，サーバ管理者又は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又はネットワークセキュリティ学校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。

(7)　サービス提供者及びサーバ管理者並びにネットワーク管理者は，脅威を排除した後，できるだけ早期のサービス回復につとめなければならない。

（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。