非武装セグメント運用に関する基準とガイドライン

2002年3月27日 情報システム会議 制定

1. 非武装セグメントの目的

学校法人関西学院の情報資産を外部の脅威・リスクから保護するために本学院はファイアウォールを設置する。一方で、本学院内には情報公開・研究・サービス提供等のために学院外を含む一般ユーザー（管理者ユーザー以外を指す）からのアクセスを必要とする機器が存在する。これらの機器を設置・接続するネットワークとして非武装セグメント(以下、DMZ)を設置する。

2. DMZの設置

本学院内に以下のDMZを設置する。それぞれのDMZについての設置目的およびネットワーク上の位置は、「ファイアウォール運用に関する基準とガイドライン」で定める。

1）公開用DMZ
- ・西宮上ケ原キャンパス公開用DMZ
- ・神戸三田キャンパス公開用DMZ
- ・システム毎の公開用DMZ（システム毎にセグメントを分割する）

2）研究用DMZ
- ・工学部研究用DMZ
- ・総合政策学部研究用DMZ

3）内部用DMZ
- ・システム毎の内部用DMZ（システム毎にセグメントを分割する）

3. DMZの管理

公開用DMZは、情報化推進機構の管轄とする。
研究用DMZは各部署の管轄とし、それぞれDMZ管理者を設置する。
DMZ管理者は、情報セキュリティ総括部署との連絡を密にし、不正侵入、不正アクセス等の不正利用に対処しなければならない。不正利用を発見した場合は、情報セキュリティ総括部署に直ちに連絡しなければならない。
研究用DMZ管理者は、DMZに設置される機器のアクセスログ等の採取を機器管理者に義務付け、情報セキュリティ総括部署からの要請に応じて、これを提出しなければならない。

4. DMZ への機器の設置

公開用DMZおよび内部用DMZへの機器の設置については、情報化推進機構長室会及びその他関連する会議の了承を必要とする。
研究用DMZへの機器の設置については、各DMZ管理者の管理下で接続を行う。
機器の設置に際しては、機器管理者を定めなければならない。
機器の管理については、設置部署・設置者が責任をもって行う。
機器の接続に際しては、既知のセキュリティホールについて、すべて対応済みの機器を設置しなければならない。また各ベンダーの提供するセキュリティ情報には留意し、パッチ等が提供された場合速やかに適用するようにしなければならない。
機器のセキュリティ対策については、機器の管理者がそれぞれ行わなければならない。
DMZに接続した機器を別のネットワークインターフェイスを用いて他の学院内ネットワークセグメントに接続してはならない。

5. DMZの通信制限

各DMZの通信制限は、「ファイアウォール運用に関する基準とガイドライン」で定める。

6. 緊急時の対応

情報セキュリティ総括部署、及びネットワーク管理者は、DMZ接続機器にセキュリティ上の極めて重大な問題が発見された場合、緊急避難的な措置として、各DMZ全体または機器をネットワークから切断することができる。

（備考）

1) 本ガイドラインは2002年4月1日から適用する。
2) 本ガイドラインは2003年4月1日から変更・適用する。
3) 本ガイドラインは2020年4月1日から変更・適用する。
4) 本ガイドラインは2021年4月1日から変更・適用する。
5) 本ガイドラインは2023年6月13日から変更・適用する。

以 上