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

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関西学院ではファイアウォールを設置する。一方で、学内には情報公開・研究のために外部からのアクセスを必要とするサーバが存在する。これらのサーバを設置・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

学内に以下の DMZ を設置する。

1)公開サーバ用 DMZ

・上ヶ原キャンパス公開サーバ用 DMZ

・神戸三田キャンパス公開サーバ用 DMZ

2)研究用 DMZ

・理工学部研究用 DMZ

・総合政策学部研究用 DMZ

3. DMZ の管理

公開サーバ用 DMZ は、情報システム室の管轄とする。

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、情報セキュリティ担当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、情報セキュリティ担当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、情報セキュリティ統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. 公開サーバ用 DMZ へのサーバの設置

公開サーバ用DMZ へのサーバの設置については、情報システム会議及びその他関連する会議の了承を必要とする。

サーバの設置に際してはサーバの管理者を定めなければならない。

サーバの管理については、設置部署が責任をもって行う。

サーバの接続に際しては、既知のセキュリティホールについては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。

サーバのセキュリティ対策については、サーバの管理者がそれぞれ行わなければならない。

公開サーバ用 DMZ に接続したサーバを別のネットワークインターフェースを用いて学内ネットワークに接続してはならない。

5. 研究用 DMZ へのサーバ等の設置

研究用 DMZ へのサーバ等の設置については、各 DMZ 管理者の管理下で接続を行う。

サーバ等の設置に際しては機器の管理者を定めなければならない。

サーバ等の管理については、機器の設置者が責任をもって行う。

サーバ等の接続に際しては、既知のセキュリティホールについては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。

サーバ等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。

研究用 DMZ に接続したサーバを別のネットワークインターフェースを用いて学内ネットワークに接続してはならない。

6. DMZ のアクセスコントロール

公開サーバ用 DMZ への通信についての制限は、「ファイアウォール運用に関する基準とガイドライン」を参照すること。

研究用 DMZ については、原則としてアクセス制限を設けない。

7. 緊急時の対応

情報セキュリティ担当部署、及びネットワーク管理者は DMZ 接続サーバ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、各研究用 DMZ 全体、または、サーバをネットワークから切断することができる。

（追加事項）

このガイドラインは、現在、公開サーバ用 DMZ に設置されている広報室管理の WWW サーバ等についても適用する。

（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。

以　上