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

本学院内に以下の 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. 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。
サーバの設置に際してはサーバ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院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院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

情報セキュリティ総括部署、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。
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。

以 上