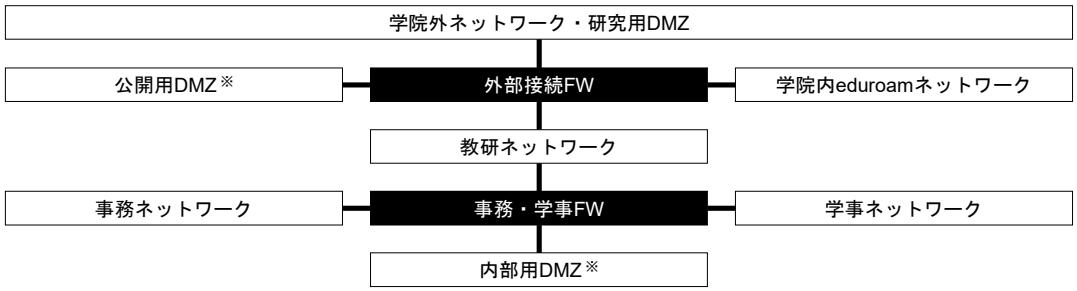
ファイアウォール運用に関する基準とガイドライン

2002年3月27日　情報システム会議　制定

1. 目的

学校法人関西学院は、学院内ネットワークの信頼性・安全性・可用性を維持するために、学院外との接続に際して、ファイアウォール（以下、FWという。）を設置する。本ガイドラインではFWの運用にあたっての方針、及び通過を許可するプロトコル等を定める。

2. ファイアウォールの構成



※：システム単位でセグメントを分割し、同DMZ内であっても異なるシステム間の通信はFWで制御される。

【図1】学院ネットワーク構成

【図1】学院ネットワーク構成 に示すとおり、FWを各ネットワークの境界に設置し、明示的に許可する通信以外を全て拒否する。
公開用サーバーを設置するためのネットワークセグメント（以下、公開用DMZという。）を設置する。
学院内でeduroamを提供するためのネットワークセグメント（以下、学院内eduroamネットワークという。）を設置する。
学院内での教育研究を目的としたネットワーク利用のためのセグメント（以下、教研ネットワークという。）を設置する。
学院内で機密性の高い通信を扱うネットワークセグメントとして、職員クライアント用のセグメント（以下、事務ネットワークという。）、主に初等部、中学部、高等部に在籍する教員クライアント用のセグメント（以下、学事ネットワークという。）、およびサーバー等を設置するためのセグメント（以下、内部用DMZという。）を設置する。
公開用DMZと内部用DMZについては、システム毎にセグメントを分割し、公開用DMZ内または内部用DMZ内の異なるシステム間の通信についても、FWにより明示的に許可する通信以外を全て拒否する。
研究用DMZについては、外部接続FWの外側に設置し、原則としてアクセス制限を設けない。

3. FWで許可するプロトコル

1) 基本方針

パスワードが平文（クリアテキスト）で流れるプロトコルの通過は原則として許可しない。
学院外からの攻撃、外部への攻撃に利用できるプロトコルの通過は原則として許可しない。
許可されていないプロトコルの通過または許可されているプロトコルの拒否が必要な機器については、機器毎に審議を行い許可または拒否するプロトコルを決定する。
許可する通信と同セッション内の後続通信については、全て許可する。
dns, icmpなどのネットワーク運営上必要なプロトコルについては、原則として許可する。

2) 詳細

各FWで許可するプロトコルは別に定める。

4. 緊急時の対応

情報セキュリティ総括部署は、セキュリティ上の重大な問題が生じた場合には、上記の通過を許可するプロトコルについても、緊急避難的に通過を不許可とすることができる。その際には、事後的にその顛末について情報化推進機構長室会に報告しなければならない。

（備考）

1）本基準は2002年4月1日から適用する。
2）本基準は2003年4月1日から変更・適用する。
3）本基準は2007年4月2日から変更・適用する。
4）本基準は2010年10月18日から変更・適用する。
5）本基準は2015年5月1日から変更・適用する。
6）本基準は2018年4月1日から変更・適用する。
7）本基準は2018年5月1日から変更・適用する。
8）本基準は2020年4月1日から変更・適用する。
9）本基準は2020年9月8日から変更・適用する。
10）本基準は2021年4月1日から変更・適用する。
11）本基準は2023年6月13日から変更・適用する。

以　上