技術発表(6)

ファイアーウォールシステムについて

IT基盤センター 作山 幸恵

ファイアーウォールシステムについて

作山　幸恵　（ＩＴ基盤センター）

１．はじめに

ファイアーウォールシステムとは、外部ネットワークと内部ネットワークの間におき、外部からの不正なアクセスや侵入を防止することを目的としたセキュリティシステムの総称を呼ぶ。

そこで、茨城大学のファイアーウォールシステムについての概要を以下に記す。

２．茨城大学のファイアーウォールについて

茨城大学のファイアーウォールシステム（以下 FW）の種類は UTM（統合脅威管理製品）の形にあたり、Fortinet 社製の Fortigate 1000A 3 台、Fortigate 300A　1 台、計 4 台のシステムで構成されている。

各 FW は、４台全て茨城大学ネットワークの入り口となる、日立キャンパスに設置されている。

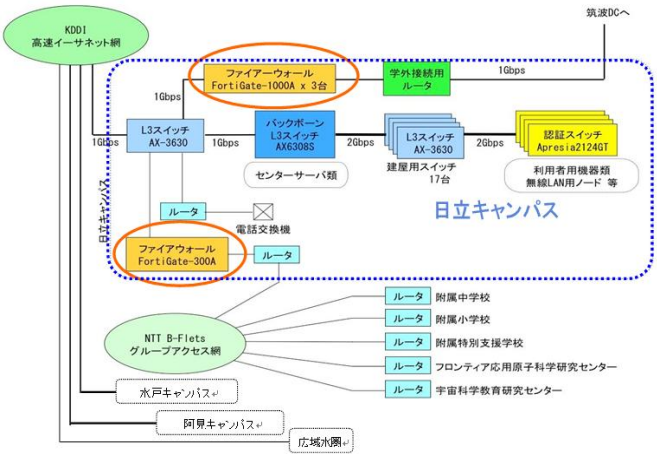


図１：茨城大学ネットワーク

３．ファイアーウォールシステム各役割

大きく役割を分けると、外部 FW（1000A）、内部 FW（1000A×2）、付属学校 FW（300A）の３つに分けられる。

外部ＦＷは、主に学外インターネットと学内間での通信について、通信の許可、不許可を制御するファイアーウォール機能と、学内ネットワークへの不正な侵入を検知、防御する IDS/IPS 機能を持つ。

内部ＦＷは、主にウィルスの検出、削除、ブロックを行うウィルススキャン、学内外間で送信されているメールに対して、スパムメールのチェックを行うアンチスパムと、学校生活に必要と思われないサイトに関して、閲覧不可にする、Web フィルタリング機能を持つ。

附属学校 FW は小中養護学校へ、さらに厳しく制限するため設けられ、内部 FW で WEB フィルタリングをしているところに、更に二重に厳しく WEB フィルタリングを施し、アクセスの制限をしている。

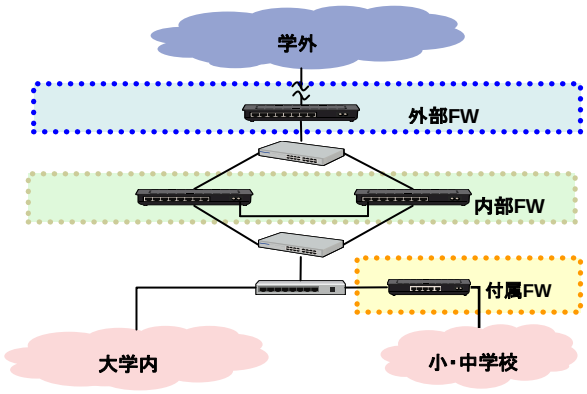


図２：FW 接続図

４．外部との通信について

茨城大学は外部 FW における、ファイアーウォール機能により、学内のセキュリティ確保のため、標準的な一部の通信ポートを除くほとんどの通信ポートは通信が不可となっている。そこで、情報機器利用登録システムによる申請サービスを用いている。

情報機器利用登録システムとは本学における情報機器(ソフトウェアも含む)の資産管理徹底、ならびに情報機器・ネットワークの運用管理効率化を目的として、IT 基盤センターによって運用されている教職員用データベースである。使用できるのは茨城大学の教職員のみである。その中の申請に、各種学外向けサーバ(Web、SSH、Mail、FTP)の運用申請と、標準外通信ポートの利用申請がある。

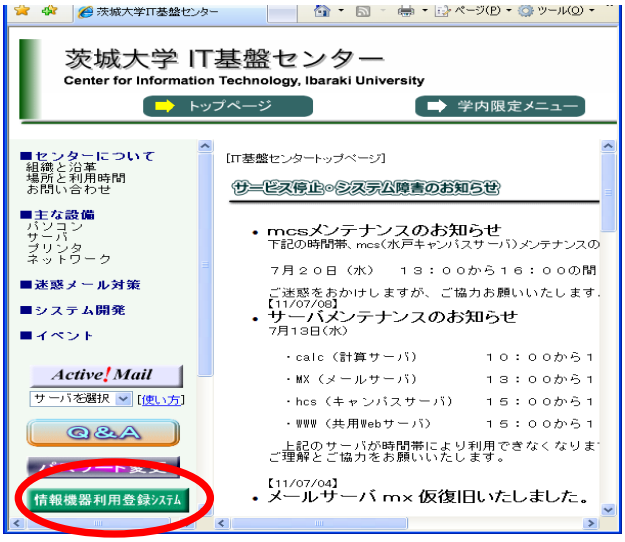


図３：IT 基盤センターTOP ページ

図４：情報機器利用登録システム

５．内部 FW２台導入理由

内部ＦＷを２台設ける理由としては、１つは負荷軽減。Web フィルタ、アンチスパム、ウィルススキャンの各機能を２台の装置で分散処理を行う事と、また、片方の装置が故障等で障害が発生した場合、もう片方の１台で通信を維持するための障害時対策が目的である。

また、内部 FW の機能の一つ、URL フィルタリングについて、犯罪性の高いサイト 反対意見が多く、論争の元となる可能性のあるサイト、違法性、 セキュリティ上問題のあるサイト等の内容を含む Web サイトの閲覧をブロックしている。

教育・研究上、フィルタリングのかかっているサイトにアクセスする必要がある場合は、申請書を提出して頂き、妥当性が認められればアクセス可能となる

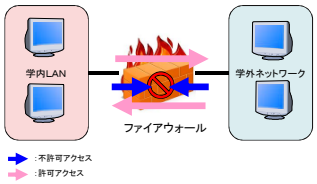
図５：URL フィルタリング

ファイアーウォールシステムについて

IT基盤センター
作山　幸恵

ファイアーウォールとは

- 外部ネットワークと内部ネットワークの間におき、外部からの不正なアクセスや侵入を防止することを目的としたセキュリティシステムの総称。



ファイアーウォールの歴史

- 1990年代　:ソフトウェア型
  :PCにソフトウェアをインストールした形のファイアーウォール
- 1990年代末:ハードウェア型
  :専用のハードウェアを用いた形のファイアーウォール
- 2000年代　:UTM(統合脅威管理製品)
  :様々なセキュリティ機能(アンチウィルス、URLフィルタ等)を搭載した統合型のファイアーウォール

⇒ 茨城大学のファイアーウォールシステムはUTMにあたる。

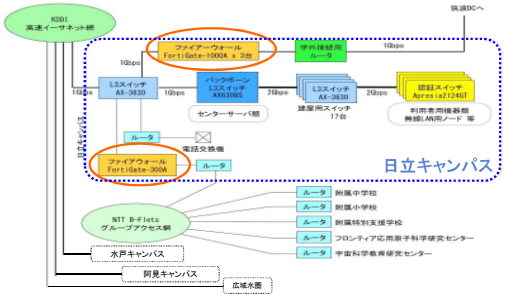
茨城大学では

- Fortinet社製の
  Fortigate 1000A 3台, Fortigate 300A　1台,
  計4台のファイアーウォールシステムで構成されている。

茨城大学
ファイアーウォールシステム
上の1台:　300A
下の3台:　1000A

茨城大学
ファイアーウォール設置場所

- 各ファイアーウォールは、 4台全て茨城大学ネットワークの入り口となる、日立キャンパスに設置されている。

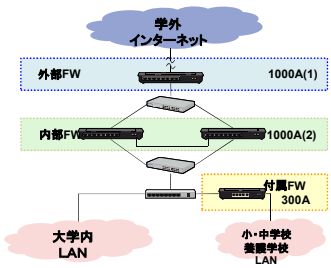


茨城大学
ファイアーウォールシステム

大きく役割を分けると

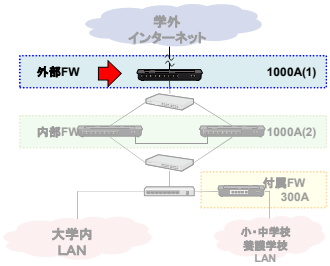
- 外部ファイアウォール
  1000A(1)
- 内部ファイアウォール
  1000A(2)
- 付属学校ファイアウォール
  300A

の3つに分けられる。



外部ファイアーウォールの役割

- ファイアーウォール機能
  - 学外インターネットと学内間での通信について、通信の　許可／不許可を制御する。
- IDS/IPS機能
  - 学内ネットワークへの不正な侵入を検知、防御する。

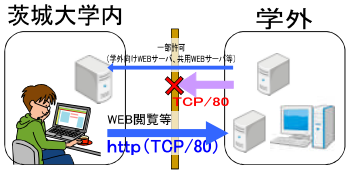


＜外部ファイアーウォールの役割＞

ファイアーウォール機能

- 送信元IPアドレス、宛先IPアドレス間で、サービス （IP、TCP、UDP） の通信の許可・不許可により設定する。
- 学内のセキュリティ確保のため、標準的な一部の通信ポートを除くほとんどの通信ポートは通信が不可となっている。

～ 一例：TCP/80 ～



TCP/80(http)に関して

＜学内→学外＞
Web閲覧等で使用されるため、殆ど開放している。

＜学外→学内＞
不正アクセス等防止のため、殆ど遮断している。運営上必要な機器、また申請を頂いている機器に関してはIP指定で開放している。

情報機器利用登録システムによる学外向けサービス

- **各種学外向けサーバ(Web、SSH、Mail、FTP)の運用申請**
  - セキュリティ対策として、学内-学外間で利用できる通信ポートは標準的なもののみに制限されている。
  - 学外に対して、Web、SSH、Mail、FTPの各サービスを提供するサーバを運用する場合には、それぞれ申請が必要。
- **標準外通信ポートの利用申請**
  - Web、SSH、Mail、FTP以外で、標準外の通信ポートを利用する必要がある場合には申請が必要。
    （例：外部とのTV会議接続等）

それぞれの登録は情報機器利用登録システムで行う。

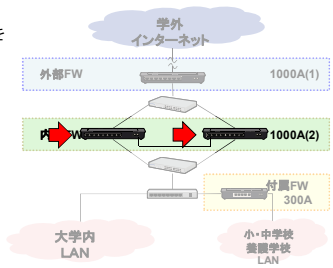
＜外部ファイアーウォールの役割＞

IDS/IPS

- ファイアーウォールで防げない攻撃をIDS/IPSにより防ぐ。
  - IDS：不正侵入検知システム（ Intrusion Detection System ）
    学内ネットワークへの不正な侵入を検知し、管理者へメール等で周知するシステム。
  - IPS：侵入防御システム　（Intrusion Prevention System）
    学内ネットワークへの不正な侵入を検知すると，それを防御するシステム。
- ファイアーウォールではIP,ポート番号などによるルールで、許可、不許可を行うため、もしパケットのデータに不正があったとしてもファイアーウォールはその通信を許可してしまう。そこで、IDS/IPSを用いる不正なパケットを検出し防御することができる。

内部ファイアーウォールの役割

- ウィルススキャン
  - ウィルスの検出、削除、ブロックを行う。
- アンチスパム
  - 学内外間で送信されているメールに対して、スパムメールのチェックを行う。
- Webフィルタリング
  - 学校生活に必要と思われないサイトに関して、閲覧不可にする。



内部ファイアーウォール2台導入理由

- 負荷軽減
  Webフィルタ、アンチスパム、ウィルススキャンの各機能を2台の装置で分散処理を行う。
- 障害時対策（冗長化）
  もし、片方の装置が故障等で障害が発生した場合もう片方の1台で通信を維持する。

＜内部ファイアーウォールの役割＞

ウィルススキャン

- 内部ファイアウォールを通過するメール（SMTP）、WEB（HTTP）、ファイル転送（FTP）に対してウィルススキャンをする。
- ウィルスを検出した場合には、ウィルスの削除または当該ファイルへのアクセスをブロックする。

＜内部ファイアーウォールの役割＞

アンチスパム

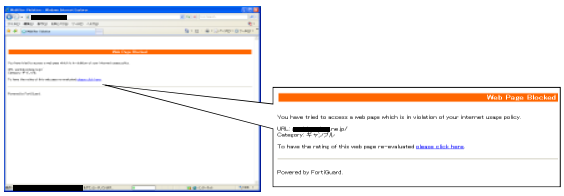
- 学外、学内間のメール送信に対し、スパムメールか否かチェックする。
- スパムメールと判断したメールに対して受信制限を実施する。

＜内部ファイアーウォールの役割＞

WEB　フィルタリング

- Web閲覧時のアクセス制限（URLフィルタリング）が導入されている。以下のような内容を含むWebサイトの閲覧をブロックしている。
  - 違法性、犯罪性の高いサイト
  - 反対意見が多く、論争の元となる可能性のあるサイト
  - セキュリティ上問題のあるサイト

教育・研究上、フィルタリングのかかっているサイトにアクセスする必要がある場合は、申請書を提出して頂き、妥当性が認められればアクセス可能となる。

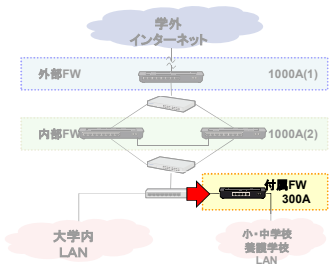


300Aの役割

- 小中養護学校へ、さらに厳しく制限する。

内部ファイアーウォールでWEBフィルタリングをしているところに、更に二重に厳しくWEBフィルタリングを施しアクセスの制限をしている。

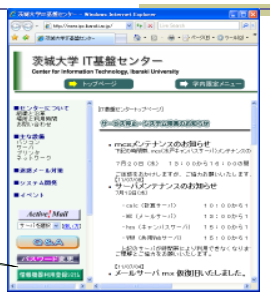
ウィルススキャンも、大学、小中学校間で施している。



情報機器利用登録システム

- IT基盤センターHP（www.ipc.ibaraki.ac.jp）上に有る。
- 茨城大学教職員が利用可能

情報機器利用登録システム

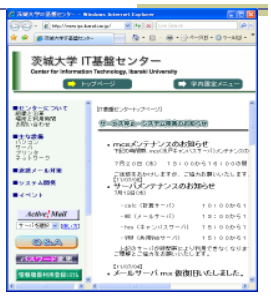


情報機器利用登録システム　登録の流れ

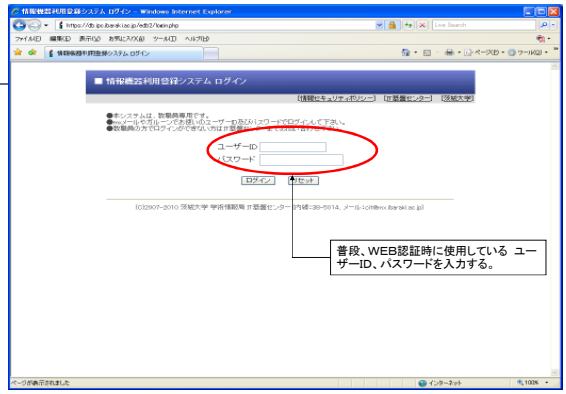
① 情報機器利用登録システムに機器を登録する。

② 固定IPを申請し、取得する。

③ 各サービス（学外向けWEBサーバ、学外向けSSHサーバ等）の申請をする。



IT基盤センター　トップページ



認証後、最初のページ