Fire Wall 透過設定申請書

情報セキュリティ管理責任者　殿

下記ホストに対する計算機センターファイアウォールでの、外部よりの下記プロトコルアクセスからの保護の解除（ファイアウォール透過）を申請します。

同ホストに対する不正アクセスが発生した場合は、私の責任において対処することを確約いたします。

申請日		2020 年　12 月　23 日			
1	システム責任者（申請者）氏名	奥原 浩之	所属・職名	電子・情報工学科	
	メールアドレス	okuhara@pu-toyama.ac.jp		内線番号	1920
2	区分	☑ 新規　☐ 継続　☐ 変更 ☐ 廃止　※変更の場合、変更箇所を備考にご記入ください			
3	プロトコル名：https　（ポート：443）				
4	ホスト名：dic515s2.　pu-toyama.ac.jp（IP アドレス：133.55.115.240）				
5	設置場所	情報工学研究室10			
	部屋番号	N-515	情報コンセント	N-515_1	
6	FireWall 透過設定期間	2020 年　12 月　23 日 ～　2021 年　3 月　31 日			※年度を越えての申請は不可
7	FireWall 透過が必要な理由（具体的に）				
	研究室の成果公開やwebサービスの学外への公開ならびに、研究で必要なIoTデータを学外から収集し蓄積するため。				
8	ホスト機種/OS（バージョン）	CentOS 7.9.2009			
	ソフトウェア名（バージョン）	Apache 2.4.46			
9	通信相手を制限する場合の付加設定情報（相手ホスト名、ドメイン名、IP 等）				
【 備考 】　※申請内容の変更があった場合もこちらに変更内容をご記入ください。					

※ 申請者は本学教職員に限ります。別紙のチェックシートは必ず添付して下さい。
（チェックシートは申請書毎に１枚提出して下さい）

※ 記載内容が不適切、不十分な場合は、申請を受け付けない場合があります。プロトコルによって透過理由が変わる場合は、同一ホストであってもプロトコル毎に申請して下さい。

※ 計算機センターからの問い合わせに対して反応がない場合は、ポートを閉塞する場合があります。

チェックシート　－ Fire Wall 透過設定申請 別紙 －

申請日　2020 年 12 月 23 日

システム責任者
（申請者）氏名：奥原 浩之

■チェック項目　　（　）内は「富山県立大学　情報セキュリティ対策基準」該当箇所

１．取り扱い情報資産（４章）
- ☐ 機密性分類Ⅰ　☐ 機密性分類Ⅱ　☑ 機密性分類Ⅲ
- ☐ 完全性分類Ⅰ　☑ 完全性分類Ⅱ
- ☐ 可用性分類Ⅰ　☑ 可用性分類Ⅱ

２．利用者（２章（５））
- ☑ 不特定（利用者 ID・パスワードを使用しない）
- ☐ 学内者全員　☐ 特定の学内者　☐ 特定の学外者

３．アクセス権管理（８章）
- ☑ システム管理者 ID・パスワードは、特定の者のみに限定している
- ☑ システム管理者 ID・パスワードは、ネットワーク経由で使用できない
- ☑ システム管理者 ID・パスワードは、十分なセキュリティ強度を有する
- ☑ 利用者 ID・パスワードは、特定の者のみに限定している
- ☑ 利用者 ID・パスワードは、十分なセキュリティ強度を有する
- ☐ 学外との通信は、特定の学外ホストやサイトとのみに限定している
- ☐ 学内ネットワークや学内他システムへのアクセスに制限を施している
- ☐ 学内ネットワークや学内他システムからのアクセスに制限を施している

４．ウイルス対策（７章（２））
- ☑ ウイルス対策を導入し、動作させている
- ☑ ウイルス侵入の検出、侵入時の対応手段を確保している

※以下（５～７）は全てのボックスにチェックが必要です。

５．設置場所の管理（６章）
- ☑ 設置場所は施錠ができ、鍵は厳格に管理している
- ☑ 設置場所への入室は、特定の者のみに限定している

６．ソフトウエアの管理（７章（１）エ）
- ☑ 導入するソフトウエアは、既知の脆弱性が無いことを確認している
- ☑ 導入するソフトウエアの脆弱性情報の入手手段を確保している
- ☑ 導入するソフトウエアの脆弱性対策を速やかに実施可能な体制である

７．緊急時対応計画（７章（３）、８章（３））
- ☑ 情報セキュリティ侵害に対する対応担当者は私である
- ☑ 侵害の検知や原因追究のためのログを取得、検証する体制を確保している
- ☑ セキュリティ侵害の疑いがある場合、計算機センターで強制ネットワーク遮断等を行うことを認める。

「FireWall 透過設定申請書」の提出上の注意

FireWall 透過設定申請書及びチェックシートは、学内情報資産管理者・学内情報資産運用担当者によるチェックを行います。下記の注意事項を熟読の上、漏れや誤りが無いよう記載ください。なお、チェックには2～4 週間かかる場合もありますので、十分余裕を持って申請下さい。

また、FireWall 透過設定申請書、チェックシート及び本注意書きは、適宜変更することがあります。最新のものを確認の上、提出ください。

[FireWall 透過設定申請書記載上の注意点]

1. **システム責任者（申請者）** **必須**
   （実対策基準　3章　組織で定義）申請するシステム及びその取扱い情報に関して責任を負うことのできる本学常勤教職員。各学内委員会委員長等。

2. **区分** **必須**

3. **プロトコル名、ポート番号** **必須**
   プロトコル名は標準的な通信方法(HTTP 等)を用いる場合に記載。ポート番号は必須で、原則、透過するホスト、ポート番号毎に1つの申請が必要。TCP,UDP も明記すること。

4. **ホスト名、IPアドレス** **必須**
   ホスト名は学外 DNS 公開の場合に記載。IP アドレスは必須

5. **設置場所** **必須**
   （実対策基準　5章 人的セキュリティ対策、6章 物理的セキュリティ対策に準拠）

6. **透過設定期間** **必須**

7. **必要理由** **必須**
   セキュリティリスクを考 慮に入れた必 要性が検 討されていること。本学重 機密性分類Ⅰの情報が取り扱われる場合は、情報セキュリティ最高責任者（学長）　の許可を、本学機密性分類Ⅱの情報が取り扱われる場合は、情報セキュリティ責任者（各主任教授・事務局長）　の許可を受 けた由を明記すること。

8. **ホスト機種/OS** **必須**、**ソフトウエア名** **必須**
   OS，ソフトウエアは、開発元によるセキュリティサポート有効期間が確認されており、その範囲内であることが証明できること

9. **付加設定情報**
   本学 FireWall 上で、通信相手ホストアドレスまたはアドレス範囲、透過する時間帯を限定する場合に記載

[チェックシート記載上の注意点]

FireWall 透過設定申請書の記入事項と矛盾がないよう記載ください。また、申請書毎にチェックシートを添付ください。

以上