所内における研究室ネットワーク体系の一元化

石井, 大輔
九州大学応用力学研究所

出版情報：九州大学応用力学研究所技術職員技術レポート. 18, pp.45-50, 2017-10. Research Institute for Applied Mechanics, Kyushu University
バージョン：
権利関係：

所内における研究室ネットワーク体系の一元化

石井　大輔

要旨

応用力学研究所におけるネットワークは 3 区分で構成されるが、中でも教職員や学生が居室等で利用できるネットワーク環境「研究室ネットワーク」内では、従来から各研究室によって様々なネットワークの物理構成や論理構成が取られ、研究室管理のもとで運用されてきた。このような個々の研究室ネットワーク体系を束ね管理するために、研究所ネットワーク全体を網羅するファイアウォールを導入し、同機と計算機室利用申請登録システムを用いた管理体制と運用ポリシーに基づいて、所内ネットワークにおけるセキュリティの確保や安全な通信環境の強化などに努めてきた。

今回その延長として、所内ネットワークセキュリティの更なる強化と運用改善を図るために、研究室ネットワーク体系を一元化することになった。本稿では、本案に係る経緯や問題点などに触れ、実際にネットワーク構成の切り替えが必要となった研究室ネットワーク体系の変更事例について紹介する。

キーワード

所内 LAN・ファイアウォール（FW）・研究室ネットワーク体系

１．はじめに

応用力学研究所（応力研，RIAM）では、研究所ネットワークにおけるセキュリティの確保と安全な通信環境の強化を図るため、2009 年に所内のネットワーク全体をカバーする高性能ファイアウォール（FW）を最上層（所外ネットワークとの境界）に導入し、所内 LAN を構築した[1]。その後、定期的な機種更新を経て、現在は豊富な機能と高い性能を実現した UTM（統合脅威管理）アプライアンス機の中で実績がある「フォーティネット社製 Fortigate 600C」を運用管理し、所外からの不正侵入に係る検知や防御をはじめ、アンチウイルス・迷惑メール対策、アプリケーション制御など、昨今における高度なセキュリティ脅威や標的型攻撃等に対して所内 LAN の包括的な保護を実現している。

現在における所内 LAN 構成の概略を図 1 に示す。応力研 FW（RIAM-FW）配下に構成される所内 LAN は、「研究室ネットワーク」「計算機ネットワーク」「DMZ ネットワーク」といった 3 つのネットワーク区分（セグメント）に大別される。「研究室ネットワーク」とは、教職員や学生が居室や実験室等でネットワークを利用できるセグメント、「計算機ネットワーク」とは、主にスーパーコンピュータシステム[2] に関係するセグメント、「DMZ ネットワーク」とは、メールサーバや www サーバを管理するセグメントを指す。本稿では「研究室ネットワーク」に焦点を当てて話題を展開するため、残りのネットワーク系についての詳述は割愛する。

２．所内 LAN および研究室ネットワークの構成例

一般に FW とは、通信遮断や侵入防護等の役目（①）を果たすほかに、ルータ機能によるプライベートネットワーク環境の構築（②）が可能であり、以降は両機能を有することを前提に話しを進める。ちなみに、RIAM-FW も当然①と②の両機能を併せ持つ機種である。

応力研ネットワーク全体を防護するための RIAM-FW が 2009 年に導入されるまでは、「研究室ネットワーク」セグメント内における各研究室のネットワーク体系は、研究室によって独自のネットワーク環境が構築され、各研究室の管理のもとで運用されてきた。この状態は図 1 で説明すると、上流の RIAM-FW（外部からの防護壁の役目）がない物理構成と等価であり、研究室によっては外部から研究室内の PC やサーバ等に直接アクセスでき得る状態であった（A 研管理の端末が外部から丸見えの状態を指す）。これは当然、悪意のある不正接続や遠隔操作等も含まれる。そのため、外部からの不正アクセスや攻撃

等から研究室内ネットワークおよび配下の通信端末を防護することを目的に、独自で FW（研究室 FW）を導入し自衛する研究室も多かった（研究室 FW で研究室ネットワーク配下を防護している B 研・C 研のような状態を指す）。

所内 LAN を構築した RIAM-FW 導入後は、研究室ネットワークとして「10.5.0.0/16」のネットワークセグメント（IP アドレス／サブネットマスク）を割り当て、各研究室はこれに対応するネットワーク構成に変更した。その結果を図化したものが、図 1 内に示す「A 研」「B 研」「C 研」の破線内の構成であり、今回の体系見直しを実施するまで実際に各研究室で構築・運用されてきたネットワーク体系の構成例である。「A 研」は、研究室 FW を設置しないネットワーク体系（10.5.0.0/16）、「B 研」は、研究室 FW を設置するが①の機能のみを利用するネットワーク体系（10.5.0.0/16 ，厳密には本機の L2 ブリッジモードとの併用）、「C 研」は、研究室 FW を設置し、①と②の両機能を利用した C 研独自のプライベートネットワーク環境で運用するネットワーク体系（192.168.1.0/24）を採用している。B 研および C 研の物理構成は、A 研の RIAM-FW によるシングルガード（所外からのリスクを低減）に比べて費用は生じるものの、より強固で堅牢な運用体系（所外から／所内からのセキュリティリスクをより低減したセキュアな通信環境）を取ることができる。

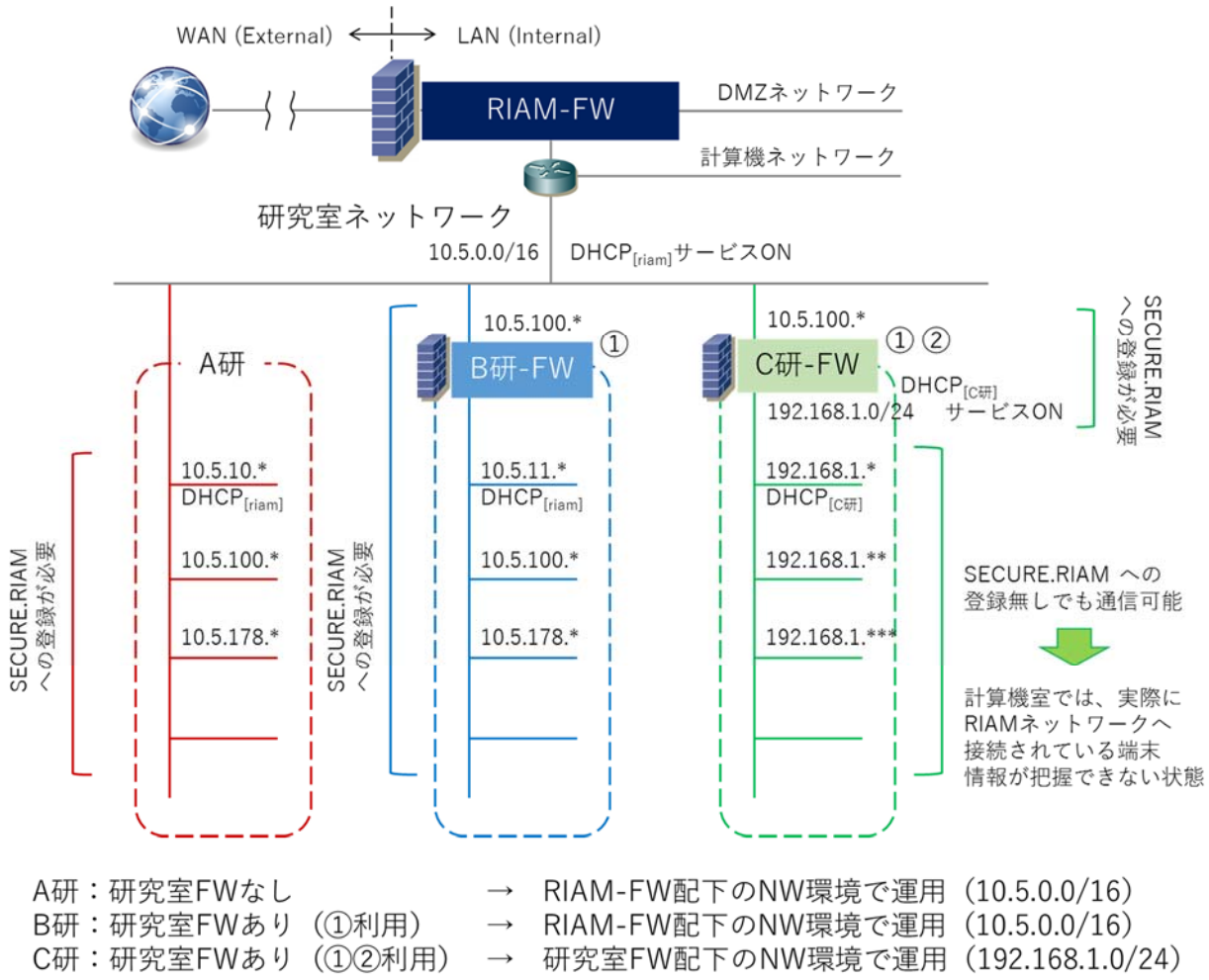

図 1　RIAM ネットワーク（所内 LAN）における研究室ネットワークの論理構成例

3．対処が必要と考えられる様々な問題点

RIAM-FW を導入した翌年からは、所内 LAN に接続して対外通信を行う通信端末は有線・無線の別を問わず、計算機室が管理・運営する利用申請登録システム（SECURE.RIAM：S.R [3]）に MAC アド

レス等の機器情報を事前登録し、利用承認を受けなければ対外通信できない、という新たなネットワークポリシーを適用した。それは、以下に挙げる主な懸念要因を解消するためであった。

● 最新のセキュリティパッチが適用されていない、ウイルス対策ソフトがインストールされていない通信端末や、一時来訪者等の部外者によって所内に持ち込まれる通信端末（安全かどうかも分からない状態の機器）が、安易に所内 LAN へ接続できないようにするため。（セキュリティリスクを抱えている可能性がゼロではない）

● セキュリティインシデントが発生した場合に、当該機器の特定と研究室ネットワーク管理者への通報・対応指示、当該機器に対する通信遮断や隔離措置が迅速かつ容易に実施できるようにするため。

その後、本運用は一定の成果を挙げてきたが、続ける中で徐々に問題として顕在化してきたのが、C 研ネットワーク体系での研究室運用であった。以下にその問題点を列記する。（RIAM ネットワーク：所内 LAN と同義）

◆ C 研ネットワークの出入口となる C 研-FW のみを計算機室 S.R に登録すれば、その配下で接続する通信端末が何台あろうとも、S.R に未登録の状態で所内 LAN に接続できてしまう。（C 研-FW が 1 対多の IP マスカレードによる②の機能で通信できてしまうため）

◆ 課金対象は C 研-FW の 1 台分のみとなり、利用端末全てを登録して課金されている他の研究室（A 研・B 研ネットワーク体系で運用している研究室）と不公平が生じている。

◆ C 研-FW 配下は､RIAM ネットワーク体系（10.5.0.0/16）と異なるネットワーク体系（192.168.1.0/24）での運用のため、C 研ネットワーク外部から内部の状況が確認できず、計算機室として RIAM ネットワークへの接続数や端末情報等が把握できない。（C 研ネットワーク内の Black Box 化）

◆ ウイルス感染端末や通信障害を引き起こす端末が、C 研-FW 配下に存在することまでは計算機室で突き止めたとしても、研究室内端末に関する情報が S.R に登録されていないため、障害端末の発見や端末への対処等が遅れる可能性がある。（C 研ネットワーク内の Black Box 化による弊害）

◆ 場合によっては、C 研-FW を通過する通信の全てを長時間遮断せざるを得なくなる。（C 研-FW 配下の全ての通信機器で、対外通信やメール送受信等が一時不可に陥るため、関係の無い利用者にも影響が出てしまう）

以上の問題を解消するため、FW のルータ機能を活用した研究室独自のネットワーク体系（C 研）での従来運用を解消させ、図 1 に示す「A 研」または「B 研」のネットワーク体系へ移行すること、また所内 LAN に接続させる全ての通信端末の情報登録（S.R へ）や、必要に応じた機器等へのネットワーク再設定等といった一連の作業を一定の猶予期間内（1 年以内）に完了すること、を対象となる研究室に求めた。

４．ネットワーク体系変更に伴う研究室側のメリット・デメリット

本課題を解消するためには、対象となる研究室側の理解と協力が不可欠である。それは、研究室によってネットワーク体系の変更に伴う作業負担や、変更作業によってサーバや利用サービスが正常に再開・復旧できるかの心配や不安、構成変更によって生じ得る費用負担の発生、等がネックになり得るからである。そこで、ネットワーク体系の変更に関する研究室側のメリット・デメリットを考え得る範囲

で先方へ事前に通知し、必要に応じて当該作業に係る技術支援を行うことで、少しでも研究室側の様々な不安や負担を和らげるよう配慮した。

メリット

（1）S.R への機器情報登録を行うことで、研究室内で管理する端末情報の一元管理ができるようになり、実態を把握しやすくなる。（見知らぬ、把握していない端末等のネットワーク接続が激減する）
（2）無線機能がある通信端末であれば、S.R に登録することによって、応力研共用 Wi-Fi サービス（riamnet）が利用可能になる。
（3）ウイルス感染等に見舞われた障害端末を特定しやすくなる上、当該機器だけの通信遮断（オフライン化）でよくなる。

デメリット

（1）使用台数分の情報調査と、S.R への登録作業が必要。
（2）固定 IP 端末が多いと課金負担が増加する可能性がある。（DHCP による IP アドレスの自動割り振りでよければ無償）
（3）固定 IP アドレスを振る必要がある端末の IP アドレス再設定の作業負担

５．具体的な変更例

今回のネットワーク体系変更を実施する必要があった研究室は 5 室程あったが、どの研究室も無事期日までに研究室ネットワーク体系の切り替えが完了した。その中で、筆者が実際に担当した以下の事例について紹介する。

今回切り替えが必要になった C 研ネットワーク体系を有する研究室の体系変更前後におけるネットワーク情報および体系概略図を、それぞれ表 1 および図 2 に示す。表 1 の情報と照合しながら図 2 を見ると分かりやすくなるが、同図中左側に示すように、従来では研究室 FW（旧 FW）配下に複数の研究室（XX 研・YY 研）が各セグメントに分割されて共同運営されていた。研究室ごとに 2 つのセグメントを運用管理していたため、旧 FW 側の LAN セグメントは 4 つ存在した。FW では、これらの 4 つの LAN と FW の外側の WAN（1 つ）の組み合わせで個々にルール（ポリシー）を設定する必要がある。WAN と LAN の独立セグメントは計 5 個あるので、設定が必要なポリシー数は 20（$_5P_2$）となり内部設定が複雑化していた。

表 1　研究室ネットワーク体系の変更前後におけるネットワーク情報

	従 来（C 研 NW 体系）	新 規（B 研 NW 体系）	備 考
IP address	192.168.1/2/10/168.*	10.5.*.*	一本化
Subnet mask	255.255.255.0	255.255.0.0	
Default gateway	192.168.1/2/10/168.*	10.5.0.254	
DNS server	192.168.1/2/10/168.*	172.16.1.*, 172.16.1.**	1st, 2nd DNS へ共通化
Domain	***.riam.kyushu-u.ac.jp	riam.kyushu-u.ac.jp	サブドメイン廃止

今回の体系変更（C 研から B 研ネットワーク体系へ）を行うにあたり、ハード的な老朽化もあったが機能面で旧 FW を継続利用することが出来なかったため、図 2 右側に示すように、新たな研究室 FW（新 FW、ブリッジモードが利用できる機種）に置き換え、LAN 側構成も 10.5.0.0/16 のセグメント 1 本で複数の研究室分のネットワークを運用管理できるようにした。すなわち、新 FW におけるポリシーは WAN1 つと LAN1 つの計 2 個の組み合わせで決定されるので、設定数は 2（$_2P_2$）となった。

表 1 にも記しているが、本変更によってネットワーク情報がスリム化（一本化・共通化・廃止）でき、

RIAM ネットワーク全体における情報と整合するようになった。利用面では、研究所全体の設定情報に一本化されたことで、研究室の利用者が自身の PC 等にネットワーク情報を設定する場合において、それまでの研究室独自情報や独自ルールを研究室ネットワーク管理者に尋ねてセッティングする必要がなくなった。また管理面では、研究室 FW の運用管理が簡素になっただけでなく、通信障害などが発生した場合に問題の切り分け（RIAM ネットワークに係る影響なのか、研究室独自ネットワークに係る影響なのか、両方の影響なのか）が容易になったため、原因特定や問題解決までの時間が短縮できるようになった。

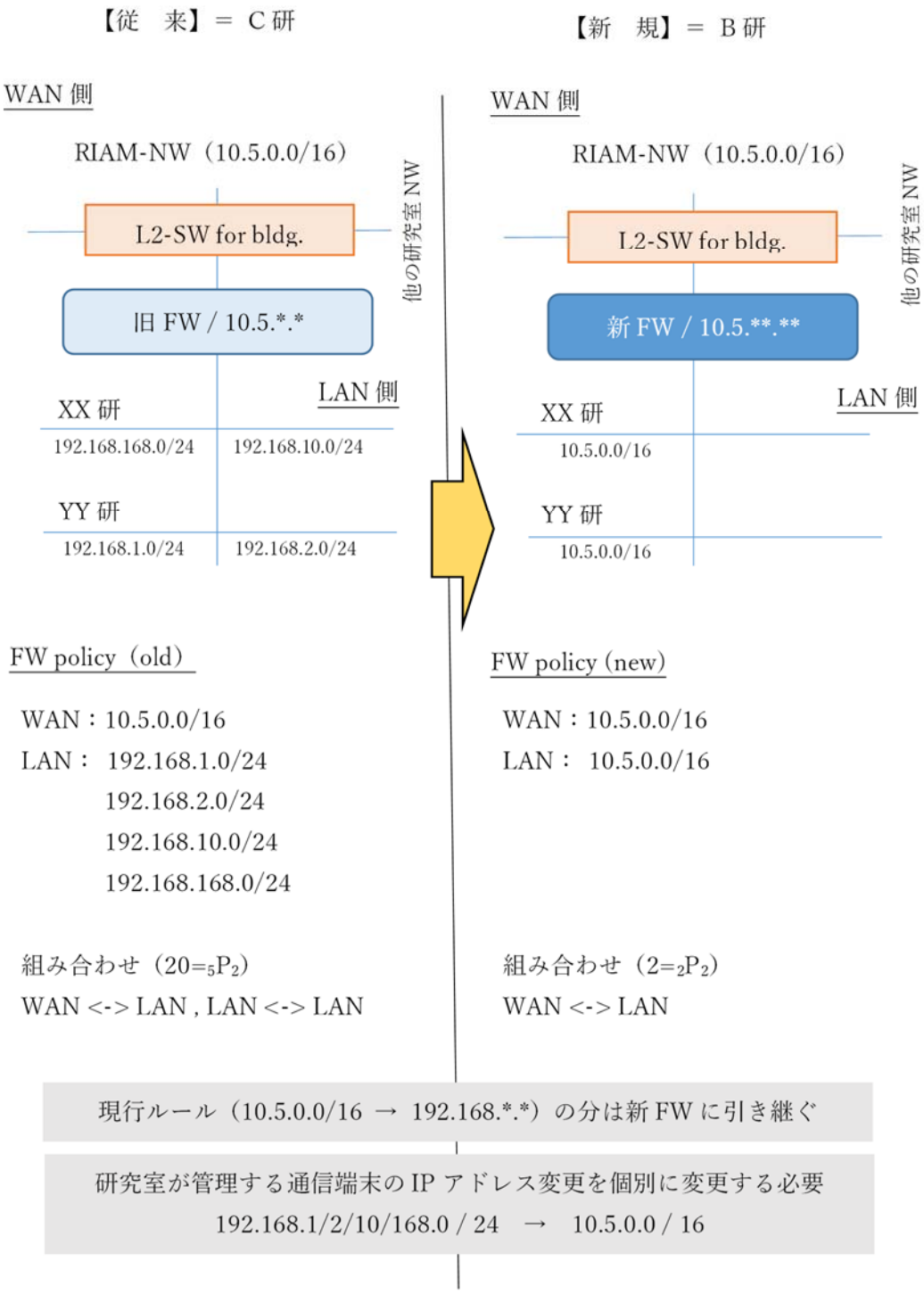

図 2　ネットワークの体系変更を実施した研究室ネットワークの概略図

６．おわりに

実際に今回の研究室ネットワーク体系の切り替えを実施した研究室は、研究所全体の 2 割程であった。応力研計算機専門委員会（研究室から選出された教員等で構成）の本案に対する理解と賛同は勿論のこと、切り替えの対象となった研究室側の積極的な協力がなければ、技術的にもマンパワー的にも腰の重い案件であったことは言うまでもない。

現在において、研究室で FW を設置する（B 研運用）または設定しない（A 研運用）の選択はあるものの、今回の切り替えによって研究室独自のプライベートネットワーク環境を有する C 研ネットワーク体系を取る研究室は無くなり、各研究室のネットワーク体系が所内で一元化された。本案の実施によって、従来から対処が必要と考えられてきた様々な問題点を解消し、RIAM ネットワーク全体におけるセキュリティの強化に繋がったことは、今後の所内ネットワーク管理に従事する上において意義深い。

参考文献

[1] 松島啓二, 石井大輔 : RIAM 計算機システムおよびネットワークインフラの更新について, 九州大学応用力学研究所技術室 技術レポート, 11, 95-99, 2010.

[2] 石井大輔 : 省エネ効果に優れた超高速スーパーコンピュータシステムの導入, 九州大学応用力学研究所技術室 技術レポート, 17, 29-32, 2016.

[3] 松島啓二, 石井大輔 : ネットワーク機器およびメール／計算機ユーザの登録・管理システム構築, 九州大学応用力学研究所技術室 技術レポート, 12, 63-71, 2011.