E-12

全国共同研究施設における情報セキュリティについて

Information Security of Joint Usage / Research Center

平井 康博　大西 克実　中野 秀男
Yasuhiro Hirai　Katumi Onisi　Hideo Nakano

１．はじめに

IT 技術の飛躍的な進歩と社会への浸透に伴い、大学における研究・教育活動においても、コンピュータ及びネットワークの利用は欠かせない物となっている。この為、各大学では様々な手法で、可用性、利便性が高く、かつ安全な情報環境の提供に努めている。特に規模の大きい大学では、キャンパス間、部局間を光ファイバや IP-VPN、広域イーサネット等の拠点間接続手法を用い、拠点側にも VLAN を利用出来るようにするなどして、地理的な制約を超えて、安全な情報共有を行おうとしている例も多々ある。　近年、情報関係の脅威は、技術の進歩に伴って多様化しており、大学側でも、技術的対策、物理的対策のみならず、セキュリティポリシーの策定や、利用者、管理者に対する情報リテラシー教育を用意する様になっている。

しかしながら、情報環境の利用者のニーズは常に変容し続けており、それが大学側の想定しない物となる事も珍しい事ではない。特に利用者側が置かれている立場に、その大学の一般的な教員や職員と異なった部分があるとそれは顕著である。

本稿では、大学における情報セキュリティの問題について、部局側からの視点で考察する事を目的とし、その為にある総合大学に所属する共同利用・共同研究拠点を主な例として取り上げる。この共同利用・共同研究拠点の事を以降　拠点 A とする。

これは、部局側が大学本部とは異なる事情を持っていた方が、より視点の差異が明白になる為であり、共同利用・共同研究拠点と言う特異性を持った拠点 A はその題材として相応しいからである。

２．共同利用･共同研究拠点

2.1 共同利用・共同研究拠点

大学における共同研究とは、大学の研究者が外部機関の研究者と、共通の課題について研究を行う事により、より優れた成果を得る事を目的とする制度である。共同利用・共同研究拠点とは、日本の大学の研究所、施設の中でも、大学の枠を超えて全国の研究者が共同利用を行える施設である。かつては、共同利用を行う場合、国立大学の全国共同利用型の附置研究所・研究施設を中心に行われるのが普通であり、その為対象の施設については国から重点的に予算配分が行われてきた。　だが、2008 年 7 月の学校教育法施行規則改正以降、全国共同利用型の附置研究所・研究施設は共同研究・共同利用拠点と名を改め、国立大学に限らず、公立、私立大学の附置研究所・研究施設についても認定が行われる様になるなどの拡大が行われた。

2012 年 7 月現在で全国 84 拠点が認定されている。

2.2 共同利用拠点の特徴

前述の様に、共同利用・研究拠点には、共同利用を目的とした研究者が多数訪れる。ここでは、このような研究者の事を共同利用者と呼ぶ。

例として下に幾つかの共同研究・共同利用拠点について、2010 年、2011 年度での共同利用採択件数を纏めた。

施設名	2011 年	2010 年
北海道大学低温科学研究所	61(件)	68
東北大学流体科学研究所	78	64
筑波大学計算科学研究センター	31	24
群馬大学生体調節研究所	28	14
千葉大学環境リモートセンシング研究センタ-	47	44
東京大学宇宙線研究所	105	97
東京工業大学応用セラミックス研究所	103	101
京都大学原子炉実験所	175	175
大阪大学レーザーエネルギー学研究センター	128	118
鳥取大学乾燥地研究センター	67	60

これらは、その年度において採択された共同利用の件数であり、その施設を訪れた共同利用者の人数と一致する訳ではない。　だが、これらの施設において、共同利用者が存在する事は常態であると言う点は十分に見てとる事が出来る。

共同利用者の多くは、共同利用・研究拠点を所有する大学に所属しない研究者である。　その為、共同利用拠点におけるネットワーク管理には、共同利用者の存在が重要な課題となる。

具体的には、共同利用者は共同利用・研究拠点を所有する大学の持つ規則やセキュリティポリシーについて無知である可能性がある事、そして共同利用者が自分自身の情報機器を持ち込んだ場合の扱いなどが挙げられる。これらの問題自体は、共同利用施設で無くとも起こり得る物ではある。　一般的な大学であっても見学や講演など、部外者が訪問する事は珍しくないし、訪問者が施設の情報環境を利用する事も珍しい事ではない。　だが、それが起きる頻度については大きな差がある。

また、一般的な大学施設では、部外者の訪問があった場合、通常は教員や職員が迎え入れる事になる為、訪問者が施設の情報環境を利用する場合に面倒をみる事が出来る。　しかし、共同利用・研究拠点では、研究が長期

†大阪市立大学　, Osaka City University

にわたる場合、施設側の教職員が常に付いていると言う考えは現実的な物とは言えない。

2.3 例に上げた拠点 A の特徴

本稿において例として取り上げる拠点 A の特徴は大きく分けて以下の 2 点が上げられる。

一つには危険物を取り扱う施設であると言う事である。これは偶に危険物を取り扱う事もあると言った話ではなく、特殊な危険物を必要とする研究や、それを用いる実験装置の使用を目的とした施設であると言う事である。この為、万が一にも外部への影響が出ないようにする為に面積が非常に広くなっている。　また、敷地は外部と遮断されており、完全な部外者の侵入は困難になっている。

二つには、拠点 A は遠隔地であり、大学本学からは直線距離で 80 キロ程度離れている。

この様に拠点 A は、共同利用拠点であるに留まらず、遠隔地である、危険物を取り扱う施設である、等の特異性を持っており、それ故に本部側との視点のずれはより大きな物になっていると考えられる。　その為に本稿ではこの拠点 A を例として取り上げる事を選んだ。

2.4 拠点 A におけるネットワーク運用上の問題

拠点 A の属する大学では、ローカル IP アドレスの情報コンセントについては、原則 LAN ケーブルを挿すだけでネットワークに接続する事が可能になっている。この運用を成立させる要因として、この大学の本部地区では、VLAN は研究室単位の狭い範囲で設定されている例が多いと言う点が上げられる。その為、管理者の目が、VLAN 全体に行き届くようになっている。また、それぞれの VLAN は独立しており、何か問題があっても VLAN 内部で留まる事になるため、各 VLAN の責任者を分担させる事ができる。

だが、拠点 A では、この運用は適切とは言えない。その理由は以下の通りである。

1. まず拠点 A では、実験装置を各研究室で共用する都合上、それぞれの研究室間の独立性は低くなる。この為、研究室単位で VLAN を切り分ける事が困難になっている。その為 VLAN は建物単位と言う広い範囲で構築している。また拠点の面積の広さから、ネットワークを介してのデータのやり取りの必要性が高く、結果 VLAN 間の通信を許容せざるを得ない
2. 前述の通り共同利用施設である為、学外の施設利用者が頻繁に訪れる。その為、大学のネットワークについての情報を十分に持たないユーザがネットワークを利用する機会が多くなっている。施設利用者向けの宿泊施設等の様に、所員の目を離れて共同利用者のみでネットワークを使用する機会も多々ある。

３．現状の考察と今後の展開

3.1 現状についての考察

2.4 で取り上げた拠点 A での問題 1.2 について、それぞれ詳細に検討を行う。

まず問題 1 についてだが、VLAN の範囲を狭くし、かつ VLAN 間での通信を制限する事には以下の二つの利点が存在する。

一つには、障害発生時に原因の発見を容易にする事が出来ると言う点である。

一例として、コンピュータウィルス感染の疑いのある情報機器を発見しなければならない場合が上げられる。コンピュータウィルスによると思われるアクセスを行っている IP アドレスが分かれば、感染の疑いのある端末が、どの VLAN にあるのかを特定する事が出来る。　ならば、VLAN の範囲が狭い方が、端末の特定が簡単なのは自明と言える。

二つには障害の影響を狭い範囲に留める事が期待できる点である。

VLAN 間の通信が遮断されていれば、いずれかの VLAN で発生した障害の影響は、その VLAN の範囲内にとどまり、他の VLAN に直接、悪影響を与える事はない。　この為、障害の影響は該当する VLAN の範囲に留まる事が期待できる。

また、この VLAN の独立によって、VLAN 管理者の責任範囲が明確化し、管理者の分担が行いやすくなる事も重要である。

だが、拠点 A では、前述の理由から比較的広い VLAN を構築し、かつ VLAN 間の通信も許容している。　その弊害は以下の様な形で現れている。

一つ目に、それぞれの VLAN が占める範囲が広く、管理者の目が全体に行きとどき難い。　この為、障害が発生した場合、原因の発見がどうしても遅れる。

二つ目に、VLAN 間の通信を許容している為、一つの VLAN で起きた障害が、施設全体に影響を及ぼし得る。一例として、コンピュータウィルスが感染したファイルが、VLAN 上の NAS に置かれている様な場合が上げられる。　VLAN 間の通信を許可している為、拠点の敷地内の何処にいようとも NAS にアクセスできる便利さはあるが、ウィルスが感染している場合、短期間で拠点内のあちこちにウィルスが感染する事態が起こりうる。

また、この VLAN 間の独立性の低さの為、VLAN 管理者は、複数の VLAN に目を配る必要が出てくる。　この為、VLAN 管理者を分担する事が難しくなっている。

次に問題 2 についてだが、共同利用者に対して、拠点 A での情報環境についての情報を与える方法として、必要最低限の情報を記述したプリントを配布しており、また共同利用者を受け入れる際に必要な説明を行うようにはしているが、それで十分と言えるかどうか疑問の余地は多いにある。

3.2 対策と目標

3.1 で取り上げた問題について、目指すべき目標と対策を纏める。

まず、問題 1 についてだが、拠点 A では、前述の理由から VLAN 間通信を完全に遮断する事は現実的ではない。しかし、VLAN 一つずつの広さに関しては検討の余地がある。　VLAN の広さを変更したとしても、VLAN 間の独立性の低さは変わらない為、管理者権限の移譲が難しい点は変わらない。　だが、それぞれの VLAN の占める範囲が狭くなれば、問題が起きた時の対応は早くなる事が期待できる。

だが、現在建物単位で VLAN の範囲を定めているのは、VLAN の範囲が何処から何処までなのかを把握しやすくすると言う意味がある。　それを変更する場合、VLAN 管理を簡単にする様な工夫が必要となる。

問題 2 に関しては、この問題を解決に近づける要素の一つとして、拠点内に大学側が用意している無線 LAN アクセスポイントの配備が進みつつある点が上げられる。この無線 LAN アクセスポイントの使用には、大学で配布しているアカウントによる認証が必要であり、共同利用者は事前に申請を行って、ゲスト用アカウントを得る必要がある。　この際に必要情報を提供する機会を作る事が出来ないか検討中である。　現在、この無線 LAN アクセスポイントは会議室等共用の場所にしか設置されていないが、それでも多くの共同利用者がゲストアカウントを申請し、これを利用している。　今後、無線 LAN アクセスポイントの配備がさらに進めば、これを利用する為のゲスト用アカウントの申請の必要性も高まる事が期待できる。

また、現在拠点 A では、共同利用申請の方法について大きな見直しを予定しており、この中で共同利用者に対する情報セキュリティについて情報を与える機会を増やす事が出来ないか検討を行う。

また、この無線 LAN の普及によって、教員が自分で設置した無線 LAN アクセスポイントの必要性を低下させる事も期待できる。　拠点 A では、登録を行い、正しくセキュリティ管理を行う事を条件に、教職員が無線 LAN アクセスポイントを設置する事を認めている。　しかし、原則 LAN ケーブルを挿せば接続できる仕様上、登録を出さずに無断で接続する例もあり、管理の甘い状態で使われる事も、過去何度か例があった。

3.3 本部と部局の視点の違い

こう言った問題が発生する根本的な原因を以下で考察する。　これは大学本部としては、全体を見なければならない為、部局の特殊事情に対応しきれない所にあると考えられる。

そこを押して無理に対応を行おうとすれば、多数の部局から各々の都合に則った要求が頻発する事になる。それに全て応えようとすれば、ネットワークの設定の複雑化は避けられない。結果としては管理コストの増大と、設定ミスによるセキュリティリスクの増大と言う結果を招く事になる。　そうなれば、基本的に大学本部側の用意した情報基盤を利用している立場である部局としても、悪影響が及ぶ事は避けられない。

それを避ける為には、本部側では個々の部局の特異性にはある程度目をつぶり、大きな視点で全体最適を目指す必要がある。　故に個々の部局の特異性の吸収は、原則として部局で行わなければならない。

今回の検討を踏まえて、この問題について考察し、提案する事が今後の課題である。

参考：

[1]文部科学省　共同利用・共同研究拠点
[2]内閣官房情報セキュリティセンター
　独立行政法人等の情報セキュリティ対策の現状
[3] 財団法人 コンピュータ教育開発センター
　学校情報セキュリティ・ハンドブック解説書

以上