



●導入の背景/課題

- ・ ナノサイエンス研究設備内にネットワーク環境を整備するにあたって、ワイヤレスの利用が必須だった。
- ・ ワイヤレスでネットワークを利用する場合、広島大学が定めるセキュリティポリシーには認証・検疫が義務付けられていた。
- ・ 認証・検疫を行うにしても、来訪者が多いため、クライアントのデバイスやOS、アンチウイルスソフトなどを限定することができず、エージェントが必須の方式では現実的ではなかった。
- ・ ネットワーク機器や利用方法などが制限されない、自由度の高いしくみが欲しかった。

●導入ソリューション

- ・ IPネットワークング
 - Cisco Catalyst 3750
 - Cisco Catalyst 2960
- ・ セキュリティ
 - Cisco NAC アプライアンス (Clean Access)
- ・ ワイヤレス
 - Cisco Aironet 1250 シリーズ

●導入効果 (期待される導入効果)

- ・ 確実な認証と検疫を実施できる環境が整った。
- ・ デバイスやOSなどを限定されることなく、ネットワークにアクセスするあらゆるデバイスのセキュリティの評価が可能になった。
- ・ 固定的なユーザはエージェントを入れて検疫・修復までを実施し、ゲストユーザはエージェントレスでセキュリティ評価を実施するなど、自由度の高い使い方が実現した。

高セキュリティの検疫ネットワークを、 自由度が高くゲストが気楽に使える環境で実現

広島大学放射光科学研究センター

広島大学放射光科学研究センター「HiSOR」は、ワイヤレスLANの普及やユーザの増加などに伴ってネットワーク環境整備に取り組み、まず2006年3月にシスコのワイヤレスLAN アクセスポイント「Cisco Aironet」を導入。接続場所を選ばないワイヤレスLANの構築を始めた。さらに、広島大学が定めるワイヤレスLANに認証・検疫を義務付けるセキュリティポリシーに則り、「Cisco NAC アプライアンス (Clean Access)」を導入して、検疫ネットワークを実現した。同施設は国内外の研究者が多く来訪し実験・研究を行うため、一時的な来訪者もネットワーク利用ができなければならなかった。そのため製品選定にあたっては、クライアントPCやOS、アンチウイルスソフトなどを限定せず、エージェントレスでも利用できることが必須だった。また、ネットワーク機器などが制限されることなく、さまざまな利用形態が可能な自由度の高いしくみを求めており、それらの要求に適合したのが、「Cisco Clean Access」だった。

研究設備内にワイヤレスLANを導入するために、 ポリシー上必須の認証・検疫システムを検討

広島大学放射光科学研究センター「HiSOR」は、国立大学唯一の放射光の研究施設として1996年に設立された。放射光とは、人類が手に入れた最も強力な光で、主に物質の分析に利用されており、タンパク質の構造解析や磁性の研究などに用いられている。2002年からは、全国共同利用施設として国内外の多くのユーザを受け入れ、ナノサイエンス等を含む幅広い研究を推進している。

このような施設での実験で得たデータの解析には情報処理が必須であり、情報処理を行うためにはネットワークが必須である。もちろん研究室では既にLANを利用していたが、利用者の増加に伴いHiSORの研究設備内でもネットワーク環境の整備が求められた。しかし、HiSORの研究設備は多くの機器が設置されたかなり広いホールであるため、そこで有線ネットワークを利用しようとする接続場所が限られてしまう。そのため、場所を選ばないワイヤレスLANを導入することにした。そこで、2006年3月にシスコのワイヤレスLAN アクセスポイント「Cisco Aironet」を3台導入し、ホール全域からネットワークアクセスが可能な環境の構築を開始した。

ただし、広島大学にはワイヤレスLANを導入する際には、何らかの認証・検疫を行う必要があるというセキュリティポリシーが規定されていたため、そのためのしくみを導入する必要があった。HiSORでは、認証・検疫システムについては、いくつかの要件があったため検討を続けることとし、まずワイヤレス環境の整備を先行し「Cisco Aironet」を設置した。放射光を使うための加速器の維持管理・改良からネットワーク管理までを担当する広島大学放射光科学研究センター 技術主任 後藤公德氏は、「当時はまだ検疫のシステムがどう動くかわかりませんでしたが、とりあえずCiscoの製品を入れておけば周りが合わせてくれるだろうと思い、Aironetを導入しました」と語っている。

その後、HiSORは、ネットワークを構築した三井情報 (当時はネクストコム) に、認証セキュリティの提案を依頼した。

高セキュリティの検疫ネットワークを、 自由度が高くゲストが気楽に使える環境で実現

広島大学放射光科学研究センター



「確実な検疫を実施しながら、自由な使い方が可能な点と、
スイッチなど他のネットワーク機器に依存せず
ネットワークの改変が不要な点を評価し、導入を決めました」

広島大学放射光科学研究センター
技術主任
後藤 公德 氏

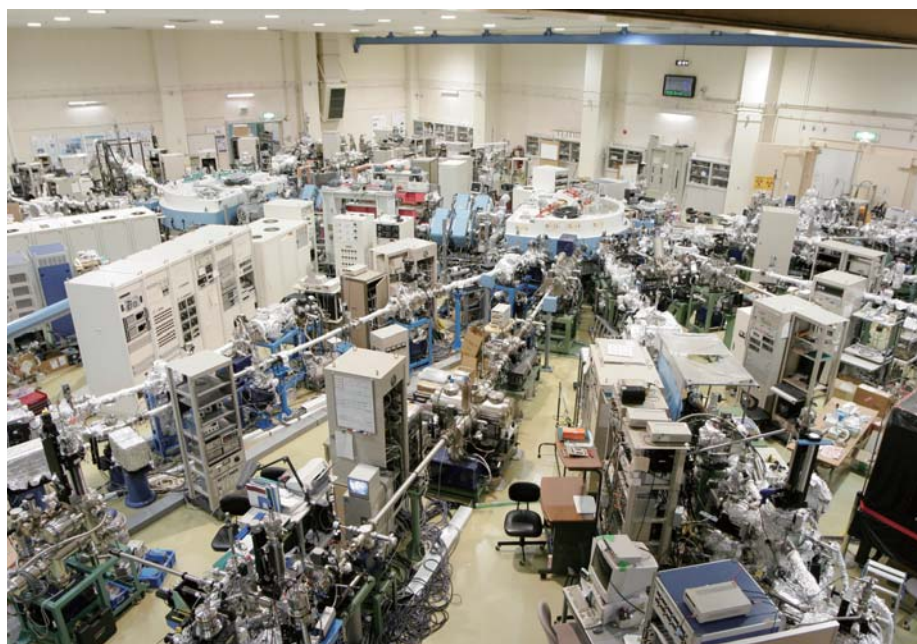
来訪者が頻繁に訪れネットワークを利用するため、 高い自由度を持ちながら確実な検疫を実現する点を評価

最初に受けた認証システムの提案は、クライアントPCのOSが限定される上、エージェントを入れる必要があり、ネットワーク機器の変更も必要だった。後藤氏は、「それは、われわれが求めるものとは異なっていました」と次のように語っている。「全国共同利用施設であるHiSORには、海外を含めた研究グループが頻繁に訪れ、2週間程度滞在をしてさまざまな実験や研究を行います。このような来訪者が持ち込むPCに、いちいちエージェントをインストールしてもらうことは、現実的ではありません。また、エージェントを入れる方式では、クライアントPCのOSが限定されてしまいます。大学の場合、企業のように利用OSを限定することはできません。さらに、アンチウイルスソフトの種類も限定され、ネットワーク機器もそのシステムに対応するものに変える必要があったため、もっと自由度の高いしゅみを求めました」

次に受けた提案は、検疫ネットワークソリューションだった。それはアンチウイルスソフトの限定はなかったものの、クライアントPCにエージェントが必要な点は同様だったことと、保守コストが高価だったため断念。なかなか決め手となる認証セキュリティシステムが決まらなかった。

そのころ、ネクストコム（当時）名古屋営業所が別の大学向けに「Cisco NAC アプライアンス（Clean Access）」を提案し、導入されたという情報が報告された。これならエージェントレスでの運用もできるということがわかったため、技術調査を開始。提案を受けたHiSORでも検討の結果、要求通りのしゅみが実現できると判断し、導入を決定した。

様々な実験機器が立ち並ぶ広島大学放射光科学研究センター



広島大学放射光科学研究センターに設置された
Cisco NAC アプライアンス (Clean Access)

高セキュリティの検疫ネットワークを、 自由度が高くゲストが気楽に使える環境で実現

広島大学放射光科学研究センター

「Cisco Clean Access」は、PC、IPフォン、ゲーム機のコンソールなどすべてのデバイスが、ネットワークにアクセスする前に、セキュリティポリシーに適合しているかどうかを識別し、脆弱性の検査と修正を行うアプライアンス装置だ。セキュリティポリシーに適合していないマシンについては遮断、隔離から修復までを行う。ネットワークへのアクセス方式は、LAN、リモート アクセス ゲートウェイ、ワイヤレス アクセス ポイントにまで拡張可能なので、デバイスが限定できず、ワイヤレス環境を利用するHiSORにうってうけだった。

「Cisco Clean Access」は、エージェントを入れると認証を行い、複数ベンダーに対応したアンチウイルス、Windows Hotfixの情報を収集し検疫を行う。一方エージェントがないゲストPCに対しても、認証と「ネットワークスキャン機能」を用いたセキュリティ状態の評価を行う。たとえば、職員や学生など学内の固定的なユーザはエージェントを入れ、来訪者はエージェントレスで利用するといった使い方が可能なのだ。

また、HiSORのネットワークには古いWindowsマシンを使った高価な測定機器も接続しており、万一それらにエージェントを入れて、ソフトウェア障害が起きてしまっは一大事だ。それらについてはMACアドレスを元にセキュリティ機能の一部をバイパスし、予期せぬトラブルを未然に防ぐよう工夫している。さらに、複数で共同利用しているPCについては、複数でIDやパスワードを共有したくないという理由から、検疫は行おうが、ネットワークログインは認証不要にした。

後藤氏は、「このように確実な検疫を実施しながら、さまざま要求に合わせた自由な使い方が可能な点と、スイッチなど他のネットワーク機器に依存せずネットワークの変更が不要な点を評価し、導入を決めました」と選択の理由を語っている。

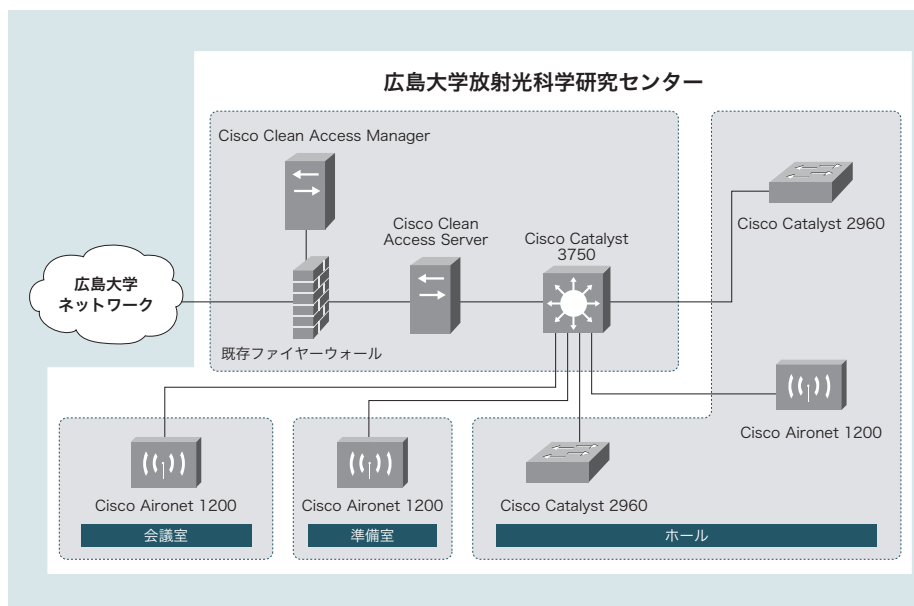


広島大学放射光科学研究センターの実験ホール内部

有線ネットワークもワイヤレスも「Cisco Clean Access」で検疫可能 接続を拒否されても、ユーザが簡単にセキュリティを更新可能

HiSORの有線ネットワークはシスコのスイッチ「Cisco Catalyst 2960」を、ワイヤレスは前述の「Cisco Aironet」を利用し、両方からのアクセスに対して、「Cisco Clean Access」が検疫を実施している。

エージェントソフトをインストールした利用者がネットワークに接続した時、たとえばWindowsのセキュリティパッチが最新でないと、その旨ポップアップ表示される。この場合、ユーザは、Windows Updateに限定的に接続が許され、誘導に従って各自でPCを安全な状態にすると接続



高セキュリティの検疫ネットワークを、 自由度が高くゲストが気楽に使える環境で実現

広島大学放射光科学研究センター

が可能になる。「Cisco Clean Access」のデータベースが、Windowsセキュリティパッチやアンチウイルスの情報を自動で更新するため、ユーザは管理者の手を借りる必要がない。

HiSORは、「Cisco Clean Access」の導入にあたって、接続を許可するPCを登録するためのマネジメントソフトを作成した。その理由を後藤氏は、「Cisco Clean Accessの管理は、全体の整合性を取るために、私がひとりで行っています。しかし、Cisco Clean Accessは、基本的に管理者だけが各種設定を行うことができるしくみになっているため、ユーザの登録や追加などの作業もすべてひとりで行わなければなりません。それでは負荷が大きいため、全体の管理は私が行いますが、利用者の登録はサブ管理者に任せるため、マネジメントソフトを作成してもらいました」と語っている。

利用方法としては、まず管理者である後藤氏が「Cisco Clean Access」に利用グループの登録を行い、各グループのサブ管理者が、新たに作成したマネジメントソフトを利用して、スイッチやAironetに対して接続を許可するPCのMACアドレスを登録することで利用可能にするしくみだ。

後藤氏は、「Cisco Clean Accessはユーザを登録するイメージですが、今回開発したマネジメントソフトはPCを登録するイメージで作りました。統制を強めている世の中の流れからすると逆行しているのかもしれませんが、全体の管理の整合性を保ちながら負荷を分散して管理を容易にするために、このような方法を選択しました」と語っている。

「Cisco Clean Access」は、まだ稼働して間もないが、なんの違和感もなく利用できるとユーザからも評価されている。

HiSORは、今回のシステムの導入により、多くの来訪研究者が利用するネットワークを、自由度を保ちながら安全に利用できる環境を整備することに成功した。今後、研究所内のワイヤレスLANが利用できるエリアを拡大し、より柔軟なネットワーク環境を実現したい意向だ。



広島大学放射光科学研究センターに設置されたワイヤレスアクセスポイント Cisco Aironetシリーズ

Profile

広島大学放射光科学研究センター

所在地：広島市東広島市鏡山2-313

設立：1996年

広島大学放射光科学研究センター「HiSOR」は、放射光科学分野の人材の育成と真空紫外・軟X線域の放射光を用いた学術研究を推進する目的で、1996年学内共同教育研究施設として発足した。その後2002年には、全国の大学の研究者が利用する施設（全国共同利用施設）として生まれ変わり、放射光科学研究の国内拠点のひとつとして位置づけられた。毎年国内外のユーザにより多数の研究が行われると共に、卒業研究・実習や学位研究なども進められ、多くの若手研究者・技術者が国際社会に飛び立ち活躍している。

<http://www.hsrc.hiroshima-u.ac.jp/>

©2007 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料の記載内容は2007年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先（シスコ コンタクトセンター）

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

お問い合わせ先