安全なギガビットネットワーク KUINS-III の構築と運用

江原 康生　高倉 弘喜　宮崎 修一　中村 素典
沢田 篤史　岡部 寿男　金澤 正憲

京都大学 学術情報メディアセンター
〒606-8501 京都市左京区吉田本町

要 旨

京都大学では 2002 年 4 月より,「安全なギガビットネットワークシステム (KUINS-III)」の運用を開始した．近年セキュリティ被害が増大する中，学内ではセキュリティ対策が不十分のままインターネットに接続されている機器が多い．また，従来運用されてきたネットワーク (KUINS-II) は，管理の管轄が各建物の入り口となるルータまでで，その先の建物内の配線や管理は部局任せだった．そのため，ネットワークのトラブルや不正アクセスによる被害が生じたときに，管理者が不在などにより状況を把握できないことが多く，学内のセキュリティレベルを維持することが困難となった．KUINS-III では，全学のセキュリティレベルの向上を主目的とし，新しいネットワークを新規に配線することにし，各部屋の情報コンセントまで管理するネットワークを設計した．これにより，約 16,000 ポートの情報コンセントの管理ができ，また 約 5000 を超える VLAN を割り当てて，きめ細かなポリシーを決定できるようにし，機器のセキュリティ向上と不正アクセスの拡散防止を試みた．本稿では，KUINS-III の構築及び運用状況の概要について述べる．

Structure and Operation of Secure Gigabit Network System, KUINS-III

Yasuo EBARA　Hiroki TAKAKURA　Shuichi MIYAZAKI　Motonori NAKAMURA
Atsushi SAWADA　Yasuo OKABE　Masanori KANAZAWA

Academic Center for Computing and Media Studies, Kyoto University
Yoshida-honsho, Sakyo-ku, Kyoto 606-8501, JAPAN

Abstract

In Kyoto university, the operation of secure gigabit network system (KUINS-III) have been started in April, 2002. Many computers which security protection is not insufficient are connected to the Internet on the campus, while security damages increase in recent year. In past campus network (KUINS-II), the network management was divided into a router in each building, and the wiring of cable and the management in the building was dependent on each department. In case damages by network trouble and the cracking occuerd, the situation could not confirm by absence of the network manager. Consequently, the improvement of security level was very difficult. To improve security level in all-campus, we designed new network system which could manage sockets in each room by new wiring in KUINS-III. We attempted to improve the security level and to prevent the diffusion for the cracking, by the management of 16,000 information sockets and the configuration with the details policy for more than 5000 VLAN. In this report, we explain the structure and the operation of KUINS-III.

1 はじめに

1989年に運用を開始した京都大学キャンパスネットワーク KUINS(京都大学統合情報通信システム)は，ATM バックボーンの導入などによる高速化を近年まで進めてきた．しかし，ネットワーク機器の高機能化やルーティングプロトコルの多様化，複雑化した現在では，受益者負担によるネットワーク運用という当初の常識が成り立たなくなりつつある．また，本学に対する不正アクセスの急増が IDS 等で確認されている状況の中で，全学で約 30,000 台の機器について高水準のセキュリティを維持することは困難であり，将来的に不正アクセスによる被害が深刻化されるのは必至と考えられる．しかし，一般的な防御策であるファイアウォールによる学外との通信遮断は，教育研究機関として有する柔軟かつ自由な通信環境を放棄することになり，本学では受け入れられない．

そこで，既存の KUINS-II/ATM ネットワーク [1] 上で運用されてきた global IP アドレス LAN と並行に，ファイアウォールで保護される代りに制約のある private IP アドレス LAN として，「安全なギガビットネットワークシステム (KUINS-III)」を構築し，ユーザが目的に応じてどちらを利用するかを選択できるようにした [2][3]．現在，KUINS-III では 4,000 を超える VLAN が構築され，12,000 台以上の機器が接続されている．

本稿では，KUINS-III の構成及び運用ポリシーについて，その概要を述べる．

2 KUINS-III の構成

2.1 概要

本学のネットワーク構成図を図 1 に示す．本学の主要キャンパスは 8 構内 (吉田地区 7 構内+宇治地区 1 構内) に分割され，キャンパス LAN の管理単位もほぼこれに従っている．また平成 15 年度には新しいキャンパスとして桂地区が開校予定である．本稿で述べる KUINS-III は濃色のライン及びそれらに接続されている機器が該当し，薄色のライン系統は既存の ATM ネットワーク (KUINS-II) を表す．

各構内はセンタールータ (CR) とギガビットイーサネット 2 回線 (吉田地区)，10 ギガビットイーサネット 1 回線 (宇治・桂地区) で接続されている．また吉田地区では，基幹スイッチ (KS) 間でバックアップ用の冗長回線を設けている．一方，遠隔地キャンパスの内，原子炉研究所 (大阪府熊取町)，付属農場 (大阪府高槻市)，生態学研究センター (滋賀県大津市)，飛騨天文台 (岐阜県)，地震予知研究センター (宮崎県)，付属火山活動研究センター (鹿児島県)，霊長類研究所 (愛知県犬山市) を IPSec ルータ (NR) による暗号化通信を行っている．

これまで本学では，原則として建物単位で大きなサブネットを割り当てていたため，アドレス空間全体では，global IP アドレスに十分な空きがあったにも関わらず，割り当て可能なサブネット数が不足し，最近では新築の建物には 27bit マスクのサブネットを構成せざるを得ない状態である．しかし全学でのサブネットの再構成を行うには膨大な時間を要するので，KUINS-III では private IP アドレス (10.224.0.0/11) を使用している．経路制御はファイアウォールルータ (FR)，センタールータ (CR)，基幹スイッチ (KS) の間で OSPF を使用している．そのオーバヘッドを減らすために，各構内毎に複数のクラス B のネットワークを割り当てている．平常時の他構内への通信はセンタールータを経由し，センタールータの障害時には基幹スイッチ間のバックアップ回線を選択する．

2.2 機器構成

2.2.1 ファイアウォールルータ (FR)

学外との接続にはファイアウォールルータとして，**Juniper M20** を設置し，以下の用途に使用している．

- 学外と global IP アドレス LAN 間通信に関して，危険性の高い通信を遮断
- 学外から private IP アドレス LAN へ流入する通信を遮断
- 学外とサーバ群 (2ヶ所) 間の通信を振り分け

2.2.2 センタールータ (CR)

Catalyst 6513(L3(レイヤー 3) スイッチ) と **NEC CX 5210**(ルータ) を設置し，以下の用途に使用している．

- 学外と global IP アドレス LAN 間の通信を中継
- 各構内の基幹スイッチ (KS) を収容し，構内を跨ぐ VLAN 間の通信を中継
- global 及び private IP アドレス LAN の各クライアントからサーバへの通信を中継

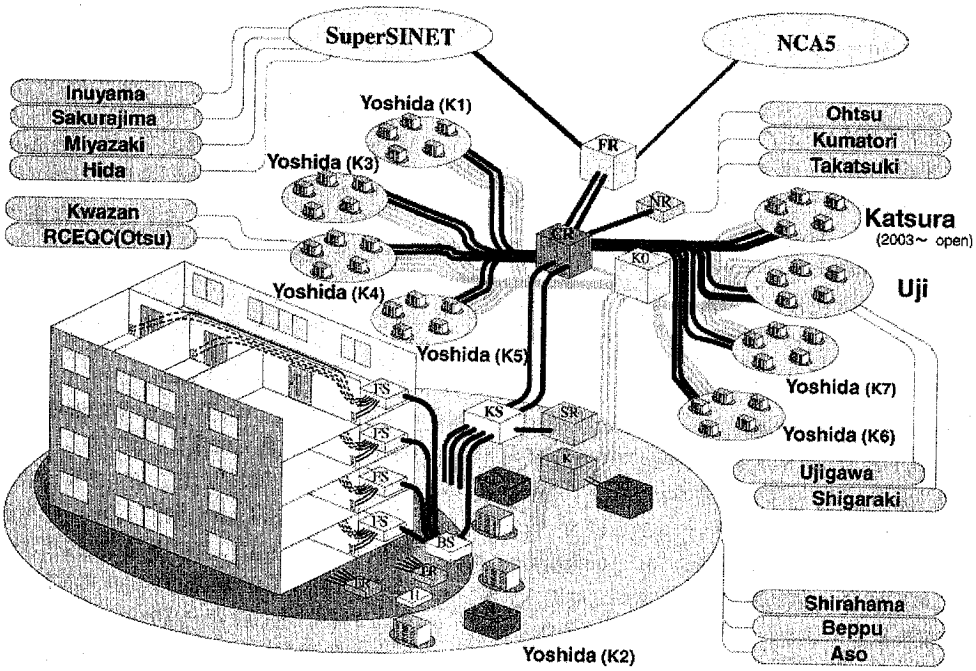

図 1: KUINS-III のネットワーク構成

2.2.3 基幹スイッチ (KS)

各構内に **Catalyst6509** または **6513**(L3 スイッチ) を 1 台づつ設置している．各構内で基幹スイッチ (KS) と global IP アドレス LAN を管理する KUINS-II ルータ (SR) と ATM スイッチ (N) とギガビットイーサネットと ATM(OC-12) でそれぞれ接続されている．基幹スイッチの主な役割は，

- 配下の構内に設置された館内スイッチを収容
- 構内の各 VLAN に対し，ACL(Access Control List) を設定
- 構内の VLAN 間通信を中継
- KS と SR 間のギガビットイーサネット回線を介して，global IP アドレス LAN と private IP アドレス LAN 間の通信を中継
- KS と N 間の ATM 回線を介して，global IP アドレスを KUINS-III VLAN に提供

2.2.4 館内スイッチ (BS)

建物を管理単位とする **Catalyst3508**(L2 スイッチ) を約 200 台設置し，建物内の末端スイッチを収容する．通常，館内スイッチは建物の情報機器室などに設置されている．

2.2.5 末端スイッチ (FS)

原則として，各階を管理単位とする **Catalyst3512**，**3524** または **3548**(L2 スイッチ) を約 700 台設置し，各部屋の情報コンセントを収容する．基幹スイッチから末端スイッチまでは 1 回線以上の光ファイバを使用し，ギガビットイーサネットで接続されている．一方，末端スイッチから各居室までは，UTP ケーブルによるファストイーサネット (100Mbps) の提供となる．なお，UTP ケーブルの距離的な制約により，末端スイッチは廊下等に設置されることが多いため，鍵付の箱に収容されている．

2.2.6 情報コンセント

従来本学では，ネットワーク管理部門の責任分界点は各部局の建物に設置されたネットワーク機器までとしていた．部局の管理下にある配線のほとんどは，必要時にボランティア作業で敷設されたため，時間経過に伴い，配線・接続状況が把握できなくなる事態に陥っていた．このため，KUINS-III ではネットワーク管理部門の責任分界点を居室の情報コンセントまでとし，そこまでの配線を管理することにした．

当初，各部屋 2 ポートを基準として，キャンパス全体に約 16,000 ポートの情報コンセントを設置し

たが，逐次追加工事が行われ，平成 15 年度開校予定の桂地区の分を合わせると，約 20,000 ポートを超える見込みである．

2.2.7 IDS(不正アクセス検出装置)

平成 10 年から運用中の IDS の経験を踏まえ，キャンパス各所に十数台の IDS(**Cisco IDS** 及び **Recourse ManHunt**) を設置した．内 9 台はセンタールータと基幹スイッチの内蔵型であり，これらを通過する通信を監視している．IDS の警報総数は誤報も含めて，一日当り平常時で 20 万件前後，ピーク時には 150 万件に達している．

2.2.8 各種サーバ群

KUINS-III は学外との直接通信を禁止することで，セキュリティレベルを高めている．private IP アドレス LAN から学外への接続には NAT(ネットワークアドレス変換) 装置の利用が一般的である．しかし NAT 装置の運用では，万一に備え，アドレス変換記録を保持する必要があるが，KUINS-III に接続される数万台のクライアント機器に関する変換記録を保持することは技術的に困難である．そのため，全学規模の NAT は運用せずに，以下のサーバを設置し，学外との接続を行う．

- 外部，内部 DNS サーバ
- メールサーバ
- Web キャッシュサーバ
- DHCP サーバ (管理サーバも含む)
- Socks，deligate サーバ
- ログ収集サーバ

このうち，メールサーバは学内と学外間，あるいは学内間のメール配送を行うと同時に，ウィルス検査も実施している．一部のサーバを除いて，それぞれ複数台を 2 箇所に分散配置している．2 箇所共に UPS と 外部給電設備を備え，一方が電源供給を絶たれても他方がサービスを引き継げるように設計している．

KUINS-III ではプリンタやファイルサーバなどを除き，DHCP による IP アドレス管理を原則としている．DHCP サーバによるアドレス発行の記録を保存することにより，万一の際に機器を特定することができる．利用頻度の高さから，DHCP サーバは基幹スイッチと同じ場所に設置している．吉田地区では各基幹スイッチのある場所に 1 台づつ配置し，計画停電の日程や地理的距離を考慮して，2 台の DHCP サーバで primary/standby の組を構成している．一方，宇治地区では，primary/standby 構成の 2 台を設置している．primary/standby の切替は，DHCP 管理サーバで制御しており，発行済みの IP アドレスなどの情報をそのまま standby 側で引き渡すことで，矛盾のない切替が可能となっている．

これらのサーバが生成するログは全てログ収集サーバが保持している．

3 VLAN の構成

3.1 VLAN の概要

KUINS-III では，VLAN 毎の管理責任者の申請に基づき，複数の情報コンセントで VLAN を構成する．各学部の特性に応じて，教官・学生部屋を全て含む研究室 VLAN，教官室のみ，学生部屋のみで構成される VLAN，各教官室で独立した VLAN などの申請に従い，現在約 4,000 の VLAN が設定されている (DHCP サーバで約 12,000 の MAC アドレスの接続が記録されている)．桂地区が開校する来年度は VLAN 数が 5,000 を超える見込みである．

ただし，各ネットワーク機器の使用上制約と障害発生時の原因調査が複雑になるため，複数の構内に跨る VLAN は原則として認めず，L3(レイヤー 3) による VLAN 間の通信を提供している．実際には，OSPF による経路制御では全ての VLAN 間で到達可能な状態になっており，アクセス可能な VLAN を ACL で定義することでアクセス制御している．

3.2 VLAN 単位のセキュリティポリシー設定

VLAN の設定・変更申請は，VLAN 管理責任者 (教職員に限定) のみが行える．VLAN 管理責任者はその VLAN に接続される機器及び使用状況を把握する必要があり，万一の場合には法的責任が及ぶ．VLAN の特性 (物理的・人的セキュリティ) に応じてアクセス制限 (技術的セキュリティ) を定め，KUINS-III として要求されるセキュリティレベルを維持することとした．図 2 にその例を示す．

(1) オープンスペース (例: 講義室)

常時施錠されていない不特定多数の出入りがあるなど物理的・人的セキュリティの確保がなされていない部屋は他の VLAN に加え，DHCP と DNS 以外のサーバへのアクセスを禁止し，global IP アドレス LAN へのアクセスは，SSH

か PPTP(Point-to-Point Tunneling Protocol) のみを許可する．つまり，ssh あるいは PPTP を介して global IP アドレス LAN に設置された機器でユーザ認証を受け，port forwarding やトンネリングを用いなければ，当該 VLAN の外 (学外も含む) との通信ができない．なお KUINS-II(global IP) への機器設置は申請制となっており，許可されていない機器については学外だけでなくサブネット内の通信もできなくなる対策を平成 15 年 1 月より講じる予定である．

(2) クローズドスペース (例: 教官室・事務室)

無人時には施錠され且つ，出入りする人も限定される部屋は物理的・人的セキュリティがある程度確保されているとして，申請に基づき他の VLAN へのアクセスや global IP アドレス LAN へのアクセスを認めている．ただし，global IP アドレス LAN からのアクセスは原則として認めていない．

3.3 アクセス制御

クローズドスペース VLAN であっても，global IP アドレス LAN の機器や他の VLAN に対する通信はその相手先とプロトコルの組を申請する必要がある．大半の VLAN では，任意の global IP アドレス機器に対して任意のプロトコルを通す申請がなされている．一方で，VLAN 管理責任者がクローズドスペースではあるが，人的セキュリティが若干低いと判断している VLAN について，特定の KUINS-II 機器 (例えば，部局のメールサーバ) に対して特定のプロトコル (SMTP と POP3 など) に通信を限定する設定や，一方向アクセスなどの設定もなされている．

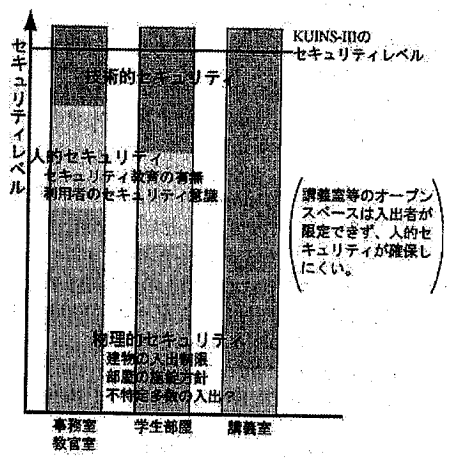

図 2: 部屋毎のセキュリティポリシーの設定

3.4 global IP アドレス VLAN

KUINS-III のもう一つの目的として，適切に管理されていない回線廃止の促進があり，そのためクローズドスペースに設置された情報コンセントに global IP アドレス LAN 環境の提供も行っている．各部屋に設置されている情報コンセント 2 ポートの内，1 つを private IP アドレスか global IP アドレスの何れかに選択できるようにした．また識別を容易にするために，private IP アドレス専用ポートには緑の蓋を，選択できるポートに黄色の蓋を設けた．

これは，基幹スイッチと ATM スイッチ (図 1 の N) 間の ATM 回線を介して，ATM ネットワークの LANE(LAN Emulation) と KUINS-III VLAN を接続することで実現している．何らかの理由により，LANE への接続が困難な場合は，VLAN の情報コンセントの 1 つを最寄りの global IP アドレス LAN のスイッチ等 (部局設置) に接続している．

4 KUINS-III のセキュリティ対策例

4.1 Policy Routing を用いた NAT 装置接続

各種サーバを介して private IP アドレス LAN から学外にアクセスできるプロトコルは限定されるため，これ以外のプロトコルを用いた学術研究を行う場合に多くの不都合が生じる．学外と直接通信できる環境を設ける一手段として，それぞれの VLAN に default gateway となる NAT 装置の設置が考えられる (図 3)．しかしこの手法では，以下の問題点が存在する．

(a) NAT 装置を介した通信のスループットが装置の性能によって制限される (特に NAT 装置を跨ぐ場合)

(b) IDS で，NAT 装置の global IP アドレスに対する (からの) 通信だけしか検査できない

(c) 他の VLAN への経路制御を NAT 装置で行う必要がある

これらの問題を回避するために，Policy Routing[4] による解決を試みる．VLAN 内のクライアントと global IP アドレス LAN との通信は次の経路を通る (図 4)．

[クライアントからの通信]

(1) クライアントは default gateway(基幹スイッチ) にパケットを送出

(2) 基幹スイッチの内蔵 IDS によりパケットを検査

(3) Policy Routing に基づき，基幹スイッチは VLAN の NAT 装置にパケットを送出

(4) NAT 装置は global IP アドレス 側に向けてパケットを転送

[クライアントへの送信]

(A) NAT 装置は global IP アドレス側で受信したパケットをクライアントへ直接転送

以上により，global IP アドレス側の IDS で NAT 装置を発信元とする通信を検査するだけでなく，private IP アドレスの通信を基幹スイッチの IDS で検査することができる．この手法は一つの通信を複数の IDS で検査するため，IDS のログ増加の一因となるが，実運用では global IP アドレス LAN の IDS で異常検知時のみ private IP アドレス LAN に関わるログを精査すれば良い．

一方，学内の global IP アドレス LAN や他の VLAN への通信は，

(1) クライアントは default gateway(基幹スイッチ) にパケットを送出

(2) 基幹スイッチの内蔵 IDS によってパケットを検査

(3') 基幹スイッチは ギガビットイーサネットで接続された KUINS-II ルータ (SR) を介して，global IP アドレス LAN，あるいは 他の VLAN に向けてパケットを転送

となり，NAT 装置を設置しない VLAN と同じ経路を通ることになる．したがって，学外からの通信を除き，private IP アドレスに関する通信を基幹スイッチで検査することが可能である．

5 まとめ

本稿では，KUINS-III の構成，VLAN の分類に応じたアクセス制御のポリシーについて述べた．KUINS-III の運用開始から 9ヶ月が経過したが，VLAN を含む各種設定等はまだ試行錯誤を続けている段階であり，今後は安定かつ効率的な運用手法の検討が課題と考える．

謝辞

KUINS-III の維持運用に，日頃からご尽力いただいている本センター情報サービス部ネットワーク担当の諸氏，構築に携わっていただいた NEC の皆様，IDS の運用に関し，ご支援いただいた日新電機の皆様に感謝いたします．

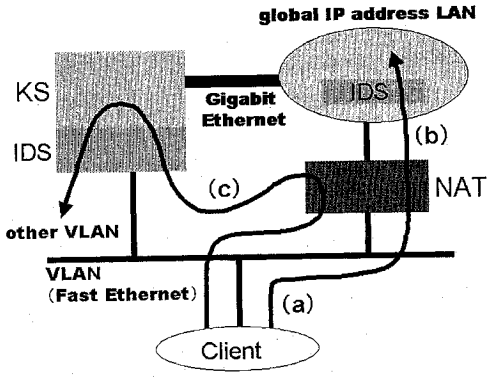

図 3: NAT 装置を用いた通常の接続

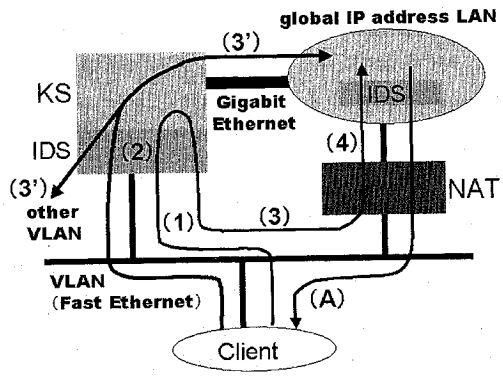

図 4: Policy Routing による NAT 接続

参考文献

[1] H.Ishibashi, Y.Okabe, M.Kanazawa: Design and Implementation of Very Large Scale ATM LAN for Kyoto University, Proceedings of the 13th International Conference on System Science, Vol.III, pp.60-67,1998

[2] 高倉 弘喜 他: 安全なギガビットネットワークシステムの構築と管理の現状, サイエンティフィックシステム研究会システム技術分科会, 2002

[3] 高倉 弘喜 他: 安全なギガビットネットワークシステム KUINS-III の構想とその構築, 第 24 回全国共同利用大型計算機センター研究開発連合発表会, pp.61-65, 2002

[4] E.J.Yoshida: 「常時接続時代のパーソナルセキュリティ対策 (第 2 回) -Routing and Remoto Access サービスのパケット・フィルタリング機能」の内容にある危険性について, 2001