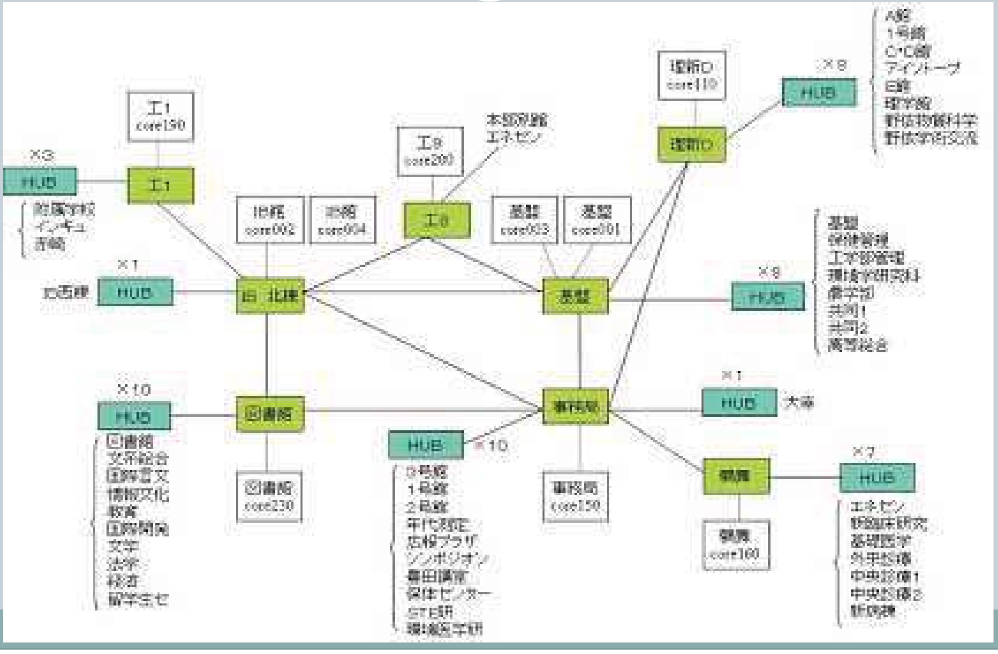
名古屋大学キャンパスネットワークNICEの新機能ーe-NICEとSecure-NICEー

名古屋大学　情報連携基盤センター
情報基盤ネットワーク研究部門
八槇　博史

e-NICEとSecure-NICE

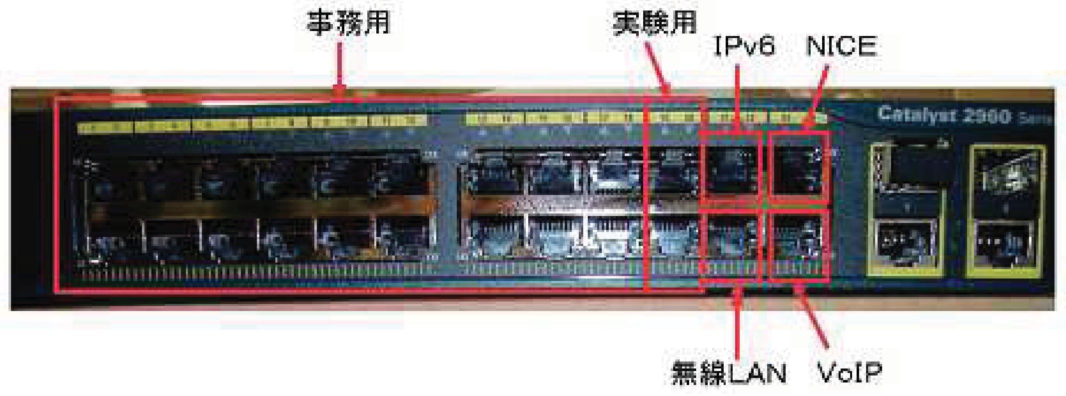
- e-NICE
  - 平成17～18年度整備
  - ギガビットの基幹ネットワーク
    - VLAN機能の活用
    - 障害時・停電時のNICE IIIのバイパス構築
    - 災害発生時のネットワークサポート
    - VoIPサービス
    - IPv6サービス
- Secure-NICE
  - 平成18～19年度整備
  - ファイアウォールの提供

e-NICE構成図



VLAN機能の活用

- ネットワーク上に複数のVLANを設定することにより、1つの基幹ネットワークを複数の用途に利用できる
  - ハブの各ポートにそれぞれVLANを割り当て
  - 端末を接続する際には所定のポートへ接続することで、所望のVLANを利用する



VLANの割り当て

VLAN	割り当てポート番号
事務用ネットワーク	1〜18
実験用ネットワーク	19〜20
IPv6ネットワーク	21
災害対策無線LANネットワーク	22
NICE	23
VoIP	24

事務用ネットワーク

- 旧来NICE II（平成5，7年度導入）の設備を利用していたものを切り替え
  - スイッチングハブ(Catalyst5000)の保守切れなど
- 新規導入のギガハブの大部分のポートを事務用ネットワークとして利用
  - 新事務用ネットワークは建物間の接続がギガビットのスター型
  - 旧来のFDDI (100Mbps)との比較で10倍以上のパフォーマンスが期待できる
  - 平成18年6月に新ネットワークへの切り替えを完了

IPv6

- IPv6専用のVLANを構築
  - 名古屋大学としてのIPv6アドレス 2001:02F8:002F::/48を取得
- 現時点では名古屋大学のIPv6以降は初期的な検討段階にとどまっている
  - いくつかの研究室が実験的に利用中

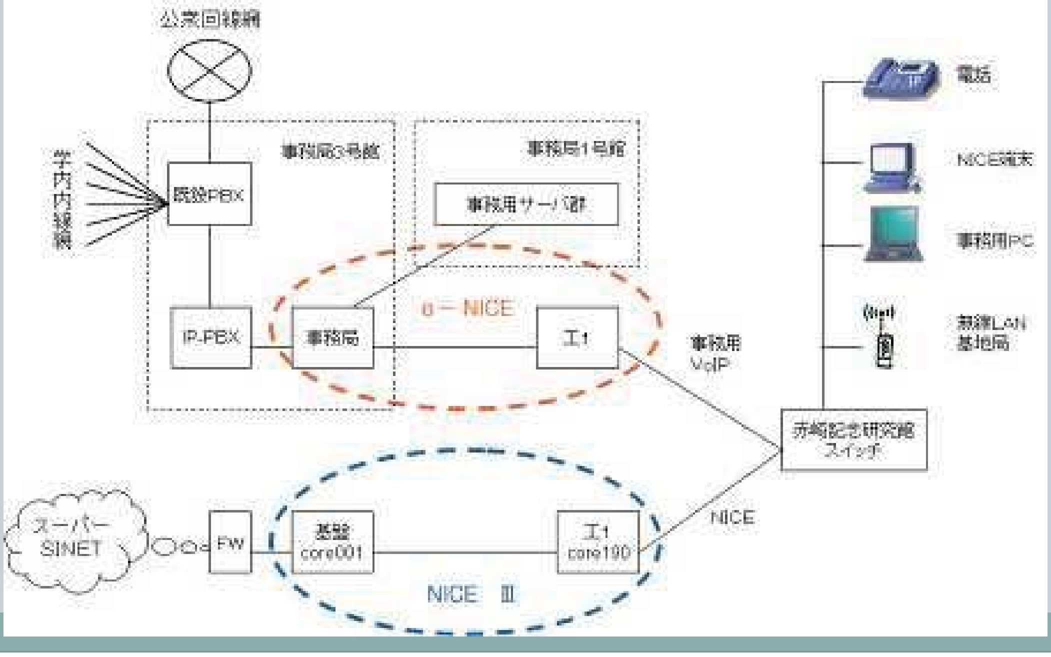
災害時対策無線LANネットワーク

- ギガビットスイッチすべてに30分間電源を供給できる無停電電源装置(UPS)を設置
  - コアスイッチには瞬間停電対応程度のUPS
- 基盤センター、附属図書館、事務局3号館への無線LAN基地局のUPS付きでの設置
  - これらの場所では学内停電時でもノートPCによりネットワーク使用可能
  - SINET3への接続機器にもUPSが設置されており、一定時間の電源供給が可能なため、災害時の安否確認などのアプリケーションへも対応が可能

VoIP (Voice over IP)

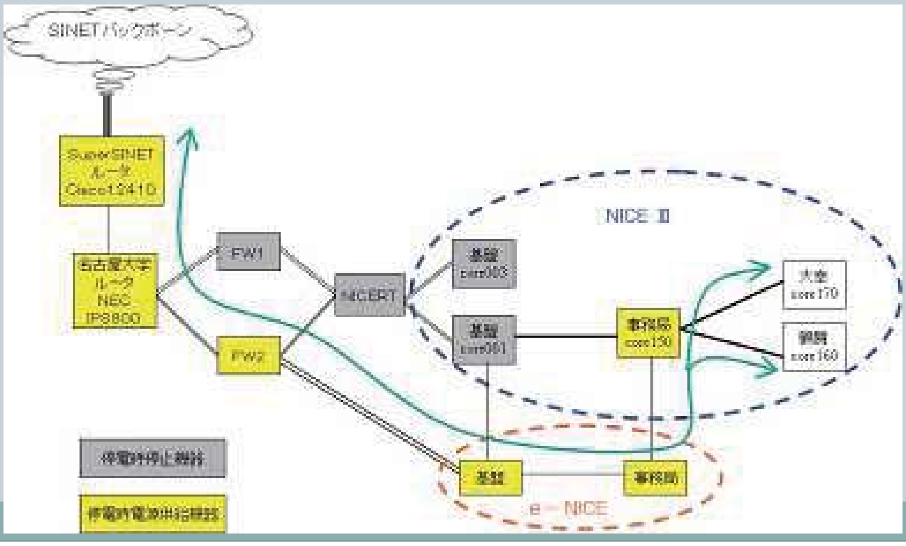
- 平成14年度以降の改修・新営の建物について、将来的な移行へ向けたVoIP対応電話設備の導入
  - 情報ラックないでのパッチパネルによる成端処理
  - UTPケーブルによる電話配線
    - モジュラー部分のみは電話用の6極2芯だが、情報用8極8芯に取り換えることでVoIP以降が可能
- テストケースとしての赤崎記念研究館（次頁）
- VoIP用VLANへの優先度の高いQoS設定
  - 他のVLANで大量の通信が発生してもVoIPの通話性能を低下させない

赤崎記念研究館のネットワーク



NICEのバイパスとしての基幹ネットワーク利用

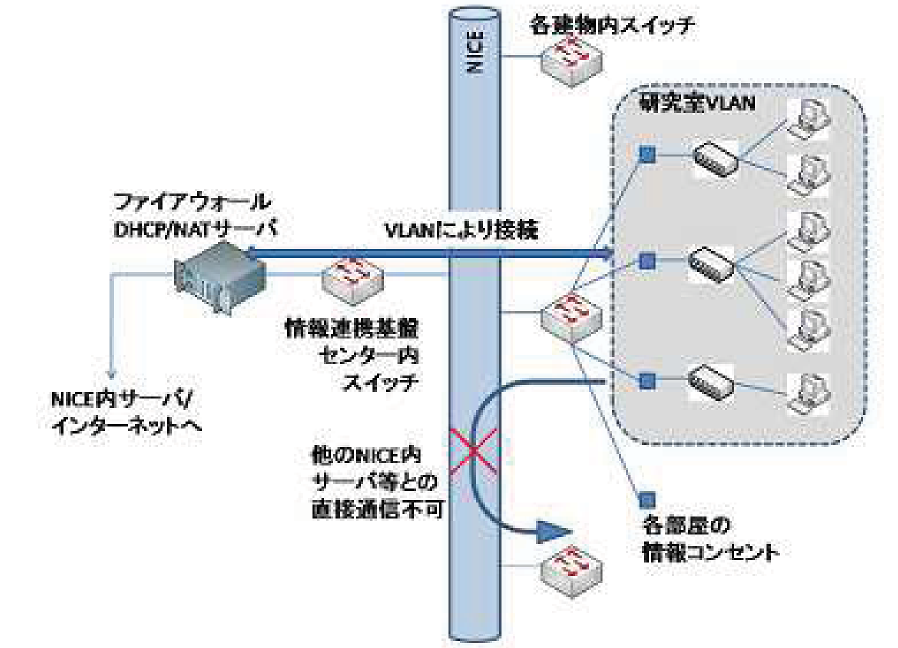
- 東山キャンパスの計画停電などの際にも、鶴舞キャンパス、大幸キャンパスでインターネットアクセスが可能



Secure-NICE

- VLANを活用し、各研究室のLANを基盤センター設置のファイアウォール以下に収容するサービス
  - 各研究室では設置済みの情報コンセントに接続する
  - 情報コンセントを一つのVLANに収容し、プライベートアドレス空間とする
  - このVLANと、センターのファイアウォール+DHCP+NATサーバとを接続する
- 平成19年4月サービス開始
  - 公開の遅れによってサービス利用数がまだ伸びていない

Secure NICEシステム概要



SecureNICE使用のメリット

- センタ提供のファイアウォールの使用
  - 自前で購入・設定する手間がはぶける
  - 安価なものと比べるとパフォーマンスがよい
    - 安価なインターネットルータには、大学ネットワークとの接続時にトラブルを起こすものもある模様
  - 研究室単位でファイアウォールを導入すると、その下がセンターから見えなくなるため、ネットワークトラブル時にセンターのサポートを受け難い
- センタ提供のDHCPサーバの使用
  - 「挿すだけ」で使用開始できる
- プライベートアドレス空間の使用
  - NATサーバ経由での外部との通信
  - 外部からの直接のワーム侵入を抑止

Secure NICEでのアクセス制御

- 外部から**VLAN**内部へのアクセスは原則不可
  - 機械が対応していないという意味ではなく、ポリシーとして
- 内部からのアクセスについては、通信可能ポートを申請に基づいて制御
  - デフォルトで以下の通信が可能

    DNS (53/udp),NTP (123/udp), HTTP (80/tcp), HTTPS (443/tcp), FTP (20-21/tcp), SMTP (25/tcp), SMTPS (465/tcp), POP3 (110/tcp), POP3S (995/tcp), IMAP4 (143/tcp), IMAP4S (993/tcp), SSH (22/tcp), TELNET (23/tcp)

Secure NICE増強

- 仕組み上、クライアントが増えるとセンターのサーバへの負荷がそれだけ上がることになる
- **NICE**内には**VLAN**対応でないスイッチが残っているため、これらの配下にあるネットワークから**Secure NICE**が利用できない
- 19年度総長裁量経費によるスイッチ置換え、ファイアウォール増設を計画中

VLAN管理システム

- e-NICE, SecureNICEなどVLAN使用のサービスが増えている
  - 従来のように設定を紙や個人に依存して記録していたのでは早晩行き詰る
  - ネットワークの設定状況が必ずしも把握しきれていないため、SEに依存しなければ設定変更もままならない状況にある
- 平成18～19年度CSI予算によってVLAN管理システムを構築
  - VLANの設定内容を記録するためのシステムが完成。新規設定のVLANから順番にデータを投入
  - 設定内容記録だけでなく、VLAN管理システムからワンタッチでスイッチの設定を行う機能までの完成をめざす

まとめ

- e-NICE
  - VLANを活用したNICEシステムの増強
  - 各種新サービスの提供
- Secure NICE
  - VLANを活用した安全なネットワークアクセスの提供
- VLAN管理システム
  - VLAN運用を効率的に行うための管理・設定システムの構築