東京大学におけるネットワークとセキュリティ対策の概要

2008.11.28

東京大学情報基盤センター
主査（情報基盤整備担当）

早野裕士

構成

- 東京大学の概要
- UTnetの概要
- セキュリティ対策等
- 東京大学の情報関連の体制等
- その他

東京大学の概要

学生　　：２８，７７３人(2007.5.1現在)
教職員　　：　７，５９２人(2007.5.1現在)
研究科･学部：　　１５
附属研究所　：　　11
全学センター：　　２１
施設等　　：全国５２ヶ所

UTnetの概要

- 学内・学外との間で様々な情報の交換を可能とする東京大学のキャンパスネットワーク
- 本郷・駒場・柏および全国にまたがる50以上の遠隔研究施設をカバー

UTnetの歴史

- UTnet1(1990): 最初のキャンパスネットワーク
- UTnet2(1996): FDDIとATMが基本
- UTnet3(2001): Giga (Fast) Ethernetが基本
- UTnet3.5(2007)：基幹部の10G化
- UTnet3.5(2008)：本郷-駒場Ⅱのキャンパス間回線10G化

UTnet3の構成と運用

- UTnet の基本構成
  - 基幹部：部局や建物の接続、学外との接続
  - 支線部：建物内の接続
- 基幹部の運用は情報基盤センターによる
- 支線部の運用は当該部局による

UTnet3基幹部

- スター型トポロジー
- L3(Layer 3)スイッチ、L2(Layer 2)スイッチ
- 12箇所のハブサイトにL3スイッチを設置
- ハブサイト間は、10Gb/s(1～2Gb/s）で接続
- 部局・建物間は、100Mb/s、1Gb/s(10Gb/s)で接続
- キャンパス間は 100M、1Gb/s、10Gb/s で接続

学外との接続

- ＳＩＮＥＴ３（国立情報学研究所の運用による（Science Information network））
- WIDE (Widely Distributed Environment プロジェクトの運用による実験ネットワーク)

UTnet3支線部

- 各建物内のネットワーク
- 支線部と基幹部との接続用にL2スイッチを各建物に設置
- 各支線部の運用は当該部局（大学院・学部・研究所・センター等）

UTnet3の特徴

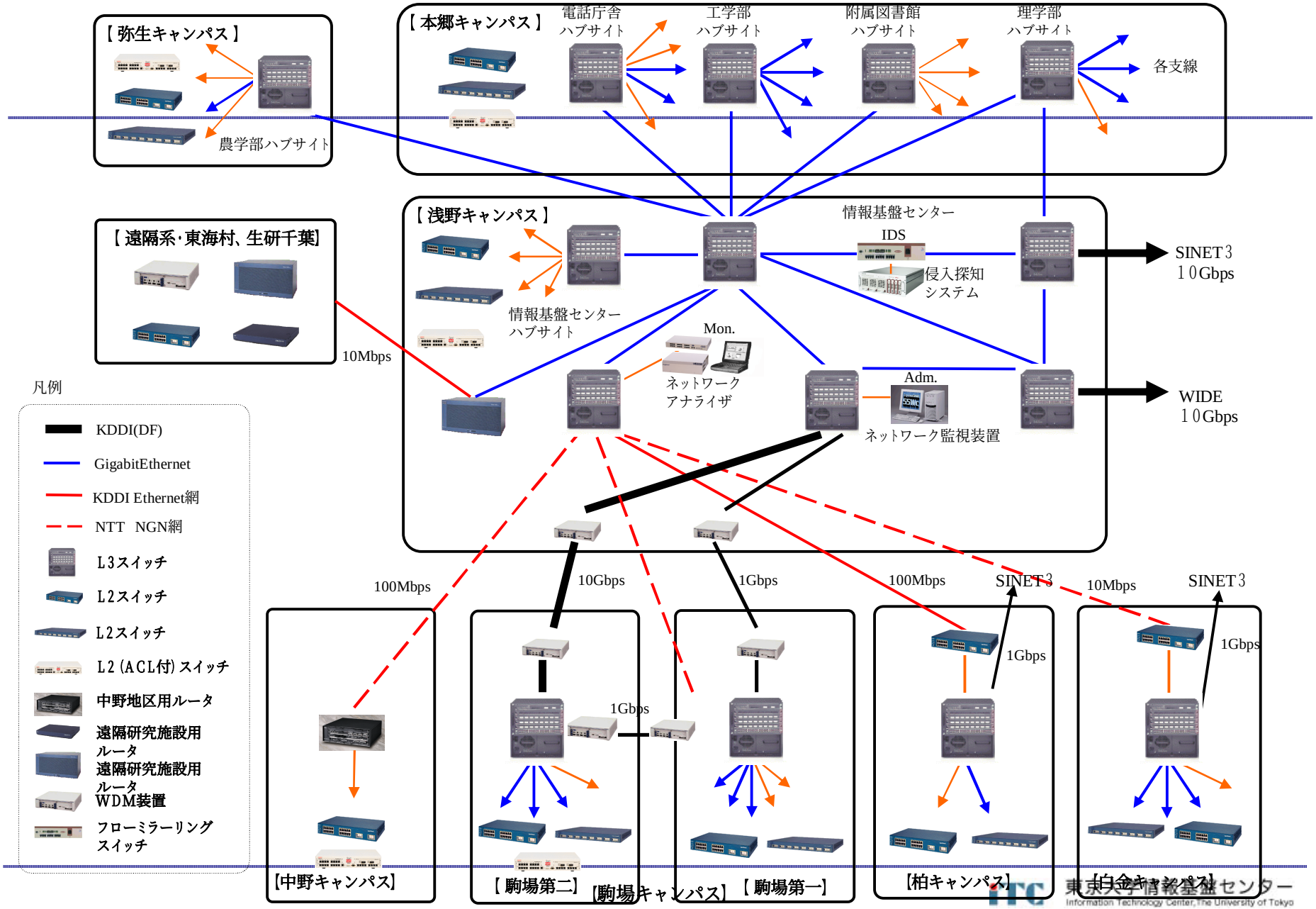
- 広帯域・高速伝送
  - 基幹部は １～１０Gb/s 規模
- VLAN (Virtual LAN)
  - 複数個所を同一論理ネットワークで
    カバーする仮想ネットワーク
- セキュリティ対策機能

UTnetの構成

- L3スイッチ　　15台
- L2スイッチ　210台
- VLAN　　601
- ポート　10Giga Ethernet　　3ポート
  Giga Ethernet　　162ポート
  Fast Ethernet　1，129ポート
- IPアドレス　109，347
  (大学全体では、／16×3　約19.7万アドレスを保有)

・光ケーブル　179区間　7，998芯

ネットワーク概念図



セキュリティ対策機能の必要性・留意点

- セキュリティインシデント
- 不正侵入・ウィルス感染等
- セキュリティ対策と利便性のバランス
- 部局による異なるセキュリティ要求条件
- 基幹部と支線部による取り組みの連携

UTnet3のセキュリティ対策

- 階層的フィルタリング
  - 学外との接続点におけるL3スイッチによるフィルタリング（全学共通対策）
  - 支線部におけるL4機能フィルタリング・ファイアウォール（部局個別対策）
- 学外との接続点における不正侵入検知システムIDS (Intrusion Detection System)
- 各コンピュータにおけるウィルス対策ソフトウェアの導入
- 遠隔セキュリティ診断（脆弱性の検知）
- セキュリティ脅威や広く使用されるソフトウェアの更新情報等の周知

階層的フィルタリング（１）

- 学外とのフィルタリング

sunrpc	TCP/UDP111
Ramenワーム	TCP515,TCP/UDP27374
Slammer	TCP1434
Sasser	TCP/UDP445
Blaster	TCP/UDP135,UDP137,UDP139

階層的フィルタリング（２）

- 学内におけるフィルタリング(ingressフィルタ)

  東京大学以外のIPアドレスを詐称したセキュリティインシデントが多くなってきたので、その予防措置として、基幹L3スイッチで、各支線ネットワーク（VLANごと）に、当該支線アドレスのみ通すフィルタを設定した。

公衆無線LAN（BBモバイルポイント）のゲートウェイ

- 既存の無線LAN設備に公衆無線ＬＡＮ（BBモバイルポイント）用のVLANを割り当てるので、新規に公衆無線LAN設備を導入した場合に懸念される電波の干渉等の無線LANの資源に関する管理が東京大学（各部局）側で行える。
- 学外者等が公衆無線ＬＡＮ（BBモバイルポイント）を利用することで、もし、何らかのセキュリティインシデント等が発生しても、東京大学のネットワークから発生したものと区別できる。
- 学外者等が公衆無線ＬＡＮ（BBモバイルポイント）を利用することで、IPアドレスによるアクセス制限をしている学内者専用のホームページや図書館でサービスしているデータベースへのアクセス制御が正しく行われる。

東大主要IPアドレス以外のサブネットアドレス割り当てについて

- 学会や会議、建物ロビーでの来訪者へのネットワークサービス等に従来から東大アドレスとして認知されている主要アドレスブロック(/16×3)以外のアドレスを用いることによって、学内からのみとしてのアクセスを許容しているサービスに対して、来訪者がアクセスするという事象を減らすことができる。

ウイルス対策ソフトウェア

ソフトウェア名	ライセンス数
ウイルスバスター2008	26,700
ウイルスバスター2008 (英語版; PC-cillin)	500
Server Protect for Windows NT	2,000
Server Protect for Linux	200
InterScan VirusWall エンタープライズエディション	サーバ台数無制限

ウイルス対策ソフトウェア

- Mac OS対応（Sophos Anti-Virus for Mac）
  Intel 版 Macにも対応

- Windows OS 多言語対応（Sophos Anti-Virus for Windows）
  日本語、英語、簡体中国語、繁体中国語、ドイツ語、
  フランス語、スペイン語、イタリア語

不正侵入検知システムIDS

・IntruShield 4000

Gigabit Ethernetモニタポート×4

Fast Ethernetレスポンスポート×2

Fast Ethernetマネジメントポート×1

ホットスワップ可能な冗長電源

最大2Gbpsのパフォーマンス

異常トラフィック監視システム

ソフトウェア
- 沖電気製　Secure Traffic Probe

- OS
  - Red Hat Enterprise Linux WS Version 3

- ハードウェア
  - Dell PowerEdge 1850
    2.8GHZ Intel Xeon
    メモリー1GB
    内臓HD　U320SCSI 146GB
    外付HD　TrusRAID 3U 500GBx16 SCSI SATA2
    Gigabit NIC x2 (1つマネージメントポート、1つモニターポートに使用)
    冗長化電源あり

東京大学のスパムメール対策の状況

メールサーバ数は、約７００台？
各部局（各メールサーバ）により、スパムメール対策はまちまち

- 迷惑メール対策装置を導入
- 迷惑メール対策のソフトウェアを導入
- 情報基盤センターのECCSメールホスティングを利用
- 何も行っていない

★全学的なスパムメール対策の検討

2007.10　製品の評価テスト
2008．２　製品の機種選定
2008．４　試行運用開始

製品の比較

製品	性能面 スパム判定 誤検知	機能面 隔離、マーク付、統計情報、ログ情報、ダイジェストメール、ユーザ単位のポリシー設定	運用面 ユーザ管理 ユーザ認証 二重化構成 障害対応	価格 本体 ライセンス料 保守料
A	×	△	×	×
B	○	△	△	×
D	○	○	△	×
E	○	○	△	△
F	○	○	△	△
マカフィー	○	○	△	○

試行運用システムについて

- スパム対策サーバ

  McAfee Secure Messaging Gateway

  SMG3400アプライアンス

  ユーザ数4，000、毎時100，000通

  スパム対策とウイルス対策の無制限ライセンス

  障害確認が15:00までの場合、翌営業日オンサイト対応

- 隔離サーバ

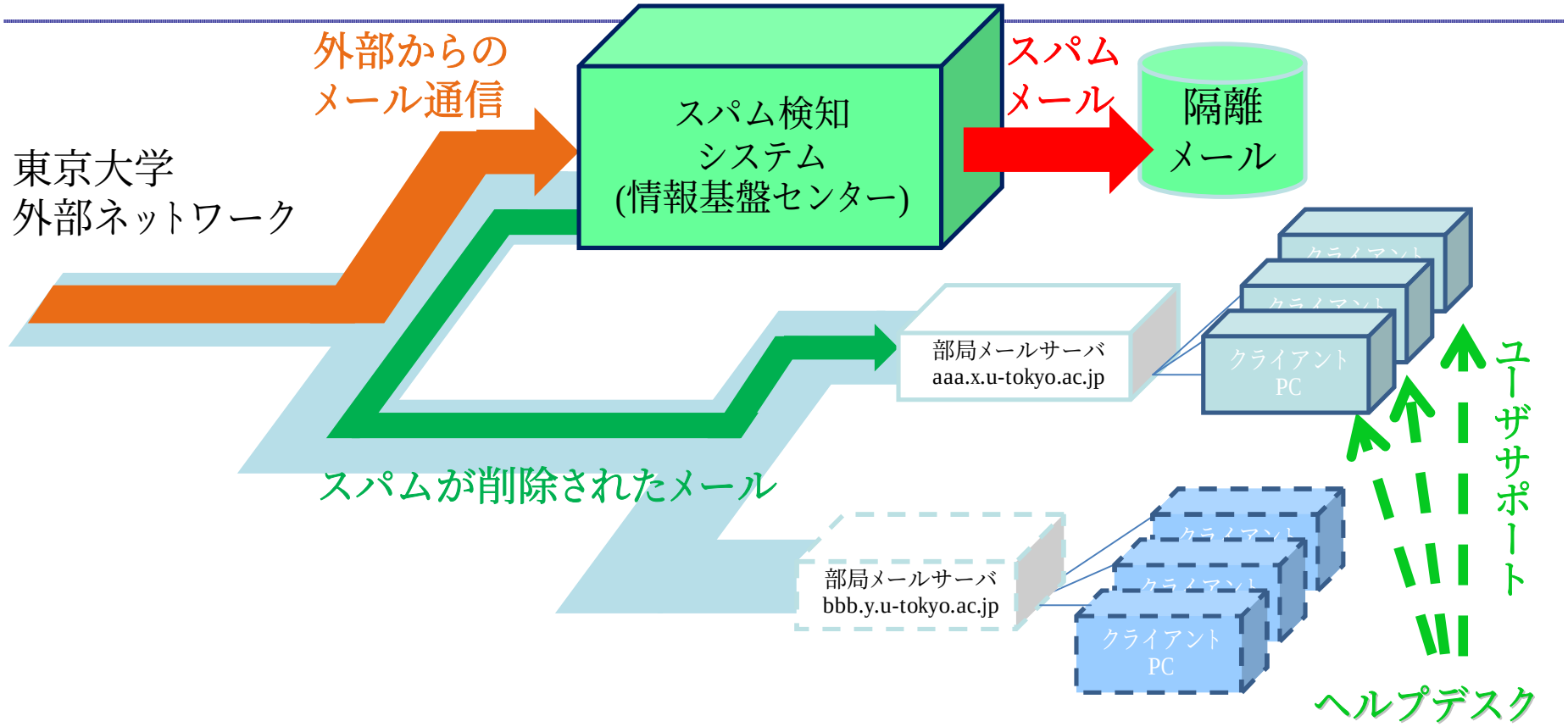
  Dell PowerEdge2950III

  CPU:デュアルコア Intel Xeonプロセッサー 2.33GHz

  メモリ:8GB

  ディスク:450GB RAID1

試行システムの概念図


外部からの
メール通信
東京大学
外部ネットワーク
スパム検知
システム
(情報基盤センター)
スパム
メール
隔離
メール
部局メールサーバ
aaa.x.u-tokyo.ac.jp
クライアント
PC
スパムが削除されたメール
部局メールサーバ
bbb.y.u-tokyo.ac.jp
クライアント
PC
ユーザサポート
ヘルプデスク

試行システムの運用（ポリシー）について（1）

- ドメイン（グループ）毎にポリシーを設定
  複数ドメインを同一ポリシーで設定可能
  受信メールのスコアにより、迷惑メールの判断を行う

- 受信メールのスコアによる迷惑メールの処理
  迷惑メールと判断された受信メールサブジェクトへの文字列付加
  迷惑メールと判断された受信メールの隔離（約1ヶ月保存）
  迷惑メールと判断された受信メールの削除

受信メールのスコアによる迷惑メール処理の
組み合わせ可能

試行システムの運用（ポリシー）について（2）

- フィッシングメールの処理

  フィッシングメールの隔離（約1ヶ月保存）
- ブラックリスト、ホワイトリストの設定

  管理者がドメイン（グループ）毎に設定可能

  ユーザが個別に設定可能

試行システムの利用状況

- 7部局、22ドメイン、約3,500メールアカウント
- スパム判定：点数累積方式
- スパムメール処理：マーク、隔離、転送、削除
- 処理の選択：点数でのしきい値で処理を選択
- テスト環境（転送先を試行システムに向ける）
- 試行運用までの流れ

  ①マーク付けで、点数の分布を調査（1週間～1ヶ月）

  ②隔離する点数を決める。しきい値は、2つ設定できる。

試行システムの今後の課題について

- メールアカウント数、受信メール総数、スパムメール数等が、どのくらいまで処理できるか、手探り状態。
- 二重化構成の運用を今年度中に構築予定。
- 他社製品の動向調査。

東京大学の情報関連の体制の概要

- 最高セキュリティ責任者
  (CISO：Chief Infomation Security Officer)
  -情報公開委員会
  -情報セキュリティ委員会
  -情報倫理委員会

- 最高情報責任者
  (CIO：Chief Infomation Officer)
  -情報システム委員会
  -情報システム本部
  -東京大学情報システム緊急対応チーム (UT-CERT)

結び

- 東京大学：http://www.u-tokyo.ac.jp/
- 情報基盤センター：http://www.itc.u-tokyo.ac.jp/
  http://www.nc.u-tokyo.ac.jp/
- UT-CERT：http://park.itc.u-tokyo.ac.jp/ut-cert/
- 情報倫理委員会：http://www.cie.u-kyo.ac.jp/index.html