移行期にあるネットワークサービスのセキュリティ

WG 報告

只木進一（佐賀大学）

はじめに：WGの問題意識

- 情報システムを巡る環境の変化
  - 多様化する利用形態
  - 肥大化する情報システム
  - 情報システムにかかるコスト増
  - 技術者の圧倒的不足

はじめに：WGの問題意識

- 高等教育機関を巡る環境
  - 情報システムに求められる質
    - 可用性、信頼性
  - 情報システムへの投資は増えない
  - 管理組織とシステム要求の不整合
- クラウド利用は避けられない？

はじめに：WGの問題意識

- ネットワーク環境の変化
  - 一人一台を超えた状況
  - パーソナルデバイスもIP接続
  - IPv4アドレスの枯渇
    - JPNICレベル
    - 組織内レベル
- IPv6対応機種は当たり前

移行期のセキュリティ

- 攻撃への防御というセキュリティも大切だが
- 基盤のセキュリティの見直しも必要ではないの？
  - クラウドは使える？
  - IPv6がバックドアになっていない？

WG概要：メンバー

- 会員

  西村(広島)、吉田(大分)、笠原(九州)、
  武蔵(熊本)、鈴木聡(KEK)、長谷川(中京)、
  鈴木常(中京)、藤本(東京電機)、
  藤村(福岡)、山守(三重)、只木 (佐賀)

- 富士通

  吉田、須永、山下、山路、石川、田口

WG活動概要

- 活動期間
  - 2012/8 – 2014/7
- 前半のテーマ
  - パブリッククラウド利用のセキュリティ上のポイント
- 後半のテーマ
  - IPv6導入のセキュリティ上のポイント

パブリッククラウド利用のセキュリティ上のポイント

パブリッククラウド利用のセキュリティ上のポイント

- 質問１：あなたの組織はクラウドサービスを利用していますか？
  1. 利用している
  2. 利用していない
  3. わからない

パブリッククラウド利用のセキュリティ上のポイント

- 質問２：クラウド利用の上で重視することは
  1. コスト
  2. 安定性
  3. 機密性（情報漏洩の危険性）
  4. わからない

クラウドサービスの現状
教育機関が組織的に利用できるもの

- 無償の汎用的サービス
  - Google Apps for Education
  - Microsoft Office365
- どうして無償なんだろう？
  - コンテンツの所有権は？
  - 突然、サービスが無くなる可能性は？

クラウドサービスの現状
教育機関が組織的に利用できるもの

- その他
  - Amazon AWS
  - Microsoft Azure
  - さくらインターネット
  - サイボーズ
- 利便性とコスト、セキュリティ

クラウドのトラブル事例

- データ喪失
- 移行トラブル
- サービス内容の急な変更
- アカウント乗っ取り

- 懸念
  - 機密性
  - 可用性

クラウド利用上のセキュリティ以外の課題

- 多数の利用者向けサービスであることから来る課題
- サービス内容の変更の可能性
  - 機能強化、インターフェイス変更
  - 有償化
- セキュリティポリシー変更
- 係争時の課題
- データセンターの場所

文書の重要度

- 組織の文書の重要度を定めるのが先決
  - 例えば4段階

重要度	取り扱い	例
重要度iV	関係者限定	個人情報
重要度III	特定部署限定	学生指導状況、仕様書、システム情報
重要度II	取り扱い注意	業務連絡、内規
重要度I	公開	広報、募集要項

サービスの信頼度

- 独立性
  - ハードウェア、OS、データ、サービス
- アクセス制限
- アクセス経路の安全
- データの暗号化
- サービス可用性

留意点

- サービスの質
  - SLA、保守
  - 問い合わせ、サービス継続
- 機能
  - ネットワーク、管理ツール
  - 保有しているライセンスが対応するか

留意点

- コスト
  - 導入時のコスト
  - 何に課金させるか
- データセンター
  - 物理的セキュリティ
  - 設置場所（国内？海外？）
- 契約内容

例：Office 365

- 認証
  - クラウド認証：ローカルと同期可能
  - ADFS連携
- データの置き場所
  - 2014年末から国内に
  - データ独立性？
- 訴訟
  - 日本の法律、東京地裁

例：Google Apps

- 認証
  - ADFS連携
- データの置き場所
  - 不明
  - 指定も可能だが有償？
- 訴訟
  - カリフォルニア州法、カリフォルニア州サンタクララ郡裁判所

クラウドサービス利用ガイドライン：チェックリスト

- サービスを利用しようとする者（担当事務など）が自分で確認する
- 自分でチェックすることで、サービスの質と期待しているサービスとの整合性を確認
- 自組織の文書管理規則類との整合性
- 広島大学の例を参考に

IPv6導入のセキュリティ上のポイント

IPv6導入のセキュリティ上のポイント

- 質問3：あなたの組織はIPv6を利用していますか？
  1. 利用している
  2. 利用していない
  3. わからない

IPv4アドレス枯渇

- 2011年、アジア太平洋地域のIPv4アドレス枯渇
  - 後発組織は、アドレスがほとんど無い
  - データセンター等で深刻？
- IPv4の次はIPv6？
  - 実際に使われているのか？

機材はIPv6レディですが

- 使っている情報機材の多くはIPv6が使える
  - クライアントPCはデフォルトで使用可
  - 何とかしてIPv6通信を行おうとするモノも居る
- 管理者が知らないうちに、組織ネットワークにIPv6ネットワークが侵入する？

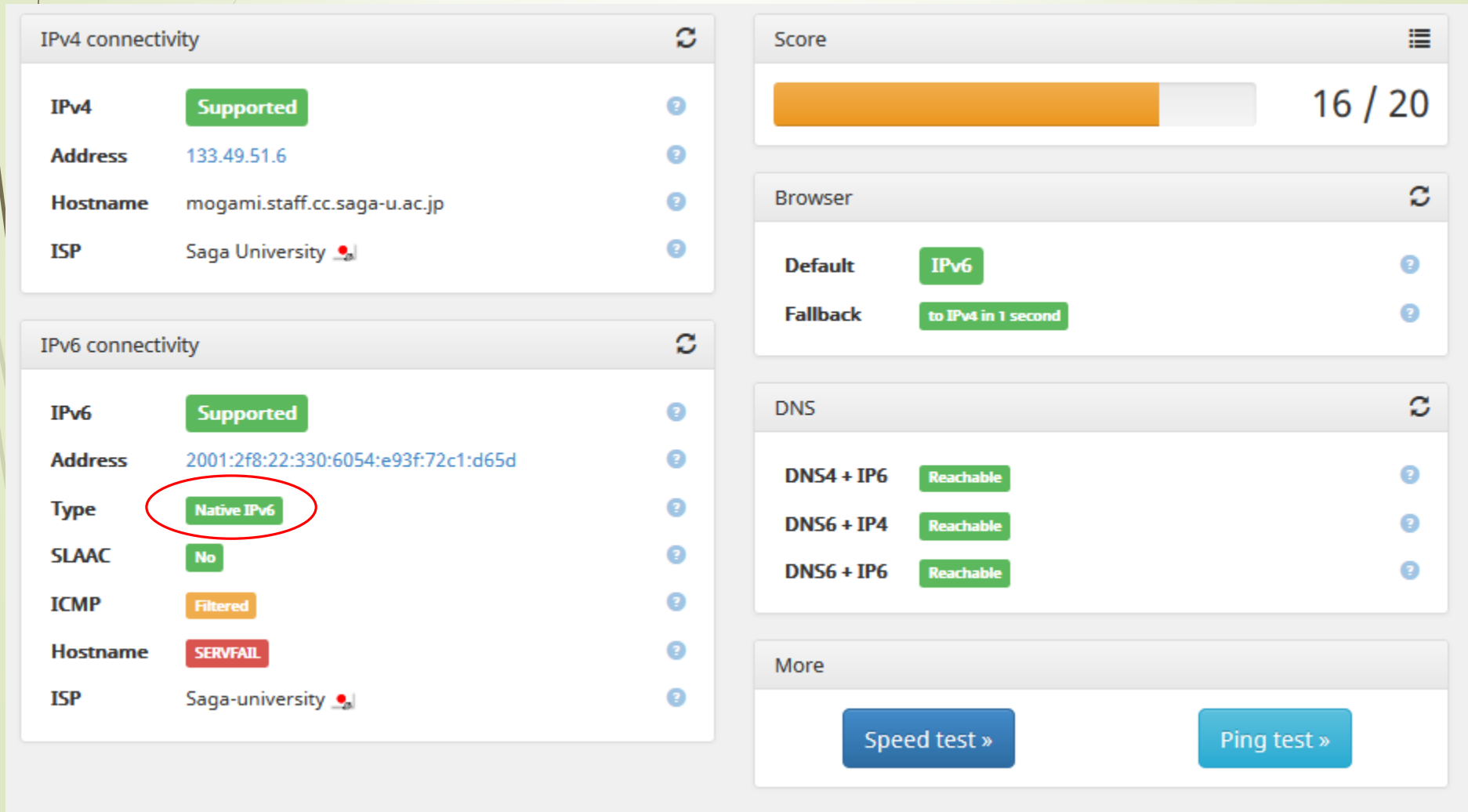
IPv6ではアドレス自動設定が基本

- IPv6アドレスは128ビット
  - 長すぎて、手動設定は実質的に無理
- 自動設定が基本
- PCは、RA (Router Advertisement)が流れていれば、IPv6アドレスを自動設定する。

- 自分の組織はIPv6を使っていない。従ってRAも流さない。つまり、PCがIPv6アドレスをとることは無い！

間違い

IPv6通信可能性の確認
http://www.ipv6-test.com/



IPv4	Supported
Address	133.49.31.124
Hostname	escape.ai.is.saga-u.ac.jp
ISP	Saga University

IPv6 connectivity

IPv6	Not supported
Address	
Type	
SLAAC	
ICMP	
Hostname	
ISP	

4 / 20

Browser

Default	IPv4
Fallback	No

DNS

DNS4 + IP6	Unreachable
DNS6 + IP4	Reachable
DNS6 + IP6	Unreachable

More

Speed test »

Ping test »

WindowsクライアントはIPv6を話したい

- IPv4しかサービスしていないネットワークに接続したWindowsクライアント
- 6to4またはteredoを使って、IPv6到達性を試す
  - FWをトンネルすることに注意
  - NAT配下でもteredoでトンネルされる

RAを流されると

- クライアントがRAを流す事例がある
- 管理者が知らないIPv6ネットワークを構成
- FWをトンネルして外と接続

トンネルの抑制

- FWでアプリケーションとして抑制
  - 6to4やteredoをアプリケーションとして認識できるFW装置の場合
- プロトコル番号やポート番号での抑制
- 6to4やteredoのサーバへのアクセス抑制

トンネルの抑制が必要なのは

- IPv6をサービスしている組織
  - IPv4のみのサブネットやIPv4プライベートネットワークからのトンネル
- IPv4のみのサービスをしている組織

IPv6との付き合い方

- DNSでのIPv4とIPv6の混在が、問題を複雑にしている
  - IPv4接続可能性の保持が必須
- 並行運用の可能性
  - サーバ類だけデュアルスタック
  - クライアント類向けIPv6シングルスタックの可能性

FW設定への留意点

- トンネルの抑制
- 無駄な問い合わせの抑制
- 偽装パケットの抑制