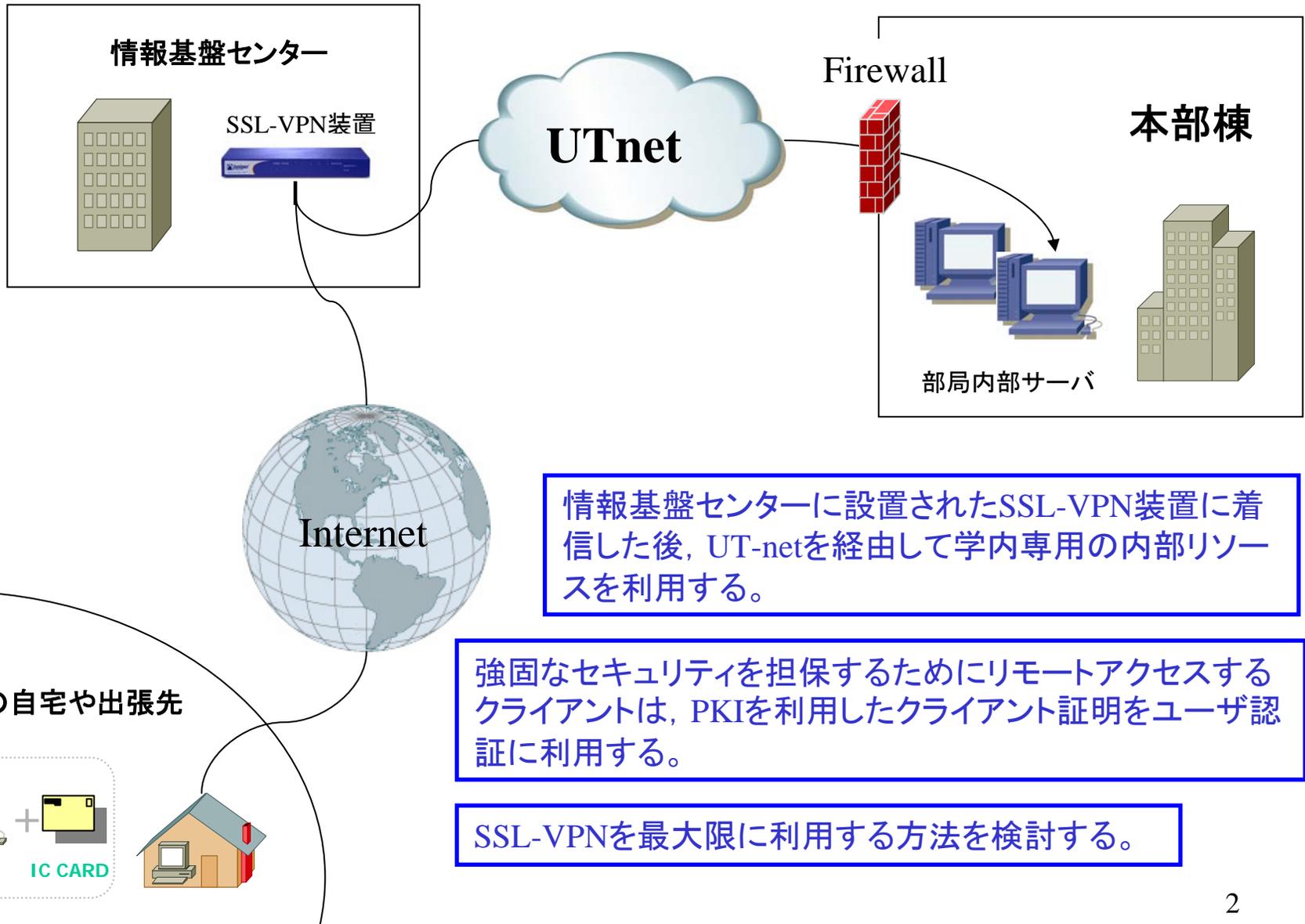


# SSL-VPN実証実験について

総務部情報課 開発チーム

夏目典大

# SSL-VPN実証実験の概要

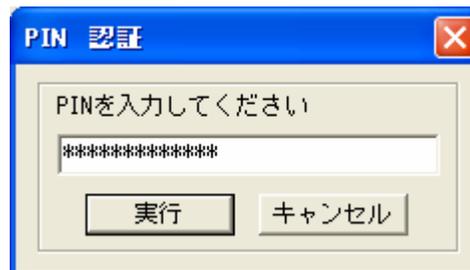


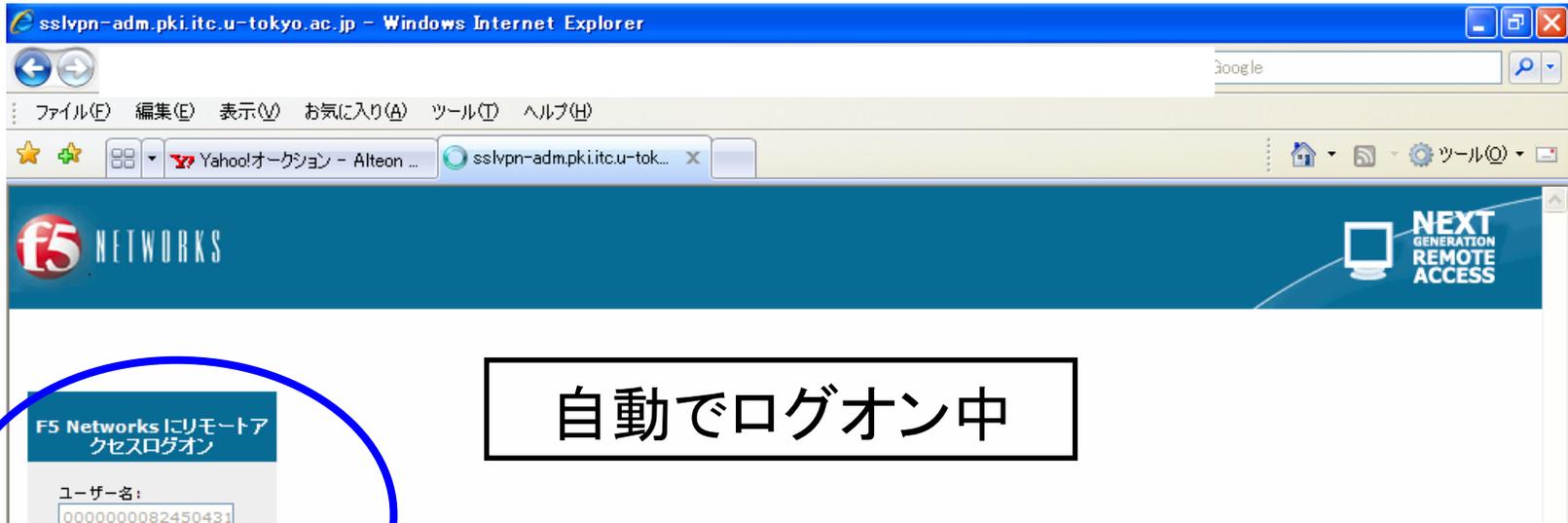
# SSL-VPNの利用

- ①ICカードリーダーにUT-CA発行のICカードを挿入する。
- ②Webブラウザを立ち上げる。
- ③https://からはじまるSSL-VPN装置のURLを入力する。



- ④PINコード入力ボックスが表示されるので、ICカードのPINコードを入力します。





自動でログオン中



SSL証明書を利用したログインではパス入力抜きで自動ログオンすることが可能

# SSL-VPN装置のポータル画面

ターミナルサーバ

- TSV\_TEST

Webアプリケーション

- 本部ウェブメール
- 本部グループウェア
- 経費精算システム
- 東京大学ホーム

信頼済みサイト 100%

管理者によって予め許可された内部イントラネットサーバのみを表示させ、利用させることが可能

内部リソースへのアクセス制御が可能

# SSL-VPN実験検証の内容

- (検証1) 東京大学の学内専用ホームページを見よう！
- (検証2) 部局内WEBメールサーバやグループウェア,  
業務アプリケーションを使ってみよう！
- (検証3) 「ターミナルサーバ」アクセスを使ってみよう！
- (番外編) クライアント・サーバ方式のアプリケーション  
を安全に利用してみたい！（IPSec-VPNのように）

NATSUME NORIHIRO ホーム - Windows Internet Explorer

Google

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

NATSUME NORIHIRO ホーム

f5 NETWORKS FirePass

NATSUME NORIHIRO ホーム Eng ログアウト

ターミナルサーバ

- TSV\_TEST

Webアプリケーション

- 本部ウェブメール
- 本部グループウェア
- 経費精算システム
- 東京大学ホーム

ツール

クリックする

(検証1)

東京大学の学内専用ホームページを見よう!

信頼済みサイト 100%

# 東京大学ホームページが表示されるので そこから学内専用ページを開くと...



[大学のホームページ](#) > [教職員のみなさまへ](#)

## 教職員のみなさまへ(学内専用ホームページ)

### お知らせ

- [東京大学規則集\(学内専用\)](#)(07.02.18現在)(注:[学外者向けページ](#)は04.5.20現在です。)
- [事務機構改革に係る提案募集](#)(07.02.06)
- [アクション・プラン全学説明会開催](#)(本郷キャンパス07.01.23、駒場キャンパス07.01.31)
- [職員ミッション「私の職場は東京大学」](#)
  - [東京大学職員ミッション、ミッション実現のための「東京大学職員7ヶ条」](#)
- [東京大学目安箱](#)(06.07.05)
- [研究協力課公募情報ホームページ](#)
- [喫煙対策ワーキンググループ\(WG\)の発足と「喫煙意見箱」の設置について](#)(06.12.07)
- [本郷構内の自転車・バイクの利用について](#)(07.03.30)
- [「早期退職制度ホームページ」の開設](#)(06.10.12)

学外からでも問題なく学内専用ページにアクセスできました

管理者が許可した以外のサイトにアクセスしようとする...

## セキュリティ例外

<http://www.itc.u-tokyo.ac.jp/> へのアクセスは拒否されます。

理由: 管理者がこのURLへのアクセスを許可していません。

「セキュリティ例外」としてアクセスすることができない

**踏み台行為による不正中継アクセスを防止**

NATSUME NORIHIRO ホーム - Windows Internet Explorer

Google

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

NATSUME NORIHIRO ホーム

f5 NETWORKS FirePass

NATSUME NORIHIRO ホーム Eng ログアウト

ターミナルサーバ

- TSV\_TEST

Webアプリケーション

- 本部ウェブメール
- 本部グループウェア
- 経費精算システム
- 東京大学ホーム

クリックする

(検証2)

部局内のWebメールサーバやグループウェア、  
業務アプリケーションを使ってみよう！

信頼済みサイト 100%

# WEBメールの場合(1)

The screenshot shows a webmail interface for 'DEEP Mail'. The main content area displays an '受信トレイ' (Inbox) with a list of emails. The interface includes a left sidebar for folder management, a top navigation bar with 'メールホーム', 'SPAM設定', and 'オプション', and a bottom status bar. A text box is overlaid on the screenshot with the text '通常通りにWebメールにアクセスできている様子'.

選択	区分	件名	添付	送信者	Date	サイズ
<input type="checkbox"/>		LONG AND SHORT TERMS LOAN OFFER REPLY I..		jasonsmith@hawaii.rr.com	2007/04/26 01:07	3.29 KB
<input type="checkbox"/>		Photoshop, Windows, Office		Mathew Carter <mylenefarmeretvovus.net@wa...>	情報なし	2.83 KB
<input type="checkbox"/>		Top listed medications 4 you		Margery Burkett <dwmmamurianm@mamurian.co...>	2007/04/25 16:54	4.22 KB
<input type="checkbox"/>		From Angela Kabaka For God's Work		ANGELA KABAKA <angela.kabaka44@yahoo.fr...>	2007/04/25 22:47	1.49 KB
<input type="checkbox"/>		Spam List [2007/04/25]		postmaster@adm.u-tokyo.ac.jp	2007/04/26 00:30	2.24 KB
<input type="checkbox"/>		Whats up		Jack Roberts <tollanad@tpn.nl>	2007/04/26 00:17	17.59 KB
<input type="checkbox"/>		FROM THE DESK OF MR MOHAMED YAYA.		<mohamed.yaya431@hotmail.co...>	2007/04/26 00:17	17.59 KB
<input type="checkbox"/>		Any idea		Newman Mel <tooleghg@growtalent.com>	2007/04/26 00:40	2.26 KB
<input type="checkbox"/>		Business Relationship		Jack Azfar <dr_jack_azfar@mailvault.com>	2007/04/25 16:38	1.97 KB
<input type="checkbox"/>		Obesity is dangerous, stop it		Antoine Villarreal <laxcshczsvew@cshczs...>	2007/04/26 00:38	5.40 KB



# WEBメールの場合(3)

The screenshot shows the DEEPMail webmail interface. The left sidebar contains a folder management section with the following items: 受信トレイ (289/1927), 送信トレイ (0/0), 送信済み (0/416), 下書き (0/0), 予約送信 (0/0), 削除済み (616/670), and SPAM (37/37). The main content area shows the '受信トレイ' (Inbox) with buttons for '選択削除' (Select Delete), 'リスト印刷' (Print List), and '受信拒否' (Reject). Below these buttons, there is a dropdown menu for '選択したメールを' (Selected emails) set to '送信済み' (Sent) and a '> 移動' (Move) button. A table with columns '選択' (Select), '区分' (Category), and '件名' (Subject) is visible, but it is empty. A blue speech bubble is overlaid on the right side of the interface, containing the text: 'WEBアプリケーションの事前検証は必須ですね。' (Pre-verification of web applications is necessary, isn't it?). At the bottom of the browser window, a yellow warning icon is present with the text: 'ページでエラーが発生しました。' (An error occurred on the page.).

WEBアプリケーションの事前検証は必須ですね。

エラー発生メールまで選択削除をしたら画面に何も表示されなくなりました。

# WEBメールの場合(4)

メール作成

フォルダ管理 [GO]

- 受信トレイ (315/1969)
- 送信トレイ (0/0)
- 送信済み (0/421)
- 下書き (0/0)
- 予約送信 (0/0)
- 削除済み (703/765)
- SPAM (45/45)

住所録  
開封確認  
ゴミ箱を空に

メールホーム SPAM設定 オプション

- \* 新たに導入されたWeb技術と業界屈指のデータベースが、迅速で正確な検索結果をご提供します
- \* バグのアーカイブのみでなく、最新のバグもより正確に検索できます
- \* Ciscoの変化や、ユーザのニーズ・条件などに柔軟に対応できるデータアーキテクチャです

さらに、新しいBug ToolkitはCisco製品とソフトウェアのバージョンを自動的に追加されますので、重要なバグ情報により早くアクセスが可能となりました。

ツールの利用状況とバグのヒット・データはすべて記録され、この情報に基づいてバグの文書化や未公開バグの公開などが決定されます。Ciscoのバグオーナーもこの情報を元にバグ修正の優先順位を決めますので、ユーザの皆様への影響も非常に大きいと言えます。

さっそく下記のリンクから新しくなったBug Toolkitを試して、その違いを実感して下さい！

<http://tools.cisco.com/Support/BugToolKit/>  
(\* サービス契約のある登録カスタマーを対象といたします)

まだ、Cisco.comに登録していらっしゃいませんか？  
下記のURLからカスタマー登録をし、Ciscoのツールと情報をご利用ください。

<http://tools.cisco.com/RPF/register/register.do>

例えばこのようにURLを記載したメールが来たとします。

この例では悪意のメールだと仮定してみましよう。

クリック

信頼済みサイト 100%

# WEBメールの場合(5)

メール作成

セキュリティ例外

<http://tools.cisco.com/Support/BugToolKit/> へのアクセスは拒否されます。

理由: 管理者がこのURLへのアクセスを許可していません。

このように許可外のドメインへの遷移は不許可にしてくれます。

こういう機能はphishing対策としても良いですね。

ページが表示されました

信頼済みサイト 100%

# GroupWareの場合(1)

The screenshot shows a web browser window displaying a GroupWare interface. The browser's address bar shows "Webアプリケーション". The page header includes the "f5 NETWORKS" logo and "FirePass" branding. The user's name "NATSUME NORIHIRO ホーム : Webアプリケーション" is visible in the top right. The main content area features a navigation menu on the left with items like "TOP", "スケジュール", "ToDo", "伝言・所在", "設備予約", "回覧板", "アドレス帳", "電子会議", "文書管理", "プロジェクト管理", "備品管理", and "アンケート". The central "スケジュール" (Schedule) section shows a calendar for April 10-16, 2007, with events like "EAS: 月次処理" and "MAC対応システム運用開始". Below the calendar is a "伝言・所在" (Message/Location) section with the text "新着伝言はありません。". A blue box with white text is overlaid on the bottom of the page, stating "正常に画面が表示できている状態". The browser's status bar at the bottom shows "ページが表示されました" and "信頼済みサイト".

正常に画面が表示できている状態

# GroupWareの場合(2)

2007年04月09日 00:10

東京大学 THE UNIVERSITY OF TOKYO

メニュー

- TOP
- スケジュール
- ToDo
- 伝言・所在
- 設備予約
- 回覧板
- アドレス帳
- 電子
- 文書
- プロ
- 備品

1	2	3	4	5	6
8	9	10	11	12	13
15	16	17	18	19	20
22	23	24	25	26	27
29	30	1	2	3	4

文字化けが発生したり、ページが一部くずれてしまっている。

# 業務アプリケーションの場合

Logout END

パスワード変更  
メンテナンス  
実行予定JOB一覧  
ロック状況確認・解除

©案件検索  
一般検索

©カードデータ検索  
未精算データ  
請求データ

Ž ¼	f)Xf^ŠÇ— Ž
•” ¼	
•” <Ç	Ž—±ç

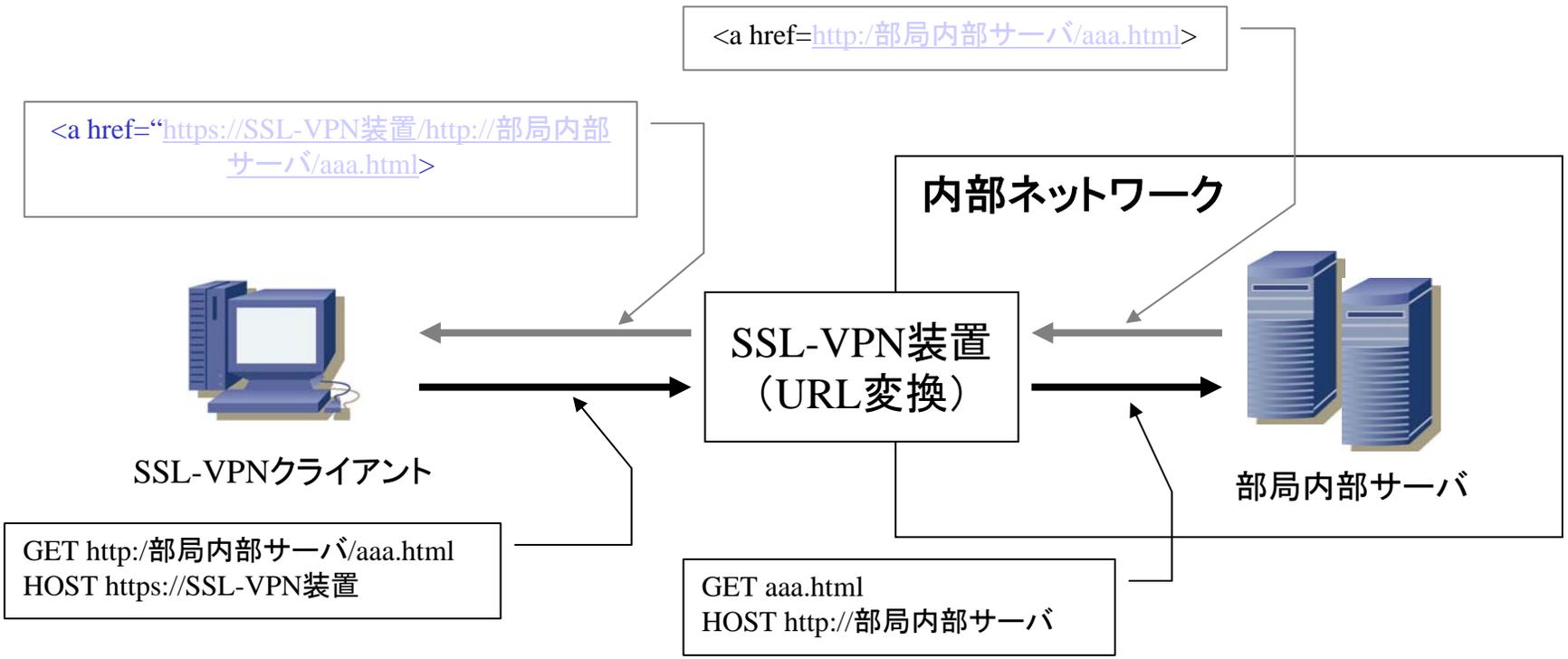
ŠÇ— ŽÖ,©,ç,i,f ƒbƒZl [fW

...)16žž,É,È,è,Û, B 4CEž,İ+0 Ø\*ú,4CEž11\*ú( ...)16žž,É,È,è,Û, B 4CEž,İ+0 Ø\*ú

Copyright (c) 2004 Hitachi High-Tech Solutions Corporation All rights reserved.

お馴染みの経費精算システムにおいても、一部文字化けが発生しました。

# リバースプロキシ方式SSL-VPNの概念図(例)



SSL-VPNクライアントから部局内部サーバへのリクエストや、逆にサーバからクライアントへのレスポンスメッセージは、SSL-VPN装置がURLを書き換えることによって交換している。

## リバースプロキシ方式SSL-VPNでのトラブル例

- ・日本語EUCコードを使用したアプリケーションと日本語JISコードを使用したアプリケーションに同時にアクセスをした場合
  - Webブラウザが文字コードを誤識別することにより文字化けが発生する可能性
- ・JavaアプレットやFlash等が内部ネットワークのサーバに直接的にアクセスするリンクを生成する場合
  - リバースプロキシにおいて必要なページ内リンクの変換を行うことができない。 など

NATSUME NORIHIRO ホーム - Windows Internet Explorer

Google

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

NATSUME NORIHIRO ホーム

f5 NETWORKS FirePass

NATSUME NORIHIRO ホーム Eng ログアウト

ターミナルサーバ

TSV\_TEST

Webアプリケーション

- 本部ウェブメール
- 本部グループウェア
- 経費精算システム
- 東京大学ホーム

ツール

(検証3)

「ターミナルサーバ」アクセスを利用してみよう!

信頼済みサイト 100%

**A new browser component is available.**

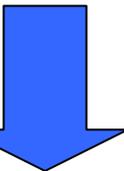
Please click on the Information Bar above if it is displayed, and choose Install ActiveX control.

If your browser security settings prevent the installation, please select an option below.

- [Install new browser component](#)
- [Do not install new browser component](#)

新規にターミナルアクセスを行う際にはActiveXコンポーネントのインストールが必要になります。

① Install. . . を押すと

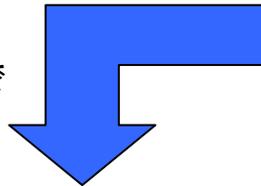


**Component installation.**

- [Download and run installation package](#)

Select "Run" when prompted for action.

② ActiveXコンポーネントがダウンロードされるので



③ 実行する。

無事にインストールできるとターミナルアクセスが利用できるようになる

F5アプリケーションアクセス - Windows Internet Explorer

TSV\_TEST 800 \* 600

Windows ログイン

Microsoft  
**Windows Server 2003 R2**  
Standard Edition

Copyright © 2005 Microsoft Corporation

Microsoft

ユーザー名(U):

パスワード(P):

OK キャンセル オプション(O) >>

これで休みの日でも  
自宅で仕事や研究が  
はかどりそう？

学内専用のターミナルサーバにアクセスすることが可能になりました。

A 般

F5アプリケーションアクセス - Windows Internet Explorer

TSV\_TEST 800 \* 600 閉じる

マイ コンピュータ MegaRAID StartupUI

マイ ネットワーク ns50\_070307

ごみ箱 Server Protected Management Console

Internet Explorer UTF-8 TeraTerm Pro

desktop.ini 統合ビューア

APC Power Chute

東京大学[ホーム] - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り リンク

アドレス(D) http://www.u-tokyo.ac.jp/index\_j.html 移動

東京大学ウェブサイトを表示するにはJavaScriptが必要です。  
ブラウザの設定をオンにしてからページをリロードしてください。

 **東京大学**  
THE UNIVERSITY OF TOKYO

[ENGLISH](#) | [サイトマップ](#)

[受験生の方](#) | [社会人・一般の方](#)

東京大学案内 | 学部・大学院・研究所・センター | 東京大学の活動 | 東京大学入学案内

  
THE UNIVERSITY OF TOKYO 130<sup>th</sup>  
創立130周年  
記念事業



ログイン後は自分のデスクトップのように、色々と利用することが可能です。

スタート | 東京大学[ホーム] - M... | 0:06

F5アプリケーションアクセス - Windows Internet Explorer

TSV\_TEST 800 \* 600

コマンド プロンプト

TCP	0.0.0.0:2260	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3052	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3628	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5005	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5168	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5169	0.0.0.0:0	LISTENING

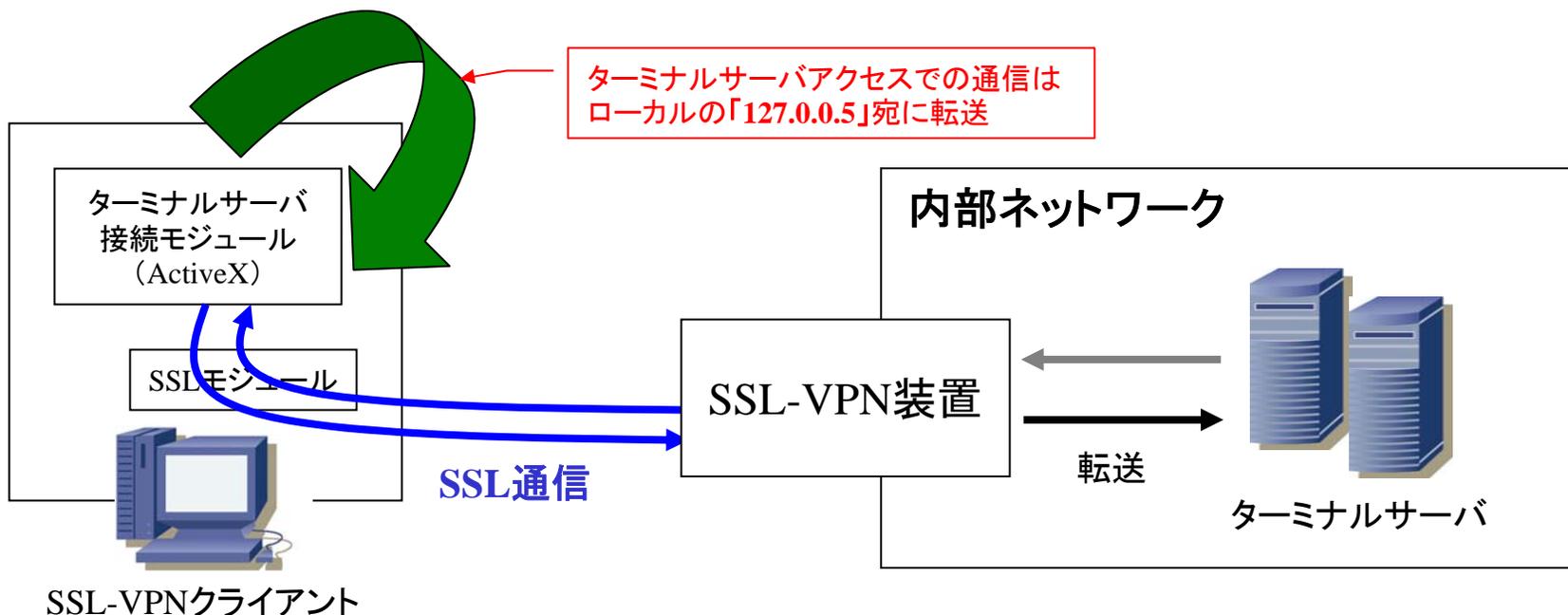
接続は SSL-VPN装置 ⇔ ターミナルサーバ

TCP	0.0.0.0:49258	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1038	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8807	0.0.0.0:0	LISTENING
TCP	127.0.0.1:10330	0.0.0.0:0	LISTENING
TCP	[redacted]:16.2:1027	[redacted]:16.2:2161	ESTABLISHED
TCP	[redacted]:16.2:2161	[redacted]:16.2:1027	ESTABLISHED
TCP	[redacted]:16.2:3389	[redacted]:04.42:60593	ESTABLISHED
UDP	0.0.0.0:161	*:*	
UDP	0.0.0.0:162	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	

C:\Documents and Settings\tsadmin>

スタート | コマンド プロンプト | 0:07

# ポートフォワード方式SSL-VPNの概念図(例)



ターミナルサーバアクセスの通信は、(今回の実証実験では)「127.0.0.5」に転送される。その後、通信はSSLモジュールによってSSL暗号化されSSL-VPN装置に送信される。SSL-VPN装置ではこの通信を内部ターミナルサーバに転送する。

ActiveX(実装によっては、Javaアプレット)をインストールしなくてはならないためクライアント側では管理者権限が必要となる。

NATSUME NORIHIRO ホーム - Windows Internet Explorer

Google

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

NATSUME NORIHIRO ホーム

f5 NETWORKS FirePass

NATSUME NORIHIRO ホーム Eng ログアウト

ターミナルサーバ

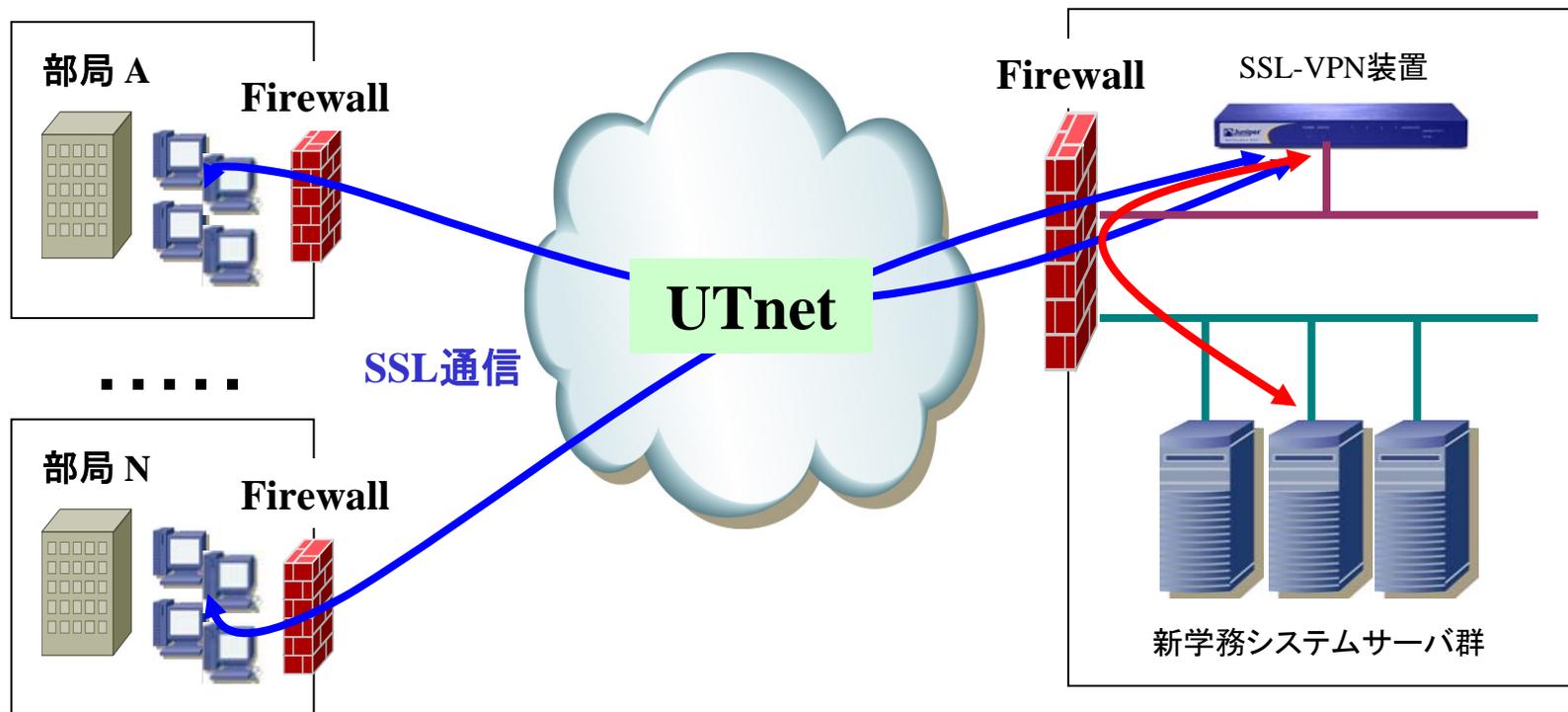
(番外編)

クライアント・サーバ方式のアプリケーション  
を利用してみたい！(IPSec-VPNのように)

本編は、実証実験とは別ですが、SSL-VPN利用の一事例  
として実際の導入事例をご紹介します。

信頼済みサイト 100%

# 新学務システムのネットワークアクセス利用例



## (必要条件)

- 各部局では、ネットワーク境界にFirewallを設置している可能性が高い。
- クライアント・サーバ方式のアプリケーションでOracle通信を利用している。
- 他プロトコルを利用する可能性(SMBなど)も将来無きにしもあらず。
- 学務データは最重要なものなので、盗聴や改ざん、なりすましによる情報詐取を防止できなければならない。

F5: FirePass AdvTest's Home - Windows Internet Explorer

Google

F5: FirePass AdvTest's Home

https://utaasgw.adm.u-tokyo.ac.j...

サマリー ネットワークアクセス セットアップ

東京大学 学務システム 終了

状況: ネットワークアクセス接続が確立されました

ページ インターネット

FirePass AdvTest's Home

Terminal Servers

- Terminal Server 77
- VNC Server
- Terminal Server 100
- 172.17.1.77

Tools

Network Access

- VPN connection

Web Applications

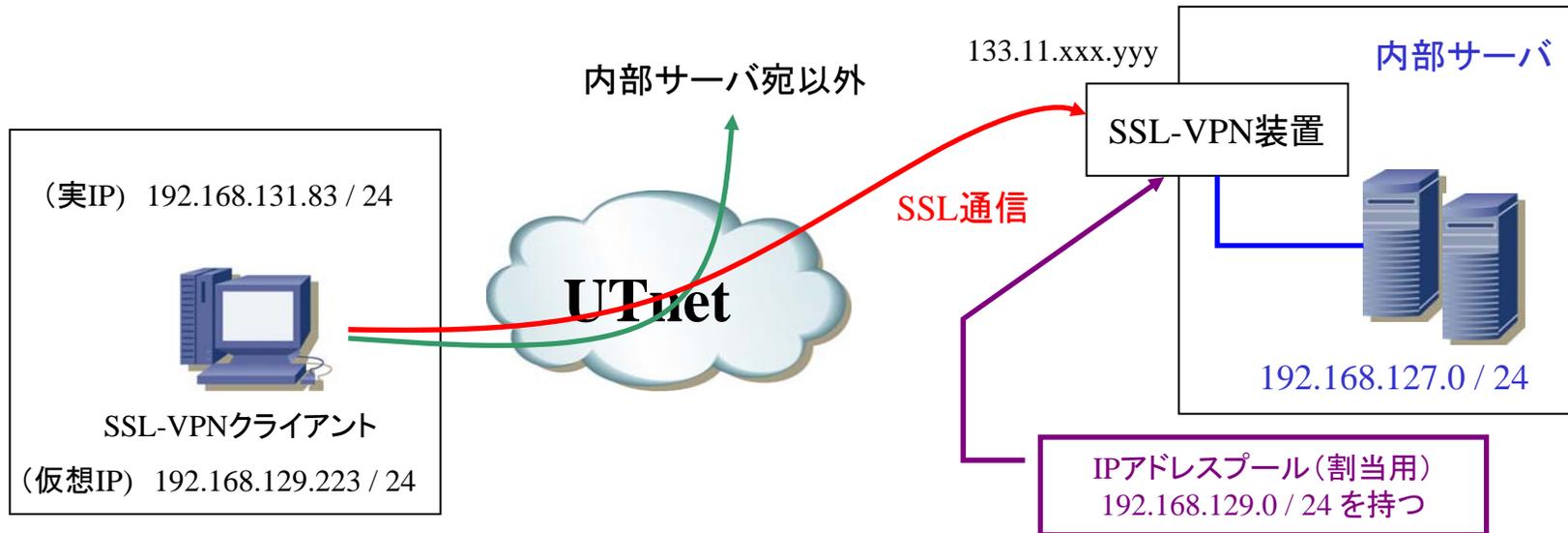
- Scalix\_WebMail
- Google

Logout

ネットワークアクセス機能では、ターミナルサーバアクセスの時と同様にActiveXがダウンロードされ、インストールできると上図の様に「ネットワークアクセス」の小窓が開き接続の進捗状況を表示する。

接続が確立された後、SSL-VPN装置との間ではあたかもIPSec-VPNのようにIPLレベルで全てのプロトコルを利用した通信が可能となる。

# L2フォワーディング方式SSL-VPNの概念図(例)



1. ActiveXによって、クライアントは仮想PPPコネクタを作成するとともに、IPアドレスの割当を受ける。
2. 内部サーバ宛以外の通信が発生した場合には、デフォルトゲートウェイに向ける。
3. 内部サーバ宛の通信の場合には、仮想PPPコネクタを経由してSSL-VPN装置に送信される。
4. SSL-VPN装置では、SSLで包まれた通信を取り出して、内部サーバ宛の通信を配送する。

ActiveX(実装によっては、Javaアプレット)をインストールしなくてはならないためクライアント側では管理者権限が必要となる。

# SSL-VPN導入のご利益(まとめ)

- Webブラウザさえあれば良く、設定の難しいVPN通信クライアントソフトを別途インストールする必要がない。
- メールでもアプリケーションでも、通信路がSSLで暗号化されているため盗聴を防ぐことができる。
- ユーザ認証で許可されたものだけが内部リソースにアクセスすることができる。(強固なセキュリティを担保)
- 他のVPNと比べ、境界機器(Firewallやルータ)の設定変更は必要ない。(SSLはだいたい許可されているため)
- 内部ネットワークへのアクセスログや利用状況ログを取得することができる。
- 初心者でも利用を容易に促進することができる。

# 今後の構想として

○高セキュリティ(機密性・完全性・可用性)を担保する必要のある学内の各部局間の通信,あるいは,学外からのリモートアクセス等の一方法として広く普及して行きたい。

○全学的な(SSL)VPN網を構築し,汎用的で安全な通信路を提供するプロジェクトを計画中

○その際には,全学での利用者をカバーするため,認証サーバを構築するとともに,統合的なID管理スキームを確立する。

○システムの権限管理問題にも解決策を見出して行きたい。

○ICカード職員証や学生証の普及状況も勘案しながら,ICカード内に電子証明書を格納し,各種サービスで利用できる下地を計画したい。

○最終的には,全学的PKIを構築することを目的とする。

# ご静聴ありがとうございました。

ご指摘やご質問等がございましたら、下記までご連絡下さいませよう、お願い致します。

また、本件に関連するご提案も積極的にお受けしております。是非お聞かせ下さい。

※ 夏目は2007年7月1日付けで異動になりました