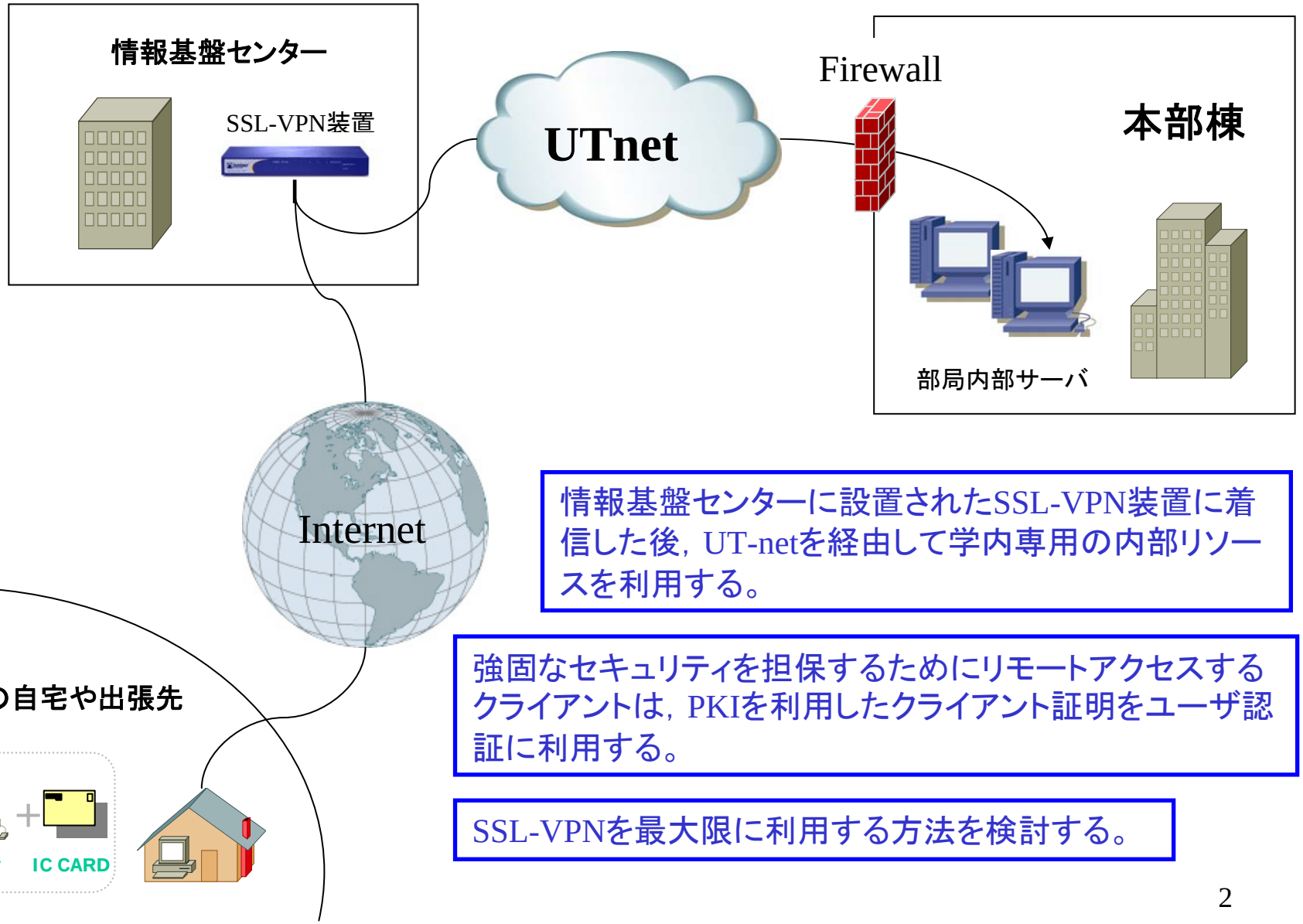
SSL-VPN実証実験について

総務部情報課　開発チーム

夏　目　典　大

SSL-VPN実証実験の概要



情報基盤センターに設置されたSSL-VPN装置に着信した後，UT-netを経由して学内専用の内部リソースを利用する。

強固なセキュリティを担保するためにリモートアクセスするクライアントは，PKIを利用したクライアント証明をユーザ認証に利用する。

SSL-VPNを最大限に利用する方法を検討する。

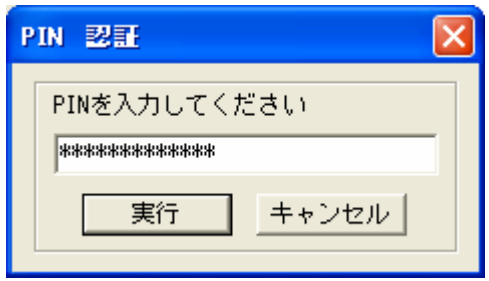
SSL-VPNの利用

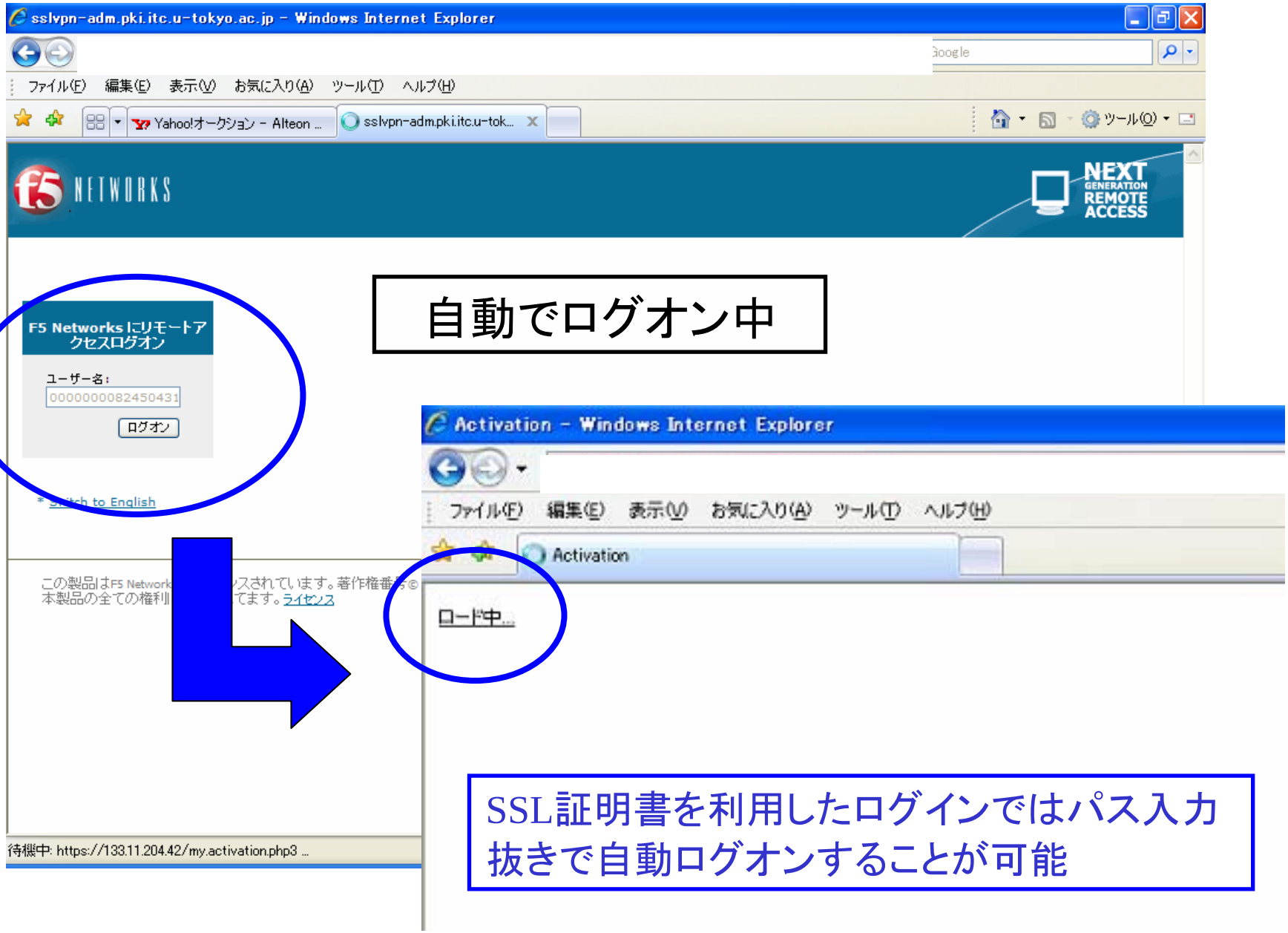
①ICカードリーダにUT-CA発行のICカードを挿入する。

②Webブラウザを立ち上げる。

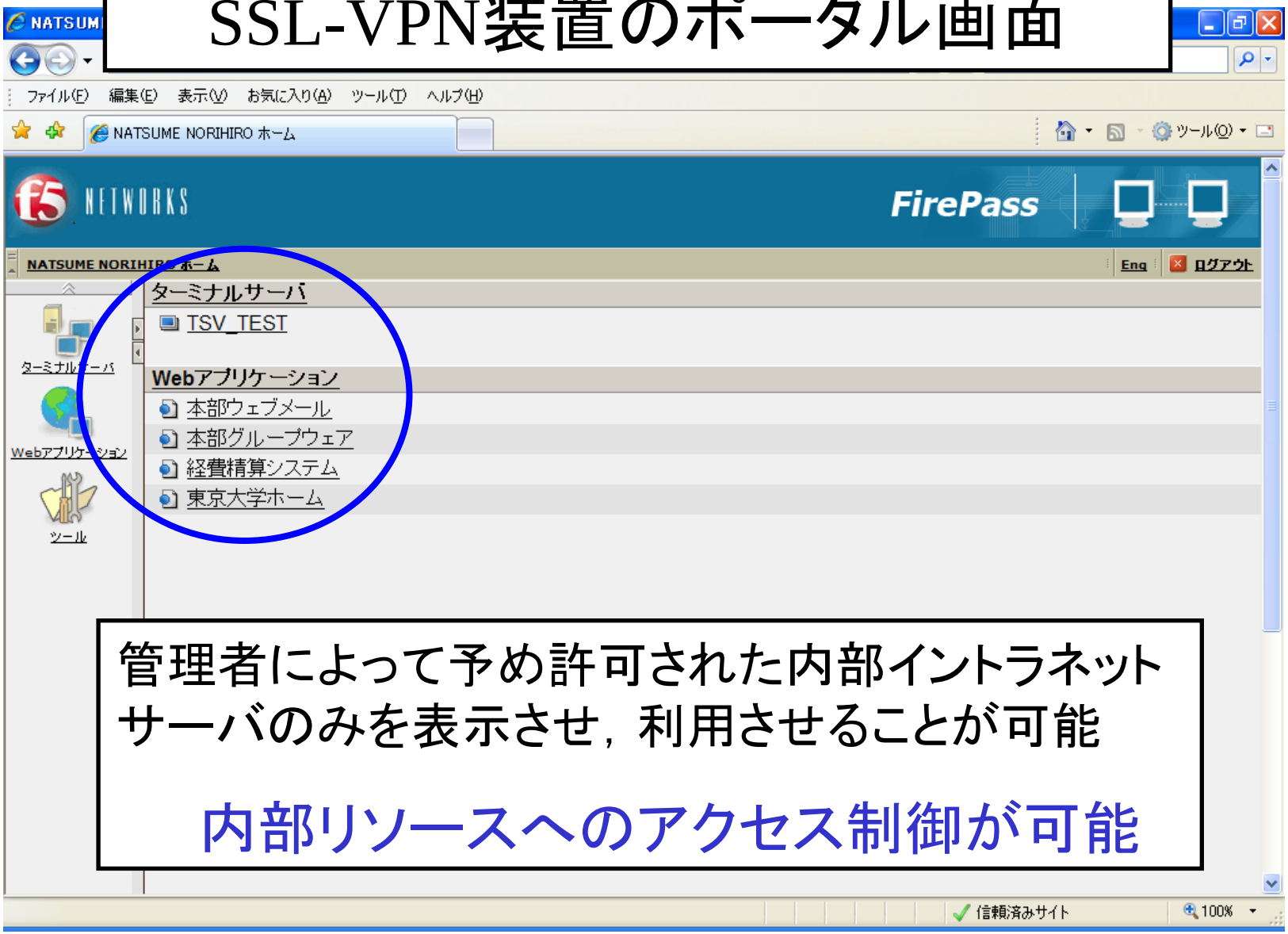
③https://からはじまるSSL-VPN装置のURLを入力する。

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。




sslvpn-adm.pki.itc.u-tokyo.ac.jp - Windows Internet Explorer
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)
Yahoo!オークション - Alteon ...
sslvpn-adm.pki.itc.u-tok...
ツール(O)
NETWORKS
NEXT GENERATION REMOTE ACCESS
F5 Networks にリモートアクセスログオン
ユーザー名:
0000000082450431
ログオン
Switch to English
この製品はF5 Network
ンスされています。著作権番
本製品の全ての権利
てます。ライセンス
待機中: https://133.11.204.42/my.activation.php3 ...
自動でログオン中
Activation - Windows Internet Explorer
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)
Activation
ロード中...
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



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

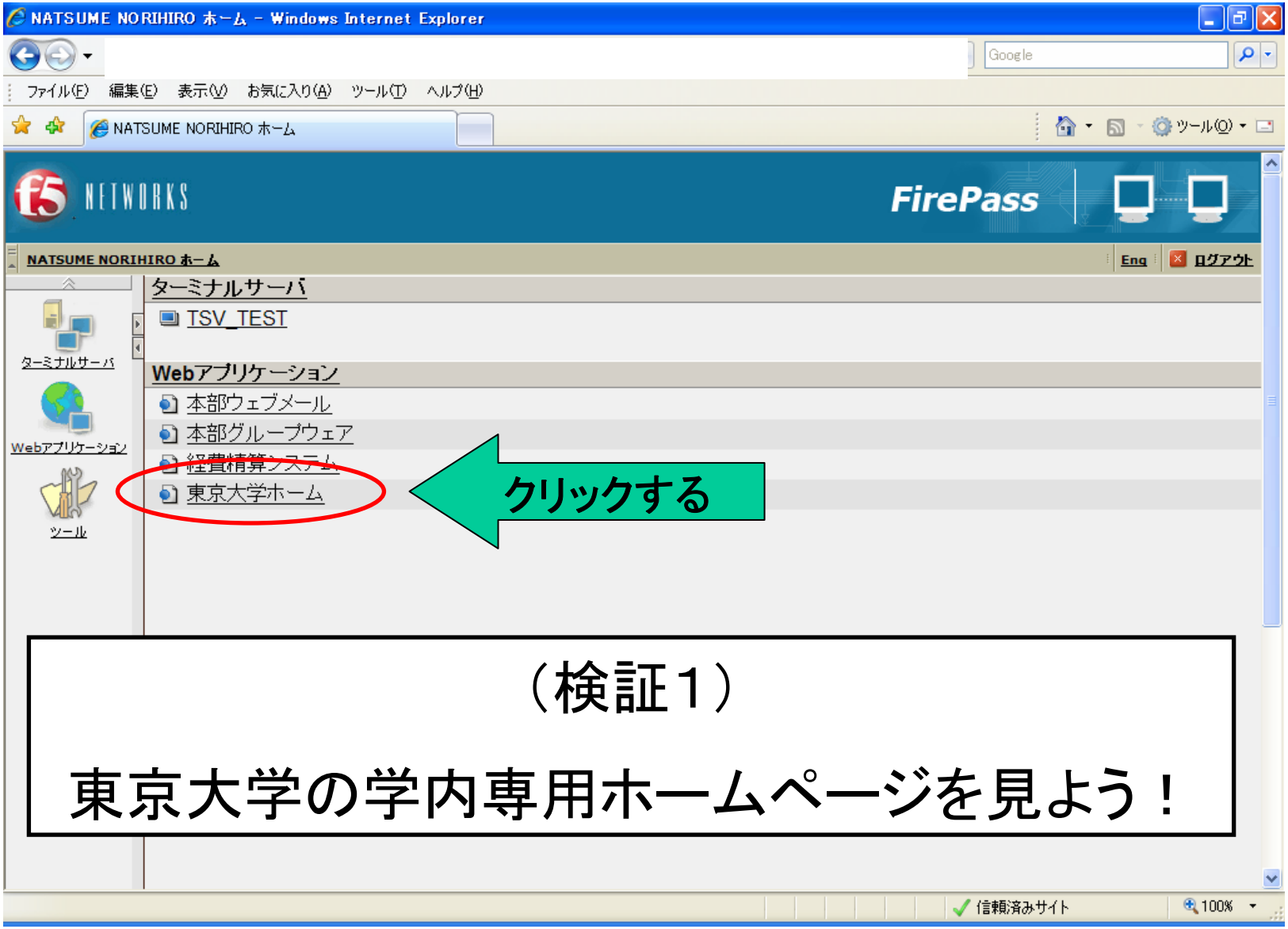
SSL-VPN実験検証の内容

- （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！

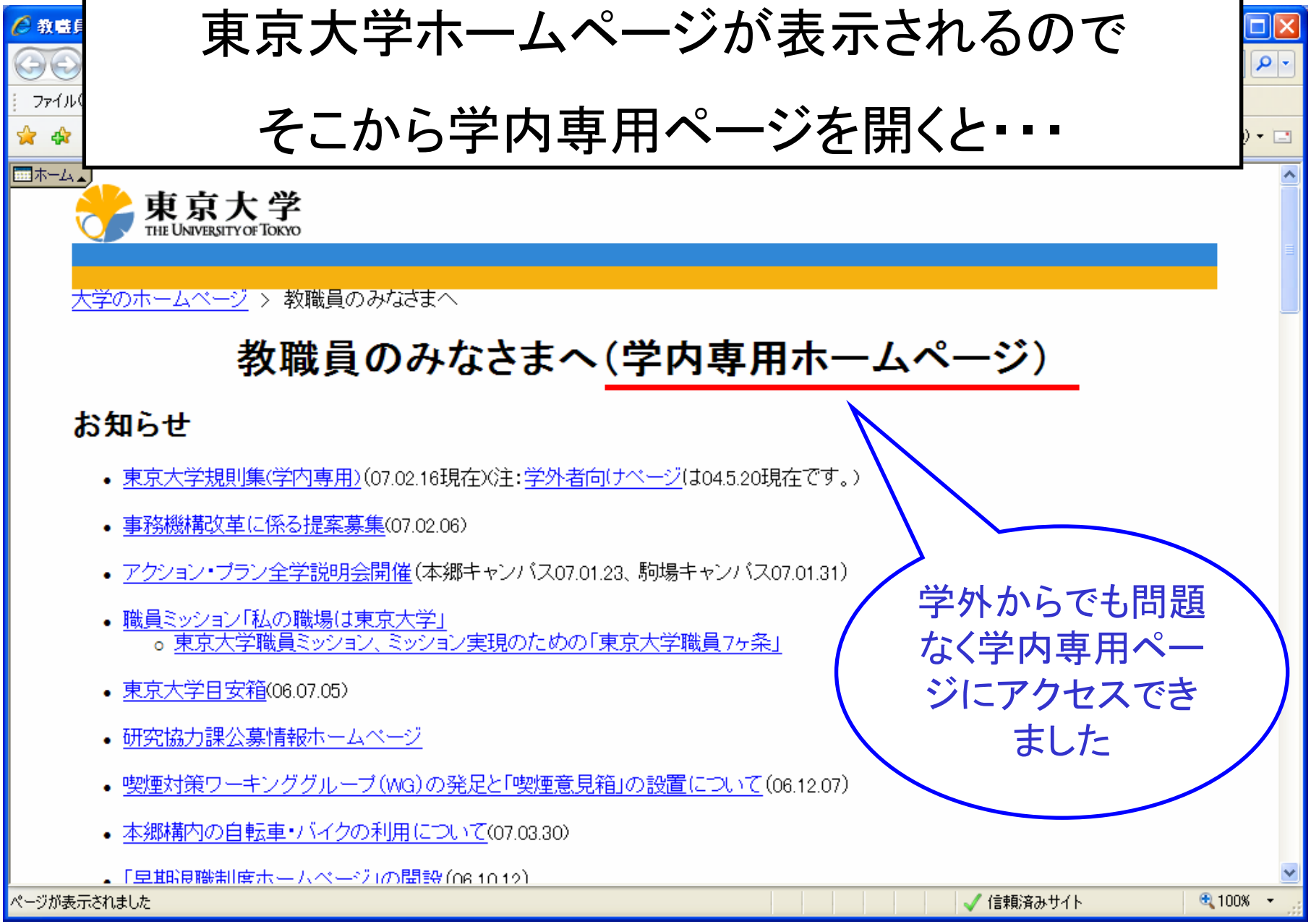
- （番外編）　クライアント・サーバ方式のアプリケーション
  を安全に利用してみたい！（IPSec-VPNのように）



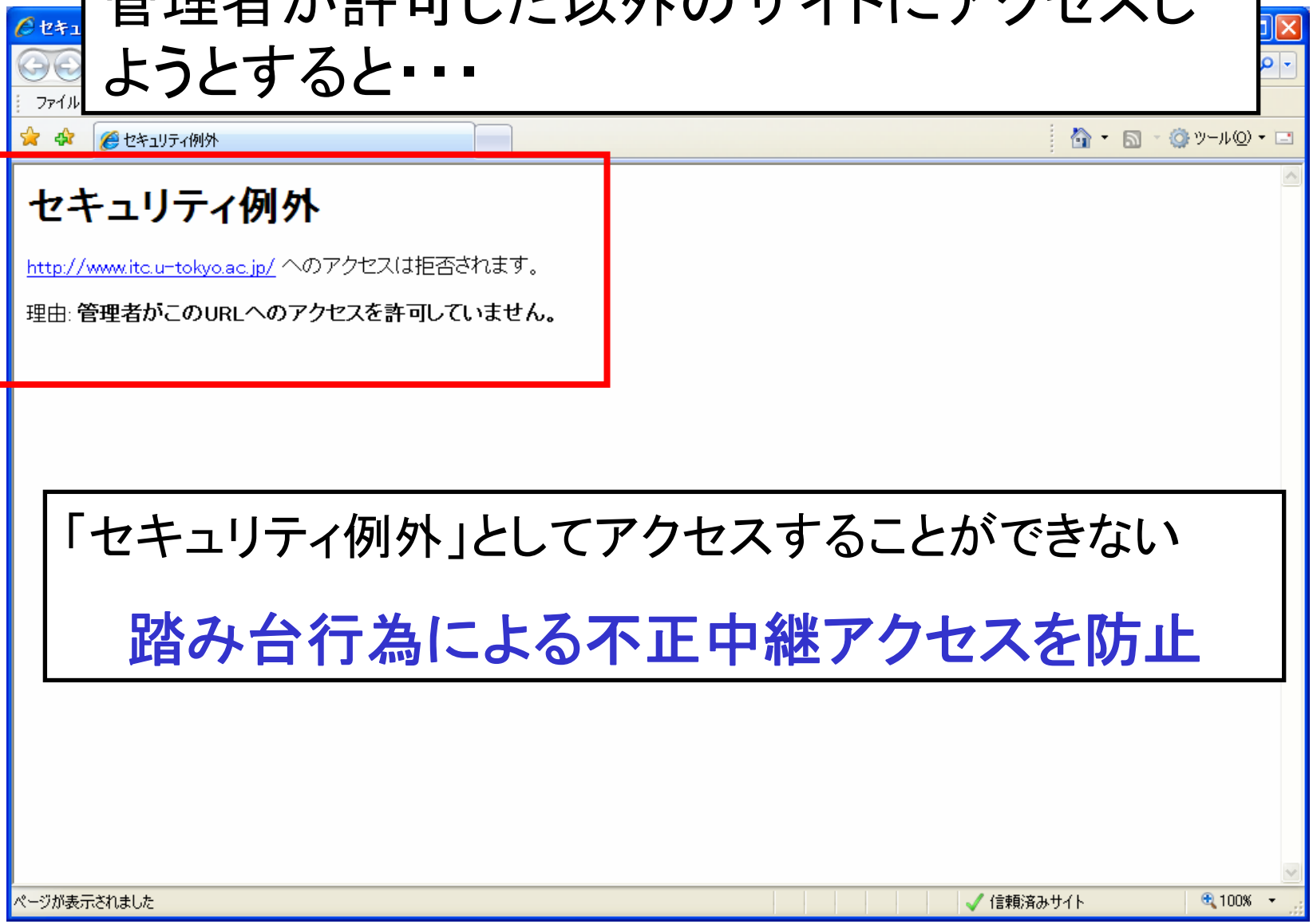
（検証１）

東京大学の学内専用ホームページを見よう！

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・・・

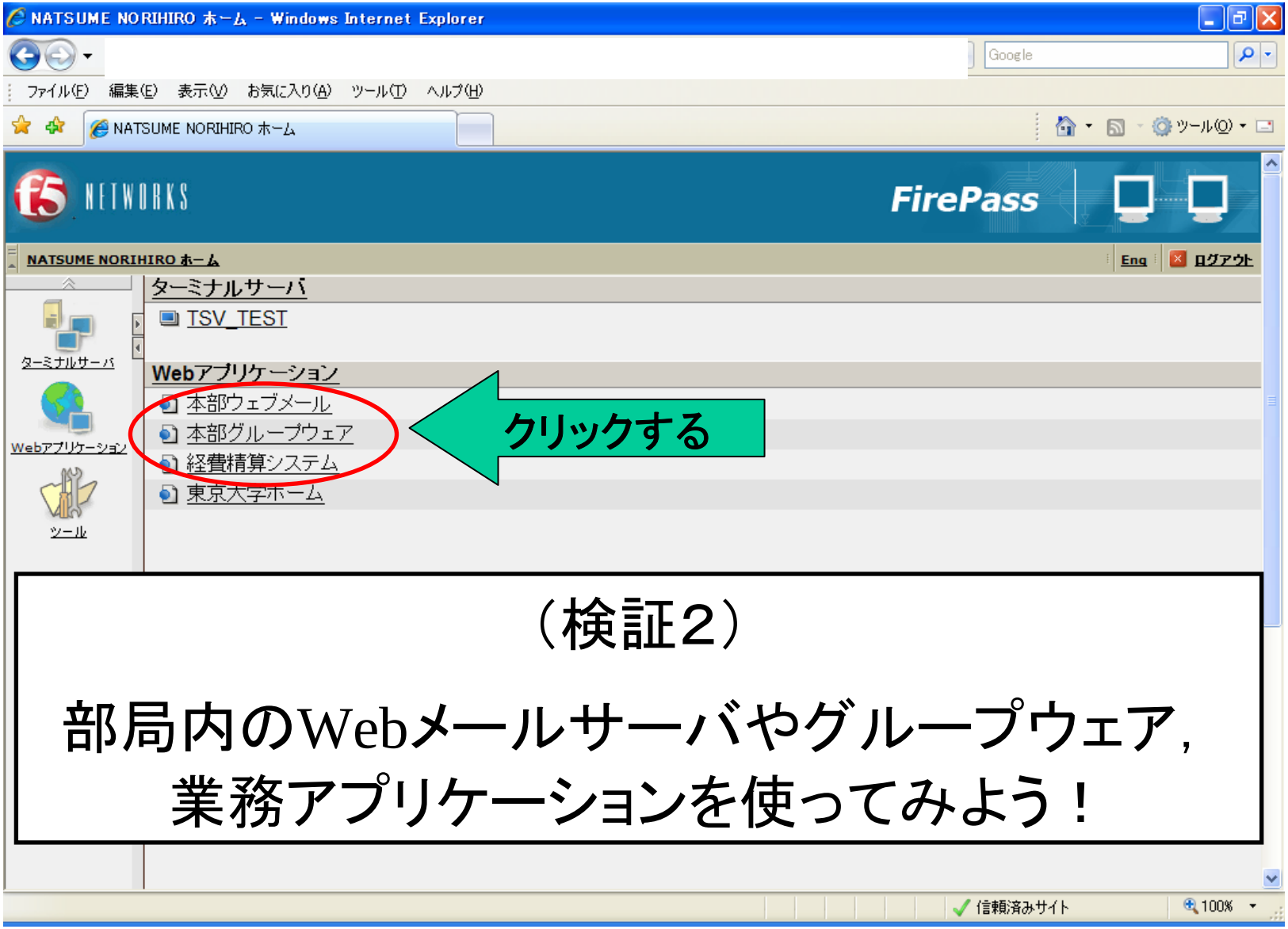


管理者が許可した以外のサイトにアクセスしようとすると・・・



「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



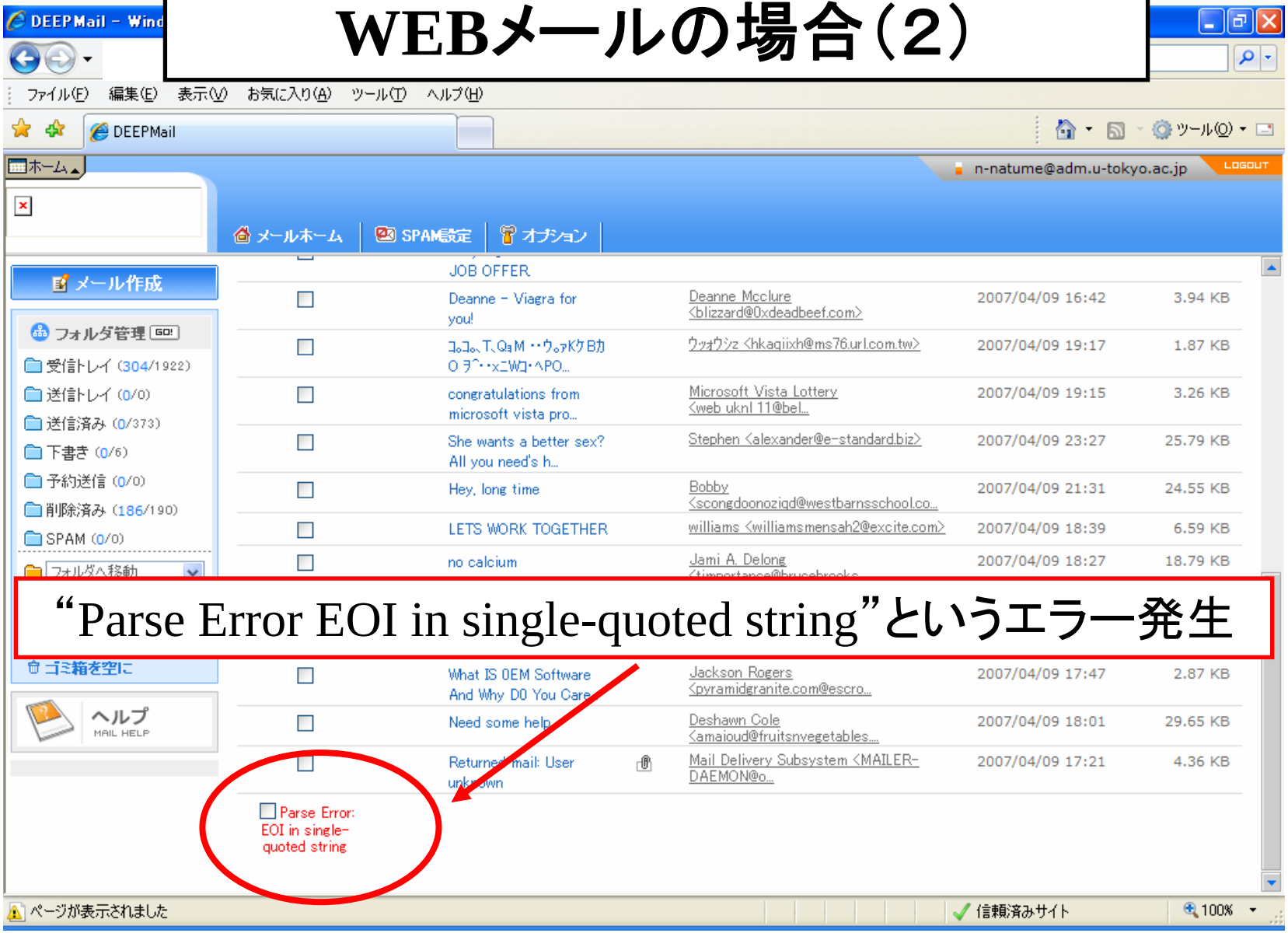
（検証２）

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！

WEBメールの場合（1）

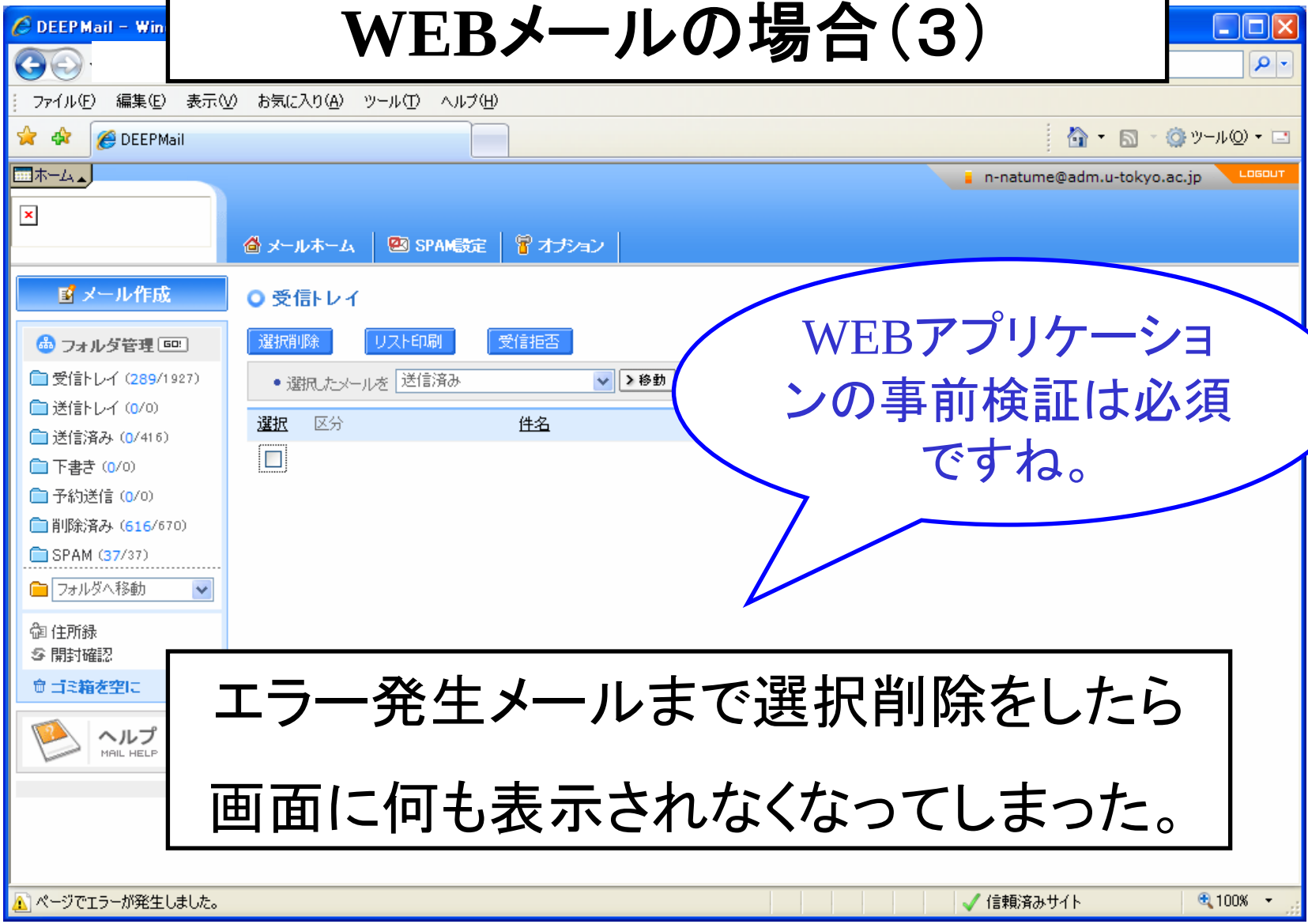
通常通りにWebメールにアクセスできている様子

WEBメールの場合（2）

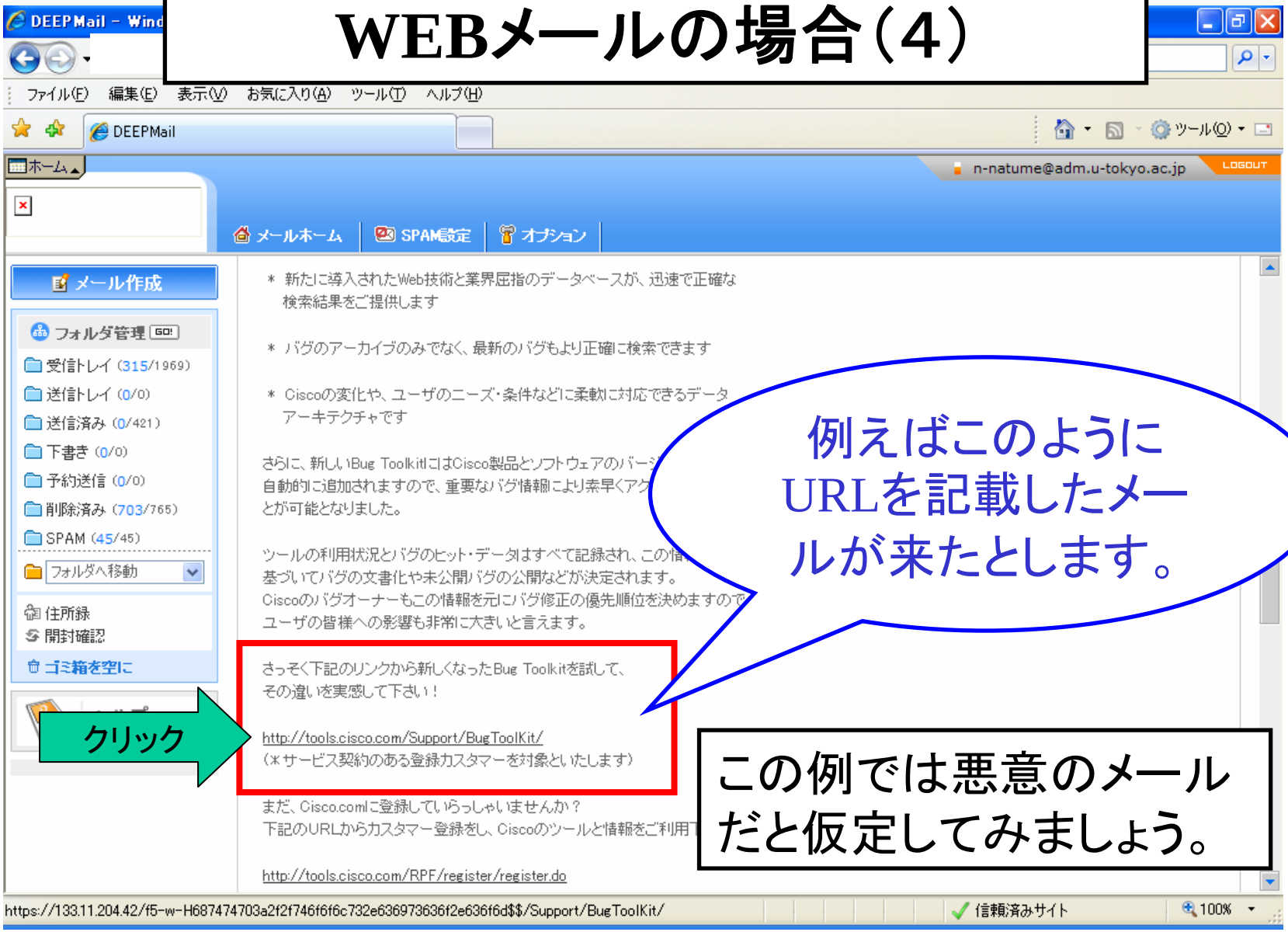


“Parse Error EOI in single-quoted string”というエラー発生

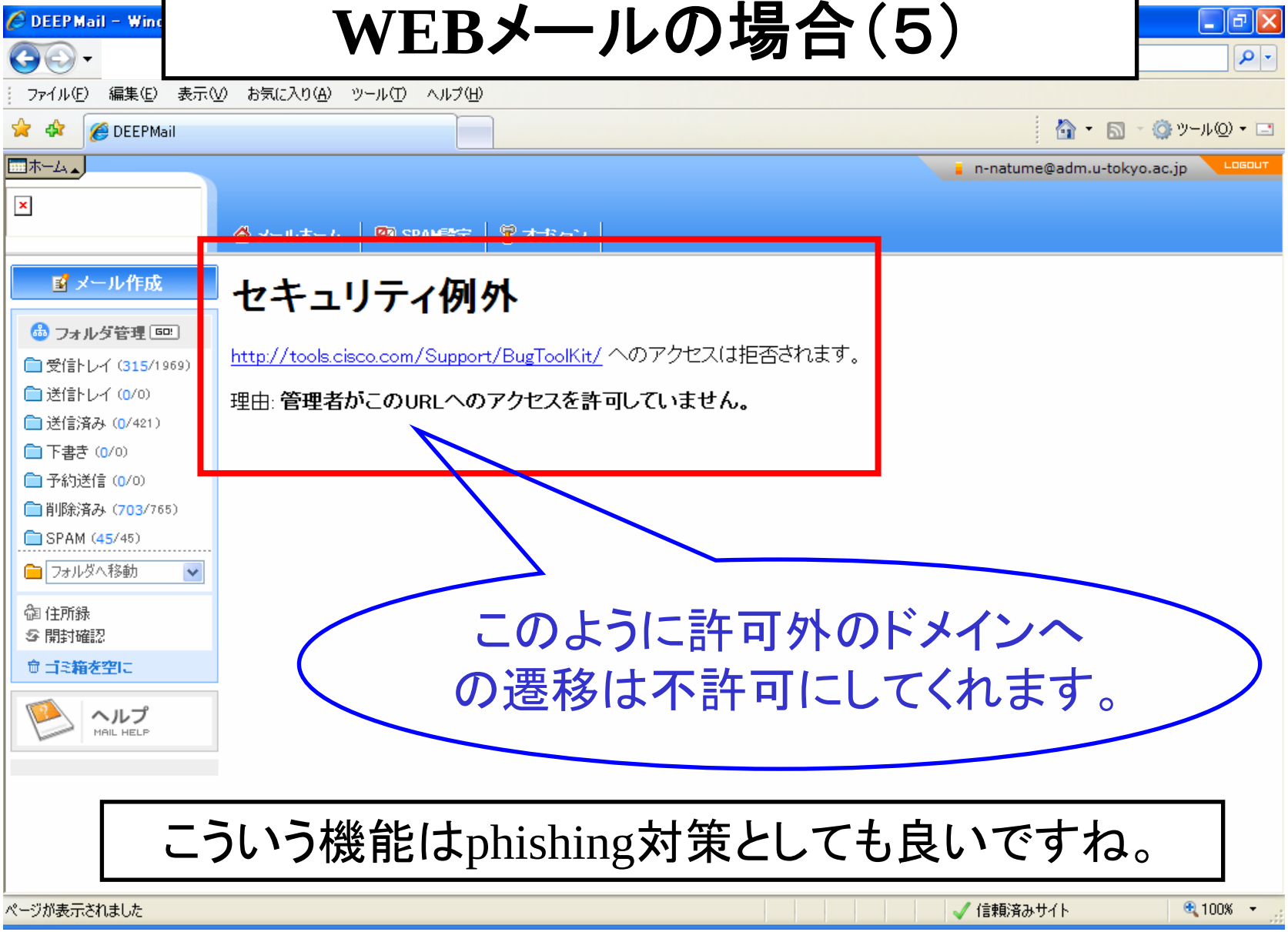
WEBメールの場合（3）


DEEPMail - Win
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)
DEEPMail
ツール(O)
ホーム
n-natume@adm.u-tokyo.ac.jp
LOGOUT
メールホーム
SPAM設定
オプション
メール作成
受信トレイ
フォルダ管理 GO!
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)
SPAM (37/37)
フォルダへ移動
住所録
開封確認
ゴミ箱を空に
ヘルプ
MAIL HELP
選択削除
リスト印刷
受信拒否
選択したメールを
送信済み
移動
選択
区分
件名
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ってしまった。
ページでエラーが発生しました。
信頼済みサイト
100%

WEBメールの場合（4）


DEEPMail
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)
DEEPMail
ツール(O)
ホーム
n-natume@adm.u-tokyo.ac.jp
LOGOUT
メールホーム
SPAM設定
オプション
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)
フォルダへ移動
住所録
開封確認
ゴミ箱を空に
＊ 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 Toolkitl...Cisco製品とソフトウェアのバー...
自動的に追加されますので、重要なバグ情報により素早くア...
と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...
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...
http://tools.cisco.com/RPF/register/register.do
クリック
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ょう。
https://133.11.204.42/f5-w-H687474703a2f2f746f6f6c732e636973636f2e636f6d$$/Support/BugToolKit/
信頼済みサイト
100%

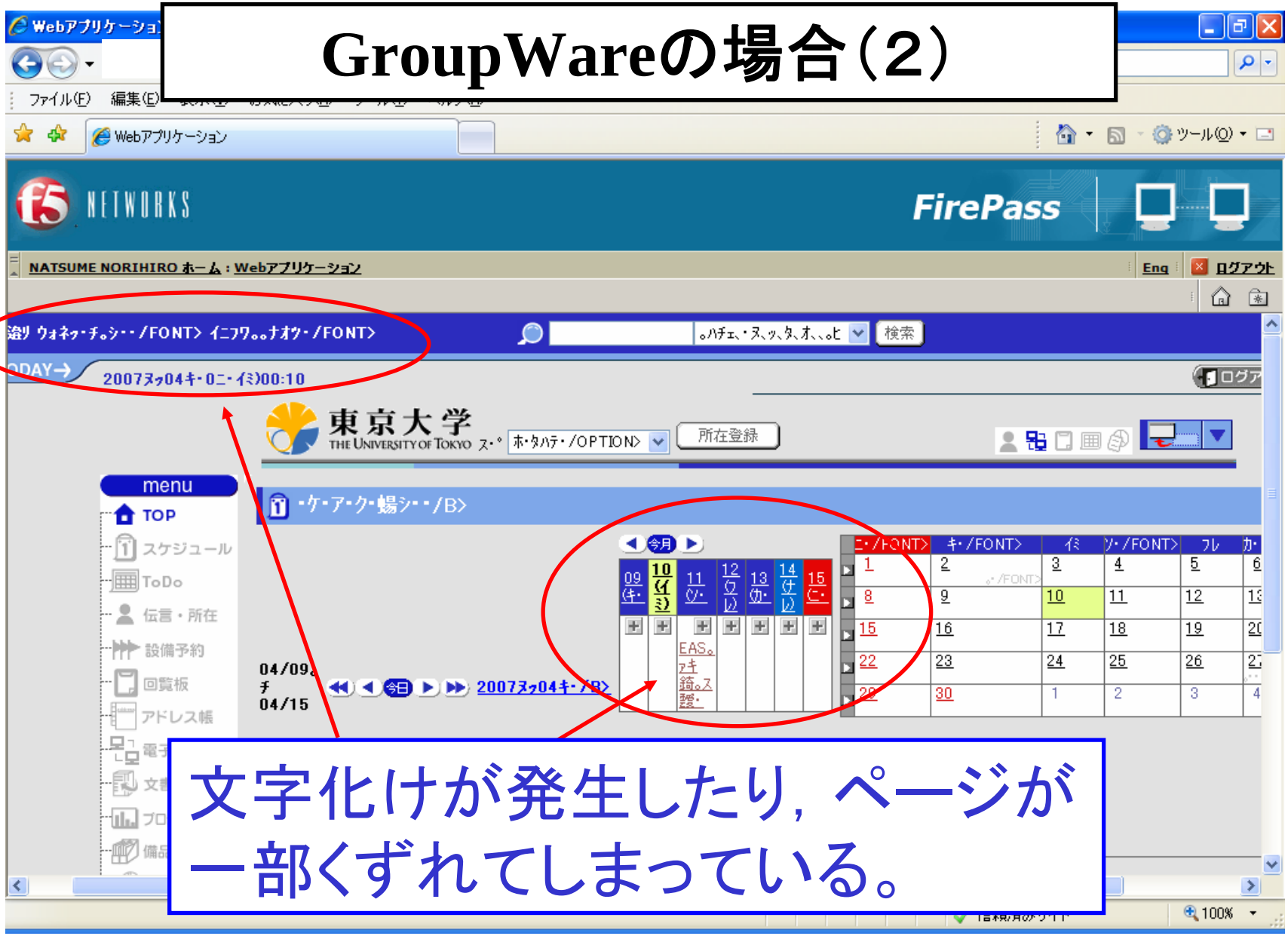
WEBメールの場合（5）



こういう機能はphishing対策としても良いですね。

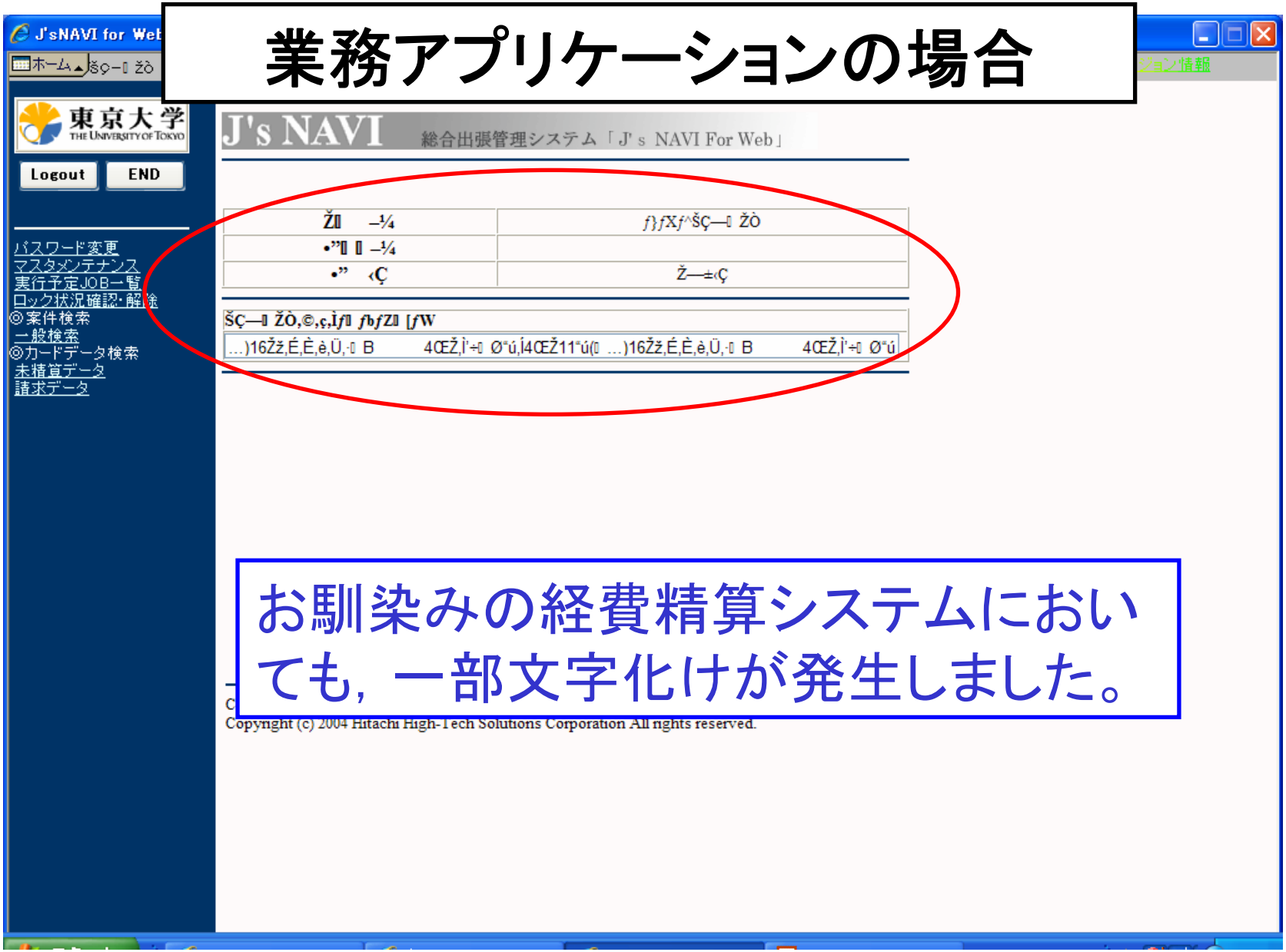
GroupWareの場合（1）

GroupWareの場合（2）



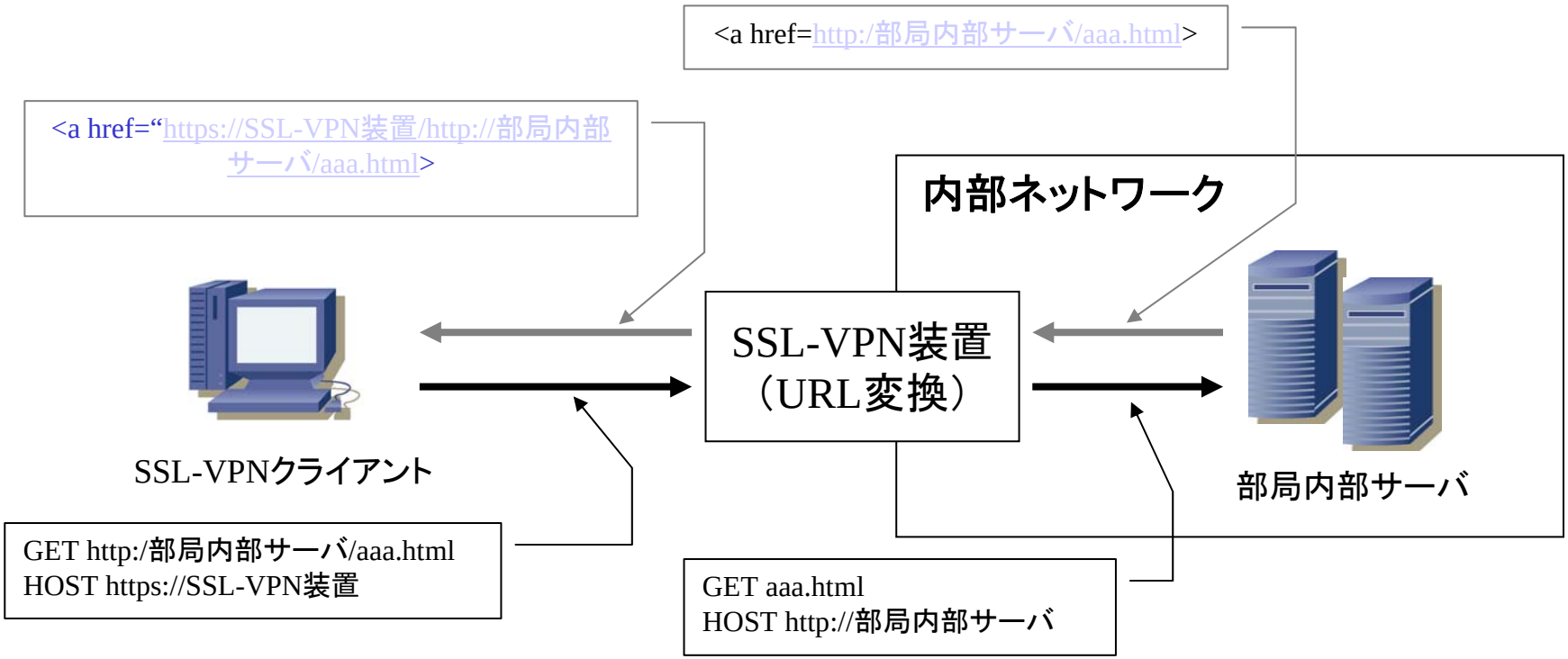
文字化けが発生したり，ページが一部くずれてしまっている。

業務アプリケーションの場合



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

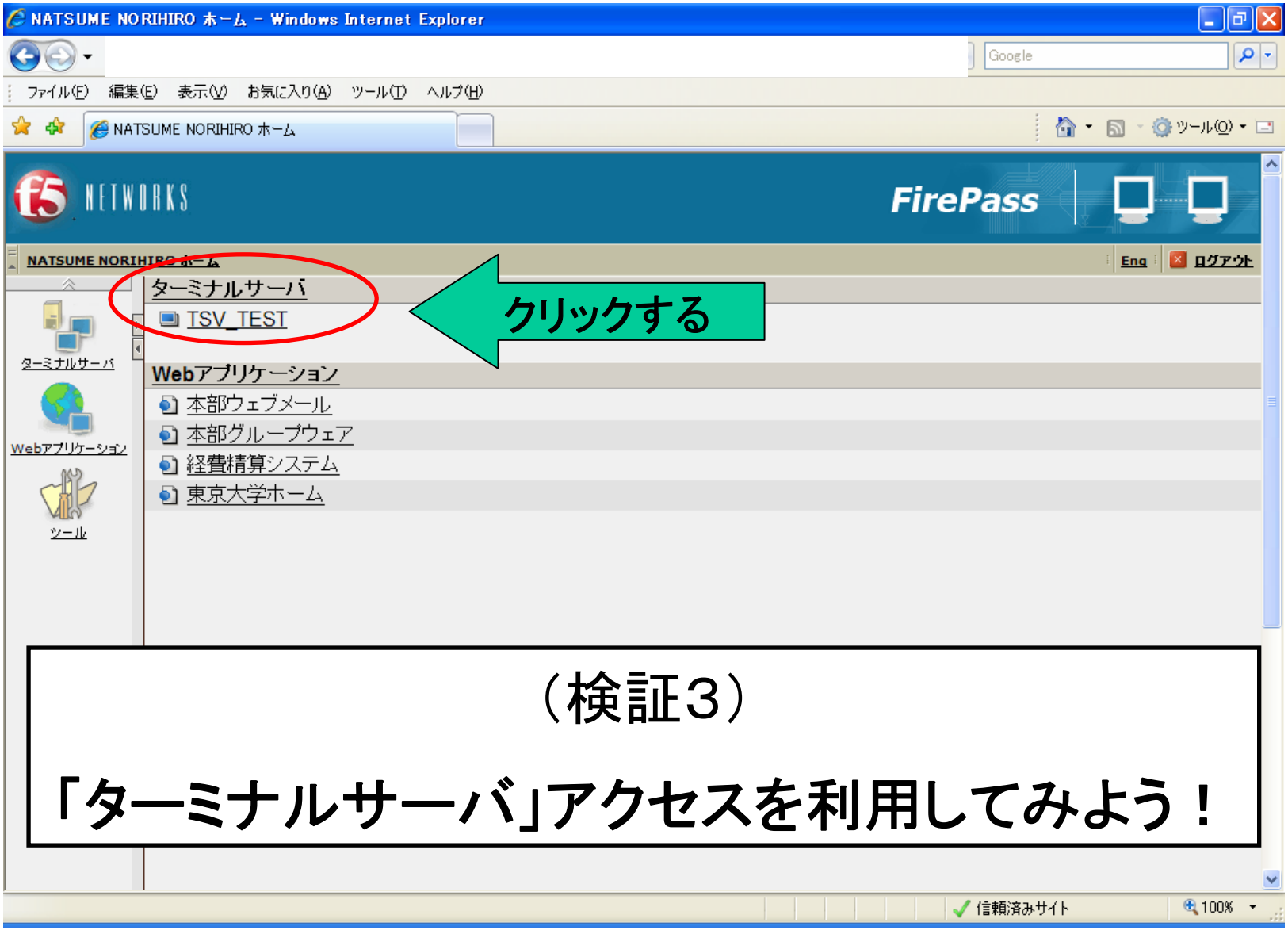
・日本語EUCコードを使用したアプリケーションと日本語JISコードを使用したアプリケーションに同時にアクセスをした場合

→ 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

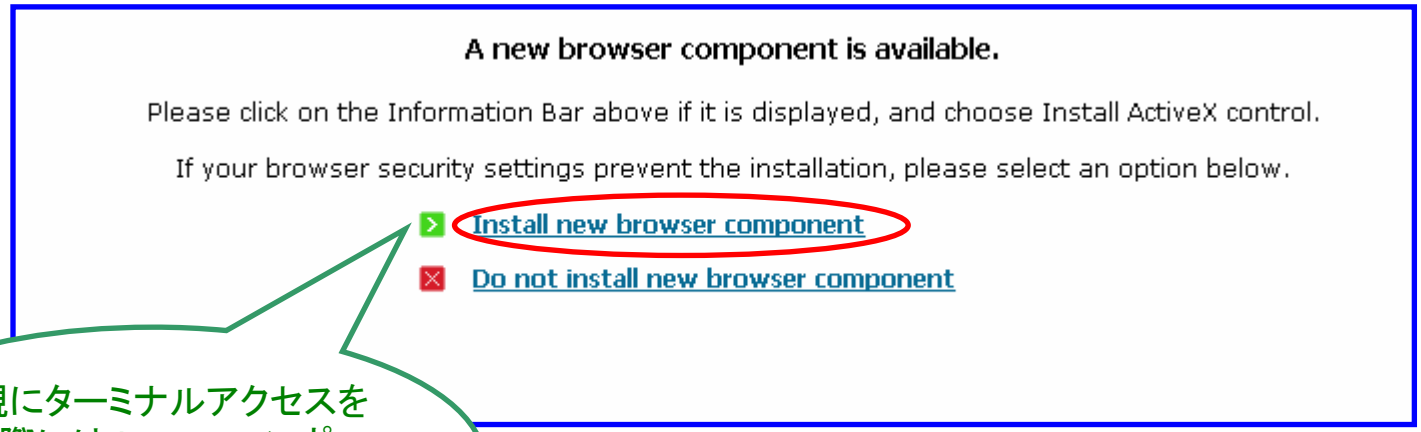
→ リバースプロキシにおいて必要なページ内リンクの変換を行うことができない。 など

NETWORKWORLDより



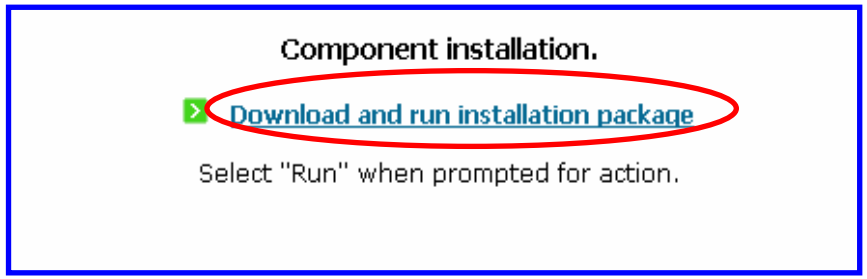
（検証３）

「ターミナルサーバ」アクセスを利用してみよう！

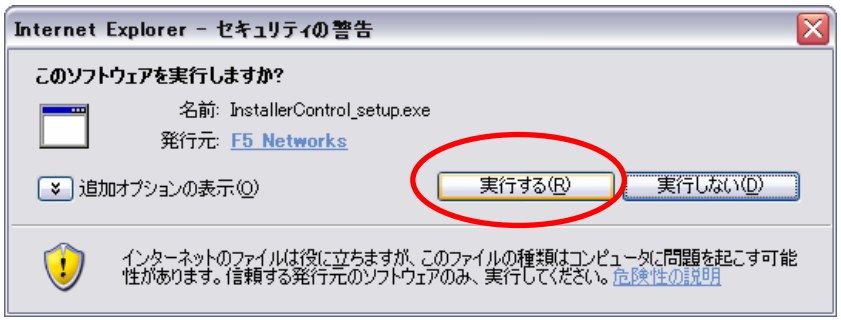


新規にターミナルアクセスを行う際にはActiveXコンポーネントのインストールが必要になります。

① Install．．．を押すと

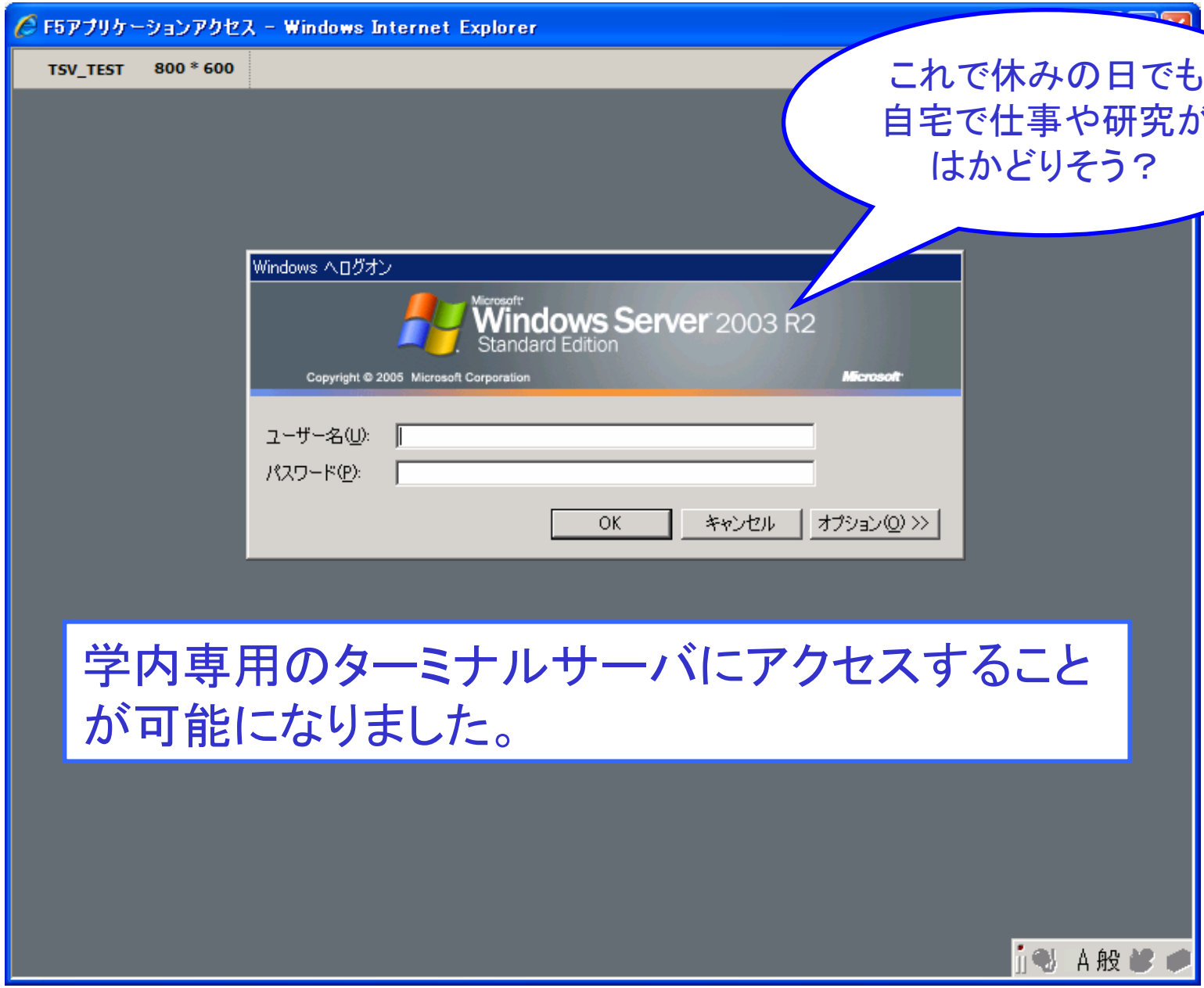


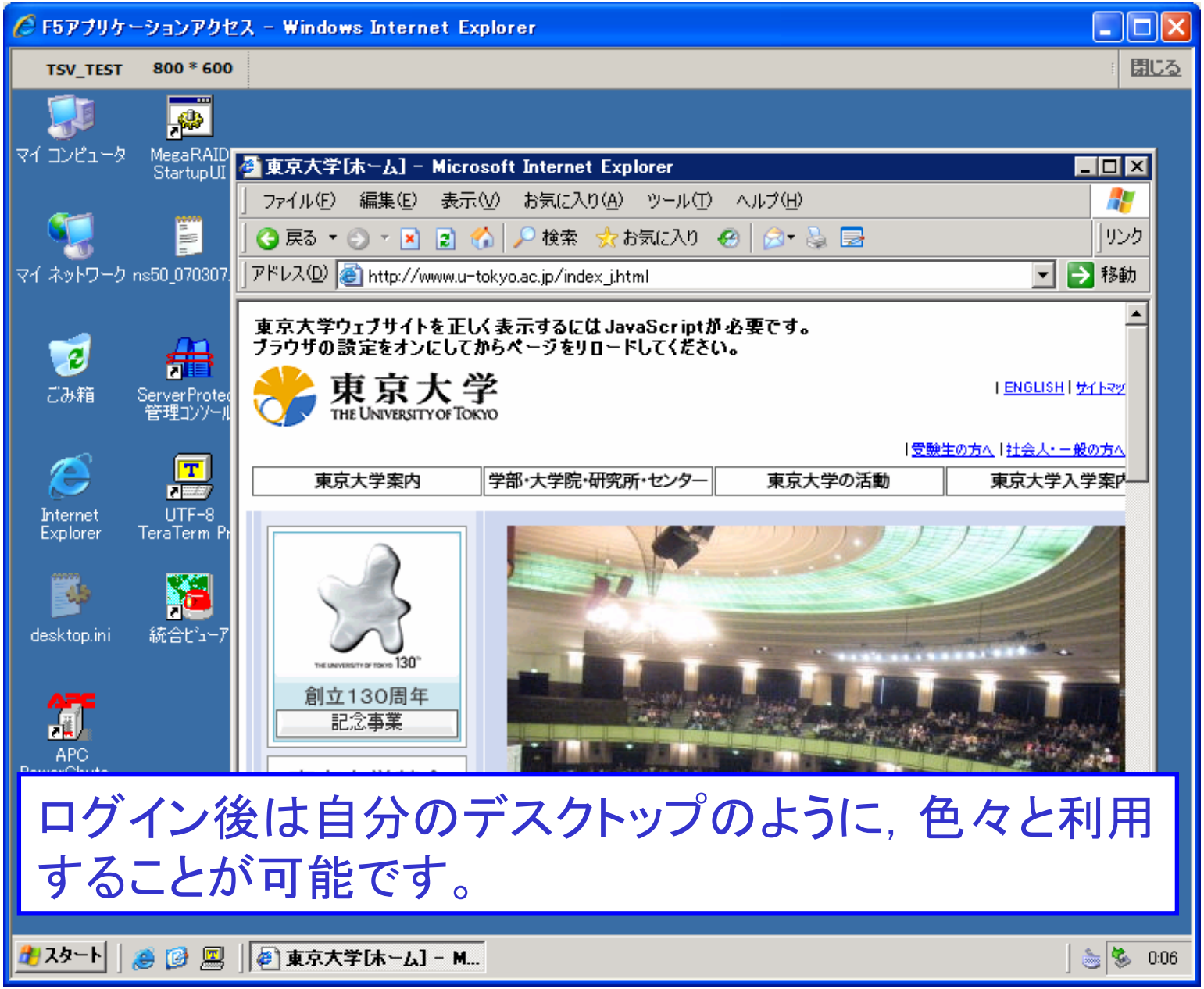
②ActiveXコンポーネントがダウンロードされるので



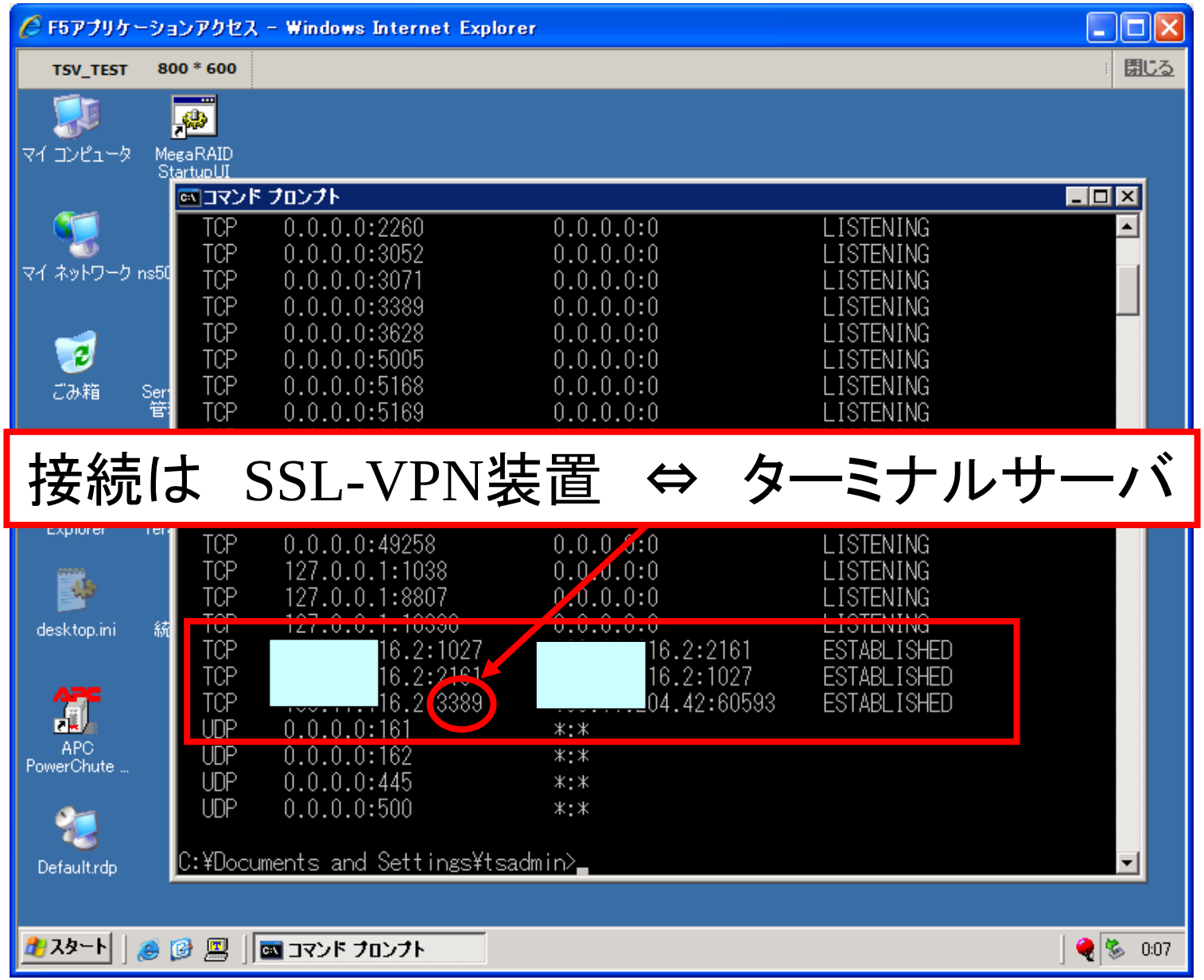
③実行する。

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

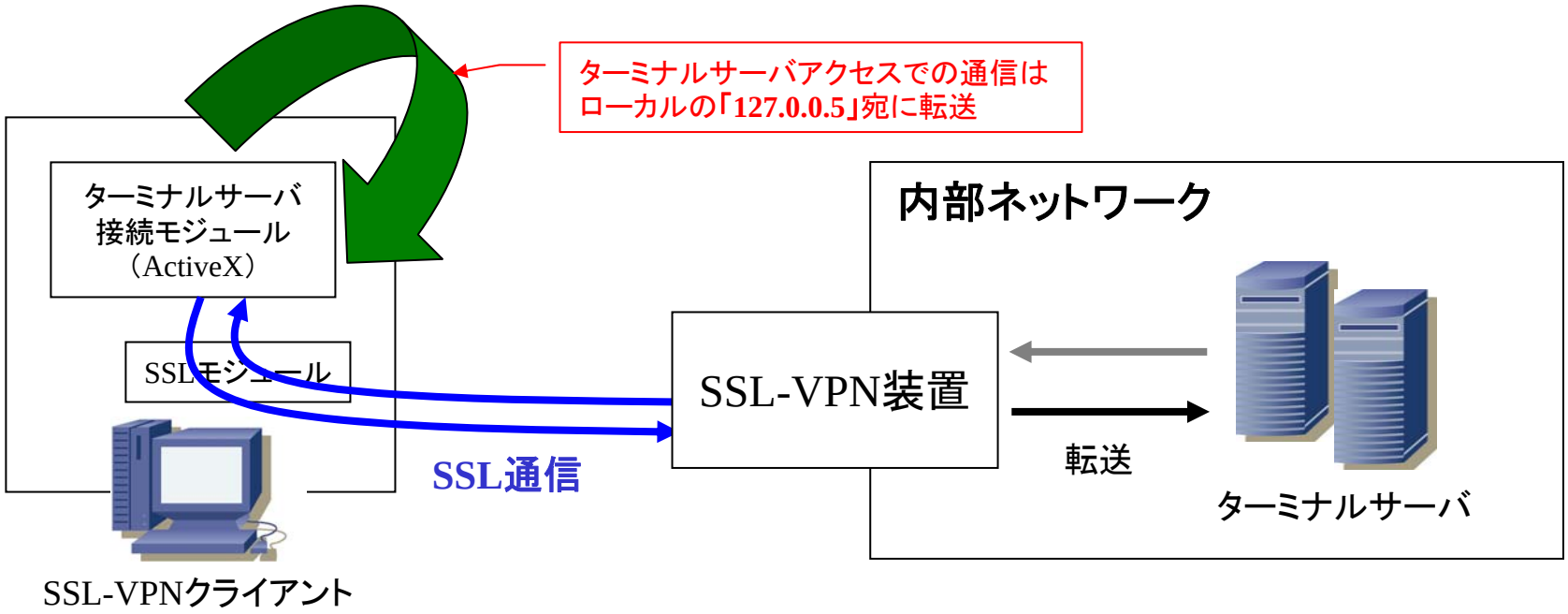

F5アプリケーションアクセス - Windows Internet Explorer
TSV_TEST 800 * 600
これで休みの日でも
自宅で仕事や研究が
はかどりそう？
Windows ヘログオン
Microsoft Windows Server 2003 R2
Standard Edition
Copyright © 2005 Microsoft Corporation
Microsoft
ユーザー名(U):
パスワード(P):
OK
キャンセル
オプション(O) >>
学内専用のターミナルサーバにアクセスすることが可能になりました。
A 般



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。

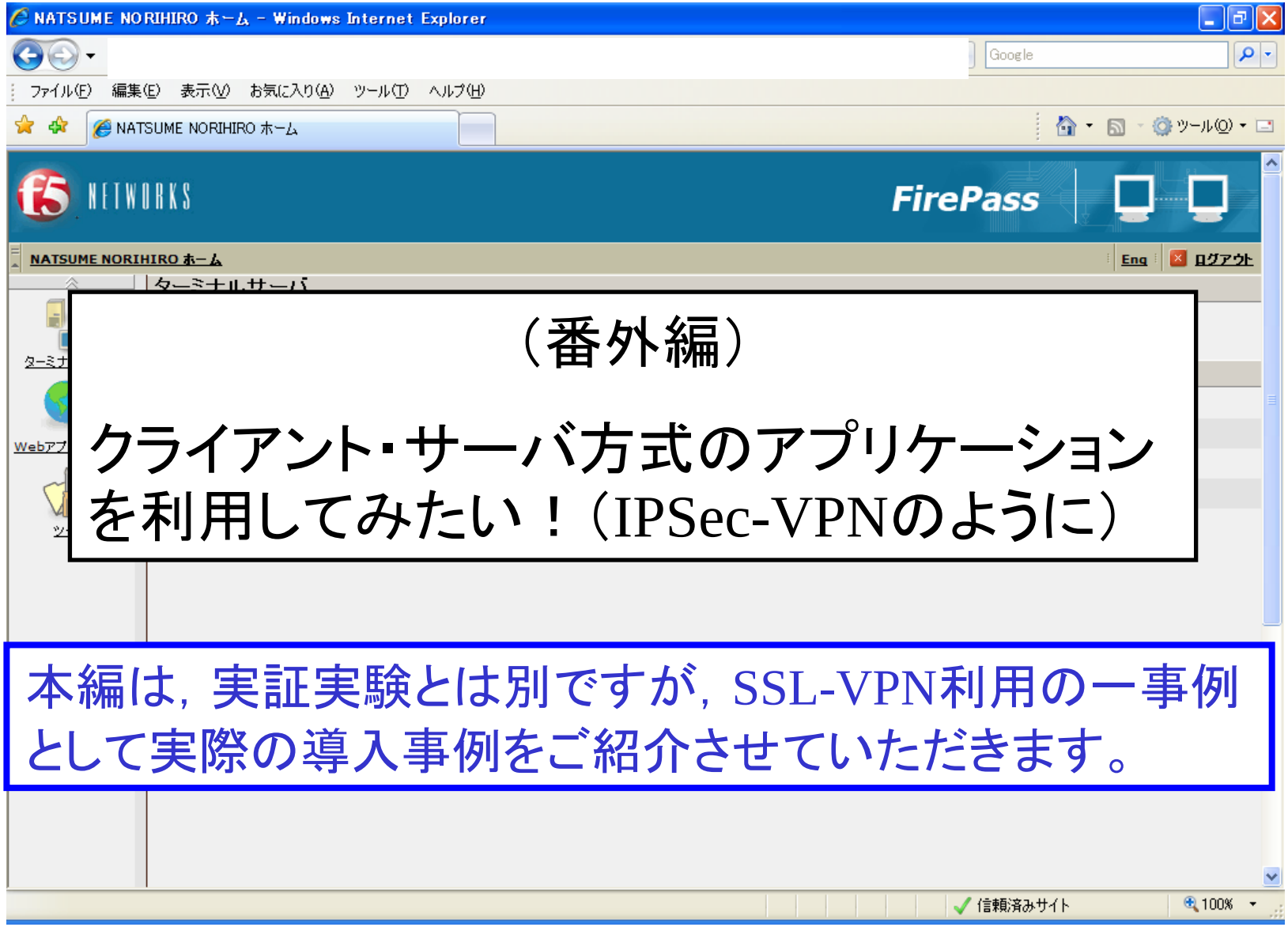

F5アプリケーションアクセス - Windows Internet Explorer
TSV_TEST 800 * 600
閉じる
マイ コンピュータ
MegaRAID StartupUI
コマンド プロンプト
TCP 0.0.0.0:2260 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3052 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3071 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3628 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5005 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
マイ ネットワーク
ごみ箱
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 16.2:1027 16.2:2161 ESTABLISHED
TCP 16.2:2161 16.2:1027 ESTABLISHED
TCP 16.2 3389 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>
desktop.ini
APC PowerChute ...
Default.rdp
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）

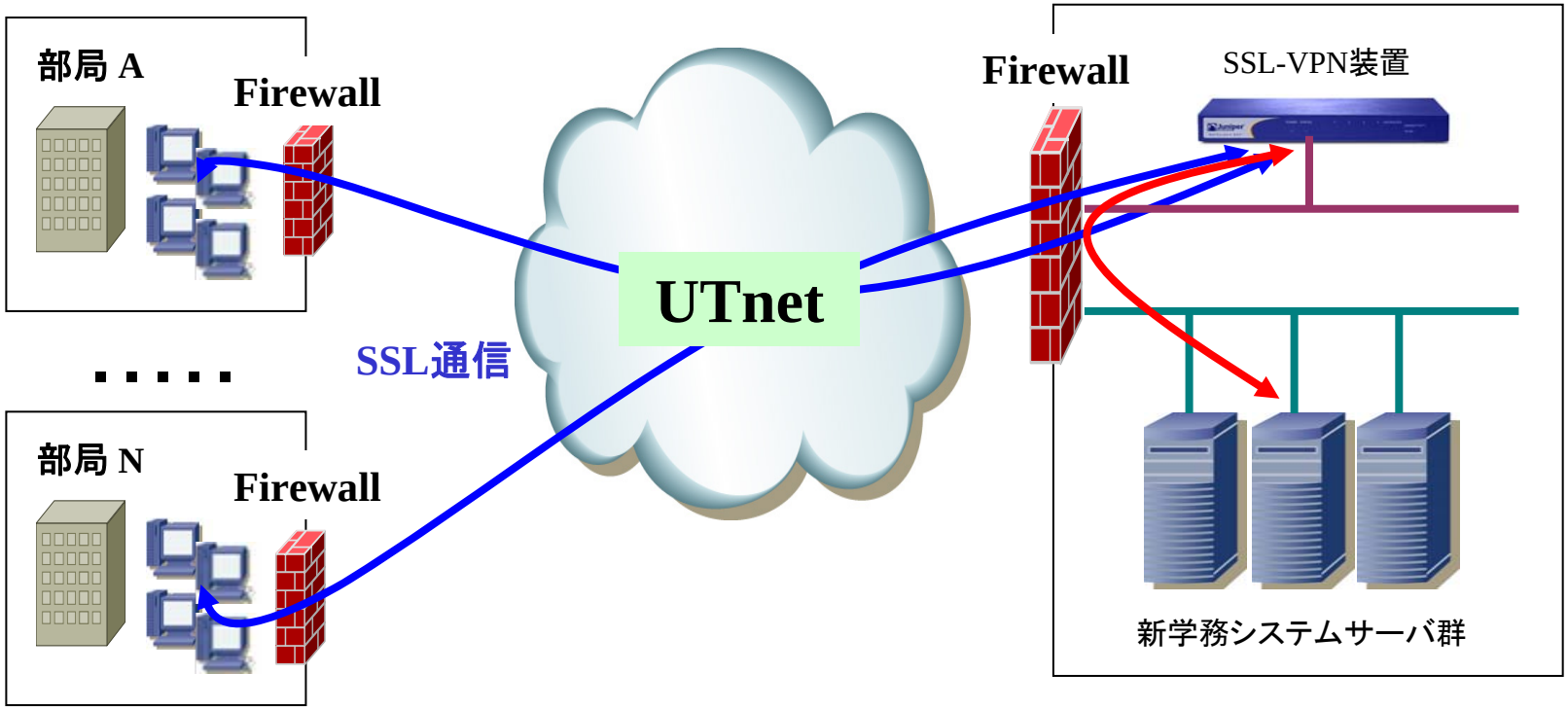


ターミナルサーバアクセスの通信は，（今回の実証実験では）「127.0.0.5」に転送される。その後，通信はSSLモジュールによってSSL暗号化されSSL-VPN装置に送信される。SSL-VPN装置ではこの通信を内部ターミナルサーバに転送する。

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
NATSUME NORIHIRO ホーム
NETWORKS
FirePass
NATSUME NORIHIRO ホーム
Eng
ログアウト
（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させていただきます。

新学務システムのネットワークアクセス利用例



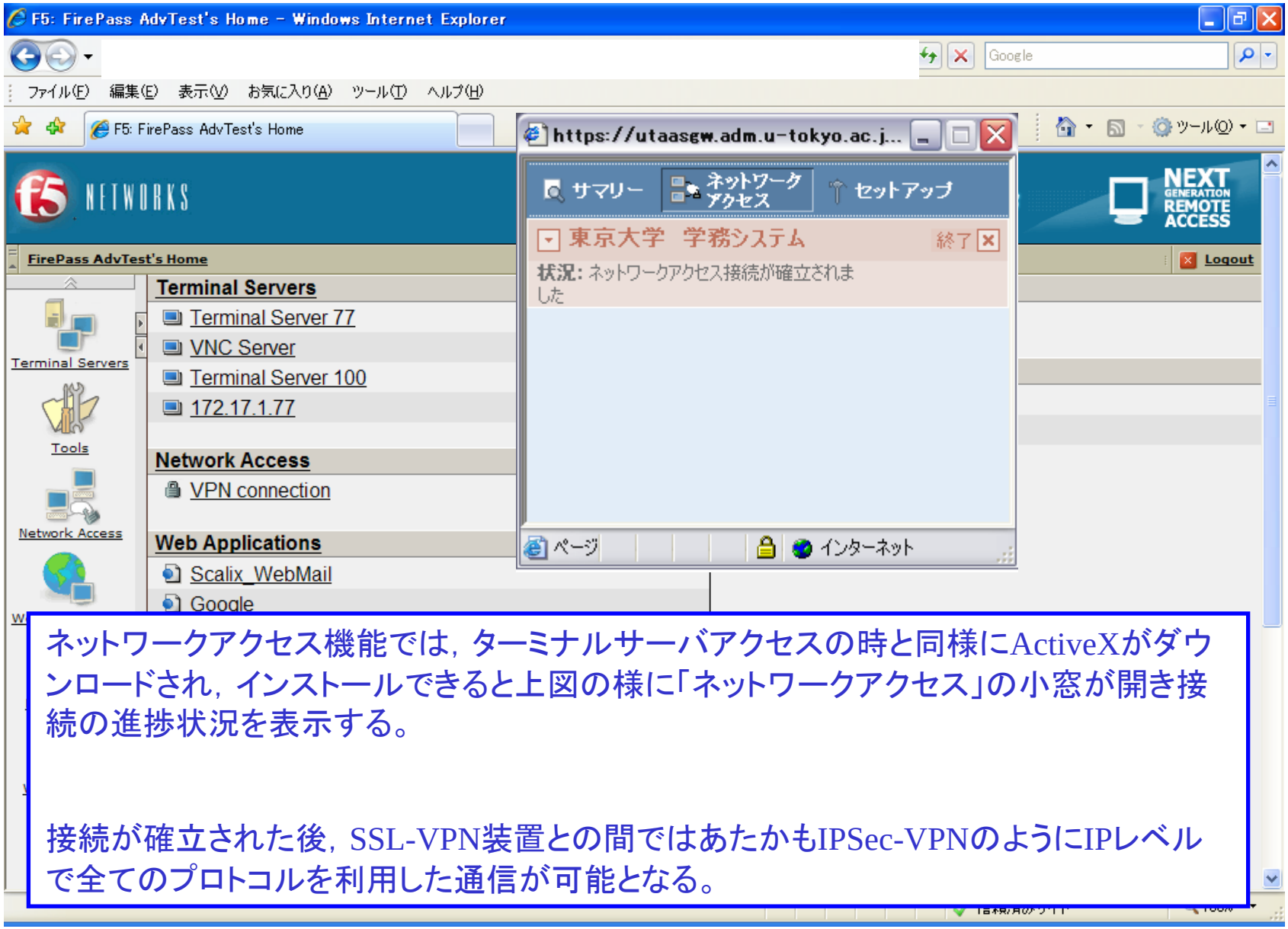
（必要条件）

〇各部局では，ネットワーク境界にFirewallを設置している可能性が高い。

〇クライアント・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。

〇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。

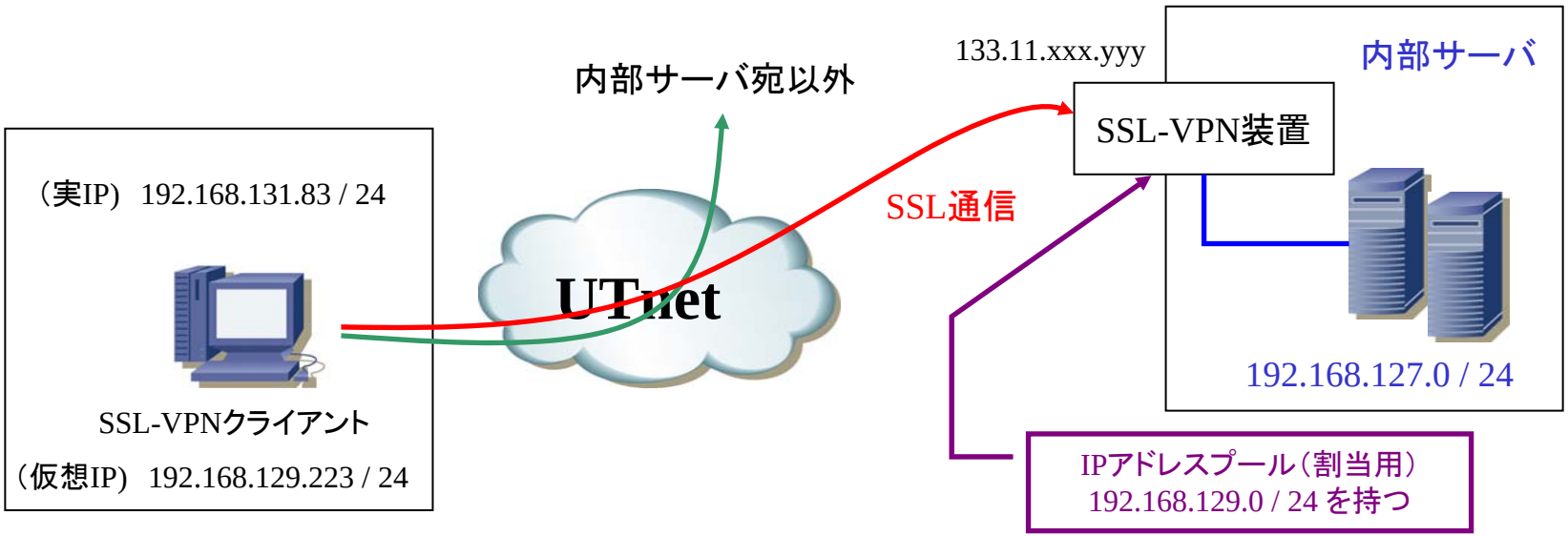
〇学務データは最重要なものなので，盗聴や改ざん，なりすましによる情報詐取を防止できなければならない。



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IP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）

〇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。

〇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。

〇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）

〇他の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）

〇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。

〇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

〇高セキュリティ（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。

〇全学的な（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

〇その際には，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。

〇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。

〇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。

〇最終的には，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すよう，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