大学の教育用ネットワークの構築

－ユーザーフレンドリなセキュリティシステム－

中部大学　学術情報センター

■ 執筆者Ｐｒｏｆｉｌｅ

岡 部　仁

中部大学　学術情報センター　技師

■ 論文要旨 ■

中部大学では更なる情報教育の柱とし，ノート PC 所持の義務化を行った．これまでの管理 PC のネットワーク環境とは別に，管理対象外の PC を教育で利用するネットワークが必要となった．

このネットワークは，セキュリティと利便性の相反する事項のバランスが特に重要となる．このため５つのコンセプトを掲げシステム構築し，またセキュリティ要件を実践的に体験させるための環境も教育の一つと構想した．

しかし，現状のセキュリティ製品は管理側の安全確保のための設計（接続させないことが基本）であり，また日本製が少なく文化の違いもあるが，未成熟である．初心者を主眼とした教育環境には適さない．ここではこれらの諸問題及びその改善について報告する．

情報化社会における安心の確保のためセキュリティは必須のアイテムであり，一般社会に浸透させるためには，「利用者のためのセキュリティ」が必要である．今後の製品開発に期待するとともに一考となれば幸いである．

■ 論文目次 ■

■ 図表一覧 ■

1　はじめに

中部大学は，東海地区名古屋近郊の春日井キャンパスと市内鶴舞の名古屋キャンパスに，6 学部 21 学科，4 研究科 11 専攻の学生数約 8,600 名の総合大学である．これまでにも情報教育及びその環境整備に力を注いできたが，更なる充実のために平成 16 年度の新入生（約２千名）からノート PC 所持の義務化を行った[参考文献 1，2]．

情報リテラシー教育が初･中等教育で行われこれを経た学生が入学する時代を迎え，大学の情報教育もより高度で実践的なものが求められる状況となった．その一つにセキュリティ教育が挙げられる．

ここでは，これを実現するための教育用のネットワーク（「e-Net」と称す．）を整備するに当たっての考慮点，そして２００６年度で３年が過ぎ接続対象台数も６千台を越え，これまでに発生した諸問題とその対応などについて述べる．

1.1　学生の PC 管理状況

企業では，専門部署が利用者の PC 環境を整備（ネットワーク設定・認証に必要なソフトウェアのインストール及びその設定など），配布する．利用者はこれを利用するのみである．

e-Net の利用者（多くは PC 管理の初心者である学生）は，管理者（教育的願望）でもあり，セキュリティ確保のための能力が求められる．

このための講義として「コンピュータ入門」が平成 16・17 年度では 18 学科・40 クラス開講され，1 年生の 96%と多くの学生が受講した．平成 16 年度に行われたアンケート「自宅（下宿）からインターネットが使えますか．」では，Yes- 39.3%，No- 34.2%，Unknown-17.0%の状況であった[参考文献 3]．インターネットが利用できる環境及び体験している学生は，必ずしも多くない．

1.2　利用者の認識

学生に対する情報セキュリティ教育は，大学の責務である．しかし，学生は失うものが見えないもの（信頼など）に対する価値観が社会人とは異なり，認証の必要性を自分のこととして認識できない[参考文献 4]．

また，大学では依然として性善説が根深く，指導する教員自身の意識も必ずしも高いとはいえないのが実情であり，責任の所在も不明瞭となりがちである．

1.3　大学の責任と課題

認証は，情報化社会に必要なセキュリティの入口であり，不正行為を防ぐ布石となる．学生は，大学にとって大切なお客である．その多くがインターネット初心者であり，時には正当な利用でも詐称などのトラブルに巻き込まれる．このような場合，学生保護の観点からも認証及びその記録を保管することが重要であり，正当な利用者の事実証明（使用していない証明も含む）のためにも認証は必須であり，大学の責任でもある．

このような状況下で，ある程度のセキュリティの確保と初心者のネットワーク接続環境の利便性とのバランスが取れた情報セキュリティ環境を整備することが課題となった．

2　e-Net のコンセプト

e-Net の利用者は PC 管理の初心者であること，セキュリティ教育の必要性から次の５つの項目をシステム構築の目標とした．

①　教育専用のネットワーク： VLAN（Virtual LAN），Fire Wall
教育のための運用ポリシーの確立を目指し，他のネットワークと論理的に独立・分離する．位置付けは，外部ネットワークとする．

②　利用責任を持たせるネットワーク： 認証システム
間違ったインターネットの秘匿性意識の排除と防衛及びなりすまし対策（正当な利用者の証明）のために利用者認証を行い，記録を保存する．

③　安全なネットワーク： Fire Wall
内外双方向を基本閉鎖型ネットワーク（大学の Fire Wall は基本開放型が多い）とし，必要なサービスのみを提供する．無線 LAN は，暗号化にも十分考慮する．

④　安心できるネットワーク：Fire Wall, IDS/IPS，ウイルス対策システム
ウイルスの感染・二次感染の防御のためにネットワークを監視し，必要に応じ一時的な通信の休止や通知を行い，予防及び事後対応にあたる．

⑤　利便性の高いネットワークサービス：認証システムなど
ネットワークの環境設定を自動化し，できるだけ簡単で場所や対象（有線／無線，デバイスなど）に依存しない操作の同一化を図る．
利用者（初心者）側からの認証を考え，ネットワーク及び認証の状態を可視化（「見える化」）する．またトラブル時の PC 情報の確認（表示）機能も検討する．

2.1　利用者認証の考え方

利用者認証について利用者が初心者であることから，次のような項目を重点に掲げた．

A)　利用者（PC）に近いところで認証を行う．
一部のネットワーク（例えば，講義室内のみなど）が使用できることによって，責任分岐点が不明確となることも避ける．

B)　認証は，PC（ハードウェア）を対象とするのではなく，利用者（人）を認証する．
PC の管理を強制的に一定レベルにすることができない，そしてセキュリティの基礎教育のために一番基本的なユーザーID／パスワードを使用する．

C)　認証・暗号化のために特別なハードウェア・ソフトウェアを必要としない．
できる限り標準的なハードウェア・ソフトウェアで実現する．

D)　操作が簡単であり，できるだけ同一の操作・概念であること．

① Webブラウザの起動

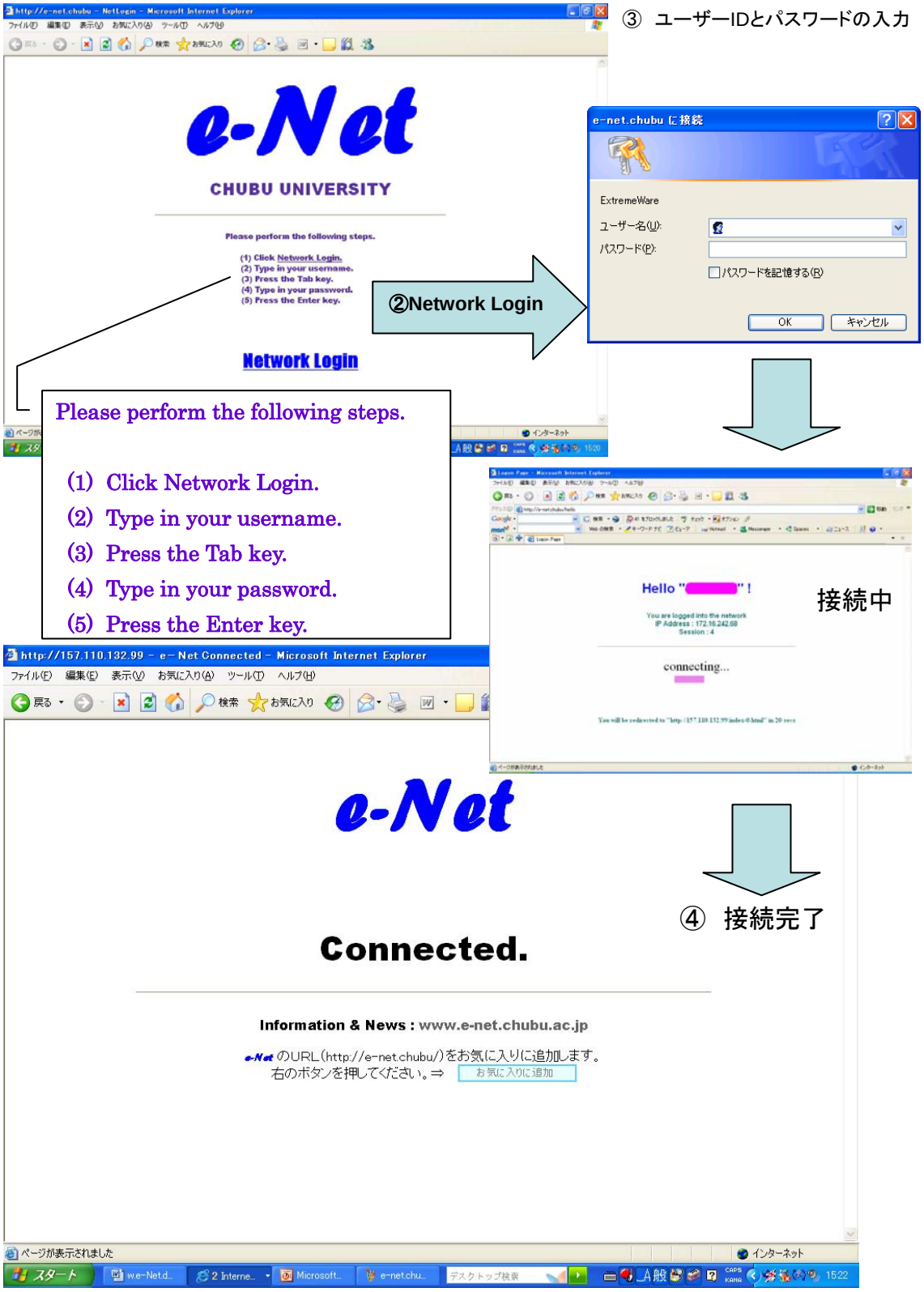


図 1 有線 LAN の認証手順

2.2　有線 LAN の認証手順　（図 1）

PC のネットワーク設定：　「自動的に取得する」（省略値設定）

① Web ブラウザの起動　→「認証画面」の自動表示

② 「Network Login」のクリック　→「ログインポップアップ画面」の表示

③ 「ユーザーID／パスワード」の入力　→「接続中」の表示

④ （約２０秒後）　→「接続完了」の表示

2.3　無線 LAN の認証手順　（図 2）

PC のネットワーク設定：　「自動的に取得する」（省略値設定）

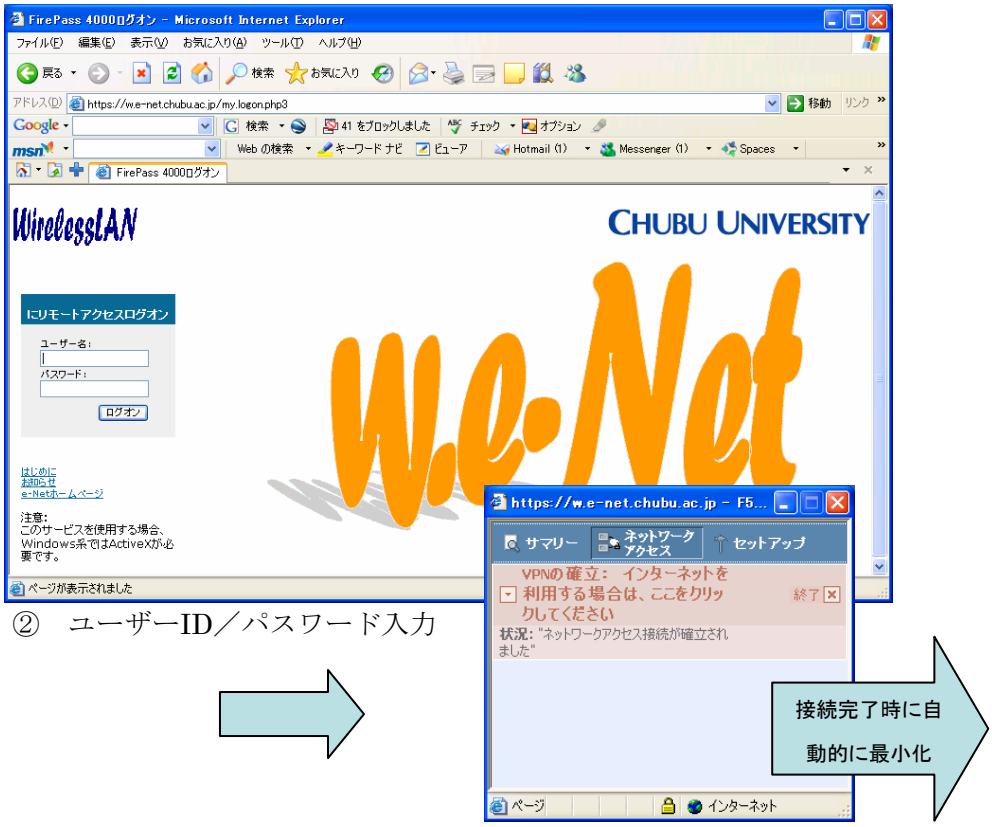
① Web ブラウザを起動し認証サイトにアクセス→　「認証画面」の表示

② 「ユーザーID／パスワード」の入力

→　「接続中」の新たなポップアップ画面の表示

接続が完了した時点で自動的に最小化

① ブラウザを起動し，認証サイト（https://w.e-net.chubu.ac.jp）にアクセス



② ユーザーID／パスワード入力

図 2　無線 LAN の認証手順

2.4　ユーザーID／パスワード

ユーザーID／パスワードは，全学の認証データベースの複製データベースで管理する．e-Net 内にマスター／スレーブの 2 台構成で認証サイトからの問い合わせに応じる．

学生のユーザーID は学籍番号（大文字）の流用（小文字）であり，末尾数字の連番性に対するセキュリティ対策は今後の課題である．

3　問題点と対策

e-Net として掲げた５つのコンセプトすべてを満足する認証システムは，システム選定時には無く，またこの種のシステムは少なく選択肢が限られた．その中で基幹ネットワーク系として導入しているメーカーが，導入時期に後発参入としての発表があり，他に見られない機能（「URL ハイジャック機能」など）があり，導入に至った．

導入以前の検証が不十分であったことは事実であるが，ID／パスワードの入力時間制限（仕様明記なし）について，SE あるいは管理者の導入テストでは発見できない問題であった．内部仕様の不具合の修正適用が別の問題を引き起こし，導入当初は安定稼動ができず，また修正に時間を要した．この中には自大学の運用において発見・改善されたものもある．また，利用が進むに伴い想定外の問題や要望などがあり，これらに対応することとなった．

3.1　有線ＬＡＮの問題点と対策など

(1) 認証サイトのアクセス問題（URL／HTTP ハイジャック機能）

ノート PC は学生の所有物である．このため，責任範囲を大学は情報コンセントまで，学生は LAN ケーブルまでとし，認証を利用者に近い情報コンセントで行うこととした．

図 3 の講義室の LAN 構成では 1 講義室で認証装置（サイト）が 3 台となり，複数となる．利用者は座る位置あるいは利用する場所ごとに認証サイトの URL を適切に入力することが求められる．これでは事実上使用できない．

この対策に認証サイトが持つ「URL ハイジャック機能」を候補し，テストした．この機能は，同一 URL で対象の認証サイトの認証画面を表示させる機能である．ここで e-Net の認証サイトの URL を「e-net.chubu.ac.jp」とすることとした．しかし，実際にはこれが指定できない．原因は，「.」（ピリオド）が２つまでしか使用できない記述形式（文化の違い？）であった．暫定として，「e-net.chubu」（これで URL と説明できない）を使用している．

認証サイトへのアクセス指導は，ブラウザの「お気に入り」への登録を指導したが普及が進まないため，接続完了画面で「お気に入り」登録のボタンを作成した（図 1）．

そして，URL 記述問題の対応の中で，「HTTP ハイジャック機能（正式名称か不明）」が提供された．これはブラウザのホームページ登録のサイトへの http 通信を横取りし認証サイトの画面を表示する機能である．利用者は，ブラウザを起動するのみで認証サイトにアクセスできる．ただし，https，FTP サイトの設定及びプロキシー設定が有効であると機能しない．

なお，現状では利用者は URL の入力を必要としないが，URL 記述の制限は別問題として対応を求めている．

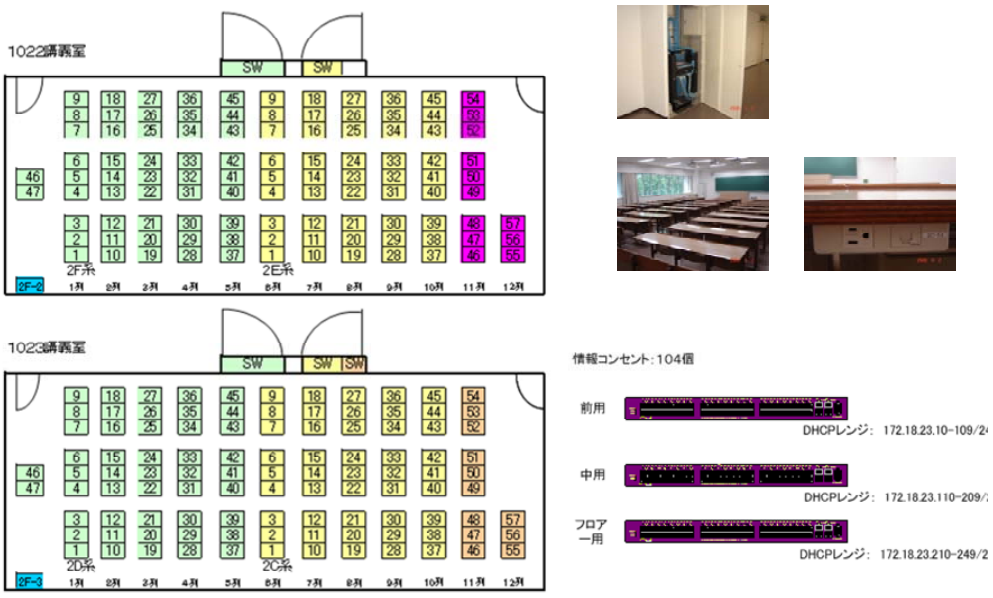


図 3　講義室の LAN 構成

備考：　・装置の騒音問題に配慮し，装置は廊下に設定した．
・机の情報コンセントは，観音開きタイプが望ましい．

(2) ユーザーID／パスワードの入力と入力時間制限の問題

認証システムでは，パスワードの英字の大／小文字を区別する．しかし，一部のシステム（Windows 系など）は，ユーザーID の英字の大／小文字を区別しない．「Caps Lock」状態で入力しても，パスワードの入力文字は表示されず，利用者は正しいパスワードを入力しているつもりであるが，認証に失敗する．初心者はこのような事態でも戸惑う．

また当初，正しいユーザーID／パスワードを入力しても認証できない状況が頻発した．調査の結果，入力に 30 秒以上の時間（入力時間制限）がかかるとエラーとなることが判明した．この仕様の明記は無く設定時間の変更もできない．30 秒は初心者には短く，また障害を持つ人にとっては大きな障壁となる．なお，テスト段階では，SE あるいは経験者が行ったことによって問題とならなかった．

メーカーからの回答は，パスワード攻撃に対するセキュリティ対策の一つとして入力時間を制限しているとのことであった．しかし，パスワードクラックツールによるブル

ートフォースアタックが実際に行われ，数万回のパスワード不一致のエラーログが記録された．1 回の入力時間制限は，昨今のプログラムによる攻撃には何の効力もない．

この対策のため，認証画面をカスタマイズして，ユーザーID／パスワードを効率よく入力する方法（Tab キーの使用など）を画面で紹介することとした．日本語表示ができない仕様のため，止む無く英文とした．簡単な英文であるが，日本語でもなかなか読もうとしない昨今の学生には，英語では効果が薄い．

更に，3 度間違えると図 4 のエラー画面が表示される．網掛けの部分はメーカー名である．この画面は変更できない．この英文が認証に失敗したことを告げる最良の内容とはとても思えない．

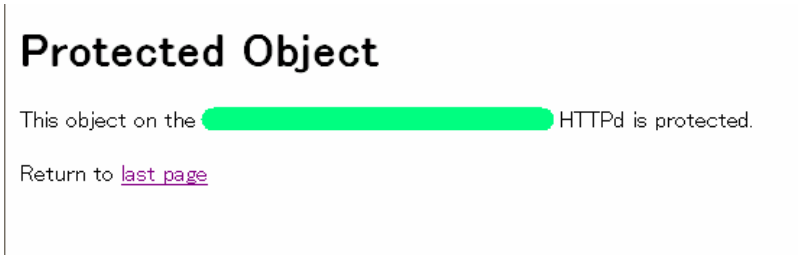


図 4　認証失敗の画面

(3) マルチサプリカント（1 ポート配下に複数端末を接続する形態）接続の問題

図 3 の講義室 LAN の構成では 1 講義室の情報コンセント数は，104 個である．通常では，48 ポートの装置 2 台と 24 ポートの装置（認証機能がある装置）の構成となるが，経費的な問題から一部を認証機能のない装置でマルチサプリカント接続とした．

しかし，マルチサプリカント接続と直接接続（1 ポートに 1 端末）形態では動作が異なることが判明した．教育環境の同一化及びメーカーの障害対応も異なったものとなったため，この形態の接続を止め，直接接続とした．なお，認証ポートの有効利用のため，1 台の認証装置を複数講義室で使用できるような配線に変更した．

(4) Logout の問題

認証の開始動作は，サーバなどの利用開始処理（Login）と同様である．そして，この利用を終了する動作（Logout）を通常必要とする（図 5）．

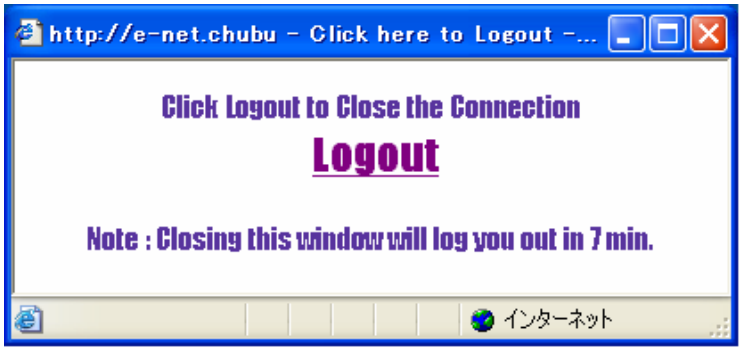


図 5　Logout 画面　（現在この画面は使用していない）

この手順を指導することが本来である．しかし，次の理由で採用しない（できない）こととした．

(a) 画面には，「Note」として注意書きがあるように，この画面を「×」（画面を閉じるボタン）で閉じた場合，約 7 分後（設定時間変更可）に認証が解消され，ネットワークが利用できなくなる．利用者は解消される原因をこれとは気づかない．
何故，画面を閉じた数分後に認証を解消させる必要性（利便性）があるのか理解できない．「×」のボタンを表示させないことは難しいことではない．

(b) この画面は新たなポップアップ画面として表示される．ブラウザのポップアップブロックが標準設定の状況で，利用者はこれを許可する操作が必要となる．表示ができない状況では，画面を「閉じた」と同様な状態となる．

(c) 表示画面の変更ができない．

(d) ログ出力には，正常な Logout 操作とケーブルの切断操作との差異はない．

なお，教育指導上必要であるとの意見もあり，Logout Web サイト（図 6）を作成し，同様なことを実現したが，実際にはほとんど利用されていない．

図 6　Logout Web サイト画面

(5) DHCP（Dynamic Host Configuration Protocol）サーバの問題

・内部／外部サーバの違い

DHCP サーバ（以下,「DHCP」と略す.）は，認証前の暫定 IP アドレス（認証サイトに接続するためのアドレス）の払出と認証後の正規 IP アドレス（ネットワークを利用するためのアドレス）の払出に用いる．認証後の正規 IP アドレスを外部 DHCP から取得するシステムが多い．しかし，次の理由から内部 DHCP を使用し，認証後にも暫定 IP アドレスを正規 IP アドレスとして使用できるシステムを選択した．

ネットワーク利用時に問題となることは，認証後の正規 IP アドレスを何時，誰が利用したかである．外部 DHCP を使用した場合は，そのログには正規 IP アドレスの払い出し時間と払い出した PC のネットワークインターフェースの Physical アドレスが記録されるのみで，ここにはユーザーID の情報はない．ユーザーID は認証前の暫定 IP アドレスの払い出し時に認証サイトのログに記録される．利用者の特定は，ユーザーID 情報とは異なった場所に記録されたログから Physical アドレスをキーに検索する必要がある．

ログの管理が煩雑となり，万一正しい利用者の特定に誤りがあった場合，認証を行う必然性が問われる．また，DHCP の機能が認証システムの一連の処理に必須なものであれば，他の機器（別メーカー）に処理を委ねることは，ある意味責任逃れである．

・DHCP の障害

現在では安定して動作しているが，導入当初は内部 DHCP のシステムバグによって認証画面が表示できない状態が頻発した．メーカーのテスト不足である．

(a) 暫定 IP アドレスが取得できない

(b) 正規 IP アドレスを重複して発行する

払い出し IP アドレスは重複問題発生時の対応として，２倍のアドレスレンジを設定した．e-Net はクラス B のローカル IP アドレスを用い，講義室や自習スペースなどの名称（数値）と IP アドレスの一部を対応付け，障害対応などが迅速にできるように考慮した．

・DNS（Domain Name System）サーバの設定問題

DHCP が提供する情報には，DNS サーバのアドレス情報がある．通常はマスターとセカンダリの２つが定義できる．しかし，現行のシステムでは一つしか設定できない．DNS サーバのダウンは，事実上ネットワークサービスの停止に繋がる．メーカーには改善を強く要望している．現状の対策として別ホストでの代行を準備している．

(6) 無通信監視機能の問題

無通信監視とは，一定時間何も通信がない状態を監視し，通信を切断する機能である．有用な利用の確保のための機能であるが，講義中のネットワーク利用には有効ではなく寧ろ邪魔となる．講義中は認証しネットワークを利用した後，これを使い続けることは少ない．断片的な利用が多くこのたびに再度認証することでは，利便性が乏しい．

この対策として，DHCP のリソース再要求時間を無通信監視の設定時間より短くし，

利用者の意識しないネットワーク利用を行うことで回避した.

3.2 無線ＬＡＮの問題点と対策など

無線 LAN（以後,「w.e-Net」と称す.）の問題点は，接続制限と暗号化の設定である．認証は，e-Net と同じユーザーID／パスワードで行う.

(1) 無線 LAN のセキュリティ機能の放棄

無線 LAN の接続制限は，PC の無線インターフェースの Physical（Ethernet）アドレスの登録による方法がある．対象者が多く，また定期的に利用者の更新がある大学環境では，運営が難しい．また，正常な情報の入手にも課題が多い.

暗号化（WEP，WPA2 など）の設定もこれを正しく適用させることは，初心者には難しく，利用に至らない可能性が高い．このため，無線 LAN 機器が持つ接続制限及び暗号化機能の利用を放棄し，上位層での SSL-VPN を利用したアプライアンスによる利用者認証と暗号化で対応した.

一部にはユーザーID／パスワードの入力時のみ SSL を利用した暗号化通信を行うものがあるが，その後の通信が暗号化されず，これでは e-Net では不十分である.

(2) ActiveX プログラムの問題

専用ツールとして ActiveX のプログラム(４個, 約 1.8MB)を自動ダウンロードする．初回のみの操作であるが, ある程度の時間を必要とする. この間何も状態が表示されず, 利用者は只待たされる．この動作は新たなポップアップウィンドで行われ，これを抑止すると正常に処理できない．今後自動ポップアップが抑止される方向であり，メーカーの改善に期待したい.

(3) 端末間通信の抑止

無線 LAN を経由した端末(PC)間の通信は, ウイルス感染防止のため抑止している．しかし，今後サーバ／クライアントの区別が無くなり，一般的な PC 間でのデータ共有サービスを提供するためには再検討が必要となる.

(4) その他

これまで，研究用の無線 AP（Access Point）の設置については，研究者にその管理を委ねてきた．しかし，周波数の重複，接続制限，暗号化またローミング問題など利用者の個別の問題ではなくなってきた. 大学組織の設備として十分なセキュリティを確保したものを整備する必要があり，今後は研究用の環境にも展開していきたい.

また, AP の設置は, 盗難対策も必要である. 今度の技術動向としては, Wi-Fi の Simple Config 規格（暗号化通信の自動設定規格）の普及が待たれる.

4　e-Net の現状

e-Net の有線 LAN の情報コンセントは，18 講義室（100～250／講義室），11 ゼミ室（～30），9 自習コーナー（～10），その他で合計 2,377 個を有する．一部にディスクトップ PC・プリンタを設置している（対象ホスト接続制限実施）．

無線 LAN（「w.e-Net」）は，AP をゼミ室，自習コーナーを中心に 81 機を配置した．この敷設状況は，「e-Net LAN map」（図 7）として，紙面及び Web で公開している．

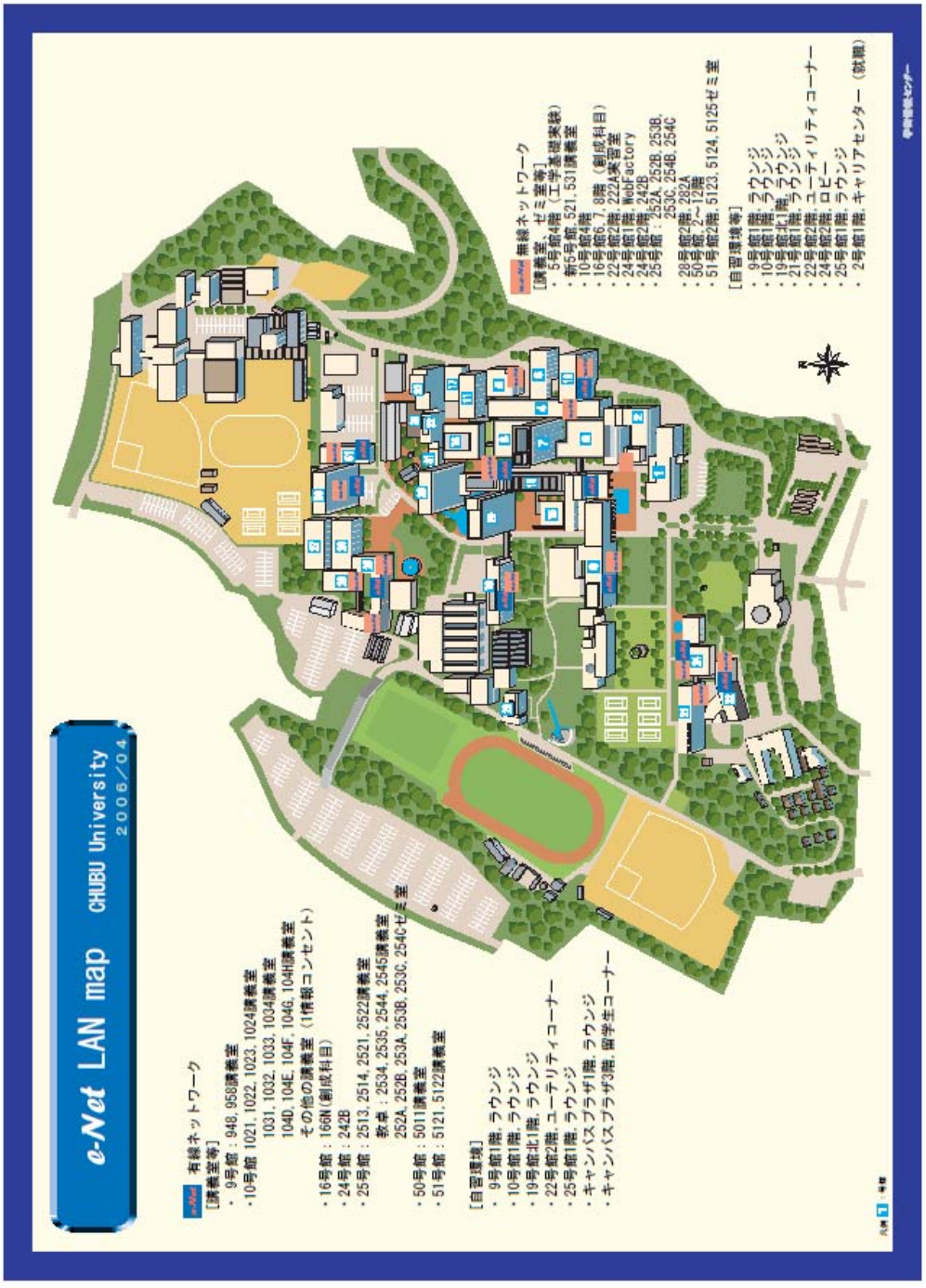


図 7　e-Net LAN map

4.1　e-Net のシステム概要　（図 8）

e-Net は Fire Wall（基本閉鎖型）を介し，キャンパスネットワークと接続している．

e-Net のネットワークポリシーは，次のようである．しかし近年は多くのサービスが http で行われ，セキュリティ的にはサービスポートの制御のみでは不十分な傾向にある．

- ◆ 外部から内部への通信：　できない
- ◆ 内部から外部への通信：　以下のサービスに限定
  - ○ Web，マルチメディアサービス
    http(80,8080), https(443), Real Player(rtsp;554,pan;7070),
    Windows Media Player (mms; 1755)
  - ○ 電子メールサービス
    smtp (25/587), pop3 (110)/pop3s (993), imap (143)/imap3 (995)
  - ○ リモート端末サービス
    telnet (23), ssh (22), ftp(20,21), sftp(115)
  - ○ その他サービス
    時間合わせサービス；ntp (123)
    DNS サービス；　Domain Name Service(53)

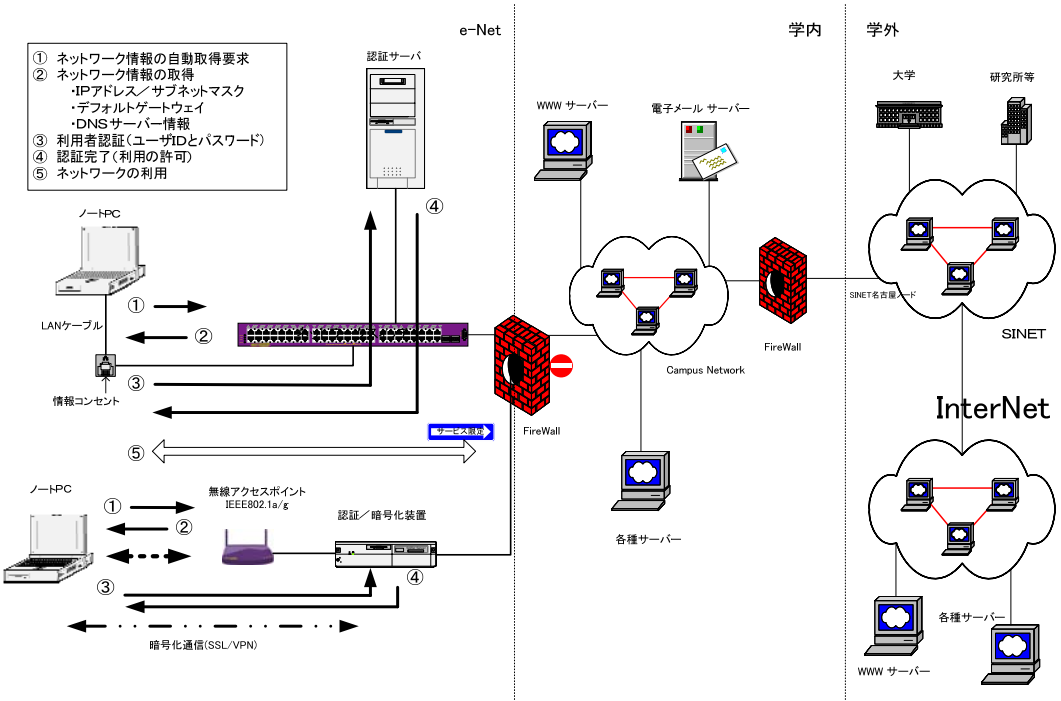


図 8　e-Net の接続概念図

4.2　ウイルス対策　（図 9）

ウイルス対策としては，ノート PC でのクライアント対策をキャンパスライセンスで契約し，実施指導している．そして多層防衛として e-Net の出入口でウイルスチェックを行っている．Web アクセスでダウンロードされる ActiveX や Java，ダウン・アップロードするファイル及び電子メールの送受信が対象である．

ノート PC をネットワークの脅威から保護する目的と，管理が十分でないノート PC がキャンパスネットワーク及びインターネットに及ぼす脅威に対しても同様に防御する．

e-Net 内の端末間通信は，ウイルスチェックを経由しないため対象とはならず，身近な PC からの感染が危惧される．この対策は今後の課題である．

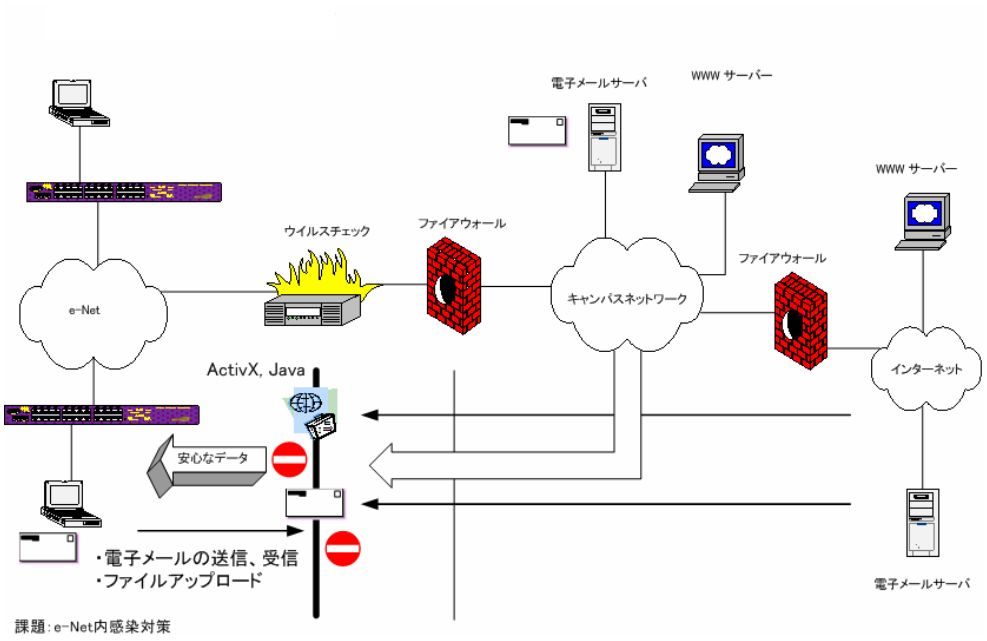


図 9　e-Net のウイルス対策

4.3　検疫システムと IDS/IDP

セキュリティ対策において，近年検疫システムの導入が検討される．しかし，e-Net では以下の理由で導入をしていない（できない）．

- 学生ノート PC は，大学の管理下にない．
- 検疫の手順が標準化（公開）されていない．
- PC の任意の情報がサーバに送られる．
- サーバから PC の任意のコマンドが実行できる．
- 限られたウイルス対策ソフトのみが対象である．
- Windows Update の強制の是非とタイミングが問題である．

ネットワークのセキュリティ対策として，大学が管理するネットワークを対象にこれを通る異常なパケットの遮断対策のために IDS（Intrusion Detection System：不正アクセス監視システム / 侵入検知システム）を導入した．IDS ではこれをタイムリーに解消するらしき機能（RSKILL）がある．しかし，事実上の効果はなく寧ろリセットパケットを送ることによる帯域の圧迫につながった．また，IDS のポートスキャン対策も単独でなく，Fire Wall との連携では即時性に欠け，現実的な対策にはならない．

IDP（Intrusion Detection and Prevention）は，誤動作（認知）回避のためのカスタマイズが大変であり，事実上の効果が得られていない．

5　認証について

認証とは，広辞苑では「一定の行為または文章が正当な手続・方式でなされたことを公への機関が証明すること」．また「本人しか持ち得ない属性を元にその属性を確認し本人であることを証明すること」などの定義がある．

通常認証は，管理者側（正確にはシステム）の立場で使用許可を与えないことが大前提として考えられる．利用者が認識する認証状態（目的のサービスを受ける）との差異が大きく，認証と目的が合致しない．利用者が認証する意義を理解できることが理想である．

5.1　認証状態の可視化（NESSI）

認証（接続）の失敗情報は，認証装置からは拒否のみでその理由もわからない（図 4）．一説には拒否理由の表示は，攻撃の情報に悪用される懸念から非表示とする考えがある．

認証後にも認証が解消される要因は多く，現在認証が正常か異常かを識別（可視化）するようなユーザーの立場にたった補助機能がない．

このため，「準備中」・「未認証」・「認証中」などの状態を表示するツール（愛称 NESSI（ネッシー）：Network State/Situation check program ）を作成・提供した．NESSI は，一定時間ごとに接続状態をチェックし，その状態を 4 つの色（図 10）で利用者に提示する．なお，特定サイトへの PING 応答が得られた場合を認証状態とするのかなどの疑問点はある．

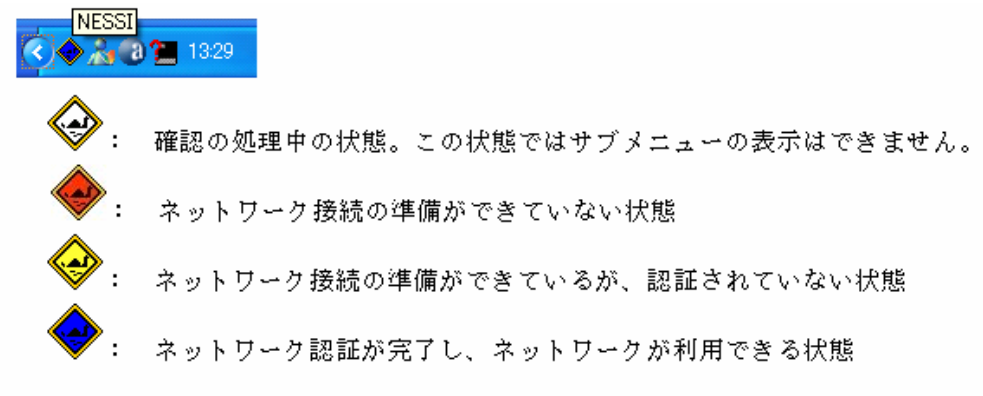


図 10　NESSI

また，トラブル時の対応には，現在のネットワーク接続の設定や状況の把握が不可欠である．しかし，これらを得るためには，専用のコマンド実行あるいは状態確認を表示させるための多くのメニュー（画面）を経由する必要があり，初心者には難しい．このため，NESSI のサブメニューでこれをワンクリックで実行する項目を追加した．その表示結果を図 11 に示す．

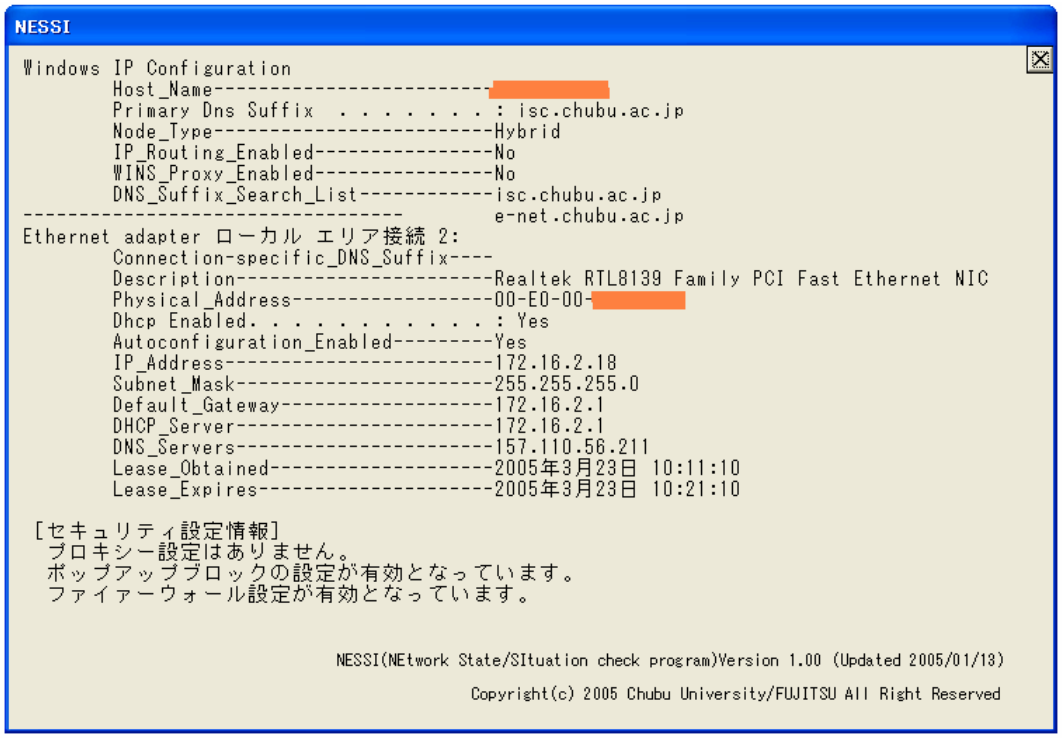


図 11　NESSI（ネットワーク状態表示）

トラブルの発生には何らかの原因があり，これが判明すればトラブルの多くは解決される．システムが複雑化すると各種要因の重複で起こるトラブルもある．

利用者の漠然とした口頭説明のみでは，トラブルを迅速に解決することは難しい．正確な状況（例えば，図 11 の画面ハードコピー）が得られれば，口頭説明以上の情報となる．

5.2　認証状態是非の要件

認証が成立するまたは解消される要件には，次のようなものが挙げられる．システム側の問題もあるが，利用者(PC)側の問題（要件）も洗い出し整理する必要がある．障害・トラブル対応及び学生指導には重要な情報となる．

- 認証システムの障害
- 無通信監視（e-Net では回避）
- PC のネットワーク設定環境の不備
- ユーザーID／パスワードの忘れ
- パスワード表示保護とキーの故障

- PC の Fire Wall 設定
- Web ブラウザ（プロキシー）設定
- インターフェースの休止（スタンバイなど，電源制御）：ディスプレイを閉じる
- LAN ケーブルの切断／障害，情報コンセントの障害
- ログアウト
- （コンピュータ名の重複：メッセージのみ）

6 セキュリティ製品の現状と対応

セキュリティ製品の多くは日本製ではない．これらを導入するには多くの企業を経由しなければばらない．障害時対応には大きな障壁となる．本学の場合，「窓口企業」→ 「販売代理店」→ 「メーカー日本支店」→ 「メーカー本社」（海外が多い）であり，一つの情報確認でも 1 週間以上かかることもある（電子メールでも）．また，販売代理店は複数存在するが，障害情報が共有されず，問題解決に時間がかかる．

そして，最大の問題は障害であることを利用者が説明（証明）し，日本支店が確認して初めて障害対応となることである．時には日本支店が認識した障害は，本社では採用されないこともあり，またその説明責任も十分ではなく，障害の情報公開も乏しい．

セキュリティ製品は，セキュリティの確保と利便性のバランスを保つためのテクノロジーの集約である．製品の信頼性及び担当者の熟練に対するメーカー責任の重要性を再認識して欲しい．

システム管理者は，セキュリティ機器の導入では障害対応・負荷分散と多層防衛を合わせて検討する必要がある．多層防衛は，1 台に集約された UTM（unified threat management：複数セキュリティ機能）製品ではなく，個別専用機が望ましい．他に導入している同一層の製品があれば，設定・管理の面からも望ましい．

更に個別の機器が故障した場合，これを代替する機構あるいは迂回機能（動的で無くても可）を検討し，導入時にテストすることも重要な事項である．

6.1 ユーザーフレンドリな認証システム

情報化社会での安全性確保のための認証は，利用者が自身のためのものであることが認識でき，初めて一般の利用者に浸透する．このためには，利用者側にたったユーザーフレンドリな認証システムが必要である．

昨今では Web2.0 系のサービスが多くなり，今後もこの方向となる．認証システムも Web ブラウザの中（ツールバー含む）で，ユーザーID／パスワードの入力，そして NESSI に相当する機能が必要である．

- ユーザーID／パスワードの入力（パスワードの保存機能なし）
- 接続（認証）状態の表示，自動更新
- PC のネットワーク環境設定状態の表示機能
- ツールバーインストール（更新）プログラム（インストール確認機能有）

また，ネットワーク認証後の各種サービスでのユーザー認証においても，情報レベルに応じたシングルサインオンへの対応も必要である．同一のユーザーID／パスワードを再度入力させる認証システムでは，利用者は使わない．なお，情報セキュリティレベルが違うサービスでは，ユーザーID／パスワードは別管理のものあるいはワンタイム・パスワードなどの考慮も必要となる．

7　おわりに

インターネットの性善説の是非を議論するものではないが，インターネットは今や一部の研究者の利用のみだけでなく一般社会の情報基盤となった．接続のみだけでなく安全・安心できるネットワーク基盤が必要とされる．この環境は一般の利用者が利用する，利用できなくてはならない状況である．

しかし，セキュリティ製品を導入する場合，詳細仕様の公開が少なく未知な部分が非常に多く，また調査にも時間がかかる．製品情報・障害情報が公開され，またユーザーフレンドリなユーザーインターフェースのセキュリティ製品が安定稼動することが必要である．

e-Net では，当初から認証を行うことを前提に利用者側の立場でシステムの構築を行った．これにより少しは，ユーザーフレンドリなシステムとなったものと思う．今後もこの方向で更なる改善を進めていきたい．

最後にシステム導入時に多くの障害が発生し，利用者には大変ご迷惑をお掛けした．特にこれをご指導いただいた先生方の我慢強いご理解があったことをここにご紹介しお礼とさせていただきたい．

参考文献

[１]　清水　幸子：　ノート PC 所有の義務化とその支援体制，私情協・大学情報化全国大会，2004 年 9 月

[２]　岡部　仁：　学生ノート PC による学内ネットワークの活用と認証について，私情協・大学情報化全国大会，2004 年 9 月

[３]　山村　正明：　教養教育科目の区分「情報リテラシー」の現状と課題，初年次情報教育に関する学内シンポジウム，2005 年 5 月

[４]　藤井　康雄，他：　自己所有ノート PC による情報処理教育，情報処理教育研究集会 2005 年 11 月