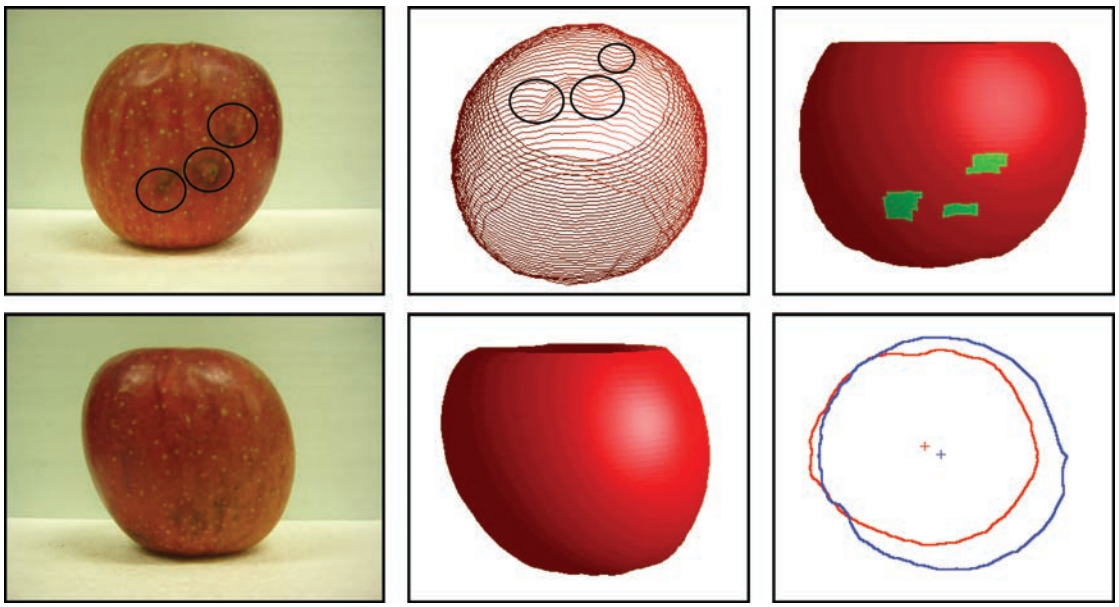
ISSN 1340-654X

弘前大学総合情報処理センター広報

HIROIN

No.21



2004. 3

Hirosaki University Center
for Computer and Communications

表紙の説明

果実形状選別への３次元計測技術の応用

農学生命科学部生物生産科学科　張　　樹　槐
zhang@cc.hirosaki-u.ac.jp

農学生命科学研究科生物生産科学専攻２年　須　藤　洋　史
h02ga301@stu.hirosaki-u.ac.jp

われわれの研究室では，より良い高品質なリンゴ果実を消費者に提供するための選果システムの開発研究を行っています。特に，現在一般的に稼動している選果システムでは計測できない果実の打撲傷の検出や形状の評価方法について，産業・医療などの様々な分野で利用されている３次元計測技術を導入し，その技術のリンゴ選果システムへの応用について検討しています。表紙のリンゴ果実の画像は，本研究室で構築した簡易的な３次元画像生成システムを用いて，果実の虫食い傷や打撲傷の識別・形状の評価方法について得られた実験結果の一例です。

上段の画像
　左：虫食い傷をもつリンゴ果実のデジタルカメラによる可視画像
　中：３次元画像生成システムによって作り出したリンゴ果実の３次元画像
　右：果実の３次元データを基に検出した虫食い傷の結果
下段の画像
　左：いびつな形状をしているリンゴ果実のデジタルカメラによる可視画像
　中：３次元画像生成システムによって作り出したリンゴ果実の３次元画像
　右：赤い線と青い線は，それぞれリンゴの頂面（ヘタ部）と底面（果梗部）の円周形状を表しており，＋マークは各断面の形状データを基に計算した重心位置です。これらの重心位置のズレと果実の高さの値を用いていびつ形状係数を算出し，果実形状の良し悪しを評価しようと考えています。

（写真：農学生命科学部生物生産科学科　張　樹槐 氏　提供）

目　　次

巻 頭 言

コンピューター情報と教育面の見込み違い

農学生命科学部長　豊　川　好　司

toyokawa@cc.hirosaki-u.ac.jp

パソコンは多機能で、多くの用途に利用できます。最近では新しい器械などに順応の苦手な高齢者も会社などで覚えたパソコンを使って、メール交信や趣味を広げるなど、愉しんでいるようです。

私にとってのパソコンは、しばらく振りにパソコンに対峙するとすっかり操作方法を忘れてしまっているので、ついつい大儀になって研究室の飾り物のようになっていました。振り返ってみるとパソコンと向き合う時間を積極的に作らなかったことと、自然現象かと思っている？記憶力低下もあって当然の成り行きでもありました。最近ようやく活用範囲の広い威力を理解するに至りました。そして周知のようにパソコンの操作は何もかも覚える必要はなく、自分に必要な使い方を知ると利用・活用の幅を広げてくれる手段となります。しかし人間の生き様の中にこれだけ広く深く入り込んだパソコンと人類の存続との関係には脅威を覚えます。

大学教育の中で最近先生方からよく聞くことは、リポートを課すと文章は言うまでもなく文字までほとんど同じ内容のものが見られ、パソコンからの情報収集によっていることが分かる、ということです。さらに情報をつなぎ合わせる作業で終わっているので、専門知識として記憶されていないことが期末試験結果に表れているので、授業方法の連続性に結びついていないということです。学生達が期限に追われてリポートを作る一面的事情はありますが、私にはリポートのこのようなことは、教育思考の基盤としてインターネットを介し、短絡的な自律的個人主義方向を強化していると思います。大学の高次とされる知識形態のなかでコンピューターの影響がどんどん大きくなり、これらのデータ・情報を思考の基礎として受け入れる考え方が広まっていると思いますが、コンピューターと私たち人類との出会いはまだ短く、文化、特に人間の精神的・内面的主観に対し、コンピューターはどのような価値を持っているのか分かっていないと思っています。コンピューターの展開と合わせて、コンピューター文化をしっかりと論じておくことが求められていると考えています。

学生達には統計計算は理屈抜きでもコンピューターが瞬時に答えを出すことが至極当たり前なことですが、私の若い頃はと言うと、サンプル数が少し多いとタイガー手動計算機を一ヶ月は回しましたから、パソコンは便利この上ないものです。手紙の例で言うと、外国とのやりとりでは約２週間はかかるのが、メールでは瞬時で届くのですから、地球規模の距離感がなくなりました。時間が無いとか、急ぐ場合には本当に有り難い器械です。大学の授業を配信したり、仕事のデータを蓄えたり引き出したりするなど、色んなことを積極的に取り込みたい人にはコンピューターは一見して有り難いテクノロジーと思います。

一方、興味のない情報が自分のパソコンに勝手に入りこみ、はたまた他律的・中傷的情報も入り乱れて、コンピューターはテクノロジーが人類文化にもたらす恩恵を衰退方向へ導いている状況があるように思います。しかし、今やコンピューターは私たちの文化生活の中で消し去ることができないものになっているようです。

ともあれコンピューターからはこんなことまでもと思える、大百科事典も比較にならない多くの情報を得ることができ、率直にたまげています。

解　説

便利は危険

理工学部電子情報システム工学科　吉　岡　良　雄
slyoshi@si.hirosaki-u.ac.jp

1．インターネットとモラル

日本において，1993年（平成５年）頃からインターネットが急速に発展してきたことはよく知られています。これは，安価なマイクロプロセッサの開発によって，安価なパーソナルコンピュータの開発とインターネットの展開が相乗的（シナジー効果）に急速に進んできたことによります。そもそもインターネット（コンピュータネットワーク）は1968年にアメリカ国防省が大学に研究委託して，研究用ARPAネットワークを構築したことから始まっています。当時は，東西冷戦時代であり，１つの大型コンピュータに情報や機能が集中して置かれていた時代でもありました。このため，そのコンピュータが攻撃され破壊された場合に，アメリカ国内のすべてがマヒしてしまうという懸念がありました。この解決策として，複数のコンピュータを通信回線で接続し，情報の分散配置や機能分散を図って，一部のコンピュータが破壊されても，国全体として機能を維持することができることを狙ったものです。そして，大学や研究所などによってインターネットの研究が始まり，徐々に拡大してきました。研究レベルでの利用ではモラルが自然に守られていました。しかし，平成５年頃に一般の利用者にまで拡大したことから，不正アクセス，情報の改ざん，情報の窃盗，嫌がらせメール送信，ウィルス送付，等の不正利用が横行し，さらにホームページによる雑多な情報（間違っている情報や公序良俗に反する情報など）が氾濫し，利用しにくくなってきています。そのように感じるのは私だけでしょうか？

2．インターネットなしでは研究が進まない

現在において，パソコンやインターネットはあたりまえのように利用されるようになってきました。大学においても，インターネットやパソコンが整備され，レポートは電子メールで，専門用語はホームページ検索で，データ整理はエクセルで，卒業研究発表はパワーポイントで，などといったように，パソコンやインターネット利用が多くなってきています。また，研究面においても，情報検索や論文検索，学会発表や論文投稿，査読などがホームページや電子メールで行われるようになり，非常に単期間でそれらが行われるようになってきました。「情報を制するものは世を制す」といわれているように，インターネットによって情報をいち早く収集して，人より早く新しい研究を進めることができるようになっています。いわゆる，インターネットなしでは，もはや研究も進まなくなったといっても過言ではありません。

3．添付ファイル付きメールは危険

最近，インターネットのインフラが整備され，通信容量も増え，以前のようにファイル転送に時間がかからなくなりました。電子メールにおいても，大きなファイルを添付して送ることも容易になってきました。電子メールで安易にファイルを添付して送ることは，ネットワークトラヒックの増大，ファイルサーバの負荷増大，コンピュータウィルスの伝播など，利用者の見えない場所で悲鳴をあげていることになります。ネットワークトラヒックの増大やファイルサーバの負荷増大は，ネットワークの応答時間を長くするとともに，ネットワーク全体がダウンしかねないことになります。このことは，エネルギー損失であるとともに，昨今のように仕事（研究）がインターネットに依存している以上，仕事（研究）の損失とな

ります。また，添付ファイルは，コンピュータウィルスを簡単に伝染してしまい，多くの人に迷惑をかけることになります。特に，メーリングリストで添付ファイルを送ると，コンピュータウィルスを一瞬のうちにばら撒くことになり，悲惨なことになりかねません。メールでの安易な添付ファイルはやめましょう。コンピュータおよびコンピュータネットワークの仕組みを理解し，正しくかつ人に迷惑をかけないように利用しましょう。

4．各自バックアップを

インターネットにパソコンを接続していると，知らないうちに個人情報や大事な情報が盗まれたり，いたずら（情報破壊など）されたりします。インターネットにパソコンを接続するということは，玄関の戸を開けて留守にするようなもので，どうぞ盗んでくださいといっているようなものです。また，インターネット接続パソコンを利用して，電子メールを読んだだけでも，またホームページにアクセスしただけでもウィルスに感染してしまいます。パソコンが一度ウィルスに感染してしまうと，OS（Windows）を含めすべてのソフトや大事な情報を消去しなければなりません。従って，大事な情報は，こまめにフロッピーディスクやCD-Rのような媒体にバックアップしておくことが必要です。以前のような小容量ハードディスクのホストコンピュータ（ファイルサーバ）であれば，情報処理センターなどで一括バックアップが行われていました。しかし，最近では音声や画像（動画）などのファイルを扱うようになったため個人で扱うファイル量が膨大になり，情報処理センターだけで一括バックアップすると数日かかってしまいます。バックアップ中は通常利用できません。最近，数分でもインターネットが利用できないと，情報処理センターに苦情がきますので，情報処理センターでの一括バックアップは不可能といっても過言ではありません。このため，最近では各自バックアップを取ってもらう方向になってきています。従って，大事な情報をパソコンに入れておきたい場合には，インターネットには接続しないことが必要です。

5．コンピュータへの過信は危険

“コンピュータが計算したから絶対正しい”という言葉をよく耳にすることがあります。コンピュータのソフトウエア（Windowsなどの基本ソフト，ワードやエクセルなどの応用ソフト等）は人間が作ったものであるため，必ずといってよいくらいバグ（誤り）があります。すなわち，プログラム（ソフトウエア）のコーディング直後では，統計的に1000行のプログラムに対して約20個のバグがあるとされています。その内，出荷までに約13個のバグが取り除かれ，残り約７個のバグは世に出てから利用者の苦情によって直します。最近のソフトウエアには何十万行というものが少なくありません。仮に，10万行のソフトウエアがあったとすれば，出荷されたソフトウエアには約700個のバグが潜んでいることになります。従って、“バグが全くないというソフトウエアはない”ということになります。そのようなソフトウエアを利用して出力された結果は果たして信用できるでしょうか？人の作ったソフトウエアで仕事（研究）をしているということは，雲の上で仕事（研究）を行っているのと同じです。コンピュータが出力した結果を過信すると，いずれ地上に叩き落とされることになります。コンピュータから出力した結果は必ず検証しましょう。

6．便利であることは危険

以上述べてきたように，インターネットの普及によって，あらゆる分野において便利になってきました。自分にとって便利であれば，他人にとっても便利であるということです。すなわち，便利であるということは，それだけ危険であるということです。便利にしろとか，便利だから云々と言われるが，その分危険性が増すことを十分認識しておかなければなりません。

インターネットセキュリティ技術

理工学部研究協力係　佐　藤　勝　人

miri@cc.hirosaki-u.ac.jp

概　要

サーバ管理者は、自分自身が管理運用するサーバに対して、サービスが停止しないように保守することと同時に、不正侵入されないようにネットワークセキュリティに対して管理運用を行うことが不可欠になってきた。本テーマでは、国立情報学研究所が主催した平成15年度第３回情報セキュリティ担当職員研修上級コースを筆者が受講した際に修得した知識と技術を交えながら、ネットワークセキュリティについて解説する。

1．はじめに

ネットワークセキュリティについて、TCP/IPアプリケーションプロトコル上で提供できるサービスは、比較的手軽に実装・使用することができる。しかし、手軽さと引き替えにセキュリティに対しての対策が整備されていない。そこで、ハッカーによる攻撃や不正侵入の現状を把握して、適切な措置を行い、常にサーバサイトを監視することが重要である。本テーマでは、さまざまなサービスの弱点と対策、不正アクセスの検出や発信元の追跡を行うためのログ分析、セキュリティの診断・監視についてどのように対応していけばよいかを解説する。

2．TCP/IPアプリケーションプロトコルの弱点

ネットワークを利用するアプリケーションは、主にトランスポートプロトコルとして、TCP（Transmission Control Protocol）とUDP（User Datagram Protocol）を利用する。今回は、TCPプロトコルの弱点について主に解説する。

2.1　TCPコネクション

TCPコネクションは、3Way-Handshakeという手続きを実施することにより、信頼性のある通信を提供する。送受信されるデータの各バイトに一連の番号（シーケンス番号）が付けられており、データを受け取った側では、どのシーケンス番号までを受け取ったかを送信元へ応答することで、送信側はデータが正しく相手に届いたことを確認する。

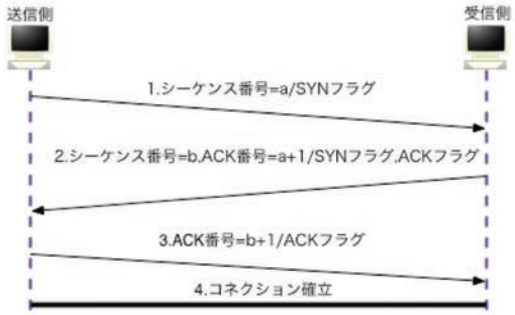


図１.3Way-Handshake

3Way-Handshakeは、送信側のホストから受信側のホストに対してSYNフラグを送信する。次に受信側のホストから送信側のホストに対して、SYN、ACKフラグを送信する。最終的に送信側のホストから受信側のホストにACKフラグが送信されて、コネクションが成立する。その後のやり取りされるデータには全てACKフラグが添付される。

・3Way-Handshakeの正常動作の確認方法

Windowsでは「ネットワークモニタ」ツールを利用すればよい。その他のOSではフリーツールのLANアナライザソフトを使用すればよい。

2.1.1　IP Spoofing Attack（IPなりすまし攻撃）

TCPコネクションを設定する際に行われる3Way-Handshakeの特性を利用して、送信元を同じにしたパケットをインターネット側から送り込むことで、ファイアーウォール内からの通信であるかのように見せかけ、内部へ侵入しようとする不正アクセスの方法である。IP Spoofingは、IPパケットのIPヘッダ情報だけの仕組みを悪用した攻撃である。

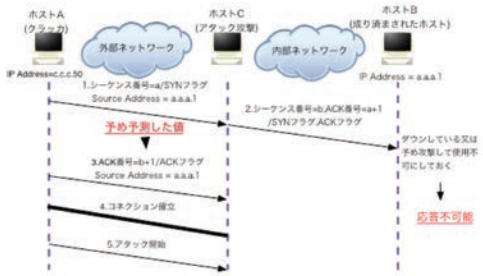


図２.IP Spoofing Attack

・対策

ルータ等の設定で、外部から送られてきた内部アドレスをソースアドレスとして使用しているパケットを廃棄するようにパケットフィルタを有効にする。

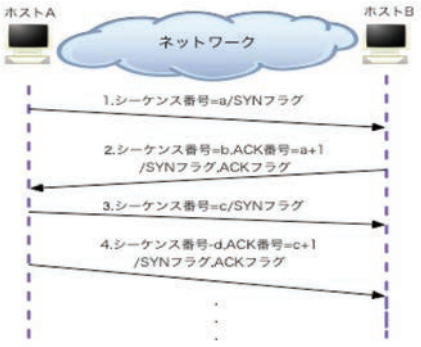
関連RFC：RFC1948シーケンス番号攻撃を防ぐ（Defending Against Sequence Number Attacks）

2.1.2　SYN Flood Attack

TCPコネクションを確立するための３Way-Handshakeを悪用した攻撃方法である。アドレスを偽造したクライアントから大量のSYNパケットをサーバに送りつける。サーバ側が受け取ったSYNパケットに対してACK/SYNパケットを送り返し、

クライアントからのACKパケットの待ち状態に入る。しかし、偽造されたアドレスからのACKパケットの返答がないため、サーバはACKパケットの待ち受けが大量に発生し、正常なアクセスを受け入れられなくなったり、システムクラッシュを引き起こすなど障害が発生する。

図３.SYN Flood Attack



SYN Flood Attackは、受信側のホストでは、SYNフラグを送信してきたときにバッファを確保するが、攻撃側（送信側）は、一方的にSYNフラグだけを大量に送信して一種のDOS攻撃に近い状態になり、受信側のホストが不能になる。

・対策

ネットワーク内でやり取りされるSYNパケットを識別するのは不可能であり、ハッカーも自分がばれないようにいろいろなアドレスを使用してくる。対策としては、OSの機能を利用して以下の設定を行う。

１．HalfOpenの最大コネクション数を制限する。

２．HalfOpenのコネクション数が増加した際に、バッファを確保しないようにする。

ホストの動きが遅くなってきた段階で、そのホストに対して同一のホストからSYNパケットが連続して送信されていることを確認した場合には、ルータやファイアーウォール等のフィルタリング等を行う事後対策を行えばよい。

関連RFC：RFC2827ネットワークのイングレスフィルタリング（Network Ingress Filtering）

2.1.3 IPソースルーティングの悪用

普通のルーティングは、ホップバイホップルーティングといい、各中継ルータが、パケットに記載された宛先ホストアドレスと経路表を参照して経路を決定する。IPソースルーティングは、IPプロトコルのオプションで発信者が宛先に届くまでに中継するホストを指定する。ソースルーティングは、IPヘッダ内の宛先IPアドレスを発信者が経路指定したアドレスで変化させながら通信する。この特徴を悪用して不正侵入を行う。

・対策

ルータ、ファイアーウォール、サーバでIPソースルーティングを禁止する。

2.1.4 フラグメントを利用した攻撃

フラグメントとは、パケット（データ）を分割する機能で、ネットワーク・インタフェースが所属するネットワークのMTU（Maximum Transmission Unit、ネットワークが送信できる最大の伝送単位：Ethernet上で扱えるMTUは1500バイト）サイズ以上のパケットを送信する場合に、元のパケットを分割して、MTUサイズ以下にして送信する。１回細分化されたパケットは、受信したマシン内部で再構成される仕組みになっている。

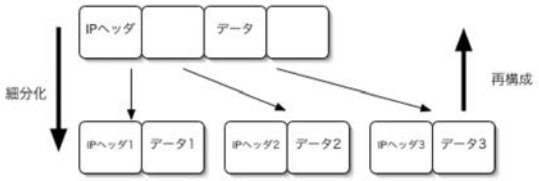


図４.IPパケットの正常な細分化/再構成

このフラグメントの機能を利用して以下の２種類の攻撃がある。尚、これらの攻撃は、IP層のファイアーウォールでのパケットフィルタリングの場合にのみ確立する。

・タイニーフラグメント攻撃

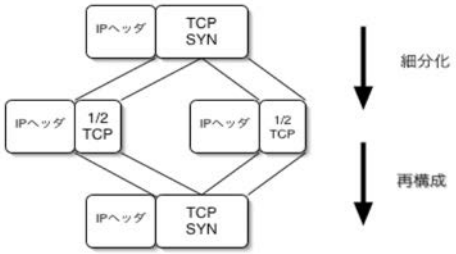


図５.タイニーフラグメント攻撃

IPパケットの分割機能を利用して非常に小さな断片に分割することにより、パケット・フィルタリングをすり抜ける攻撃方法である。IPヘッダの後に続くTCPヘッダが分割されることにより、パケットフィルタリングで確認する際に、TCPヘッダの残りの部分（SYNやACKなどの制御フラグなど）の位置にデータが無かったり、２番目のパケットに入ったりするため、パケット・フィルタリングを不正に通過してしまう。最終的に受信したマシンで再構成されると、TCPヘッダが完成されるため、3Way-Handshakeの１番目のパケットが正常に処理される。

・オーバーラッピングフラグメント攻撃

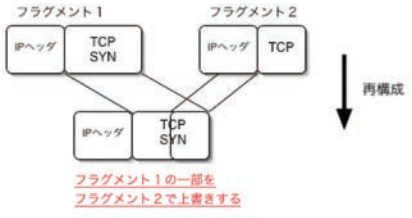


図６.オーバーラッピングフラグメント攻撃

IPパケットの分割機能を利用してオフセットが重複するような断片を生成し、パケット・フィルタリングをすり抜ける攻撃方法である。２番目以降の断片のオフセットを先頭の断片と重複させることにより、パケットフィルタリングを通過できないような

パケットでも通過させてしまう。再分化された状態では、TCPヘッダにSYNが無くても、受信したマシンで再構成されるとSYNが現れる。

その他のフラグメントを利用した攻撃としては、不正なサイズ（極端に大きい又は小さい）フラグメントを送信することで攻撃対象のホストを不能にさせる攻撃もある。

関連RFC：RFC1858IPフラグメントフィルタリングについてのセキュリティ上の考察（Security Considerations for IP Fragment Filtering）

3．TCP/IPアプリケーションプロトコルによるサービス

3.1 DNS：Domain Name System

DNS（ドメイン名解決システム）とは、IPアドレスのように各マシンの識別を数字で行っているが、人間側で数字が扱いにくいことから、文字を使用して名前を付けることが出来るようになっている。

・問題点

1）名前情報漏洩の危険性

DNSサーバは、名前やIPアドレスの問い合わせに対して、持っている情報をすべて答えてしまうことから、ハッカーはこの名前情報（名前とIPアドレスの対応を示す情報）からクラックを実行するための必要な情報を容易に収集することが可能である。また、ハッカーは自分のDNSサーバをセカンダリサーバに設定することで、プライマリサーバ上の名前情報のコピーを入手することも可能である。

2）名前情報改ざんの危険性

ハッカーは、アクセス制限をホスト名で行っている場合は、DNSサーバの情報を改ざんして、自分のIPアドレスと組織内のホスト名を対応付けすることにより、侵入を容易に行うことができる。侵入が成功すると、BSD系UNIXのr系コマンド（rsh、rlogin等）を実行して攻撃される。

・対策

1）名前情報漏洩への対策

インターネットに公開するDNSサーバは、インターネットに公開しているサーバの情報だけを登録する。セキュリティ対策として公開用のDNSサーバは、内部（組織内LANシステム）と外部（例えば、インターネット）の境界に設置するLANセグメント（LANの構成単位）上に設置する。組織内情報を扱うDNSサーバは、組織内ネットワークに設置することにより、組織内のDNSサーバには外部ネットワークからのアクセスを防ぐことができる。

2）名前情報改ざんへの対策

公開用DNSサーバを要塞化して、DNS情報を改ざんされないようにする。名前情報は定期的にチェックして、不審な情報が無いかを確認する。

DNSサーバには必ず逆引きデータを登録しておく。アクセスを受ける側のサーバでは、DNSの逆引きを利用して通信相手のアドレスの正当性をチェックする方法もある。

関連RFC：RFC2535DNSセキュリティ拡張（Domain Name System Security Extensions）

関連RFC：RFC2845DNSのための秘密鍵処理認証（Secret Key Transaction Authentication for DNS（TSIG））

3.2 電子メール（SMTP、POP）

電子メールは、ネットワークアプリケーションの中で一番多く利用されている。このアプリケーションは、非常に高機能であり様々な機能を実現できるが、この機能を悪用された場合には、広範囲に被害が生じる可能性が高い。

・問題点

1）sendmailのセキュリティホールへの攻撃

フリーソフトで有名な電子メールサーバであるsendmailは、多機能な反面、セキュリティホールを多く抱えている。その中で、ハッカーはsendmailが持つデバック機能を悪用することにより、メールサーバに成り済ますことが可能である。sendmailの特有な部分である、受信したメールをスプール中に書き込むための特別な権限を持って動作する機構を悪用されることが多い。

2）ユーザアカウントのパスワードクラック

メールサーバを利用するために登録するユーザのアカウントの数が増加することで、管理が行き届かないところで望ましくない簡単なパスワードを設定するユーザが出てくる。ハッカーにとっては、最適な標的となる。

3）メール爆弾

メールサーバを使用不可にするために、大量のメールを送りつける攻撃である。その結果、メールサーバは過負荷状態になりダウンしたり、メールのスプール領域をあふれさせてメールを使用不可にする。

4）メール内容の盗聴

普段やり取りしているメールの内容は、暗号化されずに平文で送受信される。そのため、途中のネットワークやメールサーバで盗聴される可能性がある。特に、盗聴の危険性を認識していない状態で、機密情報をメールでやり取りするのは機密事項の漏洩につながるので注意が必要である。

5）POPのIDとパスワードの盗聴

メールの内容と同様に、POPを利用してメールサーバ上のメールを読む際にユーザIDとパスワードの入力が必要になるが、この情報も暗号化されない。よって、盗聴することでユーザIDとパスワードを確認することができる。

6）SPAMメール中継

SPAMメールやメール爆弾の中継にメールサーバが利用されることにより、知らないうちに悪用され加害者扱いにされてしまう場合がある。

・対策

1）sendmailのセキュリティホールへの攻撃への対策

セキュリティホールが修正された最新バージョンのsendmailを使用する。sendmailで利用する設定ファイル群（メールをスプールするディレクトリ等）のパーミッション設定に注意する。

2）ユーザアカウントのパスワードクラックへの対策

内部と外部の境界に設置するLANセグメント（LANの構成単位）上にメールサーバを設置して、メールの中継だけを行うように設定する。このメールサーバには、組織内のネットワークに実在するユーザアカウントなどの設定をしないようにする。

3）メール爆弾への対策

根本的な対策はないが、メール爆弾を受けた場合に、攻撃を仕掛けてくるメールサーバからのメールを受信しないように設定することで対応するしかないようである。

４）メール内容の盗聴への対策
SSL等を利用してメールの暗号化を行う。
５）POPのIDとパスワードの盗聴への対策
メールサーバを分散させて信頼できるネットワーク内に限定してPOPを利用できるようにする。また、パスワードを暗号化できるAPOPと呼ばれる認証方式を使用することで、盗聴されずに済む。
６）SPAMメール中継への対策
メールサーバの利用形態のうち、他のサイトから受信したメールを更に他のサイトへメールを中継する場合に、中継を制限していない場合には、SPAMメール中継に不正利用される可能性がある。実際のメールサーバの利用形態は、
㈠ 自サイト内のユーザ間のメール配送
㈡ 自サイトから他サイトへのメール送信
㈢ 他サイトから自サイトへのメール受信
以上の形態で運用すればよい。
「POP before SMTP」や「SMTP Auth」を用いてメール送信時にユーザ認証を行う方法もある。

3.3 ファイル転送（FTP：File Transfer Protocol）

FTPとは、ネットワーク上に設置してあるコンピュータ間でファイル転送を行うようにするプロトコルである。FTPのタイプは、大きく分けて２種類に分かれる。１つは、利用者がFTPサーバに接続を要求する際に、ユーザIDとパスワードの認証を行う方法で、もう１つは、不特定多数の利用者に対して匿名のアカウントで利用できるanonymous-FTPがある。
・問題点
１）ディスク、ファイルのパーミッション設定変更による攻撃
FTPサーバ上のパーミッションの設定で、書き込み禁止の設定漏れを発見して、.rhostsに対して書き込みを行うことで、rlogin等を使用して侵入する攻撃がある。
２）公開用FTPサーバを利用したファイルの受け渡し
情報公開用のanonymous-FTPサーバで、ディレクトリに対して書き込みを許可する設定にしている場合は、ハッカーの情報交換の場としてファイルの受け渡しに使用される可能性がある。
３）公開用FTPサーバへの使用不能攻撃
情報公開用のanonymous-FTPサーバなどで、ディレクトリに対して書き込みを許可する設定にしている場合は、大量のファイルを書き込むことでディスク容量を浪費させる攻撃がある。
・対策
１）ディスク、ファイルのパーミッション設定変更による攻撃への対策
anonymous-FTPを使用する際に、ディレクトリやファイルのパーミッションの設定、アクセス範囲の限定に注意する。その中で、/etc/passwdファイルや実行ファイル等に対してアクセス拒否の設定を行う。更に、chrootコマンドによってanonymous-FTPのルートディレクトリを変更して、設定されたディレクトリの配下以外のアクセスができないように設定する必要がある。できれば、anonymous-FTPの使用は控えるべきである。
２）公開用FTPサーバを利用したファイルの受け渡しへの対策
anonymous-FTPは、読み出し、書き込み両方を許可するディレクトリは作成しないようにする。
３）公開用FTPサーバへの使用不能攻撃への対策
書き込み可能なディレクトリを準備する場合には、そのディレクトリに対して書き込み容量の制限を行い圧迫されないようにする。
関連RFC：RFC2577FTPセキュリティについての考察（FTP Security Considerations）
関連RFC：RFC1579ファイアウォールと親和性のあるFTP（Firewall-Friendly FTP）

3.4 ファイル転送（TFTP：Trivial File Transfer Protocol）

TFTPは、主にディスク装置を持たないX端末やルータ、スイッチングHUB等のネットワーク機器からブートするために必要なファイルを転送する目的で使用されているファイル転送プロトコルである。
・問題点
TFTPは、ユーザ認証機能がないので自由にアクセスできてしまう。UDPを用いてファイル転送を行う際に、ファイアーウォールでのアクセス制限の設定が困難である。
・対策
TFTPの使用は厳禁である。どうしてもやむを得ない場合には、ファイルの書き込みを禁止する。

4．TCP/IPアプリケーションプロトコル以外の問題点

4.1 無線LAN（IEEE802.11）

無線LANは、電波を使用した無線通信で構築されたネットワークをいう。

表１.主なIEEE802.11実装の比較

	802.11g	802.11b	802.11a
最大データレート	54Mbps	11Mbps	54Mbps
最大データレートの有効範囲	18m	45m	12m
周波数帯域	2.4GHz	2.4GHz	5GHz
全世界で利用可能	○	○	○
消費電力	1.5W	1W	2～2.5W

4.1.1 無線LANのセキュリティ管理

・無線LANアクセスポイントのセキュリティ対策
１）SSID（Service Set Identity：通信グループ名）
SSIDは、インフラストラクチャーモード（アクセスポイントを経由した通信）のESS-ID（Extended Service Set Identity）とアドホックモード（アクセスポイントを経由しない２台同士の通信）のBSS-ID（Base Service Set Identity）の総称で、グループ分けに使用する名前で、他の無線LANクライアントからは、通常確認できる。
・SSIDの 問題点
SSIDは、セキュリティの面から見ると、アクセスポイントのメーカー名の一部を用いたり、講座名、教官の名前の一部を用いることで、どの場所で何のメーカーのアクセスポイントを使用しているか容易に確認できてしまう。

・SSIDのセキュリティ対策
　最終的には、アクセスポイントのステルス機能を用いて、SSIDを隠しておくことにする。SSIDのID認証とMACアドレスの認証機能を組み合わせる。
２）MACアドレス（Media Access Control Address)
　MACアドレスは、各イーサーネットカードに固有のID番号で、全世界のイーサーネットカードに１枚ごとに固有番号が割り当てられており、この番号を元にカード間でデータの送受信が行われている。
・MACアドレスの問題点
　MACアドレスは、全世界で１つの固有のID番号であるが、プログラムを利用してMACアドレスを変更することで、詐称することができる。
・MACアドレスのセキュリティ対策
　アクセスポイントで、MACアドレスによるフィルタリングを行い、登録されていないクライアントからのアクセスを拒否する。
３）WEP（Wired Equivalent Privacy）
　無線通信で送信されるパケットを暗号化して有線通信と同様の安全性を持たせるための暗号化技術で、旧方式の64bitのデータを使う方式と、新方式の128bitのデータを使う方式の暗号化キーが用いられている。
・WEP の問題点
　WEPは、ユーザー認証機能が無く、暗号化に脆弱性が存在し、状況によって容易に解読が可能となる。
・WEP のセキュリティ対策
１．128bitで16進数の暗号化キーを用いる（試行期間中はクライアント側の互換性重視して64bitの暗号化キーを用いている。）
２．802.1xのポート単位の認証プロトコルを用いる。
　今現在、本無線LAN構築のシステムにどのようにIEEE802.1xを導入するか検討中である。後の章でIEEE802.1xシステムの仕組みを報告する。

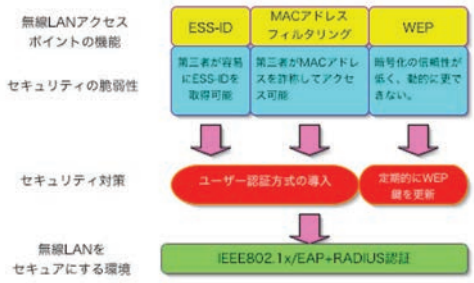


図７.セキュリティ対策

３．ホスト間のデータの送受信時にSSHを利用してSSHトンネリング機能を用いたり、IPsec等を使用して、無線LANに流れるデータを暗号化する。

4.1.2　クライアント側の無線LANセキュリティ対策

１）ネットワークサービスを安全に利用する
　使用していないネットワークサービスを停止する。使用するネットワークサービスについては、ファイアウォールを構築してサービスへのトラフィックを通過させる。WEPでの暗号化と、SSL、SSHの暗号化を組み合わせて利用するとよい。
２）ファイアウォールの構築
　ファイアウォールルール設定として、ループバックネットワークの成り済ましを防ぐ設定、偽のIPアドレスの使用を防ぐ設定を行う。
・MacOSXでのファイアウォール（ipfw）の設定例

```
#ループバックネットワークの成り済ましの防止
ipfw deny log all from any to 127.0.0.0/8
#偽のIPアドレスの使用防止
ipfw deny log all from 0.0.0.0/8 to any in
ipfw deny log all from 169.254.0.0/16 to any in
ipfw deny log all from 192.0.2.0/24 to any in
ipfw deny log all from 224.0.0.0/4 to any in
ipfw deny log all from 240.0.0.0/4 to any in
ipfw deny log all from any to 0.0.0.0/8 in
ipfw deny log all from any to 169.254.0.0/16 in
ipfw deny log all from any to 192.0.2.0/24 in
ipfw deny log all from any to 224.0.0.0/4 in
ipfw deny log all from any to 240.0.0.0/4 in
```

３）スタティックARPアドレスの設定
　ARPポイゾニングによるMITM攻撃を防止するためにARPエントリをスタティックな設定にする。
・MacOSXでのスタティックなARPエントリ設定
　arp -s〈Gateway IP Address〉〈Gateway MAC Address〉
・MacOSXでのスタティックなARPエントリ消去
　arp -d〈Gateway IP Address〉

4.1.3　無線LANをセキュアにするIEEE802.1xシステムについて

・IEEE802.1xは、端末を接続する物理的なLANポートごとに、接続してきた端末を利用するかどうかを認証する規格である。もともと有線LANでの利用を考慮した仕組みであるが、無線LANアクセスポイントと連携させることによって、無線LANをセキュアにすることができる。
・IEEE802.1xの仕組みは、EAP（PPP Extensible Authentication Protocol）認証プロトコルを用いて、RADIUSユーザー認証サーバー、無線LANアクセスポイント、無線端末、CA認証局（Certification Authority）との連携で実現できる。IEEE802.1xの認証方式は、EAP-TLS、EAP-TTLS、EAP-PEAP、LEAP（Cisco-EAP）などがある。

図８.IEEE802.1xの構成

4.2　電磁波漏洩問題（TEMPEST）

　パソコン等の電子機器を使用するときに発生する電磁波を盗聴することで、情報を再生することができるTEMPESTという手法がある。
　パソコンからの電磁波の中でも、イーサネットケーブル・コネクタ、USBケーブル・コネクタ等のシリアル伝送の信号は盗聴されやすい。また、発生する電磁波の小数点以下のレベルの違いを識別することによって、特定のパソコンの電磁波のみを盗聴することができる。更に、電源ケーブル、水道管等の導電性のものを利用した盗聴も可能である。

新情報セキュリティ技術研究会（IST）
URL http://www.j-netcom.co.jp/ist/

5．ログ分析

5.1　不正アクセスの兆候

不正アクセスが行われた場合に起きると思われる現象として以下の兆候が見られる可能性が高い。

・不明なシステムの再起動、シャットダウン
・不明なシステムのクラッシュ
・膨大なディスク領域の増加
・大量データのダウンロード
・急激な処理速度の低下
・ログファイルの急激なサイズの変化
・勤務時間外や休暇中のユーザのログイン
・存在しないアカウントを利用したログイン試行
・異なる電話回線からの同一ユーザによるログイン
・管理者が把握していないユーザアカウント
・見慣れないサイトからのアクセス
・接続禁止サイトからのアクセス
・TFTPによるファイル転送
・システム日付の変更
・不明な管理者権限の使用
・不明なアクセス権の変更
・踏み台にされている形跡がある。

これらの状況を把握するためには、ログイン、ログアウトを行ったユーザ、ホスト、アクセス権限の変更内容とその時刻等の情報を確認する。尚、パスワードに関する情報収集は厳禁である。収集したパスワード情報が不正利用されると大きなセキュリティ問題に発展するからである。

5.2　ログ分析の概要

不正アクセスの検出や発信元の追跡を行うためには、以下のようなログが必要である。

・オペレーティングシステム（UNIX、Windows等）
・ファイアーウォール
・リモートアクセス・認証サーバ（RADIUS等）
・WWWサーバ（Apache、IIS等）
・メールサーバ（sendmail、ExchangeServer等）
・ルータ（CISCOルータ等）

これらのログに関しては、ログの採取方法、ログの内容の出力項目について、ログの出力形式、ログのバックアップ方法を事前に整理する必要がある。

ログファイルの採取については、ログ情報が大量に発生すると、必要な情報を見逃してしまう可能性がある。逆にログ情報が少なすぎると不正アクセスの検出のための情報が不足してしまう。

ログの正確性について、侵入者によるログファイルの書き換え、消去、改ざんされないようにする。複数のシステム間でシステム日付を一致させる。

ログ採取の監査機能は、システムのパフォーマンス低下の要因になるので注意が必要である。

5.3　時間同期の必要性

複数のシステムにまたがってログ分析を総合的に行う場合は、各システム間での日付設定が一致していることが重要である。不正侵入された際に、ログの削除や改ざんのみだけでなく、システムの日付を変更して、ログ分析を困難にすることも考えられる。

・システム日付を合わせる方法

一般的には、NTPを利用する。NTPは、複数台のマシンで階層構造で時間同期を設定できる。

今現在、日本では、共同研究の一環として以下の組織が、日本標準時を提供する試行サービスを行っている。

・独立行政法人通信総合研究所（CRL）
・日本電信電話株式会社（NTT）
・株式会社インターネットイニシアティブ（IIJ）
・インターネットマルチフィート株式会社（MFEED）

これらのサーバは、CRLの日本標準時を刻む原子時計を直接時刻源としているため、時刻のずれ（オフセット）が非常に小さく（1000分の１秒以内）で安定している。

以下のサーバにNTPでアクセスすることで高精度な時刻情報を取得できる。（http://www.jst.mfeed.ad.jp）

・ntp1.jst.mfeed.ad.jp（210.173.160.27）
・ntp2.jst.mfeed.ad.jp（210.173.160.57）
・ntp3.jst.mfeed.ad.jp（210.173.160.87）

5.4　各種ログの種類と特徴

5.4.1　ファイアーウォールとルータのログ

ファイアーウォールとルータから取得したログについては、以下の項目を確認する。

・着信と発信のインターフェース
・発信元と宛先のIPアドレス
・使用プロトコル
・疑わしいポートに対するアクセス
・ポートスキャンのような特定のパターン

5.4.2　UNIXのログ

１）syslogd

UNIXでは、syslogdのデーモンを利用してログの採取を行っている。各サービスから出力されるメッセージをsyslog経由でテキスト形式のファイルへ出力する。syslogd経由でログを出力するためにプログラム（サービス）側とsyslogd（/etc/syslog.conf）側の両方の設定が必要である。

２）lastlog

各ユーザが最後にログインした情報を保存する。この情報は、lastlogを実行することで参照できる。

その他のユーザ情報を確認するコマンドとして以下のものがある。

・ユーザのログインやシステムのシャットダウン、再起動等の情報：lastコマンド（/var/log/wtmp）
・失敗したログインに関する情報：lastbコマンド（/var/log/btmp）
・各ユーザの最終ログイン時刻：lastlogコマンド（/var/log/lastlog）

lastlogの情報を利用して、各ユーザが前回ログインした時刻をチェックするように心がけることで、なりすましの検出が可能になる。

３）utmp

現在ログイン中のユーザー情報は、utmpバイナリファイルに記録される。これらの情報は、who、finger、usersコマンドで確認することができる。

４）wtmp

各ユーザのログイン/ログアウト、システムの再起動/シャットダウンのログ情報は、wtmpバイナ

リファイルに記録される。これらの情報は、lastコマンドで確認することができる。

5）acct

各ユーザが実行したコマンドのログ情報は、acctファイルに記録される。これらの設定は、デフォルトでは無効になっている。これらの設定を有効にする場合は、

/usr/sbin/accton ログファイル名

を実行すればよい。ログファイル名/var/log/pacctを指定することで、lastcommコマンドでログの表示が可能になる。

6）ログのフィルタリング

lastコマンドを使用すると大量にログが表示されるため、以下のオプションを指定することで、フィルタリングが可能になる。尚、lastbコマンドも同じオプション指定が可能である。

last -x reboot　　再起動の情報のみを表示
last -x shutdown　シャットダウンの情報のみを表示
last -n　　指定した行数のみを表示
last ユーザ名　　指定したユーザ情報のみを表示

lastlogコマンドについては、以下のオプションが指定可能である。

lastlog -t 日数　　指定した日数のログを表示
lastlog -u ユーザ名　指定したユーザ情報のみを表示

7）その他

システム起動時間を確認する場合は、uptimeコマンドを使用する。この情報を確認することで、不正な再起動を調査することができる。

/var/log/messsages、/var/log/secureファイルを参照することで、各サービスの情報が確認できる。

5.5　ログ分析

syslogで出力されるログについては、以下のようなキーワードに注意する。

表2.ネットワークサービスの主なキーワード

サービス	キーワード	想定される攻撃
ftp	Login incorrect	BruteForce攻撃
	passwd	Passwdファイルの不正入手・上書き
telnet	Authenticatin failed	BruteForce攻撃
	REPEATED LOGIN FAILURES	BruteForce攻撃
sendmail	reject	メールの不正中継
	rejected	不正なコマンドの実行
	allow,Sorry	不正なコマンドの実行
	Null connection	ポートスキャン
qpopper	-ERR POP EOF received	ポートスキャン
	-ERR Password supplied	BruteForce攻撃
halt	halted	不正なシャットダウン
reboot	rebooted	不正なシャットダウン
shutdown	reboot,halt,shutdown	不正なシャットダウン
login	ROOT LOGIN REFUSED ON	BruteForce攻撃
	ROOT LOGIN FAILURES ON	BruteForce攻撃
su	BAD SU	BruteForce攻撃
getty	〈tty〉	BruteForce攻撃
date	date set by	システム日付の不正変更

疑わしいアタックのパターンとして、以下のような例がある。

・毎日深夜に２回ログインを失敗する
・サーバが早朝に再起動する
・混雑しない時間帯に処理の停滞が発生する。

これらのパターンが検出された場合は、以下の点に注意してログ情報を調査する必要がある。

・異常な時間帯における正常な活動
・ベースラインを逸脱したユーザの活動
・ログイン、ファイルアクセス等の失敗
・シャットダウン、再起動（OS、サービス、デーモン）
・不明なファイルの存在
・急激なディスク空き容量の変動

5.6　メールヘッダの解析（SPAMメールについて）

SPAMメールを受信して、発信元を調べる場合はメールヘッダの解析が必要となる。SPAMメールの発信元を調べるには、Receivedヘッダを確認するのが基本となる。

Received：from AAA by BBB

上記の記述の場合は、サーバAAAからサーバBBBへメールが送信されたことを表す。複数のメールサーバによって転送される場合は、Receivedヘッダが複数存在して、下から順に記述される。

SPAMメールを受信した場合は、次の点について注意する。Fromヘッダのドメイン名とReceivedヘッダ、Message-IDヘッダのドメイン名と一致するかを確認する。この部分が一致しない場合は、発信元のメールアドレスが架空のメールアドレスの可能性がある。Receivedヘッダの偽造が可能であることから、この記述の信頼性について、IPアドレスの整合性を調べることが必要となる。

関連RFC：RFC822ARPAインターネットテキストメッセージの書式のための標準（STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES）

5.7　侵入発見後の流れ

侵入や攻撃が発覚した場合は、

・パニックに陥らない、冷静に判断する。
・手順書、マニュアルを確認する。

侵入や攻撃が発覚した場合の対処方法について、大まかな流れを以下に示す。

1）攻撃されたホストをネットワークから切り離し対処する

ネットワークから切り離して、進行中の攻撃を停止させる。（有線LANの場合：ネットワークケーブルを外す、無線LANの場合：無線の使用をOFFにする）尚、攻撃を受けたホストのシャットダウンの処理は、攻撃の追跡調査に必要な情報が失われる可能性がある。よって、シャットダウンの処理は最後の手段として考えるとよい。

2）被害を受けたホストを修復する

被害の大きい箇所から優先的に修復する。修復作業で一番重要なのは、作業内容や復旧内容を確認しながら、誤って事態を悪化させないようにする。

3）侵入、攻撃の被害状況を関係者に通知する

被害状況を通知する際は、Eメール等のインターネット以外の手段である電話やFAX等を利用する。

4）スナップショットを採取する

攻撃を受けたホストの内容を、DATやディスク

等に保存する。これらの情報を用いて、攻撃手法と脆弱性の調査に役立てる。
5）事後対策
・ハッカーに侵入された場合
ハッカーが侵入に利用したセキュリティホールを塞ぎ、ハッカーが改ざんしたもの、消去したもの、バックドアの作成、ログ等を調査する。最悪の場合は、システムの再インストールを行う必要もある。
・ハッカーに侵入が成功しなかった場合
確信犯的なケースの場合は、しばらく監視を強化して、関係者にも監視するように通知する。
6）インシデントの文書化
将来、同様の問題が発生した場合に備えて、適切な対応ができるように発生した事象について文書化しておくとよい。
7）不正アクセスの届け出を行う
最終的には、「独立行政法人 情報処理推進機構（IPA）セキュリティセンター（ISEC)」へ不正アクセス届出を行えばよい。
URL http://www.ipa.go.jp/security/ciadr/index.html

5.8 侵入発見後の処置（UNIXの場合）

5.8.1 ネットワーク切断前の作業

不正侵入を発見した場合は、これ以上被害が拡大しないように侵入されたホストをネットワークから切り離すことが必要になるが、その前段階でネットワークに接続された状況での情報収集が必要となる。
1）ホストにログインする
ハッカーに警戒されないように可能なかぎり別ホストからのリモートログインを行う。ログインする際には、一般ユーザでログインして、必要な場合にのみroot権限を使用する。
2）ネットワークの接続状況を確認する
ネットワークの接続状況を確認する際には、以下のコマンドを使用する。
・現在のログイン状況：w、whoコマンド
・過去のログイン状況：lastコマンド
これらの情報は、syslogのログが全て消去された場合には取得できない。
・ネットワーク接続状況とListenしているポートの確認：netstat an
不正なポートが確認された場合には、そのポート番号と接続時刻をメモをとって控えておく。
3）プロセスの確認
不審なプロセスの起動状況の確認：ps axf
不審なプロセスが確認された場合には、プロセス名、起動パスについてメモを控えて、後で調査する。
4）設定ファイルの確認
以下のファイルを参照して、不審なプロセスの起動設定がないかを確認する。
確認するファイル
・/etc/passwd,inetd.conf,crontab
・/etc/rc.d/rc,rc.boot,rc.local
確認するディレクトリ
・/etc/rc.d/init.d,rc2.d,rc3.d,rc4.d,rc5.d,crond

5.8.2 ネットワーク切断後の作業

以下の作業は、rootで行う。この作業を行う前にスナップショットを採取しておくとよい。
1）rootのコマンド履歴の確認
rootのコマンド実行履歴を確認して、不審なコマンド実行がないかを確認する。
2）syslogの確認
syslogの情報がハッカーによって消去されていなければ、OSの再起動、ログインの拒否、デーモンメッセージの異常について確認する。
3）不審なプロセスの確認
ネットワークを切断する前に確認された、不審なプロセスや不審なポート番号等について調査する。
・発信元ネットワーク、接続時刻の確認
w,whoコマンド、lastログ、syslog等
・コマンド履歴の確認：suコマンドの不正使用、不正なプログラムのコンパイル
・不正侵入に悪用されたアカウントの正規利用者のログイン状況
netstatコマンドでの接続状況を確認した際に、不審なポートに対する接続が発見された場合には、「バッファオーバーフロー攻撃」と「バックドアへの接続」が想定される。この場合は、不審なポートのオーナを調査するために
fuser -vn tcp/udp ポート番号
ポートとプロセスの関係について確認するには「lsof i」、「netstat -lp」
を実行すればよい。
4）不審なファイルの確認
バックドアが仕掛けられた場合等は、どこかに不審なファイルが残っていたりするため、以下のようなコマンドを実行して、不審なファイルを検出する。
・.で始まるファイル名、ディレクトリ名の検索
find / -name'.'* -print
・所有者がrootであるファイルの検索
find / -user root
・所有者がrootで、所有者権限で実行可能なファイルの検索
find / -user root -perm -4000 -ls
・更新日付が不審なファイルの検索
x日前に更新されたファイルの表示:find / -mtimex
5）パッケージの整合性の確認（Linuxの場合）
rpmパッケージを利用している場合には、
rpm -Va
上記のコマンドでパッケージの整合性を確認することができる。ただし、構築時に設定ファイルを変更している場合には、不整合と表示されるため注意が必要である。

6．セキュリティ診断・監視

6.1 脆弱性検査

ネットワーク・セキュリティ・スキャナであるnessusを用いて、遠隔地から特定のネットワークを監視して、ハッカーからの被害を受ける可能性をチェックしている。nessusは、サーバ/クライアント型のツールである。
・2004年２月現在のバージョン：2.0.10
・URL：http://www.nessus.org/
・他に必要なツール：GTK+,nmap,openssl
・nessusの設定方法
専用のユーザをnessus-adduserコマンドで作成する。サーバ/クライアント間でSSL通信で使用するためのサーバ証明書（公開鍵と秘密鍵のペア）を

nessus-mkcertコマンドで作成する。
・nessusの動作確認
　クライアントからサーバ（nessusd）へ作成した専用ユーザでログインして、検査するホストやネットワークをチェックする。

6.2　侵入検知システム（IDS：Intrusion Detection System）

　侵入検知システムは、ログやパケット情報を基にして不正侵入を検出するシステムである。
侵入検知システムを導入することによって、
・脅威の確認
・不正侵入の早期発見
・不正侵入の抑止
・管理者の負担軽減
以上の効果が得られる。

6.2.1　侵入検知システムの種類

1）ホストベース侵入検知システム
　ホストベース侵入検知システム（ホストベースIDS）は、OSや各種アプリケーションが生成するログ情報を用して不正侵入を検出する。通常は、保護対象のホストに導入する。
2）ネットワークベース侵入検知システム
　ネットワークベース侵入検知システム（ネットワークベースIDS）は、LANを流れるデータを監視して不正侵入を検出する。スイッチングハブを導入している場合は、注意が必要である。

6.2.2　侵入検知に関わるセキュリティ対策

　ネットワークベース侵入検知システムであるSnortを用いて、侵入検知を行っている。
・2004年２月現在のバージョン：2.1.1
・URL：http://www.snort.org/
・日本Snortユーザ会（Japan Snort Users Group）
　URL：http://www.snort.gr.jp/
・他に必要なツール：libpcap,openssl
・設定ファイル
　ルールセットを利用するためにsnort.confを編集して、専用ユーザ（snort）を作成する。
・Snortの動作確認方法
　有効にしたルールセットに値する攻撃を試みて、Snortのログに記載されるかをチェックする。

6.3　改ざん検出

　トロイの木馬やWebサーバのコンテンツの改ざん等の改ざんをチェックするシステムである。一般的な仕組みとして、以下の処理を行う。
1）MD5、SHA-1等のハッシュ関数の出力結果を事前に保存する。
2）定期的にハッシュ関数を実行して、事前に保存しておいた値と比較する。
3）ハッシュ関数の値が一致しなければ改ざんされたと判断する。

6.3.1　ファイル改ざんに関するセキュリティ対策

　システム内のディレクトリやファイルの書き換えをチェックを行うためのツールとしてTripwireを導入した。
・2004年２月現在のバージョン：2.3-47（フリー版）
・URL：http://www.tripwire.org/
・Tripwireの設定方法
　１．設定ファイルの作成、２．ポリシーファイルの作成、３．ベースラインデータベースの作成の順番となる。
・Tripwireの動作確認
　整合性・レポートをチェックして、ポリシーファイルの調整を行いながら、データベースを管理する。

6.4　盗聴検出

　有線LANの場合は、LANアナライザで利用されるpromiscuousモードで盗聴が行われる。今現在では、promiscuousモードで動作するマシンを検出するツールが存在する。

6.4.1　promiscuousモードで動作するマシンを検出する方法

・ネットワーク上に存在しないIPアドレスにデータを送信して反応を調査する。
・調査対象の全てのマシンにICMPメッセージを送信して、レスポンスタイムを計測する。
・ブロードキャストに対するOS固有の動作とアドレスの解釈を調査する。
・ブロードキャストアドレスの変形を指定したARPの応答を調査する。

6.4.2　盗聴検出ツール

　盗聴を検出するツール「PromiScan」がある。このツールは、Windowsのみで動作する。
・2004年２月現在のバージョン：0.27（フリー版）
・URL：http://www.securityfriday.com/ToolDownload/PromiScan/promiscan_doc.html
・他に必要なツール：WinPcap
　このようなツールを用いて、盗聴の可能性を検出することが可能となる。

7．おわりに

　筆者は情報セキュリティに携わって以来、独学で対応してきた。今回、国立情報学研究所が主催した平成15年度第３回情報セキュリティ担当職員研修上級コースを受講して、今まで抱えていた誤解を解決することができ、新たな知識・技能を修得することができた。今後の技術・技能のスキルアップを図る上で、今回修得した技術・技能を発展させていきたい。

研究開発課題

平成15年度総合情報処理センター「研究開発課題」一覧

本研究開発はセンター業務に関わるソフトウェア，データベース等の充実及び利用手段の拡充を目的とし，学内公募により，その成果を提供してもらい他の利用者に還元するよう設定されています。今年度の応募件数は6件あり運営委員会における審議の結果，下記に示す全6件が採択されました。

研究開発テーマ	部局	氏名
学内ＬＡＮ接続機器監視システムの開発	医学部	松谷秀哉（代表） 須藤勝弘
Linux+PostgreSQLによる教育用WEBデータベースシステムの開発に関する研究	医学部	佐藤達資（代表） 三浦富智 野坂大喜
常時微動連続モニターシステムの開発	理工学部	渡辺和俊（代表） 石田祐宣
無線LAN環境構築による講義室におけるVODコンテンツの有効活用	理工学部	葛西真寿（代表） 佐藤勝人
動画データを用いた免疫系細胞活性化の「評価・解析プログラム」の開発	理工学部	雨森道紘（代表） 大学院生　４名
WEBを利用した各種申請書の自動作成システムの開発及びデータのデータベース構築のための考察	理工学部	葛川寛之

研究開発報告

医学教育用マルチメディア教育コンテンツデータベースの開発に関する研究

弘前大学医学部保健学科
野　坂　大　喜　hnozaka@cc.hirosaki-u.ac.jp
三　浦　富　智　tomisato@cc.hirosaki-u.ac.jp
稲　葉　孝　志　tnappa@cc.hirosaki-u.ac.jp
佐　藤　達　資　tatusuke@cc.hirosaki-u.ac.jp

Ⅰ．はじめに

近年大学内における情報化が急速に広まり，e-Learningやバーチャルユニバーシティによる大学教育が開始されている。バーチャルユニバーシティはインターネットや通信衛星等を利用する大学教育であり，その特性上，距離や時間等の制約を受けずに「いつでも」「どこからでも」大学教育を受講できることから，社会人再教育や大学間合同講義等の新たな教育方法として期待されている。本学においてもインターネットを活用した遠隔教育への対応が期待されているが、全国的に医学教育におけるバーチャルユニバーシティへの対応は他分野に比較して遅れている状況にある。その原因の一つとして医学分野の教育用コンテンツの少なさが挙げられており、早急に医学教育用コンテンツを開発してライブラリとして蓄積していく必要がある。そこで本研究では、医学教育用コンテンツデータベースとして、顕微鏡画像を主体とする画像コンテンツの開発を行ったので報告する。

Ⅱ．システム概要

本システムは以下のハードウェアとソフトウェアで構成される。

・Server：PowerEdge300（Dell）PentiumⅢ1GMHz dual , MM 1,024Mbyte , HDD36 Gbyte（RAID5）
・Server OS：Windows 2000 server（Microsoft）
・Database：学びの扉PRO（NEC）

システム概要図を図１に示す。ユーザーとなる学生は、保健学科内に設置されたデータベースサーバーへ特別な専用ソフトを使用せず、 InternetExplorer などのWEBソフトウェアにてアクセスし、目的とする画像を検索・閲覧することが可能である。

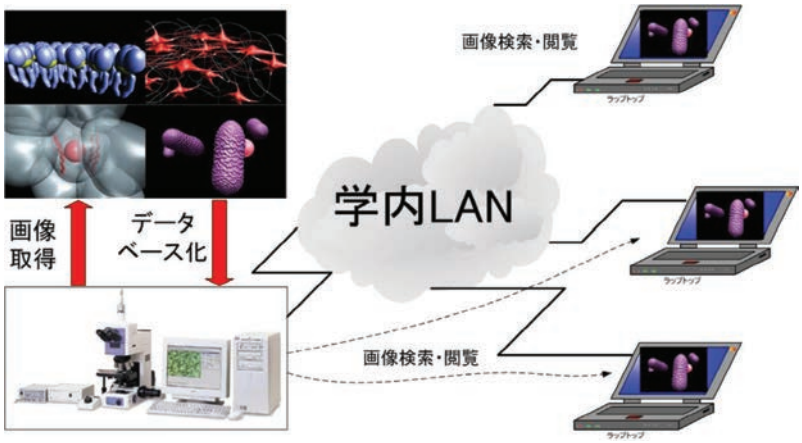


図１　システム概要図

Ⅲ. 使用方法

本システムで公開されるコンテンツは、学内ＬＡＮ限定コンテンツと公開講座等で使用可能なInternet公開コンテンツの２種に分類されている。ユーザーはメインメニュー（図２）から本システムにログインし、分類された各フォルダをクリックすることで、画像一覧（図３、４）が提供される仕組みとなっている。それぞれの画像タイトルをクリックすると目的となる画像を閲覧（図５）することが可能である。

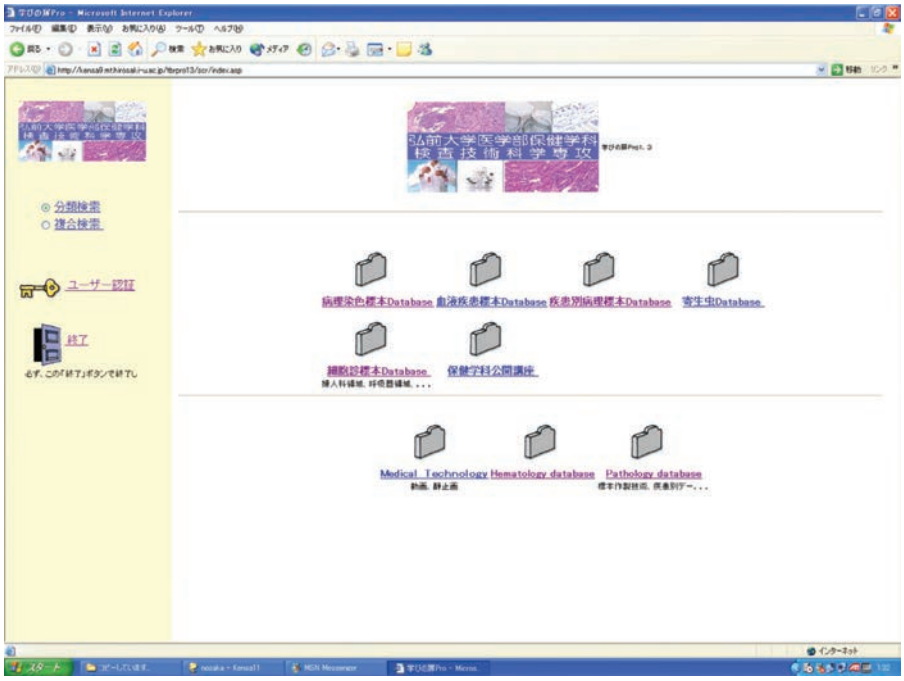


図２　メインメニュー画面

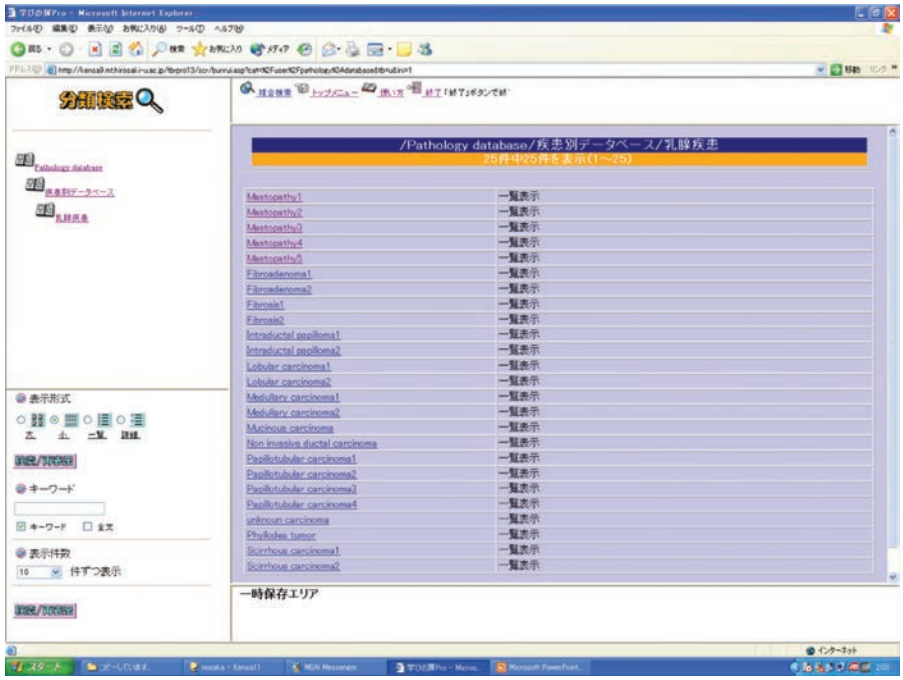


図３　一覧表示画面（簡易表示）

図４　一覧表示画面（詳細表示）

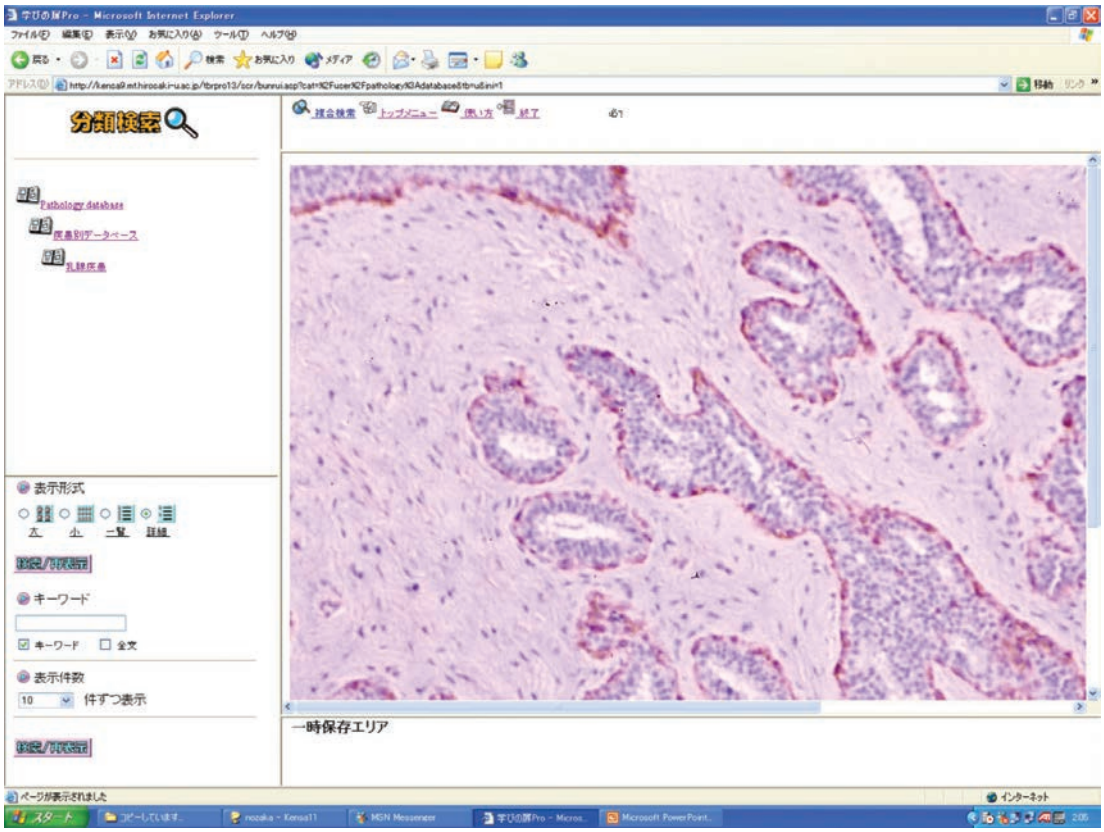


図５　画像表示画面

Ⅳ．本コンテンツの特徴

現在公開中のコンテンツ例を図６～図10まで示す。現在インターネットで公開されている病理教育用の顕微鏡画像は組織診断標本画像と細胞診断標本画像に大きく分けられており、同一症例の組織診断標本画像と細胞診断標本画像の両者を同時に提供しているシステムは皆無である。本来病理組織診断と細胞診断は相補関係にあり、病理系の学習を行う際には、組織診断標本上から得られる全体的な配列情報と細胞の特徴情報、また細胞診断標本上から得られる一つ一つの細胞の特徴情報を総合的にとらえ、理解を深める必要がある。そこで本システムでは、組織標本画像と細胞診断標本画像を併せて提供することで、学生の理解を深めるための工夫をしている。また、病理診断では疾患に特有の抗原を免疫組織科学染色や特殊染色により局在を明らかにすることで、より正確な診断や詳細な分類を行うことから、一般的なヘマトキシリン・エオジン（HE）染色やパパニコロウ（Pap）染色だけでなく、組織分類に欠かせない他の染色についても画像を併せて提供している。

Ⅴ．考察

今回我々が開発したコンテンツは医学教育分野で遠隔教育を行うだけでなく、日常の講義や実習時、あるいは自習教材として学生に提供することが可能であり、今後もコンテンツを拡張したいと考えている。しかし医学教育用コンテンツ開発の問題点として、特に病理分野における教育においては、本来正常細胞や反応性細胞などが混在する中から目的とする腫瘍細胞を見つけるという一連の顕微鏡観察作業によって初めて実習が成立することから、単に腫瘍細胞部分のみの画像を提供するという従来のコンテンツ内容については、その教育効果を実証実験によって検証する必要があると考えられる。理想的なシステムとしては従来の実習環境をまるごとそのままPC上で実現するバーチャルスライドがあるが、現時点においてプレパラート標本すべてを撮影して１枚の画像として保存するためには、ハードウェア制限が多く、未だ実現されているシステムはない。また、細胞診断標本に関しては、標本の厚みのためにオートフォーカスによって画像を撮影することも困難である。これらのことから、医学教材についてはコンテンツの開発だけでなく、新画像取得システム、あるいはその活用方法も検討することが必要であり、今後は本システムを利用して学生の教育効果を検証するとともに、新たな医学教育用画像提供システムについて研究を行いたいと考えている。

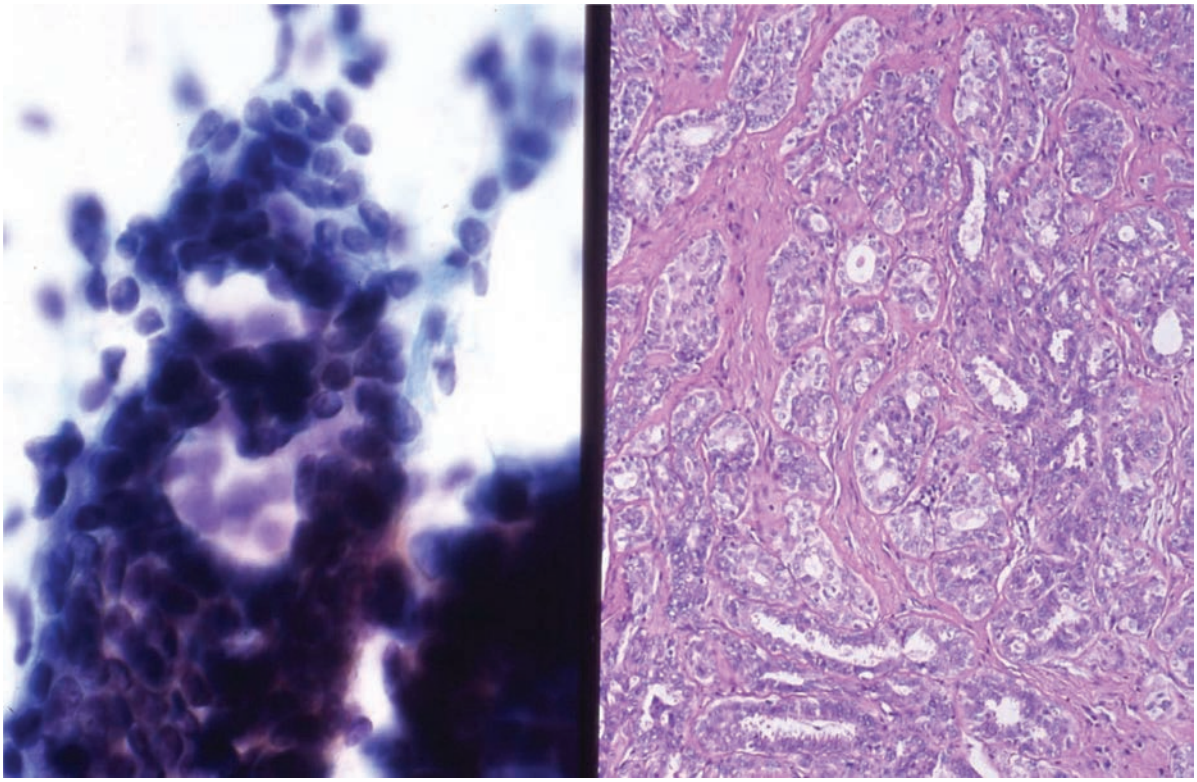


図６　乳腺腫瘍（Mastopathy）

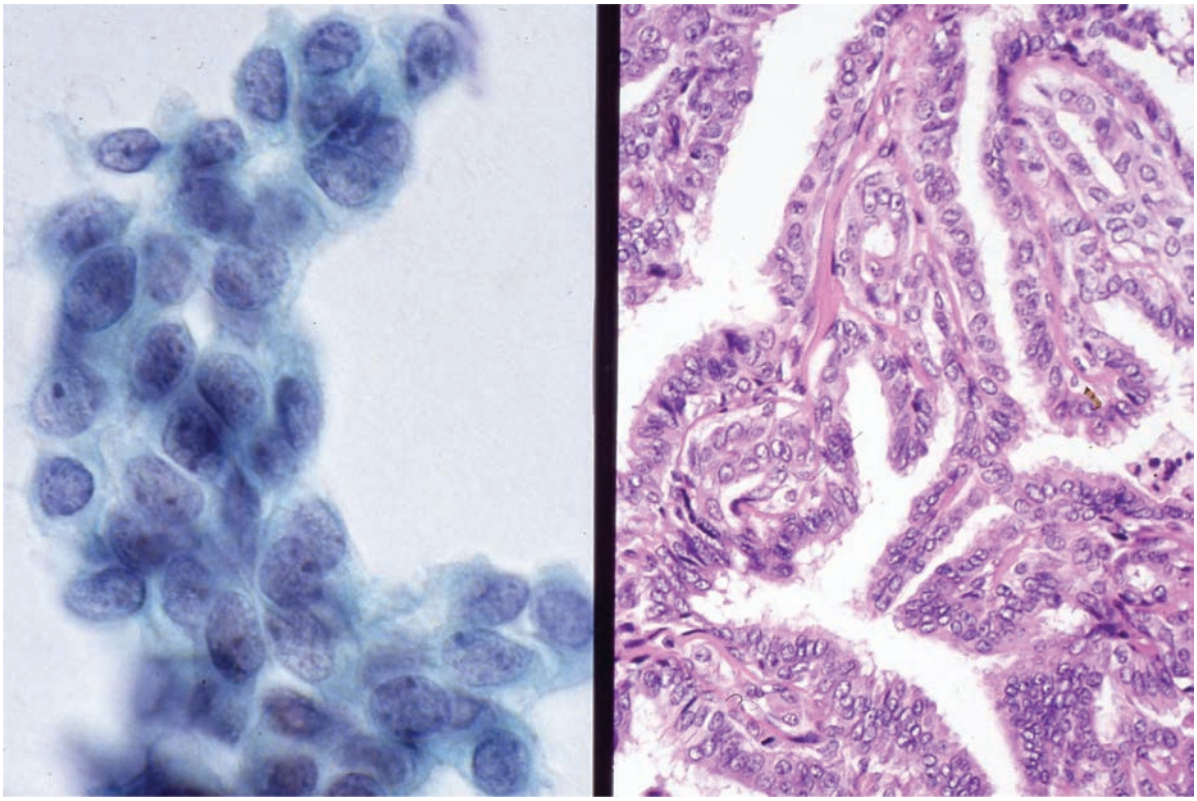


図７　乳腺腫瘍（Intraductal papilloma）

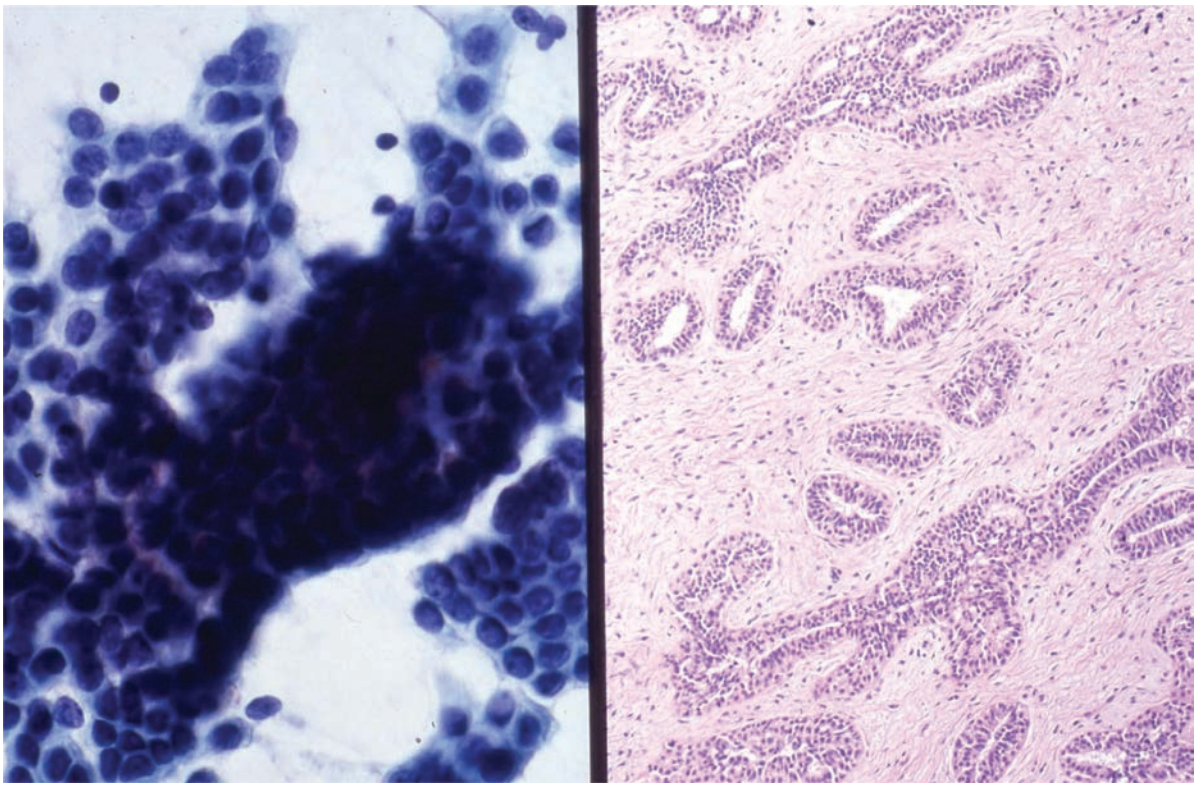


図８　乳腺腫瘍（Fibroadenoma）

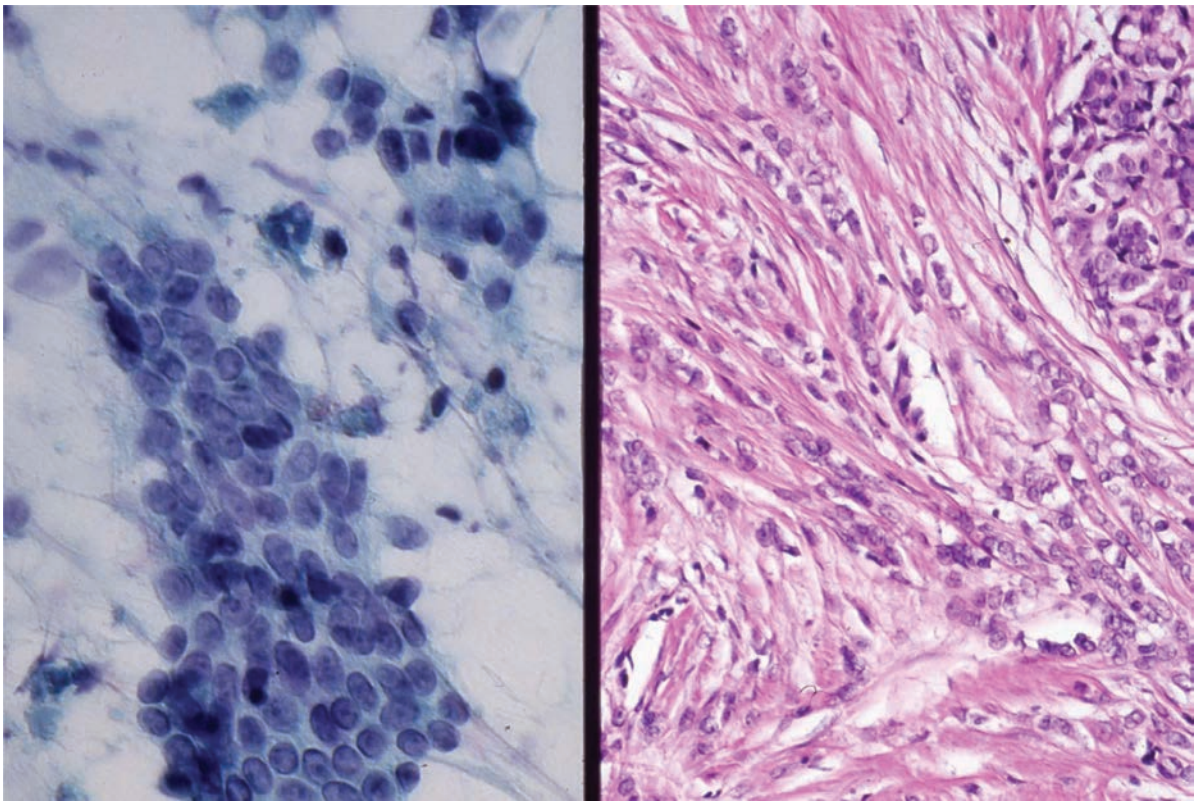


図９　乳腺腫瘍（Scirrhous carcinoma）

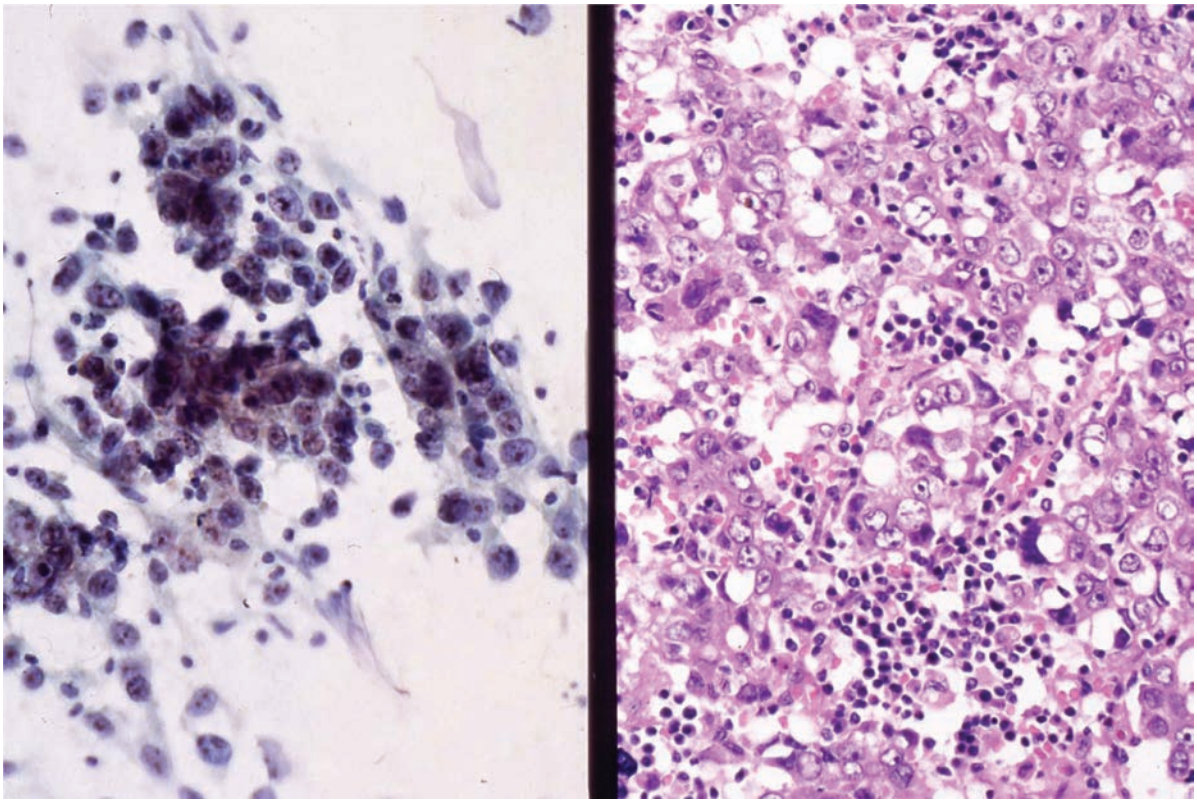


図10　乳腺腫瘍（Medullary carcinoma）

教育用システムにおける FORTRAN用グラフィックライブラリの構築

理工学部地球環境学科　市村 雅一
ichimu@cc.hirosaki-u.ac.jp
理工学部地球環境学科　葛西 真寿
kasai@phys.hirosaki-u.ac.jp

1　はじめに

現在総合情報処理センターの教育用システムは，Windows 環境と Linux 環境の２つを提供しており，Linux 環境は主に理工系の専門教育に利用されている。理工学部では，複数の学科でこの環境下での FORTRAN 言語を用いたプログラミングおよび数値解析の演習を交えた授業が行われている。FORTRAN 言語は一般的には C や Java の普及により使用者が減少しているが，初心者にも理解しやすい高級言語であることや，歴史が古く蓄積された資産が豊富であることなどを背景に一定の需要を保っている。

Linux では基本的なグラフィカル・ユーザ・インターフェースとして X Window 環境が提供されており，Xlib と呼ばれるライブラリの機能をアプリケーションから呼び出すことでユーザが自由にグラフィクス操作を行えるようになっている。しかし，このライブラリの機能を呼び出すインターフェースは C 言語の仕様に準じているため，FORTRAN から直接呼び出すのは困難である。数値解析の演習を行う場合，計算結果をいかにわかりやすく可視化するかが問題となるが，現状では計算結果を一旦ファイルに出力してから，gnuplot など別のアプリケーションに渡してグラフにする等の処理を行っている。

そこで今回，FORTRAN 言語から Xlib の機能を呼び出すためのインターフェースとなるライブラリ (libIX0) を作成した。また，利用する上での手引きとなるドキュメントを WEB ページとして作成・公開した。このライブラリを用いれば，自作の FORTRAN プログラムから直接グラフを描画できるため，数値計算を行いながら計算結果を随時可視化できるようになる。以下，作成したライブラリの詳細，使用例について報告する。

2　ライブラリの概要

本ライブラリは，Intel x86 アーキテクチャの CPU を想定した上でアセンブリ言語により作成した。アセンブラとしては，総合情報処理センターの教育用システムで実際に使用されている FORTRAN コンパイラ g77 を使用した。

ライブラリ中には，機能によって関数として呼び出さなければならないもの，サブルーチンタイプのものが混在しているが，呼び出し方法や必要な引き数については後述の WEB ページに記載されている。

関数の返り値及び引き数のタイプは全て 4 バイト整数で統一している (但し文字列変数を除く)。関数名は暗黙の型宣言 (特に宣言しなければ I~N で始まる変数は整数型になるというルール) を使用しても問題が起こらないように，全て整数型の名前になっているが，引き数については使用する側が意識しておく必要がある。以下ライブラリに含まれる関数，サブルーチンの機能別一覧を示しながら説明していく。

2.1　ウィンドウ操作

ウィンドウの生成・表示や属性の設定などの機能を持つ部分である。図を描いたり表示したりする場所を確保するためには，最低限以下の作業が必要となる。

1)　ディスプレイサーバとの接続　[`ixopendisplay`]

2) ウィンドウの生成 [ixcreatesimplewindow]

3) ウィンドウの可視化 (Mapping) [ixmapwindow]

4) X サーバへのリクエストの送出 [ixflush]

本ライブラリに含まれる Xlib 関連の機能を利用するためには，アプリケーションの始めの方で**必ず ixopendisplay を使ってディスプレイサーバとの接続をしなければならない。**その後，ixopendisplay の返り値として得られた Window ID を用いて図形描画等の機能を利用する。

これらの内容を理解するには，X Window に関する基本的な知識が必要とされるが，簡単な図を描くために本ライブラリを使用するだけならば，後述のサンプルプログラムを参考に,「おまじない」として使用すれば問題ない。

ウィンドウ操作

関数・サブルーチン名	機 能
ixopendisplay	ディスプレイサーバとの接続
irootwindow	Root Window ID の取得
ixcreatesimplewindow	ウィンドウの生成
ixmapwindow	ウィンドウの可視化 (Mapping)
ixmapsubwindows	サブウィンドウの可視化 (Mapping)
ixflush	リクエストの強制送出
iblackpixel	黒色ピクセル値の取得
iwhitepixel	白色ピクセル値の取得
ixquerycolor	RGB 値の取得 (XColor 構造体指定)
icpixel	ピクセル値の取得 (カラー名指定)
ixsetwindowbackground	ウィンドウの背景色指定
ixalloccolor	ピクセル値の取得 (XColor 構造体指定)
ixclearwindow	ウィンドウのクリア
ixgetgeometry	ウィンドウの位置や大きさを調べる
noredirect	ウィンドウマネージャの介入を阻止
ixsetwhints	ウィンドウ表示の位置，サイズの設定
ixsetinputfocus	フォーカスウィンドウの変更

2.2 グラフィクス操作

ウィンドウ上に図形を描画するためには，グラフィクス・コンテキスト (以下 GC と呼ぶ) が必要となる。GC は図形描画時のグラフィクス属性を保持しているリソースであり，例えば直線を描く時の線の幅，スタイル，色などの情報を GC に予めセットしておく必要がある。基本的には，以下のような手順となる。

1) GC の生成 [ixcreategc]

2) 属性の指定 [ixsetforeground など]

3) 図形描画 [ixdrawline など]

4) X サーバへのリクエストの送出 [ixflush]

グラフィクス操作

関数・サブルーチン名	機 能
ixcreategc	グラフィクス・コンテキスト (GC) の生成要求
ixfreegc	GC の開放
ixsetforeground	前景色の指定
ixsetbackground	背景色の指定
ixsetfunction	GC に対する機能の指定
ixsetlinewidth	直線の太さの指定
ixsetgraphicsexposures	GC の Exposure イベント無しの設定
ixdrawline	直線の描画
ixdrawrectangle	長方形の描画
ixfillrectangle	塗りつぶし長方形の描画
ixdrawpoint	点の描画
ixdrawarc	円弧の描画
ixfillarc	塗りつぶし円弧の描画

2.3 文字列描画

文字列を描画する場合の属性は，グラフィクス操作と同様に GC ににセットされているものを用いる。また，特に日本語文字列 (マルチバイト文字列) を描画するためには，言語環境の設定 (OS の設定) とフォントの指定が必要である。以下に日本語文字列表示の基本的な流れを示す。

1) 言語環境の設定 [isetlocale]
2) GC の生成 [ixcreategc]
3) 属性の指定 [ixsetforeground など]
4) フォントの指定 [ixcreatefontset など]
5) 文字列描画 [ixmbdrawstring など]
6) X サーバへのリクエストの送出 [ixflush]

文字列描画

関数・サブルーチン名	機 能
ixloadfont	フォントのロード
ixsetfont	GC へのフォントのセット
isetlocale	言語環境の設定 (OS の関数)
ixcreatefontset	フォントセットの作成
ixmbdrawstring	マルチバイト文字列の描画
ixmbdrawimagestring	マルチバイトイメージテキストの描画
ixdrawstring	1byte 系文字列の描画
ixdrawimagestring	1byte 系イメージテキストの描画

2.4 イベント関連 (キー入力，マウス関係を含む)

X Window 環境では，常にマウス，キーボード，グラフィクス等の状態を監視しており，それらに何らかの変化があるとそれを「イベント」と認識する。Xlib を利用すれば，アプリケーションからイベントの

情報を入手し，それをもとに動作を起こすことができる。本ライブラリには，イベント情報の読み込み機能を始め，キー入力やマウスの移動，ボタン押下などのイベントに関する情報入手の機能も含まれている。

イベント関連 (キー入力，マウス関係を含む)

関数・サブルーチン名	機 能
ixselectinput	イベントの選択 (イベントマスク)
ixnextevent	イベントの読み込み (イベント発生時)
ixcheckmaskevent	イベントの読み込み (real time)
inkey	キー入力検出 (アスキーコード)
incode	キー入力検出 (キーコード)
qpointer	マウス情報の取得 (real time)
getxy	マウス情報の取得 (イベント発生時)
ixwarppointer	マウスカーソルの強制移動
ixcreatefontcursor	マウスカーソルの生成 (標準マウスカーソルを利用)
ixfreecursor	マウスカーソルの開放
ixdefinecursor	指定ウィンドウ内のマウスカーソルの定義
ixundefinecursor	マウスカーソル定義の解除
wcursor	ウィンドウ内へのマウス連動十字カーソル表示
whcur	ウィンドウ内へのマウス連動横線表示
wvcur	ウィンドウ内へのマウス連動縦線表示
wboxcur	マウス連動長方形の表示
wstarea	マウスによるウィンドウ内の領域指定

2.5 画像データ操作

画像データを扱う場合，その属性を保持するためのリソース (image 構造体) を生成し，それを参照しながら処理を進める必要がある。本ライブラリには，image 構造体の生成や画像処理エリアとしてのピックスマップの作成を始めとして，画像の表示，取り込み，.xwd フォーマットでの保存等の機能が含まれている。これらの機能を利用するには，X Window 上での画像データの取扱いに関する知識が必要となる。

画像データ操作

関数・サブルーチン名	機 能
ixgetimage	ウィンドウ中の画像の取得
ixputimage	画像データの表示
ixputimagebw	画像データの表示 (白黒 1byte 画像専用)
ixcopyarea	ウィンドウ間の画像のコピー
idefaultvisual	Default Visual の取得
idefaultdepth	ピックスマップの深さの取得
ixcreatepixmap	ピックスマップの生成
ixfreepixmap	ピックスマップの開放
ixcreateimage	image 構造体の生成
ixdestroyimage	image エリアの開放
ixcreatebitmapfromdata	ビットマップの生成
xwdsave	表示画像の .xwd file への保存

2.6 プロセスへのアクセス

自作した FORTRAN プログラムから，他のプロセスへのアクセスをするための機能である。この部分は Xlib とは無関係であるが，現在授業で頻繁に利用されている gnuplot を FORTRAN からコントロールすることを目的として作成した。後述の WEB ページにサンプルプログラムを含めて使用方法の解説がある。

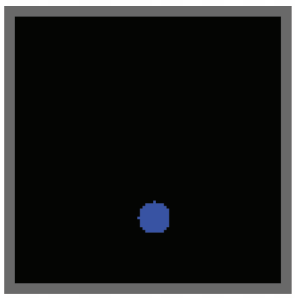
プロセスへのアクセス

関数・サブルーチン名	機 能
ipopen	プロセスの open
ipwrite	プロセスへの書き出し
ipflush	プロセス入出力バッファの flush
ipclose	プロセスの close

3 libIX0 の使用例

3.1 剛体球のアニメーション

以下に libIX0 を利用して作成したサンプルプログラムのソースリストを示す。これを実行すると，右図のような球が表示され，壁に跳ね返されながら動きまわるアニメーションが見れる。このプログラムでは，グラフィクス・コンテキストの機能を xor モードに指定し，黒の背景上で同一の図 (球) を上書きすることで，図形の描画と消去を繰り返している。



```
------------------------------------------------------------------------
c     剛体球の壁との弾性衝突プログラム
c          ir:球の半径  lx,ly:表示エリアの大きさ
      parameter (ir=6,lx=100,ly=100)

      ix=50         ! x 座標初期値
      iy=50         ! y 座標初期値
      ivx=-2        ! 初速度 (座標増分)x 成分
      ivy=5         !        〃        y 成分
      ixmin=ir      ! 中心 x 座標の最小値
      ixmax=lx-ir   !     〃    の最大値
      iymin=ir      ! 中心 y 座標の最小値
      iymax=ly-ir   !     〃    の最大値

      ichild=0
      mx=0
      my=0
      mask=0

      call ixopendisplay()          ! ディスプレイサーバとの接続
      iblue=icpixel('blue',4)       !  "青" のピクセル値取得
      igray=icpixel('dim gray',8)   ! "灰色"       〃
      iwr=irootwindow()             ! Root Window ID の取得
c     -----------  ウィンドウ生成 & ウィンドウ ID の取得 --------------
      iw=ixcreatesimplewindow(iwr,250,10,lx,ly,4,igray,iblackpixel())
```

```
      call noredirect(iw)           ! ウィンドウマネージャの介入を阻止
      call ixselectinput(iw,0)      ! イベントマスクの設定
      call ixmapwindow(iw)          ! ウィンドウの可視化
      igc=ixcreategc(iw)            ! GC の生成
      call ixsetfunction(igc,6)     ! GC の機能設定 (xor モード)
      call ixflush()                ! リクエスト送出

c     -------  円を描く -----
      call ixsetforeground(igc,iblue)                          ! 色指定
      call ixfillarc(iw,igc,ix-ir,iy-ir,2*ir,2*ir,0,360) ! 塗りつぶし円の描画
      call ixflush()                                           ! リクエスト送出

 10   continue
         call system('sleep 0.0001')  ! スピード調節
c        --------  円の消去 ( xor モードで同じ場所へ描画) ------
         call ixfillarc(iw,igc,ix-ir,iy-ir,2*ir,2*ir,0,360)
         ix=ix+ivx             ! x 座標移動
         iy=iy+ivy             ! y 座標移動
         call ixfillarc(iw,igc,ix-ir,iy-ir,2*ir,2*ir,0,360) ! 円描画
         call ixflush()        ! リクエスト送出
         if (ix.le.ixmin.or.ix.ge.ixmax) ivx=-ivx  ! 壁にぶつかったら x 反転
         if (iy.le.iymin.or.iy.ge.iymax) ivy=-ivy  !       〃       y 反転
         call qpointer(iw,ichild,mx,my,mask)       ! マウス情報取得
         if (mask.ne.0) go to 999                  ! ボタン押下で終了
      go to 10
 999  stop
      end
```

3.2 重力レンズ効果

ブラックホールが土星と地球の間を横切ったら重力レンズ効果によって，どう見えるか？point mass lens モデルを用いて計算した土星の像を libIX0 を利用して視覚化した。(図 1 参照)

一般相対性理論によれば，光も強い重力場によって経路が曲げられる。重力レンズ効果とは，遠方の天体からの光が手前の重力源によって進路を曲げられた結果，もともと一つの光源の像が複数個観測される現象である。図 2 の「レンズ効果を受けない土星の像」の各ピクセルの位置と色情報を libIX0 のサブルーチンを使って読み取り，重力レンズ方程式を解いて各ピクセルの像の位置を計算し，その位置に元画像の色情報をもったピクセルを打つという操作を繰り返す。尚，地球と土星の元画像は宇宙航空研究開発機構および国立天文台が提供している画像ファイルを利用した。

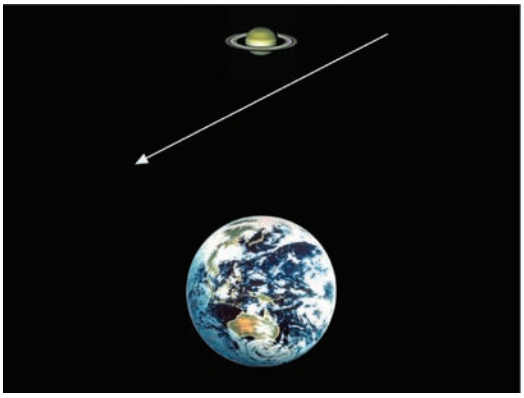


図 1: 地球と土星

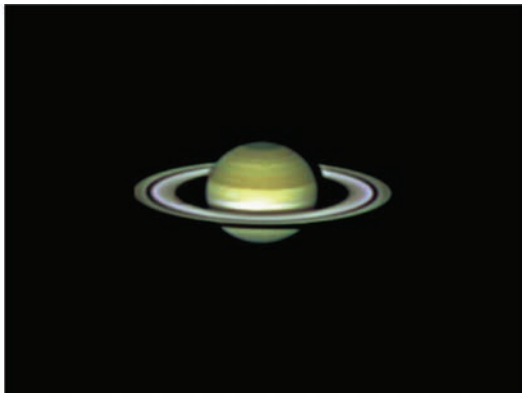


図 2: レンズ効果を受けない土星の像

上述の手法によって得られたレンズ効果を受けた像は以下のようになる。下の図 3 は，土星の像が，手前を通るブラックホールの重力場によるレンズ効果によって 2 つに見えている様子を示している。

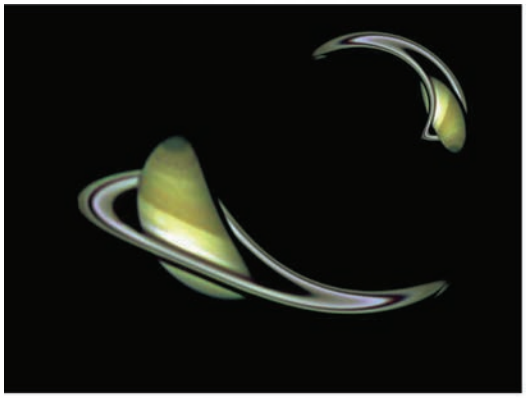


図 3: レンズ効果を受けた像

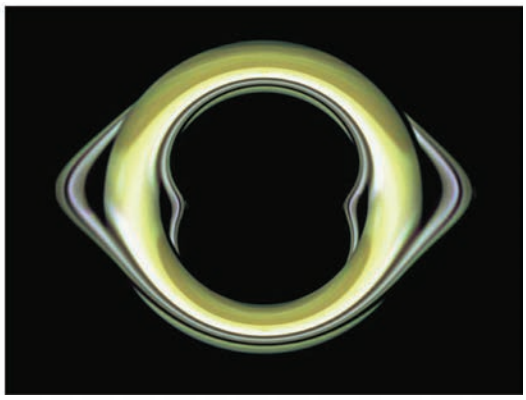


図 4: アインシュタインリング!

観測者からみて，重力レンズ天体と遠方の光源が視線方向の一直線上に並ぶ場合，重力レンズ効果によってリング状の像，アインシュタイン・リング が得られる。元々リングを持っている土星の場合はどうなるか? 上の右図のように，(土星の) リングの (アインシュタイン) リングができる!

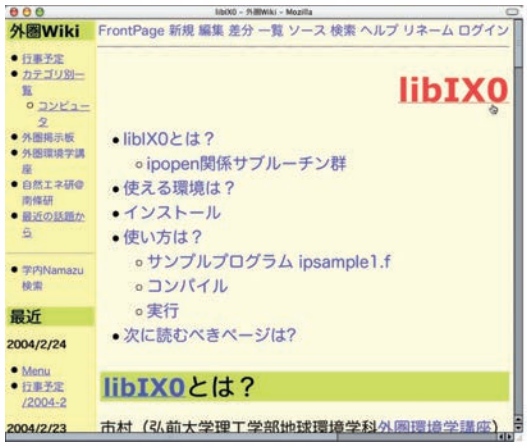
レンズ天体となるブラックホールの位置を変えると，像の位置や形がかわる．これらの様子を java script を利用したアニメーションにまとめたものは以下の URL で見ることができる。

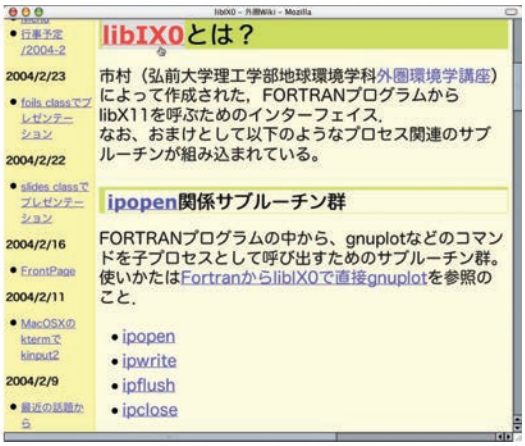
- 重力レンズでみた土星の像アニメ
  `http://windom.phys.hirosaki-u.ac.jp/member/kasai/lens-anim/`

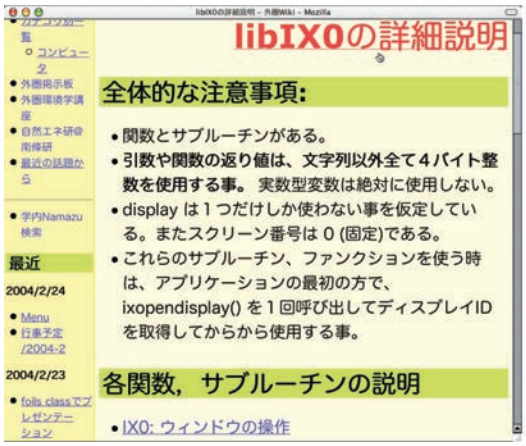
4 WEB 上の libIX0 ドキュメント: 外圏 Wiki

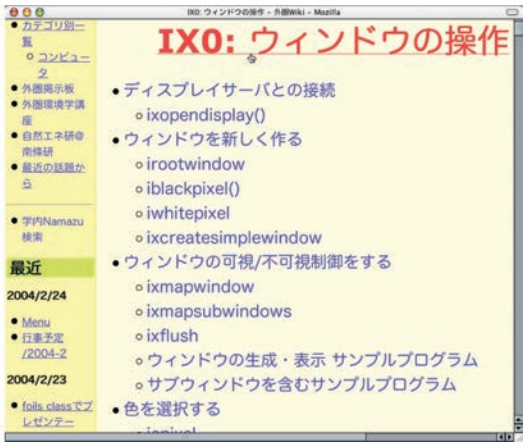
FORTRAN 用グラフィックライブラリ libIX0 のドキュメントは，我々の研究室の WEB ページ,「外圏 Wiki」からアクセスできる。ここには，ライブラリのインストール方法やプロセスへのアクセスを行う機能 (ipopen 関係) のサンプルプログラム等も掲載されている。

- 外圏 Wiki: `http://windom.phys.hirosaki-u.ac.jp/fswiki/`









5　最後に

今回作成したライブラリ libIX0 は，FORTRAN で行った数値計算の結果を，FORTRAN で可視化できるという点で非常に有用である。Xlib の機能をそのまま FORTRAN から呼び出す関数・サブルーチンが多いため，ある程度 X Window の知識が必要となるのが気になるが，これはより上位のサブルーチンを FORTRAN で作成すれば解決できる問題である。もっとも，X Window システムを学ぶための入口としては，このままで丁度良い題材となるかも知れない。

参考文献

[1] 木下凌一・林秀幸 著，X–Window Ver.11 プログラミング，日刊工業新聞社

[2] 柴山守 著，X11 による画像処理，技術評論社

自然災害映像を中心とした教育用ＶＯＤコンテンツの開発

理工学部地球環境学科　上原子　晶　久
kami@cc.hirosaki-u.ac.jp

理工学部地球環境学科　田　中　和　夫
ktana@cc.hirosaki-u.ac.jp

理工学部技術サポート室　佐　藤　勝　人
miri@cc.hirosaki-u.ac.jp

1．はじめに

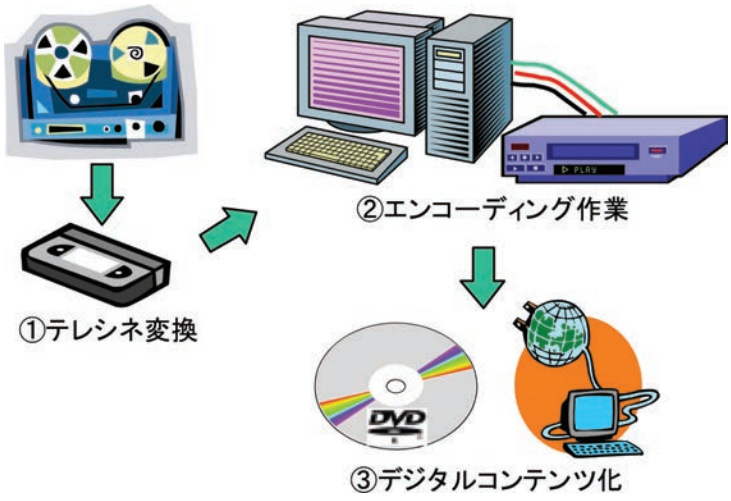
近年，ネットワーク環境の高速化により，教育現場でVOD（ビデオ・オン・デマンド）コンテンツが活用される機会が増加している[例えば1)]．本学においても，学内ＬＡＮがギガビットネットワークに移行したのを契機として，総合情報処理センターが中心となって，各種のVODコンテンツが配信されている．大学などにおける教育を目的としたVODによるコンテンツ配信の長所の一つとして，教員が授業で活用することの他に，受講者（学生）などが，授業時間以外でも当該コンテンツを閲覧できることが挙げられる．すなわち，インターネットが利用できる環境下で，受講者の都合の良い時間を利用して自習や復習などにVODコンテンツを役立てることができるのである．特に，筆者らが専門とする火山学や防災学の分野では，噴火や災害の現場，あるいはその状況を撮影した映像を見ることは，「百聞は一見にしかず」という諺に表される様に，被害の分析や情報の蓄積に非常に有効であると考えている．さらには，テープメディアなどに記録してある映像をデジタル化して，ハードディスクやDVDなどの光学メディアに保存し直すことにより，半永久的な保管が可能なる．

本稿では，筆者らの一人（田中）が実際の現場で撮影した火山の噴火映像について，VODコンテンツ化の方法，ストリーミング配信の方法，及びコンテンツの内容について概要を紹介する．なお，本プロジェクトの主要な範囲はVODコンテンツの作製であり，コンテンツのストリーミング配信については，筆者の一人（佐藤）が平成15年度理工学部研究教育プロジェクト補助金（学部長裁量経費）を受けて行ったことをあらかじめ付記する．

2．VODコンテンツ化の概要

VODコンテンツの元となる素材は以下に示した３つの動画である．

(a)　ニイラゴンゴ火山（コンゴ民主共和国）における溶岩湖の活動（撮影：1975・1982年）
(b)　ニアムラギア火山（コンゴ民主共和国）における溶岩噴泉・溶岩流（撮影：1982・1986年）
(c)　駒ヶ岳（秋田県）におけるストロンボリ式噴火（撮影：1970年）



図－１　VODコンテンツの概要

なお，これらの動画は，火山観測の際にオープンリール式の８mmフィルムで撮影したものである．音声はない．以上に示した３つの素材をデジタル化することによりVODコンテンツを作製した．その概要を図－１に示す．まず，８mmテープに記録された動画をテレシネ変換することにより，VHSテープに記録し直す．これは，図－１に示した様に，VHSのビデオデッキとパソコンを直結して動画のデジタル変換を行うためである．パソコンには，EPSON DIRECT社製の「Edi Cube MX1800HTV」を用いた．現在は，代替機種（EdiCube MW）となっているが，スペックの確認は同社サイトにて可能である[2)]．本プロジェクトで当該機種を選定した理由は，比較的安価であり，ビデオ編集用ソフトが附属していることによる．以上の装置の全景を図－２に示した．

図－２　コンテンツ作製装置の全景

図－３　ヒント情報の追加

３．VODコンテンツのストリーミング配信[3)]

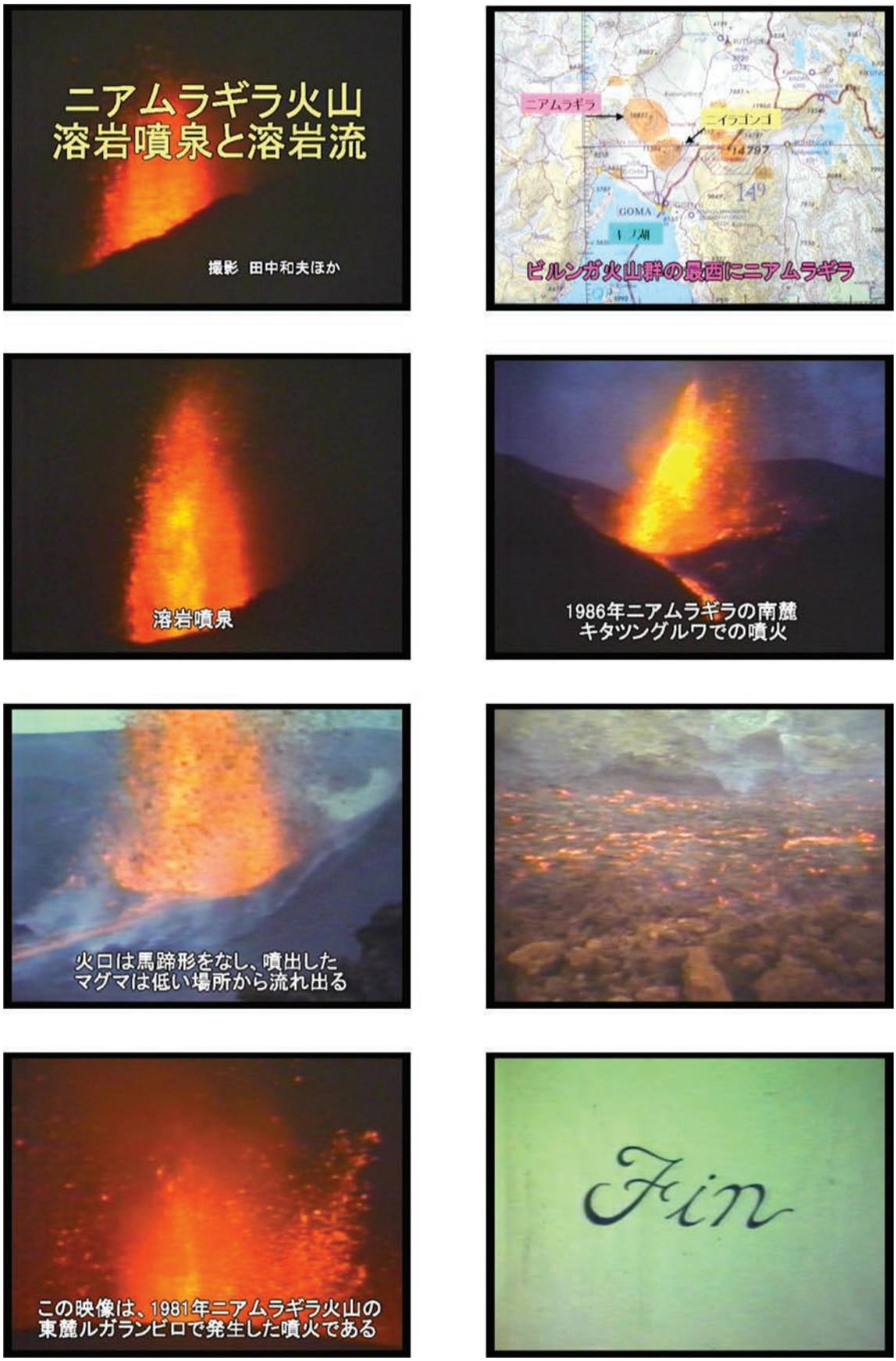
本プロジェクトにて採用した方法は，QuickTime Streaming Server５（QTSS-５）をストリーミングサーバ環境として利用する方法である．QTSS-５は無償のオープンソフトウエアであるDarwin Streaming Server５をベースとしたものである．以上は，無償であることから，ストーム配信ごとに発生するライセンス料が無料という利点がある．サーバマシンとしては，Apple社製Power Mac G５を，サーバOSはMac OS X Server 10.3を使用している．

一般的なストリーミング配信では，前節にて示した方法に従って，コンテンツとなる動画をMPEGやWindows MediaPlayer形式（拡張子は.wmv），またはQuickTime形式（拡張子は.mov）でサーバマシン内の所定のハードディスクに保存し，そのファイルについて配信方法の設定することにより配信を行う．本プロジェクトで採用したQTSS-５では，QuickTime形式，もしくはMPEG-４形式のファイルに限定して配信できるものである．ただし，実際にコンテンツを配信するためには，図－３に示したように，動画ファイルにヒント情報を追加することが必須となる．

４．火山噴火の開設とVODコンテンツの内容

火山噴火は，噴出するマグマの性質によって，その様式が数種類に分類される．それらはその噴火様式を呈する典型的な火山名を付して呼ばれる．粘性の小さなマグマを噴出するハワイ式噴火から順に、ストロンボリ式噴火、ブルカノ式噴火、粘性の大きなマグマを噴出するプレー式噴火などである．

図－４　ニイラゴンゴ火山における溶岩湖の活動



図－５　ニアムラギア火山における溶岩噴泉・溶岩流

図－6　駒ヶ岳（秋田県）におけるストロンボリ式噴火

ハワイ式噴火では、マグマの粘性が小さいので、マグマは噴水状に噴出し（溶岩噴泉)、溶岩流となって山腹を流下する．またその火口には灼熱の溶岩で満たされた湖“溶岩湖”が形成されることがある．わが国では、三宅島の1983年の噴火と伊豆大島三原山の1986年の噴火がこれに相当するが、両者とも噴火は短期間で終了し、溶岩湖は形成されなかった．

ストロンボリ式噴火では、マグマの粘性がやや大きくなり、小爆発を周期的に繰り返す．1970～71年の秋田駒ケ岳カルデラ内の中央火口丘，女岳，の噴火がこれに相当する．

ブルカノ式噴火は音響を伴う爆発的な噴火で，わが国の代表的火山である桜島や浅間山の噴火がこれに相当する．浅間山の噴火では麓の軽井沢で民家の窓ガラスが大音響のため割れたこともあった．

プレー式噴火では，マグマは粘性が大きく，固形物としてゆっくり地表に現れる．大量の火山灰などを上空高くまで吹き上げ，火砕流が生じた場合被害は甚大になる．雲仙普賢岳の1991年の噴火や有珠山の1977年の噴火がこれに相当する．

本報告で収録した映像は，わが国では観察されたことのない溶岩湖の様子，溶岩噴泉・溶岩流の流下の様子とストロンボリ式噴火である．

コンテンツに収録した映像のダイジェストをキャプチャー画面として図－５から図－７に示した．各コンテンツでは各映像の最初に火山の位置を示し，映像に関する解説をテロップで流してある．

以下に，映像の名称・火山名・撮影年月，映像の内容の順に記す．

(a) 溶岩湖の活動（９分45秒)【図－４】：ニイラゴンゴ火山，ザイール共和国（現コンゴ）
1975年３月，1977年９月，1982年７月撮影．火口縁より溶岩湖を俯瞰，距離約500m，火口底の温度約1000℃のマグマの湧き出しの映像．1977年溶岩湖の消滅時の火口，1982年溶岩湖再生の映像．火口より約500m，溶岩噴泉と溶岩流の昼夜の映像を含む．上流と下流での溶岩流の速度の差異が分かる．

(b) 溶岩噴泉・溶岩流（９分34秒)【図－５】：二アムラギラ火山，ザイール共和国（現コンゴ）
1982年１月撮影，1986年７～８月撮影

(c) ストロンボリ式噴火（８分50秒)【図－６】：秋田駒ケ岳，日本，
1970年９～10月撮影．カルデラ縁の男岳から撮影．距離約500m，直径30mの火口からの噴煙・噴石の映像が主．噴火現象では極めて珍しい噴煙環（環になったたばこの煙に同じ）の映像が含まれている．

５．おわりに

以上紹介した全コンテンツは，http://www.gōdardw.hirosaki-u.ac.jp/で閲覧することが可能である．本文中でも触れたが，閲覧にはQuickTimePlayerが必要である．現段階では，QuickTime Playerのみを対象としたストリーミング配信であるが，今後，各種の再生ソフトウエアに対応していきたいと考えている．

本プロジェクトは，平成14年度総合情報処理センター研究開発プロジェクト経費を受けて実施したものである．末筆になり恐縮だが，ここに記して関係各位に深く感謝する次第である．

参考文献

１）先生のための教育映像情報サイト：http://www.gakken-eizo.com/index.htm
２）エプソンダイレクト社ホームページ：http://www.epsondirect.co.jp/
３）佐藤勝人：教材資料を生かした学内教育用ストリーミングサーバの構築，平成15年度高エネルギー加速器研究機構技術研究会報告集，CD-ROM

ギガビットネットワークを利用した教育用ビデオ作品のオンデマンド配信

農学生命科学部　応用生命工学科　細胞工学講座　畠　山　幸　紀
hatakeya@cc.hirosaki-u.ac.jp

農学生命科学部　生物機能科学科　生命理学講座　黒　尾　正　樹
kuroo@mb.infoaomori.ne.jp

総合情報処理センター　小　倉　広　実
ogura@cc.hirosaki-u.ac.jp

1．はじめに

オンデマンドon-demandとはユーザの要求があった時に画像・音声・文字などによる情報サービスを提供する方式のことである。ホームページの閲覧やファイルのダウンロード、メールの受信などはインターネットを利用したオンデマンドのサービスである。一方、テレビやラジオ放送はオンデマンドではないサービスである。他者（送り手側）によって内容と配信時間（タイムテーブル）が決められているからである。1990年代はじめ、ケーブルテレビや光ファイバー網を使って映画を配信するビデオオンデマンド（VOD：Video On Demand）配信が行われるようになり注目されたが、企業としては採算性が合わず、撤退が相次いだ。映画を中心とした多くの作品がネット配信を想定していなかったため、著作権の関係から魅力的なコンテンツを集められず、結果として視聴者（有料会員）数が伸びなかった事が原因のひとつである。しかし21世紀に入り、ADSLやFTTHなどの高速通信、いわゆるブロードバンド回線の普及により、インターネットによる動画配信サイトが急速に増加し続けている。現在では高解像度（720×480ドット）で２時間以上の映画をまるごと配信するサイトもある。インターネットを使ったビデオオンデマンド配信を「インターネットTV」と呼ぶサイトもあるが、商標ならともかく、一般名としては適切ではないだろう。ただし、ストリーミング技術を用いたライブ配信はイメージとしてはテレビ放送に近い。

本学では2002年３月にギガビットネットワーク（高速ネットワーク回線）が敷設された。さらに2003年２月に総合情報処理センターの教育用システムが、高速ネットワークに適応した形で更新された。本学では以前よりオリジナルあるいは既成の動画コンテンツを学内外に向けて配信しているが、作品数や取り上げている分野、コンテンツの総量（のべ再生時間）などを考えると、さらに充実させる必要がある。そこで、一般あるいは専門教育の講義においても活用できるような、教育用ビデオ作品のオンデマンド配信を企画・提案した。今回は自作（オリジナル）のビデオではなく、一般あるいは教育機関向けに販売されている科学ドキュメンタリー作品をできるだけ多く配信することを考えた。また、動画のファイル形式や変換条件など、高音・高画質で配信するための条件を検討することも目的の一つである。本稿では配信用サイトの制作過程を配信契約の概要や技術情報を交えて報告する。プロジェクトの概要は、次の通りである。⑴ビデオ作品の選定と購入、⑵動画ファイルへの変換および配信条件の検討、⑶配信用Webサイトの作成、⑷教官・学生への告知（広報）。

今回作成した動画配信用Webサイトはhiroin-VODと名付け、学内限定で公開している。

http://www.stu.hirosaki-u.ac.jp/~seimei/hiroinVOD/

総合情報処理センターの教育用ホームページからリンクしている。

図１　動画配信サイトhiroin-VODのトップページ。写真はシステム更新前の農学生命科学部サテライト端末室。

２．VOD配信契約と作品の選定

著作権法により、放送されたものを録画したものや、市販されているビデオ教材をそのままネット配信することはできないため、まず、VOD配信をみとめている事がビデオ作品を選定する前提になる。数年前まではVOD配信を行うためには、製作または販売側と個別に交渉しなければならず、ほとんどの場合、配信不可という返事をもらうか、高額の配信料を要求され、結局断念しなければならなかった。今回も科学映像作品では有名な、ある映画製作会社とVOD利用が可能であるかどうか、責任者と直接交渉を行った。映画を製作する段階でスポンサーや監修者、映像資料の提供者などとVOD配信について契約しておかなければならないことや、会社側も今までVOD配信を想定していなかったということなどで、残念ながら契約は実現しなかった。しかし、最近は大学等における学内ネットワークの整備に伴い、VOD配信可能な作品を扱う業者も現われてきたため、今回はそのような業者と契約を行うこととした。従って、今回配信しているビデオ作品はすべて正規にビデオオンデマンド配信契約を結んでいるので、著作権上の問題はない。ネット接続可能な講義室でこのサイトにアクセスし、画面をスクリーンに投影して学生に見せるような使い方も可能である。ただし、動画ファイルをダウンロードして保存し、再配布することは違法行為となるので、絶対に行わないで欲しい。

契約によって詳細は異なるが、主なVOD配信契約の内容は次のようなものである。

・事業所（キャンパス）ごとの契約であること。
・作品の編集や改変は行わないこと。
・VOD配信契約料は、テープのみの販売価格の1.5～２倍。
・配信期間（５年）とするものと永久配信権の場合がある。
・ハードディスク等に取り込んだ後、作品テープの返却を求められる場合があった。

永久配信契約の場合は、著作権者より配信中止の申し出があった場合は別途協議する、という条件が付いている。また、契約料金には影響しなかったが、利用予定者や端末数の記載が必要であった。

配信するビデオ作品の選定は、VOD配信契約が可能であることが前提条件となるが、そのほか、以下のような方針で行った。

・内容的に学生の知的好奇心を刺激するような優れたものであること。
・価格および配信契約料が高額ではないこと。

作品の再生時間に対する価格も考慮する。できるだけ長い作品（30分以上）を選ぶ。

・科学英語教材としての利用も考え、２カ国語であること。

前述したようにVOD配信契約ついて調査したところ、中には配信期間を設定しているものがあったため、まず、そのような条件のない４作品を購入し、ネット配信の技術検討に用いることにした。４作品を試験配信している間に、試験配信サイト上と、農学生命科学部教官へメールでビデオ作品の推薦をお願いした。しかし、推薦していただいた作品は、VOD配信不可であったため、今回は要望に答えることは出来なかった。今回はBBCビデオ12作品、米国Telecourses教材４作品について契約を行い、VOD配信を行っている。(配信リスト参照)

図２　配信作品リストのページ

3．動画の配信条件の検討

インターネットによる動画配信が普及した背景は、ネットワークの高速化とともに動画ファイルの圧縮および配信技術の進歩がある。主な動画フォーマットと拡張子はAVI（.avi)、QuickTime（.mov)、WindowsMedia（.wmv)、RealVideo（.rm）などである。動画や音声の圧縮（エンコード)、伸長（デコード）を行う規格あるいはプログラムをコーデックcodecと言い、MPEG形式（.mpg)、DV（Digital Video）形式、最近ではDivX形式など多数存在する。複雑なのは、拡張子だけでどのコーデックを使用しているか判断できないため、同じ拡張子を持つファイルでもパソコンの環境（インストールされているコーデック）によっては再生できない場合あるということである。再生に必要なソフトウエアやプラグインについては配信サイトhiroin-VODに解説文を掲載してある。

図３　ファイル形式の選択。MPEG-１形式のファイルはどのプレーヤーでも再生できる。

科学番組を配信する場合、画質は重要である。顕微鏡映像がぼやけたり、字幕がつぶれて読めないようでは実用的ではない。また、端末上で再生されるまで時間がかかったり、コマ落ちが生じるようではいけない。画質や音質と動画のファイルサイズを決める要因は複雑で、適切なパラメーターを決定するのは難しい。そのため、どのような条件で配信用の動画ファイルを作成するかは、重要な点である。しかし、今回はインターネットによる一般向けの配信とは異なり、学内のギガビットネットワークを利用するため、ある程度、動画のファイルサイズを大きく、また転送レートを高く設定することができる。動画のソースはすべてテープ（VHS）であるため、コーデックにDVを用いた拡張AVI形式（AVI 2.0）でエンコードした。解像度は720×480ドット、フレームレートは29.97fpsで、データのバックアップの意味合いもあるので、画質の劣化が少ない形式で保存した。従来のAVI形式（AVI 1.0)で

は２Gバイトのファイル制限があり、長時間の動画は複数のファイルに分割されてしまったが、拡張AVIではファイルサイズに制限がなくなった。(但し、ディスクのフォーマットがFAT32の場合は４Gまで。) AVIからMPEG-１ (352×240ドット、ビデオビットレート1.15Mbps CBR) へ変換したものでも、ネット配信可能であったが、パソコンの環境によってはコマ落ちが見られたため、MPEG-１からさらにReal9、あるいはWindowsMedia ９形式で再エンコードしたものも用意した。設定によって画質やファイルサイズは大きく異なるが、45分の作品ではMPEG-1で472MBだったものが、WindowsMedia ９で367MB、Real9で158MBとなった。VOD配信契約の際に問い合わせたところ、同じ作品を複数の動画ファイル形式で配信することは問題ないそうである。hiroin-VODでは同じ作品をさまざまな動画ファイル形式で比較することができるので、試して欲しい。ビデオ作品の合計時間は約12時間、日本語と英語の二つのファイルを作らなければいけなかったので、合計24時間を超えるデータを変換することは大変な労力である。経験した方はわかると思うが、パソコンの性能、変換パラメーターの設定等によって異なるが、エンコードするのにソースの時間の数倍必要とするのが普通だからである。したがって、すべての作品を一斉に配信する訳には行かず、できあがったものから順次公開することとなった。

動画ファイルの作成や配信条件は教育用端末室のシステムで視聴することを前提に決定した。結果としてMPEG-１形式での配信でも大丈夫であったが、研究室等で使用するパソコンのシステム構成によっては上手く再生できない可能性もある。ファイルが再生されるまで時間がかかる場合があった。動画配信用サーバーへの同時アクセスの影響が考えられたが、同時アクセスによる負荷試験は行っていない。

図４　音声を選択するページ。音声、ファイル形式どちらを先に選択しても良い。

4．動画配信用のWebサイトの制作

動画のタイトルとリンクだけのページでは申し訳ないので、配信用のサイトをデザインした。ビデオの一場面を画像（静止画）として使用する場合には、別途、著作権者の許諾が必要で、今回の配信契約に画像の使用権は含まれてない。そのため、作品のタイトル画像はフリー素材とオリジナルの画像を使用している。フリー素材は総合情報処理センターの教育用システムのホームページで提供されているものも一部使用した。

図５　作品の解説ウインドウ。先に配信リスト一覧から作品を選び、動画ファイルを選択することも出来る。

Webページで動画を表示させるにはhrefタグを記述して直接リンクを張っても良いが、MPEG形式のように複数のプレーヤーがサポートしている形式では、ブラウザのデフォルト設定（教育用端末室ではQuickTime Player）に従ってしまうため、Real OneとWindowsMedia Playerを指定するメタファイル（拡張子.ram .asx）を使用した。メタファイルは動画ファイルの情報をプレーヤーに指示するためのテキストファイルで、データがディスクにキャッシュされないため、動画の再生開始が早くなるという利点もある。使用するブラウザやプレーヤーによる動作確認の結果はhiroin-VODの技術情報のページに記載してある。教育用システムの更新後もソフトウエアのバージョンアップが行われているため、情報は随時更新するようにしている。ブラウザによって、Webページのデザインに（意図的に）使用したFlashやJavaScriptの動作にも違いがみられるので、興味がある方は参考にしていただきたい。

hiroin-VODは学内限定であるが、リンクは自由に張っていただいて構わない。しかし、動画ファイル、メタファイルへの直接リンクはパフォーマンス低下の原因となり、また配信契約上も問題となるので絶対に行わないで欲しい。hiroin-VOD Topページにお願いしたい。

5．考　　察

ビデオ作品のネット配信はビデオテープの使用と比較した場合、以下のような利点があげられる。

・繰り返し視聴することによる理解度の向上。(オンデマンド配信)
・時間の活用：学生は講義の空き時間等に視聴することができる。(予習や講義の補足)
・教官側も授業中にビデオを見せる必要が無いので、講義時間を有効に使える。
・教官が個別にビデオ作品を購入する経費の節約。
・利用効率：例えば図書館でテープの貸し出しを行う場合よりも、効率的である。
・ビデオテープの劣化の回避。

専門および一般教育におけるインターネットを利用した講義は、情報処理以外では語学教育の一部を除いて盛んに行なわれているとは言えない。今回作成した配信サイトは、次のような科目でも利用可能ではないかと考えている。

「基礎ゼミナール」：健康の維持・管理に関する番組も用意した。精神的・肉体的に不安定になりがちな（？）大学生の生活指導に活用して欲しい。

「科学英語」：語学教育に利用するために、英語版の配信も行っている。また、BBC製作のHORIZONはスクリプトをBBCのホームページで全文公開している作品もあるので、英文を参照しながら番組を見ることによって理解を深めることができるだろう。

「専門科目」：このサイトの製作者の所属学部（農生）の関係から、「生命科学」関連の番組を中心に配信しているが、狂牛病や生命倫理を扱った作品など、他学部の学生にとっても興味深い作品が多いと思う。

本学の総合情報処理センターが提供しているBBC Worldのネット配信は、オンデマンドではなく「ライブ」と呼ばれる方式である。テレビ（衛星）放送と同じタイムテーブルであるため、大学の講義で特定の番組を利用することは困難である。これは契約上の制約による。（非常に有用で興味深い番組も多数あるので、平成16年度以降も継続して欲しい。）オンデマンド配信の最大のメリットは時間的制約からの解放である。そして、見たいと思った時にいつでも見ることができるということである。このことは学生の知的好奇心に答え、学習のモチベーションを高めることにつながるはずである。校費などでビデオ購入の際に販売元とVOD配信契約を結んでいただければ、このような形で学内ネットワーク配信を行うことができる。すでに購入したビデオも配信契約を追加契約できる作品もある。以前よりは安価になったとはいえ、一作品あたり数万円必要である。同窓会や後援会で雑誌の購入を補助している学部があるが、VODコンテンツを充実させるため、是非、ビデオ作品の購入も検討していただきたい。

ブロードバンド回線が普及し、動画配信サイトが増加したと言っても、アニメや映画などの娯楽作品が中心で、科学番組を配信しているサイトは僅かである。動画配信を生涯教育や公開講座の手段として積極的に活用している大学もある。しかし、私が見た限りでは講演の様子をそのまま流しているだけで、一般の人がそれほど「おもしろい」と感じるようなコンテンツは少ない。(スライド映像が不鮮明だったりすることも一因。) 予算の限られた地方大学でも積極性と工夫しだいで「人気コンテンツ」が生まれる可能性もある。大学の社会貢献の一つとして動画の配信を積極的に取り組んでみてはどうだろうか。

資料：配信中のタイトルリスト

米国　Telecourses 教材
- ストレスを上手にコントロールしよう　Lives in Balance
- 性的行動　Risky Business
- 病原菌との戦い　Germ Warfare
- 人体の防衛　Human defenses

BBC　ビデオ
- 人間はなぜ笑う：ADHDにおける笑いと遊びの効果　BEYOND A JOKE
- 三重苦を乗り越えて　DEAFBLIND
- 死角・SIDS（乳幼児突然死症候群）予防法研究の陰で　SUDDEN DEATH
- 呼吸と命　BREATH OF LIFE
- ある骨格の謎　SKELTON KEY
- ムーンチルドレン――紫外線と遺伝子の攻防　MOON CHILDREN
- 蚊と人間の100年戦争　MOSQUITO！
- 狂牛病　BSE（２巻組）
  - １．病原体解明への道　THE INVISIBLE ENEMY
  - ２．スチーブンは感染したのか　THE HUMAN EXPERIMENT
- ホルモン作用の不思議　BODY CHEMISTRY（３巻組）
  - １．HORMONE HELL
  - ２．HORMONE HEAVEN
  - ３．HORMONALLY YOURS

付記

１．本文中の製品名、プログラムの名称等はそれぞれの所有者の登録商標あるいは商標です。

２．本プロジェクトは、各部局のネットワーク委員会に相当する「農学生命科学部マルチメディア教育委員会」の企画として提案したものである。(平成14年度委員長：黒尾、平成15年度委員長：畠山)

（以上、文責　畠山）

広報HIROINの刊行方法の見直しとホームページの活用

教育広報専門委員会　小　山　智　史

koyama@cc.hirosaki-u.ac.jp

本号より、「広報HIROIN」の刊行方法を多少変更しましたので、ご説明させていただきます。関連して、センターのホームページのことについても触れたいと思います。

□　広報HIROINの刊行回数が年１回になりました。

従来、広報HIROINは９月と３月の年２回刊行していましたが、今年度より年１回（３月）の刊行といたしました。これに伴い、「研究開発報告」「解説記事」などは、従来どおり冊子に掲載しますが、「利用状況」と「委員会報告」はホームページに移行することにしました。これらの情報は、既に昨年度分よりホームページに掲載しています。

なお、ホットな情報やタイムリーな解説記事など、ホームページをより積極的に活用する具体的な方策について今後検討する必要があると思われます。

□　広報HIROINがA4版になりました。

冊子のサイズをB5版からA4版に変更いたしました。これに伴い、原稿執筆要項を上下左右の余白を指定するように変更しました。詳しくは次ページの要項をご覧ください。

HIROINはホームページでも閲覧できるようになっています。従来の刊行分については、スキャナで読み込むなどの方法をとりましたが、昨年度からは、冊子の印刷を発注する時にpdfファイルでの納入も指定しており、ホームページへの掲載も簡単になりました。

□　ホームページが新しくなりました。

委員会では、センタースタッフと相談しながら、センターのホームページの見直しを行いました。主な点は次のとおりです。

・トップページを９月に作り直しました。従来のデザインを踏襲したので、気付いた方は少なかったかもしれません。
・シンプルなページにしたので、ページが軽くなりました。また、項目の追加や更新がしやすくなり、更新の頻度が高くなりました。
・すべてのページに更新日を入れました。これにより、見る人が「情報の新鮮さ」を確実に判断できるようになりました。
・Webアクセシビリティについて配慮しました。ただし、まだトップページや委員会のページなど一部にとどまっています。

規則、利用状況、研究開発課題一覧、委員会報告などの他、今年度作成したセンター概要（パンフレット）も掲載されていますので、ご覧ください。

ホームページの作成はセンタースタッフの方々が分担して行っています。委員会の関わり方としては、年１度程度、その時点の状況を把握した上で、意見を具申するのが適当ではないかと考えています。

総合情報処理センターのホームページ　http://www.cc.hirosaki-u.ac.jp

HIROIN原稿募集要項

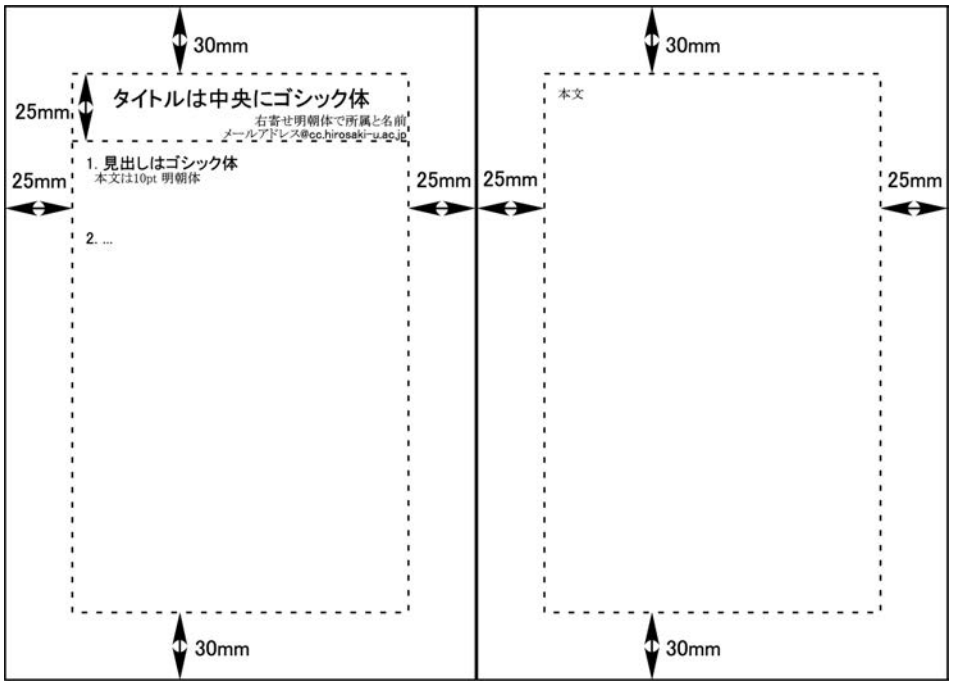
弘前大学総合情報処理センターでは，下記の要領でHIROINの原稿を募集しております。奮ってご投稿下さい。

記事の内容：

・計算機に関する論説，随想
・計算機を利用した研究の紹介，
・計算機利用に関する研究開発
・プログラムの実例と解説
・センターに対する要望，質問
・利用者相互の情報交換
・その他（センター利用者が興味を持つと思われる話題）

執筆上の注意事項：

A4サイズ（様式は下図）で印刷原稿を提出して下さい。また，できましたらE-mail等による電子化原稿（pdfや各種ワープロソフト）の提出に御協力下さい。提出時に使用したソフトウェアの種類をお知らせ下さい。希望があれば執筆者に別刷り50部を贈呈します。50部を超える分については，著者負担といたします。投稿時に申し出て下さい。



1枚目（ページ番号は入れない）　2枚目以降（ページ番号は入れない）

原稿の送付先および問い合わせ先：

〒036－8561　青森県弘前市文京町3
弘前大学総合情報処理センター　教育広報専門委員会
（0172－39－3721（直通），内線3721）
E-mail　koho@cc.hirosaki-u.ac.jp

編　集　後　記

今期の教育広報委員会において広報HIROINの編集内容が検討し直され，いくつかの変更がなされました。広報誌のサイズがB5版からA4版へ変更され，これに伴いページ設定が変わりました。また掲載内容についても見直され，業務報告や委員会報告は総合情報処理センターのホームページに掲載することとし，広報HIROINの掲載内容は解説記事や研究開発報告が中心となります。これらの委員会決定の下に広報HIROIN No.21の編集担当に選任されました。専門外の広報誌を編集するのはなかなか大変な作業と覚悟をしておりましたが，執筆者各位のご協力により予定通り何とか発刊できそうです。ここに改めて執筆者各位にお礼申し上げます。

新しく生まれ変わった広報HIROIN No.21が皆様のお手元に届くのが，国立大学の法人化と期せずして時期が重なりました。21世紀は「知の時代」とも言われ，法人化された後の大学には「知の創造と承継」を担うことが期待されております。弘前大学は個性を生かしながら，教育研究を一層発展させていかなければなりません。数年後に予定されている中間評価の時期に査定の対象となるよう，今後，広報HIROINの解説記事や研究開発報告が充実していくことを願ってやみません。（鈴木裕之）

弘前大学総合情報処理センター
教育広報専門委員会

小野寺　　進（人　文　学　部）
小　山　智　史（教　育　学　部）
須　田　俊　宏（医　　学　　部）
松　木　明　知（医学部附属病院）
石　本　　淳（理　工　学　部）
丹　波　澄　雄（理　工　学　部）
鈴　木　裕　之（農学生命科学部）
清　宮　良　昭（医療技術短期大学部）
岡　田　　潔（附　属　図　書　館）

センター主要アクセス一覧

研究用サーバ

接続システム名	ホスト名	ドメイン名	IPアドレス
総合情報処理センターWWWサーバ	period	www.cc.hirosaki-u.ac.jp	
研究用メールサーバ	mail	mail.cc.hirosaki-u.ac.jp	
研究用汎用UNIXサーバ	tsugaru	tsugaru.cc.hirosaki-u.ac.jp	
研究用計算サーバ	tappi1～8	tappi1.cc.hirosaki-u.ac.jp ～tappi8.cc.hirosaki-u.ac.jp	
学内向けニュースサーバ	news	news.cc.hirosaki-u.ac.jp	
学内向けDNSサーバ	slash	slash.cc.hirosaki-u.ac.jp	133.60.240.14
	dash	dash.cc.hirosaki-u.ac.jp	133.60.238.42

教育用サーバ

接続システム名	ホスト名	ドメイン名	IPアドレス
教育用メールサーバ	mail	mail.stu.hirosaki-u.ac.jp	
教育用WWWサーバ	c0web1	www.stu.hirosaki-u.ac.jp	

学外向けサーバ

接続システム名	ホスト名	ドメイン名	IPアドレス
WWWサーバ	www	www.hirosaki-u.ac.jp	
NTPサーバ	hirontp	ntp.hirosaki-u.ac.jp	
ニュースサーバ	owani	owani.gw.hirosaki-u.ac.jp	
DNSサーバ	moya	moya.gw.hirosaki-u.ac.jp	133.60.14.101

弘前大学総合情報処理センター広報

ＨＩＲＯＩＮ　　第 21 号

平成16年３月　発行

編　集　　弘前大学総合情報処理センター
　　教育広報専門委員会
発　行　　弘前大学総合情報処理センター
　　〒036-8561　青森県弘前市文京町３番地
　　Tel　0172-39-3721
　　Fax　0172-39-3722
印　刷　　青葉印刷株式会社
　　〒036-8171　青森県弘前市取上１-８-２
　　Tel　0172-33-8221㈹