図書館システムを取り巻くセキュリティの現状と展望

田邊（たなべ）　稔（みのる）
（メディアセンター本部課長代理）

1．はじめに

インターネット技術の進化と発展により，今日では質の良し悪しを問わず，ありとあらゆる情報がネットから簡単に入手できるようになった。また，ブロードバンドネットワークや高性能なノートパソコン，PDA（Personal Digital Assistance），携帯電話などモバイル端末の普及により，必要な情報は職場以外に自宅や外出先，および移動中の車内でも入手することができる。いわゆる「ユビキタス」環境が整備されてきた。先ごろ刊行された『インターネット白書 2005』によると，国内のブロードバンド利用者数は，3,000 万人を突破した。大学図書館においても，研究・教育に必要な論文や文献情報を商用データベース，電子ジャーナル，電子ブックなどの電子リソースとして 24 時間 365 日提供することが可能となった。

しかしながら，このような利便性を悪用したサイバーテロ，不正アクセス，ウイルス/ワーム，スパイウェア，フィッシング詐欺などの脅威は後を絶たない。また，ここ数年世間を騒がせている「情報漏洩事件」については，外部からの攻撃によるものよりも，「内部犯」によるものが大半を占めている。スタッフのノートパソコンや USB メモリなどによる情報の持ち出しは日常頻繁に行われているため，いつ情報が漏洩しても不思議はない。図書館で提供する電子ジャーナル・商用データベース（以下，EJ/DB）サービスにおける，「OpenProxy 経由の不正アクセス」や「スクリプトによるシステマチック・ダウンロード」も内部から外部への不正利用に他ならない。

そこで，このようなセキュリティ・リスクをいかに回避するか，図書館経営トップから現場スタッフ，ひいてはエンドユーザ（利用者）に至るまでのセキュリティ意識をいかに向上させるか，について模索したい。図書館システムにおけるセキュリティはシステム担当者だけが考え，取り組む問題ではなく，図書館にかかわるすべての構成員の意識改革がゴールである，ということを念頭に話を進めていきたい。

2．図書館システムの基盤と脅威

慶應義塾大学の図書館システム（以下，KOSMOS II）を支える基盤は，基幹サーバ，基幹ネットワーク，およびパソコン（以下，PC）やプリンタなどの周辺機器に大別される。KOSMOS II の基幹サーバは，三田図書館の地下 3 階サーバ室に設置されており，DB サーバ×2 台，Web（OPAC）サーバ×2 台，アレイディスク×1 台の冗長化（クラスター）構成となっている。当構成の最大の特徴は「フェイルオーバー機能」である。この機能は「サーバの停止時間を最小限に抑えたい」，「ハードウェアの障害であっても，サービスを停止させたくない」という要望を満たす機能である。これにより，メイン機の障害時，自動的にバックアップ機が IP アドレスやサーバ名をメイン機から引継ぎ，サービスを継続してユーザに提供すること（縮退運転）ができる。

また，日々更新される書誌・所蔵データ，閲覧ジャーナル，利用者データなどのバックアップは毎晩夜間に実施している。バックアップ取得したテープ（SuperDLT）は，定期的に慶應の保存書庫である白楽サテライトライブラリーへ送付し，外部保管を行っている。これは，万一三田が地震，火災，津波などの災害に遭っても，データが復旧できるようにするための危機管理対策の一環である。

基幹ネットワーク機器（CISCO Catalystスイッチ）は，各地区に 1 台ずつ設置され，各メディアセンター間の通信は VPN トンネル経由で行っている。図書館のネットワークは 3 つのセグメントから構成される。公開サーバ用のグローバルネットワーク，業務用 VPN，OPAC/CD-ROM 端末用 VPN である。これらのネットワークトラフィック監視やポートフィルタ設定などについては，インフォメーション・テクノロジー・センター（以下，ITC）が一元管理してい

る。

KOSMOS IIサーバや各種サーバについては，年に数回OSのバージョンアップ，セキュリティパッチなどのメンテナンス作業でシステムを停止している。これらの作業は，システムの安全性を保つ上では不可欠なため，本来定期的に保守時間を確保したいが，現状ではその都度システム停止の調整を行っている。但し，重大なセキュリティホールやウイルス騒ぎが発生した際は緊急停止を余儀なくされる。

PCやプリンタなどの周辺機器は，リプレースを重ねる毎にその数を増加させている。機器の購入形態は,昔のように買い取りやレンタル契約ではなく,リース契約を基本としている。リース契約期間は3〜4年である。導入数増加の要因は，仕事量の増加だけではなく,「複数で共用していたPCが1人1台環境にシフトした」,「1人で数台利用するケースが増えた」,「故障時の予備機をやや多めに導入した」ことなどがあげられる。しかし，これは同時に攻撃（被害および加害）対象が増えていることを示す。過去3回(1999年，2002年，2005年)の機器リプレースにおける周辺機器数とスタッフ数の推移を表1に示す。

表1．周辺機器数とスタッフ数の推移(5地区分)

種類/年度	1999年度	2002年度	2005年度
業務用PC	274台	376台	446台
OPAC-PC	117台	139台	156台
プリンタ	83台	93台	104台
スタッフ数	291人	287人	283人

リプレースする毎に機器の性能は向上し，1台当りの価格は低下している。同時にOSやアプリケーションの機能も同時にグレードアップしていることからバグなどによるセキュリティホールの数も増えるため，頻繁にバージョンアップやパッチ作業が必要となる。これらの手間はばかにならない。一方，モバイルPCの導入台数も増えており，以前はシステム担当者のリモートメンテナンス用として数台程度導入しただけだったが，2005年度のリプレースでは，全地区で20台導入した。理由としては，ブロードバンド環境の普及などにより，キャンパス間の移動や自宅・出張先で仕事をするケースが増えていることがあげられる。

また，パソコンだけでなく，USBフラッシュメモリによる情報の持ち出しの機会も増えている。容量にもよるが，最近では数千円程度で手に入り，ノートPCやCD-R/RWを持ち出すよりも手軽で便利だからである。さらに，USB2.0の最大データ転送速度は480Mbpsであり，従来のUSB1.1と比べて理論上40倍の速さになったことも利用促進の一要因であろう。但し，気軽に情報が持ち出せるようになると，それだけ漏洩のリスクも増すこととなる。持ち出す情報の内容にもよるが，たとえ個人情報が含まれていなくとも，企業秘密的な情報や著作権・プライバシー侵害に抵触する情報が含まれる可能性があるため，情報持ち出しのルールや制限などを決めておく必要がある。

一方，情報の持ち込みについても同様にリスク管理が必要となる。自宅や出張先でウイルス/ワーム感染したPCやUSBメモリを安易に職場のネットワークに接続したらどうなるだろうか？瞬く間にネットワークに接続されているコンピュータ全体に感染が広がることは言うまでもない。幸いなことに，現在のところメディアセンターにおいて,「最悪のシナリオ（個人情報漏洩事件)」は発生していないが，いつ発生してもおかしくない状況にある。このようなケースについてもセキュリティ・ガイドラインに組み込んで対策を講じる必要がある。

なお，参考までに大学関連で最近発生した情報漏洩事例（国内・海外）をいくつか示す。

■国内事例

・京都大学で約1,600名の情報の入ったPCが盗難（2005/5/10）
・お茶の水女子大学で，卒業予定の一部学生(106人）の名簿と，未記入の卒業証書の用紙7枚を紛失（2005/3/11）
・新潟大学の成績情報流出，PDFファイルが検索サイトのキャッシュに（2005/3/1）

■海外事例

・カリフォルニア大学バークレー校で約98,000人分の情報漏洩（2005/3/28）
・カリフォルニア州立大学チコ校の関係者約59,000人分の個人情報盗難（2005/3/22）
・ボストン大学の学内ネットワークに不正侵入事

件（2005/3/18）

情報が漏洩した場合，企業であれば，例えばノートPCを電車の網棚に置き忘れて紛失したり，家に持ち帰ったPCが盗難に遭った社員についても刑事罰が問われるケースがあるが，国内の大学においては，今のところそこまでの自己責任を問われることは少ない。これは，大学という組織が企業に比べて，「企業秘密」といった概念が薄いことや，情報漏洩事件が発生して業務が停止した場合の「1日あたりの損失額」という概念がないことが背景にある。確かに，大学においては，処罰という観点でのリスクヘッジは決めにくいかもしれないが，外部からの信頼を失ったり，ブランドイメージを傷つけたりすれば，収入の低下にもつながるため，あきらかに損失といえる。少なくとも，万一個人情報が漏れた場合の連絡体制や対応責任者および対応方法などについては最低限明確にしておく必要がある。

3．セキュリティ対策

メディアセンター本部（以下，本部）でこれまで実施してきた主なセキュリティ対策を以下に示す。

・ウイルス対策とWindowsUpdateの集中管理

本部では，数年前から，業務用PCのセキュリティ維持対策として，ウイルス対策管理ソフト（Virus Buster Corporate Edition）とWindowsUpdate管理ソフト（Update Expert）を導入し，本部管理サーバから全クライアントを集中管理している。これにより，PC間のセキュリティレベルを一定に保てる。

・新業務用PCのセキュリティ強化ポイント

2005年4月より新たにリース契約した業務用PCには，主に3つのセキュリティ対策を施した。

1）USB記憶媒体への書き出し禁止

個人情報保護対策の一環として，標準設定でUSBメモリへの書き出しを禁止した。7月より許可申請書（要所属長印）が提出されれば解除するという運用を開始した。

2）ソフトウェアの導入制限

ローカルAdminパスワードを非公開とすることにより，標準設定以外のソフトウェアを誰でも自由に導入することを禁止した。追加したい場合は，各地区のシステム担当者経由で本部宛に申請を行えば，問題の多いソフトウェア（Winny，WinMXなど）以外は許可し，管理者立会いの下で作業を行うこととした。

3）パスワードの強化

従来，パスワードを「初期状態のまま」，「すぐ予想のつく簡易なもの」，「一度設定したら何年もそのまま」としているケースが多かったことから，パスワードポリシーを次のように設定した。

・パスワード有効期限を90日間とする
・7文字以上で英大文字・英小文字・数字・記号のうち3つ以上利用する
・パスワード履歴（使いまわし）利用は3回変更以降とする

また，最も持ち出す可能性の高いモバイルPCには，情報漏洩対策ソフトとして，ディスクを丸ごと暗号化する製品「Pointsec（NEC製）」を導入した。万一PCを盗まれたり，ディスクを抜き取られても簡単には内容を解読できないしくみとなっている。

これらの施策は，規制を意図したものではなく，あくまでスタッフのセキュリティリテラシー向上が目的である。PC配布当初はやや混乱を招いたが，事務長会議での了承を得てようやく運用に至った。

・各種サーバのセキュリティ

サーバにおいては，数年前まで地区毎に分散していたホームページ用サーバを1台に集約し，セキュリティにかかるリスクと手間両面の削減を図った。メールサーバについては，ウイルスチェックやスパムチェックツールを導入してウイルス・ワーム感染を未然に防ぐことに成功した。また，SolarisやWindowsなど脆弱性の高いOSを利用するサーバは，できるだけFreeBSDやSE Linuxといった，よりセキュアなOSへ移行し，どうしても残す必要のある場合でもグローバルネットワーク上に直置きせずに，VPN内もしくはリバースプロキシ内へ置くようにしている。なお，サーバの運転監視を行うための専用機器（ぷらっとホーム「監視Blocks」）を導入して，管理対象のサーバに何等かの異変があると，システム管理者の携帯電話にメールが入ることになっており，トラブルの早期発見に努めている。

4．個人情報保護法への対応

2005年4月より，個人情報保護法が施行された。これに先立って慶應義塾全体の指針をまとめるための「個人情報保護ガイドライン委員会」が発足し，メディアセンターからも実務責任者が2名参加し

た。また，メディアセンター内でも検討委員会（以下，個人情報保護 WG)を設置し，各地区より代表者を集め集中的に検討を重ねた。しかし，図書館システムそのものに関する現状と対策については，本部システム担当に一任されたため，システムにおける個人情報の取り扱いの現状と対策案をまとめて，個人情報保護 WG へ提出することとなった。

図書館システムで取り扱う個人情報には，利用者情報を始めとして，貸出・予約・延滞などの利用記録，学内名簿・学会名簿の目録データ，スタッフのメール BOX などがある。個人情報の利用にあたっては，利用目的と許諾，入手方法，利用後のデータの返却・廃棄といった一連の流れに沿って運用基準を取り決める必要がある。特に，利用者情報については，学事センターや人事部など他部署から提供を受けるものについては,「情報のもらい過ぎ」がないように注意している。データの受け渡しについても，できるだけローカル保存は避け，FD などの媒体は利用後に直ちに返却することにしている。

利用者情報の入手経路は，実に様々で，KOSMOS II以外のサービスやシステムでは個々に利用申請書（紙）やオンラインリクエストフォームに記入させている。これらについても，利用者に対して目的を明示し,同意を得るしくみが必要となる。

また，貸出記録などは，利用者本人の思想や宗教観を類推させるものでもあり，刑事事件などが起きた場合，手がかりとして警察などから提出を要請されるケースも想定される。そのようなケースに備えて，図書館としては，利用記録の有無だけでなく，保存年限や廃棄基準などのポリシーを明確にしておく必要がある。

5．セキュリティポリシーの策定のポイント

本部システム担当では，個人情報保護対策を契機として，それまであまり本腰を入れられなかったセキュリティポリシーについて検討する機会を得た。そこで，個人情報保護を中心として「図書館システムに関わる全体のガイドラインと対策ポイント」と「業務用 PC 利用に際しての注意事項」を策定することにした。現在，図書館システムに関わる全体のガイドラインを以下の 17 項目を切り口としてまとめている最中である。

（1）ソフトウェア・ハードウェアの購入・導入
（2）サーバルーム
（3）ネットワーク構築
（4）LAN におけるマシン設置，変更，撤去
（5）サーバ等におけるセキュリティ対策
（6）クライアントにおけるセキュリティ対策
（7）ユーザ認証
（8）ウイルス対策
（9）E メール利用
（10）ウェブ利用
（11）媒体取扱い
（12）アカウント管理
（13）システム維持（パッチ適応）
（14）システム監視
（15）セキュリティインシデント
（16）セキュリティ情報収集および配信
（17）外部公開サーバ

次に，業務用 PC 利用に際しての注意事項については,「①個人情報保護と直接関連するもの」,「②個人情報保護と間接的にかかわるもの」,「③その他(一般的なネチケット，セキュリティ対策など)」の 3 つに分けてまとめることとした。①は「情報の持ち出しについて」と「情報の持ち込みについて」，②は「ソフトウエアのインストールについて」,「パスワードについて」,「ウイルス対策ソフトについて」,「WindowsUpdate について」，③は「ネチケットなど」に分けて記述した。

セキュリティ対策のポイントは，外部の脅威に対する対策と内部の脅威に対する対策の棲み分けである。外部の脅威に対しては，アクセス制御で対抗することができるが，内部の脅威に対しては，抑止策で対抗するしかない。つまり，内部の脅威に立ち向かうには現場での意識改革が必須となる。

6．認証とアクセス制御

現在提供中のサービスを含め，次世代図書館サービスを考える上でもっとも重要なセキュリティ基盤となるのが，認証とアクセス制御である。

ここ数年，図書館サービスのパーソナライズの動きが加速している。図書館システムベンダーやデータベースベンダーが提供する「マイ・ポータル」「マイ・ページ」「マイ・ライブラリ」など様々な呼び名はあるが，すべて自分用にサービスメニューをカスタマイズするための機能である。つまり，図書館が

用意したホームページやEJ/DBリストをそのまま利用するのではなく,自分がよく利用するサービス,もしくは出版社・著者・タイトルのみに絞って表示したり自由に取捨選択ができる機能である。また,キーワードを登録しておくと自動的に新着情報がメールで送付されるSDI機能もある。

いずれにせよ,これらのサービスを提供するには,本人による認証行為が必要で,本人の所属や身分などの属性情報に従って,ナビゲートするサービスの範囲を決めたり(アクセス制御),「誰が・いつ・どこに・どのくらい」アクセスしてきたかといったログ記録機能が必須となる。EJ/DBサービスの契約においても,特にリモートアクセスについては「契約する図書館が認証したVPNやプロキシ経由のアクセスに限り利用を許可する」としている出版社やプロバイダーも多い。そこで,慶應義塾共通のID(統合ID)を利用した認証システム(以下,keio.jp)と連携したサービスの開発が急がれている。現在,keio.jpは職員向けにIDが配布されているが,利用できるサービスは「共通メール」のみである。図書館では,「貸出・予約・未収金状況照会」を皮切りに,「EJ/DBリモートアクセス」についてもkeio.jpと連携を行う予定である。

7. おわりに

システム担当者が,いかに壮大なセキュリティポリシーやガイドラインを策定し,ISMSやプライバシーマークなどの第三者による評価認定を得たとしても,それ自体に満足し,スタッフ全員に浸透しなければ意味がない。また,書かれている内容が古くても効果が薄れてしまう。毎日スタッフが大量のメールを送受信し,多数のWebサイトを閲覧して仕事をしている。また,ウイルスやワームも分進秒歩で増殖しており,待ってはくれない。人間もウイルスもいわば「生もの」なのである。

結局は,わかりやすいポリシー(ガイドライン)作りと継続的な見直し,および絶え間ない啓蒙活動が必要なのである。そのためには,まず機械的に防御できるものと,現場で教育しないといけないものを分けて対応する必要がある。セキュリティを強固にしようとすればするほど,費用もかかり,運用も窮屈になる。どこまで実施すればよいか,組織のリスクヘッジをどこに置くか,はトップの判断となる。つまり,トップの早期理解と意思決定がセキュリティ対策への第一ステップとなる。

私たちシステム担当者は,積極的にトップに働きかけ,現場スタッフにもわかりやすいようなガイドラインを策定することが急務である。但し,それは一方的な「通達」のようなものではなく,オンライン掲示版やQ&A集を用意して,いつでも気軽に意見交換ができるようなしくみでなくてはならない。

ポリシー1つとっても,いきなり完璧なものなどできはしない。また,メディアセンターだけの思いだけで突き進む訳にもいかない。慶應義塾全体のIT関連ポリシーの策定を行っているITCと調整をとりながら進めて行きたい。但し,ここでもポリシーの一方的な押し付けではなく,相互のコミュニケーションに基づく運用が望ましい。例えば,メディアセンターで具体的に試行運用している対策をITCへフィードバックするのもよいだろう。いずれにせよ,まずはできるところから草の根的に対応していきたいと思っている。それが,全塾共通の「アンブレラ」的なポリシーとなって還元されれば幸いである。

参考文献

1) インターネット白書2005. 財団法人インターネット協会監修. インプレスネットビジネス, 2005.
2) すっきりわかった!セキュリティ. ネットワークマガジン編集部編. アスキー, 2005
3) ネットワークセキュリティexpert. Software Design特別編集部. 技術評論社, 2005.
4) 個人情報保護法対策セキュリティ実践マニュアル2005年度版. 日本ネットワークセキュリティ協会個人情報保護ガイドライン作成ワーキンググループ編. インプレスネットビジネス, 2005.
5) やさしく読む「個人情報保護法」.(オンライン), 入手先<http://www.atmarkit.co.jp/fsecurity/rensai/privacy01/privacy01.html>,(参照2005-07-22).
6) 実践!情報セキュリティポリシー運用.(オンライン), 入手先<http://www.atmarkit.co.jp/fsecurity/rensai/policy11/policy01.html>,(参照2005-07-22).