セキュリティガイドラインについて

宮 尾　　克　　長谷川　明生

名古屋大学のセキュリティポリシーは，本学の情報セキュリティに対する基本的姿勢を示すものとして，平成14年３月に評議会決定されました。このポリシーの精神を具体化し，学内のIT資源の安全な利用を図るための指針として，ガイドラインの策定が急がれていました。情報連携基盤センターが取りまとめ役になって，学内の10数名のメンバーがワーキンググループを構成し，策定作業が続けられていましたが，約１年の作業を経て，セキュリティガイドラインとして本年５月27日の評議会で承認されました。このガイドラインは，以下のURLでアクセスできます。ぜひ，ご覧になってください。

http://www2.itc.nagoya-u.ac.jp/security-policy/guideline/index.html

今回策定されたセキュリティガイドラインは，大学の公式文書としては初のオンラインWeb文書として公開することを目標に作業をしてきました。その理由は，この文書が，非常に変化の激しい分野を対象としているからです。そのため，ガイドラインは，セキュリティ確保のための概念や基本的事項を記述した本文と，変化が激しいと想定される技術指針やインシデント事例を提供する注意事例情報の両面からなっています。このように本文以外の技術的な説明を加えることにより，本文の改訂頻度を少なくし，緊急対応が必要な部分は事例集で対応することができるようになりました。また，公開されているWeb版は，リンクにより容易に必要な箇所を参照できるようになっています。

本学のセキュリティポリシーは，利用者の最大限のアクセス可能性を保証し，セキュリティ対策の自己責任を強調していますが，セキュリティガイドラインは，そのセキュリティポリシーの基本方針を具体化したもので，４部構成となっており，以下の図のとおりです。

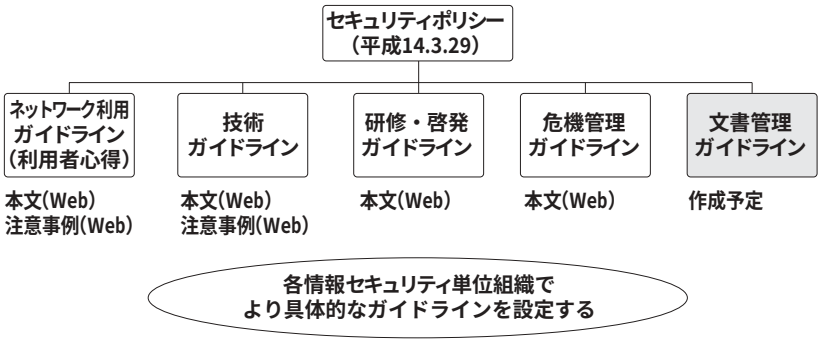

図１　情報セキュリティガイドラインの構造

このガイドラインには，大学の一員として情報機器や情報に日々接する上で理解しておくべき基本的事柄がまとめられています。さらに部局ごとに，個別事情を反映した固有のセキュリティガイドラインの策定が必要とされています。たとえば附属病院のネットワークや情報機器については，プライバシーや守秘義務に高度に配慮しなければならないので，より厳格なガイドラインが必要でしょう。

これからは学生，職員を問わず，本学の情報機器利用におけるアクセス用IDが発行される前に，研修・啓発ガイドラインに基づく教育体制によるセキュリティガイドラインの理解が求められます。そうしてこそ，セキュリティ事故の未然防止や被害の拡大防止につながり，ひいては，個々の利用者や大学の利益につながります。すべての大学構成員が，セキュリティポリシーとガイドラインを熟読されんことが期待されます。

セキュリティ確保の効果が現実にあがるようなガイドラインを作るために，利用者や管理者が最低限守るべき事柄を簡潔にまとめ，むずかしい用語をなるべく使わないようにしました。用語集や参考資料も提示されています。ここでいう管理者とは，大規模サーバの管理者のみならず，ネットに接続されたパソコンの所有者も含んでいることに注意が必要です。

ネットワーク利用ガイドライン（利用者心得）の部分では，「禁止事項」と「許可事項」の間のグレーゾーンが広くあります。そのような場合には，利用者の良識的判断に任せるようにして，余計な制限をしないようにしてあります。

今回のセキュリティガイドラインは，まだ不十分であり，今後，デジタル時代にマッチした文書管理規程（ガイドライン）の策定や，文書管理におけるプライバシー保護に対するガイドラインも必要です。

昨年のセキュリティポリシーと今回のセキュリティガイドラインを，全員で守ってこそ，情報アクセスの自由を確保することができます。これら２本柱は，セキュリティ維持活動を大学が立案するための出発点といえるものです。これら２本柱の策定を受けて，情報セキュリティを専門にあつかう「情報セキュリティ対策室」の設置が，総長の下で進んでいます。セキュリティ事故やウィルス感染等の緊急対応を行うための「情報セキュリティホットライン」の整備も準備されています。こうして，セキュリティポリシーやガイドラインに依拠し，また，大胆に見直し，本学の情報セキュリティの確保を一層推進する所存です。

（みやお　まさる：名古屋大学情報連携基盤センター情報基盤ネットワーク研究部門）
（はせがわ　あきうみ：名古屋大学情報連携基盤センター大規模計算支援環境研究部門）