情報セキュリティ ポリシー・サンプル（0.92版） 解説書

オンライン　第一版 (2003年7月2日)

本書の著作権は、執筆担当者の各人に帰属します。
本書の文章の全部あるいは一部の複製や転載、引用等、およびファイルの再配布については、ＪＮＳＡ事務局を通じて、各執筆担当者から事前の了解を得ていただく必要があります。
事前の了解を得ずに、それらの行為をすると違法となる場合がありますので、取り扱いにご注意下さい。
文章の引用などをせずに、本書を参考文献として紹介するだけの場合は、この限りではありません。その場合には、ＪＮＳＡのホームページからのファイルのダウンロードを指示するようにお願いします。
ダウンロードページは、http://www.jnsa.org/policy/guidance/ です。

JNSA
NPO日本ネットワークセキュリティ協会
Japan Network Security Association
http://www.jnsa.org/

C O N T E N T S
目　次

すべての基本となる「ポリシー（方針書）」部分を作る

セキュリティ対策の「スタンダード（標準書）」を作る

監修　日本ネットワークセキュリティ協会　佐藤慶浩

・本書のうち上記の執筆担当者の執筆部分の著作権は、それぞれ各人に帰属します。それらの使用権と版権については、NPO日本ネットワークセキュリティ協会が、著作者と共有しています。
・それ以外の部分の著作権は、NPO日本ネットワークセキュリティ協会に帰属します。
・本書に掲載した会社名、アプリケーション名および製品名などは一般に各社の登録商標または商標です。

I N T R O D U C T I O N
はじめに

この解説書では、JNSAのポリシーWG（ワーキンググループ）が作成したポリシー・サンプル（0.92版）を参考にしながら、皆様の組織に適した情報セキュリティポリシーを作成する際の助言や注意事項について解説しています。

この解説書は、ソフトバンク パブリッシングの月刊誌である「N+I NETWORK Guide」の2002年6月号から翌1月号までの全8回の連載記事をまとめて一冊にしたものです。記事の執筆は、JNSAのポリシーWGの有志メンバーが担当しました。執筆にあたっては、執筆以外の有志メンバーも加えた会合にて、助言や注意事項についての意見を出し合いました。これを執筆担当メンバーが、自分の意見に加えて、それぞれ解説文にしたものです。

この冊子で解説しているポリシー・サンプルの本文は、各回の記事の指示に従って、JNSAのWebからダウンロードして適宜参照してください。

全8回のうち、第1回は基本ポリシーについての解説です。第2回でそれ以降のスタンダード構成についての解説をしています。全体構成を知るためには、第2回をまずお読みください。第3回から第8回までのスタンダードの解説については、必ずしも順番に読む必要はなく、興味のある部分から読んでいただくこともできます。

この解説を参考に、皆様の組織での情報セキュリティ対策の立案や文書作成にお役立てください。また、WGでの活動に興味を持たれた方は、是非、JNSAの会員となっていただき、一緒に勉強できますことを楽しみにしています。

末筆ですが、各回の執筆者の方々（目次に列記）以外では、有限会社インターネット応用技術研究所の大村祥子氏、セコム山陰株式会社の平本耕造氏、日本電気エンジニアリング株式会社の茂出木孝人氏も会合に加わり執筆者の方々と共に活発な意見をいただき、無事に解説書を作成することができたことに感謝します。また、ソフトバンク パブリッシングの友保健太氏には、丁寧な校正をしていただき、わかりやすい文章の作成を行なうことができました。この場を借りてお礼申し上げます。

監修

NPO 日本ネットワークセキュリティ協会　理事
日本ヒューレット・パッカード株式会社

佐藤　慶浩

JNSAでは、動画によるCD付き冊子として『仕事でパソコンを使う人のためのセキュリティ対策講座：ネットワーク社会のここが危ない！！』を配布しています。詳細は、JNSAのホームページ（http://www.jnsa.org/cdrom/policy.html）を参照してください。

セキュリティ対策講座①
サンプルを見ながら策定する
ドンと来い！ 情報セキュリティポリシー

第 1 回（全8回）

すべての基本となる「ポリシー（方針書）」部分を作る

あらゆる企業や組織において、情報セキュリティポリシーの制定が必要だといわれて久しい。それに伴い、作成のためのノウハウ本も出ている。しかし、ポリシー作成の概念が示されるにとどまり、実際のポリシー本文を例示したものはまだ少ない。この連載では、JNSA（日本ネットワークセキュリティ協会）のセキュリティポリシー作成ワーキング・グループが公開しているポリシー・サンプルを用いて、ポリシーの考え方と作り方を解説する。

著者：NPO 日本ネットワークセキュリティ協会 理事 佐藤慶浩
ポリシー階層の解説……株式会社ラック 足利俊樹／日本ヒューレット・パッカード株式会社 永沼美保

JNSAの紹介

JNSAは2000年4月に設立され、2001年7月にNPO法人として活動を継承しました。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を、現在13のWG（ワーキンググループ）に分かれて行っています。

昨年度の主な成果物としては、「外部接続に関するセキュリティポリシーサンプル冊子」の作成、「セキュリティインシデント被害調査」におけるアンケートの実施および報告書の作成などが挙げられます。

また、複数CAの相互運用性に関する実証実験を行った「Challenge PKI 2001プロジェクト」の結果報告も、近日中にWebにて公開の予定です。その他の活動として、年1回の主催カンファレンスの開催（NSF2002、今年は6月12-13日）、毎月のセキュリティセミナーの開催、会報誌「JNSA Press」の発行（年3回）などを行っています。

＜お問い合わせ＞
特定非営利活動法人 日本ネットワークセキュリティ協会
URL：http://www.jnsa.org/
E-Mail：sec@jnsa.org

ポリシー・サンプルのダウンロード

まずは、JNSAのポリシー・サンプルの全文を、以下のWebからダウンロードしよう。

http://www.jnsa.org/policy/guidance

これを印刷して本書の横に並べて読んでいただくとよい。本講座では、その一部を解説の必要に応じてJNSAの承諾を得て転載している。引用部分は以下のような囲み表示をしてある。

> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

このようなサンプル引用に解説を加えていくことで、自社に適したポリシーを策定するための手助けを行っていく。

情報セキュリティポリシーの捉え方

情報セキュリティポリシーとは、企業や組織（以下、単に組織という）にとっての情報セキュリティに関する方針である。JNSAのポリシー・サンプルの内容は、もちろん間違ったものではないが、読者自身の組織のポリシーとしてそのまま使うべきものではない。それはなぜだろうか？ その理由を考えるときには、経営方針にたとえて考えるとよい。経営方針を定めるのに、別の会社や世の中の一般的な方針をそのまま使ったらどうだろうか？ たとえば「お客様のことを第一に考える」とか、「従業員にとっても幸せとなるべく仕事をする」などである。これは間違ったものではない。しかし、この場合、「お客様を第一に考える」は一般的に正しいが、「なぜ？」なのかが説明できなければならないし、「では、お客様にとってよければ会社の利益はなくてもよいということなのか？」などの問いにも答えられなければならない。そうでなければ、それは、自分たちの方針ではなく、ただの借り物の文章でしかないということになる。つまり、自分の組織に合ったものとは言いがたい。

だが、サンプルをたたき台として使うという手法は考えられる。ただし、サンプルがあるといっても、白紙から書き始めたのと同じ気持ちで、その内容が自分の組織に合ったものか、一文字一文字を慎重に審議することが必要である。一見あたりまえに思える文書に、「それは、なぜか？」という問いかけを徹底的に行うのである。

審議した結果、結局たたき台と同じということはあるかもしれない。しかし、「なぜ？」の議論が十分行われた場合と、行われていない場合では、その文章が組織で果たす役割は異なってくるはずである。

情報セキュリティポリシーとは、このような位置付けのものだと考えるとよい。だから、情報セキュリティ規則ではなく、ポ

リシー（方針）なのだ。

つきつめた審議を行った結果としてうまく運用されている情報セキュリティポリシーと一般的なポリシーとの間には、表面上の文章としての差異が希少であることも多い。そのため、一般的なものをベスト・プラクティスとして単純に引用すればよいのではないかと思われがちである。しかし、それはポリシー作成の際の大きな落とし穴なのである。

この種の誤解を避けるため、ポリシーの解説文には、あまり具体的な本文を示さず、概念的な説明にとどめる場合が多いのかもしれない。とはいっても、文章としてのイメージが分からないと、初めてポリシーを白紙から作成する人にとっては、その作業は困難であると思う。そこで本講座では、JNSAのポリシー・サンプルを例に出して、イメージをつかんでいただきながら、かつ、それをそのまま使うのではなく、どんなところを気にしながら文章を自分の組織に合ったものとしていくのかを解説できたらと思う。執筆には、ポリシー・サンプルを作成したワーキング・グループのメンバーの方々に協力していただく予定である。

JNSAポリシー・サンプルの役立て方

JNSAのポリシー・サンプルの構造は、図1のようなものである。全体を示すポリシーの中に、ポリシー（方針書）とスタンダード（標準書）という階層を持っている。「ポリシー」という言葉を、全体と基本ポリシーの2カ所で再帰的に使う点が少し分かりづらいかもしれない。この下にプロシージャ（手順書）を構成して、「情報セキュリティポリシー関連文書」などと呼ぶ。ただし、この構造そのものも例であることに留意していただきたい。実際には、違う構造や違う文章名にしてもよい。

ポリシー階層とスタンダード階層の境界の定義についての一般論は1つではない。例としては、スタンダードは少なくとも計測可能なものとする。すなわち、監査の対象とする。ポリシーは、必ずしも計測可能な内容でなくてもよいが、なるべく長期にわたって不変な内容とする。すなわち、精神論的なことが書いてあってもよいが、新しい技術とともに頻繁に変えないものとすることが考えられる。

情報セキュリティポリシーを作成する人たちにとって、最初に検討すべき「なぜ？」は、この構造をどうするかである。もしも、どこかの構造を単にまねたのであれば、既にその時点でポリシーに、「なぜ？」の問いかけが1つ足りないのである。

また、ポリシー作成にあたっての「原則」も明文化されず、文章の裏に潜んでいる場合が多い。

ときどき、欧米は情報セキュリティを性悪説で考えているのに、日本は性善説だからよくないという意見があるが、それらを二者択一的にとらえているなら正確な表現ではない。情報セキュリティの問題は、まず性善説での施策を行い、次に、それに加えて性悪説の対策を必要とするのである。ポリシーは、最初の性善説の出発点である。ポリシーを性悪説だけで作るのはナンセンスである。性悪者にとってポリシーは意味をなさない。彼らはポリシーに従おうと思っていない、というより、読むつもりもないのだから。ポリシーを理解し遵守する性善者の存在が前提である。遵守する彼らに、性悪説に基づく対策を担ってもらうという枠組みを構築することが必要である。

もし、組織の全員を性悪説だけで考えるとしたら、その組織は、情報セキュリティ以前に、組織としての存在が成り立たないであろう。

ここで、「性善説であれば、組織員を信頼してすべてを任せていられる」というのは誤りである。「何が善なのか、善と悪との判断基準は何なのか」について示す必要がある。それがポリシーである。このことの認識が日本では不足しているかもしれない。その足場固めをしっかりしたら、その上に、性悪説に基づく対策を構築すると、堅牢な情報セキュリティポリシーの運用が可能になる。

以上のようなことを「原則」たる作成心得として意識合わせしてからポリシーを作成するとよい。ただし、ここで示した原則も例である。この点についても検討することで、情報セキュリティの何たるかが、皆様の組織で活発に議論されることを望んでいる。

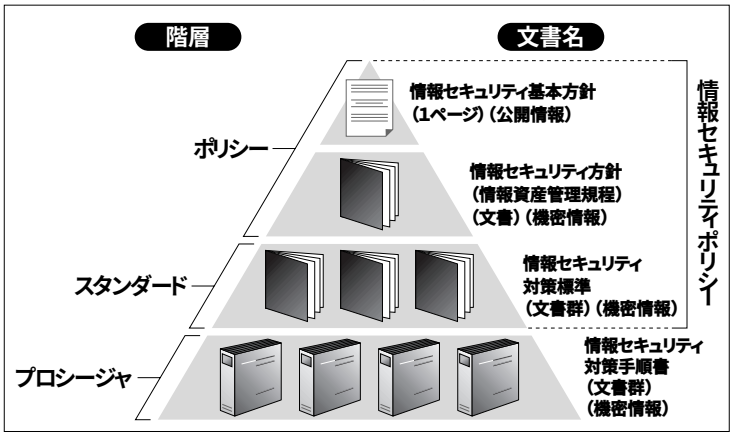
連載が進むにつれ、情報セキュリティポリシーの作成なんて「ドンと来い！」、と読者の皆様が自信を付けてもらえるように執筆者一同がんばりたいと思う。

個別の返答は必ずしもお約束できないが、連載内容に反映していきたいと考えているので、ご意見・ご感想等を電子メールにてぜひお寄せいただきたい。

E-Mail　SECURITY-POLICY@yosihiro.com

（佐藤）

図1■情報セキュリティポリシー関連文書群の全体構成



ポリシー・サンプルの作成にあたって

JNSAのワーキング・グループでは、作成したポリシー・サンプルを公開しているが、サンプルを作成しようというそもそもの目的は、“さまざまなシステムに汎用的に適用でき、かつ日本に適応する情報セキュリテ

ィポリシーの姿を示す”ことにあった。

その背景には、日本の現状におけるセキュリティ対策の問題点に対するメンバーの疑問があった。最近のセキュリティ対策においては、技術的な対策と人的な対策との融合を図っていくことが重要であるとの認識がされている。そして、その融合の実施のためには、情報セキュリティポリシーを策定し、セキュリティを管理する体制を作り、組織全体でセキュリティを管理していくことが必要であると盛んに説かれている。しかし、実際には、最初のステップである情報セキュリティポリシーが一般的にどの組織にも存在しているかというと、必ずしもそうとはいえない。

では、それはなぜだろうか。日本におけるセキュリティの管理に対する考え方や欧米との文化的な相違等、情報セキュリティポリシーの浸透を阻害している理由は今までも幾つか指摘されている。しかし、大きな比重を占める理由の1つとして、日本の風土、文化に適応した情報セキュリティポリシーのあるべき姿がどのようなものであるのか、その点が把握しきれていない、あるいは、そもそも、ポリシーとはどのようなものか、そのイメージがわかない、ということが挙げられるのではないだろうか。

このような背景があるからこそ、さまざまなシステムに汎用的に適用できるだけでなく、風土にも適応するポリシー・サンプルを策定することの意義は大きいと考えた。

ただし、ポリシー・サンプルを公開するにあたっては「功」の部分だけではなく、「罪」の部分も考えなければならない。「罪」としては、やはり自組織の情報セキュリティポリシーを安易に考え、このポリシー・サンプルをそのまま流用しようとするユーザーもいるのではないかという懸念である。この懸念は容易に考えられる点ではあるが、この「罪」の部分をもって公開しないという結論には至らなかった。それだけ、「功」の部分に重きを置いた公開であることをご理解いただきたい。

ポリシー・サンプルの構造

ポリシー・サンプルにおいては、ポリシー／スタンダード／プロシージャの3階層の構造を前提に、それぞれの定義を以下のように定めた。

●ポリシー

「情報セキュリティ基本方針」

組織の情報資産を適切に保護・管理することを経営者が意思表明したもの。

「情報セキュリティ方針」

組織全体に対する情報セキュリティの方針を示すもの。

●スタンダード：「xx標準」

情報セキュリティ方針に従い、必要な対策を分野別に規定したもの。

●プロシージャ

定められた対策を現場で運用するために、より詳細・具体的に規定したもの。

「ポリシー」部分策定時の考え方

第1回では、ポリシー部分（図1参照）の策定に焦点を当てていきたい。この部分は定義にもあるように、経営者の意思表明と組織全体に向けての情報セキュリティの方針という重要なテーマを扱っている。情報セキュリティポリシーは、組織の情報セキュリティへの取り組みについての方針を明文化したものであるため、その意思表明は、組織外と組織内両方に向けて行われるべきである。そのため、経営者の意思表明を「情報セキュリティ基本方針」として組織の内外を問わず公開文書として作成し、組織内向けの方針は「情報セキュリティ方針」とした。

情報セキュリティ基本方針の作成

情報セキュリティ基本方針は、その組織が情報セキュリティをどうとらえているか、情報セキュリティ維持への取り組みをどのように行っていくかを宣言する公開文書である。また、情報セキュリティ維持を情報セキュリティマネジメントとして、経営課題の一環として取り組む（あるいは取り組んでいる）ことを表明するという文書でもある。

そのため、文章は、分かりやすく、インパクトのあるものが望ましい。そう考えると、基本方針の作成にあたっての最大のポイントは、「強調すべきことを、簡潔に」まとめることにある。しかし、多くの方が感じているように、簡潔にまとめようとすればするほど、文章を作成するのが難しく感じることが多い。さらに、この文書には、定型文というのは存在し得ない。それぞれの組織の特徴や考え方が顕著に反映されるため、ここで書かれる文章や体裁は、それぞれの組織によって異なるはずである。

サンプルの作成にあたっては、 まずは、汎用性の高いものを目指すということを考慮し、以下の観点を含めた文章を作成した。

●ネットワークコンピュータ活用の支援、同時にセキュリティを意識した利用の促進

●情報資産の重要性の強調（「第4の資産」）

●情報セキュリティポリシー策定の宣言

●情報セキュリティポリシーの遵守義務の強調

これらのポイントは、どの組織においても、情報セキュリティを考える際の根本的なものであるはずである。基本方針作成の際のヒントとしていただきたい。また、文章表現や体裁については、たとえば、既存の規程等に既に基本方針のような宣言文がある場合には、そちらに合わせてもよいだろう。

基本方針については、分量がある必要はないと考えている。むしろ、なぜ情報セキュリティを意識することが大切なのか、なぜ情報セキュリティポリシーを定めたのか、なぜそれに従わなければならないのかといったポイントを明確にした文章のほ

うが、読み手にとってはより分かりやすいものになる。具体的には、A4判1枚に収まるもので十分である。　（永沼）

情報セキュリティ方針の作成

ポリシー・サンプルは、すべてで14章から構成されている。この構成は、組織に新たなルールを追加する上で考えなければならない・決めなければならない点が含まれている。

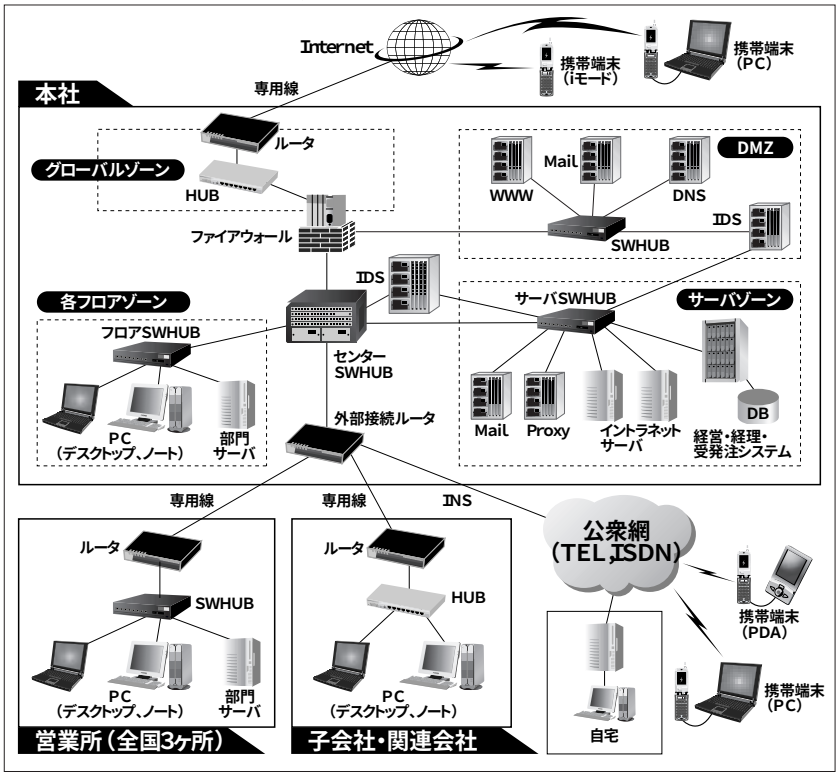
本稿では、情報セキュリティ方針の策定にあたり、ポイントとなる点に絞って説明していきたい。

検討課題1　情報セキュリティポリシーの適用範囲（ポリシー・サンプル　第2章を参照）

『情報セキュリティポリシー』の適用範囲は、当社の情報資産に関連する人的・物理的・環境的リソースも含むものとする。
当社の保有するシステムの具体例は、図2で示している範囲とする。

ポリシー・サンプルでは、適用範囲を図2のように規定し、ネットワーク構成図を用いて明確化している。情報セキュリティは、守るべき対象があってこそ対策を検討することになる。サンプルでは、守るべき対象を組織のネットワークを中心に考え、それに付随するものを含めて対象とすることにした。これは、1つの適用範囲の決め方であってこれがすべてではない。たとえば、建屋に視点を置いた適用範囲の決め方や組織が提供する業務内容（サービス）に視点を置いた考え方などがほかに存在する。当然のことながら複数の視点から適用範囲を考えてもよいだろう。重要なのは、守るべきものは何なのかという点を明確にすることと、理想論に終わらずに十分に対策が可能な範囲なのかどうかを検討することにある。

図2■株式会社○×販売・システム構成図



検討課題2　情報セキュリティポリシーの対象者（ポリシー・サンプル　第3章を参照）

本『情報セキュリティポリシー』の適用者は、経営陣、従業員を含めた、当社の情報資産を利用するすべての者である。

サンプルでは、上記のルールを規定している。この適用者の考え方は、情報セキュリティポリシーならではの考え方である。他の就業規則と一線を画する情報セキュリティポリシーのよい例であろう。通常の就業規則は、その対象者（想定読者）を正社員として規定している。そのため、たとえアルバイトや派遣社員が業務に従事していたとしても、すべての社内規則を開示する必要はない。しかし、情報セキュリティポリシーでは、適用範囲内で業務を行うすべての者を対象としなければならないため、正社員以外の者にもその規定を遵守させる方策を検討しなければならなくなる。また、これはスタンダードの範疇ではあるが、正社員以外の者に対する契約時のルールを「第三者契約に関する標準」等で規定する必要も出てくるのである。

サンプルのこの章では、それぞれの対象者に対して情報セキュリティポリシーの遵守義務を明確化している。このような当然といえば当然の事項を明記することで、無形で伝承されているルールを有形化する役割も、情報セキュリティポリシーでは担っているのである。

検討課題3　情報セキュリティポリシーの構成と位置付け（ポリシー・サンプル　第4章を参照）

ここで検討すべき事項は、①既存の規定と情報セキュリティポリシーの関係について、②情報セキュリティポリシーの3階層における役割分担の明確化、③関連規格・法令との位置付けである。

情報セキュリティポリシーを3階層の文書として構成することは、既に述べた。

しかし、新たなルールを組織に追加するには、情報セキュリティポリシーだけのことを考えるのでは不十分で、そのほかに既存の規定との関係をどのように位置付けるかが重要なポイントになる。

既存の規定として思い当たるものとしては、就業規則、文書管理規定、営業情報管理規定などが代表的である。その他にも、情報セキュリティポリシーとして体系立てられていない時点で策定されたウイルス対策規定などもあるかもしれない。既存規定も

含めて、規定の統廃合を行うことも必要になるであろう。

サンプルでは、情報セキュリティ方針を就業規則と同等の規則と位置付けているが、これも一例である。そのほかに考えられることとしては、就業規則の一条項に情報セキュリティポリシーの遵守を社員に義務付けるように改定し、情報セキュリティポリシーは既存の規定とは別枠の規定とすることも検討できる。

検討するときのポイントは、組織それぞれの風土において、どのようにすれば情報セキュリティポリシーが遵守しやすいかという点である。“遵守しやすいか”には、さまざまな意味があるが、情報セキュリティポリシーの運用のしやすさや、対象者が分かりやすいかなどの点が挙げられる。

この点は、常に情報セキュリティポリシーの運用を念頭において、検討しなければならない。その意味では、この検討をおろそかにしてしまうと、運用もままならなくなってしまうといえるであろう。

関連規格や法令に関しては、サンプルでも例を挙げているのでそちらを参考にしてほしい。

検討課題 4　情報セキュリティとは何なのか（ポリシー・サンプル第7章を参照）

情報セキュリティ対策を進めていく上で、各組織が情報セキュリティを適切に認識しなければ、先へは進めないであろう。まずは言葉の定義をして認識の統一を図らなければならない。代表的な情報セキュリティの定義としては、「機密性・完全性（保全性）・可用性」である。この定義の起源は、OECD 情報セキュリティに関するガイドラインにある。最近では、日本国内でも知名度が増しているISO/IEC17799においても、その定義を利用していることもあり、情報セキュリティの定義は、「機密性・完全性（保全性）・可用性」が一般化している。サンプルでも、この流れに準じISO/IEC17799の規定を利用している。

検討課題 5　情報セキュリティの推進体制はどうあるべきか（ポリシー・サンプル　第8章、第9章、第10章を参照）

> 当社の情報セキュリティを維持していくために、情報セキュリティ委員会を設け、全社的なマネジメント体制を整えるものとする。情報セキュリティ委員会の詳細情報に関しては、情報セキュリティ委員会構成メンバーを参照のこと。

サンプルでは、推進体制として情報セキュリティ委員会を創設することを念頭において策定されている。組織によっては、情報セキュリティ推進室、リスク管理室などといわれる体制を設けて、組織の抱えるリスクに対応する場合もある。

情報セキュリティを推進していく人間像として、①組織横断的な人脈のある人、②決算権のある人が望ましいなどといわれている。これは、理想論としてはそのとおりであるが、現実からすると、このような特定の人物を選出することは難しいであろう。その代わりに委員会を新設するのであれば、その委員会の役割や構成員に対する権限を明確に規定することで、行動しやすい土壌を準備することも検討しなければならない。どのような仕事でも人に依存してしまうのは、仕方のない部分であると思われるが、できる限りの対策は打っておきたい。

当然のことながら、セキュリティ対策を推進していく上では、委員会の新設だけではなく、その委員会を補助する体制についても検討しなければならない。サンプルでは、委員会を補助する目的で情報システム部を委員会に組み込んでいる。情報セキュリティ対策は、組織のIT機器における対策が多くを占めるので情報システム部を規定しているが、その他の部門としては、総務部門なども体制に組み込む必要があるかもしれない。総務部門は、既存規定の管理を行っているし、建屋に関する物理的な対策を以前から行っている場合が多い。その意味では、情報システム部門だけでは不十分で、総務部門の参画も検討してよいであろう。

サンプルでは人に対する権限として、情報システム部内のシステムセキュリティ責任者、システム管理者、オペレーターの新設を検討している。既存の組織でも、通常の業務を遂行するためにシステム管理者などが存在していると思われるが、セキュリティ対策を意識した人の役割も明確化するべきである。このように明確化することで、兼務による甘えを極力排除することも検討したい。

検討課題 6　情報セキュリティマネジメントの推進はどうあるべきか（ポリシー・サンプル　第11章を参照）

情報セキュリティ対策も他のマネジメントと同様にPlan→Do→Check→Actionのサイクルで管理していくものである。サンプルでは、6つの事項からこのサイクルを回すことを念頭に置いている。

Planに当たるのは、①リスク分析、②ポリシー策定である。

Doに当たるのは、③対策の実施、④教育・啓発である。

Checkに当たるのは、⑤監査・評価である。

Actionに当たるのは、⑥文書の改廃（ルールの改定）である。（図3参照）

①リスク分析

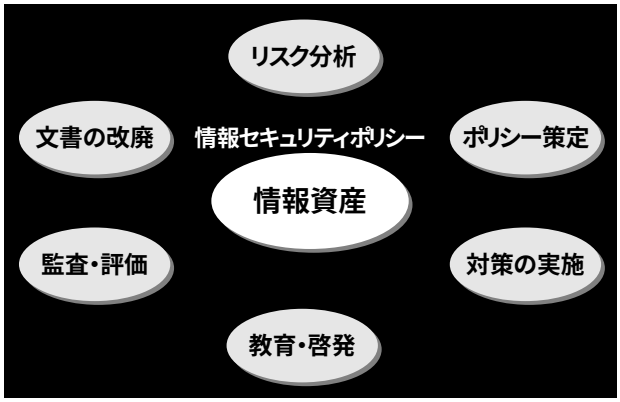
> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

サンプルでは、リスク分析を上記のように規定している。ポリシー文書ということもあり、ここでは詳細な方法論までは規定していないが、どのようにしてリスク分析を行うかはこの時点で検討したい。

適用範囲内にどのような資産が存在し、その資産にはどのような脆弱点が存在するかを認識することがこのリスク分析にあたる。しかしながら、この資産の洗い出しが簡単ではないとの話をよく聞く。それは当然のことであるが、洗い出すべき対象が組織にはあり過ぎるからである。洗い出すべき対象を絞り込む工夫を考えなければならない。

また、リスク分析の視点を変えて、定型の質問表から組織の

図3■情報セキュリティマネジメントサイクル



現状を把握するという方法も考えられる。リスク分析に許されるコスト・時間との兼ね合いから検討してほしい。

②ポリシー策定

> 『情報セキュリティポリシー』の策定・評価・レビューは情報セキュリティ委員会が行うこととする。
> 情報セキュリティ委員会では、方針および対策標準を策定することとする。
> 対策手順書に関しては、情報セキュリティ委員会より指名された各情報システムの担当者が策定し、運用しなければならない。

サンプルでは、ポリシー策定を上記のように規定している。ここは、ルールに対する責任の所在を明らかにするところである。情報セキュリティポリシー全般の責任は情報セキュリティ委員会が担い、ポリシーおよびスタンダードの策定とレビューを担当する。プロシージャは、現場担当者に策定を依頼するという筋書きである。

このようにすることで、組織としてのルールの統一性を図るとともに、現場に即したルール作りが行えるよう考慮している。

③対策の実施

> 当社で策定した『情報セキュリティポリシー』に記述した対策は、計画的に実装しなければならない。情報システム部は、セキュリティ対策実装のための計画書を策定し、情報セキュリティ委員会の承認を得なければならない。

サンプルでは、対策の実施を上記のように規定している。対策には、さまざまなものがあるが、それらを効果的に実施していく段取りを情報システム部が担うように規定している。製品やサービスの利用、自社内で行える対策などを洗い出し、それらをスケジュール化していくことが必要になってくる。

対策は、一過性のものではなく、継続して実施していく事項になるため、十分な準備を行って実施していきたい。

④教育・啓発

> 当社は、情報資産を扱うすべてのものに対し、意識向上と技術レベルの向上の両面から、積極的に情報セキュリティの教育を行うこととする。
> 当社の情報資産に関わるすべて者は、会社が提供する情報セキュリティの教育を受けなければならない。同時に、当社の情報資産に関わる者は、情報セキュリティに関する最新の情報について、自発的に情報セキュリティ委員に提言することが望ましい。

教育・啓発は、対策の一部といえば一部である。しかしながら、これを別立てで規定しているわけは、他の対策よりも強調したい部分であるからである。

セキュリティ対策には、技術的に実施できるものと社員の意識改革を行って対策（人的な対策）するものとがある。いくら技術的な対策を実施しても、社員の意識が低いままであれば、対策のしようがない。セキュリティ対策はプロセスのつながりによって強化されるが、そのプロセスをつなげる役目を担うのが人であることは、近い将来においても変わらないであろう。

⑤監査・評価

> 情報セキュリティ委員会は、定期的あるいは発見の可能性のあるときに情報セキュリティに対する脅威、脆弱性を洗い出し、その対策を検討し、『情報セキュリティポリシー』に反映させなければならない。
> それらは、監査の結果、情報資産の利用者から届けられた情報、情報セキュリティの脆弱性に関する情報の収集等の活動から得られる情報をもとに行われる場合もある。

計画的に実施してきたセキュリティ対策を、ある一定期間が過ぎてから見直すことが求められている。情報セキュリティポリシーに規定されている内容が遵守されているかどうかがここでのポイントになる。

ITの世界では、ドッグ・イヤー、マウス・イヤーと表現されているようにその技術革新はスピードをもって行われている。そのため、今は最適なソリューションでも、将来において最適なソリューションであり続ける保証はない。

また、組織が活発な活動を続けていけば、当然新たな情報資産が増えることも予想できる。それらの評価と、それらが加わることでの現状への影響を再評価することが必要である。新たな脆弱性が存在している以上は、その脆弱性に対して対策を検討しなければならない。

⑥文書の改廃（ルールの改定）

> 『情報セキュリティポリシー』の改廃は、方針は、取締役会の承認を必要とする。対策標準および実施手順は、情報セキュリティ委員会が決議する。

この規定は、②ポリシー策定の部分と関連する規定である。文書を改定し（あるいは破棄し）、組織の求めるセキュリティ要件に即した情報セキュリティポリシーは、あるべき姿であるが、改定する場合の手順なども詳細に決めておく必要がある。

①から⑥までを順を追って説明したが、このすべてのプロセスを定期的に実施することで組織のセキュリティレベルがスパイラル的に向上していくことになる。情報セキュリティポリシーの役割は、このスパイラル的に向上していく道しるべを示すことにある。（足利）

以上でポリシーについて理解していただけたことと思う。次回は、スタンダードの概要について解説する。

セキュリティ対策講座③
サンプルを見ながら策定する
ドンと来い！情報セキュリティポリシー

第 2 回（全8回）

セキュリティ対策の「スタンダード（標準書）」を作る①
準備篇～スタンダードの策定内容と構成

スタンダードは、組織における情報セキュリティ対策の要件を具体的に規定するものであり、策定に多くの労力を要するものだ。
今回は、スタンダード策定の準備段階として、まず、スタンダードの策定内容や構成などをJNSAのサンプルを用いて解説する。

著者：NPO　日本ネットワークセキュリティ協会　理事　佐藤慶浩
スタンダードの概要……NECソフト株式会社　小杉聖一／株式会社ラック　足利俊樹

本講座の読み方

まずは以下のWebサイトよりJNSAのポリシー・サンプルの全文をダウンロードしてほしい。

http://www.jnsa.org/policy/guidance

これを印刷して本書の横に並べて読んでいただきたい。本講座では、その一部を解説の必要に応じてJNSAの承諾を得て転載している。引用部分は以下のような囲み表示をしてある。

> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

このようなサンプル引用に解説を加えていくことで、自社に適したポリシーを策定するための手助けを行っていくことを目的としている。

前回は、情報セキュリティポリシーのうち、ポリシー部分（図1）について解説した。今月以降はスタンダード部分について解説する。その最初となる今回は、スタンダード部分の全般について解説する。

前回の『情報セキュリティ方針』では、社内に「情報セキュリティ委員会」を設置して、その委員会がスタンダードを作成するような例を挙げた。今回はJNSAのワーキンググループ（以下WG）でのサンプル作成の工程を例に解説する。これは、企業や組織でポリシーを作成するときの委員会作業によく似ており、WGメンバーがどのような分担で作成したのか等、読者が実際にスタンダードを作成する際の参考になるはずだ。

前半ではJNSAのWGで行ったサンプル作成作業の様子を、ポリシー・サンプルの『スタンダード概要』の内容とともに、小杉氏に解説していただく。そして、企業や組織の特色が表れるといわれるスタンダード項目の展開と、それぞれの項目でのスタンダード文章作成のポイントについて、足利氏に解説していただく。最後に、ポリシーとしての国際・国内標準への準拠についてコメントを加える。（佐藤）

セキュリティ対策を具体的に規定する情報セキュリティ対策標準（スタンダード）

情報セキュリティポリシーは、企業や組織の情報セキュリティへの取り組みについての方針を明文化したものである。そして情報セキュリティ基本方針（ポリシー）は、企業や組織が情報セキュリティを維持するための取り組みを、どのように行っていくかを宣言する文書である。このことは既に第1回で解説した。

その下位に位置する情報セキュリティ対策標準（以下スタンダ

JNSAの紹介

JNSAは2000年4月に設立され、2001年7月にNPO法人として活動を継承しました。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を、現在13のWG（ワーキンググループ）に分かれて行っています。

昨年度の主な成果物としては、「外部接続に関するセキュリティポリシーサンプル冊子」の作成、「セキュリティインシデント被害調査」におけるアンケートの実施および報告書の作成などが挙げられます。

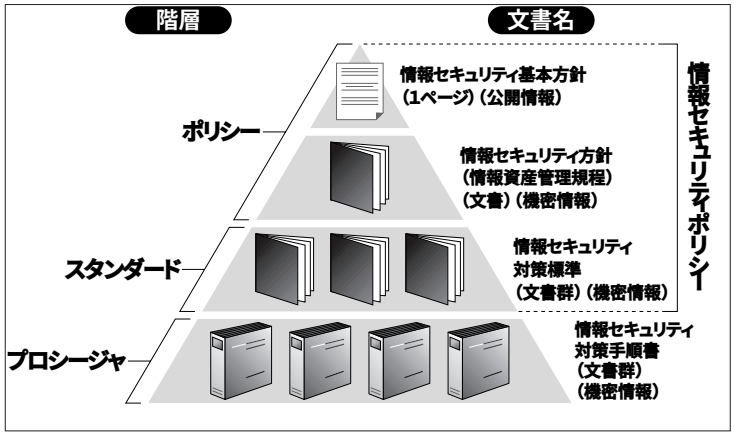
また、複数CAの相互運用性に関する実証実験を行った「Challenge PKI 2001プロジェクト」の結果報告も、近日中にWebにて公開の予定です。その他の活動として、年1回の主催カンファレンスの開催（NSF2002、今年は6月12-13日）、毎月のセキュリティセミナーの開催、会報誌「JNSA Press」の発行（年3回）などを行っています。

＜お問い合わせ＞
特定非営利活動法人　日本ネットワークセキュリティ協会
URL：http://www.jnsa.org/
E-Mail：sec@jnsa.org

ード）は、企業や組織が情報セキュリティを実現するために、ネットワーク、サーバ・クライアント、アプリケーションといった環境や、この環境の運用＆管理等において、何を守るのか？ 何から守るのか？ そのために何をするのか？を明確に記述するものだ。要するに、その企業や組織の情報セキュリティの規定書となるものである。

スタンダードは、企業や組織で行う情報セキュリティの最も重要な部分であり、企業や組織によって捉え方が異なる。そのため、策定した内容は組織によってさまざまであり、1つとして同じものは存在しない。またその内容は、誰がどのような理由で何を行うか、そしてそれをどのように維持していくかを、利用者と運用者をはじめ、情報にアクセスするすべての関係者に分かりやすく、より具体的に記述する必要がある。

図1■情報セキュリティポリシー関連文書群の全体構成



JNSAワーキンググループによるスタンダード作成作業に学ぶ

ここからは、JNSAのWGで行ったサンプル作成作業の様子をもとにいくつかのポイントを解説したい。ここで行われたポリシー・サンプル作成自体がスタンダードの作成作業である。

JNSAにはいくつかのWGがあり、今回のポリシー・サンプルは、セキュリティポリシー作成WGが2000年から2年かけて作成したものだ。2000年は、まず現在の企業や組織で共通性の高いものは「外部ネットワーク接続に関すること」であると考え、そのポリシー・サンプルを1年かけて作成し、『外部ネットワーク接続に関するセキュリティポリシー』として公開した。2001年は、それをベースに、どの企業や組織にも共通する事柄が多いと思われるモデル企業を想定し、対象項目を拡大して『情報セキュリティポリシー』を作成した。モデル企業としては、「製造や生産を伴わない販売会社」を想定した。このモデル企業では、営業部門が会社のほとんどを占めており、情報システム部門については、主として企画と運用だけを担当し、自社開発を行わないような、小型の情報システム部門を有しているという設定にした。これが今回解説するポリシー・サンプルである。

4つの作成アイテムに分けスタンダード作成作業を行う

まずスタンダードの作成手順だが、情報セキュリティ基本方針（以下ポリシー）によって情報セキュリティ委員会ができたなら、この情報セキュリティ委員会においてスタンダードを作成することになる。情報セキュリティ委員会では、スタンダードをいくつかの作成アイテムに分け、各担当者で分担し、作成スケジュールを立てて作業する。JNSAのWGでは、4つのアイテムで作業を行ってきた（図2）。

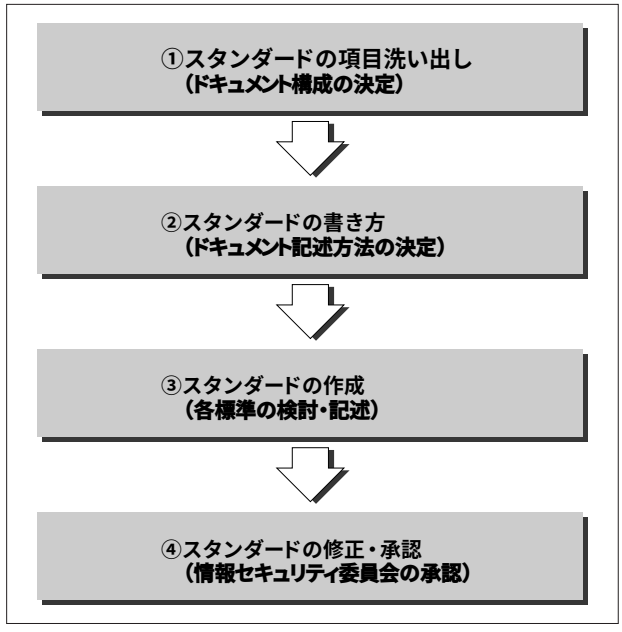
まず作成するスタンダードの構成を決めるために、どのような項目で作成するかを検討する。リスク分析を行った会社においては、その結果から必要な項目を導き出す方法が考えられる。

項目立てのサンプルとして思いつくのは、ISO/IEC17799やISMSの項目である。しかし、これらの小分類項目を使用する場合、単純に考えるとISO規格で127項目（ISMSでは134項目）のルールを準備しなければならない。これらをそのまま横一列に並べてしまうと、あまりに煩雑で、運用を考えるととても管理しきれなくなってしまうことも予想できる。また、中分類の項目を使用する場合は、逆にあまりに漠然としてしまい、「帯に短したすきに長し」的な印象を拭えない。

そのため、企業に適したスタンダード項目を検討する場合、127項目から関連する項目を紐付け、より具体的な項目名にすることが推奨される。具体的な項目名にすることで、スタンダードを参照する人の検索性を向上させることも可能になる。

この2つができたらスタンダードを各担当者で作成する。作成したスタンダードは、情報セキュリティ委員会でレビューし、修正する。最終的には、情報セキュリティ委員会委員長の承認を受け、完了となる。

図2■スタンダード作成の流れ（4つのアイテム）



ポイント1　スタンダードの構成（ドキュメント構成の決定）

スタンダードの項目については本来、ポリシー作成時に行うリスク分析の項目や、セキュリティ標準であるISO/IEC17799やISMSを参考にすることが多い。JNSAのポリシー・サンプルは、モデル企業に必要と思われる項目を、WGの作成メンバーが意見を出し合い決定した。それが、表1のスタンダード項目（29項目）である。

ポイント2　スタンダードの記述方法（記述方法の決定）

スタンダードの項目が決定したら、実際のスタンダードのドキュメント構成を決める。このドキュメント構成も企業や組織の考え方によって異なってくる。しかしこのドキュメント構成をどのようにするかも重要なポイントであるため、運用時をイメージしつつ検討し、決めるべきである。

スタンダード策定では、情報セキュリティ対策を明確化（明文化）することが、重要なポイントである。このドキュメント構成をどのようにするかは、明文化した情報セキュリティ対策を効率よく運用していくためにも重要であり、スタンダードの良し悪しにも繋がる。

スタンダードの構成を整理してみると4つになる（図3）。最終的にどのように情報セキュリティ策定を実施するかによって決まるが、JNSAのポリシー・サンプルでは、セキュリティ項目との対応とドキュメントの管理（作成や改版）を容易にできるように、1つの項目を1つのスタンダードにし、全体を管理するドキュメントと合わせて30個のスタンダードの構成にしている。ISO/IEC17799及びISMSとの対応は、ドキュメント作成後に該当ドキュメントがどの項目に対応しているかの対応表を作成すれば対応でき

表1●スタンダード項目の一覧

項番	スタンダード項目
1	物理的対策標準
2	サーバルームに関する標準
3	媒体の取扱に関する標準
4	職場環境におけるセキュリティ標準
5	ソフトウェア／ハードウェアの購入及び導入標準
6	クライアント等におけるセキュリティ対策標準
7	サーバ等におけるセキュリティ標準
8	外部公開サーバに関する標準
9	パスワードに関する標準
10	アカウント管理標準
11	ウイルス対策標準
12	電子メール利用標準
13	Webブラウザ利用標準
14	ネットワーク構築標準
15	LANにおける機器設置/変更/撤去の標準
16	社内ネットワーク利用標準
17	専用線及びVPN利用標準
18	リモートアクセスサービス利用標準
19	システム維持に関する標準
20	システム監視に関する標準
21	セキュリティ情報収集及び配信標準
22	セキュリティインシデント報告・対応標準
23	監査標準
24	プライバシーに関する標準
25	セキュリティ教育に関する標準
26	罰則に関する標準
27	スタンダード更新手順
28	プロシージャ配布の標準
29	第三者契約に関する標準

図3■スタンダードの構成は4つのパターンに整理できる

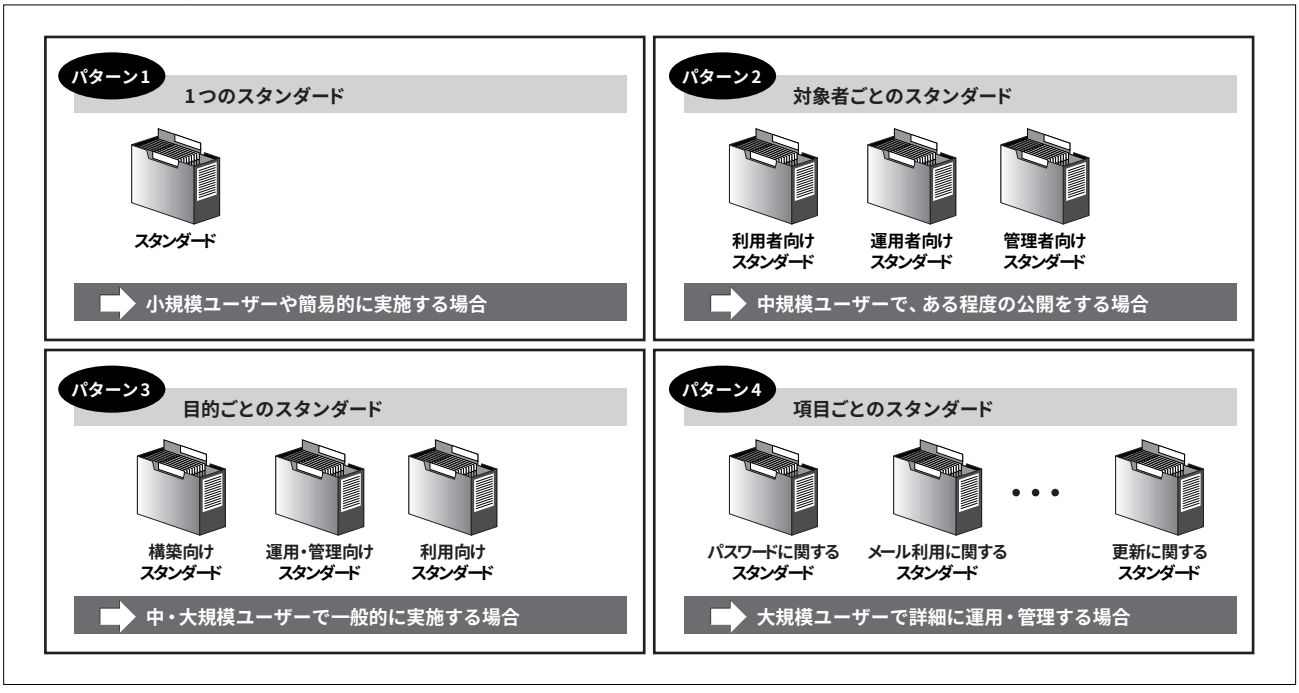


図4■ポリシー・サンプルで採用したスタンダードの項番

1. 趣旨
2. 対象者
3. 対象システム
4. 遵守事項
5. 例外事項
6. 罰則事項
7. 公開事項
8. 改訂

るので問題はない。

スタンダードの構成が決まったら、すぐに作成に入るのではなく、その前にスタンダードの記述方法を決めることになる。これは、作成したスタンダードの記述がばらばらでは、スタンダードを見る人も理解が大変になるし、内容の確認も困難になるからである。

ポリシー・サンプル作成時には、作成するスタンダードの項番について、スタンダード作成前に決めておく。まず、すべてのスタンダードに適用できる項番を作成し、作成するドキュメントごとに若干の変更を行う方法を取ればよい。JNSAのポリシー・サンプルで採用した項番を図4に示す。『スタンダード概要』については、一部ポリシーの内容も記述し、スタンダードの構成等を記述しているために項番が異なっている。

ポイント3 スタンダードの検討・作成・修正（実際の作成と修正）

スタンダードの構成と記述方法が決まったら、スタンダードの作成である。スタンダードの作文は、1つのスタンダードを担当者1名で書ける程度のものだ。逆に1つのスタンダードを複数の担当者で作文すると、検討会の実施や編集等で余計な時間がかかるため、担当者1名で実施することが望まれる。

できあがったたたき台の文章は、委員会でまず内容の確認（一般的にはレビュー）と修正を行う。最終的には情報セキュリティ委員会から、ポリシーで定めた上位の管理者層に起案して承認を受け、発布することになる。

WGでのポリシー・サンプル作成では、1つのスタンダードにつき1名の担当者がたたき台を作成し、作成されたものを他のメンバーと意見交換した。最後に全メンバーで意見交換をして、一般公開した。

『スタンダード概要』ドキュメント

それでは、スタンダードのサンプルを使って実際のスタンダードの解説をする。今回は『スタンダード概要』のなかからいくつかピックアップして解説する。

ポイント4 趣旨と対象範囲（ポリシー・サンプル参照）

1　趣旨
当社は、ネットワークコンピュータ上を流通する情報やコンピュータ及びネットワークなどの情報システム（以下、情報資産）を第4の資産と位置付け、この情報資産を重要な資産とし、保護・管理する「情報セキュリティマネジメント」を実施するために、『情報セキュリティポリシー』を策定する。
『情報セキュリティポリシー』は、「情報セキュリティ基本方針」＋「情報セキュリティ方針」と「情報セキュリティ対策標準」と「情報セキュリティ実施手順書」の3つの階層で策定・管理する。
「情報セキュリティ対策標準」は、「情報セキュリティ方針」に従い、情報資産を保護・管理するために遵守すべき事項を可能な限り具体的かつ網羅的に記載したものである。

2　対象範囲
「情報セキュリティ対策標準」の適用範囲（対象システム）は、当社の情報資産に関係する人的・物理的・環境的リソースを含むものとする。
当社の対象システムのシステム構成図を下図に示す。

趣旨と対象範囲は、既に作成している情報セキュリティ基本方針と基本的には対応する内容となる。スタンダードの作成完了時に、必要であれば、各スタンダードの趣旨のポイントを箇条書きなどでこの部分に追記すると分かりやすくなる。また適用範囲については、対象範囲が複雑であれば、その詳細説明を記述する。

ポイント5 適用者（ポリシー・サンプル参照）

「情報セキュリティ対策標準」は、当社のネットワークコンピュータを利用するすべての利用者に適用する。しかしセキュリティ対策の内容によって適用者が異なるため、各情報セキュリティ対策標準では適用者を明確に記載するものとする。
「情報セキュリティ対策標準」の適用者を、以下に示す。

(1) 当社の経営陣と従業員
(2) 子会社・関連会社の従業員
(3) 外部委託業者の従業員（派遣社員、アルバイトを含）

適用者には、スタンダード（全体）の対象者を明確かつ詳細に記述する。特に社員以外の部分には注意が必要である。なぜならば、情報セキュリティの適用は社員だけでなく、その企業や組織の情報資産を利用・管理する、すべての関係者が対象だからである。この適用者に社外の利用者を記述する場合には、その相手にも情報セキュリティ対策が必要であり、必ず両者の合意がなければならない。当然アルバイトなどの第三者や、インター

ネットを利用して内部の情報にアクセスする対象者などを入れることも必要である。

ポイント 6　用語（ポリシー・サンプル参照）

セキュリティ対策標準で用いられる用語について、以下のように定義する。
(1)セキュリティ方針
セキュリティ方針は、『情報セキュリティポリシー』の最上位に位置する文書であり、当社の情報セキュリティマネジメントにおける方針を記述したものである。
(2)セキュリティ対策標準
セキュリティ対策標準は、方針の下層に位置する文書であり、方針での宣言を受け、項目ごとに遵守すべき事項を網羅的に記述する。

用語には、スタンダード全体で利用している用語のなかから、その企業や組織で固有の用語を記載する。一般的なコンピュータ用語などを記載する必要がある場合には、別紙にすると管理が容易になる。

ポイント 7　罰則事項（ポリシー・サンプル参照）

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

罰則事項には、スタンダードに記載されている内容に違反したときの罰則事項を記載する。ポリシー・サンプルでは別途作成している『罰則に関する標準』に従うように記載しているが、この章に直接記述しても運用等への影響はない。

ただし、この罰則事項は前述した適用者が対象となるため、適用する場合には企業の就業規則との関係も考慮しなければならない。人事部門や委託契約部門などの意見も聞きながら、慎重な作成が必要な部分である。

ポイント 8　改訂（ポリシー・サンプル参照）

本標準は、平成xx年xx月xx日に情報セキュリティ委員会によって承認され、平成xx年xx月xx日より施行する。
本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。
情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。
本標準は、定期的（年1回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

改訂には、スタンダードの承認及び施行された年月日を記載するとともに、そのスタンダードの変更について記載する。

スタンダードは、1年に1回程度見直しを行い、改訂（修正）の必要性を検討する。また、ポリシーやプロシージャの変更を反映するために改訂する場合もあるので、その内容も記載しておくべきである。（小杉）

「スタンダード」は文書量が多くなる？

WGでは、上記のような流れでスタンダードを作成した。さまざまな現場で作成されるスタンダードも似たような経緯で作成されるだろう。しかしながら、筆者がスタンダードをお客様に納品するとき、ファイルを眺めながら、“ こんなにルールを守らせなければならないの？ ”などとご意見をいただくことがある。

確かに、既に多くのルールを守らせている従業員に対して、新たに守るべきルールを追加することは、出す側も気がひける。出される側は嫌悪感さえ感じるかもしれない。このような状況では、その企業にマッチしたスタンダードとはいえない。しかし、現実にそのようなギャップを発生させる要素は存在する。

例えば、現場担当者にすれば、ルールは少なければ少ないほどありがたいものであり、ルールが多ければ先の意見が出てくることになる。しかし、ポリシー作成の支援を社外に委託した管理職のなかには、内容ではなく見た目（文書の厚さ）で金額に見合ったドキュメントであるかどうかを判断する方々もおられる。このような状況下では、コンサルタントとしては、いかに無駄なく分厚いドキュメントを作成するかも腕の見せ所だったりする。

このサンプルも、その意味ではもっと贅肉を減らすことが可能である。ここでは、贅肉を減らすポイントをいくつか紹介しよう。

「スタンダード」には、説明文が多い！？

まず、1つめのポイントは、スタンダードには、解説文、説明文の量が多いということだ。コンピュータ・ネットワークのセキュリティといっても、まだまだ言葉を理解することに苦しむ人が多くいるのも事実である。そのため、遵守事項のみの文書にした場合、それこそ理解できない言葉の羅列と受け取られ、まったく守ってもらえない文書になる可能性がある。このような理由から、スタンダードの文書量がどうしても増えてしまうのである。セミナーなどでは、“ 情報セキュリティポリシーは簡潔に ”などといっていたりするが、難しいところではある。携帯電話機のマニュアルが分厚くて、開かない読者も多いことだろう。スタンダードでは、そのようなことがあってはならない。

このような説明文を極力省くことで、スタンダードの全体量を減らすことが期待できる。しかし、その弊害として、理解しがたいスタンダードになってしまうということがある。そのため、情報セキュリティポリシー教育セミナーや理解度テストなどでフォローすることも十分に検討してほしい。

スタンダード項目は必要なものから

サンプルの30項目から緊急を要する項目を洗い出し、そこから、自社のセキュリティ運用を始めることができる場合もある。

すべてを実現させようとして途中で投げ出すよりは、部分的に始めてもよいかもしれない。

本連載の次号からは、スタンダード項目を6つにグルーピングする。以下がそのグループである。

①サーバ対策なんてドンと来い集
②クライアント対策なんてドンと来い集
③ネットワーク対策なんてドンと来い集
④物理的な対策なんてドンと来い集
⑤セキュリティ運用なんてドンと来い集
⑥その他いろいろなんでもござれ集

自社にとって何が最も守らなければならないものなのかを理解し、スタンダードのできあがったグループからセキュリティ運用を行っていけば、時間に無駄がないだろう。

本連載全体を参考にしつつ、現状に即した情報セキュリティポリシーの姿を検討していただきたい。（足利）

国際・国内標準とポリシー・サンプル

次回からサンプルを使った、スタンダードの解説を始めるが、今回の表1で紹介したスタンダード項目について補足しておく。

項目については、ISO/IEC17799やISMSに一覧が示されている。JNSAのポリシー・サンプルには、それらのほとんどが含まれているが、大きな項目として、サンプルにないものは以下のとおりである。

①情報分類
②システム開発
③コンプライアンス
④事業継続計画

情報分類の項目は、非電子の文書でいう「極秘」や「社外秘」、「人事秘」などの、情報の分類を定めるためのものである。企業や組織では、「文書管理規定」などで、情報セキュリティポリシーを作成する以前に存在していることもある。

今回のJNSAサンプルでは、この部分の一般化はあまり意味のないものと考え、作成していない。この部分については、ポリシー作成の際に、自分の組織に合ったものを検討の上で定めていただきたい。既存の規定があるのなら、それに従うものとしてもかまわない。「情報分類については、『文書管理規定』の定めに従うものとする。」などのようにすればよい。ポリシー・サンプルでは、この項目がないために、ポリシーやスタンダードの本文中で、「重要な情報については」などの抽象的な表現をしている。情報分類項目があれば、それらの部分は、「極秘の情報については」などと明確にしたほうがよい。

システム開発の項目については、モデル企業が、自身ではシステム開発を行っていないものとしたため、この項目のサンプルを用意しなかった。しかし、自社運営しておらず、業務委託をしているのであれば、その委託に際しての要件をスタンダードとして明記する必要がある。

その場合には、サンプルにはないが、皆さんがポリシーを作成する際には含めるほうがよい。市販製品だけしか使用しておらず、まったく、自社での開発も開発の委託もしていないという場合には、この項目はなくてもよい。

コンプライアンスと事業継続計画の項目については、WGの作業の目的が技術指向であったため、サンプルの作成を行わなかった。これらも、実際のポリシー作成では、重要な項目である。それぞれ、法務部門や経営企画室などの方々を中心とする小委員会を作って作成したほうがよい。

コンプライアンスは、主として法令の遵守や監督官庁のガイドラインに準拠することを宣言するものである。それらは一見当たり前のことであるが、法令の遵守については、解釈の仕方について、自社の法務部の見解を示し、法律がもっているあいまいさを可能な限り明瞭にしておくべきである。法務部の人にとって当たり前のことも、一般の人にとっては当たり前とは限らないからである。監督官庁のガイドラインについては、必ずしもすべてに準拠する必要のないこともある。これについても、どの範囲で準拠するのかを明らかにしておくことで、現場の準拠に役立つ。

以上、サンプルに不足している項目を紹介したが、逆にいえば、この4つを含めれば、国際規格や日本の制度基準が示している項目一覧を満たすことができる。

具体的な目標設定ができているか？

スタンダードを策定する場合に注意しなければならないのは、具体的な目標設定をすることである。現場で達成できないとあらかじめ分かっていることを定めるのもよくない。そのような高い目標を定めたいのであれば、解決策や支援策を計画してから現場に発布すべきである。それが困難であれば、目標を下げ、下げた分のリスクを経営者層が受け入れなければならない。経営者層は、そのリスクを受け入れられないのであれば、その対策に必要とされる経営資源を割り当てる必要がある。

また、現実的ではない目標設定を一部にすれば、現場では、この「情報セキュリティポリシー」には、無理なことも書いてあるので、「できることだけやればよい」という意識が生まれてしまう。逆にそのような努力目標を極力なくすことで、「できることしか書いていないので、書いてあることを必ず遵守してください」という位置付けにしたほうが実効性のより高いものにできる。

「情報セキュリティポリシー」は、組織が単に組織員に何かを強いるものであっては意味がない。情報セキュリティ対策の要件を満たすための責務は、経営者層も含めたすべての者にある。

次回は、スタンダード項目の1番目のグループとなる「サーバ対策なんてドンと来い集」について解説する。

個別の返答は必ずしもお約束できないが、連載内容に反映していきたいと考えているので、ご意見・ご感想等を電子メールでぜひお寄せいただきたい。

E- Mail：SECURITY-POLICY@yosihiro.com（佐藤）

セキュリティ対策講座③
サンプルを見ながら策定する
ドンと来い！情報セキュリティポリシー

第 3 回（全8回）

セキュリティ対策の「スタンダード（標準書）」を作る②
作成篇～サーバ対策なんてドンと来い

スタンダードは、組織における情報セキュリティ対策の要件を具体的に規定するもの。あらゆる組織で必要不可欠なものだ。その策定には多くの労力を要するが、JNSAのポリシー・サンプルをたたき台とすることで、それを軽減できるはずだ。今回は「スタンダードの基本項目」と、すぐに対策を施すべき「外部公開サーバに関するスタンダード」について、それらの構成と策定内容をJNSAのサンプルを用いて解説しよう。

著者：NPO　日本ネットワークセキュリティ協会　理事　佐藤慶浩
基本項目……株式会社ラック　網井理恵
外部公開サーバ……大興電子通信株式会社　豊田　明

本講座の読み方

まずは以下のWebサイトよりJNSAのポリシー・サンプルのファイルをダウンロードしてほしい。

http://www.jnsa.org/policy/guidance

今回は、次の3つのサンプルをダウンロードしてほしい。

『ユーザ認証標準』
『アカウント管理標準』
『外部公開サーバに関する標準』

これらを印刷して本書の横に並べて読んでいただきたい。本講座では、その一部を必要に応じてJNSAの承諾を得て転載している。それぞれのファイルからの引用部分は、章や節の番号とともに以下のような囲み表示をしてある。

> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

このようなサンプル引用に解説を加えていくことで、自社に適したポリシーを策定するための手助けを行っていくことを目的としている。

前回は、情報セキュリティポリシーのセキュリティ対策を具体的に規定した「スタンダード」の項目を決定する方法と、それぞれの項目で記述するべき事柄の概略について解説した。今回からは、スタンダードの各項目を1つずつ取り上げて、その本文にどのような内容を記載すればよいかについての詳細な解説を行っていく。

今回の構成だが、まず、スタンダードの基本項目である『ユーザ認証標準』と『アカウント管理標準』を網井氏に解説していただく。これら2つの標準は、今回のサーバ対策と次回のクライアント対策に共通するものであり、さらにはネットワーク機器などにも適用できるものとして非常に重要な項目である。次に、サーバ対策に関する標準の解説を行う。サンプルでは『サーバ等におけるセキュリティ標準』と『外部公開サーバに関する標準』の2つを用意している。それらのうち、対策が急務といわれている『外部公開サーバに関する標準』を豊田氏に解説していただく。『サーバ等におけるセキュリティ標準』と、それらに関係する標準である『ソフトウェア／ハードウェアの購入及び導入標準』については、かなり一般的な事項を書いてあるので、本講座では特に解説を行わない。読者はそれらもダウンロードして内容を各自で確認していただきたい。

なお、今回からは、連載の第1回で紹介したモデル企業を想定したポリシー・サンプルの具体的な解説となる。そのため、これまでの連載のなかで「企業や組織」という表現を用いてきた部分を、単に「企業」や「会社」などと表現する。ただし、内容的には非営利などの「組織」であっても同様なので、読者には随

JNSAの紹介

JNSAは2000年4月に設立され、2001年7月にNPO法人として活動を継承しました。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を、4つの部会と各WG（ワーキンググループ）に分かれて行っています。

昨年度の主な成果物としては、「外部接続に関するセキュリティポリシーサンプル冊子」の作成、「セキュリティインシデント被害調査」におけるアンケートの実施および報告書の作成などが挙げられます。

また、複数CAの相互運用性に関する実証実験を行った「Challenge PKI 2001プロジェクト」の結果報告も、Webにて公開中です。その他の活動として、年1回の主催カンファレンスの開催（NSF2002、今年は6月12-13日に開催）、セキュリティセミナーの開催、会報誌「JNSA Press」の発行（年3回）などを行っています。

＜お問い合わせ＞
特定非営利活動法人　日本ネットワークセキュリティ協会
URL：http://www.jnsa.org/
E-Mail：sec@jnsa.org

時読み替えていただきたい。 （佐藤）

『ユーザ認証標準』作成のポイント

ここでは、情報システムのユーザ認証を規定した『ユーザ認証標準』作成時のポイントについて解説する。

ポイント1 対象システム（サンプル3章参照）

以下のいずれかの条件を満たす機器、システム及びアプリケーションには、ユーザ認証を用いて情報セキュリティの確保に努めなければならない。
① 汎用的に使われているOSなどでネットワーク機能を持つ機器
② ハードディスクなどの記憶媒体を持つ機器
③ ルータ
④ ユーザが用いるメールソフトウェア
⑤ 社内情報共有の為のイントラネットソフトウェア

ポリシー・サンプルでは、ユーザ認証の対象となるシステムの範囲を上記のように記載している。このサンプルでは「いずれかの条件を満たす機器」として、①～⑤までの具体例を示している。皆さんがポリシーを作成する際には、ここには実際に自社に存在する具体的な機器を列挙するようにしてほしい。特に、サンプルでは③にルータが挙げられているが、他にもファイアウォールやスイッチなどのネットワーク機器を記載することは必須になるだろう。

ポイント2 パスワード（サンプル4.3節参照）

（1）8文字以上で記号を1文字以上含むことが望ましい。

認証に利用するパスワードについても明確に規定すること。ここでは具体的に8文字という数字が記述されているが、パスワード文字数やパスワード強度についての記述は、使用する端末のセキュリティ強度によって変えてもかまわない。例えば、サーバに使用するパスワードは8文字以上、クライアントに使用するパスワードは6文字以上などという値にしてもよい。

また、このスタンダードにはクライアントに設定する標準的な値だけを記述しておいて、サーバ類のパスワード設定に関しては『外部公開サーバに関する標準』や『サーバ等におけるセキュリティ対策標準』の中で別途記述するという方法を取ってもよい。

（3）設定されたパスワードは1ヶ月に一度を目安に更新することが望ましい。

パスワードの変更は通常、2～3ヶ月程度を目安に変更させるようにするとよい。ポリシー・サンプルでは1ヶ月という短い期間が設定されているため、語尾が「望ましい」となっている。皆さんが平均的な期間を設定する場合は、語尾を「しなければならない」というような必須を意味するものにしたほうがよいだろう。

（4）パスワードは原則として該当システムの管理者が生成して管理を行うものとする。設定したパスワードは紙などに書き留めてもよいが、対象システムが特定できたり、パスワードの文字列そのものを「あらわに」書き留めたりしてはならない。

原則として、パスワードは紙や電子ファイルなどの種類にかかわらず、どんな媒体にも書き留めてはならないものである。しかし、だからといって書き留めることを完全に禁止しても、1人や2人はメモ帳などに書き留めてしまう人が必ずいるものだ。この規定ではそれを見越して、条件付きでパスワードを書き留めることを容認している。どうしてもパスワードを覚えられないという人にとっては、パスワードそのものを書き留めておくのではなくて、そのヒントになることだけをメモしておけばよいという代替案が提供されることになり、守りやすい規定になるだろう。

また、この規定の前半と後半は少し意味合いの違う内容でもあるので、皆さんが作成するスタンダードでは、切り分けて2つの規定としたほうがすっきりするかもしれない。

（2）一般に使われている単語や本人の趣味、プライベートなどから、他人に推測されやすいパスワードを使用してはならない。
（5）パスワードは口外したり、ヒントとなるような物品を身の回りに置いておいてはならない。

（5）の規定は、例えばパスワードを"Porsche"にしている人が会社のデスクにポルシェの模型を置いておくと、パスワードを簡単に推測されてしまうのでよくないということを意味している。また、（5）の後半部分は（2）と類似しているので、「口外してはならない」という内容とは切り離して、「ヒントとなるような物品を身の回りに置いてはならない」の部分は（2）にまとめてしまったほうがよいかもしれない。

サンプル「4.3 パスワード」の内容を作成するコツとしては、細かい値を規定することももちろん必要だが、覚えやすくて、忘れにくく、強度の高いパスワードの考え方をヒントとして提供するということを心掛けるとよい。このような視点で規定を記述していくことで、よりよい内容になると思う。

ポイント3 パスワードを忘れた場合の処置（サンプル4.5節参照）

（1）利用者がパスワードを忘れた場合には、システム管理者に新規パスワード発行の申請を行わなければならない。
（2）システム管理者は、申請してきた利用者が本当に本人自身であることを何らかの方法で確認しなければならない。
（3）新規パスワード発行の申請を受けたシステム管理者は、速やかに新規のパスワードを発行して、利用者に通知しなければならない。

ユーザがパスワードを忘れた場合の処置についても、詳細に規定しておく必要がある。（2）の本人確認を実現する方法と

しては、例えば電子メールによる申請であれば、メールヘッダを確認し、送信者と申請者が一致しているかを確認するなどの作業を行うとよい。電話での新規発行申請は本人を確認することが難しいので、基本的には禁止したほうがよいだろう。

パスワードを忘れた場合の処置としては、現状のパスワードを教えるのではなく、再設定を行うということが重要である。ポリシー・サンプルでは、その内容を上記の(3)で規定している。

社員のなかには、企業内でのすべてのシステムに同じパスワードを設定している者も少なからずいるだろう。万が一、申請者の本人確認に間違いがあった場合、本人になりすました悪意のある人間に現状のパスワードを知られてしまうと、該当のシステムだけでなく同じパスワードを使用している他のシステムにまで不正ログインを許してしまうことになりかねない。ここで現状のパスワードを教えるのではなく再設定するのであれば、再設定を申請したのが本人でなかった場合、当の本人はシステムにログインできなくなるため、他人に再設定されたという異常を知ることができる。このような理由から、パスワードを忘れたユーザに対して現状のパスワードを教えるべきではない。

その他、パスワードに関する規定としては、パスワードを規定回数以上間違えて入力した場合に、自動的にアカウントをロックするようなシステムを導入するなど、回数制限を加えることが望ましい。

ポイント4　ワンタイムパスワード(サンプル4.6節参照)

(1) ワンタイムパスワードはPIN番号などの認証が必要なものを用いなければならない。
(2) 時刻同期などの認証を必要としない機器は使用してはならない。
(3) ワンタイムパスワードの発生器は、PIN番号などを推測出来るような状態で携帯してはいけない。

サンプルではワンタイムパスワードについて上記のように記述されているが、あくまでもこのサンプルの対象となっている架空の企業を想定して作成されているもので、一般的なものを示しているわけではない。したがって、ワンタイムパスワードの導入自体も、リスク分析の結果と費用などを考慮して行ってほしい。企業によっては、最初からこの項目を規定する必要がないところもあるだろう。また、導入する機器が決まっている場合は、その機器について具体的に書くことが望ましい。

ポイント5　生体認証(サンプル4.7節参照)

(1) パスワードの記憶と管理が困難な場合には、生体認証を用いても良いが、最新技術動向やコストなどを勘案して、適切な方式を選択しなければならない。
(2) 生体認証を使用する場合には、生体認証のデータそのものが重要な個人情報であるので、厳重に管理しなければならない。
(3) パスワードの利用に対する利便性向上の手段としては、指紋認証などの簡単な生体認証を用いることができる。
(4) サーバルームなどの高いセキュリティを要求される場所への立ち入りの管理には、虹彩認証などの高レベルのセキュリティが期待できる認証システムを用いなければならない。

生体認証は、改ざんされにくく、なりすましが困難なのが特徴である。その上、利用者が認証情報を記憶・携帯する必要がないため、セキュリティ強度の高い認証手段として注目されている。しかし、導入費用がまだそれほど安くないので、これもワンタイムパスワードの導入と同様に、費用対効果を十分に考慮して導入を決める必要があるだろう。また、障害者を採用している企業では、生体認証を使用することで問題が起こらないように注意する必要がある。

●その他、盛り込むべき内容

一般的にユーザ認証の方法は「知識」「所有」「生体」の3種類から成るといわれている。ポリシー・サンプルのなかでは、知識による認証では「パスワード」、生体認証では「虹彩」、知識と所有物の組み合わせによる認証では「ワンタイムパスワードの発生器」を取り上げている。これらはあくまで例の1つである。生体認証としては、指紋、声紋などによる認証方法もある。その他、IDカードによる認証を採用している企業も少なくないと思うが、その場合にはIDカードの管理取り扱い方法を盛り込むことが必須となるだろう。

『アカウント管理標準』作成のポイント

次にユーザのアカウント管理について規定した『アカウント管理標準』作成時のポイントについて解説していく。

ポイント1　新規アカウントの発行(サンプル4.1節参照)

(1) 新規のアカウントが必要になった場合には、必要な権限と共に人事権を持った管理者に申請する。
(2) 申請を受けた人事権を持った管理者は、必要な権限と必要性を検討し、妥当と判断した場合には、システム管理者に新規アカウントの発行を申請する。

サンプルでは、アカウント利用者がシステム管理者に直接発行申請するのではなく、人事権を持った管理者の承認を経て、システム管理者に申請がなされるよう記述されている。これは、企業の運用体制やシステム構成に大きく依存する部分だ。皆さんの環境で必ずしもこのような運用を実現することはできないかもしれないが、その場合は実情に合った内容を記述することになるだろう。

しかしながら、アカウント利用者から直接システム管理者に発行申請させる方法は、本当に必要でないアカウントを発行してしまうなどの無駄が発生しがちである。また、悪意の人間によるなりすましを容易に許してしまうことにもなりかねないので、十分注意が必要だ。

ポイント2　アカウントの変更（サンプル4.2節参照）

（2）人事権を持つ管理職は、現在部下に与えている権限に変更があった場合には、速やかに申請を行うように担当者に指示しなければならない。特に、権限の縮小が行われた場合には、業務上の不都合とは関係なく、セキュリティ上の理由から、速やかにアクセス権限の変更の申請を行わなければならない。

サンプルには、アカウントに付与されている権限の変更についてのみ記述されている。実際の作成時には、休職者のアカウントを復職するまで停止するといった、一時的な権限の付与、及び停止についても記述するとよいだろう。

ポイント3　アカウントの削除（サンプル4.3節参照）

（1）人事異動などで不要となったアカウントは、速やかに削除・停止にしなければならない。

社員の退職によりアカウントを削除・停止する場合に、どのくらいの期間無効にするのかということも記述したほうがよい。特に電子メールのアカウントについては注意が必要だ。例えば、田中Aという社員に"tanaka@○○.co.jp"というメールアカウントを付与していたとする。その社員が退職したあとに、新しく田中Bが入社してきた場合に" tanaka@○○.co.jp"というメールアカウントを付与すると、田中A宛てのメールを田中Bが受信してしまうといった問題が発生する可能性がある。

削除したアカウントを再使用することを認めるのか、それとも永久的に使用しないのか、もしくは5年経過した後は使用してもよいとするなどの、期間を意識した規定を盛り込む。

●その他、盛り込むべき内容

ポリシー・サンプルには記述されていないが、アカウントの新規発行、変更、削除を行った際の記録はすべて保存するように規定しておくべきである。不必要なアカウントがないか確認したり、権限の付与が正しい設定になっているかなどを適宜、監査する必要もあるだろう。

また、アカウントは本人であることを認証する手段でもあるので、共有したりしないようにアカウント利用者への注意点を記述するなどの配慮をすると、よりよいものになるだろう。

（網井）

『外部公開サーバに関する標準』作成のポイント

ここからは、『外部公開サーバに関する標準』を作成する際のポイントについて解説していく。JNSAポリシー・サンプルに記載されている内容のなかでも、別な記述の仕方をしたほうがよいと思われる点など、特に注意すべき点を中心にサンプルより抜粋しながら解説する。

●標準制定が求められる背景

現在、企業で公開サーバを持つというのは、企業の宣伝、イメージアップという点では必要不可欠のものになってきている。

しかし、そのことによって盗聴、なりすまし、改ざん、不正アクセス、踏み台など、ネットワークを利用したさまざまな脅威が発生し、企業を脅かしている。そこで、『外部公開サーバに関する標準』を速やかに制定することが求められている。このスタンダードは、円滑かつ効率的なビジネスの維持と情報資産の保護を実現するための、セキュリティの管理、維持、向上を目的としたものだ。

ポイント1　対象システム（サンプル3章参照）

インターネットに接続し、不特定多数のインターネットユーザにIPアドレス及び情報を公開する情報システム、情報機器などを対象とする。対象システムの例としては外部公開サーバ（ウェブサーバ、メールサーバ、FTPサーバ、DNSサーバ、プロキシサーバなど）、ルータ、ファイアウォール及び外部公開サーバに情報を提供するデータベースサーバなどがある。

サンプルでは、対象となる外部公開サーバについて上記のように規定している。ただし、ここで規定している対象システムは、あくまで今回のサンプルの定めたモデル企業のシステムを基に規定したものである。

企業それぞれの環境、適用範囲により記述内容は変わるはずだ。例えば現在であればモバイルユーザ認証サーバといったものがあるだろう。個々の企業に適した形で作成していただきたい。

ポイント2　リスク分析の実施（サンプル4（1）節参照）

・リスク分析の実施
システム設計者は、外部公開サーバのセキュリティ設計を行う上で、必ずリスク分析を行わなければならない。リスク分析を行う上で、以下の項目を明確にしなければならない。
・保護・脅威の対象（守るべき情報）
・脅威の内容
・脅威の原因、プロセス
・対策（予防、防御、検査、対応：回復）

外部公開サーバのリスク分析について、サンプルでは上記のように規定している。リスク分析によって得られたリスク評価結果は、スタンダード、プロシージャに規定するセキュリティ要件、条件を導き出すといった役割を果たすものだ。

サンプルの『情報セキュリティ方針』において、リスク分析は情報セキュリティ委員会が行う旨が記述されている。そのため、本来は委員会によってリスク分析が検討されているはずだ。

しかし、現実問題として、『情報セキュリティ方針』を作成する時点では、大枠的なリスク分析を行えたとしても、詳細なリスク分析を行うことは難しい。詳細なリスク分析は、機器、OS、アプリケーションが揃って、実際の運用に近い状態が実現で

きた時点で、はじめて行えるものだからだ。

サンプルで、リスク分析を設計者が行うことと記述してあるのはこのためである。情報セキュリティ委員会によって検討された大枠的なリスク分析に加えて、外部公開サーバについてより詳細なリスク分析を検討し、セキュリティレベルの向上を図ることが趣旨である。

ポイント3　アクセス制御（サンプル4（1）節参照）

サンプルでは、外部公開サーバのアクセス制御について、以下の3つを規定している。

・ルータ及びファイアウォールなどによるアクセス制御
・OS、アプリケーション・サービスのアクセス制御
・データのアクセス制御

具体的な内容はサンプル「4（1）」を確認してほしい。そして、上記3つのアクセス制御について規定した文章のなかでも、特に最後の「変更履歴を含めて保管管理しなければならない。」という一文が重要である。

導入時のドキュメントは存在するが、その後の変更履歴がまったく残っていないという話をよく聞くことがある。アクセス制御については、スタンダードに規定するだけでは意味がない。規定された内容を維持、管理し、常に最新の状況を保持することが重要である。

また、アクセス制御だけではないが、変更を生じた際の承認の手続き方法を考えておくべきだ。実際の運用の立場で考えると、変更の手続きは簡単にしたいと考えがちである。よくある話だと思うが、上司が自分の便利のために、強引にセキュリティレベルを下げる変更を推し進めようとする場合を考えてみてほしい。もしもその際に、変更手続きが簡単であると、事あるごとにセキュリティレベルが低下してしまうことになりかねない。変更の手続きはそういった事態も想定し、検討していく必要があるだろう。

ポイント4　アプリケーション開発（サンプル4（1）節参照）

システム設計者は、CGI、APIなどのアプリケーション開発を行う際、リスク分析を実施し、仕様書の段階から、データの入力チェックなどの、セキュリティ対策の実施を行わなければならない。

サンプルでは、外部公開サーバ上で動作するアプリケーションについて、上記のように規定している。システム管理者は、常に最新のセキュリティ情報に注意を払わなければならない。特にバッファオーバーフロー攻撃のようなアプリケーションに依存した脆弱点については注意が必要である。

また、ツールなどにより、脆弱点の検査を行い、セキュリティ上、不備がないか確認を行うことも1つの手段である。

ポイント5　不正アクセス検知システムについて（サンプル4（1）節参照）

システム設計者は、IDSを設置する場合、設計時に以下の作業を行わなければならない。
・適用するシグネチャの選定及び必要なシグネチャの作成
・対応手順の必要なシグネチャの選定と、その対応手順書の作成

サンプルでは、上記のように規定している。このなかで記載してあるシグネチャの選定、作成においては、専門技術者に依頼するのも1つの方法である。

IDSの設置については、関心を持ち、導入を検討している方も多いだろう。だが、実際のネットワーク環境においては、製品費用、管理費用、技術的な面で導入されていない企業があるのではないだろうか。製品においては無償のものもあるが、それなりに設定・運用の技術が要求される。技術的な問題は、企業のセキュリティに割く費用が許せば専門技術者に依頼すればよい。導入にあたっては、やはり費用的な面が課題となるだろう。

ポイント6　管理体制及びシステム管理者の明確化（ポリシー・サンプル8.4（1）参照）

申請者は情報及び情報システムの正しく安全な運用を確実にするために、管理体制及びシステム管理者を明確にしなければならない。人的不注意および故意の誤用のリスクを低減するために、システム管理者及びオペレータを2名以上任命しなければならない。

外部公開サーバの管理体制について、サンプルでは複数のシステム管理者、オペレータを任命して運用することを規定している。人員は多ければ多いほどよいが、当然、人員が多ければ多いほど費用がかさむことになる。皆さんが作成するスタンダードでは、企業が現実に割ける費用に適した人員を記述するべきだ。

ポイント7　既存の外部公開サーバの申請について（サンプル4（2）節参照）

本標準が適用される以前の既存の外部公開サーバについては、3ヶ月以内に本標準に適合するようにしなければならない。3ヶ月以内に、本標準に適合しない場合、情報セキュリティ委員会は情報の公開を強制的に停止させることができる。

ここでは既存のサーバについての扱いについて記述している。ポリシーの制定以降は、新しく設置するサーバについては、ポリシーの規定を厳守してもらうことになるが、ポリシー制定以前に運用しているサーバへの適用には時間的猶予を与えるのが現実的である。そのようにすれば、既存のサーバが不適合になるからという理由だけで、本来のあるべき姿の代わりに、ポリシーの規定を甘くすることをなくすことができる。

ポイント8　検査実施手順（サンプル4（4）節参照）

外部公開サーバは、運用開始前に必ずシステム構築担当者が情

報セキュリティ委員会が指定する第三者による検査を受けなければならない。検査には以下の項目を含まなければならない。
・最新の脆弱性情報を含む検査項目
・「外部公開サーバ設置申請書」との整合性
・許可された範囲以外へのアクセスが出来ないこと
・アクセスコントロール定義の確認
・不要なサービス、不要なアカウントが存在しないこと
・推測可能なパスワードが設定されていないこと

サンプルでは、定期的な第三者の手による現在のセキュリティ状態の検査が必要であることを規定している。ここで重要なのは、検査を行う人間を、社員等ではなく第三者によるセキュリティ状態の検査まで求めるかどうかを決めることだ。

また、規定には記述されていないが、実際の検査を行う際は、セキュリティ診断ツールを用いて検査するのが一般的だろう。このような検査方法も記載しておくのがよいかもしれない。

なお、この規定の中では、検査を実施する間隔が明示されていないが、皆さんが作成するスタンダードでは明示すべきである。検査を実施する間隔については、それぞれの企業における考え方になるが、四半期または、半期に一度は検査を実施することが望ましい。

ポイント9 セキュリティレベルの維持（サンプル4(5)節参照）

システム管理者は、常に最新のセキュリティ情報を入手し、OS及びインストールされた、アプリケーション・サービスについて、随時、必要な最新のアプリケーションのバージョン、セキュリティパッチを適用しなければならない。また、これらの履歴は保管管理しなければならない。OS及びインストールされたアプリケーション・サービスに関するセキュリティホールのうち深刻なものであると判断され、かつセキュリティパッチが公開されていないものについては、別方法のセキュリティ対策の検討し、その施策を実施しなければならない。検討の結果、セキュリティ対策が無いと判断された場合は、速やかに情報セキュリティ委員会に報告し、情報の公開を停止しなければならない。この停止は、対応のセキュリティパッチの適用もしくは別の施策が実施にて、セキュリティ委員会に報告後、解除できる。

サンプルでは、常に最新のセキュリティ情報を入手し、常に最新のセキュリティパッチを適用するように規定している。

しかし、現実的には、セキュリティパッチを適用したことでアプリケーションの不具合が発生したという話をよく聞く。外部公開サーバにおいてこのようなトラブルが発生すると、セキュリティとは異なる観点で企業イメージを悪くしたり、信用を失墜させたりといったことも考えられる。

そのため現実的には難しい場合が多いかもしれないが、上記のようなトラブルが発生しないように、事前にテスト環境を用意し、テストを行い、正常に動作することを確認した後にセキュリティパッチを適用することが望ましい。そのテストのための時間と最新のセキュリティパッチを速やかに適用することのバランスを検討し、盛り込むことで、よりよいスタンダードになるだろう。

ポイント10 運用業務の委任（サンプル4(5)節参照）

システム管理者の運用業務はオペレータに委任することができるが、オペレータは運用手順書以外の操作を行ってはならない。

サンプルでは、上記のように規定している。ここでは運用業務をオペレータに委任しているが、現実的な問題として、オペレータは社員以外の外部委託業者の従業員を雇っている場合も多いのではないだろうか。この場合は、『第三者契約に対する標準』に準ずることを記述するべきだろう。

ポイント11 ログの保存、解析、時間の同期（サンプル4(5)節参照）

ログは、一時的にハードディスクなどの書き換え可能なメディアに保存されていても良いが、24時間以内に書き換え不能なメディアに転送され厳重に保管されなければならない。一時的にハードディスクなどの書き換え可能なメディアにログを記録する場合には、十分な記憶容量を確保しておき、異常な量の書き込みが発生した場合においても十分に対処できるように備えておかなければならない。ログは、その取得日から3年間は確実にシステムセキュリティ責任者のみが参照できる場所と方法で厳重に保管されなければならない。

サンプルでは、これらの項目に関しても規定している。そこで記述されている数値はあくまで目安であることに注意してほしい。ログの保存期間は長く、ログの保存を行う頻度は短く、ログ解析を行う間隔は短く、時間の同期の間隔は短くすればするほどセキュリティレベルがより強固になることは言うまでもないだろう。しかし、無理な規定をし、規定された内容を守れなくなってしまうようでは元も子もない。実際に作成する場合は、それぞれの企業に合わせた無理のない数値目標を記述していただきたい。

●その他、注意すべきポイント

ポリシー・サンプルは、あくまで架空の企業を想定したものであり、セキュリティを維持する費用などは、考慮されていない。よって、今回のサンプルが規定している基準を満たそうとした場合、それ相応の費用がかかることに注意してほしい。

また、情報セキュリティポリシーを作成することに精力を尽くし、維持していくことをおろそかにする企業が多いようだ。情報セキュリティポリシーを維持していくこと、つまり規定を守っていくのが重要であることを最後に述べておきたい。

（豊田）

次回は、スタンダード項目の2番目のグループとなる「クライアント対策なんてドンと来い集」について解説する。

個別の返答は必ずしもお約束できないが、連載内容に反映していきたいと考えているので、ご意見・ご感想等を電子メールでぜひお寄せいただきたい。

E- Mail：SECURITY- POLICY@yosihiro.com （佐藤）

セキュリティ対策講座③
サンプルを見ながら策定する
ドンと来い！ 情報セキュリティポリシー

第 4 回（全8回）

セキュリティ対策の「スタンダード（標準書）」を作る③
作成篇～クライアント対策なんてドンと来い

著者：NPO 日本ネットワークセキュリティ協会 理事 佐藤慶浩
富士通エフ・アイ・ピー株式会社 油井秀人
日新電機株式会社 井上大輔

スタンダードは、組織における情報セキュリティ対策の要件を具体的に規定するものであり、あらゆる組織で必要不可欠のものだ。その策定には多くの労力を要するが、JNSAのポリシー・サンプルをたたき台とすることで、それを軽減できるはずだ。
前回は、スタンダードのうち、サーバ対策に関連する部分について解説した。
今回は、クライアント対策に関するスタンダードについて、それらの構成と策定内容をJNSAのサンプルを用いて解説しよう。

本講座の読み方

まずは以下のWebサイトよりJNSAのポリシー・サンプルのファイルをダウンロードしてほしい。

http://www.jnsa.org/policy/guidance

今回は、次の4つのサンプルをダウンロードしてほしい。

『クライアント等におけるセキュリティ対策標準』
『ウイルス対策標準』
『電子メール対策標準』
『Webサービス利用標準』

これらを印刷して本書の横に並べて読んでいただきたい。本講座では、その一部を解説の必要に応じてJNSAの承諾を得て転載している。それぞれのファイルからの引用部分は、章や節の番号とともに以下のような囲み表示をしてある。

> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

このようなサンプル引用に解説を加えていくことで、自社に適したポリシーを策定するための手助けを行っていくことを目的としている。

⊗ クライアントPCを狙う攻撃の多様化に備えよう

前回は、サーバ対策に関する情報セキュリティポリシーのスタンダード作成について解説した。今回は、組織内部で利用されているすべてのクライアントPCに関するスタンダード作成のポイントについて解説する。

インターネットの利用は、ビジネスや組織の目的を果たすために不可欠となっている。半面、誰もが利用していることから、クライアントPCで利用する電子メールクライアントやWebブラウザを狙った攻撃が増えてきている。2001年には、「Aliz」「Nimda」「Badtrans」などが流行し、新聞やテレビで報道されたことも記憶に新しい。そして、Webブラウザをだまし、他のサイトのコードなどを実行させる「クロスサイトスクリプティング」。これは、一般ユーザにとっては防御のしようがない攻撃である。このように、今、クライアントPCが絶好のターゲットになっていることを十分に認識しなければならない。

ポリシー・サンプルでは、クライアント対策のスタンダードとして、『クライアント等におけるセキュリティ対策標準』を策定している。また、特に重要な、ウイルス、電子メール、Webブラウザの標準については別項に分け、その重要性を強調することとした。

以下、クライアント対策として重要な4つのスタンダードについて、それぞれ解説していこう。（井上）

JNSAの紹介

JNSAは2000年4月に設立され、2001年7月にNPO法人として活動を継承しました。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を、4つの部会と各WG（ワーキンググループ）に分かれて行っています。

昨年度の主な成果物としては、「外部接続に関するセキュリティポリシーサンプル冊子」の作成、「セキュリティインシデント被害調査」におけるアンケートの実施および報告書の作成などが挙げられます。

また、複数CAの相互運用性に関する実証実験を行った「Challenge PKI 2001プロジェクト」の結果報告も、Webにて公開中です。その他の活動として、年1回の主催カンファレンスの開催（NSF2002、今年は6月12-13日に開催）、セキュリティセミナーの開催、会報誌「JNSA Press」の発行（年3回）などを行っています。

＜お問い合わせ＞
特定非営利活動法人 日本ネットワークセキュリティ協会
URL：http://www.jnsa.org/
E-Mail：sec@jnsa.org

『クライアント等におけるセキュリティ対策標準』作成のポイント

ここでは、クライアントの物理的な管理や利用時の注意等を規定した『クライアント等におけるセキュリティ対策標準』作成時のポイントについて解説する。

●スタンダード策定が求められている背景

現在、多くの企業では1人1台のパソコンが支給されているだろう。あるいは、諸般の事情により、私物のノートパソコンなどを職場に持ち込んで作業している場合があるかもしれない。いずれの場合においても、企業の情報がパソコン内に格納されるため、そのパソコンそのものの管理が情報資産の管理ともいえる。パソコンの物理的な管理、利用時の注意、インストールされているソフトウェアの取り扱いなどについてのスタンダードを、早急に策定することが望まれる。

ポイント1 対象システム（サンプル3章参照）

当社より支給・貸与されたPC
※本標準内では、「PC」はノートパソコンを含んだクライアントマシンのことを指し、「ノートパソコン」は、ノートパソコンのみを指します。

サンプルでは対象を「ノートパソコンを含んだクライアントマシン」としている。しかし、最近ではPDAにもかなりの情報が格納されるようになっており、実際に業務で利用している例も見られる。そのような状況においては、PDAに関しても規定する必要があるだろう。

また、企業によっては、モバイルでの利用を前提とした機器の導入もあるだろう。その場合には、スタンダード全体にわたって、モバイルを意識した規定を検討しなければならない。

ポイント2 私物PCの使用禁止（サンプル4.1節参照）

（1）当社の業務において、従業員が使用できるPCは、当社が支給・貸与したPCのみとする。
（2）いかなる場合でも、当社システム環境に私物PCを接続・利用してはならない。

サンプルでは、企業が支給・貸与したPCとしているが、現実問題としては、派遣会社等の要員がPCを持ち込んでしまう場合があるだろう。こういったときの対応も検討しておく必要がある。また、私物PCであっても、たとえばウイルス対策ソフトが導入されており、最新のパターンファイルが格納されていることが確認できた場合など、一定の条件を満たせば接続・利用してよい、と規定してもよいだろう。

ポイント3 PCに導入するソフトウェア（サンプル4.2節参照）

（3）導入したソフトウェアは、常に最新の状態で使用することとし、情報システム部が提供するソフトウェア情報をもとに修正プログラム等を導入しなければならない。

サンプルでは上記のように規定しているが、このとおり、クライアントのソフトウェアを常に最新の状態に保つことは、現実的には困難だろう。情報システム部が提供する情報に緊急性をレベル分けし、そのレベルによって修正プログラムの適用を推奨するか、強制するといったように、対策の緊急度を分けた対応を検討するとよいだろう。

ポイント4 PCの他者への利用の制限（サンプル4.3節参照）

（1）席を離れる場合、第三者が無断でPCを利用できないようにPCにロックを掛けなければならない。

ここでは、スクリーンロックに関して規定している。他のスタンダード、たとえば、『Webサービス利用標準』でも、離席する際にはスクリーンロックすることを義務付けている。基本的には、『職場環境におけるセキュリティ標準』でこのことを記載しているので、そちらを参照するように規定したほうが改訂の際に手間がかからない。しかし、スタンダード同士の参照関係が多いと、理解に時間がかかることにもなる。各スタンダードを読んだ際にその場で理解できるように、個々に記載しておいてもよいだろう。

ポイント5 PCでの情報の取り扱い（サンプル4.4節参照）

（2）PCで一時的に機密情報を取り扱う場合、取り扱い後には、不必要となった情報を削除し、いつまでも保持してはならない。

サンプルでは、不必要になったものは削除するとしているが、削除する前にPCが故障するといったことも起こりうる。その場合、故障したPCであっても、データを削除するように徹底すべきである。また、他の媒体にコピーしてバックアップを行うこともあるが、それらも削除するかどうか検討する必要があるだろう。こういったことも考慮してスタンダードを作成すると、よりよいものになる。

ポイント6 PCの移設（サンプル4.6節参照）

（1）PCを利用するすべての従業員は、PCを勝手に移設してはならない。
（2）PCの移設が必要な場合には、情報システム部に申請し、許可を得なければならない。

移設の手順については、ポリシー・サンプルでは『LANに

おけるPC設置／変更／撤去の標準』に記載されている。ポリシー・サンプルのようにスタンダードを分けている場合は、そちらを参照する旨、記載しておいたほうがよいだろう。

ポイント7　ノートパソコンの利用上の注意事項（サンプル4.7節参照）

（1）社外にノートパソコンを持ち出す場合、盗難・窃盗に注意し取り扱わなければならない。
（2）社外でノートパソコンを利用する場合、情報の盗み見に注意し利用しなければならない。

PCの盗難は、現実的によくあることだ。したがって、実際に盗難や窃盗に遭った場合に、どのように対応するべきかについても規定しておくとよい。形式的には情報システム部に連絡することになるだろうが、その報告経路を明確にしておくことが重要である。

ノートパソコンであれば、社外で利用したり、自宅で利用したりすることもあるだろう。こういった場合の注意事項も記載したいものである。特にウイルスへの対策は、明記すべき事項である。

●その他、盛り込むべき内容

このサンプルの中では、PCは各自に配布されていることを想定している。これ以外にも、メールは利用できないが、Webブラウザだけは利用が許可されている場合など、複数の人が同一のPCを利用している環境もあるだろう。皆さんの環境で共用のPCがある場合は、その節を設けて記載するとよい。

『ウイルス対策標準』作成のポイント

ここでは、ウイルス対策を規定した『ウイルス対策標準』作成時のポイントについて解説していく。

●スタンダード策定が求められている背景

ウイルス対策の重要性については、いまさらいわずもがなだろう。このスタンダードでは、主にメールからのウイルス感染を規定している。最近では、ブラウザによるウイルス感染もあることから、httpやftpのファイル転送についても体系的に整理し、ウイルス対策を規定する必要があるだろう。

ポイント1　対象システム（サンプル3章参照）

サンプルでは、「PCおよびゲートウェイサーバ」といったようにクライアント側での対策とサーバ側での対策の両者を対象としている。だが、このことにより、記述内容が抽象的になっている部分がある。皆さんが作成するスタンダードでは、それらを分けて記載したほうがすっきりするだろう。その際、クライアントOSとして、ウイルスが発生しにくいLinuxを採用するといった規定も考えられる。コンテンツ作成には、Mac OSなどもあり得る。LinuxやMac OSは、企業のクライアントとしては多数を占めるものではなく、情報システム部門が対応できないため、導入を見合わせる場合があるかもしれない。しかし、脆弱性が少ないというメリットを生かして、これらの導入を検討してもよいだろう。

ポイント2　アンチウイルスソフトの導入（サンプル4.1節参照）

（3）選択するアンチウイルスソフトの要件には、以下の機能が含まれていなければならない。
・定義ファイルの自動更新機能（ベンダー→社内サーバ、社内サーバ→PC）
・常時スキャン機能（ファイルシステム、電子メール）

ここでは、アンチウイルスソフトの定義ファイルの自動更新機能について規定している。この機能において、ソフトウェアごとの更新方法の違いについては注意しなければならない。アンチウイルスソフトによっては、その定義ファイルを社内の決まったサーバからしか取得できないようになっているものもある。アンチウイルスソフトベンダー側のホームページでは最新のものがアナウンスされているにもかかわらず、それが取得できないというものだ。このようなときにどのような対策が取れるか機能的な調査をし、ソフトウェアに応じてその対応を規定に盛り込むことも必要になってくるだろう。

また、各サーバやPCにおいて、定義ファイルが常に最新であるかどうか確認できる機能も重要である。そのような機能をスタンダードに盛り込んでもよいだろう。

ポイント3　アンチウイルスソフトの利用（サンプル4.2節参照）

（3）対象者は、定義ファイルを毎日一度は更新するように設定しなければならない。

定義ファイルの更新は、最低でも1日1回は必要である。アンチウイルスソフトによっては、もっと短い間隔で自動更新可能なものもあるだろう。最近の新種ウイルス出現状況とその感染スピードにかんがみると、更新間隔を短く規定しておくべきである。

ポイント4　ウイルス／ワームに関する啓発教育の実施（サンプル4.5節参照）

（1）当社のPCを利用する場合には、はじめにウイルス／ワームに関する啓発セミナーを受講しなければならない。

「啓発セミナーは、『セキュリティ教育に関する標準』に則って受講する」などと、関連した標準を参照するようにしてもよいだろう。

ポイント5　情報システム部におけるウイルス対策窓口の設置（サンプル4.6節参照）

（2）ウイルス対策窓口は、社内のウイルス被害状況を掌握し、問題発生時の一次対応を実施する。

ここでも、『セキュリティインシデント報告・対応標準』を参照することと規定してもよいだろう。ただし、ウイルス発生時のように緊急を要する場合は、関連標準を参照している余裕はないだろうから、要点をここに記載しておくことをすすめる。

ポイント6　アンチウイルスソフトがウイルスを検知した場合（サンプル4.7節参照）

（1）対象者は、アンチウイルスの駆除機能を使用してウイルスを駆除しなければならない。

ここでは、ウイルス発見時には駆除することと規定している。ウイルス発見時の処置としては、駆除以外に感染ファイルそのものを削除する、感染ファイルはなんら操作せず別の場所に隔離する、といったものがある。自社の考え方により、どのように処置するかを決めるとよいだろう。また、情報システム部の中には、検出したウイルスを、デモやアンチウイルスソフトの評価用として保存しておきたい場合があるかもしれない。こういった場合は、例外条項に則って対応するのがよいだろう。

（3）ゲートウェイ上で検知した場合は同様に駆除し、情報システム部へ報告することはない。

ここで情報システム部門に報告する必要はない、としているのは、ゲートウェイでウイルスを検知した場合、自動的に情報システム部へウイルス検知が通知されることになっているからである。規定の記載方法としては、このような背景を記載すると理解されやすいものとなる。ただし、システム仕様の変更があった場合には、それに合わせて記述も変更しなければならないことは、記憶にとどめておく必要がある。

ポイント7　ウイルスに感染した場合（サンプル4.8節参照）

（2）連絡を受けたウイルス対策窓口は、PCからネットワークケーブルをはずすことを指示し、現場に急行しなければならない。

サンプルには上記のように規定されているが、この対応はいささか紋切り型といえよう。「PC」がクライアントであった場合は、ただちにケーブルから切り離すとしたほうがよい。でなければ、被害が拡大し、ウイルス対策窓口の負担が重くなる。しかし、サーバなどの場合は、予告なしにネットワークから切り離すと、編集中のファイルがなくなってしまうなどの二次災害を招く可能性がある。ウイルスに感染した機器により、その一次対応を分けることも重要である。

●その他、盛り込むべき内容

ウイルス対策としては、各クライアント側で完璧に対応していれば、特にゲートウェイ側の対応は不要かもしれない。しかし、クライアント側のPCの性能が格段によくなったとはいえ、システムの負荷を軽減するためにもゲートウェイ側で対応したほうがよいといわれている。逆に、ゲートウェイで対応していれば各PCでの対応は不要なのでは、といった意見もあるかもしれない。これらは、コストとのバランスであるとしかいえない。リスク分析に基づき対応するべきだろう。

企業によっては、侵入してくるウイルスはやむを得ないが、社外には絶対に出したくないし、社内感染とおぼしき通知のメールも出したくないといった要望もある。これらもコストとのバランスで検討するとよいだろう。

メールやブラウザ利用によるWebの閲覧は、業務になくてはならないものとなっており、その通信量は膨大なものになりつつある。安全性を求めてゲートウェイでのウイルス対策を検討した場合、サーバの二重化、負荷分散なども考慮する必要がある。これらも重要な要素であり、ポリシーとしてどこまで記載するか、JNSAポリシーWGでも議論が続いているところである。

（油井）

『電子メール対策標準』作成のポイント

ここでは、ユーザにおける電子メールの利用を規定した『電子メール対策標準』作成時のポイントについて解説する。

●スタンダード策定が求められている背景

電子メールの普及により、情報のやり取りが容易になった半面、機密データについても、故意や不注意、ウイルスを問わず、簡単に社外へ送信できるようになったことも忘れてはならない。電子メールソフトウェア自体の管理、電子メールの送受信時の注意などについても、スタンダードを策定しよう。

ポイント1　遵守事項全般（サンプル4章全般参照）

文章記載上の注意事項として、各文章には、「誰が」を規定した主語が必要である。主語がない場合、読み手に「自分はこの対象ではない」と勝手に判断されてしまう危険性がある。

ポイント2　電子メールサービス利用端末機器のセキュリティ（サンプル4.1節参照）

（1）電子メールの送受信にあたっては、情報セキュリティ委員会が指定した電子メールソフトウェアを用いなければならない。また、情報セキュリティ委員会の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。

使用する電子メールソフトウェアを指定することにより、セキ

ュリティホールなどの情報収集や、セキュリティパッチの適用、バージョンアップなどの手順書作成の手間を減らすことができる。管理するソフトウェアやOSはできる限り少なくし、セキュリティ情報の収集を実施することで、パッチ適用不備や設定不備による被害拡大を防止することが可能となる。これは、組織内で使用しているWebブラウザでも同様に実施しなければならないことである。

また、情報システム部として、情報収集、手順書の作成、連絡を実施し、ユーザにバージョンアップやパッチ適用義務を課すことにより、ユーザと情報システム部（組織の責任者）との責任範囲を明確にすることが可能となる。

（3）電子メールアドレスは初期パスワードとともに発行される。初期パスワードは直ちに変更しなければならない。また、パスワードは最低3ヶ月に一度、定期的に変更しなければならない。設定するパスワードは、『パスワードに関する標準』に則ったものとする。

組織の構成員のほぼ全員に配布される、電子メールアカウントおよびパスワードだが、配布方法や初期パスワードの選定、期限なども、スタンダード作成時に考慮してほしい。電子メールのパスワードは最も多くネットワークを流れるものであり、平文で流れるようなシステムを利用している場合には、他人にこのパスワードを見られる危険性が高い。そのため、システムによってはパスワードの有効期間を短くするなど、現状を考慮に入れた内容にする必要がある。

（4）電子メールソフトウェアの利用にあたっては、パスワードを保存してはならない。電子メールソフトウェア起動時にユーザ認証を必要とする設定にしなければならない。

サンプルでは、「パスワードを保存してはならない」ことを規定しているが、これだけでは何のパスワードなのか理解されない場合がある。電子メールソフトウェアのパスワードといっても、起動するためのパスワード、最初にサーバに接続して電子メールを読み出すためのパスワード、定期的に電子メールを読み出すためのパスワードなどがある。利便性を考えると、すべてのパスワードの保存を禁止することは、事実上できない可能性が高い。皆さんの作成するスタンダードでは、何のパスワードを保存してはいけないのかまで明確にしておくべきである。

ポイント3　電子メールで送受信される情報の保護（サンプル4.2節参照）

（1）当社の事業に関わる情報や、顧客、従業員のプライバシーに関わる情報などの機密情報は、原則として電子メールを用いて送信してはならない。

この部分は、電子メールでやり取りする内容について規定した文章となる。しかしながら、上記の内容では利用者が「何を」電子メールで送信してはいけないのかについての判断基準が具体的に分からないので、実際の利用者向けのガイドラインなどでは、「極秘情報」や「秘密情報」をあらかじめ定義した上で、「極秘情報は電子メールを用いて送信してはならない」であるとか、「秘密情報は社内の特定の電子メールアドレスにのみ送信可」などのように、情報の分類に基づいた記載を行う必要がある。

（2）業務上やむを得ず機密情報を送受信する場合は、情報セキュリティ委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

電子メールの暗号化については、送信内容が検閲できなくなるので、むやみに利用を許可せず、その利用を限定する必要がある。暗号化して電子メールを送信する場合には、電子メールのあて先に、必ず直属の上司や管理職を含め、上司に送信内容が分かるようにして送信するなどの対策を、並行して検討すべきである。これは、通常の電子メールの送信に関しても同様に実施すべきだ。

ポイント4　電子メールサービスとネットワーク保護（サンプル4.3節参照）

（4）電子メールの送信にあたっては、送信するメールサイズを考慮しなければならない。送信可能なメールサイズは、情報セキュリティ委員会にて規定された制限となっている。規定サイズ以上のメールを送信せざるを得ない場合は、分割送信することができる。分割送信時の分割サイズ、送信のタイミングを考慮するものとする。

最近では、ほとんどの組織が、電子メールの容量制限を実施している。ただし、分割してメールを送受信することは可能だ。この場合、電子メールサーバの保存容量はほぼ同じであるため、本来の容量制限の目的を満たしていないことになる。電子メールの容量を制限するなら、大きなファイルを添付する代わりにファイル交換をするためのファイルサーバを設置することを検討したほうがよいだろう。

●その他、盛り込むべき内容

電子メールに関連する、一般的ネチケットも記載しておいたほうがよいだろう。各人のネチケットが異なることは、大きなセキュリティホールになり得るからだ。

『Webサービス利用標準』作成のポイント

ここでは、ユーザにおけるWebブラウザの利用を規定した『Webサービス利用標準』作成時のポイントについて解説する。

●スタンダード策定が求められている背景

インターネットは豊富な情報源だが、組織の目的やビジネスにまったく関係のないサイトも多数存在する。業務に関係のないサイトの閲覧は、業務効率の低下だけでなく、ネットワーク負荷の増大や、ウイルスなどの業務停止をもたらすようなソフトウェア

をダウンロードする危険性も増えてくる。そこで、Webブラウザソフトウェアの管理、ホームページ閲覧時の注意などについてのスタンダードを策定しておこう。

ポイント1 業務目的以外の利用禁止（サンプル4.1節参照）

（2）対象者は、Webブラウザの利用にあたって、情報システム部が指定したWebブラウザの設定を施さなければならない。

Webブラウザ自体の設定は、セキュリティ対策上非常に重要だ。ActiveXやJava、JavaScript、VBScript、Cookieなど、セキュリティ対策上の脆弱点となりうる設定をできる限り使用できないようにすべきである（画面1）。業務上必要な場合には、そのサイトを「信頼するサイト」に登録するなどの処置を行えるように規定すべきだろう。

ポイント2 業務目的以外の利用禁止（サンプル4.2節参照）

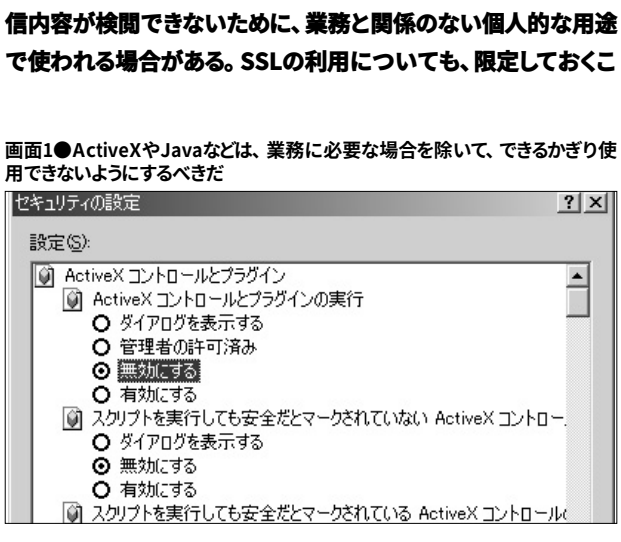
（1）対象者は、社内及びインターネット上のWebサーバへのアクセスは、業務上必要な場合のみ利用できる。

上記は私的Web閲覧の禁止を規定している文章だが、これだけでは抑止効果として足りない場合がある。「サンプル4.5節」などの、アクセスログを監視していることの明示や罰則、そして、技術的にURLフィルタなどを併用し、危険なサイトや有害サイトの閲覧を防止していくのが効果的だ。

（5）対象者は、原則として、SSL（Secure Sockets Layer）などの暗号通信を行ってはならない。但し、特に部門長の申請により、情報セキュリティ委員会が承認した場合においてSSLの通信を行うことができる。この場合、利用者は、利用目的、対象サーバ、利用機関を明確にし、情報セキュリティ委員会に報告しなければならない。

途中経路での情報漏えいの危険性が少ないことから、パスワードを入力させるサイトなどでSSLが使われている。同時に、通信内容が検閲できないために、業務と関係のない個人的な用途で使われる場合がある。SSLの利用についても、限定しておくことが望ましい。

画面1●ActiveXやJavaなどは、業務に必要な場合を除いて、できるかぎり使用できないようにするべきだ



（6）対象者は、インターネット上のWebサーバを利用した電子メールの送受信を行ってはならない。

Webサーバを利用した電子メールの送受信（以下Webメールという）についても規定しておく必要がある。このWebメールは、社内の情報漏えいを考慮すると無視できない存在だ。検閲も難しいので、業務上使う場合がないときには禁止したほうがよいだろう。

ポイント3 アクセス制御されたWebサイトの閲覧に関して（サンプル4.4節参照）

（3）対象者は、パスワードによってアクセス制御されたWebサイトの閲覧において、他人のユーザIDやパスワードなどを利用してアクセスしてはならない。

これは、「不正アクセス禁止法（http://www.ipa.go.jp/security/ciadr/law199908.html）」に対応する規定である。部外者からの攻撃だけでなく、社内から犯罪者を出さないようにするための内容を盛り込んでいくことも重要である。

●その他、盛り込むべき内容

Cookieは、Webブラウザ使用時にユーザの意識なしで情報のやり取りを行っている。一般的なユーザにとっては、その存在や脆弱性を意識することは難しいため、なんらかの規定を設けておくのがよいだろう。ただし、Cookieをすべて禁止すると、業務上非効率になることが多い。しかしながら、一般的ユーザに、Cookieの内容をすべて見た上で利用を判断させるのは、さらに非効率かつ実質的に不可能である。このあたりを含めて、Webブラウザの設定方法、インターネットの利用方法、インターネットの歩き方などをセキュリティ教育に盛り込んでおいていただきたい。

クライアントPCを使用するのは、情報セキュリティ委員会や情報システム部といった、ある程度情報セキュリティの知識を保有している人たちではないことを考慮しなければならない。情報セキュリティポリシーを実行できるような環境、教育、手順書を整備しなければならないことは、いうまでもないだろう。また、遵守事項を分かりやすくまとめたガイドラインを、小冊子もしくは社内Webなどに公開しておき、ユーザがいつでも参照できるようにしておくとよいだろう。（井上）

次回は、スタンダード項目の3番目のグループとなる「ネットワーク対策なんてドンと来い集」について解説する。

個別の返答は必ずしもお約束できないが、連載内容に反映していきたいと考えているので、ご意見・ご感想等を電子メールでぜひお寄せいただきたい。

E-Mail：SECURITY-POLICY@yosihiro.com

セキュリティ対策講座③
サンプルを見ながら策定する
ドンと来い！情報セキュリティポリシー

第 5 回（全8回）

セキュリティ対策の「スタンダード（標準書）」を作る④
作成篇～ネットワーク対策なんてドンと来い

スタンダードは、組織における情報セキュリティ対策の要件を具体的に規定するものであり、あらゆる組織で必要不可欠のものだ。その策定には多くの労力を要するが、JNSAのポリシー・サンプルをたたき台とすることで、それを軽減できるはずだ。前回は、スタンダードのうち、クライアント対策に関連する部分について解説した。今回は、ネットワーク対策に関するスタンダードについて、それらの構成と策定内容をJNSAのサンプルを用いて解説しよう。

著者：NPO 日本ネットワークセキュリティ協会 理事 佐藤慶浩
日本アイ・ビー・エム システムズ・エンジニアリング株式会社 大津留 史郎
新日鉄ソリューションズ株式会社 吉村公宏

本講座の読み方

まずは以下のWeb サイトよりJNSAのポリシー・サンプルのファイルをダウンロードしてほしい。
http://www.jnsa.org/policy/guidance

今回は、次の4つのサンプルをダウンロードしてほしい。
『ネットワーク構築標準』
『LANにおけるPC（サーバ、クライアント等）設置/変更/撤去の標準』
『リモートアクセスサービス利用標準』
『専用線及びVPNに関する標準』

これらを印刷して本書の横に並べて読んでいただきたい。本講座では、その一部を解説の必要に応じてJNSAの承諾を得て転載している。それぞれのファイルからの引用部分は、章や節の番号とともに以下のような囲み表示をしてある。

> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

このようなサンプル引用に解説を加えていくことで、自社に適したポリシーを策定するための手助けを行っていくことを目的としている。

今回の構成だが、まず、ネットワーク対策に関するスタンダードの基本である、『ネットワーク構築標準』を大津留氏に解説していただく。この標準は、第3回で解説した『ユーザ認証標準』と『アカウント管理標準』のスタンダードを前提にしているので、それらを参照しながら内容の確認をしていただきたい。次に、『LANにおけるPC設置/変更/撤去の標準』と『リモートアクセスサービス利用標準』を吉村氏に解説していただく。

『専用線及びVPNに関する標準』については、一般的な事項を書いてあるので、本講座では特に解説を行わない。読者はポリシー・サンプルをダウンロードして、各自で内容を確認していただきたい。

今回もこれまで同様に、連載の第1回で紹介したモデル企業を想定したポリシー・サンプルの解説となる。そのため、解説のなかで「企業」や「会社」などと表現するが、内容的には非営利などの組織であっても同様なので、読者の方には随時読み替えていただきたい。（佐藤）

『ネットワーク構築標準』作成のポイント

ここでは、情報システムのネットワーク構築について規定した『ネットワーク構築標準』作成時のポイントについて解説する。

JNSAの紹介

JNSAは2000年4月に設立され、2001年7月にNPO法人として活動を継承しました。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を、4つの部会と各WG（ワーキンググループ）に分かれて行っています。

昨年度の主な成果物としては、「外部接続に関するセキュリティポリシーサンプル冊子」の作成、「セキュリティインシデント被害調査」におけるアンケートの実施および報告書の作成などが挙げられます。

また、複数CAの相互運用性に関する実証実験を行った「Challenge PKI 2001プロジェクト」の結果報告も、Webにて公開中です。その他の活動として、年1回の本格カンファレンスの開催（NSF2002、今年は6月12-13日に開催）、セキュリティセミナーの開催、会報誌「JNSA Press」の発行（年3回）などを行っています。

<お問い合わせ>
特定非営利活動法人 日本ネットワークセキュリティ協会
URL：http://www.jnsa.org/
E-Mail：sec@jnsa.org

ポイント1　インターネット接続環境について（サンプル4.1節参照）

(3)インターネット接続環境に接続する機器は、ルーター、スイッチングハブ、UNIX系サーバとする(Windows系サーバについては、アプリケーションを利用するため必要な場合に接続をすることができる)。

サンプルではWindows系のサーバはなるべく使用しない旨の記述をしているが、これはWindowsサーバに関するセキュリティホールが数多く見つかってきた過去の経緯を踏まえてのことだ。最新の修正パッチが適用され、かつ十分なセキュリティ対策が施されたWindowsサーバであれば、十分インターネット接続環境で使用することができるだろう。

また、外部公開サーバで使用するOSやソフトウェアについては、本来「外部公開サーバに関する標準」で記述すべき内容だが、関連する内容で特に注意すべきものについては、特記事項としてこのように記述してもよいだろう。

ポイント2　ネットワーク接続構成について（サンプル4.2節参照）

・プロバイダと当社の境界には、ファイアウォールサーバを設置し、不正アクセスの対策を実施しなければならない。
・ファイアウォールサーバには、DMZを用意しインターネットサーバを利用できるようにしなければならない。

ファイアウォールとDMZの構成方法として、1つのファイアウォールがインターネット、DMZ、イントラネットすべてに接続される構成（図1、簡易構成と呼ぶ）と、多段ファイアウォール構成（図2）とがある。

簡易構成はコストが安くて済むが、万一ファイアウォールに侵入されたり、ファイアウォールのトラフィック制御を無効にされたりした場合、即座にイントラネットにも侵入されてしまうといったセキュリティ上のリスクがある。

これに対して多段ファイアウォール構成は、コストがかかる半面、1つのファイアウォールが無効になってDMZへの侵入を許してしまったとしても、即座にイントラネットへの侵入につながる事態を防ぐことができる。ただし、そのためには2つのファイアウォールが別の製品である必要がある。同一のファイアウォール製品を使用した場合、攻撃者は1つの攻撃方法を見つけさえすればよく、それを繰り返すことで容易にイントラネットまで侵入できてしまうからだ。

大規模なサイトでは多段ファイアウォールの考え方を拡張し、図3のようにさらにゾーンを増やして、サーバに保存するデータの重要度に応じて配置するゾーンを変える設計を行うことが多い。この場合、システムが扱うデータ（情報資産）を洗い出して、データを重要度に応じて分類し、それぞれの重要度ごとに配置するゾーンを変えた設計を行うといったステップを踏むことが重要である。実は、ポリシー・サンプルには情報資産の重要度に応じた分類の章がない。本来であれば、真っ先に情報資産の洗い出しと分類を行うべきである。

ゾーン分けと各ゾーンへのサーバやデータの配置については、多くの設計者が頭を悩ませる問題だろう。現在では、インターネットに一番近いDMZには、Proxyサーバやメールゲートウェイといった、コンテンツをまったく持たない代理サーバのみを配置し、実際にコンテンツを持つWebサーバやMailサーバはその1つ内側のゾーンに、より機密性の高いデータについてはさらにその内側のゾーンに配置して強力な認証で保護するといった設計が行われている。

また、ネットワークをWeb、Mail、DNSのサービスごとに物理

図1■簡易構成

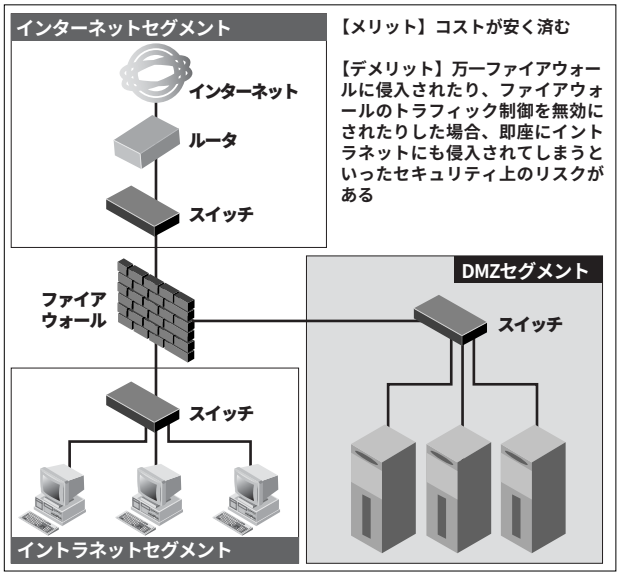
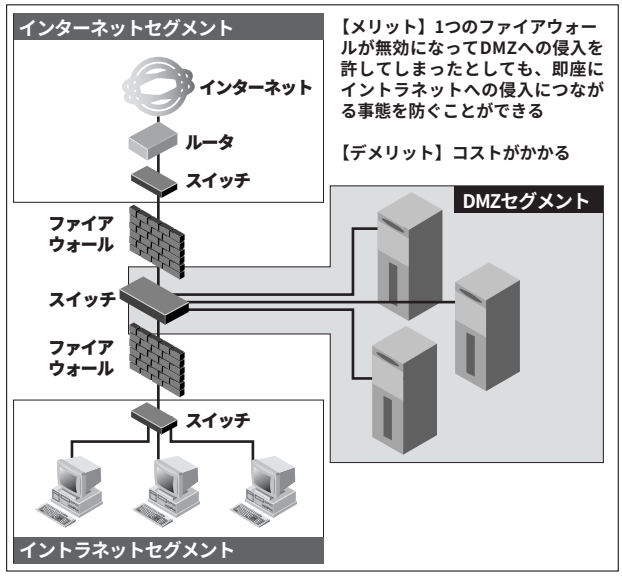


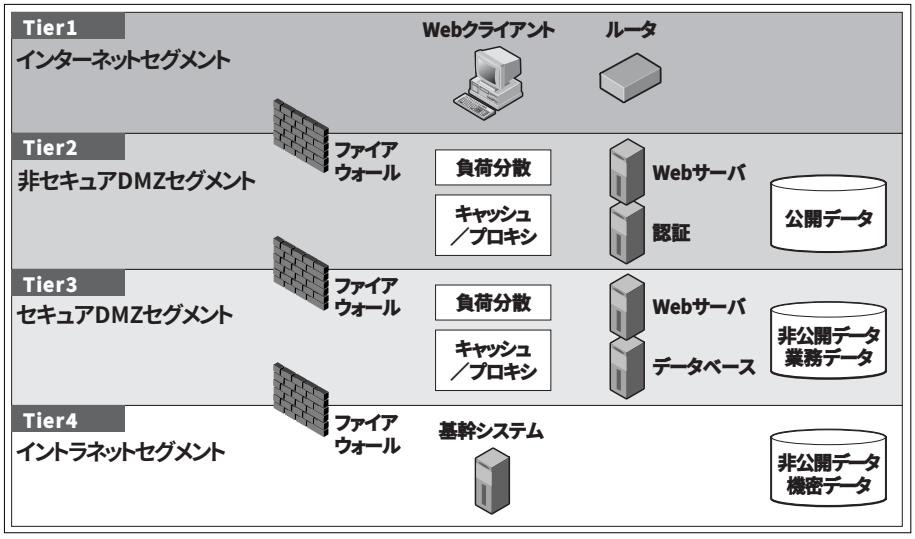
図2■多段ファイアウォール構成



的に分けるといった方法も取られている。これには2つの目的がある。1つは一斉配信メールなど、特定のサービスのトラフィックが集中する時間帯が存在する場合に、他のサービスに与える影響を回避するためだ。これはセキュリティというよりパフォーマンスの目的のように見えるが、ビジネスの継続性という観点ではセキュリティに含まれるものである。

もう1つは、万一特定のサーバに侵入されてしまった場合、そこを踏み台として、さらに他のサーバに侵入されることを防ぐためである。Mailサーバに広く使われているSendmail、DNSサーバに広く使われているBIND、Webサーバに広く使われているApacheといったソフトウェアはオープンソースのソフトウェアであり、セキュリティホールがたびたび見つかっている。こういったセキュリティホールを悪用してサーバに侵入するツールもインターネット上で出回っており、これからもセキュリティホールが見つかる可能性が比較的大きいと考えておいたほうがよい。そして、万一サーバに侵入されてしまった場合でも、そこからさらに他のサーバに侵入されることがないようにネットワークを物理的に分離してしまうというのも、有効なセキュリティ対策の1つである。

図3■拡張多段ファイアウォール構成



実際のサイトでどこまでやるべきかについては、データを保護するためにどこまでコストをかけられるか（どこまで厳重に守るべきデータであるか）に依存する。ポリシー・サンプルではシステムとして中規模のものを想定しており、コストのかからない簡単な構成を取っている。

また、連載第1回で紹介したモデル企業のシステム構成はネットワークやサーバの障害対策やインターネットと接続する回線の帯域制御について考慮したものではなく、コンポーネント（例えばファイアウォール）の障害や一時的なリクエストの集中がサイトの全面ダウンにつながる可能性がある。この点についてもリスクとコストのバランスを取りながら必要な障害対策を講じておく必要があるだろう。ビジネスに必要なサービスの継続性もセキュリティの重要な一要素である。

ポイント3　インターネットに公開するサービスについて（サンプル4.2節参照）

（2）利用できるサービス
・ファイル転送サービス
・時刻同期サービス

ご存じの読者も多いと思うが、FTPは通信内容が平文で流れるため、盗聴により、アクセスに必要なユーザIDやパスワードなどのアカウント情報が盗まれやすい通信である。アカウントが盗まれた場合のサーバへの影響を少なくするために、FTPサーバの設定により、インターネットからはファイルをダウンロード（GET）するだけでアップロード（PUT）はできないようにするといった対策を施す必要があるだろう。さらに、アカウント情報を盗まれないように、ワンタイムパスワードを使用したり、接続するユーザが限定される場合はSSHで代替して認証・暗号化を行うといった対策も検討すべきである。

また、NTPもセキュリティ上のリスクがある通信である。NTPは大雑把に言えばインターネット上のサーバに標準時刻を教えてもらうサービスだが、サーバから送られる（標準時刻の含まれた）パケットを偽造してクライアントに送り込んでしまえば、クライアントマシンの時刻を簡単に狂わせることができてしまう。NTPを各サーバのログの時刻合わせに使っている程度であれば影響はさほど大きくないだろうが、NTPで取得した標準時刻をDBサーバにも反映させ、アプリケーションの処理が時刻に依存するものであったとしたら、影響は甚大なものとなってしまう。このようなケースでは、サーバに接続可能なFMラジオ電波やGPSの標準時刻受信機、NTPサーバ機といったものが市販されているので、これを使ってサイト内に閉じたNTPのクライアント・サーバ構成を組むなどの対策が必要になるだろう。

ポイント4　無線LANについて（サンプル4.3節参照）

・スイッチングハブ（レイヤ3、レイヤ2）とハブを使用し、ビル内のネットワークとする。

ポリシー・サンプルを作成したのは昨年であり、その時点では無線LANを社内ネットワークに使用することは想定していなかった。そのため、ポリシー・サンプルには無線LANに関する記述がないが、現在では無線LANのセキュリティは業界の重要課題となっており、導入とポリシーへの記載に際しては注意深い検討が

必要である。

無線LANによく使われているWEPという暗号化プロトコルは、現在では解読方法が見つけられており、暗号解読を行うツールまで出回っている。米国では攻撃者が企業ビルの側道に車を止めて、車内からノートPCで企業の無線LANに侵入するという事件が実際に発生している。

このようなセキュリティリスクに対する対策として、WEP以外の暗号化が行われている無線LAN機器を使う、アプリケーションレベルで暗号化を行う、無線LANにはMACアドレス固定で登録制にするといった対策を検討する必要がある。

さらに、無線LANは妨害電波にも弱いといった側面があるため、半径4m以内に複数のアンテナを立てないといった規定の検討も必要だろう。

また、場合によっては、重要なデータが流れるLANは一般の社内LANと分離して無線LANは使わないといった対策も必要になるかもしれない。

ポイント5　ADSLについて（サンプル4.3節参照）

- ルーターによる専用回線接続とし、接続先は社内拠点（支店、営業所）及び子会社・関連会社とする。
- 専用線接続が困難な場合においては、情報セキュリティ委員会が認めた場合のみVPN装置を利用したインターネット接続を認める。

ADSLについても、ポリシー・サンプル作成時は現在ほど一般に広まっていなかったため、WANの1つとして想定していなかった。ADSLはインターネットに対する常時接続となるため、ポリシー・サンプルのインターネット接続に該当し、VPN装置を使ったユーザ認証・暗号化やファイアウォールの設置といった対策を検討する必要がある。ADSLによるインターネット接続に使われるADSLルータは、ほとんどが簡単なファイアウォール機能を持っている。ここで、ファイアウォールとしてADSLルータの持つ簡単な機能で十分とするのか、専用のファイアウォールを配置する必要があるのかといった考慮も必要だろう。

ポイント6　アドレス体系について（サンプル4.2節、4.3節参照）

- ルーターによるインターネットプロバイダ接続とし、プロバイダ側のネットワークはグローバルアドレスを利用しなければならない。
- 使用するアドレスは、プライベートアドレスを利用すること。
- ファイアウォールサーバでは、グローバルアドレスとプライベートアドレスの変換を行うことが望ましい。

アドレスの割り振りについてはネットワーク設計の範疇であり、セキュリティの範囲ではないように思えるが、どの機器がグローバルアドレスを持つかという点についてはセキュリティと密接に関係がある。

グローバルアドレスはインターネットと直接通信するためのアドレスであり、逆に言えば、グローバルアドレスが割り振られた機器はインターネットにサービスを公開していなくても意図に反してアクセスされてしまう可能性がある。したがって、グローバルアドレスを割り当てる必要のある機器について明確に規定し、それらの機器をいかにして保護するかを検討しておかなければならない。また、グローバルアドレスとプライベートアドレスをどこで変換するかについても明確化しておく必要があるだろう。ポリシー・サンプルではファイアウォールでのアドレス変換を望ましいものとして記述しているが、ファイアウォールでのアドレス変換を完全にルール化して「しなければならない」と記述してもよいし、アドレス変換をファイアウォールではなくルータで行うこととしてもよいだろう。

●その他、盛り込むべき内容

ポリシー・サンプルには記述されていないが、ルータやスイッチングハブ、負荷分散装置といったネットワーク機器のハードニング（セキュリティを強化すること）についても、サーバのハードニングと同様に考慮が必要である。これは、現在出荷されているネットワーク機器では、運用・管理を容易にするためにWebやファイル転送（ftp、tftp）のサーバや、セキュリティ上のリスクとなり得るfingerやproxy-arp、ソースルーティングといったサービスが初期設定の状態で立ち上がっていたりするためだ。ftpの通信がユーザIDやパスワードを平文で流すという危険性はポイント2のところで述べたとおりだ。また、tftpはサーバへのリクエストをブロードキャストで探索するため、偽の応答を返すことによって簡単にサーバになりすますことができ、偽のtftpサーバから偽造した構成ファイルをネットワーク機器にダウンロードさせることができてしまう。また、fingerが有効になっている場合、“ finger @ホスト名 ”または“ finger @IPアドレス ”というコマンドによって、リモートから対象ホストのアカウント名を得ることができてしまう。Proxy-arpはルータを越えて接続されているホストへのARP要求にルータが代理で応答する機能だが、この機能は悪用されれば攻撃者がルータの向こうに接続されているホストのIPアドレスを知ることに使われてしまう。

このように、サーバだけでなくネットワーク機器に対してもハードニングを行うということは非常に重要な考慮点である。具体的な内容については各ネットワーク機器メーカーのホームページなどでガイドが提供されているので、そちらを参照していただきたい。

また、一般的にはネットワーク上の盗聴対策としてスイッチングハブの導入が有効とされているが、スイッチングハブに接続されているホストに偽造したARP応答を送りつけ、デフォルトゲートウェイのIPアドレスに対応するMACアドレスをハッカーのホストのMACアドレスに書き換える「ARP Spoofing」という方法がある。スイッチングハブの導入が必ずしも十分な盗聴対策ではないことについても注意してほしい。

また、6.4.1の全般規定では、ネットワーク機器やネットワークに接続できる機器についての記述と、それらの設定についての記述が混在している。そのため、皆さんがポリシーを作成する際

には、項目を分けて記述したほうが分かりやすいものになるかもしれない。（大津留）

『LANにおけるPC（サーバ、クライアント等）設置／変更／撤去の標準』作成のポイント

ここからは、社内のLAN環境に接続する端末について規定した『LANにおけるPC（サーバ、クライアント等）設置/変更/撤去の標準』作成時のポイントについて取り上げる。ポリシー・サンプルでのモデル環境の条件から記述を省いた部分や、スタンダード検討時に考慮すべき点を中心に、ポリシー・サンプルから抜粋して解説する。

ポイント1　LANに接続する機材について（サンプル4.1節参照）

（1）LANに接続するPCは、『ソフトウェア／ハードウェアの購入及び導入標準』に基づいて導入されたものに限る。利用者は個人所有の機材を利用してLANに接続してはならない。

今回のポリシー・サンプルでは、個人所有の機材の扱いに関して、『PC等におけるセキュリティ対策標準』に準じた形として、社内のLAN環境への接続を認めないこととした。しかし実際には、自社・協力・派遣会社社員の個人所有PCを接続させていることも多いだろう。

また、個人資産の業務利用ではなくとも、会社からノートPCを支給するなど、会社資産を貸与している場合において、そのPCを自宅あるいは出先といった、会社の物理的な管理範囲外のネットワークに接続する利用形態が想定されるケースも多い。いったん自社管理管轄外のネットワークに接続したPCには、ウイルス感染やトロイの木馬の持ち込み等、リスクが発生する。このような場合も含め、社内LANへの接続にあたっては、セキュリティ面での影響を考慮して、慎重に検討すべきである。

個人所有PCのLAN接続を検討する場合、あるいは上述したように、社外ネットワークに接続する（可能性のある）機器を社内でも利用しなければならない場合においては、例えば次のような施策が考えられる。

まずは社内LANへの接続前に必ず所定のセキュリティ検査を実施し、持ち込み時の水際検査でセキュリティを提供する方法が挙げられる。しかしこの場合、検査の実施方法にもよるが、検査のためにかかる人手や手間、時間のロスを十分認識しておく必要がある。

次に社外ネットワークにおいてウイルス等に感染しない仕組みを提供する、といった方向で検討してみると、個人所有・会社資産を問わず、LANに接続するすべてのクライアントに対して各種のセキュリティ対策製品を導入するという方法がある。現在市場には、クライアントに導入するウイルスチェッカや、パーソナルファイアウォールと呼ばれるクライアントに対するアクセス制御を提供するソフトウェア、またそこにIDS（侵入検知）の仕組みを組み合わせた製品も存在している。製品の選択肢も多いため、投資コストに見合った現実的な選択が可能かもしれない。ただしこの場合には、各クライアントにセキュリティ製品を導入するコストを見積もること以外にも、留意すべき点が発生する。

それは、せっかく導入したセキュリティ製品であっても、例えばクライアント側で設定を停止の状態に勝手に変更されてしまうと、当然ながら目的どおりに機能しないということである。ソフトウェアの停止は極端な例かもしれないが、バージョンアップやパターンファイルのアップデート等が適切になされているか、あるいは不要な（許可していない）ソフトウェアを導入していないか、といったクライアント側の状態管理（およびその維持にかかるコスト）までを意識する必要があるだろう。

なお、こうしたクライアント側の状態を管理するための製品として、各クライアント上のファイルシステムにおいてファイルアクセスを監視し、それが許可され得るべきものかどうかをチェックする仕組みを提供するものが見受けられる。

また、別の手法として、クライアントに対して、ある一定のセキュリティレベル（例えばウイルスパターンファイルの新しさや、OS・Webブラウザに適用されているパッチレベルを条件とする）を要求し、その条件を満たした場合にのみ、社内LANあるいは特定のリソースへアクセスできる仕組みを提供するセキュリティ製品も見受けられる。自社の方針に合わせて検討してほしい。

ポイント2　LAN接続における留意点について（サンプル4.2節参照）

（1）利用者は、情報システム部が設置している以外のHUB・Router・モデム等を導入してネットワーク形態を変更してはならない。また、それらを利用して他のネットワークに接続してはならない。

利用者の勝手な判断により、結果としてセキュリティレベルを下げてしまうような行為をコントロールするのは難しい。ポリシーの規定と同時に、社内LANのネットワークトポロジーを検出するツールの利用やDHCPのリースログなどからネットワークの利用実態を検査して情報収集に努めることや、ネットワークあるいはサービス利用にあたって認証を要求するといった、不正なネットワーク利用に対して警告を発する素地を作ることを検討したい。

また、社内LANの中に、より高いセキュリティレベルを必要とするセグメントが存在する場合には、例えばパケットレベルで通信を確認し、想定外の（許可されていない）機器との通信が発生していないかどうかを監視する仕組みが必要になるかもしれない。

（2）利用者は、変更申請無しに使用機材の機能を変更、あるいは機能の追加を行ってはならない。また、許可されている目的外でLANを利用してはならない。

ここでは社内LANの利用目的そのものに関しては触れていな

いが、『社内ネットワーク利用標準』を踏まえて確認しておきたい。また次の7.4.2（4）で触れているように、必要に応じて、管理者が社内LANを流れる通信が適切かどうかを判断する仕組みの導入も検討対象になるだろう。仮に利用するサービスが規定されているWebサービスのみで目的範囲内に見えていたとしても、例えば業務外目的のWebサーフィンなど、より深いレベルでのチェックを行わなければ確認できないケースも考えられることを意識しておきたい。

（4）情報システム部は、利用者の接続形態にあわせ、適切な認証機能・暗号化機能等を提供し、情報の保護に努めなければならない。
- 無線LANを利用する場合には、認証および暗号化機能を利用すること
- SwitchingHUB等を利用して、利用者間でのパケットキャプチャができない仕組みを用いること
- LANに接続する機器の通信は、『社内ネットワーク利用標準』に照らして適切な通信のみに限定すること
- リモートアクセスについては、『リモートアクセスサービス利用標準』に照らして適切な通信のみに限定すること
- 各サーバへのアクセス状況については、『監視に関する標準』に基づいて対処すること

この項では情報の保護を意識しつつ、情報システム部で果たすべき事柄に関してごく簡単に、大まかなところを整理するにとどめた。皆さんの環境で検討を加える際には、社内LANの利用形態やその接続形態を意識してポリシーを作成する必要があるが、セキュリティ技術そのものが日々新しくなるなかでは（セキュリティ侵害の技術も日進月歩だが）、細部にわたっての仕組みを特定した記述とすることは難しいかもしれない。

しかしそれでも、社内LANに接続する利用者すべてが、不用意に他人の情報を入手し得る環境に置かれないようにするという、一種の予防的側面から記述できることがないか、検討を重ねることをお勧めしたい。

なお、ポリシー・サンプルの作成時には、以下に示すとおり、簡単な実装例を想定していた。

1つは、DHCPによるアドレスリースにおいて認証を組み合わせる方式である。例えば社外からの来訪者がDHCP環境において情報コンセントに勝手に接続しても情報を与えない仕組み、あるいは部署・職種によってアクセスできる情報レベルが異なっている場合に適切な処理を提供する仕組みを想定していた。

またもう1つの例は、スイッチのVLAN設定と認証機能の組み合わせになる。MACアドレスレベルでアクセス可能なセグメントをコントロールすることができるため、導入可能な環境であれば効果は高いかもしれない。ただし、これらの想定時には、例えば1つのPCを複数のフロアで利用したいというニーズに応えられるか、または同じPCを複数で利用している場合にはどうするかといった、より具体的なところまで踏み込んだ検討までには至らなかった。皆さんが行うポリシー作成においては、それらも検討課題に含めることをお勧めしたい。

『リモートアクセスサービス利用標準』作成のポイント

最後に、リモートアクセスによる社内ネットワーク利用について規定した『リモートアクセスサービス利用標準』作成時のポイントを解説する。

ポイント1 リモートアクセス時に利用できるリソースに関して（サンプル4.5節参照）

（3）リモートアクセスでは、社内に設置されたサーバのみにアクセスすることができる。ただし、申請により許可された社員についてはインターネットへアクセスすることもできる。

自宅からのインターネットアクセスの低価格化、高速化が容易に実現できるようになった現在では、ダイヤルアップによる社内LAN接続を経由して、そこからインターネットへのアクセスを行うことはあまりないかもしれない。ここでは明示的に申請行為を挟むことで、利用者によるリモートアクセス回線、および企業のインターネットアクセス回線（帯域）の無駄遣いを抑止する意味合いも込めて記述している。

ポイント2 リモートアクセス時における検査と監視に関して（サンプル4.9節参照）

・情報システム部は、定期的（年4回）にダイヤルアップルータおよびサーバ、モデムなどによる社内ネットワークへの接続環境が不正に用意されていないか検査しなければならない。

利用者判断での勝手な機器追加については、すでに『LANにおけるPC（サーバ、クライアント等）設置/変更/撤去の標準』の7.4.2（1）への解説でも触れた。利用実態の情報収集といった、仕組みでの対応を検討することと併せて、場合によっては罰則規定と絡めながら、望ましくないネットワーク環境とならないように利用者のセキュリティ意識を高める活動も重要な施策となる。

今回の内容として取り上げたポリシー・サンプルの範囲では、実際の運用にあたって管理者側で留意すべき問題点のほかに、利用者側のセキュリティ意識に依存しがちな部分も多い。ユーザへの啓発活動や教育といった継続的な取り組みについても、ぜひ検討していただきたい。（吉村）

次回は、スタンダード項目の4番目のグループとなる「物理的な対策なんてドンと来い集」について解説する。

個別の返答は必ずしもお約束できないが、連載内容に反映していきたいと考えているので、ご意見・ご感想等を電子メールでぜひお寄せいただきたい。（佐藤）

E-Mail：SECURITY-POLICY@yosihiro.com

セキュリティ対策講座③
サンプルを見ながら策定する
ドンと来い！ 情報セキュリティポリシー

第 6 回（全8回）

セキュリティ対策の「スタンダード（標準書）」を作る⑤
作成篇～物理的な対策なんてドンと来い

著者：NPO 日本ネットワークセキュリティ協会 理事 佐藤慶浩
日立ソフトウェアエンジニアリング株式会社 岡本一弘

スタンダードは、組織における情報セキュリティ対策の要件を具体的に規定するものであり、あらゆる組織で必要不可欠のものだ。その策定には多くの労力を要するが、JNSAのポリシー・サンプルをたたき台とすることで、それを軽減できるはずだ。
前回は、スタンダードのうち、ネットワーク対策に関連する部分について解説した。
今回は、物理的な対策に関するスタンダードについて、それらの構成と策定内容をJNSAのサンプルを用いて解説しよう。

本講座の読み方

まずは以下のWebサイトよりJNSAのポリシー・サンプルのファイルをダウンロードしてほしい。

http://www.jnsa.org/policy/guidance

今回は、次の4つのサンプルをダウンロードしておくとよい。

『物理的対策標準』
『サーバルームに関する標準』
『職場環境におけるセキュリティ標準』
『媒体の取り扱いに関する標準』

これらを印刷して、本書の横に並べて読んでいただきたい。

本講座では、その一部を解説の必要に応じてJNSAの承諾を得て転載している。それぞれのファイルからの引用部分は、章や節の番号とともに以下のような囲み表示をしてある。

> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

このようなサンプル引用に解説を加えていくことで、自社に適したポリシーを策定するための手助けを行っていくことを目的としている。

今回は、物理的な対策に関するスタンダードの主要部分である『物理的対策標準』と『サーバルームに関する標準』、および『職場環境におけるセキュリティ標準』を岡本氏に解説していただく。最後に『媒体の取り扱いに関する標準』について解説する。

これまで同様、連載の第1回で紹介したモデル企業を想定したポリシー・サンプルの解説となる。解説のなかでは「企業」や「会社」などと表現するが、内容的には非営利の組織であっても同様なので、読者の方は随時読み替えていただきたい。 （佐藤）

『物理的対策標準』および『サーバルームに関する標準』作成時のポイント

ここではまず、物理的なセキュリティ対策について規定した『物理的対策標準』と『サーバルームに関する標準』作成時のポイントについて解説する。なお、以下の解説では2つのポリシー・サンプルの項番を区別するため、『物理的対策標準』をA、『サーバルームに関する標準』をBと記す。

ポイント1 サーバルームとセキュリティ区画の定義（サンプルA.4.1節およびB.4.1節参照）

『サーバルームに関する標準』ではサーバルームを以下のように定義している。

JNSAの紹介

JNSAは2000年4月に設立され、2001年7月にNPO法人として活動を継承しました。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を、4つの部会と各WG（ワーキンググループ）に分かれて行っています。

昨年度の主な成果物としては、「外部接続に関するセキュリティポリシーサンプル冊子」の作成、「セキュリティインシデント被害調査」におけるアンケートの実施および報告書の作成などが挙げられます。

また、複数CAの相互運用性に関する実証実験を行った「Challenge PKI 2001プロジェクト」の結果報告も、Webにて公開中です。その他の活動として、年1回の主催カンファレンスの開催（NSF2002、今年は6月12-13日に開催）、セキュリティセミナーの開催、会報誌「JNSA Press」の発行（年3回）などを行っています。

＜お問い合わせ＞
特定非営利活動法人 日本ネットワークセキュリティ協会
URL：http://www.jnsa.org/
E-Mail：sec@jnsa.org

A.4.1　サーバルームの定義
(1) サーバルームの定義は「重要度の高い情報資産が格納されているサーバがまとめて設置される部屋」とする。重要度の高い情報資産については別途定める。

「サーバルーム」と言ったときに想定されるものにはかなり幅がある。例えば「オフィス内でサーバをまとめて置いている作業部屋」程度のものを思い浮かべる人もいれば、「特に重要なサーバを厳重に監視するための部屋」のようなものを想像する人もあるだろう。サンプルでは後者に近いものを想定し、対策のレベルを設定している。

一方、『物理的対策標準』では、セキュリティ区画の設定について以下のように規定している。

B.4.1　セキュリティ区画の設定
(1) 重要度の高い機器・設備を設置する場所にはその重要度に応じたセキュリティ区画が設定されなければならない。

したがって、サーバルームもセキュリティ区画の一種として、その設定と運用を規定している。

ポイント 2　他の標準との連携によるセキュリティレベルの維持（サンプルA.4.1節参照）

(2) 電子化されたデータとして保存する重要度の高い情報資産は、『クライアント等におけるセキュリティ対策標準』および『媒体の取り扱いに関する標準』に基づいて管理される場合を除き、サーバルームに設置するサーバでのみ保存されなければならない。

サーバルームでは一定以上のセキュリティ確保が期待できるため、電子データとなっている重要度の高い情報資産は可能な限りサーバルーム内で管理することで、効率的なセキュリティ対策が行える。したがって、できる限りサーバルーム以外での重要度の高いデータの定常的な利用は避けることが望ましい。

しかし、実際には一般オフィスやモバイル環境でのデータ利用が必要な場合も出てくる。そこで、このようなデータ利用のセキュリティを確保するためには、他の標準で十分な対策を規定し、組織全体としてのセキュリティレベルを維持すべきである。

ポイント 3　セキュリティ区画での対策の設定（サンプルB.4.1節参照）

(5) セキュリティ区画は区画およびそこに設置する機器・設備等に関するセキュリティ上の各種のリスクを評価した上で必要な対策を実施しなければならない。リスクの要素には以下のものがある。
・盗難、破壊、地震、火災、水害等の水の事故、ほこり、振動、化学作用、電源事故、電磁波、静電気等

セキュリティ区画については、その中に置く情報資産の重要度についてさまざまなレベルが考えられる。そのため、『物理的対策標準』では(5)の規定のようにリスクの評価とそれに応じた対策の実施を求め、具体的な対策は明確に示していない部分がかなりある。一方、サーバルームは重要度が高いサーバの設置を前提としているため、『サーバルームに関する標準』では想定したレベルに即した対策内容がより具体的に記述してある。皆さんの組織でこのようなセキュリティ区画やサーバルームについての標準を作成する場合には、区画のレベルやレベルごとに要求する対策を具体的に設定してもよいだろう。**表1**に『物理的対策標準』のセキュリティ区画と『サーバルームに関する標準』でのサーバルームの対策の設定について相違点の比較を示したので参考にしていただきたい。

また、一般のオフィスについても何も対策をしないということは考えにくい。いわば「最低レベルのセキュリティ区画」として扱うべきである。

ポイント 4　サーバルームの設置（サンプルA.4.2節参照）

(1) サーバルームは独立した部屋として設置し、一般オフィスとの共用や他社オフィスとの隣接は避けなければならない。
(4) サーバルームの出入り口は原則1ヶ所に限定し、施錠設備を設けなければならない。

図1はサーバルームを設置したオフィスのレイアウトの例である。ここで示した例ではフロア全体を自社のオフィスとして利用しており、サーバルームは一般オフィス等に囲まれた形で設置している。このように、サーバルームは屋外や他社オフィスには接しないようにすることで侵入等のリスクを低くできる。もし、やむを得ずサーバルームを屋外に接する場所に設置しなければならない場合には、監視カメラ等、他の方法で対策を補強することを検討すべきである。

また、サーバルームのような区画の区切り方については、次のような方法が考えられる。どの方法を取るかは、情報資産の重要度とコストの兼ね合いで判断すべきである。
・低いパーティションで区切る
・天井までのパーティションで区切る
・(新築、改築時に) 建物自体の壁で区切る

表1●「セキュリティ区画」と「サーバルーム」での主な対策設定の相違点（ポリシー・サンプルでの設定）

比較項目	セキュリティ区画での対策設定	サーバルームでの対策設定
出入り口	数は規定なし、施錠設備必要	原則1ヶ所、施錠設備必要
窓	規定なし（リスク評価に基づく対策を要求）	極力設置を避ける、網付きガラス・強化ガラスの利用
防犯設備		防犯カメラ、侵入報知機等の設置検討
非常用連絡設備		非常電話、非常ベル等の設置検討
コピー・FAX等		設置禁止
入室メンバ	登録メンバの制限	登録メンバの制限、受付または認証装置によるチェック
長時間作業	規定なし（リスク評価に基づく対策を要求）	同伴者が必要
無許可撮影・録音		禁止

(3) サーバルームの外観は目立ちにくいものとし、室名表示等も最小限にとどめなければならない。
(5) サーバルームに窓を設けることは極力避け、設ける場合は網付きガラス・強化ガラス等を用いなければならない。

室名表示や窓の設置を避けることは、サーバルームやそこに設置した重要なサーバの存在をできるだけ隠そうという考え方に基づいている。極秘レベルの情報資産を保護する場合には、このような考え方を取ることが多い。一方、サーバルームに対して窓を積極的に設け、できるだけ多くの目で監視できるようにするという方法を取る場合もある(ただし、それでも屋外に面した窓は設置を避けるべきである)。いずれにしても、サーバルームの設置方法は、そこに置く情報資産の重要度(被害があった場合の被害金額等)と設備の強度(対策コストの掛け方)の兼ね合いで検討すべきである。

ポイント5 サーバルームの設備(サンプルA.4.2節参照)

(6) サーバルームには設置する機器・設備の重要度に応じて、防犯カメラ、侵入報知機等の防犯設備の設置を検討しなければならない。
(7) サーバルームには必要に応じて、非常電話、非常ベル等の非常用連絡設備の設置を検討しなければならない。
(8) サーバルームにはコピー・FAX等、情報の複写や送信のための設備を設置してはならない。

コピー・FAX設備は、情報持ち出し防止のために設置を禁止すべきである。ただ、サーバや設備の保守作業時に利用したい場合もあるかもしれない。そのような場合には、次のいずれかの運用が考えられる。

・サーバルームの外にある設備の利用で対応する。
・許可があった場合にのみ動作可能な形(パスワードでの利用制限機能付き等)でサーバルームに設置し、運用する。

ポイント6 サーバルームの入退室管理(サンプルA.4.3節参照)

(1) サーバルームは従業員不在時には施錠しなければならない。
(3) サーバルームへの入室は、受付または認証装置(入館カード、パスワード入力、生体認証)等によって特定の登録メンバに制限されなければならない。

(1)の規定は、施錠を従業員が手動で管理している場合の管理方法を規定する内容になっている。一方、(3)の規定は電子的な認証での入室(扉の開閉)も想定しており、複数の施設のパターンに関する規定が混在している。皆さんがこのポリシー・サンプルを利用する場合には、組織の状況に合わせて取捨選択と書き換えを行っていただきたい。

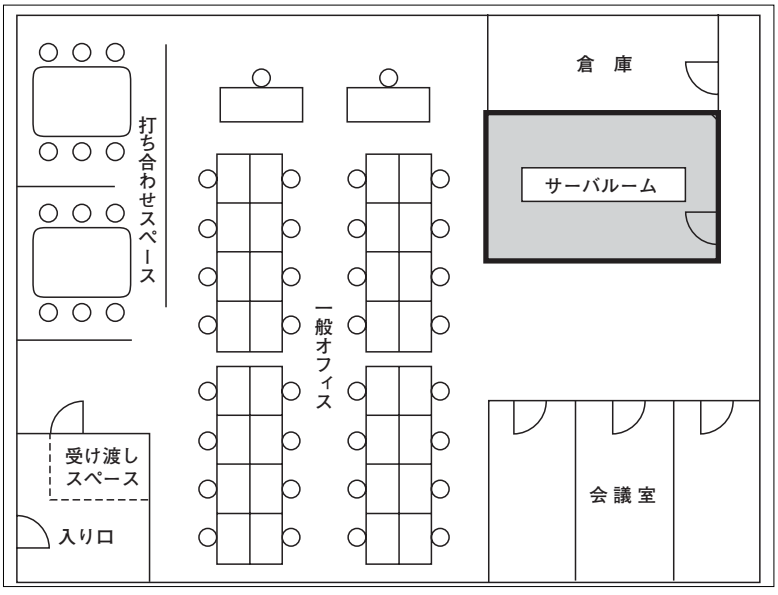
なお、特に厳密な入退室管理を必要とする場合には、次のような設備を利用する方法が考えられる。

・インターロック(2枚のドアの同時開放を避けることで1人ずつしか入れないしくみ)
・2人同時に操作しないと開錠できない扉(1人だけでの在室を防止する)

また、入退室と施錠については、消防法等で規定される非常時の避難経路の確保との関連についても注意が必要である。例えば、電子ロックの扉も停電時にサムターン(開閉つまみ)で開くつくりになっている等の配慮が必要となる。

さらに、作業員の出入りという意味では、ビル管理との兼ね合いで、警備スタッフの巡視による入室が避けられない場合も考えられる。このような場合には、契約でのセキュリティ遵守事項設定と機器に対する不用意なアクセス防止対策実施で対処することになる。

図1■サーバルームを設置したオフィスのレイアウトの例



ポイント7 サーバルームでの作業管理(サンプルA.4.3節参照)

(4) サーバルームへの未登録者の入室および作業実施については管理責任者の許可と登録メンバの同伴がなければならない。
(8) サーバルーム内で長時間作業を行う場合は一人では実施せず、必ず同伴者を伴わなければならない。

サーバルーム内での作業は、基本的に複数のスタッフによる相互牽制が働く状態で行われるべきである。また、協力会社の社員や契約社員が出入りするオフィスでは、協力会社の社員や契約社員だけが部屋にいる状態を作らないようにすべきである。もし業務上そのような運用が難しい場合には、作業状況の記録・監視など、他の対策によって管理を強化する方法も考えられる。

(9) サーバルーム内で管理責任者の許可なく撮影・録音を行ってはならない。

撮影や録音は、そこから入手した情報からセキュリティを破ろうとする、いわゆるソーシャルエンジニアリングに利用される可能性があるため、管理すべきである。ソーシャルエンジニアリング対策は、このような方法と後述する職場環境のセキュリティ対策との組み合わせで行うべきである。

(10) サーバルームには作業に必要のないものを置いてはならない。もし置いてあった場合は速やかに撤去しなければならない。

(10) の規定は、主にサーバルームの備品を意識して記述されている。故意の情報持ち出しや不用意な情報漏えいにつながるような物品は極力排除すべきである。具体的な例を挙げると、サーバルーム内への無線LAN機器の設置などは禁止すべき事項の1つである。

また、サーバルームの備品だけでなく、作業者の持ち込む物品についても配慮すべきである。ノートパソコンの持ち込みについてはその届出を義務付け、実際に持ち込む際には機器の確認を行うようにするとよい。その他、携帯電話の利用管理については「ポイント5」で述べたコピー・FAX設備の場合と同様に、運用面での配慮が必要である。

ポイント 8　点検と見直し（サンプルA.4.3節参照）

(5) サーバルームに入室可能な登録メンバは定期的に見直さなければならない。
(6) サーバルームに入室不要となった登録メンバは速やかに登録を解除し、入室のための認証を無効にしなければならない。
(11) サーバルーム内の環境（機器・設備の有無、配置、利用状況等）は定期的に点検しなければならない。

(5)、(6) の規定は、異動や退職等によって入室の必要がなくなったスタッフの権限を利用した不正な入室を防ぐためのものである。また、(11) の規定は、不正な情報の収集や持ち出しのリスクを低減するために重要である。こういった監査・監視の観点からの対策は運用がおろそかになりがちなので、実施記録を確実に残すなどの注意が必要である。

ポイント 9　機器・設備の設置（サンプルB.4.3節参照）

(1) 機器・設備の設置位置については、不正な操作が実施しにくく、不用意な操作ミス（間違いや見落とし）が起こりにくいように配慮しなければならない。
(2) 重要度の高い機器・設備は他のものと分離して設置しなければならない。
(3) 機器を設置する場合、落下や損傷の防止措置をとらなければならない。

機器・設備の設置場所や設置方法については、規定に示されているようなリスクのほか、盗難や情報の持ち出しなどを含むさまざまなリスクを考慮して決定する必要がある。サーバルームの場合、サーバの重要度に応じてその設置に利用するラックについても次のような保護機能のあるラックを使用するべきである。

・鍵付きラック（不正操作や盗難の防止）
・転倒防止、機器落下防止機能付きのラック（地震による機器損傷の防止）

この他、規定に書かれていない機器・設備の設置に関する注意点としては、次のようなものがある。

・重要度の高いものは窓や入り口から見えにくい場所に置く。
・ノートPCの盗難対策として持ち出し防止のチェーンを付けるか、退社時に鍵の掛かる戸棚にしまうようにする。
・電磁波による情報漏えいを防止するため、部屋に電磁シールドを導入する。あるいはもっと簡略な方法として、機器をなるべく壁から遠ざけて設置する。

『職場環境におけるセキュリティ標準』作成時のポイント

次に、物理的な対策と運用面での関連が深い『職場環境におけるセキュリティ標準』作成時のポイントについて解説する。

ポイント 1　クリアデスクポリシーとクリアスクリーンポリシーの呼称（サンプル4.1節および4.2節参照）

4.1　書類・媒体等の取り扱いと保管（クリアデスクポリシー）
4.2　画面に表示する情報の管理（クリアスクリーンポリシー）

「クリアデスクポリシー」「クリアスクリーンポリシー」という表現は、BS7799等で使用されるなど、セキュリティポリシーの分野では一般的に使われるようになっている。ただ、この表現自体は意味する内容が伝わりにくいため、本ポリシー・サンプルではその主な内容を意味する日本語の見出しをメインの見出しとしている。

ポイント 2　机上の書類や媒体の管理レベル（サンプル4.1節参照）

(1) 従業員は使用していない書類や媒体をキャビネット等へ収納し、机上等に放置してはならない。

机上の書類や媒体からの情報漏えいを防止するためには管理が必要だが、その具体的な方法については管理のレベルや実施する状況によってさまざまなものが考えられる。具体的な方法の例を次に示す。

・すべての書類や媒体を鍵の掛かる場所へしまう。
・机上にものを残さない。

・書類等はすぐには見えない状態にしておく(伏せておく等)。

これらの方法をどのように適用するかについては、まず書類・媒体の重要度を考慮して決定すべきである。また、実施する状況に合わせて「離席時には伏せておく。退社時には鍵の掛かる場所へしまう」といった形での適用も現実的かつ有効と考える。

ポイント3　情報資産の金庫での保管(サンプル4.1節参照)

(2)従業員は重要度の高い書類や媒体を施錠保管し、特に必要な場合は耐火金庫・耐熱金庫に保管しなければならない。

耐火金庫は書類等の保管を想定したものであり、格納した紙が燃えることはないが、媒体等は変質して使用不能となってしまう可能性がある。一方、耐熱金庫は熱に弱い媒体の耐熱温度を超えないように設計されており、媒体を火災によるリスクから保護することができる(ただし、保護可能な媒体の範囲(保証する温度のレベル)には製品によって違いがあるので注意)。また、耐火金庫が既にあり、耐熱金庫の導入がコストの面で困難である場合に、耐火金庫と消火設備の組み合わせによって媒体の損傷に関するリスクを低減するような運用も考えられる。

ポイント4　コピー機、FAX、プリンタ等の入出力書類の管理(サンプル4.3節参照)

(2)従業員はコピー機、FAX、プリンタ等の入出力書類を放置してはならない。特に重要度の高い書類は印刷および送受信の間、従業員が常に機器に(FAXの場合は送受信の両側とも)立ち会うようにしなくてはならない。

書類の放置は盗み見や盗難の危険性があると分かっていても、実際の職場ではよく見られる問題であり、注意すべき点である。ミスコピー(失敗したコピー用紙)の処分、誤操作や「出てこないと思った印刷が後で出てきた」等で出力された書類の放置防止などは、意識向上と(定期的なチェックなどの)管理のしくみの両面で取り組むべきである。

ポイント5　搬入物の受け渡し管理(サンプル4.4節参照)

(1)搬入物の受渡しについては受渡し場所を設置し、『サーバルームに関する標準』で定めたサーバルームおよび『物理的対策標準』で定めたセキュリティ区画とは分離しなければならない。
(2)受渡し場所への従業員以外のスタッフによるアクセスは、必ず従業員の監視付きで行い、アクセスを記録しなければならない。
(3)搬入物の受入れを行う従業員は受入れの際に危険物持込や情報漏洩等のリスクがないかどうか点検しなければならない。

搬入物の受け渡しについては、搬入物の配送を行うスタッフに関するリスクと、搬入物そのものに関するリスクを考慮して管理の方法を決める必要がある。(1)と(2)の規定はこの前者に対応し、物理的なセキュリティ対策に関する部分で説明した建物の構造や入退室管理にかかわる部分である。宅配便等の配達スタッフが簡単にオフィスの内部に入ることができてしまうということは案外多いのではないだろうか。最低限の受け渡しの手順を決めておくとともに、オフィスの出入り口付近にソーシャルエンジニアリングの対象となりそうな情報の掲示や放置がないよう配慮すべきである。

一方、(3)の規定は後者に対応する。想定される問題は映画やドラマでの事件を思わせるものかもしれないが、宛先が不明確だったり、不審な様子があったりする搬入物については、内容の確認等を慎重に実施しておくに越したことはない。

ポイント6　会議での盗み聞き防止対策(サンプル4.5節参照)

(1)従業員は電話や立ち話、オープンな会議スペースでの発言について、盗み聞きを防止するよう配慮しなければならない。

(1)の規定ではオープンな会議スペースでの盗み聞き防止に言及しているが、オープンでない会議室についても盗み聞き防止について考慮する必要がある。そんな中でも極秘レベルの内容の会議を行う場合には、防音設備のあるスペースで行うことを検討すべきである。しかし、多くの会社では本格的な防音設備を持つ会議室を準備することは費用の面で難しいと考えられる。

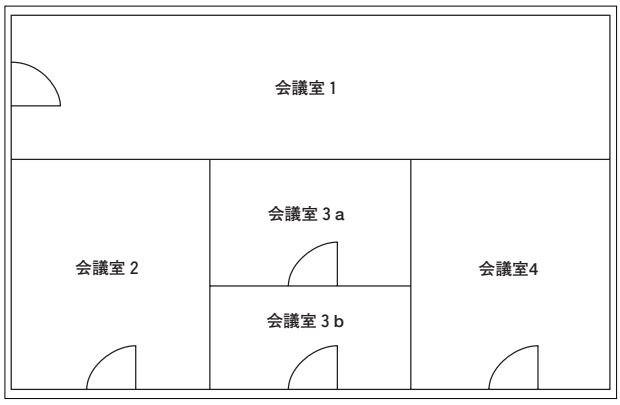
そのような場合の代替策として、**図2**のような形で会議室を設置し、極秘レベルの会議は図中の全会議室を確保した上で中央の会議室3aを使って行う(他の会議室は施錠する)といった方法も考えられる。

●その他、注意すべきポイント

『職場環境におけるセキュリティ標準』では、さまざまな観点での盗み見の防止対策が記述してあるが、その他にもそれぞれの職場の状況に応じてリスクを見直し、対策を講じるようにしていただきたい。例えば、窓のブラインドの管理などは、多くの職場で注意すべき点である。

また、盗み見の防止以外についても、職場環境におけるセキ

図2■会議室の設置の仕方の例



ュリティは職場の状況によってさまざまな異なるリスクが存在すると考えられる。したがって、ポリシーの策定の前に十分なリスクの分析を行うべきである。

さらに、本章での要求事項には、基本的な動作や手続きの徹底が必要な項目が多い。つまり、従業員のセキュリティの重要性に対する理解やセキュリティ対策への意識の高さが要求される。そこで、計画的な教育を行うとともに、職場でのミーティングやイントラネットを通じてさまざまな教育・啓発活動を実施することをお勧めする。（岡本）

『媒体の取り扱いに関する標準』作成時のポイント

ポイント1 対象者の定義（サンプル2節参照）

> (2) 対象者
> PC等の修理を依頼するすべての従業員。
> 媒体の使用、処分を行うすべての従業員。

ここでは、単に「媒体の使用、処分を行うすべての従業員」とすることもできるが、PC等の修理の際に、そのなかに入っている情報への配慮の意識付けをするため、あえて、「PC等の修理を依頼するすべての従業員」とした。

特にPC等の修理や廃棄の場合、そのなかの情報のバックアップや移行のことだけに気を取られ、機密性の高い情報の削除を忘れないようにしなければならないからである。

ポイント2 修理・廃棄などの実施体制（サンプル4節参照）

サンプルでは、修理や廃棄などの実施は、現場ではなく、情報システム部が一括して行うことを想定した。職場の規模や技術的な知識の有無により、現場で実施するという体制も考えられるので、適宜、検討していただきたい。

ポイント3 PC 等修理の取り扱い（サンプル4.1節参照）

内部に情報を蓄積しているPC等の修理を社外に依頼する際には、そのPCに対して媒体と同じ管理を実施する必要がある。このことは、意外と不注意になりやすい。

このため、サンプルではハードディスク等の装置を取り外して修理を依頼することにしたが、その状態では修理ができない場合があるかもしれない。そのようなときには、ハードディスク装置の修理に際しての規定を設ける必要がある。たとえば、修理業者と守秘義務契約の締結をすることを盛り込むとよい。機密性の極めて高い情報が入っている場合には、情報の回復によるメリットと機密漏洩のリスクのバランスによって、修理をあきらめる判断も必要である。

また、修理するものにどのような情報が格納されているかによっては、注意が必要である。というのも、修理直前には高い機密性のある情報を処理していなくとも、それ以前に処理していた場合、ハードディスクの内部には、それらの情報の断片が残っている可能性があるからだ。特に修理の際には、そのような削除したはずの情報が復元される可能性が高い。こうした事態を考慮して、時をさかのぼって検討しなければならない。本来、媒体にも同じ注意が必要だが、修理に出すことのない媒体の場合は、ある程度管理を緩和するのが、現実的な運用となることもある。

ポイント4 媒体の移動（サンプル4.3節参照）

サンプルでは、搬送時の機密漏洩の予防だけに配慮したが、暗号などを用いて、保護対策も施すほうがよい。逆に、そのようにすれば、搬送手段の制限の緩和を行うことも検討できる場合がある。

ポイント5 媒体の再使用（サンプル4.4節参照）

サンプルでは、媒体の種類ごとの具体的な手順を規定しなかったが、追記型のCD-Rと、CD-RWの違いを一般の人が区別するのは難しいかもしれない。これらについては、単に媒体の取り扱いよりも、媒体への処理に使用するソフトウェアの使用制限などと併せて、具体的な注意事項を従業員に教育・啓発などする必要がある。

●その他注意すべきポイント

日々、取り扱う媒体の情報量が増えているため、媒体の管理は重要な課題になってきている。サンプルでは一般的な考え方を示したが、利便性とコスト、機密漏洩のリスクを検討した上で、それぞれの組織や職場単位で適切なバランスを保った管理を決定する必要がある。

また、情報を暗号化することで、機密情報の漏洩の保護に役立てることもでき、それによって媒体管理の自由度を高めることもできる。その場合には、暗号鍵の保管と回復策を別のスタンダードなどで定めることが必要である。

早いもので、次回はスタンダード項目としては最後から2番目、全体を通しては6番目のグループとなる「セキュリティ運用なんてドンと来い集」について解説する。

個別の返答は必ずしもお約束できないが、連載内容に反映していきたいと考えているので、ご意見・ご感想等を電子メールでぜひお寄せいただきたい。

E-Mail：SECURITY-POLICY@yoshiro.com

サンプルを見ながら策定する
ドンと来い！情報セキュリティポリシー

第7回

セキュリティ対策の「スタンダード（標準書）」を作る⑥

作成篇__セキュリティ運用なんてドンと来い

スタンダードは、組織における情報セキュリティ対策の要件を具体的に規定するものであり、あらゆる組織で必要不可欠のものだ。
その策定には多くの労力を要するが、JNSAのポリシー・サンプルをたたき台とすることで、それを軽減できるはずだ。
前回は、スタンダードのうち、物理的な対策に関連する部分について解説した。
今回は、セキュリティの運用に関するスタンダードについて、それらの構成と策定内容をJNSAのサンプルを用いて解説しよう。

筆者＝佐藤慶浩（NPO 日本ネットワークセキュリティ協会 理事）、城石憲宏（新日鉄ソリューションズ株式会社）、寺井晶子（株式会社NTTデータ）

JNSAの紹介

JNSAは2000年4月に設立され、2001年7月にNPO法人として活動を継承しました。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を、4つの部会と各WG（ワーキンググループ）に分かれて行っています。

昨年度の主な成果物としては、「外部接続に関するセキュリティポリシーサンプル冊子」の作成、「セキュリティインシデント被害調査」におけるアンケートの実施および報告書の作成などが挙げられます。

また、複数CAの相互運用性に関する実証実験を行った「Challenge PKI 2001プロジェクト」の結果報告も、Webにて公開中です。その他の活動として、年1回の主催カンファレンスの開催（NSF2002、今年は6月12-13日に開催）、セキュリティセミナーの開催、会報誌「JNSA Press」の発行（年3回）などを行っています。

<お問い合わせ> 特定非営利活動法人 日本ネットワークセキュリティ協会
URL：http://www.jnsa.org/ E-Mail：sec@jnsa.org

本講座の読み方

まずは以下のWebサイトよりJNSAのポリシー・サンプルのファイルをダウンロードしてほしい。

http://www.jnsa.org/policy/guidance

今回は、次の4つのサンプルをダウンロードしておくとよい。

『システム維持に関する標準』
『システム監視に関する標準』
『セキュリティ情報収集及び配信標準』
『セキュリティインシデント報告・対応標準』

これらを印刷して本書の横に並べて読んでいただきたい。

本講座では、その一部を解説の必要に応じてJNSAの承諾を得て転載している。それぞれのファイルからの引用部分は、章や節の番号とともに以下のような囲み表示をしてある。

> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

本講座はこのようなサンプル引用に解説を加えていくことで、自社に適したポリシーを策定するための手助けを行っていくことを目的としている。

今回は、『システム維持に関する標準』を城石氏に、『システム監視に関する標準』と『セキュリティインシデント報告・対応標準』を寺井氏に解説していただく。『セキュリティ情報収集及び配信標準』については解説を省くが、サンプルを参照して、自分の組織に見合ったものにしていただきたい。

今回もこれまで同様に、連載の第1回で紹介したモデル企業を想定したポリシー・サンプルの解説となる。そのため、解説のなかでは「企業」や「会社」などと表現するが、内容的には非営利などの組織であっても同様なので、読者の方には随時読み替えていただきたい。（佐藤）

『システム維持に関する標準』作成のポイント

企業のPCやサーバにOSやアプリケーションを導入する際や、システムを構築する際には、既知のバグやセキュリティホールに対して最新のパッチなどを適用するといった対策が行われているだろう。しかし、バグやセキュリティホールは、運用開始後にも新たに発見されるものだ。そうしたバグによる障害やセキュリティ侵害による障害からサーバやシステムを守るために、運用開始後も何らかの対応を施し、セキュリティレベルを維持していく必要がある。

ここでは『システム維持に関する標準』作成のポイントについて解説する。

ポイント1 パッチ適用のルール（サンプル4.1節参照）

本節ではパッチ適用のルールについて記述しているが、パッチはその緊急度に応じて大きく2種類に区別できる。1つは重大なバグ修正やマシンをクラッシュさせてしまうほどの危険度の高

いセキュリティホール修正のように、即座に適用しなければならない緊急度の高いパッチ、もう1つは即座に適用する必要はなく定期メンテナンス時に適用すればよいという緊急度の低いパッチである。その判断基準についてはポリシー・サンプル「セキュリティ情報収集及び配信標準」を参考にしてほしい。

サンプルでは緊急度の高いパッチと低いパッチの区別をしていないが、それぞれによって作業の手順などが変わることも考えられる。皆さんが作成するポリシーでは、これらを区別して検討してもよいだろう。

また、重要なサーバへパッチを適用する場合は、テスト用マシンを用意して事前にテストをしておくのがよいだろう。特に、独自開発したシステムがある場合には、パッチを適用することによりシステムに影響を及ぼす場合が考えられる。例えば、アプリケーションでOSのライブラリを使用しているときなどに、OSのパッチを適用した際にこのライブラリに変更が加わり、アプリケーションがエラーを出すなどといったことも考えられる。

このようなことがないように事前にテストを行い、異常が出ないかどうかを確認することも大切だ。実際にスタンダードを作成する際には、こういったことも考慮して検討すればよりよいものになるだろう。

> (1)弊社システムの管理者及び使用者は、『セキュリティ情報収集及び配信の標準』に基づいて情報システム部より配信されたパッチ適用の指示に対して、自分が管理または使用している全てのマシンに対して速やかにパッチを適用しなければならない。
> (2)情報システム部は社内全てのマシンに対して、(1)のパッチが指示通り適用されているかを確認する事が望ましい。

ポリシー・サンプルでは、(1)で指示があったら速やかにパッチを適用しなければならないと義務づけて、(2)で確実に適用しているかを確認させるようにしている。(1)の「速やかに」を具体的に「指示があってから1日以内」などにしてもよいだろう。また、(2)は「望ましい」となっているが、「しなければならない」と義務づけてもよいだろう。

> (3)パッチ適用作業によるサービスの停止など他システムへの影響が大きく、速やかに(1)のパッチが適用出来ない場合、システム管理者は情報システム部に連絡しなくてはならない。その場合、システム管理者はパッチ適用計画を作成し、情報システム部に提出すること。それに基づいてパッチを適用しなければならない。

(3)では、(1)に従えない場合に、サーバ管理者にパッチ適用計画を立てさせ、必ず適用させるように規定している。また、パッチが適用されていない期間に何らかの回避策がある場合にはその回避策を実施、回避策がない場合には対象サーバの監視を強化するなどの対策を取るべきである。

> (5)パッチ適用中に何らかのトラブルが発生した場合、作業者はトラブルの内容を情報システム部に報告しなければならない。
> (6)情報システム部は(5)のトラブルの報告を受けた場合、関係各部への連絡を行い今後の対応をする必要がある

(5)、(6)はパッチ適用中にトラブルが発生した場合の対処方法である。

ポリシー・サンプル4.4.(3)でパッチ適用前のバックアップを定義しているので、このデータでトラブル発生前の状態に戻し、今後の対応を協議する必要がある。その際に原因の究明を行い、次回作業の手順やスケジュールなどを検討すべきだろう。

ポイント2　パッチの取得及び配布方法(サンプル4.2節参照)

パッチの取得に関しては、そのパッチが信頼できるものかを検証する必要がある。メーカーから配布されるCD-ROMは信頼してよいと思われるが、パッチをWebサイトからダウンロードする場合は、ダウンロードするものが本当に正規のものか、そのサイトが信頼できるのかということを確認する必要があるだろう。

現状、パッチをインターネットから入手するのであれば、最も安全と思われるのはSSLや電子証明されているWebサイトからダウンロードすることだろうが、すべてのサイトがそういった設定を施していることは少なく、何を信じるべきかを検討しておく必要があるだろう。

サンプル・ポリシーではメーカーおよびベンダーを信頼した視点から記述しているが、フリーのソフトウェアなどはその信頼性を考慮したほうがよいだろう。

ポイント3　サーバのバックアップについて(サンプル4.4節参照)

バックアップは、パッチ適用時に障害が発生した場合や、セキュリティ侵害、自然災害などによる障害からサーバやシステムを素早く容易に復旧するために非常に重要である。

バックアップを検討する際のポイントとして、

1)バックアップの対象データ
2)リストア(データの復旧)の作業手順
3)バックアップのスケジュール

の3つを押さえておくとよい。

1)のバックアップの対象データは大きく分けて2種類ある。1つはOSやアプリケーションなどのファイル、もう1つはそのサーバ上でアプリケーションが使用しているデータである。アプリケーションが使用しているデータ(例えばデータベースのデータ)はアプリケーション自体がバックアップ機能を実装していることが多く(Oracleならarchiveログ機能でバックアップを行っている)、運用面などで一括りにはできないため、ここでは言及しない。ポリシー・サンプルはOSやアプリケーションなどのファイル

表1●バックアップの種類と特徴

フルバックアップ	対象システム内のファイルすべてのバックアップを取る方法。バックアップを取得するのに時間がかかるが、この1回のリストア作業で元の状態に戻すことができる。
差分バックアップ	前回のバックアップからの追加更新された情報のみバックアップする方法。フルバックアップに比べ取得するデータが少ないため短い時間でバックアップが行える。
増分バックアップ	前回のフルバックアップ後に追加更新された情報をバックアップする方法。差分バックアップに比べ1回の取得データは日々多くなる。

について考えて作成してある。

なお、OSやアプリケーションなどのファイルのバックアップには、「フルバックアップ」「差分バックアップ」「増分バックアップ」などの種類がある。これはバックアップデータの対象によって分けられている(**表1**参照)。

2)のリストアの作業手順は、バックアップ全体の方針やスケジュールをも決定しかねない重要な作業である。したがって、リストアについても十分な検討が必要だ。

その際の考慮点としては以下のことが考えられる。

- いつの状態にまで戻す必要があるのか

対象となるデータの重要性や更新頻度などによって異なってくるが、これによりバックアップのスケジュールが決まってくる。例えば、障害が起きた前日まで戻す必要があるならば、最低でも日次にバックアップを取る必要がある。

- リストア後の動作確認作業

リストアから障害が起きた時間までに変更した点(ファイルの修正など)があった場合は、その変更を行う必要がある。例えば、ウイルスチェックサーバのパターンファイルはリストアによって最新ではなくなる場合があるので注意が必要だ。

- リストア作業の案内について

リストア作業を行う前にその旨をユーザーに連絡し、データが消失する可能性があること、リストア後に消失したデータの再入力が必要であることを案内すべきだろう。

3)のバックアップのスケジュールは1)、2)を決定すればほぼ決まってくるだろう。

> (1)業務上重要なサーバ(WWWサーバ、mailサーバ、経営・経理・受発注システムなど)については、そのデータ及びlogを定期的にバックアップしなければならない。

サンプルでは「サーバは定期的にバックアップすること」と一括りで記述してあるが、実際にはサーバごとに考えたほうがよい。例えば、朝9時から夜18時まで稼働しているシステムがあり、17時に障害が発生したとしよう。その日の最初の状態にまで戻せばいいのであれば日次でバックアップが必要だ(**図1A**)。1時間前の16時の状態に戻したいのであれば1時間ごとのバックアップが必要だ(**図1B**)。最新の状態まで戻したいのであれば、Bの1時間ごとの間隔を10分ごとにするなど、アプリケーションの機能を使用する必要があるだろう(**図1C**)。このように、どの状態に戻すかによってバックアップスケジュールは変わってくる。また、バックアップの方法も変わってくる。日次のバックアップなどは運用時間外で行うことが多く、時間的に余裕があるため、フルバックアップが可能だろう。だが、運用時間中に行うバックアップでは作業時間的にもデータの更新などを考えた場合にも、差分や増分バックアップで行うのが望ましい。

このようにバックアップのスケジュール、種類の決定は、対象となるデータの重要度や増加量、障害時にいつまでの状態に復旧させるのかなどによって異なってくるので、バックアップを行うサーバごとに検討してほしい。

また、サンプルではサーバについてのみ記述してある。しかし最近では、ノートPCに顧客データを入れたり、電子メールのデータをPC上に入れて外出先で確認したりと、クライアントのノートPCにも重要なデータが入っていることが多いだろう。そのような場合は、クライアントPCについても検討したほうがよい。

ポイント4　バックアップ媒体の取扱について(4.5節参照)

> (1)バックアップ媒体はテープとする。

サンプルでは(1)のように規定しているが、サーバとクライアントでは使用する媒体も異なるだろう。バックアップで取得するデータの量にもよるが、クライアントの場合CD-RやDVDなども選択肢として考えられる。サーバは1本で数GBを記憶できるテープデバイスを使用するのが一般的だろう。

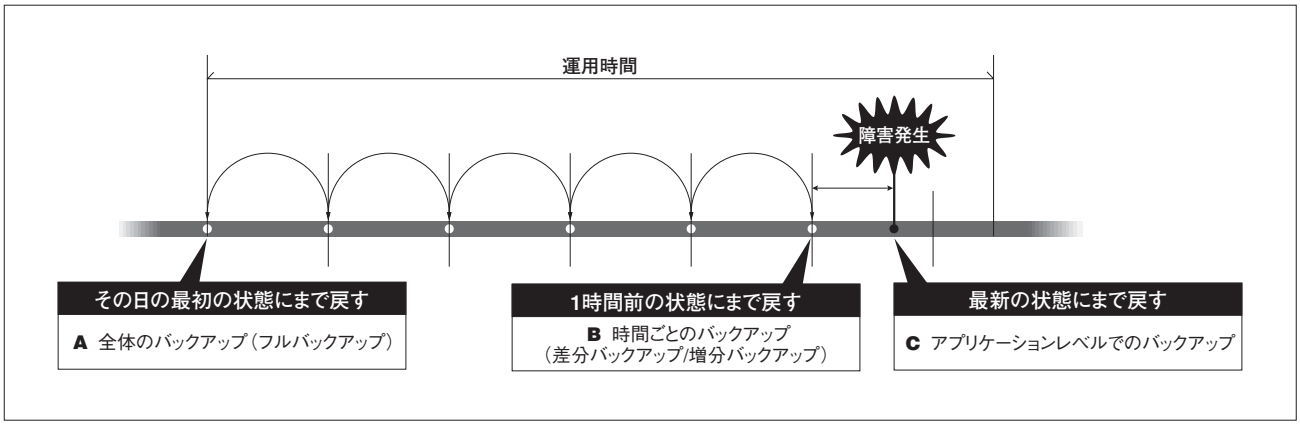
> (2)システムバックアップは過去2回分のバックアップデータを保持することが望ましい。

システムバックアップ保持期間についてここでは過去2回分としてあるが、回数でなく期間(3ヶ月間など)で検討することもできる。データの必要性に応じて検討してほしい。また、取得の際に正／副2つのデータを取ってバックアップの信頼性を上げることもよく行われている。

> (3)バックアップに使用する媒体は、鍵付きの保管場所に置くなど、サーバ管理者が責任をもって管理しなければならない。

バックアップデータの保管場所にも注意を払うべきである。サーバ管理者が鍵付きの保管場所で保管するのがよいだろう。また、遠隔地で取得したデータを輸送する場合、その運び方なども検討する必要があるだろう。また、たとえ媒体を盗まれたと

図1■バックアップのスケジュール、種類の決定



してもデータ自体を暗号化しておくことで、容易に中身が見られないようにするといった工夫も必要だろう。

媒体は管理台帳を作成し、その中身がいつ記録されたものなのか明確にすることも重要である。

●その他、検討すべき内容

サンプルで記述しているパッチ適用やデータバックアップ、リストアのように停止することができない場合などは、オンラインバックアップを検討したり、代替機や代替システムといったものを検討したりする必要があるだろう。特に代替機や代替システムは、オンライン作業の利便性だけでなく、障害時のサーバ／システム復旧を容易にするのに有効だろう。このような方法もポリシー作成時に検討してほしい。（城石）

『システム監視に関する標準』作成のポイント

ここでは情報システムの監視について規定した『システム監視に関する標準』作成時のポイントについて解説する。

ポイント1　対象システムのログによる監視について（サンプル4.1節参照）

ポリシー・サンプルでは情報システムの監視について大きく2つの節（4.1節、4.2節）に分類しているが、このうち4.1節は対象システムのログを用い、セキュリティ侵害時の原因を過去に遡って調査することや、システムおよびネットワークの利用状況を後日分析することを主な目的として記述されている。

さて、対象システムのログによる監視についてのスタンダード作成のポイントは、

1）取得対象・取得内容を明確にすること
2）取得したログの保管方法・保管期間を明確にすること
3）ログ解析の確実な実施を義務付けること

である。

> （1）情報システム部は、対象システムに関して次にあげるログを取得すること。なお取得されたログは24時間以内に書き換え不能なメディアに転送し、3年間、安全に保管すること。
> 取得対象：
> ①ログオン・ログオフの記録　②サーバのアクセスログ
> ③ファイアウォールのログ　④主要なネットワーク機器のログ
> ⑤システムログ
> 取得内容：
> ①アクセス時刻　②発信元/先アドレスとポート番号
> ③アクセス成功/失敗　④認証成功/失敗

取得内容については、そのログを取得後、単に保管するのか、適宜解析するのかなどの用途を考えて決めるとよい。

対象システムのログは一定期間、保管しておく企業が多いが、ここで問題となるのがログの保管期間の設定である。

ポリシー・サンプルでは上記のように設定しているが、この他にも対象システムの利用目的やシステム規模、ユーザー数に応じてさまざまな保管期間が考えられるだろう。また、取得するログデータ量が多い場合、システムの性能への影響、安全な保管場所の不足、管理コストの増大といった問題が生じる可能性もある。実際にスタンダードを作成される場合は、これらの要素を考慮して個々の企業に適した規定を作成していただきたい。

> （2）情報システム部は、許可された処理だけが実行されていることを確認するために、ログを月1回解析すること。

ログ解析の頻度についても明確にしておくことが望ましい。頻度について「定期的に」や「必要に応じて」といった曖昧な表現を用いると、運用上、実効性に欠ける恐れがある。スタンダード作成時には、必ず具体的数値を盛り込むことがポイントである。ただし、スタンダードでは全社共通の監視方針のみを示し、具体的な数値は各部門において別途作成する下位文書（プロシージャ等）に盛り込むという方法もあるだろう。具体的な数値は、監視するシステムが取り扱う情報の重要性によって異なる。また、組織規模が大きく、部門によってネットワーク環境や利用状況が異なる場合などは、具体的数値の設定を各部

門に委任することで、より円滑なスタンダードの運用が期待できる。

ポイント2　侵入検知システムによる監視について（サンプル4.2節参照）

不正アクセスをリアルタイムで把握・対処するためには、侵入検知システムによる常時監視が有効である。侵入検知システムによる監視についてのスタンダード作成のポイントは次の事項である。

1）守りたい箇所、すなわち侵入検知システムを設置するセグメントやホストを明確にすること
2）不正アクセスのパターンを記したシグネチャデータベースを常に最新化することを義務付け、日々発見される新たな攻撃手法に対応すること
3）不正アクセスが発見された場合の対応手順や連絡体制を明確にすること
4）侵入検知システムのログの分析と保管方法について規定すること

2）はシグネチャ型の侵入検知システムを導入した場合のポイントだが、この場合シグネチャに存在しない未知の攻撃手法に対応することができない。未知の攻撃に対しては、兆候検知型の侵入検知システムを導入することが効果的である。こちらの検知技術では、普段のネットワークやコンピュータの定常状態と比較して変則的なアクセスパターンを発見した場合に攻撃の可能性有りとみなす。そのため、シグネチャベースの侵入検知システムのように頻繁なデータベース更新作業が不要で、かつ未知の攻撃にも対応可能だ。しかし兆候検知型の場合、兆候イベントの設定が不適切だとシグネチャ型よりも誤報率が高くなる等の問題点もある。スタンダード作成にあたっては、侵入検知システムの導入目的、設置場所、運用体制等を考慮の上、規定を作成していただきたい。

●その他、検討すべき内容

ポリシー・サンプルは情報システムの監視に焦点を絞り、システム障害、情報システムへの不正アクセス、それに伴う情報流出等の被害を防止することを目的としている。しかしながら、組織全体の情報セキュリティ管理においては情報システムの監視のみならず、警備員の配置、居室への入退室管理といった人的・物理的側面への配慮も重要な要素であることにも留意していただきたい。

ここまで『システム監視に関する標準』について解説してきたが、監視はセキュリティインシデント対応においても重要な役割を担う。次に解説するセキュリティインシデント対応のためのスタンダード『セキュリティインシデント報告・対応標準』にも密接にかかわってくるものである。

『セキュリティインシデント報告、対応標準』作成のポイント

ポリシー・サンプルでは、セキュリティインシデント対応の時間軸に従って、「平時の準備」「セキュリティインシデント発生時」「再発防止計画」という3つの段階に分けて遵守事項を分類している。

ポイント1　平時の準備について（サンプル4.1節参照）

「平時の準備」に関する規定には、セキュリティインシデントの発生をできる限り予防するための対応策と、万が一セキュリティインシデントが発生した場合でも速やかに原因究明と復旧がなされるための準備事項を記載すべきである。

ポリシー・サンプルには「平時の準備」として、次のような項目が記載されている。皆さんの組織でスタンダードを作成される場合にもこれらの項目は最低限、含めることをお勧めする。

1）従業員のセキュリティ意識向上
2）ウイルス対策
3）セキュリティ情報の収集（パッチ適用等）
4）システム監視（ログ取得）
5）システム監視（侵入検知システム）
6）バックアップの取得
7）復旧に必要なリソース確保
8）各システムの復旧優先度の決定

また、あらかじめ想定していなかったセキュリティインシデントには対応できない、または対応できたとしても復旧作業が大幅に遅れてしまう可能性が高い。そのためスタンダード作成時には、最悪のインシデントレベルを想定して事前の準備と対応策を練っておくことがポイントとなる。

例えばポリシー・サンプルには次のような記載がある。

> （6）情報システム部は、インシデント発生後のシステムの復旧作業に役立てるために「システム維持に関する標準」に基づいて、適切にバックアップを取得しなければならない。なお、バックアップは必要に応じて遠隔地にコピーを保管することが望ましい。

後半に記載されたバックアップ（コピー）の遠隔地保管は、情報システムおよびバックアップ（原本）が設置された建物自体が

表2●バックアップの種類と特徴

復旧優先度	業務復旧までの許容時間
3	業務が停止することは許されない
2	24時間以内に復旧しなければならない
1	3日以内に復旧しなければならない
0	インシデント発生時は停止してもよい

倒壊してしまうような災害や爆破事故等を想定した規定である。地盤の異なる別拠点にバックアップ(コピー)を保管しておくことにより、大切な顧客データや取引情報の喪失を防ぐことができるので、インシデントからの復旧速度は格段に向上するはずである。

> (7)情報システム部は、インシデント発生後のシステムの復旧作業に必要なリソースを検討し、確保しておかなければならない。
> (8)情報セキュリティ委員会は、各システムの復旧優先度を決定しなければならない。復旧優先度の決定は、対象システムにおいて運用される業務の停止許容時間を観点において行う。(表2参照)

情報システムの復旧にはバックアップを用いるが、インシデントレベルによってはOSやアプリケーションの再インストールやハードウェア/ソフトウェアの再調達が必要になり、復旧まで時間がかかる場合もある。このような事態には有効な対策としてホットスタンバイ、コールドスタンバイといった二重化が挙げられるだろうが、実際の現場においてはコスト上の制約もありすべてのシステムに十分なセキュリティ投資ができるとは限らない。そのためにスタンダードに盛り込むべき観点が、情報システムの「復旧優先度」であり、この観点により重要箇所を絞り込んだ効果的な投資が可能となるのである。**表2**を例にとって説明すると、個人のクライアントマシンや社内利用に閉じられた情報システムは、業務復旧までの許容時間が比較的長いと考えられ、復旧優先度は0〜1あたりに位置付けられるだろう。それに対して、公共性の高いシステムや人命にかかわるシステムはより迅速な復旧が求められるため、復旧優先度は2〜3に位置付けられるだろう。

ポイント2　セキュリティインシデント発生時(サンプル4.2節参照)

セキュリティインシデント発生時は、状況が混乱しがちであるため、スタンダード作成にあたっては、次の事項に気をつけていただきたい。

1)誰がやるべき事項なのかを明確にすること
2)責任権限者を明確にすること
3)連絡体制を明確にすること

> (3)情報セキュリティ委員会は必要に応じて組織横断的なタスクフォースを設け、状況把握や対応方法の指示にあたることができる。

情報システムが業務の隅々にまで浸透している現在では、セキュリティインシデントの対応においても広報・法務・人事といった社内組織の協力が必要なケースも多い。このようなケースに備え、スタンダード作成にあたっては組織横断的なタスクフォースの招集権限を情報セキュリティ委員会に与えておく必要がある。

ポイント3　再発防止計画(サンプル4.3節参照)

> (2)情報セキュリティ委員会は発生したインシデントのうち、以下の要件を満たすものについては、再発防止計画と共に取締役会に報告しなければならない。
> <要件>
> ・社外の第三者からのセキュリティ侵害により当社が被害者となる場合
> ・顧客や取引先等の社外に対して当社が加害者となる場合

情報セキュリティ委員会や情報システム部によって検討された再発防止計画は、従業員に周知されなければならないが、特に深刻なものについては取締役会に報告し、全社的なリスクマネジメントの判断材料とするべきである。ポリシー・サンプルでは『セキュリティ方針』の中でセキュリティインシデントの取締役会への報告を義務付けているが、セキュリティインシデントは軽微なものから重大なものまで多岐にわたる。そのすべてを漏れなく報告していては、本当に重要な事項が埋もれてしまう恐れがある。そのためスタンダード作成の際は、引用例のように取締役会へ報告すべきインシデントの要件を定義しておき、軽微なものは件数だけにするなどして、ある程度重要事項を絞り込んで上層部へ報告することが現実的な方法だろう。

ポイント4　運用の見直し(サンプル5節参照)

最後に「運用の見直し」についても少し触れておく。

ポリシー・サンプル中の「訓練」とは、実際にセキュリティインシデントが起こった場合を想定して、一連の対応手順通りに疑似訓練してみることである。これにより、規定上の回復許容時間と実際の所要時間が乖離していないか? スタンダードに規定された手順に問題はないか?といった視点で運用を見直すことができる。

また5.3節で触れているようにインシデント対応が終了するつど、一連の対応手順について改善点を検討するべきである。これら日々の運用とその見直しの蓄積があってこそ、ポリシーによる情報セキュリティ施策は、よりよいものに改善されていくのである。　(寺井)

連載の最終回となる次回では、「その他いろいろなんでもござれ集」として、その他のスタンダード項目を解説する。

※この連載へのご意見・ご感想等を電子メールでお寄せください。今後のワーキンググループの励みにさせていただきます。

E-Mail:SECURITY-POLICY@yosihiro.com

サンプルを見ながら策定する
ドンと来い！情報セキュリティポリシー

最終回

セキュリティ対策の「スタンダード（標準書）」を作る⑦

作成篇__その他いろいろなんでもござれ集

スタンダードは、組織における情報セキュリティ対策の要件を具体的に規定するものであり、あらゆる組織で必要不可欠のものだ。その策定には多くの労力を要するが、JNSAのポリシー・サンプルをたたき台とすることで、それを軽減できるはずだ。前回は、スタンダードのうち、物理的な対策に関連する部分について解説した。今回は、セキュリティの運用に関するスタンダードについて、それらの構成と策定内容をJNSAのサンプルを用いて解説しよう。

筆者＝佐藤慶浩（NPO 日本ネットワークセキュリティ協会 理事）、土屋茂樹（株式会社NTTデータ）、野坂克征（株式会社シーフォーテクノロジー）、
中川裕之（日本ヒューレット・パッカード株式会社）

JNSAの紹介

JNSAは2000年4月に設立され、2001年7月にNPO法人として活動を継承しました。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を、4つの部会と各WG（ワーキンググループ）に分かれて行っています。

昨年度の主な成果物としては、「外部接続に関するセキュリティポリシーサンプル冊子」の作成、「セキュリティインシデント被害調査」におけるアンケートの実施および報告書の作成などが挙げられます。

また、複数CAの相互運用性に関する実証実験を行った「Challenge PKI 2001プロジェクト」の結果報告も、Webにて公開中です。その他の活動として、年1回の主催カンファレンスの開催（NSF2002、今年は6月12-13日に開催）、セキュリティセミナーの開催、会報誌「JNSA Press」の発行（年3回）などを行っています。

<お問い合わせ> 特定非営利活動法人 日本ネットワークセキュリティ協会
URL：http://www.jnsa.org/ E-Mail：sec@jnsa.org

本講座の読み方

まずは以下のWebサイトよりJNSAのポリシー・サンプルのファイルをダウンロードしてほしい。

http://www.jnsa.org/policy/guidance

今回は、次の4つのサンプルをダウンロードしておくとよい。

『監査標準』
『セキュリティ教育に関する標準』
『委託時の契約に関する標準』
『プライバシーに関する標準』

これらを印刷して本書の横に並べて読んでいただきたい。

本講座では、その一部を解説の必要に応じてJNSAの承諾を得て転載している。それぞれのファイルからの引用部分は、章や節の番号とともに以下のような囲み表示をしてある。

> 当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

本講座は、このようなサンプル引用に解説を加えていくことで、自社に適したポリシーを策定するための手助けを行っていくことを目的としている。

今回は『監査標準』を土屋氏に、『セキュリティ教育に関する標準』を野坂氏に、そして『委託時の契約に関する標準』を中川氏に順番に解説していただく。『プライバシーに関する標準』については、昨今の状況について簡単な説明を最後に加える。

今回もこれまで同様に、連載の第1回で紹介したモデル企業を想定したポリシー・サンプルの解説となる。そのため、解説のなかでは「企業」や「会社」などと表現するが、内容的には非営利などの組織であっても同様なので、読者の方には随時読み替えていただきたい。（佐藤）

『監査標準』作成のポイント

ここでは、情報セキュリティシステムが正しく機能しているかどうかを確認する『監査標準』作成時のポイントについて解説する。

ポイント1 監査標準の内容について（サンプル1節参照）

> 本標準では、情報セキュリティマネジメントの監査にかかわる事項を規定する。

監査標準というと、BS7799やISMSを思い浮かべてしまうかもしれないが、本来は、企業における監査の考え方、また監査人の行動指針について記述すべきものである。監査組織や監査人は、監査にあたって何を（What）監査するのか、どの程度（How）監査するのかが決まっている必要がある。何を監査するのかという問いに対しては、一般的には企業の情報セキュリティポリシーや各種スタンダードがあるかどうか、またそれらに従って行動しているかどうかを調べる。これは、特に監査標準のな

かで規定する必要はない。一方、どのように監査するのかについては、規定のどの部分（観点）を監査するのか、どの程度の深さで監査するのか、誰が監査人になるのか、問題が発見されたらどうやって報告するのか、報告書には最低限何を書かなければならないのかといった内容を決めておく必要がある。まさにこれらの目標設定が、監査標準に記述するべき内容となる。

ポイント2　監査人の選定について（サンプル4.1節参照）

（4）監査組織は、被監査組織、対象に対して独立していなければならない。もし独立した監査組織を構成できない場合には、相互監査体制をとることで、できる限り独立性を維持しなければならない。

監査は本来、すべての部門から独立した部門が実施すべきだが、企業の規模によっては人材の確保が難しい場合も多々あるだろう。一般的には以下の4つのパターンが考えられる。皆さんの組織にふさわしいものを検討してほしい。

- パターン1：外部に監査を依頼する

費用はかかるが、企業内の人材に負荷をかけなくてすむため、業務に最も影響が少なく、経済合理性は高いともいえる。

- パターン2：社内の独立した監査人が行う

内部監査の一環として、情報セキュリティに関する項目も含めることで、実施は可能となる。この場合にはセキュリティ専門の人材を新たに確保することが一般的である。

- パターン3：相互監査を行う

企業内の各部門から監査人を選定し、他部門をお互いに監査し合う。企業規模が小さすぎて常勤の監査人を確保するほどでもない場合や、企業規模が大きすぎて常勤の監査人を確保できない場合に選択されることがある。

- パターン4：自己検査を行う

チェックリストに基づき自己採点を行う。最も運用が楽ではあるが、信頼性が低い。申告された報告からサンプリングを行って実際に監査を行うという合わせ技もある。

ポイント3　監査の密度について（サンプル4.2節参照）

（4）監査組織は、計画した監査項目のそれぞれについて、問題点が内在する可能性について検討し、予測される内部統制リスクを判断した上で、実施手続きや監査のサンプリング密度を決定しなければならない。

実際に監査を行うときは、監査項目リストを作成することになるが、これはマネジメントの成熟度、事業内容のばらつき具合、求められる保証の度合いなどによって大きく変わってくる。つまり、毎回同じ監査項目を用いるのではなく、監査のたびに項目を見直すことが望ましい。

ポイント4　ネットワークの脆弱性チェックについて（サンプル4.3節参照）

（4）監査人は、システム監査ツールを使用するとき、システムへの影響に細心の注意を払わなければならない。監査時には、一般へのサービスは停止していることが望ましい。

最近は脆弱性のチェックが行えるフリーのツールが出ているので、最低限のチェックはある程度の技術力のある人であればできるようになってきた。しかし、間違った設定のままで実行してしまい、思わぬところから悲鳴が聞こえることもある。またフリーのツールは対応している脆弱性のデータベースが最新のものではない場合があるので、一般的には外部のベンダーを利用するほうが精度の高いチェックが行える（サンプル4．1（5）参照）。

ただし、これらの商用／フリーのツールは既存の脆弱情報を基に確認をするものなので、ネットワークに対するパッチ当ての管理が迅速に行われている場合には、新たな問題点の指摘には至らないことになる。

一方、最近は無断で設置された無線LANのアクセスポイントや、ひそかに構築されたRAS等も脆弱性として取り上げられているため、リスク分析に基づいて、どのような観点でのチェックが必要なのかを検討する必要がある。

ポイント5　PDCAサイクルについて（サンプル4.3節参照）

（5）監査人は、セキュリティ方針と、実際のマネジメント活動を比較して、有効性についての判断をしなければならない。判断する観点としては以下を含む。
・（途中省略）
・PDCAサイクルの適切な実施

PDCAとは、Plan、Do、Check、Actionの省略であり、計画、実行、確認、是正および改善を指す。ここで、すべての管理策が単一のサイクルで回っているわけではないことに注意をしなければならない。例えば監査を実行する場合は、監査計画→監査実行→監査報告→是正計画→是正実行→是正の確認といった具合に、PDCAサイクルは2種類回っていることになる。それぞれの管理項目において、PDCAがどれだけ実行されれば合格とするのかについては、注意する必要がある。

ポイント6　監査結果の報告について（サンプル4.4節参照）

（1）監査組織は監査結果を元に監査報告書を作成し、情報セキュリティ委員会へ報告しなければならない。

監査の結果は、概要および詳細な情報とともに報告書として提出されることになるが、単に問題点を羅列するよりも、点数付け等の指標を設けたほうが効果的である。ただし、点数付けというのはとても難しく、特定の手法として一般化されていない。そのため、点数付けにあたっては、企業に合った独自指標を作ることになる。

ここで注意が必要なのは、セキュリティを点数付けする場合、詳細項目ごとの点数の平均値を総合評価するだけではなく、最低値を選択して検討することも加えるべきということだ。なぜなら、全体的なセキュリティレベルは、そのなかで最も低いレベル程度しかないからである。ただし、中期計画のなかで段階的にマネジメントを確立していく方針の場合は、指標値として平均値をとって成熟度を見るという考え方もある。

ポイント7　是正措置について（サンプル4.5節参照）

（1）情報セキュリティ委員会は、監査組織からの報告を受けて、是正措置の計画立案をし、実行の判断をしなければならない。

監査によって発見された問題は、誰かが是正措置を講じなければならない。セキュリティ監査では、その実施および検証の責任を持つのは監査組織ではなく情報セキュリティ委員会であることが多いように見受けられる。ポリシー・サンプルにおいても、情報セキュリティ委員会が是正措置を講じるよう規定している。だが、セキュリティ以外の監査の世界を見てみると、システム監査やISO9000では、監査人が検証責任を持つこともある。また会計監査の世界においては、財務諸表に関する法定監査の是正措置は監査人の責務ではないが、SAS70監査では監査人にも是正措置に対する保証責任がおよぶ。つまり、誰がどのような責任を持つのかについては、特に決まったやり方があるわけではないということだ。そのため、皆さんの作成するスタンダードにおいても、組織独自の方式を採用して問題ないだろう。

（土屋）

『セキュリティ教育に関する標準』作成のポイント

ここからは、セキュリティの教育と訓練について規定した『セキュリティ教育に関する標準』作成時のポイントについて解説する。

●標準制定が求められる背景

セキュリティ教育・啓発に関する規定は、本講座の第1回で、「情報セキュリティ方針の説明においても記載すべき項目」とした規定である。よりよいポリシーや手順が策定されたとしても、それを実際に使用する側の認識に不足や誤りがあれば、十分な効果を得ることができない。そこで、『セキュリティ教育に関する標準』を規定することが求められる。このスタンダードは、対象者がセキュリティに対して正しい認識を持ち、それを維持し続けることを目的としたものである。

ポイント1　対象者について（サンプル2節参照）

教育、訓練の対象者は、当社のコンピュータに携わっているすべての人を対象とする。
〈例〉
教育対象者：経営者、システム管理者、オペレータ、利用者、第三者利用者　訓練対象者：システム管理者、オペレータ

情報セキュリティの適用は、社員だけでなく、その企業や組織を利用し、または管理する、すべての関係者が対象となる。この規定では、就業規則など社員に限定した規定とは異なり、情報を取り扱うコンピュータに携わる者であれば、社員であるなしにかかわらず、教育、訓練の対象となることを定義している。すべての対象者にどのような教育を行うべきか、または行う必要がないと判断するのか、最初にしっかりとした定義付けを行い、対象者に漏れがないように注意したい。

また、サンプルでは例外の規定項目があるが、対象者の部分で注記しておけば、これはなくてもよいだろう。

ポイント2　教育のタイミングについて（サンプル4.1節参照）

一般説明会
情報セキュリティ部門は、年に1回、コンピュータに携わるすべての人に対して、セキュリティに関する説明会を実施しなければならない。

サンプルでは、情報セキュリティ部門が説明会を実施すると規定している。しかし、教育の対象範囲が広い場合には、教育に関する部分に対してかなりの時間と労力が必要になることが考えられる。そのような企業では教育により力を入れる意味で、別に専門の教育担当として教育部門を設けてもよいだろう。また、「年1回」という説明会の実施においても、皆さんの組織の状況に合わせた実施時期やタイミングに書き換えていただきたい。

ポイント3　部署間の異動について（サンプル4.1節参照）

社内異動者への教育
各部署のセキュリティ責任担当者は、社内異動者に対して、異動時に、その部署の情報セキュリティに関して教育を実施しなければならない。

各部署には、固有の部外秘対応があるものだ。各部署のセキュリティ責任担当者は、このことを十分に認識した上で、社内異動により異動してきた者に対して、その部署に合ったセキュリティ教育を実施することが必要である。

また、サンプルにはないが、役職によって取り扱う情報が異なる場合は、昇格する者に対して、昇格時に、その役職に合ったセキュリティ教育の実施を検討する必要がある。

ポイント4　違反の再発防止について（サンプル4.1節参照）

再教育
情報セキュリティ部門は、セキュリティ違反者に対して、セキュリティの再教育を実施し、違反の再発防止に努めなければならない。

セキュリティ違反者に対するセキュリティ教育は、違反の再発防止を目的に行うものだ。より効果的に行うためには、例えば運転免許では、事故や違反の多い人は次の講習会までのサイクルを短く、さらに講習会自体の密度を一般の人よりも濃くするなどということを実施している。そのような例にならって、規則を遵守している者への教育と、違反を犯した者への教育について、サイクルや密度に違いを設けることも効果的である。

ポイント5　契約社員および協労者への教育について（サンプル4.1節参照）

契約社員および協労者への教育
各部署のセキュリティ責任担当者は、契約社員および協労者に対して、部署の情報セキュリティに関して、許可された権限と責務に応じた教育を実施しなければならない。

契約社員および協労者に対しては、事前に正式な契約に基づき、許可された権限と義務が決定されていなければならない。契約社員と協労者で業務内容が異なる場合は、それぞれ分けて規定することも必要になる。

また、サンプルでは、契約社員と協労者に対するセキュリティ教育を受け手側の企業で行うことを定義しているが、送り手側の企業でセキュリティ教育を行うことも考えられる。送り手側の企業との関係や、皆さんの組織の状況に合わせて書き換えていただきたい。

ポイント6　教育内容について（サンプル4.1節参照）

・情報セキュリティの問題の持つ意味を理解
・組織や個人の情報セキュリティの重要性
・セキュリティ対策
・情報セキュリティ計画
・データ所有者の責任
・モラル教育
・禁止事項に関しての教育他
・啓発

サンプルでは、教育内容を上記のように記述している。

ここでいう「啓発」では、最近のセキュリティ動向や他社のセキュリティインシデント情報などの生きた情報を用いるとより効果的である。

また、サンプルではセキュリティ対策の実施手順についての教育を「セキュリティ対策」に含めているが、別に分けて記載してもよいだろう。その他、追加すべき項目としては、事業に関係する法律の解説などが挙げられる。

職務内容や役職によって、必要なセキュリティ内容に大きな差が生じることもある。その場合は、職務内容や役職ごとに必要なセキュリティ内容の重み付けを行い、優先度が高いものを中心に、セキュリティ教育の実施を検討するとよいだろう。

ポイント7　訓練の担当者について（サンプル4.2節参照）

情報セキュリティ部門ならびに、各部署のセキュリティ責任担当者は、セキュリティに責任をもつ対象者に対し、定期的に、以下の訓練内容について、訓練資料を使用し、セキュリティの訓練を実施しなければならない。
〈訓練内容〉
・リスク分析
・セキュリティ対策についての導入、管理、運用、利用等
・セキュリティ問題の検出、検知、報告、復旧等

実際にセキュリティ訓練を実施するのは、セキュリティ方針で定めるところの各部のセキュリティ担当者もしくはその担当者に任命された者が担当することが望ましい。

ただし、あまり担当者に負荷がかかるようであれば、定期的に行う一般説明会のサイクルを短くし、そちらでセキュリティ教育を行うなど、兼ね合いを考慮するとよい。

●その他、盛り込むべき内容

ポリシー・サンプルには記述されていないが、組織にセキュリ

ティポリシーを浸透させる環境作りも大切である。例えば、対象者が自分に必要な対象項目だけを、必要なときに素早く検索できるよう、社内用のセキュリティサイトを設けるとか、情報セキュリティに関するタイムリーな情報を定期的にメーリングリストで流すなどである。ただし、あまり押し付けがましくすると逆効果になりかねないので、バランスには気を付けたい。

セキュリティ教育によってセキュリティ意識の向上および維持を図ることは重要である。しかし、対象者の意識を常に維持し続けることは難しい。対象者が継続的に取り組んでいけるよう、皆さんの組織の状況に合った、効率的なセキュリティ教育が実施できることを支援するようなスタンダードを目指してほしい。

（野坂）

『委託時の契約に関する標準』作成のポイント

ここからは、自社の業務の外部への委託について規定した『委託時の契約に関する標準』作成のポイントについて解説する。

ポイント1　趣旨について（サンプル1節参照）

> 本標準は、当社の業務を外部の業者に委託し、実施する場合の契約における問題および委託作業時の問題を未然に防ぐことを目的とする。

本スタンダードは「当社の業務を外部の業者に委託」する場合に限定して記述しており、想定する例として、情報システムの構築・運用などが挙げられる。

しかし、委託とは限らない単なる「第三者との契約」によって、企業の情報資産に外部の者のアクセスが可能になる場合も考えられる。両者を区別して考える必要がある場合は、誤解のないように言葉の定義を確実に行うとよいだろう。

ポイント2　対象者について（サンプル2節参照）

> 委託を行う全ての従業員

企業の業務を外部に委託する場合、外部の者が企業の情報資産にアクセスすることになるため、そこには多くのリスクが存在する。しかし、情報セキュリティに関する標準を社内規定として制定するならば、それは従業員に対するものであって、その効力は委託先には及ばない。したがって、委託先がこの標準に違反する行為を犯したとしても、罰則を適用することはできないのである。

このような状況でセキュリティを維持するためには、委託先が守るべき要件を、契約書で明確に規定することが重要である。この標準においても、委託先の選定と契約内容に記載する事柄を中心に遵守事項を規定する。

ポイント3　委託先の選定について（サンプル4.1節参照）

> （1）委託を行う者は、委託先として信頼できる業者を選ばなければならない。

委託先選定の資料を作成する手段の1つとして、「ヒアリングによる事後調査」が挙げられる。

委託業者が契約のとおりに業務を行ったか、自社のセキュリティを損なう行為を行わなかったか、などについて関係する従業員にヒアリングを行い、その業者の信頼度を見直し、次回以降の選定資料とするのである。つまり、委託先の選定におけるPDCAサイクルの、Cの実行である。この場合、委託業務終了後にヒアリングによる調査を行う旨をあらかじめ通知しておくと、委託先の情報セキュリティへの認識が高まり、好循環をもたらすかもしれない。

ポイント4　委託時の契約について（サンプル4.2節参照）

契約を「作業者による作業支援」に対して結ぶか、「サービス提供」を対象に結ぶかによって、審査や契約内容は異なるものとなる。

作業支援について契約する場合、その業務の性質によっては、審査時にその作業者の職歴、賞罰などまで提出を求める場合がある。

一方、サービス提供を対象にする場合は、業者と契約を取り交わし、作業者個人を特定することはなく、委託業者を信頼して最低限で済ませることが一般的だろう。しかし、その業務にかかわる人を限定して、契約を取り交わすことも可能ではある。

本標準では、作業支援の契約に基づいて、業務の委託を行うことを前提としている。

> （1）委託を行う者は、委託業務の仕様以外に、機密保持に関する以下の契約事項を盛り込まなければならない。
> ・委託業者は、当社の業務で知り得た情報を第三者に開示してはならない。

委託業者が第三者に機密を漏えいした場合、機密保持の契約を取り交わしていれば、賠償金は支払ってもらえるだろう。しかし、個人情報の漏えいなどによって一度失墜した信頼を取り戻すのは非常に困難であり、お金では代替不可能な場合も考

えられる。このような事態を防ぐために、たとえ機密保持契約を結んでいたとしても、委託業者に開示する情報を明確にし、不必要な情報は開示しないことが重要である。

また、立ち入りを許可する作業者および施設も明確にしておくべきである。サンプルには記載されていないが、これらの事柄は、できる限り契約書またはそれに類する文書に盛り込むとよいだろう。

ISO/IEC17799にもあるように、第三者に対して許可されるアクセスの種類は、論理的アクセス、物理的アクセスに分けられ、これらによって発生するリスクも異なる。委託時には、このことも考慮して、外部からのアクセスによるリスクを把握し、管理しなければならない。また、機密保持のほかに、成果物などの取り扱いは知的財産権にもかかわる事柄である。法律も考慮に入れて、内容を規定していただきたい。

（2）委託を行う者は、委託業務の仕様以外に、情報管理に関する以下の契約事項を盛り込まなければならない。

・委託業者は、当社の業務を行うにあたって情報管理責任者を明確にしなければならない。
・委託業者は、当社の業務を行うにあたって入手した情報を適切に管理しなければならない。
・委託業者は、入手した情報をリストアップし、常に授受の状況を明確にしなければならない。
・委託業者は、入手した情報を閲覧・利用できる者を特定し、明示しなければならない。
・委託業者は、電子媒体で納品する場合、ウイルスが含まれていないことを確かめなければならない。

サンプル（2）の第2項に関連して、委託先がそれらをどのように実現するか、その具体的な方法を契約時に記述してもよい。機密性の観点から具体例を挙げると、重要なファイルにはパスワードロックや暗号化を施す、記録媒体は施錠可能なキャビネットに保管し、鍵は○○および△△が持つ、などが考えられる。

第4項に関連して、作業者の変更が行われる際の手続きも契約時に定めておくとよい。「委託先が作業者を変更する場合、変更予定日の○○日前までに当社に届け出なければならない」「作業者の技能が満たない等、委託業務の実施に支障が出ると判断した場合、当社は改善の申し入れができる」などのように、問題となりそうなことは、あらかじめ契約に盛り込んでおきたい。また、作業者が作業を終了および退社した後にも機密保持義務が継続するように、委託先に対策をとってもらうとよいだろう。

（4）委託を行う者は、委託業務の仕様以外に、再委託に関する以下の契約事項を盛り込まなければならない。
・委託業者は、再委託を行うためには、当社に事前の承認を得なければならない。

委託の再委託といった委託の連鎖については、その状況を確実に管理すべきである。

委託が数回繰り返された果てに、無関係のまったく信用できない相手が委託業務を請け負っていた、という笑い話にならない実例もある。再委託を承認する際の基準は、資本関係があるか、契約のみの関係かなど、再委託先との関係によって異なるだろう。

再委託によるセキュリティの質の低下を防ぐために、「委託業者は、再委託を行うにあたって、当社の契約書の文面を使用しなければならない」という条項を加えてもよい。ただし、ここまで規定すると情報セキュリティ以外の観点にも関係してくるので、その際には契約を担当する部署と調整を行うべきだろう。

●その他、検討すべき内容

委託先に遵守してもらうべき事項として、本スタンダードでは「機密保持」「情報管理」「品質管理」「再委託」の4つに分けて項目を記載したが、この個所を他のスタンダードに関連付けることも可能である。

具体的には以下のように行う。まず、「委託先は、以下の標準で定められた事項を遵守しなければならない」として、該当するスタンダードをその下に列記する。列記したスタンダードの遵守事項を抜き出して、社外の人を対象にした文面になるように編集し直し、別文書を作成する。契約書には、その別文書を参照するような文を記載すればよい。（中川）

『プライバシーに関する標準』改善へのコメント

サンプルでは「プライバシー」と題したが、昨今では「個人情報保護」と呼ぶほうがよいだろう。サンプル作成時には間に合わなかったが、JNSAの個人情報保護についてのワーキンググループや情報ネットワーク法学会（http://www.in-law.jp/）における法律の観点での勉強会の情報を参考に内容を検討していただくとよい。本格的に取り組むのであれば、プライバシーマーク認定制度（http://privacymark.jp/）がある。

本講座での情報セキュリティポリシーの解説は、これで最後である。スタンダードの文書を構成するには、これまで解説してきたスタンダードのほかに、付則として以下の3つがJNSAのサンプルにある。これらを加えて標準を完成させていただくとよい。

『罰則に関する標準』
『スタンダード更新手順』
『プロシージャ配布の標準』

※この連載へのご意見・ご感想等を電子メールでお寄せください。今後のワーキンググループの励みにさせていただきます。
E-Mail：SECURITY-POLICY@yosihiro.com

NPO日本ネットワークセキュリティ協会会員　行動指針

NPO日本ネットワークセキュリティ協会は、ネットワーク社会の情報セキュリティレベルの維持・向上及び日本における情報セキュリティ意識の啓発に努めるとともに、最新の情報セキュリティ技術および情報セキュリティへの脅威に関する情報提供などを行うことで、情報化社会へ貢献することを目的としております。

そのため、以下の通り会員の行動指針を定め、規範とするよう努めます。

会員は、この指針の遵守に努め、会の目的を共有するにふさわしい姿を目指します。

1. 自ら情報セキュリティポリシーを定め、他の手本となるような運用に努めます。
2. お客様の情報などの重要情報に関して、その取扱い手続きを明確にし、管理するように努めます。
3. 自ら取り扱う製品およびサービスについて、その情報セキュリティレベルの維持・向上に努めます。
4. 自ら公開するインターネットサイトおよびメール等のサーバ類について、その情報セキュリティレベルの維持・向上に努めます。
5. 情報セキュリティに関連する法規・法令等を遵守します。
6. 自らの構成員に対して、情報セキュリティポリシー及びその実施手順について教育・訓練を繰返し実施することに努めます。
7. クラッキングなどの不正行為を許さず、その撲滅に努めます。

NSAの活動について

インターネットを中心に情報ネットワーク社会が形成されていく中で、ネットワークセキュリティは必要不可欠なものになっています。JNSA（日本ネットワークセキュリティ協会）は、2000年4月に任意団体として設立し、2001年7月にNPO（特定非営利活動法人）として承認されました。現在は4つの部会に分かれて、ネットワークセキュリティに関する啓発、教育、調査研究および情報提供などを幅広く行なっています。

主な活動としては、政策部会でのセキュリティインシデント被害調査、個人情報保護ガイドラインの作成、セキュリティ監査基準の策定など、技術部会でのポリシー・サンプルの策定、無線LAN相互接続実験、PKI相互運用実験など、教育部会での産学協同プロジェクトによるスキルマップの作成、マーケティング部会での年に一度のセキュリティカンファレンスの開催、会報誌の発行、セキュリティ啓発CD-ROMの作成等を行なっております。

連絡先

特定非営利活動法人 日本ネットワークセキュリティ協会
〒136-0075
東京都江東区新砂1-6-35 T.T.ランディック東陽町ビル 1階
TEL 03-5633-6061　FAX 03-5633-6062　E-Mail: sec@jnsa.org
URL: http://www.jnsa.org/

西日本支部
〒530-0047
大阪府大阪市西天満2-3-14 西宝天満ビル4階（株）ヒューコム内
TEL 06-6362-2666