情報セキュリティ方針（ポリシー）の必要性と策定方法
～ 企業は従業員(人)による情報セキュリティの維持に、どう対処すべきか ～

佐藤　慶浩
日本ヒューレット・パッカード株式会社

セキュリティに関する書籍や資料の中で、セキュリティ方針(ポリシー)という言葉を目にすることがあるのではないだろうか。その言葉の意味から、なんとなく重要そうなものであることは想像できると思うが、それが実際にどんなものであるかが説明されることは意外に少ない。セキュリティ方針を策定し、かつ日本企業でそれを運用するためには、その必要性を理解しセキュリティ方針の定義を日本の組織文化に合ったものとしてフレームワーク化しなければならない。ここでは日本企業におけるセキュリティ方針の策定と運用について解説する。

The needs and building of Information Security Policy
～ Planning the scheme how to enforce corporate's requirement of Information Security on people ～

Yoshihiro Sato
Hewlett-Packard Japan, Ltd.

You may assume that Security Policy is something of important by the meaning of itself, during reading the word of it on books and articles regarding to information securities. There was, however, no chance of describing what the Security Policy meant in real. It was known only by whom have actually build it by themselves. In order to build the Security Policy and then to maintain it in Japanese organization, you must understand the reason why it is important and make a framework which meets its positioning to chemistry of Japanese organization. This report explains about the definition, needs and building of Information Security Policy.

セキュリティ方針のレベル

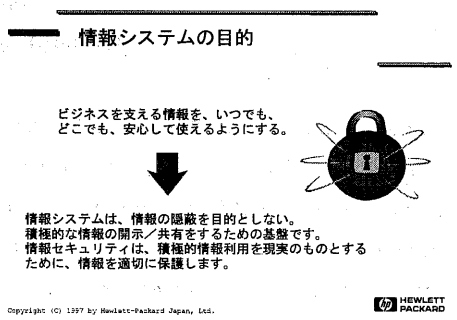
セキュリティ方針とセキュリティポリシーはまったくの同義である。しかし、セキュリティ方針と言った場合、その定義にはレベルがあって、企業全体のセキュリティ方針、それから部門のセキュリティ方針そしてコンピュータシステム単体のセキュリティ方針というように様々なレベルがある。これらのレベルを正しく理解しておく必要がある。それらのレベルは３段階に大別できる。もっとも下のレベルは、装置やソフトウェアなどの方針に関するもので主として技術的なことだけを言及するものである。これに加えて、運用や管理方法などのプロセスまでを含めた２番目の段階のレベルがある。日本で多く知られているのは、この段階までである。しかし、この段階では人々の行動規範までは言及しないため、それについては通常は非電子的情報を対象と

する既存の規定文書などを拡大解釈して済ませることになる。しかし、今日の情報システムはビジネス活動と密接なものとなっており、例外処理の発生するビジネスの現場においては、ビジネス目標の達成と情報セキュリティ維持とのトレードオフを個人が判断することは、技術やプロセスとは異なるセキュリティの問題を生み出している。この問題を人的領域として方針化するのが、３番目のレベルである。技術とプロセスと人を扱う、この最上位に位置するセキュリティ方針を情報セキュリティ方針という。本書では、この企業全体の情報システムに関するものという定義での「情報セキュリティ方針」について説明する。紙面の都合上、以後、単にセキュリティ方針と称することにするが、本書ではそれらはすべて「情報セキュリティ方針」を意味する。

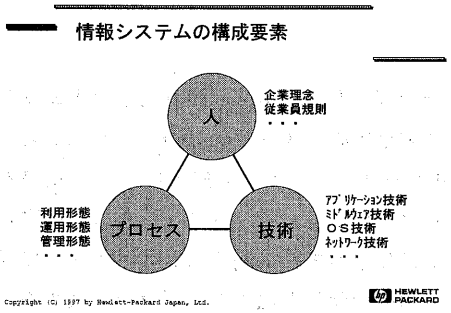
情報システムの目的

情報システムの目的は、ビジネスを支える情報をいつでも、どこでも、安心して使えるようにすることと考えることができる。情報システムそのものは情報の隠蔽を目的とするのではなく、積極的な情報開示や共有をするための基盤である。積極的な情報の開示や共有をするための手段として情報を保護する必要があるが、保護することが目的ではない。情報セキュリティは、定められたセキュリティの要件を満たしつつ、積極的な情報の開示、共有をするために、貴重な情報を正しく守るということである。

従業員のアクセスが制限されるものは社内の全電子情報の１０％にも満たないのではないか。当社のなかではもっと低く、全電子情報のうち全従業員が共通には見れないものは５％くらいである。ほとんどの情報は従業員が見れる、そのうちお客様に提出することができる情報が８～９割を占めている。このように、情報の保護ではなく情報の開示／共有を目的として情報システムがあると考えている。



情報システムの構成要素

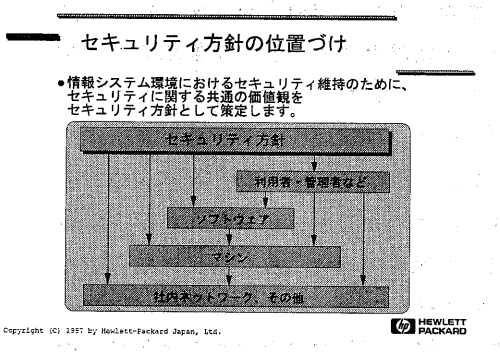


情報システムの構成要素を考えると、ハードウェア、ソフトウェア、アプリケーションなどの技術があり、これを使うのが人で、人が技術をつかうためにプロセスがある。技術に関しては、アプリケーション技術、ミドルウェア技術、ＯＳ技術、ネットワーク技術などがあり、人に関しては、たとえば企業理念とか従業員規則などがつかさどっている。人と技術を結び付けるものとしては、コンピュ

ータの利用形態であり、利用形態から利用手引書があったり、運用手引書、管理手引書があるということになる。情報システムは、技術・人・プロセスから成り、人が絡んでいることを忘れてはいけない。

セキュリティ方針の位置づけ

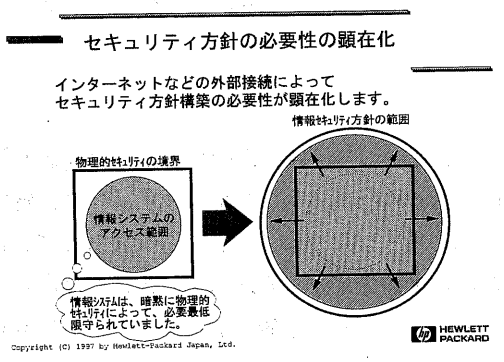
人が絡むことから、最初に必要となるものがセキュリティを維持するための共通の価値観である。セキュリティとは何なのかという価値観、それを定めるものがセキュリティ方針である。メインフレームのようなホスト型情報システムでは、ユーザのできることは限られていた。システムの開発者が設計した画面の中で、決められた手順で情報を処理していた。このためシステム管理者がセキュリティ上好ましくないと考えることは、その手段を提供せず、また、手順書においての禁止事項として細かく指示することができた。つまり、集中的な制御が可能であった。しかし、近年のオープンシステムを組み合わせたシステムでは、ユーザの自由度は飛躍的に広がっている。例えば、業務連絡や社外の取引先との連絡に電子メールを使うといった場合、機密情報が社外に流出することは、故意にも過失にも容易に起こり得ることである。電子メールを技術として使い、それで業務連絡というプロセスを実現した場合、セキュリティの維持には「人」が重要な要素として関わってくる。情報システムが特化型のものから、より汎用化したものになる傾向は、近年のビジネスの目標達成に必要なことである。汎用化することは、ユーザによるシステム利用の自由度があがったことを意味する。以前のように画面上のエントリ内容を制限することで、集中的に制御することは困難になったのである。このような環境において、セキュリティ維持をするには、技術や手順だけを制限するのではない、もっと人の行動規範に視点を向けた枠組み、すなわち、情報セキュリティ方針が必要である。



情報セキュリティの背景

情報システムのセキュリティは元来あたりまえのものであり、コンピュータが出てきたときから既に存在していた。1950年代にホストコンピュータが商用で使われ始めたときからシステムのセキュリティは誰かが考えてくれていたわけである。しかし、物理的に外部と遮蔽された環境においては、従業員の個人的なモラルや技術力に依存したセキュリティの維持はある程度機能していても、インターネットなどによって外部と接続されるようになると十分ではなくなる。企業に損害を与える要因が多くなってくるからである。

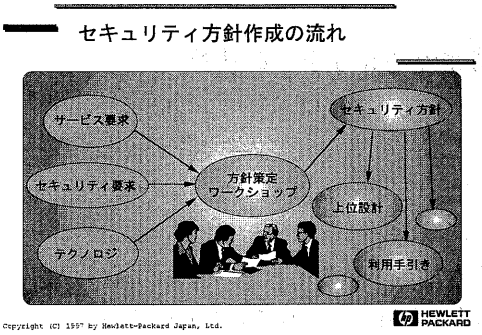
セキュリティ方針の必要性の顕在化



従来のホストコンピュータシステムでは、基本的に情報システムのアクセス範囲は物理的なセキュリティの境界の中に存在していた。物理的なセキュリティの境界とは建物のセキュリティや警備員などである。その中にいる限りは情報システムは暗黙に必要最低限は守られていた。たとえば社外秘の情報を机の上に置いていても、建物自体は警備会社によって保護されているために、それが社外の人に見られるということはない。電子情報も同じで、物理的なセキュリティの中にある限りはある程度ルーズであっても、それがすぐに問題にならないことも多かった。しかし情報システムのアクセス範囲が広がってきて物理的なセキュリティの境界を越えてしまうようになると、情報セキュリティとして守る壁を用意しなければ攻撃の対象になってしまうことが起こってきた。情報セキュリティというものを利用者個人が直接考えなければいけなくなり、セキュリティ方針策定の必要性が顕在化してきたわけである。また、近年の企業環境として正社員以外の契約社員や雇用員などによる情報システムの利用もセキュリティの新たな課題である。

セキュリティ方針作成の流れ

セキュリティ方針を策定するには、サービス要求とセキュリティ要求をバランスさせることが必要である。たとえばインターネット接続をして社外とメールをしたい、あるいは web から情報を取ってきたいという場合、インターネットに接続して社外から全く攻撃を受けなくするという解はない。そのためにはインターネットに接続しないということだが、そうするとサービスが成り立たなくなる。このバランスを取るためにテクノロジーが介在する。すなわちファイアウォールというテクノロジーができたからインターネットに接続してもセキュリティがある程度守られて、社外と電子メールのやり取りができるわけである。セキュリティ、サービス、テクノロジーの３つのバランスを考えながら検討を進め、出来上がったものがセキュリティ方針となる。このセキュリティ方針がユーザ向けの利用手引きやアプリケーションの開発指針(ガイドライン)に展開される。



重要なことは、サービス要求が本当に満たされるのかについての同意を十分に取っておくことである。たとえば、一番厳しい認証の仕組みとして全ユーザーが個人認証を受けるとする。いったん認証されればその人は権限を与えられた情報にいくらでもアクセスできサービス要求は満たされるが、認証を行っているセキュリティサーバーがダウンしたときに何が起きるかを想定しなければならない。全ての情報にアクセスできなくなり、手元のＰＣすら使えなくなった場合にどう対応するかは、非常に難しい問題である。明日までに営業活動用の資料を作らなければいけないのに認証システムが壊れた時、一人は、会社のセキュリティ方針として認証ができない限りはコンピュータリソースを使ってはいけないということなので、それを守り、知っている範囲内でワープロ書きだけをして失注した。別の一人は、認証装置を外して勝手にコンピュータを使い、結果的に十分な資料が作れたために受注したといった場合、どちらが責められて、どちらが誉められるべきかということはセキュリティ方針として事前に議論されているべきである。せっかくセキュリティを守っても営業成績が悪いということで査定が悪くなったとしたら、セキュリティ方針を守ることがばからしいことになってしまう。この部分のバランスも考えておく必要がある。

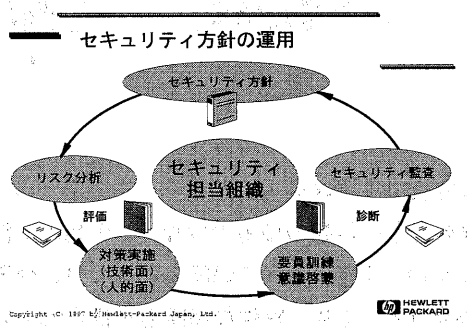
受け入れるリスクとのトレードオフ

明日の営業利益とセキュリティのどちらを取るかといった場合、それが現場任せになってはいけない。つまり、このときにトレードオフされるのは、直接的には生産性ではなくリスクの受容であるという認識が肝要である。そのため、これを解決するためには経営会議レベルでの承認が必要であると考えるべきなのである。

セキュリティ方針は、企業におけるセキュリティ目標についての経営陣からの意志表明である。セキュリティ方針と規則集との違いは、規則が単に従業員に対して行動を強いるのに対して、方針は従業員に対する支援体制が示される点である。

重要なことは、「明日の営業活動に支障があるとしても守らなければいけないことはどこまでなのか」ということを方針策定の段階で議論しておかないと、結果的には誰も守ってもらえないものになってしまうということである。その価値観を作るのがセキュリティ方針である。

セキュリティ方針の運用



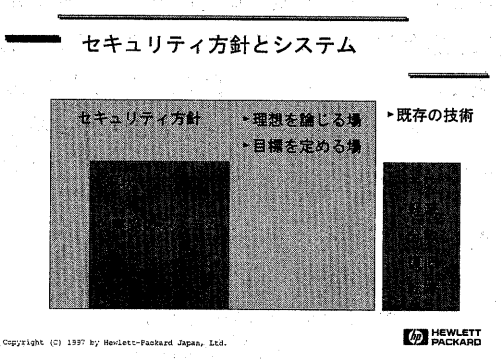
セキュリティ方針ができると企業としての目標が定まるので、その目標に対しての現状である情報システムセキュリティのリスク分析が行われる。この分析によって具体的な実施策を作っていくことができる。対策実施に関しては、技術的側面と人的側面がある。技術というのは設定すれば設定したとおりにコンピュータや装置が実行するが、人に関しては手順書を書いても手順書どおりやるかどうかはわから

ない。このため人に関しては要員の訓練、意識啓蒙が必要になってくる。また対策の実施、要員訓練、啓蒙が正しく行われているかはセキュリティに関する監査で評価する。監査の結果、方針に不十分なものがあれば方針を更新することもある。新たなリスクが出てきたらリスク分析を行う。たとえば、手順書を作っているのに従業員が守っていないということであれば、要員訓練を徹底するということで、方針に沿うように戻していくことができる。セキュリティ方針なくしてセキュリティ監査を実施すると、それは監査ではなく調査に終わってしまうことも、セキュリティ方針の策定の必要性を示唆するものである。このように、セキュリティ方針の維持は運用の対象であることを忘れてはならない。

この中核に情報セキュリティの担当組織というものを位置づけることができる。これは責任を持たされてやる仕事であり、セキュリティを責任担当としてやるということである。しかし、必ずしも部署名が必要だということではなく、営業、情報システム、開発などから選抜して、定期的に作業を行なうセキュリティ担当タスクフォースを作ってもよい。いずれにしても、個々人の動機付けで行なうのではなく、正規の業務として運用することが重要である。

セキュリティ方針の定義

既に情報システムができあがってビジネスをしている企業において方針策定の段階で、実際のシステムはセキュリティ方針をすぐに満たす必要はない。つまり、現状が全てを満たすような限られた条件の中で方針を策定すべきではない。セキュリティ方針は自分の会社のセキュリティに関しての理想を論じる、あるいは目標を定める場にすべきである。そうでないと、結果的にセキュリティ方針の更新の頻度が多くなり、また経営層の承認を取るのが難しくなってくる。



方針が承認された後のセキュリティガイドラインを作成する上での観点として、一般的なリスク管理と同様に、予防、軽減、分散、復旧、転嫁がある。まずはセキュリティの問題を予防し、万一セキュリティに問題が起こってしまったら何らかの軽減をしなければいけない。それから、応急処置が終わった後には、復旧をする。復旧のためには予め何らかの事を分散しておかねばいけない。さらに復旧で計画予算以外のお金が出てしまったということに備えて保険がある。ただし、保険は現状では情報システムセキュリティについてはほとんど機能しない。なぜならば、一般的に保険の対象は情報の価値ではなく、労働の工数になっているからである。付加価値は査定してもらえない。また、通常の保険の約款では、企業内でセキュリティ侵犯があった場合には保証の対象外となる。近年、特殊な保険も準備されているが、一般的には、情報システムのセキュリティの転嫁は非常に難しい。

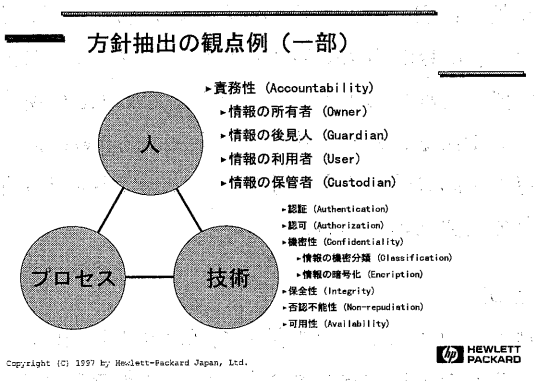
重要なのは「セキュリティを守るのは常識だ」という言葉で済ませてはいけないということで

ある。なぜ自分の会社がセキュリティに取り組んでいるのかを論じないといけない。営業マンにとってのセキュリティの常識と、情報システムにとってのセキュリティの常識というのはまだまだ違う。コンピュータ上に倫理観というものが確立されれば「セキュリティを守るのは常識だよ」という言葉ですませられるかもしれないが、セキュリティの常識という言葉は人によって、部署によって、部門によって違う。この意味で、セキュリティ方針を考える時に企業では必ずこれを論じておかないと、実際には理想も目標も違うものになっていく。その観点からもセキュリティ方針を作らなければいけない。

セキュリティフレームワーク

セキュリティに関するコンポーネント群の関係を整理し、系統立てた構造を有するセキュリティ方針のことを当社ではセキュリティフレームワークと呼んでいる。方針とフレームワークとは包括的な関係になっている。

セキュリティフレームワークは先頭に「序説」、次に「目的」、ビジネスに対して普遍の事柄を定義した「原則」があり、「運用方法」、「方針」となる。個々の方針は非常に端的なもので、通常２ページくらいに収める。普通の企業でコンピュータシステムを構築しようとすると、方針のステートメントは３０～４０くらいだが、ブレイクダウンをどこまでやるかという問題でありカテゴリーでまとめてもよい。人とプロセスと技術を考えなければいけないと言ったが、システム関連の人はエンジニアなので技術のところは容易にブレイクダウンできるが、人に関して何を考えていけばいいのかは難しい問題だと思う。人の観点で物事を考える際の切り口としては、情報の所有者、利用者、情報サービスの提供者の３種類がある。情報サービスの提供者としての立場、あるいは情報システムの利用者の部分はある程度分かるが、所有者の立場も忘れてはならない。この所有と利用と提供という言葉は、技術者にはヒントになるのではないか。



具体例（序説）

内容を見てあまりに当たり前な文章でがっかりするかもしれないが、セキュリティ方針がどんなものかの具体例として紹介する。ここでは紙面の都合上、序説の全文ではなく一部を紹介する。ただし、ここで紹介する例は、これからセキュリティ方針を策定しようとする方々にとってのたたき台にはならないし、推奨例にもならないことに注意していただきたい。その理由については、後程説明する。

序説には「このフレームワークはセキュリティ維持に必要な指示を設定し、広範に用いる手引きを提供し、社内でのセキュリティ関連の施行への参画を上級管理職が支持していることを明らかにする」とある。この文章では、セキュリティに関して自分の業務として参画するということについて会社が経営会議でそれを支持している、セキュリティ維持に時間を使うことは業務だ、ということを会社が認めていると文章で宣言する。

次に「このセキュリティ方針のフレームワークが存在しており、従業員に対して継続的に教育をすることは、情報が不正に扱われた際に、企業自身を法的に保護する上でも必要です」という文章がある。これは、何か事が起こった時にそれが再発防止できるということを論理的に言えるように、それがこの「法的に」という言葉に表れている。これは必ずしも従業員の責任を明確にして、問題を起こした従業員を首にするぞという意味ではない。たとえば、方針の目標と現実とは違うので、セキュリティを一生懸命やっても間違って機密情報が外に出てしまったとする。それに対して、再発防止の方策を対外的にメッセージとして出せなければいけない。

法律的には機密として扱われたものが機密情報だと定義されており、機密維持の努力を説得できないと、情報が不法に利用されたのではなく、機密保持に必要な業務を怠ったのだとして、一方的に責められてしまうことになる。これは誰も運用していないセキュリティ方針があるだけでは不十分であることを意味する。また、従業員に対して継続的な教育をするということは、たとえば毎年１回説明すると中途で入ってきても必ず１年以内には方針を知るチャンスがある、ということで重要なのである。

まとめ

完成したセキュリティ方針の文章は当たり前の内容となることが多い。しかし、セキュリティ方針はそれを策定するために企業内で部門を超えて議論し共通の価値観を見出すという過程に、むしろ重要な意味がある。よその会社の経営方針を文章としてだけまねる者はいない。また、セキュリティ方針は絶対的に必要かという問いへの答えは、経営方針なくして営業活動ができないかという問いへの答えと通ずるものがある。セキュリティ方針もまた同じで、他から文章を借りてくるだけでは意味がない。自分の企業で議論して作成してはじめて意味のあるものになる。

以上のようなことを議論する策定作業の運営にあたっては、最新の技術知識や、技術的なことに加えてディスカッションにまつわるスキルを必要とする場合があるが、そのような部分は社外からの協力をコンサルティングとして得ることも検討できるであろう。

コンサルティングとしては、セキュリティ方針のたたき台を示して提供するのは比較的やさしい。しかし、それでは、その企業にとって実際に運用されるようなセキュリティ方針にはならない。当たり前と思っていることが、なぜ当たり前なのかをディスカッションするその過程によって、その言葉や言い回しは企業ごとの文化を反映し、全従業員が「セキュリティを守るのは当たり前」だと思える文章に仕上がると考えている。

ここでの説明が情報セキュリティ方針の策定のきっかけや参考になれば幸いである。