10'00"00 インターネット10分講座

MIN SEC 1/100S INTERNET

経営実務（業務執行）視点に立ったセキュリティ対策～サーバールームから役員室へ～

この「インターネット10分講座」では、インターネットの基礎的な技術について掘り下げてお伝えすることが多いですが、今回はいつもと少し趣向を変えて、経営実務の視点で考えるセキュリティ対策について取り上げます。「セキュリティ対策の重要性」が声高に叫ばれる中、本稿は、セキュリティ技術者にはもちろん、管理部門や経営層の方々にとっても、真に有意なセキュリティ対策を考える上でのヒントになるのではないかと思います。

セキュリティに関わる事件や事故が連日のように報道されています。これらの報道を見ているだけでは気づきにくいのですが、データを調べていくと想像以上に深刻な状況が見えてきます。セキュリティへの懸念は、単に対策への投資を求められるばかりでなく、新しい技術の導入を見送る大きな要因ともなっています。

長らく、セキュリティ対策は、「ネットワークの分離」と「アンチマルウエア（アンチウィルス）などのセキュリティツールの適用」が基本的なフレームワークとされてきましたが、このフレームワークでは、現状の脅威への対策ができないばかりではなく、利便性と生産性を犠牲にすることが求められます。しかし、今、企業や組織に求められるのは、ITの利用を犠牲にすることではなく、セキュリティを利便性や生産性と共に高めることにあり、組織の経営や事業に対するITの貢献と、これを支えるためのリスク対策を明確に示すことです。

一方で、「セキュリティによる経営に対する貢献」と言われても、技術を中心に業務をしてきた人間にとっては、それがどのような”ゲーム”であるのか、つまり企業経営における業務執行（オペレーション）とは何か、が分からないことが多いと思います。本稿では、筆者がセキュリティベンチャー企業で体験した、コンサルティング事業の事業責任者やCIO（最高情報責任者）として経営に参加した経験の中で、自分なりに理解した技術系の人間が経営を考える際に求められる視点をご紹介します。

◆ マネジメントという言葉について

日本でマネジメントという言葉を使う場合、人事管理や庶務管理を意味することが多いように思います。これに対して、米国企業で使うマネジメントは、経営や付随する数字の管理を意味する業務執行（オペレーション）を指すことがほとんどです。ちなみに、日本では、COO（最高執行責任者）という役職はあまり馴染みがありませんが、COOは業務執行という経営の中核を統括する重要な役職になります。

マネジメントの違いを理解するためのメタファーとして、佐々淳行氏の例え話※1をよく使わせていただいています。佐々淳行氏によれば、米英のリーダーシップは、狩猟（マンモス狩り）が基本なので、獲物が捕れないと村人が飢えてしまうため、リーダーは殺されるか追放されてしまいます。そして、獲物が捕れた場合でも、分配を間違えるとやはり殺されることになるので、事前に何をすれば、どれだけの分配があるのか決めておきます。外資系企業で働いていると、ロールやコミットメントという単語がよく出てきますが、これら言葉の背景に、この見方を当てはめると理解しやすいと思います。筆者自身の経験ですが、初めて米国企業に入社した当日に、突然「A社の案件をどちらにするか決めてください」と言われて戸惑ったことがあります。「まだ状況が把握できていないので、ここで私が決めるのは難しい」と言うと、「マネージャが決めないで、誰が決めるのですか?」と心底不思議そうに言われました。

これに対して、日本のリーダーシップは、農耕を基本とした調整役という側面が強く、日照りなどで凶作になったとしても、リーダー（村長）が殺されることや追放されることはありません。「日本企業に成果主義は合わない」と言われることがありますが、成果主義の導入に失敗した事例の根底には、このようなモデルの違いを理解していないケースが多いと考えています。調整型のマネジメントのままで、評価だけを狩猟型にしても良い成果は出ないと思います。

※1「平時の指揮官、有事の指揮官」佐々淳行著 1995年4月1日 株式会社クレスト社発行

◆ セキュリティの二つの切り口

「セキュリティと経営」という話題になると、多くの場合、事故や事件が起きたときのビジネスインパクトが主要な論点となります。もちろん、ビジネスインパクトは重要な視点なのですが、起きてもいない突発事態（異常系）の話を経営に組み込むことは難しいと考えています。セキュリティを経営に組み込んでいくためには、セキュリティを異常系ではなく、正常系として業務に組み込むことが重要で、そのためには「ガバナンス」という視点が有効だと考えています。この違いについては、アメリカ合衆国の連邦法である「上場企業会計改革および投資家保護法（Sarbanes-Oxley Act of 2002、以下、米国SOX）と、日本の「（金融商品取引法が規定する）内部統制報告制度（以下、JSOX）」と呼ばれる制度に関する私見をご紹介します。

米国SOXは、Enron社やWorldcom社等の経営者と監査法人が深く関わった不正行為の再発防止を目的として制定された連邦法です。私が勤務した日本法人も米国SOXの監査対象となり、CFO（最高財務責任者）と共に監査を受けることになりました。

監査では、財務会計にかかわる一連の動きを明らかにするワークフローと、ワークフロー上で利用されるシステムのアカウント管理が主要な対象でした。つまり、内部不正を防止する仕組みを保証するための仕組み（Application Control：業務処理統制）が適切に実装されていることに対する監査が中心ということです。これに対して、JSOXでは技術的なセキュリティを中心とした仕組み（General Control：全般統制）が中心のように見受けられます。昨年2015年に大きな話題になった日本年金機構の事件についても、本来であれば米国SOXが唱えるようなガバナンスの視点に基づいた言及が必要だと考えるのですが、そのような視点での議論は専門家の間でもあまり聞いたことがなく、ネットワーク分離やマルウエア検知の有無といった、要素技術の議論に終始しているように思います。

このように、セキュリティ対策には「全般統制」と「業務処理統制」の二つの切り口がありますが、全般統制を中心とした不正アクセス対策では、経営的な視点でセキュリティを議論することが難しいと言えるでしょう。経営にセキュリティを組み込んでいくためには、業務処理統制を中心としたガバナンス、つまり事業や業務執行におけるITとセキュリティのあるべき状態（正常系）を定義することが不可欠だと考えています。

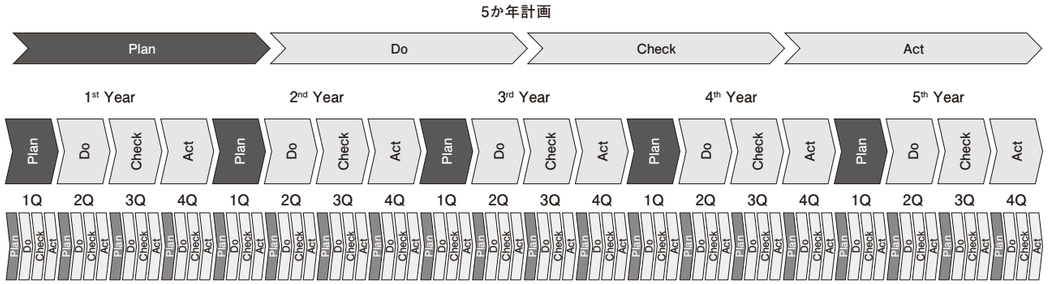
◆ 経営サイクルでPDCAを考える

セキュリティが経営の一部になるには、当然ながら経営サイクルをベースとすることが必要だと考えています。そして、経営サイクルをベースにすることで、マネジメントサイクルとしてのPDCA（Plan-Do-Check-Act）が見えてきます。

一般的な経営では、複数の事業が走っていても、毎年一つの事業計画が策定され、（例えば）四半期ごとに結果を評価し、年間の計画を守るための対策や修正（下方修正、上方修正）などの事業計画の見直しを行います。

セキュリティについても、同じ経営のサイクルに沿って、計画の立案、結果の評価、対策や修正が必要です。事業計画にも乗らず経営会議でも議論されない状況で

－経営サイクルのPDCA－



は、経営の一部になったとは言えないと考えます。そして、経営のサイクルに乗せていくためには、数値化・指標化が不可欠です。

◆ 簡単なことから数値化する

何を数値化すればよいのかは、正解のない問いかけかもしれません。まずは自らが数値化できるものから数値化し、これを指標として評価を続けることが、より適切な答えを得るための鍵になると考えています。簡単な数値化もできない組織が、高度で素晴らしい数値化や、それに基づいた評価ができるはずはありません。セキュリティからは少し外れる部分もありますが、例として、筆者が米国企業の日本法人でCIOを務めた時の経験をご紹介します。

筆者がCIOに就任した当初、実は「我々は徹夜も当たり前で、こんなに頑張ってます!」という意味での残業時間くらいしか、経営会議に報告できることがありませんでした。これに対して、「残業が多いのは能力がないからではないか」という問いかけと、「そもそも、ITのトラブルが多すぎる」という指摘を受けました。IT部門が管理する各システムの稼働率はそれほど悪い数字ではなかったのですが、日本の営業時間帯に故障が起きると、タイムゾーンの違いから対応に時間がかかり、日本ではまったく仕事にならないケースも少なくなく、この状況がIT部門に対する不信感の要因となっていました。日本法人でできることはキッチリとやっており、責任も果たしているとの意識もあったのですが、議論を進める中で、それを示す数字がどこにもないことに気が付きました。

そこで、いくつかの簡単なシステムを作り、利用者目線での稼働率を計測することにしました。その一つは、定期的にメールの送受信を行い、配信に要した時間を記録し、一定時間以上に遅延が生じた場合には、米国の本社を含めた関係者に警告を送付するというものです。これだけのことなのですが、利用者がトラブルに気付く前に手が打てるようになり、トラブルが日本の営業時間が始まる前に解決することも増え、クレームは劇的に減少しました。そして、経営会議においても、システムの稼働率を客観的な数字で提示し、業務と成果を協議するための共通の基盤を作ることができました。

◆ 事故対策としてのヒヤリハット

同じ頃に、数値化を考える上での重要なヒントとして「ヒヤリハット」を教えていただく機会がありました。ヒヤリハットは、「一つの重大事故の背後には29の軽微な事故があり、その背景には300の異常が存在する」という、ハインリッヒの法則に基づいた労働災害防止のための考え方です。重大事故は発生頻度が低くコントロールが難しいことから、300の異常に着目し、これらを管理していくという試みと言えます。

私がセキュリティ面で実施したことの一つに、システムやネットワークの監視を行い、ポリシー違反などの問題があった場合にはプロセスに従った対処を徹底する、というものがあります。もちろん、取るに足らないような違反もあるのですが、当事者ばかりではなく、関係者に問題行為であることを認識させることで、問題行動をやめさせ、重大な事故を未然に防ぐ効果があったと考えています。また、問題状況を指標化することにより、教育や啓発の課題、ポリシーを順守できる状況にあるのか、ポリシー自身の合理性はあるのか等を評価することが可能になりました。

セキュリティを経営的な視点で扱うためには、このように「数値化」が鍵となりますが、ここで重要なのは「コントロールが可能な数値に着目すること」です。例えば、「情報漏えいを起こさない」という目標をそのまま数値化した場合、事故が起きるまで は「0件」という数値が並び、事故が起きたときに突然「1件」という数字に変わります。「0件」を管理しても、何の対策も見えてきません。管理可能で適切なKPI（Key Performance Indicator：重要業績評価指標）を見つけていく必要があります。

適切なKPIの設定はなかなか難しいのですが、バランススコアカード（BSC：Balanced Score Card）と呼ばれる業績評価の手法では、財務の視点、顧客の視点、業務プロセスの視点、学習と成長の視点から、KPIを構造的に分析します。ヒヤリハットの考え方やBSCは、セキュリティが、どのように経営に関わっていくかを分析し、提示していくための良いツールの一つだと考えています。**（表1）**

◆ 結び

昨今の大きな事件を受けて、セキュリティは「サーバールームから役員室へ」と言われるようになっています。これは、セキュリティに係る人たちに対して、役員室で議論できる経営的な視点がより求められるようになったと言うことができるでしょう。

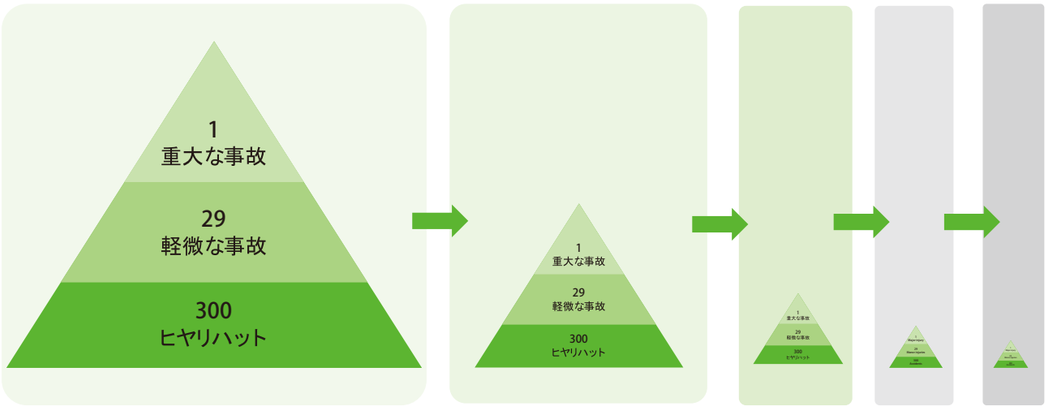
一方で、セキュリティを担当している人たちが、本当の意味で経営陣と話し合いができる機会はまれで、唯一の機会はセキュリティ事故が起きたときではないかと思います。しかし、事故が起きてからでは遅いので、事故を想定した具体的な演習を設計していくことが、組織として経営の中にセキュリティを組み込んでいく、良いきっかけになるのではないでしょうか。

これまで、セキュリティ対策は、ワームやウィルス対策を脅威の中心としたものが多かったこともあり、セキュリティ製品やグローバルスタンダードと言った、「組織外」に答えがあると考えられてきました。しかし、脅威が明確な目的を持った昨今の標的型攻撃等に変化した現状では、「組織内」の状況にしか答えはありません。事故を想定した演習は、「組織内」の状況を明確にし、組織全体でのセキュリティ対策を進める重要な機会になると考えています。

今や、セキュリティを、単に担当者や技術上の問題ではなく、企業や組織の経営の一部として捉えることは不可欠です。そして、経営者がセキュリティを理解することを待つよりは、セキュリティに関わる人たちが経営に関与する機会を増やしていくことが重要だと考えています。

（日本マイクロソフト株式会社
チーフセキュリティアドバイザー 高橋正和）

ー ハインリッヒの法則による事故軽減 ー



●ハインリッヒの法則におけるヒヤリハットに着目することで、重大な事故を防止する。

表1：
ーバランススコアカード（BSC）による重要業績評価指標（KPI）の分析例ー

効果項目		実際の効果 あった	実際の効果 なかった	当初の意図 あった	当初の意図 なかった
A（業績）：売上又は収益改善につながった					
	A１：営業・販売等の管理コストの削減ができた	1	2	1	2
	A２：調達単価の引き下げが実現できた	1	2	1	2
	A３：売上の拡大につながった	1	2	1	2
	A４：機会損失の減少につながった	1	2	1	2
	A５：その他収益改善につながった	1	2	1	2
B（顧客）：顧客満足度の向上、新規顧客の開拓につながった					
	B１：製品・サービスの品質向上につながった	1	2	1	2
	B２：新規顧客の開拓に成功した	1	2	1	2
	B３：既存の顧客に対し満足度向上が図れた	1	2	1	2
	B４：顧客からの提案が新たなビジネスにつながった	1	2	1	2
	B５：その他新たな市場の開拓につながった	1	2	1	2
C（業務）：業務革新、業務効率化につながった					
	C１：在庫の圧縮につながった	1	2	1	2
	C２：開発・製造・納品等のリードタイム短縮ができた	1	2	1	2
	C３：作業効率の向上や連携の向上が図れた	1	2	1	2
	C４：他社との協業の強化・効率化が図れた	1	2	1	2
	C５：その他業務革新・業務効率化につながった	1	2	1	2
D（学習）：従業員の満足度向上や職場の活性化につながった					
	D１：社員のスキル向上につながった（担当業務の拡大、再訓練期間の短縮、一人当たり売上向上など）	1	2	1	2
	D２：職場の活性化につながった（従業員からの提案が増えた、従業員の提案を採択する機会が増えた、業務目標との連動率が向上したなど）	1	2	1	2
	D３：社内の情報活用効率が改善した（情報システムの利用度が上がった、顧客情報を社員が見る機会が増えた、品質管理や営業などに関する新たなフィードバックが増えたなど）	1	2	1	2
	D４：意思決定の迅速化が図れた	1	2	1	2
	D５：その他従業員満足度、職場活性化につながった	1	2	1	2

出典：経済産業省 情報処理実態調査（平成16年）情報処理実態調査票
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/johoshori161.pdf