ロシア
技術ニュースレター
Russian Technical News Letter

ロシアにおける
情報セキュリティシステムの運用

ROTOBO

社団法人ロシア東欧貿易会
〒104-0033　東京都中央区新川１－２－１２　金山ビル
Tel.　（ 03 ）　3551-6215　　Fax.　（ 03 ）　3555-1052　　http://www.rotobo.or.jp

エグゼクティブサマリー

今号では、“ロシアにおける情報セキュリティシステムの運用”と題して、ロシアの指導的システムインテグレータのひとつであり、情報セキュリティの分野にも特化して、独自の情報保護手段を提供するメーカーでもあるABITEL社グループの専門家に寄稿を依頼した。ロシア語の原題の直訳は“保護された情報システムの運用”である。日本の企業経営者には意味が伝わりにくいという懸念から、前述の通り題を変更した。しかしながらこの原題には非常に意味の深いものがあり、この原題の持つ意味を考察しながら、エグゼクティブサマリーをまとめたい。

今日の企業経営に「情報システム」が欠かせないことは、誰も疑うことの無い事実である。企業が成長し従業員が増え、活動の場も海外に広がり、グローバルな視点でリソースを管理し、ダイナミックな経営を行なっていくには、情報システムの持つ能力とスピードが不可欠である。そして、この様な情報システムに対する投資の重要性も、今日の企業経営者は充分認識している。また、その情報システムのセキュリティを保護することの重要性についても、昨今の情報漏洩による企業の損失や信用の失墜のニュースが流れる度に、意識を新たにしている課題である。

然しながら、情報システムのセキュリティを保護することの重要性を議論する前に、企業経営者はその特殊性について、まず正しく認識しなければならない。

情報システムを構成する主要なコンポーネント、例えばサーバシステムは、数年間その設定に変更を要求することなく充分に稼動する。世界中の拠点を結ぶネットワークシステムも、生産や物流活動、販売活動を支えるERPやCRM等のアプリケーションシステムも、構築が完了し稼動し始めれば、次の大幅なシステム更新の時期が来るまで、基本的にはその役割を担い稼動し続ける。仮に不具合があったとしてもその原因は直ぐに特定され、適切な対応方法は初めから想定されている。

だが、この情報システムを「保護すること」、あるいは「保護し続けること」の難しさは、今日しっかりと保護されている情報システムであっても、明日は脆弱であることが判明するかもしれない、しかも、何が原因となり脆弱性が露見するかについて、持ち主である企業経営者や情報システム管理責任者が知りもしないという点にある。変更を要求することなく稼動し続ける情報システムに対し、日々新しいセキュリティに対する脅威、ウィルス、攻撃手段が出現する。セキュリティに対する新しい脅威の出現を考慮に入れてない、または間違って運用されている情報システムは、膨大な投資を行い構築しても、稼動開始数カ月後には適性を失い、脆弱になっていく。そしてハッカーの攻撃、ウィルスの侵入、ユーザのいい加減な動作や意図的な内部関係者によりもたらされるセキュリティ関連事件の被害が現れてから、持ち主たる企業経営者や情報システム管理責任者は「気づく」のである。

保護された情報システム、あるいは、保護され続ける情報システムの運用は、情報システムのコンポーネントの耐障害性と情報システム全体の動作の連続性を要求することと同じくらい厳しい要求である。そして、この「情報セキュリティシステム」が単に直接的な物質の損失を保護するだけでなく、自社の活動分野にお

ける市場での競争優位性、評判、そして顧客やパートナーのより高いレベルでの信頼を保つものであることを、充分理解する必要がある。

大きくて複雑な情報システムであればあるほど、セキュリティの保護に関して適用される決定の組み合わせの幅が広い。企業活動がダイナミックで新しい情報システムを先進のテクノロジーを使い構築する機会が増えれば増えるほど、これまでに経験の無い新しい脅威にさらされる機会が増大される。攻撃実施方法やツールは常に改良されており、その普及の早さは爆発的に発達している。情報システムの複雑さが増すことで、必ずそのコンポーネントと保護ツールの脆弱性が促進され、この脆弱性を積極的に利用して、さまざまな種類の攻撃、データ伝送やサービス提供のネットワーク停止、重要な付属文書の作業の停止、機密データの盗難やその他の行為が実行される危険性を伴っている。

論文は、情報システムのセキュリティを保護することの特殊性、すなわち、情報システムが複雑であればあるほど、新しければ新しいほど、脅威にさらされる機会が増大し、保護し続けないと直ぐにでも陳腐化し、脆弱性が増大する性質のものであることを指摘している。そして、そのような「情報セキュリティシステム」を運用する企業のスタッフの役割と、企業としてそのスタッフを養成・設置することに関する認識のあり方についても言及している。

2004年に自社リソース保護システムの問題で苦労した企業の半分（このような企業は世界に様々な評価で80%もあった）は、保護ツールを充分装備し、全ての必要な分野に高度な技術を持つスタッフを持っているとみなしていた、という興味深い事実がある。

情報セキュリティシステムを正しく運用し、維持するためには、スタッフは常に自分の知識レベルを維持し、企業で利用される保護ツールとシステムの全組み合わせの特殊学習をしなければならない。大きくて複雑な情報システムにおいては、この条件の実行はかなり多大な出費を要する。スタッフの作業経験が、特に非常事態の克服において本質的な意義を持っている職務である。何故なら、スタッフが非常事態に遭遇した経験を持てば持つほど、非常事態を起こした原因の特定とその除去に関する行動、その他起こりうる問題の解決に関する行動はより適切で的確になり、企業が損害を被る確立は低くなる。この様なスタッフは、もちろん、しかるべく労働賃金水準を要求する。これが、多くの企業にとって難しい条件となってくる。

企業経営者の立場から見ると、この様な特殊で、狭く、かつ日々脅威との葛藤を続けて研鑽を必要とする専門的な知識を必要とする分野のスタッフを、高い労働賃金水準を保ち、自社で養成・雇用していくことの是非の判断を要求される。論文では、「情報セキュリティシステム」をどう運用するか、というテーマと共に、アウトソーシングという視点で、誰に委任するかというテーマにも言及している。セキュリティ分野におけるアウトソーシングは、まだ広く普及している状況には無い。何故なら、情報セキュリティ市場は、情報システムの市場より新しい、あるいは、遅れている市場だからであるが、今後は明るい見通しを持っていると思われる。様々な理由により、自社の情報セキュリティ運用部門を発展させる意向を持たない企業には、アウトソーシングサービスの検討も、ひとつの選択と考えられる。また、作業の大部分を自社の力で実行することを目指している会社の場合は、この分野の品質の高いコンサルティングを提供し、特に困難な課題を実行する場合に自社の要員に対する支援を提供し、独立会社としての的確な提言を行なってくれる「情報セ

キュリティ・コンピタンスセンター」のサービスを利用することも、高いレベルの品質の維持と相対的なコストの低減を両立させる選択肢となりうる。

ロシアの情報セキュリティ技術の高さは、多くの業界関係者、企業経営者が期待を寄せるものではあるが、その根底にある、情報セキュリティシステム運用に関する企業経営の立場からの視点と考え方に、あらためて学ぶところがあるものと評価する。

本稿の目的

この論文で我々は、情報テクノロジー（IT）と情報セキュリティ分野における国内及び世界のサービス市場での基本的な傾向を概観し、IT製品やサービスの顧客企業の最新需要を分析する。

システムインテグレータとして、またセキュリティ分野におけるインテグレータとしての弊社固有の長年にわたる歴史は、ロシアにおける市況を単に反映しているだけでなく、IT製品やサービスの販売分析が示しているように、なんらかの傾向の現象をわずかにリードしてもいる。これは、情報システムを運用し発展させている我々の顧客も含めたロシア企業で形成されている状況に合致するよう、我々が努力していることを意味している。

この論文は、セキュリティのツールとシステムを設置し動かしている企業が、保護された情報システムの運用と関連する全てのニュアンスとこの分野に存在している問題を、より完全に理解し、さらにより良い方法でこれらの問題を解決する案について考えることに役立つものである。

1. ロシア国内におけるサービス

1.1 ITとセキュリティのサービス市場の状況と傾向

ロシアと世界で実施される調査によると、情報セキュリティ市場は４～５年前の情報テクノロジー市場に「似ている」とのことである。これは当然、第一に、セキュリティ分野における製品とサービスの市場がIT市場全体の一部分であること、第二に、全ての企業が最初は自社活動のオートメーション化に取り組んだか、あるいは現在も取り組んでおり、その後で自社リソースの保護に取り組むため「遅れ」をとっていること、これらによって説明される。

ここ数年に見られる情報テクノロジー分野の基本的な傾向は、ますます多くの企業が情報システムの構築プロセスを完了し、システム運用段階に移行していることと関連がある。これは、いつも完全に要求を満足させ、十分プロフェッショナルだというわけではないITコンポーネントの技術サポートとアフターサービスに対する需要の伸びが著しいことを意味している。

これから近い将来の数年間の情報セキュリティ市場に特徴的となる傾向は、IT分野でみられているものと同じである。つまり、情報保護ツールとシステムを納入する段階から、サービスへの移行が徐々に起こっているということである。ますます多くの顧客が保護ツールとシステムの開発・導入の段階を過ぎ、導入した決定の技術サポートとアフターサービスが必要となってきている。

このサービスに何が含まれるのか、具体的な企業のなんらかの特性のもとに誰がそれを行わなければならないかについては、次の章で述べる。今はまず、保護された情報システムをどのような条件で運用するかを分析する。

企業はますます積極的に自社のITシステムに保護ツールを装備している。世界におけるこれらツールの販売規模の伸びは、各種ツールで少なくとも10%となっており、ヴァーチャル・プライベート・ネットワーク（VPN）とLAN用ファイアウォールの市場は13%の伸びを示した。一方、比較的「新しい」保護ツール（例えば、文脈分析）市場は、さらに速いスピードで伸びている。

ロシアにおける保護ツールとシステムの市場はさらにダイナミックに発展している。この２年間で毎年約50%の成長となっている（ロスビジネスコンサルティング社（RBK）の調べによると、2003年に5,000万ドル、

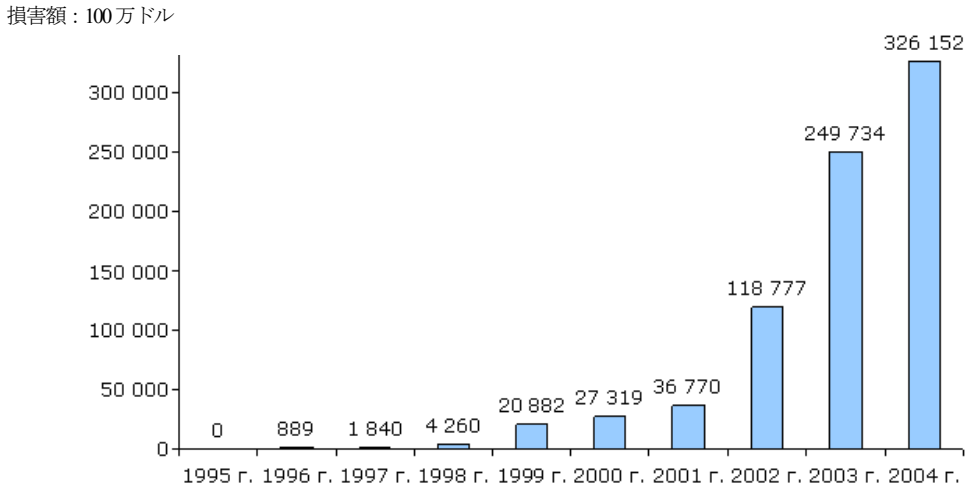
2004年に約１億ドル以上だったのと比較して、2005年は約１億4,000万ドル）。情報リソースは、ITシステムにしかるべきツールが装備されるにつれ、よりしっかりと保護されてきているように見える。

しかし、2003年には約40%の企業が保護システムの問題で何らかの損害をこうむっており、2004年にはそのような企業が80%以上になった！不正アクセスと攻撃の発生数は毎年絶えず増加している。例えば、機密データの盗難または漏洩数は、一年間に２倍以上増えた。

攻撃やその他のセキュリティ事件が発生した場合の損害もますます顕著になっている。Cnewsで提供されたmi2g社の記録によると、1995年から始まった毎年の経済損害の伸びは、一度も30%を下回ったことがなく、100%を超えたこともあった。

（第1図）コンピュータ攻撃による世界の損害総額

（単位　100万ドル）



（出所）mi2g社　2004年

セキュリティ関連問題の被害を受けなかった企業の中で、十分に保護され攻撃の撃退に備えているとみなした企業は、３分の１を少し超える程度だった（38%）。

保護ツールとシステムの市場が確固たるテンポで毎年成長しているときにこのようなことが起こっており、ますます多くの企業が、より完璧で総合的になってきている保護システムを装備している。

このことが物語っているのは、まず、情報セキュリティ分野に特有のいくつかの特徴についてであり（ITでは、例えば、オートメーション化への投資額が増加すると、普通、ビジネスで起こりうる損失は減少する。セキュリティ分野では、一定の条件が満たされるときだけである）、次に、保護ツールを購入してインストールすることだけでは、完全に企業リソースのセキュリティ問題は解決されないということである。自社リソースに対して起こりうる侵害に対して、単に「防壁を建てる」のではなく（たとえうまく設計され、そつなく設置されていたとしても）、防壁が時間の経過とともにずっと信頼性のあるものとして残るよう、そのために努力することが必要である。

もちろん、全般的な市況と統計データの分析から得られた結論が、具体的なひとつの企業をそんなに動揺させることはないかもしれない。そのような企業は自社独自の問題と特性を持っているからである。よって、我々は、リソースのセキュリティ分野がどのような特性を持っているのか、そして、保護システムが確実に作動するために企業は何をしなければならないのかを理解するために、保護された情報システムを運用している組織における状況に注目する。

2. 保護システムを導入し運用している企業における状況

今日、事実上、全ての企業が自社リソース保護の重要性を理解している。多くは、情報セキュリティシステムが単に直接的な物質の損失を保護するだけでなく、それが（自社活動分野における）市場での競争の優位性、評判、そして顧客とパートナーのより高いレベルの信頼を保つものであることも理解している。よって現在、全ての企業が何らかの規模で自社リソース保護に出資している。個別のツールまたは複合的なセキュリティシステムが、各ITシステムに設置されている。

保護された情報システムを運用する段階での基本的な課題は、達成されたセキュリティレベルの維持である。これは、ITコンポーネントの耐障害性と情報システム全体の動作の連続性を要求することと同じくらい厳しい要求である。近代的な保護ツールが装備されている情報システムの運用は、十分複雑で特殊な課題である。

2.1 保護されたITシステム運用の特殊性

セキュリティツールとシステム運用の基本的な特殊性は（他のITコンポーネントと違って）、今日しっかりと保護されている情報システムでも、明日は脆弱であることが判明するかもしれない、しかも、このことを持ち主が知りもしない、ということである。

サーバシステムは、数年間、その設定に変更を要求することなく十分に稼動する。この際、その不具合（例えば、プロセッサー故障）はすぐにはっきり分かる。同時に、セキュリティに対する新しい脅威の出現を考慮に入れていない、または間違って運用されている保護システムは、数カ月後には適性を失い、脆弱になっていく。しかし、持ち主がこれに「気づく」のは、ハッカーの攻撃、ウィルスの侵入、ユーザのいい加減な動作及びその他のセキュリティ関連事件の害が現れてからである。

これには、グローバルな性質を帯びた、いくつかの客観的な原因がある。

まず、情報システムの複雑さが増すことで、必ずITコンポーネントと保護ツールの脆弱性が促進されることである。この脆弱性を積極的に利用して、様々な種類の攻撃、データ伝達やサービス提供のネットワーク停止、重要な付属文書の作業の停止、機密データの盗難やその他の行為が実行されている。

次に、セキュリティに対する新しい脅威、ウィルス、攻撃手段が出現する。攻撃実施方法やツールは常に改良されており、その普及の早さは爆発的に発達している（企業システムを数秒で故障させることもでき、このようなケースの顕著な例は多い）。被害の大きさは時としてビジネスにとってほとんど「致命的な」ものとなる。

また、多かれ少なかれ、具体的な企業と具体的な情報システムに特有のものとなりうる一連の特性も存在する。

例えば、大きくて複雑な情報システムでは、保護に関して適用される決定の組み合わせの幅がかなり広いことがある。様々な生産者の多種多様な保護ツールが利用され、これらのツール間の相互関係は、複合的なセキュリティシステムという枠内において、かなり複雑である。そのほか、現代の保護ツールの作業メカニズムそれ自身が、どんどん複雑になってきており、攻撃の発見、トラフィックのフィルタリングやその他の保護機能実施の方法も、より「精巧な」ものが適用されている（文脈分析が顕著な例）。

このように、リソースセキュリティの現実的な管理のためには、多くのツールの複雑な相互関係作業の全体像が必要である。技術的な観点からも、またこのようなシステムの運用に責任を負っているスタッフの実際的能力の観点からも、課題は単純ではない。

さらにもうひとつの問題がある。特に、セキュリティの複合的なシステムの運用にとって緊急な問題である。それは生産者が、改善や、新しい機能を追加し、エラーの訂正という変更を含む新しい製品バージョンを常に生産していることである。それで、これらの変更を常にモニタリングし、それらを自分のシステムに設定する必要がある。企業システムを攻撃するために利用された多くの脆弱性は、攻撃の時に発見され、保護ツールまたは攻撃されているITコンポーネントの生産者に知らされるというのは周知の事実だが、この脆弱性は、単にしかるべく修正モジュール（パッチ）を設置することによって、攻撃の数週間前あるいは数ヶ月前に除去出来たものだ。

全てのこういった新しく導入されるものをフォローするためには、常にそれらを追跡し、このような種類の事件をモニタリングする必要がある。こういったことが出来ない場合、セキュリティシステムはあっという間にその課題の遂行をストップしてしまう。

2.2 ITインフラとセキュリティの進化

保護された情報システムの運用の特殊性は、その構成と構造に変更がもたらされることである。かなり大きな組織の作業を保障している情報システムは、実際、決して静的ではないということが経験上示されている。ITシステムの拡大、新しいコンポーネントの追加やその他の変更、これらは、変化する主要な活動プロセスと情報システムが密接に関係して稼動しているので、当然の不断のプロセスである。新しい情報サービスが現れ、積極的に新しい情報技術が導入されると、一定の段階でシステムを最適化する必要性が出てくる。結果として、計画過程で採択された企業リソースの情報セキュリティ保障に関する決定は、システムのリソースを保護する使命を帯びているが、あっという間にシステムとの一致を失う。

例えば、情報量の増加、新しいセグメントの追加、仕事場の拡大、これらは保護のメカニズムと手順の効率性を下げるので、要求されているリソースの保護水準を保持するためには、セキュリティシステムそのもののスケーリングが要求される。

ITシステムの可能性の拡大、新しい情報サービスの追加と新しい技術（例えばWi-Fi）の導入は、新しいリスクと保護の脆弱性を招く。これらのリスクを除去するためには、新しい技術のための情報保護の特殊な局面を全て即座に考慮に入れる必要がある。

よって、変化する情報システムにおいて重要なのは、適切な保護メカニズムを単に導入することではなく、与えられたセキュリティ水準を運用する過程で維持することである。このためには、保護ツールの労働能力を維持するだけでなく、リソース保護の水準管理を一回ずつ、または定期的に実施することが必要であり（「リソース保護の分析と管理」の章を参照）、このことが、情報システムの変更導入の際でもこの水準を保証する。

2.3 スタッフ

現代のセキュリティへの脅威は原則的に克服でき、脆弱性は除去でき、全体として、リソース保護確保の課題は、我々が前述したような複雑な条件においても実行できる。ただ、セキュリティシステムを正しく運用し、維持することが必要である。これは、保護ツールの技術的な支援、システム内で発生しているセキュリティ関連事件のモニタリングと分析、リソース保護の定期的な管理、非常事態の克服及び損害の除去といった、不断の定期的な作業の全体的なシステムの実施を意味している。

これらの作業を実施するためには、まず、しかるべき技術とソフトウェアが必要であり、次に、技術と十分な経験を有する十分な数のスタッフが必要である。現代のセキュリティ技術は、実際、かなり効果的で良質だが、いずれにせよ、特に企業リソース保護システムにおける非常事態の克服において、人間、人間の思考と経験にこれらが取って代わることはできない。

主として大企業の多くには、情報セキュリティのメンテナンスに携わる自社の部、サービス、あるいは管理局そのものがある。今日、世界の大企業の81%に、企業リソース保護に責任を負う、セキュリティサービス部の責任者として任命された者が配置されている。

情報セキュリティ関連の自社内の組織を持ついくつかの企業は、保護システムを運用する段階で外部の専門企業を誘致しない。これは、自社の専門家を維持する支出の方が、保護されるITシステムにとってのリスクに対する支出より少ないとみなしているからである。いくつかのケースにおいて、これは事実である（疑問は後で述べる）が、一連の条件を遂行する際のみである。

実際に、自社内の組織の力でセキュリティシステムの運用課題とサービスを効率的に解決することは、企業に必要数のスタッフが常駐していることにほかならない。

興味深い事実がある。2004年に自社リソース保護システムの問題で苦労した企業の半分（このような企業は世界に様々な評価で80%もあった）は、保護ツールを十分装備し、全ての必要な分野に高度な技術を持つスタッフを持っている、とみなしていた。去年一年間で保護システムにおける欠陥で苦労しなかった（または目に見える損害を被らなかった）企業のうち、課題に取り組むスタッフは、IT専門家の約10%という十分良い比率で存在する。しかし、このような企業は、残念ながら少数派である（世界の平均は、せいぜい４分の１）。企業では、コンピュータの記憶容量があっという間に増大し、オートメーション化の近代的で複雑なツールである生産管理システム、データベース管理システム、書類作成システム、電子商取引等が導入され、最後に情報セキュリティシステムが導入されている。しかし、社内組織の勤務スタッフは課題解決の必要がある複雑さと規模に比例して増加しているのでは全くない。

企業内でセキュリティシステムの維持とメンテナンスに従事している十分な数の専門家は、情報セキュリティ分野と情報技術の関連分野の高い教養を持っていなければならない。というのも、企業の多くで利用されている保護ツールの組み合わせの幅は、かなり広く、それらの作業メカニズムは毎年複雑になっているからである。正しい、そして効果的な（重要！）保護システムの作業に責任を持つスタッフの養成レベルは、そのような作業条件と合致すべきである。

スタッフは、常に自分の知識レベルを維持し、企業で利用される保護ツールとシステムの全組み合わせの特殊学習をしなければならない。大きくて複雑な情報システムにおいては、この条件の実行はかなり多大な出費を要する。

このほか、スタッフの作業経験が、特に非常事態の克服において、本質的な意義を持っている。スタッフが非常事態に遭遇した経験を持てば持つほど、停止のローカライゼーションと除去に関す

る行動、その他の起こりうる問題の解決に関する行動は、より適切で的確になり、企業が損害を被る確立はより低くなる。

このようなスタッフは、もちろん、しかるべく労働賃金水準を要求する。これが、多くの企業にとって難しい条件となっている。

セキュリティの複合的なシステムのメンテナンスは、管理機能とその他の機能のオートメーション化がしかるべき段階になければ不可能である。これは、セキュリティ管理者とその幹部（課長や部長）にとって、しかるべく技術やソフトウェアが存在することを意味している。スキャナー、モニタリングツール、セキュリティ管理ツール、事件の相関ツール、ITコンポーネントの保護分析ツール、統計受理ツール、報告書作成ツール、こられがさらにもうひとつの支出項目となるわけである。

それでも、全ての前述した条件を実施していても、企業リソース保護に責任を負う企業スタッフは、その日々の活動において多くの問題とぶつかっている。

2.3.1 セキュリティ管理者にとっての典型的な問題

管理者にとって最もはっきりした、しばしば出くわす問題は、内蔵された保護機能を持つネットワークデバイス、LAN用ファイアウォール、コンテンツ管理システム、攻撃発見その他といったサービス保護ツールと関連のITコンポーネントからの大量（千または数万）のメッセージが絶えないことである。これら全てのメッセージは、実際には圧倒的多数が重大なものではなく、現実的な攻撃やその他の重大事件について語るものではないが、とにかく、セキュリティにおける問題と関連している。しかし、それらの中には、現実的に保護ネットワークのリソースに損害を与えうる、緊急の対応を要求する事件の一部も存在する。

このような環境において、管理者は、２つの課題を解決する必要がある。正しく事件を解釈し、現実的に注意を要するものだけを選択すること、そして、正しく、迅速に、現実的に重大なメッセージに対応することである。

管理者機能（多くの保護ツールからの事象の分析と相互関係）の自動化ツールを利用しても、サービススタッフはこのような事象の流れにおいて方向付けすることが難しくなることは明らかであり、重大ではない、またはウソのメッセージに対応し、他の、重大で深刻な結果をもたらすものを見逃すという現実的なリスクが存在する。

純然たる状態でのこの問題の存在のほか、セキュリティサービス担当スタッフはさらにもうひとつの問題とぶつかる。システムで起こっている事象を理解する水準を上げるためには、ITの特質の理解を深めることが必要だが、セキュリティサービス担当スタッフには、分析ともっぱらセキュリティの特質を持つほかの作業に割く時間と機会が残っていない。また、保護ツールのITコンポーネントの機能化に関する全ての問題をITサービスに移管するという案もある。

例えば、攻撃発見システムは、SQLネットプロトコルのデータベース管理システムOracle DBMSのサーバに進入する攻撃を伝える。この攻撃の深刻さを理解するためには、セキュリティ管理者はDBMSの管理者レベルでOracleサーバ動作の細かいところまで理解する必要がある。しかし、ネット技術とネット設備、ウェブとその他の付属文書、WindowsとNovellその他の分野のドメインといった分野からのこのような攻撃事象は数百に及ぶ。セキュリティサービスは、例えば、監査のような、事象を客観的に解釈することができ、情報技術の全分野に詳しい専門家を持つか、多くの苦労を抱えるITサービスにこの機能を転嫁するか、しなければならない。

2.3.2 セキュリティ部とセキュリティサービスの長にとって典型的な問題

セキュリティ部とセキュリティサービスの責任者にとって主要な課題は、どのような条件下においても企業の情報リソース保護の安定した水準を確保することである。このような部とサービスの責任者の圧倒的多数（世界で86%）は、企業のセキュリティに責任を負っており、直接最高幹部を前にして活動報告を行う。

セキュリティサービスの責任者には、現時点における全体的なシステムの保護レベルに関する情報取得の効果的なツール、また変化の中におけるこの水準の管理ツールも必要であることは明らかだ。

多くの場合、自社のスタッフからこのような情報を受け取ることは困難である。少なくとも、リソース保護分析の特別な技術ツール、リソース保護評価方法、また時間が必要だからである。そして、独立した企業のエキスパートによる判断ではなく、自社スタッフによる判断なので、受理した情報は客観的ではない。

企業の情報リソースの保護状態を保持する責任を全面的に負っているのは、セキュリティサービスの幹部であるため、まさにこの幹部が、現代の条件に合致する状態に企業のセキュリティシステムを維持する仕事を組織し確保しなければならない。このような仕事に属するのは、かなり頻繁に現れるセキュリティへの新しい脅威や様々な攻撃のモニタリング、利用されているソフトウェア及びハードウェアにおける脆弱性の追跡（保護システムだけでなく、全ての情報システム）である。これらの仕事の成果として、時機を得た、しかるべき変更を保護ツールとシステムと、ITコンポーネントの調整に導入すること、または、新しい稼動条件と合致する保護システムを追加/近代化すること、また計画書、取扱説明書の変更がなされるはずである。この課題そのものが複雑で手間のかかるもので、現存するセキュリティサービスにとっては時として重すぎるものである。しかし、どんな場合でも、このサービスの責任者は、必要な仕事を実施しなければならず（外部の専門企業を誘致することも可能）、明確なビジョンと成果を持っていなければならない。

セキュリティに責任を負っているメンバーにとって、さらにもうひとつの複雑な問題がある。それは、変更される情報システムリソースの保護レベルの維持である（「ITインフラとセキュリティの進化」の章を参照）。実際、なんらかの変更が保護されているITシステムそれぞれの構造と構成にもたらされ、そういった変更がセキュリティの観点からあまり本質的なものではなく、保護システムに変更をもたらすことを要求しない場合もあれば、全面的な近代化を要求する場合もある。

多くの企業、特に、大企業及びこの数年間ダイナミックに発展している企業では、セキュリティ部とセキュリティサービスの幹部には毎週（もっと頻繁でなければ）、新しい市場の獲得、新しいサービスの提供等、企業の事業展開に向けられたITインフラの発展と近代化に関するプロジェクトが持ち込まれる。おそらく最も顕著な例は、セルラー通信のオペレーターである。そして、これら全てのプロジェクトは、新しいセグメントの追加、新しいオフィスと支局の接続、新しい、より近代的な技術の導入等に関する提案を含んでいるが、これらは全てセキュリティの観点から鑑定を要求しており、この情報セキュリティに関する要求は、企業のセキュリティシステムの適正な変更で後に示されるはずである。

繰り返すが、セキュリティの観点からのITプロジェクト鑑定そのものが、骨が折れるもので、専門家の高い技能熟練度を要求する。必要な変更の導入課題もまた、物質的だけでなく、人的資源を要求する。

2.3.3 企業の責任者のために

セキュリティ部とセキュリティシステムの指導者による努力の成果は、運用している情報システムのリソースが、現存する条件に従って、確実に保護されていることで現れる。これは当然、業務への然るべき融資を意味している。周知のとおり、情報セキュリティの予算はIT予算の10%となるべきだが、世界の企業のほ

ぼ半数がこの予算を約３％としており、３分の１の企業は４～６％の範囲である。10分の１の企業だけが企業リソース保護にITシステム費用の約10%を分割している。

なんらかのプログラム技術ツールを購入し、保護に関する一定の施策を実施する資金を捻出する（あるいは捻出しない）ためには、企業の幹部は、どのようにしてこれがITシステムのセキュリティレベルに反映されるのかを理解する必要がある。現在どれだけ企業リソースは保護されているのか（または脆弱なのか）、この状況は時が経てばどのように変化するのか、現存する保護の問題の現実的な原因は何か（利用されているセキュリティのツールとシステムの不足、スタッフの怠慢、セキュリティの課題の重要性が最も低いためにITサービスの調整に必要な訂正を強制的に導入することが不可能なこと等）？

今日、企業の約３分の１が、全くこのような種類の分析を実施しておらず、自社リソース保護レベルの管理をしていない。

情報セキュリティのために十分な資金が出されておらず、「由々しい事の起こらぬ」うちは作業を実施しないというケースがしばしば見受けられる（このような状況は、この分野での専門企業に「不正な金儲け」をさせる）。世界で３分の１の企業だけがこのような管理を定期的に実施している。

統計でも、企業のセキュリティ状態について、また現存するリスクと事件についての報告が、質的には不十分だが、大量にそして頻繁に幹部に提出されることが示されている。セキュリティ状態に関する報告を四半期ごとに提出するか、半年に一度提出している企業は、多くて３分の１ほどで、さらに、少なくとも３分の１（34%）の企業が報告を全く提出していないか、またはせいぜい、特殊なケースに関するなんらかの特別報告を準備している。

企業幹部は（セキュリティ管理者や関係する部とサービスの責任者とは異なり）、何のために自社リソースのセキュリティに投資する必要があるのか、その根拠、または、企業リソース保護への投資の効率性判断の、短くて分かりやすい報告を必要としている。

リソースのセキュリティ状態に関する統計受理や報告書作成手段があっても、自社のスタッフやセキュリティ部とセキュリティサービスの幹部が詳細な技術報告書を集め、それらを支出の論的根拠として組み立て直すことは難しい（純粋に技術的な複雑さと、価格その他の基準に適正な、現実的に必要な保護の手段とツールの選択という問題がある）。

部分的にこのことが原因で、幹部は事業の脆弱性と情報システムの確実で安全な働きに依存していることを自覚しないこともある。

2.3.4 社内組織の相互関係の問題

情報システムのリソース保護の確保と管理は、ITサービスとセキュリティサービスの幹部の普遍的な課題であることは、原則的に明らかである。時として、例えば、セキュリティサービスのスタッフが、ITサービスの仕事を管理することが必要になるケースもある。例えばこれは、すでに言及したITインフラ発展課題であり、セキュリティ上の理由によって示唆された場合、保護のツールと手段の適用だけでなく、しばしばITプロジェクトへの変更導入を要求する（ITコンポーネントの調整、その接続図等）。また、日常的な、より「些細な」課題も存在し、それはいくつかのサービスの一致した相互関係が必要となる（IT社内組織、情報セキュリティサービス、保護サービス、HR社内組織等）。例えば、新しい従業員を雇用する、彼に仕事場を与える、アクセス全権を提供する等。

我々の観察によると、ITサービスとセキュリティサービスの相互関係は、目前の課題の解決にとっていつも十分効果的であるとは限らない。情報セキュリティの確保の過程に参加する全員の間で責任と義務の範囲

の分割が不明瞭であることが見受けられ、これらのサービスの間に「利害の衝突」が存在する（ITサービスにおいて、情報セキュリティの課題の優先性は低いことがしばしばである）。前述したスタッフの問題とその他の問題全体で、これは運用しているシステムの現実的な保護管理の複雑さ、緊急事態への適正な対処の複雑さ等を意味している。

2.3.5 ユーザ

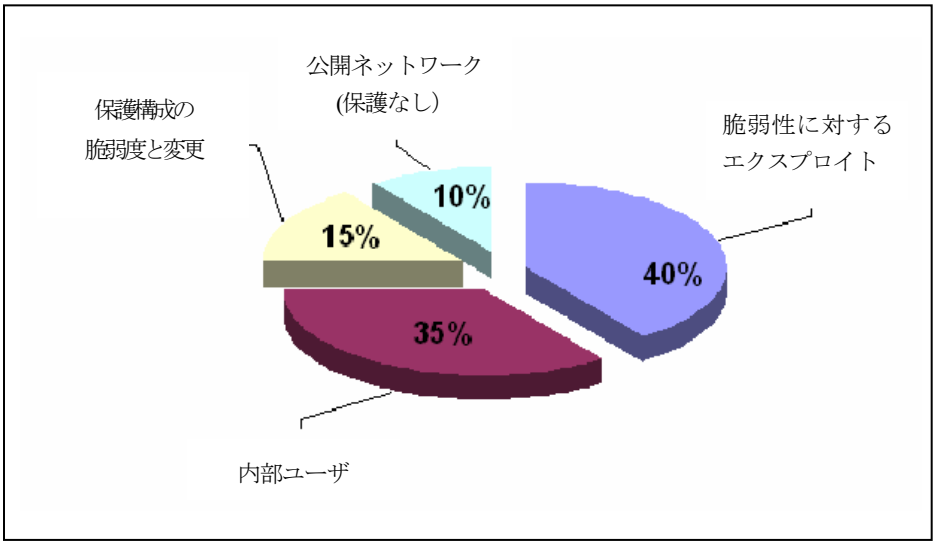
従業員のユーザカテゴリを検討したい、というのも、まさにユーザが保護された仕事場を使用し、保護された情報及びその他の企業リソースを利用しているからである。この関係において、ユーザの規律と素養が企業の情報セキュリティ保障のために大きな意義を持っているが、企業のユーザは、情報保護は彼らの義務ではなく、押し付けられた機能であるとしばしばみなしている。最近数年では、企業活動のオートメーション化レベルの成長がかなり速い状況で、ユーザの知識、経験及び専門的技量の平均レベルは「遅れをとって」いる。一方これは、ユーザの作業プラットフォームの作業違反から、企業にとって重大なサブシステムとサービス（例えば、電子メールシステムまたはウェブサービスシステム）のロックにいたる、ユーザ動作の粗雑さがはなはだ深刻な結果を招きうることを示している。それによって、企業の保護システム構築努力は無になることがある。

アクセス権の提供または制限は、多くの企業にとってはさらにもうひとつの問題である。ユーザは、ユーザにとって本当は必要ない（少なくとも勤務時間中は）リソースへの（内部または外部の）アクセスを提供するよう管理者に要求するか、彼らに必要なソフトウェアを独自にインストールし、調整できるようにするために、何らかのシステム（自分の作業プラットフォームの）におけるより広い（管理者の）権利を提供するよう要求する。管理者は、然るべく指示があれば拒否することも出来るが、かなり高い地位にある従業員が自分の権利の拡大を依頼してきたり、友情関係のために拒否することができないケースもしばしばある。このような従業員の能力と規律が実際高い水準にない場合、その害は顕著なものとなりうる。

損害の規模は、内部の従業員が故意に自社の企業に反する行為をした場合、より大きなものとなる。なぜなら、合法的なユーザはこのために、ユーザにとって単純な、そして特別な技能も知識も要求しないものを含め、多くの可能性と手段を持っているからである。

次のような統計がある。2004年、基本的なセキュリティ問題（80%の企業で見られた問題）の出所は、外部のものだったが、2005年上半期には、保護システムにおける欠陥で損害を被った企業の大部分（約30%）で、問題の出所はまさに企業内部にあったのである。今日、セキュリティシステムにおける違反全体の70%以上が内部従業員によるものだという意見もある。内部の出所からの予算損失額もまた、毎年爆発的に増え続けている。

（第2図）攻撃の種別 （2005年3月）



図から分かるように、保護問題全体の３分の１はユーザの過失による（怠慢な）行為である。情報システムコンポーネントにある現存の脆弱性と「弱い」ITコンポーネントの調整を利用したことに関連するその他の事件の中にも、悪意を持った内部の者による攻撃がある（まさにこのような攻撃が最も危険である）。

このことが証明しているのは、不誠実、または単に怠惰な合法ユーザから情報リソースと技術を保護することが大変重要になったが、すでに有名でよく把握された情報セキュリティ分野と比較して、それは特別なプログラム技術ツールの特別なアプローチと適用を要求することである。この課題の解決は、保護された情報システムの運用過程において、企業で実施されている総合的な作業に絶対に含まれるべきである。

2.4 結果として…

この章で述べてきたことから明らかなのは、保護された情報システムを運用している企業にとって重要なことは、自社リソースのセキュリティ（または脆弱性）の現実レベルに関する情報を持つことと、このレベルの管理である。つまり、このレベルに効果的に作用する可能性も含めて、違反を見つけて阻止し、スタッフの（ユーザとしても、管理者としても）行為を管理すること、事業にとって否定的な結果を避けること、そして最終的には、情報リソース保護への投資は正しかったと確信を持つことである。

しかし、情報セキュリティシステムの創設に投資した全ての企業で、彼らのリソースが、運用段階で、現存している全ての脅威や攻撃から保護されているという確信があるわけではない。幹部やセキュリティに責任を負っている者全員に、今起こっているITシステムの保護における違反、これらの違反の原因または罪のある従業員について知らされるわけではない（しばしば明らかになるのは結果だけで、しかも「強烈に目立った」ものだけ）。従来通り、明瞭で客観的なリソース保護の全体像と企業セキュリティへの投資の正当性と保全性への確信を、全ての幹部が持っているわけではない。

この状況をどう改善するかは、次の章で述べる。

3. どう運用するか？

3.1 運用段階における作業の全体構成

情報保護のツールとシステムの運用は、情報システムの保護に必要なレベルを確保することを可能にしている複合的な作業を含まなければならない。このような作業に属するのは、

- システムの正しい運用 – システムに対して提示される要求に最も正確に合致する状態での保護ツールの維持、システムの近代化と新しいコンポーネントのテスト研究
- リアルタイムモードで、セキュリティに関係する、システムで起こっている事案のモニタリングと分析、重大事案への対応
- システムのセキュリティ管理–保護のテスト研究、潜在的な問題の発見、規則の動作チェック
- 非常事態の克服–問題のローカライゼーションと被害の予防・解消
- 情報セキュリティ分野における事案のモニタリング – 新しい脆弱性の出現、セキュリティと新しい種類の攻撃の脅威、保護システムへの必要な変更の導入

これらの作業によって、提示されるセキュリティの要求、また現在の傾向と新しい情報セキュリティ技術によりぴったり合致する状況で保護される情報システムを維持することが可能となり、企業のセキュリティポリシーの執行を追跡し、システムへの侵入及びその他の不正な攻撃を予防し、戦略的かつ適性に保護システム内における違反や、セキュリティの観点から本質的なその他の事案に対応することが可能となる。

3.2 誰に委任するか？

いくつかの案があり、そのそれぞれが具体的な企業条件においてプラスとマイナスをもっている。

情報セキュリティ関連の社内組織の力で全ての作業を遂行することは、全ての企業にとって実行可能な課題ではない。このような企業がぶつかる基本的な問題は、スタッフ数の不足と、スタッフの不十分な技能、必要な器具一式と作業遂行方法（例えば、非常事態の際）、テストスタンド等の欠如である。これは、大部分の企業にとって、情報技術分野のサービスは、セキュリティ分野ならなおさら、主たる活動ではないから当然である。さらにもうひとつ、このようなアプローチには重要な問題がある。自社の情報システムに関する客観的な情報と、社内で起こっている事件に関する客観的な情報の欠如である。根拠付けられた計画立案と保護作業の投資のため、また、例えば、セキュリティ分野の複雑な事案を検討する際、障害の出所が企業内部にあることによってこの課題の解決が個別の力では複雑になりうるとき、独立した専門的な評価が必要となる。

全ての企業が自社の力で保護システムを運用し維持したいわけではない。多くにとって最適な解決方法であるのは、システムの保護の確保に関する企業システムの運用機能を、情報セキュリティ分野を専門に扱っている外部担当者に、部分的に委譲することである。

このような解決方法のメリットは明らかである。専門企業には、普通、高度な技術をもつ経験豊かなスタッフ、テストスタンド、作業実施のための器具一式、緊急事態における動作の規則と方法等がある。貴社で技術的な問題が発生した場合、専門サービス企業の今までの経験では、その問題はおそらくすでに遭遇したものなので、解決方法を専門企業はすでに知っていることになる。よって、作業の質も当然高くなる。

多くの企業は、基本的なビジネスを全く中断させないで、稼動している自社リソースを確実に保護するものを持ちたいと考えている。このような企業の幹部は、外部の執行者であるアウトソーサに企業リソースの安全維持と管理を全て委任することを望んでいる。なぜなら、これは自社のセキュリティサービスの発展に投資するよりも時々有益であるからである。IT分野のサービスのアウトソーシングは世界で広く普及しており、ロシアでもますます積極的に普及している。セキュリティ分野におけるアウトソーシングは今のところまだ広く普及していない（すでに述べたように、情報セキュリティ市場はIT市場から「遅れている」ので）が、明るい見通しを持っているので、我々はこのサービスにまるごと一章をささげる。

保護システム運用過程で外部執行者を誘致する場合のこれら全てのプラス面にもかかわらず、外部執行者と一緒に企業システムへの外部組織のアクセスと関連したリスクが起こる。機密情報の撒き散らし、セキュリティ分野における起こりうる事件に対する責任その他である。

よって、外部執行者の選択の際には、その企業が持っている様々なIT分野におけるサービス提供経験と、情報セキュリティサービスの提供経験、証明されたサービスエンジニアの存在を考慮に入れ、機密性の法的面と技術面の保障に注意を向ける必要がある（臨時ユーザとアクセス方法、外部スタッフの動作登録、厳格な鑑定その他）。

このような条件を実行すれば、専門企業の誘致によって、情報システムのセキュリティ維持に関する出費を最大限に抑え、最も高いレベルと質の維持を達成することが可能となる。そして、基本的な企業活動に集中することができる。

専門企業側が提案するセキュリティ分野における様々な種類のサービスは、サービスの組み合わせ（最低限の「ホットライン」から24時間モードでの非常出張まで）や、サービスの時間パラメータ、機動性のレベル、具体的な顧客の条件に作業を「関連付ける」レベル等の点で優れている。

3.3 サービスの選択に影響を与える条件

様々な企業にはオートメーション化の規模と程度、セキュリティに対する要求のレベル、使用するリソース保護手段とその導入段階、予算的な可能性と人的可能性等の本質的な差異がある。よって、これら企業は、様々な種類のサービスを求める。サービスの構成要素には次の条件が影響を与える：

1．企業に自社のITサービス／セキュリティサービス（またはその他の情報セキュリティに責任を持つ社内組織）が存在するか？

2．サービス維持の保護システムが確保されているか？誰がそれを実施しているか（生産者、ITサービスまたはセキュリティサービス自体、納入者、誰もいない）。

3．保護システムサービス、問題発見と非常事態解決のための自社スタッフは十分か？

4．情報システムのセキュリティと信頼性／耐障害性の保障に対する要求は企業内で高まったか？

5．望ましくない結果を招くセキュリティ障害やその他の事案が発生しているか？具体的にどのようなものか？頻度は？どのような結果（損害）か？

6．サービススタッフは、どのようにして、違反その他のセキュリティの危機的事案を知るのか？通知体制は整備されているか？

7．被害が出る前に問題状況の排除に着手することに成功しているか？

8．セキュリティ管理ツールが、自動的な／オートメーション化された対応動作を実行する可能性を提示しているか？これらの可能性は利用されているか？

9．情報システム（IS）リソースのセキュリティモニタリングを実施しているか？どのようにしてセキュリティ事案の管理と分析を行っているか？

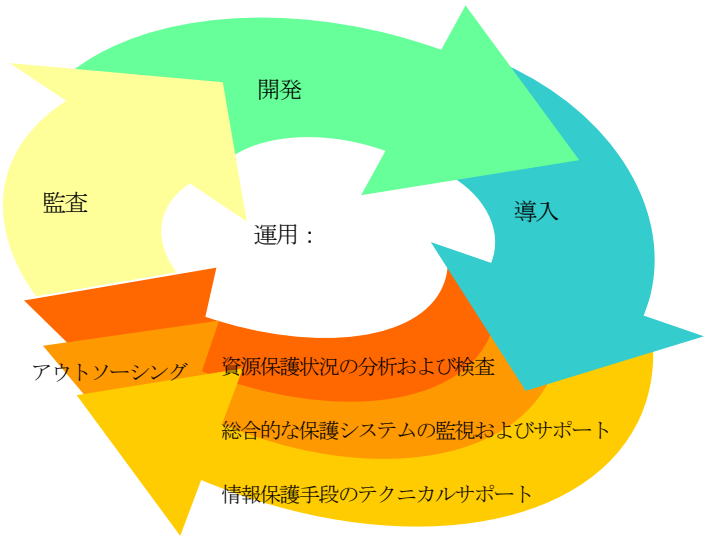
10. ISの安全性の現実レベル評価は実施されているか？どのような手段で、どれくらいの頻度で、誰が実施しているか？保護における脆弱性の発見をする際、適正な手段が適用されているか？

11. 統計と報告のシステムは存在しているか？統計情報はセキュリティサービス／IT サービスの幹部まで届いているか？この情報は保護システム発展／近代化の決定採択のために利用されているか？

4. 保護されたITシステムに対するサービスの種類

上記特徴に基づき会社をそれぞれの種類のサービスを必要とする幾つかのグループに暫定的に分類することができる。

（第3図）情報セキュリティシステムの運用段階におけるサービスの種類



情報保護手段を運用している小規模な会社にはそれらの手段に対する品質の高いテクニカルサポートが必要である。この種のサービスにより保護手段運用における問題を避け、発生した技術的な不具合を実務的に解決することができる。

（異なるメーカーの）数種の製品をベースに保護システムの導入を行っている、或いは既に導入済みの会社には、個々の保護手段の賢い運用以外に情報システム全体のセキュリティを管理できる総合的なシステムのテクニカルサポートが必要である。

下記のような様々な規模の会社の場合、すなわち

- 現時点のリソース保護状況レベルに関する客観的な情報を望んでいる会社の場合
- 一定期間保護状況レベルを管理することを望んでいる会社の場合
- 既存の保護の有効性を評価し、その開発あるいは更新の作業を計画している会社の場合

リソース保護状況の１度の、定期的あるいは連続的な分析調査が行われる。この作業により情報システムセキュリティレベルに関する全体的・客観的情報が得られ、情報保護システムの更新作業の計画や投資を行う場合に役立つ。

様々な理由により自社の情報セキュリティ運用部門を発展させる意向を持たない企業にはアウトソーシングサービスが提案できる。

作業の大部分を自社の力で実行することを目指している会社の場合、情報セキュリティ問題のコンピタンスセンターのサービスが必要である。そのようなセンターはこの分野の品質の高いコンサルティングを行い、特に困難な課題を実行する場合に会社の要員に対して支援を行い、独立会社の意見が必要な場合などにおいて専門家として振舞うことができる。

以下の諸章ではこれらすべての種類のサービスについて詳細に述べる。

5. 保護手段および保護システムのテクニカルサポート

品質の高いテクニカルサポートは保護手段および保護システムだけでなく情報システム全体の効率的で信頼できる動作の必要条件である。保護手段の幾つかのサポートサービス、例えば新しいバージョン、プログラムの修正（パッチ）の発表、使用されている（アンチウィルス、攻撃シグネチャーその他の）データベースの更新、さらにweb-その他のリソース（テクニカルドキュメンテーション、知識ベースその他）へのアクセスの提供などはメーカー自身が行っている。

これらのサービスは必要であるが、これらの手段を用いて自身の機能を効果的に実行するためにはさらにそのメンテナンス、他の手段およびシステムとのインテグレーション、セキュリティ事象の解釈等が必要である。メーカーは遠方であること、時差があること、発注者の特殊性を知らないこと、その他の理由からしばしばこれらのサービスを余り実務的、効果的に行わない。メーカーから直接テクニカルコンサルティングを受けることは電子メールや電話でそのサービスセンターに問い合せること（海外のメーカーの場合これは通常英語によるヨーロッパや米国への通話や電子リクエストとなり、メーカーの現地時間修正を加味して回答を得ること）を意味する。それも、問題がクリティカルでなく、待つ余裕がある場合である。

しかし、事柄が保護システム動作の不具合あるいは早急な解決を必要とするその他の技術的問題である場合、遠方にあり保護対象システムの特殊性を知らないメーカーのサービスセンターは十分に実務的に支援を行うことができない（問題の詳細を確認したり、保護手段のログの抜粋を送付したり、その他の作業が余儀なくされる）。

この状況は、広く使われている保護手段のロシアや海外のメーカーが顧客へのサービス提供を直接ではなく、通常指導的なインテグレータ企業の構成に含まれる専門のサービスセンターの手を借りて行うようになっている事と関係がある。海外メーカーのロシア代表部は通常１～２人位のエンジニアを抱えており、このエンジニア等は主にメーカーの介入を必要とする特に困難な技術的問題の解決に当って自社のパートナーインテグレータの専門家を支援して、彼らと作業を行っている。パートナーである保護システム納入業者の専門サービスセンターは全ての顧客企業のテクニカルサポートに必要な人数のエンジニアを抱えている可能性がある。

通常、納入業者には幾つかのレベル（シルバー、ゴールド、プラチナあるいは別名）のサポートがあり、それぞれはサービスの組合せとその実行機動性の程度が異なり、具体的な発注会社の要求の下に個別に選択される。保護手段のテクニカルサポートサービスは下記を含む。

- 「ホットライン」、すなわち労働時間内あるいは１日24時間体制の電話あるいは電子メールによるコンサルティング
- 保護手段動作の不具合およびその他の技術的問題の診断および解決のためのリモート支援
- 特別な監視および管理手段による技術的問題のリモート解決
- 保護手段の機能検査、標準的な更新、潜在的な問題の解明などのための予防的な訪問
- 不具合の解消および特殊な状況の影響除去のための緊急訪問

そのようなサポートにより保護手段運用の信頼性を保証し、その動作の有効性を高め、技術的な問題の検出、ローカライゼーションおよび除去の時間を大幅に短縮できる。

インテグレータの専門サービスセンターのサービスにはメーカーのサポートに比べてひとつの重要な利点がある。すなわち企業において様々なメーカーの製品をベースとした情報セキュリティシステムが稼動している場合、これら全ての手段のサポートを１実行者から調達できることである。その場合、様々な問題について何社ものメーカーに問い合せをする必要はなくなる。しかもこれらのメーカーはシステム全体でなく各個別の手段のサポートしか行わない（ところが、例えば異なる保護手段のメッセージが実際は同一の攻撃を証明しており、そのような問題の正しい解決には会社の全セキュリティシステムの特殊性に関する知識が必要である）。

例えば、多数のユーザ、オフィスおよび通信チャンネルを持つ会社では様々なメーカーのかなり多数の保護手段、すなわちネットワーク間のファイアウォール、攻撃検出システム、トラフィックコンテクスト解析システムその他が使用されている。しかも、セキュリティへの要求は十分に高い可能性がある（例えば、サービスプロバイダーあるいはファイナンス組織の場合である）。情報セキュリティシステムは総合的システムとして動作しているため、全てのコンポーネントの特性を考慮して、検出を行う必要がある。そのためには情報セキュリティ部のスタッフ等（その人数は大手企業の場合でも全部で１人か２人である！）にこれら全ての手段の取扱い方法を教える必要がある。これらのスタッフは使用される保護手段を全てメンテナンスし、パッチの発行に注意し同時にそのインストールを行い、ITシステムの変化を追跡し、必要に応じて保護システムの環境設定を調整／変更し、さらに緊急の課題（動作不具合、ウィルスその他の攻撃の影響の排除）の解決に備えなければならない。このような会社のための最適な結論は専門サービスセンターによる情報セキュリティシステムの総合的なサポートである。その際、保護システムの管理および運転の日常業務は自社の少数のスタッフの手に残してもよい。

総合的な保護システムをサポートするためには、個々のコンポーネントの賢い運用以外にセキュリティシステム全体の連続チェック、様々な保護手段からの事象（イベント）の収集と分析およびクリティカルな事象（イベント）への実際的な対応が必要である。したがって、総合的な保護システムのテクニカルサポートは個々の手段のサポートの場合に比べより広範な組合せのサービスを含む、すなわち

- 保護手段の構造、設置、機能動作モードおよび設定の調査およびそれらの固定
- 「ホットライン」、リモート支援、予防訪問および緊急訪問を含む情報保護手段動作機能の集中検査およびテクニカルサポート
- 発生しているセキュリティ事象（イベント）の検査、（必要な場合）それらに対する対応

- 対応時間は発生した問題のクリティカル度により決定される

様々なメーカーの保護手段を扱った経験を持ち、多くのメーカーのパートナーである専門サービスセンターは用いられる保護手段動作の有効性および信頼性を高めることができる。

そのような総合的テクニカルサポートはリソースのセキュリティ、情報システム動作の信頼性、保護状態およびセキュリティポリシー実行の検査を保証し、侵犯、故障その他のクリティカルな事象（イベント）によるリスクや損害を低減することができる。

6. リソース保護状況の分析および検査

保護状況レベルの検査は、リソースの保護状況あるいは脆弱性の程度を判定し、会社の情報セキュリティ確保計画全体の有効性を評価することを可能とすることから、会社のセキュリティ計画の非常に重要な部分である。具体的な目的に応じて、情報リソース保護状況の分析および検査の作業は１度に（すなわち、１年または半年に１回）、定期的に（すなわち、週または月に１度）あるいは連続して行うことができる。

１度に行う分析では、その時点における情報システムリソースおよびITコンポーネントのセキュリティ（あるいは脆弱性）レベルに関する客観的な情報が得られる。この情報により、情報システム保護や情報セキュリティシステム改善／発展のための作業の根拠ある計画や投資、セキュリティ障害の摘発と阻止、その被害の評価およびその原因の排除、さらに企業セキュリティへの投資の有効性の評価などが可能となる。

そのような分析の枠内で行われる作業は下記のものを含む。

- セキュリティの観点からの情報システムの仕様の分析
- ITコンポーネント、適用メカニズムおよび保護手段の構成の分析
- 専用手段（保護状況スキャナー）を用いた情報システムコンポーネントの脆弱性の検出と分析
- 情報システムリソース保護状況の評価
- 必要な保護状況レベル確保のための勧告の作成（実行）

作業の結果は詳細な報告書となり、それは情報システムにおいて明らかにされた問題点に関する詳しい情報、さらにそれらの問題点を解決する（既存の保護手段や措置の調整および更なる追加の）提案などを含むものとなる。

保護状況の連続分析により一定の期間におけるシステムのセキュリティレベルの検査を行い、変化する条件下においてそれを必要なレベルに維持することが出来る。

例えば、多数のユーザ、複数のオフィスおよび（インターネットを含む）様々な外部ネットワークへの接続を抱える大企業ではITインフラストラクチャーの変化に追従することは非常に困難である。企業では保護システムが導入されて稼動している、保護手段は多数であり、情報システムの信頼性およびセキュリティへの要求は非常に高い。当然、管理部門は現時点に存在するセキュリティへの脅威（ハッカーの攻撃、ITコンポーネントにおけるあらゆる脆弱性の利用、クリティカルなアプリケーション実行のダウンなど）に対抗する企業の保護システムの能力に関心がある。

しかしながら、このような条件下ではセキュリティ業務自体の専門スタッフでさえ現時点においてITシステムが曝されている脆弱性を評価することは困難である。先ず第１に、専門スタッフ数は余り多くないはずである。ところがこのような問題は真剣に取組む必要がある。すなわち、保護状況分析システムが存在する

としても、そのシステムが出力する膨大な一般データや報告を処理し、セキュリティ確保の最新技術その他を駆使しなければならない。さらに、重要なのは単にITシステムの中に脆弱性を発見することだけでなく、IT業務のスタッフと一緒にそれを排除する方法および手順を作成し合意しなければならないことである。第二点として、自社のスタッフはそのような評価を行う十分な資格と経験を持っていない可能性がある（このような場合には、使用される保護手段全ての教育でも不十分である）。

そのような会社の最適な解決手段は、毎月の脆弱性報告および評価を伴う定期スキャニングを含むリソース保護状況の検査サービスである。最初の分析における作業の構成は、１度の作業の場合と同じである。多くの場合、最初の分析およびスキャニングにおいてセキュリティレベルは「不合格」と判定され、報告には保護システム中に見出された多量の脆弱性の記述が含まれ、その中に直ちに実行する必要のある最もクリティカルなものが示される。報告に含まれる勧告に基づき、セキュリティおよびIT業務部はシステム中の全ての主要な最も危険な脆弱性を除去する。

さらに、一定の期間（通常１年）保護システムのコンポーネントにおけるセキュリティの新しい脅威および脆弱性の連続監視、スキャニング法（例えば、毎週１回）による脆弱性の定期的検出、および主要コンポーネントの構成分析が行われる。定期的に提出される報告は保護システムにおいて明らかにされた脆弱性の分析、その危険性レベルの評価および（必要に応じた）その除去のための勧告を含む。その周期は具体的な会社の要求により決定される（毎月１回、四半期毎）。

したがって、保護状態における情報システムリソース維持の課題は、自社のIT業務、セキュリティ業務および専門会社の連携作業により解決される。セキュリティ業務は信頼できる独立の外部組織を持っており、その組織がそのシステムのリソース保護状況を確認する。IT業務はITコンポーネント設定における脆弱性除去に関する十分実行可能で分かりやすい、しかも非常に詳細に作成された勧告が得られる。会社の管理部門には実行された作業とリソースセキュリティの現状に関してさらに要約された簡潔な報告が提出される。

7. セキュリティ部門におけるアウトソーシングサービス

情報技術に対する外部組織（アウトソーシング）サービス利用の急速な拡大は全世界的な傾向である。

情報セキュリティサブシステムのアウトソーシングサービスはこの市場で最も急速に成長している分野のひとつである。Gartner Groupの評価によれば、2005年には世界の大企業の60%以上が自社のリソースのセキュリティ確保機能の１部を外部組織アウトソーシングに依託することになる。IDC社の評価によれば、2004年における情報セキュリティ分野において提供されたアウトソーシングサービスの規模は約35%の年間成長を示した。

ロシアでは、企業のアウトソーシングへの関心は、ITサービス市場全体への関心と同様、ここ３～４年に観測されるようになった。ロシアの企業の間では情報技術分野の支出の50%以上はハードおよびソフト支援への支出である。これらの支出のうちのアウトソーシング部分を判定することは非常に難しいが、現在の評価ではITサービス市場の10%以上である。

すでに述べたように、情報セキュリティ市場、サービス部門を含めIT市場より「遅れている」が、すでに今日においては多くのロシア企業（通常、これらの企業はITをアウトソーシングに出した経験を持つ）は専門のアウトソーシング会社のサービスを利用している。

セキュリティ分野においてアウトソーシングとは保護システムのメンテナンスおよび管理機能を一定期間外部の実行者に完全にあるいは部分的に委託することと理解されている。その際、実行者はその機能実行の指定品質レベル（問い合わせに対する保証対応時間、機能ダウンが発生した場合の機能回復の保証期間その他）を保証する必要がある。アウトソーシング枠内の作業は発注会社においても、実行会社においても実行される場合がある。

7.1 外部サービス会社の提供するサービスの需要

企業が情報セキュリティ分野における外部専門家を使う主な理由は、IT分野の場合と同じく２つある。

第１の理由はセキュリティシステムのメンテナンスと管理の費用を節約する意向と関連した経済的な目的である。多くの企業にとってこの目的はより切実となっている、これを自社の力で解決する場合、コストと効果の問題が発生する。この場合、理想的には多数の狭い範囲の専門スタッフ（あるいは１人でも、非常に高い資格の専門スタッフ）を抱え、彼らにワークステーションを準備して与え、定期的に彼等の教育を行い、高額の給料を支払うことが必要である。外部の専門家を利用すれば、かなりの資金を節約できる。

ロシアでは、アウトソーシングサービスの導入が経済的に有利であると考えている企業のうちの大部分は大企業、西欧スタイル経営の企業、あるいは外国企業の代表部である。

第２の理由は、情報セキュリティのような一定の狭い分野において深い知識と経験実績を備えた専門家が不足していることである。ところが、（少なくとも十分資格のある）外部実行会社は内部に最新技術を備え、（自社では保証が困難な）提供サービスの高品質を保証することが出来る。

例えば、国営組織においては、「特別な」扱いが必要な機密情報が扱われることから、セキュリティシステムはしばしば非常に高価で複雑なものとなる。ところが、この場合労働賃金レベルはそのようなシステムを扱うことのできる高い資格の専門家を維持することが出来ない。

小規模な会社では、保護システムを扱うために新しい要員を雇用することが常に目的に沿っているとは言えない。別個のスタッフに委託するには保護確保機能が余りに少ないが、同時に現在のスタッフにそれを委託するには多すぎるような場合がある。そのような場合、アウトソーシングは高い資格を備え、必要な仕事を必要な品質レベルで実行する専門スタッフの「仮想の半分」を１年間取得することを可能とする。

例えば、年間の厳しい支出計画は多くの組織の特徴的な問題である。通常、国営企業は人材の教育や採用、その他の物に計画外の資金を出すことができない。アウトソーシングは毎年のサービス費用、すなわちどの位必要でそれ以上は不可能という状況をバランスさせることができる。

アウトソーシングを用いるもうひとつの理由は、国営組織の多くに見られる頭脳流失の現状である（低賃金は資格のある人材を引き止めることは出来ない）。このような場合、具体的な人物に依存しない運用組織を持つことは非常に重要な必須事項となる。スタッフは病気したり、休暇を取ったりする場合がある、その場合でもシステムの稼動能力およびセキュリティレベルに影響があってはならない。

アウトソーシングはスタッフの病気、休暇あるいは解雇に関係なく必要なサービスレベルを提供することができる。賢いサービス提供業者は、保護されたシステム自体およびそのシステムにおける全ての動作が厳密に規定されており、したがってITシステムはもはやリソース保護の有効性の鍵を握る１人のスタッフが知っている「ブラックボックス」ではなくなるような形で発注者と相互関係を構築する。

そして、最終的に、ITおよびセキュリティが事業活動の本筋でない多くの会社は自社のインフラストラクチャーを発展させる価値はないと決定する。情報セキュリティシステムのサポート機能をアウトソーシング

に委託することにより会社はビジネスにとってより重要な課題に力を集中することができる。

7.2 障壁と恐怖

ITアウトソーシングサービスの主な障害は自社のリソースおよびシステムに対する管理を失う恐怖と外部実行者への不信である。

セキュリティ分野におけるアウトソーシングサービスの利用における障壁もほぼ同じである。企業管理部門の主要な恐怖のひとつは機密およびクリティカルに重要な情報の漏洩と喪失への恐れである。そのようなサービスの発注者は、その内部リソースへのアクセスがハッカー、競争相手などに開示されないことの確認を望んでいる。

Digital Research社の調査によれば、アウトソーシングサービスを利用している会社における情報漏洩の主要経路は正規従業員の行為（約60%のケース）である。情報喪失の残りの40%強のケースもアウトソーシングとは関係がない、その原因はかなりつまらない理由（ノートブック、書類、データメディアなどの紛失）によるユーザの不注意である。調査の結果は十分に説明ができるものである、またユーザの不注意および一般的理解レベルについては既に述べた。

さらに、情報技術分野と情報セキュリティ分野におけるサービスを比較すると、外部サービス組織がデータベース、サーバ、バックアップコピーシステムその他ITコンポーネントを扱う場合、外部のスタッフが保存データに直接アクセスすることである。しかしセキュリティ分野のサービス会社のスタッフは保護手段へのみアクセスするが、情報そのものに対してはアクセスしない。

機密情報およびクリティカルなシステムがアウトソーシングに出されてもより脆弱となることはないという基本的な保証がアウトソーシング会社の高い資格、規律および責任である。

よく言われるように、アウトソーシングサービスは高価であるということは、甚だ疑問な障害であり、そのような障害は市場に存在するサービスオファーを調査し同様な業務に対する自社経費の評価を行うことにより取り払うことができる。多数の顧客にサービスを提供するそれなりに大手のサービス会社に委託すれば、それらの会社は大量サービスを行っているので（例えば、ITコンポーネントにおけるセキュリティの新しい脅威および脆弱性の監視がひとつの部課で全ての発注者に対して行われるが、発注者自身が自社に同様な部課で維持するのは遥かに高価なものとなる）、その価格は明らかにより低いものとなる。この問題における困難さは、むしろアウトソーシングの経済的メリットの計算法とサービス品質の評価法である。

自動化レベルの高い、業務のセキュリティと連続性の保証に対して高度の要求をもつ会社（主として大手）は、サービス会社が彼等のシステムの特殊性の十分な知識を持たず、サービス品質のレベルの低いことがアウトソーシング利用の障害であると考えている。そのような欠点はセキュリティ部門の全てのサービス業者が持っているわけでは全然なく、その中の幾つかの業者は完全に良心に基づいて業務を行っている。

もちろん、セキュリティ分野におけるサービス業務市場のこの部門は未だ若く、十分文明化し成熟していないこともその影を落としている。実際に高品質のサービスを提供できるセキュリティ分野のサービス会社は今のところ少ない。選択の幅が狭ければ、ユーザは業者を比較したり、あるいは品質が不満な場合に切り替えたりすることはできない。アウトソーシングサービスの潜在的な需要家の立場では、大部分の業者がこの品質での長期の業務実績と十分な顧客「プール」を持っていないという理由による業者に対する自然な不信感がある。

しかしながら、一定の条件を遵守すれば、アウトソーシングサービスの潜在的な需要家は最適のケースを

選択することができる、そのためには専門的なサービス業者を選択し、その業者との関係を正しく構築する必要がある（以下の項目参照「基本的に、ロシアの情報セキュリティ市場における優良企業の数は少なくない。優良IT会社の数についても同様である。残る問題はこの２つのグループのオーバーラップする部分を見付け、選択したサービス業者との関係を賢く構築することである。

7.3 サービス会社の選択

残念なことに、情報セキュリティのみに特化した会社はしばしばサービス提供の経験や整備されたスキームが不十分である。さらに、それらの会社には保護システム運用課題解決の際にしばしば必要となる関連するIT分野の専門家が通常居ない。

様々なIT分野のサービス提供に特化している会社の中には同時に情報分野においてもプロとしての十分な専門知識経験を備えているところは少ない（多くの会社には情報セキュリティの小さな部課があるだけでこの市場における歴史も浅い）。

保護されたシステムの運用課題は総合的な性格のものであるので、発生する多くの問題は情報技術諸分野の境界上にあり、情報セキュリティの機能は大手会社、できれば大規模で複雑なITシステムおよび情報セキュリティシステムの構築およびメンテナンスの経験のあるインテグレータに依頼すべきである。そのような会社の中で作業実行者を選択するための判定基準は幾つかある。

その最初の部分はサービス会社の資格に関するもので、発注者の所にある全ての保護手段およびシステムのサービスを行う能力をその会社が備えていることを確認する。想定される実行者がロシア企業のITシステムにおいて広く運用されている保護システムや技術納入業者の大多数と長期パートナー関係を持っていること、メーカーでの資格教育および認定を受けた資格のあるサービスエンジニアを必要な人数抱えていることが重要である。

実行者は技術および機器、すなわち保護システムにおける様々な技術的問題をエミュレート（シュミレート）しその振舞いのいろいろなケースを研究する試験ラボ、ITコンポーネントの保護状況分析用の特殊ツールその他を備えている必要がある。

オファーされるサービスは（最低レベルのテクニカルサポートから鑑定調査およびアウトソーシングまでを含む）総合的で、柔軟性があり、具体的な会社の条件に適応できるものでなければならない。例えば、ITシステム動作のセキュリティ・信頼性に特に要求の高い会社のメンテナンスの場合、すべての必要なリソースを集め発生した問題を最迅速に解決する要求およびその実施に対して直ちに取り掛かることのできる担当テクニカルサポートマネージャを置くことが実行者に求められる。

多くの会社にとって実行者がサービスセンターをモスクワだけでなくその他の都市に持っていることも重要である、その数が多いほど保護された分散システムのサービスの品質が高くなりコストは低くなる。判定基準の他の部分はサービス会社の経験と評判に関するものである。

7.4 アウトソーシング、サービスの種類とレベル

今日オファーされているアウトソーシングサービスの全体はその種類（セキュリティ手段とシステムのメンテナンス、分析課題その他）およびレベル（セキュリティの管理、検査）により分類できる。

わが社の解釈では、純粋に保護された情報システムレベルのサポートに関係のない幾つかのサービス（設計審査、セキュリティの複雑な事件の解明その他）は情報セキュリティ問題に関するコンピタンスセンター

の枠に含まれる（第８章参照）。

総合的にこの２つのグループのサービス業務は事実上あらゆる企業のリソース保護に関するあらゆる課題を解決することができる。

アウトソーシングサービスは企業の必要性および特殊性、すなわち保護のために用いられるひとまとめの決定、情報システム運用の実績経験、利用できる人材および機器などに応じて選択される。

7.4.1 情報保護手段の管理

外部実行者に委託できる最低レベルのサービスは保護手段の管理とメンテナンスである。アウトソーシングには大抵（またそれは理に適ったことであるが）、管理に非常に高い資格と動作に関する深い理解が要求されるセキュリティ確保の複雑な手段が依託される。その中には攻撃検出および保護状況検査の手段、トラフィックの内容分析およびフィルタリングシステムその他「細かい」設定、発生する事象の正しい解釈および運用プロセスにおいて全体としてかなりの注意を必要とするその他の手段が含まれる。さらに、発注会社のユーザに対しては保護手段のメンテナンスと関連した質問の受入れと処理を１日24時間体制で保証提供できる。

外部のサービス会社は情報保護手段の導入および統合化のサービスを行い、その１日24時間体制のメンテナンスおよびテクニカルサポートを実行し、ソフトウェアの標準的なアップデートを行い、必要に応じてその設定の修正を行い、機器のハード部分のバックアップを行うことができる。

その際、保護手段のポリシーおよび運転規則の作成、さらにこれらの手段からのレポートの取得は発注会社のセキュリティ業務の職掌に残され、アウトソーサはセキュリティポリシーの要求に応じた保護手段の設定のみを保証する。

7.4.2 セキュリティシステムのアウトソーシング

次のレベルは情報セキュリティ全システムのアウトソーシングへの発注である。この場合サービス組織は単に適用保護システムの稼動能力と正しい構成に対して責任を負うだけでなく、全総合的な手段により保証されるリソースの保護状況の信頼できるレベルに対する責任も負う。

そのために、前項に列挙した機能以外に、アウトソーサはシステムセキュリティ状態の（オフラインあるいはオンラインモードの）常時監視、発生事象の分析とその解釈、（攻撃やその他の重要な事象の可能性に関する間接的な証明となる）クリティカルなシステムパラメータの状態および変化の監視を行い、事象への対策を講じる（あるいは発注会社の担当者に然るべき指示を出す）。必要な場合はクリティカルな問題を解決するために緊急出動を行う。

その際、発注会社のセキュリティ業務はアウトソーサが記録しその行動をフィックスするログおよびサービス会社が提出するセキュリティ事故、原因、影響および講じられた対策に関する報告に基づき、外部のサービス会社のサービスの品質の検査を行う。

7.4.3 分析課題

様々な理由により、大幅な人的および機器リソースを必要とし、また専門家に高い資格だけでなく作業の実績経験が要求される分析課題もアウトソーシングに出すべきである。それにはセキュリティの新しい脅威、脆弱性および攻撃方法の出現に関するデータの収集および分析調査、保護される情報システムへのその危険性の評価およびリソース保護における脆弱性の除去（あるいはその除去勧告を発注会社の担当者へ与えること）などが含まれる。

作業の構成内容は原則的に一定期間提供される「リソース保護状況の分析と検査」サービスにおけるものと同じである。その他の分析調査サービス、すなわちセキュリティ分野における事故の調査、情報セキュリティの観点からの情報システムにおける変更の評価その他については「情報セキュリティ問題のコンピタンスセンター」の章に詳細に述べられている。

7.5 情報セキュリティ機能のアウトソーシング委託の準備対策

もちろん、先ず第１に、全ての組織はいかなる条件の下に自社のリソース保護確保を外部の会社に委託すべきか、さらにそのようなサービスの利用がビジネスにとって何をもたらすか（これについては「外部サービス会社の提供するサービスの需要」の項目で触れた）を明確にする価値はある。外部組織のサービスの必要性が明らかな場合、先ず第１に、ではどの機能、課題および保護要素をアウトソーシングに委託すべきかを決める必要がある。

セキュリティ確保システムを外部サービスに委託することが更なるリスクと脅威の発生を想定することを考慮すれば、特に複雑な組織構造の大手企業の場合、総合的な準備措置を講ずる必要がある。この準備作業の一部も外部の実行者が行うことができる、しかしそれにはセキュリティ業務の管理機能が存在しそのサイドからの管理が必ず行われることが条件である。

アウトソーシング委託への準備のためにはITシステムおよび保護システム運用の実績経験、さらに会社のその他の特殊性の分析調査を行う必要がある。これらのデータを出発点として、情報セキュリティ条件維持の要求や外部サービス業務条件におけるセキュリティ確保のスキームを作成する必要がある。その結果となるものが実行時のこのスキーム導入の組織・技術措置計画である。すなわち手段およびシステムの外部業務移行の各段階、必要条件およびリソース（例えば、追加のソフト・ハード）その他である。情報セキュリティの観点から外部組織との関係の規定手順（「サービス会社との関係の規定手順」の項参照）、さらに外部組織の行動の監視（モニタリング）および協定と関連した企業の情報システム業務の新しい課題の定義も作成されたスキームの重要な部分である。

外部サービス会社の行動管理の課題はクリティカルな重要課題であり、内部セキュリティ業務の基本的な課題となる。それを効果的に解決するためには、監視システムを構築するかあるいは既存のシステムに追加を行う必要がある、すなわち情報セキュリティシステムのコンポーネントおよびITコンポーネント（ネットワーク、サーバ、アプリケーションシステムその他）の管理、フィルタリングおよび登録イベントログ（ログファイル）の分析の追加手段、さらに、組織のコンピュータネットワークを通して転送される情報、システムおよびアプリケーションユーザの行動、情報リソースおよびシステム、認証方法その他へのアクセス方法の管理手段が必要である。監視システム運用の手順、すなわち管理が必要なコンポーネント、管理行動の頻度、それぞれの対応形式、ログファイルを含む情報保存手順などを定める必要がある。その後、監視システムは運用のために企業の内部セキュリティ業務へ引き渡されなければならない。

もうひとつの重要な条件、すなわちアウトソーサがその機能をリモートで実行する場合、全てのリモート接続のセキュリティと信頼性を確保する必要がある。そのために、外部のサービス会社は発注会社とのバーチャルプライベートネットワークを構築しその保護されたチャンネルのバックアップを構築する必要がある。

7.6 アウトソーシングのメリット

アウトソーシングサービス需要家が受ける主なメリットは（作業が要領よくきちんと組織された場合）、

情報セキュリティシステム運用時の費用の削減、要員問題の解決および同時に得られる対応する作業実行の品質向上である。

アウトソーサは類似の作業実行の実績経験および全ての必要なリソース、すなわち狭い範囲の専門の高い資格の専門家、特別なソフト・ハード手段およびテストステーションなどを備えており、これら全てが労働日や労働時間の間だけでなく１日24時間体制となっているので、アウトソーシングの技術を用いることにより、会社が被害を蒙るリスクを低減することができる。

その際、リソース保護システムは、それを扱う発注会社のユーザからも、メンテナンス会社からも隔離されたものとなる。リソース保護システムの信頼性および稼動能力は発注会社の状況に依存しないものとなる。セキュリティ分野の幾つかの分析課題、すなわち新しい脅威、「セキュリティホール」や脆弱性、攻撃方法の出現に関する情報の収集および分析調査、情報システムコンポーネント保護状況に対するその影響の評価は多大な時間、専門家および知識が必要であるので自社の力だけで解決することは原理的に困難である。しかしながら、それらはリソース保護状況に大きな影響を及ぼす、すなわち保護システムは最新の傾向に対応している必要がある、それゆえ無視することはできない。

業務の本筋でない機能に対する責任をアウトソーサに委託することにより、自社の主要なビジネス課題の解決に力を集中し、本来のビジネスの効率を高めることができる。

8. 情報セキュリティ問題のコンピタンスセンター

コンピタンスセンター、これはリソース保護の非常に異なる様々な条件および要求をもつ様々な規模の企業に役立つ総合的なサービスである。その主旨は一定の範囲の分析調査、コンサルティングおよびその他のサービスを受ける設定期間付の「利用権」である。

コンピタンスセンターの範囲内で、外部会社の技術専門家は発注会社が関心をもつ問題についてコンサルティングを行い、情報を提供し、さらに情報セキュリティ分野および情報技術関連分野におけるその他の種類の作業を実行することができる。

コンピタンスセンターの利便性はいかなる時点においてもその時点でまさに必要なサービスを利用できることである。例えば、具体的な事象（イベント）がその情報システムにとってクリティカルか否かを理解するために保護手段あるいはITコンポーネントのイベントログ内のレコードの分析および解釈に支援を仰ぐ場合などである。あるいは、緊急作業、例えばネットワーク間のファイアウォールあるいは外部攻撃検知撃退システムの導入を休日だけで（労働日にそのような作業を行なえばITシステムの稼動に支障を来たすのでそれはできない、またポリシーや規則を含め完全導入を短期間で自社の力だけで行うことも不可能である）行うために資格のある専門家を呼ぶ場合である。

外部の専門組織は発生した特殊な状況の克服あるいは困難なセキュリティ事故の調査の支援を行うことができる。保護システムの故障およびその他の不都合な事故は通常最も予期していない時点、例えば祭日、休暇中その他の場合に発生し、社内に専門家を見付けることがしばしば不可能である。サービス会社ではそのような専門家は１日24時間体制で常駐しており、発生した状況を克服するために彼らを支援に差し向けけることができる。

困難なセキュリティ事故の調査はしばしば全く異なるIT分野の専門家の緊急投入およびそのお互いの協力

作業を必要とする。企業内にそのような専門家を在籍させ必要な時点で彼らをグループで招集する困難な問題以外に別の困難な問題もある。

例えば、データベースからデータが盗まれた場合である。セキュリティ業務のスタッフには何ができるであろうか？自社の戦力はわずかである。最低限、データベースの専門家そして恐らく他の分野の専門家も必要である。しかも、情報の漏洩源が社内にある可能性があることも状況を困難なものとしている場合がある。そのような場合、状況を解決するためにはやはり外部の独立したプロの専門家が必要である。

また、外部の専門会社は情報セキュリティ障害により発生した対外的摩擦状況の解決において発注会社の利益を代表することもできる。

コンピタンスセンターの範囲内においてもうひとつの重要な側面の仕事がおこなわれる、すなわちITインフラストラクチャー変更（機能スキームの新規接続、変更、計画に基づいたシステムの完成作業）の評価あるいはセキュリティの観点からのITプロジェクトの審査である。

例えば、社内において主に新しいサービスの導入や拡張と関連したIT構造の再構築が殆ど連続的に行われている場合である。セキュリティ業務においては驚異的な頻度でプロジェクトが目白押しとなる。ネットワーク、メールシステムの更新、新サービスの導入、例えばSAP、Lotus文書システム、データベースの改修、支社の接続など、考えられる変更リストは長大なものとなる。これら全てのプロジェクトにセキュリティ基準遵守の要求を出す必要があるが、このような状況下においてはどのセキュリティ業務も対処できない。

市場で需要がコンスタントに伸びているサービスを提供している大手および飛躍的に発展している会社では、ITシステムの発展および更新は事実上連続的なプロセスである。

新規導入が提案されている状態におけるセキュリティ要求事項作成の準備あるいは支援、再編問題の会議における能力のある外部組織の参加その他により、セキュリティ業務の「負担を軽くする」だけでなく、より根拠のある現実的なセキュリティ対策を作成する支援を行うことができる、それは外部会社の場合全ての必要な専門家を（しかも情報技術の他の分野の専門家も含め）集めることができるからである。さらに、同じ分野で業務を行う複数の発注会社はしばしば類似の問題、例えば保険会社、テレコム通信会社、銀行その他それぞれに特有の問題を抱えている。したがってセキュリティ分野の専門会社にとっては発注者の問題は高い確率で既に知られている問題なのである。

9. サービス業者

基本的に、ロシアの情報セキュリティ市場における優良企業の数は少なくない。優良IT会社の数についても同様である。残る問題はこの２つのグループのオーバーラップする部分を見付け、選択したサービス業者との関係を賢く構築することである。

9.1 サービス会社の選択

残念なことに、情報セキュリティのみに特化した会社はしばしばサービス提供の経験や整備されたスキームが不十分である。さらに、それらの会社には保護システム運用課題解決の際にしばしば必要となる関連するIT分野の専門家が通常居ない。

様々なIT分野のサービス提供に特化している会社の中には同時に情報分野においてもプロとして

の十分な専門知識経験を備えているところは少ない（多くの会社には情報セキュリティの小さな部課があるだけでこの市場における歴史も浅い）。

保護されたシステムの運用課題は総合的な性格のものであるので、発生する多くの問題は情報技術諸分野の境界上にあり、情報セキュリティの機能は大手会社、できれば大規模で複雑なITシステムおよび情報セキュリティシステムの構築およびメンテナンスの経験のあるインテグレータに依頼すべきである。そのような会社の中で作業実行者を選択するための判定基準は幾つかある。

最初の部分はサービス会社の資格に関するもので、発注者の所にある全ての保護手段およびシステムのサービスを行う能力をその会社が備えていることを確認する。想定される実行者がロシア企業のITシステムにおいて広く運用されている保護システムや技術納入業者の大多数と長期パートナー関係を持っていること、メーカーでの資格教育および認証を受けた資格のあるサービスエンジニアを必要な人数抱えていることが重要である。

実行者は技術および機器、すなわち保護システムにおける様々な技術的問題をエミュレートし、その振舞いのいろいろなケースを研究する試験ラボ、ITコンポーネントの保護状況分析用の特殊ツールその他を備えている必要がある。

オファーされるサービスは（最低レベルのテクニカルサポートから鑑定調査およびアウトソーシングまでを含む）総合的で、柔軟性があり、具体的な会社の条件に適応できるものでなければならない。例えば、ITシステム動作のセキュリティ・信頼性に特に要求の高い会社のメンテナンスの場合、すべての必要なリソースを集め発生した問題を最迅速に解決する要求およびその実施に対して直ちに取り掛かることのできる担当テクニカルサポートマネージャを置くことが実行者に求められる。

多くの会社にとって実行者がサービスセンターをモスクワだけでなくその他の都市に持っていることが重要である、その数が多いほど保護された分散システムのサービスの品質が高くなりコストは低くなる。

判定基準の他の部分はサービス会社の経験と評判に関するものである。先ず第１に、市場における業者のプロとしての実績経験およびそのようなサービス実施の成功例が重要である、それは彼等の実施した仕事の品質レベルを証明するものである。したがって、サービス業者の選択に当っては評判のよい大手の有名会社に的を絞るべきである。

9.2 サービス会社との関係の規定手順

調達するすべてのサービスは指定品質レベルのものでなければならない。情報セキュリティのような分野においてはこれらのサービスは非常に重要な意味をもつ。したがって、サービス会社との接触では必ずサービス自体の仕様（特性パラメータ）、サービス品質管理の仕様（特性パラメータ）、さらに品質の低いサービスに対する実行者の責任を最も正確かつ詳細に決定する必要がある。

外部のサービス組織との契約では特に下記の諸点を規定する必要がある。

- サービステリトリーおよび対象
- サービス提供時間（勤務時間内、１日24時間）
- 問い合わせあるいは事故に対する対応時間およびその解決の最大期間
- 発生した問題のタイプおよび困難さに応じた問い合わせに対する対応方法
- 報告提出の手順および形式
- 追加費用の問題（例えば、システムに発生した脆弱性を急遽除去する必要がある場合など）

- 機密保持の要求

これらの諸点に関する条件設定が不完全であったり、不正確な場合、外部サービス利用のすべてのメリットを損なうだけでなく、被害を蒙ることもある。

例えば、契約の中に問い合せに対する対応時間が規定されていない場合、実行者は情報が伝えられた問題の解決について長時間「考え込む」こともあり得る、ところがその間に初期の段階では止めることができたであろうウィルスやその他の攻撃が、例えばすでに重要なアプリケーションのサーバをダウンさせてしまう。この場合、実行者に対して遅れたことに対するクレームを出すことは無駄である。

また、問い合せに対して実行者が対応する方法についても規定しておくことも重要である、例えばネットワーク機器あるいは保護手段において設定した規則の修正問題で外部会社がセキュリティ管理者に対して行う支援などの場合、電話相談で十分な場合がある。さらに複雑な技術的な問題の場合には、恐らく発生した問題のリモート診断および外部のサービスエンジニアによる解決（保護されたチャンネルを通した保護手段の操作）が役に立つであろう。しかし、リモート支援が有効でないクリティカルな場合には、発注会社現場への緊急出動が必要となる場合がある（ここでもまた、この出動を長時間待つようなことにならず、到着した専門家がこのような場合にすべて準備された作業を行い、その品質に対して実行者が責任を持つようにすることが重要である）。

外部サービス会社が提出する報告および記録情報はその活動の主要な管理手段である。どのような形式で、どのくらいの頻度で、またどの程度の詳細度でこの情報を提出するのか、必ず契約書に規定されていなければならない。

したがって、賢く作成されたサービス契約では予め合意した判定基準により実行者の作業を管理でき、サービスが実行されなかったり必要な品質が満たされていない場合、責任を問うことができる。

10. ABITELグループについて

ABITEL社グループはロシアにおける指導的システムインテグレータのひとつであり、情報セキュリティの分野にも特化している、また独自の情報保護手段のメーカーでもある。

ABITELの抱える人材は、世界のセンターや情報セキュリティおよび情報技術の分野における製品や技術の世界的な納入業者において研修を受け、高いレベルのプロ資格をもつ。

高資格の人材とマネジメントおよびABITELの技術的組織的可能性を合わせ持つことにより、大手企業顧客に対しても、個々の発注者に対しても会社は最良の業務パートナーのひとつとなっている。

2005年４月に日本に独立法人「Abitel Data K.K.」を開設し、ABITELグループは、情報セキュリティシステムの納入、インストール、設定およびサポートの総合業務を含む全範囲のサービスを日本市場に提案する可能性を獲得した。