資産運用会社に潜むリスクとセキュリティ対策

昨今、標的型メール攻撃や内部犯行によるデータ漏えいによる大きな被害が発生しており、従来とは異なるセキュリティ対策が必要とされている。平成27年12月にはサイバーセキュリティ経営ガイドラインが公表され、資産運用会社においても経営者によるセキュリティ対策推進が求められている。

資産運用会社に想定されるリスク

昨今、標的型メール攻撃や内部犯行による情報漏えい等のセキュリティインシデントによるリスクが高まっている。金融機関もその例外ではない。例えば、金融業界における情報漏えいによる顧客のサービス解約率は5.6%に上るという調査結果がある[1)]。資産運用会社では、大手企業と異なりセキュリティ事故は起きにくいと考えているIT担当者もいるようだ。しかし中小企業でも情報が盗まれた（流出した）事例は、顧客情報で4.9%、業務情報（機密情報等）で3.9%あると報告されている[2)]。また、退職者の半数は企業の機密データを保持し、その40%が新しい仕事に使おうとしているという報告もある[3)]。経営者は、大企業でなくてもセキュリティリスクに晒されていることを認識しなければならない。

それでは、具体的に資産運用会社にはどのようなリスクがあるのだろうか。IPA[4)]は情報セキュリティ対策ベンチマーク[5)]というサービスの中で、事業構造上の脆弱性を図る指標として6項目を提示している。①正社員割合（従業者数に対する割合）、②総拠点数（国内外の拠点の数）、③IT依存度、④インターネット依存度、⑤ビジネスパートナーへの依存度、⑥年間離職率、である。様々な意見があると思うが、ここでは①が低く②～⑥が高いほど脆弱性が高いと仮定し、資産運用会社のリスクと対策を考えてみたい。

資産運用会社では、少数精鋭で業務を遂行するため、IT依存度（③）が高く、機密情報をファイルサーバに集約して格納することが多いと思われる。ファイルサーバへのアクセス制限、アクセスログの取得及びPCからのデータ持ち出し制限などの対策がなされていなければ、標的型メール攻撃、非正社員（①）及び退職者（⑥）によるデータ漏えいのリスクが高くなる。

また、資産運用会社は組織をコア業務に集中させることが多く、ビジネスパートナーへの依存度（⑤）が高いのではないだろうか。印刷会社、販社、カストディアン、ファンド組入れ先、スポンサー・評価機関、情報ベンダー、運用委託先等である。このようにパートナーは多種多数存在するが、一方で業務量は少量であり、個別にシステムやネットワークを構築・維持できるほどの規模ではない。そのため、電子メール、Web閲覧やFTPなどのインターネットに依存（④）した情報連携が多くなると想定される。標的型メール攻撃や内部犯行による情報漏えいでは、適切な対策が打たれていないと、これらの技術を利用して外部の情報共有サイトへアップロードしたり外部の個人メールにファイル添付して送付したりすることで、簡単に重要情報を持ち出すことができてしまう。さらに、パートナーがサイバー攻撃被害を受けることもリスクとして捉える必要がある。このように、自社にとってのリスクが潜在する対象範囲を一部の社員や基幹システムに限定することはできない。読者も自社の状況でリスクを分析・評価し脆弱性を検証していただきたい。

資産運用会社に求められるセキュリティ対策

こうしたリスクへの対策を促すために、当局も様々な指針等を打ち出している。平成27年4月には証券取引等監視委員会事務局「金融商品取引業者等検査マニュアル[6)]」が一部改正され、（3）安全対策の整備の中に「②サイバーセキュリティ管理態勢の整備」が追記された。

NOTE

1) IBM「2015年情報漏えい時に発生するコストに関する調査：グローバル分析」
2) IPA「企業におけるサイバーリスク管理の実態調査2015」
3) Symantec「What's Yours is Mine：How Employees are Putting Your Intellectual Property at Risk」
4) 独立行政法人情報処理推進機構（https://www.ipa.go.jp/）
5) http://www.ipa.go.jp/security/benchmark/
6) http://www.fsa.go.jp/sesc/kensa/manual/kinyusyouhin.pdf
7) Computer Security Incident Response Teamの略。組織内で発生した情報セキュリティ問題に対応するチーム。
8) http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html
9) Chief information security officerの略。組織内の情報セキュリティ担当責任者。
10) 以下は10項目の要約である。詳しくは8）を参照していただきたい。
1.リーダーシップの表明と体制の構築
2.サイバーセキュリティリスク管理の枠組み決定
3.リスクを踏まえた攻撃を防ぐための事前対策
4.サイバー攻撃を受けた場合に備えた準備
11) 付録Cでは、ガイドラインと、情報セキュリティマネジメントに関する国際規格であるISO/IEC27001及び27002との関係を示している。
12) IPA「情報セキュリティ人材の育成に関する基礎調査」
13) NRIグループではセキュリティ対策に関連して次のような製品・サービスを提供している。「CIO/CISO支援」「セキュリティポリシー策定支援」「組織内CSIRT構築・運用・評価」「セキュリティ診断／設計開発支援」「標的型メール攻撃被害シミュレーション」「セキュリティ事故対応支援」「端末セキュリティ」「人材育成・研修」「ログ監視サービス」「メール誤送信防止」「メールフィルタ」「プライベートクラウド」等 http://www.nri-secure.co.jp/service/index.html

投信運用業者がサイバーセキュリティを経営上の重大な課題と認識し、以下の対策を取ることを求めている。

- 体制整備（監視、報告、広報、CSIRT[7]）
- 多層防御（入口対策、出口対策、内部対策）
- 被害の拡大防止措置
- システム脆弱性に対する適時対策
- セキュリティ水準の定期的な評価の実施と対策の向上
- 業務やリスクに見合った認証方式の導入や不正防止策
- コンティンジェンシープランの策定、訓練、見直しの実施及び業界横断的な演習への参加
- サイバーセキュリティ人材育成、拡充計画策定と実施

これらの対策の特徴は、サイバー攻撃の被害を受けることを前提とした整備が求められていることである。

平成27年12月には経済産業省よりサイバーセキュリティ経営ガイドライン[8]が公表された。ここでは、経営戦略上ITの利活用が不可欠である企業の経営者が、サイバー攻撃から企業を守る観点で認識する必要がある「3原則」が示された。

- 経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
- 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策を進めることが必要
- 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

また、情報セキュリティ対策を実施する際の責任者となる担当幹部（CISO[9]等）に経営者から指示すべき「重要10項目[10]」が示されている。加えて付録として、具体的なチェックシートや望ましい技術対策等も掲載されており、これらを考慮した対応が求められている。付録ではさらに、ガイドラインと国際規格との関係も示している[11]。将来的に国際規格を意識した情報開示や国際標準の認証取得を求めているものと思われる。

これからのセキュリティ管理態勢の整備について

2020年の東京オリンピック開催に向けて、ITの高度利用が推進される中、IT人材の不足、情報セキュリティの対策範囲の拡大が想定される。IPAの報告によると、国内の従業員100人以上の企業において情報セキュリティに従事する技術者は約23万人、不足人材数は約2.2万人と推計されている[12]。また、この23万人のうち約14万人に対しては、更に何らかの教育やトレーニングが必要とされている。このような中で有効な人材を獲得し維持することは、資産運用会社にとって困難だろう。

しかし、最近では外部の専門企業による管理態勢の診断と整備支援、手が回りにくかったログ分析支援や低価格なクラウドを利用したセキュリティソリューション[13]などのサービスが出てきており、活用しやすくなってきている。ただし、これらの外部リソースもやがて奪い合いとなるだろう。是非、手遅れとならぬように経営層自らが推進して、セキュリティ管理態勢の整備と維持に取り組んで頂きたい。

Writer's Profile

出井 智 Satoshi Idei
資産運用基盤サービス部
上級テクニカルエンジニア
専門はITインフラ設計
focus@nri.co.jp