クローズアップ

現実の脅威に対する管理策の強度を判定

世界初の情報セキュリティ格付専門会社がスタート

株式会社アイ・エス・レーティング　常務取締役（企画担当）　長野敏利氏　http://www.israting.com/

2008年7月1日、企業や組織の情報セキュリティの信頼度を評価して格付するサービスがスタートした。
サービスを提供するのは30社が出資して設立された株式会社、アイ・エス・レーティングだ。情報セキュリティに関する認証制度としてはISO27001やプライバシーマークなどがあるが、格付制度ではマネジメントの仕組みやセキュリティの運用状況に加え、具体的な管理策の強度までを評価する。格付制度の策定経緯と内容、制度の定着やグローバル展開のための課題などについて担当者にお話を伺った

格付制度誕生の背景

2008年5月2日、企業の情報セキュリティの信頼度を評価して格付する情報セキュリティ格付専門会社、アイ・エス・レーティングが設立された。出資したのは格付投資情報センター、松下電器産業、富士ゼロックス、富士通、野村総合研究所など18社で、その後ソニーや東京電力などが増資を引き受け、サービスの提供を開始した7月1日時点での株主は30社になった。「情報セキュリティ格付制度が生まれ、世界初の専門会社アイ・エス・レーティングが設立された背景には、大きく二つの事情があります」と語るのは、同社の常務取締役で企画担当の長野敏利氏。

1つは、経済産業省の産業構造審議会情報セキュリティ基本問題委員会における討議だ。2007年5月10日に公表された報告書「グローバル情報セキュリティ戦略」には情報セキュリティ先進国の実現のための戦略が提案されており、「情報セキュリティ対策の成熟度向上等に向けた市場メカニズムの強化策」の1つとして「情報セキュリティ対策状況に係る情報開示を通じた民間格付の促進等」と記されている。

もう1つのきっかけは、食品偽装などの問題が引き続き起こったが、その当事者の中に環境のISO14000や品質のISO9000の認証を取得していた企業があったことだ。その時の社会の論調は、「なぜ、そういう企業にISOを認証したのだ」というものだった。

もともと、ISO9000やISO14000はマネジメントシステムを評価する認証制度であり、実際の製品の品質を保証する制度ではない。同様に、情報セキュリティにおける規格のISO27001も対象はマネジメントであり、必ずしも情報セキュリティのレベルを保証するものではない。今、社会が要請している情報セキュリティの評価制度は、単にマネジメントが回っているかを見るのではなく、それにプラスして情報セキュリティのレベルを評価する新たな仕組みにある（図1）。

格付制度の検討は2006年初め頃から開始され、2007年7月18日には「情報セキュリティ格付制度研究会」を発足した。発起会社は格付投資情報センター、NTTコミュニケーションズ、松下電器産業、富士ゼロックスの4社で、東京海上日動火災保険、凸版印刷、富士通、野村総合研究所、三菱総合研究所、みずほフィナンシャルグループ、三井物産が参画。オブザーバーとして経済産業省、総務省、金融庁、情報処理推進機構（IPA）などが名を連ねた。そして2007年末から2008年初頭には大体の方向性が固まり、5月のアイ・エス・レーティング設立を迎えることとなった。

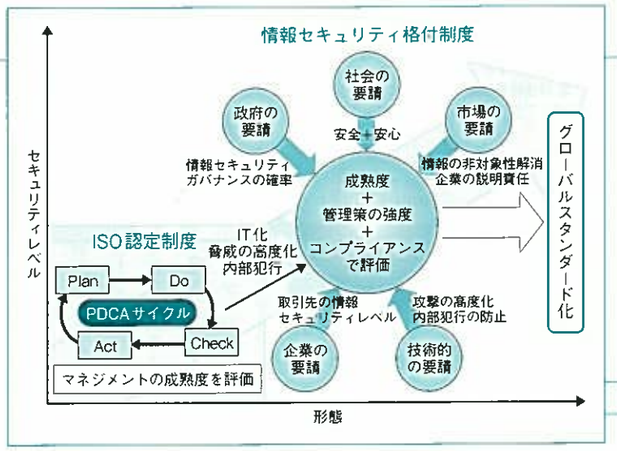

図1　時代が要請する情報セキュリティ格付

格付審査

情報セキュリティ格付制度の信頼性を高め、普及させるためには、格付を行う第三者機関の信頼性と中立性を確保しなければならない。

これを確保するための仕組みとして、アイ・エス・レーティングでは以下の考え方を導入している。まず、株主企業1社からの出資は全体の20%未満と制限されている。また、役職者とアナリストは出向元との兼務が禁止（当初2年間は例外）されており、株主・会員企業1社からの出向者は全体の20%未満に制限されている。さらに株主・会員1社への業務委託も、全体の20%未満と定められている。当然、株主・会員は、格付会社のインサイダー情報を自らの事業展開に活用してはならない。

アイ・エス・レーティングによる格付サービスの提供開始は2008年7月1日だが、長野氏は「課題はやはりISO27001やプライバシーマーク制度との違いを周知し、格付取得のメリットを理解してもらうこと」だという。

プライバシーマークの対象は個人情報に限られている。要件は2つで、1つは個人情報保護法にある法的要求事項への対応だ。たとえば、情報を預かるときに利用目的を明示し、承諾を得る。目的外使用はしないなど。もう1つは安全管理への対応であり、預かった情報をどう管理するか、という情報セキュリティの課題である。

ISO27001はITや電子データに関するマネジメントシステムが対象だ。データの中には個人情報も含まれているので、プライバシーマークの範囲（安全管理）と一部重なっている。ISO27001の取得によりPDCAサイクルの高度化を図ることで、企業や組織に情報管理の風土を構築するなどの効果が大きい。

一方、格付制度では、風土作りだけではなく、実際の取引などに必要な被格付組織の情報管理のレベルを明確に表す。格付制度は、実際の管理策強度までを測るとともに、企業の信頼度や企業間取引での判断材料を提供する。ISO27001の規格をベースにしつつも、サービスの観点から見るとまったくの別物である。加えて脅威に対する対策の強度、コンプライアンスへの取り組みなどを評価するのが、アイ・エス・レーティングが提供する格付制度ということになる。格付審査で高評価を得たとしても、100%情報漏えいなどが発生しないと保証はできないが、実際のリスク回避策を評価することから、高い信頼性を期待できる。

格付のランクは最高AAA（トリプルA）からB（シングルB）までの16段階が設定されている。格付審査は次の3つのステップで行われる。まずステップ1が、「管理体制をみる」ステップで、情報セキュリティの統

■3つのサービス
1.「自己診断カルテ」は、ウェブを使ったセルフチェックツール
2.インディケーション評価は、組織の実力把握のための評価サービス
3.評価結果を受けて、必要に応じてレベルアップを図った後に本格的な格付を取得

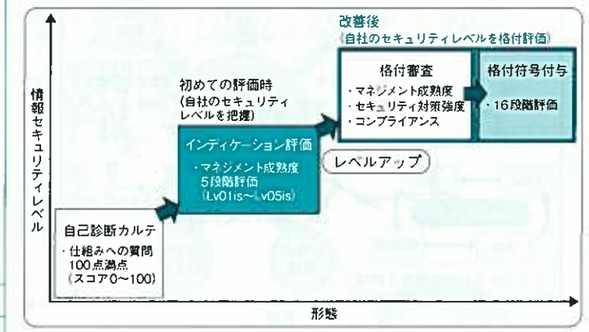

図2　3つのサービス

括部門（ルールを作成している部署）において、管理体制に関する文書を審査。続いて統括部門トップのインタビューを行い、文書の内容について確認を行う。

ステップ2は「管理体制の運用、成熟度をみる」ステップだ。格付の対象となる組織において、ルールが正しく運用されているかをチェックする。事前に質問書を渡して回答してもらい、その内容を見ながら現地調査を実施すると同時に現場責任者のインタビューも行う。

最後のステップ3は『重要情報についてリスクと対策の強度をみる』ステップだ。インタビューを通じ、格付対象の部門の中で最も重要な情報資産を選定する。そしてその重要情報の流れに沿って対象部門の業務フローを作成し、そこでの想定リスクと対策について現地調査を行う。同時にインタビューやテクニカルテスト等も実施して審査する。そしてアナリストによる3つのステップの審査が終了すると、独立組織である格付委員会が開催され、審議により格付符号が決定される。

格付のためのクライテリア（評価基準）は、評価分野をISO27001に完全準拠して作成されている。そして評価項目に格付け提供価値を盛り込んだところに特徴がある。評価カテゴリーと評価基本要件は133分野、個別要件として500～1000の評価項目が用意されている。ISO27001には無い格付制度独自の項目としてはたとえば、発注元から預かった情報を元にソフトウェアの試作品（たとえばDVD・RAMなどのメディア）を作成した場合の試作品の管理方法などがある。

アイ・エス・レーティングによる格付審査の特徴は2つある。ひとつは、○×方式ではなく、どのレベルまでできているかを4段階で評価すること。さらにステップ3では、重要な情報資産を特定し、それぞれのリスクにスポットを当てたリスクアプローチという審査を初めて導入していること。リスクに観点を絞ったところに特徴がある。長野氏は「現場できめ細かい調査をすることで、16段階の格付を可能にしている」と語る。ここで気になるのは、すでにISO27001やプライバシーマークの認証を取得している企業が格付を受ける場合だ。特にISO27001に準拠して格付制度の評価分野が定められており、重複する評価項目も多い。長野氏は「現場方法もステップ1と2は、基本的に評価項目としてはISO27001と同様です。特にステップ1は文書審査が中心ですから、ISOの審査の報告書を提出していただければ、相当省略が可能だと思います。同様に個人情報の管理の部分のみについていえば、プライバシーマーク関連の書類も有効だと思います。一方、ステップ2はきちんと現場を確認しなければなりませんから、必ずしも簡略化が可能だとはいえません。」と説明する。

格付支援サービス

アイ・エス・レーティングは世界初の情報セキュリティ格付専門会社だが、各社が個別の基準で取引先等のセキュリティ評価をすること自体は、すでに多くの会社で行われている。たとえばSCM上位企業が新たに取引先に対して詳細なチェックシートを送付し、セキュリティ体制を評価した上でどのレベルまでの機密情報を渡せるかを判断している。

問題は、各社が独自のクライテリアで評価しているため、コストと手間が積み重なっていることにある。また取引先の企業は、上位企業各社

から、重複して評価を受けなければならない。そこに第三者機関が共通のクライテリアで評価された格付制度があれば、発注元は審査にかける手間が省ける上に、新たな取引先を探す際にも有用だ。一方、受注側も1回の評価で済み、結果が良ければ新たな発注元との付き合いができるなど、事業機会が生まれる期待がある。

ただ、情報セキュリティ格付を取りたいと考えていても、費用をかけた結果、低い評価が出てしまっては、ビジネス上逆効果になってしまう。そこでアイ・エス・レーティングでは、3段階のサービスを考えている（図2）。

その最上位は言うまでもなく、正式な格付審査だ。そして「まず自社のセキュリティレベルを把握してから格付を取るか判断したい」という企業向けに現在、『インディケーション評価』の開発が進められている。これは格付の審査項目の中からいくつかを選んで審査し、セキュリティレベルを5段階評価で表す。ビジュアルな形で弱点も分かるようにする予定だ。その結果を受けて問題があると分かった部分を修正し、正式な格付取得へステップアップしてもらおうという仕組みだ。

さらに入門編のサービスとして『自己診断カルテ』も開発中だ。企業や組織の担当者がウェブ画面の質問に答える形で、自分の職場の情報セキュリティの現状を入力すると、セキュリティレベルの評価が点数で表示される。その結果を元に、インディケーション評価、格付取得へと進んでもらうのが狙いだ。

アイ・エス・レーティングでは、出資企業の他に会員企業を募っている。会員になれば、格付結果の詳細を閲覧でき、さまざまな関連情報が入手可能になる。初年度の目標会員数は500社だ。

情報セキュリティ格付制度の構想発表以来、数多くの反響が寄せられているが中でも関心が高いのは格付け結果を使うユーザー企業とその取引先、そしてISO27001でビジネスをしている会社だという。グローバルな格付会社に求められる要件から見て、格付審査を外部委託するのは難しいが、前段階のインディケーション評価については会員になったISO認証会社等の中立機関と連携できる可能性があり、検討中だ。

グローバル展開の課題

格付制度の課題として長野氏は次の3つを挙げている。

まずは、格付制度の定着。格付を取得する企業を増やす一方で、これまで独自のクライテリアで評価していた企業に格付を利用してもらう。実際、評価していた企業側には格付制度に対する期待が大きいが、取引先に格付取得を要求することは、下請法における禁止行為にあたる可能性もある。ポイントはやはり格付取得側に経済的、ビジネス上の効果を納得してもらえるかどうかにある。そのための場作り、雰囲気作りが急務だ。

第2の課題はグローバル展開。ISO27001の元は英国の規格だったように、ISOは欧州中心に出てきている。情報セキュリティ格付は、日本から発信する新しい仕組みだ。格付制度には、制度自体の定着とクライテリアの策定という2つのポイントがある。現在のクライテリアは、日本の会社の事業特性に応じた評価項目で構成されているため、すべてが海外の会社にも適用可能とは言えない。そこで今後、さまざまな国の代表的な企業の参加を募り、世界的に通用するクライテリアの策定を行う予定だ。

3つ目の課題は、まだ先の話ではあるが、情報セキュリティ格付事業で得た経験とノウハウを生かした、格付対象の拡大だ。現在、情報管理全般や事業継続、SCM強化などが候補として挙げられている。

当面の最大の課題はやはり、格付取得企業の獲得だ。長野氏は『従来、日本の製造業における課題はQCD、質とコスト、納期でした。ところがコンプライアンスや環境問題への対応、そしてIT化・電子化が進んだ今日、今は、クリーン調達、グリーン調達、加えて情報セキュリティが必須。世の中、情報セキュリティをしているのが当たり前です。やらないのでは市場から出て行かざるを得ません。情報セキュリティ格付取得には、大きなメリットがあることを理解して欲しい』と結んだ。