経営層にみる,IT及び情報セキュリティのガバナンス
～ CISO Award制度導入を通した考察～

伊藤由紀美[a]
[a] *Y&I ジャパン*
東京都品川区西五反田

Abstract

21世紀初頭において,CIO(最高情報責任者)の役割は確実に定着してきた.日経BP社の「CIO of The Year」の受賞制度は,それを象徴するものでもある.

CIOとは「企業等の組織における重要な経営資源としての情報資産である情報や情報システムに対する戦略等の方向性を示すべき経営層である」という解釈は一般的になったと考える.

CIOの業績評価とは,IT(情報及び情報システム)に対するITガバナンスの評価と考えて良いだろう.このITの領域に,側面から割り込んできた情報セキュリティの位置づけは,ここ数年で変容してきた.

情報セキュリティのガバナンスに対しては,場合によってはCIOが兼務を行うが,米国ではCISO(最高情報セキュリティ責任者)という経営層の役割である事が一般的になり始めている.

筆者は,昨年(2014年)から日本CISO協会の事務局長として活動の企画・運営及び推進等を担当し,初回のCISO Award制度を立ち上げた.同制度導入において,相対的評価を行うツールとして経済産業省の「情報セキュリティ対策のベンチマーク」等を参照した.

初回の受賞企業数社のうち「オブ・ザ・イヤー」に値する企業は一社のみであったが,同企業では,CEOがCISOを兼務するという興味深い特徴が見られた.

守りが目的で内向きだった情報セキュリティ対策等は,サイバー攻撃の常態化やクラウドサービスやスマートデバイスの活用の進展により,より戦略的な位置づけを期待されていると考える.

今後,経営層におけるCISOの役割のレビューや評価を行うにあたり,CIOのそれと同様に検討する意義もあると考える.
また今回のショート報告を通し,CISOとCIOは同化せずとも確実に接近しており,共にリスク戦略を磨く必要があると考える.

Keywords: ITガバナンス,情報セキュリティガバナンス,CISO(最高情報セキュリティ責任者),
日本CISO協会,CISO Award

1.背景

筆者[1]は, 2013年度の国際CIO学会春季大会において,CIO of the Yearの10年目と初代の受賞者との面識をきっかけに,10年間のCIOのロールモデルの変遷に興味を持ち,自らのコンサルティング経験とも関連付けを試みながら,自主研究結果の発表の場を頂戴した. (*詳細は文献[2]ご参照.)

昨今はGRC(ガバナンス・リスク・コンプライアンス)でのコンサルティング業務にシフトしており,組織において,主に情報セキュリティ等の分野を中心に責任を持つ,CISO(Chief Information Security Officer)と称されるマネジメント領域との関連性が強くなった.

また,昨年より縁あって,日本CISO協会の事務局長に従事しはじめ,NISC（総務省）,業界の関連企業等の官民等とのコンタクトの機会が増してきた.

2年前の研究では,関連の多くの文献や学会の先行する研究者の方々の知見を拠り所にして,ぶれない方向の結果を整理できたが,情報セキュリティやガバナンスは別として,CISO学に相当する関連文献も皆無であるため,日頃からの協会等の活動の状況報告等を中心にして分析や情報提供等を行う.

また,後半はCIOとの関連性の観点でも,何がしかの視座を提供する.

2.ガバナンスの潮流

「ガバナンス（Governance）」とは,もともとはITだけの領域ではなく,企業等の組織が社会的責任を配慮した内部統制のしくみである.

[1]Y&Iジャパン代表　伊藤由紀美：平成2年技術士（情報工学）登録.経営とITを統合するコンサルタント.主な専門は流通&マーケティング,内部統制,国際協力.GRC(ガバナンス・リスク・コンプライアンス)等のコンサルティング.2014年より日本CISO協会 事務局長に従事.
URL:http://www.yijapan.com/

日本ではJ-SOX(金融商品取引法)の法制化とともに,市場における組織の秩序のための内部の主要なメカニズムとみなされている.

3. ITガバナンスと情報セキュリティガバナンス

また「ITガバナンス」という言葉も,内部統制（IT統制）が経営管理の一分野と位置付けられつつ浸透してきた.主に企業の情報資産を広くITと捉えた領域といえる.

では,これに近接する,情報セキュリティガバナンスとは,どう考えるべきかについて,下記に示す.

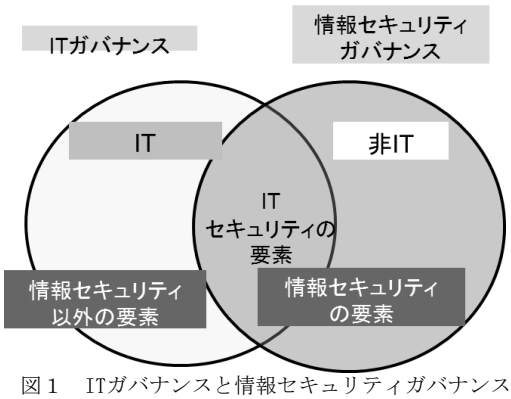

図１　ITガバナンスと情報セキュリティガバナンス

出典：文献[4]

3.1 ITガバナンス

図1に示す様に,電子的な資産以外の紙媒体等を非ITと捉えた場合,昨今のネットワーク社会で起こる数々のサイバーセキュリティは,ITガバナンスの領域でもあるが,情報セキュリティ分野としては重要領域になり,相互に取り組む分野として外延化している.

3.2 情報セキュリティガバナンス

経済産業省が2009年に公表した「情報セキュリティガバナンス導入ガイダンス」を元に, ISO/IEC 27014が国際提案された.それを基に,現在,情報セキュリティガバナンスに関するJIS化が進んでいる.

我が国では,企業等の組織の重要な情報システムに投資し構築していくといった重要な仕事は,CIO等による情報化戦略のもとに業務改革を推進してきた領域であるが,昨今の様に,既製のクラウドサービスをうまく活用するという利用者優位の時代になってくると,ITの分野で情報セキュリティの知見も大いに必要になってくるだろう.

3.3 ITと情報セキュリティの異なるガバナンス

ITガバナンスと情報セキュリティのガバナンスのそれぞれの領域を概観してみる.ITガバナンスはCIOの仕事で,攻めの領域である.情報セキュリティガバナンスは,今後,存在意義が高まるだろうCISO(最高報セキュリティ責任者)の仕事だが守りの領域・・.と単純に割り切って役割を限定する事ができるのだろうか?

4. 日本CISO 協会とAward制度

経営層の役員の職務名（CXO: Chief X Officer）として確実にCIOは一般の社会人にも知られ定着してきた.

しかしながら,欧米の外資企業や,IT系の国内企業を除いては,CISOという職位自体は,ほぼ知られていない.そんな厳しい状況の中,日本CISO協会は少数の発起人によって産声を上げた.

4.1 日本CISO協会とは

2014年2月に前身の活動を引き継ぎ,(一般社団法人)日本CISO協会は「日本のCISOが一同に集い,IT環境におけるセキュリティ情報の共有を行う場」をめざし発足した.また,企業等の情報セキュリティ担当の責任者や委員会等の個人の方々に規模の大小を問わず正会員として登録頂き,現在約45社前後で構成される.

4.2 CISO Award制度の発足

小規模組織のメリットを活かし,日本CISO協会では,優れたCISOを称える制度を,優れたCFOやCIOのそれに対する制度等と同様にCISO Award制度として起案し新制度の発足に至った.

5. CISO の評価方法の検討

5.1 情報セキュリティベンチマークの活用

筆者は,とりあえず王道となる情報セキュリティに係る評価の手法等を調査し,前述した経済産業省の一連の情報セキュリティガバナンスに関するコンセプト等を確認した.

情報セキュリティベンチマークについては,文献[3][6]の情報等を参照した.このベンチマークの主要な評価項目はISO 27001:2006をベースにしている.

5.2 客観的評価の必要性

本ベンチマーク自体は,組織がISMS認証迄は取得しないものの,自社の情報セキュリティに関する態勢を客観的にセルフ評価でき,特に年次で連続的な評価ができる事が特徴といえる.また組織の規模に依らず,業態等を加味して要求される情報セキュリティレベルによって,3グループ毎で相対的なスコアが提示される.

5.3 CISO Award応募方法（ツール作り）

本ベンチマーク自体は27の設問からなるが,そのうち,組織的な取り組み状況を確認する以下に関する8項目のみ,CISO Awardのエントリーの際に回答頂く事とした.

管理規程
リスクアセスメント
推進体制
資産分類
情報の工程毎安全対策
業務委託契約
従業者との契約
従業者への教育

回答としては,経営者の指示と承認のもとに方針やルールを定め,全社的に周知・実施している等の場合は４,それに加え他社の模範となるべきレベルは5となる.

また上記の回答のエビデンスとして規程類の提出と,応募者のスキル概要等の提示を,応募ルールに加えた.

6. CISO 10 Award 2014の結果

6.1 審査において確認できたこと

応募においては,協会や制度の知名度もない中で,多数には至らなかったものの,辛うじて推薦等も交えて,受賞企業を選出する事ができた.

また,委嘱した審査員は,国会議員,コンサルタント会社社長,総務省（元NISC）参事官,大学教授,およびIT系メディア企業編集長の構成とした.

2014年10月末の審査において,「より経営層に直結すべき存在」という原点を再認識した上で,あらためて,この前提により,本来のCISO of the Yearに該当する受賞企業としては一社のみを選出した.

6.2 受賞企業の特長

受賞企業（受賞者）の東京海上日動システムズ株式会社（宇野社長）が選出された最大の理由は,以下の革新力により,CEOという経営層の立場で自ら推進してきた事の圧倒的な強みにあった.

「15規程を3規程,318のルールを78ルールへとスリム化した革新力」

また,後付けではあるが,以下の様な宇野社長のコメントも協会の関連者に共有した.

「IT進展のメリットはビジネスプロセスの変革でデメリットは情報セキュリティの不安であり表裏一体です.顧客接点を含めたビジネスプロセスの変革を推進するCEOが,情報セキュリティを別のこととして誰かに任せることはできないと考え,2012年にCEOとCISOを兼ねることを決断しました.」（*出展：日経新聞電子版,2014年12月*）

7. CISO 10 Award 2015にむけたブラッシュアップ

7.1 評価内容の再考

初年度の「CISO 10 Award 2014」は,トライアル的なアプローチではあったが,結果を残すことにつながった.

改めて,このAward制度を振り返り,今年度のブラッシュアップを行う事を検討している.

■<u>他社の模範となるべきポイントの強調（案）</u>

8つの質問への回答は,応募企業において4以上であってほしい.卓越する部分について,その具体的なポイントを提示して頂く事で質的な評価を行う.

7.2 取り組みの改善

初年度は,まずは「制度の普及」を重視した.また,受賞企業にとっては,目立ったインセンティブはないものの,協会が当初想定した以上に,プラスの価値を感じて頂いたと思料する.

協会としては,ある期間集中して制度をアピールするのではなく,日頃の各種の地道な情報共有,交流会,及び啓蒙活動等を通して,普通の活動イベントとして定着できる事をねらう.

8. CISOに係るトピックや動向

(1) OWASPジャパンの「CISO Survey」

グローバルな任意団体で,Webサプリケーションのセキュリティに関する知見を共有するOWASP（Open

Web Application Security Project)の日本チャーターでは,ここ数年「CISO Survey」を実施しており,昨年度は日本からも多数の調査協力がされた.

CISOの役割に関する質問に対しては,グローバルでは,アプリケーションセキュリティに関する方針,基準及びガイドラインの策定や,リスク評価に対するポイントが高いが,日本からの回答は,より実務的なネットワークセキュリティ（防御）等を相対的に重視する傾向が見られた.

(2) IBMの調査等

2014年版のIBMグローバルでのCISOアセスメントでは,138名のセキュリティ責任者へのインタビューがなされ,CIOやVice Presidentの兼務等もあるものの,約63%の組織で,CISOという職位が任命されているという報告がされている.[*出典:文献[1]*]

また,昨今の共通的な課題として,経営におけるセキュリティの位置づけが,よりビジネスの側面で総合的に重要性を持つようになったという認識傾向が見られる.

また,外部からの脅威への懸念は増しているが,それと格闘する為には,CISOは内外へ影響を与えるべきというレポートがされている.

9. CISO とCIOの関係性（考察）

(1) CISOが持つべきコンピテンシー

東京海上日動システムズ株式会社（宇野社長）のケースや,グローバルな組織におけるCISOに対する認識は,ある意味でCIOに近づいている事を示している.

(2) CIOとの関連において

筆者の2013年の発表では,CIOのロールモデル（To-Be）を以下の様に整理した.

CIOの主たる役割は,ビジネスイノベーション
- CIO(担当)の専任化は必須
- 主要スキルや資質は,ビジネス知識と幅広い経験,加えてリーダーシップ
- 全体最適を見据えたIT経営
- CEOに近づく

CIOとCISOの同時化は考えにくく,必ずしもCISOはCIOの指揮命令下にあるとも考えにくい.

それぞれのITガバナンスと情報セキュリティガバナンスのコンピテンシーの領域から,互いのエッセンスを取り込んで近づく必要があると考える.

10. 日本CISO 協会としての貢献

(1) ベストCISOのアイコン作り

CISO 10 Award 2014の成果となった,受賞者のベストプラクティス(アイコン)を,具体的に増やして行く事で,間接的にCISOの地位向上に貢献できれば幸いである.

(2)CXOとしての多面的な評価

CISOに限らず,経営層における,各種のCXOにおいても,関連各所でモデルやスキルセット等を整理していく事を検討されたい.

(3) 今こそリスクマネジメントに対する感性を高めるべき.

日頃,情報セキュリティに関連するコンサル業務等をお手伝いする中で,ビジネスリスクはおろか,組織におけるITリスクやオペレーションリスクに関する情報共有やポリシー策定に対し優先されず,リスクマネジメントや可視化しにくいBCP等の領域は非常に関心の薄い位置づけにされている.

一朝一夕には改善を促しづらいが,今こそ優れたCISOやCIOは,リスク管理に舵をとり,ブラッシュアップするべきである.

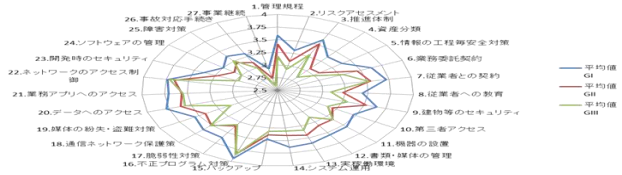

図2 リスクマネジメントのコンピテンシー
出典：情報セキュリティ対策ベンチマーク ver4.3の診断の統計情報を基に筆者が加工（IPAサイト）

11. 文献

[1] IBM[2014]『2014最高情報セキュリティー責任者（CISO）アセスメントからの洞察』

[2] 伊藤由紀美[2013]『21世紀のCIOの実像～ロールモデルの変遷と社会的変化～』,国際CIO学会ジャーナル第8号

[3] 情報処理推進機構[2012]『情報セキュリティ対策ベンチマーク(企業・組織のためのセキュリティ対策自己診断ツールVer.4.x)』,マネジメントのしおりシリーズ(4), 情報処理推進機構セキュリティセンター

[4] 小池 聖一・パウロ他[2011]『経営者のためのITガバナンスの実務』,中央経済社

[5] 礒部大[2010]『IT経営におけるCIOの役割』,武蔵大学論集

[6] 情報処理推進機構[2008]『情報セキュリティ対策ベンチマーク活用集』