情報セキュリティガバナンスの確立

組織の経営陣が取り組むべき行動指針の一つ

Winner's & Company
ウィナーズ・アンド・カンパニー株式会社
経営ソリューション部門
2015.02.04

情報セキュリティガバナンスの確立（背景）

情報化社会の発展に伴い、情報資産の管理が重要な経営課題になっています。弊社では、情報セキュリティに関する国家政策や社会的要請などを踏まえて、お客様のおかれている状況に適した情報の利活用と的確なリスク対策のバランスを図りつつ、情報セキュリティガバナンスの確立をご支援いたします。

社会的要請　期待

2010年11月、企業で相次ぐIT関連の事故や不祥事による影響は個別企業の問題に留まらず、社会・経済全体に波及してしまいます。企業は企業市民の一員としての責務を果たす意味からも、情報セキュリティガバナンス確立の実装への取り組みが求められています。

参考：国際標準化機構（ISO） ISO26000 ⇒ http://www.iso.org/iso/home/standards/iso26000.htm

経済産業省　リスク

2005年3月、経済産業省が公表した『企業における情報セキュリティガバナンスのあり方に関する研究会』報告書にて、企業の経営陣が取り組むべき行動指針の一つとして「社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義しました。

参考：商務情報政策局 http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

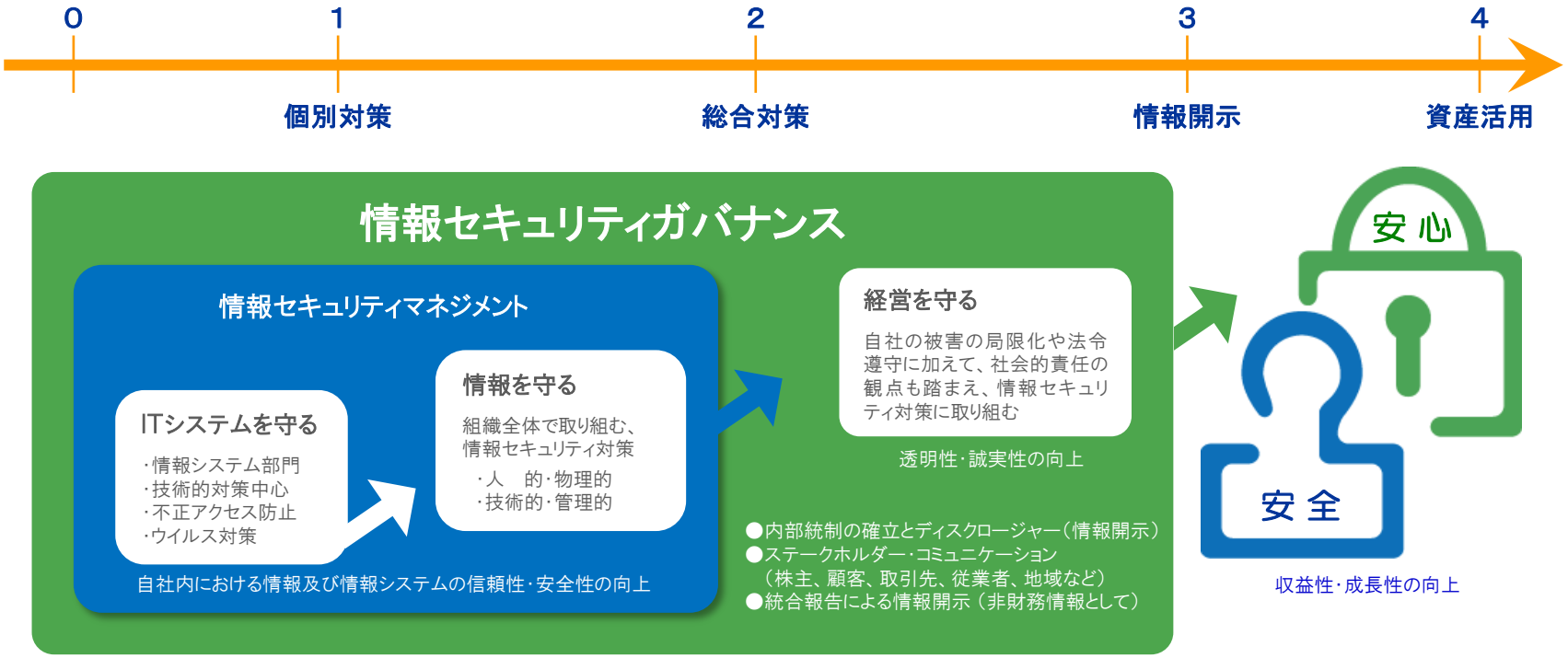
内閣官房（NISC）　機会

2013年6月、情報セキュリティ政策会議（内閣官房 情報セキュリティセンター：NISC）は「安全なサイバー空間」を実現するための新たな中期戦略として『サイバーセキュリティ戦略』を策定。世界最高峰のIT国家を目指して、安全・安心を強化する情報セキュリティの確保に力を入れています。

参考：内閣官房情報セキュリティセンター http://www.nisc.go.jp/index.html

情報セキュリティガバナンスの確立（イメージ）

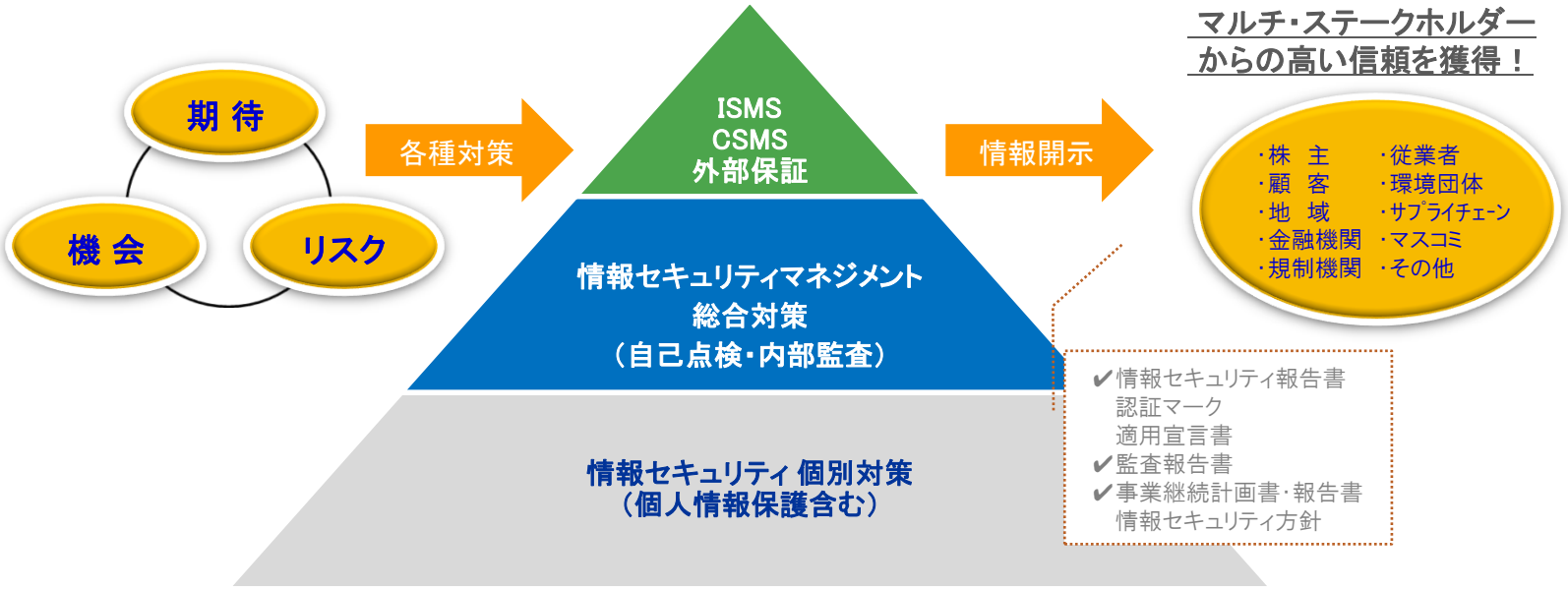
情報セキュリティガバナンスの確立には、個別対応～総合対応～情報開示の3ステップがあります。企業価値を評価する指標とされる情報セキュリティ関連の取り組みには、ステークホルダーの期待に応えつつ、リスクを軽減し、機会の最大化を実現できる施策が必要です。



独立行政法人情報処理推進機構（IPA）が公表した「2013年度 情報セキュリティ事象被害状況調査」において、情報セキュリティガバナンス、マネジメント関連対策の実施が前年比2～6%増加した旨の調査報告がありました。IPA調査: http://www.ipa.go.jp/security/fy25/reports/isec-survey/

情報セキュリティガバナンスの確立（捉え方）

取り組みの信頼性を高めるために、独立した外部保証をお客様、企業・取引先が求める場合がありますが、ステークホルダーとの良好な関係を前提に、「情報セキュリティ報告書」等を情報開示（情報共有）し、ダイヤローグ（対話）を通じて説明責任を果たすことでも、情報セキュリティガバナンスは確立できます。



CSMS（Cyber Security Management System）とは、産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステム

情報セキュリティガバナンスの確立（支援サービス）

信頼性・安全性の向上　期 待

A-1 セキュリティポリシー策定支援

網羅的・体系的対策、継続性がポイントです。中でも情報セキュリティポリシーの策定は、企業全体としての情報セキュリティ対策の要であり、可能な限り迅速な策定が求められます。

A-2 情報セキュリティ簡易診断・情報セキュリティ教育

情報セキュリティ対策は、組織によって何をどこまで実施するかの判断基準や意思決定プロセスは異なります。IPAセキュリティベンチマークやセキュリティ診断ツールの結果から解決策を見出します。

透明性・誠実性の向上　リスク

B-1 情報セキュリティ報告書作成支援

企業の情報セキュリティの取り組みの中でも、社会的関心の高いものについて情報開示することにより、顧客や投資先などのステークスホルダーから適正な評価を受けることが可能です。

B-2 情報セキュリティ監査

優れたセキュリティシステムを導入しても、ルール通りに運用されていなければ効果は期待できません。情報セキュリティの管理状況を検証し適切に運用するためには、情報セキュリティ監査が有効です。

収益性・成長性の向上　機 会

C-1 ISMS 認証取得支援（規格改訂対応含む）

情報化の進展、外部環境の変化、影響範囲の拡大、不正の増加など、情報セキュリティの重要性は日々高まっています。社員の意識を改革し、情報セキュリティを強化するためにはISMSが有効です。

C-2 事業継続管理（BCM）体制整備支援

コンプライアンス・CSR等の社会的要請、内部統制・ステークスホルダーの信頼性確保など、事業継続管理（BCM）や事業継続計画（BCP）は、企業間連携の複雑化などから早期導入が必要です。

C-3 プライバシーマーク導入支援

個人情報保護法の制定後も多発する個人情報流出事件など、世間の関心は高まる一方です。電子データ化された個人情報は流出の危険性が高く、個人情報は流れ出すとコントロールが効きません。

C-4 各種コンサルティング

情報セキュリティガバナンス等に関するアドバイス、運用ツール開発並びに、リスクマネジメント関連のコンサルティングを行います。
ERM、COBIT、ITIL、GTO、各種クラウドガイドラインなどを利活用します。

情報セキュリティガバナンス導入ガイダンス（経済産業省H21.6抜粋）

情報セキュリティ対策は、昨今、多くの事故が報道され、その対応が急務とされているにも関わらず、今なお多くの企業において「（企業の利益に直結しない）コスト」の位置付けであり、対策を実施することの重要性が十分に理解されていない。しかし、企業内・企業間における情報資産の効率的・効果的利活用が企業活動の成否を左右する現在。経営者は、情報資産の管理が経営戦略そのものであり、それを支えるリスク管理の一環としての情報セキュリティ対策こそバリューチェーン・サプライチェーンの高付加価値化を支える重要な要素であること、グループ統制の観点に立ち、正面から対峙しなければならない経営課題であることを改めて認識する必要がある。加えて、経営者は、企業が保有する情報の中に、法令や契約で利用が制限されている情報が含まれ、取扱にリスクが伴うケースもあること、また、顧客等が企業に対して適法性のみならず適正性を期待していることにも配慮する必要がある。

例えば、実際に情報流出やシステムダウン等の事故が発生した場合、企業が適法な範囲で事故に対処したとしても、それだけでは、顧客や取引先、従業員等を含む利害関係者から適切な評価を受けられず、一層の透明性や事業継続性の確保を求められる可能性がある。そのような状況に備え、情報セキュリティに取り組む姿勢や事故対応等の情報を適切に開示し、説明責任を遂行している企業事例も見ることができる。

こうした現状を鑑み、経営陣においては、自らの経営課題の一つとして、情報資産に係る機密性、完全性、可用性の観点を取り入れて、リスク管理を捉え直すことが重要である。すなわち、様々なリスクのうち、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み（経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組み）を構築・運用する、すなわち情報セキュリティガバナンスの確立に取り組むべきである。

経済産業省では、企業における情報セキュリティ対策を、従来の対症療法的なアプローチから、企業価値を高めるための投資対象として位置付けるアプローチの重要性・優位性を示すため、平成16年度に「企業における情報セキュリティガバナンスのあり方に関する研究会」を開催して情報セキュリティガバナンスの考え方を示した。続けて、平成17・18年度と、情報セキュリティガバナンス確立実現の促進ツールとして、「情報セキュリティ対策ベンチマーク」、「情報セキュリティ報告書モデル」及び「事業継続計画策定ガイドライン」を開発・公開し、これらの活用事業を推進してきた。さらに平成19年度からは、リスク管理の必要性を軸に、情報セキュリティガバナンスの定義を明確化するとともに、情報セキュリティガバナンスの確立を妨げる問題点に焦点を当て、その解決策の指針となる成果を策定してきた。

本書は、経営陣と管理者層・従業員層の間でリスクや対策についての共通認識が乏しく、全体最適化された構築・運用がなされないという問題への対処指針として、経営陣が取り組むべき行動の指針を示す。…以下省略

註）2014年現在、情報セキュリティガバナンス協議会（ISGA）に調査・研究主体が移管され、経済産業省はオブザーバーとして協力しています。

お問い合わせ

ウィナーズ・アンド・カンパニー株式会社
経営ソリューション部門　担当：森成、土屋、小泉
〒150-0013　東京都渋谷区恵比寿1-15-4
電話 03-5475-6568　FAX 03-5475-6569
E-mail　info@winners-co.jp
URL http://www.winners-co.jp

【情報セキュリティ普及啓発】
内閣官房情報セキュリティセンター(NISC)
http://www.nisc.go.jp/

【提携・会員】
株式会社日本CSR認証登録機構(JCSR)
株式会社セントラル(CEC)
新経済連盟(JANE)
統制技術研究機構(GTO)
日本ファンドレイジング協会(JFRA)
日本経営倫理士協会(ACBEE)
環境プランニング学会(EPS)
日本経営倫理学会(JABES)
日本イノベーション融合学会(IFSJ)