

第2版

情報セキュリティガバナンス 取締役会と役員に対するガイダンス

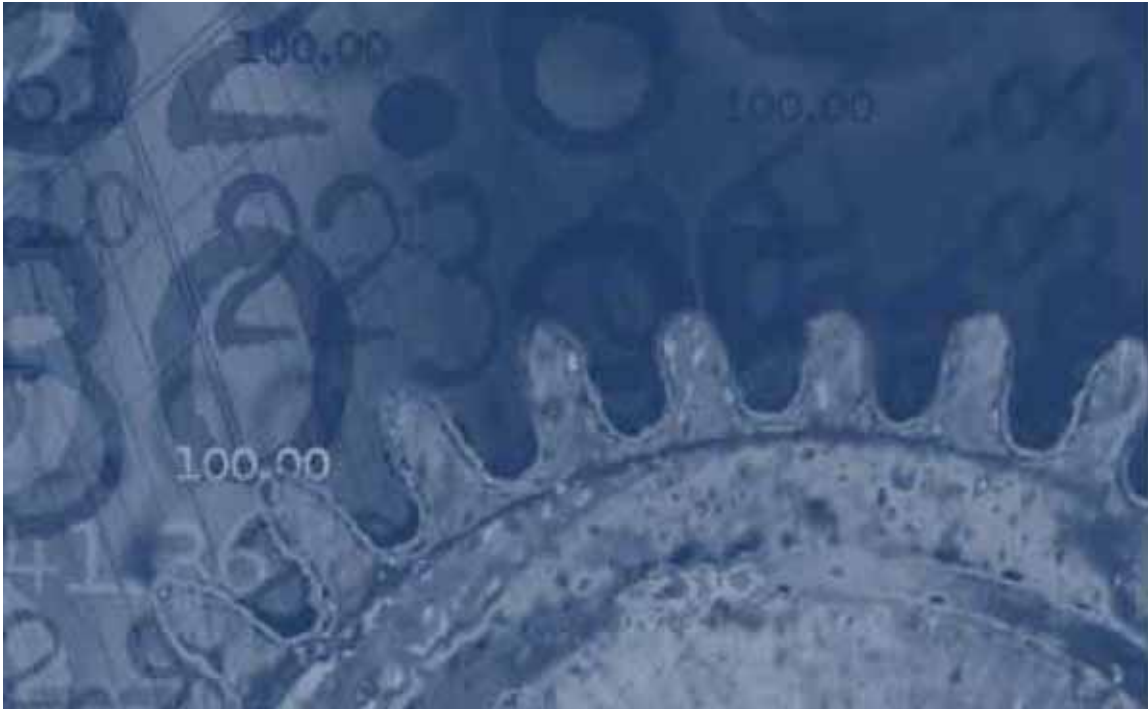


IT
GOVERNANCE
INSTITUTE®

ITGI Japan

空白ページ

情報セキュリティガバナンス 取締役会と役員に対するガイダンス



「ネット犯罪と最重要の情報資産に対する脅威が増大しつつある状況で、取締役会ならびに上位の役員は、ガバナンスのレベルでこれらの資源のセキュリティとインテグリティを保証する役割を全面的に負っている。」

- シャーリー・M・ハフステッドラー (SHIRLEY M. HUFSTEDLER) 取締役会
ハーマン・インターナショナル・インダストリーズ (HARMAN INTERNATIONAL INDUSTRIES)

安全なビジネスの運用を実現するためには、組織は有効なセキュリティガバナンス戦略を持つ必要がある。

- スニル・ミスラ (SUNIL MISRA) 最高セキュリティ責任者兼マネージングパートナー、ユニシス株式会社

「情報セキュリティおよびそのガバナンスが複雑で非常に重要なものであるため、情報セキュリティは、組織の最高のレベルまで高められることが求められる。最重要な資源として、情報は組織の存続と成功に最低限必要な他の資産同様に扱われる必要がある。」

- テリー・ハンコック (TERRY HANCOCK) CEO、イージー・アイ・グループ (EASY I GROUP)

IT ガバナンス協会®

IT ガバナンス協会 (ITGI™) (www.itgi.org) は、企業の情報技術に指針を与え、コントロールする際の国際的な考え方や標準を発展させる目的で、1998年に設立された。有効な IT ガバナンスによって、IT がビジネスの達成目標をサポートし、IT に対するビジネスの投資を最適化し、IT 関連のリスクおよび機会を管理することを保証する。IT ガバナンス協会はオリジナルの研究、電子版のリソース、さらにケーススタディを提供することで、経営者、さらに取締役会がその IT ガバナンスに関する責任を果たすことを支援する。

This Work is translated into Japanese from the English language version of *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition* by ITGI Japan with the permission of the IT Governance Institute. ITGI Japan assumes sole responsibility for the accuracy and faithfulness of the translation.

本稿は、『情報セキュリティガバナンス：取締役会と役員に対するガイダンス 第2版』を、ITGI より許可を受けて日本 IT ガバナンス協会 (ITGI JAPAN) が英語から日本語に翻訳をした。ITGI JAPAN が翻訳の正確性及び信頼性について責任を負っている。

免責事項

The IT Governance Institute (the “Owner”) has designed and created this publication, titled *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition* (the “Work”), primarily as an educational resource for boards of directors, executive management and IT security professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, boards of directors, executive management and IT security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

IT ガバナンス協会 (以下「所有者」という) は、『情報セキュリティガバナンス：取締役会と役員に対するガイダンス 第2版』(以下「本書」という) というタイトルのこの刊行物を、第一に取締役会および役員、さらには IT セキュリティの専門家の教育用の資料として立案し、作成した。所有者は、本書の何らかの部分を利用することで、結果が成功に終わることが保証されていることを主張するものではない。本書はあらゆる適切な情報、手続き、試験を含んでいると考えられてはならないし、また他の情報、手続き、試験を除外しているものとも考えられてはならない。何らかの特定の情報、手続き、試験の正確さを決定する際に、取締役会および役員、さらには IT セキュリティの専門家は、特定のシステムあるいは情報技術の環境が示す特定の状況に自らの判断を適用する必要がある。

情報開示

©2006 IT Governance Institute. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of ITGI.

Copyright © 2006 by the IT Governance Institute. 無断転載・複製・転載を禁ずる。

本書のいかなる部分も、使用・転写・複製・改変・配布・展示・情報検索システムへの保存、何らかの手段 (電子式、機械式、電気複写、録音その他) による何らかのフォームでの転送は、事前に IT ガバナンス協会 (ITGI) の書面による許可がない限り、これを行うことはできない。

IT ガバナンス協会 (ITGI)

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
電話番号: +1.847.590.7491
Fax: +1.847.253.1443
電子メール: info@itgi.org
ウェブサイト: www.itgi.org

ISBN 1-933284-29-3

Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition (情報セキュリティガバナンス：取締役会と役員に対するガイダンス 第2版)
アメリカ合衆国にて印刷

本冊子は IT Governance Institute が 2006 年に出版した “*Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*” の翻訳版である。

英文版における謝辞

编者より

IT ガバナンス協会 (ITGI) は次のメンバーに感謝を捧げたい。

ITGI 評議会

Everett C. Johnson, CPA, Deloitte & Touche LLP (前), 米国, アメリカ合衆国, 国際会長
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, シンガポール, 副会長

William C. Boni, CISM, Motorola, アメリカ合衆国, 副会長
Jean-Louis Leignel, MAGE Conseil, フランス, 副会長
Lucio Augusto Molina Focazzio, CISA, コロンビア, 副会長
Howard Nicholson, CISA, City of Salisbury, オーストラリア, 副会長
Bent Poulsen, CISA, CISM, VP Securities Services, デンマーク, 副会長
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, Focus Strategic Group, 香港, 副会長
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, アメリカ合衆国, 前国際会長
Robert S. Roussey, CPA, University of Southern California, アメリカ合衆国, 前国際会長
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi, アメリカ合衆国, 評議員
Ronald Saull, CSP, Great-West Life and IGM Financial, カナダ, 評議員
Erik Guldentops, CISA, CISM, ベルギー, 顧問, IT ガバナンス協会 (ITGI)

著者および重点グループ

W. Krag Brotby, CISM, Senior Security Consultant, アメリカ合衆国, 著者
Jennifer Bayuk, CISA, CISM, Bear Stearns & Co. Inc., アメリカ合衆国
Curtis Coleman, CISM, CISSP, MSIA, Seagate Technology LLC, アメリカ合衆国
Leonardo Garcia, CISA, CISM, CISSP, BS 7799LA, ISO 9000LA, Innovaciones Telemáticas, アメリカ合衆国
Ronda R. Henning, CISM, CISSP-ISSAP, CISSP-ISSMP, Harris Corporation, アメリカ合衆国
Stephen R. Katz, CISSP, Security Risk Solutions LLC, アメリカ合衆国
William Malik, CISA, Malik Consulting LLC, アメリカ合衆国
Yogita Parulekar, CISA, CISM, CA, Oracle Corporation, アメリカ合衆国
Eddie Schwartz, CISA, CISM, CISSP, MCSE, Securevision LLC, アメリカ合衆国
Darlene Tester, CISM, CISSP, JD, CHSS, Caveo Technology, アメリカ合衆国
Marc Vael, Ph.D., CISA, CISM, KPMG, ベルギー

ISACA の公認情報セキュリティマネージャ® (CISM®) 評議会

David Simpson, CISA, CISM, CISSP, Chair, CQR Consulting, オーストラリア
Kent Anderson, CISM, Network Risk Management LLC, アメリカ合衆国
Evelyn Anton, CISA, CISM, UTE, ウルグアイ
Claudio Cilli, CISA, CISM, CIA, CISSP, Tangerine Consulting, イタリア
Robert Coles, Ph.D., CISA, CISM, MBCS, 英国
Kyeong-Hee Oh, CISA, CISM, CISSP, Green Soft, 韓国
Hitoshi Ota, CISA, CISM, Mizuho Corporate Bank Ltd., 日本
Ashok Pawar, CISA, CISM, CAIIB, State Bank of India, インド
Gary Swindon, CISM, Orlando Regional Healthcare, アメリカ合衆国

ITGI 委員会

William C. Boni, CISM, 委員長, Motorola, アメリカ合衆国
Jean-Louis Leignel, 副委員長, MAGE Conseil, フランス
Erik Guldentops, CISA, CISM, ベルギー
Tony Hayes, Queensland Government, オーストラリア
Anil Jogani, CISA, FCA, Tally Solutions Ltd., 英国
John W. Lainhart IV, CISA, CISM, IBM Business Consulting Services, アメリカ合衆国
Ron Saull, CSP, Great-West Life and IGM Financial, カナダ
Michael Schirnbrand, CISA, CISM, CPA, KPMG LLP, オーストリア
Eddy Schuermans, CISA, PricewaterhouseCoopers LLP, ベルギー

主題に関する専門の校閲担当者

Julia Allen, Carnegie-Mellon, アメリカ合衆国
William Barrett, CISA, CPA, CRP, Ernst & Young LLP, アメリカ合衆国
Endre P. Bihari, CISM, CCSA, GAICD, MCSE, Performance Resources, オーストラリア
Chris Boswell, CISA, CISSP, CA, アメリカ合衆国
Claudio Cilli, CISA, CISM, CIA, CISSP, Tangerine Consulting, イタリア
Candi Carrera, Tellindus, ルクセンブルグ
Ulises Castillo, CISA, Scitum, SA de CV, メキシコ
Milthon J. Chavez, CISA, CISM, CIFI, MCH Consultoria Integral, ベネズエラ
Amitava Dutta, Ph.D., CISA, George Mason University, アメリカ合衆国
Chris Ekonomidis, CISA, CISSP, Ernst & Young LLP, アメリカ合衆国
Lawrence A. Gordon, Ph.D., University of Maryland, アメリカ合衆国
Erik Guldentops, CISA, CISM, ベルギー
Gary Hardy, ITWinners, 南アフリカ
Avinash W. Kadam, CISA, CISM, CISSP, CBCP, MIEL e-Security Pvt. Ltd., インド
John W. Lainhart IV, CISA, CISM, IBM Business Consulting Services, アメリカ合衆国
Alexandra Lajoux, National Association of Corporate Directors, アメリカ合衆国

Cory Notrica, CISA, CISM, CISSP, Ernst & Young LLP, アメリカ合衆国
Vernon R. Poole, CISM, IPFA, Sapphire Technologies, 英国
N. Ramu, CISA, FCA, Lovelock & Lewes, インド
Robert S. Roussey, CPA, University of Southern California, アメリカ合衆国
Howard A. Schmidt, CISM, CISSP, Former Chief Security Executive, eBay and Microsoft, アメリカ合衆国
Gad J. Selig, Ph.D., PMP, University of Bridgeport and GPS Group Inc., アメリカ合衆国
Dirk Steuperaert, CISA, PricewaterhouseCoopers, ベルギー
Johann Tello-Meryk, CISA, CISM, Primer Banco del Istmo, パナマ
Ghassan Youssef, MSc., CISM, Bank Audi, Audi Saradar Group, レバノン

次の ITGI のアフィリエイトとスポンサーにも感謝を捧げる。

ISACA chapters
Commonwealth Association of Corporate Governance
Bindview Corporation
CA

英文版における謝辞（続き）

ITGI は、次の機関に対して感謝を捧げる。

ユニシス社が、その寛大なるサポートとスポンサーとしての協力により、『情報セキュリティガバナンス：取締役会と役員に対するガイダンス 第2版』の開発に大きく貢献したことに對して謝意を表する。

ITGI は、以下の組織が本プロジェクトに対して行った支援に対して感謝を捧げる。



情報セキュリティガバナンス 取締役会と役員に対するガイダンス 第2版の日本語版によせて

経営者層の方々のために本書は書かれたものです。

本書のキーメッセージは、なぜ、セキュリティのガバナンスが必要なのかです。

従来のセキュリティの対策ではなにが不十分なのか。

環境の変化として10年以内に情報のスピードは30倍以上になるだろう。

経営資源の中で人、金よりも知識、情報がより重要なものになり、経営戦略と整合性のとれたセキュリティ方針が必須である。

すべての業務担当役員はその責務としてセキュリティ方針をたてモニタリングする必要がある。

なにをしなければいけないのか、本書を一読ください。

日本ITガバナンス協会 会長 松尾 明

ITGI Japanの翻訳活動の成果として、COBIT関連の書物に加え、“情報セキュリティガバナンス”の日本語訳を公開することができました。翻訳レビューを担当したISACA東京支部を代表して、関係者の皆様に感謝の意を表します。

ISACAの3つの柱である、ITガバナンス、アシュアランス、セキュリティの中で、COBITシリーズではITガバナンスとアシュアランスに議論の中心が置かれていますが、セキュリティの議論を抜きにしては、ITガバナンスは成り立ちません。そういった意味で、ITガバナンス協会から情報セキュリティガバナンスのガイダンスを発信できることに大きな意味があると考えます。

この書物は、COBITやVAL-ITと同様に、CIOをはじめとする経営トップの方々にとって有益であると同時に、情報システムの企画・開発・運用に携わる方、そしてITを利用するすべての方にも有益なものと考えます。多くの皆様に活用していただくことを期待します。

ISACA 東京支部 2006-2007 会長

高須 昌也

翻訳協力

ISACA 東京支部

大茂 幸子 (アイ・ピー・エム ビジネスコンサルティング サービス株式会社、CISA)

鈴木 貴志 (グローバルセキュリティエキスパート株式会社、CISA)

山内 哲也 (あらた監査法人、CISA)

日本 IT ガバナンス協会

中村 努 (日本 IT ガバナンス協会理事、ISACA 東京支部 2006-2007 常務理事)

日本語版の発行に際し、
株式会社野村総合研究所が、スポンサーとしての協力により、
『情報セキュリティガバナンス：取締役会と役員に対するガイダンス 第2版』の
翻訳に大きく貢献したことに対して謝意を表す。



空白ページ

目次

イントロダクション	12
1. 情報セキュリティガバナンスとは - 概観.....	15
所望の結果.....	15
知識と情報資産の保護.....	16
情報セキュリティガバナンスの利点	16
プロセスの統合	17
2. 情報セキュリティと情報セキュリティガバナンスが重要とされる理由 ...	19
情報セキュリティガバナンスの定義	21
3. 情報セキュリティガバナンスに関わるべき人は?	25
取締役会/役員会	25
役員	25
運営委員会.....	26
最高情報セキュリティ責任者 (CISO)	26
4. 取締役会/評議員会および上級役員は何をするべきか.....	26
指示と結果の関係を示すマトリックス.....	28
5. どのような示唆に富む問いが行われるべきか	30
情報セキュリティ関連の問題を見つけ出すための問い.....	30
経営者が情報セキュリティ関連の問題に対処する方法を見つけ出すための問 い.....	30
情報セキュリティガバナンスのプラクティスを自己評価するための問い...	31
6. 情報セキュリティガバナンスが提供するべきこと	32
戦略との整合	32
リスクの管理.....	32
資源の管理.....	32
成果の測定.....	33
価値の提供.....	33
7. 情報セキュリティガバナンスはどのように変化しているか	35
8. 情報セキュリティガバナンスの導入に成功するために可能なこと	37
取締役に対する問い	37
役員に対する問い.....	37
9. 組織が情報セキュリティガバナンスに関する比較を行う方法	39
成熟度レベルの説明	39
付録 - 規制団体ならびに標準化団体の情報セキュリティガバナンスに関する ガイダンス	42
参考文献	46

イントロダクション

組織は今日、ガバナンスの世界的な変革に直面しており、それは情報マネジメントのプラクティスに直接の影響を及ぼしている。保護されるべき情報と、実現したサービスが提供する情報の、これらの情報の全体の価値に重点をおく必要性が増大している。過去 10 年間に幾つかの著名な組織が破綻に至ったことで、組織ガバナンス、セキュリティ、コントロールおよび透明性の向上を目的とした一連の複雑な新しい法律および規制が、法や制度および規制の当局者によって作り上げられる結果となった。

ハッカー、ワーム、ウィルス、テロリストから受ける情報システム破壊の重大な脅威が組み合わさった結果として、情報の保持とプライバシーに関する新旧の法律では、情報の管理にガバナンスの観点からアプローチする必要性が生じている。それは、組織の最も重大な資産である、情報および評判を保護することである。

情報とその処理システムが、実質的には全ての組織にとって重要である。信頼のできる情報にアクセスできることが、ビジネスの遂行には欠くことのできない構成要素となった。実際、ますます多くの企業にとって、**情報こそがビジネス**となっている。

情報に依存する度合いが増大していることは、10 年以上前にピーター・ドラッカー（Peter Drucker）が次のように述べたときから明白であった。

「技術が普及し情報が商品化して、情報の役割は、従来重要であった土地、労働、資産と、重要性の点では同様な資源へと変化するに至った」¹

その間に、情報の価値上昇とこれに依存する度合いが飛躍的に増大した。このように速まったペースが、予見可能な将来の時点にかけて衰えることなく続くことを示唆する材料には、枚挙にいとまがない。ガートナー社は最近、今後 10 年以内に、組織は情報を今日よりも概して 30 倍のスピードで処理することになるだろうと見積もっている²。大部分の情報技術の運用で見られる混乱、目だつた脆弱性、さらに絶えることのない非常事態の活動を考えると、これは楽観できる状態ではない。

組織は情報関連の犯罪および破壊行為が、増大する世界の犯罪の要素の選択肢になろうとしている状況を、依然として目の当たりにしている。既存の制度は、無数の対立する法制度や不十分なリソースが足かせとなって、これらのアクティビティの総数や影響を軽減することに成功していなかった。それゆえ、最重要の情報資源を保護するという課題の大部分は、役員と取締役会の肩の上にまともにはかかっている。

最近まで、セキュリティの重点は圧倒的多数の情報を処理し保存する IT システムを保護することに置かれ、情報そのものには置かれていなかった。しかし、このアプローチは範囲が狭すぎて、現在必要とされる統合のレベル、プロセスの保証、

¹ Drucker, Peter; 'Management Challenges for the 21st Century', Harpers Business, 1993

² Hallawell, Arabella; *Gartner Global Security and Privacy Best Practices*, Gartner Analyst Reports, USA, 2004, www.csoonline.com/analyst/report2332.html

全体の保護を実現できない。

今日の複雑で、相互に関連した世界で、有効性とサステナビリティを達成するために、情報セキュリティは、組織の最高レベルで対処される必要があり、IT部門に押し込まれる専門的な技術問題と見なされるべきではない。

情報セキュリティでは、情報を十分に受けることによってアプローチの視野を広げて、組織の情報とこれに基づいた知識を、それがどのように処理され、加工され、転送され、また保管されるかに関わらず、適切に保護する必要がある。このアプローチでは、全ての情報資源に関わるリスク、利益、プロセスから構成される世界に対処している。情報のセキュリティは、他の組織の最重要の資源同様に、企業全体のレベルで対処される必要がある。

情報セキュリティは、技術に関わる問題であるばかりでなく、十分なリスク管理、報告、説明責任に関わるビジネスとガバナンスの課題でもある。セキュリティが有効であるためには、役員が、発生しつつある脅威とそれに対する組織の対応を評価する過程に積極的に関与することが必要である³。

組織が世界経済で競争力を保ち続けようと努力している際は、多くの場合、自動化のためにより多くの情報システムの配置が必要であるにもかかわらず、その自動化を通じてコストの削減をしなければならないという絶えず存在するプレッシャーに対処している。役員がこれらのシステムに対する依存を強めていく一方、このシステムは、企業の存続を脅かす可能性のある、徐々に範囲を拡大するリスクに対して脆弱なものになってきた。この事情の組み合わせによって、役員は、情報セキュリティという問題に有効に対処する方法に関して、困難な決定に直面することを強いられている。これに、多数の新しい、そして既存の法律や規制が準拠性ならびにさらに高いレベルの説明責任を求めてきている事情が加わっている。

データガバナンス委員会⁴では、取締役会の責任をレビューおよび承認の側面に重点を置いており、最近、取締役会が情報セキュリティに関する戦略的なオーバーサイトを行うべきことを勧告しているが、それには次の点が含まれている。

1. 情報および情報セキュリティの組織にとっての重要性を理解する
2. 情報セキュリティへの投資について、組織の戦略とリスクプロファイルとの整合をレビューする
3. 包括的な情報セキュリティプログラムの開発ならびに導入を承認する
4. プログラムの妥当性ならびに有効性に関して、役員に定期的な報告を求める

これに関して、管理に当たる取締役会と役員は、次の点を検討しなければならない。

- 情報資源が最適化されることを保証する目的で、現在ならびに将来行われる情報資源に対する投資の規模と収益
- 技術が組織とビジネスのプラクティスを劇的に変化させ、これによってコスト

³ Corporate Governance Task Force, 'Information Security Governance: Call to Action', USA, 2004

⁴ IBM, *Data Governance Council, Oversight of Information Security*, USA, 2005

を削減しながら新しい機会と価値を作り出す可能性

統治を行う取締役会と役員はさらに、次の点が上記に関連して悪化するかどうかということを検討する必要がある。

- 情報および情報の提供を行うシステムならびに通信に対する依存度の増大
- 企業が直接管理できない組織に対する依存
- 情報をパートナー、サプライヤ、顧客と共有する必要性の増大
- 情報セキュリティの失敗から発生する評判および企業価値に対する影響
- 情報の重要性に関する、企業のトップレベルにおける方向づけの失敗

役員はこれらの問題について検討し、これに対処する責任がある。一方で、取締役会が、情報セキュリティを企業ガバナンスの取り組みの中心的な部分とすることに対する期待がますます高まっている。この取り組みは、IT ガバナンスの目標と整合し、さらに他の最重要の資源を管理するために実施するプロセスと統合する必要がある。

本書の目的は、取締役会と上級役員に対して、最重要のビジネスプロセスをサポートする最重要な情報資産を保護するための基盤、根拠、さらに承認を受けたアプローチを提供することにある。

このガイドは、世界で主導的な役割を果たす IT ガバナンスの問題と原則の研究を専門とした団体が作成したもので、上にあげたような懸念に対処するために書かれたものである。このガイドは、次にあげるような基本的な問題をカバーしている。

- 情報セキュリティガバナンスとは何か
- 情報セキュリティガバナンスの重要性
- 情報セキュリティガバナンスの責任を負う者

このガイドはさらに、次の点に関する現実的なアドバイスを与えている。

- 情報セキュリティガバナンスが提供するべきこと
- 情報セキュリティに関して問いかけるべき質問
- 情報セキュリティガバナンスが進化する過程
- 組織の情報セキュリティガバナンスに関する成熟度レベルを測定する方法

1. 情報セキュリティガバナンスとは - 概観

情報セキュリティガバナンスとは、取締役会と上級役員の任務である。情報セキュリティは、企業ガバナンスにとって不可欠で透明性を有する部分であり、ITガバナンスフレームワークと整合している必要がある。上級役員にはこれらの問題について検討し、情報セキュリティにより提起される懸念および機密性に対応する責任がある一方で、取締役会が、情報セキュリティを企業ガバナンスの取り組みの中心的な部分とすることに対する期待がますます高まっている。この取り組みは、ITガバナンスの目標と整合し、さらに、既に実施されている、他の最重要の資源を管理するために実施するプロセスと統合する必要がある。

有効な企業ガバナンスならびに情報セキュリティガバナンスを遂行するために、取締役会と上級役員は、企業の情報セキュリティプログラムに期待することに関して、明確な理解を持っている必要がある。取締役会と上級役員は、情報セキュリティプログラムの導入の方法、既存のセキュリティプログラムに関連した自分たちの状態の評価方法、および有効なセキュリティプログラムの戦略と目標の決定方法について知っている必要がある。

情報セキュリティガバナンスにはさまざまな側面がある一方、「情報セキュリティとは何か」という問題に重点を置くことを助ける問題がいくつかある。これらの問題は次のようなものである。

- 情報セキュリティガバナンスの望ましい結果
- 知識と情報資産の保護
- 情報セキュリティガバナンスの利点
- プロセスの統合

所望の結果

情報セキュリティガバナンスは、情報を保護するリーダーシップと、組織構造、さらにプロセスから構成されている。この組織構造ならびにプロセスが成功するために最も重要なのは、全ての当事者が、建設的な関係、共通の言語、問題に対処するための共同でのコミットメントに基づいて、効果的な交流を行わっていることである。情報セキュリティガバナンスの5つの基本的な成果には、次のものが含まれているはずである。

1. 戦略的整合：情報セキュリティとビジネスの戦略が戦略的に整合し、組織の目標をサポートしている
2. リスクの管理：リスクを管理・軽減し、さらに情報資源に生じる可能性のある影響を許容可能なレベルにまで減少するよう、適当に対策している
3. 資源の管理：情報セキュリティに対する知識とインフラストラクチャを効率的かつ有効に利用している
4. 成果の測定：情報セキュリティガバナンスの指標を測定し、モニタリングし、またこれについて報告し、組織の目標が達成されていることを保証している
5. 価値の実現：組織の目標をサポートする情報セキュリティ投資を最適化することで、価値が実現されている

ガバナンスとは、戦略的指針を与え、目標が達成されることを保証し、リスクが適正に管理され、企業の資源が妥当な形で利用されていることを確実にすることを目標とした、取締役会と役員が実行する任務ならびにプラクティスの総体である。

IT Governance Institute, 『取締役会のためのITガバナンスの手引き、第2版』, USA, 2003, www.itgi.org. 英国勅許管理会計士協会(CIMA)および国際会計士連盟(IFAC)も、2004年にこの定義を採用している。

全米取締役協会（NACD）は、米国の取締役会と取締役が加盟する主要な団体であるが、ここでも情報セキュリティの重要性は認識されている。全米取締役協会は、取締役会が最低限行うべき4つの主要なプラクティス、ならびに各項目についての主要な特定のプラクティスを勧めている。4つのプラクティスは、取締役会の運営方法の現実性に基づくもので、次のようなものである⁵。

- 情報セキュリティを取締役会の基本方針に盛り込む
- 情報セキュリティのリーダーを明確化し、このリーダーに常に説明責任を与え、またリーダーに対するサポートを保証する
- 組織の情報セキュリティポリシーの有効性を、検討と承認を通じて保証する
- 情報セキュリティを主要な委員会に委任し、またこの委員会に対する十分なサポートを保証する

知識と情報資産の保護

データは情報の原料である。データ自体は、これが情報の提供が可能になるように整理され、操作されない限り、利益をもたらさない。情報は、意味、関連性、目的を持つデータであると定義されてきた。これらの特性がなければ、情報を保護し、さらに、これを保持するために資源を増やす正当な理由は、ほとんどあり得ないことは明確である。情報は、知識の基本をなす。情報を集め、何か有益なことを実現するために使用できる状態にしたとき、それは知識となる。知識は情報から作り出される。一方、知識は捕捉され、運搬され、整理された情報として保管される。

情報とこれに基づいた知識が情報資産、すなわち、ビジネスの最重要な資産であり、これがない場合、組織が簡単に機能停止してしまうものであると認識される度合いは増加している。この情報と知識はビジネスを可能にするものであり、これを適切に保護するよう、組織に対して要求する。ただし、今日の複雑で、相互に関連した世界で、有効性とサステナビリティを達成するために、情報セキュリティは組織の最高レベルで対処される必要があり、IT部門に押し込められる専門的な技術問題と見なされるべきではない。

知識は急速に、生産性の唯一の要因となり、資本と労働をいずれも脇に追いやっている。

ドラッカー、前掲書

企業のセキュリティの目的で管理を行うことは、適切なセキュリティをビジネスの無視できない要件であると見なすことを意味する。組織の役員、すなわち取締役会、上級役員、全ての取締役等の人々が、企業の有効なセキュリティのためにビジネスの必要性を確立し強化することがなければ、組織の望むセキュリティの状態を明確化し、達成し、維持することはない。持続可能な能力を達成するために、組織は企業のセキュリティをガバナンスレベルにあるリーダーの任務にする必要があり、準拠性に沿って行動し準拠性を強制する権威や説明責任、資源がない他の組織の任務にしてはならない⁶。

情報セキュリティガバナンスの利点

情報セキュリティガバナンスは顕著な利点を生み出すが、これには次のようなものが含まれる。

- 良好なガバナンスを実行する組織が共有する価値の増加
- 情報セキュリティ関連のリスクを、定義され許容されるレベルにまで減少させ

⁵ National Association of Corporate Directors, 'Information Security Oversight: Essential Board Practices', USA, 2001

⁶ Allen, Julia; *Governing for Enterprise Security*, Carnegie Mellon University, USA, 2005

- ることで、ビジネスの運用において、予見性を増大させ不確かさを減少する
- 情報の不正確さや相当の注意義務が欠けていたことの結果として、民事あるいは法律上の責任を負う可能性の増大からの保護
 - 限られたセキュリティ資源の配賦を最適化する構造ならびにフレームワーク
 - 有効な情報セキュリティポリシーとそのポリシーへの準拠性の保証
 - 情報のセキュリティに関わる効率的で有効なリスクの管理、プロセスの改善、迅速なインシデントへの対応の基礎付けを確実にを行う
 - 最重要の決定が間違った情報に基づいていないという保証のレベル
 - 最重要なビジネスのアクティビティ、たとえば合併や買収、あるいはビジネスプロセスの復旧、規制による対応等の間に、情報を保護するための説明責任

これらの利点は、次のことによって目に見える価値を組織に追加する。

- 顧客関係において信頼性を増大する
- 企業の評判を保護する
- プライバシーの侵害の可能性を減少する
- 取引相手とのやり取りの際にさらなる信頼性を提供する
- 電子取引を処理する新しく改善された方法を実現する
- 予見されている結果をもたらすこと、すなわち、プロセスを妨害する可能性のあるリスク要因を軽減させることで、運用コストを減少させる

2003年には、マッキンゼー社（McKinsey）がインスティトゥーショナル・インベスター社（Institutional Investors Inc.）と共同で、主要な国際的投資家は、管理が行き届いていることで知られる企業の株式には、割増金を払う意志があると結論づけた⁷。割増金は、1996年の11%から16%の間の値から、2000年には18%から28%の間の値に変動した。コントロールおよび証明の有効性開示に対する要請は、財務報告規定と法律上の要件の出現と共に増加した。この調査は、十分に有効なセキュリティガバナンスには明確な意味があることを示唆している。

良好な情報セキュリティの利益は、リスクの減少のみならず、もし何かがあまくいかなない場合には、その影響の減少にもある。良好な情報セキュリティにより、ビジネスを行う相手である他者からの評判、信頼性、ならびに信頼が改善され、セキュリティのインシデントから回復する際に無駄な時間と努力を回避することで、効率を高めることにもなりうる⁸。

プロセスの統合

セキュリティが、関連性はあるが独立した機能に分割される傾向が強まってきているため、組織のセキュリティに関するマネジメント保証プロセスは、これらを統合することがますます重要になってきた。これは、セキュリティおよび運用の効率性全体の向上に役立つ。

これらのアクティビティは場合によって分断され、さまざまな報告構造を有したサイロに分割される。これらのアクティビティは、異なった用語を用いており、

アバディーンの調査中の組織) 全てのうち、28%がクラス最高のレベルでセキュリティプログラムを運用しているが、所見からクラス最高の[セキュリティ]ガバナンスプログラムを運用しているのは、10%に満たないことが明らかになった*。

* 'Best Practices in Security Governance', Aberdeen Group, USA, 2005

⁷ McKinsey and Institutional Investors Inc., 'McKinsey/KIOD Survey on Corporate Governance', January 2003,

www.mckinsey.com/client-service/organization-leadership/service/corpgovernance/pdf/cg_survey.pdf

⁸ IT Governance Institute, COBIT® Security Baseline, USA, 2004, www.itgi.org

一般的に、時として共通するところの少ない、そのプロセスと結果の異なった理解を反映する傾向がある。これにより、継ぎ目なくこれらのアクティビティを統合することが、不可能とは言わないまでも、困難なものになっている。結果には、重複するセキュリティのイニシアチブが含まれていて、資源が無駄遣いされたり、大きな隙間があって深刻なセキュリティの損害につながったりすることがある。これを示す例として、修理技術者を装った2人の人が、電子的にはセキュリティが確保されたデータベースサーバそのものを税関事務所から物理的に入手したケースがあげられる。他の例としては、技術的にはセキュリティが確保されたネットワークが、不正な注文を処理するのに使用されたケースがある。いずれの場合でも、マネジメントプロセスの統合の欠如により大きなすき間が生じ、結果として深刻な影響をもたらしている。

スタートからゴールまでマネジメントのプロセスとそのコントロールを評価することで、さまざまな機能の間にセキュリティの隙間が発生する傾向を軽減することができる。

2. 情報セキュリティと情報セキュリティガバナンスが重要とされる理由

情報セキュリティの主要な達成目標は、組織に対する不利な影響を縮小し、リスクを許容できるレベルにすることにある。情報セキュリティは、情報資産を損失のリスク、業務の断絶、悪用、許可なく開示されること、アクセス不可、損害から保護する。また情報セキュリティは、増大し続ける情報の不正確さや損失、その保護において相当の注意義務が欠けていたことの結果として、組織が直面する民事あるいは法律的な責任が発生する可能性に対して保護する。

情報セキュリティは、物理的なものも電子的なものも、人や技術に関するものか、取引相手、顧客、サードパーティに関するものかどうかに関わりなく、全ての情報プロセスをカバーする。情報セキュリティは、情報のライフサイクルおよび情報の組織内での使用を通じて、情報の保護、機密性、可用性、インテグリティに対処している。

フィッシングその他のサイバー攻撃を含め、情報犯罪が劇的に増大したことから、今日ではセキュリティの向上が要件ではないと主張する者はほとんどいない。新しいワームやマルウェアや、機密性のある顧客情報の損失、知的財産の盗難が報告される件数が増大したことによって、上級役員はこれらの問題に対処する以外に選択肢がほとんどなくなった。情報セキュリティは、健全なマネジメントと適用される技術の間のバランスを取ることを必要とする。ネットワークが広く使われるようになると、個人や組織は、電子ビジネスを促進する一方で、個人情報のプライバシーや、情報の機密性を保護する組織側の必要性に関わる他のリスクを懸念するようになる⁹。

情報を処理するシステムやプロセスは、企業全体で広く使用されるようになった。施設や設備、人など、他の資産を損失しても組織は生き残るかもしれないが、その最重要の情報（会計ならびに財務報告情報や、運用ならびにプロセスに関する知識および情報）あるいは顧客データを失っては、継続することのできる組織はほとんどない。この資源が示すリスク、利益、機会により、情報セキュリティガバナンスが、ガバナンス全体で最重要の側面になった。

情報セキュリティは、IT ガバナンスと整合し、戦略、概念、計画、導入、運用に統合された、企業ガバナンスにとって不可欠な構成要素であるべきである。最重要の情報の保護は、マネジメントの戦略の中で検討されるべき主要なリスクの一つとなる必要があり、成功に寄与する重大な要因と認識するべきである。

情報セキュリティは、情報のライフサイクルおよび情報の組織内での使用を通じて、情報その機密性、可用性、インテグリティを保護することを目的としている。

それゆえ、情報セキュリティガバナンスには上級役員のコミットメント、セキュリティを意識した文化、良好なセキュリティのプラクティス、さらに方針への準拠性が必要である。文化を変えるよりソリューションを買う方が容易であるが、最も安全なシステムであっても、教育を十分に受けず、訓練を受けず、また注意力がなく無関心な人員によって使用された場合には、十分なレベルでのセキュリティを達成することはできない。

情報セキュリティは、企業のビジネスプロセスや戦略と明確にリンクした包括的

⁹ 前掲書、IT Governance Institute, COBIT *Security Baseline*

なセキュリティ戦略を必要とする、トップダウンのプロセスである。セキュリティは、物理的であるものも技術的であるものも、端から端まで、全ての組織プロセスに対処することが必要である。

セキュリティの全ての関連の要素に組織のセキュリティ戦略が対処することを保証するために、さまざまなセキュリティ標準が作成され、ガイダンスを提供し、包括性を保証してきた。最も広く使用されているものには、COBIT (*Control Objectives for Information and related Technology*)、ISO 17799、さらに米国の FIPS 規格 200 や NIST 800-53 などの他の標準がある。

正式なセキュリティ戦略は、部分的には、組織の目標を反映し、戦略の各要素に対処する包括的なセキュリティポリシーを作成し配置することで導入される。有効なガバナンスを提供するためには、ポリシー別に一連の企業標準が作成され、役割ならびに責任が割り当てられた上で、許容されるプロセスと手続きの境界線を設定する必要がある。実行中のプロセスの一環として、全ての人員に対して教育、意識、訓練を行い、セキュリティが確保された信頼できる行動を保証する必要がある。

セキュリティポリシーをふくむ、包括的なセキュリティプログラムには、次のものが含まれる。

- セキュリティポリシーの作成/維持
- 役割、責任、権限、説明責任の割り振り
- 標準、指標、プラクティス、手続きから構成されるセキュリティおよびコントロールフレームワークの作成/維持
- 定期的なリスク評価およびビジネスインパクト分析
- 情報資産の所有者の分類と割り振り
- 人、プロセス、技術に対する十分で、有効かつテスト済みのコントロール
- セキュリティの全ての組織のプロセスへの統合
- セキュリティの要素をモニタリングするプロセス
- 情報セキュリティのインシデントの管理
- 情報のユーザならびにサプライヤに対する、有効な本人確認ならびにアクセスの管理プロセス
- セキュリティ成果の有効なモニタリングと指標
- 全てのユーザ、役員、取締役会の構成員の、情報セキュリティ要件に関する教育
- 年次的に情報セキュリティ評価を行い、成果レポートを取締役会に対して提出
- 情報セキュリティの欠陥に対処するための是正措置の計画
- セキュリティプロセスの運用の訓練
- 中断および災害が発生した場合の、業務継続のための計画の作成とテスト

いくつかのセキュリティプログラムの側面には、他の側面に比べて上級役員にとっての関係がある場合がある。たとえば、日本やフランス、カナダ、インド、アメリカ合衆国やオーストラリアのような国は、規制あるいは規定、または法律の観点から財務報告を行うためのコントロールの妥当性ならびにテストに重点を置いている。情報セキュリティは、コントロールの行き届いた財務報告にとっては最重要の要件である。ヨーロッパ連合 (EU) 内では、セキュリティと個人情報の機密性に関する限り、プライバシーの観点に重点を置くことがこれと同程度、あ

るいはこれ以上の意義を持っている。

組織には、パートナーシップや顧客との契約による取り決めから発生した、特別なセキュリティ要件あるいは目的も発生する可能性がある。それゆえ、検討したことが企業のポリシーならびに手続きと緊密に整合し、さらに十分な資源が配賦され、これによって企業全体の戦略をサポートすることを役員が保証することが、最も重要である。

包括的セキュリティプログラムでは、層を成した一連の技術的、非技術的な防護策およびコントロール（すなわち、安全および環境セキュリティ対策、境界セキュリティおよび物理的セキュリティ、バックグラウンドチェック、アクセスコントロールセキュリティ対策、ユーザ ID、パスワード、IT 技術指標、さらには手動および自動の手続き）を通じて、情報資産を保護する。これらの防護策およびコントロールは、必要なものであり、脅威や脆弱性の問題に対処して、結果として発生する可能性のある影響を一定の、許容できるレベルにまで抑えるものである必要がある。必要性のある主要なコントロールとその目的は、COBIT の中で包括的にカバーされている。

情報セキュリティガバナンスの定義

情報セキュリティガバナンスは、企業ガバナンスの部分集合であり、戦略的指針を提供し、目標が達成されることを保証し、適切にリスクを管理し、組織の資源を妥当な形で利用し、企業のセキュリティプログラムが成功したか失敗したかをモニタリングするものである。

十分な資源が配賦され、これによって企業全体の情報セキュリティ戦略をサポートすることを役員が保証することが、最も重要である。

情報セキュリティは、情報のあらゆる側面（口頭、文書、印刷、電子的媒体その他の媒体）および情報の処理（作成されたもの、閲覧されたもの、転送されたもの、保存されたもの、破壊されたもの）を取り扱うものである。情報セキュリティは、ネットワークインフラストラクチャテクノロジーの領域内の情報セキュリティである IT セキュリティとは対照をなす。

通常、機密情報がエレベータでの会話の中で漏洩し、通常のメールで送付された場合、これは IT セキュリティの範囲外である。

しかし、情報セキュリティの観点から見ると、セキュリティが破られたという事実と比べて、損害の性格や種類はさほど重要ではない。セキュリティが破られたという事実こそが重大な懸念なのである。

有効な情報セキュリティガバナンスを達成するためには、役員は包括的な情報セキュリティプログラムの開発と維持の方向づけを行うためのフレームワークの確立を行い、これを維持する必要がある。

情報セキュリティガバナンスのフレームワークは、一般的に次の要素から構成されている。

- 情報セキュリティガバナンスのリスク管理の方法論
- ビジネス目標および IT 目標に明確にリンクした包括的なセキュリティ戦略
- 有効なセキュリティ組織構造
- 保護される情報の価値を取り上げたセキュリティ戦略と、その提供
- 戦略、コントロール、規制の各側面に対処するセキュリティポリシー

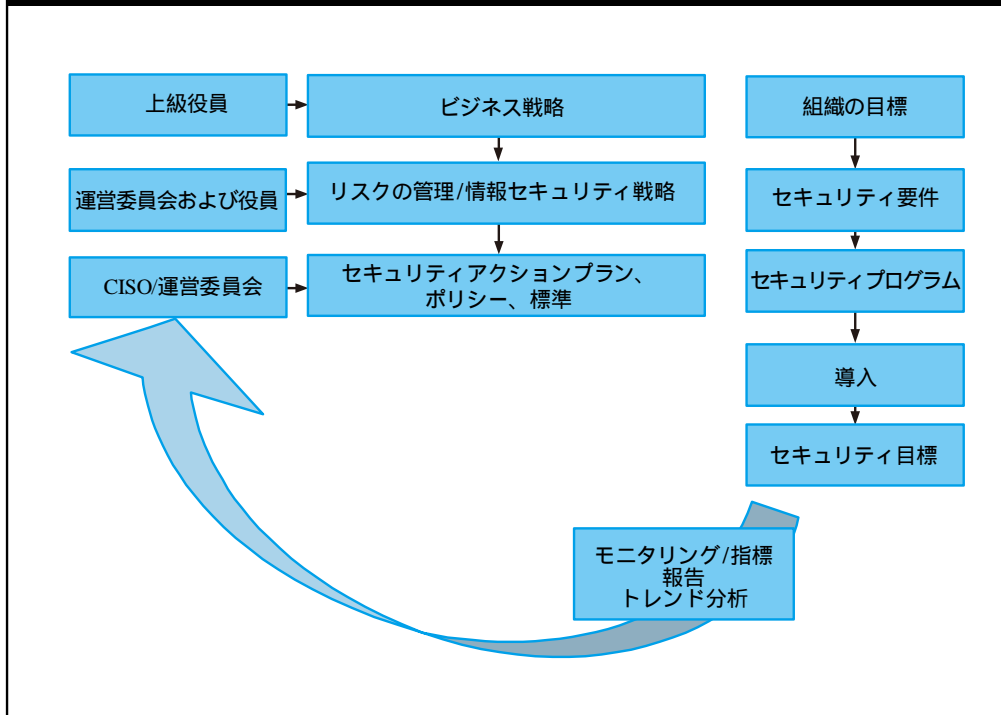
- 手続きとガイドラインがポリシーに準拠していることを保証するポリシー別のセキュリティ標準
- 準拠性を保証し、有効性とリスクの軽減に関してフィードバックを提供するための、制度化されたモニタリングプロセス
- セキュリティポリシー、標準、手続き、リスクを継続的に評価し更新する過程を保証するプロセス

一方、このフレームワークは、有害事象の影響を制限することで、組織の達成目標をサポートし、運用の予見性を許容できるレベルで提供する、費用効率の高い情報セキュリティプログラム開発の基礎となる。プログラム全体の目標は、情報資産がその価値、あるいはこの資産が損害を受けた場合に組織に発生するリスクに見合ったレベルで、保護を提供することにある。

このフレームワークは、この目標実現をサポートする一連のアクティビティを生じさせる。図 1 は、ビジネス目標と統合したセキュリティ戦略の作成時に必要な人という構成要素を示している。

統合を促進するために、ビジネス戦略は、リスクの管理および情報セキュリティ戦略の作成に対して提言の一つを与える。その他の提言は、ビジネスプロセス、リスクの評価、ビジネスに対する提言の分析、さらにビジネスプロセスの成功に決定的な役割を果たす情報資源である。規制の要件もまた、セキュリティ戦略を作成する際に考慮される必要がある。セキュリティ要件は、リスクの管理アクティビティの成果の一つであり、これらのセキュリティ要件との関連で見た企業の現状と共に、計画アクティビティに対して提言を行う役割を果たす。計画段階に対するその他の提言としては、所望のセキュリティ状態を達成するために利用可能な資源および適用される制約がある。

図1 - 情報セキュリティガバナンス概念図



戦略は、導入されればセキュリティ目標を達成することになる、一つあるいは複数のセキュリティプログラムから構成されるアクションプランの基礎となる。戦略とアクションプランには、モニタリングに関する条件と、成功のレベルを決定する定義された指標が含まれていなければならない。これによって、最高情報セキュリティ責任者(CISO)および運営委員会に対してフィードバックが提供され、またこのフィードバックによって進行中の修正が可能になり、さらにセキュリティのイニシアチブが定義された目標を満たすための軌道にのっていることを保証することにもなる。

役員と取締役が、どのような情報資源がどのレベルの保護を必要としているかが分かれば、情報セキュリティのベースラインの作成と、この導入が可能になる。情報セキュリティのベースラインは、情報資源が保護されるために提供される必要のある許容される最低限のセキュリティである。ベースラインは、資産の外からの影響に対する機密性およびその重要性によって異なる。ベースラインは、企業全体において、技術的標準、手続き上の標準、人員面での標準の形で表すことができる。ベースラインは通常、COBIT や ISO 17799 のように広く認められた標準や、FIPS 規格 200 や NIST SP 800-53、さらに企業情報セキュリティ作業部会 (CISWG) 等、ある国に特有のガイダンス、さらに組織が、リスク軽減にかかるコストとの比較で考慮した、許容できるレベルのリスクについての決定を組み合わせたものを利用して作成される。ベースラインの一例としては、COBIT セキュリティベースライン (Security Baseline)¹⁰があるが、これは専門家であるユーザ、ホームユーザ、経営者、役員、上級役員、取締役会/評議員会に対して、セキュリティに関する意識づけを与え、ガイダンスを提供するものである。

¹⁰ 前掲書、IT Governance Institute, COBIT Security Baseline

情報セキュリティの範囲で新たに発生しつつある定義により、情報の有益性や所有といった概念が、特に後者は、盗難、偽装、不正に対処することを目的として、追加されようとしている一方で、ネットワーク経済により、電子取引の信頼性と説明責任に対する不可欠なニーズが新たに発生した。

この背景の中で、セキュリティ目標は、次の点がクリアされたときに達成される。

- 情報が必要なときに利用および使用可能であり、情報を提供するシステムは、攻撃に対する抵抗力があり、攻撃を受けても回復することが可能である（*可用性*）
- 情報が、それを知る必要のある人だけが閲覧可能で、また知る必要のある人だけに開示されている（*機密性*）
- 情報が許可なく変更されることから保護されている（*インテグリティ*）
- 企業の所在地間、または外部の取引相手とのビジネス上のやり取り、さらには情報交換が信頼のおけるものである（*真正性および否認防止性*）

可用性、機密性、インテグリティ、さらに真正性および否認防止性の相対的な優先順位ならびに重要性は、情報システムの中のデータと、そのデータが使用されるビジネス上の背景に応じて異なる。たとえば、インテグリティは特に、マネジメントに関わる情報が、重要な戦略関連の決定ならびに財務報告に影響力をもっているため重要である。法的な規制、規則の観点からは、機密性が今日では最も重要である。機密性は、個人、財務、あるいは医療に関する情報や企業秘密の保護、その他の形態の知的財産（IP）に関わっているため、今日では最も重要である。

3. 情報セキュリティガバナンスに関わるべき人は?

取締役会/役員会

組織の利害関係者の利益の保護は、上級役員の基本責任である。これは、ビジネスに対するリスクを理解して、このリスクがガバナンスの観点から確実に対処されることが含まれている。これを効果的に行うためには、情報セキュリティガバナンスを組織の企業ガバナンスフレームワーク全体と統合して、情報セキュリティのリスクも含めたリスクの管理を行うことが必要になる。

情報セキュリティガバナンスには、戦略の指針と機動力が必要である。情報セキュリティガバナンスには、コミットメント、資源ならびに情報セキュリティの管理責任の割り当て、さらには取締役会がその意向が満たされているかどうか判断するための手段が必要となる。経験的に、情報セキュリティの有効性は、上級役員の情報セキュリティ方針の承認への関与ならびに適切なモニタリングおよび報告とトレンド分析を示したメトリックスにかかっていると見える。

取締役会は組織の情報資産と、現在進行中のビジネスの運用における重要性について意識している必要がある。取締役会に対して、定期的に包括的リスク評価およびビジネスインパクト分析の結果を高いレベルで提供することによって実現できる。また、ビジネスの情報資産への依存度評価によっても実現しうる。これらのアクティビティの結果には、取締役会が保護を求める主要な資産の認証/承認および保護レベルおよび優先順位が、相当な注意義務について承認された標準に鑑みて、適切なものであることを確認することも含まれている。

経営者の姿勢は有効なセキュリティガバナンスに大いに役立つものとなるはずである。上級役員がセキュリティポリシーを遵守していなかったら、下位の人員に対して遵守を期待することはできない。目に見える形で、定期的に取締役会の構成員が、本来あったセキュリティポリシーを確認することは、セキュリティに対する期待が全企業レベルで満たされることを保証する基礎となる。遵守しなかった場合の罰則が決定され、取締役会のレベルから下位に対して周知され、施行される必要がある。

役員

有効なセキュリティガバナンスの導入と組織の戦略的セキュリティ目標を定義することは、複雑で、困難な課題である。この課題を成功させるために、リーダーシップと役員による継続的なサポートが必要である。有効な情報セキュリティ戦略を作成するには、事業単位の管理者とプロセスオーナーとの統合と協力が必要である。

成功と考えられる結果は、情報セキュリティアクティビティが、組織の目標をサポートする形で整合している状態である。目標の達成度は、情報セキュリティプログラムの効果が定義され、不利益を被る事象の影響が許容可能なレベルであるかどうかを測定することができる。

この一例としては、アメリカ連邦政府のサイバーセキュリティがある。これは、セキュリティに関して明確な権限と実行責任を割り当て、この任務を遂行していることに関して、官僚に常に説明責任を与え、セキュリティ要件を予算および資

取締役が必ず行う必要のあるプラクティスは次のものである。

- 情報セキュリティを取締役会の基本方針に盛り込む
- 情報セキュリティリーダーを特定し、常に説明責任を与え、これに対するサポートを確保する
- 企業の情報セキュリティポリシーの有効性を、検討および承認の手続きを通じて確保する
- 情報セキュリティを主要な委員会に割り当てる*

* 前掲書、National Association of Corporate Directors

本計画プロセスに統合することを要請している¹¹。

運営委員会

情報セキュリティは組織の全ての側面に影響を与える。セキュリティへの配慮に影響を受ける全ての利害関係者が関与するためには、運営委員会の役員が設置される必要がある。この委員会の構成員には、最高経営責任者（CEO）あるいはこの指定を受けた者、事業単位の役員、最高財務責任者（CFO）、最高情報責任者（CIO）/ITディレクター、最高セキュリティ責任者（CSO）、最高情報セキュリティ責任者（CISO）、人事部、法務部、リスク管理部、監査部、業務部、広報部といったものが含まれる。運営委員会は、役員らの意図と指針の周知のための有効な経路であり、セキュリティプログラムと組織の目標の整合を保証するために、継続的に使用可能な基礎を提供する。さらにこの委員会は、行動変革を達成して、良好なセキュリティプラクティスとポリシーへの準拠性を促進する文化へと到達するには欠くことができない。

最高情報セキュリティ責任者（CISO）

全ての組織には、この役職名であるかどうかは別にしてCISOがいる。情報セキュリティ部や情報セキュリティ部長が設置されている場合や、CISOが事実上CIOやCSO、CFOである場合や、また若干のケースでは、CEOと同一の場合もある。情報セキュリティに関する懸念の範囲は非常に広いため、要求される権限と責任を、最終的に最高レベルの役員あるいは執行役員が引き受けることは避けられない。不履行による法律上の責任は、命令構造を上へ上がっていく形で広がり、最終的には上級役員と取締役会がこれを引き受けることになる。これが認識できず適切なガバナンス構造を導入することができなかつた場合は、上級役員自身に責任があり、これに付随して義務を負っていることに気づかない結果にもなりかねない。さらにこのような状況では、多くの場合、組織の目標に対する有効なセキュリティアクティビティの整合がない結果となる。組織が情報に依存していること、さらにこれに対する脅威が増していることを、より多くの組織が理解し始めたため、賢明な経営者は情報セキュリティ責任者の地位を最高レベルの役職者あるいは役員にまで高めつつある。この地位が存在することを確保すると、この地位にある者に対して責任と権限、さらに必要とされる資源を割り当て、経営者と取締役会による健全な情報セキュリティガバナンスに対する意識や、この問題へのコミットメントがあることは明らかになる。

4. 取締役会/評議員会および上級役員は何をするべきか

取締役会と経営者には、情報セキュリティガバナンスが確実に施行されるために、いくつかの基本的な責任がある。両者に重点を置かなければならない問題には、次のようなものがある。

情報セキュリティが管理されなければならない理由を理解する

- リスクや脅威が現実のもので、企業に重大な影響をもたらす可能性がある
- 風評被害の影響が大きい
- 有効な情報セキュリティには、トップダウン方式で調整し統合したアクションが必要である
- IT投資が、十分であり誤った方向に向かう可能性がある

¹¹ The US National Strategy to Secure Cyberspace, 2003, www.whitehouse.gov/pcipb

- 文化と組織の要因が同様に重要である
- 規則と優先順位を確立し、施行する必要がある
- 取引相手と電子的手段で取引を行う場合に、信頼(トラスト)を示しておく必要がある
- システムセキュリティの信頼性を、全ての利害関係者に対して示す必要がある
- セキュリティのインシデントが公に開示される可能性がある

取締役会レベルでのアクション

- 情報セキュリティに関して知識を得る
- 指針を設定する、すなわち、ポリシーと戦略を推進し、全体のリスクの概要を定義する
- 情報セキュリティに関する試みに資源を提供する
- 経営者に責任を割り当てる
- 優先順位を設定する
- 変化をサポートする
- リスクの意識に関する文化の価値を定義する
- 内部および外部の監査人から保証を得る
- 経営者がセキュリティ関連の投資およびセキュリティの改善を測定して、プログラムの有効性に関してモニタリングし報告する

上級役員レベルでのアクション

- ポリシーが組織の管理主体によって承認され、関連する役割と責任が割り当てられたら、標準、指標、プラクティス、手続きから構成されるセキュリティとコントロールフレームワークの作成を管理する(デザイン)¹²。
- ビジネスの提言を受けて、セキュリティポリシーの作成の指針を設定する(ポリシーの作成)
- 個々の役割、責任、および権限が明確に周知され、全ての者に理解されていることを確保する(役割と責任)
- 脅威や脆弱性が特定され、分析され、モニタリングされ、相当の注意義務に関して業界のプラクティスが利用されることを求める
- セキュリティインフラストラクチャの設置を求める
- 発生する可能性のあるコントロールの優先順位づけを可能にする資源が利用可能であり、対抗措置が期限どおりに導入され、効果的に確実に維持される方針を設定する(導入)
- セキュリティの侵害を検知し、確実に修正されるモニタリングの方法を確立する。これによって、現実に存在する侵害も、侵害の疑いのあるものも迅速に特定され、調査され、それに対する対応が講じられるようにする。さらに、現状での方針、標準、最低限許容されるセキュリティプラクティスへの準拠性を確保する(モニタリング)
- 定期的なレビューやテストが行われることを求める
- 侵入検知やインシデントへの対応を導入するのに役立つプロセスを実施する
- モニタリングや指標により情報が保護され、情報システムを安全に運用するために適正なスキルが利用可能であり、セキュリティのインシデントが適当な時点で対処されることが確保されることを求める。セキュリティ対策およびプラクティスについての教育が、組織のセキュリティプログラムの成功には最も重

¹² このサブセクションでハイライトされたキーワードについては、International Federation of Accountants' guideline, *Managing Security of Information*, USA, 1998 を参照。

要である。(意識、訓練、教育)

- セキュリティがシステム開発のライフサイクルプロセスの構成要素として確実に考慮される、このプロセスの各段階において、明確に対処されている

指示と結果の関係を示すマトリックス

有効な情報セキュリティガバナンスと、マネジメントの指示との間関係を、図2に示した。ここにあげた指示は全てを網羅しようとしたものではないものの、取締役会および役員が責任を負ういくつかの主要な課題とレベルが示されている。

図2 - マネジメントの指示と成果の関係

役員レベル	戦略との整合	リスクの管理	価値の提供	成果の測定	資源の管理	統合
取締役会/役員会	整合が証明されるように目標を設定する。	全てのアクティビティおよび規制の準拠性に適用されるリスクの管理ポリシーについて、指針を設定する	セキュリティアクティビティのコストおよび保護される情報の価値を報告するために指針を設定する	セキュリティの有効性について指針を設定する	ナレッジマネジメントと資源の利用のポリシーに対する指針を与える	プロセス統合を行う方針に対する指針を与える
上級役員	セキュリティをビジネス目標に統合するプロセスを開始する	役割と責任には、全てのアクティビティのリスクの管理が含まれていることを保証する。規制に対する準拠性をモニタリングする	セキュリティイニシアチブおよび保護される情報の価値についてのビジネスケーススタディを要求する	セキュリティアクティビティについて報告するためのモニタリングと指標を要求する	知識の取得と効率性の指標のためのプロセスを確保する	統合に関する全てのマネジメントプロセスの機能と計画の監視を行う
運営委員会	セキュリティ戦略と統合への試みを検討し、これを支援し、事業単位マネージャおよびプロセスオーナーが統合をサポートしていることを保証する	発生しつつあるリスクを明確化し、事業単位セキュリティプラクティスを推進し、準拠性に関する問題を明確化する	ビジネス機能に役立つセキュリティイニシアチブ、および実現されるサービスに関連して提供される価値の妥当性を検討し、これについて助言する	どのセキュリティイニシアチブがビジネス目標を満たすか検討して助言する	知識の取得と普及のためのプロセスを検討する	最重要のビジネスプロセスとマネジメントの保証提供者を特定する。保証統合の試みに指針を与える
最高情報セキュリティ責任者	セキュリティ戦略を作成し、セキュリティプログラムとイニシアチブを監視し、現在の整合性に関して、事業単位マネージャおよびプロセスオーナーと連絡を取る	リスク評価ならびにビジネスインパクト評価を保証し、リスク軽減戦略を作成し、ポリシーならびに規制への準拠性を強化する	セキュリティ資源の利用状況と有効性、さらに評判および信頼の提供についてモニタリングする	モニタリングアプローチ、指標の収集アプローチ、分析アプローチ、および報告アプローチを作成し、これを導入する。セキュリティアクティビティに指針を与え、モニタリングする	知識の取得と普及のための方法を開発する。有効性ならびに効率性のための指標を開発する	他のマネジメントプロセス機能と連携する。ギャップと重複部分を特定し、これに対処する

5. どのような示唆に富む問いが行われるべきか

第8章は、体系づけられたプラクティスを提供する。しかし、情報セキュリティガバナンスの担当者は、情報セキュリティ関連の問題を見つけ出し、この問題に関して最初の情報を得るために、示唆的で意識を喚起する問いが必要になる場合がある。

情報セキュリティ関連の問題を見つけ出すための問い

- セキュリティ部門長/CISO がビジネスマネジメントを満足させ、また報告しているか
- 経営者がセキュリティ関連の決定に最後に関与したのはいつか。経営者は、セキュリティ関連のソリューションを推進する過程にどれぐらいの頻度で関与しているか
- 経営者は、セキュリティ責任者が誰か知っているか。担当の人員はそれを知っているか。他の者はそれを知っているか
- 社員がセキュリティインシデントを発見した時、セキュリティインシデントであると認識できるのか、または気がつかないか。それに関してすべきことを認識しているか
- 会社が何台のコンピュータを所持しているか把握しているか。経営者は不足を認識しているか
- 損失評価ならびに災害復旧計画が実施されているか
- 経営者は、方針、法律、規制の要件に違反するか、あるいはこの情報が漏れたときに混乱または競争における不利益を生じさせるおそれがある情報(顧客データ、戦略計画、財務情報、研究結果等)を全て特定しているか
- 会社は最近ウィルスやマルウェアの攻撃を受けたか。最近12ヶ月以内で成功した攻撃は何回あったか
- 侵入が発生したか。どれぐらいの頻度で発生し、影響はどのようなものか
- 何名が組織のシステムを利用しているかを把握しているか。許可されたアクセスかどうか、あるいはシステム利用者が何をしているか把握しているか
- セキュリティは結果論と考えられているか、あるいは前提条件と考えられているか

セキュリティ問題を結果論として処理しないこと。発展のライフサイクルのあらゆる局面において、この問題に対処すること。

経営者が情報セキュリティ関連の問題に対処する方法を見つけ出すための問い

- 企業がITリスクおよびセキュリティ関連のリスクに対する自らの立場を明確にしているか。その立場はどちらかといえばリスク回避的なものか、リスクテイキングなものか
- 情報セキュリティ投資額と用途は把握されているか。支出を正当化する方法は、最近12ヶ月以内で、セキュリティを改善するための目的でどのようなプロジェクトに取りかかったか
- スタッフの何割が、去年のセキュリティ研修に参加したか。マネジメントチームの何割が研修を受けたか
- 経営者が組織の情報およびシステムへのアクセスを持っている人を決定する方法は、どのようなものか。この決定はどれぐらいの頻度で再度取り上げられているか
- 組織がどのようにしてセキュリティのインシデントを検知しているか。このインシデントは、どのようにしてエスカレーションされ、経営者はこのインシデ

- ントに対して何を行っているか
- 経営者は、大規模なセキュリティのインシデントからの復旧する準備ができて
いるか
 - 上にあげた問題を全てカバーするセキュリティプログラムは存在するか。この
プログラムを遂行する者について、明確な説明責任があるか
 - IT スタッフは、コンピュータフォレンジック/一連の証拠保管に関する配慮を
理解しているか

情報セキュリティガバナンスのプラクティスを自己評価するための問い

- 経営者は、セキュリティに関する問題が企業の中で対処されていることを確信
しているか
- 経営者は、最近の情報セキュリティ関連の問題とベストプラクティスを意識し
ているか
- 企業はインシデント、脅威、脆弱性の通知、シェアリングサービスに関与して
いるか
- 業界のベストプラクティスは何か、どのようにして企業がそれと比較できるか
- 経営者は、情報セキュリティに関する企業の要件を定期的に明確化し、周知し
ているか
- 経営者は、企業が情報セキュリティの改善にどれほどの投資を行わなければな
らないかという点について、何らかの考えがあるか
- 情報セキュリティ関連の問題が、ビジネスおよび IT 戦略を発展させる際に検
討されているか
- 経営者は、セキュリティの状態とセキュリティ改善プロジェクトについて定期
的に報告を受けているか
- 経営者は、独立した情報セキュリティの監査やレビューを設定しているか。役
員は、推奨事項を実行しているか

6. 情報セキュリティガバナンスが提供するべきこと

主要な達成目標は、プロセスあるいはサービスの達成目標についての情報を提供するのに役立つ。すなわち、この達成目標を効果的に利用することによって、組織の目標が満たされているかどうかを決定することができる。情報セキュリティガバナンスは、適正に導入されれば、第1章に記載された5つの基本的な成果を提供するはずである。COBITから選択された達成目標のいくつかは、次のような形で提示される。

戦略との整合

組織の目標をサポートする、情報セキュリティにおける戦略の整合という達成目標を達成することは、しばしば困難になる。次のような達成目標を検討すること。

- ITセキュリティのコスト、利益、戦略、方針およびサービスレベルについて、透明性と理解を確保する。
- 包括的な一連のITセキュリティポリシーを作成する。
- IT戦略、ポリシー、コントロールフレームワークを周知させる。
- ITセキュリティポリシーを施行する
- ビジネスインパクトに関連するセキュリティインシデントを定義する
- リスクがIT目標ならびに資源に与えるビジネスインパクトについて明確な理解を確立する
- 事業継続計画をサポートするIT継続計画を確立する

情報セキュリティの主要な達成目標は、組織に対する有害事象を、リスクの許容される範囲内までに抑えることにある。

リスクの管理

リスクを管理して情報資産に生じる可能性のある影響を減らし、許容されるレベルにまで抑えるために、次のような達成目標を検討すること。

- 全てのIT資産を捕捉し、これを保護する
- ITセキュリティに発生するリスクの可能性と影響を確立し、これを減少させる
- 定期的なリスク評価を上級役員と主要なスタッフと共に遂行する
- 最重要な機密データへのアクセスを、許可されたユーザのみに許可する
- 最重要な機密情報が、それにアクセスできない人から確実に保護する
- セキュリティの脆弱な部分とインシデントを特定し、モニタリングし、報告する
- 遂行可能なテストおよび維持されるIT継続計画を作成する

情報セキュリティの主要な達成目標は組織に対する有害事象を、リスクの許容される範囲内までに抑えることにある。それゆえに、主要な指標は、組織が被った情報セキュリティインシデントが与える有害な影響である。有効なセキュリティプログラムは、影響の軽減という傾向を示している。定量的な指標には、長期的な影響のトレンド分析が含まれている。

資源の管理

情報セキュリティの知識およびインフラストラクチャは、効率的にかつ有効に利用されなければならない。次のような達成目標を検討すること。

- 情報のインテグリティとプロセスのためのインフラストラクチャを維持する。
- 全てのIT資源を捕捉し、これを保護する

- IT サービスおよびインフラストラクチャが、エラー、巧妙な攻撃、災害による機能不全に抵抗力があり、かつ回復力がある
- アプリケーションや技術ソリューションの適正な使用ならびに成果を確保する

成果の測定

情報セキュリティプロセスを測定し、モニタリングし、また報告すれば、組織の目標の達成が確保される。次の指標を一例として検討すること。

- 公衆の評判にダメージを与えるインシデントの件数
- セキュリティ要件を満たしていないシステムの数
- アクセス権限を与え、変更し削除するのにかかる時間
- 不正アクセスによる侵入の疑いがあるもの、また実際に発生した侵入の件数と種類
- 防御された悪意のあるコードの件数と種類
- セキュリティインシデントの件数と種類
- 古くなったアカウントの数と種類
- 許可されていないIPアドレス、ポート、トラフィックが拒絶された件数
- 許可されたアクセス権、廃棄されたアクセス権、リセットされたアクセス権、変更されたアクセス権の件数

価値の提供

セキュリティに関する投資は、組織の目標をサポートするよう最適化されるべきである。セキュリティに関するアクティビティでは資源が消費される。最適の投資レベルは、セキュリティに関する戦略達成目標が達成され、許容されるリスクに対する対応を組織ができるだけ低いコストで達成できた場合に発生する。次のような達成目標が考慮されねばならない。

- 自動化したビジネスの取引と情報交換を信頼することができることを保証する
- 必要なITサービスが利用可能であることを確認する
- ITサービスが断絶する可能性を最小限に抑える
- セキュリティの脆弱な部分とインシデントの影響を最低限に抑える
- ITサービスが中断した場合、また変更された場合、ビジネスの影響が最低限であることを確保する
- 重要なITリスクに対して費用対効果のあるアクションプランを確立する

本書において先に述べたとおり、プロセスの統合は、情報セキュリティガバナンスにおいてますます関心が高まっている領域である。これは、その大部分が、組織の変化に迅速に対応したいという必要性に推進されたもので、組織のセキュリティ関連のアクティビティを分割しようとする傾向に重点を置いている。それゆえ、このアクティビティについて、適正なマネジメントプロセスの保証を確保する必要がある。

情報セキュリティガバナンスへのアプローチには、プロセスとアクティビティが最初から最後まで、意図したとおりに機能し、隠れたリスクを軽減することを保証する。このアプローチの導入に成功するということは、次のことから明らかになる。

- 情報資産の保護にギャップが存在しない。
- 不必要なセキュリティの重複が排除されている。
- 保証アクティビティがシームレスに統合されている。
- 役割と責任が十分に定義されている。
- 保証提供者がその保証関係の役職との関係を理解し、定期的に互いに連携する。

7. 情報セキュリティガバナンスはどのように変化しているか

情報セキュリティガバナンスの向上の要件は、近い将来も継続することが予想される。セキュリティ関連の出費がリスクの増大に対応して増加している一方で、セキュリティがなりすまし犯罪や不正、さらに顧客の個人情報の大規模な損失、またその他の情報システムの犯罪や破壊的な目的での使用は変わることなく続いている。多くの研究で共通して、情報セキュリティはガバナンスレベルの懸念として対処される必要があるという、本書が提示した結論を支持している。

従来は技術的なソリューションに重点を置いていたが、この立場はセキュリティが基本的に、マネジメントの問題であり、最高レベルで対処されるべきという理解に置き換える必要がある。組織の資産が以前に比べて無形化しているため、情報資産の保護における注意義務は、以前にもまして注意と資源が必要になる。さらに、有効な情報セキュリティガバナンスが、多くの法律および規制/法定の要件に適切に対処するために必要となりつつある。この問題に対処することができない組織は、競争上不利な状況に置かれ、技術的に巧妙さを増している犯罪者の餌食になっていることに気づくだろう。市場がガバナンスの重要性についての知識を深めているため、株価がガバナンス（良いものも悪いものも）に結びつく度合いを増していることが見受けられる。

オペレーショナルリスクの管理、全面的な財務情報の開示、個人情報保護に関する厳格な規制に伴って、機運としては世界的にプライバシーやサイバー犯罪の問題に対処する方向に向かっている。多くの地域では、法律を制定してよりよいセキュリティガバナンスのプラクティスを求める過程にある¹³。組織は、世界的にセキュリティの状況が改善され、セキュリティやプライバシーの機能不全が経済、組織および個人にとってさらに安いものになるまで、継続的に監視が厳しくなっていくことを期待している。

組織は、重要な情報資産を十分に保護することができないという事実がさらに目につくようになり、また許容できないものになっていくと考える必要がある。賠償責任は、最終的には取締役はその責任がに向かうことになる。上級役員は、十分なセキュリティが存在しないことは、リスクの先延ばしを意味し、回復するためのコストは調達が不可能な賠償責任や脅威につながっていくことを理解する必要がある。

インターネットセキュリティの侵害を公表したケースで、その会社の市場価値に悪い影響が出ているという結果が示されている。例示した侵害を受けた会社は、その公表から平均して2日後には、その市場価値の2.1%を損失しており、侵害1件あたり時価総額を平均すると16億5千万ドルの損失となっている*

* *International Journal of Electronic Commerce*, volume 9, number 1, fall 2004

¹³ セキュリティ侵害法、www.perkinscoie.com/content/ren/updates/privacy/092605.htm

経営者は、大きな過失が直接的に財務上の結果につながるリスクが、拙劣なガバナンスと標準以下のプラクティスが公に明らかになることも考慮すべきである。このような事態は、一方で、株価の下落に反映されるであろう、評判の損失につながる可能性を含んでいる。

アバディーングループ（Aberdeen Group）が行った調査¹⁴で提供された証拠から、セキュリティが有効でないことを原因とする損失は、既知の広く使用されているセキュリティプラクティスを用いることで、90%まで減少することができる。これだけでも、責任のある経営者がアクションを起こすことの動機としては十分である。

組織は、情報セキュリティに対する考え方を変えつつある。情報セキュリティが組織に対して提供することのできる価値、またどのようにして情報セキュリティが利害関係者の価値の向上と維持に貢献するかに一層重点が置かれるようになりつつある。さらに、グローバリゼーションがかつてないほどに拡大していること、プライバシーの準拠性の問題、法律ならびに規制の要件、また軽率で過失を犯したと見なされた組織に対する不利な措置がとられる可能性といったことを考えると、取締役会や上級役員は、ガバナンスの懸念として、有効な情報セキュリティに対処することが賢明であるという考えがますます広まっている。

クラス内随一の[セキュリティ]レベルで営業している会社は、経済的損失を収益の1%以下に抑えている。一方、他の組織は、5%を上回る損失率を計上している*。

*前掲書、Best Practices in Security Governance

¹⁴ アバディーングループ、前掲書

8. 情報セキュリティガバナンスの導入に成功するために可能なこと

次の質問は、取締役会ならびに上級役員に対して、有効な情報セキュリティガバナンスが実施されている（あるいは実施されていない）度合いについて判断を始めるための適切な方法を例として示している。これは、ガバナンスを担当する者が問うべき問いである。

取締役に対する問い

- 取締役会は、組織が情報に依存していることを理解しているか
- 組織が情報セキュリティの価値と重要性を認識し、セキュリティを意識した環境を育むというあるべき経営トップの姿勢を定着させているか
- 組織にはセキュリティ戦略があるか。もしそうであれば、このセキュリティ戦略はビジネス戦略と整合しているか
- 取締役会は、規制を遵守していない場合は、組織が賠償責任を負う可能性があることを理解しているか。機密情報が損なわれた場合は、損害賠償が発生する可能性があることを取締役会は理解しているか
- 組織が大規模なセキュリティのインシデントを被った経験があるか。このインシデントの組織に対するコストは、算定されているか
- 情報セキュリティが取締役会の基本方針の項目であるか。情報セキュリティプログラムの状態について取締役会に報告するスケジュールがあるか
- マネジメントは、情報セキュリティに関して方針声明を発したことがあるか。もしあれば、この方針声明は検討、更新、承認を受けるものか？
- 最重要の情報が利用不可能になったり、損なわれたり失われたりした場合、組織は営業を続けられるか。収益の損失、顧客の喪失、投資家の信頼の喪失に関して、セキュリティのインシデントがどのような結果をもたらすか。インフラストラクチャが操業停止になったときに、どんな結果が生じるか
- 情報資産は法律と規制に準拠しているか。取締役会は、準拠性を保証するために、何を始めたか
- 監査委員会は情報セキュリティにおけるその役割を理解しているか、また、役員および監査人と共に、どのようにして指針を設定しているか
- CISO あるいは組織の情報セキュリティの管理を専門に担当する役員がいるか
- 人員がそのセキュリティについての責任を意識した状態を保証するための、適切な訓練と意識向上プログラムがあるか

役員に対する問い

- 取締役会は、どのようにして情報セキュリティに関する問題について情報を得られる状況を維持しているか。セキュリティのリスクならびにセキュリティの改善の状況について取締役会に対して行った最後の報告は、いつ行われたか。
- 情報セキュリティプログラムの作成、導入、管理について責任を負う者として、誰が任命されているか、またこの者には説明責任が常に与えられているか
- セキュリティ関連の役割と責任が明確に定義され、周知されているか
- CISO、あるいはセキュリティ目標を達成するのに十分な権限と資源をもった役員がいるか
- 組織はそのネットワークセキュリティをサードパーティによってチェックしてもらったことがあるか
- ビジネスインパクト評価が行われたことがあるか
- 情報セキュリティ資産の重大性ならびに機密性に関して最後にリスク評価が

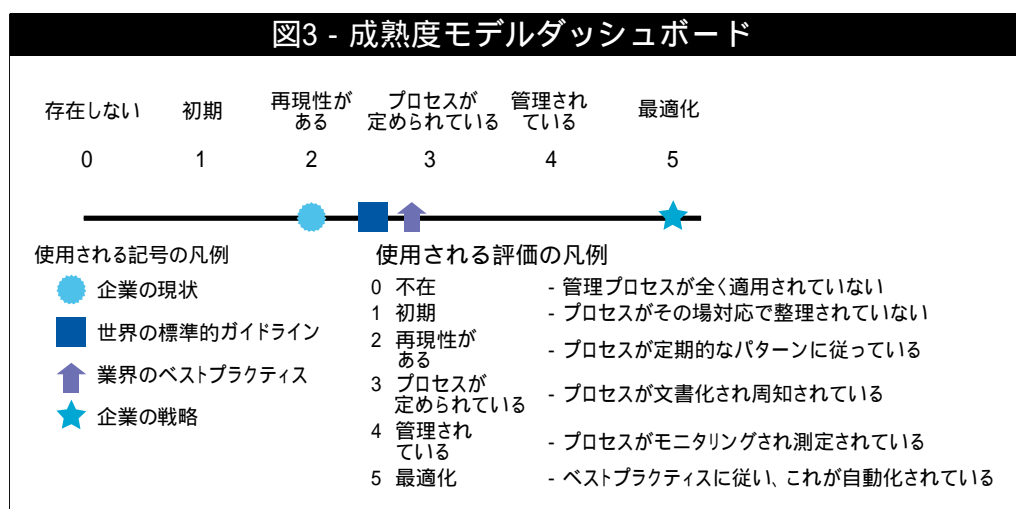
行われたのはいつか。次回のリスク評価はいつの予定か

- リスク評価は、最重要の情報を利用不可能になったり、損なわれたり失われたりした場合、組織は営業を続けられるかという問題を考慮しているか。収益の損失、顧客の喪失、投資家の信頼の喪失に関して、セキュリティのインシデントがどのような結果をもたらすか、リスク評価はカバーしているか。リスク評価は、インフラストラクチャが操業停止になったときに、どんな結果が生じるかを判断しているか
- CEO が、情報セキュリティ評価を要請しており、結果をスタッフと検討し、取締役会に報告しているか
- 情報セキュリティのインシデント/緊急事態に対処する、有効で実証済みのプロセスがあるか
- 業務継続/災害復旧計画が実施されているか。この計画は実際の状況で検証されているか。定期的にテストが行われているか
- リスク評価は、どの情報資産が法律と規制に準拠しているかを考慮しているか。リスク評価は、法律と規制への準拠性を保証するための十分な手続きにつながっているか
- 情報セキュリティのリスク評価は、IT マネジメントおよびビジネスマネジメントの会合で通常基本方針の項目であるか。役員は改善のイニシアチブを追求しサポートしているか
- 組織にはセキュリティ戦略があるか。もしそうであれば、このセキュリティ戦略はビジネス全体の戦略と緊密に整合しているか
- 情報セキュリティとビジネス目標の整合を保証するための、現在行われているプロセスがあるか
- 人員がそのセキュリティについての責任を意識した状態を保証するための、適切な訓練と意識向上プログラムがあるか
- 情報資産が十分に保護されていることを保証するための、情報資産分類プロセスが実施されているか

9. 組織が情報セキュリティガバナンスに関する比較を行う方法

取締役会と役員は、組織内の成熟度のランクを付けるために、情報セキュリティガバナンスの成熟度モデルを利用することができる。ITリスクが参照されているとき、ITリスクは情報セキュリティの文脈の中で検討される必要がある。このモデル¹⁵は、次を行うための方法として、徐々に適用することが可能である

- 尺度に対する自己評価で、組織が図3に示したうちのどこに位置するかを決定する
- 必ずしもトップレベルにある必要はないが、組織を尺度上のどの位置につけたいかという目標に基づいて、自己評価の結果を利用して将来の発展の目標を設定する
- この目標と現在の状況とのギャップ分析に基づき、この目標を達成するためのプロジェクトを作成する
- プロジェクトの分類ならびにそのコストに比較した有益な影響の分析に基づき、プロジェクトの作業に優先順位をつける



成熟度レベルの説明

0 不在

- プロセスとビジネス決定に関するリスク評価は行われていない。組織は、セキュリティの脆弱な部分と開発プロジェクトの確実でない部分に関連したビジネスインパクトを考慮していない。リスクの管理が、ITソリューションの調達やITサービスの提供に関して、明確化していない。
- 組織は情報セキュリティの必要性を認識していない。セキュリティの保証に関する責任と説明責任が割り当てられていない。情報セキュリティのマネジメントをサポートする指標が導入されていない。情報セキュリティの報告も、情報セキュリティの侵害に対する対応プロセスも行われていない。認識できるシステムセキュリティの管理プロセスが全く存在しない
- ITの運用に対するリスク、脆弱性や脅威、あるいはITサービスの喪失の、ビジネスに対する影響についての理解が全くない。サービスの継続性が役員の注意を要する問題として考慮されていない

1 初期/その場対応

- 組織はITリスクをその場対応で検討しており、定められたプロセスやポリシーは存在しない。プロジェクトのリスクに関する公式でない評価が、プロジェクト毎に決定された上で行われている。
- 組織は情報セキュリティの必要性を認識しているが、セキュリティ意識は個人によって異なる。情報セキュリティは問題に反応する形で対処されており、測定されていない。責任が明

¹⁵ IT Governance Institute, COBIT 4.0, USA, 2005 をもとに調整したもの

確でないため、情報セキュリティの侵害が発見された場合、責任追及型の対応が発生する。情報セキュリティの侵害に対する対応は予見できない。

- サービスの継続に関する責任は、正式なものではなく、権限は制限されている。役員はサービスの継続に係るリスクと、その必要性について認識しつつある。

2 再現性はあるが、直感的

- IT リスクが重要であり、検討される必要があることについて、理解が生じつつある。リスク評価のアプローチは存在しているが、プロセスは成熟しておらず、発展途上である。
- セキュリティの保証に関する責任と説明責任が、情報セキュリティ調整者に割り当てられているが、この者に管理権限はない。セキュリティ意識はばらばらで、限られたものである。情報セキュリティの情報が作成されているが、分析はされていない。セキュリティは、情報セキュリティのインシデントに反応して、サードパーティの提言を採用する形で、組織の特定の必要性に対処しないような対応を取りがちである。セキュリティポリシーは作成されつつあるが、不十分なスキルとツールがまだ使用されている。情報セキュリティに関する報告が不完全で、誤解を招くようなものであるか、あるいは関連性がない。
- サービスの継続に関する責任は割り当てられている。サービスの継続に対するアプローチは、分断されている。システムの可用性に関する報告が不完全で、ビジネスインパクトを考慮していない。

3 定められたプロセスがある

- 組織全体でのリスクの管理ポリシーによって、いつ、どのようにしてリスク評価を行うかが定義されている。リスク評価は、文書化され、訓練を通じて全てのスタッフが使用可能な定められたプロセスに従っている。
- セキュリティ意識は存在しており、役員がこれを後押ししている。セキュリティ意識報告が標準化し、定式化している。情報セキュリティの手続きが定められ、セキュリティポリシーおよび手続きに関する構造に適合している。情報セキュリティの責任は割り当てられているが、一貫して施行されていない。情報セキュリティ計画が存在し、リスク分析とセキュリティソリューションを推進している。情報セキュリティ報告が、ビジネスよりもITに重点を置いている。その場対応的に侵入テストが行われている。
- 役員がサービスの継続の必要性について、一貫して周知している。可用性の高いコンポーネントとシステム二重化運用をばらばらに適用している。最重要のシステムとコンポーネントの一覧が厳格に維持されている。

4 管理、測定されている

- リスクの評価が標準化した手続きであり、この手続きに従うことについての例外をITマネジメントが認識している。ITリスクの管理は、上級レベルの責任を負った定められた管理職である可能性が高い。上級マネジメントとITマネジメントは、組織が許容することができるリスクのレベルを決定し、リスク/収益率の標準化した指標を持っている。
- 情報セキュリティの任務が明確に割り当てられ、管理され、施行されている。情報セキュリティのリスク分析およびインパクト分析が一貫して行われている。セキュリティポリシーとプラクティスが完成されており、特定のセキュリティベースラインがある。セキュリティ意識報告が義務化している。ユーザID、認証、許可が標準化しているスタッフのセキュリティ証明が確立している。侵入テストが標準化および定式化したプロセスであり、改善につながっている。費用便益分析が、セキュリティ指標の導入をサポートする形で、利用される度合いが徐々に増している。情報セキュリティプロセスが、組織全体のセキュリティ関連の役割と調整されている。情報セキュリティ報告がビジネス目標にリンクしている。
- サービスの継続に関する責任や標準が施行されている。可用性の高いコンポーネントを含め、システム二重化運用のプラクティスが一貫して配置されている。

5 最適化

- リスクの管理が、構造化した組織全体のプロセスが施行され、定期的に行われ、十分に管理されている段階にまで発展している。
- 情報セキュリティが、ビジネスマネジメントとITマネジメントが共同で負う責任であり、企業のセキュリティビジネス目標に統合されている。情報セキュリティ要件が明確に定義され、最適化され、確認されたセキュリティ計画に含まれている。セキュリティに関する役割が、計画段階ではアプリケーションに統合され、エンドユーザがセキュリティの管理について説明責任を負う度合いが徐々に増している。情報セキュリティ報告が、最重要のシステムについての自動アクティブモニタリングアプローチを利用して、変化しつつあるリスクおよび発生しつつあるリスクについて早期に警告を与える。インシデント、自動化されたツールにサポートされた、正式な事故対応手続きにより、迅速に対処されている。
定期的なセキュリティ評価により、セキュリティ計画の導入の有効性が評価される、新しい脅威と脆弱性に関する情報が体系的に収集および分析され、十分に軽減する方向でのコントロールが迅速に周知され、導入される。侵入テストおよびセキュリティインシデントの根本原因の分析、事前のリスクの特定が、継続的な改善の基礎となっている。セキュリティプロセスおよび技術が、組織全体で統合されている。
- サービスの継続計画および事業継続計画が統合され、整合され、日常的に維持されている。継続的なサービスの必要性について、ベンダーや主要なサプライヤから賛同を得ている。

付録 -

規制団体ならびに標準化団体の情報セキュリティガバナンスに関するガイダンス

情報のセキュリティ、および情報を処理ならびに加工するシステムのセキュリティを扱う、数多くの国際的な標準化および規制団体が存在する。以下は全てを網羅するリストではなく、むしろこれらの主要な標準や団体のうちのいくつかが、どのようにして情報セキュリティの問題に対処しているか、その雰囲気を変えようとするものである。アプローチ、分割、重点は大きく異なっているが、セキュリティ標準と目標は一貫している。

COBIT® 4.0 (2005年)

IT ガバナンス協会 (ITGI) が開発し、広めたものである COBIT® (*Control Objectives for Information and related Technology*) は、企業がその目標を達成するために必要とする情報を、IT が提供する必要があるという前提から出発している。COBIT は、プロセスの重視とプロセスの所有を促進することに加えて、企業の信用、資質、およびセキュリティの必要性に注目し、ビジネスが IT に求めるものを一般的に定義するために使用される、7 つの情報要請規準を示している。それは、有効性、効率性、可用性、インテグリティ、機密性、信頼性、準拠性である。

COBIT はさらに、IT を 4 つの領域 (計画と組織 [PO]、調達と導入 [AI]、サービス提供とサポート [DS]、モニタリングと評価 [ME]) に属する 34 の IT プロセスに分けている。COBIT フレームワークは、20 以上のプロセスのうち、懸念されている情報セキュリティの問題に対処している。しかし、情報セキュリティに最も直接関係する 4 つのプロセスは、次のものである。

- PO6—マネジメントの意図と指針の周知
- PO9—IT リスクの評価と管理
- DS4—サービスの継続の保証
- DS5—システムのセキュリティの保証

あらゆるプロセスに関して、次の通りレベルの高いコントロール目標が定義されている。

- この IT プロセスにおいて、どの情報要請基準が最も重要であるかを明確化する
- どの資源が通常利用されているかリスト化する
- この IT プロセスをコントロールする際に重要な点を考慮する

COBIT はさらに、コントロールの導入の際のベストプラクティスや、これらの目標に立脚した包括的な監査ガイドラインや成熟度モデルを求める、役員と IT の実務担当者に対して、200 以上の細かいコントロール目標を示している。

COBIT はマネジメントとガバナンスのレイヤー (層) を包括するもので、役員に次のものを提供する。

- 成果の測定の要素 (全ての IT プロセスで結果の指標および成果要因)
- 各 IT プロセスについての簡潔で、技術的でないベストプラクティスを提供する、成功の鍵となる要因のリスト
- IT に対するコントロールのベンチマーキングや意思決定を支援する、成熟度モデル

COBIT セキュリティベースライン (2004年)

ITGI が発行したものであり、IT 利用に関するリスクに加えて、セキュリティを扱っている。COBIT フレームワークを利用して、このガイダンスは、全てのユーザ、すなわち、一般家庭、中小企業、さらにより大きい組織の役員と取締役会が実行し、導入することが容易な形で、IT セキュリティの特定のリスクに重点を置いている。このガイダンスでは、次の要素を示している。

- 読んで有益な箇所は次のものである。
 - 情報セキュリティ入門 - 意味と範囲

- セキュリティが重要な理由、うまくいかない最も一般的な事項の例
- リスクを捕捉するための示唆に富む問い
- ISO 17799 に主要なコントロールと位置づけを示す、COBIT ベースのセキュリティベースライン
- 特定の読者に対して基本的な意識に関するメッセージを示す、6つの情報セキュリティサバイバルキット
- 技術的なセキュリティリスクを含む付録

情報システムのセキュリティのガイドライン（2002年）

経済開発協力機構（OECD）の『情報システムのセキュリティのガイドライン（Guidelines for the Security of Information Systems）』は、情報システムのセキュリティ用フレームワークを構築しようとしている国、あるいは企業を支援することを目的としている。このガイドラインの目的は次のとおりである。

- リスクおよび情報システムの保護に対する意識を喚起する
- 一般的なフレームワークを提供することで、情報システムセキュリティのための有効な指標、プラクティス、手続きの作成と実施を援助し、かつこの問題に関して公共セクターと民間セクターの協力を促進する
- 情報システムに対する信頼、その導入、利用を促進する
- 情報システムの国家的ならびに国家間での開発、利用、セキュリティを促進する

このフレームワークは、法律、倫理規範、技術的指標、マネジメントやユーザのプラクティス、大衆の教育/意識向上アクティビティをカバーしている。最終的に意図するところは、このガイドラインは政府、公共セクターおよび民間セクター、社会が進捗を測定する際に参照する、ベンチマークとしての機能を果たすことである。

情報のセキュリティの管理（1998年）

1998年に、国際会計士連盟（IFAC）は情報セキュリティの目標を、「情報とその情報を提供する情報システムと通信手段に依存している人の利益を、可用性、機密性、インテグリティの機能不全によって生じる損害から保護すること」と定義している。いかなる組織でも、上の3つの基準が満たされたとき、すなわち、情報システムが必要なときに利用可能で（可用性）、データおよび情報がそれを知る権利のある人にもみ開示され（機密性）、かつ、データおよび情報が許可されない変更から保護されたとき（インテグリティ）、セキュリティ目標が満たされたと判断できる。

可用性、機密性、さらにインテグリティは、情報システム内のデータおよびそれが利用されるビジネス上の背景に応じて、異なった優先順位と意義を獲得することがある。

連邦政府情報システムにおけるセキュリティ管理策アセスメントガイド NIST 800-53A（初回公開版 2005年）

本書はアメリカ国立標準技術研究所（NIST）が、そのアメリカ連邦情報セキュリティ管理法（FISMA）2002年版、公法 107-347の規定による法定の責任を推進する目的で作成された。NISTは、十分な情報セキュリティを全ての官庁の運用ならびにその資産に提供するために、最低要件も含め、標準やガイドラインの作成に責任を負っているが、この標準やガイドラインが、全米のセキュリティシステムに当てはまっていない。このガイドラインは、アメリカの官庁が使用するために作成されたが、ボランティアベースで活動する非政府機関にも適当なものとなる。このガイドラインの利点のいくつかは、次のようなものである。

- セキュリティコントロールを選択し特定するための、一貫した、比較可能で、再現性のあるアプローチを促進する
- 情報システム用の最低限のコントロールについて勧告する
- 情報システム用のセキュリティコントロールの常に変動するカタログを推進する
- セキュリティコントロールの有効性を確認するための技術と手続きの発展の基礎をなす

本書の目的は、連邦情報処理標準 (FIPS) 200、さらに『連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項』(Minimum Security Controls for Federal Information Systems) (2005 年 12 月刊) の刊行まで、アメリカ連邦省庁に対して、ガイダンスを提供することであった。

情報セキュリティのマネジメントのための実践規範 ISO 17799 (2005 年)

国際標準化機構 (ISO) 17799、『情報セキュリティのマネジメントのための実践規範』は、情報システムが商工業の分野で利用されている場合に、大部分の状況に必要とされるコントロールの範囲を明確化するための基準点としての役割を果たす。

これは、あらゆる規模の組織が使用するのに適している。情報を、他の重要なビジネス資産と同様に、組織にとって価値を持ち、それゆえ適切に保護される必要がある資産として扱っている。情報セキュリティは、ISO 17799 の中では、次の項目を保護することであると説明されている。

- 機密性 - 情報が、アクセスを持つことを許可された人のみがアクセス可能であることを保証すること
- インテグリティ - 情報とそのプロセスの正確さと完全さを保護すること
- 可用性 - 許可されたユーザが、必要なときに情報ならびに関連の資産にアクセスできることを保証すること

この標準は、セキュリティリスク評価に基づいている。これは、さまざまな成果の中でも、主にセキュリティスタッフのコストの正当化、さらに生産性の向上の基礎を提供する。

情報セキュリティは、さまざまな脅威から情報を保護し、これによって業務の継続性、ビジネスに対する損害の軽減、投資に対する収益の最大化、ビジネスチャンスへの投資を保証する。セキュリティはこれに適した一連のコントロールを導入することで実現するが、このコントロールはポリシー、プラクティス、手続き、組織構造および/またはソフトウェアの機能から構成される。ISO は、他にも ISO 15048、『IT セキュリティの評価基準』(Evaluation Criteria for IT Security) などの標準を発行している。

システム信頼性のための Trust サービス (SysTrust) 原則および基準 (2003 年)

アメリカ公認会計士協会 (AICPA) およびカナダ勅許会計士協会 (CICA) が、Trust サービス (SysTrust) という、経営者、顧客、ビジネスパートナーの快適性を向上させることを目的とした保証サービスを発表した。SysTrust のサービスには、保証サービスを提供し、4 つの基本原則、すなわち可用性、セキュリティ、インテグリティ、保全性との比較で測定した場合に、システムが信頼できるものか評価する公認会計士を必要とする。

- 可用性 - システムが、サービスレベル説明書あるいはサービスレベル契約書に記載の運用ならびに使用の目的で利用可能である。
- セキュリティ - システムは許可のない物理アクセスならびに論理アクセスから保護されている。
- インテグリティ - システムの処理が完全で、正確で、期限とおりにかつ許可されている
- 保全性 - 必要なときに、システムは、その可用性、セキュリティ、インテグリティの妨げとなることも対立することもない形で更新可能である。

SysTrust は、信頼性のあるシステムを、特定の期間特定の環境で、深刻なエラー、深刻な障害、深刻な機能不全もなく、運用できるシステムであると定義している。このシステムの境界は、システムオーナーによって定義され、次の主要なコンポーネントを含んでいる。このコンポーネントとは、インフラストラクチャ、ソフトウェア、人、手続きおよびデータである。

SysTrust は拡張性があり、そのため、企業は柔軟的に、確認のために SysTrust 原則の一部を選択

することができる。全ての基準に関して表明された意見は、システム全体の信頼性に関する意見となる。会計士は、可用性あるいはセキュリティなど、個々の基準に関して、意見を表明することもできる。

情報セキュリティのグッドプラクティス標準（2005年）

情報セキュリティフォーラム（ISF）編『情報セキュリティのグッドプラクティス標準』は、参加者の研究および現実的経験に基づいている。「この標準は、情報セキュリティの問題にビジネスの観点から対処しており、組織の情報セキュリティ措置を評価するために、現実的な基盤を提供するものである。この標準は、コントロール下にある最重要な情報システム関連のビジネスリスクを維持するために主要な組織が行うべき措置に重点を置いている。」¹⁶それぞれの領域は、細かいセクションに分かれ、合計で135件のコントロールが行われる。

ISFは、一般的に、標準を導入すれば、次の点で組織の役に立つとしている。

- 国際的なベストプラクティスへ移行し、ビジネスのインテグリティを維持する
- 情報リスクの幅と深みを管理する
- サードパーティが、情報セキュリティに専門的に対処してくれるという信頼を構築する
- 主要なインシデントからの断絶の可能性を減少させる
- 増大するサイバー犯罪の脅威に対処する
- 法律および規制の要件に準拠する

この標準は、セキュリティを5つの構成要素をなす領域に分けている。

- セキュリティの管理
- 最重要のビジネスの応用
- コンピュータのインストール
- ネットワーク
- システムの開発

情報セキュリティガバナンス：アクションの要請（2004年）

2003年12月、アメリカ国土安全保障省が共同で、アメリカカリフォルニア州サンタクララ（Santa Clara）で全国サイバーセキュリティサミットを開催した。直接の成果は、コーポレートガバナンス作業部会を含め、民間セクターによる5つのタスクフォースの設立である。このレポートにおいて、この作業部会は、情報セキュリティガバナンスを企業の取締役会レベルの優先事項にすることを呼びかけている。主要な重点事項は、時間をかけて成果を体系的に改善するというプロセスの後に続く達成目標を持って、プロセスを始めることである。

このレポートは、政府や業界が起こすアクションについて多くの勧告を行っており、たとえば次のものが含まれる。

- 組織は、このレポートに記載された情報セキュリティガバナンスフレームワークを採用し、サイバーセキュリティをその企業のガバナンスプロセスに埋め込まなければならない。
- 組織はウェブサイト上で、自分たちの成果を評価しその結果を取締役会に対して報告する作業部会によって開発されたツールを用いる意思が自分たちにはあることを示すことで、情報セキュリティガバナンスに対するコミットメントについて広く周知しなければならない。
- アメリカ国土安全保障省は、情報セキュリティガバナンスフレームワークとの中核をなす一連の原則を承認し、また民間セクターに対して、サイバーセキュリティをコーポレートガバナンスの試みの一つにすえるよう勧告するであろう。
- トレッドウェイ委員会組織委員会（COSO）は、『内部統制：統合フレームワーク（Internal Controls—An Integrated Framework）』を改訂し、明確にセキュリティガバナンスに対処するものとする必要がある。

¹⁶ Information Security Forum, *Standard of Good Practice for Information Security*, version 4, UK, 2003

参考文献

- Aberdeen Group, 'Best Practices in Security Governance', USA, 2005
- Allen, Julia; *Governing for Enterprise Security*, Carnegie Mellon University, USA, 2005
- American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, *Privacy Framework Principles and Criteria*, USA and Canada, 2005
- American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, *SysTrust Principles and Criteria for Systems Reliability*, USA and Canada, 2003
- 'Building Security in the Digital Resource: An Executive Resource', *Business Roundtable*, 2002
- Business Software Alliance, 'Information Security Governance: Toward a Framework for Action', USA, 2003
- Corporate Governance Task Force, *Information Security Governance: Call to Action*, USA, 2004
- Corporate Information Security Working Group (CISWG), *Report of the Best Practices and Metrics*, USA, 2004
- Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standard, (FIPS) PUB 200, *Minimum Security Requirements for Federal Information and Information Systems, Initial Public Draft*, USA, 2005
- Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems, Initial Public Draft*, USA, 2005
- Department of Commerce, National Institute of Standards and Technology, Draft Special Publication 800-26 Revision 1, *Guide for Information Security Program Assessments and System Reporting*, USA, 2005
- Drucker, Peter; 'Management Challenges for the 21st Century', *Harpers Business*, 1993
- European Union (EU), *EU Privacy Directive*, 1995
- General Accounting Office, *Federal Information System Controls Audit Manual*, USA, 1999
- General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, USA, 1996
- Federal Financial Institutions Examination Council, *IT Examination Handbook: Management*, USA, 2004, www.ffiec.gov/ffiecinfbase/html_pages/it_01.html
- Federal Information Security Management Act (FISMA), USA, 2002
- Hallawell, Arabella; *Gartner Global Security and Privacy Best Practices*, Gartner Analyst Reports, USA, 2004, www.csoonline.com/analyst/report2332.html
- IBM, Data Governance Council, *Oversight of Information Security*, USA, 2005
- 'Information Security Addendum to Principles of Corporate Governance', *Business Roundtable*, USA, 2003
- Institute of Internal Auditors, *Information Security Governance: What Directors Need to Know*, USA, 2001
- Institute of Internal Auditors, *Information Security Management and Assurance: A Call to Action for Corporate Governance*, USA, 2000
- Institute of Internal Auditors, *Presenting the Information Security Case to the Board of Directors*, USA, 2001

Information Security Forum, *Standard of Good Practice for Information Security*, version 4, UK, 2003

International Federation of Accountants, *International Information Technology Guidelines—Managing Security of Information*, USA, 1998

International Organisation for Standardisation, *Code of Practice for Information Security Management*, ISO 17799, Switzerland, 2005

IT Governance Institute, *Board Briefing on IT Governance*, 2nd Edition, USA, 2003

IT Governance Institute, COBIT 4.0, USA, 2005, www.itgi.org

IT Governance Institute, *COBIT Security Baseline*, USA, 2004, www.itgi.org

KPMG, *Creating Stakeholder Value in the Information Age: The Case for Information Systems Governance*, UK, 2004, www.kpmg.co.uk/services/ras/irm/isg.cfm

McKinsey and Institutional Investors Inc., ‘McKinsey/KIOD Survey on Corporate Governance’, January 2003, www.mckinsey.com/clientservice/organizationleadership/service/corpgovernance/pdf/cg_survey.pdf

Moulton, Rolf; Robert Coles; ‘Applying Information Security Governance’, *Computers and Security*, Elsevier Ltd., UK, 2003

National Association of Corporate Directors, ‘Information Security Oversight: Essential Board Practices’, USA, 2001

Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks—Towards a Culture of Security*, France, 2002

The US National Strategy to Secure Cyberspace, USA, 2003



ITGI *Japan*