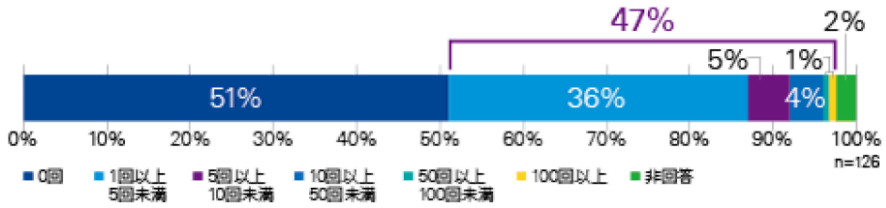
ISGA
Information Security Governance Association

情報セキュリティガバナンス協議会のご紹介

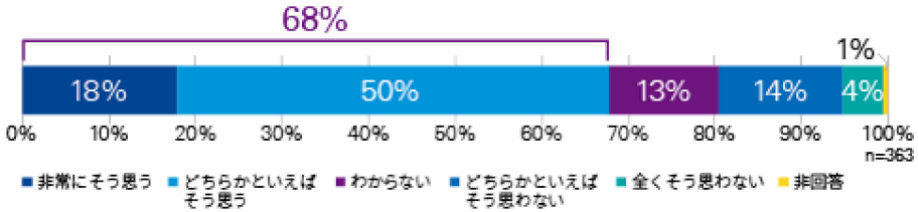
Information Security Governance Association

背景

- 日本企業の35%の企業が過去1年間にサイバー攻撃を受け、うち47%の企業において実際に被害が発生
- 約7割の企業が「サイバー攻撃の予防は取締役会で議論すべき」と考えています。
- 日本企業は米欧企業に比べ、「経営層のリスク感度が低い」「経営層にITやセキュリティの重要性を理解してもらえない」「経営とセキュリティの両方を理解している人材がいない」を挙げる割合が高く、経営層の認識が課題である点が特徴的

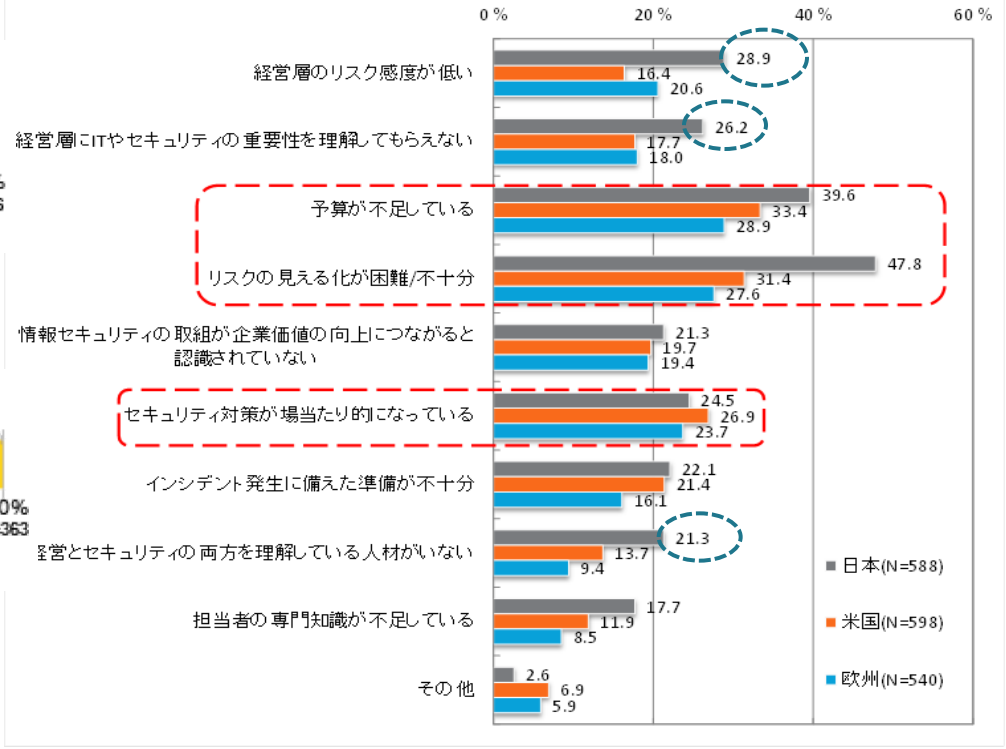


サイバー攻撃によって被害が発生した回数



サイバー攻撃の予防は取締役レベルで議論すべき

（出典：KPMGコンサルティング、「サイバーセキュリティ調査2016」, 2016/05）



情報セキュリティ対策を進めるうえでの課題点

（出典：IPA「企業のCISOやCSIRTに関する実態調査2016」報告書, 2016/05）

サイバーセキュリティ経営ガイドライン

経済産業省・情報処理推進機構「サイバーセキュリティ経営ガイドライン」より

■サイバーセキュリティは経営問題

•ビジネスを脅かすサイバー攻撃は避けられないリスクであり、セキュリティへの投資が必要。

•企業価値のためにセキュリティ投資をすべきか、経営判断が求められる。

•サイバー攻撃により社会に対して損害を与えてしまった場合、社会から経営者のリスク対応の是非、さらには経営責任が問われることもある。

■経営者が認識する必要がある「３原則」

•セキュリティ投資に対するリターンの算出はほぼ不可能であり、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。

•自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要。

•平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要。

情報セキュリティガバナンスを確立することで、
サイバーセキュリティ経営を合理的に実現できる可能性

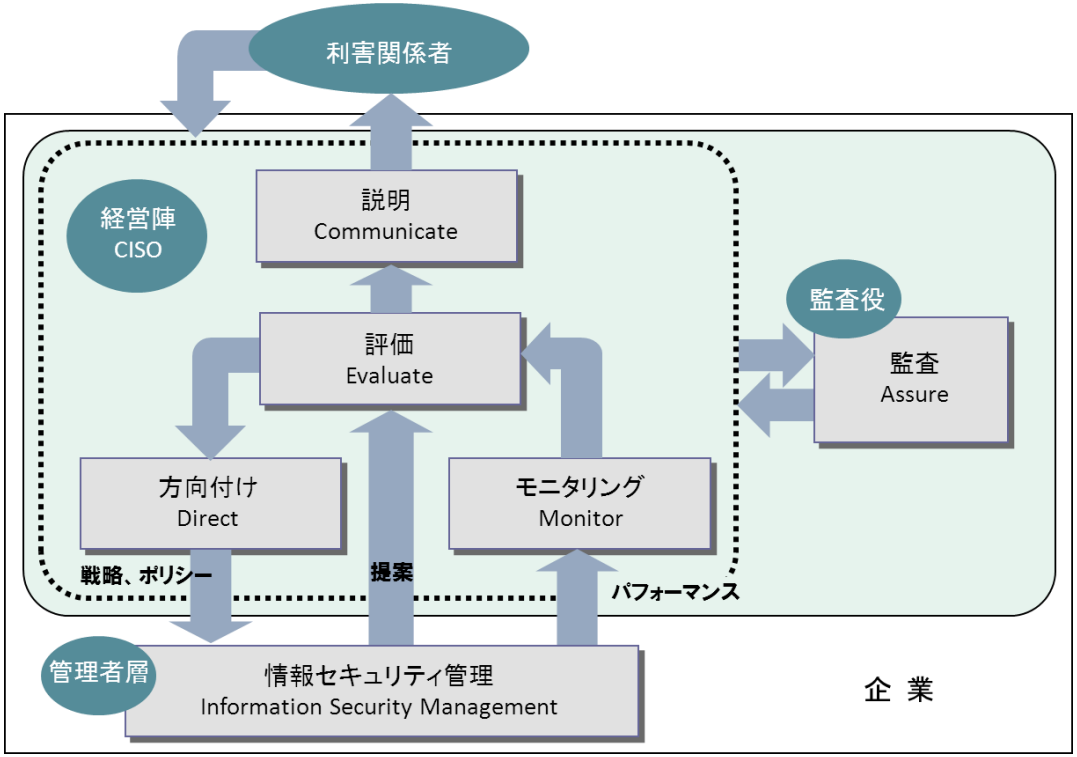
情報セキュリティガバナンスとは

- セキュリティの取組みが進まない企業の問題：
  - 経営陣が自社の情報リスクを把握していない、判断できない（**丸投げ**）
  - セキュリティの取組みがルーチンワーク化（**思考停止**）
  - 対症療法と部分最適化に終始（**機能不全**）
- **情報セキュリティガバナンス**は、企業組織がこうした状況を打破するのに有効な取組み
- 国際標準(ISO/IEC 27014:2013 Governance of Information Security)が2015年7月にJIS化(JIS Q 27014)

経済産業省による
情報セキュリティガバナンスの定義

情報・ITに係るリスク管理を狙いとして、利害関係者から求められる情報セキュリティにかかわる意識や取組み、それに基づく業務活動を組織内に徹底させるための仕組み（**経営者が組織内の状況をモニタリングし方針を決定する仕組み及び市場に対する開示と市場による評価の仕組み**を指す）を構築・運用すること

（出典：経済産業省
「情報セキュリティガバナンス導入ガイダンス」，
2009/06）



情報セキュリティガバナンスのフレームワーク

（出典：経済産業省「情報セキュリティガバナンス導入ガイダンス」,2009/06をもとにISO/IEC 27014:2013 の内容を一部反映）

情報セキュリティガバナンス協議会について

■ 目的

日本企業は、今や深刻な経営課題となった情報リスクと対峙する必要に迫られています。しかし、対症療法的な対応ではなく、リスク管理の観点から情報リスクを適切に管理することが重要であり、そのためには、「情報セキュリティガバナンス」の確立が効果的です。情報セキュリティガバナンスは、経済産業省を中心に検討が進められ、現在、多くの組織で導入が試みられています。

その一方、情報セキュリティ責任者が「他社の事例を参考にしてレベルを上げていきたい」と考えても、そうした知見の共有は進みにくい状況にあります。自社の情報セキュリティの取り組みを組織外に対しては説明しづらいといった制約があるためです。そこで、協議会では、こうした課題を改善し、情報セキュリティガバナンスの普及啓発や導入支援をよりいっそう進め、企業自らが、情報リスクを適切に管理し、社会全体で見たセキュリティコストの抑制と、企業の国際競争力確保に寄与できる環境を実現することを目指します。

■ 設立

2012年5月21日

■ 役員等：

会　　長	土居　範久（慶應義塾大学　名誉教授）
幹事企業	株式会社ジェイティービー　　新日本有限責任監査法人 積水化学工業株式会社　　日本コムシス株式会社 株式会社三菱総合研究所
会計監査	丸山　満彦

協議会の活動と特徴

ISGA
Information Security Governance Association

■ 本協議会は、経営陣が情報リスクについて正しく理解し、組織として適切なリスク管理と情報セキュリティ対策を実施することをめざし、以下の事業に取り組みます。

①情報リスクの管理に関する知見の共有（会員向け事業）
- ベストプラクティスの共有（会員企業限定の意見交換 等）
- 会員向けセミナー / 勉強会の開催（有識者の講演、経済産業省との意見交換 等）

②情報セキュリティガバナンスに関する普及啓発
- 一般企業向けの啓発用情報の発信（HP、冊子、セミナー等）

③情報セキュリティガバナンス関連コンテンツの整備
- 情報セキュリティガバナンス関連の基準・ガイドライン等の策定・改訂等

■ 本協議会の特徴は、以下のとおりです。

【1】ユーザ企業主導
ユーザ企業の主導で、ユーザ企業によるユーザ企業のための活動を行います。

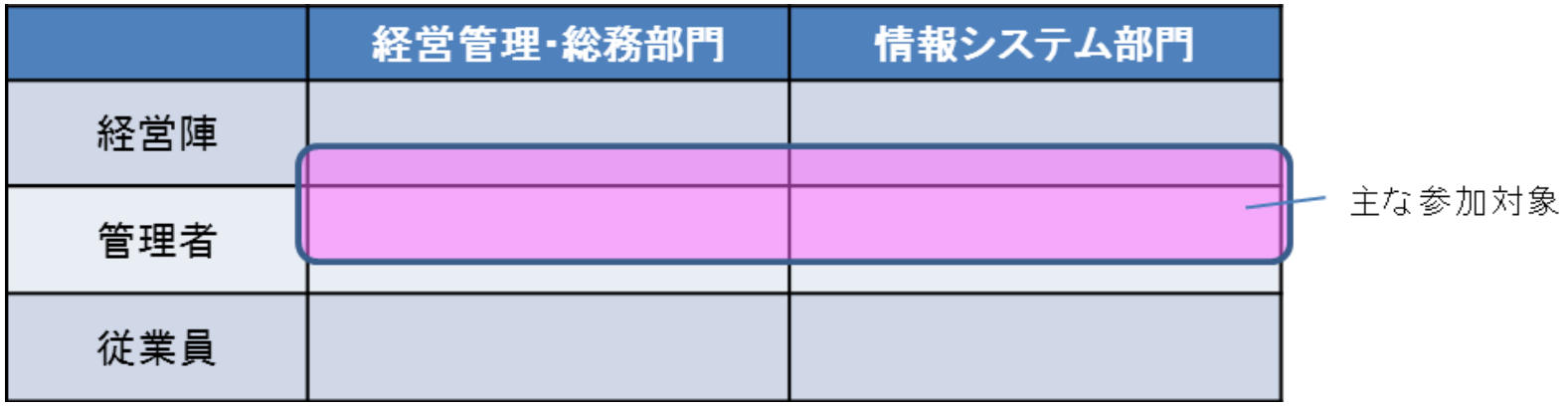
【2】経営的観点
情報リスクや情報セキュリティがテーマですが、主な論点として、技術や製品ではなく、経営の観点に沿った組織や統制、ガバナンス等のあり方を採り上げます。

【3】政府との連携
経済産業省とも連携し、情報セキュリティ政策の提言や支援に取り組みます。

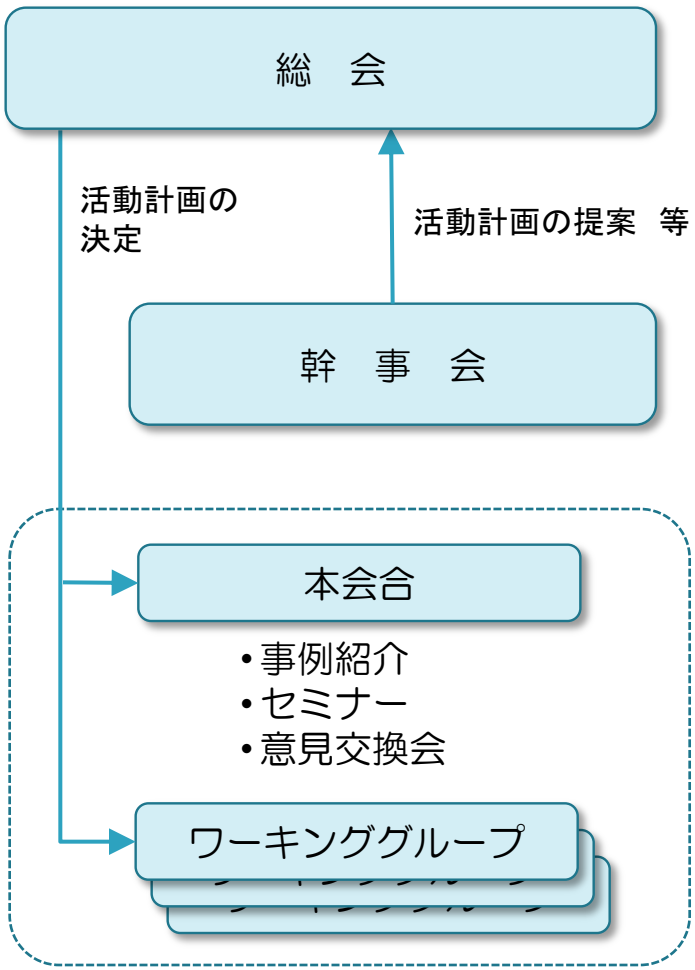
参加対象

■ 協議会では、ITセキュリティと情報管理の管理職の方を対象に、経営の観点に基づいた議論を行います。これは他の団体には見られない特徴です。

- 情報リスクに関する責任者の方 （CEO、CIO、CISO、CSO ）
- 情報システム部門の管理職の方 （ITセキュリティご担当）
- 経営管理部門・総務部門の管理職の方 （情報管理ご担当）



協議会の運営体制①



会　長

【会長の役割】

- 総会の議長
- メディア等への協議会の紹介

幹事会員

【幹事会員の役割】

- 幹事会・総会への参加
- 協議会の運営に関わる事項の協議
  - 規程の制定及び改正
  - 活動方針
  - 事業報告・会計報告
  - その他運営に必要な事項
- HP等での社名の公表
- 事務局業務

一般会員

【一般会員の役割】

- 総会への参加
- 事例紹介
- ワーキンググループ等の調査研究活動

協議会の運営体制②

会員等	概要	役割・責務
幹事会員	•協議会設立後に、協議会の経営を行う会員。 •協議会設立時の幹事会員は、発起人が就任する。 •また、新たな幹事会員は、幹事会員の推薦と幹事会の承認を経て追加する。	•幹事会・総会への参加 •協議会の運営に関わる事項の協議 - 規程の制定及び改正 - 活動方針 - 事業報告・会計報告 - その他運営に必要な事項 •HP等での社名の公表 •事務局業務
一般会員	•幹事会員以外の会員。 •加入申込書で申し込み後、幹事会の承認を受けて加入する。	•総会への参加 •事例紹介 •ワーキンググループ等の調査研究活動

協議会の運営体制③

入会申込書で選択

区分＼資格	ユーザ会員	ベンダ会員
幹事会員	【参加者の規定】 自組織もしくは自グループの情報セキュリティ管理に関する責任を担う者。 【協議会への貢献】 本協議会の会合において必要な場合、自組織もしくは自グループにおける情報セキュリティガバナンスの取組事例を、自らの事業に支障のない範囲で説明する。	【参加者の規定】 情報セキュリティに関する事業を担当する者、または、自組織もしくは自グループの情報セキュリティ管理に関する責任を担う者。 【協議会への貢献】 本協議会の会合において必要な場合、情報セキュリティガバナンスに関連する自らのツール・サービス、または情報セキュリティガバナンスの取組事例を可能な範囲で説明する。
一般会員		

会員企業等

■ 会員企業・団体

- EMCジャパン株式会社
- 株式会社 インフォセック
- グローバルセキュリティエキスパート株式会社
- 京王電鉄株式会社
- 株式会社ジェイティービー
- 清水建設株式会社
- 新日本有限責任監査法人
- 積水化学工業株式会社
- 石油資源開発株式会社
- 株式会社高島屋
- デロイトトーマツリスクサービス株式会社
- 日興アセットマネジメント株式会社
- 日本コムシス株式会社
- 日本たばこ産業株式会社
- 日本電気株式会社
- 富士ゼロックス株式会社
- 富士通株式会社
- 富士フィルム株式会社
- 株式会社三菱総合研究所
- 三菱電機インフォメーションネットワーク株式会社
- 持田製薬株式会社

■ オブザーバ

- 経済産業省

（2016/6/21現在）

2015年度の活動①全体会合

7/30　成果報告会／総会（第13回全体会合）
「セキュリティ保険のメリットと課題」
東京海上日動火災保険株式会社　企業商品業務部 商品開発担当　教学　大介　様
ワーキンググループ成果報告会
年度事業計画

9/18　第14回全体会合
「情報セキュリティの見える化に向けたIT活用 ～ GRCを活用した国内外事例紹介 ～」
デロイトトーマツリスクサービス株式会社　GRC推進担当マネジャー　渡部　豊　様
「情報セキュリティガバナンスの国際標準化 ～『JIS Q 27014:2015 情報セキュリティガバナンス』の解説 ～」
株式会社三菱総合研究所 社会ICT事業本部 サイバーセキュリティグループ　川口 修司

12/15　第15回全体会合
「「サイバーセキュリティ経営ガイドライン(案)」について」
経済産業省 商務情報政策局 情報セキュリティ政策室 室長補佐　山下　浩司　様
事例紹介：「富士ゼロックスにおける情報セキュリティガバナンスの取組み」
富士ゼロックス株式会社　総務部リスクマネジメントグループ グループ長　神林　彰　様
ワーキンググループ中間報告会

3/9　第16回全体会合
「ゲヒルンの診断事例から」
ゲヒルン株式会社　代表取締役　石森　大貴　様
ワーキンググループ最終報告会

2015年度の活動②WG

■ WG1：情報セキュリティ活動の見える化に関する検討

一般に、情報セキュリティ活動に関する明確な尺度がないため、組織の情報セキュリティ担当部門では、どのように情報セキュリティ活動の状況や課題を把握し、経営陣に報告するか、悩むケースが多いと考えられる。

2012年度は、事例分析等を通じて、測定項目や評価方法等の暫定案を策定するとともに、情報セキュリティ活動の見える化に関する事例を整理し、問題とその改善案をとりまとめた。その一方、経営陣がそもそも情報リスクや情報セキュリティ活動に関心が薄く、適切な評価がなされていない現状も指摘された。

これを受けて、2013年度はこうした状況を変える新たなアプローチとして、経営陣が最も関心を寄せる事項、すなわち経営目標や事業方針・計画等に必要な情報セキュリティの取組みに焦点を当て、情報リスクや必要な対策の見える化をめざし、モデルの具体化に取り組んだ。

さらに、2014年度は、これらの成果の整理と具体的な活用を目指して、2012年度の成果を活用したデータの整備と、2013年度の成果の発展（新たな業種でのモデルの策定）に取り組んだ。

本年度は、「現状」に関するセキュリティ評価と「将来（事業戦略・計画）」におけるセキュリティの導出モデルについて、さらなる発展・高度化をめざす。

■ WG２：内部犯行問題に関する検討

2014年に発覚した内部者による大量の個人情報漏えい事件を契機として、内部不正への対策が急務となっている。2014年度はIPAのガイドライン・チェックリストを基に、内部不正対策を議論し、現場でより活用しやすいチェックリストを作成した。本年度は、2014年度のWGで十分に検討できなかった項目について議論するとともに、新たな観点から内部不正対策を検討する。

- 多分野の理論やケーススタディを行い、内部不正対策に応用できる知見を検討して対策に反映
- 資料を基に内部不正対策への応用可能性を議論し、活用方策等を検討

お問い合わせ先

情報セキュリティガバナンス協議会　事務局
株式会社三菱総合研究所
社会ICT事業本部　サイバーセキュリティグループ　川口、綿谷

〒100-8141 東京都千代田区永田町二丁目１０番３号

電話 03-6705-6047　　FAX 03-5157-2195
E-mail　isga@mri.co.jp
http://www.isga.jp/

発行：2016年4月