ISGA
Information Security Governance Association

情報セキュリティガバナンス協議会
2015 年度　ワーキンググループ1
最終報告

情報セキュリティ活動の見える化に関する検討

目次

１．背景・目的

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。

そこで、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を見える化し、組織として適切に対応するため、経営陣、情報セキュリティ責任者及びスタッフ、現場の情報セキュリティ担当者のそれぞれに必要な行動や仕組みを具体化した。

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（アンケート調査）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、「経営を説得するための『見える化』」の実現策として、「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検討してきたが、これらの成果のさらなる発展・高度化をめざした。具体的には、過去3カ年のWGでの成果とそこから導出された検討課題を中心に、本年度の取組みを検討した。

2. 検討メンバー

株式会社 インフォセック	田中　洋
京王電鉄株式会社	細田　正実
石油資源開発株式会社	藤井　雅久
デロイト・トーマツ・リスクサービス株式会社	渡部　豊
富士ゼロックス株式会社	堀　　浩隆
富士通株式会社	西見　俊彦
株式会社三菱総合研究所	川口　修司
三菱電機インフォメーションネットワーク株式会社	昆　　資之
持田製薬株式会社	山野邊　渉

（社名：五十音順　氏名：敬称略）

（事務局）

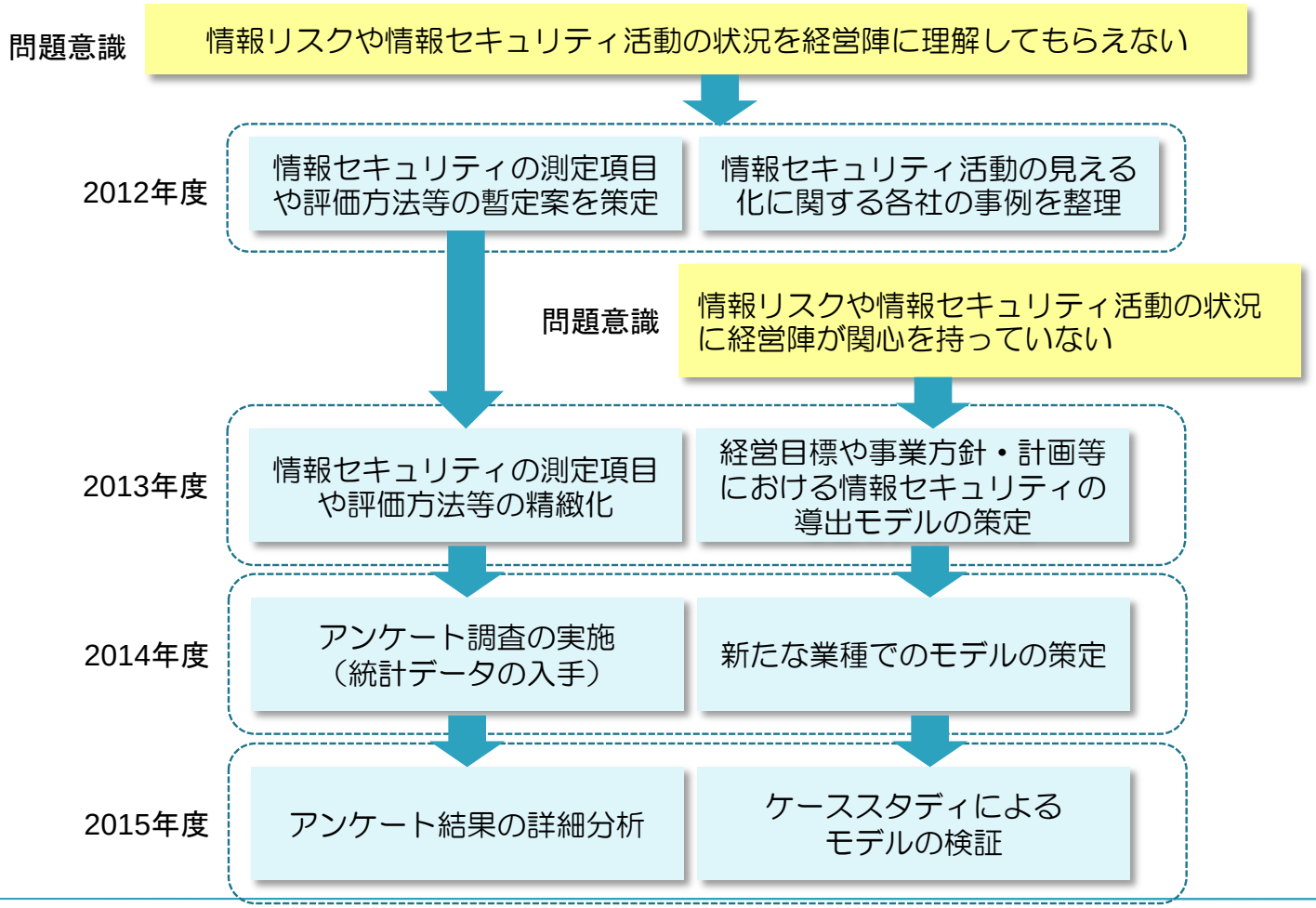
株式会社三菱総合研究所	綿谷　謙吾

３．2015年度の検討経緯

第１回	8／28（金）	キックオフ、論点整理	（三菱総合研究所）
第２回	9／15（火）	検討テーマに関する議論	（デロイト・トーマツ・リスクサービス）
第３回	10／22（木）	検討テーマに関する議論	（三菱総合研究所）
第４回	11／17（火）	分科会作業	（石油資源開発）
第５回	12／9（水）	分科会作業・中間報告準備	（インフォセック）
本会合	12／15（火）	本会合/中間報告	（三菱総合研究所）
第６回	1／19（火）	分科会作業	（MIND）
第７回	2／16（火）	分科会作業	（富士通）
合　宿	2／26（金）- 27（土）	分科会作業	
第８回	3／1（火）	最終報告書準備	（富士ゼロックス）
本会合	3／9（水）	本会合/最終報告	（三菱総合研究所）

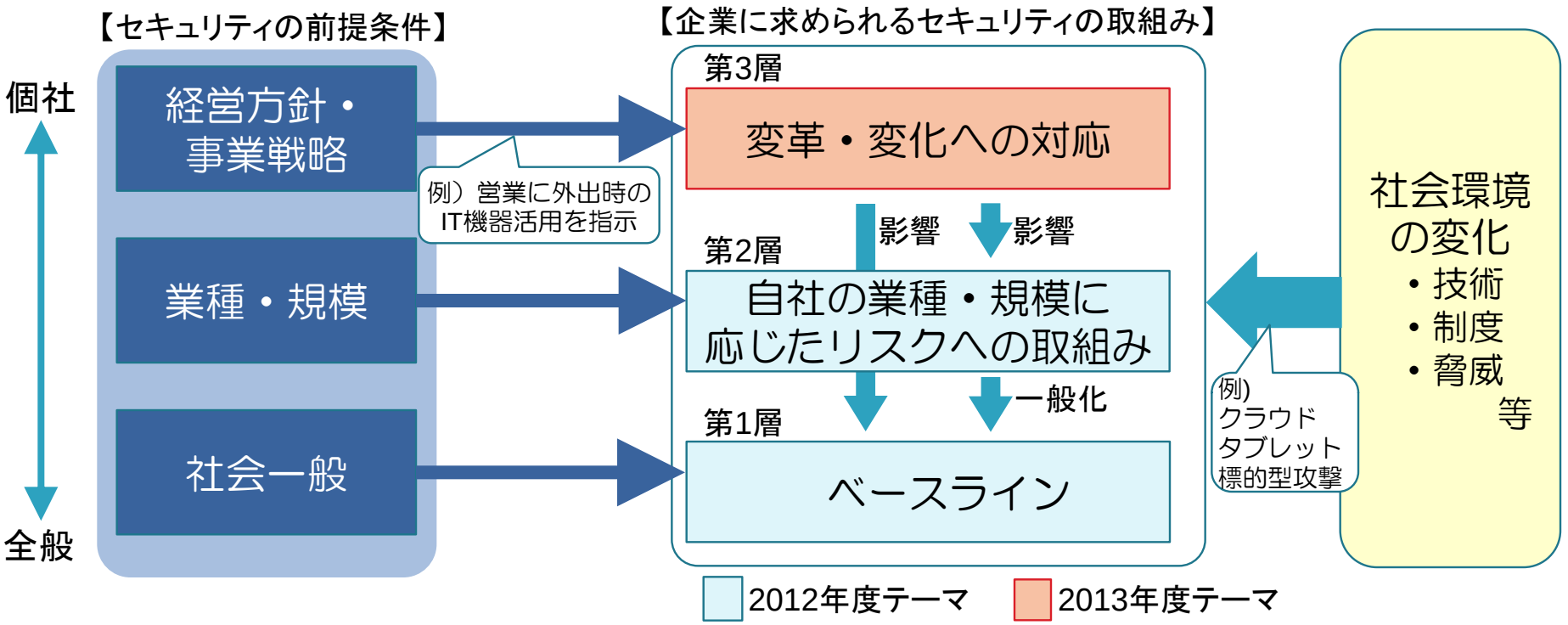
４. 取組みの概況

- 本WGの動機＝「セキュリティの現場と経営陣の認識のギャップを見える化で埋める」
- 本WGにおける検討の概況を以下に示す。



5. 基本的な考え方（仮説）

- 本検討では、企業に求められるセキュリティを3層構造で捉える。
  - **第1層：企業の属性によらず、ベースライン（常識）として取り組むべき対策**
  - **第2層：企業の業種や規模に応じて追加する対策**
  - **第3層：個社の方針や戦略に伴う変革・変化に対応するための対策**
- 社会環境の変化（技術・制度・人材の変化、脅威の多様化、影響の拡大等）はすべての層に作用する。
- 第1層、第2層は2012年度の成果、第3層は2013年度の成果によってモデル化している。

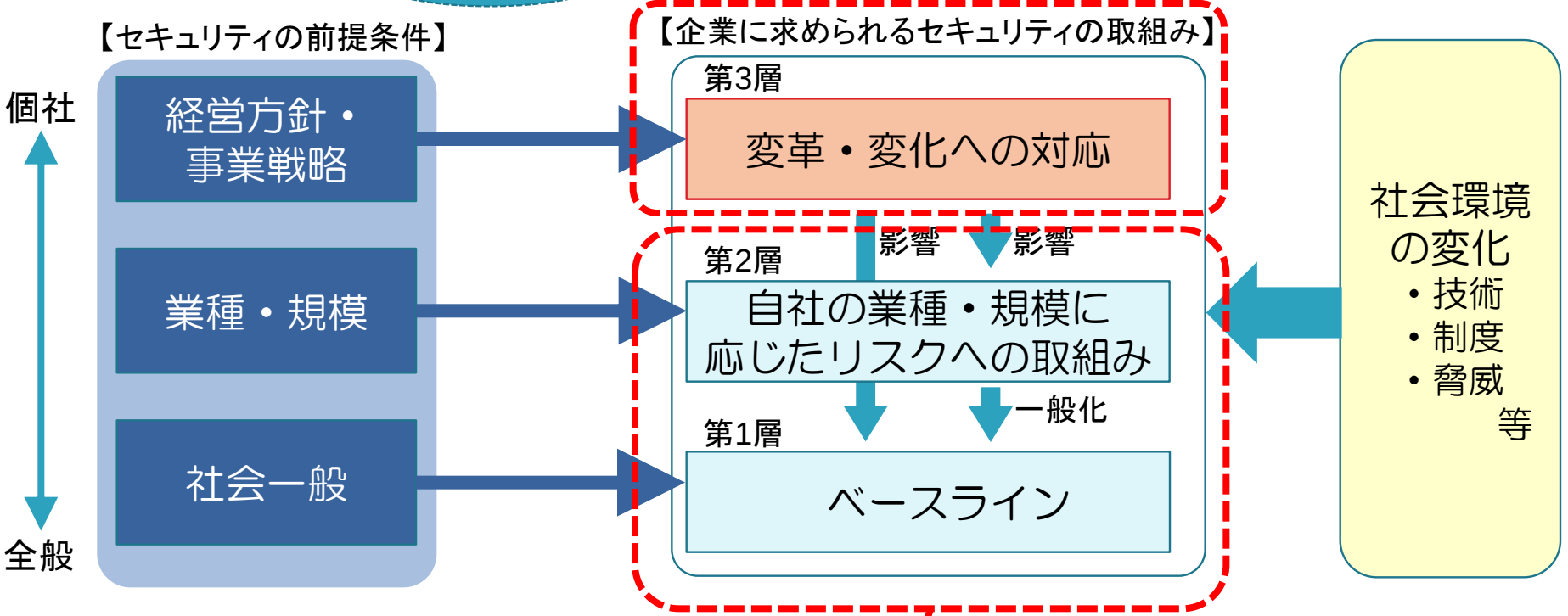


6. 検討方針

■ 2つのチームに分かれて検討を実施。

(2) 第3層の検証・精緻化：ケーススタディからモデルを検証
- 事例に基づいてフローモデルを改訂（精緻化、フィードバック）し、フローモデルを実現するためのポイントを分析

チームB



(1) 第1層・第2層の分析深化：調査データを有効活用
- 昨年度のWebアンケート調査項目を、脅威や技術の動向を踏まえた第１層の対策項目（必須）と、企業の業種や規模に応じて強化する第2層の対策項目に整理し、データを分析

チームA

7. 検討結果
(1) 第1層・第2層の分析深化
①活動の背景

Information Security Governance Association

■**背景**

- 情報セキュリティ対策の有効性の測定・評価に関する研究は数多く行なわれてきた。ただし、ユーザのニーズを満たす情報セキュリティ対策の評価に関する測定方法は確立されていない
  - ✓ 成熟度評価とは別に、対策の強度という観点で自社の取組が適切なのかを測る方法も必要
  - ✓ 必要とされる対策の強度　＝　リスクに対する対策の必要十分性

- 自社のセキュリティレベルをできるだけ客観的に評価できる手法がほしい
  - ✓　2012年度から、客観的かつ相対的に情報セキュリティレベルを評価できるようにするため、「情報セキュリティ対策評価ツール」を作成

- 自社データとの比較に用いる他社データの整備が必要
  - ✓　ISGA会員企業15社にアンケート調査を実施（大問42、小問252）。
  - ✓　一般企業に対するWebアンケート調査（80項目）を実施し、1000件超の比較対象となる他社データを集積（デロイトトーマツリスクサービス株式会社様のご協力）

- 情報セキュリティ対策必須項目、企業の業種や規模に応じて強化する対策項目など、企業にとって望ましい情報セキュリティ水準を示すことが出来ていない

7. 検討結果
(1) 第1層・第2層の分析深化
②活動の目的および2015年度ゴール

Information Security Governance Association

■**目的**

- 2012年度に作成した情報セキュリティ対策項目をあらためて整備し、2014年度にISGA会員企業およびWebアンケート調査で収集した対策実施状況のデータを分析し、有効活用できるようにする

✓ 情報セキュリティ対策実施状況を評価するツールの整備
「我が社の対策は一般的なレベルと較べてどうなんだ？」
「同業種・同規模の中ではどうなんだ？」

“企業セキュリティの3層構造”モデルの精緻化
第1層（ベースライン対策）・第2層（業種・規模に応じたリスク対策）とは、具体的には何なのか？

■**2015年度のゴール（目標）**

① 第１層・第２層の情報セキュリティ対策項目の分類

② 第２層の企業タイプ分類（どのような企業が何の対策を実施するか）および企業タイプ毎の望ましい対策水準の例示

7. 検討結果
(1) 第1層・第2層の分析深化
③活動計画

■ 2015年度活動内容およびスケジュール

I. 情報セキュリティ対策項目に対する、第1層・第2層に分類する考え方(基準)の明確化
[2015年9～10月]

II. 情報セキュリティ対策項目の第1層・第2層項目分類作業
[2015年11～12月]

III. 分類結果にもとづく業種別対策状況、リスクのタイプによる企業分類などの知見の導出
[2016年1～3月]

■ 分析対象データソース

- 情報セキュリティ対策項目（2012年度作成、2013年度更新。大問42＋小問252）
- ISGA会員企業アンケート調査データ（大問42＋小問252）
※今回分析に使用したデータは15社回答のうち従業員1000人以上の13社分のみを対象。
- 一般企業向けWebアンケート調査（小問のみ80項目）
※今回分析に使用したデータは、企業が特定されており重複を含まない従業員1000人以上規模のデータ262社分を抽出して分析。

■ 活動担当者（順不同、敬称略）

藤井　雅久（石油資源開発株式会社）、堀　　浩隆（富士ゼロックス株式会社）、
山野邊　渉（持田製薬株式会社）、田中　洋（株式会社 インフォセック）

7. 検討結果
(1) 第1層・第2層の分析深化
④活動結果

■ 2015年度活動実績

No.	タスク	活動実績
1	情報セキュリティ対策項目に対する、第1層・第2層に分類する考え方(基準)の明確化	WG1会合：10/22、11/17 臨時MTG：12/4
2	情報セキュリティ対策項目の第1層・第2層項目分類作業	WG1会合：12/09、1/19
3	分類結果にもとづく業種別対策状況、リスクのタイプによる企業分類などの知見の導出	WG1会合：2/16、3/01

■ 活動成果

a. 第1層・第2層分類基準の明確化
b. 第1層・第2層項目分類結果
c. 業種・規模別の対策実施率分析による知見（発見事項）

7. 検討結果
(1) 第1層・第2層の分析深化
⑤活動成果-1

a. 第1層・第2層分類基準の明確化

対策項目の実施率分析および個々の内容を吟味して、以下の分類基準を定義した。

- **第1層： 企業の属性によらず、ベースライン（常識）として取り組むべき対策**
  - ✓ 調査データ全体として実施率が非常に高い対策項目（例：アンチウィルス）

    [具体的分類基準]

    (1) 一般企業向けWebアンケート調査データ
    回答「1 ほぼ当てはまる」「2 一部当てはまる」の合計が90%以上の対策項目

    (2) ISGA会員企業アンケート調査データ（※Webアンケート調査データが無い対策項目）
    対策実施有無の回答「はい」が90%以上の対策項目
  - ✓ 情報セキュリティガバナンス上、最低限必須の対策項目（例：ポリシー策定）

    [具体的分類基準]

    対策内容が以下に当てはまる対策項目
    経産省・IPA「サイバーセキュリティ経営ガイドライン」にて経営者が指示すべき事項として明記されている対策項目。
    社内ルールを定めて周知すればよいだけの対策項目であり、かつセキュリティ上とくに重要性が高い項目か、費用や運用面で実施できない理由がない対策項目。
- **第2層： 企業の業種や規模に応じて追加する対策**
  - ✓ 業種・規模、または何らかの他の要因によって実施される対策項目

    [具体的分類基準]

    第1層の条件に当てはまらない対策項目はすべて、業種・規模または何らかの他の要因によって実施の有無が判断されていると考え第2層に分類した。

※なお第3層は、各社の経営方針・事業戦略に基づき決定される対策項目であるため、ここでの分類には含まない。（本報告書7(2)の検討対象）

7. 検討結果
(1) 第1層・第2層の分析深化
⑤活動成果-2

ISGA
Information Security Governance Association

b. 第1層・第2層項目分類結果

前頁の分類基準に基づき、大問42＋小問251*の計293項目を以下のとおり分類した。

* 質問項目のうち、セキュリティ対策ではなく、会社としての公式SNS利用有無を尋ねる小問1項目を除外した。

分類および判断基準	Webアンケート調査項目	ISGA会員調査項目	合計項目数	・項目例
第1層：ベースライン対策	**16**	**165**	**181**	
対策項目の実施率が非常に高い（90%以上）対策項目	10	160		・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5		・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	**64**	**48**	**112**	
全体的な業種別傾向（後述）による実施率の対策項目	12	—		・重要情報の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	—		・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	—		・ヒヤリハットの報告義務付け ・サーバ運用作業ログの記録
調査項目数合計	**80**	**213**	**293**	

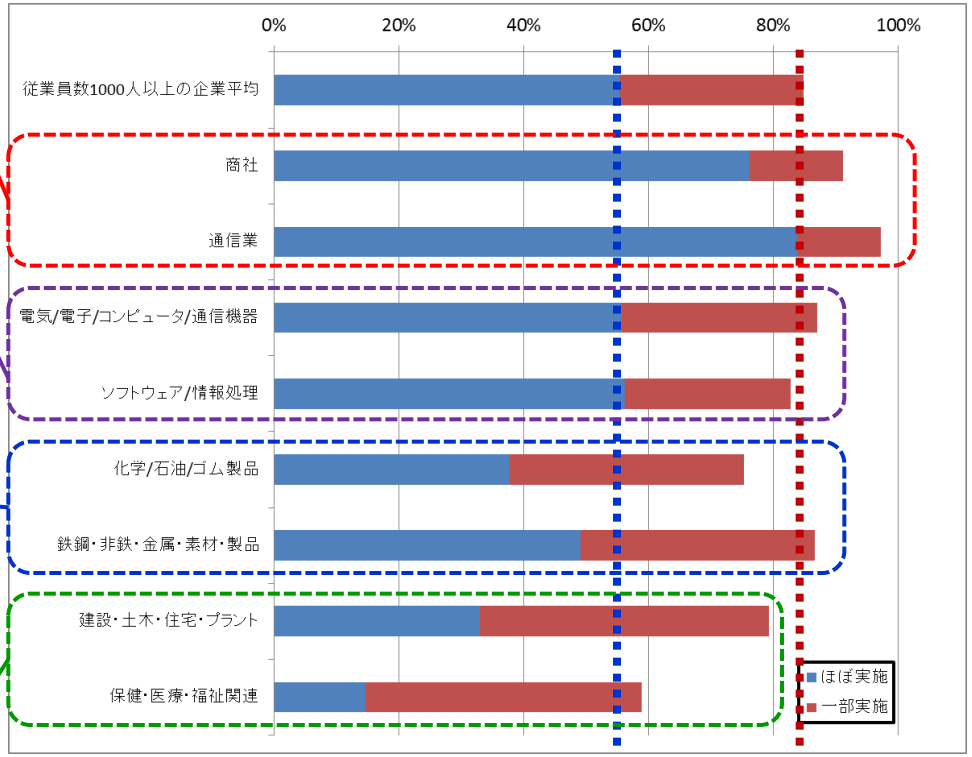
7. 検討結果
(1) 第1層・第2層の分析深化
⑤活動成果-3

c. 業種・規模別の対策実施率分析による知見(発見事項)

■ 業種別の対策実施率からの発見事項(1)

□ 業種別の対策実施率は、全体的に以下の傾向がある。

- 情報系業種:「商社」「通信業」
  ⇒対策実施率が高い
- 電子機器・コンピュータ系業種:
  「電気/電子/コンピュータ/通信機器」
  「ソフトウェア/情報処理」
  ⇒対策実施率が平均的
- 材料製造系業種:
  「化学/石油/ゴム製品」
  「鉄鋼・非鉄・金属・素材・製品」
  ⇒対策実施率が低い
- 現場系業種:
  「建設・土木・住宅・プラント」
  「保健・医療・福祉関連」
  ⇒対策実施率が低い



上図:全対策項目における業種別の
対策実施率の平均値

7. 検討結果
(1) 第1層・第2層の分析深化
⑤活動成果-3

ISGA
Information Security Governance Association

c. 業種・規模別の対策実施率分析による知見(発見事項) つづき

■業種別の対策実施率からの発見事項(1): 考察

- 情報系業種 : 「商社」 「通信業」 ⇒対策実施率が高い
  - 1000人以上の大企業ではM&A等インサイダー情報、通信の秘密など法規制対象の情報をもちコンプライアンスが重視されていると考えられる。

- 電子機器・コンピュータ系業種:「電気/電子/コンピュータ/通信機器」「ソフトウェア/情報処理」⇒対策実施率が平均的
  - 良い意味でも悪い意味でも「セキュリティ対策慣れ」しており、顧客・社会が期待する平均的な水準までの対策実施は積極的ながら、より高いレベルの自主的な取り組みは乏しいと考えられる。
  - 形式的にだけ対策を行い、実効性が空洞化するケースも考えられるため、継続的な水準向上が望まれる。

- 材料製造系業種:「化学/石油/ゴム製品」「鉄鋼・非鉄・金属・素材・製品」
  ⇒対策実施率が低い
  - これまでICT活用度があまり高くなかった材料製造系では、対策実施率が低いことは妥当と言える。
  - 今後は制御系システムへのサイバー攻撃に備える必要があり、意識の転換が必要。

- 現場系業種:「建設・土木・住宅・プラント」「保健・医療・福祉関連」⇒対策実施率が低い
  - 専門性の高い従業員が、現場での臨機応変な対応が求められる業種であり、一般的な企業と比較してユーザーの認証・アクセス制御等の対策が困難な場合もある(例えば救急医療の現場では、カルテ閲覧の度に桁数の多いパスワードを要求することはできない)。そのような場合はログ記録・モニタリングを強化することでリスクに対処可能。
  - また現場業務とは関係なく、きちんと実施できるはずの対策項目でも実施率が低い傾向にある(たとえばルール整備、サーバ管理、等)。これらの業種は、機微な個人情報や重要施設の設計情報などを扱うことが多い。また昨今は大規模ランサムウェア被害なども発生しており、困難だからと諦めずに出来る対策から実施していく事が望まれる。

7. 検討結果
(1) 第1層・第2層の分析深化
⑤活動成果-3

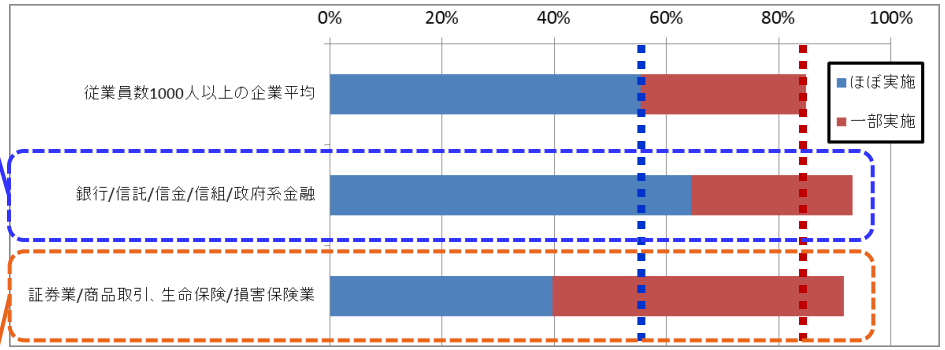
c. 業種・規模別の対策実施率分析による知見（発見事項） つづき

■ 業種別の対策実施率からの発見事項（2）

□ 金融系業種の対策実施傾向について

- 「銀行/信託/信金/信組/政府系金融」では、全業種平均と較べて、対策を「ほぼ実施」している割合が高い。
（金融庁管下での規制によると思われる。）

- 一方、「証券業/商品取引」および「生命保険/損害保険業」では、「一部実施」している対策は多い一方、「ほぼ実施」している対策は全業種平均よりも少ない



上図：全対策項目における金融系業種の対策実施率の平均値

考察：

- 好意的に解釈すれば「保護すべき対象を絞り込んで集中的に対策している」と言える。一方で「金融庁・証取委の検査対象となる部分のみ対策して、それ以外は手を抜いているのでは？」という懸念もある。
- 昨今の攻撃手法は「対策が弱い箇所での感染を足掛かりに、内部ネットワークに浸透して重要情報を入手する」というケースが増加。これらの金融系業種でも、社内ITインフラ全体としての対策強化が望まれる。

7. 検討結果
(1) 第1層・第2層の分析深化
⑤活動成果-3

c. 業種・規模別の対策実施率分析による知見（発見事項） つづき

■業種別の対策実施率からの発見事項（3）　※今後の要分析事項

□ そのほか、直感的推測とは異なる傾向として、以下のような発見が得られている。
これらの理由を探るために、今後より掘り下げた詳細分析をおこなうことで必要。

- 大部分の対策項目では、従業員規模の大きい企業ほど、対策の実施率が高い
ただし一部の項目（ヒヤリハット報告義務付け、等）で、1万人以上の大企業では実施率が下がる
- 一部の製造業（自動車/自動車部品、機械・機械部品・精密機械、等）で、全体的傾向とは別に、
特定の対策項目のみ実施率が高いケースあり
- 一部の業種（鉱業・電力・ガス/その他エネルギー、等）で、従業員規模の違いにより、対策実施率が
大きく異なるケースあり

7. 検討結果
(1) 第1層・第2層の分析深化
⑥今後の展望・課題

Information Security Governance Association

■ 現時点で見えている方向性:

- 今後、さらに掘り下げた分析を行うことにより、業種別・規模別での対策実施率の傾向について、さらに多くの知見を得られる見込みがある
- それらの知見を積み重ねて、企業の業種別・規模別で「一般的にどのような対策を行っているか」および「行うべきか」の答えに近づくことができるかもしれない

■ 検討を要する課題:

- 現状のアンケート回答データの限界
  - ✓ 業種を16種類に分類したが、対策実施率を決定づけるためには、より細分化した業種が必要である可能性が高い
  - ✓ 細分化した分析のために、さらに回答者数を増やす必要がある
  - ✓ 業種・規模以外の要因についても要調査
  - ✓ 回答者の主観判断であることは避けられない

  ⇒さらに費用をかけて追加データを取得するか。調査対象者である「大企業のセキュリティ担当者」は全体数が限られており、費用に見合う追加データが得られない可能性もある。調査方法自体を見直すことも考えるべき。
- 各社における情報セキュリティガバナンスの向上に役立つツールとして、どのような形をとるべきか。得られたデータや知見を、どのような形に整形するのがよいか。

7. 検討結果
(2) 第3層の検証・精緻化
①活動目的-1

■背景

- 近年、多くの日本企業において、以下に示すように情報セキュリティガバナンスを取り巻く変化は著しく変化しており、従来の情報セキュリティ対策だけでは不十分ではないかとの認識が高まっているものと考えられる

  企業の経営環境の変化：グローバル化・多角化などグループ経営への対応の要請　など

  情報技術活用の変化：クラウド活用、タブレット・スマートフォン、BYODの活用　など

- 一方で、多くの企業ではこれまでもJ-SOX（IT統制）やISMS、個人情報保護法対応等を行ってきたにもかかわらず、サイバーテロの顕在化など従来の対応だけでは捕捉しきれない多様化・複雑化した新たな情報セキュリティリスクが発生し、これらに対して十分に対応できているとはいいがたい状況となりつつあるといっても過言ではない
- しかしながら、このような状況の中で、従来の情報セキュリティへの取り組みだけでは
  ー経営陣や社内の理解を得ることが難しい
  ー必要な情報セキュリティ対策に十分な予算が確保されていない
  などの課題があり、新たな情報セキュリティリスクへの対応を含めた抜本的な対策が難しい状況にある
- 海外企業では、ガバナンス・リスク・コンプライアンス（GRC）というコンセプトに基づき、CISO（Chief Information Security Officer）が中心となって、情報セキュリティガバナンスを含むITリスク管理の抜本的な見直しが活発である

7. 検討結果
(2) 第3層の検証・精緻化
②活動経緯-1

■ ヒアリング結果

- 「第3層に対応している」とする大手サービス業C社にヒアリングを実施

情報セキュリティガバナンスを考える重要ポイント

ビジネスリスクの視点で情報セキュリティリスクを考える

ビジネスリスク

情報セキュリティリスク

意思決定	リスク管理委員会の形態
理解促進	委員会サポート組織
共通認識	情報セキュリティ目的
適切な報告	現場の管理態勢

7. 検討結果
(2) 第3層の検証・精緻化
②活動経緯-2

Information Security Governance Association

■ 検討の論点（C社へのヒアリング結果から導出）

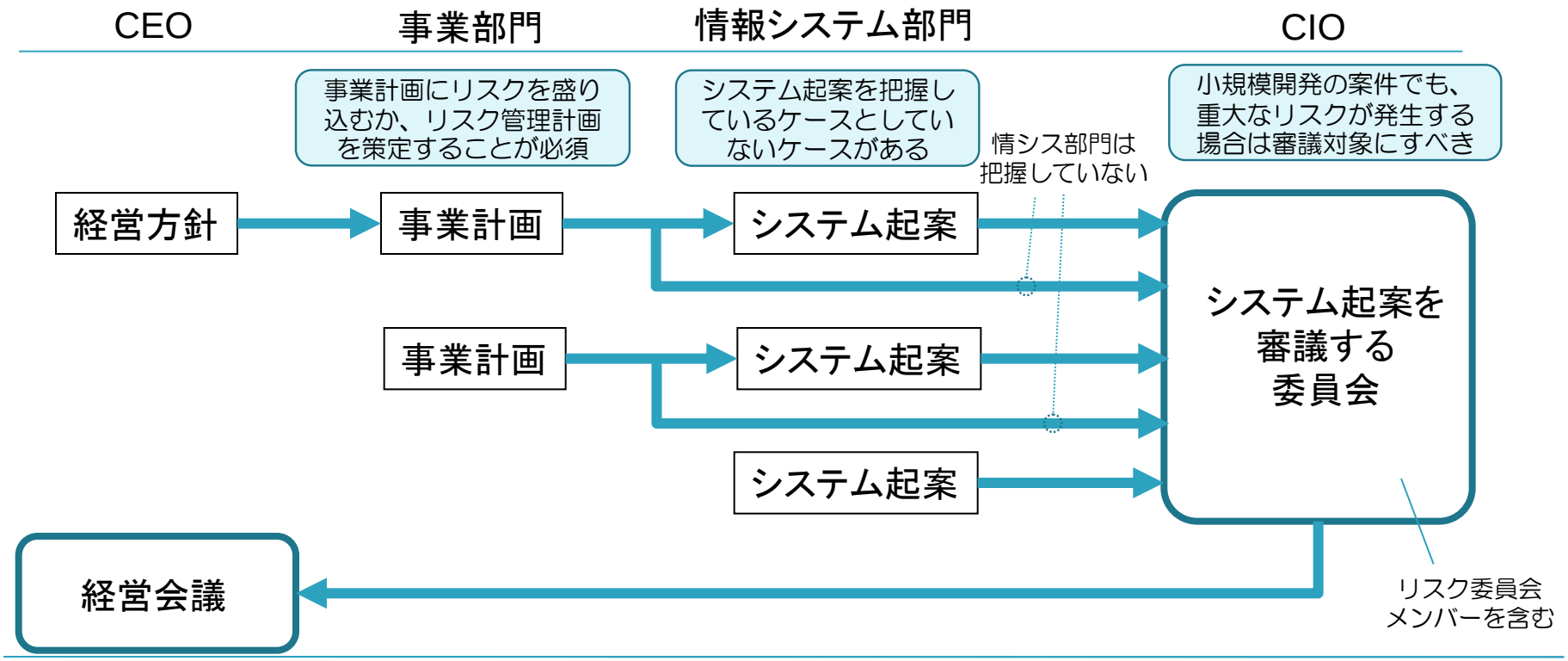
経営陣	自社のリスク管理委員会の形態	・座長はだれか ・委員会参加メンバーはだれか ・事務局はどこの部署か ・どのような内容が議論されているか	経営が継続的に関心を払う
管理組織	委員会サポート組織	・委員会をサポートする部署の有無、オーナーシップ ・サポート組織はどのような活動を実施しているか ・サポート組織から委員会に対してどのような報告をどれぐらいの頻度で実施しているか	経営をサポートできるメンバーアサイン（CISOなど）
ビジネスとセキュリティの関係	情報セキュリティ目的	・ビジネスリスクと情報セキュリティリスクが一体で検討されているか ・情報セキュリティについて、委員会・サポート組織でどのような議論が行われているか ・ビジネスリスクの一環として、情報セキュリティが現場に周知されているか	ビジネスリスクと一体でセキュリティリスクを検討する
現場	現場の管理態勢	・インシデント報告、対応はどのような内容で誰が・誰に報告しているか ・セキュリティインシデントの発生状況、フォローアップ状況が経営陣に報告されているか ・リスク洗い出しは現場で実施されているか	報告・フォローアップ態勢を確立する

7. 検討結果
(2) 第3層の検証・精緻化
③活動成果-1

ITリスク、情報セキュリティリスクを適切に経営が理解できる仕組みが必要

- C社の場合、システム起案を審議する委員会でフォローアップ
- 事業計画、リスクに対して各起案が妥当かどうかを審議する場として委員会を設置
- その際、セキュリティリスクについても検討することを要求、リスク委メンバーも参加
- CIOの役割が重要 - システム起案はすべてここを通る、ここを通らないと予算化されない
  - CIOがシステムの要否やリスクを適正に判断し、戦略的に投資する必要

CIOが適任でないと、仕組みが機能しないケースも



7. 検討結果
(2) 第3層の検証・精緻化
③活動成果-2

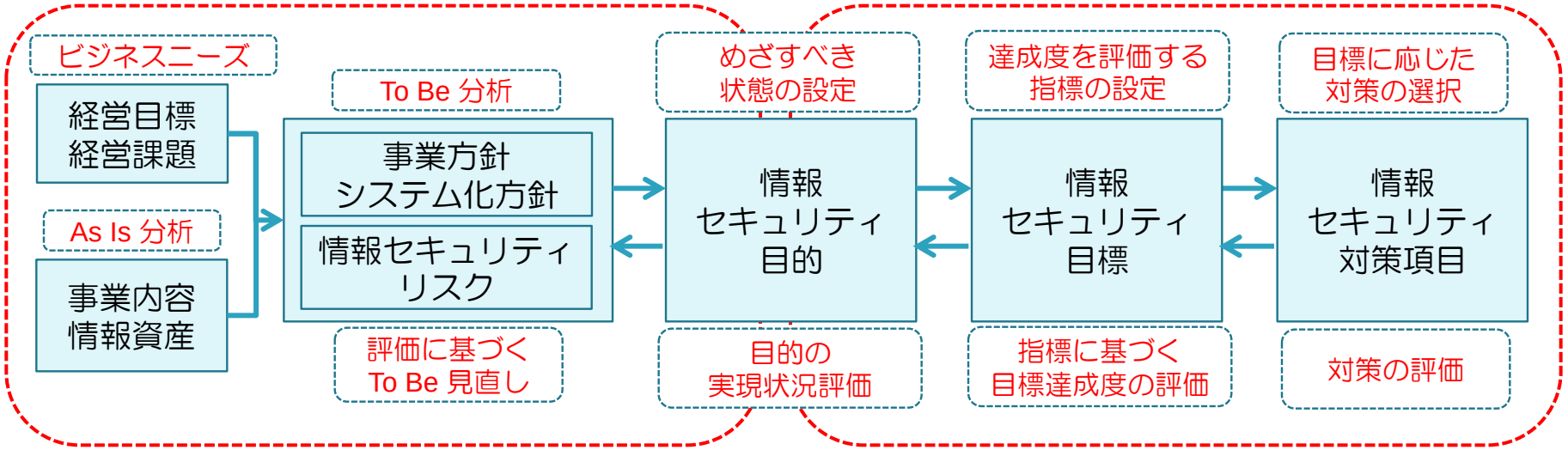
第3層を実装する上で、「変化」に対応し、情報セキュリティリスクを検討する仕組みが必要

- そのためには、システム起案を経営会議に出す前に、セキュリティリスクを審議する機能が不可欠
- C社の場合の機能：

  ①リスクマネジメントプロセス（全社のリスク洗出し → 重大リスク抽出）

  ②経営指示、起案 → 委員会（CIO）によるチェック → 経営会議

□ 情報セキュリティリスクのチェック



7. 検討結果
(2) 第3層の検証・精緻化
④結論と今後の課題

■ 第三層をうまく機能させるためのポイント

- CIOを設置・機能させること
  ← CEOの主導、人材確保、CIOのセキュリティ意識向上
- CIOがすべてのシステム起案について把握できること
  ← 予算、お墨付き等による権限確保
- CIOがシステム起案のセキュリティリスクについて議論できること
  ← CIOがセキュリティを理解している、もしくはCIOの周りにセキュリティをサポートする補佐(CISO)がいる
- 形骸化しないようにCEOが目を光らせること(内部監査活用も有効)

■ 実装を促す手段

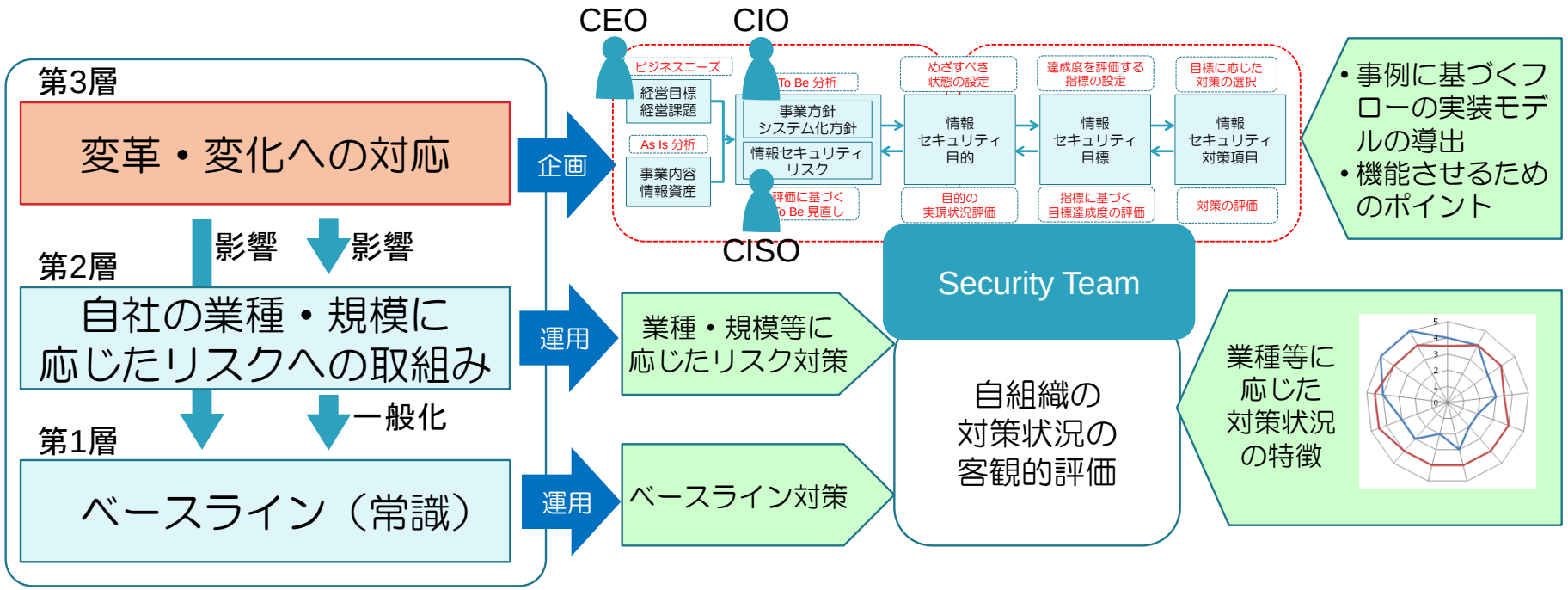
- 予算
- 人事・評価
- CEOからの指示(お墨付き、介在)
- 外圧(中央省庁、顧客、取引先、株主、社会等)
- 既存施策との融合(内部統制等)

今後の対応
情報システムを取り巻く各企業の現状を踏まえてモデルの汎用化、実現に向けた課題と対応策の提言が必要

8. まとめ

■ 三層モデルの捉え方：
- 第1層、第2層 ＝ 既存のセキュリティ対策の運用
- 第3層 ＝ IT企画案におけるセキュリティリスクへの対応（企画）
＜ ITガバナンスが機能していることが重要 ＞

■ 「①第1層、第2層の分析深化」「②第3層の検証・精緻化」を実施
- ① ⇒ 第1層、第2層の対策項目を分類し、業種等に応じた対策状況の特徴を抽出
- ② ⇒ 事例に基づき第3層（フロー）の実装モデルとそれを円滑に機能させるためのポイントを導出



ISGA
Information Security Governance Association

参考資料

2012年度の成果：評価方法

ISGA
Information Security Governance Association

41問

236問

【全体的な評価結果】

- 大問１問につき１～４点のスコアを付ける。
- 対策分野別に集計した平均得点〕を、レーダーチャート形式で図示する。
- 他社での平均得点を同様のレーダーチャートで図示し、これと自社の図とを比較する。

世間一般の対策状況とくらべて、対策が十分なのか／対策が不足しているのか／対策を実施しすぎなのか

【大問ごとの評価結果】

- 大問単位での回答（１～４点）を表またはグラフで図示する。また大問ごとに他社の平均得点を掲載し、自社の回答と比較できるようにする。
- 自社のリスク状況から見て、重点的に行うべき対策は強調する。

自社にとって特に重要な対策が他社平均に比べて不足していないか
自社にとって重要でない対策が他社平均よりも対策し過ぎていないか

【小問ごとの評価結果】

- 具体的に対策単位での実施状況を見るために、小問単位での対策実施有無の回答を整理する。
- 小問ごとに他社での実施率を併記する。

他社の多くで実施している対策と自社で実施済み対策とを比較

今後、評価事例が多数集まれば、業種別・企業規模別などにより、自社のリスクと似通った他社の対策状況と比較を行うことも可能

2012年度の成果：評価項目のイメージ

Information Security Governance Association

対策分野別に作成

【オフィスの入退管理】

大問１０．オフィス（建物・フロア・部屋）への防犯対策を実施していますか。

［ 選択肢 ］
- ほぼ実施済み　（８０～１００点のイメージ）
- 大部分は実施済み　（５０～７９点のイメージ）
- 大部分は未実施　（３０～４９点のイメージ）
- ほぼ未実施　（　０～２９点のイメージ）

小問１０－１．扉や窓は、開放時以外は施錠している　（はい／いいえ）

小問１０－２．入退出の記録をとっている　（はい／いいえ）

小問１０－３．部外者が入る際はバッジ等を着用させる　（はい／いいえ）

小問１０－４．接客等の区画ははっきり区別している　（はい／いいえ）

該当するリスク

【サーバ、ネットワーク】
- なし

【PC、モバイル機器、電子媒体、紙媒体】
- 第三者の不正な立ち入りによる持ち出し・盗難
- 第三者の盗み見
- 第三者が立ち入れる場所での端末、媒体の盗難
- 端末、媒体の不正な持ち出し

全体評価に活用
４段階評価

個別対策の進捗状況の比較に活用
１ or 0で回答

第1層・第2層項目分類結果
Webアンケート（1/8）

分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要情報の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

Webアンケート	分類	分類理由
会社全体の情報セキュリティの責任者を定めている	第１層	実施率が非常に高い（90%以上）
情報セキュリティの実作業を担う担当者が設置されている	第１層	実施率が非常に高い（90%以上）
情報セキュリティに関するリスク分析をして、対策の見直し等をしている	第１層	情報セキュリティガバナンス上、最低限必須
重要な情報について分類が定められている	第１層	実施率が非常に高い（90%以上）
重要度分類による情報の取り扱いルールが定められている	第１層	情報セキュリティガバナンス上、最低限必須
情報の取り扱いルールを従業員全員に教育している	第１層	実施率が非常に高い（90%以上）
重要な情報の保管場所には、一部の人しかアクセスできないようにしている	第１層	実施率が非常に高い（90%以上）
重要な情報（紙文書、データ等）を台帳・管理簿などの一覧にして、保管場所や管理責任者を記録している	第2層	業種・規模または何らかの他の要因による
重要な情報の紙文書やデータについて、定期的に棚卸しをしている	第2層	業種・規模または何らかの他の要因による
情報セキュリティに関する事故が発生した時に従業員が報告する連絡先が定められている	第１層	情報セキュリティガバナンス上、最低限必須
情報セキュリティに関する事故発生に至らなくても、事故が発生した恐れがあった場合（ヒヤリハット等）にも、従業員に報告させている	第2層	業種・規模または何らかの他の要因による
内部不正の有無を定期的にチェックしている	第2層	業種・規模または何らかの他の要因による
内部不正のチェック結果を経営陣に報告して、対策の見直し等をしている	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
Webアンケート（2/8）

分類および判断基準	Webアンケート調査項目(80)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要情報の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

Webアンケート	分類	分類理由
内部不正の疑いを発見した時に、匿名で通報できる窓口を設置している	第2層	業種・規模または何らかの他の要因による
内部不正を行った従業員の罰則が定められている	第１層	情報セキュリティガバナンス上、最低限必須
内部不正に対する方針や事例について、全従業員に教育を実施している	第2層	業種・規模または何らかの他の要因による
紙文書には重要度の分類が分かるようにしている	第2層	業種・規模または何らかの他の要因による
重要な情報を含む紙文書は、持ち出す時は管理責任者の許可を得る	第2層	業種・規模または何らかの他の要因による
重要な情報を含む紙文書は、配送する時は決められた方法に従う	第2層	業種・規模または何らかの他の要因による
利用者1人にIDを1つずつ割り当てている（IDは共有しない）	第１層	情報セキュリティガバナンス上、最低限必須
利用者のパスワードは、定期的に変更するよう、システムで強制している	第2層	業種・規模または何らかの他の要因による
利用者のパスワードは、英字・数字・記号を全て含むようシステムで制限している	第2層	業種・規模または何らかの他の要因による
利用者のパスワードは、7文字以上にするようシステムで制限している	第2層	業種・規模または何らかの他の要因による
過去4つ以上のパスワードと同じパスワードを使用できないようシステムで制限している	第2層	業種・規模または何らかの他の要因による
システムの画面を一定時間、操作しないで放置すると、再度パスワード入力が求められるようになっている	第2層	業種・規模または何らかの他の要因による
システムへのログイン試行は、一定回数以上できないようになっている	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果 Webアンケート（3/8）

分類および判断基準	Webアンケート調査項目(80)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

Webアンケート	分類	分類理由
データの改ざんが深刻な問題になるシステムでは、改ざんを検知する仕組みがある	第2層	業種・規模または何らかの他の要因による
インターネットからアクセス可能なシステムは、本番リリース前に脆弱性診断を行っている	第2層	業種・規模または何らかの他の要因による
社内からのみアクセス可能なシステムでも、特に重要なサーバーに対しては、脆弱性診断を行っている	第2層	業種・規模または何らかの他の要因による
運用作業は通常、決められた手順書にもとづいて実施する	第１層	情報セキュリティガバナンス上、最低限必須
運用作業のログは、システムで記録している	第2層	業種・規模または何らかの他の要因による
運用担当者による不正行為やミスを発見するために、運用作業のログは時々チェックされている	第2層	業種・規模または何らかの他の要因による
運用作業のログや記録は、改ざんできないように保管している	第2層	業種・規模または何らかの他の要因による
管理者の特権ID（Administrator権限、root権限）を使用する作業は常時監視し、不正行為を検知するようにしている	第2層	業種・規模または何らかの他の要因による
本番システムの変更は、決められた責任者の事前承認を得て実施する	第１層	情報セキュリティガバナンス上、最低限必須
本番システム変更作業のログは、システムで記録する	第2層	業種・規模または何らかの他の要因による
変更作業の担当者による不正行為やミスを発見するために、本番システム変更作業のログはチェックされる	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果 Webアンケート（4/8）

分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機密の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

Webアンケート	分類	分類理由
本番システム変更作業のログや記録は、改ざんできないように保管している	第2層	業種・規模または何らかの他の要因による
社内のネットワークの重要な結点（社内外の通信や重要サーバーへの通信が必ず通過する点）に、不正侵入検知／防止システム（IDS/IPS）を設置している	第2層	業種・規模または何らかの他の要因による
極めて厳しい機密管理を要する情報がある場合は、より厳しく通信を制限したネットワークセグメントでのみ取り扱っている	第2層	業種・規模または何らかの他の要因による
サーバーやシステムのアクセスログやイベントログを取得している	第2層	業種・規模または何らかの他の要因による
主要なネットワーク機器のアクセスログやイベントログを取得している	第2層	業種・規模または何らかの他の要因による
取得しているアクセスログ・イベントログ等を定期確認または常時監視している	第2層	業種・規模または何らかの他の要因による
アクセスログ・イベントログ等の監視システムまたはサービスを利用して、不正や異常を自動検知している	第2層	業種・規模または何らかの他の要因による
ファイアウォール、WAF、IDS/IPS等のログを常時監視し、不正アクセスの兆候を検知している	第2層	業種・規模または何らかの他の要因による
重要な情報を含む電子データは、ファイルサーバー等に保存する（PCに長期間保存しない）	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
Webアンケート（5/8）

分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

Webアンケート	分類	分類理由
重要な情報を保存したPC・電子媒体は、配送する時は決められた方法に従う	第2層	業種・規模または何らかの他の要因による
PCでの電子媒体への書き込みを、ルール上、禁止している	第2層	業種・規模または何らかの他の要因による
PCでの電子媒体の書き込みを、システム的に制限している	第2層	業種・規模または何らかの他の要因による
重要な情報を電子媒体に保存した場合、不要になり次第、データ消去や媒体廃棄をする	第2層	業種・規模または何らかの他の要因による
PCの操作ログを取得して、サーバーで保管するシステムを導入している	第2層	業種・規模または何らかの他の要因による
取得している操作ログを定期確認または常時監視している	第2層	業種・規模または何らかの他の要因による
社外へ持ち出すことがあるPCは、業務データをシステム的に自動でバックアップしている	第2層	業種・規模または何らかの他の要因による
PCのパスワードは、定期的に変更するよう、システムで強制している	第2層	業種・規模または何らかの他の要因による
PCのパスワードは、英字・数字・記号を全て含むようシステムで制限している	第2層	業種・規模または何らかの他の要因による
PCのパスワードは、7文字以上にするようシステムで制限している	第2層	業種・規模または何らかの他の要因による
過去4つ以上のパスワードと同じパスワードを使用できないようシステムで制限している	第2層	業種・規模または何らかの他の要因による
PCの管理者権限（Administorator権限）を、利用者には付与しない	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果 Webアンケート（6/8）

分類および判断基準	Webアンケート調査項目(60)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要情報の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

Webアンケート	分類	分類理由
業務で利用してよい携帯電話・スマートフォン・タブレットをルールで限定していますか	第１層	情報セキュリティガバナンス上、最低限必須
携帯電話・スマートフォン・タブレットには、紛失・盗難時の遠隔消去機能を設定する	第2層	業種・規模または何らかの他の要因による
携帯電話・スマートフォン・タブレットには、液晶画面の覗き見を防止するフィルター（プライバシーフィルター）を装着する	第2層	業種・規模または何らかの他の要因による
WindowsサーバーとPCすべてに、ウイルス対策ソフトをインストールしてウイルス定義ファイルを常時最新にしている	第１層	実施率が非常に高い（90%以上）
スマートフォン・タブレットには、ウイルス対策アプリをインストールする。またはウイルス対策アプリが不要な端末（iPhone/iPad）を利用する	第2層	業種・規模または何らかの他の要因による
社外とのメール送受信は、ネットワーク経路上でウイルスチェックされる	第１層	実施率が非常に高い（90%以上）
社内からインターネットのWebサイトへのアクセスは、ネットワーク経路上でウイルスチェックされる	第2層	業種・規模または何らかの他の要因による
PCでの電子媒体の読み取りを、システム的に制限している	第2層	業種・規模または何らかの他の要因による
重要な情報を取扱うサーバーやPCまたはネットワークに、未知のマルウェアを検知できる対策製品を導入している	第2層	業種・規模または何らかの他の要因による
PCのパッチ適用は、自動で実施している	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果 Webアンケート（7/8）

分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要情報の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

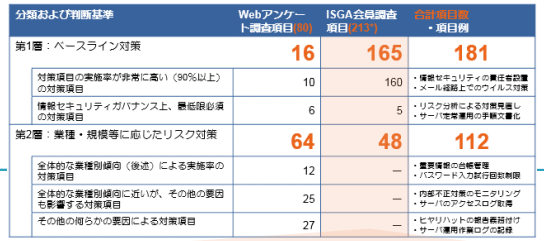
Webアンケート	分類	分類理由
会社のPCやスマートフォン・タブレットで使用する標準ソフトやアプリを定めている	第2層	業種・規模または何らかの他の要因による
利用者は標準以外のソフトやアプリを、勝手にインストールできないようになっている。または、勝手にインストールしたら管理者が必ず気付くようになっている	第2層	業種・規模または何らかの他の要因による
会社のPCやスマートフォン・タブレットで、本来使用が制限されている機能を使用させないようになっている。または、使用したら管理者が必ず気付くようになっている	第2層	業種・規模または何らかの他の要因による
PCからインターネット上のWebサイトへのアクセスは、フィルタリングしている	第2層	業種・規模または何らかの他の要因による
指定以外の電子メールソフトやウェブ上のメールサービスの利用は禁止している	第１層	実施率が非常に高い（90%以上）
業務内容を含む電子メールを、私物のメールアドレスへ転送することは禁止している	第2層	業種・規模または何らかの他の要因による
社外秘以上の情報を電子メールで社外に送信する際は、ファイルの暗号化やパスワード付与を行うルールとしている	第2層	業種・規模または何らかの他の要因による
社外秘以上の情報を電子メールで社外に送信する際に、ファイルの暗号化やパスワード付与を自動的に行う仕組みがある	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
Webアンケート（8/8）

分類および判断基準	Webアンケート調査項目(80)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要情報の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

Webアンケート	分類	分類理由
電子メールを社外に送信する際に、再確認を促すシステムがある	第2層	業種・規模または何らかの他の要因による
リモートアクセスの接続時にはID・パスワードのみではなく、2要素以上の認証方式を使用している	第2層	業種・規模または何らかの他の要因による
インターネットからアクセスできるWebサイトを持っている場合、重要な情報（ID・パスワード、顧客の個人情報、等）の送受信は、暗号化通信（HTTPS）で行っている	第2層	業種・規模または何らかの他の要因による
社内の通信であっても、ID・パスワード等の重要な情報の送受信は、暗号化通信で行っている	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
ISGA会員調査（1/22）

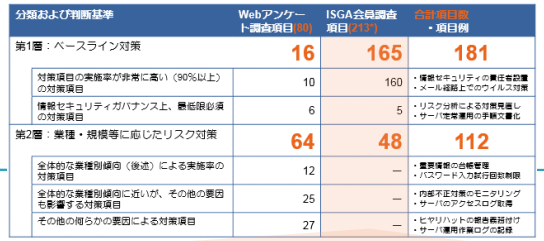


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機密の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書作成 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
情報セキュリティに関する方針または規定を定めていますか。	第１層	実施率が非常に高い（90%以上）
会社として情報セキュリティの取り組み方針または基本となる規定を文書化し、社内に周知していますか。	第１層	実施率が非常に高い（90%以上）
方針または規定に即して情報セキュリティ対策が行われていますか。	第１層	実施率が非常に高い（90%以上）
定期的または状況の変化に応じて、方針または規定を見直していますか。	第１層	実施率が非常に高い（90%以上）
従業員が業務において順守すべき、情報セキュリティに関する実施事項や禁止事項を文書化し、社内に周知していますか。	第１層	実施率が非常に高い（90%以上）
会社として情報セキュリティの構築や推進を行う体制がありますか。	第１層	実施率が非常に高い（90%以上）
会社として守るべき情報を明確にしていますか。	第１層	情報セキュリティガバナンス上、最低限必須
情報セキュリティ対策の実施状況のチェックを行っていますか。	第１層	実施率が非常に高い（90%以上）
情報セキュリティに関する自己点検を行っていますか。（部門部署毎/個人毎の実施単位を問いません）	第１層	実施率が非常に高い（90%以上）
情報セキュリティに関する内部監査を行っていますか。（業務監査等において同様の内容を実施している場合も含みます）	第１層	実施率が非常に高い（90%以上）
内部監査の結果、発見された不備の改善を行っていますか。	第１層	実施率が非常に高い（90%以上）
法令順守のための体制がありますか。	第１層	実施率が非常に高い（90%以上）
会社の業務に関係する情報セキュリティ関連の法令を把握し、管理していますか。（例：不正アクセス禁止法・不正競争防止法・刑法（ウイルス作成罪）、その他業種特有の法令）	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（2/22）

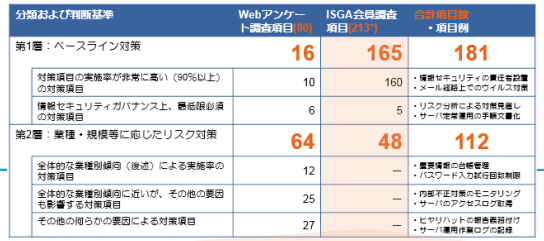


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
定期的または時宜に応じて、関連する法令の新規制定・改正・廃止等の変化を確認していますか。	第１層	実施率が非常に高い（90%以上）
関連法令の確認の結果、変化がある場合には、社内の規定やルールにその内容を反映していますか。	第１層	実施率が非常に高い（90%以上）
個人情報を保護するための体制がありますか。	第１層	実施率が非常に高い（90%以上）
個人情報保護の方針または規定を文書化し、社内に周知していますか。	第１層	実施率が非常に高い（90%以上）
個人情報の取り扱いについてのルールを文書化し、社内に周知していますか。	第１層	実施率が非常に高い（90%以上）
個人情報管理の責任部門を定めていますか。	第１層	実施率が非常に高い（90%以上）
外部の業務委託先との契約に際して、情報セキュリティに関する事項を契約に含めていますか。	第１層	実施率が非常に高い（90%以上）
業務委託先の選定にあたり、ISO/IEC27001・プライバシーマークの認証を取得していること等、委託先の情報セキュリティの水準を考慮していますか。	第１層	情報セキュリティガバナンス上、最低限必須
業務委託先とは守秘義務契約を交わしていますか。（交わしていない場合、業務委託契約に守秘義務条項を含んでいますか。）	第１層	実施率が非常に高い（90%以上）
必要な委託先に対して、情報セキュリティ対策の実施状況を確認するルールを規定していますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（3/22）



分類および判断基準	Webアンケート調査項目(80)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機密の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
情報セキュリティ事件・事故が発生した場合の対応体制がありますか。	第１層	実施率が非常に高い（90%以上）
情報セキュリティ事件・事故の種類に応じて、対応部門・担当を定めていますか。	第１層	実施率が非常に高い（90%以上）
情報セキュリティ事件・事故発生の連絡を受けて、対応する際の手順および報告・連絡先を定めていますか。	第１層	実施率が非常に高い（90%以上）
情報セキュリティ事件・事故の対応後、教育コンテンツや社内通知等を通じて、情報セキュリティ事件・事故の内容や対応策の内容等を社内に周知し、類似の事件・事故が再発することを防止する仕組みがありますか。	第１層	実施率が非常に高い（90%以上）
会社として有事の際の事業継続に関わる体制がありますか。	第１層	実施率が非常に高い（90%以上）
災害や事故等の予期せぬ出来事の発生に対して、定められた連絡体制や手続きを従業員や関係者に配付、あるいはシステムマニュアル等でいつでも確認できるようになっていますか。	第１層	情報セキュリティガバナンス上、最低限必須
予期せぬ出来事に対応する訓練を実施していますか。	第2層	業種・規模または何らかの他の要因による
定期的にまたは必要に応じて、連絡体制・手続き・システムマニュアルを見直していますか。	第１層	実施率が非常に高い（90%以上）
内部不正をリスクとして認識し、対策に取り組んでいますか。	第１層	実施率が非常に高い（90%以上）
従業員に、情報セキュリティ遵守を義務づけていますか。	第１層	実施率が非常に高い（90%以上）
全従業員（派遣、パート、アルバイトを含む）に対して、就業規則あるいは宣誓書により、会社の情報を無断で第三者に開示、漏えいすることのないよう守秘義務を課していますか。	第１層	実施率が非常に高い（90%以上）

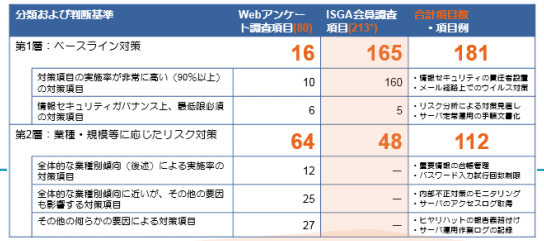
第1層・第2層項目分類結果
ISGA会員調査（4/22）

分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書類付け ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
従業員の入社時の教育に、情報セキュリティに関する内容を含めていますか。	第１層	実施率が非常に高い（90%以上）
全従業員に対して、定期的に情報セキュリティ教育を実施していますか。	第１層	実施率が非常に高い（90%以上）
従業員の退職・異動等の際には貸与した情報機器や鍵等の返却を確認していますか。	第１層	実施率が非常に高い（90%以上）
全従業員が個人的にソーシャルメディア（Facebook、Twitter、ブログ等）を利用する際のルールを定めていますか。	第2層	業種・規模または何らかの他の要因による
ソーシャルメディア（Facebook、Twitter、ブログ等）の個人利用について全従業員への教育・研修を行っていますか。	第2層	業種・規模または何らかの他の要因による
貴社が運営している公式のソーシャルメディア（Facebook、Twitter、ブログ等）に対する運用ルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
主要なオフィス（建物・フロア・部屋）すべてに、防犯対策を実施していますか。	第１層	実施率が非常に高い（90%以上）
オフィス内の外部に接する扉や窓は、開放時以外は施錠していますか。	第１層	実施率が非常に高い（90%以上）
接客や配達物の受け渡しを行う区画と、オフィス内の第三者が立ち入るべきでない区画とは、はっきり区別していますか。	第１層	実施率が非常に高い（90%以上）
オフィスへの入退出者を記録していますか。（例：カード式入退管理装置のログ、入退室記録簿等）	第2層	業種・規模または何らかの他の要因による
第三者がオフィスに入室する際には、勝手な行動を取ることができないようにする対策を実施していますか。（例：目に見える所にカード等の証明書を着用する、常時従業員が付き添う等）	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
ISGA会員調査（5/22）

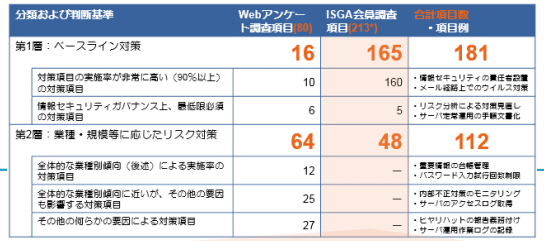


分類および判断基準		Webアンケート調査項目(60)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策		16	165	181
	対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
	情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策		64	48	112
	全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機密の台帳管理 ・パスワード入力試行回数制限
	全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
	その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
紙媒体の取り扱いルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
重要な情報を含む紙媒体の盗難防止策を講じていますか。（例：不使用時の施錠保管等）	第１層	実施率が非常に高い（90%以上）
重要な情報を含む紙媒体を廃棄する場合には、そのまま廃棄せず、情報を読み取ることができないような方法で廃棄していますか。（例：シュレッダーで裁断する、廃棄業者に溶解処理を依頼する、等）	第１層	実施率が非常に高い（90%以上）
重要な情報を含む紙媒体を廃棄業者に引き渡す場合は、廃棄証明書を受領していますか。	第１層	情報セキュリティガバナンス上、最低限必須
サーバーやネットワーク機器の設置場所（建物・部屋）に、防災対策を実施していますか。	第１層	実施率が非常に高い（90%以上）
建物・部屋の地震対策を実施していますか。（例：免震・耐震等）	第１層	実施率が非常に高い（90%以上）
サーバーラックやサーバー本体の転倒防止対策を実施していますか。（例：ボルト等による床への固定等）	第１層	実施率が非常に高い（90%以上）
建物・部屋の火災対策を実施していますか。（例：耐火、消火設備、火災・煙検知器等）	第１層	実施率が非常に高い（90%以上）
建物・部屋の水害対策を実施していますか。（例：防潮壁等）	第2層	業種・規模または何らかの他の要因による
サーバーやネットワーク機器を設置している場所（サーバールーム等）の温度および湿度を監視していますか。	第１層	実施率が非常に高い（90%以上）
停電時に正常にサーバーやネットワーク機器を停止するために、無停電電源装置（UPS）を設置していますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（6/22）

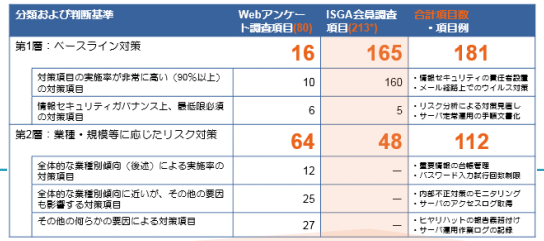


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機能セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
特にサービス停止の防止が厳しく要求される情報システムやネットワークを保有する場合、非常用発電機（自家発電装置）を設置していますか。	第１層	実施率が非常に高い（90%以上）
特にサービス停止・通信途絶等の防止が厳しく要求される情報システムやネットワークを保有する場合、通信経路の二重化等の対策を実施していますか。	第2層	業種・規模または何らかの他の要因による
サーバー設置場所（建物・部屋）への不正侵入対策を実施していますか。	第１層	実施率が非常に高い（90%以上）
サーバーはデータセンターに設置していますか。	第2層	業種・規模または何らかの他の要因による
サーバー設置場所の部屋への侵入者を検知する仕組みがありますか。（例：警報装置や警備員等）	第2層	業種・規模または何らかの他の要因による
サーバー設置場所の部屋へは、必要な要員以外が出入りできない仕組みがありますか。（例：暗証番号式あるいはカード式の入退管理装置、鍵による施錠等）	第１層	実施率が非常に高い（90%以上）
防犯カメラによって、サーバー設置場所の部屋への出入りまたは作業の様子を記録していますか。	第１層	実施率が非常に高い（90%以上）
定期的にまたは時宜に応じて、サーバー設置場所の部屋への入室権限を持つ要員を見直していますか。	第１層	実施率が非常に高い（90%以上）
サーバーをサーバーラックに設置し、施錠していますか。	第１層	実施率が非常に高い（90%以上）
システムのユーザーID・アクセス権を管理していますか。	第１層	実施率が非常に高い（90%以上）
利用者のID・アクセス権の付与・変更・削除を、正規の権限者が承認する手続きが定められていますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（7/22）

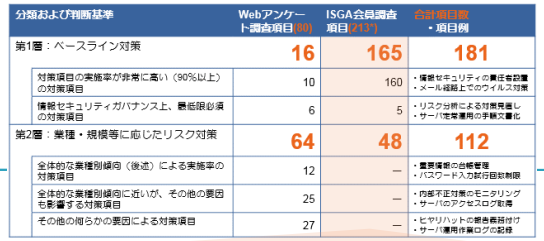


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機密の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
利用者のID・アクセス権に関して、従業員が一人で勝手に付与・変更・削除が行えない（または、行ったことを管理者が必ず気付く）ようになっていますか。	第１層	実施率が非常に高い（90%以上）
利用者の職務内容に応じて、必要最低限のアクセス権を付与するようになっていますか。	第１層	実施率が非常に高い（90%以上）
異動・退職等の理由で不要になった利用者のアクセス権は、ただちに変更・削除されるようになっていますか。	第１層	実施率が非常に高い（90%以上）
利用者のID・アクセス権を少なくとも1年に1回は見直して、異動・退職等の理由で不要になったものがあれば、変更または削除していますか。	第2層	業種・規模または何らかの他の要因による
利用者がシステムを使用する際、パスワード等による認証が必要ですか。	第１層	実施率が非常に高い（90%以上）
利用者のパスワードは、定期的に変更するルールとしていますか。	第１層	実施率が非常に高い（90%以上）
システムが稼働するサーバーのOSにログインできる人を制限していますか。	第１層	実施率が非常に高い（90%以上）
サーバーOSにログインする担当者１人に対してIDを１つずつ割り当てていますか。	第2層	業種・規模または何らかの他の要因による
担当者が共有するIDがある場合、誰がそのIDを利用したか特定することができますか。	第2層	業種・規模または何らかの他の要因による
担当者が共有するIDがある場合、担当者の異動・退職時に、ただちにパスワードを変更していますか。	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
ISGA会員調査（8/22）

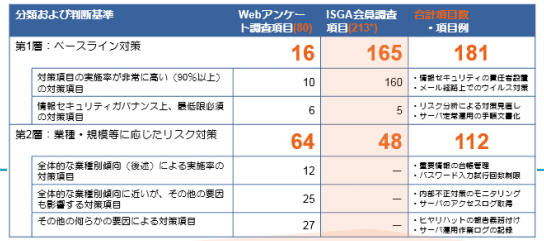


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策		16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機能セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策		64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
担当者のID・アクセス権の付与・変更・削除を、正規の権限者が承認する手続きが定められていますか。	第１層	実施率が非常に高い（90%以上）
担当者のID・アクセス権に関して、一人で勝手に付与・変更・削除が行えない（または、行ったことを管理者が必ず気付く）ようになっていますか。	第１層	実施率が非常に高い（90%以上）
特権（Administorator、root権限等）は、担当者の職務内容に応じて必要最低限の担当者だけに付与していますか。	第１層	実施率が非常に高い（90%以上）
1つのシステムにシステム管理者を複数配置し、情報システムの管理者IDごとに必要最低限の権限範囲の割り当てを行い、相互に監視できるようにしていますか？	第2層	業種・規模または何らかの他の要因による
異動・退職等の理由で不要になった担当者のアクセス権は、ただちに変更・削除されるようになっていますか。	第１層	実施率が非常に高い（90%以上）
担当者のID・アクセス権を少なくとも1年に1回は見直して、異動・退職等の理由で不要になったものがあれば、変更または削除していますか。	第2層	業種・規模または何らかの他の要因による
担当者がサーバーOSを操作する際、パスワード等による認証が必要ですか。	第１層	実施率が非常に高い（90%以上）
担当者のパスワードは、推測が容易でない一定以上の長さの文字列にするようシステム的に制限していますか。	第2層	業種・規模または何らかの他の要因による
サーバーOSの画面・コンソールは、操作がない状態が一定時間続いた場合、再度操作する時に、パスワード等の入力が求められるようになっていますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（9/22）

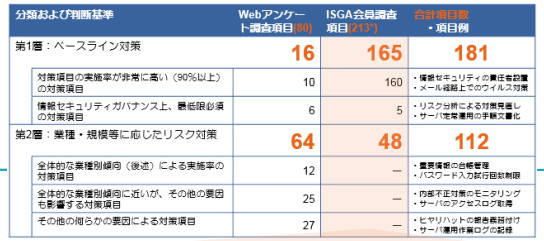


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機器セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
ID・パスワードの入力試行回数に制限を設けていますか。（例：IDを無効化する、一定時間の経過後に再度ログオンの試行ができるようにする等）	第2層	業種・規模または何らかの他の要因による
リモートアクセスにより担当者がサーバーOSにアクセスする場合、アクセス場所または情報機器等を制限する技術的手段を講じていますか。（例：コールバック、IPアドレスの制限、電子証明書、ワンタイムパスワード等）	第2層	業種・規模または何らかの他の要因による
重要なネットワーク機器（ファイアウォール、ルータ、スイッチ等）の設定画面にログインできる人を制限していますか。	第１層	実施率が非常に高い（90%以上）
ネットワーク機器の設定を変更できる権限は、担当者の職務内容に応じて必要最低限の担当者だけに付与していますか。	第１層	実施率が非常に高い（90%以上）
担当者がネットワーク機器の設定を変更する際、パスワード等による認証が必要ですか。	第１層	実施率が非常に高い（90%以上）
リモートアクセスにより担当者がネットワーク機器の設定を変更する場合、アクセス場所または機器等を制限する技術的手段を講じていますか。（例：コールバック、IPアドレスの制限、電子証明書、ワンタイムパスワード等）	第2層	業種・規模または何らかの他の要因による
サーバー構築時に要塞化に関する対策を実施していますか。	第１層	実施率が非常に高い（90%以上）
ベンダーが導入時に設定しているサーバーOSやパッケージソフトウェアのデフォルトIDを、無効化またはパスワード変更していますか。	第１層	実施率が非常に高い（90%以上）
サーバーOSのサービスやプロトコルのうち、システムの要件上、必要のないものを無効化していますか。	第１層	実施率が非常に高い（90%以上）

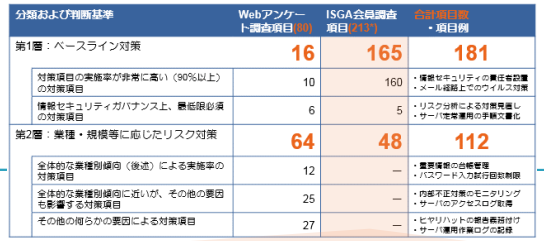
第1層・第2層項目分類結果
ISGA会員調査（10/22）



分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策		16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策		64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA会員調査	分類	分類理由
インターネットからアクセスできる重要なサーバーに対して、そのアクセス経路上にウェブアプリケーションファイアウォール（WAF）またはIDS/IPS等を設けていますか。	第2層	業種・規模または何らかの他の要因による
システムの脆弱性診断を実施していますか。	第１層	実施率が非常に高い（90%以上）
インターネットからアクセス可能なサーバーに対して、定期的にまたは時宜に応じて脆弱性診断を行っていますか。	第１層	実施率が非常に高い（90%以上）
システムの開発・導入および運用に関するルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
システムの開発・導入および運用の際に考慮すべきセキュリティ要件についてのルールを文書化していますか。（例：アクセス制御、バックアップ、ウイルス対策等）	第2層	業種・規模または何らかの他の要因による
個々のシステム開発・導入における要件定義の段階で、システムに必要なセキュリティ要件を定めていますか。	第2層	業種・規模または何らかの他の要因による
個々のシステム開発・導入における要件定義、設計・開発・導入、テストの各段階で文書を作成し、最新版を保管していますか。 (例：システム要件定義書、システム仕様書/設計書、テスト手順/結果、プログラムソースコード、パラメーター設定一覧等)	第2層	業種・規模または何らかの他の要因による
定めたセキュリティ要件通りに運用していることを確認していますか。（例：アクセス権限の棚卸、バックアップの保管状況、ウイルス対策状況等）	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
ISGA会員調査（11/22）

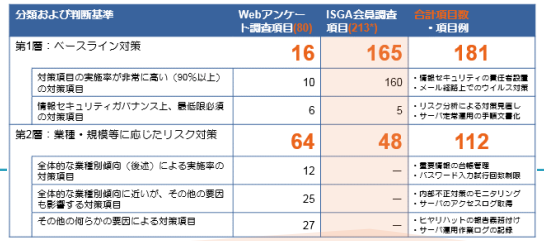


分類および判断基準	Webアンケート調査項目(80)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要情報の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
ウェブアプリケーションを開発する場合、脆弱性のあるアプリケーションを作らないよう、セキュアコーディングの基準に則った開発を開発者に行わせていますか。（例：SQLインジェクション・バッファオーバーフロー・クロスサイトスクリプティング・CSRF・アクセス制御の不備等の脆弱性を作り込まないプログラミング手法のIPA・OWASP・SANS等のガイド、開発ベンダー独自基準等）	第2層	業種・規模または何らかの他の要因による
会計系、金融系、電子商取引（BtoB/BtoC）、在庫管理等、不正やミスによる誤入力が深刻な問題になるシステムでは、利用者の入力値や処理結果の正しさを確認していますか。（例：入力値の桁数・範囲・文字種等のシステム的チェック、複数人による入力値のチェック、上長による結果の確認等）	第2層	業種・規模または何らかの他の要因による
サーバーやシステム、ネットワークの運用作業についてのルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
運用作業の実施を確認できる記録を作成していますか。（例：作業記録簿の記入、システム的なログ等）	第１層	実施率が非常に高い（90%以上）
運用作業に際して、開発担当者を運用環境にアクセスさせないようにしていますか。（例：システム的にアクセスを制限する、物理的に入室を制限する、アクセスするとログに記録が残る等）	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
ISGA会員調査（12/22）

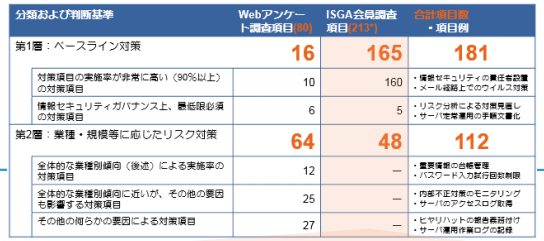


分類および判断基準	Webアンケート調査項目(80)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機器セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
サーバーやシステム、ネットワークの変更作業を行う際の手続きを定めていますか。	第１層	実施率が非常に高い（90%以上）
変更作業に係るテストを実施する際には、実データを使用しないようにしていますか。	第１層	実施率が非常に高い（90%以上）
変更作業は、テスト済みの手順に基づいて実施していますか。 （例：テスト環境や開発環境でのテスト済みの手順、運用環境での実施実績のある手順等）	第１層	実施率が非常に高い（90%以上）
変更作業の事前承認、実際に行った作業、作業後の動作確認と結果について、変更管理の記録として保管していますか。	第１層	実施率が非常に高い（90%以上）
変更作業に際して、開発担当者を運用環境にアクセスさせないようにしていますか。（例：システム的にアクセスを制限する、物理的に入室を制限する、アクセスするとログに記録が残る等）	第2層	業種・規模または何らかの他の要因による
システム障害の予防・復旧対策を実施していますか。	第１層	実施率が非常に高い（90%以上）
システム障害が発生した場合の調査・対応手順を定めていますか。	第１層	実施率が非常に高い（90%以上）
障害時の影響が大きいシステムは、必要な時間内に復旧できるよう、機器の冗長構成または代替機器の準備をしていますか。	第１層	実施率が非常に高い（90%以上）
障害時の影響が大きいシステムは、機器を定期的に点検・保守していますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（13/22）

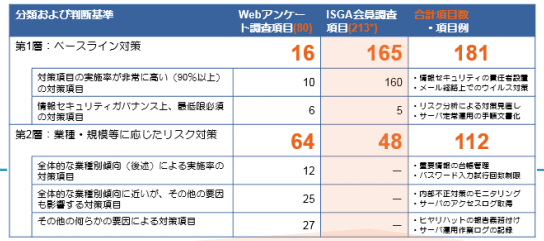


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
データのバックアップを取得していますか。	第１層	実施率が非常に高い（90%以上）
システム障害・災害等に備えて、システムや業務データの復旧に必要なバックアップデータを十分な頻度で取得していますか。	第１層	実施率が非常に高い（90%以上）
システムや業務データが復旧できるよう、リカバリの手順を文書化し、システムに変更があれば反映していますか。	第１層	実施率が非常に高い（90%以上）
文書化したリカバリ手順は、実機でテストしていますか。	第１層	実施率が非常に高い（90%以上）
サーバーやネットワーク機器の設定ファイルのバックアップを定期的に取得していますか。	第１層	実施率が非常に高い（90%以上）
特に喪失すると致命的な影響があるデータは、バックアップの記録媒体を遠隔地に設置または保管していますか。	第１層	実施率が非常に高い（90%以上）
社内のネットワーク図およびネットワークに接続する情報機器の一覧（PC、サーバー、ネットワーク 情報機器）を作成していますか。	第１層	実施率が非常に高い（90%以上）
社内のネットワークに接続する情報機器の導入・変更・廃止の手続きが定められていますか。	第１層	実施率が非常に高い（90%以上）
社内のネットワークに新たな情報機器を接続する際に、会社として求めるセキュリティ対策を定めていますか。（例：ウイルス対策、セキュリティパッチの適用等）	第１層	実施率が非常に高い（90%以上）
許可を得ていない情報機器を社内のネットワークに接続した場合、技術的に検知する手段を講じていますか。（例：ウイルス対策・セキュリティパッチ未適用の情報機器の検出、MACアドレス・電子証明書などによる未許可の情報機器の特定等）	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
ISGA会員調査（14/22）

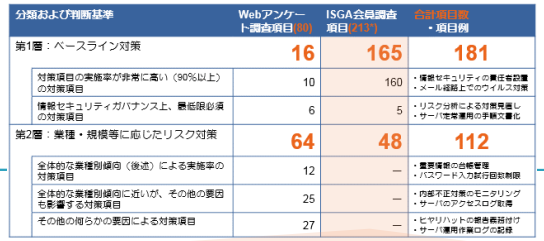


分類および判断基準		Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策		16	165	181
	対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・境界セキュリティの責任者設置 ・メール経路上でのウイルス対策
	情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策		64	48	112
	全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
	全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
	その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
社内のネットワークを複数のセグメントに分割していますか。	第１層	実施率が非常に高い（90%以上）
サーバーを設置するネットワークセグメントは、ファイアウォールやルータ等で通信を制限していますか。（例：通信元/先IPアドレス、ポート番号等）	第１層	実施率が非常に高い（90%以上）
インターネットからアクセス可能なサーバーがある場合は、社内ネットワークとは別のネットワークセグメント（DMZ）に設置していますか。	第１層	実施率が非常に高い（90%以上）
ソフトウェアについて、ベンダーとのサポート契約を結んでいますか。	第１層	実施率が非常に高い（90%以上）
PCによる社外との通信（電子メール、ウェブ閲覧、ファイル転送など）は、通信経路とポート番号をファイアウォールやルータ等で制限していますか。	第１層	実施率が非常に高い（90%以上）
ウイルス感染などの緊急時に、ネットワークを管理する担当者が社内のネットワークから個々のセグメントを物理的にまたは論理的に切り離せるようにしていますか。（例：物理的にルータやスイッチからケーブルを抜く、ネットワーク管理ツールより遠隔でVLANを切り離す等）	第１層	実施率が非常に高い（90%以上）
ファイアウォールやルータ等によるアクセス制御ルールの登録・変更・削除の手続きを定めていますか。	第１層	実施率が非常に高い（90%以上）
ファイアウォールやルータ等によるアクセス制御ルールに、不備や更新漏れがないか定期的に見直しを実施していますか。	第2層	業種・規模または何らかの他の要因による
サーバーやシステム、ネットワークの稼働状況を監視またはチェックしていますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（15/22）

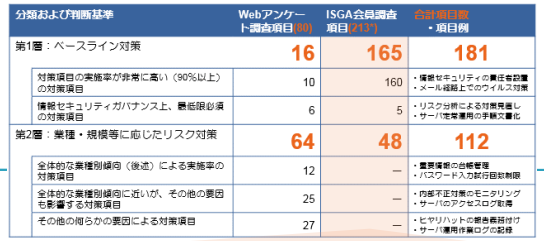


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機能セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
サーバーやシステムの稼働状況を監視またはチェックするルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
ネットワークの稼働状況を監視またはチェックするルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
サーバーやシステムに障害や遅延・停止などが発生した場合に、被害が大きくなる前に気付くことができる仕組みがありますか。（例：死活監視、ログ監視、利用者からの報告等）	第１層	実施率が非常に高い（90%以上）
ネットワークに障害や遅延・停止などが発生した場合に、被害が大きくなる前に気付くことができる仕組みがありますか。（例：障害監視、利用者からの報告等）	第１層	実施率が非常に高い（90%以上）
サーバーやシステムのリソースに関して、監視する項目を定めていますか。（例：CPU使用率、メモリー使用量、ディスク容量等）	第１層	実施率が非常に高い（90%以上）
サーバーやシステムのリソースの使用状況が事前に定めた閾（しきい）値を超えた場合に、自動的に通知する仕組みがありますか。	第１層	実施率が非常に高い（90%以上）
社内のネットワークの帯域使用状況に関して、把握する方法を定めていますか 。（例：常時監視、週次・月次等での定期的なチェック等）	第１層	実施率が非常に高い（90%以上）
社内のネットワークの帯域使用量が事前に定めた閾（しきい）値を超えた場合に、自動的に通知する仕組みがありますか 。	第2層	業種・規模または何らかの他の要因による
サーバーやシステム、ネットワークのログを取得していますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（16/22）

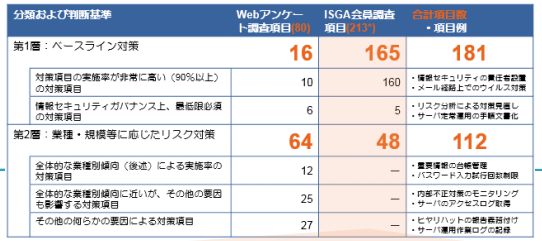


分類および判断基準	Webアンケート調査項目(80)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策		16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策		64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
PCで外部とメールを送受信する時に、メールサーバーでログを取得していますか。	第１層	実施率が非常に高い（90%以上）
PCで社内から外部のウェブサイトにアクセスする時に、ネットワーク経路上でログを取得していますか。（例：プロキシサーバーのアクセスログなど）	第１層	実施率が非常に高い（90%以上）
アクセスログ・イベントログ等を、改ざん等から保護された安全な場所で保管していますか。	第2層	業種・規模または何らかの他の要因による
取得している各種ログの関連性を保持し、経緯を正確に追跡できるように、ログを取得するサーバーやネットワーク機器の時刻を同期していますか。	第１層	実施率が非常に高い（90%以上）
業務で利用するPCを管理していますか。	第１層	実施率が非常に高い（90%以上）
業務に利用してよいPCを規定するルールを定めていますか。（例：会社貸与PCのみとし私物利用を禁止、私物PCの利用を認める条件を規定等）	第１層	実施率が非常に高い（90%以上）
1台のPCは、1人の利用者に割り当てられていますか。	第2層	業種・規模または何らかの他の要因による
複数の利用者で共有するPCがある場合、誰がそのPCを利用したか特定することができますか。	第１層	実施率が非常に高い（90%以上）
複数の利用者で共有するPCがある場合、担当者が変わった時に、ただちにパスワードを変更していますか。	第１層	実施率が非常に高い（90%以上）
利用者へのPCの貸与・利用者変更・返却の手続きが定められていますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（17/22）

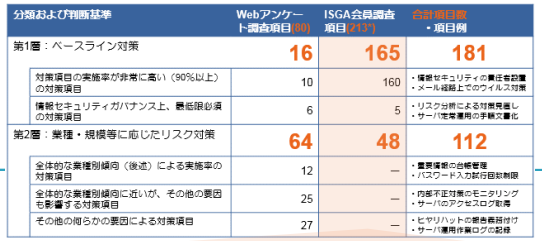


分類および判断基準	Webアンケート調査項目(80)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
異動・退職等の理由で不要になったPCは、ただちに返却されるようになっていますか。	第１層	実施率が非常に高い（90%以上）
社内のPCの利用者を少なくとも1年に1回は見直して、異動・退職等の理由で不要になったものがあれば、返却させていますか。	第１層	実施率が非常に高い（90%以上）
業務で利用する電子媒体を管理していますか。	第１層	実施率が非常に高い（90%以上）
業務に利用してよい電子媒体のルールを定めていますか。（例：会社貸与の電子媒体のみとし私物利用を禁止、私物電子媒体を利用してよい条件を規定等）	第１層	実施率が非常に高い（90%以上）
会社が貸与する電子媒体の貸与・利用者変更・返却の手続きを定めていますか。	第１層	実施率が非常に高い（90%以上）
異動・退職等の理由で不要になった電子媒体は、ただちに返却されるようになっていますか。	第１層	情報セキュリティガバナンス上、最低限必須
社内の電子媒体の利用者を少なくとも1年に1回は見直して、異動・退職等の理由で不要になったものがあれば、返却させていますか。	第１層	実施率が非常に高い（90%以上）
会社が貸与する電子媒体を、パスワード等で保護していますか。	第１層	実施率が非常に高い（90%以上）
PCおよび電子媒体を利用する際の取り扱いルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
ノートPCの盗難防止策を講じていますか。（例：セキュリティワイヤーの使用、離席・退社時の施錠保管等）	第2層	業種・規模または何らかの他の要因による

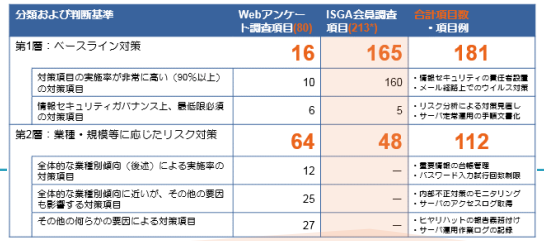
第1層・第2層項目分類結果
ISGA会員調査（18/22）



分類および判断基準		Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策		16	165	181
	対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
	情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策		64	48	112
	全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
	全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
	その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA会員調査	分類	分類理由
離席時に、パスワードによって保護されたスクリーンセーバーが作動するようPCを設定していますか。	第１層	実施率が非常に高い（90%以上）
重要な情報を保存した電子媒体の盗難防止策を講じていますか。（例：不使用時の施錠保管等）	第１層	実施率が非常に高い（90%以上）
PC・電子媒体を社外へ持ち出す際の紛失・盗難防止策を実施していますか。	第１層	実施率が非常に高い（90%以上）
持ち出しの際に順守すべきルールを文書化し、周知していますか。（例：携行中に飲酒しない、電車の網棚に置かない、車内に放置しない、海外出張先のホテルでは施錠保管する、使用中は放置して離席しない等）	第１層	実施率が非常に高い（90%以上）
社外への持ち出しを許可しているPC・電子媒体を特定していますか。	第2層	業種・規模または何らかの他の要因による
社外への持ち出しを許可しているPC・電子媒体の棚卸（所在確認）を定期的に実施していますか。	第2層	業種・規模または何らかの他の要因による
PC画面の覗き見を防止するフィルター（プライバシーフィルター）等を使い、盗み見を防止していますか 。	第2層	業種・規模または何らかの他の要因による
社外に持ち出すPCに、シンクライアントまたはそれに相当する技術的手段を講じていますか。	第2層	業種・規模または何らかの他の要因による
重要な情報をPCに保存して持ち出す際、管理責任者の許可を得るルールとしていますか。	第１層	実施率が非常に高い（90%以上）
社外への持ち出しを許可しているPCの記憶領域を暗号化していますか。	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（19/22）

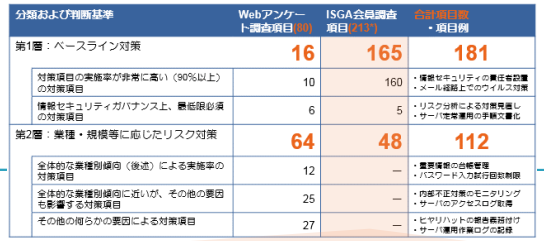


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策		16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策		64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
重要な情報を電子媒体に保存して持ち出す際、管理責任者の許可を得るルールとしていますか。	第１層	実施率が非常に高い（90%以上）
社外への持ち出しを許可しているUSBメモリ・外付けHDD等の記憶領域を暗号化していますか。	第2層	業種・規模または何らかの他の要因による
重要な情報を保存して社外に持ち出すCD/DVD等は、ファイルにパスワードを設定していますか。	第2層	業種・規模または何らかの他の要因による
PCを操作する際、パスワード等により利用者を認証していますか。	第１層	実施率が非常に高い（90%以上）
PCのパスワードは、定期的に変更するルールとしていますか。	第１層	実施率が非常に高い（90%以上）
ID・パスワードの入力試行回数に制限を設けていますか。（例：IDを無効化する、一定時間の経過後に再度ログオンの試行ができるようにする等）	第2層	業種・規模または何らかの他の要因による
業務で利用する携帯電話・スマートフォン等を管理していますか。	第１層	実施率が非常に高い（90%以上）
利用者への携帯電話・スマートフォン等の貸与・利用者変更・返却の手続きが定められていますか。	第１層	実施率が非常に高い（90%以上）
異動・退職等の理由で不要になった携帯電話・スマートフォン等は、ただちに返却されるようになっていますか。	第2層	業種・規模または何らかの他の要因による
社内の携帯電話・スマートフォン等の利用者を少なくとも1年に1回は見直して、異動・退職等の理由で不要になったものがあれば、返却させていますか。	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
ISGA会員調査（20/22）

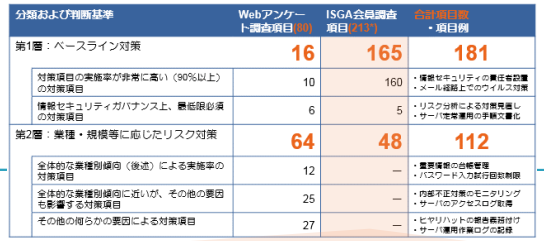


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
携帯電話・スマートフォン等を利用する際の取り扱いルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
業務に利用する携帯電話・スマートフォン等に、暗証番号によるロック機能を設定していますか。	第2層	業種・規模または何らかの他の要因による
コンピュータウイルス対策を実施していますか。	第１層	実施率が非常に高い（90%以上）
WindowsPCにウイルス対策ソフトウェアをインストールし、最新のウイルス定義ファイルで定期的にウイルスチェックが行われる状態に設定していますか。	第１層	実施率が非常に高い（90%以上）
ウイルス感染の可能性に気付いた時の連絡先とすぐ行うべき対応を周知していますか。（例：ネットワークから切り離す等）	第１層	実施率が非常に高い（90%以上）
ウイルス感染の連絡を受けた後の対応部門・担当および対応手順を定めていますか。	第１層	実施率が非常に高い（90%以上）
脆弱性を適時に把握し、対応するための仕組みを整備していますか。	第１層	実施率が非常に高い（90%以上）
脆弱性に関する最新情報を継続的に収集していますか。（例：脆弱性情報を提供するベンダーとのサポート契約・脆弱性に関する情報を提供するメーリングリストやウェブサイト等）	第１層	実施率が非常に高い（90%以上）
サーバーOSまたはパッケージソフトウェアの脆弱性情報について、リスクの大きさとシステムへの影響を考慮して、セキュリティパッチ等の適用要否を判断していますか。	第2層	業種・規模または何らかの他の要因による

第1層・第2層項目分類結果
ISGA会員調査（21/22）

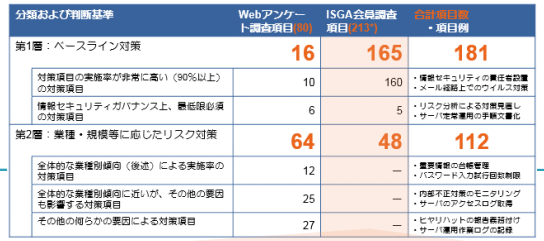


分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・機密セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
PCのOSまたはパッケージソフトウェアに対して、システム上の制約がある場合を除いて、最新のセキュリティパッチ等を適用していますか。（例：ツール等による自動実施、従業員に対しパッチ適用を都度指示する等）	第１層	実施率が非常に高い（90%以上）
PCへのセキュリティパッチ等の適用漏れを避けるため、適用したことを報告させて確認していますか。	第2層	業種・規模または何らかの他の要因による
従業員が会社のPCやスマートフォン等で利用するソフトウェア、ウェブサイトまたはサービスについてのルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
利用者がPCやスマートフォン等に標準以外のソフトウェアをインストールする際の手続きを定めていますか。	第１層	実施率が非常に高い（90%以上）
会社として利用を禁止するウェブサイトまたはサービスを定めていますか。	第１層	実施率が非常に高い（90%以上）
社内のネットワークは、重要情報を不正に持ち出し可能なファイル共有ソフトやSNS、外部のオンラインストレージ等に対してフィルタリングしていますか。	第１層	実施率が非常に高い（90%以上）
電子メールの利用に関するルールを定めていますか。	第１層	実施率が非常に高い（90%以上）
盗聴のリスクがあるネットワーク通信の経路は、盗聴対策を実施していますか。	第１層	実施率が非常に高い（90%以上）
社外から社内ネットワークへリモートアクセスする際は、SSL-VPN等の第三者が介入できない通信方法を利用していますか。	第１層	実施率が非常に高い（90%以上）
社内ネットワークに接続する無線LANを設置する際には、十分な強度をもつ暗号方式によって暗号化を行っていますか。（例：WPA2等）	第１層	実施率が非常に高い（90%以上）

第1層・第2層項目分類結果
ISGA会員調査（22/22）



分類および判断基準	Webアンケート調査項目(40)	ISGA会員調査項目(213*)	合計項目数・項目例
第1層：ベースライン対策	16	165	181
対策項目の実施率が非常に高い（90%以上）の対策項目	10	160	・情報セキュリティの責任者設置 ・メール経路上でのウイルス対策
情報セキュリティガバナンス上、最低限必須の対策項目	6	5	・リスク分析による対策見直し ・サーバ定常運用の手順文書化
第2層：業種・規模等に応じたリスク対策	64	48	112
全体的な業種別傾向（後述）による実施率の対策項目	12	–	・重要機器の台帳管理 ・パスワード入力試行回数制限
全体的な業種別傾向に近いが、その他の要因も影響する対策項目	25	–	・内部不正対策のモニタリング ・サーバのアクセスログ取得
その他の何らかの要因による対策項目	27	–	・ヒヤリハットの報告書提出 ・サーバ運用作業ログの記録

ISGA
Information Security Governance Association

ISGA会員調査	分類	分類理由
社内ネットワークに接続する無線LANを設置する際には、社外から社内ネットワークに接続できないように、電波状況を調査し、電波到達範囲を制限していますか。	第2層	業種・規模または何らかの他の要因による
社内ネットワークに接続する無線LANを設置する際には、接続を許可する情報機器を制限していますか。（例：MACアドレス、電子証明書等）	第2層	業種・規模または何らかの他の要因による
情報機器・電子媒体の種類に応じた廃棄（リース品は返却）の方法を定めていますか。	第１層	実施率が非常に高い（90%以上）
情報機器を廃棄・返却する前に、内部に保存しているデータやソフトウェアの情報を、復元が不可能な方法で消去していますか。（消去が不可能な場合、物理的に破壊していますか。）	第１層	実施率が非常に高い（90%以上）
情報機器を廃棄業者に引き渡す場合は、廃棄証明書を受領していますか。	第１層	実施率が非常に高い（90%以上）
第一層不要となった情報機器を他の部門で再利用する場合は、情報機器内のデータを削除してから引き渡していますか。	第１層	実施率が非常に高い（90%以上）
電子媒体を廃棄する前に、内部に保存しているデータを復元が不可能な方法で消去していますか。（消去が不可能な場合、物理的に破壊していますか。）	第１層	実施率が非常に高い（90%以上）
電子媒体を廃棄業者に引き渡す場合は、廃棄証明書を受領していますか。	第１層	実施率が非常に高い（90%以上）
不要となった電子媒体を他の部門で再利用する場合は、電子媒体内のデータを削除してから引き渡していますか。	第１層	実施率が非常に高い（90%以上）

第3層のフローモデル（改訂案）