ISGA
Information Security Governance Association

情報セキュリティガバナンス協議会
2014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

1．背景・目的
2．検討メンバー
3．検討経緯
4．基本的な考え方
5．情報セキュリティレベル評価ツール
6．事業戦略目標とセキュリティを結びつけるロジック
7．今後の課題

2015年7月30日

1．背景・目的

ISGA
Information Security Governance Association

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。

そこで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。

本年度は、これらの成果の整理と具体的な活用を目指して、以下の取組みを行う。

- 2012年度の成果を活用したデータの整備
- 2013年度の成果の発展

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
グローバルセキュリティエキスパート株式会社	服部　康治
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
日興アセットマネジメント株式会社	竹内　英稔
日本電気株式会社	甲田　輝彦
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	橋詰　雅樹
持田製薬株式会社	山野邊　渉

（社名五十音順　敬称略）

（事務局）

株式会社三菱総合研究所	井上　信吾、綿谷　謙吾

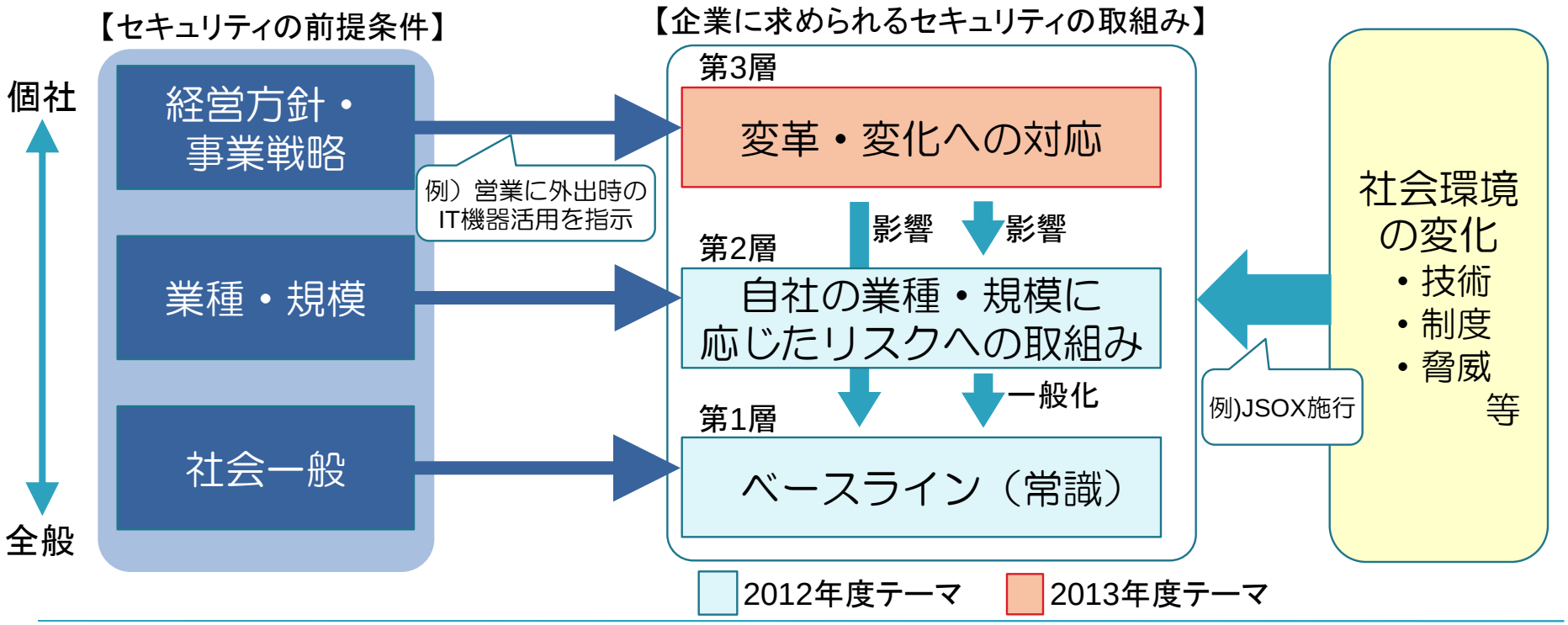
３．検討経緯

■ **会合**

第１回	8／29（金）	キックオフ、論点整理	（三菱総合研究所）
第２回	9／26（金）	検討方針について	（インフォセック）
第３回	10／24（金）	テーマ・方法の検討	（デロイト・トーマツ・リスクサービス）
第４回	11／21（金）	テーマ・方法の検討/分科会作業	（京王電鉄）
第５回	12／12（金）	分科会作業	（京王電鉄）
本会合	12／15（月）	中間報告	（三菱総合研究所）
第６回	1／16（金）	分科会作業	（三菱総合研究所）
第７回	2／20（金）	分科会作業	（日興アセットマネジメント）
合宿	2／27（金）～28（土）【宿泊集中討議】		（CSSC等）
第８回	3／12（木）	報告書の作成	（三菱総合研究所）
本会合	3／18（水）	最終報告	（三菱総合研究所）

4. 基本的な考え方①

- 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。



４. 基本的な考え方②

■ 本検討の狙いは「経営を説得するための『見える化』」
■ これまでの取組みに沿って2テーマに分けて、それぞれ検討を進める。
- 情報セキュリティ対策のレベルを比較するツールの整備
- 経営目標・経営課題とセキュリティを結びつけるロジックの整備

【課題1】
情報セキュリティ対策の
レベルを評価するツールの整備

【課題2 】
経営目標・経営課題とセキュリティを
結びつけるロジックの整備

【Aチーム】

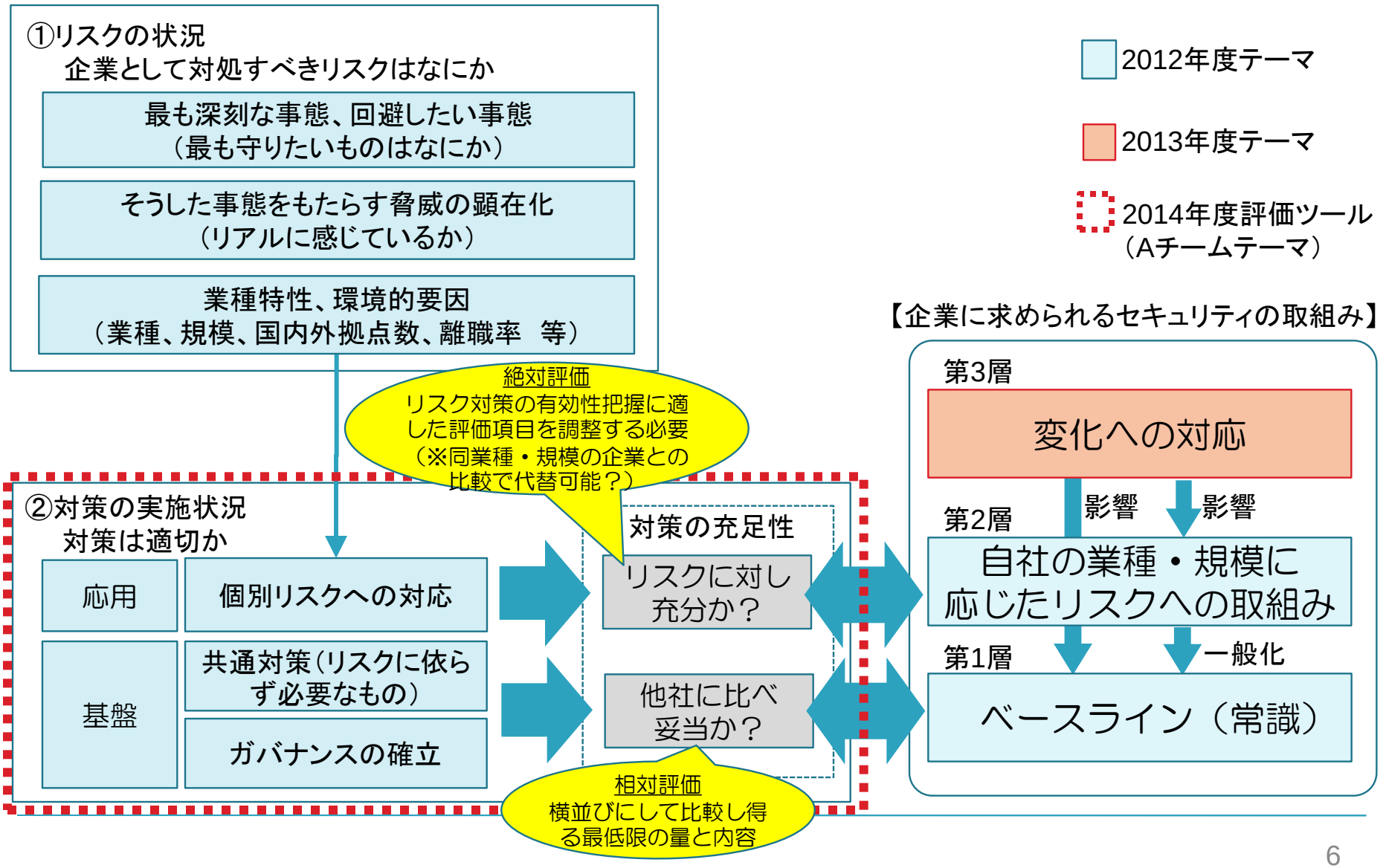
インフォセック	田中
石油資源開発	藤井
日本電気	甲田
MIND	橋詰
持田製薬	山野邊
日興アセット	竹内

【Bチーム】

京王電鉄	細田
GSX	服部
DTRS	渡部
富士通	西見
三菱総合研究所	川口

5．情報セキュリティレベル評価ツール
(1) 評価項目の全体構造

ISGA
Information Security Governance Association



5．情報セキュリティレベル評価ツール
(2) 評価方法

■情報セキュリティレベル評価ツール構成
8つの対策分野、42の大問および256の小問から構成。
※2012年度成果物から対策項目を一部追加・見直し。および回答方法を簡略化

■評価シートのイメージ

質問11：	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。	はい／いいえ／対象外
11-1	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。	はい／いいえ／対象外
11-2	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。	はい／いいえ／対象外
11-3	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）	はい／いいえ／対象外
11-4	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）	はい／いいえ／対象外

【大問】
「いいえ」なら小問は回答不要
（全て「いいえ」扱い）

【小問】
全体のおよそ8割以上に対策を実施済みの場合に「はい」（目安）

5．情報セキュリティレベル評価ツール
(3) 試行結果（会員企業編：対策項目）

●ISGA会員企業に対して評価ツール全項目のアンケートを実施（15社が回答）

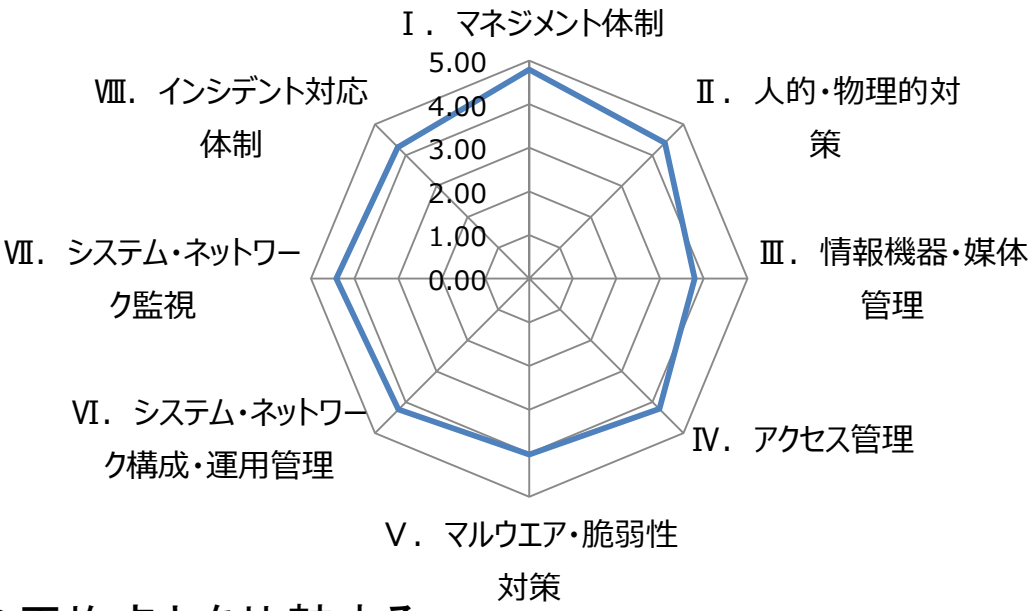
－対策分野ごとに5点満点に換算し、左図のとおり視覚化。

－会員企業での平均点は、全分野でおよそ4点前後となった。

－特に「**Ⅰ．マネジメント体制**」は平均4.79点であり、**対策の実施率が高**かった。

－一方、「**Ⅲ．情報機器・媒体管理**」は平均3.79点であり、**未実施の対策がやや多かった**。

予備調査結果（会員企業15社平均）



●評価ツールの活用方法（例）

－会員企業が自社評価と、会員企業の平均点とを比較することで、自社が手薄な対策分野の把握に利用。

－個別の対策（小問の項目）について、会員企業での平均実施率を参考にすることで、自社で今後対策を導入すべきかどうかの検討に利用。

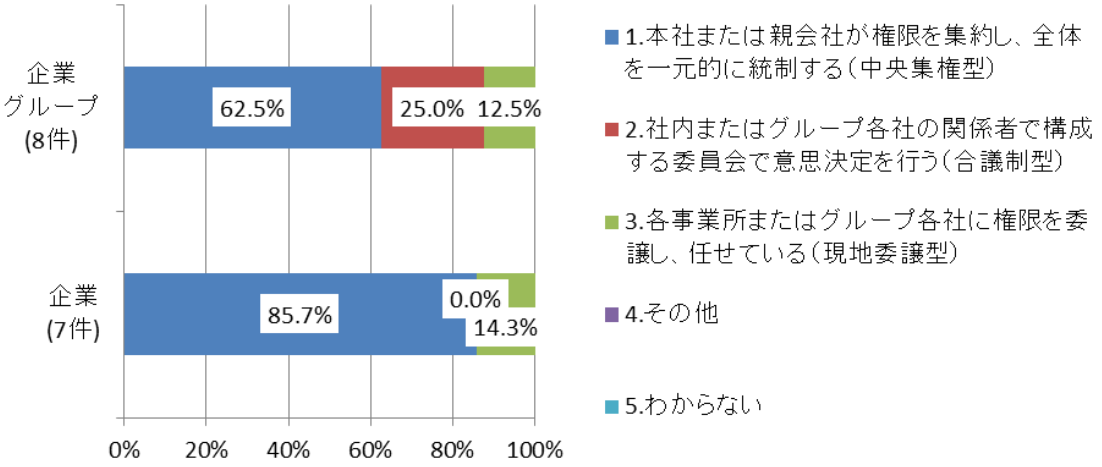
※会員企業調査データは、自社回答を提出した企業に配布予定。

5．情報セキュリティレベル評価ツール
(3) 試行結果（会員企業編：ガバナンス）

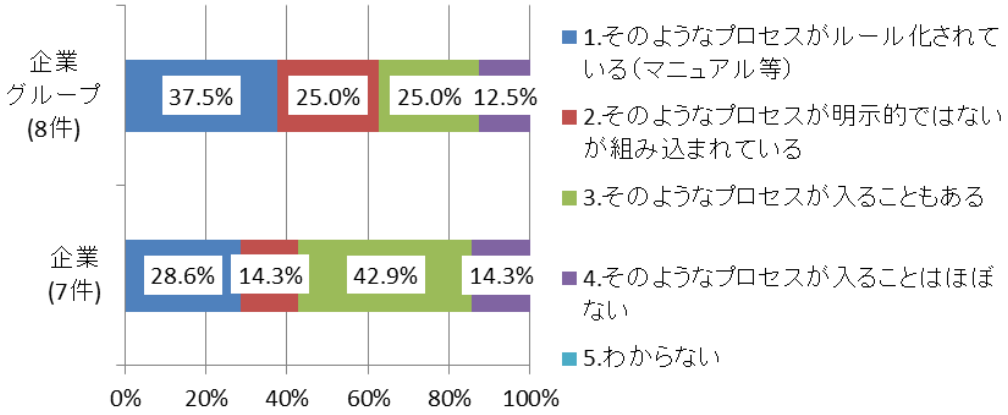
●ISGA会員企業に対してガバナンスの現状認識と課題のアンケートを実施（15社が回答）

●企業グループを対象とした回答が8件、企業を対象とした回答が7件

－企業またはグループ全体の統治（コーポレートガバナンス）は、中央集権型が主だが、企業グループでは合議制型が25%を占める。



－**事業戦略・事業計画立案の工程で、情報リスクを検討するプロセス**が組み込まれているのは、企業グループの場合62.5%、企業の場合42.9%に留まる。



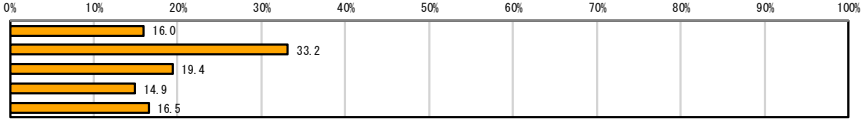
5．情報セキュリティレベル評価ツール
(3) 試行結果（Web調査編：調査概要）

ISGA
Information Security Governance Association

●評価ツールの小問256問から80問を抽出、一般企業の情報セキュリティ担当者を対象にWebモニタアンケート調査を実施（協力：デロイト・トーマツ・リスクサービス様）。1046件を回収。

回答者の内訳（企業規模）

		実数	%
全体		1046	100.0
1	100人以上　300人未満	167	16.0
2	300人以上　1，000人未満	347	33.2
3	1，000人以上　3，000人未満	203	19.4
4	3，000人以上　10，000人未満	156	14.9
5	10，000人以上	173	16.5



●企業の重複可能性を排除しかつ正社員数1000名以上の回答222件に絞って分析。

●Web調査結果の活用方法（例）

－全体的な回答の平均から、会員企業のセキュリティレベルの傾向を把握。

－個別の対策80項目について、同規模・同業種での平均実施率を参考にして、自社の今後の対策導入の検討に利用。

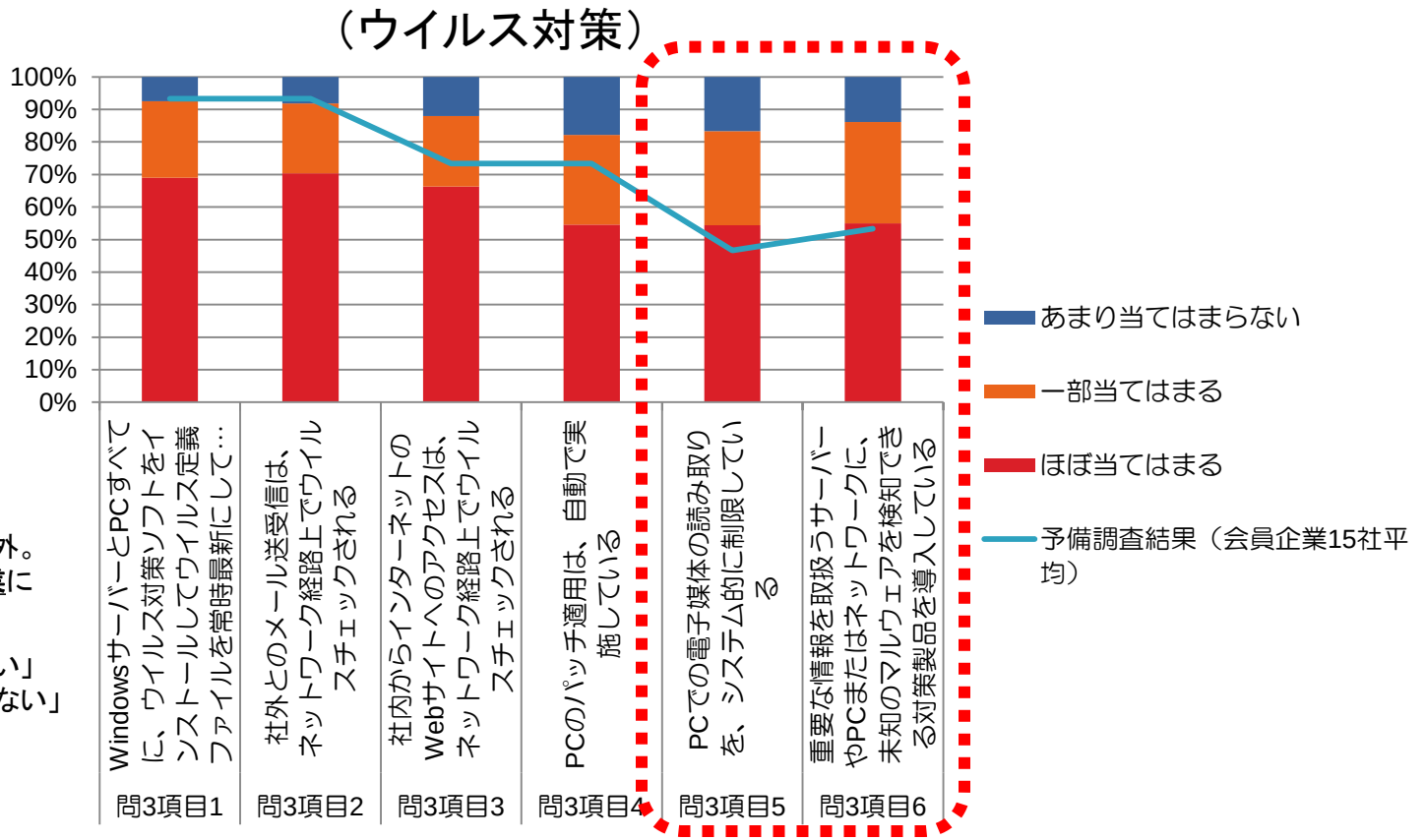
		実数	%
全体		1046	100.0
1	農林水産	3	0.3
2	鉱業・電力・ガス/その他エネルギー	18	1.7
3	建設・土木・住宅・プラント	52	5.0
4	不動産	15	1.4
5	木材/紙・パルプ/繊維製造/印刷	11	1.1
6	化学/石油/ゴム製品	15	1.4
7	医薬品/化粧品	11	1.1
8	鉄鋼・非鉄・金属・素材・製品	23	2.2
9	水産加工/食料品/飲料/酒類	17	1.6
10	電気/電子/コンピュータ/通信機器	75	7.2
11	自動車/自動車部品	28	2.7
12	機械・機械部品・精密機械	53	5.1
13	その他製造業	86	8.2
14	運輸/倉庫	37	3.5
15	商社	56	5.4
16	百貨店/スーパー	7	0.7
17	コンビニエンスストア	0	0.0
18	その他流通・小売	24	2.3
19	銀行/信託/信金/信組/政府系金融	33	3.2
20	信販/消費者金融	0	0.0
21	証券業/商品取引	15	1.4
22	生命保険/損害保険業	18	1.7
23	その他金融	6	0.6
24	通信業	33	3.2
25	ソフトウェア/情報処理	183	17.5
26	リース・レンタル	1	0.1
27	ホテル/旅行代理店	7	0.7
28	外食/フードサービス	6	0.6
29	調査・コンサルティング・シンクタンク	5	0.5
30	広告代理店	0	0.0
31	その他サービス業	112	10.7
32	新聞/出版/放送	5	0.5
33	学校・教育	19	1.8
34	保健・医療・福祉関連	30	2.9
35	研究開発・研究機関	4	0.4
36	政府・地方公共団体・各種法人・団体等	20	1.9
37	その他	18	1.7

5．情報セキュリティレベル評価ツール
(3) 試行結果（Web調査編：調査結果①）

●大部分の対策について、ISGA会員企業15社の平均実施率は、Web調査による一般企業の平均実施率（「ほぼ当てはまる」に相当）よりも高かった。

●ISGA会員企業の平均実施率が一般企業を下回った対策項目を以下に抜粋。

情報漏えい防止策の一つとして、**電子媒体への書き込みは制限しているが、読み取りには制限を設けていない**ケースもあると考えられる。

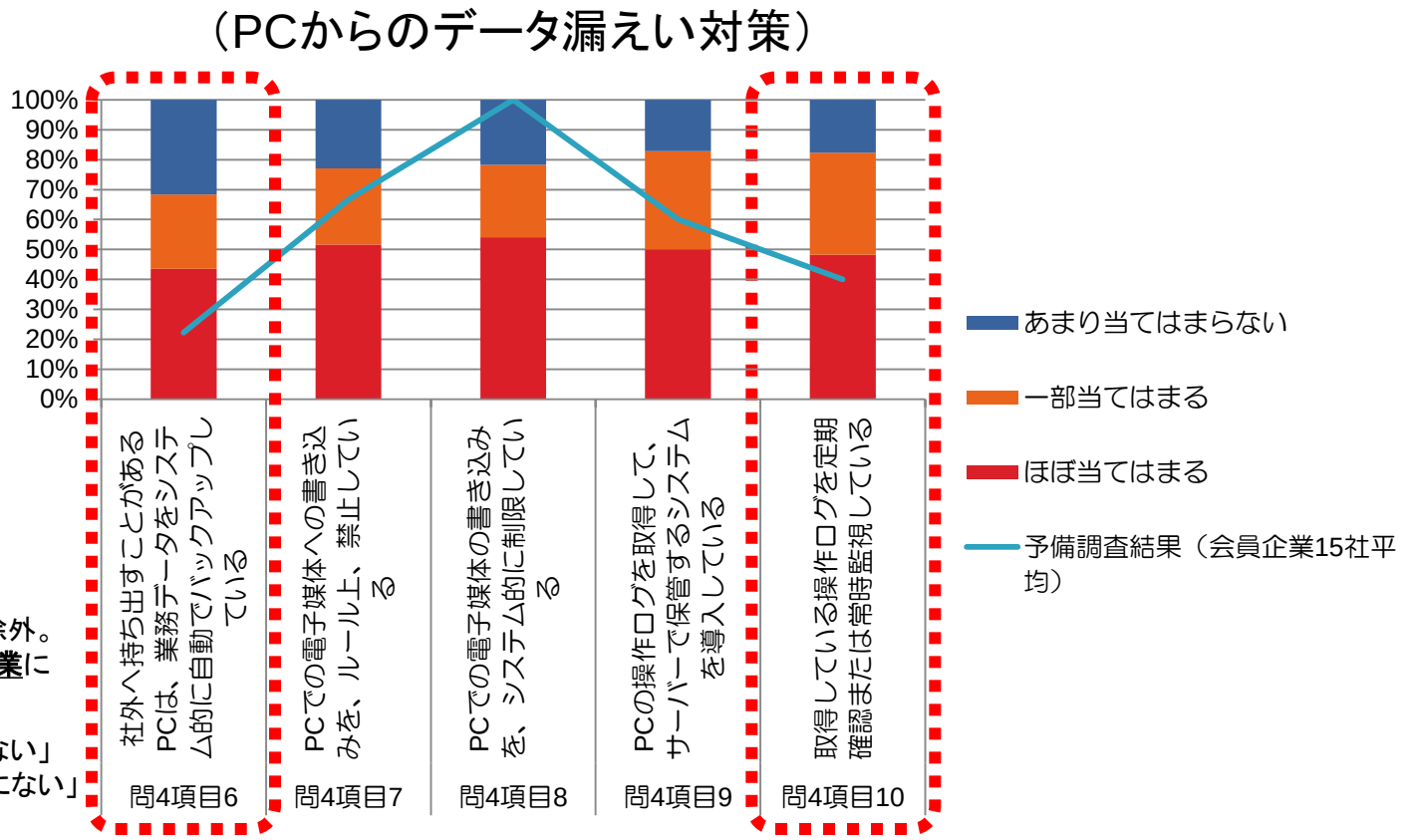


※右図のWeb調査集計対象：
企業の重複または企業不明を除外。
かつ**正社員数1000名以上の企業**に限定した222件。

※また回答が「わからない／知らない」「対策の対象となるものが社内にない」の場合は集計から除外。

5．情報セキュリティレベル評価ツール
(3) 試行結果（Web調査編：調査結果②）

- 社外持ち出しPCのデータを自動バックアップしている回答の割合は、ISGA会員企業15社平均が一般企業に比べ低かった。ただし、**PC本体には業務データの保存を禁止しているケース**も多いと考えられる。
- 情報漏えい防止・抑止のため、PC操作ログ等を定期的にモニタリング運用している一般企業が約半数に上った。一方で、**ログは取得しているが、人的リソースの問題やログ監視・分析システムの未導入等により、常時監視までは網羅的に十分できていない**企業もあるのではないかと考えられる。



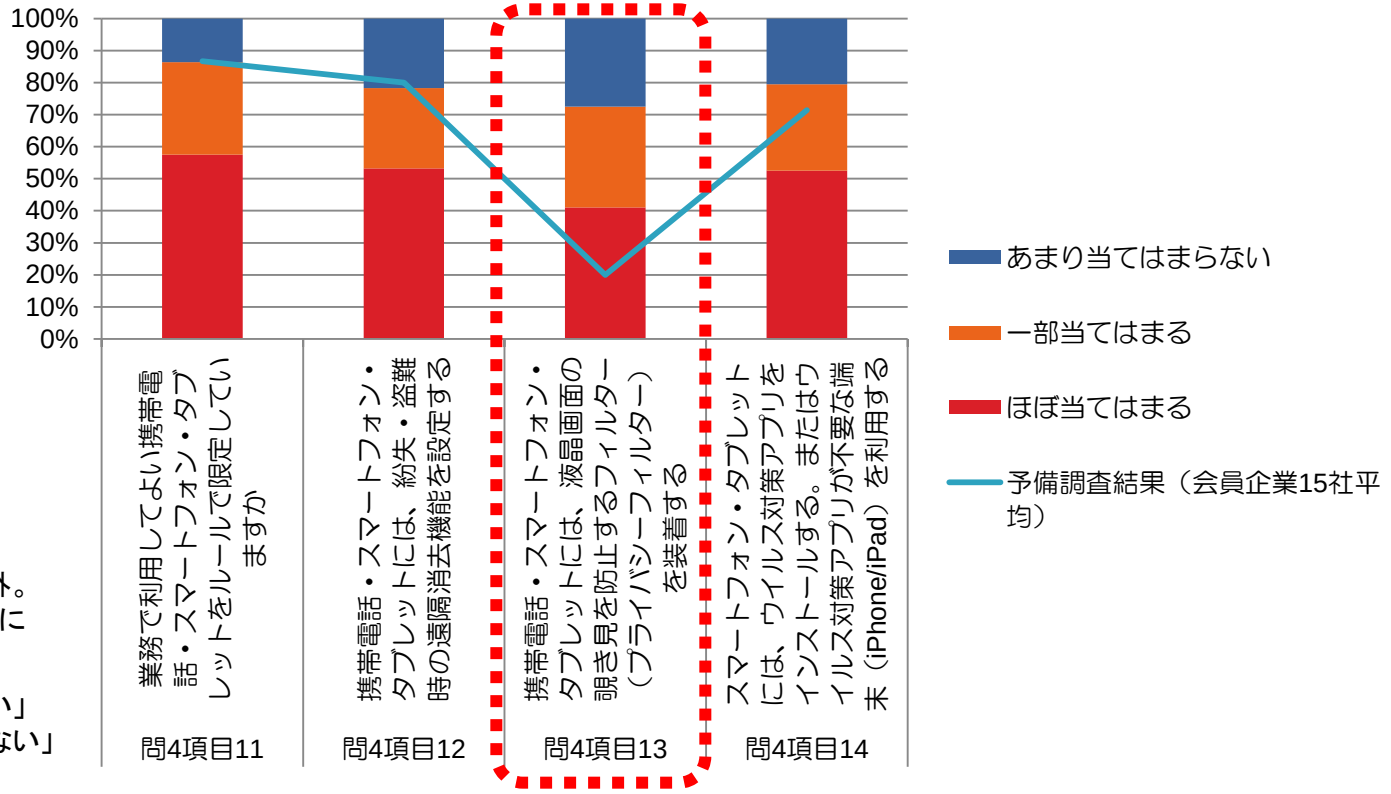
※右図のWeb調査集計対象：
企業の重複または企業不明を除外。
かつ**正社員数1000名以上の企業**に限定した222件。

※また回答が「わからない／知らない」「対策の対象となるものが社内にない」の場合は集計から除外。

5．情報セキュリティレベル評価ツール
(3) 試行結果（Web調査編：調査結果③）

- 秘密情報を扱う企業においては、外出先においても特に高いセキュリティレベルが求められるため、周囲からの覗き見による情報漏えい防止策の一つとして、画面にフィルターを装着している率も高いものと考えられる。
- ただし、フィルターの装着率はISGA会員企業15社平均が一般企業に比べ低い結果になった。

（携帯電話・スマートフォン・タブレットの情報漏えい対策）

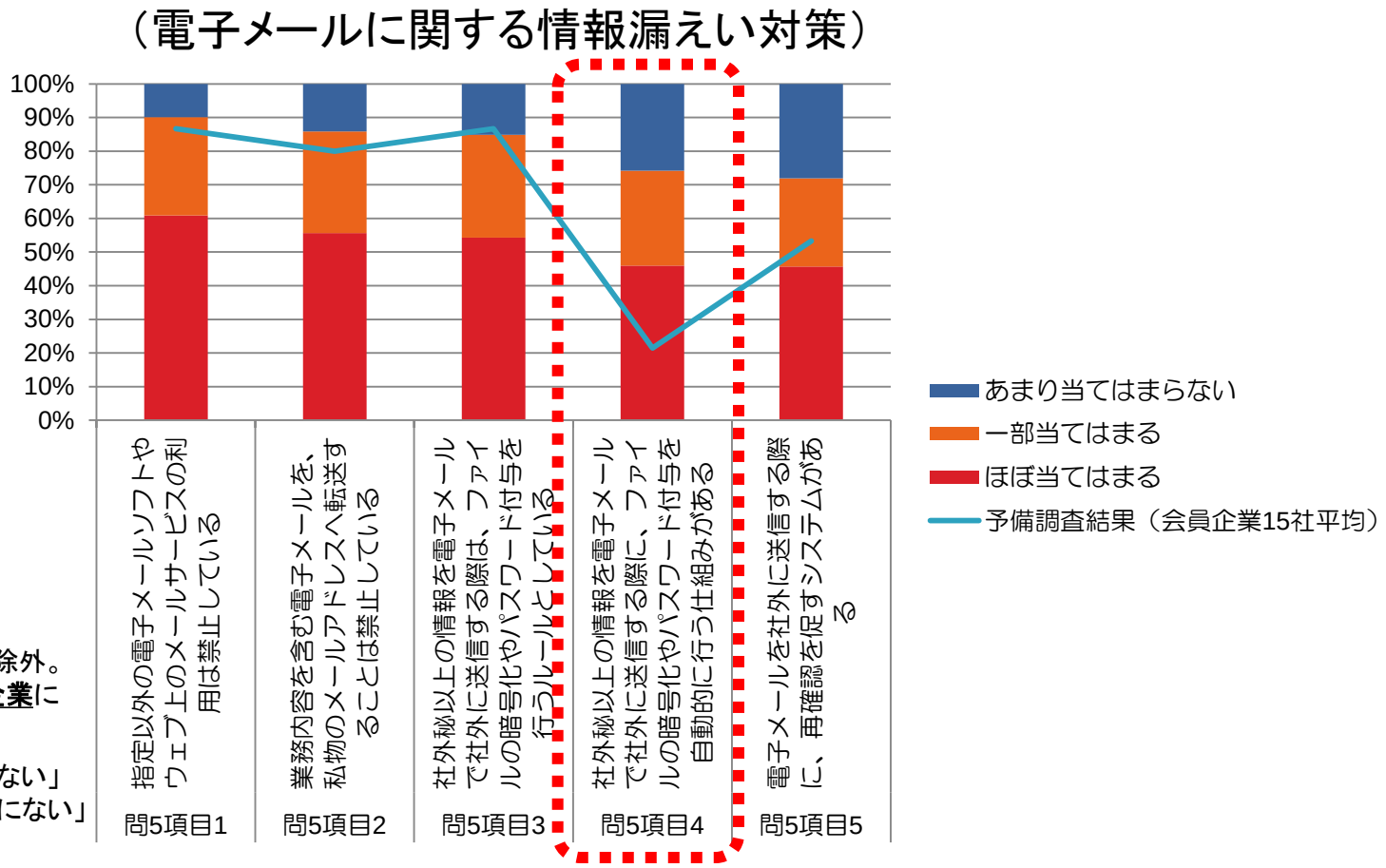


※右図のWeb調査集計対象：
企業の重複または企業不明を除外。
かつ**正社員数1000名以上の企業**に限定した222件。

※また回答が「わからない／知らない」「対策の対象となるものが社内にない」の場合は集計から除外。

5．情報セキュリティレベル評価ツール
(3) 試行結果（Web調査編：調査結果④）

- 添付ファイル自動暗号化等のシステムは、一般企業ではIT企業を中心に導入が進みつつある。
- 一方、ISGA会員企業の多くは、現段階では**従来の取組みにとどめている**（都度ユーザがファイルにパスワードを設定するルール等）、あるいは自動暗号化システムの導入を検討している状況と思われる。

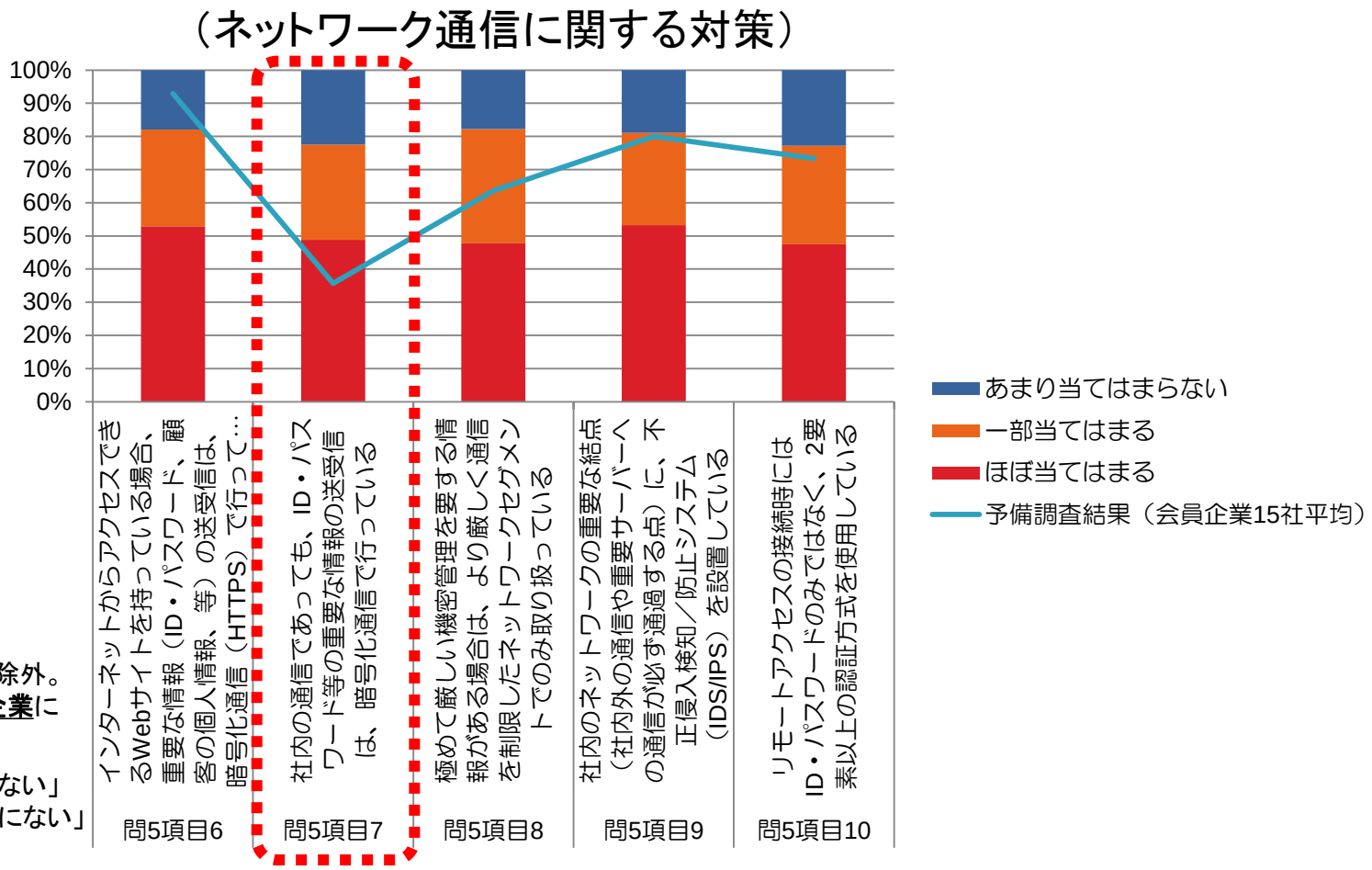


※右図のWeb調査集計対象：
企業の重複または企業不明を除外。
かつ**正社員数1000名以上の企業**に限定した222件。

※また回答が「わからない／知らない」「対策の対象となるものが社内にない」の場合は集計から除外。

5．情報セキュリティレベル評価ツール
(3) 試行結果（Web調査編：調査結果⑤）

- ISGA会員企業は、社外からの攻撃への対策に比べ、社内ネットワークにおける暗号化経路の導入のような**社内ネットワーク上の対策が遅れている**傾向があると考えられる。



※右図のWeb調査集計対象：
企業の重複または企業不明を除外。
かつ**<u>正社員数1000名以上の企業</u>**に限定した222件。

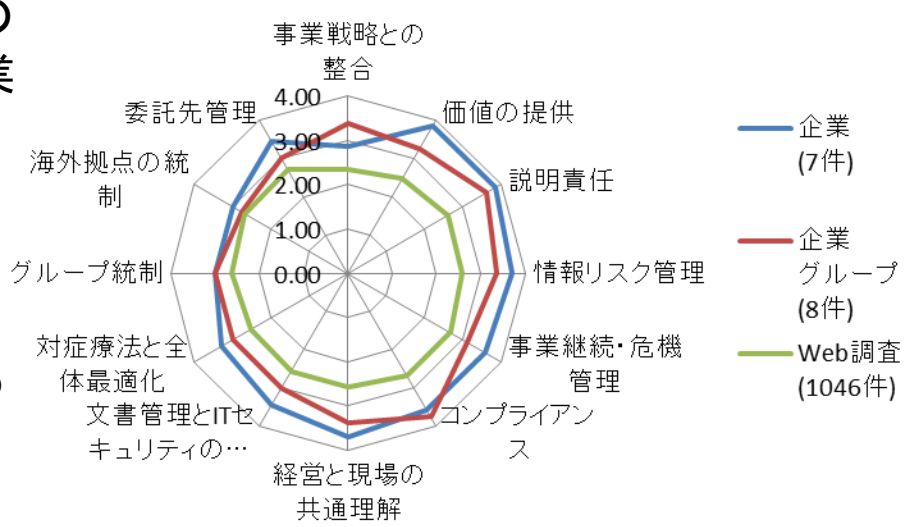
※また回答が「わからない／知らない」「対策の対象となるものが社内にない」の場合は集計から除外。

5．情報セキュリティレベル評価ツール
(3) 試行結果（Web調査編：調査結果⑥）

●ガバナンスに関する課題12項目とISGA会員企業の比較：

－すべての課題について、ISGA会員企業の回答の平均は、Web調査による一般企業の回答の平均よりも高い（自社または自グループの課題ではない）。

－「企業」を対象としている会員企業の回答の平均は高い（その課題と関係がない）が、「**事業戦略との整合**」は2.86に留まる（わからない～疑いがある）。



1.該当する事象が発生したことがある
2.該当する事象が発生した疑いがある
3.該当する事象が発生したかどうかわからない
4.該当しない

●Web調査による一般企業の回答は、すべての課題について、2～3の間にあり、課題間に大きな差はなかった。

← 経営の目線で断言できる回答が少なかったため？

※会員企業調査データは、自社回答を提出した企業に配布予定。

５．情報セキュリティレベル評価ツール
(3) 試行結果（その他）

●評価ツールのその他の活用方法（例）

－**複数部署・拠点間の比較として利用**

・事業本部ごと、または国内外の拠点ごとに対策状況が異なる場合に、各部署・拠点でそれぞれ評価ツールに回答記入する。

・各部署・拠点の評価点を比較することで、とくに対策が立ち後れている部署・拠点を洗い出したり、部署・拠点の対策実施のモチベーションとして利用する。

－**グループ企業のセキュリティレベルの参考指標として利用**

・グループ内に業種・規模が異なる子会社・関連会社が多数ある場合に、各社でそれぞれ評価ツールに回答記入する。

・Web調査結果データから、グループ各社に類似の業種・規模での対策実施率を算出して、各社の評価点と比較することで、それぞれの会社に相応しいレベルに達しているか判断する際の参考にする。

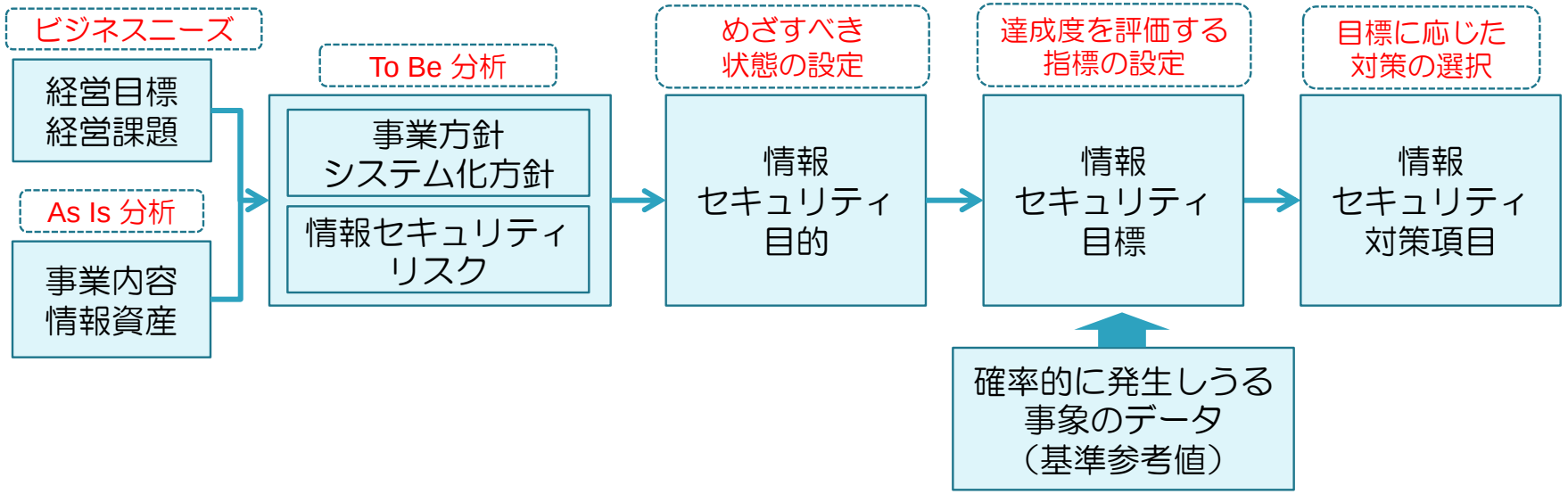
●活用における課題

－80項目だけでなく、全対策項目（小問256項目）についての一般企業データ収集

－回答者の主観による影響を回避できるデータ収集方法の検討

6．経営目標・経営課題とセキュリティを結びつけるロジック
(1) 検討経緯

- 2013年度は、「経営目標・経営課題」から「情報セキュリティ対策項目」を導出するフローをモデル企業に当てはめて、ウォークスルーを試みた。
- 本年度は、フローモデルを前提に、経営課題やシステム化方針から情報セキュリティ目的・目標を導出するとともに、CIO、CISO、システム管理者などが具体的に担うべき役割、必要とする情報、必要とする意思決定について明らかにすることを目標に置いた。
- モデル企業設定に当たっては、企業の概要と経営目標を設定し、これに対して直近の営業状況と企業トップの問題認識までを所与とした。



6．経営目標・経営課題とセキュリティを結びつけるロジック
(2) モデル企業の設定　①概要

ISGA Information Security Governance Association

● 各工程の具体化を図るため、「Bエレクトロニクス」を設定し、その経営課題や事業方針を策定した。

【概況】
- 昭和28年、B工業株式会社として設立
- 現在の連結売上高は約8,000億円
- 独自の製品開発力を有し、系列販売店への徹底的なガバナンスによる「**一枚岩での経営**」により評価は高く、早くから海外進出も積極的に行ってきた。
- しかしながら、系列販売店の経営者の世代交代や海外での系列販売店を中心とした不正取引の増大**で従来の主力事業の落ち込み**が見られている。
- さらに価格重視の顧客ニーズに対して、従来の系列販売店経由では競争力がなく、かつ家電製品自体の需要の落ち込みから、**多角化戦略**を実施している。

【主要事業の再編】

チャネル販売事業部（売上比50%）	基幹事業である家電製品の系列販売代理店、大型量販店経由でのチャネル販売を実施
ソフトウェア事業部（売上比25%）	2010年、Cシステム社をM&Aにより買収し、組織再編時にB社の一事業部として取り込んだ
ダイレクト販売事業部（売上比25%）	2008年より事業開始。従来の製品への信頼をベースに大きく業績を伸ばしている

【システム部門の再編】
- システム部門については、**B社の情報システム部と旧Cシステム社の社内システム部門と併合**
- 旧Cシステム社のコーポレートシステム部（社内システム担当）のマネージャを新たにシステム部長に任命
- 経営陣から、**B社と旧Cシステム社のシステム統合**を命じられる

【システムの現況】

経理システム	Bエレクトロニクス社のERPにCシステム社を統合
業務系システム	基本的にそれぞれの業務システムを継続利用
人事システム	人事制度の調整が進まず、給与計算システムは2系統が共存
グループウェア	旧Bエレクトロニクス社のグループウェアを全社基盤と設定
ネットワーク基盤	ドメインの統一、ネットワークポリシーの一元化

6．経営目標・経営課題とセキュリティを結びつけるロジック
(2) モデル企業の設定　②経営課題

Information Security Governance Association

● 組織再編後1年を経過した2012年3月の状況：
・組織再編により、売上は当初見込みの8,000億円を達成
・営業利益率、経常利益率は組織再編前より低下
・海外拠点の成長率は当初の見込みより低く、同業他社以下

【CEOの考え】
● これらの状況を踏まえ、CEOは以下の懸念点を抱いている。
・**Cシステムを合併した効果**は出ているのか。同社のノウハウ、人材を既存の業務改善に活用したいが、環境整備を含めうまくいっているのか。
・利益率の低下は、昨年発生した次の問題が影響しているのではないか。
　－ チャネル販売事業部の欧州拠点で発生した**代理店情報の流出**
　－ ダイレクト販売事業部で発生した**個人情報流出**

経営課題と対応方針

経営課題	対応方針
合併時に暫定対応した、システム環境の統合が進んでいない	システムの統合は早急に進める。
発生した問題（インシデント）の事業への影響を適切に把握できていない（自身もわかっていない）	発生した問題（インシデント）の事業への影響を把握し、必要な手当を速やかに行うとともに、そこからの学びを各事業部の戦略実行、オペレーションに活かす。
発生した問題での反省（学び）が各事業のオペレーションに活かせていない（再発防止、情報の共有等）	

6．経営目標・経営課題とセキュリティを結びつけるロジック
(3) 情報セキュリティ目的

ISGA
Information Security Governance Association

●システム化方針から情報セキュリティリスクと対応する情報セキュリティ目的を設定する

システム化方針		情報セキュリティリスク	情報セキュリティ目的
早期のシステム統合を目指す	[経理システム] Bエレクトロニクス社のERPにCシステム社を統合	• **システム統合に伴う組織間の課題（制度設計の齟齬等）が機密性や可用性を損なう問題を招く**可能性がある • セキュリティ統制を一元化する場合、両社のポリシーを比較して、**低い方に設定**せざるを得ない	• **システム統合に伴う情報セキュリティ上の問題の解消** - 組織間の課題の把握 - 優先すべき課題への対応
	[業務システム] 基本的にそれぞれの業務システムを継続利用		
	[人事システム] 人事制度の調整が進まず、給与計算システムが2系統のまま	（人事制度が統合していないため、システムの統合開発が進められない）*	
	[グループウェア] 旧Bエレクトロニクス社のグループウェアを全社基盤と設定	（過去の情報資産とその活用方法を、全社でどのように共有するか決まっていない）*	
	[ネットワーク基盤] ドメインの統一、ネットワークポリシーの一元化	• ネットワークに潜む**脆弱性の把握に手間がかかる**	
• インシデントに対する手当を速やかに行う • インシデントに関する反省を各事業部の戦略実行、オペレーションに活かす		• 可用性が優先される中で、**管理者権限管理の不備**により不正行為が発生する	• **インシデント対応強化** • **再発防止策の徹底**

*) 情報セキュリティリスクではないが、システム化方針を実現する上での課題である

6．経営目標・経営課題とセキュリティを結びつけるロジック
(4) 情報セキュリティ目標

Information Security Governance Association

●情報セキュリティリスクと対応する情報セキュリティ目的から、達成すべき情報セキュリティ目標を次のように定める。

情報セキュリティリスク	情報セキュリティ目的	情報セキュリティ目標
•システム統合に伴う組織間の課題（制度設計の齟齬等）が機密性や可用性を損なう問題を招く可能性がある •セキュリティ統制を一元化する場合、両社のポリシーを比較して、低い方に設定せざるを得ない •ネットワークに潜む脆弱性の把握に手間がかかる	•システム統合に伴う情報セキュリティ上の問題の解消 - 組織間の課題の把握 - 優先すべき課題への対応	[システム統合前の目標] **•統合に関する組織間の課題**の洗い出し **•全社的な優先順位の再調整*** **•セキュリティポリシーの統合** [システム統合時の目標] •システム統合の方針・設計レベルでの**脆弱性評価**
•管理者権限管理の不備により不正行為が発生する	•インシデント対応強化 •再発防止策の徹底 •内部犯行対策の強化 •管理者権限の管理	[システム統合時の目標] **•ネットワーク監視**の実施 •厳格な**管理者権限の管理** [システム統合後の目標] **•CSIRTの整備** **•内部犯行の厳罰化** •職場環境における**コミュニケーションの強化**

*) 優先順位の設定には、セキュリティ以外の要因も加味される

６．経営目標・経営課題とセキュリティを結びつけるロジック
(5) 得られた知見

Information Security Governance Association

- 人事政策の統合などがなされなければ、そもそもシステム統合はできず、最低限でも、**政策決定の責任**については明確にする必要がある。
- **CIOの経営における役割と責任**を明確にすることが、システムの完全性、可用性を担保するために必要である。
- CISOには、CIOと連携しながらも**独自の役割**が存在する。情報漏えいの原因究明や事後対応などは、CIOとは別の判断があり、時には相互に調整を要する。
- システム環境が流動的な中では、**通常のセキュリティ対策が機能しない場合**もある。
- **経営計画から発生したシステム化計画やセキュリティ目標が、実際のシステム運用管理におけるセキュリティ対策に影響を与える**可能性がある。その影響があまりに大きいとすれば、CISO、CIOは、計画の変更を求めたり、阻害要因を調整するなどの役割を当然に期待される。
- 経営においては、これらの要素をCIO、CISOが正しく把握し、適切なリスク評価を行える体制を構築することが、失敗しないシステム、堅牢な情報セキュリティ体制を築くために必要。

7. 今後の課題

ISGA
Information Security Governance Association

■ 今後の課題として、以下の項目が挙げられる。

- **情報セキュリティレベルの評価データの充実**
  - ✓ 小問全256項目を対象とした調査の実施
  - ✓ 規則や対策の設定に関する遵守状況の把握
- **第2層の分析**
  - ✓ 業種・企業規模に基づく詳細な分析
- **クラウドとの関係**
  - ✓ クラウド上にシフトした場合の評価方法
- **第1層、第2層と第3層の関係**
  - ✓ 情報セキュリティレベルの成果とフローモデルの関係に関する検討
- **フローの理論化**
  - ✓ 汎用性を高めるためのフローの理論化
- **CIO、CISOのあり方（機能、役割、責任）**