ISGA
Information Security Governance Association

情報セキュリティガバナンス協議会
2013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

コンテンツ

2014年6月30日

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、以下の点で悩むケースが多いと考えられる。

・情報セキュリティ活動の状況や課題等をどのように把握するか
・情報セキュリティ活動の状況や課題等を経営陣にどのように報告するか

前者については、現在、各社が状況把握のために行っている情報収集・分析の方法を比較・整理する方向と、情報セキュリティ上の様々な脅威に対し、どのような対策をどこまでとるのが妥当か、各社の取組やリスクの許容範囲等を比較し、妥当な水準の考え方を明らかにする方向がある。

昨年度のワーキンググループ（WG）では，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，情報セキュリティ活動が経営陣に適正に評価される構造が十分に形成できておらず，理解を得ることに苦労している状況が明らかになった。その背景には，以下の問題が挙げられる。

・情報セキュリティの取組みがどれだけビジネスに貢献しているかわかりにくく，情報セキュリティ活動やその向上が経営陣に訴求しにくい
・日常的な業務を支える基本的な情報セキュリティ対策は，経営陣にとって「適正に管理運用されて当たり前」のものであり，その取組みに対する関心が薄い

そこで，本年度のWGの活動では，経営陣が情報セキュリティ活動に関心を持ち，その評価を適正に行うことを目指し，以下の目的を設定する。

・経営陣に効果的に訴求する情報セキュリティ活動の提示方法を提案する
・経営陣が情報セキュリティ活動の妥当性について容易に評価できる仕組みを提案する

2. 検討 メンバー

■ **検討メンバー　（社名：五十音順　氏名：敬称略）**

EMCジャパン株式会社	矢野 薫(2014年2月まで)
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
株式会社ジェイティービー	戸田 磨
新日本有限責任監査法人	勝村 学
積水化学工業株式会社	竹内 守
石油資源開発株式会社	藤井 雅久
株式会社高島屋	井上 哲三
デロイトトーマツリスクサービス株式会社	渡部 豊
日本電気株式会社	甲田 輝彦
富士ゼロックス株式会社	杉森 裕司
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テクノロジー株式会社	橋詰 雅樹
持田製薬株式会社	山野邊 渉
（事務局）	
株式会社三菱総合研究所	江連　三香

３．検討経緯

第１回	7／31（水）	キックオフ、論点整理	（三菱総合研究所）
第２回	8／29（木）	見える化の目的について	（日本電気）
第３回	9／25（水）	検討方針について 事例紹介（積水化学様）	（積水化学）
第４回	10／22（火）	検討方針について 事例紹介（日本電気様）	（持田製薬）
第５回	11／25（月）	検討方針及び検討体制について	（京王電鉄）
第６回	12／16（月）	分科会作業	（トーマツ）
第７回	1／17（金）	分科会作業	（インフォセック）
合宿	2／14（金）～15（土）【宿泊集中討議】		（WG1、WG2合同：京王電鉄様の会議施設等）
第８回	2／20（木）	分科会作業	（富士通）
第９回	3／07（金）	報告書の作成方針	（インフォセック）
第10回	3／28（金）	報告書について	（三菱電機インフォメーションテクノロジー）

4. 全体構成　(1) 問題意識

■情報セキュリティ活動やその向上に対する経営陣の関心が乏しい
- 情報セキュリティの取組みがどれだけビジネスに貢献しているかわかりにくい
- 経営陣にとって、セキュリティ対策が適正に管理運用されることは「当たり前」
- 事件・事故が起きない限り、情報リスクについてあまり考えない

どうしたらリスクや、情報セキュリティの取組みのビジネスへの貢献を経営陣に評価してもらえるか

← 経営陣が最も関心のある領域でリスクや必要な取組みを説明する

■情報セキュリティ活動の現状が適切か否か、判断が難しい
- リスクに対し対策が適切であるかを絶対的に評価することは困難
- 他組織の取組みと比較して妥当性を評価することは可能だが、比較可能なデータを集積する必要がある

どうしたら取組みが十分かどうかを客観的に評価してもらえるか

← 目的・目標を明確化し、評価可能な指標を設定する

■合理的なコストの範囲でリスクを「ゼロ」にするのは困難であることが理解されない
- 「リスクを許容する」ということが理解されず，情報セキュリティ担当者の取組みを正しく評価できない可能性も

どうしたら残留リスクが許容できることを理解してもらえるか

← 直感的にイメージできる参考値を活用する

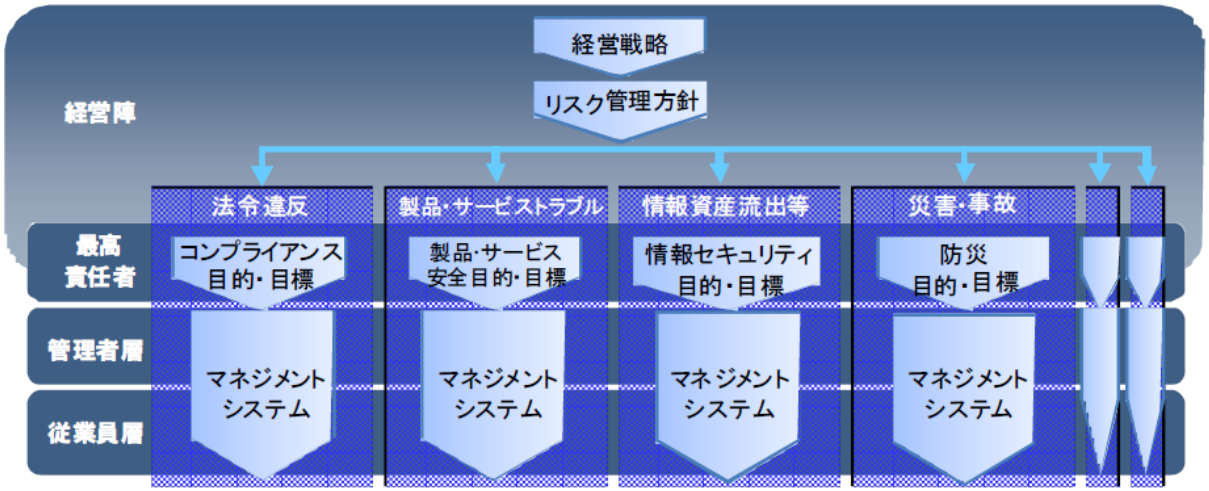
4. 全体構成　(2) 基本的な考え方

■検討目標

- 経営陣の打ち出す中期計画、経営目標、事業方針等に必要な情報セキュリティの取組みに焦点を当て、情報セキュリティ活動がビジネスに直結する構造を提示
- 情報セキュリティ活動について評価可能な仕組みを提示

■検討の視点

- 「情報セキュリティガバナンス導入ガイダンス」で提示されたフレームワークを参考に、経営目標・経営課題から情報セキュリティ対策項目を導くプロセスを想定
- モデル企業を想定し、上記のプロセス（仮説）を適用して、その実用性を評価



リスク管理方針と目的・目標の関係

（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）

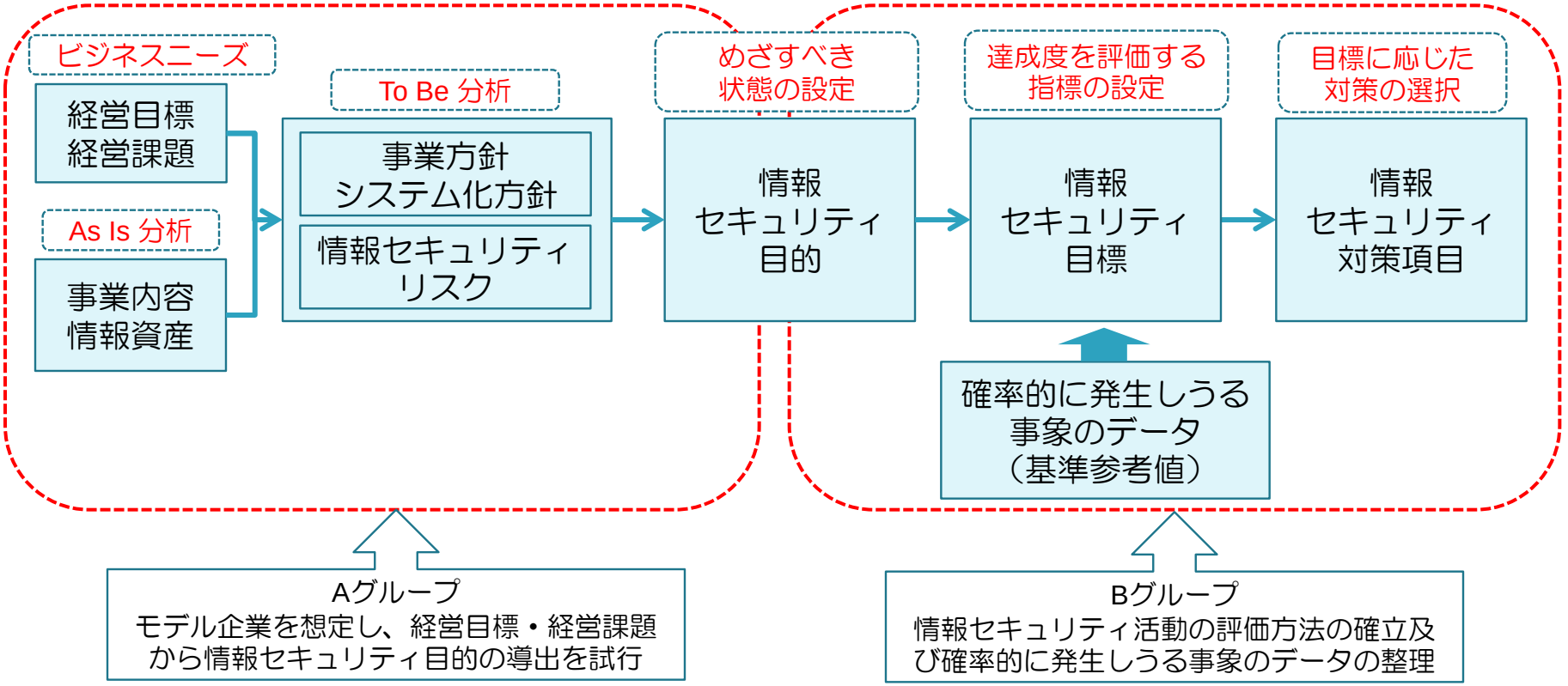
情報セキュリティ目的
リスク管理方針の実現に向けて、情報セキュリティ分野で達成すべき最終の状態（ゴール）

情報セキュリティ目標
情報セキュリティ目的を実現するために一定の時間内に達成すべき状態（マイルストーン）。達成度を計測する指標値として明確化

4. 全体構成　(3) 検討方針

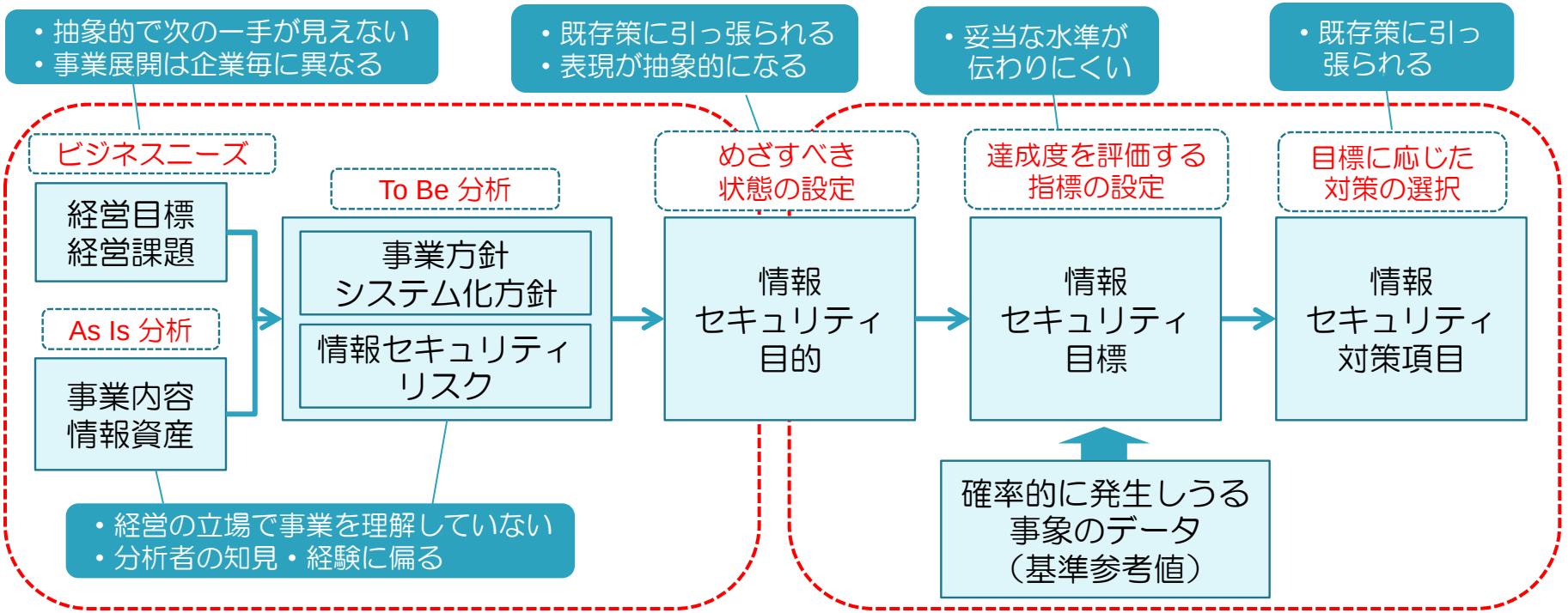
■ **検討方針・体制**

- 基本的な考え方に基づき、経営目標・経営課題から情報セキュリティ対策項目に連なるフローを設定、各工程を具体化することで、各社が参考にできる考え方を示す
- フローを上流・下流の2つに分け、それぞれ検討グループを設置する



試しに検討してみると・・・

- 簡単に一般化・定式化できるものではない



- ある程度具体的なイメージがないと議論が難しい ⇒ 「モデル」を設定して論点を具体化する

5. モデル企業の設定

ISGA
Information Security Governance Association

・各工程の具体化を図るため、モデル企業（百貨店A社）を設定し、その経営課題や事業方針を策定した。

■モデル企業A社の設定
・大手小売業
・老舗、ブランド力あり
・アジアを中心に海外店舗を展開
・顧客情報の保護を重要視
・顧客情報を活用した新たな展開にも関心あり

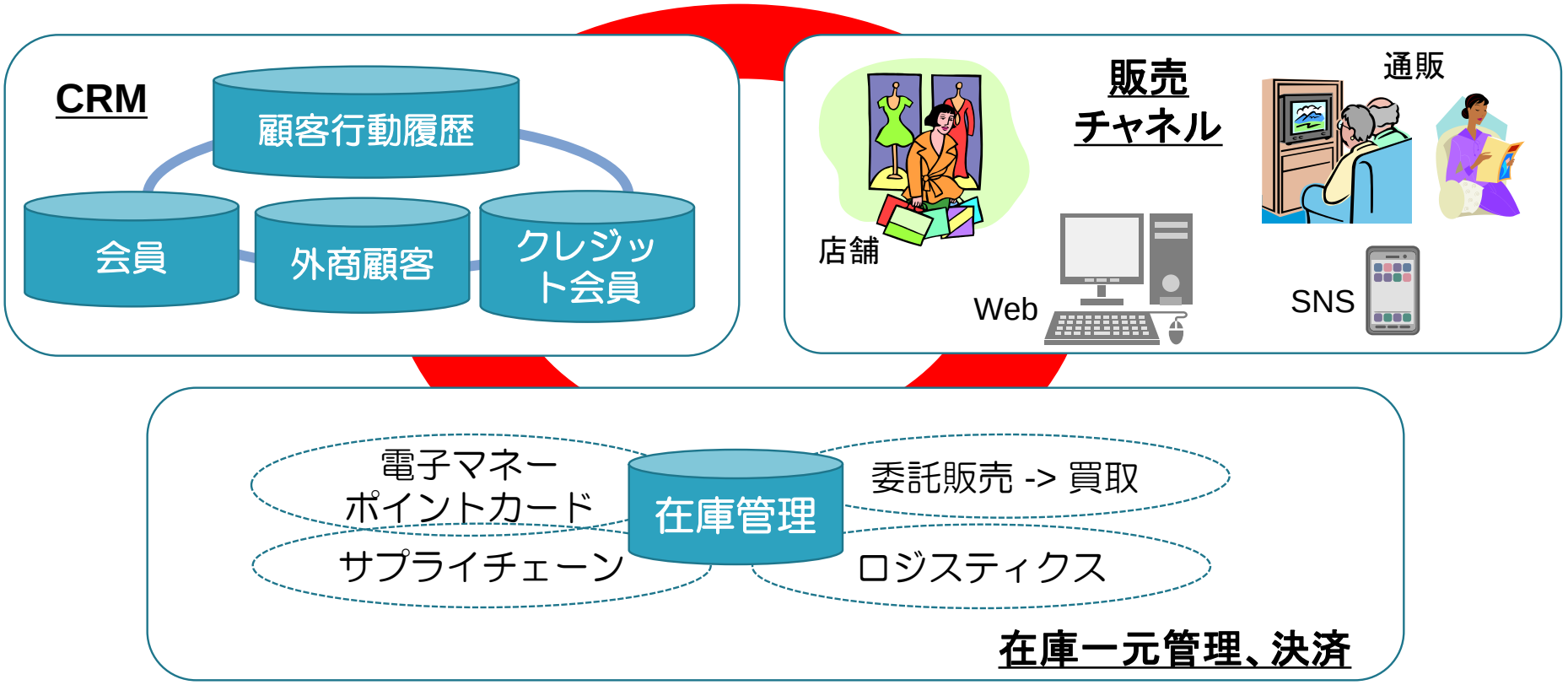
■業界を取り巻く環境
- 若者による百貨店離れの進行、郊外型のショッピングモール・アウトレットの台頭など厳しい市場環境
- 各社は生き残りをかけ、再編や改革に向けた取組みに着手

■経営課題
①店舗の補完機能の整備
・来店顧客の高齢化への対応
・遠距離顧客のロイヤリティ維持
②アジア富裕層の獲得
・ブランドイメージの浸透
・「安心・安全」のセールスポイント化

■事業方針
(a) オムニチャネルの展開
・販売機会の多面的拡大
・ターゲティング×チャネル×商圏
(b) 顧客行動分析
・購入商品や行動の把握→潜在ニーズの掘り起し
・来店頻度に応じた販売促進策の実施
・多様なデータを組み合わせて利用できる統合環境
(c) 海外商圏の本格展開
・国内店舗の営業ノウハウの現地展開
・海外拠点における情報活用の自由度向上

（参考）オムニチャネルとIT

- オムニチャネルとは、実店舗やネットショップ等の販売チャネルや流通チャネルを統合し、どのような販売チャネルからも同じような利便性で商品を購入できる環境を実現すること。
- オムニチャネルにおけるITの役割として、あらゆる顧客接点から同質の利便性を有する注文・購入環境、顧客情報の統合管理、在庫や決済、流通の一元管理などの方向が挙げられる。



6. 経営課題と対応方針

- 経営目標に基づき経営課題を抽出、対応方針を明らかにする。

オムニチャネル展開に関する課題と対応方針

課題	対応方針
店舗・チャネル単位の販売実績で評価するため、オムニチャネル展開に協力が得られない	• 評価体系の見直し • 顧客情報の一元化 • データウェアハウスによる横断的分析
商品別に在庫引当や受発注の仕組みが異なるため、横断的な適性在庫の確保が困難	• 委託販売商品の自社在庫管理への切替え • 在庫管理システムの統合、DWHとの連動
顧客ニーズに合わせた商品の紹介など適切な広告宣伝活動ができていない	• 顧客ニーズに応じた広告宣伝活動 • 顧客ニーズを把握する情報インフラ整備

アジア圏富裕層に向けた外商モデルの展開に関する課題と対応方針

課題	対応方針
従来、海外店舗には外商部門がなく、進出国での設立が急務	• 外商要員の現地採用、アウトソーシング • 顧客管理システム、外商管理システムの機能強化

7. 情報セキュリティ目的

ISGA
Information Security Governance Association

- システム化方針とITリスクから情報セキュリティ目的を設定する。

システム化方針	想定される 情報セキュリティリスク	情報セキュリティ目的
オムニチャネル展開を見据えたデータ統合の実現	データガバナンスの欠如による不適切なデータ更新及び参照	各情報の管理区分、管理者、利用者の明確化し、不適切な扱いがなされないよう管理を徹底する
販売チャネルとしてのインターネットの積極活用	インターネットを経由した個人情報、クレジットカード情報等の漏洩及び盗難	インターネット経由で授受および発信する情報について、厳格に情報管理レベルを定め、それにあわせた適切なセキュリティレベルを定義する
海外拠点での重要情報の活用の促進	海外拠点の現地職員、業務委託先での不適切な機密データの取扱	海外拠点の現地職員や外部委託先に対してA社の情報セキュリティ関連規程の遵守を徹底する

※通常は、事業方針に対して現行のシステムを評価し、
必要なシステムイメージを明確化

8. 情報セキュリティ目標　(1) フレーム

ISGA
Information Security Governance Association

- 情報セキュリティ目的が達成すべき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（当年度）		
データガバナンスの欠如による不適切なデータ更新及び参照	各情報の管理区分、管理者、利用者の明確化し、不適切な扱いがなされないよう管理を徹底する	現行の職務分掌にあわせたデータ管理ルールをユーザに浸透させる	＋	達成指標
		データ管理者（データオーナー）が各所管データの利用状況、取扱状況を適宜モニタリングし、報告する	＋	達成指標
インターネットを経由した個人情報、クレジットカード情報等の漏洩及び盗難	インターネット経由で授受および発信する情報について、厳格に情報管理レベルを定め、それにあわせた適切なセキュリティレベルを定義して管理する	インターネット経由で情報を授受するシステムの管理レベルを定めて実施することにより、不正アクセス等による情報漏えい及び盗難を防止する	＋	達成指標
		自社SNSでの情報発信について、発信プロセスの整備及びモニタリングを行い、不適切な情報の流出を防止する	＋	達成指標
海外拠点の現地職員、業務委託先での不適切な機密データの取扱	海外拠点の現地職員や外部委託先に対してA社の情報セキュリティ関連規程の遵守を徹底する	現地職員、外部委託先へのセキュリティ関連規程の遵守徹底により機密情報の漏えいを防止する	＋	達成指標
		各事業部門の責任者と拠点責任者が遵守状況を適宜モニタリングし、適宜経営陣に報告する	＋	達成指標

8. 情報セキュリティ目標　(2) 達成指標①

ISGA Information Security Governance Association

- 情報セキュリティ目標の達成指標を、サンプルー覧を参考にして選び、自社に合うよう手を加える（インシデント抑制目標）

想定され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（当年度）（達成指標）	（算出方法）	（基準値）
インターネットを経由した個人情報、クレジットカード情報等の漏洩及び盗難	インターネット経由で授受および発信する情報について、厳格に情報管理レベルを定め、それにあわせた適切なセキュリティレベルを定義して管理する	インターネット経由で情報を授受するシステムの管理レベルを定めて実施することにより、不正アクセス等による情報漏えい及び盗難を防止する	PCのウイルス感染発生率 ＝ （PCウイルス感染の年間報告件数）／（全PC台数）	○%以下
			サーバの不正アクセス被害発生率 ＝ （不正アクセスによるデータ漏洩・改ざん・消失等の実際の被害が発生したサーバ数）／（全サーバ台数）	○%以下
		自社SNSでの情報発信について、発信プロセスの整備及びモニタリングを行い、不適切な情報の流出を防止する	自社SNSでの不適切な書き込み実施率 ＝ （管理部門に報告された不適切な書き込み発生件数）／（全従業員数）	○%以下

情報セキュリティ目標
サンプルー覧
（インシデント抑制目標）

分類				インシデント	目標（指標）	算出方法
情報システム的脅威	偶発			トラフィック／処理の過負荷、容量オーバー	サービス停止率	（自社で提供している特定サービスについて稼動率等のSLAが存在する場合。免責の事由による停止を除く） ・年間のサービス停止時間／1年間 （※免責の事由による停止時間は除外）
				HW障害、SW障害、NW障害		
	人為	アクセス権限なし		コンピュータウィルス等の悪意あるソフトウェア	PCのウイルス感染の報告回数	感染報告件数／全PC数
				DDoS攻撃	（目標例なし）	（目標例なし）
				不正アクセスによる改ざん・破壊	サーバへの不正アクセス被害件数	不正アクセスにより実際の被害（データ漏えい・改ざん・消失等）の発生数を0件にする
				不正アクセスによる漏洩		
		アクセス権限あり	故意	情報の改ざん・破壊	（目標例なし）	（目標例なし）
				無許可の利用者・不正な方法でのリソース使用	社用PCの私的利用件数	（ゲーム等私的目的のソフトウェアのインストール、私的目的のウェブアクセス、等を検知できる場合） ・私的目的でのIT利用に関する警告or処分件数／全従業員数
				ソフトウェアや外部サービスの違法な使用	ソフトウェアライセンス違反率	・Adobe Acrobatについて、PC棚卸しの結果、発見されたライセンス違反の導入数／Adobe Acrobatがインストールされ ているPC数
					不正ソフトウェア導入率	（会社でインストール禁止ソフトウェアを定めている場合。例：P2Pファイル共有ソフト、価値できないフリーソフト、等） ・PC棚卸しorIT資産管理ソフトでのチェックの結果、会社で禁止しているソフトウェアをインストールしていたPC数／全PC数
				電子メール等通信経由の情報漏えい	情報の不正送信数	・内部者が外部に情報を持ち出したと思われる事故件数／全従業員数
					メールの誤送信数	（メール誤送信をしたら報告が管理部門にあがる仕組みになっている場合） ・年間のメール誤送信報告数／全社員数
					FAXの誤送信数	（FAX誤送信をしたら報告が管理部門にあがる仕組みになっている場合） ・年間のFAX誤送信報告数／全社員数
					掲示板・ブログ・SNS・ツイッター等での情報漏えい数	（業務時間中・業務外を問わず、SNS等で不適切な書き込みをした／書き込みを発見したら報告が管理部門にあがる仕組みになっている場合） ・年間のSNS等での情報漏えい事故報告数／全社員数
			過失	システム利用時のミス	（目標例なし）	（目標例なし）
				システム運用時のミス	（運用・変更のミスに関する）サービス停止率	自社で提供している特定サービスについて、運用・変更作業のミスによる年間のシステム停止時間／1年間 （※運用・変更ミス以外での停止時間は除外）
				システム変更時のミス		

サンプルー覧から当てはまる指標を選択
（必要に応じ自社に合うようカスタマイズ）
OR
サンプルー覧を参考にしてオリジナルの達成指標を作出

8. 情報セキュリティ目標　(2) 達成指標②

ISGA Information Security Governance Association

- 情報セキュリティ目標の達成指標を、サンプルー覧を参考にして選び、自社に合うよう手を加える（対策実施目標）

想定され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（当年度）	（達成指標）	（算出方法）	（基準値）
海外拠点の現地職員、業務委託先での不適切な機密データの取扱	海外拠点の現地職員や外部委託先に対してA社の情報セキュリティ関連規程の遵守を徹底する	現地職員、外部委託先へのセキュリティ関連規程の遵守徹底により機密情報の漏えいを防止する	海外拠点におけるセキュリティ規程整備率	（情報セキュリティ規定を策定済みの海外拠点数）／（全海外拠点数）	○%以下
			海外拠点における情報セキュリティ研修実施率	（全海外拠点における情報セキュリティ研修受講者数）／（全海外拠点の従業員数）	○%以下
			海外拠点における文書分類ルール遵守率	（内部監査時に重要情報書類のうち「重要」ラベルが貼付されていた数）／（内部監査時にラベル有無を確認した書類の総数）	○%以下
			海外拠点における情報保管場所の施錠ルール遵守率	（定期点検時に重要情報保管キャビネットのうち施錠されていた数）／（定期点検時に確認した重要情報保管キャビネットの総数）	○%以下
		各事業部門の責任者と拠点責任者が遵守状況を適宜モニタリングし、適宜経営陣に報告する	海外拠点での定期点検実施率	（当該年度中に自己点検の実施報告を上げた海外拠点数）／（全海外拠点数）	○%以下
			海外拠点でのインシデント報告ルール浸透率	（海外拠点向けアンケートで「インシデント発生時の報告先は？」に正解した回答者数）／（全海外拠点の従業員数）	○%以下
			海外拠点におけるモニタリング報告の提出率	（対策状況・インシデント件数などを報告するモニタリング報告書を締切日までに上げた海外拠点数）／（全海外拠点数）	○%以下

情報セキュリティ目標
サンプルー覧
（対策実施目標）

対策分野	指標（指標）	算出方法（例）
マネジメント体制 例： 組織、体制、規程、PDAサイクル、など	各部署or全社でのセキュリティ関連会議の開催回数・参加率	・年間の情報セキュリティ委員会or マネジメントレビューの開催実績回数/計画回数 ・年間の情報セキュリティ委員会or マネジメントレビューに年間X回以上参加した委員数/全委員 ・各部署でのセキュリティミーティングに年間X回以上参加した従業員数/全従業員
	各部門での自己点検実施率	（各部署に年1回以上の自己点検or監査を実施する、というポリシーがある場合） ・年1回以上の自己点検or監査を実施した部署数/全部署数
	国内外のグループ会社におけるセキュリティ管理体制の整備率	・セキュリティ規定を策定済みのグループ会社数/全グループ会社数 ・セキュリティ担当部署or担当者を設置済みのグループ会社数/全グループ会社数
物理的対策 例： ICカード入退システム、社員証着用、施錠設備、監視警備、など	保管場所の施錠率	（重要情報の保管されている施設・キャビネット・ロッカー等は常時施錠するポリシーの場合） 重要情報の保管されている施設・キャビネット・ロッカー等を定期点検で確認した結果、施錠されていた数/確認した施設・キャビネット・ロッカー等の数
	監視・警備導入率	（各地に多数の拠点があり、警備会社を導入するポリシーの場合） ・セコム等を導入している拠点数/全拠点数
人的対策 例： 教育、訓練、誓約書、など	不審メール訓練成績(開封率)	添付ファイル開封者数/訓練対象者数
	情報セキュリティ教育実施率	・受講者数/全従業員（役員・正社員・契約社員・派遣社員等の短期含む） ・部署別研修の実施部署数/全部署数 ※Eラーニング、集合研修、等
	情報セキュリティ標語の社内募集に対する応募率	・標語1つ以上出した部署数/全部署数
情報機器・媒体管理 例： PC・媒体の持ち出し管理、媒体の施錠管理、など	データ保管場所ルールの遵守率	（会社からの貸与PCの情報漏えいリスク軽減のため、不要となった重要情報はPCに残さず、サーバに保管するポリシーである場合） ・定期自己点検での管理者による目視チェックの結果、PC内に重要情報が長期保管されていたPC数/全PC数
	紙文書のラベリングルール遵守率	（重要情報には「重要」とラベル貼付するポリシーの場合） 監査でラベル貼付の有無を確認した結果、適守されていたキングファイル数/監査で確認したキングファイル総数
	PC持ち込みルール遵守率	（私物PCの無断持ち込みを禁止するポリシーの場合） ・年間で発見された私物PCの無断持ち込み件数（＝違反者数）/全従業員数

8. 情報セキュリティ目標　(2) 達成指標③

- 情報セキュリティ目標の達成指標に対して、達成判断の基準値を決める（基準参考値が参考になる）

情報セキュリティ目標（当年度）	（達成指標）	（算出方法）	（基準値）
インターネット経由で情報を授受するシステムの管理レベルを定めて実施することより、不正アクセス等による情報漏えい及び盗難を防止する	PCのウイルス感染発生率	＝（PCウイルス感染の年間報告件数）／（全PC台数）	0．5%以下
	サーバの不正アクセス被害発生率	＝（不正アクセスによるデータ漏洩・改ざん・消失等の実際の被害が発生したサーバ数）／（全サーバ台数）	0．0%以下
自社SNSでの情報発信について、発信プロセスの整備及びモニタリングを行い、不適切な情報の流出を防止する	自社SNSでの不適切な書き込み実施率	＝（管理部門に報告された不適切な書き込み発生件数）／（全従業員数）	1．0%以下

比較対象として参考になりそうな統計値を選択して、自社としての基準値を決める

自動車を運転して交通事故を起こす	1.1%（発生しうる事故）
搭乗予定の航空機が欠航する	1.6%（発生しうる事故）
住宅火災で死亡する	0.001%（許容できない事故）
交通事故で死亡する	0.003%（許容できない事故）
殺人に遭う	0.001%（許容できない事故）
SNSに不適切な書き込みをしてしまう	3.3%（よくおきる事故）

確率的に発生しうる事象のデータ（基準参考値）

ISGA
Information Security Governance Association

事件事故		年間の発生率	
災害	家が火事に遭う	0.02%	許し難い
	住宅火災で死亡する	0.001%	絶対許せない
	落雷で死亡する	0.000002%	絶対許せない
事故	自動車を運転して交通事故を起こす	1.1%	許したくないがありうる
	交通事故で負傷する	0.6%	許し難い
	交通事故で死亡する	0.003%	絶対許せない
	労働災害に遭う（死亡または休業４日以上の死傷）	0.2%	許し難い
	労働災害に遭い死亡する	0.002%	絶対許せない
サービス事故	搭乗予定の航空機が遅延する	7.25%	たまにはある
	搭乗予定の航空機が欠航する	1.62%	許したくないがありうる

事件事故		年間の発生率	
犯罪	窃盗に遭う	0.8%	許したくないがありうる
	詐欺に遭う	0.03%	許し難い
	殺人に遭う	0.001%	絶対許せない
病気	インフルエンザにかかる	11.0%	よくある
	がんで死亡する	0.3%	許し難い
ライフイベント	失業する	4.0%	許したくないがありうる
	離婚する	0.8%	許したくないがありうる

9. 情報セキュリティ対策項目

ISGA
Information Security Governance Association

- 達成指標の基準値をクリアして情報セキュリティ目標を達成するために、セキュリティ対策項目一覧より、達成指標に対応づく対策を実施する。

情報セキュリティ目標（当年度）

（達成指標）	（算出方法）	（基準値）
インターネット経由で情報を授受するシステムの管理レベルを定めて実施することより、不正アクセス等による情報漏えい及び盗難を防止する	サーバの不正アクセス被害発生率 ＝ （不正アクセスによるデータ漏洩・改ざん・消失等の実際の被害が発生したサーバ数） ／ （全サーバ台数）	0 0%

一般的なセキュリティ対策項目一覧（脅威×対策マトリクス）

達成指標に対応づけられた対策を確認して、自社で未実施／不十分な対策について実施計画をたてる

			物理的脅威						情報システム的脅威				
			偶発		人為				偶発		人為		
					アクセス権限なし		アクセス権限あり				アクセス権限なし		
							故意 ＼ 過失						
			災害等（地震、洪水、落雷、火事、テロなど）	設備の事故（停電、断水、空調故障、ケーブル損傷など）	不正な立ち入りによる持ち出し・盗難	（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	端末、媒体の移送時の紛失、盗難、破損	トラフィック／処理の過負荷、容量オーバー	HW障害、SW障害、NW障害	コンピュータウイルス等の悪意あるソフトウェア	不正アクセスによる改ざん・破壊	不正アクセスによる漏洩
		機密性			X	X	X	X	X	X	X	X	X
		完全性	X		X	X	X	X	X		X	X	
		可用性	X	X	X	X	X	X	X	X	X	X	
対策分野	No.	大問	小問数										
Ⅱ．人的・物理的対策	8	従業員の入社・退職に関わる情報セキュリティ対策がありますか。	2					サーバ ネットワーク PC モバイル機器 電子媒体 紙媒体					
	9	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。	9	サーバ ネットワーク	サーバ ネットワーク								
	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。	4			PC 電子媒体 紙媒体	PC 電子媒体 紙媒体	PC 電子媒体 紙媒体					
	11	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。	6			サーバ ネットワーク	サーバ ネットワーク	サーバ ネットワーク					
Ⅳ．アクセス管理	22	PCにログインできる人を制限していますか。	8									PC	PC
	23	システムのユーザID・アクセス権を管理していますか。	14								サーバ	サーバ	サーバ
	24	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。	13								サーバ	サーバ	サーバ
	25	重要なネットワーク機器(ファイアウォール、ルータ、スイッチなど)の設定画面にログインできる人を制限していますか。	3									ネットワーク	ネットワーク
Ⅴ．不正侵入対策	26	コンピュータウイルス対策を実施していますか。	8								サーバ ネットワーク PC	サーバ ネットワーク PC	サーバ ネットワーク PC
	27	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。	4								サーバ	サーバ	サーバ
	28	脆弱性を連時に把握し、対応するための仕組みを整備していますか。	5								サーバ PC モバイル機器	サーバ PC モバイル機器	サーバ PC モバイル機器
	29	システムの脆弱性診断を実施していますか。	3								サーバ	サーバ	サーバ
	30	システムを開発・導入および運用に関するルールを定めていますか。	5						サーバ	サーバ	サーバ	サーバ	サーバ
	31	システム障害の予防・復旧対策を実施していますか。	4						サーバ	サーバ			

対策項目No.23の詳細項目

①利用者1人に対して１つのID割当て
②利用者ID・アクセス権付与・変更・削除の承認手続き整備
③利用者のID・アクセス権を社員が一人で付与・変更・削除が行えない仕組み
④利用者の職務内容に応じた必要最低限のアクセス権付与
⑤異動・退職など不要になった利用者アクセス権の即時変更・削除
⑥利用者ID・アクセス権の定期見直し
⑦システム利用時のパスワード等による認証
⑧利用者パスワードの定期変更ルール
⑨利用者パスワードの強制的変更
⑩利用者パスワードの文字種制限
⑪利用者パスワードの文字数制限
⑫利用者パスワードの過去履歴に対する再使用制限
⑬無操作状態が一定時間続いた場合のパスワード入力要求
⑭ID・パスワードの入力試行回数制限

自社サーバで未実施 or 不十分な対策を選び、今年度の実施計画として策定する。

■サーバへの不正アクセスに関する対策項目（大問）

No.23：システムのユーザID・アクセス権管理
No.24：システムが稼働するサーバOSのログインユーザー制限
No.26：コンピュータウイルス対策
No.27：サーバ構築時の要塞化
No.28：脆弱性把握・対応の仕組み整備
No.29：システムの脆弱性診断
No.30：システムの開発・導入及び運用ルール制定
No.34：データのバックアップ取得
No.36：社内ネットワークのセグメント分割
No.39：サーバやシステム、ネットワークのログ取得

10. 今後の課題

■現行システムに関する情報セキュリティ目標の達成指標の設定
・価値創造に向けた新たな業務プロセスや将来のシステムではなく、現行のシステムに関する情報セキュリティ目標やその達成指標のあり方について検討する。

■モデルパターンの多様化
・対象業種を多様化して，今回と同様に経営目標・経営課題，事業方針・計画等から情報セキュリティ目的・目標を導出できるか検証することにより，様々な企業が参考にできるようにバリエーションを確保する。
・既存のシステムの運用や改善を対象とした場合の情報セキュリティ目的・目標はどのように設定すべきか，経営陣がリスク管理の方針を明確にしている場合にはどうすべきかなど，フォーカスのポイントやプロセスに関する多様化も検討が必要。

■情報セキュリティ目的の導出プロセスの確立
・ステークホルダーや経営陣が最も関心を寄せる事項である経営目標・経営課題から「情報セキュリティ目的」を導くためのプロセスを多くの企業で実践できるようにするための手法を確立する。

■経営方針・経営課題に直結しない情報セキュリティ活動の貢献度評価
・経営方針・経営課題には直結しないが，疎かにしてはならない情報セキュリティ活動も存在する。これらの情報セキュリティ対策にも，必要な予算を割り当て，経営層の指示を得て実施し，その成果を企業への貢献度として評価する枠組みが必要となる。