1　「情報」資産は企業に不可欠な経営資源

今や情報は、「人・モノ・金」以上に、企業にとって欠かせない経営資源であり、経営や戦略の意思決定に欠かせないものになっています。
ネットや業務で収集された情報（ビックデータ）は、営業活動やサービスの提供、商品の配送等さまざまな形で日常業務の中で利用され、さらには経営判断や経営戦略の策定に活用されます。
企業にとって価値のある「情報」資産を守り、経営目的を達成するための情報セキュリティ対策（マネジメントシステム）に取り組むことは、これからの企業にとって最重要課題となっています。

なぜなら・・・

（例１）　システム障害や不正アクセス等のセキュリティ事故によって、情報が使用できなくなった
→業業務が中断し、顧客や取引先に大きな迷惑をかけることになりかねない

（例２）　受注管理システムが停止してしまった
→注文を受け付けることができずにビジネスチャンスを逃す可能性がある

（例３）　組織の機密技術情報が海外に流出した
→ノウハウや技術流出により、得られるはずの利益を得られず、損失が出る

また、さまざまな原因で頻繁に起こっている情報漏えい事故ですが、事故を起こしてしまった場合は、企業は多大な損害を受けるばかりか、社会的信用までも失ってしまいます。

※「情報資産」と「資産」について
ISMSでは、これまで「情報資産」という表現を一般的に使っていましたが、情報そのものだけでなく、情報を取り扱う設備、人、プロセスなども組織にとっては重要な「資産」であると考え、最近では「資産」という表現を用いることが多くなっています。情報は組織の「資産」のひとつとして位置づけられています。
※本講座では、上記の考え方に基づき「資産」という表現を使用します。

2　個人情報流出・漏えい事件の事例

過去に起きた個人情報漏えいインシデント（事件・事故）の規模と事例です。

過去の大きな事故からの反省や、対策の整備等が行われた影響でしょうか、漏えい人数については2007年の大きな事故を境に下降傾向にあります。

しかし、これら統計は日本国内だけの統計のため、クラウド化したインフラやグローバル化した組織形態が進展している中では正確に把握しきれなくなっているのが現状です。

漏えいの原因については、従来から大きな変化はありませんが、トップ10の集計をみると、不正アクセス等の窃取行為以外の、管理ミス、誤操作、紛失・置き忘れ等の従業員（人）のうっかりミスや管理法の手違いを原因とするものが84.5%と大半を占めています。

これらはヒューマンエラーとしてとらえられますが、人的な対策として担当者へのセキュリティ教育を、そして、組織的な対策としてヒューマンエラーを減らす予防効果が期待できる仕組み・手順作りが重要だといえます。

情報セキュリティトラブルの主な原因

1） 携帯電話、スマートディバイスの紛失・置き忘れ（32.4%）
2） 電子メールの誤送信（27.1%）
3） ノートPCの紛失・置き忘れ（21.2%）
4） 社員証・入館証の紛失・置き忘れ（20.9%）
5） FAXの誤送信（19.7%）
6） 配送物の誤配または紛失（16.5%）
7） USBメモリ等の可搬記憶媒体の紛失・置き忘れ（13.8%）
8） 情報機器、物品類の盗難／窃取による情報漏えい（13.5%）
9） 業務書類の紛失・置き忘れ（11.6%）
10） 名刺類の紛失・置き忘れ（8.8%）

上場企業を中心とした3,000社の調査（2012年度）より

ヒューマンエラーは必ず起こることを前提として暗号化等の漏えい対策や、紛失しても被害が拡大しない対策も合わせて行うことを検討する必要があります。

今後はさらに、業務で利用されているスマートフォンなどのBYOD利用を原因とした情報漏えいやデータロスが増加すると考えられ、組織としての早急な対策が望まれます。

組織の許可を得ずに、私用のスマートデバイスを業務利用する「シャドーIT」による盗難や紛失のリスクは非常に高いことから、従業員は、いくら利便性が高いといっても自重しなければなりません。

大切なことは、その問題の本当の原因を究明し、真摯に対策をすることですが、根本原因として組織文化や風土、慣習等の影響が大きいのが現実です。マネジメントシステムによってリスクに強い組織への変革が望まれます。

2012年（上半期）個人情報漏えいインシデント　概要データ

漏えい人数	123万9,626人
インシデント件数	954件
想定損害賠償総額	347億9,865万円
一件あたりの漏えい人数	1,349人
一件あたりの平均想定損害賠償額	3,787万円
一人あたりの平均想定損害賠償額	5万7,710円

参考：「2012年　情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」
2013年4月30日／NPO 日本ネットワークセキュリティ協会

■ **三菱UFJ証券**（2009年4月）

システム部の幹部社員が顧客情報約149万件を持ち出し、そのうち約５万人分を名簿業者に売却。損失額は、70億円以上と試算されている（うち、５億円は、該当者に送られた１万円のギフト券の総額）。また、本事件で逮捕・起訴された三菱UFJ証券の元社員の容疑は、「不正アクセス禁止法違反」と「窃盗」であった。現行法では、電子データは窃盗罪の対象にならないため、顧客データを格納したCD（物品）の盗難に対しての容疑となった。

■ **アリコジャパン**（2009年7月）

外資系生命保険大手アリコジャパンのホストコンピュータに置かれていたカード情報ファイルが抜き取られ、クレジットカード情報約１万８千人分が流出。ホストコンピュータに対し、業務委託先企業の社内コンピューターから不自然なアクセス履歴があったことが判明したことから、委託先社員が不正に持ち出した可能

性が大きいとされている。

■ **アミューズ**（2009年8月）

大手芸能プロダクションのアミューズの通販サイト「アスマート」で商品を購入した顧客情報のうち、クレジットカード情報３万4988件、メールアドレス11万6911件が流出。「アスマート」の運営を委託されていた業者のサーバに中国から不正アクセスがあり、データベース上の個人情報が流出した恐れがあるとされている。

■ **陸上自衛隊**（2009年8月）

陸上自衛隊の隊員が、隊員の個人情報ファイル「隊員出身地カード」のデータ約14万人をCDに複製し、都内の不動産業者に売却。「隊員出身地カード」には隊員本人の氏名、性別、生年月日、所属、階級、出身校などのほか、親などの氏名、住所、電話番号、子どもの氏名、生年月日、学校名などが記載されていた。

■ **デジタルダイレクト**（2009年9月）

三菱商事の子会社、デジタルダイレクトが運営する２つの通販サイト「saQwa（サクワ）ネットショッピング」と「fun style shopping（ファンスタイルショッピング）」が、海外からの不正アクセスを受け、両サイトにアクセスしたことがある顧客のクレジットカード情報やメールアドレスなどの個人情報約5万2000件が流出。

■ **ソニー**（2011年4月）

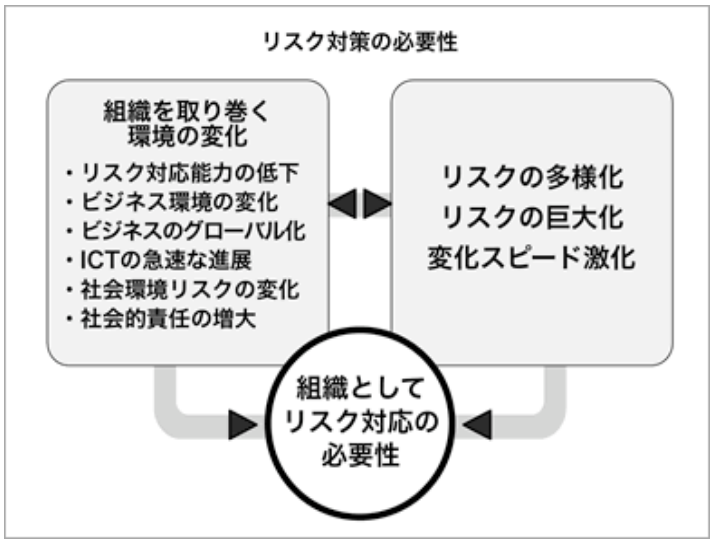
プレイステーション３（PS３）とプレイステーション・ポータブル（PSP）のネットワーク接続「プレイステーションネットワーク（PSN）」の不正アクセスにより、全世界で7700万件、日本で743万件ものPSN利用者の個人情報が流出。氏名や住所、性別等の基本的な情報の他、パスワード、クレジットカード番号、購入履歴等も流出の可能性があると発表された。記録としては過去最悪の件数であり「プレイステーションネットワーク（PSN）個人情報流出事件」と呼ばれている。

■ **ベネッセ**（2014年7月）

ベネッセコーポレーションが最大約2,070万件の顧客情報が漏えいした可能性があると発表した。調査の結果、原因はデータベースのアクセス権を持つ関係者（再委託先システム技術者）が名簿業者への売渡目的で窃取したことがわかった。システムの委託先は、ISMS（情報セキュリティマネジメントシステム）やPMS（プライバシーマーク）を取得していたにもかかわらず本事件が起きたことは、認証や認定を取得しているというだけではなく、マネジメントシステムを継続的かつ有効に機能させていたかが問われる。また、IT業界特有の委託や派遣を多用する慣習の中で、社内だけではなく、外部委託先や派遣社員においても、十

分な配慮・対策がされていたかが問題となる。そしてベネッセや情報流用した組織も、倫理的な問題だけではなく、営業活動も制限され、大きく株価を下げる等の事態が発生した。

3　今、なぜ情報セキュリティが必要なのか



【法令規制等の順守（コンプライアンス）要求】

順守については、法令規制の範囲さえ逸脱しなければ問題ないということではなく、社会的責任にも配慮した組織・人としての正しい倫理観。そして組織の風土（文化）として醸成していくことが大切です。

・個人情報保護法

2005年４月の個人情報保護法の完全施行の影響もあり、情報セキュリティ事故がメディアで大きく報道されていることからも分かるように、情報セキュリティ問題に対する社会的な関心は年々高まっています。

企業間でも、情報の機密性の確保が要求されるようになってきており、プライバシーマークやISO27001（ISMS）といった審査機関等による第三者評価制度の認定を受けていることを取引の条件としたり、取引先査定の条件とする企業も増加しています。

また、第三者認証の取得を義務付けないまでも、自社独自の情報セキュリティ基準を明確に打ち出し、取引先に対する具体的なセキュリティ要求事項の提示や監査を通して、取引先の格付けを行なう企業も出てきました。

・不正競争防止法（技術情報／営業秘密の流出）

最近の事案では、日本企業のスマートメモリの機密技術情報が、関連事業所で働いていた技術者によって海外の競合他社に本人の就職というカタチで流出しました。不正競争防止法で規制対策されているにもかかわらず、国内の技術情報が退職者によって持ち出されるという事件が多発しています。しかし、法の度重なる改定強化にもかかわらず、組織において効果的な対策ができていないのが現状です。

・契約上のセキュリティ義務

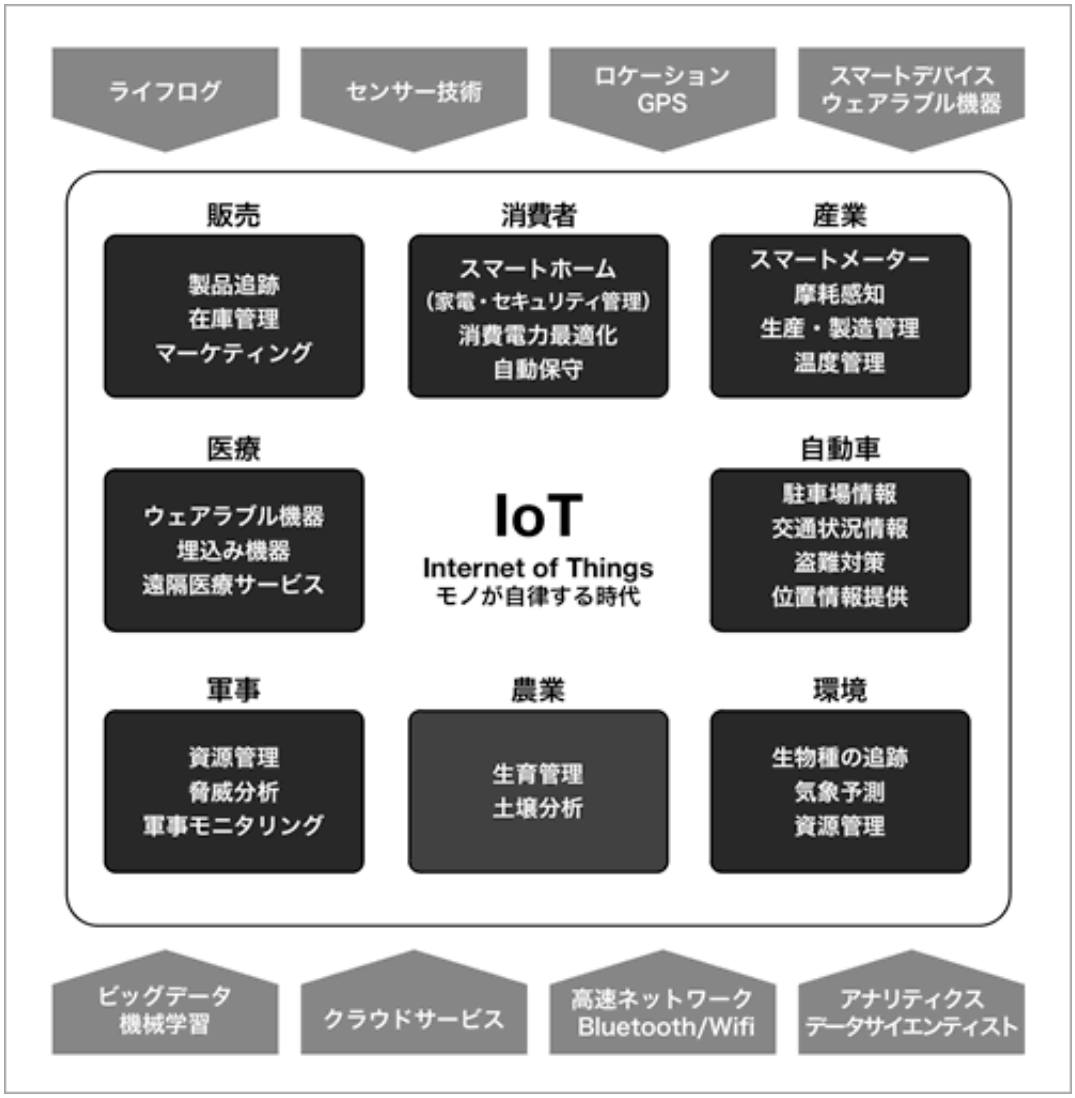
利害関係者（顧客や従業員を含む）との契約の中で取り決められ、約束されるセキュリティ保護要求（機密保持契約や個人情報保護等）を確実に履行する必要があります。

【環境の変化】

・ICTの進展による社会環境の変化

ICTの進展スピードは早く、近年のスマートデバイス（スマートフォンやタブレット、ウエアラブル機器等）の普及とSNS（ソーシャルネットワーク）の広がりによって様々なコミュニケーションが行われることになり、飛躍的に情報量が増加し、ビックデータ時代といわれています。そしてその活用効果は、2012年には日本国内の全産業で売上高を61兆円（総務省）押し上げたと分析されています。

また、医療、自動車、住環境を含むさまざまな場所や生活で利用される機器がネットワークにつながり、より利便性を高めようとするIoT（Internet of Thing）化に向けて時代は急速に進んでいます。



しかし、それらの情報の中には、プライバシー（個人情報、健康情報、行動等）にかかわり、他者には知られたくない情報も多く含まれます。また、それらの機器がコントロールができなくなる可能性もあります。もちろん、サイバーテロや悪用されることで、個人だけではなく社会的に大きなリスクが存在することになります。

・リスクの多様化

このように、ICTによる利便性の影には、必ず大きなリスクが存在することを忘れてはなりません。ビックデータ、クラウドサービス、モバイル、SNS、IoTこれらの進歩を

背景として、今までにない新しいリスクも数多く発生する可能性があります。

新聞やテレビのニュースを賑わすような重大なセキュリティトラブルはどこの企業でも起こる可能性があり、程度の差はあれ、あらゆる企業に情報セキュリティに関するリスクは存在します。とくにICTの急速な進化によって、そのリスクは拡大し続けていることを忘れてはなりません。

しかし、日々起こっている、情報セキュリティ事故等の原因を調査すると、人的要因の事故が多くの割合を占めていることがわかります。ヒューマンエラーとして片付けてしまうわけにはいきません。本当の原因を究明し、有効な再発防止策を実施していくことが必要です。

いままでは、従業員１人あたり１台のパソコンや電子機器を利用する程度でした。しかし、現在は、自宅のPCだけではなく、スマート機器（スマートフォンやタブレット等）を複数持ち、さまざまな場所で業務利用することが一般的になってきました。
2020年には、一人当たり6.58台のインターネットデバイスが接続されると予想されています。

そして今、個人デバイスを業務利用するBYOD（Bring Your Own Device）という利用形態が進行しています。組織から正式に個人所有機器の業務利用について許可されていないにもかかわらず、勝手に利用するいわゆる「シャドーIT」も増加する中、情報流失や喪失に関するリスクはいままでになく、大きくなっていると言わざるを得ません。

ネットワーク環境や機器の発展とともに、従業員一人ひとりが重要なデータをどこでも、すぐ利用できる環境になっていますが、個人の不注意が引き起こすセキュリティトラブルが、ネットワークを介して組織全体や外部にまで大きな影響を及ぼし、収拾がつかない事件・事故が多発しているのが現状です。

したがって・・・

→情報セキュリティに関するリスクを放置しておくことは企業の存続をも脅かしかねない問題であり、さらにサプライチェーンや多くの利害関係者から組織的な対策が要求されています。

→現在のICTに依存した社会環境を見ると、大企業、中小企業、国内、海外、業種を問

わず、情報セキュリティ対策はビジネスを行っていく上で、必須の要件となっています。

→しかし多くの中小企業では、環境変化への対応が柔軟的にできず、情報セキュリティ対策が不十分な企業も多い中、率先して情報セキュリティ対策に取り組むことは他社との差別化を図ることにつながり、中長期的に見ると、マネジメントによる組織変革によってビジネスチャンスを拡大する可能性も秘めています。

これらの状況をみると、情報セキュリティに取り組むか否かは、これからの企業の生き残りをかけた課題となっていると言っても過言ではありません。

そしてこれからは、その場しのぎ的なセキュリティ対策ではなく、情報セキュリティマネジメントシステムとして組織的に取り組み、各々が多様に変化するリスクに対して情報リテラシー能力を高め、組織活動としての成熟度が評価される時代へと変化しています。

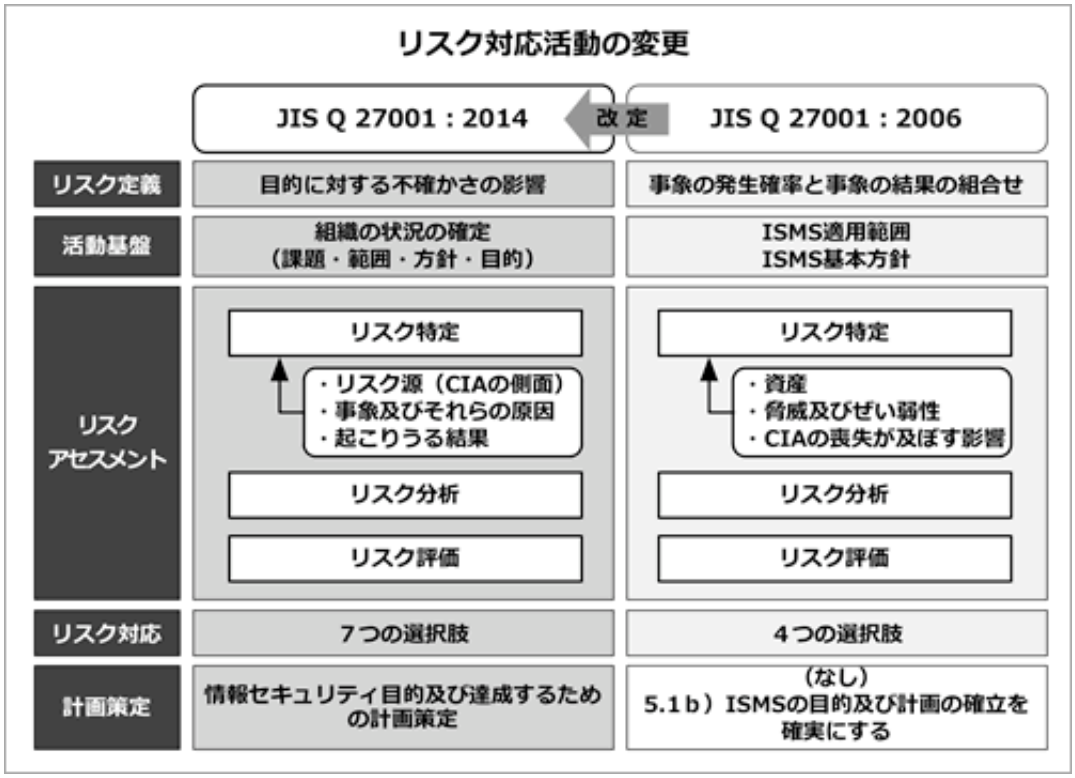
4 ISMS / ISO27001規格の改定

情報セキュリティ対策の重要性が高まる中、2005年にリリースされたISMS / ISO27001の規格が、2013年10月に改定されました。
日本国内では、JIS Q 27001：2014として2014年３月にリリースされました。

今回の改訂では、ISO補足指針によりマネジメントシステム規格の共通化が図られ、複数のマネジメントシステムを運用する組織が、システムの統合化をしやすいように意図されています。また、リスクマネジメントの原則的な考え方として共通の原則と指針（ISO31000）が採用されました。

このことは、ISMSにとっても影響を及ぼすこととなりました。

＜改定のポイント＞



（1）ガバナンス強化への取り組み（活動基盤）

まず、最初にマネジメントシステムに取り組む際に、「組織の状況」を理解し、確定することが要求されています。

組織の外部・内部の環境、そして、利害関係者の要求を十分把握し、組織の取り組みの目的を明確にすることが求められています。

そして、経営層によるリーダーシップによって、マネジメントシステムが組織の目的に沿って、事業プロセス全体に有効に機能することに重点が置かれました。

（2）事業プロセスとの統合（計画策定）

マネジメントシステムを組織全体のプロセスと統合することで、目的に対して各々の活動が乖離することがないことを要求しています。

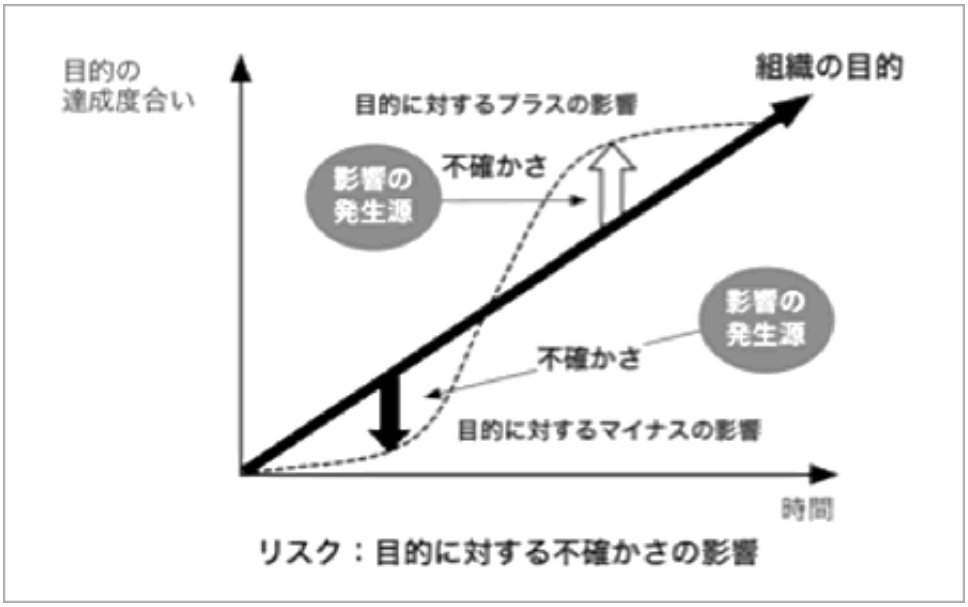
（3）リスク定義とリスクアセスメントの変化

リスクの定義が、従来の「事象の発生確率とその結果の組み合わせ」から、「**目的に対する不確かさの影響**」という考え方に変化しています。

これは、リスクというものが、目的に対して、マイナス（好ましくない）方向だけではなく、プラス（機会）の方向にも影響する「不確かさ」ということをあらわしています。いわゆる「予期せぬ成功」ということもリスクの範疇としてとらえることができる訳です。

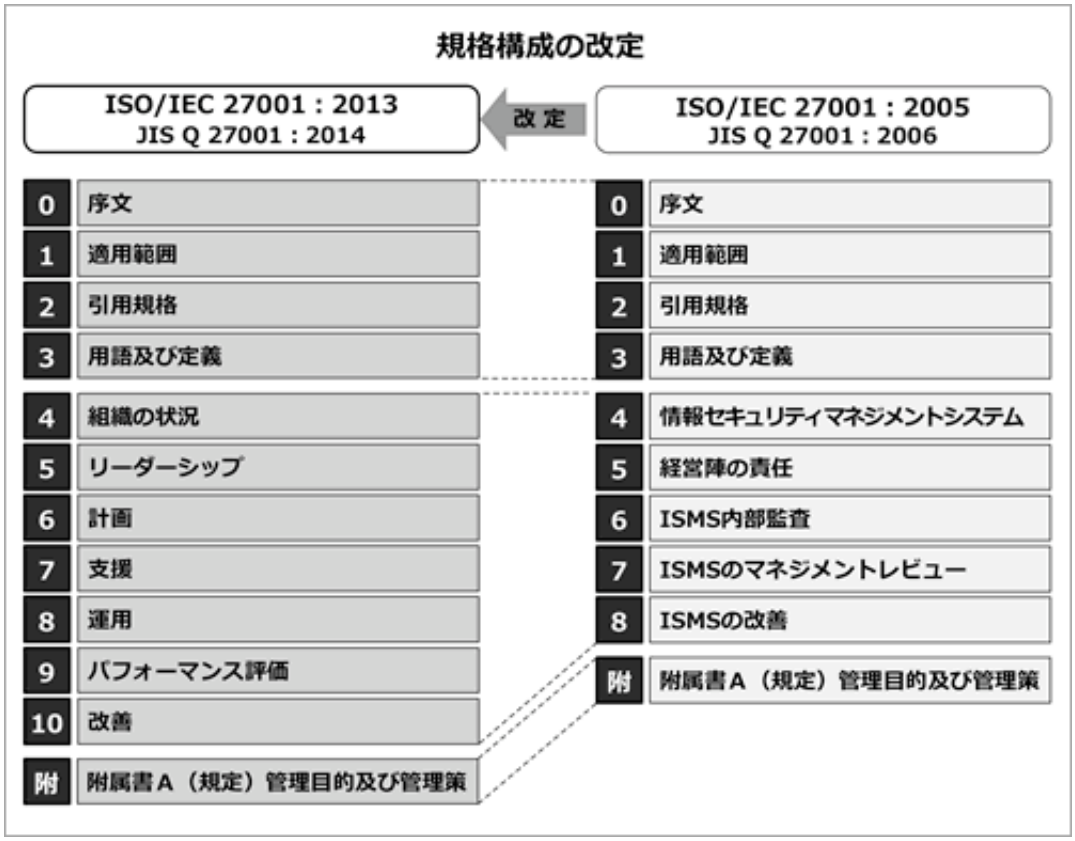
しかし、情報セキュリティにおいては、従前通りマイナス（負）のリスクをコントロールすることで、情報活用において支障をきたさないようにすることが主な活動となります。

よって、ISO27000の定義の中にあるように、「**情報セキュリティリスクは、脅威が情報資産のぜい弱性又は情報資産グループのぜい弱性に付け込み、その結果、組織に損害を与える可能性に伴って生じる。**」という今までの考え方が変わるわけではありません。



（４） 規格構成の改定

規格項目（箇条）が、MSS（Management System Standard）の導入で増え、要求項目は箇条４～箇条１０が必須事項となりました。



5　リスクマネジメントという考え方１（ISO31000）

リスクマネジメントの原則と指針がISO31000（2009年）という規格によって定義されていますが、この規格の原則と指針が、今回の改定に取り入れられました。

また、ISOのリスクマネジメントシステム（品質、環境、事業継続、食品衛生等）は、このISO31000の原則と指針のフレームワークとの整合性がとられることになりました。そしてリスクマネジメントの原則として、以下のように定義しています。

リスクマネジメントの原則

リスクマネジメントは・・・

- 価値を創造する
- 組織のすべてのプロセスにおいてカバーする
- 意思決定の一部として機能する
- 不確かさ（リスク）に明確に対処する
- 体系的かつ組織的で、変化に対応できる
- 利用可能な最善の情報に基づく
- 組織に合わせて作られている
- 人的および文化的要因を考慮に入れる
- 透明性があり、かつ、包含的である
- 動的で、繰り返し行われ、変化に対応する
- 組織の継続的改善および強化を促進する

このようにリスクマネジメントは、単にリスクを回避するというネガティブなものではなく、組織の目的に沿って柔軟的に取り組むことができ、企業価値を創造し、組織が継続的にリスクに対処することで、ビジネスを優位に導くものとしています。

また、このフレームワークは、「リスクマネジメント」および「リスクの運用管理」をカバーするための考え方として、

（１）リスクマネジメント：リスクを効果的に運用管理するための組織活動の仕組み（枠組みおよびプロセス）

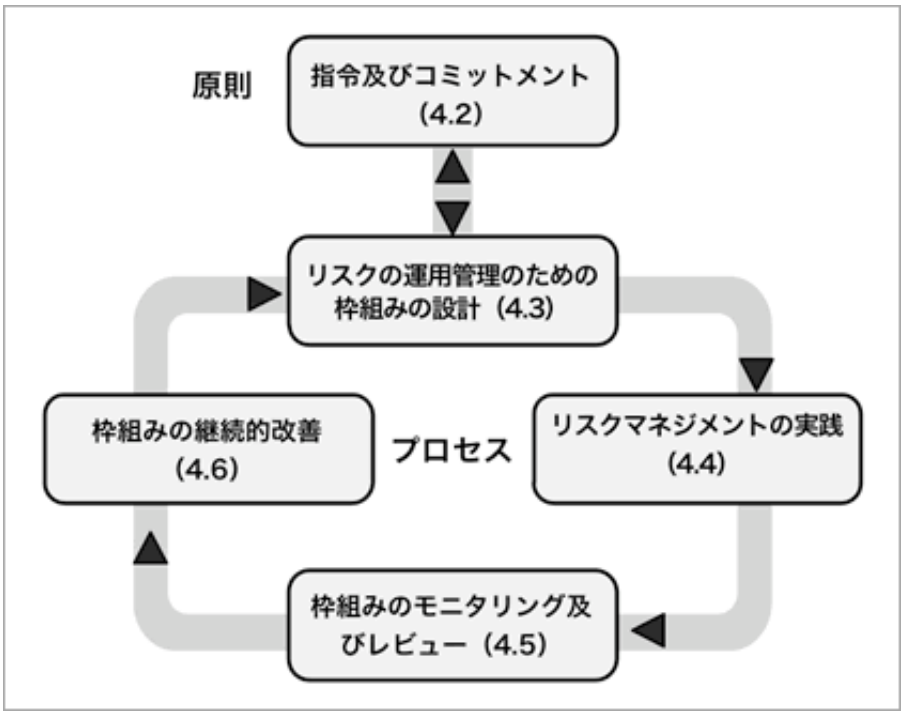
（２）リスクの運用管理：その構造を特定のリスクに適用するための方法

の２つの側面を持っています。

ISO 31000：2010のリスクの運用管理のための原則、それを取り巻く枠組み、およびリスクマネジメントプロセスの関係は、以下の図のようなプロセスアプローチ（PDCA）構造になっています。

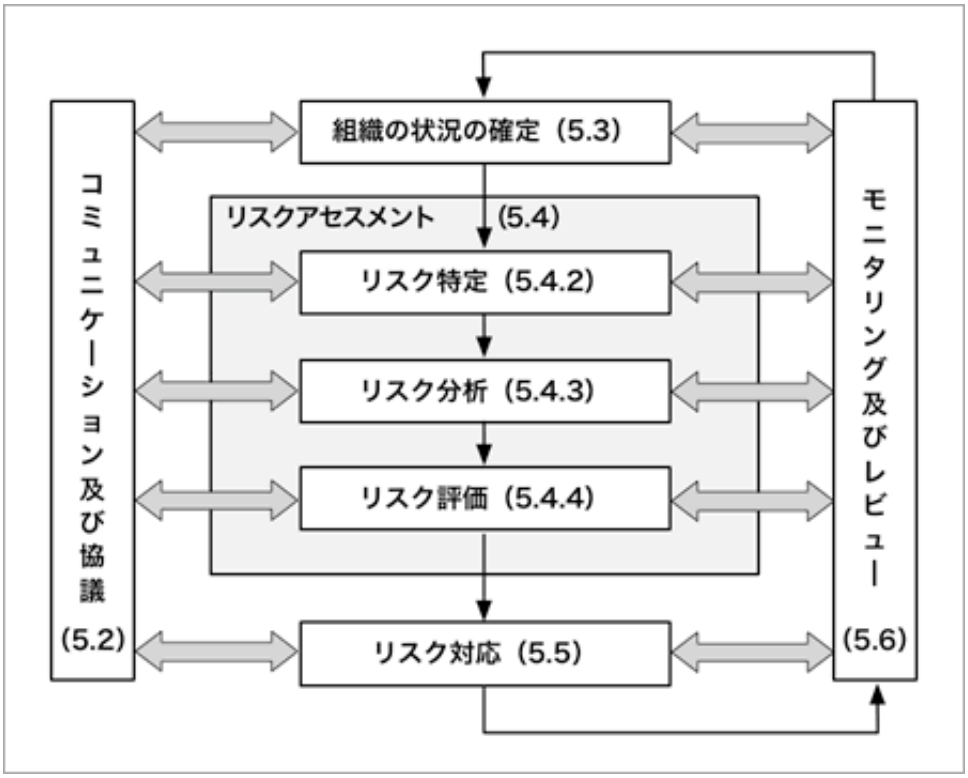
（１） 組織のリスクマネジメント活動プロセス

「指令及びコミットメント」を受けて、組織活動プロセスのPDCAが運用されます。



（２） リスク対応プロセス

そして、（１）の組織活動の中でリスクに対する取り組みである以下のプロセスが実施されます。



このように、組織のリスクマネジメントの仕組みとリスクに対する取り組みのプロセスの２層構造になっています。

情報セキュリティマネジメントシステム（ISMS）においても、マネジメントとしての組織の活動とリスクに対する取り組みについての２つの側面からとらえ、実践すること

で効果を上げることができます。

事業を妨げる阻害要因をコントロールするためのリスクマネジメントであり、経営理念の実現や目標を達成するために必要不可欠な事業戦略。

情報セキュリティ対策の重要性を頭では分かっていても、厳しい経済状況の中、貴重な時間と資金を使ってまでする必要があるのか？日常業務もしなければならないのに、情報セキュリティなんてお金にならないものに時間をとられるのは無駄！などと思う人もいるかもしれません。

たしかに、情報セキュリティの取り組みは直接的に企業に利益をもたらすものではなく、逆にある程度のコストが必要です。また、情報セキュリティ対策を確立するには時間がかかり、日常業務以外の仕事が一時的に増えることにもなるでしょう。

しかし、それでもなお、情報セキュリティに取り組む意義はあるといえます。それが企業の利益、目標の達成にもつながるからです。情報セキュリティは、経営理念の実現や目標を達成するために必要不可欠なビジネス上のリスクマネジメントです。

ISO31000では、この組織の目的（目標）に対して、まず最初に「組織の状況」を明確にすることを要求しています。このようにリスクマネジメントは、組織の目的達成を実現するために必要不可欠な取り組みとして設計されています。

そして、その目的は適切なリスクマネジメントによる企業価値の創造や顧客満足の獲得であって、情報セキュリティはあくまでも手段でしかないこと。

また、ISMSもガバナンス（組織の統治機能）を通じて、組織の目的を達成するための取り組みであり、情報セキュリティ対策することだけが目的ではないことを十分理解しなければなりません。