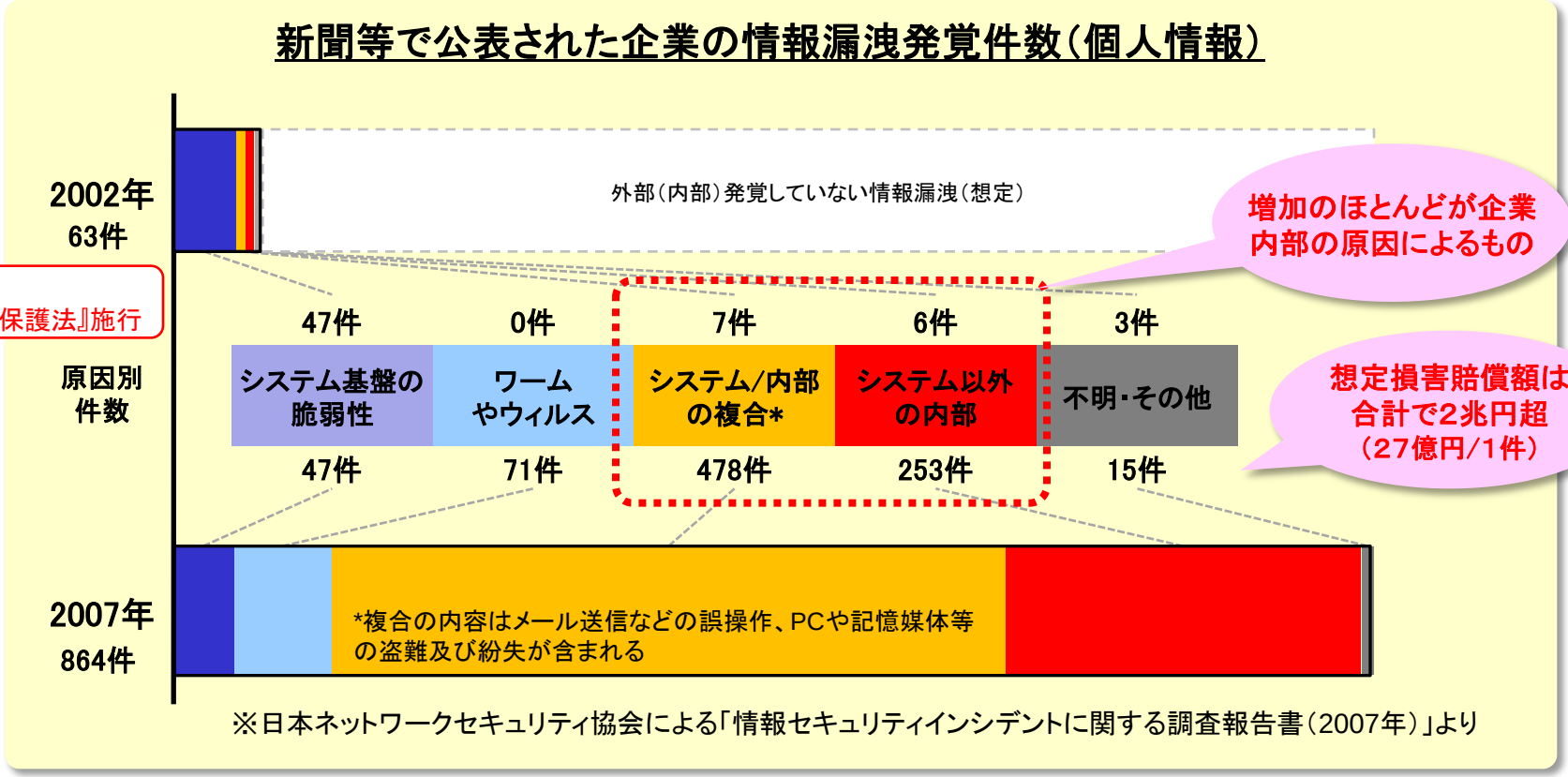
情報セキュリティリスク診断サービス
のご紹介

株式会社MONET
コンサルティング事業部

1. 企業情報漏洩事件の傾向とその要因

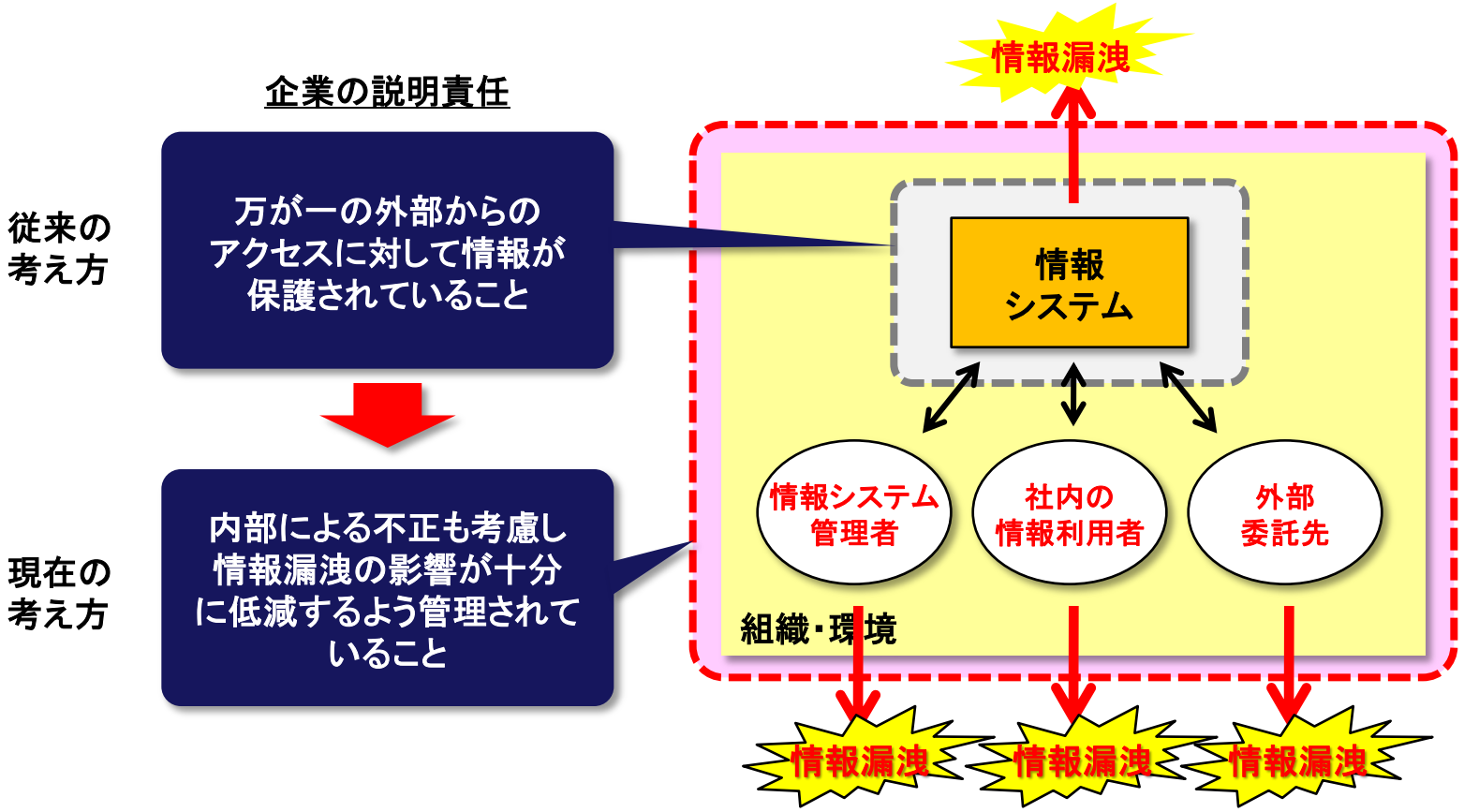
2003年の『個人情報保護法』施行後、新聞等に公表された企業の情報漏洩事件が増加しており、損害賠償等の企業の損失も看過できないほど増大しています。増加した情報漏洩事故は、企業の内部における管理上のミス・不正によるものがそのほとんどとなっています。



2. 情報セキュリティに関する企業の説明責任

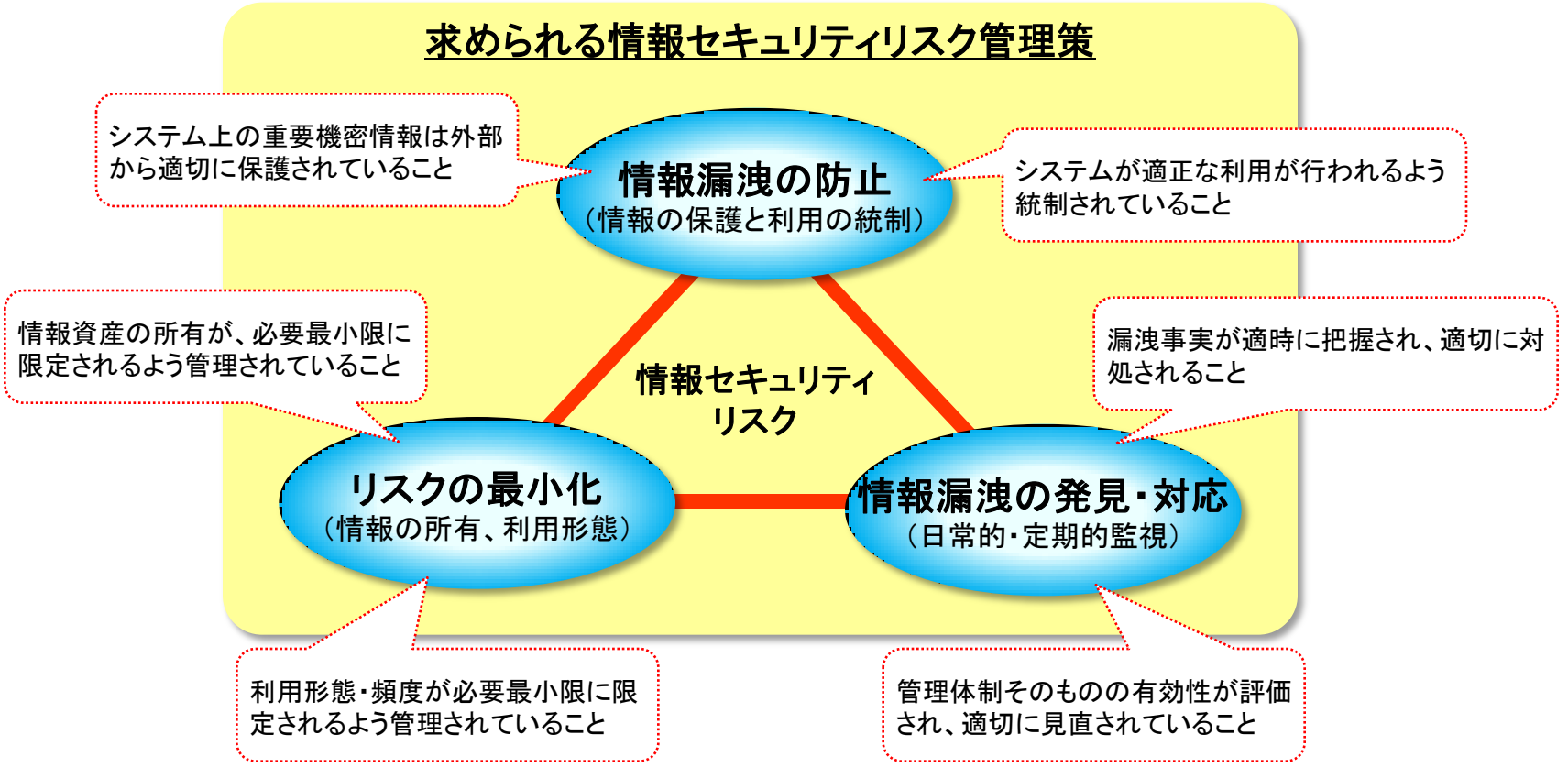
昨今においては、重要な情報が、外部から保護されていることだけではなく、企業の内部の要因 等によって“情報漏洩は起きるものである”という前提に基づき、企業は万が一情報漏洩が発生した際の影響を低く抑える努力を怠っていないことについて、顧客・ステークホルダーに対する説明責任を果たすことが求められています。

情報漏洩対策に対する企業責任の考え方の変化



3. 情報セキュリティリスク管理の考え方

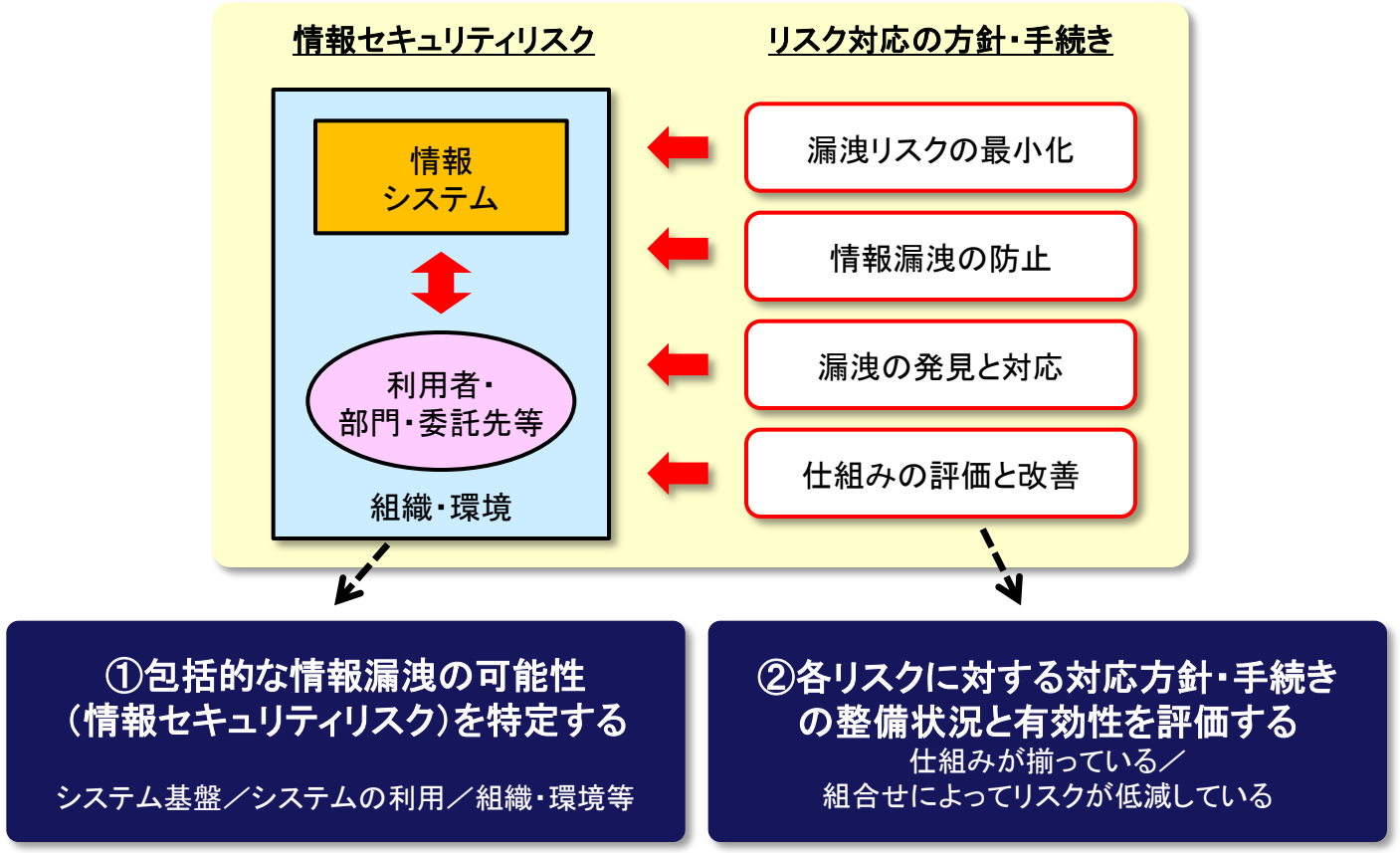
企業が情報漏洩による影響を十分に低減できていると言えるためには、情報セキュリティリスクの重要性に応じて、「情報漏洩の防止」「情報漏洩の発見・対応」「リスクの最小化」のそれぞれを目的とした対策がバランスよく連携して機能していることが保証されている必要があります。



4. 情報セキュリティリスク診断のフレームワーク

弊社の情報セキュリティリスク診断サービスでは、情報漏洩の可能性を「情報システム」「システムの利用」「組織・環境」のそれぞれの側面で特定し、リスクの重要性に応じた対応方針・手続きが漏れなく、あるいは、連携して有効に機能しているかについて、お客様の現状を調査、診断致します。

情報セキュリティリスク診断のフレームワーク



5. 情報セキュリティリスク診断の流れ

『情報セキュリティ管理基準（経済産業省）』を基に弊社が作成した、『情報セキュリティリスク一覧』に基づき、関連部門へのインタビュー等を通じて、保有情報資産及び対応状況の実態を調査し、情報漏洩リスクの影響の重要性を考慮した対策状況の脆弱点、是正の優先度を提示いたします。また、継続的な有効性を維持するためのモニタリング項目及び方法についてお客様におかれての実施検討を支援いたします。

作業ステップ	概要
1. 現在の対応状況の実態把握	情報漏洩リスクに対する、リスク最小化／漏洩防止／発見と対応のそれぞれにおいてどのような仕組みが整備されているかをインタビュー等にて調査します。
2. リスク対応の有効性検証	整備されている仕組みが個別に、及びそれぞれの組み合わせによって十分機能しているかを評価し、検討すべき脆弱点を抽出します。
3. リスク重要性の評価と対策課題の抽出	脆弱点が認められた情報漏洩リスクの影響の重要性（情報の性質・量及び漏洩の発生可能性）を評価し、脆弱点についての対策の要否、優先度を判断します。
4. 情報セキュリティ強化策の策定	リスクの最小化／漏洩防止／発見と対応において効率の良い組み合わせを考慮し、具体的な改善策を策定します。また、定期的なモニタリングの対象項目とを監視方法を検討します。

6. 期待される効果

関連部門へのインタビュー等を通じた診断活動は、活動自体が、情報漏洩の発生の抑止につながり、また、お客様における適正な管理レベル・基準としてセキュリティポリシーをより具体的にする上での実態に即した基礎情報が得られるといった効果が期待されます。

期待される効果

1. 現在の対応状況の実態把握

- ●現場における情報セキュリティへの認識度合・漏洩事実や兆候などの実態の理解
- ●調査対象部門に対する、情報セキュリティリスクへの理解・意識づけによる不正な取り扱いの抑止

2. リスク対応の有効性検証
3. リスク重要性の評価と対策課題の抽出

- ●現状の情報セキュリティリスクの影響の重要性（脅威の度合）の把握
- ●情報の種別・重要性に対応する、対策レベル（どこまで・どの程度が妥当か）を具体化（実現可能な具体的な管理基準）するための基礎情報の取得

※ISMS認証取得を検討されている場合、リスクアセスメント活動の効率化、精度の向上につながる基礎情報として利用できます。

7. 情報セキュリティリスク(評価項目)(ご参考)

弊社が提供する『情報セキュリティリスク一覧』には、以下のように区分された『情報セキュリティリスク』と対応状況の判断指標が整理されています。

『情報セキュリティリスク』評価項目シートの内容(一部抜粋)

『情報セキュリティリスク』の区分一覧

1. 情報セキュリティに関する基本方針
2. 組織・管理体制
3. 資産の管理
4. 人的資源の管理
5. 物理的アクセス
6. **ユーザーアクセス**
7. 管理者アクセス
8. ネットワークアクセス
9. リモートアクセス
10. 外部ネットワークの利用
11. モバイルの利用
12. 電子メール及びその他情報の交換
13. Webアプリケーションその他対外サービス
14. 媒体の管理
15. プログラムファイル・データの保護
16. ソースプログラム
17. システム開発・変更・保守
18. システムの運用・管理
19. 不正

《リスク内容 例》
システムに保存された情報に、使用権限のない者がアクセスし、不正または誤って利用する。

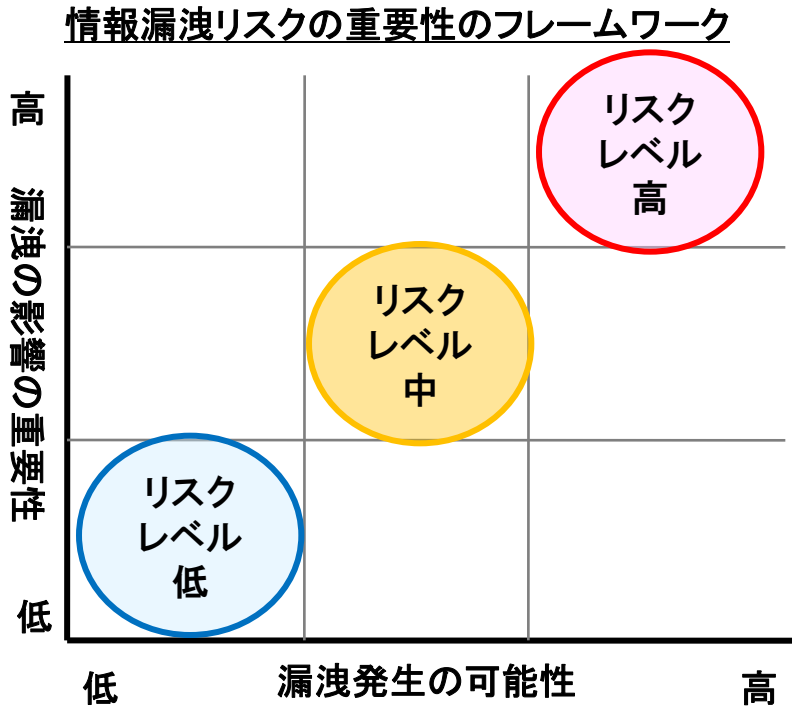
《確認項目 例》

漏洩リスクの最小化	システムへのアクセス権限者が情報に対する必要最低限に維持されるようどのような仕組みが整備されているか。
情報漏洩の防止	アクセス権限のない者が重要なシステム情報にアクセスしないようどのような仕組みが整備されているか。
漏洩の発見と対応	アクセス権限のない者による情報へのアクセスを適時に発見し、外部に情報が漏洩しないようどのような対応の仕組みが整備されているか。
仕組みの評価と改善	認められていないアクセスの予防及び発見に係る仕組みが有効に機能しているか検証し、必要に応じて改善する仕組みが整備されているか。

※弊社がご提供する評価項目案は、経済産業省「情報セキュリティ管理基準」、日本公認不正検査士協会「不正リスク評価ツール」を参考に独自に整理したものです。

8. 情報漏洩リスクの重要性と対策案検討の考え方

適切な情報セキュリティ管理の構築にあたっては、対象となる情報の性質（影響）及び、漏洩が発生する可能性による影響の重要性に沿った一定の基準（フレームワーク）を構築し、展開することを推奨します。
基準を構築することは、情報セキュリティに係る環境の変化に対応した見直しを行う上でも重要なものとなり得ます。



ポイント①
リスクの重要性の高いものにより強固な対策を実施（予防・発見・監査全て行う等）

ポイント②
重要性の段階（しきい値）を設定し、象限毎の対策基準を設定

ポイント③
定期的にリスクの重要性を評価し、個々の対策の有効度合いを検証

ポイント※
重要性に沿った対策のあり方を具体的な情報セキュリティポリシーとして規定

株式会社MONET　コンサルティング事業部の紹介

コンサルティング事業部のサービス

事実分析（ファクト・ファインディング）を基盤とした業務支援・助言／指導及び事実認識に基づいた業務・システムソリューションの策定を支援いたします。

①事業・プロセス分析/評価、セルフアセスメント支援

経営、業務の品質・効率性の分析・評価、及び効果的な対策を講じるための改善ポイントの提案。
クライアント自身による継続的な評価・改善を行うためのセルフアセスメント活動（CSA）の導入の支援。

事業・プロセス診断/評価	事業やプロセスの現状を事実ベースで把握し、目的の達成に最も効果的な改善ポイントの提案を行います。 また、正しい事実認識を行うための分析・評価をお客様自身で実施できるよう支援します。
統制自己評価（CSA）の推進	自分たちの業務を自ら評価・改善する仕組みを定着させ、業務の品質や効率性が自発的に維持・向上される企業へと成長させます。

②内部監査・評価運営支援

内部統制報告制度（J－SOX）対応、企業内不正（不祥事）・情報漏洩リスクなどに対する取り組みの有効性の評価に関する、手続きの構築及び、評価作業の支援。

内部統制制度対応（J-SOX/US-SOX）	財務報告の不正・誤謬に焦点を絞り、網羅的かつ効率的な内部統制報告制度対応を支援します。
コンプライアンス（CSR・法令遵守・不正防止）対応	対象とするコンプライアンスリスクの定義をもとに、適切な評価方法の策定や評価の実施を支援します。

③継続的モニタリング　改善プロセス構築支援

企業の目的達成への取り組みを維持・継続するための、日常的なモニタリングシステムの構築支援。方針・規定の整備、運用プロセスの構築、プロセス改善の支援。

プロセス・マネジメント改善	モニタリングの手続きを組み込んだ業務プロセスの構築と運用を支援することによって、企業の目標達成を実現します。
システムリスク・情報セキュリティ対応（ISMS/PCI DSS等）	システムを利用することにより発生するリスクに対する診断・監査活動や、その結果に基づいた対応策の策定や実施を支援します。
システム管理・運用プロセス構築・評価・改善（COBIT/ITIL等）	特定の基準に準拠したシステム管理・運用プロセスの構築やプロセスの定着化、プロセスをモニタリングする仕組みの構築を支援します。

株式会社MONET コンサルティング事業部の紹介

コンサルティング事業部の実績・ノウハウ

MONETのコンサルティング事業部は、幅広い業種のお客様に対して、内部統制制度対応やシステム管理・運用プロセス構築を中心とした実績を持っております。

支援実績企業

- フィルムメーカー
- 自動車メーカー
- 画像機器メーカー
- 重機メーカー
- 自動車部品メーカー
- 複合事務機メーカー
- 印刷会社
- 石油精製会社
- 記録メディア製造会社
- 精密機器メーカー
- 消費者金融
- 印刷機器メーカー

各種団体に所属し、また、弊社メンバーが各種資格を保有し、日々最新の情報を入手しサービス内容に反映をさせております。

＜弊社の所属団体＞

- 日本内部監査協会
- 日本公認不正検査士協会
- 日本ネットワークセキュリティ協会
- 日本セキュリティ監査協会

＜弊社メンバーの保有資格＞

- 公認内部監査人 （CIA）
- 公認情報システム監査人 （CISA）
- 公認不正検査士 （CFE）
- 内部統制評価指導士 （CCSA）
- ISMS審査員補
- 個人情報保護法検定
- その他（情報処理、ソフトウエア技術者、ERP/DB認定資格等）

事実認識の追求と、先進的ソリューション

日時計（sun dial）のシンボルに示される「文字盤」は、真理（ゆるぎなき価値基盤）を表し、偏りなき目で事実を捉える姿勢を意味します。そして、「針」は「方角」と「時」を表し、現在の位置と向かうべき方向を指し示し、時代をリードする取り組みを意味しています。

MONETは、調査・診断・監査の支援を通じて、お客様の事実に基づいた本質の理解と正確な判断を支援し、時代をリードする独創的・先進的なソリューションの提供を通じてお客様の業務革新に貢献することをミッションとしております。