第一回　SMFGホスピタルカンファレンス

個人情報保護管理体制整備への取組みについて
(Premium版)

2005年03月03日

株式会社日本総合研究所　研究事業本部
小野　彰

主な内容

- 間近となった個人情報保護法施行
- 続発する個人情報漏洩
- 情報セキュリティ管理の必要性
- 情報セキュリティ対策のポイント
- 情報セキュリティポリシーの策定
- 情報資産の調査・整理とリスク分析
- コンプライアンスプログラムの策定
- 情報セキュリティ管理のための体制整備
- 情報セキュリティ管理のためのコントロール（技術面）
- 攻めの対策へ（コスト→プロフィットへの展望）

間近となった個人情報保護法施行

日本総研
The Japan Research Institute, Limited

■個人情報保護法の経緯

年月	実施内容	対象
平成15年5月	個人情報保護法成立	対象：5,000人以上の個人情報を保有する企業が対象。従業員情報も含む。 個人情報の種類：個人が特定できる情報。氏名、電話番号だけでも対象。
平成17年4月	完全施行	

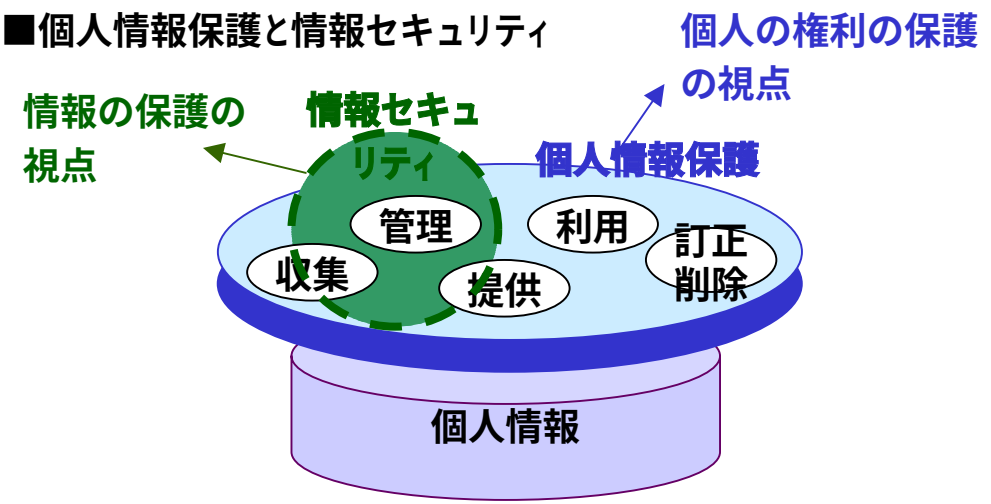
■個人情報保護法の概要

■利用目的の特定
■利用目的を超えての個人情報の取扱禁止
■不正手段による個人情報取得の禁止
■本人同意なしの第三者への個人情報の提供禁止
■本人要求によるデータの開示
■個人情報の取扱に関する苦情の適切･迅速処理

✖ 個人情報は企業の資産

@ 個人情報は個人のもの

■個人情報保護と情報セキュリティ



続発する個人情報漏洩

日本総研
The Japan Research Institute, Limited

■個人情報の漏洩事例

対象	時期	漏洩事故内容	対応･顛末	損害リスク
京都府宇治市	1998年5月	住民基本台帳の情報（基本4情報）が委託業者から名簿業者へ販売された	市議3人が市へ損害賠償訴訟、**1人1.5万円の賠償が確定**（市の管理責任の観点から）。その後、市民1人が市へ115万円の損害賠償請求を新たに提訴。	集団訴訟の場合（住基情報22万件）→32.6億円の賠償額の可能性
エステサロンTBC	2002年5月	Webアンケート回答者3.7万件の情報（基本4情報、電話番号、スリーサイズ、プロポーションの悩み等）が8時間閲覧可能だった。	被害者10人が**1人115万円の損害賠償を請求**。	3.7万人×115万円＝425億円の損害賠償の可能性
ローソン	2003年6月	会員56万人分の情報（氏名、住所、生年月日、携帯電話番号等）が情報システムから社外へ流出。	**カード会員全員115万人に謝罪文と商品券500円を郵送**。 社長･役員、システム管理会社社長･役員が10～30%減給3ヶ月間。	1人1万円として、56万人×1万円＝56億円の賠償の可能性
ソフトバンクBB	2004年1月	会員451万人分の情報（氏名、住所、電話番号、メールアドレス他）が内部関係者により持ち出し	**会員全員451万人に金券500円を送付**。 対策費総額40億円。	1人1万円として、451万人×1万円＝451億円の賠償の可能性

■刑事事件の事例

事件	概要
都市銀行の顧客データ流出に係る業務上横領	ソフトウェア開発会社社員が，都市銀行向けプログラム開発業務に従事していた際，顧客データをフロッピーディスクにコピーし持ち出し，２０万円で売却（業務上横領）。
ＮＴＴ職員による電話個人情報漏示をめぐる贈収賄	ＮＴＴ職員が，電話加入者の住所氏名等の秘密情報を漏示し，職務上不正の行為に対する賄賂合計約８９万円を収受したもの（ＮＴＴ法違反）
信用情報機関から信用情報を不正に入手した貸金業法違反	人名義で貸金業登録をして信用情報機関から信用情報を入手して，これを売却しようと企て，3名共謀の上，貸金業を営む意思がないのにあるように装い，他人名義で貸金業者の登録を受けたもの（貸金業法違反）

情報セキュリティ管理の必要性

日本総研
The Japan Research Institute, Limited

■情報システムを取り巻く脅威

情報化の進展（多様化、大量化、依存度の増大）、外部環境の変化（脅威の増加）、影響範囲の拡大（広域化、高密度化）、不正の増加

- 企業内で扱う情報が多様化、大量化し、業務のコンピュータシステムへの依存度も増大
- 社内だけではなく、社外企業・機関とのネットワークを通じた連携も広域化、高密度化
- 情報および情報システムに対する人的、技術的、物理的脅威が多様化、増加
- 顧客情報に関しては故意・不正に関する脅威が大きい
- リスク顕在化による問題や損害が発生した場合、自社だけでなく顧客や関連企業・機関との取引に多大な影響

■もぐらたたきの限界

場当たり的、もぐらたたき的セキュリティ対策の限界

- 事故が起きてから対処を検討
- 他社事例を見て対処
- 一般的な雛形をそのまま流用

- マネジメントの欠如、リスクが把握できていない、担当以外はわからない
- 貴社に合致しないリスクへの対応になる可能性
- 経験が改善に結びついていない

- **漏れや抜けのない対策の立案、実施がポイント**
- **設備、環境、人事、技術、契約、運用等の視点で対策**
- **事前防止、事後対策**
- **事業戦略、経営ポリシーとの合致**

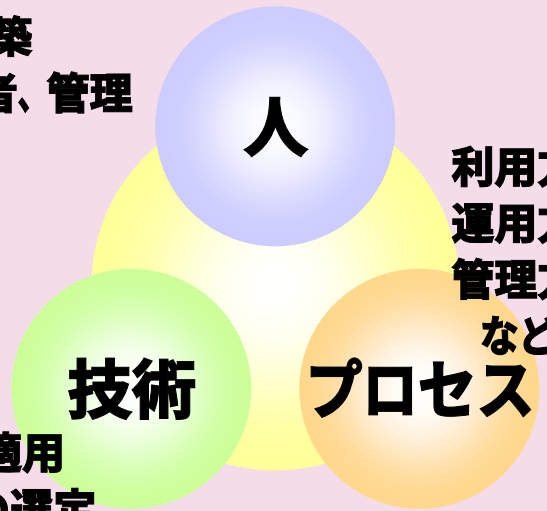
情報セキュリティ対策のポイント(1)

日本総研 The Japan Research Institute, Limited

■バランスの取れた対策

対策を実施するリスク(プロジェクト対象)

管理体制の構築
利用者、運用者、管理者ごとの規準



利用方法
運用方法
管理方法
など

明文化

- 必須行為
- 推奨行為
- 禁止行為
- 許諾行為
- 義務
- 権限留保
- 権限放棄

最適な技術の適用
適切なベンダの選定

バランス

受容・移転・転嫁するリスク

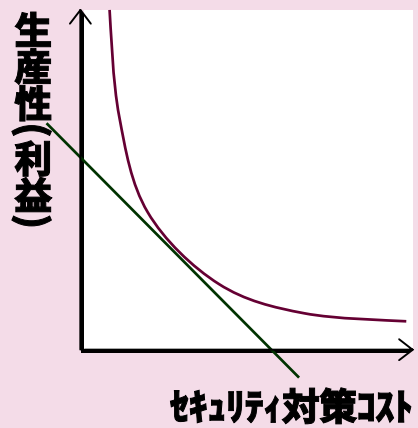
リスク保有
リスク移転
リスクファイナンス　等
～　による解決　　cf. SLAアウトソーシング契約、保険など

情報セキュリティ対策のポイント(2)

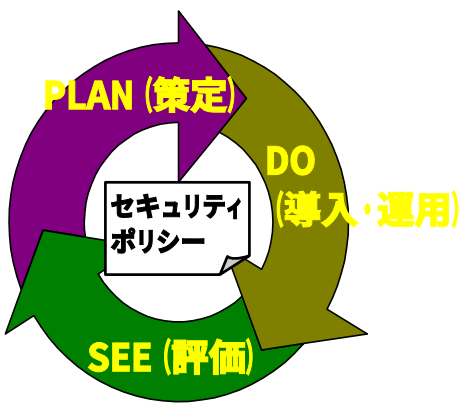
日本総研
The Japan Research Institute, Limited

■効率性とのトレードオフ

●一般に、セキュリティ強度を増加するほど、効率や生産性・利益が減少する。
●厳重・周到すぎる対策は遵守されず、逆に脆弱性を増大させる



■マネジメントサイクル運用



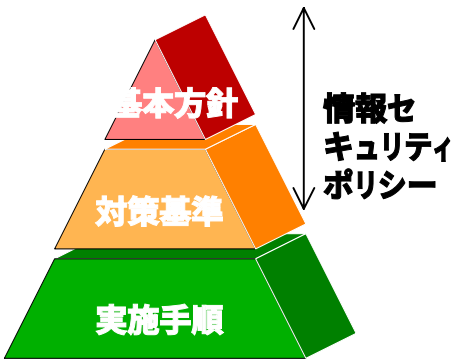
●環境変化、技術進展などによる見直しの実施

PLAN	DO	SEE
●情報セキュリティポリシー策定 ●基本計画の策定 ●組織、運用体制の整備、任命 ●実施計画の策定 ●実施手順(マニュアル) 作成・改定	●情報セキュリティ教育 ●動機付けの手段として ●方法 ●説明会 ●社内研修 ●講習会 (内部、外部) ●モニタリング	●監査 ●内部監査 ●外部監査

情報セキュリティポリシーの策定

日本総研
The Japan Research Institute, Limited

■情報セキュリティポリシーとは？



●組織の情報セキュリティに関する方針
●情報セキュリティを確保するための取組を包括的に規程した文書
●事業戦略、経営ポリシーとの合致

基本方針の例
1．目的
2．ポリシーの位置付け
3．対象範囲
4．マネジメント体制
5．準拠性
6．罰則

対策基準の例
1．情報の取扱
2．物理セキュリティ
3．要員セキュリティ
4．技術セキュリティ
5．情報システム開発
6．アウトソーシング
7．事業継続計画

■対象とする情報

●情報資産
顧客情報、営業機密、財務情報、信用情報、取引情報、・・・

※本来は、企業で取り扱うすべての情報が対象となるが、経営に重大な影響を与える情報資産にフォーカスして検討することが効果的

情報資産の調査・整理とリスク分析

日本総研
The Japan Research Institute, Limited

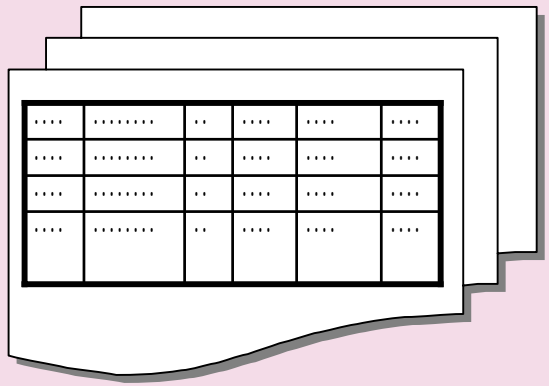
■情報資産の調査・整理

●管理対象とする情報（資産）は、どこにどれだけ存在するか？

個人情報管理台帳の例

1. 情報の名称
2. 含まれる個人情報の内容・種類
3. 個人情報収集の目的
4. 入手方法
5. 管理・保管方法、管理責任者
6. 預託・提供の有無　　等々

部門毎に作成



■リスク分析

●対象となる情報（資産）のリスク度は？

情報資産	情報資産の価値				脅威					脆弱性		リスク値
	機密性	完全性	可用性	評価値	生成・受領時	保管時	利用時	返却・廃棄時	評価値	脆弱性	評価値	

日本総研
The Japan Research Institute, Limited

■コンプライアンスプログラムの策定

●コンプライアンスプログラムとは？

JIS Q 15001における定義は次の通り

「事業者が、自ら保有する個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメントシステム」

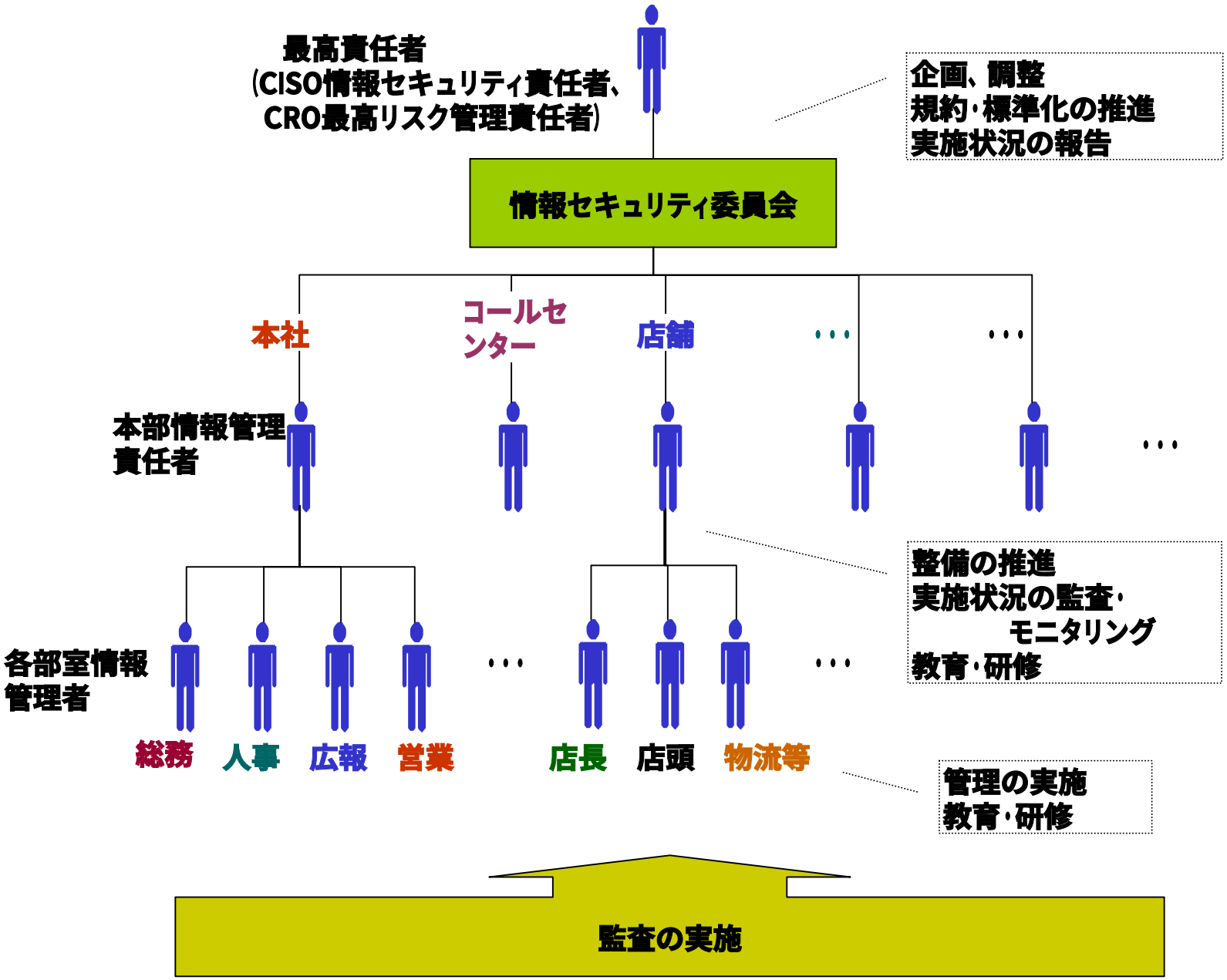
●コンプライアンスプログラムを構成する文書・規程の例

・個人情報保護マニュアル
・個人情報に関する保護方針

・文書管理要領
・教育・訓練要領
・内部監査実施要領
・お客様相談対応要領
・入退館管理要領
・機密情報管理要領
・緊急時対応要領

・情報システム安全対策基準
・コンピュータ不正アクセス管理基準
・ネットワーク安全対策基準
・コンピュータウィルス対策基準

情報セキュリティ管理のための体制整備



情報セキュリティ管理のためのコントロール（技術面）

日本総研
The Japan Research Institute, Limited

■技術面の対策のキーワード

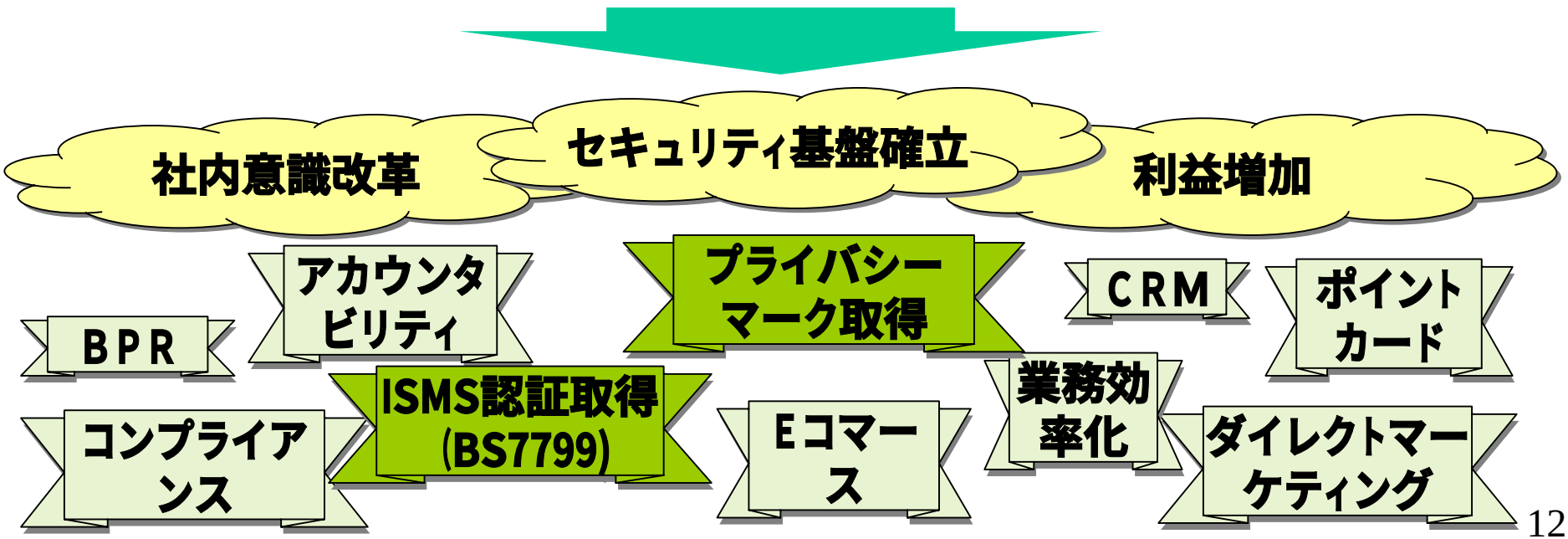
認証関連	ワンタイムパスワード、ICカード、PKI、バイオメトリクス、デジタル署名、タイムスタンプ、シングルサインオン
暗号関連	暗号化ソフト
ファイアウォール関連	ファイアウォール、VPN、ルータ、DMZ
セキュリティ検査･監視	検査ツール、監視ツール、ログ解析ツール、IDS
ウィルス対策	サーバ型、クライアント型
フィルタリング	Web監視、メール監視
施設関連	入退室管理
事業継続対応	バックアップ、二重化、ストレージ、保険
セキュリティサービス	セキュリティ検査、不正アクセス監視、電子認証、インターネットVPN、ファイアウォール管理

攻めの対策へ（コスト→プロフィットへの展望）

日本総研 The Japan Research Institute, Limited

■セキュリティ対策の効果

対内（対企業内）効果	対外（対企業外）効果
本質的な情報セキュリティの向上	企業価値の向上
説明責任（アカウンタビリティ）の明確化	運用基準明確化によるサービス品質の向上
安全な情報の共有化	信頼性のアピール
職場の情報整備による業務の効率化	同業他社に対する優位性の確保



おわりに

- 情報セキュリティ対策のためには、情報システム部門だけが頑張るのではなく、経営トップの支援のもとに、関係する各部門の積極的な関与が重要です。
- また、コンプライアンス・プログラムを単に制定するだけではなく、確実に実行できる体制の確立が必要です。
- 全ての部門が参加する、個人情報保護委員会のような委員会を設置することも、情報セキュリティ対策には効果的です。
- 間近に迫った個人情報保護法施行に向け、何もかも、と慌てるよりも、対策の全体像を把握した上で、施策の優先順位を明らかにして取り組むことも重要でしょう。