IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報セキュリティガバナンスについて

2006年3月23日

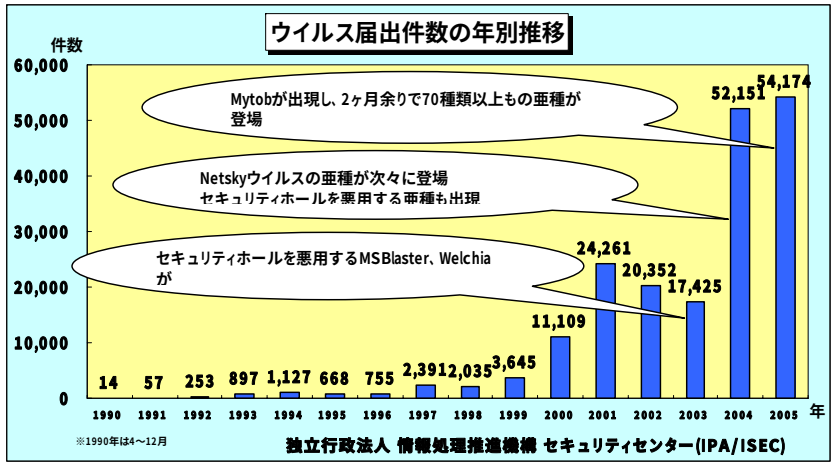
独立行政法人　情報処理推進機構
セキュリティセンター長　三角育生

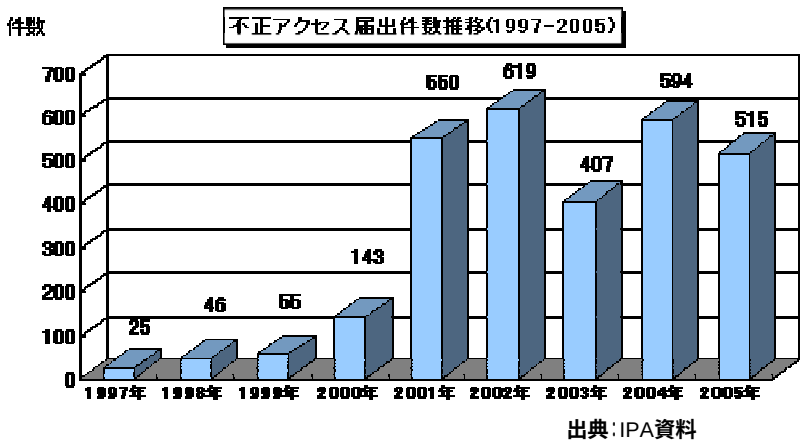
http://www.ipa.go.jp/security/

情報セキュリティを巡る現状認識

- **発生する問題の量的増加**
  - コンピュータウイルス、不正アクセスの届出の増加
  - インターネット取引拡大等により、金融、クレジット、電力等の重要業種においても問題が増大傾向
  - 体制の更なる強化、社会全体のリテラシー向上が不可欠
- **脅威の質的変化**
  - 愉快犯的行為から経済的利得目的化、組織化･分業化
  - 脅威の質の変化に対応するための体制構築が不可欠
- **自律的な対応の必要性**
  - 対処療法から自律的･継続的な対応の必要性

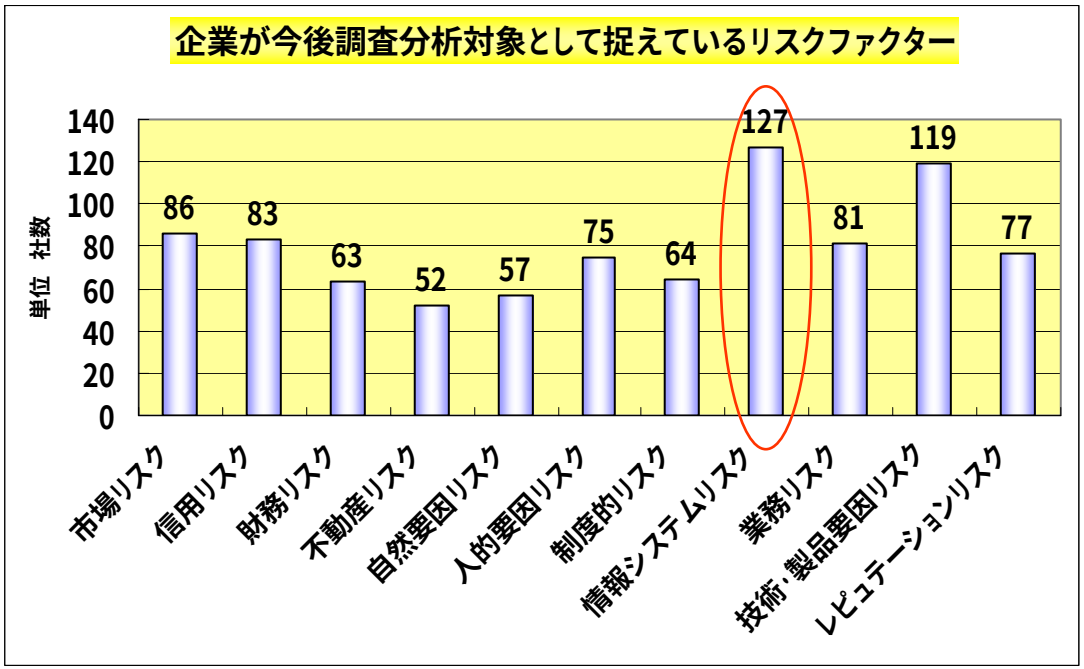
（経済産業省資料を参考に作成）





出典：IPA資料

経営課題としての情報セキュリティの位置付け



経済産業省　2003年事業リスク評価・管理人材育成システム開発事業　アンケート調査より作成　有効回答数（1009票）

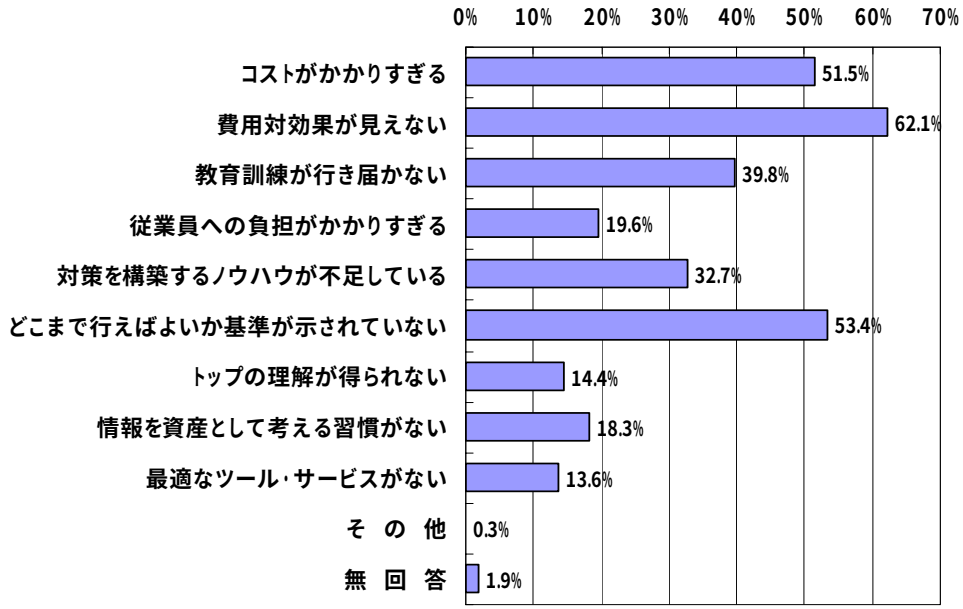
- ITが社会や顧客への影響、経営に与える影響が大きくなっている。
- 「情報システムのリスク」を挙げる企業は多い。
- 経営課題としての認識を高めることが必要。

出典：経済産業省資料

情報セキュリティ対策の現状

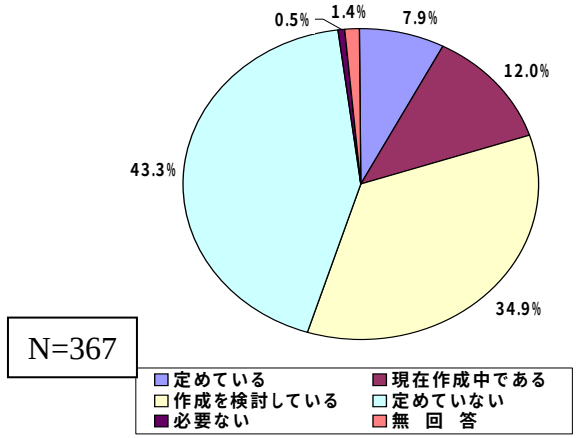
- 我が国企業が情報セキュリティ投資を行う上で障害と感じる主な要因は、
  ①費用対効果が見えない（62.1%）
  ②どこまで行えばよいか基準が示されていない（53.4%）
- 我が国企業の緊急事態対応計画は、策定済が7.9%、現在作成中が12.0%にとどまる。
- IT事故の発生可能性を無くすことはできない以上、企業は本来、IT事故発生時の被害局限化と早期復旧が重要であり、そのための事業継続計画（BCP）を策定すべき。

大手･中堅企業における情報セキュリティ投資の障害（重要インフラ業種を除く）



出所：警察庁「不正アクセス行為対策等の実態調査」（2003年12月）より事務局作成

大手･中堅企業における緊急事態対応計画の策定状況（重要インフラ業種を除く）



米KPMG"KPMG 2002 BUSINESS CONTINUITY STUDY"の調査(2002年)によると、米国では、BCP策定済の企業は67%、策定中の企業は29%であり、未対応企業は4%に過ぎない。

出典：経済産業省資料

情報セキュリティガバナンスとは

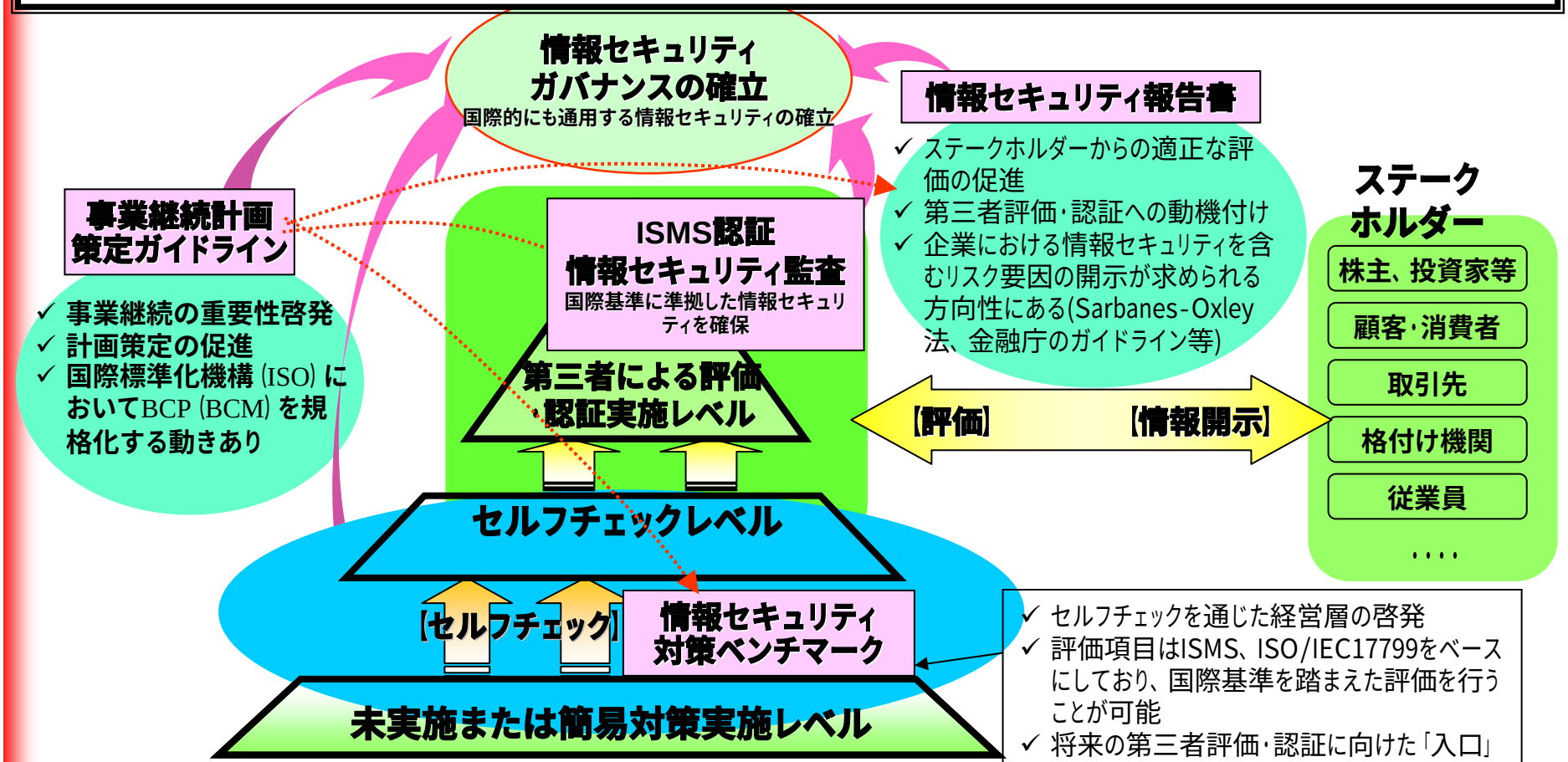
	従来の 情報セキュリティ対策	情報セキュリティガバナンス
目的	自社内における情報システムの信頼性・安全性の確保	ステークホルダー（株主、顧客、取引先等）に対する責任
責任主体	システム部門	経営層
方法	対症療法的対策	内部統制の確立と ディスクロージャー

- 社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること、すなわち「**情報セキュリティガバナンス**」の確立が求められる。

出典：経済産業省資料

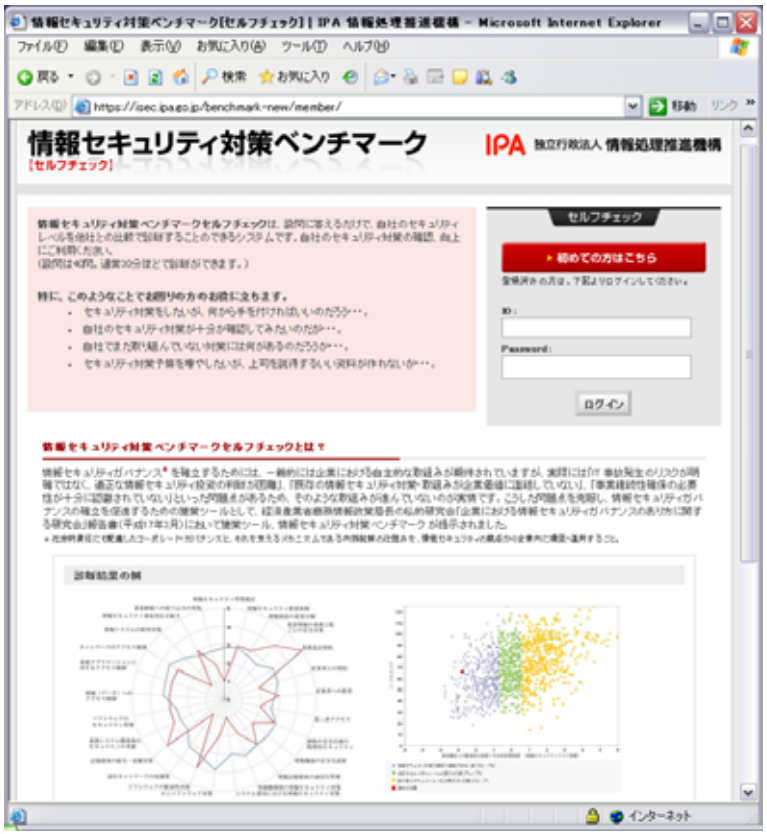
施策ツールとISMS認証等との基本的関係

■自己評価をベースとしつつ、必要な場合は第三者による客観評価に耐えうる仕組みの構築が重要
■企業活動のグローバル化を考慮し、国際基準との整合性等にも配慮



出典：経済産業省資料

情報セキュリティ対策ベンチマークシステム



第1部：情報セキュリティ対策状況に関する設問　25問
第2部：事業内容に関する設問　15問

設問のサンプル

- ✓ 情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。
- ✓ 導入しているソフトウェアに対して適切な脆弱性対策を実施していますか。
- ✓ 主要な業務に関わるプロセスのうち、インターネットに依存している割合はどの程度ですか。

情報セキュリティ対策ベンチマークシステム
http://isec.ipa.go.jp/benchmark-new/

情報セキュリティ報告書モデル

情報セキュリティ報告書の記載項目（フルセット）

①基礎情報
- ✓報告書の発行目的
- ✓利用上の注意
- ✓対象期間、責任部署等

②経営者の情報セキュリティに関する考え方
- ✓企業の情報セキュリティに関する取り組み方針
- ✓対象範囲対象範囲
- ✓報告書におけるステークホルダーの位置付け、ステークホルダーに対するメッセージ

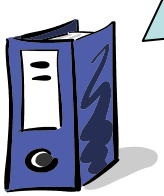
③情報セキュリティガバナンス
- ✓情報セキュリティマネジメント体制（責任の所在、組織体制、コンプライアンス等）
- ✓情報セキュリティに関わるリスク
- ✓情報セキュリティ戦略

④情報セキュリティ対策の計画、目標
- ✓アクションプラン
- ✓数値目標（対策ベンチマークのスコア等）

⑤情報セキュリティ対策の実績、評価
- ✓計画に対する実績、評価
- ✓事故報告

⑥情報セキュリティに係る主要注力テーマ
- ✓ 特に強調したい取組み、テーマを選択し、その状況を紹介（例：個人情報保護、事業継続計画等）

⑦第三者評価・認証
- ✓ 第三者評価・認証に係る取り組み
  - 認証の取得状況(ISMS、プライバシーマーク)
  - 情報セキュリティ監査の実施状況　等



情報セキュリティ報告書

発行主体にとっての効果

説明責任の遂行
・事業に影響するIT関連のリスクが小さいことを対外的に説明

新たな事業付加価値創出
・事業戦略の反映
・ブランドの確立

リスク低減に関する説明をステークホルダーから求められる企業
【必要最低限の項目・内容】

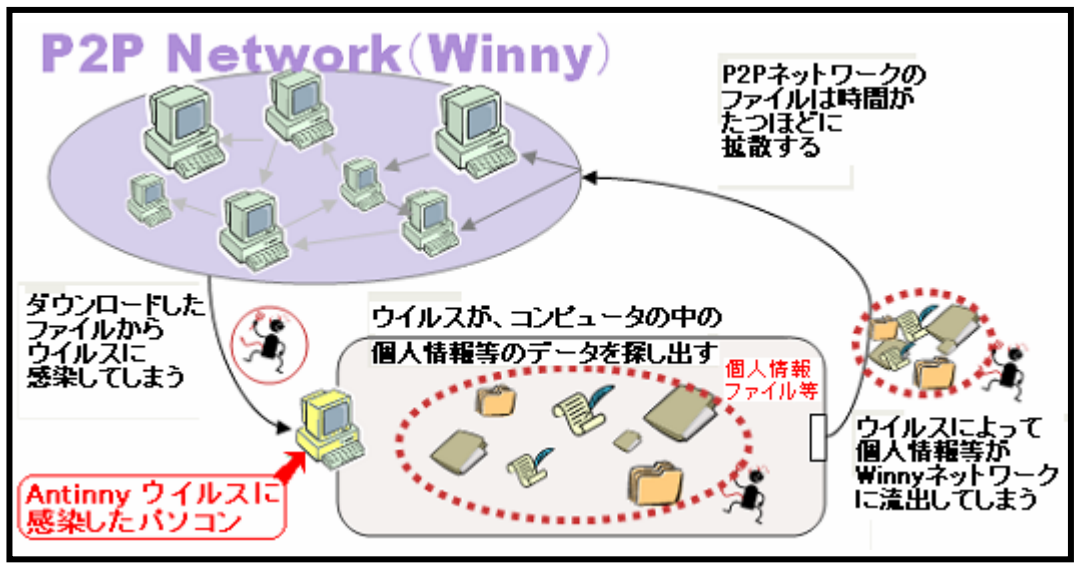
自社の事情に応じて記載項目や内容のレベルを選択

情報セキュリティへの取り組みが競争優位に寄与する企業
【すべての項目・内容】

経済産業省資料を基に作成

情報漏えい対策を説明するとき（例）①

- 最近、ファイル交換ソフト(Winny)を介したウイルスに感染したことが原因で個人情報等の情報漏えいが頻発。
- 公表されたケースからみられる原因：
  ①予算の関係でパソコンの割り当てが不足していて、私有パソコンを使っていた
  ②情報を持ち出さないようルールはあったが、徹底されていなかった
  ③ウイルスに感染していることに気づいていなかった
- 組織の個人情報保護（情報漏えい等）対策を説明するとき：



Http://www.ipa.go.jp/security/topics/2006310_winny.html

情報漏えい対策を説明するとき（例）②

- 漏えいして困る情報を取り扱うパソコンにはWinnyを導入しない
- 職場のパソコンに許可無くソフトウエアを導入しない
- 職場のパソコンを外部に持ち出さない
- 職場のネットワークに、私有パソコンを接続しない
- 自宅に仕事を持って帰らなくて済むよう作業量を適切に管理する
- 職場のパソコンからUSBメモリやCD等の媒体に情報をコピーしない
- 漏えいして困る情報を許可なくメールで送らない
- ウイルス対策ソフトを導入し最新の定義ファイルで監視する
- 不審なファイルは開かない

私有パソコンを使わないように再徹底
ルールを再徹底し、チェックを強化
ウイルス対策を再徹底

Http://www.ipa.go.jp/security/topics/2006310_winny.html

情報漏えい対策を説明するとき（例）③

情報セキュリティ報告書　（部分）

◇情報セキュリティに関する取組み方針

- 個人情報保護

…当社では、個人情報保護ポリシーに基づき、…お客様の個人情報のための体制を構築・運用し、継続的に改善に取り組んでいます。…個人情報ポリシーを全社に適用する…全従業員に定期的に個人情報保護教育を実施し、…定期的に個人情報保護体制の評価を行い、その結果を対策に反映します。

◇情報セキュリティガバナンス

- 推進体制の構造と活動

…情報システムのダウン、コンピュータウイルスやワーム、不正アクセス、情報漏えいといった事故が発生した場合には、事業継続計画に則り、情報システム部の主導で適切かつ迅速に問題の早期解決を図ります。

- 情報セキュリティマネジメント体制　（教育・研修関連）

情報セキュリティポリシーに基づく社内ルールを定め、…当社の社員は、入社時点から、情報セキュリティやコンプライアンスを含む実践的な情報システム利用研修を定期的に受講しており、そうした問題に係る十分な知見を有して…

経済産業省資料を基に作成

情報漏えい対策を説明するとき（例）④

◇情報セキュリティ戦略

…個人情報管理上のリスクの一つに、社員が業務遂行のため顧客データを社外に持ち出し、紛失、盗難、ウイルスに感染した私有パソコンからのファイル流出などのケースが挙げられます。そこで、社員による個人情報データファイルの持ち出しを原則として全て禁止し、私有パソコンの接続を許可制とするとともに、…お客様情報については、高水準の情報セキュリティレベルを有し…データセンター、カスタマーセンターを活用し、原則として個別のお客様情報を社員が直接取り扱うことがないよう、業務フローと情報システムを設計しています。

◇情報セキュリティ対策の計画、目標

当社では、…○年からリスクの最小化を実現するプロセスと、それを支える情報システムの構築に着手しており、…情報システムではプログラムのインストール制限･管理、重要事項へのアクセス制限、顧客情報等の暗号化、私有パソコンの接続制限、ウイルス対策を徹底し、…社員の高いモラルを確保するため、入社時から定期的に顧客情報の管理に関する研修を実施…

数値目標　…　社員の年一回以上の個人情報保護研修の受講率の目標を100%…

⋮

経済産業省資料等を参考に作成

情報漏えい対策を説明するとき（例）⑤

◇情報セキュリティ対策の実績、評価
…計画に則り、○月から○月の○ヶ月間をかけて、…に関する内部監査を実施しました。具体的には、社内の業務部、…を対象とし、正式な業務プロセスと実際の作業フローとのギャップや情報システムの実現している環境について検証し、改善すべき点を洗い出しました。…

社員に対し個人情報保護研修の受講率は100%に達しました。…

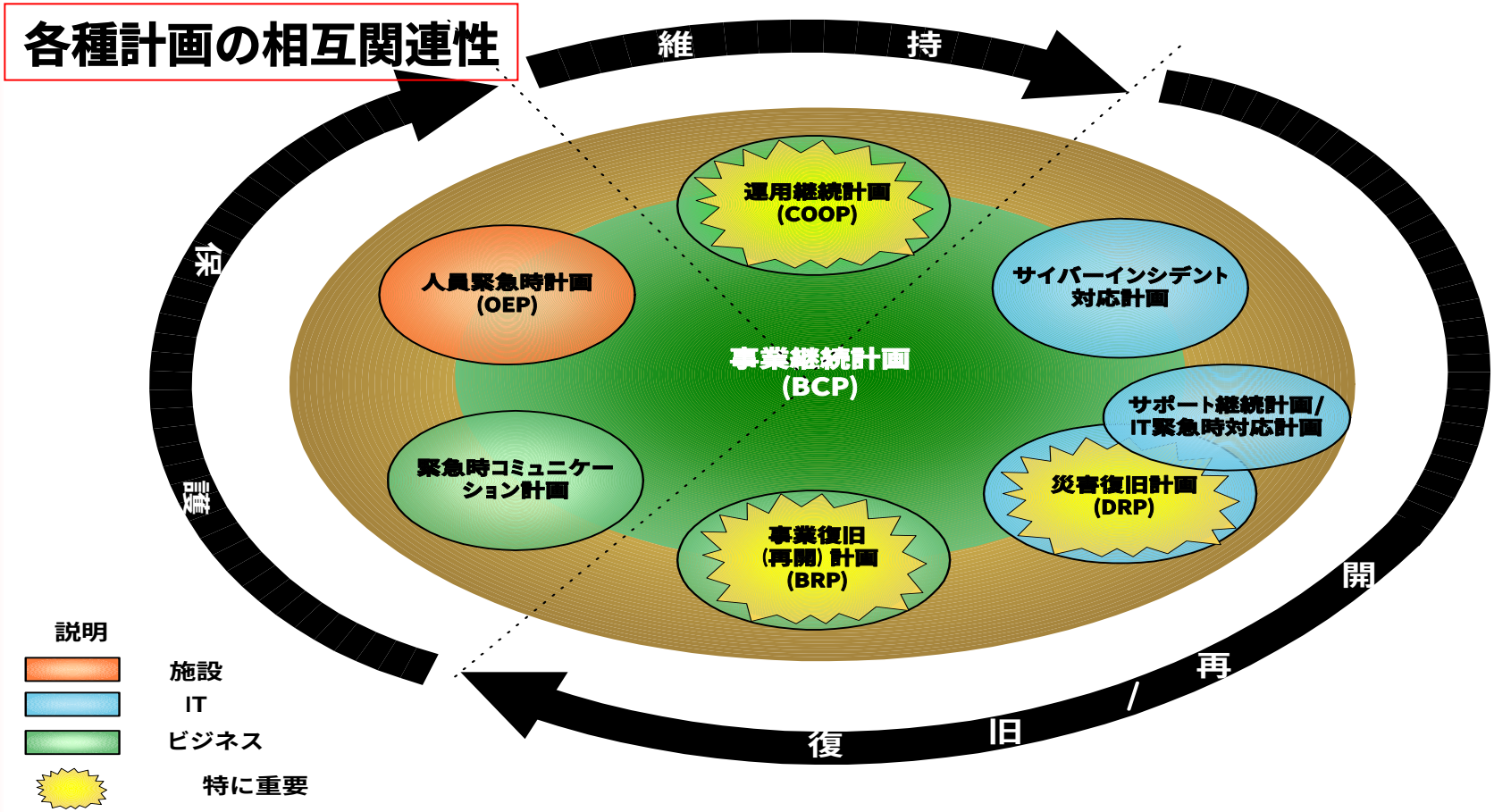
実績に対する評価：個人情報保護については、委託先、情報環境、研修の観点からみて、高いレベルの環境を確保していることが確認できました。…

◇情報セキュリティに係る主要注力テーマ：「個人情報保護（情報漏えい対策）」
……
個人情報の管理方法
物的・技術的管理：…書類に「秘」の文字を入れ…情報へのアクセスできる者を限定し、アクセス権者の履歴を記録、…私有パソコンの接続制限、USBメモリ等の利用制限…
人的・法的管理：社員と秘密保持契約を締結…社内でのルールを構築し、社内教育を定期的に行い…情報を持ち出すことのないように、個人情報の持ち出しを禁止しております。…
組織的管理：個人情報を保有する組織全体のマネジメントに取り組み、情報セキュリティ管理体制の整備を行っております。特に、個別のお客様情報については、高水準の情報セキュリティレベルを有し、サービス品質保証契約を取り交わしたデータセンター、カスタマーセンターを活用しています。

経済産業省資料等を参考に作成

BCPプロセス（IT緊急時対応計画の位置づけ）

各種計画の相互関連性



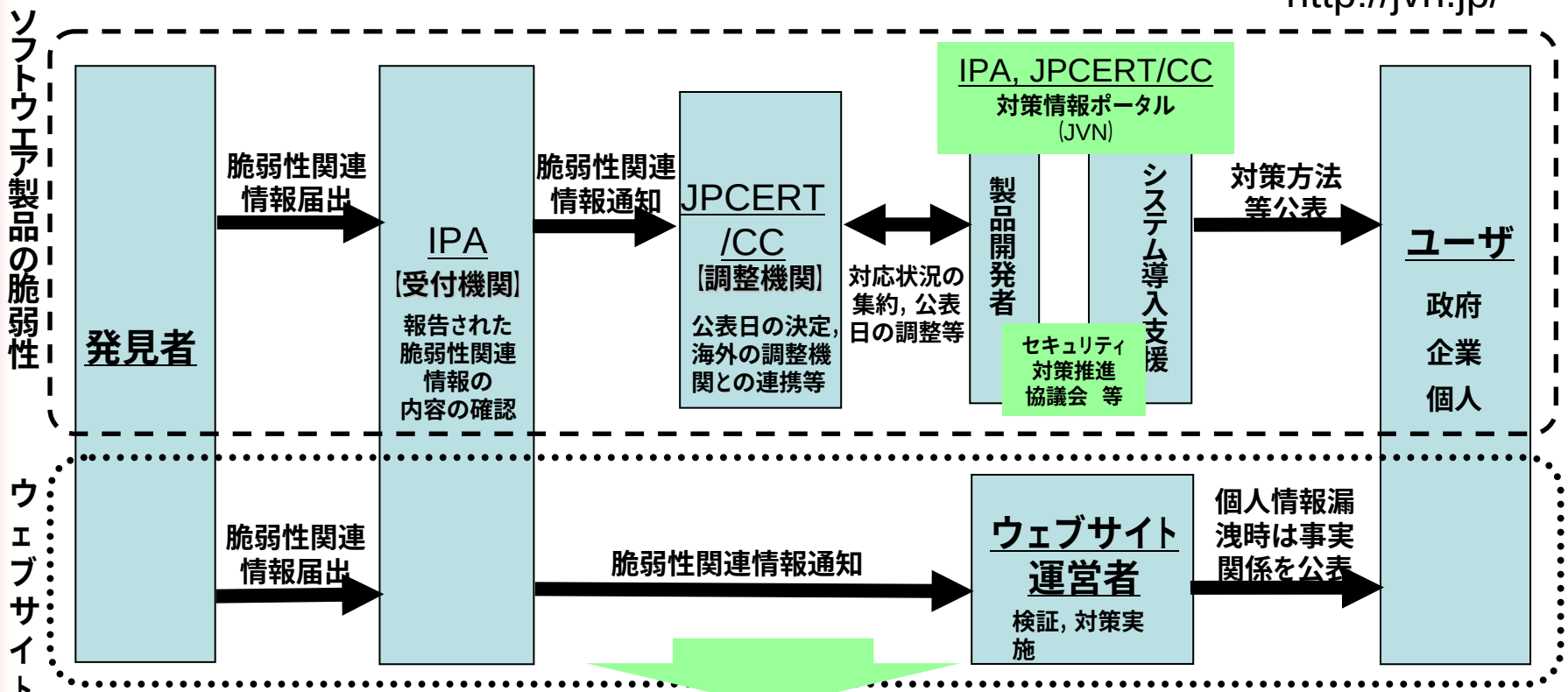
IT緊急時対応計画は、組織やビジネスプロセスの継続を含む広範囲な緊急事態対策の対象に含まれるため、策定および更新において、各計画間の連携をとる必要がある。

出典: NIST SP800-34 ITシステムにおける緊急時対応計画ガイド
http://www.ipa.go.jp/security/publications/nist/documents/SP800-34-J.pdf

(参考) 情報セキュリティ早期警戒パートナーシップ

- 「情報セキュリティ早期警戒パートナーシップ」

http://jvn.jp/



【期待効果】

①製品開発者及びウェブサイト運営者による脆弱性対策を促進
②脆弱性関連情報の放置･危険な公表を抑制
③個人情報等重要情報の流出や重要システムの停止を予防

出典： 報道資料”「情報セキュリティ総合戦略」策定について”，経済産業省 (2003年10月10日)

独立行政法人　情報処理推進機構
セキュリティセンター（IPA/ISEC）

〒113-6591
東京都文京区本駒込２－２８－８
　文京グリーンコートセンターオフィス１６階
ＴＥＬ ０３（５９７８）７５０８　　ＦＡＸ ０３（５９７８）７５１８
電子メール　isec-info@ipa.go.jp
ＵＲＬ　http://www.ipa.go.jp/security/