JNSA NSF2009

変える力を、ともに生み出す。
NTT DATAグループ

【B5】パネルディスカッション

個人情報保護法は、どこへ行く
～事業者の誤解と、適正な個人情報保護のあり方～

《経営者層の視点および国際的な視点から》

2010年1月27日
株式会社ＮＴＴデータ
西尾　秀一

個人情報保護法施行後の取り組み

法令遵守！

- ゲート装置、監視カメラや情報漏洩防止ソフト導入など「わかりやすい」個人情報保護対策にお金をつぎ込む
- （現場の業務効率が多少下がっても）個人情報保護対策、ルールを徹底させる（とにかくやれ！）
  例：ＵＳＢメモリ使用禁止、ノートＰＣ持ち出し禁止
- 社員教育や監査を定期的に実施する
- ＩＳＭＳ認証（ISO27001）やＰマークを取得する
- 情報漏洩事故を起こした社員や取引先を厳しく処分する

その結果どうなったか・・・

- 個人情報漏洩事件、事故は相変わらず発生している
  （有効な対策を実施できているのか？）
- 現場の業務効率は「多少」ではなく、「かなり」低下しているケースもある
- ルールや対策の抜け道を見つける風潮が拡がった
- なぜそのルールを守らなければならないのか、なぜその対策を実施する必要があるのかを考えなくなった
- 逆に社員のプライバシーが保護されなくなった？？

経営者層の悩み・・・

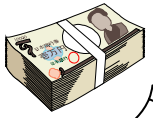
個人情報保護法施行後も事件、事故が減らないが、うちの会社や関連会社、アウトソーシング先は大丈夫か？

顧客や取引先から厳しい要求事項をつきつけられているから仕方ない・・・

対策は打っているが、社員等に浸透しているのか？

どこまでやれば責任を果たしていることになるのか？

費用対効果は？？



CPO（Chief Privacy Officer）の設置

社内のプライバシー保護状況の監視

- プライバシーポリシーの策定と社内への導入
- プライバシー保護を重視する文化の創造
  - ・顧客情報の取り扱いに関する社内研修の実施 等
- ダメージコントロール
  - ・実際に顧客情報の漏えいが発生したときの対応 等

ＮＰＯ日本プライバシープロフェッショナル協会・日本ＣＰＯ委員会

http://www.jppa-npo.org/topics/index.html

CPOが管理する効果的な個人情報保護対策投資

1. リスクの把握と優先順位付け

- リスクがどこにあり、その大きさはどの程度かを把握した上で、
- 最もリスクの高いところから改善する
- 技術（製品）導入だけにコストが集中していないか？
- 予防措置だけでなく、事件、事故への備えはあるか？

2. 施策の実行管理の徹底

- 施策実施の責任者を明確にする
- 教育、訓練は投資を無駄にしないための有効な手段
- ボトルネックが発生した場合には素早く回避策を検討する

3. 施策の効果の把握

- 定期的に施策実施の効果を把握する
- 効果はできるだけ定量化して報告させる
- ビジネスへのインパクトも同時に把握する

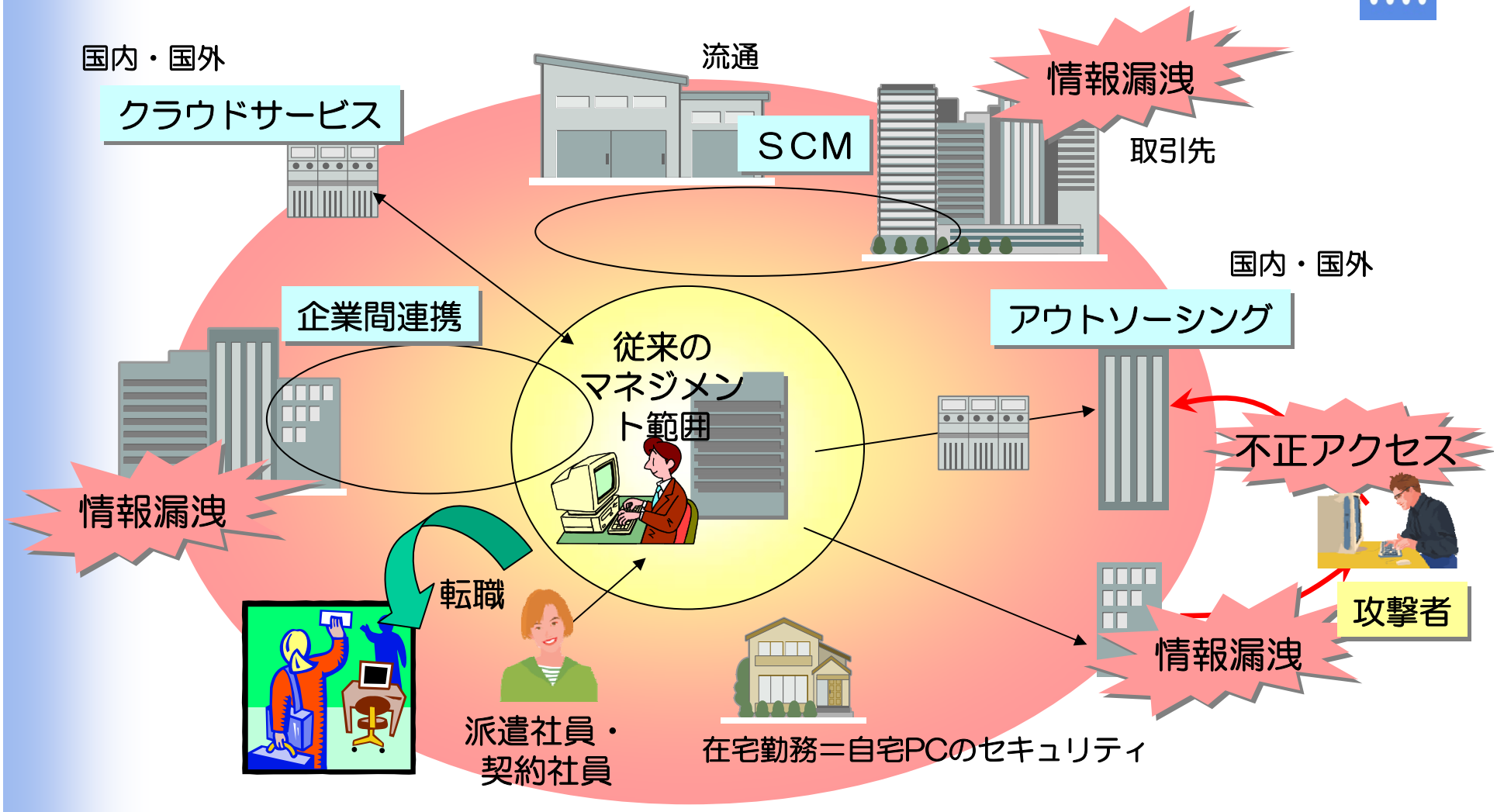
経営者層の関心の変化

弊社へのお客さまからのご相談内容の変化

内容	外部からの不正侵入対策、ウィルス対策 →内部関係者からの情報漏洩対策（ミス防止を含む）
範囲	個別システム、個別組織のセキュリティ対策 →企業全体、グループ全体の情報漏洩対策（しかもワールドワイド）
レベル	必要最小限のセキュリティ対策 →社会的責任を果たす、顧客・株主等への説明責任を果たすのに必要十分な情報漏洩対策

日本の法律の対象外

拡大・変化する個人情報管理の範囲



クラウドサービス利用と個人情報保護の課題

- ✓クラウドデータセンタが設置されている国のデータ保護法に従う必要がある
  例：米国政府は米国内のデータを閲覧する権利があるため、カナダ政府機関は米国クラウド・ホスティングサービスの利用を禁止
- ✓米国では個人情報を外部に預ける場合と自社内で保管する場合で法律の保護レベルが異なるとされている
- ✓ＥＵデータ保護指令の水準を満たしていない第三国データセンタへの個人データの移転はできない
- ✓中国のように個人情報保護法がない国におけるサービス提供およびサービス利用はどうするか？

自己紹介

西尾　秀一（にしお　しゅういち）

（株）ＮＴＴデータ
ビジネスソリューション事業本部
ネットワークソリューションＢＵ
セキュリティソリューション担当

・１９９７年よりセキュアシステム構築、セキュリティ情報共有、セキュリティ評価などの技術開発およびコンサルティングに従事
・２００１年にＢＳ７７９９（現在のＩＳＯ２７００１）の国内初認証に統括マネージャとして参画
・この間、情報サービス産業協会（ＪＩＳＡ）セキュリティ委員会委員として、会員企業へのセキュリティ教育、啓発に努めると共に、セキュリティに関する政策提言活動を行う
・現在、日本ネットワークセキュリティ協会（ＪＮＳＡ）理事、日本情報セキュリティ監査協会（ＪＡＳＡ）幹事、ＩＰＡ情報システム等の脆弱性情報の取扱いに関する研究会委員、日本データ通信協会タイムビジネス協議会（ＴＢＦ）企画運営委員等。
・日本ベリサイン（株）監査役。