Business Assurance Co,Ltd.

【B5】パネルディスカッション

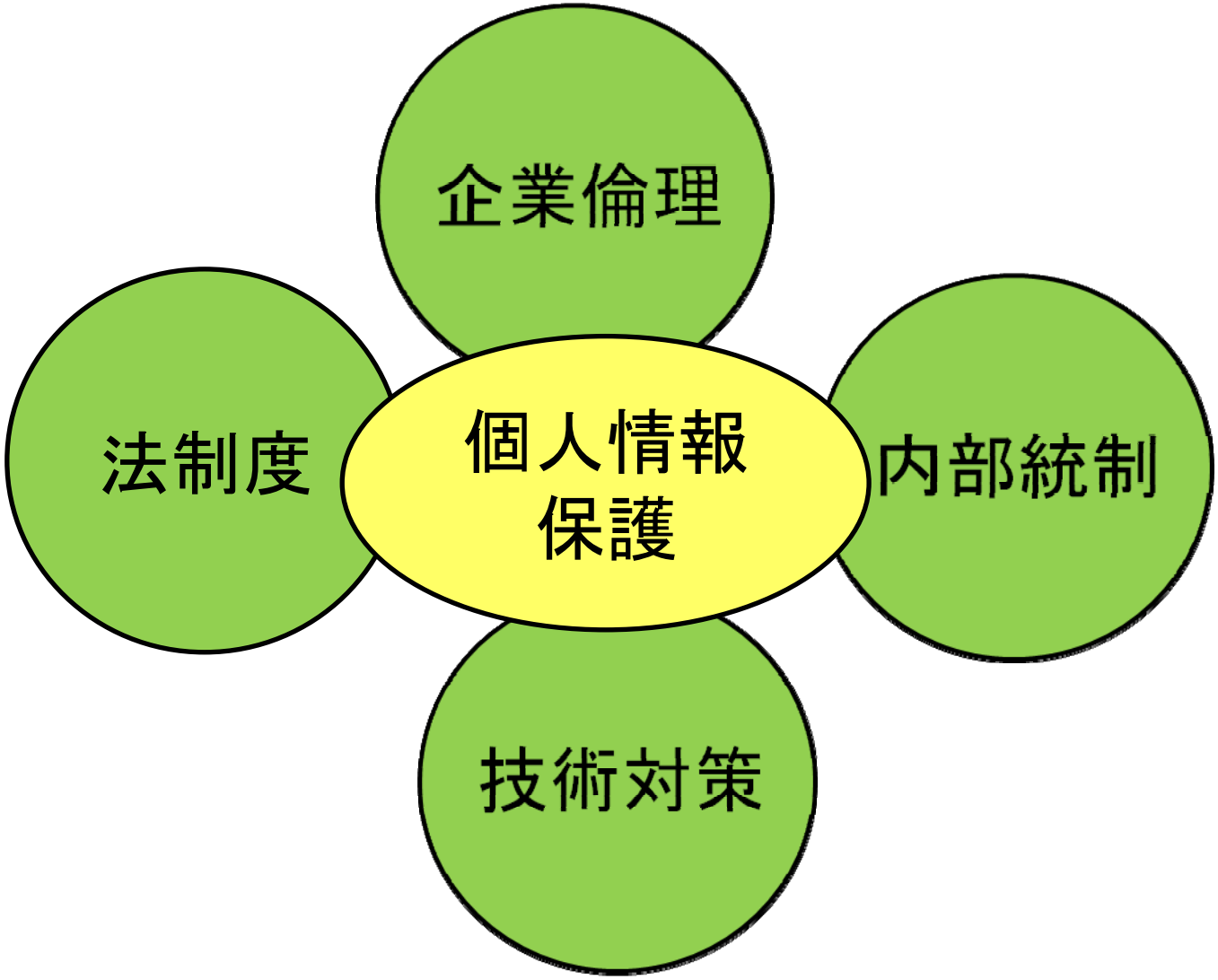
個人情報保護法は、どこへ行く

～事業者の誤認と、適正な個人情報保護のあり方～

今、企業に求められるプライバシー保護

2010年1月27日
ネットワンシステムズ株式会社
ビジネスアシュアランス株式会社
山崎　文明

個人情報保護を支える4つの要素



我が国の個人情報保護の課題

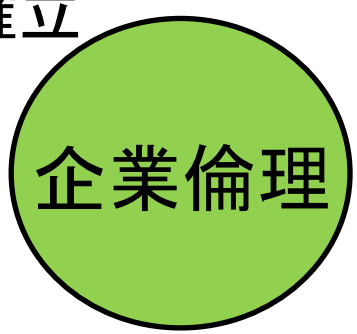
- 個人情報保護法 ≠ プライバシー保護法
  - データ件数による個人情報取扱事業者の定義
  - データベースを構成しなければ適用除外
  - 実態は「個人情報取扱法」
  - 欧州との比較においても改正が求められる3項目
    - **機微な情報収集の制限**
      - 人種的・民族的出自、政治的意見、宗教的信条、労働組合への加入、健康状態、性生活、犯罪の前科・容疑、犯罪・容疑の手続・処分・判決
    - **データマイニング（データマッチング）の制限**
    - **第三国へのデータ移転の制限**
      - 「個人データは、ヨーロッパ経済地域以外の国又は地域が個人データの取扱いに関しデータ主体の権利及び自由について十分な水準の保護を確保している場合を除き、その国又は地域に移転してはならない」
  - 急がれる漏えい事件の抑止対策としての名簿業者規制
    - 名簿業者の届け出制と身元確認の義務付け

法制度

我が国の個人情報保護の課題

求められる企業倫理

- 生活者の期待に応えるプライバシーポリシーの確立
  - 機微な情報を取得しない
  - 一線を越えたデータマイニングを実施しない
  - 国外でのデータ入力やDBの構築を行わない
  - 共同利用を名目とした個人情報の売買を行わない
  - 共同利用者の開示と共有情報の透明化
  - 自己情報のコントロール権に配慮した情報削除
- 個人情報保護教育からプライバシー保護教育への転換
  - 疑わしきは個人情報
  - オプトアウト至上主義から
    自己情報のコントロール権の尊重主義へ



我が国の個人情報保護の課題

- 個人情報保護のための技術対策の再確認
  - 個人情報取扱ポリシーの確立
    - 必要のない個人情報を保存しない
    - 必要以上の期間、個人情報を保存しない
    - データ伝送時は暗号化
    - 個人が特定できるデータアイテムの暗号化
    - 個人PCに個人情報を記録しない
    - 個人情報へのアクセスの制限
    - 個人情報へのアクセス記録の保存と分析
  - セキュリティの実装基準の作成と
    バリューチェーン全体への適用
    - 参考にできるPCI　DSS

PCI DSSとは

■ PCI DSS

- 国際カードブランド5社（JCB・American Express・Discover・MasterCard・VISA ）が、カードビジネス関連事業者向けに定めたカード会員データを保護するためのセキュリティ対策の「最低基準」
- 対象は、全てのデータ処理関係者（カード発行者、加盟店、サービスプロバイダー・・・）

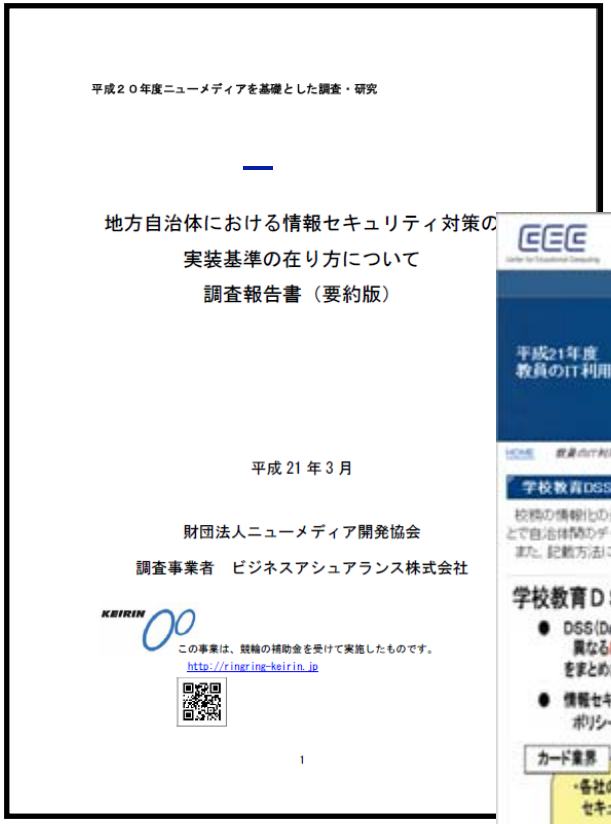
- 自己責任を基本としたISMSと絶対主義のPCI DSS

「パスワードの選択及び利用時に正しいセキュリティ慣行に従うことを利用者に要求しなければならない。」ISO/IEC27001:2005（JIS Q27001:2006）

PCIDSS要件 8 ： コンピュータにアクセスする利用者毎に個別の IDを割り当てること
8.5.8　グループ、共有または汎用のアカウントとパスワードを使用しないこと。
8.5.9　ユーザー・パスワードは少なくとも90 日ごとに変更する。
8.5.10 最小パスワード長は少なくとも7 文字以上にする。
8.5.11 数字と英字の組合せから成るパスワードを使用する。
8.5.12 直近4回に使用されたパスワードは、新しいパスワードとして使用できないようにする。
8.5.13 ユーザーIDをロックアウトすることにより、連続したアクセス試行を6回以内に制限する。
8.5.14 ロックアウト時間は30分間、またはアドミニストレータがユーザーIDを有効にするまでとする。

自治体DSS　学校教育DSS普及の取り組み

■ 自治体DSS
– ニューメディア開発協会


平成２０年度ニューメディアを基礎とした調査・研究

地方自治体における情報セキュリティ対策の
実装基準の在り方について
調査報告書（要約版）

平成 21 年 3 月

財団法人ニューメディア開発協会
調査事業者　ビジネスアシュアランス株式会社

この事業は、競輪の補助金を受けて実施したものです。
http://ringring-keirin.jp

1

■ 学校教育DSS
コンピュータ教育開発センター

技術対策

委嘱名	WG	氏名	所属
委員長		中川 正樹	東京農工大学 教授
副委員長	＊	山崎 文明	ビジネスアシュアランス株式会社 代表取締役社長
委員		赤倉 貴子	東京理科大学 教授
委員		榎本 竜二	東京都立工業高等学校 教諭
委員		大澤 一郎	独立行政法人 産業技術総合研究所 主任研究員
委員	＊	梶本 佳照	三木市立教育センター 所長
委員		宋住 伸子	津田塾大学 教授
委員	＊	曽田 耕一	NPO法人 上越地域学校教育支援センター 常務理事
委員	＊	豊田 祥一	ビジネスアシュアランス株式会社 執行役員
委員	＊	藤村 裕一	福井教育大学 准教授
委員	＊	三宅 健次	千葉大学教育学部付属中学校 教諭

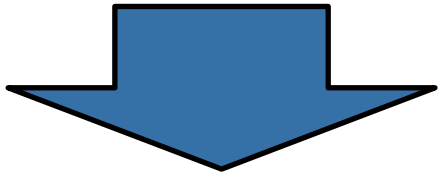
自治体DSS　学校教育DSS普及の取り組み

- 全国どの市町村でも一律に安全・安心な情報システム
  - ISMSから一歩進んだデータセキュリティ基準（DSS)へ
- 自治体DSS / 学校教育DSSの普及施策

技術対策

- 政府の認知
- ツールの整備（解説書、用語集、ガイドライン、評価ツール）
- DSS準拠セキュリティモデルのコンペ
- モデル自治体、モデル学校での実装と評価試験
- 義務化と免責制度
- 助成金制度

- 医療版DSSへの取り組み



プライバシーデータ・セキュリティ・スタンダード（PDSS）
個人情報を扱う一般企業への義務化もしくは免責条件化などなど

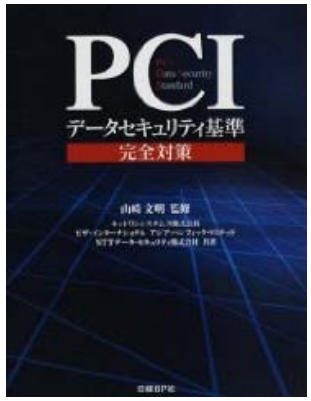
我が国の個人情報保護の課題

内部統制の有効性検証

- 防げたはずの部内者の犯行
- 「Need to Knowの原則」の徹底
  - 職位が上だから・・・
- 職務分掌（Segregation of duty）
  - 重要作業は必ず相互監視下で実施
  - 性善説から性弱説で業務分掌を設計
  - 必ず不法行為が検知、発覚する仕組み

自己紹介

ビジネスアシュアランス株式会社（http://www.biz-assure.co.jp）
事業内容　：　監査事業および監査関連事業
所在地　：　東京都品川区東品川2-2-8　スフィアタワー天王洲
代表取締役社長　：山崎　文明
システム監査技術者
医療情報技師
システム監査、情報セキュリティ、個人情報保護に関する専門家として
情報セキュリティに関する政府関連委員会委員を歴任。



価格　：　2,940円
判型　：B5変形判／247ページ
ISBN　：　4-8222-6223-5
発行　：日経BP社
発売　：日経BP出版センター
2008年4月14日発行

■　委員などの就任実績
内閣官房安全保障危機管理室　情報セキュリティ対策推進室WG委員
警察大学校不正アクセス犯罪等対策専科講師
学校セキュリティ検討委員会委員（経済産業省）
サイバーテロ演習評価委員会委員（経済産業省）
不正プログラム調査研究委員会委員（警察庁）
サイバーセキュリティ調査研究委員会委員（警察庁）
先導的ITスペシャリスト育成推進プログラム外部評価委員会委員（文部科学省）
専門ADR委員(戦略的IT紛争解決 IT-ADRセンター)
工学院大学技術者能力開発センター客員講師

■　お問い合わせ
電話:03-5462-0698
メール：toiawase@biz-assure.co.jp

ビジネスアシュアランス株式会社