

自治体総合フェア2008  
自治体テーマセミナー

# 自治体情報セキュリティ対策の最新動向と課題

～ますます重要になる住民個人情報保護～

2008年7月17日

---

工学院大学 技術者能力開発センター客員講師  
山崎文明

# 我が国の個人情報保護法の課題

## ■ 個人情報保護法改正議論

- 拡大解釈による弊害
- 過剰反応
  - － 緊急時の個人情報提供拒否

## ■ 「個人情報の保護に関する基本方針」の一部変更

(2008年4月25日閣議決定)

- いわゆる「過剰反応」を踏まえた取組

昨今、プライバシー意識の高まりや個人情報を取り扱う上での戸惑い等の様々な要因から、社会的な必要性があるにもかかわらず、法の定め以上に個人情報の提供を控えたり、運用上作成可能な名簿の作成を取り止めたりするなど、[いわゆる「過剰反応」が生じている](#)。

国民生活審議会は、「個人情報保護に関する取りまとめ(意見)」(平成19年6月29日)において、法の具体的な内容の広報・啓発等、[いわゆる「過剰反応」対策に万全を期することを求め](#)、政府も、個人情報保護関係省庁連絡会議を開催し、今後の対策を決定(「個人情報保護施策の今後の推進について」(平成19年6月29日決定))し、実施している。(中略)

また、[いわゆる「過剰反応」が生じる背景](#)には、個人情報によって識別される特定の個人が自らの個人情報の取扱いに不安を感じていることも一因としてあると考えられることから、法の適切な運用等により、個人情報の適切な取扱いを図っていく必要がある。

# 我が国の個人情報保護法の課題

## ■ 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・容疑の手續・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」

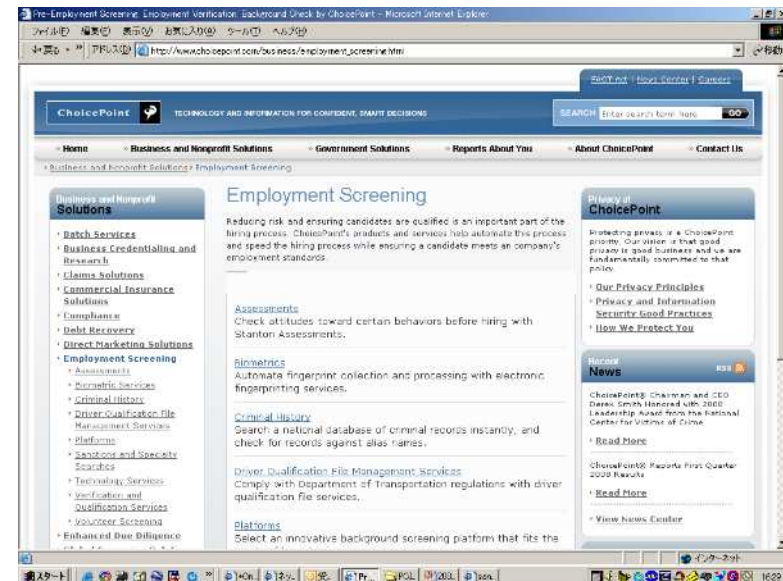
# 名寄せされる個人情報

## ■ 米国企業に見るデータマイニングの実態

- 増加し続けるデータマッチング・キー
  - 携帯電話番号、クレジットカード番号、電子マネー番号、
- 商品として扱われる個人情報 データブローカー
- 世界最大の個人情報販売会社 Choice Point社
  - 売上 1000億円 NYSE上場 従業員5千名以上
  - 2億2千万人 170億レコード 250テラバイト
  - DBT「AutoTrackXP」

## ■ 問われるセキュリティとプライバシーのバランス

- Nanny
  - サイバー空間上のnanny



# 益々重要になる自治体のセキュリティ

## ■ 住基カード普及促進のため転居後も継続使用

- 総務省は住民基本台帳カードの普及を進めるためカードを取得した市町村から別の市町村へ引っ越すと失効する仕組みを改め、転居後も継続して同じカードを使えるようにする方針を決めた。今後、偽造防止策の技術的課題を詰め、転居時のカード返納を義務付けた規定を住民基本台帳法から削除するなど具体的な制度改正の検討に入る。住基カードでは利用者から「使い勝手が悪い」との声が出ていた。(5月11日 共同ニュース)

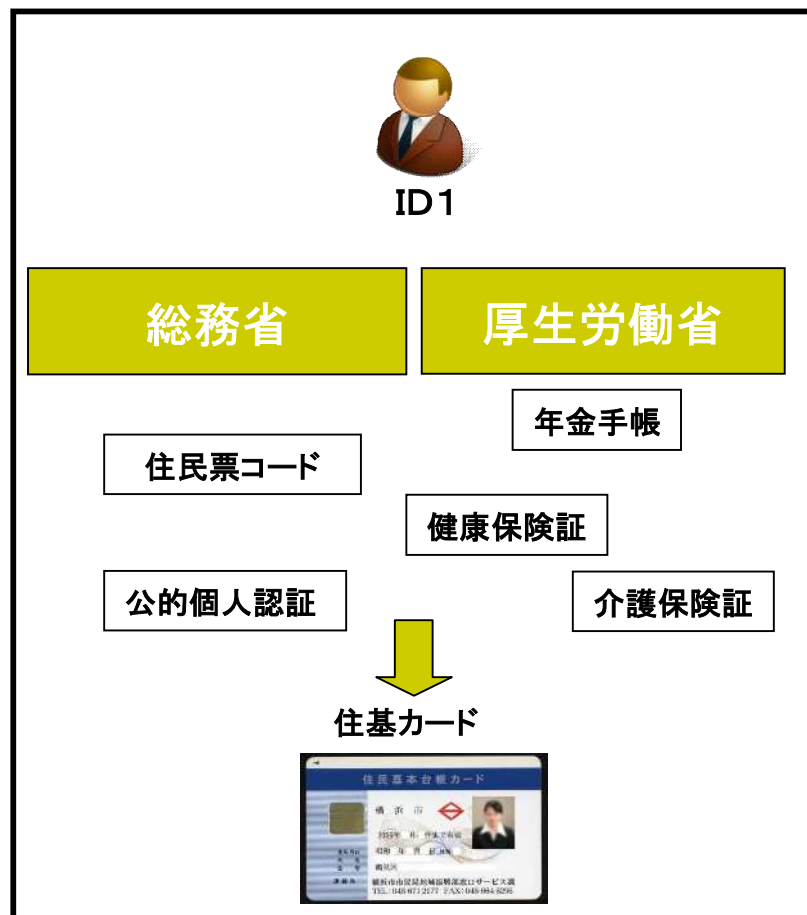
# 益々重要になる自治体のセキュリティ

## ■ 社会保障・住基一体カード 厚労・総務省が発行を検討

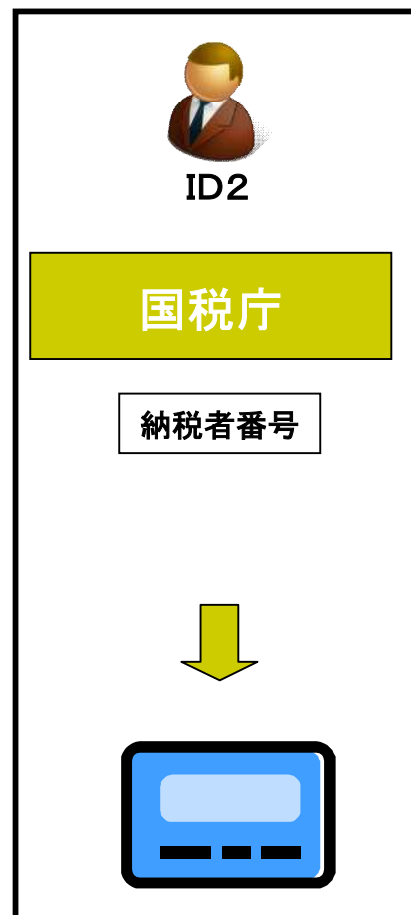
- 厚生労働省が2011年度の発行を目指して準備を進めている社会保障カードと、総務省がすでに発行している住民基本台帳カードを1枚に統合することで両省が検討に入った。住基ネットの活用によってシステム投資などを節約する。治療記録から住所情報まで一つのシステムでつながることから、プライバシーを保護するための情報管理の徹底が課題になる。新しいカードは「社保・住基カード」(仮称)。厚労省の原案によると同カードの発行主体は同省で、発行窓口は住基カードと同様に市町村が担う。原則として1人に1枚ずつ無料で発行する方向。持っていないと健康保険が使えないなどの不便が出てくるため、最終的にはほぼすべての国民が所持することになりそうだ。(5月31日 日本経済新聞)

# IDの附番とデータマイニング対策

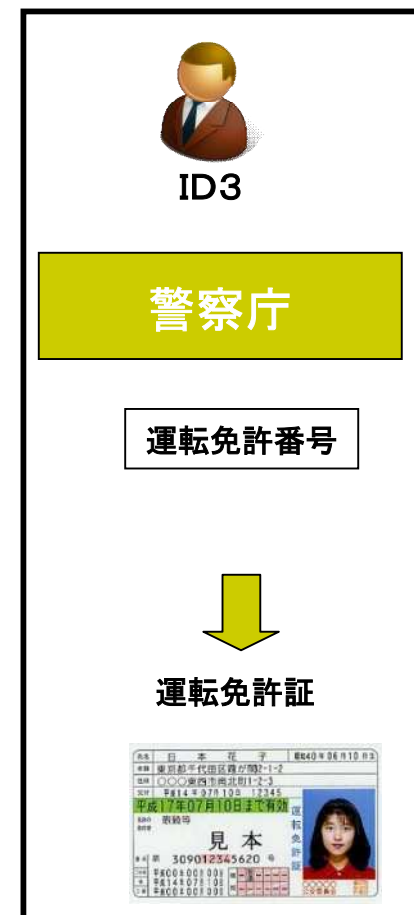
FLAT MODEL



SEPARATED MODEL



SEPARATED MODEL



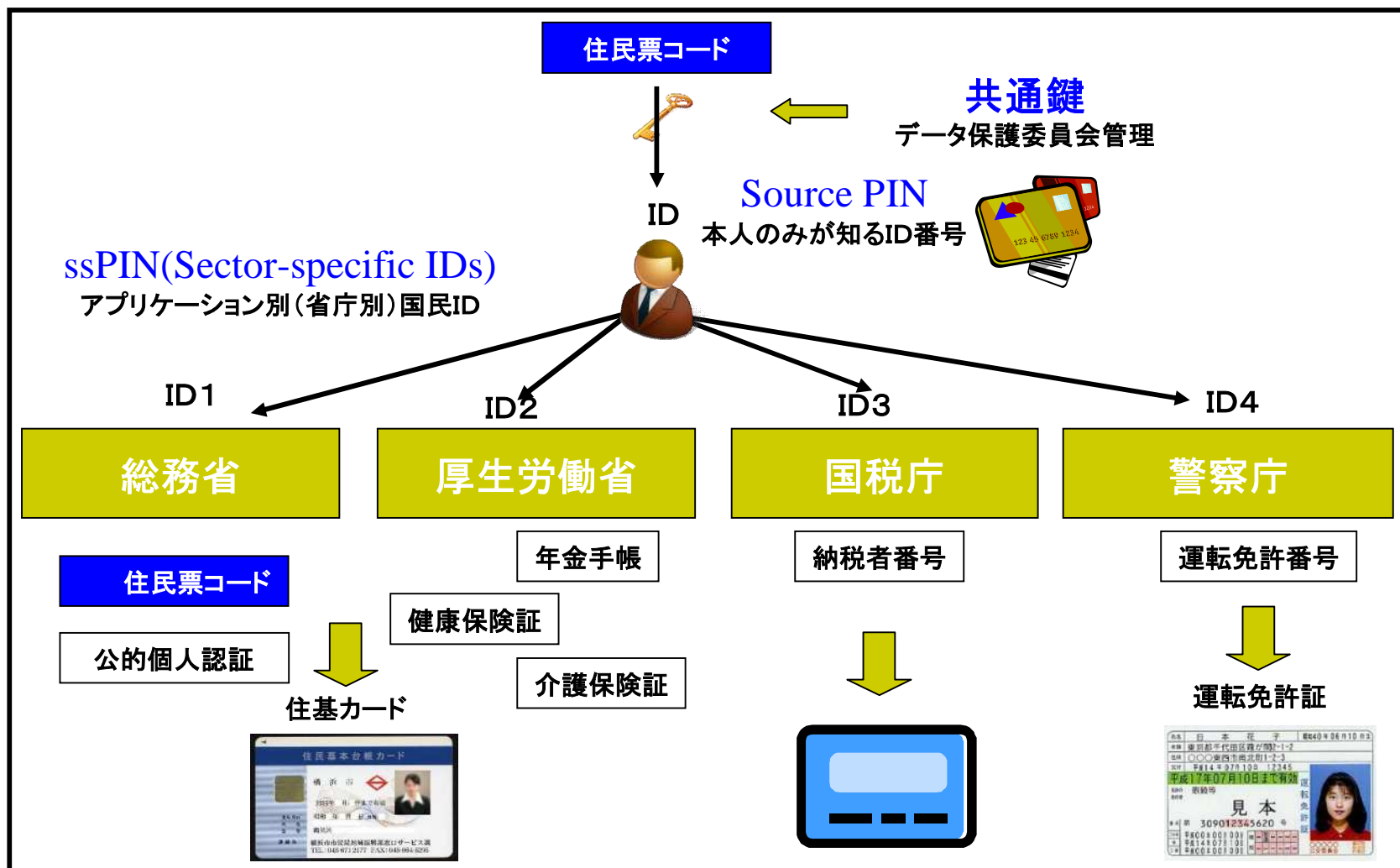
# IDの附番とデータマイニング対策

---

- フラットモデル (Flat Model)
  - ID漏えい被害が広範囲に及ぶ
  - 再附番に膨大なコストと労力が必要
  
- セパレートモデル (Separated Model)
  - ID漏えい被害はアプリケーション単位に止まるが利便性が劣る
  - 再附番に膨大なコストと労力が必要
  
- セクトラルモデル (Sectoral Model)
  - 利用者は1つのIDで異なるアプリケーションにアクセスでき、かつID漏えい被害はアプリケーション単位に止まる

# IDの附番とデータマイニング対策

## SECTORAL MODEL



# システムに求められる新たな視点

---

## ■ 本人が自分の情報を確認できる仕組み

- 個人情報へのアクセス記録
- (年金納付記録、治療履歴……)

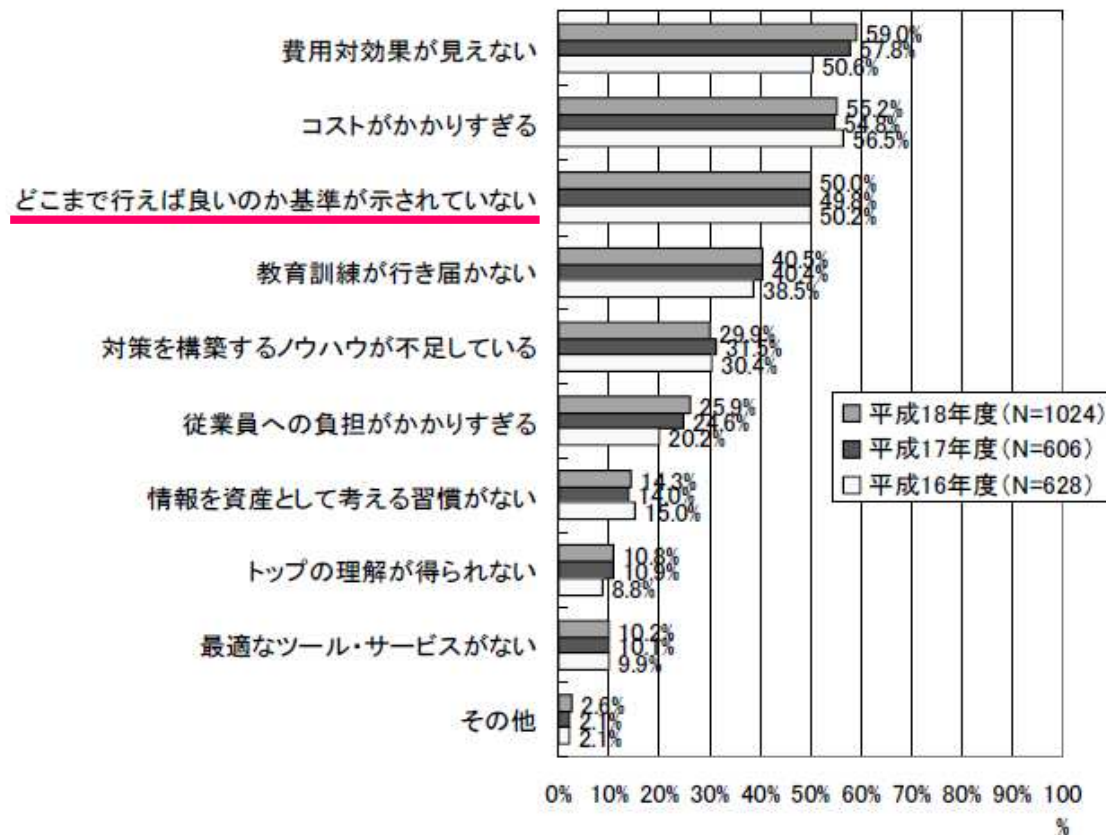
## ■ 情報漏えいに強い仕組み

- 漏えい情報の極小化
- (再附番の容易性)

# ポリシー策定済自治体100%

## ■ 半数は何をどこまでやればいいのかわからない

【経年変化】情報セキュリティ対策実施上の問題点



日本人が  
最も苦手な  
自己責任

「平成19年1月不正アクセス対策等の実態調査（警察庁生活安全局情報技術犯罪対策課）」より抜粋

# 実装基準の普及に乗り出した産業界

## ■ Payment Card Industry Data Security Standard

- 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…）

## ■ PCI DSSの本質はサプライチェーン・リスクマネジメン

- カード会員データを住民個人情報と読み替えると自治体にも当てはまる考え方



価格 : 2,940円(税込み)  
判型 : B5変形判/約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

# 実装基準としてのPCIDSS

安全なネットワークの構築・維持	要件 1 : カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること 要件 2 : システムパスワードと他のセキュリティ・パラメータにベンダー提供のデフォルトを使用しないこと
カード会員データの保護	要件 3 : 保存されたカード会員データを安全に保護すること 要件 4 : 公衆ネットワーク上でカード会員データを送信する場合、暗号化すること
脆弱性を管理するプログラムの整備	要件 5 : アンチウイルス・ソフトウェアを利用し、定期的に更新すること 要件 6 : 安全性の高いシステムとアプリケーションを開発し、保守すること
強固なアクセス制御手法の導入	要件 7 : カード会員データへのアクセスを業務上の必要範囲内に制限すること 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 要件 9 : カード会員データへの物理的アクセスを制限すること
定期的なネットワークの監視 およびテスト	要件 10 : ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること 要件 11 : セキュリティシステムおよび管理手順を定期的にテストすること
情報セキュリティ・ポリシーの整備	要件 12 : 情報セキュリティに関するポリシーを整備すること

# 自己責任のISMS vs PCI DSS

■ 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回に使用されたのと同じパスワードは、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。

# 導入が求められる自治体版DSS

- 何をどこまでやればいいのか判断できていない現実
  - わかりやすい説明責任 クレジットカード会社なみのセキュリティ対策
- 各自治体のポリシーに委ねていて良いのか
  - セキュリティ対策のボトムラインを明確に関係会社に要求
  - 実装レベルのベースライン標準仕様を固める時期
    - 欧米のエンタープライズでは使用製品まで規定
  - 目指すべきは **One World**
- GAP分析が示す今後の道筋
  - あと幾ら投資が必要かは首長はじめ経営にとって重要な情報

## Local Government DSS

# 講師紹介



価格 : 9,975円(税込み)  
判型 : B5変形判/約280ページ  
ISBN : 4-8222-2131-8  
発行 : 日経BP社  
発売 : 日経BP出版センター  
2004年10月1日発行

工学院大学 技術者能力開発センター客員講師  
ビジネスアシュアランス株式会社 代表取締役社長  
山崎 文明(やまさき ふみあき)  
システム監査技術者(経済産業省)  
英国規格協会 BS7799情報セキュリティ・スペシャリスト  
(元)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  
(元)警察庁不正アクセス犯罪等対策専科講師  
平成19年度学校セキュリティ検討委員会委員  
平成18年度学校セキュリティ検討委員会委員  
平成17年度学校セキュリティ検討委員会委員  
平成16年度経済産業省サイバーテロ実験評価委員  
平成13年度警察庁不正プログラム調査研究委員会委員  
平成12年度警察庁サイバーセキュリティ調査研究委員会委員



価格 : 1,680円(税込み)  
判型 : 四六判/272ページ  
ISBN : 4-8222-2061-3  
発行 : 日経BP社  
2005年1月11日発行

警察政策学会正会員  
日本リスク・マネジメント学会正会員  
システム監査、ネットワークセキュリティ、セキュリティポリシーに関する専門家。  
大手会計監査法人にてシステム監査に永年従事。  
著書に、「すべてわかる個人情報保護」(日経BP社 最新刊)、「情報セキュリティハンドブック」(オーム社)、「情報セキュリティと個人情報保護 完全対策」(日経BP社)、「システム監査の方法」(中央経済社)、「コンティンジェンシー・プランニング」(日経BP)、「セキュリティマネジメント・ハンドブック」(日刊工業新聞社)等がある。



「学校情報セキュリティ・ハンドブック改訂版(平成18年度)」  
財団法人コンピュータ教育開発センターから無償配布中