総務省

地方公共団体における情報セキュリティ対策の現状

H20.9.4　**基本計画検討委員会**

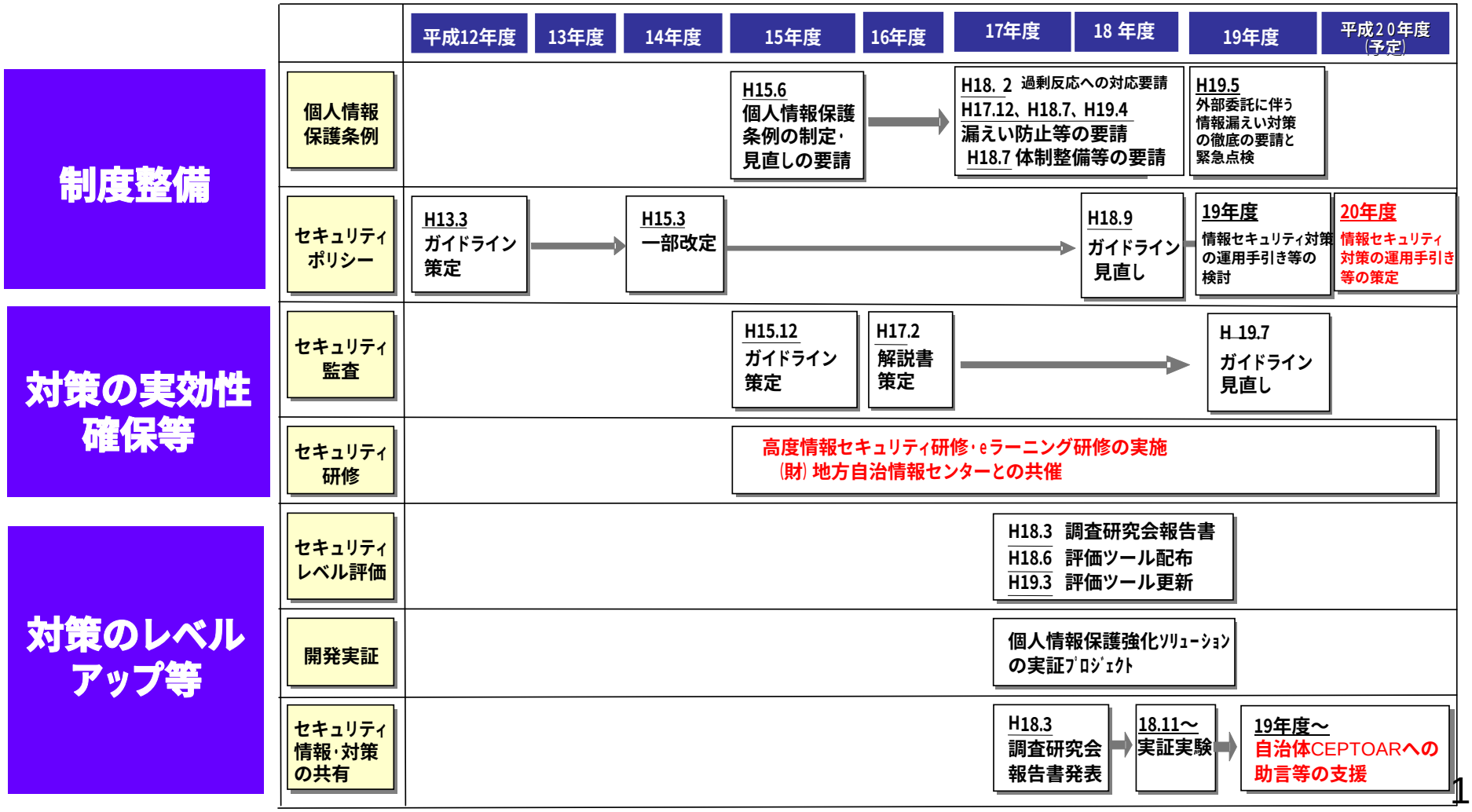
総務省自治行政局地域情報政策室

資料２

個人情報保護・情報セキュリティ対策強化の取組

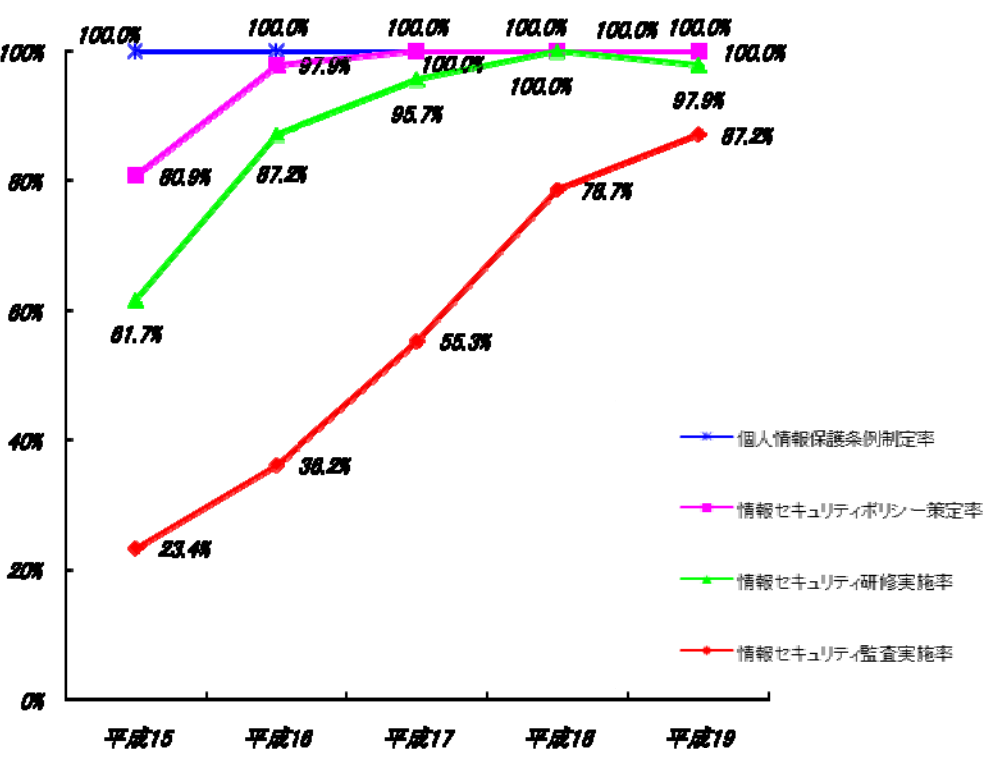
総務省

○ 個人情報保護条例や情報セキュリティポリシーの整備などの制度整備を推進
○ また、平成１５年度より対策の実効性確保等のため情報セキュリティ監査や研修を支援
○ さらに、平成１７年度より対策のレベルアップ等を図るため、各団体のセキュリティレベルの評価ツールの作成や個人情報保護強化のための開発実証、情報・共有分析センター創設支援を実施

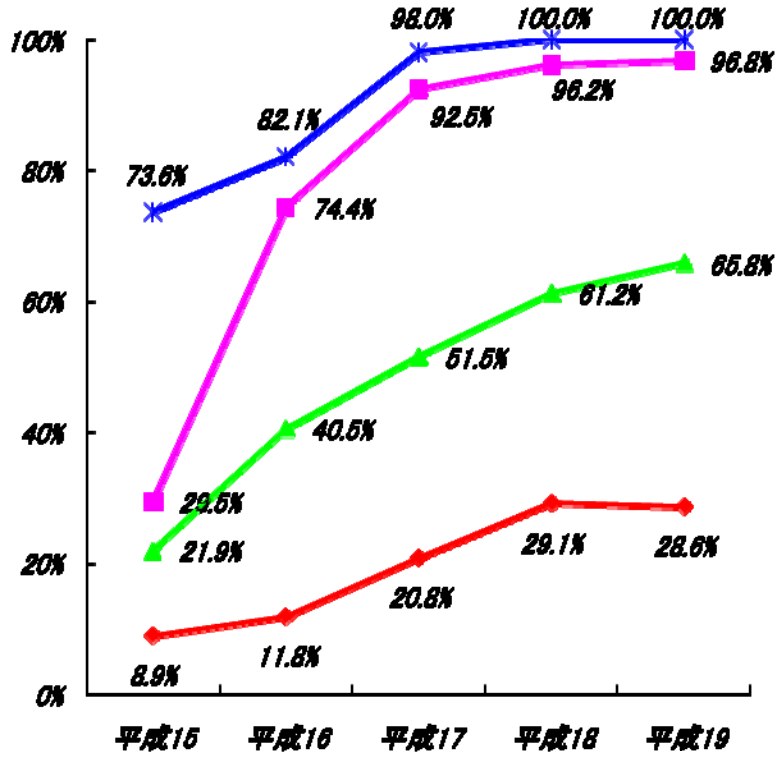


情報セキュリティ対策の現状

総務省



都道府県



市町村

外部委託に伴う情報漏えい事案について

総務省

電算業務の再委託を受けた会社の従業員が、データを自宅に持ち帰り、自宅パソコンに保存したところ、自宅パソコンからファイル交換ソフト「Winny」を通じて情報が流出する事案が発生

＜本事案から判明した課題＞

① 業務の委託先事業者による無断での再委託 ② 従業員によるデータの無断持ち出し

③ 業務委託終了後のデータの返還・廃棄の不徹底

＜対応策＞

Ⅰ 緊急点検と総務省への報告

● 無許可での再委託の有無 ●データの無断持ち出しの有無 ●業務終了後のデータの返還・廃棄の確認

Ⅱ 厳正な対応の地方公共団体への要請

● 個人情報保護条例の罰則対象に受託業者を追加していない団体が依然として約4割存在(H18.4.1現在)。
このため、罰則対象に受託業者を追加することを要請。

● 契約に違反した場合に、委託業者に対し、厳正な措置(違約金・損害賠償請求・契約解除・入札資格の制限等)をとることを要請。

● 委託業者に対する監督(報告徴収・立入検査など)の強化を要請。等

Ⅲ さらに住民基本台帳情報の取扱いの厳格化に関する検討会を開催

地方公共団体における情報セキュリティポリシーに関するガイドラインの見直し（平成18年9月）

総務省

Ⅰ　地方公共団体のセキュリティ対策の水準を強化

- 情報漏えい防止等のため取るべき対策や生体認証等最近の技術的動向を踏まえた規定を追加
- セキュリティ対策を強化する観点から、各地方公共団体において必要に応じ実施することが望まれる事項については、「推奨事項」と明記して例文に挿入
- 地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献することが望まれる旨、記述　　等

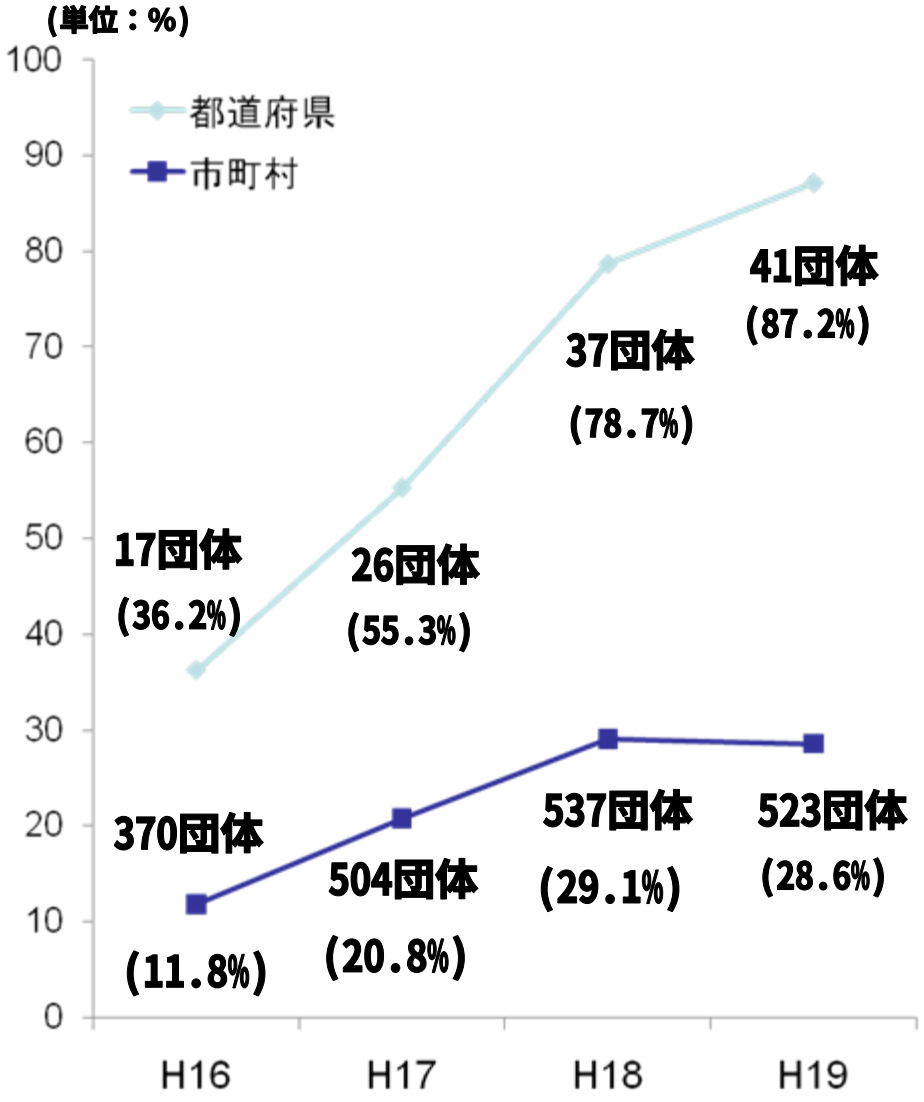
Ⅱ　重要インフラ指針への対応

- 重要インフラ指針において列記された項目に対応
- 情報のライフサイクルに着目した対策の明示
- 機密性、完全性、可用性の観点からの情報の格付けや取扱い制限の明示　等

Ⅲ　分かりやすい表現に変更

- 全体を、「総則」、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」の三章構成に整理
- 情報セキュリティ対策基準の構成を、PDCAサイクルを踏まえて変更。また、各対策の説明を、趣旨、例文、解説の順に統一
- 責任主体を明記し、権限と責任を明確化　等

情報セキュリティ監査の推進



総務省等の施策等

□情報セキュリティ監査ガイドラインの見直し
・情報セキュリティポリシーガイドラインの改定（平成18年9月）を踏まえ、構成、内容等を全面的に見直し
□情報セキュリティ内部監査研修の実施
・LASDECと共同で開催している情報セキュリティ研修において実施
□内部監査アドバイザーの派遣(LASDEC)
□地方財政措置

地方公共団体独自の工夫

(例)
□職員を内部監査要員として育成
□外部監査の実施で監査技法を習得
□県と県内市町村によるセキュリティ監査の共同アウトソーシングを実施し、セキュリティレベルを相対比較

地方公共団体における情報セキュリティ監査に関するガイドラインの見直し（平成19年7月）

総務省

地方公共団体の情報セキュリティ水準の向上を推進するため、「地方公共団体における情報セキュリティポリシーに関するガイドライン」の全部改定（平成１８年９月）に続き、「地方公共団体情報セキュリティ監査ガイドライン」（平成１５年１２月）を全面的に見直した。

新ガイドラインの構成

第1章　総則
ガイドラインの目的、策定の経緯、監査の意義と種類、ポリシーガイドラインとの関係、構成

第2章　監査手順
準備、計画、実施、報告、結果への対応、結果の公表、フォローアップ監査、外部監査人の調達

第3章　監査項目
対象範囲、組織体制、情報資産の分類と管理方法、物理的セキュリティ、人的セキュリティ、技術的セキュリティ、運用、評価・見直し

付録
監査証拠例一覧／索引、監査実施要綱（例）、監査実施計画書（例）、監査報告書（例）、監査業務委託仕様書（例）、監査業務委託契約書（例）

新ガイドラインの特徴

1．監査水準の強化
・ポリシーガイドラインに対応
　・個人情報の漏えい等のさまざまな情報セキュリティ侵害事案の発生
　・新たな技術対策の動向
　・政府の情報セキュリティ政策　等

2．監査の準備作業の軽減
・ポリシーガイドラインに即した内容

3．監査項目の簡素化
・３１７項目に簡素化（旧ガイドラインは９７５項目）
・はじめて情報セキュリティ監査を行う場合等の初期段階における必須の監査項目として１１０項目選定

地方公共団体職員を対象とする情報セキュリティ研修

総務省

総務省と(財)地方自治情報センター(LASDEC)が共催

高度情報セキュリティ研修 19年度まで

情報セキュリティ対策の中核を担う高度な知識・技術を持つ人材の育成を短期間で集中的に行うことを目的として実施。

＜平成19年度の研修実績＞※e-ラーニングによる情報セキュリティ研修に統合

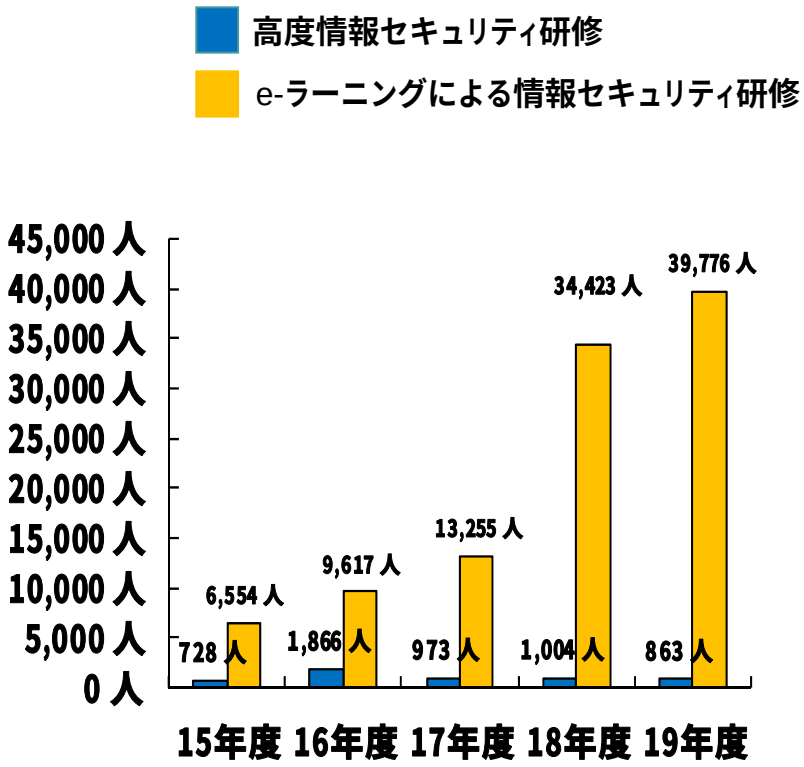
■ 全国主要都市で開催

- ○ 情報セキュリティ管理研修　5日間×13回
- ○ 情報セキュリティ基礎技術研修　5日間×13回
- ○ 情報セキュリティ応用技術研修　5日間×13回
- ○ 情報セキュリティ内部監査研修　5日間×13回

■ 受講者数：各研修30名　合計863名

e－ラーニング 延べ10万人が受講

地方公務員を対象にインターネットを用いたe-ラーニングによる情報セキュリティ研修を実施。



受講者数の推移

＜平成20年度の研修予定＞

■情報セキュリティポリシーガイドライン(平成18年9月)を踏まえ、セキュリティ対策のための組織体制に基づいて5つのコースを設定。

コース名	対象者	内容
統括責任者コース	副市町村長、CIO補佐官等	情報資産の管理、セキュリティ対策実施の基本的事項等
管理職員コース	部局長、課室長等	各部局等における情報セキュリティ対策実施の基本的事項等
情報システム職員コース	情報システム担当課長等	個々の情報システムの開発、運用等の場面におけるセキュリティ対策実施の基本的事項等
一般職員コース	すべての職員等	情報セキュリティの考え方等必要最小限の知識の解説
新採用職員コース	新規採用者等	すべての職員の身近に存在する脅威、その対策等の解説

ＬＡＳＤＥＣによる「自治体セキュリティ支援室」の設置

(財) 地方自治情報センターは、平成１９年３月３０日に地方公共団体における情報セキュリティ対策の支援を行う「自治体セキュリティ支援室」（ＬＡＳＣ（Local Authorities Security Support Center)を設置

【自治体セキュリティ支援室が行う主な業務】

(1) 自治体CEPTOARとしての業務

ア 内閣官房情報セキュリティセンター(NISC)から総務省を通じて提供されるIT障害等をLGWANメールにより地方公共団体へ**一斉通知**

イ LGWANを活用し**メールマガジン**、**ポータルサイト**により、情報セキュリティ対策に関する各種情報提供(自治体の事故事例・取組事例、JPCERT/CCの早期警戒情報等)

(2) 情報セキュリティ支援事業(IDSによる庁内LAN監視)

インターネットから庁内LANに出入りする不正アクセスやウイルスを監視装置で常時モニター(１８，１９年度)

(3) 情報セキュリティ遠隔診断

Webサーバ、メールサーバ及びネットワーク機器等を外部から遠隔診断することにより、セキュリティホールの発見と是正策を提供

(4) Webアプリケーション診断

ＳＱＬインジェクション(ホームページ改ざんの手口の一つ)などのwebアプリケーションを狙った攻撃に対する脆弱性の診断

(5) 人材育成（研究開発部、教育研修部との共催）

ｅーラーニング、内部監査アドバイザーの派遣、情報セキュリティ講師の派遣等

(注) ＣＥＰＴＯＡＲとは、Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略。重要インフラ分野で整備する「情報共有・分析機能」のこと。

情報セキュリティ強化に向けた取組み

総務省

◆地方公共団体における情報セキュリティ対策の強化が必要

- 個人情報の漏えいなどの情報セキュリティに関する事故が相次いで発生。
- 情報セキュリティポリシーレベルでの制度面は整備されつつあるが、具体的な運用レベルになると不十分な団体が多い。

◆ 運用面からの対策が不十分

- 情報資産のリスク分析や情報システムに関する事業継続計画(BCP)の策定など、具体的な実施方法が分からない等の理由により、実施されにくいものがある。

運用の手引き・ツールの作成

「電子自治体の推進に関する懇談会セキュリティWG」（座長：大山永昭東京工業大学教授）において、以下の検討を実施

情報資産の リスク分析ツール	ICT部門の業務継続計画 （BCP）ガイドライン策定 (8/21通知、公表)	外部委託時の個人情報 漏えい防止対策 (契約書のひな型等)