個人情報保護ガイドラインと情報セキュリティ監査について

2004年6月29日

経済産業省　商務情報政策局
情報セキュリティ政策室
田辺雄史
tanabe-takefumi@meti.go.jp

本日の内容

1．個人情報保護ガイドラインの概要

2．情報セキュリティ監査の動向

3．情報セキュリティ政策の最近の動き

4．まとめ

1．個人情報保護ガイドラインの概要

定義　その1

「個人情報データベース等」を事業に用いている者＝「個人情報取扱事業者」

「個人情報取扱事業者」が、個人情報の保護の義務を負うとしているため、本ガイドラインで、「個人情報」、「個人情報データベース」とは何か、どのような事業者が「個人情報取扱事業者」にあたるのか 等について具体的事例とともに示す。

法第2条　この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。

ガイドライン

◆氏名、性別、生年月日等に限られず、個人の身体、財産、職種、肩書き等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされているものや、映像、音声も含まれ、暗号化されているかどうかを問わない。

◆「生存する個人」は日本国民に限られず、外国人も含まれるが、法人その他の団体は「個人」に該当しないため、法人等の団体に関する情報は含まれない。

定義　その2

個人情報データベース等

法第2条2　この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるものをいう。

一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

ガイドライン

◆特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した個人情報を含む情報の集合物

◆コンピュータを用いなくても、カルテや指導要録など、紙面で処理した個人情報を一定の規則（例えば、五十音順、年月日順等）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているもの

定義　その3

個人情報取扱事業者

法第2条3　この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。

一～五　（略）

ガイドライン

◆国の機関、地方公共団体、独立行政法人以外で、取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ない者※1を除いた、個人情報データベース等を事業の用に供している者。

※1：個人情報データベース等を構成する個人情報によって識別される特定の個人の数※2の合計が過去6ヶ月以内のいずれの日においても5000人を超えない者。

※2：カーナビ、電話帳のような他人の作成による氏名、住所又は電話番号のみを含んでいる個人情報データベースで、新たに個人情報を加えたり、他の個人情報を付加したりして、データベースそのものを変更するようなことをせずに、事業の用に供する場合は、その個人情報データベース等に含まれる個人の数は、上記※1の「特定の個人の数」には算入しない。

個人情報取扱事業者の義務

■事業者の義務のうち、特に、「利用目的の特定、通知・公表」、「安全管理措置」、「従業者の監督」、「委託先の監督」、「第3者提供の制限」については、義務の中核となることから、できるだけ具体的にとるべき措置を示す。

利用目的の特定（第15条関係）

法第15条　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的(以下「利用目的」という。)をできる限り特定しなければならない。

2　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

ガイドライン

◆利用目的の特定に当たっては、可能な限り具体的に特定するとともに、個々の処理の目的を特定するにとどめるのではなく、個人情報取扱事業者において最終的にどのような目的で個人情報を利用するかを特定する必要がある。

◆「○○事業※における商品の発送、新商品情報のお知らせ、関連するアフターサービス」等を利用目的とすることが挙げられる。単に「当社の事業活動」、「お客様のサービスの向上」等を利用目的とすることは、できる限り特定したことにはならない。

※「○○事業」の特定に当たっては、社会通念上、本人から見てその特定に資すると認められる範囲に特定することが望ましい。例えば、日本標準産業分類の中分類から小分類程度の分類が参考になる。

安全管理措置（法第２０条関係）

法第２０条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

ガイドライン

◆個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、及び技術的安全管理措置を講じなければならない。

◆その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱い状況等に起因するリスクに応じ、必要かつ適切な措置を講じる。（本ガイドラインでは、各安全管理措置を講じる際に望まれる事項を具体的に示した。）

各措置について

組織的安全管理措置

◆安全管理について従業者（法第２１条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下規程等という）を整備運用し、その実施状況の確認を行うことをいう。組織体制の整備、規程等の整備と規程等に従った運用、個人データ取扱台帳の整備、評価、見直し及び改善、事故又は違反への対処などがある。

人的安全管理措置

◆従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練などを行うことをいう。雇用及び契約時における非開示契約の締結や、従業者に対する教育・訓練の実施などがある。

物理的安全管理措置

◆物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止などの措置をいう。入退館（室）管理の実施、盗難等に対　する対策、機器・装置等の物理的な保護などがある。

技術的安全管理措置

◆技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視など、個人データに対する技術的な安全管理措置をいう。アクセスにおける識別と認証、アクセス制御、アクセス権限の管理、アクセスの記録、情報システムに対する不正ソフトウェア対策、移送・通信時の対策、情報システムの動作確認、情報システムの監視などがある。

情報セキュリティ監査との関係

個人データの安全管理措置の評価、見直し及び改善をする上で望まれる事項
～組織的安全管理措置の一部～

- 監査計画の立案と、計画に基づく監査（内部監査又は外部監査）の実施
- 監査実施結果のとりまとめと、代表者への報告
- 監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善

2．情報セキュリティ監査の動向

「情報セキュリティ監査制度」とは

- 「情報セキュリティ監査制度」とは、(1)企業等の情報セキュリティ対策（外部からの不正アクセス防止の設定をしているか、情報管理責任者を任命しているか等）について、(2)客観的に定められた国の基準に基づいて、(3)独立した専門家が(4)評価（保証または助言）する制度。
  - http://www.meti.go.jp/policy/netsecurity/audit.htm
    - 2003年4月、「情報セキュリティ管理基準」及び「情報セキュリティ監査基準」を、経済産業省告示により公表。これに基づき、制度運用開始。
    - 監査主体は「情報セキュリティ監査企業台帳」に登録され(380事業主体)、公表。毎年7月に更新。「日本セキュティ監査協会」（ＪＡＳＡ）にて、監査の質の向上のための取り組み。

- 地方自治体向けの情報セキュリティ監査については、2003年12月総務省が「地方公共団体情報セキュリティ監査ガイドライン」を策定。
  - http://www.soumu.go.jp/s-news/2003/031225_12.html

制度の位置付けを改めて整理すると・・・

■ 基準も主体も「義務付け」ではなく「推奨」からスタート

- まずは、全プレイヤーが乗る「一つの基盤」を構築
- バラバラであった「情報セキュリティ監査」の統一
- ユーザの選択を助ける
- 各主体への展開は「カスタマイズ」
- そういう意味では、各主体への展開は監査主体の能力に大きく依存
- 「一つの基盤」の上で、監査の質の向上を指向

制度開始後1年間に起こったこと（その1）

■ 日本セキュリティ監査協会（JASA）の設立

- 監査の質の向上を図るための取り組みを行うための組織
- 「普及促進部会」「技術部会」「スキル部会」「調査研究部会」を設置し活動
- 「技術部会」では監査マニュアルの策定、「スキル部会」では監査人研修の実施、資格制度のあり方の検討等・・・
- 現在、「審査委員会」の設置を検討中。協会加盟組織の質の確保を指向。

http://www.jasa.jp/

JASA 特定非営利活動法人 日本セキュリティ監査協会 http://www.jasa.jp

制度開始後1年間に起こったこと（その2－1）

■ 「監査」を調達等の基準に位置づける動き

– 防衛庁

- 「防衛関連企業における情報セキュリティ確保について」
  http://www.jda.go.jp/j/info/security/index01.htm
- 防衛庁が「体系」（「基本方針」、「基準」（37の管理項目）、「実施要領」）を策定
- 防衛庁の情報システム受注企業に対し、その企業における「体系」の策定を要求
- 防衛庁策定の「体系」との適合性を「監査」
- 平成16年4月以降の契約に適用

制度開始後1年間に起こったこと（その2－2）

■ 「監査」を調達等の基準に位置づける動き

– VISA

- **クレジットカード情報の漏えいを防止する「アカウント情報セキュリティ（AIS）プログラム」を策定**
  (2004/5/18)
  http://www.visa.co.jp/secured/index.shtml
- **VISAカード決済の月間平均取扱件数によって以下を実施**
  - **問診票による自己診断**
  - **脆弱性スキャニングテスト**
  - **訪問調査**
- **「監査を受けていると検証作業が免除される可能性もあります」（上記HPより）**

制度開始後1年間に起こったこと（その3）

■ 個人情報漏洩事件と監査

- 事件後の対応の中に「監査」を入れるケース
- ACCAの例
  - 「情報セキュリティ監査および情報セキュリティ教育の実施について」（2004/4/20）
    http://www.acca.ne.jp/release/040420.html
  - 再発防止策の一環として情報セキュリティ監査の実施（2004/4～6）を決定。併せて、今後の情報セキュリティ監査の定期的な実施も宣言。
  - 特に、「個人情報保護の管理体制・プロセス」、「情報セキュリティの管理体制・プロセス」、「システムセキュリティの確保」の3点を中心。
- 事後対応ではなく、事前対応で行っておくべきもの

問題点は？

■ 市場は拡大したか？

- 「情報セキュリティ監査実施の要請が増えている」のは事実。客観的数値はJASAに調査を委託。それを待ちたい。
- しかし・・・
  - 「経営」の中に監査の実施が位置づけられていない。まだ、「情報システム部門」の問題。
  - セキュリティポリシーの策定段階にあるところは、監査は将来のこと。
  - 「外部監査」にはまだまだ抵抗あり
- 「経営」と「技術（実際の対策）」を両立する「社会基盤」として形成していく必要性

今後の方向性

■ ユーザサイド

- 企業経営における「情報セキュリティ監査」の位置付けの明確化
  - IR
  - 個人情報保護
  - コンプライアンス
  - 格付け　etc.
- 業務形態別の「管理基準」の必要性
- なお、「公的分野」は推奨ではなく、「義務化」の加速化

■ サプライサイド (監査主体)

- 「質の向上」が急務
- 「資格制度」「監査主体の審査」による「信頼」の獲得
- 将来的には「義務付け」「保証」に耐えうる基盤の形成
- JASAの活動を支援

ここ1年の動き
～経営と組織に関して～

- **リスク管理・内部統制に関する研究会報告書**
  - 「リスク新時代の内部統制」平成15年6月
  - リスクマネジメントと内部統制の重要性
  - モニタリングと健全な内部監査
  - クライシスマネジメント
- **企業の社会的責任（CSR）に関する懇談会**
  - 4月28日 スタート、夏頃報告書とりまとめ
  - CSRは一般的に、経済面に加え社会面、環境面の行動を包含し、内容的にもコンプライアンス（法令遵守）から環境保全、消費者保護、公正な労働基準、人権、安全衛生、地域社会貢献など幅広い要素から構成
  - ①企業の社会的責任（CSR）の基本的性格、効果を明らかにした上で、②我が国企業のCSRへの円滑な自主的取組を促すとともに、③これが的確に評価される事業環境の整備に必要な施策の在り方 等について検討

3．情報セキュリティ政策の最近の動き

いま何が問題か？

■「情報セキュリティ」の世界を俯瞰すると・・・

- 「セキュリティ」「安心・安全」は時代のキーワード
- 「セキュリティ対策が重要である」との総論に異論なし
- しかし・・・
  - 「サプライサイド」の気運は盛り上がるも投資は思うように進まない
  - 政府・自治体のセキュリティは大丈夫？
  - 重要インフラは？
- 一方で、「個人情報漏洩」は喉元に。

第1期から第2期に入った情報セキュリティ政策

METI 経済産業省

インターネット幕開け　　電子商取引離陸　　ニューエコノミー／IT革命

クリッパーチップ構想（米）　　暗号輸出規制の緩和

暗号政策ガイドライン（OECD）　　AES選定　　国際標準化

COCOM解散　ワッセナー成立　　米国サイバーセキュリティ戦略

CCアレンジメント（→ISO/IEC15408）

セキュリティ・マネジメント（ISO/IEC17799）

EU個人情報保護指令案　　EU電子署名指令案

電子政府イニシャチブ　　2003.4　「総合戦略」

ハッカー対策行動計画／サイバーテロ対策行動計画

大規模プラントセキュリティ対策

NIRT創設

セキュリティ技術開発支援

JPCERT/CCの創設支援　　暗号技術評価（CRYPTREC）

IPAセキュリティセンター　　セキュリティ評価認証開始

ウィルス等対策基準改訂　　電子署名・認証法

ISMS適合性評価制度

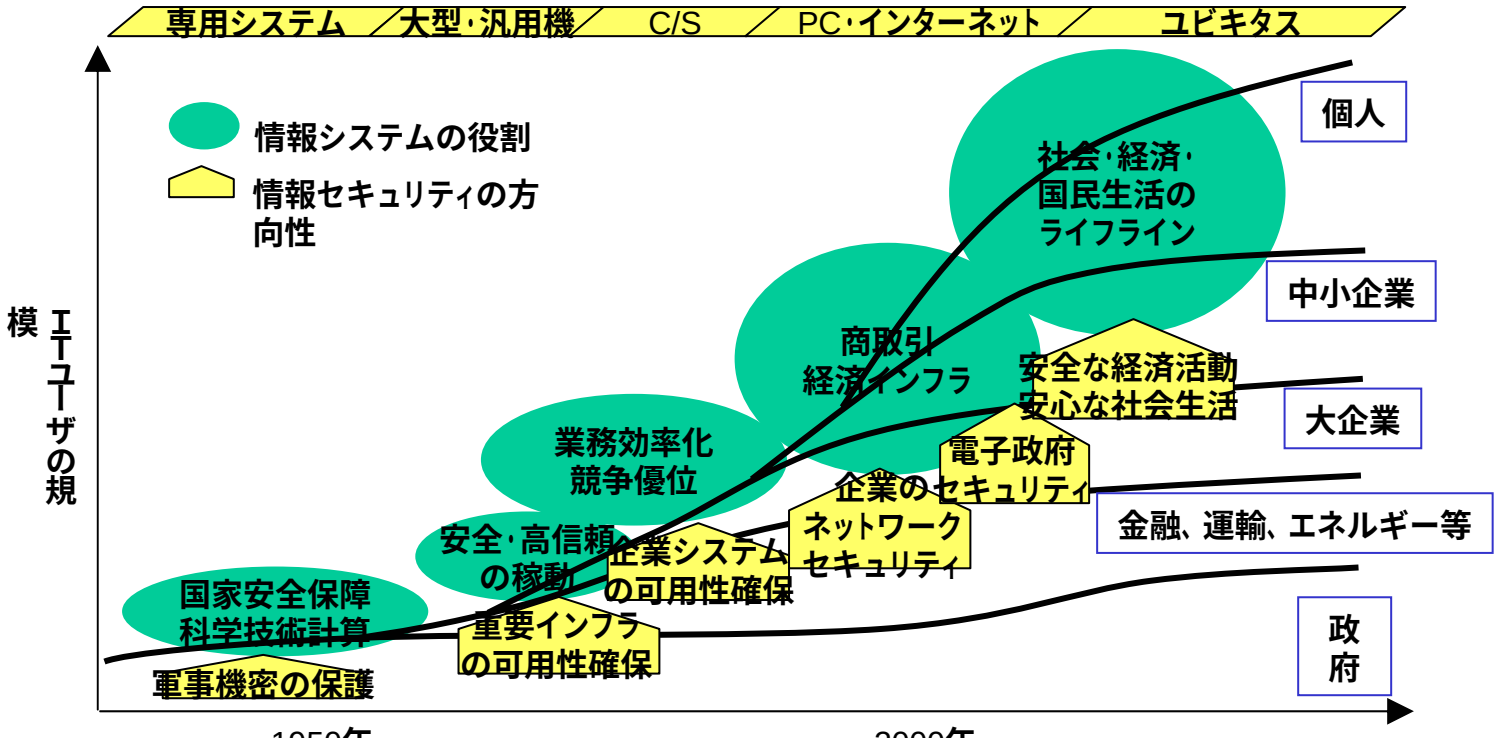
情報セキュリティ監査

「第2期」の基本認識①
～経済・社会の「神経系」となったIT

METI 経済産業省

■ 経済・社会の「神経系」となったITと新次元のリスク

- ITはここ近年急速に発展・普及し、「経済・社会の『神経系』」に。
- また、情報システムは複雑化し、これまでになかった新次元のリスクに直面。



「第2期」の基本認識②
～「予防偏重」から「事故前提」の新しい基盤への移行

– ①ITの「神経系」化と、②情報システム構造の複雑化、そして、③攻撃可能期間の短縮化により、情報セキュリティ対策は、今までの「予防偏重」型から「事故前提」型（「情報セキュリティに絶対はなく、事故は必ず起こるもの」）への移行が必要な時代に。

脆弱性番号	脆弱性・対策方法の公表		Exploitコード出現		ウイルス等の攻撃発生
MS02-039	2002/7/29	2ヵ月	2002/9/25	4ヵ月	2003/1/25 SQL Slammer
MS03-026	2003/7/17	10日	2003/7/27	16日	2003/8/12 Blaster
MS03-039	2003/9/11	4日	2003/9/15	5ヵ月	2004/2/11 Welchia.B
MS03-043	2003/10/16	3日	2003/10/19	？	？
MS03-049	2003/11/12	1日	2003/11/13	2ヵ月	2004/2/11 Welchia.B
MS04-007	2004/2/11	3日	2004/2/14	？	？
MS04-011	2004/4/14	11日	2004/4/25	6日	2004/5/1 Sasser

急速に短縮化

情報セキュリティ総合戦略（2003年10月10日発表）

～世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上～

- 3つの戦略と42の具体的施策項目の提示
- http://www.meti.go.jp/policy/netsecurity/strategy.htm

基本目標　***世界最高水準の「高信頼性社会」の構築***

戦略1　***しなやかな「事故前提社会システム」構築（高回復力・被害局限化の確保）***

→「情報セキュリティに絶対はない」との前提の下で、事故の回避（予防）・被害局限化・回復の最適化を図った対応の徹底化

戦略2　***「高信頼性」を強みとするための公的対応の強化***

→「高信頼性」を強みとするため、国家的視点から、技術基盤・制度基盤両面にわたる公的対応を強化

戦略3　***内閣機能強化による統一的推進***

(参考) 最近の米国の主な動き

- **全米サイバーセキュリティサミット(2003/12)とその成果**
  - 国土安全保障省（DHS）が米国情報技術協会（ITAA）、BSA、TechNet、米国商工会議所の4団体との共催で「全米サイバーセキュリティサミット」を開催。民間セクターと政府関係者が情報セキュリティ政策について議論
  - 「民間セクターが自ら直面している課題に立ち向かわない場合、法的にサイバーセキュリティ対策の強化を民間セクターに義務づけようとする動きが勢いづくことになる。」（DHS次官補）
  - サミットでは5つのTFを設置し、ホワイトペーパーを策定することを決定。
    - ①家庭でのPC利用者及び中小企業者に対する啓蒙活動
      → 中小企業向けガイド、一般向けセキュリティツールキット、教育機関での啓発、メディアによるキャンペーン　等
    - ②サイバーセキュリティ早期警戒システム構築　→　Early Warning Contact Networkの構築、ISACの統合　等
    - ③情報セキュリティを企業統治の一部に位置付けるためのTF　→　企業の情報セキュリティ・チェックツールの公表(75項目)
    - ④技術規格・コモンクライテリア
    - ⑤セキュリティ強化をソフトウェア開発のライフサイクルの観点から取り組むTF
  - サミット後、上記4団体を中心に「National Cyber Security Partnership（NCSP）」が結成、上記TFの検討を実施
- **全米規模のサイバーテロ演習“Livewire”の実施（2003/10）**
  - 民間セクターと政府、地方政府等の関係者300人が参加。
  - 各省庁・機関間のより優れた調整や民間セクターと行政機関との調整が必要との認識。
- **官民協力によるサイバー警報メーリングリスト（National Cyber Alert System）を開始（2004/01）**
  - 脆弱性や攻撃の警告、広報、対処法等を電子メールで通知するメーリングリストサービスを開始。
  - 専門家向けの報告と警告、一般ユーザ向けのヒントと警告、計4種類のサービスを提供。
- **情報セキュリティに関する団体設立**
  - 情報セキュリティ関連企業12社が発起人となり、非営利団体「Cyber Security Industry Alliance（CSIA）」を設立（2004/2）。元大統領補佐官のポールカーツ氏が事務局長に就任。
  - 企業の最高セキュリティ責任者（CSO)によるグループ「Global Council of CSOs」が発足。（2003/11）
- **連邦情報セキュリティ管理法（FISMA）に基づく政府機関の評価**

2．セキュリティ（安全・安心）政策の強化（Ｂ：Block and Back-up: Security）

1）「IT社会を守る」（公共分野・重要インフラの情報セキュリティ強化と人的基盤の充実）

（1）情報セキュリティ補佐官の設置等

官民における情報セキュリティ対策を一層推進するため、速やかに情報セキュリティ専門調査会を改組するとともに、2004年4月までに内閣官房に情報セキュリティ対策についての助言・支援を行う情報セキュリティ補佐官（仮称）を置き、民間専門家から委嘱する。（内閣官房）

（2）各府省庁の情報セキュリティ確保

各府省庁の情報セキュリティ水準を客観的に把握し、政府全体で統一のとれた安全対策を推進するため、内閣官房の人員増強を図るなど政府の情報セキュリティ体制を段階的かつ速やかに強化しつつ、以下の施策を実施するため基本方針及び具体策について2004年6月までに検討を行い結論を得る。（内閣官房及び関係府省庁）

① 攻撃の予兆や被害に関する情報収集・分析
② 各府省庁の情報セキュリティ対策の評価
③ 各府省庁の情報システムとその運用に関する安全基準の策定

IT戦略本部
（平成16年6月15日）での決定事項

METI 経済産業省

情報セキュリティ基本問題委員会について

IT戦略本部

- 政府のIT政策のうち情報セキュリティ分野の政策に関する基本的な問題について一元的かつ集中的に議論
- 政府の情報セキュリティ政策についての中長期的な計画を策定し、IT戦略本部に報告

情報セキュリティ専門調査会

情報セキュリティ
基本問題委員会

内閣官房
情報セキュリティ
対策推進室

情報
セキュリティ
補佐官

連携

各省庁

- 現在各省庁が実施中の施策について、政府全体としての横断的な視点からの整合性、効率性、実効性などを検証
- 政府が情報セキュリティの確保のため取り組むべき方向を明確化

○情報セキュリティの専門家を専門調査会の委員に新たに任命
○新たに任命した委員により基本問題委員会を設置

経済産業省の新規施策

■ 以下の柱にて新規施策実行中

- コンピュータセキュリティ問題に関する早期警戒体制の拡充・強化（脆弱性関連情報流通の枠組み構築）
- 重要インフラセキュリティ（先鞭としての電力分野）
- 企業経営とIT事故に関する検討

コンピュータ・セキュリティ問題に関する早期警戒体制の拡充・強化
～脆弱性関連情報流通の枠組み構築～

METI 経済産業省

➢経済産業省では、コンピュータウイルス・不正アクセスなどのコンピュータ・セキュリティ問題に関する早期警戒体制の構築として、①と②の取組を実施してきたところ。

➢この度、本体制を拡充・強化するために、③を実現。本年4月6日に公表し、7月から体制の運用を開始する予定。

①コンピュータウイルス・不正アクセス届出（IPA　1990年～，JPCERT/CC　1996年～）

②インターネット定点観測（JPCERT/CC　2003年11月～）

③脆弱性関連情報流通の枠組み構築（IPA，JPCERT/CC　2004年（予定）～）

1990年

各企業でコンピュータ導入が進むにつれ、コンピュータウイルスによる被害が発生・増加。

被害原因を事後的に確認し、被害を局限化

①コンピュータウイルス・不正アクセス届出制度

被害発生を周知し、その拡大を抑制

2000年

インターネットの急激な普及により、インターネット経由のウイルスや不正アクセスによるトラブルが急増

被害原因をリアルタイムに把握・分析し被害を局限化

②インターネット定点観測

トラフィックの状況をリアルタイムに把握し、ネットワークの異常発生を検出

- ソフトウエアの脆弱性を悪用したウイルスや不正アクセスが急増。
- ウェブサイトの脆弱性を悪用され個人情報等が漏洩するケースが増加

被害原因を事前に把握し被害の発生を抑制

③脆弱性関連情報流通の枠組み構築

1)脆弱性関連情報を機密を保持しつつ関係者間で流通させ、
2)対策を迅速にユーザに供給する仕組み

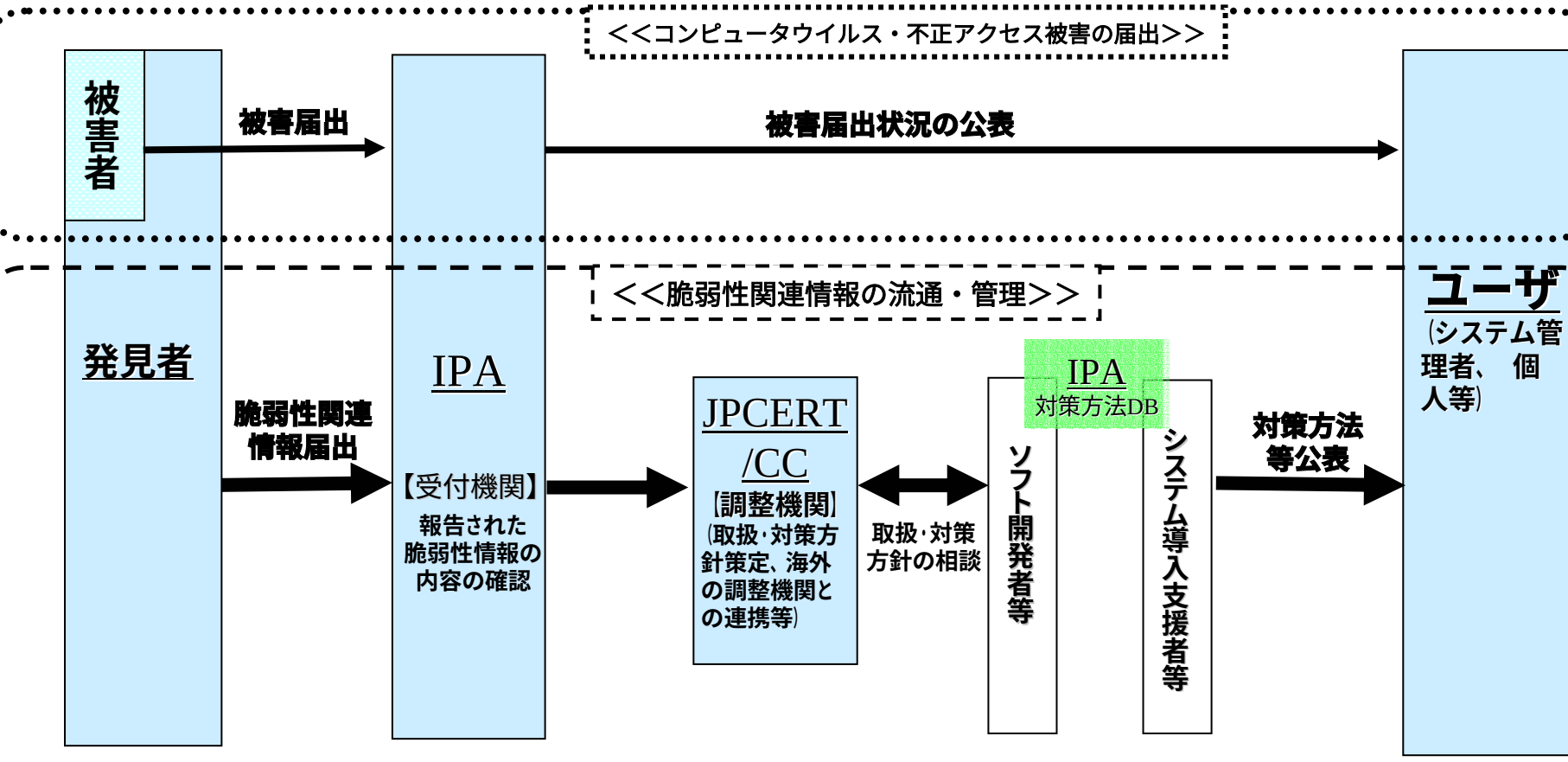
時間軸

コンピュータ早期警戒体制の整備
～スキーム～

別紙２

METI 経済産業省

コンピュータウイルス及び不正アクセス等の問題の早期発見・公表に加え、ソフトウエア等の脆弱性に関する情報の流通／管理を含めた体制へと早期警戒体制の拡充・強化を図る。



STEP1
リスク情報の収集

STEP2
対策方法の確定

STEP3
対策方法等の公表

狙っている効果と今後のスケジュール

■ 本枠組み構築によって実現を目指している効果

- ソフトウエア製品開発者及びWebサイト運営者による脆弱性対策の促進
- 脆弱性関連情報の放置･危険な公表を抑制
- 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

■ 今後のスケジュール

- 4月30日　公的ルール（告示）案をパブリックコメント（～5月28日）
- 6月下旬　告示制定
- 7月上旬　告示施行／IPA及びJPCERT/CCにおいて、実際の脆弱性関連情報の取り扱いを開始

■ 報告書掲載ＵＲＬ

- http://www.meti.go.jp/policy/netsecurity/vulnerability.htm

「企業経営におけるIT事故対応に関する研究会」の開催（案）

METI 経済産業省

1．背景と趣旨

- 情報システムは組織運営、事業管理、対外ネットワークの構築など事業を行うために必要不可欠なインフラとなり依存度が急激に増したが、それに伴い情報システム・情報資産に係るインシデント（IT事故）が企業の継続的な事業・サービス提供を脅かすリスクとなった。
- 以上のようなIT事故に係るリスクの増大が現実になっているものの、経営者層までその認識が広まっておらず、また必要性を認識していても、「**どの程度のセキュリティ投資を行えばよいか**」というベンチマークがなく、投資に逡巡する例も見られる。
- また、万が一IT事故が発生した場合の早急な復旧、事業継続性の確保が、国際的に見ても企業の競争力の重要な要素となる中、我が国においては、「事業継続性」のための対策が遅れているのが現状。
- こうした状況を踏まえ、**IT事故対応と企業経営の関係を全体的に整理し、情報セキュリティ確保への取り組みが企業価値向上に繋がるために必要な方策を提示**するために、経済産業省では「企業経営におけるIT 事故対応に関する研究会」（案）を設置し、検討を開始する予定。

2．検討項目（案）

- 情報セキュリティ対策のベンチマーク（指標）の策定
  - 業務形態別の「対策ベンチマーク」の策定と自己評価ツールの開発
  - 「対策ベンチマーク」と連動した「IT事故データベース」の構築のあり方
  - 「対策ベンチマーク」及び「IT事故データベース」を活用した保険のあり方
  - 情報セキュリティ監査との連動のあり方
  - 企業の「格付け」との関係
- 「事業継続計画」の策定手順の提示

3．今後の予定（案）

- 2004年7月　研究会設置、検討開始
- 2005年3月　報告書、アウトプットの策定

4．まとめ

今年度の展望

■ 政府レベルでは…「ナショナルセキュリティ」

- 「官」のセキュリティ対策の再度巻き直し
  - 「ベストプラクティス」への決意
- 官民連携した「社会インフラ」の整備（早期警戒システムetc.）
- 重要インフラ対策の見直し
- 内閣機能強化による推進

■ 民の市場は…「ユーザサイドセキュリティ」

- 「サプライサイド」の盛り上がりから「ユーザサイド」主導の動きへ
- 個人情報保護（漏洩対策）は大きな契機に
- METIは「企業経営におけるIT事故対応に関する研究会」等を開催し、「ユーザサイド」の視点に立った政策ツールを提供する予定
- 「情報セキュリティ監査」についてもここで加速

ご静聴ありがとうございました

METI 経済産業省

Contact

田辺　雄史（Tanabe Takefumi）

経済産業省
商務情報政策局 情報政策ユニット
情報セキュリティ政策室

TEL：**０３－３５０１－０３９７**
E-mail：tanabe-takefumi@meti.go.jp
URL：http://www.meti.go.jp