METI 経済産業省

情報セキュリティ対策は企業価値を高められるか？

～個人情報保護法に向けた準備と情報セキュリティ政策の最新動向～

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

本日の内容

METI 経済産業省

- **最近の動向**
- **政府内の最近の動き**
  - 情報セキュリティの体制
  - 情報セキュリティ基本問題委員会
  - e-文書イニシアティブ
- **個人情報保護法の動き**
- **経済産業省の政策の紹介**
  - 情報セキュリティ早期警戒パートナーシップの動き
  - 組織的セキュリティ対策事業
  - 技術的セキュリティ対策事業

2

情報セキュリティのスコープの変遷

METI 経済産業省

- 「サプライサイド」→「ユーザサイド」
- 「技術」→「マネジメント」
- 「事後対応（Response）」→「抑止（Prevent）」
- 「情報システム部門の問題」→「経営者層の問題」
- 「IT事故対策」→「個人情報保護（情報漏洩）対策」
- 「コーポレートガバナンス」→「情報セキュリティガバナンス」
- 「予防偏重社会」→「事故前提社会」
- 「システムを止めない対策」→「ビジネスを止めない対策」
- 「収益を生まない分野」→「信頼性を確保するための分野」

3

新たなる脅威

METI 経済産業省

- 携帯電話へのワーム感染（SymbOS.Cabir、2004.6.14）、ウイルス感染
- DVDレコーダーが（コメント）スパムの踏み台に？
- 情報家電のセキュリティ対策も必要な時代へ
- P2P環境の整備に伴って、既存の防御（ファイアウォール等）策にも限界が存在？

4

利便性とリスク（脆弱性）の関係

METI 経済産業省

	紙媒体、紙に書かれた情報	電子媒体、電子的な情報
複製	複製を繰り返すと劣化する	劣化せず複製可
修正	困難	容易
可視性	物理的に存在（確認が容易）	電子的に存在（確認にアプリケーション等が必要）
送受信	郵便等を利用（電子的送受信に比べて少し面倒）	電子メール、その他のプロトコルを使用（簡単に送信可能）
情報の蓄積	紙の物理的容量分のスペースが必要	小型の媒体に大量の情報を蓄積可

5

METI 経済産業省

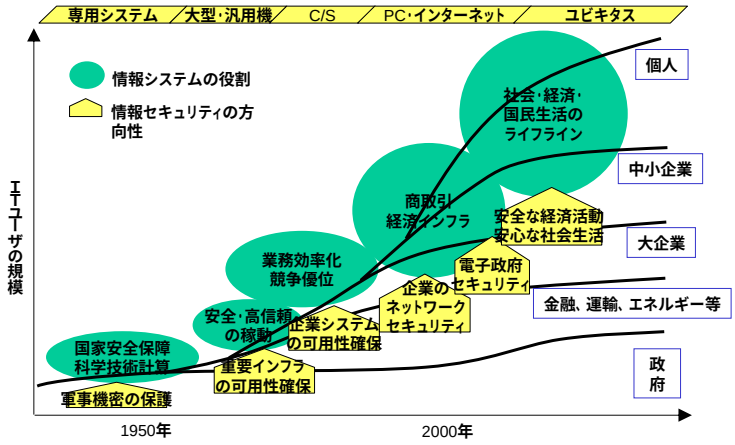
最近の動向

情報セキュリティを取り巻く時代の変化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」となった情報技術（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、ウイルスやサイバー攻撃、犯罪など、これまでになかった新次元のリスクに直面。



情報セキュリティを取り巻く時代の変化②
～「予防偏重」から「事故前提」への移行

METI 経済産業省

「予防偏重」型の対策から「事故前提」の対策への移行

- 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。
- そのためには、**官民連携した国家レベルの対策基盤**が必要。

国民生活や経済活動を脅かすサイバー攻撃やシステム障害

	事件・事故の事例
国	政府ホームページが改ざんされる。
地方自治体	自治体のシステムがウイルス感染し、一時庁内システムの運用を停止。
重要インフラ（電力）	米国で電力会社のシステムが進入を受け、電力供給停止などの攻撃が可能な状態に陥った。
（金融）	みずほ銀行のシステム統合に伴うシステム障害発生、サービスが停止。
国民生活	昨年8月ブラスターワームの流行により個人用PCの多くが感染、対応に苦慮。

短縮化する攻撃可能期間

脆弱性（セキュリティホール）名	脆弱性の公表・修正プログラム配布		攻撃コード出現		攻撃発生
MS02-039	2002/7/29	2ヵ月	2002/9/25	4ヵ月	2003/1/25 SQL スラマー
MS03-026	2003/7/17	10日間	2003/7/27	16日間	8/12 ブラスター
MS03-039 ※	2003/9/11	4日間	2003/9/15	5ヵ月	2004/2/11 Welchia.B
MS03-049 ※	2003/11/12	1日間	2003/11/13	2ヵ月	2004/2/11 Welchia.B
MS04-007 ※	2004/2/11	3日間	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

※ブラスターと同程度の被害を発生させる可能性のある脆弱性（セキュリティホール）

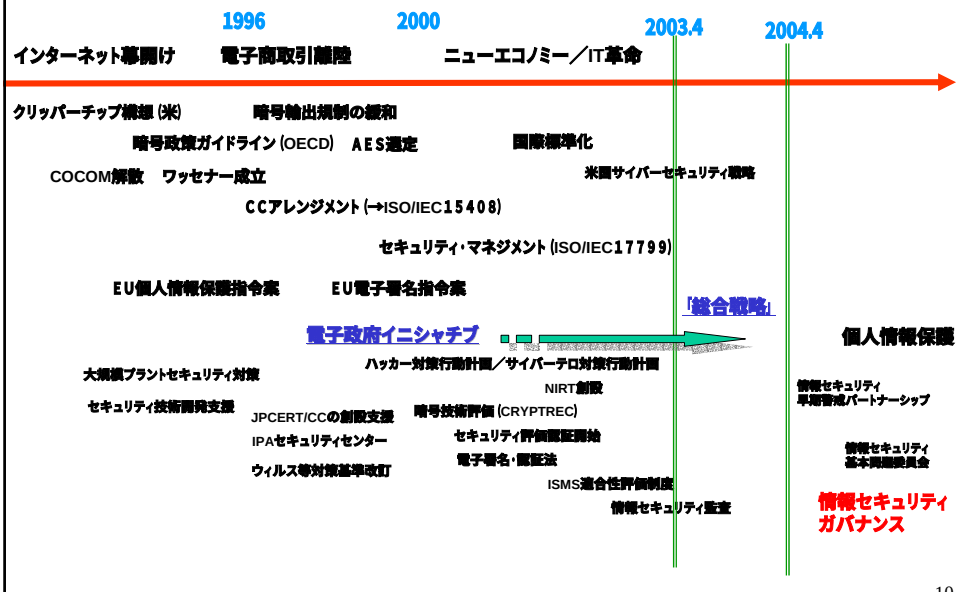
METI 経済産業省

政府内の最近の動き

政府における情報セキュリティ体制
情報セキュリティ基本問題委員会
e文書法関連

第1期から第2期に入った情報セキュリティ政策

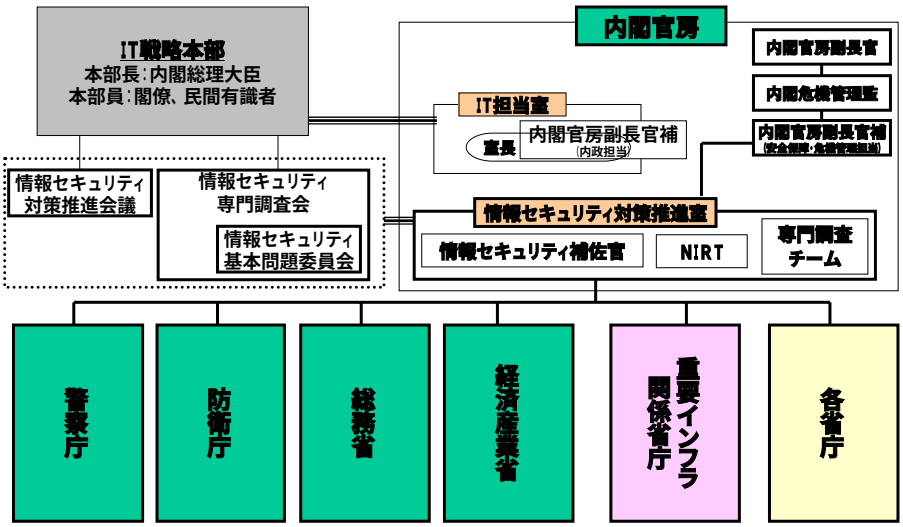
METI 経済産業省



10

政府の情報セキュリティ施策実施体制

METI 経済産業省



11

最近の動き

METI 経済産業省

- **7月22日　IT戦略本部下の専門調査会内に、基本問題委員会を設置**
- **7月26日　情報セキュリティ対策推進会議幹事会において、以下の基本方針を決定**
  - 攻撃の予兆や被害についての情報収集・分析に係る基本方針について
  - 各府省庁の情報システム及びその運用に関する安全基準の策定に係る基本方針
  - 各府省庁の情報セキュリティ対策の評価に係る基本方針
- **7月27日　第一回　基本問題委員会の開催**
  - 8月6日　第一回　基本問題委員会分科会の開催
  - 8月23日　第二回　基本問題委員会分科会の開催
  - 9月1日　第三回　基本問題委員会分科会の開催
- **9月6日　第二回　基本問題委員会の開催**
- **9月10日　IT戦略本部の開催**
  - 9月17日　第四回　基本問題委員会分科会の開催
  - 10月8日　第五回　基本問題委員会分科会の開催
  - 10月19日　第六回　基本問題委員会分科会の開催
- **10月26日　第三回　基本問題委員会の開催（予定）**

以下のスライドはIT戦略本部資料から引用

12

「情報セキュリティ基本問題委員会」の構成と検討内容

METI 経済産業省

構成

○IT社会の基盤となる情報セキュリティに関する基本的な課題について、優先順位を付けて検討。

○専門家の知見を集約して**「情報セキュリティ政策に関する国家としての戦略」を策定**し、**IT戦略本部に提言**。

検討内容

○当面の優先課題として以下を設定。

(課題1) 情報セキュリティ政策全般の実行体制の見直し

(課題2) 政府自身の情報セキュリティ対策の強化

(課題3) 重要インフラの情報セキュリティ対策の強化

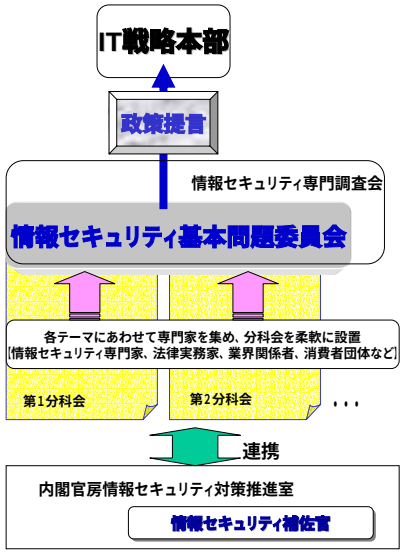
(課題4)個人情報などの情報管理・流通のあり方の検討

○本年10月末に第1次提言、来年3月末に第2次提言（予定）。

委員

〔委員長〕
金杉明信　日本電気（株）代表取締役社長
〔委員〕
伊藤泰彦　KDDI（株）取締役（執行役員専務）
後藤滋樹　早稲田大学教授
寺島実郎　（株）三井物産戦略研究所所長
中村直司　（株）NTTデータ代表取締役副社長
村井　純　慶應義塾大学教授

（※別途、情報セキュリティの専門家等を集めた分科会を設置し、知見を集約。）



13

第1次提言の射程（情報セキュリティ問題全体における位置付け）

METI 経済産業省

情報セキュリティのグランドデザインの確立
実効性のある対策と施策の実施

(課題1) 情報セキュリティ政策全般の実行体制の見直し

(課題2) 政府自身の情報セキュリティ対策の強化

政府組織

◆ 民間のカウンタパートとしての信頼足り得る存在
◆ 国際的な信頼醸成
◆ バランスある技術投資の実施
◆ 透明性の確保

第1次提言（'04/10末）

重要インフラ

◆ 依存可能な基盤としての機能提供
◆ 検証可能な機能設計と事業継続性確保
◆ 重要インフラ相互間の連携と協力

第2次提言（'05/03末）

企業

個人

◆「セキュリティ文化」の参加者としての積極的な取り組み
◆ 個人情報保護問題やプライバシー問題に対するコンセンサスの形成

第3次提言（'05/07末）

14

e-文書イニシアティブの背景

METI 経済産業省

○企業活動における書面交付等の主要手続は、既にインターネットで行うことが可能であるが、保存関係は包括的には措置されておらず。

（書面一括法（H12.11）、改正商法（H13.11）等により可能。行政手続における申請等も、本年2月施行の行政手続オンライン化法により可能。）

○行政機関での文書の電子保存は、行政手続オンライン化法により可能。一方で、**企業等への紙の保存義務規制は緩和されておらず、電子保存を容認するよう強く求められている。**

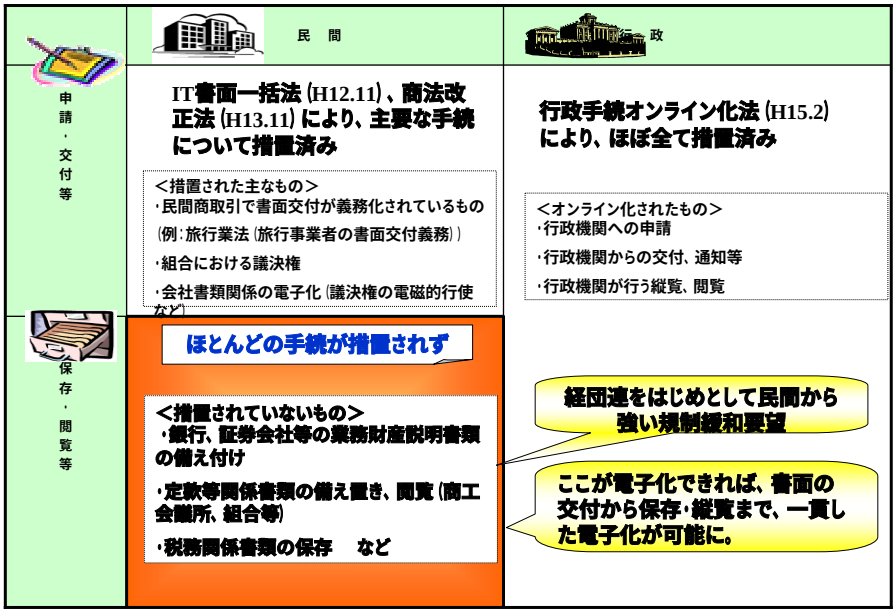
○電子保存の容認により、文書の保管・運搬コストが大幅に削減されるだけでなく、書面という物理的制約から解放され、情報技術を利用することで、ビジネスプロセス自体の一段の改革が可能に。企業経営の効率化、競争力向上に大きく寄与することが期待される。

（例：税務関係書類保管コスト（経団連試算）　年3000億円）

15

（参考）民間・行政の書面手続における電子化を可能とする措置の状況

METI 経済産業省



16

e-文書法の立案方針（ポイント）

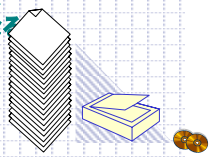
METI 経済産業省

題名：「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」

（通称 e-文書法）1

「e-文書法」＝「通則法」と「整備法」により構成。
- ・通則法：電子保存容認に関する共通事項を定める。
- ・整備法：通則法のみでは手当てが完全でない場合等の規定整備を行う。

- 通則法は、行政手続オンライン化法の法スキームと同様になる予定
  （主務省令で定めるところにより電磁的記録による保存等が可能になる）
- 通則法により措置する法律数は、約２５０本（当省関係：約６０本）
  （通則法形式の採用により、個別に法改正せずに電子保存を容認。）



- 税務関係書類も、原則的に全ての書類の電子保存を容認。
  （適正公平な課税の確保のため、一部書類については対象にしない。）
- 一部の文書について電子保存対象外となる法律（約５０本）

（例）・緊急時に即座に確認する必要があるもの：船舶に備える安全手引書など

・現物性が極めて高いもの：免許証、許可証など

17

e-文書法のイメージ

METI 経済産業省

通則法＋整備法により、原則、民間文書の電子保存を容認

≪通則法≫
民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律案（仮称）

- 第1条関係（目的規定）　民間事業者等が電磁的記録による保存等をできるようにするための共通事項を定める。
- 第2条関係（用語の定義）
- 第3条~第6条関係
  - ①保存等の電磁化可能規定　主務省令で定めるところにより、電磁的記録による保存・縦覧等を行うことができる。
  - ②書面みなし規定　①により行われた保存等については、書面により行われたものとみなす。
- 第7条関係（適用除外規定）　電子化になじまないものを列記し、法第3条から第6条の規定を適用を行わない
- その他（第8条・第9条関係）　地方公共団体における推進、主務省令の定義

≪整備法≫
民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律案（仮称）

- 通則法との調整等　通則法の規定では十分ではないものについて、個別法の一部改正により所要の規定を整備。

18

主務省令との関係

METI 経済産業省

通則法案第3条関係の電磁的記録による保存可能化規定のイメージ

（電磁的記録による保存）
第三条　民間事業者等は、保存のうち当該保存に関する他の法令の規定により書面により行わなければならないものとされているものについては、当該法令の規定にかかわらず、**主務省令で定めるところにより**、書面の保存に代えて当該書面に係る電磁的記録の保存を行うことができる。

電磁的記録による保存の具体的要件は、主務省令で定められることになる。

書面の内容、性格により、真実性・可視性等を確保するための要件の要請の程度が異なりうるため、**具体的電磁的記録による保存の方法等については、法令の所管府省の主務省令で定める**。

電磁的記録による保存の要件の考え方

METI 経済産業省

何故、保存に際して要件を定めるのか

書面と電子データの性質の相違

書面
①直接、目で見ることができる
②原本とコピーの区別が可能（特に、押印などがあれば）
③改ざんすれば、痕跡が残りやすい
④長期間保存しても問題が少ない

電子データ
①直接、目で見ることができない
②原本と全く同一のコピーを作成できる
③痕跡を残さずに改ざん可能
④長期間保存した実績に乏しい？

よって、書面の内容、性格により、電子データで保存するに際して適切な手当てを決めておかなければならないものが存在。
また、適切に手当てすることにより、電子データの特性を生かして書面以上の利便性を得ることも可能。

20

METI 経済産業省

個人情報保護法の動き

個人情報保護ガイドライン

METI 経済産業省

- **パブリックコメントの回答を発表（平成16年10月13日）**
- **コメント件数は約520件**
- **主な意見**
  - **記述の趣旨をより明確化することを望む意見（約2割）**
  - （例）団体に関する情報は個人情報に含まれない旨の記述があるが、団体に関する情報であっても、代表者の氏名等の情報は、個人情報に該当するので、注釈が必要。
  - **個別事案の解釈を求める意見（約4割）**
  - （例）第三者から個人情報を取得してダイレクトメールを送付する場合は、当該ダイレクトメールの同封物又は封筒に利用目的を記載するという方法で、速やかな利用目的の通知・公表の義務（法第18条第1項）を果たしていると考えて良いか。
  - **法の解釈指針から逸脱する内容に関する意見（約1割）**
  - （例）法の目的が「個人情報の適正な取り扱いの確保」にあることから、法の適用を受ける事業者の範囲を、政令で定める「個人情報取扱事業者」の要件（データベースを構成する個人情報によって特定される個人の数が5000を超える場合）に限定することなく、全ての事業者を法の適用対象とすべき。
  - **その他（約3割）**

http://www.meti.go.jp/feedback/data/i41013bj.html

22

ガイドラインの特徴・性格

METI 経済産業省

1．事業者の取組を支援するための具体的指針

基本方針及び個人情報保護法第8条に基づき、経済産業省所管の事業者等が個人情報の適正な取扱いを確保するために行う取組を支援するための具体的指針として策定。

2．具体的な事例を掲載

個人情報保護法に関する対応を行うに際して具体的なイメージが持てるよう、参考事例を掲載。事例については、法のルールに適合している例と違反している例の双方について記述し、事業者が具体的にどのような対応を行えば良いのか分かるような工夫を行った。

3．従業員の個人情報の取扱いについて

経済産業省所管の事業者等が、個人情報保護法に関する対応について全て理解できるようにするため、従業員の個人情報に関する部分も記述。従業員の個人情報の取扱いの部分については、厚生労働大臣と経済産業大臣の共同で作成を行った。

4．行政の透明性の確保

「勧告」「命令」及び「緊急命令」については、個人情報取扱事業者が、本ガイドラインで、「しなければならない」と明記したものについて、必要な措置を講じたか否かを基に判断して行うこととし、行政の透明性の確保を図った。

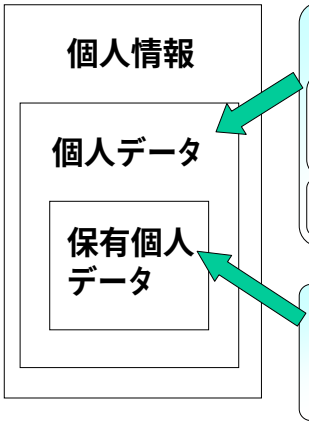
23

個人情報・個人データ・保有個人データ （6頁～）

METI 経済産業省

法第2条第4項　この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。

法第2条第5項　この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は1年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。



ガイドライン

◆「個人データ」とは、個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報をいう。

【個人データに該当する事例】
・個人情報データベース等から他の媒体に格納したバックアップ用の個人情報
・コンピュータ処理による個人情報データベース等から出力された帳票等に印字された個人情報

【個人データに該当しない事例】
・個人情報データベース等を構成する前の入力帳票に記載されている個人情報

ガイドライン

◆保有個人データ」とは、個人情報取扱事業者が、本人又はその代理人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する「個人データ」をいう。

◆個人情報取扱事業者が個人データを受託処理している場合で、その個人データについて、何ら取決めがなく、自らの判断では本人に開示等をすることができないときは、本人に開示等の権限を有しているのは委託者であって、受託者ではない。

24

個人情報取扱事業者の義務

METI 経済産業省

■法第15条から法第36条に個人情報取扱事業者の義務が定められている。事業者が具体的に対応を行う際に、事業者が分かりやすいように、本ガイドラインで、具体的な事例とともに示す。

1．利用目的による制限等
- ○ 利用目的をできる限り特定しなければならない。（第15条）
- ○ 利用目的の達成に必要な範囲を超えて取り扱ってはならない。（第16条）

2．適正な取得、正確性の確保、安全管理措置等
- ○ 偽りその他不正の手段により取得してはならない。（第17条）
- ○ 取得したときは利用目的を通知又は公表しなければならない。（第18条）
- ○ 正確かつ最新の内容に保つよう努めなければならない。（第19条）
- ○ 安全管理のために必要な措置を講じなければならない。（第20条）
  - ※漏えい時の被害・事業の性質・リスクに応じた、必要かつ適切な措置であること
- ○ 従業者・委託先に対し必要な監督を行わなければならない。（第21、22条）

3．第三者提供の制限
- ○ 本人の同意を得ずに第三者に提供してはならない。（第23条）
  - ※例外：オプトアウト（本人の求めに応じて提供を停止できることとしている場合）

4．本人の関与
- ○ 利用目的等を本人の知り得る状態に置かなければならない。（第24条）
- ○ 本人の求めに応じて保有個人データを開示・訂正・利用停止等を行わなければならない。（第25条～第27条）

5．苦情の処理
- ○苦情の適切かつ迅速な処理に努めなければならない。（第31条）

個人情報全般が対象

個人情報のうち「個人データ」（データベース化された情報）が対象

保有個人データが対象

＊ ***各義務規定には適宜除外事由あり***

25

安全管理措置（法第20条） （23頁～）

METI 経済産業省

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、及び技術的な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。）

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、その実施状況を確認すること。

具体的には、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。

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・訓練などの措置。

物理的安全管理措置

入退館（室）の管理、個人データの盗難の防止対策、機器・装置等の物理的な保護などの措置。

技術的安全管理措置

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。

具体的には、アクセスにおける識別と認証、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。

26

2－4　従業者の監督（法第21条）　（33頁～）

METI 経済産業省

法第21条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

ガイドライン

◆個人情報取扱事業者は、法第20条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない。

◆「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業主の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。

◆安全管理措置の一環として従業者をビデオ及びオンラインによるモニタリングを実施する場合についての留意点についても記述。

［従業者に対して必要かつ適切な監督を行っていない場合］

・従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、あらかじめ定めた間隔で定期的に確認せず、結果、個人データが漏えいした場合

・内部規程等に違反して個人データが入ったノート型パソコンを繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合

［従業者のモニタリングを実施する上での留意点］

◆個人データの取り扱いに関する従業者及び委託先の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリング（以下「モニタリング」という）を実施する場合は、次の点に留意する。等

・モニタリングの目的、即ち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。

・モニタリングの実施に関する責任者とその権限を定めること。

・モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること。

・モニタリングの実施状況については、適正に行われているか監査、又は確認を行うこと。

27

委託先の監督（法第22条）　（34頁～）

METI 経済産業省

法第22条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

ガイドライン

◆個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、法第20条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければならない。

◆「必要かつ適切な監督」には、委託契約において、当該個人データの取扱に関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれる。なお、優先的地位にある者が委託者の場合、受託者に不当な負担を課すことがあってはならない。

◆委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意する。

［受託者に必要かつ適切な監督を行っていない場合］

・個人データの安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えいした場合。

・個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合。

・再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合。

［個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項］

○委託者及び受託者の責任の明確化

○個人データの安全管理に関する事項

・個人データの漏えい防止、盗用禁止に関する事項

・委託契約範囲外の加工、利用の禁止

・委託契約範囲外の複写、複製の禁止

・委託契約期間

・委託契約終了後の個人データの返還・消去・廃棄に関する事項

○再委託に関する事項

・再委託を行うに当たっての委託者への文書による報告

○個人データの取扱状況に関する委託者への報告の内容及び頻度

○契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）

○契約内容が遵守されなかった場合の措置

○セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

28

第三者への提供（法第２３条第１項・第２項）（３６頁～）

METI 経済産業省

第２３条第１項　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。　一～四（略）

第２項　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。　一～四（略）

ガイドライン

◆個人情報取扱事業者は、あらかじめ、本人の同意を得ないで、個人データを第三者に提供してはならない。同意の取得に当たっては、事業の性質及び個人データの取扱い状況に応じ、本人が同意に係る判断を下すために必要と考えられる合理的かつ適切な範囲の内容を明確に示すこと。

［第三者提供とされる事例］
・親子兄弟会社、グループ会社の間で個人データを交換する場合
・フランチャイズ組織の本部と加盟店の間で個人データを交換する場合
・同業者間で、特定の個人データを交換する場合
・外国の会社に国内に居住している個人の個人データを提供する場合

［第三者提供とされない事例］
・同一事業者内で他部門へ個人データを提供すること。

◆個人情報取扱事業者は、第三者提供におけるオプトアウトを行っている場合には、本人の同意なく、個人データを第三者に提供することができる。

◆「第三者提供におけるオプトアウト」とは、提供にあたり当たりあらかじめ、以下のⅰ．～ⅳ．の情報を、本人に通知し、又は本人が容易に知り得る状態に置いておくとともに、本人の求めに応じて第三者への提供を停止することをいう。

ⅰ．第三者への提供を利用目的とすること。
ⅱ．第三者に提供される個人データの項目
ⅲ．第三者への提供の手段又は方法
ⅳ．本人の求めに応じて第三者への提供を停止すること。

［オプトアウトの事例］
・住宅地図業者（表札や郵便受けを調べて住宅地図を作成し、販売（不特定多数への第三者提供））
・データベース事業者（ダイレクトメール用の名簿等を作成し、販売）

29

２－７　第三者への提供の例外（法第２３条第４項）（３９頁～）

METI 経済産業省

法第２３条第４項　次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。

第１号　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合。

第３号　個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

ガイドライン

委託

◆個人データの取扱いに関する業務の全部又は一部を委託する場合は、第三者に該当しない。個人情報取扱事業者には、委託先に対する監督責任が課される（法第２２条関連）。

［業務の委託の事例］
・データの打ち込み等、情報処理を委託するために個人データを渡す場合
・百貨店が注文を受けた商品の配送のために、宅配業者に個人データを渡す場合

共同利用

◆個人データを特定の者との間で共同して利用する場合、以下のア）～エ）の情報をあらかじめ本人に通知し、又は本人が容易に知り得る状態に置いておくとともに、共同して利用することを明らかにしている場合は、第三者に該当しない。

ア）共同して利用される個人データの項目
イ）共同利用者の範囲（本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要ない場合もある。）
ウ）利用する者の利用目的（共同して利用する個人データのすべての利用目的）
エ）開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称

［共同利用を行うことがある事例］
・グループ企業で総合的なサービスを提供するために利用目的の範囲内で情報を共同利用する場合

30

保有個人データの公表・開示（法第２４条～）　（４２頁～）

METI 経済産業省

法第２４条第１項　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。　一～四（略）

法第２５条第１項　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。）を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。（以下略）

法第２６条第１項　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正、追加又は削除（以下この条において「訂正等」という。）を求められた場合には、（中略）利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。

法第２７条第１項　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第１６条の規定に違反して取り扱われているという理由又は第１７条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。

保有個人データに関する事項の公表
↓
保有個人データの本人への開示
↓
保有個人データの訂正・利用停止等

ガイドライン

◆個人情報取扱事業者は、**保有個人データ**について、一定の情報を本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

◆個人情報取扱事業者は、**本人から、自己が識別される保有個人データの開示（存在しないときにはその旨を知らせることを含む。）を求められたとき**は、本人に対し、書面の交付による方法（開示の求めを行った者が同意した方法）により、遅滞なく、当該保有個人データを開示しなければならない。

◆個人情報取扱事業者は、本人から、**保有個人データに誤りがあり、事実でないという理由によって訂正等を求められた場合**には、原則として、訂正等を行い、訂正等を行った場合には、その内容を本人に対し、遅滞なく通知しなければならない。

◆個人情報取扱事業者は、本人から、**手続違反の理由により保有個人データの利用停止等が求められた場合**には、原則として、当該措置を行わなければならない。なお、利用の停止等を行った場合には、遅滞なく、その旨を本人に通知しなければならない。

31

METI 経済産業省

経済産業省の政策の紹介

情報セキュリティ早期警戒パートナーシップ
組織的情報セキュリティ対策
技術的情報セキュリティ対策

政策の柱

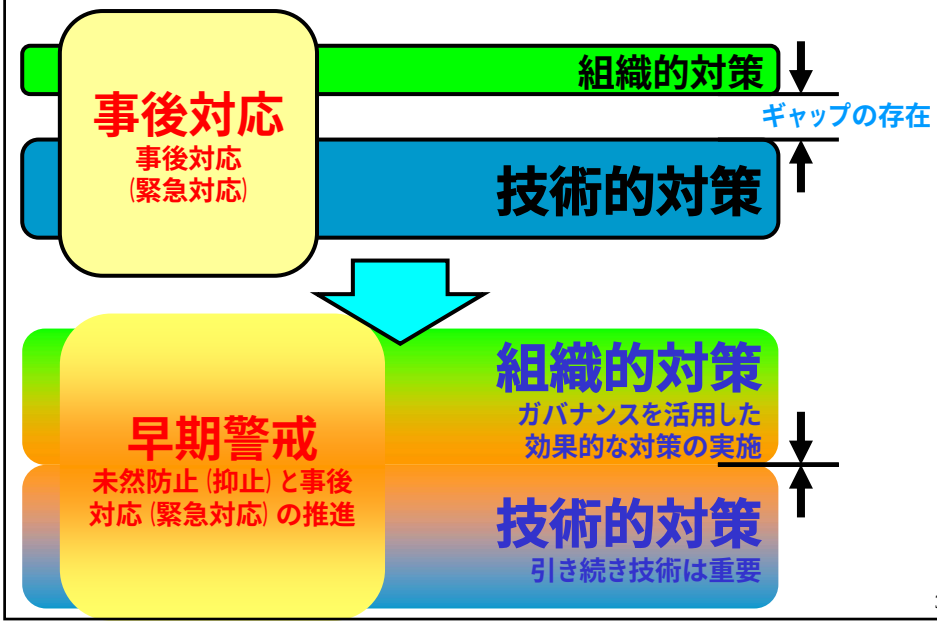
METI 経済産業省

- **情報セキュリティ早期警戒パートナーシップ**
  - インシデントの抑止と緊急対応
- **組織的情報セキュリティ対策**
  - 技術からマネジメント。情報セキュリティガバナンスの時代へ。
- **技術的情報セキュリティ対策**
  - 情報セキュリティはやはり「技術」が基本。
- **重要インフラにおける情報セキュリティ対策**
  - 電力分野におけるサイバーテロ演習

33

これからの対策のあり方

METI 経済産業省



34

METI 経済産業省

情報セキュリティ早期警戒パートナーシップ

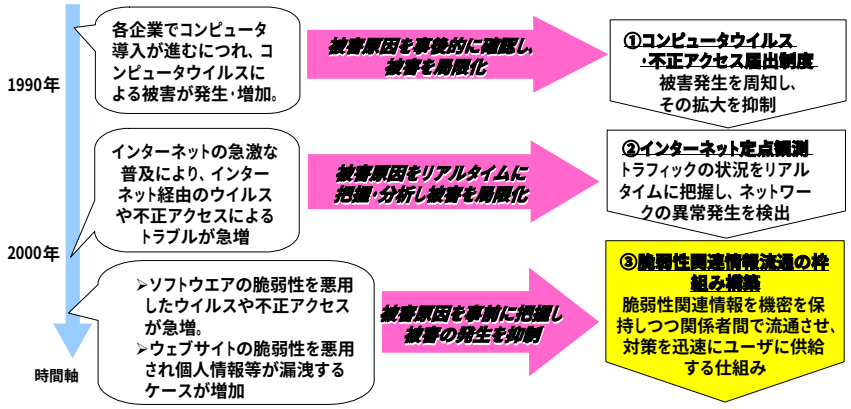
コンピュータウイルス、不正アクセス届出制度
インターネット定点観測
脆弱性情報流通体制の整備

コンピュータセキュリティ早期警戒体制の整備 ～経緯～

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し、早期にトラブルを発見・公表することで、その被害を局限化するための仕組み作りに取り組んできた。

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7月試験運用開始）
※脆弱性：コンピュータウイルス等による被害の原因となり得る、ソフトウエア製品に内在する安全性上の問題箇所



36

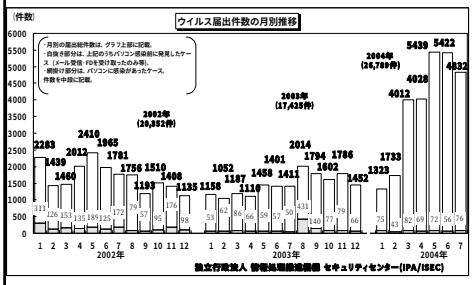
①コンピュータウイルス･不正アクセス届出

METI 経済産業省

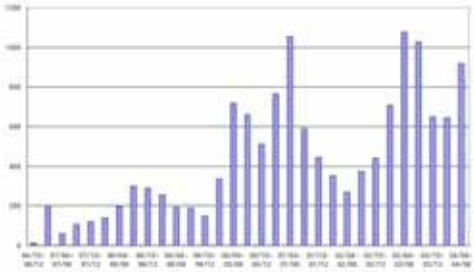
- IPA*、JPCERT/CCにおいてコンピュータウイルスや不正アクセスの相談受付を実施
- IPAは、平成2年度よりコンピュータウイルス、不正アクセスの届出機関として活動
  - ◆感染被害の拡大と再発防止のため、統計データを公開
- JPCERT/CCでは、平成8年10月より不正アクセス等の情報の収集･相談窓口を設置
  - ◆「情報の受付」「現象、状況、手口等の把握」「関連する技術情報の提供」を実施

*) 独立行政法人情報処理推進機構

IPAにおけるコンピュータウイルスの届出件数の推移



JPCERT/CCにおける不正アクセス等の届出件数の推移



96年　04年

37

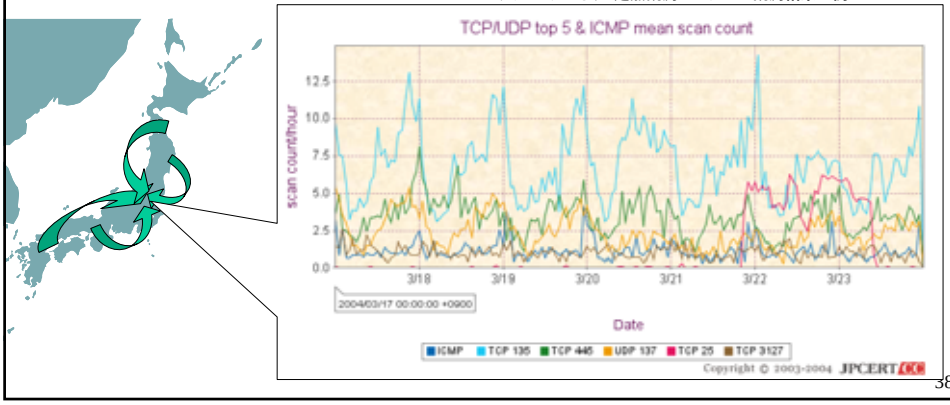
②インターネット定点観測

METI 経済産業省

- インターネット上に設置した複数のセンサーから得られる情報を解析し、ネットワーク･システム管理者向けにHP上で公開
- 観測データや脆弱性情報等を総合的に評価し、予報として提供することをめざす
- JPCERT/CC*において構築、平成15年12月より情報公開開始
- 平成16年3月には観測データを国別に解析し、海外の関連機関に提供する事業を開始

*) JPCERTコーディネーションセンター。不正アクセス等の緊急対応に関する相談窓口や脆弱性情報の公表等に関する調整を行う。

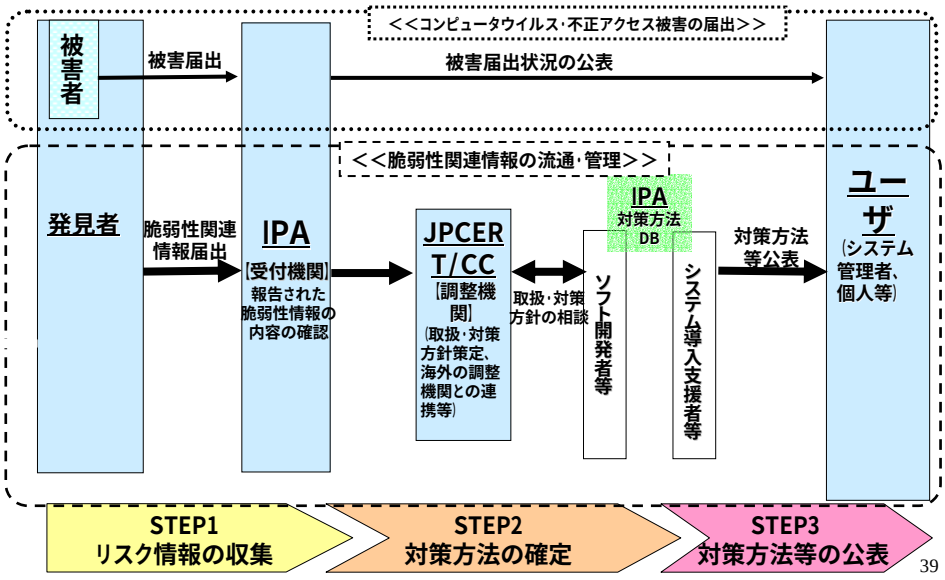
JPCERT/CCにおけるインターネット定点観測システムの観測結果の例



38

③コンピュータセキュリティ早期警戒体制の整備 ～スキーム～

METI 経済産業省



39

脆弱性情報取扱いについて

METI 経済産業省

http://jvn.jp/

40

METI 経済産業省

組織的情報セキュリティ対策

情報セキュリティ監査の概要
情報セキュリティガバナンス

変えなければならない意識

METI 経済産業省

ありがちな思い込み

- ウイルス対策ソフトを入れたから大丈夫…
- ファイアーウォールを入れたからハッカーからはやられない…
- セキュリティポリシーを作成したからレベルは上がった…

しかし…

- ✓ハッカーの技術は日々進歩
- ✓ウイルスも毎日のように新種が発生
- ✓内部の犯罪が8割を占めるという現状

- ✓情報セキュリティ対策に終わりはない
- ✓性悪説に立った「統制」の手法の導入が必要

- ✓最善の解としての「情報セキュリティマネジメント」の導入

42

情報セキュリティガバナンスの概念

METI 経済産業省

■ Information Security Governance

– *"To develop and promote a coherent governance framework to drive implementation of effective information security programs"* (Corporate Governance Task Force Report, NCSP, April 2004)

■ (参考) Culture of security

– *"a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks"* (2002 OECD Security Guidelines, page 8).

43

米国での動き

METI 経済産業省

■ **Sarbanes-Oxley 法 (2002年7月成立)**

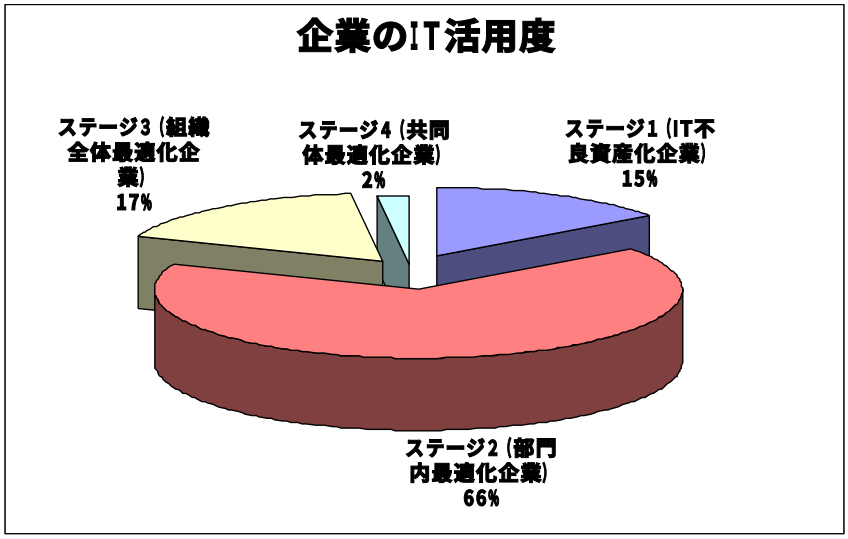
- CEO および CFO が内部監査の結果について責任を負うことを規定し、コーポレートガバナンスの徹底を明確化した法律。
- 情報セキュリティ対策の徹底について直接言及はしていないが、法律に準拠するためには情報セキュリティ対策が必須となる。
- IT との関連性が高いのは Section 404 であり、CEO・CFO・監査官に対して、会計報告書の作成プロセスが正確であることおよび一般的基準を満たすことを保証しなければならないと規定している。これによって企業は、会計報告書の作成に関わる全ての情報システムについて、法律が規定する基準を満たす事を保証しなければならなくなるため、結果的に情報セキュリティ対策を強化する必要に迫られることになる。

ITの企業経営への浸透により、企業の財務体質を適正に示すための情報セキュリティ対策も重要な時代へ。

44

企業におけるIT活用度

METI 経済産業省



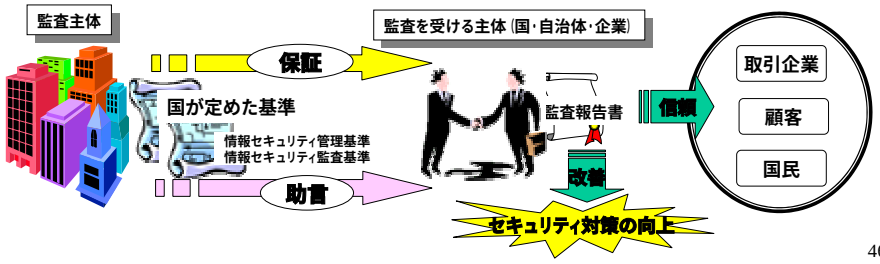
出典：経済産業省「我が国企業のIT化に対応する企業経営分析」

45

「情報セキュリティ監査制度」とは

METI 経済産業省

- 「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。「日本セキュリティ監査協会」（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



46

情報セキュリティ対策はコストか？

METI 経済産業省

- 情報セキュリティ対策なんてできればやらない方が良い？
- 情報セキュリティ対策が重要なのはわかるけど、頑張れば何とかなるのでは？→根性を強いられる情報システム部門
- トータルなセキュリティ対策で管理コストを削減できないか？
- ROSI (Return On Security Investment) の検討
- 対策を取らなかったときの被害と対策を取ったときの被害の関係がわかれば…
- でも、人並みに出来ているかどうかもわからない…

47

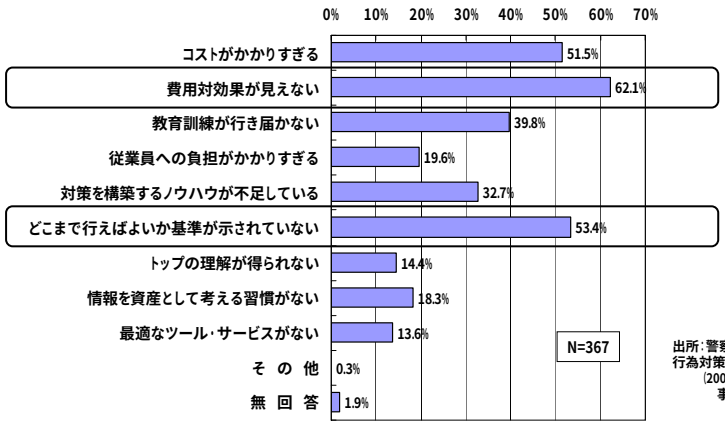
情報セキュリティ対策の現状

METI 経済産業省

情報セキュリティ投資の阻害要因は投資効果の不明確さと、投資判断のための指標の不在

➢ 我が国企業が情報セキュリティ投資を行う上で障害と感じる要素は、
①費用対効果が見えない（62．1%）
②どこまで行えばよいか基準が示されていない（53．4%）

大手・中堅企業における情報セキュリティ投資の障害（重要インフラ業種を除く）



出所：警察庁「不正アクセス行為対策等の実態調査」（2003年12月）より事務局作成

48

あるべき姿と問題点

METI 経済産業省

あるべき姿

- 高度にネットワーク化されたIT社会では、企業一社のIT事故によるトラブルが社会・経済全体にも影響する可能性。従って、企業の情報セキュリティ確保は、企業単体の問題に留まらず、IT社会を構成する一員としての企業の責務といえるのではないか。（個人情報保護法における「安全管理措置」の義務化といった法的要請に対するコンプライアンスは必須。）
- 国は、「高信頼性社会」*の実現をめざし、企業のコンプライアンスや社会的責任を踏まえた情報セキュリティ対策の実施を促進する社会環境を整備すべきではないか。

*)「高信頼性社会」は、経済産業省「情報セキュリティ総合戦略」（2003年10月）の基本目標において規定

問題点

(1) IT事故発生のリスクが明確でなく、適正な情報セキュリティ投資の判断が困難

- どの程度のコストをかけて、どのような対応を行うべきなのかといった、情報セキュリティの**投資判断のための指標**が求められているのではないか。

(2) 既存の情報セキュリティへの「対策」「取組」が企業経営に効果的に適合していない可能性

- 安定したネットワーク環境や、個人情報や機密情報の安全な取扱い等を求める社会の要請に応えるための情報セキュリティ確保に係る取組が、**企業価値向上**に直結していないのではないか。

(3) 事業継続性確保の必要性が十分に認識されていない

- 事業におけるIT依存度が高まりつつある現在、事業継続の観点から**IT事故発生時の対応手続**を定めておくことが必要不可欠ではないか。

49

企業における情報セキュリティガバナンスに関する研究会

METI 経済産業省

- 本研究会では、**企業*が、IT事故について、自身の被害の局限化という観点に留まらず、コンプライアンスの確保やIT社会の一員としての社会的責任という観点から、情報セキュリティを適正なレベルで確保する構造（情報セキュリティガバナンス）**を企業・社会に実装することをめざし、そのために有効なツールや、それらを企業・社会に普及させていく方策について検討する。

※検討対象は主に情報システムの「ユーザ企業」。ただし、重要インフラ業種は特別なリスクを有し、別途高いレベルのリスク管理策を検討する必要があるため対象から除く。

企業が情報セキュリティを適正なレベルで確保することを促進するツール

情報セキュリティ対策ベンチマーク

- ISO17799等のコントロール／サブコントロールに該当する具体的対策を整理し、セルフチェック等に有用なベンチマークの指標を開発する。
- さらに、IT事故データ収集のあり方や被害想定額算出手法について調査し、ベンチマークデータと連動したリスク評価の可能性を模索する。

情報セキュリティ報告書モデル

- 環境報告書、知的財産報告書等と同様、企業のコンプライアンスや社会的責任を説明するIRの一環として、自らの情報セキュリティポリシーやそれを実現する対策の実施状況について対外的に公表する「情報セキュリティ報告書」を提唱し、そのモデル案を策定する。

事業継続計画策定ガイドライン

- 企業がIT事故発生時にも事業運営を継続的に維持するための事業継続計画（BCP）について、その策定手順や検討項目、事例等を紹介する「事業継続計画策定ガイドライン」を策定する。

企業・社会への普及方策

・ISMS、情報セキュリティ監査との連携
・情報セキュリティ格付け
・損害保険との連携　　等

年度内までにとりまとめを予定

企業・社会における情報セキュリティガバナンスの実装

50

METI 経済産業省

技術的情報セキュリティ対策

暗号技術
ITセキュリティ評価・認証
電子認証基盤の整備

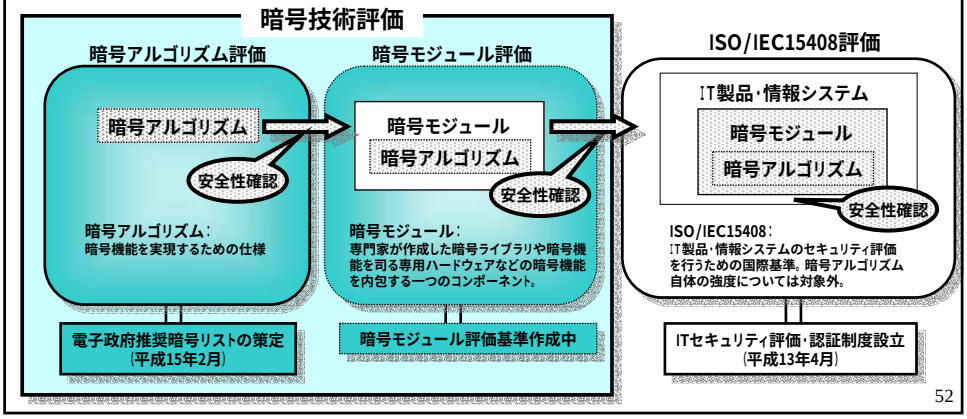
情報セキュリティ技術の評価

METI 経済産業省

➢ **情報セキュリティ対策を向上させるためには、①IT製品・情報システム、②IT製品・情報システムに組み込まれる暗号モジュール（暗号製品）、③暗号モジュールに実装される暗号アルゴリズムのそれぞれについて、第三者が安全性を評価することが必要。**

- ✓IT製品・情報システムについてはISO/IEC15408に基づいた第三者評価・認証制度が存在。
- ✓**暗号アルゴリズムについてはCRYPTRECにて第三者評価を実施し、電子政府推奨暗号リストを作成。**
- ✓**暗号モジュールについては、現在、安全性評価基準・試験基準を作成中。**

・CRYPTREC（Cryptography Research and Evaluation Committees）：総務省・経済産業省が実施している暗号技術評価プロジェクト

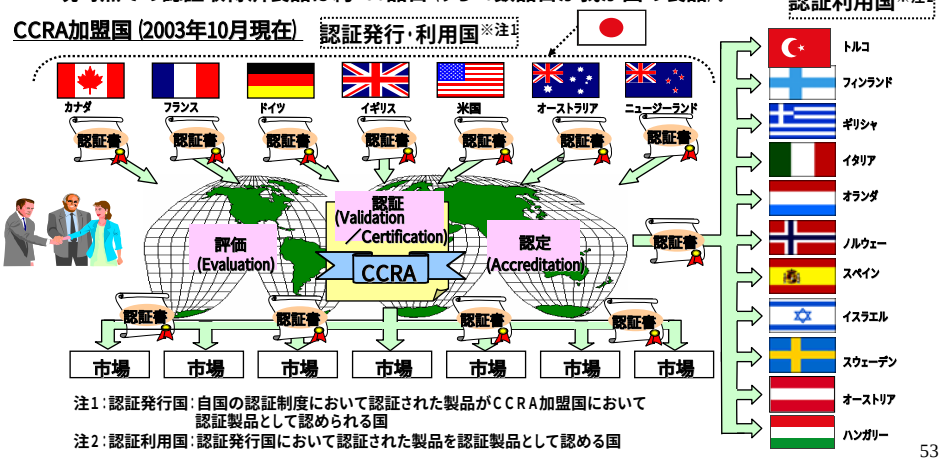


52

CCRA
(Common Criteria Recognition Arrangement)

METI 経済産業省

- CCRA(Common Criteria Recognition Arrangement)とは、各国の政策実施機関が IT製品等の安全性を客観的に評価した結果を国際的に相互承認するための枠組み。1998年にISO/IEC15408(別名：Common Criteria)に基づく評価を開始して、米英仏独加5か国の政策実施機関により設立された。
- 我が国は19番目の加盟国。
- 現時点での認証取得済製品は約150品目（うち10数品目が我が国の製品）。



注1：認証発行国：自国の認証制度において認証された製品がＣＣＲＡ加盟国において認証製品として認められる国
注2：認証利用国：認証発行国において認証された製品を認証製品として認める国

53

次世代認証基盤

METI 経済産業省

- **ITの浸透によって、認証の世界はますます拡大・複雑化**
  - 様々なレベルでの認証が必要に（強い認証も必要だが、利便性も極めて重要）。
- **電子署名だけではなく電子認証も重要**
- **バイオメトリクス等認証技術の評価の推進**
  - 統一的な評価尺度について考えてみる。
- **統合管理、分散管理できる環境の整備**
- **人～端末からサーバーまで、トータルな認証基盤（本人認証、属性認証、機器認証、コンテンツ認証、機能認証…）**
- **PKI、TCG(Trusted Computing Group)、Liberty Alliance等の動き**

54

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

URL：http://www.meti.go.jp

55