

# 情報セキュリティとプライバシー

1995年当時、インターネット時代の到来を機に情報資産の保護が切実な問題となり、企業における情報セキュリティ対策への関心が一気に高まったことがあります。セキュリティ対策で重要なのはセキュリティ基準であり、そのためには企業のセキュリティ・ポリシーの作成が大切とされ、各企業がこぞって自社のセキュリティ・ポリシーを打ち出したものです。しかし現実にはポリシーが先行したきらいがあり、それが運用の現場で生かされていない状況が多々報告されました。せっかくのポリシーが使用されずに、今では陳腐化してしまっている例も多く見られます。

近年、情報セキュリティの確立は企業活動を支えるマネジメント・システムの一つとしてとらえられ、その重要性がますます増えると同時に、実際の運用における知識と知恵が求められています。また、企業の情報セキュリティには、プライバシー対策という新たな経営課題も加わっています。すなわち、個人情報の悪用や漏えいを防ぎ、個人のプライバシーを保護するための法律「個人情報保護関連5法」が2003年5月に成立し、既に施行された基本法部分を除き、2005年4月1日に施行されます。

このような情報セキュリティとプライバシー保護についての貴社の備えは十分でしょうか。情報システムとその環境が刻々と変化する中、情報セキュリティ対策も新しい考え方と技術を備えながら絶えず変容し続ける必要があるでしょう。

そこで今号は「情報セキュリティとプライバシー」特集とし、その考え方から実践方法、テクノロジーまでの多角的なアプローチの中で、できるだけ最新の情報を掲載することに留意しました。

## Perspectives in this Issue

### Information Security and Privacy

Back in 1995, with the advent of e-Business, security of information assets suddenly became a primary area of concern. At that time, security standardization was considered to be most crucial for information security, and almost all of the enterprises rushed to develop their own security policies. However, in reality, these policies tended to be too advanced to implement in real-world applications and were not exercised at operational levels. Today, we see many examples of these valuable policies forgotten and obsolete.

Today, practicing information security is considered as one of the management systems that support enterprise activities, and at the same time, with its significance increasing, services and tools in putting information security into operation are relatively easy to get from vendors. However, many serious information exposure accidents are being reported everyday and external security threats like Virus and Cracking are increasing in numbers much faster than before. Furthermore, companies have to be prepared for the enactment of "Act for the Protection of Personal Information" in April 1, 2005.

Obviously, to deal with these new situations, we need to understand what is happening in the rapidly changing real world of Information Security and Privacy, and to take an effective way of choosing management methodology, tools and operational practices.

This special issue on "Information Security and Privacy" covers, as wide as possible, the latest information of diverse approaches to the issues ranging from ways of thinking to implementation methods and technologies.

プライバシー保護の管理に、まずはCPOの設置を

近ごろでは、CEO( Chief Executive Officer : 最高経営責任者 )とかCIO ( Chief Information Officer : 最高情報責任者、IT担当役員 )というように、米国流の役職名を採用する国内企業も増えてきました。では、CPOのことはご存じでしょうか？

CPOとは、Chief Privacy Officer( 最高プライバシー責任者 )のこと。プライバシー保護に厳しい欧米では以前から設けている企業が多かったのですが、国内でも2005年4月の「個人情報保護関連5法」の施行を前に、その設置が急がれています。

従来、企業はお客様に対して担当部門ごとに接点を持っていました。しかし、個人情報保護法の精神は「個人としてのお客様」と「個人情報取り扱い事業者としての企業」の1対1の関係を想定しており、企業は全社の情報を取りまとめ、個人に対応できなければなりません。すなわち、その背後には全社として一貫した戦略や方針があり、各部門が具体的にどのような基準で個人情報を取り扱い、どのようにお客様の要望にこたえていくかが明確に把握されていなければならないこととなります。

このような体制の確立のために中心的役割を担うリーダー、それがCPOであり、一般的にはCIOやCSO( Chief Security Officer )とは別に設けられます。プライバシー保護のための企業の体制づくりには、まずCPOを任命し、その下に各事業部門や本社スタッフ部門を交えたクロス・ファンクションによるコア・チームを編成し、その中で、個人情報の取り扱い方針、ITシステムの追加・変更・開発を含んだ全社統一の施策を進めていくことが有効です。また、社員に対しては、個人情報保護についての社内規定順守を進めるとともに、プライバシー保護についての正しい理解を促す教育や意識改革を積極的に行い、企業文化として根付かせていくことが望まれます。

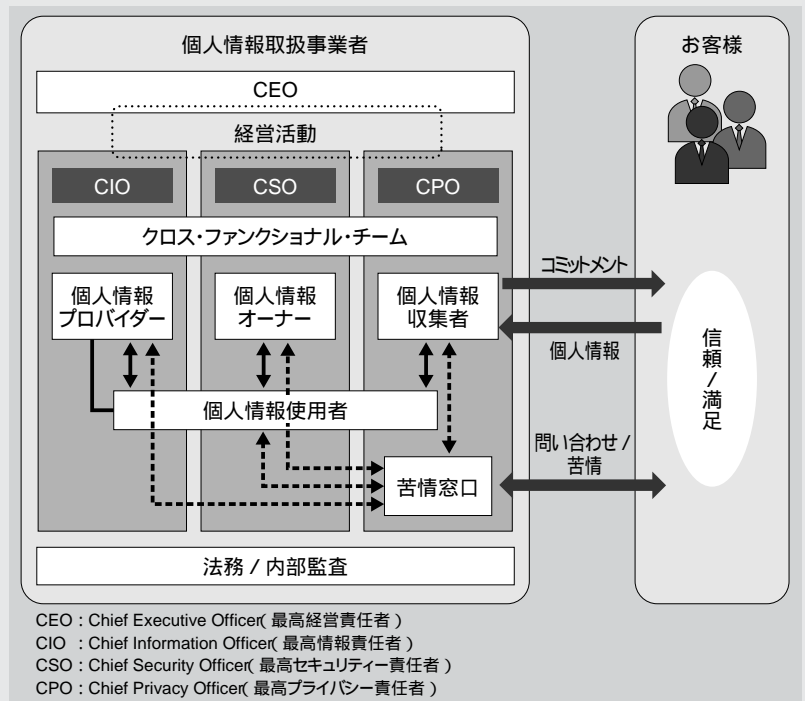


図. 個人情報管理体制