# セキュリティコンサルティングの現状とNECの取り組み

## Trend of Security Consulting Businesses and NEC's Consulting Business Menu

杉浦　昌*
Masashi Sugiura


### 要　旨

コンサルティングには様々な種類があります。本稿では，代表的なセキュリティコンサルティングについて述べ，それに対応するNECのセキュリティコンサルティングソリューションの概略を紹介します。

There are various kinds of security consulting businesses. This paper describes our concept for security consulting business, and introduces our corresponding security consulting business menu.


### 1．まえがき

NECのセキュリティソリューションの体系iBestSolutions/Securityは，現在，大きく分けて，情報漏えい対策，サイバーアタック対策，総合アイデンティティ管理，セキュリティマネジメントの4つのソリューションからなります。そしてこれらのソリューションは，教育，アウトソーシング，運用支援，設計・構築，コンサルティングという具体的な作業を通じて実現されます（**図1**）。

これは代表的なセキュリティ構築をモデル例とした場合の位置付けです。現実のセキュリティ対策においては，より幅広い様々なフェーズにおいてセキュリティコンサルティングが求められる場合があります。

そこで本稿では，最初にセキュリティコンサルティングそのものについて解説し，それに対応してNECが実際にどのようなコンサルティングメニューを提供しているかを述べます。

### 2．セキュリティコンサルティングとは

コンサルティングとは，高度な専門的知識や経験を背景に，お客様がかかえる問題点を摘出したり課題を解決したりする行為です。従来は主に企業経営や財務，会計などの分野において行われていましたが，IT（情報システム）が複雑化，高度化するとともに，企業経営において重要な位置を占めるようになってきて，IT分野に特化したコンサルティング，いわゆるITコンサルティングあるいはシステムコンサルティングと呼ばれるものが発生しました。

その後，企業経営の根幹までもゆるがしかねないような重大なセキュリティ事件や事故が多発する一方，その対応に高度な専門的知識と経験が必要とされることから，セキュリティの分野において顧客の課題の摘出や問題解決を行う，セキュリティコンサルティングが行われるようになってきました。

しかし，セキュリティコンサルティングの内容は多岐にわたっており，その正確な定義は明確には定まっていません。そこでNECは，セキュリティコンサルティングをそのアプローチ方法によって，メソドロジー（方法論）コンサルティング，ソリューションコンサルティング，適用コンサルティングの3つに分けて考えています。

以下にそれぞれについて述べます。

#### 2.1　メソドロジー（方法論）コンサルティング

個々のセキュリティ上の問題や課題を，特定の技術や製品を適用することによって解決するのではなく，対象とな

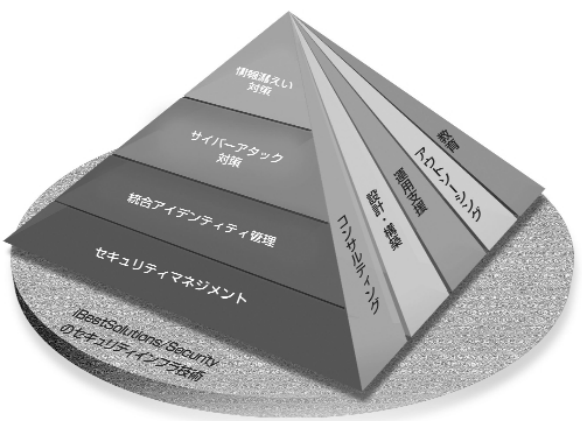


**図1　iBestSolutions/Security**
**Fig.1　iBestSolutions/Security.**

＊ IT基盤システム開発事業部
IT Platform Systems Development Division.

る組織やシステムに対して，あるメソドロジーを適用することによって解決するアプローチです。顧客がかかえる顕在化した問題を直接解決するだけでなく，顧客自身が気付いていない潜在的な真の原因，真の問題点を摘出することもあります。

このアプローチでは，セキュリティ対策の考え方やセキュリティポリシー，組織のあり方やその運営，組織内の権限と責任のあり方，内部教育などのマネジメント的な要因からセキュリティを考えます。さらに，目前の問題解決だけでなく，中・長期的な視点でセキュリティを考えます。

問題解決を行うため，顧客のプロセスそのものの変革をめざすことも多いため，コンサルティングもプロセス的なアプローチをとります。

実際の組織への適用に際しては，メソドロジーそのものは普遍性があるものの，問題解決のために適用する具体的なセキュリティ技術や製品は状況に応じてその時々で最適なものを選びます。ある特定の技術や製品に縛られることなくコンサルティングを遂行するので，自社が取り扱っている技術や製品ではなく他社の技術や製品の採用を勧めることもあります。

メソドロジーコンサルティングを実施するコンサルタントには，セキュリティ全般に関する幅広い技術を有した上で，深い洞察力と確かな考察力，問題摘出能力，問題解決能力を持っていることが要求されます。

具体的には，ネットワークやコンピュータのセキュリティ技術に精通しているだけでなく，組織におけるセキュリティ対策の実践的な経験や知識を持つとともに，セキュリティ対策のメソドロジーを理解した上で，組織の経営者やリーダなどのマネジメント層の視点を併せ持つことが必要です。さらに，技術の流れや法制度の動向，規格・基準の動向，行政の動きなどを把握し，セキュリティの考え方の潮流の本質を把握している必要があります。

**図2**に，セキュリティにおけるメソドロジーコンサルティングの特性を記します。

○戦略レベルで解決策を考える。
○セキュリティ対策の方法論に則ってコンサルティングを行う。
○セキュリティマネジメントの観点から問題解決を行う。
○問題解決のため，顕在化していない本質的な課題を摘出してその解決をはかる場合もある。
○セキュリティ製品やSIとは独立して行われるのが普通である。
○コンサルタントには，次のような領域における高度かつ幅広いスキルと経験が要求される。
・組織のセキュリティマネジメント
・リスクアセスメント，リスクマネジメント
・ITセキュリティ技術
・セキュリティの国際標準や規格
・法制度や認定制度
・特定の製品やSierに偏らない公平性，客観性
○ITベンダー内の独立したコンサルティング部門，あるいはセキュリティ専門のコンサルティング会社が行う場合が多い。
○個別対応的な要素が多いため，高価格になりがちである。

**図2　メソドロジーコンサルティングの特性**
**Fig.2　Characteristics of methodology consulting.**

### 2.2　ソリューションコンサルティング

セキュリティ対策に効果のある個別の技術や製品群を適用することによって，顧客のセキュリティ上の問題点や課題を解決しようとするアプローチです。

セキュリティ技術は，現実的な数々の対応策の経験から発展してきたものが数多くあります。反対に，実際にセキュリティの現場で実運用されたことのない技術は，それが理論上どんなに優れたものであっても，あくまでも実験的な未完成のものとしか評価されません。このような技術を実際に適用するには十分な事前評価と試用期間が必要です。このため，現実のセキュリティ対策では，実践の場においては評価の定まった定石といえる対応策を採用することが多くみられます。限られた費用的・時間的・人的リソースの制約のもとで間違いのないセキュリティ対策を効率的に行うためには，それら定石のなかからとるべき対応策を選択して実施することが現実的です。このセキュリティ対策の定石を使いやすい形でまとめたものがセキュリティソリューションです。ソリューションを適用することによって顧客の問題を解決するコンサルティングがソリューションコンサルティングです。

ソリューションコンサルティングの作業内容には様々なものがありますが，実施するためには，具体的なセキュリティ対策技術と実践的な知識が必要です。また，単に製品技術や知識を持つだけでなく，それを組み込んだシステムの設計・構築から日々の運用までの全体を設計する力が必要です。

顧客のセキュリティ対策のプロジェクトと同時進行あるいはその一部としてコンサルティングを実施することも多いので，コンサルタントにプロジェクトマネジメントの能力が求められることもあります。

このため，ソリューションコンサルティングは，多くは大規模システムやミッションクリティカルなシステムの構築や運用を行うことのできる技術力と経験のあるITベンダーが実施しています。

ITベンダーの場合，顧客の業務システムやアプリケーション構築を行う顧客担当部門とは別の部門に属するセキュリティ専門家が，顧客や顧客システムを担当しているSE部門と意見交換を実施しながらコンサルティングを行う場合が多くみられます。

SE部門とは別の部門がセキュリティコンサルティングを行うことにより，コンサルティングの公平性・中立性を維持しつつ顧客の個別の用件やシステムの状況に合ったコンサルティングを実施することができます。

**図3**に，セキュリティにおけるソリューションコンサルティングの特性を記します。

○戦術レベルで解決策を考える。
○ITセキュリティ技術の視点から課題解決を行う。
○セキュリティ対策に効果のある技術やシステム，対策手法をもとにして，コンサルティングを行う。
○コンサルタントには，高度で幅広いITセキュリティ技術のスキルと実践経験が要求される。
○ITベンダー内のセキュリティ技術に詳しい部門，あるいはセキュリティ専門のSI・構築会社が行う場合が多い。

**図3　ソリューションコンサルティングの特性**
**Fig.3　Characteristics of solution consulting.**

### 2.3　適用コンサルティング

近年のITシステムの高度化，大規模化に伴い，セキュリティ製品やシステムを利用するためには高度な技術と利用形態に合わせた設定が必要になってきました。このような，製品やシステムを顧客に合わせた形に設定するための作業を行うコンサルティングが適用コンサルティングです。

適用コンサルティングは，たとえばPKI（Public Key Infrastructure）システムの構築や，組織内のPC上のOSやアプリケーションソフトのバージョン管理のシステム，パッチ管理システム，きめ細かいアクセス管理システム，ドキュメント管理システムなど，主に利用に高度な設定を要する製品やシステムに関連して行われます。

ファイアウォールのような一般化した製品やシステムにおいても適用コンサルティングが必要な場合があります。たとえば，ネットワークの利用形態やコンピュータシステムが特殊であったり，非常に複雑なネットワーク構成であったり，高いパフォーマンスあるいは高い信頼性が要求されたりする場合には，適用コンサルティングが有効です。

顧客の状況によっては，ITシステムの概要設計や最適設計なども含むことがあります。場合によっては機器のコンフィギュレーション作業までを含むこともあります。

適用コンサルティングはITベンダーにおいて多く行われています。特に，製品に関連する形で提供されるコンサルティングの多くがこれに属します。

**図4**に，セキュリティにおける適用コンサルティングの特性を記します。

その他，セキュリティ製品を販売している会社の場合は，その製品を顧客に適用するためのシステム設計作業をコンサルティングと呼んでいる場合もあります。さらに，その製品の販売促進活動までもコンサルティングと称している場合もあります。これらは本来のコンサルティングとは異なるものですが，実際のセキュリティ対策にとっては重要なものです。

○セキュリティ対策の執行レベルで問題解決を行う。
○製品やシステムを顧客に適用する作業である。
○その製品やシステムについて詳しい技術者がコンサルティングを行う。
○次のような作業を行う場合が多い。
　・その製品を用いたシステムの設計作業
　・その製品やシステムのコンフィギュレーション作業
　・その製品を用いたシステムの運用基準の作成作業
　・その製品に関する技術的な相談
○そのセキュリティ製品を取り扱っているベンダー内の一部門が実施する場合が多い。
○その製品に習熟しているため，短期間・低価格で実施できる場合が多い。
○特定の製品やシステムを用いることを前提としてコンサルティングを実施するため，場合によっては最適解とならない危険性がある。

**図4　適用コンサルティングの特性**
**Fig.4　Characteristics of application consulting.**

## 3．NECのセキュリティコンサルティング

セキュリティコンサルティングには以上のように多くのものがありますが，NECは，組織のセキュリティマネジメントにとって重要であるPDCAサイクルの考え方をもとにして，様々なセキュリティコンサルティングを行っています。以下にそれを説明します。

### 3.1　PDCAマネジメントサイクルとマネジメント

近年は，様々な分野において，PDCAマネジメントサイクルの重要性が叫ばれてきています。セキュリティマネジメントもこのPDCAマネジメントサイクルに則って行うことが効果があることが分かっています。PDCAマネジメントサイクルとは，組織の運用を，Plan（計画），Do（実行），Check（評価），Act（改善）の4つのプロセスに分類して進める考え方です。もともとは品質管理の分野で盛んになった考え方ですが，広く一般性があることから，業務改善など，様々な分野に適用されるようになってきました（**図5**）。

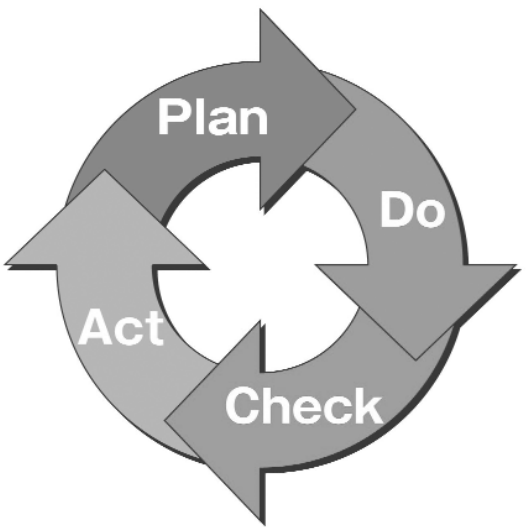


**図5　PDCAマネジメントサイクル**
**Fig.5　PDCA management cycle.**

**表　NECのセキュリティコンサルティングメニュー**
**Table　NEC's security consulting menu.**

| コンサルティング名 | 内　容 | 関連する主なPDCAサイクル |
|---|---|---|
| 情報セキュリティポリシー策定支援サービス | 情報セキュリティポリシーの策定 | Act, Plan |
| ISMS認証取得支援サービス | JIS X 5080（ISO17799）に基づく審査制度であるISMS適合性評価制度の認証取得を支援 | Plan, Do |
| 情報セキュリティ監査サービス | セキュリティ監査の専門家がお客様のセキュリティ状況を監査 | Check |
| ISO15408認証取得支援サービス | ISO15408（セキュリティ評価基準）の認証取得を支援するコンサルテーションサービス | Plan, Do |
| 情報漏えい対策導入サービス | ツールと統制によるお客様の現状に即した対策をコンサルティング | Plan, Do |
| セキュリティインシデント情報提供サービス | セキュリティインシデントに関する最新情報を提供 | Do |
| セキュリティ診断サービス | 擬似アタックを試み、セキュリティホールを効率的に発見 | Check |
| セキュリティマネジメント監査サービス | セキュリティ監査の専門家がお客様のセキュリティマネジメント状況を監査 | Check, Act |
| サーバ要塞化サービス | サーバのセキュリティ向上のための設定変更他を行うコンサルティングサービス | Do |
| セキュリティ緊急対応サービス | セキュリティに関する緊急対応対策の実施 | Do |
| 個人情報保護コンサルティング | 個人情報保護法の施行に対応するための総合的なコンサルティング | Plan, Do, Check, Act |

### 3.2　PDCAサイクルとNECのコンサルティングメニュー

NECは，セキュリティ対策におけるPDCAサイクルの各プロセスごとにコンサルティングメニューを用意しています。

さらに，このPDCAサイクルの一段階上位の階層である，組織のPDCAサイクルをどうやって構築し進めていくかという，マネジメントサイクルそのものをマネジメントするためのセキュリティ戦略策定や，セキュリティポリシーの策定，セキュリティ評価基準であるISO/IEC15408への製品やシステムの適合の支援，セキュリティマネジメントの公的な認証制度であるISMS適合性評価制度やプライバシーマークの取得支援，組織内の教育や啓発体制の構築支援，組織内のセキュリティ対策や運用管理の状況を監査するセキュリティ監査，最近多発しているセキュリティ侵害や情報漏えいなどの事件・事故に対する緊急対応活動，セキュリティ教育活動などの各種コンサルティングも行っています。

**表**に，PDCAサイクルに照らしたNECのセキュリティコンサルティングメニューを示します。

### 3.3　NECのセキュリティコンサルティングの特長

NECは，通信方式の研究や規格作りから，政府官公庁およびその関連機関や業界団体の各種委員会活動，先進・大規模ネットワークシステムの設計構築とその運用・保守，お客様の業務内容に合わせたシステムの構築やアプリケーションプログラムの開発，様々なIT製品の設計・製造，システム導入後のお客様の教育まで，IT分野において幅広い活動を行っています。

また，NEC自身，16万台のコンピュータが4,000のLANに接続された最先端の大規模ネットワークを日常の業務に活用しています。このため，そのセキュリティ対策についても常に最新・最善のものを用いており，IT技術の活用とそのセキュリティの運用維持について豊富な経験を有しています。

NECは，これらを生かした様々なコンサルティングメニューを用意しています。

## 4．むすび

以上，NECのセキュリティコンサルティングに対する考え方を述べ，それに対応するコンサルティングメニューを紹介しました。

NECは今後も，最先端の高い技術力と豊富な経験を背景として，お客様の要望に沿った最適なコンサルティングサービスを提供していく所存です。

### 筆者紹介

Masashi Sugiura
**杉浦（すぎうら）　昌（まさし）** 1983年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター センター長。