NECのセキュリティソリューション戦略

Strategy of NEC's Security Solutions

木村道弘*
Michihiro Kimura

要　旨

企業にとって，セキュリティ確保は急務となっていますが，技術の革新，社会構造の流動化，価値観の変化により，新たな課題が顕在化し，従来型の対策ではセキュリティ確保が困難になっています。

本稿では，最近の企業環境の変化に対する，NECのセキュリティへの取り組み方針，並びに，具体的なセキュリティソリューションとサービスの概要を紹介します。

For an organization, the security measure is a pressing need. By the technical innovation, fluidization of social structure and diversification of values, new issues on security become obvious, so it is difficult for the present measure to maintain security.

In this paper, after surveying the issues resulting from changes of the enterprise environment, the strategy of NEC's security business and an outline of security solutions and services are introduced.

1．はじめに

企業の情報セキュリティの現状を，保護資産，脅威，対策のそれぞれの観点から見ると，まず，保護資産に関しては，電子データの大量生成傾向が相変わらず続き，e文書法（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）の成立も相まって，今後もこの増加傾向は続くと予想されます。次に，脅威に関しては，国内外のインターネット定点観測でも明らかなように，脆弱性を突いたインターネットからのワーム攻撃や不正侵入攻撃は絶え間なく続いています。また，PCの盗難や紛失も絶えません。その一方で，対策に関しては，情報セキュリティへの関心が高まってきたとはいえ，予算的な措置も含め地道な対策が進まないのが現状です。

本稿では，以降，第2章で最近の変化を概観し，第3章で対処方針と課題を紹介します。課題については，NEC技報，Vol.56，No.12，「セキュリティ特集」[1]でも述べましたが，ここに概略を再掲します。第4章では，NECのセキュリティソリューション戦略を紹介し，第6章と第7章でそれぞれセキュリティソリューションとサービスを紹介します。

2．最近の企業環境の変化

最近の企業環境を見てみると，技術，社会構造，価値観のそれぞれの面で大きな変化が見られます。技術については，機器の小型軽量大容量化が進み，最近では，1kg未満のノート型PC，数GBのUSBメモリ，Webブラウザと数百万画素のカメラ付き携帯電話など，オフィス環境を簡単に持ち運びできるようになってきました。モバイルや無線LANの普及がこれを支えています。社会構造については，終身雇用制の崩壊とともに，雇用の流動化が進んでいます。事業の根幹をアウトソースすることも珍しいことではなくなってきました。価値観については，企業や組織に対して社会的責任を求める風潮が急速に強まってきました。牛肉偽装事件や欠陥車隠し事件など，社会問題化した事例は枚挙に暇がありません。また，個人に関するデータは個人のものであるという認識のもとに，自分でコントロールしたいという意識改革が進みつつあります。

このような，企業環境の変化に伴って，セキュリティ関連の事故，事件が多発しています。職場に持ち込んだPCによるワームの蔓延，ノートPCの盗難や紛失による機密情報や個人情報漏えい事件が後を絶ちません。特に，個人情報については流失件数が大規模化する傾向にあります。セキュリティ事故は，損害賠償など直接的な損失のみならず，信用失墜，格付け低下など企業経営に多大な影響を及ぼします。セキュリティの確保は，取引先や投資家との信頼関係構築の上でも，事業を継続する上でも不可欠なものであり，IR活動としても重要です。

3．対処方針と課題

多くの企業は，セキュリティ対策の必要性は認識しているが，何から着手し，対策をどこまで実施すればよいのか

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

分からない，専門要員もいないというのが現状です。また，社会構造の変化で，今までの方法ではセキュリティ確保が困難になってきています。相応のセキュリティを確保するには，管理の透明化に加え，事故は起こるものと考え，事故を前提とした対策をとることが必要です。事業継続のためには，事故の影響を最小限にとどめ，致命的な結果に至らせないことが求められます。また，社会環境や脅威は日々変わるため，継続的な対策強化も必要です。

企業におけるセキュリティ確保には，技術的な課題に加えて，人や組織に依存する多くの課題を解決する必要があります。以下では，多くの企業が抱えている課題を列挙します。

（1）客観的評価

セキュリティは単にその企業や組織だけの問題ではありません。これからは，取引先や顧客などのステークスホルダーに対して，その企業のセキュリティ対策が必要十分であることを，客観的評価に基づいて説明する必要（説明責任）があります。

（2）ガバナンス徹底

セキュリティはIT戦略を効果的に遂行するITガバナンス対象の主要な位置付けにあります。しかしながら，実態は，ルールの周知だけではセキュリティを確保できないことから，従来手法による管理の限界が見えてきており，新たな視点での管理の徹底が必要です。

（3）個人ID保護とプライバシ保護

個人や守るべき資産はIDによって識別されます。IDを正しく認識し，不正にIDを使われないよう保護すると同時に，安全かつ利便性を損なわないことが求められます。また，IDによる認証と個人情報とは密接にかかわっており，厳密な認証は，それだけ相手に個人情報を提供することになり，プライバシ保護との両立も求められます。

（4）不正行動抑止

不正操作による情報改ざんや情報漏えいへの対策は，外部からの侵入者やアクセス権限を持たない内部者よりも，本来アクセスする権限を持った者が不正行為を働くケースの方が対策は困難であり，内部者に対するプライバシを考慮した不正行動の抑止が課題です。

（5）追跡可能性と証拠保全

発生した事象を正しく把握し，侵入経路や侵入手法を特定することは，その後の対策に繋がります．セキュリティに関する監査証跡はこの点で重要であり，証拠として改ざん防止対策のほか，プライバシ保護や匿名性などとの両立が求められます。

（6）文書の長期保存

電子文書を長期に保存し，後日証拠として参照可能にするためには，電子文書が改ざんされていないことと，その時点で確かに存在したことを証明できる必要があり，OSやAPの絶え間ないバージョンアップや媒体劣化を克服した長期保存が課題となっています[2)]。

4．NECのセキュリティ戦略

NECのセキュリティ事業に対する基本戦略は，**図1**に示すように，方法論としてのソリューションと，具体的なサービスの2つの軸から，お客様の課題解決を図ろうとするものです。ソリューション軸は，セキュリティマネジメント，統合ID管理，サイバーアタック対策，情報漏えい対策の4層から構成されます。一方，サービス軸は，コンサルティング，設計・構築，運用，アウトソーシング，教育から構成されます。そして，個々のソリューションに対しては，技術的コンピタンスの裏付けのもとに，マネジメントサイクルに即して一貫したサービスと製品群を提供しています。

セキュリティ分野におけるNECの技術コンピタンスは，署名，暗号，生体認証などの要素技術から，PKI（Publik Key Infrastructure），フィルタリング，異常行動検知などのシステム技術に至るまで多岐にわたっています。グリッドコンピューティングのセキュリティや量子暗号などIT環境のさらなる進歩に適応した新たな取り組みも進めています。

NECのビジネスポジションは，**図2**に示すように，ソリ

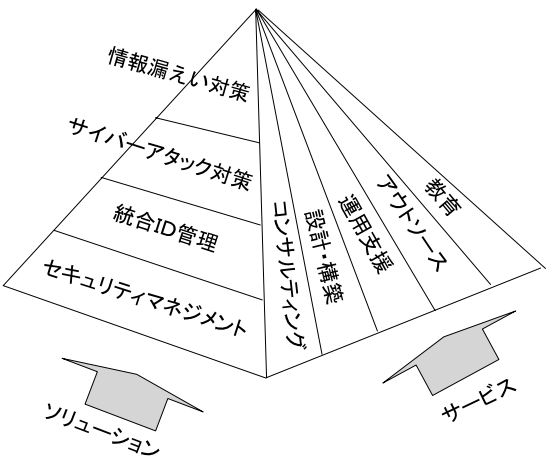

図1　iBestSolutions/Securityの概要
Fig.1　Overview of iBestSolutions/Security.

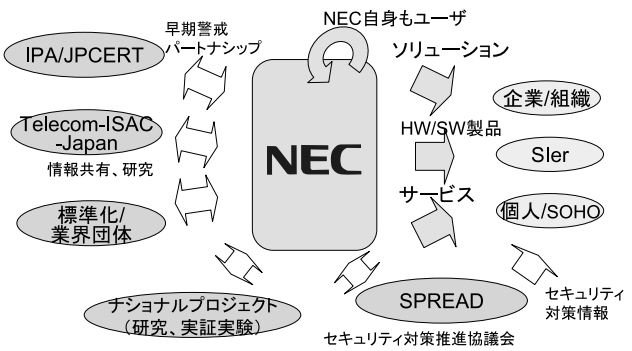

図2　NECのセキュリティビジネスポジション
Fig.2　NEC 's security business position.

ューション提供者という立場だけでなく，ハードウェアおよびソフトウェア製品提供者であり，インターネット総合サービス提供者でもあります。また，NECグループ全体で360拠点，15万人のユーザでもあり，社内で検証されたソリューションを提供できる強みがあります。

5．セキュリティソリューション

NECのセキュリティソリューションは，“管理の第一歩は可視化して数えることから始まり，徹底は確認する仕掛けを組み込むことで成り立つ”というコンセプトのもとに成り立っています。

管理の基本の1つは現状把握です。社内にサーバやPCが何台存在し，それぞれの最新セキュリティパッチの適用状況，最新ワクチンの導入状況が把握できていなければ管理のしようがありません。どのような個人情報がどこに格納され誰が管理しているのかが把握できていなければ管理のしようがありません。

また，管理を徹底するということは，単に報告を受けるだけでは不十分です。確認する仕掛けを組み込み，確認結果（すなわち証拠）をもとに管理することが必要です。

（1）セキュリティマネジメント

セキュリティを継続的に確保するにはPDCAサイクルを回し,新たな脅威に備える必要があります。セキュリティマネジメントソリューションは，組織としてセキュリティマネジメントサイクルを回す仕組み（＝プロセス）を構築します。客観的なマネジメント基準としては，ISO17799やISO15408などの国内外の標準を導入し，信頼の高いマネジメントサイクルの構築を実現します。

（2）統合ID管理

個人や参加システムなどのIDを適切に管理し，利用者が本人であることを確認（authentication）し，資源への利用許可（authorization）に従ってアクセスを制御し，かつアクセスの記録を取ることは，あらゆるサービスの基盤です。統合ID管理ソリューションは，ディレクトリや権限管理についても企業や組織の統廃合に耐える統合的な認証基盤を構築します。

（3）サイバーアタック対策

ワーム対策は，インターネットや持ち込みPCに対する水際対策と内部の耐性向上対策があります。前者の代表は，ファイアウォールや検疫セグメントによる持ち込みPCからのワーム感染防止です。後者はパッチやワクチン適用などの予防措置の徹底が必要ですが，管理を人手に頼っていては徹底は覚つきません。サイバーアタックソリューションは，ITを活用した新たなセキュリティ基盤を構築し，徹底したガバナンスを可能にします。**図3**は，サイバーアタック対策の概念図を示しています。

（4）情報漏えい対策・電子文書保全

情報漏えい対策の基本として，個人認証の強化，業務システムに対する不正操作の抑止，コピーや外部持ち出しの制限，暗号化が挙げられます。情報漏えい対策ソリューションは，ツールの導入だけでなく，体制やルールと一緒になって効果を発揮します。**図4**は情報漏えい対策の概念図です。

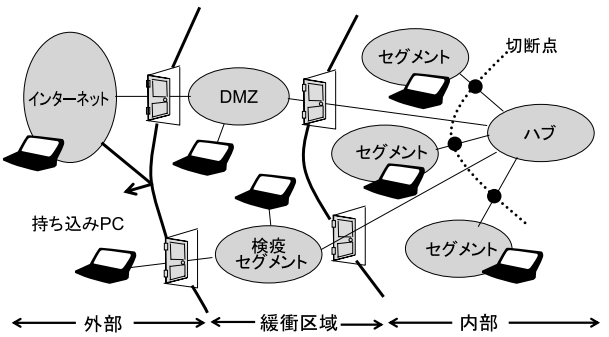

図3　サイバーアタック対策の概要
Fig.3　Conceptual model for cyber attack protection.

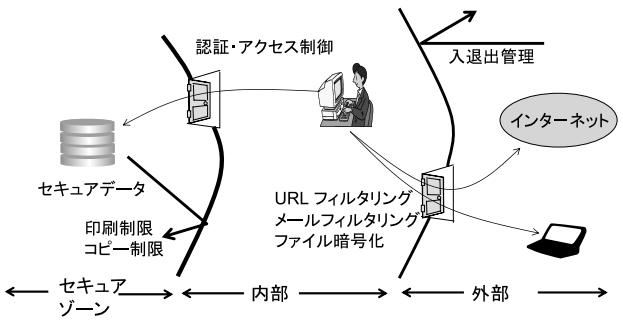

図4　機密保護の概念モデル
Fig.4　Conceptual model for secret protection.

電子文書の安全な保存もこのソリューションのスコープ範囲です。紙の文書に替わって電子文書を原本として扱えるよう，滅失，破壊や改ざんから電子文書を守るとともに，長期にわたる見読性の確保（必要なときに検索でき人間が読める環境を確保しておくこと）を可能にします。

6．セキュリティサービス

セキュリティサービスは，システムの企画から運用まで，セキュリティ対策を深くかつ網羅的に支援します。最新の技術と豊富な経験を兼ね備えたセキュリティのプロフェッショナルが，セキュリティ対策にかかるお客様の負担を大幅に削減します。

（1）コンサルティング

経営戦略とIT戦略の橋渡しを行い，組織に合わせた情報セキュリティポリシーの策定，ISO17799，ISO15408，ISMS適合性評価制度，セキュリティ評価制度などの国内外の標準規格や法律，制度，政府ガイドラインなどに基づいた情報セキュリティ監査の実施や，各種の情報セキュリティに関する認証取得支援など，情報セキュリティマネジメントに関するコンサルティングを提供します。

（2）設計および構築

管理の可視化と結果の確認というコンセプトに従って，

適切な製品選定を行うとともに，ネットワーク，サーバ，アプリケーションから入退室管理などの物理環境に至るまで横断的にとらえ，セキュアなシステムの運用設計や構築を支援します。

（3）運用支援

専任の組織が，セキュリティの運用業務を代行し，様々な不正侵入，ウイルス，ワームの脅威に対して，万全な監視体制のもとに的確なセキュリティ対策を行い，お客様の運用負担を軽減します。ウイルス対策要員の不足，監視体制の脆弱さ，セキュリティ管理コストの増大などの不安や課題を抱えるお客様に最適なサービスです。

（4）アウトソーシング

お客様が，本来の事業や業務に専念していただけるように，システムの複雑なセキュリティ管理を代行します。システムを安全かつ確実に活用するためには，きめ細かなセキュリティ管理と絶え間ない状況監視が不可欠です。しかし，システム運用に十分な人材を確保できないと安全性が保証されず，セキュリティ管理コストが突出するようでは企業資源のロスを生み出す原因になります。アウトソーシングサービスは，システムのセキュリティに関する管理全般を，信頼性の高いデータセンターで24時間365日代行します。

（5）教育（Training Service）

利用者のためのセキュリティコースと，技術者のためのセキュリティコースを用意し，体系立てたコースと自由に選択できるカリキュラムがお客様のスキルアップをお手伝いします。

7．むすび

以上，当面するセキュリティ課題と，その解決のためのセキュリティ戦略およびセキュリティソリューションの概要について紹介しました。日々変化する環境のなか，セキュリティの重要性はますます高まりつつあります。セキュリティソリューション，サービスおよび製品の継続的な強化は，将来にわたって安心安全なシステムを約束する鍵であるといえます。

参考文献

1） 木村；「NECのセキュリティへの取り組み」，NEC技報，Vol.56，No.12，pp.3～5，2003-12.

2） 「デジタル情報の長期可溶性と保存，記録，文書，エンタープライズコンテントマネジメントに関する公共セクターのためのAIIM業界白書」

筆者紹介

Michihiro Kimura

木村　道弘（きむら　みちひろ） 1973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アーキテクチャ戦略主幹。上級システムズアーキテクト。