セキュリティ診断・監視コンサルティングサービス

Security Consulting Service : Vulnerability Analysis and Intrusion Detection System

吉野　恭明 YOSHINO Yasuaki
広島　和弘 HIROSHIMA Kazuhiro
北折　昌司 KITAORI Shoji

インターネットを活用するあらゆる情報システムは，世界中のクラッカー達(注1)からセキュリティ上の欠陥をついた攻撃を受けることになる。したがって，システムをインターネットにさらす前に擬似攻撃を行い，欠陥を調べるセキュリティ診断サービスが必要となる。これは，既に運用を開始しているシステムに対しても，有効な防御手段を探すきっかけとなる。また，こうした攻撃が実際に行われているかを常時モニタするセキュリティ監視システムも，現状を知りすばやい対策を行う意味でその重要性が高まっている。

当社のセキュリティ診断サービスとセキュリティ監視システム構築支援サービスは，総合的なセキュリティコンサルティングサービスの一環であり，国際規格ISO17799に基づく情報セキュリティポリシーの実践を支援するものである。

Any information system connected to the Internet could be attacked by crackers located throughout the world. It is therefore necessary to identify holes in security before a system is set up and connected to the Internet. A vulnerability analysis service is helpful for scanning all security holes in the system. Then, when the system is put into operation, an intrusion detection system (IDS) watches for attack signatures and sends an alarm to the administrators.

Our vulnerability analysis service and IDS integration service are parts of the Toshiba security consulting service, which supports the implementation of an enterprise's security policy based on the ISO 17799 international standard.

1 まえがき

既に，インターネットは日常にごくありふれた存在になりつつある。だれもが携帯電話で電子メールを交換し，ブラウザで世界中を検索し，ときには商品の売買を行っている。しかし，インターネットのセキュリティは，そのれい明期からそれほど進歩していない。それどころか，システムが多様かつ複雑になったのに伴って，セキュリティホールと呼ばれる欠陥が次々と発見されるようになってしまった。今や，企業の情報システムにおいてインターネットを使うということは，こうした欠陥をつく世界中のクラッカー達からの攻撃に，その企業自身をさらすことを意味する。そして，一つの欠陥あるいは攻撃を見逃せば，直ちに企業の顔であるホームページが書き換えられたり，顧客情報のような重要な情報資産が奪われたりするのである。

こうした事態に対処するために，まず対象となる情報システムにどんな欠陥が存在するのか，あるいは現在どのような攻撃をどれくらい受けているのかということをきちんと調査する必要がある。これがセキュリティ診断である。更に，攻撃状況をモニタし，攻撃の性質や重要度に応じた適切な処置を直ちに行うことができるように，セキュリティ監視システムが必要になる。そして，これらをコントロールすることで，常に一定のセキュリティレベルを維持させるのがセキュリティポリシーである。

ここでは，当社が行っているセキュリティ診断サービス及びセキュリティ監視システム構築支援サービスについて述べるとともに，セキュリティポリシーの策定と運用への展開について考察する。

(注1)　他人のコンピュータシステムに攻撃をしかけたり，不正な侵入や情報の破壊・改ざんを行う者。

2 セキュリティ診断サービス

セキュリティ診断には，ホスト内部から設定情報などを調べる方式と，ネットワーク上から擬似攻撃を試みる方式（図1）

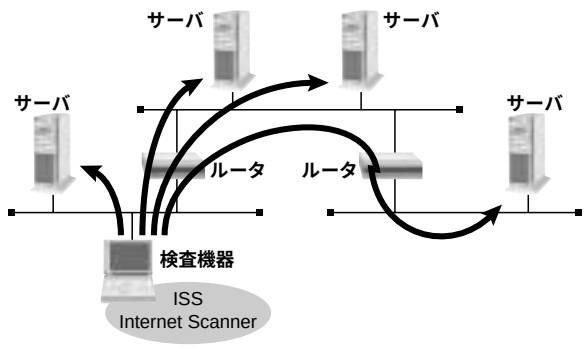


図1．ネットワーク型セキュリティ診断の構成　ネットワークを経由して擬似攻撃を試みることで弱点を発見する。
Network-based vulnerability analysis

がある。当社では，世界的に定評の高いISS社（Internet Security Systems, Inc.）[(1)]の診断ツールInternet Scanner及びSystem Scannerを主に用いてセキュリティ診断サービスを行っている。

Internet Scannerは，800以上のセキュリティホールに関して実際に攻撃を試み，その効果を検証する強力な診断ツールである。実際に攻撃することにより，例えば，ファイアウォールが有効に機能しているかといった，実システムでなければ検証が難しい複合的なセキュリティホールを見つけ出すことができる。一方，System Scannerは，ホスト内部から設定情報を入手して詳細な分析を行うことができる。したがって，ネットワーク上からは検出できなかった問題点や基本ソフトウェア（OS）設定上のミスなどを発見することが可能となる。この両者を適切に組み合わせることによって，効率よくかつ漏れなくセキュリティホールを見つけ出すことができる。

しかし，こうしたツールを用いてセキュリティ診断を行ううえで，考慮しなければならない点が三つある。

⑴　診断の対象となるホストはどれか，またどのような攻撃を想定して検査を行うのかといった“診断目的”

⑵　攻撃が有効であった場合にシステムがダウンしてしまうことも考えられるので，診断実施のタイミングや回復を考慮するといった“診断計画”

⑶　ツールから得られる非常に詳細なセキュリティホール情報を整理することで，対策に結びつける“診断理解”

したがって，当社のセキュリティ診断サービスでは，単にツールを適用するというだけでなく，事前にお客さまへのヒアリングを入念に行い，診断目的と診断計画を明確にするとともに，診断後にはツールから得られる情報を理解しやすいレポートにまとめ，報告会を行うことで理解を深めていただくまでをサービスの対象としている。この流れを図2に示す。

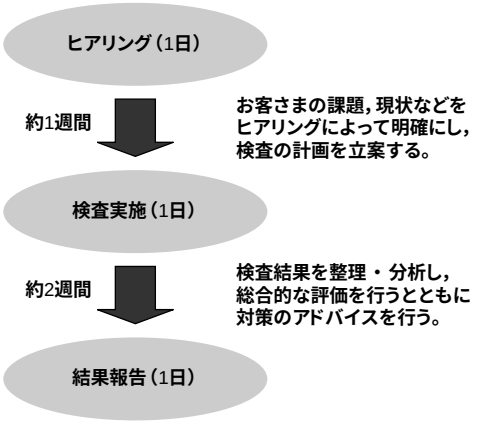


図2．セキュリティ診断作業スケジュール　ホスト5台以下の例を示す。約1か月の期間が必要である。
Schedule of vulnerability analysis service work

また，“シグネチャー”と呼ばれるセキュリティホール情報は年間4回から6回更新され，そのたびに増え続けている。これは，日々新しいセキュリティホールが発見され，それに基づく新たな攻撃が発生していることを意味している。したがって，セキュリティ診断を行い，セキュリティホールを洗い出し，その対策を完全に行ったとしても，その有効性は日々失われてしまうものと考えなければならない。そこで，当社ではセキュリティ診断サービスを定期的に実施していただくメニューを用意している。これにより，セキュリティレベルを維持するとともに，前回の診断時との差異を述べた差分レポートによって，よりいっそう理解を深め，適切な対策を立てることができる。

更に，当社では一定期間だけネットワークを監視し，そのログを解析することによって，どのような攻撃が行われているのかを分析する攻撃状況診断サービスも行っている。当社のセキュリティ診断サービスのメニュー体系を図3に示す。

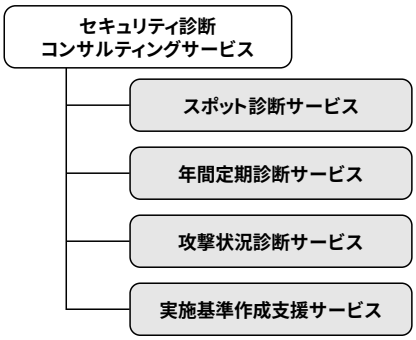
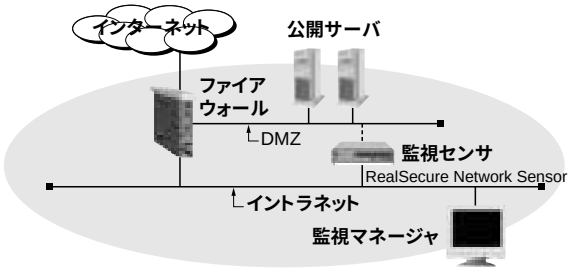


図3．当社のセキュリティ診断サービス体系　診断を日常の運用に取り入れるため，多角的なサービスを実施している。
Menu of vulnerability analysis service

3　セキュリティ監視システム構築支援サービス

ISS社のRealSecure Network Sensorは，ネットワーク上を流れるパケットを監視するカメラに相当する。セキュリティ監視システムでは，この監視カメラを操作し，情報を映すモニタに相当するWorkgroup Managerと組み合わせて使用される。セキュリティ監視システムのもっとも基本的な構成を図4に示す。

しかし，実際には，このような単純な構成によって利用されることは少ない。ファイアウォールやルータが二重化されていたり，負荷分散されていたり，あるいはダイヤルアップ接続がネットワークに飛び込んでいたりと，ネットワーク構成は千差万別である。また，近年の通信の高速化により，ネットワークを監視するセンサ自身が負荷分散を考えなければならない場合もある。更に，診断のときと同様に，何を監視するのか，攻撃が検出されたらどうするのかといったことを



DMZ：DeMilitarized Zone（保護するネットワークと外部ネットワークとの間に追加されるネットワーク）

図4．基本的なセキュリティ監視システムの例　DMZに置かれた公開サーバをイントラネット内部から安全に監視する。
Basic architecture of intrusion detection system

明確にしなければ，結局はセキュリティ監視システムの構成すら決めることができない。

そこで，当社では，こうした企業のネットワーク事情やセキュリティポリシーに合ったセキュリティ監視システム構成やその設定などについて，アドバイスを行うセキュリティ監視システム構築支援サービスを行っている。基本的な構築の作業スケジュールを図5に示す。

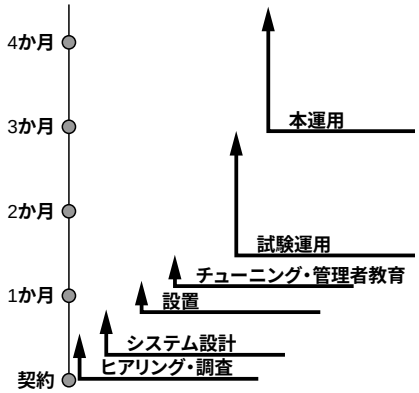


図5．セキュリティ監視システムの構築スケジュール　約3か月で本運用に入る典型的なシステム構築例を示す。
Typical service schedule for intrusion detection system

RealSecure Network Sensorは，攻撃を検出し通知するだけでなく，ファイアウォールと連携して自動的に攻撃を遮断したり，TCP（Transmission Control Protocol）コネクションの切断を試みたりするような防御機能を備えている。また，攻撃検知と連動してカスタマイズ可能なスクリプトを起動させることができるため，独自の自動防御機構を構築することも可能である。しかし，基本的に，攻撃検知後のアクションは企業のシステム運用に依存する面が極めて強い。つまり，防御を完全に自動化することは現実的でなく，熟練したシステム運用者の判断が必要ということである。これが，セキュリティ監視システムを導入するときに最大の問題になることも考えられる。

セキュリティ監視システムの運用を考えた場合，それが一般のネットワーク監視システムと連携あるいは統合すべきという発想は極めて自然である。RealSecure Network Sensorは，ネットワーク監視システムとして普及しているOpenViewやTivoliと連携する機能を持っている。これにより，例えば，運用管理者は攻撃状況とネットワークやサービス稼働状況とを同時に監視することが可能になり，システム管理者がよりいっそう正しい状況判断を行うのに役だつと考えられる。図6はRealSecure Network SensorとOpenViewを連携させたネットワーク統合管理システムの例である。

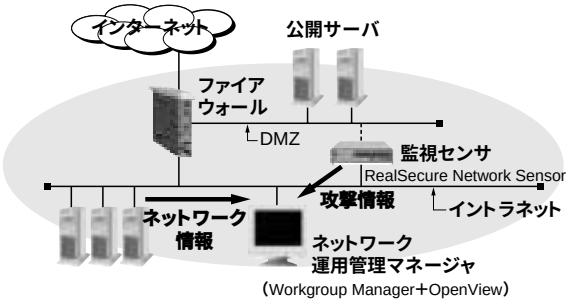


図6．ネットワーク管理と連携したセキュリティ監視システム　攻撃情報とネットワーク・サーバ情報を同時に監視することで正確な判断が可能になる。
Integration of network management system and IDS

しかし，このような高度なシステムを構築しても，最後の判断はシステム管理者が行わなくてはならない点に変わりはない。今後，こうした高いスキルを持った管理者をどのように育成していくか，あるいは企業として運用体制をどのように築いていくかが大きな課題になると考えられる。

4 セキュリティポリシーへの展開

昨年，セキュリティポリシーに関する一つの国際標準ISO17799（Code of Practice for Information Security Management）が策定された。これは，セキュリティポリシーとは何かを定義し，実際のシステムに即した130余りの具体的なセキュリティ要件を示したガイドラインである。わが国では，これのJIS化作業が進められ，本誌が発行されるころにはJISとして規定されているかもしれない。日本政府は，2000年7月にこれを先取りする形で政府機関向けのセキュリティポリシーガイドライン[(2)]を公表するとともに，通商産業省（当時，現経済産業省）は，JIS規格に基づくセキュリティ認定制度を2001年度に発足させると発表した[(3)]。

セキュリティポリシーは単なる方針や理念ではない。企業に代表される組織が，その情報セキュリティを確実に向上させていく，あるいは高いレベルに維持し続けるための仕組みを象徴するものである。したがって，セキュリティポリシーというドキュメントが完成しても，セキュリティポリシーを作ったことにはならない。それをどのように運用し，末端のシステムや組織の構成員まで浸透させていくかが重要なのである。この点を，政府の“情報セキュリティポリシーに関するガイドライン”では，図7のようなサイクルを用いて説明している。

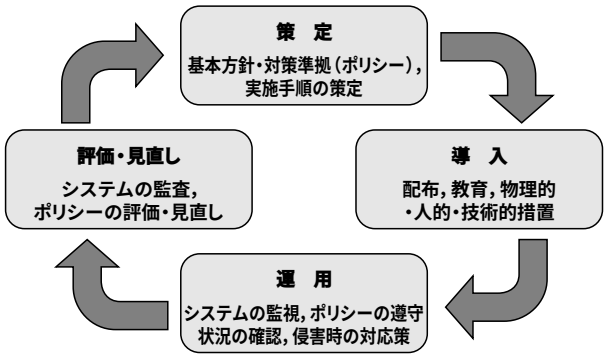


図7．セキュリティポリシーの実施サイクル　四つのフェーズを繰り返すことで，実際的なセキュリティの向上を図る。
Implementation cycle for IT security policy

このサイクルは，ちょうどPlan-Do-See-Checkモデルを適用したような，セキュリティを維持向上させていく無限の循環を意味し，その中心にあって，この循環の根拠あるいは原動力となるのがセキュリティポリシーというわけである。したがって，こうした考え方に基づく認定制度でも，単にセキュリティポリシーの有無が審査されるのではなく，こうしたセキュリティプロセスが組織として作られているか，あるいは機能しているかが問われるものと推定される。

当社のセキュリティ診断サービスは，このサイクルの中では“評価”に位置づけられる。すなわち，ここで行われるリスク分析の一つの手段として利用されることになる。セキュリティ診断サービスによって，リスク分析は，机上の検討では得られない生々しい現状を扱うことが可能になるであろう。また，セキュリティ監視システムの構築は“導入”の一つとなる。これにより，従来は見えなかった侵入攻撃を常時モニタすることが可能になる。

しかし，当社のセキュリティサービスはこれにとどまらず，セキュリティポリシーによるサイクル全体に貢献できるものであると考えている。例えば，セキュリティ診断サービスでは，単に“評価”として診断を行うのではなく，その後の方針を決める“策定”に結びつくアドバイスを行う。また，セキュリティ監視システム構築支援サービスは，単に“導入”として構築するだけでなく，その後の“運用”に対する支援を行うものである。

このように，二つのサービスはそれぞれ複数のフェーズに関係し，その連携を深めることで，セキュリティポリシーに基づくサイクルを円滑に循環させる働きを持っている。これにより，セキュリティポリシーをいっそう強固で実効力のあるものにすることができるであろう。

5　あとがき

当社のセキュリティ診断サービス及びセキュリティ監視システム構築支援サービスは，企業のセキュリティポリシーの実践を助け，セキュリティレベルの維持向上を目指したものである。そのため，お客さまとのコミュニケーションを大切にし，実際に診断や監視システム構築を行う前のヒアリングや，後のレポートなどに重点を置いたコンサルティングサービスと位置づけている。

今後は更に，企業の広範囲なセキュリティに対する要件にこたえられ，総合的なセキュリティコンサルティングサービスとして，インターネット社会の健全な秩序作りに貢献できるよう努力を続けていきたい。

文　献

(1) Internet Security Systems Inc.：http://www.iss.net/
(2) 首相官邸 セキュリティ対策推進会議：情報セキュリティポリシーに関するガイドライン，http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html
(3) 経済産業省（旧通商産業省）情報セキュリティ政策：http://www.meti.go.jp/kohosys/topics/10000098/
(4) 電子情報技術産業協会（JEITA（旧JEIDA））セキュリティ委員会：http://it.jeita.or.jp/jhistory/committee/security/index.html

吉野　恭明　YOSHINO Yasuaki
e-ソリューション社 SI技術開発センター SI技術担当。
セキュリティ診断・監視サービスの開発に従事。
Systems Integration Technology Center

広島　和弘　HIROSHIMA Kazuhiro
e-ソリューション社 戦略企画部 商品開発担当主務。
セキュリティサービス企画に従事。
e-Solution Co. Strategic Planning Div.

北折　昌司　KITAORI Shoji
e-ソリューション社 SI技術開発センター SI技術担当主務。
セキュリティサービスの開発に従事。
Systems Integration Technology Center