セキュリティプラットフォームサービス

Security Platform Services

新藤　清史　　**小林　英彦**

■ SHINDOH Kiyoshi　　■ KOBAYASHI Hidehiko

IT（情報技術）プラットフォームサービスの一つに，セキュリティプラットフォームサービスがある。“セキュリティ”という単語を10人に聞くと，10通りの答えが返ってくる。したがって，セキュリティプラットフォームを検討する際には，個別ソリューションの機能のみならず，包括的な視点での検討が必要である。

東芝では，実際の情報システムを見据えたトータルなセキュリティソリューションをお客さまに提供している。

One of the information technology platform services is the security platform service. If 10 people are asked the meaning of the word *security*, 10 different replies can be expected. When a security platform is being examined, examination not only of the functions of individual solutions but also from a comprehensive viewpoint is required.

Toshiba provides total security solutions based on an understanding of the actual information system.

1 まえがき

ITの進化や社会情勢の変化とともに，それに必要となるセキュリティ対策も複雑化，高度化している。東芝のセキュリティソリューションでは，セキュリティポリシーの策定からシステム設計，構築，運用までをトータルに提供し，お客さまにとってベストなソリューションでビジネスをバックアップすることを目指している。

ここでは，当社の考えるセキュリティソリューションと，その中で使用する代表的なソリューションについて述べる。

2 東芝のセキュリティソリューション

“セキュリティの確保”は難しいテーマだが，その基本は以下の3点に帰着される。

⑴　何から何を守るか
　　→どんな脅威から，どんな資産・情報を

⑵　誰が何をしてよいか，何にアクセスしてよいか
　　→権限とアクセス制御

⑶　方針やルールを決め，守り守らせ，確認すること
　　→ポリシー，運用，監査

一般に，組織経営管理サイクルと情報システムサイクルがある。当社のセキュリティソリューションでは，これらのサイクルを組み合わせた形で展開することにより，組織経営に基づく一貫性の高いセキュリティシステムの実現を目指している（**図1**）。

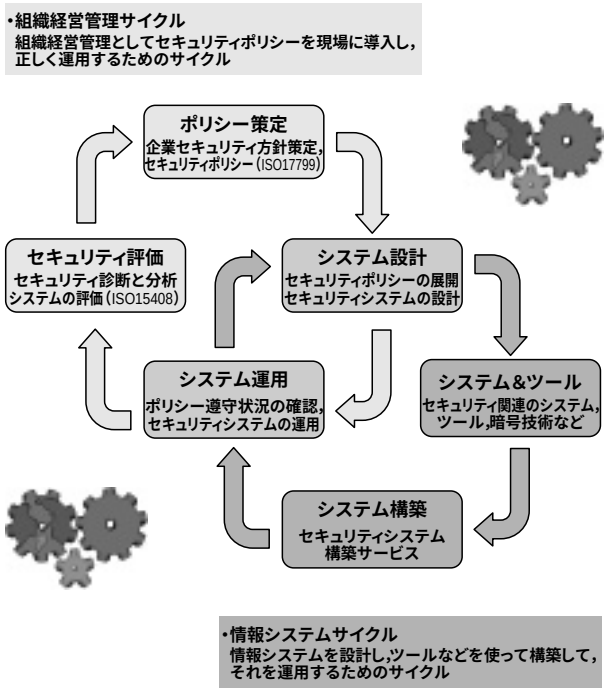


図1．東芝セキュリティソリューションのサイクル―当社のセキュリティソリューションは，組織経営管理サイクルと情報システムサイクルを融合させる。

Cycle of Toshiba security solution

これらのサイクルを実現するため，当社では**図2**に示すようなソリューションを用意している。これらのうち代表的なものについて，以下の章で述べる。

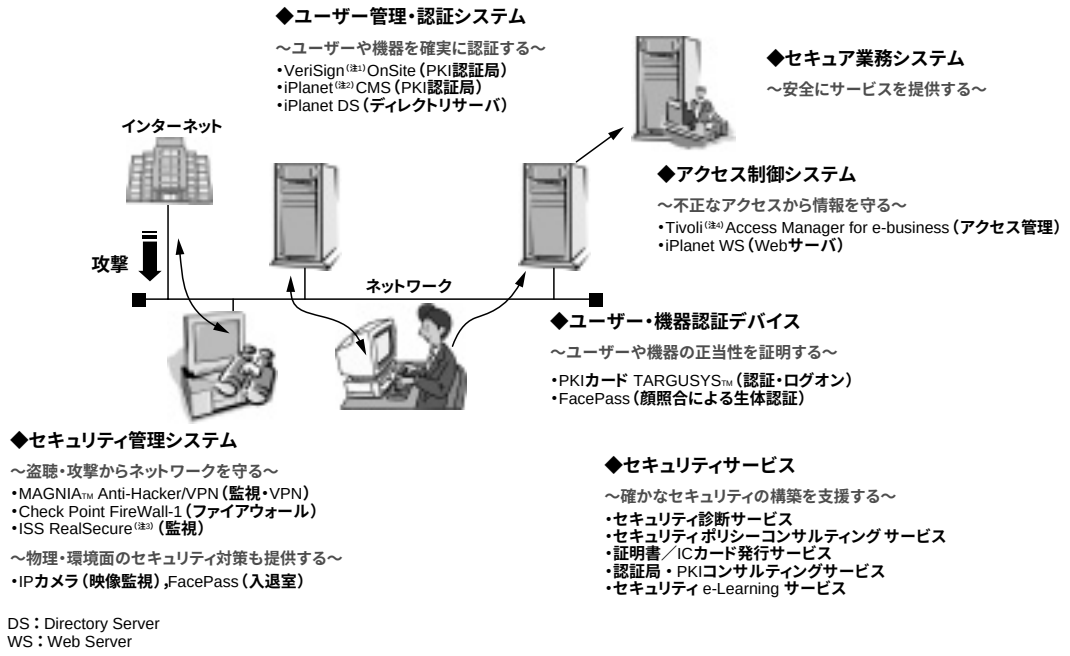


図2. 東芝のセキュリティソリューション― 当社の持つセキュリティソリューションを，製品群を中心に一覧にしたものである。
Toshiba security solutions

3 経営管理サイクルのソリューション

経営管理サイクルから見た当社のセキュリティソリューションの代表的なものとして，企業経営を踏まえたセキュリティポリシーサービスと，現状把握のためのセキュリティ診断サービスがある。

3.1 セキュリティポリシーサービス

セキュリティシステムの第1段階として，企業としての，特に企業経営の視点から導き出されるセキュリティポリシーの作成があり，昨今，その重要性が叫ばれている。セキュリティ管理のグローバルスタンダードの代表として，製品・システムのセキュリティ評価基準であるISO（国際標準化機構）15408と，セキュリティ管理・運用の実践規範であるISO17799がある。

セキュリティポリシーは，単に紙に記載されたものではなく，それが全社的に実行されて，初めて効果の出るものである。サンプルポリシーはインターネットなどに多くあるが，単にそれを持ってくるだけでは実行は伴わない。個々の項目について自社の現状など比較し，適用できる形で作成していく必要がある。当社のセキュリティポリシー作成支援サービスでは，以下のようなステップを踏んで，お客さまのポリシー作成を支援していく（**図3**）。

また，作成されたポリシーの適切な運用も重要な項目である。日本でもセキュリティポリシーが適切に運用されているかを評価する動きが出てきている。これがISMS（Information Security Management System）認定制度である。当社では，みずからがISMS認定制度を受けるとともに，その際に得られたノウハウを踏まえて，お客さまのISMS認定取得に向けたコンサルティングサービスも今後展開していく。

3.2 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がある。当社では，世界的に定評の高いISS社（Internet Security Systems Inc.）の診断ツールInternet Scanner®(注5)を主に用いて，セキュリティ診断サービスを実施している。

Internet Scannerでは，1,000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。ただし，ツールは絶対ではなく，セキュリティホールの誤検出や擬似攻撃によるシステムダウンが発生するケースも少なくないのが実情である。

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だけではなく，事前に入念なお客さまのヒアリングを実施して診断目的と診断計画を明確にするとともに，診断後には，ツールから得られた情報を入念に分析し，理解しやすい

（注1） VeriSignは，Veri Sign社の登録商標。
（注2） iPlanetは，米国及びその他の国における米国SunMicrosystems，Inc.の商標又は登録商標。
（注3） RealSecureは，Internet Security Systems Inc.の米国における登録商標。
（注4） Tivoliは，IBM Corporationの米国及びその他の国における商標。
（注5） Internet Scannerは，Internet Security Systems Inc.の商標又は登録商標。

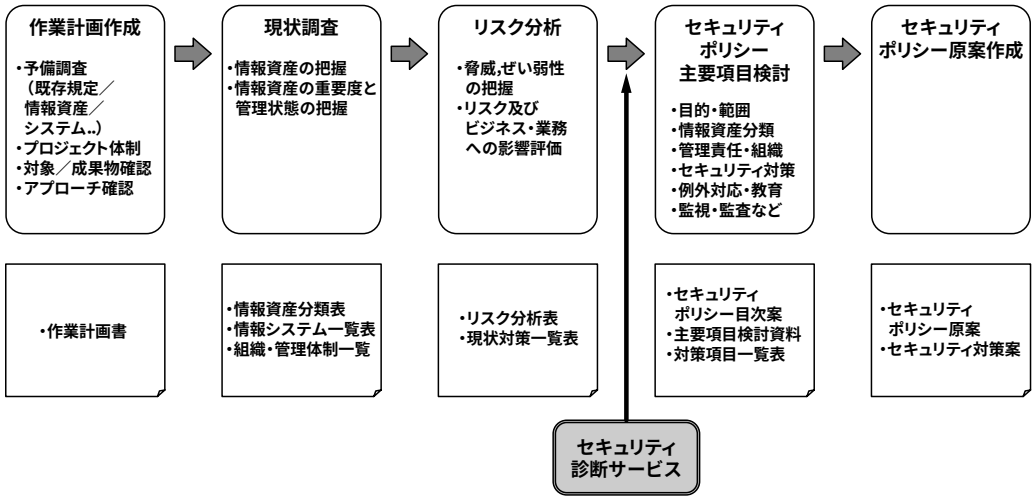


図3．セキュリティポリシー策定の流れ— セキュリティポリシー作成の一例を示す。
Flow of security policy formulation

レポートにまとめたうえで，報告会を実施することにより，お客さまの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。

日々，新しいセキュリティホールが発見されているのは周知のとおりである。したがって，セキュリティ診断サービスで検出できるのは，診断時点でのセキュリティ対応状況であり，未来永劫（えいごう）の保証ができるものではない。セキュリティ定期診断サービス（年2回・年4回）とともに，診断後の日々の運用提案を含めたセキュリティ運用コンサルティングや，セキュリティポリシーへのフィードバックといったコンサルティングサービスも併せて実施している。

4 情報システムサイクルのソリューション

情報システムサイクルにおけるセキュリティソリューションの代表的なものについて述べる。いずれのソリューションも，単に製品を導入するだけではなく，どのように使用していくとセキュリティを守ることができるのか，というコンサルテーションが肝要である。お客さまのニーズに従い，これらのソリューションを組み合わせて展開していく。

4.1 認証システムソリューション

インターネット／イントラネットを利用する際，盗聴や改ざん，なりすまし，否認といったリスクを回避する方法の一つとして，情報の暗号化や電子署名が有効であるとされており，公開鍵暗号方式を元に暗号化や電子署名を利用した，セキュリティインフラのPKI（Public Key Infrastructure）が注目されている。

PKIでは，発行元の認証局を信頼することが電子証明書を信頼することになり，認証局がPKIにおける信頼の基盤になる。つまり，信頼できる認証局を構築し運用することがPKIを成功させる重要な鍵の一つといっても過言ではない。

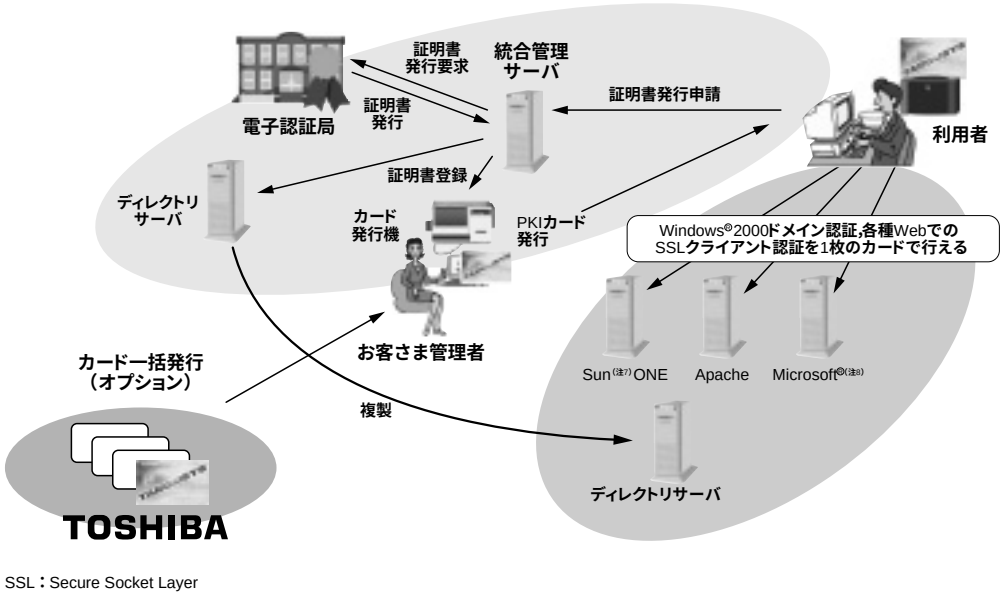
ただし，PKIにおいては，信頼できる認証局が強固なセキュリティにより安全に運用していたとしても，加入者の秘密鍵は加入者の責任で守る必要がある。昨今のパソコンの小型化などで持ち運びが便利になった反面，パソコン上に格納されている秘密鍵が盗まれ，盗聴や改ざんも発生している。

そこで注目されているのがICカードである。PKI対応のICカードでは，秘密鍵と公開鍵の鍵ペア，及び電子証明書を格納することができる。秘密鍵を使用して暗号化処理を行うことはできるが，カード内の秘密鍵を盗み出すことは難しい。

このような状況にかんがみて，当社ではPKI対応のICカードシステム TARGUSYS$_{TM}$（ターガシス）を開発している。TARGUSYS$_{TM}$は代表的なブラウザ及びメーラに対応しているほか，Windows®[注6]2000のスマートカードログオン機能にも対応している。

ICカードを用いたPKIシステムは，その構築にもノウハウが必要だが，重要な点の一つに，その運用がある。ICカードを紛失した場合の対応など，実際にエンドユーザーへ展開した場合，管理者側の作業は少なくない。また，ICカードをPKIカードとして使用するだけではなく，表面印刷を行ったうえで，従業員証として活用した事例もある。そのような場合，運用の重要性はますます高くなってくる。TARGUSYS$_{TM}$は単なるICカードではなく，その運用管理まで含めたシステムであり，その運用方針まで含めたコンサルティングサービスである（**図4**）。

（注6） Windowsは，米国Microsoft Corporationの米国及びその他の国における商標又は登録商標。



SSL：Secure Socket Layer

図4. TARGUSYS$_{TM}$の全体像— TARGUSYS$_{TM}$は単なるICカードだけではなく，その発行管理まで含めたシステムである。
Overview of TARGUSYS$_{TM}$ system

4.2　アクセス制御管理システムソリューション

多くの業務がシステム化されるに伴い，システムごとにユーザーアカウントやパスワードが必要になるが，ユーザーが覚えきれずに簡単なパスワードを設定したり，場合によっては紙に書いてはっておく，といったケースも見受けられる。

その解決策の一つとして，昨今ではシングルサインオン ソリューションが注目を集めている。シングルサインオン ソリューションを導入すると，エンドユーザーは1回の認証ですべてのシステムがアクセス可能になり，エンドユーザーの利便性が向上する。

しかし，シングルサインオン ソリューションのメリットは，エンドユーザーの利便性だけではない。多くのシングルサインオン ソリューションでは，ユーザーごと及びシステムごとのアクセス制御が実装可能である。これにより，本来権限のないユーザーが参照できない情報を確実に守ることができるとともに，シングルサインオン対象システム側で必要以上にアクセス制御を意識することなくシステム実装が可能になる（**図5**）。

また，アクセス制御の基本の一つに，ユーザー情報の管理がある。ユーザー＝従業員であるケースが多いが，従業員情報は人事システムなどの基幹システムで管理されているケースが多い。昨今のアクセス制御システムでは，ユーザー情報が LDAP（Lightweight Directory Access Protocol）に基づくデータベース（DB）に格納されているのが一般的になりつつあり，この設計も重要な要素になっている。

単にシングルサインオン（アクセス制御）ミドルウェアを導入するだけではなく，基幹システムとの連携や，場合によってはユーザーアカウントの設定ルール作り，適切なアクセス制御のためのグルーピングといったコンサルティングサービスも併せて実施している。

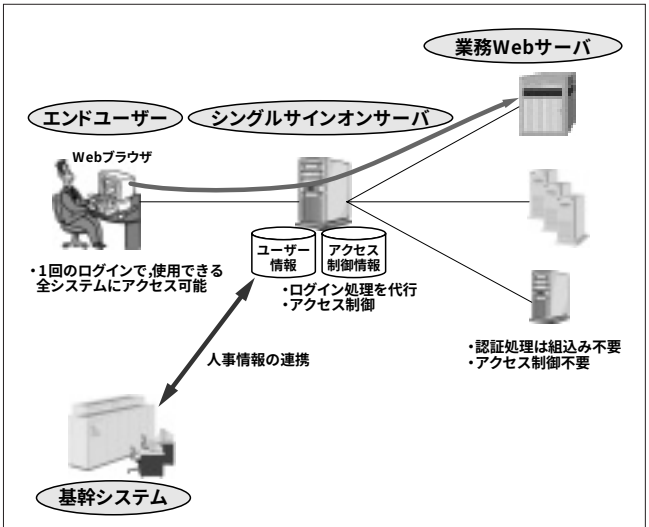


図5. アクセス制御管理システムのイメージ— シングルサインオンサーバでログイン処理とアクセス制御を実施する。
Image of access control system

4.3　ネットワークセキュリティソリューション

情報システムのセキュリティ管理を実現する方法として，

（注7）Sunは，米国及びその他の国における米国 SunMicrosystems,Inc.の商標又は登録商標。
（注8）Microsoftは，米国 Microsoft Corporationの米国及びその他の国における商標又は登録商標。

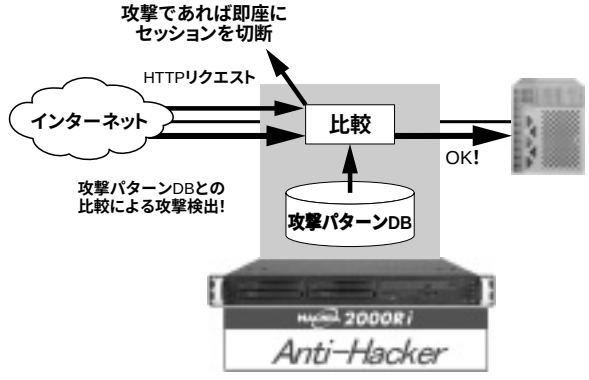
ネットワーク上を流れるパケットという観点からは，以下の２点が考えられる。

⑴　不正パケットが入り込むのを防ぐ。

⑵　不正パケットが流れていないかを監視する。

不正パケットが入り込むことを防ぐ代表的な製品がファイアウォールである。当社では，アプライアンスサーバであるMAGNIA$_{TM}$ 2000Ri/FireWall-1と，CheckPoint Software Technologies社のFireWall-1[注9]を商品化している。アプライアンスサーバを使用すると，サーバ自体のセキュリティ設定は完了しており，後はファイアウォールの設計と設定だけで導入が完了する。ただし，サーバのOS（基本ソフトウェア）などは選択できない。

また，当社独自製品として，Webサーバ，メールサーバ，DNS（Domain Name System）サーバに特化した，不正アクセス防御用のアプライアンスサーバであるMAGNIA$_{TM}$ 2000Ri/Anti-Hackerがある。Anti-Hackerは様々な攻撃パターンをDBとして持ち，例えばWebサーバへのすべてのアクセスを逐一攻撃パターンDBと比較する。パターンが一致し不正アクセスとして判断した場合には，即座にそのセッションを遮断し，Webサーバへはアクセスが行かないようにする（**図6**）。



HTTP：HyperText Transfer Protocol

図6．Anti-Hackerのセッション遮断イメージ ― 攻撃パターンデータベースとマッチするHTTPリクエストは，Webサーバには届かない。

Image of HTTP session blocked by Anti-Hacker

（注9）　FireWall-1は，Check Point Software Technologies Ltd.の商標。

不正パケットが流れていないかを監視する際には，当社では，セキュリティ診断サービスと同様，ISS社の監視ツールRealSecureを主に用いている。セキュリティ監視システム構築支援サービスでは，お客さま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について，お客さまのヒアリング，監視項目のチューニング，お客さま管理者の教育などを実施している。

5　あとがき

当社の情報セキュリティプラットフォームサービスについて述べてきた。紙面の都合で，個々のサービスについては十分に書ききれない面があるのはご了承いただきたい。

今後は更に，お客さまの広範囲なセキュリティに関する要求に応えられ，総合的なセキュリティサービスを提供できるよう，サービス内容の見直しや拡充といった努力を続けていきたい。

文　献

⑴　Internet Security Systems Inc.<http://www.iss.net>,（参照 2002-12-03）.
⑵　吉野恭明，ほか．セキュリティ診断・監視コンサルティングサービス．東芝レビュー．**56**，7，2001，p.38－41.
⑶　能勢健一朗，ほか．PKI構築サービスとPKIカードシステムTARGUSYS$_{TM}$．東芝レビュー．**56**，7，2001，p.34－37.

新藤　清史　SHINDOH Kiyoshi

e-ソリューション社 ネットワークインテグレーション・サービス事業部 営業技術第二担当主務。セキュリティシステムの構築サービス業務を経て，現在は運用管理ソリューションの設計業務に従事。
Network Integration Services Div.

小林　英彦　KOBAYASHI Hidehiko

e-ソリューション社 ネットワークインテグレーション・サービス事業部 営業技術第二担当主務。セキュリティ診断・監視サービスの開発業務に従事。
Network Integration Services Div.