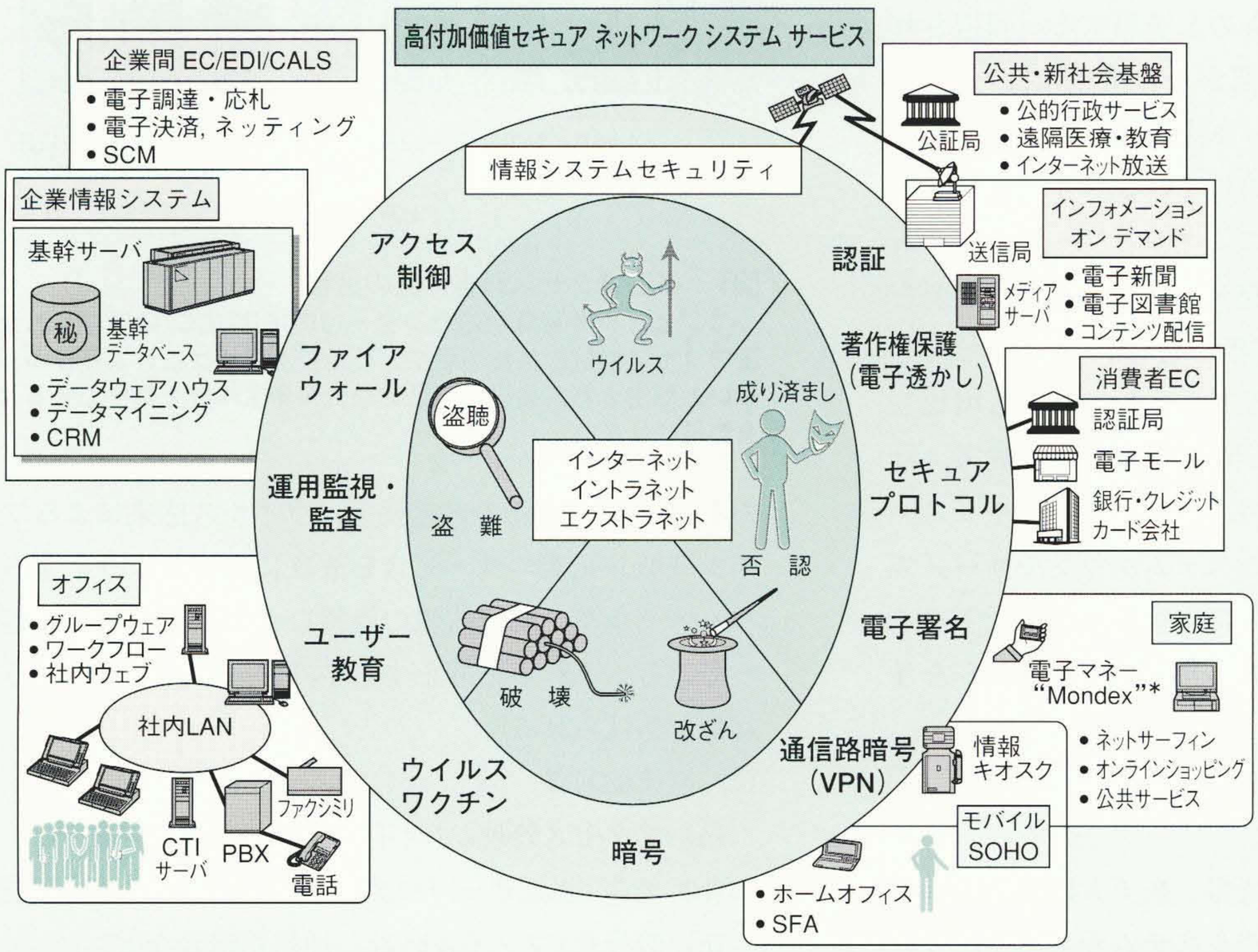
# トータルな情報システムセキュリティを提案する製品・サービス体系“Secureplaza”

## Hitachi's Products and Services Framework for Providing Total Information System Security

金野千里　*Chisato Konno*　角田光弘　*Mitsuhiro Tsunoda*
塩入亮太　*Ryôta Shioiri*　兼子忠彦　*Tadahiko Kaneko*




注：略語説明ほか
EC（Electronic Commerce）
EDI（Electronic Data Interchange）
CALS（Commerce at Light Speed）
SCM（Supply Chain Management）
CRM（Customer Relationship Management）
CTI（Computer-Telephony Integration）
PBX（Private Branch Exchange）
VPN（Virtual Private Network）
SOHO（Small Office, Home Office）
SFA（Sales Force Automation）
＊Mondexは，Mondex International Limitedの登録商標である。

**セキュア ネットワーク コンピューティングのシステムコンセプト**

「企業ー家庭ー社会」がセキュア，シームレス，グローバルなネットワークで接続され，多様な高付加価値サービスが実現されつつある。強固でフレキシブルな情報システムセキュリティ技術が，ネットワークシステムサービスの発展を支えている。

インターネットは急速な進展を遂げており，全世界で4,300万台以上のホストコンピュータが接続され，1億人（国内1,000万人）以上が利用するシステムへと拡大している。「企業ー家庭ー社会」がシームレスなネットワークで接続され，それぞれのユーザーのための適正なシステムサービスが，どこからでも安全に提供される高度情報化社会への展開が期待されている。

そのためには，ネットワークに接続されているシステムやネットワークで配信される情報のセキュリティ（安全性）保証が不可欠であり，接続範囲やシステムサービスの広がりに比例して，その重要性はますます高まっている。盗聴や盗難，成り済まし，改ざん，破壊などの想定される脅威（リスク）に対して，アクセス制御，暗号によるデータ保護，認証などをはじめとする情報システムセキュリティ対策により，高付加価値で安全なネットワーク システム サービスが実現できる。

日立製作所は，このインターネット・イントラネット・エクストラネットの着実な発展を支える，トータルなシステム セキュリティ ソリューション“Secureplaza”を提案している。

## 1　はじめに

イントラネット・インターネットの浸透が，急速に進んでいる。企業システムでは，Webによる情報共有・情報発信から始まって，グループウェア，DB（Database）アクセス，既存の基幹システムの情報処理と連携した意思決定支援やデータウェアハウス，顧客へのマスカスタマイゼーションサービスなど，業務革新につながる幅広い応用が展開されつつある[1]。一方，グローバルでシームレスなネットワークシステムには，種々の脅威（リスク）が存在する。このネットワークコンピューティングの拡大は，システム・情報のセキュリティ（安全性）保護が確立されて初めて可能となる。

ここでは，日立製作所が提案している，トータルなシステム セキュリティ ソリューション“Secureplaza”について述べる。

## 2 被害および損失

わが国で報告されている不正アクセス被害の届け出状況の推移を**図1**に示す[2]。このような届け出は急速に増加しており，また実際には，不正侵入されている事実を把握してないユーザーも数多いものと予想する。報道されているものだけでも，組織内部からの情報の持ち出し，個人情報の流出，インターネットを経由した事件や，数億円に及ぶ実被害の報告が増加している。

このような被害と損失について，ネットワーク システムサービスで先行する米国の調査データによると，主要な241組織の被害額合計は，1997年に約1億ドルであったものが，1998年には約1億3,600万ドルと30%以上も増加している[3]。被害は，盗難による情報価値自体の被害，計算機リソースの盗用による被害，ネットワークやシステム破壊に対する修復の被害，システムダウンやサービス障害による業務収益被害，さらに，組織の信用低下やイメージダウンの被害など，組織に複合的なダメージを与えている。

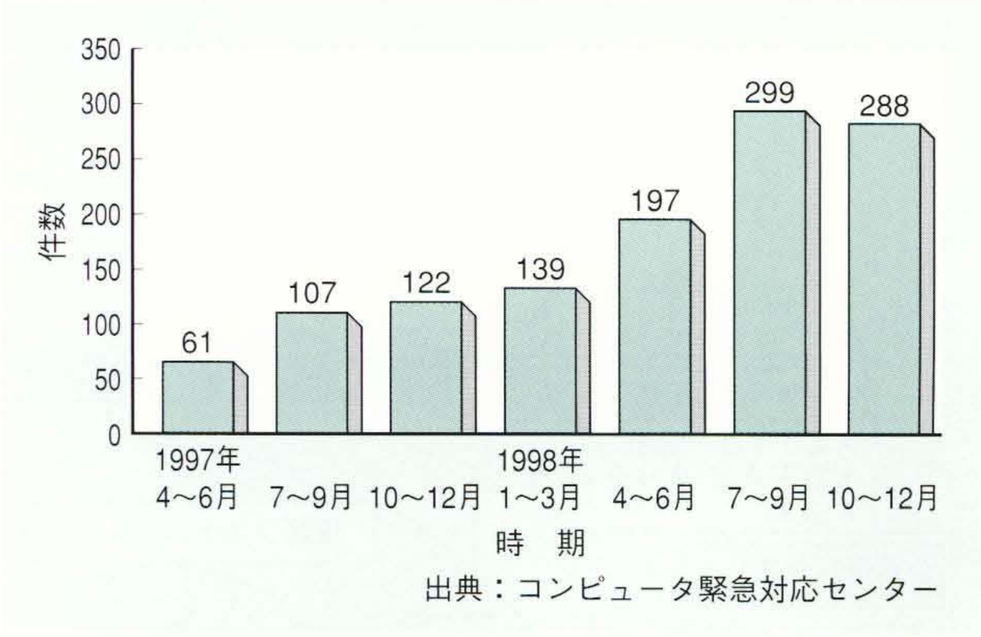



**図1 不正アクセス報告件数の推移**
コンピュータ緊急対応センター(JPCERT/CC)に届けられた不正アクセス件数の推移を示す。ただし，実態はこれよりはるかに多いと想定され，実際の不正アクセス発生件数を類推できるような数値ではない。

## 3 ネットワークシステムでの脅威

ネットワークに接続された情報システムに想定される脅威としては，システム内部やシステムからネットワーク経由で配信される情報双方に対する，(1) 盗難，(2) 盗聴，(3) 破壊，(4) 改ざん，(5) 成り済まし，(6) ウイルス，(7) 交信内容否認などがある。実際には，セキュリティホール(セキュリティ上の欠陥)からのシステムへの不正侵入，Webの書き換え，ウイルス感染によるファイル破壊，正規のサービスを故意に妨害しようとするスパムメールや，内部情報の盗難などの被害が頻繁に起こっている。これらを抑止する手段として，以下のような対策があげられる[4]。

(1) 直接的対策
- (a) アクセス管理(ファイアウォールなど)
- (b) 認証(認証サーバやディジタル証明書の利用など)
- (c) 暗号化(ファイル暗号，通信路暗号など)

(2) 間接的対策
- (a) セキュリティ監視，監査
- (b) アンチウイルスプログラム
- (c) セキュリティ教育

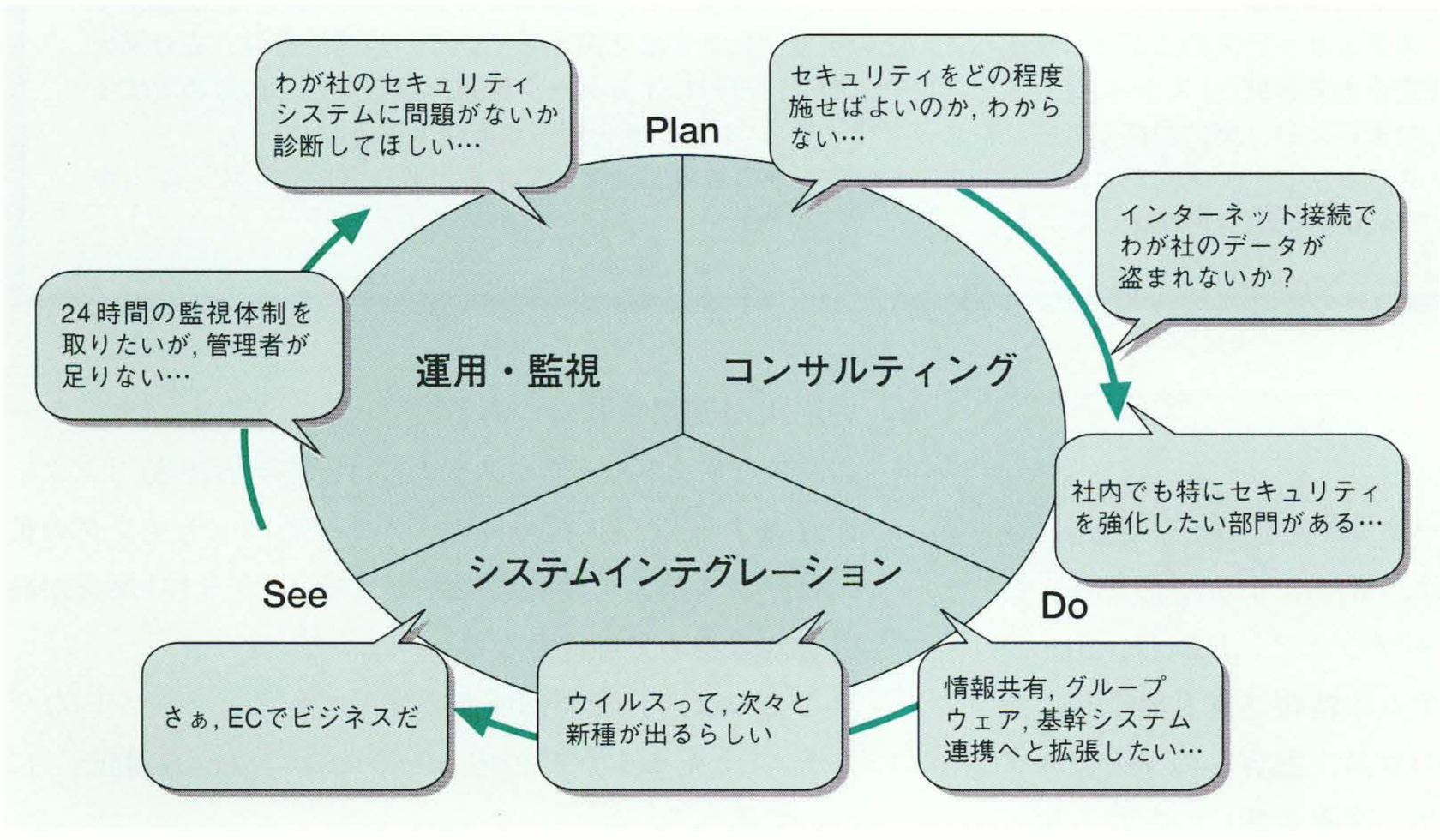



**図2 情報セキュリティに対するユーザーニーズ**
システムのライフサイクルの各フェーズで，セキュリティに対するさまざまな不安およびニーズがある。

## 4 セキュアシステム実現の要件

前章で述べた多様な脅威に対して，一律に強度の高いセキュリティ対策を講ずれば済むというものではない。システムへの投資コストがかかるだけでなく，運用コストや操作性にも影響(操作手順の増加)を与えるからである。実現するそれぞれの情報システムやサービスの中に存在する資産，脅威，想定される被害について評価を行うことにより，適切な対策を選択することが重要となる。

その実現にあたっては，システムのトータルプロセスから見た場合，大別して以下に述べる3段階のフェーズがある。新規のシステム構築だけでなく，既存のシステムやそのネットワークサービスの拡張に際しては，各フェーズごとに多様な要求や不安が生じる(**図2**参照)。これらの諸条件にトータルに対応できるセキュリティ対策が望まれる。

### 4.1 プランニング(Plan)

(1) セキュリティポリシーの策定

セキュリティポリシーとは，「保護する資産の定義」，「だれから守るか」，「脅威の評価」，「セキュリティに対してどれだけのコストを払うか」を抽出，整理し，セキュリティ確保の基本方針を明確化したものである。システムやサービスのセキュリティ対策では，最上流の検討項目である。

(2) セキュリティ診断

すでに構築済みのシステムやサービスに対して，セキュリティホールの診断や侵入(ペネトレーション)テストなどにより，セキュリティの危険度とその対策を抽出するための診断や分析を行う。

### 4.2 構築(Do)

(1) システム設計

セキュリティポリシーとセキュリティ診断に基づいた具体的な対策として，ファイアウォールの設置個所や暗号化(ファイル，通信路)範囲，認証方式，運用方式などの決定を行う。

(2) インテグレーション

設計に従って，製品コンポーネント群を用いることにより，既存システム部分との連携も含めて，セキュリティ機能を実装する。

### 4.3 運用・監視，監査(See)

導入したセキュリティ対策を実現するサーバやソフトウェアの運用にあたっては，運用のノウハウだけでなく，セキュリティ攻撃と不正利用の早期検知を定常的に監視することが重要である。セキュリティ対策は一過性のものではなく，新しいアタック手法やセキュリティホール，ウイルスなどに対して継続的な対応が必要となる。また，システムがあらかじめ定められたポリシーに沿って運用されているかについて，システム，情報，およびユーザーを含めた監査も重要となる。欧米諸国などでは，外部からだけではなく，社内不正などがセキュリティ脅威の上位に位置づけられてきている。

## 5 Secureplazaの製品・サービスの体系

Secureplazaは，セキュリティを実現するハードウェア

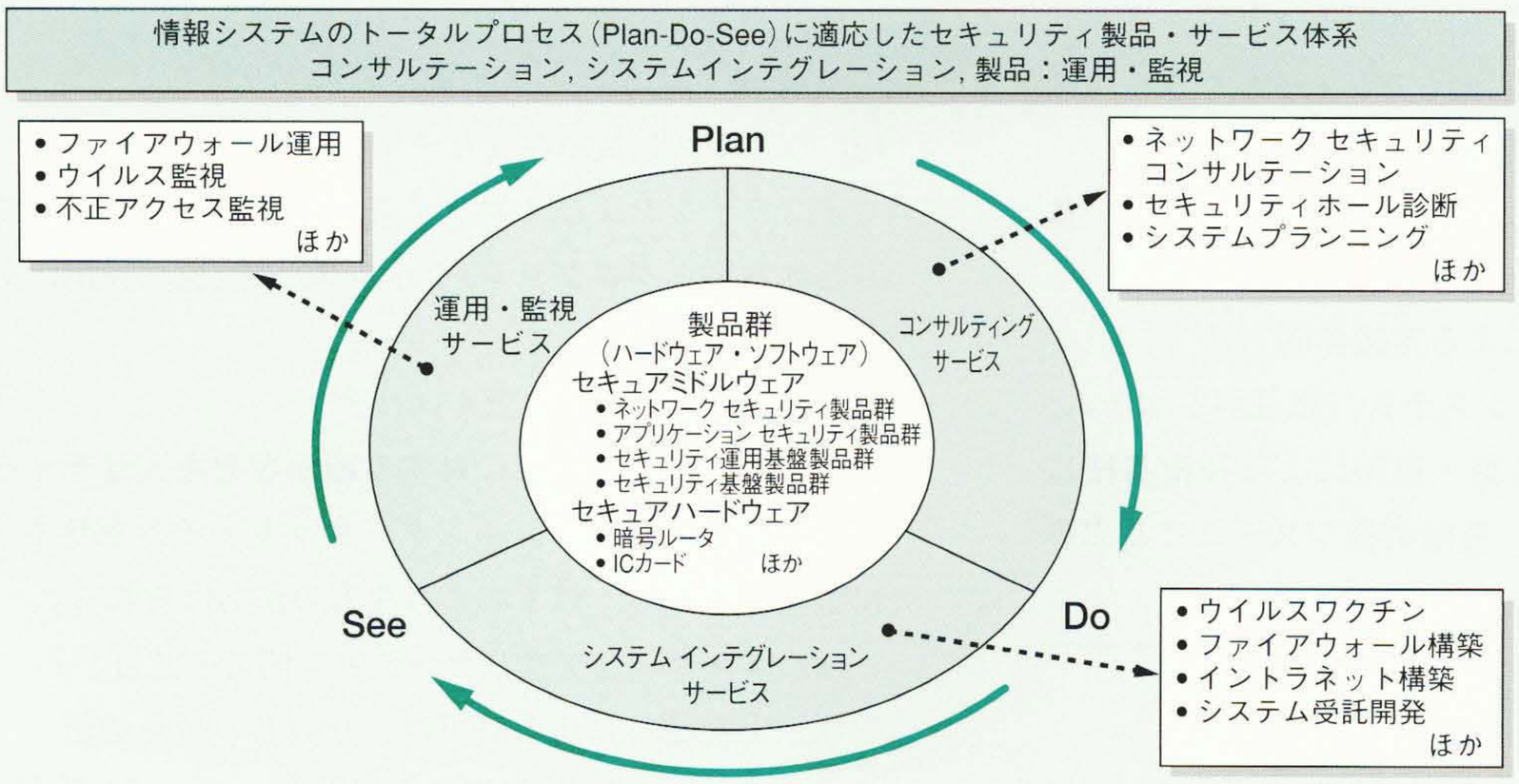
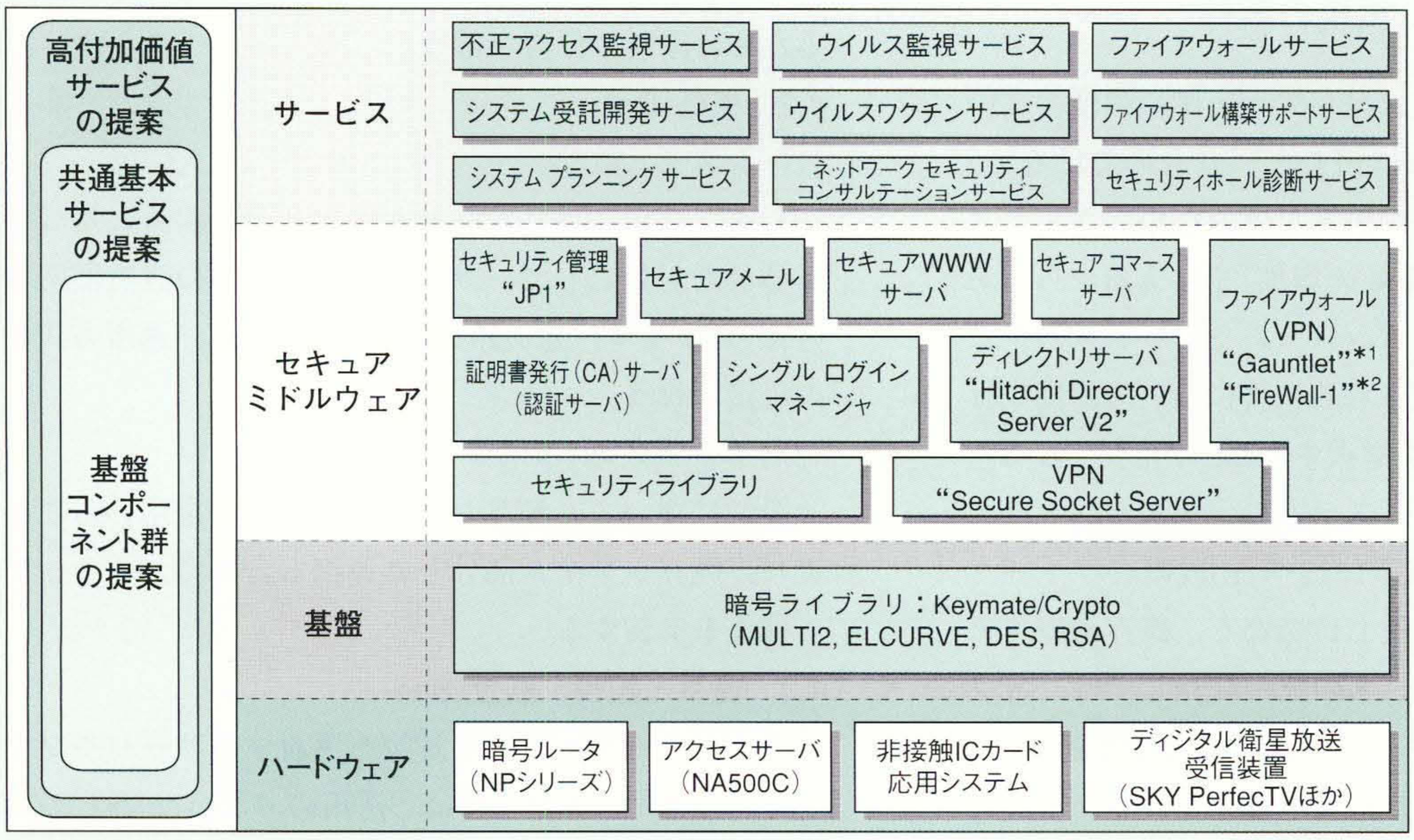



**図3 Secureplazaの体系**
システムのさまざまなライフサイクルでのセキュリティに対する具体的ニーズと，それを受けたSecureplazaの商品体系を示す。




注1：略語説明ほか
WWW(World Wide Web)
VPN(Virtual Private Network)
CA(Certificate Authority)
SECE(Secure Electronic Commerce Environment)
*1 Gauntletは，米国Network Associates,Inc.の商品名称である。
*2 FireWall-1は，CheckPoint Software Technologies, Ltd.の商標である。
注2：□(日立製作所製品)

**図4 Secureplazaを構成する製品・サービス群**
トータルなシステムセキュリティを実現するSecureplazaを構成するハードウェア，ソフトウェア，サービスの階層を示す。

からソフトウェアに至る個々の製品群を核として，それらを活用してセキュアなシステムを設計，構築，運用するためのサービス群で構成されている(**図3**参照)。その階層構造を**図4**に示す。各セキュアシステムは，これらを縦断的に活用することによって実現される。

Secureplazaの特徴について以下に述べる。

(1) Plan－Do－Seeのシステムのライフサイクルと具体的ニーズに対応

(a) コンサルティング：セキュリティポリシーの策定支援，セキュリティ診断サービス

(b) システムインテグレーション：ファイアウォール，認証サーバ，暗号などを活用したセキュアシステムの設計と構築支援

(c) 運用・監視：日立製作所の運用センタで，ユーザーシステムの運用代行，ファイアウォールやウイルス監視サーバの24時間の監視代行

(2) ハードウェア・ソフトウェア・サービスの三位一体のトータルサポート

(3) セキュリティの専門家による支援体制

先行システム(電子商取引システム，認証局システム，エクストラネットなど)の構築・運用による技術蓄積に裏付けられたネットワーク，各種業種システムに及ぶ専門技術者による支援体制

## 6 Secureplazaのセキュリティサービス

Secureplazaを構成するサービス(**図5**参照)について以下に述べる(ハードウェア・ソフトウェア技術と製品については本特集の別論文参照)。

### 6.1 サービス体系

Secureplazaのサービスは，セキュリティの対策対象で区分した以下の三つのサービス群から成る。各サービスは，システムの各ライフサイクルに応じたサービスメニューで構成する。

(1) ネットワークセキュリティ

等価なサービスが提供されるネットワークの接続範囲への不正侵入を抑止する。具体的には，インターネット・イントラネット利用環境下での，以下の制御などがあげられる。

(a) インターネットなどの外部からのアクセス制御

(b) セキュリティポリシーの異なる，別サイト(管理領域)からのアクセス制御

(2) ウイルス対策セキュリティ

オンラインおよびオフラインで持ち込まれたり，持ち出される不正プログラム(ウイルス)の監視，検出，対策を実施する。

(3) アプリケーションセキュリティ

サイト内のリソースに対する細かなセキュリティを実現する。具体的には，インターネット・イントラネット利用環境下での，以下のようなものがあげられる。

(a) ユーザーとアプリケーション間での認証

(b) 上記認証による許可ユーザーとの暗号通信

(c) ファイルの保護(アクセス制御，ファイル暗号)

## 6.2 サービスメニュー

システムの各ライフサイクルの側面から，代表的なサービスメニューについて以下に述べる。

### 6.2.1 プランニングサービス

(1) ネットワークセキュリティ コンサルテーション

脅威分析，要件整理，およびセキュリティポリシー設計に基づいて，基本仕様を提案するサービスである〔**図6**(a)参照〕。典型的な企業情報システムを例として，中核的なセキュリティポリシー設計の概要フローを以下にあげる。

(a) ステップ1：守るべき情報などの特定とその重要度の決定(情報種類，格納場所，機密度レベルなど)

(b) ステップ2：システムと情報などへアクセスできるユーザーの明確化など(社外，社内階層，部門，職位など)

(c) ステップ3：個々の情報とシステム機能などへのユーザー権限の確定(読取り，書込み，実行，削除，アクセス権の変更などへのシステム権限範囲と権限者の確定)

(d) ステップ4：守るべき情報とシステム機能などへのネットワーク上の脅威の特定

(e) ステップ5：脅威によるダメージ範囲の特定と，セキュリティ対策の策定

最後に，企業は，上記のステップを経て策定したセキュリティポリシーをトップポリシーとして決定し，これを順守していくことになる。

(2) セキュリティホール診断サービス

グローバルなIP(Internet Protocol) アドレスを持つマシン〔ファイアウォール，WWW，DNS(Domain Name System)，メールサーバなど〕に対して，インターネット経由で，セキュリティホールの修復検証やパスワード設定，パケット盗聴，改ざんなどの診断を行う。

### 6.2.2 構築サービス

セキュリティポリシーやセキュリティ診断結果に基づいて，セキュアシステムの設計，構築を実施するサービスである。典型的な設計手順の概要について以下に述べる。

まず，セキュリティポリシーに基づいて，サービス内容，サービス利用の方向，利用者と関与者の集合関係などを明確化し，システム設計を行う。

(1) ベースアーキテクチャの設計

(a) ネットワーク構成

(b) サイト(管理領域)の確定，サイトを越えた通信方式

(c) サービスに対応した通信路暗号化範囲の設定と，実現方式

(2) 認証方式の設計

(a) 通信相手サイトの認証方式

(b) 利用者の認証方式

(3) 運用・管理方式の設計

このような汎用的な対応に加え，目的の明確な個別ニーズに対しては，ファイアウォール構築サポート，認証システム構築サポート，VPN(Virtual Private Network)構築サポート，ウイルス ワクチン サービスなどを用意している。

### 6.2.3 運用・監視サービス

システムの運用・監視が，導入したセキュリティの水準を維持していくうえで重要な要素であることは2章で述べた。しかし実際には，運用要員の確保や技術獲得への対応，24時間の監視体制などの課題がある。これらにこたえるために，日立製作所は，システム運用やセキュリティ監視のユーザーの負荷軽減を目的として，「日立Compassportセンタ」で，サーバの運用・監視などの各種

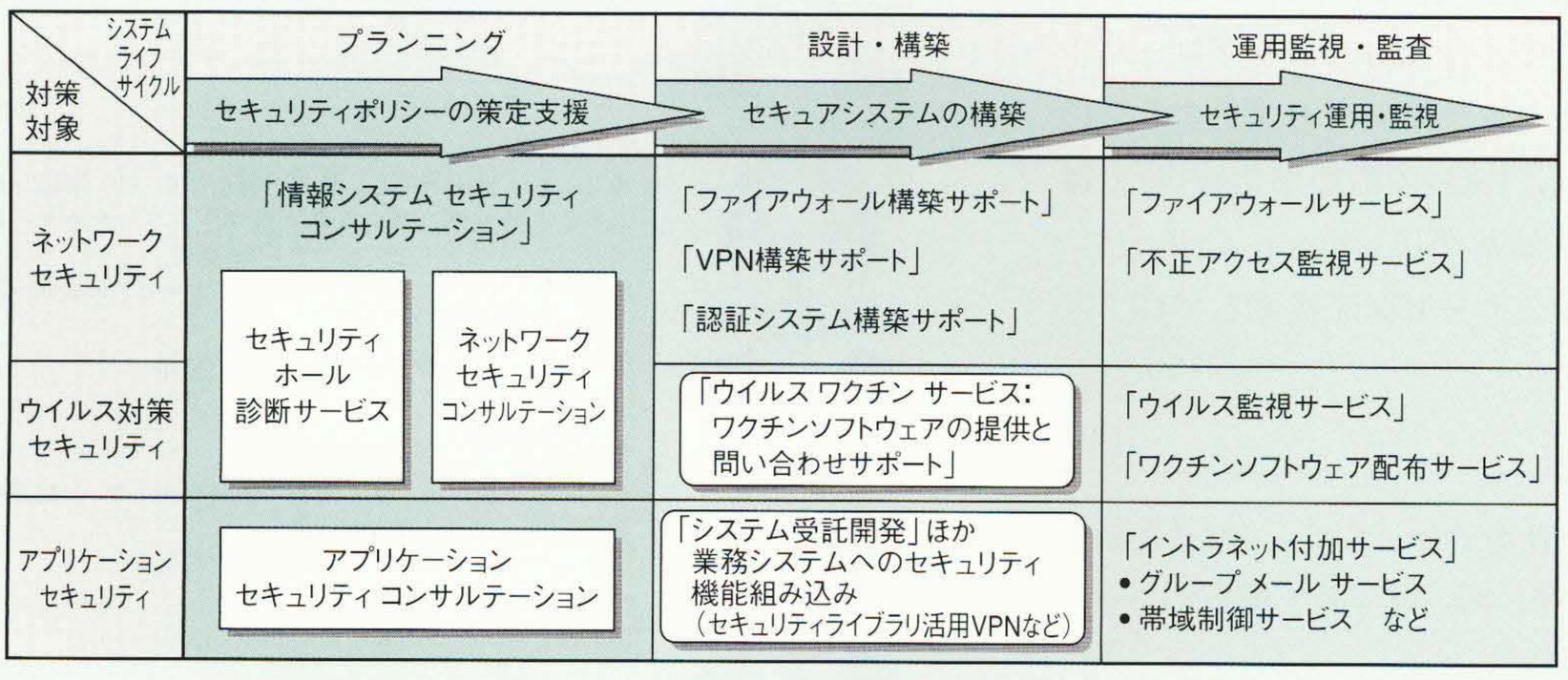



**図5 Secureplazaのサービス体系**

システムライフサイクルの上流から下流まで，各システムのセキュリティ対策をそろえるSecureplazaのセキュリティサービス体系を示す。

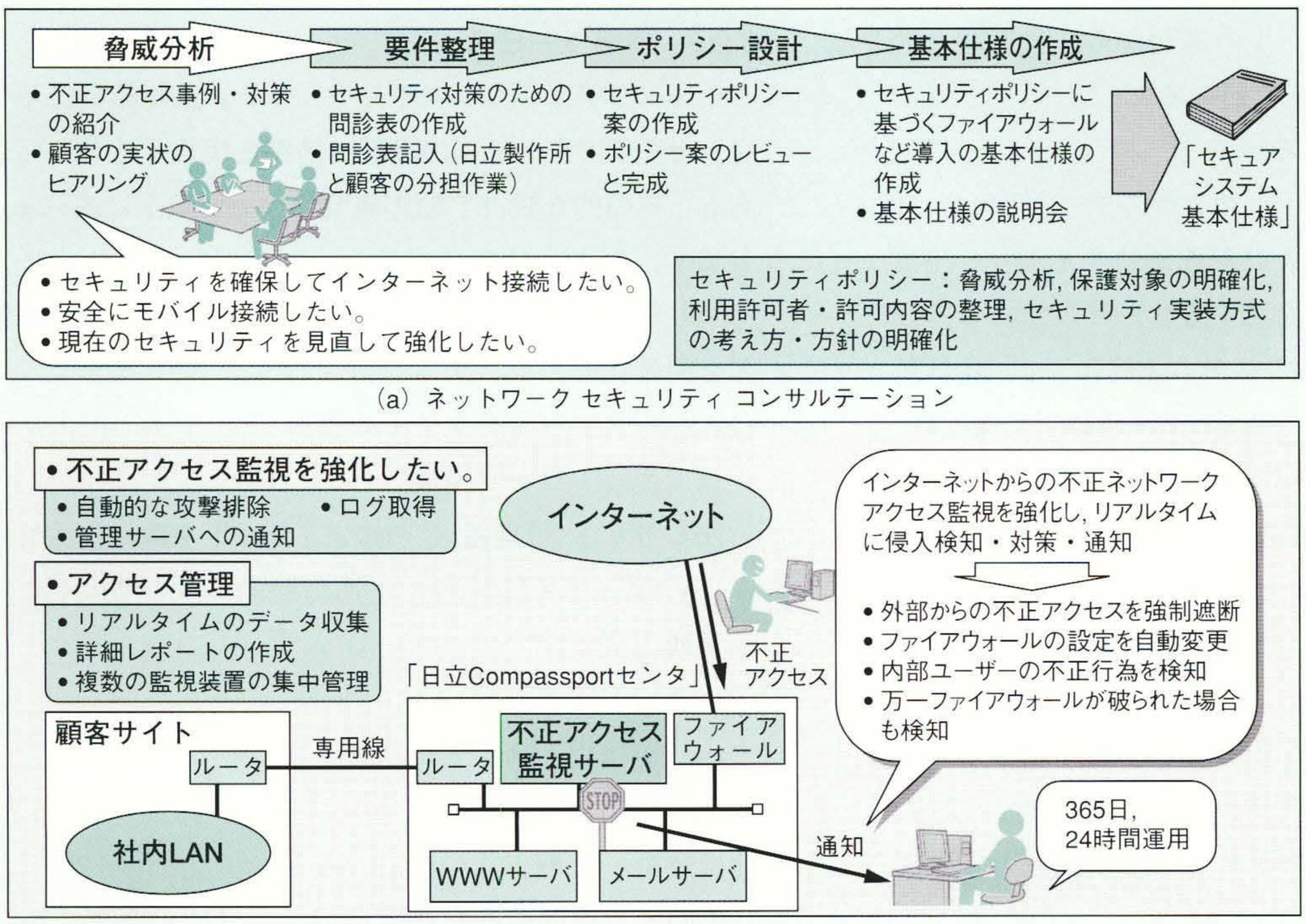



**図6 セキュリティサービスの具体例**

顧客のもとでのコンサルテーション, 顧客に代わって行うアウトソーシングサービスなど, Secureplazaでは各種のサービスメニューを用意している。

代行・アウトソーシングサービスを用意している。不正アクセス監視サービスのサービスイメージを**図6**(b)に示す。

## 7 おわりに

ここでは, イントラネット・インターネットシステムの急速な発展に不可欠な基盤である情報システムセキュリティに対して, システムの上流から下流に至るトータルなセキュリティを実現する製品・サービス体系“Secureplaza”について述べた。

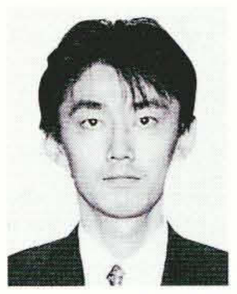
企業での情報共有・情報発信や業務間連携による業務革新, 家庭への新しいメディア配給インフラストラクチャー, 社会での流通・金融・行政ネットワークサービスなどの実現と充実を目指して, 今後も, よりグローバルでシームレスなトータル セキュリティ ソリューションの開発を進めていく。さらに, ISO(国際標準化機構)で標準化されるセキュリティ評価基準(Common Criteria)[5]に準拠した製品群や対応するサービスを提案していく考えである。

### 参考文献など

1) 大島, 外：日立製作所が目指すネットワーク時代の新しい情報システム, 日立評論, **80**, 5, 386～390(平10-5)
2) http：//www.jpcert.or.jp/
3) CSI/FBI：Computer Crime Survey, 1998
4) 佐々木, 外：インターネットセキュリティ, オーム社(1996)
5) http：//csrc.nist.gov/cc/ccv20/ccv2list.htm

### 執筆者紹介

**金野千里**
1977年日立製作所入社, 情報・通信グループ 新事業推進センタ セキュリティ事業推進室 所属
現在, セキュリティ関連製品の企画に従事
理学博士
情報処理学会会員, 日本応用数理学会会員
E-mail：c-konno @ comp. hitachi. co. jp



**塩入亮太**
1992年日立製作所入社, 情報・通信グループ 新事業推進センタ セキュリティ事業推進室 所属
現在, セキュリティ関連製品の企画に従事
E-mail：r-shioiri @ comp. hitachi. co. jp

**角田光弘**
1987年日立製作所入社, 情報・通信グループ 情報システム事業本部 情報システム事業部 ネットワーク&サービス本部 ネットワークビジネス企画部 所属
現在, セキュリティ ソリューション サービスの企画・開発に従事
E-mail：tsunoda @ system. hitachi. co. jp

**兼子忠彦**
1970年日立製作所入社, 情報・通信グループ 公共情報事業部 官公システム第3部 所属
現在, 官公庁情報システムのSE業務に従事
情報処理学会会員
E-mail：t-kaneko @ jkk. hitachi. co. jp