「e社会」の進展に向けたセキュリティ

松井　一成　　芦田　元之

インターネットは，21世紀の世界を支える社会的インフラとして，経済，社会，生活，文化などの様々な社会活動の発展の原動力となり，これからの企業活動，個人の生活，社会活動，価値のあり方に大きな変革をもたらすことが期待されている。しかし，インターネットは，オープンなシステムであるが故に，外部からの不正侵入や情報の漏洩などが比較的容易であり，多様で複雑なリスクが存在する。健全なネットワーク社会を築くためには，インターネットにおけるセキュリティ対策が重要な時代となってきた。本稿では，21世紀へ向けてのセキュリティ対策と当社の取組みについて述べる。

「e社会」の脆弱性

情報通信技術の発展は，我々の社会生活を根本的に変えつつある。従来の人，物，金を中心とした社会構造が，情報および通信自体が価値を持つ構造へと変化し始めている。電気，ガス，水道といったライフラインに加え，ネットワークが新たなライフラインになり，さまざまな社会活動がネットワークの存在を前提として行われる「e社会」が形成されつつある。

行政も，「e社会」へ向けて，IT革命の掛声の下に，EC（電子通商）基盤整備，電子政府の実現，教育の情報化，個人情報･セキュリティ確保の環境整備，インターネット利用促進等の政策を強力に推し進めている。「e社会」の健全な発展のためには，社会的基盤であるネットワークに対する情報セキュリティシステムの充実が必須である。ネットワーク化した「e社会」の社会経済活動の範囲は，日本国内にとどまらず，世界へと広がるグローバル化へと進展している。同時に情報セキュリティに対する脅威も，同様に世界規模に及ぶことになる。

従来の社会構造では，セキュリティ対策とは人，物，金を保護することであったが，「e社会」では，情報そのものの価値を重視し，情報の保護を成功のキーとしている。

「e社会」におけるセキュリティ対策を，以下の3つの視点から検討する。

(1) インターネット利用者の拡大

インターネットの利用者数は，1998年から急激に伸びている。携帯電話のiモードのインターネット利用拡大などにより，2000年以降も更に普及が進むことが予想されている。利用者の拡大に伴い，個人情報の漏洩やプライバシーの侵害などの脅威が考えられる。

(2) ネットワーク端末の多様化

インターネットに接続可能な携帯端末，ゲーム機やデジタル家電などが普及し，コンビニキオスク端末のようなインターネットを利用した販売インフラも普及する。これらの端末で扱われるカードなどの利用者情報の保護やサービス妨害に対するセキュリティ対策の強化が必要になる。

(3) インターネットサービスの多様化

ソフトウェアやゲーム，ビデオ，書籍等のコンテンツの流通サービスのような新たなサービスの提供が増加する。コンテンツ流通では，不正コピー，著作権侵害に対する対策が必要になる。

「e社会」におけるセキュリティ脅威の具体例を以下に示す（図1参照）。

・不正侵入―システムへのアクセスを許されていない者が，データ破壊や情報の入手などの悪意を持って不正にシステムにアクセスすること

・盗聴―ネットワークやシステム上のデータを第3者が不当に盗んだり，盗聴すること

・改ざん―ネットワークやシステム上のデータを第3者が不当に改ざん，消去すること

・サービス妨害―同時に多数の不正アクセスを集中させるなどにより，システムの正常な動作やサービスを妨害すること

・なりすまし―他人になりすましシステムに不正にアクセスすること

・内部者による脅威―従業員等の社内関係者が社内システムに不正アクセスを行い，システムの動作妨害や情報を盗むこと。顧客情報の流出等がこれに当る。

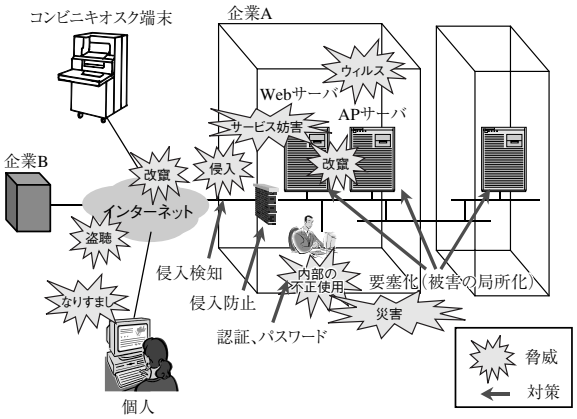


図1　情報セキュリティ脅威

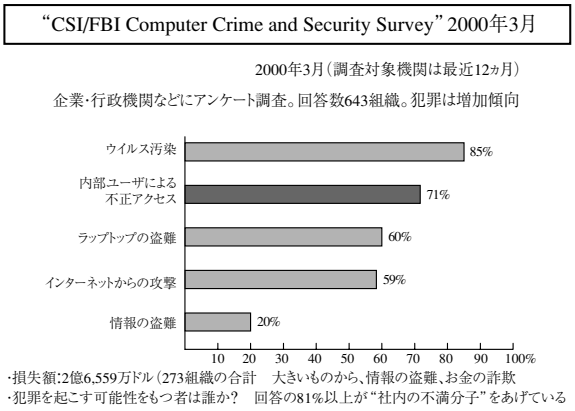


図2　米国の情報セキュリティの現状

セキュリティ先進国である米国におけるこれらの脅威の現状を図2に示す。コンピュータ犯罪は，インターネットの普及に比例して増加している。特に，回答社の71%が内部ユーザによる不正アクセスの被害があり，内部犯罪の防止が企業の重要な課題となっている。

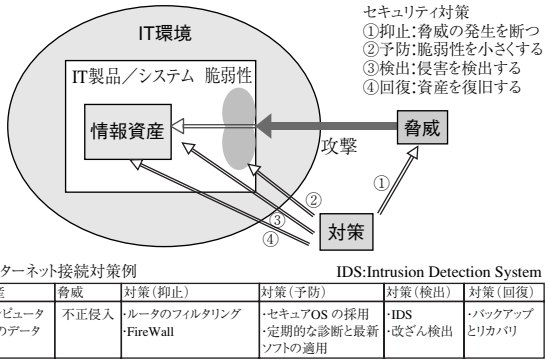
セキュリティ対策のあり方

(1) セキュリティ対策の視点

想定される脅威を分析し，この脅威に対する対策として，抑止，予防，検出および回復の面からの対策を検討する（図3参照）。

抑止は，セキュリティ脅威の発生を断つ対策であり，アクセス制御（ファイアウォール），認証などが抑止対策に該当する。

予防は，コンピュータシステムの脆弱性を低減する対策である。最新のソフトウェアを使用して，できる限り



インターネット接続対策例　　IDS:Intrusion Detection System

資産	脅威	対策（抑止）	対策（予防）	対策（検出）	対策（回復）
コンピュータ上のデータ	不正侵入	・ルータのフィルタリング ・FireWall	・セキュアOSの採用 ・定期的な診断と最新ソフトの適用	・IDS ・改ざん検出	・バックアップとリカバリ

図3　セキュリティ対策の考え方

セキュリティーホールのない状態を保つこと，要塞OSの使用やデータの暗号化が予防対策に該当する。

検出は，加えられた脅威を検知する対策である。不正侵入検知システムや改ざん検出がこれに該当する。

回復は，発生した被害から元の状態に復旧するための対策である。システムの二重化，バックアップ，リストア等がこれに該当する。

(2) セキュリティ保護対策

セキュリティ保護対策としては，セキュリティ管理・評価の対策と技術的対策がある。セキュリティ脅威を分析した上で，セキュリティ管理・評価の対策と技術的対策を連携させ，統合的なセキュリティ保護対策を取ることが重要である。

・セキュリティ管理・評価

セキュリティ管理・評価の対策として，セキュリティポリシー[1] と情報技術セキュリティ評価基準（CC: Common Criteria）[2] がある。

セキュリティポリシーは，企業の経営方針に基づき，どの情報資産を，誰が，何故，どのようにして守るか，を明確に定義した企業の基本方針であり，経営者が全従業員に与える指針である。企業の最優先課題である内部ユーザによる不正アクセスを防ぐために，セキュリティポリシーの従業員への浸透が必須である。米国のほとんどの大企業は，セキュリティポリシーを定めている。日本では，最近，セキュリティポリシーの必要性がようやく認識され始めた段階である。

金融機関では，セキュリティポリシーが金融監督庁の監査項目に加えられている。政府は，2000年8月に「情報セキュリティポリシーに関するガイドライン」を発行し，2000年度末に各省庁のセキュリティポリシーの運用開始を目指している。ISOでは，2000年9月の投票で，英国のセキュリティ対策ガイドBS7799 （Information

Security Management）を国際標準のベースとして検討することが決っている。

情報技術セキュリティ評価基準は，セキュリティ要求仕様書に従って製品/システムが設計され，セキュリティ機能が漏れなく実装されているかを評価するための基準である。情報技術セキュリティ評価基準は，1999年12月にISO化，2000年7月にJIS化された。通産省は，情報技術セキュリティ評価基準を認証するための「セキュリティ評価認証体制」を，2001年度から運営する方針を2000年9月に発表した。2001年度からの電子政府システムの調達に，この認証制度が導入される予定であり，今後のセキュリティ関連の製品･システムの開発に大きな影響を与えることになる。

・セキュリティ技術対策

セキュリティの抑止，予防，検出および回復の視点から脅威分析を行い，コスト，セキュリティ強度および利便性のバランスを考慮した最適な技術的対策を採用しなければならない。セキュリティ技術対策は，図5の情報セキュリティプラットフォーム内の技術である。

沖電気のセキュリティソリューション

「e社会」の発展に伴なって，今後，想定されるセキュリティ脅威と保護対策について述べた。これらの考察を基に，当社では，情報セキュリティシステムのトータルソリューションを情報セキュリティサービス，情報セキュリティプラットフォームの2面から体系化している（図4参照）。

情報セキュリティプラットフォームは，情報セキュリティ技術対策を体系化し，具体的な製品群を示している。高信頼性システム製品群は，沖電気が高い評価を得ているオンライントランザクション処理（OLTP）やデータベースの二重化を含めた高信頼性技術によるシステム構築を示している。

情報セキュリティサービスは，高信頼性システム構築技術と情報セキュリティプラットフォームで示されている製品群を組合わせて，各企業の状況に応じた最適なセキュリティ保護対策を提供するサービスである。セキュリティ対策プロセスの診断，脅威分析，設計構築，運用の4つのプロセスに対応したセキュリティレビュー，コンサルティング，システ構築，運用支援／ハウジングの各サービスからなる。

次世代侵入検知システム[3] EMERALD，要塞OSであるVirtualVault，電子透かし[4]，虹彩技術による個人認証システムのアイリス，およびSET プロトコルを実現しているInfomerceは，「e社会」を支えるセキュリティ対策技術として特に期待されている。ここでは，最高レベルのDMZ（De-Militarized Zone）を構築するためのキーとなるEMERALDとVirtualVaultの概要を述べる。

EMERALDは，既に知られている不正アクセスをパターン化して検知する従来の方法に加えて,確率推論手法による未知の不正アクセスの検知を可能にしているのが特徴である。

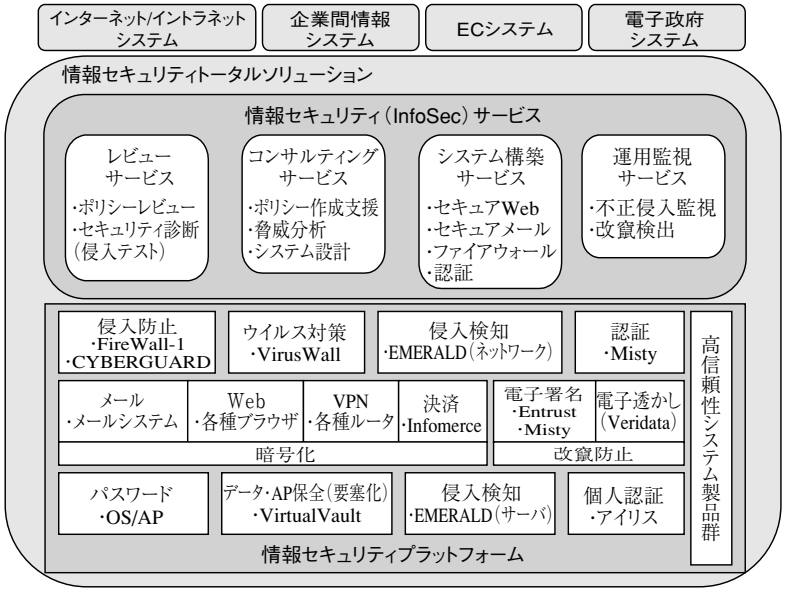


図4　情報セキュリティソリューション体系

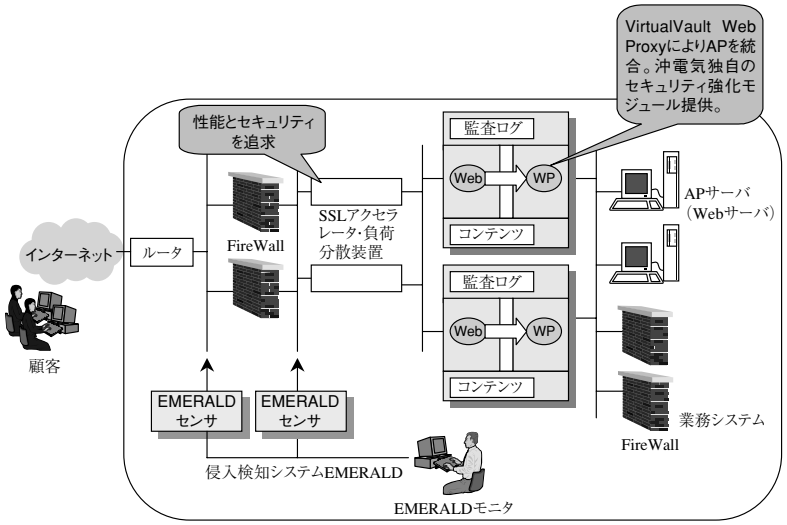


図5　システム構築例

VirtualVaultは，米国国防省のセキュリティレベルを規定しているオレンジブックのBレベル相当のセキュアなOSを採用した高信頼性要塞化Webサーバプラットフォームである。通常のOSでは，特権ユーザにすべての権限が集中し，プログラム間で自由に通信ができるため，セキュリティホールなどを利用して侵入され，特権ユーザの権利を奪われると，あらゆる操作を許すことになる。侵入者は，プログラム間通信を利用して内部のサーバにまで被害を及ぼすことができる。VirtualVaultは，これらの攻撃を防ぐため，特権の細分化によるリスク分散，外部プログラムからのコンテンツのアクセス禁止，プログラム間通信は認証されたプログラムに限定するなどのセキュリティ機能を強化している。また，VirtualVault WebProxyを使うことにより，既存のWebサーバおよび各種Webサーバのセキュリティを強化できる。このVirtualVault WebProxyは，バッファーオーバフローや不正スクリプトの実行を遮断する当社独自の機能強化が行われている。

方式	ファイアウォール	要塞Webサーバ（Virtual Vault）	侵入検知
対策分類	抑止対策（不正プロトコル遮断）	予防対策（脆弱性を小さくする）	検出対策（検出後の遮断機能有）
対象	ネットワーク全体	WWWサーバ	ネットワーク全体
遮断方式	・アドレスとプロトコルによるフィルタリング ・静的設定	—	・アドレス ・TCPセッション切断 ・動的設定
遮断の目的	未然防止	—	事後の被害拡散防止
サービス妨害攻撃	一部の攻撃には対応	—	有効（検出）

図6　装置の役割分担

eビジネスにおけるWebサーバは，外部に情報公開するとともに，内部の業務系システムとも連携する必要があり，特にセキュリティの強化が必要である。当社は，EMERALD，VirtualVault，ファイアウォールおよびルータをインテグレートして，最高レベルのセキュリティ機能および性能を持つWebシステムを提供している（図5参照）。ファイアウォール[5]とVirtualVaultは，高可用性および高信頼性を保つために二重化を行っている。負荷分散装置は，Webサーバの負荷分散と128ビットSSL暗号化のアクセラレータの機能を有している。図6に各装置の役割を示す。

100%のセキュリティ対策は，ありえない。一つの対策に依存するのは危険であり，万が一を想定して，複数の対策によるリスク軽減が必要である。

EMERALDについては，現在は，Sun上で動くが，今後は，他のプラットフォームでの展開を考えている。VirtualVaultについては，ウエブトランザクションWebLogicとの連携を検討している。

セキュリティシステムの運用を行うためには，高い知識とノウハウが必要であり，ユーザ自身が運用を行うのは無理であり，侵入検知システムやVirtualVaultの運用監視サービスを提供している。今後は，ウイルスやファイアウォールの運用監視および，万が一不正アクセスにより損害を被ったときのためのセキュリティ保険を含めた総合セキュリティ運用監視サービスの検討を行っている。 ◆◆

■参考文献

1）武内，他：セキュリティポリシー，沖電気研究開発第183号
2）山本，他：情報セキュリティ国際標準化動向，沖電気研究開発第183号
3）武内，他：侵入検知システム，沖電気研究開発第183号
4）須藤，他：改ざん検出可能な電子透かし，沖電気研究開発第183号
5）橘：高可用性ファイアウォール，沖電気研究開発第183号

●筆者紹介

松井一成：Kazushige Matsui.システムソリューションカンパニー ビジネスソリューション事業部長
芦田元之： Asanobu Ashida.システムソリューションカンパニー ビジネスソリューション事業部 情報セキュリティ担当部長