情報セキュリティ動向と対策

芦田　元之　　矢野　達朗

インターネットをベースとした近年の情報通信技術の発展は，経済，社会，生活，文化などのさまざまな社会活動の発展の原動力となっているだけでなく，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している。従来の人，物，金を中心とした社会構造から情報および通信自体が価値を持つ構造へと変革しており，ネットワークが新たな社会インフラとなってきている。ネットワーク化の進展は，オープン技術であるインターネットが中心であり，外部からの不正侵入や情報漏えいなどのコンピュータ犯罪が生まれ，大きな社会問題となっている。

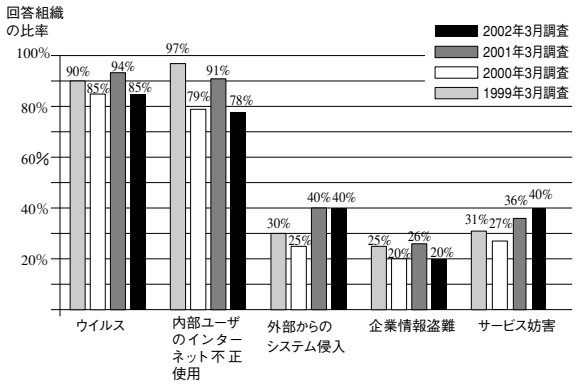
ブロードバンド化と常時接続，無線LANを利用したリモートアクセスなど利用形態の進展につれて，新たなコンピュータ犯罪やプライバシー保護の問題がクローズアップされてきている。

社会インフラであるネットワークの安全性と信頼性を確保するためには，コンピュータ犯罪に対する的確なセキュリティ対策が必須であり，それは企業の自己責任でもある。

コンピュータ犯罪動向

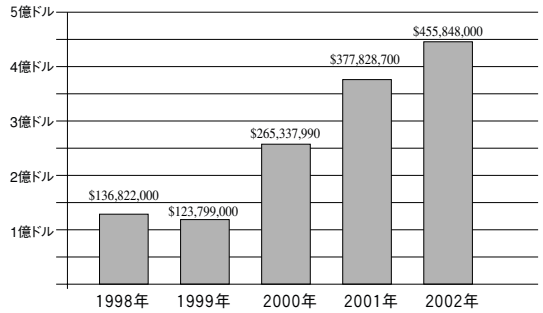
2001年は，コードレッド事件やNimda事件で多くの企業が，不正アクセスによる被害を受けた年である。図1は，CSI（コンピュータセキュリティ研究所）/FBIによるコンピュータ犯罪とセキュリティに関する調査報告（2002年3月）の不正アクセス動向を示している。調査は，企業・行政・研究機関などにアンケート調査を行い，回答者の被害を受けた割合を示している．2002年の回答者数は，455組織である。2001年は484，2000年は583，1999年は460組織である。

2002年調査の特徴は，いくつかの分野で，被害を受けた組織が減少していることである。ウイルス汚染は，94%から85%に減少している。これは，組織内のウイルス対策が，効果を上げているからであると考えられる。内部ユーザによるインターネットの不正利用が減少しているのは，セキュリティポリシーの浸透や不正利用の監視体



”CSI/FBI Computer Crime and Security Survey”2000/2001/2002年3月（調査対象期間は最近12ヵ月）

図1　情報セキュリティに関する調査報告（米国）



2002年の調査では、回答者の80%が経済的損失を認識しているが、被害額を出したのはその44%である。

出典　CSI/FBI 2002 Computer Crime and Security Survey

図2　コンピュータ犯罪による回答機関の被害額

制の効果が出始めているからであると思われる。逆に2001年に多くの有名企業が被害を受けたサービス妨害は増加している。全体的には，内部犯罪は減少傾向であるが，外部からの攻撃は以前にまして激増している（図3参照）。図2は，図1と同じCSI/FBIの報告書にある回答組織のコンピュータ犯罪による経済的被害額を示している。アンケートに回答した組織の85%が，コンピュータ犯罪により金銭的被害を受けたことを認識しており，44%の組織は，被害額を見積もっている。2002年の被害額は，約4.6

億ドルで，20%以上の高い伸びを示している。特に額の多いのは，企業情報の盗難（2002年約1.7億ドル）である。サービス妨害による被害額（2002年約1.2億ドル）も次いで多いと報告されている。この被害額は，この調査のアンケートに回答した組織の総計であり，全米での被害額は非常に大きい額になる。

図3は，CERT/CC（米国コンピュータ緊急対応センタ），JPCERT/CC（日本コンピュータ緊急対応センタ）に対する不正アクセス届出状況の推移を示している。この数値は，JPCERT/CCが受け付けた届出件数であり，実際の不正アクセスを示しているものではない。2000年は，官公庁のホームページ改ざん事件をきっかけに，不正アクセスは，爆発的に増えている。2001年は，中国ハッカー集団による無差別攻撃事件，Sadmind/IIS，CodeRed，Nimdaなど既知のセキュリティホールを悪用したワームの出現により，爆発的に増加した2000年をさらに上回る最悪の状況を示している。

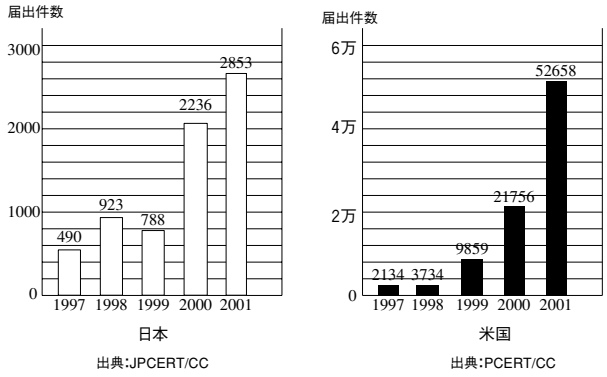


図3　不正アクセス発見届け出状況

不正アクセスの方法は，常に進化している。昨年度の特徴は，今までに知られている攻撃方法を，巧妙に複合化していることである。CodeRedの数ヵ月後に出現したNimdaは，CodeRedと同じセキュリティホールを利用したものである。常に新しいバージョンを導入，警告の出されたパッチの手当て，設定の見直しなどの対策を怠らなければ，多くの場合，被害を未然に防ぐことができたはずである。米国の調査会社であるガートナーグループは，2005年までに起きるサイバー攻撃のうち90%は，パッチなどが提供されている既知のセキュリティホールを利用したもので，20%の企業がコンピュータ犯罪の被害を受ける。被害回復に要するコストは，セキュリティ対策コストの1.5倍になると予測している。したがって，システムにインストールされているOSやアプリケーションに関するセキュリティ情報の収集，この情報に基づくセキュリティパッチの適用といった常日頃のシステム管理が，セキュリティ対策に必須である。

セキュリティ意識

2002年2月に米国の調査会社Harris Interactive社が，企業の個人情報取扱いに関する米国の消費者の意識調査を発表している。消費者の最大の関心事トップスリーは，「企業が無断で個人情報を他社に流すこと」（75%），「オンライントランザクションの安全性」（70%），「ハッカーによる個人情報の盗難」（69%）である。基本的に，米国の消費者は，企業の個人情報の取扱いを信用していないが，企業がプライバシーポリシーを明確にし，企業のプライバシーポリシーに遵守して運用しているかについて第三者監査を行うのであれば，信用できると回答している。また，第三者によるこの監査は，企業の義務であると考えている。

日本での同様の調査報告はないが，個人・企業ともに個人情報の取扱いを含めたセキュリティについての意識が希薄である。個人情報流失については，毎日のように新聞紙上をにぎわしていることが，セキュリティに対する希薄さを如実に示している。また，法規制による情報保護が不十分であり，処罰があまりにも軽すぎることも一因になっていると考えられる。企業のセキュリティ対策不足による被害は，企業の信用・信頼が失墜するだけでなく，消費者自身も被害にあうことを，消費者自身も認識しなければならない。

法規制と企業責任

2000年1月の官公庁のホームページ改ざん事件をきっかけに，コンピュータ犯罪に対する法規制の整備・強化が進められている。

- 「不正アクセス行為の禁止等に関する法律」
  （2000年2月施行）
- 「情報セキュリティに関するガイドライン」
  （2000年7月施行）
  各省庁のセキュリティポリシー作成と侵入検知システム装備の義務化
- 「犯罪捜査のための通信傍受に関する法律」
  （2000年8月施行）
- 「個人情報保護基本法制に関する大綱」
  （2000年10月施行）
  個人情報保護法については，国会で継続審議
- 「IT書面一括法（書面の交付等に関する情報通信技術の利用のための関係法律の整備に関する法律）」
  （2001年4月施行）

- 「支払用カードの偽造等の犯罪に関する刑法改正」（2001年7月施行）
- 「電子契約法（電子消費者契約および電子承諾通知に関する民法の特例に関する法律）」（2001年12月施行）

コンピュータ犯罪に関する法規制の特徴は，犯罪を犯したものに対する罰則を決めているだけでなく，企業に対する管理対策を義務化していることである。すなわち，情報セキュリティ対策は，企業の自己責任なのである。実際に企業がコンピュータ犯罪を被れば，被害が甚大になることを認識しなければならない。具体的には，以下のような被害が生じる。

●サービス妨害	ビジネス機会の損失
●ホームページ改ざん	企業イメージの失墜
●踏み台	企業信用の失墜
	被害者からのクレーム
●システムの停止	サービスの停止
	ビジネス機会の損失
●システムの復旧	コスト増加
●個人情報流失	企業信用の失墜
	被害者からの訴訟
	関連機関への説明責任

図2に示しているように，コンピュータ犯罪による被害額は年々増加している。これらの被害によるコストを考えると，セキュリティポリシーに基づくセキュリティ対策にかかるコストのほうが遥かに少ないと言える。
セキュリティ対策は，企業にとって必須の保険と認識すべきである。すでに述べたように，セキュリティポリシーに基づくセキュリティ対策を遵守して運用している企業は，消費者の信頼を獲得することにもなる。セキュリティポリシーに基づくセキュリティ対策を遵守して運用していることを証明するために，日本情報処理開発協会が行っている「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」を利用する方法がある。

セキュリティ対策

一般にシステムを構築するときは，システム設計を行い，この設計にしたがってシステムを構築して終わらせる場合が多い。セキュリティが要求されるシステムでも，ファイアウォールを導入すれば十分と考え，従来と同じ工程でシステム構築する企業が大多数である。しかし，最近の不正アクセスのほとんどは，ファイアウォールをすり抜けて，被害をもたらしている。セキュリティを必要とするシステムでは，現状を診断，分析し，さらに改善していくライフサイクルが重要である。図4にセキュリティ対策プロセスを示す。

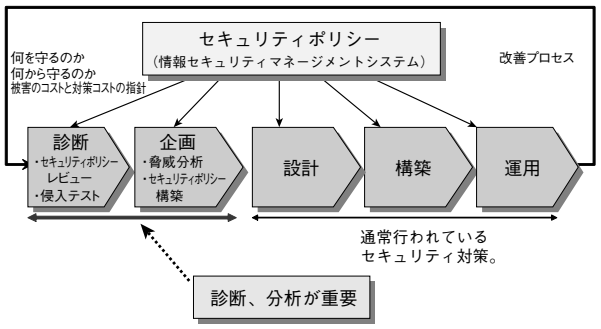


図4　セキュリティ対策プロセス

セキュリティポリシーは，企業の情報資産保護の必要性・考え方・基本方針であり，セキュリティに対する企業の指針である。各種の規定類は，セキュリティポリシーとの整合が必要になる。セキュリティが求められるシステムは，このセキュリティポリシーに準拠して開発しなければならない。

診断フェーズは，セキュリティレビューと呼ばれており，システムの運用がセキュリティポリシーにしたがって行われているかのレビューを行う。また，システムへの侵入テストを行いシステムに脆弱性がないかもチェックする。

企画フェーズは，セキュリティレビューに基づき，セキュリティポリシーや運用規定を見直す。また，脅威分析を行い，セキュリティ要件を洗い出す。システムは，このセキュリティ用件にしたがって，設計・構築・運用を行う。図5は，外部要因によるセキュリティ脅威に対するセキュリティ対策の具体例である。セキュリティ対策プロセスの重要なことは，システムの運用後，さらに診断フェーズに戻り，改善プロセスを繰り返すことである。環境は常に変化している。また，コンピュータ犯罪は年々進化して，セキュリティホールも増加している。このような状況に対応するために定期的な診断は必須である。

セキュリティを強固にするために，ファイアウォールや，侵入監視システムを導入するが，セキュリティ機器の運用はログ解析等の高度な技術力が要求される。セキュリティの強度を維持するために運用代行やリモート監視等のアウトソーシングを行うのも有効である。

当社のセキュリティサービス

当社は，セキュリティ対策プロセスの各工程に対し，各種のサービスを用意し，世界で実績のあるトータルサー

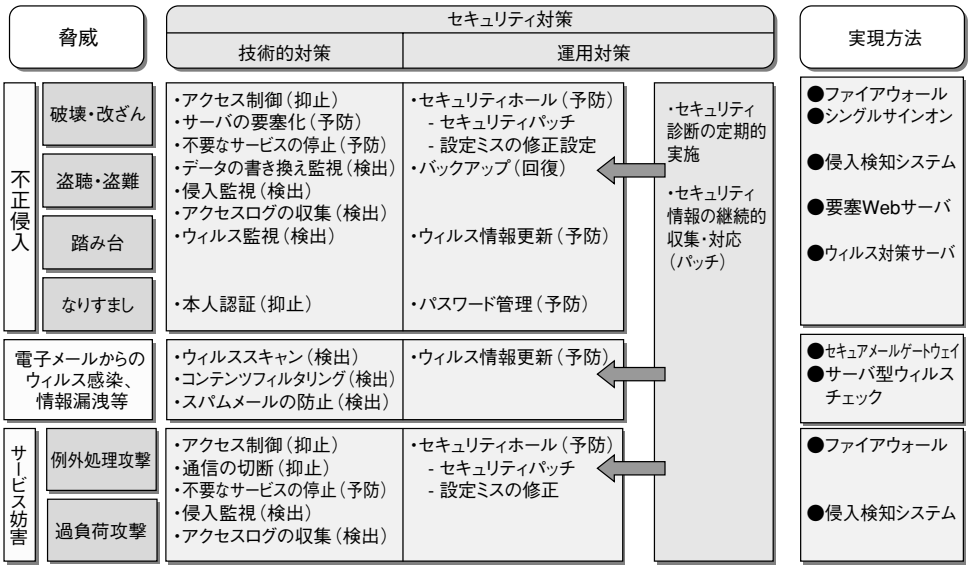


図5　脅威とセキュリティ対策例

ビスの提供を行っている。

上流工程である診断，企画の工程では，国際標準およびSRIコンサルティング社（現レッドサイレン社）の方法論に準拠したセキュリティポリシーサービスを提供している。一般的に，上流のコンサルティングについては，ベンダー系は，技術的領域は得意であるが，非技術的領域（管理，組織，人事など）は弱く，コンサルティング専門企業はシステム固有のセキュリティに弱く，一般論に偏り具体策に弱いと言われている。当社は，SRIコンサルティング社（現RedSiren社）との提携により，非技術的領域を含めたノウハウを有している。

セキュリティ対策プロセスの各工程におけるサービスを充実させるために，沖電気グループの特徴を生かしたサービス提供を行っている（図6参照）。

上流の診断，企画フェーズを主として沖コンサルティングソリューションズ（OCS），設計からシステム構築を沖電気，運用・保守については沖電気カスタマアドテック（OCA）が担当している。

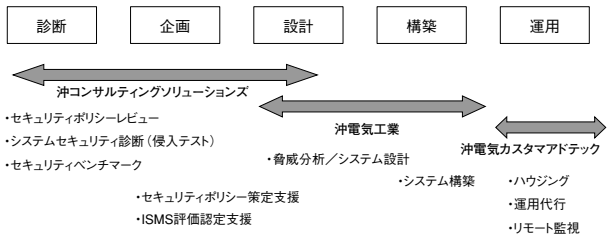


図6　セキュリティ対策プロセスと沖グループの取り組み

ま と め

ネットワークが社会インフラであるとの認識は，広く認められているにもかかわらず，コンピュータ犯罪が激増している割には，日本企業のセキュリティ対策は進んでいない。一方，米国では事件が起こると常に企業責任が問われる社会であるため，セキュリティポリシーに基づくセキュリティ対策が進んでいる。日本でセキュリティ対策が進んでいない理由としては，①セキュリティに対する投資効果が見えない，②トップの理解が得られない，③危機意識が薄い日本的風土，等が考えられる。ガートナーグループの調査報告によれば，被害を受けると，セキュリティ対策コストの1.5倍の費用が必要になる。セキュリティ対策は，一種の保険と考えて取り組むべきである。セキュリティ対策には，100%はなく，セキュリティを求めれば求めるほどコストはかかり，利便性も失われていく。重要なのは，リスク分析を行い，保護すべき資産に見合った投資を行うことである。 ◆◆

●筆者紹介

芦田元之：Asanobu Ashida.沖コンサルティングソリューションズ株式会社 シニアコンサルタント
矢野達朗：Tatsuro Yano.金融ソリューションカンパニー 金融ソリューション開発本部 ネットセキュリティ開発部 部長