

# FIP IT BOX

## ASP&IDCニュース

Contents / January, 2002

**IASP&IDC** ネットワーク上に潜む脅威  
政府の動きと企業の対応  
FIPのセキュリティサービス

発行日 2002年1月18日  
発行元 販売推進統括部 企画推進部  
東京都江東区青海2-45 タイム24ビル  
連絡先 03-5531-5120/info@fip.fujitsu.com  
URL <http://www.fip.fujitsu.com/>

富士通エフ・アイ・ピー株式会社

セキュリティ

## 企業活動を脅かすサイバー犯罪

～ セキュリティリスク管理の重要性～

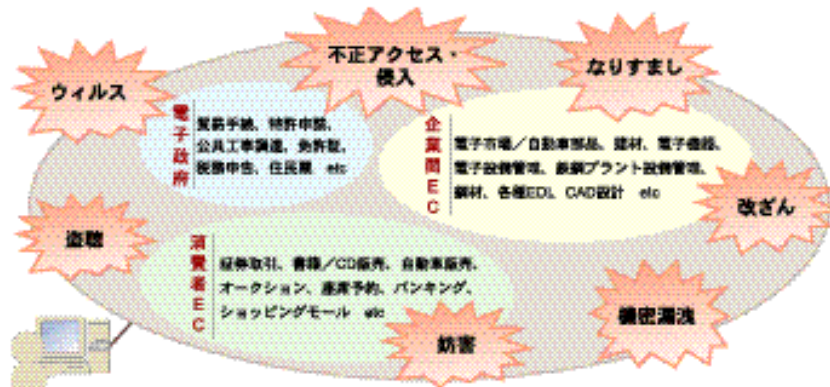
西暦2000年問題がようやく落ち着いた2000年1月後半、官公庁のホームページがハッカーと呼ばれる不正侵入者によって書き換えられる事件が立て続けに発生し、大きな波紋を呼びました。また2001年夏以降、CodeRed（コードレッド）やNimda（ニムダ）・BADTRANS（バッドトランス）などの悪性のコンピュータウイルスが世界的にまん延し、多くの企業が被害を受けています。

インターネットは、ビジネスのプロセスや消費者行動を大幅に変え、企業活動および日常生活の一部となってきていますが、一方でその企業活動を揺るがす新たな脅威、いわゆる「サイバー犯罪（ネットワーク上における犯罪行為）」が急激に増えてきており、各企業のネットワークセキュリティ対策が急務となっているのです。

### ネットワーク上に潜む脅威

それでは、これら企業にとって脅威である「コンピュータウィルス」や「不正アクセス」とはどのようなものなのでしょうか。

【ネットワーク上に潜むさまざまな脅威】



脅威	内容<現実世界での例>
盗聴	通信路等でデータを盗む <電話の盗聴>
なりすまし	他人になりすまし取引などを行う <いたずら電話による出前>
機密漏洩	社内機密文書の社外漏洩 <個人電話番号等の流出>
改ざん	データ等の改ざん <契約書等の文書のねつ造>
妨害	大量のデータによるサイト攻撃 <無言電話、抗議デモ行進>
不正アクセス・侵入	コンピュータへの不正侵入 <銀行へ侵入し現金強奪>
ウィルス	コンピュータウィルスの侵入 <インフルエンザ等のまん延>

参考(図): セコムトラストネット(株)ホームページ

【メール機能を悪用して感染する主なウイルス】

ウイルス名	特徴(行為)
W32/Ske(Happy99) W32/MTX	メール送信時にウイルスを添付したメールを同じ宛先に送信
W32/ExplorerZip	メール受信時に送信者へウイルスを添付したメールを送信
VBS/LOVELETTER	登録アドレスにウイルスを添付したメールを送信
W32/Navidad	受信トレイにあるメールを再利用して、ウイルスを添付したメールを送信
W32/Hybrid	送受信メール、Webサイト等から取得したアドレス宛にウイルスを添付したメールを送信
W32/Sircam W32/Nimda	登録アドレス、Webサイトから取得したアドレス宛にウイルスを添付したメールを送信

(出典: IPA 資料)

### コンピュータウイルスと不正アクセス

コンピュータウイルスとは「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラム」です。その種類は、文書ファイルなどに感染する「マクロ型ウイルス」、Eメールなどネットワークを介して拡散する「ワーム型ウイルス」など多様で、ここ数年の届出件数は著しく増加しています。

また不正アクセスとは、システムへの利用権限がないハッカーなどが、システムを不正に使用した

り、破壊(クラック)を行うことです。その多くは、不正侵入するための事前調査(アクセス形跡)の段階で済んでいます。実際に不正アクセスされたケースでは、パスワードの盗用により本人になりすましてオンラインショッピングされたり、利用もしていないダイヤルQ2などから請求が来たという例もあります。

変わりがく脅威のタイプ  
従来ウイルスによる被害は、受取った本人のパソコンが起動しなくなるとか、データが消えるというように、個人の問題で済んでいるものが殆どでした。また、企業の顔でもあるホームページが怪しげな情報に書き換えられるなど、一時的な業務妨害はあっても、企業

### 変わりゆく脅威のタイプ

活動に直接影響を及ぼすものではありませんでした。

しかし昨今のサイバー犯罪は、このような愉快犯のレベルから企業の根幹を攻撃するものに変化してきており、且つ復旧費用も膨大となっています。例えば2000年5月に世界中に広がった「ラブレター・ウイルス」は、5日間で約67億ドルの損害を与えたとも言われています。

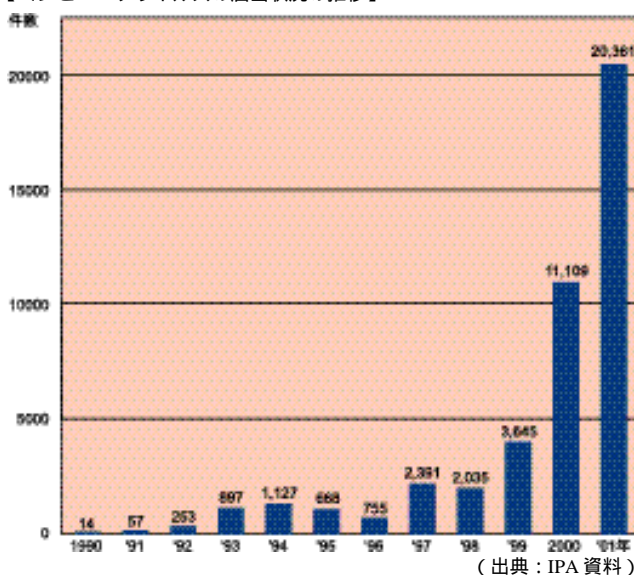
そして最も深刻な問題は、自社のみならずお客様や取引先へも被害が及び、その企業の信用失墜や訴訟にまで発展する可能性があることで、企業のセキュリティ対策はもはや無関心では済まなくなっています。

政府の動きと企業の対応

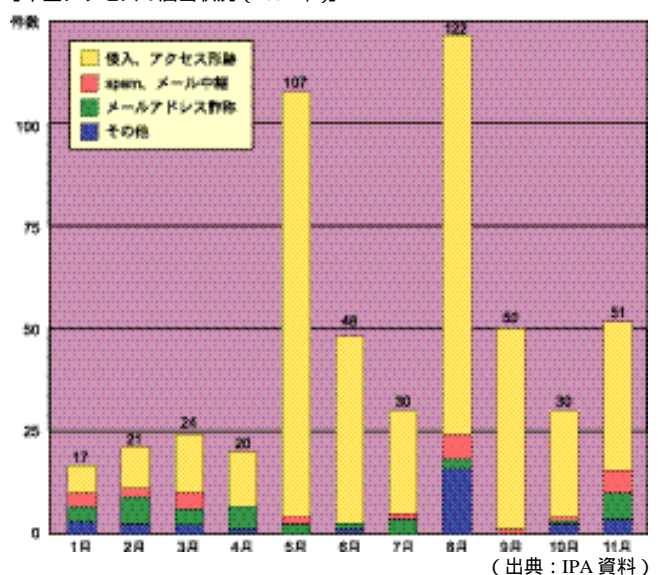
### 法律等の整備

これまでコンピュータ犯罪については、情報の改ざんや消去があつて初めて犯罪として処罰されてきました。しかし情報の盗用・改

【コンピュータウイルスの届出状況の推移】



【不正アクセスの届出状況(2001年)】



ざんなどのハイテク犯罪が増加し、またその被害金額も莫大であるため、原因となる不正アクセス行為自体を取り締まる必要が出てきたのです。そこで2000年2月、「不正アクセス禁止法（不正アクセス行為の禁止等に関する法律）が施行され、2001年6月までの同法による検挙件数は、44件（警察庁発表）にもものぼります。

さらに、2001年11月には「サイバー犯罪条約」に日本政府も署名しました。サイバー犯罪条約とは世界規模で増加するインターネット犯罪に対処するためにできた国際条約です。この署名によりサイバー犯罪に関する国内法がさらに整備されることでしょう。

### 企業としての取組み

次に、企業の重要な取組みとして「セキュリティ管理サイクル」の実践が挙げられます。ネットワークセキュリティ上の欠陥を洗い出し、企業としてのセキュリティ方針の策定。それに基づく堅牢なシステムの構築。そしてシステムの定期的な監視と情報収集により、

新たな欠陥が見つければまた塞ぐというように、適正なセキュリティ環境の維持には、常に管理サイクルを念頭におく必要があるのです。

### セキュリティ・ポリシーの策定

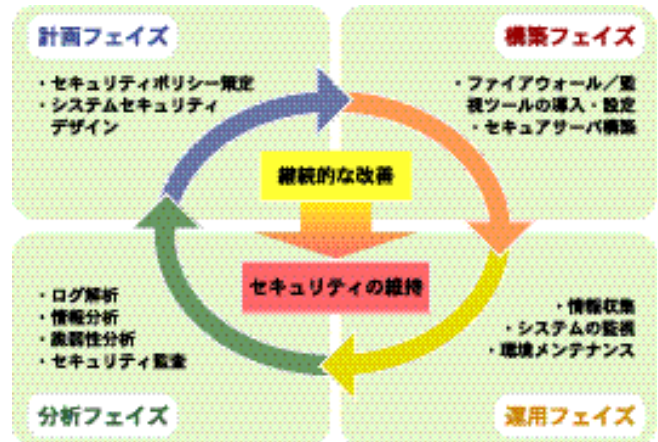
この管理サイクルを運営するためには、トップダウンによるセキュリティ・ポリシーの策定が不可欠です。これは、その企業がネットワークセキュリティを維持するための基本的なルールを定めただけのものですが、このような憲法や法律に相当する決まりがないと、各自バラバラな行動をとりかねません。

そこで、これらのルールを作り、従業員全員に周知徹底させることが必要なのです。それでは、ルール作りのポイントについて防火対策と比

較して見てみましょう。

セキュリティの維持対策は、どこの企業でも一般的に行われている防火対策と同じです。消防法では防火責任者を定めることになっていますが、ネットワークセキュリティにおいても運用責任者を明確にし、問題発生時に統率行動が取れることが重要です。更にインターネットへの接続口も、火気取扱い場所のように限定する必要があります。火種になりそうなものについては利用を制限し、最低限の設備として、防火壁や消火器に相当する「ファイアウォール」や

【セキュリティ管理サイクル】



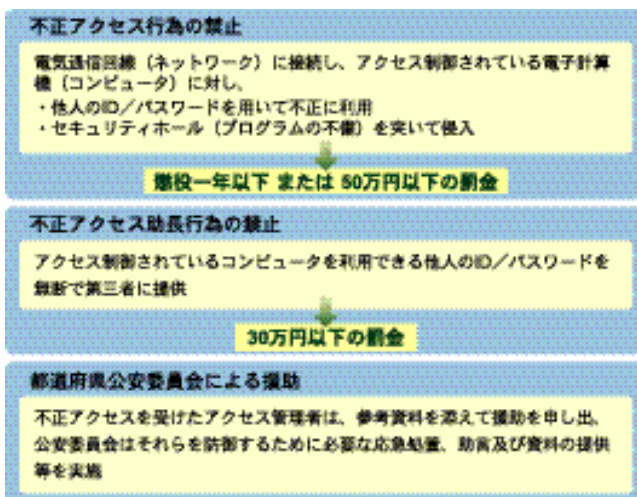
【防火対策とセキュリティ対策の比較】

防火対策	ネットワークセキュリティ対策
防火責任者	運用責任者
喫煙場所/取扱危険物の限定	利用サービスの限定
避難訓練	不正アクセス対応の事前プラン策定
防火壁	ファイアウォール
消火器	ログ取得による監視、アンチウイルスソフト
放火犯	ハッカー/クラッカー
火事の発生	不正アクセスの発生
消防隊	CSIRT <sup>*1</sup> (JPCERT/CC <sup>*2</sup> )
初期消火活動	サーバの隔離

参考：東京書籍（株）東書ネット「学校におけるインターネットとセキュリティ」

\*1 : Computer Security Incident Reponse Team  
セキュリティ・インシデント（不正アクセス等）に対応する組織  
\*2 : JaPan Computer Emergency Response Team Coordination Center  
日本における唯一の CSIRT

【「不正アクセス禁止法」の概要】



「ウイルス対策ソフト」も導入します。

また、もし侵入を受けてしまったら、それ以上被害を拡大させないためにサーバをネットワークから切り離したり、JPCERT/CC<sup>\*2</sup>への報告と援助の申請も必要となってきます。

### 個人レベルで実践すべきこと

もちろん個人の意識改革も不可欠です。例えば、ウイルス対策ソフトを各パソコンに導入したとしても、検出するためのデータが最新のものでなければ意味がありません。またパソコンを起動する際のパスワードも、最初に設定したまま1回も変更していない人も時々見受けられますが、これは不正侵入者などにIDやパスワードが盗まれた時に永久に不正アクセスを許し続ける温床ともなるのです。

## FIPのセキュリティサービス

### セキュリティ対策支援サービス「SafePort」

当社では、不正アクセス防止を目的としたセキュリティ対策支援サービス「SafePort」(セーフポート)を、国内のセキュリティビジネスの草分けである(株)ラック及びウイルス対策の権威である(株)シマンテックと技術提携し、2000年4月より提供しています。

本サービスでは、インターネットサイトの共通基盤対策として、セキュリティ危険度に関する検査結果及び改善策を提示する「監査サービス」お客様の要望に対しセキュリティに関する適切な提案を行う「コンサルティングサービス」お客様のご利用目的に基づき

ネットワークや各種サーバの設定を行う「構築サービス」。そして、ネットワークなどを24時間365日監視し、もし侵入があった場合その対策を講じる「監視サービス」「保守サービス」をそれぞれ提供し、お客様のセキュリティ管理サイクルの実践を支援いたします。

また、最重要課題であるセキュリティポリシー策定に関しても、当社内での実践経験を生かし、お客様の利用環境に即したポリシー策定支援を計画しています。

しかし、ブロードバンド時代を反映したインターネットには、冒頭の絵に示したような不正アクセス以外の多くの脅威に対処しなければなりません。そこで、イントラネットまでを含めたウイルス対策サービスや、e-Japan構想で更に拡大が予想される電子商取引につき、安全性を考慮したサイト構築のための支援など、時代のニーズに合ったサービスの提供を予定しています。

### 堅牢なセキュリティ環境を誇るIDC セキュリティ環境を適正に運用

するには、専門組織や人材の育成などの情報セキュリティ対策とともに、インフラ面での対策も必要であり、これにはかなりの費用と労力が必要とされます。

当社では、経済産業省の安全対策基準のほか、当社独自の安全対策強化基準をクリアした信頼性の高いIDCを全国各地に配置しています。また東京センタにおいては、2001年12月に、情報セキュリティマネジメントシステム(ISMS)<sup>\*3</sup>適合性評価制度の認証を国内最大範囲で取得しました。

今後は、ISO9001が実証する高品質な運用サービスや先にご紹介したセキュリティサービスに加え、今回のISMS認証取得により、グローバルスタンダードを踏まえた安全性・信頼性に基づく付加価値の高いデータセンタサービスを提供し、お客様のシステムが常に安全であり続けるよう支援してまいります。

\*3: Information Security Management System  
審査登録機関:(財)日本品質保証機構(JQA)

【「SafePort」サービス体系図】

対応	区分	サービス内容	対象となる脅威
セキュリティポリシー策定 (提供予定)		全社方針の策定 ・保護すべきデータ、アクセスコントロール ・ウイルス/不正アクセス対策、緊急対応	・全脅威への対応方針が必要時にインターネット利用に際するポリシーが重要
インターネットサイト監査・コンサルティング・構築・監視・保守		インターネットサイトの共通基盤対策 ・ツール及び類似的なセキュリティ検査 ・セキュリティに関する適切な提案 ・ネットワーク/サーバのセキュリティ強化策 ・ネットワーク監視/不正侵入等の被害対応 ・セキュリティ情報収集/修正パッチ適用	・不正アクセス/侵入 ・ウイルス ・不適切サイトの利用 ・詐害 ・BroadBand常時接続の脅威
ウイルス対策 (提供予定)		各種ウイルス対策 ・機器/ソフトの選定、適用 ・パターンファイル更新等の運用・保守 ・ウイルス駆除対策	・ウイルス ・BroadBandにより個人の利用環境が大きく変化しており対策が必須
電子商取引安全性確保 (提供予定)		PKI、GPKI基盤の確立 ・認証システム(パーソナル認証、電子認証、証明書等) ・否認禁止	・なりすまし、改ざん ・機密漏洩 ・盗聴