

はじめに

21世紀最初の年となった平成12年度の国内におけるパーソナルコンピュータ出荷台数実績は、対前年度比21%増の1,200万台と見込まれ、次年度にあっては、対昨年実績見込み比13%増の1,360万台との予測がなされている（社団法人電子情報技術産業協会）など、国内におけるパーソナルコンピュータの普及は拡大の一途を辿っている。

また、日本のインターネット普及人口比率は、今年中には米国を上回って56.5%となると予測されているほか（情報通信研究所「インターネットの普及予測について」）、インターネットを利用している企業は約8割に達しているとの調査結果も出ている（平成11年度郵政省（現総務省）「通信利用動向調査」の結果）。

このように、パソコンとインターネットの普及拡大により、情報流通の高速化、ボーダレス化が急速に進展したことで、これまでの現実社会に加えて、電腦空間上の社会、いわばサイバー社会が形成されつつある。

この新しい社会が、我々にとって安全で住み良い社会となってもらいたいと願うのは私だけではないだろうが、残念ながら、現実社会と同様、あるいはそれ以上に、このサイバー社会においても、「改ざん」や「なりすまし」、「データ破壊」、「不正アクセス」などといった脅威が、その安寧を侵害しているのである。

一方で、現実社会に企業等からの依頼を受けて、その施設や商品のセキュリティを確保するというサービスが存在するように、サイバー社会においても、ネットワークを通じて行われる不正アクセスなどの不正行為から、コンピュータシステムやネットワークを守るというサービス、いわばサイバーセキュリティサービスが存在する。

やがて大きく成長して、我々の生活や企業活動に深く関わりを持つようになるサイバー社会において、セキュリティの確保というのは、現実社会よりも強く求められるとも考えられる。このような情勢の中で、サイバーセキュリティサービスは、今後ますます重要な存在となるであろう。

今回、財団法人社会安全研究財団が設置した「サイバーセキュリティ調査研究委員会」においては、委嘱を受けた12人の委員が、このサイバーセキュリティサービスに関する実態調査を計画・実施し、その結果などをもとに、今後のサイバーセキュリティサービスについて意見交換を行った。本報告書は、当委員会での成果についてまとめたものである。

本報告書が、今後のサイバーセキュリティサービスの健全な発展の一助となれば幸いである。

平成13年3月

サイバーセキュリティ調査研究委員会

委員長

辻井重男

サイバーセキュリティ調査研究委員会委員（敬称略）

辻 井 重 男 （委員長）	中央大学理工学部教授
大 木 栄 二 郎	日本アイ・ビー・エム株式会社 ビジネス・イノベーションサービス 主席コンサルタント
小 倉 久 宜	財団法人金融情報システムセンター 監査安全部長
小 林 偉 昭	社団法人日本防犯設備協会 情報セキュリティ調査委員会委員長
小 屋 晋 吾	トレンドマイクロ株式会社 ビジネスパートナー営業部長
高 橋 正 和	アイ・エス・エス株式会社 国際技術部長
田 尾 陽 一	セコム株式会社 サイバーセキュリティ事業部 取締役事業部長
三 輪 信 雄	株式会社ラック 不正アクセス対策事業本部 取締役本部長
安 富 潔	慶應義塾大学法学部教授
山 崎 文 明	グローバルセキュリティエキスパート株式会社 専務取締役
坂 明	警察庁生活安全局生活安全企画課 セキュリティシステム対策室長
高 橋 守	警察庁情報通信局技術対策課 調査官

◇◇ 目 次 ◇◇

はじめに

第1章 調査の概要.....	1
1. 調査の目的.....	1
2. 調査対象.....	2
3. 調査方法.....	3
第2章 サイバーセキュリティサービス事業者の現状.....	6
1. サイバーセキュリティサービス事業者.....	6
2. サイバーセキュリティサービスの提供状況.....	13
3. サイバーセキュリティサービス事業者における人材.....	24
4. 顧客情報の漏洩防止.....	26
5. サイバーセキュリティサービス事業者の課題.....	30
第3章 ユーザ企業におけるサイバーセキュリティへの取り組みの現状.....	32
1. ネットワークの利用状況.....	32
2. サイバーセキュリティへの対応状況.....	35
3. サイバーセキュリティ対策への取り組み状況.....	37
4. サイバーセキュリティサービスの利用状況.....	46
第4章 サイバーセキュリティサービスの課題.....	52
1. サイバーセキュリティサービス業界の抱える課題.....	52
2. ユーザ企業が抱える課題.....	56
第5章 サイバーセキュリティサービスの発展のために必要な取り組み.....	58
資料編.....	63

第1章 調査の概要

1. 調査の目的

近年、企業活動や社会活動の多くは情報システムに依存するようになってきている。

これまでの情報システムは汎用コンピュータなどによるコンピュータ単体での処理が主であり、情報（データ）のやり取りへの意識は希薄であった。VANやEDIといった専用ネットワークの利用はあったが、ネットワーク毎に仕様が異なり、誰でもが簡単にアクセスできるものではなかった。

しかし、近年、インターネットの急速な普及により情報システムのあり方が急激に変化している。オープンネットワークであるインターネットでは、標準化された技術の利用により、遠隔地の企業や消費者などとも簡単に情報のやり取りが行える。企業でいえば、社内の情報はもとより、社外の情報についても、これまでよりもはるかに簡単に利用できる。また、個々の消費者と双方向に情報をやり取りすることも行える。

多くの可能性を持ったネットワークとしてインターネットへの注目が高まっており、企業における活用の仕方にも製品紹介といったPRを主としたものから、顧客向けの電子商取引や取引先との連絡や受発注といった、より業務と密接に関連した分野にまで広がっている。

その一方で、外部からネットワークを通じて情報システムに対して行われる不正アクセスやコンピュータウイルスといった新たな脅威が増えてきている。2000年1月に発生した各省庁ホームページの改ざん事件や、2000年2月に発生した米ヤフー社や米アマゾン・コム社等へのDDoS攻撃によるサービス妨害事件などが起きている。また最近では、インターネット上で配布されているツールを利用することで、専門的な技術知識を持たなくとも不正アクセスを試みるのが可能になっており、ネットワークを利用する上で、こうした脅威を受ける可能性は高まってきている。

特に、ネットワークの活用範囲が、より業務に関連するようになるに従って、ネットワーク上の脅威が、企業活動や社会に与える影響や損害は多大なものになる可能性がある。

IT革命などと呼ばれるネットワーク社会の効用を享受するためには、ネットワーク上における高度な安全性を確保し、利用者の信頼を築くことが必要である。個々の企業等においても、ネットワーク上の脅威に対する十分なサイバーセキュリティ対策を施すことが喫緊の課題となっている。

しかしながら、コンピュータウイルスや不正アクセスの手法は、日々技術革新が行わ

れており単独の企業で十分な対策を行っていくことは難しくなっている。また、サイバーセキュリティ対策を行っていくためには、情報システムの技術的な分野の取り組みだけでなく、社員や組織のモラルや管理体制といった運用面での取り組みについても行っていくことが重要になる。このように広範にわたるサイバーセキュリティ対策を継続的に行うことは、セキュリティの専門的な人材やノウハウのない、ユーザ企業が単独で行っていくことは難しい。そのため、サイバーセキュリティに関する専門的な知識やノウハウを持った事業者がセキュリティ対策を委託するケースが増えてきている。

このような背景から、現在、サイバーセキュリティサービスに関連するビジネスが成長してきているが、まだ市場の立ち上がり期でもあり、業界として様々な課題に直面していることが想像される。

そこで、本調査では、サイバーセキュリティサービス事業者の実態について調査するとともに、業界が抱える課題について整理し、そのうえでサイバーセキュリティサービス事業の健全な発展を促すために必要となる方策等について検討を行うことを目的とする。

2. 調査対象

本調査では、サイバーセキュリティサービスを、セキュリティポリシー関連サービスやセキュリティチェック（監査、検査、診断）、監視（不正アクセス検知、ログ監視、ログ解析等）、セキュリティ関連のトレーニングなどのサイバーセキュリティに関連したサービスのことと定義する。すなわち、ルータやサーバなどのハードウェアやソフトウェアの販売についてはサイバーセキュリティサービスとして含まないこととする。

具体的には本調査では、以下のサイバーセキュリティサービスを想定する。

- セキュリティポリシー関連のサービス
- セキュアなシステム設計・構築・運用（ファイアウォール、VPN、電子認証システム、セキュアサーバ など）
- セキュリティチェック（監査、検査、診断）
- 監視（不正アクセス検知、ログ監視、ログ解析等）
- ウィルス対策（ウィルス監視、ウィルス情報提供・アップデート）
- 緊急対応（不正アクセスなどの被害を受けた際の現場への急行、サービス停止等）
- 障害復旧（データリカバリ、データバックアップ）
- 情報提供（不正アクセス関連情報提供など）
- セキュリティ関連のトレーニング（教育、研修）

3. 調査方法

(1)サイバーセキュリティサービス事業者アンケート調査

サイバーセキュリティサービスを提供している事業者を対象に 300 社を抽出、郵送によるアンケート調査を実施した。

【調査名】

サイバーセキュリティサービスに関する実態調査

【調査対象】

サイバーセキュリティサービス事業者並びに大手システムベンダー企業 300 社

【調査方法】

郵送によるアンケート調査票の配布・回収

【調査期間】

2000 年 11 月 29 日～2000 年 12 月 15 日

【配布数】

300 通

【回収結果】

有効回答数 41 通（回収率 13.7%）

(2)サイバーセキュリティサービス事業者インタビュー調査

サイバーセキュリティサービスを提供している事業者 15 社を対象にインタビュー調査を実施した。

【調査対象】

サイバーセキュリティサービス事業者 15 社

【調査項目】

- ・ サービス概要
- ・ 採用、教育状況
- ・ 顧客情報等の管理体制
- ・ 事業上の課題
- ・ 必要となる環境整備

【調査手法】

訪問面接調査

(3)企業アンケート調査

サイバーセキュリティへの取り組み状況やサイバーセキュリティサービスの利用状況について、東証一部・二部上場企業 2,009 社を対象に郵送によるアンケート調査を実施した。

【調査名】

サイバーセキュリティの取り組みに関する調査

【調査対象】

東証一部・二部上場企業 2,009 社

【調査方法】

郵送によるアンケート調査票の配布・回収

【調査期間】

2000年12月6日～2000年12月20日

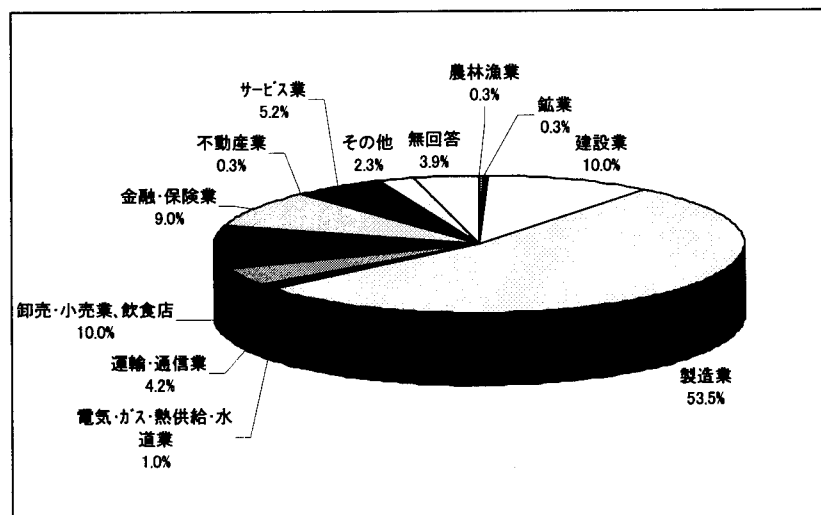
【配布数】

2,009 通

【回収結果】

有効回答数 310 通（回収率 15.4%）

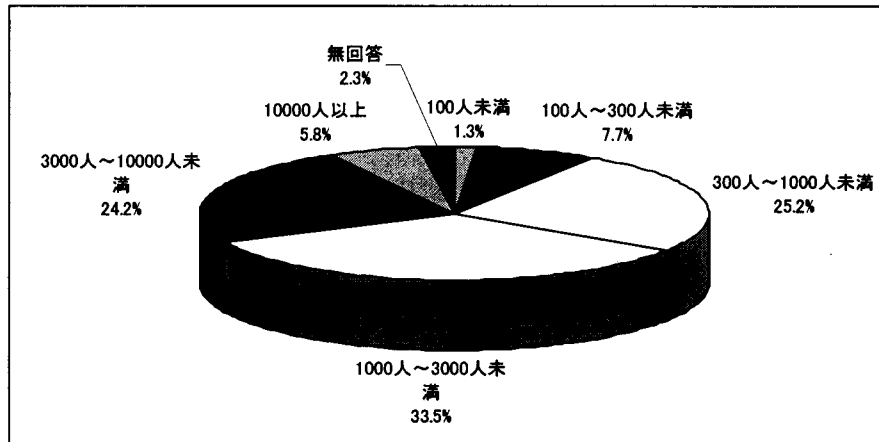
図表1-1 回答企業の業種構成



資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

（注）第3章以降の分析では、農林漁業・鉱業の企業はその他に、不動産業はサービス業に含めた。

図表1-2 回答企業の従業員数



資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

(4)企業インタビュー調査

ユーザ企業 2社を対象にインタビュー調査を実施した。

【調査対象】

ユーザ企業 2社

【調査項目】

- ・セキュリティ対策状況
- ・サイバーセキュリティサービス利用状況
- ・サイバーセキュリティサービス利用上の課題
- ・必要となる環境整備

【調査手法】

訪問面接調査