

# サイバーセキュリティの取り組みに関する調査

～「サイバーセキュリティに関する調査」ご協力をお願い～  
拝啓、時下、ますます御清祥のこととお喜び申し上げます。

警察庁所管の財団法人社会安全研究財団「サイバーセキュリティ調査研究委員会」では、「サイバーセキュリティの取り組みに関する調査」を実施させて頂くことになりました。

インターネットの急速な普及などを背景として、社会活動の幅広い分野におけるネットワークの利用が行われるようになっていきます。これに伴い、不正アクセスやコンピュータウイルスなどのネットワークに対する脅威が社会や企業活動に与える影響は多岐にわたっており、サイバーセキュリティ対策の必要性が高まっています。

一方で、急速な技術革新や技術の高度化に伴い、ユーザ企業単独で、適切なセキュリティ対策を継続的に実現していくことは、コスト的にも人材的にも難しくなっています。こうした流れの中、アウトソーシングサービスとしてサイバーセキュリティサービスを利用する企業が増えてきています。

今回の実態調査は、当委員会においてサイバーセキュリティサービス業界の健全な発展方策の検討を行うにあたって、サイバーセキュリティへの取り組みを行われているユーザ企業の方々に、サイバーセキュリティ対策や外部サービス利用の実態等についてお聞きするものです。

つきましては、お忙しいところ誠に恐縮ではございますが、このアンケートの趣旨をご理解いただき、ご協力頂きますようお願い申し上げます。

ご記入いただきました調査票は同封の返信用封筒（切手不要）で平成12年12月20日（水）までに投函いただきますようお願い申し上げます。

平成 12 年 12 月

なお、このアンケートは株式会社三和総合研究所に委託して実施してまいります。ご不明の点がございましたら、下記担当までお問い合わせ下さいますようお願い申し上げます。

## 【アンケートの趣旨について】

〒101-0047 東京都千代田区内神田 1-7-8 大手町佐野ビル  
(財)社会安全研究財団 (担当：中井) Tel: 03-3219-5177

## 【アンケートの内容について】

〒105-8631 東京都港区新橋 1-11-7 新橋三和東洋ビル  
(株)三和総合研究所 研究開発第2部 (担当：佐藤 (前)、五味、白藤) Tel 03-3572-9034

会社名	
本社の所在地	〒 (    -    )
この調査票についての連絡先 部署名・氏名・電話番号	部署： 氏名： (    ) 電話番号： (    ) e-mail：

## 1. 貴社の概要

(1) 設立年月	(西暦) 年 (    ) 月
(2) 資本金額	※                          十億                          百万円
(3) 業種	1. 農林漁業                          7. 卸売・小売業、飲食店 2. 鉱業                                  8. 金融・保険業 3. 建設業                              9. 不動産業 4. 製造業                              10. サービス業 5. 電気・ガス・熱供給・水道業    11. 公務 6. 運輸・通信業                    12. その他
(4) 年間売上高(総売上高) (統計的な処理を行うため、個別企業の情報は公開致しません)	※                          十億                          百万円 (平成11年4月1日から平成12年3月31日までの1年間又は最も近い決算日前の1年間について記入してください。)
(5) 総従業員数 (有給役員、臨時・日雇を含む) (統計的な処理を行うため、個別企業の情報は公開致しません)	千                          人 (平成12年3月31日現在又は最も近い決算日現在で記入してください。)

2. ネットワークの利用状況について

問1 貴社では、インターネットを利用していますか。

1. 全社的に利用している	(問 1-1、問 1-2 にもご回答ください)
2. 一部の事業所または部門で利用している	(問 1-1、問 1-2 にもご回答ください)
3. 利用していないが具体的に利用する予定がある	
4. 利用していないし具体的な予定もない	

問 1-1 貴社がインターネットを利用し始めた時期はいつですか。

1. 1989 年以前	5. 1997 年
2. 1990 年～1994 年	6. 1998 年
3. 1995 年	7. 1999 年
4. 1996 年	8. 2000 年

問 1-2 貴社の本社でのインターネットとの接続回線速度はどのくらいですか。

1. 64kbps 以下	4. T1 (1.5Mbps) 以上 6Mbps 以下
2. 64kbps 超、128kbps 以下	5. 6Mbps 超
3. 128kbps 超、T1 (1.5Mbps) 未満	

問2 貴社では公開用の Web サーバを運用していますか。

1. 運用している
2. 運用していないが具体的に運用する予定がある
3. 運用していないし具体的な予定もない

問3 貴社では社内システムへのリモートアクセスを可能にしていますか。

1. 可能にしている
2. 可能にしないが具体的に可能にする予定がある
3. 可能にしないし具体的な予定もない

問4 貴社では社内や社外においてどのような用途に暗号を採用していますか。(複数回答)

1. 暗号メール
2. 記録媒体上の情報 (ファイルの暗号化)
3. 認証情報 (電子証明書など)
4. クレジットカード番号などの重要なトランザクションデータの転送
5. 利用していない

3. セキュリティへの取り組み状況

問5 貴社には専任のセキュリティ対策の担当者がいますか

1. 専任の担当者を設置していて、任務と権限を明確にしている
2. 専任の担当者を設置しているが、任務と権限はあまり明確ではない
3. コンピュータシステム運用管理者がセキュリティ対策についても兼任している
4. コンピュータシステム運用管理者以外がセキュリティ対策についても兼任している
5. セキュリティ対策担当者は設置していない
6. その他 (具体的に: )

問6 貴社では経営理念に基づき、セキュリティ対策のあり方などに関する基本方針を規定したセキュリティポリシーを定めていますか。

1. 定めている	4. 定めていない
2. 現在作成中である	5. 必要ない
3. 作成を検討している	

問7 セキュリティポリシーに基づき、具体的な操作や業務処理手順などを定めたセキュリティガイドラインを定めていますか。

1. 定めている	4. 定めていない
2. 現在作成中である	5. 必要ない
3. 作成を検討している	

問8 セキュリティポリシーは主にどの部門が中心となって作成しましたか。

1. 情報システム部門	4. 総務部門
2. 情報セキュリティ担当部門	5. その他 (具体的に: )
3. 経営企画部門	

問9 貴社ではどのくらいの頻度でシステム監査を行っていますか。

1. 数年に1回	4. 特に実施していない
2. 年1回	5. その他 (具体的に: )
3. 年数回	

問10 貴社では、下記に示すようなセキュリティ関連の取り組みを行っていますか、それぞれの項目毎にお答え下さい。

取り組み	取り組んでいる	取り組みを予定している	取り組んでいないが必要性を認めている	取り組みの必要性を感じない	わからない/知らない
ウイルス対策	1	2	3	4	5
不正アクセス対策	1	2	3	4	5
PKI(電子認証)	1	2	3	4	5
社内システムにおける暗号利用(ファイル暗号、暗号メール等)	1	2	3	4	5
不正アクセスやウイルス等の被害に対するセキュリティ保険の適用	1	2	3	4	5
BS7799等国際標準に準拠したセキュリティポリシーの策定	1	2	3	4	5
調達時や自社システムの安全性評価等への情報セキュリティ評価基準(ISO15408)の活用	1	2	3	4	5
従業員に対するセキュリティ教育・研修の実施	1	2	3	4	5

4. コンピュータウイルス対策について

問11 貴社ではこれまでにコンピュータウイルスに感染したことがありますか。

1. ある (→問11-1、問11-2にもご回答ください。)

2. ない

問11-1 コンピュータウイルス感染によって受けた被害の規模はどの程度でしたか。

1. 全社的な被害

2. 局所的な被害

3. 実害なし

4. その他(具体的に: )

問11-2 コンピュータウイルスに感染した経路・原因はどのようなものですか。(複数回答)

1. インターネットからダウンロードしたファイルやソフトウェアから

2. 電子メールの添付ファイルから

3. 外部から入手したフロッピーディスクやCD-ROM等の記録媒体から

4. わからない

5. その他(具体的に: )

問12 貴社ではウイルスチェックソフトの導入をしていますか。

1. クライアントにウイルスチェックソフトを導入している (問12-1にもご回答ください)

2. サーバにウイルスチェックソフトを導入している

3. 導入を検討している

4. 導入していない

問12-1 クライアント用ウイルスチェックソフトは、貴社のパソコン全体のどのくらいのパソコンに導入されていますか。

1. 10%未満	2. 10%~30%未満	3. 30%~50%未満
4. 50%~70%未満	5. 70%~90%未満	6. 90%~100%未満
7. 100%		

問13 ウィルス対策に関する問題点は何か。(複数回答)

1. コストがかかりすぎる
2. 従業員教育が徹底できない
3. 対策を講じるノウハウ・知識が不足している
4. 対策を講じる人材が不足している
5. どこまでやればよいかわからない
6. 要求に合致する製品・サービスがない
7. その他(具体的に: )
8. 特に問題はない

5. 不正アクセス対策について

問14 貴社ではこれまでに不正アクセスの被害を受けたことがありますか。

1. ある

2. ない

問15 貴社では不正アクセス対策としてどのような対策に取り組んでいますか。(複数回答)

1. パスワードの活用

2. ワンタイム・パスワードを使用

3. 指紋認証などのバイオメトリクス認証(生体認証)を使用

4. ファイアウォールの設置

5. アクセス制御ソフトウェアの使用

6. アクセスログの記録、分析

7. 不正なアクセスが行われていないかネットワークを監視

8. システム上にセキュリティホールなどがないか検査、診断

9. その他(具体的に: )

問16 不正アクセス対策に関する問題点は何か。(複数回答)

1. コストがかかりすぎる

2. 従業員教育が徹底できない

3. 対策を講じるノウハウ・知識が不足している(具体的に: )

4. 対策を講じる人材が不足している

5. どこまでやればよいかわからない

6. 要求に合致する製品・サービスがない

7. その他

8. 特に問題はない

6. サイバーセキュリティサービスの利用について

問17 貴社では情報セキュリティ対策を行うにあたって、アウトソーシングサービス（サイバーセキュリティサービス）を利用していますか。

1. 利用している (→ 問 17-1、問 17-2、問 17-3 にもご回答ください)
2. 利用を検討している (→ 問 17-1、問 17-2、問 17-3 にもご回答ください)
3. 利用していない (→ 問 17-4 にもご回答ください)

問 17-1 貴社がご利用になっているサイバーセキュリティサービスはどのようなものですか。(複数回答)

	利用している	利用を検討している
セキュリティポリシー関連のサービス	1	2
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、セキュアサーバ等)	1	2
セキュリティチェック(監査、検査、診断)	1	2
監視(不正アクセス検知、ログ監視、ログ解析等)	1	2
ウイルス対策(ウイルス監視、ウイルス情報提供・アップデート)	1	2
緊急対応(不正アクセスなどの被害を受けた際に、現場への急行、サービスを停止等)	1	2
障害復旧(データリカバリ、データバックアップ)	1	2
情報提供(不正アクセス関連情報など)	1	2
セキュリティ関連のトレーニング(教育、研修)	1	2
その他(具体的に: )	1	2

問 17-2 貴社がサイバーセキュリティサービスを利用する理由は何ですか。(複数回答)

1. 専門業者の方が高い専門性やノウハウ、技術力
2. 専門業者の方が最新情報を持っている
3. 社内担当者だけでは人員が不足
4. 24 時間にあわせて対応できる体制
5. 社内で行うよりもコストが安い
6. その他(具体的に: )

問 17-3 差し支えなければ、貴社が利用しているサイバーセキュリティ事業者名をご記入ください。

問 18 にお進み下さい

問 17-4 貴社がサイバーセキュリティサービスを利用しない理由は何ですか。(複数回答)

1. 社内に高い専門性やノウハウ、技術力があり、必要性がない
2. 社内担当者だけで必要な人員が確保されるため、必要性がない
3. 社内にノウハウの蓄積を行いたい
4. コストが負担できない
5. 要求に合致するサービスが提供されていない
6. 機密情報の漏洩につながることに懸念される
7. その他(具体的に: )

問18 サイバーセキュリティ事業者の選定にあたって重視することは何ですか。(複数回答)

1. 高度な技術力
2. 信用(顧客情報の保護)
3. 実績
4. 価格
5. 迅速な対応
6. 自社のシステム、業務に対する理解
7. 経営の安定性、継続性
8. その他(具体的に: )

問19 貴社がサイバーセキュリティサービスを利用する上での課題は何ですか。(複数回答)

1. 事業者の技術力などを判断する目安がなく事業者の評価・選定ができない
2. 事業者の信用などを判断する目安がなく事業者の評価・選定ができない
3. 事業者に関する情報が不足しており、サービス提供している事業者を見つけにくい
4. 事業者の情報管理体制に不安がある(企業情報の漏洩などにつながるおそれ)
5. サービスの価格体系(相場)がわからない
6. その他(具体的に: )

問20 サイバーセキュリティサービスの利用環境を整備していくためには、どのような取り組みを行っていく必要があるとお考えですか。(複数回答)

1. サービスのガイドラインの整備
2. サービスの質などの目安になる公的な評価制度の整備
3. サービスの質などの目安になる業界団体等による自主的な評価制度の整備
4. セキュリティ関連の人材育成に関連した公的な支援
5. ユーザ企業に対するセキュリティ対策・知識等の普及・啓発
6. 関連法規などの整備
7. その他(具体的に: )

問21 サイバーセキュリティサービス事業者、業界に対する要望をお聞かせ下さい。

ご協力いただき誠にありがとうございました。