情報セキュリティガイドライン

国土交通省

目　次

Ⅰ．はじめに

近年における情報化の発展に伴い、企業規模に関わらず、事業を推進する上で情報活用は不可欠となってきており、３ＰＬ事業者もその例外ではない。そのような中で、情報の漏洩や盗難等による問題も発生しており、マスコミ等でも報じられる問題にまで発展することも少なくない。

このような背景をもとに、政府では「重要インフラの情報セキュリティ対策に係る行動計画」を策定、これを受けて国土交通省では「物流分野における情報セキュリティ確保に係る安全ガイドライン」を策定している。

インターネットや情報システムの発展により、情報がさまざまな形で保管・流通する中で、３ＰＬ事業においても情報セキュリティの確保は重点的に取り組むべき事項のひとつであり、事実荷主企業からの情報セキュリティ確保に関する要請も高まってきている。

しかし、３ＰＬ事業者は荷主企業の要望に応じて適切なセキュリティレベルを確保することが求められており、そのためにかかるコストについて両者の認識が必要である。

こうした現状に対応するため、2006 年 11 月から「３ＰＬ事業促進のための環境整備に関する調査検討委員会」を開催し、物流事業者及び荷主企業双方の実態を踏まえながら、３ＰＬ情報セキュリティガイドラインをテーマの一つと位置づけ検討を行った。

Ⅱ．ガイドライン策定の背景

企業におけるコンプライアンスが重視されるなか、内部統制、リスク管理といったコーポレートガバナンスの確立は３ＰＬ事業者としても急務である。３ＰＬ事業者において情報セキュリティ管理態勢の整備は、その一端を担うものであり、企業としての信頼獲得要素の一つであるといえよう。

３ＰＬ事業者は、荷主企業からの委託業務を推進するにあたり、さまざまな情報を荷主企業とやりとりし、これを事業者内で保管し、利活用することが必要である。

荷主企業から預かった情報はもとより、３ＰＬ事業を推進するにあたり独自に知り得た荷主企業の情報等に関しても、これらがひとたび漏洩・紛失・盗難などの被害にさらされた場合、荷主企業への損失に発展する危険性があることから、十分に留意しなければならない。国土交通省が物流事業者に対して行ったアンケートでも、荷主企業が３ＰＬ事業者を検討／選定する上で情報セキュリティ対応の重視度合いについて、「極めて重要な検討ポイント」との回答が４５％、「他条件と同様に考慮すべきポイント」との回答が４０％であった。

このように、これまで荷貨物そのものに対する安全管理に比べて、情報セキュリティ管理は留意される度合いが低かったが、今後は情報セキュリティについても重要視されるようになることから、３ＰＬ事業者として情報セキュリティ管理について検討することが必須である。

このような背景をうけ、本委員会にて３ＰＬ事業者として実施すべき情報セキュリティ管理をまとめたガイドラインを策定し、本ガイドラインを公表するに至ったものである。

Ⅲ．ガイドラインの目的

本ガイドラインは、各物流事業者が自社に適した情報セキュリティ管理を推進し３ＰＬ事業拡大に資することを目的とし、３ＰＬ事業者が情報セキュリティ管理を行うにあたり、最低限実施すべき点およびポイントとなる事項について内容を絞って定めたものである。事業者ごとに情報セキュリティ対策の実施状況は異なることから、今後３ＰＬ事業および情報セキュリティに取り組む企業が実施すべき基本的な事項を定めた。

なお当該ガイドラインは、荷主企業から預かった情報や委託業務の過程で知りえた荷主企業の情報などの漏洩を防ぐことを目的として定めたが、３ＰＬ事業においては逆に物流事業者が荷主企業に３ＰＬ事業のスキルや業務ノウハウなどを提供する場面も考えられる。そのため、物流事業者が荷主に提供する情報の管理について留意し

ておくことが必要となる。

Ⅳ．本ガイドラインの構成（盛り込む内容の概要）

本ガイドラインでは、物流事業者の情報セキュリティ管理にあたり、以下の各章において留意すべき点を示す。本ガイドラインを参考に、物流事業者は自社の状況にあった情報セキュリティ管理態勢を検討し、具体的な対策を実施することを望むものである。

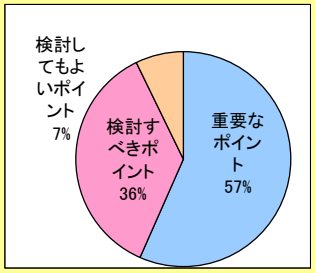
１．情報セキュリティ管理組織体制
２．情報セキュリティ規程類の整備
３．情報の漏洩防止策
　３．１．情報の保管
　３．２．情報の利用制限
　３．３．ID・パスワードの管理
　３．４．電子メール・インターネットの利用
　３．５．ウィルス対策
　３．６．パソコンや外部記憶媒体の持ち出し
　３．７．入室管理
　３．８．情報の廃棄
４．外部委託管理
５．事業継続計画
６．研修・教育の実施
７．事件・事故発生時対応
８．監査・点検

Ⅴ．アンケート分析結果

１．３ＰＬ事業計画における情報セキュリティの重要性

物流事業者

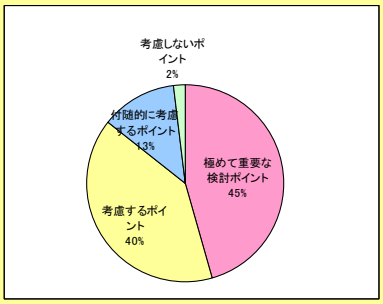
Q5　情報セキュリティの重要度認識



（有効回答：２９４社）

荷主企業

Q8　3PL事業者の選定と情報セキュリティ対応



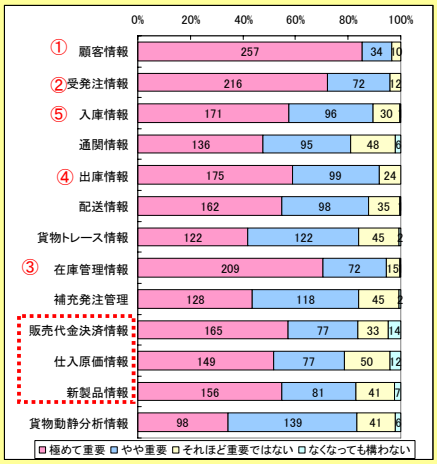
（有効回答：５５社）

物流事業者、荷主双方に対するアンケート結果では、物流事業者において情報セキュリティの重要視度合いについて「３ＰＬ事業推進にあたり、極めて重要なポイントである」と回答した割合は５７％、「３ＰＬ事業におけるほかの機能とほぼ同様に検討すべきポイントである」と回答した割合は３６％であった。一方荷主企業では、３ＰＬ事業者を選定する際における情報セキュリティの重要視度合いについて「極めて重要なポイントである」との回答が４５％、「他の条件とほぼ同様に検討すべきポイントである」と回答した割合が４０％であった。これらの結果より、３ＰＬ事業における情報セキュリティは、荷主からも重要視されていると同時に、３ＰＬ事業者においても重視すべきポイントであると認識されていることがわかる。

２．情報セキュリティ対策に関する課題

物流事業者

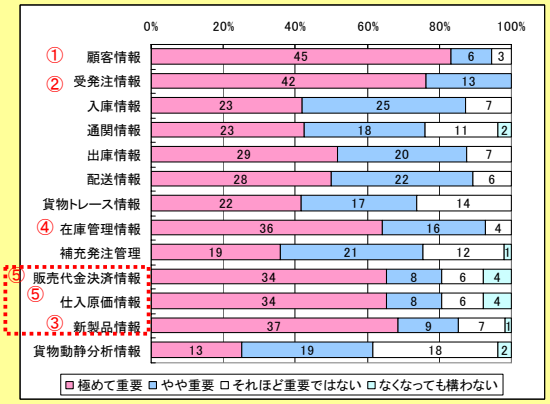
Q3　荷主と交換する情報



グラフ中の数値は社数

荷主企業

Q3　3PL事業者と交換する情報

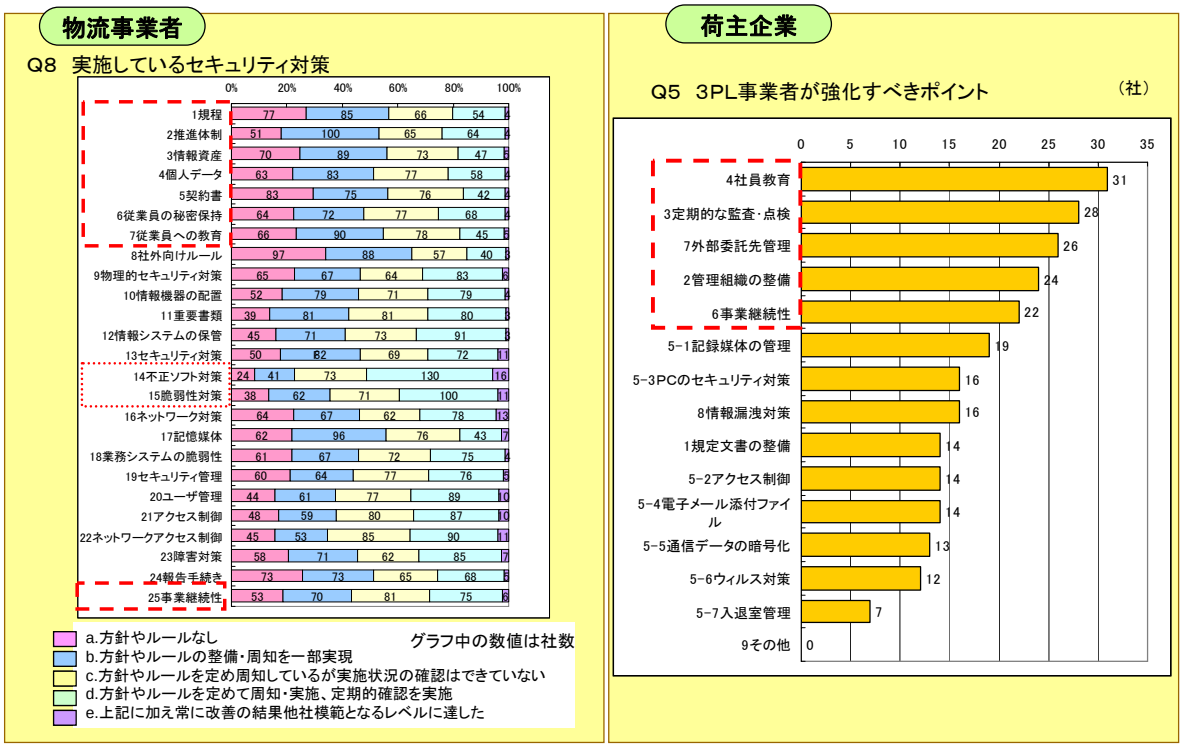


グラフ中の数値は社数

３ＰＬ事業において荷主と交換する情報の重要性認識に関するアンケートでは、「極めて重要」「やや重要」の回答を合計すると、物流事業者、荷主業者ともに顧客情報、受発注情報、在庫管理情報、入庫情報、出庫情報、配送情報が上位６位を占めており、両者の情報の重要度に対する認識は合致していると思われる。

しかしこの中で「極めて重要」と回答した情報（上図の①～⑤）にのみ着目すると、荷主企業では上位５位に入っている新製品情報（第３位）、販売代金決済情報、仕入原価情報（第５位）は、物流事業者においては６位以下との認識であり、ここに両者の意識の乖離が見られる。

荷主企業が安心して業務委託できる３ＰＬ事業者を目指すにあたり、荷主にとって何が重要な情報であるかを的確に認識し、情報セキュリティ対策を講じるにあたってはこれらの情報について特に留意することが必要である。取扱う全ての情報に対して高度なセキュリティ対策を講じることは事実上困難である。そのため、重要な情報が何か、そしてこの情報を取扱う上でどのようなリスクが生じる可能性があるのかを分析し、対応策にメリハリをつけることが、情報セキュリティ対策における費用対効果を最大にするためにも重要な点であると考える。



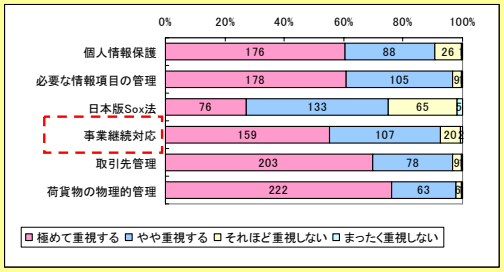
情報セキュリティ対策に関し、荷主企業が３ＰＬ事業者に対してあまり実施できていない／強化すべきと考えるポイントとして挙げている上位５位は、「社員教育」「定期的な監査・点検」「外部委託先管理」「管理組織の整備」「事業継続性」である。具体的なセキュリティ対策そのものもさることながら、それ以上に企業としての組織的な対応を望んでいることが伺える。

物流事業者におけるセキュリティ対策実施状況は、「規程整備」、「推進体制整備」、「情報資産の重要性レベル分け管理」、「個人データ等重要な情報の業務工程ごとの対策措置」、「業務委託時の契約書へのセキュリティ事項記載」、「従業員へのセキュリティ義務の明確化」、「従業員への教育」といった、情報セキュリティに対する組織的な取り組み状況については、実施度合いが低い。一方で「不正ソフトウェア（ウィルス等）対策」、「ソフトウェアの脆弱性に対する定期的な修正プログラムの適用」といった、通信ネットワークおよび情報システムの運用管理、情報システムへのアクセス制御など、情報システムに対する具体的な対策の実施度合いが高い。

このことから、今後３ＰＬ事業者としては、企業としての情報セキュリティガバナンスを効かせるための組織的対応態勢を整備していくことが必要と考える。

物流事業者

Q1　3PL事業に際し、重視するポイント

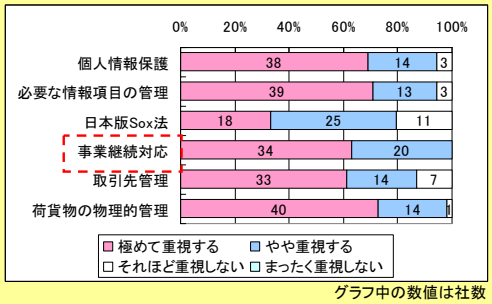


グラフ中の数値は社数

（有効回答：個人情報保護：292社、必要な情報項目の管理：293社、
日本版SOX法：279社、事業継続対応：288社、取引先管理：291社、
荷貨物の物理的管理：292社）

荷主企業

Q1　3PL委託に際し、重視するポイント



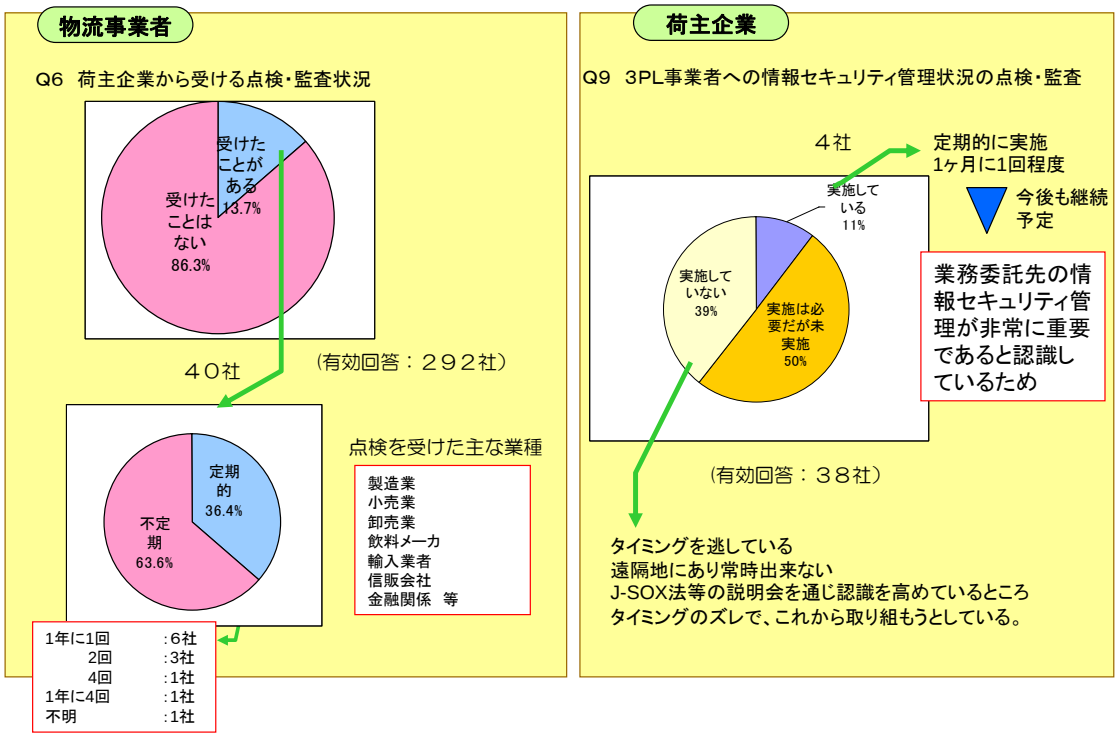
グラフ中の数値は社数

(有効回答：個人情報保護：55社、必要な情報項目の管理：55社、
日本版SOX法：54社、事業継続対応：54社、取引先管理：54社、
荷貨物の物理的管理：55社）

荷主企業は災害時における３ＰＬ事業者の事業継続性についてもほぼ全社が重要視していることがわかる。一方で物流事業者も同様に重視しているものの、５％程度の事業者は「それほど重視しない」「まったく重視しない」という回答であった。

この結果は、前図の荷主企業が「３ＰＬ事業者に対してあまり実施できていない／強化すべきと考えるポイント」「物流事業者が実施しているセキュリティ対策」の結果にも表れている。荷主企業としては委託先の事業継続対応が重要なポイントであるが、物流事業者はまだまだこれに対応できていないという実態がある。

災害時等緊急時の対応計画については、初期対応、暫定対応、復旧手順について定めた対応計画（事業継続計画）を定めることが必要である。事業継続の範囲や対応の即時性等は荷主企業業務への影響が大きいことから、対応計画については荷主企業と内容について十分に検討を行い、対応範囲と手順を明確に合意しておくことが必要と考える。



荷主企業による３ＰＬ事業者への情報セキュリティ管理状況に関する点検・監査の実施状況は、「実施している」が１１％、「実施は必要と思うが実施していない」が５０％、「実施していない」が３９％であった。

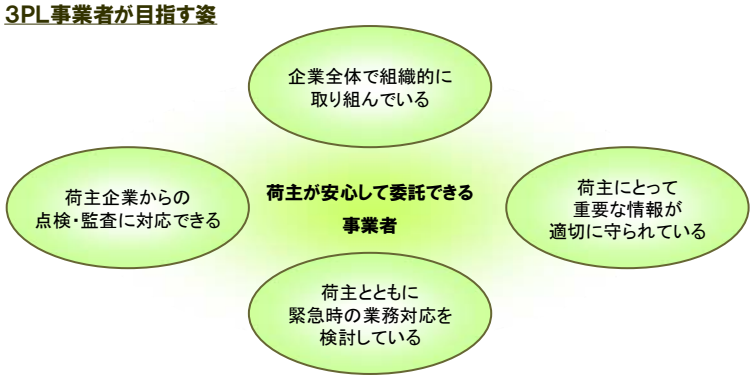
「実施している」うち４社は、１ヶ月に１回程度定期的に実施しており、実施の理由としては「業務委託先の情報セキュリティ管理が非常に重要であると認識しているため」としている。

一方「実施していない」理由として、必要ないと考えている以外に、「タイミングを逃している」「遠隔地にあり常時実施できない」「タイミングのズレ」など、実施の意思はあるが今後の課題との回答があった。

また物流事業者も１３．７％が荷主から点検・監査を受けた経験を持ち、うち３６．４％は定期的に実施されている。

これらのことから、荷主企業におけるコーポレートガバナンスへの取り組みの向上、情報セキュリティに対する意識向上、などの潮流から、今後業務委託先である３ＰＬ事業者への情報セキュリティに関する点検・監査を実施する企業が増加することが考えられる。

以上のアンケート結果より、情報セキュリティ面から荷主が安心して委託できる３ＰＬ事業者としてのポイントは以下の４点であると考える。



①企業全体で組織的に取り組んでいる

全社的に情報セキュリティ意識を浸透させ、情報セキュリティ上各従業員がやるべきことを明確にすると同時にこれらを確実に実施するためには、企業全体で組織的に情報セキュリティに取り組む必要がある。規程を整備し、管理組織体制を構築し、従業員への浸透教育を実施することは、３ＰＬ事業者が荷主の信頼を得るために必要な取り組みである。

②荷主にとって重要な情報が適切に守られている

荷主が業務上重要と認識している情報を、適切に管理することが必要である。そのためには、取扱う情報の重要度を的確に把握し、委託業務においてこれらの情報がおかれている状況を把握することでリスクを分析し、リスクに応じた対応策を講じることが必要である。これにより情報セキュリティ対策に関し、より高い費用対効果を得ることができる。

なお、重要度を把握するためには、荷主とコミュニケーションをとり、荷主から提供される各種情報の重要度を明確化することが望ましい。

③荷主とともに緊急時の業務対応を検討している

災害等の緊急事態発生時、受託している業務に関してどのような対応をするかについて検討し計画を策定することは、３ＰＬ事業者および荷主企業の業務への影響を最小限にするために必要なことである。計画を策定する際には、対応範囲や復旧手順、復旧時期等について荷主企業と十分に検討を行った上で定めることが、緊急事態発生時に荷主企業とのトラブルを避け速やかに復旧作業を進める意味でも必要と考える。

④荷主企業からの点検・監査に対応できる

荷主企業において３ＰＬ事業者の情報セキュリティ管理状況が重要な選定基準のひとつ

となってきていると同時に、これまでの委託先に対しても今後点検・監査は増加傾向になると考えられる。このことから、荷主から情報セキュリティに関する点検・監査を受けることを想定し、規程や組織体制の整備に加え、自社で点検等を実施しその結果を提出するなど、荷主に対する自社の情報セキュリティ管理状況に関する報告・情報発信の方法を検討することが望ましいと考える。

また情報発信の手段としては「ＩＳＭＳ（情報セキュリティマネジメントシステム）認証」の取得、「プライバシーマーク」の取得など、情報セキュリティ等に関する第三者認証制度を活用することも有効であろう。

以上の点について、「情報セキュリティガイドライン」においても網羅した内容とした。これらのポイントに留意し、本ガイドラインに基づいて各企業に最適な情報セキュリティ管理を実施することを期待する次第である。

Ⅵ．情報セキュリティガイドライン

１．情報セキュリティ管理組織体制

■情報セキュリティを管理する組織・体制を整備・確立すること。
■各管理者、責任者の責務を明確にすること。

情報セキュリティを推進するためには、全社統一的に管理を行うための組織・体制を構築することが必要である。当該組織は、各事業者の情報セキュリティ管理規程を定めるとともに、これを全社的に運用・推進するための責務を担うものである。

組織体制としては、全社的な情報セキュリティ管理の責任者を設置するとともに、各部署、現場に情報セキュリティ管理のための責任者を置き、情報セキュリティの管理および推進を行う。

組織体制として設置した各管理者、責任者について、各々の情報セキュリティ管理上の責務を明確にする。

組織および責任者の種類および責務の例としては、以下が挙げられる。

○情報セキュリティ管理責任者

事業者の情報セキュリティについて総括的な責任を持つ。全社的な情報セキュリティ方針の策定および推進を行う責務を負う。経営者、役員などが当該管理責任者となる。

○情報セキュリティ管理者

所管業務における情報セキュリティの実施を管理する責務を負う。および営業所長など現場の管理者や、本社各部課の部課長などが当該管理者となる。

社員やパート・アルバイト、派遣社員等を含む全従業員にまで管理が行き届くような組織体制を構築しなければならないことから、上記例を参考に組織および責任者の種類については、自社の規模や特性を鑑みて各事業者に最適なものを構築することが必要である。

２．情報セキュリティ規程類の整備

■情報セキュリティ基本方針を策定すること。
■情報セキュリティ基準または実施手順書を策定すること。

３ＰＬ事業者の情報セキュリティ管理に関する取り組み姿勢、および実施内容について定めた、情報セキュリティ管理に関する規程文書を定めることが望ましい。

当該規程類を文書で定めることで、全従業員が情報セキュリティ管理として実施しなければならないことを明確に知ることができると同時に、荷主企業に対しても適切な管理が実施されている事業者であると示すことができる。

情報セキュリティ規程は一般的には、以下の 3 段階で作成される。

○情報セキュリティ基本方針（情報セキュリティポリシー）

事業者としての情報セキュリティの重要性認識と、これに対する企業としての取り組み方針を記述したもの。

情報セキュリティ基本方針は、経営者によって承認され、全従業員に周知する。

○情報セキュリティ基準（情報セキュリティスタンダード）

情報セキュリティ基本方針に従い、情報セキュリティ上実施すべき事項について具体的に記述したもの。

○情報セキュリティ実施手順（情報セキュリティプロシジャ）

情報セキュリティ基準に従い、実施すべき事項についてより詳細かつ具体的に記述したもの。現場従事者が参考できるよう業務ごとに作成されることが多く、日常の業務において実施すべき事項を記述する。

しかし、規程類については必ずしも上記 3 段階で策定する必要はない。日常業務にて各従業者が実施すべき事項について体系的に文書化し、企業としての取り組み内容を明確化する目的で策定することから、事業者の規模や特性に応じて、段階を多くまたは少なく設定してもよい。

３．情報の漏洩防止策

■対象となる情報資産を洗い出すこと。
■情報資産の重要度およびリスク分析の結果に応じて対応策を検討すること。

情報の漏洩防止策を講じるにあたり、管理対象となる情報資産の重要性について分析を行い、重要度の高い情報についてはより高いセキュリティ対策を講じなければならない。情報セキュリティ対策にメリハリを付けて効果的な投資を行うためには、まず各事業者において守るべき情報が何かを洗い出し、明確化する必要がある。そのうえで、洗い出された各情報資産の重要度と、保管・移送状況などに応じてリスクの分析を行い、対応策を検討することが望ましい。

３ＰＬ事業においては特に、荷主から預かっている情報や、荷主とやりとりする情報については留意することが必要である。以下の情報は特に重要であることから、取り扱い場面や、保管・移送の状況に応じて情報漏洩に対する具体策を定める必要がある。

・顧客情報
・受発注情報
・在庫管理情報
・入出庫情報
・配送情報

また流通加工業務を実施する３ＰＬ事業者は、上記情報に加え、値付けに関する情報、新製品に関する情報、なども取扱う可能性がある。また、複数の会社の同様の情報を扱う可能性も高い。これらの情報は荷主企業にとっては他社との差別化を図るための非常に重要な情報であることから、外部または他社に漏洩することのないよう、対策を講じることが必要である。

対象となる情報（守るべき情報）は、「情報資産管理台帳」のような形でとりまとめ、取り扱い場面や保管・移送状況などについて整理しておくと、情報セキュリティ管理を継続的に実施する上で有効である。「情報資産管理台帳」には、情報の重要度、保管場所、情報項目、保管方法、保管期限、セキュリティ対策の状況、などについて記入することで、当該情報がさらされているリスクについて分析を行い、適切なセキュリティ対策の実施に資することができる。

なお、重要度を把握するためには、荷主とコミュニケーションをとり、荷主から提供される各種情報の重要度を明確化することが望ましい。

３．１．情報の保管

■重要度に応じた情報保管方法を明確にすること。
■重要度の高い情報は、特定者しか利用できない場所に保管すること。
■重要度の高い情報は、バックアップまたは複写の必要性を検討し、必要がある場合にはバックアップまたは複写を取得すること。バックアップまたは複写した情報についても、原本と同様の情報漏洩策を講じること。

情報の保管場所は、重要度に応じて定める必要がある。特に、重要度の高い情報については、保管場所から情報が漏洩することがないよう、保管方法および保管場所を定める必要がある。この際、「３．２．情報の利用制限」と併せて、保管されている情報を取扱うことができる者を制限することも必要である。

また、業務継続性の観点から、業務上重要度の高い情報については、バックアップまたは複写の必要性について検討する。バックアップ・複写の検討にあたっては、これらの保管に必要な場所や資源、バックアップ／複写した情報の漏洩防止

策などについても考慮に入れ、必要性について十分検討することが必要である。

３．２．情報の利用制限

■情報の重要度に応じて、利用できる者を制限すること。
■情報の種類に応じて、利用できる者を制限すること。

情報の漏洩を防止するためには漏洩の機会を最小化するため、情報の取り扱い者を制限し、取り扱い担当者以外の者が取扱うことのないようにすることが望ましい。

利用者の制限は、当該情報の重要度や種類に応じて定める。例えば、重要度が高い情報に関しては役職者のみ取り扱い可能とする、営業所ごとに担当荷主の情報のみ取り扱い可能とする、等が考えられる。

制限の方法については、紙や外部記憶装置[6]に保存されている情報については施錠できる場所に保管して鍵を責任者が管理する、パソコンや情報システムなどで出力する情報については ID／パスワードを設定してパソコンや情報システムを取扱うことができる者を制限する、などの方法がある。具体的な制限方法については、情報の種類や取り扱い場面に応じて実行可能な最適な対策を講じることが必要である。

３．３．ＩＤ・パスワードの管理

■ＩＤ・パスワードの管理方法を明確化すること。
■パスワードは推測されにくいものとし、定期的に変更すること。
■ＩＤ・パスワードの不正利用を察知した場合の対応方法を明確化すること。

パソコンや情報システムのＩＤ・パスワードは、情報の取扱いを制限するために設定されるものであることから、情報漏洩を防ぐための入り口である。このことから、ＩＤ・パスワードの利用者における管理方法について明確に定め、これを全利用者に周知徹底しなければならない。

ＩＤ・パスワードの管理方法として明確化すべきものとしては、以下が挙げられる。

○ＩＤ・パスワードの発行・削除方法

当該パソコンや情報システムを利用する人を必要最小限に限定し、必要な者に対してのみＩＤ・パスワードを発行すること。また、退職等により不要になった場合には、速やかに当該ＩＤ・パスワードを削除すること。

○ＩＤ・パスワードの利用方法

---

[6] 外部記憶装置とは、CD、DVD、フロッピィディスク、USB メモリなど、電子データを保存することができる持ち運び可能な媒体のことである。大量のデータを保存することができるため、保存するデータによっては取扱いに十分注意する必要がある。

同一のＩＤ・パスワードを複数人で共有することがないようにすること。

○ＩＤ・パスワードの保管方法

ＩＤ・パスワードは各利用者が他者に知られないように責任を持って管理することとし、パスワードを紙等にメモし、見やすいところに貼るなどの行為を行わないようにすること。

また、パスワードは他者が推測されにくいものにし、定期的に変更するよう、指導することが必要である。

さらにＩＤ・パスワードが盗難される、または当該ＩＤ・パスワードを使って不正にパソコンや情報システムが利用されたことを発見した場合の対応方法について、管理責任者への報告手順などを明確に定め、これを全利用者に周知することが必要である。

３．４．電子メール・インターネットの利用

■電子メールの利用方法について定めること。
■インターネットの利用方法について定めること。

電子メールやインターネットは荷主との情報交換や情報収集に用いられるツールであるが、コンピュータウィルスへの感染や、誤送信などにより、情報漏洩につながる危険性がある。電子メールやインターネットの利用方法については、これに伴う危険を認識した上で、従業員に対して注意喚起を行うとともに、利用方法および利用制限に関する具体的な指導を行うことが必要である。

３．５．ウィルス対策

■パソコンにはウィルス対策ソフトをインストールすること。
■ウィルス対策ソフトの定義ファイルを定期的に更新し、常に最新の状態にすること。
■定期的にウィルスやスパイウェア検索を行うこと。
■パソコンがウィルスに感染した場合の対処方法について、周知徹底を行うこと。

電子メールやインターネット、外部記憶装置などを介してコンピュータウィルスに感染すると、情報漏洩や業務妨害などにつながる危険性があり、取引先にも被害が拡大することが考えられる。そのため、ウィルス対策ソフトを導入し、定期的に検索することで、感染を予防することが必要である。

ウィルスは日々進化しているため、ウィルス対策ソフトは一度インストールしたままではなく、定期的に定義ファイルを更新し、最新のウィルスに対応できるようにすることが必要である。

また、パソコンがウィルスに感染した場合の対処方法について具体的に定め、

全従業員または全利用者に周知徹底を図ることが必要である。

３．６．パソコンや外部記憶媒体の持ち出し

■ノートパソコンや外部記憶媒体の社外への持ち出しに関する管理方法を明確にすること。

ノートパソコンや外部記憶媒体は、小型ながら大量のデータが保存されており、紛失から大量の情報漏洩につながる危険性があることから、本来あるべき場所からの持ち出しには十分に留意することが必要である。やむを得ない場合以外は社外に持ち出さない、持ち出す場合には管理責任者の許可を得る、移動中は手放さない、など具体的な管理方法を定め、全従業員に周知徹底を図ることが必要である。

また、例えばある荷主向けの流通加工業務に携わる従業員が、販売価格や新製品に関する情報を外部記憶媒体に入れて外部に持ち出したり、他の荷主企業向けの作業エリアに持ち出すことがないよう、「３．７．入室管理」と併せて管理を行うことも有効である。

３．７．入室管理

■場所ごとに許可された者以外が入室できないように入室管理を行うこと。

■重要度の高い情報が保管されているエリアについては、特に厳重な入室管理を行うこと。

事務所や倉庫、作業場所など、出入りする社員または外部者と、そこで取扱う情報の重要度とを検討した上で、必要と判断した場合には許可された者以外は出入りできないような管理を行うことが必要である。特に部外者の出入りにあたっては、入退室管理簿をつけるなどにより、誰がいつどのような目的で出入りしたかがわかるようにすることが必要である。

また、当該エリアで取扱う情報の重要度によっては、社内であっても限られた者しか入室できないような特別なエリアを設けて厳重な管理を行うことが必要である。

３．８．情報の廃棄

■紙情報の廃棄ルールについて明確に定めること。

■パソコンや外部記憶媒体の廃棄ルールについて明確に定めること。

情報廃棄の管理不足により情報が漏洩してしまうことは少なくない。重要な情報についてはシュレッダーなどにより復元に困難な状態にして廃棄する、大量の情報廃棄の場合には廃棄業者に委託し、焼却または溶解処分するなど、重要度に

応じた廃棄方法を明確に定めることが必要である。

パソコンや外部記憶媒体は、システム上の「ごみ箱」にデータを移動する、「削除」するなどの操作を行っても、データを復元することが可能であることから、重要な情報が保存されていたものに関しては、削除のための特別なソフトウェアを用いてデータを完全消去する、もしくは物理的に破壊するなどの処理が必要である。特にパソコンをリースやレンタルしており返却する際には、データの廃棄について十分注意することが必要である。

これらの廃棄ルールについて明確に定め、全従業員に周知徹底することが必要である。

４．外部委託管理

■外部委託先の選定にあたっての選定手続および選定基準を明確にすること。
■外部委託先に重要な情報を委託する場合には、当該情報の安全管理を図られるよう、必要に応じて指導および監督を行うこと。

３ＰＬ事業者からさらに外部に業務の一部または全部を委託する場合、外部委託先にて情報漏洩等の事故が発生した場合は３ＰＬ事業者も荷主から責任を問われる可能性がある。このことから、外部委託を行う場合には、委託先の情報セキュリティ管理に関して、事前に確認する必要がある。情報セキュリティ管理に関する項目も含めた、外部委託先の選定基準について定めておくことが望ましい。

また、外部委託先との委託契約書において、自社に準ずる情報セキュリティを講じる等の情報セキュリティに関する要求事項について、明確に定めておくことも有効である。

また、重要な情報を委託する場合には、必要に応じて委託先の管理状況を視察、指導するなどの方法をとることが望ましい。

５．事業継続計画

■緊急事態発生時の対応計画（事業継続計画）について定めること。
■緊急事態発生時の組織体制について定めること。
■緊急事態発生時の初期対応、暫定対応および復旧手順について定めること。
■事業継続計画は最新の状況に対処するため、定期的に実行訓練を行い見直すこと。

３ＰＬ事業者にとって、受託業務を行う上で情報システムは大変重要である。

地震などの大規模災害や、火災・水害などの局所災害発生時の対応について、予め手続を明確に定めておくことが必要である。被災時の業務中断は荷主企業の業務にも影響を及ぼすことから、受託業務の重要性を分析し、中断時の暫定的な対応方法、早期復旧に向けた対応手順などについて、具体的に定めておくことが必要である。

また緊急事態発生時の対応方法については、荷主企業とも普段から話し合い、荷主企業も含めた対応計画を作成することが望ましい。

６．研修・教育の実施

■情報セキュリティ規程の内容に関して従業員に周知・徹底するための研修・教育を実施すること。
■研修・教育は、経営者、社員、契約社員等を含む全従業員に対して実施すること。

情報セキュリティ規程に策定した、情報セキュリティ対策内容について、全従業員が知り、実施するよう、全従業員を対象とした研修・教育を実施することが必要である。

規程を定めたり組織体制を構築するだけでなく、実際にこれを運用し、３ＰＬ事業実施の現場においてこれを実践していくことが最も重要である。このためには、情報セキュリティ対策がなぜ必要で、具体的に何を実施するべきなのか、従業員に研修・教育を通じて徹底していく必要がある。

研修・教育の内容としては、以下の例が挙げられる。

〔研修・教育内容例〕

- 情報セキュリティに対する認識を高めるための一般研修
- 自社における規程、組織体制、取組状況に関する企業研修
- ３ＰＬ事業現場において実施すべき事項に関する現場研修
- 情報システムなど専門業務に携わる人に対する専門研修

情報セキュリティに関する一般的な内容の研修・教育は、業界団体や専門業者が主催している社外セミナー等を活用することも考えられる。しかしこの場合も、同社としてどのような規程を設けており、具体的に何をしなければならないかについては各事業者にて従業員に周知・徹底するための研修・教育を実施することが必要である。全員が同じ教育を受けて認識を共有することが重要である。

さらに、情報システム管理など情報セキュリティ上特別に留意すべき業務に従事している従業員に対しては、より専門的かつ詳細な内容で研修・教育を行うことが望ましい。

７．事件・事故発生時対応

■事件・事故発生時の対応方法について、具体的な手順を明確に定め、全従業員に周知・徹底すること。
■事件・事故発生時の連絡先や連絡手段について明確化しておくこと。

情報セキュリティに関する情報漏洩などの事件や事故が発生した場合に備え、連絡先や連絡方法、対応方法などについて予め具体的に定めておくことが必要で

ある。また事件・事故の内容によっては、全社的な対応をとるための対策委員会を招集し、対応を検討することも必要である。

特に事件・事故の内容によっては荷主への影響も考えられることから、事件・事故発生時の速やかな報告と対処は必須である。事件・事故発生時の対応方法については、荷主企業とも普段から話し合い、荷主企業も含めた対応計画を作成することが望ましい。

８．監査・点検

■情報セキュリティ対策の実施状況について、定期的に点検を行うこと。
■必要に応じて、社内または社外の第三者の情報セキュリティに関する監査を受けること。

情報セキュリティ対策の実施状況について、定期的に点検し評価を行うことは、情報セキュリティ対策を継続的に運用していく上で重要である。策定した情報セキュリティ規程や対策が現場にて実施できているかどうかを点検・評価し、実施できていない場合は指導強化する必要がある。また、点検・評価することにより、定めた対策自体が現場業務に即さない場合も明らかになることから、現場実態に即した実効性のある情報セキュリティ対策を講じるためにも有効である。

現場における点検は、例えば年１回程度、チェックリストを用いて実施することが考えられる。さらに各現場の結果を全社的にまとめて状況を分析することも有効である。

また、必要に応じて第三者の監査を受けることで、対策が適切に実施されているかを客観的な視点から確認することが望ましい。

これらの監査・点検は実施するだけではなく、結果を分析することが最も重要である。結果を受けて、指導強化や対策の見直しなどを繰り返し実施することで、情報セキュリティ管理を向上していくことができる。

Ⅶ. おわりに

物流事業者が３ＰＬ事業を実施するにあたり、荷主企業の情報を取り扱うことなしに、３ＰＬ事業を遂行することはできない。また、受託業務の拡大とともに取扱う情報の種類も多様化する。そこで取扱う情報について整理して重要度を可視化し、これに基づいて適切な情報セキュリティ対策を講じることが、物流事業者と荷主企業双方にとって有効である。

本ガイドラインの内容は、３ＰＬ事業者として実施すべき基本的な情報セキュリティ管理について述べたものである。実現の方法についてはさまざまな対応策があることから、自社の規模や特性を分析した上で、自社に最適な対策を定めることを切に望む次第である。

Ⅷ. 参考資料

○物流分野における情報セキュリティ確保に係る安全ガイドライン（国土交通省）
○情報セキュリティマネジメントシステム適合性評価制度　ISMS 認証基準（財団法人情報処理開発協会）