「中小企業の情報セキュリティ対策ガイドライン」 ー「組織的な情報セキュリティ対策ガイドライン」より

情報セキュリティ対策チェックリスト

項目番号	内容	チェック
1. 情報セキュリティに対する組織的な取り組み状況		
1-1	情報セキュリティに関する経営者の意図が従業員に明確に示されていますか？	□
1-2	情報セキュリティ対策に関わる責任者と担当者が明示されていますか？	□
1-3	管理すべき重要な情報資産を区分していますか？	□
1-4	重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定めていますか？	□
1-5	外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取っていますか？	□
1-6	従業者（派遣を含む）に対してセキュリティに関して就業上何をしなければいけないかを明確にしていますか？	□
1-7	情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与えていますか？	□
2. 物理的セキュリティ		
2-1	重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行っていますか？	□
2-2	重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人的災害に配慮し適切に配置･設置していますか？	□
2-3	重要な書類、モバイル PC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行っていますか？	□
3. 情報システム及び通信ネットワークの運用管理状況		
3-1	情報システムの運用に関して運用ルールを策定していますか？	□
3-2	ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行っていますか？	□
3-3	導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行っていますか？	□
3-4	通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施していますか？	□
3-5	モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施していますか？	□
4. 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況		
4-1	情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理（パスワードの管理など）を行っていますか？	□
4-2	重要な情報に対するアクセス権限の設定を行っていますか？	□
4-3	インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISP サービス　等）を行っていますか？	□
4-4	無線 LAN のセキュリティ対策（WPA2 の導入等）を行っていますか？	□
4-5	ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行っていますか？	□
5. 情報セキュリティ上の事故対応状況		
5-1	情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握していますか？	□
5-2	情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の緊急時に、何をすべきかを把握していますか？	□

情報セキュリティ対策ベンチマーク ver.3　25 項目の質問一覧

大項目１．情報セキュリティに対する組織的な取組状況	
①	情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。
②	経営層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか。
③	重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱いをするための方法を定めていますか。
④	重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。
⑤	外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。
⑥	従業者（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。
⑦	経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施していますか。
大項目２．物理的（環境的）セキュリティ上の施策	
①	特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。
②	顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。
③	重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。
④	重要な書類、モバイル PC、記憶媒体などについて適切な管理を行っていますか。
大項目３．情報システム及び通信ネットワークの運用管理	
①	情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。
②	情報システムの運用に際して、必要なセキュリティ対策を実施していますか。
③	不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエアなど）への対策を実施していますか。
④	導入している情報システムに対して、適切なぜい弱性対策を実施していますか。
⑤	通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。
⑥	モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。
大項目４．情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況	
①	情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理、利用者の識別と認証を適切に実施していますか。
②	情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。
③	ネットワークのアクセス制御を適切に実施していますか。
④	業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。
⑤	ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。
大項目５．情報セキュリティ上の事故対応状況	
①	万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。
②	情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。
③	何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。

「中小企業の情報セキュリティ対策ガイドライン」

ー「委託関係における情報セキュリティ対策ガイドライン」より

委託先における情報セキュリティ対策事項

本紙は、委託元が委託先に確認する情報セキュリティ対策事項で、「情報セキュリティ対策は別途定める～による。」というような契約時において示される別紙の例である。

注）機密保持条項（例示案）との整合性は取っていない

委託元から委託先に開示する機密情報（以下「機密情報」という）の管理に関し、委託先が実施する情報セキュリティ対策の事例を示す。なお、具体的に多くの事例を示すため事例相互の整合性は保証されていないので、適宜選択すること。

委託契約では、機密情報の取扱に関して、必要かつ適切な安全管理措置について、委託者、受託者双方が同意した内容を事前に具体的にする必要がある。具体的な実施策がなく、委託元が委託先に対して、事故が発生した場合の損害賠償のことについてだけしか契約に盛り込まないということは望ましくない。

これらの事例を参考に、機密情報の種類、業務委託関係などの諸条件を考慮して、委託元は、委託先と協議のうえ、委託先が実施する適切な情報セキュリティ対策を指示すべきである。

1. 情報セキュリティに対する組織的な取組み

1.1 機密情報の利用、保管、持ち出し、消去、破棄における取り扱い手順を定める

- ✧ 機密情報は、他の情報と区別して保管すること。
- ✧ 機密情報の管理者を定めること。
- ✧ 機密情報にアクセスできる人の範囲を定めること。
- ✧ 最新の従事者（管理責任者を含む）を「従事者台帳」で管理すること。
- ✧ 機密情報を受領した場合には、「機密情報管理台帳」に記録すること。
- ✧ 機密情報の利用記録を残しておくこと。
- ✧ 機密情報を複製または電子メールで送信する場合には、事前に委託元の承認を得ること。
- ✧ 機密情報を複製または電子メールで送信した場合には、「機密情報管理台帳」に所在地およびその管理者を記録すること。機密情報および機密情報を取り扱う機器の保安区分外への持ち出しは禁止すること。
- ✧ 機密情報を持ち出す場合、事前に委託元の承認を得ること。
- ✧ 機密情報を持ち出す場合、事前に機密情報の管理者の承認を得ること。
- ✧ 機密情報を持ち出す場合、ファイルの暗号化を行うこと。
- ✧ 機密情報を格納する記憶媒体は、セキュリティロック機能を有すること。
- ✧ 持ち出しの利用を終えた機密情報は、正しく消去されているか確認すること。
- ✧ 機密情報を扱う業務の担当を外れた従業者（管理責任者を含む）が保有していた機密情

報の廃棄・消去を確認すること。

- ✧ 機密情報および機密情報が化体された物（試作品等）の廃棄手順を定めること。
- ✧ 委託業務の終了時、機密情報が安全に廃棄、消去されたことを示す記録を整備すること。また、委託元に報告すること。
- ✧ 機密情報を格納していたサーバを廃棄、売却またはリース返却する時は、データ消去ツールなどでデータの完全消去を行うこと。
- ✧ バックアップのルールを定め、定期的に実施すること。機密情報を扱う情報システムの全てのバックアップ媒体は、機密区分に応じた管理を行うこと。
- ✧ 機密情報を含む裏紙は利用しないこと。
- ✧ 機密情報が記された FAX、プリントアウトその他の書類が長時間放置されたままにならないようなルールの運用をすること。
- ✧ 情報セキュリティが適正に維持、運用されていることを確認するため、定期的に確認すること。
- ✧ 定期的に機密情報取り扱い業務の内部点検を実施すること。

1.2 機密情報に係る業務の再委託に関する事項を定める

- ✧ 業務の再委託を行う場合は、実施理由・必要性、内容、再委託先についての書面を事前に委託元に提出し承認を得ること。
- ✧ 再委託先と機密保持に関する契約を締結すること。委託元から委託先に求める情報セキュリティ要求事項と同等の内容を含めること。

  項目例：

  ＊守秘義務
  ＊機密保持の対象となる情報の範囲
  ＊守秘義務期限
  ＊使用目的の制限
  ＊アクセス者は必要最小限に限定
  ＊機密情報の管理方法
  ＊機密情報の複製の制限
  ＊委託契約終了後の機密情報の返却または廃棄の規定
  ＊委託元からの機密保持に関する確認措置の規定
  ＊契約違反時の措置
  ＊無断での再委託の禁止
  ＊私用 PC の業務使用禁止
- ✧ 機密情報に係る再委託先との業務について手順を文書化すること。

- ✧ 再委託先における情報セキュリティ対策が適切に維持・運営されていることを定期的に確認すること。
- ✧ 機密情報を再委託先に開示する場合には、機密情報であることを明示すること。
- ✧ 再委託先への機密情報の受け渡しに関する記録を行うこと。
- ✧ 再委託先への機密情報の受け渡しに際し、暗号化を行うこと。
- ✧ 再委託先に開示した機密情報の廃棄・消去に関する記録を再委託先から取得すること。

1.3 機密情報を扱う従事者に対して遵守事項の周知と、情報セキュリティに関わる知識習得の機会を与える

- ✧ 機密保持に関する遵守事項を従事者に周知させること。
- ✧ 機密保持を実践するために必要な教育を定期的に行い、受講記録を作成すること。
- ✧ 機密情報を公衆の場（居酒屋や電車の中など）で公言しないこと。

2 物理的セキュリティ

2.1 機密情報を保管および扱う場所の入退管理と施錠管理を行う

- ✧ 機密情報を保管および扱う区域を定めていること。
- ✧ 機密情報を保管している部屋（事務室）又はフロアーへの侵入を防止するための対策を行っていること。
- ✧ 機密情報を保管している部屋（事務室）又はフロアーに入ることができる人を制限し、入退の記録を取得していること。
- ✧ 機密情報が格納された記憶媒体、紙資料、ノート PC 等は施錠管理すること。
- ✧ 機密情報を取り扱う情報システムを格納するサーバルームへの入退館の記録やサーバへの作業記録を保存し、事故が発生した際、後からトレースできるようにすること。
- ✧ 鍵または ID カードなどの保管や所有について定期的に確認すること。
- ✧ 入退出記録（カメラ画像を含む）を定期的に確認すること。

2.2 機密情報を保管および扱う場所への個人所有物の持込み・利用を禁止する

- ✧ 個人所有の PC・記憶媒体等（※）の持込みを禁止すること
- ✧ 個人所有の PC・記憶媒体等（※）の業務利用を禁止すること。
- ✧ 個人所有の PC の社内ネットワーク接続を禁止すること。
- ✧ 記憶媒体等（※）の利用は会社貸与品のみとし、個人所有の記憶媒体等（※）の利用を禁止すること。

※記憶媒体（SD カード、USB メモリ等）、カメラ付き携帯電話、携帯情報端末（PDA）、

音楽プレーヤーなど

3 機密情報が格納される情報システムの運用管理

3.1 ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行う

- ✧ ウイルス対策ソフトを導入し、パターンファイルの更新を定期的に行っていること。
- ✧ ウイルス対策ソフトが持っている機能（ファイアーウォール機能、スパムメール対策機能、有害サイト対策機能）を活用すること。
- ✧ サーバやクライアント PC について、定期的なウイルス検査を行っていること。
- ✧ ノート PC には、BIOS パスワード、HDD パスワードの設定および暗号化ソフトの導入をすること。
- ✧ Winny 等、組織で許可されていないソフトウェアのインストールを禁止していること。禁止ソフトがインストールされていないか定期的に確認すること。
- ✧ 機密情報をコピーして持ち出さないよう、記憶媒体が接続できない設定とすること。
- ✧ 情報システムの時刻は定期的に同期をとること。
- ✧ 業務に不要な web サイトへのアクセスを制限すること。

3.2 情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行う

- ✧ 脆弱性の解消（修正プログラムの適用、Windows update 等）を行っていること。
- ✧ 不要なサービスの停止など、セキュリティを考慮した設定を実施するなどの対策が施されているかを確認すること。
- ✧ Web ブラウザや電子メールソフトのセキュリティ設定を行うこと。

4 機密情報へのアクセス制御の状況

4.1 機密情報へのアクセスを制限するために、利用者 ID の管理（パスワードの管理など）を行う

- ✧ 機密情報が扱える利用者毎に ID とパスワードを割当て、その ID とパスワードによる識別と認証を確実に行うこと。
- ✧ 利用者 ID の登録や削除に関する規程を整備すること。
- ✧ パスワードは有効期限を設け、定期的に変更すること。また、空白のパスワードや単純な文字列のパスワードを設定しないよう利用者に求めること。
- ✧ 離席する際は、パスワードで保護されたスクリーンセーバーでパソコンを保護すること。
- ✧ PC やサーバ、ネットワーク機器を社内ネットワークに接続する場合は、機密情報管理者の承認を得ること。
- ✧ 従業者への機密情報アクセス権の付与状況を定期的に見直し、必要のないアクセス権を削

除すること。

- ✧
- ✧ 遠隔診断ポートの利用は、保守サポートなどの必要な場合のみに限定すること。
- ✧ 遠隔診断ポートを利用した接続は、認証機能やコールバック機能等を備えるなど、適切なセキュリティ対策を施すこと。

5 情報セキュリティ上の事故対応

5.1 機密情報漏えいが判明した時に、状況を把握し委託元にすみやかに報告する

- ✧ 機密情報漏えい発生時の体制および連絡網を整備し、すべての従事者に周知すること。
- ✧ 機密情報漏えいが発生した場合、漏えいの発生が疑われる場合、または漏えいに至る可能性のある問題が発見された場合には、すみやかに機密情報管理者に報告すること。
- ✧ 機密情報について上記の問題が発生した場合、すみやかに委託元に報告すること。
- ✧ 機密情報漏えいが発生した場合には、委託元と再発防止策を協議し、従事者に周知すること。

「中小企業の情報セキュリティ対策ガイドライン」

ー「委託関係における情報セキュリティ対策ガイドライン」より

―機密保持条項（例示案）の件―

本書は、業務委託をおこなうにあたり取引基本契約書、個別契約書、覚書、NDA、打合せや口頭による確認、また売買契約書、代理店契約書等、あるいは発注書、仕様書等を通じておこなわれる機密情報の取扱いに係る事項を、「業務委託契約に係る機密保持条項（例）」としてまとめたものである。

実務的には、業務委託の内容、取扱われる情報の性質等によって、条項および条項の内容を取捨選択し、また運用上の工夫などにより、過不足の無い実効性ある機密情報管理をおこなわなければならない。また、業務委託先が海外の場合は、法律、商習慣、社会的習慣等が異なるので（日本の取引習慣は通用しないことが多いので）、誤解が生じないよう明確に記述する必要がある。

尚、SaaS や ASP などのサービスを利用する場合であっても、業務委託契約書や SLA（サービスレベルアグリメント）で、機密保持に係る事項を保証させる必要がある。

本書で言うところの機密情報とは、文書、図面、写真、図書、電磁的記録媒体、製品、部品、材料あるいは特定の設備等の「機密を化体している物理的対象物上（内）の情報」を言い、通信途中の情報、頭の中にある記憶、身につけた技能等、物理的所在を明らかにすることが困難な情報を含まない。従って、これらを機密保持の対象とする必要がある場合は、これらを扱うにふさわしい別途の法律等の根拠に基づいた取決め（契約）をおこなう必要がある。

　

「業務委託契約に係る機密保持条項（例）」

甲：委託元
乙：委託先

第○条（機密保持）

１．乙は、本契約の履行にあたり、甲が機密である旨指定して開示する情報および本契約の履行により生じる情報[注]（以下「機密情報」という）を機密として取扱い、甲の事前の書面による承諾なく第三者に開示してはならない。ただし、次の各号のいずれかに該当する情報については、この限りではない。

① 開示を受けたときに既に公知であったもの
② 開示を受けたときに既に乙が所有していたもの
③ 開示を受けた後に乙の責によらない事由により公知となったもの
④ 開示を受けた後に第三者から守秘義務を負うことなく適法に取得したもの
⑤ 開示の前後を問わず乙が独自に開発したことを証明し得るもの

注：「本契約の履行により生じる情報」の取扱いについては、別の条項で規定すること。尚、本契約の履行に伴って乙から甲へ開示等がなされる乙が保有する機密情報がある場合の当該情報の取扱については、別の条項で規定することが望

２．甲が乙に機密である旨指定して開示する情報は、表１（本案では、特に例示しない）の通りである。

なお、表１は甲乙協力し常に最新の状態を保つべく適切に更新するものとする。

３．乙は、甲より開示された機密情報の管理につき、乙が保有する他の情報、物品等と明確に区別して管理するとともに、以下の事項を遵守する。

(1) 機密情報の管理責任者及び保管場所を定め、善良なる管理責任者の注意をもって保管管理する。
(2) 機密情報を取り扱う従業員を必要最小限にとどめ、上記保管場所以外へ持ち出さない。
(3) 機密情報の管理責任者名、機密情報を取り扱う従業員名及び機密情報の保管場所を、○年○月○日までに甲に報告 する。また、報告内容に変更が生じた場合には、変更が生じた月に提出する以下の(8)の具体的管理状況の報告において、当該変更内容を甲に報告する。
(4) (3)にて報告した機密情報を取り扱う従業員に対して本契約の内容を周知徹底させ、機密情報の漏洩、紛失、破壊、改ざん等を未然に防止するための措置を取る。
(5) 甲の書面による承諾を得た場合を除き、機密情報を複写、複製せず、また、機密情報を開示、漏洩しない。但し、政府機関又は裁判所の命令により要求された場合、その範囲で開示することが出来る。なお、その場合には、甲にその旨をすみやかに通知すること。
(6) 機密情報は本契約の目的の範囲でのみ使用する。
(7) 事故発生時には直ちに甲に対して通知し、事故再発防止策の協議には甲の参加を認める。
(8) 委託期間満了時または本契約の解除時、機密情報（(5)に基づく複写、複製を含む）を甲に返却、または自己で廃棄の上廃棄の証拠を甲に報告する。
(9) (8)にかかわらず、甲から返却また廃棄を求められたときは、機密情報（(5)に基づく複写、複製を含む）を甲に返却、または自己で廃棄の上廃棄の証拠を甲に報告する。

(10) 乙は、甲に対して、機密情報の以下の具体的管理状況を毎月月末に報告する。乙は、甲が乙の事務所における機密情報の管理状況を確認するために乙の事務所への立入検査を希望する場合には、当該検査に協力する。また、甲は乙に対して是正措置を求めることができ、乙はこれを実施するものとする。

①委託契約範囲外の加工、利用の禁止の遵守

②委託契約範囲外の複写、複製の禁止の遵守

③安全管理措置状況

第○条（再委託）

１．乙は、本業務（の全部、または一部）を第三者へ再委託する場合、甲の事前の書面による同意を得ずに、再委託してはならない。

２．前項の規定に基づき本業務を再委託する場合、乙は自己が負う義務と同等の義務を再委託先に対して書面にて課すとともに、甲に対して再委託先に当該義務を課した旨を書面により報告し、かつ乙は当該機密情報開示に伴う全責任を負うものとする。また、乙は次項第 3 号の再委託先からの報告を、第○条（機密保持）第３項の具体的管理状況の報告時にあわせて甲に報告する。

３．前項に加え、乙は再委託先から次の各号の同意を得なければならない。また、乙は、当該同意を得た旨を甲に書面で報告する。

①事故発生時には直ちに甲に対しても通知すること

②事故再発防止策を協議する際には甲の参加も認めること

③再委託先における機密情報の具体的管理状況の報告は、甲の閲覧も可とすること

【コメント】

以下に示すような「機密保持条項に関連する他の条項」については、業務委託期間終了又は本契約の解除後も、合理的な期間に渡り存続させることがのぞましい。

第○条（権利義務の譲渡）
第○条（成果の帰属）
第○条（損害賠償）
第○条（法令等の遵守義務）
第○条（協議事項）
第○条（紛争の解決）

また、第○条（守秘義務）の規定は、「業務委託期間終了又は本契約の解除後○年間有効とする」の如く有効期間を示すことがのぞましい。