情報セキュリティ対策

運用規程

協栄コンサルタント株式会社

目　　次

情報セキュリティ対策運用規程

(基本方針)

第1条　情報セキュリティとは、会社の情報システムを取り巻く様々な脅威から情報資産を機密性・完全性・可用性(三大要素)の確保を行いつつ正常に維持する為に必要なセキュリティ対策に取組み、業務活動を継続的かつ安定的に行なえるよう対策を取ることを基本方針に定めます。

・機密性とは、許可された者だけが情報資産にアクセスできる状態を確保する。

・完全性とは、情報資産が正確及び完全であることを常に維持すること。

・可用性とは、許可された者が必要な時に確実に情報資産を利用できること。

1. 情報資産の保護

当社は、情報資産の機密性、完全性及び可用性を確実に保護するために、組織的、技術的に適切な対策を講じます。

2. 法令等の遵守

当社は、情報セキュリティに関する法令、規則を遵守します。

3. 教育・研修の実施

当社は、役員、従業員が、情報資産の重要性を十分に認識するように、必要な教育・研修を実施します。

4. 継続的な改善

当社は、「情報セキュリティ対策運用規程」及び関連する諸規則、管理体制の評価と見直しを定期的に実施し、情報セキュリティ対策の継続的な改善を図ります。

(対策基準)

第2条　取り扱う情報資産について機密性、完全性及び可用性の側面から重要度に応じて技術的対策、物理的対策、人的対策の 3 つに分類し応じた対策を次に講じます。

1. 技術的対策

情報システムやネットワークなどの IT 環境で発生する脅威のことで、不正アクセスやなりすまし、データーの改ざん、コンピューターウィルスなどの脅威となる技術的な対策を行う。

2. 物理的対策

施設や機器などの物理環境で発生する脅威のことで、不正侵入や機器破損、機器故障、停電等の脅威から物理的に保護する。

3. 人的対策

情報の取扱など人手作業で発生する脅威の事で、不正行為やデーターの持ち出し、誤操作などが脅威となるので情報セキュリティに関する権限及び責任者を定め、情報セキュリティ対策基準の内容を周知徹底するなど、役員・従業員への教育及び啓発を行う。

(実施手順)

第3条　会社や組織においては、たった一人の不注意が、ウィルスへの感染や情報漏洩といった脅威に繋がることもあります。役員・従業員の一人ひとりが情報セキュリティ対策の必要性を理解し、自覚を持って取り組むことが必要です。次の実施手順には、それぞれの対策基準ごとに、実施すべき情報セキュリティ対策の内容を具体的に手順として記載しています。役員・従業員は、各項目の内容を参照しながら会社や組織の情報セキュリティ対策に従って下さい。

情報セキュリティ対策
実施手順１

項　　目	対　　策
１保　管	①　機密情報は、他の情報と区別して保管する。 ②　機密情報は机上に放置せず鍵付き書庫に施錠保管する事を原則とし最終退室時には書庫の施錠を確認する。 施錠した鍵については、管理者を明確にする。 ③　機密情報を社内の LAN 上のパソコンに保存する場合は、専用のフォルダを作成しアクセス権の設定を適切に行いデーターの管理者を定める。 ④　パソコンについては、ログイン用のパスワードで管理し、退室時には電源の OFF を確認する。パスワードは定期的に変更する。 ⑤　機密情報のバックアップは、定期的に行ない故障や誤操作で重要情報が消失しないよう対策を取る。外部記憶媒体にデーターを保存する場合は施錠可能な場所に保管する。
2.持ち出し	①　社外業務での機密情報の持ち出しは、情報漏洩事故を引き起こす大きな要因となるのでウッカリ置き忘れの紛失、盗難等にあっても情報漏洩に繋がらないよう情報そのものを他人には触れない、開かない、読めない状態にしておく必要がある。 紙媒体(書類等)であれば必要な時以外は鞄から出さない、ファイルバインダーやクリアファイルにきちんと綴じ鞄には鍵をかけ放置をしないで体から離さないようにする。 ②　USB 等の電子媒体であれば、データーの暗号化(パスワードによるロック)、媒体をなくさない為の工夫(大きなタグやストラップに付け体から離さない、落としてもすぐにわかるように鈴を付ける)などのような盗難、紛失対策を必要とする。 ③　パソコン(ノートブック PC、タブレット PC、スマートフォンのモバイル機器)に情報を格納した状態で持ち出す場合は、それらの情報が漏洩しない為にログインパスワードで他人がパソコンの中身を開けないようにする必要がある。 ④　情報の持ち出しに関しては、安易な持ち出しを防止するために情報の持ち出し管理をする必要がある。情報を持ち出す際には上長の許可を取り、持ち出す情報の記録をきちんとつけるなど管理を必要とする。万が一、持ち出した情報を紛失した場合、どんな情報がなくなったのかすぐに明確にできるような管理が重要である。 ⑤　携帯電話を業務で利用している場合は、個人情報など携帯の中に重要な情報が入っているので暗証番号によるセキュリティロックをかける事とする。
3.廃棄について (紙媒体等)	①　重要な情報が記載された書類を廃棄する場合は、ゴミ箱には捨てず関係者以外の目に触れないようにシュレッダーを利用する。 廃棄書類は裁断するまで管理を行い、放置は厳禁とする。 ②　CD、DVD 等の外部記憶媒体を廃棄する場合は、メディアシュレッダーにて裁断をする。シュレッダー等がない場合は割って廃棄する。 ③　USB メモリー、SD カード、ハードディスクドライブ等はファイルの削除機能及び初期化などで消去する。完全に消去できない場合は、専用のデーター消去ソフトを利用する。

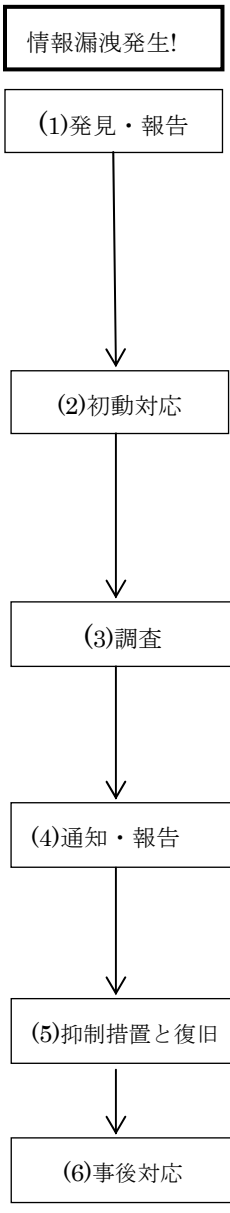
情報セキュリティ対策
実施手順２

項　　目	対　　策
3.廃棄について (パソコン等)	①パソコンなどの記憶媒体に保存された情報等は、「ファイル削除」などの操作をしても、復元ツールを用いて情報を取り出す事が可能なので消去ソフトウェアを利用し情報を確実に消去する。 ②FAX やコピー機を廃棄する場合、最近の機器には処理性能を向上させるために、内部にメモリをもっており FAX 送信やコピーを行う際にそれらのデーターがメモリに記憶されている為、この内容が情報漏洩する危険性があるので廃棄する場合は専門の業者に依頼し、メモリの内容を完全に消去してから廃棄する。 ③デジタルカメラや携帯電話も同様な内部メモリに情報が記憶されているので廃棄の際はデーター消去を行うか、データー消去に自信がない場合は専門業者に廃棄を依頼する。
4.事務所について	①無許可の人の立ち入りを禁止する。 ②退社時には、机の上の備品やノートパソコンなど引き出しに片づけ鍵をかけ盗難防止対策をする。 ③最終退室者は事務所を退室する際に机の上、パソコンの電源、消灯、施錠のチェックを行い記録の管理する。 ④事務所の修理、コピー機、空調等のメンテナンスを外部業者に依頼する場合は、事務所内の従事者が必ず立会う事とする。 ⑤夜間の警備については、警備会社のセキュリティシステムに依頼しているが通報があった場合の対応と連絡体制の管理を行う。
5.パソコンについて	①業務で利用するパソコンについては、会社で用意し会社の管理下で利用する。私物パソコンの持ち込み利用は禁止とする。 ②社内のパソコンについては、ネットワーク上にフォティゲートを設置し統合脅威管理(ウィルス対策、アンチスパム、侵入防止システム、コンテンツファイリング)を行っているので常に情報が最新となっていてウィルス対策も自動管理で行われている。ファイル交換ソフトのインストール、インターネットの閲覧等には制限がかけられており自動的に遮断される仕組みとなっている。外部記憶媒体等を利用する際も自動的にスキャンがかけられ安全なファイルのみを利用する事ができる。 ③パソコンの設定変更については、システム管理会社への問い合わせを必要とするので許可なく変更を禁止とする。
6.メールについて	①電子メールを送る前には、目視にて送信先アドレスの確認をするなど宛先の送信ミスを防ぐよう徹底をする。 ②複数人にメールを送る場合は、Bcc 機能を活用するなどメールアドレスを誤って他人に伝えてしまわないよう注意する。 ③重要情報をメールで送る場合は、重要情報をドキュメント(ファイル)化し、そのファイルをパスワード保護した状態で電子メールに添付する。
7.バックアップ について	①重要情報のバックアップについては定期的に行ない、故障や誤操作などに備えて重要情報が消失しないよう対策をとる。 ②バックアップを外部記憶媒体に保存する場合は、施錠可能な場所に保存し関係者以外に見られないよう管理を行う。 ③不要になったバックアップは常に安全に廃棄する。

情報セキュリティ対策
実施手順３

項　　目	対　　策
8.従業員について	①　従業員を採用した際に守秘義務がある事を確認した旨の「誓約書」等を書いてもらい、守れなかった場合に罰則がある事を伝える。具体的内容については業務を遂行する都度に業務に関わる情報あるいは業務上知り得た情報の扱いなど再確認し何が機密(守秘義務)で守るべきルールかを明確に伝える。 ②　情報セキュリティ対策の社内教育を定期的に行ないセキュリティ事故が起きないよう従業員に対して意識付けを行う。
9.取引先について	①　取引先との契約書には秘密保持(守秘義務)の項目を盛り込み委託業務として扱う情報に個人情報や企業情報を含んでいた場合には、それらの情報が外部に漏れたりしないように情報の重要性、秘密性を明確にし、場合によってはその管理方法まで明確に指示をする。 ②　業務委託先での事故が発生した場合の業務委託元の管理責任や、業務委託先での業務遂行責任について責任の範囲を明確にし、事故が起きてからの対応が速やかに実施できるような体制をとる。

10.事後対応について



情報漏洩に関する兆候や具体的な事実確認をした場合は、責任者に報告し速やかに情報漏洩の体制をとり不正アクセスや不正プログラムなど情報システムからの情報漏洩の可能性がある場合は、不用意な操作はせず、システム上に残された証拠を消さないよう保存する。外部からの通報があった場合は、相手の連絡先等を必ず控える。

対策本部を設置し当面の対応方針を決定する。情報漏洩の二次被害の防止のために必要な応急処置を行い、情報が外部からアクセスできる様な状態にあったり被害が広がる可能性がある場合には、これらを遮断する措置をとり情報の隔離、ネットワークの遮断を行う。

適切な対応について判断を行うために 5W1H(いつ、どこで、誰が、何を、なぜ、どうしたのか)の観点で調査し情報を整理し、原因の事実関係を裏付ける情報や証拠を確保する。

漏洩した個人情報の本人、取引先など関係各所への通知を行う。漏洩した個人情報の本人については特別の理由がない限り通知を行い、紛失・盗難のほか不正アクセス、内部犯行など犯罪性がある場合には警察に届出をする。

情報漏洩によって発生した被害の拡大の防止と復旧及び再発防止に向けた具体的な取り組みを行い、停止したネットワーク、外部との通信等の復旧を行う。

抜本的な再発防止対策を検討し実施し、調査報告書を作成し必要に応じて開示を行う。責任が内部職員にあれば処分手続きを行う。

(改善措置)

第 4 条　情報セキュリティ管理者は、業務上発見された問題、従業員からの指摘による問題が発生した場合は、自己点検において指摘された問題等に対する再発防止のため、その原因を除去する為の措置を講じなければならない。

(規則の見直し)

第 5 条　情報セキュリティ管理者は、「情報セキュリティ対策運用規程」について、自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ必要があると認めた場合は、担当取締役に報告し改善を行うものとする。

附　　則

平成 28 年 4 月 1 日　制定