アース環境サービス株式会社 Earth Environmental Service Co., Ltd.

ESCO News Letter

第4巻 第8号　　発行日　2015年12月15日

「情報管理」は万全ですか？

－情報の取り扱いと対策が企業の存続を左右します－

企業活動における「情報」とは

現代社会において、「情報」は「人」「物」「金」「時間」と並ぶ企業活動の主要5資源の1つとして挙げられていますが、ご存知の通り、「情報」は企業に利益をもたらす反面、命取りとなる一面ももっており、諸刃の剣と言えます。つまり現代社会において、「情報」の取り扱いには細心の注意が必要なのです。

『情報漏えい０（ゼロ）』をめざす取組み

弊社では、2012年12月に国際規格であるISMS（情報セキュリティマネジメントシステム）の認証を全社（国際本部除く）で取得し、『情報漏えい0（ゼロ）』をめざし日々の業務を行っています。

お客様に「THC（総合環境衛生管理）」を提供する際には、クレーム情報や、現場の情報等が必要になりますが、それらの「情報」は機密情報に該当しますので、取扱いには細心の注意が必要です。万一にも、些細なミスや悪意の操作などにより、情報が流出するようなことがあれば、お客様をはじめステークホルダーへの信頼や期待を裏切ることになり、一瞬にしてその存続が危ぶまれることになります。昨今の大手企業の情報漏えい事件における社会への影響を考えると、他人事では済まされません。

そこで弊社は、お客様と秘密保持の文面を取り交わすだけでは情報セキュリティの担保はできないと考え、ISMSの認証を取得し、委員会の設置、全社の各種情報の掌握、ルール作成、教育、監視を行い、情報漏えい対策に全社で取組んでいます。

ＩSMSとPマークの違い

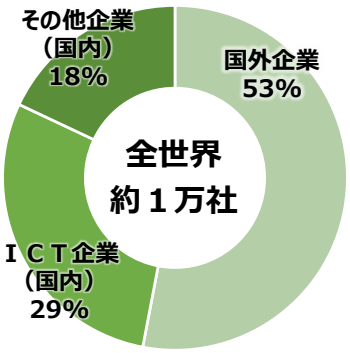
Pマークは個人情報を対象としていますが、ＩSMSは個人情報を含めた情報全般を対象としています。よってＩSMSの維持管理は、より大変な労力と知識が必要とされますが、企業として情報漏えい防止対策に最善の手立てを施すことになりますので、一定の安心感と社会的な責任を果たすことになります。

ＩSMS	Information Security Management Systemの略語：国際規格 組織（企業、部、課など）における情報セキュリティを管理するための仕組みで、情報セキュリティ管理システムとも言われています。 **ISMSが維持･担保を要求する３つの方針** 【機 密 性】　・・・・ 情報が漏れないこと 【可 用 性】　・・・・ 必要なときにすぐ使えること 【完 全 性】　・・・・ 情報を正しく保護していること
Pマーク	Privacymark Systemの略語：国内規格 個人情報のみを対象に情報を管理します。

この号の内容

ISMS認証取得社数と傾向

全世界での取得件数約１万件のうち、日本国内での取得が約半分と多くを占めており、日本国内における自社防衛意識の高さ、取引先からの要求の高さが伺えます。



出展：ISMS適合性評価制度に関するアンケート調査結果報告書（JIPDEC情報マネジメント推進センター）より

ＩSMSの活動の
一部をご紹介します！

- 重要書類は
鍵付の棚に保管！
- 重要データは
取扱者を限定！
- データは、
東西2か所でバックアップ！
- ＰＣには
セキュリティ設定！
- ＰＣソフトウェアには
使用制限！
- 車内に資料を
放置しない！
- ＦＡＸ等は
送信先をWチェック！
- 帳票には、
保管期限を設定！
- メールは、
ログを記録して追跡可能に！
- ＩSMSの活動情報は
全社に展開！
- 定期的に
ＩSMS教育を実施！
- 退社時は、
机上に書類を置かない！
- 重要情報記載の
ゴミは裁断！
- 事務所の入退室管理、
防犯対策を実施！
- 退職者の情報持出ゼロ確認、
事務所への入室不可設定！
- 防災活動を
定期的に実施！

情報管理不足（脆弱性）がもたらすもの

情報は、最先端の技術やノウハウ、営業（顧客）情報、社員情報等、多種多様に存在しており、その中には個人情報保護法等の法律が適用され、その遵守が求められるものもあります。

「情報」がデータとなり世界と繋がっているネット社会において、情報漏えい対策を性善説で運営していくことは、企業責任を果たしていない（危険の放置）と言っても過言ではありません。

情報管理不足による事故事例

企業の情報管理不足が引き起こす事故の中でも、経営に大きなダメージを与える具体例を紹介します。自社でも起こりうる危険性がないか確認してみてはいかがでしょうか。

事例 ①

会社に不満を持った従業員又は退職者が、機密情報等のデータを抜き取りマスコミに提示した。

要　因	社 内	社 外
	○	○

事例 ②

秘密保持契約を取り交わした取引先の従業員が、入手した情報を金銭目当て又は興味本位でネットに公開した。

要　因	社 内	社 外
	○	○

事例 ③

社外の第三者が、情報を保管しているサーバーをメール等を通じて攻撃し、情報を公開した。又は改ざん、破壊した。

要　因	社 内	社 外
	―	○

事例 ④

従業員が正しいと思って実施した作業が、お客様の大切な情報を漏えい、又は削除することになった。

要　因	社 内	社 外
	○	―

事故の要因は「社内」に限らず、「社外」にも存在します。

Check！ 自社の機密（重要）情報を開示している取引先の情報管理について、確認されていますか？

脅威と予防

万一自社の従業員や、社外の協力会社の情報管理が不足していたことで上記のような事故が起きれば、これまで築き上げた会社の信用は一瞬にして失墜し、経営危機に陥ることは必至です。経営者は経営責任が問われ、企業規模によっては社会現象をも引き起こす事態になることでしょう。

命とりにもなり得る情報管理の不備は、「企業にとっての脅威」となるわけです。

上記で紹介したような事故を防ぐためには、情報全般のリスク分析（アセスメント）の実施が必要です。

予防対策に必要な項目例

- 権限管理
- データの保管方法
- ルール周知や教育
- 強固なデータ管理
- データ等のログ管理
- 取り扱い基準
- 業務手順
- 組織運営
- 監視（確認）

etc.

情報管理にもディフェンス対策を

食品業界では、食品への意図的な異物の混入を防止するための「フードディフェンス」という考え方がありますが、製品を製造販売していくうえで発生する情報（特に機密情報）の管理についても同様のことが言えます。情報を対象としたディフェンス対策を施さないことは、「リスクを保有した状態」であり、早急に対策を検討されることをお奨めします。

併せて、機密情報を共有する可能性がある取引先や協力会社の選定基準として、全社でのISMSの認証取得（又は準じた仕組みを持っている）を必須とされることをお奨めします。

「衛生管理」も「情報管理」も企業活動を継続していくための投資です。「まさか?!」「気にはしていたが…」「情報システム部門に任せて安心していたのに…」という不測の事態が起こらないよう、従業員全員（情報の取扱者全員）が、万一の事態に備えることが企業の存続に必要な条件となります。

ISMS構築・運用の簡単な流れ（ご参考）

構　築

構築①　【組織開設】
構築の為の委員会設立

構築②　【対象物の設定】
情報資産の台帳作成・整理等
（データ・書類・建物他）

構築③　【リスク洗い出し】
各資産のリスク*を洗いだす
＊ 漏えい・紛失・盗難・消去・改ざん等

構築④　【リスク分析・評価】
各資産のリスク影響度を算出

構築⑤　【リスク対応計画】
各資産のリスク対応計画を立案し、実行していく

構築⑥　【規定・手順書等作成】
情報資産保全の為、規定書等を作成・整備する

構築⑦　【教育】
対象者に運用開始の為の教育を行う
→ 審査申請 → 承認

運　用

運用①　【組織・教育・目標】
組織を構築し、対象者にISMS教育・活動目標の設定を行う

運用②　【情報の見直し・監視】
運用状況の確認・監視・監査

運用③　【活動】
活動は、PDCAサイクルで確認
協力会社への指導も実施
→ 審査申請 → 承認

ISMS活動は、
① **情報に関わるすべてを対象に**
② **従業員全員が**
③ **同じ知識(意識)をもって**
④ **毎日(365日)活動する**
ため、継続には労力が必要ですが、情報管理以外にも、業務の見える化や合理化といった効果も得られます。

アース環境

総合環境衛生管理で
社会に貢献します

本件に関してのお問合せは、
03-3253－0640
ホームページもご覧ください
http://www.earth-kankyo.co.jp/