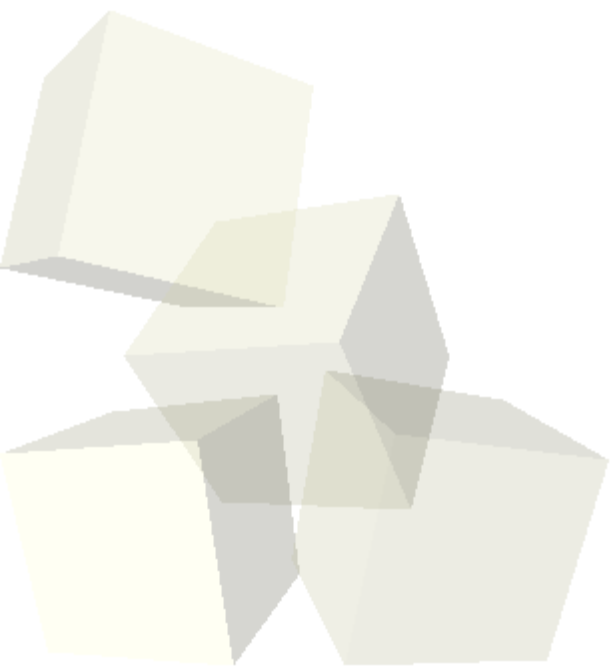




「ISOと情報セキュリティ」

山下 亮一
2009年9月14日



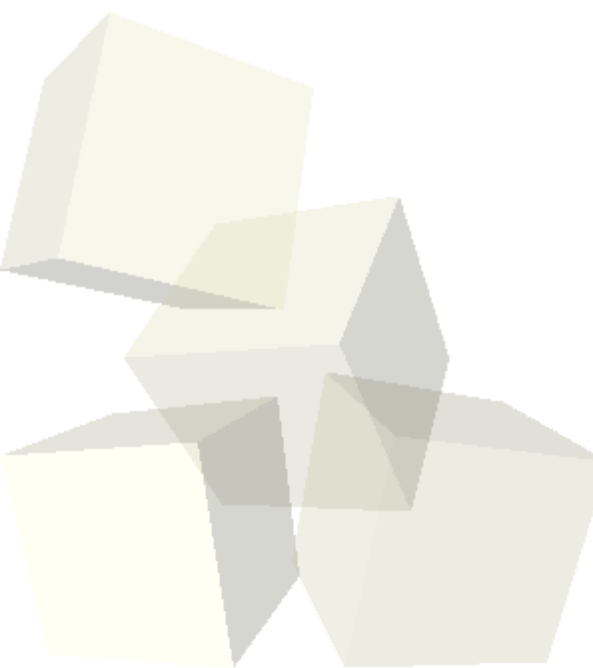
ISOって知っていますか？

- ISO9001 認証取得、ISO 14001 認証取得等の表示を見たことはありませんか？
- これはマネジメントシステム(経営のしくみ・ルール)に関する国際規格について、中立の審査機関から企業として規格を守る仕組みが機能していることを証明を受けたことを意味しています。
(これを第三者認証制度といいます)
- 90年代からヨーロッパを中心に広がり始め、大企業や公官庁が調達条件や調達先評価に用いる傾向があったことから広く普及しています。
- 様々な規格がありますが、もっともメジャーなのが品質に関するISO9001と環境に関するISO14001です。
- 第三者認証を得るには企業規模にもよりますが、100万～300万ほどかかります。
取引上の必要性も考えてよく検討しましょう。
- でも考え方を経営に活かす分には認証を受けなくても市販の解説書等で学ぶだけでも十分です。
- インターネット上の解説書も活用しましょう。

- 「〇〇さんに聞けば分かる」で大丈夫？
 - ・ 業務の流れを整理し仕組みとして体系化しましょう。(ルール作り)
 - ・ ひよっとするとムダな作業が見つかるかも
 - ・ 新しい人が入った時の教育がし易くなる
- 「たしか△△△って話だったはず」はトラブルの元
 - ・ 人の記憶頼みはやっぱり危険
 - ・ メモでいいので記録を残しましょう
- 「ちゃんとやってるはず」は管理じゃありません
 - ・ ルールが守られているかどうかは確認しないと分かりません。
 - ・ 異なる立場の方が確認することで意外な視点での発見があるかも
- 「守りましょう!」の掛け声だけではルール違反の対策になりません
 - ・ そもそもなぜルール違反が起きたのかを分析しましょう。
 - ・ 実際の現場では想定外のこともあります。
想定外の場合の対処のルールはありますか？
 - ・ 人間にミスはつきものです。
ミスを防ぐ工夫の余地はありませんか？
- PDCA サイクルを繰り返しましょう。



- 情報セキュリティ事故は多発しています。
- もし自分の会社で起きたらどうなるか？
- 事故の発生を防ぐこと、もし発生しても被害を最小限にすることがリスク対策の基本です。
- パソコンだけではなく、仕事で取り扱うすべての書類や機器について考えましょう。
- 人の記憶のなかにも営業秘密に相当するものはあるはず。





- 公官庁や各種団体が提供する教材等を活用しよう
 - ◆ 5分でできる自社診断
 - ◆ 情報セキュリティ理解度チェック

