ロール管理についての「モヤモヤ」

2016年1月21日

株式会社 マインド・トゥー・アクション
中島浩光

自己紹介

中島浩光（なかじま　ひろみつ）

- 株式会社マインド・トゥー・アクション　代表取締役
- アクセンチュア、日本CA、インフォセックを経て独立、現職にいたる。
- 情報セキュリティコンサルタント
- 教育コース「セキュアシステム設計」の開発、講師
- ID管理WGに設立当初より参加、現在ロール管理テーマリーダー
- ID管理ガイドライン、エンタープライズロール管理解説書主要執筆者

今日話すこと

- 2014年に「エンタープライズロール管理解説書」を出した。
- でも、なんか、納得いかない！

- その納得いかないこと＝「モヤモヤ」について、執筆者間で考えて、議論してみたので、その結果について話します。

「ロール管理」って何？

- 「エンタープライズロール管理解説書」を読んでみましたか？

- 「ロール管理」
  - 情報システムにおける利用者の権限を「役割＝ロール」として管理を行うこと。

質問

- 皆様の組織で「ロール管理」、上手くいっていますか？

「パンドラの箱」

- ID管理WGが出来て今年で10年。
- 重要なテーマであるにも関わらず、ロール管理の話は2012年度にやっと始まった。

- ID管理WGのメンバーの間でもロール管理は「パンドラの箱」＝開けてはいけない、誰が開ける？という感じ。
- というのも、WGのメンバーが「難しい」と直感的に感じていた。

箱を開けてみたら・・・

- ロールの種類を考えた。
- ロールの構造を考えた。
- ロールの設計・導入手順を考えた。
- ロールの運用を考えた。
- サンプル事例も考えた。

- うん、書けた！！えらい！！

- あれ、でもなんか納得いかない！「パンドラの箱」じゃなかったのか？

「パンドラの箱」の理由

- 実際の現場では、ロール管理が上手くいっていない。
- 「上手くいっていない」状態ってどういう状態？
- 上手くいかない理由は何なのか？
  - 設計での落とし穴
  - 実装での落とし穴
  - 運用での落とし穴

- このあたり＝「モヤモヤ」

ロール管理が「ダメな状態」

- ロールの更新がされない
- 不要なロールの存在
- 巨大なロール
- 万能ロール
- ロールの数が多い
- ロールの使用目的不明

「ダメな状態」がもたらすもの

- システムの不正利用
- 情報漏えい
- 非効率
- 「ダメな状態」による負のスパイラル

「ダメな状態」になる理由（設計）

- 巨大なロールを作る
  - メンバーが多過ぎ
  - 最少権限の原則を無視
- ロールの名前が訳のわからない状態
  - 名前に数字とかコードが入っている
  - 似たような名前がたくさん
- ロールの数が多過ぎ
  - 組織の規模に比べて数が多過ぎ。
  - 体系化されているならいいのだが。
  - 似たようなロールがたくさんある。
- 現場の業務に合っていないロール
  - 定義された職務分掌と現実が違う。

「ダメな状態」になる理由（実装）

- 入れ子が出来ないシステム
- ロールがパラメータ化されていない
- ロールのプロビジョニングが自動化できないorしない

「ダメな状態」になる理由（運用）

- 「派生ロール」が増えていく
  - メンバーや権限がちょっとだけ違うロール
- ロールが消されない
  - いつか使うだろう
  - 消すと障害が発生するかも
  - 消すための承認者・責任者が不明・不在
  - 棚卸をしていない
- ロールのメンバーの更新情報が来ない
  - 人事情報に入っていないメンバー

処方箋（設計）？

- ロール管理の導入＝業務の整理
- 調査は念入りに
- 運用を考えた設計
- ロールの構造の柔軟性の確保
- ビジネスロールとアプリケーションロールの違いをきちんと理解すること
- 設計における「コンセプト」が重要

処方箋(実装)？

- ロール管理の対象スコープに入れるか入れないか？

- 出来るだけ手作業の運用は減らす。

処方箋(運用)？

- 棚卸はちゃんとする。
- ロールの用途がちゃんと分かるようにしておく。
- ロールの例外運用を考えておく。
- 設計段階での「コンセプト」を崩さない。

やっぱりパンドラの箱だった・・・

- いろんな所に落とし穴がある・・・・
- ロール管理は「難しい」or「大変」
- 「コンセプト」の確立と維持

エルピス

- パンドラの箱に最後に残ったもの
- 一般に知られた解釈では「希望」
- 期待（偽りの希望）
- 希望＝災厄？
  - 希望があるために、苦痛に耐えながら生きなければならない・・・・

ということで

- 「モヤモヤ」を解消すべく、
「エンタープライズロール管理解説書」
の改訂作業を実施中。

- エルピスになるのか、それとも、その
前に飛び出している「災厄」なのか？

ありがとうございました