信頼される安心を、社会へ。
SECOM

JDCCセキュリティWGの活動紹介

@ JANOG39 meeting

2017/1/19

セコム株式会社　IS研究所
水戸 和

- 初めまして、水戸と申します。
- セコムの研究所でデータセンターに関する研究やロボット（クラウド・ネットワーク・ロボット）に関する研究をしています。
- L1/0（建屋層）とL8（ユーザー層）大好き！
- 日本データセンター協会ではセキュリティWGのリーダー補佐をやっています。
- JANOG初参戦です。

■Securityの語源は

Se(取り除く)-Cure(心配・気遣い)

データセンターを“心配なく”使っていただくための
日本データセンター協会の取り組みを紹介します。

身近なセキュリティの話から

(利用者目線で)

Q1.データセンターの所在地って
　　なんで秘密にしないといけないんですか？

という質問に便利なツールがあります

みなさん、

- 「金融情報システムセンター(FISC)」や「ISMS認証」ってご存知ですか？
- 

金融情報システムセンター
金融機関等コンピュータシステムの
安全対策基準・解説書(第8版)

や 

日本規格協会
JIS Q 27002:2006
情報技術−セキュリティ技術−
情報セキュリティマネジメントの
実践のための規範

って読んだことありますか？

FISC安対基準

具体的に“やらないといけないこと/やってはいけないこと”を書いてある

設備.6　「看板等を外部に出さないこと」

解説：外部からの侵入、破壊行為などの人為的災害を未然に防止するため、コンピューターセンターなどの所在を示した表示板、看板などは外部に出さないことが望ましい。

設備.24　「室名等の表示は付さないこと」

解説：侵入、破壊、機密漏えいを防止するため、コンピュータ室・データ保管室の室名等の表示は付さないこと。

FISC安対基準だけ見ると、どこにも

“利用者がその所在地を口外してはいけない”

とは書いていない。

一方で、

多くのデータセンターが取得している ISMS認証の参考基準では

１１．物理的及び環境的セキュリティ

目的：**組織の情報及び情報処理装置に対する許可されていない物理的アクセス、損傷及び妨害**を防止するため。

管理策：(11.1.3)オフィス、部屋及び設備に対する物理的セキュリティを設計し適応することが望ましい

実施の手引：適応可能な場合、建物を目立たせず、その目的を示す表示は最小限とし、情報処理活動存在を示すものは建物の内外を問わず、一切表示しない。

要するに、

- 「組織の情報及び情報処理装置に対する許可されていない物理的アクセス、損傷及び妨害」をリスクと考えるなら、何らか策を講じろと書いてある。

→具体的内容はDC事業者に依存

ということで、

細かく/はっきりなツール：
FISC安対基準(管理策ベース)

大まか/柔軟なツール：
ISO/IEC 27001(リスクベース)

A. ISMS認証を取得している
DC事業者が所在地の公表によるリスクを想定している場合、
それ相応の管理策を**事業者が**とる場合があります。

例：センター利用にあたっての契約約款への明記
違反した場合の罰則規定(入館拒否等)
(民法の財産権・所有権から認められる、施設管理権/損害賠償の範囲で？)

応用編として

Q2. (事業者目線で)

　構内接続したほうがよさそうなお客さん同士がいるんだけど、そんなお客様がいることって、秘密にしないといけないの？

疑問①

DC事業者が(例えば)ISMS認証を取得していて、それへの影響がありうる？

疑問②

利用者がどこのセンターを利用しているかを営業秘密にしているのでは？

疑問①

DC事業者が(例えば)ISMS認証を取得していて、それへの影響がありうる？

→A. Q1の応用、ほかの管理策で充当すればよい

疑問②

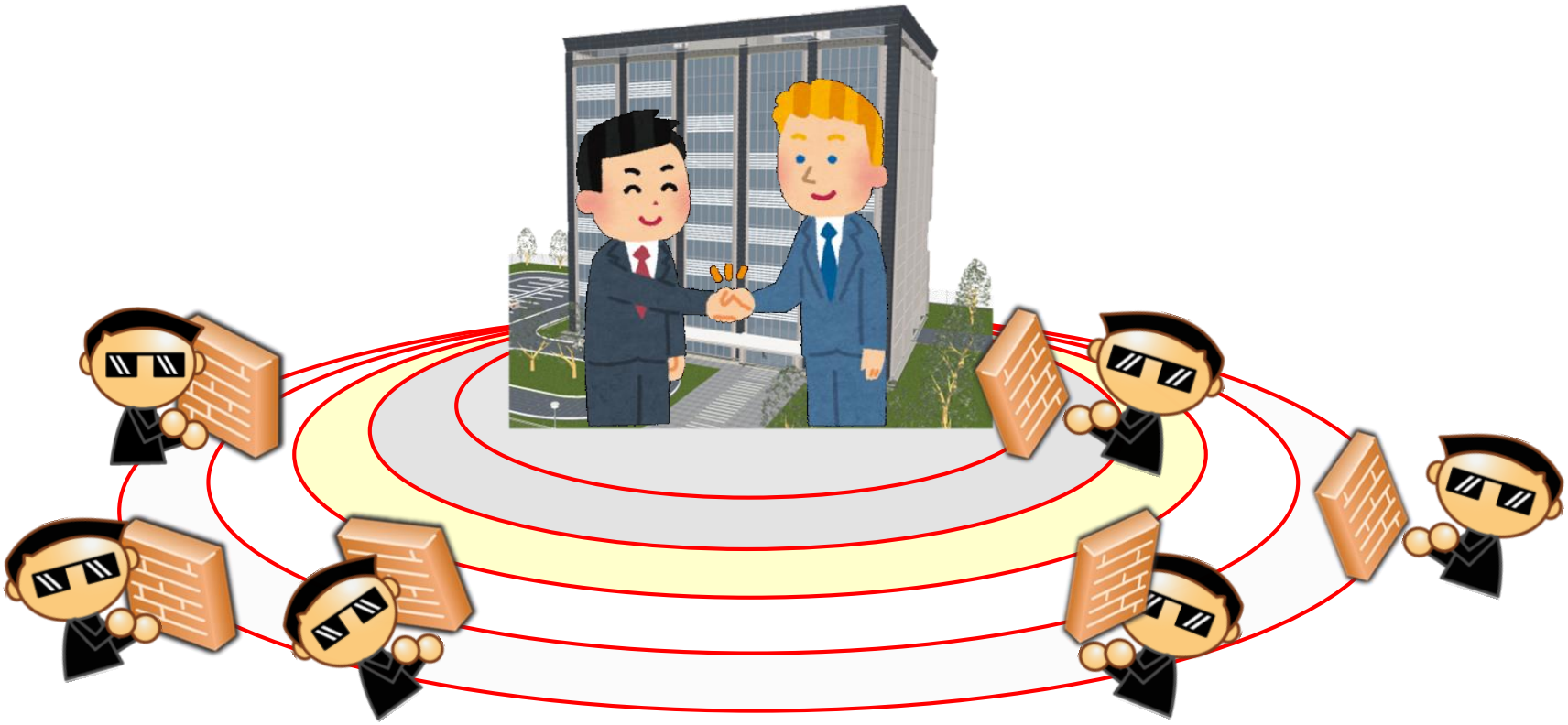
利用者がどこのセンターを利用しているかを営業秘密にしているのでは？

→A. 各社のポリシーに“基準”はない、難しい

JDCCフューチャーセンター的には

Se(取り除く)-Cure(心配・気遣い)

- 利用者が、心配せずに、最小限の秘密で自由に相互接続できる世界を作るのもデータセンター事業者の役割！



そんな便利な基準の動向について

管理策ベースの基準はとても便利。
わかりやすい。

でも、それでいいの？

- 管理策ベースの管理は、適切に更新されないと無駄・見落としを生んでしまう可能性がある。
- FISCもFintech時代を見据えて方針を再確認（≠転換）

1．情報システムに会する安全対策の達成目標は、個々の情報システムのリスク統制に応じて、必要十分な内容で決定されるべき。

2．情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較秤量したうえで、情報システム予算内での新規開発などの調整のみならず、経営資源全体も視野に入れ企業価値の最大化を目指して、決定されるべきである。

3. 上記原則が順守されたうえで、妥当な意思決定が行われ適切に運営されている限りにおいては**安全対策は独自に決定することが可能である**。

4．金融機関が保有する重大な外部性を有する情報システム、および機微情報を有する情報システムにおいては、上記に加えて、その社会的・公共的な観点からこのシステムの外部性や保有情報の機微性を考慮に入れた安全対策の達成目標が設定されるべきである。

金融情報システムセンター
「金融機関における外部委託に関する有識者検討会報告書」 より抜粋

リスクベースの基準はとても柔軟。
様々なケースに適応できる。

でも、それでいいの？

■リスクベースの管理は、どのように手当てがなされているのかをブラックボックス化してしまい「心配」を生んでしまう可能性がある。

特に、クラウドサービスに関しては

–利用者と事業者の間で情報が非対称になりがち。

–電気通信事業に比べて責任の分界が複雑になりがち。

- そこで、一昨年からクラウドサービスの**管理策に焦点を当てた基準、ISO/IEC27017 が登場**し、それに基づいた認証サービス等が登場している。

ISO/IEC 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

信頼される安心を、社会へ。SECOM

ISO/IEC 27001:2013

本文(マネジメントシステム)

6.1.2　情報セキュリティリスクアセスメント
6.1.2　b）情報セキュリティリスク対応の管理策決定

付属書A(114の管理策)

5　情報セキュリティのための方針群
⋮
18　順守

ISO/IEC 27017:2015

本文(管理策、クラウド固有の実施の手引き)

5　情報セキュリティのための方針群
⋮
18　順守

付属書A（クラウドサービス拡張管理策）

CLD 6.3.1　クラウドコンピューティング環境における役割及び責任の共有および分担
CLD 8.1.5　クラウドサービスカスタマーの資産の除去
CLD 9.5.1/2　仮想コンピューティング環境における分離/要塞化
CLD 12.1.5　実務管理者の運用のセキュリティ
CLD 12.4.5　クラウドサービスの監視
CLD 13.1.4　仮想及び物理ネットワークのセキュリティ管理の整合

ISO/IEC 27002:2013

（管理策、実施の手引き）

5　情報セキュリティのための方針群
⋮
18　順守

例えば、、

12.1.2　変更管理

「変更管理においては、直接的・間接的に影響を受けるユーザーを特定し適切に通知する」
→依存関係が複雑になるクラウドにおいては体系づけられた管理が行われている必要がある
→「ITILに準拠した手順の体系化等が必要になる」 という意見も、、

https://www.isms.jipdec.or.jp/seminar/cloud/shiryou-1.pdf
https://www.isms.jipdec.or.jp/topics/ISO27017/iso27017_CLS_outline.pdf
等から作成

このように

- 社会や技術の変化に合わせて管理策/リスクベースいずれのアプローチも徐々に形を変えている。

- 事業者・利用者ともにツールへの継続的な「ケア」は必要。

そこで、JDCCの取り組み

「データセンター セキュリティ ガイドブック」

- 発行者
  日本データセンター協会
- 発行日
  2013年8月 （2015年8月 改訂）
- 目的
  データセンターの利用者および事業者に「データセンターの適切なセキュリティ」とは何かを示す
- 内容
  - データセンターの提供するサービス
  - サービスにおいて想定される脅威
  - 脅威に対して実施される管理策
  - セキュリティに係わる基準・認証制度等
- 分量
  - 144ページ(付録含む)
- 入手方法（無償公開）

“データセンター　セキュリティ　2015”のキーワードで検索

- マネジメントシステム適合性証明制度
  - ISMS　ISO/IEC 27001
  - ITSMS　ISO/IEC 20000
  - BCMS　ISO 22301
  - CSMS　IEC 62443-2-1
- 安対制度
  - JQA　情報システム安全対策適合性証明制度
- その他の基準・認証制度
  - JDCC ファシリティスタンダード
  - ASPIC　情報開示認定制度
  - JASA 情報セキュリティ監査制度・クラウド情報セキュリティ監査制度
  - CSA STAR認証制度
  - 海外の基準
    - Uptime Institute “Tier Performance Standard”
    - ANSI/TIA-942
    - ANSI/BICSI-002
- 分野ごとの基準・ガイドライン
  - 医療分野
    (医療情報システムの安全管理に関するガイドライン/ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン/医療情報を受託管理する情報処理事業者向けガイドライン)
  - 政府分野 (政府機関の情報セキュリティ対策の為の統一基準群)
  - 金融・信販分野 (FISC安全対策基準/PCI-DSS)
  - 自治体分野 (LGWAN-ASPファシリティサービス登録)

2017年版にUpdateします。

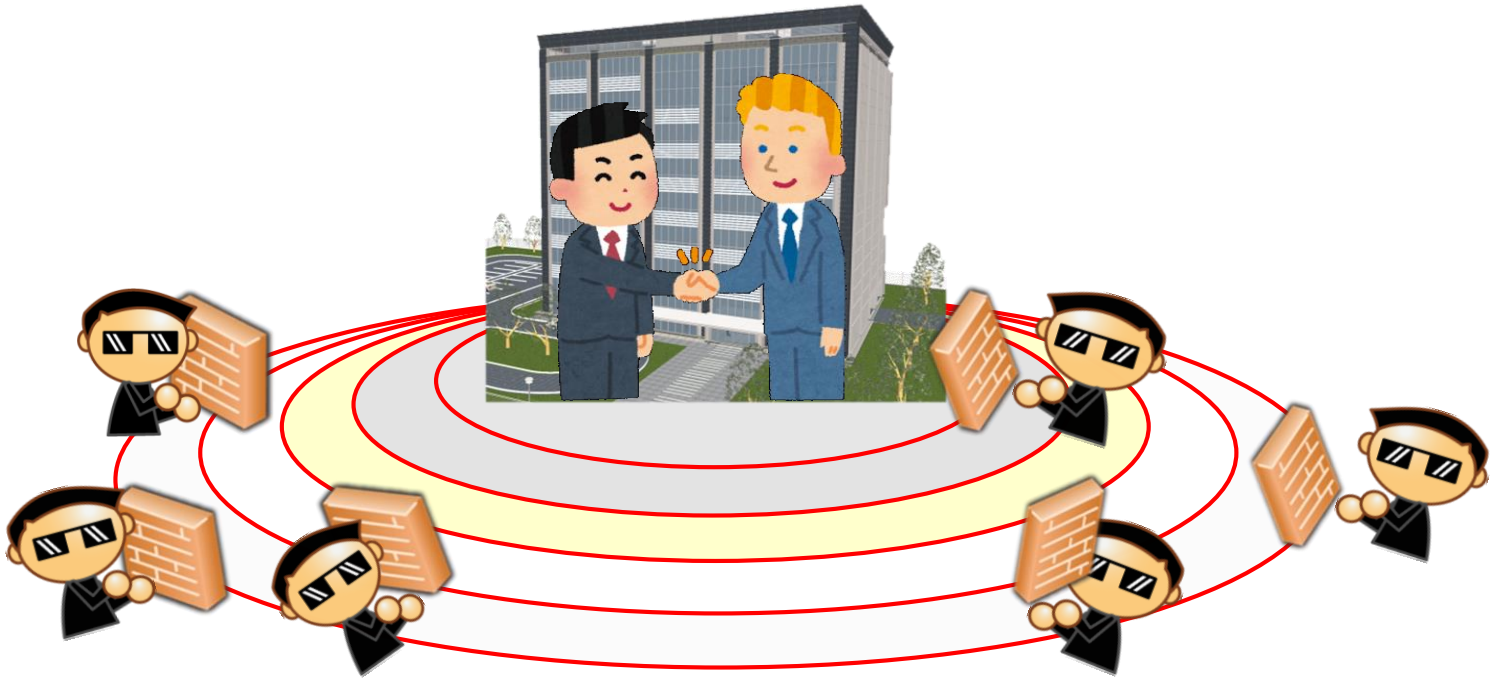
JDCCフューチャーセンター的には

- 日本データセンター協会セキュリティWGでは「データセンター事業者/利用者」も含めた様々なステークホルダーのためのコミュニケーションツールとしてセキュリティガイドブックを作ってきました。

- が、コミュニケーションする人、文化をデータセンター業界に根付かせ、**「出会い」**を作らないと意味がない。

→そこで、JDCCフューチャーセンター

JANOGやフューチャーセンターの活動を通じて、
「出会い」の環境をつくり



「セキュア」なデータセンターを提供することで、
皆様が気楽に「動き出せる」環境をつくりたい！

と、思うのですが、

さくらインターネット高峯さん、

いかがでしょう？