大企業からの個人情報漏洩に対するMRCの適用

2009/01/10　JSSM　第3回ITリスク学研究会

東京電機大学　情報セキュリティ研究室
竹下数明、江口慶、川上昌俊、富永子南

目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

背景(1/3)

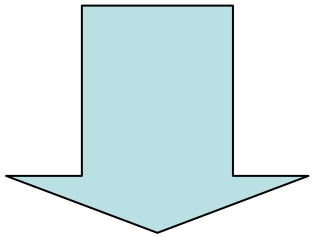
- 近年、個人情報の漏洩が相次ぎ、企業はその対応に追われている

- 2007年　個人情報漏洩件数　**864件**
  漏洩人数　**3053万1004 人**

出展:NPO日本ネットワークセキュリティ協会,「2007年度情報セキュリティインシデントに関する調査報告書Ver.1.5」
http://www.jnsa.org/result/2007/pol/incident/2007incidentsurvey_v1_5.pdf

背景(2/3)

- 対策を行う場合、どの対策がどのような効果をもたらすのか、正確に判断し、複数の関与者間で対策の合意をとる必要がある



- MRCの適用を行うのが効率がよい

背景(3/3)

- 大手生命保険会社における以下の3部門を対象とした個人情報漏洩問題をMRCへ適用した
  - システム管理部門
  - 事務部門
  - 営業部門
- フォルトツリーの頂上事象
  - 個人情報が流出

部門ごとに分ける理由:

・各部門ごとに従業員数が異なる

・各部門ごとに掛けられる費用が異なる

・各部門ごとに扱う要素が異なり、対策も異なってくる

目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

各部門における組織状況

	システム管理部門	事務部門	営業部門	合計
従業員数	500人	9,500人	30,000人	**40,000人**
デスクトップPCの数	500台	9,500台	30,000台	**40,000台**
ノートPCの数	0台	5,000台	30,000台	**35,000台**
ポータブルHDDの数	100個	5,000個	1,000個	**6,100個**
部屋の数	3部屋	30部屋	100部屋	**133部屋**
サーバ室に入れる人数	20人	0人	0人	**20人**
紙媒体の使用	なし	あり	あり	

関与者

メールを監視するなんて！
プライバシーの侵害だ！

従業員

従業員のメールを監視してでも
個人情報を守れ！

メールを監視する以外にも
方法はあるけど・・・
お金がかかりすぎるよ

経営者

決定事項

- 対策適用期間
  - 3年
- 目的関数
  - Min{漏洩確率×被害リスク＋対策コスト}
- 個人情報の価値
  - NPO日本ネットワークセキュリティ協会の「2007年度情報セキュリティインシデントに関する調査報告書」※の漏洩個人情報価値の求め方を利用

※http://www.jnsa.org/result/2007/pol/incident/2007incidentsurvey_v1_5.pdf

個人情報価値の計算式

- 個人情報価値
  ＝ 基礎情報価値 × 機微情報度 × 本人特定容易度
  ＝ 500 × $\{10^{(3-1)} + 5^{(1-1)}\}$ × 6
  ＝ 303,000 （円）

目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

入力した対策案とその理由(1/5)

- #1「1年に4回パスワードを変更しなければいけないようシステムを設定する」
  - パスワード変更の処理を行うだけなので費用が安く、しかも高い効果を望むことが出来る
- #2「サーバーとデスクトップPCとノートPCに業務に不要なソフトのインストールを禁止する」
  - P2Pソフトからの流出や、ウィルスに感染する危険性も減るので、漏洩確率が減る
- #3「サーバに対して電子媒体を使用できない処置を行う」
  - サーバから個人情報を電子媒体に書き出すことが出来なくなるため、漏洩確率が減る

入力した対策案とその理由(2/5)

- #4「社内の各部屋に監視カメラを設置し、社内の様子を撮影することにより不審な行動を監視する」
  - 故意による電子媒体や紙媒体の持ち出しを抑止出来る
- #5「URLフィルタリングツールを導入し、Webフリーメールの使用や掲示板の書き込みを禁止する」
  - Webフリーメールや掲示板経由での漏洩確率を減らすことができる
- #6「社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ、送れないようにする」
  - 社外の方へメール誤送信した場合、早期発見が可能である

入力した対策案とその理由(3/5)

- #7「添付ファイルを含んでいるメールの社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ送れないようにする」
  - 社外の方へメール誤送信した場合、早期発見が可能であり、添付ファイルからの情報漏洩が抑えられる
- #8「デスクトップPCとノートPCに対して電子媒体への書き出し時に強制暗号化を行う処置を取る(会社外のPCでは復号化できない)」
  - 会社外のPCでは復号出来ないため、電子媒体を紛失しても高い確率で情報漏洩が抑えられる
- #9「強制暗号化を行うポータブルHDDを全従業員へ配布する」
  - 暗号化処理が強制的に行われているために、かなりの確率で情報漏洩が抑えられる

入力した対策案とその理由(4/5)

- #10「ノートPCのハードディスク暗号化を行う」
  - ハードディスクが暗号化されているため、盗難にあった場合でも高い確率で情報漏洩が抑えられる
- #11「シンクライアント(ノートPC)の導入」
  - ノートPCにデータが残らないので、かなりの確率で情報漏洩を防ぐことが出来る
- #12「会社から個人情報を含んだ印刷物の持ち出しを制限するルールを作る」
  - ルールを作るだけなので費用をあまりかけずに、事故による漏洩を減らせる

入力した対策案とその理由(5/5)

- #13「印刷物へ強制的に印刷者の情報の透かしを挿入することにより、印刷物の管理を徹底してもらう」
  - 透かしを入れることで印刷物の扱い方の意識が高まり、漏洩確率を減らすことが出来る
- #14「IDSを設置し、サーバなどに攻撃が行われていないか監視する」
  - サーバに対する不正行為を検知することで、サーバからの漏洩確率を減らすことが出来る
- #15「会社に入るための入退出管理(カード式)システムを採用する」
  - 部外者の立ち入りをかなりの確率で防ぐことが出来、第三者の行動を抑制できる

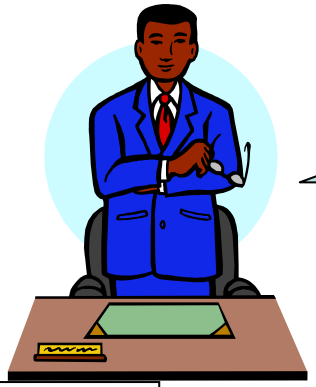
目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

何も対策をしない時の解

- システム管理部門で何も対策をしない時の漏洩確率は0.1506548（回/年）となった

現状の解を見ての話し合い

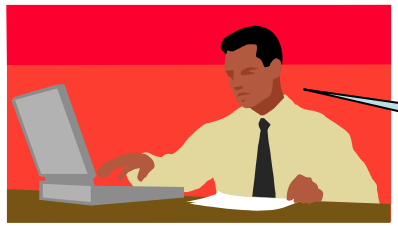


経営者

対策コストは5,000,000円以下に収めて欲しい。

漏洩確率は0.13以下に収めて欲しい。

顧客



従業員

利便性負担度は1.8以下、プライバシー負担度は1.0以下に収めて欲しい。

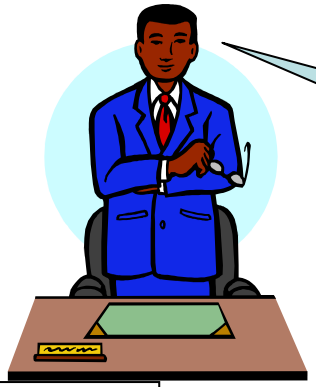
システム管理部門における最適解1

- 先の制約条件から最適解を求めると、以下のようになった

漏洩確率	0.1003824（回/年）
対策コスト	4,909,000（円）
利便性負担度	1.7
プライバシー負担度	1.0
目的関数の値	9,659,831,510（円）
対策案	#1, #3, #4, #7

#1：1年に4回パスワードを変更しなければいけないようにシステムを設定する(8文字以上)
#3：サーバに対して電子媒体（USBメモリー、CD/DVD、ポータブルHDD）を使用できない処置を行う
#4：社内の各部屋に監視カメラを設置し、社内の様子を撮影することにより不審な行動を監視する
#7：メールのフィルタリングツールを導入し、メールの送受信を制限する（添付ファイルを含んでいるメールの社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ、送れないようにする）

現状の解を見ての話し合い

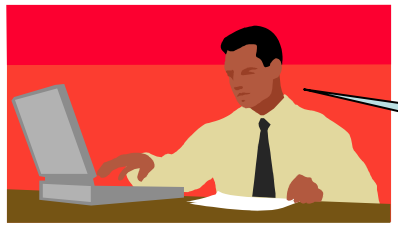


経営者

対策コストは問題ない。

漏洩確率も問題ない。

顧客



従業員

対策案#4は採用しない
で欲しい。

システム管理部門における最適解2

- 先の制約条件から最適解を求めると、以下のようになった

漏洩確率	0.1006312（回/年）
対策コスト	4,309,000（円）
利便性負担度	1.7
プライバシー負担度	0.5
目的関数の値	9,659,831,510（円）
対策案	#1, #3, #7

#1：1年に4回パスワードを変更しなければいけないようにシステムを設定する(8文字以上)
#3：サーバに対して電子媒体（USBメモリー、CD/DVD、ポータブルHDD）を使用できない処置を行う
#7：メールのフィルタリングツールを導入し、メールの送受信を制限する（添付ファイルを含んでいるメールの社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ、送れないようにする）

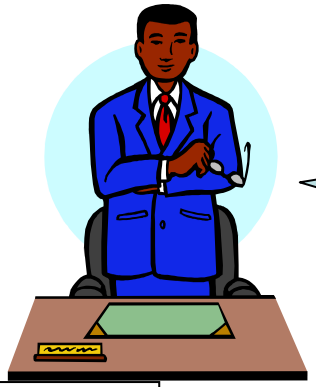
目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

何も対策をしない時の解

- 事務部門で何も対策をしない時の漏洩確率は0.2229192（回/年）となった

現状の解を見ての話し合い



経営者

対策コストは200,000,000円以下に収めて欲しい。

漏洩確率は0.2以下に収めて欲しい。

顧客

従業員

利便性負担度は3.0以下に、プライバシー負担度は1.0以下に収めて欲しい。

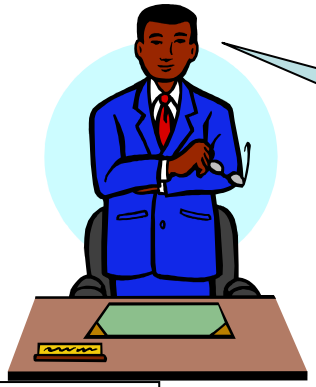
事務部門における最適解1

- 先の制約条件から最適解を求めると、以下のようになった

漏洩確率	0.1499854（回/年）
対策コスト	32,257,700（円）
利便性負担度	3.0
プライバシー負担度	0.6
目的関数の値	9,952,661,121（円）
対策案	#1, #2, #6, #12

#1：1年に4回パスワードを変更しなければいけないようにシステムを設定する(8文字以上)
#2：サーバーとデスクトップPCとノートPCに業務に不要なソフトのインストールを禁止する
#6：メールのフィルタリングツールを導入し、メールの送受信を制限する
（社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ、送れないようにする）
#12:会社から、個人情報を含んだ印刷物の持ち出しを制限するルールを作る

現状の解を見ての話し合い

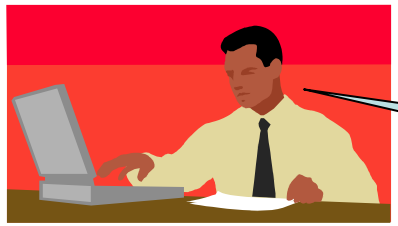


経営者

対策コストは問題ない。

漏洩確率も問題ない。

顧客



従業員

対策案#6、#7は採用しないで欲しい。

事務部門における最適解2

- 先の制約条件から最適解を求めると、以下のようになった

漏洩確率	0.193998（回/年）
対策コスト	33,772,700（円）
利便性負担度	2.4
プライバシー負担度	0.5
目的関数の値	10,026,805,014（円）
対策案	#1, #2, #4, #12

#1：1年に4回パスワードを変更しなければいけないようにシステムを設定する(8文字以上)
#2：サーバーとデスクトップPCとノートPCに業務に不要なソフトのインストールを禁止する
#4：社内の各部屋に監視カメラを設置し、社内の様子を撮影することにより不審な行動を監視する
#12:会社から、個人情報を含んだ印刷物の持ち出しを制限するルールを作る

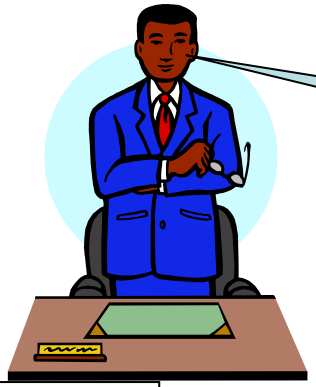
目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

何も対策をしない時の解

- 営業部門で何も対策をしない時の漏洩確率は0.5491134（回/年）となった

現状の解を見ての話し合い



経営者

漏洩確率が高いから、対策コストは多めに出そう。

漏洩確率が高い。
漏洩確率は0.4以下に収めて欲しい。

顧客

従業員

利便性負担度は3.0以下に、プライバシー負担度は1.0以下に収めて欲しい。

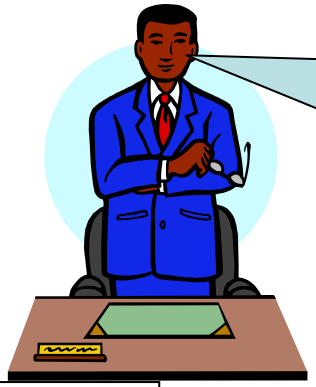
営業部門における最適解1

- 先の制約条件から最適解を求めると、以下のようになった

漏洩確率	0.2002667（回/年）
対策コスト	818,858,700（円）
利便性負担度	3.0
プライバシー負担度	0.6
目的関数の値	10,644,023,022（円）
対策案	#1, #2, #6, #8, #12

#1:1年に4回パスワードを変更しなければいけないようにシステムを設定する(八文字以上)
#2:サーバーとデスクトップPCとノートPCに業務に不要なソフトのインストールを禁止する
#6:メールのフィルタリングツールを導入し、メールの送受信を制限する
（社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ、送れないようにする）
#8:デスクトップPCとノートPCに対して電子媒体（USBメモリー、CD/DVD、ポータブルHDD）への書き出し時に強制暗号化を行う処置を取る（会社外のPCでは復号化できない）
#12:会社から、個人情報を含んだ印刷物の持ち出しを制限するルールを作る

現状の解を見ての話し合い

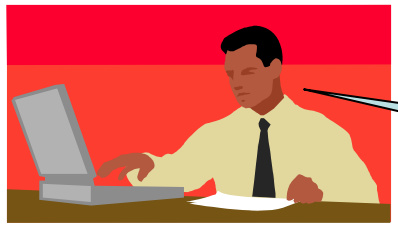


経営者

対策コストが高すぎるが、対策コストを減らすと漏洩確率が高くなりすぎるから止むを得ない。

漏洩確率は0.3以下に収めて欲しい。

顧客



従業員

対策案#6、#7は採用しないで欲しい。

営業部門における最適解2

- 先の制約条件から最適解を求めると、以下のようになった

漏洩確率	0.2535281（回/年）
対策コスト	814,373,700（円）
利便性負担度	2.4
プライバシー負担度	0
目的関数の値	10,715,936,245（円）
対策案	#1, #2, #8, #12

#1:1年に4回パスワードを変更しなければいけないようにシステムを設定する(八文字以上)
#2:サーバーとデスクトップPCとノートPCに業務に不要なソフトのインストールを禁止する
#8:デスクトップPCとノートPCに対して電子媒体（USBメモリー、CD/DVD、ポータブルHDD）への書き出し時に強制暗号化を行う処置を取る（会社外のPCでは復号化できない）
#12:会社から、個人情報を含んだ印刷物の持ち出しを制限するルールを作る

目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

各部門における最適解のまとめ

	システム管理部門	事務部門	営業部門
漏洩確率	0.1006312（回/年）	0.193998（回/年）	0.2535281（回/年）
対策コスト	4,309,000（円）	33,772,700（円）	814,373,700（円）
利便性負担度	1.7	2.4	2.4
プライバシー負担度	0.5	0.5	0
目的関数の値	9,660,215,835（円）	10,026,805,014（円）	10,715,936,245（円）
対策案	#1, #3, #7	#1, #2, #4, #12	#1, #2, #8, #12

各部門における最適解のまとめ

- 下記の対策案を全て採用し、会社全体としてMRCを適用した

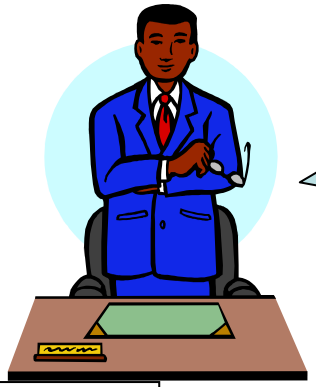
	システム管理部門	事務部門	営業部門
漏洩確率	0.1006312（回/年）	0.193998（回/年）	0.2535281（回/年）
対策コスト	4,309,000（円）	33,772,700（円）	814,373,700（円）
利便性負担度	1.7	2.4	2.4
プライバシー負担度	0.5	0.5	0
目的関数の値	9,660,215,835（円）	10,026,805,014（円）	10,715,936,245（円）
対策案	#1, #3, #7	#1, #2, #4, #12	#1, #2, #8, #12

3部門を通しての最適解1

漏洩確率	0.0999154（回/年）
対策コスト	945,971,700（円）
利便性負担度	3.1
プライバシー負担度	1.0
目的関数の値	10,494,835,486（円）
対策案	#1, #2, #3, #4, #7, #8,#12

#1:1年に4回パスワードを変更しなければいけないようにシステムを設定する(8文字以上)
#2:サーバーとデスクトップPCとノートPCに業務に不要なソフトのインストールを禁止する
#3：サーバに対して電子媒体（USBメモリー、CD/DVD、ポータブルHDD）を使用できない処置を行う
#4：社内の各部屋に監視カメラを設置し、社内の様子を撮影することにより不審な行動を監視する
#7：メールのフィルタリングツールを導入し、メールの送受信を制限する（添付ファイルを含んでいるメールの社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ、送れないようにする）
#8:デスクトップPCとノートPCに対して電子媒体（USBメモリー、CD/DVD、ポータブルHDD）への書き出し時に強制暗号化を行う処置を取る（会社外のPCでは復号化できない）
#12:会社から、個人情報を含んだ印刷物の持ち出しを制限するルールを作る

現状の解を見ての話し合い



経営者

対策コストが高すぎるので最も対策コストがかかっている対策案#8は採用しないで欲しい。
できれば、対策コストは2億円以下にしたい。

漏洩確率は問題ない。

顧客

従業員

対策案#4は採用しないで欲しい。また、利便性負担度は3.0以下にして欲しい。

3部門を通しての最適解2

- 先の制約条件から最適解を求めると、以下のようになった

漏洩確率	0.1513397（回/年）
対策コスト	131,556,700（円）
利便性負担度	2.9
プライバシー負担度	0.5
目的関数の値	9,784,549,794（円）
対策案	#1, #2, #3, #7, #12

#1：1年に4回パスワードを変更しなければいけないようにシステムを設定する(8文字以上)
#2：サーバーとデスクトップPCとノートPCに業務に不要なソフトのインストールを禁止する
#3：サーバに対して電子媒体（USBメモリー、CD/DVD、ポータブルHDD）を使用できない処置を行う
#7：メールのフィルタリングツールを導入し、メールの送受信を制限する（添付ファイルを含んでいるメールの社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ、送れないようにする）
#12:会社から、個人情報を含んだ印刷物の持ち出しを制限するルールを作る

目次

- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

最終的な最適解

漏洩確率	0.1513397（回/年）
対策コスト	131,556,700（円）
利便性負担度	2.9
プライバシー負担度	0.5
目的関数の値	9,784,549,794（円）
対策案	#1, #2, #3, #7, #12

#1：1年に4回パスワードを変更しなければいけないようにシステムを設定する(8文字以上)
#2：サーバーとデスクトップPCとノートPCに業務に不要なソフトのインストールを禁止する
#3：サーバに対して電子媒体（USBメモリー、CD/DVD、ポータブルHDD）を使用できない処置を行う
#7：メールのフィルタリングツールを導入し、メールの送受信を制限する（添付ファイルを含んでいるメールの社外メールアドレスへの送信は、直属上長にCCでメールの複製を送信しなければ、送れないようにする）
#12:会社から、個人情報を含んだ印刷物の持ち出しを制限するルールを作る

目次

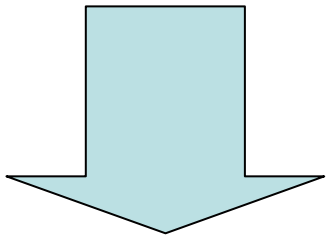
- 背景
- 企業におけるパラメータ
- 入力した対策案とその理由
- リスクコミュニケーションの過程
  - システム管理部門におけるリスクコミュニケーション
  - 事務部門におけるリスクコミュニケーション
  - 営業部門におけるリスクコミュニケーション
  - 3部門を通してのリスクコミュニケーション
- 最終的な最適解
- 考察

考察(1/2)

- 営業部門は従業員数が多いため、他の部門と比べて
  - 漏洩確率がやや高め
  - 対策コストが膨大
- システム管理部門は従業員数が少なく、紙媒体やノートPCを扱わないため
  - 漏洩確率が低い
  - 必要な対策は少なくて済む
  - 対策コストも少なくて済む

考察(2/2)

- ロールプレイではそれぞれの部門の特徴に特化した話し合いができたため、合意形成が取りやすかった
- 3部門に分けてMRCを適用し、それぞれの部門でどのような対策が有効なのかがわかっていたため、会社全体としてMRCを適用する回数が少なく済んだ



- 大企業の場合、部門ごとに分けて合意形成を行うことは有効であると考えられる

- 御清聴ありがとうございました