JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

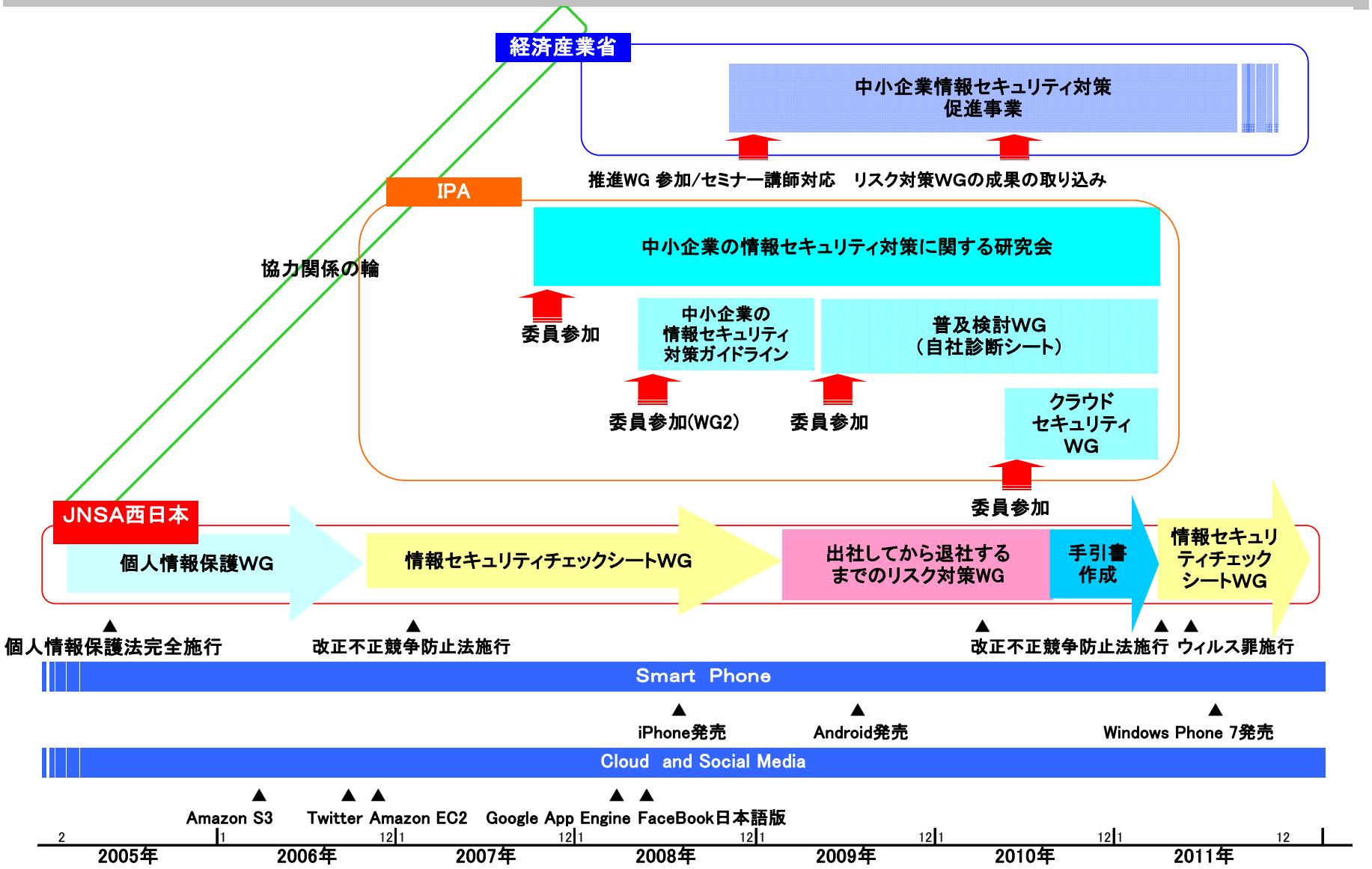
「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」の活用

嶋倉　文裕
JNSA西日本支部

2011年10月5日

NSF 2011 in Kansai

JNSA西日本支部の中小企業セキュリティ活動

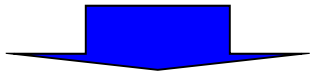


日常の危機管理

これまでの活動で認識した中小企業の限界

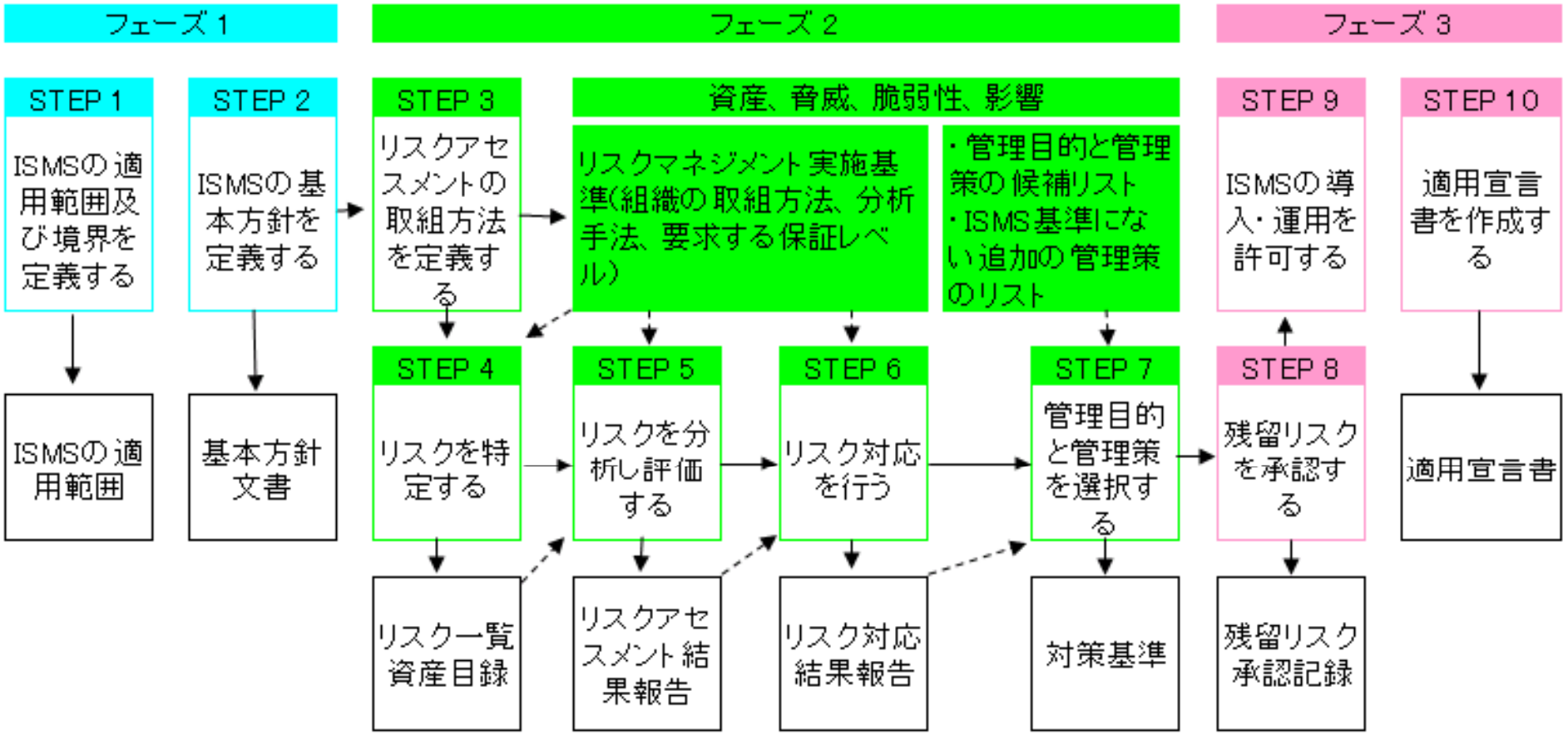
これまでの活動から見えた中小企業のセキュリティ

- トラブル経験がなく、自社は大丈夫と考えている。
- 情報セキュリティを理解できる人がいない。
- SI‘er、ベンダーに丸投げ、情報資産の保管・格納場所さえ分からない。



このような状況で、リスク対策が企業にとって重要であるかを理解させることができるか？

ISMSによるアプローチ手法



リスクアプローチ手法

・資産管理台帳からのアプローチ
企業の保有する情報資産を洗い出し、その資産に対するリスク分析・評価をおこなうアプローチ。

- システム管理者、資産の管理者だけで洗い出しが可能。
  ただし、ファイルサーバなどで集約的に管理されていなければ難しい。
- 資産の名称が同じでも業種、企業、部署、個人により内容は異なる。
- 資産の管理が不十分な場合、洗い出しが困難。
- 洗い出しの粒度が細かくなりがち。

リスクアプローチ手法

実は。。。
「情報セキュリティチェックシートWG」で情報資産管理台帳の洗い出しのアプローチを試みたが、固定資産台帳との区別がつかない、業界特有の資産名を例示しないと理解ができない、などの事実がわかりました

当時の活動の詳細
「中小企業の情報セキュリティ対策支援WG活動報告書」
http://www.jnsa.org/result/2008/west/0812report.pdf

リスクアプローチ手法

・業務からのアプローチ
　企業の持つ業務プロセスを洗い出し、その業務プロセスを構成する各業務に対するリスク分析・評価をおこなうアプローチ。

- それぞれの業務を行う担当者が、業務を洗い出す必要がある。
- 業種、企業、部署、個人によって業務はそれほどに変わらない。

例:「業務」の捉え方にもよるが、PCを利用した書類の作成、共用ファイルサーバへの情報格納、など仕事のやり方に着目すると変わらないと考える

リスクアプローチ手法

- 業務からのアプローチ
  - 資産の管理が不十分でも、業務の洗い出しは可能。
  - 洗い出しの粒度が大雑把になる可能性はある。

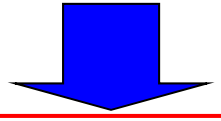
出社してから退社するまでのリスク対策WG

JNSA

「出社してから退社するまでのリスク対策WG」が考えたこと

中小企業では、十分な資産の洗い出しをすることが難しい。

業務からアプローチする方が、リスクと紐付けし易い（資産価値の把握は困難になるが）、トラブル経験がなく、自社は大丈夫と考えている中小企業にとって、セキュリティ対策の契機となる可能性がある。



日常の業務のなかで、ヒューマンエラーを少なくする仕組みと、社員の意識の向上や、スキルアップ

業務からのアプローチ手法

大きく、５つの日常サイクルと２つの特別な業務に分類

日常サイクル	
出社	出社時の会社への入館方法
社内	社内の仕事の仕方
社外	社外の仕事の仕方
退館・退出	会社をでるときの振る舞い、退館方法
帰宅	自宅での仕事の仕方や家族との会話
特別な業務	
人事管理	入社、退職、人事評価
システム管理	システム管理者の仕事

業務からのアプローチ手法

業務の洗い出し方法

とにかく、まずは抽出し、それから整理
“業務“そのものではなく、共通的な業務のやり方にフォーカスし洗い出す

- IT系の業務
- 非IT系の業務

業務からのアプローチ手法

洗い出した業務

ＩＴ系の業務
セキュリティエリアへのアクセス
PCの起動・ログイン
PCを使用した業務
ＰＣ・媒体の廃棄・処分
メールの受信確認
メールの送信（本文）
メールの送信（添付）
PCによる文書の保存
PCによる文書の作成
PCによるプリンタの使用
共有サーバの利用
WEBサイトへのアクセス
インターネットで収集した情報の利用
外部サービスを利用したファイル交換

業務からのアプローチ手法

洗い出した業務

非ＩＴ系の業務
FAXの送信
コピー使用
社内の人間とのコミュニケーション
書類の受け渡し・発送（見積書等）
記録媒体の発送
書類、記録媒体の保管
書類の保管・廃棄
電話での会話
業務の委託
離席
社外者との打ち合わせ
社内会議

業務からのアプローチ手法

リスクの洗い出し方法

洗い出した**業務**と情報を**保存、処理する場所**より
リスクを洗い出し

	脆弱性に起因する要素（人が何処何処で何々する）																										
	業務（人が何々する）	業務対象		情報を保存・処理する場所																								
		その業務をする人	業務を管理する人	建物（入り口）	部屋・エリア他	キャビネット	机上	PC	サーバ	ネットワーク	アプリケーション	USB他（媒体）	表示モニタ	紙	プリンタ	FAX	コピー機	ゴミ箱	会話	電話	携帯電話	ホワイトボード	ファイル交換等（外サ）	廃棄業（外サ）	委託業者（外サ）	宅配・郵送（外サ）
出社	入館		○	○																							
社内	セキュリティエリアへのアクセス		○		○																						
			○		○																						
	PCの起動・ログイン		○					○																			
			○					○																			

業務からのアプローチ手法

リスクの洗い出し方法

目標とするセキュリティ要件、現状のセキュリティレベルから想定するリスク事象を書き出す

	脆弱性に起因する要素（人が何処何処で何々する） 業務(人が何々する)	セキュリティ要件(目的)	現状のセキュリティレベル	リスク事象(リスクシナリオ)
出社	入館	許可されていない第三者のアクセスを防止する	従業員かどうかを識別、認証する仕組みが無い	社員以外の人間が社員になりすまし入館する
社内	セキュリティエリアへのアクセス	許可されていない部外者のアクセスを防止する	取り扱う情報の種類・重要度に応じたエリア分けがされていない	許可されていない人間が権限者になりすましセキュリティエリアに入る
		許可されていない部外者のアクセスを防止する	入退室記録が無い	重要な情報を扱うエリアへの入退室記録が無く、情報漏えい発生後、事件を追跡できない
	PCの起動・ログイン	情報への許可されないアクセスを防止する	PCに自動ログインの設定を行っている	利用者権限を持たない者がPCにアクセスでき、PCから利用できる情報を漏えいしてしまう
		情報へのアクセスを特定する	共通IDを利用している	共通IDを利用しているため、個人を特定するログを残せない、またパスワードの漏えいする可能性が高い
		情報への許可されないアクセスを防止する	パスワードが簡単なため覗き見で判ってしまう パスワードをメモとして書き貼り付けている	ログオン時の覗き見やパスワードをメモ書きし貼り付けていることによりパスワードが漏えいし、重要情報に不正アクセスされる

業務からのアプローチ手法

対策の検討

リスクから対策を検討、そのさい技術と人の両方を考える

	脆弱性に起因する要素（人が何処何処で何々する） 業務(人が何々する)	対策の仕組み	対策(技術的)	対策(人的)
出社	入館	社員証、入館システム(IDカード、バイオ認証、パスワード認証)、警備員、社員用と外部用の入り口が分離されている、無人受付がある、セキュリティカメラ	従業員に個人を特定できる社員証を与え、入館システムでチェックする	従業員に個人を特定できる社員証を与え、人がチェックする
社内	セキュリティエリアへのアクセス	ゾーニング（エリア分け）、入室システム(IDカード、バイオ認証、パスワード認証)、セキュリティカメラ	取り扱う情報の重要度に応じたエリア分けをし、システム的に入退室管理をする	取り扱う情報の重要度に応じたエリア分けをし、規程等ルールで入退室管理をする
		入退室システム、セキュリティカメラ	システム的に入退室記録（ログ）を残す	入退室の担当者が入退室者の入退室記録を管理台帳に記入する
	PCの起動・ログイン	システム特権をユーザアカウントに与えない。 自動ログインをさせないツールの導入。 自動ログインの設定をやめる	自動ログインの設定を解除し、ユーザアカウントから特権を除去する	自動設定を許可しない旨のルールの作成
		利用者ごとのIDの作成	利用者ごとのIDの作成	
		適当な強度（8文字以上、英数字記号の組み合わせ）を持つパスワードを設定できるIDを作成し、定期的に変更する パスワードを書いた紙を人目にさらさない	システムのパスワードポリシーを設定しユーザに強制的に複雑なパスワード、定期的パスワードの変更をさせる	パスワード文字数、文字列の組み合わせ、変更の周期等についてのパスワードポリシーをルール化しユーザに周知徹底する

業務からのアプローチ手法

対策が実行されているかのチェック

対策を導入したあと、それが的確に実行されているか、**チェックするポイント**も考える

	脆弱性に起因する要素（人が何処何処で何々する） 業務（人が何々する）	対策（技術的）	対策（人的）	対策のチェックポイント
出社	入館	従業員に個人を特定できる社員証を与え、入館システムでチェックする	従業員に個人を特定できる社員証を与え、人がチェックする	退職、人事異動した社員の社員証のたな卸しを定期的におこなう
社内	セキュリティエリアへのアクセス	取り扱う情報の重要度に応じたエリア分けをし、システム的に入退室管理をする	取り扱う情報の重要度に応じたエリア分けをし、規程等ルールで入退室管理をする	入退室（エリア）のアクセス権限表の確認および実際のカードでの確認
		システム的に入退室記録（ログ）を残す	入退室の担当者が入退室者の入退室記録を管理台帳に記入する	システムのログまたは入退室管理台帳の確認
	PCの起動・ログイン	自動ログインの設定を解除し、ユーザアカウントから特権を除去する	自動設定を許可しない旨のルールの作成	PCの自動設定がされていないことを確認する
		利用者ごとのIDの作成		システムまたはPCのアカウントの設定を確認する
		システムのパスワードポリシーを設定しユーザに強制的に複雑なパスワード、定期的パスワードの変更をさせる	パスワード文字数、文字列の組み合わせ、変更の周期等についてのパスワードポリシーをルール化しユーザに周知徹底する	システムのパスワードポリシーを確認する

手引書へのまとめ

JNSA

この取り組みの結果を手引書にまとめました。
ただし、WGでは「紙」媒体のリスクについても検討しましたが、手引書では、“対象がIT”、または“対策がITで可能”なものとし、それ以外は省いています。

http://www.jnsa.org/result/2010/chusho_security_tebiki.html

手引書とWGの違い

手引書で省いたもの

（１） 対象が紙・物に関するもの　※

（２） 電源、空調等の設備管理に関するもの

（３） 対策できないもの、対策が中小企業レベルでは難しいもの

- 経営者、システム管理者等の権限者の不正
- DoS攻撃

（４） 個人情報保護に関するもの

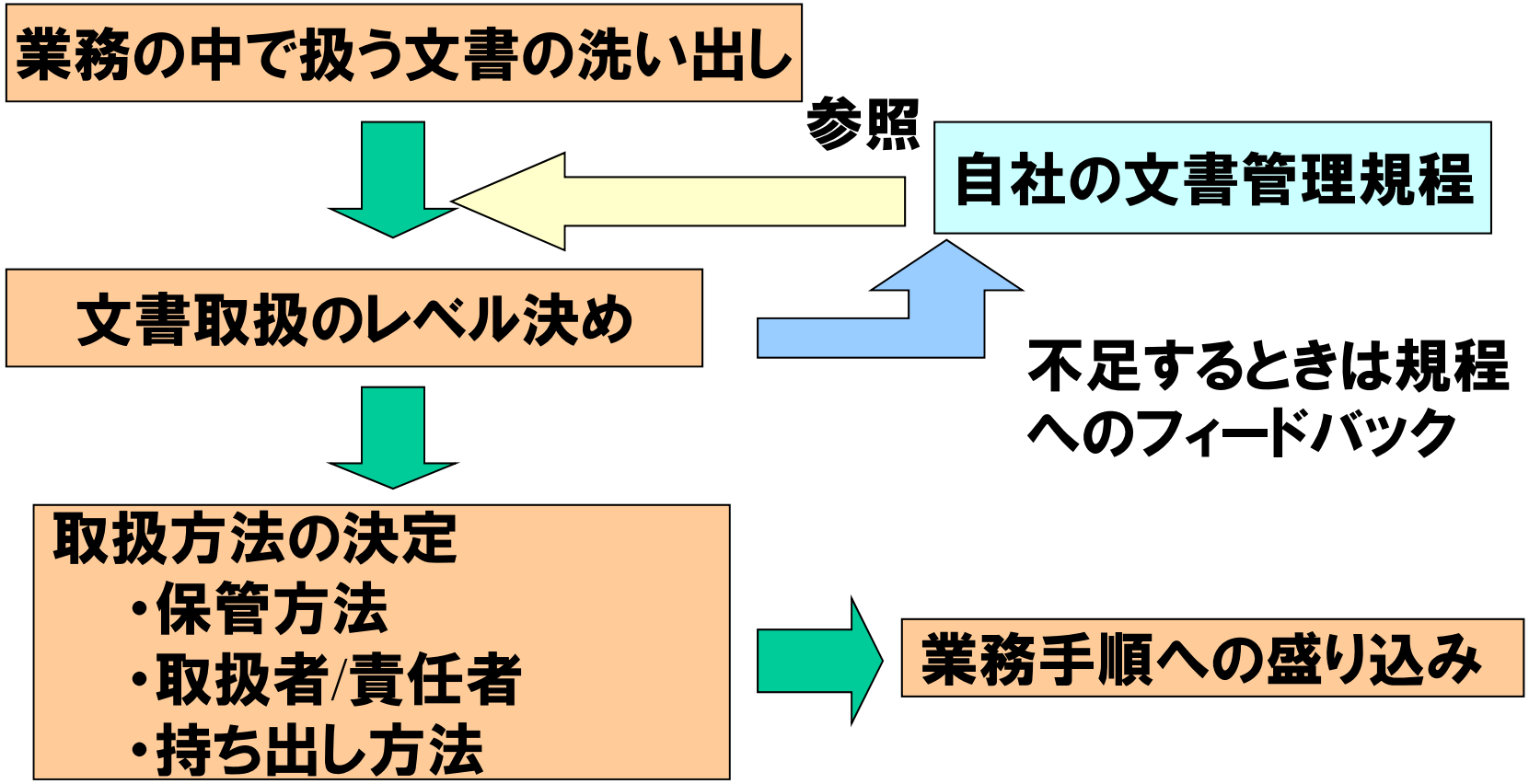
（５） 委託管理に関するもの

（６） 対策が教育・啓蒙になるもの

手引書では参考資料を提示

※ 手引書では記憶媒体、PCの持ち出し、廃棄などを盛り込んでおり、紙についても同様なシーンのリスクの把握は可能

参考）紙の対策

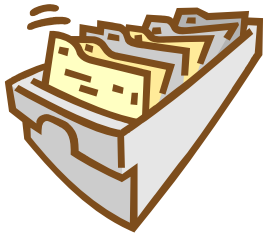


参考）紙の対策

保管方法のポイント

ちょっとしたファイングの方法でミス防止

- 書類の混在を防止するファイリングの単位
- ラベルやカラーによる見た目での間違い防止



手引書の体系

「第１部　情報セキュリティ管理策」
「第２部　業務に基づく情報セキュリティ対策」
の二部から構成

第１部はISMS的に管理策を中心に整理
第２部は業務ベースに整理
手引書では、この２つを結びつけている
（手引書の第１部は第２部をベースに整理）

→　中小企業が苦手とするISMSアプローチと業務からのアプローチを結びつけることで、リスク認識をし易く！

手引書の体系

「第１部　情報セキュリティ管理策」

青字は情報システム管理の観点

1. セキュリティ境界と入退室管理
2. 認証と権限
3. ウイルス及び悪意のあるプログラムに対する対策
4. パッチの適用
5. バックアップ
6. ログの取得
7. 記憶媒体の管理
8. 暗号化
9. アプリケーションの利用

手引書の体系

「第1部　情報セキュリティ管理策」

青字は情報システム管理の観点

10. 電子メールの利用
11. 外部サービスの利用
12. ネットワークのアクセス制御
13. クリアデスク・クリアスクリーン
14. 変更管理
15. 構成管理
16. 障害・事故管理
17. 容量・能力の管理
18. Webの開発・管理

手引書の体系

1.セキュリティ境界と入退室管理

(1) 管理目的

情報と情報機器への許可されていないアクセスを防止するため

(2) 管理策

① 情報と情報機器のある場所を保護するため、門、入口、壁、仕切り等の物理的な境界を設定する

② 設定された境界を越える権限を許可された者のみに与え、許可されないアクセスを防止するために、境界にカード制御による入口、守衛等の設備を設置する

手引書の体系

(3) 運用で心がけるポイント

① 退職、人事異動に伴う、アクセス権限の見直しを行う

② 定期的に入退室記録を確認する

(4) 関連する管理項目

認証と権限、クリアデスク・クリアスクリーン

手引書の体系

「第2部　業務に基づく情報セキュリティ対策」

「出社」、「社内業務」、「社外業務」、「退社」、「帰宅」、「システム管理業務」の6種類、62業務

出社	1業務
社内業務	31業務
社外業務	12業務
退社	1業務
帰宅	2業務
システム管理業務	15業務

手引書の体系

業務No.2	セキュリティエリアへのアクセス
情報を処理・保存するための実体	■建物・部屋・エリア　□キャビネット　□机上　□PC　□サーバー □ネットワーク　□アプリケーション　□記憶媒体（USBメモリー他） □プリンター　□FAX　□コピー機　□携帯電話　□電子機器（ICレコーダー、カメラ他）　□外部のサービス（ファイル交換サービス等）
影響	■機密性　■完全性　■可用性　□適法性
脅威の主体	□システム管理者（本人）　□システム管理者（本人外） □従業員（本人）　■従業員（本人外）　■訪問者　□外部 □偶発的要因
責任者	□システム管理者　■業務・人事管理者　□従業員

手引書の体系

セキュリティの対策の目的	情報と情報機器への許可されていないアクセスを防止するため
現状のセキュリティレベル	取り扱う情報の重要度に応じたエリア分けをしていない
リスクシナリオ	許可されていない者がセキュリティエリアに入り権限のない情報を閲覧する
技術的対策	取り扱う情報の重要度に応じたエリア分けをし、システム的（入退室管理システム）にエリア管理（入退室管理）をする
人的対策	取り扱う情報の重要度に応じたエリア分けをし、ルール等でエリア管理（入退室管理）をする
運用で心がけるポイント	・エリア（室）のアクセス権限表に退職者、人事異動が反映されているか確認する ・エリア入退（入退室）カードの確認及び棚卸を行う
備考	

関連する管理策：1.セキュリティ境界と入退室管理 ①,② 2.認証と権限 ③,④

情報セキュリティチェックシートとの紐づけ

情報セキュリティチェックシートとの紐付け

情報セキュリティチェックシート

２つの対象者向けから構成
・経営者、経営層向け
・情報セキュリティ責任者・担当者

ISO27001　管理策をベースに策定

詳細は下記、URLを
http://www.jnsa.org/seminar/2008/1217nsf2008/data/1217-C2-01checksheetA3.xls

情報セキュリティチェックシートとの紐付け

情報セキュリティチェックシートと手引書との紐付け

管理策

手引書　業務No.

No.	キーワード	付属書A他	9-5紐付け	トラブル事象例
1	情報セキュリティ方針	システム管理基準　Ⅰ.情報戦略　1.全体最適化(1),(6) A.5.1.1 情報セキュリティ基本方針文書 A.5.1.2 情報セキュリティ基本方針のレビュー	無し	機密性、完全性、可用性のバランスを取ったシステムの利用方針がないと全てのトラブルに発展する可能性がある
2	責任の明確化	システム管理基準　Ⅰ.情報戦略　2.組織体制 2.1(1),2.2(1) A.6.1.1 情報セキュリティに対する経営陣の責任 A.6.1.2 情報セキュリティの調整 A.6.1.3 情報セキュリティ責任の割当て A.6.1.4 情報処理設備の認可プロセス A.6.1.6 関係当局との連絡 A.6.1.7 専門組織との連絡 A.6.1.8 情報セキュリティの独立したレビュー A.8.1.2 選考 A.8.1.3 雇用条件 A.8.2.1 経営陣の責任 A.8.2.3 懲戒手続き A.8.3.1 雇用の終了又は変更に関する責任 A.8.3.2 資産の返却	1,2,21	責任の明確化ができていないとトラブル時の対処が遅れたり、事後の対処が的確に出来ない等の可能性がある

情報セキュリティチェックシートとの紐付け

情報セキュリティチェックシートと手引書のそれぞれの特徴

- 情報セキュリティチェックシートはISMSベースのため、手引書の第１部より範囲が広い。
- 情報セキュリティチェックシートのトラブル事象は、知識、経験が少ない中小企業の方にとって、管理策からトラブル事象が結びつきにくい。
- 手引書の第２部は、現状のセキュリティレベルとリスクシナリオがあり、業務に潜むリスクが理解しやすいが、リスクの把握、対策がポイント的になる。

情報セキュリティチェックシートとの紐付け

JNSA

情報セキュリティチェックシートと手引書との紐付けができると、何が良いのか．．．．

- ISMS管理策ベースの情報セキュリティチェックシートの網羅性を活かす。
- 情報セキュリティチェックシートのトラブル事象が、業務ベースのリスクシナリオと結びつくことで、リスクについて、理解しやすい。
- 情報セキュリティチェックシートには対策欄がない(※)が、手引書と結びつくことで管理策の対策を理解しやすい。

※オリジナルのシートには対策欄は存在するが、未記入

チェックシートと手引書の両方からのアプローチ

JNSA

ポリシー観点からのアプローチ
チェックシート

手引書
業務の観点からのアプローチ

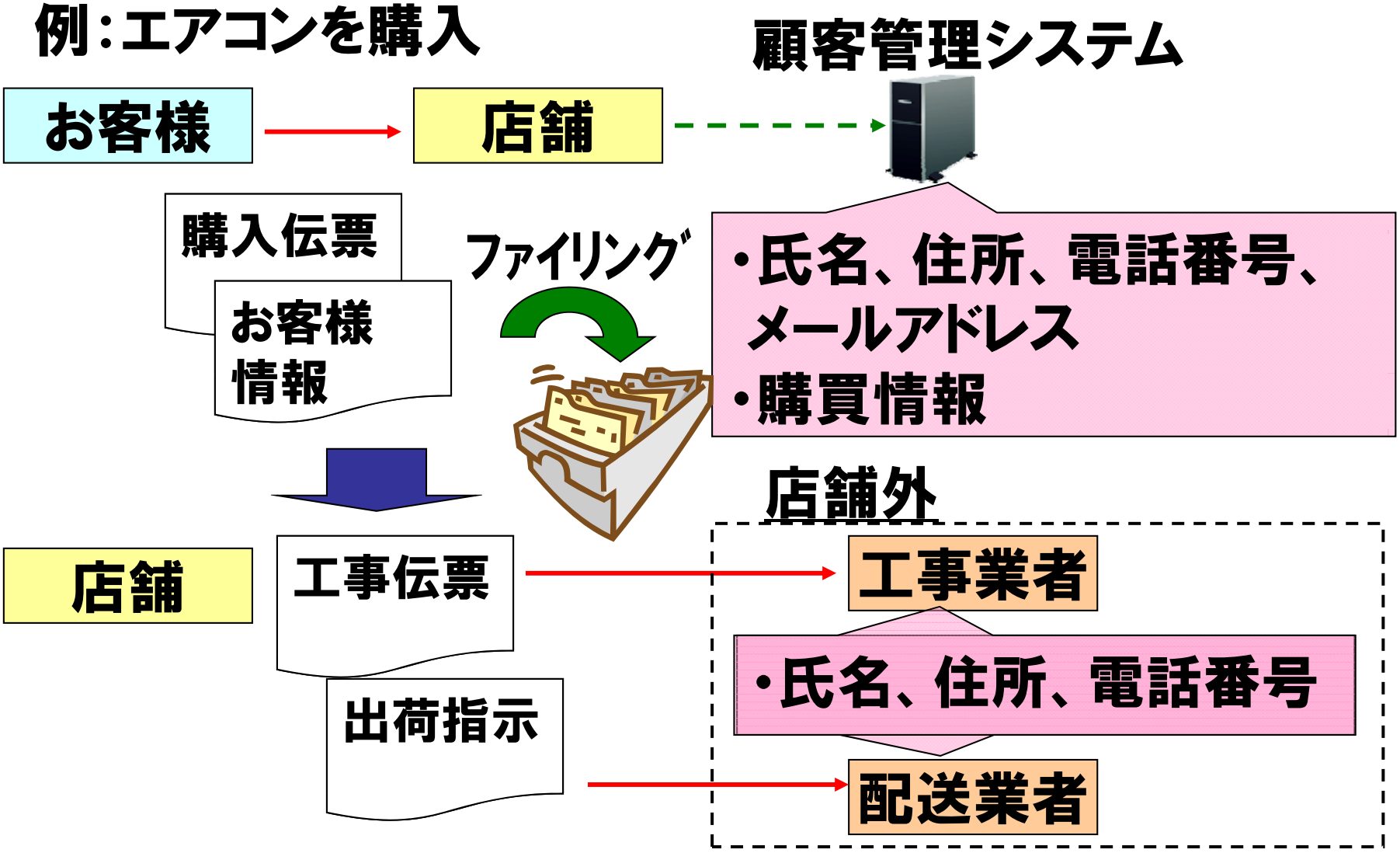
- ポリシーへの準拠性チェック
- 該当業務にとって対策していないことによるリスクの有無、大きさの把握

対策の必要性・優先順位付けの判断

具体的な業務からの
アプローチ案

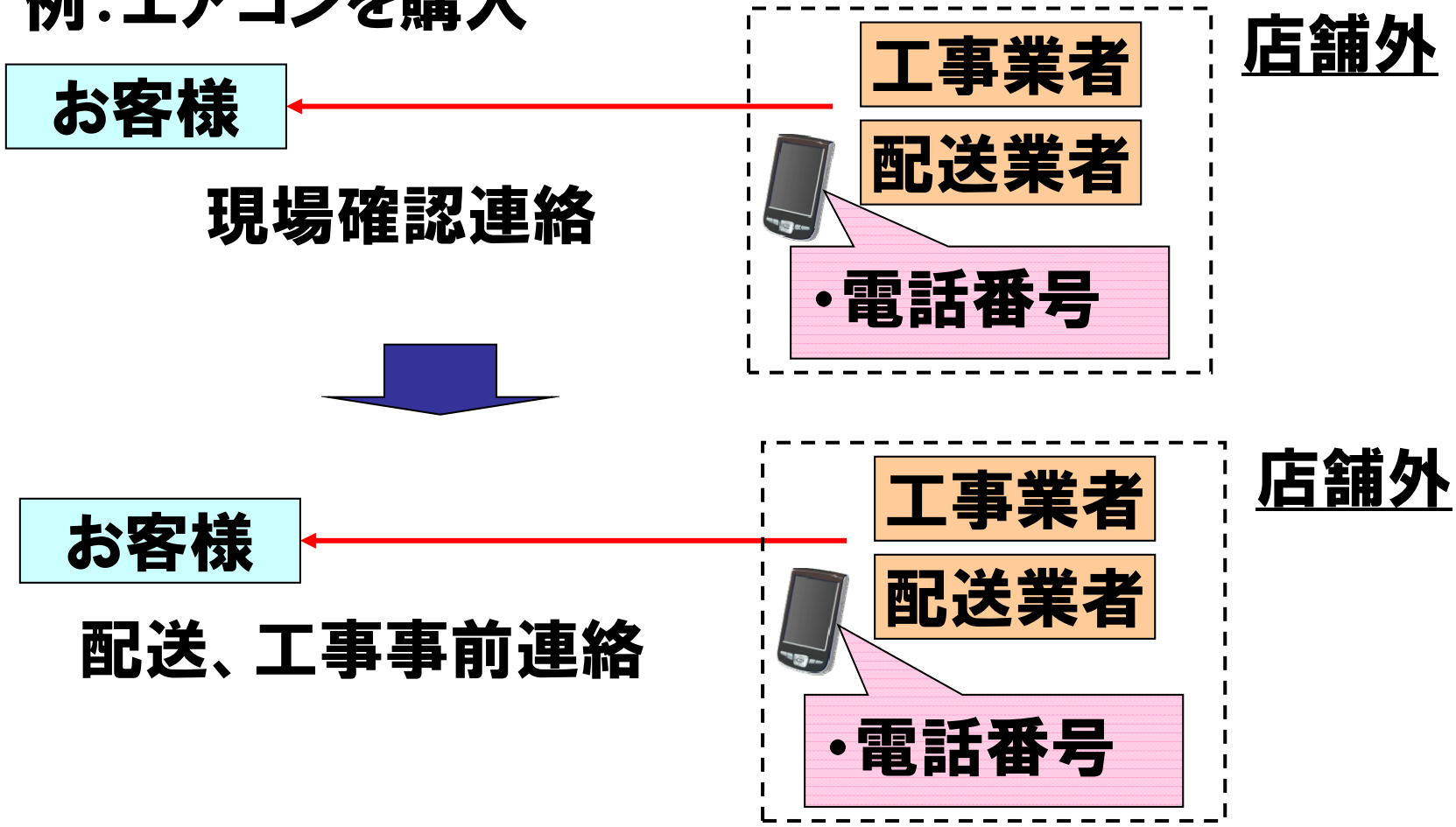
電気店で電気製品購入(１)

例:エアコンを購入



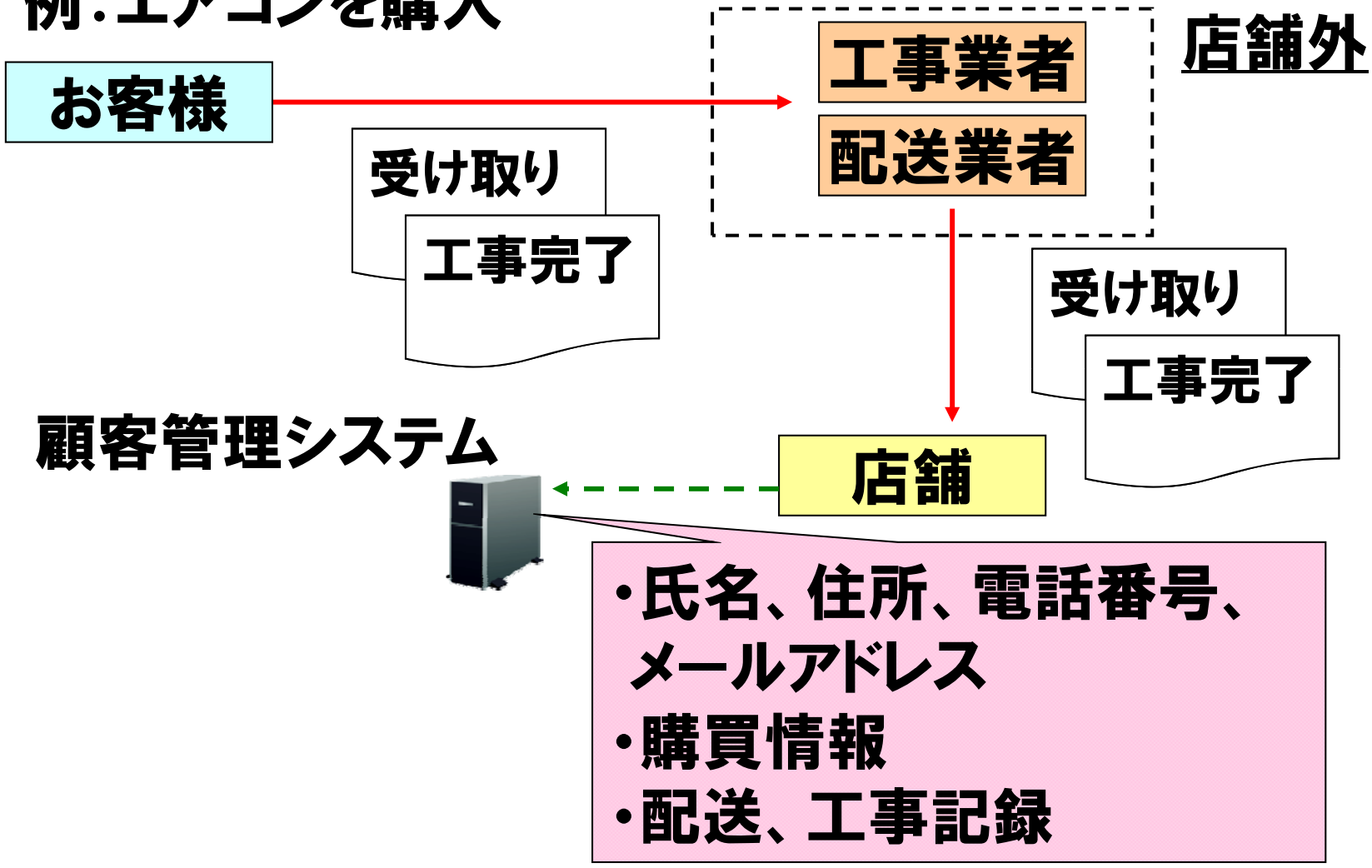
電気店で電気製品購入(２)

例:エアコンを購入



電気店で電気製品購入(３)

例:エアコンを購入



情報格納先と業務からの想定リスクの洗い出し

最終的に業者側に残った情報

保存先	形式	情報内容
顧客管理システム	電子	住所、氏名、電話番号、メールアドレス、購買記録
購入伝票	紙	住所、氏名、電話番号、決済情報、
受け取り工事完了	紙	住所、氏名、電話番号
配送、工事担当者の携帯電話	電子	氏名、電話番号

業務
共有サーバの利用
サーバの管理業務

想定リスク
誤入力
不正アクセス
障害後の復旧不可

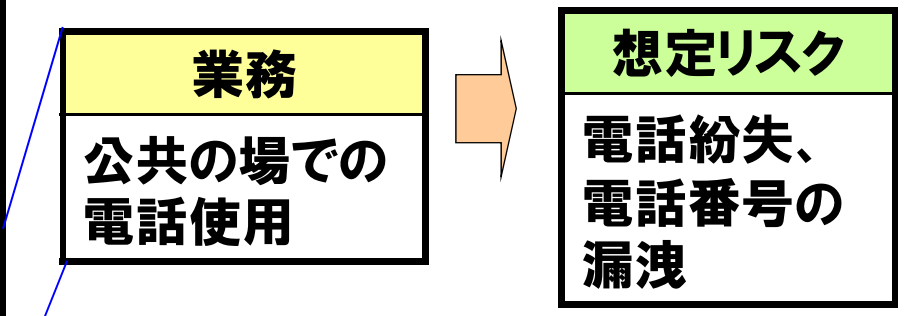
業務
書類の保管
書類の廃棄

想定リスク
紛失
不正持ち出し
誤廃棄

情報格納先と業務からの想定リスクの洗い出し

一時的に外部に持ち出す情報

保存先	形式	情報内容
工事見積り 受け取り 工事完了	紙	住所、氏名、電話番号
配送、工事担当者の携帯電話	電子	氏名、電話番号



洗い出したリスクと管理策の検討

最終的に事業者側に残った情報

保存先	形式	情報内容	リスク	管理策
顧客管理システム	電子	住所、氏名、電話番号、メールアドレス、購買記録	アクセス権限のない者による不正アクセス、情報の漏洩	アクセス時の認証とアクセス権限管理
購買伝票	紙	住所、氏名、電話番号、決済情報	誤廃棄、不正持ち出しによる情報の漏洩	鍵付ロッカーでの保管

洗い出したリスクと管理策の検討

最終的に事業者側に残った情報

保存先	形式	情報内容	リスク	管理策
工事見積り書 受け取り 工事完了	紙	住所、氏名、電話番号	誤廃棄、不正持ち出しによる情報の漏洩	鍵付ロッカーでの保管
配送、工事担当者の携帯電話	電子	氏名、電話番号	紛失による情報の漏洩	登録の禁止、リダイヤルの削除の目視確認

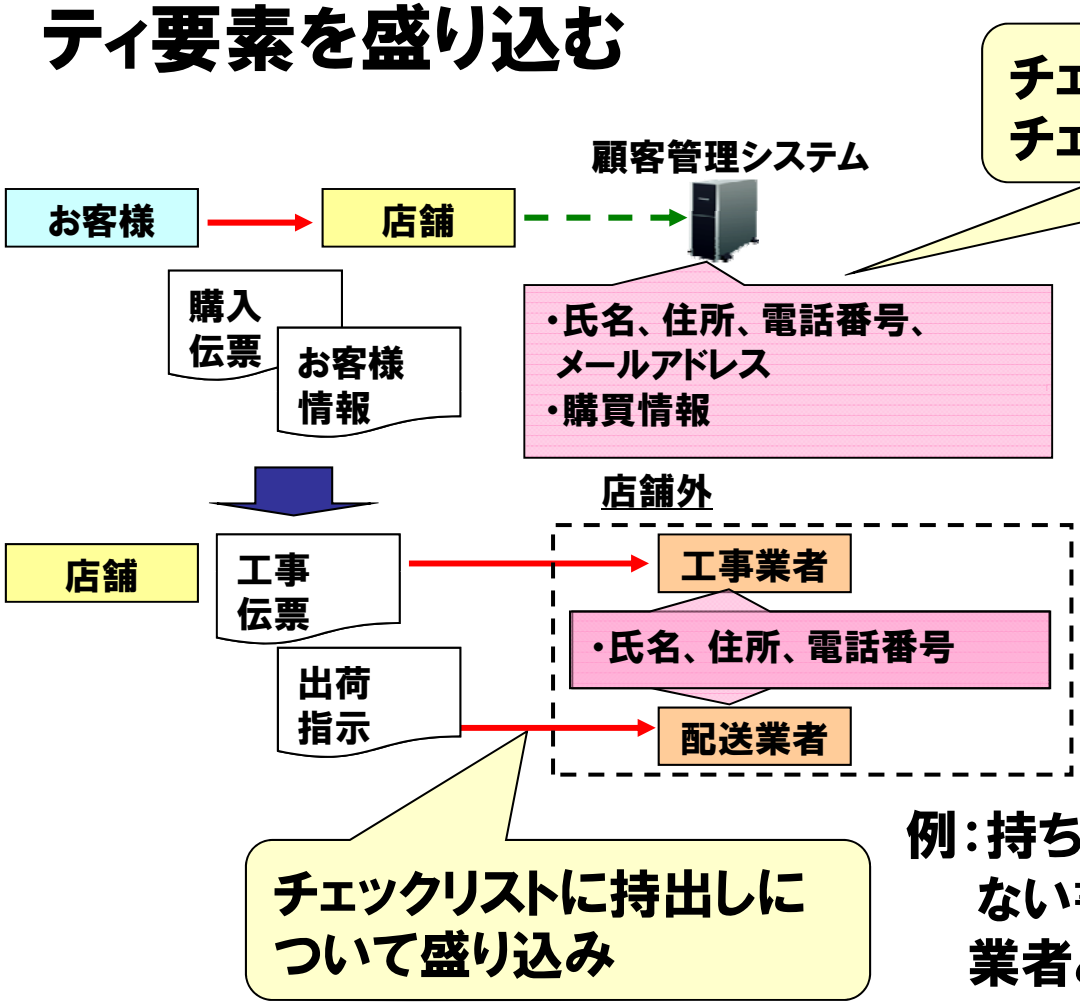
洗い出したリスクと管理策の検討

一時的に外部に持ち出す情報

保存先	形式	情報内容	リスク	管理策
工事見積り 受け取り 工事完了	紙	住所、氏名、 電話番号	紛失による情報の 漏洩	当日分のみの 持ち出し
配送、工事 担当者の 携帯電話	電子	氏名、電話番 号	紛失による情報の 漏洩	登録の禁止

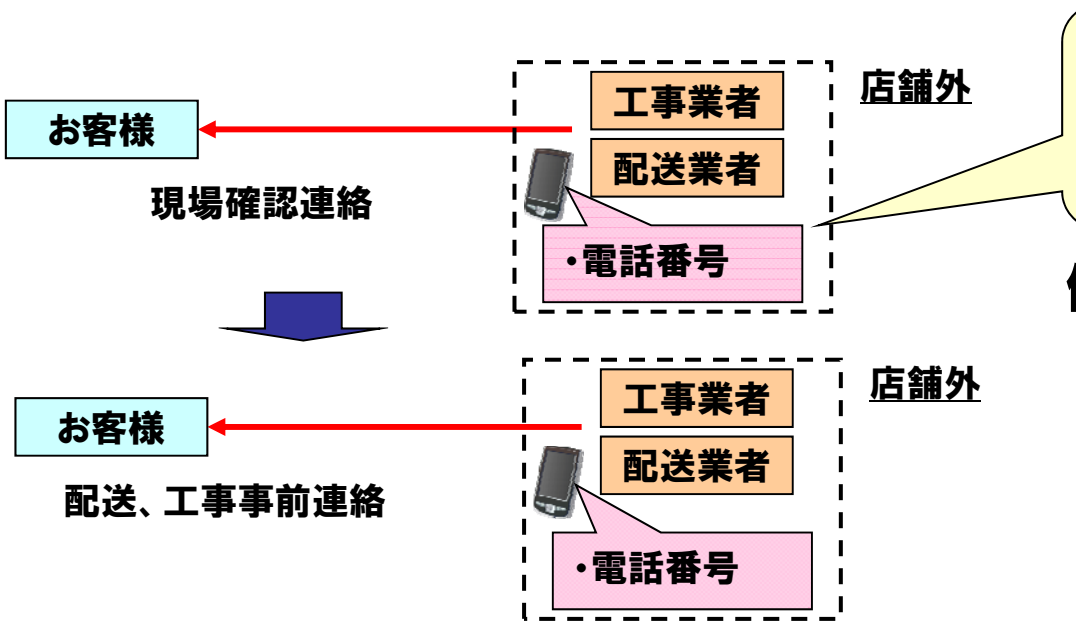
業務手順にセキュリティ要素の盛り込み

業務の作業チェックリストを作成し、その中にセキュリティ要素を盛り込む



業務手順にセキュリティ要素の盛り込み

業務の作業チェックリストを作成し、その中にセキュリティ要素を盛り込む



チェックリストに携帯電話への電話番号の登録について盛り込み

例：電話帳に登録していない、
リダイヤルを消去したこと
を確認したか
携帯はリモートロック、
リモートワイプか定期的に
確認したか

手順書、チェックシートの今後

今後の作業

手引書

「情報セキュリティチェックシート」との紐付けで検出した「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」修正

情報セキュリティチェックシート

中小企業が実際に実践できる情報セキュリティ対策アプローチ手法の提示、チェックシートのバージョンアップやライフプロセスベースのリスク視点での対策シート作成

今後の作業

JNSA

共通

クラウド、スマートフォンなどの新デバイスへの対応

- クラウド利用のリスク

  中小企業のクラウド利用シーン

  - Public Cloud SaaS利用
  - ASP利用

  自社でシステムをもつリスク、持たないリスクどっち？

- スマートフォン利用のリスク

  中小企業のスマート利用シーン

  - 社外でのPublic Cloudにアクセスする端末
  - 会社支給　or 個人所有
  - Android vs iPhone

  スマートフォンのリスク、PCのリスク　違いは？

ご清聴ありがとうございました。

引き続き、午後のセミナーをお楽しみに