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

2011 年 3 月 30 日版

NPO 日本ネットワークセキュリティ協会　西日本支部

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

2011 年 3 月 30 日版

NPO 日本ネットワークセキュリティ協会　西日本支部

はじめに

企業における情報セキュリティ対策のレベルアップには中小企業の情報セキュリティ対策の向上が欠かせないとして、セキュアジャパン 2010 にも中小企業に対する情報セキュリティ対策支援が盛り込まれていますが、リスクの変化に応じた対応を機動的に行う要求に、中小企業の環境・体制が阻害要因となり、コスト感のある複数かつ重畳的な施策に追随していけないため、中小企業の対策スピードは期待に反して上がらない現状にあります。

そこで、JNSA 西日本支部では優秀な技術を持ち、産業の要となっている中小・零細企業が多く存在する関西から、中小企業の情報セキュリティ対策は如何にあるべきか！を手引きとして作成・提供する活動を 2004 年からスタートさせました。2006 年には「中小企業向け個人情報保護対策チェックシート」を、2008 年には「中小企業向け情報セキュリティチェックシート」をそれぞれ作成・公開し、情報セキュリティ対策の入り口となる情報資産の洗い出しと情報資産の管理台帳の整備を支援するための「情報資産管理台帳ワークシート」を併せて提供、チェックシートの作成、アンケート調査の過程で得られた成果を、「中小企業の情報セキュリティ対策支援活動報告書」として取りまとめ公開しました。

チェックシートやワークシートの提供・アンケート調査の過程で明らかになった課題は、中小企業にとって保有する情報資産を洗い出し、リスクの評価、対策を行うことは、非常に敷居の高いことであり、独力ではたいへん厳しいと言う結果でした。
そこで、課題克服に資するとともに、これまでの西日本支部の活動の集大成として、中小企業ならどこでも行っている一般的な業務に潜む情報セキュリティ上のリスクを洗い出し、評価、対策することを支援する「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」を作成することとしました。

もちろん、人が不注意によって犯してしまう過ちをゼロにすることは不可能です。しかし、それゆえに不祥事や事故に学び、その発生頻度を減らし、発生時の被害を極力抑え込むための改善が不断の努力、組織を挙げた取り組みのもとに行われなければなりません。

リスクを評価した業務は 200 を超えるものとなりましたが、このうち本手引きでは読者のみなさんに是非行って欲しい情報セキュリティ対策を 18 の管理項目ごとに纏め、情報セキュリティの基礎知識レベルで取り組むことが出来る 62 の業務に基づく情報セキュリティ対策として整理統合、対策の選択を有効性・効率性とコスト感から判断でき

る様に技術的対策と人的対策に分けて記述するとともに運用で心がけるポイントを併記しています。

読者自身の情報セキュリティ対策の手引書として活用戴くことで、様々な業種・規模の読者のみなさんに日常の業務処理における必見・愛読の書として活用いただければ幸いです。

NPO 日本ネットワークセキュリティ協会
顧問・西日本支部長
井上　陽一

目次

導入部

1.概要

「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」(以下、「本手引き」という)は、抽象的あるいは技術的に難解になりがちな情報セキュリティ対策について、平易な具体的対策例を紹介することで、対象となる中小企業が出来る限り手間と時間を掛けずに、情報セキュリティ対策を実践できるように作成した手引きである。

提示する管理策は、中小企業であればどこでも行っている一般的な業務に潜む情報セキュリティ上のリスクを想定し、業務の継続を阻害する極端な管理策あるいは禁止事項を避け、日常、合理的に行える管理レベルを目指すように配慮した。

2.本手引きの対象企業

中小企業基本法第 2 条では、中小企業を業種・従業員数・資本規模の 3 つの要素から定義しているが、本手引きでは、中小企業であればどこでも行っている一般的な業務に着目した情報セキュリティ対策の実践を支援することとしているため、業種・資本規模に関わらず、従業員数 300 人以下を便宜上中小企業として扱う。

また、日本ネットワークセキュリティ協会　西日本支部(以下、「JNSA 西日本支部」という)では、多年に亘る中小企業における情報セキュリティ対策の実態調査・研究の結果から、中小企業を、情報セキュリティにおける対策の要請から表 0-1 のとおり、4 つの分類に定義している。

上付き(N)は参考資料の番号を示す

分類群	企業分類	情報セキュリティの意識	情報セキュリティ対策の要請	管理レベル
Ⅰ	他企業との取引のウエイトが高い企業	◎	複数の取引先から情報セキュリティ対策を求められている。	取り扱う情報に応じてISMS、プライバシーマークなど第三者認証の取得
Ⅱ	自社の情報セキュリティ対策が必要で対策することの必要に迫られている企業	○	第三者認証の取得までは必要とはしないが、企業価値向上・内部統制等目的から対策する事の必要に迫られている。	本手引き
Ⅲ	自社の情報セキュリティ対策が必要であるが実践が伴わない企業	△	守るべき情報資産があり、守らねばならない必要意識が漠然とはあるが、費用対効果が見えず躊躇・逡巡しており、情報セキュリティ対策の実践が求められている。	
Ⅳ	情報セキュリティ対策の必要を感じていない企業	×	対外的な影響は少なく限定的であり、必要最低限の情報セキュリティ対策とその妥当性の検討が求められている。	

表 0-1 情報セキュリティにおける対策の要請による中小企業の分類[1]

本手引きでは分類群Ⅱ、ⅢとⅣに分類される企業が対象となる。分類群Ⅰに分類される「他企業との取引のウエイトが高い企業」は、ISMS(Information Security Management System)認証[2][3]やプライバシーマーク認証[5][6]を取得、あるいはそれらと同等の強いセキュリティ管理策を要求されており、すでに十分なセキュリティ管理レベルに達していると考えられるため、本手引きの対象から除外した。

3.本手引きの対象読者

本手引きの対象読者は、中小企業で、実際にシステムの運用管理に携わっているシステム管理者、または何らかのシステムの運用管理に携わっている方(システムの運用管理を外部委託している場合、委託先の管理業務も含む)を対象としている。

4.本手引きの使用方法

本手引きは、「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２部から構成されている。

上付き[N]は参考資料の番号を示す

(1) 第 1 部　情報セキュリティ管理策

第 1 部では中小企業に行なって欲しい情報セキュリティ対策を 18 の管理項目としてまとめ、管理項目ごとに管理策を記述している。

なお、各管理策において、大きな投資及び技術的・運用的に難しいものについては参考として記述している。

(2) 第 2 部　業務に基づく情報セキュリティ対策

第 2 部では、中小企業で行う業務を大きく、「出社」、「社内業務」、「社外業務」、「退社」、「帰宅」、「システム管理業務」に分け、各業務に潜むセキュリティ上の脆弱性(現状のセキュリティレベル欄)により発生する可能性があるリスク(リスクシナリオ欄)に対応した情報セキュリティ対策を、技術的な対策と人的な対策に分け記述している。

なお、記載した業務は企業の行う業務をすべて網羅している訳ではない。また、その業務に付随するセキュリティ上の脆弱性、及びリスクに関しても、すべて網羅している訳ではない。「5.管理策から省いた項目」に記述するように意図的に管理策から省いた項目もあり、第 2 部で記載したリスク及び管理策に対応するだけでは十分ではないことに注意して欲しい。

(3) 第 1 部と第 2 部の対応

「第 1 部　情報セキュリティ管理策」と「第 2 部　業務に基づく情報セキュリティ対策」の対応は第 1 部の初めに記載しているので、第 1 部に目を通して頂き、何の為にその管理策を行うのかが理解頂けない場合は、第 2 部と紐づけて参照頂きたい。

(4) 情報セキュリティ対策シート

第 2 部の最後に白紙の「情報セキュリティ対策シート」を用意した。読者自身が、本手引きを参考に※、自社の業務に潜む脆弱性、リスクを洗い出し、自社に相応しい対策を考え、さらには新たな業務、脆弱性、リスクに対応するための定期的な見直しを、「運用で心がけるポイント」を参考に継続・実践されることで、セキュリティ強度の向上につながれば幸いである。

(5) 追補版の作成

本手引書でのリスクシナリオは近年通常的に発生しているインシデントを参考に引用しているが、スマートフォーン、タブレットに代表される新しいデバイスの出現に伴う業務、脆弱性、リスクに対応する情報セキュリティ対策についても追補版として継続的に公表したいと考えている。

※「業務」とは異なる「情報資産」からのリスク対策のアプローチについて、「付録　2.情

上付き(N)は参考資料の番号を示す

報資産の洗い出しについて」に記載した。また「図　付録-2 ISMS 構築のステップ(JIS Q 27001:2006)」は「業務」「資産」に関係なく共通的にアプローチできる構築ステップなのでぜひ参考にして欲しい。

5.管理策から省いた項目

本手引きの管理策の対象は、“対象が IT であるか対策が IT で可能”なもののみとした。このため、次に列挙した(1)から(6)は、管理策の対象から省いた。なお(4)、(5)、(6)に関しては、関連するリンクを参考資料に記載したので、参考にして欲しい。

(1) 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) ＩＴで対策できないもの、対策が中小企業レベルでは難しいもの
    ① DoS 攻撃
    ② 経営者、システム管理者等の権限者の不正
(4) 個人情報保護に関するもの[5][6][7][8]
(5) 委託先管理に関するもの[17]
(6) 対策が教育・啓蒙になるもの[18]

上付き[N]は参考資料の番号を示す

第１部　情報セキュリティ管理策

0.1.第 1 部と第 2 部との対応

第1部		第2部
本手引き管理項目	管理策	業務No.
1.セキュリティ境界と入退室管理	①	1,2,22,28,57
	②	1,2,22,28
	③	3
2.認証と権限	①	1,4,12,21,28,35,41,42,46
	②	4,21,42
	③	1,2,3,5,21,42
	④	1,2,21
	⑤	21
	⑥	6
3.ウイルス及び悪意のあるプログラムに対する対策	①	7
	②	7
	③	13,58
	④	13,58
	⑤	25
	⑥	25
	⑦	58
4.パッチの適用	①	8,60
	②	
5.バックアップ	①	9,23,50
	②	9,23,48,49,50
	③	23,50
6.ログの取得	①	3,55
	②	54
	③	55
	④	55
	⑤	
7.記憶媒体の管理	①	12,38,40
	②	32
	③	
	④	11
	⑤	
8.暗号化	①	14,16,20,35,38,39,40,44,46
	②	
	③	14,16,20
9.アプリケーションの利用	①	47
	②	47
	③	19
	④	37
	⑤	17
	⑥	17
	⑦	20
10.電子メールの利用	①	
	②	15
	③	14,16
	④	14
	⑤	

上付き(N)は参考資料の番号を示す

第1部		第2部
本手引き管理項目	管理策	業務No.
11.外部サービスの利用	①	24,26
	②	
12.ネットワークのアクセス制御	①	36,59,61
	②	59,61
	③	42,43
	④	59,61
	⑤	59,61
	⑥	31
	⑦	30,31,57
	⑧	25
13.クリアデスク・クリアスクリーン	①	45
	②	27,33,34,45
	③	29
	④	18
14.変更管理	①	48
	②	48
	③	48
	④	48
	⑤	49
	⑥	49
15.構成管理	①	10,51
	②	51
	③	
16.障害・事故管理	①	53
	②	52
	③	52
17.容量・能力の管理	①	56
	②	56
18.Webの開発・管理	①	62
	②	59
	③	59,61
	④	61
	⑤	61

上付き(N)は参考資料の番号を示す

0.2.凡例

(1) 管理目的
　管理策を行う目的
(2) 管理策
　中小企業が行うべき具体的な情報セキュリティ対策
　大きな投資及び技術的・運用的に難しいものは“(参考)”として記述している
(3) 運用で心がけるポイント
　セキュリティ対策を継続していくうえでの運用における注意点
(4) 関連する管理項目
　関連する管理項目を列挙

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情報と情報機器が設置されてい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、許可されてい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・機能を設置する
　③境界を越えて入ってくる、あるいは出ていく者の記録(誰が、いつ)を保存する
(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

2.認証と権限

(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

上付き(N)は参考資料の番号を示す

(2) 管理策

①入館・入室設備、PC(BIOS、OS)、サーバー、ネットワーク、アプリケーション、携帯電話等にアクセスするための個人及びプログラムを認証する仕組みを構築・設定する

②認証には、ID カード、デバイス(IC カード、USB キー等)、パスワード、バイオメトリックス(指紋認証、静脈認証等)等の、第三者が簡単に悪用できない仕組みを用いる

③認証のためのユーザ ID は個人を特定できるように付与する

④ユーザ ID は職務権限に応じた、情報と情報機器へのアクセス権限を付与する

⑤特権は、システム管理者、業務の管理者等特別の職務権限を持った者だけに付与する

⑥パスワード[9]は例えば「8 文字以上に設定し、
大文字、小文字、数字、特殊文字の 4 つを組み合わせ、
3 カ月に 1 度変更する」
(以降「」をパスワードポリシーとする)とする。

(3) 運用で心がけるポイント

①退職、人事異動に伴う、ユーザ ID、アクセス権限の見直しを行う

②特権は初期設定の Administrator は使用せず、システム管理者の個別ユーザ ID に特権を付与する

(4) 関連する管理項目

セキュリティ境界と入退室管理、アプリケーションの利用、電子メールの利用、ネットワークのアクセス制御、Web の開発・管理

3.ウイルス及び悪意のあるプログラムに対する対策

(1) 管理目的

情報の漏えい、改ざん、破壊及びソフトウェアの改ざん、破壊を防止するため

(2) 管理策

①ウイルス及び“悪意のあるプログラム”(悪意のあるプログラムをマルウエアと言い、ワーム、スパイウエア、トロイの木馬、ボット、アドウエア等を指す)を検知、除去するアンチウイルスソフトウェアを導入し、新しいエンジン・パターンファイルがリリースされるとすぐに更新する

②コンピューター(PC、サーバー)をアンチウイルスソフトウェアで定期的(1 週間に 1 度程度)にスキャンする

③USB メモリー、CD-ROM 等の記憶媒体及びネットワーク経由(Web、メール、FTP 等)で取得したファイルをアンチウイルスソフトウェアで使用前に、自動又は手動でスキャンする

④USB メモリー、CD-ROM 等の記憶媒体へのファイルの移動・コピー、メールへのファ

上付き[N]は参考資料の番号を示す

イル添付時に、ファイルをアンチウイルスソフトウェアで自動又は手動でスキャンする
⑤危険な Web サイトにはアクセスしない。アンチウイルスソフトウェアに危険な Web サイト警告機能がある場合は、機能を有効にし、警告ソフトの指示に従う
⑥アクセスする Web ページをスキャンする
⑦アンチウイルスソフトウェアの導入は、PC だけではなく、企業内のサーバー(メール、ファイル、Web、FTP、DNS、Proxy 等)及びゲートウエイ(インターネットから企業への入り口)への導入についても考慮する

(3) 運用で心がけるポイント
①コンピューター上でアンチウイルスソフトウェアのエンジン・パターンファイルが最新に更新状態であることを確認する
②定期的にアンチウイルスソフトウェアがコンピューターをスキャンしていることを確認する

(4) 関連する管理項目
記憶媒体の管理、アプリケーションの利用、障害・事故管理

4.パッチの適用

(1) 管理目的
公開されている技術的脆弱性の悪用によって生じる情報の漏えい、改ざん、破壊、及びシステム(ソフトウェア、ネットワーク機器)の破壊、停止を防止するため

(2) 管理策
①使用しているソフトウェア(OS、ミドルウエア、アプリケーション)、ネットワーク機器の脆弱性が発見された場合は、パッチを適用する
②パッチ適用による副作用がある場合に備え、切り戻すための手順を確立する

(3) 運用で心がけるポイント
①現状のソフトウェア、ハードウェアの構成及びパッチの適用状況を把握する

(4) 関連する管理項目
バックアップ、変更管理、構成管理

5.バックアップ

(1) 管理目的
情報及びシステム(ソフトウェア、サーバー、ネットワーク)を障害・事故から保護するため

上付き(N)は参考資料の番号を示す

(2) 管理策

①どの情報、どのシステム(ソフトウェア、サーバー、ネットワーク)構成をバックアップする必要があるのかを明確にする

②どの時点の情報あるいはシステム構成に戻る必要があるのか(RPO=Recovery Point Objective)、何時までに復旧する必要があるのか(RTO=Recovery Time Objective)により、バックアップの方法(フルバックアップ、差分バックアップ、頻度)及びメディアの種類(NAS、Tape、CD-R 等)を考慮する

③停止できないシステム(ソフトウェア、サーバー、ネットワーク)には冗長化(RAID、構成の 2 重化)、UPS の設置を考慮する

(3) 運用で心がけるポイント

①確実にバックアップによりリストア(データを元の状態に戻すこと)できることを確認する

②想定される障害・事故に対して、リカバリー(障害・事故から元の状態に戻すこと)計画を策定し、定期的にリカバリーテストの実施状況（テスト結果が RPO と RTO に整合していること）を確認する

(4) 関連する管理項目

変更管理、構成管理、障害・事故管理

6.ログの取得

(1) 管理目的

許可されていない情報処理活動の検知、システム異常の検知及び障害・事故を分析するため

(2) 管理策

①許可されていない情報処理活動(不正アクセス等)を検知するために、リソース(ファイル、ソフトウェア、ネットワーク機器等)へのアクセスの成功・失敗・警告・エラー、ユーザのログイン・ログアウトに関するログを取得し分析する

②システム(ハードウェア、ソフトウェア)の異常を検知するため、システムの警告・エラーログを取得し分析する

③イベントが発生した時刻を正確に把握するため、システム機器は標準時間に同期させる

④ログを必要な期間保存(6 カ月以上)するための十分なストレージ容量を確保すると共に、ログの改ざん・変更・削除から保護する

⑤許可されていない情報処理活動を検知するために、ユーザ PC の活動履歴を取得し分析する(参考)

(3) 運用で心がけるポイント

上付き(N)は参考資料の番号を示す

①必要なログがすべて取得され必要な期間保管されていることを確認する
②ログが定期的に分析、報告されていることを確認する

(4) 関連する管理項目

変更管理、構成管理、障害・事故管理

7.記憶媒体の管理

(1) 管理目的

情報の漏えい、改ざん、消去、破壊を防止するため

(2) 管理策

①記憶媒体の数量、所在を管理する
②使用した記憶媒体(ハードディスク、テープ、USB メモリー、CD、DVD、スマートカード等)を廃棄する場合は、保存した情報が解読できないように、信頼できる方法で、記憶媒体の物理的破壊[10]、情報の磁気的な消去または上書き消去[11]を行う
③重要な情報を保存した記憶媒体は、製造者の仕様に従って、適切な環境(磁気、湿度、温度などの制限)及びセキュリティの確保(耐火金庫、施錠管理)できる場所に保存する
④許可されていない記憶媒体の使用ができないように、PC、サーバーのデバイス制御を行う(参考)
⑤バックアップデータを記憶媒体に長期保管する場合は、記憶媒体の寿命を考慮し、定期的に、バックアップデータを新規記憶媒体に移動する等適切な処置を行う(参考)

(3) 運用で心がけるポイント

①定期的に記憶媒体の棚卸を実施し、数量、所在を確認する
②磁気的にデータ消去した場合は、廃棄前に情報が消去されていることを確認する

(4) 関連する管理項目

ウイルス及び悪意のあるプログラムに対する対策、バックアップ

8.暗号化

(1) 管理目的

暗号化により情報の漏えい、改ざんから情報を保護するため

(2) 管理策

①インターネット、無線 LAN、電子メール、記憶媒体の持ち出し(PC の持ち出しを含む)等、組織の物理的セキュリティ境界を越えて、情報を使用する場合は、暗号技術(ネッ

上付き[N]は参考資料の番号を示す

トワークの暗号化、情報の暗号化)の利用を検討する

②暗号アルゴリズムは信頼できるもの(12)を選択する

③暗号を使用して情報を授受する場合は、鍵の受け渡し方法を考慮する(例えば、電子メールに情報を暗号化して添付する場合は、鍵は、相手方に電話等電子メールとは別の方法で伝達しておく等)

(3) 運用で心がけるポイント

①無線 LAN の設定に適切な通信プロトコル(WPA2 など)が使用されて通信されていることを確認する

②持ち出す必要のある記憶媒体が暗号化されていることを確認する(暗号化の設定がされている等)

(4) 関連する管理項目

バックアップ、電子メールの利用

9.アプリケーションの利用

(1) 管理目的

アプリケーション・ソフトウェアの利用に伴う、情報の漏えい、改ざん、破壊から情報を保護するため

(2) 管理策

①有償、無償を問わず組織が許可したソフトウェアのみを使用する

②大きな脆弱性の存在が明らかなファイル共有ソフト、P2P(Winny、Share 等)の使用は禁止する

③電子ファイルを外部に提供する必要がある場合は、情報そのもの以外に、ファイルのプロパティ、ヘッダー、フッターにある情報も確認し外部に公開すべきでない情報は消去する

④プレゼンテーションソフトを使用し、外部に提案を行う場合は、PC のデスクトップ上にある外部に公開すべきでない情報は見えないようにする

⑤登録機能を使用して FAX 送信する場合は、登録間違いによる誤送信を防止するために宛先番号を確認して送信する

⑥FAX 送信する場合は、送信前に送信相手に、送信することの連絡、送信後に受信確認を行う

⑦重要な情報を保存する場合は、保存後に情報の重要度及び属性が容易に判断できるようにファイル名を命名する

(3) 運用で心がけるポイント

①無許可ソフトウェアがユーザ PC にインストールされていないか定期的に棚卸を実施

上付き(N)は参考資料の番号を示す

する

(4) 関連する管理項目

認証と権限、ウイルス及び悪意のあるプログラムに対する対策、暗号化

10.電子メールの利用

(1) 管理目的

電子メールに含まれた情報を、漏えい、改ざんから保護するため

(2) 管理策

①電子メールサービスの利用にあたってはユーザ認証を行う

②同時に複数の宛先にメールを送信する際､宛先のメールアドレスを受信者に公開したくない場合は BCC を利用する

③重要な情報は、本文に記載せず、添付ファイルとし、暗号技術を利用する

④誤送信を低減するため、誤送信防止ソフトウェアを導入する(参考)

⑤改ざんされた場合に問題が発生する情報には、電子署名の利用をする(参考)

(3) 運用で心がけるポイント

①電子メールの利用に何らかのユーザ認証が行われることを確認する

(4) 関連する管理項目

認証と権限、暗号化

11.外部サービスの利用

(1) 管理目的

外部サービスの利用に際し、組織の要求する情報セキュリティ及びサービスレベル[13]を確保し、維持するため

(2) 管理策

①外部サービスの利用に際し、セキュリティレベル(情報漏えい対策、ウイルス対策、障害・事故対策、災害対策等)、サービスレベル(対応時間、サービス可能時間、リソースの使用保証等)の確認を実施する

②サービス提供者とセキュリティレベル、サービスレベルを取りきめ契約を締結する(参考)

(3) 運用で心がけるポイント

①外部サービスに要求するセキュリティレベル、サービスレベルを確認する

上付き[N]は参考資料の番号を示す

(4) 関連する管理項目

無し

12.ネットワークのアクセス制御

(1) 管理目的

ネットワークを経由した情報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インターネット等の外部ネットワークと組織のネットワークの境界には、ファイアーウォール、ルータなどのアクセス制御装置を設置しアクセス制御を行う

②公開用の Web サーバー、メールリレーサーバー等は内部ネットワークとはファイアーウォールで隔てた別のネットワーク(DMZ)に設置する

③外部から組織のネットワークに接続する場合、許可された者のみに接続を許すために、適切な認証を行い、安全な接続(SSL-VPN、IPsec、PPTP 等)を行う

④外部ネットワークと内部ネットワーク、外部ネットワークと DMZ 間の通信プロトコル(=サービス：HTTP、HTTPS、FTP、SMTP、POP 等)は必要最低限のもののみ許可する

⑤公開サーバー、内部サーバー共に不要なサービスは停止する

⑥無線 LAN を使用する場合は、WPA2 等の安全な暗号化方式を用い、暗号鍵を設定する

⑦特定の場所または特定の PC、端末からの接続のみ許可するために PC、端末の識別子(IP アドレス、MAC アドレス等)での認証を行う(参考)

⑧危険な Web サイトにアクセスできないように Web フィルタリングを導入する(参考)

(3) 運用で心がけるポイント

①通信に不要なプロトコル、ポートが使用できないことを確認する

②外部からの接続をする場合、認証が有効であることを確認する

(4) 関連する管理項目

セキュリティ境界と入退室管理、認証と権限

13.クリアデスク・クリアスクリーン

(1) 管理目的

情報への許可されていないアクセスを防止するため

上付き(N)は参考資料の番号を示す

(2) 管理策

①重要な情報は、業務終了後施錠管理可能な場所に保管する

②PC 及び端末は、業務終了後はログアウトまたは電源を切り、離席時にはログアウト(ログオフ)またはパスワード付きのロック(パスワード付きスクリーンセーバーの設定)を行う

③会議室(特に外部の者と利用する会議室)は、利用終了後、重要な情報が放置されていないか、室内及びホワイトボード等の確認を行う

④プリンター、FAX 及びコピー機は重要な情報を印刷、FAX 授受及びコピー後、文書が機器に放置されていないか確認する

(3) 運用で心がけるポイント

①クリアデスク・クリアスクリーンポリシーが実行されているか業務終了後に確認する

(4) 関連する管理項目

セキュリティ境界と入退室管理、認証と権限

14.変更管理

(1) 管理目的

すべてのシステム(ハードウェア、OS、ミドルウエア、アプリケーション)に対する変更を一元的に管理して、障害・事故発生の可能性を最小限にすると共に、障害・事故発生時に障害・事故から速やかに回復するため

(2) 管理策

①変更が失敗した場合の切り戻し方法(バックアップからのリカバリー等)を検討する

②いつ、誰が、何を、どう変更したのかを記録する

③変更による影響範囲を洗い出す

④変更計画、変更手順を作成する

⑤検証またはテストを実施する(参考)

⑥検証またはテストに実データを使用する場合は、データの漏えい、破壊から保護する(参考)

(3) 運用で心がけるポイント

①変更に伴い変更記録が残されているか確認する

(4) 関連する管理項目

バックアップ、構成管理、障害・事故管理

上付き(N)は参考資料の番号を示す

15.構成管理

(1) 管理目的

すべてのシステム(ハードウェア、OS、ミドルウエア、アプリケーション)に対する構成情報を一元的に管理して、障害・事故の発生可能性を最小限にすると共に、障害・事故発生時に障害・事故から速やかに回復するため

(2) 管理策

①システムのソフトウェア(OS、ミドルウエア、アプリケーション)とハードウェアの構成要素を把握し、ラインセンス管理、バージョン管理、サポート情報の管理を行う

②各システム(業務システム、メールシステム、WEB システム、ネットワーク等)がどのようなハードウェア、OS、ミドルウエア、アプリケーションの組み合わせにより構成されているのか(構成情報)を管理する

③構成管理情報と変更管理情報、障害・事故管理情報を整合させる(参考)

(3) 運用で心がけるポイント

①システム構成図、ネットワーク構成図を確認する

②構成情報が現状のシステムを反映しているか確認する

(4) 関連する管理項目

バックアップ、変更管理、障害・事故管理

16.障害・事故管理

(1) 管理目的

システム障害(システム・サービスの停止、誤動作、破損等)、セキュリティ事故(情報漏えい、改ざん、アクセス違反、ウイルス感染、外部からの攻撃等)が発生した場合、根本原因を取り除き、再発防止を行うため

(2) 管理策

①システム障害、セキュリティ事故の発生に備え、連絡網を整備し、障害・事故発生時は連絡網に従い報告する

②障害・事故が発生した場合は、いつ、誰が、何を、どのようにして、障害・事故を発生させ、その結果どうなったのかを記録する

③記録から障害・事故発生の根本原因を追及し、それを取り除き、再発防止を行う

(3) 運用で心がけるポイント

①障害・事故発生時の連絡網が組織の実情を反映しているか確認する

②障害・事故発生時の記録が保存されているか確認する

上付き(N)は参考資料の番号を示す

(4) 関連する管理項目

ウイルス及び悪意のあるプログラムに対する対策、バックアップ、変更管理、構成管理、容量・能力の管理

17.容量・能力の管理

(1) 管理目的

システムの容量・能力(CPU、メモリー、記憶媒体、ディスク IO、ネットワーク帯域等)を業務の変化に合わせ最適化することにより、障害・事故発生の可能性を最小限にするため

(2) 管理策

①システム容量・能力を定期的に測定する

②業務が円滑に行われるためのシステム容量・能力の閾値(threshold)を設定し、業務変化に伴うシステム処理容量の増加により、この閾値を越える見込みがある場合は、事前に、システム容量・能力の増強を行う(参考)

(3) 運用で心がけるポイント

①システム容量・能力の測定結果を確認する

(4) 関連する管理項目

障害・事故管理

18.Web の開発・管理

(1) 管理目的

情報の漏えい、改ざん、破壊及びソフトウェアの改ざん、破壊を防止するため

(2) 管理策

①組織の知的財産は明示的に著作権の表示を行うか、容易に複製できないように技術的に保護する

②Web に公開する情報は改ざんから保護するため、必要なアクセス制御(ルータ、ファイアーウォール、OS、Web サーバー、アプリケーション等での制御)を行う

③顧客の個人情報等、第三者の情報を保存する場合は、「安全な Web アプリケーション構築の手引き」[14][15]に従い、Web システムを開発・構築する(参考)

④組織の外部から、公開している Web サイトに悪意のある攻撃が無いか、WAF、IPS、IDS、外部の監視サービス等を用い監視を行う(参考)

上付き[N]は参考資料の番号を示す

⑤定期的に Web サイトの強度、運用、管理方法に関して、第三者機関の検査または監査を実施する(参考)

(3) 運用で心がけるポイント

①公開されている Web サイトが改ざんされていないか定期的に確認する

②改ざん、漏えい事故が発生した場合の、対処方法(リカバリー方法、届け出等)を確認する

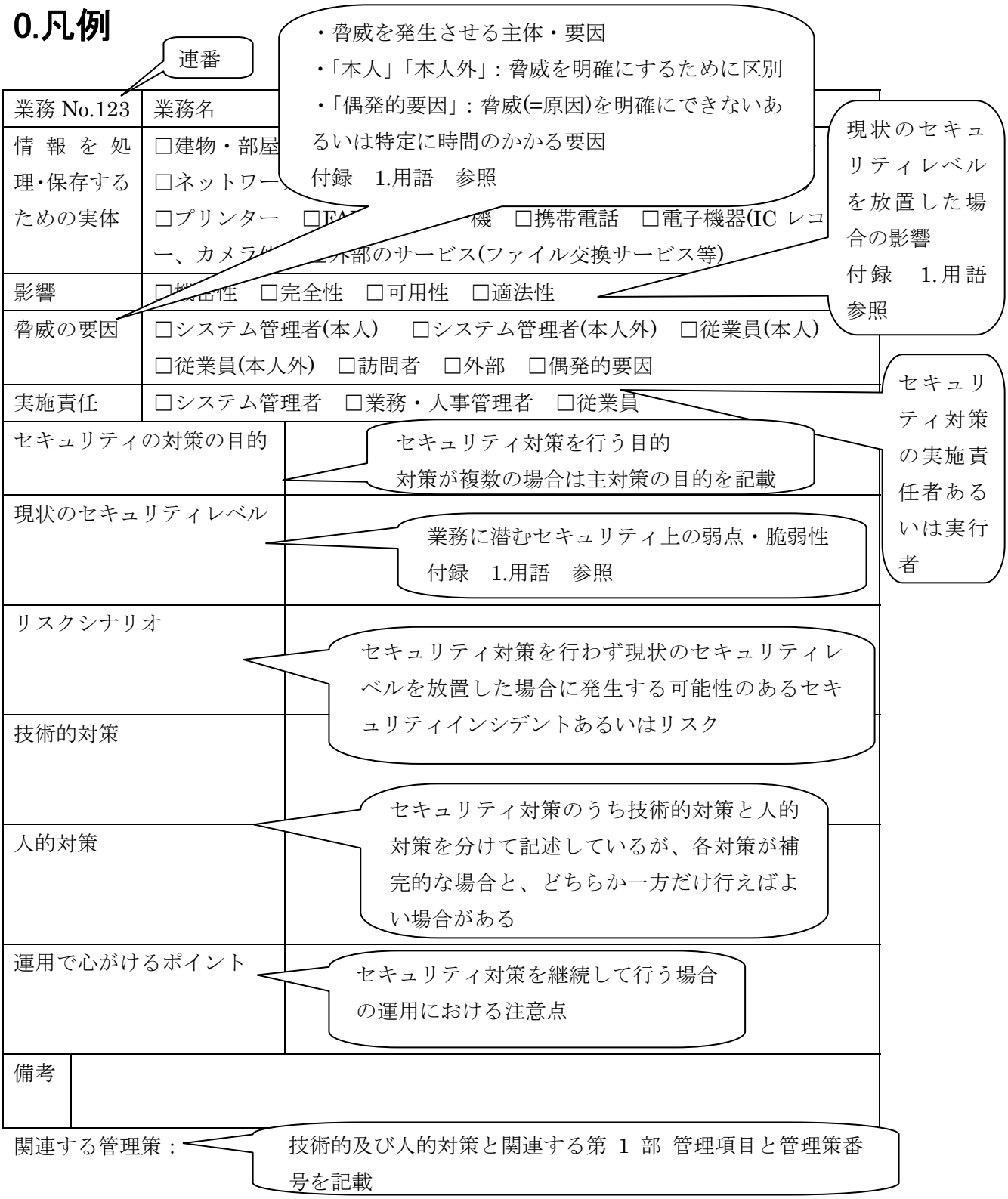
(4) 関連する管理項目

認証と権限、バックアップ、ネットワークのアクセス制御、変更管理、構成管理、障害・事故管理

上付き(N)は参考資料の番号を示す

第 2 部　業務に基づく情報セキュリティ対策

0.凡例



業務 No.123	業務名
情報を処理･保存するための実体	□建物・部屋 □ネットワー □プリンター　□FA　機　□携帯電話　□電子機器(IC レコーダー、カメラ 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
脅威の要因	□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
実施責任	□システム管理者　□業務・人事管理者　□従業員
セキュリティの対策の目的	
現状のセキュリティレベル	
リスクシナリオ	
技術的対策	
人的対策	
運用で心がけるポイント	
備考	

関連する管理策：

上付き(N)は参考資料の番号を示す

1.出社

業務 No.1	入館
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
脅威の要因	□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
実施責任	□システム管理者　■業務・人事管理者　□従業員

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	従業員かどうかを識別、認証する仕組みが無い
リスクシナリオ	従業員以外が従業員になりすまし入館する
技術的対策	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
人的対策	従業員に個人を特定できる社員証を与え、人(守衛)がチェックする
運用で心がけるポイント	退職、人事異動した従業員の社員証の棚卸を定期的に行う

備考	従業員には、正社員の他、契約社員、派遣社員、パート・アルバイトなど非正規の社員も含んでいる

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 ①,③,④

上付き(N)は参考資料の番号を示す

2.社内業務

業務 No.2	セキュリティエリアへのアクセス 1 【エリア分け】
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
脅威の要因	□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
実施責任	□システム管理者 ■業務・人事管理者 □従業員

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

上付き(N)は参考資料の番号を示す

業務 No.3	セキュリティエリアへのアクセス 2 【入退室記録】
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
脅威の要因	□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
実施責任	□システム管理者 ■業務・人事管理者 □従業員

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	エリアアクセス(入退室)の記録を取っていない
リスクシナリオ	重要な情報を扱うエリア(室)への入退室記録が無く、情報漏えい発生時、誰がいつエリア(室)に入退したのかわからない
技術的対策	エリア管理(入退室管理)システムでアクセス記録(ログ)を取る
人的対策	エリア(室)への入退管理台帳を備え、誰が・いつ・何の目的でアクセスしたのか記録する
運用で心がけるポイント	定期的にアクセス記録を確認する
備考	

関連する管理策：1.セキュリティ境界と入退室管理 ③ 2.認証と権限 ③ 6.ログの取得 ①

上付き(N)は参考資料の番号を示す

業務 No.4	PC の起動・ログイン１ 【自動ログインの設定】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員

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	PC に自動ログインの設定を行っている
リスクシナリオ	PC に物理的にアクセスできる人は誰でも PC を使用でき、PC から利用できる情報を漏えいする
技術的対策	PC の自動ログインの設定を解除し、個人認証しなければログインできないようにする
人的対策	
運用で心がけるポイント	PC を起動し、PC の使用に認証が必要なことを確認する

備考	

関連する管理策：2.認証と権限 ①,②

上付き(N)は参考資料の番号を示す

業務 No.5	PC の起動・ログイン 2 【共通ＩＤの使用】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員

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	共通 ID を使用して PC を使用している
リスクシナリオ	共通 ID を使用しているため、個人を特定するログを残せず、情報漏えい等セキュリティ事故発生時に犯人を特定できない
技術的対策	個人を特定できる個別のユーザ ID を作成して使用する
人的対策	
運用で心がけるポイント	ID の棚卸を実施し、PC または認証システムの ID がユーザ個別に設定されているか確認する
備考	

関連する管理策：2.認証と権限 ③

上付き(N)は参考資料の番号を示す

業務 No.6	PC の起動・ログイン 3 【パスワードポリシーの使用】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員

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	簡単なパスワード(数字 4 桁など)を使用している
リスクシナリオ	簡単なパスワードを使用しているためログオン時の覗き見によりパスワードが漏えいし、情報にアクセスされる
技術的対策	認証システムのパスワードポリシーを設定(複雑なパスワード、定期的パスワードの変更)し、ユーザに強制的にパスワードポリシーを使用させる
人的対策	パスワードの文字数、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
運用で心がけるポイント	・認証システムのパスワードポリシーを確認する ・パスワードルールが周知徹底されているかユーザに確認する
備考	

関連する管理策：2.認証と権限 ⑥

上付き(N)は参考資料の番号を示す

業務 No.7	PC を使用した業務 1 【アンチウイルスソフト導入と使用ルール】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員
セキュリティの対策の目的	情報の漏えい、改ざん、破壊及びソフトウェアの改ざん、破壊を防止するため
現状のセキュリティレベル	アンチウイルスソフトウェアを導入していない、あるいは導入していてもエンジン・パターンファイルを更新していない
リスクシナリオ	・アンチウイルスソフトウェア未導入によりウイルスに感染する ・エンジン・パターンファイルを更新していないためウイルスに感染しても検知できない
技術的対策	各 PC にアンチウイルスソフトウェアを導入し、アンチウイルス統合管理システムで各 PC を管理する
人的対策	各 PC にアンチウイルスソフトウェアを導入し、正しいアンチウイルスソフトウェアの使用ルールを定める(エンジン・パターンファイルの更新、定期的なウイルススキャン等)
運用で心がけるポイント	・各 PC にアンチウイルソフトウェアが導入され、プロセスが起動していることを確認する ・各 PC のエンジン・パターンファイルが更新されていることを確認する ・定期的に各 PC がウイルススキャンされていることを確認する
備考	

関連する管理策：3.ウイルス及び悪意のあるプログラムに対する対策 ①,②

上付き(N)は参考資料の番号を示す

業務 No.8	PC を使用した業務 2 【セキュリティパッチの適用】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員
セキュリティの対策の目的	公開されている技術的脆弱性の悪用によって生じる情報の漏えい、改ざん、破壊、システムの破壊、停止を防止するため
現状のセキュリティレベル	OS､アプリケーションにセキュリティパッチを適用していない
リスクシナリオ	OS, アプリケーションのセキュリティパッチ未適用により、脆弱性を狙った攻撃にさらされ、コンピューターを乗っ取られ、その結果、情報が漏えいする
技術的対策	各 PC の OS､アプリケーションのセキュリティパッチ適用を自動的に行うように設定する
人的対策	OS､アプリケーションの新しいセキュリティパッチがリリースされるごとに、各 PC のセキュリティパッチを適用する
運用で心がけるポイント	各 PC に最新のセキュリティパッチが適用されていることを確認する
備考	

関連する管理策：4.パッチの適用 ①

上付き(N)は参考資料の番号を示す

業務 No.9	PC を使用した業務 3 【重要な情報の管理】
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
脅威の要因	□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
実施責任	□システム管理者 □業務・人事管理者 ■従業員

セキュリティの対策の目的	情報及びシステムを障害・事故から保護するため
現状のセキュリティレベル	重要な情報を PC にのみ保存している
リスクシナリオ	PC のハードディスク障害によりディスクに保存していた重要な情報を損失する
技術的対策	ネットワークファイル(ファイルサーバー上のファイル)とオフラインファイルを同期するように設定する
人的対策	定期的に PC から重要なファイルをファイルサーバーに保存する
運用で心がけるポイント	PC のディスクとファイルサーバーを定期的に確認する(ファイルがコピーまたは移動されていることを確認する)
備考	

関連する管理策：5.バックアップ ①,②

上付き(N)は参考資料の番号を示す

業務 No.10	PC を使用した業務 4 【ライセンス管理】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	すべてのシステムに対する構成情報を一元的に管理して、障害・事故の発生可能性を最小限にすると共に、障害・事故発生時、障害・事故から速やかに回復するため
現状のセキュリティレベル	ソフトウェアのライセンス管理ができていないため、必要なソフトウェアライセンス本数を購入できていない
リスクシナリオ	・アプリケーションを使用する必要があるユーザが、ライセンス不足のため、アプリケーションを使用できない ・ライセンス違反でソフトウェアベンダーから損害賠償を求められる
技術的対策	資産管理システムを導入し、ソフトウェアライセンスの管理を行う
人的対策	PC にソフトウェアをインストールする場合、使用できるソフトウェアライセンスを確認して実施する
運用で心がけるポイント	定期的に PC にインストールされているソフトウェアの棚卸を実施する

備考	経営者、システム管理者が故意にライセンス違反をすることは想定していない

関連する管理策：15.構成管理 ①

上付き(N)は参考資料の番号を示す

業務 No.11	PC を使用した業務 5 【個人所有の記憶媒体の使用】
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
脅威の要因	□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
実施責任	■システム管理者 ■業務・人事管理者 ■従業員

セキュリティの対策の目的	情報の漏えいを防止するため
現状のセキュリティレベル	業務に無制限に個人所有の記憶媒体(USB メモリー等)の使用を容認している
リスクシナリオ	セキュリティ対策ができていない個人所有の記憶媒体を使用し、盗難・紛失により情報が漏えいする
技術的対策	デバイス制御システムを導入し、許可した記憶媒体のみ使用できるようにする
人的対策	業務で個人所有の記憶媒体を使用できる条件をルール化する、あるいは個人所有の記憶媒体の使用を禁止する
運用で心がけるポイント	・不正に記憶媒体を使用していないか、デバイス制御システムのログを定期的に確認する ・ユーザがルールを知っているか確認する
備考	

関連する管理策：7.記憶媒体の管理 ④

上付き(N)は参考資料の番号を示す

業務 No.12	PC を使用した業務 6 【記憶媒体の使用】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員

セキュリティの対策の目的	情報の漏えいを防止するため
現状のセキュリティレベル	USB メモリーなど記憶媒体のセキュリティ基準､利用基準を定めておらず、無制限に USB メモリー他記憶媒体を使用している
リスクシナリオ	USB メモリー他記憶媒体を使用して事務所内に置き忘れ､いつのまにか紛失し、そこから情報漏洩する
技術的対策	暗号化機能、PIN や指紋認証付の付いた USB メモリー等の記憶媒体を使用する
人的対策	キーチェーンに接続して使用する等、紛失しないような工夫をする
運用で心がけるポイント	定期的に記憶媒体の所在確認を行う
備考	

関連する管理策：2.認証と権限 ① 7.記憶媒体の管理 ①

上付き(N)は参考資料の番号を示す

業務 No.13	メールの受信確認
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
脅威の要因	□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
実施責任	■システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	情報の漏えい、改ざん、破壊及びソフトウェアの改ざん、破壊を防止するため
現状のセキュリティレベル	メールのウイルス対策をしていない
リスクシナリオ	ウイルス付のメールを受け取り、メールを開いて感染してしまう
技術的対策	アンチウイルスソフトウェアのメールチェック機能を有効にする
人的対策	不審なメール、スパムメール、送り先及び件名に心当たりのないメールは開かずに削除する
運用で心がけるポイント	アンチウイルスソフトウェアのメールチェック機能が有効かどうか確認する
備考	

関連する管理策：3.ウイルス及び悪意のあるプログラムに対する対策 ③,④

上付き(N)は参考資料の番号を示す

業務 No.14	メールの送信 1【宛先確認】
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
脅威の要因	□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
実施責任	□システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	電子メールに含まれた情報を、漏えいから保護するため
現状のセキュリティレベル	宛先を確認せずにメールを送信している
リスクシナリオ	宛先間違いによる誤送信で情報が漏洩する
技術的対策	誤送信防止ツールを導入する
人的対策	・重要な情報を送付する場合はパスワード付きの暗号化ファイルにし、添付する。送信後、電話で送信相手にパスワードを連絡する ・一度送信相手に送信したメールを利用して再送信する
運用で心がけるポイント	重要な情報は暗号化ファイルとして添付、パスワードが記載されていないか、送信済みトレイを確認する
備考	

関連する管理策：8.暗号化 ①,③ 10.電子メールの利用 ③,④

上付き(N)は参考資料の番号を示す

業務 No.15	メールの送信 2 【宛先指定】
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
脅威の要因	□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
実施責任	■システム管理者 ■業務・人事管理者 ■従業員

セキュリティの対策の目的	電子メールに含まれた情報を、漏えいから保護するため
現状のセキュリティレベル	TO、CC、BCC の違いを理解せずにメールを使用している
リスクシナリオ	複数人に同時に電子メールを配信(同報)する際、TO、CC、BCC の使用を誤り、第三者に他人のメールアドレスを漏洩してしまう
技術的対策	メーリングリスト用のソフトウェアを利用する
人的対策	ユーザに基本的なメールの使用方法を知っているか確認し、知っている者のみにメールアカウントを付与する
運用で心がけるポイント	定期的な TO、CC、BCC の宛先の使用方法の確認テストを実施する

備考	

関連する管理策：10.電子メールの利用 ②

上付き(N)は参考資料の番号を示す

業務 No.16	メールの送信 3 【添付フアイル】
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
脅威の要因	□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
実施責任	□システム管理者 □業務・人事管理者 ■従業員

セキュリティの対策の目的	電子メールに含まれた情報を、漏えいから保護するため
現状のセキュリティレベル	重要情報を添付する場合、暗号化を行わず、そのまま添付している
リスクシナリオ	電子メールの送信者から受信者への経路上でメール情報が盗まれ、重要情報が漏えいする
技術的対策	重要情報を添付する場合はファイルを暗号化し、パスワードは電話等別の手段で伝達する
人的対策	
運用で心がけるポイント	メールのログまたは送信済みメールの記録を確認し、ファイルが暗号化され、パスワードがメール本文に書かれていないことを確認する
備考	

検索：8.暗号化 ①,③ 10.電子メールの利用 ③

上付き(N)は参考資料の番号を示す

業務 No.17	FAX 送信
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
脅威の要因	□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
実施責任	□システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	アプリケーション・ソフトウェアの利用に伴う、情報の漏えいから情報を保護するため
現状のセキュリティレベル	FAX で重要情報を送信する場合、宛先を確認せずに送信している
リスクシナリオ	FAX 番号を誤り、送信間違いをし、重要情報が漏洩する
技術的対策	番号の登録機能を利用する
人的対策	一度 FAX で空情報をテスト送信し、送信先に届いたことを確認後、リダイアル機能を利用し重要情報を送信する
運用で心がけるポイント	番号登録機能を利用する場合においても、故意または過失で番号が変更されていることがあるので、定期的に登録番号を確認すると共に送信時には宛先番号を確認する
備考	

関連する管理策：9.アプリケーションの利用 ⑤,⑥

上付き(N)は参考資料の番号を示す

業務 No.18	コピー機の利用
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
脅威の要因	□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
実施責任	□システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	情報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	重要情報をコピーする際、コピー機から離れている
リスクシナリオ	コピーされた重要情報をコピー機に放置し、アクセス権を持たない者に情報を持ち去られる
技術的対策	
人的対策	重要情報をコピーする際はコピー機から離れず、コピー後は情報をすぐに持ち帰る
運用で心がけるポイント	重要情報が残されていないかコピー機を定期的に確認する
備考	

関連する管理策：13.クリアデスク・クリアスクリーン ④

上付き(N)は参考資料の番号を示す

業務 No.19	PC による文書の作成 1 【文書の再利用】
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
脅威の要因	□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
実施責任	□システム管理者 □業務・人事管理者 ■従業員

セキュリティの対策の目的	アプリケーション・ソフトウェアの利用に伴う、情報の漏えいから情報を保護するため
現状のセキュリティレベル	文書を再利用する場合のリスクが明確になっていない
リスクシナリオ	他社向けに作成した資料を再利用し、他社名がヘッダーに残ったまま別の顧客に提出してしまう
技術的対策	アプリケーションにある“ドキュメント検査”機能を利用し文書をレビューする
人的対策	・文書の雛型を作成し、それを利用する ・文書再利用のルールの策定及びチェック項目を作成する
運用で心がけるポイント	外部に提出する際は、別の人間が文書のレビューをする
備考	“ドキュメント検査”機能の有無はアプリケーションに依存する

関連する管理策：9.アプリケーションの利用 ③

上付き(N)は参考資料の番号を示す

業務 No.20	PC による文書の作成 2 【他社情報の管理)
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
脅威の要因	□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
実施責任	□システム管理者 ■業務・人事管理者 ■従業員

セキュリティの対策の目的	アプリケーション・ソフトウェアの利用に伴う、情報の漏えいから情報を保護するため
現状のセキュリティレベル	他社に関する重要情報(電子ファイル)も含めた情報の命名規則がない
リスクシナリオ	他社に関する重要情報が自社の情報と混在してしまい、他社情報へのアクセス権限を持たない者にまで、情報が流出してしまう
技術的対策	・企業(他社)ごとにフォルダーを作成し、アクセス権を定め、その企業に関連する情報はそのフォルダーに保存する ・他社に関する重要情報は暗号化して保存する。パスワード(鍵)はアクセス権限を持つ者のみで共有する
人的対策	ファイルの命名規則を策定し、情報を保存する時に、他社重要情報と自社情報の違いが分かるようにする
運用で心がけるポイント	命名規則どおり他社から委託された情報が保存されているか確認する
備考	

関連する管理策：8.暗号化 ①,③ 9.アプリケーションの利用 ⑦

上付き(N)は参考資料の番号を示す

業務 No.21	共有サーバーの利用 1 【ネットワーク経由によるアクセス】
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
脅威の要因	□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
実施責任	■システム管理者 ■業務・人事管理者 □従業員

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	共有サーバーのアクセス制御をしていない(ネットワークに接続できる者は誰でも共有サーバーにアクセスができる)
リスクシナリオ	職務上情報へのアクセス権限を持たない者がネットワーク経由で共有サーバーにアクセスし、情報を閲覧する
技術的対策	共有サーバーに職務に応じたアクセス制御を設定し、ID とパスワード等で認証を行う
人的対策	
運用で心がけるポイント	定期的に職務に応じたアクセス権限の棚卸を実施する
備考	

関連する管理策：2.認証と権限 ①,②,③,④,⑤

上付き(N)は参考資料の番号を示す

業務 No.22	共有サーバーの利用 2 【物理的アクセス】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

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	共有サーバーが事務所内に設置されており、誰でも物理的にアクセスができる
リスクシナリオ	共有サーバーにアクセス権限を持たない者が直接サーバーにログインし、情報を閲覧する
技術的対策	共有サーバーを施錠可能なラックに設置するか、セキュリティエリア内に移設する
人的対策	
運用で心がけるポイント	ラックの施錠状況を確認する

備考	サーバーに物理的にアクセスできる場合、ネットワーク経由でサーバーにアクセスするより簡単にサーバーにログインできる可能性が高い

関連する管理策：1.セキュリティ境界と入室管理 ①,②

上付き(N)は参考資料の番号を示す

業務 No.23	共有サーバーの利用 3 【バックアップ】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	情報及びシステムを障害・事故から保護するため
現状のセキュリティレベル	共有サーバーのバックアップを行っていない
リスクシナリオ	共有サーバーのハードディスク障害によりデータが損失する
技術的対策	・RAID 構成など情報保存領域の冗長化を行う ・RPO、RTO に応じてバックアップ計画を作成し、それに従ってバックアップを行う
人的対策	
運用で心がけるポイント	・冗長化構成の構成メンバーに障害が発生していないか定期的に確認する ・情報が確実にバックアップメディアに収納されているか確認する
備考	

関連する管理策：5.バックアップ ①,②,③

上付き(N)は参考資料の番号を示す

業務 No.24	外部サービスを利用したファイル交換
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
脅威の要因	□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
実施責任	■システム管理者　■業務・人事管理者　□従業員

セキュリティの対策の目的	外部サービスの利用に際し、組織の要求する情報セキュリティ及びサービスレベルを確保し、維持するため
現状のセキュリティレベル	外部サービスのセキュリティ強度を確認せずに利用している
リスクシナリオ	セキュリティレベルの低いサービス業者を利用し、情報を漏えいする
技術的対策	
人的対策	外部サービスのセキュリティ強度を明確にし、強度不足の場合は、社内で暗号化等セキュリティ強度を補完してサービスを利用する
運用で心がけるポイント	社内のセキュリティ基準(ウイルス対策、暗号化通信等)と利用するサービスのセキュリティ強度を比較する
備考	

関連する管理策：11.外部サービスの利用 ①

上付き(N)は参考資料の番号を示す

業務 No.25	WEB サイトへのアクセス 1 【閲覧】
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
脅威の要因	□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
実施責任	■システム管理者 ■業務・人事管理者 ■従業員
セキュリティの対策の目的	ネットワークを経由した情報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	業務に関係しない WEB サイトの閲覧を禁止していない
リスクシナリオ	業務上必要のない WEB サイトを閲覧し、ウイルス感染、詐欺被害、情報漏えい被害に遭うリスクが大きくなる
技術的対策	・WEB フィルタリングを導入し、危険なサイトへのアクセスを禁止する ・WEB サイトが安全かどうか判断するツール(アンチウイルスソフトウェアの機能の一部として提供されていることが多い)を利用し、危険なサイトにはアクセスしない
人的対策	アクセスしてはいけない WEB サイトのリストを作成しルールでアクセスを禁止する
運用で心がけるポイント	・WEB のアクセスログを確認し、ユーザが危険なサイトにアクセスしていないことを確認する ・WEB サイトを利用した悪意のある攻撃等に関する情報を収集し、ユーザに危険を周知する
備考	

関連する管理策：3.ウイルス及び悪意のあるプログラムに対する対策 ⑤,⑥

12.ネットワークのアクセス制御 ⑧

上付き(N)は参考資料の番号を示す

業務 No.26	WEB サイトへのアクセス 2 【サービスレベルの確認】
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
脅威の要因	□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
実施責任	■システム管理者 ■業務・人事管理者 □従業員

セキュリティの対策の目的	外部サービスの利用に際し、組織の要求する情報セキュリティ及びサービスレベルを確保し、維持するため
現状のセキュリティレベル	サービスレベルを確認せずに、外部の提供する WEB メールサービスを利用している
リスクシナリオ	想定したサービスレベルに達していない外部の提供する WEB メールサービスを利用し、データの損失、長時間のサービス停止の障害に遭遇する
技術的対策	
人的対策	社内の要求するサービスレベル(停止時間、障害対策等)を十分満たす WEB メールサービスを利用する
運用で心がけるポイント	社内の要求するサービスレベルと WEB メールサービスのサービスレベルを比較する
備考	

関連する管理策：11.外部サービスの利用 ①

上付き(N)は参考資料の番号を示す

業務 No.27	離席
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
脅威の要因	□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
実施責任	■システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	情報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	PC にログインしたまま(他者が利用できる状態)離席をしている
リスクシナリオ	他の従業員に無断で PC を使用され､PC からアクセスできる情報を閲覧される
技術的対策	パスワード付きのスクリーンセーバーの設定を PC に行う
人的対策	離籍時はログアウト(ログオフ)を行う
運用で心がけるポイント	パスワード付きのスクリーンセーバーの設定は 15 分以内に設定するようにする
備考	

関連する管理策：13.クリアデスク・クリアスクリーン ②

上付き(N)は参考資料の番号を示す

業務 No.28	訪問者との打ち合わせ 1 【訪問者の識別】
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
脅威の要因	□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
実施責任	□システム管理者 ■業務・人事管理者 ■従業員

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	訪問者と従業員が識別できていない
リスクシナリオ	訪問者が重要な情報を閲覧する
技術的対策	訪問者(部外者)が重要情報にアクセスできないように入退室・エリア管理を行う
人的対策	訪問者を特定できるビジターカード等を配布し、従業員と識別し、重要情報にアクセスできる場所には従業員が付き添う
運用で心がけるポイント	定期的にビジターカードの棚卸を実施する
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 ①

上付き(N)は参考資料の番号を示す

業務 No.29	訪問者との打ち合わせ 2 【会議室の使用】
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
脅威の要因	□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
実施責任	□システム管理者 ■業務・人事管理者 ■従業員

セキュリティの対策の目的	情報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	会議室の使用ルールが決まっていない
リスクシナリオ	・ホワイトボードの消し忘れにより、重要な情報を訪問者が閲覧する ・会議室に置き忘れた書類を訪問者が社外に持ち出す
技術的対策	
人的対策	チェックシートを作成し、会議室の使用後、置き忘れがないか、ホワイトボードの消し忘れがないか等、確認する
運用で心がけるポイント	実際にチェックシートが利用され必要な項目がチェックされているか確認する

備考	

関連する管理策：13.クリアデスク・クリアスクリーン ③

上付き(N)は参考資料の番号を示す

業務 No.30	訪問者との打ち合わせ 3 【訪問者によるネットワークへの接続】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	ネットワークを経由した情報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	(訪問者を含め)ネットワーク(有線)へのアクセスが制限されていない
リスクシナリオ	訪問者が会議室にあるネットワークに接続し、社内サーバーにアクセスする
技術的対策	・端末認証(MAC 認証等)を行い許可された PC のみネットワークへの接続を許可する ・ネットワークのポートに鍵付きプロテクターを付け、無許可の PC が接続できないようにする
人的対策	訪問者がある場合は会議室のネットワークを一時使用不能にしておく
運用で心がけるポイント	訪問者がアクセス可能な場所にあるネットワークが無許可使用できないことを確認する
備考	

関連する管理策：12.ネットワークのアクセス制御 ⑦

上付き(N)は参考資料の番号を示す

業務 No.31	訪問者との打ち合わせ 4 【訪問者による無線ネットワークへの接続】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	ネットワークを経由した情報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	(訪問者を含め)ネットワーク(無線)へのアクセスが制限されていない
リスクシナリオ	訪問者が無線ネットワークに接続し、社内サーバーにアクセスする
技術的対策	・端末認証(MAC 認証等)を行い許可された PC のみネットワークへの接続を許可する ・堅牢な暗号化技術(WPA2 等)を使用し定期的に暗号化鍵を変更する
人的対策	訪問者がある場合は会議室のネットワークを一時使用不能にしておく
運用で心がけるポイント	無線アクセスポイントに接続する際、暗号化鍵の入力を求められることを確認する
備考	社内、社外を問わず無線のアクセスポイントへのアクセスは電波が届く範囲で可能である

関連する管理策：12.ネットワークのアクセス制御 ⑥,⑦

上付き(N)は参考資料の番号を示す

業務 No.32	PC・記憶媒体の廃棄・処分
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
脅威の要因	□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
実施責任	■システム管理者　■業務・人事管理者　■従業員

セキュリティの対策の目的	情報の漏えいを防止するため
現状のセキュリティレベル	PC、記憶媒体の廃棄手順を定めていない
リスクシナリオ	PC、記憶媒体の情報が不完全な消去状態(OS でデータを削除しただけ)で廃棄されたため、情報が復元され漏えいする
技術的対策	・読み取りができないように物理的破壊を行う ・データ消去ツールを使い、データを上書きする
人的対策	廃棄業者に廃棄処分を依頼し、廃棄した旨を証明するマニフェストを取得する
運用で心がけるポイント	データをツール等で消去した場合は、作業が確実に終了したことを確認する(PC が起動できない等)

備考	PC のデータは OS の機能を使用し削除しただけでは、ツールを使用し容易にデータの復元が可能である

関連する管理策：7.記憶媒体の管理 ②

上付き(N)は参考資料の番号を示す

3.社外業務

業務 No.33	公共の乗り物での業務
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
脅威の要因	□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
実施責任	□システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	許可されていない情報へのアクセスを防止するため
現状のセキュリティレベル	情報の内容を意識せず、PC を公共の乗り物で使用している
リスクシナリオ	近隣の乗客が重要な情報を盗み見する
技術的対策	覗き見防止フィルタ(液晶フィルム)を使用する
人的対策	重要なファイルは公共の場所では使用しない
運用で心がけるポイント	覗き見防止フィルタ(液晶フィルム)を使用しても見える角度を認識しておく
備考	

関連する管理策：13.クリアデスク・クリアスクリーン ②

上付き(N)は参考資料の番号を示す

業務 No.34	取引先への訪問
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
脅威の要因	□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
実施責任	□システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	情報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	取引先訪問時における PC の取り扱いを決めていない
リスクシナリオ	離席した際に、取引先に取引とは関係ない重要な情報を閲覧(PC を操作)される
技術的対策	パスワード付きのスクリーンセーバーの設定を行う
人的対策	離席する際は、PC をログアウト(ログオフ)する
運用で心がけるポイント	外部で PC を使用する場合はパスワード付きのスクリーンセーバーの設定をしていても、離席の際は、PC からログアウトするか電源を切る
備考	

関連する管理策：13.クリアデスク・クリアスクリーン ②

上付き(N)は参考資料の番号を示す

業務 No.35	PC を持って出張に行く 1 【モバイルパソコンの管理】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員

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	持ち出し PC の取り扱いを決めていない
リスクシナリオ	公共の交通機関利用時に荷物棚や駅などに PC が入った鞄を置き忘れ、紛失する、あるいは置き引きに遭う
技術的対策	BIOS のパスワード設定及び PC ログインのための ID、パスワードを設定し、またハードディスクは暗号化をしておく
人的対策	常に PC は携帯し、電車の棚や座席の下など目の届かない場所へ放置しない
運用で心がけるポイント	BIOS のパスワード設定、PC ログインのための ID、パスワードの設定、ハードディスクは暗号化設定を確認する
備考	

関連する管理策：2.認証と権限 ① 8.暗号化 ①

上付き(N)は参考資料の番号を示す

業務 No.36	PC を持って出張に行く 2 【公共のネットワーク利用】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員

セキュリティの対策の目的	ネットワークを経由した情報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	社外で PC を使用する場合でも社内と同じセキュリティレベルで使用している(社外の方がセキュリティレベルを厳しくすべき)
リスクシナリオ	・ホテル等の公共のネットワークに接続した際、同じホテルの利用者から PC に対して不正なアクセスが行われ､PC 内の情報を盗まれる ・公共のネットワーク利用時に通信の内容を盗聴され、送受信した情報を盗まれる
技術的対策	・通信キャリアが提供する 3G サービスなどを利用する ・パーソナルファイアーウォールを設定(外部で利用する必要最低限のプロトコル、サービスのみに通信を許可)する
人的対策	信頼できないネットワークへは接続しない
運用で心がけるポイント	パーソナルファイアーウォールの設定内容を確認し、外部で利用する必要最低限のプロトコル、サービスのみに通信が許可されていることを確認する
備考	

関連する管理策：12.ネットワークのアクセス制御 ①

上付き(N)は参考資料の番号を示す

業務 No.37	取引先でのプレゼンテーション
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
脅威の要因	□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
実施責任	□システム管理者　□業務・人事管理者　■従業員
セキュリティの対策の目的	アプリケーション・ソフトウェアの利用に伴う、情報の漏えいから情報を保護するため
現状のセキュリティレベル	日常業務で使用している PC をそのまま(デスクトップ上のショートカット名等意識すること無しに)プレゼンテーションに使用している
リスクシナリオ	・デスクトップ上においたショートカット名から重要な情報(取引先名等)が漏えいする ・誤ったオペレーションにより、デスクトップ上の重要情報を開き、情報が漏洩する。
技術的対策	プレゼンテーション時はデスクトップアイコンの表示を非表示モードにしておく
人的対策	PC のデスクトップ上から重要情報の削除、不要なデータの削除等のプレゼンテーション用の環境を準備しておく
運用で心がけるポイント	・プレゼンテーション用の環境に容易に切り替えられるか確認する ・プレゼンテーションをする環境が適切か確認する
備考	

関連する管理策：9.アプリケーションの利用 ④

上付き(N)は参考資料の番号を示す

業務 No.38	記憶媒体を持って出張に行く 1 【記憶媒体の管理】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員

セキュリティの対策の目的	情報の漏えいを防止するため
現状のセキュリティレベル	社外での記憶媒体の取り扱い方法を明確にしていない
リスクシナリオ	公共の交通機関利用時に荷物棚や駅などに記憶媒体が入った鞄を置き忘れ、紛失する、あるいは置き引きに遭う
技術的対策	情報は暗号化して記憶媒体に保存する
人的対策	常に記憶媒体は携帯し、電車の棚や座席の下など目の届かない場所へ放置しない
運用で心がけるポイント	・定期的に記憶媒体の棚卸を実施する ・各 PC に暗号化ツールがインストールされているか又は USB メモリーが暗号化対応のものか確認する
備考	

関連する管理策：7.記憶媒体の管理 ① 8.暗号化 ①

上付き(N)は参考資料の番号を示す

業務 No.39	記憶媒体を持って出張に行く 2　【インターネットカフエの利用】
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
脅威の要因	□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
実施責任	■システム管理者　■業務・人事管理者　■従業員

セキュリティの対策の目的	暗号化により情報の漏えいから情報を保護するため
現状のセキュリティレベル	インターネットカフェなどセキュリティを確保できない場所での記憶媒体の使用を禁止していない
リスクシナリオ	インターネットカフェで利用した PC にインストールされていた不正なソフトウェアにより、記憶媒体に保管していた情報を盗まれる
技術的対策	記憶媒体に保存する情報は暗号化をする
人的対策	インターネットカフェなどセキュリティを確保できない可能性のある場所での情報の利用を禁止する
運用で心がけるポイント	記憶媒体内の情報が暗号化されていることを確認する
備考	

関連する管理策：8.暗号化 ①

上付き(N)は参考資料の番号を示す

業務 No.40	取引先との記憶媒体の授受
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
脅威の要因	□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
実施責任	□システム管理者　■業務・人事管理者　■従業員

セキュリティの対策の目的	情報の漏えいを防止するため
現状のセキュリティレベル	記憶媒体の受け渡し方法が決められていない
リスクシナリオ	記憶媒体が紛失した場合、授受記録が無いため、事件・事故発生当時の管理責任が不明確になる
技術的対策	組織間で共有できる暗号化方法を取りきめ、情報は暗号化して記憶媒体に保存する
人的対策	記憶媒体(情報)の受け渡しには授受記録を取り保管する
運用で心がけるポイント	記憶媒体の棚卸と記憶媒体の授受記録の確認
備考	

関連する管理策：7.記憶媒体の管理 ① 8.暗号化 ①

上付き(N)は参考資料の番号を示す

業務 No.41	公共の場所での携帯電話使用
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
脅威の要因	□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
実施責任	□システム管理者　■業務・人事管理者　■従業員

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ないアクセスを防止する
現状のセキュリティレベル	携帯電話の取り扱い方法を明確にしていない
リスクシナリオ	携帯電話を置き忘れる、あるいは紛失し、メール内の重要な情報及びアドレス帳の個人情報が漏えいする
技術的対策	・PIN 付きのロックをかける ・遠隔でデータを消去できる機能のものを使用する
人的対策	落下防止ストラップを利用する
運用で心がけるポイント	各携帯電話の設定をチェックし、ロックが設定されているか確認する
備考	

関連する管理策：2.認証と権限 ①

上付き(N)は参考資料の番号を示す

業務 No.42	社内へのリモートアクセス 1 【第三者による覗き見】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 ■従業員

セキュリティの対策の目的	ネットワークを経由した情報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	社内へのリモートアクセス時に、第三者が傍にいる事を意識せずに接続している
リスクシナリオ	社内へのリモートアクセス方法・認証方法を傍にいる第三者に覗き見され、社内ネットワークに接続されてしまう
技術的対策	・社外からリモートアクセスできるサーバー、サービスの範囲を最小限にしておく ・ID・パスワード認証に加え端末認証、物理的認証トークン、生体認証などの要素を加える
人的対策	・社内にリモートアクセスする際、周囲に社外の人がいないことを確認してから接続する ・リモートアクセスのパスワードを定期的に変更する
運用で心がけるポイント	外部からのアクセスログを定期的に確認する
備考	

関連する管理策：2.認証と権限 ①,②,③ 12.ネットワークのアクセス制御 ③

上付き(N)は参考資料の番号を示す

業務 No.43	社内へのリモートアクセス 2 【平文通信】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	ネットワークを経由した情報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	社外から社内へのリモートアクセスに平文(暗号化されていない)で通信している
リスクシナリオ	クライアント(社外の PC)から接続ポイント(社内のリモートアクセスサーバー)間が平文通信のため盗聴され情報が漏えいする
技術的対策	社外からのリモートアクセスには SSL-VPN、IPSec、PPTP などの暗号化通信技術を使用する
人的対策	
運用で心がけるポイント	リモートアクセスサーバーの通信設定に SSLVPN、IPSec、PPTP などの暗号化通信技術が使用されていることを確認する
備考	

関連する管理策：12.ネットワークのアクセス制御 ③

上付き(N)は参考資料の番号を示す

業務 No.44	社用車の利用
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
脅威の要因	□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
実施責任	■システム管理者　□業務・人事管理者　■従業員

セキュリティの対策の目的	暗号化により情報の漏えいから情報を保護する
現状のセキュリティレベル	社用車に荷物(重要な情報)を載せたままであることが常になっている
リスクシナリオ	駐車時など車から離れた際に車上荒しに遭い、車内に置いていた PC や記憶媒体が盗まれる
技術的対策	PC のハードディスク、記憶媒体は暗号化しておく
人的対策	社用車から離れる際は、PC や記憶媒体は車内に放置せず携帯する
運用で心がけるポイント	外部に持ち出す PC、記憶媒体が暗号化に対応しているか確認する
備考	

関連する管理策：8.暗号化 ①

上付き(N)は参考資料の番号を示す

4.退社

業務 No.45	業務終了
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
脅威の要因	□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
実施責任	□システム管理者　■業務・人事管理者　■従業員

セキュリティの対策の目的	情報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	机上の PC・書類・記憶媒体等を放置しての帰宅が許されている(クリアーデスク・クリアスクリーンポリシーが無い)
リスクシナリオ	PC・書類・記憶媒体を机上に放置したまま帰宅し、社内に残ったアクセス権の無い者が情報を閲覧する
技術的対策	PC に ID・パスワード付きのスクリーンセーバーの設定を行う
人的対策	帰宅時には PC をログアウト(ログオフ)し机上の書類･記憶媒体をすべて指定された場所へ収納し、重要情報の収納場所は施錠する
運用で心がけるポイント	業務終了後の机上の確認をする
備考	

関連する管理策：13.クリアデスク・クリアスクリーン ①,②

上付き(N)は参考資料の番号を示す

5.帰宅

業務 No.46	会社の PC を持ち帰っての作業 1 【自宅での盗難・不正アクセス】
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
脅威の要因	□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
実施責任	□システム管理者 □業務・人事管理者 ■従業員

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	自宅での会社 PC の使用ルールが無い
リスクシナリオ	・自宅に空き巣が入り会社 PC を盗まれる ・自宅に来た者に会社 PC を使用され情報が漏えいする
技術的対策	・ID・パスワードの設定に加えて BIOS レベルのパスワードを設定する ・会社 PC のハードディスクの暗号化を行う
人的対策	・家族、友人にも会社 PC の ID・パスワードは開示しない ・会社 PC と自宅 PC で同じパスワードを使用することを禁止する
運用で心がけるポイント	会社 PC の ID･パスワードの設定の確認及びハードディスクの暗号化の確認をする
備考	

関連する管理策：2.認証と権限 ① 8.暗号化 ①

上付き(N)は参考資料の番号を示す

業務 No.47	会社の PC を持ち帰っての作業 2 【ソフトウェアのインストール】
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
脅威の要因	□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
実施責任	■システム管理者 ■業務・人事管理者 ■従業員

セキュリティの対策の目的	アプリケーション・ソフトウェアの利用に伴う、情報の漏えい、改ざん、破壊から情報を保護するため
現状のセキュリティレベル	ソフトウェアの PC へのインストール規制が無い
リスクシナリオ	ソフトウェア(自宅で購入したソフトウェア、フリーソフトウェア、シェアソフトウェア、Winny、Share 等)を無許可で会社 PC にインストールし、そのソフトウェアの脆弱性により、ネットワークを通じて第三者に情報が漏えいする
技術的対策	ユーザのアカウントからソフトウェアのインストール権限を削除する
人的対策	ソフトウェアを会社 PC にインストールする場合は、申請を行うように定め、システム管理者がソフトウェア使用のリスクを判断した後、インストールを行う
運用で心がけるポイント	無許可のソフトウェアが会社 PC にインストールされていないかソフトウェアの棚卸を実施する
備考	

関連する管理策：9.アプリケーションの利用 ①,②

上付き(N)は参考資料の番号を示す

6.システム管理業務

業務 No.48	業務アプリケーションの設定変更作業 1　【一元管理】
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
脅威の要因	□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
実施責任	■システム管理者　□業務・人事管理者　□従業員

セキュリティの対策の目的	すべてのシステムに対する変更を一元的に管理して、障害・事故発生の可能性を最小限にするとともに、障害・事故発生時、障害・事故から速やかに回復するため
現状のセキュリティレベル	業務アプリケーションの設定変更作業をシステム管理者個人の力量に頼っている
リスクシナリオ	間違った設定をアプリケーションに行い、アプリケーションが停止し、障害原因が分からず障害が長期化する
技術的対策	障害時に早期に復旧できるように、アプリケーションのデータ及び設定情報のバックアップを取得しておく
人的対策	・アプリケーション設定変更についてのレビュー承認制度を導入し、影響範囲、変更計画、切り戻し計画等をレビューする ・アプリケーション変更の作業記録を残す
運用で心がけるポイント	・作業前に RPO(Recovery Point Objective)を満たしたバックアップがあることを確認する ・作業ごとに作業記録が作成されていることを確認する
備考	

関連する管理策：5.バックアップ ② 14.変更管理 ①,②,③,④

上付き(N)は参考資料の番号を示す

業務 No.49	業務アプリケーションの設定変更作業 2 【検証テスト】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	すべてのシステムに対する変更を一元的に管理して、障害・事故発生の可能性を最小限にするとともに、障害・事故発生時、障害・事故から速やかに回復するため
現状のセキュリティレベル	アプリケーションの検証テストに実データを使用している
リスクシナリオ	アプリケーション設定変更の検証テストに実データを使用し、設定間違いにより情報を破壊あるいは漏えいしてしまう
技術的対策	・アプリケーションデータのバックアップを取得しておく ・検証にはテスト用(ダミー)データを用いる ・重要なデータ項目はマスクしておく
人的対策	検証テストでの実データ使用の条件、ルールを作成する
運用で心がけるポイント	実データを使用する場合は作業前に RPO(Recovery Point Objective)を満たしたバックアップがあることを確認する
備考	

関連する管理策：5.バックアップ ② 14.変更管理 ⑤,⑥

上付き(N)は参考資料の番号を示す

業務 No.50	サーバーの管理業務 1 【冗長化、バックアップ】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	情報及びシステムを障害・事故から保護するため
現状のセキュリティレベル	ストレージ構成の冗長化をしておらず、また定期的なバックアップも取得していない
リスクシナリオ	ハードディスク障害によるサーバーの停止及びデータの損失が発生する
技術的対策	・ストレージの冗長化構成(RAID、リプリケーション等)を行う ・バックアップを定期的に行う
人的対策	データファイル、構成ファイルを定期的に他記憶媒体にコピーする
運用で心がけるポイント	・冗長化構成メンバーに故障が発生していないか監視する ・バックアップ、冗長化が RPO、RTO を満たしているか確認する
備考	

関連する管理策：5.バックアップ ①,②,③

上付き(N)は参考資料の番号を示す

業務 No.51	サーバーの管理業務 2 【構成管理】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	すべてのシステムに対する構成情報を一元的に管理して、障害・事故発生の可能性を最小限にするとともに、障害・事故発生時、障害・事故から速やかに回復するため
現状のセキュリティレベル	サーバー(ハードウェア、OS、アプリケーション)の構成管理を行っていない
リスクシナリオ	サーバー(ハードウェア、OS、アプリケーション)の構成情報(機器構成、OS・アプリケーション・関連ソフトウェアの構成・バージョン)が誤っているため、設定変更時に障害を引き起こす
技術的対策	
人的対策	サーバーの導入時及び変更時の設定情報、構成情報を保管する
運用で心がけるポイント	サーバーの構成情報と実際の現状構成を突き合わせて確認する
備考	

関連する管理策：15.構成管理 ①,②

上付き(N)は参考資料の番号を示す

業務 No.52	サーバーの管理業務 3 【障害管理】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	システム障害、セキュリティ事故が発生した場合、根本原因を取り除き、再発防止を行うため
現状のセキュリティレベル	障害管理を行っていない
リスクシナリオ	・障害管理を行っていないため、小さな障害を放置し、やがて大規模な障害に発展してしまう ・障害管理を行っていないため、過去に発生した障害が再発した場合、迅速に対応できない
技術的対策	
人的対策	些細な障害から大規模障害まで報告を行い、障害の原因と障害から復旧までの記録を残す
運用で心がけるポイント	障害記録の確認及び是正・予防処置の確認をする
備考	

関連する管理策：16.障害・事故管理 ②,③

上付き(N)は参考資料の番号を示す

業務 No.53	サーバーの管理業務 4 【障害・問題発生時の連絡体制】
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
脅威の要因	□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
実施責任	■システム管理者 ■業務・人事管理者 □従業員

セキュリティの対策の目的	システム障害、セキュリティ事故が発生した場合、根本原因を取り除き、再発防止を行うため
現状のセキュリティレベル	障害、問題発生時の連絡体制がない
リスクシナリオ	事故・障害発生時に連絡体制が無いため報告漏れ・遅れが発生し、事故・障害対応に時間を要する
技術的対策	
人的対策	障害、問題発生時の連絡体制を整備する
運用で心がけるポイント	連絡体制には社内のみならずサポート業者、取引業者、警察、監督諸官庁等の外部も考慮に入れること
備考	

関連する管理策：16.障害・事故管理 ①

上付き(N)は参考資料の番号を示す

業務 No.54	サーバーの管理業務 5 【システムログの取得】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	許可されていない情報処理活動の検知、システム異常の検知及び障害・事故を分析するため
現状のセキュリティレベル	サーバーのシステムログを取得していない
リスクシナリオ	サーバーのシステムログを取得していないため問題を早期に発見できない、あるいは発生後、原因が追求できない
技術的対策	サーバーのシステムログを取得し、定期的にレビューを行い問題が発生していないことを確認する
人的対策	
運用で心がけるポイント	問題発生時に比較するため、サーバーが正常な状態のシステムログを保存しておく
備考	

関連する管理策：6.ログの取得 ②

上付き(N)は参考資料の番号を示す

業務 No.55	サーバーの管理業務 6 【アクセスログの取得】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	許可されていない情報処理活動の検知、システム異常の検知及び障害・事故を分析するため
現状のセキュリティレベル	サーバーのアクセスログを取得していない
リスクシナリオ	アクセスログを取得していないため、サーバーへの不正アクセスを早期に発見できない
技術的対策	サーバーのアクセスログを取得し、定期的にレビューを行い不正アクセスが発生していないことを確認する
人的対策	
運用で心がけるポイント	・サーバーの時間を標準時間と同期しておく ・ログは 6 カ月以上保存しておく
備考	

関連する管理策：6.ログの取得 ①,③,④

上付き(N)は参考資料の番号を示す

業務 No.56	サーバーの管理業務 7 【負荷状況の監視】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	システムの容量・能力を業務の変化に合わせ最適化することにより、障害・事故発生の可能性を最小限にするため
現状のセキュリティレベル	サーバーのリソース(CPU、メモリー、記憶媒体、ディスク IO、ネットワーク帯域等)の使用状況を監視していない
リスクシナリオ	サーバーの負荷状況を監視していないため、リソースの限界を超えサーバーを利用してしまい、障害が発生する(OS 領域に割り当てたハードディスクが一杯になりシステムが停止する等)
技術的対策	サーバーの監視ツールを導入、負荷状況を監視し、状況に適合するリソースの増強や構成変更の実施を行う
人的対策	定期的にサーバーの負荷状況を監視し、監視結果に基づいたリソースの増強や構成変更の実施を行う
運用で心がけるポイント	各リソースの閾値を決めておく
備考	

関連する管理策：17.容量・能力の管理 ①,②

上付き(N)は参考資料の番号を示す

業務 No.57	ネットワークの管理業務
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
脅威の要因	□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
実施責任	■システム管理者　□業務・人事管理者　□従業員

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	許可の無いネットワーク機器の社内ネットワークへの接続を制御していない
リスクシナリオ	利用者がシステム管理者の許可無しに、ネットワーク機器を社内ネットワークに接続し、ループを発生させ、社内ネットワークが利用できなくなる
技術的対策	・端末(MAC)認証を行い、許可しないネットワーク機器は接続できないようにする ・ループ防止対策の設定をネットワーク機器にする
人的対策	ネットワークのポートに鍵付きプロテクターを付ける
運用で心がけるポイント	ユーザはシステム管理者の許可無しに、アクセス可能な場所にあるネットワークを使用できないことを確認する
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
12.ネットワークのアクセス制御　⑦

上付き(N)は参考資料の番号を示す

業務 No.58	レガシーシステム(アプリケーションが古いため最新の OS に対応できないシステム)の管理
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
脅威の要因	□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
実施責任	■システム管理者　■業務・人事管理者　□従業員

セキュリティの対策の目的	情報の漏えい、改ざん、破壊及びソフトウェアの改ざん、破壊を防止するため
現状のセキュリティレベル	保守サポートの無い OS、ハードウェア機器を使用しているため、セキュリティパッチ等のセキュリティ対策が行えない
リスクシナリオ	ネットワーク経由でレガシーシステムとデータ共有を行い、レガシーシステムにウイルスを感染させる
技術的対策	データはウイルスチェック可能な UTM 装置等を経由させ、レガシーシステムに入力する
人的対策	レガシーシステムでデータを使用する前に、別のシステムでウイルスチェックを行う
運用で心がけるポイント	定期的にレガシーシステムのバックアップを取得する

備考	レガシーシステムとは、一般的に、時代遅れとなった古いシステムのことを言う

関連する管理策：3.ウイルス及び悪意のあるプログラムに対する対策 ③,④,⑦

上付き(N)は参考資料の番号を示す

業務 No.59	Web(ホームページを含む)サイトの開発・管理業務１ 【重要情報の管理】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	情報の漏えいを防止するため
現状のセキュリティレベル	重要情報を公開 Web サーバー上に保存している
リスクシナリオ	公開 Web サーバー上に保存している重要情報が Web サーバーのセキュリティホールを利用され漏えいする
技術的対策	重要情報は公開 Web サーバーとは別のネットワークセグメントにあるサーバー上に保存し、外部からアクセスできないようにアクセス制御を行う
人的対策	
運用で心がけるポイント	公開 Web サーバー上に重要情報が保存されていないことを確認する
備考	

関連する管理策：12.ネットワークのアクセス制御 ①,②,④,⑤

18.Web の開発・管理 ②,③

上付き(N)は参考資料の番号を示す

業務 No.60	Web(ホームページを含む)サイトの開発・管理業務 2 【パッチの適用】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	公開されている技術的脆弱性の悪用によって生じる情報の改ざんを防止するため
現状のセキュリティレベル	公開 Web サーバーにセキュリティパッチを適用していない
リスクシナリオ	公開 Web サーバーのセキュリティホールを利用され、ホームページを改ざんされる
技術的対策	
人的対策	セキュリティパッチがリリースされるとすぐに適用する
運用で心がけるポイント	・公開 Web ページが改ざんされていないか定期的に確認する ・公開 Web サーバーに使用しているアプリケーション、ミドルウエアを洗い出し、脆弱性情報の収集を定期的に行う
備考	

関連する管理策：4.パッチの適用 ①

上付き(N)は参考資料の番号を示す

業務 No.61	Web(ホームページを含む)サイトの開発・管理業務 3 【開発】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	情報の漏えい、改ざん、破壊及びソフトウェアの改ざん、破壊を防止するため
現状のセキュリティレベル	公開 Web サイトの開発時に、セキュリティを意識せず開発している
リスクシナリオ	セキュリティを意識せず公開 Web サイトを開発したため、脆弱性が多数存在し、クロスサイトスクリプティング等によりサイト利用者がセキュリティ被害に遭う
技術的対策	WAF(Web Application Firewall)を導入する
人的対策	公開 Web サイトの開発時は OWASP、IPA などの開発ガイドラインに従い開発を実施する
運用で心がけるポイント	定期的に第三者機関の検査または監査を実施する
備考	

関連する管理策：12.ネットワークのアクセス制御 ①,②,④,⑤

18.Web の開発・管理 ③,④,⑤

上付き(N)は参考資料の番号を示す

業務 No.62	Web(ホームページを含む)サイトの開発・管理業務 4 【著作権】
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
脅威の要因	□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
実施責任	■システム管理者 □業務・人事管理者 □従業員

セキュリティの対策の目的	情報の漏えい、改ざん、破壊及びソフトウェアの改ざん、破壊を防止するため
現状のセキュリティレベル	会社が著作権を持つ情報に対して､公開 Web サーバーの利用者に著作権を主張していない
リスクシナリオ	会社が著作権を持つ公開 Web サーバー上の情報を､利用者に不正(知らずに)に利用される
技術的対策	カット&ペーストできない Web ページを作成する
人的対策	会社がその情報に対して著作権を所有することを明示的に表示する
運用で心がけるポイント	

備考	

関連する管理策：18.Web の開発・管理 ①

上付き(N)は参考資料の番号を示す

7.情報セキュリティ対策シート

業務 No	
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
脅威の要因	□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
実施責任	□システム管理者　□業務・人事管理者　□従業員

セキュリティの対策の目的	
現状のセキュリティレベル	
リスクシナリオ	
技術的対策	
人的対策	
運用で心がけるポイント	

備考	

上付き(N)は参考資料の番号を示す

付録

1.用語

(1)情報資産

JIS Q 27002:2006 には次のような資産の事例がある[(2)]

① 情報：データベース及びデータファイル、契約書及び同意書、システム文書、調査情報、マニュアル、事業継続計画、証跡、保存情報等

② ソフトウェア資産：業務用ソフトウェア、システムソフトウェア、開発ツール、ユーティリティソフトウェア等

③ 物理的資産：コンピューター、ネットワーク装置、取り外し可能な媒体等

④ サービス：計算処理サービス、通信サービス、暖房、電源、空調、照明等

⑤ 人：保有する資格、技能、経験

⑥ 無形資産：組織の評判、イメージ

(2)機密性(Confidentiality)

許可されていない個人、グループ、組織、システムに対して、情報を使用不可又は非公開にする特性

(3)完全性(Integrity)

情報資産の正確さ及び完全さを保護する特性

(4)可用性(Availability)

許可された個人、グループ、組織、システムが要求したときに、アクセス及び使用が可能である特性

(5)適法性(Compliance)

法令、規則または契約上のあらゆる義務、及びセキュリティ上のあらゆる要求事項に対する遵守

(6)脅威(Threat)

情報資産の機密性、完全性、可用性に危害を与える原因となる事象で、人為的(意図的、作為的)なものと環境的(地震、落雷など)なものに分類される

上付き(N)は参考資料の番号を示す

(7)脆弱性(Vulnerability)

脅威によって利用されるおそれのある弱点

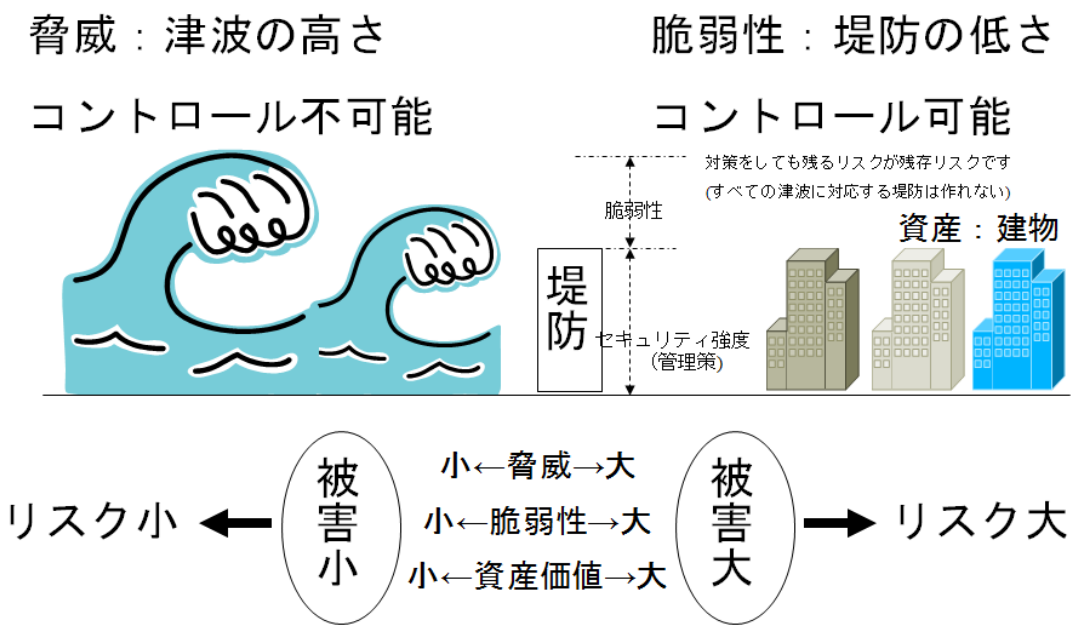


図　付録-1 脅威と脆弱性

2.情報資産の洗い出しについて

組織が情報を適切に管理し、機密性、完全性、可用性を守るための包括的な枠組みである ISMS の構築ステップでは、企業の保有する情報資産を洗い出し、洗い出した情報資産に対して、リスクを特定・分析・評価・対応、情報セキュリティ対策を順次行っていく。

上付き(N)は参考資料の番号を示す

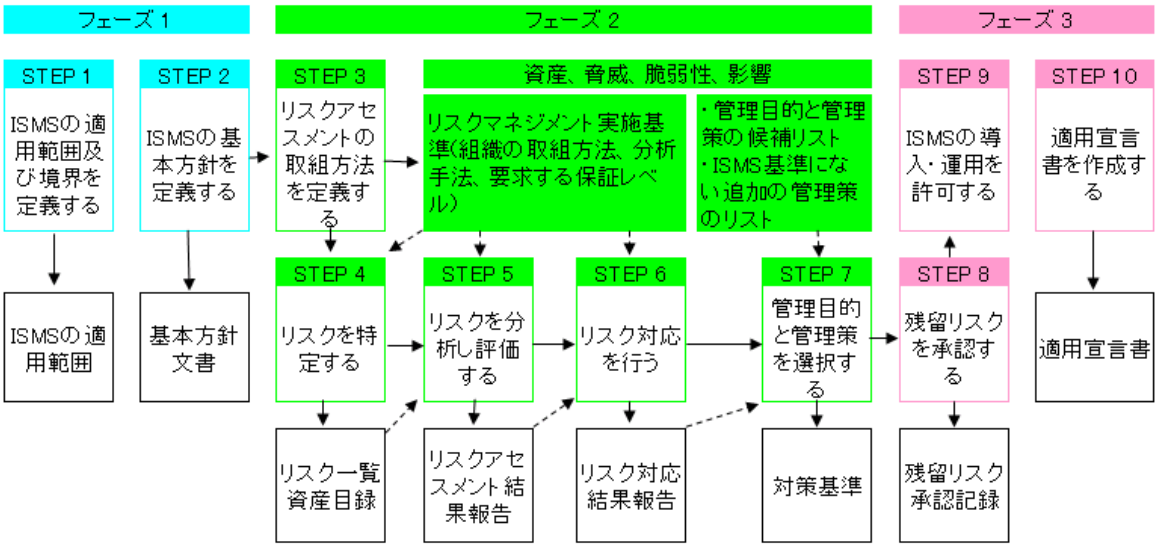


図　付録-2　ISMS 構築のステップ（JIS Q 27001:2006）[2]

この情報資産をベースにした情報セキュリティ対策アプローチには次のような課題がある。

(1) 作業が膨大であり、金銭面、工数面で企業に非常な負担を強いる

(2) 専門的な知識が必要であり、独力で行うことが難しい

(3) 情報資産を洗い出した後に、発生する新規の情報については、次の情報資産の洗い出しまで、リスク対応・対策から漏れる可能性がある

しかし、組織がどんなレベルの情報を保有しているのか？ あるいは、各レベルの情報が漏えいした場合にどんな影響があるのか？ を把握しておくことは情報セキュリティ対策を行うにあたって、過剰な対策、投資を防止する意味において有効であるので、ここでは情報の分類例を 2 例紹介しておく。

まず、ISMS では組織の持つ資産を、機密性、完全性、可用性の規準から資産を評価する方法を例示している。表 付録-1 機密性基準による情報の分類例を示す。

上付き[N]は参考資料の番号を示す

資産価値	クラス	説明
1	公開	第三者に開示・提供可能 情報漏えいした場合、損失は無い
2	社外秘	社内のみ開示・提供可能 情報漏えいした場合、損失または売り上げ減
3	秘密	特定の関係者または部署のみに開示・提供可能 情報漏えいした場合、大きな損失または大幅な売り上げ減
4	極秘	所定の関係者のみに開示・提供可能 情報漏えいした場合、倒産の可能性

表 付録-1 機密性基準による情報の分類例[2]

また、日本セキュリティ監査協会(JASA)では「2010 年度 情報セキュリティ監査シンポジウム公演資料」[16]の中で、取り扱う情報を、情報漏えいが発生した場合のインパクトを基準に、表 付録-2 情報資産のカテゴリ分類(例)に示すように 5 つのカテゴリに分類している。

カテゴリ	定義	インパクト例	情報例	管理レベル
Ⅳ	社会全体に重要な被害 (国全体)	・国家レベルの影響 ・損害補償"莫大" ・お金で解決レベルを越える ・取引停止	国防関連等国家機密や人命の安全に関わるきわめて重要な情報	特別な体制と管理策 (絶対に漏洩させない！)
Ⅲ-2	社会的インフラに重要な被害	・重要社会インフラに影響 ・損害補償額"大" ・金銭保証(顧客/エンドユーザともに個別対応) ・営業活動停止(長期)	ライフライン等重要社会インフラの維持安全に関わる情報	強い管理策＋外部監査＋α (通常の管理策と異なる)
Ⅲ	組織活動、組織資産、または個人に **重大な被害**	・特定個人・顧客への影響 ・損害賠償額は"中" ・金銭保証(顧客：個別対応、エンドユーザ：金券相当) ・営業活動一時停止	個人情報：個人情報及び法人個人情報のうち、受委託業務に関わる情報 **Ⅲ-A** その他：きわめて重要度の高い営業秘密情報(特に重要な技術ノウハウetc)、公開前の財務情報 **Ⅲ-B**	強い管理策＋外部監査
Ⅱ	組織活動、組織資産、または個人に **相当な被害**	・対外的な影響が少ない ・監督官庁への報告レベル ・損害賠償額は"小～中" ・営業対応稼働が中心	重要な営業秘密情報、社員個人情報、取引先法人個人情報	通常の管理策＋内部監査
Ⅰ	組織活動、組織資産、または個人に **限定的な被害**	・影響は少なく限定的 ・監督官庁への報告レベル	委託先社員に公開している(委託先内限り)機密性の低い情報	通常の管理策

表 付録-2 情報資産のカテゴリ分類(例)[16]

※ JASA 2010 年度 情報セキュリティ監査シンポジウム公演資料

「今日から実践！ サプライチェーン情報セキュリティ管理と監査の活用」より

上付き[N]は参考資料の番号を示す

3.本手引き管理項目とISMS 詳細管理策との対応

本手引き管理項目	ISMS-ISO/IEC27001:2005-付属書A 対応管理策
1.セキュリティ境界と入退室管理	A.9.1.1,A.9.1.2
2.認証と権限	A.11.2.1,A11.2.2,A.11.2.4,A.11.5.1,A.11.5.2,A.11.5.3,A.11.6.1
3.ウイルス及び悪意のあるプログラムに対する対策	A.10.4.1,A10.4.2
4.パッチの適用	A.12.6.1
5.バックアップ	A.10.5.1
6.ログの取得	A.10.10.1,A.10.10.2,A.10.10.3,A.10.10.4,A.10.10.5,A.10.10.6
7.記憶媒体の管理	A.10.7.1,A10.7.2
8.暗号化	A.12.3.1,A.12.3.2
9.アプリケーションの利用	
10.電子メールの利用	A.10.8.4
11.外部サービスの利用	A.10.2.1
12.ネットワークのアクセス制御	A.11.4.2,A.11.4.3,A.11.4.5,A.11.4.6,A.11.4.7
13.クリアデスク・クリアスクリーン	A.11.3.3
14.変更管理	A.10.1.2,A12.5.1
15.構成管理	A.7.1.1,A.12.4.1
16.障害・事故管理	A.13.1.1,A.13.1.2,A.13.2.2
17.容量・能力の管理	A.10.3.1
18.Webの開発・管理	A.10.9.1,A.10.9.2,A10.9.3

表 付録-3 本手引き管理策と ISMS 詳細管理策の対応

※ISMS-ISO/IEC27001:2005-付属書 A　対応管理策は関連度が最も近いものを紐づけた。

上付き(N)は参考資料の番号を示す

4.システム概念図

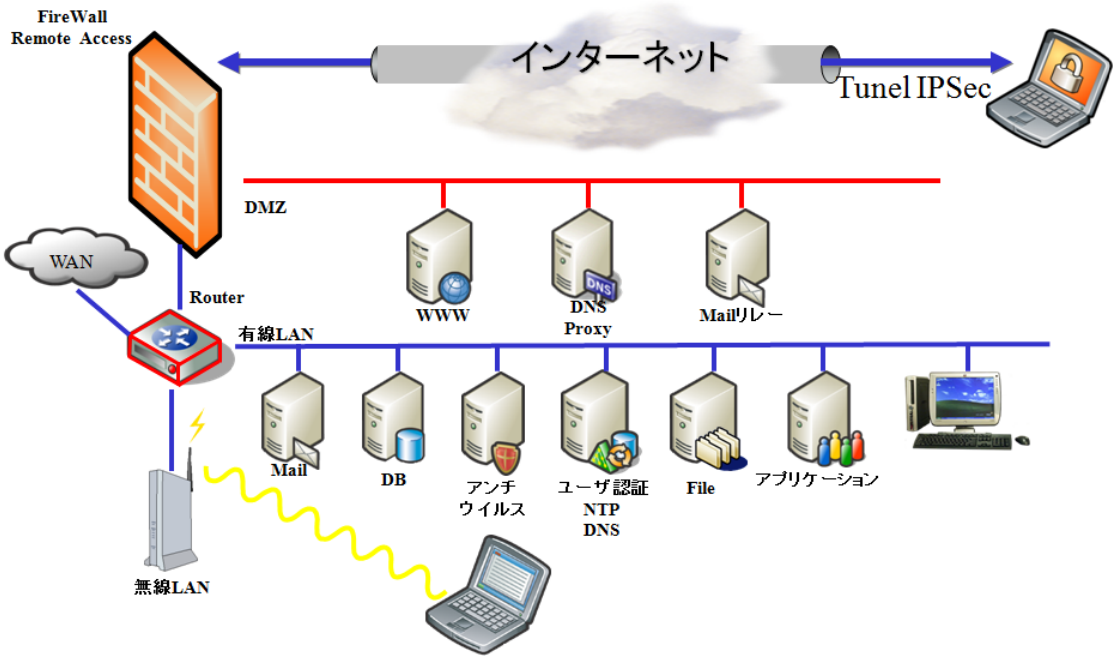


図　付録-3 システム概念図

※　図　付録-3 は本手引きを読む上で参考になるように記載したもので、推奨するシステムの概念図ではない。

上付き(N)は参考資料の番号を示す

参考資料

(1) NPO 日本ネットワークセキュリティ協会(JNSA)
2008 年度活動成果物「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

(2)財団法人　日本情報処理開発協会(JIPDEC)
「ISMS ユーザガイド　-JIS Q 27001:2006(ISO/IEC 27001:2005)対応-」
http://www.isms.jipdec.jp/doc/JIP-ISMS113-21.pdf

(3)日本工業標準調査会審議
「JIS Q 27001:2006(ISO/IEC 27001:2005)
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システム―要求事項」
発行　日本規格協会

(4) NPO 日本ネットワークセキュリティ協会(JNSA)
「情報セキュリティプロフェッショナル教科書」
発行　アスキー・メディアワークス

(5)財団法人　日本情報処理開発協会(JIPDEC)　プライバシーマーク事務局
「JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン―第 2 版―」
http://privacymark.jp/reference/pdf/guideline_V2.0_100917.pdf

(6)日本工業標準調査会審議
「個人情報保護マネジメントシステム-要求事項（JIS Q 15001:2006)」
発行　日本規格協会

(7) NPO 日本ネットワークセキュリティ協会(JNSA)
2006 年度活動成果物「個人情報保護対策チェックシート集計結果」
http://www.jnsa.org/result/2006.html

(8) NPO 日本ネットワークセキュリティ協会(JNSA)
「個人情報保護法対策セキュリティ実践マニュアル 2005 年度版」
発行　インプレス ネットビジネスカンパニー

(9)Japan Vulnerability Notes
「共通セキュリティ設定一覧 CCE 概説 (パスワード編)」
http://jvndb.jvn.jp/apis/myjvn/cccheck/cce_password.html

(10)社団法人　電子情報技術産業協会
「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項」
http://it.jeita.or.jp/perinfo/committee/pc/JEITA_HDDdata100219F.pdf

(11)社団法人　電子情報技術産業協会
「データ消去に関する各種規格のご紹介」
http://it.jeita.or.jp/infosys/committee/network/guideline0407/standard.html

(12)総務省　経済産業省
「電子政府推奨暗号リスト」
http://www.cryptrec.go.jp/images/cryptrec_01.pdf

(13)経済産業省
「SaaS 向け SLA ガイドライン」
http://www.meti.go.jp/press/20080121004/03_guide_line_set.pdf

(14)The Open Web Application Security Project
「安全な Web アプリケーション構築の手引き
　-The Open Web Application Security Project-」
http://www.owasp.org/index.php/Main_Page

(15)独立行政法人 情報処理推進機構(IPA)
「安全なウェブサイトの作り方」
http://www.ipa.go.jp/security/vuln/documents/website_security.pdf

(16) NPO 日本セキュリティ監査協会(JASA)
2010 年度　情報セキュリティ監査シンポジウム公演資料
「今日から実践！ サプライチェーン情報セキュリティ管理と監査の活用」
http://www.jasa.jp/seminar/sym2010/pdf/s2010tokyo03.pdf

(17)独立行政法人 情報処理推進機構(IPA)
中小企業の情報セキュリティ対策ガイドライン「委託関係における情報セキュリティ対策ガイドライン」
http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-itaku.pdf

(18)総務省
「国民のための情報セキュリティサイト」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/download.htm

＊リンク先は２０１１．３．３１現在のものです。

NPO 日本ネットワークセキュリティ協会　西日本支部　WG メンバー

西日本支部長	井上　陽一	JNSA 顧問
WG リーダー	元持　哲郎	アイネット・システムズ株式会社
	浅野　二郎	
	礒元　芳昭	株式会社 OSK
	宇佐川　道信	パナソニック電工株式会社
	大財　健治	株式会社ケーケーシー情報システム
	久保　寧	富士通関西中部ネットテック株式会社
	小柴　宏記	株式会社ケーケーシー情報システム
	齋藤　聖悟	株式会社インターネットイニシアティブ
	嶋倉　文裕	富士通関西中部ネットテック株式会社
	田口　智子	株式会社 ラック
	堀内　敦	株式会社 OSK
	宮下　勝彦	ヒューベルサービス株式会社
オブザーバ	近畿経済産業局	地域経済部　情報政策課