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」活用方法

元持哲郎
アイネット・システムズ株式会社
JNSA西日本支部

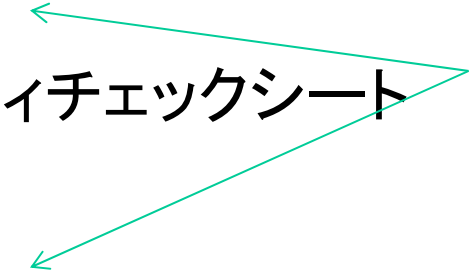
2014年 2月21日

# 最初に

- 情報セキュリティは中小企業にこそ必要!!
  - 機密性は、情報資産へのアクセスを最小限度に留めることで、購入する情報資産の金額を最小にします。
  - 完全性は、情報資産が正確、正しく動くことを保証し、業務を効率化します。
  - 可用性は、欲しい情報を欲しい時に入手できることで、業務時間を短縮します。

# 各ツールの位置付け

- Why: 9to5 (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　略称)
  - リスクの認識
  - セキュリティ対策
- How:情報セキュリティチェックシート
  - 現状の把握
  - セキュリティ対策
  - PDCAを回す
- What:JNSAソリューションガイド
  - 具体的な製品、サービスの選定



共通
ISO27001/27002:2005

# 9to5の対象企業

## 従業員300人以下

| 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。 | 9to5 |
| 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。 | |

ソリューションガイド

チェックシート

西日本支部 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」より

# 9to5の目的

- 中小企業の業務に伴うリスクが認識できる
- 中小企業が具体的なリスク対策が行える
- 情報の洗い出し無でセキュリティ対策が可能

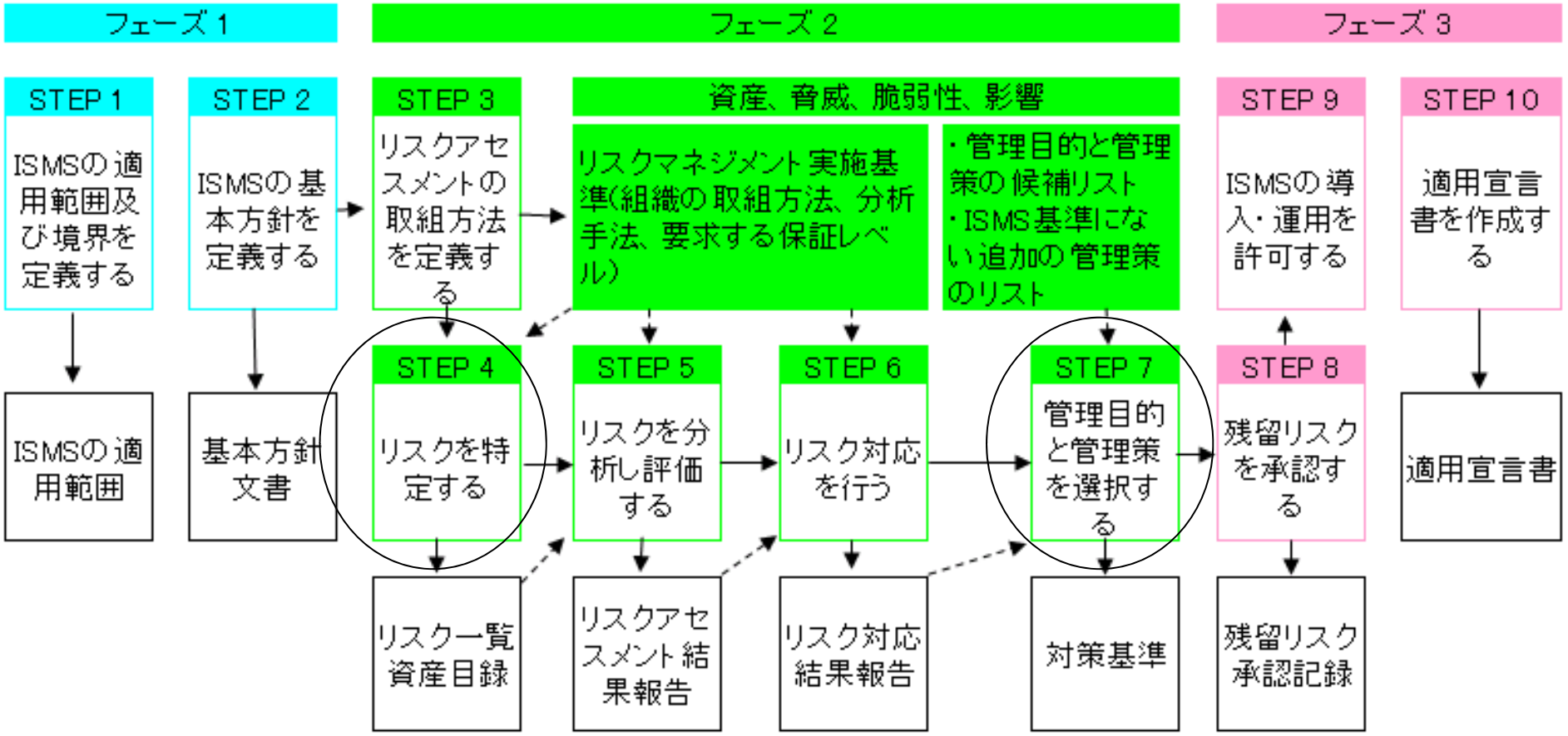
# 9to5の対象者

- 企業のシステム管理者
- システム管理を外注している管理者
- 中小企業を指導するITコーディネータ、IT企業

# 9to5の管理策から省いた項目

- 対象が紙・物に関するもの
- 電源、空調等の設備管理に関するもの
- 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
- 個人情報保護に関するもの
- 委託管理に関するもの
- 対策が教育・啓蒙になるもの

# 9to5の対応範囲




※JIPDEC ISMSユーザーズガイドより

情報セキュリティチェックシートの範囲

# 9to5の構成

- 導入部
  - 1.概要
  - 2.本ガイドライの対象企業
  - 3.本ガイドラインの対象読者
  - 4.本ガイドラインの使用方法
- 第1部
  - 21の情報セキュリティ管理項目(2011年版：18)
- 第2部
  - 69業務に基づく情報セキュリティ対策例(2011年版：62)
- 付録
- 参考資料

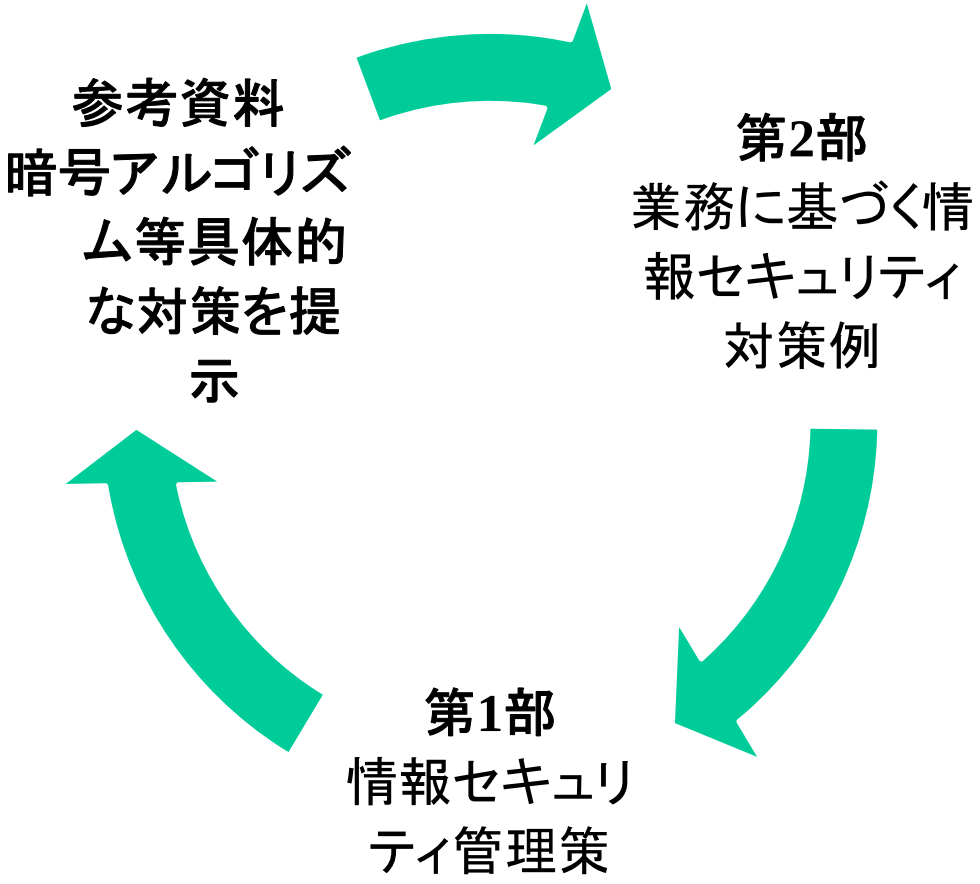
# 9to5の第1部

| 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.クラウドサービスの利用 | A.10.2.1 |
| 3.障害・事故管理 | A.13.1.1,A.13.1.2,A.13.2.2 |
| 4.IT継続性 | A.14.1.1,A.14.1.2,A.14.1.3,A.14.1.4,A.14.1.5 |
| 5.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 |
| 6.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 |
| 7.パッチの適用 | A.12.6.1 |
| 8.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 |
| 9.記憶媒体の管理 | A.10.7.1,A10.7.2 |
| 10.スマートデバイスの利用 | A.9.2.5,A11.7.1,A.11.7.2 |
| 11.電子メールの利用 | A.10.8.4 |
| 12.Webの開発・管理 | A.10.9.1,A.10.9.2,A10.9.3 |
| 13.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 |
| 14.バックアップ | A.10.5.1 |
| 15.容量・能力の管理 | A.10.3.1 |
| 16.変更管理 | A.10.1.2,A12.5.1 |
| 17.構成管理 | A.7.1.1,A.12.4.1 |
| 18.SNSの利用 | A.10.8.4 |
| 19.暗号化 | A.12.3.1,A.12.3.2 |
| 20.アプリケーションの利用 | |
| 21.クリアデスク・クリアスクリーン | A.11.3.3 |

# 9to5の第2部

- 出社　　1業務(2011年版:1業務)
- 社内業務　　33業務(2011年版:31業務)
- 社外業務　　15業務(2011年版:12業務)
- 退社　　1業務(2011年版:1業務)
- 帰宅　　4業務(2011年版:2業務)
- システム管理業務　15業務(2011年版:15業務)

# 9to5の活用方法



# 活用事例①

| | |
|---|---|
| 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 □スマートデバイス □電子機器(IC レコーダー、カメラ他) □クラウドサービス(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 |

# 活用例①

| | |
|---|---|
| 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<br>・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：5.認証と権限 ⑥

# 活用例①

**5.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

**(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、スマートデバイス（スマートフォン、タブレット）、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、ワンタイムパスワード、二段階、IDカード、デバイス(ハードウェアトークン、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)等及びこれらの組み合わせ(複数要素認証)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「12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アクセスする情報の重要度、情報機器のある場所及び情報にアクセスする場所により認証の強度を検討する

**(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、クラウドの利用、SNS、スマートデバイスの利用

# 活用例①

(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

表1. パスワード関連項目を対象としたCCE識別番号と推奨値

| CCE-ID | | セキュリティ項目 | セキュリティ設定ガイド | | |
|---|---|---|---|---|---|
| XP | Vista | | DISA(*a) | FDCC(*b) | マイクロソフト |
| CCE-2981-9 | CCE-2883-7 | パスワードの最低文字数設定<br>(パスワードの長さ) | 14文字以上 | 12文字以上 | 8文字以上 |
| CCE-2920-7 | CCE-2967-8 | パスワードの有効期間 | 60日以下 | 60日以下 | 90日以下 |
| CCE-2994-2 | CCE-2323-4 | パスワードの履歴管理<br>(同じパスワードを連続して使えない回数) | 24個以上 | 24個以上 | 24個以上 |
| CCE-2439-8 | CCE-3240-9 | パスワードの変更禁止期間 | 1日以上 | 1日以上 | 1日以上 |
| CCE-2986-8 | CCE-3177-3 | ログオンできなくなるまでのパスワード入力失敗回数(アカウントのロックアウトのしきい値) | 3回以内 | 5回以内 | 50回以内 |
| CCE-2466-1 | CCE-2715-1 | パスワード入力失敗回数のリセットまでの期間<br>(ロックアウトカウントのリセット) | 60分以上 | 15分以上 | 15分以上 |
| CCE-2928-0 | CCE-2363-0 | ログオン不可状態からの復旧時間<br>(ロックアウト期間) | ロックアウト期間を永久 | 15分以上 | 15分以上 |
| CCE-2980-1 | CCE-3050-2 | スクリーンセーバーが起動するまでの時間<br>(スクリーンセーバーのタイムアウト) | 15分以下 | 15分以下 | - |
| CCE-4500-5 | CCE-4290-3 | パスワード付きスクリーンセーバー | 要設定 | 要設定 | - |

# 活用例①

| 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,.2,22,30,65 |
| | ② | 1,.2,22,30 |
| | ③ | 3 |
| 2.クラウドサービスの利用 | ① | 25,26,28 |
| | ② | 24,25,26,28 |
| | ③ | |
| 3.障害・事故管理 | ① | 60 |
| | ② | 59 |
| | ③ | 59 |
| 4.IT継続性 | ① | 57 |
| | ② | |
| | ③ | |
| 5.認証と権限 | ① | 1,4,12,21,30,37,44,45,51 |
| | ② | 4,21,24,45 |
| | ③ | 1,2,3,5,21,45 |
| | ④ | 1,2,21 |
| | ⑤ | 21 |
| | ⑥ | 6 |

# 活用例②

| | |
|---|---|
| 業務 No.48 | スマートデバイスを利用した業務【OS・アプリケーションの設定】 |
| 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<br>□ネットワーク　□アプリケーション　□記憶媒体(USB メモリー他)<br>□プリンター　□FAX　□コピー機　■スマートデバイス　□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)<br>□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 | スマートデバイスの利用に伴う、情報の漏えい、改ざん、破壊を防止するため |
| 現状のセキュリティレベル | スマートデバイスの使用に関するガイドラインが無い |
| リスクシナリオ | 顧客・パートナー情報を含んだスマートデバイスのアドレス帳と SNS が自動同期になっており、さらに SNS 招待メール機能が有効になっていたため、SNS から顧客・パートナーへ招待メールが送信されてしまった |

# 活用例②

| | |
|---|---|
| 技術的対策 | デバイス管理ツールを利用しスマートデバイスの管理を行う |
| 人的対策 | ・スマートデバイス使用に関するガイドラインを策定する<br>・SNS 使用に関するガイドラインを策定する |
| 運用で心がけるポイント | スマートデバイスの OS、アプリケーションのバージョンアップに伴う設定変更に注意する |
| 備考 | |

関連する管理策：10.スマートデバイスの利用 ④,⑤,⑨ 18.SNS の利用 ①

# 活用例②

**10.スマートデバイスの利用**

(1)管理目的

スマートデバイス(スマートフォン、タブレット)の利用に伴う、情報の漏えい、改ざん、破壊を防止するため

**(2)管理策**

①スマートデバイスの資産管理を行う

②ジェイルブレイク、ルート化を禁止する

③製造者及びキャリアの提供するパスコードロック、自動ロック、パスコード入力に失敗した場合のデータ消去、リモートワイプ、暗号化、ウイルス及び悪意のあるプログラムに対する対策機能は有効にしておく

④有償、無償を問わず組織が許可したアプリケーション(ソフトウェア)のみ使用を許可する

⑤有償、無償を問わず組織が許可したクラウドサービスのみ使用を許可する

⑥スマートデバイス、アプリケーションの脆弱性情報を入手し、リリースされたセキュリティパッチは必ず適用する

⑦社外でWi-Fi、赤外線、Bluetoothネットワークに接続する場合は、信頼できるネットワークのみ利用する

⑧重要な情報をスマートデバイス以外にバックアップする手順を備える

⑨スマートデバイスの使用ガイドライン(21)(22)(23)を定める。

**(3)運用で心がけるポイント**

①位置情報とアプリケーション、スマートデバイスとクラウドサービス及びSNSとの自動連携機能の設定を確認し、意図しない連携を防止する

②定期的にスマートデバイスの棚卸しを実施すると共に設定状況を確認し、セキュリティパッチの適応状況、許可アプリケーション以外使用されていないことを確認する

**(4)関連する管理項目**

認証と権限、パッチの適用、記憶媒体の管理、暗号化、バックアップ、クラウドサービスの利用、SNSの利用

# 活用例②

**18.SNSの利用**

**(1)管理目的**

従業員が SNSを私的利用するに際し、企業情報の漏えいを防止すると共に、企業の信用失墜を防止するため。

**(2)管理策**

①従業員がSNSを利用する場合の、勤務先名の記載可否、企業が持つ公開情報についての記載可否または記載範囲・記載条件、SNS上での顧客、取引先社員との交友方法、私的情報の記載内容、利用方法について、SNS使用ガイドライン(24)を定める

**(3)運用で心がけるポイント**

①使用デバイス(PC、スマートフォン、タブレット)とSNSの設定により、使用デバイス上のデータ、写真、位置情報とSNSが自動連携されることに注意する

②SNSの設定変更、機能追加による情報漏えいに注意する

③従業員の法律、公序良俗に違反するSNSの記載により、企業の信用失墜の可能性があることに注意する

④SNSセキュリティ設定の問題により、SNSのアカウントが乗っ取られ、悪用される可能性のあることに注意する

**(4)関連する管理項目**

認証、クラウドサービスの利用

# 活用例②

NPO 日本ネットワークセキュリティ協会(JNSA)

「スマートフォンの安全な利活用のすすめ
～ スマートフォン利用ガイドライン ～」

http://www.jnsa.org/result/2012/smap_guideline_v1.0.pdf

一般社団法人　日本スマートフォンセキュリティ協会(JSSEC)

「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」

http://www.jssec.org/dl/guidelines2011_v1.1.pdf

一般社団法人　日本スマートフォンセキュリティ協会(JSSEC)

「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン　補足資料」

http://www.jssec.org/dl/BYOD_BasicData2012_v1.0.pdf

NPO 日本ネットワークセキュリティ協会(JNSA)

「SNSの安全な歩き方
～セキュリティとプライバシーの課題と対策～」

http://www.jnsa.org/result/2012/SNS-WG_ver0.7.pdf

# 活用例②

| 第1部 | | 第2部 |
|---|---|---|
| 本手引き管理項目 | 管理策 | 業務No |
| 10.スマートデバイスの利用 | ① | |
| | ② | 49 |
| | ③ | 44,49 |
| | ④ | 48,49 |
| | ⑤ | 48,49 |
| | ⑥ | |
| | ⑦ | 42 |
| | ⑧ | |
| | ⑨ | 48,49 |
| 13.ログの取得 | ① | 3,62 |
| | ② | 61 |
| | ③ | 62 |
| | ④ | 62 |
| | ⑤ | |
| 14.バックアップ | ① | 9,23,57 |
| | ② | 9,23,55,56,57 |
| | ③ | 23,57 |
| 15.容量・能力の管理 | ① | 63 |
| | ② | 63 |
| 16.変更管理 | ① | 55 |
| | ② | 55 |
| | ③ | 55 |
| | ④ | 55 |
| | ⑤ | 56 |
| | ⑥ | 56 |
| 17.構成管理 | ① | 10,58 |
| | ② | 58,64 |
| | ③ | |
| 18.SNSの利用 | ① | 48,53,54 |

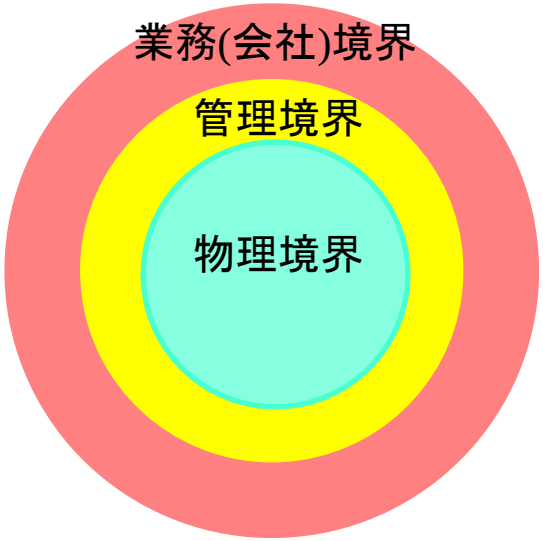
# 9to5の公開

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

2014年版もJNSA Webサイトで公開致します

# 対策課題

- 従来の高リスクの課題
  - 企業外の情報資産、業務活動
- 今後の高リスクの課題
  - 企業の資産外の情報機器
  - 業務外の従業員の活動



# 最後に

- 対策をおこなうための優先順位が必要!!
  - リスクの起こる頻度
  - 業務の重要度
  - 業務で関連する情報の重要度　付録
  - 現状の対策レベル

ご清聴ありがとうございました。