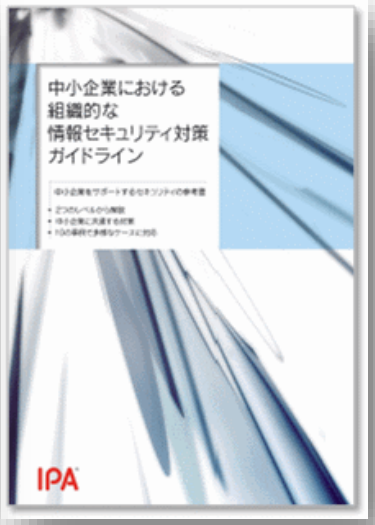
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

中小企業の情報セキュリティ対策ガイドライン
～内容の理解と組織での活用～

JNSA マーケティング部会
持田　啓司
（株式会社ラック）

中小企業の
情報セキュリティ対策ガイドラインとは

- IPAにより作成された、中小企業に求められる情報セキュリティ対策を、中小企業ならではの視点から実現するための方策を提示したガイドライン
- 初版は2009年発行。本編と三つの別冊で構成、別冊「５分でできる！情報セキュリティ自社診断」は中小企業にて広く利用されている



ガイドライン改訂の背景

- 発行後7年、IT環境の急速な変化への対応
  - スマートデバイス（スマートフォン、タブレット端末）の業務利用の浸透
  - モバイルコンピューティング、クラウドサービスの普及
- 新たな脅威への対応

	10大脅威2009年	10大脅威2015
1位	変化を続けるウェブサイト改ざんの手口	ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞやｸﾚｼﾞｯﾄｶｰﾄﾞ情報の不正利用
2位	アップデートしていないクライアントソフト	内部不正による情報漏えい
3位	悪質なウイルスやボットの多目的化	標的型攻撃による諜報活動
4位	対策をしていないサーバ製品の脆弱性	ウェブサービスへの不正ログイン
5位	あわせて事後対応を！情報漏えい事件	ウェブサービスからの顧客情報の窃取
6位	被害に気づけない標的型攻撃	ハッカー集団によるサイバーテロ
7位	深刻なＤＤoS攻撃	ウェブサイトの改ざん
8位	正規のアカウントを悪用される攻撃	ｲﾝﾀｰﾈｯﾄ基盤技術を悪用した攻撃
9位	クラウド・コンピューティングのセキュリティ問題	脆弱性公表に伴う攻撃
10位	ｲﾝﾀｰﾈｯﾄｲﾝﾌﾗを支えるプロトコルの脆弱性	悪意のあるスマートフォンアプリ

ガイドライン改訂の背景

- 社会的要請・法的責任拡大への対応
  - 個人情報保護法改正
  - マイナンバー法施行
  - 改正不正競争防止法

- 中小企業の実態に対応
  - 経営者への情報セキュリティ意識向上が必要
  - 情報セキュリティ対策の社内担当者が不在

IPA 情報セキュリティ10大脅威 2017

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	**1位**	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	**2位**	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	**3位**	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	**4位**	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	**5位**	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	**6位**	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	**7位**	ウェブサービスへの不正ログイン	9位
8位	情報モラル欠如に伴う犯罪の低年齢化	**8位**	IoT 機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	**9位**	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT 機器の不適切な管理	**10位**	インターネットバンキングやクレジットカード情報の不正利用	8位

中小企業の情報セキュリティ対策ガイドライン第2版

- 中小企業の経営者やIT担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン
  - 経営者が認識すべき「3原則」、企業として取り組むべき「重要7項目の取組」
  - 情報セキュリティ対策の具体的な導入手順や課題の改善手順
  - すぐに使える「情報資産管理台帳」や「リスク分析シート」等の雛形

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

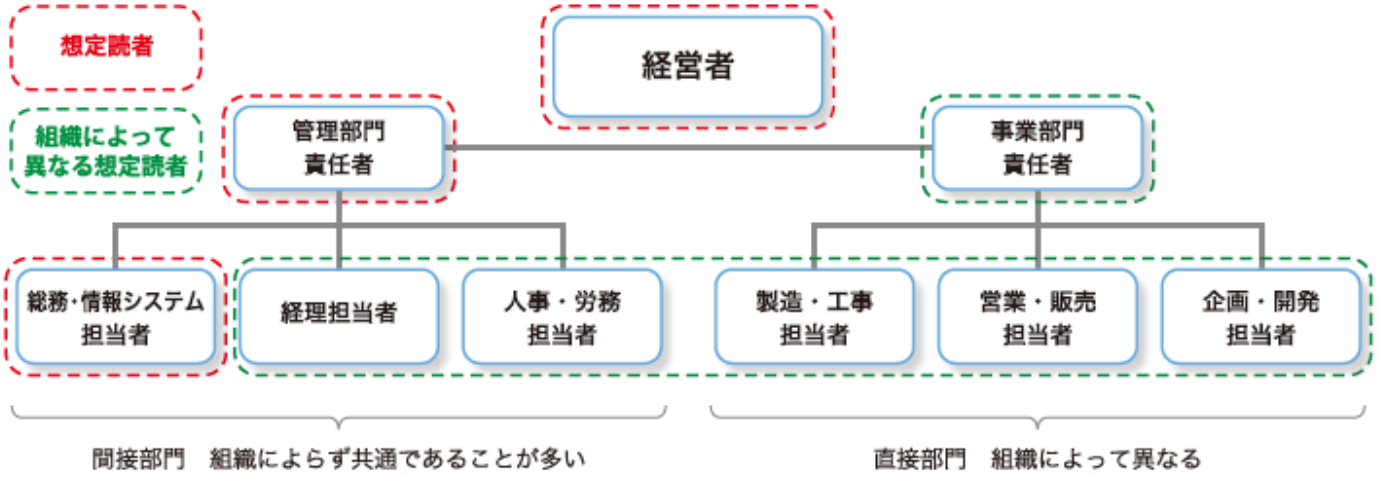
ガイドラインの構成

- 情報セキュリティ対策の考え方や実践方法について説明するもので、本編2部と付録より構成されています

構成			概要
本編	第1部 経営者編		経営者が自らの責任で対応しなければならない事項について説明しています。
	第2部 管理実践編		重要な情報に対する管理責任がある立場の方向けに、組織的な情報セキュリティ管理の進め方について説明しています。
付録	付録1 情報セキュリティ5か条		企業の規模を問わず必ず実行していただきたい重要な対策を5か条にまとめ説明しています。
	付録2 5分でできる！情報セキュリティ自社診断		あまり時間をかけることなく実行することで効果がある対策25項目の診断シートです。
	付録3 わが社の情報セキュリティポリシー	ツールA リスク分析シート	情報資産管理台帳、脅威の状況、対策状況チェックをもとに自社のリスクを試算できます。
		ツールB 情報セキュリティポリシーサンプル	ツールAの結果をもとに、自社に適した情報セキュリティポリシーを策定するためのひな形です。

対象組織・想定読者

- 対象組織
  - 業種を問わず中小企業及び小規模事業者
  - 法人のほか、個人事業主や各種団体も含む
- 想定読者
  - 組織の経営者
  - 経営者の指示のもとで重要な情報を管理する方



第1部 経営者編

経営者の関心事から情報セキュリティに対する認識を喚起

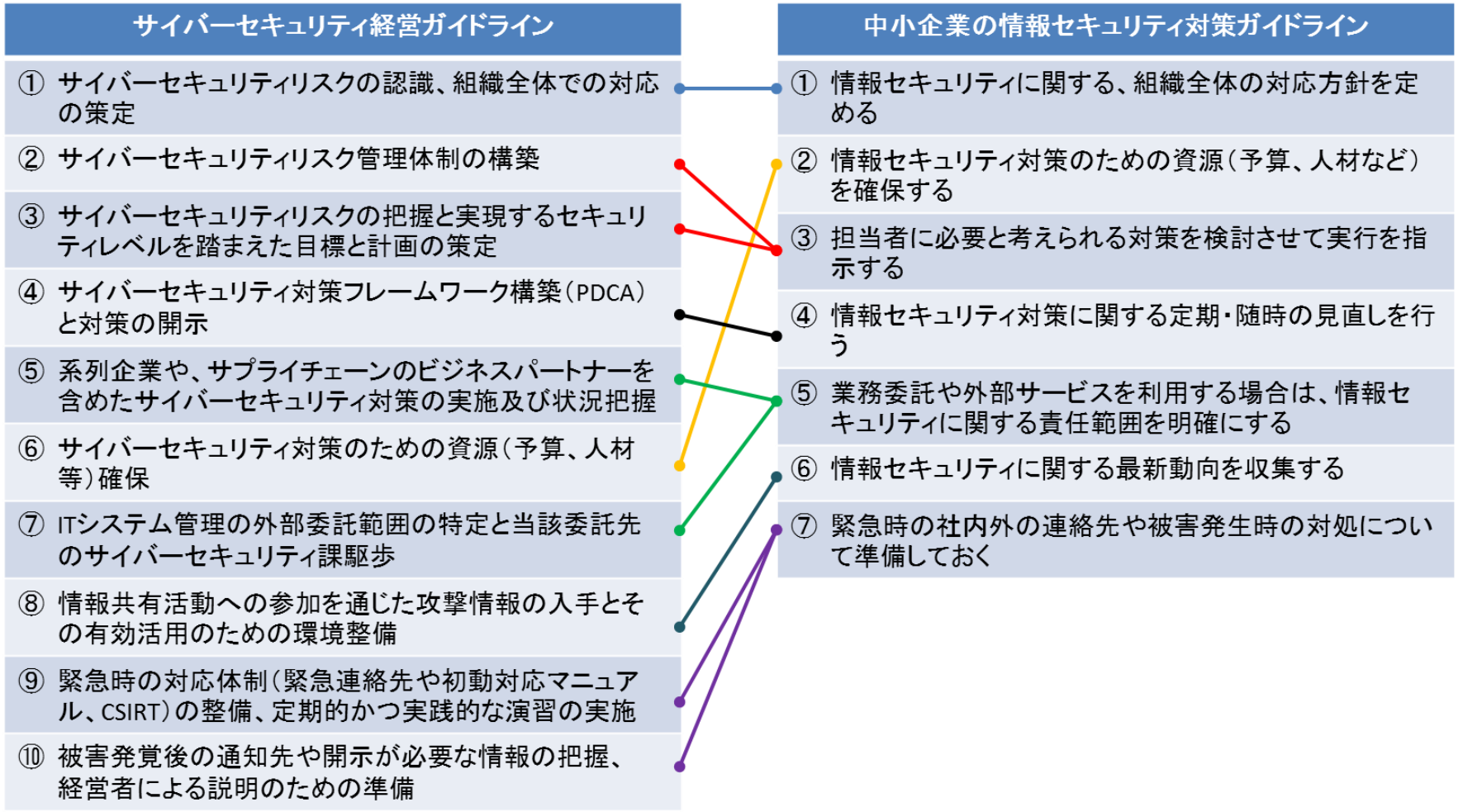
- 事故により企業が被る不利益
  - 金銭の喪失 … 経済的損失例
  - 顧客の喪失 … 顧客の減少例
  - 業務の喪失 … 業務の支障例
  - 従業員への影響
- 経営者が負う責任
  - 法的責任 … 刑事罰・被害者や会社に対する損害賠償責任
  - 関係者や社会に対する責任 … 顧客・取引先に対する責任

第1部 経営者編

経営者の立場でやるべきことを「３原則」「7取組」として提示

原則1	情報セキュリティ対策は経営者のリーダーシップで進める
原則2	委託先の情報セキュリティ対策まで考慮する
原則3	関係者との情報セキュリティに関するコミュニケーションは、どんなときにも怠らない
取組1	情報セキュリティに関する、組織全体の対応方針を定める
取組2	情報セキュリティ対策のための資源（予算、人材など）を確保する
取組3	担当者に必要と考えられる対策を検討させて実行を指示する
取組4	情報セキュリティ対策に関する定期・随時の見直しを行う
取組5	業務委託や外部サービスを利用する場合は、情報セキュリティに関する責任範囲を明確にする
取組6	情報セキュリティに関する最新動向を収集する
取組7	緊急時の社内外の連絡先や被害発生時の対象について準備しておく

（参考）サイバーセキュリティ経営ガイドラインの重要１０項目と中小企業の情報セキュリティ対策ガイドラインの重要７項目の関係性



第２部 管理実践編

特に意識していない

Step1
まず始める

情報セキュリティ５か条

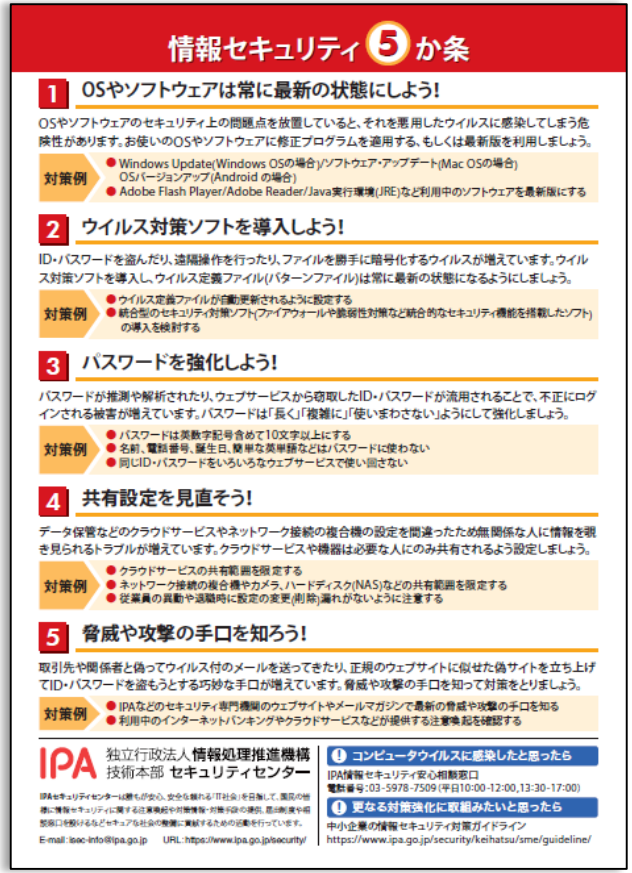
JNSA

一般的なＩＴ環境で、すぐに実行できる基本的対策

【活用例】

情報セキュリティを特に意識していない
小規模事業者や個人事業主の職場で、

- 経営者または管理者が朝礼で説明
- A4で印刷して従業員に配付
- A3で印刷してオフィスに掲示



情報セキュリティ５か条

1 OSやソフトウェアは常に最新の状態にしよう!

OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

対策例
- Windows Update(Windows OSの場合)/ソフトウェア・アップデート(Mac OSの場合)
  OSバージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/Java実行環境(JRE)など利用中のソフトウェアを最新版にする

2 ウイルス対策ソフトを導入しよう!

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。

対策例
- ウイルス定義ファイルが自動更新されるように設定する
- 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)の導入を検討する

3 パスワードを強化しよう!

パスワードが推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使いまわさない」ようにして強化しましょう。

対策例
- パスワードは英数字記号含めて10文字以上にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じID・パスワードをいろいろなウェブサービスで使い回さない

4 共有設定を見直そう!

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えています。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

対策例
- クラウドサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスク(NAS)などの共有範囲を限定する
- 従業員の異動や退職時に設定の変更(削除)漏れがないように注意する

5 脅威や攻撃の手口を知ろう!

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

対策例
- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

IPA 独立行政法人 情報処理推進機構 技術本部 セキュリティセンター

IPAセキュリティセンターは誰もが安心、安全な暮らしを実現する「IT社会」を目指して、国民の皆様に情報セキュリティに関する注意喚起や対策情報・対策手段の提供、思い創造や相談窓口を設けるなどセキュアな社会の実現に貢献するための活動を行っています。

E-mail：isec-info@ipa.go.jp　URL：https://www.ipa.go.jp/security/

コンピュータウイルスに感染したと思ったら
IPA情報セキュリティ安心相談窓口
電話番号：03-5978-7509（平日10:00-12:00,13:30-17:00）

更なる対策強化に取組みたいと思ったら
中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

演習①

- 個人ワーク（5分）
  - 各自で自社は5か条がどの程度できているかチェックしましょう。

1 OSやソフトウェアは常に最新の状態にしよう！
2 ウイルス対策ソフトを導入しよう！
3 パスワードを強化しよう！
4 共有設定を見直そう！
5 脅威や攻撃の手口を知ろう！

- 講師から状況チェックの質問
  - 対策内容は理解できるか？
  - すべて定期的にチェックできているか？

できる範囲で実施している

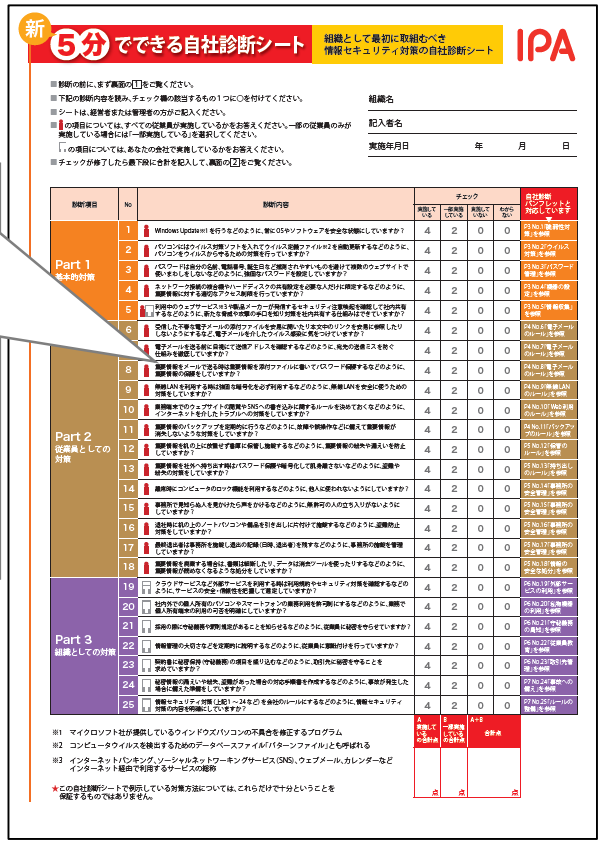
Step2
現状を知り改善する

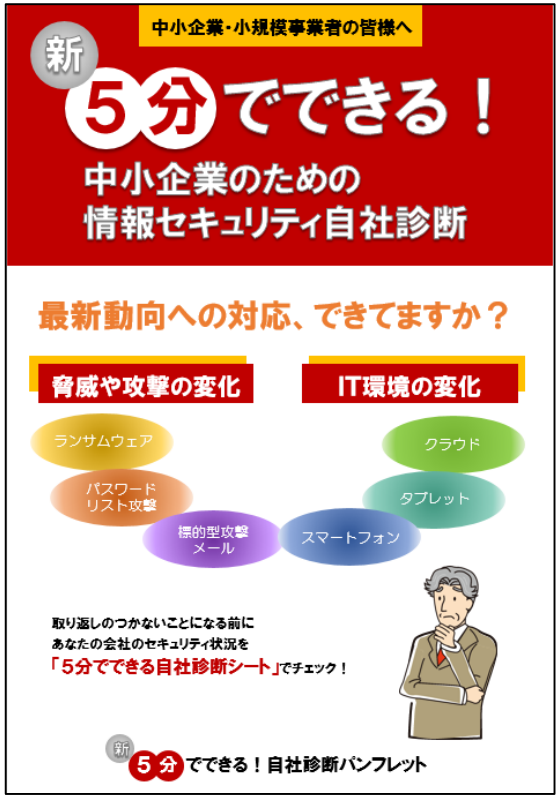
5分でできる！ 情報セキュリティ自社診断

JNSA

25の診断項目に答えるだけで、自社の情報セキュリティの問題点を簡単にチェック

- 基本的対策（5項目）
  脆弱性対策、ウイルス対策、パスワード強化など
- 従業員としての対策（13項目）
  事務所の安全管理、持ち出し、廃棄、電子メール、Web利用など
- 組織としての対策（7項目）
  従業員、取引先、ルールなど





演習②

- 個人ワーク（10分）
  - 「5分でできる自社診断」により、各自で自社の状況について自社診断を実施。

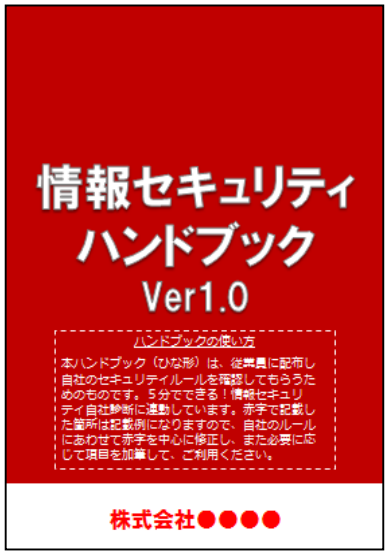
- 講師から状況チェックの質問
  - 基本、従業員、組織の、それぞれよくできている部分と、あまりできていない部分を理解する
  - できていない部分については、なぜできていないかを考える

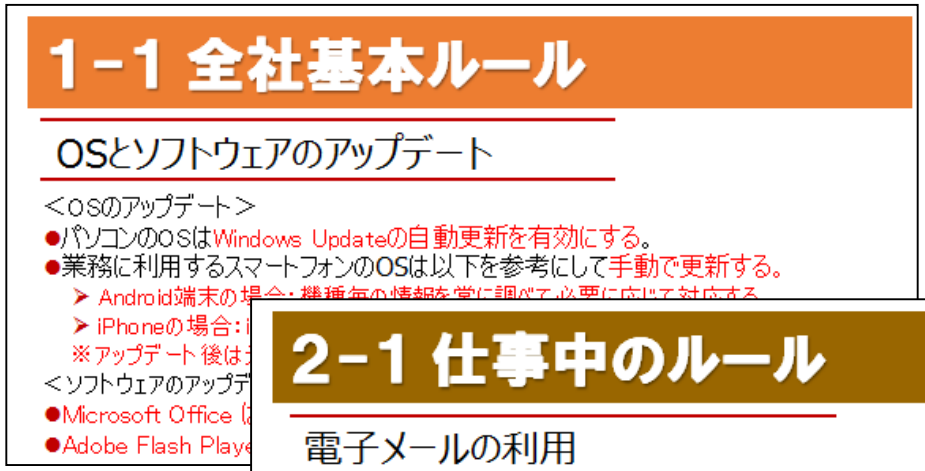
できる範囲で実施している

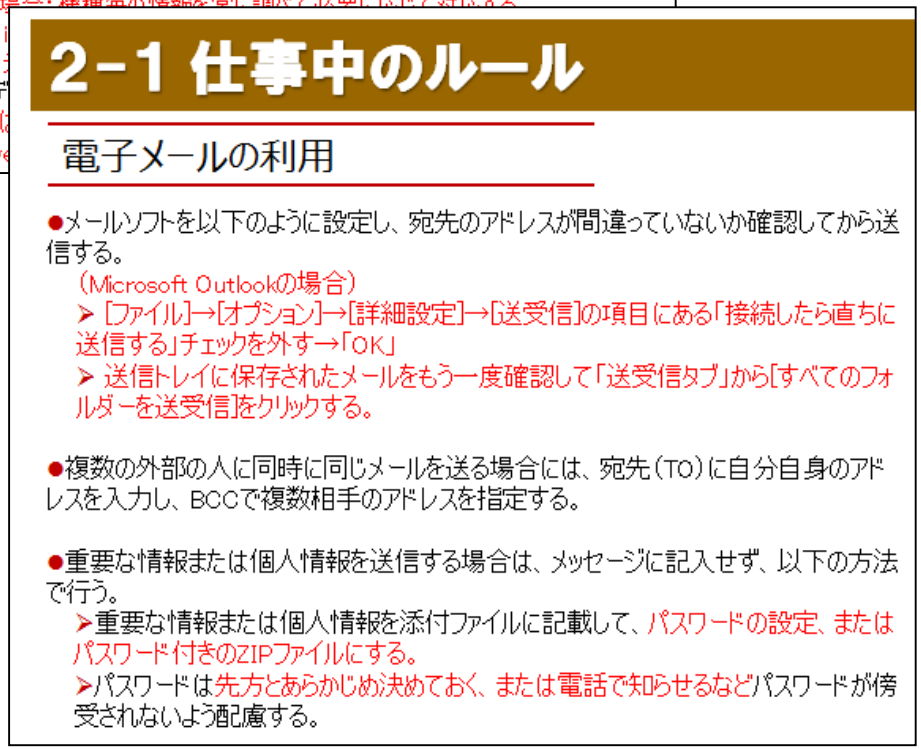
Step2
現状を知り改善する

情報セキュリティ ハンドブックでルール化

JNSA







【活用例】

社内ルールを定め「情報セキュリティハンドブック」で周知

- 経営者または管理者が従業員に説明会を実施
- 印刷して従業員に配付

組織的に取り組みたい

Step3
本格的に取り組む

わが社のポリシー策定

JNSA

手順1 情報資産管理台帳を作成する

どのような情報資産があるか洗い出して重要度を判断する。

手順2 リスク値の算定

リスクの大きさを算定し対策が必要な情報資産を把握する

手順3 情報セキュリティ対策を決定

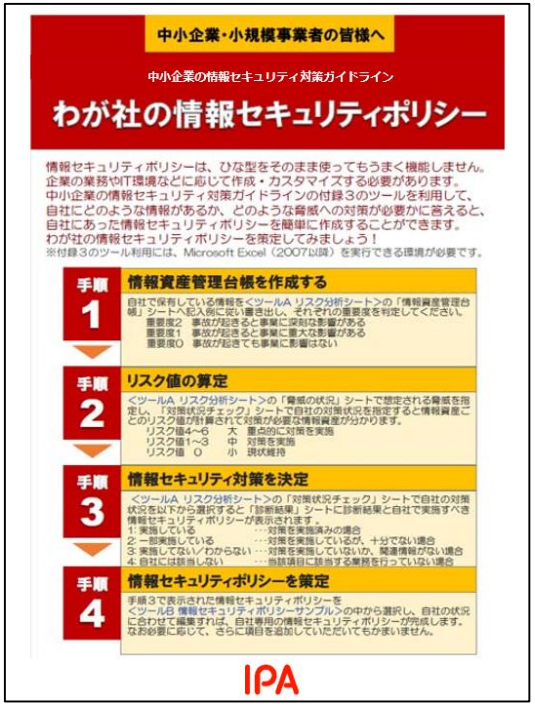
対策を決める

手順4 情報セキュリティポリシーを策定

対策を社内ルールにする

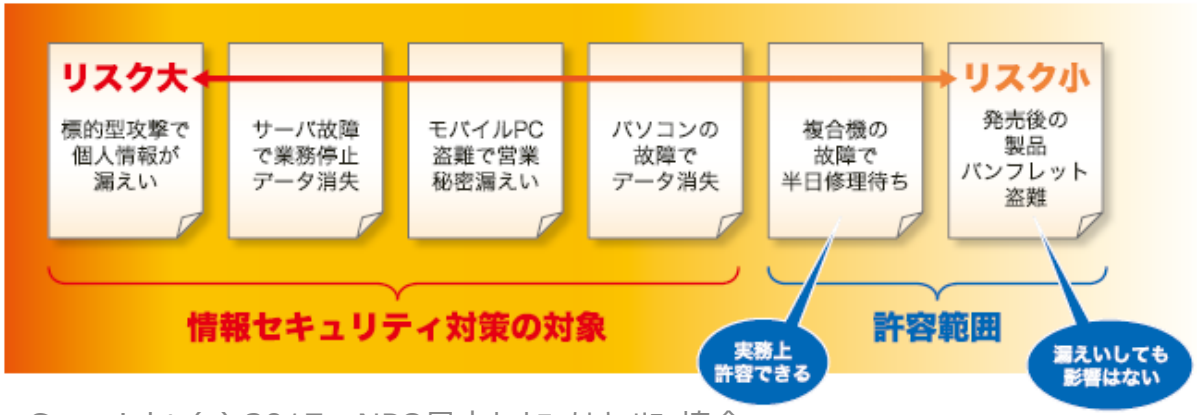
中小企業の情報セキュリティ対策ガイドライン付録３
わが社の情報セキュリティポリシー

- 中小企業において情報セキュリティポリシーを策定し、これをもとに対策を実践していくための手順について説明しています
  - <ツールＡ　リスク分析シート>と、<ツールB　情報セキュリティポリシーサンプル>を手順に従って埋めていくことで、簡単に自社のセキュリティポリシーを作ることが可能です



ポリシー策定の基本的な考え方

- 自社に適合したポリシーを策定
  - 企業が直面するリスクは、事業領域や取り扱う情報、企業を取り巻く環境によっても異なるため、ポリシーのサンプルを入手して社名を変えるだけではうまく機能しません。
- リスクの大きなものから重点的に対策を実施
  - 限られた予算を有効に使うには、あらかじめリスク分析を行い、いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、リスクが大きなものから重点的に対策を定めます。



重要度を図る上でのリスクの洗い出し

ガイド補足

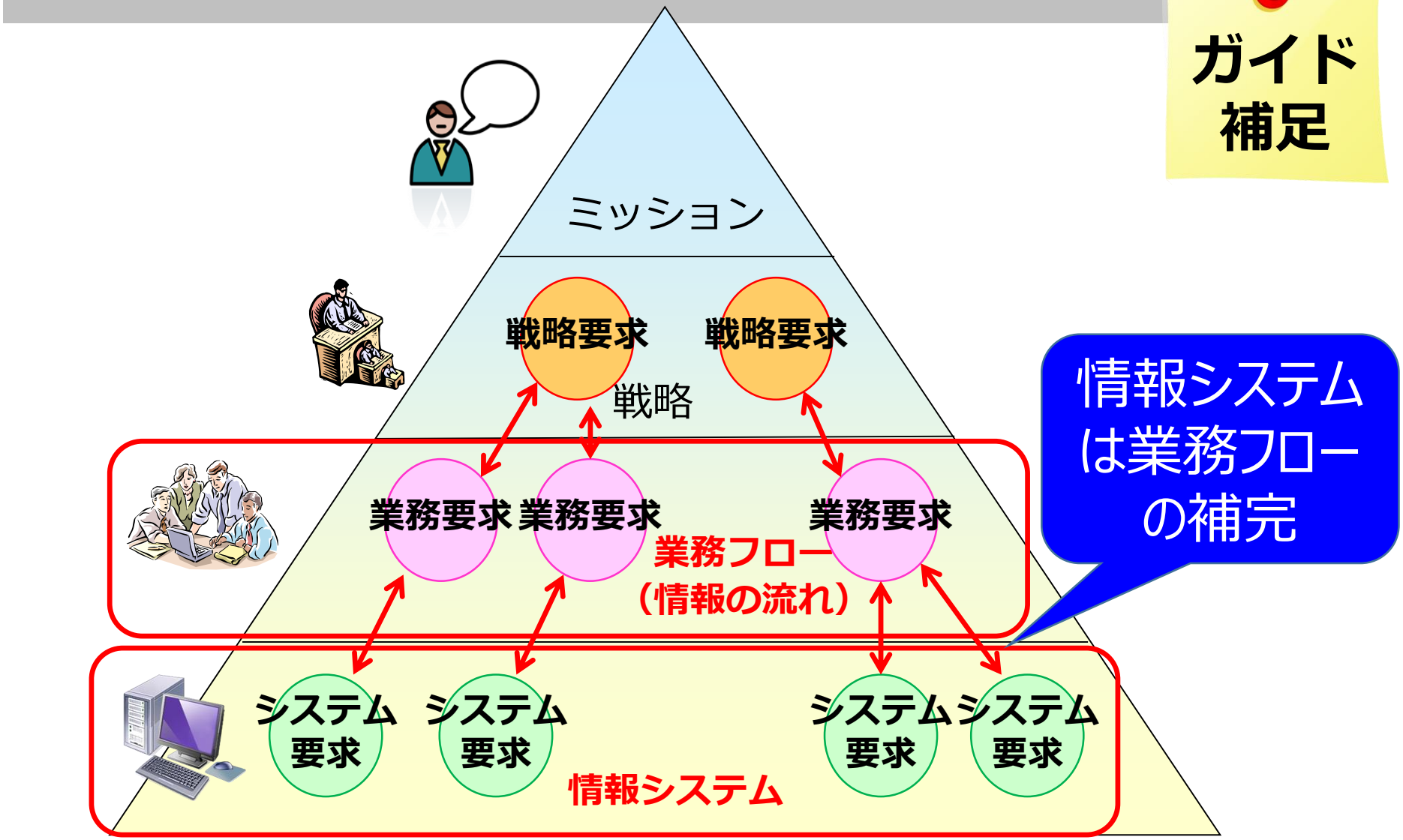
- 「リスク」は可能性であり、「脅威」は組織に損害や影響を与える可能性であるリスクを引き起こす要因。
- リスクを考える際には、“機密性”“完全性”“可用性”が損なわれる事象(要因：脅威)を考えます。

“機密性”の欠如	非開示情報（秘密情報、設定情報、システム構成等）の露呈、流出に結び付く事象。
“完全性”の欠如	取り扱う情報の誤り、改ざん、欠落に結び付く事象。
“可用性”の欠如	情報システムの停止、処理の遅延、情報資産の消失、利用不可に結び付く事象。

企業経営における業務と情報システム

JNSA

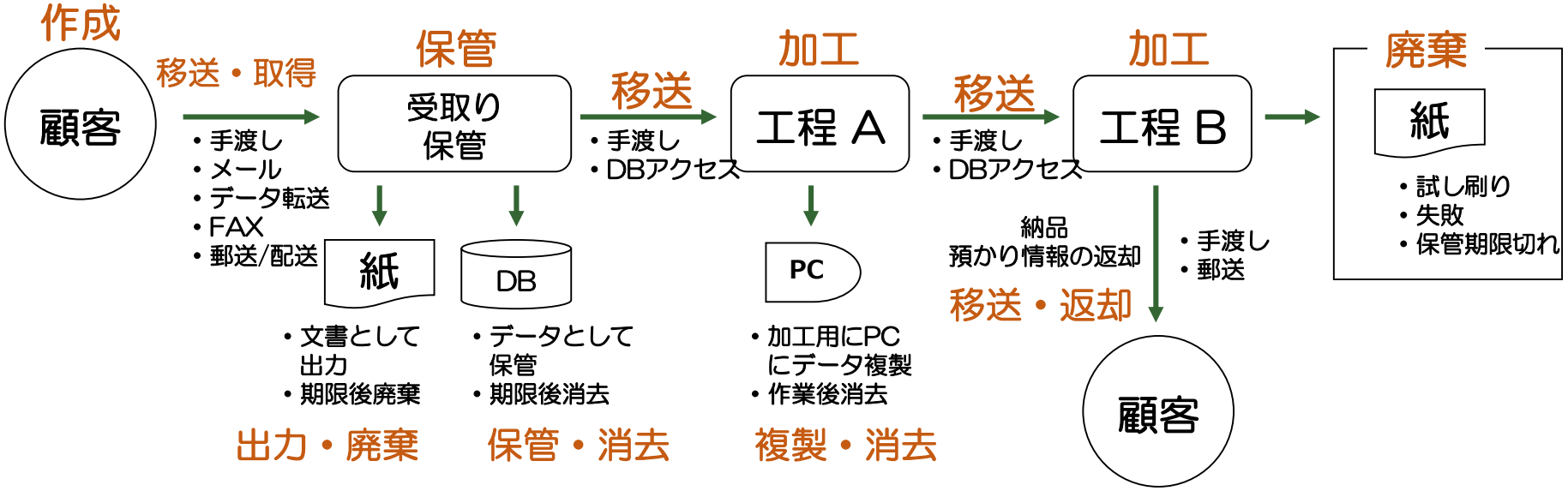
ガイド補足



業務フローに関するリスクの洗い出し・

ガイド補足

- 分析対象となる業務フローを 作成／取得、加工、複製、出力、保管、移送、廃棄／消去／返却 に分解して、業務工程毎にリスクを洗い出し、セキュリティ対策を検討する。
- 複雑な業務フローでも、また、異なる業務であっても各工程には大きな差がないことから、工程まで分解することで分析が単純化できる。



手順1：情報資産管理台帳を作成する

- 業務で利用する電子データや書類の中から、漏えいや改ざんが起きたり必要な時に利用できないと事業に影響するものや、顧客や従業員の個人情報を「情報資産管理台帳」に記入する
- 情報資産を一通り洗い出し、機密性、完全性、可用性それぞれの評価値を記入する
- 機密性・完全性・可用性の評価値から重要度を判定する

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値			重要度	保存期限	登録日	現状の状況から想定されるリスク（入力不要・自動表示）					
						個人情報	要配慮個人情報	マイナンバー	機密性	完全性	可用性				脅威の発生頻度（「脅威の状況」シートで設定）	脆弱性（「対策状況チェック」シートで設定）	被害発生可能性		リスク値	
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有		有	2	0	0	2		2016/7/1	3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	4	リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有		有	2	2	2	2		2016/7/1	2:特定の状況で発生する（年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	2	リスク中
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	2	2	1	2	7年	2016/7/1	3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	4	リスク大
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で発生する（年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	1	リスク中
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で発生する（年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	1	リスク中
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			2	2	2	2		2016/7/1	3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	4	リスク大
共通	電子メールデータ	Gmailに転送	担当者	総務部	クラウド	有			2	2	2	2		2016/7/1	3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	4	リスク大

情報資産台管理帳記入例

情報資産の洗い出しの際の疑問点

ガイド補足

- 情報資産の洗い出しは、日常的に行うことがない作業であり、初めての人は見当がつかず、解釈に戸惑うことが多い

  ＜典型的な疑問＞

  - ファイル１件づつ、帳票１枚づつ洗い出すのか
  - 電子メールは１件づつリスクを評価するのか
  - 出席者名が記載されている議事録は個人情報なのか
  - 一時的に預かっているデータは台帳に記入するのか
  - 名称が決まっていないデータや書類はどのように記入するのか

- 指導する側が手順を明確にしておく必要がある

管理台帳への入力方法

⑥ 媒体・保存先

選択：書類,可搬電子媒体,事務所PC,モバイル機器,社内サーバー,クラウド。

書類と電子データの両方を保有している場合は２行に分けて入力。

⑦ 個人情報の種類

個人情報、要配慮個人情報、マイナンバーが含まれる場合は、該当欄にそれぞれ「有」を入力。

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				保存期限	登録日
						個人情報	要配慮個人情報	マイナンバー	機密性	完全性	可用性	重要度		
①	②	③	④	⑤	⑥	⑦			⑧				⑨	⑩

①「重要度」の指定(機密性)

- 「情報資産管理台帳」シートに、以下基準を参考に評価値を入力

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	2	法律で安全管理(漏えい、滅失又はき損防止)が義務付けられている	●個人情報(個人情報保護法で定義) ●特定個人情報(マイナンバーを含む個人情報)
		守秘義務の対象として指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品･サービスに関わる非公開情報
		自社の営業秘密として管理すべき(不正競争防止法による保護を受けるため) 漏えいすると自社に深刻な影響がある	●自社の独自技術･ノウハウ ●取引先リスト ●特許出願前の発明情報
	1	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客(取引先)との商取引に関する情報
	0	漏えいしても事業に影響はない	●自社製品カタログ ●ホームページ掲載情報

①「重要度」の指定(完全性・可用性)

完全性 情報や情報の処理方法が正確で完全である	2	法律で安全管理(漏えい、滅失又はき損防止)が義務付けられている	●個人情報(個人情報保護法で定義) ●特定個人情報(マイナンバーを含む個人情報)
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	1	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	0	改ざんされても事業に影響はない	●廃版製品カタログデータ

可用性 許可された者が必要な時に情報資産にアクセスできる	2	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供しているECサイト ●顧客に提供しているクラウドサービス
	1	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ(インターネット向け事業の場合)
	0	利用できなくなっても事業に影響はない	●廃版製品カタログ

情報資産の重要度判断基準

重要度 情報資産の価値事故の影響の大きさ		
	2	機密性・完全性・可用性評価値のいずれか、またはすべてが「2」の情報資産
	1	機密性・完全性・可用性評価値のうち最大値が「1」の情報資産
	0	機密性・完全性・可用性評価値すべてが「0」の情報資産

- （重要度の算出例）
- 機密性２、完全性１、可用性０→重要度２
- 機密性１、完全性１、可用性１→重要度１
- 機密性０、完全性１、可用性０→重要度１
- 機密性０、完全性０、可用性０→重要度０

②「脅威」の指定

- 「脅威の状況」シートで、媒体・保存先ごとの脅威がどのくらいの頻度で発生する可能性があるかを「対策を講じない場合の脅威の発生頻度」欄に表示されるリストから1～3のいずれかを選択します。

社内サーバー	情報搾取目的の社内サーバーへのサイバー攻撃	3：通常の状態で発生する（いつ発生してもおかしくない）
	情報搾取目的の社内サーバーでの内部不正	2：特定の状況で発生する（年に数回程度）
	社内サーバーの故障による業務に必要な情報の喪失	1：通常では発生しない（数年に1回未満）

媒体・保存先　個別の脅威　脅威の発生頻度（1～3から選択）

具体的な手口の分析による脅威の洗い出し例

ガイド補足

- コンピュータへの侵入
  - 侵入・漏えい経路
- 不正アクセス
  - 技術的脆弱性の利用（OS、アプリ・・・）
  - アクセス権奪取(PW総当たり、デフォルトPW、ソーシャルエンジニアリング・・・)
  - 権限利用　他
- 不正プログラムの侵入
  - マルウェア感染（メール、ダウンロード、記憶媒体）
  - 開発段階での混入
  - 手入力　他
- その他
  - 業務妨害、業務外利用、システム利用不可、遅延、紛失、盗難、覗き見に結び付く脅威

脅威の要因

ガイド補足

- 洗い出したリスクの要因となる脅威を整理し、次の対策検討の材料にします。

	人的脅威		環境的脅威
	故意	偶発	
外的要因	・外部の者によるなりすまし侵入 ・外部の者による通信経路途中の盗聴 ・マルウェア	・外部の者の施設への迷い込み ・開発者のプログラムミス ・顧客の入力ミス	・地震 ・火災 ・水害 ・電源障害 ・空調障害
内的要因	・管理者による情報持ち出し ・社員による情報の改ざん ・管理者によるログの削除	・社員による不必要なアクセス行為 ・誤送信 ・移送中の情報紛失 ・誤削除 ・情報の誤廃棄	・火災 ・システム障害 ・媒体の劣化

③「脆弱性」の指定

- 「対策状況チェック」シートで55項目の「情報セキュリティ診断項目」ごとに自社における実施状況を「回答値」欄に表示されるリストから1～4のいずれかを選択します。

(6)物理的セキュリティ対策	業務を行う場所に、第三者が許可無く立入できないようにするための対策(物理的に区切る、見知らぬ人には声をかける、等)が講じられていますか？	2：一部実施している
	最終退出者は事務所を施錠し退出の記録(日時、退出者)を残すなどのように、事務所の施錠を管理していますか？	1：実施している
	高いセキュリティを確保する区域には、許可された者以外は接近できないような保護措置がなされていますか？	3：実施していない/わからない
	秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体等の持込み・利用は禁止されていますか？	4：自社に該当しない

情報セキュリティ診断項目(チェック項目)

回答値(1～3+4:該当しない)

手順2：リスク値の算定

- 手順１で洗い出した情報資産について、リスク値（リスクの大きさ）を、「重要度」と「被害発生可能性」の2つの要素の掛け合わせで算定する

リスク値 ＝ 重要度 × 被害発生可能性

被害発生可能性 ＝ f(脅威，脆弱性)

重要度 ＝ 機密性・完全性・可用性から判断
脅威　＝ 脅威がどの程度起こりうるか
脆弱性 ＝ 脅威対策がどの程度できているか

- 重要度、被害発生可能性、脅威、脆弱性は3段階の数値、リスク値は大・中・小で表す

重要度	2	事故が起きると ●法的責任を問われる ●取引先、顧客、個人に大きな影響がある ●事業に深刻な影響がある など企業の存続を左右しかねない
	1	事故が起きると事業に重大な影響がある
	0	事故が起きても事業に影響はない
被害発生可能性	3	高：通常の状況で被害が発生する（いつ発生してもおかしくない）
	2	中：特定の状況で被害が発生する（年に数回程度）
	1	低：通常の状況で被害が発生することはない

脅威	3	通常の状況で脅威が発生する（いつ発生してもおかしくない）
	2	特定の状況で脅威が発生する（年に数回程度）
	1	通常の状況で脅威が発生することはない
脆弱性	3	対策を実施していない（ほぼ無防備）
	2	部分的に対策を実施している
	1	必要な対策をすべて実施している
リスク値	4～6	大：深刻な事故が起きる可能性大
	1～3	中：重大な事故が起きる可能性有
	0	小：事故が起きても被害は許容範囲

④リスク値の算定

- 手順１の①から③を入力すると「情報資産管理台帳」シートの右側「リスク値」欄に情報資産ごとのリスク値が表示されます。リスク値に応じて以下のように対応を検討します。
  - リスク大・・・重点的に対策を実施
  - リスク中・・・対策を実施
  - リスク小・・・現状維持

現状の状況から想定されるリスク（入力不要・自動表示）					
脅威の発生頻度（「脅威の状況」シートで設定）	脆弱性（「対策状況チェック」シートで設定	被害発生可能性		リスク値	
3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	4	リスク大
2:特定の状況で発生する （年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	2	リスク中

情報資産ごとの脅威の発生頻度

情報資産ごとの脆弱性（対策状況）

情報資産ごとの被害発生可能性（高・中・低の3段階）

情報資産ごとのリスク値（大・中・小の3段階）

演習③

- グループワーク（10分）
  - 数名で、自社の情報資産のうち、「重要度」「脅威」「脆弱性」について判断が出来にくいものがないか、あるとすれば判断出来にくい要因は何かを話し合ってみましょう。

- 数グループ発表

手順3：情報セキュリティ対策を決定

- リスク値の大きいものから対策を検討し、自社に適した対策を決定します
- 対策は以下のように区分して検討する
  - リスクを低減する
    - 自社で実行できる情報セキュリティ対策を導入、ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げる
  - リスクを保有する
    - 事故が発生しても許容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持する
  - リスクを回避する
    - 仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくす
  - リスクを移転する
    - 自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げる

対策の手順

- 「情報資産管理台帳」シートの右側「リスク値」で「リスク大」と表示されたものから対策を検討します。
- 「診断結果」シートの「対策状況チェックの診断結果」の実施率が低いことでリスク値が大きくなっている可能性がありますので、実施率が低くなっている対策の種類について「対策状況」シートを見直します。

対策の種類 (情報セキュリティポリシー名称)	情報セキュリティポリシー策定の必要性	対策状況チェックの診断結果 (対策の実施率)	<ツール B> 情報セキュリティポリシーによる対策規定の要否
(1) 組織的セキュリティ対策	◎	62.5%	ポリシーで対策を規定して下さい
(2) 人的セキュリティ対策	◎	33.3%	ポリシーで対策を規定して下さい
(3) 情報資産管理	○	14.3%	ポリシーで対策を規定して下さい
(4) マイナンバー対応	○	100.0%	ポリシーで対策を規定して下さい

対策のためのリスクの原因究明

JNSA

ガイド補足

- リスクの原因は、脅威をもたらすものによって異なる。
  - 故意？ ミス？ 災害？
  - 故意による脅威は、攻撃手口も考慮する必要があります
- リスクの原因は、情報資産の特性や管理方法によって異なる。
  - 情報資産の特性：
    - 紙は燃える・破れる・装置が無くても読める
  - マネジメント的原因：
    - ルールが無い、ルールに不備がある、教育したが理解されていない、ルールが守られていない・・・
  - 技術的原因：
    - 技術的な脆弱性が放置されている、アクセス制御が不十分、属人的対策に依存・・・
  - 物理的原因：
    - 脆弱な境界、入退室制限の不備・・・
  - 人的原因：
    - 怠惰、思い込み、悪意・・・

リスク低減のための手段			
予防	防御	抑止	検知
放置するといずれ損失につながるリスクに対応すること	攻撃を防ぐこと	不正を思いとどまらせること	脅威を察知すること

情報システム環境のセキュリティ対策の例

ガイド補足

- 技術的対策の適用例
  - アクセス制御　・バックアップ
  - ネットワーク管理　・冗長化
  - モニタリング容量　・パフォーマンス管理
  - 脆弱性管理　・障害対応
- 集中と分散
  - 重要な情報とそうでない情報は分離し、重要情報は集中管理する
  - 個人情報とクレジットカード番号は隔離して管理する　等
- 業務の標準化とシステム構成の整理
  - 不正＝正常な状態ではないこと → 正常な状態の定義 → 標準化
  - 守るべき要所と監視する箇所を集約 → システム構成の整理

演習④

- グループワーク（10分）
  - 数名で、自社の情報資産のうち、重要度の高いものに対する対策方法、その対策実施基準を話し合ってみましょう。

- 数グループ発表

手順4：情報セキュリティポリシーを策定

- 決定した情報セキュリティ対策を社内の正式なルールとして文書化し、「情報セキュリティポリシー」としてとりまとめる

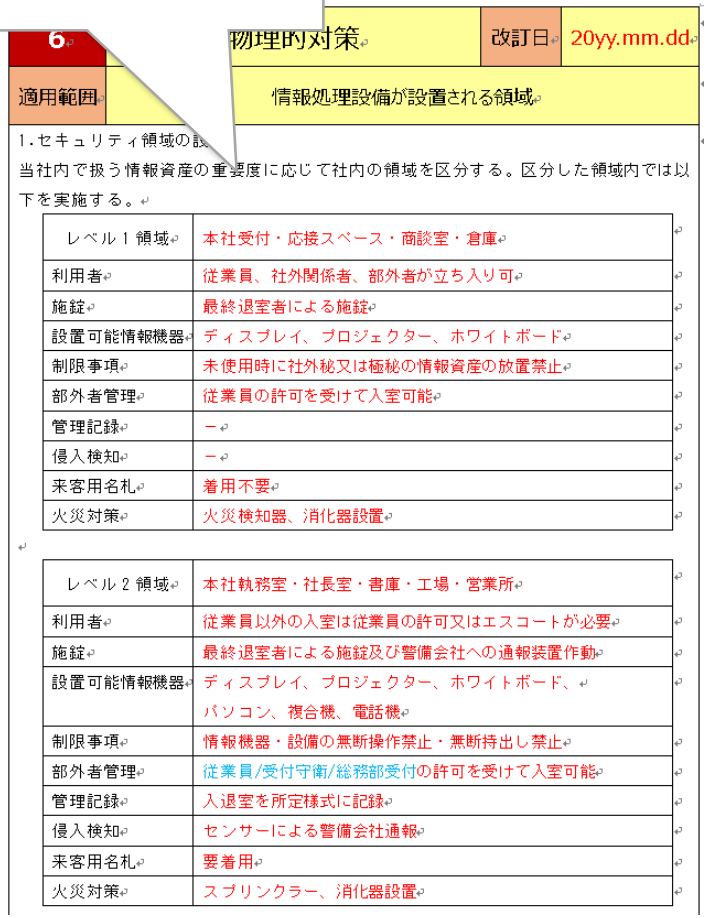
No.	情報セキュリティポリシー名称	適用条件
1	組織的対策	（原則としてすべての企業）
2	人的対策	（原則としてすべての企業）
3	情報資産管理	（原則としてすべての企業）
4	マイナンバー対応	（原則としてすべての企業）
5	アクセス制御及び認証	（原則としてすべての企業）
6	物理的対策	（原則としてすべての企業）
7	IT機器利用	（原則としてすべての企業）
8	IT基盤運用管理	（原則としてすべての企業）
9	システムの開発及び保守	社内でシステム開発を行う場合
10	委託管理	業務委託を行う場合
11	情報セキュリティインシデント対応及び事業継続管理	（原則としてすべての企業）
12	社内体制図	従業員数２名以上
13	委託契約書機密保持条項サンプル	委託先と秘密情報や個人情報等の重要な情報の授受が発生する場合

付録３で用意している情報セキュリティポリシーサンプル

自社の情報セキュリティポリシーを完成

- 「診断結果」シートに従い、「ポリシーで対策を規定して下さい」と表示された項目について、「<ツールB>情報セキュリティポリシーサンプル」を使い、自社向けに編集して、情報セキュリティポリシーを完成させます。
  - サンプルに明記されていなくても必要な対策や有効な対策があれば、追記や更新を行ってください。

編集すべき箇所を
赤字・青字で表示



6	物理的対策	改訂日	20yy.mm.dd
適用範囲	情報処理設備が設置される領域		

1.セキュリティ領域の設

当社内で扱う情報資産の重要度に応じて社内の領域を区分する。区分した領域内では以下を実施する。

レベル１領域	本社受付・応接スペース・商談室・倉庫
利用者	従業員、社外関係者、部外者が立ち入り可
施錠	最終退室者による施錠
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード
制限事項	未使用時に社外秘又は極秘の情報資産の放置禁止
部外者管理	従業員の許可を受けて入室可能
管理記録	－
侵入検知	－
来客用名札	着用不要
火災対策	火災検知器、消化器設置

レベル２領域	本社執務室・社長室・書庫・工場・営業所
利用者	従業員以外の入室は従業員の許可又はエスコートが必要
施錠	最終退室者による施錠及び警備会社への通報装置作動
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード、パソコン、複合機、電話機
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止
部外者管理	従業員/受付守衛/総務部受付の許可を受けて入室可能
管理記録	入退室を所定様式に記録
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	スプリンクラー、消化器設置

注意点：委託時の対策

- 「情報セキュリティポリシー」サンプルの「委託管理」で委託先の情報セキュリティ対策に対する評価基準を決め、「委託契約書機密保持条項サンプル」を契約書に明記する。

10	委託管理	改訂日	20yy.mm.dd
適用範囲	情報資産を取り扱う業務の委託		

1. 委託先の評価（クラウドサービスの利用を除く）
1.1 委託先評価基準
社外移又は極秘の情報資産の処理あるいは授受を伴う業務を外部の組織に委託する場合は、委託先の情報セキュリティ管理について、下記の評価基準に基づいて評価する。
（委託先評価基準）

社内管理体制	①経営者による情報セキュリティ基本方針がある。
	②情報セキュリティ管理責任者を置いている。
	③情報セキュリティ対策を定める規定等を整備している。
	④情報セキュリティ事故に対する対応手順がある。
従業員の監督	⑤全ての従業者に情報セキュリティに関する教育を実施している。
	⑥従業者から秘密保持に関わる誓約書等を取得している。
オフィス内のセキュリティ	⑦顧客の情報を扱う領域への入退室を管理している。
	⑧顧客の情報の保管について施錠管理を実施している。
情報機器・媒体の取扱い	⑨機器・媒体の盗難防止措置を講じている。
	⑩媒体の無断複製、不正持出しを防止する措置を講じている。
	⑪媒体の移送、受け渡し時の保護措置を講じている。
	⑫媒体の安全な消去、廃棄の手順を整備している。
サーバー・パソコン等の管理	⑬業務で使用するサーバー・パソコンのウイルス対策を行っている。
	⑭業務で使用するサーバー・パソコンは利用者認証機能を設定している。
	⑮業務で使用するサーバー・パソコンに利用制限等を設け管理している。

1.2 委託先の選定
評価結果に基づき委託先を選定し、情報セキュリティ責任者の承認を得る。
1.3 委託契約の締結
委託契約書には、下記に関する事項を明記する。
①当社の社外秘又は極秘の情報資産及び個人情報の守秘義務
②再委託についての事項
③事故時の責任分担についての事項
④委託業務終了時の当社が提供した社外秘又は極秘の情報資産及び個人情報の返却又は廃棄、消去についての事項

13	委託契約書機密保持条項サンプル	改訂日	20yy.mm.dd
適用範囲	委託契約の締結時		

1. 委託契約時の秘密保持契約条項
社外秘以上の機密性がある情報の処理あるいは授受を伴う業務を外部の組織に委託する場合は、契約に以下の秘密保持条項を規定するか、別途文書により合意する。

＜秘密保持契約条項サンプル＞
（甲：委託元、乙：委託先）
注：ここに示す内容は、外部委託に関する契約書における秘密保持に関する条項として示すものです。甲と乙がそれぞれ相手から秘密として提供される情報を秘密保持する義務を負う双務契約の形式としています。

第○条（秘密保持）
1. 甲及び乙は、本契約の履行にあたり、相手方が秘密である旨指定して開示する情報および本契約の履行により生じる情報（以下「秘密情報」という）を秘密として取扱い、相手方の事前の書面による承諾なく第三者に開示してはならない。ただし、次の各号のいずれかに該当する情報については、この限りではない。
①開示を受けたときに既に公知であったもの
②開示を受けたときに既に自ら所有していたもの
③開示を受けた後に自らの責によらない事由により公知となったもの
④開示を受けた後に第三者から守秘義務を負うことなく適法に取得したもの
⑤開示の前後を問わず自らが独自に開発したことを証明し得るもの
2. 甲が乙に秘密である旨指定して開示する情報は、別表１（本来では、後に例示しない）、乙が甲に秘密である旨指定して開示する情報は、別表２（本来では、後に例示しない）の通りである。なお、別表１及び別表２は甲乙協力し常に最新の状態を保つべく適切に更新するものとする。
3. 甲及び乙は、相手方より開示された秘密情報の管理につき、自ら保有する他の情報、物品等と明確に区別して管理するとともに、以下の事項を遵守する。
(1) 秘密情報の管理責任者及び保管場所を定め、善良なる管理責任者の注意をもって保管管理する。
(2) 秘密情報を取り扱う従業員を必要最小限にとどめ、上記保管場所以外へ持ち出さない。

注意点：対策の実行

- 策定した「情報セキュリティポリシー」を組織全体で役割を決めて実行する

分　類	それぞれの役割
経営者	●情報セキュリティ対策に必要な予算・人材の確保 ●情報セキュリティ方針の策定 ●管理者層への指示、目標達成状況の確認
管理者層	●部下に対するポリシーの説明 ●必要に応じたポリシーの改善 ●異常に関する監視
一般従業員	●ポリシーで定められた情報セキュリティ対策の実行

対策実行時の注意点

ガイド補足

- PDCAを回すこと
  - 実施中のセキュリティ対策の有効性や実施度を測るために定期的なチェックを行う。
  - チェック方法
    - セキュリティを評価するためには、各セキュリティ対策について“聞く”“見る”“試す”という方法を適用する。

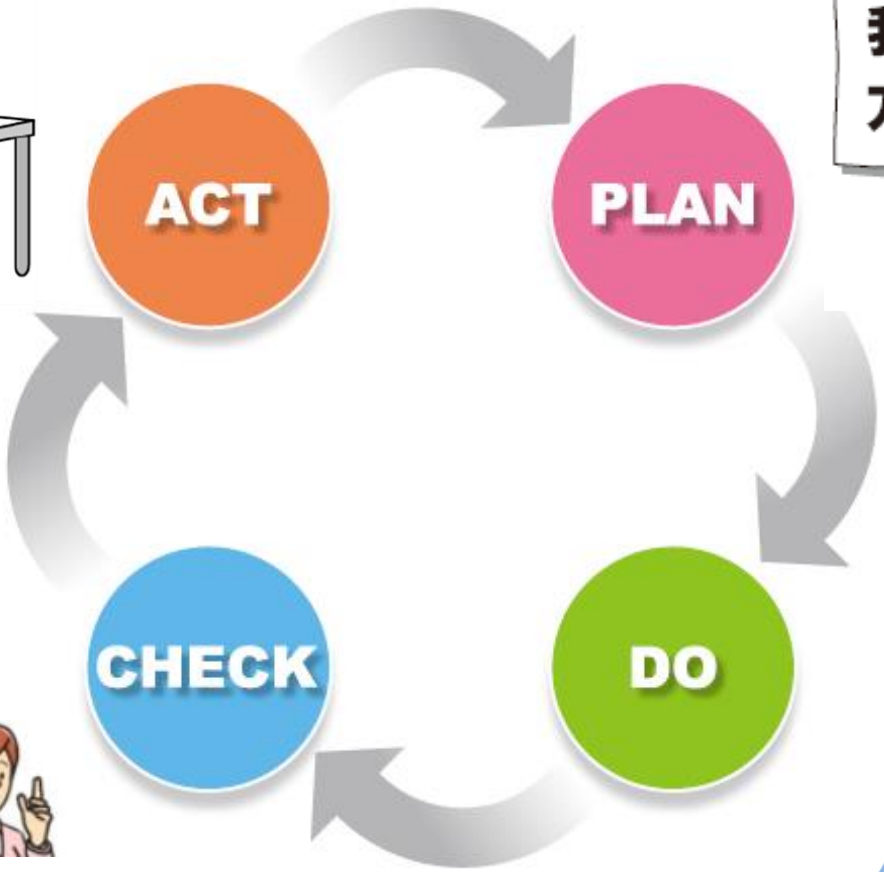
チェック方法	解　説
見る	規定文書や記録等を読む、現地の状態を見る、操作を目前で実施してもらう等により確認する方法。
聞く	関係者にセキュリティ対策の運用について口頭や文書で質問して解答を求める確認方法。
試す	チェック者自身が操作等を実施して対策の妥当性や適否を確認する方法。

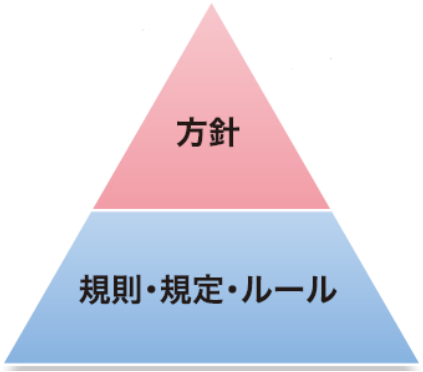
※ ひとつのセキュリティ対策に複数のチェック方法が割り当てられることがある。

改善し向上したい

Step4
改善を続ける

情報セキュリティ対策のさらなる改善に向けて





SECURITY ACTION 制度概要

- 中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度
- 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階の取組み目標を用意

1段階目（一つ星）
ガイドライン付録の「情報セキュリティ5か条」に取り組むことを宣言

2段階目（二つ星）
ガイドライン付録の「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティポリシー（基本方針）を定め、外部に公開したことを宣言

- ロゴマークをポスター、パンフレット、名刺、封筒、ウェブサイト等に無償で使用でき、情報セキュリティ対策の取組みをアピール可能
- 申込方法：申込書をメール・FAXでIPAに送付
- URL：https://www.ipa.go.jp/security/security-action/

申込受付

	申込受付	二つ星	二つ星	普及賛同企業※
申込者	**使用規約確認**	• SECURITY ACTION ロゴマーク使用規約(自己宣言事業者)		• SECURITY ACTION ロゴマーク使用規約(普及賛同企業)
	使用申込 メール/FAX	• SECURITY ACTION ロゴマーク使用申込書（新規）	• SECURITY ACTION ロゴマーク使用申込書（新規） • 5分でできる！情報セキュリティ自社診断シート※任意提出	• SECURITY ACTION ロゴマーク使用申込書（普及賛同企業） • 概要説明資料等
事務局（IPA）	**申込受付** ※申込書を受理後1～2週間	• 申込書類の内容不備確認		• 申込書類の内容不備確認
	ロゴマークの使用許諾 メール	• ロゴマークの種類、ダウンロード方法(パスワード等)を連絡		• ロゴマークの種類、ダウンロード方法(パスワード等)を連絡
申込者	**ロゴマークダウンロード**	SECURITY ACTION ★ セキュリティ対策自己宣言	SECURITY ACTION ★★ セキュリティ対策自己宣言	SECURITY ACTION ★ セキュリティ対策自己宣言　SECURITY ACTION ★★ セキュリティ対策自己宣言

※普及賛同企業は、SECURITY ACTION制度の趣旨に賛同し、当該制度の普及促進のために、ロゴマークを使用する企業

ありがとうございました。

NPO 日本ネットワークセキュリティ協会
〒105-0003
東京都港区西新橋１－２２－１２
JCビル4F
TEL：03-3519-6440
E-Mail：sec@jnsa.org