

# 2018年度 セキュリティプレゼンターカンファレンス

---

独立行政法人情報処理推進機構 (IPA)  
セキュリティセンター

## プレゼンターアップデート

1. 中小企業向け普及啓発事業
2. 新作コンテンツのご紹介

## スキルアップトレーニング

1. 情報セキュリティ対策支援サイトを  
活用した対策の始め方
2. SECURITY ACTION制度を活用した  
セキュリティ対策指導



プレゼンターアップデート

# 1. 中小企業向け普及啓発事業

# 2018年度 活動全体像



【凡例】 : 制度/インフラ : 取組み : 支援 : 参加

## 中小企業等

情報セキュリティに関心の薄い層(主に小規模企業)

対策の必要性を感じている層(主に中規模企業)

SECURITY ACTION  
自己宣言

啓発セミナー  
への参加

情報収集

地域の講習会  
への参加

具体的対策に  
関する相談

ツール活用

社内講習会  
の開催



経営者、  
セキュリティ担当者



経営者、  
セキュリティ担当者



経営者、  
セキュリティ担当者

New

啓発セミナー  
開催

団体内の  
研修会開催

セキュリティ  
関連情報周知

地域の講習会  
開催

協力団体  
／協力者



普及賛同  
企業等

New

警察／  
地域経済団体



中小企業  
支援者※2



セキュリティ  
プレゼンター

IT導入  
補助金

協議会※1

ロゴマーク  
使用申込受付

研修会/  
啓発セミナー  
への講師派遣

協議会  
開催

地域の講習会  
開催支援

プレゼンター  
カンファレンス

ガイドライン  
改訂  
ツール提供  
(ガイドライン等)

講習能力養成  
セミナー開催

SECURITY  
ACTION制度

セキュリティプレゼンター制度

対策支援  
システム



企業へ直接的な働きかけ

団体関係者の知識向上/民間協力者の育成

企業内教育担当者の育成

※1 全国商工会連合会、日本商工会議所、全国中小企業団体中央会、中小企業診断協会、全国社会保険労務士会連合会、日本税理士会連合会、日本ネットワークセキュリティ協会、ITコーディネータ協会、中小企業基盤整備機構、情報処理推進機構  
※2 経営指導員、税理士、社労士、中小企業診断士など

## ● 講習能力養成セミナーの開催

- 中小企業経営者、IT・情報セキュリティ担当者を対象とし、情報セキュリティ管理のための能力向上を目的として、地域商工団体やNPO法人などの協力のもと、国内各地域でセミナーを開催。

## ● セキュリティプレゼンターカンファレンス

- セキュリティプレゼンターの指導力向上と情報交換を目的としたカンファレンスを開催。

講習能力養成セミナー	
主催	独立行政法人情報処理推進機構
共催	2018年4～6月に各地域の共催団体を公募
開催期間	2018年7～11月
開催地	国内20か所程度
参加対象者	中小企業の経営者、IT・情報セキュリティ担当者
参加目標	1,000名(各会場50～100名程度)
開催概要	3.5時間(13:00～16:30)でセキュリティの最新動向を学ぶとともに、IPAの啓発ツールを使った社内講習会を実施できる能力を育成する

セキュリティプレゼンターカンファレンス	
主催	独立行政法人情報処理推進機構
日程	2018年6～7月(北海道、宮城、東京、愛知、大阪、広島、香川、福岡) 2018年11～12月(東京、大阪)
開催地	国内10会場
参加対象者	セキュリティプレゼンター
参加目標	360名(各会場20～80名程度)
開催概要	3時間(14:00～17:00)でセキュリティに関する支援スキルを習得し、地域における講習会講師として活動する能力を養成する

# 活動概要(2/3)

## ● 地域の講習会開催支援

- ・ 講習を行うための講習会テキストデータ及び補助教材の提供
- ・ 情報セキュリティ相談窓口の設置
- ・ 中小企業の方々に「中小企業向け情報セキュリティ対策講習会」を実施していただける方を募集

地域の講習会		開催支援	
対象となる講習会	<ul style="list-style-type: none"><li>・ 2019年2月末までに開催すること</li><li>・ 開催時間は、最低1時間以上とする</li><li>・ 参加者は、原則10名以上とする</li><li>・ 参加対象は、中小企業とする</li><li>①自社を対象とした講習会は不可</li><li>②1社のみを対象とした講習会は不可</li><li>・ 講師は、セキュリティプレゼンターとして登録したものであること</li><li>・ 参加費は無料で開催すること</li><li>・ 講習能力養成セミナーの内容もしくは教材を使うこと</li></ul>	申請方法	「セキュリティプレゼンター支援サイト」にログインし、活動告知を追加。活動告知公開後、以下の情報を事務局に連絡。 ・セミナー開催日 ・セミナー名 ・開催地 【提出先】 <a href="mailto:isec-semi-req@ipa.go.jp">isec-semi-req@ipa.go.jp</a>
職務	<ul style="list-style-type: none"><li>・ 中小企業の企業内の情報セキュリティ対策を行う経営者等に対して、講習能力養成セミナーの内容、及び教材に基づいて、講習を行うこと</li><li>・ 当日、講習会実施後、参加者にアンケートを記載してもらい、全員分を回収すること</li><li>・ 開催後1週間以内に開催報告書と回収したアンケートを提出すること</li></ul>	注意事項	<ul style="list-style-type: none"><li>・ 講習会講師と講習会申請者は同一であること</li><li>・ 参加者が10名を下回ることが予想される場合は、速やかに事務局へ連絡すること</li><li>・ 参加者には講師は含まないこと</li><li>・ 講習会実施承認後の会場変更、実施の取り下げ等の計画変更があった場合には、速やかに事務局まで連絡すること</li><li>・ 報告書は講習会終了後1週間以内に提出すること</li><li>・ 原則として申請はセキュリティプレゼンターお一人当たり1回のみとする</li></ul> ※講習会開催申請内容に不備がある場合や、申請が予定を上回った場合にはお断りすることもあります
謝金	上記職務のとおり講習会を実施し、報告書を作成・提出することに対する謝金として、3万円を支払う	開催承認通知	提出いただいた申請内容に基づいて、必要条件を確認し、数日中に開催の可否をE-mailでご連絡 ※必要に応じて電話等での開催方法等の確認を行う場合もあります

## ● 啓発セミナーへの講師派遣

- 地域の機関・団体が主催する中小企業向け啓発セミナーへ情報セキュリティ講師を派遣。

## ● 研修会への講師派遣

- 中小企業支援者を対象とした研修会へ情報セキュリティ講師を派遣。  
中小企業支援者による啓発資料配布等の啓発活動を推進。

## ● 情報セキュリティ対策支援サイト

- 中小企業の情報セキュリティ対策の向上を目的としたポータルサイト。
- 中小企業向けに無償の診断ツールやeラーニング等を提供。
- セキュリティプレゼンター向けに啓発コンテンツ等を提供。

## ● 中小企業の情報セキュリティ普及推進協議会

- **SECURITY ACTION**自己宣言につながる効果的な普及活動を協議し、中小企業における情報セキュリティの意識啓発及び自発的な対策の策定、実践の促進を図る。

- 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段階の取り組み目標を用意



セキュリティ対策自己宣言

## 1段階目（一つ星）

「情報セキュリティ5か条」に取り組むことを宣言



セキュリティ対策自己宣言

## 2段階目（二つ星）

「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



## ● 情報セキュリティ対策への取組みの見える化

- ☞ ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに印刷することで自らの取組み姿勢をアピール



## ● 顧客や取引先との信頼関係の構築

- ☞ 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに



## ● 公的補助・民間の支援を受けやすく

- ☞ SECURITY ACTIONを要件とする補助金の申請、普及賛同企業等から提供される様々な支援策が利用可能



# (参考)IT導入補助金について



**IT導入補助金 申請要件になりました**

**はじめましょう情報セキュリティ!**

**SECURITY ACTION**

SECURITY ACTION は中小企業自らが  
情報セキュリティ対策に取り組むことを  
自己宣言する制度です。

SECURITY ACTIONを宣言  
することにより、ITツール導入  
のための補助金申請が可能。

- 実施主体: 経済産業省
- 補助対象経費: ソフトウェア、クラウド利用費、導入関連経費等
- 補助金の上限額・下限額・補助率

上限額	50万円
下限額	15万円
補助率	1/2以下

- 詳細はWebサイトをご確認ください👉 <https://www.it-hojo.jp/>

プレゼンターアップデート

## 2.新作コンテンツのご紹介

# 映像で知る情報セキュリティ

<https://www.ipa.go.jp/security/keihatsu/videos/>

IPA

本日配布

- 情報セキュリティに関する様々な脅威と対策を**10分程度のドラマ**で分かりやすく解説した映像コンテンツ**11タイトル**をDVD(企業・組織向け)で提供中
- YouTube「**IPAチャンネル**」では24タイトルをいつでも試聴可能



●あなたのパスワードは大丈夫?  
～インターネットサービスの不正ログイン対策～

主な対象	ユーザー全般	形式	ナビゲーション	時間	約10分
NEW!!			内容	インターネットサービスを利用するにあたり、ログイン用のパスワード設定で注意すべきこと、更には不正ログイン対策に非常に有効な2段階認証について説明します。	
インターネット接続機器					
●あなたの家も狙われている!? 家庭教師が教えるネット家電セキュリティ対策!					
主な対象	ユーザー全般	形式	ドラマ	時間	約14分
NEW!!			内容	ネットワークカメラや無線ルーターなど家庭にあるインターネットにつながる機器の基本的なセキュリティ対策を説明します。	

# 情報セキュリティ10大脅威2018

<https://www.ipa.go.jp/security/vuln/10threats2018.html>

IPA

本日配布

- 2006年からIPAが毎年発行している資料
- 「10大脅威選考会」の投票により  
情報システムを取り巻く脅威を順位付けして解説



# 章構成

## ● 1章 情報セキュリティ対策の基本

- IoT機器の内、家庭で使われることが多い「**情報家電**」にターゲットを絞って、情報セキュリティ対策の基本を解説

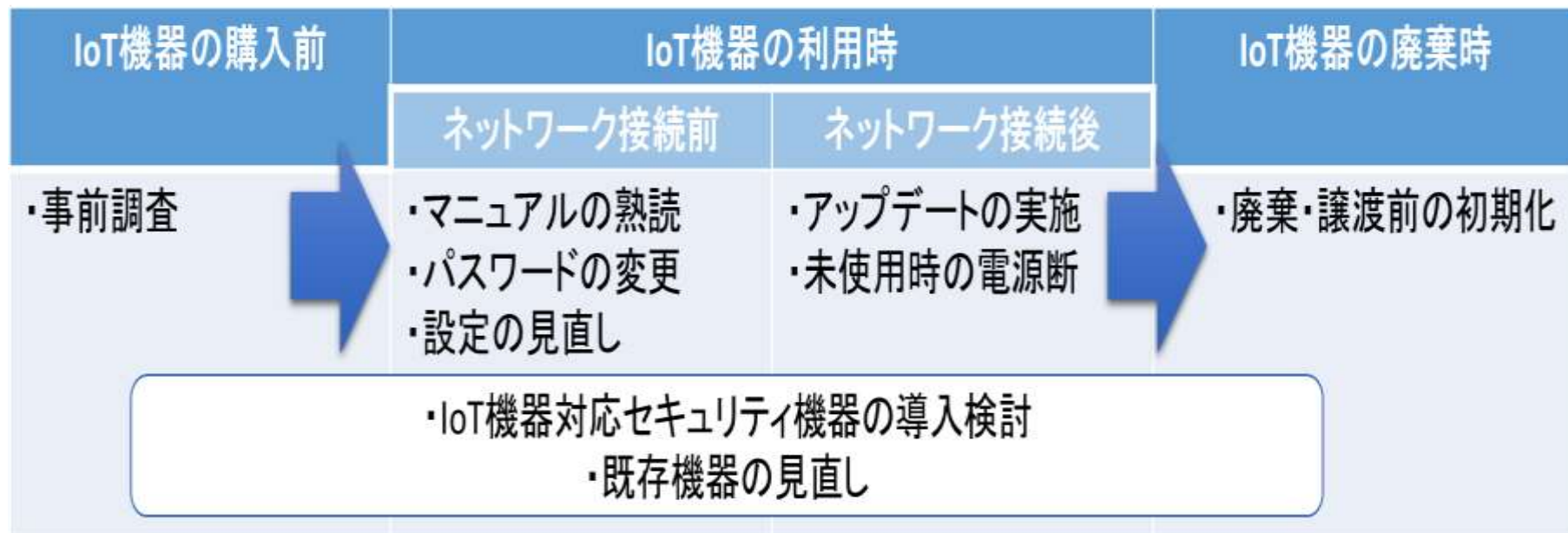
## ● 2章 情報セキュリティ10大脅威 2018

- 昨年同様、「**個人**」と「**組織**」の10大脅威を解説
- **組織内の立場を細分化**し、注意すべき脅威を整理

## ● 3章 注目すべき脅威や懸念

- 仮想通貨
- WPA2の脆弱性





### 情報セキュリティ船中ハ策 —IoT機器(情報家電)編—

- 一、事前調査  
～後悔先に立たず～
- 二、マニュアルの熟読  
～初心忘れるべからず～
- 三、パスワードの変更  
～敵に塩を送ることのなきように～
- 四、設定の見直し  
～転ばぬ先の杖～
- 五、アップデートの実施  
～善は急げ～
- 六、使用しないときは電源オフ  
～火のないところに煙は立たぬ～
- 七、廃棄・譲渡前の初期化  
～立つ鳥跡を濁さず～
- 八、IoT機器対応セキュリティ機器の  
導入検討  
～予防は治療に勝る～





# 第2章 情報セキュリティ10大脅威 2018

昨年 順位	個人の脅威	順位	組織の脅威	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	標的型攻撃による被害	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	2位
7位	ネット上の誹謗・中傷	3位	ビジネスメール詐欺による被害	ランク 外
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	4位	脆弱性対策情報の公開に伴う 悪用増加	ランク 外
4位	ウェブサービスへの不正ログイン	5位	脅威に対応するための セキュリティ人材の不足	ランク 外
6位	ウェブサービスからの個人情報の 窃取	6位	ウェブサービスからの個人情報の 窃取	3位
8位	情報モラル欠如に伴う犯罪の 低年齢化	7位	IoT機器の脆弱性の顕在化	8位
5位	ワンクリック請求等の不当請求	8位	内部不正による情報漏えい	5位
10位	IoT機器の不適切な管理	9位	サービス妨害攻撃による サービスの停止	4位
ランク 外	偽警告によるインターネット詐欺	10位	犯罪のビジネス化 (アンダーグラウンドサービス)	9位

昨年と  
同順位

新たに  
ランクイン

インターネット上のサービスを  
悪用した攻撃

ウェブサイトの改ざん、不正ログイン  
インターネットバンキングの不正利用

ランク外へ

# 【紹介】ビジネスメール詐欺注意喚起レポート IPA

← 注意喚起レポート本紙  
(BECの説明、事例と手口説明等)

← 注意喚起レポート添付資料  
(攻撃手口の詳細な説明)

注意喚起レポートの要約版  
↓ (レポート要点の説明)



BEC IPA

検索

## 第3章 注目すべき脅威や懸念

### 3.1 仮想通貨の安全性と危険性

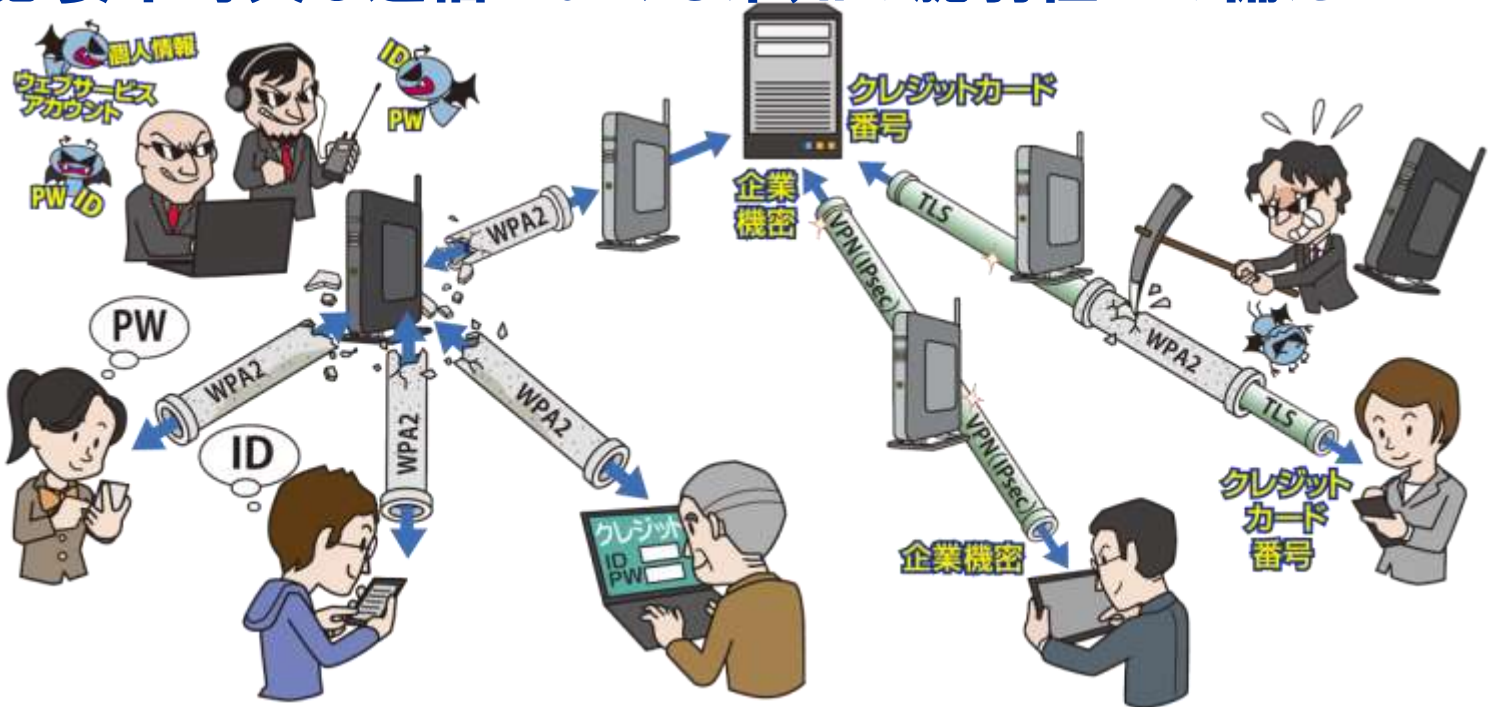
～暗号技術に基づくブロックチェーン技術の応用における脅威～



- ・仮想通貨とは何か
- ・仮想通貨の入手方法、保管方法
- ・仮想通貨交換事業者への攻撃
- ・安全性と危険性、注意すべきこと

## 第3章 注目すべき脅威や懸念

### 3.2. セキュリティプロトコルとその実装に潜む脆弱性 ～必要不可欠な通信における未知の脆弱性への備え～

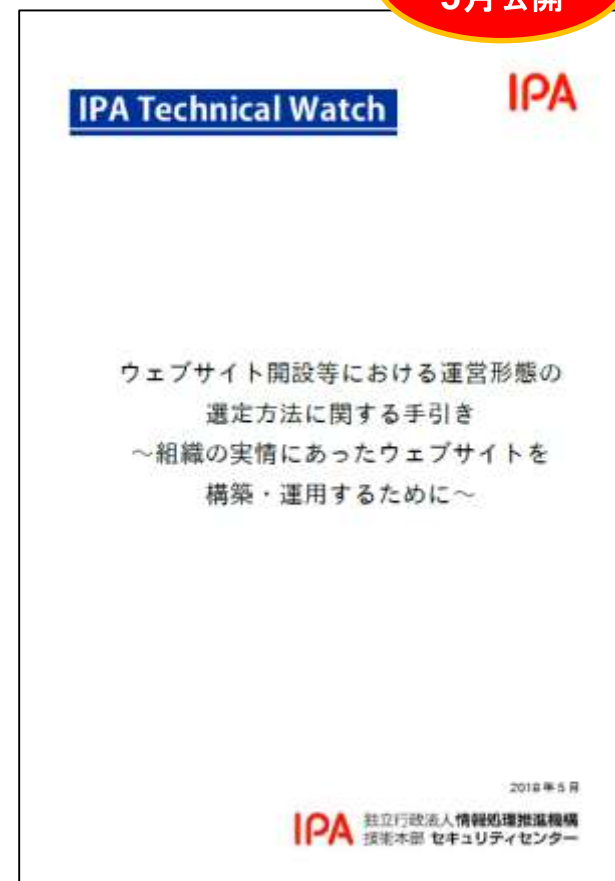


- ・WPA2に対する攻撃「KRACKs」
- ・WPA/WPA2における複数の脆弱性
- ・今後の備え: 脆弱性対策と多層防御

## ● ウェブサイト開設等における運営形態の選定方法に関する手引き

- 主に小規模事業者を対象に、ウェブサイトの新規開設、刷新において、クラウドサービスなどの運用形態別にメリット・デメリット、およびセキュリティ対策に必要な確認項目を整理

2018年  
5月公開





## ● IoT製品・サービス脆弱性対応ガイド

- ・ 制御システムを利用されている企業の皆様が、制御システムを使い続けていく上で、今後検討が必須となるセキュリティリスクを説明した資料
- ・ 具体的な対策を示した参考資料

参考1. 情報セキュリティ早期警戒パートナーシップ

参考2. パートナーシップからIoT製品の脆弱性情報が届けられた際の対応方法や注意点

参考3. 脆弱性対策情報データベース: JVN iPedia

参考4. IPA「つながる世界の開発指針」

参考5. IPA「IoT開発におけるセキュリティ設計の手引き」

参考6. IPA「つながる世界のセーフティ&セキュリティ設計入門」

参考7. IoT推進コンソーシアム・総務省・経済産業省「IoTセキュリティガイドラインver1.0」

参考8. IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

2018年  
3月公開





- 制御システムのセキュリティリスク分析ガイド  
～セキュリティ対策におけるリスク分析実施のススメ～
  - ・ 重要インフラや産業システムの基盤となっている制御システムのセキュリティを抜本的に向上させるのに重要な位置付けとなるセキュリティリスク分析を、事業者が実施できるようにするためのガイド
  - ・ ガイド別冊：制御システムに対するリスク分析の実施例
  - ・ 活用の手引き



2017年  
10月公開

## ● 2017年度

- データ利活用における重要情報共有管理に関する調査
- CISO等セキュリティ推進者の経営・事業に関する役割調査
- ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査
- 第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査
- 2017年度情報セキュリティに対する意識調査 
- 「企業のCISOやCSIRTに関する実態調査2017」報告書 

P27参照

P28参照



2017年  
12月14日  
公表

### ＜調査結果のポイント＞

- 悪意ある投稿経験者の投稿後の心理で、最も多いのは、「気が済んだ、すっきりした」で35.6%、前年比4.3%増
- 恋人など相手が非常に近い間柄であれば、「自身の性的な姿を撮影した写真や動画」をSNSで共有しても構わないと考えるスマートデバイス利用者は7.4%、PC利用者が5.3%
- 一方、「SNSで自身の性的な写真や動画を撮影して投稿した」ことを問題があると認識している回答割合57.5%であり、1割程度増加
- PCの習熟レベルが最も低い層(ITスキル標準 レベル1)で、全体平均と比較して5%～30%程度低いセキュリティ対策の実施率  
Windows Update等のセキュリティパッチ更新実施率は21.1%
- 公衆無線LANの利用率は5.0%増加し、36.5%に

2017年  
4月13日  
公表

### ＜調査結果のポイント＞

- 現在、CISOに期待されている役割、スキルは、セキュリティ偏重。セキュリティ部門と経営層をつなぐ橋渡しとしての役割は、まだ企業では認知されていない。
- 日本ではCISOが任命されている組織の割合は6割程度で、欧米と20ポイント以上の差がある。また、日本では多くのCISOが他の役職と兼任であり、専任CISOの多い欧米とは異なる。
- 日本ではCISOの半数以上(58.7%)が、セキュリティ要員(人数)は十分だと回答。一方現場では不足感が過半数。
- CSIRTを設置したものの、期待したレベルを満たしていると解釈していない日本
- 経営層の情報セキュリティへの関与は、重要インフラ企業でも6割～7割程度に留まる日本

## ● インシデント発生時の初動調査の手引き ～WindowsOS標準ツールで感染を見つける～

- 標的型攻撃における調査の全体像がわかる早見表をつけており、インシデント検知時の「感染しているかどうか」から、対策実行後の「対策の有効性」まで、どのような調査をすべきかがわかるように解説
- 標的型攻撃マルウェアの特性やOS上の留意点について解説
- 情報収集コマンドの解説に実行例を多く記載
- 実例をもとにした解説や攻撃事例と痕跡を紹介

2018年  
3月公開



# サイバーセキュリティ経営ガイドライン

参考



[http://www.meti.go.jp/policy/netsecurity/mng\\_guide.html](http://www.meti.go.jp/policy/netsecurity/mng_guide.html)

- サイバーセキュリティ経営ガイドライン Ver2.0
- 公表日:2017年11月16日(木)
- 改訂のポイント:
  - ・ 3原則を維持しつつ、重要10項目を見直し
  - ・ NISTのサイバーセキュリティフレームワークとの対応関係の提示
  - ・ 付録C「インシデント発生時に組織内で整理しておくべき事項」を追加、等

1.リーダーシップの表明と体制の構築	<経営者がリーダーシップをとった対策の推進>
(1) セキュリティポリシーの策定	セキュリティマネジメント体制の構築
(2) サイバーセキュリティリスク管理体制の構築	(1) セキュリティポリシーの策定
2.サイバーセキュリティリスク管理の枠組み決定	(2) サイバーセキュリティリスク管理体制の構築
(3) リスクの把握、対策目標と計画の策定	(3) セキュリティ対策のための資源確保
(4) PDCAの実施と対策の開示	セキュリティリスクの特定と対策の実装
(5) サプライチェーンセキュリティ対策の実施	(4) リスクの把握、対策目標と計画の策定
3.サイバー攻撃を防ぐための事前対策	(5) リスク対応策（防御・検知・分析）の実施
(6) セキュリティ対策のための資源確保	(6) PDCAの実施と対策の開示
(7) ITシステム管理の委託範囲の特定	サイバー攻撃を受けた場合に備えた体制構築
(8) 情報共有活動への参加	(7) 緊急時の対応体制の整備
4.サイバー攻撃を受けた場合に備えた準備	(8) 復旧体制の整備
(9) 緊急時の対応体制の整備	<サプライチェーンセキュリティ対策の推進>
(10) 被害発覚後の準備	(9) サプライチェーンセキュリティ対策の実施
	<関係者とのコミュニケーションの推進>
	(10) 情報共有活動への参加

新規追加項目      類似項目をマージ



# 新国家資格 「情報処理安全確保支援士」

IPA

**通称：登録セキスペ**  
**(登録情報セキュリティスペシャリスト)**

サイバーセキュリティに関する実践的な  
知識・技能を有する専門人材を育成・確保

## ①人材の質の担保

- ・「情報セキュリティスペシャリスト試験」をベースとした  
新たな試験の合格者を登録
- ・継続的な講習受講義務により、最新の知識・技能を維持

## ②人材の見える化

- ・資格保持者のみ資格名称を使用
- ・登録簿の整備・登録情報の公開(希望しない者を除く)

## ③人材活用の安心感

- ・国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務

企業における安全な情報システムの  
企画・設計・開発・運用を支援、  
サイバーセキュリティ対策の指導・助言を実施

情報処理安全確保支援士  
試験受験

登録簿へ登録  
(申請が必要)

登録情報の  
公開

資格名称の  
使用

講習受講



# 新国家資格 「情報処理安全確保支援士」



- 過去に、「情報セキュリティスペシャリスト試験」又は「テクニカルエンジニア(情報セキュリティ)試験」を合格した方が、情報処理安全確保支援士(登録セキュリティスペ)になれる申請の期日が迫っています。

**申請受付期日：2018年8月19日（日）当日消印有効**

- 期日を超えると、登録には「情報処理安全確保支援士試験」の合格が必要となります。
- 申請に必要な書類を揃える時間が必要です。早めにお手続きください。

スキルアップトレーニング

# 1. 情報セキュリティ対策支援サイトを 活用した対策の始め方



## ● 情報セキュリティ対策を、「始めたい」「強化したい」「学びたい」中小企業の方々をサポートするポータルサイト

- 5分でできる！自社診断 & ポイント学習
- セキュリティプレゼンター支援
- **SECURITY ACTION** 自己宣言者サイト





# 5分でできる！ 自社診断 オンライン版

- **5分でできる！ 自社診断**は、中小企業において実施が望まれている基本的な情報セキュリティ対策の**状況を診断できるツール**です。
- 25の質問に答えるだけで診断できます。

**自社診断**

5分でできる自社診断シート

Part 1 基本的対策

1-1 Windows Update（マイクロソフト社が提供しているウィンドウズパソコンの不具合を修正するプログラム）を行うなどのように、常にOSやソフトウェアを安全な状態にしていますか？

実施している 一部実施している 実施していない わからない

1-2 パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル（コンピュータウイルスやマルウェアとも呼ばれる）を自動更新するなどのように、パソコンをウイルスから守るために

実施している 一部実施している 実施していない わからない

1-3 パスワードは自分の名前、電話番号、誕生日など覚えやすいものを選んで複数のウェブサイトにパスワードを設定していますか？

実施している 一部実施している 実施していない わからない

1-4 ネットワーク接続の通信機やハードディスクの共有設定を必要な人だけに限定するなどのを行っていますか？

実施している 一部実施している 実施していない わからない

1-5 利用中のウェブサービス（インターネットバンキング、ソーシャルネットワークサービス、インターネット経由で利用するサービスの利用）や製品メーカーが発信するセキュリティ注意喚起や攻撃の予告を知り対策を社内共有する仕組みはできていますか？

実施している 一部実施している 実施していない わからない

新 中小企業・小規模事業者の皆様へ

**5分でできる！**

中小企業のための  
情報セキュリティ自社診断

最新動向への対応、できていますか？

脅威や攻撃の変化 IT環境の変化

ランサムウェア クラウド  
パスワードリスト攻撃 タブレット  
標的型攻撃メール スマートフォン

取り返しのつかないことになる前に  
あなたの会社のセキュリティ状況を  
「5分でできる自社診断シート」でチェック！

5分でできる！ 自社診断パンフレット

# 5分でできる！ 自社診断 オンライン版

- **診断結果に即した推奨資料と活用方法の説明が表示されます。**
- 該当資料にもすぐにアクセスでき、今後の対策に必要な**資料を探す必要はありません。**
- 5分でできる！ 自社診断の**アカウントを作成**すると、診断結果を保存することができ、過去5回分の診断結果や**全体、同業種での比較**を行うことができます。



## 推奨資料と活用方法

**推奨資料と活用方法**

診断結果に基づいて、推奨資料と活用方法を紹介します。

**推奨資料**

- **セキュリティ対策の基礎知識**：セキュリティ対策の基礎知識を学ぶための資料です。
- **セキュリティ対策の最新動向**：最新のセキュリティ対策の動向を学ぶための資料です。
- **セキュリティ対策の実践例**：実際のセキュリティ対策の実践例を学ぶための資料です。
- **セキュリティ対策のチェックリスト**：セキュリティ対策のチェックリストを学ぶための資料です。
- **セキュリティ対策のチェックリスト**：セキュリティ対策のチェックリストを学ぶための資料です。

**活用方法**

- **推奨資料のダウンロード**：推奨資料をダウンロードして、自分の環境に合わせて活用してください。
- **推奨資料の活用**：推奨資料を活用して、自分の環境に合わせて対策を実行してください。
- **推奨資料の共有**：推奨資料を共有して、他の企業や個人にも活用してもらってください。

**推奨資料と活用方法**

診断結果に基づいて、推奨資料と活用方法を紹介します。

**推奨資料**

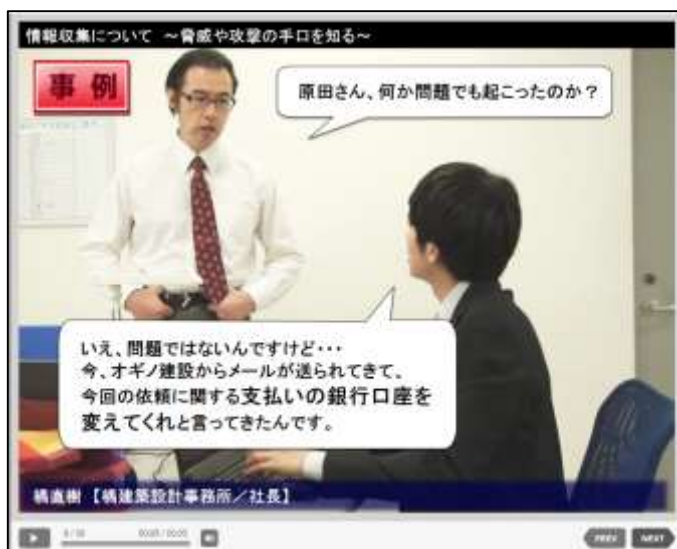
- **セキュリティ対策の基礎知識**：セキュリティ対策の基礎知識を学ぶための資料です。
- **セキュリティ対策の最新動向**：最新のセキュリティ対策の動向を学ぶための資料です。
- **セキュリティ対策の実践例**：実際のセキュリティ対策の実践例を学ぶための資料です。
- **セキュリティ対策のチェックリスト**：セキュリティ対策のチェックリストを学ぶための資料です。
- **セキュリティ対策のチェックリスト**：セキュリティ対策のチェックリストを学ぶための資料です。

**活用方法**

- **推奨資料のダウンロード**：推奨資料をダウンロードして、自分の環境に合わせて活用してください。
- **推奨資料の活用**：推奨資料を活用して、自分の環境に合わせて対策を実行してください。
- **推奨資料の共有**：推奨資料を共有して、他の企業や個人にも活用してもらってください。

# 5分でできる！ポイント学習

- **5分でできる！ポイント学習**は、中小企業で働く方を対象とした、1テーマ5分で情報セキュリティについて勉強できる**学習ツール**です。
- 職場での日常ひとコマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら**正しい対処法を学ぶ**ことができます。



事例



正しい対処法

# 5分でできる！ポイント学習

- 学習後にはその内容に関する確認テストを用意しています。
- テスト結果を確認することで、学習の**理解度をチェック**できます。
- 5分でできる！ポイント学習の**アカウントを作成**すると、都合の良いタイミングで学習の中断・再開ができ、これまでの学習進捗状況を表形式で確認することができます。
- コース内の確認テストに全て正解した場合は、「**修了証**」を**発行**できます。

【確認テスト】 No.5

Q1 ☒ 正解

次のセキュリティ対策について、適切なのはどれが答えなさい。

正答	回答	選択肢
		テレビニュースなどで注意喚起していた詐欺メールが、会社のメールアドレスに届いたので、直ぐに削除した。
		取引先から添付ファイル付きのメールが届いたが、身に覚えがないので、メール内に書かれていた連絡先に確認のメールを送った。
<input checked="" type="radio"/>	<input checked="" type="radio"/>	利用しているインターネット/バンキングから、新たな詐欺メールの注意喚起メールが届いたので、会社内や家族内で情報を共有した。

解説

詐欺メールなどの攻撃や犯罪の手口を事前に知っていることで、被害に遭いづらくなります。情報の収集元として、IPA が公開している「安心相談窓口だより」や、官公庁やセキュリティ企業が公表しているレポートが参考になります。定期的に情報を収集し、社内や家族、知り合いの中で情報を共有し、被害に遭わないように備えておきましょう。もしその様なメールが届いたら、勝手に削除したり、送り主に連絡をするのではなく、システム管理者の指示に従い、適切に対処しましょう。





# 普及啓発コンテンツの提供



## 普及啓発コンテンツ

### 概要

- ・普及啓発コンテンツは、セキュリティプレゼンター登録された方が利用可能な、情報セキュリティ普及のためのツールです。地域の講習会開催やご自身の学習用としてご利用ください。
- ・「署名なし」ボタンを選択すると、セキュリティプレゼンターの情報が印字されずにダウンロードされます。署名印刷を希望される場合は、「署名入り」ボタンを選択してください。（「署名入り」が作成できる資料に有効な指定です）

◀前 1 2 3 次▶  
(1-10/26)

登録件数 26件

コンテンツ名：	セキュリティプレゼンターカンファレンス2017②	ダウンロード：
コンテンツ説明：	2018/3/12開催時の講演資料（抜粋版）です。	署名なし
アップロード日：	2018-04-03 13:39:31	
コンテンツ名：	映像で知る情報セキュリティ「陽だまり家族とパスワード～自分を守る3つのポイント～」(PowerPoint版)	ダウンロード：
コンテンツ説明：	映像で知る情報セキュリティ「陽だまり家族とパスワード～自分を守る3つのポイント～」の講習会テキストのPowerPoint版です。解説ノート付です。改編して講演する場合にご利用ください。	署名なし
アップロード日：	2017-12-27 16:57:43	
コンテンツ名：	映像で知る情報セキュリティ「あなたの書き込みは世界中から見られてる～適切なSNS利用の心得～」(PowerPoint版)	ダウンロード：
コンテンツ説明：	映像で知る情報セキュリティ「あなたの書き込みは世界中から見られてる～適切なSNS利用の心得～」の講習会テキストのPowerPoint版です。解説ノート付です。改編して講演する場合にご利用ください。	署名なし
アップロード日：	2017-12-27 16:25:36	

- 活動地域や保有資格などを条件にセキュリティプレゼンターを検索することができます
- 2018年3月以前に登録の方は、新システム移行後の登録情報の確認・編集をお願いします

### セキュリティプレゼンター詳細

ログインID  
パスワード  
ログイン  
(パスワードを忘れた方はこちら)

アカウントを申請したい方  
セキュリティプレゼンター登録申請  
セキュリティプレゼンターへの参加  
メニュー

項目	値
氏名	相田 アイビー
氏名(フリガナ)	アイビー 相田
氏名(フリガナ)	アイビー 相田
プレゼンター写真	
活動地域	東京都、埼玉県、神奈川県、千葉県
生年月日	
メールアドレス	ipa@ipa.go.jp
所属機関	113-0591
郵便番号	東京都
〒郵便局/郵便	東京都本郷3-20-8
住所	東京都目黒区センタービル

所属情報-1	
所属組織名	株式会社安全支援
所属組織名(カナ)	カブシキガイシャアンゼンシエン
部署	情報セキュリティ支援部
役職	情報セキュリティコンサルタント
連絡先電話番号	03-5978-7508
連絡先住所	東京都文京区本郷3-20-8
連絡先メールアドレス	ipa@ipa.go.jp
主要取得資格	情報セキュリティスペシャリスト試験 ITコーディネータ
その他の取得資格	情報処理安全確保支援士、システム監査技術者、公認情報システム監査人(CISA)、ISMS審査員、QMS審査員、ITコーディネータ、知的財産管理技能士
自己PR	情報セキュリティ関連に關する支援、監査等を中心に活動しています。
受講研修履歴	5分で出来る「情報セキュリティ会社診断」 5分で出来る「情報セキュリティポイント学習」

- 活動告知を登録し、承認されるとTOPページに掲載されます

Home > セキュリティプレゼンター支援TOP

## セキュリティプレゼンター支援

ログイン

ログインID

パスワード

ログイン

[パスワードを忘れた方はこちら](#)

活動告知

一覧を見る

セキュリティプレゼンターのセミナー情報等をご紹介します。  
注意：記載されている告知は、セキュリティプレゼンターからの申請をそのまま掲載している情報であり、IPAが開催等に関して責任を負うものではありません。問い合わせ等については、直接セキュリティプレゼンターにお問合せ下さい。

開催日	セミナー名	開催地	講師
2018年06月04日	情報セキュリティ対策の基本	神奈川県	田中 孝典
2018年06月14日	<a href="#">サイバーセキュリティ対策セミナー</a>	京都市	吉村 浩明
2018年06月14日	情報セキュリティ対策セミナー	大阪府	山中 多佳子

- 活動実績を登録し、承認されるとプレゼンター詳細画面に掲載されます
  - ・ 活動分類は、セミナー開催/セミナー受講/ちらし配布/事例提供/アンケート

スキルアップトレーニング

## 2. SECURITY ACTION制度を活用した セキュリティ対策指導



# 中小企業の 情報セキュリティ対策と指導のポイント

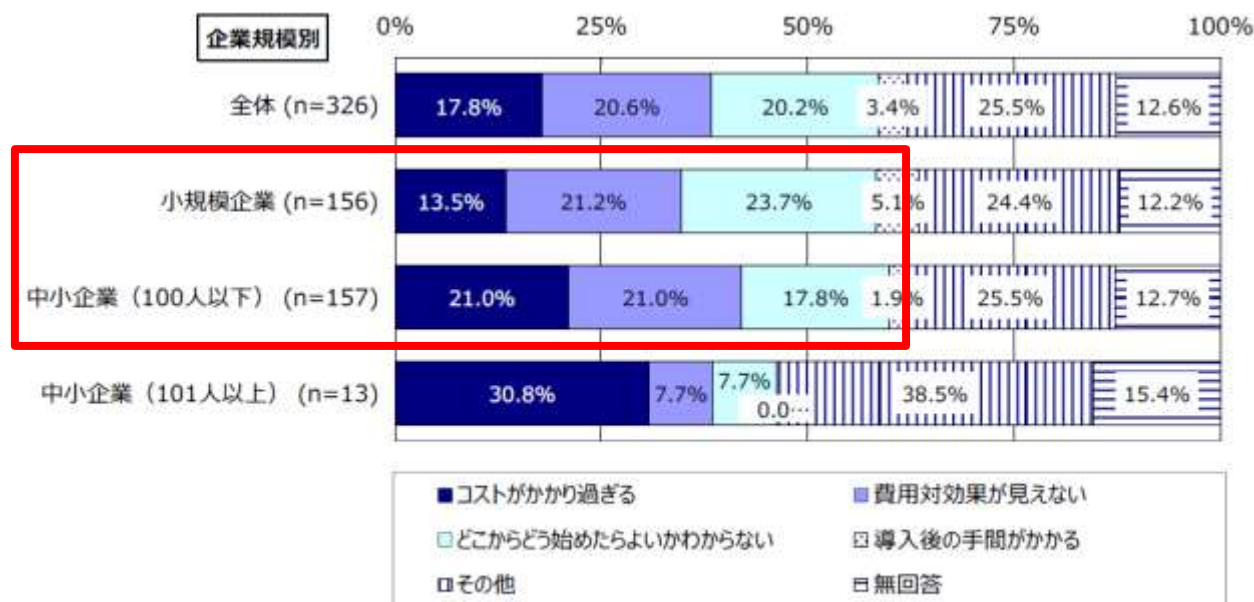


図 2-86 情報セキュリティ対策が含まれない理由（企業規模別）  
（IPA「2016年度中小企業における情報セキュリティ対策の実態調査」から）

■理由1 コストがかかり過ぎる ➡ 少ないコストでも可能な対策

■理由2 費用対効果が見えない ➡ 組織の脅威に対して効果的な対策

■理由3 どこからどう始めたらよいかわからない ➡ 組織に合った段階的な取組み

中小企業の情報セキュリティ対策ガイドラインに沿った取組みから始める

- 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」、経営者がやらなければならない「重要7項目の取組」を記載
  - 情報セキュリティ対策の具体的な進め方や実施、改善について手順を分かりやすく説明
  - **SECURITY ACTION**の取組みを支援するツールをCDに収録



# 情報セキュリティ対策ガイドラインと SECURITY ACTION の位置づけ

- 「中小企業の情報セキュリティ対策ガイドライン」に従って取組みます

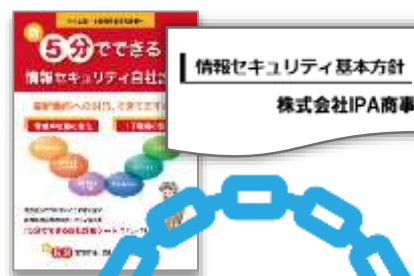
## Step1 まず始める



セキュリティ対策自己宣言

情報セキュリティ5か条

## Step2 現状を知り改善する



セキュリティ対策自己宣言

自社診断＋  
情報セキュリティ基本方針

## Step4 改善を続ける

## Step3 本格的に取り組む





セキュリティ対策自己宣言

# 1段階目（一つ星）

**「情報セキュリティ5か条」に取り組むことを宣言する**

企業の規模に関わらず、必ず実行していただきたい  
重要な対策を5か条にまとめています。

# 情報セキュリティ5か条

- 一つ星を使用するには、「情報セキュリティ5か条」に取り組むことを宣言

## 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！
- 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！

中小企業・小規模事業者の皆様へ

### 情報セキュリティ **5** か条

ウチには秘密なんかないなあ...

いいえ、こんな情報があるはずですよ!

- 従業員のマイナンバー、住所、給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り値や取引実績
- 新製品の設計図などの開発情報
- 取引先から“取扱注意”として預かった情報

サイバー攻撃といっても、被害など知っているのでは?

漏れたら大変! こんなダメージが!

- 被害者への損害賠償などの支払い
- 取引停止、顧客流出
- ネットの遅延などによる生産効率のダウン
- 従業員の士気低下

情報セキュリティ対策と言っても、何をすれば良いのかわからない組織では、裏面の5か条を守るところから始めてみましょう。

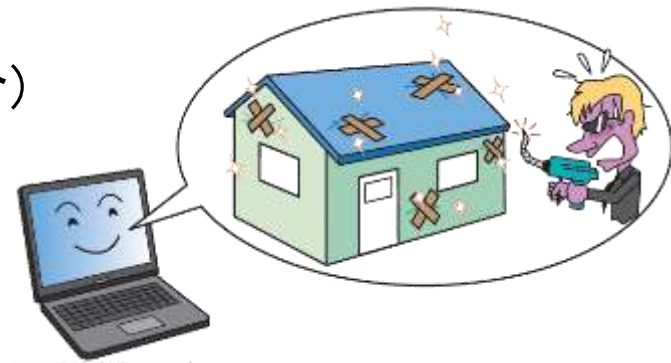
裏面をご覧ください

# 1 OSやソフトウェアは常に最新の状態に

- 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

- 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)を導入する



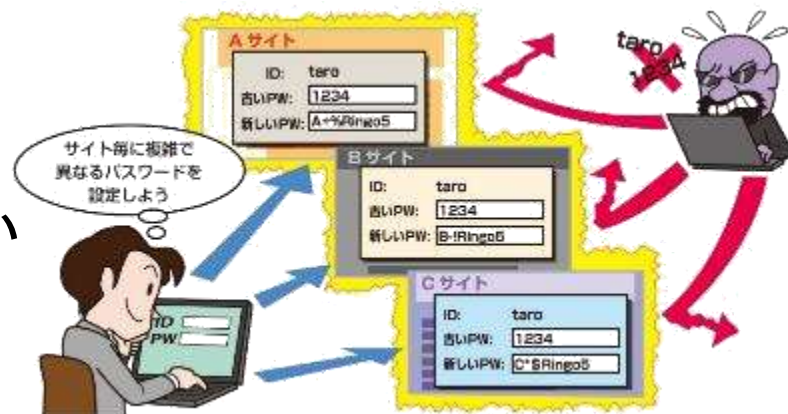


### 3 パスワードを強化

- 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」「使い回さない」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長い文字数にする
- ・ 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

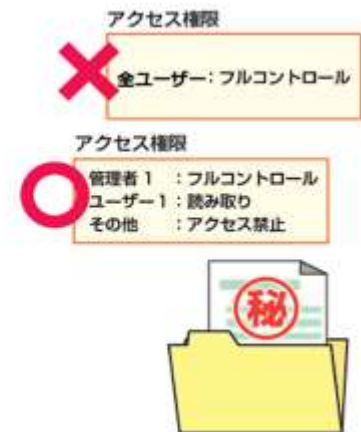


## 4 共有設定を見直す

- 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る

- 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し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しましょう。

### ＜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



# グループディスカッション：一つ星宣言

社長から以下の依頼がありました。  
セキュリティプレゼンターとしてどのように対応すべきか  
グループで意見交換してください。


わが社では、IT導入補助金の申請とあわせてSECURITY ACTION一つ星を宣言した。「情報セキュリティ5か条」を社員に配付したところ、社員から質問があった。私には答えることができないので、指導して欲しい。




# グループディスカッション：社員からの質問

以下の質問に対してグループで意見交換してください。

**1** OSやソフトウェアは常に最新の状態にしよう！

 自分のパソコンのOSやソフトウェアが最新の状態かどうか、どうしたら分かりますか？


**2** ウイルス対策ソフトを導入しよう！

 無償のウイルス対策ソフトを使っていますが、それではいけないのですか？

**3** パスワードを強化しよう！

 「パスワードの強化」とは、具体的にどのようなパスワードを使えば良いのですか？

**4** 共有設定を見直そう！

 わが社で共有設定を実施している機器やサービスとして具体的にどのようなものがあるのですか？

**5** 脅威や攻撃の手口を知ろう！

 社内にセキュリティに詳しい人がいないのですが、どうしたら良いのですか？

# 情報セキュリティ5か条は 10大脅威にも有効な対策！！

- 「10大脅威」の順位は毎年変動するが、  
基本的な対策の重要性は長年変わらない

## 情報セキュリティ**5**か条

順位	組織の脅威	ソフトウェア の更新	ウイルス 対策ソフト	パスワード の強化	設定の 見直し	手口を 知る
1位	標的型攻撃による情報流出	○	○		○	○
2位	ランサムウェアによる被害	○	○		○	○
3位	ビジネスメール詐欺	○	○	○		○
4位	脆弱性対策情報の公開に伴い 公知となる脆弱性の悪用増加	○	○			○
5位	セキュリティ人材の不足	—	—	—	—	—
6位	ウェブサービスからの個人情報の 窃取	○	○	○	○	○
7位	IoT機器の脆弱性の顕在化	○				○
8位	内部不正による情報漏えい				○	○
9位	サービス妨害攻撃による サービスの停止				○	○
10位	犯罪のビジネス化 (アンダーグラウンドサービス)	○	○	○	○	○

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！

凡例：○ 対策効果あり、または、部分的に効果あり





セキュリティ対策自己宣言

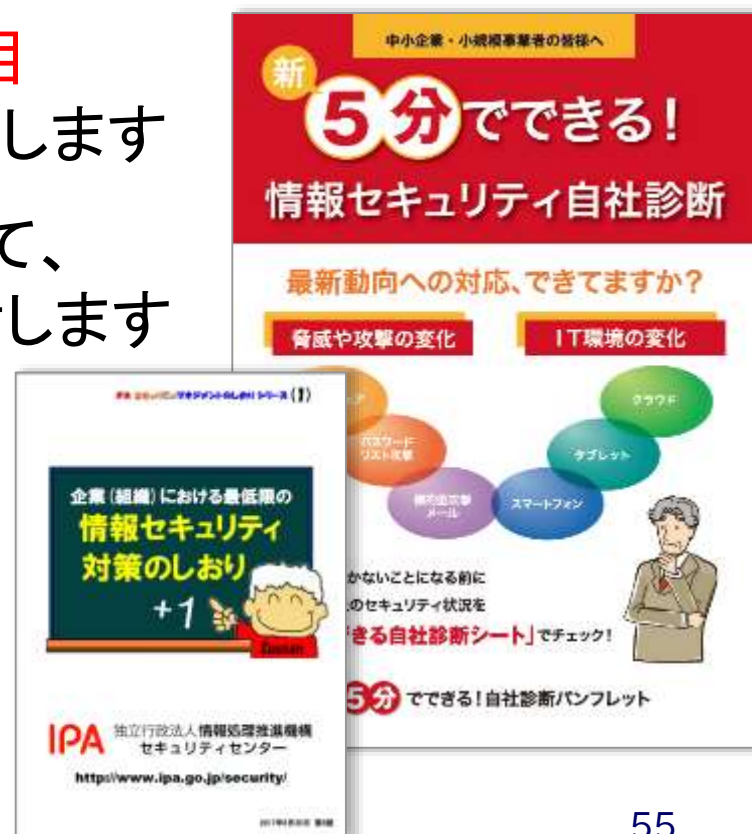
## 2段階目（二つ星）

**「5分でできる！情報セキュリティ自社診断」を実施し、  
「情報セキュリティポリシー（基本方針）」を定め、  
公開したこと宣言する**

あまり費用をかけることなく、実行することで効果がある  
情報セキュリティ対策を25項目に絞り込んだものです。

# 5分でできる！情報セキュリティ自社診断IPA

- 二つ星を使用するには、まず  
「**新** 5分でできる！情報セキュリティ自社診断」で  
自社のセキュリティ状況を把握します
  - ・ **セキュリティ対策に関する25項目**  
に答えて、自社の問題点を把握します
  - ・ **パンフレット**や**しおり**を参考にして、  
不足している対策の導入を検討します
  - ・ 対策を社内で周知するために、  
「**情報セキュリティハンドブック**  
**ひな型**」を活用できます



- あまり費用をかけることなく、実行することで効果がある絞り込んだ25項目の情報セキュリティ対策

## ☑ 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  
※情報セキュリティ5か条と同じ

## ☑ 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

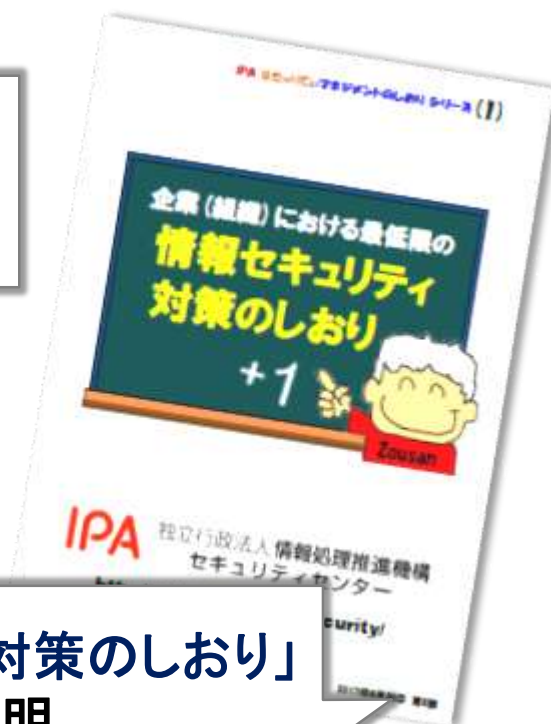
[illegible]

# 5分 できる！情報セキュリティ自社診断 対策の決定

- 実施できていなかったり、実施状況にバラツキがある項目は、パンフレット等を参考に、対策を決定します



「パンフレット」  
診断項目解説  
対策例紹介



「情報セキュリティ対策のしおり」  
詳しく説明

**5分** できる！情報セキュリティ自社診断

# 情報セキュリティハンドブックの作成

- 情報セキュリティハンドブック(ひな形)を編集して、対策をルール化します

「情報セキュリティハンドブックひな形」

修正する箇所は**赤字**

選択する箇所は**青字**

## 情報セキュリティ ハンドブック (ひな形)

ハンドブックの使い方

本ハンドブック(ひな形)は、従業員に配付し自社のセキュリティルールを定めてもらうためのものです。5分でできる！情報セキュリティ自社診断に準拠しています。赤字で記載した箇所は編集例になりますので、自社のルールにあわせて赤字を中心に変更し、また必要に応じて項目を追加して、ご利用ください。

株式会社〇〇〇〇

自社用に編集

## 情報セキュリティ ハンドブック

株式会社IPA商事

3-3 従業員のみなさんへ

従業員の方へ

3-2 全社共通のルール

全社共通のルール

3-1 全社共通のルール

全社共通のルール

2-5 仕事中のルール

仕事中のルール

2-4 仕事中のルール

仕事中のルール

第1版



# 基本方針の策定・公開

- 「ツールB 情報セキュリティポリシーサンプル」を参考にするなどして、セキュリティポリシー（基本方針）を策定・公開します

中小企業の情報セキュリティ対策ガイドライン 付録3 <ツールB>

### 情報セキュリティポリシーサンプル

本ツールは、中小企業向けの情報セキュリティポリシーのサンプルです。各社に合わせたサンプルを制作し、自社で実施する情報セキュリティ対策に活用してください。

※本ツールは、自社の事情に合わせた内容（削除、追加等）に必要に応じて編集は、自社の事情に合わせた内容にしてください。

目次
1 組織的対策（基本方針）
2 組織的対策
3 人的対策
4 情報資産管理
5 マイナンバー対応
6 アクセス制御及び認証
7 物理的対策
8 IT設備利用
9 IT設備運用管理
10 システム開発及び保守
11 委託管理
12 情報セキュリティインシデント対応及び事業継続管理
13 社内統制
14 委託契約書機密保持条項サンプル

## 自社用に編集

### 株式会社IPA商事

お取引サービス  
Sales Service

お問い合わせ  
Inquiry

会社情報  
Company Information

---

#### 情報セキュリティ基本方針

会社情報のご案内について

##### 情報セキュリティ基本方針

当社は、人財育成事業を中心としてお客様のニーズに応えてきました。今後も、お客様にご満足いただけるサービスを提供するために、高度情報社会における情報資産を適切・迅速・正確などの観点から守り、お客様ならびに社会の信頼に堪えるべく、情報セキュリティ基本方針を定め、自社の情報セキュリティに対する取り組みの根拠といたします。

- 1. 社内体制および情報セキュリティポリシーの整備**  
当社は、セキュリティの維持及び改善のために必要と判断する体制、技術等を適切に整備し、情報セキュリティの正式な規程として定めます。
- 2. リーダーシップにおける責任および継続的改善**  
当社の経営者は、本方針の策定により、当社及びお客様の利益を守るために、情報セキュリティの維持及び改善の責任を負います。
- 3. 法令、契約上の要求事項の遵守**  
当社の経営者は、事業活動に利用する情報資産に開示する法令、規制、規範及びお客様との契約上のセキュリティ要求事項を遵守します。
- 4. 従業員への教育**  
当社の経営者は、情報セキュリティの維持及び改善のために必要と判断、技術等を適切に整備し、情報セキュリティの正式な規程として定めます。
- 5. 委託契約書機密保持条項の整備**  
当社は、情報セキュリティに関する法令、規制、規範及びお客様との契約に開示する規定が適切でセキュリティ要求への対応のための体制を整備し、適正及び適切な体制を整備します。

●●●●●●●●  
株式会社○○○  
代表取締役社長 田中 一郎

ツールB 情報セキュリティポリシーサンプル

ホームページで公開



# 情報セキュリティポリシー（基本方針）サンプル

- 基本方針は、取引先・顧客の期待や、事業における必要性を考慮して策定しましょう

## <情報セキュリティ基本方針サンプル>

当社は、●●事業を中核としてお客様のニーズに応えてきました。今後も、お客様にご満足いただける製品・サービスを提供するために、高度情報化社会における情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、情報セキュリティ基本方針を定め、当社の情報セキュリティに対する取り組みの指針といたします。

### 1. 社内体制および情報セキュリティポリシーの整備

当社は、セキュリティの維持及び改善のために必要な管理体制を整備し、必要な情報セキュリティ対策を社内の正式な規則として定めます。

### 2. リーダーシップにおける責任および継続的改善

当社の経営者は、本方針の遵守により、当社及びお客様の情報資産が適切に管理されるよう主導します。

### 3. 法令、契約上の要求事項の遵守

当社の従業員は、事業活動で利用する情報資産に関連する法令、規制、規範及びお客様との契約上のセキュリティ要求事項を遵守します。

### 4. 従業員の取組み

当社の従業員は、情報セキュリティの維持及び改善のために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

### 5. 違反及び事故への対応

当社は、情報セキュリティに関わる法令、規制、規範及びお客様との契約に関わる違反及び情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響を低減します。

（出典）IPA「中小企業の情報セキュリティ対策ガイドライン」  
情報セキュリティポリシーサンプル（CD-ROMに収録されています。）

○年○月○日  
株式会社○○○○  
代表取締役社長 ○○○○

# 社内展開例

- ハンドブックの印刷配付や、社内ポータルに掲示する
- 説明会などを実施して、実践を促す



# ケース演習：二つ星宣言に向けたアクションIPA

一つ星を宣言した企業が二つ星を目指すことになり、社長から支援を依頼されました。  
セキュリティプレゼンターとしてどのように支援すべきか、グループでまとめてください。

## 【依頼企業の概要】

企業名：株式会社IPAサービス  
所在地：東京都文京区  
従業員：10名  
          営業3名 制作5名 事務2名  
          ※IT担当者不在  
業 種：広告代理業  
現在の取組み段階：一つ星

## 【依頼企業の状況】

- 取引先からセキュリティ対策の要求があった
- 情報セキュリティポリシー（基本方針含む）は未整備
- 自社診断の実施結果：70点  
特に「組織としての対策」の点数が低い  
→従業員の意識付け、会社のルールなど

# ケース演習：二つ星宣言に向けたアクションIPA

二つ星宣言の進め方を社長に説明するための簡潔なアクションプランを作ってください。

## 例

何を	いつ	誰が	どのように
情報セキュリティ基本方針の策定	7月中	社長	ガイドライン付録の基本方針をもとに、依頼企業の取引先・顧客を考慮して策定



[事務局・発行]独立行政法人情報処理推進機構(<https://www.ipa.go.jp/>)

〒113-6591 東京都文京区本駒込2丁目28番8号

文京グリーンコートセンターオフィス

テキストに関してのお問合せ:[isec-semi@ipa.go.jp](mailto:isec-semi@ipa.go.jp)

2018年6月初版発行