中小企業いばらき

CONTENTS

September

9

2022 No.767

クローズアップ

中小企業の情報セキュリティ対策ガイドラインの概要

写真　茨城県遊技業協同組合
（写真紹介、組合紹介記事は表紙裏ページに掲載）

発行　茨城県中小企業団体中央会　https://www.ibarakiken.or.jp/
〒310-0801　水戸市桜川2-2-35　電話029-224-8030（代）

表紙の紹介

業界の未来を見据えた改革を推進
～社会貢献活動で地域社会との共存～

茨城県遊技業協同組合

茨城県遊技業協同組合（平文暉朗理事長）は、昭和55年、県内のパチンコホールの健全経営の推進と組合員の経済的地位の向上を目的に設立。

レジャー白書2021によると、国内のパチンコ・パチスロの市場規模（貸玉、貸メダル料金の累計額）は、コロナ禍の影響もあり、パチンコ業界への参加人口、市場規模ともに減少し続け、とりわけ参加人口は、過去最低の710万人と厳しい状況が続いている。

このような中、同組合では、遊技人口を回復するためのファン感謝デーの開催のほか、のめり込みや依存防止対策など遊技が過度にならないような予防対策にも尽力している。

また、コロナ対策においても、同業界からクラスターを発生させないという強い決意の下、「パチンコ・パチスロ店営業における新型コロナウイルス感染症の拡大予防ガイドライン」を基に、業界ぐるみで感染防止対策に努めている。

そして、同組合では地域社会との共存を図り、パチンコ・パチスロ遊技が国民から親しまれ、幅広い客層から支持される大衆娯楽となるよう、様々な社会貢献活動に取り組んでいる（以下参照）。

○昨年９月、組合員の従業員やその家族、また県内外の企業・団体等にも希望を募り、コロナワクチンの職域接種を実施［表紙写真：左上］。その活動が評価され、ひたちなか商工会議所から顕彰表彰（特別賞）を受賞［表紙写真：右上］。また、一般社団法人パチンコ・パチスロ社会貢献機構の第17回社会貢献大賞で、都道府県部門の最優秀賞を受賞した。
○茨城新聞社主催の第47回県選抜中学野球大会に協賛金を贈呈。同大会閉会時の表彰式で組合役員が選手にメダルを授与した［表紙写真：左下］。
○その他、日頃から地域の防犯対策、青少年の健全育成活動に尽力。社会福祉事業へも支援している。

同組合では、厳しい経営環境下にあるからこそ、これまでの業界のあり方を抜本的に見つめ直し、業界の未来を見据えた改革を実行していくとしている。

特集 クローズアップ

中小企業の情報セキュリティ対策ガイドラインの概要

近年、大企業のみならずサプライチェーンを構成する中小企業においてもサイバー攻撃の脅威に晒されている実情が明らかになっています。

最近の事案からも、業種や事業規模を問わず中小企業もサイバー攻撃や不審なアクセス等の脅威に晒されているといえます。

そして、もし被害に遭ってしまった場合には、数千万円の損害が発生してしまうおそれがあり、自社のみならず取引先も含めて操業が停止してしまうおそれもあります。

また、日々サイバー攻撃の高度化・巧妙化が進む中で、サプライチェーン全体におけるサイバーセキュリティ対策の強化も求められています。

このような中、中小企業においてもサイバーセキュリティ対策の実施、強化が求められていますが、中小企業では情報セキュリティ対策に関する知識やノウハウが十分でないことから、独立行政法人情報処理推進機構（IPA）は、『中小企業の情報セキュリティ対策ガイドライン』を作成し、公開しており、本号では、本ガイドラインの概要（経営者編）を紹介します。詳細は以下ウェブサイトをご確認いただき、情報セキュリティ対策を推進してください。

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

情報セキュリティ対策ガイドライン　検　索

当会といたしましても、セミナー等の開催や専門家派遣事業などを通じて、組合等や中小企業の情報セキュリティ対策のお手伝いをいたします。

はじめに　『経営者の皆様へ』

本ガイドラインは、中小企業の皆様に情報を安全に管理することの重要性について認識いただき、中小企業にとって重要な情報[1]を漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や段階的に実現するための方策を紹介することを目的としたものです。

1　重要な情報
営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報のことです。経済的価値を指し「資産」を加え、「情報資産」と呼ばれることがあり、このガイドラインでも「重要情報」に加え「情報資産」と表記します。

～情報セキュリティ対策は、経営に大きな影響を与えます～

情報セキュリティ対策を実施して対外的にアピールすることで、企業としての信頼性を確保し、売上を伸ばしている企業がある一方、情報セキュリティ対策を疎かにしたために秘密情報や個人情報の漏えいを発生させ、業績は落ち込み、経営を揺るがしかねない高額な賠償金を支払った企業もあります。

～対策の不備により経営者が法的・道義的責任を問われます～

現代社会では、金銭や物品だけでなく、情報にも価値や権利が認められます。例えば、個人情報保護法では、事業者に対して個人の権利利益の保護、安全管理措置などの管理監督が義務付けられており、これらへの違反が認められると場合によっては会社に罰金刑が課されます。さらに、取締役や監査役は、別途、会社法上の忠実義務違反の責任を問われることもあります。

～組織として対策するために、担当者への指示が必要です～

企業の継続的な発展のために、また、経営責任を果たすためには、担当者に任せきりにすることなく、経営者が自社の情報セキュリティについて明確な方針を示すとともに自ら実行していくことが必要です。情報セキュリティ対策は、経営者が主導し、必要な範囲を網羅し、関係者と連携して組織的に実施しなければ機能しません。経営者はこれらを認識したうえで、情報セキュリティ対策の取り組みを担当者に指示する必要があります。

1．情報セキュリティ対策を怠ることで企業が被る不利益

ITの普及や利活用により経営効率が向上した反面、ITの普及以前には想定し得なかった秘密情報や個人情報の漏えいによる高額の損害賠償や金銭的損失を伴う事故が増えています。さらに、近年では、事故やその影響も多様化し、金銭的損失以外の不利益も顕著になっています。こうした事故による不利益は、情報セキュリティ対策を行うことで、経営上受容できる範囲まで減らすことができます。

ここでは、情報セキュリティ対策の必要性に対する理解を深めていただくために、対策が不十分なために起きる事故と、それにより企業が被る不利益を次に挙げる4点に要約して説明します。

（企業が被る不利益）

●金銭の損失
●顧客の喪失
●業務の停滞
●従業員への影響

これらを参考に、自社で起きかねない情報セキュリティ上の事故とは何か、どの業務にそのような心配があるか、自社の経営において最も懸念される事態は何かなどを具体的に思い描くことが、経営者が情報セキュリティ対策を認識する第一歩です。このような思考実験が経営者によるリスク認識の基礎となります。

(1) 金銭の損失

取引先などから預かった機密情報や個人情報を万一漏えいさせてしまった場合は、取引先や顧客などから損害賠償請求を受けるなど、大きな経済的損失を受けることになります。

一方、こうした損害賠償などによる損失だけでなく、インターネットバンキングに関連した不正送金やクレジットカードの不正利用などで直接的な損失を被る企業の数も増えています。

事例１　ウイルス感染で数日間業務が停止し、数千万円の被害が発生

（所在地：東京都/業種：情報通信業/従業員規模：101 ～ 300名）

社内のパソコンやサーバーがウイルスに感染し、数日間に亘った業務停止に至る障害が発生した。復旧のために徹夜で対応したが、その間の会社としての被害額は推計で数千万円に上る。原因は、被害が発生するまで、セキュリティ対策ソフトを全く導入していなかったことである。その後、ウイルス対策ソフトや技術的な対策の導入、情報セキュリティ規則の制定、プライバシーマークやISMS認証取得に取り組み、再発防止に努めている。

(2) 顧客の喪失

重要な情報に関する事故を発生させると、その原因が何であれ、事故を起こした企業に対する管理責任が問われ、社会的評価は低下します。同じ製品やサービスを提供している企業が他にあれば、事故を起こしていない企業の製品やサービスを選択する顧客が増えるのは自然なことであり、事故の発覚直後には大きなダメージを受けることになります。

大手メーカーのサプライチェーンに位置する企業の場合は、これまで継続してきた受注が停止に追い込まれることにもなりかねません。事故を起こした企業は再発防止に努め、事故を起こさずに事業を続けていくことが必要ですが、低下した社会的信用の回復には時間を要するため、事業の存続が困難になる場合もあります。

事例２　顧客情報の入ったパソコンの紛失事故により取引先の信用を失墜

（所在地：東京都/業種:情報通信業/従業員規模:101 ～ 300名）

従業員が顧客情報の入ったパソコンを持ち出した時に紛失事故が発生した。顧客に対して紛失の報告をしたが信用を失うこととなった。原因は、会社として情報セキュリティに対する意識が高くなかったため、持ち出しに関する明確なルールや手続きを定めておらず、従業員がパソコンを自由に持ち出せる環境であったことである。その後、情報機器の暗号化などの対策を実施するとともに、パソコンの持ち出しルールを含めた情報セキュリティ規程を整備して従業員へ情報セキュリティ教育を行った。

(3) 業務の停滞

日常業務で使用している業務システムに事故が発生すると、原因調査や被害の拡大防止のために、運用中の情報システムを停止したり、インターネット接続を遮断しなければならないことがあります。その結果、電子メールが使えなくなるなど、業務が停滞し、納期遅れや営業機会の損失が生じるなど、事業全体に影響が出てしまいます。

事例３　ウイルス感染により基幹システムが一週間停止

（所在地：静岡県/業種：製造業/従業員規模：51 ～ 100名）

従業員がメールに添付されていたウイルス付きのファイルを不用意に開いたことで感染し、基幹システムで障害が発生した。システムベンダーの協力を得て障害対応を行ったが、復旧するまでの１週間、基幹システムが使用できなくなった。原因は不審メールを受信した際の対処方法を詳しく教育していなかったことである。その後、朝礼などを利用して従業員へ情報セキュリティ教育を行うとともに、迷惑メール除去ツールを導入した。

(4) 従業員への影響

情報セキュリティ対策の不備を悪用した内部不正が容易に行えるような職場環境は、従業員のモラル低下を招く要因となります。さらに事故を起こしたにも関わらず、従業員のみを罰して管理職が責任を取らないような対応は、従業員が働く意欲を失うおそれがあります。情報漏えいなどの事故による企業としてのイメージダウンを嫌って、転職する従業員も現れます。また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。ある経営者は「個別の損害より、職場環境が暗くなったことが一番困った」と

語っています。

2．経営者が負う責任

情報セキュリティ対策を的確に指揮しなかったことに起因する業績の悪化などが経営者の責任であることは言うまでもありませんが、それ以外の経営者の「法的責任」と「社会的責任」について説明します。

(1) 経営者などに問われる法的責任

企業が個人情報などの法的な管理義務がある情報を適切に管理していなかった場合、経営者や役員、担当者は（表１）に示すような刑事罰その他の責任を問われることになります。

- ●個人情報やマイナンバーに関する違反の場合は刑事罰が科される恐れがあります。また、個人情報保護委員会[2]による立入検査を受ける責任もあります。
- ●民法上の不法行為とみなされた場合は、経営者が個人として損害賠償責任を負う場合もあります。

2　個人情報保護委員会
　個人情報保護委員会は、公正取引委員会と同様の高い独立性を有する機関です。

（表１）

情報管理が不適切な場合の処罰など

法令	条項	処罰など
個人情報保護法 個人情報の保護に関する法律	40条　報告及び立入検査 83条　個人情報データベース等不正提供罪[3] 84条　委員会からの命令に違反 85条　委員会への虚偽の報告など 87条　両罰規定	委員会による立入検査、帳簿書類等の物件検査及び質問 １年以下の懲役又は50万以下の罰金 6月以下の懲役又は30万円以下の罰金 30万円以下の罰金 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
マイナンバー法（番号法） 行政手続における特定の個人を識別するための番号の利用等に関する法律	48条　正当な理由なく特定個人情報ファイルを提供 49条　不正な利益を図る目的で、個人番号を提供又は盗用 50条　情報提供ネットワークシステムに関する秘密を漏えい又は盗用 51条　人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入、不正アクセス等により個人番号を取得 53条　委員会からの命令に違反 54条　委員会への虚偽の報告など 55条　偽りその他不正の手段により個人番号カード等を取得 57条　両罰規定	4年以下の懲役若しくは200万円以下の罰金又は併科 3年以下の懲役若しくは150万円以下の罰金又は併科 同上 3年以下の懲役又は150万円以下の罰金 2年以下の懲役又は50万円以下の罰金 1年以下の懲役又は50万円以下の罰金 6月以下の懲役又は50万円以下の罰金 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
不正競争防止法 営業秘密・限定提供データに係る不正行為の防止など	3条　差止請求 4条　損害賠償請求 14条　信頼回復措置請求	利益を侵害された者からの侵害の停止又は予防の請求 利益を侵害した者は損害を賠償する責任 信用を害された者からの信用回復措置請求
金融商品取引法 インサイダー取引の規制など	197条の2　刑事罰 207条第1項2号　両罰規定 198条の2　没収・追徴 175条　課徴金	5年以下の懲役又は500万円以下の罰金又はこれらの併科 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑 犯罪行為により得た財産の必要的没収・追徴 違反者の経済的利得相当額
民法	709条　不法行為による損害賠償	故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う

3　データベース等不正提供罪
　改正個人情報保護法で新設され、役員・従業者等が不正な利益を図る目的で個人情報データベース等を他者に提供したり盗用した場合は処罰対象になります。

(2) 関係者や社会に対する責任

適切に管理することを前提に預かった情報を漏えいしてしまった場合に問われるのは、前述の法的責任に加え、その情報の提供者や顧客などの関係者に対する責任もあります。また、情報漏えい事故は、営業機会の喪失、売上高の減少、企業のイメージダウンなど、自社に損失をもたらしますので、会社役員が会社法上の責任（会社に対する損害賠償責任）を問われ株主代表訴訟を提起されることもあり得ます。さらには、取引先との信頼関係の喪失、業界全体のイメージダウンにもなってしまいます。したがって、情報セキュリティ対策は、顧客・取引先・従業員・株主などに対する経営者としての責任を果たすためにも重要です。

個人情報保護法

個人情報保護法は、企業や団体に個人情報をきちんと大切に取り扱ったうえで、有効に活用できるよう共通のルールを定めた法律です[4]。「氏名」、「住所」、「生年月日」、「住所・電話番号・メールアドレス」などの連絡先、「顔写真」など、事業によって取り扱う個人情報は様々です。従業員情報や取引先の名刺も個人情報にあたりますので、従業員名簿やメールのアドレス帳などを作成している事業者は、保有する個人情報が少なくても、個人情報取扱事業者（個人情報データベース等を事業の用に供している者）となり、この法律が適用されます。

個人情報保護法について詳しく知るには個人情報保護委員会のウェブサイトを確認してください。

○個人情報保護委員会のウェブサイト
https://www.ppc.go.jp/

4 個人情報保護法第１条には、「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」とあることから、個人情報保護とは企業が被る損害の防止だけではなく、個人の人格的、財産的な権利利益に対する侵害防止を目的としていることに留意する必要があります。

不正競争防止法

企業が持つ営業情報や技術情報などの中には、秘密とすることで差別化や競争力の源泉となる情報もあります。そのような情報が漏えいすると、研究開発投資の回収機会を失ったり、社会的な信用の低下により顧客を失ったりと大きな損失を被ることになります。秘密としている情報を不正競争防止法により営業秘密として法的保護を受けるためには、①～③の要件をすべて満たす必要があります。

①秘密として管理されていること（秘密管理性）
②生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であること（有用性）
③公然と知られていないこと（非公知性）

3. 経営者は何をやらなければならないのか

企業で情報セキュリティを確保するための、経営者の役割を説明します。情報セキュリティの確保に向けて、経営者は、(1) に示す「３原則」について認識したうえで、(2) に示す「重要７項目の取組」の実施を指示する必要があります。

(1) 認識すべき「３原則」

経営者は、以下の３原則を認識し、対策を進める必要があります。

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

経営者は、IT活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策を進めます。現場の従業員は、安心して業務に従事できる環境を求める一方、利便性が低下し、面倒な作業を伴う対策には抵抗感を示しがちです。そこで、情報セキュリティ対策は、経営者が判断して意思決定し、自社の事業に見合った情報セキュリティ対策の実施を主導します。

情報セキュリティガバナンス

情報セキュリティガバナンスは、経営者が企業戦略として情報セキュリティ向上に取り組むための枠組みです。

この枠組みは、経営者が懸念する避けるべき重大事故などを示して「方向付け」を行い、対策の進捗や点検等により状況を「モニタリング」し、その効果を「評価」して方向付けを見直すサイクルを骨格としています。

経営者がリーダーシップを発揮する枠組みでもあります。

○経済産業省「情報セキュリティガバナンスの概念」のウェブサイト
https://www.meti.go.jp/policy/netsecurity/secgov-concept.html

原則２　委託先の情報セキュリティ対策まで考慮する

業務の一部を外部に委託するにあたって重要な情報を委託先に提供する場合、委託先がどのような情報セキュリティ対策を行っているか考慮する必要があります。委託先に提供した情報が漏えいしたり、改ざんされたとき、それが委託先の不備だったとしても、事故の影響を受ける者から委託元としての管理責任を問われることになります。そのため委託先や、共同で仕事を行っているビジネスパートナーなどの情報セキュリティ対策に関しても、自社同様に十分な注意を払います。また、受託している場合には、委託元の要求に応じる必要があります。

原則３　関係者とは常に情報セキュリティに関するコミュニケーションをとる

業務上の関係者（顧客、取引先、委託先、代理店、利用者、株主など）からの信頼を高めるには、普段から自社の情報セキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。情報セキュリティに関する取組方針を常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際にも、説明責任を果たすことができ、必要以上の不安を与えることなく、信頼関係を維持することができます。

(2) 実行すべき「重要７項目の取組」

中小企業で情報セキュリティを確保するための経営者の役割を説明します。経営者は、以下の重要７項目の取組について、自ら実践するか、実際に情報セキュリティ対策を実施するうえでの責任者・担当者に対して指示します。場合によっては、経営者自らが実行することも必要になると考えます。

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

情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかなどについて、自社に適した情報セキュリティに関する基本方針を定め、宣言します。自社の経営において最も懸念される事態は何かを明確にすることで具体的な対策を促し、組織としての方針を立てやすくなります。

取組２　情報セキュリティ対策のための予算や人材などを確保する

情報セキュリティ対策を実施するために、必要な予算と担当者を確保します。これには事故の発生防止だけでなく、万が一事故が起きてしまった場合の被害の拡大防止や、復旧対応も含みます。情報セキュリティ対策には高度な技術が必要なため、専門的な外部サービス[5]の利用も検討します。

5　専門的な外部サービスについては、IPAが公開している「情報セキュリティサービス基準適合サービスリスト」を活用することができます。

取組３　必要と考えられる対策を検討させて実行を指示する

懸念される事態に関連する情報や業務を整理し、損害を受ける可能性（リスク）を把握したうえで、責任者・担当者に対策を検討させます。必要とされる対策には予算を与え、実行を指示します。実施する対策は、社内ルールとして文書にまとめておけば、従業員も実行しやすくなり、取引先などにも取り組みを説明する際に役に立つので、併せて指示します。実行を指示した情報セキュリティ対策がどのように現場で実施されているかにつき、月次や四半期ごとなど適切な機会をとらえて報告させ、進捗や効果を把握します。

取組４　情報セキュリティ対策に関する適宜の見直しを指示する

取組３で指示した情報セキュリティ対策について、実施状況を点検させ、取組１で定めた方針に沿って進んでいるかどうかの評価をします。また業務や顧客の期待の変化なども踏まえて基本方針なども適宜見直しを行い、致命的な被害につながらないよう、対策の追加や改善などを行うように、責任者・担当者に指示します。

取組５　緊急時の対応や復旧のための体制を整備する

万が一に備えて、緊急時の対応体制を整備します。被害原因を速やかに追究して被害の拡大を防ぐ体制を作るとともに、的確な復旧手順をあらかじめ作成しておくことにより、緊急時に適切な指示を出すことができます。整備後には予定通りに機能するかを確認するため、被害発生を想定した模擬訓練を行うと、意識づけや適切な対応のために効果的です。経営者のふるまいについても、あらかじめ想定しておけば、冷静で的確な対応が可能になります。

取組６　委託や外部サービス利用の際にはセキュリティに関する責任を明確にする

業務の一部を外部に委託する場合は、委託先でも少なくとも自社と同等の対策が行われるようにしなければなりません。そのためには契約書に情報セキュリティに関する委託先の責任や実施すべき対策を明記し、合意する必要があります。

ITシステム（電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど）に関する技術に詳しい人材がいない場合、自社でシステムを構築・運用するよりも、外部サービスを利用した方が、コスト面から有利な場合がありますが、安易に利用することなく、利用規約や付随する情報セキュリティ対策などを十分に検討するよう担当者に指示する必要があります。

取組７　情報セキュリティに関する最新動向を収集する

情報技術の進化の早さから、実施を検討するべき対策は目まぐるしく変化します。自社だけで把握することは困難なため、情報セキュリティに関する最新動向を発信

している公的機関[6]などを把握しておき、常時参照することで備えるように情報セキュリティ担当者に指示します。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

6　情報セキュリティに関する最新動向を発信している公的機関
IPA（特定独立行政法人情報処理推進機構）のウェブサイト
https://www.ipa.go.jp/security/index.html
NISC（内閣サイバーセキュリティセンター）のウェブサイト
https//www.nisc.go.jp/

4.「SECURITY ACTION」一つ星を宣言しよう！

「SECURITY ACTION（セキュリティアクション）」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。安心・安全なIT社会を実現するために創設されました。

IT社会では、企業経営においてもIT活用による「攻め」と同時に「守り」が不可欠です。身近なところから情報セキュリティ対策を始めましょう。

SECURITY ACTIONの進め方は以下を参照してください。

①取り組み目標を決める

取り組み目標に応じて「★一つ星」と「★★二つ星」のロゴマークがあります。

・「一つ星」ロゴマークを使用するには…

中小企業の情報セキュリティ対策ガイドライン付録の情報セキュリティ５か条に取り組んでください。

すでに同等の取り組みができている中小企業は「二つ星」から始めてください。

【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！

・「二つ星」ロゴマークを使用するには…

中小企業の情報セキュリティ対策ガイドライン付録の「５分でできる！情報セキュリティ自己診断」で自社の状況を把握したうえで、情報セキュリティ基本方針を定め、外部に公開してください。

②自己宣言する

SECURITY ACTIONロゴマークをポスター、パンフレット、名刺、封筒、会社案内、ウェブサイト等に表示して、自らの取り組みをアピールすることができます。

情報セキュリティへの取り組みを宣言している中小企業等としてSECURITY ACTIONのウェブサイトに掲載されます。

③ステップアップしよう

「一つ星」から始めた中小企業等は、情報セキュリティをさらに向上させるために「二つ星」にステップアップしましょう。

「二つ星」から始めた中小企業等は、情報セキュリティをさらに有効にするために情報セキュリティ規程の策定及び規程の継続的な見直しによる新たな脅威等への対応を実施しましょう。

SECURITY ACTION　一つ星ロゴマーク

［注意事項］

・「SECURITY ACTION」は、情報セキュリティ対策状況等をIPAが認定するものではありません。

・「SECURITY ACTION（セキュリティアクション）」の取り組みに関してウェブサイト等において次のような不適切な表現をすると、第三者の誤解を生ずる可能性がありますのでご注意願います。

不適切な例　「一つ星の認定を受けました」、
「一つ星を取得しました」
適切な例　「一つ星を宣言しました」

○SECURITY ACTION公式サイト
https://www.ipa.go.jp/security/security- action/