特定非営利活動法人
ITコーディネータ沖縄

2025

デジタル・セキュリティの重要性とその対策

https://www.itc-okinawa.jp

2024/12/01 ©

企　画：広報委員会
執　筆：山原　朝哉
編集・スライド化：生成　AI

Contents

特定非営利活動法人
ITコーディネータ沖縄

01

デジタル・セキュリティの意義

デジタルトランスフォーメーションにおけるセキュリティ

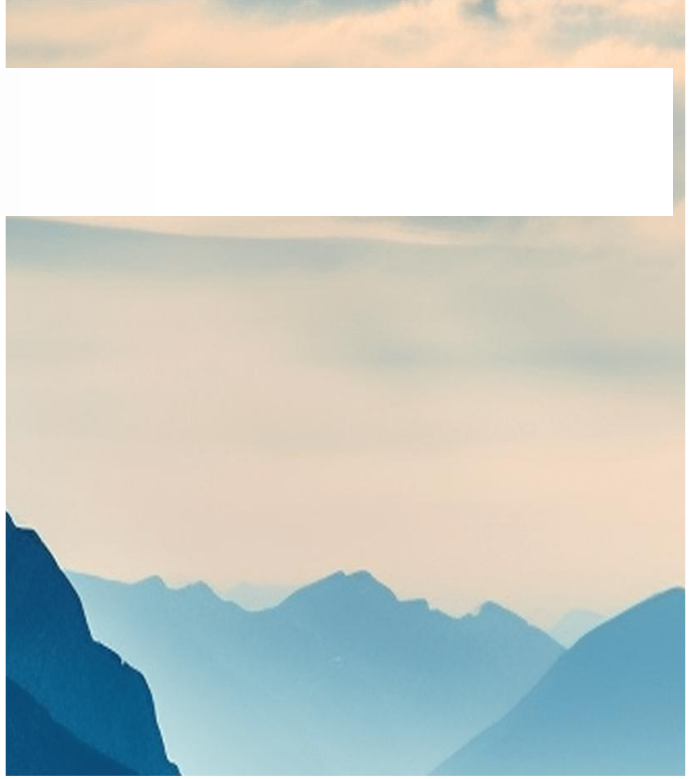
クラウドサービスの重要性とリスク

組織がデジタルトランスフォーメーション（DX）を推進するにあたり、クラウドサービスの利用が不可欠です。しかし、クラウドサービスを利用する際には、セキュリティリスクも伴います。組織のデータがクラウドに保存されるため、不正アクセスやデータ漏洩のリスクが増加します。これらのリスクを軽減するためには、しっかりとした認証システムや暗号化技術の導入が必要です。
クラウドサービスを通じた外部環境との連携は、業務の効率化と迅速な意思決定を可能にします。ただし、これに伴うリスクも無視できません。特に多様なデバイスからのアクセスが増えることで、セキュリティの確保が困難になることがあります。これに対処するためには、多要素認証やエンドポイントの保護が重要です。
クラウドサービスの利用によるリスク管理には、サービスプロバイダーとの契約内容の確認や、定期的なセキュリティ監査が必要です。これにより、サービスの品質と安全性を確保し、リスクを最小限に抑えることができます。

リモートワークのセキュリティ課題

リモートワークの普及に伴い、企業は従業員の自宅からのアクセスを許可する必要があります。これにより、セキュリティリスクが大幅に増加します。従来のセキュリティ対策だけでは不十分な場合が多く、リモートワーク専用のセキュリティ対策が求められます。
リモートワークにおけるセキュリティ対策としては、VPN（仮想プライベートネットワーク）の利用や、業務用デバイスのセキュリティ対策が挙げられます。これにより、安全な通信経路を確保し、データの漏洩や不正アクセスを防ぐことが可能です。
リモートワークのセキュリティを強化するためには、従業員の教育や訓練も重要です。セキュリティ意識の向上を図ることで、企業全体のセキュリティレベルを向上させることができます。また、定期的なセキュリティチェックや、ポリシーの見直しも必要です。

セキュリティ対策の全体像



セキュリティフレームワークの導入

情報セキュリティマネジメントシステム（ISMS）は、企業が情報セキュリティを体系的に管理するためのフレームワークです。これにより、企業はリスクを特定し、適切な対策を講じることが可能になります。また、ISMSは国際的なセキュリティ基準に基づいており、高い信頼性を持っています。
ISMSを導入することで、企業はセキュリティリスクを低減し、信頼性の高いデジタル環境を維持することができます。さらに、ISMSは継続的な監視と改善プロセスを含んでおり、セキュリティ体制の向上を図ることができます。
フレームワークの導入には、企業全体での協力が不可欠です。各部署が協力してセキュリティリスクを管理し、適切な対策を実施することで、企業全体のセキュリティレベルを大幅に向上させることが可能です。

IPAセキュリティアクション制度

IPA（情報処理推進機構）が提供する「セキュリティアクション」は、中小企業向けの情報セキュリティ対策支援プログラムです。情報セキュリティ意識を高め、実践を推進する「7つの実践」に基づき、取り組みを宣言することで★一つ星を取得できます。さらに、具体的な実施内容を報告すると★★二つ星が認定されます。この7つの実践には、ウイルス対策ソフトの導入、ソフトウェアの更新、パスワードの適切な管理、セキュリティ教育の実施などが含まれます。認定を受けた企業はマークを使用して、対外的にセキュリティ対策を行っていることを示せます。特に導入が簡単で、専門知識がなくても始められるため、情報セキュリティの第一歩として中小企業に適しています。

セキュリティ認証制度の種類

Pマークの取得とメリット

Pマーク（プライバシーマーク）は、個人情報保護に関する基準を満たしていることを示す認証制度です。このマークを取得することで、企業は顧客や取引先に対して個人情報を適切に管理していることを証明できます。Pマークの取得は、特にBtoCビジネスにおいて顧客の信頼を得るために重要です。Pマークの取得には、個人情報保護に関する厳格な基準を満たす必要があります。これにより、企業は個人情報の適切な管理体制を構築し、データ漏洩や不正利用を防ぐことができます。
Pマークを取得することで、企業は外部からの評価を高め、競争優位性を確保することができます。特に、個人情報保護が重視される現代において、Pマークの有無はビジネスの信用度を大きく左右する要素となります。

ISMSの導入と効果

ISMS（Information Security Management System）は、情報資産を包括的かつ体系的に保護するための管理システムで、ISO/IEC 27001規格に基づいて運用されます。その目的は、組織内の「機密性」「完全性」「可用性」という情報セキュリティの3要素を維持し、リスクを適切に管理することです。ISMSの導入ではまず、組織内の情報資産を特定し、それに関連するリスクを評価（リスクアセスメント）します。その後、リスクの低減策を計画し、実行（Plan-Do）、その結果を評価（Check）、必要に応じて改善（Act）するPDCAサイクルを継続的に運用します。これにより、組織全体で情報セキュリティ対策が有効に機能する体制を整えます。ISMS認証を取得することで、取引先や顧客に対して情報セキュリティへの取り組みを証明し、信頼性を高めることが可能になります。また、サイバー攻撃や情報漏洩などのトラブルを未然に防ぐことで、法的リスクやブランド価値の毀損を回避する効果も期待されます。特に大企業や規模の大きなプロジェクトでは、ISMSの導入が競争優位性を生む重要な要素となることも多く、情報セキュリティの課題に真摯に向き合うための有効な手段として広く利用されています。

中小企業向けのセキュリティ対策

中小企業の情報セキュリティリスク

中小企業は限られたリソースの中で情報セキュリティ対策を講じる必要があります。そのため、効率的かつ効果的なセキュリティ対策が求められます。中小企業にとっての主なリスクとしては、サイバー攻撃やデータ漏洩があります。
中小企業が直面する情報セキュリティリスクには、フィッシングやマルウェアの感染が含まれます。これらのリスクに対処するためには、基本的なセキュリティ対策を徹底することが重要です。例えば、パスワードの管理やソフトウェアのアップデートの徹底が挙げられます。
中小企業は大企業と比べてセキュリティリソースが限られているため、外部の専門家やサービスを利用することも検討すべきです。特に、セキュリティ監査やコンサルティングサービスを活用することで、効果的な対策を講じることができます。

iSSO認証の導入と効果

iSSO（Information Security Standard of Okinawa）は、中小企業向けの情報セキュリティマネジメント規格です。企業が直面する情報リスクを効果的に管理するために設計されています。iSSO認証を取得することで、中小企業は国際的なセキュリティ基準に準拠した管理体制を構築し、リスクを低減することが可能になります。
iSSO認証の特徴には、グローバルスタンダードに配慮した情報セキュリティ管理の強化や、運用の容易性とコストへの配慮があります。これにより、中小企業でも無理なくセキュリティ対策を導入することができます。
iSSO認証を通じて、沖縄の企業は情報セキュリティの強化を図り、持続可能な成長を実現することが期待されています。認証の取得により、企業は外部からの信頼を得ることができ、ビジネスの継続性と競争力を高めることができます。

特定非営利活動法人 ITコーディネータ沖縄

02

ITコーディネータ沖縄の支援

支援内容の概要

01. 現状分析とリスク特定

ITコーディネータ沖縄は、企業に適したセキュリティポリシーの策定支援を行っています。セキュリティポリシーは、組織の情報セキュリティに関する基本方針を明確にし、全従業員に周知徹底することが重要です。セキュリティポリシーの策定には、企業の業務内容やリスクプロファイルに基づいた具体的な対策を含めることが求められます。これにより、企業全体で統一されたセキュリティ対策を実施することができます。
ポリシーの策定後は、定期的な見直しと改善が不可欠です。ITコーディネータ沖縄は、企業が適切なタイミングでポリシーを更新し、最新のセキュリティ状況に対応できるよう支援を行います。

02. セキュリティポリシーの策定

ITコーディネータ沖縄は、企業の現在のセキュリティ状況を評価し、リスクを特定するための支援を行っています。これにより、企業は自社のセキュリティ体制の強化ポイントを明確にすることができます。
現状分析のプロセスには、企業内の情報資産の評価や、脅威と脆弱性の特定が含まれます。このプロセスを通じて、企業はリスクを定量的に把握し、効果的な対策を講じることができます。
リスク特定の結果に基づいて、企業は優先的に対策を講じるべきリスクを明確にすることが可能です。これにより、限られたリソースを効果的に活用し、セキュリティの向上を図ることができます。

教育と研修

01

従業員向けセキュリティ教育

従業員向けセキュリティ教育は、企業のセキュリティ体制の強化において重要な役割を果たします。ITコーディネータ沖縄は、従業員がセキュリティ意識を向上させるための教育プログラムを提供しています。
セキュリティ教育には、基本的なセキュリティ知識の習得や、実際の攻撃手法に対する対策が含まれます。これにより、従業員は日常業務において適切なセキュリティ対策を実践することができます。
定期的な教育と訓練を通じて、従業員のセキュリティ意識を継続的に向上させることが重要です。これにより、企業全体のセキュリティ文化の醸成が促進され、組織全体で一貫したセキュリティ対策を実施することが可能です。

02

専門家による研修プログラム

ITコーディネータ沖縄は、情報セキュリティの専門家による研修プログラムを提供しています。このプログラムは、企業内のセキュリティ担当者が高度なセキュリティ技術や知識を習得するために役立ちます。
研修プログラムには、最新のセキュリティ技術や攻撃トレンドに関する講義、実践的なハンズオンセッションが含まれます。これにより、セキュリティ担当者は実践的なスキルを身につけることができます。
専門家による研修を通じて、企業内のセキュリティ担当者は迅速かつ効果的にセキュリティインシデントに対応する能力を高めることができます。これにより、企業全体のセキュリティ体制が強化され、リスク管理が向上します。

継続的なサポート

定期評価と改善提案

ITコーディネータ沖縄は、セキュリティ導入後も定期的な評価と改善提案を行い、企業のセキュリティ体制の強化を支援します。定期評価により、セキュリティリスクの変化に対応した対策が可能になります。
定期評価のプロセスには、現行のセキュリティ対策の有効性の評価や、新たなリスクの特定が含まれます。これにより、企業は常に最新のセキュリティ状況に対応できる体制を維持することができます。
改善提案では、具体的な対策や新たな技術の導入が提案されます。これにより、企業はセキュリティレベルを継続的に向上させ、最新の脅威に対する対応力を高めることができます。

外部監査と認証支援

ITコーディネータ沖縄は、企業が外部監査や認証を受ける際の支援も行っています。これにより、企業は第三者評価を通じてセキュリティ対策の有効性を確認し、必要な改善点を明確にすることができます。
外部監査では、専門家による客観的な評価が実施され、企業のセキュリティ体制の強化が図られます。認証支援では、各種セキュリティ認証取得に向けた準備や申請手続きがサポートされます。
外部監査と認証取得を通じて、企業は外部からの信頼を得ることができ、ビジネスの信用度が向上します。また、認証を取得することで、顧客や取引先に対してセキュリティに対する取り組みを示すことができ、競争力を強化することができます。

特定非営利活動法人
ITコーディネータ沖縄

03

まとめと今後の展望

デジタル・セキュリティの重要性の再確認

DX推進とセキュリティのバランス

企業がデジタルトランスフォーメーション（DX）を推進するにあたり、デジタルセキュリティの確保は極めて重要です。DXとセキュリティのバランスを取ることで、企業は効率と安全性を両立させることができます。

特定非営利活動法人
ITコーディネータ沖縄

2025

Thanks for your attention

https://www.itc-okinawa.jp

2024/12/01 ©

企　画：広報委員会
執　筆：山原　朝哉
編集・スライド化：生成　AI