



DIRECT HOLDINGS

安全なECサイトを
作りたい！

セキュリティ対応の 基本のき

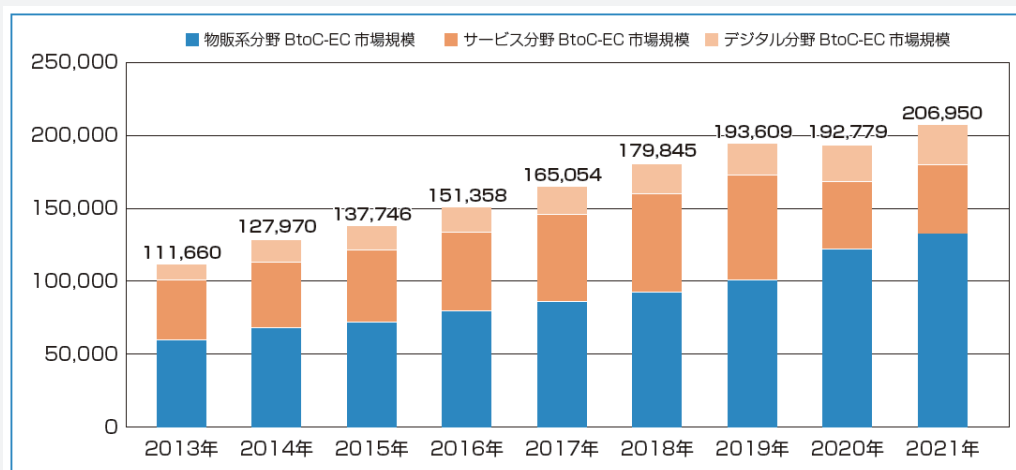


▶ 目次

- はじめに
- ① 情報セキュリティ対策は必須
- ② 個人情報取扱マニュアルの作成
- ③ 外部委託先の管理
- ④ 各種管理規定の整備
- おわりに

▶ はじめに

近年、私たちの生活に欠かせない存在となったオンラインショッピング。しかし、この利便性の裏には様々な**デジタル取引に伴うリスク**が潜んでいます。そこで、ECサイトが**安心感と信頼性を確保するために着実にやっている情報セキュリティ対策**にフォーカスしてみましょう。この記事では、**ECサイト運営において欠かせない情報セキュリティ対応**に焦点を当て、その必要性和具体的な取り組みについて探っていきます。



出典: 経済産業省「令和3年度デジタル取引環境整備事業(電子商取引に関する市場調査)」

◀ BtoC-EC 市場規模の経年推移 (単位: 億円)

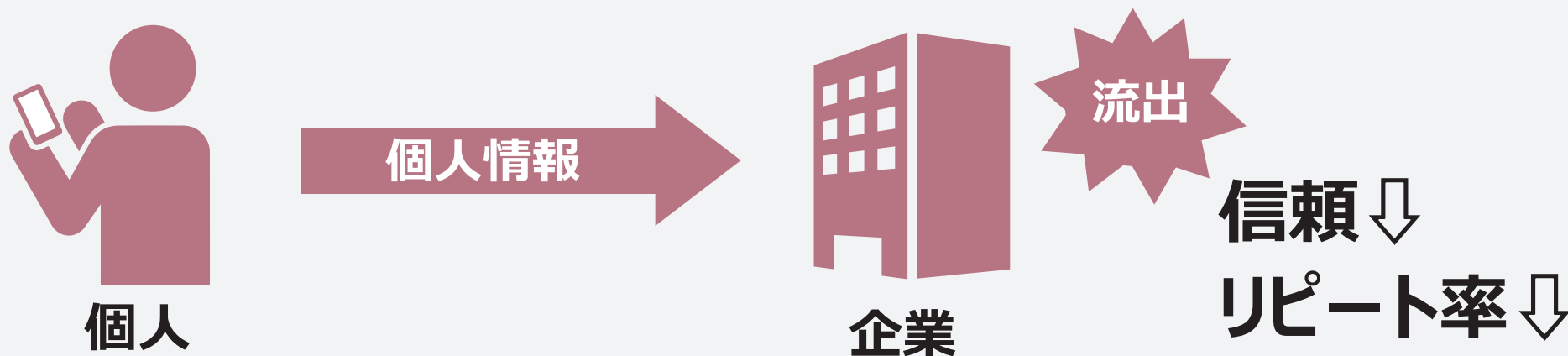
▶ 1. 情報セキュリティ対策は必須

現代のデジタル時代において、ECサイトの運営における情報セキュリティ対策は不可欠です。その理由を以下の6点にまとめました。

① 顧客情報の保護

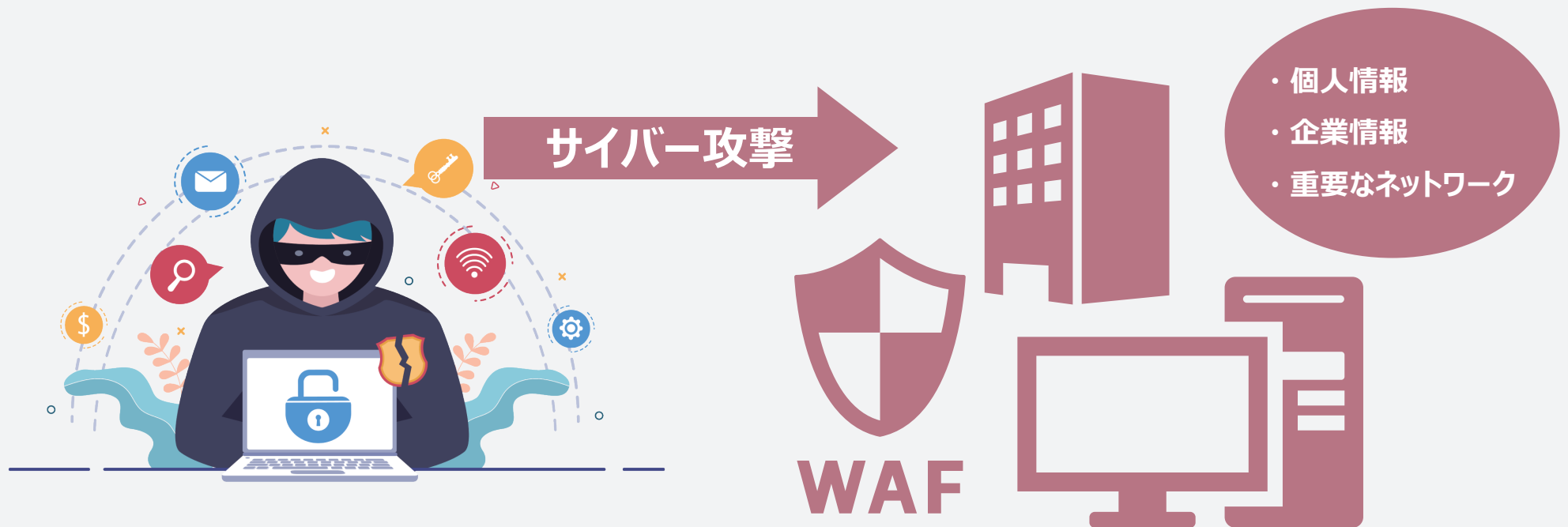
ECサイトでは、顧客の個人情報やクレジットカード情報などの貴重なデータを取得します。これらの情報が漏洩すると、顧客の信頼を失い、リピート購入や口コミでの広がりが阻害される可能性があります。

情報セキュリティ対策によって、顧客情報を適切に保護し、顧客の安心感を高めることが重要です。



② データ漏洩による損失防止

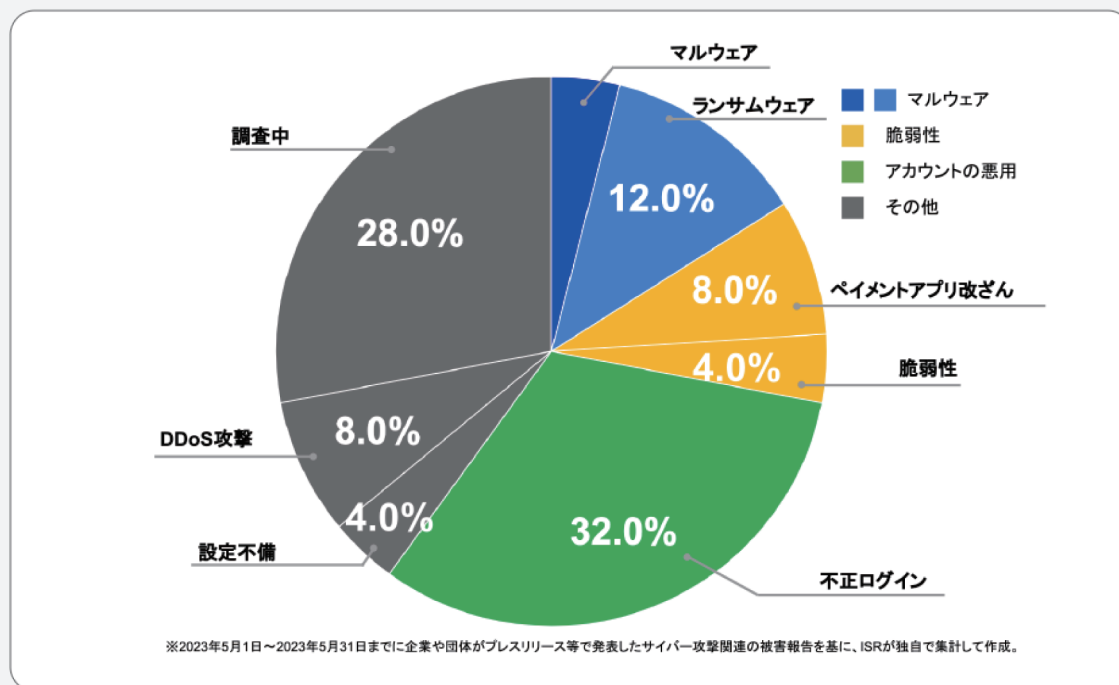
EC サイトは大量の取引データを扱います。万が一、データ漏洩が発生すれば、企業にとって**深刻な経済的損失**につながる可能性があります。**情報セキュリティ対策**によって、**不正アクセスやハッキング**などからデータを守り、**事業の持続性を確保**します。



③ インターネットの脅威への防御

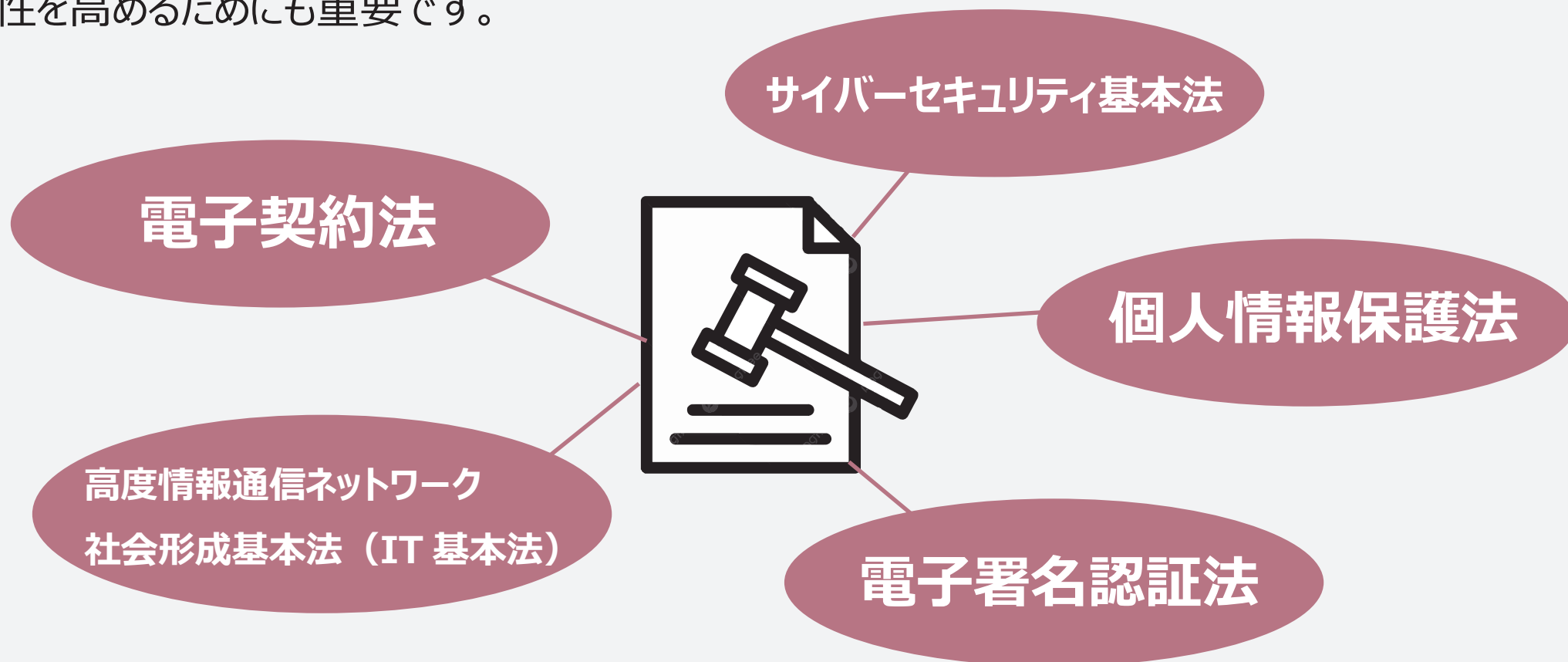
インターネット環境は常に進化しており、**様々なサイバー攻撃やマルウェアの脅威**が存在します。EC サイトは 24 時間稼働しており、いつでも攻撃対象になる可能性があります。情報セキュリティ対策は、**常に最新の脅威に対応し、サイトを守るために欠かせません。**

▶ 2023 年 5 月度に企業や団体が
発表したサイバー攻撃の攻撃手法



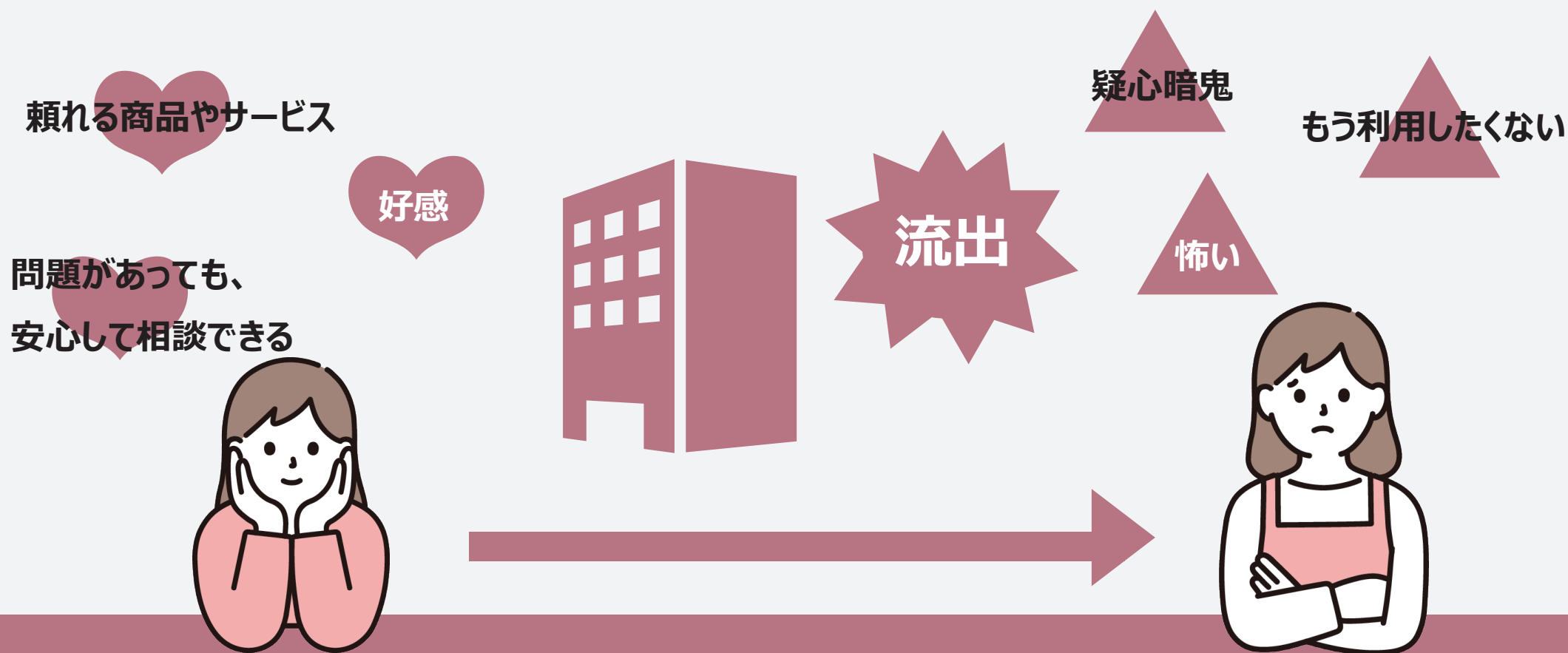
4 法的要件と規制順守

個人情報保護法やクレジットカード業界の規制など、情報セキュリティに関する法的要件と規制が存在します。これらを遵守することは法的な責任だけでなく、企業の信頼性を高めるためにも重要です。



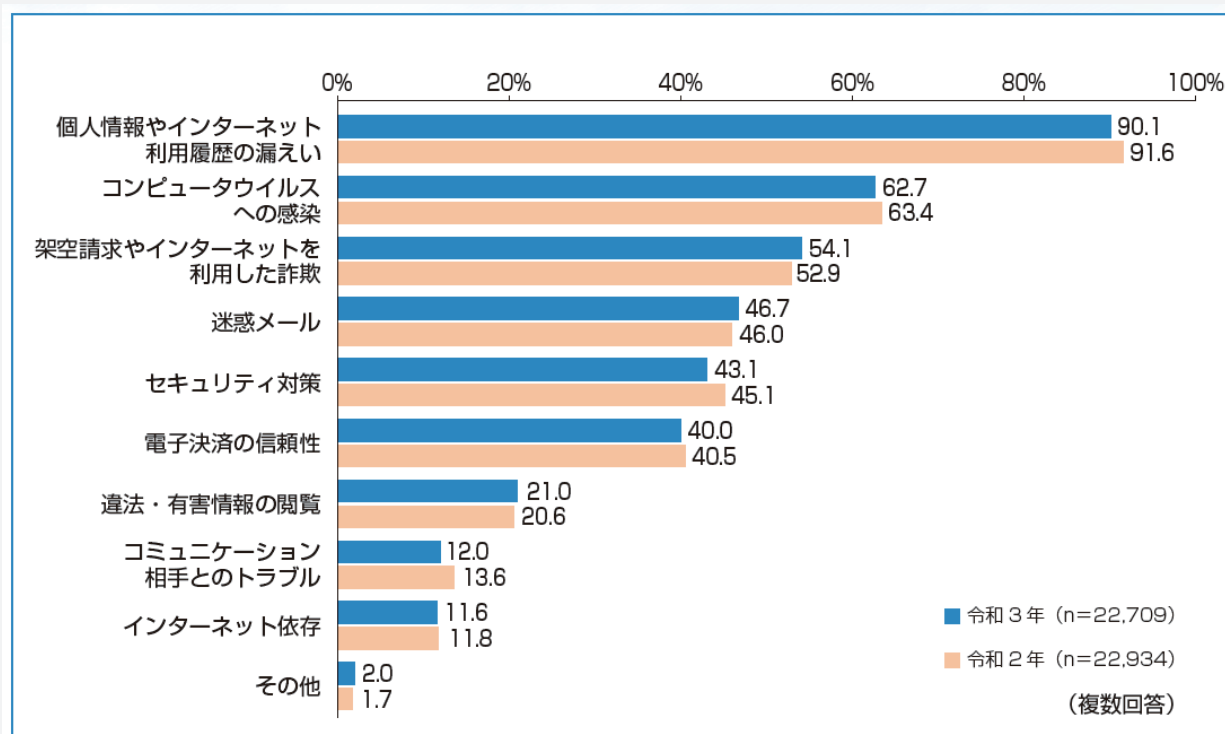
5 ブランドイメージの維持

情報漏洩やセキュリティインシデントは、**企業のブランドイメージに深刻な影響を与える**可能性があります。顧客は安全性を重視し、信頼できる EC サイトを選択します。情報セキュリティ対策によって、**ブランドイメージを維持し、競争力を高める**ことができます。



6 サービス提供の信頼性

情報セキュリティ対策がしっかりと整備されている EC サイトは、**信頼性の高いサービスを提供できるという点で競合他社よりも優位に立ちます。** 顧客はセキュリティに不安を抱えるサイトよりも安心してショッピングを楽しむことができます。



出典: 総務省「令和3年通信利用動向調査の結果(概要)」(令和4年5月)別添2 P.26
https://www.soumu.go.jp/main_content/000815653.pdf

◀ インターネット利用で感じる
不安の内容

このような理由から、**EC サイトの情報セキュリティ対策は企業の成長と継続的な成功に欠かせない要素**と言えます。顧客の信頼を確立し、同時にセキュリティリスクを最小限に抑えるためには、**真剣に情報セキュリティ対策に取り組むことが不可欠**です。この対策がなければ、企業の成長やブランドの維持が難しくなるでしょう。

具体的には、法的な要件を順守するために個人情報保護法をはじめとする法令を遵守するだけでなく、**個人情報取扱マニュアルの作成**も重要です。これにより、法令順守だけでなく、**顧客の個人情報を適切に管理し、安全に取り扱う基盤を築くことが可能となります。**



▶ 2. 個人情報取扱マニュアルの作成

個人情報取扱マニュアルは、**情報セキュリティに関する具体的な方針や手順を明確化した文書**です。例えば、個人情報の収集・利用・提供に関する基本方針や、アクセス制御やデータの暗号化といった技術的な対策について詳細に記載されます。

また、個人情報取扱マニュアルは、**従業員に対する適切な教育・訓練の基礎**ともなります。マニュアルを徹底的に理解し、遵守することで、**情報セキュリティ対策の重要性を従業員全体に浸透させることができます**。



▶ 3. 外部委託先の管理

ECサイトの運営においては、**システム開発や保守・運用などの業務を外部委託する場合もあります**。しかし、外部委託先が適切な情報セキュリティ対策を講じていない場合、重大なリスクを抱えることになります。

ここでは、

- ▶ 適切な外部委託先の選定
 - ▶ 情報セキュリティを外部委託する際の注意点
- を紹介します。



1 外部委託先の選定基準

情報セキュリティにおいて外部委託先を選定する際には、以下の基準を重視することが重要です。

専門知識と経験

外部委託先が持つ専門知識と経験は、情報セキュリティの高度な管理や対策を実施する上で欠かせません。セキュリティに関する適切な資格や実績、過去の成功事例などを評価しましょう。

セキュリティ対策体制

外部委託先がどのようなセキュリティ対策体制を整えているかを確認します。情報セキュリティポリシーや実施されているセキュリティ対策の内容を明確に把握し、要件に適合しているかを確認しましょう。

セキュリティリスク評価と対応策

外部委託先がセキュリティリスク評価を実施し、適切な対応策を立てているかを確認します。セキュリティインシデントへの対応や予防策の計画性が重要です。



インシデント対応体制

セキュリティインシデントが発生した際に、**外部委託先がどのような対応体制を取るか**を把握します。**迅速で適切な対応**が取れるかを確認し、信頼性を評価しましょう。



契約内容とサービスレベル

契約内容を慎重に検討し、サービス提供レベルや違約金なども含めて詳細に確認します。**情報セキュリティに関する明確な責任を定めた契約**を締結することが重要です。



サプライチェーンの管理

外部委託先がさらに下位の業者などを使っている場合には、**そのサプライチェーンも含めてセキュリティ対策が取られているか**をチェックしておく**と安心です**。委託先が適切な管理を行っているかを確認しましょう。

2 外部委託先を選定するときの注意点

では、実際に外部委託先を選定する際には、どのような点に気を付ければよいのでしょうか。
重要なポイントは 5 つあります。

リスク評価と最小限の権限付与

委託先には信頼性を求めますが、リスクを完全に排除することは困難です。適切なリスク評価を行い、必要最小限のシステムへの権限を付与するようにします。

セキュリティ監査と定期的な評価

委託先のセキュリティ対策が有効であることを確認するために、定期的なセキュリティ監査を実施します。
定期的な評価により、セキュリティレベルが維持されているかを確認しましょう。



契約書の明確化

契約書には**情報セキュリティに関する事項を明確に記載し、委託先の責任や義務を明確にします。**
違約金などの細かい部分も含めて、**契約内容を慎重に検討しましょう。**



インシデント報告と情報共有

委託先がセキュリティインシデントを経験した場合には、**適切なタイミングで報告を受ける体制を整えます。**
情報共有を通じて、**迅速な対応が可能となります。**



継続的なコミュニケーション

委託先とのコミュニケーションを継続的に行うことで、**お互いの理解を深め、セキュリティに関する意識を高めます。** 変更があった際にも**迅速に共有することが重要です。**

これらの基準と注意点を踏まえ、**情報セキュリティを適切に管理するための外部委託先選定を行いましょう。**



▶ 4. 各種管理規定の整備

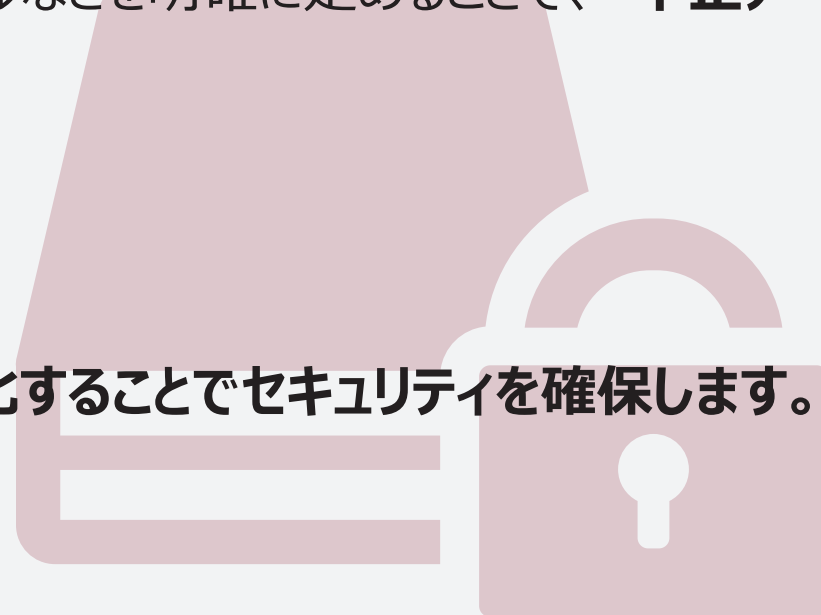
EC サイトの情報セキュリティ対策を徹底するためには、**各種管理規定の整備**が必要です。
具体的な管理規定としては、以下のような項目が挙げられます。

アクセス制御のルールと手続きの明確化

システムへのアクセス権限の管理やパスワードのルールなどを明確に定めることで、**不正アクセス**のリスクを低減します。

データの暗号化

顧客の個人情報や重要なデータは、**適切に暗号化**することでセキュリティを確保します。





バックアップと災害対策

データの定期的なバックアップと、災害発生時の対応策を策定することで、データの保全を図ります。



セキュリティインシデントへの対応手順

セキュリティインシデントが発生した場合の対応手順を明確に定め、迅速かつ適切な対応ができる体制を整えます。

これらの管理規定は、組織全体で共有され、実施されることが重要です。従業員に対して適切な教育・訓練を行い、管理規定の重要性を認識させることが必要です。

▶ おわりに

ECサイトの運営においては、**情報セキュリティ対策は不可欠です。****個人情報取扱マニュアルの作成、外部委託先の管理、各種管理規定の整備**など、様々な取り組みが求められます。これらの対策を継続的に実施し、顧客の個人情報を適切に保護することで、**安心・安全な EC サイトの運営**を実現しましょう。情報セキュリティへの取り組みは、**組織の信頼性向上や競争力の強化**にもつながります。



最後までお読みいただき、 ありがとうございました。



DIRECT HOLDINGS

ダイレクト・ホールディングスは、
デジタル・マーケティング事業、
SNS マーケティング事業、PR・
キャスティング事業をはじめ、多
彩な人材やノウハウを持つ広告
代理店です。

マーケティングに関するお困りご
と、ご相談がある際は、お気軽
にご連絡ください。

【お問い合わせ】

東京本社 〒163-1439

東京都新宿区西新宿 3 丁目 20 番 2 号

東京オペラシティタワー 39 階

電話番号：03-6416-4822

FAX：03-6416-4823

contact@direct-holdings.co.jp