# 情報セキュリティの7要素とは？定義や対策を簡単に解説

情報セキュリティの7要素とは、「機密性」「完全性」「可用性」という情報セキュリティの3要素に「真正性」「責任追跡性」「否認防止」「信頼性」の4つの新しい要素を追加した7つを指します。

|  |  |
| --- | --- |
| 機密性 | 許可されたユーザーだけが情報にアクセスできることを指す |
| 完全性 | 情報に誤りがなく完全である状態を保護して、維持することを指す |
| 可用性 | 情報へアクセスする権限を持つユーザーが、必要な時にアクセス可能であることを指す |
| 真正性 | 情報にアクセスしているユーザー・端末が、許可された人物やシステムであることを明確にする状態を指す |
| 責任追跡性 | 情報やシステムに対する操作が、誰によってどのように行われたのかを明確にすることを指す |
| 否認防止 | 情報資産に関する問題が発生した際、その原因となる人物が、後から否認できないよう証明することを指す |
| 信頼性 | システムの処理やデータ操作が、欠陥や不具合なく実行されることを指す |

これらを網羅的に確保・維持することで、外部攻撃や内部不正、ヒューマンエラー、災害などによって引き起こされるセキュリティリスクを防止することができます。

また、企業・組織が抱えるセキュリティリスクを把握し、それに応じて以下の情報セキュリティ対策を行うことも重要です。

1. **技術的対策**…ハードウェア・ソフトウェア面からセキュリティリスクを防止するための対策
2. **人的対策**…ヒューマンエラーなど人が原因で発生するセキュリティリスクを防止するための対策
3. **物理的対策**…災害などの物理的な要因で発生するセキュリティリスクを防止するための対策

この記事では、情報セキュリティの7要素の定義やそれぞれの要素を確保・維持するための対策を解説します。

**▼この記事を要約すると**

* 情報セキュリティとは、企業・組織が保有する**情報資産をサイバー攻撃や内部不正などから守ること**を指す
* 情報セキュリティリスクとは、組織が利用するシステムやサービス、保有する情報資産に対して悪影響を及ぼすリスクのことを指し、「**脅威**」と「**脆弱性**」の2つに大別できる
* 情報セキュリティの3要素とは、**機密性**(Confidentiality)・**完全性**(Integrity)・**可用性**(Availability)のことで、3つの頭文字をとってCIAとも呼ばれる
* 近年では、情報セキュリティの3要素に加えて「**真正性**」「**責任追跡性**」「**否認防止**」「**信頼性**」の4つを加えた7つの要素が提唱されている
* 情報セキュリティ対策は、大きく分けると「**技術的対策**」「**人的対策**」「**物理的対策**」の3つがある

情報セキュリティとは

情報セキュリティとは、企業・組織が保有する**情報資産をサイバー攻撃や内部不正などから守ること**を指します。  
情報資産には機密情報をはじめ、企業のブランドやイメージ、技術情報や業務のノウハウ、情報を保管する機器類も含まれます。

また情報セキュリティは、前述したサイバー攻撃や内部不正への対処はもちろん、災害や設備の事故などを想定したBCP※1を考慮する必要もあります。  
組織として必要な対処は多岐にわたるため、情報セキュリティは策定して終わりではなく、継続的にPDCAサイクルを回して改善を続けることが大切です。  
  
※1 BCP：事業継続計画。災害や事故、テロなどの緊急事態を想定し、そのような場合においてもできる限り事業を継続させるための計画。

情報セキュリティにおけるリスク

情報セキュリティにおけるリスクとは、組織が利用するシステムやサービス、保有する情報資産に対して悪影響を及ぼすリスクのことを指します。  
個別のリスクは多岐にわたりますが、組織のリスクは「脅威」と「脆弱性」の2つに大別することができます。

脅威

情報セキュリティの脅威は、情報の安全性やシステムの正常動作を妨げる要因を指し、「意図的脅威」「偶発的脅威」「環境的脅威」の3つに分類されます。

1. **意図的脅威**…外部攻撃や内部不正など、人間が意図的に発生させる脅威
2. **偶発的脅威**…ヒューマンエラーにより意図せず発生する脅威
3. **環境的脅威**…火事や地震、落雷などの災害による脅威

脆弱性

脅威を発生させる可能性を持つ、セキュリティ対策上の弱点を指します。  
建物の耐震・耐火構造などの物理的な脆弱性やソフトウェアの不具合、システム障害や機密情報管理体制の不備などが該当します。  
何も起こらなければ被害は発生しませんが、脅威を引き起こす原因であるため脆弱性への対処は重要なセキュリティ対策です。

情報セキュリティの3要素とは

情報セキュリティの3要素とは、**機密性**(Confidentiality)・**完全性**(Integrity)・**可用性**(Availability)のことで、3つの頭文字をとってCIAとも呼ばれます。

機密性(Confidentiality)

許可されたユーザーだけが情報にアクセスできることを指します。  
完全性(Integrity)

情報に誤りがなく完全である状態を保護して、維持することを指します。  
情報の改ざんはもちろん、メンテナンス不足により内容が古い状態なども完全性が損なわれていると言えます。  
可用性(Availability)

情報へアクセスする権限を持つユーザーが、必要な時にアクセス可能であることを指します。  
システムの障害や災害で情報にアクセスできない状態は、可用性が損なわれていると言えます。  
システムや電源の多重化、BCPが主な対策です。

また、情報セキュリティの3要素は「[**ISO/IEC 27001**](https://www.jqa.jp/service_list/management/service/iso27001/)」にてバランスよく維持することが求められています。

「ISO/IEC 27001」とは、ISMS※2を構築・運用する上で満たさなければならない、要件やルールを国際的な規格として定めたものです。

情報セキュリティの7要素（追加された4つの新要素）とは？

情報セキュリティの3要素である「機密性」「完全性」「可用性」は広く知られているところですが、近年ではそれに加えて「**真正性**（Authenticity）」「**責任追跡性**（Accountability）」「**否認防止**（non-repudiation）」「**信頼性**（Reliability）」の4つを加えた7つの要素が提唱されています。

真正性（Authenticity）

情報にアクセスしているユーザー・端末が、許可された人物やシステムであることを明確にする状態を指します。  
悪意のある人物がアカウント情報を盗んでシステムへアクセスできるといった状態は、真正性が損なわれていると言えます。

真正性を確保・維持するための対策としては

1. **デジタル署名**
2. **生体認証を含む多要素認証**

などが挙げられます。

責任追跡性（Accountability）

情報やシステムに対する操作が、誰によってどのように行われたのかを明確にすることを指します。

責任追跡性を確保・維持するための対策としては

1. **ファイルへのアクセスログ**
2. **端末操作ログ**
3. **デジタル署名**

などが挙げられます。

否認防止（non-repudiation）

情報資産に関する問題が発生した際、その原因となる人物が、後から否認できないよう証明することを指します。  
行為を指摘した際、証拠がなければ言い逃れることも可能であり、事実確認が困難になるケースもあります。  
責任追跡性と同様にアクセスログや端末の操作ログを取得し、確実に保存することが主な対策です。

信頼性（Reliability）

システムの処理やデータ操作が、欠陥や不具合なく実行されることを指します。  
意図していない処理によりデータに変更が加えられると、そのデータは完全性を失い、情報としての信頼性は著しく低下します。

信頼性を確保・維持するための対策としては

1. **システム設計時のレビュー・テストの徹底**
2. **マニュアル・ルールの策定**

などが挙げられます。

情報セキュリティ対策の種類

情報セキュリティを高めるための対策は、大きく分けると以下の3つがあります。

1. **技術的対策**
2. **人的対策**
3. **物理的対策**

技術的対策

技術的対策とは、ハードウェア・ソフトウェア面からセキュリティリスクを防止するための対策です。

具体的には以下のような対策が該当します。

1. **アンチウイルスの導入**
2. **ファイアウォールやIDS／IPSの設置**
3. **ログ監視**
4. **データの暗号化**

人的対策

人的対策は、ヒューマンエラーや従業員による不正な情報の持ち出しなど、人が原因で発生するセキュリティリスクを防止するための対策です。

具体的には以下のような対策が該当します。

1. **従業員へのセキュリティ教育の実施**
2. **マニュアル・ルールの策定**

物理的対策

物理的対策とは、紛失・破壊・災害といった物理的な要因で発生するセキュリティリスクを防止するための対策です。

具体的には以下のような対策が該当します。

1. **監視カメラの設置**
2. **入退室記録の管理**
3. **警備員の配置**
4. **オートロックの設置**