ビジネスパーソンが知っておくべき情報セキュリティ入門ガイド

～基礎が分かれば仕事もスムーズ～

目次

Securify

1.情報セキュリティの定義

情報セキュリティの定義

Securify

情報セキュリティという言葉は、
一般的には情報の**「機密性」「完全性」「可用性」**を確保することと定義されています。

許可された者だけがアクセスできる

情報が正確で完全な状態を保持

必要な時にいつでもアクセスできる

情報セキュリティの定義

機密性（Confidentiality）とは、許可された者だけがアクセスできることです。
許可されていない利用者をアクセスすることができないようにしたり、データを閲覧することはできるが書き換えることはできないようにしたりします。
機密性が侵害されると、許可されていない者がデータを閲覧、持ち出す可能性があります。

情報セキュリティの定義

Securify

完全性（Integrity）とは、保有する情報が正確であり、完全である状態を保持することです。
情報が不正に改ざんされたり、破壊されたりしないことを指します。
完全性が侵害されると、侵入者がWebサイトやデータベース上の情報を改ざんし、情報が信頼できないものとなる場合があります。

情報セキュリティの定義

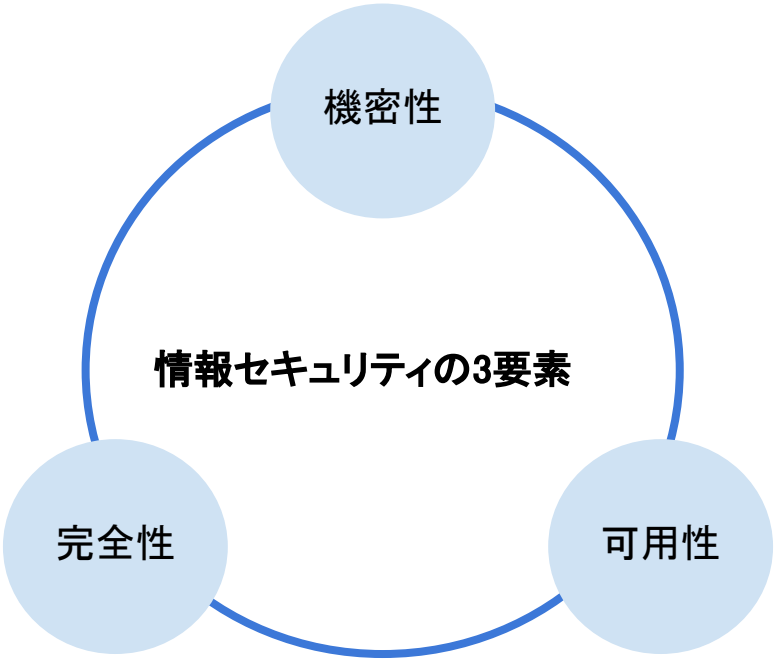
Securify

可用性（Availability）とは、許可された者が必要なときにいつでも情報にアクセスできるようにすることです。
つまり、可用性を維持するということは情報を提供するサービスが常に動作するということを表します。可用性が侵害されると、攻撃者が自社のWebサーバにアクセスを集中してダウンさせ、サービスを利用できなくする場合があります。

情報セキュリティの定義

Securify

下記の3要素が満たされている状態が、情報セキュリティが満たされている状態と言えます。
逆に何か一つでも満たされていない状態であれば、満たされていない部分について対策を講じる必要があります。



情報セキュリティの定義

Securify

情報セキュリティを考える上で最も大切なことは、

組織において「最も大切な守るべきもの」を決めることです。

守るべきものはなにか（中でも最重要なものはなにか）

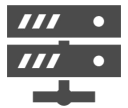
顧客情報…
顧客管理データベースなど

取引先情報…
取引先管理ファイルなど

製品情報…
従業員の端末や管理システムなど

財務情報…
経理システムなど

顧客向けサービス…
Webサーバなど



情報セキュリティの定義

何を守るべきかを把握する上でのヒントとして、あなたの会社の **情報資産**を考えてみましょう。

情報資産とは、組織において価値を有する「システム」「データ（従業員の記憶や知識含む）」を指します。情報資産を棚卸し、情報資産台帳を作成することで組織の情報資産を把握できます。

分類	例
情報資産	ファイル・データベース・契約書
物理的資産	コンピュータ・サーバ
ソフトウェア資産	業務用ソフトウェア・OS
人的資産	人・保有する資格・技能・経験
無形資産	組織の評判・イメージ
サービス	計算処理・通信サービス・設備（暖房、証明、電源、空調）

2.情報セキュリティ対策における観点

情報セキュリティ対策における観点

Securify

情報セキュリティ対策には3つの考え方があります。次ページで上記の具体的な例を見てみましょう。

	観点1	観点2	観点3
内容	**技術的対策**	**物理的対策**	**人的対策**
目的	悪意ある攻撃によるウイルス感染や不正アクセス、データ漏えいなどに対応するための対策です。	不法侵入や破壊、紛失や災害などのセキュリティリスクに対応するための対策です。	従業者のミスや不正など、人によるセキュリティリスクに対応するための対策です。
留意点	目的が多岐にわたるため、自社にとって何が適切であるかを見極めることが重要です。	物理的なオフィス環境や立地により異なる部分も多くあることを念頭に置き、対策を練りましょう。	ルールを決めるだけでなく、社員に遵守してもらうような風土づくりも重要です。

情報セキュリティ対策における観点 ①技術的対策

Securify

情報セキュリティ対策のうち、
ハードウェアやソフトウェアからの対策を **技術的対策** と呼び、下記の内容を含みます。

取り組み

セキュリティツール・システムの導入や設定

- ウイルス対策ソフト
- ファイアウォールやIDS/IPS
- ログ監視ツール
- アクセス管理
- ディスクやデバイスの暗号化

仕組み化

ツール導入以外にも現状のルールに一工夫することで実現可能

- ホワイトリスト・ブラックリストの活用
- OSやソフトウェアの更新ルール設定
- 権限の見直しと管理
- データDLに関するルールの厳格化

情報セキュリティ対策における観点 ②物理的対策

Securify

情報セキュリティ対策のうち、
データやIT機器が所在する場所への対策を **物理的対策** と呼び、下記の内容を含みます。

取り組み

オフィスのセキュリティ向上

- 入退館時に認証を要求
- 監視カメラ設置
- 警備員の配備
- 覗き見対策（壁・パーティションなど）
- PC持ち出し防止ワイヤーロック
- 書類持ち出し防止（キャビネットの施錠

仕組み化

人の出入りに対する管理

- 入退館や来客の記録
- 社員証の携帯・掲示

情報セキュリティ対策における観点 ③人的対策

Securify

情報セキュリティ対策のうち、
人ならびに人が発生させるリスクへの対策を **人的対策**と呼び、下記の内容を含みます。

取り組み

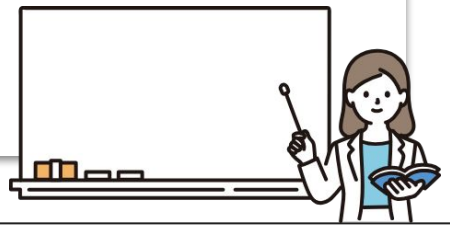
従業員のセキュリティ意識に対する教育

- 情報セキュリティ教育
- コンプライアンス教育
- 業務ミス防止のためのトレーニング

仕組み化

確立した手順に基づき作業を行う

- ルールの明確化・周知活動を実施
- マニュアルの作成・更新を実施
- 違反発生時の懲戒手続きを明確化



3.情報セキュリティを確保するためのステップ

情報セキュリティを確保するためのステップ

Securify

1.守るべきものを確定する

「何を守るか」を理解し、確定させます。※P9参照

情報セキュリティを確保するためのステップ

Securify

1.守るべきものを確定する

「何を守るか」を理解し、確定させます。※P9参照

2.リスクを確認する

守るべきものを、「どのようなリスクから守るのか」を確認し、リスクを特定します。

情報セキュリティを確保するためのステップ

Securify

1.守るべきものを確定する

「何を守るか」を理解し、確定させます。 ※P9参照

2.リスクを確認する

守るべきものを、「どのようなリスクから守るのか」を確認し、リスクを特定します。

3.特定されたリスクに対処する

特定されたリスクに対し、「発生確率」「被害」などの観点から、対処を決定します。
高確率・被害大のリスクは優先的に対処すべきですが、低確率・被害小のリスクは
あえて対処を行わない場合もあります。
対処を実施した後は、引き続きリスク確認、対処、状況整理というサイクルを繰り返します。

4.情報セキュリティ対策が不十分な場合に発生する被害

情報セキュリティ対策が不十分な場合に発生する被害

Securify

情報セキュリティ対策が充分でなく、下記のような攻撃・事故が発生した際に、
組織や企業に重大な被害が生じる場合があります。

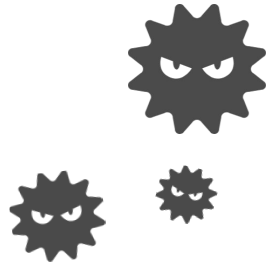
攻撃・事故	ウイルス感染	不正アクセス	情報漏えい	災害などによる機器障害
解説	コンピュータウイルスが機器に感染した結果、システムやデータの破壊、情報の漏えいが発生。	攻撃者がインターネットを経由してシステムに侵入した結果、システムやデータ破壊、情報漏えいが発生。	誤送信、内部犯行、無線LANの不正傍受、なりすまし攻撃などの結果、情報の漏えいが発生。	火災、地震、雷などの自然災害が発生した結果システムの破壊やデータの消失などが発生。

情報セキュリティ対策が不十分な場合に発生する被害

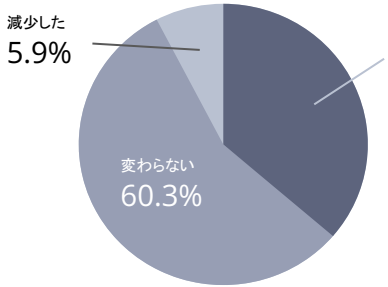
Securify

被害

- 自社ならびに他社への損害、損害賠償
- ブランドイメージ低下
- サービス停止やデータ消失による顧客離れ
- 組織の競争上の優位を損なう



2020年4月以降に受けたサイバー攻撃



日経新聞の調査でも2020年4月以降に
サイバー攻撃が増加したと回答する
企業は33.8% にも上りました。

日経新聞（7/20）より

次ページで紹介する、**スリーシェイクが提供している「Securify」**を利用することで、
情報セキュリティの技術的対策の一部として活用が可能ですので、ぜひお試しください。

Securify（セキュリファイ）とは

Webアプリケーションの
継続的セキュリティを簡単に実現

Securify

Securify（セキュリファイ）は自社のプロダクトに対して、
手軽に、何度でも脆弱性診断の実施を可能にし、
セキュリティレベルを可視化・DevSecOpsへの取り組みをサポートします。

▶ **まずは0円のフリープランへお申し込みください**