EXECUTIVE CYBER SECURITY

経営者のための情報セキュリティー入門

「最低限、何があれば会社を動かせるか？」

イー・レンジャー株式会社 | 2026年10月

この資料の目的

情報セキュリティに関係する出来事

- 相次ぐ情報漏洩
- PHPの脆弱性
- ランサムウェアによる業務停止
- 地震や大規模水害

この資料では、以下をわかりやすく説明します

- **情報セキュリティの定義**
- **経営者の役割と基本的な考え方**
- **情報の簡易棚卸し**

（注）ISO/IEC 27001・27000の考え方を参考に、当社が独自に作成した教育資料です

（基本概念）情報セキュリティとはCIAを維持することです

C｜機密性

Confidentiality

許可されていない人に、知られてはいけない情報を守ること

例：顧客情報・設計図

I｜完全性

Integrity

情報が正確で改ざんされていない状態を維持すること

例：振込先・受発注・在庫

A｜可用性

Availability

必要なときに情報が使える状態を維持すること

例：生産・受注・出荷

CIAの維持が情報セキュリティの定義、目標です

（基本概念）脅威とリスクは違う

脅威・脆弱性｜情報資産に被害を与える可能性のある原因や弱点

サイバー攻撃、PHPの脆弱性、地震・水害、火災
従業員による持ち出し、PCにコーヒーをこぼす

リスク｜脅威によって自社が被る可能性のある損害（注記も参照）
CIAへの影響を評価する（リスクアセスメント）

受発注システムの停止（重大）

サイバー攻撃、PHPの脆弱性を悪用した攻撃、地震・水害、火災、USBで情報を盗まれること：脅威としては同列

セキュリティ対策は「脅威があるから」ではなく、「自社のリスク評価」に基づいて行います。

（注）社会的な損害（第三者への被害、法令違反など）につながる可能性も考慮することが必要です
マルウェアの感染 → 取引先への攻撃

（基本概念）管理策 — 対策は自社のリスクで決める

リスク｜脅威によって自社が被る可能性のある損害

（例）受発注システムの停止（重大）

管理策｜具体的な対策

システムを最新版に維持する。
毎日バックアップを取得し、他所へ30日間保管する。

管理策は人的資源、コストなどの観点から決めます
管理策とともに代替計画を策定することも重要です

残留リスク： 管理策を実施した後も残るリスク

（例） 担当者に連絡がとれない
バックアップを取得していても、障害時に正常に復旧できず、業務停止が長期化する可能性

（基本概念）リスクを「受容」する

全てのリスクをゼロにはできません。
リスクを受容するかどうかは、経営者が定めた判断基準に基づいて決定し、必要に応じて見直します。

対策するが残留するリスク

低減する努力はするが、コストや人的資本を鑑みて受容する。

対策せず残留するリスク

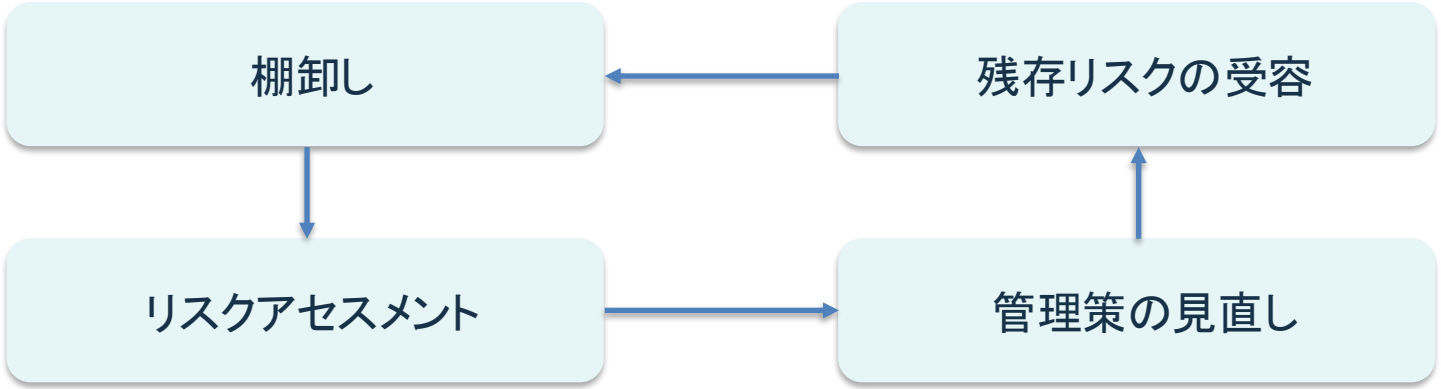
影響が限定的で許容範囲なので、対応を延期・見送る

受容は「放置」ではなく、「リスクを認識して受け入れること」です。

（注意）自社のCIAが低くても、踏み台化・法令・取引先への影響は重要です。

（基本概念）CIAを維持改善する

脅威とともにリスクは変化します。
情報資産の種類・量・重要度も変化します。
人的資源や委託先も変化し、情報技術は進化します。



PDCAを回し、定期的に経営者レビューを行って、新しいリスクの評価・残存リスクの再評価し、CIAを維持改善します。

今日、経営者に考えていただきたいこと

問い①

社外に絶対漏洩してはいけない情報は何か？

（注）適切な手続きに基づく情報共有を除く

問い②

内容が変わると、会社の存続に関わる重大な損失が発生する情報は何か？

問い③

会社を動かすために絶対に必要な情報は何か？

すべてが重要に見えても、経営への影響には差があります。
①、②、③について必要最低限な情報資産を見極める経営判断が必要です。

（必要最低限）バックアップがあってもすぐに復旧できるとは限りません

クラウドバックアップがある場合

10TBを全量復旧

実効100Mbpsで転送する場合
理論上 約9.3日
※転送だけの時間

100GBを優先復旧

同じ条件なら
理論上 約2.2時間
※転送だけの時間

復旧するためには、最低限以下の手続きが必要です。
・戻せるバックアップがあることの確認（バックアップが消されたり、暗号化されてないことの確認）
・データの転送
・データの整合性確認：バックアップ取得後の取引や変更履歴を確認し、必要なデータを補完・照合する。アクセス権限も確認する。
・テスト：システム全体が正しく動くか、取引先と連携するデータが正常化など
・復旧：社内外への連絡

優先的に復旧する情報資産を見極める経営判断が必要です。

（必要最低限）「すべて重要」とすると復旧できないかもしれません

すべて最優先にした場合

費用・人員・復旧時間が分散する。

「どれから戻すか」決められない

最小限を選んだ場合

復旧対象と順番が明確

限られた資源を事業再開に集中
復旧を遅らせる業務に関わる利害関係者がすぐわかる

復旧の手順の明確化 → 訓練（可能である場合）により、復旧に要する時間をシミュレートできる状態が理想です。

（必要最低限）事業の優先度と停止許容時間を決める

経営者が決める

どの事業を優先するか

何時間・何日まで停止できるか

手作業など代替手段はあるか

IT担当者が具体化する

必要なシステム・データを特定する

復旧手順・所要時間の見積もりと検証

バックアップの計画と訓練の実施

必要に応じて委託先に協力を依頼する

技術的に「戻せる順番」と、経営上「戻すべき順番」は違います
ダウンタイムゼロではなく、何時間・何日ならダウンできるか（在庫確保など）という考え方が無理がありません。

（情報の棚卸） まずは「どんな情報資産があるか」

どこに、どんな形態（電子、紙、メディア）でどんな情報があるかをざっくり調べます

（例）ファイルサーバーにある情報の場合
ファイル単位で調べるのは大変なので、業務・フォルダー単位でも。

× ファイル単位

全ての情報（ファイル、書類、メディア）を1件ずつ調べる

→ 時間がかかり、継続できない

○ 業務・システム･情報の種類単位

受発注／生産管理／図面／会計／顧客情報

→ 管理責任者と保管場所を記録します

（例）システムの場合
受注出荷システム／生産管理システム／CAD／ CAM／経理システムなど。

最初は「どこにどんな情報があるか」を知るだけでも。
定期的に棚卸しが継続できる（PDCAできる）レベルで実施します。

（情報の棚卸）今日から始める「簡易棚卸し」

1. 業務を挙げる

受発注・製造・出荷・設計・会計など止まると困る業務を列挙します。

情報の媒体、在処、責任部門を記載します

2. CIAを判定

社外秘か／正確さが重要か／利用不可能になったインパクト

を評価します。

3 . 最小限を決める

緊急復旧する業務・データを決め、復旧時間を設定します。

復旧時間の目標は可用性（A)に連動します。
可用性（A)は完全性（I)に制約されることがあります。

最初から完璧を目指さず、業務責任者と一緒に小さく始めるのがリーズナブルです。

（情報の棚卸）簡易棚卸しの記録はこんなイメージで

◎ :該当かつ重要　　△: 該当かつ重要ではない
○: 該当　　ー: 該当しない

業務・情報	媒体	保管場所		責任者	C	I	A	復旧目標
受注情報	電子ファイル	ファイルサーバー	営業部フロア	営業部	○	◎	◎	24時間
	受注システム	業務サーバー	総務部フロア		○	◎	◎	24時間
製造図面	電子ファイル	ファイルサーバー	製造部フロア	製造部	○	◎	◎	24時間
	紙	キャビネットA	製造部フロア		○	—	—	電子ファイルから印刷可
決算情報	経理システム	クラウド	A社に委託	経理部	○	◎	△	1週間
	紙	キャビネットA	経理部フロア		—	△	—	システムから再発行可

復旧目標は仮置きして、後でIT担当者（委託先）と実現可能性を検証します。
これらの情報資産のそれぞれについて、脅威・リスクを列挙し、管理策を策定します（後述）

（情報の棚卸） AI時代のセキュリティ対策

簡易棚卸し

脅威・リスク・管理策の候補の洗い出し

AIに簡易棚卸し結果を渡して候補を洗い出す

（注）AIに社外秘情報は伝えない

脅威･リスク･管理策の検討

自社に当てはまるか検討する

リスクの受容と管理策の実施

実施する管理策、受容するリスクを決める
管理策を実施する（必要に応じて委託先と連携する）

定期的な見直しにもAIを活用し、新たな脅威や管理策の候補を検討します

（情報の棚卸）経営者が決めておくべき「事故時の判断」

業務停止

止める業務／続ける業務／代替方法

対外説明

顧客・取引先・当局への連絡判断

復旧順位

まず戻す業務・データ・システム

責任と権限

誰が決裁し、誰が実行するか

障害発生直後は考える時間がありません。
事前に障害対応チームを決めて手続きを明確化・文書化し、訓練するのが望ましいです。

（情報の棚卸）復旧は3段階で考える

第1段階｜緊急復旧

受注・出荷・稼働中の図面
最低限の業務再開に必要なもの

第2段階｜通常復旧

過去案件・会計資料など
業務を正常化するもの

第3段階｜後日復旧

古い写真・保管資料など
後から戻してもよいもの

「最初に戻すもの」が少ないほど、事業を再開しやすくなります。
緊急時には「戻す必要がないもの」をあらかじめ分けて保管することも有効です。

警察庁の一次資料から

ランサムウェアは中小企業にも現実のリスク

226件

2025年の被害報告件数

143件

中小企業の被害件数

61／92件

侵入経路の回答でVPN機器

19／92件

侵入経路の回答でRDP

一次資料：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」統計編 pp.120,122–126

ランサムウェア時、CIAの棚卸しが経営判断を助ける

C｜漏えい

漏洩した情報が社外秘であるか否かの判断

→ 影響調査・顧客説明の判断

I｜改ざん

改ざんされた情報が、事業継続性にどの程度影響があるのか

→ 復旧計画の基本情報

A｜停止

利用不可能となった情報が、事業継続性にどの程度影響があるのか

→ 復旧計画の基本情報

棚卸しは「全ての判断の土台」になります。

本資料の利用について

「経営者のための情報セキュリティー入門」
© 2026 イー・レンジャー株式会社

本資料は、Creative Commons Attribution 4.0 International（CC BY 4.0）ライセンスの下で公開しています。
https://creativecommons.org/licenses/by/4.0/deed.ja

出典を明示していただければ、複製・再配布・改変・商用利用が可能です。
改変した場合は、その旨を明示してください。

本資料は情報セキュリティに関する一般的な教育を目的としており、個別の組織における安全性を保証するものではありません。

※第三者が権利を有する素材および当社の商標・ロゴは、CCライセンスの対象外です。