中小企業事業継続研修会
(全12講座)
第10回　事前対策（１）
情報バックアップ
IT・情報セキュリティ（サイバーテロ）

2022年10月31日月曜日

説明者　指田　朝久
特定非営利活動法人事業継続推進機構　副理事長

主催　特定非営利活動法人 事業継続推進機構(BCAO)

内容

- ◆情報システム依存度と分類
- ◆経営者の認識
- ◆情報バックアップ
- ◆IT・情報セキュリティ
- ◆IT-BCP様式
- ◆維持管理
- ◆社員教育と演習の重要性
- ◆ITに強いアドバイザーとの連携
- ◆補助金の活用
- ◆ビジネスチャンスにつなげる

出典：ＩＴ・サイバータスクフォース作成

情報システム依存度と分類（例:松竹梅）

出典：ＩＴ・サイバータスクフォース作成

システムはどれくらい重要？

◆ システムが止まったら！　「BCは地震防災ではない」ところから再認識

◆ BIAをシステムの観点から見直す

BIAの原点　何等かの事由で事業が止まる

優先すべき重要業務、中核業務は何か

どの仕事、どのサービス、どの製品、どのお客様？

それは、いつまでにどれくらいの量の復旧が必要？

◆ 重要業務、中核業務のシステム依存度は

その仕事をするために、情報システムは何が必要？

使うデータ、使うシステム、端末・パソコン、手順書、

ユーザーマニュアルを明確に特定する

出典：ＩＴ・サイバータスクフォース作成

松竹梅のどこかに所属するのかを認識する

システム依存度で対応が大きく分かれる
あなたのシステム依存度はどこの区分か？

区分	システムの依存度	備考
松	システムが止まると、手作業では業務ができない	大企業、中堅企業と同じ対策が必要 ISMS,経営ガイドラインの全面順守 お金がかかるがやむなし
竹	いざとなれば手作業で代替する。 データがあればなんとかなる	メールが使えれば、webが使えれば　なんとかなる。例えば、 請求書や支払い書類はメールに添付ファイルしている、給与台帳は紙で金庫
梅	その場でかんがえても何とかなると思っている。 （しかし、実際はどうしていいかわからないかも）	パソコン1台でこなしている ITリテラシー：システムのことはよくわからない

区分によって、対応が求められる厳しさやお金のかけ方の必要性が変わってくる

出典：ＩＴ・サイバータスクフォース作成

業務の重要度を分ける　①3段階の例示

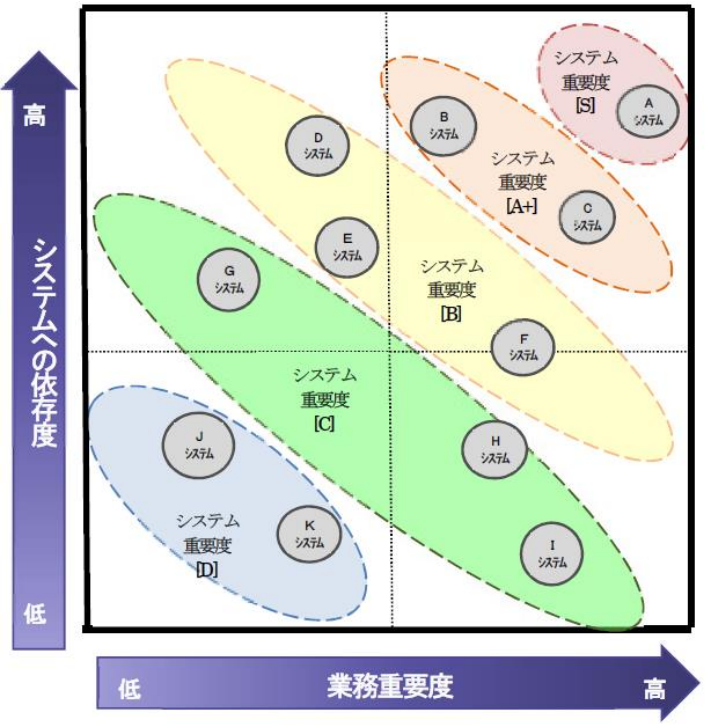
		業務重要度		
		低	中	高
システム依存度	高	B	A	S
	中	C	B	A
	低	D	C	B

RTO（目標復旧時間）	例1	例2	例3
優先復旧 S	0（速やかに）	3時間以内	17時間以内
A	12時間以内	6時間以内	24時間以内
B	24時間以内	24時間以内	3日以内
C	3日以内	72時間以内	7日以内
D	リスク受容	（規定なし）	7日以降

レベル	ヨコ軸（業務重要度）	タテ軸（システム依存度）
3	・対策における根幹業務 ・情報の提供・共有や企業市民として欠かせない業務 ・命・安全にかかわる業務	・他のシステムの仮想化基盤となるシステム ・多人数への情報共有や即時性が求められるシステム ・即時性が求められる業務に関するシステム ・膨大なデータ、高度な抽出する業務や複雑な計算、シミュレーションを必要と知る業務関連システム
2	・被災従業員や顧客が最低限困らないための業務	・システムがないと効率が大幅に落ちるor品質に大幅なばらつきが生じる業務のシステム
1	・上記1，2以外の、災害時対応において比較的不要不急の業務	・データ件数少or処理平易な業務に関連システム ・紙ベースで代替可能な業務システム

出典：表については経産省IC-BCP指針、総務省ICT-BCP指針をＩＴ・サイバータスクフォースにて加筆・修正

業務の重要度を分ける　②5段階の例示



出典：図は総務省ＩＣＴ－ＢＣ構築資料

レベル	横軸（業務重要度）	縦軸（システム依存度）※下記注参照
5	・対策本部根幹業務（被害情報把握、ＳＯＳ発信等） ・勤務者の救出、地域救助要請等	・膨大なデータから複雑条件で抽出する業務 ・複雑な計算等が必要で、人手では品質が大幅低下、または時間膨大となる業務 ・不特定多数と情報連携が前提のシステム
4	・勤務者の安心安全関連業務 衣食住、インフラ復旧、安全/環境/衛生関係　等 ・受援力に関する業務	上記ほどではないが大量データ、高度／複雑な計算/条件抽出、シミュレーション、多数の情報連携必須業務で、人手では品質低下、長時間になる業務関連システム
3	・業務継続や勤務生活再建の前提に関連する業務	・処理は平易だがデータ量が膨大なシステム ・処理が高度で熟練者以外では品質低下するシステム
2	・業務継続や勤務生活関連業務 ・復旧指針に合致する業務	上記ほどではないが効率が下がる、あるいは品質が下がる業務関連のシステム
1	・システム復旧後に入力等の作業をすればよい業務	・延期できる業務のシステム ・不要不急の業務のシステム

※注）社員の「手」では実行不可能な業務を行っているシステム、という回答が各部門（現場）から寄せられる場合もある。
しかしシステムが導入される前は社員の「手」で実施してきた業務であることを念頭にランク審査・選定・レベル分けすべき

出典：表については総務省ICT-BCP構築指針をＩＴ・サイバータスクフォースにて企業向けに加筆・修正

経営者の認識

出典：ＩＴ・サイバータスクフォース作成

7

経営者が負う責任
と
やるべきこと

<目次>

はじめに
第１部　経営者編
第２部　実践編
付録１～７

出典：情報処理推進機構

講演者の個人的見解が含まれます。すべてがBCAOの正式見解ではありません。

1. 情報漏洩が組織に与える影響

- 情報セキュリティ対策を怠ることで秘密情報や個人情報の漏洩による高額な賠償請求や金銭的損失を伴う事故が増加しています。
- 事故による不利益は、情報セキュリティ対策を行うことで、経営上受容できる範囲まで減らすことが出来ます。（漏洩も中断も同様に検討必要）

影　響	内　　容
損害賠償	情報漏洩によって損害が生じた人・組織への損害賠償
対応費用	原因調査・再発防止策のかかる費用、謝罪広告等による広報費用など
機会損失	サービス中断、社会的信用の失墜による売上低下や取引中止など
法的制裁	各国の法令（個人情報保護法・GDPR等）による刑事罰（罰金・入札停止等）

出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

中小企業の被害事例

製造業A社の場合 従業員数50名・年間売上10億円

工場内PCのランサムウェア感染で
生産ラインを1日停止。

想定被害額 *1,040*万円
年間売上の約1%の損害

費用損害
調査・復旧費用　1,000万円

利益損害
逸失利益　40万円

小売業B社の場合 従業員数10名・年間売上3億円

ショッピングサイトへの不正アクセスで1万名分の会員情報が漏えい。
サイトは2週間閉鎖。

想定被害額 *3,570*万円
年間売上の約12%の損害

賠償損害
損害賠償　100万円
訴訟費用　300万円
費用損害
調査・復旧費用　1,650万円
お客様対応費用（お詫び・お見舞金など）
600万円
新聞への社告掲載　500万円
法律相談　20万円
利益損害
逸失利益400万円

出典：損害保険協会

2. 経営者が負う責任

2-1. 経営者に問われる法的責任

◆ 企業が個人情報等の法的な管理義務がある情報を適切に管理していない場合、経営者には次のような刑事罰が科される恐れがあります。

法令	処罰など
個人情報保護法	顧客の個人情報を漏洩させてしまった場合、委員会による立入検査・帳簿等の物件検査及び質問（一年以下の懲役または５０万円以下の罰金）
マイナンバー法	顧客から預かったマイナンバーを漏洩または別用途に使用した場合、違反条項により６月から４年以下の懲役又は５０万円～２００万円以下の罰金
不正競争防止法	顧客の営業機密を漏洩したり不正使用を行った場合に、利益を侵害された者から侵害の停止、又は予防の請求があった場合、損害賠償責任、信用回復措置請求
金融商品取引法	顧客の機密情報を得てインサイダー取引などを行った場合、５年以下懲役若しくは５００万円以下の罰金、犯罪行為により得た財産の没収・追徴
民法	故意又は過失によって他人の権利又は法律上保護される利益侵害した者の損害賠償責任

出典：ＩＴ・サイバータスクフォース作成

2-2. 関係者や社会に対する責任

- 預かった情報を漏洩した場合、法的責任に加えて、その情報の提供者や顧客等の関係者に対する責任が発生します。
- 情報漏洩事故は、営業機会の損失、売上減少、企業のイメージダウンなど、自社に大きな損失をもたらします。

取引先との信頼関係の喪失
業界全体のイメージダウン

↓

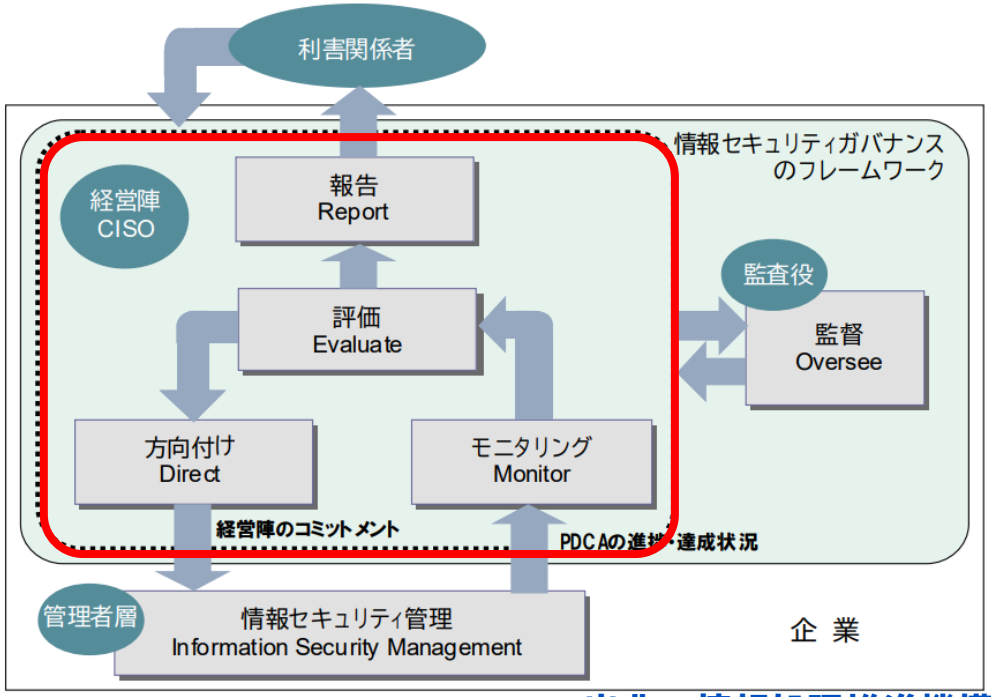
顧客・取引先・従業員・株主等に対する経営責任

出典：情報処理推進機構

3. 経営者がやるべきこと

責任3-1. 認識すべき 「3原則」

- 《原則１》
- 情報セキュリティ対策は、経営者のリーダーシップで進める
- 経営者は、IT活用の推進にあたっては、情報セキュリティ対策の重要性を認識し、自ら リーダシップを発揮して対策を進めることが必要である。



情報セキュリティガバナンスは、経営者が企業の戦略として、情報セキュリティ向上に取組む為の枠組みである。

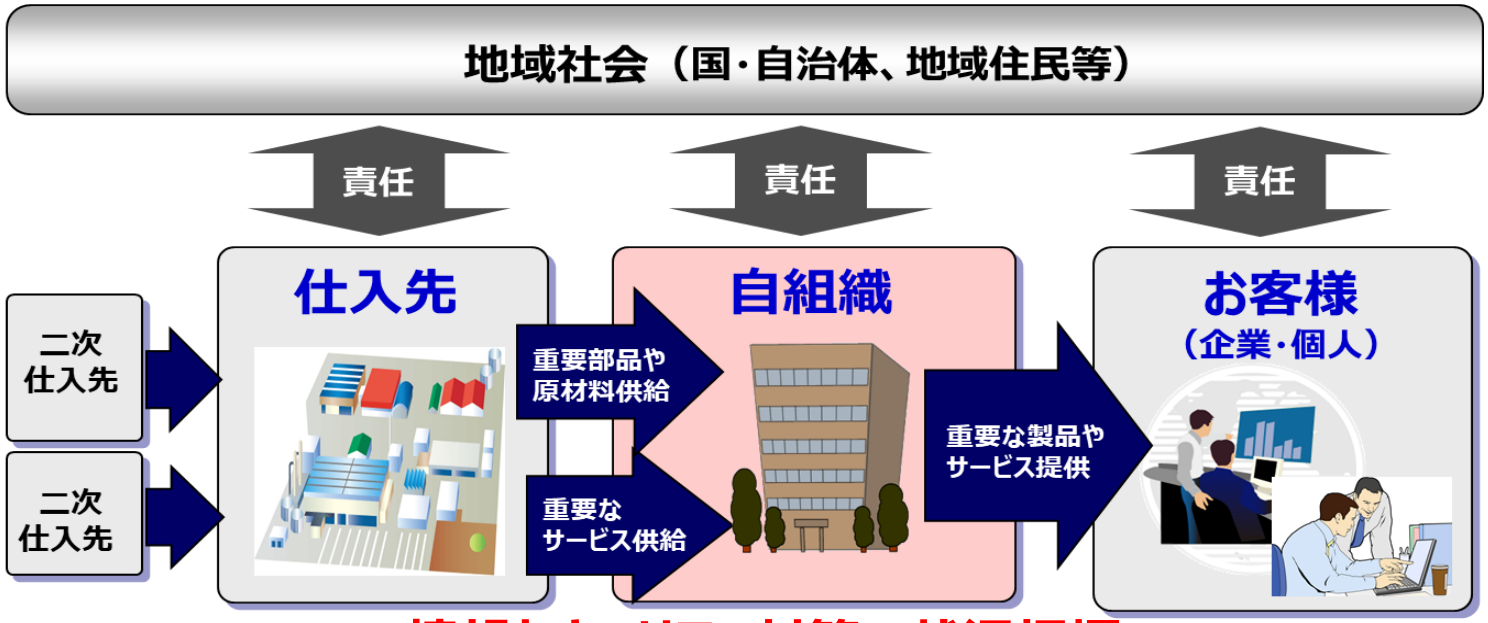
経営者が懸念する重大事故（顧客の個人情報の漏洩、サイバー攻撃によるシステムの停止等）を示して方向付けを行い、対策の進捗や点検により、状況のモニタリングを行いながら評価・見直しを行い、継続的に改善することが重要ある。

出典：情報処理推進機構よりＩＴ・サイバータスクフォース追記

3. 経営者がやるべきこと

- ◆ 《原則２》
- ◆ 　取引先の情報セキュリティ対策まで考慮する
- ◆ 自社は勿論のこと**お客様やビジネスパートナー等**の取引先を含めたサプライチェーン全体（注）に対する情報セキュリティ対策の実施状況を確認し、不十分な場合は、その対処を検討する必要がある。

（注：少なくとも直接取引のある企業を確認し一緒に進めていく）



ー 情報セキュリティ対策の状況把握 ー

出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

3. 経営者がやるべきこと

◆ 《原則３》

◆ 　関係者とは常に情報セキュリティに関するコミュニケーションとる

◆ 平時はもちろん緊急事態発生時のいずれにおいても、情報セキュリティリスクや対策に係わる情報開示など、関係者との適切なコミュニケーションが重要である。

情報セキュリティに関する取組み方針を常日頃より伝えておくことで、サイバー攻撃によるウイルス感染や情報漏洩などが発生した際にも、説明責任を果たすことができ、信頼関係を維持することが出来る。

出典：情報処理推進機構

講演者の個人的見解が含まれます。すべてがBCAOの正式見解ではありません。

3. 経営者がやるべきこと

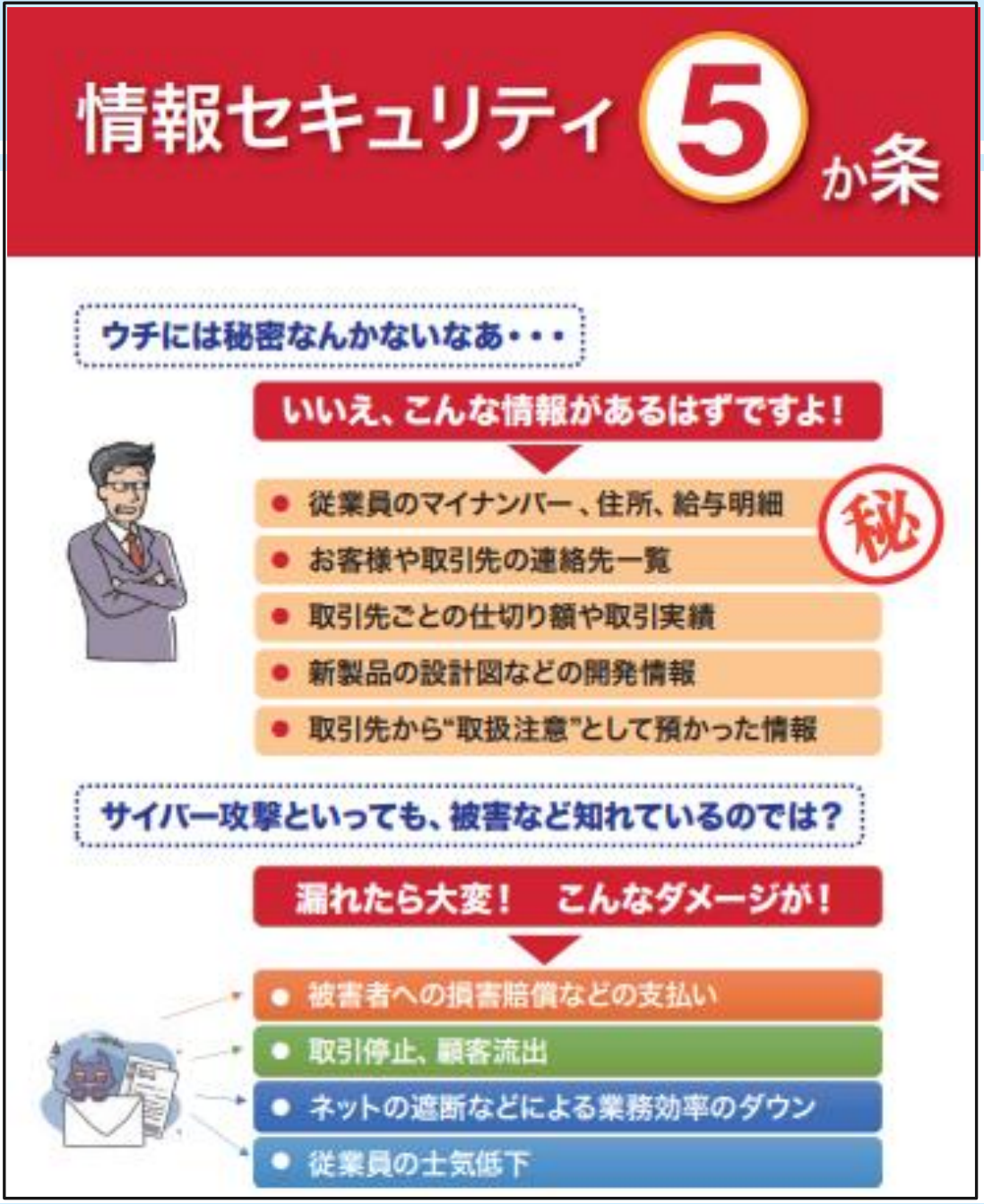
◆3-2. 実行すべき 「重要7項目」 の取組み

◆ 経営者は、重要７項目の取組みについて、自ら実践するか、責任者・担当者に対して指示する。

取組１	情報セキュリティに関する組織全体の対応方針を定める
取組２	情報セキュリティ対策の予算や人材等を確保する
取組３	必要と考えられる対策を検討させて実行を指示する
取組４	情報セキュリティ対策に関する適宜の見直しを指示する
取組５	緊急時の対応や復旧のための体制を整備する
取組６	委託や外部サービス利用の際には、セキュリティに関する責任を明確にする
取組７	情報セキュリティに関する最新動向を収集する

次ページ

出典：情報処理推進機構よりＩＴ・サイバータスクフォース追記



《５か条》

1. ＯＳやソフトウエアは常に最新状態しよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃手口を知ろう！

（一つ星）

（二つ星）

出典：情報処理推進機構

情報バックアップ

出典：ＩＴ・サイバータスクフォース作成

18

情報バックアップ

◆３拍子揃ったバックアップ

「早い」「安い」「旨い」

① 迅速なリストア、セットアップの方法

② お金がかからないバックアップの方法

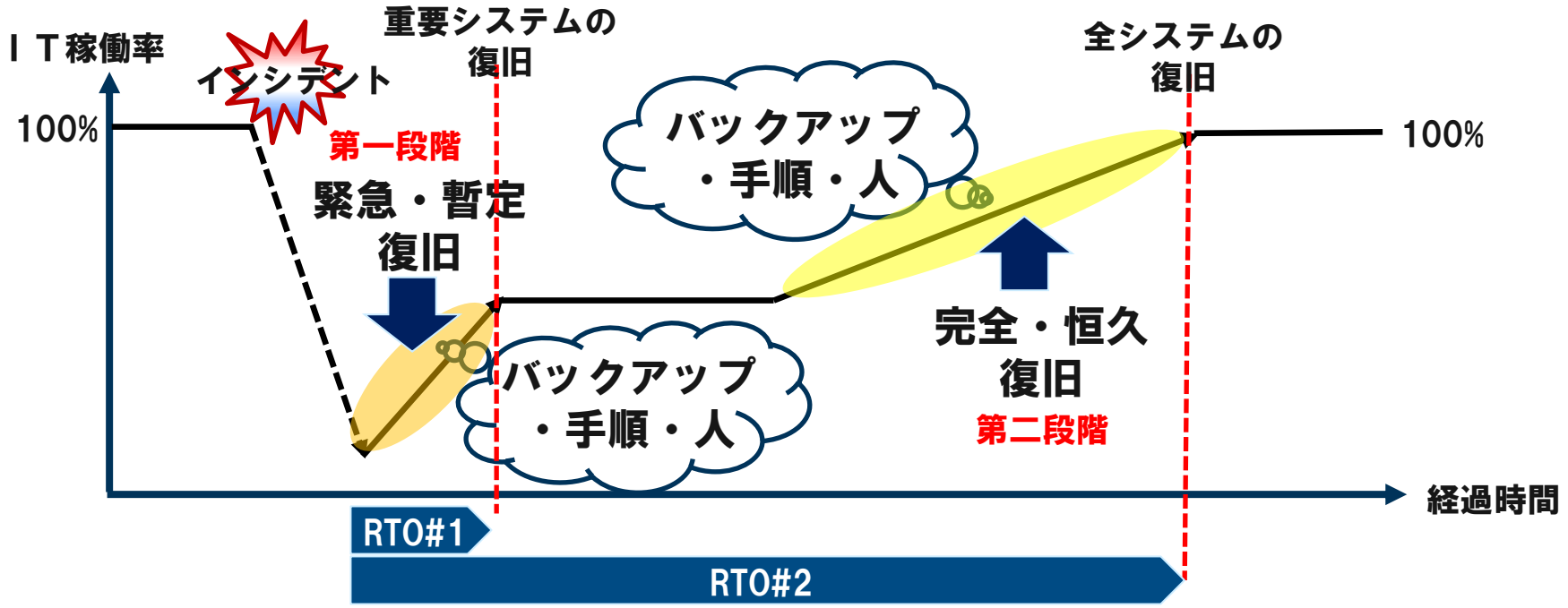
③ 簡単で確実な回復方法

出典；テック・ジェイ大塚

情報バックアップ

◆「全システムの復旧」から逆にたどり、各段階で必要なバックアップ、手順、作業員、連絡指示系統を整理する

図１「インシデント発生から全システム復旧までのながれ



3拍子揃った復旧とは、復旧対象とRTOのメリハリを付けた復旧戦略を作ること　BIAとシステム依存の説明を参照

出典；テック・ジェイ大塚

情報バックアップ

◆ 第一段階　緊急・暫定復旧の手順

◆あらかじめバックアップを持ち、手順書を準備し、平時に定期的に訓練演習を行う。

０．状況の定着確認（状況が落ち着ちついたことを確認）＊注１、注２

１．被害調査

２．バックアップの手配

３．復旧作業

４．ITサービス回復、業務再開

- ◆ ＊注１；先行して２．バックアップの手配を行うことは可能
- ◆ ＊注２；復旧中の２次災害（被害）を避けるために状況定着を確認することが重要
- ◆ バックアップシステムは重要システムをとりあえず稼働させる考えのため本番システムより「縮退」構成となることが多い
- ◆ 事前にバックアップしたデータを戻す場合、バックアップした時点から直近までに発生したデータはシステムから失われるので、回復後、再度システムに入力が必要になる。

出典；テック・ジェイ大塚

情報バックアップ

◆　第二段階　完全・恒久的復旧方法

◆本番システムを回復して緊急・暫定システムから切り戻す。たいがい、被災調査後に実施計画を策定する場合が多い

1．被害調査
2．被災したIT資源の入れ替え、回復
3．計画的業務一時中断、緊急・暫定復旧システムからのバックアップ
4．アプリ＆データのリストア
5．稼働の確認
6．完全・恒久システムへの切り戻し
7．業務継続

出典；テック・ジェイ大塚

情報バックアップ

◆バックアップ対象、５つのＩＴ構成要素

【クライアント側】		【サーバー側】
オペレータ、操作手順書	第五層 人	運用オペレータ、運用手順書、指示命令系統
パソコンアプリ＆データ、	第四層 ソフト	各サーバーのアプリ＆データ＆システムバックアップ
パソコン、Prt、管理サーバ	第三層 ハード	ドメインサーバ、アプリサーバ DBサーバー
電気、通信回線・機器	第二層 インフラ	電気ガス水道、通信回線・機器
オフィス・作業場	第一層 建屋	データセンター建屋

インシデントによって被災対象（復旧しなければならないもの）が変わります

（例）戦争、地震災害、火災、長期間の停電、ネットワーク異常、ランサムウエア、ＩＴ障害、感染症によるＩＴ要員の不足

出典；テック・ジェイ大塚

情報バックアップ

◆松・竹・梅ケースの対応例

松

- ＩＴシステムの棚卸しを行い**システム管理台帳**を整備した。
  不要、老朽化システムの廃止を行った
- **外部サービス（クラウド）**利用を検討しＩＴ予算の圧縮を実現するとともに
  新たにバックアップ契約をした
- **３－２－１バックアップ**に基づきアプリ・データバックアップ運用を見直した

竹

- **メール、SNS、Webアクセス**を重要システムとし、被災時に復旧可能にする
  バックアップを計画・実施した
- **ファイルサーバ構築**し重要文書を保管しそのバックアップを検討・構築した
- ランサムウエアに備え、３－２－１バックアップに基づきアプリ・
  データバックアップ運用を見直した

梅

- 日常のセキュリティの見直しと強化
- 停電に備え**簡易的な発電機、蓄電装置を追加した**
- 人のバックアップとしてアプリの**ログオンユーザーIDとパスワードの保管**と
  緊急時の**引き出し手順**を決めた（本人以外の人）
- 信頼できる外部ベンダーによるバックアップデータ遠隔地保管サービスを採用

３－２－１バックアップ；３、本番以外2つのバックアップコピーを保持、２つの異なる媒体にバックアップする、１つはオフライン遠隔地に保管すること

出典；テック・ジェイ大塚

IT・情報セキュリティ

出典：ＩＴ・サイバータスクフォース作成

25

業務・業種による自社のITの依存度

種別	システムの依存度	取るべき情報セキュリティ対策
松	システムが止まると、手作業では業務ができない	➢ 体制・規程整備 ➢ ゼロトラスト対策 ➢ 全従業員向けEラーニング ➢ 標的型攻撃メール訓練 ➢ 脆弱性診断 ➢ 各種認証取得（ISMSなど）
竹	いざとなれば手作業で代替する。データがあればなんとかなる	➢ 公的リファレンスによる対策 • 体制・規程の整備 • リスクアセスメント、対策実施 ➢ 全従業員向けEラーニング
梅	その場でかんがえても何とかなると思っている。 （しかし、実際はどうしていいかわからないかも）	➢ 「情報セキュリティ5か条」の実施 ➢ 外部媒体へのデータバックアップ

出典：ＩＴ・サイバータスクフォース作成

お金がかからないIT・情報セキュリティの方法

◆ 公的リファレンス利用による体制・規程の整備

- ➢ まずは政府、公的機関が発行しているガイドラインを利用
  - 「サイバーセキュリティ経営ガイドライン」
    本編の他に解説書、実践のための
    プラクティス集も用意されている

サイバーセキュリティ経営ガイドライン Ver 2.0実践のためのプラクティス集

- 「中小企業の情報セキュリティ対策ガイドライン」
  各種付録、説明資料、動画コンテンツもあり

出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

お金がかからないIT・情報セキュリティの方法

◆ OS、ソフトウェアの最新化

→ゼロデイ攻撃被害よりセキュリティパッチ未対応による被害の方が多い

セキュリティパッチの対応状況を確認するには

「MyJVNバージョンチェッカー」（無償提供）

◆ 従業員のセキュリティ教育（Eラーニング）

→情報処理推進機構（IPA）が無償で提供

- ※特に「情報セキュリティ啓発 映像コンテンツ」は31本の動画が提供されており、理解しやすい

→無料で学べるオンライン講座gacco（無料）

- 「これだけは知っておきたい無線LANセキュリティ対策」も見る価値あり

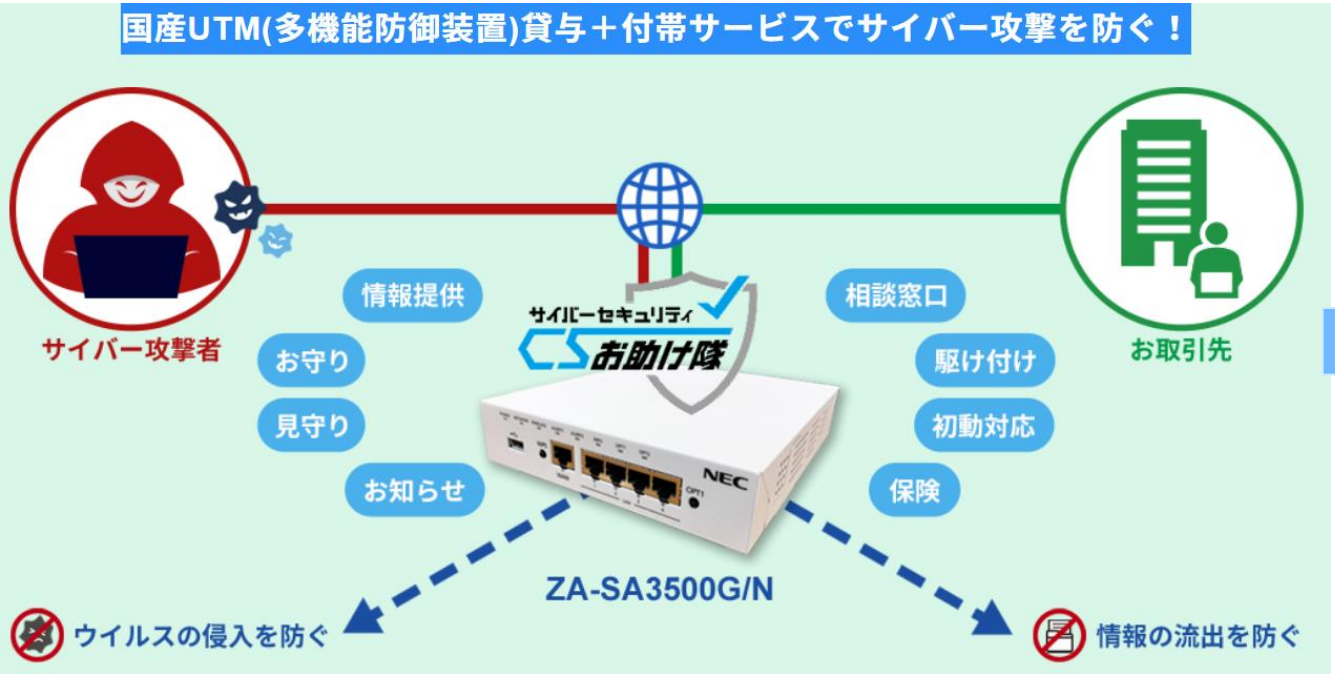
出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

お金がかからないIT・情報セキュリティの方法

◆ サイバーセキュリティお助け隊サービス

情報処理推進機構（IPA）がサイバー攻撃に遭った際の事後対応策支援を中心とした、中小企業向けサイバーセキュリティ対策支援の仕組みの構築を目的とした実証事業「サイバーセキュリティお助け隊事業」を実施

https://www.ipa.go.jp/security/otasuketai-pr/



中小企業でも
導入・維持できる
価格で
ワンパッケージで
提供

【価格例】大阪商工会議所「商工会議所サイバーセキュリティお助け隊サービス」
会員：6,600円／月　非会員：8,250円／月

出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

維持管理

出典：ＩＴ・サイバータスクフォース作成

30

維持管理

◆IT・情報セキュリティ（サイバーテロ）の対策の実施
◆IT・情報セキュリティ（サイバーテロ）の点検
◆IT・情報セキュリティ（サイバーテロ）の是正
◆経営者の見直し
◆社員教育と演習

出典：ＩＴ・サイバータスクフォース作成

社員教育と演習の重要性

出典：ＩＴ・サイバータスクフォース作成

32

社員教育と演習の重要性

- 中小企業の多くのところでは、IT専属の担当者がいない
- 一旦やられてしまったら対応が難しい、お客様にも迷惑を掛ける
- 社長だけが頑張るのではなく、みんなで頑張る

- （１）社員教育
  - ◎　中小企業も狙われていることを社員が認識することが第一歩
  - ◎　普段の言葉を使う。ワナクライ、マルウェア、などは使わない
  - ◎　大原則「変なことするな、おかしかったら社長にすぐ話せ」

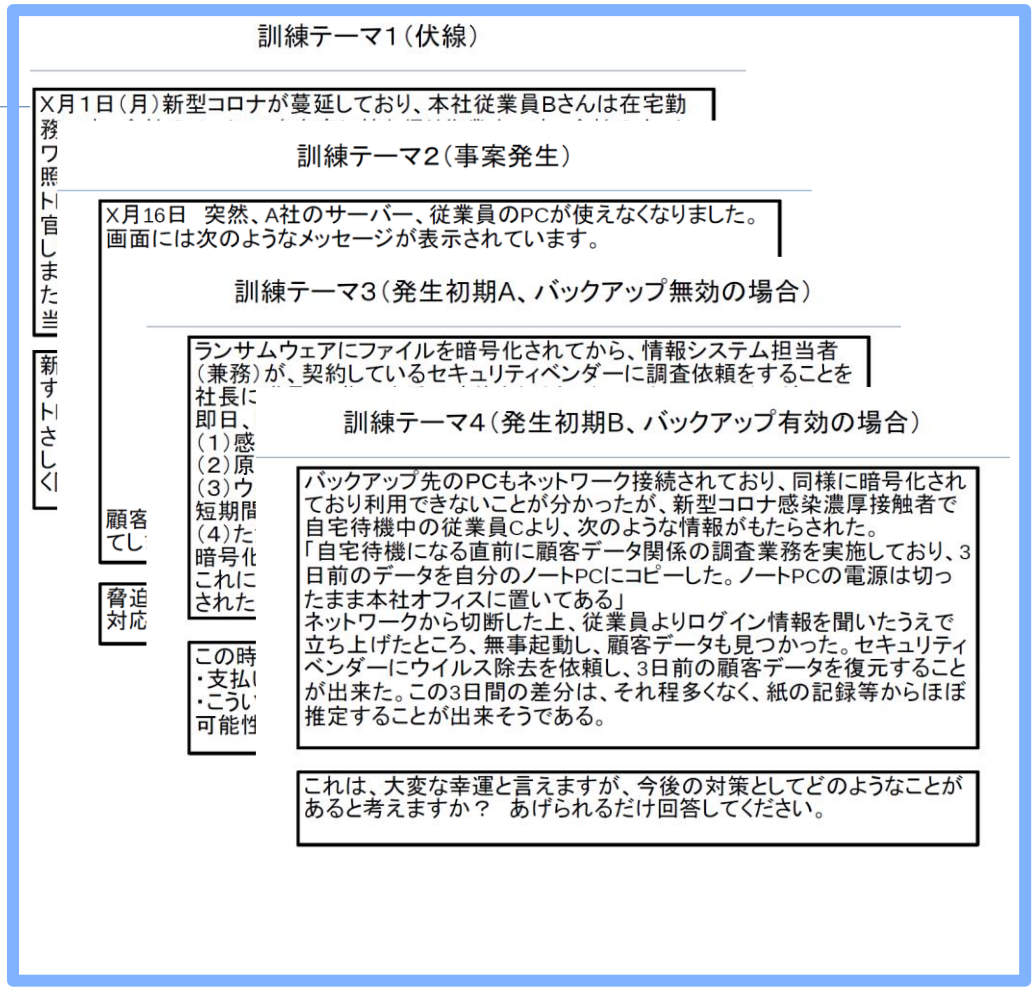
- （２）演習
  - ◎　地震に特化していると、安否確認から始まる。でも？
  - ◎　標的型メール訓練　“松”企業は必要
  - ◎　シナリオ型演習で臨場感を持つことが有効　“松竹梅”全部必要

出典：ＩＴ・サイバータスクフォース作成

オンラインによるサイバー攻撃演習（サンプル）

想定組織・業務等

- 以下のような組織を想定しました。**今回用の全くの仮想のものです。**
  - 対象組織（A社）は個人を対象とするサービス業者（BtoC：例えば、教育、保険などを想定）である。本日は、会員制スポーツジムを想定する。
  - 岡山市に本社事業所があり、本社所在地を含めて近隣数か所にジムがある。従業員数は数十人と想定。
  - 顧客情報を含むの業務データは、本社にあるサーバー上に記録・保管されているが、作業中のデータが従業員のPCにも存在する。バックアップについては、本社内に別PCが設置されている（ここは、設問毎に設定したい）。
  - 本社事業所内では、社内ネットワークにて各自の業務用PCと上記サーバーが接続されている。各ジムにもPCがあり本社サーバーにVPN接続している。
  - 従業員は、個々の電子メールアカウントを所有し、個々の業務利用のPCからインターネットへの接続が出来る。
  - 入会申し込み用のメールアドレスは外部公開されているが、従業員のメールアドレスは公開されていない。
  - インターネット接続は本社経由で行われているが、従業員PCを外部に持ち出し設定をすればネット接続ができる。また、ジムのPCもVPNを外せばネット接続ができる。
  - 本社に情報システム担当者（兼務）が1名いる。
  - セキュリティ事業者（セキュリティソフト提供会社）とのサポート契約を結んでおり、基本的対策は導入済で、緊急時には対策の支援をしてもらうことになっている。



出典：ＩＴ・サイバータスクフォース作成

講演者の個人的見解が含まれます。すべてがBCAOの正式見解ではありません。
34

IT-BCPの様式について

出典：ＩＴ・サイバータスクフォース作成

情報資産のBCPとして備えること

◆1つの対策案は

「中小企業の情報セキュリティ対策ガイドライン」を参考にすること

ガイドライン等のダウンロード

（本編）

- 本編：中小企業の情報セキュリティ対策ガイドライン第3版（全60ページ、32.56MB）
  - 付録1：情報セキュリティ5か条（全2ページ、726KB）
  - 付録2：情報セキュリティ基本方針（サンプル）（全1ページ、35KB）
  - 付録3：5分でできる！情報セキュリティ自社診断（全8ページ、1.9MB）
  - 付録4：情報セキュリティハンドブック（ひな形）（全11ページ、212KB）
  - 付録5：情報セキュリティ関連規程（サンプル）（全51ページ、179KB）
  - 付録6：クラウドサービス安全利用の手引き（全8ページ、2.8MB）
  - 付録7：リスク分析シート（全7シート、99KB）

（付録1）

（付録3）

（付録6）

出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

情報セキュリティ関連規定サンプル

◆特に参考になるのが

3．情報資産管理

10．情報セキュリティインシデント対応ならびに事業継続管理

1	組織的対策	1 ページ
2	人的対策	3 ページ
3	情報資産管理	5 ページ
4	アクセス制御及び認証	8 ページ
5	物理的対策	11 ページ
6	ＩＴ機器利用	13 ページ
7	ＩＴ基盤運用管理	21 ページ
8	システム開発及び保守	25 ページ
9	委託管理	27 ページ
10	情報セキュリティインシデント対応ならびに事業継続管理	34 ページ
11	個人番号及び特定個人情報の取り扱い	40 ページ

（Ver.1.6）

出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

情報資産管理

1.情報資産の管理
- 1.1情報資産の特定と機密性の評価
- 1.2情報資産の分類の表示
- 1.3情報資産の管理責任者
- 1.4情報資産の利用者

2.情報資産の社外持ち出し

3.媒体の処分
- 3.1媒体の廃棄
- 3.2媒体の再利用

4.バックアップ
- 4.1バックアップ取得対象
- 4.2バックアップ媒体の取り扱い
- 4.3クラウドサービスを利用したバックアップ

出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

情報セキュリティインシデント対応ならびに事業継続管理

1.対応体制
2.情報セキュリティインシデントの影響範囲と対応者
3.インシデントの連絡及び報告
4.対応手順
　4.1漏えい・流出発生時の対応
　4.2改ざん・消失・破壊・サービス停止発生時の対応
　4.3ウイルス感染時の初期対応
　4.5届出及び相談
5.情報セキュリティインシデントによる事業中断と事業継続管理
　5.1想定される情報セキュリティインシデント
　5.2復旧責任者及び関連連絡先
　5.3事業継続計画

出典：情報処理推進機構よりＩＴ・サイバータスクフォース作成

留意点

5.情報セキュリティインシデントによる事業中断と事業継続管理

代表取締役は、情報セキュリティインシデントの影響により当社事業が中断した場合に備え、以下を定める。

5.1 想定される情報セキュリティインシデント

以下のインシデントによる事業の中断を想定する。

- 情報セキュリティインシデント：大型地震の発生に伴う設備の倒壊、回線の途絶、停電等による〇〇システム停止
- 想定理由：当社の事業は、商品の販売から請求回収までの業務を〇〇システムに依存しているため、停止した場合は事業の継続が困難になり多大な損失が発生

5.2 復旧責任者及び関連連絡先

被害対象	復旧責任者	関係者連絡先
電源設備 空調機	総務部長	〇〇電力△△支店 (株)〇〇設備
（〇〇システム） ハードウェア ソフトウェア ネットワーク機器 回線サービス バックアップクラウドサーバー	インシデント対応責任者 情報システム管理者	(株)〇〇システム開発 (株)△△ネットワークサービス (株)◇◇マネージドサーバー
顧客	営業部長	営業部取引先リスト参照
従業員人的被害	総務部長	従業員名簿参照

5.3 事業継続計画

インシデント対応責任者は、想定する情報セキュリティインシデントが発生し、事業が中断した際の復旧責任者の役割認識及び関係者連絡先について、有効に機能するか検証する。復旧責任者は、被害対象に応じて復旧から事業再開までの計画を立案する。

引用元のテンプレート中の事業継続計画は、防災や初動中心などの狭義のBCPに寄っている感あり

より個別具体的な復旧プロセスは別途整備する必要がある

既存のBCPを参考に精緻化すべき

ＩＴ／サイバーリスクは漏洩事故対応と密接に関係する特徴もあるため、具体的な復旧・漏洩のプロセス（手順書等）は、BCPの概要文書の下、他のハザードへの対応の手順書とは別に整備することも有効である。

出典：情報処理推進機構より
ＩＴ・サイバータスクフォース作成

ITに強いアドバイザーとの連携

出典：ＩＴ・サイバータスクフォース作成

被災時の対策

◆ある程度対策を行っていた場合

- ➢当該システムの隔離
- ➢空間の作成と警告
- ➢（ITに強いアドバイザーとの連携）

◆行っていなかった場合

- ➢関係省庁、関係する会社への通報
- ➢専門企業への協力依頼
- ➢（ITに強いアドバイザーとの連携）

出典：ＩＴ・サイバータスクフォース作成

被災時の対策

◆一般に企業内で対応できること

◆不審なメールを開かない、添付ファイルや掲載ＵＲＬをむやみにクリックしない、ということを、勤務者、狙われやすい子会社、中小取引企業等への浸透・周知・徹底

専門知識が必要なインシデントハンドリング、セキュリティインシデント対応

組織構築、サイバー演習は**専門業者**に委託することも１つの方法

出典：ＩＴ・サイバータスクフォース作成

中小企業のセキュリティ課題

セキュリティ対策を経営課題としてとらえる

■中小企業における人材不足・情報不足・連携不足■

1）DX、IoT、AIを見据えたIT利活用
2）トレンド情報の入手先・相談先
3）サプライチェーンの一部としてのセキュリティへの取組み

情報処理安全確保支援士（RISS）

出典：ＩＴ・サイバータスクフォース作成

身近にいる相談者 ＝ 情報処理安全確保支援士

「情報処理安全確保支援士」とは、
セキュリティ対策を推進する人材の国家資格です。

サイバーセキュリティ対策の重要性が社会的に高まる中で
それを担う人材の育成・確保のため誕生しました。

■中小企業における人材不足・情報不足・連携不足■

1）DX、IoT、AIを見据えたIT利活用
2）トレンド情報の入手先・相談先
3）サプライチェーンの一部としてのセキュリティへの取組み

中小企業のセキュリティ課題を解決できる人材

出典：ＩＴ・サイバータスクフォース作成

情報処理安全確保支援士はみなさんの近くにいます

「情報処理安全確保支援士」検索サービス
⇒ https://riss.ipa.go.jp/

登録番号	登録年月日	氏名		自宅	更新期限	登録更新回数	試験合格年月	オンライン講習修了年月日	実践講習修了年月日	得意分野	保有スキル	勤務地	勤務先名称
008013	2018年04月01日	大久保	茂人	岡山県	2024年03月31日	1回	2017年12月	2021年12月26日	2020年12月28日	事業継続マネジメント システム企画立案 プロジェクトマネジメント IT運用コントロール 営業業務	コミュニケーション力 （戦略）　システム戦略立案手法 （支援活動）　リスクマネジメント手法 （保守・運用）　ITサービスマネジメント業務管理技術 （支援活動）　情報セキュリティ	岡山県	プラスエス
	2018年				2024年			2020年	2019年	基盤システム構築 運用設計	（システム）　ハードウェアの基礎技術 （システム）　ハードウェアの構築技術		

出典：情報処理推進機構

補助金の活用

出典：ＩＴ・サイバータスクフォース作成

47

令和3年度サイバーセキュリティ対策促進助成事業/東京都中小企業振興公社

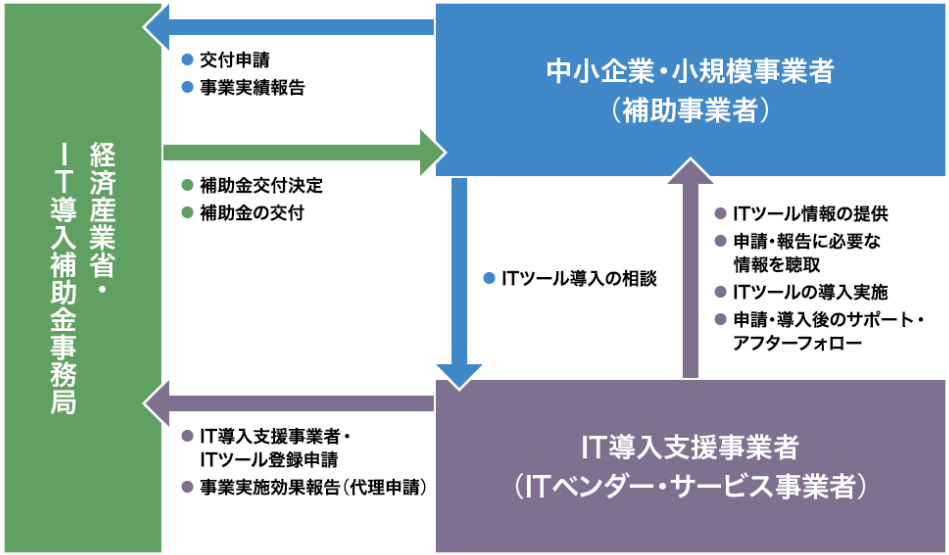
- 中小企業者等が自社の企業秘密や個人情報等を保護する観点から構築したサイバーセキュリティ対策を実施するための設備等の導入を支援する制度。

- 助成対象事業者:IPA(独立行政法人 情報処理推進機構)が実施しているSECURITY ACTIONの2段階目(★★二つ星)を宣言している都内の中小企業者・中小企業団体
- 助成対象経費:サイバーセキュリティ対策を実施するために必要となる下記の機器等の導入、およびクラウド利用に係る経費
  - (1)統合型アプライアンス(UTM等)
  - (2)ネットワーク脅威対策製品(FW、VPN、不正侵入検知システム等)
  - (3)コンテンツセキュリティ対策製品(ウィルス対策、スパム対策等)
  - (4)アクセス管理製品(シングル・サイン・オン、本人認証等)
  - (5)システムセキュリティ管理製品(アクセスログ管理等)
  - (6)暗号化製品(ファイルの暗号化等)
  - (7)サーバー(最新のOS搭載かつセキュリティ対策が施されたものに限る)
  - (8)標的型メール訓練
- 助成率:助成対象経費の1/2以内
- 助成額:1,500万円(下限額　30万円)※標的型メール訓練に関しては別途規定
- 申請方法:事前予約による対面受付

出典；東京都中小企業振興公社

IT導入補助金

◆ IT導入補助金とは、日々のルーティン業務を効率化させるITツールや情報を一元管理するクラウドシステム等、生産性の向上のため業務プロセスの改善と効率化に資する汎用的なITツールの導入に活用できる補助金です。特に、複数の業務工程を広範囲に非対面化する業務形態の転換が可能なIT ツールの導入をしえする制度。



通常枠

	通常枠	
種類	A類型	B類型
補助額	30万～150万円未満	150万～450万円以下
補助率	1/2以内	
プロセス数※1	1以上	4以上
ITツール要件（目的）	類型ごとのプロセス要件を満たすものであり、労働生産性の向上に資するITツールであること。	
賃上げ目標	加点	必須
補助対象	ソフトウェア費・導入関連費等	

※1：「プロセス」とは、業務工程や業務種別のことです。

デジタル化基盤導入類型

種類	デジタル化基盤導入類型	
補助額	ITツール	
	5万円～50万円以下	50万円超～350万円
補助率	3/4以内	2/3以内
対象ソフトウェア	会計ソフト、受発注ソフト、決済ソフト、ECソフト	
賃上げ目標	後日公開予定	
補助対象	ソフトウェア費・クラウド利用料（最大2年分補助）・導入関連費	

＋

ハードウェア購入費用	PC・タブレット等 ：補助率1/2以内、補助上限額10万円
	レジ・券売機等：補助率1/2以内、補助上限額20万円

出典：東京都中小企業振興公社

講演者の個人的見解が含まれます。すべてがBCAOの正式見解ではありません。

テレワーク促進助成金/東京しごと財団

- 助成金の概要
- 在宅勤務・モバイル勤務等を可能にする情報通信機器等の導入により、テレワーク環境を整備する都内中堅・中小企業が支給決定日以後に新たに取り組むもの（発注・契約等を含む）かつ支給決定日から3か月以内に完了する取組みで、実績報告時までに支払いを終えた経費が対象。

事業者の規模（常時雇用する労働者数）	助成金の上限	助成率
30 人以上 999 人以下	250 万円	2 分の 1
2 人以上 30 人未満	150 万円	3 分の 2

- 助成対象事業者の要件
- 1.常時雇用する労働者が 2 名以上かつ 999 名以下で都内に本社または事業所を置く中堅・中小企業等
- 2.都が実施する「テレワーク東京ルール実践企業宣言制度」に登録していること（実績報告時まで）

出典：東京都しごと財団

情報バックアップ、IT・情報セキュリティ（サイバーテロ）対策を実施しつつ

ビジネスチャンスにつなげる

補助金の活用

ものづくり・商業・サービス生産性向上促進補助金

事業再構築補助金

出典：ＩＴ・サイバータスクフォース作成

51

◆まとめ

① 松竹梅をみきわめましょう
② 経営者の肩にかかっています
　担当まかせにせず自ら先頭に
③ まずは、情報セキュリティ5か条（ｐ17）
　からはじめよう

出典：ＩＴ・サイバータスクフォース作成