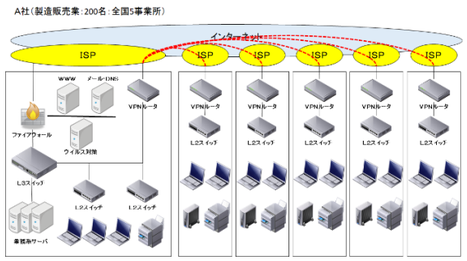
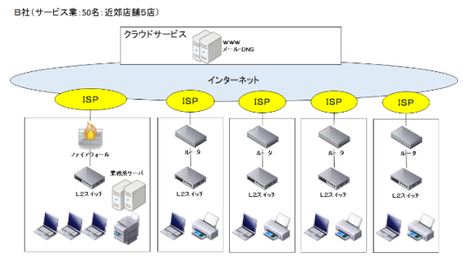
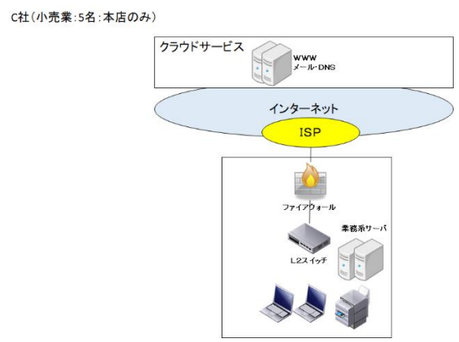
１．モデル企業例

中小企業庁：「中小企業・小規模企業者の定義」

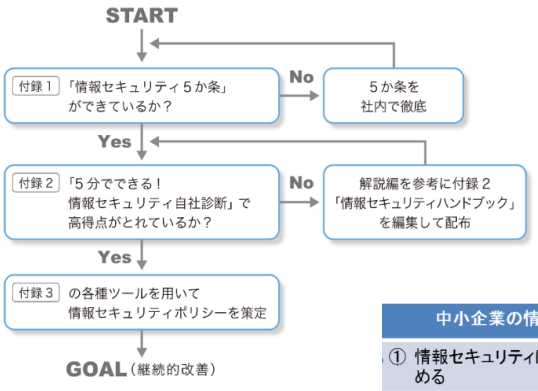
業　種	中小企業者（下記のいずれかを満たすこと）		小規模企業者
	資本金の額又は出資の総額	常時使用する従業員の数	常時使用する従業員の数
①製造業、建設業、運輸業 その他の業種（②～④を除く）	3億円以下	300人以下	20人以下
②卸売業	1億円以下	100人以下	5人以下
③サービス業	5,000万円以下	100人以下	5人以下
④小売業	5,000万円以下	50人以下	5人以下

情報セキュリティ検討対象のモデル企業例

		従業員	拠点	情報セキュリティ担当	情報システム環境	情報システム構成図（例）	主なソフトウェア　（2017年1月現在） （脆弱性対策に特に考慮が必要なソフトウェアの例）
Ａ社	製造販売業	200	全国5事業所	情報システム部門が担当者5名で主に自社のシステム開発・運用が主業務	【導入しているシステム及びサーバ等】 ・販売管理や生産管理、会計、給与等の業務システム用とグループウェア、ファイルサーバなどで数台 【端末台数】 ・従業員の数だけＰＣ有り ・一部の営業担当にはタブレット支給。社外から販売管理システムの利用が可能 【セキュリティ対策】 ・サーバ、ＰＣ、タブレットにウイルス対策 ・外部とのネットワークにファイアウォール ・1台のＰＣでインターネット、メール、社内システム利用 ・会計や給与は担当部署の従業員のみ利用可能		□サーバＯＳ ※下記以外はサポート終了。（ ）内はサポート期限 ・Windows Server 2008（～2020年1月14日） ・Windows Server 2012（～2023年10月10日） ・Windows Server 2016（～2027年1月11日） □クライアントＯＳ ※下記以外はサポート終了。（ ）内はサポート期限 ・Windows 7（～2020年1月14日） ・Windows 8（～2023年1月10日） ・Windows 10（～2025年10月15日） □ブラウザ ※下記以外はサポート終了。 ・Internet Explorer11
Ｂ社	サービス業	50	近郊店舗５店	・以前に情報システム会社にいた従業員1名が総務業務と兼務。 ・主担当は総務業務	【導入しているシステム及びサーバ等】 ・販売管理や会計、給与等の業務システム用とグループウェア、ファイルサーバなどで数台 【端末台数】 ・店舗のＰＯＳとＰＣがそれぞれ1台。 ＰＯＳから販売管理へデータの自動取込。 ・本店の従業員の数だけＰＣ有り、数台。 【セキュリティ対策】 ・サーバ、ＰＣにウイルス対策 ・1台のＰＣでインターネット、メール、社内システム利用		・Microsoft Edge ・Google Chrome ・Firefox ・Safari ・Opera □Officeソフト（表計算、ワープロ等） ・Microsoft Office 2010（～2020年10月13日） ・Microsoft Office 2013（～2023年4月11日） ・Microsoft Office 2016（～2025年10月14日） □その他ソフトウェア ・PDF表示、検索、印刷、操作 （Acrobat Reader等）
Ｃ社	小売業	5	本店のみ	社長が担当。 奥様が会計と給与処理。 販売管理は社長と他の従業員が共用で利用。自分の担当分の処理。	【導入しているシステム及びサーバ等】 ・販売管理、会計、給与等はそれぞれのＰＣで処理 【端末台数】 ・ＰＣ3台 【セキュリティ対策】 ・ＰＣにウイルス対策 ・1台のＰＣでインターネット、メール、社内システム利用		・ファイル圧縮・解凍 （7-Zip、Lhaplus、+Lhaca等）

２．ガイドライン等の（概要）

中小企業の情報セキュリティ対策ガイドライン第2.1版



【図5】本ガイドラインの使用方法

中小企業の情報セキュリティ対策ガイドライン

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
② 情報セキュリティ対策のための資源（予算、人材など）を確保する
③ 担当者に必要と考えられる対策を検討させて実行を指示する
④ 情報セキュリティ対策に関する定期・随時の見直しを行う
⑤ 業務委託や外部サービスを利用する場合は、情報セキュリティに関する責任範囲を明確にする
⑥ 情報セキュリティに関する最新動向を収集する
⑦ 緊急時の社内外の連絡先や被害発生時の対処について準備しておく

情報セキュリティ5か条

① OS やソフトウェアは常に最新の状態にしよう！	OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。 【対策例】 ●Windows Update（Windows OSの場合）/ソフトウェア・アップデート（macOSの場合）/OSバージョンアップ（Android の場合） ●Adobe Flash Player／Adobe Reader／Java実行環境（JRE）など利用中のソフトウェアを最新版にする
② ウイルス対策ソフトを導入しよう！	ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにしましょう。 【対策例】 ●ウイルス定義ファイルが自動更新されるように設定する ●統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)の導入を検討する
③ パスワードを強化しよう！	パスワードが推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。 【対策例】 ●パスワードは英数字記号含めて10文字以上にする ●名前や誕生日、簡単な英単語などはパスワードに使わない ●同じパスワードをいろいろなウェブサービスで使い回さない
④ 共有設定を見直そう！	データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えています。 クラウドサービスや機器が、無関係な人に共有されていないか設定を確認しましょう。 【対策例】 ●クラウドサービスの共有範囲を限定する ●ネットワーク接続の複合機やカメラ、ハードディスク（NAS）などの共有範囲を限定する ●従業員の異動や退職時に設定の変更（削除）漏れがないように注意する。
⑤ 脅威や攻撃の手口を知ろう！	取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。 【対策例】 ●IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る ●利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

ネットワークビギナーのための情報セキュリティハンドブックVer2.11

４つのポイントでセキュリティを守る

１．システムを最新に保つ。セキュリティソフトを入れて防ぐ
　〇セキュリティソフトを導入して守りを固めよう
　〇パソコン本体とセキュリティの状態を最新に保とう
　〇スマホやネットワーク機器も最新に保とう
　〇ソフトやアプリは信頼できる場所から。権限にも気をつける

２．複雑なパスワードと多要素認証で侵入されにくくする
　〇パスワードの安全性を高める
　〇パスワードの使い回しをしない
　〇パスワードを適切に保管する
　〇秘密の質問にはまじめに答えない。多要素や生体認証を使う

３．攻撃されにくくするには侵入に手間（コスト）が係るようにする

４．心の隙を作らないようにする（対ソーシャルエンジニアリング）

その他
・無線LANを安全に使用する（設定、暗号キー）
・Webを安全に利用する（暗号化通信、EV-SSL証明書、サイバー攻撃、二段階認証）
・メールを安全に利用する（スパム、暗号化）

〇自社の環境でどの脅威が起こりうるか？

〇これらの脅威から守る対策はどのような対策が必要か？

サイバーセキュリティ経営ガイドラインＶｅｒ１．１

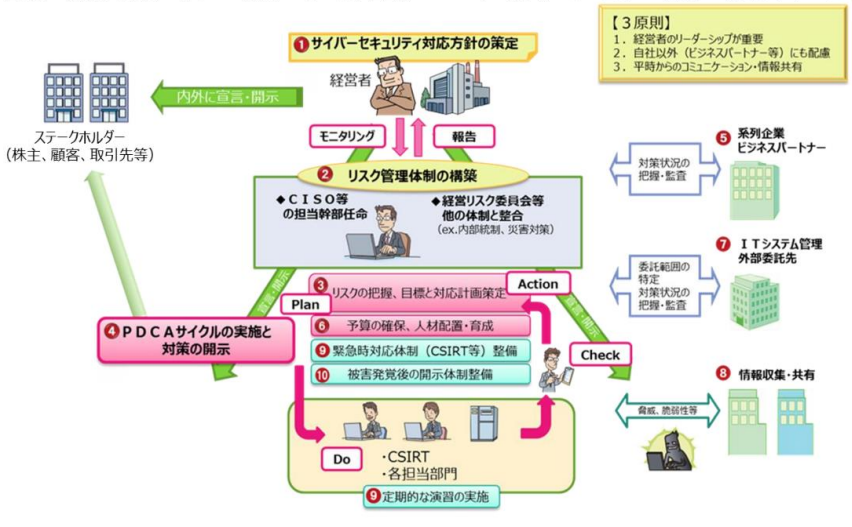
表　０－１　本解説書の構成と想定読者

本ガイドラインの重要 10 項目	本解説書における 10 項目の略称	想定読者	
		経営者	CISO 等
–	0．はじめに	○	○
1．サイバーセキュリティリスクの認識、組織全体での対応の策定	1．サイバーセキュリティ対応方針の策定		○
2．サイバーセキュリティリスク管理体制の構築	2．リスク管理体制の構築		
3．サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定	3．リスクの把握、目標と対応計画策定		
4．サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示	4．PDCA サイクルの実施と対策の開示		
5．系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握	5．系列企業・ビジネスパートナーの対策実施及び状況把握		
6．サイバーセキュリティ対策のための資源（予算、人材等）確保	6．予算確保・人材配置及び育成		
7．IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保	7．IT システム管理の外部委託		
8．情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備	8．情報収集と情報共有		
9．緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施	9．緊急時対応体制の整備と演習の実施		
10．被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備	10．被害発覚後の必要な情報の把握、開示体制の整備		

11月16日に
Ver2.0が公表

付録１ ガイドラインの３原則と重要 10 項目概要図

経営者が認識する必要がある「３原則」に基づき、経営者が CISO 等に指示すべき「重要 10 項目」の概要を以下に示します。



情報セキュリティ１０大脅威２０１７（組織）

第1位　標的型攻撃による情報流出
特定の組織に対して、メールの添付ファイルやウェブサイトを利用してPCにウイルスを感染させ、そのPCを遠隔操作して、別のPCに感染を拡大し、最終的に個人情報や業務上の重要情報を窃取する

第2位　ランサムウェアによる被害
PCやスマートフォンにあるファイルの暗号化や画面のロックを行い、復旧させることと引き換えに金銭を要求する手口に使われるウイルス

第3位　ウェブサービスからの個人情報の窃取
ウェブサービスの脆弱性を悪用し、ウェブサービス内に登録されている住所や氏名やクレジットカード情報が窃取され悪用される

第4位　サービス妨害攻撃によるサービスの停止
攻撃者に乗っ取られたIT機器等から構成されたボットネットにより、企業や民間団体等、組織のウェブサイトや組織の利用しているDNSサーバーに大量のアクセスを行うDDoS（分散型サービス妨害）攻撃されサービスや業務が停止

第5位　内部不正による情報漏えいとそれに伴う業務停止
組織内部の職員や元職員による、情報の不正な持ち出し等の不正行為により情報漏えい

第6位　ウェブサイトの改ざん
コンテンツ管理システム（CMS）等に存在する脆弱性を悪用し、ウェブサイトが改ざんされること。
復旧までウェブサイトを停止することになり、特にオンラインショッピング等を運営している場合、事業上の被害が大きい。
また、閲覧者がウイルスに感染するように改ざんされた場合、社会的信用を失うことにつながる。

第7位　ウェブサービスへの不正ログイン
ウェブサービスへの不正ログインの多くがパスワードリスト攻撃によって行われている。
ウェブサービスの利用者がパスワードを使い回している場合、不正ログインが行われる恐れがある。

第8位　IoT機器の脆弱性の顕在化
自動車や医療機器の脆弱性が昨年に続いて公表された。またIoT（Internet of Things）機器の脆弱性を悪用してボット化することで、インターネット上のサービスやサーバーに対して大規模なDDoS攻撃が行われる

第9位　攻撃のビジネス化（アンダーグラウンドサービス）
犯罪に使用するためのサービスやツールがアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている。
攻撃に対する専門知識に詳しくない者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がる恐れがある。

第10位　インターネットバンキングやクレジットカード情報の不正利用
ウイルス感染やフィッシング詐欺により、インターネットバンキングの認証情報が攻撃者に窃取され、正規の利用者になりすまし、不正送金や不正利用される

３．情報セキュリティ対策の進め方

は『中小企業の情報セキュリティ対策ガイドライン第２．１版』に記載されている事項

ステップ１

経営者に
情報セキュリティリスク対策の必要性を
認識し理解してもらう

おわりに　本書で用いている用語の説明

情報セキュリティとは
「情報の機密性、完全性、可用性を維持すること」

企業の取引情報、経営情報、顧客情報などの重要な情報が、
〇社外に漏洩（ろうえい）したり、（関係者以外にもれる）
〇社外から盗み見られたり、（関係者以外がアクセスできる）
〇改ざん、破壊されたり、（情報が書き換えられる、壊される）
〇必要な時に、必要な情報が見られない
このようなことが起きないようにすること

第１部－１．情報セキュリティ対策を怠ることで企業が被る不利益

情報セキュリティの被害を受けると
〇情報が漏洩（ろうえい）すると
・取引先や顧客への二次被害
・取引先や顧客から損害賠償請求
・情報システムなどの利用差し止めによる業務停滞
・管理責任を問われ社会的評価の低下
・企業のイメージや信用の失墜

〇情報が改ざん・破壊されると
・情報システムが利用できないことによる業務停滞
・情報の復旧にかかる費用
・取引先や顧客へ情報の再提出依頼による信用の失墜

〇情報が必要な時に見られないと
・情報システムが利用できないことによる業務停滞
・ホームページなど社外に提供しているものであれば
取引先や顧客への信頼の失墜
・機会損失による売り上げ低下

〇共通して
・情報セキュリティ事故対応に伴う従業員の
・従業員のモチベーションの低下

ステップ２

経営者、情報セキュリティ責任者に
自社の情報セキュリティリスクを
認識し理解してもらう

■ＩＴＣ備後　追加事項

自社の環境を整理する
自社の環境がどのようになっているかを知り、
脅威にはどのようなものがあるのか、
自社の環境では、どのような脅威が想定されるのか
を知る
〇自社の環境整理（システム構成図など）
・パソコンやサーバ等の情報機器にはどのようなものがあるか
・それらはどのようなネットワーク（通信回線）につながっているか
・情報機器にはどのようなソフトウェアが入っているか
・情報機器は、だれが、いつ、どこで、使っているか
〇どのような脅威があるか
・「情報セキュリティ10大脅威（毎年公表される）
〇自社の環境ではどのような脅威が想定されるか
・「別紙　情報セキュリティ　脅威：対策（案）表」に記載して確認する

第2部－１．情報セキュリティ管理実践の進め方

どのような情報資産があり、想定される脅威（前記）を特定した上で、対策を検討する
〇「情報セキュリティ５か条」
・基本的な対策が、現在の自社の環境でどこまでできているかを確認する
〇「５分でできる！情報セキュリティ自社診断」
・従業員の対策や組織の対策についても、現在、自社でどこまでできているかを確認する
（Part1基本的対策は「情報セキュリティ5か条」と同じ）

別紙「情報セキュリティ　脅威：対策（案）表」
別紙「情報セキュリティ対策　事例（案）」
を利用する

ここまでで、
〇情報セキュリティ対策の必要性
〇自社の情報セキュリティの脅威
〇自社の情報セキュリティ対策の現状
を理解する

ステップ３

経営者、情報セキュリティ責任者に
情報セキュリティリスク対策を誰に、何をやってもらうかを
認識し理解してもらう

第１部－３．経営者は何をすればよいか

取組３：担当者に必要と考えられる対策を検討させて実行を指示する
事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な**対策を検討**させます。
検討した対策ごとに**予算**を与え、担当者を任命し、実行を指示します。
実施する対策は、**社内ルールとして文書**にまとめておけば、従業員も実行しやすくなり、
取引先などにも取り組みを説明する際に役に立つので、併せてしじします。
★この時点で
「自社の脅威とリスク」
「対策案と予算案」
「対策方針」⇒　情報セキュリティポリシー
「実施する対策、決定予算、実施スケジュール」
⇒　情報セキュリティ対策実施計画
「社内ルールの文書化」
⇒　情報セキュリティ実施手順、説明会資料

第2部－４．情報セキュリティポリシーの策定

情報資産台帳を作成する
「付録の資料を使い診断を行う」
・情報資産管理台帳：記入しその資産の重要度を評価
・脅威状況シート：資産台帳の基準となる想定脅威を設定
・対策状況チェック：資産台帳の基準となる想定脆弱性を設定
・診断結果：ポリシーで規定するか否かが分かる

★このツールでは情報セキュリティポリシーで規定するかどうかのみ分かる

第2部－４．情報セキュリティポリシーの策定

手順４情報セキュリティポリシーを策定
（４）情報セキュリティ対策の実行
【各階層の役割】
経営者　　：　予算・人材の確保、方針の策定、
管理者への指示、状況の確認
管理者層　：　ポリシーの説明・改善、監視
一般従業員　：　定められた対策の実行

ステップ４

情報セキュリティ責任者、担当者に
情報セキュリティ対策を
実践してもらう

第２部－１．情報セキュリティ管理実践の進め方

「中小企業の情報セキュリティ対策ガイドライン」の使用方法
付録１：「情報セキュリティ５か条」ができているか？
⇒５か条を社内で徹底
付録２：「５分でできる！情報セキュリティ自社診断」で
高得点がとれているか？
⇒「情報セキュリティハンドブック」を編集して配布
付録３：「情報セキュリティポリシー」を策定

★上記ガイドラインの手順でも良いが・・・
「脅威：対策（案）表」にて
〇どのような対策をすべきか
〇どのくらいの期間が必要か
〇どのくらいの費用が掛かるか
を「情報セキュリティ対策実施計画」を作る
それに従い進める

第2部－３．３　5分でできる！情報セキュリティ自己診断

情報セキュリティ対策実施計画の考え方
「情報セキュリティ自己診断」から

基本的対策：技術的・物理的な対策
（例）ソフトウェアのアップデートの自動化、
ウイルス対策ソフトの適用、最新化の自動化
従業員としての対策：従業員の振る舞いとしての対策
（例）教育・研修、情報セキュリティ規定・実施手順
組織としての対策：情報セキュリティ方針、契約内容、順守規定等の対策
（例）情報セキュリティポリシー、従業員誓約書、
就業規則、取引先契約

〇「情報セキュリティ対策実施計画」の策定・実施の考え方
・優先順の決め方
・情報セキュリティ対策の実施方法
など

ステップ５

経営者、情報セキュリティ担当者に
情報セキュリティ対策の実施状況を
評価・改善してもらう

第２部－５．情報セキュリティ対策のさらなる改善に向けて

(1)情報セキュリティマネジメントサイクルによる継続的改善
(2)情報セキュリティ対策に関する標準規格
(3)情報セキュリティ監査・点検の実施

★上記ガイドラインの手順で・・・
〇監査や点検はどうするか？
・「情報セキュリティ自社診断」を継続的に行う？
〇新たな脅威やリスクをどう反映していくか？
・毎年１０大脅威の確認
・IPAの情報セキュリティのメルマガ
〇自社の環境の変化にどう対応するか？

４．情報セキュリティ 脅威：対策（案）表

自社の環境で該当する箇所に○印を付け
それに該当する脅威を認識し対策を行う

２０１８年版が発表されているが、詳細の
公表は２０１８年３月末なので公表され

自社の環境で●印の箇所に左の脅威が起こりうる可能性

起こりうる脅について右の対策を行う（対策内容は別紙「情報セキュリティ対策事例（案）」参照）

脅威				環境												対策（案）																				
																基本的対策					従業員としての対策									組織としての対策								
				社外メール	Web閲覧	WEBサービス利用・提供	ホームページ有	LAN無線	取引先と情報交換有り	私物の機器を利用	社外から接続している環境がある	IoT機器利用	インターネットバンク等			①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲	⑳	
				自社環境												【脆弱性対策】OSやソフトウェアは常に最新の状態にしよう！	【ウイルス対策】ウイルス対策ソフトを導入しよう！	【パスワード管理】パスワードを強化しよう！	【機器の設定】共有設定を見直そう！	【情報取集】脅威や攻撃の手口を知ろう！	【電子メールのルール】見覚えのないメールは疑ってみる	【無線LANのルール】無線LANの盗聴や無断使用を防ぐ	【Web利用のルール】インターネットを介したトラブルを防ぐ	【バックアップのルール】不足の事態に備えてバックアップ	【保管のルール】重要情報の放置を禁止する	【持ち出しのルール】重要情報は安全な方法で持ち出す	【事務所の安全管理】機器・備品の盗難防止対策を行う	【情報の安全な処分】重要情報は復元できないように消去する	【守秘義務の周知】従業員に守秘義務について理解してもらう	【従業員教育】従業員の定期的な教育を行う	【私物機器の利用】個人所有端末の業務での利用可否を決める	【取引先管理】取引先に秘密保持を要請する	【外部サービスの利用】信頼できる外部サービスを使う	【事故への備え】事故に備えて事前に準備する	【ルールの整備】情報セキュリティ対策をルール化する
分類	脅威	手口等	No.																																	
１０大脅威2017（組織）	(1)標的型攻撃による情報流出	メールからウイルス感染「ばらまき型」「やり取り型」	1																																	
		Webからウイルス感染「水飲み場型」	2	●	●	●	●				●					■	■	■	■	■	■		■		■				■				■		■	■
		標的組織の関連会社が踏み台に	3																																	
	(2)ランサムウェアによる被害	メールの添付ファイルやリンクからランサムウェア感染	4																																	
		Webからランサムウェアに感染（脆弱性等を悪用）	5	●	●	●	●		●	●	●					■	■	■	■	■	■		■	■	■				■	■				■	■	■
		感染したPCだけではなく、共有サーバー等別の機器にも影響	6																																	
	(3)Webサービスからの個人情報の窃取	共通的に使われるソフトウェア（OpenSSL,Apache,Struts,WordPress等）の脆弱性を悪用	7																																	
		Webアプリケーションの脆弱性を悪用	8			●				●	●					■	■	■	■	■			■	■	■				■	■		■	■	■	■	■
		リモート管理用のサービスから侵入	9																																	
		顧客情報の窃取やその情報の悪用	10																																	
	(4)サービス妨害攻撃によるサービスの停止	ボットネットの利用	11																																	
		リフレクター攻撃（脆弱なルーター等に対して応答先を偽って通信）	12			●	●				●					■	■	■	■	■			■						■			■	■	■	■	■
		DNS水責め水責め攻撃（権威DNSサーバーに負荷を掛ける攻撃）	13																																	
	(5)内部不正による情報漏えいとそれに伴う業務停止	職場環境や処遇の不満 処遇面（業務多忙、給与）の不満や復讐等の個人的な利益の享受を目的	14																																	
		アクセス権限の不適切な付与 必要以上なアクセス権の付与等	15	●	●	●		●	●	●	●							■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
		システム操作記録と監視の未実施 不正に気づきにくく、不正の発覚が遅れる	16																																	
	(6)Webサイトの改ざん	ソフトウェアやWebアプリケーションの脆弱性を悪用	17																																	
		リモート管理用のサービスからの侵入	18			●	●				●					■	■	■	■	■			■	■					■			■	■	■	■	■
		ウイルス感染や主義主張・自己顕示に悪用される	19																																	
	(7)Webサービスへの不正ログイン	パスワードの推測攻撃	20																																	
		パスワードリスト攻撃（別サービスから窃取したIDやパスワード）	21			●				●	●					■	■	■	■	■									■								
		サービスに不正ログインされ、個人情報の窃取やポイントを不正利用される	22																																	
	(8)IoT機器の脆弱性の顕在化	IoT機器の脆弱性を悪用してウイルスに感染させる	23																																	
		ウイルス感染後、Ddos攻撃を行い組織のサービスを妨害する	24										●			■	■	■	■	■									■				■		■	■
		不正利用や情報窃取される場合も	25																																	
	(9)攻撃のビジネス化（アンダーグランドサービス）	アンダーグラウンドで売買されているツール・サービスを購入・レンタル	26	●	●	●				●	●					■	■	■	■	■	■		■	■	■				■	■		■	■	■	■	■
		ツールの機能により様々な被害	27																																	
	(10)インターネットバンキングやクレジットカード情報の不正利用	ウイルスに感染したパソコンが不正送金の被害に遭う	28	●	●	●							●			■	■	■	■	■	■		■							■			■	■	■	■
		フィッシング詐欺により入力した認証情報が窃取される	29																																	

５．情報セキュリティ対策　事例（案）

対策（案）			具体策（例）※IPA資料を基に作成	投資概要
基本対策	①	【脆弱性対策】 OSやソフトウェアは常に最新の状態にしよう！	●利用しているソフトウェアを常に最新版にする 取り組み：自動更新の設定にする。 脆弱性情報（IPAメルマガ等）による更新 サポート終了ソフトの更新 対象例：別紙「モデル企業例」の主なソフトウエア参照 留意事項：ソフトウェアを最新版にすることで利用しているものが正常に動かなくなることも考えられるので事前に確認すること	○自動更新の設定のみであれば作業のみで自社で行う場合は投資の必要はない ○サポートが終了しているソフトウェアは買い替えが必要
			●対象機器が多い場合は、 【理由】 ・ネットワーク負荷が増大する ・適切に更新されているかの管理工数大 【対策】 ・WSUS（Windows Server Update Services）など社内に更新サーバを設けるなど対策を行う ・資源管理ツールなどを利用し対象機器が適切に更新されているかを管理する	○社内用更新サーバや資源管理ソフトなどの投資が必要
	②	【ウイルス対策】 ウイルス対策ソフトを導入しよう！	●全ての機器にウイルス対策ソフトを導入し、ウイルス定義ファイルを常に最新にする 取り組み：ウイルス定義ファイル等を自動更新するように設定する。 ウイルス定義ファイルができる前に侵入したウイルスを検知するために定期的に全てのスキャンを実行する。 特記事項：総合セキュリティ対策ソフトはウイルス対策のみならず、迷惑メール、フィッシング対策、Webサイト安全対策などの機能があるものがあるので機能を確認して導入すると良い。	○ウイルス対策ソフトの購入又は更新契約 （注）無償や安価なソフトは個人使用で企業では使用できないものがほとんどなので注意が必要。 （特）Windows Defenderでも相応のウイルス対策は出来るので機能を確認して利用すると追加投資は必要ない。
			●対象機器が多い場合は、 【理由】 ・ネットワーク負荷が増大する ・適切に更新されているかの管理工数大 【対策】 ・ウイルス対策サーバなど社内に更新サーバを設けるなど対策を行う ●モバイル機器がある場合は、それも対策をすること	○社内用更新サーバなどの投資が必要 ○モバイル機器がある場合は、そのライセンスも必要となる。 モバイル機器対応の総合セキュリティ対策ソフトなどにすること投資を低減できる
	③	【パスワード管理】 パスワードを強化しよう！	●強固なパスワードを使用する 取り組み：10文字以上の英数字記号を組み合わせる 名前、電話番号、誕生日などは使わない 複数のWebサービスで同じパスワードを使いまわさない 定期的（3～6ヶ月）にパスワードを変更する 参考：総合セキュリティ対策ソフトではパスワード管理機能があるものがあるので利用を検討しても良い	○取り決めと適正な運用だけなので投資は必要ない
			●多くのID/パスワードを運用しないといけない場合は、Active Directoryの利用や統合認証システムなど検討するのも良い ●より強固なアクセス管理を行う場合は、生体認証やIDカードなどと併用する二要素認証なども検討すると良い	○Active Directory,統合認証システムなど導入に投資が必要 ○二要素認証など導入に投資が必要

５．情報セキュリティ対策　事例（案）

対策（案）			具体策（例）※IPA資料を基に作成	投資概要
	④	【機器の設定】 共有設定を見直そう！	ネットワークに接続されている機器等が不正に使用されないように（必要な利用者のみが使えるようにする）アクセス管理を徹底する ●利用するID／パスワードなどが適切（利用権限のある人）に設定されているか定期的に確認する ●異動や退職時にID／パスワードを変更・削除を確実に行う ●ネットワークに接続する機器のID／パスワードは、納品時の規定値のままにしない 【対象例】 パソコン、ファイルサーバ（NAS含む）、業務システム、クラウドサービス（データ保管、業務システム、情報共有など）などID／パスワード等を設定してアクセス管理を行っているものすべて	○セキュリティ管理者の作業
			●対象が多い場合も同様	
	⑤	【情報取集】 脅威や攻撃の手口を知ろう！	●情報セキュリティ事故や注意喚起情報を確認して社内で共有する仕組みを作る 【情報収集】 ・報道による情報セキュリティ事故の情報収集 ・メーカー等が発信する注意喚起情報 ・IPA等の情報セキュリティ関連組織から注意喚起 （IPA、NISC、JPCERT/CC、SPREAD、警察庁サイバー犯罪対策プロジェクト、全国銀行協会など） 【社内共有】 ・メールや掲示板で知らせる ・定期的な収集情報の発表会や研修会	○ほとんどが無料のメールマガジン登録で可能
			●対象が多い場合も同様	
従業員としての対策	⑥	【電子メールのルール】 見覚えのないメールは疑ってみる	●①、②の対策を行う ●不審なメールの添付ファイルは開かないやURLリンクに安易にアクセスしない、また、不審なメールを社内で共有する 取り組み：「情報セキュリティポリシー」や「メール利用の手引き」を作成し、社内で共有する 参考資料： ・IPAの「標的型攻撃メール＜危険回避＞対策のしおり」 ・IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」	○「情報セキュリティポリシー」や「メール利用の手引き」の作成と説明会でセキュリティ管理者の作業 ○総合セキュリティ対策ソフトには迷惑メール対策やフィッシング対策機能があるものもあり
			●対象が多い場合は、「メール無害化システム」の検討	○メール無害化システムの導入に投資が必要
		宛先の送信ミスを防ぐ	●メールやFAXを送る前に送信先を再確認する ●メールはTO、CC、BCCを使い分けて指定する 取り組み：「情報セキュリティポリシー」や「メール利用の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「メール利用の手引き」の作成と説明会でセキュリティ管理者の作業
			●メールソフトによっては再確認を促す機能があるので検討する	○メールソフトによっては投資が必要
		重要情報を送信するときは保護する	●重要情報を送るときは添付ファイルを暗号化してパスワードで保護する。パスワードは別の手段で連絡する 取り組み：「情報セキュリティポリシー」や「メール利用の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「メール利用の手引き」の作成と説明会でセキュリティ管理者の作業
			●対象が多い場合は、「メール暗号化システム」の検討	○メール暗号化システムの導入に投資が必要

５．情報セキュリティ対策　事例（案）

対策（案）			具体策（例）※IPA資料を基に作成	投資概要
	⑦	【無線LANのルール】 無線LANの盗聴や無断使用を防ぐ	●暗号化設定（WPA2-PSK）を利用する ●パスフレーズは長くて推測されにくいものを使用する 参考資料： ・IPAの「無線LAN＜危険回避＞対策のしおり」 ・IPAの「暗号化による＜情報漏えい＞対策のしおり」	○「情報セキュリティポリシー」や「メール利用の手引き」の作成と説明会でセキュリティ管理者の作業
			●対象が多い場合でさらなる強固なセキュリティをするときは、複数の無線 LAN 機器を一括管理できるような無線 LAN スイッチと認証サーバの利用を検討する	○無線 LAN 機器を一括管理できるような無線 LAN スイッチと認証サーバの導入に投資が必要
	⑧	【Web利用のルール】 インターネットを介したトラブルを防ぐ"	●インターネットの利用ルールを作る ●SNSの利用ルールを作る 取り組み：「情報セキュリティポリシー」や「インターネット利用の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「インターネット利用の手引き」の作成と説明会でセキュリティ管理者の作業
			●Webフィルタリング機能を導入することでシステム的にインターネットの利用を制限する	○Webフィルタリングは総合セキュリティ対策ソフトに機能があるものやUTM装置（統合脅威管理(Unified Threat Management)）で集中管理できるものまであり、用途と予算に応じて投資を検討
	⑨	【バックアップのルール】 不足の事態に備えてバックアップ	●重要情報のバックアップを定期的に行う （できるだけ自動化し忘れないようにする） ●バックアップは元の場所とは別に保存する 取り組み：「情報セキュリティポリシー」や「バックアップの手引き」を作成し、社内で共有する 留意事項： ・バックアップから戻せることも確認しておく ・バックアップから情報が漏えいしないようにする ・不要になったら確実に消去する	○「情報セキュリティポリシー」や「バックアップの手引き」を作成と説明会でセキュリティ管理者の作業 ○バックアップ媒体に投資が必要 ○総合セキュリティ対策ソフトにはバックアップ機能があるものもあり
			●対象が多い場合は、バックアップシステムの導入を検討する	○バックアップシステムに投資が必要
	⑩	【保管のルール】 重要情報の放置を禁止する	●机の上をきれいにする ●重要情報は鍵付き書庫に保管し施錠する 取り組み：「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成と説明会でセキュリティ管理者の作業 ○鍵付き書庫を購入する場合は投資が必要
			●対象が多い場合も同様	
	⑪	【持ち出しのルール】 重要情報は安全な方法で持ち出す	●重要情報の持ち出しは許可制にする ●ノートパソコン、スマートフォン、USBメモリなどはパスワードロック（セキュリティロック含む）をかける（ハードディスクドライブを暗号化） ●荷物は放置しない 取り組み：「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成し、社内で共有する 「持ち出し管理台帳」などで管理する	○「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成と説明会でセキュリティ管理者の作業 ○暗号機能付きUSBメモリ等を新たに購入する場合は投資が必要
			●モバイル機器の対象が多い場合は「モバイルデバイス管理ツール」などの導入も検討	○「モバイルデバイス管理ツール」を導入する場合は投資が必要

５．情報セキュリティ対策　事例（案）

対策（案）			具体策（例）※IPA資料を基に作成	投資概要
	⑫	【事務所の安全管理】 機器を勝手に操作させない	●離席時にコンピュータのロックをする ●退社時にパソコンの電源を切る ●ログインパスワードを利用して他人がパソコンを使うことを防ぐ 取り組み：「情報セキュリティポリシー」や「安全管理の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「安全管理の手引き」を作成と説明会でセキュリティ管理者の作業
			●対象が多い場合も同様	
		見知らぬ人には声を掛ける	●事務所で見知らぬ人を見かけたら声をかける ●受付を設置する 取り組み：「情報セキュリティポリシー」や「安全管理の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「安全管理の手引き」を作成と説明会でセキュリティ管理者の作業
			●対象が多い場合も同様	
		機器・備品の盗難防止対策を行う	●退社時に机の上のノートパソコンやタブレット端末、外部記録媒体を引き出しなど鍵付き保管場所に保管する 取り組み：「情報セキュリティポリシー」や「安全管理の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「安全管理の手引き」を作成と説明会でセキュリティ管理者の作業
			●対象が多い場合も同様	
		オフィスの戸締りに気を配る	●鍵の管理を徹底する ●最終退出者は事務所を施錠し退出記録を残す 取り組み：「情報セキュリティポリシー」や「安全管理の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「安全管理の手引き」を作成と説明会でセキュリティ管理者の作業
			●対象が多い場合も同様	
	⑬	【情報の安全な処分】 重要情報は復元できないように消去する	●消去ソフトを利用する ●重要書類はシュレッダーか溶解する ●物理的に壊してから処分する（外部記録媒体等） ●専門業者に消去を依頼する 取り組み：「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成と説明会でセキュリティ管理者の作業 ○専門業者に依頼する場合は投資が必要
			●対象が多い場合も同様	
組織としての対策	⑭	【守秘義務の周知】 従業員に守秘義務について理解してもらう	●守秘義務があることを知らせる ・何が機密（守秘義務の対象）なのか明確にする ・機密を守る方法も明確にする（業務ルール等） ・守られなかった場合の罰則も用意する（就業規則等） 取り組み：「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成と説明会でセキュリティ管理者の作業 ○必要により「就業規則」や「誓約書」等も検討
			参考資料： 経済産業省：「秘密情報の保護ハンドブック～企業価値向上に向けて～」 経済産業省：「営業秘密管理指針」	
			●対象が多い場合も同様	
	⑮	【従業員教育】 従業員の定期的な教育を行う	●情報管理の大切さを定期的に説明する ●社内研修会を開催する 取り組み：「情報セキュリティポリシー教育・研修計画」を作成し、実施する（1回／年以上） 参考： ハインリッヒの法則：1件の重大な事故の背景には、29件の軽微な事故の背景には300件の事故に至らなかった問題が存在する	○「情報セキュリティポリシー教育・研修計画」を作成、実施でセキュリティ管理者の作業
			●対象が多い場合も同様	

５．情報セキュリティ対策　事例（案）

対策（案）			具体策（例）※IPA資料を基に作成	投資概要
	⑯	【私物機器の利用】 個人所有端末の業務での利用可否を決める	●個人所有パソコン、スマートフォンを業務利用する場合は許可制にする ●業務利用する場合のルールを決める 取り組み：「情報セキュリティポリシー」や「安全管理の手引き」を作成し、社内で共有する	○「情報セキュリティポリシー」や「安全管理の手引き」を作成と説明会でセキュリティ管理者の作業
			参考：業務利用のルール ・OSや利用しているアプリケーションの脆弱性は解消されている ・業務が利用するデータあるいは業務処理そのものに悪影響が出る可能性のあるアプリケーションなどのソフトの利用禁止（インストール禁止） ・セキュリティ対策ソフトを正しく利用している ・業務としての処理を行った場合は、利用した業務データ等を不必要に保存せず、速やかに削除（できれば完全消去）する	
			・会社が用意した電子メール環境やリモートアクセス環境以外、あるいは会社が用意した記憶媒体以外を利用したデータの受け渡しは行わない ・パソコンそのものの利用制限ができるログインパスワードの設定や、記憶された大事な情報は暗号化するなどのセキュリティ対策（情報漏えい対策）が施されている	
			●対象が多い場合も同様	
	⑰	【取引先管理】 取引先に秘密保持を要請する	●秘密保持の内容を明確にした契約書を作る 取り組み：「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成し、社内で共有する 「契約書（雛型）を作成し共有する	○「情報セキュリティポリシー」や「重要情報取扱の手引き」を作成と説明会でセキュリティ管理者の作業 ○「契約書（雛型）」の作成
			参考：秘密情報（守るべき情報）とは ・顧客情報・個人情報 ・委託元（取引先）から預かった各種（業務）情報 ・企業（組織）固有のノウハウ・テクニックなどの技術情報・企業（組織）戦略情報 ・その他、漏れると企業（組織）活動に大きな支障をきたす情報（企業機密・営業機密）	
			参考資料： 経済産業省：「秘密情報の保護ハンドブック～企業価値向上に向けて～」 経済産業省：「営業秘密管理指針」 「不正競争防止法」（営業機密の定義あり） 不正競争防止法で保護される要件 ・秘密として管理されている（秘密管理性） ・事業活動に有用な情報である（有用性） ・公然と知られていない（非公知性）	
			●対象が多い場合も同様	
	⑱	【外部サービスの利用】 信頼できる外部サービスを使う	●利用規約や補償内容、セキュリティ対策などを確認して事業者を選ぶ 取り組み：「情報セキュリティポリシー」や「インターネット利用の手引き」を作成し、社内で共有する 参考資料： ・IPAの「クラウドサービス安全利用のすすめ」	○「情報セキュリティポリシー」や「インターネット利用の手引き」の作成と説明会でセキュリティ管理者の作業
			●対象が多い場合も同様	

５．情報セキュリティ対策　事例（案）

対策（案）			具体策（例）※IPA資料を基に作成	投資概要
	⑲	【事故への備え】 事故に備えて事前に準備する	●重要情報の流出や、盗難があった場合の対応手順書を作成する 取り組み：「事業継続計画」を作成し、「事故対応マニュアル」や「対応体制」を明確にする	○「事業継続計画」、「事故対応マニュアル」、「対応体制」等の作成の作業
			参考資料： ・中小企業庁の「中小企業BCP策定運用指針」 ・IPAの「情報漏えい発生時の対応ポイント集」	
			●対象が多い場合も同様	
	⑳	【ルールの整備】 情報セキュリティ対策をルール化する	●情報セキュリティ対策として、診断シート項目のNo.1～24までをルール化して社内で共有する ●ルールに問題があれば改善する 取り組み：「情報セキュリティポリシー」や前記の各種手引きやマニュアル等を作成し共有する	○「情報セキュリティポリシー」や前記の各種手引きやマニュアル等の作成
			●対象が多い場合も同様	