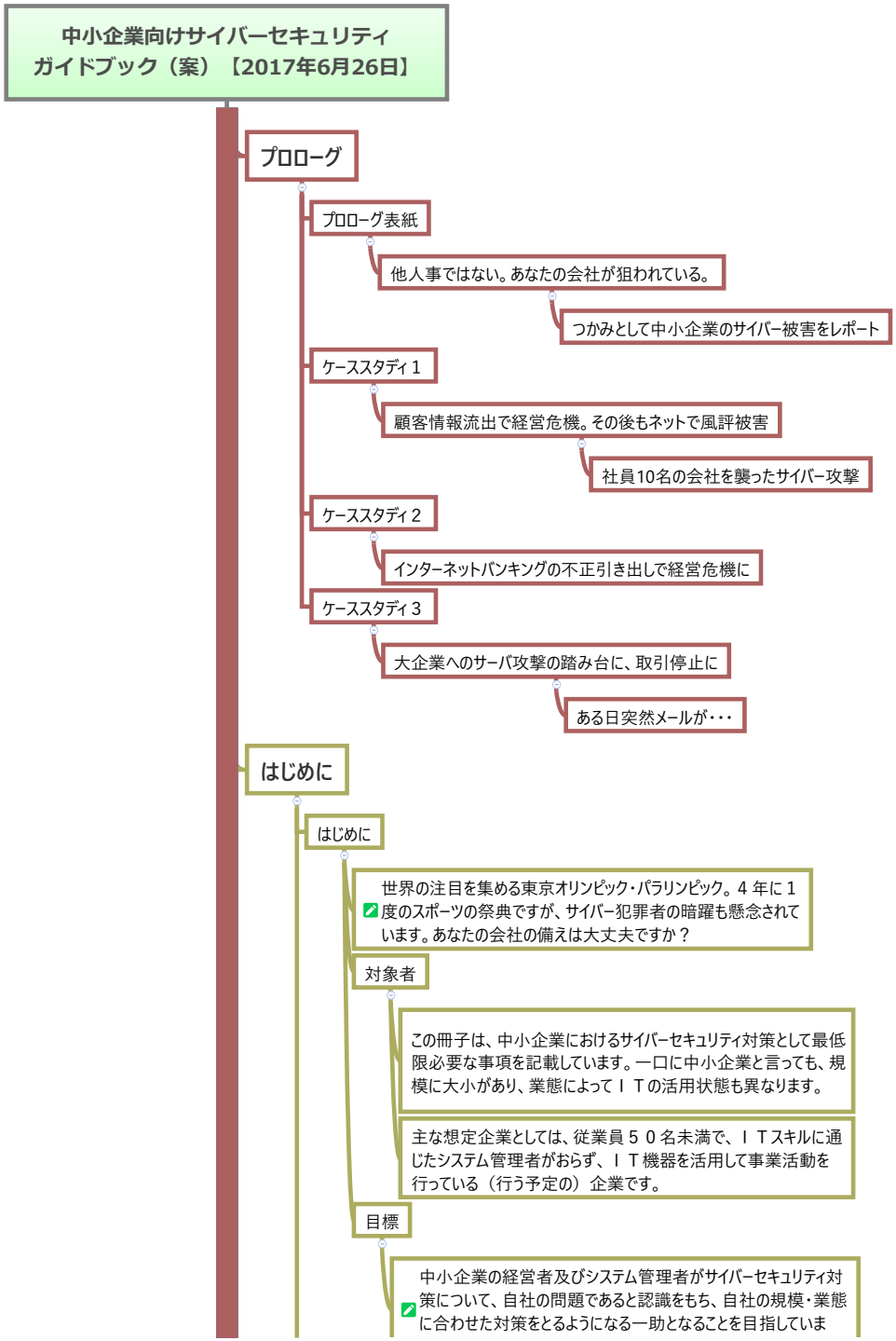
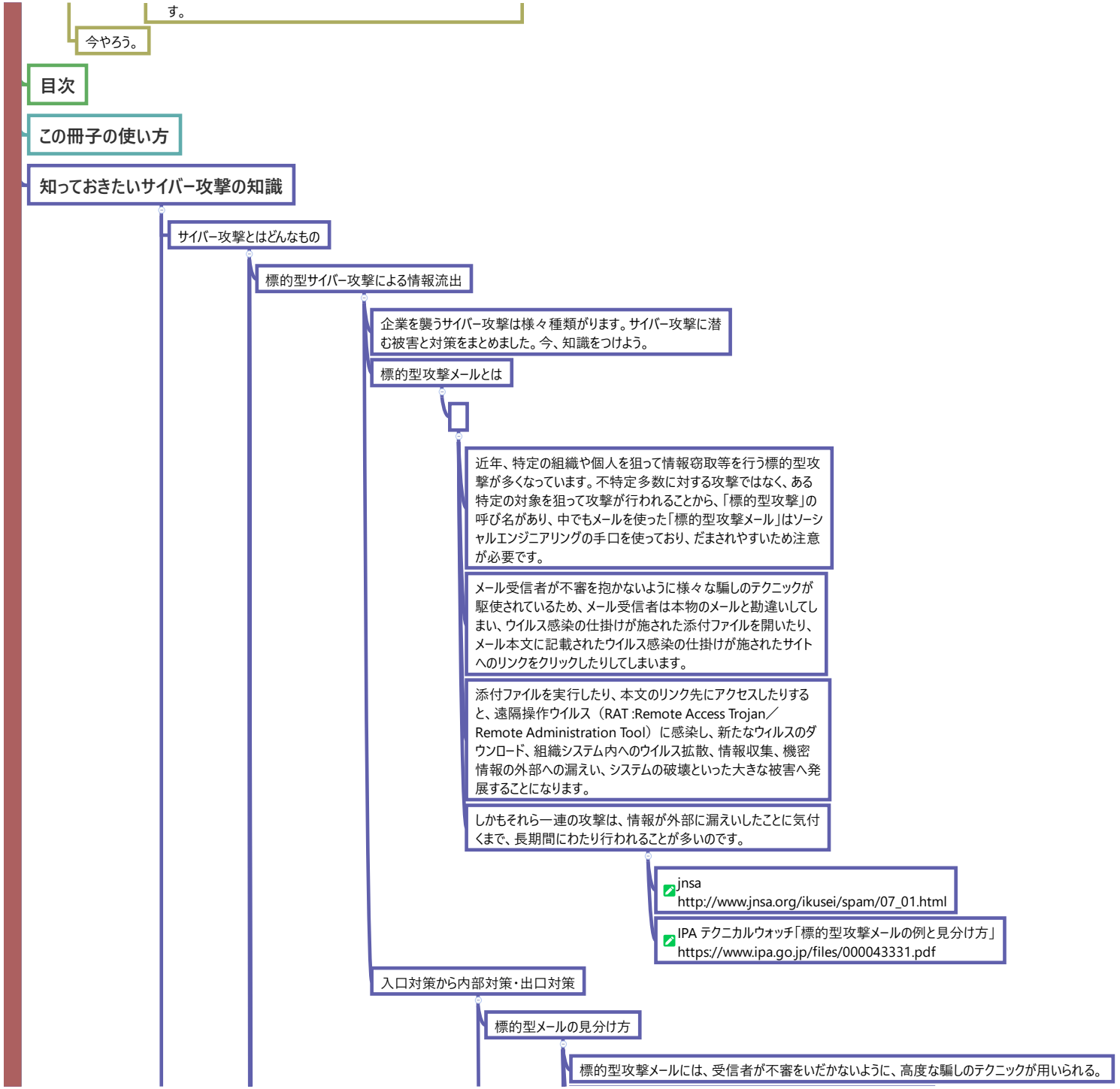
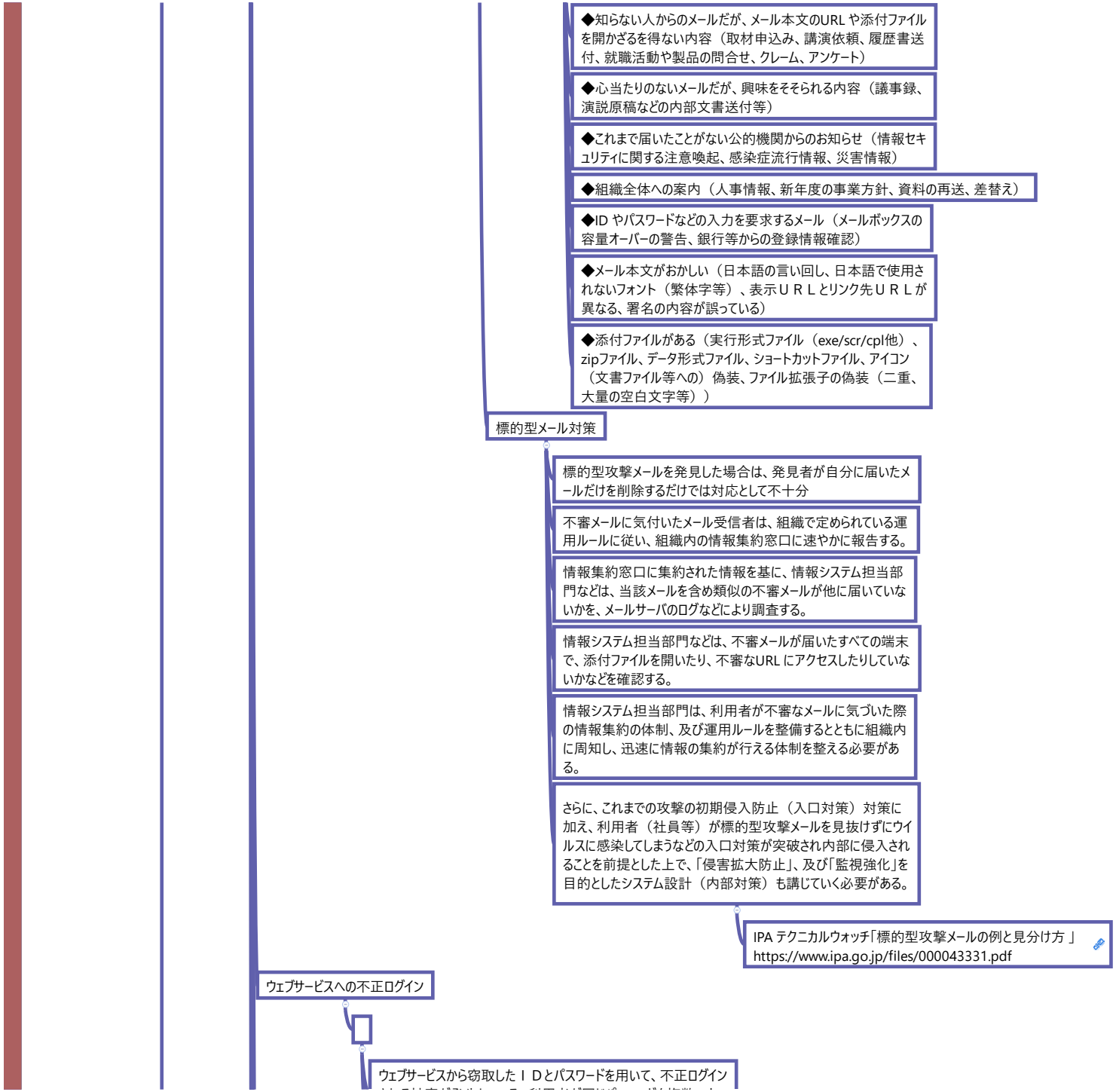
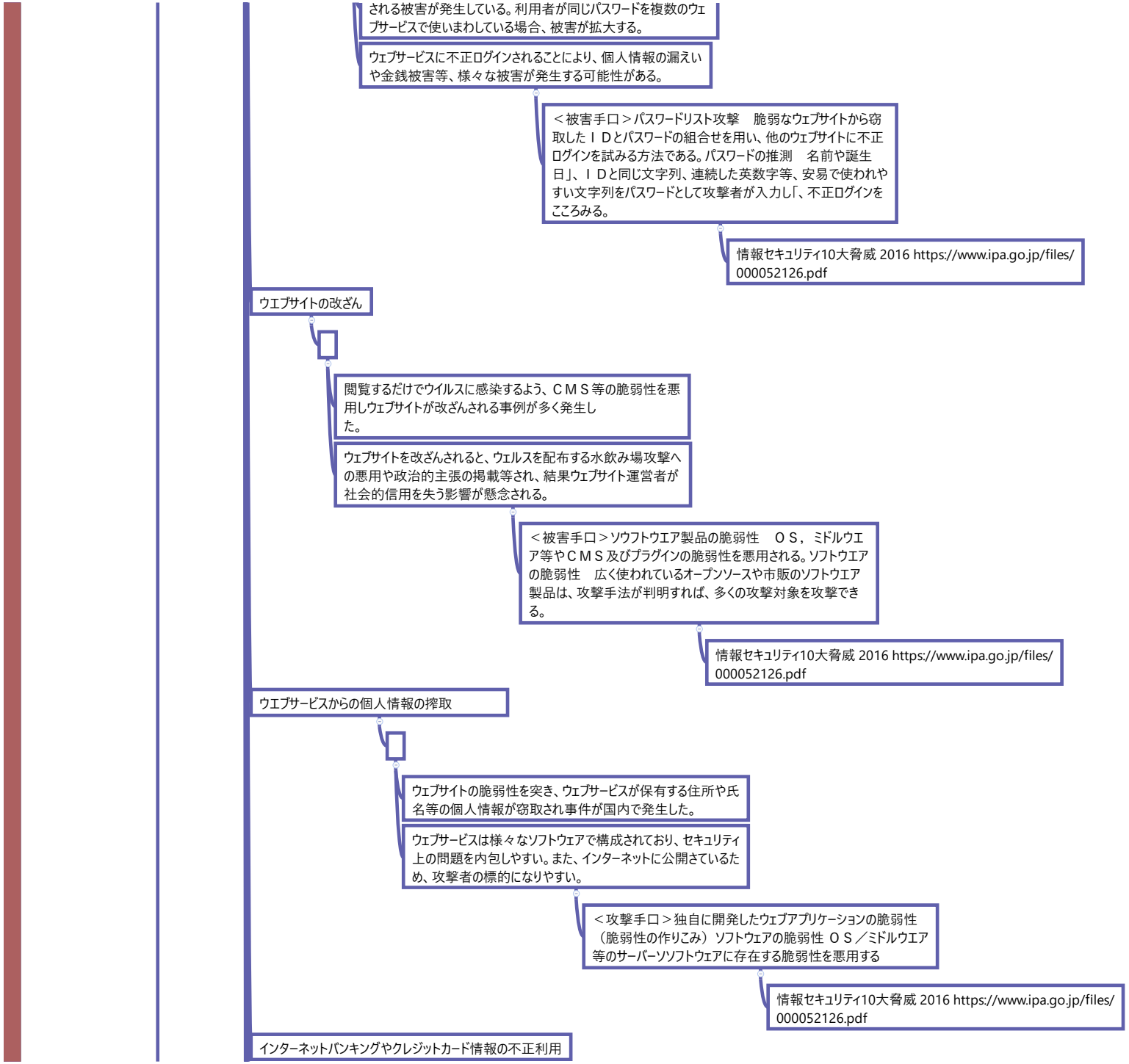
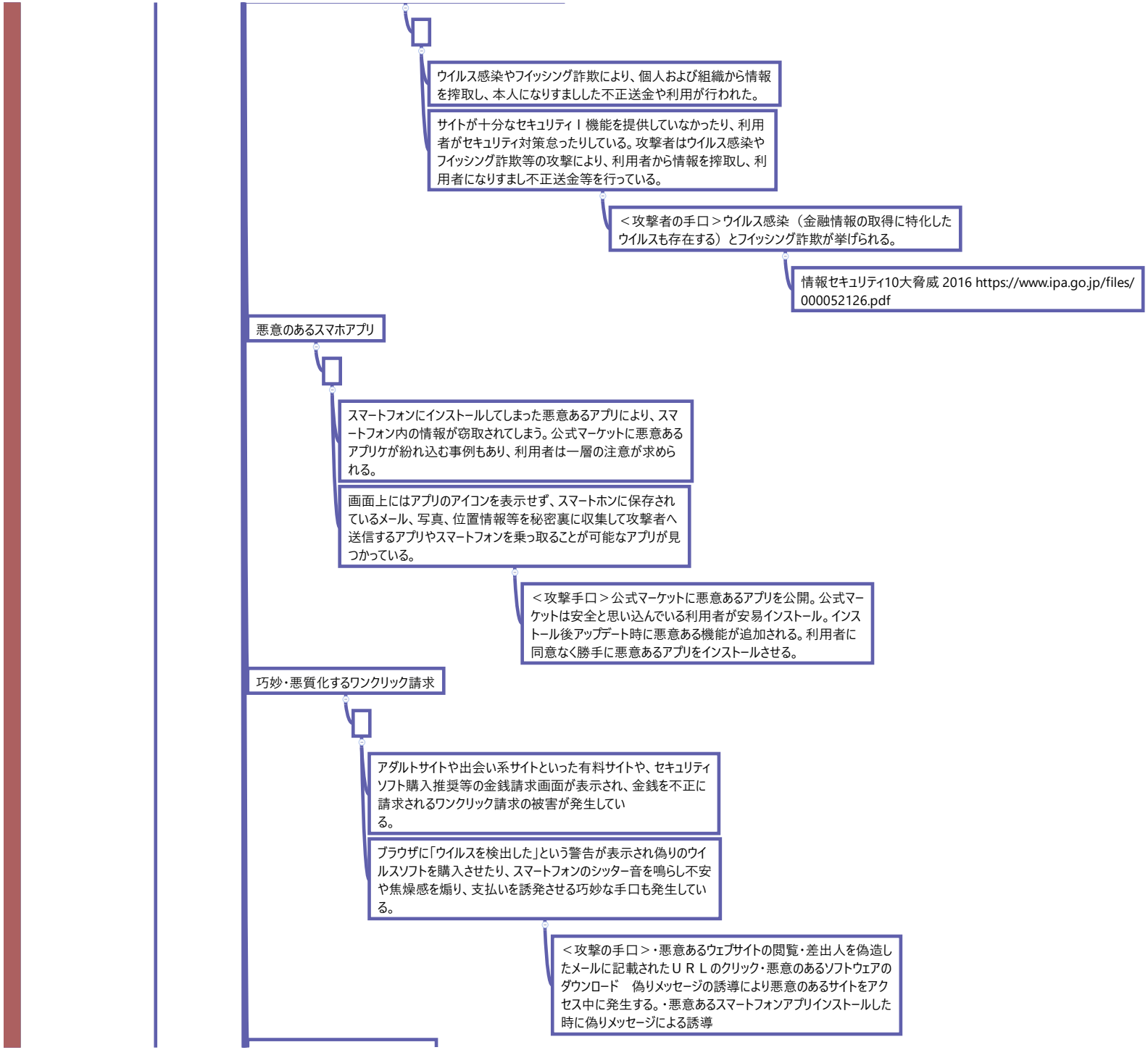
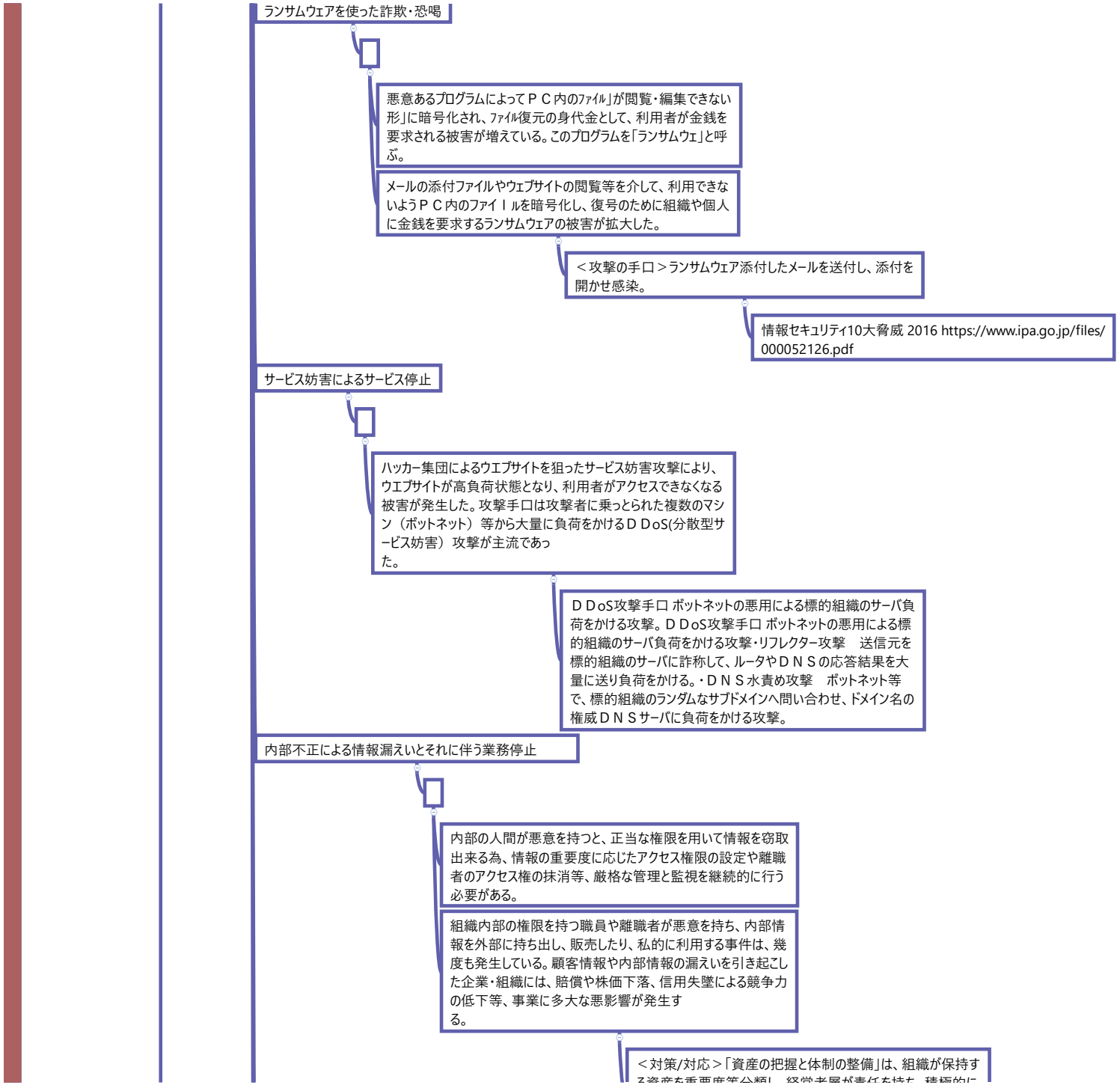

中小企業向けサイバーセキュリティ
ガイドブック（案）【2017年6月26日】
プロローグ
プロローグ表紙
他人事ではない。あなたの会社が狙われている。
つかみとして中小企業のサイバー被害をレポート
ケーススタディ１
顧客情報流出で経営危機。その後もネットで風評被害
社員10名の会社を襲ったサイバー攻撃
ケーススタディ２
インターネットバンキングの不正引き出しで経営危機に
ケーススタディ３
大企業へのサーバ攻撃の踏み台に、取引停止に
ある日突然メールが・・・
はじめに
はじめに
世界の注目を集める東京オリンピック・パラリンピック。４年に１度のスポーツの祭典ですが、サイバー犯罪者の暗躍も懸念されています。あなたの会社の備えは大丈夫ですか？
対象者
この冊子は、中小企業におけるサイバーセキュリティ対策として最低限必要な事項を記載しています。一口に中小企業と言っても、規模に大小があり、業態によってＩＴの活用状態も異なります。
主な想定企業としては、従業員５０名未満で、ＩＴスキルに通じたシステム管理者がおらず、ＩＴ機器を活用して事業活動を行っている（行う予定の）企業です。
目標
中小企業の経営者及びシステム管理者がサイバーセキュリティ対策について、自社の問題であると認識をもち、自社の規模・業態に合わせた対策をとるようになる一助となることを目指してい

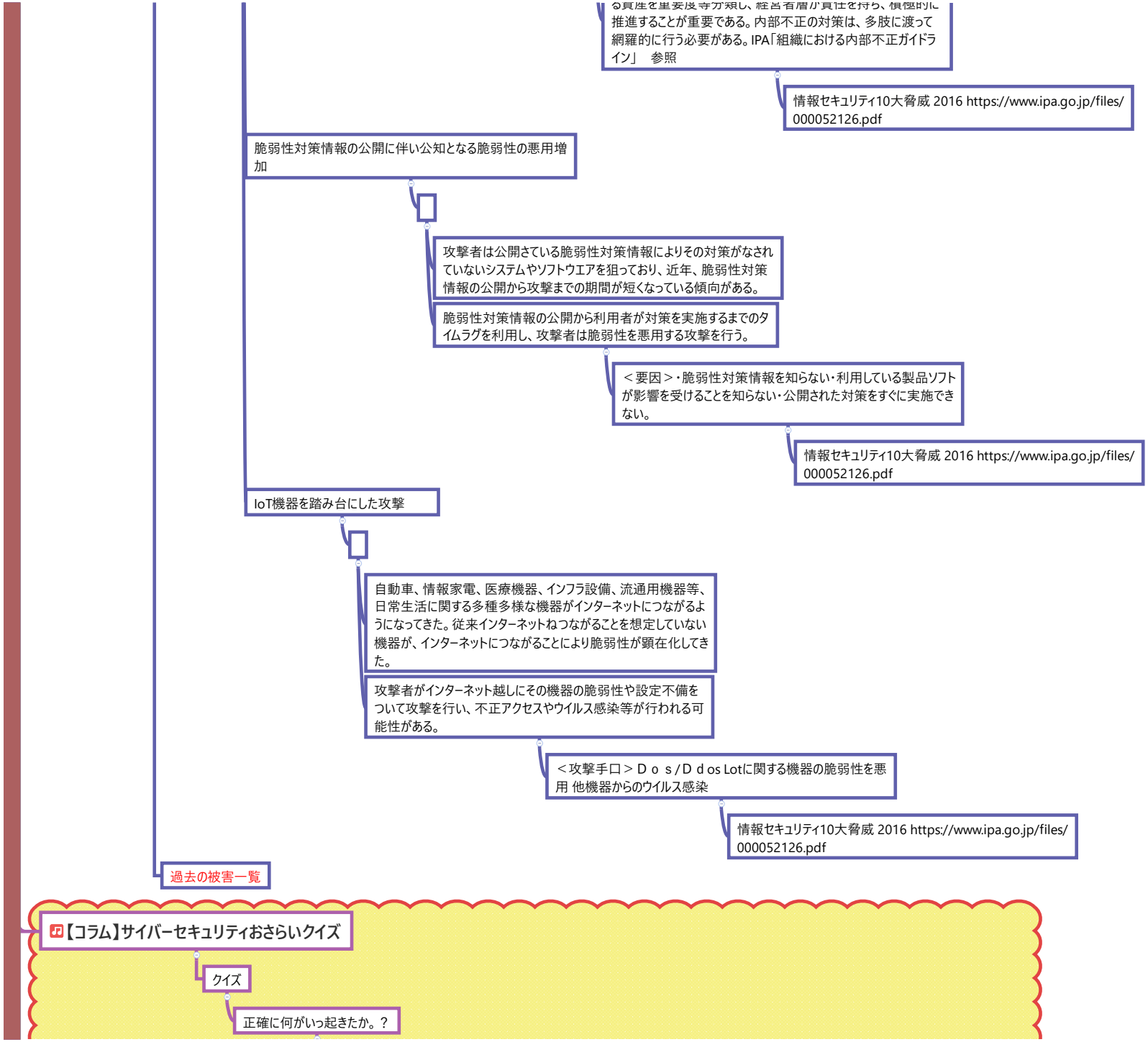

す。
今やろう。
目次
この冊子の使い方
知っておきたいサイバー攻撃の知識
サイバー攻撃とはどんなもの
標的型サイバー攻撃による情報流出
企業を襲うサイバー攻撃は様々種類がります。サイバー攻撃に潜む被害と対策をまとめました。今、知識をつけよう。
標的型攻撃メールとは
近年、特定の組織や個人を狙って情報窃取等を行う標的型攻撃が多くなっています。不特定多数に対する攻撃ではなく、ある特定の対象を狙って攻撃が行われることから、「標的型攻撃」の呼び名があり、中でもメールを使った「標的型攻撃メール」はソーシャルエンジニアリングの手口を使っており、だまされやすいため注意が必要です。
メール受信者が不審を抱かないように様々な騙しのテクニックが駆使されているため、メール受信者は本物のメールと勘違いしてしまい、ウイルス感染の仕掛けが施された添付ファイルを開いたり、メール本文に記載されたウイルス感染の仕掛けが施されたサイトへのリンクをクリックしたりしてしまいます。
添付ファイルを実行したり、本文のリンク先にアクセスしたりすると、遠隔操作ウイルス（RAT :Remote Access Trojan／Remote Administration Tool）に感染し、新たなウィルスのダウンロード、組織システム内へのウイルス拡散、情報収集、機密情報の外部への漏えい、システムの破壊といった大きな被害へ発展することになります。
しかもそれら一連の攻撃は、情報が外部に漏えいしたことに気付くまで、長期間にわたり行われることが多いのです。
jnsa
http://www.jnsa.org/ikusei/spam/07_01.html
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」
https://www.ipa.go.jp/files/000043331.pdf
入口対策から内部対策・出口対策
標的型メールの見分け方
標的型攻撃メールには、受信者が不審をいだかないように、高度な騙しのテクニックが用いられる。


◆知らない人からのメールだが、メール本文のURL や添付ファイルを開かざるを得ない内容（取材申込み、講演依頼、履歴書送付、就職活動や製品の問合せ、クレーム、アンケート）
◆心当たりのないメールだが、興味をそそられる内容（議事録、演説原稿などの内部文書送付等）
◆これまで届いたことがない公的機関からのお知らせ（情報セキュリティに関する注意喚起、感染症流行情報、災害情報）
◆組織全体への案内（人事情報、新年度の事業方針、資料の再送、差替え）
◆ID やパスワードなどの入力を要求するメール（メールボックスの容量オーバーの警告、銀行等からの登録情報確認）
◆メール本文がおかしい（日本語の言い回し、日本語で使用されないフォント（繁体字等）、表示ＵＲＬとリンク先ＵＲＬが異なる、署名の内容が誤っている）
◆添付ファイルがある（実行形式ファイル（exe/scr/cpl他）、zipファイル、データ形式ファイル、ショートカットファイル、アイコン（文書ファイル等への）偽装、ファイル拡張子の偽装（二重、大量の空白文字等））
標的型メール対策
標的型攻撃メールを発見した場合は、発見者が自分に届いたメールだけを削除するだけでは対応として不十分
不審メールに気付いたメール受信者は、組織で定められている運用ルールに従い、組織内の情報集約窓口に速やかに報告する。
情報集約窓口に集約された情報を基に、情報システム担当部門などは、当該メールを含め類似の不審メールが他に届いていないかを、メールサーバのログなどにより調査する。
情報システム担当部門などは、不審メールが届いたすべての端末で、添付ファイルを開いたり、不審なURL にアクセスしたりしていないかなどを確認する。
情報システム担当部門は、利用者が不審なメールに気づいた際の情報集約の体制、及び運用ルールを整備するとともに組織内に周知し、迅速に情報の集約が行える体制を整える必要がある。
さらに、これまでの攻撃の初期侵入防止（入口対策）対策に加え、利用者（社員等）が標的型攻撃メールを見抜けずにウイルスに感染してしまうなどの入口対策が突破され内部に侵入されることを前提とした上で、「侵害拡大防止」、及び「監視強化」を目的としたシステム設計（内部対策）も講じていく必要がある。
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 」
https://www.ipa.go.jp/files/000043331.pdf
ウェブサービスへの不正ログイン
ウェブサービスから窃取したＩＤとパスワードを用いて、不正ログイン


される被害が発生している。利用者が同じパスワードを複数のウェブサービスで使いまわしている場合、被害が拡大する。
ウェブサービスに不正ログインされることにより、個人情報の漏えいや金銭被害等、様々な被害が発生する可能性がある。
＜被害手口＞パスワードリスト攻撃　脆弱なウェブサイトから窃取したＩＤとパスワードの組合せを用い、他のウェブサイトに不正ログインを試みる方法である。パスワードの推測　名前や誕生日」、ＩＤと同じ文字列、連続した英数字等、安易で使われやすい文字列をパスワードとして攻撃者が入力し「、不正ログインをこころみる。
情報セキュリティ10大脅威 2016 https://www.ipa.go.jp/files/000052126.pdf
ウエブサイトの改ざん
閲覧するだけでウイルスに感染するよう、ＣＭＳ等の脆弱性を悪用しウェブサイトが改ざんされる事例が多く発生した。
ウェブサイトを改ざんされると、ウェルスを配布する水飲み場攻撃への悪用や政治的主張の掲載等され、結果ウェブサイト運営者が社会的信用を失う影響が懸念される。
＜被害手口＞ソウフトウエア製品の脆弱性　ＯＳ，ミドルウエア等やＣＭＳ及びプラグインの脆弱性を悪用される。ソフトウエアの脆弱性　広く使われているオープンソースや市販のソフトウエア製品は、攻撃手法が判明すれば、多くの攻撃対象を攻撃できる。
情報セキュリティ10大脅威 2016 https://www.ipa.go.jp/files/000052126.pdf
ウエブサービスからの個人情報の搾取
ウェブサイトの脆弱性を突き、ウェブサービスが保有する住所や氏名等の個人情報が窃取され事件が国内で発生した。
ウェブサービスは様々なソフトウェアで構成されており、セキュリティ上の問題を内包しやすい。また、インターネットに公開さているため、攻撃者の標的になりやすい。
＜攻撃手口＞独自に開発したウェブアプリケーションの脆弱性（脆弱性の作りこみ）ソフトウェアの脆弱性 ＯＳ／ミドルウエア等のサーバーソフトウエアに存在する脆弱性を悪用する
情報セキュリティ10大脅威 2016 https://www.ipa.go.jp/files/000052126.pdf
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


ウイルス感染やフイッシング詐欺により、個人および組織から情報を搾取し、本人になりすましした不正送金や利用が行われた。
サイトが十分なセキュリティＩ機能を提供していなかったり、利用者がセキュリティ対策怠ったりしている。攻撃者はウイルス感染やフイッシング詐欺等の攻撃により、利用者から情報を搾取し、利用者になりすまし不正送金等を行っている。
＜攻撃者の手口＞ウイルス感染（金融情報の取得に特化したウイルスも存在する）とフイッシング詐欺が挙げられる。
情報セキュリティ10大脅威 2016 https://www.ipa.go.jp/files/000052126.pdf
悪意のあるスマホアプリ
スマートフォンにインストールしてしまった悪意あるアプリにより、スマートフォン内の情報が窃取されてしまう。公式マーケットに悪意あるアプリケが紛れ込む事例もあり、利用者は一層の注意が求められる。
画面上にはアプリのアイコンを表示せず、スマートホンに保存されているメール、写真、位置情報等を秘密裏に収集して攻撃者へ送信するアプリやスマートフォンを乗っ取ることが可能なアプリが見つかっている。
＜攻撃手口＞公式マーケットに悪意あるアプリを公開。公式マーケットは安全と思い込んでいる利用者が安易インストール。インストール後アップデート時に悪意ある機能が追加される。利用者に同意なく勝手に悪意あるアプリをインストールさせる。
巧妙・悪質化するワンクリック請求
アダルトサイトや出会い系サイトといった有料サイトや、セキュリティソフト購入推奨等の金銭請求画面が表示され、金銭を不正に請求されるワンクリック請求の被害が発生している。
ブラウザに「ウイルスを検出した」という警告が表示され偽りのウイルスソフトを購入させたり、スマートフォンのシッター音を鳴らし不安や焦燥感を煽り、支払いを誘発させる巧妙な手口も発生している。
＜攻撃の手口＞・悪意あるウェブサイトの閲覧・差出人を偽造したメールに記載されたＵＲＬのクリック・悪意のあるソフトウェアのダウンロード　偽りメッセージの誘導により悪意のあるサイトをアクセス中に発生する。・悪意あるスマートフォンアプリインストールした時に偽りメッセージによる誘導


ランサムウェアを使った詐欺・恐喝
悪意あるプログラムによってＰＣ内のﾌｧｲﾙ」が閲覧・編集できない形」に暗号化され、ﾌｧｲﾙ復元の身代金として、利用者が金銭を要求される被害が増えている。このプログラムを「ランサムウェ」と呼ぶ。
メールの添付ファイルやウェブサイトの閲覧等を介して、利用できないようＰＣ内のファイｌルを暗号化し、復号のために組織や個人に金銭を要求するランサムウェアの被害が拡大した。
＜攻撃の手口＞ランサムウェア添付したメールを送付し、添付を開かせ感染。
情報セキュリティ10大脅威 2016 https://www.ipa.go.jp/files/000052126.pdf
サービス妨害によるサービス停止
ハッカー集団によるウエブサイトを狙ったサービス妨害攻撃により、ウエブサイトが高負荷状態となり、利用者がアクセスできなくなる被害が発生した。攻撃手口は攻撃者に乗っとられた複数のマシン（ボットネット）等から大量に負荷をかけるＤＤoS(分散型サービス妨害）攻撃が主流であった。
ＤＤoS攻撃手口 ボットネットの悪用による標的組織のサーバ負荷をかける攻撃。ＤＤoS攻撃手口 ボットネットの悪用による標的組織のサーバ負荷をかける攻撃・リフレクター攻撃　送信元を標的組織のサーバに詐称して、ルータやＤＮＳの応答結果を大量に送り負荷をかける。・ＤＮＳ水責め攻撃　ボットネット等で、標的組織のランダムなサブドメインへ問い合わせ、ドメイン名の権威ＤＮＳサーバに負荷をかける攻撃。
内部不正による情報漏えいとそれに伴う業務停止
内部の人間が悪意を持つと、正当な権限を用いて情報を窃取出来る為、情報の重要度に応じたアクセス権限の設定や離職者のアクセス権の抹消等、厳格な管理と監視を継続的に行う必要がある。
組織内部の権限を持つ職員や離職者が悪意を持ち、内部情報を外部に持ち出し、販売したり、私的に利用する事件は、幾度も発生している。顧客情報や内部情報の漏えいを引き起こした企業・組織には、賠償や株価下落、信用失墜による競争力の低下等、事業に多大な悪影響が発生する。
＜対策/対応＞「資産の把握と体制の整備」は、組織が保持する


る資産を重要度等分類し、経営者層が責任を持ち、積極的に推進することが重要である。内部不正の対策は、多肢に渡って網羅的に行う必要がある。IPA「組織における内部不正ガイドライン」 参照
情報セキュリティ10大脅威 2016 https://www.ipa.go.jp/files/000052126.pdf
脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
攻撃者は公開さている脆弱性対策情報によりその対策がなされていないシステムやソフトウエアを狙っており、近年、脆弱性対策情報の公開から攻撃までの期間が短くなっている傾向がある。
脆弱性対策情報の公開から利用者が対策を実施するまでのタイムラグを利用し、攻撃者は脆弱性を悪用する攻撃を行う。
＜要因＞・脆弱性対策情報を知らない・利用している製品ソフトが影響を受けることを知らない・公開された対策をすぐに実施できない。
情報セキュリティ10大脅威 2016 https://www.ipa.go.jp/files/000052126.pdf
IoT機器を踏み台にした攻撃
自動車、情報家電、医療機器、インフラ設備、流通用機器等、日常生活に関する多種多様な機器がインターネットにつながるようになってきた。従来インターネットねつながることを想定していない機器が、インターネットにつながることにより脆弱性が顕在化してきた。
攻撃者がインターネット越しにその機器の脆弱性や設定不備をついて攻撃を行い、不正アクセスやウイルス感染等が行われる可能性がある。
＜攻撃手口＞Ｄｏｓ/Ｄｄos Lotに関する機器の脆弱性を悪用 他機器からのウイルス感染
情報セキュリティ10大脅威 2016 https://www.ipa.go.jp/files/000052126.pdf
過去の被害一覧
【コラム】サイバーセキュリティおさらいクイズ
クイズ
正確に何がいっ起きたか。？

インシデント対応の最も大切な部分のひとつであり、最も省略されがちなのが、学習と改善である。各インシデント対応チームは新しい脅威に対して進化し、技術を向上させ、教訓を学ぶべきである。

①正確に何がいっ起きたか。②スタッフとマネジメント層がどの程度うまく事件に対処したか。文書化された手順に従ったか。それは適切だったか。③すぐに必要なった情報はなにか。④復旧を妨げたかもしれないステップやマネジメント層は、どのような行動をとるか。⑤次に同様なの事件が起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか。⑥どのような是正措置があれば、将来にわたって同じような事件が起きるのを防げるか。⑦将来事件を検出、分析、軽減するために、どのようなツールやソースが追加で必要」となるか。

コンピュターセキュリティインシデント対応ガイド NIST800-61（参照IPA和文訳)

【02】すぐやろうサイバー攻撃アクション

今すぐできるサイバー攻撃の備えをまとめました。しっかりとした事前の備えが、もしもの時、あなたの会社や大切な従業員をまもります。今やろう。

サイバー攻撃に対して何ができるか（全体イメージ）

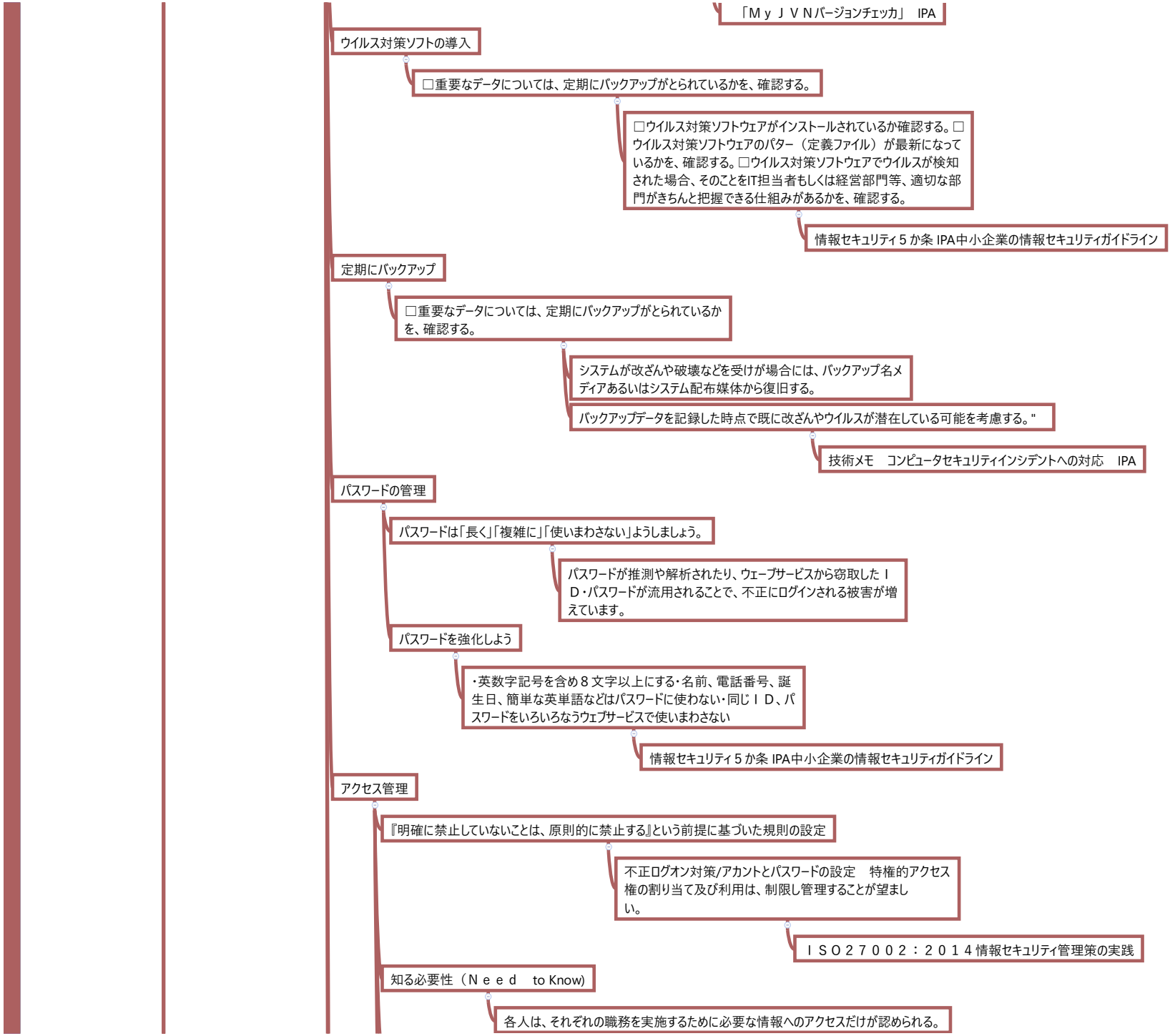
今やろう！５＋２の備えと社内使用パソコンへの対策

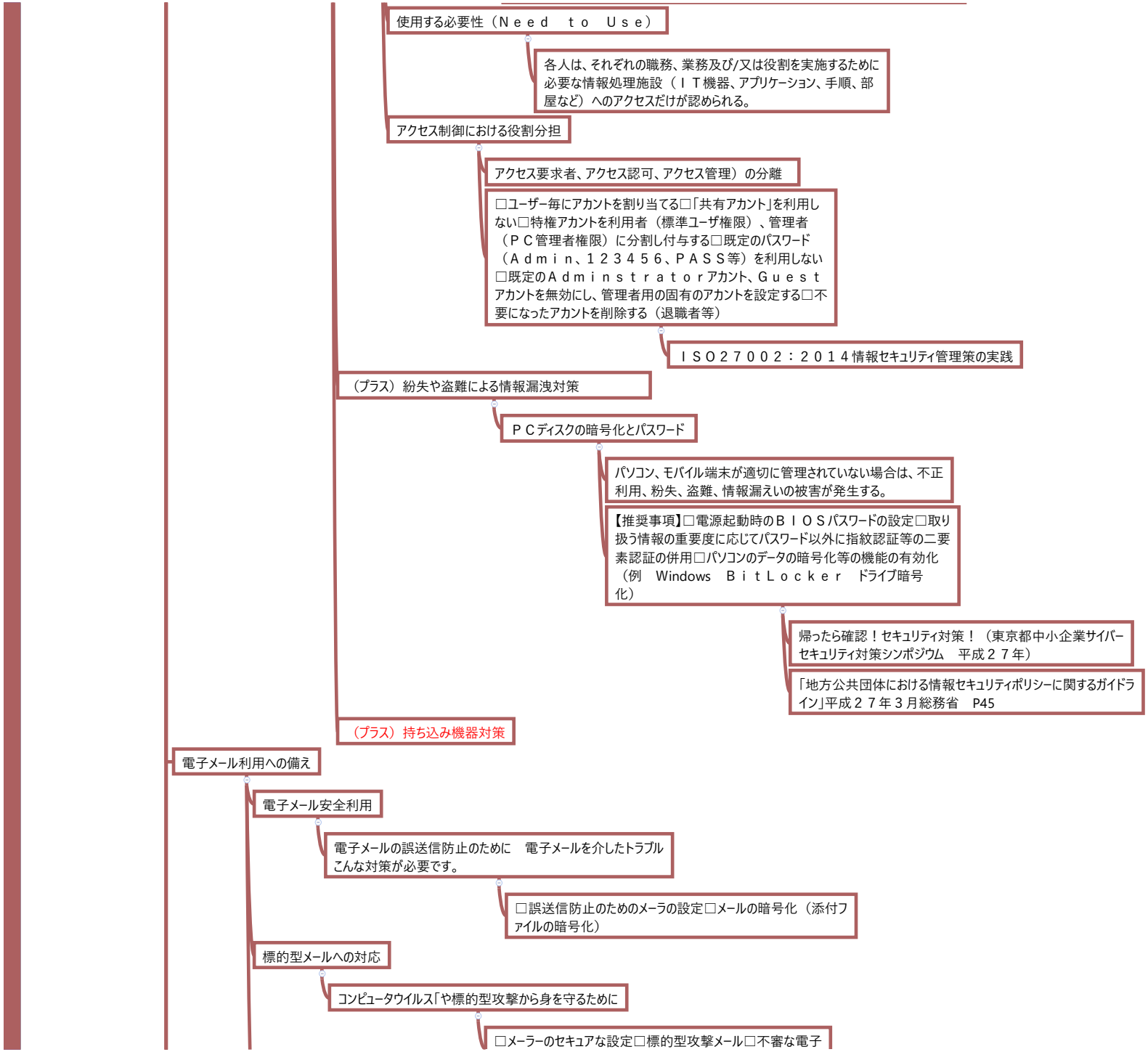
帰ったら確認！セキュリティ対策！（東京都中小企業サイバーセキュリティ対策シンポジウム　平成２７年）

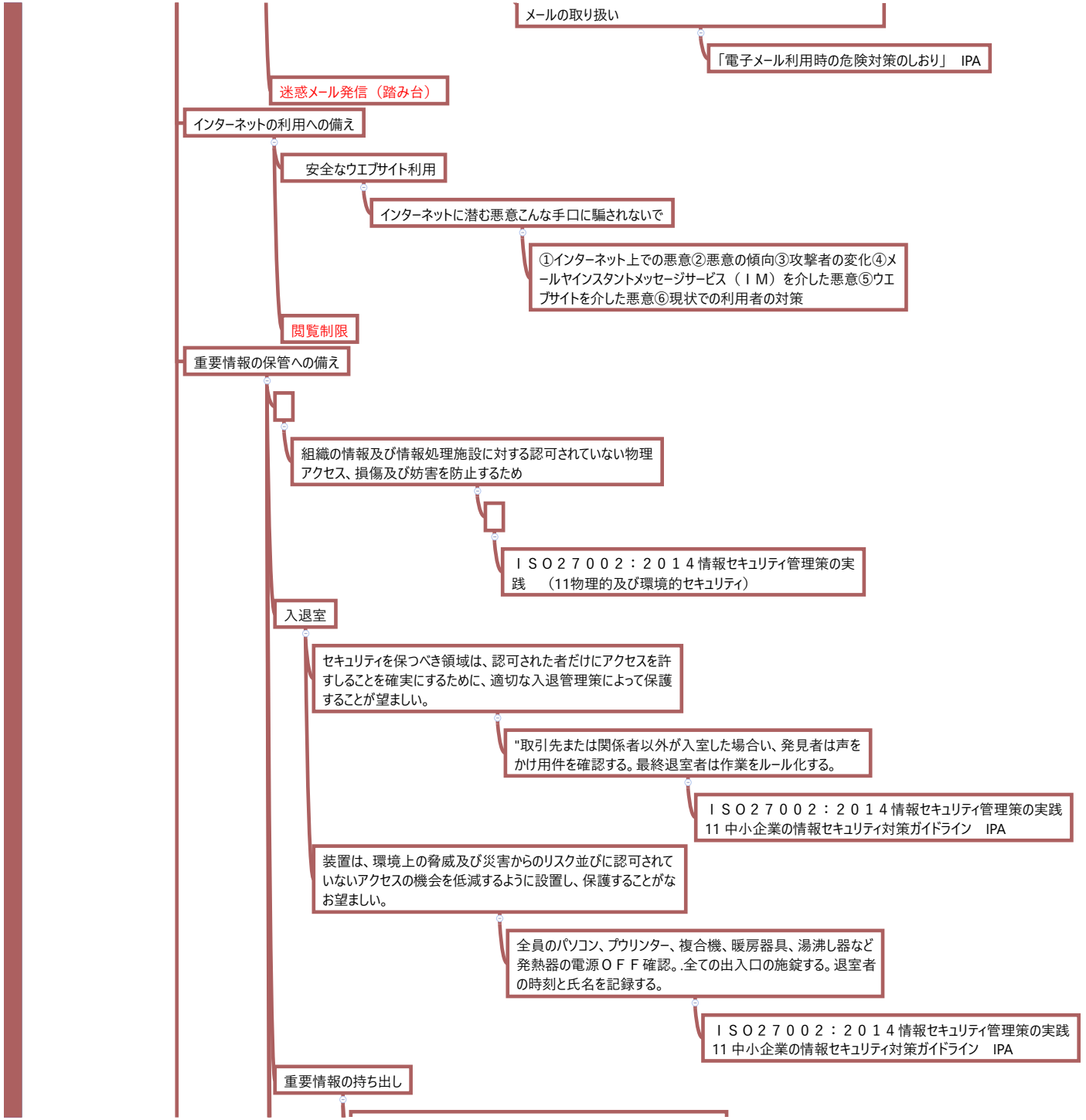
ＯＳとソフトウェアのアップデート

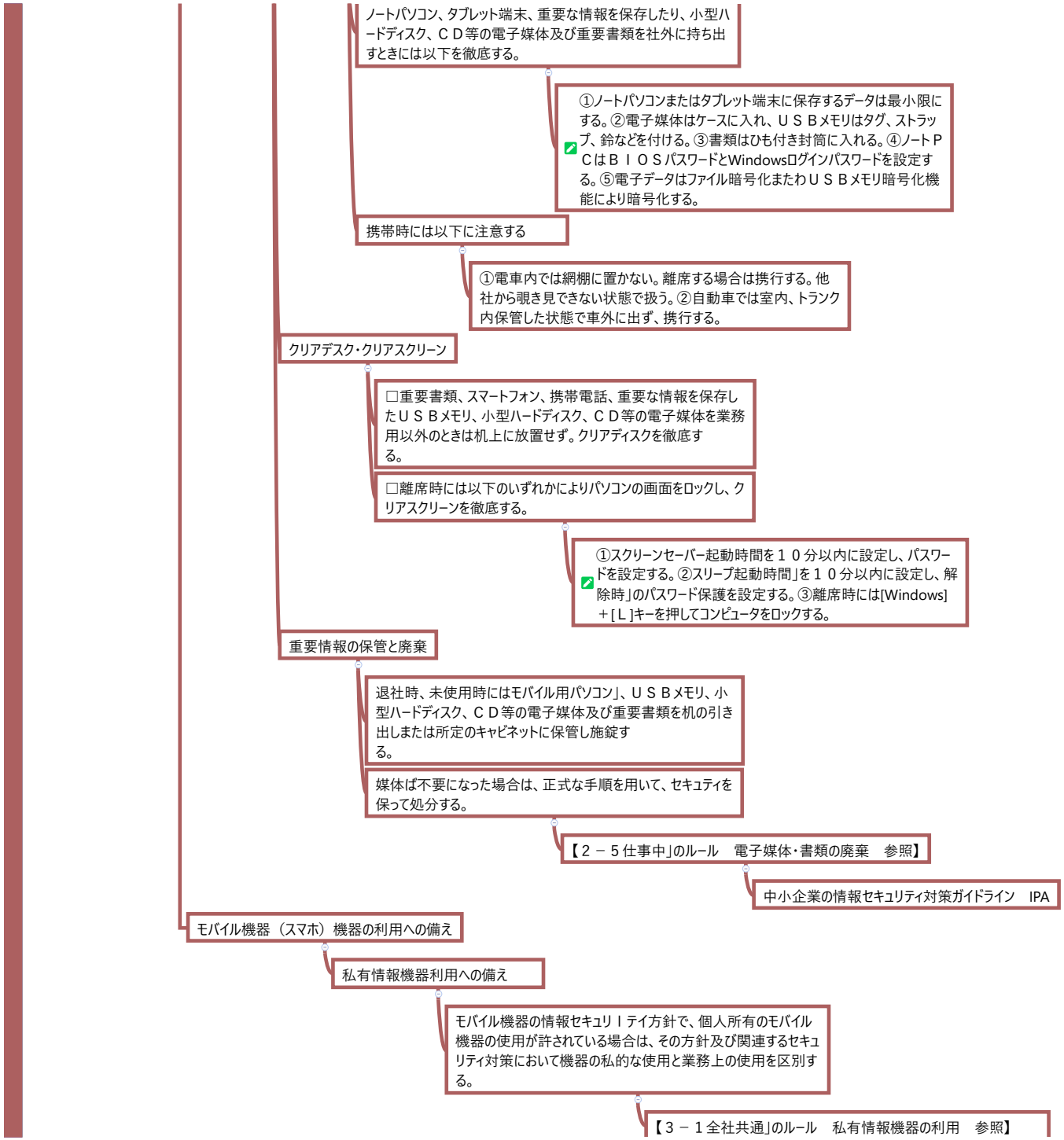
常にサイバーセキュリティについて点検を怠らない　パソコンにインストールされているソフトウェア製品の「バージョンをチェックする」

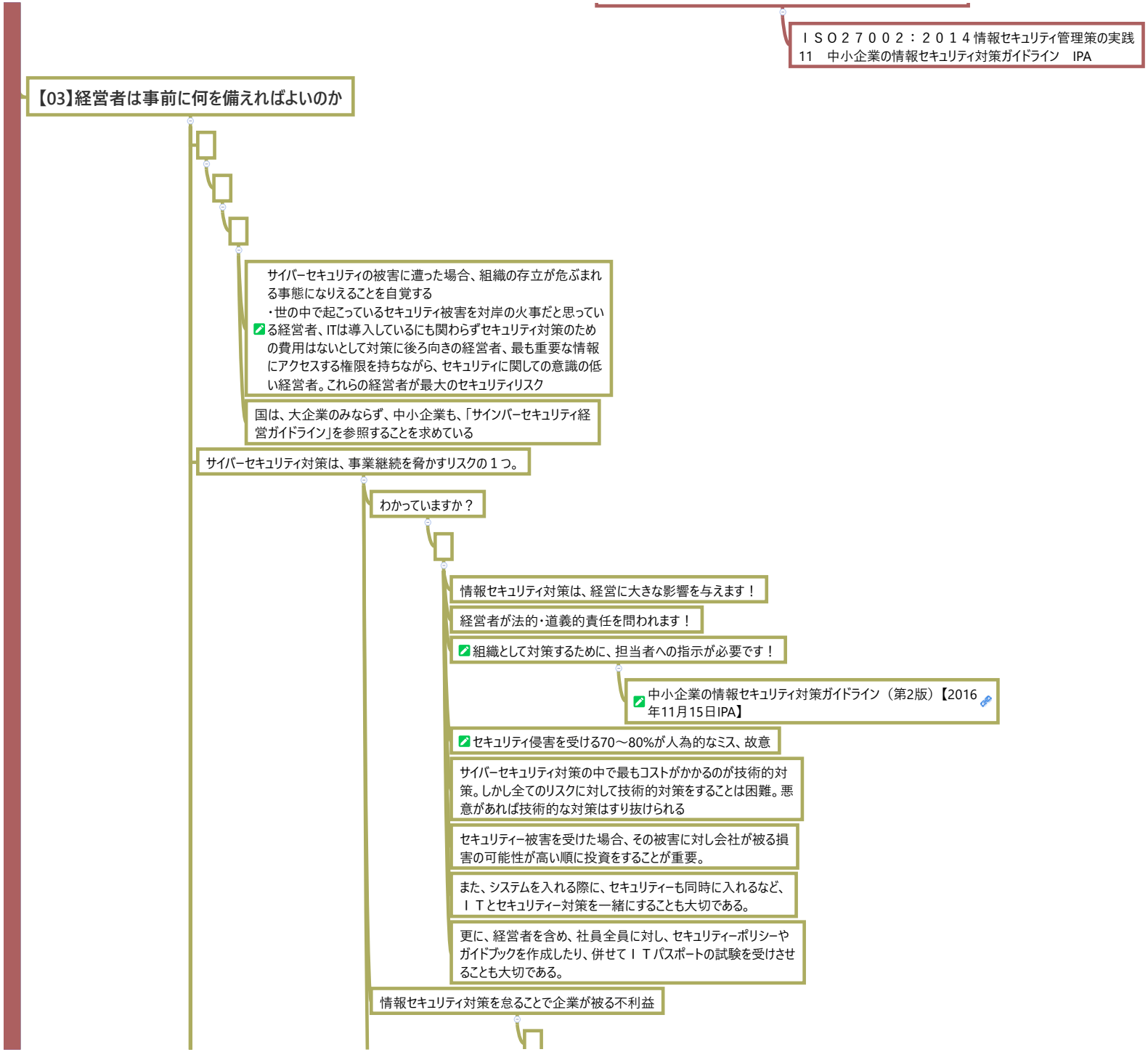
□ＭｙＪＶＮバージョンチェツカの利用

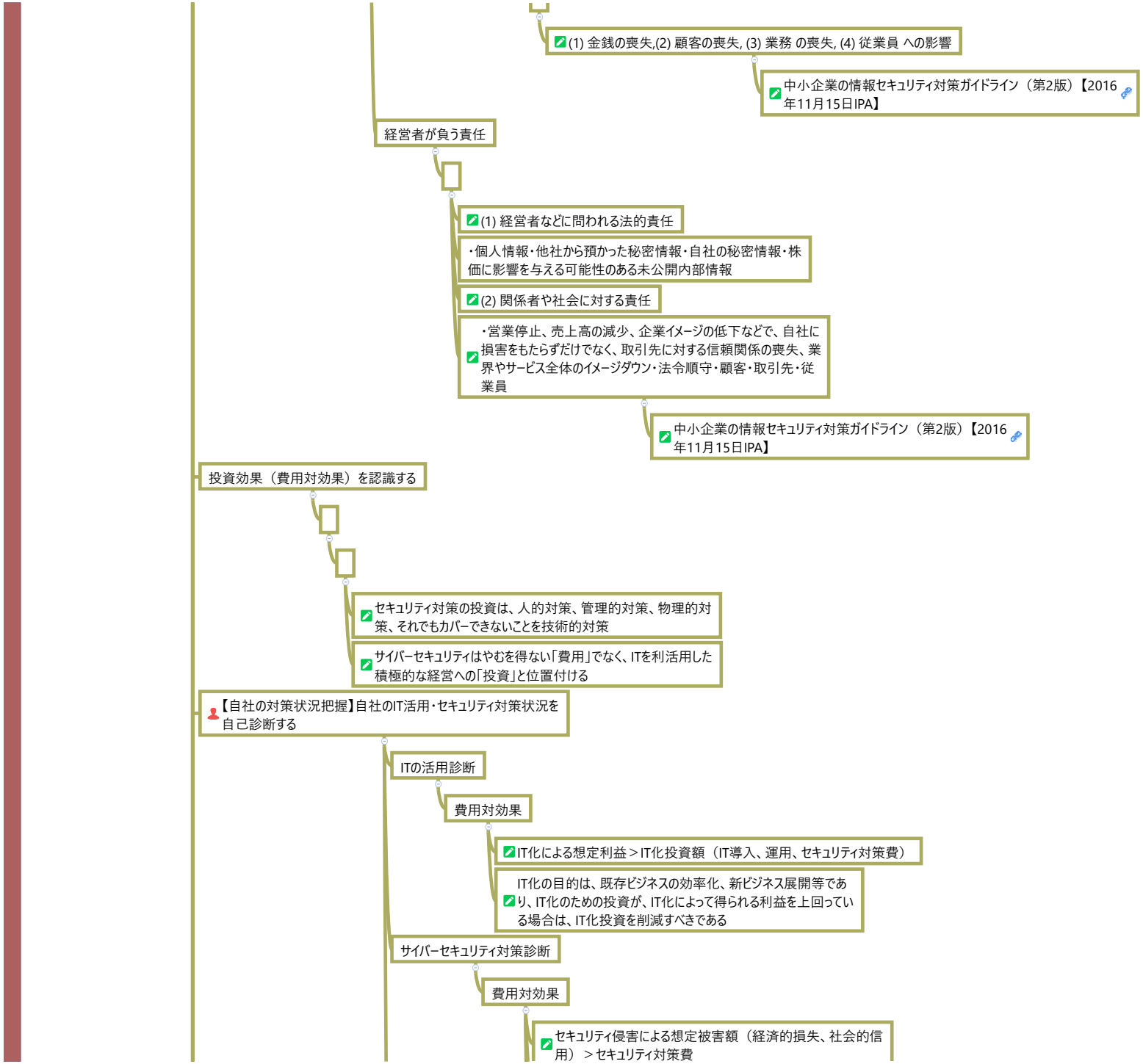

「ＭｙＪＶＮバージョンチェッカ」　IPA
ウイルス対策ソフトの導入
□重要なデータについては、定期にバックアップがとられているかを、確認する。
□ウイルス対策ソフトウェアがインストールされているか確認する。□ウイルス対策ソフトウェアのパター（定義ファイル）が最新になっているかを、確認する。□ウイルス対策ソフトウェアでウイルスが検知された場合、そのことをIT担当者もしくは経営部門等、適切な部門がきちんと把握できる仕組みがあるかを、確認する。
情報セキュリティ５か条 IPA中小企業の情報セキュリティガイドライン
定期にバックアップ
□重要なデータについては、定期にバックアップがとられているかを、確認する。
システムが改ざんや破壊などを受けが場合には、バックアップ名メディアあるいはシステム配布媒体から復旧する。
バックアップデータを記録した時点で既に改ざんやウイルスが潜在している可能を考慮する。"
技術メモ　コンピュータセキュリティインシデントへの対応　IPA
パスワードの管理
パスワードは「長く」「複雑に」「使いまわさない」ようしましょう。
パスワードが推測や解析されたり、ウェー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。
パスワードを強化しよう
・英数字記号を含め８文字以上にする・名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない・同じＩＤ、パスワードをいろいろなうウェブサービスで使いまわさない
情報セキュリティ５か条 IPA中小企業の情報セキュリティガイドライン
アクセス管理
『明確に禁止していないことは、原則的に禁止する』という前提に基づいた規則の設定
不正ログオン対策/アカントとパスワードの設定　特権的アクセス権の割り当て及び利用は、制限し管理することが望ましい。
ＩＳＯ２７００２：２０１４情報セキュリティ管理策の実践
知る必要性（Ｎｅｅｄ　to Know)
各人は、それぞれの職務を実施するために必要な情報へのアクセスだけが認められる。

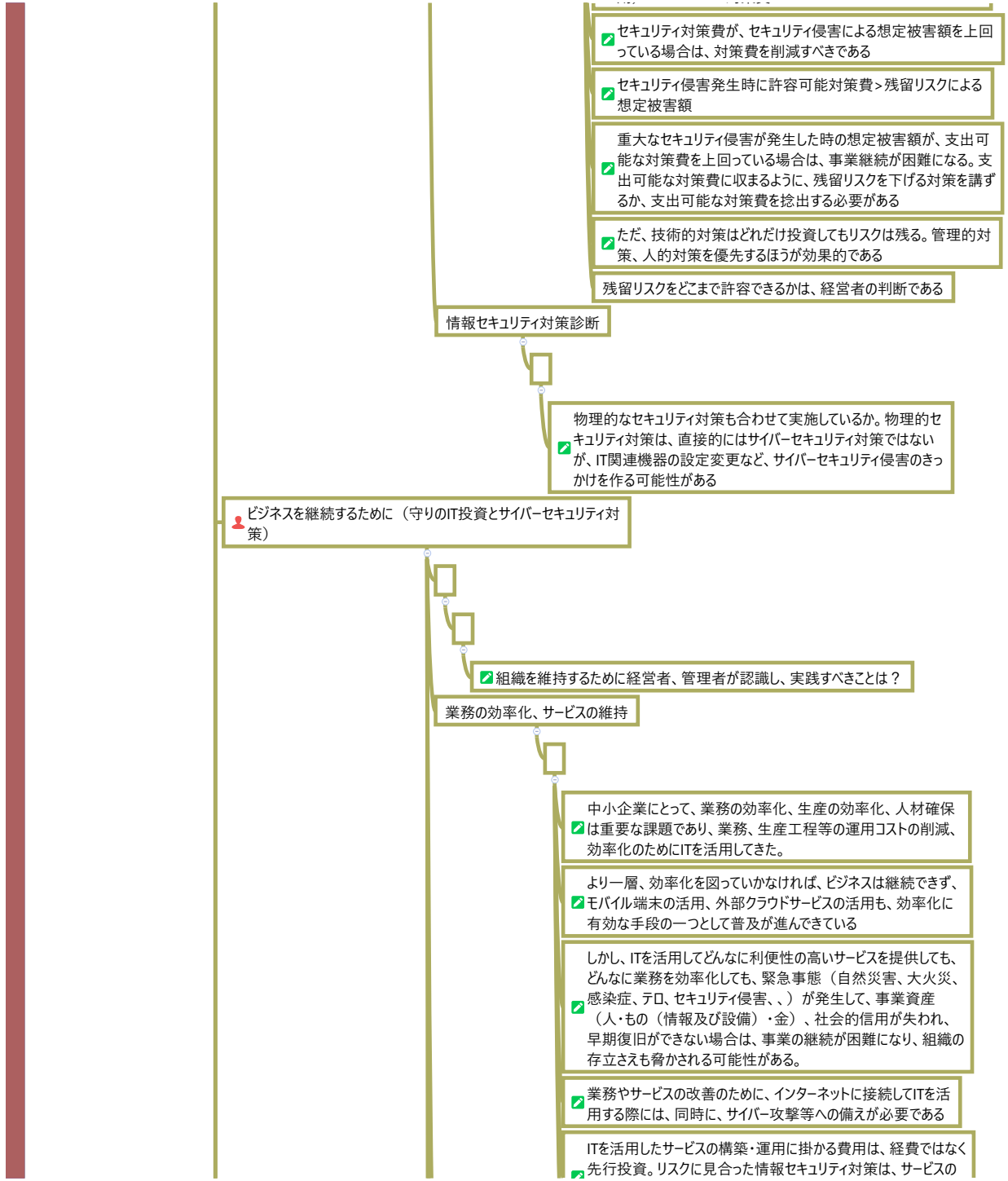

使用する必要性（Ｎｅｅｄ　ｔｏ　Ｕｓｅ）
各人は、それぞれの職務、業務及び/又は役割を実施するために必要な情報処理施設（ＩＴ機器、アプリケーション、手順、部屋など）へのアクセスだけが認められる。
アクセス制御における役割分担
アクセス要求者、アクセス認可、アクセス管理）の分離
□ユーザー毎にアカントを割り当てる□「共有アカント」を利用しない□特権アカントを利用者（標準ユーザ権限）、管理者（ＰＣ管理者権限）に分割し付与する□既定のパスワード（Ａｄｍｉｎ、１２３４５６、ＰＡＳＳ等）を利用しない□既定のＡｄｍｉｎｓｔｒａｔｏｒアカント、Ｇｕｅｓｔアカントを無効にし、管理者用の固有のアカントを設定する□不要になったアカントを削除する（退職者等）
ＩＳＯ２７００２：２０１４情報セキュリティ管理策の実践
（プラス）紛失や盗難による情報漏洩対策
ＰＣディスクの暗号化とパスワード
パソコン、モバイル端末が適切に管理されていない場合は、不正利用、粉失、盗難、情報漏えいの被害が発生する。
【推奨事項】□電源起動時のＢＩＯＳパスワードの設定□取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証の併用□パソコンのデータの暗号化等の機能の有効化（例　Windows　ＢｉｔＬｏｃｋｅｒ　ドライブ暗号化）
帰ったら確認！セキュリティ対策！（東京都中小企業サイバーセキュリティ対策シンポジウム　平成２７年）
「地方公共団体における情報セキュリティポリシーに関するガイドライン」平成２７年３月総務省　P45
（プラス）持ち込み機器対策
電子メール利用への備え
電子メール安全利用
電子メールの誤送信防止のために　電子メールを介したトラブルこんな対策が必要です。
□誤送信防止のためのメーラの設定□メールの暗号化（添付ファイルの暗号化）
標的型メールへの対応
コンピュータウイルス「や標的型攻撃から身を守るために
□メーラーのセキュアな設定□標的型攻撃メール□不審な電子

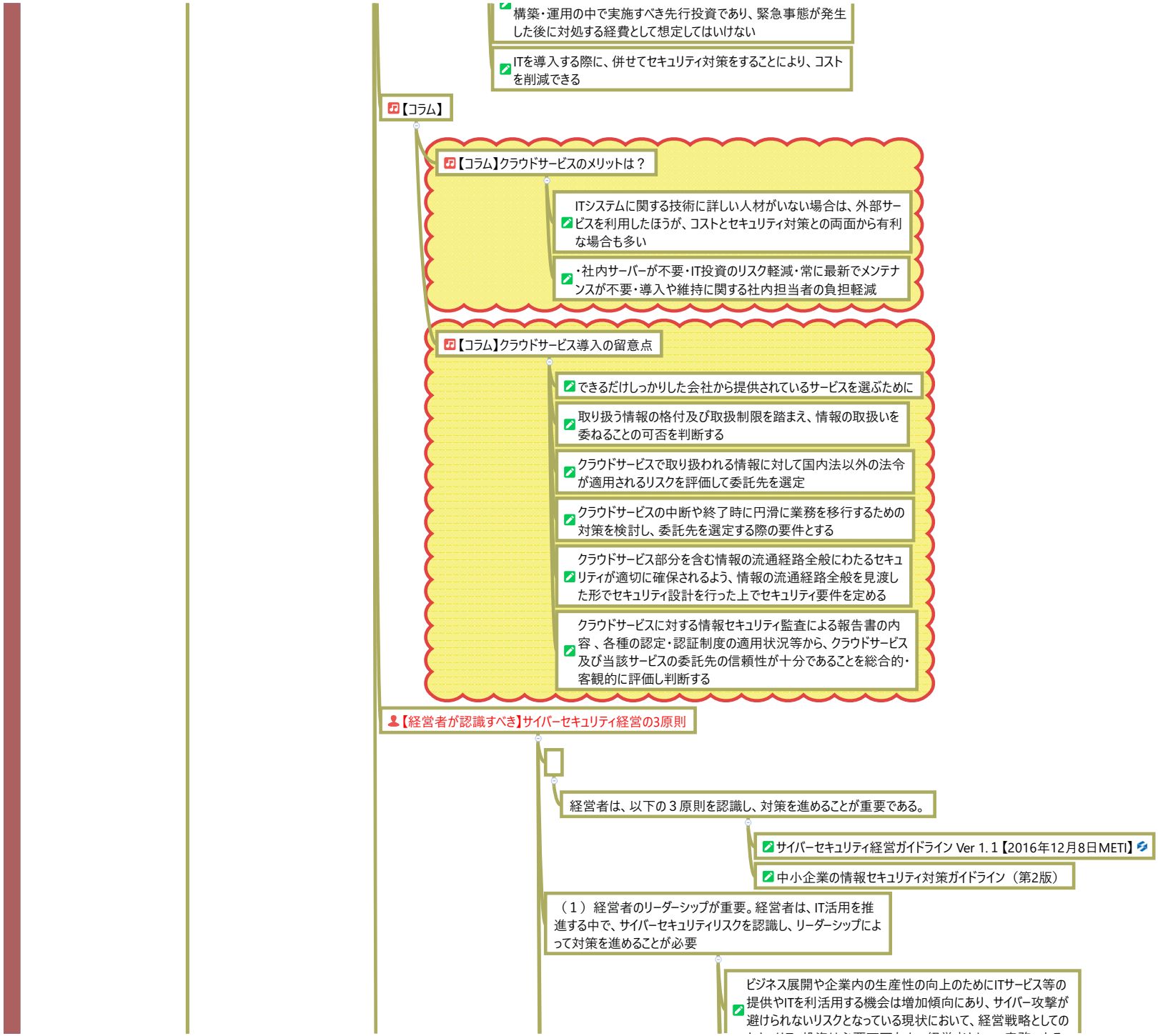

メールの取り扱い
「電子メール利用時の危険対策のしおり」 IPA
迷惑メール発信（踏み台）
インターネットの利用への備え
安全なウエブサイト利用
インターネットに潜む悪意こんな手口に騙されないで
①インターネット上での悪意②悪意の傾向③攻撃者の変化④メールやインスタントメッセージサービス（ＩＭ）を介した悪意⑤ウエブサイトを介した悪意⑥現状での利用者の対策
閲覧制限
重要情報の保管への備え
組織の情報及び情報処理施設に対する認可されていない物理アクセス、損傷及び妨害を防止するため
ＩＳＯ２７００２：２０１４情報セキュリティ管理策の実践　（11物理的及び環境的セキュリティ）
入退室
セキュリティを保つべき領域は、認可された者だけにアクセスを許すしることを確実にするために、適切な入退管理策によって保護することが望ましい。
"取引先または関係者以外が入室した場合い、発見者は声をかけ用件を確認する。最終退室者は作業をルール化する。
ＩＳＯ２７００２：２０１４情報セキュリティ管理策の実践
11 中小企業の情報セキュリティ対策ガイドライン　IPA
装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護することがなお望ましい。
全員のパソコン、プウリンター、複合機、暖房器具、湯沸し器など発熱器の電源ＯＦＦ確認。.全ての出入口の施錠する。退室者の時刻と氏名を記録する。
ＩＳＯ２７００２：２０１４情報セキュリティ管理策の実践
11 中小企業の情報セキュリティ対策ガイドライン　IPA
重要情報の持ち出し

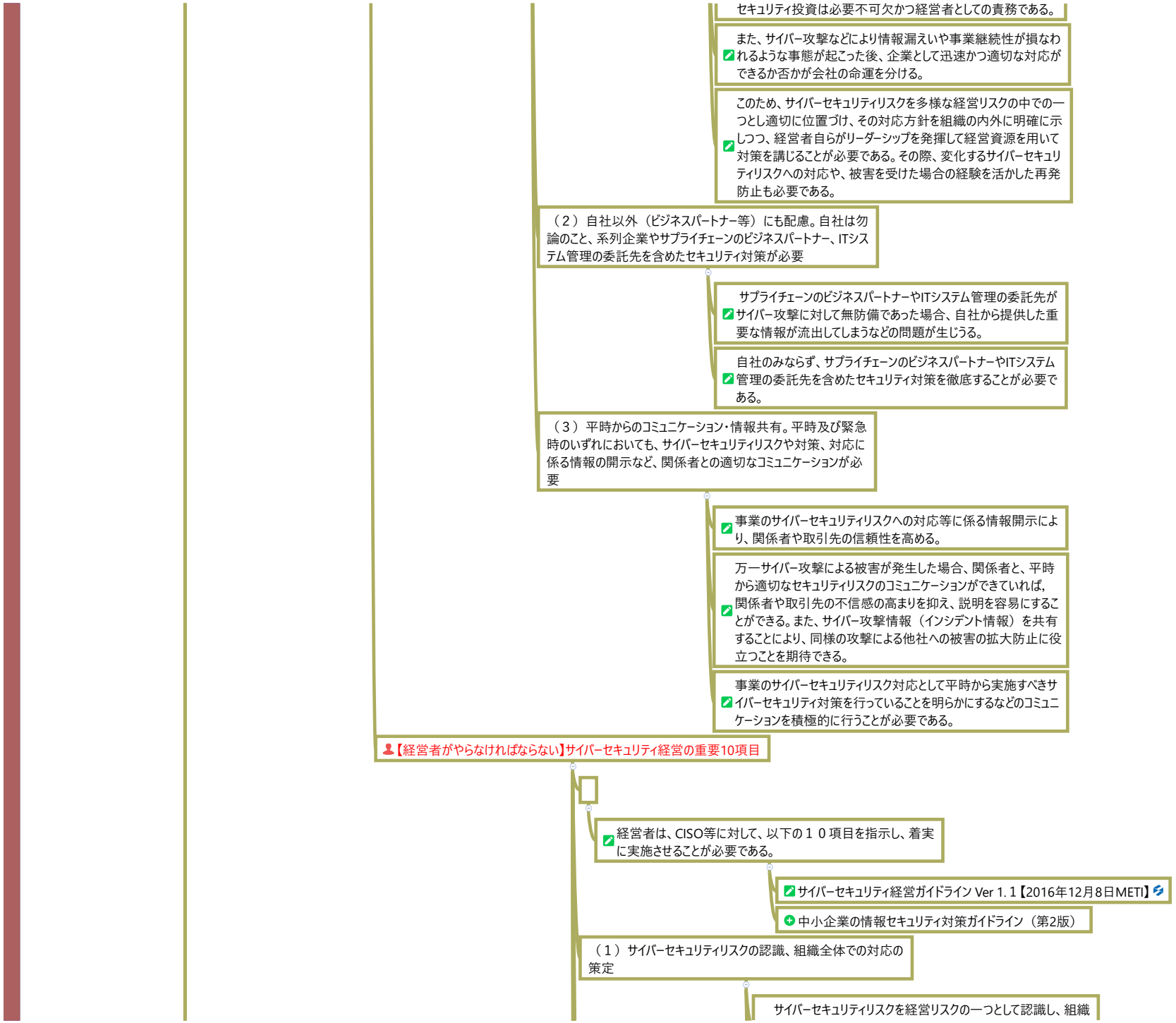

ノートパソコン、タブレット端末、重要な情報を保存したり、小型ハードディスク、ＣＤ等の電子媒体及び重要書類を社外に持ち出すときには以下を徹底する。
①ノートパソコンまたはタブレット端末に保存するデータは最小限にする。②電子媒体はケースに入れ、ＵＳＢメモリはタグ、ストラップ、鈴などを付ける。③書類はひも付き封筒に入れる。④ノートＰＣはＢＩＯＳパスワードとWindowsログインパスワードを設定する。⑤電子データはファイル暗号化またわＵＳＢメモリ暗号化機能により暗号化する。
携帯時には以下に注意する
①電車内では網棚に置かない。離席する場合は携行する。他社から覗き見できない状態で扱う。②自動車では室内、トランク内保管した状態で車外に出ず、携行する。
クリアデスク・クリアスクリーン
□重要書類、スマートフォン、携帯電話、重要な情報を保存したＵＳＢメモリ、小型ハードディスク、ＣＤ等の電子媒体を業務用以外のときは机上に放置せず。クリアディスクを徹底する。
□離席時には以下のいずれかによりパソコンの画面をロックし、クリアスクリーンを徹底する。
①スクリーンセーバー起動時間を１０分以内に設定し、パスワードを設定する。②スリープ起動時間」を１０分以内に設定し、解除時」のパスワード保護を設定する。③離席時には[Windows]＋[Ｌ]キーを押してコンピュータをロックする。
重要情報の保管と廃棄
退社時、未使用時にはモバイル用パソコン」、ＵＳＢメモリ、小型ハードディスク、ＣＤ等の電子媒体及び重要書類を机の引き出しまたは所定のキャビネットに保管し施錠する。
媒体ば不要になった場合は、正式な手順を用いて、セキュティを保って処分する。
【２－５仕事中」のルール　電子媒体・書類の廃棄　参照】
中小企業の情報セキュリティ対策ガイドライン　IPA
モバイル機器（スマホ）機器の利用への備え
私有情報機器利用への備え
モバイル機器の情報セキュリＩテイ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において機器の私的な使用と業務上の使用を区別する。
【３－１全社共通」のルール　私有情報機器の利用　参照】

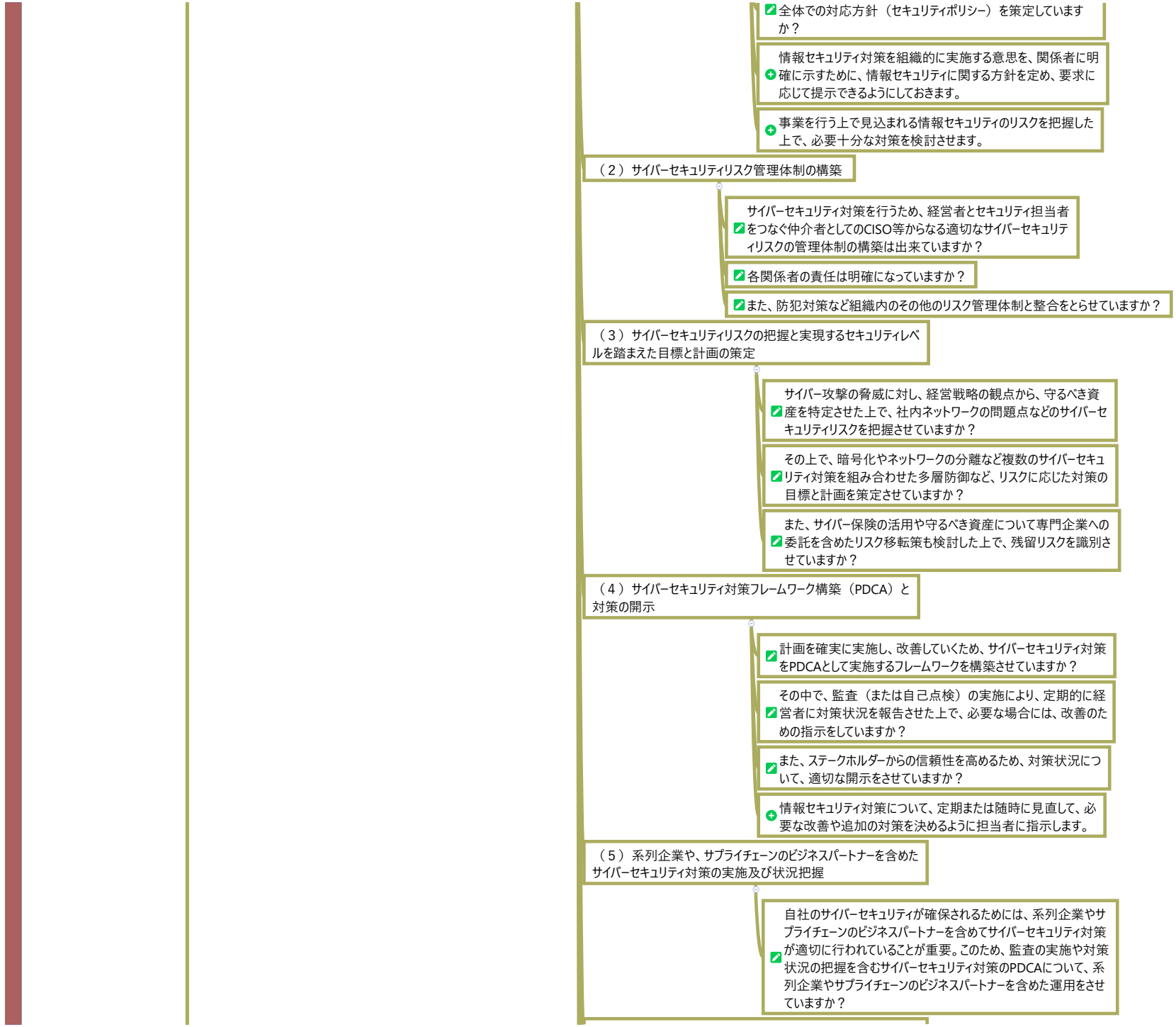

ＩＳＯ２７００２：２０１４情報セキュリティ管理策の実践
11　中小企業の情報セキュリティ対策ガイドライン　IPA
【03】経営者は事前に何を備えればよいのか
サイバーセキュリティの被害に遭った場合、組織の存立が危ぶまれる事態になりえることを自覚する
・世の中で起こっているセキュリティ被害を対岸の火事だと思っている経営者、ITは導入しているにも関わらずセキュリティ対策のための費用はないとして対策に後ろ向きの経営者、最も重要な情報にアクセスする権限を持ちながら、セキュリティに関しての意識の低い経営者。これらの経営者が最大のセキュリティリスク
国は、大企業のみならず、中小企業も、「サインバーセキュリティ経営ガイドライン」を参照することを求めている
サイバーセキュリティ対策は、事業継続を脅かすリスクの１つ。
わかっていますか？
情報セキュリティ対策は、経営に大きな影響を与えます！
経営者が法的・道義的責任を問われます！
組織として対策するために、担当者への指示が必要です！
中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】
セキュリティ侵害を受ける70～80%が人為的なミス、故意
サイバーセキュリティ対策の中で最もコストがかかるのが技術的対策。しかし全てのリスクに対して技術的対策をすることは困難。悪意があれば技術的な対策はすり抜けられる
セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要。
また、システムを入れる際に、セキュリティーも同時に入れるなど、ＩＴとセキュリティー対策を一緒にすることも大切である。
更に、経営者を含め、社員全員に対し、セキュリティーポリシーやガイドブックを作成したり、併せてＩＴパスポートの試験を受けさせることも大切である。
情報セキュリティ対策を怠ることで企業が被る不利益

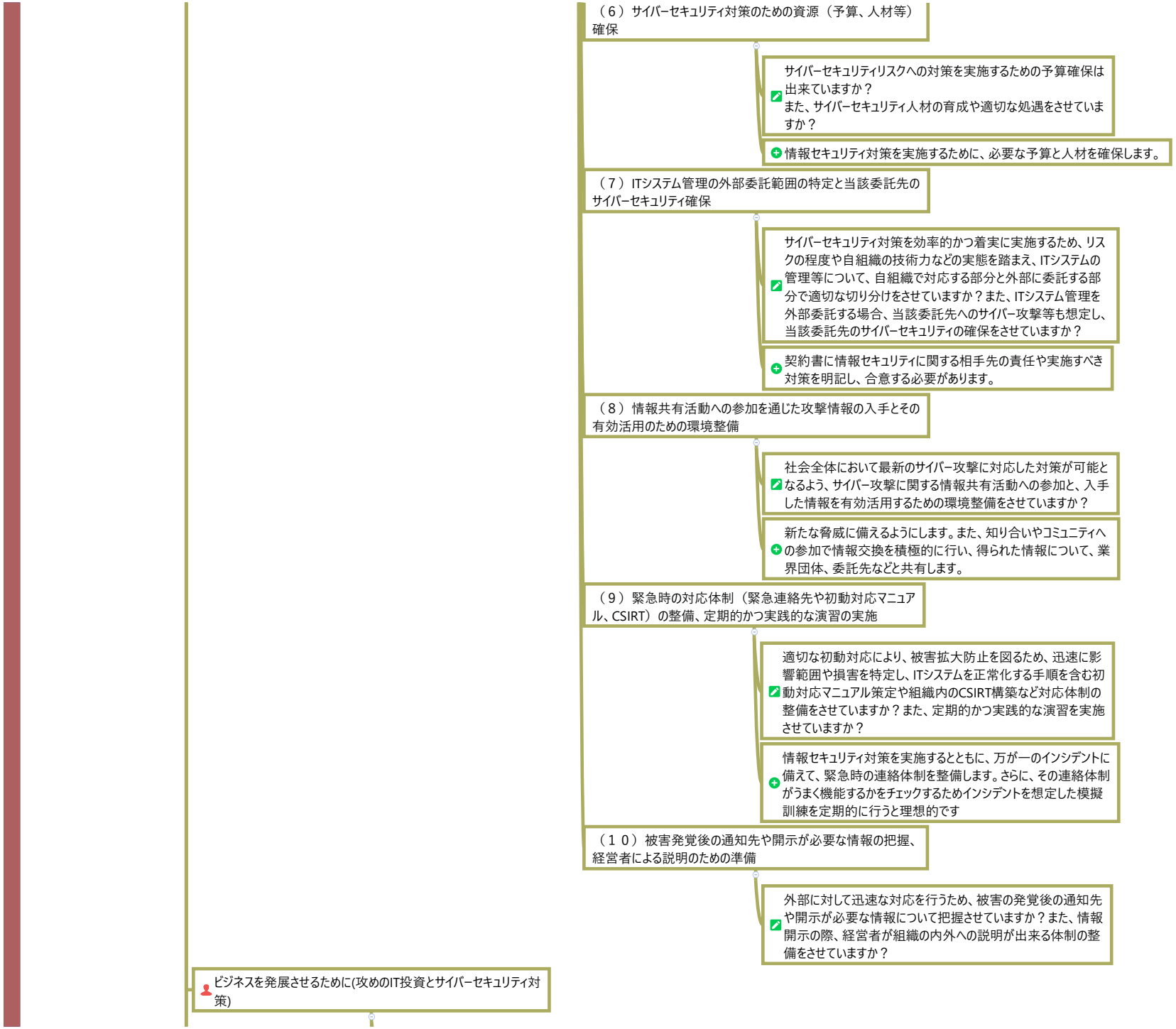

(1) 金銭の喪失,(2) 顧客の喪失, (3) 業務 の喪失, (4) 従業員 への影響
中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】
経営者が負う責任
(1) 経営者などに問われる法的責任
・個人情報・他社から預かった秘密情報・自社の秘密情報・株価に影響を与える可能性のある未公開内部情報
(2) 関係者や社会に対する責任
・営業停止、売上高の減少、企業イメージの低下などで、自社に損害をもたらすだけでなく、取引先に対する信頼関係の喪失、業界やサービス全体のイメージダウン・法令順守・顧客・取引先・従業員
中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】
投資効果（費用対効果）を認識する
セキュリティ対策の投資は、人的対策、管理的対策、物理的対策、それでもカバーできないことを技術的対策
サイバーセキュリティはやむを得ない「費用」でなく、ITを利活用した積極的な経営への「投資」と位置付ける
【自社の対策状況把握】自社のIT活用・セキュリティ対策状況を自己診断する
ITの活用診断
費用対効果
IT化による想定利益＞IT化投資額（IT導入、運用、セキュリティ対策費）
IT化の目的は、既存ビジネスの効率化、新ビジネス展開等であり、IT化のための投資が、IT化によって得られる利益を上回っている場合は、IT化投資を削減すべきである
サイバーセキュリティ対策診断
費用対効果
セキュリティ侵害による想定被害額（経済的損失、社会的信用）＞セキュリティ対策費

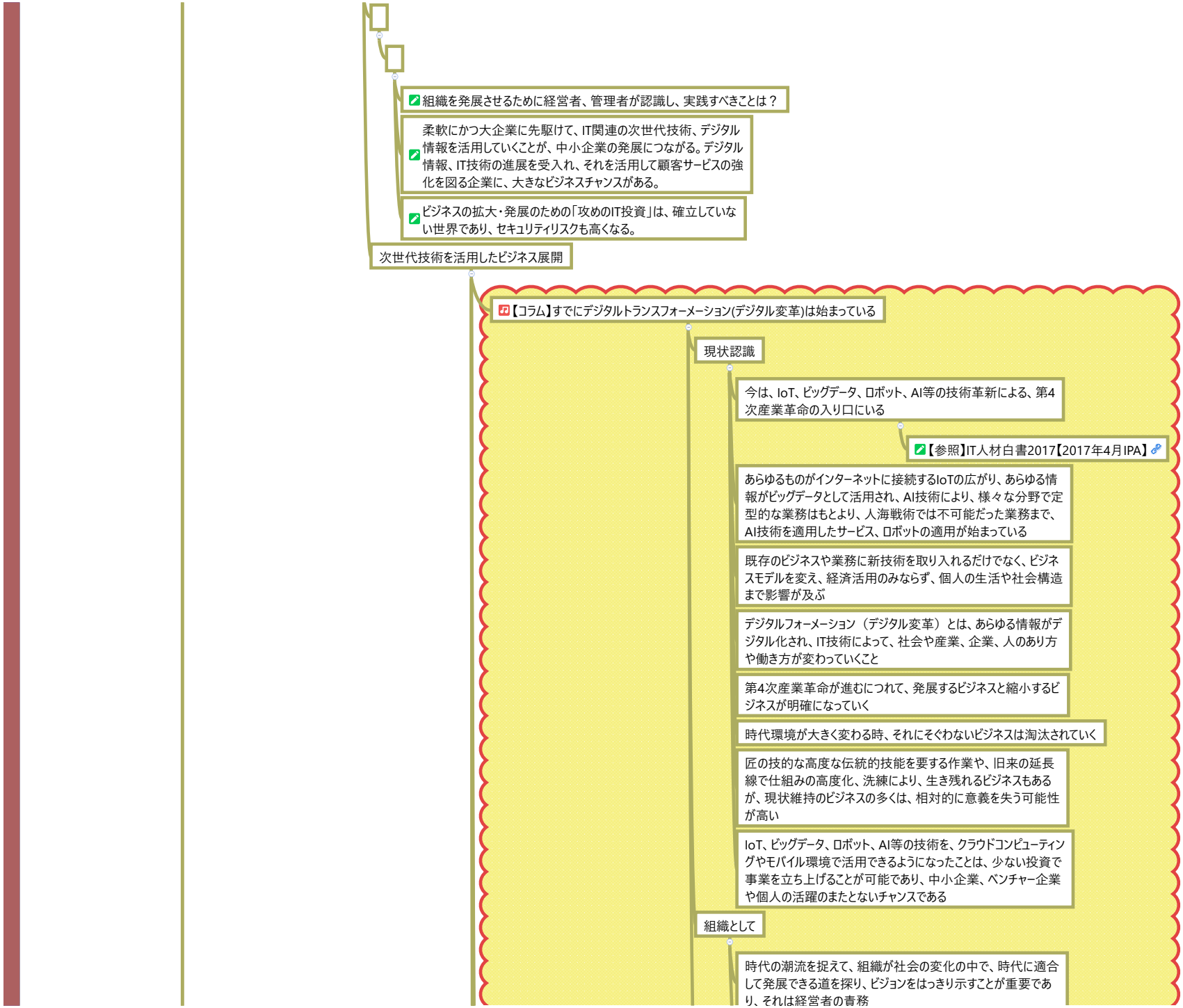

セキュリティ対策費が、セキュリティ侵害による想定被害額を上回っている場合は、対策費を削減すべきである
セキュリティ侵害発生時に許容可能対策費＞残留リスクによる想定被害額
重大なセキュリティ侵害が発生した時の想定被害額が、支出可能な対策費を上回っている場合は、事業継続が困難になる。支出可能な対策費に収まるように、残留リスクを下げる対策を講ずるか、支出可能な対策費を捻出する必要がある
ただ、技術的対策はどれだけ投資してもリスクは残る。管理的対策、人的対策を優先するほうが効果的である
残留リスクをどこまで許容できるかは、経営者の判断である
情報セキュリティ対策診断
物理的なセキュリティ対策も合わせて実施しているか。物理的セキュリティ対策は、直接的にはサイバーセキュリティ対策ではないが、IT関連機器の設定変更など、サイバーセキュリティ侵害のきっかけを作る可能性がある
ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）
組織を維持するために経営者、管理者が認識し、実践すべきことは？
業務の効率化、サービスの維持
中小企業にとって、業務の効率化、生産の効率化、人材確保は重要な課題であり、業務、生産工程等の運用コストの削減、効率化のためにITを活用してきた。
より一層、効率化を図っていかなければ、ビジネスは継続できず、モバイル端末の活用、外部クラウドサービスの活用も、効率化に有効な手段の一つとして普及が進んできている
しかし、ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、セキュリティ侵害、、）が発生して、事業資産（人・もの（情報及び設備）・金）、社会的信用が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性がある。
業務やサービスの改善のために、インターネットに接続してITを活用する際には、同時に、サイバー攻撃等への備えが必要である
ITを活用したサービスの構築・運用に掛かる費用は、経費ではなく先行投資。リスクに見合った情報セキュリティ対策は、サービスの

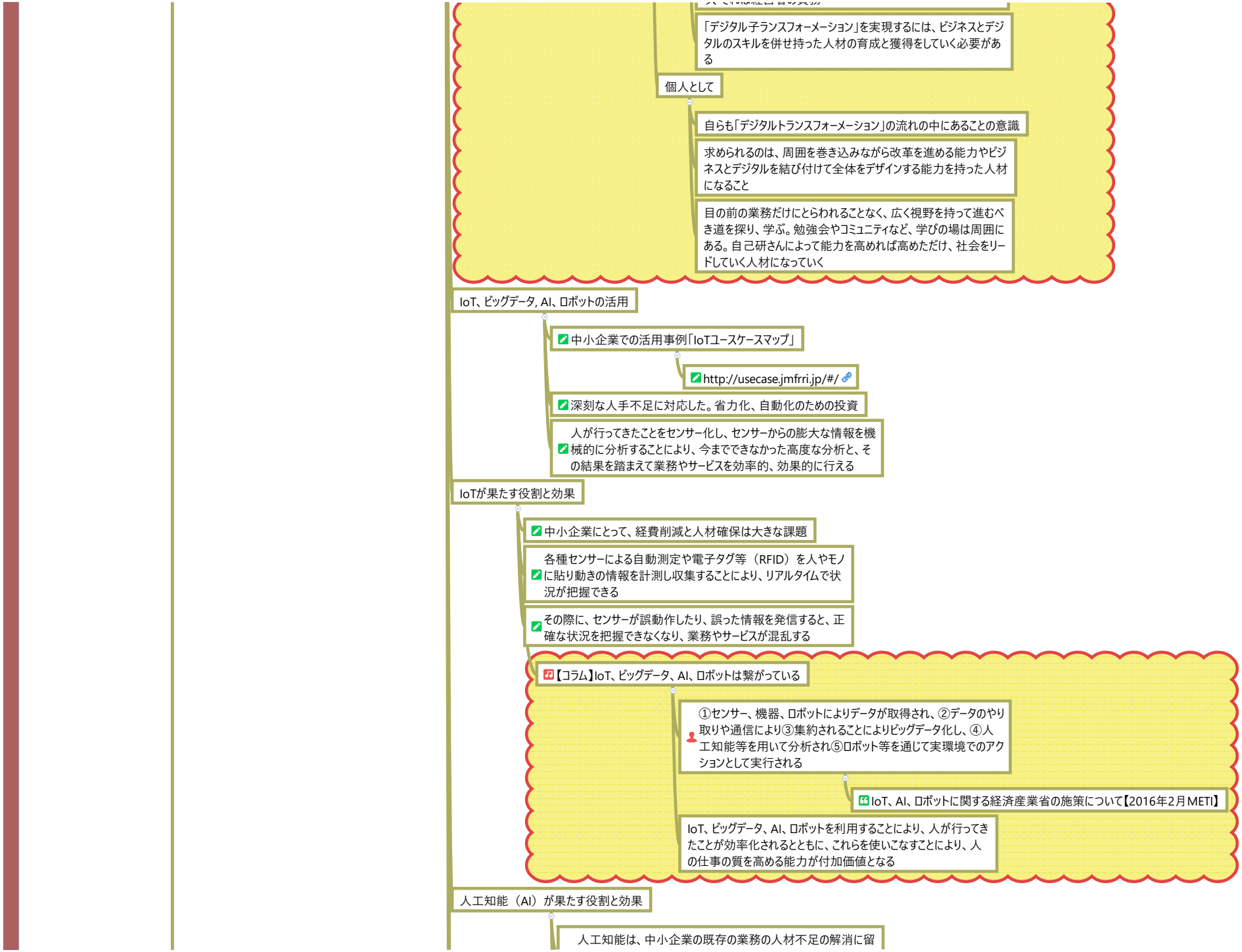

構築・運用の中で実施すべき先行投資であり、緊急事態が発生した後に対処する経費として想定してはいけない
ITを導入する際に、併せてセキュリティ対策をすることにより、コストを削減できる
【コラム】
【コラム】クラウドサービスのメリットは？
ITシステムに関する技術に詳しい人材がいない場合は、外部サービスを利用したほうが、コストとセキュリティ対策との両面から有利な場合も多い
・社内サーバーが不要・IT投資のリスク軽減・常に最新でメンテナンスが不要・導入や維持に関する社内担当者の負担軽減
【コラム】クラウドサービス導入の留意点
できるだけしっかりした会社から提供されているサービスを選ぶために
取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する
クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定
クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とする
クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める
クラウドサービスに対する情報セキュリティ監査による報告書の内容 、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断する
【経営者が認識すべき】サイバーセキュリティ経営の3原則
経営者は、以下の３原則を認識し、対策を進めることが重要である。
サイバーセキュリティ経営ガイドライン Ver 1.1【2016年12月8日METI】
中小企業の情報セキュリティ対策ガイドライン（第2版）
（１）経営者のリーダーシップが重要。経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
ビジネス展開や企業内の生産性の向上のためにITサービス等の提供やITを利活用する機会は増加傾向にあり、サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としての

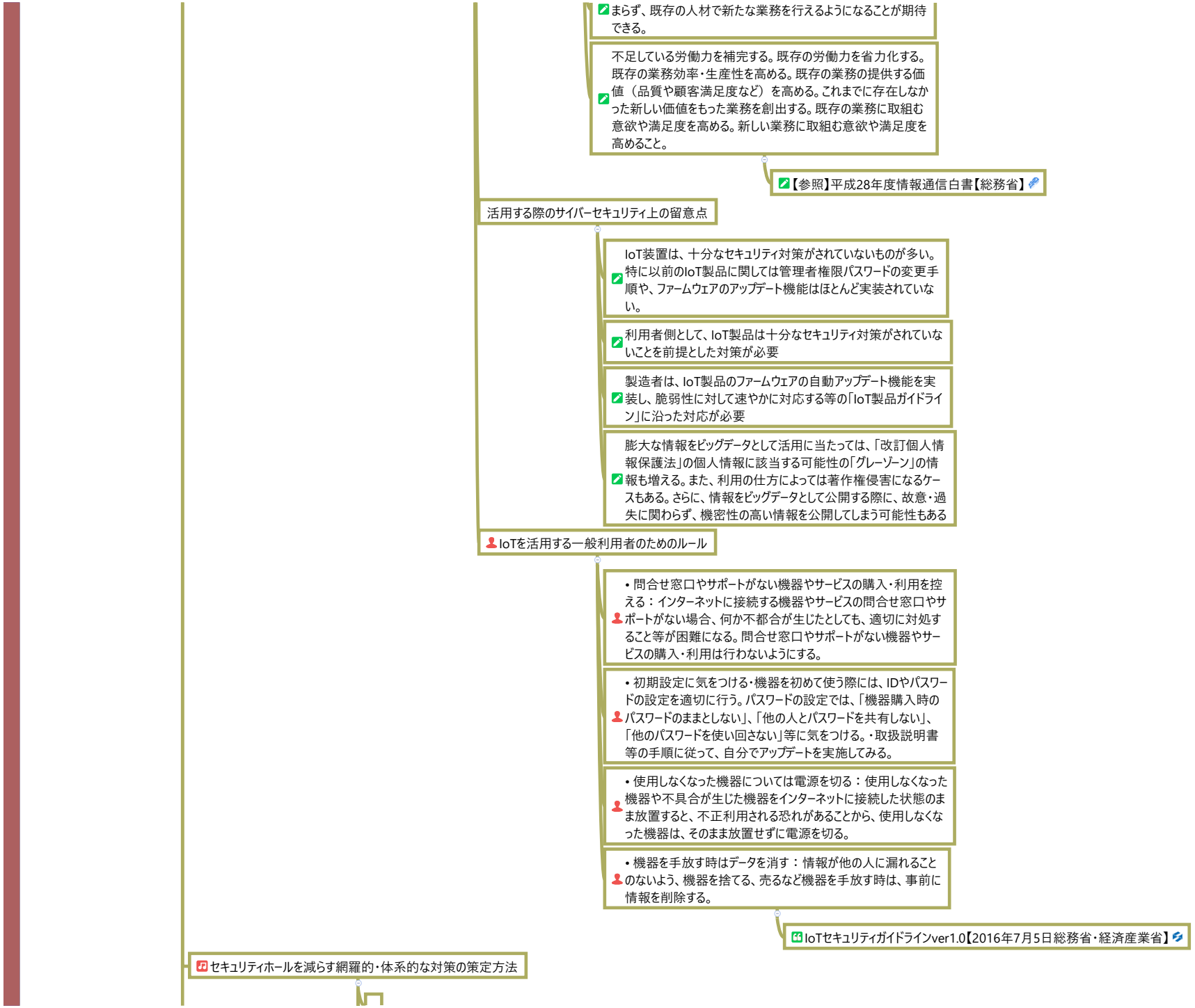

セキュリティ投資は必要不可欠かつ経営者としての責務である。
また、サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった後、企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。
このため、サイバーセキュリティリスクを多様な経営リスクの中での一つとし適切に位置づけ、その対応方針を組織の内外に明確に示しつつ、経営者自らがリーダーシップを発揮して経営資源を用いて対策を講じることが必要である。その際、変化するサイバーセキュリティリスクへの対応や、被害を受けた場合の経験を活かした再発防止も必要である。
（２）自社以外（ビジネスパートナー等）にも配慮。自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要
サプライチェーンのビジネスパートナーやITシステム管理の委託先がサイバー攻撃に対して無防備であった場合、自社から提供した重要な情報が流出してしまうなどの問題が生じうる。
自社のみならず、サプライチェーンのビジネスパートナーやITシステム管理の委託先を含めたセキュリティ対策を徹底することが必要である。
（３）平時からのコミュニケーション・情報共有。平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要
事業のサイバーセキュリティリスクへの対応等に係る情報開示により、関係者や取引先の信頼性を高める。
万一サイバー攻撃による被害が発生した場合、関係者と、平時から適切なセキュリティリスクのコミュニケーションができていれば，関係者や取引先の不信感の高まりを抑え、説明を容易にすることができる。また、サイバー攻撃情報（インシデント情報）を共有することにより、同様の攻撃による他社への被害の拡大防止に役立つことを期待できる。
事業のサイバーセキュリティリスク対応として平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行うことが必要である。
【経営者がやらなければならない】サイバーセキュリティ経営の重要10項目
経営者は、CISO等に対して、以下の１０項目を指示し、着実に実施させることが必要である。
サイバーセキュリティ経営ガイドライン Ver 1.1【2016年12月8日METI】
中小企業の情報セキュリティ対策ガイドライン（第2版）
（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
サイバーセキュリティリスクを経営リスクの一つとして認識し、組織

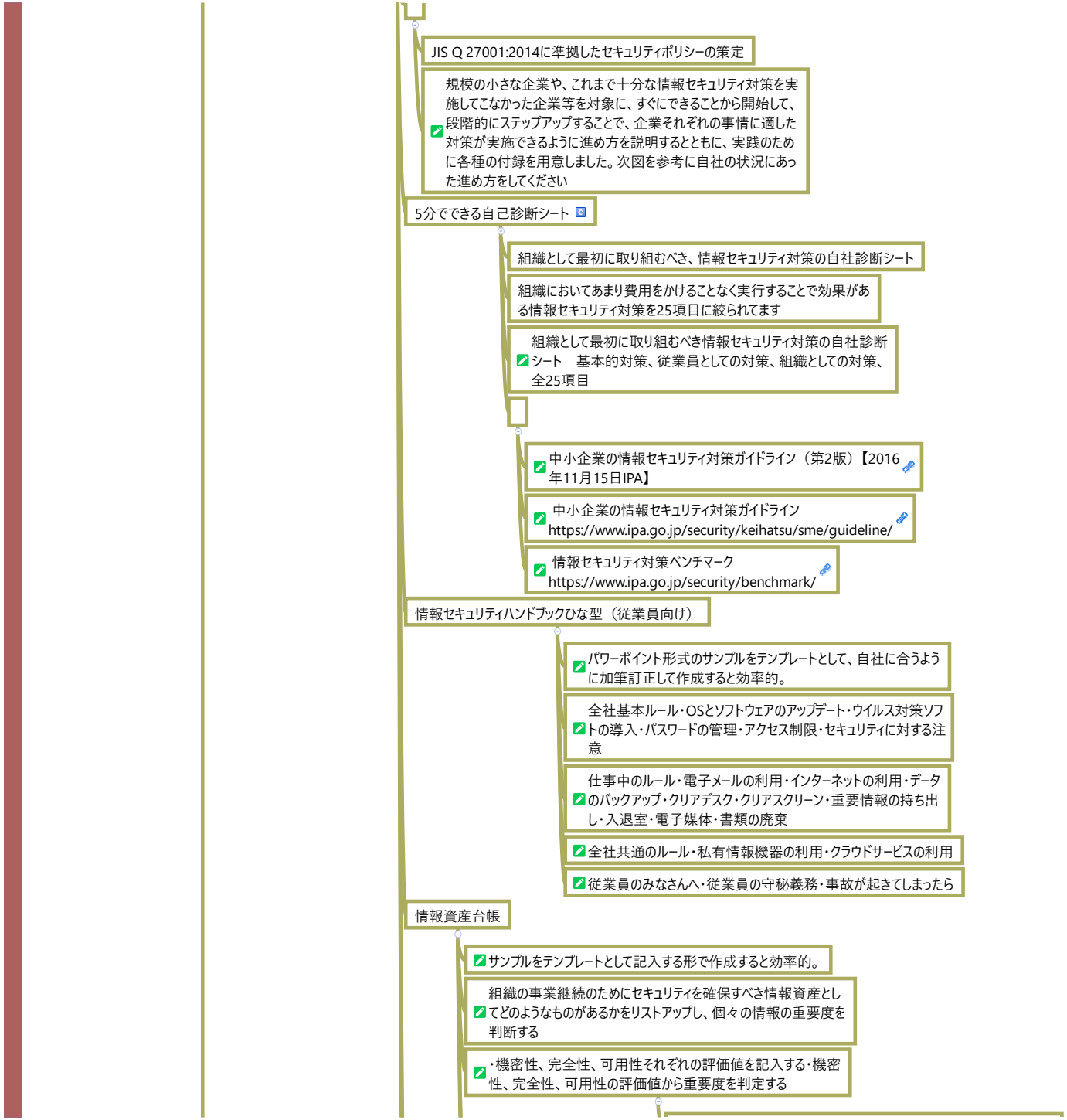

全体での対応方針（セキュリティポリシー）を策定していますか？
情報セキュリティ対策を組織的に実施する意思を、関係者に明確に示すために、情報セキュリティに関する方針を定め、要求に応じて提示できるようにしておきます。
事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な対策を検討させます。
（２）サイバーセキュリティリスク管理体制の構築
サイバーセキュリティ対策を行うため、経営者とセキュリティ担当者をつなぐ仲介者としてのCISO等からなる適切なサイバーセキュリティリスクの管理体制の構築は出来ていますか？
各関係者の責任は明確になっていますか？
また、防犯対策など組織内のその他のリスク管理体制と整合をとらせていますか？
（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
サイバー攻撃の脅威に対し、経営戦略の観点から、守るべき資産を特定させた上で、社内ネットワークの問題点などのサイバーセキュリティリスクを把握させていますか？
その上で、暗号化やネットワークの分離など複数のサイバーセキュリティ対策を組み合わせた多層防御など、リスクに応じた対策の目標と計画を策定させていますか？
また、サイバー保険の活用や守るべき資産について専門企業への委託を含めたリスク移転策も検討した上で、残留リスクを識別させていますか？
（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
計画を確実に実施し、改善していくため、サイバーセキュリティ対策をPDCAとして実施するフレームワークを構築させていますか？
その中で、監査（または自己点検）の実施により、定期的に経営者に対策状況を報告させた上で、必要な場合には、改善のための指示をしていますか？
また、ステークホルダーからの信頼性を高めるため、対策状況について、適切な開示をさせていますか？
情報セキュリティ対策について、定期または随時に見直して、必要な改善や追加の対策を決めるように担当者に指示します。
（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
自社のサイバーセキュリティが確保されるためには、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てサイバーセキュリティ対策が適切に行われていることが重要。このため、監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、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運用をさせていますか？

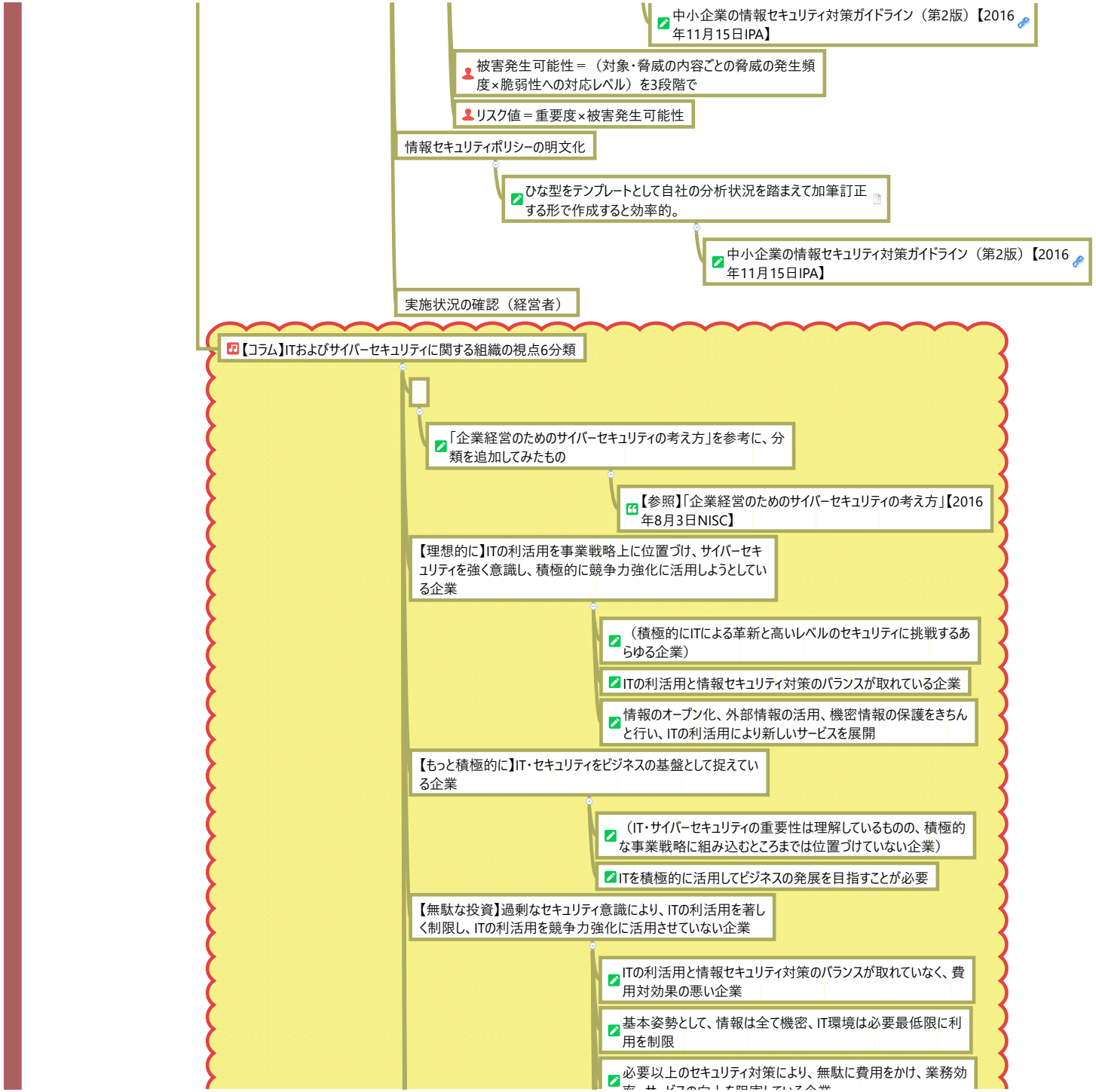

（６）サイバーセキュリティ対策のための資源（予算、人材等）確保
サイバーセキュリティリスクへの対策を実施するための予算確保は出来ていますか？
また、サイバーセキュリティ人材の育成や適切な処遇をさせていますか？
情報セキュリティ対策を実施するために、必要な予算と人材を確保します。
（７）ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
サイバーセキュリティ対策を効率的かつ着実に実施するため、リスクの程度や自組織の技術力などの実態を踏まえ、ITシステムの管理等について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせていますか？また、ITシステム管理を外部委託する場合、当該委託先へのサイバー攻撃等も想定し、当該委託先のサイバーセキュリティの確保をさせていますか？
契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する必要があります。
（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
社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動への参加と、入手した情報を有効活用するための環境整備をさせていますか？
新たな脅威に備えるようにします。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。
（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
適切な初動対応により、被害拡大防止を図るため、迅速に影響範囲や損害を特定し、ITシステムを正常化する手順を含む初動対応マニュアル策定や組織内のCSIRT構築など対応体制の整備をさせていますか？また、定期的かつ実践的な演習を実施させていますか？
情報セキュリティ対策を実施するとともに、万が一のインシデントに備えて、緊急時の連絡体制がうまく機能するかをチェックするためインシデントを想定した模擬訓練を定期的に行うと理想的です
（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
外部に対して迅速な対応を行うため、被害の発覚後の通知先や開示が必要な情報について把握させていますか？また、情報開示の際、経営者が組織の内外への説明が出来る体制の整備をさせていますか？
ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

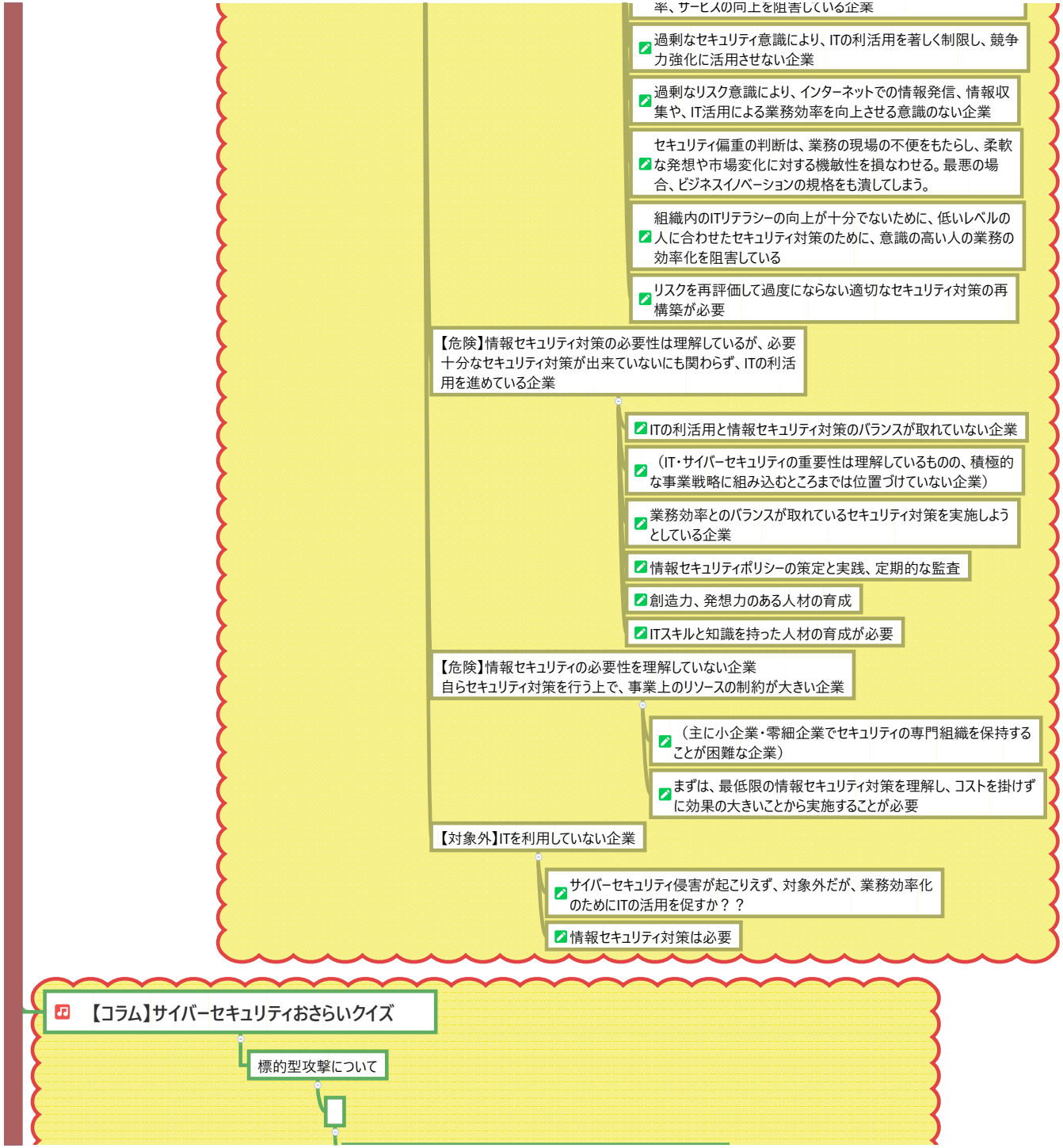

組織を発展させるために経営者、管理者が認識し、実践すべきことは？
柔軟にかつ大企業に先駆けて、IT関連の次世代技術、デジタル情報を活用していくことが、中小企業の発展につながる。デジタル情報、IT技術の進展を受入れ、それを活用して顧客サービスの強化を図る企業に、大きなビジネスチャンスがある。
ビジネスの拡大・発展のための「攻めのIT投資」は、確立していない世界であり、セキュリティリスクも高くなる。
次世代技術を活用したビジネス展開
【コラム】すでにデジタルトランスフォーメーション(デジタル変革)は始まっている
現状認識
今は、IoT、ビッグデータ、ロボット、AI等の技術革新による、第4次産業革命の入り口にいる
【参照】IT人材白書2017【2017年4月IPA】
あらゆるものがインターネットに接続するIoTの広がり、あらゆる情報がビッグデータとして活用され、AI技術により、様々な分野で定型的な業務はもとより、人海戦術では不可能だった業務まで、AI技術を適用したサービス、ロボットの適用が始まっている
既存のビジネスや業務に新技術を取り入れるだけでなく、ビジネスモデルを変え、経済活用のみならず、個人の生活や社会構造まで影響が及ぶ
デジタルフォーメーション（デジタル変革）とは、あらゆる情報がデジタル化され、IT技術によって、社会や産業、企業、人のあり方や働き方が変わっていくこと
第4次産業革命が進むにつれて、発展するビジネスと縮小するビジネスが明確になっていく
時代環境が大きく変わる時、それにそぐわないビジネスは淘汰されていく
匠の技的な高度な伝統的技能を要する作業や、旧来の延長線で仕組みの高度化、洗練により、生き残れるビジネスもあるが、現状維持のビジネスの多くは、相対的に意義を失う可能性が高い
IoT、ビッグデータ、ロボット、AI等の技術を、クラウドコンピューティングやモバイル環境で活用できるようになったことは、少ない投資で事業を立ち上げることが可能であり、中小企業、ベンチャー企業や個人の活躍のまたとないチャンスである
組織として
時代の潮流を捉えて、組織が社会の変化の中で、時代に適合して発展できる道を探り、ビジョンをはっきり示すことが重要であり、それは経営者の責務

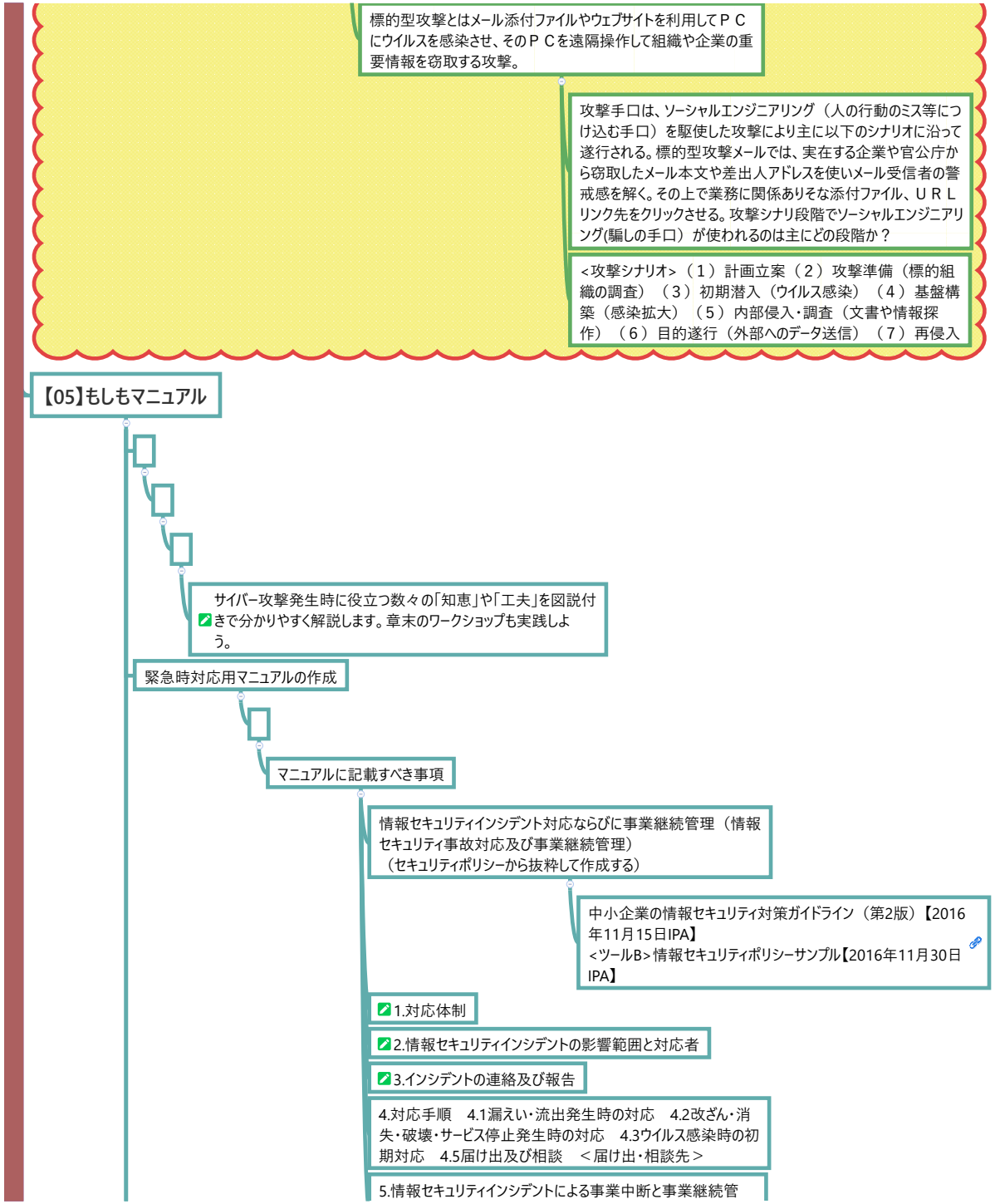

「デジタル子ランスフォーメーション」を実現するには、ビジネスとデジタルのスキルを併せ持った人材の育成と獲得をしていく必要がある
個人として
自らも「デジタルトランスフォーメーション」の流れの中にあることの意識
求められるのは、周囲を巻き込みながら改革を進める能力やビジネスとデジタルを結び付けて全体をデザインする能力を持った人材になること
目の前の業務だけにとらわれることなく、広く視野を持って進むべき道を探り、学ぶ。勉強会やコミュニティなど、学びの場は周囲にある。自己研さんによって能力を高めれば高めただけ、社会をリードしていく人材になっていく
IoT、ビッグデータ, AI、ロボットの活用
中小企業での活用事例「IoTユースケースマップ」
http://usecase.jmfrri.jp/#/
深刻な人手不足に対応した。省力化、自動化のための投資
人が行ってきたことをセンサー化し、センサーからの膨大な情報を機械的に分析することにより、今までできなかった高度な分析と、その結果を踏まえて業務やサービスを効率的、効果的に行える
IoTが果たす役割と効果
中小企業にとって、経費削減と人材確保は大きな課題
各種センサーによる自動測定や電子タグ等（RFID）を人やモノに貼り動きの情報を計測し収集することにより、リアルタイムで状況が把握できる
その際に、センサーが誤動作したり、誤った情報を発信すると、正確な状況を把握できなくなり、業務やサービスが混乱する
【コラム】IoT、ビッグデータ、AI、ロボットは繋がっている
①センサー、機器、ロボットによりデータが取得され、②データのやり取りや通信により③集約されることによりビッグデータ化し、④人工知能等を用いて分析され⑤ロボット等を通じて実環境でのアクションとして実行される
IoT、AI、ロボットに関する経済産業省の施策について【2016年2月METI】
IoT、ビッグデータ、AI、ロボットを利用することにより、人が行ってきたことが効率化されるとともに、これらを使いこなすことにより、人の仕事の質を高める能力が付加価値となる
人工知能（AI）が果たす役割と効果
人工知能は、中小企業の既存の業務の人材不足の解消に留

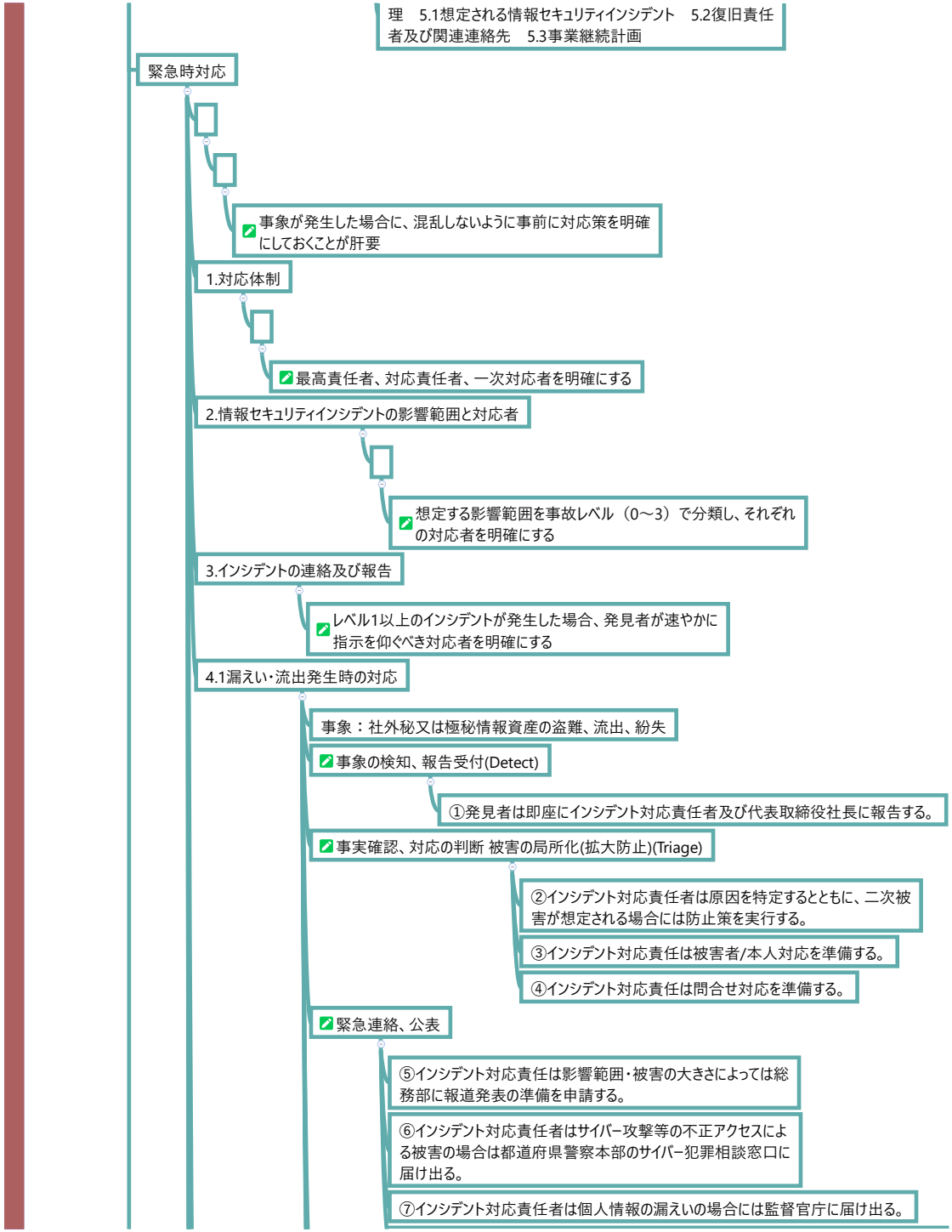

まらず、既存の人材で新たな業務を行えるようになることが期待できる。
不足している労働力を補完する。既存の労働力を省力化する。既存の業務効率・生産性を高める。既存の業務の提供する価値（品質や顧客満足度など）を高める。これまでに存在しなかった新しい価値をもった業務を創出する。既存の業務に取組む意欲や満足度を高める。新しい業務に取組む意欲や満足度を高めること。
【参照】平成28年度情報通信白書【総務省】
活用する際のサイバーセキュリティ上の留意点
IoT装置は、十分なセキュリティ対策がされていないものが多い。特に以前のIoT製品に関しては管理者権限パスワードの変更手順や、ファームウェアのアップデート機能はほとんど実装されていない。
利用者側として、IoT製品は十分なセキュリティ対策がされていないことを前提とした対策が必要
製造者は、IoT製品のファームウェアの自動アップデート機能を実装し、脆弱性に対して速やかに対応する等の「IoT製品ガイドライン」に沿った対応が必要
膨大な情報をビッグデータとして活用に当たっては、「改訂個人情報保護法」の個人情報に該当する可能性の「グレーゾーン」の情報も増える。また、利用の仕方によっては著作権侵害になるケースもある。さらに、情報をビッグデータとして公開する際に、故意・過失に関わらず、機密性の高い情報を公開してしまう可能性もある
IoTを活用する一般利用者のためのルール
• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える：インターネットに接続する機器やサービスの問合せ窓口やサポートがない場合、何か不都合が生じたとしても、適切に対処すること等が困難になる。問合せ窓口やサポートがない機器やサービスの購入・利用は行わないようにする。
• 初期設定に気をつける・機器を初めて使う際には、IDやパスワードの設定を適切に行う。パスワードの設定では、「機器購入時のパスワードのままとしない」、「他の人とパスワードを共有しない」、「他のパスワードを使い回さない」等に気をつける。・取扱説明書等の手順に従って、自分でアップデートを実施してみる。
• 使用しなくなった機器については電源を切る：使用しなくなった機器や不具合が生じた機器をインターネットに接続した状態のまま放置すると、不正利用される恐れがあることから、使用しなくなった機器は、そのまま放置せずに電源を切る。
• 機器を手放す時はデータを消す：情報が他の人に漏れることのないよう、機器を捨てる、売るなど機器を手放す時は、事前に情報を削除する。
IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】
セキュリティホールを減らす網羅的・体系的な対策の策定方法

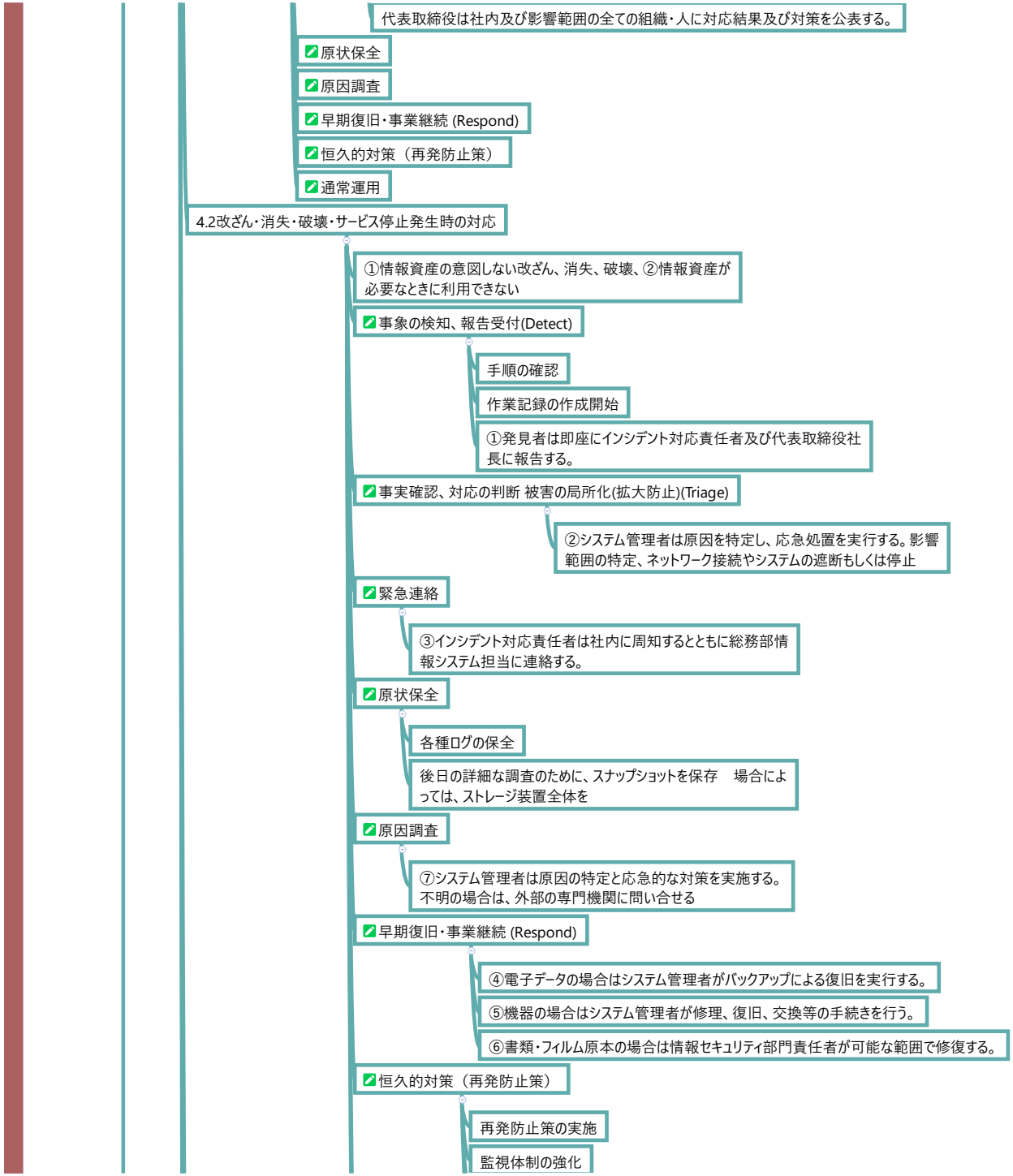

JIS Q 27001:2014に準拠したセキュリティポリシーの策定
規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業等を対象に、すぐにできることから開始して、段階的にステップアップすることで、企業それぞれの事情に適した対策が実施できるように進め方を説明するとともに、実践のために各種の付録を用意しました。次図を参考に自社の状況にあった進め方をしてください
5分でできる自己診断シート
組織として最初に取り組むべき、情報セキュリティ対策の自社診断シート
組織においてあまり費用をかけることなく実行することで効果がある情報セキュリティ対策を25項目に絞られてます
組織として最初に取り組むべき情報セキュリティ対策の自社診断シート　基本的対策、従業員としての対策、組織としての対策、全25項目
中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】
中小企業の情報セキュリティ対策ガイドライン https://www.ipa.go.jp/security/keihatsu/sme/guideline/
情報セキュリティ対策ベンチマーク https://www.ipa.go.jp/security/benchmark/
情報セキュリティハンドブックひな型（従業員向け）
パワーポイント形式のサンプルをテンプレートとして、自社に合うように加筆訂正して作成すると効率的。
全社基本ルール・OSとソフトウェアのアップデート・ウイルス対策ソフトの導入・パスワードの管理・アクセス制限・セキュリティに対する注意
仕事中のルール・電子メールの利用・インターネットの利用・データのバックアップ・クリアデスク・クリアスクリーン・重要情報の持ち出し・入退室・電子媒体・書類の廃棄
全社共通のルール・私有情報機器の利用・クラウドサービスの利用
従業員のみなさんへ・従業員の守秘義務・事故が起きてしまったら
情報資産台帳
サンプルをテンプレートとして記入する形で作成すると効率的。
組織の事業継続のためにセキュリティを確保すべき情報資産としてどのようなものがあるかをリストアップし、個々の情報の重要度を判断する
・機密性、完全性、可用性それぞれの評価値を記入する・機密性、完全性、可用性の評価値から重要度を判定する

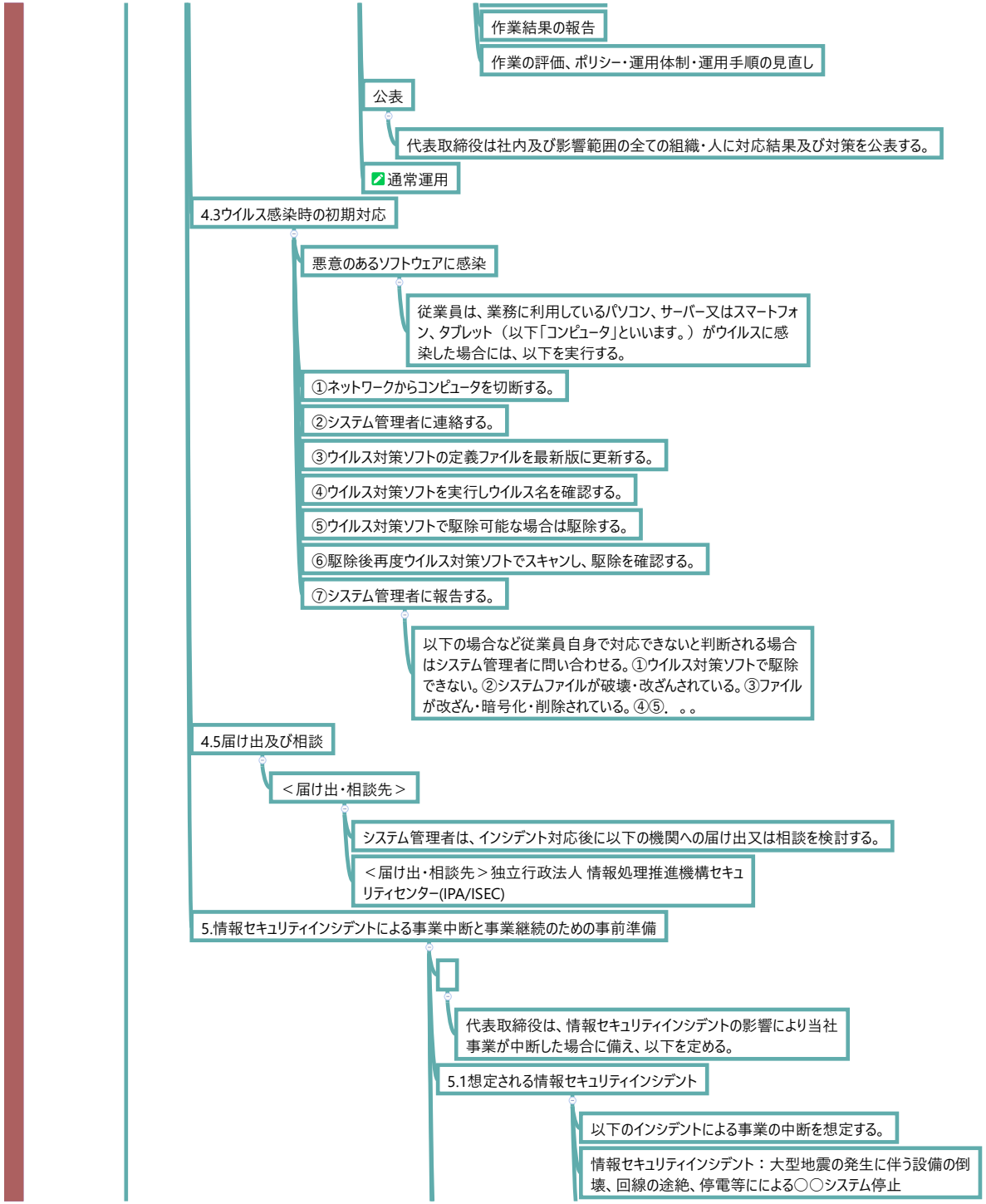

中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】
被害発生可能性＝（対象・脅威の内容ごとの脅威の発生頻度×脆弱性への対応レベル）を3段階で
リスク値＝重要度×被害発生可能性
情報セキュリティポリシーの明文化
ひな型をテンプレートとして自社の分析状況を踏まえて加筆訂正する形で作成すると効率的。
中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】
実施状況の確認（経営者）
【コラム】ITおよびサイバーセキュリティに関する組織の視点6分類
「企業経営のためのサイバーセキュリティの考え方」を参考に、分類を追加してみたもの
【参照】「企業経営のためのサイバーセキュリティの考え方」【2016年8月3日NISC】
【理想的に】ITの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に競争力強化に活用しようとしている企業
（積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）
ITの利活用と情報セキュリティ対策のバランスが取れている企業
情報のオープン化、外部情報の活用、機密情報の保護をきちんと行い、ITの利活用により新しいサービスを展開
【もっと積極的に】IT・セキュリティをビジネスの基盤として捉えている企業
（IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置づけていない企業）
ITを積極的に活用してビジネスの発展を目指すことが必要
【無駄な投資】過剰なセキュリティ意識により、ITの利活用を著しく制限し、ITの利活用を競争力強化に活用させていない企業
ITの利活用と情報セキュリティ対策のバランスが取れていなく、費用対効果の悪い企業
基本姿勢として、情報は全て機密、IT環境は必要最低限に利用を制限
必要以上のセキュリティ対策により、無駄に費用をかけ、業務効

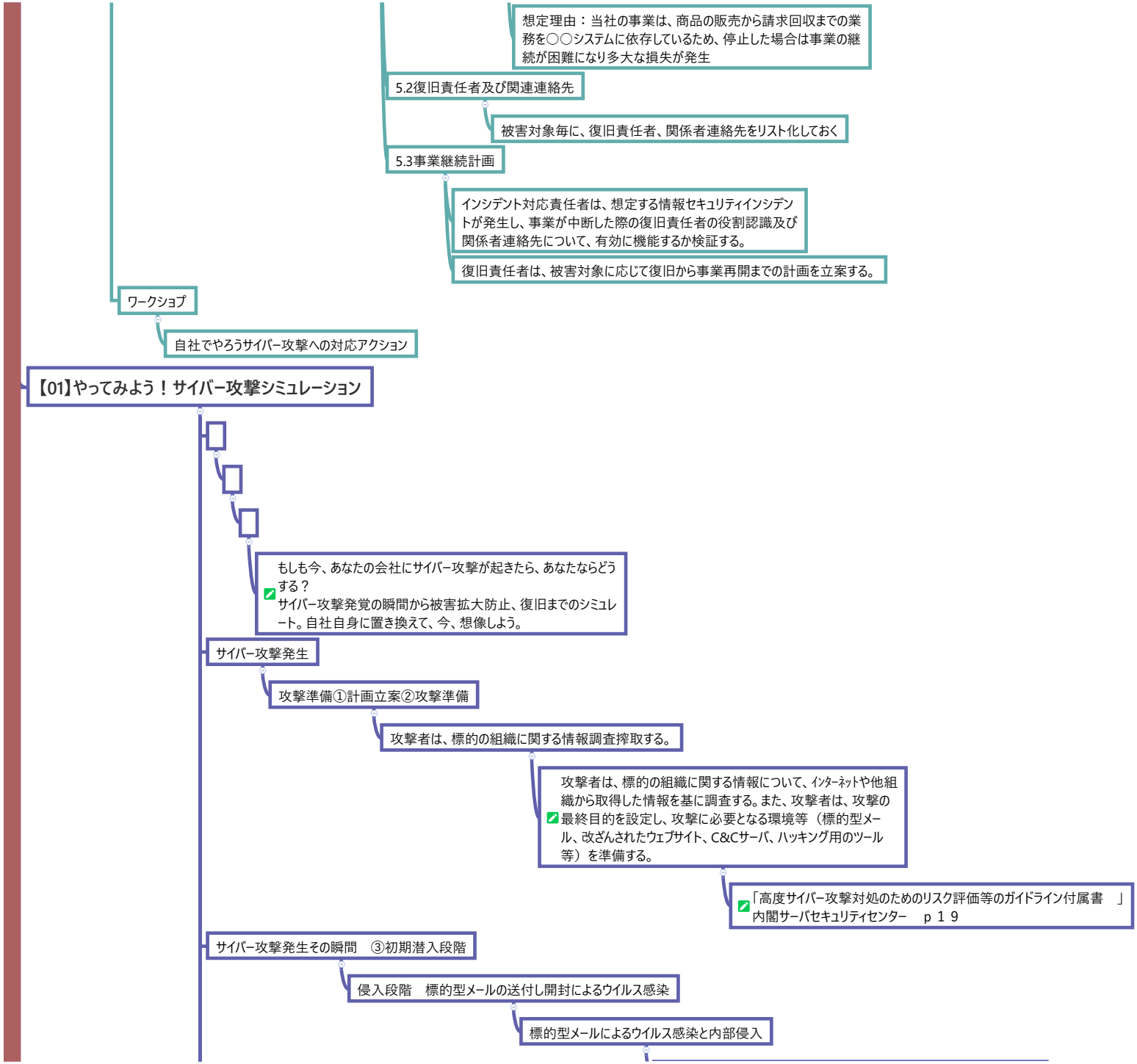

率、サービスの向上を阻害している企業
過剰なセキュリティ意識により、ITの利活用を著しく制限し、競争力強化に活用させない企業
過剰なリスク意識により、インターネットでの情報発信、情報収集や、IT活用による業務効率を向上させる意識のない企業
セキュリティ偏重の判断は、業務の現場の不便をもたらし、柔軟な発想や市場変化に対する機敏性を損なわせる。最悪の場合、ビジネスイノベーションの規格をも潰してしまう。
組織内のITリテラシーの向上が十分でないために、低いレベルの人に合わせたセキュリティ対策のために、意識の高い人の業務の効率化を阻害している
リスクを再評価して過度にならない適切なセキュリティ対策の再構築が必要
【危険】情報セキュリティ対策の必要性は理解しているが、必要十分なセキュリティ対策が出来ていないにも関わらず、ITの利活用を進めている企業
ITの利活用と情報セキュリティ対策のバランスが取れていない企業
（IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置づけていない企業）
業務効率とのバランスが取れているセキュリティ対策を実施しようとしている企業
情報セキュリティポリシーの策定と実践、定期的な監査
創造力、発想力のある人材の育成
ITスキルと知識を持った人材の育成が必要
【危険】情報セキュリティの必要性を理解していない企業
自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業
（主に小企業・零細企業でセキュリティの専門組織を保持することが困難な企業）
まずは、最低限の情報セキュリティ対策を理解し、コストを掛けずに効果の大きいことから実施することが必要
【対象外】ITを利用していない企業
サイバーセキュリティ侵害が起こりえず、対象外だが、業務効率化のためにITの活用を促すか？？
情報セキュリティ対策は必要
【コラム】サイバーセキュリティおさらいクイズ
標的型攻撃について

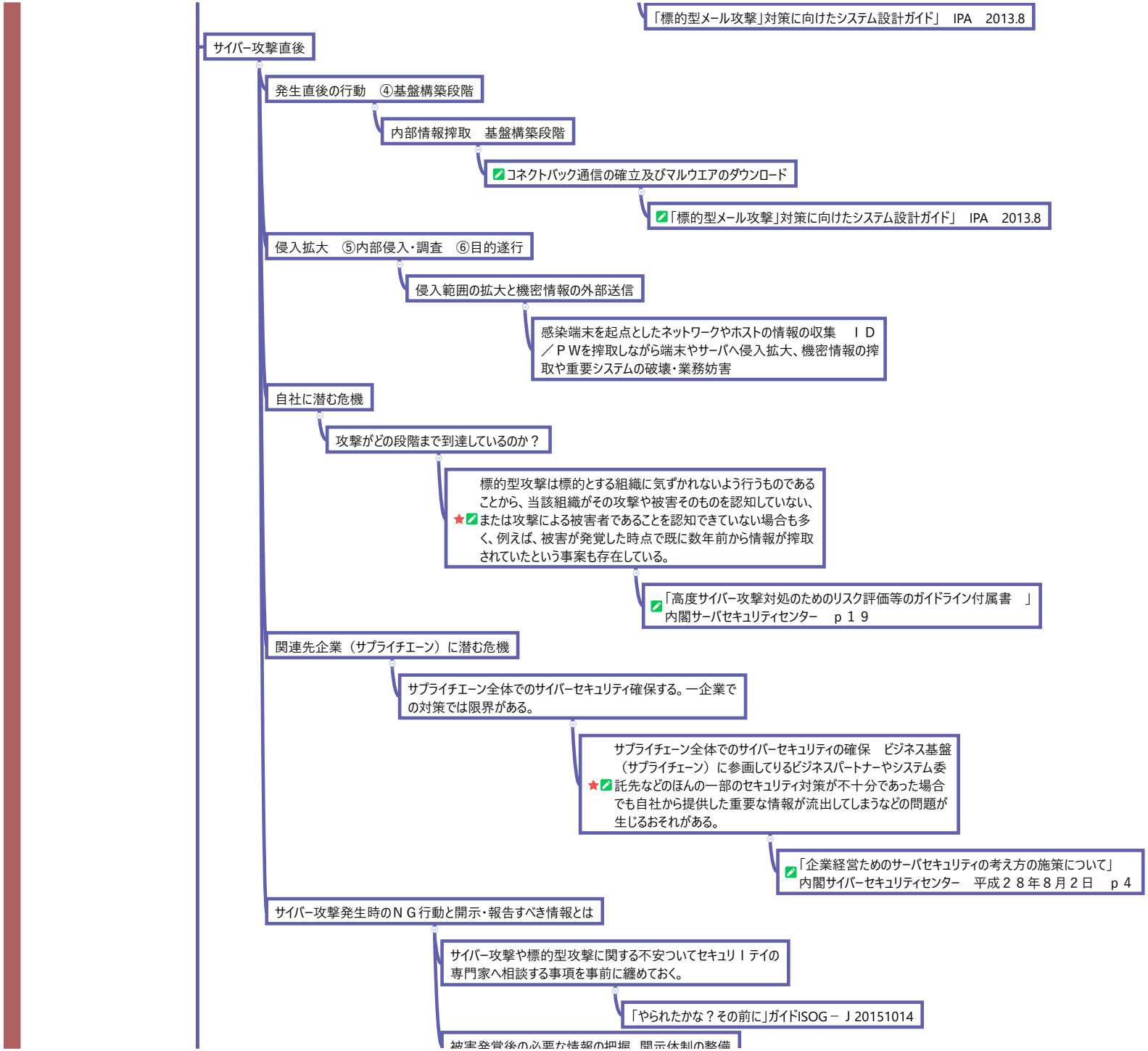

標的型攻撃とはメール添付ファイルやウェブサイトを利用してＰＣにウイルスを感染させ、そのＰＣを遠隔操作して組織や企業の重要情報を窃取する攻撃。
攻撃手口は、ソーシャルエンジニアリング（人の行動のミス等につけ込む手口）を駆使した攻撃により主に以下のシナリオに沿って遂行される。標的型攻撃メールでは、実在する企業や官公庁から窃取したメール本文や差出人アドレスを使いメール受信者の警戒感を解く。その上で業務に関係ありそな添付ファイル、ＵＲＬリンク先をクリックさせる。攻撃シナリ段階でソーシャルエンジニアリング(騙しの手口）が使われるのは主にどの段階か？
<攻撃シナリオ>（１）計画立案（２）攻撃準備（標的組織の調査）（３）初期潜入（ウイルス感染）（４）基盤構築（感染拡大）（５）内部侵入・調査（文書や情報探作）（６）目的遂行（外部へのデータ送信）（７）再侵入
【05】もしもマニュアル
サイバー攻撃発生時に役立つ数々の「知恵」や「工夫」を図説付きで分かりやすく解説します。章末のワークショップも実践しよう。
緊急時対応用マニュアルの作成
マニュアルに記載すべき事項
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（情報セキュリティ事故対応及び事業継続管理）
（セキュリティポリシーから抜粋して作成する）
中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】
<ツールB>情報セキュリティポリシーサンプル【2016年11月30日IPA】
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届け出及び相談　＜届け出・相談先＞
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

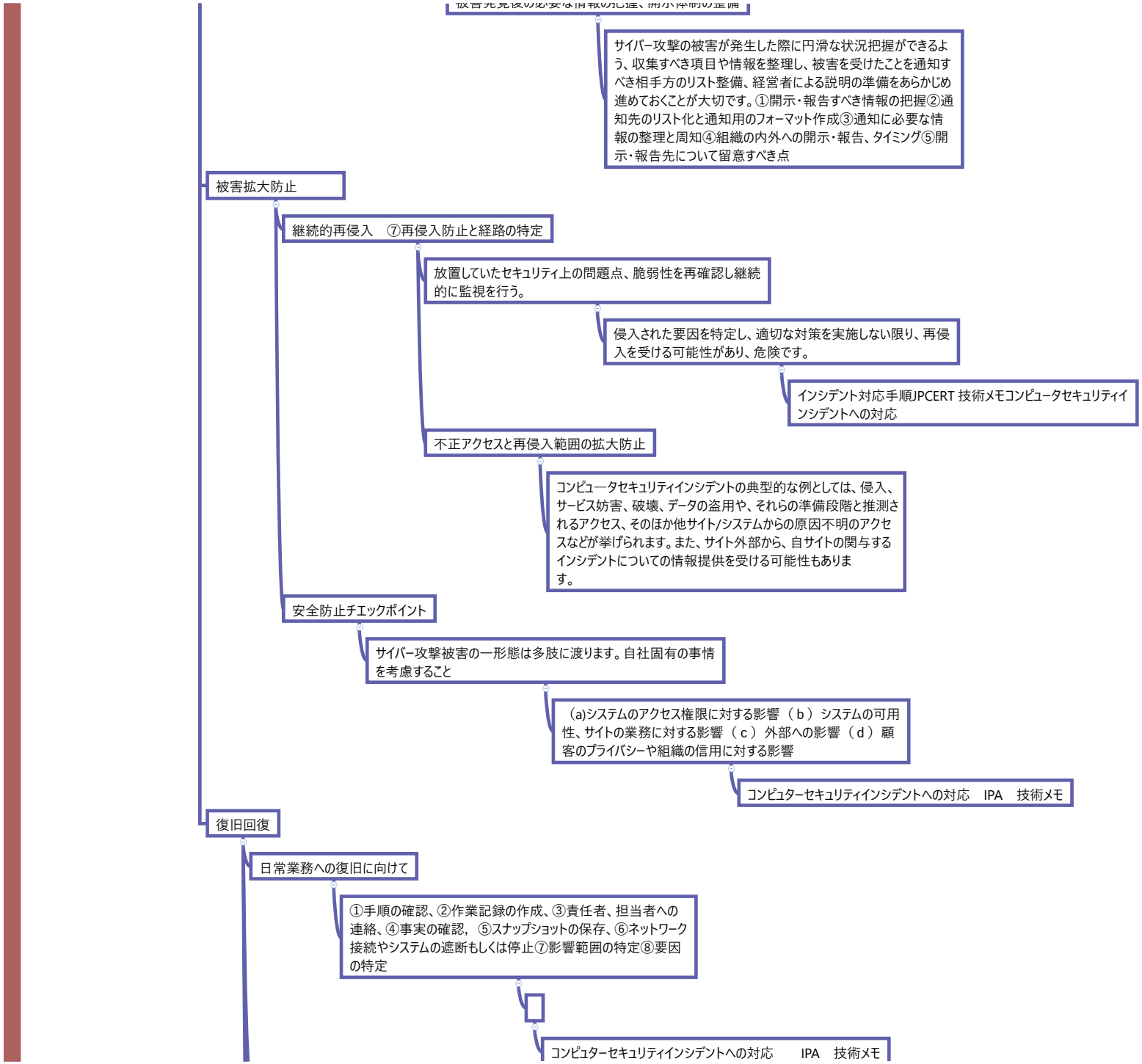

理　5.1想定される情報セキュリティインシデント　5.2復旧責任者及び関連連絡先　5.3事業継続計画
緊急時対応
事象が発生した場合に、混乱しないように事前に対応策を明確にしておくことが肝要
1.対応体制
最高責任者、対応責任者、一次対応者を明確にする
2.情報セキュリティインシデントの影響範囲と対応者
想定する影響範囲を事故レベル（0～3）で分類し、それぞれの対応者を明確にする
3.インシデントの連絡及び報告
レベル1以上のインシデントが発生した場合、発見者が速やかに指示を仰ぐべき対応者を明確にする
4.1漏えい・流出発生時の対応
事象：社外秘又は極秘情報資産の盗難、流出、紛失
事象の検知、報告受付(Detect)
①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。
事実確認、対応の判断 被害の局所化(拡大防止)(Triage)
②インシデント対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。
③インシデント対応責任は被害者/本人対応を準備する。
④インシデント対応責任は問合せ対応を準備する。
緊急連絡、公表
⑤インシデント対応責任は影響範囲・被害の大きさによっては総務部に報道発表の準備を申請する。
⑥インシデント対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出る。
⑦インシデント対応責任者は個人情報の漏えいの場合には監督官庁に届け出る。

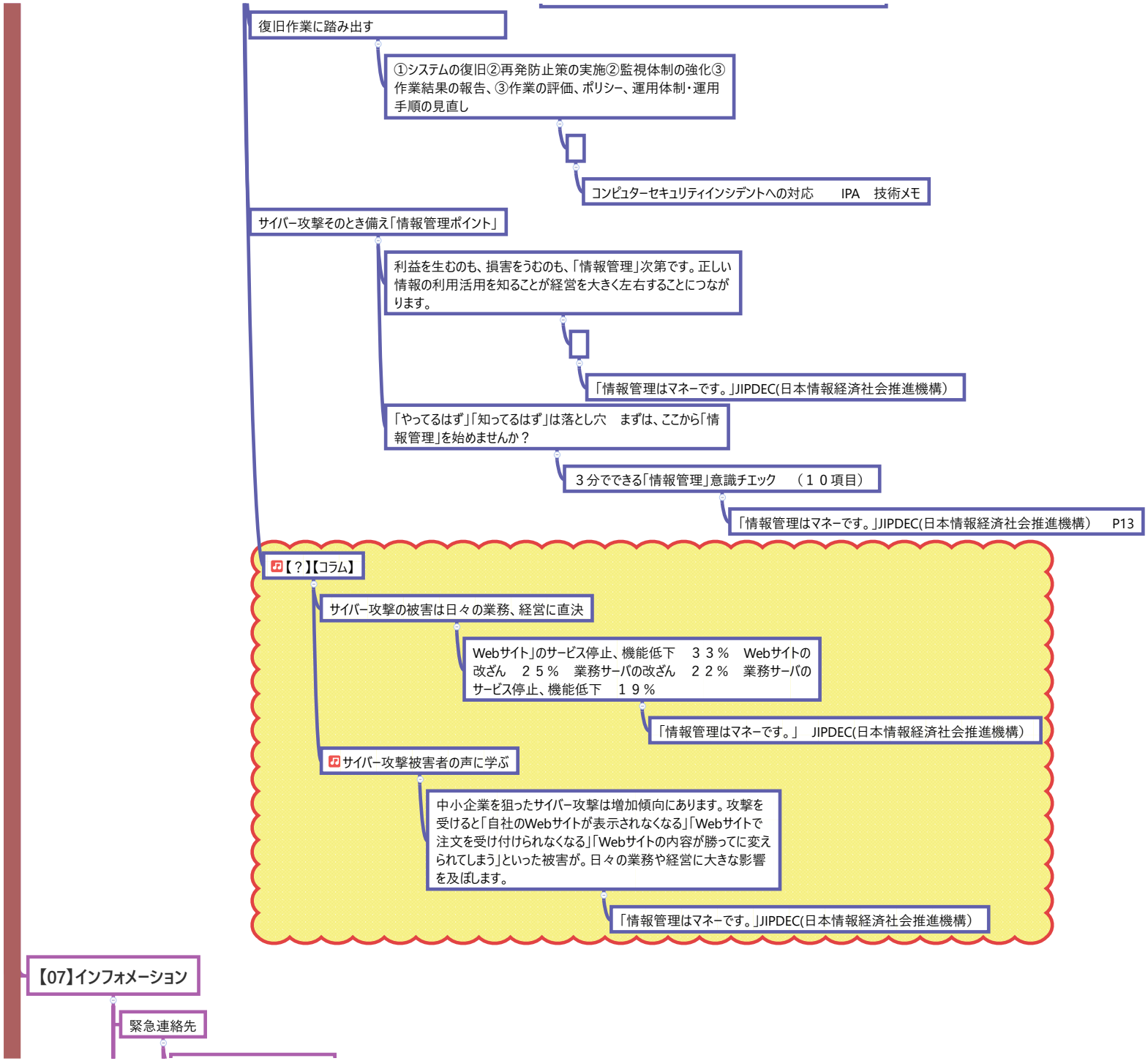

代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。
原状保全
原因調査
早期復旧・事業継続 (Respond)
恒久的対策（再発防止策）
通常運用
4.2改ざん・消失・破壊・サービス停止発生時の対応
①情報資産の意図しない改ざん、消失、破壊、②情報資産が必要なときに利用できない
事象の検知、報告受付(Detect)
手順の確認
作業記録の作成開始
①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。
事実確認、対応の判断 被害の局所化(拡大防止)(Triage)
②システム管理者は原因を特定し、応急処置を実行する。影響範囲の特定、ネットワーク接続やシステムの遮断もしくは停止
緊急連絡
③インシデント対応責任者は社内に周知するとともに総務部情報システム担当に連絡する。
原状保全
各種ログの保全
後日の詳細な調査のために、スナップショットを保存　場合によっては、ストレージ装置全体を
原因調査
⑦システム管理者は原因の特定と応急的な対策を実施する。不明の場合は、外部の専門機関に問い合せる
早期復旧・事業継続 (Respond)
④電子データの場合はシステム管理者がバックアップによる復旧を実行する。
⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。
⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。
恒久的対策（再発防止策）
再発防止策の実施
監視体制の強化

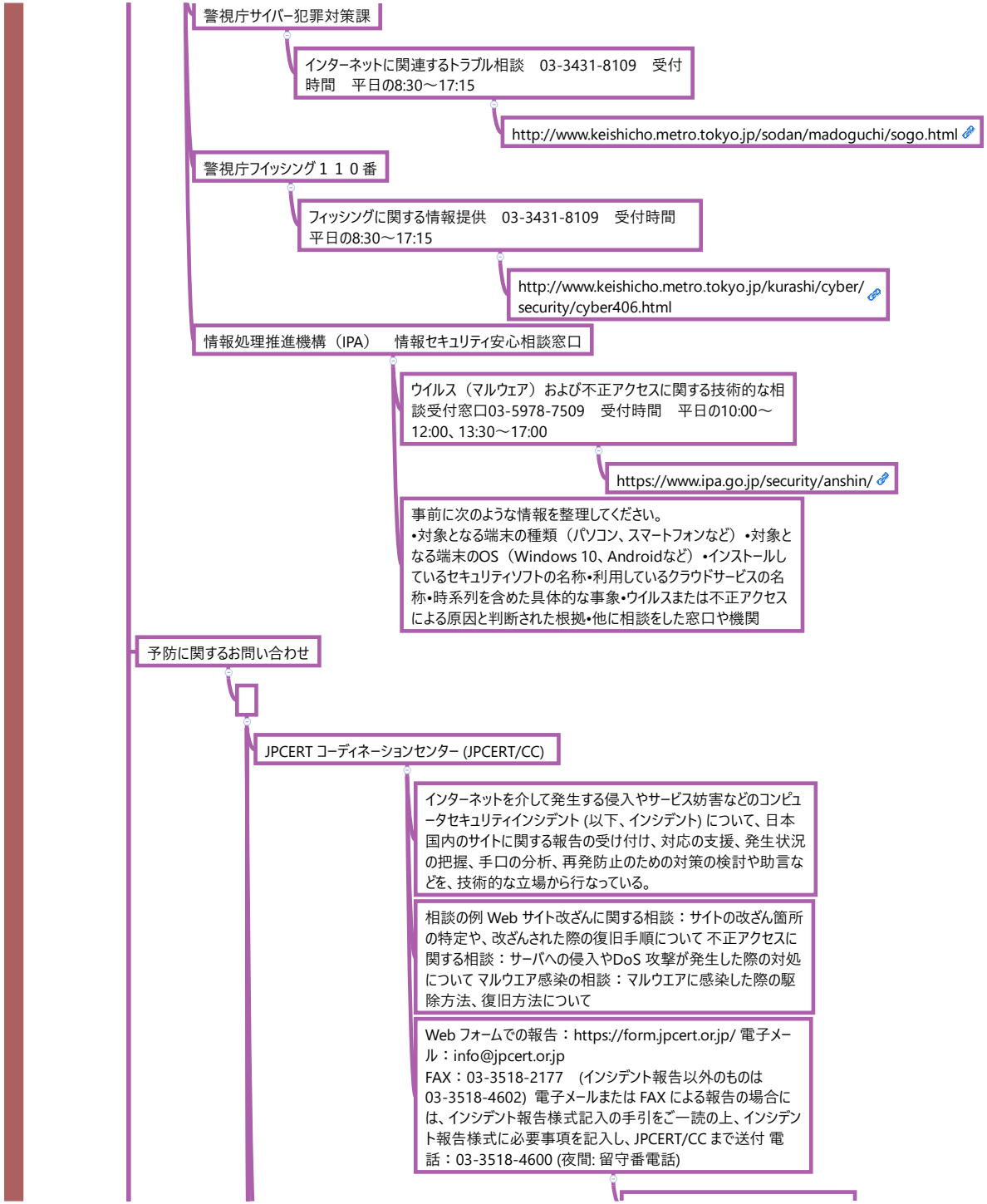

作業結果の報告
作業の評価、ポリシー・運用体制・運用手順の見直し
公表
代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。
通常運用
4.3ウイルス感染時の初期対応
悪意のあるソフトウェアに感染
従業員は、業務に利用しているパソコン、サーバー又はスマートフォン、タブレット（以下「コンピュータ」といいます。）がウイルスに感染した場合には、以下を実行する。
①ネットワークからコンピュータを切断する。
②システム管理者に連絡する。
③ウイルス対策ソフトの定義ファイルを最新版に更新する。
④ウイルス対策ソフトを実行しウイルス名を確認する。
⑤ウイルス対策ソフトで駆除可能な場合は駆除する。
⑥駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認する。
⑦システム管理者に報告する。
以下の場合など従業員自身で対応できないと判断される場合はシステム管理者に問い合わせる。①ウイルス対策ソフトで駆除できない。②システムファイルが破壊・改ざんされている。③ファイルが改ざん・暗号化・削除されている。④⑤．。。
4.5届け出及び相談
＜届け出・相談先＞
システム管理者は、インシデント対応後に以下の機関への届け出又は相談を検討する。
＜届け出・相談先＞独立行政法人 情報処理推進機構セキュリティセンター(IPA/ISEC)
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のための事前準備
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、停電等にによる○○システム停止

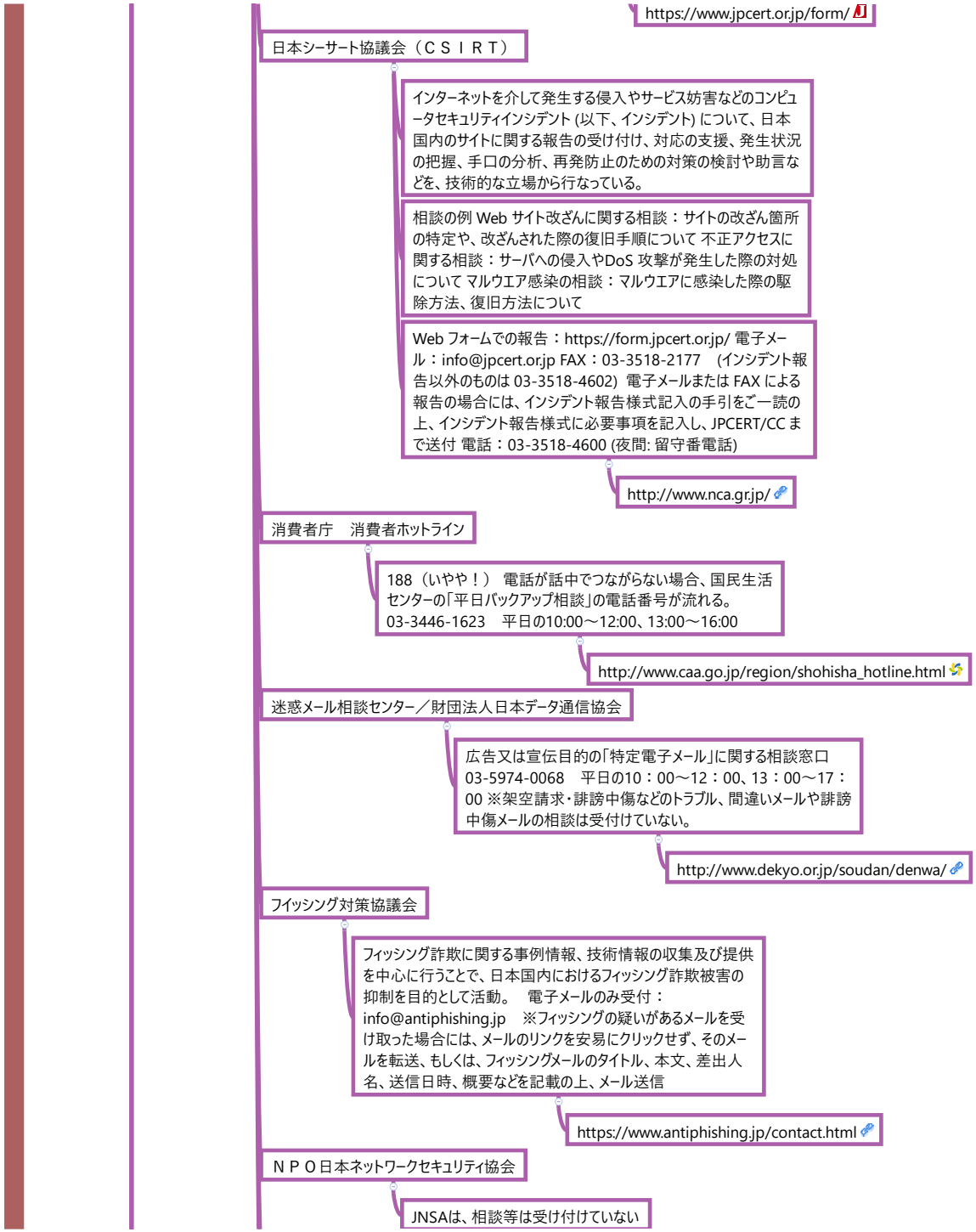

想定理由：当社の事業は、商品の販売から請求回収までの業務を○○システムに依存しているため、停止した場合は事業の継続が困難になり多大な損失が発生
5.2復旧責任者及び関連連絡先
被害対象毎に、復旧責任者、関係者連絡先をリスト化しておく
5.3事業継続計画
インシデント対応責任者は、想定する情報セキュリティインシデントが発生し、事業が中断した際の復旧責任者の役割認識及び関係者連絡先について、有効に機能するか検証する。
復旧責任者は、被害対象に応じて復旧から事業再開までの計画を立案する。
ワークショプ
自社でやろうサイバー攻撃への対応アクション
【01】やってみよう！サイバー攻撃シミュレーション
もしも今、あなたの会社にサイバー攻撃が起きたら、あなたならどうする？
サイバー攻撃発覚の瞬間から被害拡大防止、復旧までのシミュレート。自社自身に置き換えて、今、想像しよう。
サイバー攻撃発生
攻撃準備①計画立案②攻撃準備
攻撃者は、標的の組織に関する情報調査搾取する。
攻撃者は、標的の組織に関する情報について、ｲﾝﾀｰﾈｯﾄや他組織から取得した情報を基に調査する。また、攻撃者は、攻撃の最終目的を設定し、攻撃に必要となる環境等（標的型メール、改ざんされたウェブサイト、C&Cサーバ、ハッキング用のツール等）を準備する。
「高度サイバー攻撃対処のためのリスク評価等のガイドライン付属書　」内閣サーバセキュリティセンター　ｐ１９
サイバー攻撃発生その瞬間　③初期潜入段階
侵入段階　標的型メールの送付し開封によるウイルス感染
標的型メールによるウイルス感染と内部侵入

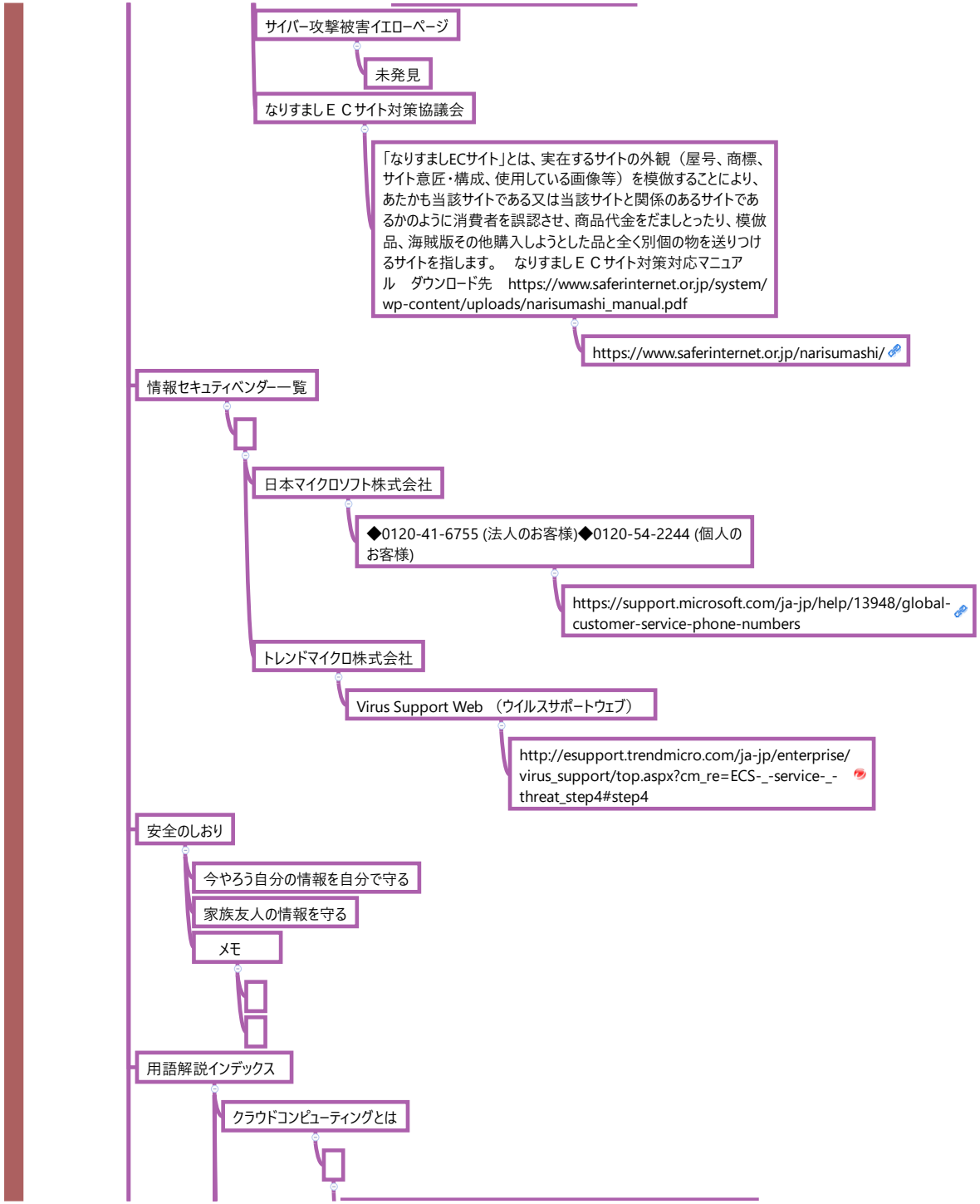

「標的型メール攻撃」対策に向けたシステム設計ガイド」　IPA　2013.8
サイバー攻撃直後
発生直後の行動　④基盤構築段階
内部情報搾取　基盤構築段階
コネクトバック通信の確立及びマルウエアのダウンロード
「標的型メール攻撃」対策に向けたシステム設計ガイド」　IPA　2013.8
侵入拡大　⑤内部侵入・調査　⑥目的遂行
侵入範囲の拡大と機密情報の外部送信
感染端末を起点としたネットワークやホストの情報の収集　ＩＤ／ＰＷを搾取しながら端末やサーバへ侵入拡大、機密情報の搾取や重要システムの破壊・業務妨害
自社に潜む危機
攻撃がどの段階まで到達しているのか？
標的型攻撃は標的とする組織に気ずかれないよう行うものであることから、当該組織がその攻撃や被害そのものを認知していない、または攻撃による被害者であることを認知できていない場合も多く、例えば、被害が発覚した時点で既に数年前から情報が搾取されていたという事案も存在している。
「高度サイバー攻撃対処のためのリスク評価等のガイドライン付属書　」内閣サーバセキュリティセンター　ｐ１９
関連先企業（サプライチエーン）に潜む危機
サプライチエーン全体でのサイバーセキュリティ確保する。一企業での対策では限界がある。
サプライチェーン全体でのサイバーセキュリティの確保　ビジネス基盤（サプライチェーン）に参画してりるビジネスパートナーやシステム委託先などのほんの一部のセキュリティ対策が不十分であった場合でも自社から提供した重要な情報が流出してしまうなどの問題が生じるおそれがある。
「企業経営ためのサーバセキュリティの考え方の施策について」内閣サイバーセキュリティセンター　平成２８年８月２日　ｐ４
サイバー攻撃発生時のＮＧ行動と開示・報告すべき情報とは
サイバー攻撃や標的型攻撃に関する不安ついてセキュリＩテイの専門家へ相談する事項を事前に纏めておく。
「やられたかな？その前に」ガイドISOG－Ｊ20151014
被害発覚後の必要な情報の把握　開示体制の整備

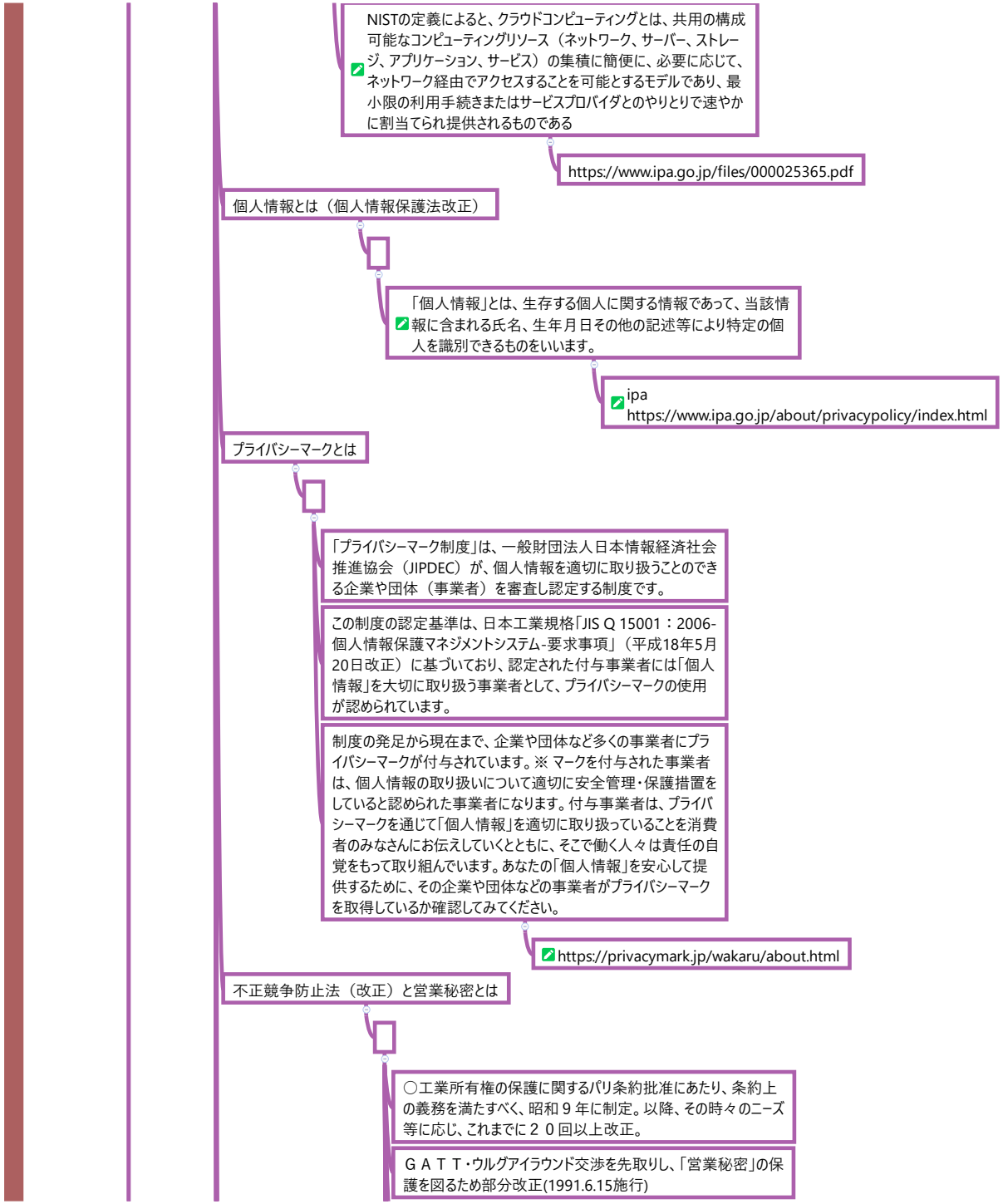

被害発見後の迅速な情報の把握、開示体制の整備
サイバー攻撃の被害が発生した際に円滑な状況把握ができるよう、収集すべき項目や情報を整理し、被害を受けたことを通知すべき相手方のリスト整備、経営者による説明の準備をあらかじめ進めておくことが大切です。①開示・報告すべき情報の把握②通知先のリスト化と通知用のフォーマット作成③通知に必要な情報の整理と周知④組織の内外への開示・報告、タイミング⑤開示・報告先について留意すべき点
被害拡大防止
継続的再侵入　⑦再侵入防止と経路の特定
放置していたセキュリティ上の問題点、脆弱性を再確認し継続的に監視を行う。
侵入された要因を特定し、適切な対策を実施しない限り、再侵入を受ける可能性があり、危険です。
インシデント対応手順JPCERT 技術メモコンピュータセキュリティインシデントへの対応
不正アクセスと再侵入範囲の拡大防止
コンピュ―タセキュリティインシデントの典型的な例としては、侵入、サービス妨害、破壊、データの盗用や、それらの準備段階と推測されるアクセス、そのほか他サイト/システムからの原因不明のアクセスなどが挙げられます。また、サイト外部から、自サイトの関与するインシデントについての情報提供を受ける可能性もあります。
安全防止チエックポイント
サイバー攻撃被害の一形態は多肢に渡ります。自社固有の事情を考慮すること
（a)システムのアクセス権限に対する影響（ｂ）システムの可用性、サイトの業務に対する影響（ｃ）外部への影響（ｄ）顧客のプライバシーや組織の信用に対する影響
コンピュターセキュリティインシデントへの対応　IPA　技術メモ
復旧回復
日常業務への復旧に向けて
①手順の確認、②作業記録の作成、③責任者、担当者への連絡、④事実の確認，⑤スナップショットの保存、⑥ネットワーク接続やシステムの遮断もしくは停止⑦影響範囲の特定⑧要因の特定
コンピュターセキュリティインシデントへの対応　IPA　技術メモ


復旧作業に踏み出す
①システムの復旧②再発防止策の実施②監視体制の強化③作業結果の報告、③作業の評価、ポリシー、運用体制・運用手順の見直し
コンピューターセキュリティインシデントへの対応　IPA　技術メモ
サイバー攻撃そのとき備え「情報管理ポイント」
利益を生むのも、損害をうむのも、「情報管理」次第です。正しい情報の利用活用を知ることが経営を大きく左右することにつながります。
「情報管理はマネーです。」JIPDEC(日本情報経済社会推進機構)
「やってるはず」「知ってるはず」は落とし穴　まずは、ここから「情報管理」を始めませんか？
３分でできる「情報管理」意識チエック　（１０項目）
「情報管理はマネーです。」JIPDEC(日本情報経済社会推進機構)　P13
【？】【コラム】
サイバー攻撃の被害は日々の業務、経営に直決
Webサイト」のサービス停止、機能低下　３３％　Webサイトの改ざん　２５％　業務サーバの改ざん　２２％　業務サーバのサービス停止、機能低下　１９％
「情報管理はマネーです。」　JIPDEC(日本情報経済社会推進機構)
サイバー攻撃被害者の声に学ぶ
中小企業を狙ったサイバー攻撃は増加傾向にあります。攻撃を受けると「自社のWebサイトが表示されなくなる」「Webサイトで注文を受け付けられなくなる」「Webサイトの内容が勝ってに変えられてしまう」といった被害が。日々の業務や経営に大きな影響を及ぼします。
「情報管理はマネーです。」JIPDEC(日本情報経済社会推進機構)
【07】インフォメーション
緊急連絡先


警視庁サイバー犯罪対策課
インターネットに関連するトラブル相談　03-3431-8109　受付時間　平日の8:30～17:15
http://www.keishicho.metro.tokyo.jp/sodan/madoguchi/sogo.html
警視庁フィッシング１１０番
フィッシングに関する情報提供　03-3431-8109　受付時間　平日の8:30～17:15
http://www.keishicho.metro.tokyo.jp/kurashi/cyber/security/cyber406.html
情報処理推進機構（IPA）　情報セキュリティ安心相談窓口
ウイルス（マルウェア）および不正アクセスに関する技術的な相談受付窓口03-5978-7509　受付時間　平日の10:00～12:00、13:30～17:00
https://www.ipa.go.jp/security/anshin/
事前に次のような情報を整理してください。
•対象となる端末の種類（パソコン、スマートフォンなど）•対象となる端末のOS（Windows 10、Androidなど）•インストールしているセキュリティソフトの名称•利用しているクラウドサービスの名称•時系列を含めた具体的な事象•ウイルスまたは不正アクセスによる原因と判断された根拠•他に相談をした窓口や機関
予防に関するお問い合わせ
JPCERT コーディネーションセンター (JPCERT/CC)
インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデント (以下、インシデント) について、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている。
相談の例 Web サイト改ざんに関する相談：サイトの改ざん箇所の特定や、改ざんされた際の復旧手順について 不正アクセスに関する相談：サーバへの侵入やDoS 攻撃が発生した際の対処について マルウエア感染の相談：マルウエアに感染した際の駆除方法、復旧方法について
Web フォームでの報告：https://form.jpcert.or.jp/ 電子メール：info@jpcert.or.jp
FAX：03-3518-2177　(インシデント報告以外のものは 03-3518-4602) 電子メールまたは FAX による報告の場合には、インシデント報告様式記入の手引をご一読の上、インシデント報告様式に必要事項を記入し、JPCERT/CC まで送付 電話：03-3518-4600 (夜間: 留守番電話)


https://www.jpcert.or.jp/form/
日本シーサート協議会（ＣＳＩＲＴ）
インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデント (以下、インシデント) について、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている。
相談の例 Web サイト改ざんに関する相談：サイトの改ざん箇所の特定や、改ざんされた際の復旧手順について 不正アクセスに関する相談：サーバへの侵入やDoS 攻撃が発生した際の対処について マルウエア感染の相談：マルウエアに感染した際の駆除方法、復旧方法について
Web フォームでの報告：https://form.jpcert.or.jp/ 電子メール：info@jpcert.or.jp FAX：03-3518-2177　(インシデント報告以外のものは 03-3518-4602) 電子メールまたは FAX による報告の場合には、インシデント報告様式記入の手引をご一読の上、インシデント報告様式に必要事項を記入し、JPCERT/CC まで送付 電話：03-3518-4600 (夜間: 留守番電話)
http://www.nca.gr.jp/
消費者庁　消費者ホットライン
188（いやや！） 電話が話中でつながらない場合、国民生活センターの「平日バックアップ相談」の電話番号が流れる。
03-3446-1623　平日の10:00～12:00、13:00～16:00
http://www.caa.go.jp/region/shohisha_hotline.html
迷惑メール相談センター／財団法人日本データ通信協会
広告又は宣伝目的の「特定電子メール」に関する相談窓口
03-5974-0068　平日の10：00～12：00、13：00～17：00 ※架空請求・誹謗中傷などのトラブル、間違いメールや誹謗中傷メールの相談は受付けていない。
http://www.dekyo.or.jp/soudan/denwa/
フィッシング対策協議会
フィッシング詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の抑制を目的として活動。　電子メールのみ受付：info@antiphishing.jp　※フィッシングの疑いがあるメールを受け取った場合には、メールのリンクを安易にクリックせず、そのメールを転送、もしくは、フィッシングメールのタイトル、本文、差出人名、送信日時、概要などを記載の上、メール送信
https://www.antiphishing.jp/contact.html
ＮＰＯ日本ネットワークセキュリティ協会
JNSAは、相談等は受け付けていない


サイバー攻撃被害イエローページ
未発見
なりすましＥＣサイト対策協議会
「なりすましECサイト」とは、実在するサイトの外観（屋号、商標、サイト意匠・構成、使用している画像等）を模倣することにより、あたかも当該サイトである又は当該サイトと関係のあるサイトであるかのように消費者を誤認させ、商品代金をだましとったり、模倣品、海賊版その他購入しようとした品と全く別個の物を送りつけるサイトを指します。　なりすましＥＣサイト対策対応マニュアル　ダウンロード先　https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf
https://www.saferinternet.or.jp/narisumashi/
情報セキュティベンダー一覧
日本マイクロソフト株式会社
◆0120-41-6755 (法人のお客様)◆0120-54-2244 (個人のお客様)
https://support.microsoft.com/ja-jp/help/13948/global-customer-service-phone-numbers
トレンドマイクロ株式会社
Virus Support Web （ウイルスサポートウェブ）
http://esupport.trendmicro.com/ja-jp/enterprise/virus_support/top.aspx?cm_re=ECS-_-service-_-threat_step4#step4
安全のしおり
今やろう自分の情報を自分で守る
家族友人の情報を守る
メモ
用語解説インデックス
クラウドコンピューティングとは


NISTの定義によると、クラウドコンピューティングとは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるものである
https://www.ipa.go.jp/files/000025365.pdf
個人情報とは（個人情報保護法改正）
「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるものをいいます。
ipa
https://www.ipa.go.jp/about/privacypolicy/index.html
プライバシーマークとは
「プライバシーマーク制度」は、一般財団法人日本情報経済社会推進協会（JIPDEC）が、個人情報を適切に取り扱うことのできる企業や団体（事業者）を審査し認定する制度です。
この制度の認定基準は、日本工業規格「JIS Q 15001：2006-個人情報保護マネジメントシステム-要求事項」（平成18年5月20日改正）に基づいており、認定された付与事業者には「個人情報」を大切に取り扱う事業者として、プライバシーマークの使用が認められています。
制度の発足から現在まで、企業や団体など多くの事業者にプライバシーマークが付与されています。※ マークを付与された事業者は、個人情報の取り扱いについて適切に安全管理・保護措置をしていると認められた事業者になります。付与事業者は、プライバシーマークを通じて「個人情報」を適切に取り扱っていることを消費者のみなさんにお伝えしていくとともに、そこで働く人々は責任の自覚をもって取り組んでいます。あなたの「個人情報」を安心して提供するために、その企業や団体などの事業者がプライバシーマークを取得しているか確認してみてください。
https://privacymark.jp/wakaru/about.html
不正競争防止法（改正）と営業秘密とは
○工業所有権の保護に関するパリ条約批准にあたり、条約上の義務を満たすべく、昭和９年に制定。以降、その時々のニーズ等に応じ、これまでに２０回以上改正。
ＧＡＴＴ・ウルグアイラウンド交渉を先取りし、「営業秘密」の保護を図るため部分改正(1991.6.15施行)

全面改正（①ひらがな化、②法目的の明記、③不正競争行為の類型拡充（著名表示冒用行為・商品形態模倣行為）、④損害賠償額の推定規定の新設、⑤法人重課規定の創設等）（1994.5.1施行）

「知的財産戦略大綱」(2002年7月)における指摘事項の実施のため部分改正（①営業秘密の刑事的保護の導入 ②民事的救済措置の強化、③ネットワーク化への対応）(2004.1.1施行)

営業秘密の保護強化、模倣品・海賊版対策の強化、罰則の強化、条番号の整序のため部分改正(2005.11.1施行)

→周知表示の混同惹起行為となる商品等の税関での輸入差止制度の導入（関税定率法の一部改正）

営業秘密、秘密保持命令違反罪に係る刑事罰の強化、商品形態模倣行為の刑事罰の強化（2007.1.1施行）

→不競法違反物品の税関での輸出差止制度の導入（関税法の一部改正）（2007.1.1施行）

営業秘密侵害罪に係る刑事罰の強化のため部分改正（①営業秘密を不当に保有し続ける行為（領得行為）についても処罰対象に追加、②目的要件の拡大（不正の競争の目的→図利・加害の目的に変更） など）（2010.7.1施行）

①営業秘密の内容を保護するための刑事訴訟手続の整備（秘匿決定、呼称等の決定、公判期日外での証人尋問等）、②技術的制限手段に係る規律の強化（規制対象装置の範囲の拡大、刑事罰の導入）のため部分改正（2011.12.1施行）

経済産業省
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/27kaiseigaiyou.pdf

外部委託契約とＳＬＡ（サービスレベルアグリーメント）

外部委託契約とＳＬＡ　◆ＳＬＡ、という用語の定義はどのようなものか。【解説】ＳＬＡという用語は、ISO/IEC20000-1:2005においては次のように定義されています。サービス及び合意されたサービスレベルを文書化した、サービスプロバイダと顧客間の書面による合意。ただしこれではわかりにくいと思います。そこで、「情報システムに係る政府調達へのＳＬＡ導入ガイドライン」でのＳＬＡの定義を参考にしてみます。ＩＴサービスの提供者と委託者との間で、ＩＴサービスの契約を締結する際に、提供するサービスの範囲・内容及び前提となる諸事項を踏まえた上で、サービスの品質に対する要求水準を規定するとともに、規定した内容が適正に実現されるための運営ルールを両者の合意として明文化したもの。どちらについても、共通していえることは、・委託元と委託先との合意が必要・文書化（明文化）が必要といったことです。なお、後者ではガイドラインの性質上、「ＩＴサービス」という用語を用いていますが、「ＩＴ」の文字を取り外して考えると、ＳＬＡの用語の定義が非常に見えやすくなるかと思います。【参考文献】（１）情報システムに係る政府調達へのＳＬＡガイドライン（独立行政法人情報処理推進機構、平成16年）参照：http://www.meti.go.jp/kohosys/press/

0005140/1/040414it2.pdf

総務省
http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/local_support/pdf/cio_text18_t_18.pdf

マイナンバーのセキュリティ考慮事項

平成28年1月から、マイナンバーカードの交付が開始されます。　マイナンバーカードは、本人の申請により交付され、個人番号を証明する書類や本人確認の際の公的な身分証明書として利用でき、また、様々な行政サービスを受けることができるようになるICカードです。交付手数料は、当面の間無料です（本人の責による再発行の場合を除く）。表面には　?氏名　?住所　?生年月日　?性別　?顔写真　?電子証明書の有効期限の記載欄　?セキュリティコード　?サインパネル領域（券面の情報に修正が生じた場合、その新しい情報を記載（引越した際の新住所など））　?臓器提供意思表示欄　が記載され、個人番号は裏面に記載されます。　マイナンバーカードは、金融機関等本人確認の必要な窓口で身分証明書として利用できますが（※）、個人番号をコピー・保管できる事業者は、行政機関や雇用主等、法令に規定された者に限定されているため、規定されていない事業者の窓口において、個人番号が記載されているカードの裏面をコピー・保管することはできません。　※マイナンバーカードを身分証明書として取り扱うかどうかは、最終的には各事業者側の判断となりますので、一部の事業者では利用できない場合があります。

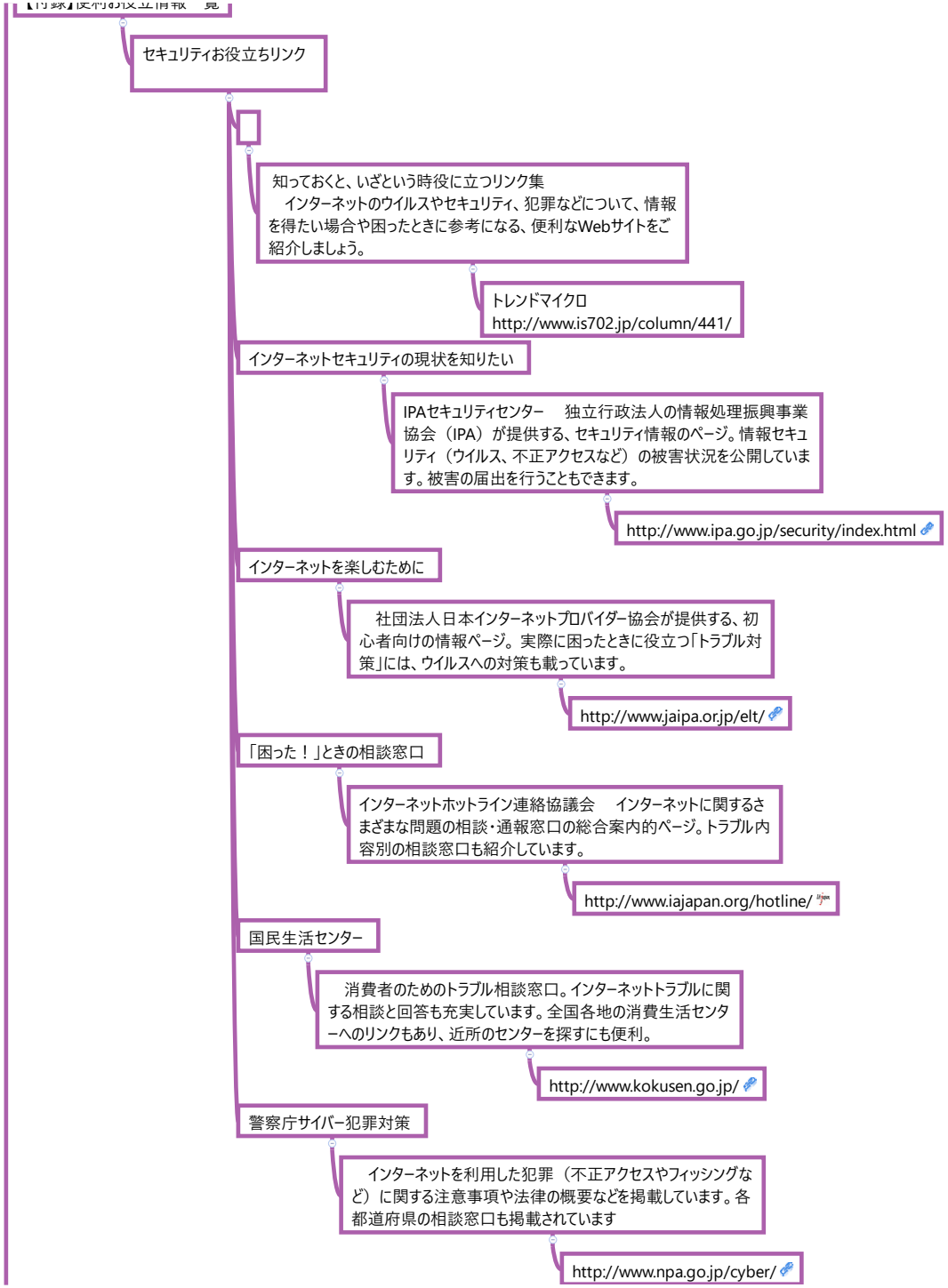
総務省　http://www.soumu.go.jp/kojinbango_card/03.html#security

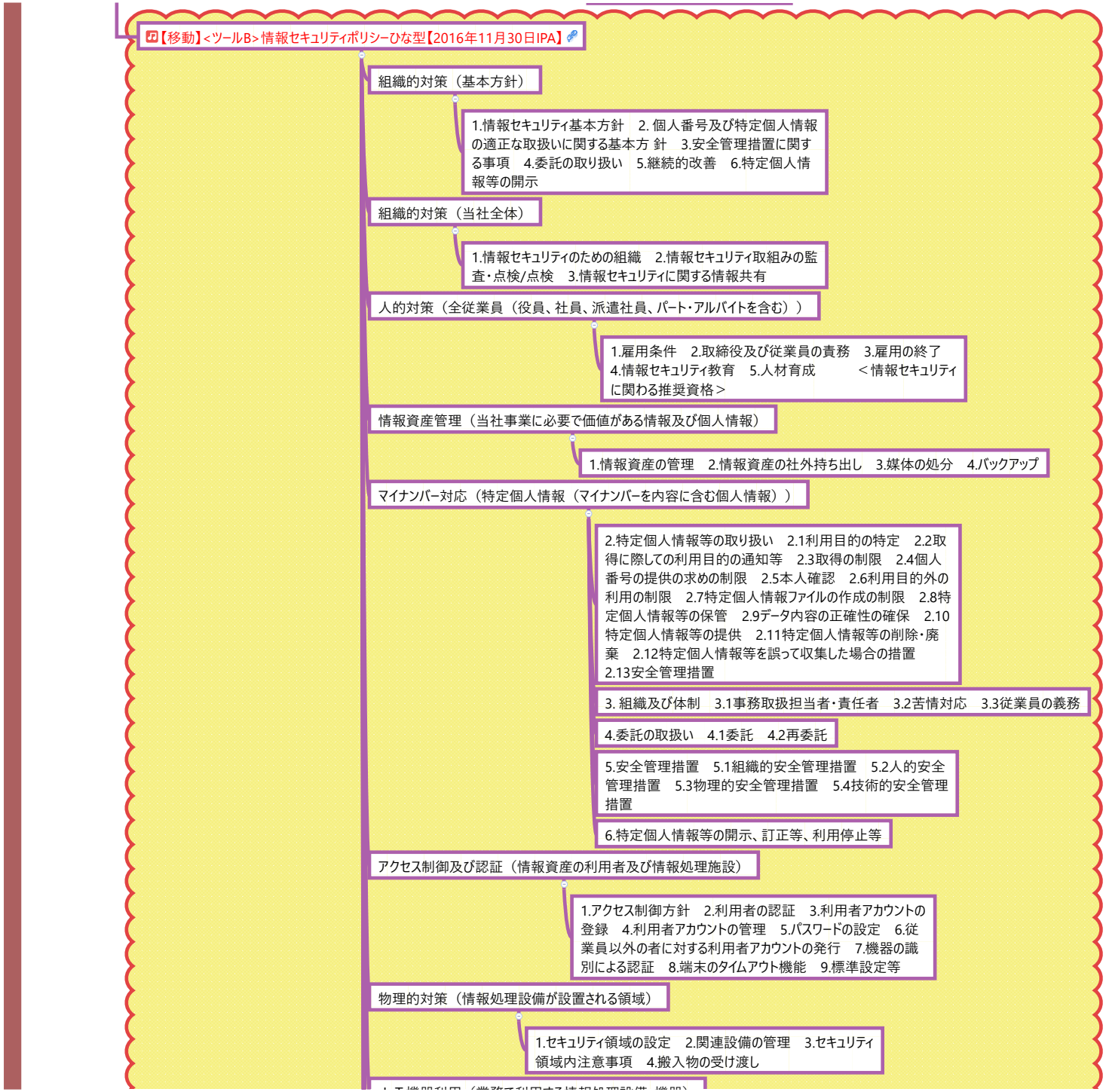
物理（環境的）セキュリティとは

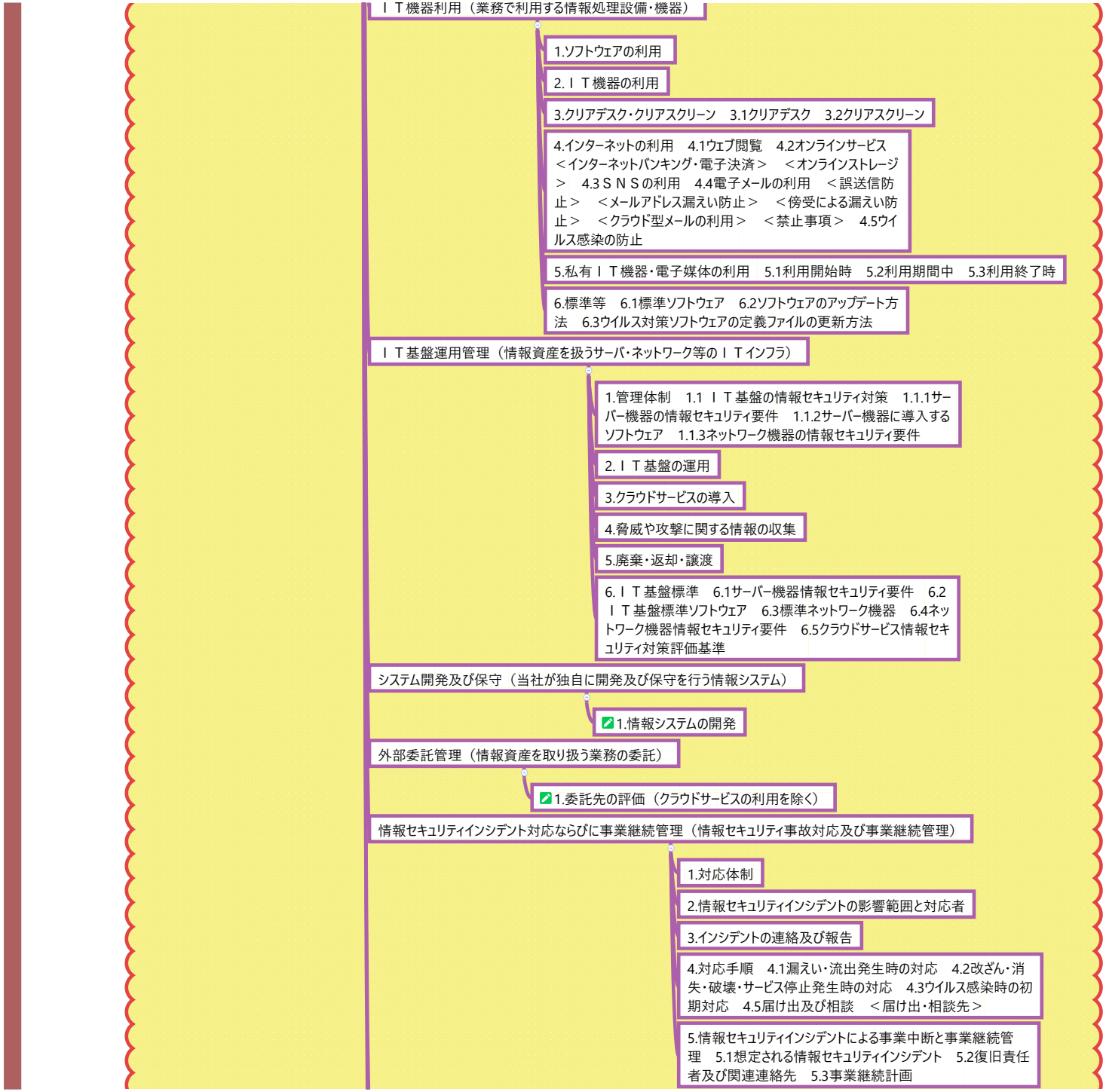
物理的セキュリティ対策の強化　企業では社員の他にさまざまな訪問客に加え、派遣社員、アルバイト、パートなど、多様な勤務形態の従業員がオフィスを出入りします。オフィスへの入退管理を強化して、正当な用件のない部外者を社内へ不正に侵入させないようにしましょう。　オフィスの施錠管理を行う　入退室の履歴を記録に残す（台帳記入など）　身分証を発行し、従業員に携帯させる　出入りが激しい場所については、不審者がいないかどうかを常に留意する　また、可能ならば、以下のような対策を実施すると、より効果的です。　セキュリティカードなどで出入り口の制限を行う　出入り口に守衛を配置したり、監視カメラを設置したりする　バイオメトリクス（生体認証）など、より強固なシステムを導入する

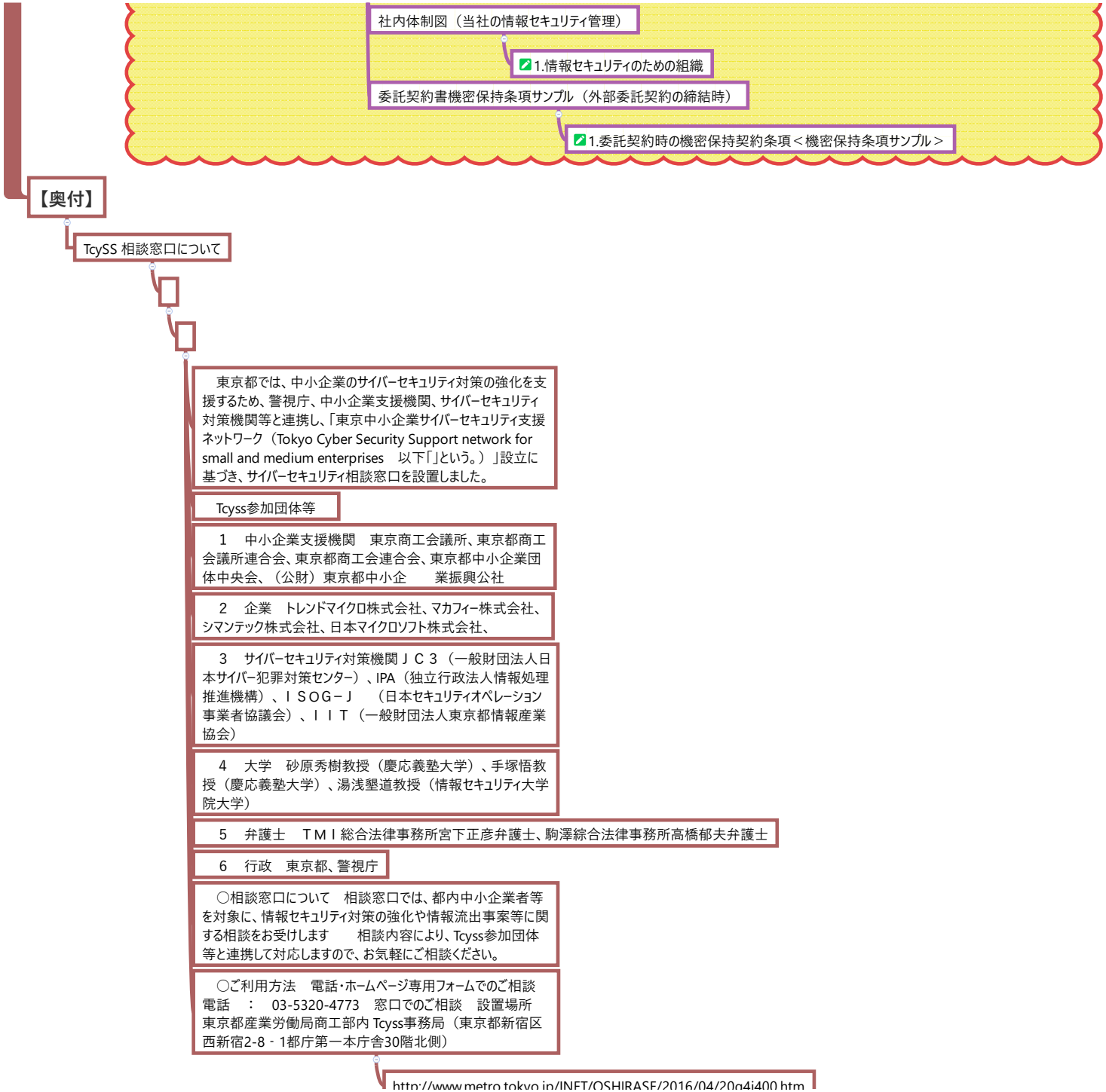
経済産業省
http://www.jnsa.org/ikusei/engineering/09_03.html

【付録】便利お役立情報一覧


【付録】便利お役立情報一覧
セキュリティお役立ちリンク
知っておくと、いざという時役に立つリンク集
インターネットのウイルスやセキュリティ、犯罪などについて、情報を得たい場合や困ったときに参考になる、便利なWebサイトをご紹介しましょう。
トレンドマイクロ
http://www.is702.jp/column/441/
インターネットセキュリティの現状を知りたい
IPAセキュリティセンター　独立行政法人の情報処理振興事業協会（IPA）が提供する、セキュリティ情報のページ。情報セキュリティ（ウイルス、不正アクセスなど）の被害状況を公開しています。被害の届出を行うこともできます。
http://www.ipa.go.jp/security/index.html
インターネットを楽しむために
社団法人日本インターネットプロバイダー協会が提供する、初心者向けの情報ページ。実際に困ったときに役立つ「トラブル対策」には、ウイルスへの対策も載っています。
http://www.jaipa.or.jp/elt/
「困った！」ときの相談窓口
インターネットホットライン連絡協議会　インターネットに関するさまざまな問題の相談・通報窓口の総合案内的ページ。トラブル内容別の相談窓口も紹介しています。
http://www.iajapan.org/hotline/
国民生活センター
消費者のためのトラブル相談窓口。インターネットトラブルに関する相談と回答も充実しています。全国各地の消費生活センターへのリンクもあり、近所のセンターを探すにも便利。
http://www.kokusen.go.jp/
警察庁サイバー犯罪対策
インターネットを利用した犯罪（不正アクセスやフィッシングなど）に関する注意事項や法律の概要などを掲載しています。各都道府県の相談窓口も掲載されています
http://www.npa.go.jp/cyber/


【移動】<ツールB>情報セキュリティポリシーひな型【2016年11月30日IPA】
組織的対策（基本方針）
1.情報セキュリティ基本方針　2. 個人番号及び特定個人情報の適正な取扱いに関する基本方 針　3.安全管理措置に関する事項　4.委託の取り扱い　5.継続的改善　6.特定個人情報等の開示
組織的対策（当社全体）
1.情報セキュリティのための組織　2.情報セキュリティ取組みの監査・点検/点検　3.情報セキュリティに関する情報共有
人的対策（全従業員（役員、社員、派遣社員、パート・アルバイトを含む））
1.雇用条件　2.取締役及び従業員の責務　3.雇用の終了
4.情報セキュリティ教育　5.人材育成　＜情報セキュリティに関わる推奨資格＞
情報資産管理（当社事業に必要で価値がある情報及び個人情報）
1.情報資産の管理　2.情報資産の社外持ち出し　3.媒体の処分　4.バックアップ
マイナンバー対応（特定個人情報（マイナンバーを内容に含む個人情報））
2.特定個人情報等の取り扱い　2.1利用目的の特定　2.2取得に際しての利用目的の通知等　2.3取得の制限　2.4個人番号の提供の求めの制限　2.5本人確認　2.6利用目的外の利用の制限　2.7特定個人情報ファイルの作成の制限　2.8特定個人情報等の保管　2.9データ内容の正確性の確保　2.10特定個人情報等の提供　2.11特定個人情報等の削除・廃棄　2.12特定個人情報等を誤って収集した場合の措置
2.13安全管理措置
3. 組織及び体制　3.1事務取扱担当者・責任者　3.2苦情対応　3.3従業員の義務
4.委託の取扱い　4.1委託　4.2再委託
5.安全管理措置　5.1組織的安全管理措置　5.2人的安全管理措置　5.3物理的安全管理措置　5.4技術的安全管理措置
6.特定個人情報等の開示、訂正等、利用停止等
アクセス制御及び認証（情報資産の利用者及び情報処理施設）
1.アクセス制御方針　2.利用者の認証　3.利用者アカウントの登録　4.利用者アカウントの管理　5.パスワードの設定　6.従業員以外の者に対する利用者アカウントの発行　7.機器の識別による認証　8.端末のタイムアウト機能　9.標準設定等
物理的対策（情報処理設備が設置される領域）
1.セキュリティ領域の設定　2.関連設備の管理　3.セキュリティ領域内注意事項　4.搬入物の受け渡し


ＩＴ機器利用（業務で利用する情報処理設備・機器）
1.ソフトウェアの利用
2.ＩＴ機器の利用
3.クリアデスク・クリアスクリーン　3.1クリアデスク　3.2クリアスクリーン
4.インターネットの利用　4.1ウェブ閲覧　4.2オンラインサービス＜インターネットバンキング・電子決済＞　＜オンラインストレージ＞　4.3ＳＮＳの利用　4.4電子メールの利用　＜誤送信防止＞　＜メールアドレス漏えい防止＞　＜傍受による漏えい防止＞　＜クラウド型メールの利用＞　＜禁止事項＞　4.5ウイルス感染の防止
5.私有ＩＴ機器・電子媒体の利用　5.1利用開始時　5.2利用期間中　5.3利用終了時
6.標準等　6.1標準ソフトウェア　6.2ソフトウェアのアップデート方法　6.3ウイルス対策ソフトウェアの定義ファイルの更新方法
ＩＴ基盤運用管理（情報資産を扱うサーバ・ネットワーク等のＩＴインフラ）
1.管理体制　1.1 ＩＴ基盤の情報セキュリティ対策　1.1.1サーバー機器の情報セキュリティ要件　1.1.2サーバー機器に導入するソフトウェア　1.1.3ネットワーク機器の情報セキュリティ要件
2.ＩＴ基盤の運用
3.クラウドサービスの導入
4.脅威や攻撃に関する情報の収集
5.廃棄・返却・譲渡
6.ＩＴ基盤標準　6.1サーバー機器情報セキュリティ要件　6.2ＩＴ基盤標準ソフトウェア　6.3標準ネットワーク機器　6.4ネットワーク機器情報セキュリティ要件　6.5クラウドサービス情報セキュリティ対策評価基準
システム開発及び保守（当社が独自に開発及び保守を行う情報システム）
1.情報システムの開発
外部委託管理（情報資産を取り扱う業務の委託）
1.委託先の評価（クラウドサービスの利用を除く）
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（情報セキュリティ事故対応及び事業継続管理）
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届け出及び相談　＜届け出・相談先＞
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


社内体制図（当社の情報セキュリティ管理）
1.情報セキュリティのための組織
委託契約書機密保持条項サンプル（外部委託契約の締結時）
1.委託契約時の機密保持契約条項＜機密保持条項サンプル＞
【奥付】
TcySS 相談窓口について
東京都では、中小企業のサイバーセキュリティ対策の強化を支援するため、警視庁、中小企業支援機関、サイバーセキュリティ対策機関等と連携し、「東京中小企業サイバーセキュリティ支援ネットワーク（Tokyo Cyber Security Support network for small and medium enterprises　以下「」という。）」設立に基づき、サイバーセキュリティ相談窓口を設置しました。
Tcyss参加団体等
1　中小企業支援機関　東京商工会議所、東京都商工会議所連合会、東京都商工会連合会、東京都中小企業団体中央会、（公財）東京都中小企　　業振興公社
2　企業　トレンドマイクロ株式会社、マカフィー株式会社、シマンテック株式会社、日本マイクロソフト株式会社、
3　サイバーセキュリティ対策機関ＪＣ３（一般財団法人日本サイバー犯罪対策センター）、IPA（独立行政法人情報処理推進機構）、ＩＳＯＧ－Ｊ　（日本セキュリティオペレーション事業者協議会）、ＩＩＴ（一般財団法人東京都情報産業協会）
4　大学　砂原秀樹教授（慶応義塾大学）、手塚悟教授（慶応義塾大学）、湯浅墾道教授（情報セキュリティ大学院大学）
5　弁護士　ＴＭＩ総合法律事務所宮下正彦弁護士、駒澤綜合法律事務所高橋郁夫弁護士
6　行政　東京都、警視庁
○相談窓口について　相談窓口では、都内中小企業者等を対象に、情報セキュリティ対策の強化や情報流出事案等に関する相談をお受けします　　相談内容により、Tcyss参加団体等と連携して対応しますので、お気軽にご相談ください。
○ご利用方法　電話・ホームページ専用フォームでのご相談
電話　：　03-5320-4773　窓口でのご相談　設置場所
東京都産業労働局商工部内 Tcyss事務局（東京都新宿区西新宿2-8 - 1都庁第一本庁舎30階北側）
http://www.metro.tokyo.jp/INET/OSHIRASE/2016/04/20g4i400.htm