資料１

「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」改定のポイントについて（案）

総務省

2021年10月22日

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の改定等に係る検討会

「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」の改定の方向性について

令和２年度改定

■自治体の効率性・利便性の向上とセキュリティ確保の両立の観点からガイドラインを改定

「三層の対策」の一部見直し（マイナンバー利用事務系の特定通信、LGWAN接続系とインターネット接続系の分割の見直し）、LGWAN接続系へのリモートアクセス等について改定を実施

令和３年７月の政府統一基準群改定のポイント

1. クラウドサービスの利用拡大を見据えた記載の充実
2. 情報セキュリティ対策の動向を踏まえた記載の充実
3. 多様な働き方を前提とした情報セキュリティ対策の整理

令和３年度改定の方向性

■令和２年度の改定内容を維持しつつ、政府統一基準群の改定内容や最新の動向を踏まえた情報セキュリティ対策を追加

※「自治体の三層の対策 」の抜本的見直しを含めた新たなセキュリティ対策の在り方については、デジタル庁における検討と連携し、随時検討を行う

「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」の主な改定内容及び改定のポイントについて

主な改定内容	改定のポイント
Ⅰ.業務委託・外部サービス利用時の情報資産の取扱い	①外部サービスを再定義した上で取り扱う情報に応じた適切なセキュリティ対策の実施 ⇒政府統一基準群と同様に、外部サービスを再定義し、取り扱う情報に応じた適切なセキュリティ対策を記載 ②外部サービス利用時のライフサイクルに渡るセキュリティ要件の追加 ⇒政府統一基準群と同様に、外部サービス利用時のライフサイクルに渡るセキュリティ要件の追加や外部サービスの利用承認に関する規定を記載 ③クラウドサービス選定の指標・基準等 ⇒ISMAPやISO/IEC27017等の第三者認証の積極的な活用を推奨
2.情報セキュリティ対策の動向を踏まえた記載の充実	未知の不正プログラム対策製品やソフトウェア等を導入するだけでは十分ではなく、監視体制やCSIRTとの連携が必要なことを留意点として記載
3.多様な働き方を前提とした情報セキュリティ対策	①テレワーク実施時のセキュリティ対策 ⇒テレワークに係る運用面に関する対策を記載 ②支給以外の端末（BYOD）利用時のセキュリティ対策 ⇒端末に情報を保存できないようにするための機能を設ける等の対策を記載 ③Web会議サービス利用時のセキュリティ対策 ⇒Web会議に無関係の者が参加できないようにする対策等を記載
4.マイナンバー利用事務系から外部接続先（eLTAX、ぴったりサービス）へのデータのアップロード	マイナンバー利用事務系からのデータのアップロードについて、リスク分析の結果を踏まえ、認めるかの判断を行う。

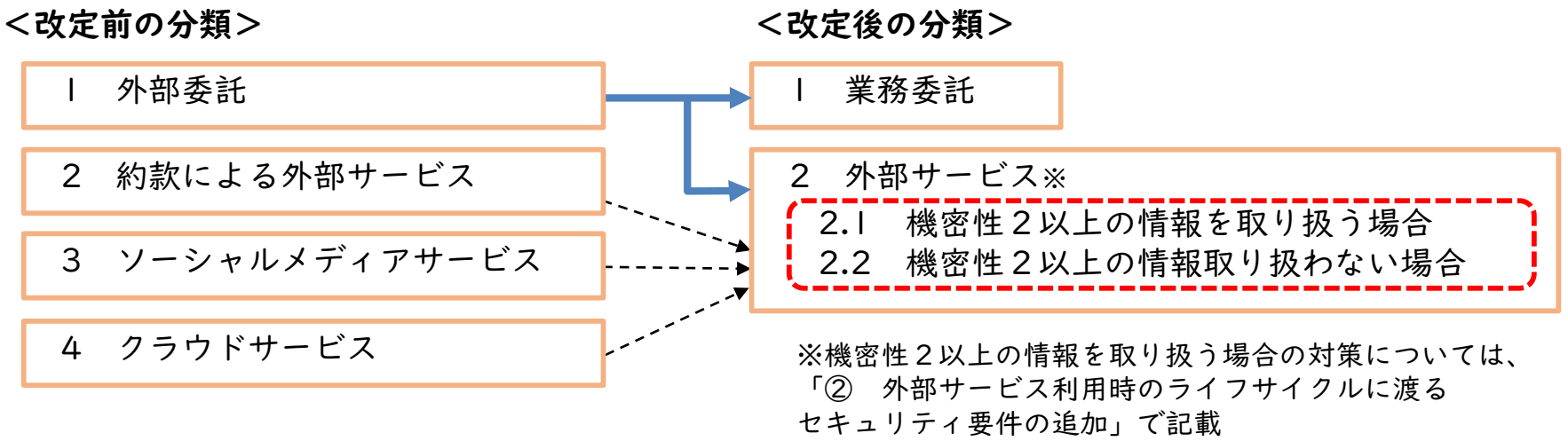
改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（１/４）

①　外部サービスを再定義した上で取り扱う情報に応じた適切なセキュリティ対策の実施

改定の概要

➢　「外部委託」、「約款による外部サービス」、「ソーシャルメディアサービス」及び「クラウドサービス」の定義の境目が曖昧となっているため、政府統一基準群と同様に「業務委託」と「外部サービス」に分けた上で、「機密性２以上の情報を取り扱う場合」と「機密性２以上の情報を取り扱わない場合」により求めるセキュリティ対策のレベルの整理を行う。

※民間事業者等が不特定多数の利用者に対して提供するSNS等の画一的な約款や規約等への同意のみで利用可能となる外部サービス（従来の「約款による外部サービス」）については、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として機密性２以上の情報を取り扱うことはできない点は、従前より変更なし。



【参考】業務委託及び外部サービスの分類

政府統一基準群における業務委託及び外部サービスの分類

	用語の定義		具体例
業務委託	機関等の業務の一部又は全部について、契約をもって外部の者に実施させる		➢ 情報システムの開発、構築及び運用業務 ➢ アプリケーション・コンテンツの開発業務 ➢ 業務運用支援業務（統計、集計、データ入力、媒体変換等） ➢ プロジェクト管理支援業務 ➢ 調査・研究業務（調査、研究、検査等）
外部サービス	機関等外の者が一般向けに情報システムの一部又は全部の機能を提供する	要機密情報を取り扱う場合	➢ クラウドサービス ➢ Ｗｅｂ会議サービス ➢ ＳＮＳ（ソーシャルネットワーキングサービス） ➢ 検索サービス、翻訳サービス、地図サービス ➢ ホスティングサービス
		要機密情報を取り扱わない場合	

政府統一基準群における「クラウドサービス」の定義
事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの

改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（２/４）

②　外部サービス利用時のライフサイクルに渡るセキュリティ要件の追加

改定の概要

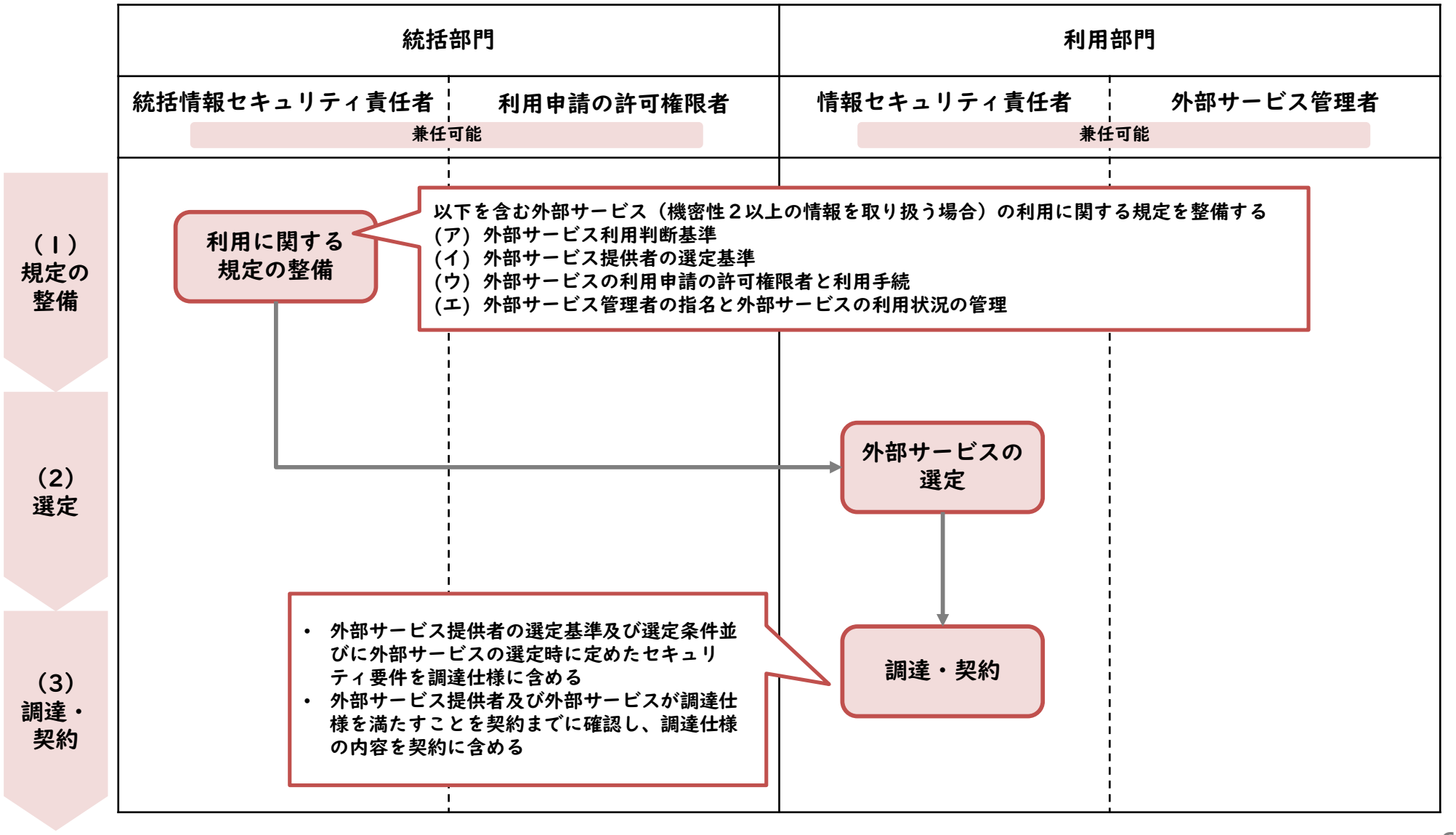
➢ 外部サービス利用時のライフサイクルに渡るセキュリティ要件の追加

機密性２以上の情報を取り扱う外部サービスを利用する際のセキュリティ対策について、政府統一基準群と同様に選定・契約・導入・構築・運用・保守・更改・廃棄等の各フェーズの規定をISO/IEC27017:2015を参考に追記する。

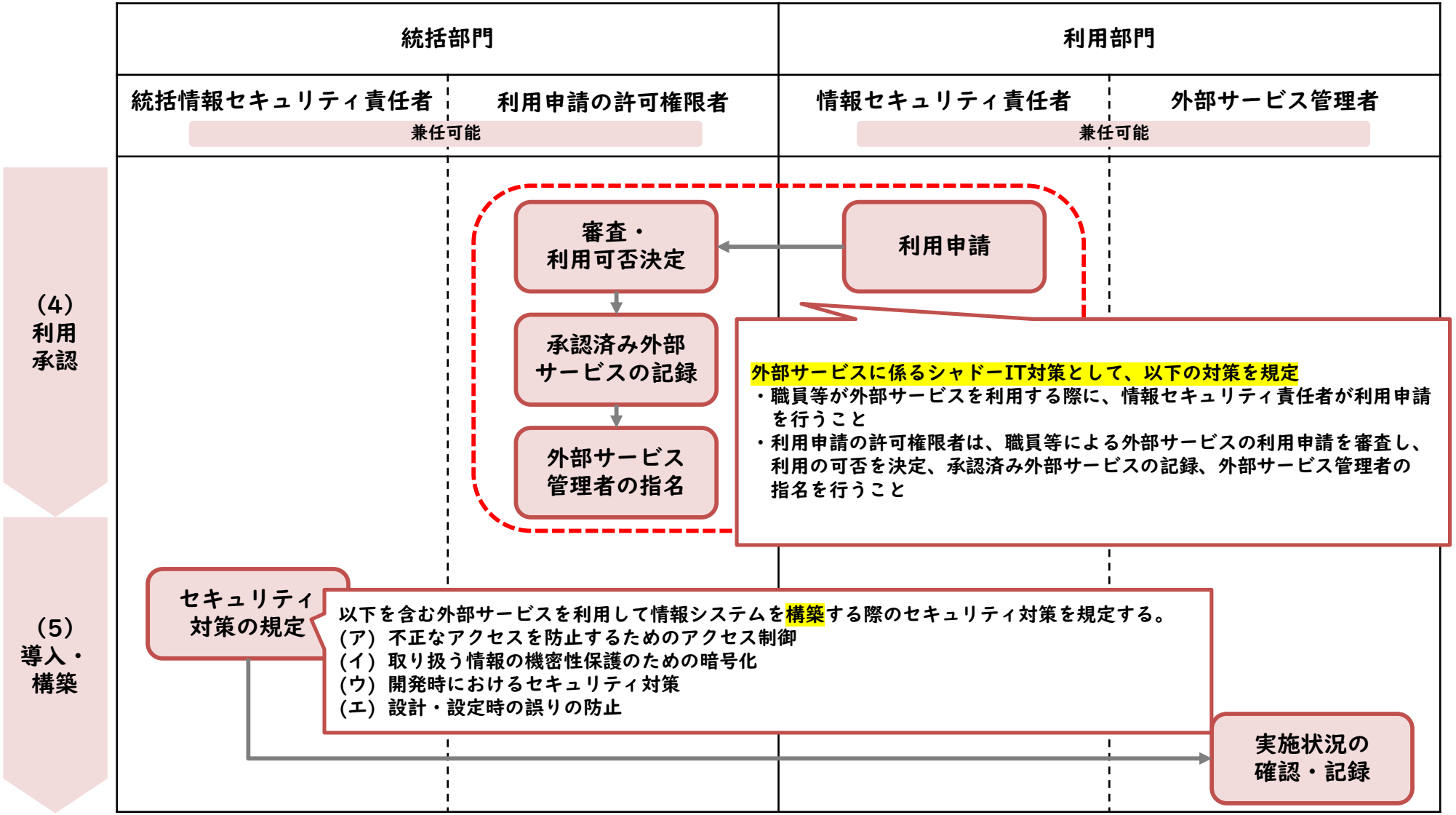
➢ 外部サービスに係るシャドーIT対策

組織の承認を得ずに職員等が外部サービスを利用するシャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。シャドーIT対策として、外部サービス利用時の組織内での申請・審査・承認の手続の規定を整備するよう求める。

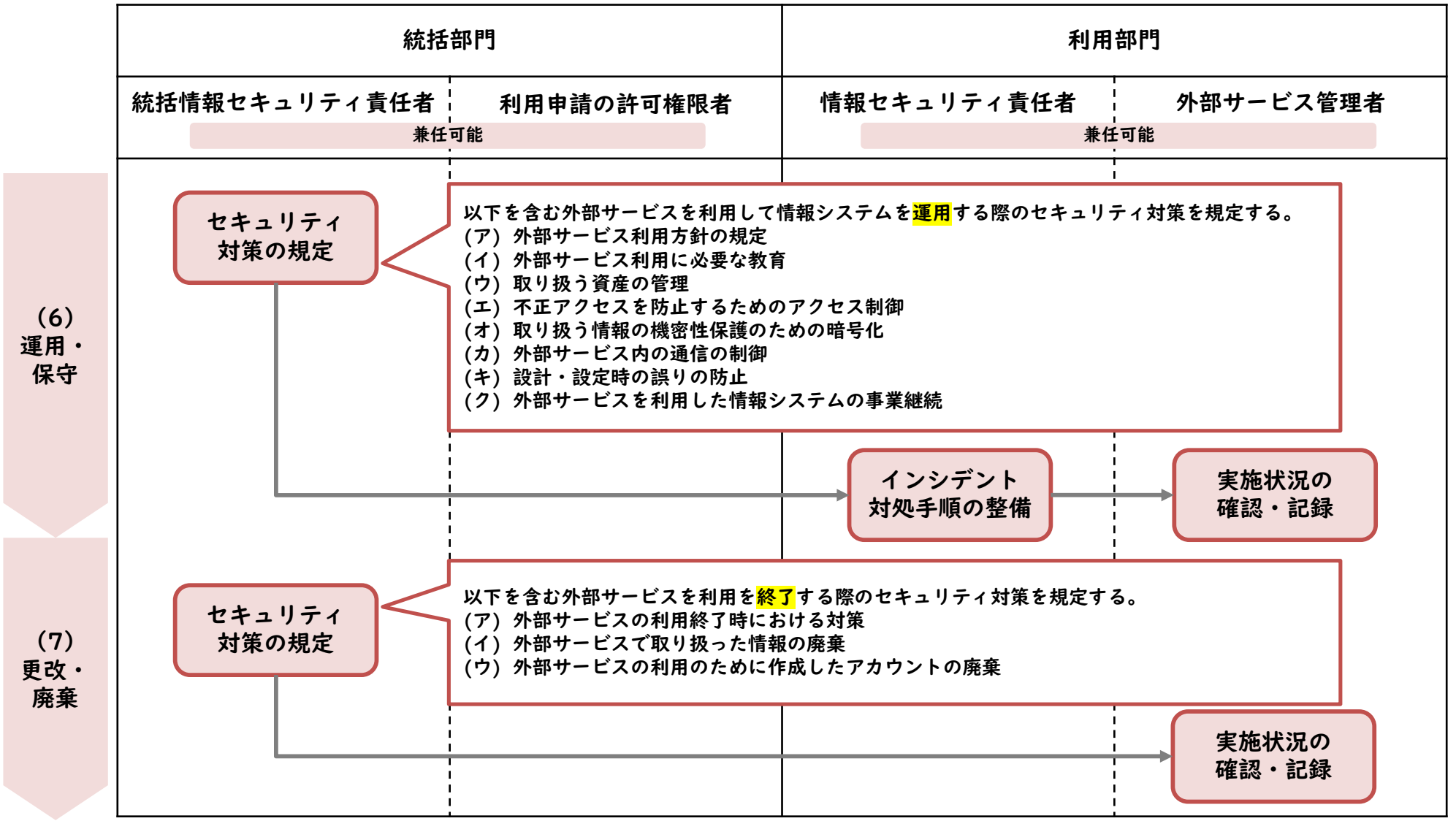
【参考】機密性2以上の情報を取り扱う場合の外部サービス利用の流れ（1/3）



【参考】機密性2以上の情報を取り扱う場合の外部サービス利用の流れ（2/3）



【参考】機密性2以上の情報を取り扱う場合の外部サービス利用の流れ（3/3）



【参考】外部サービス利用に関する役職毎の役割について

部門	役職名	役割等	想定される役職
統括部門	統括情報セキュリティ責任者	CISO及び副CISOの補佐 情報セキュリティ責任者に対して情報セキュリティに関する指導及び助言を行う者	情報政策担当部長　等
	利用申請の許可権限者	外部サービス利用の申請を審査する者	情報政策担当課長　等
利用部門	情報セキュリティ責任者	当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する	各部局長　等
	外部サービス管理者	利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者	所管課長・係長　等
	職員等	職員、非常勤職員等	各職員

地方公共団体の規模等によっては、兼任することも想定される

改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（３/４）

③　クラウドサービス選定の指標・基準等

政府統一基準群の改定概要

要機密情報（機密性２以上の情報）を取り扱う外部サービスのうちクラウドサービスの選定基準として政府情報システムのためのセキュリティ評価制度（ISMAP）の管理基準に従うことが追記されている。

【 基本対策事項 】＜4.2.1(1)(a)(イ)関連＞

4.2.1(1)-1統括情報セキュリティ責任者は、遵守事項4.1.1(1)(a)(イ) で整備を求めている「委託先の選定基準」と同等の規定となるよう外部サービス提供者の選定基準を策定すること。また、クラウドサービス選定における外部サービス提供者の選定基準は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」（以下「ISMAP」という。）の管理基準に従い策定すること。

改定の概要

- クラウドサービス選定の指標・基準等については、今後、クラウドサービスの活用が進んでいくことが予想されることから、監査報告書や認証制度を積極的に利用するように記載の見直しを行う。

- ISMAPについては、自治体の規模等を考慮し、一律に基準を設けることはせずに参考とすべき第三者認証の一つとして追加する。

※クラウドサービスの利用については、今後、デジタル庁におけるガバメントクラウドを活用した実証実験の検討状況等を踏まえ、引き続き検討を行う。

改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（４/４）

③　クラウドサービス選定の指標・基準等

＜現行：対策基準（解説）＞

（新設）※章立ての変更

8.4. クラウドサービスの利用
【解説】

　このような評価に当たって、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。
　なお、参考となる認証には、ISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、日本セキュリティ監査協会のクラウド情報セキュリティ監査やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告書であるSOC報告書（Service Organization Control Report）を活用することも考えられる。クラウドサービス利用時のセキュリティ対策や内部統制に関する報告書等については、以下を参照されたい。
参考：国際規格
「ISO/IEC 27017（安全なクラウドサービス利用のための分野別ISMS 規格）」
参考：日本セキュリティ監査協会
「クラウド情報セキュリティ管理基準」
「クラウド情報セキュリティ監査制度規程」

ISMAPを参考とすべき第三者認証の一つとして追加し、監査報告書や認証を積極的に利用するように記載を見直し

＜改定案：対策基準(解説)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）
【解説】
（２）外部サービスの選定
　このような評価に当たって、外部サービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。
　なお、選定条件となる認証にはISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、ISMAPの管理基準を満たすことの確認やISMAPクラウドサービスリスト等のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス事業者等のセキュリティに係る内部統制の保証報告書であるSOC報告書（Service Organization Control Report）を活用することを推奨する。外部サービス利用時のセキュリティ対策や内部統制に関する報告書等については、以下を参照されたい。
参考：国際規格
「ISO/IEC 27017（安全なクラウドサービス利用のための分野別ISMS 規格）」
参考：日本セキュリティ監査協会
「クラウド情報セキュリティ管理基準」
（https://jcispa.jasa.jp/documents/）
「クラウド情報セキュリティ監査制度規程」
（https://jcispa.jasa.jp/cloud_security/jcispa_regulation/）

改定のポイント２：情報セキュリティ対策の動向を踏まえた記載の充実（１/１）

改定の概要

- 政府統一基準群では、常時アクセス判断・許可アーキテクチャの考え方があることを紹介した上で、採用する際の対策としてEDR等の対策が示された。現行ガイドラインでは、インターネット接続系に業務端末を配置したモデル（βモデル、β’モデル）について、従来のモデルと比較してセキュリティ上のリスクが高まることからEDR等の対策を記載している。
- 今回新たに政府統一基準群に記載された対策については、既に現行ガイドラインで同様の記載がなされていることから対策導入に関する新たな記載の見直しは行わないが、導入後の運用面に関する記載については不十分であることから追記を行う。

※常時アクセス判断・許可アーキテクチャの考え方については、「自治体の三層の対策 」の抜本的見直しを含めた新たなセキュリティ対策の在り方等の検討の中で引き続き検討を行う。

＜現行：対策基準（解説）＞

３　情報システム全体の強靭性の向上
（注１０）未知の不正プログラムへの対策（エンドポイント対策）
　未知の不正プログラム対策として、OSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。

運用面に関する記載を追記。また、昨年度の検討会での議論の経緯から、引き続きEDRという個別の名称は用いずに機能面のみで記載

＜改定案：対策基準(解説)＞

３　情報システム全体の強靭性の向上
（注１０）未知の不正プログラムへの対策（エンドポイント対策）
　未知の不正プログラム対策として、OSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。なお**製品の導入だけでは未知の不正プログラムの対策とはならない。監視体制やCSIRTとの連携等組織的な対策と合わせて検討が必要となることに留意する必要がある。**

【参考】政府統一基準群における常時アクセス判断・許可アーキテクチャ等に関する記載

政府統一基準群（抜粋）

- **「ゼロトラストアーキテクチャ」とは、**データやサービス等のリソースへのアクセス毎に認証・認可を行い、利用者や端末、エリアなどを無条件に信頼しないという考え方をとるモデルである。

- **基本対策事項6.1.2(1)-1 f）「常時アクセス判断・許可アーキテクチャ」について**

　従来の境界型セキュリティアーキテクチャ（守るべき情報が機関等内にあることを前提とし、これらを機関等外の脅威から守るためにインターネットとの境界で防御を行うことを基本とする情報セキュリティ対策の考え方。）では、信頼されたエリアからのアクセスについては、アクセス制御がされない事も多く、一度アクセスを許可した端末・ユーザや信頼できると判断された内部イントラネット等からの脅威に対応できない課題があった。常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ、ゼロトラストセキュリティ等と呼称される。）では、データやサービス等のリソースへのアクセス毎に認証・認可を行い、利用者や端末、エリアなどを無条件に信頼しないという考え方をとるモデルを基本とすることでその課題に対応する。

　常時アクセス判断・許可アーキテクチャにおいて、アクセスルールを策定する際には、業務に必要な最小限の権限とし、可能な限り細かく設定される必要がある。そのためには組織の資産や業務について十分な理解と分析が必要となることから、組織全体へ一度に適用することは難しいため、組織のリスク評価等を踏まえ適用を優先するケースから段階的に導入する事が考えられる。

　また、常時アクセス判断・許可を行うための機器等に対して不正アクセスやサービス停止が発生した際には対象の業務全体への影響が発生することから、それら機器等については適切な構成管理と監視、冗長構成とするなどの対応が必要である。

- **基本対策事項6.2.2(1)-6「感染拡大の防止」について**

　端末やサーバ装置（エンドポイント）の活動を監視し、不正プログラム等の検知や対処を行うEDR（Endpoint Detection and Response）ソフトウェア等を利用し、複数台にわたって統合的に監視を行うことで、感染した装置を早期にネットワークから切り離す仕組みの導入。ただし、一般的にEDRソフトウェアは導入後の運用・保守段階において、専門的な知識を持った人材による膨大なログの分析が必要になることから、マネージドセキュリティサービス（Managed Security Service：MSS）と呼ばれる、ログ分析等を行うSOC（Security Operation Center）業務を委託できるサービスの利用なども検討するとよい。

【参考】現行ガイドラインにおけるβ・β’モデルを採用する場合の技術的対策

現行ガイドラインの記載

■「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」（抜粋）

3.情報システム全体の強靭性の向上
（３）インターネット接続系③　【解説】

β’モデルを採用する場合の必須のセキュリティ対策

対策区分	セキュリティ対策	概要
技術的対策	未知の不正プログラム対策（エンドポイント対策）	・従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。
	業務システムログ管理	・インシデントの兆候検知や、インシデント発生後の調査に使用するため、業務システムのログの収集、分析、保管を実施する。
	情報資産単位でのアクセス制御	・情報資産の機密性レベルに応じて業務システム単位でのアクセス制御を行う。文書を管理するサーバ等は課室単位でのアクセス制御を必須とし、係単位でのアクセス制御は推奨とする。

β’モデルについては、定期的な脆弱性診断、プラットフォーム診断等の実施が有効である。加えて、情報漏えいに対する対策として、以下の対策も有効である。

・万一ファイルが外部に漏えいしても解読できないよう、データベースやファイルの暗号化
・組織が定義したポリシーに従ってデータへの操作を監視・制限し情報の流出を防止（Data Loss Prevention）
・組織が許可していない外部接続先のサービスへのアクセスを監視、遮断

（注１０）未知の不正プログラムへの対策（エンドポイント対策）

未知の不正プログラム対策として、OSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。

改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（１/１）

改定の概要

①テレワーク実施時のセキュリティ対策

現行ガイドラインでは、令和２年度の検討会での検討結果を踏まえテレワークとして想定される技術的なモデル（LGWAN-ASPサービスを利用したモデル、インターネット接続系を経由したモデル等）を記載しているが、運用面に係る対策の記載がないため、政府統一基準群の記載を参考に、テレワーク実施場所等の運用面に係る対策を追記する。

・テレワーク実施前及び実施後に職員がチェックすべき項目を定めチェックを実施させること
・画面ののぞき見や盗聴を防止できるような環境を選定すること　等

②支給以外の端末（BYOD）利用時のセキュリティ対策

現行ガイドラインにおいても、BYODの利用手順や技術的な対策を一部記載しているが、政府統一基準群で対策の詳細な内容が記載されたことから、政府統一基準群の記載を参考に、端末に情報を保存できないようにするための機能を設ける等の対策を追記する。

・利用者が端末に情報を保存できないようにするための機能を設けること
・利用申請手続（利用者、目的、利用する情報、端末等）を職員に遵守させること　等

③Web会議サービス利用時のセキュリティ対策

現行ガイドラインでは、Web会議サービス利用に特化したセキュリティ対策の記載がないため、政府統一基準群の記載を参考に、 Web会議に無関係の者が参加できないような対策等を記載する。

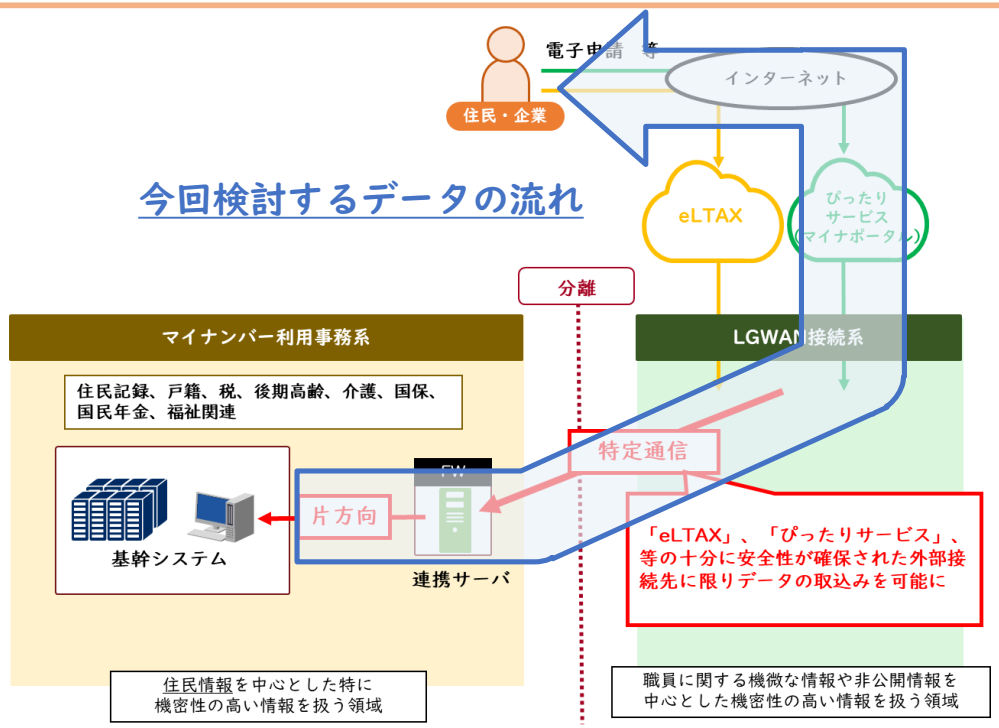
・なりすましが疑われるなどの不審な参加者を会議室から退室させること
・ビデオカメラで撮影されれば会議内容は保存されるため、会議で取り扱う情報を確認する必要があること　等

改定のポイント４：マイナンバー利用事務系から外部接続先（eLTAX、ぴったりサービス）へのデータのアップロード（１/１）

改定の概要

- 現行のガイドラインでは、国等の公的機関が構築したシステム等十分に安全性が確保された外部接続先（例：eLTAX、ぴったりサービス）に限り、インターネット経由の申請等のデータをマイナンバー利用事務系へ電子的に移送（片方向通信）することを可能としている。ユーザーからの要望等を踏まえ、マイナンバー利用事務系から十分に安全性が確保された外部接続先へのデータのアップロードについて、リスク分析の結果を踏まえて、追加で必要となるセキュリティ対策を記載することで双方向通信を認めるかの判断を行う。

※リスク分析については、地方公共団体の協力のもと「制御システムのセキュリティリスク分析ガイド第2版」（ＩＰＡ）を参考に、実際のネットワーク構成、サーバ構成等について事業被害ベースのリスク分析を実施し、結果を次回の検討会で報告予定



【参考】事業被害ベースのリスク分析について①

事業被害ベースのリスク分析とは、「回避したい事業被害を明確化し、事業被害を引き起こすと想定される攻撃について、**事業被害の大きさと、攻撃の発生可能性と受容可能性（脆弱性）の相乗値によって、事業のリスクを評価するリスク分析手法**」である。

➢ **事業被害ベースのリスク分析の流れ**

①事業被害（製造停止、供給停止、システム破壊、機密情報の漏えい等）を定義し、事業被害レベルを評価する
事業に直接影響を及ぼす被害を洗い出し、各事業被害について現実化した場合の事業への影響の大きさを評価する。

②事業被害を引き起こす攻撃シナリオを検討する
供給停止を引き起こすシナリオとして、供給を制御する装置に不正な制御コマンドを送るケースや、制御装置のソフトウェア自体や設定に攻撃（改ざん等）を行うケース等、様々なケースを検討する。

③攻撃シナリオを実現する攻撃ツリーを構成する
攻撃シナリオを、必要に応じてサブ攻撃シナリオに分類する。

④攻撃ツリーが発生する可能性を評価する
攻撃ツリーを構成する一連の攻撃ステップにおける攻撃の難易度や想定する攻撃者等を考慮して、その攻撃ツリーの発生する可能性を評価する。

⑤攻撃ツリーが攻撃を受容する可能性を評価する
攻撃ツリーを構成する一連の攻撃ステップについて、各攻撃ステップに対する対策の充分性を評価し、その攻撃ツリーが攻撃を受容する可能性を評価する。

⑥攻撃ツリーのリスク値を算定する
①と④⑤の相乗値でリスク値を算定する。

出典：「制御システムのセキュリティリスク分析ガイド第２版」（2020年３月　IPA）
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html#section10

【参考】事業被害ベースのリスク分析について②

用語	説明
攻撃シナリオ	事業被害ベースのリスク分析において、事業被害を引き起こす可能性のある攻撃拠点・攻撃対象・最終攻撃を具体化したシナリオ
攻撃ステップ	攻撃ツリーを構成する個々の攻撃手順
攻撃ツリー	事業被害ベースのリスク分析において、攻撃シナリオに含まれる攻撃拠点・攻撃対象・最終攻撃に加えて、攻撃シナリオを実現する攻撃者・侵入口・経由を具体化した一連の攻撃手順
リスク値	保護対象が損なわれる各々のリスクに対して、被害の大きさと脅威の発生可能性／受容可能性を、相対評価可能な値として算定した値 事業被害ベースのリスク分析においては、事業被害レベル、脅威レベル、脆弱性レベルの評価値を基に算定する、各々の攻撃ツリーの総合的なリスクレベル
リスク分析	保護すべきシステムやそれによって実現している事業（サービス等含む）に対する脅威によって生じる被害とその大きさ、脅威の発生可能性と受容可能性等を、リスクレベルとして明確化するプロセス

出典：「制御システムのセキュリティリスク分析ガイド第２版」（2020年３月　IPA）
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html#section10