資料３

# 電磁的記録媒体を利用しないデータ連携における リスクアセスメントの実施について

総務省

令和８年６月８日
自治行政局 住民制度課
サイバーセキュリティ対策室

# 背景・目的

**論点①**

- クラウドサービスやスマートフォン利用の浸透によりデジタルを活用したワンストップサービスが主流となっている中、データの受け渡しに電磁的記録媒体（以降「USBメモリ等」という。）を都度利用することによる業務の生産性の低下やUSBメモリ等の管理不備による紛失等による情報漏えい等のリスクが課題となっている。また、サイバー攻撃の高度化を受け、境界型防御のみに依拠した「三層の対策」の見直しも必要な状況にある。そのため、従来の「三層の対策」に拘ることなく、**ゼロトラストアーキテクチャの考え方を採用したUSBメモリ等を用いないデータ連携モデルについても検討した上でクラウド特有のリスクを抽出するとともに必要な対策を明確にし**、DXが推進可能なモデルを明らかにすることが必要である。
- 上記の趣旨に照らし、第21回検討会で提示した、**フロントヤードとバックヤード間の業務連携を考慮したユースケース**をもとに、LGWAN-ASPまたは、パブリッククラウドにおける**電子申請サービスと各領域（マイナンバー利用事務系、LGWAN接続系、インターネット接続系）間のデータ連携を行う4つのモデル**に対し**リスクアセスメントを行い**各モデルにおけるセキュリティ上の脅威や脆弱性のレベルを明らかにする。

**＜リスクアセスメントを実施する4モデル（第20回検討会にて提示）＞**

| 区分 | 運用環境 | セキュリティ・アプローチ |
|---|---|---|
| 検証モデル①a | オンプレミス（ファイル連携サーバ） | 境界セグメントを配置 |
| 検証モデル①b | オンプレミス（ファイル交換システム） | 境界セグメントを配置 |
| 検証モデル①c | オンプレミス（クラウドストレージ） | ローカルブレイクアウト |
| 検証モデル② | クラウド | クラウドにおけるアクセス制御 |
| 検証モデル③ | クラウド（一部オンプレ） | ゼロトラストアーキテクチャ |
| 検証モデル④ | クラウド | API連携 |

# リスクアセスメント手法の概要

- リスクアセスメントは、**「資産ベースのリスク分析」と「事業被害（事象）ベース」**※の両方のリスクアセスメントを行うことで相互補完性を確保し**総合的な評価**に繋げる。
- 「制御システムのセキュリティリスク分析ガイド 第2版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」（2026年4月版 IPA）を参照するものの**攻撃の起点・戦術、クラウドサービスに関する脅威や攻撃ツリー等**に関しては、**世界的に標準なってる各ドキュメントを参考**にリスクアセスメントを実施する。
- **資産の重要度や事業被害における評価ポイントに、マイナンバー利用事務系を中心とした住民サービスへの影響を特に考慮する。**
- クラウド環境においては、**特定のクラウドサービスの利用を前提**とせずにアセスメントを実施する。

**（1）資産ベースのリスク分析**

保護すべきシステムを構成する各資産（サーバ、端末、通信機器等）を対象に、その「重要度（価値）」、想定される「脅威の発生可能性」、脅威に対する「脆弱性」の３つを評価指標として、リスクを評価する分析手法

**（2）事業被害ベースのリスク分析（攻撃シナリオと攻撃ツリーによる分析）**

システムで実現している事業やサービスに対して、回避したい「事業被害とそのレベル」、その被害を起こしうる「攻撃ツリーの発生可能性」、攻撃に対する「脆弱性」の3つを評価指標として、リスクを評価する分析手法

※政府機関等の対策基準策定のためのガイドライン（令和7年度版）(令和7年9月5日 一部改定)においてもリスク特定のアプローチとして示されている。（p53～p54）

# リスクアセスメントの実施手順

■ 本リスクアセスメントは以下の手順で進める。リスクアセスメントの対象とする検証モデル及びユースケースを定義し、資産ベースのリスク分析及び事業被害ベースのリスク分析を行う。

**ユースケース・データフローの整理**

マイナンバー利用事務系と他の領域とのデータ連携を軸に
リスクアセスメントを行う自治体業務のユースケースを整理する。

**検証モデル（４モデル）の作成**

検証を行うモデルを定義し、その構成要素を整理し
ネットワーク構成図を作成する。

**今年度の検討事項**

**資産ベースのリスク分析**

**事業被害ベースのリスク分析**

4モデル（三層の対策ベース・クラウド・ゼロトラストアーキテクチャ・API連携）に対して資産ベースと事業被害ベースのリスク分析を実施。

**総合的な分析**

脅威や脆弱性から算出されるリスク値をもとに、各モデルにおけるリスクと必要な対策について整理。
USBメモリ等を利用する際のリスクと比較し、自治体が今後目指す方向性や対応について整理。

**ガイドラインへの反映の検討**

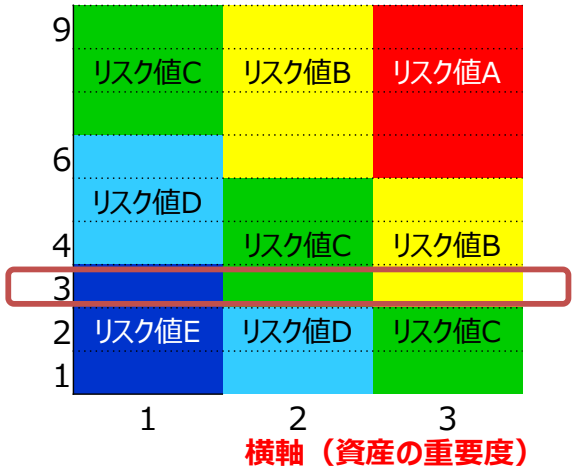
今年度のガイドラインに反映する内容を検討し改定案を検討。

# 資産ベースのリスク分析計画：分析の進め方と指標の定義

■ 資産ベースのリスク分析は、保護すべき制御システムを構成する資産群を明確化し、各資産に対するシステム構成上及び運用管理上に想定される脅威について、各資産の重要度と、その脅威の発生可能性と受容可能性（脆弱性）の相乗値によって、資産のリスクを評価するリスク分析手法である。各指標は、以下のとおり定義した。

**縦軸**

**（脅威レベル×脆弱性レベル）**




**横軸（資産の重要度）**

**資産の重要度が1の場合において、脅威レベル×脆弱性レベルが3以下となる場合は、リスク値がEとなり、「リスクが非常に低い」という結果になる。**

**一方、資産の重要度が3の場合は、脅威レベル×脆弱性レベル3であっても、リスク値はBとなり「リスクが高い」という結果になる。**

| リスク値 | 意味 |
|---|---|
| A | リスクが非常に高い。 |
| B | リスクが高い。 |
| C | リスクが中程度。 |
| D | リスクが低い。 |
| E | リスクが非常に低い。 |

脅威レベルの定義

| 評価値 | 判断基準 | |
|---|---|---|
| | ①攻撃対象の論理的配置による分類 | ②攻撃対象の物理的配置による分類 ※補足的に使用 |
| 3 | インターネットからアクセス可能なネットワーク上にある資産に対して、攻撃が試みられる可能性がある。 | 誰でもアクセス可能な場所にある資産に対して、攻撃が試みられる可能性がある。 |
| 2 | イントラネット上にある資産に対して、攻撃が試みられる可能性がある。 | アクセス可能な人を限定した場所にある資産に対して、攻撃が試みられる可能性がある。 |
| 1 | インターネットから分離されたネットワーク上にある資産に対して、攻撃が試みられる可能性がある。 | 多要素認証機能を用いた入室制限等、アクセス可能な人を著しく限定した場所にある資産に対して、攻撃が試みられる可能性がある |

対策レベルと脆弱性レベルの対応

| 対策レベル | 判断基準 | 脆弱性レベル |
|---|---|---|
| 3 | • 当該脅威（攻撃手段）において、複数の「防御」「検知/被害把握」可能な対策項目を**多層**で実施しており、攻撃が成功する可能性は低い。（**有効な対策が二つ以上**） | 1 |
| 2 | • 当該脅威（攻撃手段）において、「防御」「検知/被害把握」可能な対策項目を実施している。即ち、**対策が一つ**以上備わっているが、十分とは言えないため、攻撃が成功する可能性は中程度である。 | 2 |
| 1 | • 当該脅威（攻撃手段）にいて、「防御」「検知/被害把握」可能な対策項目を実施していない。即ち対策が一つも実施されておらず、攻撃が成功する可能性は高い。<br>• 対策項目は実施されているが、**既知の脆弱性に対し、パッチが未適用である等、脆弱性の管理ができていない状態**であり、攻撃が成功する可能性は高い。 | 3 |

資産の重要度

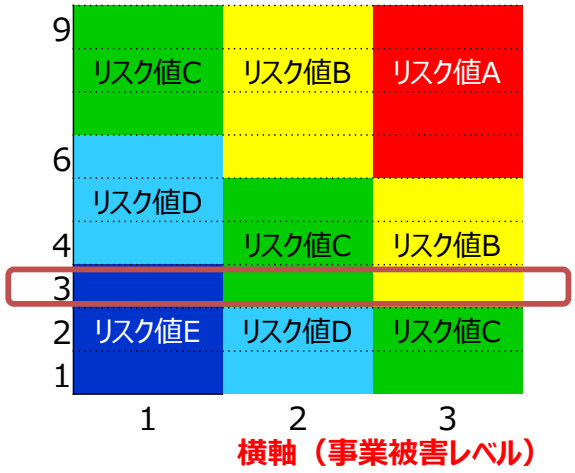
| 評価値 | 評価基準 |
|---|---|
| 3 | • **マイナンバー情報の漏えい、毀損**が生じる。<br>• システム・ネットワークの基盤が攻撃されマルウェア感染、設定の改ざんなどの攻撃をされた場合、地方公共団体のマイナンバー利用事務系に係るシステムが停止するなど住民サービスに影響する。 |
| 2 | • **LGWAN接続系、インターネット接続系**のシステムがマルウェアに感染する等で自治体機密性3C・機密性2に相当する**情報の漏えいや毀損**が生じる。 |
| 1 | • 資産が攻撃された場合、住民サービス・業務に**影響がない。**<br>• 資産が攻撃された場合、**システムが停止するが即時復旧または代替が可能**である。 |

# 事業被害ベースのリスク分析計画：分析の進め方と指標の定義

■ 事業被害ベースのリスク分析は、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。各指標は、以下のとおり定義した。

**縦軸**

**（脅威レベル×脆弱性レベル）**




**資産の重要度が1の場合において、脅威レベル×脆弱性レベルが3以下となる場合は、リスク値がEとなり、「リスクが非常に低い」という結果になる。**

**一方、資産の重要度が3の場合は、脅威レベル×脆弱性レベル3であっても、リスク値はBとなり「リスクが高い」という結果になる。**

| リスク値 | 意味 |
|---|---|
| A | リスクが非常に高い。 |
| B | リスクが高い。 |
| C | リスクが中程度。 |
| D | リスクが低い。 |
| E | リスクが非常に低い。 |

脅威レベルの定義

| 評価値 | 判断基準 | |
|---|---|---|
| | ①攻撃対象の論理的配置による分類 | ②攻撃対象の物理的配置による分類 ※補足的に使用 |
| 3 | インターネットからアクセス可能なネットワーク上にある資産に対して、攻撃が試みられる可能性がある。 | 誰でもアクセス可能な場所にある資産に対して、攻撃が試みられる可能性がある。 |
| 2 | イントラネット上にある資産に対して、攻撃が試みられる可能性がある。 | アクセス可能な人を限定した場所にある資産に対して、攻撃が試みられる可能性がある。 |
| 1 | インターネットから分離されたネットワーク上にある資産に対して、攻撃が試みられる可能性がある。 | 多要素認証機能を用いた入室制限等、アクセス可能な人を著しく限定した場所にある資産に対して、攻撃が試みられる可能性がある |

対策レベルと脆弱性レベルの対応

| 対策レベル | 判断基準 | 脆弱性レベル |
|---|---|---|
| 3 | • 当該脅威（攻撃手段）において、複数の「防御」「検知/被害把握」可能な対策項目を**多層**で実施しており、攻撃が成功する可能性は低い。（**有効な対策が二つ以上**） | 1 |
| 2 | • 当該脅威（攻撃手段）において、「防御」「検知/被害把握」可能な対策項目を実施している。即ち、**対策が一つ**以上備わっているが、十分とは言えないため、攻撃が成功する可能性は中程度である。 | 2 |
| 1 | • 当該脅威（攻撃手段）にいて、「防御」「検知/被害把握」可能な対策項目を実施していない。即ち対策が一つも実施されておらず、攻撃が成功する可能性は高い。<br>• 対策項目は実施されているが、**既知の脆弱性に対し、パッチが未適用である等、脆弱性の管理ができていない状態で**あり、攻撃が成功する可能性は高い。 | 3 |

事業被害レベル

| 評価値 | 判断基準 |
|---|---|
| 3 | 資産が失われた、もしくは不正に操作された場合、事実上の被害大となる。<br>－システムの停止が**マイナンバー利用事務系の業務停止**につながる<br>－不正利用による**マイナンバー利用事務系の業務継続に支障をきたす**<br>－**マイナンバー利用事務系の情報漏えい、不正アクセス等により社会的な問題に発展**する |
| 2 | 資産が失われた、もしくは不正に操作された場合、事実上の被害中となる。<br>－マイナンバー利用事務系に影響はなく、**LGWAN接続系、インターネット接続系の業務に一部、限定されるなどの支障をきたす** |
| 1 | 資産が失われた、もしくは不正に操作された場合、事実上の被害小となる。<br>－マイナンバー利用事務系に影響はなく、他の業務にも情報漏えいなどはなく**業務への影響はない** |

# 事業被害ベースのリスク分析計画：事業被害及び事業被害レベルの定義

- 評価指標「事業被害」とは、**システムによって実現している事業が損なわれた場合の被害の大きさ**を表す。
- 評価値「事業被害レベル」は、評価指標「事業被害」（事業が損なわれた場合の被害の大きさ）を**3 段階（1～3）**で評価した値である。
- 本事業で用いる事業被害は特に**機密性・完全性・可用性の観点及び財政的な被害を想定**し、下表のとおりとする。
  ※事業被害は各モデルで同一とする。ただし、クラウドを活用するモデルでは、クラウド固有の事業被害を追加する。（下表④）

＜本リスク分析における攻撃目標に対する事業被害の想定事業被害レベルの対応＞

| 事業被害 | 事業被害レベル | 本リスク分析における攻撃目標（例） |
|---|---|---|
| ① 基幹業務システムが停止し、窓口業務、オンライン申請等の行政サービスが提供できなくなる | 3 | • 基幹業務システム（福祉関連システム） |
| ② 個人情報が漏えいし、住民の信頼を損なう、また、法令違反の問題が生じる | 3 | • 基幹業務システム（福祉関連システム） |
| ②´ 内部の文書・情報（自治体機密性3C・機密性2）の破壊・改ざん・漏えいにより、行政運営の公平性・公正性が失われる、または、業務に支障をきたす | 2 | • 内部情報システム（文書管理・財務会計システム） |
| ③ 住民データが破壊・改ざんされ、誤った行政手続を行ってしまう | 3 | • 基幹業務システム（福祉関連システム） |
| ④ 大量の通信等により多額の課金が行われる（※クラウド活用の場合） | 1 | • クラウド管理コンソール |

# 事業被害ベースのリスク分析計画：攻撃ルートの考え方

- 自治体のIT環境を想定した仮想モデルを対象とし、国際的に標準で利用されているMITRE ATT&CK Enterprise※3 のInitial Access ※4テクニックに準拠し検討した上で、**各モデルの環境に現実的に成立し得る侵入起点を抽出**し、前述の事業被害（機密性・完全性・可用性＋財政的被害）を生じさせる攻撃ルートを設計した。
- オンプレ環境・クラウド環境における攻撃ステップは、MITRE ATT&CK のタクティクス（戦術）の流れを基本として**具体化**している。

＜想定する起点（MITRE ATT&CKのInitial Access）※1＞

| 項番 | MITRE ATT&CK（Initial Access のテクニック） | 起点 | 選定理由 |
|---|---|---|---|
| T1659 | Content Injection | 水飲み場型攻撃等による端末のマルウェア感染 | **インターネット接続系の業務端末**はWeb 閲覧・メール受信を行うため、侵害が発生する可能性が高い |
| T1189 | Drive-by Compromise | 水飲み場型攻撃等による端末のマルウェア感染 | |
| T1566 | Phishing | ・標的型メール等を利用した認証情報の窃取<br>・添付ファイル等からの端末のマルウェア感染 | |
| T1190 | Exploit Public-Facing Application | ・申請システムの申請データへのマルウェア添付、不正なコード埋め込み<br>・APIの脆弱性を利用したシステムへの攻撃 ※2 | ・**申請システム**はインターネットから直接アクセス可能であり、内部システムへ不正なデータ、マルウェアが持ち込まれる可能性がある<br>・セキュリティコントロール 配下から漏れた**API**が存在する可能性がある |
| T1091 | Replication Through Removable Media | マルウェアが埋め込まれたUSBメモリを郵送・接続させることで端末が感染 | **USBメモリ等の可搬媒体**がデータ受渡しに使われるため、LGWAN接続系の閉域性の突破に利用される可能性がある |
| T1078 | Valid Accounts | ・窃取したクラウドアカウントの認証情報を利用し、業務システム等のリソースへアクセス（認証基盤を通過する）※2 | **正規認証情報の窃取**により、認証基盤を「正規ユーザ」として通過する可能性がある |

※1：オンプレミス環境における運用・保守事業者のリモート保守を起因としたリスクは、**閉域網を利用したリモート保守とする**ことで本リスクアセスメントの対象外とした
※2：クラウド環境に限定

＜MITRE ATT&CKのタクティクス（Initial Access以降）と攻撃ルートの対応＞

| 段階 | タクティクス | 本アセスメントの攻撃ルートとの対応 |
|---|---|---|
| 侵入 | Initial Access | 左記 Initial Access |
| 侵害の確立 | Execution | 不正コード・添付ファイル実行<br>（クラウド）管理コンソール操作 |
| | Persistence | C2サーバとの接続確立・遠隔操作<br>（クラウド）APIトークン等の保持 |
| | Privilege Escalation | 各系のADの侵害<br>（クラウド）IAMの過剰権限の悪用 |
| | Stealth | 申請データ内への不正データの潜伏<br>（クラウド）正規通信に偽装した通信の実施 |
| | Defense Impairment | セキュリティ対策サーバの無効化<br>（クラウド）監査ログ・アラート無効化 |
| 内部展開 | Credential Access | 認証情報の窃取（ダンプ・保存情報取得）<br>（クラウド）MFAの回避・トークン窃取 |
| | Discovery | ネットワーク構成・AD権限調査<br>（クラウド）クラウドリソース列挙 |
| | Lateral Movement | FWの突破、データ連携経路経由の展開<br>（クラウド）正規認証で他クラウドサービスへ遷移 |
| 目的達成準備 | Collection | ファイル・データ収集<br>（クラウド）APIレスポンス取得、ストレージダンプ |
| | Command and Control | C2サーバによる遠隔操作 |
| | Exfiltration | メール・外部通信を用いた情報の持ち出し<br>（クラウド）外部アカウントへの転送 |
| 被害 | Impact | 前述の事業被害 |

※3：MITRE ATT&CK Enterprise（サイバー攻撃手法を体系化した世界共通の指標一覧）
※4：Identity and Access Management

# リスクアセスメントの実施・結果報告書の作成スケジュール

■ リスクアセスメントの結果報告書作成にあたり必要となる作業及びスケジュールの概要は下表のとおり。資産ベースのリスク分析シート及び事業被害ベースのリスク分析シートを作成した上で、リスクアセスメント結果報告書を作成予定である。