資料１

構成員・地方公共団体等からの主な意見と対応について

総務省

2021年12月20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

構成員・地方公共団体等からの主な意見と対応一覧（1/2）

項番	改定のポイント	意見	意見を踏まえての対応	該当箇所
①	1.業務委託・外部サービス利用時の情報資産の取扱い	外部サービスの取扱いについて、地方公共団体が理解しやすいように留意点を追加するなどして理解を促す必要があるのではないか。	地方公共団体が理解しやすいように代表的な外部サービスの留意点を追記する。	改定のポイント P.3、4 改定案 iii-151
②	1.業務委託・外部サービス利用時の情報資産の取扱い	外部サービス利用に慣れていない地方公共団体の職員に対して、クラウドサービスの利用ガイドラインを整備した方がよいのではないか。	NISCが策定した「クラウドを利用したシステム運用に関するガイダンス」（令和３年11月30日）を地方公共団体の職員がクラウドサービスを利用するにあたっての参考文書としてガイドライン上に明記する。	改定のポイント P.3、4 改定案 iii-147
③	1.業務委託・外部サービス利用時の情報資産の取扱い	米国クラウド法（CLOUD Act）では、米国の捜査機関から、米国内に本社を持つクラウド事業者に対して、日本国内にあるデータの開示要求の可能性があるが、過去に地方公共団体についての事例はあるのか。	事例は確認していない。一般論としてデータの差押えが発生する可能性があるため、引き続き検討を行う。	-

構成員・地方公共団体等からの主な意見と対応一覧（2/2）

項番	改定のポイント	意見	意見を踏まえての対応	該当箇所
④	2.情報セキュリティ対策の動向を踏まえた記載の充実	昨年度のガイドライン改定で新たに無害化の手法として認められた目視での確認と振る舞い検知等によりファイルを取り込む方式に関して、「目視」で何をすればよいのかの分かりにくいため、補足説明を加えるべきではないか。	地方公共団体が理解しやすいように補足説明を追記する。	改定案 ⅲ-44
⑤	3.多様な働き方を前提とした情報セキュリティ対策	今回新たに詳細な内容が追加されたBYODについて、セキュリティ対策が不十分となりやすいため、端末を限定する仕組みや追加のセキュリティ対策が必要ではないか。	BYODのセキュリティ対策について、端末を限定する仕組みや追加のセキュリティ対策を追記する。	改定のポイント P.15 改定案 ⅲ-68
⑥	3.多様な働き方を前提とした情報セキュリティ対策	今回新たに追加されたWeb会議サービス利用時の対策について、地方公共団体の実際の運用に配慮した記載とするため、Web会議に招待される場合についても記載してほしい。	地方公共団体の運用に配慮して留意点を追記する。	改定のポイント P.15 改定案 ⅲ-93
⑦	4.マイナンバー利用事務系から外部接続先へのデータのアップロード	利便性向上の観点から重要だと考えるが、リスクアセスメントを実施し、セキュリティ上問題がないことの説明ができるようにすべきではないか。	リスク分析の結果を踏まえ、マイナンバー利用事務系から外部接続先へのデータのアップロードを認めるとともに、地方公共団体に対して、ガイドライン記載の必要となる情報セキュリティ対策の徹底を働きかける。	改定のポイント P.16 改定案 ⅲ-39

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（1/3）

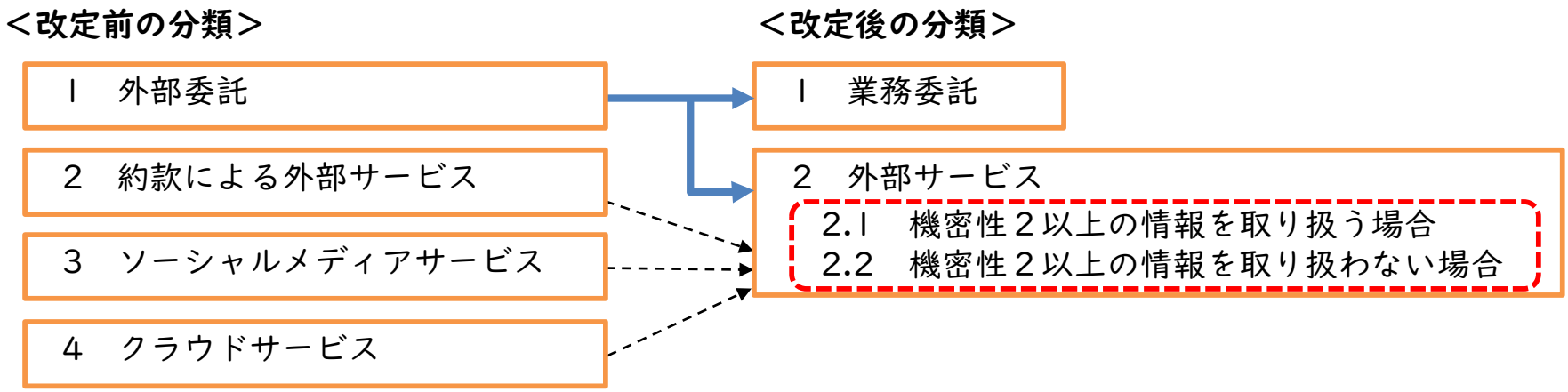
意見①：外部サービスの取扱いについて、地方公共団体が理解しやすいように留意点を追加するなどして理解を促す必要があるのではないか。

対応①：地方公共団体が理解しやすいように代表的な外部サービスの留意点を追記する。

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、機密性２以上の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。



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（2/３）

＜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】

（２）外部サービスの選定

（略）

「政府機関・地方公共団体等における業務での LINE 利用状況調査を踏まえた今後の LINE サービス等の利用の際の考え方（ガイドライン）」を参考に、代表的な外部サービス（SNSサービス、オンライン申請サービス、検索サービス、翻訳サービス、地図サービス等）の利用事例を追記

＜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

（略）

⑨情報の取扱手順

（略）

（注４）外部サービスには様々なサービスがあり、利用においては以下のような点に留意する必要がある。

・SNSサービスの利用においては、公式アカウントを利用した相談業務等を行う際に、SNSサービス提供事業者とは別の委託先に適切にセキュリティが確保されたシステムを構築させ、相談内容や住民の個人情報がSNSサービス提供事業者側に残らず、委託先等のデータベース等に直接格納・保管されるシステム構成とする必要がある。ただし、機密性２以上の情報を取り扱わない場合は、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の利用が許容される。

・オンライン申請サービスの利用においては、住民側のスマートフォンアプリ上のQRコードを後日窓口でかざし申請手続を行うようなサービスの場合、住民等の個人情報が外部サービス提供事業者側に残らないシステム構成とする必要がある。

・検索サービス、翻訳サービス及び地図サービスの利用においては、検索の文言、写真、動画、翻訳の内容及び履歴などがマーケティングや情報収集のために蓄積される場合がある。

・自組織が直接契約する収納代行業者がSNSサービスを介してキャッシュレスサービスを利用する場合は、自組織が保有する住民等の個人情報をキャッシュレスサービス事業者に提供する仕組みとならない構成とする必要がある。

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（３/３）

意見②：外部サービス利用に慣れていない地方公共団体の職員に対して、クラウドサービスの利用ガイドラインを整備した方がよいのではないか。

対応②：NISCが策定した「クラウドを利用したシステム運用に関するガイダンス」（令和３年11月30日）を地方公共団体の職員がクラウドサービスを利用するにあたっての参考文書としてガイドライン上に明記する。

「クラウドを利用したシステム運用に関するガイダンス」について

内閣官房内閣サイバーセキュリティセンター（NISC）が、増加するクラウドサービスの利用について、サービスを使った環境の構築や運用などを行うに当たり、クラウドサービスの利用者がサービスの基本を理解し、インシデントの発生を可能な限り抑制することや、インシデントが発生した際の対応の重要性などを説明した利用者向けガイダンス。

主な記載内容

- クラウドサービスのメリット（調達や導入の負担軽減）やデメリット（利用者が制御できない環境や領域の存在）
- クラウド事業者、利用者などのステークホルダーの確認（利用者、構築者、クラウド事業者等）
- クラウド利用の注意点（設定不備、仕様変更への対応等）
- インシデント発生時の連携の在り方（連絡体制の構築等）　など

執筆協力者

※五十音順：敬称略

アマゾン ウェブ サービス ジャパン合同会社
株式会社エヌ・ティ・ティ・データ
グーグル・クラウド・ジャパン合同会社
クラスメソッド株式会社
グローバルセキュリティエキスパート株式会社
シスコシステムズ合同会社
株式会社セールスフォース・ドットコム
株式会社ディー・エヌ・エー
一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会
日本マイクロソフト株式会社
弁護士 北條 孝佳
楽天グループ株式会社
株式会社ラック
立命館大学 情報理工学部 情報理工学科 教授 上原 哲太郎

改定のポイント２：情報セキュティ対策の動向を踏まえた記載の充実（１/２）

意見④：昨年度のガイドライン改定で新たに無害化の手法として認められた目視での確認と振る舞い検知等によりファイルを取り込む方式に関して、「目視」で何をすればよいのかの分かりにくいため、補足説明を加えるべきではないか。

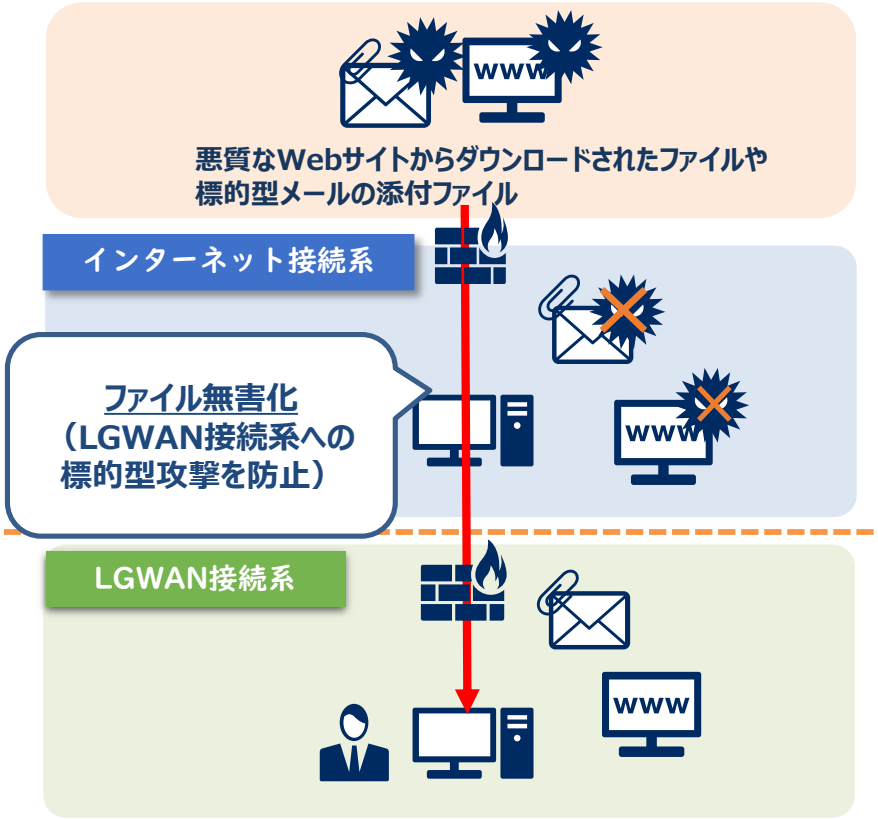
対応④：地方公共団体が理解しやすいように補足説明を追記する。

【参考】令和２年度ガイドライン改定での無害化手法の見直し

改定前のガイドラインでは「ファイル無害化」の手法としてサニタイズ処理のみ記載されていたが、サンドボックス、振る舞い検知及びEDRについても、サニタイズと同様に未知のマルウェア対策として有効となっていることから、サニタイズ処理以外についてもファイル無害化の手法として認める。

改定前ガイドラインの「ファイル無害化」の手法

① ファイルからテキストのみを抽出
② ファイルを画像PDFに変換
③ **無害化するサービス等を活用してファイルを無害化（サニタイズ処理：ファイルを一旦分解した上で危険因子を除去しファイルを再構築し分解前と同様なファイル形式に復元する）**



改定後ガイドラインの「ファイル無害化」の手法

① ファイルからテキストのみを抽出
② ファイルを画像PDFに変換
③ サービス等を活用してサニタイズ処理（ファイルを一旦分解した上で危険因子を除去した後、ファイルを再構築し、分解前と同様なファイル形式に復元する）
④ **インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等で危険因子が含まれていないことを確認**

改定のポイント２：情報セキュティ対策の動向を踏まえた記載の充実（２/２）

＜現行：対策基準（解説）＞

３　情報システム全体の強靭性の向上
（３）②
【解説】
・OS等の修正プログラムの適時適用（自治体情報セキュリティ向上プラットフォームの利用等）
・アンチウイルスソフトウェアの最新化（定義ファイルのアップデート等）
・業務に必要なファイルやメール等の定期的なバックアップの実施
また、上記のLGWAN接続系における対策に加え、業務システムの停止を狙ったマルウェアの感染を防ぐ対策として、LGWAN接続系端末にアプリケーションホワイトリストを設定し、実行できるアプリケーションの制限等を行うことを強く推奨する。
（注５）サニタイズ処理等を実現する手法は多岐にわたるため、適正な製品を選定し導入することが望ましい。
（注６）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系からLGWAN接続系へマルウェア感染を防ぐ必要がある。

補足説明を追記

＜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
（３）②
【解説】
・OS等の修正プログラムの適時適用（自治体情報セキュリティ向上プラットフォームの利用等）
・アンチウイルスソフトウェアの最新化（定義ファイルのアップデート等）
・業務に必要なファイルやメール等の定期的なバックアップの実施
また、上記のLGWAN接続系における対策に加え、業務システムの停止を狙ったマルウェアの感染を防ぐ対策として、LGWAN接続系端末にアプリケーションホワイトリストを設定し、実行できるアプリケーションの制限等を行うことを強く推奨する。
（注５）「目視で確認」とは、ファイルが添付されたメールを開く際に、送信元は適切か（見覚えのないアドレス、フリーアドレスではないか）メールの件名や内容が適切か（見慣れない日本語やフォントが使用されていないか）などを確認することである。未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等の製品の導入に加え、人的対策として「目視で確認」を求めるものである。
（注６）サニタイズ処理等を実現する手法は多岐にわたるため、適正な製品を選定し導入することが望ましい。
（注７）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系からLGWAN接続系へマルウェア感染を防ぐ必要がある。

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（1/2）

意見⑤：今回新たに詳細な内容が追加されたBYODについて、セキュリティ対策が不十分となりやすいため、端末を限定する仕組みや追加のセキュリティ対策が必要ではないか。

対応⑤：BYODのセキュリティ対策について、端末を限定する仕組みや追加のセキュリティ対策を追記する。

＜現行：対策基準（解説）＞	＜改定案：対策基準(解説)＞
（新設）	5.1.職員等の遵守事項 【解説】 ②支給以外のパソコンやモバイル端末等の業務利用 （略） （注６）支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、利用者の機密情報の持出しを防ぐこと以外にも支給以外の端末のOS改造による脆弱性や不正なアプリケーションの利用による支給以外の端末の不正プログラム感染による情報漏えい等に留意する必要がある。また、支給以外の端末の盗難・紛失等による情報漏えいや不正アクセスのリスクにも注意が必要である。そのため、以下のような対策を講じ、許可された端末や利用者であることを確認する仕組みを導入し、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又は端末に保存される情報を暗号化するための機能を設けたりする必要がある。 ・シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。 ・ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。 ・端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。 ・ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。 ・端末のOS改造の検知、私有領域へのデータのコピーの制御やアクセスログ取得等の機能を持つMDM（Mobile Device Management）、MAM（Mobile Application Management）等のソフトウェアを利用して支給以外の端末を管理する。 ・電子証明書による端末認証や、接続する機器のIPアドレス、MACアドレス等の認証情報を利用し端末を制限する機能及び多要素認証による利用者を識別・認証する機能を設ける。

MDM（Mobile Device Management）、MAM（Mobile Application Management）による管理例の記載を追記

電子証明書による端末認証、IPアドレス・MACアドレス等の認証情報を利用した端末制限及び多要素認証による利用者の識別・認証の対策を追記

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（2/2）

意見⑥：今回新たに追加されたWeb会議サービス利用時の対策について、地方公共団体の実際の運用に配慮した記載とするため、Web会議に招待される場合についても記載してほしい。

対応⑥：地方公共団体の運用に配慮して留意点を追記する。

＜現行：対策基準（解説）＞	＜改定案：対策基準(解説)＞
（新設）	6.1. コンピュータ及びネットワークの管理 【解説】 （21）Web会議サービスの利用時の対策 職員等は、Web会議サービスの利用に当たり、以下の情報セキュリティ対策を実施する必要がある。 ・原則として、自組織から支給された端末を利用すること。 ・原則として、自組織で許可されたWeb会議サービスを利用すること。 ・利用するWeb会議サービスのソフトウェアが、最新の状態であることを確認すること。 ・機密性２以上の情報を取り扱う場合は、可能な限りエンドツーエンド（E2E）の暗号化を行うこと。 ・機密性２以上の情報を取り扱う場合は、Web会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2Eの暗号化を利用できなくなる機能を可能な限り使用しないこと。 ・音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。 また、職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう以下の情報セキュリティ対策を講ずる必要がある。 ・会議室にアクセスするためのパスワード等をかける。 ・会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知する。 ・待機室を設けて参加者と確認できた者だけを会議室に入室させる。 ・なりすましや入れ替わり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。 (注１８) Web会議サービスを利用する場合、Web会議サービスのソフトウェアで録画等を防止する設定を行っていても、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、会議内容は会議の参加者に保存されることを前提として、会議で取り扱う情報を確認する必要がある。 (注１９) Web 会議サービスでは音声・映像、参加者のメールアドレス等の属性等様々な個人情報を取り扱うことが考えられるため、Web会議に招待される場合は、原則として、許可されたWeb会議サービスを利用する。やむを得ず自組織で許可されていないWeb会議サービスに招待される場合は、サービスの利用はあくまでも限定的な利用とし、機密性２以上の情報を含んだチャットへの書き込みや資料共有を行わないなど、情報を保存させないような利用手順を定める必要がある。

Web会議サービス利用時の対策の中で、地方公共団体の運用に配慮してWeb会議に招待される場合の取扱いを追記

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）

意見⑦：利便性向上の観点から重要だと考えるが、リスクアセスメントを実施し、セキュリティ上問題がないことの説明ができるようにすべきではないか。

対応⑦：リスク分析の結果を踏まえ、マイナンバー利用事務系から外部接続先へのデータのアップロードを認めるとともに、地方公共団体に対して、ガイドライン記載の必要となる情報セキュリティ対策の徹底を働きかける。

改定の概要

- リスク分析の結果を踏まえ、マイナンバー利用事務系から外部接続先へのデータのアップロードを認めるとともに、地方公共団体に対して、必要となる情報セキュリティ対策の徹底を働きかける。

※必要となるセキュリティ対策のチェックリストを作成・周知することで、設定漏れなどによるインシデントの発生を防止する。併せて、事業者に対しても、必要となるセキュリティ対策の徹底を要請。