自治体情報セキュリティ対策の見直しのポイント

総務省

2020年５月

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

検討の経緯

「三層の対策」

2015年の年金機構の情報漏えい事案を受け、**短期間**で自治体の情報セキュリティ対策を抜本的に強化　＝**「三層の対策」**

⇒　**インシデント数の大幅な減少を実現**

一方で、

①ユーザビリティへの影響

- ✓ **自治体内の情報ネットワークの分離・分割による事務効率の低下**
  例：マイナンバー利用事務系のシステムへのデータの取込み、インターネットメールの添付ファイルの取得など

②新たな時代の要請

- ✓ **行政アプリケーションを自前調達方式からサービス利用式へ**
  （政府における「クラウド・バイ・デフォルト」原則）
- ✓ **行政手続を紙から電子へ**（デジタル手続法を受けた行政手続のオンライン化）
- ✓ **働き方改革**（テレワーク等のリモートアクセス）
- ✓ **サイバー攻撃の増加、サイバー犯罪における手口の巧妙化**　　**等**

「三層の対策」の効果や課題、新たな時代の要請を踏まえ、

効率性・利便性を向上させた新たな自治体情報セキュリティ対策を検討

※「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」において検討

「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」にも反映

（参考）いわゆる「三層の対策」概要

2015（H27）年～2017（H29）年

「三層の対策」によるセキュリティ強化

市区町村におけるネットワーク構成（イメージ）

① 個人番号利用事務系では、端末からの情報持ち出し不可設定等を図り、住民情報流出を徹底して防止

② LGWAN接続系とインターネット接続系を分割し、LGWAN環境のセキュリティ確保

③ 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度な情報セキュリティ対策を実施

2015.5　年金機構の情報漏えい事案発覚後、有識者による「自治体情報セキュリティ対策検討チーム」を設置
2015.11　検討チームより自治体の対策内容（「三層の対策」）について報告
2015.12　総務大臣通知により自治体に「三層の対策」を要請
2016.1　自治体が「三層の対策」に取り組むための補助金（H27補正）の説明会
2017.7　自治体による「三層の対策」への対応完了

これまでの議論の経過

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

	石井夏生利	中央大学国際情報学部教授
	上原哲太郎	立命館大学情報理工学部教授
	岡村　久道	弁護士　京都大学大学院医学研究科講師
(座長)	佐々木良一	東京電機大学総合研究所特命教授
	庄司　昌彦	武蔵大学社会学部メディア社会学科教授
	長峯　道宏	千葉市総務局情報経営部業務改革推進課長（2020年４月から）
	塗師　敏男	横浜市総務局しごと改革室ICT担当部長
	半田　嘉正	富山県経営管理部情報政策課情報企画監
	三輪　信雄	総務省最高情報セキュリティアドバイザー
	若杉　健次	港区総務部情報政策課長（2020年４月まで）

■オブザーバ

総務省自治行政局住民制度課
総務省サイバーセキュリティ統括官室
地方公共団体情報システム機構

※敬称略、五十音順

開催実績

※ 検討会のほか、WGを開催（全３回）

	【主な議題】
■ 第１回 （令和元年12月3日）	・検討会の運営について ・新たな自治体情報セキュリティ対策について
■ 第２回 （令和元年12月23日）	・ ワーキンググループの設置について ・新たな自治体情報セキュリティ対策について・ユーザビリティの改善について
■ 第３回 （令和２年１月31日）	・ワーキンググループでの検討状況について ・ 新たな自治体情報セキュリティ対策について
■ 第４回 （令和２年2月28日）	・ワーキンググループでの検討状況について ・新たな自治体情報セキュリティ対策について
■ 第５回　※書面開催 （令和２年４月20日）	・自治体情報セキュリティ対策の見直しについて（素案）
■ 第６回 （令和２年５月15日）	・自治体情報セキュリティ対策の見直しについて（案） ・今後の進め方について（案）

とりまとめの概要

①とりまとめの位置付け

○　検討会において、**自治体情報セキュリティ対策の見直しに係る具体的施策**をとりまとめ
○　総務省に対して、次期自治体情報セキュリティクラウドの在り方についての自治体への助言や**「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**などを提言

②具体的施策

自治体の**効率性・利便性の向上とセキュリティの確保の両立を実現**する観点から以下を実施

（１）**「三層の対策」の見直し**
（２）**業務の効率性・利便性向上策（各論）**
　　（パブリッククラウドの活用、リモートアクセス、庁内無線LAN）
（３）**次期「自治体情報セキュリティクラウド」の在り方**
（４）**昨今の自治体における重大インシデントを踏まえた対策の強化**
（５）**各自治体の情報セキュリティ体制・インシデント即応体制の強化**
（６）**ガイドラインの適時の改定**

③今後のスケジュール

○　**自治体の予算要求時期等を見据え、早急に自治体に提示すべき事項（次期「自治体情報セキュリティクラウド」の在り方等）は、自治体へ助言**
○　本とりまとめを踏まえ、**ガイドラインについて、2020年夏を目途に改定**

ポイント①：「三層の対策」の見直し

見直しの方向性

○マイナンバー利用事務系の分離に係る見直し

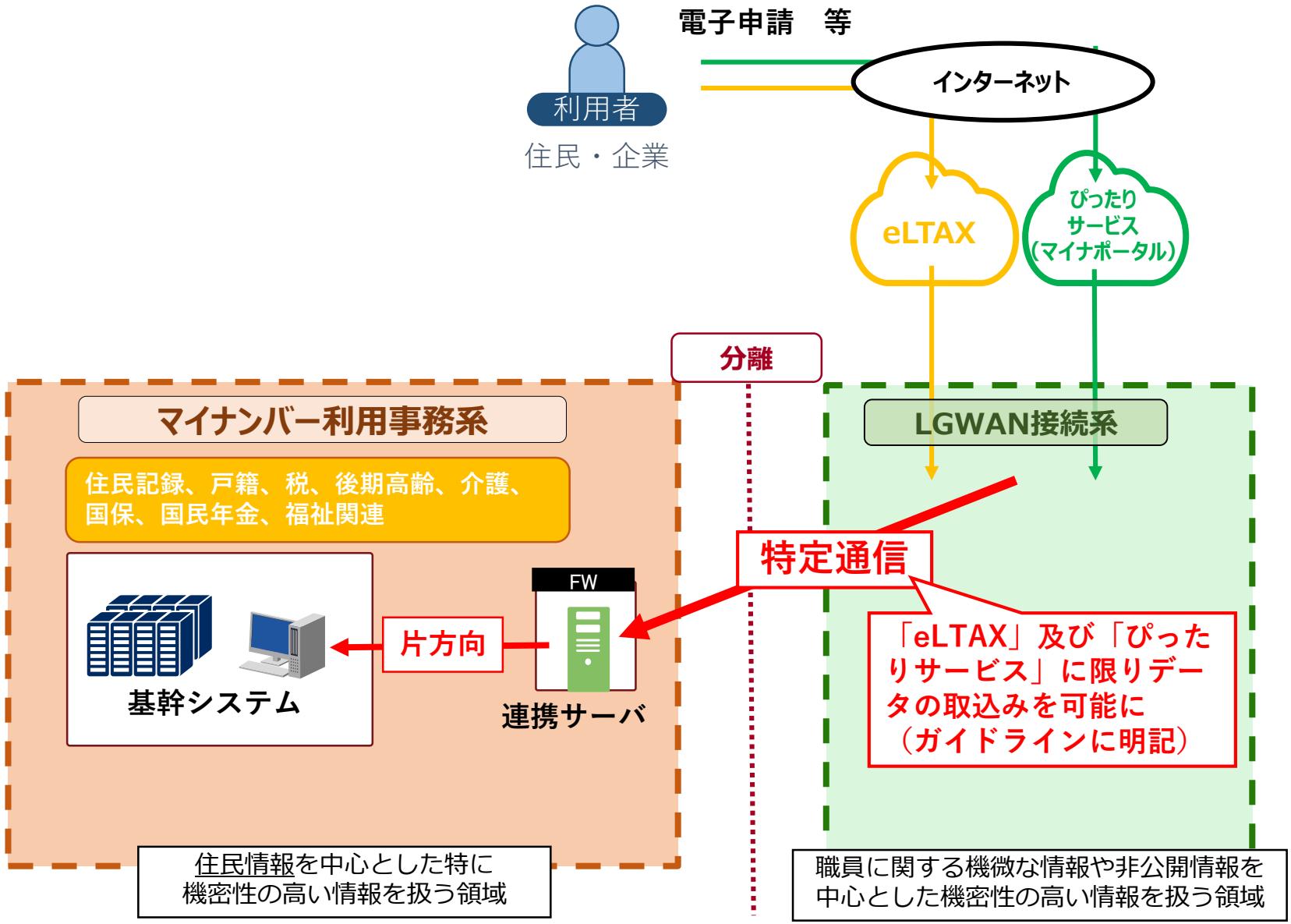
- 住民情報の流出を徹底して防止する観点から**他の領域との分離は維持**
- 十分にセキュリティが確保されていると**国が認めた特定通信（ガイドラインに明記、ex. eLTAX、マイナポータルを活用したぴったりサービス）に限り、**インターネット経由の申請等のデータの**電子的移送を可能**とし、**ユーザビリティの向上**及び**行政手続のオンライン化に対応**

○LGWAN接続系とインターネット接続系の分割に係る見直し

・クラウド・バイ・デフォルト原則やテレワーク等の新たな時代の要請を踏まえて、従来の**「三層の対策」の基本的な枠組みを維持**しつつ、効率性・利便性の高いモデルとして、**インターネット接続系に業務端末・システムを配置した「新たなモデル」（βモデル）を提示**

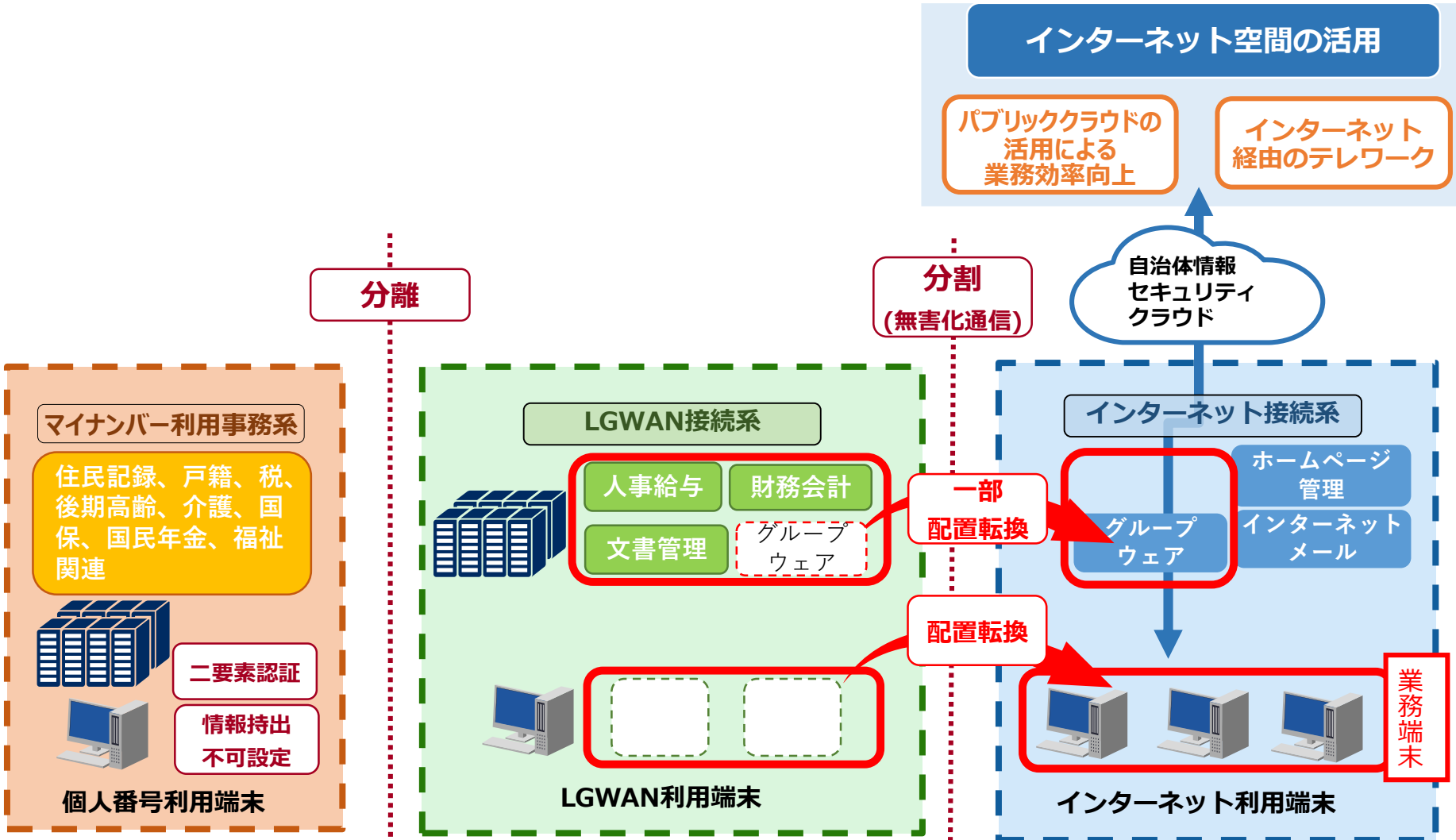
・ただし、自治体によっては対応可能なセキュリティ対策のレベルには差があることから、新たなモデルの採用に当たっては、情報資産単位でのアクセス制御、監視体制やCSIRTなど緊急時即応体制の整備、個々の職員のリテラシー向上など**人的セキュリティ対策の実施が条件となる。**

（参考）マイナンバー利用事務系の分離に係る見直しのイメージ



（参考）新たなモデル（βモデル）のイメージ

- 業務端末の一部をインターネット接続系に移行するとともに、業務システムの一部もインターネット接続系に移行



住民情報を中心とした特に機密性の高い情報を扱う領域

職員に関する機微な情報や非公開情報を中心とした機密性の高い情報を扱う領域

インターネットメールや機密性の低い情報を扱う領域

ポイント②：次期自治体情報セキュリティクラウドの在り方

次期「自治体情報セキュリティクラウド」の在り方

基本的な考え方

- 現行の自治体情報セキュリティクラウドは**セキュリティレベルに差**
  ⇒ **国が最低限満たすべき事項（標準要件）を提示**し、**民間ベンダがクラウドサービスを開発・提供**することにより、**セキュリティ水準の確保**と**コストの抑制**を実現
- 各団体の求める水準に応じて、オプション機能を柔軟に選択
- 可用性・コストを考慮し、接続回線（インターネット回線・専用線サービス等）を柔軟に選択
- 都道府県が主体となって構築することで市区町村を含めて情報セキュリティ対策が浸透、県と市町村間の連携が密になりインシデント対応や二次被害防止に効果
  ⇒ **引き続き、都道府県が主体となり調達・運営**し、市区町村のセキュリティ対策を支援（複数の都道府県の共同調達・運営も可）

サイバー攻撃の増加など新たな脅威や現行課題への対応による機能要件の追加

- 高度なセキュリティレベルを確保するため、**セキュリティ専門人材による監視機能（SOC）を強化**（仕様を統一）
- **災害時等のアクセス集中を想定した負荷分散機能（CDN）を追加**
- 暗号化された通信に対する監視機能を追加

その他のオプション機能

- 自治体事務の効率化に資するメールやファイルの無害化機能等をオプション機能として例示

今後の対応

○ 上記を踏まえ、**次期自治体情報セキュリティクラウドの在り方を決定**し、自治体へ通知
○ さらに、自治体の予算要求時期等を見据え、**技術的要件等の詳細を検討**し、自治体へ通知

ポイント③：昨今の重大インシデントを踏まえた対策強化

（１）情報システム機器の廃棄時におけるセキュリティの確保

発生した事案

✓ 昨年12月6日、神奈川県において、リース契約満了により返却したハードディスクの盗難による情報流出が発生

⇒ 同日、**当面の対応**として、重要情報が大量に保存された記憶装置については、**物理的な破壊又は磁気的な破壊の方法により行うとともに、地方公共団体の職員が当該措置の完了まで立ち会いを行うなど確実な履行の担保**を要請

再発防止策の概要

① **ワーキンググループでの検討結果を踏まえて**、情報システム機器を廃棄、リース返却等をする場合、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、**情報の機密性に応じた方法**により、**情報を復元困難な状態にする措置を徹底する必要がある**ことを助言

（参考）

分類	機器の廃棄の方法	廃棄の確認の方法
マイナンバー利用事務系に該当するもの	**①物理的な方法による破壊**（注）	**・職員による立ち会いによる確認 ・庁内において情報の復元が困難な状態までデータの消去を行った上で、物理的破壊の完了証明書の確認**
機密性２以上に該当するもの	①物理的な方法による破壊、②磁気的な方法による破壊、③ＯＳ等からのアクセスが不可能な領域も含めた領域をデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去　のうちいずれかの方法を選択	適切な方法による確認
機密性１に該当するもの	上記①～⑤の方法の他、⑥ＯＳ等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアによる上書き消去　のうちいずれかの方法を選択	適切な方法による確認

（注）リース契約による場合も、リース契約終了後、物理的破壊を行う旨、予め入札における仕様に明記の上、契約に位置付けることが望ましい。

② 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時に上記内容を記載

ポイント③：昨今の重大インシデントを踏まえた対策強化

（２）「Jip-Base」で発生した障害を踏まえた再発防止策

発生した事案

✓ 昨年12月4日、**日本電子計算株式会社が提供する地方公共団体向けクラウドサービス「Jip-Base」**に障害が発生し、**全国53団体453システム**に影響を与え、**その一部については、要介護認定、各種証明書の発行、ホームページの閲覧等に長期間の支障が発生**

✓ 障害原因は、①不具合の発生したストレージを利用していたシステムが利用不可になったこと、②一部データにアクセスできない状態が生じたこと、③一部のバックアップデータの取得不備

✓ **地方公共団体側の課題**として、**重要なシステムが重要度の低いシステムと同じサービスレベルで構築**されていること、**契約書に必要な事項が記載されていないこと**等について有識者から指摘

再発防止策の概要

① 地方公共団体への助言

✓ 地方公共団体に対し、**システムに求められるサービスレベルを十分に検討の上**、バックアップを含め、**必要なサービスレベルを保証させる契約締結の実施等を助言**

② クラウドサービス事業者への対応

✓ 地方公共団体を対象にクラウドサービスを展開する主な事業者に対し、自治体と同様の要請

①②を通じて、必要なサービスレベルについて、地方公共団体及びクラウドサービス事業者間の共通認識を醸成し、その内容を盛り込んだ契約の締結を促進

※ 今後、地方公共団体がクラウドサービスを安全に利用するための留意事項を整理し、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時に反映

ポイント④：各自治体の情報セキュリティ体制・インシデント即応体制の強化

○　各自治体の情報セキュリティ体制・インシデント即応体制の強化に向けて、現在、総務省及び地方公共団体情報システム機構が実施している以下の取組を着実に実施。

実践的サイバー防御演習（CYDER）の確実な受講

✓未受講の地方公共団体を中心とした計画的な受講の推進

インシデント対応チーム（CSIRT）の設置及び役割の明確化の推進

✓小規模自治体のためのCSIRT構築の手引きの作成
✓説明会の開催

演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有の推進

✓インシデント対応訓練（基礎・高度）
✓分野横断的演習

啓発や訓練を通じた各自治体の職員のセキュリティ・リテラシーの向上

✓リモートラーニングによる情報セキュリティ研修（eラーニング）
✓情報セキュリティ対策セミナー（集合研修）
✓情報セキュリティに関する技術講習会