自治体情報セキュリティ緊急強化対策について

～自治体情報セキュリティ対策検討チーム　中間報告～

総 務 省

平成２７年８月１２日（水）

総務省地域力創造グループ

主な論点

１．組織体制の再検討、職員の訓練等の徹底

（１）CISO・CSIRTの設置等
（２）インシデント連絡ルートの再構築（多重化）
（３）緊急時対応計画の見直しと緊急時対応訓練の逐次実施
（４）特に標的型攻撃に対する対策の徹底

２．インシデント即応体制の整備

（１）インシデント連絡ルートに沿って、都道府県による支援体制を再確認
（２）不正通信の監視機能の強化
（３）自治体情報セキュリティ支援プラットフォーム（仮称）の創設

３．インターネットのリスクへの対応

（１）安全性の確認
（２）システム全体の強靱性の向上
（３）自治体情報セキュリティクラウドの検討

４．総務省の役割

1．組織体制の再検討、職員の訓練等の徹底

（1）CISO・CSIRTの設置等

最高情報セキュリティ責任者（CISO）を設置し、その任務を明らかにするとともに、CISOを支え、自治体情報セキュリティ対策を推進するCSIRT等の組織を構築することが必要。

CSIRTとは、情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制
（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（H27.3改訂）より）

（2）インシデント連絡ルートの再構築（多重化）

各自治体のインシデント対応体制を再確認し、インシデント発生時の国までの連絡ルートを再構築（多重化）すること。

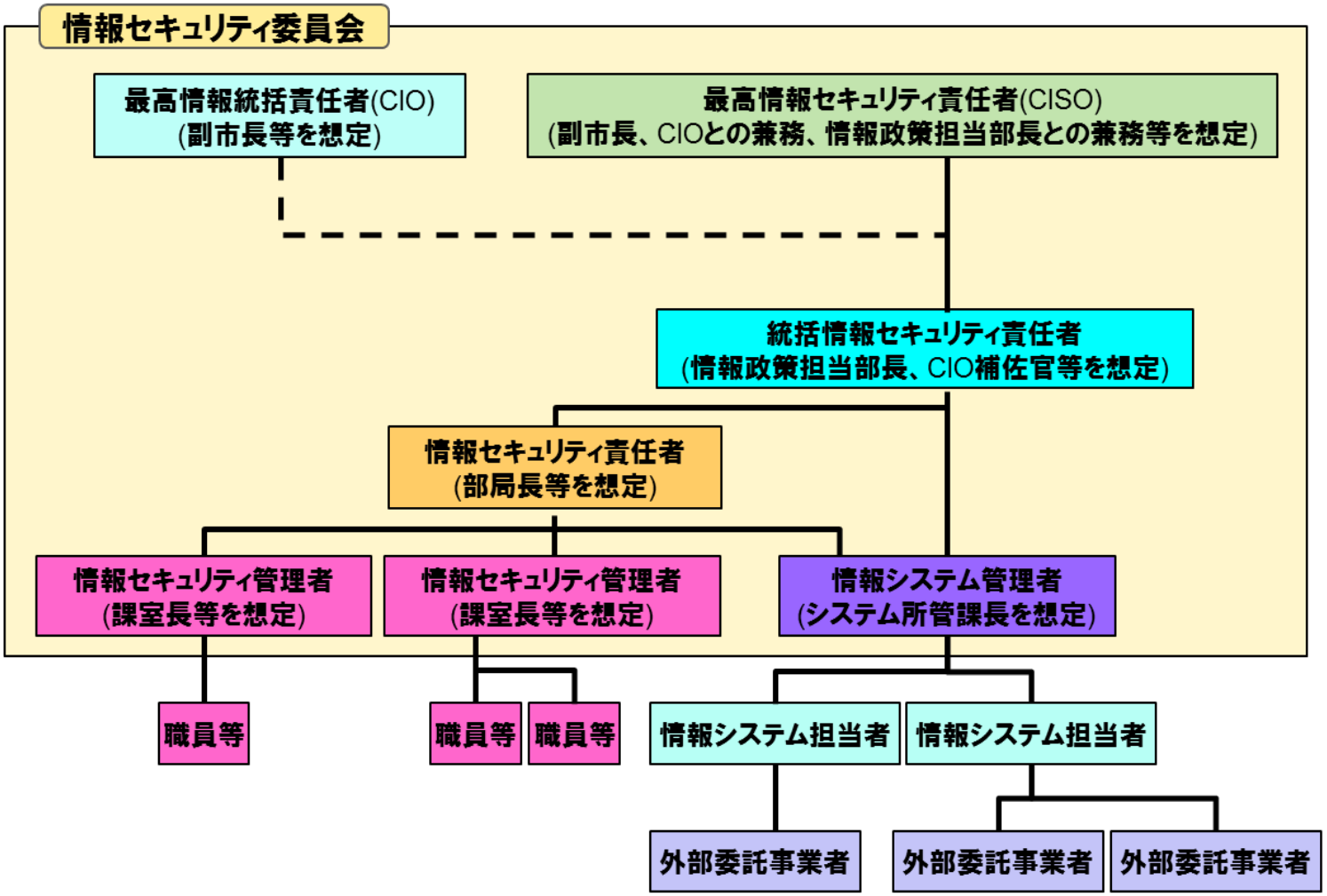
➡ 担当者レベルで直ちに対応できるようにルートを整備するとともに多重化を図ること

市区町村 ⟶（一斉同報）

- 都道府県
- 総務省
- 当該市区町村庁内
  （CISOまでの連絡ルートの整備を含む）

※　受理確認の徹底（特にメール、FAXの場合）

1の(1)参考　　情報セキュリティ推進の組織体制例



※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(H27.3改訂)より

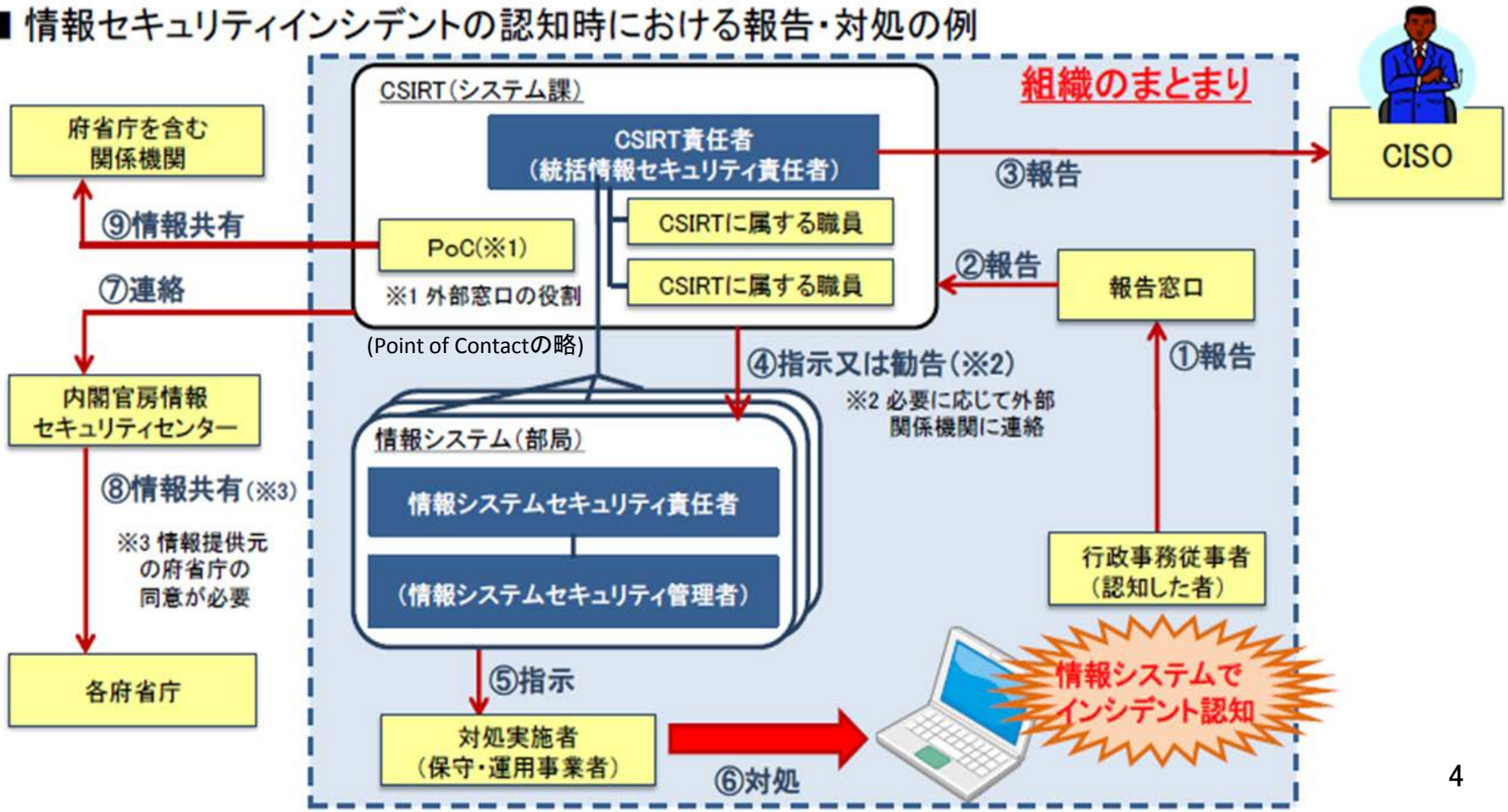
1の(1)参考
「政府機関の情報セキュリティ対策のための統一基準群(平成26年度版)について」より

2．2．4　情報セキュリティインシデントへの対処　［参考］

■ CSIRTとは

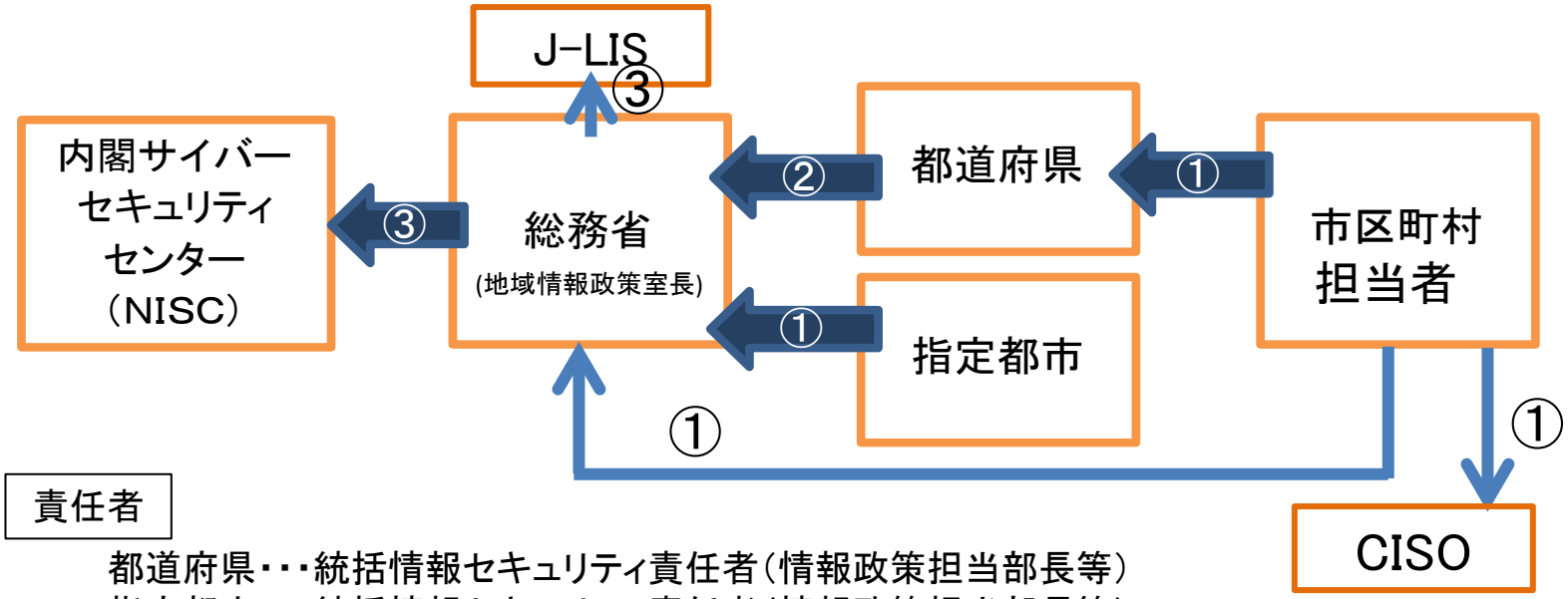
Computer Security Incident Response Teamの略。
府省庁の情報システムに対する情報セキュリティインシデントが発生した際に、当該府省庁が発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等ををを迅速かつ的確に行うことを可能にするための機能を有する体制

■ 情報セキュリティインシデントの認知時における報告・対処の例



1の(2)参考　インシデント連絡フロー

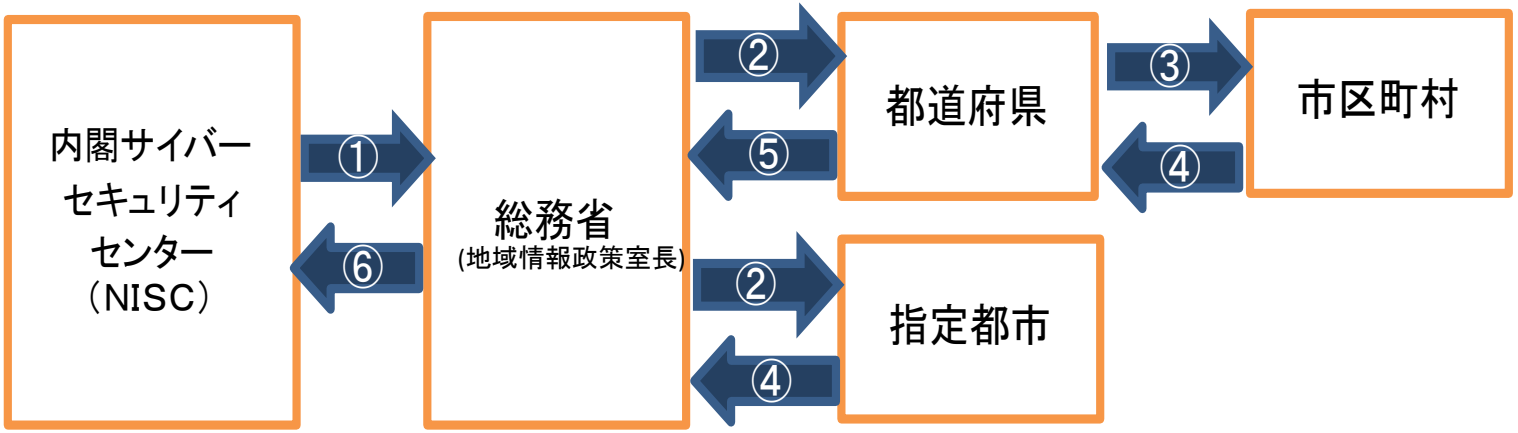
○各地方公共団体が検知したインシデントの選択ルートについて



責任者

都道府県・・・統括情報セキュリティ責任者（情報政策担当部長等）
指定都市・・・統括情報セキュリティ責任者（情報政策担当部長等）
市区町村・・・統括情報セキュリティ責任者（情報政策担当部長等）

（参考）NISCが検知したインシデントの選択ルートについて



1．組織体制の再検討、職員の訓練等の徹底

（3）緊急時対応計画の見直しと緊急時対応訓練の逐次実施

特に標的型攻撃に対する緊急時対応計画の見直しと緊急時対応訓練の逐次実施（都道府県単位、全国訓練）

※　標的型攻撃への対応（例）

必要な連絡を行う
プロキシサーバをチェックし、外部への不審な通信を事案発覚後6時間以内に調査

（1）検査できない場合
- ○ 外部へのWebアクセス及びPCからのメール送受信を遮断（ネット遮断）
- ○ セキュリティ事案対処専門家と共に対応

（2）検査できて不審な通信が1台のPCから行われている
- ○ PCの隔離　※
- ○ 引き続き不審な通信の監視を続ける

（3）検査できて不審な通信が2台以上のPCから行われている
- ① 外部へのWebアクセス及びPCからのメール送受信を遮断（ネット遮断）
- ② 不審なアクセスが、人間の操作に起因するものかを確認
  - ○ 人間による操作で、不審なサイトへ誘導されたもので、ウイルス感染ではないことが確定された場合、ネット遮断を解除し緊急体制を解除

1.　組織体制の再検討、職員の訓練等の徹底

※　標的型攻撃への対応（例）　（続）

（3）検査できて不審な通信が2台以上のPCから行われている（続）

③ 不審なアクセスが、ウイルスによるものと疑われる場合

○ PCの隔離 ※

○ AD（Active Directory）のログを確認して、人間以外のログオン（成功・失敗）を検査

（不審なログオンが発見された場合）

・管理者権限の不正アクセスが見つかった場合

→LANを停止させ、セキュリティ事案対処専門家と共に対応

・管理者権限ではなかった場合

→PCの隔離　※

○ 感染範囲特定のできるセキュリティ事案対処専門家と共に対応

○ 感染範囲の特定・除去ができたと合理的に判断できた場合、ネット遮断を解除する

※ PCの隔離手順

・ 調査の妨げになるのでウイルスワクチンによるスキャンは行わないこと

・ 対象PCの電源断（バッテリーを抜くかコンセントを抜く、分からない場合には電源ボタンの長押し（LANケーブルの抜線よりも先に行うこと））

1.　組織体制の再検討、職員の訓練等の徹底

（4）特に標的型攻撃に対する対策の徹底

入口対策

① 注意喚起（不審なメールは届ける）
② 訓練メール

内部対策

① AD（Active Directory）ログの定期的確認
- 管理者端末以外からの管理者ログオンの成功/失敗
- ユーザ端末からのログオンの失敗

② 管理者端末でのメール、Webブラウザ使用禁止

出口対策

○ 不審な通信の確認（プロキシログ）

1の(4)参考
「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(H27.3改訂)」より

～ 3．6．5不正アクセス対策 ～

(7) 標的型攻撃

標的型攻撃による外部から庁内への侵入を防ぐため、標的型攻撃メール受信時の人的対策のほか、電磁的記録媒体やネットワークに対する技術的対策についても次の例のような対策を行うこと。また、これらの対策が適切に実施されているかをモニタリングし、確かめる必要がある。なお、対策の検討にあたっては、「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」(平成26年6月26日　情報セキュリティ対策推進会議)及び「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」(平成26年6月25日　内閣官房情報セキュリティセンター)も参照されたい。

① 人的対策例(標的型攻撃メール対策)

- 差出人に心当たりがないメールは、たとえ興味のある件名でも開封しない。
- 不自然なメールが着信した際は、差出人にメール送信の事実を確認する。
- メールを開いた後で標的型攻撃と気付いた場合、添付ファイルは絶対に開かず、メールの本文に書かれたURLもクリックしない。
- 標的型攻撃と気付いた場合、システム管理者に対して着信の事実を通知し、組織内への注意喚起を依頼した後に、メールを速やかに削除する。
- システム管理者は、メールやログを確認し、不正なメールがなかったかチェックする。
(事後対策)

1の（4）参考
「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（H27.3改訂）」より

～３．６．５不正アクセス対策～（続）

（7） 標的型攻撃

② 電磁的記録媒体に対する対策例

- 出所不明の電磁的記録媒体を内部ネットワーク上の端末に接続させない。
- 電磁的記録媒体をパソコン等の端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。
- パソコン等の端末について、自動再生（オートラン）機能を無効化する。
- パソコン等の端末について、電磁的記録媒体内にあるプログラムを媒体内から直接実行することを拒否する。

③ ネットワークに対する対策例

- ネットワーク機器のログ監視を強化することにより、情報を外部に持ち出そうとするなどの正常ではない振る舞いや外部との不正な通信を確認し、アラームを発したりその通信を遮断する。
- 不正な通信がないか、ログをチェックする。（事後対策）

２．インシデント即応体制の整備

（１）インシデント連絡ルートに沿って、都道府県による支援体制を再確認

特に、都道府県については、市町村等におけるインシデント発生時において、インシデント即応体制の主体として事案対処に当たることが期待される。

このため、予め各都道府県ごとに、都道府県CSIRTと市町村CSIRTの連携体制を構築しておくことが必要。

2. インシデント即応体制の整備

（2）不正通信の監視機能の強化

アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を点検

① 全自治体において、プロキシログを収集・保存し、疑わしきものをフィルタリングする等の対策を実施することを検討すべき。

② 各都道府県において、当該都道府県庁及び市町村のプロキシログの疑わしきものを収集・保存・分析を行う対策を実施することを検討すべき。

監視デバイス	監視の対象と手法	ツール例	人による分析要否
プロキシサーバ/webフィルタ （出口対策）	外部への通信ログを収集	BlueCoat SG、McAfee Email and Web Security、i-Filter	必要 ・外部レピュテーションとの突合 ・既知マルウェアと類似したアクセスパターンの検出

※その他サンドボックス、仮想ブラウザ等のツールもある。

2. インシデント即応体制の整備

（3）自治体情報セキュリティ支援プラットフォーム（仮称）の創設

次のような機能を有する自治体情報セキュリティ支援プラットフォーム（仮称）を構築し、運用しながら、都道府県のインシデント即応能力の継続的向上を図る仕組みを導入すべき。

①インシデント関連掲示板により、インシデント情報を共有

- 自治体情報セキュリティに関する情報を掲載。
  過去に発生したインシデント事例等の紹介

②情報セキュリティQ&Aにより、自治体の喫緊の課題に対応

- Q&Aのサマリー情報掲載。
  （他自治体の詳細を参照したい場合は、参照依頼を行い、投稿した自治体がOKの場合に参照可能とする）

サマリーを転記

- 問診表にて相談を投稿。
- 予め登録された情報セキュリティ専門人材からの回答
- メール通知機能
  （情報セキュリティ専門人材・自治体へ通知）

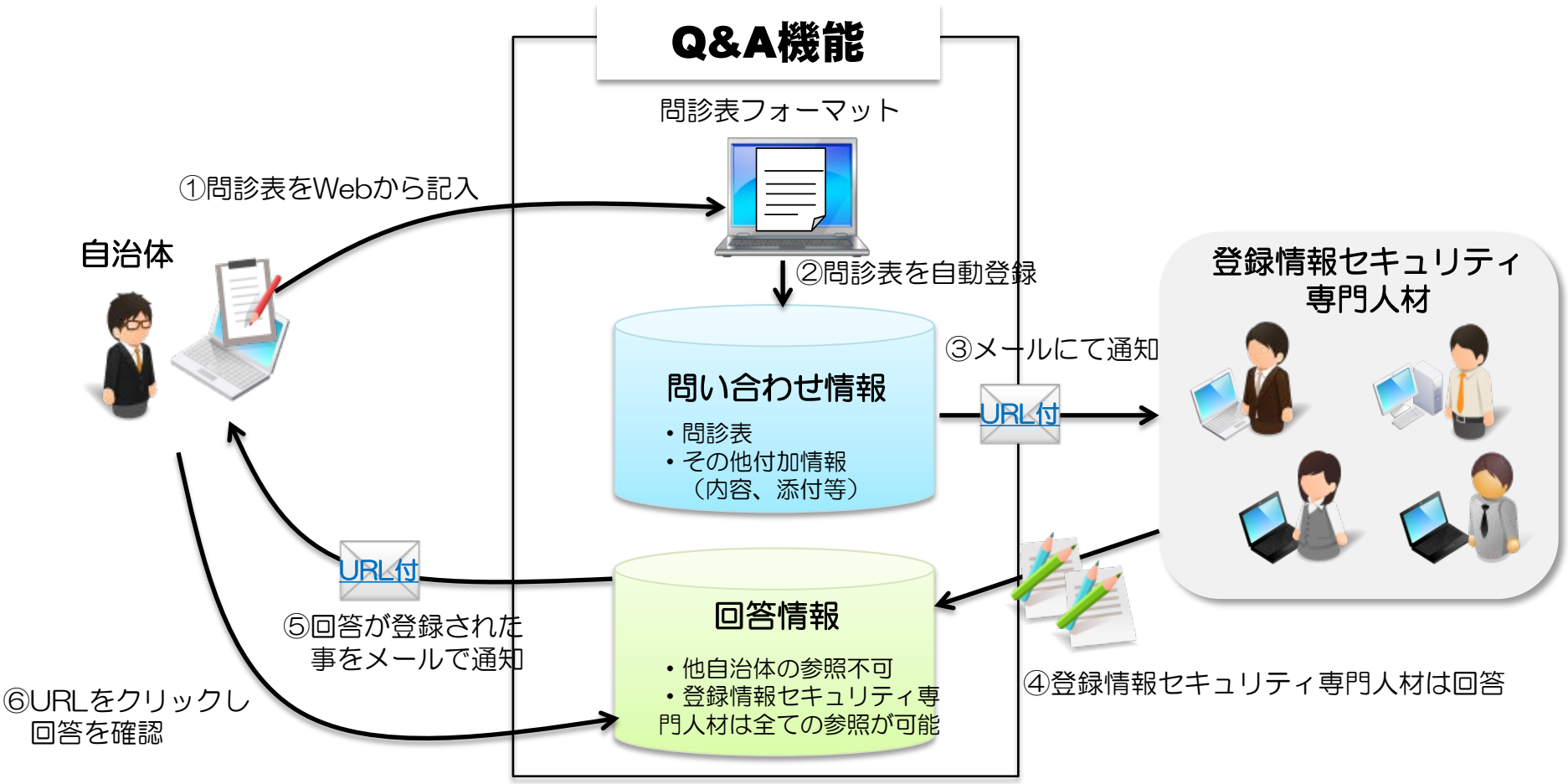
③ワーキンググループの組成（情報セキュリティ専門人材から構成）

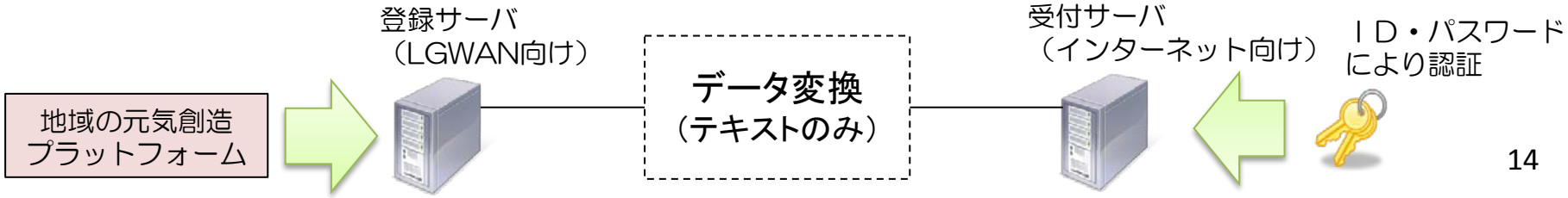
- インシデント初動マニュアルや対処訓練マニュアル等を作成の上、自治体に提供

④その他関連情報の提供

- 自治体情報セキュリティの関連情報
- その他情報

自治体情報セキュリティ支援プラットフォーム（仮称） Q&A機能の概要





３　インターネットのリスクへの対応

（１）安全性の確認

マイナンバー制度が施行されるまでに、庁内の住民基本台帳システム（既存住基）がインターネットを介して不特定の外部との通信を行うことができないようになっていることを確認することが望まれる。

（２）システム全体の強靱性の向上

情報提供ネットワークシステムの稼働を見据え、機密性はもとより、可用性や完全性の確保にも十分配慮された攻撃に強い内部ネットワーク等の構築を図ることが望まれる。

（３）自治体情報セキュリティクラウドの検討

自治体における不正通信の監視機能の強化等への取組に際し、より高い水準のセキュリティ対策を講じるため、インターネット接続ポイントの集約化やセキュリティ監視の共同利用等（自治体情報セキュリティクラウド）の検討を進めるべき。

4. 総務省の役割

本中間報告が指摘する「自治体情報セキュリティ緊急強化対策」を自治体が円滑に実施できるよう、必要な措置を講じることが総務省に期待される。

自治体情報セキュリティ対策検討チーム

【構成員】（敬称略）

	上原　哲太郎	立命館大学情報理工学部情報システム学科　教授
	岡村　久道	弁護士　国立情報学研究所客員教授
（座長）	佐々木　良一	東京電機大学未来科学部教授 （内閣官房サイバーセキュリティ補佐官）
	三輪　信雄	総務省最高情報セキュリティアドバイザー
	原田　智	京都府政策企画部情報政策統括監
	大高　利夫	藤沢市総務部参事兼ＩＴ推進課長
	佐野　茂樹	上田市総務部広報情報課係長

【開催状況】

第１回会合　平成27年７月９日（木）
第２回会合　平成27年８月３日（月）
第３回会合　平成27年８月12日（水）