資料６－２
※一部非公開※

ICTサイバーセキュリティ政策分科会

地方自治体情報セキュリティの現状

2024年4月26日

合同会社KUコンサルティング
髙橋　邦夫

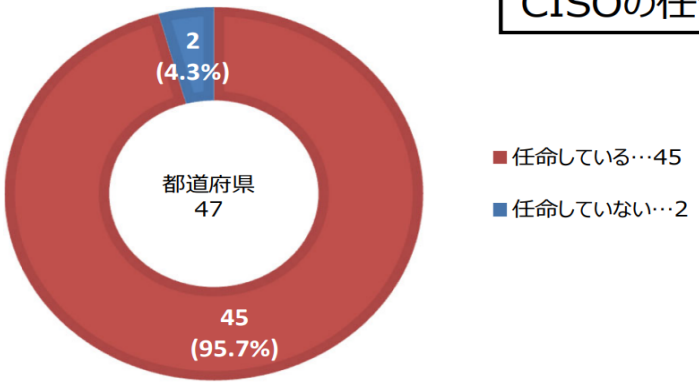
統計からは万全に見えるが・・

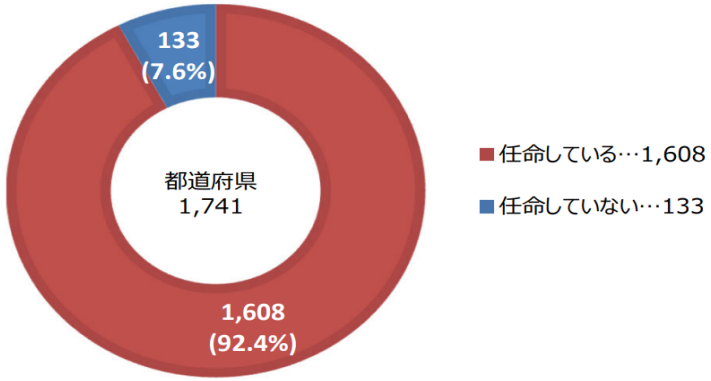
① 組織体制・規程類の整備

1 CISOの任命

都道府県では45団体（95.7%）、市区町村では1,608団体（92.4%）がCISOを任命している。
また、任命している団体のうち、役職の内訳及び外部デジタル人材の任用の有無は次のとおりである。

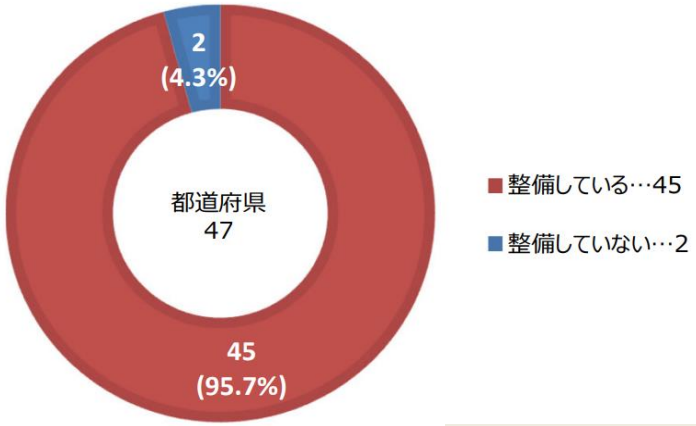
CISOの任命

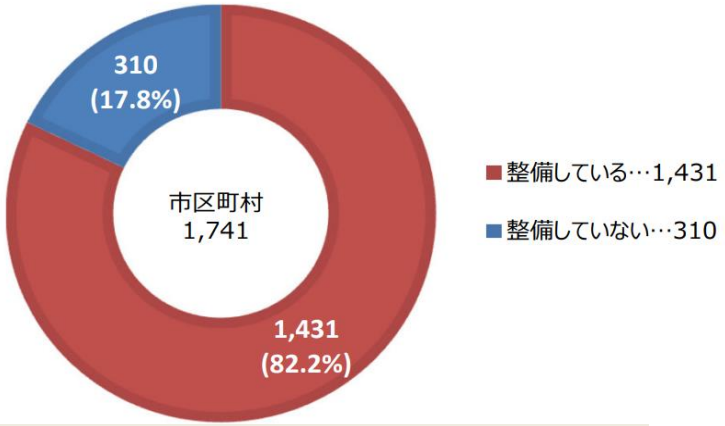




2 CSIRT（情報セキュリティインシデントに対処するための体制）の整備

都道府県では45団体（95.7%）、市区町村では1,431団体（82.2%）が整備している。





「自治体DX・情報化推進概要」令和4年度調査結果より

CSIRTについては必ずしも自治体規模に比例ではない

（2）人口段階別（市および特別区。指定都市を除く。）　（　）内数字は%

	団体数	CSIRT(情報セキュリティインシデントに対処するための体制）を整備している
５０万人以上	15	14(93.3)
４０万～５０万人未満	21	19(90.5)
３０万～４０万人未満	29	27(93.1)
２０万～３０万人未満	47	41(87.2)
１０万～２０万人未満	149	133(89.3)
５万～１０万人未満	246	201(81.7)
５万人未満	288	243(84.4)
合　　計	795	678(85.3)

（3）人口段階別（町村）　（　）内数字は%

	団体数	CSIRT(情報セキュリティインシデントに対処するための体制）を整備している
５万人以上	2	2(100.0)
４万～５万人未満	18	11 (61.1)
３万～４万人未満	45	31 (68.9)
２万～３万人未満	78	64 (82.1)
１万～２万人未満	264	213 (80.7)
５千～１万人未満	230	182 (79.1)
５千人未満	289	230 (79.6)
合　　計	926	733 (79.2)

（2）人口段階別（市および特別区。指定都市を除く。）　（　）内数字は%

	団体数	情報セキュリティ対策の監査・点検			
		情報セキュリティについて内部監査のみを実施している	情報セキュリティについて外部監査のみを実施している	情報セキュリティについて内部監査及び外部監査を実施している	情報セキュリティポリシー等の遵守状況について、自己点検を実施している
５０万人以上	15	7(46.7)	1(6.7)	6(40.0)	12(80.0)
４０万～５０万人未満	21	8(38.1)	2(9.5)	11(52.4)	16(76.2)
３０万～４０万人未満	29	19(65.5)	1(3.4)	7(24.1)	22(75.9)
２０万～３０万人未満	47	27(57.4)	2(4.3)	9(19.1)	32(68.1)
１０万～２０万人未満	149	68(45.6)	14(9.4)	22(14.8)	102(68.5)
５万～１０万人未満	246	104(42.3)	23(9.3)	32(13.0)	139(56.5)
５万人未満	288	130(45.1)	9(3.1)	17 (5.9)	140(48.6)
合　　計	795	363(45.7)	52(6.5)	104(13.1)	463(58.2)

（3）人口段階別（町村）　（　）内数字は%

	団体数	情報セキュリティ対策の監査・点検			
		情報セキュリティについて内部監査のみを実施している	情報セキュリティについて外部監査のみを実施している	情報セキュリティについて内部監査及び外部監査を実施している	情報セキュリティポリシー等の遵守状況について、自己点検を実施している
５万人以上	2	0 (0.0)	0 (0.0)	2(100.0)	1(50.0)
４万～５万人未満	18	7(38.9)	2(11.1)	2 (11.1)	8(44.4)
３万～４万人未満	45	18(40.0)	2 (4.4)	1 (2.2)	23(51.1)
２万～３万人未満	78	30(38.5)	4 (5.1)	3 (3.8)	39(50.0)
１万～２万人未満	264	108(40.9)	13 (4.9)	6 (2.3)	137(51.9)
５千～１万人未満	230	110(47.8)	6 (2.6)	7 (3.0)	115(50.0)
５千人未満	289	121(41.9)	9 (3.1)	11 (3.8)	139(48.1)
合　　計	926	394(42.5)	36 (3.9)	32 (3.5)	462(49.9)

「自治体DX・情報化推進概要」令和4年度調査結果より

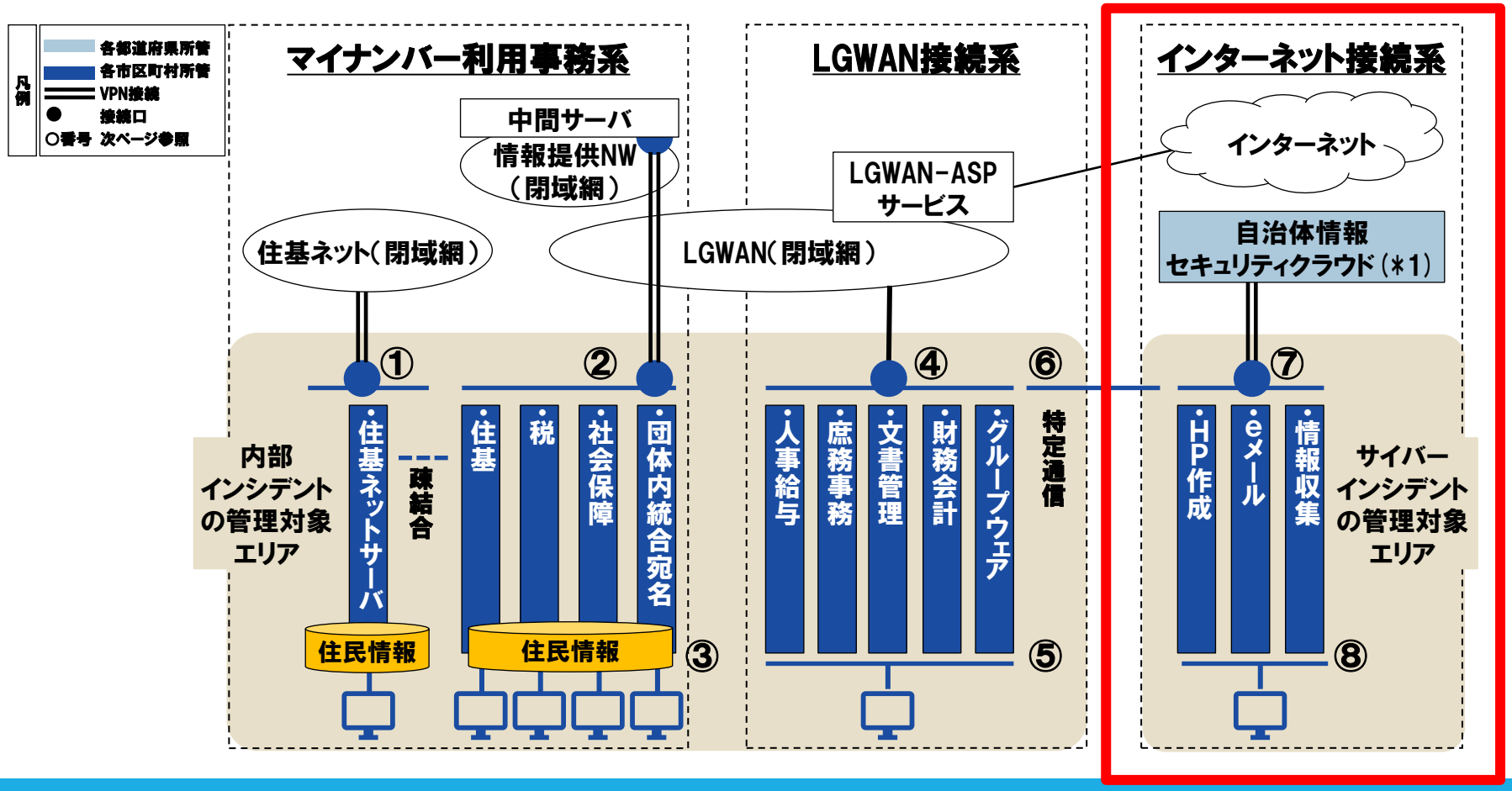
完全防御は幻想
検知後にどう対応するか

- 「防御」は時間稼ぎ
- いかに攻撃（被害）を見つけるか
- 見つけた後、どう動くか（報告・連携）

「起きた」とき、組織の内外で様々な連携が必要となる。

■ インターネット接続系

- 公開系のホームページがサイバー攻撃（DDoS、SQLインジェクション等）を受けることもある。
- 業務データは残さない前提でも、漏洩により影響が生じる情報が全くない状況が常に保たれていると言えるか

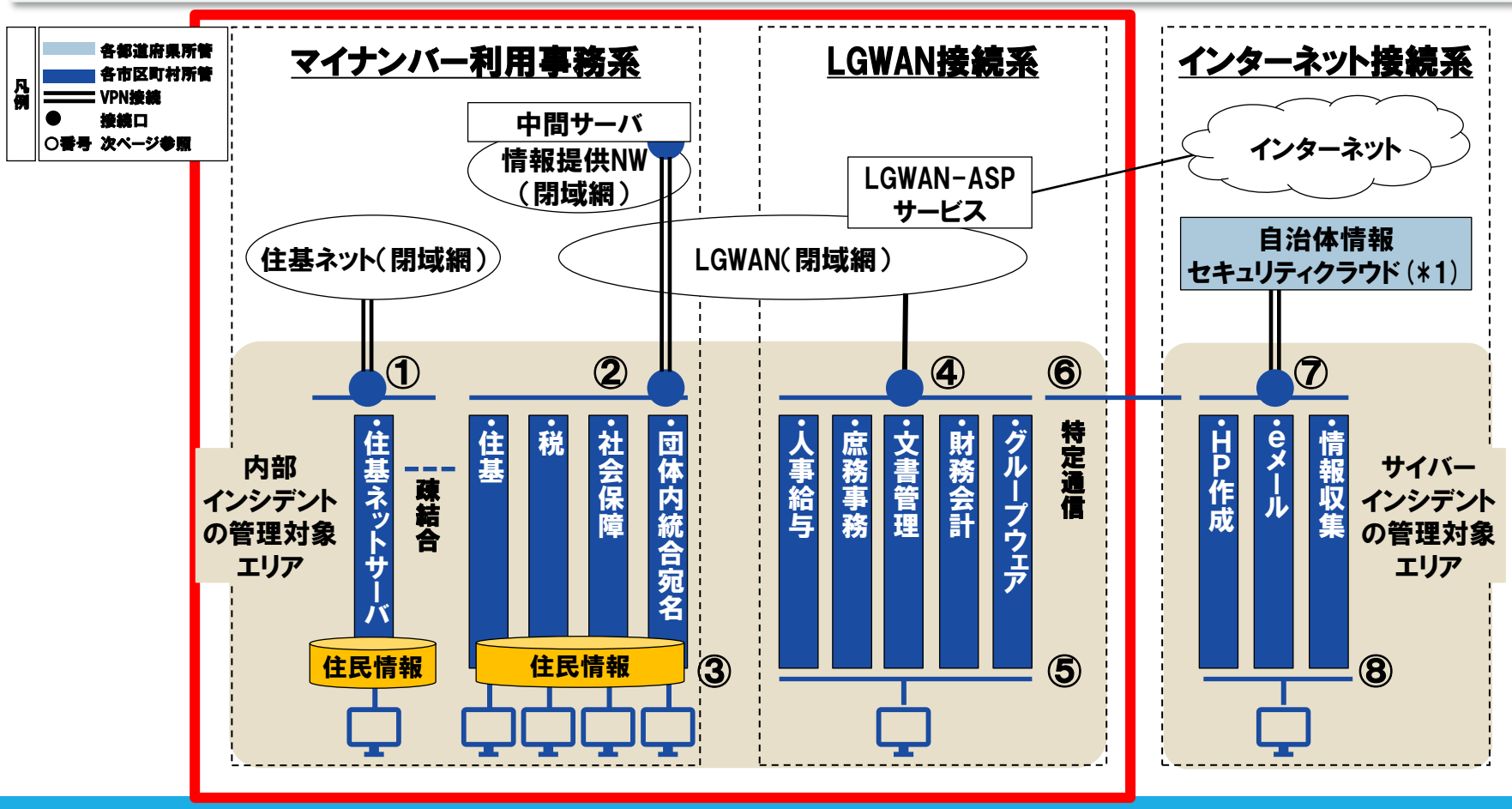


■ LGWAN接続系

インターネット接続系とは分割され、無害化通信によるファイルの切り離しが行われているが、データ通信が全く発生しない訳ではない（ファイル転送や媒体によるデータの移出入はある）

■ マイナンバー利用事務系

- 外部ネットワークからの攻撃に対して強固であっても、媒体によるデータの移出入やクラウドサービス利用など、別の経路からの情報漏えいやマルウェア感染、データ滅失等の可能性は十分有り得る。
- 扱っている情報の性質上、セキュリティインシデント発生時は即時対応が求められる。



内部職員の「過失」による事故は依然として多い

- 個人情報の漏えいに関しては、メール誤送信や紛失等、人為的ミスによる漏えいが依然として多い
- 増加傾向にある

原因			2021	2020	2019
漏えい	誤送付	宛名間違い等	353	314	400
		封入ミス	333	323	329
		配達ミス	0	137	58
		メール誤送信	**1128**	764	590
		FAX誤送信	124	110	136
	その他		570	454	446
紛失・盗難	紛失		380	394	421
	盗難	車上荒し	4	5	5
		置き引き等	14	3	6
その他			142	140	152
合計			3,048	2,644	2,543

JIPDEC　プライバシーマーク推進センター　2021年度「個人情報の取り扱いにおける事故報告集計結果」より引用

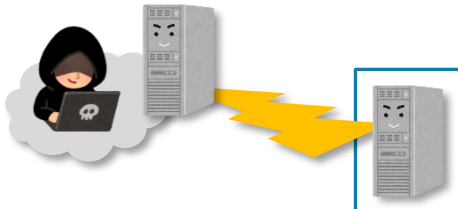
内部職員の「過失」による事故は依然として多い

（注１３）一般的に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を CSIRT と呼ぶ。CSIRT の持つ機能や在り方は組織によって様々であるが、まずは、地方公共団体においては情報セキュリティに関する統一的な窓口の機能を有する体制を整えることが重要である。

※「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（令和5年3月版）」より引用

サイバー攻撃に限らず、情報セキュリティの統一的な窓口として求められる自治体「CSIRT」

連絡窓口が明確になっていないことによる困った実例



通報機関

そちらのサーバがC&Cサーバと通信していることを確認…

どなたかITのわかる方に繋いで頂けないでしょうか…

インシデント連絡窓口不明のため代表電話に連絡（ITとは関係ない、企画系の担当につながる）

何かのいたずらと認識されてしまう…

何度か連絡するも、取り合ってもらえず

被害団体

シーアンド？不正？何？そもそも誰？怪しい電話…

しつこい迷惑電話だった～

放置

きちんと情報を受け取ってもらえるまで、数か月の期間を要してしまった…

そのような事態を防ぐためには…

セキュリティインシデントに関する情報の一元化と、
インシデント対応の即応体制を実現する「CSIRT」の
運用が有用である。

**インシデント情報の一元化、適切な対応を行うため、
情報セキュリティの統一的な窓口として
「CSIRT」の整備・活動の有効化を目指しましょう！**

CSIRT構築･運用の流れ

フェーズ１　CSIRTの設置

① 検討チームの立ち上げ

② 設置に向けた検討

③ 設置作業の実施

フェーズ２　CSIRT運用の準備

① 必要な情報の確認

② 監視連絡体制等の整備

③ 訓練の実施

必要な情報の確認　～常に最新の状態を維持するもの～

必要な情報	内容
インシデントに係る注意喚起情報	J-LISが注意喚起等の緊急連絡を掲載する「情報セキュリティ支援サイト」(LGWAN)を毎日確認する。 また、同情報を配信するLASCセキュリティ情報提供メール（J-LISからの情報提供メール）に自団体のPoCメールアドレスを登録する。
インシデントへの対応の連絡先	人事異動や組織改編、外部委託事業者や外部の専門家の変更等、必要に応じて見直し、最新の状態を保つ。
外部委託事業者への依頼内容	インシデント発生に際して、外部委託事業者（システムベンダー等）に依頼できる作業内容と責任の範囲を確認、明文化。
関連する規程類	インシデント対応に係る実施手順、団体内部及び外部機関への報告様式類等、インシデント対応時に参照、利用する可能性のある規程類が最新版か確認。
業務システム・ネットワークの構成	組織全体の業務システム・ネットワーク概要図、体制図を整備。個別のシステム構成図、ネットワーク構成図についても、常に最新化されていることを確認、把握しておく。
ログ	重要情報へのアクセス履歴、その他システムログ等の証跡が適切に取得され、保全されていることを確認する。

自治体情報セキュリティで大事なこと

情報のデジタル化はセキュリティレベル向上

報道がなされている事件・事故はアナログ
＝＞　多くが人為的ミスか紙・媒体での情報漏えい

情報をデジタル化することで、対策が増える
＝＞　誰が、いつ、どこから情報を見たのかが判明
＝＞　暗号化・パスワードなど複数の方法で守れる
（許された者だけが情報にアクセス）

本人の情報は本人が確認できる（守れる）

自治体DX推進と情報セキュリティ

DXを進めることで、セキュリティレベルを上げる

○　業務改革と情報セキュリティはセット
＝＞　セキュリティ事故、事件を防ぐため手法を変える
＝＞　複数の人間がチェックする体制は限界に

○　人でなくても出来ることをDXで実現する
＝＞　人間が介在することでミスは発生する
＝＞　AIやRPAを利用して極力人の介在を減らす
＝＞　そもそも作業が必要か、自動化することが大事