「自治体の情報セキュリティ対策と情報の共有について」

重要インフラ情報セキュリティフォーラム2008
H20. 2. 20(水)　秋葉原コンベンションホール

石川家継 (ishikawa@lasdec.or.jp)

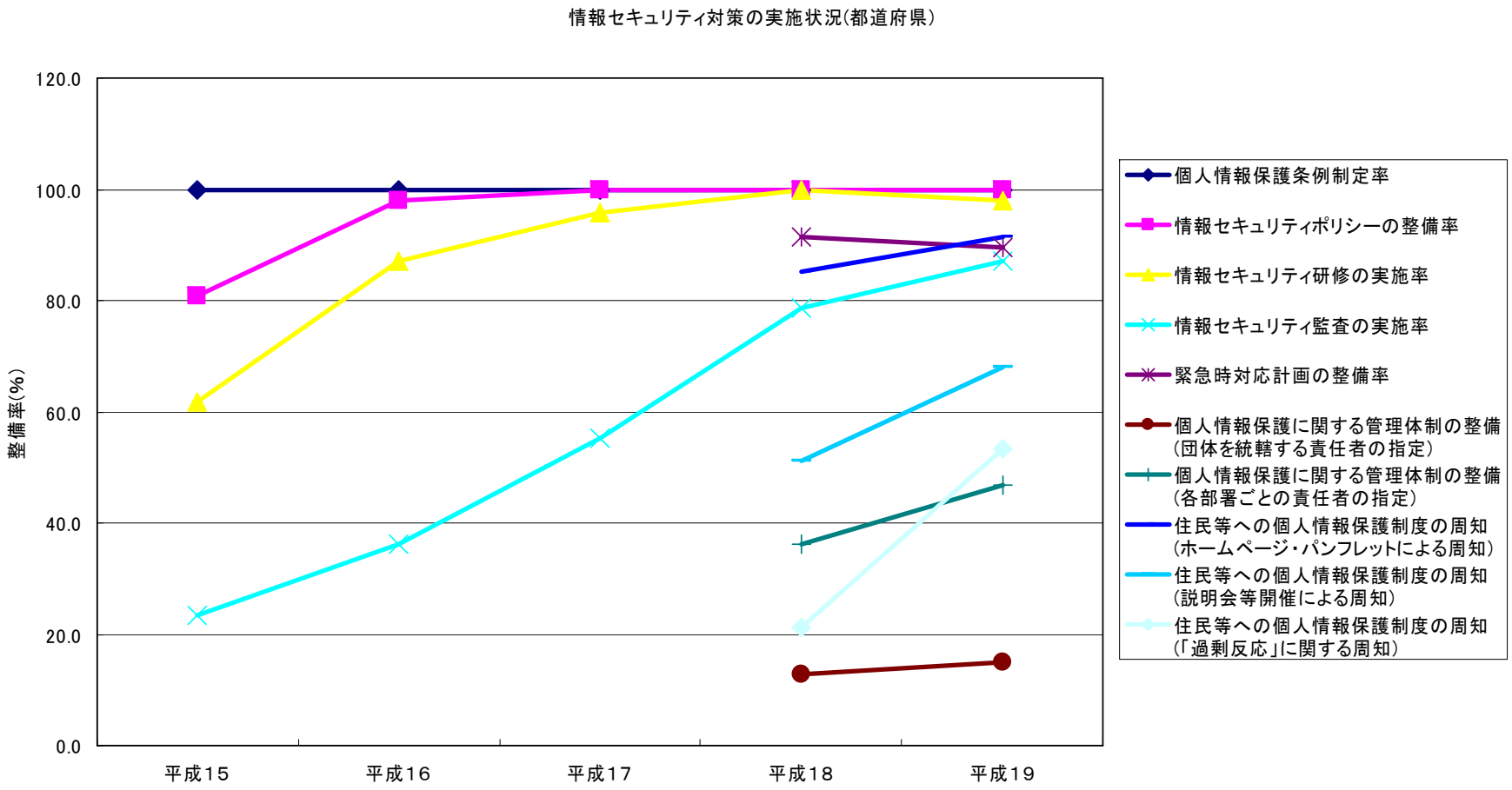
(財)地方自治情報センター
http://www.lasdec.nippon-net.ne.jp/
LASDEC(Local Authorities Systems Development Center)
自治体セキュリティ支援室
（LASC：ラスク）Local Authorities Security Support Center

本日の説明項目

- 自治体における情報セキュリティ対策の現状
  - 情報セキュリティ対策の実施状況
  - 情報セキュリティ関連事故(上半期)
- セキュリティ支援事業の概要
  - 情報セキュリティ遠隔診断
  - ウェブアプリケーション脆弱性診断
  - 情報セキュリティ内部監査を支援するアドバイザーの派遣
  - LGWAN-ASPを活用した情報セキュリティ支援事業（IDSによる庁内～インターネット監視）
  - 人材育成　等
- 事例紹介
  - 事故事例、優良事例
- セキュリティ情報の共有

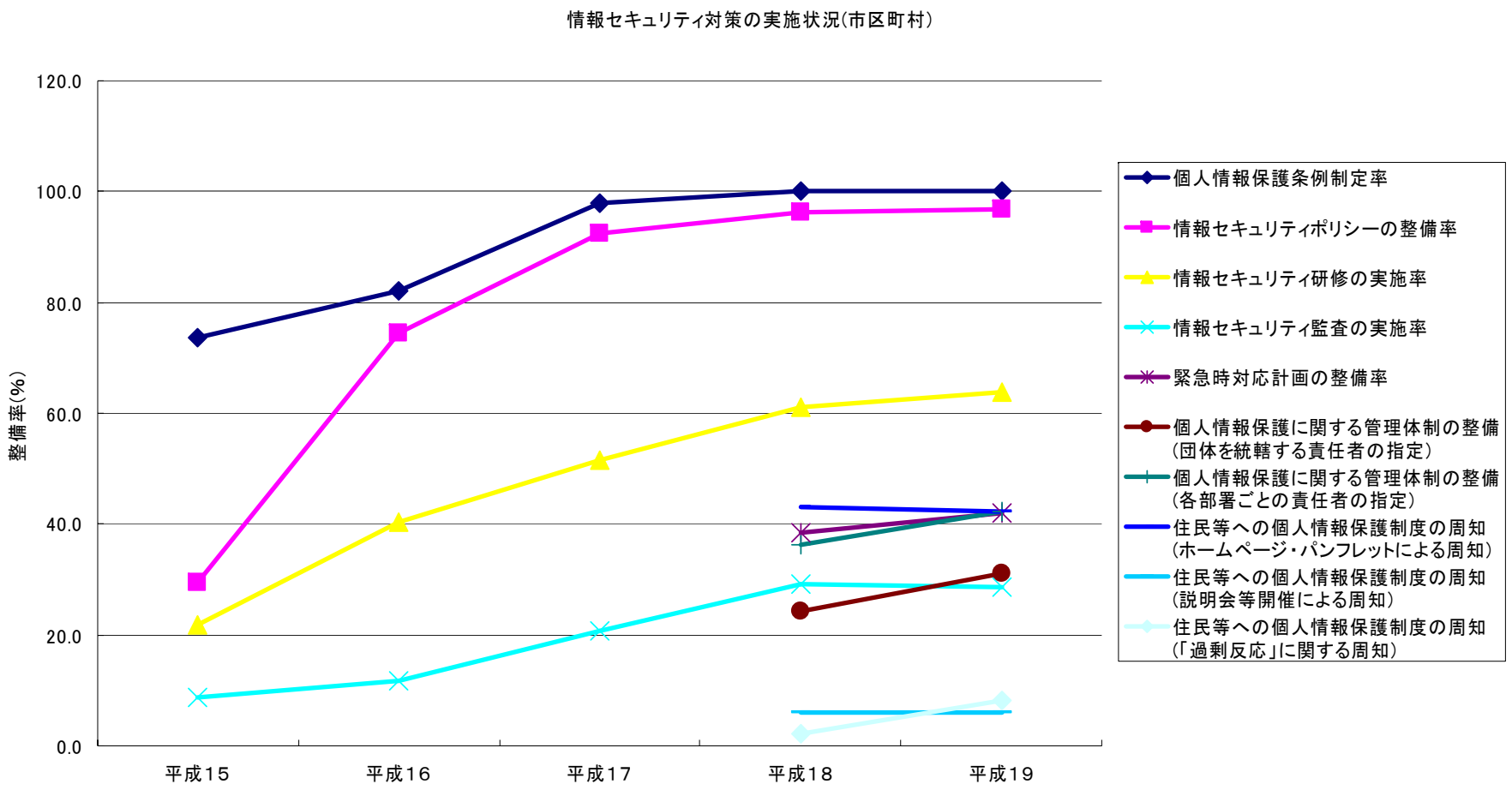
自治体における情報セキュリティ対策の現状

情報セキュリティ対策の実施状況(都道府県)



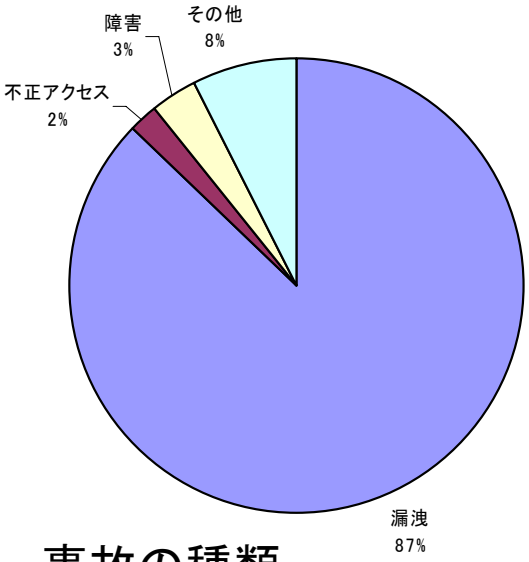
(H19.4.1現在　総務省調査)

情報セキュリティ対策の実施状況 (市区町村)



(H19.4.1現在　総務省調査)

情報セキュリティ関連事故等(19年度上半期)

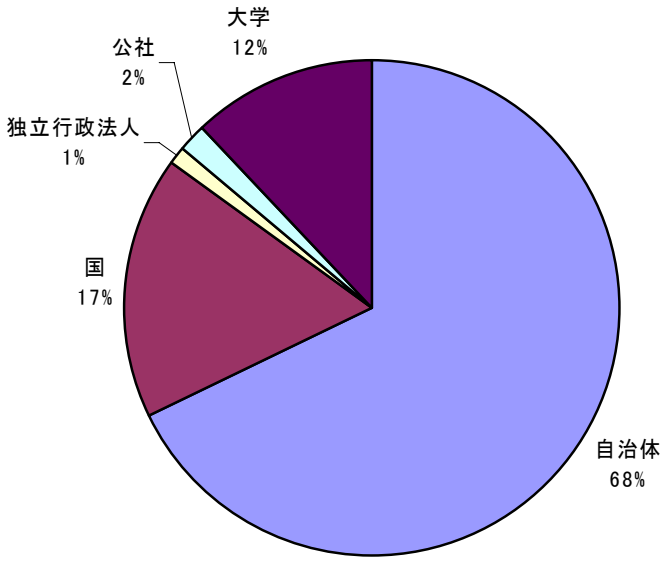


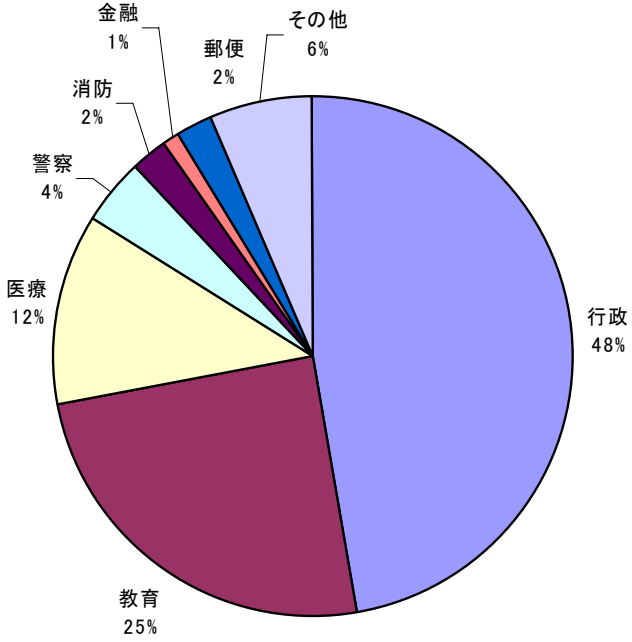
事故の種類

19.4.1から9.30までの上半期に起きた情報セキュリティ事故(公共部門)

合計は93件(自治体セキュリティ支援室調)

事故の団体





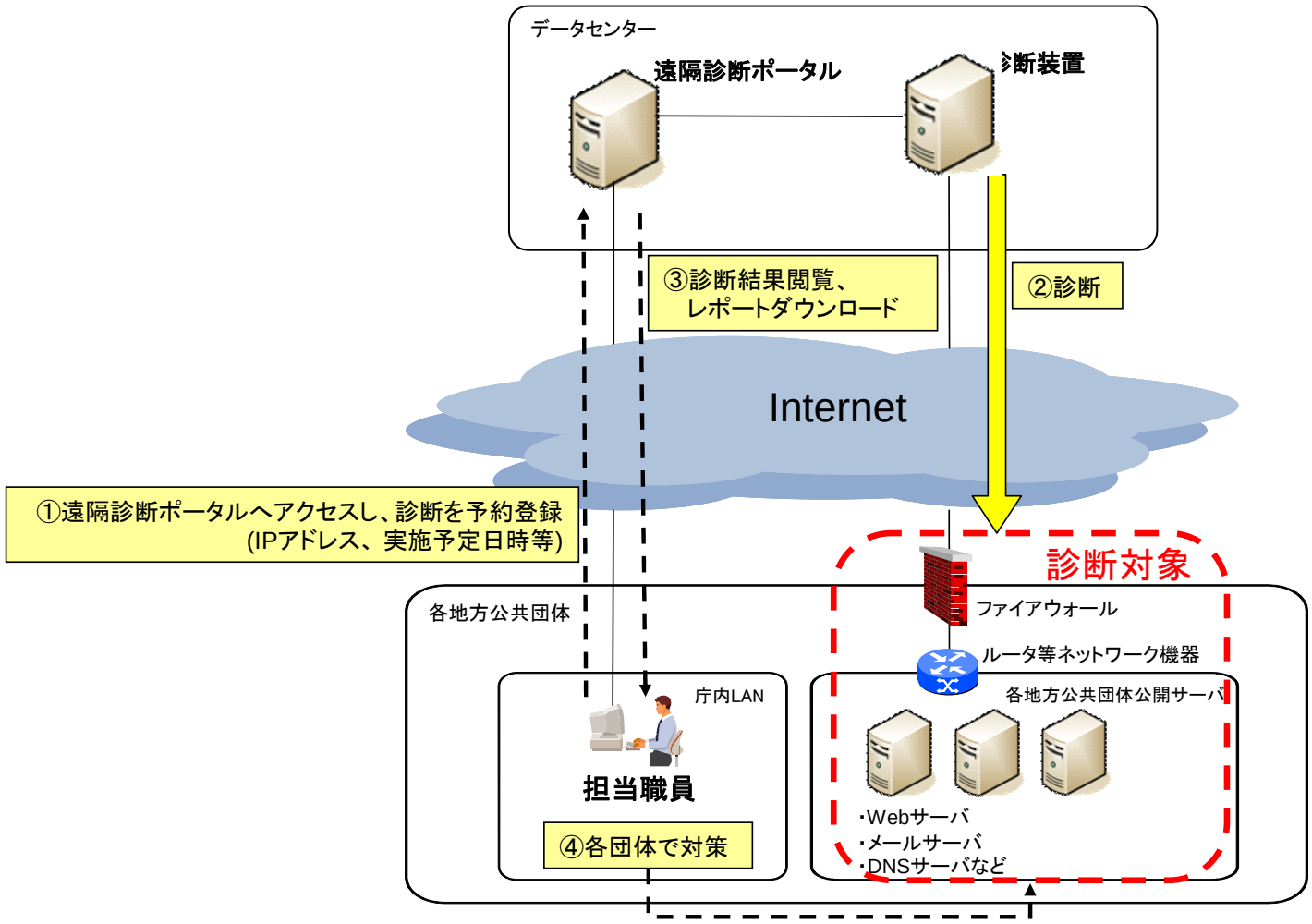
事故の種別

セキュリティ支援事業の概要

情報セキュリティ遠隔診断

- 対象：Webサーバ、メールサーバ及びネットワーク機器等
- インターネットから対象機器を遠隔診断
- わかりやすい診断結果レポートの提供
- セキュリティホールの発見と是正策の提供
- 遠隔診断結果レポート説明会の開催(試行)

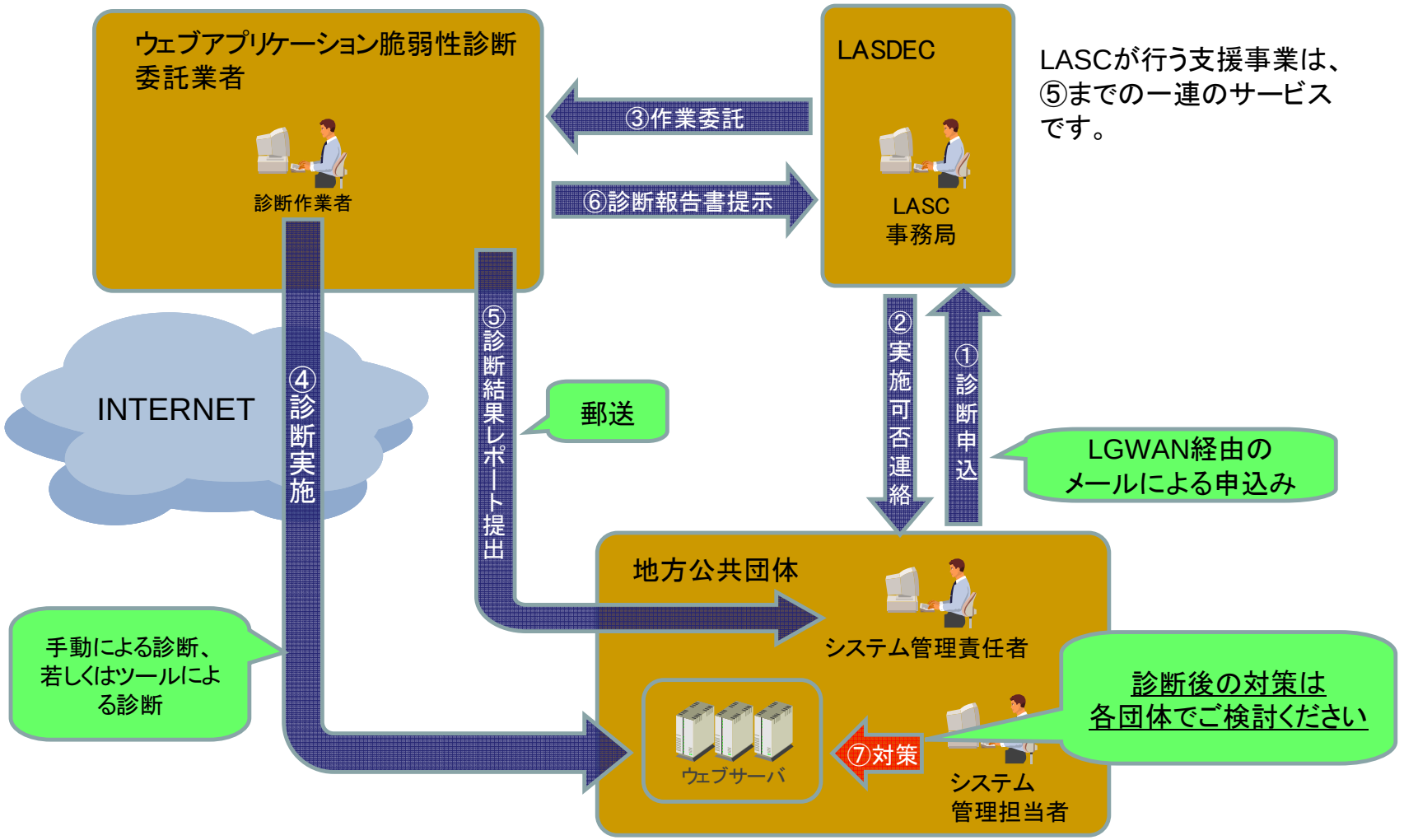
遠隔診断利用イメージ



ウェブアプリケーション脆弱性診断

- ウェブアプリケーション全般の診断項目
  - クロスサイト・リクエスト・フォージェリー
  - バックドア、デバックオプション
  - エラー処理状況
  - エラーメッセージによるロジックの流出
  - クライアント側コメント
  - ファイルアップロード
  - ファイルダウンロード
- 通信に関する診断項目
  - リファラ情報
- セッション管理に関する診断項目
  - セッションID利用状況
  - セッションフィクセイション
  - Cookieの濫用
  - ログアウト機能
- 認証に関する診断項目
  - ユーザ認証処理
  - アカウントロック機能
- アクセスコントロールに関する診断項目
  - 利用者が割り当てられている権限を超えた機能実行可否
- パラメータ操作に関する診断項目
  - HTTPヘッダ・インジェクション
  - クロスサイト・スクリプティング
  - SQLインジェクション
  - OSコマンド・インジェクション
  - パス・トラバーサル
  - SSIコマンド・インジェクション
  - メールヘッダ・インジェクション
- Webサーバに関する診断項目
  - バナーチェック
  - ディレクトリ・リスティング
  - 強制ブラウジング・不要なファイルの公開

ウェブアプリケーション脆弱性診断実施イメージ概要

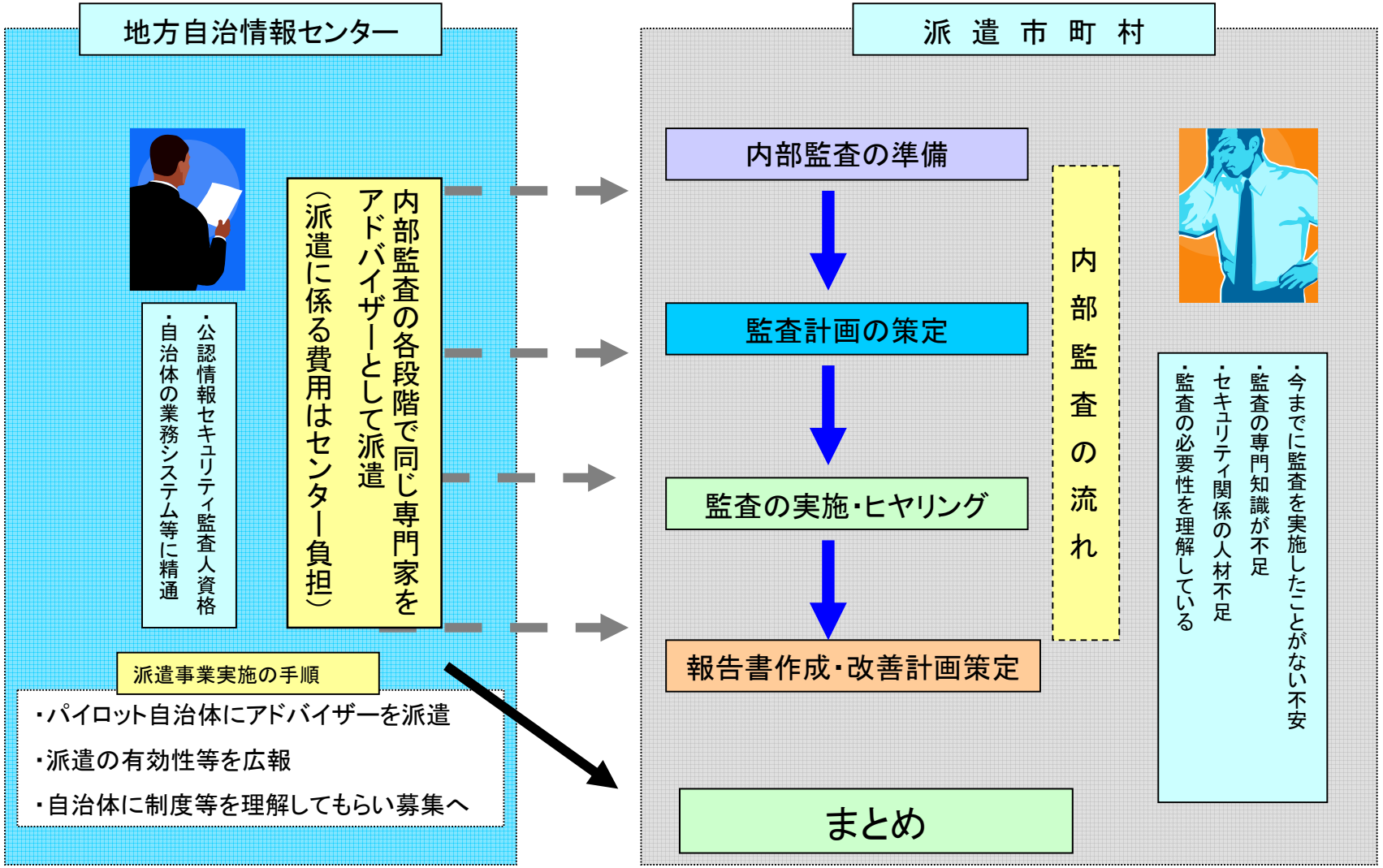


LASCが行う支援事業は、⑤までの一連のサービスです。

情報セキュリティ内部監査を支援するアドバイザーの派遣

- 情報セキュリティ内部監査を支援
- 監査計画作りから実施、改善報告でサポート
- JASA公認情報セキュリティ監査人同等のレベル
- 自治体の業務及びシステムに精通
- パイロット団体8団体で試行中
- 来年度制度化予定(監査未実施市町村を優先)

派遣のイメージ



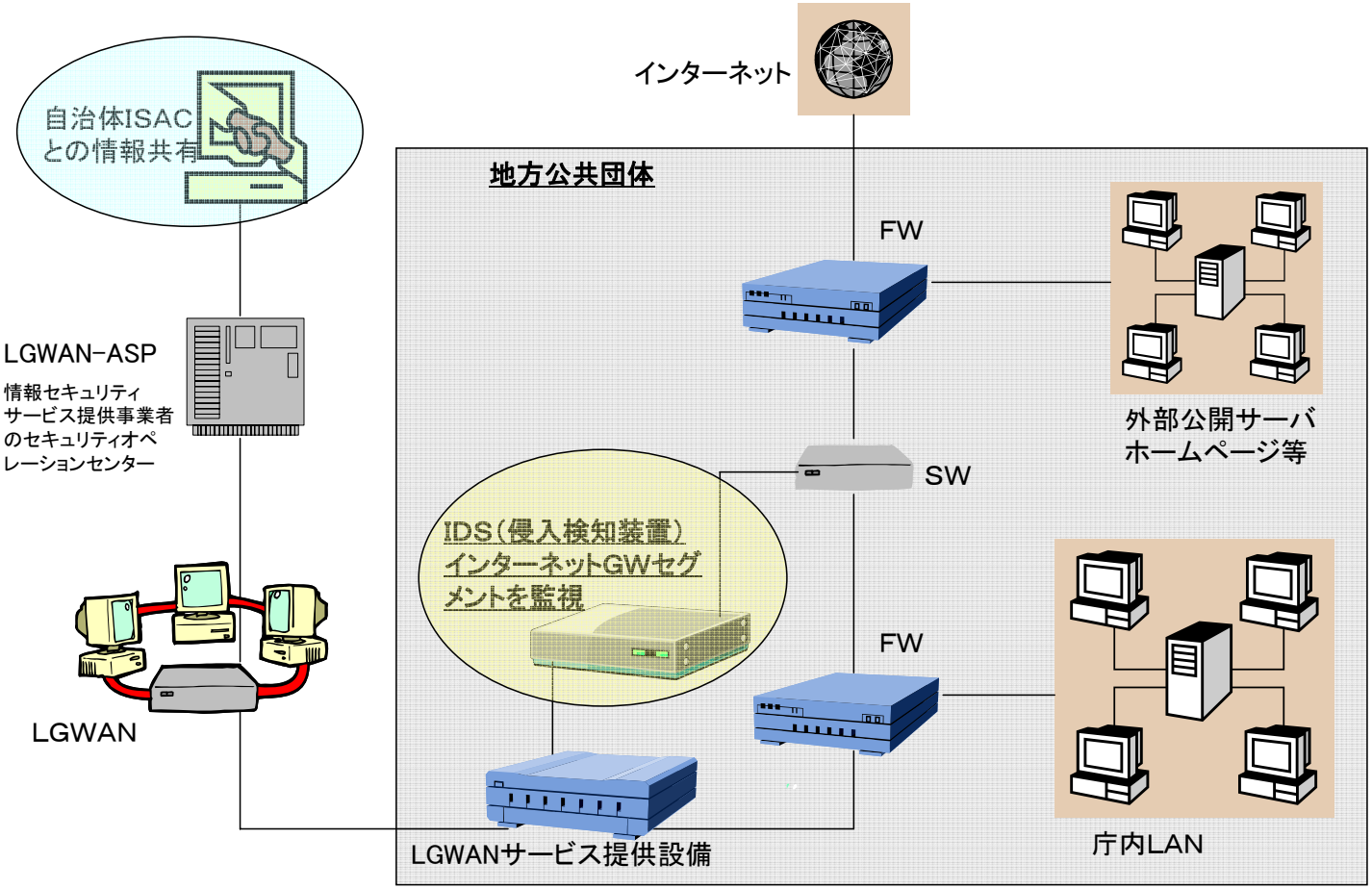
LGWAN-ASPを活用した情報セキュリティ支援事業（IDSによる庁内～インターネット監視）

- インターネット～庁内LAN間
- 不正アクセスやウイルス等8項目
- IDS(侵入検知装置)で常時モニター
- 重要度(高)のイベントは即通知(電話)
- 今年度は6ヶ月監視(19年8月～20年1月)

不正アクセスの試み
不正アクセスのための各種スキャン行為
攻撃コードの実行
バックドア通信

運用妨害コンピュータウィルスの活動
P2Pファイル共有ソフト(Winny等)の利用
WebMailやメッセンジャーソフトの利用
Spyware等のインストールや活動

LGWAN-ASPを活用した情報セキュリティ支援事業　接続図



人材育成（研究開発部、教育研修部との共催）

- eーラーニング(インターネットを利用)
  - 基礎コース、応用コース、上級コース
  - 基礎コースを5回に増加
- 高度情報セキュリティ研修
  - 管理研修、基礎技術研修、応用技術研修、内部監査研修
  - 13会場(東京、名古屋、高松、札幌、広島、仙台、横浜、鳥取、静岡、鹿児島、さいたま、大阪、福岡)
- H20年度の方向性
  - 内容の精査を図っている
  - 動画を取り入れたeーラーニング学習へ

LASC(自治体セキュリティ支援室)ポータルサイト

事例紹介

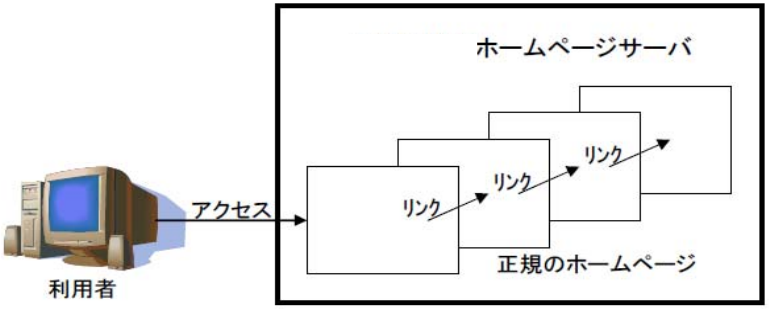
A市ホームページへの不正侵入

(市ホームページの発表より)

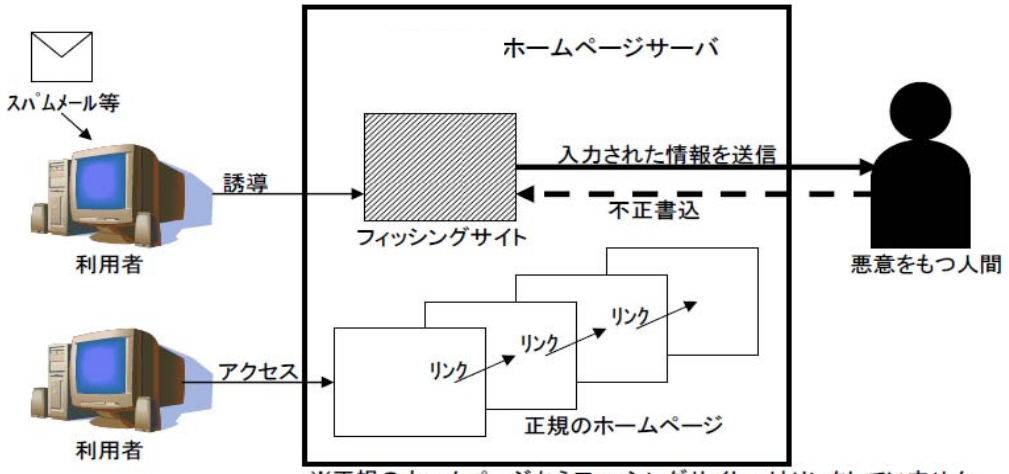
1. 概要
   - 平成19年11月27日、市ホームページ内の「教育ポータルサイト」に、アメリカのオークション等を業務とする会社の擬似ページ(英語)が作成され、利用者情報を不正取得するフィッシング行為」の踏み台とされる被害が確認された
   - 同日18:30頃に市ホームページを緊急閉鎖し、現在のところ再開の目途が立たない状況
2. 経過(11月27日)
   - 17:35 頃・市が利用している通信事業者より、市ホームページの不正利用の可能性があるとの連絡を受ける。
   - 状況を調査し、不正使用の状況を確認
   - 18:30 頃・市ホームページを緊急閉鎖する
3. これまで確認できた被害状況
   - 教育ポータル内への不正ページ(フィッシング行為に使用されたと思われる)の書込み
   - 上記のほか、数箇所に不正ファイルの書込みが確認された。
   - ※このため、サイト公開は当面不可能と判断
4. 個人情報等への影響
   - 11月28日現在、個人情報流出の可能性は低い状況
5. 今後の対応
   - 侵入原因の調査
   - 代替市ホームページの臨時開設
   - 市ホームページの再構築(セキュリティチェックを徹底)
6. 1/31 ホームページ全復旧

フィッシングサイト不正書込の状況

通常のホームページ閲覧の流れ



今回の事案



※正規のホームページからフィッシングサイトへはリンクしていません。

（市ホームページの発表より）

職務に関係ないサイト閲覧し、サーバをダウンさせた職員を処分 – ○○市

- ○○市は、職務と無関係なサイトを閲覧し、サーバをダウンさせた環境局の課長級職員に対し減給2カ月の懲戒処分を行った
- 7月5日午後4時37分から54分の間、業務用パソコンを使って職務とは無関係のサイトにアクセス
- その結果、同サイトから大量のアクセスが同市サーバに対して発生。
- その負荷で同市のインターネット接続用サーバが7分間ダウン
- 庁舎内でインターネットが使用できなくなった

職務に関係ないサイト閲覧し、ウイルス感染未遂 – △△市

- ある管理職によるアダルトサイトの閲覧
- ウイルス侵入をFirewallで撃退
- 職務専念義務違反で減給1/10、1ヶ月

△△市が課長を懲戒処分
個人情報ネット流出で

- ファイル交換ソフト「ウィニー」を介し業務で扱った個人情報などをインターネット上に流出。
- 男性課長（51）を減給6カ月（10分の1）の懲戒処分。
- 監督責任で同部部長を訓告、副市長を口頭での厳重注意とした。
- **無許可**で業務上の情報を自宅のパソコンで扱う。
- 業務上のデータを持ち出す場合、所属長の許可が必要。
- **課長はウイルス対策ソフトなどを導入していなかった。**
- ウィニーなどのファイル交換ソフトの導入禁止。
- データの持ち出しを原則禁止。

外部監査から内部監査へ

- 大阪府吹田市
  - 日経ガバメントテクノロジー(web版)「情報セキュリティ監査の基本とトレンド第４回」参照
  - 外部監査を先に実行
  - 監査人から監査のノウハウを学ぶ
  - 内部監査は相互監査方式
- 岡山県津山市
  - LASDECの住基ネット外部監査を積極的に活用
- 埼玉県小鹿野町
  - セキュリティポリシーを条例化
  - 教育委員会などの機関もシステムを一体整備

ITによる市民との協働

- 神奈川県藤沢市：情報セキュリティの日表彰
  - 内部・外部監査の実施
  - 国際規格の情報セキュリティマネジメントシステム(ISMS)の認証を先行的に取得
  - 庁内情報ネットワークへのシンクライアント及び生体認証の導入
  - 事業の継続的な計画(IT-BCP)の策定
  - 全職員を対象としたセキュリティ研修や訓練の実施
- インターネット安全教室
  - ボランティアが講師

セキュリティ情報の共有

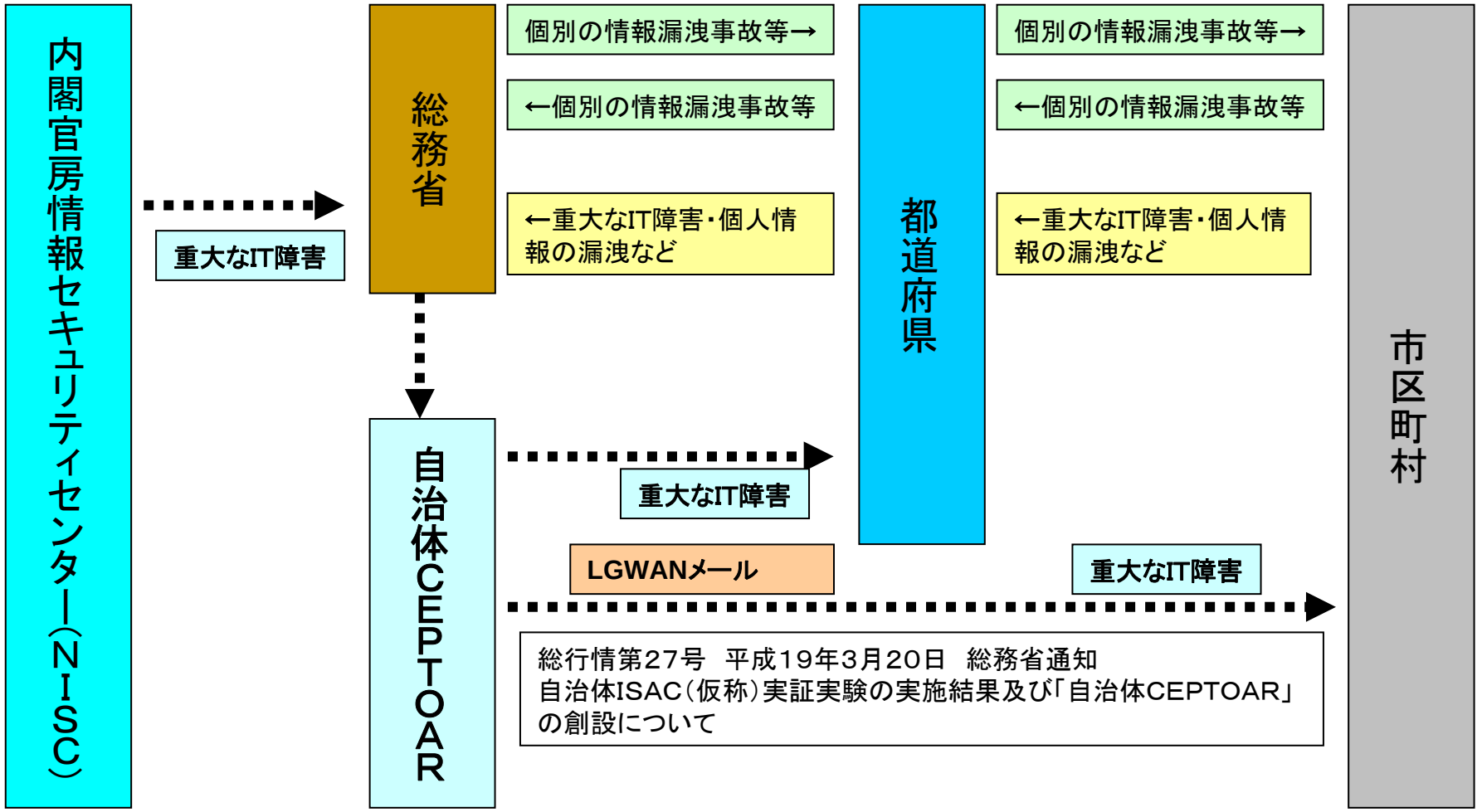
重大なIT障害情報

- 緊急度(高)で72時間以内の対応
- NISC発足後、幸いにも今まで該当なし
- 具体例
  - セキュリティホール等を発見した場合や、プログラム・バグを発見した場合等であって、他のインフラ事業者等に同じ問題が生じるおそれがあると認められる場合
  - サイバー攻撃の発生又は攻撃の予告がある場合、災害による被害が予測される場合等、他の重要インフラ事業者等の重要システムが危険にさらされていると認められる場合
- 情報共有レベル
  - Aの場合・・・関係する業務担当ラインの職員及び関係するシステムの保守業者等で、かつ業務の関係者のみ
  - Wの場合・・・公共向けの情報で、ホームページ等での公表可
- ２／１２　訓練
  - 自治体へは事前通告なし

その他のセキュリティ情報

- 総務省から提供されるセキュリティに関する情報
- 有限責任中間法人 JPCERT コーディネーションセンターからの脅威・注意喚起情報
- 独立行政法人情報処理推進機構（IPA）等、情報セキュリティ関係機関から収集した情報
- 地方公共団体から収集したセキュリティに関する各種情報
- ASP監視事業者から入手したセキュリティ監視に関する情報(匿名の統計データを分析、活用)
- 遠隔監視やウェブアプリ診断データ(匿名の統計データを分析、活用)
- その他これらに付随する情報

緊急時のセキュリティ情報の流れ



ご清聴ありがとうございました。

(財)地方自治情報センター
自治体セキュリティ支援室長
石川家継　ishikawa@lasdec.or.jp