NISC National Information Security Center

# 地方公共団体における
# 情報セキュリティ対策への取組み

2008年２月14日（木）

内閣官房情報セキュリティセンター（NISC）

http://www.nisc.go.jp/

資料９－１

# 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見直し（平成18年9月）

## Ⅰ　地方公共団体のセキュリティ対策の水準を強化

- 情報漏えい防止等のため取るべき対策や生体認証等最近の技術的動向を踏まえた規定を追加
- セキュリティ対策を強化する観点から、各地方公共団体において必要に応じ実施することが望まれる事項については、「推奨事項」と明記して例文に挿入
- 地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献することが望まれる旨、記述　　等

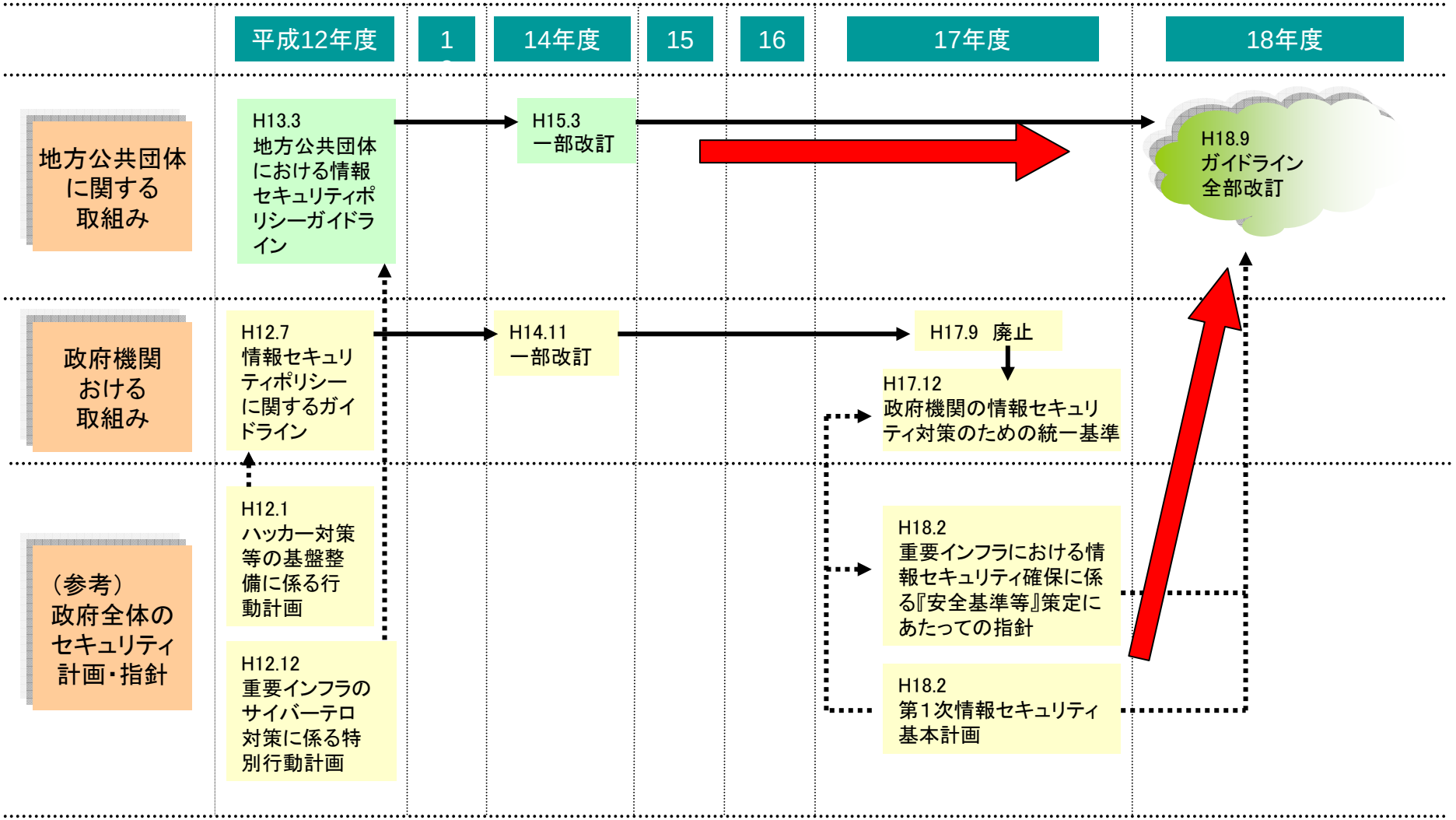
## Ⅱ　重要インフラ指針への対応

- 重要インフラ指針において列記された項目に対応
- 情報のライフサイクルに着目した対策の明示
- 機密性、完全性、可用性の観点からの情報の格付けや取扱い制限の明示　等

## Ⅲ　分かりやすい表現に変更

- 全体を、「総則」、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」の三章構成に整理
- 情報セキュリティ対策基準の構成を、PDCAサイクルを踏まえて変更。また、各対策の説明を、趣旨、例文、解説の順に統一
- 責任主体を明記し、権限と責任を明確化　等

# 情報セキュリティポリシー等に関する取組の推移



# 新ガイドラインの構成

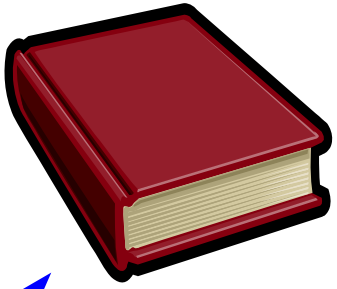
ガイドライン
（平成13年版/平成15年一部改定）

〇〇市情報セキュリティポリシー
平成〇〇年〇〇月〇〇日　策定
平成〇〇年〇〇月〇〇日　一部改定
〇〇市情報推進化委員会了承
地方公共団体配付版

主な参考資料
·安全基準の必要事項の掲載
·政府統一基準を参考
·ISO/IEC17799(2005)を参考

最近の技術動向の反映
組織的な活動に関するノウハウ

新ガイドライン



第1章　総則

第2章　基本方針

第3章　対策基準

- 全体を、総則、情報セキュリティ基本方針、情報セキュリティ対策基準の三章構成に整理した。
- 情報セキュリティ対策基準の構成を、趣旨、例文、解説等の順に統一した。
- 最新の技術的動向を踏まえた内容にするとともに、表現を簡潔で分かりやすいものに変更した。

# 新ガイドラインの主な変更点

***《情報セキュリティ基本方針》***

・基本的事項を規定する形式のもののほか、宣言書の形式のものを例示

***《組織体制に関する事項》***

・情報セキュリティの専門家をアドバイザーとして置くことを規定【推奨事項】

・情報セキュリティ委員会で毎年度、改善計画を策定することを規定【推奨事項】

・監査人と被監査人とを同一人が兼務しないことを規定

***《情報資産の分類と管理に関する事項》***

・情報資産の分類方法を重要度に基づく分類から、基本的に機密性、完全性、可用性に基づき分類することに変更

・情報セキュリティ担当者が情報資産に管理責任を負うことを明記

・情報資産の取扱いを、情報のライフサイクル（作成、入手、保管、送信、運搬、提供・公表及び廃棄）ごとに整理

***《施設・設備面での対策》***

・管理区域（情報システム室等）の入退室管理を強化

・ ネットワーク回線の適切な選択と管理について規定

・ パソコン端末に関する盗難及び情報漏えい対策を強化

*《職員等に対する対策》*

・情報漏えいの防止策として、情報資産の持ち出し制限、私物パソコンの使用制限等の強化策を明記
・すべての職員等を対象に、毎年度１回以上研修を受講できるようにすることを規定【推奨事項】
・情報セキュリティ事故等に関し、住民からの報告を受ける窓口を設置することを規定【推奨事項】

*《技術面での対策》*

・電子メールに関するセキュリティ対策を強化
・盗聴防止のため、無線LANのセキュリティ必要要件を具体化
・インターネットに接続していないシステムの不正プログラム対策を規定
・不正プログラム対策において、外部の専門家の支援を受けられる体制作りを規定【推奨事項】

*《運用面での対策》*

・職員等の端末及び記録媒体等の利用状況調査を明記
・事業継続計画との整合性の確保を規定
・外部委託契約の契約項目として、事故時の委託先の公表等を明記
・外部委託を行う場合の委託先選定において、委託先の情報セキュリティ対策状況をISMS の国際規格の認証取得状況等を参考にして判断することを規定【推奨事項】
・情報セキュリティポリシーが適用されない例外措置を規定

*《評価・見直しに関する事項》*

・監査結果を踏まえた、該当部署の対応義務を明記
・点検結果に対する職員等の対応義務を明記

# LASDEC（財団法人　地方自治情報センター）による支援事業

**自治体における情報セキュリティ対策向上のため、平成19年3月に「自治体セキュリティ支援室（LASC　Local Authorities Security Support Center ラスク）」を設置。**

## ◎　自治体CEPTOARとしての業務

（1）　内閣官房情報セキュリティセンター(NISC)から総務省を通じて提供されるIT障害等をLGWANメールにより地方公共団体へ一斉通知

（2）　LGWANを活用した電子メール、自治体セキュリティ支援室ポータルサイトにより、情報セキュリティ対策に関する各種情報提供（自治体の優良取組事例・事故事例、各種点検ツール、早期警戒情報等）

## ◎　LGWANーASPを活用した情報セキュリティ支援事業

インターネットから、応募自治体の庁内LANに出入りする不正アクセスやウイルスをIDS(侵入検知装置)で常時モニター 全体的な監視概要は自治体セキュリティ支援室ポータルサイトで共有し、セキュリティ事故の未然防止に寄与

## ◎　情報セキュリティ遠隔診断

Webサーバ、メールサーバ及びネットワーク機器等を外部から遠隔診断することにより、セキュリティホールの発見と対応策を応募自治体に提供

## ◎　e-ラーニングによる情報セキュリティ研修

地方公務員を対象に、住民に信頼される電子自治体の実現に必要な情報セキュリティ対策を確立するとともに、最新のセキュリティ技術や個人情報の取扱いに関する専門知識及びノウハウを有する人材を育成することを目的に、インターネットを利用したe-ラーニングによる情報セキュリティ研修事業を実施。

## ◎　高度情報セキュリティ研修

地方公共団体の職員の希望者を対象に、①管理研修　②基礎技術研修　③応用技術研修　④内部監査研修　の4メニューを実施