



報道資料

平成 21 年 6 月 22 日
内閣官房情報セキュリティセンター (NISC)

情報セキュリティ政策会議第 22 回会合の開催について

—「セキュア・ジャパン2009」の決定等—

本日、「情報セキュリティ政策会議」(議長:内閣官房長官)の第 22 回会合が開催され、その概要は以下のとおり。

1. セキュア・ジャパン2009決定～「事故前提社会」に向けた具体的取組みの開始～

本日、我が国の情報セキュリティ政策に係る年度計画であるセキュア・ジャパン2009が決定された。従来の事前防御に焦点を当てた年度計画を発展させ、情報セキュリティ事故が生じうることを前提に、官民において対応策を構築していくことに焦点が当てられている。

本計画は、我が国の新たな情報セキュリティ政策の方向性を定める「第 2 次情報セキュリティ基本計画」(本年2月3日決定。以下「第2次基本計画」という。)に基づき、2009年度において各府省庁が取り組む施策を具体的に示したもの。

なお、本案については、平成21年5月8日から5月29日までの間、意見の募集を実施したところ、7企業・団体から延べ 44 件、5個人・グループから延べ16件、計 60 件の意見が寄せられ、その内容は、政府の取組みの更なる加速的な推進に向けての参考となるものが多数であった。

寄せられた意見を踏まえ、「セキュア・ジャパン2009(案)」の施策一件について地方公共団体における情報資産のリスク分析・評価に関する記述を追加したほか、注釈の追加等、より見やすく分かりやすくするための編集を行った。寄せられたコメントについては、「セキュア・ジャパン2009」の施策実施、政策立案等の情報セキュリティ政策の推進にあたっての貴重な御意見として、適切に対応していく。

(別紙 1 参照)

2. 政府機関の公開ウェブサーバ及びメールサーバの集約化

政府機関が保有する公開ウェブサーバ及びメールサーバの現状等が報告され、セキュリティ向上、コスト削減の観点から、2013年度末までに政府機関の公開ウェブサーバ及び電子メールサーバを半減することを目標とするなどの方針が決定された。

(1) 現状

- 政府機関全体で公開ウェブサーバ約1,000台、電子メールサーバが約1,900台
- 本年4月以降複数発生した政府機関HP改ざん事案において、関係政府機関の対応に遅れが見られた

(2) 問題認識

- 統制なく多数のサーバを設置・運用すると、コストが増大し、緊急時に迅速かつ的確な対応が困難となるなどセキュリティリスクが高まる
- 障害・事故等発生時における緊急連絡体制が、十分機能していない場合がある

(3) 今後の取組

- 公開ウェブサーバ及び電子メールサーバについては、2013年度末までに、政府機関全体として少なくとも半減することを目標とする
- 各府省庁は、公開ウェブサーバ及び電子メールサーバに係る集約化計画を定め、本年12月に予定される情報セキュリティ政策会議に報告
- 今年度の重点検査等においてサーバの設置・運用の詳細な状況について把握するとともに、障害・事故等発生時における緊急連絡体制について点検（別紙2参照）

3. 重要インフラの情報セキュリティに関する「安全基準」策定指針は今秋改定予定

「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」については、従来からの「本編」に加え、対策項目の具体化を例示する「対策編」を新たに設ける方針。現在、重要インフラ専門委員会において改定のための検討が進められている。

「本編」については、重要インフラ専門委員会で検討を行い、改定案を9月目処に作成し、その後の情報セキュリティ政策会議で決定する。

（別紙3参照）

※ 本日の会議資料は、内閣官房情報セキュリティセンターのホームページにおいて公表します。

(<http://www.nisc.go.jp/conference/seisaku/index.html#seisaku22>)

※ 「情報セキュリティ政策会議」は、平成17年5月30日のIT戦略本部決定によって設置されました。

(<http://www.nisc.go.jp/press/pdf/050530seisaku-press.pdf>)

経緯

[第20回情報セキュリティ政策会議(H20.2.3)]

- 第2次情報セキュリティ基本計画が政策会議において決定。



[第21回情報セキュリティ政策会議(H20.5.8)]

- 「セキュア・ジャパン2009(案)」について審議を実施、パブリックコメントに付すことを決定。

意見募集及び結果の概要

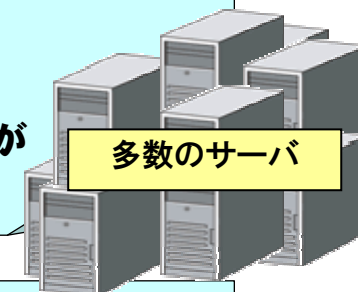
- 実施期間: 平成21年5月8日(金) ~ 平成21年5月29日(金)
- コメント総数: **60件** 【内訳: **7企業・団体から延べ44件、5個人・グループから延べ16件**】
- コメント概要: 施策に対する見解、施策実施に当たっての配慮要望、施策の基本的方向性についての評価等。
 - ・ 電子政府推進の大前提となる国民・企業IDの早期導入に向けた検討において広く国民の理解を得るため、社会保障番号、納税者番号、国民電子私書箱等の検討段階からNISCが参画し、安心なシステム構築に貢献すべき。
 - ・ 政府調達におけるセキュリティ確保の一環として、契約前に予めセキュリティレビューを行うことを盛り込むべき。
 - ・ 積極的に民間のセキュリティ資格の周知拡大をお願いしたい。
 - ・ 国と企業が連携しながら戦略的に国際貢献できる体制の整備のために、より具体的な施策・工程表を検討すべき。
 - ・ 表現上の指摘等

コメントへの対応

- 地方公共団体における情報資産のリスク分析・評価に関する記述を追加した。
- 見やすさ・分かりやすさの向上に係る変更等を行った。
- 御意見の内容により、今後の政策立案や施策実施にあたっての参考とするなどの活用を検討する。

現 状

- ・ 政府機関全体において多数のサーバを保有。
(公開ウェブサーバ約1,000台、電子メールサーバ約1,900台(平成20年11月1日時点))
- ・ 本年4月以降複数発生した政府機関のHP改ざん事案において、関係政府機関の対応の遅れが見られた。

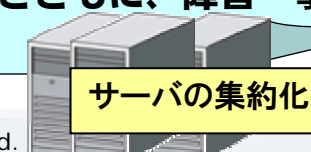


問題認識

- ・ 統制なく多数のサーバを設置・運用すると、コストが増大し、緊急時に迅速かつ的確な対応が困難となるなどセキュリティリスクが高まる。
- ・ セキュリティ向上の観点、また、コスト削減の観点からも、既存の最適化等の状況を踏まえつつ、各府省庁の業務や実情に応じて、サーバの集約化を推進する必要がある。
- ・ 障害・事故等発生時における緊急連絡体制が、十分に機能していない場合がある。

今後の取組

- ・ 公開ウェブサーバ及び電子メールサーバについては、2013年度末までに、政府機関全体として少なくとも半減することを目標とする。
- ・ 各府省庁においては、最適化計画の枠組みも活用し、省全体の2010年度からの公開ウェブサーバ及び電子メールサーバに係る集約化計画を定め、本年12月に予定される情報セキュリティ政策会議に報告する。
- ・ 今年度の重点検査等においてサーバの設置・運用の詳細な状況について把握するとともに、障害・事故等発生時における緊急連絡体制について点検する。



政府機関のサーバ集約化について

平成21年6月22日
情報セキュリティ政策会議決定（案）

政府機関全体においては、公開ウェブサーバ約1,000台、電子メールサーバ約1,900台など多数のサーバを保有している状況である（2008年度 政府機関の情報セキュリティ対策の実施状況に関する重点検査及び評価結果について（平成21年2月3日情報セキュリティ政策会議報告））。

統制なく多数のサーバを設置・運用すると、コストが増大し、緊急時に迅速かつ的確な対応が困難となるなどセキュリティリスクが高まるという問題がある。

セキュリティ向上の観点、また、コスト削減の観点からも、既存の最適化等の状況を踏まえつつ、各府省庁の業務や実情に応じて、今後、以下の方針で、サーバの集約化を推進する。

<今後の方針>

- 1 政府機関の公開ウェブサーバ及び電子メールサーバについては、2013年度末までに、政府機関全体として少なくとも半減することを目標とする。
- 2 各府省庁においては、最適化計画の枠組みも活用し、省全体の2010年度からの公開ウェブサーバ及び電子メールサーバに係る集約化計画を定め、本年12月に予定される情報セキュリティ政策会議に報告する。

「指針※の見直し」の進め方について

※重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針
(2006年2月2日 情報セキュリティ政策会議決定、2007年6月14日改定)

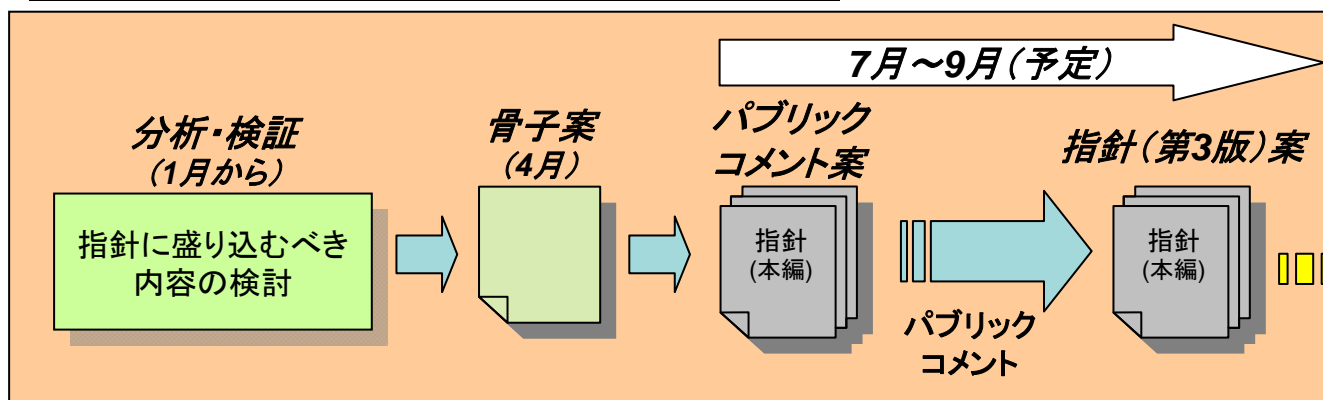
○第1次行動計画においては、指針の策定・見直し、これを踏まえた各分野毎の安全基準等の策定・見直しを実施。これらの定期的な見直しサイクルが確立。

○第2次行動計画では、指針の改定は原則として3年に1度とし、対策項目の具体化の例示の充実を図る。

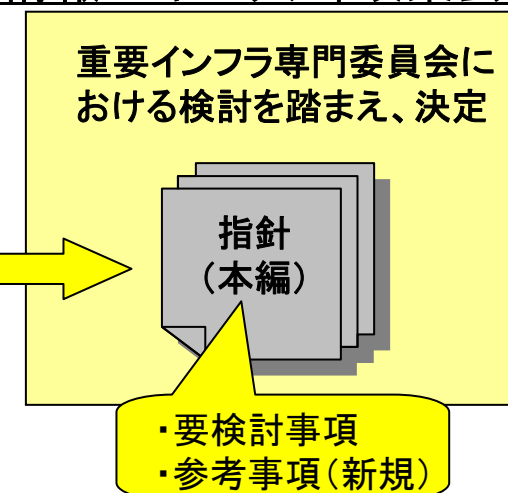
進め方

- ①指針(第3版)本編は、現行の「要検討事項」に加え、検討が望まれる項目を新たに「参考事項」として記載
⇒ 重要インフラ専門委員会においてパブリックコメントまで含め検討を行い、これを踏まえ、情報セキュリティ政策会議で決定
- ②新たに設ける対策編は、対策項目の具体化を例示
⇒ 重要インフラ専門委員会でとりまとめ

重要インフラ専門委員会における検討



情報セキュリティ政策会議



(※) 対策項目の具体化を例示する「対策編」については、重要インフラ専門委員会でとりまとめる。