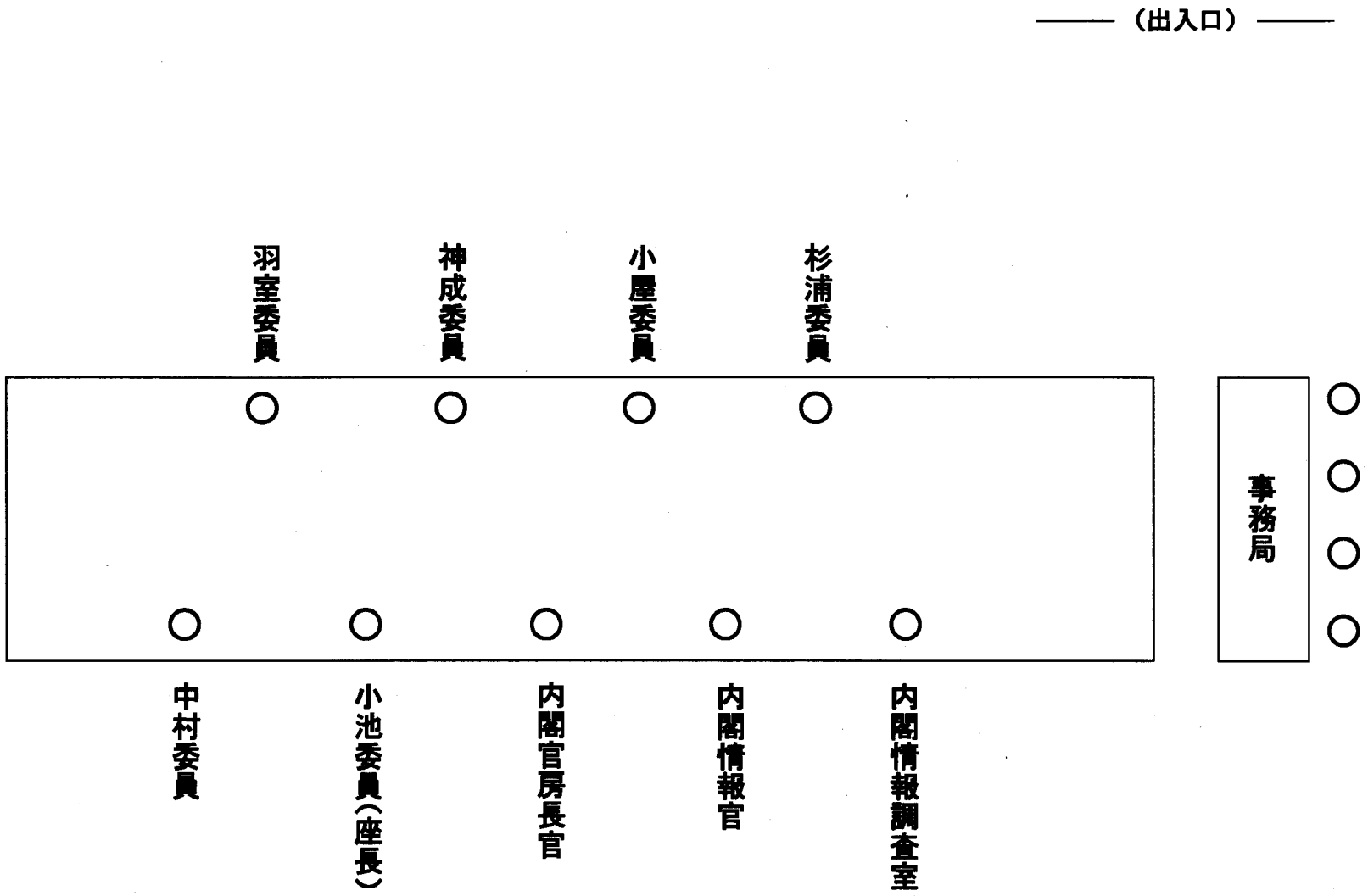
第1回情報保全システムに関する有識者会議　座席表

平成22年12月17日(金)午後2時～午後3時　於:官邸4階大会議室



配付資料

資料１　政府における情報保全に関する検討委員会の開催について

資料２　情報保全システムに関する有識者会議の開催について

資料３　情報保全システムに関する有識者会議の運営について（案）

資料４　情報保全システムの検討スケジュール（案）

資料５　脅威に関する現状認識

資料６　「カウンターインテリジェンス機能の強化に関する基本方針」の概要

資料７　特別管理秘密に係る基準

資料８　政府機関の情報セキュリティ対策の枠組み

資料９　政府機関の情報セキュリティ対策のための統一基準（第４版）

対外非公表　取扱注意

機密性２情報　配付資料３

（案）

情報保全システムに関する有識者会議の運営について

平成２２年１２月○○日
情報保全システムに関する有識者会議決定

情報保全システムに関する有識者会議（以下「会議」という。）の運営については、以下のとおりとする。

1　議事の非公開について

会議は、非公開とする。

2　議事要旨の公開について

会議の議事要旨は、原則として、会議終了後、発言者名を付さない形で、速やかに公開する。

3　配付資料の公開について

会議における配付資料の公開については、内容に応じて可否を判断する。

4　記者ブリーフについて

会議の内容については、会議終了後、事務局が記者ブリーフを実施する。

（了）

１．盗難や持出し等の脅威

(1) 可搬型電磁的記録媒体や文書の盗難等

○　庁舎外へ持ち出すことができるＵＳＢメモリ等の可搬型電磁的記録媒体が厳重に管理されていないことにより、それらが盗取され、また、盗取されても把握することが困難となるおそれがある。

○　行政事務従事者が特に機密性の高い情報を取り扱う情報システム（以下単に「情報システム」という。）から電磁的記録を媒体や書面へ不用意に出力するなど、管理されていない複製が作成されることにより、それが盗取され、また、盗取されても把握することが困難となるおそれがある。

○　執務を行っていないときには執務机の上に文書等を放置せず、端末のディスプレイにも情報を表示しないというポリシーが徹底されず、関係者以外に情報を盗み見られるおそれがある。

(2) 機器の盗難等

○　モバイルコンピュータに関する正規の使用方針が定められていないことにより、モバイルコンピュータの盗難又は紛失及びこれらに伴う情報流出のリスクがある。

(3) 秘密取扱い施設への不正侵入等

○　建物、ドア及び窓に対する物理的な防護水準が低い、秘密取扱い施設内の監視が不十分等の原因により、不正侵入や無許可立入りが発生するおそれがある。

○　秘密取扱い施設に入退室するすべての者について、適切な入退室管理が行われていない場合がある。

(4) 無許可機器による情報の持出し

○　管理区域内に無許可で持ち込まれたコンピュータ、電磁的記録媒体、デジタルカメラ、携帯電話等を使用され、情報が持ち出されるおそれがある。

２．無権限者等による不正な操作等の脅威

(1) 不適切な権限管理等

○　情報システムの利用許可、ユーザ管理、権限管理及びアクセス制御が確実に実施されず、権限を与えられていない者による不正なシステム操作又は利用が発生するおそれがある。

○　管理者権限行使による作業を監視する体制が必ずしも十分でない。

(2) 権限の詐称

○　情報システムにアクセスする主体の識別及び認証メカニズムが不十分な場合がある。

○　ネットワーク上で暗号化せずパスワードを転送するなど、主体認証情報が適切に保護されていない場合がある。

○　パスワードを人目につきやすい場所に放置するなど、主体認証情報が適切に保護されていない場合がある。

(3) 情報システムの管理体制の不備

○　権限を与えられていない者による不正アクセス行為又は基準に準拠しない行為を監視する体制が必ずしも十分でない。

○　情報システムのセキュリティの維持・管理のために必要な技能を備えた十分な数の職員が割り当てられていない場合がある。

３．悪意のある者による情報システムに対する攻撃の脅威

(1) ネットワークを利用した外部からの侵入

○　ネットワークの構造上の脆弱性、不正に入手した認証情報、通信回線等の物理的な脆弱性等を悪用して情報システムに侵入され、情報の収集、破壊等が行われるおそれがある。

(2) ハードウェアの改ざん

○　悪意のある者により電子計算機にセキュリティホールが組み込まれるなど、ハードウェアの改ざん行為によって情報が探知及び収集され、又は破壊されるおそれがある。

(3) ソフトウェアの改ざん

○　独自に開発したソフトウェアに悪意のある者によりセキュリティホールが組み込まれるなど、ソフトウェアの改ざん行為によって情報が探知及び収集され、又は破壊されるおそれがある。

○　安全性が確認されていないソフトウェアが情報システムにインストールされることにより、情報の流出、データの破壊、セキュリティ機能の無効化などが生じるおそれがある。

(4) 情報流出のおそれのあるインタフェイス等の利用

○　情報の流出に利用されるおそれのあるインタフェイスや機能が利用可能な状態で放置され、悪意のある者がこれを利用することによって情報が探知及び収集され、又は破壊されるおそれがある。

４．情報システムの誤作動の脅威

(1) 機器の誤作動

○　安全性の確認されていない機器が接続されることによって情報システムが誤動作を起こし、情報の流出、データの破壊、セキュリティ機能の無効化などが生じるおそれがある。

(2) ソフトウェアの誤作動

○　意図せざる脆弱性によってソフトウェアが誤作動し、情報の流出、データの破壊、セキュリティ機能の無効化などが生じるおそれがある。

○　設定の変更等によってソフトウェアが誤作動し、情報の流出、データの破壊、セキュリティ機能の無効化などが生じるおそれがある。

５．操作ミスの脅威

○　情報システムの操作説明書が作成されていない、配付されていない又は周知されていないなどの理由で、行政事務従事者が情報システムの操作方法等を十分に理解しておらず、操作ミス、誤入力等が発生するおそれがある。

○　情報システムのユーザインタフェイスが複雑で、行政事務従事者の操作ミス、誤入力等が発生するおそれがある。

６．その他

(1) 部内者の情報セキュリティ違反行為

○　行政事務従事者のセキュリティ違反を監視するためのメカニズムが不十分であるため、セキュリティ違反に対する抑止効果が小さく、また、事故発生後に適切に対処することができないおそれがある。

○　データの不正処理、無許可アクセス、その他の情報セキュリティ関係規程の違反に対する制裁措置が明確でなく、行政事務従事者に対する抑止及び再発防止の効果が必ずしも十分でない。

(2) 廃棄又は再利用された電磁的記録媒体からの情報復元

○　特に機密性の高い情報の処理に使用した電磁的記録媒体を廃棄する場合や再利用する場合において、十分な破壊処置を行わなかったために当該電磁的記録媒体にデータが容易に回復できる状態で残されていたり、当該電磁的記録媒体に残されたデータの電磁的痕跡が抽出され、復元されたりすることによって情報が流出するおそれがある。

(3) 契約業者による情報セキュリティ侵害

○　情報システムの保守・点検契約を締結している業者の故意又は過失による行為によって情報が流出し、又はデータが破壊されるおそれがある。

○　特に機密性の高い情報の処理業務を委託した業者との間で情報セキュリティ対策に関する契約条項を締結しておらず、委託先業者が不適切に情報を取り扱うおそれがある。

(4) セキュリティパッチの不適用

○　パッチを適用せず、ソフトウェアのバグ等を放置することにより、誤作動、データ破壊、セキュリティ機能の無効化等が発生するおそれがある。