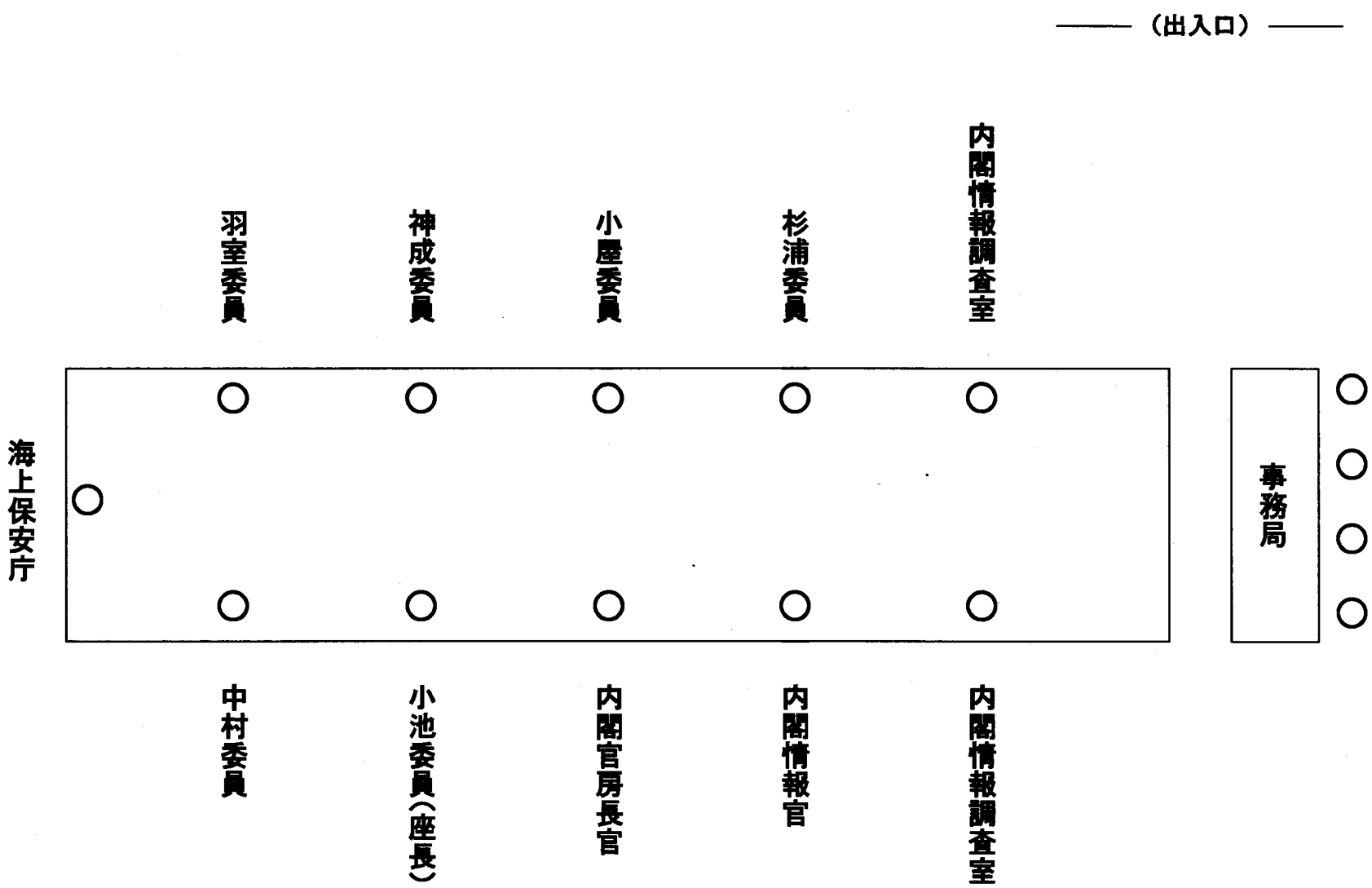
第4回情報保全システムに関する有識者会議　座席表

平成23年5月20日（金）午後1時30分～午後3時30分　於：官邸4階大会議室



機密性２情報（関係者限り）

配布資料

特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について

（報告書）

（案）

平成２３年５月　日

情報保全システムに関する有識者会議

機密性２情報（関係者限り）

機密性２情報（関係者限り）

はじめに

当会議は、昨年１２月、政府における情報保全に関する検討委員会から、特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について意見を示すよう要請を受け、以後数次にわたる会合において議論を重ねてきた。本報告書は、これらの議論を踏まえ、特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し特に留意すべき事項について、当会議としての意見を取りまとめたものである。

Ⅰ　総論

ＩＴ技術やネットワーク社会の進展が著しい現在、情報が一旦ネットワーク上に流出するや極めて短期間に世界規模で広がり、もはや取り返しのつかない事態に陥ってしまう。こうした環境の中で、我が国政府における情報保全の万全をいかに図るかが極めて重要な課題になっている。

情報保全を図る上で、情報を取り扱う職員に対する教育など、人的な面での対策の強化が不可欠であることは論をまたないが、同時に、職員による故意の情報漏洩のリスクが常に存在することも念頭に置き、万一職員が情報漏洩を企図しても物理的に困難、もしくは後日判明するという心理的抑止力のためその証拠が保全されるように、システム上必要な対策が講じられていなければならない。

当会議では、特別管理秘密等の特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状や、過去発生した情報漏洩事案及び事後強化した対策等を踏まえた上で、守るべき情報、対象となるシステム及び想定される脅威について整理し、情報漏洩防止等のために必要と考えられる措置について取りまとめた。

情報漏洩を防止する観点からは、情報の取扱いについてあらかじめ厳しい制限を加えることとしがちであるが、それだけでは、運用面に過大な負担を与える場合があることから、業務に支障のないように、実情を踏まえバランスの取れた対策を実施することが求められる。

また、情報漏洩のリスクを完全にゼロにすることは不可能であるため、事前予防だけでなく、万が一漏洩事案が発生した際には迅速に状況を把握して適切な事後対応を可能とするための対策にも力を入れることが肝要である。

ＩＴ技術の急速な発展を踏まえると、情報保全システムに対する脅威も逐次変化することが想定される。当会議では、将来想定される脅威についても議論を行ったところ、特に機密性の高い情報を取り扱う政府機関においては、技術の動向やこれらを悪用した脅威について常に情報収集を行い、途切れることなく適時適切に対策をとっていく必要がある。

第１　守るべき情報及び対象となるシステム

当会議では、守るべき情報として、特別管理秘密をはじめとした特に機密性の高い情報を念頭に置き、議論を行った。特に機密性の高い情報を取り扱う政府機関においては、これらの情報をインターネットと接続されていないクローズ系のシステムで取り扱っている。また、クローズ系のシステムとは別に、インターネットに接続されたオープン系のシステムがあり、外部との連絡等に使っている。情報漏洩防止のため、機密性の高い情報を含む文書の作成や保存は、原則としてクローズ系のシステムで行い、オープン系のシステムではできないものとしている。

以上を踏まえれば、特に機密性の高い情報の漏洩防止のためのシステム上の対策としては、基本的にクローズ系のシステムのサーバ及び端末内の情報が同システムの外部に流出することがないように必要な措置を講じれば足りるように思われる。

しかしながら、実務上は、外部との連絡のためクローズ系のシステムから機密性の低い情報を電磁的記録媒体へ書き出し、オープン系のシステムに読み込む必要がある場合がある。この際、不正プログラム等により、本来クローズ系にあるべき機密性の高い情報が全く意図せずに電磁的記録媒体に書き込まれる可能性があり、オープン系で当該電磁的記録媒体を読み込んだ際に、機密性の高い情報がオープン系に移され、さらにインターネットを通じて外部に流出するおそれは否定できない。

以上から、オープン系のシステムについても、特に機密性の高い情報の流出経路となるおそれがあるという観点から、所要の措置を講じる必要がある。

一方、スタンドアロン端末については、現状では、出張時の記録に使用するなど特段機密性の高い情報を取り扱わないものと、クローズ系以上に機密性の高い情報を取り扱うためにネットワークを構成していないものがある。一般にスタンドアロン端末は管理が十分に行き届かない傾向にあると言われることから、スタンドアロン端末についてはその必要性について検討し、運用するに当たっては、厳格な管理を徹底する必要がある。

第２　想定される脅威

情報漏洩の脅威として、①物理的持ち出しによる情報漏洩、②外部通信による情報漏洩、③出張時の通信からの情報漏洩を想定している。（別添１参照）

物理的持ち出しによる情報漏洩とは、管理区域内の執務室等に設置された情報システムから、管理区域外に通信以外の方法でデータが持ち出されることであり、例としては、情報システムから電磁的記録媒体にデータを書き出し、当該電磁的記録媒体を物理的に管理区域外に持ち出すことが挙げられる。

次に、外部通信による情報漏洩とは、管理区域内の執務室等に設置された情報システムから、管理区域外に通信によってデータが送出されることであり、例としては、オープン系システムの端末からインターネットに情報が送信されることが挙げられる。

また、出張時の通信からの情報漏洩とは、出張先から本府省庁に通信を行う場合に通信経路上で情報を窃取されることである。出張時には、出張者と本府省庁間で機密性の高い情報の送受信が発生しうるところ、当該送受信を可能な限り安全に行うための基準についても例外的な措置として設けることとした。

第３　対策ポイント

守るべき情報及び対象となるシステム、そして想定される脅威について整理した上で、必要と考えられる措置を６項目にまとめ、各項目ごとに漏洩防止のための対策ポイント及び事後調査のための対策ポイントを設定した（下表及び別添２参照）。漏洩防止のための対策ポイントは、データの電磁的記録媒体への書き出しや紙への出力等についてシステム上で強制力を持って制限するこ

とにより、直接的に情報漏洩を防ぐための対策のポイントである。一方、事後調査のための対策ポイントは、データに対して行われた操作等を記録し、事後的に確認することを可能としておくことにより、事案発生時に漏洩の範囲等被害状況を迅速に把握し、適切な事後対応を行うための対策のポイントである。

情報保全システムに必要と考えられる措置は多岐に渡るところ、現時点で最も優先されるべき喫緊の対策は、電磁的記録媒体へのデータの書き出し制限及びログの保存である。インターネットを介した情報漏洩対策について以前から取り組まれているのに比べ、電磁的記録媒体を介した情報漏洩については、昨今の情報漏洩事案の経路になるなど対策が遅れている上、電磁的記録媒体の記憶容量が大きいことから情報漏洩が発生した場合の被害が大きくなるおそれが高い。以上から、電磁的記録媒体へのデータの書き出しを的確に制限することが求められる。ログの保存については、情報漏洩のリスクを完全にゼロにすることが不可能であり、特に情報を管理する立場の者による故意の漏洩に対してはログの検証による事後的追及以外に対策がないため、必須である。また、ログが残ること自体が不正行為に対する抑止力となることも期待される。

＜必要と考えられる措置及び対策ポイント＞（下線は喫緊の課題）

必要と考えられる措置		漏洩防止のための対策ポイント	事後調査のための対策ポイント
1	端末のデータの書き出し対策	電磁的記録媒体への書き出し制限（Ⅰ）	電磁的記録媒体への書き出しログ（ⅰ）
2	印刷・コピー対策	印刷・コピーの制限（Ⅱ）	印刷ログ（ⅱ）
3	電子機器及び紙の持ち出し及び持ち込み対策	電子機器及び紙の持ち出し及び持ち込みの制限（Ⅲ）	入退館等の記録（ⅲ）
4	外部への通信制御	外部への通信制限（Ⅳ）	外部との通信ログ（ⅳ）
5	アクセス制御	アクセス制限（Ⅴ）	個人認証（ⅴ） 端末・サーバ内のアクセスログ（ⅵ） 端末・サーバ間の通信ログ（ⅶ）
6	出張時の通信対策	出張時に使用する端末及び通信回線の制限（Ⅵ）	－

Ⅱ　各論

第１　必要と考えられる措置

個別の措置については別添３参照。

なお、必要と考えられる措置には、システム上の措置だけではなく、システム上の対策が困難なためシステム以外の対策となっているものも含まれている。

１　端末のデータの書き出し対策

総論でも触れたとおり、クローズ系のシステムで管理している機密性の高い情報がその外部に出る契機となるのは、クローズ系の端末から電磁的記録媒体へのデータの書き出しであるから、これについて適切に管理することが極めて重要である。

一方、本来機密性の高い情報を取り扱わないこととしているオープン系のシステムについても、電磁的記録媒体を介して機密性の高い情報が移されるおそれがあり、そうした場合には、オープン系がインターネットを通じた外部への情報流出の経路となる可能性のみならず、オープン系端末から当該情報が更に別の電磁的記録媒体に書き出されてしまう可能性も否定できない。このため、端末から電磁的記録媒体へのデータの書き出しについては、オープン系においてもクローズ系に準じた措置が必要であると考えられる。

端末からのデータの書き出しについては、単に規則で制限し、職員にその遵守を求めるに留まらず、システム上強制力のある制限を行うことが必要である。具体的には、端末から電磁的記録媒体へ書き出す際に自動的に暗号化を行い、

当該媒体のデータは組織外の端末では復号できないようにするなどの措置が想定される。組織外の端末で利用できる形で書き出すことが必要な場合には、管理者の許可を得てこれを行うこととする。

次に、私用の電磁的記録媒体を持ち込み、これにデータを書き出すことも大きなリスクであることから、これについても規則で禁止するだけではなく、システム上であらかじめ登録されていない電磁的記録媒体を検知して使用不可とする措置や、仮に私用の電磁的記録媒体にデータを書き込んだとしても、組織外の端末では利用できないことにする措置などが必要である。

また、日常的に発生する電磁的記録媒体への書き出しが適切に行われていることを事後的に確認可能とするため、電磁的記録媒体へのデータの書き出しに関するログや許可の記録を必要十分な期間保存し、定期的に監査を行うことが求められる。公用の電磁的記録媒体の持ち出しを防止するため、原則として集中保管し、定期的に所在確認を行うことなども必要である。

さらに、書き出したデータのトレーサビリティを確保するため、必要に応じ、電子データに電子透かしを導入すること等について検討することが望ましい。

２　印刷・コピー対策

守るべき情報がクローズ系のシステムの外へ出ていく経路としては、プリンタにより印刷した文書や、それをさらにコピー機により複製した文書が物理的に持ち出されることも挙げられる。印刷物等は、電磁的記録媒体と比較すればその情報量に限りがあるが、プリンタやコピー機は一般に複数の職員が共用しているため、印刷した者が不明確となったり、印刷物の取り忘れが起こるおそ

れがあり、ひいては情報の不要な拡散へとつながる可能性がある。

これらを踏まえ、印刷やコピーについても組織的な管理により、必要な者が必要なだけ行うことを担保することが必要である。システム上は、コピー機やプリンタ等に備えられた認証機能等のセキュリティ機能を活用するほか、印刷に関するログや許可の記録を必要十分な期間保存し、定期的に監査を行うことが求められる。

また、必要に応じ、監視カメラの設置や複製防止用紙の利用、持ち出し防止タグの取付け等についても導入を検討することが望ましい。

３　電子機器（ＰＣ、携帯電話、カメラ、電磁的記録媒体等）及び紙の持ち出し及び持ち込み対策

守るべき情報が外部に流出する場合の経路として、外部との通信のほか、当該情報が記録された電子機器や紙が物理的に管理区域外に持ち出されることが考えられる。これを防止するためには、電子機器及び紙の持ち出し及び持ち込みを制限する必要がある。

職員については、あらかじめ許可された電子機器以外は持ち込み禁止とし、抜き打ち検査等によって抑止力を持たせるほか、ＩＤカード等による入退館、入退室の管理を適切に行う必要がある。また、電子機器及び紙の持ち出しについては、必要に応じ、特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に持ち出し防止タグを貼付し、庁舎の出入り口等において検知する機能を備えることについて検討することが望ましい。

一方、保守業者等がサーバ室等に立ち入り、保守等の作業を行うことが避け

られないところ、保守業者等のサーバ室等への出入りや電子機器の持ち込みについても管理する必要がある。

さらに、電子機器の持ち込み、入退館及び入退室の記録やログを必要十分な期間保存し、定期的に監査を行うことが求められる。

４　外部への通信制御

総論でも触れたとおり、インターネットと接続されているオープン系システムについては、外部との通信によって職員の意図と関係なくデータが不正に送出されるおそれがある。このため、業務に必要な通信のみを許可し、不必要な通信を制限することとともに、通信のログを必要十分な期間保存し、定期的に監査を行うことにより情報漏洩を防止する必要がある。

５　アクセス制御

情報保全においては、「Need to Know」の原則の徹底が不可欠であるところ、システム上はアクセス制御がその基盤となるものである。

個人認証については、データに対する操作を行った本人を事後的に特定できることを担保する必要があり、あらかじめ登録された本人のみがログインできる生体認証方式の採用等が求められる。また、ユーザーがファイルを作成する際にアクセス制限を自動的にかける仕組みを導入するなど、アクセス制限を確実に実施する必要がある。

また、個人認証ログ、端末・サーバ内のアクセスログ、端末とサーバ間の通信ログ等を必要十分な期間保存し、定期的に監査を行うことが求められる。

６　出張時の通信対策

出張者と本府省庁間で特に機密性の高い情報の送受信を業務上やむを得ず行う場合には、出張者が使用する端末においては常時暗号化を講じた通信回線を使用すること及び当該端末については紛失等に備え、ハードディスクの暗号化等を行っておくことが必要である。

７　その他

上記１から６の中には整理していないが、定期的な監査等を行うための体制整備や訓練の実施、委託先における情報の取扱いの管理や、印刷物の廃棄方法、ログの改ざんへの対策など、これまでに述べた諸対策の実効性を高めるための対策は多岐に渡っている。これらについても必要に応じて実施すべきことは言うまでもない。

また、無線ＬＡＮについては、暗号を破る技術が年々進化しているため、専門家の意見を聞きながらセキュリティ対策の更新を随時行わなければ、安全性を確保することは難しい。また、無線ＬＡＮを導入するに当たっては、無線ＬＡＮが使用不可能となった場合を想定して、有線通信等を用いた代替手段を備えておく必要がある。

第２　将来想定される脅威

情報保全に関わる電子機器や技術は多岐に渡り、これらに関連する将来の脅威として多様なものが想定されうるところ、最近社会的に利用が拡大し、近い

将来、特に機密性の高い情報の漏洩防止等の観点から対応を検討する必要性が高いものとして、以下のものが挙げられる。さらに、技術的進歩の速度を踏まえると、今後新たな技術を悪用した脅威に晒されるおそれは十分にあることから、特に機密性の高い情報を取り扱う政府機関においては、常に関連する情報の収集及び分析を行い、途切れることなく適時適切に対策をとっていく必要がある。

○　スマートフォン

現在普及が進んでいるスマートフォンについては、ユーザーによるソフトウェアのインストールを制限することが困難であるなどの問題がある。機密性の高い情報を取り扱う場合は、こうしたスマートフォンの機能や脆弱性などを踏まえ、使用を制限する又はその安全性を十分に確保するための特段の措置をとるなどの対応を検討する必要がある。

○　クラウドコンピューティング

クラウドコンピューティングには、海外サーバを利用する場合の情報保全上のリスク、大量の演算を安価に行うことができるようになることにより暗号解読の可能性が高まるリスク、特定の業者を使い続けないと業務が継続できなくなるリスクなども指摘されており、その安全性が十分に確保されるまでは、機密性の高い情報の取り扱いに関し、使用を制限するなどの対応を検討する必要がある。

おわりに

特に機密性の高い情報を取り扱う政府機関の情報保全システムの確立は、我が国を取り巻く現下の厳しい情勢にかんがみれば、まさに喫緊の課題である。

当会議としては、政府において、本報告書の内容を十分踏まえつつ、①守るべき情報が確実に保護されるシステムとすること、②運用面に過度の負担を与えることのないシステムとすること、③万一情報漏洩等の事案が発生した際は、迅速かつ適切な事後対応が可能なシステムとすることの３点を基本とし、国家と国民の発展に資する情報保全システムに必要と考えられる対策が速やかに進められること、及びその進捗状況が適切にフォローアップされることを強く期待するものである。