第2回研究会主なご意見等について（1/4）

資料1

ポリシーガイド関連

項	分類	ページ	構成員ご意見	ご意見の取り込み方法
1	リスク分析	ポリシー P10,88	「高度サイバー攻撃対処のためのリスク評価等のガイドライン」についても参照すべき。	「1.6.4 リスク分析の実施」及び「標的型攻撃(解説)」にガイドラインを参照することを追記いたしました。
2	用語	ポリシー P23	電磁的記録媒体： 電子計算機や通信回線装置に内蔵される内蔵電磁的記録媒体が含まれていないので、追記すべき。 また、DLTは磁気テープなどの方がよいのではないか。	統一基準の記述に合わせて変更いたしました。
3	組織体制	ポリシー P27	図表11： CIOとCISO間の線は違和感がある（兼務しているというのであれば分かるが）。 CISOから統括情報セキュリティ責任者に指示することもあるはずなので、見直してほしい。	CISOから統括情報セキュリティ責任者に指示する形に修正いたしました。
4	組織体制	ポリシー P29	(9)情報セキュリティに関する統一的な窓口の設置 「…核となる体制を既存の仕組み等を活用する…」 →「…核となる体制を危機管理等の既存の仕組みを活用する…」に変更してはどうか。	ご意見のとおり修正いたしました。
5	外部委託（クラウドサービス等）	ポリシー P38	(6)庁舎外への機器の設置 国際的な情報セキュリティの第三者認証の具体例が欲しい。	「…、ISO/IEC27001認証等の国際的な情報セキュリティの第三者認証制度の取得状況等によって確認する。」の文言を追記いたしました。
6	最新法令対応（番号法）	ポリシー P44	番号法を見据えた対策として以下を盛り込むことが必要。 ・二要素認証 ・モニタリング ・監査 ・標的型攻撃対策	モニタリング(3.6.5)、監査(3.9.1)、標的型攻撃対策(3.6.5)に盛り込み済み。 二要素認証については追記いたしました(3.4.4に追記)。
7	支給以外の端末	ポリシー P50	②支給以外のパソコンやモバイル端末等の業務利用 「やむを得ず支給以外の…」以下が非常に長く分かりにくい。	ご意見をふまえ、箇条書きに変更いたしました。 「原則禁止とする。やむを得ず支給以外の端末を使用する場合は以下の対策を実施することが必要である。 ・XXXXXXX ・XXXXXXX」

第2回研究会主なご意見等について（2/4）

項￥	分類	ページ	構成員ご意見	ご意見の取り込み方法
8	外部委託（クラウドサービス等）	ポリシー P65	（8） 「なお」以降の文中の「高度なセキュリティ対策を行う必要がある」が抵抗感がある。外で実施するときと内で実施するときに、いずれも高度なセキュリティ対策をとる必要があるのではないか。	「高度な」を具体例を踏まえて以下のように修正いたしました。 「…VPN接続による通信経路の暗号化や本人認証等の高度なセキュリティ対策を行う必要がある。」
9	ネットワークの利用	ポリシー P72	（注4） 公衆無線LANに限定しない方がよいのでは。 「なお、その場合でも基幹系のネットワークへのアクセスは禁止とし、電子メールやグループウェア等へのアクセスに限定することが求められる。」は削除したほうがよいのではないか。等。	ご意見を踏まえ、「なお」以下を削除し、利用する場合のセキュリティ対策を追記いたしました。 「（注４）庁外から庁内のネットワークや情報システムにアクセスする際に公衆無線LAN等の庁外通信回線を利用することは原則禁止であるが、やむを得ず利用する場合は、統括情報セキュリティ責任者の許可を得た上で、必要最小限の範囲のみのアクセスとする。さらに、アクセスログを取得し、不正なアクセスがないかを定期的に確認することが求められる。」
10	標的型攻撃	ポリシー P86	−P86 (6)標的型攻撃 メールに注意する、事後対策としてのログの確認についても記述が必要。 ①電磁的記録媒体に対する対策例②ネットワークに対する対策例だけでは、技術的対策に偏りすぎているため、人的対策も必要、という形で書いたらどうか。	標的型攻撃メール対策を中心とした人的対策について追記を行い、人的対策、技術的対策（技術的な入口対策、不正な振る舞いを検知する内部対策、ログ取得等の事後対策）の形といたしました。
11	外部委託	ポリシー P102	・ポリシー102ページ例文1③「クラウドサービスを利用して外部に情報を保存する場合は」を、「クラウドサービスを利用する場合は」に変更する。また、「確保されている保管場所を保存するサービス」を「確保されているサービス」に変更する。	ご意見のとおり修正いたしました。
12	外部委託（サプライチェーンリスク等）	ポリシー P106	⑧再委託に関する制限事項の遵守 (注8)ICTサプライチェーン ・サービス利用は今後増えてくるし、再委託同様契約が問題となる。 ・ASPサービスガイドにそのあたりが記載されていればよいがNISCの方針が今年度中に出る模様。 ・ICTサプライチェーンには、電気・ガス等の広義の意味も入って来るので、どの観点なのか明記した方がよい。（ここでは狭義の意味と考えられる）。	NISCの方針を参照することを追加いたしました。 「…詳細については、「○○○」（平成○年○月　内閣サイバーセキュリティセンター）を参照されたい。」

第2回研究会主なご意見等について（3/4）

監査ガイド関連

項	分類	ページ	構成員ご意見	ご意見の取り込み方法
1	監査手順準備	監査 P12	図表2.2 ポリシーの図表11の変更に合わせるべき。 セルフチェック、内部監査、外部監査というストーリーの中で、このガイドがどこで使うものなのか位置づけを書いた方がよいのではないか。	ポリシーの図表11の変更に合わせ、図表2.2を修正いたしました。 ガイドをどこで使用するものかという点について、「1.3 情報セキュリティ監査の意義と種類 (2)内部監査と外部監査」を補足する形で、追記を行い（P4）、図表1.1（P5）を追記いたしました。
2	フォローアップ監査	監査 P25	-P25 フォローアップ監査 重要なのに少ししか触れられていない。	フォローアップ監査の実施方法により、どのような観点が必要なのかを具体的に追記し、フォローアップ監査の必要性を強調するよう、修正いたしました。
3	外部監査人の調達	監査 P26	監査を外部委託する際は、外部委託事業者が適切に監査できることを担保するために、外部委託事業者の監査の質に関する基準が必要ではないか。	監査プログラム責任者の責任に外部委託事業者の監査の質に関する要件を追記いたしました。
4	監査項目	監査項目82	監査項目「パソコン、モバイル端末及び電磁的記録媒体を用いる場合」を「パソコン、モバイル端末及び電磁的記録媒体を用いる、あるいは庁内ネットワークに接続する場合」に変更する。 ・許可基準が必要である。	ご意見のとおり修正いたしました。
5	監査項目	監査項目83	監査項目「パソコン、モバイル端末及び電磁的記録媒体を庁内ネットワークに接続する場合」を「パソコン、モバイル端末及び電磁的記録媒体を庁内ネットワークに接続することを許可する場合」に変更する。 ・「□ 私物パソコン等ネットワーク接続許可申請書/承認書」を追加してはどうか。	ご意見のとおり修正いたしました。
6	監査項目	監査項目216	・システム部門向けの確認内容を記述すべき ・「システム部門がNo.209～215を管理しているか？」というような記述がよいのではないか。 ・記述例：公衆回線の接続口が、以下の対策を実施していることを確認する。 -許可を得ている -アクセス範囲の極小化を実施している -アクセスログの取得と確認を行っている　など	ご意見のとおり修正いたしました。

第2回研究会主なご意見等について（4/4）

項	分類	ページ	構成員ご意見	ご意見の取り込み方法
7	監査項目	監査項目281	・以下の管理策が実施されていることを確認する。 「①技術的な対策」 「②通信事業者への対応の体制」 「③監視の体制」の3つに分けて監査項目を作ってはどうか。	ご意見のとおり修正いたしました。
8	監査項目	監査項目282	・監査項目281と同じご意見。 ※監査実施での確認事項は箇条書きで書く。	ご意見のとおり修正いたしました。
9	監査項目	監査項目 316～318	・監査資料の例に「□ 外部委託事業者選定時の記録」を追加する。	ご意見のとおり修正いたしました。
10	監査項目	監査項目318	・監査実施の例は箇条書きにする。 ・記述例：クラウドサービス事業者の選定に当たっては、No.316～317の他、追加で以下が実施されていることを確認する。 －①：ポリシーガイドから引用 －②：同上 －③：同上	ご意見のとおり修正いたしました。