第３号議案

# 情報セキュリティ監査の実施について

（案）

情報セキュリティの維持・向上を目的とした第３回情報管理会議（平成２８年３月３１日）において策定した平成２８年度の対策推進計画に基づき、平成２８年度の情報セキュリティ監査を、以下のとおり、実施することとする。

１．　情報セキュリティ監査の実施概要

情報セキュリティ監査は内閣サイバーセキュリティセンター（ＮＩＳＣ）が各省庁に対して実施している監査に準じたものとし、マネジメント監査とペネトレーションテストで構成する。

２．　期間

平成２８年１１月～平成２９年２月

３．　実施方法

外部委託により実施。入札方法については以下のとおり。

（１）調達方法

一般競争入札（最低価格落札方式）

（２）入札スケジュール

| | |
|---|---|
| 平成２８年　９月１４日（水） | 公告 |
| 平成２８年　９月２１日（水）１０時開始 | 入札説明会 |
| 平成２８年　９月２７日（火）１７時迄 | 入札に関する問い合わせ締切 |
| 平成２８年　９月２９日（木）迄 | 問い合わせに対する回答を公表 |
| 平成２８年　１０月５日（水）１５時必着 | 入札締切 |
| 平成２８年　１０月１１日（火）迄 | 落札結果通知 |
| 平成２８年　１０月２６日（水） | 落札者との契約締結 |

（３）入札説明書（仕様書含む）

入札説明書は、別紙入札説明書一式の通り。なお、公告時にウェブサイト上で開示する。

（４）落札者の決定

開札の実施および落札者の決定は、総務部長が行うこととする。なお、落札者との契約締結にあたっては、別途、理事会にて議決をする。

以　上

【添付資料】

別紙１　入札説明書一式

（内訳：入札説明書、入札仕様書、適合証明書、質問票）

別紙１

# 電力広域的運営推進機関
# 情報セキュリティ監査業務委託
# 入札説明書

電力広域的運営推進機関

平成２８年９月

1　業務名

電力広域的運営推進機関　情報セキュリティ監査業務委託

2　調達方式

一般競争入札（最低価格落札方式）で行う。

3　入札

3.1　入札資格

（1）平成２８・２９・３０年度の競争参加資格（全省庁統一資格）の「役務の提供等」において、Ｃ等級以上に格付けされており、関東・甲信越地域の資格を有する者であること。

（2）入札説明会に参加した者であること。

（3）各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止を受けていない者であること。

（4）予算決算及び会計令(昭和 22 年勅令第 165 号)第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

（5）予算決算及び会計令第 71 条の規定に該当しない者であること。

（6）会社更生法（平成 14 年法律第 154 号）に基づく更生手続開始の申立て又は民事再生法（平成 11 年法律第 225 号）に基づく再生手続開始の申立てがなされている者でないこと（但し、会社更生法に基づく更生手続開始の申立て又は民事再生法に基づく再生手続開始の申立てがなされている者で、手続開始の決定後、競争参加資格の再認定を受けている者を除く。）。

（7）自己、自社若しくはその役員等（注 1）が、暴力団員による不当な行為の防止等に関する法律第 2 条に定める暴力団、暴力団員又はその他反社会的勢力（注 2）でない者であること。

（注１）取締役、監査役、執行役、支店長、理事等、その他経営に実質的に関与している者。

（注２）暴力団準構成員、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団、暴力団又は暴力団員と社会的に非難されるべき関係を有する者、暴力団員でなくなった時から 5 年を経過しない者等、その他これに準じる者。

（8）破壊活動防止法に定めるところの破壊的団体およびその構成員でない者であること。

（9）経済産業省が公表している平成 27 年度「情報セキュリティ監査企業台帳」において以下に定める項目（5 項目）に該当すること。

I.　「IT 関連業務内容」に、「セキュリティ監査」を登録していること。

II.　「セキュリティ関連業務」に「リスク評価／脆弱性評価サービス」及び「情報セキュリティ監査（助言型）」を登録していること。

III.　「セキュリティ監査対象の分野・業種」に「公務（官公庁・自治体 等）」を登録していること。

IV. 「取得している監査関連」の認証に「ISMS 適合性評価制度」を登録していること。

V. 「前年度の情報セキュリティ監査の実績」に「助言型監査-企業外監査(官公庁・自治体)」として 1 件以上の実績があること。

(10) 監査の第三者性を担保するため、本機関の「OA システム」、「スイッチング支援システム」、「広域機関システム」に関わる業務（企画、設計、開発、構築、運用、保守又は支援のいずれかに関する業務）の受注者でないこと。また、受注者の関係事業者及び関係会社等ではないこと。

(11) 監査人のうち 1 名を監査責任者とし、監査責任者は以下の資格のいずれかを保持していること。

I. 特定非営利活動法人日本セキュリティ監査協会 (JASA) が認定する公認情報セキュリティ主任監査人又は公認情報セキュリティ監査人

II. 経済産業大臣が認定するシステム監査技術者

III. 特定非営利活動法人日本システム監査人協会(SAAJ)が認定する公認システム監査人(CSA)

IV. 情報システムコントロール協会(ISACA)が認定する公認情報システム監査人(CISA)

3.2 入札説明会の実施

下記日時で入札説明会を実施する。入札を希望する者は参加すること。

日　　時：平成 28 年 9 月 21 日（水）10 時 00 分～（60 分程度）

場　　所：東京都江東区豊洲 6-2-15

電力広域的運営推進機関

参加資格：上記 3.1 の入札資格を満たす者

そ の 他：・入札を希望する事業者は必ず参加すること(不参加の場合は入札できないものとする)

・参加人数は各社 2 名までとする

・受付にて名刺を 1 枚提出すること

3.3 入札方法

平成 28 年 10 月 5 日（水）15 時必着で以下書類を郵送または持参すること。

（1）提出書類

・全省庁統一資格 資格審査結果通知書(写)

・入札資格(9)を証明する「平成 27 年度情報セキュリティ監査企業台帳」の該当部分(写)

・契約書(案)

・適合証明書

・見積もり書(別途封入すること)

（2）提出先

〒135 - 0061

東京都江東区豊洲 6-2-15

電力広域的運営推進機関　総務部経理グループ　情報セキュリティ監査業務委託入札係

3.4　入札保証金及び契約保証金

免除

3.5　落札者の決定

予定価格の制限の範囲内で最低の価格をもって申込みをした者を落札者とする最低価格落札方式とする。ただし、落札者となるべき者の入札価格によっては、その者より当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の制限の範囲内の価格をもって入札した他の者のうち、最低価格をもって入札した者を落札者とすることがある。

3.6　落札結果の通知

平成 28 年 10 月 11 日（火）までに、入札者に対して落札結果を通知する。

3.7　入札の無効

本公告に示した一般競争入札参加資格のいずれかを欠く者のした入札、入札までに不渡手形または不渡小切手を出す等、履行能力を認められない者が行った入札、提出資料に虚偽の記載をした者のした入札及び入札に関する条件に違反した入札は無効とする。

4　業務委託期間

平成 28 年 11 月初旬　から　平成 29 年 2 月末

5　納入物

(ア)監査実施計画書

(イ)監査通知書

(ウ)監査調書

(エ)監査報告書

(オ)監査報告書概要

6　完了期限(納入物の提出期限)

平成 29 年 2 月 28 日(火)

7　検収条件

納入物の検査合格(納入物の内容が本契約の内容に適合していると判断された場合)をもって、検収

とする。

8　支払条件

検収後、60 日以内に支払いする。

9　見積条件

・見積金額には本契約の履行に関して必要な一切の費用を含めること

・見積書には入札金額の総額および内訳(入札仕様書の 4.1.1 から 4.3 までそれぞれの工数がわかるようにすること。さらに細分化しても可。)を必ず記載すること

・見積書には記名押印のうえ提出すること

※尚、必要に応じて見積金額の算定根拠を明示していただく場合があります

10　秘密保持及び個人情報の保護

本入札に際して知り得た広域機関の業務上、技術上の秘密及び情報（個人に関する情報含む）を目的外使用しないこと。また、第三者に漏えいしないこと。

11　特記事項

（1）　本説明書及び入札仕様書に記載されている事項について不明な点は、平成 28 年 9 月 27 日（火）17 時までに下記問い合わせ先へ電子メールで問い合わせることとする。問い合わせへの回答は、平成 28 年 9 月 29 日（木）までに電力広域的運営推進機関ウェブサイトの本入札公告上に開示する。

問い合わせ先：keiyaku@occto.or.jp

ウェブサイト：http://www.occto.or.jp/oshirase/chotatu/index.html

（2）　本説明書に記載のない事項及び疑義については、協議のうえ決定することとする。

（3）　本入札結果については、落札者との契約締結後、原則として、契約相手方、契約締結日及び契約金額等の契約の概要を公表することとする。

以上

別紙１

# 電力広域的運営推進機関
# 情報セキュリティ監査業務委託
# 入札仕様書

電力広域的運営推進機関

平成 28 年 9 月

1　目的

電力広域的運営推進機関（以下「本機関」という。）の各組織及び各情報システムにおいて適切な情報セキュリティの管理又は対策が実施されているかについて、第三者の立場から確認及び必要な助言を行い、本機関における情報セキュリティを維持向上させることを目的とする。

2　基本方針

本入札における情報セキュリティ監査は、セキュリティ対策強化のための体制・制度が機能しているかの検証による監査（以下「マネジメント監査」という。）と本機関の情報システムに対する疑似的攻撃による監査（以下「ペネトレーションテスト」という。）の 2 本立てで監査を行うこととする。

3　業務委託内容

受託者は、以下に示す情報セキュリティ監査業務を、公正かつ客観的な立場で実施すること。なお、監査は助言型監査とする。

監査業務の実施にあたっては、「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）（平成 28 年 8 月 31 日策定）」（以下「政府統一基準」という。）、及び本機関が定める情報セキュリティ関連規程(以下「情報セキュリティ関連規程」という。）の内容を理解したうえで監査を実施すること。

監査実施の結果、不適合の箇所等があった場合、具体的かつ適切な助言をするとともに、不適合となる明確な事由等がある場合は提示すること。

3.1　マネジメント監査

3.1.1 政府統一基準と情報セキュリティ関連規程との準拠性に関する監査

情報セキュリティ関連規程が政府統一基準に準拠していることの確認を行う。

3.1.1.1 対象となる情報セキュリティ関連規程

(1)情報管理規程

情報管理体制、情報区分について定めた規程である。

(2)情報セキュリティ対策規程

情報システム全体において具体的なセキュリティ対策について定めた規程である。

(3)OA システムの運用細則に関する規程

役職員が日常業務で利用するメール、ファイルサーバ、イントラネット等を提供する OA システムに関して個別具体的な運用を定めた規程である。

(4)スイッチング支援システムの運用細則に関する規程

本機関の会員に提供しているスイッチング支援システムに関して個別具体的な運用を定めた規程である。

(5)EB システムの運用細則に関する規程

銀行が提供するオンラインバンキングシステムの利用に関して個別具体的な運用を定めた規程である。（１０月以降施行予定）

3.1.2 情報セキュリティ関連規程と被監査部門の運用との準拠性に関する監査

本機関の被監査部門における実際の運用が、情報セキュリティ関連規程に準拠しているかの確認を行う。具体的には、関連文書の調査、被監査部門からのヒアリング調査を行うほか、必要に応じ、情報セキュリティの技術的対策の実施状況についてシステムの目視、事務所内の観察等を行う。

3.1.2.1 対象となる被監査部門

以下の部門ごとに情報管理責任者(計 6 名)を設置しているため、それぞれ 2 時間程度のヒアリング調査は必須とする。

(1)総務部

(2)企画部

(3)計画部

(4)運用部

(5)紛争解決対応室

(6)監査室

3.1.2.2 対象となる情報システム

以下のシステムごとにシステム管理者(兼務があるため計 2 名)を設置しているため、それぞれ 2 時間程度のヒアリング調査は必須とする。

(1)OA システム

(2)スイッチング支援システム

(3)EB システム

3.2　ペネトレーションテスト

3.2.1 インターネット経由での診断

ルーター、スイッチ、ファイアウォール、サーバや OS、各種サービス等プラットフォームに対する診断を対象とし、SQL インジェクションなどに代表される Web アプリケーション診断は対象外とする。ツールによる診断に加えて、診断の網羅性や精度を向上させるためにセキュリティ有識者による手作業での検査を実施すること。

3.2.1.1 対象となる情報システムとグローバル IP

別紙のとおり。※入札説明会で配布する。

3.2.1.2 診断項目

以下の通りとし、DDoS 攻撃耐性診断は対象外とする。なお、必要に応じて受託者にて診断項目を追加してもかまわない。

(イ)インターネット側からの攻撃によるサーバへの侵入可否の検証という観点

ホスト存在確認

ポートスキャン

サービス稼働状況確認(バックドア等不要なサービスの確認含む)

脆弱性検出

サーバ(Web/メール/DNS/Proxy など)のセキュリティ設定上の不備確認

認証試行

(ロ)侵入できた場合の管理者権限の昇格可否の検証という観点

エクスプロイトコード(攻撃コード)を利用したアクセス権限取得、権限昇格可否の確認

脆弱性を組み合わせた複合的な要因での問題検出

踏み台としてほかのサーバを攻撃される可能性確認

3.2.2 オンサイトでの診断

本機関の新豊洲事務所に診断機材を持ち込み、無線 LAN の脆弱性を診断する。

3.2.2.1 対象となる無線 LAN

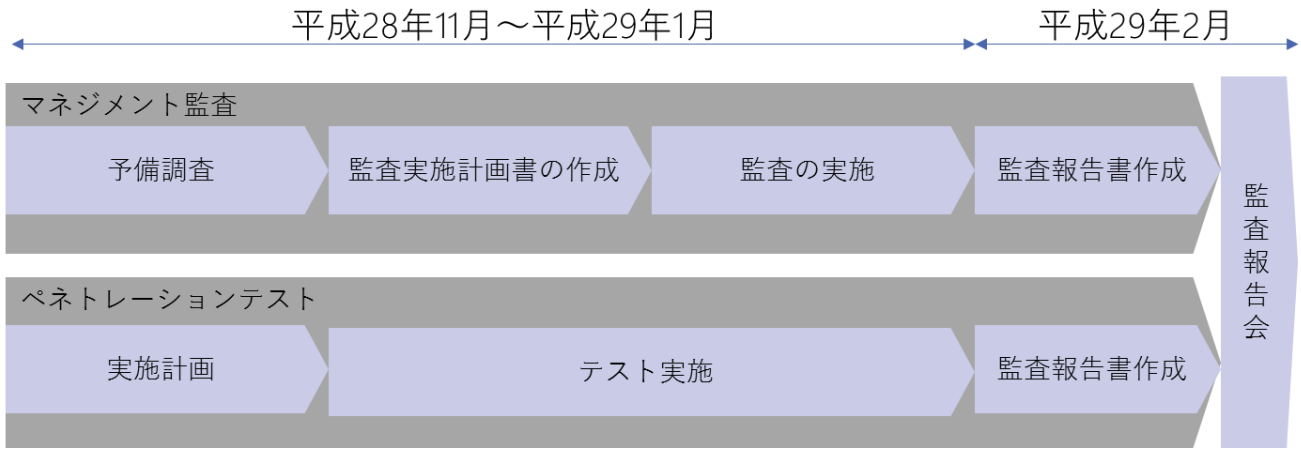
別紙のとおり。※入札説明会で配布する。

3.2.2.2 診断項目

フロア内の不正 AP 検出、正規 AP への侵入可否判定を行う。

## 4 進め方

「3 業務委託内容」にて記述した業務については、以下図の進め方に従うこととする。




### 4.1 マネジメント監査

#### 4.1.1 予備調査

以下の通り予備調査を行い、監査計画作成の準備を行う。

(1)政府統一基準、情報セキュリティ関連規程の内容を把握する。

(2)本機関の組織体制やシステム構成等の内容を把握する。

(3)対象システムの概要を把握し、必要により設計書、運用ルール等を把握する。

4.1.2 監査実施計画書の作成

本機関担当者と打ち合わせを行い、以下の項目を含む監査実施計画書を作成する。

(1)監査目的

(2)監査対象

(3)被監査部門、その責任者及び担当者

(4)監査手法

(5)監査の判断の尺度とする基準

(6)監査実施概要

(7)監査実施責任者及び実施担当者の体制

(8)監査実施スケジュール

(9)監査実施場所

(10)その他必要と思われる項目

また、被監査部門に監査の実施内容、スケジュール、準備事項等を事前に通知するため、必要事項を記載した監査通知書を作成する。

4.1.3 監査の実施

監査実施計画書に従い、必要な監査を実施し監査調書を作成する。監査調書には次の項目を含むこと。

(1)件名、作成日、監査責任者名

(2)監査実施日、監査実施場所及び監査項目

(3)被監査部門名及び被監査部門対応者

(4)監査詳細項目、監査資料名、監査手法及び監査結果（課題の有無及び内容）

(5)検出事項とその影響度

(6)所見

4.1.4 監査報告書作成

実施した監査に関する全ての事項について、正確かつ漏れなく必要な事項を整然と分かるように工夫して結果を取りまとめ、以下の事項を含む監査報告書を作成すること。また、監査報告書の概要版も作成すること。

(1)監査実施期間

(2)監査対象範囲

(3)監査の基準

(4)総合的所見

(5)監査意見

(6)不適合となった個所に関する想定されるリスク及び具体的な助言

(7)遵守事項の整備状況の妥当性及び運用状況の準拠性に関する監査を実施した旨及びその結果

4.2　ペネトレーションテスト

4.2.1 実施計画

稼働中のシステムに対する診断を含むこと、また受託者側の対応キャパシティも考慮する必要があることから、受託者と本機関の担当者とで診断内容、診断実施日、時間帯を調整する。

4.2.2 テスト実施

マネジメント監査と並行して平日日中帯に実施することとする。なお、実施中に危険度が高い脆弱性で早急な対応が必要と思われる個所が発見された場合、緊急速報として、発見された脆弱性と推奨する対策を簡単にまとめたものをメールで送信すること。緊急速報は診断後翌営業日以内を目標に送信すること。

4.2.3 監査報告書作成

テストの結果を分析し、以下の事項を含む監査報告書を作成すること。また、監査報告書の概要版も作成すること。

(1)発見された脆弱性

(2)脆弱性詳細

(3)リスク

(4)具体的な対策案

4.3　監査報告会

本機関の役員向け報告会及び担当者向け報告会の 2 つを開催する。

前者は監査報告書の概要版に基づいて行うこととし、10 分程度にまとめること。

後者の日程は本機関の担当者と調整する。

5　その他

① 本業務のペネトレーションテストに必要な診断機器、診断ツール類、設定費用、インターネット回線通信費等は本契約に含めるものとする。

② 本業務について、作業場所や作業端末等は受託者にて確保するものとする。

③ 本仕様書に記載の事項は、本入札のために限り使用することとし、目的外使用や第三者への漏えいをしないこと。

④ この仕様書に定めのない事項について必要のある時は、委託者と受託者が都度協議し、決定するものとする。

以　上

別紙1

御社名

㊞

# 適合証明書

| 区分 | 入札説明書記載箇所 | 機能 | 適合※1 | 補足※2 |
|---|---|---|---|---|
| 入札資格 | 3.1（1） | 平成２８・２９・３０年度の競争参加資格（全省庁統一資格）の「役務の提供等」において、Ｃ等級以上に格付けされており、関東・甲信越地域の資格を有する者であること。 | | |
| | 3.1（2） | 入札説明会に参加した者であること。 | | |
| | 3.1（3） | 各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止を受けていない者であること。 | | |
| | 3.1（4） | 予算決算及び会計令(昭和22年勅令第165号)第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。 | | |
| | 3.1（5） | 予算決算及び会計令第71条の規定に該当しない者であること。 | | |
| | 3.1（6） | 会社更生法（平成14年法律第154号）に基づく更生手続開始の申立て又は民事再生法（平成11年法律第225号）に基づく再生手続開始の申立てがなされている者でないこと（但し、会社更生法に基づく更生手続開始の申立て又は民事再生法に基づく再生手続開始の申立てがなされている者で、手続開始の決定後、競争参加資格の再認定を受けている者を除く。）。 | | |
| | 3.1（7） | 自己、自社若しくはその役員等（注1）が、暴力団員による不当な行為の防止等に関する法律第2条に定める暴力団、暴力団員又はその他反社会的勢力（注2）でない者であること。<br>（注１）取締役、監査役、執行役、支店長、理事等、その他経営に実質的に関与している者。<br>（注２）暴力団準構成員、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団、暴力団又は暴力団員と社会的に非難されるべき関係を有する者、暴力団員でなくなった時から5年を経過しない者等、その他これに準じる者。 | | |
| | 3.1（8） | 破壊活動防止法に定めるところの破壊的団体およびその構成員でない者であること。 | | |
| | 3.1（9） | 経済産業省が公表している平成27年度「情報セキュリティ監査企業台帳」において以下に定める項目（5項目）に該当すること。<br>I.「IT関連業務内容」に、「セキュリティ監査」を登録していること。<br>II.「セキュリティ関連業務」に「リスク評価／脆弱性評価サービス」及び「情報セキュリティ監査（助言型）」を登録していること。<br>III.「セキュリティ監査対象の分野・業種」に「公務（官公庁・自治体 等）」を登録していること。<br>IV.「取得している監査関連」の認証に「ISMS適合性評価制度」を登録していること。<br>V.「前年度の情報セキュリティ監査の実績」に「助言型監査-企業外監査(官公庁・自治体)」として1件以上の実績があること。 | | |
| | 3.1（１０） | 監査の第三者性を担保するため、本機関の「OAシステム」、「スイッチング支援システム」、「広域機関システム」に関わる業務（企画、設計、開発、構築、運用、保守又は支援のいずれかに関する業務）の受注者でないこと。また、受注者の関係事業者及び関係会社等ではないこと。 | | |
| | 3.1（１１） | 監査人のうち1名を監査責任者とし、監査責任者は以下の資格のいずれかを保持していること。<br>I. 特定非営利活動法人日本セキュリティ監査協会（JASA）が認定する公認情報セキュリティ主任監査人又は公認情報セキュリティ監査人<br>II. 経済産業大臣が認定するシステム監査技術者<br>III. 特定非営利活動法人日本システム監査人協会(SAAJ)が認定する公認システム監査人（CSA）<br>IV. 情報システムコントロール協会(ISACA)が認定する公認情報システム監査人(CISA) | | |

※1　適合については，“○（要件を満たしている）”，“△（条件付きで要件を満たしている，代替手段で要件を満たす）”，“×（要件を満たしていない）”で記述をお願いします。また，“△”を記入した場合は，補足欄に説明をご記入ください。

※2　補足すべき事項がある場合は，その内容を補足欄に記入してください。また，添付資料がある場合は同封し提出をお願いします。

「電力広域的運営推進機関　情報セキュリティ監査業務委託」に関する質問等

**別紙1**

| No. | 質問日 | 質問者<br>（会社名，所属，役職，氏名） | 仕様書該当箇所<br>（ページ，項目等） | 質問 |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |