原議保存期間１年 （令和9年３月31日まで）

警視庁刑事部暴力団対策課長
各道府県警察本部組織犯罪対策主管課長
（参考送付）
各管区警察局広域調整担当課長
殿

事務連絡
令和７年１０月３日
警察庁刑事局組織犯罪対策部
組織犯罪対策第一課理事官

総合行政ネットワーク回線又はインターネット回線を利用した暴力団排除等のための部外への情報提供について

暴力団排除等のための部外への情報提供については、「暴力団排除等のための部外への情報提供について（通達）」（令和６年２月26日付け警察庁丙組組一発第26号）により運用されているところであるが、この度、地方公共団体と警視庁又は道府県警察本部との間（以下「照会実施機関間」という。）で文書により行われる暴力団員等該当性情報の照会及び回答（以下「属性照会」という。）について、別添１「情報セキュリティ要件」を全て充足するなど、情報セキュリティの安全性が担保されている場合には、総合行政ネットワーク回線（以下「ＬＧＷＡＮ回線」という。）又はインターネット回線（以下「一般回線」という。）の電子メール機能等を用いた運用を行うことを妨げるものではないと整理したことから、各都道府県警察においては、必要に応じて地方公共団体の照会担当部局と協議を行い、適正な運用に努められたい。

なお、本件に関しては、警察庁長官官房技術企画課と協議済みである。

記

１　属性照会に用いる文書の性質及び取扱い上の留意事項

属性照会に用いる照会書及び回答書（以下「照会文書」という。」は、「警察における情報セキュリティに関する対策基準について（通達）」（令和５年９月28日付け警察庁丙技企発第61号ほか）に規定する機密性２（中）情報に該当する。

よって、照会文書をＬＧＷＡＮ回線や一般回線を用いて送受信する場合には、各都道府県警察で規定する情報セキュリティポリシー上の機密性２（中）情報を送受信する際の要件を充足することはもとより、より安全性を担保した方法で行われる必要がある。

２　使用可能な回線について

照会文書の送受信に用いられる回線については、地方公共団体が整備するＬＧＷＡＮ回線又は都道府県警察が整備した一般回線を利用すること。

３　属性照会の方法

⑴　ＬＧＷＡＮ回線を用いた属性照会

ＬＧＷＡＮ回線を用いた属性照会を行う場合については、同回線で接続された端末（以下「ＬＧＷＡＮ端末」という。）の電子メール機能を用いて、暗号化した照会文書等を送受信する方法又はＬＧＷＡＮ端末内に属性照会業務の関係者であって、照会文書を閲覧する必要がある者以外がアクセスできないようにアクセス制限を設けた共有フォルダを作成し、暗号化した照会文書を当該共有フォルダに蔵置する方法により行うこと。

⑵　一般回線を用いた属性照会

一般回線を用いた属性照会を行う場合については、同回線で接続された端末の電子メール機能を用いて暗号化した照会文書を送受信する方法又は地方公共団体がインターネットを通じたファイルを送受信するためのサービス等を利用して照会文書のダウンロード先を通知する方法により行うこと。

４　ＬＧＷＡＮ回線又は一般回線を用いた属性照会を行う際の留意事項

⑴　ＬＧＷＡＮ回線又は一般回線を用いた属性照会に係る回答内容の制限

一般的に、属性照会の対象者が排除対象者に該当する場合においては、当該回答書に排除対象者の個人情報の他、排除対象となる理由を記載する必要があり、排除対象者に該当しない場合の回答と比べ、より機微な個人情報を提供することになる。

よって、ＬＧＷＡＮ回線又は一般回線を用いて回答を行うことができるものは、属性照会の対象者が排除対象者に該当しない場合に限ることとする。

⑵　暴力団情報の提供に関する申合せ等の見直し

属性照会が､暴力団情報の提供に関する申合せ等に基づいて行われている場合には、照会実施機関間における照会文書の受渡し方法に係る規定の変更及び情報セキュリティを遵守する旨の覚書を締結するなど適切な措置を講ずること。

⑶　照会文書の押印省略及び様式の見直し

ア　照会文書の押印省略

照会文書に押印を必要とする様式である場合には、省略を検討すること。

なお、これまでに警察庁から押印を必要とする照会文書の様式を示している場合であっても、省略は差し支えないものとする。

イ　回答書の見直し

都道府県警察から地方公共団体に対して発出する回答書については、属性照会の実効性を損なわない性質であることはもちろんのこと、個人情報に触れる記載が無いように構成を見直すこと。

５　警察庁との事前協議

ＬＧＷＡＭ回線又は一般回線を用いた属性照会を実施しようとする場合には、別添２「情報セキュリティチェック表」を作成の上、同チェック表及び関係資料を警察庁刑事局組織犯罪対策部組織犯罪対策第一課暴排係宛てに送付し、事前協議を行うこと。

【本件担当】

組織犯罪対策第一課 暴排係（800-723-4412、4482）

企画法令係（800-4425）

別添１

情報セキュリティ要件（ＬＧＷＡＮ利用）

１　情報セキュリティインシデント発生時の措置

都道府県警察本部の暴力団対策を主管する課（以下「暴力団対策主管課長」という。）と地方公共団体照会担当課（以下双方を併せて「照会実施機関」という。）との間（以下「照会実施機関間」という。）で行われる暴力団員等該当性の照会に関して、情報インシデント事案が発生した場合には、双方に速報するものとする。

なお、速報を要する情報セキュリティインシデント事案は、照会実施機関間で行われる照会文書の送受信及び授受に関する

- 情報流出事案
- 照会文書の送受信及び授受に用いる端末（以下「照会利用端末」という。）に関する不正プログラム感染事案、不正アクセス事案、サイバー攻撃事案
- 照会利用端末の不正利用事案
- 個人所有の機器等の不正使用事案（照会文書を個人所有の機器等において不正に処理した事案）
- その他社会的反響が大きいと予想される事案

とする。

２　端末に関する情報セキュリティ要件

(1)　情報漏えい・不正利用対策

ア　照会利用端末は、公費で整備された端末を利用し、指定された端末以外で照会業務を行わないこと。

イ　照会利用端末は指定された場所のみで利用すること。

ウ　照会業務は、照会利用端末でのみ行い、在宅勤務時など庁舎外では行わないこと。

エ　照会利用端末は、セキュリティワイヤーによる固定等の盗難防止対策を行うこと。

オ　照会利用端末の利用者のログイン時の認証方式は、原則として生体認証とする。やむを得ずＩＤ及びパスワードを使用する場合は、強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスワードを使用すること。

パスワードを使用する場合は、知る必要がない者に知られるような状態で放置しないよう適切に管理すること。

カ　照会利用端末のオートログイン機能を無効化すること。

キ　最長で15分間照会端末を操作しない場合は、スクリーンセーバー等により端末がロックされるようにすること。

ク　照会利用端末の画面は、部外者から視認できないよう照会利用端末の設置場所に配意すること。

ケ　照会利用端末を本人以外のユーザーアカウントで使用しないこと。

コ　照会利用端末の管理者と利用者の権限を分離すること。

サ　照会利用端末のユーザーアカウントを分離すること。

ただし、システムの運用上の制約により、やむを得ず利用者に共用アカウントを付与する必要がある場合は、利用者を特定できる仕組みを設

けた上で、共有アカウントの取扱いに関する規定を整備し、その規定に従って付与すること。

シ　照会利用端末の利用者が、情報システムを構成する機器等の改造（新たな機器等の接続、ソフトウェア追加等）を許可なく実施できないこと。

ス　照会利用端末の利用者に対し、端末画面の接写及び情報の持ち出しを禁止する規定が設けられていること。

(2)　不正プログラム対策

ア　照会利用端末には、サポートが終了している又は脆弱性が存在するバージョンのＯＳは利用しないこと。

イ　照会利用端末には、不正プログラム対策ソフトウェアをインストールし、定義ファイル等を常に最新の状態に保つこと。

　不正プログラム対策ソフトウェアの選定にあっては、必要なセキュリティ対策を検討した上で導入する製品等を選定すること。

(3)　セキュリティホール対策

　照会利用端末に導入されているソフトウェアにセキュリティホールが発見されたときは、照会利用端末を管理する者（以下「システム管理者」という。）に情報共有するとともに、速やかにその影響を検討し、必要な措置を講じること。

3　電子メール利用に関する情報セキュリティ要件

(1)　照会に利用するメールアドレスは、照会実施機関間で固定し、当該メールアドレス以外で照会文書の送受信を行わないこと。

(2)　照会に利用するメールアドレスを用意し、当該メールアドレスにアクセス権を付与するなど、照会業務に従事する者以外の者が当該メールアドレスを利用することができない措置を講じること。

(3)　照会に利用するメールアドレスで、照会業務以外のメールの送受信を行わないこと。

(4)　利用するメールアドレスは、当該メールアドレスのドメイン名に行政機関であることが保証されるドメイン名を使用すること。

(5)　電子メールにより照会文書を送信する際には、送付する文書の作成者情報等、当該ファイルから付属する情報を削除するとともに、暗号化を行うなど情報漏えいを防止する対策を講じること。

　また、原則として、警察から送信する照会文書は印字を禁止したＰＤＦとすること。

(6)　照会文書にパスワードを設定して暗号化し、当該パスワードを電子メール以外の方法で伝達するなど、秘匿性を確保すること。

　また、当該パスワードについては、強固なパスワードに必要な十分な桁数（英大文字・英小文字・数字を22文字程度）を備えた第三者に容易に推測できないパスワードを使用し、知る必要がない者に知られるような状態で放置しないよう適切に管理を行い、人事異動の都度変更するなど、定期的な変更を行うこと。

(7)　電子メールにより照会文書を送信したときは、送信後直ちに端末から当該情報を消去すること。

(8)　電子メールにより照会文書を受信したときは、当該情報を確認後、直ちに受信端末から消去すること。

(9)　電子メールにより受信した照会文書を、照会利用端末として指定された端末以外に送信しないこと。

(10) 送受信した照会文書が消去されていることを照会実施機関の上席者によって確認する体制を構築し、少なくとも月に１回以上の確認を行うこと。
(11) 電子メールにより受信した照会文書を、定められた保存先以外に保存しないこと。
　また、受信した照会文書を、庁舎外に持ち出さないこと。
(12) 不審な電子メールを受信した時は、開封せずにシステム管理者に連絡すること。
(13) 電子メールのなりすましの防止策を講ずること。

４　共有フォルダ利用に関する情報セキュリティ要件
(1)　共有フォルダを用いて、照会文書の授受を行う場合は、共有フォルダに、照会文書を閲覧する権限がある者以外の者がアクセスできないようにアクセス制限を設けること。
(2)　共有フォルダ内に蔵置する照会文書は、パスワードによる暗号化を行い閲覧を制限すること。
　パスワードは、強固なパスワードに必要な十分な桁数（英大文字・英小文字・数字を22文字程度）を備えた第三者に容易に推測できないパスワードを使用すること。
　当該パスワードの伝達方法にあたっては、秘匿性を確保すること。
　また、当該パスワードについては、知る必要がない者に知られるような状態で放置しないよう適切に管理を行い、人事異動の都度変更するなど、定期的な変更を行うこと。
(3)　共有フォルダ内に照会文書を蔵置する際には、蔵置する文書の作成者情報等、当該ファイルから付属する情報を削除するとともに、暗号化を行うなど情報漏えいを防止する対策を講じること。
　また、原則として、警察が蔵置する照会文書は印字を禁止したＰＤＦとすること。
(4)　共有フォルダ内に蔵置した照会文書については、照会実施機関において確認後、直ちに端末から当該情報を消去すること。
(5)　共有フォルダに蔵置した照会文書が放置されていないことを照会実施機関の上席者によって確認する体制を構築し、少なくとも月に１回以上の確認を行うこと。
(6)　共有フォルダに蔵置した照会文書を、定められた保存先以外に保存しないこと。
　また、照会文書を庁舎外に持ち出さないこと。

５　ログ管理
(1)　利用者のログインに係るログを５年以上（ログが記録されたときから５年以上とする。）保存（電磁的記録方式による保存とする。以下同じ。）すること。
　また、地方公共団体照会担当課においては、利用者のログインに係るログを３年以上保存すること。
(2)　照会利用端末のメール送受信、共有フォルダへのアクセス及び外部記録媒体の利用に係るログを保存すること。
(3)　(2)のログデータ及び照会文書の印字に係るログを保存すること。
(4)　(1)から(3)までのログは、システム管理者のみが閲覧可能であり、不正な消去、改ざん及び不正なアクセスがなされないように、アクセス制御を行うこと。

別添１

情報セキュリティ要件（インターネット回線利用）

１　情報セキュリティインシデント発生時の措置

都道府県警察本部の暴力団対策を主管する課(以下「暴力団対策主管課長」という。）と地方公共団体照会担当課（以下双方を併せて「照会実施機関」という。）との間(以下「照会実施機関間」という。)で行われる暴力団員等該当性の照会に関して、情報インシデント事案が発生した場合には、双方に速報するものとする。

なお、速報を要する情報セキュリティインシデント事案は、照会実施機関間で行われる照会文書の送受信に関する

- ・情報流出事案
- ・照会文書の送受信に用いる端末（以下「照会利用端末」という。）に関する不正プログラム感染事案、不正アクセス事案、サイバー攻撃事案
- ・照会利用端末の不正利用事案
- ・個人所有の機器等の不正使用事案(照会文書を個人所有の機器等において不正に処理した事案)
- ・その他社会的反響が大きいと予想される事案

とする。

２　サーバに関する情報セキュリティ要件

(1)　ネットワーク環境

サーバを接続するネットワークと他機関のネットワークとの接続部分には、ファイアウォール等を設置し、業務上必要のない通信を遮断していること。

電子メールサーバが電子メールの不正な中継を行わないように設定されていること。

(2)　サーバ間通信の暗号化

電子メールサーバ間にあっては、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、次に掲げる事項を例とする電子メールに関する通信の暗号化を行うこと。

(ア) SMTPによる電子メールサーバ間の通信をTLSにより保護する。

(イ) S/MIME等の電子メールにおける暗号化及び電子署名の技術を利用する。

(3)　不正プログラム対策

サーバには、不正プログラム対策ソフトウェアを導入し、定義ファイル等が常に最新の状態に保たれること。

(4)　セキュリティホール対策

サーバに導入されているソフトウェアにセキュリティホールが発見されたときは、速やかにその影響を検討し、必要な措置を講じること。

３　端末に関する情報セキュリティ要件

(1)　情報漏えい・不正利用対策

ア　照会利用端末は、公費で整備された端末を利用し、指定された端末以外で照会業務を行わないこと。

イ　照会利用端末は指定された場所のみで利用すること。

ウ　照会業務は、照会利用端末でのみ行い、在宅勤務時など庁舎外では行わないこと。

エ　照会利用端末は、セキュリティワイヤーによる固定等の盗難防止対策を行うこと。

オ　照会利用端末の利用者のログイン時の認証方式は、原則として生体認証とする。やむを得ずＩＤ及びパスワードを使用する場合は、強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスワードを使用すること。

　パスワードを使用する場合は、知る必要がない者に知られるような状態で放置しないよう適切に管理すること。

カ　照会利用端末のオートログイン機能を無効化すること。

キ　最長で15分間照会端末を操作しない場合は、スクリーンセーバー等により端末がロックされるようにすること。

　また、地方公共団体照会担当課においては、最長で30分間照会端末を操作しない場合、スクリーンセーバー等により端末がロックされるようにすること。

ク　照会利用端末の画面は、部外者から視認できないよう照会利用端末の設置場所に配意すること。

ケ　照会利用端末を本人以外のユーザーアカウントで使用しないこと。

コ　照会利用端末の管理者と利用者の権限を分離すること。

サ　照会利用端末のユーザーアカウントを分離すること。

　ただし、システムの運用上の制約により、やむを得ず利用者に共用アカウントを付与する必要がある場合は、利用者を特定できる仕組みを設けた上で、共有アカウントの取扱いに関する規定を整備し、その規定に従って付与すること。

シ　照会利用端末の利用者が、情報システムを構成する機器等の改造（新たな機器等の接続、ソフトウェア追加等）を許可なく実施できないこと。

ス　照会利用端末の利用者に対し、端末画面の接写及び情報の持ち出しを禁止する規定が設けられていること。

(2)　不正プログラム対策

ア　照会利用端末には、サポートが終了している又は脆弱性が存在するバージョンのＯＳは利用しないこと。

イ　照会利用端末には、不正プログラム対策ソフトウェアをインストールし、定義ファイル等を常に最新の状態に保つこと。

　不正プログラム対策ソフトウェアの選定にあっては、必要なセキュリティ対策を検討した上で導入する製品等を選定すること。

(3)　セキュリティホール対策

　照会利用端末に導入されているソフトウェアにセキュリティホールが発見されたときは、照会利用端末を管理する者（以下「システム管理者」という。）に情報共有するとともに、速やかにその影響を検討し、必要な措置を講じること。

4　電子メール利用に関する情報セキュリティ要件

(1)　照会に利用するメールアドレスは、照会実施機関間で固定し、当該メールアドレス以外で照会文書の送受信を行わないこと。

(2)　照会に利用するメールアドレスを用意し、当該メールアドレスにアクセ

ス権を付与するなど、照会業務に従事する者以外の者が当該メールアドレスを利用することができない措置を講じること。
(3)　照会に利用するメールアドレスで、照会業務以外のメールの送受信を行わないこと。
(4)　利用するメールアドレスは、当該メールアドレスのドメイン名に行政機関であることが保証されるドメイン名を使用すること。
(5)　電子メールにより照会文書を送信する際には、送付する文書の作成者情報等、当該ファイルから付属する情報を削除するとともに、暗号化を行うなど情報漏えいを防止する対策を講じること。
　また、原則として、警察から送信する照会文書は印字を禁止したＰＤＦとすること。
(6)　照会文書にパスワードを設定して暗号化し、当該パスワードを電子メール以外の方法で伝達するなど、秘匿性を確保すること。
　また、当該パスワードについては、強固なパスワードに必要な十分な桁数（英大文字・英小文字・数字を22文字程度）を備えた第三者に容易に推測できないパスワードを使用し、知る必要がない者に知られるような状態で放置しないよう適切に管理を行い、人事異動の都度変更するなど、定期的な変更を行うこと。
(7)　電子メールにより照会文書を送信したときは、送信後直ちに端末から当該情報を消去すること。
(8)　電子メールにより照会文書を受信したときは、当該情報を確認後、直ちに受信端末から消去すること。
(9)　電子メールにより受信した照会文書を、照会利用端末として指定された端末以外に送信しないこと。
(10) 送受信した照会文書が消去されていることを照会実施機関の上席者によって確認する体制を構築し、少なくとも月に１回以上の確認を行うこと。
(11) 電子メールにより受信した照会文書を、定められた保存先以外に保存しないこと。
　また、受信した照会文書を、庁舎外に持ち出さないこと。
(12) 不審な電子メールを受信した時は、開封せずにシステム管理者に連絡すること。
(13) 電子メールのなりすましの防止策を講ずること。

５　インターネットを通じたファイルを送受信するためのサービス等(以下「ファイル転送サービス」という。）利用に関する情報セキュリティ要件
(1)　ファイル転送サービスを利用して、照会文書のダウンロード先を通知するメールを送信する際には、同メールのメールアドレス（以下、「通知用メールアドレス」という。）を固定するとととともに、それ以外のメールアドレスを使用しないこと。
(2)　通知用メールアドレスは、そのドメイン名が、行政機関のものであることが保証されるものであること。
(3)　ファイル転送サービスにより照会文書を送信する際には、送付する文書の作成者情報等、当該ファイルから付属する情報を削除するとともに、暗号化を行うなど情報漏えいを防止する対策を講じること。
(4)　照会文書は、パスワードを設定して暗号化し、当該パスワードを電子メール以外の方法で伝達するなど、秘匿性を確保すること。
　また、当該パスワードについては、強固なパスワードに必要な十分な桁数（英大文字・英小文字・数字を22文字程度）を備えた第三者に容易に推測できないものを使用して適切に管理し、人事異動の都度変更するなど、定期的な変更を行うこと。

(5)　ファイル転送サービスを利用する場合は、アップロードしたファイルが一定期間後に自動的に消去される仕様となっていること。
(6)　不必要な照会文書がアップロードされたままになっていないことを送信側の上席者によって確認する体制を構築し、少なくとも月に１回以上の確認を行うこと。
(7)　警察がファイル転送サービスを使用する場合には、事前に警察庁に協議すること。

６　ログ管理
(1)　利用者のログインに係るログを５年以上（ログが記録されたときから５年以上とする。）保存（電磁的記録方式による保存とする。以下同じ。）すること。
　また、地方公共団体照会担当課においては、利用者のログインに係るログを３年以上保存すること。
(2)　照会利用端末のメール送受信及び外部記録媒体の利用に係るログを保存すること。
(3)　(2)のログデータ及び照会文書の印字に係るログを保存すること。
(4)　(1)から(3)までのログは、システム管理者のみが閲覧可能であり、不正な消去、改ざん及び不正なアクセスがなされないように、アクセス制御を行うこと。

別添2

LGWANを利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
1　情報セキュリティインシデント発生時の措置						
(1)	1	情報セキュリティインシデントが発生した場合において、照会実施機関間で速報体制が構築されているか	・速報対象となる情報セキュリティインシデントは照会実施機関間で合意がなされているか	□合意がされている □合意がされていない	□合意がされている □合意がされていない	
			・部内での速報先は把握しているか（例～情報システム課〇〇係など）	部内通報先 （　　）	部内通報先 （　　）	
2　端末に関する情報セキュリティ要件						
(1)	2(1)ア	照会利用端末が整備されているか	・照会に用いる端末は公費で整備された端末であるか	□公費整備端末である □公費整備端末ではない→不可	□公費整備端末である □公費整備端末ではない→不可	
			・個人所有機器ではないか	□個人保有機器である→不可 □個人保有機器ではない	□個人保有機器である→不可 □個人保有機器ではない	
			・指定された端末以外で照会業務が行われないよう、指示がなされているか	□されている □されていない→不可	□されている □されていない→不可	
			・指定されたパソコンの管理担当課 ・指定台数	・パソコン管理所属 （　　） ・指定台数　　台	・パソコン管理所属 （　　） ・指定台数　　台	
(2)	2(1)イ	照会利用端末の利用場所は指定されているか	・照会利用端末の設置場所が指定されているか（設置場所はどこか）	・端末の設置場所の指定 □指定されている □指定されていない→不可 ・端末設置所属 （　　） ・端末設置場所 （　　）	・端末の設置場所の指定 □指定されている □指定されていない→不可 ・端末設置所属 （　　） ・端末設置場所 （　　）	
(3)	2(1)ウ	庁舎外で照会業務を行わない措置が執られているか	・庁舎外から照会業務を行わないよう、徹底されているか	□されている □されていない→不可	□されている □されていない→不可	
(4)	2(1)エ	照会利用端末の盗難防止対策はなされているか	・盗難防止対策の有無及びその内容(例～セキュリティワイヤーによる固定など)	・盗難防止対策の有無 □あり □なし→補完措置を記載 ・盗難防止対策の内容 （　　）	・盗難防止対策の有無 □あり □なし→補完措置を記載 ・盗難防止対策の内容 （　　）	
(5)	2(1)オ	照会利用端末のログイン時の認証方法に問題はないか	・ログイン時の認証方法(ID及びパスワード又は生体認証の別)	ログイン時の認証方法 □ID及びパスワード □生体認証	ログイン時の認証方法 □ID及びパスワード □生体認証	
			・パスワード認証の場合には、定められたセキュリティポリシーに則った、十分な桁数を備えた第三者に容易に推測できなパスワードとなっているか	□なっている □なっていない→不可	□なっている □なっていない→不可	

別添2

LGWANを利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(5)	2(1)オ	照会利用端末のログイン時の認証方法に問題はないか	・ID及びパスワードによる認証の場合、机のデスクマットなどにID及びパスワードが貼付されていないか	ID・パスワードが第三者から視認できる状態になっていないか □なっていない □なっている→不可	ID・パスワードが第三者から視認できる状態になっていないか □なっていない □なっている→不可	
(6)	2(1)カ	照会利用端末のオートログイン機能は無効になっているか	・ログイン時のオートログイン機能は無効化されているか	□無効化されている □無効化されていない→不可	□無効化されている □無効化されていない→不可	
(7)	2(1)キ	照会利用端末のスクリーンセーバーによるロック機能が設定されているか	・スクリーンセーバーロックの設定の有無 ・スクリーンセーバー起動時間の設定に問題はないか（最長でも15分端末操作がない場合にスクリーンセーバーが作動するようになっているか。また、地方公共団体照会担当課にあっては、最長でも30分端末操作がない場合にスクリーンセーバーが作動するようになっているか。）	・スクリーンセーバーロックの設定の有無 □あり □なし→原則不可 ・スクリーンセーバー起動時間 （　　分）	・スクリーンセーバーロックの設定の有無 □あり □なし→原則不可 ・スクリーンセーバー起動時間 （　　分）	
(8)	2(1)ク	照会利用端末の画面が部外者から視認できない措置が執られているか	・照会利用端末の画面が、来庁者等第三者から視認されない場所に設置もしくはのぞき見防止フィルタを貼る等の措置がなされているか	□第三者から画面が見えない措置がなされている □措置されていない→不可	□第三者から画面が見えない措置がなされている □措置されていない→不可	
(9)	2(1)ケ	照会利用端末を本人以外のユーザーアカウントで使用させないための措置が執られているか	・照会利用端末利用終了後、ログアウトするよう徹底されているか	・利用後のログアウトについて指示が徹底されているか □されている □されていない→不可	・利用後のログアウトについて指示が徹底されているか □されている □されていない→不可	
			・照会利用端末には、照会担当者別にユーザーアカウントが割り振られているか	□　割り振られている □　割り振られていない 　→補完措置を記載	□　割り振られている □　割り振られていない 　→補完措置を記載	
			・照会利用端末を本人以外のユーザーアカウントで使用してはいけない旨の管理規定が部内で整備されているか	・本人以外でのアカウントで照会端末を使用してはいけない旨の規定整備の有無 □あり □なし	・本人以外でのアカウントで照会端末を使用してはいけない旨の規定整備の有無 □あり □なし	
(10)	2(1)コ	照会利用端末の管理者と利用者の権限が分離されているか	照会利用端末の管理者と利用者の権限が分離されているか	□分離されている □分離されていない→不可	□分離されている □分離されていない→不可	
(11)	2(1)サ	照会利用端末のユーザーアカウントが分離されているか	照会利用端末のユーザーアカウントが分離されているか	□分離されている □分離されていない ↓ ・利用者を特定するための仕組 （　　） ・共有アカウントの取扱いに関する規定の整備状況 □あり □なし	□分離されている □分離されていない ↓ ・利用者を特定するための仕組 （　　） ・共有アカウントの取扱いに関する規定の整備状況 □あり □なし	

別添2

LGWANを利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(12)	2(1)シ	照会利用端末の利用者が、情報システムを構成する機器等の改造を許可なく実施できないようになっているか	新たな機器等の接続、ソフトウェアの追加等を許可なく実施できないようになっているか	□なっている □なっていない→不可	□なっている □なっていない→不可	
(13)	2(1)ス	照会利用端末の利用者に対し、端末画面の接写及び情報の持ち出しを禁止する規定が設けられているか	当該規定が整備されているか	□整備されている □整備されていない→不可	□整備されている □整備されていない→不可	
(14)	2(2)ア	照会利用端末のOS及び更新状況に問題はないか	・照会利用端末のOS及びバージョンの種類	OSの種類 （　　）	OSの種類 （　　）	
(15)	2(2)イ	照会利用端末にウイルス対策ソフトを導入し定義ファイル等は常に最新の状態に保たれているか	・不正プログラム対策ソフトウェア導入の有無及びソフトウェア名	・不正プログラム対策ソフトウェア導入の有無 □導入されている □導入されていない→不可 ・ウイルス対策ソフトウェア名 （　　）	・不正プログラム対策ソフトウェア導入の有無 □導入されている □導入されていない→不可 ・ウイルス対策ソフトウェア名 （　　）	
			・定義ファイルの更新状況（常に最新の状態に保たれているか）	パターンファイルの番号 （　　） アップデート日付 （　　）	パターンファイルの番号 （　　） アップデート日付 （　　）	
(16)	2(3)	照会利用端末の導入ソフトウェアにセキュリティホール対策がなされているか	・導入ソフトウェアにセキュリティホールが発見された場合の対応要領が定められているか ・定められている場合には、具体的な対応要領について（例～情報管理課に報告など）	・対応要領の有無 □定められている □定められていない ・対応要領（ ）	・対応要領の有無 □定められている □定められていない ・対応要領（ ）	
3　電子メール利用に関する情報セキュリティ要件						
(1)	3(1)	照会に利用するメールアドレスは、照会実施機関間で固定され、当該メールアドレス以外でメールの送受信を行わない取決めがなされているか	照会に利用するメールアドレスは、照会実施機関間で固定されているか	固定されたメールアドレス （　　）	固定されたメールアドレス （　　）	
			固定メールアドレス以外で照会文書の送受信を行わないよう取決められているか	□決められている □決められていない→不可	□決められている □決められていない→不可	
(2)	3(2)	照会に利用するメールアドレスは照会用に新規で用意されたものであるか	・メールアドレスは新規に用意されたものであるか	□新規作成 □既存メールを利用（理由： ）	□新規作成 □既存メールを利用（理由： ）	

別添2

LGWANを利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(2)	3(2)	照会業務に従事する者以外の者が照会用メールアドレスを利用できない措置が講じられているか	・照会利用メールアドレスのアクセス権は業務上必要な職員にのみ付与されているか	□されている □されていない ↓ メールアドレスに対するアクセス権の付与ができない場合、照会利用者以外が当該メールアドレスを利用できない措置の内容（　　）	□されている □されていない ↓ メールアドレスに対するアクセス権の付与ができない場合、照会利用者以外が当該メールアドレスを利用できない措置の内容（　　）	
(3)	3(3)	メールアドレスを照会業務以外のメールの送受信に利用していないか	・メールアドレスを照会業務以外のメールの送受信に利用していないか	□していない □している→原則不可	□していない □している→原則不可	
(4)	3(4)	利用するメールアドレスのドメイン名に行政機関であることが保証されるドメイン名が使用されているか	・照会実施機関双方ともにメールアドレスに「lg.jpドメイン又は都道府県型ドメイン」を使用しているか	□使用している □使用していない→不可	□使用している □使用していない→不可	
(5)	3(5)	照会文書を送信する際には、作成者情報等当該ファイルから付属する情報を削除する対策が執られているか	・サニタイズ処理を行う対策が執られているか	□執られている □執られていない	□執られている □執られていない	
		警察が送信する回答文書に対する適切な措置は執られているか	・警察から送信する照会文書は印字を禁止したPDFとなっているか	□なっている □なっていない→理由及び保全措置を記載		
(6)	3(6)	照会文書に設定されたパスワードの共有方法	・具体的な共有方法について	共有方法 □対面 □電話	共有方法 □対面 □電話	
		照会文書の暗号化措置が執られているか	・暗号化がパスワード設定による場合には、22桁以上で英大文字、英小文字、数字の組み合わせとなっているか	□なっていない □なっている	□なっていない □なっている	
(7)	3(6)	照会文書に設定されたパスワードの定期変更についての取決めがなされているか	・人事異動の都度、パスワードの変更が行われるよう取決めがなされているか ・具体的な変更頻度	パスワード変更の取決め □されている □されていない→不可 パスワードの変更頻度 （　　）	パスワード変更の取決め □されている □されていない→不可 パスワードの変更頻度 （　　）	
(8)	3(7)	電子メールで照会文書を送信後、直ちに端末から当該情報が消去されているか	・送信した照会文書が、直ちに消去されていることについて、部内で確認する体制が構築されているか	□体制がとられている ↓ 具体的な確認方法（例～〇〇課長による月１回以上のメールボックスの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	□体制がとられている ↓ 具体的な確認方法（例～〇〇課長による月１回以上のメールボックスの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	

別添2

LGWANを利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(9)	3(8)	電子メールで照会文書を受信した際に、情報確認後、直ちに受信端末から消去されているか	・受信した照会文書が、直ちに消去されていることについて、部内で確認する体制が構築されているか	□体制がとられている ↓ 具体的な確認方法（例～○○課長による月１回以上のメールボックスの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	□体制がとられている ↓ 具体的な確認方法（例～○○課長による月１回以上のメールボックスの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	
(10)	3(9)	電子メールで受信した照会文書を、照会利用端末として指定された端末以外に送信しないための措置が取られているか	・個人所有の機器等に転送してはならない旨の部内規定が整備されているか	□整備されている □整備されていない	□整備されている □整備されていない	
(11)	3(10)	電子メールで送受信した照会文書が削除されていることを確認するための確認体制が構築されているか	・(9)から(11)までの部内での確認方法について、照会実施機関間で合意がなされているか（覚書などを想定している）	□合意がなされている □合意がなされていない	□合意がなされている □合意がなされていない	
(12)	3(11)	電子メールにより受信した照会文書を、定められた保存先以外に保存しないための対策がなされているか	・定められた保存先は外部回線に接続されていない端末であるか	□接続されていない □接続されている	□接続されていない □接続されている	
			・具体的な保存方法 （例～承認を受けたUSBを利用して、外部回線に接続されていないPWAN端末に移行する。） （例～電子メールで送信された照会書を印字して庁舎内に備付けの照会書綴りに編綴する。）	具体的な保存方法（ ）	具体的な保存方法（ ）	
(13)	3(12)	不審な電子メールを受信したときには、開封せずシステム管理者に速報する体制が構築されているか	・速報先が指定されているか ・不審なメールを受信した際の対応要領について周知されているか	・速報先の指定状況 □指定されている □指定されていない ・不審メール到達時の対応要領 □周知されている □周知されていない	・速報先の指定状況 □指定されている □指定されていない ・不審メール到達時の対応要領 □周知されている □周知されていない	
(14)	3(13)	電子メールのなりすましの防止策が講じられているか	・電子メールのなりすまし防止策が講じられているか（具体的内容）	□講じられている 具体的な内容（ ） □講じられていない	□講じられている 具体的な内容（ ） □講じられていない	
4　共有フォルダ利用に関する情報セキュリティ要件						
(1)	4(1)	共有フォルダに照会文書を閲覧する権限がある者以外の者がアクセスできないようにアクセス制限が設けられているか	・共有フォルダのアクセス権限は照会文書の閲覧権限がある者のみに制限されているか	□されている □されていない→不可	□されている □されていない→不可	

別添2

LGWANを利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(2)	4(2)	共有フォルダ内に蔵置する照会文書はパスワードによる暗号化措置が執られているか	・照会文書の暗号化措置が執られているか	□執られている □執られていない→不可	□執られている □執られていない→不可	
			・暗号化がパスワード設定による場合には、22桁以上で英大文字、英小文字、数字の組み合わせとなっているか	□なっていない □なっている	□なっていない □なっている	
		照会文書に設定されたパスワードの共有方法	・具体的な共有方法について	共有方法 □対面 □電話 □その他 （　　）	共有方法 □対面 □電話 □その他 （　　）	
		照会文書に設定されたパスワードの定期変更についての取決めがなされているか	・人事異動の都度、パスワードの変更が行われるよう取決めがなされているか ・具体的な変更頻度	パスワード変更の取決め □されている □されていない→不可 パスワードの変更頻度 （　　）	パスワード変更の取決め □されている □されていない→不可 パスワードの変更頻度 （　　）	
(3)	4(3)	照会文書を蔵置する際には、作成者情報等当該ファイルから付属する情報を削除する対策が執られているか	・サニタイズ処理を行う対策が執られているか	□執られている □執られていない	□執られている □執られていない	
		警察が蔵置する回答文書に対する適切な措置は執られているか	・警察が蔵置する照会文書は印字を禁止したPDFとなっているか	□なっている □なっていない→理由及び保全措置を記載		
(4)	4(4)	共有フォルダ内に蔵置した照会文書については、照会実施機関において確認後、直ちに端末から消去されているか	・照会文書を確認後、直ちに共有フォルダから消去する旨の規定が整備されているか	□　整備されている □　整備されていない	□　整備されている □　整備されていない	
(5)	4(5)	共有フォルダ内の照会文書が放置されていないことを確認する体制が構築されているか	・受信した照会文書が、放置されていないことについて、部内で確認する体制が構築されているか	□体制がとられている ↓ 具体的な確認方法（例～○○課長による月１回以上の共有フォルダの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	□体制がとられている ↓ 具体的な確認方法（例～○○課長による月１回以上の共有フォルダの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	
(6)	4(6)	共有フォルダに蔵置した照会文書を、定められた保存先以外に保存しないための対策がなされているか	・定められた保存先は外部回線に接続されていない端末であるか	□接続されていない □接続されている	□接続されていない □接続されている	
			・具体的な保存方法 （例～承認を受けたUSBを利用して、外部回線に接続されていないPWAN端末に移行する。） （例～電子メールで送信された照会書を印字して庁舎内に備付けの照会書綴りに編綴する。）	具体的な保存方法（ ）	具体的な保存方法（ ）	

別添2

LGWANを利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(6)	4(6)	照会文書を庁舎外に持ち出さない規定が整備されているか	・照会文書を庁舎外に持ち出さない規定の有無	□整備されている □整備されていない	□整備されている □整備されていない	
5 証跡の管理						
(1)	5(1)	システム管理者によって、利用者のログインに係る証跡を5年以上保存しているか（地方公共団体照会担当課にあっては3年以上）	・照会利用端末のログインに係る証跡が保存されるようになっているか	□保存されている □保存されていない	□保存されている □保存されていない	
(2)	5(2)	システム管理者によって、メールの送受信、共有フォルダへのアクセス及び外部記録媒体の利用に係る証跡を5年以上保存しているか	・照会利用端末のメール送受信、共有フォルダへのアクセス及び外部記録媒体の利用に係る証跡が保存されるようになっているか	□保存されている □保存されていない	□保存されている □保存されていない	
(3)	5(3)	システム管理者によって、メールデータ印字及び照会文書の印字に係る証跡を5年以上保存しているか	システム管理者によって、メールデータ印字及び照会文書の印字に係る証跡を5年以上保存されるようになっているか	□保存されている □保存されていない	□保存されている □保存されていない	
(4)	5(4)	(1)から(3)までの証跡はシステム管理者のみが閲覧可能であり不正な消去、改ざん及び不正なアクセスがなされないようにアクセス制御が行われているか	・ログがシステム管理者によって適切に保管されているか	□適切に保管されている □適切に保管されていない	□適切に保管されている □適切に保管されていない	

別添2

インターネット回線を利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
1　情報セキュリティインシデント発生時の措置						
(1)	1	情報セキュリティインシデントが発生した場合において、照会実施機関間で速報体制が構築されているか	・速報対象となる情報セキュリティインシデントは照会実施機関間で合意がなされているか	□合意がされている □合意がされていない	□合意がされている □合意がされていない	
			・部内での速報先は把握しているか（例～情報システム課〇〇係など）	部内通報先 （　　）	部内通報先 （　　）	
2　サーバに関する情報セキュリティ要件						
(1)	2(1)	サーバのネットワーク環境のセキュリティ対策がなされているか	・ファイアウォール設定の有無（ネットワーク構成図の確認）	□あり □なし	□あり □なし	
(2)	2(2)	電子メールサーバ間にあっては、インターネットを介して通信する電子メールの盗聴及び改ざん防止のため、電子メールに関する通信の暗号化がなされているか	・電子メールサーバ間において電子メールに関する通信の暗号化がなされているか （例～SMTPによる電子メールサーバ間の通信をTLSにより保護、S/MIME等の電子メールにおける暗号化及び電子署名の技術を利用など）	□暗号化されている ↓ （具体的内容：　　） □暗号化されていない→不可	□暗号化されている ↓ （具体的内容：　　） □暗号化されていない→不可	
(3)	2(3)	サーバの不正プログラム対策がなされているか	・不正プログラム対策ソフトウェア導入の有無及びソフトウェア名	・不正プログラム対策ソフトウェア導入の有無 □　されている □　されていない→不可 ・ソフトウェア名 （　　）	・不正プログラム対策ソフトウェア導入の有無 □　されている □　されていない→不可 ・ソフトウェア名 （　　）	
			・定義ファイルの更新状況（常に最新の状態に保たれているか）	パターンファイルの番号 （　　） アップデート日付 （　　）	パターンファイルの番号 （　　） アップデート日付 （　　）	
(4)	2(4)	サーバのセキュリティホール対策がなされているか	・セキュリティホールが発見された場合の対応要領が定められているか ・定められている場合には、具体的な対応要領について（例～情報管理課に報告など）	・対応要領の有無 □定められている □定められていない→補完措置を記載 ・対応要領（ 　　）	・対応要領の有無 □定められている □定められていない→補完措置を記載 ・対応要領（ 　　）	

別添2

インターネット回線を利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
3 端末に関する情報セキュリティ要件						
(1)	3(1)ア	照会利用端末が整備されているか	・照会に用いる端末は公費で整備された端末であるか	□公費整備端末である □公費整備端末ではない→不可	□公費整備端末である □公費整備端末ではない→不可	
			・個人所有機器ではないか	□個人保有機器である→不可 □個人保有機器ではない	□個人保有機器である→不可 □個人保有機器ではない	
			・指定された端末以外で照会業務が行われないよう、指示がなされているか	□されている □されていない→不可	□されている □されていない→不可	
			・指定されたパソコンの管理担当課 ・指定台数	・パソコン管理所属 （　　） ・指定台数　　台	・パソコン管理所属 （　　） ・指定台数　　台	
(2)	3(1)イ	照会利用端末の利用場所は指定されているか	・照会利用端末の設置場所が指定されているか（設置場所はどこか）	・端末の設置場所の指定 □指定されている □指定されていない→不可 ・端末設置所属 （　　） ・端末設置場所 （　　）	・端末の設置場所の指定 □指定されている □指定されていない→不可 ・端末設置所属 （　　） ・端末設置場所 （　　）	
(3)	3(1)ウ	庁舎外で照会業務を行わない措置が執られているか	・庁舎外から照会業務を行わないよう、徹底されているか。	□されている □されていない→不可	□されている □されていない→不可	
(4)	3(1)エ	照会利用端末の盗難防止対策はなされているか	・盗難防止対策の有無及びその内容(例～セキュリティワイヤーによる固定など)	・盗難防止対策の有無 □あり □なし→補完措置を記載 ・盗難防止対策の内容 （　　）	・盗難防止対策の有無 □あり □なし→補完措置を記載 ・盗難防止対策の内容 （　　）	
(5)	3(1)オ	照会利用端末のログイン時の認証方法に問題はないか	・ログイン時の認証方法(ID及びパスワード又は生体認証の別)	ログイン時の認証方法 □ID及びパスワード □生体認証	ログイン時の認証方法 □ID及びパスワード □生体認証	
			・パスワード認証の場合には、定められたセキュリティポリシーに則った、十分な桁数を備えた第三者に容易に推測できなパスワードとなっているか	□なっている □なっていない→不可	□なっている □なっていない→不可	
			・ID及びパスワードによる認証の場合、机のデスクマットなどにID及びパスワードが貼付されていないか	ID・パスワードが第三者から視認できる状態になっていないか □なっていない □なっている→不可	ID・パスワードが第三者から視認できる状態になっていないか □なっていない □なっている→不可	

別添2

インターネット回線を利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(6)	3(1)カ	照会利用端末のオートログイン機能は無効になっているか	・ログイン時のオートログイン機能は無効化されているか	□無効化されている □無効化されていない→不可	□無効化されている □無効化されていない→不可	
(7)	3(1)キ	照会利用端末のスクリーンセーバーによるロック機能が設定されているか	・スクリーンセーバーロックの設定の有無 ・スクリーンセーバー起動時間の設定に問題はないか（最長でも15分端末操作がない場合にスクリーンセーバーが作動するようになっているか。また、地方公共団体照会担当課にあっては最長でも30分端末操作がない場合にスクリーンセーバーが作動するようになっているか。）	・スクリーンセーバーロックの設定の有無 □あり □なし→原則不可 ・スクリーンセーバー起動時間 （　　分）	・スクリーンセーバーロックの設定の有無 □あり □なし→原則不可 ・スクリーンセーバー起動時間 （　　分）	
(8)	3(1)ク	照会利用端末の画面が部外者から視認できない措置が執られているか	・照会利用端末の画面が、来庁者等第三者から視認されない場所に設置もしくはのぞき見防止フィルタを貼る等の措置がなされているか	□第三者から画面が見えない措置がなされている □措置されていない→不可	□第三者から画面が見えない措置がなされている □措置されていない→不可	
(9)	3(1)ケ	照会利用端末を本人以外のユーザーアカウントで使用させないための措置が執られているか	・照会利用端末利用終了後、ログアウトするよう徹底されているか	・利用後のログアウトについて指示が徹底されているか □されている □されていない→不可	・利用後のログアウトについて指示が徹底されているか □されている □されていない→不可	
			・照会利用端末には、照会担当者別にユーザーアカウントが割り振られているか	□　割り振られている □　割り振られていない 　→補完措置を記載	□　割り振られている □　割り振られていない 　→補完措置を記載	
			・照会利用端末を本人以外のユーザーアカウントで使用してはいけない旨の管理規定が部内で整備されているか	・本人以外でのアカウントで照会端末を使用してはいけない旨の規定整備の有無 □　あり □　なし	・本人以外でのアカウントで照会端末を使用してはいけない旨の規定整備の有無 □　あり □　なし	
(10)	3(1)コ	照会利用端末の管理者と利用者の権限が分離されているか	照会利用端末の管理者と利用者の権限が分離されているか	□分離されている □分離されていない→不可	□分離されている □分離されていない→不可	
(11)	3(1)サ	照会利用端末のユーザーアカウントが分離されているか	照会利用端末のユーザーアカウントが分離されているか	□分離されている □分離されていない ↓ ・利用者を特定するための仕組 （　　） ・共有アカウントの取扱いに関する規定の整備状況 □あり □なし	□分離されている □分離されていない ↓ ・利用者を特定するための仕組 （　　） ・共有アカウントの取扱いに関する規定の整備状況 □あり □なし	
(12)	3(1)シ	照会利用端末の利用者が、情報システムを構成する機器等の改造を許可なく実施できないようになっているか	新たな機器等の接続、ソフトウェアの追加等を許可なく実施できないようになっているか	□なっている □なっていない→不可	□なっている □なっていない→不可	

別添2

インターネット回線を利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(13)	3(1)ス	照会利用端末の利用者に対し、端末画面の接写及び情報の持ち出しを禁止する規定が設けられているか	当該規定が整備されているか	□整備されている □整備されていない→不可	□整備されている □整備されていない→不可	
(14)	3(2)ア	照会利用端末のOS及び更新状況に問題はないか	・照会利用端末のOS及びバージョンの種類	OSの種類 （　　）	OSの種類 （　　）	
(15)	3(2)イ	照会利用端末にウイルス対策ソフトを導入し定義ファイル等は常に最新の状態に保たれているか	・不正プログラム対策ソフトウェア導入の有無及びソフトウェア名	・不正プログラム対策ソフトウェア導入の有無 □されている □されていない→不可 ・ウイルス対策ソフトウェア名 （　　）	・不正プログラム対策ソフトウェア導入の有無 □されている □されていない→不可 ・ウイルス対策ソフトウェア名 （　　）	
			・定義ファイルの更新状況（常に最新の状態に保たれているか）	パターンファイルの番号 （　　） アップデート日付 （　　）	パターンファイルの番号 （　　） アップデート日付 （　　）	
(16)	3(3)	照会利用端末の導入ソフトウェアにセキュリティホール対策がなされているか	・導入ソフトウェアにセキュリティホールが発見された場合の対応要領が定められているか ・定められている場合には、具体的な対応要領について（例～情報管理課に報告など）	・対応要領の有無 □定められている □定められていない ・対応要領（ ）	・対応要領の有無 □定められている □定められていない ・対応要領（ ）	
4　電子メール利用に関する情報セキュリティ要件						
(1)	4(1)	照会に利用するメールアドレスは、照会実施機関間で固定され、当該メールアドレス以外でメールの送受信を行わない取決めがなされているか	照会に利用するメールアドレスは、照会実施機関間で固定されているか	固定されたメールアドレス （　　）	固定されたメールアドレス （　　）	
			固定メールアドレス以外で照会文書の送受信を行わないよう取決められているか	□決められている □決められていない→不可	□決められている □決められていない→不可	
(2)	4(2)	照会に利用するメールアドレスは照会用に新規で用意されたものであるか	・メールアドレスは新規に用意されたものであるか	□新規作成 □既存メールを利用（理由： ）	□新規作成 □既存メールを利用（理由： ）	
		照会業務に従事する者以外の者が照会用メールアドレスを利用できない措置が講じられているか	・照会利用メールアドレスのアクセス権は業務上必要な職員にのみ付与されているか	□されている □されていない ↓ メールアドレスに対するアクセス権の付与ができない場合、照会利用者以外が当該メールアドレスを利用できない措置の内容（ ）	□されている □されていない ↓ メールアドレスに対するアクセス権の付与ができない場合、照会利用者以外が当該メールアドレスを利用できない措置の内容（ ）	

別添2

インターネット回線を利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(3)	4(3)	メールアドレスを照会業務以外のメールの送受信に利用していないか	・メールアドレスを照会業務以外のメールの送受信に利用していないか	□していない □している→原則不可	□していない □している→原則不可	
(4)	4(4)	利用するメールアドレスのドメイン名に行政機関であることが保証されるドメイン名が使用されているか	・照会実施機関双方ともにメールアドレスに「lg.jpドメイン又は都道府県型ドメイン」を使用しているか	□使用している □使用していない→不可	□使用している □使用していない→不可	
(5)	4(5)	照会文書を送信する際には、作成者情報等当該ファイルから付属する情報を削除する対策が執られているか	・サニタイズ処理を行う対策が執られているか	□執られている □執られていない	□執られている □執られていない	
		警察が送信する回答文書に対する適切な措置は執られているか	・警察から送信する照会文書は印字を禁止したPDFとなっているか	□なっている □なっていない→理由及び補完措置を記載		
(6)	4(6)	照会文書に設定されたパスワードの共有方法	・具体的な共有方法について	共有方法 □対面 □電話 □その他 （　　）	共有方法 □対面 □電話 □その他 （　　）	
		照会文書の暗号化措置が執られているか	・暗号化がパスワード設定による場合には、22桁以上で英大文字、英小文字、数字の組み合わせとなっているか	□なっていない □なっている	□なっていない □なっている	
(7)	4(6)	照会文書に設定されたパスワードの定期変更についての取決めがなされているか	・人事異動の都度、パスワードの変更が行われるよう取決めがなされているか ・具体的な変更頻度	パスワード変更の取決め □されている □されていない→不可 パスワードの変更頻度 （　　）	パスワード変更の取決め □されている □されていない→不可 パスワードの変更頻度 （　　）	
(8)	4(7)	電子メールで照会文書を送信後、直ちに端末から当該情報が消去されているか	・送信した照会文書が、直ちに消去されていることについて、部内で確認する体制が構築されているか	□体制がとられている ↓ 具体的な確認方法（例～〇〇課長による月1回以上のメールボックスの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	□体制がとられている ↓ 具体的な確認方法（例～〇〇課長による月1回以上のメールボックスの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	

別添2

インターネット回線を利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
(9)	4(8)	電子メールで照会文書を受信した際に、情報確認後、直ちに受信端末から消去されているか	・受信した照会文書が、直ちに消去されていることについて、部内で確認する体制が構築されているか	□体制がとられている ↓ 具体的な確認方法（例～○○課長による月１回以上のメールボックスの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	□体制がとられている ↓ 具体的な確認方法（例～○○課長による月１回以上のメールボックスの目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	
(10)	4(9)	電子メールで受信した照会文書を、照会利用端末として指定された端末以外に送信しないための措置が取られているか	・個人所有の機器等に転送してはならない旨の部内規定が整備されているか	□整備されている □整備されていない	□整備されている □整備されていない	
(11)	4(10)	電子メールで送受信した照会文書が削除されていることを確認するための確認体制が構築されているか	・(9)から(11)までの部内での確認方法について、照会実施機関間で合意がなされているか（覚書などを想定している）	□合意がなされている □合意がなされていない	□合意がなされている □合意がなされていない	
(12)	4(11)	電子メールにより受信した照会文書を、定められた保存先以外に保存しないための対策がなされているか	・定められた保存先は外部回線に接続されていない端末であるか	□接続されていない □接続されている	□接続されていない □接続されている	
			・具体的な保存方法 （例～承認を受けたUSBを利用して、外部回線に接続されていないPWAN端末に移行する。） （例～電子メールで送信された照会書を印字して庁舎内に備付けの照会書綴りに編綴する。）	具体的な保存方法（ ）	具体的な保存方法（ ）	
(13)	4(12)	不審な電子メールを受信したときには、開封せずシステム管理者に速報する体制が構築されているか	・速報先が指定されているか ・不審なメールを受信した際の対応要領について周知されているか	・速報先の指定状況 □指定されている □指定されていない ・不審メール到達時の対応要領 □周知されている □周知されていない	・速報先の指定状況 □指定されている □指定されていない ・不審メール到達時の対応要領 □周知されている □周知されていない	
(14)	4(13)	電子メールのなりすましの防止策が講じられているか	・電子メールのなりすまし防止策が講じられているか（具体的内容）	□講じられている 具体的な内容（ ） □講じられていない	□講じられている 具体的な内容（ ） □講じられていない	

別添2

インターネット回線を利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
5 ファイル転送サービス利用に関する情報セキュリティ要件						
(1)	5(1)	ファイル転送サービスを利用して、照会文書のダウンロード先を通知するメールを送信する際には、同メールのメールアドレス（通知用メールアドレス）を固定するとともに、それ以外のメールアドレスを使用していないか	通知用のメールアドレスは、固定されているか	通知用メールアドレス （　　）	通知用メールアドレス （　　）	
			固定された通知用メールアドレス以外のものを使用しないように取り決められているか	□決められている □決められていない→不可。	□決められている □決められていない→不可。	
(2)	5(2)	通知用メールアドレスは、そのドメイン名が行政機関のものであることが保証されるものであるか	通知用のメールアドレスは、行政機関のものと判別できるような行政型ドメイン又は都道府県型ドメインを使用しているか	□使用している □使用していない→不可	□使用している □使用していない→不可	
(3)	5(3)	照会文書を送信する際には、作成者情報等当該ファイルから付属する情報を削除する対策が執られているか	サニタイズ処理を行う対策が執られているか	□執られている □執られていない	□執られている □執られていない	
(4)	5(4)	照会文書は、パスワードを設定して暗号化し、当該パスワードを電子メール以外の方法で伝達するなど、秘匿性を確保しているか。	具体的な共有方法について	共有方法 □対面 □電話 □その他 （　　）	共有方法 □対面 □電話 □その他 （　　）	
(5)	5(4)	当該パスワードについては、強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないものを使用して適切に管理し、人事異動の都度変更するなど、定期的な変更を行っているか	暗号化がパスワード設定による場合には、22桁以上で英大文字、英小文字、数字の組み合わせとなっているか	□なっている □なっていない	□なっている □なっていない	
(6)	5(5)	ファイル転送サービスを利用する場合は、アップロードしたファイルが一定期間後に自動的に消去される仕組になっているか	自動消去の仕組みについて	□なっている→消去するまでの期間について記載 □なっていない→理由及び補完措置を記載	□なっている→消去するまでの期間について記載 □なっていない→理由及び補完措置を記載	
(7)	5(6)	ファイル転送サービスにアップロードした照会文書が残されたままになっていないことを送信側の照会実施機関の上席者において確認する体制を構築し、少なくとも月１回以上の確認を行えるか	幹部による確認作業について	□体制がとられている→具体的な確認方法（例～〇〇課長による月１回以上のメールボックス等の目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可 □該当なし	□体制がとられている→具体的な確認方法（例～〇〇課長による月１回以上のメールボックス等の目視確認を行い、確認状況を利用管理簿等で管理する） □体制がとられていない →不可	

別添2

インターネット回線を利用した暴力団員等該当性照会実施時の情報セキュリティチェック表

確認内容			確認事項	措置状況		措置状況に対する補完措置
				警察	地方公共団体	
6 証跡の管理						
(1)	5(1)	システム管理者によって、利用者のログインに係る証跡を5年以上保存しているか（地方公共団体照会担当課にあっては3年以上）	・照会利用端末のログインに係る証跡が保存されるようになっているか	□保存されている □保存されていない	□保存されている □保存されていない	
(2)	5(2)	システム管理者によって、メールの送受信及び外部記録媒体利用に係る証跡を5年以上保存しているか	・照会利用端末のメール送受信及び外部記録媒体利用に係る証跡が保存されるようになっているか	□保存されている □保存されていない	□保存されている □保存されていない	
(3)	5(3)	システム管理者によって、メールデータ及び照会文書印字に係る証跡を5年以上保存しているか	システム管理者によって、メールデータ及び照会文書印字に係る証跡を5年以上保存しているか	□保存されている □保存されていない	□保存されている □保存されていない	
(4)	5(4)	(1)から(3)までの証跡はシステム管理者のみが閲覧可能であり不正な消去、改ざん及び不正なアクセスがなされないようにアクセス制御が行われているか	・ログがシステム管理者によって適切に保管されているか	□適切に保管されている □適切に保管されていない	□適切に保管されている □適切に保管されていない	