別紙３

電気通信事業における個人情報保護ガイドライン及び解説改正案に対する意見及びそれに対する考え方

ガイドライン及び解説 関係箇所	意見	考え方
意見１	匿名化処理を行った後の情報の利用については、利用目的として特定するべき。	
第５条　（利用目的の特定） （解説）⑵	２　解説第５条関係⑵ 匿名化するだけなら利用目的として特定する必要はないとしても、匿名化した後の情報を利用することは利用目的として特定すべきであり、そのことを明記するべきである。 つまり、例えば、ただ匿名化して保管するだけなら利用目的として特定する必要はないとしても、「匿名化した後でその情報を自社の営業方針の設定に利用する」であるとか、「匿名化した後で第三者に提供する」などは、利用目的として特定され、本人に通知されているべきものである。 （個人）	利用目的の特定は、個人情報を対象とするため、個人情報に該当しない場合は必要ありません。
意見２	技術的保護措置が講じられていたとしても、漏えいの危険性を皆無にするわけではなく、本人への通知や事実の公表を省略すべきではない。	
第２２条　（漏えい等が発生した場合の対応） （条文） 第１項及び第２項	ガイドライン第 22 条第１項及び第２項 技術的保護措置は、情報を読まれる危険を相応に小さくはするが、皆無にするわけではないので、本人への通知や漏えいに関する事実などの公表をしなくてよいことにするのは適切でない。 保護措置を破る技術も日々進んでいる。本人への通知や漏えいに関する事実などの公表がなければ、もし保護措置が破られて被害が発生しても、それがその情報漏えいによる二次被害だと本人が思い付きにくく、適切な措置がとれずに被害が拡大する。 また、実際に漏えいが起きた場合の心配のほかに、個人情報の紛失等があっても本人への通知や漏えいに関する事実などの公表がないこともあるという仕組みになるので、その認識を心理的に詐欺などに利用される心配が増す。例えば	適切な暗号化措置（電子政府推奨暗号リスト又は ISO/IEC18033 に掲げられている暗号アルゴリズムによる暗号化措置）、暗号化された情報及び復号鍵の適切な管理がなされていれば、現時点の技術では、その内容を解読することが極めて困難です。 以上の考え方を踏まえ、今回のガイドライン改正において、本人に対して二次被害が生じないよう適切な技術的保護措置が講じられている場合は、公表等の手続を省略できるとしたものです。 なお、適切な技術的保護措置を講じていたとしても、総務省への報告を省略するものではないため、総務省では当該報告を踏まえ、適切な技術的保護措置がなされていたも

	「ある電子ファイルが手に入り、解読に成功したところ、あなたの個人情報と思われる。ついては…」などと話を持ちかけられたとき、情報漏えいについて本人あての通知を受けていなくても、一概にその話が偽りと思えなくなり、話に乗ってしまって巧みに誘導される心配が増す。 （個人）	のか検証することになります。
意見３	解説部分において、ノートブック型パーソナルコンピュータ等を対象としていることを明記するべき。	
第２２条　（漏えい等が発生した場合の対応） （解説） (2)　第２段落	解説文の「『パーソナルコンピュータ等』とは」が、ガイドラインの「ノートブック型パーソナルコンピュータ等」からの引用だと考えると、①で「ノートブック型のパーソナルコンピュータ」と記載があり「パーソナルピュータ」の中にノートブック型のものも含まれるように読め、少し分かりにくいかと思いましたので、「『ノートブック型パーソナルコンピュータ等』とは」としてはいかがでしょうか。 （変更案） 「『ノートブック型パーソナルコンピュータ等』とは、個人情報が記録可能な機器である①ノートブック型のパーソナルコンピュータ～」 （個人）	御指摘を踏まえ、本ガイドライン解説の改正案を修正します。 『修正案』 「ノートブック型パーソナルコンピュータ等」とは、個人情報が記録可能な機器であるノートブック型のパーソナルコンピュータのほか、携帯電話端末、ＰＤＡ等の通信端末機器、ＵＳＢなどの外部記録媒体等の一般に持ち出して利用される機器を念頭に置いたものである。
意見４	データの削除方式について、技術的に確証のとれた削除方法を規定するべき。	
第２２条　（漏えい等が発生した場合の対応） （解説） （２）②　ii 【７、８頁】	データ削除方法の規定 単純なデータ削除では、復元可能であるため、技術的な確証のとれた削除方法を規定する必要がある。例：現米国国家安全保障局（NSA）推奨方式、金融庁推奨方式など） （個人） 複合鍵や暗号化された情報の削除につきまして、単純なデータ削除では、復元可能であるため、ガイドラインでは技術的な確証のとれた削除方法を規定する必要があると考えます。 （例：現米国国家安全保障局（NSA）推奨方式、金融庁推奨方式など） （株式会社メトロジー）	復元可能な方法であれば削除がなされていないと考えます。適切な削除方法としては、例えば、JEITA の「パソコン廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項」に則った手法（例：専用ソフトウェアによるデータ消去）、あるいは NIST 800-88 で Purging（実験室レベルでデータ復元不可能と定義）に分類されている手法（例：Secure Erase コマンド）又は相当の手法（例：ATA Enhanced Secure Erase コマンド）を想定しております。
意見５	遠隔操作により復号鍵の削除だけではなく、特定データそのものを削除する	

	ことと選択が可能であることが望ましい。	
第２２条　（漏えい等が発生した場合の対応） （解説）	２．データの削除範囲指定 　複合キーのみの削除のみでなく、特定データそのものを削除の選択が可能であること。　これは、暗号化ソリューションを導入していても、実際の運用で、操作可能な状態のまま、紛失、盗難されていることが多い。その際には、複合キーを削除してもデータにアクセスが可能で、データの閲覧ができてしまいます。利用者の利用状況に応じて複合キーおよびデータの消去の 2 つの選択ができることが望ましいです。 　また、操作可能な状態で、紛失した場合した場合のファイルの操作履歴を取得して管理できる機能を有していると、情報漏洩範囲を特定できるようになります。 （個人）	適切な暗号化措置（電子政府推奨暗号リスト又はISO/IEC18033 に掲げられている暗号アルゴリズムによる暗号化措置）、暗号化された情報及び復号鍵の適切な管理がなされていれば、現時点の技術では、その内容を解読することが極めて困難です。 　なお、操作可能な状態のまま、紛失、盗難にあった場合には、個人情報の漏えいのおそれがある場合もあるため、「個人情報の漏えい等に際し、①及び②の技術的保護措置が有効に実施されていること」を要件としています。 　情報漏えい範囲については、本ガイドライン改正案で記録媒体内の個人情報の保存先として利用可能な全領域を対象として暗号化措置を講じるものであることを求めています。
意見６	遠隔操作により記憶媒体内の復号鍵と暗号化された情報を削除可能な状態を確保することが望ましい。	
第２２条　（漏えい等が発生した場合の対応） （解説）	「電気通信事業における個人情報保護に関するガイドライン及び解説の改正案」における解説の箇所につきまして、原案には反対し下記の修正意見を提出いたします。 【改定案原文】 （ⅱ）遠隔操作により記憶媒体内の復号鍵又は暗号化された情報（あるいはその両方）を削除できかつ記憶媒体内の復号鍵又は情報を削除するまでの間に、復号鍵の複製、情報の閲覧、複写がされていないことを権限者側で確認できること。 【改定案に対する具体案】 （ⅱ）遠隔操作により記憶媒体内の復号鍵と暗号化された情報を削除可能な状態を確保すること。	適切な暗号化措置（電子政府推奨暗号リスト又はISO/IEC18033 に掲げられている暗号アルゴリズムによる暗号化措置）、暗号化された情報及び復号鍵の適切な管理がなされていれば、、現時点の技術では、その内容を解読することが極めて困難です。 　なお、③の「技術的保護措置が有効に実施されていること」については、復号鍵を暗号化された情報と分離している場合には、その復号鍵のすべてが権限者の管轄下に存在すること、また秘密分散法を用いるならば、紛失した暗号化された情報と分離されていない復号鍵の構成部分では復号ができず、かつ分離されている構成部分のすべてが権限者の管轄下に存在することを想定としています。 　また暗号化された情報と分離されていない場合には、当該復号鍵が複製、情報を閲覧等される前に、復号鍵又は暗

	【修正意見の理由】 ガイドラインに従い、暗号化ソリューションを導入し複合鍵の削除を実行したとしても、実際の運用ではパーソナルコンピュータ等を操作可能な状態のまま紛失、盗難されているため、このままでは情報へのアクセス、閲覧が可能であるためです。 ガイドラインとしては、複合鍵と情報の双方を削除可能な状態にしておくことを定める必要があると考えております。 複合鍵と情報のどちら、またはその両方を削除する必要があるのかは、運用状況に応じて電気通信事業者が判断するものと思われます。 同項の③において、「技術的保護措置が有効に実施されていること」とありますが、保護策の有効な実施を証明することは難しく、このままですと電気通信事業者は、暗号化措置を導入・管理すれば、パーソナルコンピュータ等を紛失および盗難発生時した場合にも、複合キーを削除することだけで事実関係を本人に通知する必要はないと判断し、利用者が不利益を受ける事象が発生するのではないかと非常に危惧いたします。 （株式会社メトロジー）	号化された情報（あるいはその両方））が削除されたことが、権限者側で確認できることを想定としています。
意見７	海外での利用を想定した漏えい対策ソリューションが必要と考える。	
第２２条　（漏えい等が発生した場合の対応） （解説）	海外での利用対応 パソコンの盗難は、海外に持ち出した場合に発生していることが多いため、海外での利用を想定した対策が重要です。特に、日本国内で設計した技術情報を持って、海外の製造拠点に渡航する場合に、パソコンの紛失があれば、日本国の技術を漏洩して国益に大きく影響してしまうことが考えられます。そのため、海外での利用環境の際でも、同等な漏洩対策ソリューションが必要と考えられます。 （個人）	現状の個人情報保護法では、国内に拠点を構える企業であれば、当該法人は「個人情報取扱事業者」に該当します。また、日本から海外に持ち出した個人情報についても、個人情報取扱事業者としての義務が課せられているため、安全管理措置を講じることは国内外問わず求められるものと考えます。
意見８	個人情報の漏えい等の発生時に、適切な技術的保護措置が講じられていれば問題ないのか。	
第２２条　（漏えい等が発生した場合の対応） （解説）	情報の漏えいについての組織的な決定後、見解を持つに至るには、事実関係の調査、証拠の取り扱い、証言の有無、内規による規範のレベルの高低が公表されたりして、収支決算との影響を受けることが予想されて後、人事案件とさえ	漏えい等発生時に適切な技術的保護措置が講じられていなかった場合には、本人への通知や総務省へ直ちに報告することが求められます。一方で、漏えい等発生時に本ガ

	成ることがありますので、ノートブック型パーソナルコンピュータ等の紛失又は盗難により当該個人情報の漏えい等本人に対して、二次被害が生じないよう適切な技術的保護措置が講じられ、遅滞なく総務省に直ちに報告するものと代えることができる場合、本改正によって、次世代型のいわゆる「クラウド」と呼ばれる通信（送受信）に伴い、個人情報の漏えいが発生したときが、最も適切な、技術的保護措置が講じられていると知っていたと解するとできたとしても、問題はないのか。 （個人）	イドラインの要件を満たす適切な技術的保護措置が講じられているならば、直ちに本人へ二次被害が生じるものではないと考えますので、個人情報の漏えい等の発生時に求められる手続を一部省略することが可能となるよう措置したものです。