技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準（案）、技術等情報漏えい防止措置認証業務の実施の方法の一部を改正する告示（案）及び技術等情報漏えい防止措置の実施の促進に関する指針の一部を改正する告示（案）に関する意見公募手続の結果について

令和６年８月１６日
経済産業省
貿易経済安全保障局
経済安全保障政策課技術調査室

「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準（案）、技術等情報漏えい防止措置認証業務の実施の方法の一部を改正する告示（案）及び技術等情報漏えい防止措置の実施の促進に関する指針の一部を改正する告示（案）に対する意見募集」について、令和６年６月５日から同年７月４日まで意見公募手続を実施しました。
提出意見と提出意見を考慮した結果については以下のとおりです。

※行政手続法第四十三条第二項の規定に基づき、提出意見は整理又は要約しています。
※本件意見募集とは直接関係のない御意見（１件）に対して、経済産業省の考え方は示しませんが、承っております。

	提出意見	提出意見を考慮した結果
1	実施の方法告示案の７枚目の改正後欄の５行目「作成した文書」は「作成が求められる文書」などのほうがよい。作成されていない場合もあるのだから。	ご指摘を踏まえ、修正させていただきます。
2	業界団体へのヒアリングを踏まえ、自工会、部工会サイバーセキュリティガイドラインのレベル１の項目を網羅するとしたことは、有意義だと思います。しかし、自工会、部工会ともに次段階へ進まれています。T 社どの主導で行われているサイバーセキュリティガイドラインの次ステップへの移行も視野に入れて改定を進めて頂きたいと思います。	頂いた御意見は今後の施策の参考とさせていただきます。
3	基準告示案の３ページの義務項目を達成するために適切と考えられる手段欄の最下行の３行上「暗証番号」と、同１０ページの同欄の８行「鍵番号」との違いは、何か？	大きな違いはないので、「暗証番号」に統一させていただきます。

4	義務項目にある「管理者」には国の機関（議員・各省庁・役所）も含まれると思います。それを明記すべきだと思います。	御質問の「管理者」が何を指すか必ずしも定かではありませんが、「管理責任者」や「情報システム管理者」を指すとすれば、これは事業者内での管理の責任担当者を指すものであり、ご指摘の主旨とは異なります。
5	該当箇所 4 管理対象情報が電子情報である場合のアクセスの制限等 第 4 事業者は、自社が構築する管理情報システムを構成するネットワークシステム、及びアプリケーションについて不正アクセスを防止するために、必要な措置を講ずる。 意見内容 バックアップについて第 5 節の「第 5 事業者は情報システムを、継続的に利用できるよう、必要な措置を講ずる。」で述べられていますが、第 4 節でバックアップした保存情報(バックアップデータ)に関する不正アクセスを防止するための処置が記述されていません。 システム障害やサイバー攻撃にあった際に、システムを復元するために保存情報(バックアップデータ)が必要になりますが、保存情報が外部から攻撃されてしまうといざというときに復元できないことになります。よって、保存情報は外部からのサイバー攻撃が届かないように、システムやネットワークから切り離して保管することが重要になります。 特に近年問題になっているランサムウェアはデータを勝手に暗号化して使用できなくし、そのデータを復号するために金銭を要求するものです。これに対する対策として保存情報(バックアップ)があれば復元が可能です。しかし、その保存情報自体がランサムウェアの攻撃対象となってしまっては意味がないため、システムやネットワーク	ご指摘のバックアップデータの暗号化については、IV の第 13 の 7 において、「事業者は、管理対象情報を電子政府推奨暗号を用いて暗号化する。」との記載により対応しています。 バックアップデータのシステムおよびネットワークからの切り離しについては、ご指摘の様な方法が、セキュリティ上より強固であることは理解していますが、義務項目の達成手段として、当該水準まで要求基準とするかには議論があり、今回は含めておりません。今後の検討において参考にさせていただきます。

	から切り離して保管することが重要です。 また、保存情報が入ったストレージが盗難や持ち出しにあうと情報漏洩となってしまうため暗号化して保管することが重要になります。 よって、以下の2項目を4章第4節に追加することを提案します。 14. 事業者は、保存情報(バックアップデータ)をシステムおよびネットワークから切り離して保管することで、ランサムウェア等のサイバー攻撃から情報を守る 15. 事業者は、保存情報(バックアップデータ)を暗号化して保管し、盗難や持ち出しによる情報漏洩を防止する	
6	事業者の技術等の情報の管理について、国で示した基準に即して守られているかどうかの認証が複雑なため認証機関による認証が受けられる認証制度も簡易になるのでいいと思われますが重要なのは漏えいを絶対に無いようにすることだと思います。 認証機関や業界団体の指摘であっても、事業者の技術等の情報の管理について、国で示した基準に即して守られているかどうかが重要なので、その点が厳格に守られればいいと思います。 技術や研究開発の漏えいは日本の安全保障にも直結しますので国で示した基準に即して遵守されているかの定期的な確認や調査など管理体制が甘くならないように、きっちりと管理するというのが重要だと思われます。	貴重な御意見をありがとうございます。今後の参考とさせていただきます。