全Ｌ協保安・業務Ｇ８第１６４号
令和８年１０月１５日

会　員　各位

（一社）全国ＬＰガス協会

不正アクセスによる情報漏えい等の事案を踏まえた
注意喚起及び情報提供に係る協力依頼について（お知らせ）

標記につきまして、経済産業省より、不正アクセスによる情報漏えい事案等を踏まえたサイバーセキュリティ対策の徹底について周知依頼がございましたので、下記のとおりお知らせいたします。

最近、国内企業・組織において、不正アクセスによる情報漏えい等の被害が相次いで発生しており、サプライチェーンを通じた侵害も確認されています。
このため、内閣官房国家サイバー統括室（ＮＣＯ）、（一社）ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）及び個人情報保護委員会より、ウェブシステム等の適切な管理、脆弱性への迅速な対応、ＡＰＩ経由のアクセス対策、個人情報の適切な管理等を徹底するよう注意喚起が行われています。

各事業者におかれましては、自社のみならずサプライチェーン全体でのセキュリティ確保を意識し、経営層主導による対策の推進、脆弱性情報の早期把握・対応、「ゼロトラスト」の考え方を踏まえた対策など、一層のサイバーセキュリティ対策の徹底をお願いいたします。

また、万が一サイバー攻撃等による被害が発生した場合には、被害状況等の迅速な把握及び対応のため、経済産業省への情報提供にご協力くださいますようお願いいたします。
なお、詳細につきましては、添付の経済産業省通知及び関係資料（別紙１～４）をご確認くださいますようお願いいたします。

つきましては、都道府県協会におかれましては会員に対し、また、直接会員及び賛助会員におかれましては営業所等に対し、ご周知くださいますようよろしくお願いいたします。

以　上

発信手段：Ｅメール
担当：保安・業務グループ　岩田、橋爪

2026 年 10 月 9 日

不正アクセスによる情報漏えい等の事案を踏まえた
注意喚起及び情報提供に係る協力依頼

経済産業省　商務情報政策局
サイバーセキュリティ課

最近、国内企業・組織において、サプライチェーンを通じた侵害を含め、第三者からの不正アクセスに起因する情報漏えい等の被害が相次いで発生しております。

こうした状況を踏まえ、国家サイバー統括室（NCO）から、「不正アクセスによる漏えい等の事案を踏まえた対応について」[1]として、国内の事業者等に対し、ウェブシステム等の適切な管理、サプライチェーンを通じた侵害への対策、データの適切な管理などの対策の徹底を促す注意喚起が行われております。

また、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）からも、「直近で相次いでいる国内組織における不正アクセスに関する注意喚起」[2]として、現時点で確認されている攻撃手法等に基づき、API 経由のアクセスへの対策等の実施を推奨する注意喚起が行われております。

さらに、個人情報保護委員会からも「大規模な漏えい等事案を踏まえた対応について（注意喚起）」[3]として、個人情報等の適切な取扱い及び不正アクセスによる個人データ漏えい防止のための対策を促す注意喚起が行われております。

関係各位におかれましては、これらの注意喚起を御参照いただき、自社のみならず、サプライチェーン全体でセキュリティを管理するという認識の下、①組織のトップによる主導、②脆弱性情報の早期把握と対応、③「ゼロトラスト」への移行など、一層の対策の徹底に取り組んでいただきますようお願いいたします。

また、万が一サイバー攻撃による被害が発生した場合には、以下のとおり、被害状況等に係る情報提供に御協力いただきますようお願いいたします。

---

1 https://www.cyber.go.jp/pdf/press/taiou.pdf
2 https://www.jpcert.or.jp/at/2026/at260030.html
3 https://www.ppc.go.jp/files/pdf/261007_houdou.pdf

＜被害発生時の情報提供のお願い＞

経済産業省の所管業界の事業者様におかれましては、サイバー攻撃またはその可能性があるインシデントによる被害が発生した場合には、経済産業省の担当課室（業所管課室）まで、速やかに御一報ください。

■　提供いただきたい情報について

下記の情報について、可能な範囲で御提供くださいますようお願いいたします。

・発覚から現在に至るまでの時系列（発生日時、発覚日時等）
・被害状況（情報漏えい、システムの停止等）
・攻撃種別（ランサムウェア攻撃、不正アクセス攻撃、DDoS 攻撃等）　など

■　情報提供いただいた後の対応について

事態の早期収束及び拡大防止に向けて、以下の対応を支援いたします。

・サイバー攻撃等のインシデントに係る関係専門機関の御紹介
・今後の対応に関する助言　等

■　その他留意事項

・提供いただいた情報は、適切に管理いたします。また、事業者様の同意なく公表することはありません。
・なお、サイバー脅威の分析に活用するとともに、官民での情報共有を促進する観点から、事業者様から承諾いただいた上で、国家サイバー統括室に当該情報を共有させていただく場合がございます。
・また、被害拡大防止や攻撃手口の把握、他の事業者への注意喚起等につなげる観点から、サイバー事案に係る犯罪被害に遭われた場合には、警察への通報・相談についても積極的に御検討ください。

なお、経済産業省では、サプライチェーンを構成する企業のセキュリティ対策状況を共通の基準で評価・可視化することで、委託元企業・委託先企業双方の負担を軽減しつつ、サプライチェーン全体のセキュリティ水準の底上げを図る「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度)」について、2027 年 3 月の制度開始に向け、準備を進めています。

また、企業の皆様がサイバーセキュリティ対策を進める際に活用いただける各種支援策を用意しております。詳しくは、経済産業省ホームページよりご確認ください。

＜主な支援策＞

・ここから始めるセキュリティ！―SECURITY ACTION 自己宣言―
・あなたの会社を守ります！―サイバーセキュリティお助け隊サービス―
・サプライチェーン強化に向けた中小企業支援策！―SCS 評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）の活用―
・ぜひお読みください！―中小企業の情報セキュリティ対策ガイドライン―
・困ったら専門家へ御相談を！―情報処理安全確保支援士（登録セキスペ）―
・サイバー攻撃の被害に遭ってしまったら御活用を！―中小企業のためのセキュリティインシデント対応の手引き―

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html

以上