2026年11月6日

お取引先の皆さま

東京電力ホールディングス株式会社
セキュリティ統括室長
調達部長

# サイバーセキュリティ対策に関する注意喚起とご協力のお願い

平素より東京電力グループの事業活動に格別のご理解とご協力を賜り、厚く御礼申し上げます。

昨今、国内の企業・組織において、不正アクセスによる情報漏えい事案が相次いでおります。システムの脆弱性を悪用した侵入に加え、ID・パスワード等の認証情報の窃取・不正利用、委託先・取引先やクラウドサービスを経由して影響が拡大する事案など、サイバーセキュリティ上の脅威は多様化しています。

これらの事案は、発生した企業だけでなく、その取引先や関係企業にも影響を及ぼすおそれがあります。また、一つのアカウントやシステムへの不正アクセスが、個人情報・重要情報の漏えいや業務停止などにつながり、サプライチェーン全体の事業活動に重大な影響を及ぼす可能性があります。

このような状況を踏まえ、国家サイバー統括室（NCO）においても、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が行われています。つきましては、その趣旨を踏まえ、情報漏えいの未然防止および影響拡大の防止に向け、貴社の管理体制、事業内容、システム環境および取り扱う情報に応じて、以下の事項を改めてご確認いただくとともに、従業員その他業務に従事する方々への周知および必要な対応について、ご協力くださいますようお願いいたします。

なお、以下の事項は、各社の状況に応じた対策の確認をお願いするものであり、平時における対応状況のご回答またはご報告をお願いするものではありません。ただし、事案発生時には、法令、契約および既存の連絡手続等に基づくご対応をお願いいたします。

① 認証情報の適切な管理
- ID・パスワードの適切な管理および使い回しの防止
- 多要素認証（MFA）の活用
- 不審なメールやWebサイトによる認証情報窃取への注意

② システム等の適切な管理
- 利用する機器、OS、ソフトウェアおよびクラウドサービスの脆弱性情報の把握
- セキュリティ更新プログラムの適時適切な適用

③ 情報の適切な管理

・個人情報および秘密情報の適切な管理

・業務上不要となった情報の削除・廃棄

・アクセス権限の適切な管理

④ インシデント発生時の迅速な対応

・不正アクセス、情報漏えい等のインシデントまたはそのおそれを認識した場合の速やかな社内報告

・法令、契約等に基づく関係先への速やかな連絡

・東京電力グループに関連する情報への影響が懸念される場合の速やかな連絡

お取引先の皆さまにおかれましては、本注意喚起の趣旨をご理解いただき、情報漏えいの未然防止および影響拡大の防止に向け、ご協力くださいますようお願い申し上げます。

以上

【参考資料】

・国家サイバー統括室（NCO）「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」（URL：https://www.cyber.go.jp/pdf/press/taiou.pdf）