



このように、リモートアクセスは、ネットワークのセキュリティを確保するために、適切な対策を講ずることが重要です。また、リモートアクセスのログを適切に管理し、不正アクセスの検出や調査に活用することが求められます。

リモートアクセスのセキュリティを高めるためには、多要素認証やVPNの利用が有効です。また、定期的なセキュリティアップデートや脆弱性診断の実施も重要です。さらに、リモートアクセスのポリシーを明確にし、従業員への教育・啓発を行うことが、セキュリティ意識の向上につながります。

また、IoTデバイスの増加に伴って、リモートアクセスのセキュリティリスクも高まっています。2018年には、IoT関連のセキュリティインシデントが9%増加したと報告されています。TelnetやSSHなどの脆弱なプロトコルの利用を避け、より安全な通信手段の導入が求められています。

リモートアクセスのセキュリティを確保し、業務の効率化とセキュリティの両立を実現することが、現代の企業にとって重要な課題です。

リモートアクセスのセキュリティを高めるためには、多要素認証やVPNの利用が有効です。また、定期的なセキュリティアップデートや脆弱性診断の実施も重要です。さらに、リモートアクセスのポリシーを明確にし、従業員への教育・啓発を行うことが、セキュリティ意識の向上につながります。

... ..

... ..

- ... ..
- ... ..
- ... ..

... ..

[Remotely controlled EV home chargers – the threats and vulnerabilities](#)

... .. IoT

[New trends in the world of IoT threats](#)