

## 組織内におけるCSIRT運営

### NTTDATA-CERT

NTTデータグループでは、平時の活動を通じてインシデントの発生を未然に防止するとともに、インシデントを早期に検知し、緊急対応を迅速かつ正確に行うための組織内CSIRTとして「NTTDATA-CERT」を運営しています。

#### 新たなセキュリティリスクに備えた活動

NTTDATA-CERTは、2000年以降、各事業部門で独自に実施されていた社内のCSIRT活動を集約し、2010年7月に発足しました。主な活動としては、最新の攻撃手法やインシデントの発生状況など、セキュリティに関する広範な情報収集・情報分析・情報発信をはじめ、通信監視、緊急対応、研究開発、外部連携が挙げられます。サイバー攻撃の目的や手口が年々変化する中、最新のリスクに対処できるよう注力しています。

#### 内外と連携した幅広い活動

NTTDATA-CERTの活動範囲はNTTデータグループ内にとどまりません。JPCERTコーディネーションセ

ンター(JPCERT/CC)や日本シーサート協議会(NCA)に加盟している各社のCSIRT等、外部のセキュリティ組織と幅広く連携しています。

これにより迅速なセキュリティ関連情報の共有が行われ、情報セキュリティ事案の早期検知や早期対応を可能にしています。

#### OSINTを活用した活動

NTTDATA-CERTの運営に当たっては、政府の公式発表やマスメディアによる報道、論文・技術資料など、合法的に入手できる情報を積極的に活用するオープン・ソース・インテリジェンス(OSINT)のアプローチを取り入れています。日々収集した情報はNTTDATA-CERTの情報分析専門家が分析し、セキュリティの動向を予測して、セキュリティ関連ニュースや四半期レポートとしてNTTデータグループ各社へ配信しています。

また、この情報はサイバー攻撃監視の強化や次期研究開発テーマの選定など、NTTデータグループのセキュリティ戦略・対策に活かされています。

#### NTTDATA-CERTの目指す姿

