SNBL セキュリティ基本方針

SNBL security standard policy

新日本科学グループの倫理綱領第四条に規定されているように、SNBLer(新日本科学グループの全役職員)は、業務上で知り得た個人と企業の情報について秘密保持を厳守することが義務づけられています。秘密情報の漏洩やプライバシーの侵害等の事態は、事の大小を問わず、決して発生させず、常に高い社会的信頼を保ち続けなければなりません。

ここに、新日本科学グループが企業セキュリティを最重要視することを、改めて明確に宣言いたします。

1. 定義

1) SNBL セキュリティ基本方針

当基本方針を指し、新日本科学グループの企業セキュリティの基本方針を示すものである。

2) SNBL セキュリティ対策基準

新日本科学グループの全役職員が行動規範として遵守しなければならない共通のルールを定める。企業セキュリティ基本方針の枠組みに応じて規定される文書である。企業活動全般に係る秘密情報等のセキュリティ基準「ビジネスセキュリティ対策基準」とコンピュータシステムの運用管理ならびに利用上のセキュリティ基準「コンピュータシステム情報セキュリティ対策基準」に大別される。

3) 各種規程集（標準操作手順書もしくは業務手順書 SOP: Standard Operating Procedures）

SNBL セキュリティ対策基準の具体的な実践手段を定める。目的別に具体的かつ詳細に規定した文書である。

2. 原則

1) 新日本科学グループは、すべての企業活動に係る情報資産に対して、機密度および重要度に基づく相応の情報セキュリティ対策を講じる。

2) 全役職員は、セキュリティ管理において割り当てられた責任と権限に基づき、新日本科学グループの情報資産の保全に努めなければならない。万一違反した場合には、違反行為の態様・結果の重篤性等に応じて社員就業規則の懲戒規定を適用することがある。

3) 全役職員は、常に企業セキュリティ意識の浸透・向上・啓発に努めなければならない。

4) 情報技術の進展に合わせて、適宜「ビジネスセキュリティ対策基準」ならびに「コンピュータシステム情報セキュリティ対策基準」ならびに「規程集(SOP)」の見直しを図り、最善の方策を追求する。

3. 適用範囲

当基本方針は、役員、従業員を含めた、新日本科学グループの所有する情報資産、情報システムを取り扱うすべての者に適用されるものとする。

4. 体制

企業セキュリティに関する主管部門を総務人事部門および情報システム部門とする。

5. その他

1）企業セキュリティ教育

定期的に、また必要に応じて実施する企業セキュリティ教育等によってセキュリティポリシーの周知徹底を図る。

2）業務継続計画

業務継続の維持が困難と判断される大規模な自然災害や障害、その他のリスクに対しては、リスクマネジメント管理の緊急対応計画との整合性を図りながら対応すること。

以上

2003 年 10 月 01 日制定
2011 年 10 月 01 日改定
2024 年 1 月 31 日改定