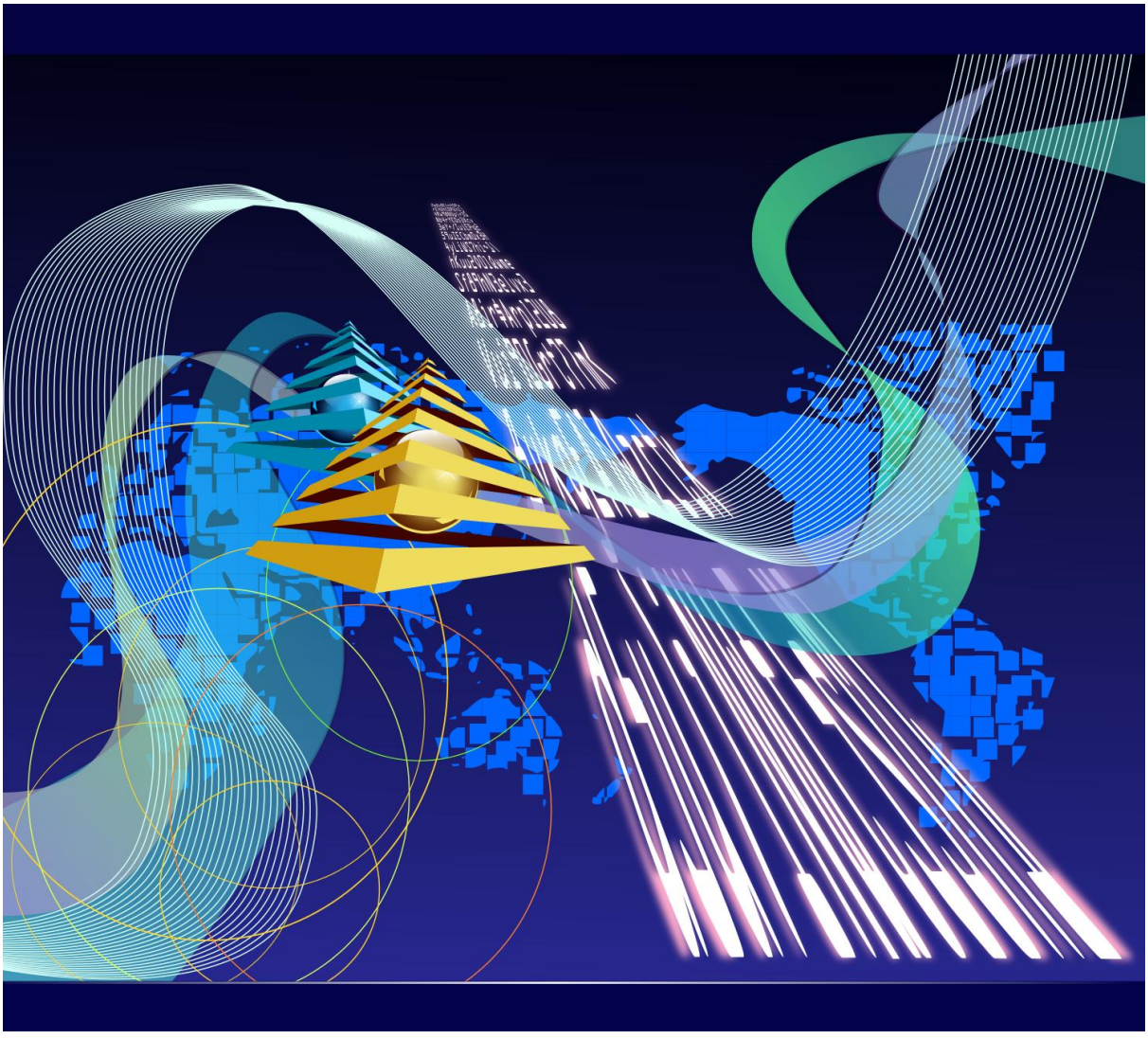
NAGANO SCIENCE

情報セキュリティレポート

Information Security Report



INDEX

トップメッセージ

当社は当初機器メーカーとしてスタートを切りましたが、近年は製薬企業様の品質試験分野における重要なプロセスを代行する、BPO サービス事業の割合が著しく高まってきました。この BPO サービス事業においては、製薬企業様の重要なデータを発生させたり収集したりすることが日常化しています。さらに、メーカー機能とサービス提供機能を高度に連携させていく取り組みの中で、メーカー機能側でもお客様にとって重要なデータの生成と蓄積が急速に増加しつつあります。

このような事業特性の大きな変化に対応し、増大するお客様からの強い期待に応え、引き続きこの分野におけるリーディングカンパニーとして飛躍していくために、今般の国際的な情報セキュリティに係る規格である ISO/IEC 27001:2013(JIS Q 27001:2014)の認証取得を契機に、情報セキュリティに対する取り組みレベルを大きく引き上げていきます。

まずは、お客様のデータ（情報）を直接取り扱う部署あるいはその可能性が高い部署に限定し、認証取得しました。いずれは、BPO サービスのさらなる高度化・複雑化に伴い、必要に応じて、対象部署の拡大を計画していきます。

多くのお客様は、当社のことを強く信頼してくださっています。お客様の重要データを今まで以上に組織的かつ大切に取り扱い、情報漏えい等のセキュリティ事故は当然のこと、データの不整合や不足などの事態も徹底的に防ぐよう組織活動を徹底してまいります。

2014 年 12 月
ナガノサイエンス株式会社
代表取締役社長　長野 大造

情報セキュリティの考え方

当社では、情報セキュリティを重要な経営課題のひとつと認識しています。
情報は弊社のビジョンを実現するためになくてはならないものと位置づけ、サイエンスベースの考え方の実現への重要インプットと考えています。そのためにお客様から安心して情報をいただけるシステムづくりを目指します。
情報を活用し、製品・サービス等のブレイクスルーを実現することが、ステークホルダーへの責務と同時に社会貢献を果たすことになると考えます。
お客様からいただいた情報に対して漏えいを起こさない、正しく情報を保管する、有効に活用すること、のバランスを図り PDCA サイクルを回して継続的にマネジメントレベルの向上に努めていきます。

情報セキュリティ・マネジメントシステム（ISMS）

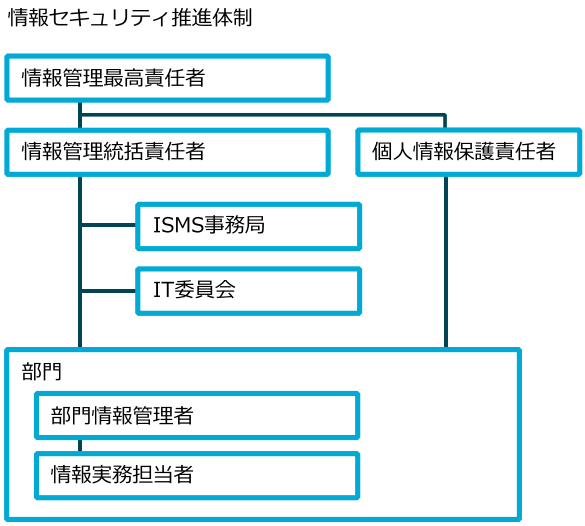
ISMS 文書体系

当社では情報セキュリティの基本的なルールとして、「情報セキュリティ・ポリシー」とそれに準ずるガイドラインやルールを定めています。
情報セキュリティ・ポリシーは、当社が情報を扱う上での基本的な考え方や原則を明示しています。
ガイドラインは、ISMS 推進体制、機密度に応じた情報の分類、導入・運用・監視・レビュー・改善・教育などまとめた ISMS を運用していく上での基本文書です。

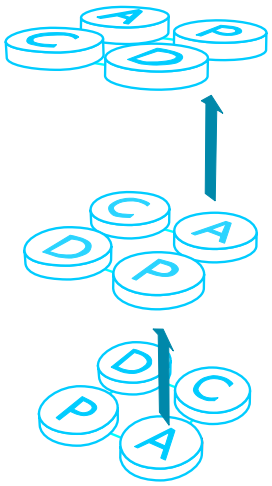
ルールは、情報を取り扱う上での遵守事項を情報の種類・設備・ツール等毎に具体的に示しています。また、インシデント発生時の対応方法・遵守事項・その後のフィードバックについて、IT-BCM 対応についても記載しています。
具体的な手順レベルについては項目毎にハンドブックに展開しています。

情報セキュリティ推進体制

情報セキュリティ確保のためには、トップの関わりが重要です。当社では社長自ら「情報管理最高責任者」として体制をリードしています。
情報管理統括責任者は機密情報の管理全般に関する事項を関連部門と調整します。
個人情報保護責任者は会社が所有する個人情報全般の責任者です。
情報を所有する各部門の責任者は部門情報管理者として部門内の情報を把握、管理し、それらの漏えい防止に努めること。また、情報実務担当者を指名し、実質的に情報の管理をさせることとしています。



情報セキュリティマネジメントサイクル



情報セキュリティマネジメントは他のマネジメントシステム同様に PDCA のサイクルに従って運用しています。

情報セキュリティには、リスクが存在しますが、リスクを評価した上でサイエンスによりリスクを低減させる「リスクとサイエンスの融合」に取り組んでいきます。

Plan では、情報セキュリティ方針の策定、情報セキュリティ施策の検討・策定、情報セキュリティ教育の計画を行います。

Do では、情報セキュリティ施策の実施・運用を行います。

Check では、情報セキュリティ運用状況の点検、IT 委員会等による環境変化等への対応検討、内部監査、マネジメントレビューを行います。

Action では、マネジメントシステムの見直し、検討結果による施策への反映を行います。

情報セキュリティ第三者評価

当社では、情報セキュリティの取組に対する第三者評価として ISO/IEC27001:2013 (JISQ 27001:2014)の認証取得を行いました。

情報セキュリティ関連法令、業務上のセキュリティ要件等を順守してまいります。

GMP 領域における PIC/S CSV ガイドラインにおいて「IT インフラのアクセス管理」に言及されているように情報システムの適格性確認の重要度が増しています。

情報セキュリティの取り組み

人的・組織的な取り組み

社員一人ひとりが情報セキュリティの重要性を認識し、適切に情報を取り扱えるよう、教育や注意喚起を徹底することが欠かせないと考えています。

社内では情報システムグループが中心となり、教育や啓蒙を定期的に実施し、日常業務レベルまで浸透させる活動を続けています。

全社的な議論の場として、IT 委員会を設けて日々変化する ICT 技術の検討や既存の仕組みの検討・見直し・対応を図っています。

また、社内で使用するサービスやシステムを導入する際には、情報セキュリティの 3 要素（Confidentiality/Integrity/Availability）を考慮した評価を実施しています。

システムの運用フェーズにおいては、重要なシステムについて定期的なアクセス権限のレビューを実施して適切なアクセス権限状態が保たれていることを確認しています。

区分	内容
教育	入社時情報セキュリティ教育
	情報リテラシー教育
	定期的な e ラーニング教育
常設委員会	IT 委員会、ISMS 事務局

技術的な取り組み

a. アクセスコントロール

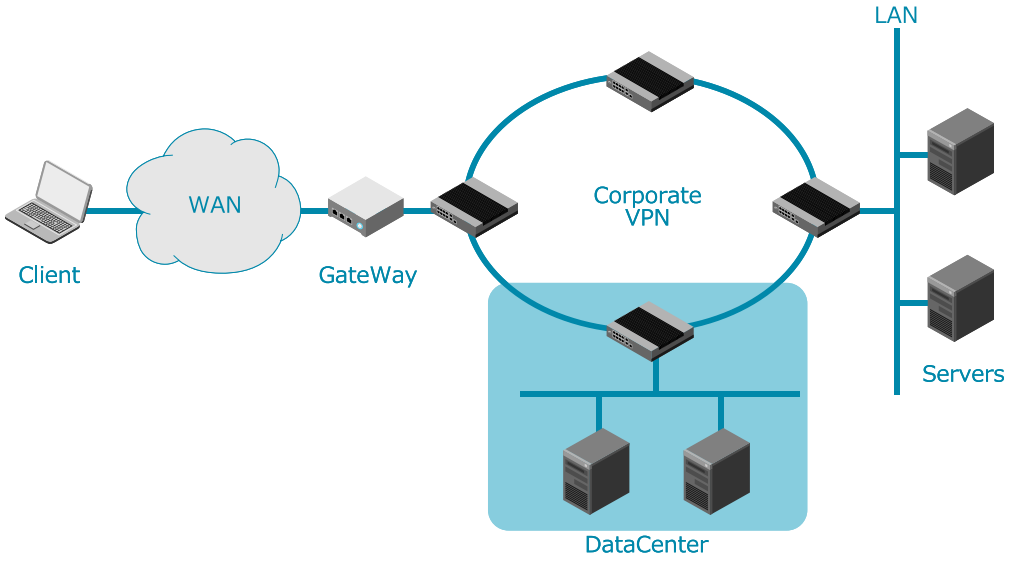
ファイルサーバや各種システムへのアクセスは、「必要な人のみ、必要な権限を与える」を原則としています。組織変更などに伴う変更や削除についてもルールに則り対応しています。

アクセスコントロールの一例として、バリデーション実施後の記録は電子データ化した上で、アクセス権限設定した社内サーバに保存しております。情報をいつでも利用できる形で、高い機密性を保持しながら保管していることでお客様の記録のバックアップとしても機能します。

b. ネットワークセキュリティ

各拠点間にVPNを構築し、安全なデータ通信の仕組みを運用していますが、迅速なビジネスを展開する上で欠かせない社外から社内にあるシステムへの接続のために SSL-VPN を導入しています。

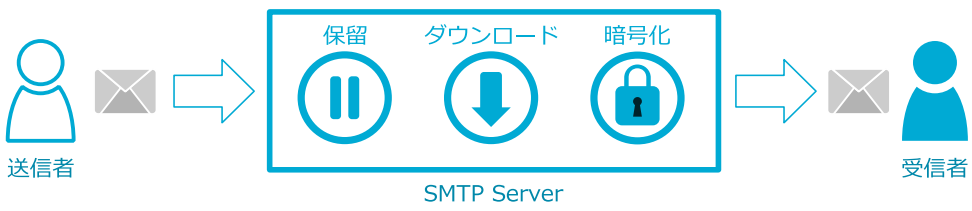
社内ネットワークに存在する限定したシステムに対して、接続可能な PC を限定し、接続ユーザ識別子とパスワードにより認証できたセッションのみ接続可能としてセキュリティを確保しております。



c. メールセキュリティ

メールはお客様はじめ様々なステークホルダーと情報のやりとりをする一般的なツールですが、意図した送信先以外への誤送信は情報セキュリティインシデントとなりえます。メール誤送信を防止するための仕組みを用意して全社で運用しています。

また、社外からのメールに含まれる脅威への対策としてメールサーバにスパムメールを自動判別するフィルタ機能を持たせています。



d. エンドポイントセキュリティ

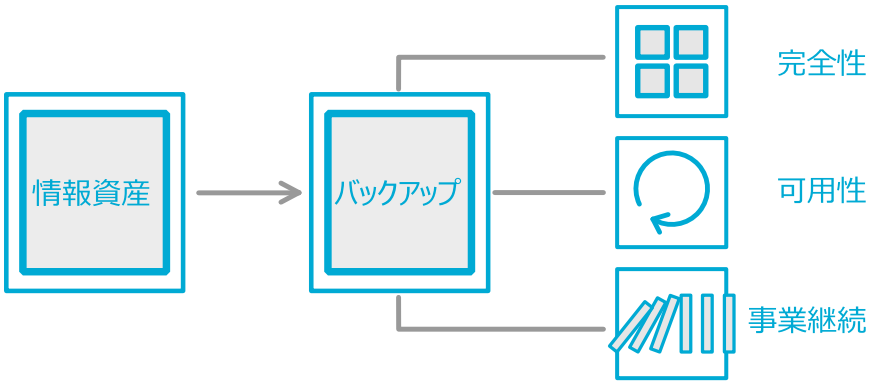
PC や携帯電話は社外で使用することが多い機器です。これらから情報が漏えいするリスクがあるため社外に持ち出した際の情報漏えいリスクを低減する仕組みを導入しています。

・ PC に対するセキュリティ対策実施
・ PC へのアンチウイルスソフトの導入と自動アップデート設定
・ 携帯電話のリモートワイプおよびロック設定
・ 社外ネットワークへの接続は Wi-Fi ルータ使用（有線 LAN への直接接続禁止）

e. バックアップ

データが使うべきときに使えないのはデータの可用性や完全性を著しく損ねるだけでなく、事業継続にも関わる問題です。データに関してリスク評価を実施してバックアップの必要性や条件（バックアップ頻度、世代数、バックアップ先、媒体、ツールなど）について判断しています。

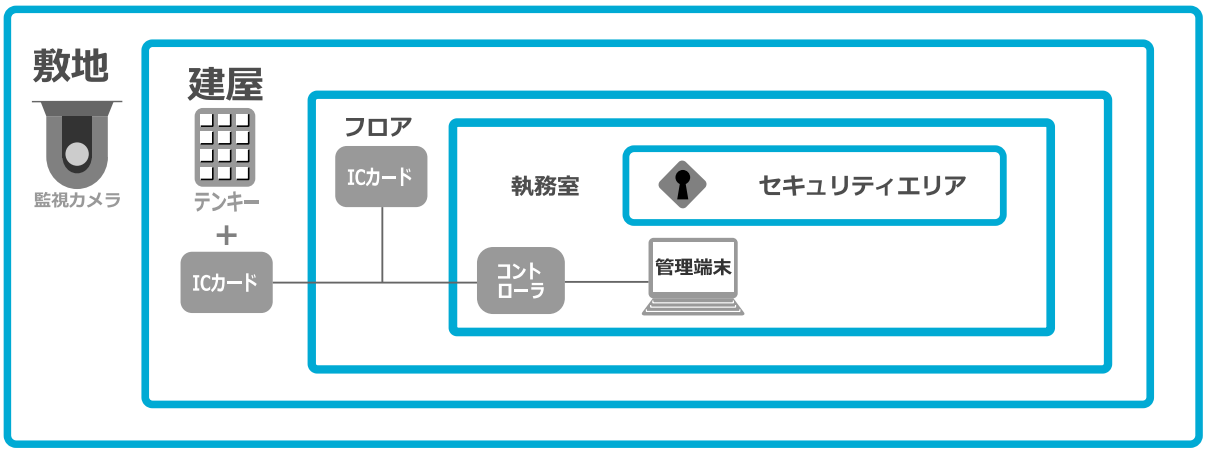
バックアップおよびリストアの手順を定め、必要なものについてはリストアの確認を実施しています。



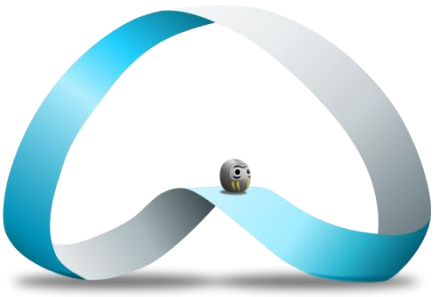
物理的セキュリティの取り組み

情報漏えいへの不正アクセス防止や不正侵入防止のために物理的セキュリティ対策が有効です。当社では、拠点ごとに二重化対策を実施しております。

ID カードを利用して建屋への入館やビル内の移動時の入室制限を行っています。



BCM に関する取り組み



開発・営業・サポートなどの各事業プロセスにおいてサイエンスベースの合理的な意志決定のための根拠データや新たな製品・サービスの核となるデータを「重要情報群」と位置づけております。
それらデータの生成・移動・保存・活用の各プロセスにおける情報セキュリティリスクを低減させる活動に取り組んでいます。
また、リスクが顕在化した場合の早期復旧のための仕組みも構築しています。
レジリエンスの高い情報セキュリティシステムの構築に努めていきます。

個人情報管理について

個人情報の取扱いに万全を期することは、当社の社会的責務と考え、個人情報を安全に管理するために個人情報保護に関する法令、国が定める指針その他の規範を遵守します。
個人情報の管理に関する体制を構築し、責任を明確にした上で、その取扱いに関するルールを設けルールに則った運用をしております。
個人情報を保有するにあたり、個人情報を適切に管理するために本レポートに記載している技術面、組織面の安全対策を実施しております。また、運用ルールの妥当性や有効性を定期的に見直しています。

2015 年 04 月 30 日更新