未来を、ひろげる。
HIROGIN HOLDINGS

News Release

2025 年 9 月 1 日

「サイバーセキュリティ基本方針」の策定について

株式会社ひろぎんホールディングス（社長 部谷 俊雄）およびグループ会社では、近年増々高まるサイバーセキュリティのリスクに対応するため、「サイバーセキュリティ基本方針」を策定しましたので、下記のとおりお知らせいたします。

記

1. 背景と目的

近年、インターネットや AI などの新たな技術の急速な普及により、各種サービスのデジタル化が進展し、利便性が大きく向上する一方で、サイバー攻撃の手口も高度化・巧妙化し、情報漏洩や不正アクセスなどのリスクが増大しています。特に銀行や証券会社等の金融機関においては、社会インフラとしての重要な役割を担う中で、サイバーインシデントの脅威が金融サービス利用者の利益や金融システム全体の安定に大きな影響を及ぼす可能性が高まっています。

こうした状況を踏まえ、当社グループは、地域社会の発展とお客さまの信頼に応えるべく、サイバーセキュリティの強化を経営の重要課題のひとつと位置づけ、サイバーセキュリティ管理態勢および適切な防御策を講じるための基礎とし、グループ全体でサイバーリスクへの対応力を高めるべく、「サイバーセキュリティ基本方針」を策定いたしました。

これらの取り組みの意義を地域社会やお客さまに対して表明し、ご安心いただくために、本件「サイバーセキュリティ基本方針」を公表するものです。

2．「サイバーセキュリティ基本方針」の概要（全文は別紙のとおり）

以下の 5 つの柱を中心に、サイバーセキュリティ対策を推進してまいります。

(1)経営課題としての認識	経営会議・取締役会で定期的に議論・検証し、経営主導の継続的なリスク対策を推進します。
(2)経営方針の策定と意思表明	サイバーリスクに対応する経営方針を策定し、社内外のステークホルダーへの意思表明を行うとともに、各種報告書等へ記載・開示します。
(3)社内外体制の構築・対策の実施	必要な人員の配置、最新技術の導入等により、サイバーインシデントへの先行的な対策および予防的措置を講じます。
(4)対策を講じたシステムやサービスの社会への普及	お客さまに安心して当社グループのサービスをご利用いただくための対策を講じます。
(5)安心・安全なエコシステムの構築への貢献	関係官庁や組織と連携し、サプライチェーン全体、ひいては社会全体のサイバーセキュリティ強化に貢献します。

なお、別紙「サイバーセキュリティ基本方針」については、当社ウェブサイトに公開します。

以 上

本件に関するお問い合わせ先

株式会社ひろぎんホールディングス
業務統括部 IT 統括グループ
TEL（082）245 – 5151（代表）

サイバーセキュリティ基本方針

株式会社ひろぎんホールディングスおよびグループ会社(*)（以下、「当社グループ」）は、〈地域総合サービスグループ〉として、地域社会における当社グループの存在意義を明確に示すとともに、当社グループ・従事者の回帰すべき原点として制定したパーパス『幅広いサービスを通じて、地域社会と共に、「未来を、ひろげる。」』を実現するため、多種多様なサービスの提供とその維持・発展に努めています。

現代社会では、インターネットや AI 等の新たな技術の普及により、金融サービスのデジタル化が急速に進み、インターネットバンキングや QR 決済等のサービスが普及し、企業や個人の重要なデータがオンラインで管理されるようになりました。それに対して、金融インフラを狙うサイバー攻撃による情報漏洩や不正アクセスの被害が増加しており、手口も高度化・巧妙化する中、サイバーインシデント発生のリスクの高まりとともに、その脅威は、金融サービス利用者の利益を害し、また金融システムの安定に多大な影響を及ぼしかねないものとなっています。

当社グループでは、こうした脅威に対応しお客さまに安心してご利用いただけるサービスを提供するため、不正アクセスやデータ漏洩を防止するための最新技術の導入と、従事者の教育・訓練の徹底による厳格な管理態勢の構築に努めます。

(*)グループ会社・・・株式会社ひろぎんホールディングスの連結子会社

1.経営課題としての認識

経営者自らが最新情勢への理解を深めることを怠らず、DX を進める上で必須となるサイバーセキュリティを投資と位置づけて積極的な経営に取り組みます。また、経営者自らが現実を直視して DX の推進およびデジタル化に伴うリスクと向き合い、サプライチェーン全体を俯瞰したサイバーセキュリティの強化を経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組みます。

具体的には、サイバーリスクを当社グループのトップリスクの 1 つとして定義し、取締役会・経営会議等で定期的に議論・検証し、DX およびデジタル化とサイバーセキュリティ対策の両立を意識して、適切なリソースを配分し、経営主導で継続的にリスク対策を推進します。

2.経営方針の策定と意思表明

特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けたBCP(事業継続計画)の策定を行います。経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努めます。

具体的には、高度化するサイバーリスクに対応するためにグループ各社の CSIRT メンバーで構成される「ひろぎんグループ CSIRT」を設置し、定期的な訓練や演習、手順書や規定整備等の平時の備えに加え、有事の際には専門の協力会社と共同で 24 時間 365 日での緊急対応に取り組みます。また、統合報告書等を通じてサイバーセキュリティ強化の取り組みについて開示します。

3.社内外体制の構築・対策の実施

予算・人員等のリソースを適切に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じ、経営・企画管理・技術者・従事者の各層における人財育成や教育を行います。また、サイバーセキュリティ対策のガイドラインの活用や、政府によるサイバーセキュリティ対策支援活動との連携等を通じて、取引先や委託先を含めたサプライチェーン対策に努めます。

具体的には、サイバーセキュリティに係る専担部署に必要な人員を配置の上、DX およびデジタル化と働き方改革といった環境変化を踏まえた最新のサイバーセキュリティ技術を導入し、サイバーインシデントへの先行的な対策および予防的措置を講じます。また、サイバーセキュリティに係る専担部署から独立した部署によるチェック・監査を通じて、その実効性を高めていきます。

人的対策については、グループ役職員全体のサイバーセキュリティに関するリテラシー向上として定期的に研修やメール訓練を行います。専門人財の確保・育成については、外部からの採用や専門機関・金融 ISAC 等によるサイバーセキュリティトレーニングを通じ、積極的に取り組みます。

また、当社グループだけでなくクラウドサービス等委託先、取引先へのモニタリング等を継続して行い、サプライチェーン対策を実践します。

4.対策を講じたシステムやサービスの社会への普及

システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努めます。

具体的にはお客さまが安心して金融サービスをご利用いただけるよう最新のサイバーセキュリティ対策ソリューションを導入し、サイバーリスクの脅威に対して先行的・予防的に対応できる態勢を整備します。また、お客さまが金融サービスをご利用になる際の安全意識の啓発に努めます。

5.安心・安全なエコシステムの構築への貢献

関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワークの構築を図ります。また、各種情報を踏まえた対策に関して注意喚起することによって、サプライチェーン全体、ひいては社会全体のサイバーセキュリティ強化に貢献します。

具体的には、金融庁、国家サイバー統括室、情報処理推進機構、警察等の関係官庁等からの要請事項への対応および適時適切な報告を行うとともに、金融 ISAC、JPCERT 等のサイバーセキュリティに関する情報機関等と積極的に情報交換を行い、社会全体のサイバーセキュリティ対策の向上に努めます。

(2025 年 9 月 1 日　策定)