

金融機関向けサイバーセキュリティ 監査・アセスメントサービス

EY新日本有限責任監査法人
Technology Risk事業部

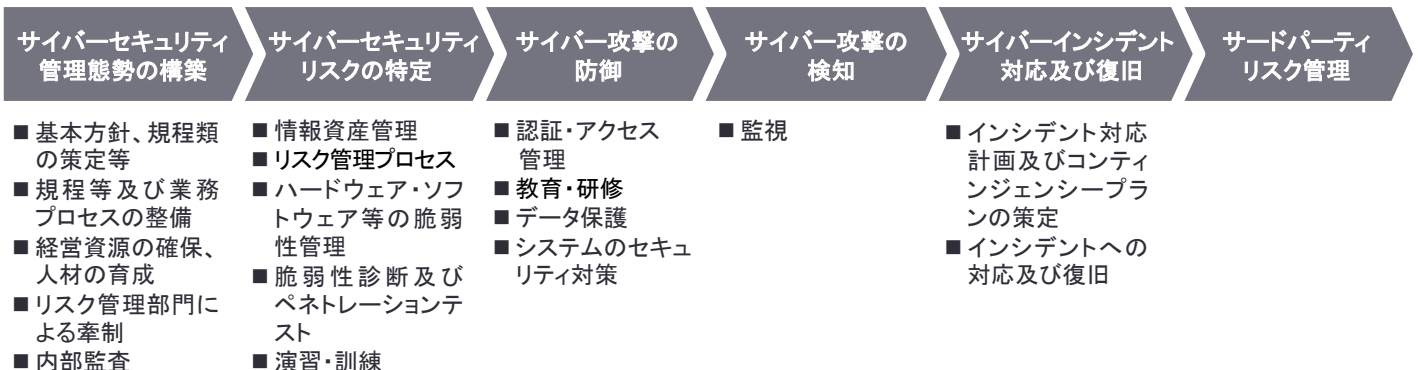
昨今のサイバーセキュリティ被害の深刻度が増している中、金融機関においてもランサムウェア攻撃によるデータ暗号化や業務停止、外部委託先の端末がマルウェアに感染することによるデータ流出事案等が発生しています。銀行等、生命保険、損害保険、証券及び資金決済分野の事業者は社会の重要インフラ事業者に指定されており、サイバーインシデント発生時に顧客や金融システムへの影響を最小化するため、サイバー攻撃による業務停止や信用失墜を防ぐ強固なセキュリティ体制が不可欠です。

■ EYができること

国内では、金融庁から令和6年10月4日に「金融分野におけるサイバーセキュリティに関するガイドライン」が公表されており、各金融機関で対応が行われています。また、大手金融機関では、これまで広く利用されてきたFFIEC Cybersecurity Assessment Toolの廃止を受けてCyber Risk InstituteのCRI Profileへの移行が進められています。EYでは、金融機関で広く活用されている国内外のガイドライン等に基づき、監査・アセスメントからロードマップ策定、施策推進まで一環したサポートが可能です。



■ 金融分野におけるサイバーセキュリティに関するガイドライン



The better the question.
The better the answer.
The better the world works.



Shape the future
with confidence

■ CRI Profileとは

CRI Profileは、米国の非営利団体Cyber Risk Institute(CRI)が金融機関や業界団体等と連携して開発した、金融業界向けのサイバーセキュリティ及びITリスク管理の評価フレームワークであり、進化し続ける脅威に対し効果的に対抗し、テクノロジーやサイバーセキュリティに関するリスク管理の効率的なアプローチとして開発されました。CRI Profileは、NIST Cybersecurity Framework(NIST CSF)をベースに、金融機関に求められるリスク管理・ガバナンス・統制要件をより実務的・具体的な管理策として体系化されています。

■ CRI Profileの特徴

CRI Profileでは、組織が社会に及ぼすImpactの大きさによりTier1～4に分類します。この分類(Tier)により、全318(v2.1時点)の管理策のうち、評価対象となる項目数が異なります。自組織がどのTierに該当するかは、「Impact Tiering Questionnaire」と呼ばれる9項目の質問回答により診断できます。

■ CRI Profileのカテゴリと管理策数

カテゴリ	管理策数
GV:GOVERN(統治)	97
ID:IDENTIFY(識別)	64
PR:PROTECT(防御)	74
DE:DETECT(検知)	24
RS:RESPOND(対応)	16
RE:RECOVER(復旧)	11
EX(サプライチェーンリスク管理)	32
合計	318

■ Tier定義及び評価対象となる管理策数

Tier	定義	管理策数
Tier1	National/Super-National Impact 世界経済の安定性に影響を与える可能性のある組織	318
Tier2	Subnational Impact 全国規模で影響を与える可能性のある組織	311
Tier3	Sector Impact 地域の金融サービスセクターに影響を与える可能性のある組織	282
Tier4	Localized Impact 100万人未満の顧客で地域的な組織	208

■ CRI Profile評価の意義、EYの支援

CRI Profileは、金融業界向けのサイバーリスク評価として規制当局や業界団体から国際的に認知され、グローバルで活用されています。EYは、国内外におけるIT、セキュリティ評価に関する豊富な経験に基づき、金融業界におけるサイバーセキュリティのプロフェッショナルとグローバルに連携して、組織における課題特定と改善施策の推進を支援します。

お問い合わせ先

EY新日本有限責任監査法人 Technology Risk事業部

URL: ey.com/ja_jp/technology-risk

サービス担当者またはウェブサイトお問い合わせフォームよりお問い合わせください

EY | Building a better working world

EYは、クライアント、EYのメンバー、社会、そして地球のために新たな価値を創出するとともに、資本市場における信頼を確立していくことで、より良い社会の構築を目指しています。

データ、AI、および先進テクノロジーの活用により、EYのチームはクライアントが確信を持って未来を形づくるための支援を行い、現在、そして未来における喫緊の課題への解決策を導き出します。

EYのチームの活動領域は、アシュアランス、コンサルティング、税務、ストラテジー、トランザクションの全領域にわたります。蓄積した業界の知見やグローバルに連携したさまざまな分野にわたるネットワーク、多様なエコシステムパートナーに支えられ、150以上の国と地域でサービスを提供しています。

All in to shape the future with confidence.

EYとは、アーnst・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーnst・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。EYによる個人情報の取得・利用の方法や、データ保護に関する法令により個人情報の主体が有する権利については、ey.com/privacyをご確認ください。EYのメンバーファームは、現地の法令により禁止されている場合、法務サービスを提供することはありません。EYについて詳しくは、ey.comをご覧ください。

EY新日本有限責任監査法人について

EY新日本有限責任監査法人は、EYの日本におけるメンバーファームであり、監査および保証業務を中心に、アドバイザリーサービスなどを提供しています。詳しくは、ey.com/ja_jp/about-us/ey-shinnihon-llcをご覧ください。

© 2026 Ernst & Young ShinNihon LLC.
All Rights Reserved. ED None

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務およびその他の専門的なアドバイスをを行うものではありません。EY新日本有限責任監査法人および他のEYメンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家に相談ください。

ey.com/ja_jp