実践サイバーレジリエンス

実践ガイド

目次

3 はじめに

4 共創

5 サイバーレジリエンスを成功に導く10のステップ

16 実装ロードマップ

17 サイバーレジリエンスの枠組み

18 まとめ

19 貢献者

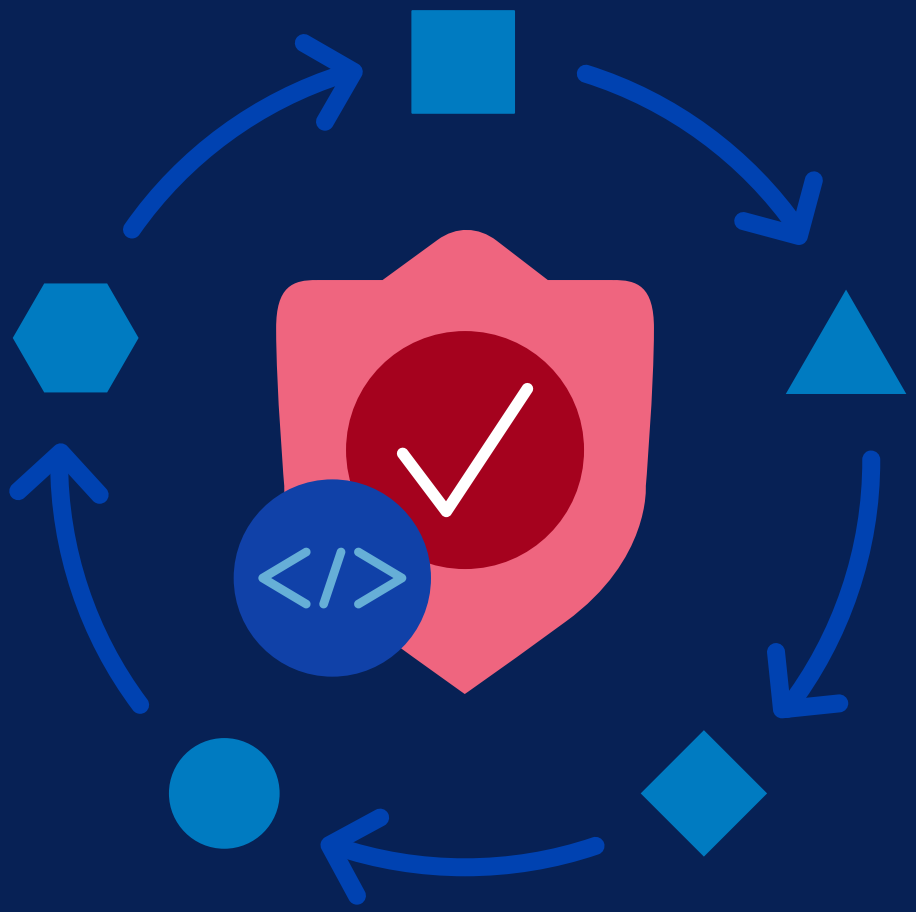
はじめに：企業のサイバーレジリエンスを構築するための10ステップのプレイブック

セキュリティリーダーは、進化するサイバー脅威に予防的に対処することで、組織のレジリエンスを向上させ、リスクの影響を最小限に抑えることができます。このプレイブックでは、セキュリティ投資と運用効率を最適化しながら、企業のサイバーレジリエンスを構築し維持するための10のステップについて解説します。

主な所見

- サイバーレジリエンスをビジネス目標と一致させている組織は、効果的な投資の最適化とリスクの最小化を実現しています。
- 運用レジリエンスを維持しながら新たな技術を安全に統合できるかどうかが、多くのセキュリティリーダーにとっての課題となっています。
- サイバーレジリエンスの取り組みにはCXOのサポートが不可欠ですが、確実にチャンスをものにするためには十分な準備とコミュニケーションも必要です。
- 堅牢なガバナンスの枠組みを構築し、セキュリティ意識の高い文化を育てることで、組織はサイバーインシデントに確実に対応し復旧できます。

これは、アジアの動的なテクノロジーハブ3拠点における47人の業界リーダーの知識と実体験を集約して導き出された洞察です。



共創

このプレイブックでは、金融サービスから技術までさまざまな部門を代表する経営陣や、CISO、CIO、セキュリティアーキテクトなど、アジアの動的なテクノロジーハブ3拠点における37人の業界リーダーの知恵と実体験を集約して導き出された洞察を紹介します。この多地域連携により、サイバーレジリエンスに対する多様な視点が集結し、各地域固有の課題や革新的な手法も加わり、さらに豊かなものになりました。

ムンバイ

専門家は、基盤となるガバナンスとリスク管理を確立するために、サイバーレジリエンスを戦略的ビジネス目標と一致させ、グローバルなコンプライアンスの枠組み（ISO 27001、NIST CSF）を企業運営に統合することを焦点としました。

バンガロール

地域のソートリーダーは、新しい技術をセキュアに統合することの重要性を強調し、革新と適応可能性を提唱しました。このセッションでは、自己修復システムやゼロトラストアーキテクチャ、そして AI を活用した脅威予測モデリングなどの高度な実践が紹介されました。

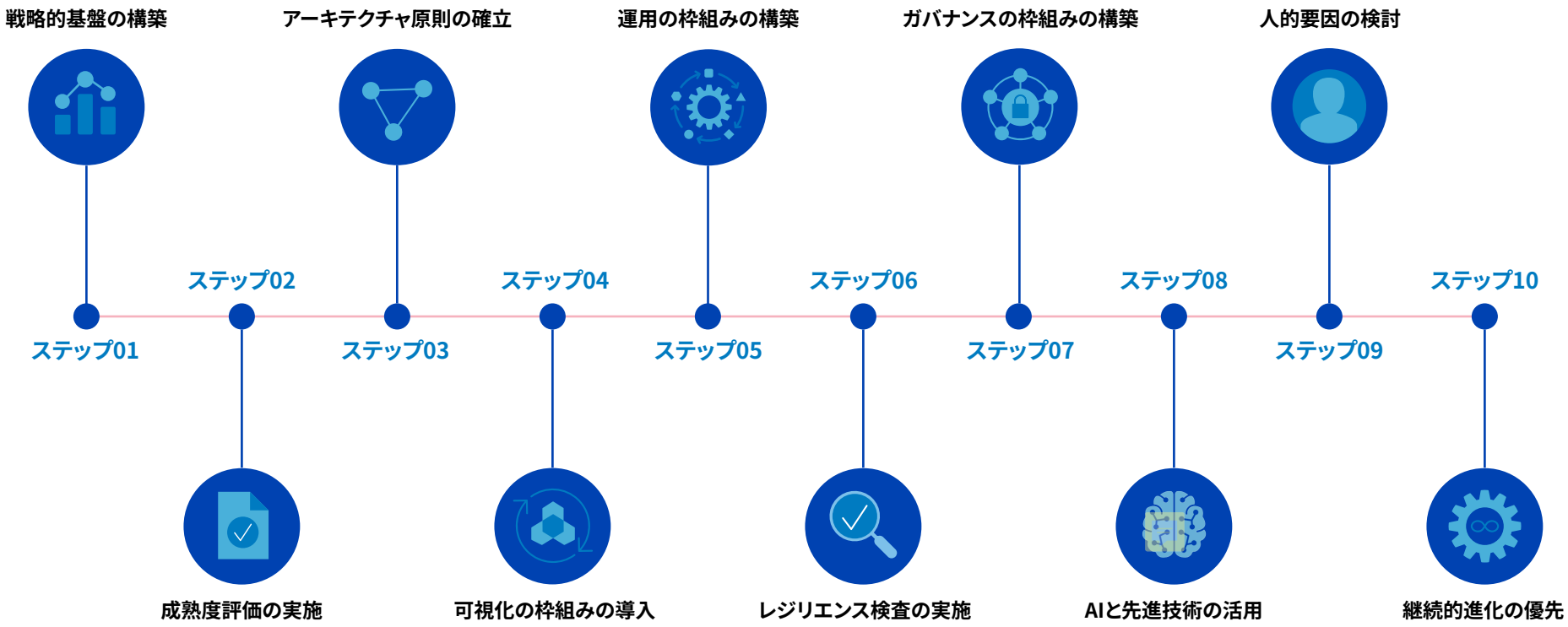
クアラルンプール

参加者は、予防的な脅威管理とインシデント対応による卓越した運用を実現するために、リアルタイムの監視、AI を活用した分析、混乱を最小限に抑えるためのクラウドレジリエンスを優先事項に挙げました。

東京

ガバナンス、コンプライアンス、誤検知を重点的に、AI を活用したセキュリティの課題について議論が行われ、レジリエンスを強化し、労働力ギャップを解消するための重要な戦略として、自動化、AI 検証の枠組み、リスク管理委員会が挙げられました。

サイバーレジリエンスを成功させるための10のステップ



ステップ01
戦略的基盤

目的
セキュリティの現状とビジネスの優先順位を関連付け、レジリエンスへの取り組みを始めます。この基盤は成功のために不可欠です。

根拠
この基盤により、セキュリティへの投資が、孤立した意思決定ではなく、戦略的要因となります。

結果
セキュリティプログラムにより、事後反応的な防御の枠組みがビジネス戦略の予防的要因に変わります。

1.1　ビジネスインパクト分析の実施
- 重要なシステムに優先順位を付け、依存関係を評価する
- 測定可能なROI指標に基づき、セキュリティ投資とビジネス目標を関連付ける
- ビジネス目標の進化に合わせ、戦略的整合性を定期的に見直す
- ビジネスプロセスとセキュリティ管理の相互依存性を文書化する

1.2　リスク許容度の枠組みの定義
- SLAと連動した明確なリスクしきい値を設定する
- リスクコミュニケーションのための財務損失モデルを作成する
- 業界標準の許容リスクレベルを設定する
- 四半期ごとにリスク許容度を見直し、更新する

1.3　コンプライアンス要件の統合
- 世界標準（ISO 27001、NIST CSF）を運用に組み込む
- コンプライアンスを戦略的優位性として活用する
- 継続的な監視システムを導入する
- コンプライアンス文書を最新の状態に保つ

ステップ02
成熟度評価

目的
セキュリティ体制を包括的に評価し、長所、ギャップ、機会を特定します。この評価により、変革基準が構築されます。

根拠
現在の能力を測ることで、組織は、戦略に整合した投資を行い、包括的なセキュリティ対策を実現できます。

結果
セキュリティプログラムを現状から目標の状態へと進化させる、データを活用した明確なロードマップを作成できます。

2.1　現状の分析
- 既存のセキュリティ管理と能力を見直す
- 組織のセキュリティ文化を評価する
- サードパーティのセキュリティリスクを評価する
- 技術スタックとセキュリティツールを文書化する

2.2　能力ギャップの特定
- 業界ベンチマークと現状を比較する
- リスク影響度に基づきギャップに優先順位を付ける
- 能力強化ロードマップを作成する
- 各能力の成功指標を定義する

2.3　目標状態の定義
- 現実的な成熟度目標を設定する
- ビジネスの目的に合わせる
- 段階的な改善計画を策定する
- 目標測定の枠組みを構築する

ステップ03
アーキテクチャ原則

目的
レジリエンスの背骨となる、ゼロトラストの適応型セキュリティアーキテクチャを確立し、新たな脅威に合わせて進化させます。

根拠
従来の境界ベースのセキュリティでは、最新の脅威に対抗できません。防御と迅速な復旧を両立できるアーキテクチャが必要です。

結果
俊敏なビジネスを実現しながら、脅威を自動的に検出し、それに対応して適応する、将来を見据えたセキュリティインフラストラクチャを導入できます。

3.1　ゼロトラストアーキテクチャの導入
- 継続的な検証を行いながら、役割ベースのアクセス制御を導入する
- 重要な資産にマイクロセグメンテーションを行う
- 強力な認証メカニズムを実装する
- セキュリティを重視してネットワークアーキテクチャを設計する

3.2　適応型レジリエンスの構築
- 自動復旧メカニズムを導入する
- アクティブ-アクティブ構成を導入する
- クラウドベースの冗長化を実現する
- マイクロサービスアーキテクチャを活用する

3.3　先進技術の統合
- AIを活用したSIEMソリューションを導入する
- ベンダーニュートラルなクラウドアーキテクチャを実装する
- APIセキュリティ管理を標準化する
- IoTとエッジコンピューティングのインフラストラクチャを保護する

ステップ04
可視化の枠組み

目的
すべての資産、脅威、リスクを包括的に可視化します。見えないものを守ることはできません。

根拠
エンドツーエンドで可視化できなければ、脅威は検出されず、リスクが隠れたままとなり、危険なセキュリティの死角が生まれます。

結果
セキュリティの全体像を把握することで、脅威を予防的に検出し、情報に基づいて意思決定できるようになります。

4.1　資産管理の強化
- 資産の自動検出ツールを導入する
- リアルタイムの資産管理を維持する
- シャドー IT 活動を監視する
- 資産間の依存関係や関係性を追跡する

4.2　脅威検出の導入
- AI を活用した脅威分析を導入する
- リアルタイムの脅威監視を実現する
- 脅威インテリジェンスフィードを統合する
- アラートの優先順位付けの枠組みを構築する

4.3　リスクダッシュボードの作成
- 役員レベルのリスク可視化を構築する
- 主要なリスク指標を追跡する
- コンプライアンス状況を監視する
- 予測リスク分析を導入する

ステップ05
運用の枠組み

目的
ツールの統合、ワークフローの自動化、チームへの権限付与により、セキュリティ運用を事後反応型から事前対応型に変えます。

根拠
サイロ化された運用と手動のプロセスでは、脅威への対応が遅れ、セキュリティリソースに負担がかかります。

結果
セキュリティ運用を合理化することで、迅速な対応と効率的な拡張が可能になり、チームは戦略的優先事項に集中できるようになります。

5.1　対応計画の策定
- 詳細なインシデントプレイブックを作成する
- 事業継続計画に合わせる
- 明確なエスカレーション手順を決める
- コミュニケーションプロトコルを確立する

5.2　セキュリティツールの統合
- セキュリティプラットフォームを統合する
- セキュリティワークフローを自動化する
- クロスプラットフォームの統合を可能にする
- ログを一元管理する

5.3　セキュリティチームの強化
- 役割ベースのセキュリティツールを提供する
- ルーチンタスクを自動化する
- 共同対応を可能にする
- ナレッジマネジメントシステムを実装する

ステップ06
レジリエンス検査

目的
厳格な検査と継続的な測定により、セキュリティレジリエンスを検証します。仮説は行動によって立証されなければなりません。

根拠
未検査のセキュリティ対策は、最も必要なときに失敗することが多くあります。定期的な検査により、攻撃者よりも先にギャップを特定できます。

結果
実戦で実証されたセキュリティプログラムにより、実世界でも保護と復旧が確実になります。

6.1　定期的な評価の実施
- 侵入検査を計画する
- 脆弱性評価を実施する
- 災害復旧訓練を実施する
- 事業継続計画を検査する

6.2　対応の有効性の測定
- 平均検出時間を追跡する
- 平均対応時間を監視する
- 復旧時間目標を評価する
- 復旧時点目標を検証する

6.3　継続的改善の実施
- 教訓を文書化する
- 対応プレイブックを更新する
- 検査手順を改良する
- ベストプラクティスを共有する

ステップ07
ガバナンスの枠組み

目的
セキュリティプログラム全体で説明責任と倫理的意思決定を推進する、構造化されたガバナンス体制を確立します。

根拠
強力なガバナンスにより、セキュリティへの取り組みが集中的に、説明責任を果たし、一貫性を持って実行されます。

結果
周到なセキュリティプログラムにより、明確なポリシーとリーダーシップを通じて、革新と管理を両立できます。

7.1　管理体制の確立
- セキュリティ運営委員会を設置する
- 報告系統を定義する
- 意思決定権限を設定する
- 定期的に見直す

7.2　AIガバナンスの構築
- AIリスクの枠組みを構築する
- 倫理ガイドラインを確立する
- AIシステムの有効性を監視する
- 説明責任評価基準を決める

7.3　ポリシーの枠組みの維持
- セキュリティポリシーを定期的に更新する
- 業界標準に合わせる
- コンプライアンス要件を監視する
- ガバナンス手順を文書化する

ステップ08
AIと先進技術

目的
AIや新たな技術を活用し、責任ある実装を確実にしながら
セキュリティ機能を強化します。

根拠
従来のセキュリティ手法では、最新の脅威に対応できないので、
AIと先進技術が不可欠です。

結果
将来を見据えたセキュリティプログラムにより、自動化とAIを活用し、
マシンスピードで脅威を検出、防止、対応できます。

8.1　AIセキュリティソリューションの導入
- AIを活用したXDRを導入する
- 脅威対応を自動化する
- 予測分析を導入する
- AIモデルの有効性を監視する

8.2　新たな技術の保護
- 革新の枠組みを構築する
- 「セキュリティ・バイ・デザイン」を実施する
- セキュアなクラウド導入を実現する
- IoTセキュリティ管理を導入する

8.3　技術ガバナンスの維持
- 技術リスクを監視する
- セキュリティ管理を更新する
- 技術依存関係を追跡する
- セキュリティ影響を評価する

ステップ09
人的要因

目的
文化、スキル開発、継続的な学習を通じて、従業員を最強の
セキュリティ資産に変えます。

根拠
技術だけではセキュリティを確保できません。人間の行動と専門知識は、
サイバーレジリエンスの重要な要素です。

結果
すべての従業員がサイバーレジリエンスに積極的に貢献できる、
セキュリティ意識の高い組織となります。

9.1　セキュリティ文化の構築
- セキュリティ意識向上プログラムを導入する
- ゲーム型トレーニングを実施する
- セキュリティチャンピオンを選出する
- 報奨の仕組みを構築する

9.2　セキュリティ人材の育成
- キャリア開発パスを設定する
- 資格認定プログラムを実施する
- メンターシップイニシアチブを確立する
- スキル開発を支援する

9.3　継続的な学習の環境の提供
- トレーニングリソースを提供する
- 脅威情報を共有する
- ナレッジシェアリングを実現する
- 学習コミュニティを作る

ステップ10
継続的進化

目的
体系的な評価と適応を通じてサイバーレジリエンスを強化する動的な枠組みを構築します。

根拠
進化する脅威に対抗するには、サイバーレジリエンスに不可欠である継続的な適応を実施する、動的なセキュリティ対策が必要です。

結果
学習、変化する脅威、新しいベストプラクティスにより進化する適応型セキュリティプログラムを実施できます。

10.1　総体的な評価の実施
- 管理の有効性と成熟度を測定する
- 脅威インテリジェンスとインシデントパターンを分析する
- ビジネスへの影響と整合性を評価する
- コンプライアンスとリスク管理体制を見直す

10.2　能力強化の重点化
- 検出および対応メカニズムを強化する
- 技術的能力を向上させる
- チーム能力を向上させる
- セキュリティ運用を最適化する

10.3　戦略的適応の優先順位付け
- セキュリティ戦略とロードマップを更新する
- リソースと投資を再調整する
- ポリシーと手順を改善する
- 次のサイクルへ洞察を橋渡しする

実装のロードマップ

フェーズ 1：基盤
（0 ～ 6 か月）

- 初期リスク評価を実施する
- ガバナンスの枠組みを構築する
- 基本的なセキュリティ管理を導入する
- セキュリティ意識向上トレーニングを始める

フェーズ 2：拡張
（6 ～ 12 か月）

- 最新セキュリティソリューションを導入する
- AI を活用した機能を導入する
- 監視と対応を強化する
- セキュリティプログラムの範囲を拡大する

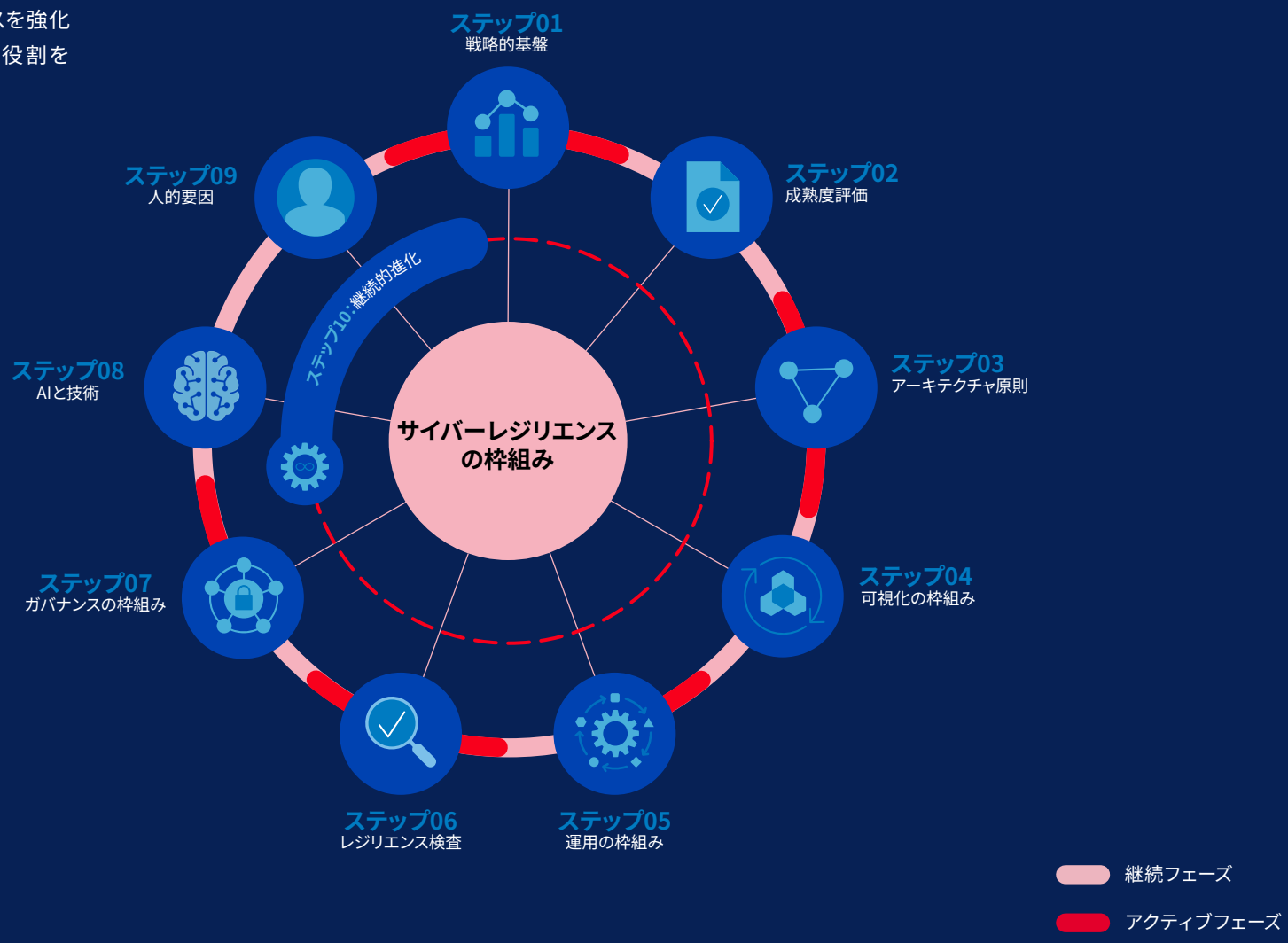
フェーズ 3：最適化
（12 か月以降）

- 予測能力を実現する
- 自動化を大規模に実施する
- セキュリティ運用を最適化する
- 成熟したセキュリティ体制を実現する

サイバーレジリエンスを成功させるための10のステップ

効果的なサイバー防衛には、積極的な導入と継続的な評価をシームレスに統合した、動的で進化し続ける枠組みが必要です。

各構成要素は、サイバーレジリエンスを強化および維持する上で極めて重要な役割を果たします。



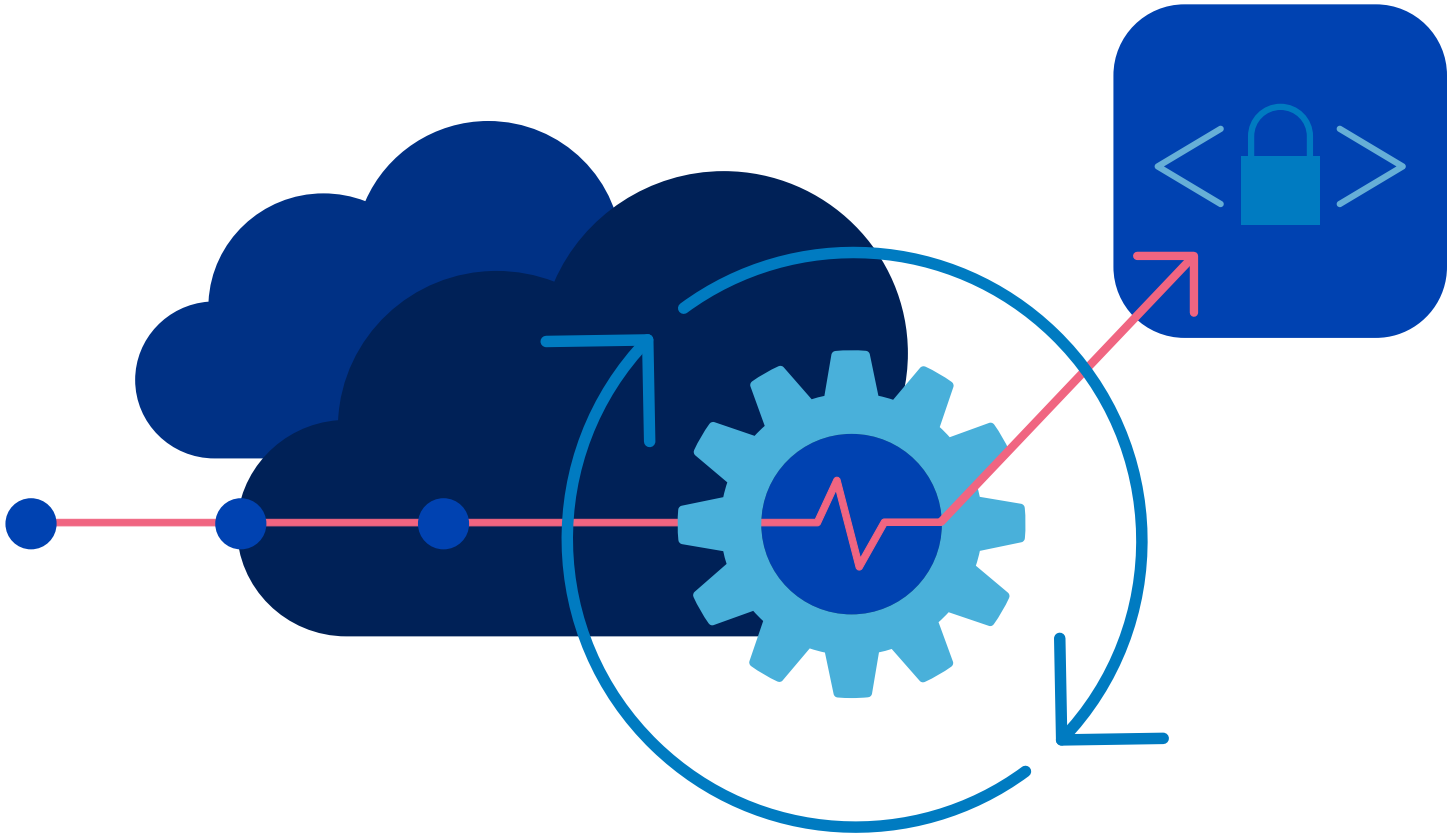
まとめ

サイバーレジリエンスの構築は、技術、人材、プロセスの連携を必要とする継続的な取り組みです。このプレイブックでは、ビジネスの成長と革新を実現しながら組織のセキュリティ体制を強化するための構造的な手法について説明しました。この枠組みを定期的に見直し、更新することで、進化する脅威に対する継続的な有効性を確保できます。

詳細

セキュリティ投資と業務効率を最適化しながら、企業のサイバーレジリエンスを強化する方法について詳しくは、こちらをご覧ください。

効果的なサイバー防衛には、各構成要素がサイバーレジリエンスの維持において重要な役割を果たす、動的で進化し続ける枠組みが必要です。



貢献者

Abhijit Chakravarthy
Kotak Bank、執行副社長

Abhishek Jha
Citi Global Markets India、最高情報セキュリティ責任者

Amitabh Sharan
DHL IT Services、エクスプレスソリューション、システムインテグレーション、ドメイン責任者

Amogh Zade
ECGC、副最高技術責任者

Arif Bhatkar
Godrej Infotech、情報技術セキュリティ部門責任者

Ashutosh Pathak
Manipal Global Education、IT部門責任者

Azril Rahim
Tenaga Nasional Berhad、サイバー脅威インテリジェンス管理部門責任者

G Saravanan
Thomson Hospital、グループ最高情報責任者

Hilal Ahmad Lone
Razorpay、最高情報セキュリティ責任者

James Thang
UCSI Group Holdings、グループ最高情報責任者

Lalit Trivedi
FlexM、情報セキュリティ部門責任者

Maz Mirza
KWAP、最高デジタル責任者

Mohd Hanapi Bin Bisni
Petra Energy Berhad、グループIT部門責任者

Munish Blaggan
ICICI Bank、インフラストラクチャグループ、技術部門責任者

Nehal Shah
IDBI Bank、副最高技術責任者

Dr. Naresh Kumar Harale
Reserve Bank Information Technology (ReBIT)、最高情報セキュリティ責任者兼サイバーセキュリティ部門バーティカルヘッド

Dr. Pawan K Sharma
Tata Motors、最高情報セキュリティ責任者

Philip Varughese
DXC Technology、DXCセキュリティ、アプライドインテリジェンス、プラットフォーム、エンジニアリング部門グローバルヘッド

Praveen Samariya
Medi Assist、最高技術責任者

Raghu P
Canbank Factors Limited、最高技術責任者

Rahul Malhotra
Intertrust Group-CSC、グローバルIT、上級副社長

Sanbir Singh Keer
Deloitte、サイバー戦略・トランスフォーメーション、サードパーティリスク管理、常務取締役

Sazul Samsuri
KAF Investment Bank、デジタルバンキング部門最高ビジネス責任者

Dr. Sekar Jaganathan
Kenanga Investment Bank、最高ビジネス責任者

池辺 晋一郎
ジュピターショップチャンネル株式会社、IT本部サイバーセキュリティ対策室長

Srinivas Jaggumantri
Infosys、金融サービス部門最高技術責任者

Srikanta Sahoo
LTIMindtree、IT部門シニアディレクター

Vasudev Puranik
Accenture、セールスエクセレンス、グローバルIT部門常務取締役兼最高情報責任者

F5について

F5は、マルチクラウドアプリケーションサービスおよびセキュリティ企業であり、
より良いデジタル世界の実現に取り組んでいます。
F5は、世界最大かつ最先端の企業組織と提携し、
オンプレミス、クラウド、エッジなど、
あらゆる場所のアプリとAPIを保護し、最適化しています。
F5のソリューションをご利用いただくことで、
みなさまの顧客に優れた安全なデジタル体験を提供し、
常に脅威に先んじることができます。
詳細については、f5.comをご覧ください（NASDAQ: FFIV）。

©2025 F5, Inc. All rights reserved. F5およびF5のロゴは、米国およびその他の国におけるF5, Inc.の商標です。
その他のF5の商標は、f5.comに記載されています。ここに記されているその他の製品、サービスまたは企業名は、各所有者の商標である可能性があります。
F5, Inc.は明示的にも暗黙的にも承認または提携を主張していません。DC 03.25 | EBOOK-1590043229