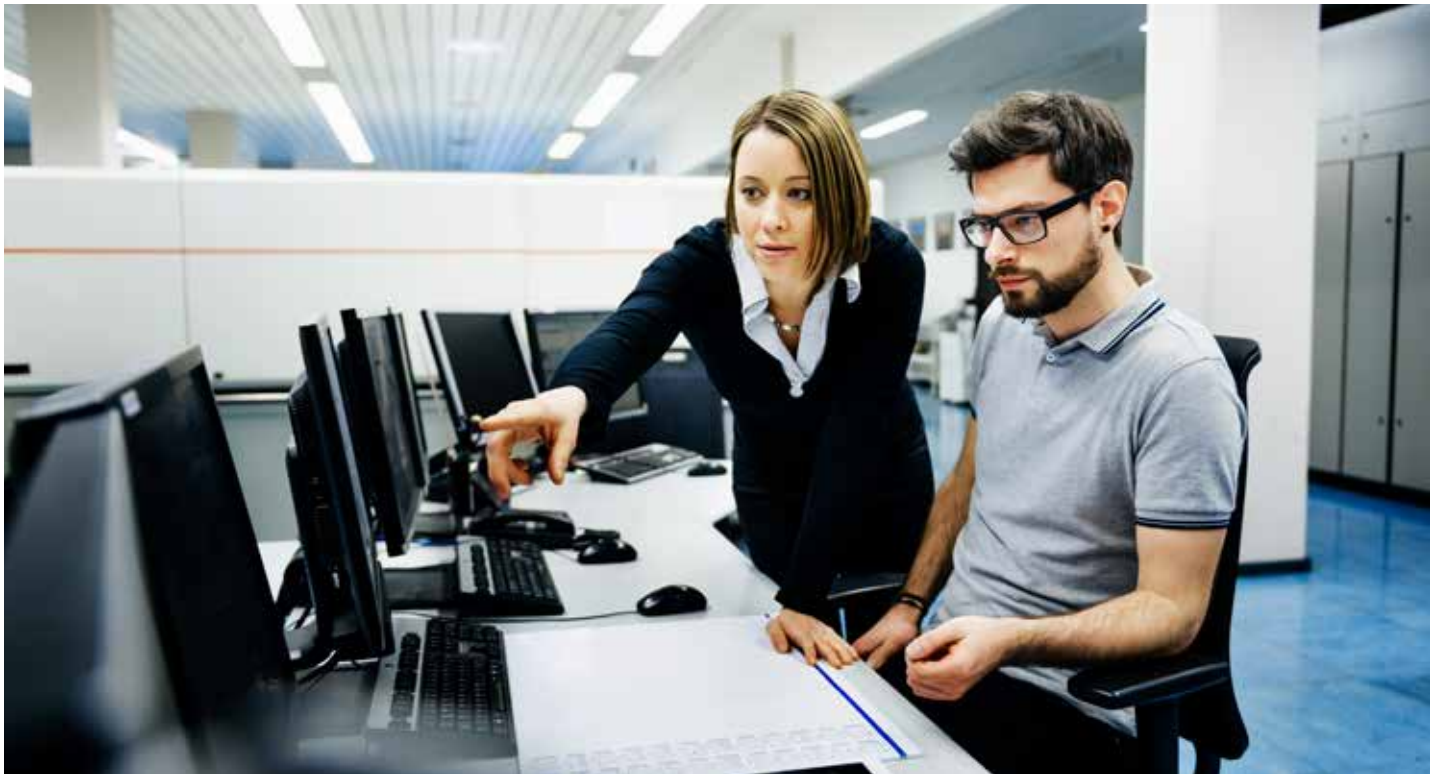
ホワイトペーパー

今日のSOCを構築する

リスク、リソース、そして現実のバランス

verizon business



絶え間なくサイバー脅威に晒されている今日において、セキュリティオペレーションセンター（SOC：security operations centre）は、組織におけるサイバーセキュリティの司令塔として、アラートの監視、インシデントの検知、そしてリアルタイムでの脅威対応を指揮しています。

適切なサイバーセキュリティ体制を構築するには、リスク許容度と、利用可能なリソースおよび専門知識とのバランスを的確に取ることが重要です。インハウス型、ハイブリッド型、または完全なアウトソース型のいずれのアプローチを選択するにしても、まず組織は重要な資産、リスク許容度、コンプライアンス要件、および予算を評価する必要があります。

インハウスのSOCは、運用とセキュリティ対策を完全に管理できる利点があります。しかし、これには多額の初期投資が必要であり、組織の保護やリスク軽減の維持および強化には、人材や技術面で継続的なコストが発生します。

一方、マネージドSOCサービスは、グローバルな脅威動向を把握し、24時間365日体制で監視を行う専門のアナリストへのオンデマンドアクセスを提供します。これにより、組織は既存の機能、専門知識、テクノロジー、そして拡張性を活用でき、自社でのチーム構築に伴う複雑さ、時間増、コスト増を回避できます。

現在では多くの組織がハイブリッド型のアプローチを採用しています。そうすることで、内部リソースを高度な業務や意思決定に集中させる一方で、日常的な運用業務の中核をパートナーが担います。

インハウスSOCの構築には、テクノロジー、人材、プロセスが必要

テクノロジーは、あらゆるサイバー防衛戦略の要です。セキュリティ情報イベント管理（SIEM：security information and event management）、セキュリティオーケストレーション、自動化、および対応（SOAR：security orchestration, automation and response）、エンドポイント検出および対応（EDR：endpoint detection and response）などのセキュリティツールは連係し合いながら、脅威の特定、調査、および軽減を可能にします。

ほとんどのテクノロジーエコシステムにおいてクラウドサービスが広く普及する中、SOCはハイブリッドかつ動的環境内で、設定ミス、アプリケーションプログラミングインターフェイス（API：application programming interface）の脆弱性、および不正アクセスを監視する必要があります。ゼロトラストアプローチによる監視活動とは、すべてのユーザ、デバイス、アプリケーションを検証し、機密システムやデータへの不正アクセスリスクを軽減することを意味します。今日のSOCの主な目的は、侵害が拡大する前に異常をリアルタイムで検知し、脅威を自動的に封じ込めることにあります。

攻撃者は人工知能（AI）を積極的に利用し、攻撃を自動化しています。これにより、脆弱性の発見、高度にカスタマイズされたフィッシング攻撃、マルウェアの難読化をかつてない規模で加速させているのです。これに対抗するため、SOCはAIおよび機械学習を活用し、迅速な異常の検出、トリアージの自動化、予測分析の実施を可能にしています。これらのツールは、アナリストが不要なノイズを除去し、優先度の高い脅威への対応に集中できるよう支援します。

また、SOCは、従来のマルウェアを超える新たな脅威に適応する必要があります。ディープフェイクを用いたフィッシング攻撃や生成AIによる音声詐欺の増加により、ソーシャルエンジニアリング攻撃の検出が一層困難になっており、継続的な監視体制の確立が不可欠です。

今日のSOCは、被害が発生する前に新たな攻撃手法を特定するために、包括的な脅威インテリジェンスフィード、AIを活用した分析、リアルタイムの行動監視を統合し、進化する脅威に先手を打って対応する必要があります。

人材：人が担う役割

最前線では、SOCアナリストやプロアクティブな脅威ハンターが最初に脅威への対応を行い、アラートに優先順位付けし、誤検知を除外します。より複雑なケースについては、詳細な分析、脅威の封じ込め、ならびに部門間での連携対応を実施するために上位部署へのエスカレーションが行われます。

SOCアナリストは、攻撃手法を分析し、異常を検出するとともに、従来のセキュリティ対策をかいくぐる可能性のあるパターンを特定することを目指します。

これらのスキルに対して高い需要があり、リアルタイムのインシデント対応、攻撃手法、および脅威インテリジェンスに関する専門知識が求められます。

多くの組織は、サイバーセキュリティエキスパートの慢性的な不足に対処するため、既存のITスタッフのスキル向上に取り組んでいます。ただし、このプロセスには一定の時間を要するため、保護体制に一時的な空白が生じ、移行期間中にサイバー攻撃のリスクが高まる可能性があります。

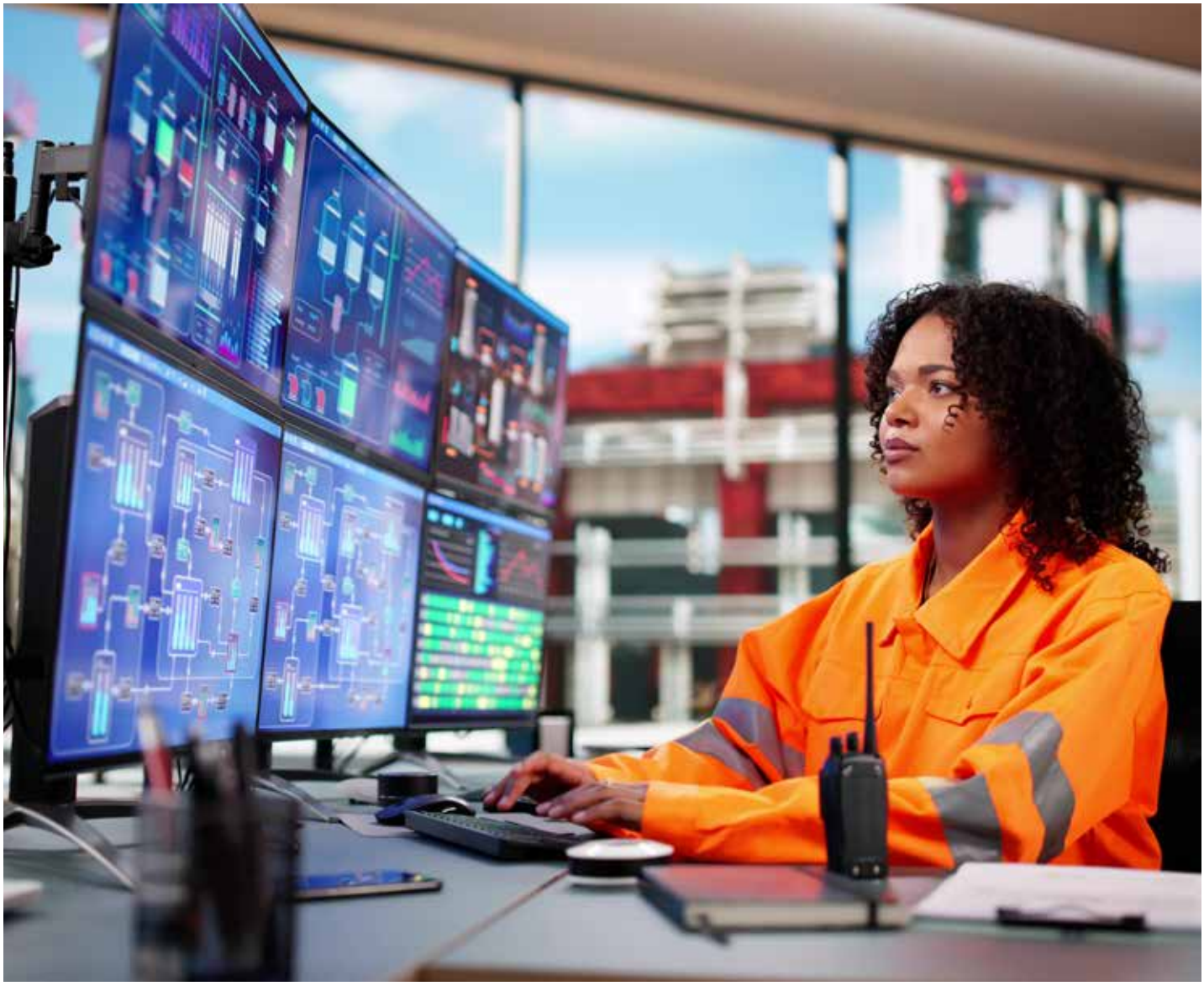
組織は、24時間365日体制のセキュリティ監視を実現するために、必要なスキルセットおよびリソースが適正な水準に達しているかを慎重に検討する必要があります。また、営業時間外においても対応機能が適切に維持されているかを考慮する必要があります。

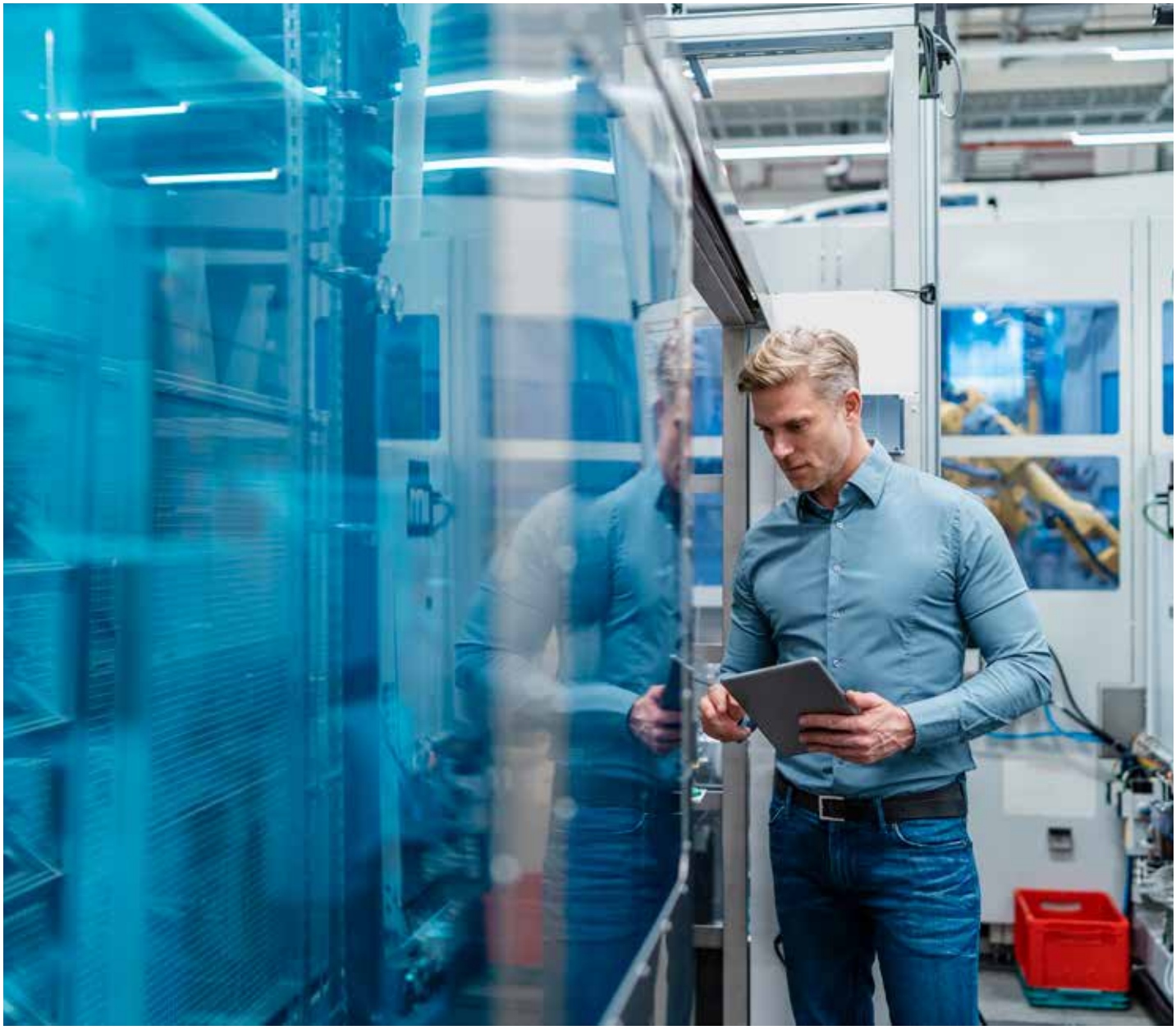
プロセス：IT運用、脅威検出、およびプレイブック

一般的に、プロセスはテクノロジーと人を結びつける接着剤のような役割を果たします。たとえば、IT運用プロセスでは、役割やワークフローの設定を通じて、組織が許容可能なリスクレベルを規定します。さらに、これにより責任の所在が明確になり、セキュリティチームによる更新プログラムやパッチ適用の確実な実施、および定められたポリシーに基づいたアラートのエスカレーションを可能にします。

脅威検出プロセスは、新たな脅威に対応するため、動的で継続的に改善される必要があります。定期的な見直しや維持・更新が行われない場合、既知および潜在的なリスクに対する可視性は、時間の経過とともに著しく低下する恐れがあります。

最後に、セキュリティアラートを適切に調査、管理するためには、明確なプレイブックが不可欠です。プロセス改善には、変化する脅威や脆弱性に対する効果および関連性を常に維持するための専任リソースが必要となります。





アウトソーシングの採用

SOC機能をパートナーにアウトソースすることで、コスト削減、セキュリティ運用の拡張、および最先端の専門知識へのアクセスが可能になります。自社でフルタイムのセキュリティチームを維持する代わりに、24時間365日体制の監視、自動化、およびエキスパートによる脅威インテリジェンスを活用できることで、受動的なサービス提供ではなく、統合されたセキュリティチームとしての機能を実現します。これにより、企業とその顧客がサイバー攻撃によって被るコストと影響を直接的に軽減することができます。

ただし、すべてのSOCプロバイダーが同じ機能を提供できるわけではありません。マネージドセキュリティサービスプロバイダー（MSSP：managed security services providers）は、ログ監視、脆弱性スキャン、ならびにコンプライアンス要件に準拠したセキュリティ対策に重点を置いています。MSSPは、規制要件に準拠したレポート作成や監視サービスを提供しますが、一般的にリアルタイムの脅威ハンティングやプロアクティブなインシデント対応機能は備えていません。

一方、マネージドの検出および対応（MDR：managed detection and response）を提供するプロバイダーは、自社内に専任の対応チームを持たない組織にとって、そのギャップを埋めるのに役立ちます。

ハイブリッド共同管理型SOC

ハイブリッド型の共同管理SOCでは、組織が重要なセキュリティ機能に対する管理権限を保持しながら、24時間365日体制の監視、脅威インテリジェンス、そして自動化をアウトソーシングすることが可能です。これにより、柔軟性が確保され、リスクの高い業務は自社で管理しつつ、脅威の検出とインシデント対応にはエキスパートの専門知識を活用することができます。

SOCパートナーを選択する際には、業界の専門知識、対応スピード、コンプライアンス対応力、およびAIを活用した脅威インテリジェンスなどの要素を慎重に評価する必要があります。適切なパートナーは、組織のセキュリティニーズとの整合性があり、自社内チームと効果的に連携し、脅威をリアルタイムで検出・対応するために必要な領域の機能を提供します。

組織は、選定したSOCパートナーが、効果的かつ適応性の高いハイブリッドSOCの構築のために、プロセスおよびテクノロジーの統合に関して柔軟性と透明性を備えているかを慎重に見極める必要があります。

特に重要な検討事項：コスト、専門知識、リスク

インハウスのSOCは、組織の戦略と運用要件、リスクへの露出度、および規制上の義務に特化して構築されるため、セキュリティ運用とデータに対するより良い管理を実現します。

しかし、インハウスSOCを維持するには、テクノロジーとサイバーセキュリティ人材の両方への継続的な投資が必要です。組織は、高度なセキュリティツールを継続的に更新しつつ、競争の激しい雇用市場において、スキルを持ったエキスパートの採用、育成、および定着を図る必要があります。

SOCパートナーとの提携は、迅速かつ的確なインシデント対応を可能にするさまざまなサービスが提供されるため、インハウスSOCの代替手段としても有効です。SOCパートナーは、組織のインフラと企業文化に深く組み込まれることが可能な専門チームを通じて、組織のITおよびセキュリティ機能と緊密に統合されることも可能です。このアプローチにより、常時稼働するカスタマイズされたセキュリティ体制が提供されることになります。

インハウスチームは、強力な脅威インテリジェンスや組織の環境に対する深い理解を提供できる一方で、こうしたチームの構築および維持には多大な時間と投資が必要となります。チームの立ち上げ期間には、カバーするべき領域にギャップが生じ、サイバーリスクが高まる可能性があります。一方、アウトソーシングのSOCプロバイダーは、即時の拡張や専門的なノウハウを提供できますが、自社チームのような組織に関する知識や現場での存在感を欠く場合があります。SOCのアプローチを検討する際には、インハウス型、アウトソーシング型、またはハイブリッド型のいずれであっても、企業文化に対する適合性、既存のセキュリティツールへの習熟度、規制遵守、そして組織の運用柔軟性に対する姿勢などが、重要な検討要素となります。

自社での運用であれアウソーシングであれ、SOCは規制要件や業界特有のセキュリティ要件の両方に整合する必要があります。これらの規制要件では、コンプライアンスを維持するために組織が継続的な監視、監査、およびプロアクティブなセキュリティガバナンスを実施する必要があります。

SOCの構築は一過性のプロジェクトではなく、継続的な監視・維持・適応を必要とする、“生きて”進化し続ける運用プロセスです。こうした適応力は、絶えず変化し拡大するサイバー脅威の状況に加え、機敏性とコスト効率を求めるビジネスニーズの変化によって向上していくのです。

最新のテクノロジー、専門知識、そしてセキュリティ戦略への継続的な投資が行われなければ、たとえ高度に構築されたSOCであっても、急速に陳腐化し、効果が著しく失われる可能性があります。

詳細はこちら

お客様のSOC要件に最適なアプローチに関する詳細は、ベライゾンビジネスの営業担当までご連絡ください。メール：apaccontactus@verizon.com またはverizon.com/business/en-au/contact-us/をご覧ください。