高度化するサイバー攻撃に対処するマネージド・セキュリティ・サービス

成島 佳孝 Narishima Yoshitaka
笠井 真一 Kasai Shinichi
佐藤 隆行 Sato Takayuki
森 正樹 Mori Masaki
藤田 晶彦 Fujita Akihiko

近年，複雑化かつ巧妙化するサイバー攻撃により，企業や組織のセキュリティリスクが増大している。また，クラウドサービスの普及，情報家電や制御系装置のインターネットへの接続により，守るべき情報システムが複雑化している。
マネージド・セキュリティ・サービスは，コンサルティングからセキュリティ施策の適用，運用サービスまでを提供する統合的なサービス群である。日立グループの知見を生かしたインシデント対応の技術支援や，構築・運用ノウハウを活用したセキュリティイベント監視サービスなど，防御する情報システムに応じたソリューションの提供が可能であり，社会インフラの安全・安心に寄与するものである。

1. はじめに

IT（Information Technology）の活用により，利用者の利便性を高めた高度な社会インフラが実現されつつある。このように社会インフラにおけるITシステムの役割が高まるにつれ，安全・安心を確保するためのセキュリティはますます重要になっている。

近年，複雑化かつ巧妙化するサイバー攻撃により，企業や組織のセキュリティリスクが増大している。標的型メール攻撃の高度化やDDoS（Distributed Denial of Service：分散型サービス拒否）攻撃の大規模化などである。サイバー攻撃は，特定の組織・個人をターゲットとし，機密情報や個人情報の窃取，ITシステムのサービス不能を執拗（よう）に狙うようになり，最終的に金銭を要求するケースも増えている。

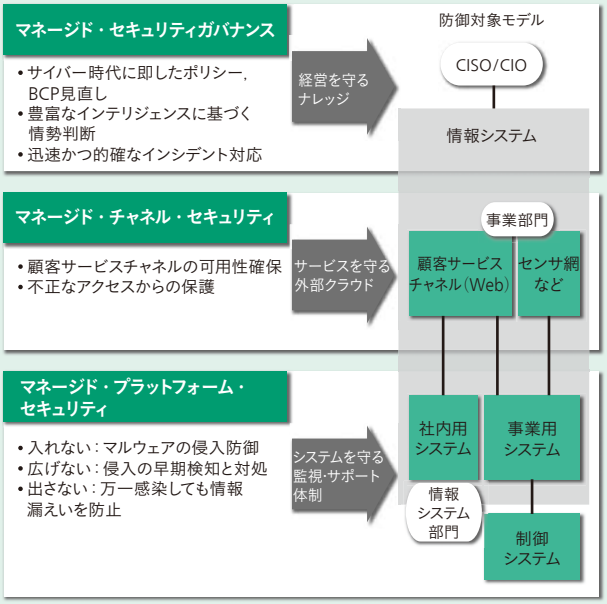
守るべき情報システムも，今までは組織内に設置されていたものが，クラウドサービスの普及によって組織外，そしてインターネット上に位置するようなった。組織内情報システムとクラウドサービスが連携して利用されるようにもなり，セキュリティの境界が曖昧になるとともに，セキュリティ管理が複雑化している。また，PC（Personal Computer）などのIT機器だけでなく，情報家電や制御系装置などもインターネットに接続されるようなったことで，サイバー攻撃の影響を受け得るシステム環境も膨大になり，脅威が増大している。

こうした脅威に対し，サイバー攻撃から情報システムを保護するために多層防御によるセキュリティ対策を講じていくことはもとより，攻撃を受けた場合にも，いち早くインシデントを検知し，迅速にインシデント対応を実施することで被害を最小限にとどめることの必要性が高まっている。そのためには，複雑化したITシステムを常に監視するための高度なログ管理システムや，迅速に対策を講じるための専門スキルを持った技術要員・体制の確保など監視体制の強化が求められる。また，情報システム部門が抱える運用負荷が増大していることや，対応するセキュリティの専門性が高まっていることから，セキュリティ対策・運用の外部委託のニーズが広がっている。

ここでは，複雑化かつ巧妙化するサイバー攻撃から，社会インフラや情報システムを守るための包括的なセキュリティ対策群であるマネージド・セキュリティ・サービスについて述べる。

2. マネージド・セキュリティ・サービス

サイバー攻撃をはじめとした脅威に対抗するため，日立グループは，マネージド・セキュリティ・サービスを提供している。これは，社会インフラ分野を含むさまざまな業種や業態の企業，官公庁，自治体など向けに，コンサルティングからセキュリティ施策の適用，運用サービスまでをトータルに支援するセキュリティソリューションで



カテゴリ	サービスメニュー	機能概要
マネージド・セキュリティガバナンス	セキュリティコンサルサービス	• セキュリティポリシー策定支援 • セキュリティリスク分析支援 • 事業継続マネジメント策定支援
	セキュリティ診断サービス	• ITインフラに対する脆（ぜい）弱性診断 • マルウェア調査
	インテリジェンスサービス	• システムにおける脆弱性情報提供 • 特定サイトにおける風評被害調査 • インシデントレスポンス支援
	CSIRT技術支援サービス	• 組織内CSIRT運用支援 • 標的型攻撃メール訓練
マネージド・チャネル・セキュリティ	Webサイトプロテクションサービス	• Webアプリケーションファイアウォール • WebサイトへのDDos対策
	Webサイトチェックサービス	• Webシステムに対する脆弱性診断 • 改ざん検知
マネージド・プラットフォーム・セキュリティ	メールセキュリティサービス	• アンチウイルス，アンチスパム • コンテンツフィルタリング
	Webセキュリティサービス	• Web閲覧におけるURLフィルタリング • アンチウイルス
	セキュリティイベント監視サービス	• 統合ログ管理 • ログの相関分析
	仮想サーバプロテクションサービス	• 仮想UTM運用支援

注：略語説明　BCP（Business Continuity Plan），CISO（Chief Information Security Officer），CIO（Chief Information Officer），IT（Information Technology），CSIRT（Cyber Security Incident Readiness/Response Team），DDoS（Distributed Denial of Service），URL（Uniform Resource Locator），UTM（Unified Threat Management）

図1｜マネージド・セキュリティ・サービスのメニュー一覧

マネージド・セキュリティ・サービスのそれぞれのカテゴリーが防御する対象システムを示す。表には，各カテゴリーにラインアップされるサービスメニューを列挙した。

ある。

このサービスは，セキュリティ対策・運用の外部委託ニーズの拡大を受けたITシステムの運用フェーズでのセキュリティ管理を代行するサービスであり，「ITを守る」だけでなく，「ITで守る」ための統合的なセキュリティサービス群となっている。「マネージド・セキュリティガバナンス」，「マネージド・チャネル・セキュリティ」，「マネージド・プラットフォーム・セキュリティ」の3つのカテゴリーで構成されており，防御対象の情報システムやその組織での役職・担当部門に応じて適切なソリューションを提案し，提供することが可能である（図1参照）。

このサービスの3つの特長について以下に述べる。

2.1　動的セキュリティ管理を実現

マネージド・セキュリティ・サービスにおける脆（ぜい）弱性を抱えないための対策強化として，組織内CSIRT（Cyber Security Incident Readiness/Response Team）の構築やBCP（Business Continuity Plan）の見直しといった計画（Plan）から，対策・運用（Do），点検・監査（Check），そして改善・是正（Act）の「PDCAサイクル」による改善に加え，監視（Observe）から情勢判断（Orient），意思決定（Decide），そして行動（Act）という一連の流れにより，迅速かつ合理的な意思決定や施策を実現する「OODAループ」の概念も採用している。これによって運用段階での動的セキュリティ管理の強化を図り，インシデントの発生を前提とした情報セキュリティポリシーの設定やセキュリティ対策の強化・迅速化を実現している（図2参照）。

2.2　プロフェッショナル集団のインシデント対応のノウハウを適用

日立グループ内には，サイバー攻撃対策を担うCSIRTとして活動し，インシデント対応に多くのノウハウを持つHIRT（Hitachi Incident Response Team）というプロフェッショナル集団がある。このHIRTやグローバルパートナーと連携し，顧客の組織内CSIRTに代わってインテリジェ

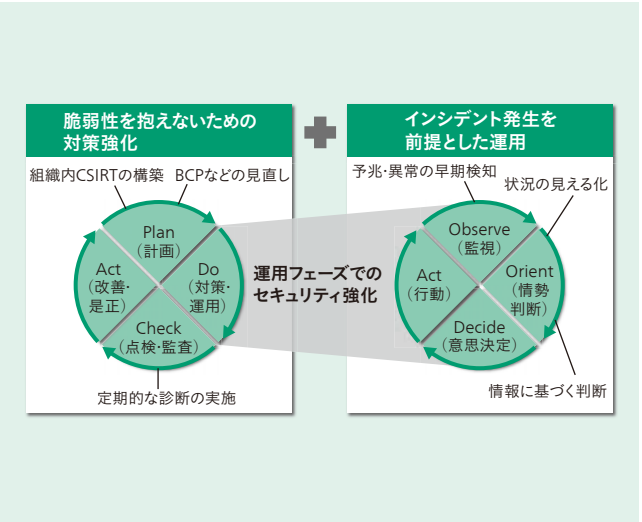


図2｜PDCAサイクルとOODAループの関係

PDCA（Plan, Do, Check, Act）サイクルによる継続的な改善に加え，その運用フェーズでのセキュリティ強化としてOODA（Observe, Orient, Decide, Act）ループに基づく運用を採用している。

ンス情報を分析・監視し，関連する情報と必要な対応について情報を提供する「CSIRT技術支援サービス」などの各種サービスを備え，極めて高度なセキュリティ運用・管理を24時間365日体制で対応している。

2.3　クラウド環境への柔軟な対応

オンプレミス環境，クラウド環境，さらには分散したクラウド環境など，複合的なシステム環境に対し，統合的なセキュリティ対策や運用を提供する。また，クラウド環境ではこれまで困難だった個別のきめ細かいセキュリティ対策が可能な「仮想サーバプロテクションサービス」や「セキュリティイベント監視サービス」などのサービスを提供することにより，クラウド環境への柔軟な対応を実現している。

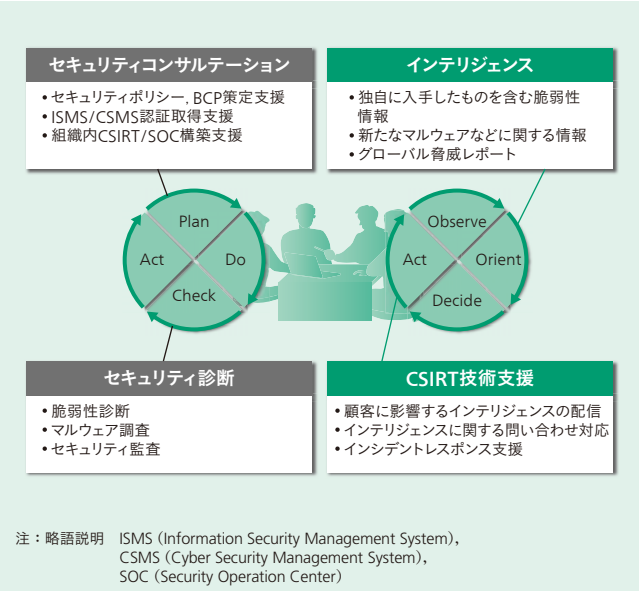
3.　各カテゴリーとサービスメニュー

マネージド・セキュリティ・サービスの3つのカテゴリーごとに，注目すべきサービスメニューについて説明する。

3.1　マネージド・セキュリティガバナンス

経営を守るマネージド・セキュリティガバナンスは，日立グループ内の情報システム管理および顧客のビジネスの支援活動で蓄積したナレッジを基にした専門コンサルテーションサービスなどで構成される（図3参照）。

社会インフラやITシステムの情報セキュリティを確保するためには，情報セキュリティマネジメントにおけるPDCAサイクルによって継続的改善活動を推進していくことが有効である。セキュリティコンサルサービスでは，



注：略語説明　ISMS（Information Security Management System），
CSMS（Cyber Security Management System），
SOC（Security Operation Center）

図3｜マネージド・セキュリティガバナンスのメニュー構成
マネージド・セキュリティガバナンスにラインアップされるサービスメニュー，およびそのメニューとPDCAサイクル，OODAループの関連づけを示す。

情報セキュリティマネジメントの国際基準であるISO/IEC 27001 に基づき，組織のセキュリティポリシー策定やセキュリティリスク分析の支援を実施する。このようなセキュリティマネジメントの取り組みを顧客に提供して定着を図ることで，組織的・計画的なセキュリティ管理を促進する。

巧妙化するサイバー攻撃に対しては，迅速にインシデント対応を実施していくための仕組みや体制が必要となる。新たに発生したサイバー攻撃手法や新たに発見された脆弱性，サイバーテロの情報など，価値ある情報をいち早く入手することで，サイバー攻撃対策においても優位に立てる。このような脅威情報を，全世界規模のインテリジェンス網を用いて収集し，速やかに網羅的に提供するサービスとしてインテリジェンスサービスがある。単に技術情報だけでなく，攻撃に関する意図情報や周辺状況を併せて提供することで脅威の大きさをより具体的に判断できるようにしている。また，既知の脆弱性情報から，新たに発見されたゼロデイ脆弱性，さらには未来の脅威を予測した脆弱性情報も提供可能な情報として備えており，組織の体制に応じた情報量にすることができる。

最終的には，収集した脅威情報や後述するログ管理システムを前提に，いかにインシデント対応を運用していくかが重要なポイントであり，その役割を担うのが組織内CSIRTである。昨今，この体制の必要性が高まり，金融機関をはじめとしたさまざまな組織で体制構築が行われている。新たに発足した組織に対して，インシデント対応やサイバー攻撃解析などの運用支援を提供するのがCSIRT技術支援サービスである。今後，サイバー攻撃のさらなる進化に伴い，より高いセキュリティの専門性が求められることが想定され，このような支援サービスの必要性は高まっていくと考えている。

3.2　マネージド・チャネル・セキュリティ

サービスを守るマネージド・チャネル・セキュリティは，顧客の公開Webサイトに対する脅威を外部クラウドで保護するサービスである。

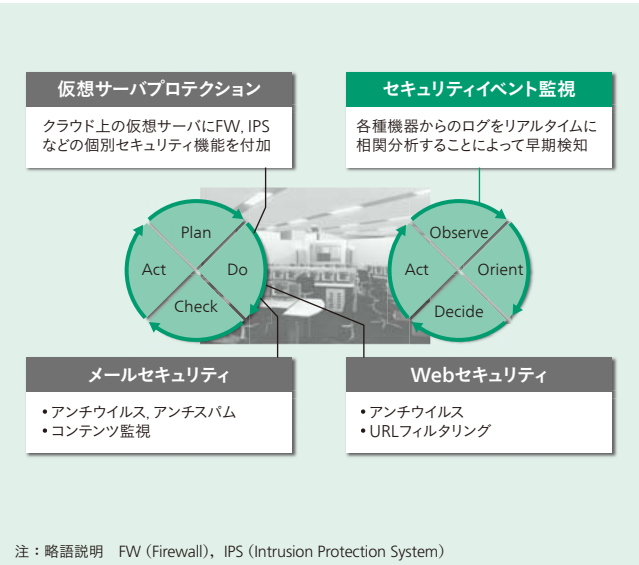
今やビジネスに欠かせないシステムとなり，企業情報の提供や各種取り引きといった実ビジネスに利用されている公開Webサイトは，常にインターネットにさらされていることにより，攻撃者にとっては格好のターゲットとなっている。最近では，脆弱性を突いたWebサイト改ざん事例が多くなっている。以前は主に国旗などの画像を表示するものであったが，最近のWeb改ざんでは，見た目には分からない形でウイルスを仕込まれるといった事例が多くなっている。そのサイトにアクセスした利用者は，知らず

にウイルス感染し，最終的には個人情報などを窃取される。Webサイトを改ざんされた組織は，被害者であるだけでなく，Web利用者に対しては加害者になり得る可能性もあり，セキュリティ強化は喫緊の課題である。Webサイトプロテクションサービスは，全世界に分散された大規模プラットフォームを活用したDDoS攻撃対策サービスやWAF（Web Application Firewall）サービスにより，公開Webサイトを継続的に保護することが可能である。

3.3　マネージド・プラットフォーム・セキュリティ

システムを守るマネージド・プラットフォーム・セキュリティは，顧客の情報システム，さらには制御システムを脅威から保護するサービスである（**図4**参照）。

多層防御の考えに基づいており，マルウェアを侵入させない「入口対策」，侵入されても拡散を防止し，早期検知を行う「拡散対策」，感染しても情報漏えいなどを防止する「出口対策」がラインアップされている。情報漏えいを許さない出口対策も重要ではあるが，対策の第一歩である入口対策により，標的型攻撃メールなどの組織内への侵入を少なくすることが必要である。メールセキュリティサービスは，高精度なアンチスパム機能，複数の商用ウイルススキャナと独自の人工知能エンジンを組み合わせたアンチウイルス機能などを兼ね備えたSaaS（Software as a Service）型のサービスである。それぞれの高度な検知機能により，組織内への不要なメールの侵入を削減することが可能となり，組織の作業効率を向上させることができる。また，SaaS型の特徴を生かし，セキュリティ対策の導入期間短縮，費用削減，管理負荷低減を図ることが可能である。



注：略語説明　FW（Firewall），IPS（Intrusion Protection System）

図4｜マネージド・プラットフォーム・セキュリティのメニュー構成
マネージド・プラットフォーム・セキュリティにラインアップされるサービスメニュー，およびそのメニューとPDCAサイクル，OODAループの関連づけを示す。

日立クラウドソリューション「Harmonious Cloud」をはじめ，クラウドの利用が進んでいる。クラウド導入のメリットとしては，コスト削減や開発期間短縮が挙げられる。その一方で，セキュリティ面での不安が利用にあたっての障壁となっている。マネージド・セキュリティ・サービスでは，各クラウド基盤が提供するセキュリティに加えて，仮想サーバプロテクションサービスとして，システム個別のFW（Firewall），IPS（Intrusion Protection System）などの機能を提供することで，オンプレミス環境と同様のきめ細かい設定やログ分析を提供している。

このようにオンプレミス環境だけでなく，仮想化技術を活用したクラウド環境が混在するシステムにおいても，各種機器を定期的に監視して見えないセキュリティ異常を早期に検知し，インシデント対応につなげることが必要である。セキュリティイベント監視サービスは，クラウドを含む複合環境のシステムに対して統合的に監視を実施し，インシデントを早期に検知するためのサービスである。日立のSOC（Security Operation Center）と連携し，専門部隊による高度かつ迅速なインシデント対応のサポートを併せて提供している。

4.　導入事例・導入効果

マネージド・セキュリティ・サービスは，セキュリティ対策を包括するサービス群として提供されている。サービスメニューの導入事例を以下に述べる。

メールセキュリティサービスは，金融機関をはじめとする多くの企業で利用されている。導入後の効果として，高い検知率により，企業内の負荷が低減できたことが多くの顧客から報告されている。24時間365日のサポート体制が用意されており，いつ起こるか分からないインシデントに対して，常に窓口対応できる点も評価されている。また，導入期間が短いため，標的型メール攻撃を受けている際に導入を進め，対策として講じることができたケースもある。

セキュリティイベント監視サービスは，かつては内部統制などの基準に準拠し，ログの取得・保管を目的として導入されていたが，最近では，サイバー攻撃を積極的に検知することを目的として導入される例が増えている。大量に収集されるログに対し，実績に基づく最適な検出ルールを適用することで，インシデントと思われる事象をリアルタイム相当で検出することが可能になる。また，専門エンジニアの支援サービスを併せて利用することで，検出後のインシデント対応も大幅に時間を短縮することが可能になるだけでなく，被害の進行を抑えることもできる。結果として被害の影響を受けないようにする，あるいは最小限にすることができる（**図5**参照）。

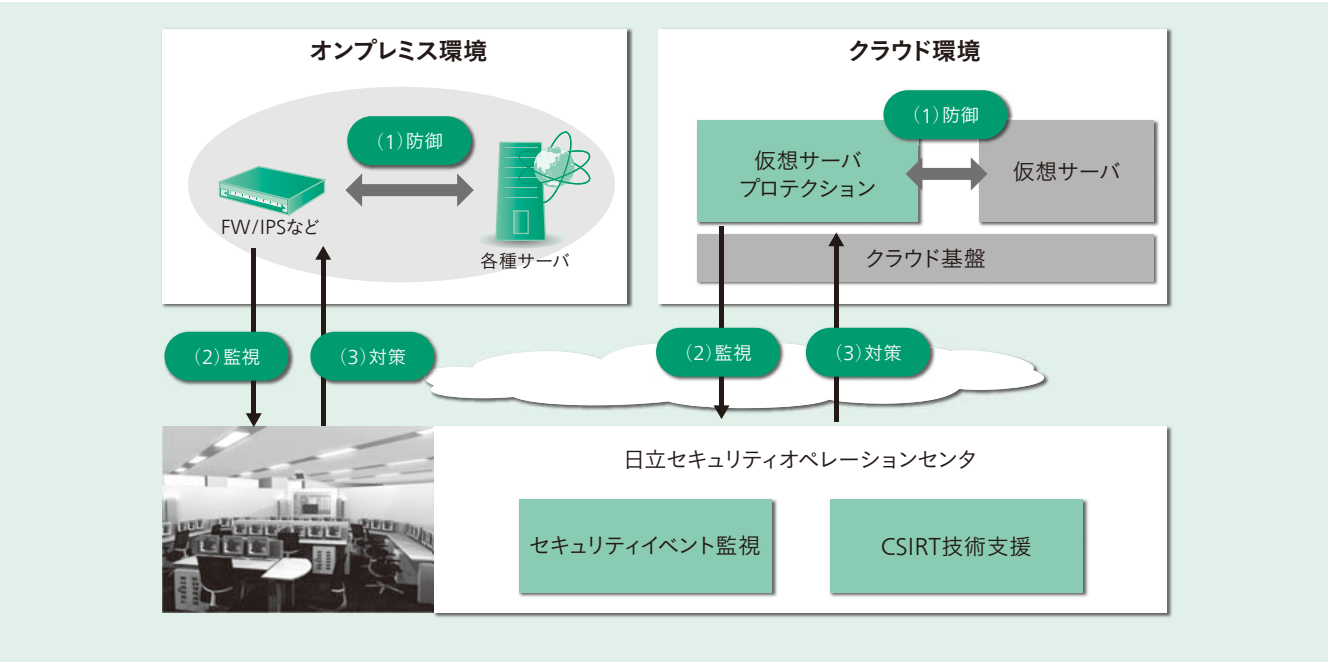


図5｜セキュリティイベント監視サービスの概要
オンプレミス環境，クラウド環境のいずれにも提供可能である。受託サービスとしての，防御・監視・対策のセキュリティ運用の関係性を示す。

5. おわりに

ここでは，複雑化かつ巧妙化するサイバー攻撃から，社会インフラや情報システムを守るための包括的なセキュリティ対策群であるマネージド・セキュリティ・サービスについて述べた。

日立グループは，みずからも事業者として，多様化するシステム環境から高度化するサイバー攻撃まで，さまざまなセキュリティ課題に取り組んでいる。その中では，専門スキルを有するメンバーの知見によって対応策を選定し，ベストプラクティスとしてのセキュリティ施策を講じている。これからも実際に適用したノウハウと最新技術を活用し，マネージド・セキュリティ・サービスのメニューの拡充を図る。これは，社会イノベーションを実現していくための取り組みであり，長年培ってきたインフラ技術に，高度なIT，セキュリティ施策を組み合わせることでその構築に努めている。そこでは，企業システムだけでなく制御系システムを含む社会インフラシステムにも適用可能なセキュリティ対策を強化する。

これからも顧客のパートナーとしてあらゆる課題に取り組み，共に解決を図っていくことで，安全・安心な社会の実現に貢献できるものと考える。

参考文献など

1) 情報セキュリティ アドバイザリーボード：総務省における情報セキュリティ政策の推進に関する提言（2013.4），
http://www.soumu.go.jp/main_content/000217000.pdf

執筆者紹介


成島 佳孝
日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティソリューション本部 システム第一部 所属
現在，セキュリティサービスの提案・導入に従事


笠井 真一
日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティソリューション本部 システム第一部 所属
現在，セキュリティサービスの提案・導入に従事


佐藤 隆行
日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティソリューション本部 システム第一部 所属
現在，セキュリティサービスの開発・提案・導入に従事


森 正樹
日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティソリューション本部 Secureplaza販売推進センタ 所属
現在，セキュリティサービスを含むセキュリティソリューションの拡販に従事


藤田 晶彦
株式会社日立システムズ クラウドICTサービス事業グループ ネットワークサービス事業部 ネットワークインテグレーション本部 第三部 所属
現在，セキュリティサービスの開発・提案・導入に従事