E&U企業における最新セキュリティー

スマートメーターにおけるセキュリティー対応方針

IBMセキュリティー・オペレーション・センターが支援している平均的なE&U(Energy and Utilities:エネルギー&公益)企業では、セキュリティー・イベントが毎週約200万件あり、セキュリティー・インシデントも毎週約3件の頻度で起こっています。これらは外部および内部犯行によるものであり、E&U企業はその対応に迫られています。E&U企業においてセキュリティー対策を検討するためには、セキュリティー業界スタンダードとセキュリティー脅威の事例を参考にしながら、想定されるリスクを明確にしていくことが重要です。

本稿では、スマートメーターに関するセキュリティーを事例として取り上げながら解説します。

1. E&U企業におけるセキュリティーの現状

2015年1月、IBMセキュリティー・サービスにより、2014年度E&U企業におけるサイバー・セキュリティー・インテリジェンス・インデックスの指標[1]が発表されました。これは、IBMセキュリティー・オペレーション・センター(SOC:Security Operation Center)が、ネットワーク・セキュリティー監視サービス(IBM Managed Network Security Services)を行っているE&U企業(調査を実施した133カ国、多業種1000企業の中のE&U企業)を対象に、E&Uの平均的な企業についてのセキュリティーの状況をまとめたものです。なおここでの平均的なE&U企業とは、社員数が1000～5000名で、自社ネットワークに約500のセキュリティー機器を設置している企業です。

平均的なE&U企業において、2013年1月から12月までに起きたセキュリティー・インシデントに関する調査結果(**図1**)から以下のことが判明しています。

①検知されたセキュリティー・イベント(システムやネットワークにつながっているセキュリティー機器からの異常信号)は、毎週約200万件。

②上記イベント中でセキュリティー攻撃と認定できるの

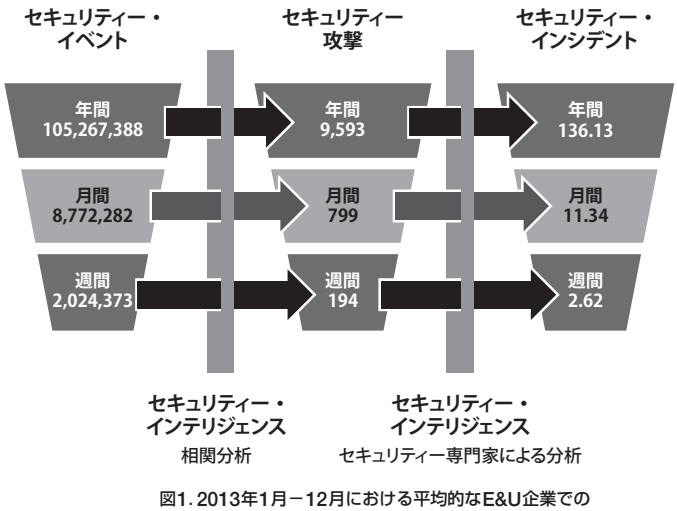

図1. 2013年1月－12月における平均的なE&U企業でのセキュリティー・インシデント調査結果[1]

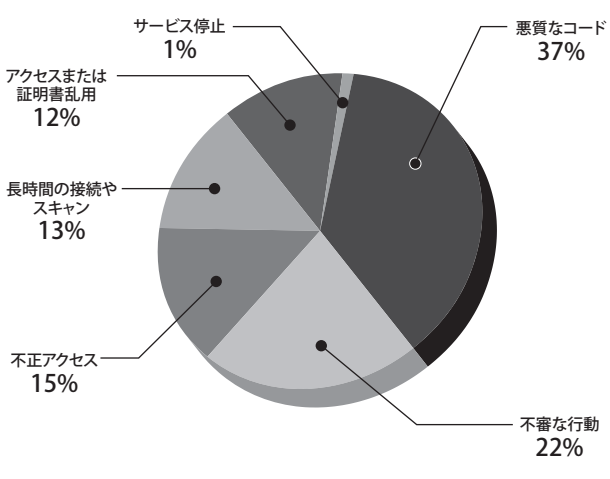

図2. 発見したインシデントの内容分類

は、毎週194件。

③セキュリティー・インシデント（事業運営に影響を与えたり、情報セキュリティーを脅かしたりする事件や事故）は毎週約3件。

この数字はすなわち、「毎週200万件のセキュリティー・イベント情報の中から、早急に3件のセキュリティー・インシデントを識別し対応する必要がある」ということを意味しています。

その対応は、人海戦術では非常に難しいと言えます。IBMでは、セキュリティー・インテリジェンスにより、膨大なセキュリティー・イベントの中からセキュリティー攻撃を識別し絞り込んだ後、セキュリティー専門家が分析しセキュリティー・インシデントを確定することができるため、このような調査・分析が可能です。セキュリティー・インテリジェンスとは、企業全体のセキュリティー関連の情報を活用し、高度なインテリジェンスを適用することでより迅速に脅威を検出し、より効率的にリスクを優先順位付けし、コンプライアンス・アクティビティーを自動化できるようにすることです。

年間にすると、平均的なE&U企業では1.05億件のセキュリティー・イベントが起こっています。2013年度の小売業界の平均的企業では年0.67億件、金融業界の平均的企業では年1.02億件であったことから、E&U企業ではほぼ金融業界に相当する数のセキュリティー・イベントが起こっていることが分かります。

図2は、セキュリティー・インシデントを分類した結果です。

①発見されたインシデントの37%が悪意のあるコードであった。悪意のあるコードとはデータを破壊する、破壊または侵入プログラムを実行する、またはそれ以外の方法で被害者のコンピューター・データのセキュリティーや整合性を侵害するためにプログラムに不正に挿入されるウイルス、ワームなどのプログラムのこと。

②発見されたインシデントの35%が、不審な行動（連続したログイン失敗や普段使用しない社員のアクセスなど）と思われる事象や持続した接続やスキャンなどの偵察活動だった。

③発見されたインシデントの27%は、不正アクセスおよびアクセスや証明書の乱用だった。

以上により、セキュリティー・インシデントとして、マルウェアなどの悪意のあるコード、システムへ侵入しようとする活動や実際の不正アクセスなどが行われていることが確認できました。

図3は、上記インシデントを実行した攻撃者の分類結果です。

①外部犯行者が全体の56%を占めている。

②外部と内部の犯行者が共謀した件は22%で、外部犯行者が加担したと考えられるインシデントは①と合わせて全体の約8割である。

③内部犯行は17%。

外部犯行者の多くは想定敵国が悪意を持って雇った人物と想定され、その人物が目立たない従業員であった場合にはインシデントが長期にわたって見つかりにくいという傾向があり、結果として大きな損害を及ぼすことに

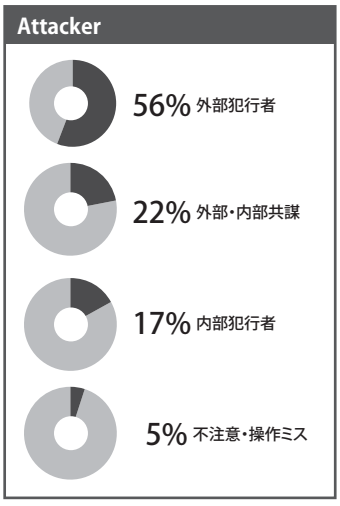

図3. 発見したインシデントの実行者分類

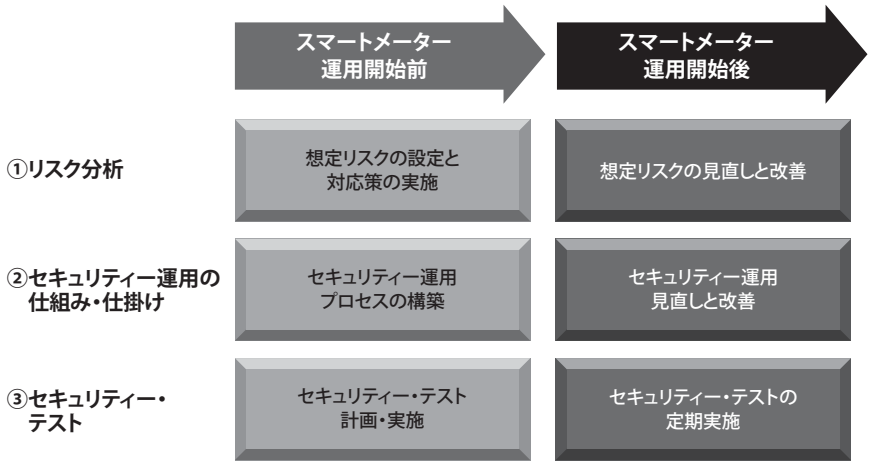

図4. スマートメーター運用におけるセキュリティー全体像[2]

なります。

今回の調査結果から、①調査を実施したE&U企業のデータを平均的なE&U企業として正規化したことで平均3件/週のインシデントがあったこと、②E&U企業は絶えずセキュリティーの脅威にさらされ、その実行者は外部犯行者が多いが内部犯行者の場合もある、ということが分かります。実際には企業の環境や規模なども異なるため、より多くのグローバルでの事例を参考にして想定される脅威を設定し対策を検討することが、今後起こりうるインシデントに対応する精度を上げるために重要です。特に、ライフラインである電力の安定供給は必須であり、想定する脅威を網羅するために多くの事例を参照することは不可欠です。IBMでは、多くのグローバル事例を知的財産として所有しており、これらを活用したコンサルティングを行っています。

では、E&U企業は具体的にどのような対応をしていくべきなのか、スマートメーターを例に取って次章以降で説明していきます。

2. スマートメーター運用における セキュリティー対応方針

E&U企業がスマートメーター運用においてセキュリティーを担保するには、運用開始前後それぞれで対応が必須です。対応方針を、

(1)セキュリティー・リスク分析
(2)セキュリティー運用の仕組み・仕掛け
(3)セキュリティー・テスト

の3つの観点から検討するべきです。**図4**は、運用開始前、運用開始後それぞれの対応方針を決める上での検討項目を示したものです。

(1)セキュリティー・リスク分析

最初はセキュリティー・リスク分析です。情報セキュリティーの規範であるISO27001/27002および制御セキュリティーのガイドラインIEC62443[3]でもリスク分析が推奨されており、スマートメーター関連システムのセキュリティー対策を検討するに当たっても同様にリスク分析を適用するべきです。グローバル標準であるスマート・グリッド・サイバー・セキュリティーに関するガイドラインNISTIR 7628[4] では、想定リスクを設定し、セキュリティー対策を検討してガイドラインを作成したことが明記されています。また、最初にセキュリティー対策を設定した後にも増えていく脅威に対応するためには、リスク分析の実施について定期的な見直しと改善が必須です。

(2)セキュリティー運用の仕組み・仕掛け

次にセキュリティー運用の仕組み・仕掛けです。セキュリティー・イベントを検知し対応するための仕組み・仕掛けをスマートメーター運用開始前に設定し、事前に検証することが重要です。運用後、実際にセキュリティー・インシデントに対応しながら運用プロセスを追加修正するなど、定期的な見直しと改善が必須です。日本では一部の電力会社を除いてスマートメーターはまだ導入段階であり、適切なスマートメーターのセキュリティー・オペレーション・センターの体制や、セキュリティー・イベントを検知後にインシデント対応チーム(CSIRT:Computer Security Incident Response

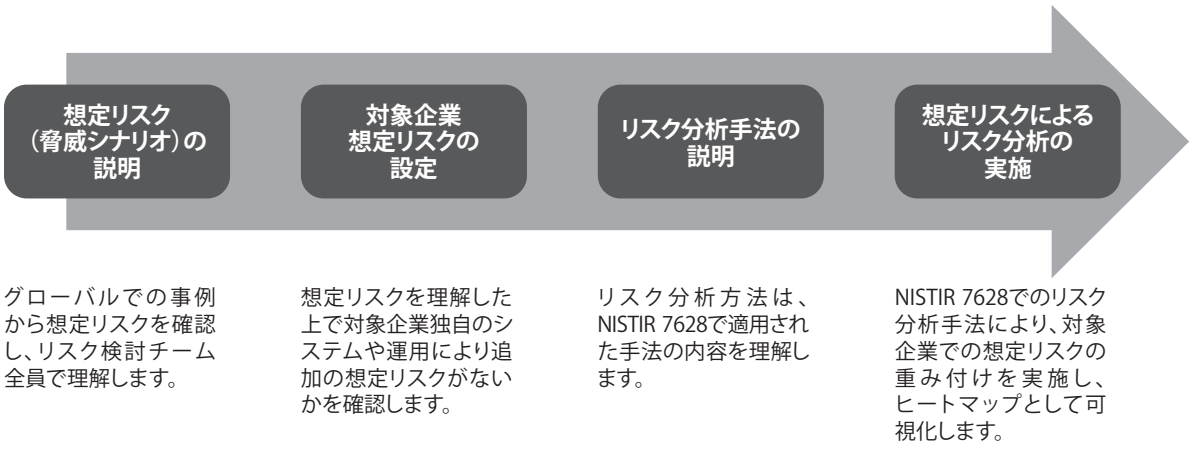

図5. セキュリティー・リスク分析ステップ[2]

Team)で解決するまでの体制・業務プロセス、およびセキュリティー・ツールなどを決めて導入していくことが課題となっています。

また、スマートメーターには、情報機器のIT(Information Technology)としての側面と、制御機器のOT(Operational Technology)としての側面をどのように融合していくのかが、日本だけでなく海外でも課題となっています。セキュリティー・インシデントの予兆監視を実施するには、ITシステムに設置したセキュリティー機器からの情報だけでなく、スマートメーターなどの制御機器から発信された異常時のイベントの原因が、障害によるものなのかセキュリティー・インシデントなのかを区別できることが必要です。IBMでは、スマートメーター機器からのイベント情報をSIEM(Security Information and Event Management)ツールであるIBM Security QRadarのインプット情報として取り込むことで、ITとOTを融合させた形でセキュリティーの予兆監視を支援しています。

(3)セキュリティー・テスト

最後にセキュリティー・テストです。セキュリティー対策が正しく実装されていることを確認するために、セキュリティー・テストを計画し運用開始前に実施する必要があります。また、増え続けるセキュリティー・インシデントに対応するためには、定期的にセキュリティー・テストを実施することが必須です。

ここ以降は、(1)～(3)の話をまとめていきます。

まず、リスク分析について説明します。NISTIR 7628の中で、スマートメーターにおけるセキュリティー脅威を明確にした上で、企業に損害や影響を与える可能性である想定リスクを設定し、その想定リスクに対する対策を検討することが推奨されています。**図5**では、この内容に沿ってIBMで実施しているリスク分析の流れを説明しています。

①グローバルでの事例から想定リスクを確認し、リスク検討チーム全員で理解する。

②対象企業におけるスマートメーター関連システムの固有な部分を把握し、グローバル事例と同様の想定リスクと固有の想定リスクを検討する。

③NISTIR 7628で推奨されたリスク分析手法を理解し、リスクの判定基準も設定する。

④想定リスクごとの実現可能性とインパクトを設定した結果を、ヒートマップに表し(**図6**)、想定リスクの対応優先順位を決める。

次に、スマートメーターを運用する上では、セキュリティーを維持・向上するための実施項目についてPDCAサイクルを回していくことが重要です。セキュリティー・テストについても含めて以下にその概要を説明します。

●Plan/計画

リスク分析を実施して想定リスクを設定した後、リスクを低減させる計画を以下の3つの観点から策定します(**図7**)。

①セキュリティー対策設定

ここでは前述したNISTIR 7628でのハイレベル・セキュリティー要件、およびグローバル事例を参照しながら、自社としての対策を設定します。さらに、想

実行可能性	インパクト				
	Very Low / Insignificant	Low / Minor	Midium / Moderate	High / Major	Very High / Catastrophic
Almost Certain	*T24*		*T54,T55*	*T2,T8,T38, T45*	
Likely	*T56*	*T6,T12,T13,T14, T27,T34,T36, T49,T63,T66*	*T5,T10,T16,T17, T21,T37,T41, T43,T60,T62,T67 T70*	*T7,T11,T19,T20, T28,T29,T33,T39, T40,T46,T47,T48 T51,T52,T61*	*T1*
Possible	*T25*	*T9,T15,T31,T32, T64*	*T18,T44,T58,T65*	*T22,T23,T26,T50, T68,T69*	
Unlikely		*T3,T3,T57,T65*	*T53,T59*		*T42*
Rare		*T35*			

※*TXX*は、設定した想定リスクの番号

図6. セキュリティー想定リスク・ヒートマップ[5]

定リスクの対応優先順位とセキュリティー対策投資とのバランスを考えて対策ロードマップを作成します。

②セキュリティー運用プロセスの構築

セキュリティー対策は技術的対策と運用対策から成ります。技術的対策とは、リスク分析で設定した想定リスクに対して、リスクの重要度（＝実現可能性×インパクト）を下げるための技術的なセキュリティー対策のことであり、例えば、暗号化に関するセキュリティー対策、構成管理に関するセキュリティー対策、ネットワークや通信に関わるセキュリティー対策などが挙げられます。一方、セキュリティー運用対策は、インシデント対応を実行するための準備から検知・分析、封じ込め・根絶・復旧および事件後の対応までのプロセスで想定されるリスクの対策として設定します。

セキュリティー運用プロセスの構築は、運用対策の一つとして実施していきます。こちらもインシデント対応のグローバル標準であるNIST SP800-61 [6]、およびグローバルでの運用プロセス事例を参照して、TO-BEプロセス（あるべき姿）の達成目標を設定する必要があります。

③セキュリティー・テスト計画

スマートメーター関連システム情報を理解した上でセキュリティー対策が正しく実装されていることを確認するホワイトボックス・テストと、仮想外部攻撃者からの攻撃に対応するセキュリティー対策が正しく実装されているかをスマートメーター関連システム情報を得ることなしに確認するブラックボックス・テスト（ペネトレーション・テスト）について、グローバルで実施されているテスト事例を参照しながら計画します。

ブラックボックス・テストは基本的に仮想外部犯行によるテストであるため、すべての脅威を想定してテストするのではなく、まずホワイトボックス・テストで設定したセキュリティー対策が正しく実装されていることを確認した上で実施します。何度も繰り返しテストすることを避けることができ、効率良く実施できます。

●Do/実行

実行段階では以下の3つを行います（**図8**）。

①セキュリティー対策実施

設定したセキュリティー対策が、正しく基本設計、および詳細設計に反映されているかを確認します。

②セキュリティー運用実施

セキュリティー対策のうち、運用対策としてセキュリティー運用組織、および業務プロセスを設定します。

③セキュリティー・テスト実施

計画したテスト計画に基づきシステムテストおよびホワイトボックス・テストを実施し、セキュリティー対策が適用できたことを確認した後、ブラックボックス・テストを実施し、運用開始前の最終確認とします。

●Check&Act/チェック&アクト

チェック、アクト段階では以下3つを行います（**図9**）。

①想定リスクの見直しと改善

電力会社は、攻撃するツールや手法が進歩するに従って新たなセキュリティー・インシデントも増えるため、運用開始前に設定した想定リスクに追加していく必要があります。従って、定期的にリスク分析を実施することが重要です。セキュリティー対策も、ロードマッ

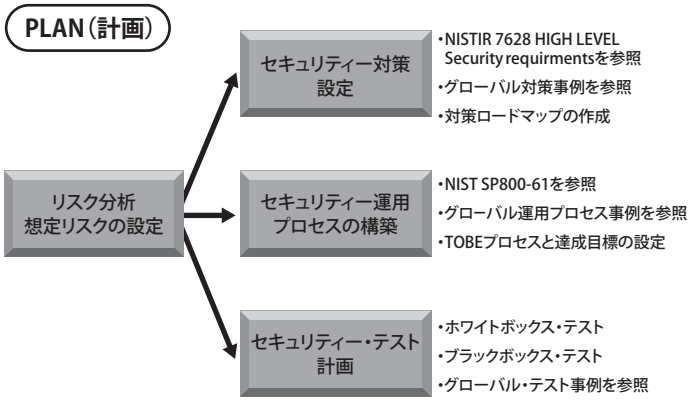

図7. 計画段階で実施すべき事項[2]

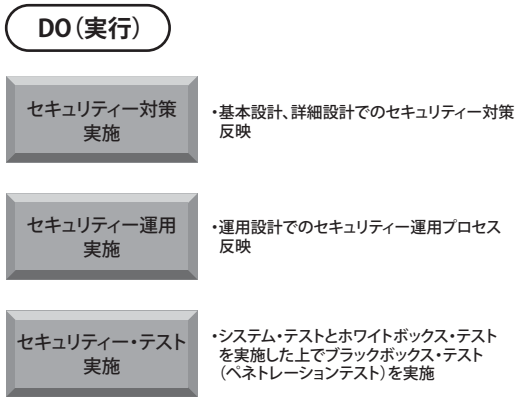

図8. 実行段階で実行すべき事項[2]

プ通りに適用できているのか、新たな対策が必要になっていないかなどを定期的に確認していく必要があります。

②セキュリティー運用見直しと改善

セキュリティー運用をプロセス通りに実施できるかを運用開始前に確認すべきであることは、前述のとおりです。開始後も問題なく運用できているかを定期的に評価することで、セキュリティー運用達成度をより定量的に把握することができます。

③セキュリティー・テストの実施

セキュリティー・テストも、システム改変があった場合などに再テストの必要性を見直すべきです。特にブラックボックス・テスト（ペネトレーション・テスト）については、新たな攻撃ツールや新たな攻撃手法が開発されていることがありますので、定期的に必要性を見直し実施すべきだと考えます。

3. 最後に

スマートメーターが導入されると、各家庭にあるスマートメーターと電力会社間の双方向通信が実現し、各家庭と電力会社間がつながります。また、原子力発電所やその他の電力関連制御システムも、システム間の通信によって、より精度が高く効率的な制御を実現しようとすると、従来は完全に外部と遮断していた場所からもつながるケースが出てきます。つまり、E&U企業において今まで外部とは遮断していたシステムも外部とつながっていくことで、セキュリティー脅威がますます増えていくことになり、セキュリティー想定リスクも増えていくことが予想されます。それに対応するためには、リスク分析を定期的に実施していくことが重要です。

スマートメーターのセキュリティーのみならず、スマート・グリッド、原子力やE&Uにおける制御システムについても、今回説明したリスク分析手法と同様のアプローチをしていくべきです。

現在IBMは、日本を含めグローバルでE&U企業のこの分野についてコンサルティングから実装・運用までEnd to Endでご支援しています。これからも日本を含めグローバルで一体となったチームで、E&U企業のセキュリティーに貢献してまいります。

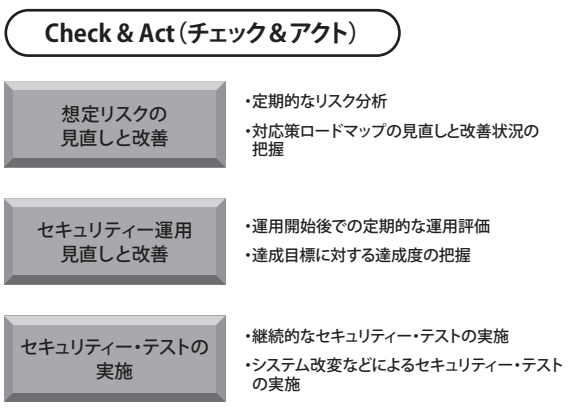

図9. チェック、アクト段階で実施すべき事項[2]

[参考文献]

[1] IBM：IBM Security Services 2014 Cyber Security Intelligence Index for Energy and Utilities, http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03049usen/SEW03049USEN.PDF

[2] Saitoh, T. and Dougherty, S. ; Latest Smart Meter Security Operation, International Smart grid EXPO (2015).

[3] IPA：制御システムにおけるセキュリティマネジメントシステムの構築に向けて～ IEC62443-2-1の活用のアプローチ ～, http://www.ipa.go.jp/files/000014265.pdf

[4] NIST：NISTIR 7628 Guidelines for Smart Grid Cybersecurity, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[5] Dougherty, S. and Saitoh, T. :Smart Meter Deployment Threat and Vulnerability Analysis and Response, Journal of Energy and Power Engineering, vol2, No2, pp.199-213 (2015).

[6] NIST：Computer Security Incident Handing guide, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

日本アイ・ビー・エム株式会社
グローバル・テクノロジー・サービス事業
セキュリティ, AP／コンサルサービス
Energy&Utility担当 アソシエート・パートナー

齋藤 高樹
Takaki Saitoh

日本IBM製造開発部門でハードウェア開発に従事した後、コンサルティング部門にて主に製造業の開発に関する業務改革をリードする。現在は、Energy&Utilitiesのセキュリティーに関するアソシエート・パートナーとしてとして、日本でのスマートメーター・セキュリティー・プロジェクトのPMおよび日本におけるビジネス展開を担当している。

IBM Corporation
Global Critical Infrastructure Security Services（CISS）
IBM Security
Energy & Utilities Leader
Smart Grid Cyber Security & Privacy Architect

Steven Dougherty

スマート・グリッドや制御システムなど電力業界でのサイバー・セキュリティーの第一人者として世界で広く認知されている。スマート・グリッド・サイバー・セキュリティーの業界ガイドラインであるNISTIR 7628のワーキング・グループの委員をはじめ、多くの規格作成業務に参加。