URL https://journal.ntt.co.jp/article/36074
DOI https://doi.org/10.60249/25091201

NTTドコモビジネス
プラットフォームサービス本部　マネージド＆セキュリティサービス部
Business Information Security Officer
エバンジェリスト

竹内文孝　Fumitaka Takeuchi

サイバーリスクマネジメントのエバンジェリスト（伝道者）として，啓蒙と市場活性化，産業の発展をめざす

2024年末から2025年初頭にかけて，航空会社や金融機関等がDDoS（Distributed Denial of Service）攻撃を受け，大きな社会的混乱が発生しました．国立研究開発法人情報通信研究機構（NICT）が運用している大規模サイバー攻撃観測網（NICTER）のダークネット観測で確認された総観測パケット数が，2015年の約632億から2023年には約6197億と9.8倍となっており（総務省令和６年版情報通信白書），サイバー攻撃は増加傾向にあります．こうしたサイバー攻撃はDDoS攻撃をはじめ，侵入によるデータ改ざん，ランサム攻撃等多様な手口があり，最近ではAI（人工知能）を利用したフェイクメールによる詐欺等新たな手口も登場しています．サイバー攻撃をはじめとするセキュリティリスクの低減，インシデント発生からの早期回復等の対応を準備するのが「サイバーリスクマネジメント」です．サイバーリスクマネジメントをエバンジェリスト（伝道者）として啓蒙し，産業の発展に向けて挑戦している，NTTドコモビジネス　竹内文孝氏に，サイバーリスクマネジメントとエバンジェリストの活動，お客さまに誠実に寄り添いつつ行うディスカッションに対する思いを伺いました．

インシデントの発生を前提として，その抑制から回復までを準備するサイバーリスクマネジメント

エバンジェリストについて紹介いただけますか．

NTTドコモビジネス（旧NTTコミュニケーションズ）のエバンジェリストは，2014年に「自身の専門テーマを軸に発信・提言し，市場の活性化・拡大を目的に活動する人材を指し，社会・産業の発展，お客さまの課題解決に貢献すべく多方面にわたって活動を行う」ことを目的に制定されました．当初は，クラウド，ネットワーク，セキュリティ，アプリケーションの４カテゴリーごとに１名ずつ選出され活動を開始しました．翌2015年には新カテゴリーのIoT（Internet of Things）が追加され，メンバもIoTの１名，既存カテゴリーに２名追加され，７名で活動してきました．その後カテゴリー追加・改変，メンバが追加され，2025年現在で，AI ４名，IoT ２名，セキュリティ５名，地域・中小DX １名，プラットフォーム・ネットワーク９名の５カテゴリー，21名で活動しています．

私は，2001年に「GuardIT」というセキュリティサービスの開発・運用に携わって以来，2003年に，社内外関係なくセキュリティ監視・運用の課題解決を目的としたSOC（Security Operation Center）を創設し，2009～2010年にM&Aしたドイツのセキュリティ企業Integralis社，スウェーデンのマネージドセキュリティサービス企業Secode社のPMIにかかわり，この３つのSOCを統合し設立されたNTT Com Securityの日本法人代表取締役社長への就任を経て，現職のマネージド＆セキュリティサービス部Business Information Security Officerに至るまでセキュリティにかかわり続けています．私たちのSOCは日々巧妙化するサイバー攻撃に対抗するため，ネットワークや端末に配置されたセキュリティ機能のログを収集し，相関的なリアルタイム分析によって脅威を検出し，お客さまへの通知そして対処まで，幅広い技術を

駆使したサービスを提供しています．また，2003年のSOC設立当初から高度な運用技術をお客さまにご理解いただくため，実際のオペレーション模様を見学できるコースを設け，お客さまとのQ&Aやディスカッションをとおして啓蒙活動・営業活動を行っていました．これがまさにエバンジェリストの活動に近いもので，2015年にサイバーリスクマネジメントの観点から，セキュリティを専門としたエバンジェリストとして活動することにつながりました．

サイバーリスクマネジメントとはどのようなものなのでしょうか．

サイバーリスクマネジメントとは，セキュリティインシデントが発生することを前提として，インシデントの抑制から回復までの対応を準備しておくことです．具体的には，①権限を持つ人しか情報にアクセスできない（機密性），②情報が常に正確な情報に確保されている（完全性），③情報が必要なときにいつでも利用できる（可用性），④動作の主体が本物であると証明できる（真正性），⑤ある主体の動作を説明できる（責任追跡性），⑥ある主体の動作証跡を残し明確にできる（否認防止），⑦ある主体を一貫して期待通りに動作できる（信頼性）という情報セキュリティの7要素を維持することです．

サイバーリスクは，システム環境，物理的な環境，従業員（人）・組織，業務プロセス・取引先，法規制・社会情勢，攻撃・犯罪・災害といったあらゆるところに内在しており，システムの脆弱性をねらった攻撃，ランサム攻撃，DDoS攻撃等システムに関係するものから，不注意による情報漏洩，ビジネスメール詐欺，内部不正による情報漏洩等人為的なものまで，多様なものがあります（**図1**）．また，インシデント発生の可能性や発生時の影響度により，リスクへの対応は異なります（**図2**）．

攻撃手法は種々ありますが，攻撃者の行動パターンはほぼ決まっています（**図3**）．第一段階で攻撃者は侵害対象となる弱点（脆弱性放置や設定不備等）を探す偵察行動を行います．したがって，弱点を減らすことが「ねらわれない環境」となり，万が一標的になったとしても「攻撃の難易度が上がる」（この2点を「衛生管理」といいます），つまり手間がかかることになり，攻撃の矛先が別に向かうことになります．

インシデントが発生した場合は，インシデント対応ライフサイクルに従って，異常検知から当該被疑端末の封じ込め（ネットワークからの切り離し等の影響を最小化する措置），復旧対応，事故後の処理を行うことになります．インシデント対応ライフサイクルは事故が起きる前提で一連の対応を準備することから始まり，日々の運用監視がベースとなる小さな改善と，重大事故発生時の対策強化となる大きな改善の2つの改善サイクルを回しながら，継続的に最適化していくことが重要になります．

昨今，イノベーション創出に向けて，DX（デジタルトランスフォーメーション）推進およびAI活用が注目されています．DXにおいては，各種の業務システムがネットワークに接続され，さらにはクラウド化されてきています．AIについても，対話型のAIから推論型AI，エージェントが洗練されてきて自律型AI，そしてその先にはイノベーションを支援する革新型AI，組織全体の仕事に対応できる組織型AIへと進化していくと考えられます．

現在のAI，特にChatGPTのような生成AIは，インターネット上の情報を検索して回答を生成するものが主流です．DXにおいてもAIにおいても，オープンなネットワーク環境がベースとなっています．オープン化により弱点が増えることになり，攻撃者からねらわれやすくなります．また，AIの普及に伴って対話型の問題解決プロセスの過程で意図せず情報漏洩につながるケースや，AI生成した情報に公平性やプライバシー保護の配慮が不足し社会的リスクにつながったケース，AI利用者の規定違反や単純ミス，さらにはディープフェイクによる詐欺等，新たなタイプのサイバーリスクが顕在化し報道されています．

従来，多くの企業ではセキュリティ対策はコストととらえられて，個別の対策が講じられてきましたが，DX推進×AI活用によるイノベーション創出のための投資として，境界防御，多層防御，監視運用といった従来の防衛的な対応策に加えて，セキュリティ事故を前提とした事業継続性の確保や経営基盤の強靭化を目的としたサイバーリスクマネジメントの新たな展開が求められています（**図4**）．

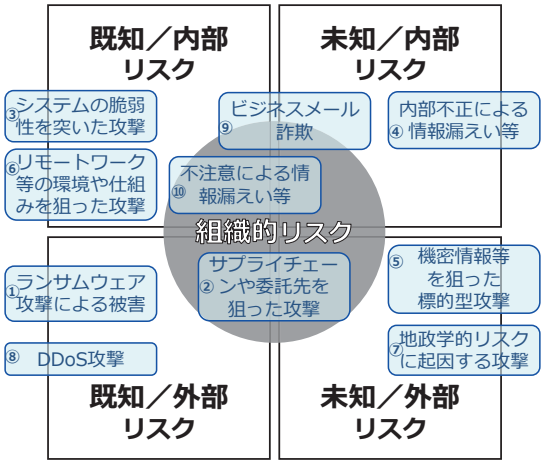

図1　サイバーリスクの例

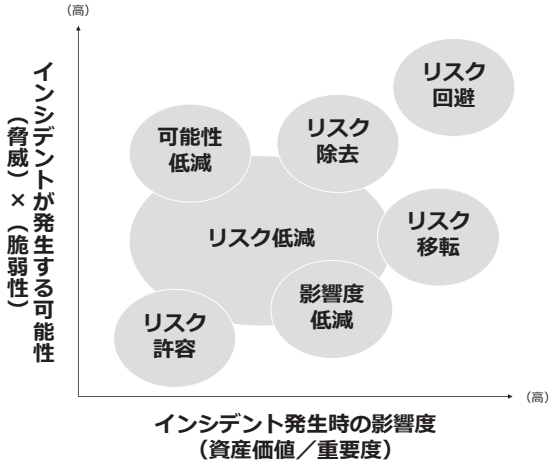

図2　サイバーリスクへの対応

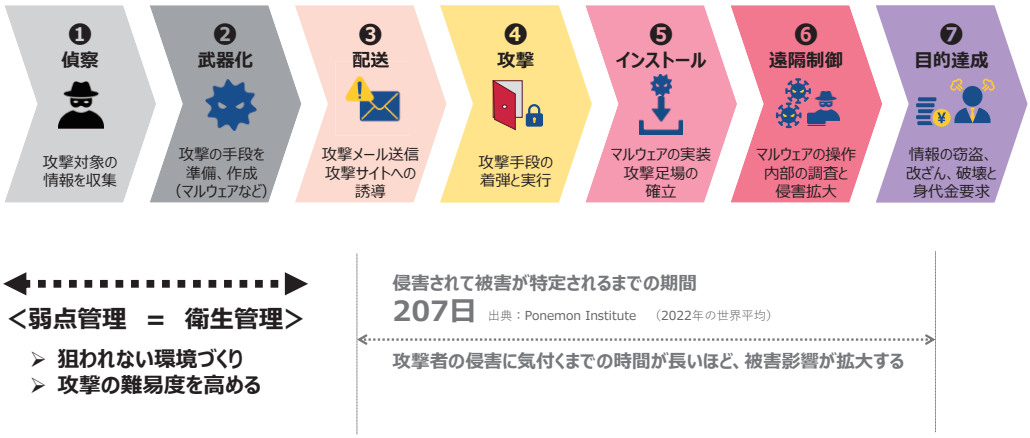

図３　攻撃者の行動パターン

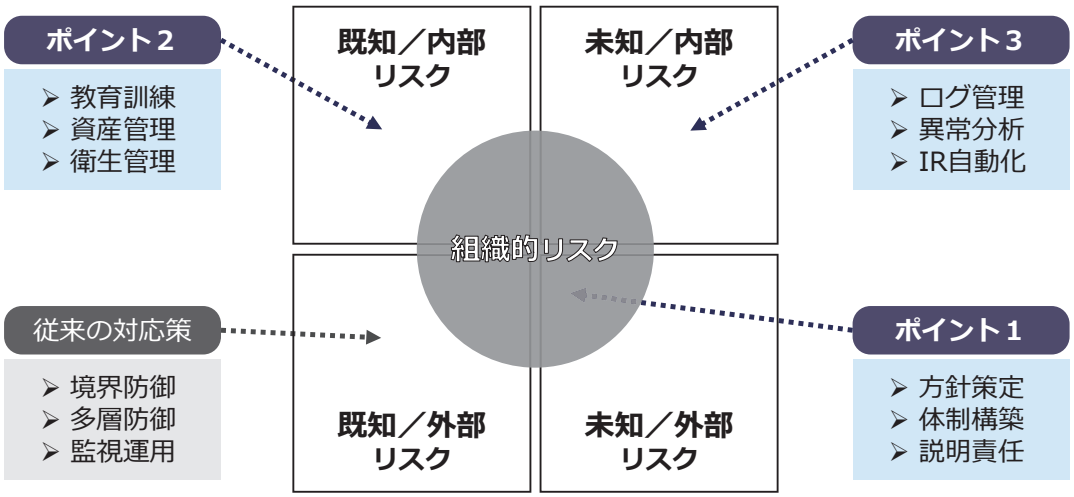

図４　DX推進×AI活用に求められるサイバーリスクマネジメント

エバンジェリストとしてどのような活動をされているのでしょうか．

講演会・セミナーや執筆活動のほか，個別のお客さま対応等による啓蒙活動が中心です．

講演会・セミナーは，電子情報通信学会，公益社団法人企業情報化協会等関連団体，JBpressやITmedia等のメディア，国内各地の商工会議所など経済団体のほか，ブラジル日本商工会議所主催セミナーなど海外出張対応，およびNTTグループ主催の講演会・セミナーに年間10件程度登壇しています．

このほか，各種メディアへの記事掲載，連載も行っており，執筆活動としては，2019年８月に『決定版サイバーリスクマネジメント』（NTT出版）を上梓しました．

さらに，通常の業務としてSOCの運用や総合リスクマネジメントサービス「WideAngle（ワイドアングル）」等のセキュリティ関連プロダクトも担当しています．こうした業務と連携したかたちでエバンジェリストとしての啓蒙活動も精力的に行っています．具体的にはSOC見学のプログラムの中で，サイバーリスクマネジメントに関する提言やお客さまが持つ個々の課題へのアドバイス，意見交換をしています．このほか，お客さまラウンドテーブルという企画も主催しています．これは，お客さまを３～４社程度招待し，半日かけてお客さまどうしでセキュリティの課題抽出から対策等の取り組みをディスカッションしていただくことにより，情報や課題意識を共有していただくもので，私がそのファシリテータを行っています．これにより，お客さまが自社のセキュリティレベルを他社比較によって認識し，お客さまの工夫・事例を紹介し合うことで，同業種・異業種関係なく新たな気付きを得ることができます．お客さまどうしがこの場でしか聞けない深いディスカッションにより相乗効果が出てきますので，お客さまの評判が良い企画です．

そして，こうした活動が，市場開発やマーケティングにもつながっています．ここ２年間で約110件のSOC見学を対応しました．そのうち35件に私がエバンジェリストとして対応し，27件で見学後の営業活動に展開，18件でWideAngleをはじめとするサービスの受注につながりました．SOC見学にお越しいただくお客さまの潜在ニーズを的確に掘り起こすことができている結果だと思うので，まさに「自身の専門テーマを軸に発信・提言し，市場の活性化・拡大を目的に活動する人材」というエバンジェリストと

しての役割を果たしているのではないかと自負しています．

お客さまに誠実に寄り添いつつ，ディスカッションを通して勉強することで，エバンジェリストとしての能力を磨く

エバンジェリストとして高度なスキルや知見が必要になると思いますが，それはどのように磨いているのでしょうか．

私にとっての１番の勉強の題材は，SOC見学者の対応やお客さまラウンドテーブルにおけるお客さまとのディスカッションにあります．講演会やセミナーでもお客さまとの接点はあるのですが，こちらからの情報提供がメインになるので，新たな気付きなどの題材はお客さまとのディスカッションの中に豊富にあります．

SOC見学会で私からお客さまへ問いかける振りは毎回ほぼ同じような内容の話をするのですが，お客さまの反応や質問のポイントは個々に異なります．こうしたディスカッションにおいて，新しい課題やお客さまが苦労されている点等が具体的に明確になり，それに対してどうしていくのかといった提言をしたり，お客さまの話に関する情報収集や理解を進めることが，とても良い勉強の機会になっています．

それから，2005年にCISSP（Certified Information Systems Security Professional）という，国際的に認められた情報セキュリティ・プロフェッショナル認定資格を取得したのですが，３年ごとの認定更新を行っています．更新の要件として，専門性に関するセミナーやトレーニングコースの受講，通常の業務とは異なる独自性の高いプロジェクトの経験，サイバーセキュリティに関する記事の出版，情報セキュリティに関連したプレゼンテーションの準備や情報セキュリティ教育の実施等が必要であり，これらをとおして世の中の動向を含めた勉強をしています．

エバンジェリストとしてどのようなことを意識して活動しているのでしょうか．

「お客さまに誠実に寄り添う」ことを心掛けています．エバンジェリストの活動の中でお客さまと接する機会が多いのですが，それぞれ業種業態に応じた独特の問題点・課題を意識されているうえに，自社のセキュリティをご担当されているお客さまが多いので，私もその場で即答できないこともあります．このようなときは，適当に回答することはせず，お客さまの立場や問題点の背景なども踏まえて，後日回答させていただくようにしています．これにより，私自身も勉強になりますし，お客さまとの信頼関係が深まると感じています．

振り返ってみると，エバンジェリストになったばかりのころは，より大規模の講演会・セミナーにより多く登壇することが１つの目標になっていたのですが，３～４年経過したころから，セミナーでは質疑の時間は取るものの話が一方通行であることに気付き，お客さまラウンドテーブルを企画しました．ラウンドテーブルでは，私も含めて参加者全員でディスカッションができ，それにより理解が深まり，啓蒙活動としての成果が出ています．それ以降，参加者とのコミュニケーションが大切だという思いが強くなり，「お客さまに誠実に寄り添う」ことの意識がより一層強くなりました．

サイバーリスクマネジメントの分野は次々と新しいキーワードが登場してくるのですが，基本的な行動としては脆弱性の排除とそのコントロールが重要となります．これは基本的な要素として変わるものではありません．そこで，お客さまとのコミュニケーションにおいては，基本的な行動の大切さを繰り返し伝えつつ，お客さまの問題点・課題に回答していくように意識しています．

今後どのようなことをやりたいのでしょうか．

セキュリティの世界は，大企業から徐々に対応が展開されてきています．ところが，大企業で一生懸命セキュリティ対策を行ったとしても，例えばサプライチェーンの中にある中堅・中小企業は未対策である場面が非常に多くあり，これがサプライチェーンリスクとして顕在化してきています．中堅・中小企業においては，セキュリティの重要性に対する意識は形成されてきているのですが，依然コストや人材的な課題により，対応がなかなか進まない状況です．

2022年のNTTドコモグループ再編以前は，NTTコミュニケーションズは大企業を中心とした法人のお客さまがターゲットであり，私たちのセキュリティ関連のビジネスもこうしたお客さまとのお付き合いが中心でした．NTTドコモグループ再編以降は，中堅・中小企業のお客さまもターゲットとなりました．これをいい機会として，コスト・人材的な課題をクリアしながらセキュリティ対策を講じることで，この層のお客さまのセキュリティレベルアップをしていきたいと思います．

お客さまと接する機会を増やす中で，自分の力を110%発揮して成長する

後進やパートナーへのメッセージをお願いします．

お客さまと対面する機会をより多く持つことが，自分にとって非常にいい糧となります．お客さまとの対面は，提案活動，プレゼンテーションはもちろんですが，トラブルやお客さまにおけるインシデント発生等に際して，その解決のお手伝いをする場面にもあります．大切なのはそのときにお客さまとコミュニケーションすることです．こうした機会は自分にとってさまざまな意味で勉強になり，それが将来の自分にとっての非常にいい糧になるのです．

それから，「立場が人を育てる」という言葉がありますが，その立場にいればいいというものではありません．そして，与えられた立場の範囲で自分の可能性が制限されるものでもありません．立場により自分が育っていくためには，自分の力を110%発揮することをめざして，チャレンジし続けてください．