URL https://journal.ntt.co.jp/article/39526
DOI https://doi.org/10.60249/26063102

NTT西日本のCybersecurity Primary Careの取り組み

サイバー攻撃の高度化と人材不足が深刻化する中，多くの企業が「何を，どこまで対策すべきか分からない」状態に置かれています．NTT西日本では，医療における「かかりつけ医」の発想をセキュリティ領域に応用したCybersecurity Primary Care（CPC）を提唱し，お客さまのセキュリティ環境を伴走して継続的に守る取り組みを推進しています．本稿では，CPCのコンセプトと事業展開，今後の展望を紹介します．

なぜ今，セキュリティに「かかりつけ医」が必要か

■サイバーリスクの深刻化

事業のデジタル化が加速する中，サイバーリスクは企業の事業継続を左右する経営課題へと変化しています．ランサムウェア*1による業務停止，サプライチェーン*2を経由した情報漏洩など，サイバー攻撃は企業規模や業種を問わず影響を拡大させています．かつてはIT部門の技術的問題として扱われていたセキュリティが，いまや取締役会の議題となる時代です．

とりわけ深刻なのは，攻撃者側の手法が高度化・組織化していることです．生成AI（人工知能）の悪用によるフィッシングメールの巧妙化，ゼロデイ脆弱性*3を突いた攻撃の増加など，防御側の対応を上回る速度で攻撃手法は進化を続けています．攻撃対象も，大企業に限らず，中小企業やサプライチェーンの末端企業にまで広がっています．「うちは狙われるような会社ではない」と考えていた企業が被害に遭うケースも報告されており，従来の認識を見直す必要性が指摘されています．

■対策の実態と課題

こうした脅威の増大にもかかわらず，多くの企業ではセキュリティ対策が十分に機能していません．特に中堅・中小企業においては，限られた経営資源の中でセキュリティにどれだけ投資すべきかの判断そのものが難しい状況です．そして，その要因は複合的です．

まず，深刻な人材不足があります．国内のセキュリティ人材は約11万人が不足しているとされ，専任の担当者を配置できない企業が大半を占めます．次に，人的要因の問題です．サイバー攻撃の原因の約7割は人的要因に起因するとされていますが，従業員への教育・啓発は一過性のものにとどまりがちです．さらに，侵入経路の約60%でパッチ*4が未適用であるという調査結果は，日常的な運用管理の不備が攻撃の入口を広げている現実を示しています（**図1**）．

多くの企業の担当者が抱える課題感は，「何を，どこまで対策すれば十分なのか分からない」「誰に相談したらいいのか分からない」という言葉に集約されます．セキュリティ製品やサービスは数多く存在しますが，自社にとって何が最適かを判断できる人材や知見が社内にないのです．結果として，対策が後手に回り，問題が顕在化してから初めて専門家に頼るという悪循環に陥っています．

■医療との類似構造

ここで，医療の世界に目を向けてみます．私たちの健康管理には，「かかりつけ医」という存在が欠かせません．日常的に体調を把握し，予防的なアドバイスを行い，異変があれば早期に発見

*1 ランサムウェア：コンピュータ内のデータを暗号化し，復元と引き換えに身代金を要求する不正プログラムの総称．
*2 サプライチェーン：原材料の調達から製品の販売に至るまでの一連の事業活動の連鎖．
*3 ゼロデイ脆弱性：ソフトウェアの修正プログラムが提供される前に悪用される，未修正のセキュリティ上の欠陥．
*4 パッチ：ソフトウェアの不具合や脆弱性を修正するために提供される更新プログラム．

予算の最適化	対策の遅れが会社の信頼・事業に直結する中必要な予算と施策の妥当性を判断できていない
専門知識の不足	高度化する脅威に対し，社内人材のみでは対応力が不足している
リスクの不透明さ	残存リスクが可視化されず，経営判断の根拠が不十分な状態にある
技術進化への対応	脅威の変化に社内対応が追いつかず，最適な手段の選定が困難
法令遵守の複雑さ	多様化する規制への対応範囲が不明瞭で，専門的な解釈と支援が求められている
教育と意識向上	教育の方法や効果的な進め方が定まらず，社員の意識醸成が進まない

図1　セキュリティ対策における経営上の課題

図2　医療とサイバーセキュリティの共通点

して対処する．必要に応じて専門医を紹介する．こうした継続的な関係性に基づく健康管理の仕組みが，医療の世界では当たり前のものとなっています（**図2**）．

サイバーセキュリティにおいても，同様のアプローチが必要ではないでしょうか．症状が出てからでは手遅れになるのは，人体もIT環境も同じです．日常的な管理・予防・早期発見の仕組みがなければ，被害は拡大し，回復にかかるコストも膨らみます．

つまり，企業のセキュリティにも「かかりつけ医」が求められているのです．自社の状態を普段から把握し，予防策を講じ，異変を早期に検知し，いざというときには迅速に対処する．そうした支援の継続的な仕組みが，今もっとも必要とされています．

図3　Cybersecurity Primary Care の基本思想

Cybersecurity Primary Careのコンセプト

■CPCの基本思想

NTT西日本が提唱するCybersecurity Primary Care（CPC）は，単発のセキュリティ製品導入やスポット対応ではなく，お客さまとの継続的な関係性の中でセキュリティ環境を守り続けるという考え方です（**図3**）．

医療におけるプライマリ・ケア*5が，特定の疾患だけでなく患者全体の健康を継続的に管理するように，CPCはお客さまのセキュリティ環境全体を包括的かつ継続的に支援することをめざします．

従来のセキュリティ対策は，特定の脅威や規制への対応を目的としたプロダクトアウト的な「点」の施策いわば「個別最適型の対応」になりがちでした．ファイアウォール*6を導入したら終わり，セキュリティ研修を年1回実施したら終わり，という対応です．しかし，国の動向としてセキュリティに関する変化は激しく，サイバー脅威も常に進化しています．こうした「点」の対策では，変化に追従することが困難です．

CPCは，この「点」（プロダクトアウト：個別最適型）の施策を「線」（カスタマーサクセス：課題解決型）の支援へと転換する発想です．お客さまの状況を継続的に把握し，変化に応じた最適な対策を提案し続けることで，セキュリティの課題を一緒に解決していきます．

重要なのは，CPCは特定の製品やサービスの名称ではないということです．CPCはNTT西日本のセキュリティに対するコンセプト・考え方であり，その考え方に基づいて多様なサービスを展開しています．お客さまとの長期的な信頼関係の中で，お客さまの事業成長とセキュリティの両立を支える．それがCPCの根幹にある思想です．

■NIST CSFと医療のとらえ方

CPCのフレームワークは，米国国立標準技術研究所（NIST）が策定したサイバーセキュリティフレームワーク（CSF）*7を基盤としています．NIST CSFが定義するセキュリティ対策の各機能を，私たちは医療の観点から次のようにとらえ直しています（**図4**）．

「健康管理」に相当する領域では，セキュリティ方針の策定やアセスメント，IT資産管理，脆弱性診断といった活動を行います．これはNIST CSFにおける「統治（Govern）」「識別（Identify）」に対応します．

---

*5　プライマリ・ケア：患者の健康問題に対し，総合的・継続的に対応する初期段階の医療サービス．
*6　ファイアウォール：外部ネットワークからの不正なアクセスを遮断し，内部ネットワークを保護する仕組み．
*7　NIST CSF：米国国立標準技術研究所が策定したサイバーセキュリティ対策の国際的な指針．

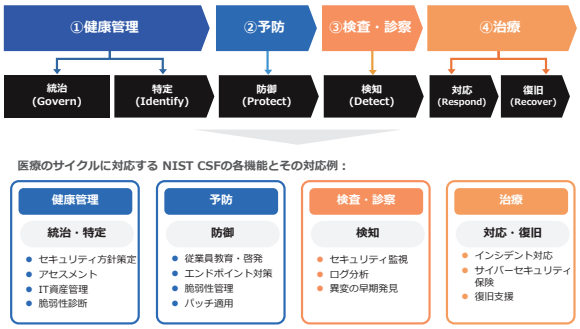

図４　NIST CSF と医療の対応関係

「予防」に相当する領域では，従業員への教育・啓発，エンドポイント対策，脆弱性管理，パッチ適用などを推進します．NIST CSF の「防御（Protect)」に対応する活動です．

「検査・診察」に相当する領域では，セキュリティ監視やログ分析を通じて異変の早期発見に努めます．NIST CSF の「検知（Detect)」に対応する活動です．

「治療」に相当する領域では，インシデント発生時の対応やサイバーセキュリティ保険の活用を含む復旧支援を行います．NIST CSF の「対応（Respond)」「復旧（Recover)」に該当します．

■めざす価値

CPC がめざすのは，お客さまのセキュリティ環境を伴走して継続的に守ることです．お客さまが安心して本業に集中できる状態を実現するために，セキュリティの「かかりつけ医」としてそばに寄り添い続ける．それが CPC の提供する価値です．

セキュリティは一度対策すれば終わりではなく，事業環境の変化，新たな脅威の出現，法規制の更新に合わせて常にアップデートし続ける必要があります．CPC は，そうした変化の中でもお客さまが迷わないよう，羅針盤の役割を担います．

CPC を基盤としたセキュリティ事業の展開

■プロダクトアウト提案の限界

従来のセキュリティ事業では，「この製品を導入すれば安全です」というプロダクトアウト*8型の提案が一般的でした．しかし，この提案手法には構造的な限界があります．

お客さまの事業環境，IT 環境，組織体制，従業員のリテラシー水準は企業ごとに大きく異なります．また，国の施策や顧客ニーズは常に変化しています．画一的な製品提案では，こうした個別性や変化への対応が難しいのです．結果として，導入した製品が十分に活用されない，あるいは新たな脅威に対応できないといった事態が生じてきました．

CPC では，製品ありきではなく，お客さまの課題を起点とした提案に転換しています．まずお客さまの話を聞き，現状を把握し，本当に必要な対策を一緒に考える．この順序を徹底することが，CPC の事業展開における基本方針です．

■CPC の取り組み全体像

CPC の取り組みは，前述した医療のとらえ方に基づき，「健康管理」から「治療」までを一貫してカバーする体制を構築しています．

具体的には，セキュリティアセスメントによる現状把握，教育・啓発プログラムの提供，セキュリティ監視・分析サービスによる常時観察，脆弱性診断による定期検査，インシデント対応支援による緊急時の治療まで，セキュリティライフサイクルの全段階にわたるサービスをラインアップしています．

お客さまは，自社の課題や状況に応じて，CPC の枠組みの中で適切な支援を受けることができます．医療に例えれば，町のクリニックのかかりつけ医が日々の健康管理を行いつつ，有事の際には高度な技術を持つ総合病院の専門医と連携して対応するイメージです．セキュリティ対策の全体像が見えることで，お客さまは個別の施策の位置付けや優先順位を理解しやすくなります．

■伴走型セキュリティ対策支援の基本プロセス

CPC のコンセプトを具体化するサービスの１つが，伴走型セキュリティ対策支援サービスです．このサービスは以下のプロセスで進行します．

①　アセスメント：まず，お客さまのセキュリティ環境の現状を体系的に評価します．技術的な対策状況だけでなく，組織体制，運用プロセス，従業員の意識レベルまで包括的に確認します．

②　ヒアリング：アセスメント結果を踏まえ，お客さまの経営課題や事業戦略と照らし合わせながら，セキュリティ上の優先課題を一緒に整理します．

③　ケアプラン策定：優先課題に基づき，お客さまに最適なセキュリティ対策の計画（ケアプラン）を策定します．すべてを一度に実施するのではなく，優先順位を付けた段階的な対策を提案します．

④　よろず相談：ケアプラン実行中はもちろん，日常的にセキュリティに関するあらゆる相談におこたえします．「こんなメールが届いたが大丈夫か」「新しいクラウドサービスを導入したいが注意点は何か」といった日常的な疑問にも対応します．

このプロセスは一度きりのものではありません．お客さまの環境変化やセキュリティ動向の変化に合わせて，定期的・継続的にアセスメントとケアプランの見直しを行います．セキュリティを取り巻く状況は激しく変化しますが，その変化にお客さまを置き去りにしない．それが伴走型セキュリティ対策支援サービスの本質です．

セキュリティ評価制度への対策

■サプライチェーンセキュリティ評価制度の動向

経済産業省では，企業のサイバーセキュリティ対策状況を可視化するサプライチェーンセキュリティ評価制度*9の整備を進めて

*8　プロダクトアウト：提供者側の製品・技術を起点とした提案手法．顧客の課題を起点とするマーケットインの対義語．

います．この制度は，企業のセキュリティ対策水準を段階的に評価し，取引先やステークホルダに対してセキュリティの取り組み状況を示すことを目的としています．

サプライチェーン全体のセキュリティ水準向上が求められる中，この評価制度への対応は多くの企業にとって避けて通れない課題となりつつあります．特に取引先から一定の評価水準を求められるケースが増えており，制度への対応が事業機会の確保にも直結する状況が生まれています．

■伴走型セキュリティ対策支援サービスにおける評価制度対応

伴走型セキュリティ対策支援サービスでは，サプライチェーンセキュリティ評価制度の評価項目を基にしたアセスメントを実施しています．お客さまの現在の対策状況を評価制度の基準に照らして可視化し，不足している対策や改善すべきポイントを具体的に提示します．

このアセスメントは，単にチェックリストを埋める作業ではありません．お客さまの事業内容やリスク特性を踏まえたうえで，評価制度の各項目がなぜ必要なのか，自社にとってどの程度の優先度があるのかを丁寧に説明しながら進めます．CPCの国の動向を継続的に注視する姿勢は，ここにも反映されています．社会や顧客のニーズに即したかたちでCPCの支援内容を見直し続けることが，お客さまへの価値提供の源泉です．

■お客さまの声

実際に伴走型セキュリティ対策支援サービスをご提案させていただいたお客さまからは，さまざまなお声をいただいています．

「サプライチェーンセキュリティ評価制度への対応が必要だと感じていたものの，社内のセキュリティ状況を把握できておらず，何からどう手を付ければよいのか分からなかった」「セキュリティ対策のコンサルティングは高価なイメージがあり導入に踏み切れなかった」「セキュリティの推進が一部の詳しい社員のスキルに依存しており属人化のリスクを感じていた」など，課題は一社一社で異なります．

こうしたお客さまに対して伴走型セキュリティ対策支援サービスを提案する中で，特に喜ばれているのは，大手コンサルティングファームと比較して手の届きやすい価格設定であること，セキュリティの専門知識を持つ有識者が継続的にサポートする安心感，そしてNTTブランドが持つ長年の通信インフラ運用で培った信頼――これらが経営層への説明材料としても有効であるという点です．

評価制度への対応は，単なるコンプライアンス対応ではなく，自社のセキュリティ水準を客観的に把握し，計画的に改善していく契機となります．CPCはその過程を一緒に歩むパートナーとして，お客さまの取り組みを支えています（**写真**）．

*9 サプライチェーンセキュリティ評価制度：経済産業省が整備を進める，企業のサイバーセキュリティ対策状況を段階的に評価・可視化する制度．

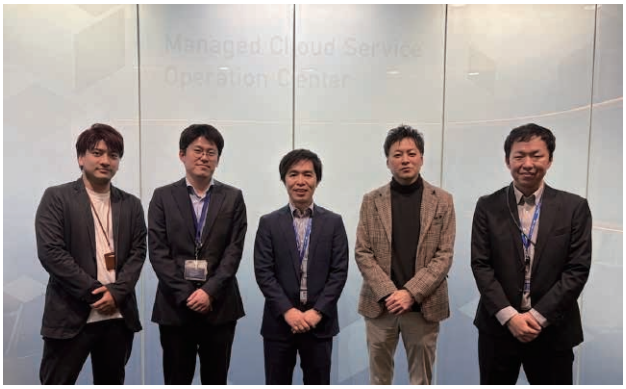

写真　Cybersecurity Primary Care推進の中心メンバー
（左より，松田悠佑，三宅広剛，鈴木雅士，門川大介，手柴弘樹）

今後の展望

CPCの最終ゴールは，単にセキュリティ事故を防ぐことでも，最新技術を導入することでもありません．お客さまにとって「困ったときに最初に相談できる」「平時から当たり前に頼れる」――セキュリティの「かかりつけ医」として，常に伴走し続ける，なくてはならない存在になること．それがCPCのめざす姿です．

セキュリティにおける「かかりつけ医」の本質とは，「事故を防ぐ専門家」ではなく，「不安を抱えさせない関係性」を継続的に提供する存在であることだと私たちは考えています．お客さまが日々の業務の中でセキュリティに対する漠然とした不安を感じることなく，本業に集中できる状態をつくること．そのために，平時の相談から有事の対応まで，一貫して寄り添い続ける関係性こそが，CPCの提供する最大の価値です．

そして，一社一社のお客さまへの伴走は，サプライチェーン全体，ひいては社会全体のセキュリティ水準の底上げにつながります．サプライチェーンの中で一社でも脆弱な企業があれば，そこが全体のリスクとなります．CPCを通じてより多くの企業のセキュリティ水準を向上させることが，安心・安全なデジタル社会の実現に貢献すると確信しています．

NTT西日本は，CPCを通じて，サイバーセキュリティを「特別なもの」ではなく，「日常の健康管理」のようにとらえる発想を社会に広げていきます．

■参考文献

(1) meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
(2) https://doi.org/10.6028/NIST.CSWP.29
(3) IPA（独立行政法人情報処理推進機構）：“情報セキュリティ10大脅威 2025,” 2025.
(4) https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

◆問い合わせ先

NTTビジネスソリューションズ
バリューデザイン部　マネージドサービス部門
マネージドビジネス担当

from