日立社内におけるサイバーレジリエンス強化に向けた取り組み

デジタル社会において，膨大かつ多様なデータが価値を生み出す一方で，安心・安全への脅威も飛躍的に高まっている。また，昨今のコロナ禍においてテレワークが推進されるなど働き方が大きく変わり，今後のセキュリティのあり方にも変革が必要となりつつある。
本稿では，ネクストノーマルな社会に向けて，現在，日立が取り組んでいるサイバーレジリエンス強化のためのサイバーセキュリティ戦略を，「統制」，「協創」，「自分ゴト化」の観点で紹介する。

村山 厚 | Murayama Atsushi
西村 健 | Nishimura Takeshi
渡部 真理 | Watanabe Mari

1. はじめに

昨今の企業を取り巻く環境からセキュリティを考えてみると，DX（デジタルトランスフォーメーション）と働き方改革という二つの新潮流がポイントになっている。DXにおいては，IoT（Internet of Things），AI（Artificial Intelligence）技術の急速な発展，ITプラットフォームのクラウド利用，生産・製造・開発現場のデジタル化への対応など，今までのオンプレミス中心の対策とは異なる発想が必要であり，そのクラウドプラットフォームにつながる機器が多様化し，増加するのに伴って，攻撃確率は格段に上昇するものと考える。また，働き方改革においては，新型コロナウイルスの感染拡大により，新しい働き方を余儀なくされている状況で，効率的かつ安全に業務を遂行するためのセキュリティ対策が求められている。

次に，セキュリティの脅威を振り返ってみると，2020年度はさまざまなインシデントが発生した年となった。今まで以上に標的型攻撃は高度化および多様化し，ランサムウェアにおける脅迫手法を情報窃取に応用するなど，従来の攻撃手法が複合的に用いられている。そして，社会インフラへの大規模な攻撃も多数発生している。

劇的な変化を続ける環境へ柔軟に適応し，かつ昨今のサイバー攻撃リスクへ的確に対応するためには，これらをプロアクティブに分析したサイバーセキュリティ戦略の立案と，サイバー攻撃が事業に影響を及ぼすことを前提としたサイバーレジリエンスの強化が必要になると考える。

本稿では，このような状況において，日立としてサイバーレジリエンス強化のために取り組んでいることを「統制」，「協創」，「自分ゴト化」の観点から述べる。

2. ゼロトラストセキュリティに向けた取り組み：統制

大きなコンセプトは,「サイバーセキュリティを経営課題として位置づけたセキュリティ対策を継続的かつ着実に実行する。しかし，絶対の安全はないと考え，有事の際には短い時間で回復できる抵抗力をつける」ということである。これを具現化するために取り組んできた内容を述べる。

昨今の主流となっている標的型攻撃への対策を中心に振り返ってみると，2011年は増加する標的型攻撃に対応するため，境界面の情報窃取対策の強化を実施した。次に，2017年はランサムウェア「WannaCry」事案への対応として，システム破壊への対策を強化し，サイバーセキュリティを経営課題として位置づけ，セキュリティガバナンス強化の推進を行った。

そして現在は，世の中の潮流や高度化・複合化しているサイバー攻撃への対応として，新たなセキュリティ対策に着手している。取り組みの核となるのは，ITプラットフォームのクラウド化に伴うゼロトラストセキュリティ対策の実装である。

実装にあたっては，業務システムのクラウド化の活性化および働き方改革の動向により，従来の境界型ITインフラからの変革が必要であるとの結論に至り，大きく舵を切った。具体的な考え方を**図1**に示す。

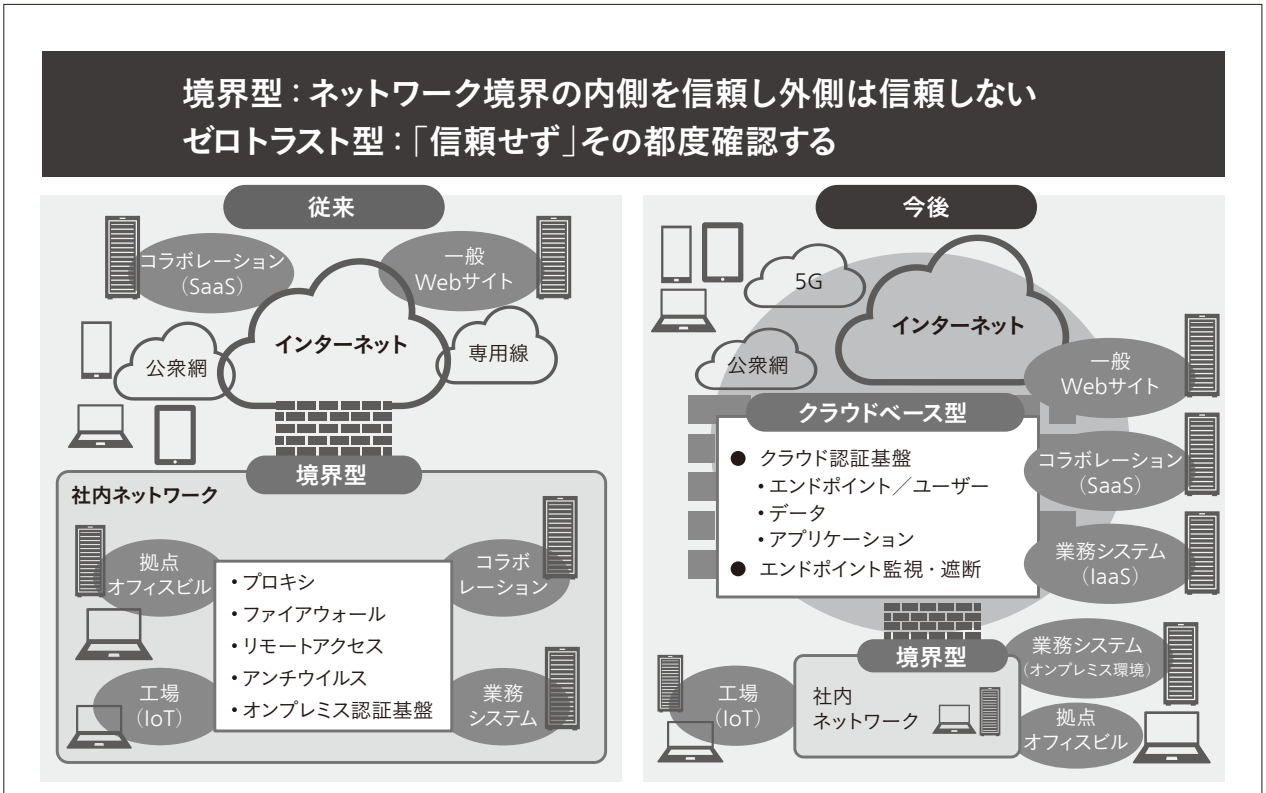
同図に示すとおり，今後のアーキテクチャの主流であるクラウドをベースとし，従来の境界型も併せたハイブリッドな構成での最適なセキュリティをめざしている。これらのクラウドベースITアーキテクチャを基準とするゼロトラストセキュリティを実現するうえでの重要な三つの要素に関して以下に述べる。

一つ目は,「認証」である。昨今のクラウド利用において，多要素認証のないクラウドシステムは，不正アクセスを受ける確率が非常に高い。そのためにもクラウドベースでの認証のあるべき姿を考え,特権管理強化,個々のユーザーの認証強化を推進している。

二つ目は,「エンドポイント」である。これはいわゆるパソコンやサーバ，スマートフォンだけでなく，クラウドシステムやアプリケーションまで含めたトータルシステムとしてのエンドポイント強化を目標にしている。また，併せて，ネットワークゲートウェイやデータそのも

図1｜クラウドベースITアーキテクチャの考え方

これからのアーキテクチャの主流であるクラウドをベースとし，今までの境界型をも包含したハイブリッドな構成での最適なゼロトラストセキュリティの構築を推進していく。



注：略語説明
5G（Fifth Generation），SaaS（Software as a Service），IaaS（Infrastructure as a Service），IoT（Internet of Things）

ののセキュリティを含めて検討を推進している。

最後は「サイバー統合監視」である。今までは境界型のネットワークにおける各種ログの分析・対応を中心に行ってきたが，今後は，クラウド，エンドポイントなどのあらゆるログを収集・相関分析し，インシデント対応をしていく必要がある。そのためにも，従来のサイバーセキュリティ監視を発展させた監視システムおよび体制の検討を開始している。

3. セキュリティエコシステム構築に向けた取り組み：協創

大きなコンセプトは，「社内のみならず，社外の各分野とセキュリティエコシステムを協創する」ということである。本来の業務が異なる部門であっても，セキュリティ活動という一つの目標に向かって相互に協力し合うことが，結果的に組織における事業活動の維持・拡大を可能にすると考える。

一般的にはセキュリティというとIT部門との連携と思いがちであるが，有事の際の対応では，IT部門に加えて広報，人事・勤労，法務などのあらゆる部門と連携しなければならない。また，セキュリティ対策の対象範囲が拡大している中，モノづくり部門や品質保証部門，調達部門などともしっかりと連携しないと，これらの対応はうまく機能しない。日立は，WannaCryの一件以降，会社一丸となってサイバー攻撃の脅威に対抗するために，このようなセキュリティエコシステムの構築が重要と考え，推進している。その要素となるのが，「モノ」，「人・組織」，「社会」が「つながる」という考え方である。以下にそれぞれの内容について述べる。

3.1
モノが「つながる」

DXでは，さまざまなつながりが新たな付加価値の創出や社会課題の解決をもたらす。これらを実現するために，IoTに代表される機器やシステムなどのモノが「つながる」環境が必要となり，これに対し，日立は，あらゆる環境において網羅的なサイバーセキュリティ対策に取り組んでいる。

3.2
人・組織が「つながる」

今までつながっていなかったモノが「つながる」中でセキュリティを確保するには，異なる組織が相互に協力して対策を推進することが必要になる。「統制」による対策徹底に加えて，立場，組織の垣根を越えたコミュニティづくりを行い，自身の役割を再認識すると同時に，周囲との連携を深めることで，人・組織が「つながる」活動を推進している。

3.3
社会が「つながる」

つながりは日立の中だけに限ったことではない。サイバーセキュリティ対策に取り組んでいる国，学校，企業との脅威情報や対策実行時の課題共有など，枠組みを越えたコミュニティの形成が必要不可欠になると考える。各企業や組織が，これらのコミュニティから得られたノウハウを自分たちのセキュリティマネジメントサイクルにフィードバックし，さらに広げるといった，社会が「つながる」活動も，積極的に推進している。

4. 新たなセキュリティ啓発に向けた取り組み：自分ゴト化

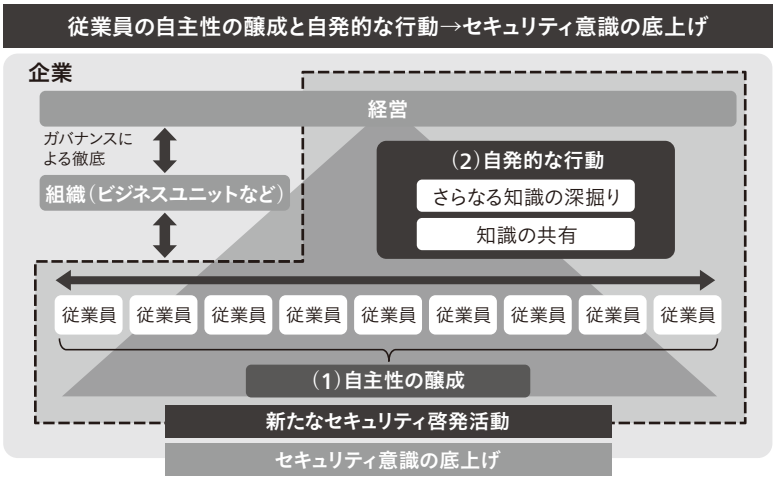
昨今の新型コロナウイルス感染拡大により，多くの人々が新しい働き方を余儀なくされた。日立もテレワークの導入を一気に加速させ，在宅勤務を標準としたこれからの働き方を推進するための施策に取り組んでいる。

一方で，サイバー攻撃の脅威はますます高まっており，テレワークの推進には十分なセキュリティ対策が不可欠である。今まで攻撃者の主なターゲットは組織のITの脆弱性であったが，テレワーク中心の働き方においては，「セキュリティ意識の脆弱性」が狙われることが想定される。オフィス以外で仕事をすることにより，慣れない環境の中，つい気が緩んだり，近くに相談できる相手がいなかったりと，誰もがリスクと隣り合わせになる。

本来，セキュリティ対策は，「IT」，「プロセス」と「ヒト」の3要素でバランスを取る必要がある。実態としては，「IT」，「プロセス」の整備は都度必要な対策をしているが，「ヒト」すなわち啓発や教育は，後手に回ってしまっているという傾向が見られ，世の中の状況に合わせた効果的な施策が実施できていないという課題がある。昨今の劇的な環境変化に対応するため，そして，これからの日立としてのセキュリティリスクを低減するためには，従業員への啓発・教育を拡充し，よりバランスの取れたセキュリティ対策を推進する必要があるとの考えに至った。

そのため，これからは「一人ひとりのセキュリティ意

図2｜これからのセキュリティ啓発のめざす姿
既存のガバナンス徹底に加え，従業員の自主性の醸成と，自発的な行動により，セキュリティ意識の底上げをする活動を推進していく。



識の向上こそが最後の砦である」と考え，既存のガバナンス徹底に加え，従業員の自主性の醸成と，自発的な行動により，セキュリティ意識の底上げを図る活動をスタートした（**図2**参照）。

これは，義務感からセキュリティ対策に取り組むのではなく，自らセキュリティに興味を持ってもらい，従業員が心から共感し，自分ゴトとして取り組むことをめざしているものである。具体的には，従業員が自発的にセキュリティに触れ，実践し，その知識を従業員どうしが共有することで，さらに意識を高め合えるような場の提供を推進していく。

5. おわりに

本稿では，日立としてサイバーレジリエンス強化のために取り組んでいることを「統制」，「協創」，「自分ゴト化」の観点から述べた。

日立は，自社における「統制」をしっかりと行うとともに，社外への活動などを通じて，産・官・学が「協創」する社会全体でのセキュリティエコシステムの構築を進めていく。

また，組織を守る大きな砦をつくるために，「自分ゴト化」を推進し，従業員一人ひとりがセキュリティを正しく理解し，あるべき姿に向かって働くことができる意識づくりをめざす。

これらの「統制」，「協創」，「自分ゴト化」を実現することで，新しい日常をより安心・安全かつ快適に過ごせるように，また，そこに潜むリスクを回避できるように，日立はサイバーレジリエンスのさらなる強化に取り組んでいく。

執筆者紹介

村山 厚
日立製作所 情報セキュリティリスク統括本部
情報セキュリティ戦略企画本部 所属
現在，セキュリティガバナンス戦略企画業務に従事

西村 健
日立製作所 情報セキュリティリスク統括本部
情報セキュリティ戦略企画本部 企画部 所属
現在，情報セキュリティ企画業務およびセキュリティ啓発業務に従事

渡部 真理
日立製作所 情報セキュリティリスク統括本部
情報セキュリティ戦略企画本部 企画部 所属
現在，セキュリティ啓発における企画立案業務に従事