Overview

ニューノーマル・アフターコロナを支えるセキュリティの実現に向けて

吉田 達也 | Yoshida Tatsuya
池田 芳紀 | Ikeda Yoshinori

1. はじめに

近年，企業ではAmazon Web Services※1) やMicrosoft Azure※2) に代表されるパブリッククラウドの活用が進展している。

この流れは，企業でのオンプレミスシステムの管理負担の軽減や，特定拠点に依存しない働き方の増加などにより従前から広まりつつあるが，コロナ禍によりさらに大きな広がりを見せた。

セキュリティの視点から見ると，これまではオフィスなどの「特定の場所」に社員やパートナーなど「特定の人物」が集まり，会社支給の「特定の機器」を用いた業務が行われていた。そのため，「オフィスに集まる」ことで機密情報などのセキュリティを確保していたと言える。

ところが，リモートワークの急激な進展はこれらの前提をすべて覆した。つまり，「会社外の場所」が前提となり，パブリックネットワークを介したパブリッククラウド上の業務は理論的には「誰でもアクセスが可能」となり，企業によっては「個人所有（または手配）の機器，BYOD（Bring Your Own Device）」を用いることも許容される状況となった。

それに呼応するように，あらゆるデバイスや人物による接続を信用しない「ゼロトラスト」の概念が認知を高めている。

「ゼロトラスト」では「誰でも」，「どこからでも」のアクセスを許容するため，オフィスに特定の人物が集まるといった従来以上の強力な本人認証が必要となる。これまで認証で一般的に行われていたパスワード認証においても高度なものが求められるが，パスワードの複雑化は利便性の低下を招くなど，セキュリティは利便性とトレードオフの関係にあった。複雑なパスワードの使い分けや，頻繁な変更要求により，利用者の負荷は非常に大きなものとなっていたため，生体認証技術を活用した多要素認証などセキュリティと利便性の両立が昨今のトレンドとなりつつある。

システム管理者側の視点では，システムがクラウドへ移行することで，各種ログの可視化や分析の自動化が実現したほか，セキュリティ監視も容易となることでシステム全体のセキュリティ強化と省力化が可能となった。これらはふるまい検知など新たなサイバー攻撃への対策の一助ともなっている。

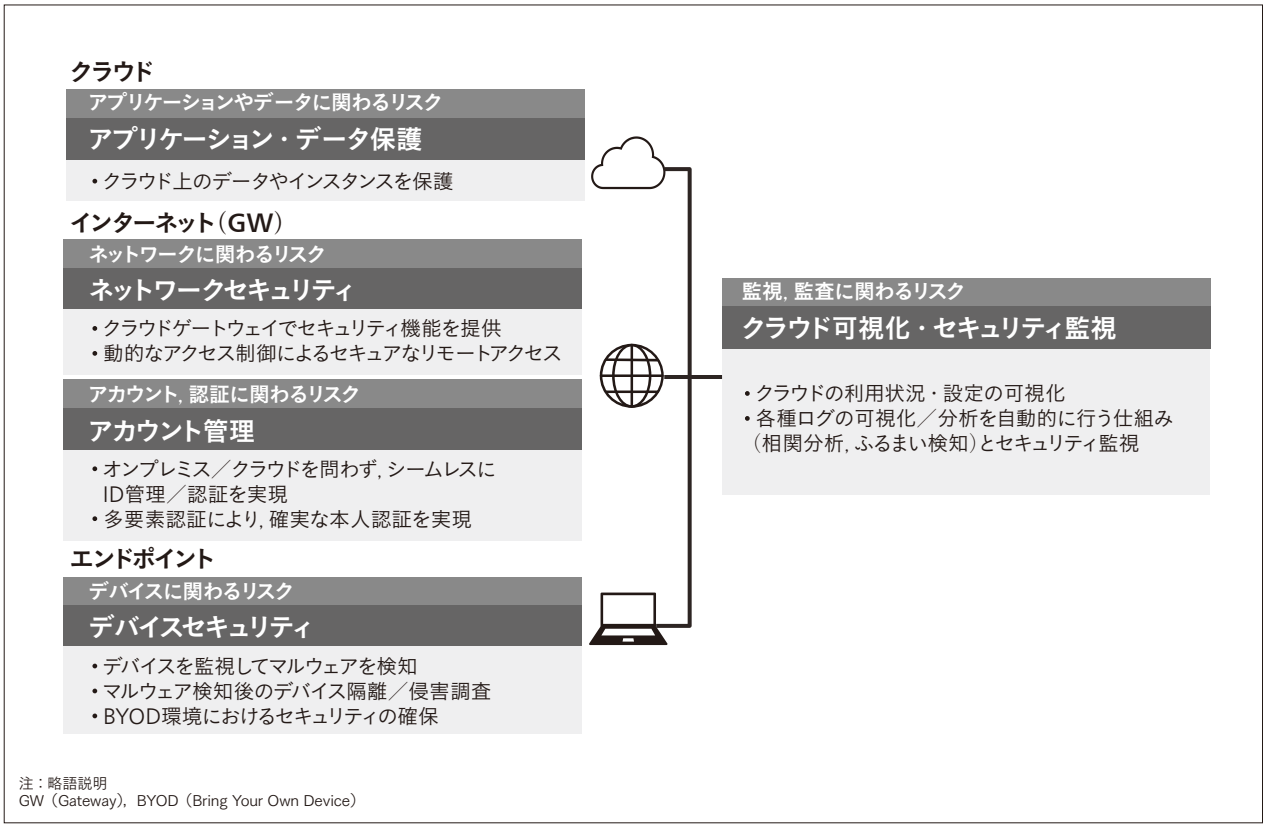
また，クラウド化により監視作業のアウトソーシングも普及しつつあり，専門家による高度で迅速な分析と対策が一部で実現されている。

クラウド化やネットワークのオープン化は外部からの攻撃リスクがクローズアップされやすい傾向にあるが，システム運用者と利用者の双方のセキュリティ強化においてメリットをもたらすものとして進化しつつある（**図1**参照）。

※1）Amazon Web Servicesは，Amazon.com, Inc.またはその関連会社の米国およびその他の国における登録商標または商標である。
※2）Microsoft Azureは，Microsoft Corporationまたはその関連会社の米国およびその他の国における登録商標または商標である。

図1｜ゼロトラストで適用する主な対策

ゼロトラストでは「クラウド」,「インターネット(GW)」,「エンドポイント」の各領域で対策を行い，システム全体の可視化とセキュリティ監視を行う。



注：略語説明
GW（Gateway），BYOD（Bring Your Own Device）

2. 攻撃対象の多様化による社会生活への影響

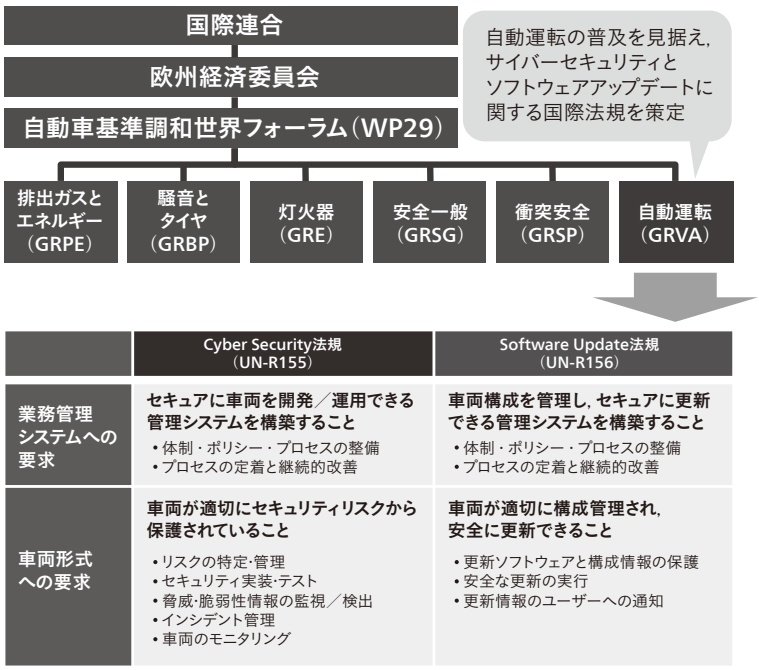
近年，サイバー攻撃が現実の社会生活にまで影響を及ぼし始めている。この点で，セキュリティを取り巻く課題の深刻さは次のステップへ進んだと言える。

これまでサイバー攻撃の代表的な手法であるランサムウェアの被害の多くは電子データに限られていたが，昨今の被害はそこにとどまらないものとなっている。実際に2021年の前半だけでも，米国ではサイバー攻撃によって石油供給が多大な影響を受けたほか，水道施設でも飲用水の成分調整システムが不正に遠隔制御されるなど，多くの問題が発生している。

こうした社会インフラを支える制御システムの多くは，従来,「特殊なシステムだから」,「クローズドシステムだから」といった理由でセキュリティ対策が積極的に行われない傾向にあった。しかし，APT（Advanced Persistent Threat：高度標的型攻撃）に代表されるターゲットを特定した特殊な攻撃の発生と，経済活動や社会生活への実害発生により，現在ではITシステムと同様の対策が必須となっている。

これらの対策として，制御システム向けのセキュリティ標準であるIEC 62443シリーズに準拠したセキュリティ対策が多くの現場で実践されている。IEC 62443シリーズは，制御システムやコンポーネント自身のセキュリティ機能だけでなく，制御システムやコンポーネント開発事業者の開発プロセス，制御システム運用事業者の管理および運用プロセスも対象としている。

また，こうした動きはIoT（Internet of Things）化するさまざまな機器に対しても同様である。例えば，自動車においては，半導体の供給問題がニュースになるほどにコンピュータによって制御される部分が増加し，それに伴いOTA（Over the Air）など無線によるソフトウェアアップデートが一般化しつつある。そのため，将来の自動運転を見据えた取り組みとしてWP29（World Forum for Harmonization of Vehicle Regulations Working Party 29：自動車基準調和世界フォーラム）の定める規則やISO/SAE21434などの規格が国際的に策定されており，プロダクトセキュリティへの対応が各自動車メーカーやサプライヤに求められている（**図2**参照）。これまで非コンピュータと見なされていたものが急速にIoTシステムの一部となることで，あらゆる機器にセキュリティ対策が求められる時代になりつつある。



注：略語説明
WP29（World Forum for Harmonization of Vehicle Regulations Working Party 29）

図2｜自動車のサイバーセキュリティ規格概要

自動車基準調和世界フォーラム（WP29）では，コネクテッド化が進む自動車のセキュリティ基準を策定している。

3. 日立のセキュリティ事業への取り組み

先に述べたとおり，現代のセキュリティにおいてはITだけでなく，OT（Operational Technology）やIoTも含めたあらゆる機器への対応が求められる。これらは一つのソリューションで実現できるものではなく，複数の対策の連携が重要となる。

日立はこの問題を解決するため，日立グループ内にグループ間事業連携の組織体を整備してグループのセキュリティソリューションを一元化し，一丸となって安心・安全を提供するよう取り組んでいる（**図3**参照）。

日立のセキュリティは，以下に挙げる三つの強みを持つ。

(1) 日立グループ約35万人のグローバルでのITインフラを守るセキュリティの知見

(2) 幅広い実業での深いドメインノウハウ（さまざまな

注：略語説明
OT（Operational Technology），IoT（Internet of Things）

図3｜日立グループ間セキュリティ事業連携の概要

日立グループのセキュリティ事業体が一体となり，事業の推進・強化を行う。

分野でのIT，OT，IoTシステム）
(3) セキュリティの根幹となる「認証」を支える独自開発の生体認証技術

高度なセキュリティは，単純にセキュリティ技術が高いだけでは実現できず，セキュリティを導入する事業やシステムに対する深い理解と，実際に運用する際の利便性や継続性を伴うことで初めて実現すると日立は考える。

そこで，日立は約35万人の従業員を支えるサイバーセキュリティ技術や，SOC(Security Operation Center)，SIRT（Security Incident Response Team)などを通じて培った知見のほか，さまざまな社会インフラ設備の構築や運用の実績を基に，顧客へ実践的なセキュリティを提供する。監視カメラや入退管理システムに代表されるフィジカルセキュリティ技術も例外ではない。顔認証や行動検知技術を用いた不審人物や物体の発見，行動阻止に関連するソリューションも組み合わせ，さまざまな脅威から多面的に顧客の資産を保護していく。また，今後は単に守るだけではなく，高度な知識と経験を有する専門家や，AI（Artificial Intelligence）によるログ解析・行動検知技術の応用によって，より効率性や安全性の高い業務の実現に役立つセキュリティソリューションを提供していく。

4. セキュリティとAIの融合によるプライバシー保護・倫理との関係

近年，セキュリティ分野でもAIが活用されており，より高度なリスク検出がサイバーセキュリティおよびフィジカルセキュリティの両面で実現しつつある。サイバーセキュリティではプログラムのふるまい型検出による未知のマルウェアの特定，フィジカルセキュリティでは顔認証や履歴の分析によるマーケティングなど，新たな経済活動への活用が可能となった。

しかし，これらの活用に際しては同時にプライバシーを中心とした倫理面での配慮が必要となる。例えば，先に述べたフィジカルセキュリティ技術においても，以前は「ただ見るだけ」であった監視カメラでAIとの融合により人物認証が可能となった結果，不審人物の発見に効果を発揮する反面，技術的には個人の行動トレースも可能となった。すでに，誤認識により無関係の人物がイベント会場から排除されるケースも確認されており，今後もセキュリティ技術とAIの融合によるさまざまな問題が生じる可能性が指摘されている。

そのため，各国でAIの倫理的な運用に向けたガイドラインなどが整備されつつあり，日立もAIが多様化，複雑化する課題に対して的確に対処することを目的として2021年2月に社会イノベーション事業における「AI倫理原則」を策定した。

個人の認証や行動などプライバシー情報の適切な取り扱いは，あらゆるシステムにおいて重要な要素となる。日立は，個人のプライバシー，利益を侵害しないシステムの実現に向けて，長年のプライバシー保護対策のノウハウとサイバー・フィジカルそれぞれのセキュリティ技術を活用し，効果的な対応を継続的に行っている。

5. おわりに

生活や仕事のあり方が大きく変わる現代において，重要性を増すセキュリティには絶え間ない進化が求められる。サイバーおよびフィジカルのセキュリティは今や攻撃を防ぐための必要経費ではなく，ゼロトラストによって実現する新しい働き方など，次世代のイノベーションを起こすためのツールとしても活用されるものへ変容している。

日立は，本特集で紹介するセキュリティ技術やソリューションを顧客に提供し，ニューノーマル・アフターコロナの時代においても安心・安全と高い利便性を提供するべく進化を続け，社会のさらなるイノベーションの実現に貢献していく。

参考文献など

1) 日立ニュースリリース，社会イノベーション事業における「AI倫理原則」を策定（2021.2），
https://www.hitachi.co.jp/New/cnews/month/2021/02/0222.html
2) 日立製作所，制御システムセキュリティの標準化動向～IEC 62443の最新状況と認証制度の紹介～（2020.2），
https://www.jpcert.or.jp/present/2020/ICSR2020_04_HITACHI.pdf

執筆者紹介

吉田 達也
日立製作所 サービス＆プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティイノベーション本部
セキュリティ事業開拓部 所属
現在，サイバーセキュリティソリューションの拡販活動に従事
CISSP

池田 芳紀
株式会社日立コンサルティング
スマート社会基盤コンサルティング第2本部 所属
現在，セキュリティ戦略策定コンサルティングに従事
情報処理安全確保支援士