URL https://journal.ntt.co.jp/article/30707
DOI https://doi.org/10.60249/24122001

ビジネスのイネーブラーとしてのセキュリティ ―後編―

セキュリティが事業の「イネーブラー」，すなわちビジネスの価値提供に不可欠なものとなっている海外事例を紹介します．１つは，SBOM（Software Bill Of Materials）により実現している高度なモビリティサービスの事例，もう１つは，セキュリティソリューションの組合せによって医療情報が利用可能となっている事例です．これらの内容と，セキュリティが実現した価値について紹介し，セキュリティが新たなビジネスと不可分なものとなっていることについて述べます．

イネーブラーとしてのセキュリティ

本誌11月号の前編では，サイバーセキュリティに関する現状をみるとともに，セキュリティの意義が，「追加負担」から事業にとって不可欠な原価へと変化し，セキュリティをより高品質なものとすることで，会社の将来の成長を守り，ひいては事業の拡大にもつながることについて述べました．本稿では，そのようなセキュリティが，イネーブラーとなっている事例についてみていきます．

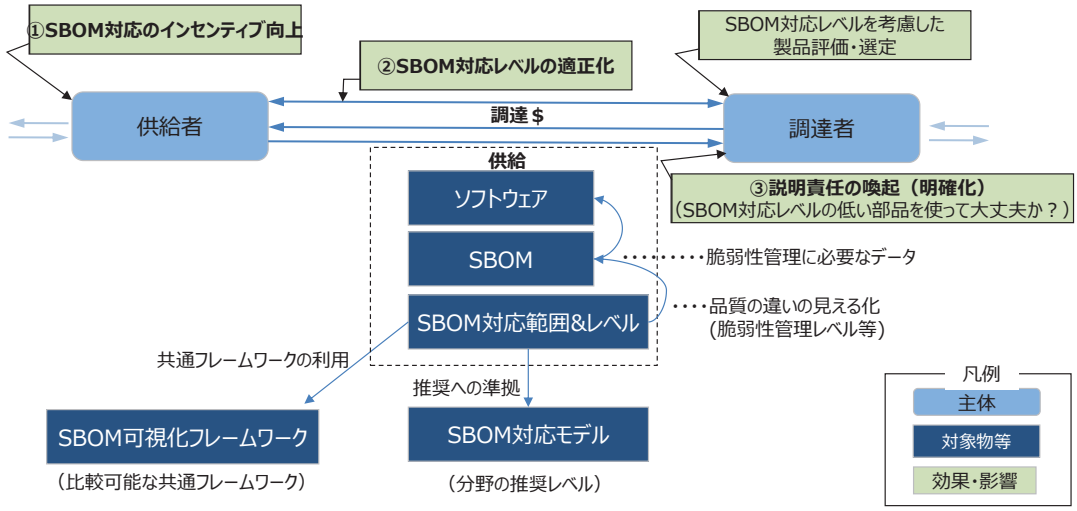
ビジネスにおけるセキュリティ機能の活用事例①：SBOMが可能にするモビリティの進化

■概要

前編では，セキュリティを車におけるシートベルトやエアバッグに例えましたが，最近では，「SDV（Software Defined Vehicle）」が注目を集めています．SDVは，直訳すると「ソフトウェアによって定義される車」という意味です．車の機能の多くがソフトウェアで制御されることから，通信機能によってソフトウェアを更新し，自動車の機能や性能を改善することができます．例えば，車がユーザに引き渡されて利用されてからであっても，後から自動運転機能を追加するといったことが可能になります．経済産業省は，SDVについて，日本車の販売目標を2030年に国内外で計1200万台，世界シェア３割とする目標を掲げています．

SDVにおいては，セキュリティが極めて重要な構成要素となります．車が遠隔操作され，車内外の人々に危害を加えるといった脅威もありますが，攻撃によってある日，車が動かなくなり，回復のために金銭を要求されるといった脅威も指摘されています．プライバシーも重要です．SDVでは膨大な量のデータが生成され，収集されます．いつどこに行くか，運転の習慣はどのようなものか，音楽などの車内エンタテインメントの利用状況といったことだけでなく，車内での会話や車内カメラの映像を収集する車もあるとされています．このような，収集されたデータの扱いには，一定の注意が払われることになるでしょう．車から得られるデータは，自動車メーカやサービスプロバイダがさまざまな改善を行ったり，運転手や乗客の体験をパーソナライズしたりするのに役立ちます．SDVのソフトウェアは，車の制御を司るだけではなく，車に関するあらゆる情報を扱うことになりますので，SDVのセキュリティは，車を安全に動かすだけでなく，車が提供するあらゆるサービス，体験の質を高める要となるのです．

SDVのセキュリティを実現するには，SDVを構成するソフトウェアが完全に把握・管理され，意図したとおりに動くものになっていることが必要です．これを実現するのが，SBOM（Software Bill Of Materials）です．これはいわばソフトウェアの「部品表」です．SDVは，実際の車と同じように，膨大な数の「部品（ソフトウェア）」で成り立っており，その中には，外部のリソースやオープンソースソフトウェアも含まれています．SDVの開発が１社だけで完結することはなく，サプライチェーン全体にわたって，さまざまな開発者や企業がかかわっています．また，開発にはさまざまなフェーズがあり，時間の経過とプロジェクトの進行に従って，ソフトウェアはアップデートされますし，追加，削除されることもあります．SBOMの活用によって，これらすべてを管理し，ソフトウェア開発のプロセス全般において，構成物（コンポーネント）と，ソフトウェア間の関係がどのようになっているかを把握することが可能になります．これはセキュリティの維持や，ライセンスの管理などの自社での管理を容易にするだけでなく，コンプライアンス対応を効率的に証明するのにも有効です．例えば，経済産業省の「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 2.0」[(1)]では，SBOM対応範囲の可視化による，SBOMの利用者（ソフトウェアの供給者と調達者）の関係と効果が示されています（**図**）．効果としては，供給側にとっても脆弱性管理レベルの高さを示すことが可能になること，SBOM 対応レベルが費用対効果の観点から適正化されること，調達者の



出典：経済産業省 商務情報政策局 サイバーセキュリティ課「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 2.0」

図　SBOM 対応モデルの利用者の関係と効果

意識の向上を促し，一般社会や取引先への説明責任の喚起につながることなどがあるとされています．このように，ソフトウェア開発における供給者，調達者それぞれがSBOMを積極的に活用により，ソフトウェアの品質を高めることが期待されています．

また，米国の「Executive Order on Improving the Nation's Cybersecurity（国家のサイバーセキュリティ改善に関する大統領令）」でも，以下のようにSBOMの活用が明記されています．

- ソフトウェアコードまたはコンポーネントに関するデータ，出所（起源）について正確かつ最新の状態を維持するとともに，ソフトウェア開発プロセスに存在する内部および第三者のソフトウェアコンポーネント，ツール，サービスに関し管理された状態を維持し，かつこれらの管理について定期的に監査を行い，実効性を確保すること．
- 購入者に対して，各製品について，直接または公開Webサイトへの掲載により，ソフトウェア部品表（SBOM）を提供すること．

この大統領令に基づき，商務省により，SBOMの最低限の要素が**表**のように定められています．各コンポーネントに関する基本情報の明確化についてだけでなく，自動化サポートや，プラクティスとプロセスにも言及されています．「プラクティスとプロセス」においては，「既知の未知」として，未知であると把握していることを明記することや，「誤りの許容」も含まれており，必ずしも最初から完全性を要求するのではなく，継続的な改善を前提としているのも特徴的です．

また，前述したように，SDVではソフトウェアを更新できることが特徴となっています．これにより機能追加や不具合の修正を行うことができるのは大きなメリットである一方，SDVが外部とのやり取りを行う際には，不正アクセスを受けてはなりません．このため，SBOMによる管理に加えて，通信の暗号化やデジタル署名などにより，ソフトウェアが正当なものであることを確実にすることも重要です．

それから，運輸業界では，車両データの活用に関して，景気変動に伴う貨物量の変化，競争の激化，経済環境の不安定化や，コストの上昇，労働力不足により，フリートマネジメント（車両管理）が一層重要になっています．車両管理を効率化するためには，貨物スペースの空き状況，搭載している貨物の量，気温，湿度など，さまざまなデータをトラックから収集し，それに基づく意思決定とオペレーションを行う必要があります．運送会社にとっては，これが効率性と収益率を高める決め手となる経営データとなりますので，このようなデータ分析と意思決定には，信頼性の高いシステムが不可欠です．このようなシステムの開発にも統合的なSBOMなどのセキュリティソリューションが活用されています[(2)]．

SDVや車両データの活用においては，一度システムをつくれば終わりではなく，急速に変化する社会や市場の環境に応じた不断の改善，アップグレードが求められます．開発者は，より迅速に新たな機能を開発し，提供しなくてはなりません．統合的なSBOMなどのセキュリティソリューションは，システム全体のセキュリティを高めるだけでなく，システム開発全体のプロセスを効率化することで，より高度な機能を迅速に市場に投入することを可能にしています．

■ビジネスへの寄与

前述のような事例からは，SDVのソフトウェアや車両データ分析のシステムとその通信のセキュリティが，車の安全性を確保するだけでなく，車の品質と信頼性を高め，運転手や顧客（荷主や配送先も含めて）

表　米国商務省電気通信情報局によるSBOMの最小要素の定義

カテゴリー名称	概要	定義
データフィールド （Data Fields）	各コンポーネントに関する基本情報を明確化すること	以下の情報をSBOMに含めること ・サプライヤー名 ・コンポーネント名 ・コンポーネントのバージョン ・その他の一意な識別子 ・依存関係 ・SBOM 作成者 ・タイムスタンプ
自動化サポート （Automation Support）	SBOMの自動生成や可読性等の自動化をサポートすること	SBOMデータは機械判読可能かつ相互運用可能なフォーマットを用いて作成され，共有されること．現状では，国際的な議論を通じて策定された，SPDX，CycloneDX，SWIDタグを用いること
プラクティスとプロセス （Practices and Processes）	SBOMの要求，生成，利用に関する運用方法を定義すること	SBOMを利活用する組織は，以下の項目に関する運用方法を定めること ・SBOMの作成頻度 ・SBOMの深さ ・既知の未知 ・SBOMの共有 ・アクセス管理 ・誤りの許容

SPDX：Software Package Data Exchange
SWID：Software Identification

出典：経済産業省 商務情報政策局 サイバーセキュリティ課「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 2.0」
※米商務省「The Minimum Elements For a Software Bill of Materials (SBOM)」を基に経済産業省が作成したもの

の体験すべてをより良いものとするのに寄与していることが理解できます．もしSBOMなどのセキュリティソリューションがなかったら，SDVの膨大かつ頻繁に入れ替わる「部品」を管理したり，競争力のある経営とオペレーションの源となるデータ活用を行うシステムの質を維持向上させたりすることはできないでしょう．もはやセキュリティをなくてもすぐには困らない，後付けで追加するオプションとみることはできません．セキュリティの存在によって初めて，SDVや経営データの活用が成り立っているといえるのではないでしょうか．

これはすなわち，このようなプロダクトやサービスの企画，開発においては，はじめからセキュリティを組み込んでおかなければ，求める品質や信頼性は実現できない，ということでもあります．これからのプロダクトやサービスの企画，開発では，初期段階からセキュリティに関する専門的な知見を加えることによる，新たな価値の創造が求められるといえるでしょう．

ビジネスにおけるセキュリティ機能の活用事例②：「データ完全性」が変える医療情報の活用

■概要

ITの社会的役割が高まるとともに，重要かつセンシティブな情報がITで処理されることも増えています．しかし，その情報が盗まれたり，改変されたり，あるいは必要なときに利用できなくなったりしたら，重大な損害が生じることから，情報は極めて慎重に扱われています．そのような情報の代表的なものの１つとして，医療情報が挙げられるでしょう．

一方で，医療に関するデータは大きな価値を持ちます．データに基づく分析は重要であり，分散しているデータを一元化し活用することで，患者本人により良い医療サービスを提供したり，社会全体で医学研究を進歩させることができる可能性があります．しかし，データの活用にあたっては，データの分散（サイロ化）が問題になっています．個人の医療情報は，医療機関，薬局，医療保険の運営者，研究機関などに分散されています．

関係者間での不適切なデータ共有は，プライバシー，セキュリティ，さらには生命倫理上のリスクを伴います．このため，データを複数の管理主体に分散し，安易な紐付けをしない（できない）ようにすることが，セキュリティ，特にプライバシーの確保に寄与していることも事実ではあるものの，そのままではデータ活用の妨げとなってしまいます．

この課題を克服し，患者に最適な医療を提供しつつ，研究やイノベーションに医療情報を活用するため，倫理とコンプライアンスへの適応も含めた新たなアプローチが提案されています．システムの個々の機能におけるセキュリティを確保するだけでなく，システムの設計にあたり，セキュリティの観点から根本的な再検討を行い，個人の医療情報を強固なセキュリティで保護するとともに，本人に医療情報の統合，同意，共有の権限を保持させる取り組みが生まれているのです．

米国のEquideum Healthは，「Data Integrity and Learning Networks：

DILNs：データ完全性と学習のネットワーク」というソリューションを提供していますが，これは，検証可能な本人確認と同意の確認，官民ハイブリッド型ブロックチェーン，分散型AI（人工知能）と，改ざんが抑止されている監査証跡により，組織を超えた安全な情報共有を実現するとしています[3]．また，このソリューションでは，個人データ用の，プライベートで，自己管理が可能なクラウドベースのストレージ（保管庫）を提供しており，これによって個人が自分の情報を完全に管理することができるようになっています．このソリューションは，Intelの機密コンピューティング技術やMicrosoftのソリューションなど，ハードウェア，ソフトウェア両方での，さまざまな技術を組み合わせて実現されています．このソリューションにより，例えば，米国の退役軍人向けのプラットフォームでは，本人が学術研究や臨床研究など，自身のデータの使用について詳細な同意を与えることを選択した場合に，報酬の受け取りを可能にするといった，新しいビジネスが出てきています[4]．

■ビジネスへの寄与

多くの人にとって，自分の医療情報を安易に他者に提供することには，大きな抵抗があるのではないでしょうか．そして，もちろん問題は個人の不安だけではありません．セキュリティに関する懸念を「気の持ちよう」として軽視してしまうと，結果として関係者の積極的な支持と行動（この事例では医療情報の共有と活用）を得ることは難しくなってしまいます．この事例でみられるように，重要かつセンシティブな情報においては，プライバシー，セキュリティ，倫理上の懸念などから，データ活用に慎重な対応が求められることがあります．このような場合でも，より高度で包括的な（エンド・ツー・エンドの）セキュリティソリューションによってデータの保護を確実にし，すべての関係者の信頼も担保することによって，これまでは困難だったデータの活用が可能になるのです．上記の事例では，このようなプラットフォームによって新たなデータの活用が可能になり，新たなデジタルビジネスが生まれ，本人を含むすべての関係者が価値と利益を享受できる可能性が生まれています．これも，セキュリティがあることによって初めて実現したサービスといえます．このようなサービスを実現させるためにも，企画，開発段階からセキュリティを前提として組み込むことが，成功のための重要な鍵の１つとなるのではないでしょうか．

まとめ：ビジネスのイネーブラーとしてのセキュリティ

11月号と今号にわたって，セキュリティに関する現状と，セキュリティがビジネスのイネーブラーとなっている動きについてみてきました．セキュリティというと，どうしても脅威の拡大と，「機密性・完全性・可用性」の確保，すなわち負の影響を防ぐことが注目されがちです．しかし，それだけでなく，セキュリティを確保することで，新たなビジネスが可能となることがあるのです．

これまで，いわゆる「インターネット」の世界では，「ベストエフォート」すなわち，できるだけのことはするが何かあっても責任は負わない，との考え方があり，ITシステムにおいても，その考え方を踏襲したものがありました．しかし，そのようなシステムでは，人命や社会の根幹にかかわるような重要でセンシティブな情報を扱うことには慎重にならざるを得ず，高いサービス品質を求められる重要なシステムでは，先進的なデジタル技術の恩恵を受けづらい，という側面もありました．しかし，ITシステムの社会的な役割が増すとともに，古い「ベストエフォート」の概念を超える安全性，信頼性を実現するセキュリティソリューションが生まれ，それによって，これまでになかった先進的なITシステム，データと価値の流れが創出されてきています．ここにおいて，セキュリティは付属品ではなく，新たなビジネスと不可分な事業の一部であり，その質を高めることが全体価値の向上にもつながります．

このようなセキュリティによる価値創出は，従来のITシステムにセキュリティソリューションを追加するだけで実現するものではありません．基となるビジネスを創出し提供する事業者，ITサービスプロバイダ，機器・ソフトウェアベンダ，法・倫理に関する専門家など，各社（者）が持つ専門知とビジネス上の優位性を組み合わせ，企画，開発の段階から，セキュリティを組み込んだ新たなエコシステムを形成する必要があります．イノベーションや新たなビジネスの実現には，これまで以上に分野を超えた「共創」が求められているといえるでしょう．

■参考文献

(1) 経済産業省 商務情報政策局 サイバーセキュリティ課：“ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 2.0，” 2024.8.
(2) https://documents.vicone.com/partner-story/primax-partner-story.pdf
(3) https://equideum.health/solutions/
(4) https://www.intel.com/content/www/us/en/customer-spotlight/stories/equideum-health-customer-story.html

※ (2)～(4)のサイト情報は，執筆時点（2024年10月）で得られたものに基づきます．

株式会社 情報通信総合研究所
左高大平