4 ブロックチェーン技術のセキュリティ応用

「誰が見ても同じ」を実現するブロックチェーン型セキュリティ情報流通フレームワーク

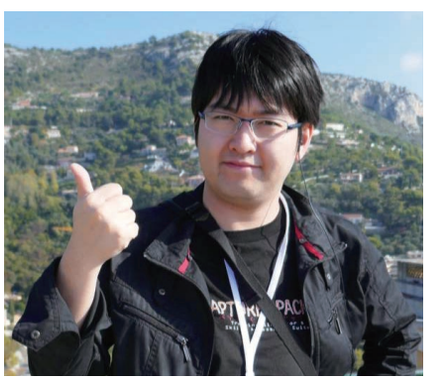
イノベーションセンター　テクノロジー部門　プロジェクトリーダー　**西野 卓也**

セキュリティ対策ではサイバーリスク情報のライフサイクルマネジメントが重要だが、現場のコスト意識をその運用に反映できていない。ブロックチェーン型セキュリティ情報流通フレームワーク「Metemcyber」は、情報配布の活発さとコスト意識の共有により、セキュリティ体制の健全性を組織横断で評価する。

日々進化する脅威と情報資産への適切なアクセス管理

厳しいセキュリティ認証、データベースの暗号化、社員のセキュリティ研修、専門チームによるセキュリティ監視や脆弱性調査、近年ではゼロトラストやふるまい検知など、複雑化するサイバー脅威に立ち向かうため、セキュリティ管理者は様々なアプローチでセキュリティの確保を行っている。一方、実際の被害は驚くほど単純なミスが原因であることも少なくない。パッチの適用漏れやパスワードの使い回しがその代表例である。多層防御の観点では、それぞれのセキュリティ対策が漏れなく例外なく施されていることが前提となるが、その前提を担保するためにはライフサイクルマネジメントと呼ばれるアクションが必要となる。

ライフサイクルマネジメントはある種の資産管理であるといえるが、サイバーセキュリティの観点からは物理資産だけではなく、情報資産(information assets)もその対象となる。情報資産の代表的なものは顧客情報である。サイバー攻撃は多くの場合、情報資産の破壊または窃盗を目的とするため、セキュリティ対策として情報資産へのアクセスを適切に管理する必要がある。一方、「情報資産へのアクセスが適切に管理されている」ことを示す情報を、セキュリティ分野ではサイバーリスク情報（図１）と呼び、脅威や脆弱性に関する「攻撃情報」、予防や検知に関する「制御情報」、資産や損失に関する「影響情報」の３区分によって構成されている。そして、サイバーリスク情報も、セキュリティ担当者によるライフサイクルマネジメントの対象である。ただし、セキュリティ管理者と現場の担当者の間には情報の非対称性が存在し、セキュリティ管理者が不適切なリスク評価を下している場合も少なくない。その場合、セキュリティ管理者は、現場の担当者と攻撃者だけが知っている情報をインシデントの後に改めて聞くことになる。



西野 卓也

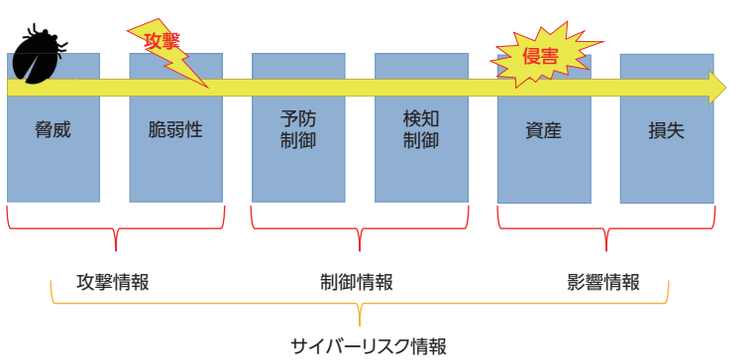


図１　サイバーリスク情報を用いたサイバー攻撃による被害の流れ

サイバーリスク情報の正しいライフサイクルマネジメント

多くの場合、セキュリティに関する

通知を現場の担当者は煩わしく思っている。影響情報に基づいて脆弱性情報やサイバー攻撃の周知を行い、その攻撃情報を受け取った現場がどれだけのコストをかけて制御情報を更新していくのか、その取捨選択がサイバーリスク情報の正しいライフサイクルマネジメントの姿である。しかし、多くのセキュリティ管理者はこのライフサイクルマネジメントの運用に無頓着である。当然、表計算ソフトで対策状況を集計させる運用はすぐに破綻する。それはライフサイクルマネジメントの状態同期コストが高すぎるからだ。また、現場で実際に消費されるコストは非常に重要な指標となる。パスワードの変更コストが極端に低い担当者がいた場合、パスワードマネージャがなければパスワードの使い回しを疑う必要があるだろう。社外もまた、関連会社やサードパーティに対するサイバー攻撃が連鎖的な被害を生みだす可能性は高い。これらを踏まえると、大きく分けて3つの課題が浮かび上がる。

①「ライフサイクルマネジメントの状態が、現場とセキュリティ管理者で同様に見えるか」
②「その情報を更新するコストはどれくらいか」
③「コストの高さは関連会社で共通した問題なのか、その現場だけの問題なのか」

ブロックチェーン型セキュリティ情報流通フレームワーク「Metemcyber」

上記の課題における第1の要件は、データベースの所在である。単一の場所での運用もしくは、複数の場所での分散が考えられる。セキュリティのインシデントは関連会社間の訴訟問題に発展する恐れがあり、参加者の間でデータを持ち合う分散モデルが適切である。第2の要件は、定量的なコストの評価だ。評価基準が普段の作業ならば、現場の担当者が見積もるべきだろう。第3の要件は、ライフサイクルマネジメントの状態や発生するコストを透過的に共有することだ。これらの要件から生まれたものがMetemcyber（図2）である。Metemcyberでは、参加者間で利害関係が発生してもデータベースの単一性を期待できるブロックチェーン型アーキテクチャを採用した。また、暗号通貨とスマートコントラクトの機能を使えば、現場の担当者が定量的なコストを情報配布の販売価格としてセキュリティ関係者等の関係者へ表現できることが分かった。情報配布の活発さと情報更新のコストを参加者に対してチェーン上で透過的に共有する仕組みにより、組織のセキュリティ健全性を比較し、現場の負担を抑えたベストなセキュリティ対策を模索することができる。

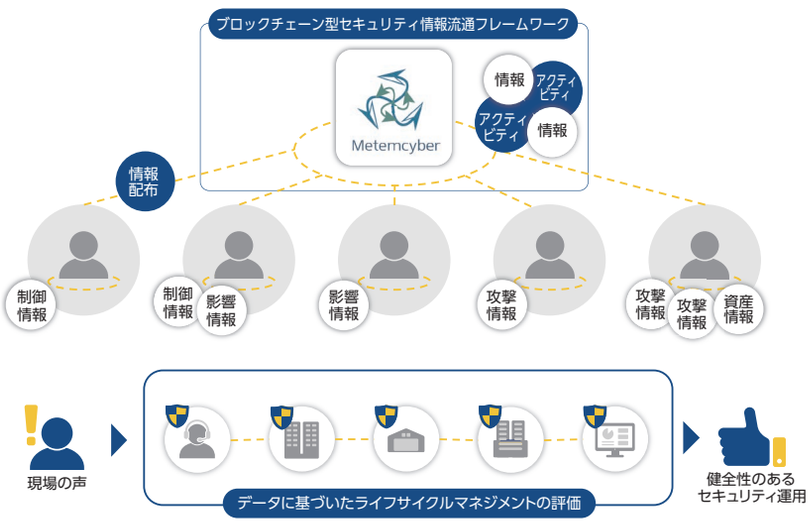


図2　ブロックチェーン型セキュリティ情報流通フレームワーク「Metemcyber」

Metemcyberの適用例の1つはサプライチェーンのセキュリティ健全性の評価だ。「サービス担当者＋セキュリティ管理者＋関連会社」の組み合わせを例に考える。「全端末のパスワード変更」タスクをサービス担当者が10ptsのコストと見積もった場合、そのタスクの結果はセキュリティ管理者へ10ptsで販売される。つまり、セキュリティ管理者の所持ポイントが100ptsならば、そのタスクをサービス担当者に依頼できる回数は10回が限度となる。セキュリティ管理者は、サービス担当者とのセキュリティ意識の差を販売価格から確認し、情報配布の活発さを他社と比較することで、自社のセキュリティ健全性の多面的な評価が可能だ。

2020年11月現在、Metemcyberは情報流通のメカニズムとセキュリティ健全性評価の検証のため、専門家を交えた実証実験を開始した。影響情報は取り扱いがセンシティブであるため、サイバー脅威情報の共有によって効果測定を行っている。活発なフィードバックサイクルが情報の質を向上させ、効果的なセキュリティ対策を促すことに繋がるだろう。