Vol.2022-DPS-190 No.30
Vol.2022-CSEC-96 No.30
2022/3/11

業務継続性のためのセキュリティデジタルツインの提案

田村　悠[1]　辻　大輔[1]　Doenhoff, Jens[1]　磯部　義明[1]　重本　倫宏[1]　川口　信隆[1]
仲小路　博史[1]

概要：近年，サイバー攻撃による脅威はますます増大している．特に，今まではインターネットから隔離されているから安全とされてきた制御システムへの攻撃による社会インフラへの影響は甚大である．また，デジタルツインやそれを用いたCPSの実現，コネクテッドカーなど，制御システムは徐々にサイバー空間と近接してきており，制御システムに対するセキュリティ対策は急務である．しかし，制御システムに対する脆弱性対応は，その対応が制御システム全体に対してどのような影響を及ぼすか不明であること，またその評価に時間とコストがかかる事を理由に，現場や運用者が消極的なことが多い．本研究では，脆弱性診断及び対策立案の際に，その対策適用によるシステム全体の可用性・業務継続性を評価することで，可用性が重要視される制御システムにおいてもセキュリティ対策の自動適用を実現する「セキュリティデジタルツイン」を提案する．本手法により，対策立案にかかる時間およびコストを削減し，迅速に対策の自動適用ができることを確認した．

”Security Digital Twin(SDT)” for ensuring security and business continuity of Cyber Physical System(CPS)

Yu Tamura[1]　Daisuke Tsuji[1]　Jens Doenhoff[1]　Yoshiaki Isobe[1]　Tomohiro Shigemoto[1]
Nobutaka Kawaguchi[1]　Hirohumi Nakakoji[1]

1. はじめに

近年，サイバー攻撃による脅威はますます増大している [1]．また，昨今ではサイバー攻撃の脅威に晒される対象が，コンピュータやサーバといった情報機器だけでなく，工場やプラントなどの制御機器及びシステムにまで拡大している．これらの機器類は従来，物理的又は論理的に外部と分離独立しているため安全とされていた．しかし，2010年9月にイランの原子力発電所で発生したStuxnetによるサイバー攻撃 [2]，2021年5月にアメリカの石油パイプラインで発生したランサムウェアによるサイバー攻撃 [1] など，制御システムも情報システムと同様に適切なセキュリティ対策を講じる必要性が高まっている．

また，今日ではデジタルツインを用いたCPS(Cyber Physical System)の実現も進んでいる．これは，IoT(Internet of Things)技術の進歩や，5G(第5世代移動通信システム)の実用化による，多数のセンサが同時にデータを収集し，それらを直接サイバー空間へ送ることができるようになった事などが理由として挙げられる．CPSの実現により，生産効率の向上や予測予防保守など，さまざまなメリットが得られるとされているが，同時に制御システムがさらにサイバー空間に近づくこととなり，より一層サイバーセキュリティの脅威に晒されることとなる．

これらに対して，システムの構成等の情報から，システムの脆弱性を発見し，対策を立案する既存技術，既存研究は [3], [4], [5] など多数存在する．また，当該技術を用いたセキュリティ支援サービス等も存在する．しかし，制御システムにおいては，セキュリティパッチの適用やファームウェアの更新，設定変更などといったシステムに対する変更について，変更対象の機器の正常な動作の担保だけでなく，その機器の挙動に影響を受ける他の機器やシステム全体，しいては業務継続性に対して負の影響を及ぼさないこ

[1] (株) 日立製作所
Hitachi Ltd.

とが強く求められる．これは，情報機器と異なり物理的に動く部分などを持つため，問題発生時に機器や，その機器の周囲にいる人間に対して影響が出る可能性があること，また，情報システムと異なりテスト環境や冗長性の担保のための副系を構築・維持するコストが膨大で現実的でない事などがある．これは，たとえサイバー攻撃への対策であっても同様であり，そのため，現状制御システムにおいては，迅速なセキュリティ対策の適用ができないことが多い．

本研究では，セキュリティ対策の立案時に，その対策を適用した際に，システムの可用性及び業務の継続性にどのような影響が発生するかを可視化することで，業務継続性を担保したセキュリティ対策の提案が可能となるセキュリティデジタルツインを提案する．本手法により，脆弱性の公開から，業務継続性を踏まえたセキュリティ対策の立案までを迅速に行うことが可能となり，また，業務継続性への影響が許容範囲に収まる場合は，対策の自動適用も可能となる．

以下，まず 3 章で既存研究について述べる．次に 4 章で，既存研究を制御システムに適用する上での問題点を述べる．次に，5 章で提案手法について述べる．最後に 6 章でまとめと今後の課題を述べる．

2. デジタルツインと CPS

2.1 デジタルツイン

デジタルツインとは，Grieves ら [6] が PLM(Product Lifecycle Management) として提唱したコンセプトを起源とした，実世界の仮想空間での表現方法，及びそのコンセプトである．（デジタルツインの定義）の中で，デジタルツインとは「潜在的または実際の物理的な製品を，ミクロの原子レベルからマクロの幾何学レベルまでを完全に記述する一連の仮想的な情報構造体」であると定義している．前記の定義に基づくデジタルツインによると「製造された物理的な製品を検査することで得られるあらゆる情報」を得られると述べている．

デジタルツインは，当初 PLM として提唱したものであるため，当初製造分野から注目されている概念である．特に欧州（ドイツ）においては，Industrie4.0 における「スマートファクトリーの実現」のコア技術とされている．しかし，今日では，IoT 分野の技術の発展と，多数のセンサを低遅延・同時接続可能とした 5G の実用化により，製造業に限らずさまざまな分野で DX(デジタルトランスフォーメーション) を実現するための技術の一つとして名前が挙がるようになった．

デジタルツインの当初の定義は前述した通りだが，PLM 以外も含めた多分野を包括する定義は現存せず，現在その定義は曖昧である [7]．本論においては，Draft 版ではあるが，多分野での適用を想定した NIST[7] で述べられた「デジタルツインとは，物理的または知覚的な実世界のエンティティ，コンセプト，または概念を電子的に表現（デジタル表現）したものである」という定義を用いるものとする．

2.2 CPS(Cyber Physical System)

CPS とは，実世界（フィジカル空間）にある多様なデータをセンサ等で収集し，サイバー空間で分析，知識化を行い，そこで創出した情報や価値を現実世界にフィードバックすることによって社会問題を解決するという仕組み，及びそれを実現する技術である．本論では，CPS の各ステップを以下のように標記する．

(1) 収集：実世界にある多様なデータをセンサ等で収集する
(2) 蓄積：実世界から収集されたデータをサイバー空間に蓄積する
(3) 分析：蓄積されたデータを分析し，新たな情報や価値を生成する
(4) 活用：分析の結果を元に実世界にフィードバックする

収集は，各種センサ技術や IoT，5G によって収集できるデータの量や範囲を拡大している．

蓄積については，クラウドコンピューティング技術の発展と，5G 通信技術による低遅延・多数同時接続性により，大規模なデータを高速かつ安価に蓄積することが可能となった．

そして，分析技術はビックデータ解析や AI を用いた分析技術などより，収集したデータから目的の事柄に関する分析や解析を行うことが可能となってきている．

デジタルツイン技術は，CPS における収集・蓄積・分析の技術の集大成ともいえる．

デジタルツイン技術を用いた CPS の例としては，ゼネラル・エレクトリック社の風力発電インフラへの CPS 活用 [8] が挙げられる．風量発電インフラにおいては，風力発電用部品の消耗度は設置場所により大きく異なることや，発電機の設置場所が洋上等の容易にアクセスできない場所であることが多いことなどから，メンテナンスに大きな課題があった．そのため，従来は過去の実地経験から割り出されたデータを元に発電機の向きを設定したり，保守タイミングを設定していた．本技術では．風力発電の発電機に多数のセンサ等を設置し，デジタルツインで再現・分析することにより，風車部品の寿命・劣化予測による予測保守と，風向きに合わせた発電量の最大化を実現した．これにより，継続利用できる部品は継続利用し，逆に摩耗が早い部品は早めに交換することで，保守コストの削減と故障によるダウンタイムの削減を実現し，さらに発電量の最大化による利益の最大化を図ることに成功した．

3. 既存研究

本章では，システムの構成等の情報から，システムの脆弱性を発見し，対策を立案する既存研究・技術について述

べる．なお，本章で単に「システム」と呼称する場合は，複数の機器から構築され，ネットワーク等によって接続された機器群全体を指す．

Phillips ら [3] らが最初に提唱した Attack Graph は，ネットワークによって接続されたシステム群に対するサイバー攻撃において，攻撃可能な経路をすべて表示した有向非環状グラフである．Attack Graph はノードがネットワークのノード，攻撃の事前条件，事後条件等を示し，エッジが攻撃を可能にする条件を持つことを示す形で書かれることが多い．Attack Graph はネットワークを介した攻撃のプロセスを記述する能力が高く，多くのセキュリティリスク評価等の研究で用いられる．但し，Attack Graph はあくまで攻撃パスの体系的な記述法，及び machine-readable な形を定義しているにすぎず，後述の手法等を用いない場合は通常，人間が手作業で Attack Graph を作成することとなる．

Attack Graph をシステムの情報等から生成する研究は多数行われている．そのうちの一つが，Ou ら [4] が提唱した MulVAL である．これはシステムの構成や脆弱性情報をベースにネットワークに接続されたシステム全体の攻撃経路と攻撃手法を Attack Graph として生成する研究である．この研究では，システムの構成や脆弱性の有無を Datalog で記述し，提案されたアプリケーションで解析をすることにより，当該システムの Attack Graph が生成され，攻撃の可否やその経路，悪用される可能性のある脆弱性を可視化することを可能としている．また，この研究では同時に，OVAL(Open Vulnerability and Assessment Language) の形式で取得されたシステムの情報を読み込み，Datalog 形式に変換することも行っており，これにより，数千台規模のマシンで構成されたネットワークでも数秒で攻撃経路が解析可能であると述べている．

Hadar ら [5] はデジタルツインを用いて収集したシステムの情報に基づき，脆弱性と攻撃手法を関連付け，最終的にいくつかの制約条件の下でリスクを迅速に低減させるための対策適用の優先順位を提示する手法を提案している．この研究においては，デジタルツインを用いて現に稼働しているシステムから情報を収集する．収集した情報から ISO/IEC 27001[9] や NIST SP800-53(Rev.4)[10] 等で定義されている Security Control(SC) をベースとした Security Controls' Requirements(SCRs) を検出する．次に検出した情報を元に，攻撃パスを Attack Graph を用いて算出する．算出された攻撃パスを元に，SC の導入，つまりセキュリティ対策の適用がどのくらい攻撃リスクを軽減するか算出する．これにより，システムの規模によっては数千とある SC をリスク低減度合いで並べ替え，どの SC まで適用すれば何%リスクを削減することができるか算出することに成功した．これにより，定量的なリスク低減度に基づいたセキュリティ対策の優先付けが可能となり，効率的なセキュリティ対策の提案が可能となった．

4. 既存研究の制御システム適用における問題点

前述した研究を始めとした各種既存研究は，主に攻撃経路の推論とリスク評価，及びその対策立案を主としている．これは，システムにおけるセキュリティリスクを分析する場合には，セキュリティに関する専門的知識を持つ専門家が必要だが，すべての組織がセキュリティの専門家を抱えることは現実的に不可能であるという理由がある．

そのため，前述のようなさまざまな研究手法によって，専門家がいなくてもセキュリティ分析が可能な技術が提案されてきた．

さらに，Hadar ら [5] の研究は，対策の立案をした上でその対策が減らすリスクと，どこまで対策を適用すればどの程度リスクが下がるかを定量的に示したことにより，多数の対策の中から効率的に優先度の高い対策の適用を促すことに成功し，セキュリティ対策を従来より容易なものとした．

しかし，本研究においてターゲットとした制御システムにおいては，前述の研究では未解決の問題がある．それは，制御システムにおける対策コストの高さと，対策実施にかかる時間の長さの大きく二つである．

4.1 制御システムにおける対策コストの高さ

制御システムにおいては，対策実施に当って行う必要のあるテストにおいて莫大なコストがかかり，場合によってはそれはリスクを大幅に上回る可能性がある．

制御システムは，IT システムと比較して，同じ脆弱性に対する対策適用でも制御システムの方が対策コストが高くなる傾向がある．

制御システムは，工場やプラント，発電所などさまざまなところで用いられているが，いずれも業務用として用いられるため，可用性の要求は一般的なパーソナルコンピューターよりも高い．そのため，セキュリティ対策の適用といったイレギュラーな操作を行う場合，それが機器本体，システム，及び業務にどのような影響を及ぼすかをテストし，業務継続性に支障がでないか確認する必要がある．機器やその用途によっては，ロジックの変更により 0.5 秒の処理遅延が発生するようになった，というだけで問題になることもあり，テストの重要性は一般的なコンピュータよりも高いと言える．但し，可用性の要求が高いのは，IT においてもエンタープライズ向けの機器やサービスも同様である．

しかし，IT システムとの大きな差は，通常は非稼働のバックアップシステムやテスト環境の構築・維持に莫大なコストがかかり，通常それは受入不可能なレベルであることである．制御システムにおいてバックアップシステムを

保持するということは，単純に検討すれば，工場であれば，普段は使わない工場をもう一棟持つことを意味し，それはITシステムにおける「同一構成をもう一つ持つ」以上に導入コストは莫大である．また，仮にその膨大な導入コストを受け入れた場合でも，運用コストも例えば以下のようなものが考えられる．

- 機器の維持費：制御システム，特に物理的に可動する部分を持つ機器は，定期的に動かし，メンテナンスを行わないと使用不能となる．
- 土地・建物の維持費：同じ工場をもう一つ持つこととなるため，土地・建物に係る様々な維持費・税金等が発生する．
- 上記の管理人員コスト：上記を管理するための人員を雇用する人件費等のコストが発生する

こういった理由で，バックアップシステムや実環境と同じ構成のテスト環境の保有には膨大なコストが発生するため，対策実施コストが高く，場合によってはそれはセキュリティリスクに見合わない場合がある．

4.2 対策に係るリードタイムの長さ

コストの高さは前述したとおりだが，一方でミッションクリティカルなシステムの場合，莫大なコストをかけてバックアップシステムやテスト環境を保有することがある．しかし，仮にそのコスト面の問題が解決できた場合においても，対策実施の為のテストに係る時間が長く，日々増加するセキュリティの脅威に追いつかないという問題がある．

前述したとおり，可用性が重要視される制御システムでは，セキュリティ対策と言ったイレギュラーな対応を行う場合は，それが業務継続性に支障が出ないことを多数の試験によって確認することとなる．しかし，それは物理的な機器を用いたテストであり，迅速なものとは言い難い．特に，多数の稼働パターンでの挙動を試験する場合，稼働パターンの変更や，長時間稼働時の挙動変化の観測に膨大な時間がかかる．

しかし，脆弱性やセキュリティリスクは日々増加の一途をたどっており，このような対応速度では到底脆弱性に対応しきれない．

5. セキュリティデジタルツインの提案

本提案手法である「セキュリティデジタルツイン (Security Digital Twin: SDT)」は，業務継続性を確保したセキュリティ対策を立案し適用するものである．図1は提案手法の概要を示した図である．

5.1 提案手法における目的

4章で述べた問題点を元に，本提案手法では，低コストかつ迅速に，業務継続性を確保したセキュリティ対策を立案し，自動で適用することを目的とする．

5.2 提案手法の要件

前記の目的を達成するための要件を検討し，以下の3つの要件が必要であると考えた．

(1) 実システムから，システムの構成や状態，挙動を収集できること
(2) 収集した情報を元に，業務継続性を満たすセキュリティ対策を立案する事
(3) 立案した対策を実システムに自動的に適用すること

本論では，このうち主に「収集した情報を元に，業務継続性を満たすセキュリティ対策を立案する」要件について，詳細な要件と機能を検討した．以後，この部分を「コアシステム」と呼称する

5.3 コアシステム詳細要件の検討

コアシステムに関する要件を検討し，以下の5つの要件が必要であると考えた．

(1) 実システムをサイバー空間上で再現できること
(2) サイバー攻撃や攻撃を防ぐための対策等を模擬できること
(3) 時間変化に伴うシステムの挙動の変化が任意の粒度で観測可能であること
(4) 複数の状況（攻撃，対策等）について並行して、かつ実機で行うテストより短い時間でシミュレーションが可能であること
(5) リスク削減と業務継続性を最大限確保した対策が立案されること

上記に基づき，セキュリティデジタルツインの構成を検討した．

5.4 セキュリティデジタルツインの提案概要

図1は提案手法の概要を示した図である．

本手法は，システム構成やその挙動，業務継続性を示す指標となる値などを実環境から収集し，サイバー空間上にモデル（以下，SDTモデルと呼称）を生成，SDTモデルに対してサイバー攻撃やその対策の適用等を反映した上でシステムの挙動をシミュレーションすることにより，既存研究と同様に攻撃リスクや対策適用によるリスク低減度合いを分析すると同時に，その対策がセキュリティ以外，すなわち可用性や業務継続性にどのような影響を及ぼすかを分析するものである．そして，この分析でセキュリティ対策による業務継続性への影響がない，もしくは許容できる範囲である場合，自動でシステムに対してセキュリティ対策を適用することが可能となる．これは，制御システムセキュリティにおけるCPSの自動化を実現し，既存の非ミッションクリティカルな情報システムにおけるセキュリティパッチの自動適用に類似した運用がより低リスクに可能と

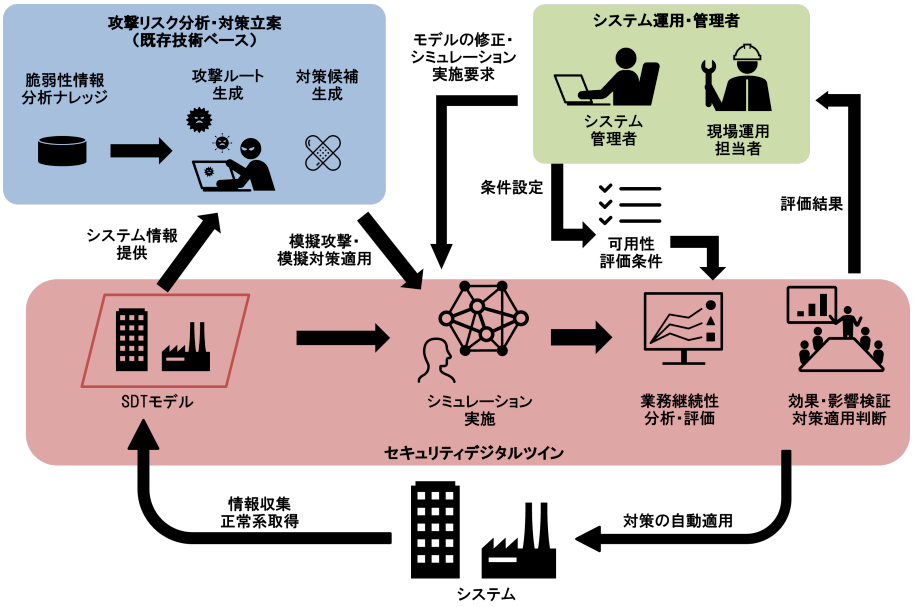

図 1 提案手法の概要
Fig. 1 Abstruct of Proposal method.

なる．

以下，SDT モデルの概要，アーキテクチャ，及びユースケースを述べる．

5.5 SDT モデルの概要

本手法でシミュレーションに用いるモデルである SDT モデルは，従来までのセキュリティ分析技術に用いられる，ある特定の時間における構成を示したモデルと異なり，システムの状態と連続した時間軸を持つ「ふるまい」を表現するモデルとして定義することで，SDT における適切なセキュリティ対策の立案と業務継続性の分析を可能とした．

従来，セキュリティリスクの分析において用いられてきた情報としては，システムの構成情報，オペレーティングシステムやそのバージョン，通信ルールなどの静的な情報が大半を占める．しかし，これらの情報はある時点でのその機器を構成する情報の一部である．

しかし，サイバー攻撃や，攻撃対策によるシステムに対する可用性や業務継続性への影響を分析する場合，現状の構成が時間を追うことによってどのような変化をし，どのような挙動をするかを知る必要がある．

そのため，SDT モデルに関して，時間オートマトンや時間ペトリネット等に代表される時間の概念を取り入れた状態遷移モデルを用いて，システムの挙動を定義している．

5.6 SDT アーキテクチャ

図 2 は SDT の主な機能の構成を図示したものである．以下，機能と該当する要件について述べる．なお，要件については，5.2 の (1)，(3) については左記の通りに，5.2 の (2) については，さらに 5.3 で述べた詳細要件を併せて

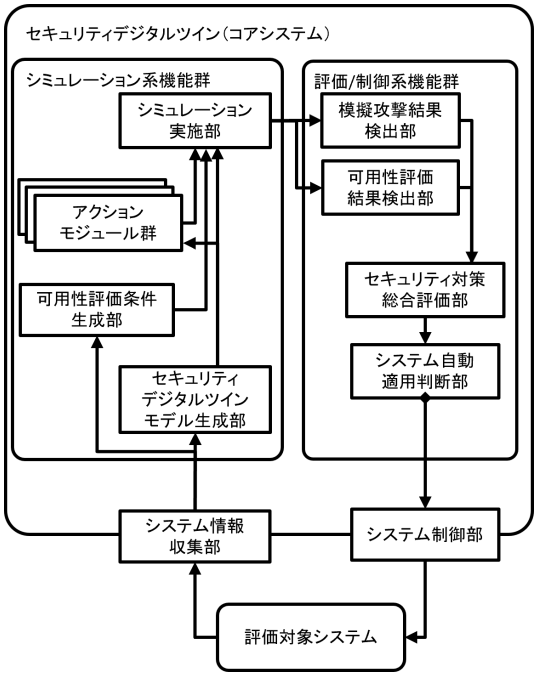

図 2 SDT の構成
Fig. 2 Architecture of SDT.

(2)-(1) といった形で記載する．複数の詳細要件に該当する場合は (2)-(1,2) といった形で記載する．

5.6.1 システム情報収集部

セキュリティ対策を実施したいシステムからシステムの情報を収集する機能 (1).

5.6.2 セキュリティデジタルツインモデル生成部

収集した情報からデジタルツインを生成した上で，シミュレーションに必要な SDT モデルを生成する機能 (2)-(1).

5.6.3 可用性評価条件生成部

業務継続性を判定する指標である，システムの可用性を評価するための，シミュレーション結果が満たすべき条件を生成する機能 (2)-(5).

5.6.4 アクションモジュール群

対象システムに対するアクション（操作）を定義し，SDT モデルに適用できる形にする機能．アクションモジュール群の例としては，既存の脆弱性評価技術をベースにした，システムへの攻撃を模擬する模擬攻撃モジュールや，対策立案モジュールなどが挙げられる (2)-(2,4,5).

5.6.5 シミュレーション実施部

SDT モデルを用いて，模擬攻撃や模擬対策適用を実施して，システムの挙動をシミュレーションする機能 (2)-(2,3,4).

5.6.6 模擬攻撃結果検出部

シミュレーション実施部のシミュレーション結果から，各シミュレーション結果における模擬攻撃や対策適用における，セキュリティ面における挙動を検出する機能 (2)-(2,3,4).

5.6.7 可用性評価結果検出部

シミュレーション実施部のシミュレーション結果から，各シミュレーション結果における模擬攻撃や対策適用における，可用性の面における挙動を検出する機能 (2)-(2,3,4).

5.6.8 セキュリティ対策総合評価部

模擬攻撃結果検出部と可用性評価結果検出部の結果を元に，セキュリティ上のリスクと業務継続性について分析・評価する機能 (2)-(3,5).

5.6.9 システム自動適用判断部

可用性評価条件とセキュリティ対策総合評価部の結果を元に，業務継続性の確保が可能な対策を立案し，条件を満たす場合にシステムに対して自動適用を行う機能 (2)-5).

5.6.10 システム制御部

システム自動適用判断部の指示により，対象システムにセキュリティ対策を適用する機能 (3).

5.7 SDT での対策適用までの流れ

SDT における，セキュリティ対策適用のステップは，以下のとおりである．

(1). 正常系モデル生成

システムに接続した SDT は，システム情報収集部から収集した情報を元に，正常状態のシステムのデジタルツインモデル及び SDT モデルを生成する．このモデル生成は定期的に行われ，常に最新の情報に更新される．

(2). 可用性評価条件生成

正常系モデルが生成された SDT で，システムの管理者は業務継続性が確保できる条件を設定する．例えば，「機器 A は 3 分以上停止しないこと」「ライン B の稼働率が 50%を下回らないこと」などといった形で設定する．

(3). システムの脆弱性のスキャン

アクションモジュール群を構成する模擬攻撃モジュールは，SDT モデルを用いて脆弱性評価を行う．実施タイミングは，ユーザが指定する，脆弱性情報が更新されたら行うなど，さまざまなトリガを設定可能なものとする．また，脆弱性が発見され，攻撃パスが通る場合，その攻撃からシステムを守る対策の候補を対策立案モジュールで対策を立案する．

このステップは基本的に既存研究の技術をベースに実現する．

(4). セキュリティ対策の業務継続性評価

前ステップでシステムへ攻撃可能な脆弱性が発見され，対策が立案された場合，当該対策について業務継続性にどのような影響が発生するか評価を実施する．この時，シミュレーション実施部では，対策適用時（複数ある場合はそれぞれ）と対策非適用時について，対策の適用動作と攻撃動作を時系列に沿って順番に行い，システムの挙動をシミュレートする．

シミュレートした結果に基づき，模擬攻撃結果検出部では，攻撃を主因としたシステムの挙動の変化を，可用性評価結果検出部では対策適用を主因としたシステムの挙動の変化を検出し，セキュリティ対策総合評価部に渡す．

セキュリティ総合評価部では，上記抽出されたシステムの挙動の変化から，以下の情報を分析する．

- 対策を適用しなかった場合，システムはどのようなリスクを負うか
- 複数の対策がある場合は，それぞれの対策によりシステムのセキュリティリスクはどの程度軽減可能か．具体的には，攻撃の難易度や，攻撃されたことによるシステムへの被害などを分析．
- 複数の対策がある場合は，それぞれの対策によりシステムの業務継続性への影響はどの程度か．対策適用により動かなくなったシステムや機能がないか．また，一時的に停止する必要のあるシステムや機能はあるか．

(5). セキュリティ対策のシステムへの適用

分析された情報はシステム自動適用判断部に送られ，システム自動適用判断部では，可用性評価条件生成部で設定された受け入れ可能な業務継続性レベルの範囲内で最大限リスクを軽減できる対策を選択し，システム制御部を経由してシステムに対して自動適用される．また，受け入れ可能な対策がない場合は，その旨をシミュレーション実施者や，自動実行の場合はシステムの管理者に通知し，シミュレーション結果を表示，対策の実施を促す．

5.8 業務継続性評価の例

SDT で行う業務継続性評価の例を以下に示す．

本節では，単純化のため，機器単体で構成されるシステムの業務継続性評価を例に述べる．

以下の 2 種類の機器（システム）を定義する．

システム A
: 可用性要件が厳しい機器で，定期メンテナンス以外での停止は短時間であっても許容されない．現在システムに脆弱性 C が存在する

システム B
: 可用性要件が比較的緩い機器で，業務時間中に起きる短時間の停止は許容される．現在システムに脆弱性 C が存在する

システム A 及びシステム B に存在する脆弱性 C は，重大な脆弱性（CVSSv3 スコアが高い）で，攻撃方法も広く知られており，直ちに悪用可能な状態であるものとする．攻撃者は，システム A 及びシステム B について，脆弱性 C をついた攻撃として以下の 2 つの攻撃シナリオがあるものとする．

攻撃シナリオ D
: 容易に悪用可能な攻撃シナリオである．攻撃対象システムの特定のポートへのアクセスが可能であれば攻撃が可能である．

攻撃シナリオ E
: 悪用が難しい攻撃シナリオである．攻撃対象システムが，標準では無効になっている特定の脆弱な設定を有効にしている場合で，攻撃対象システムと同じセグメントに攻撃者が存在する場合は攻撃が成功する

攻撃シナリオ D，攻撃シナリオ E は何れもパッチ修正が施されたアップデート（対策 F）を実施すれば脆弱性がなくなるが，当該アップデートにはシステムの再起動が必要であるとする．また，これとは別に回避策（対策 G）として，攻撃シナリオ D のみ防御可能なものがあるとする．例えば、Web Application Firewall(WAF) の設置やルール追加で，攻撃シナリオ D の特徴を持った通信をブロックするなどがある．

この時，SDT では表 1 ような評価を実施する．

表 1 において，「防御成功（シナリオ名）」は，シナリオ名に書いた攻撃シナリオについて，当該対策で防御に成功したかどうかを示しており，成功した場合は○となる．また，業務継続性影響については，当該対策適用によって業務継続性に影響が出る場合に×，出ない場合に○とした．

- システム A において，対策 F を実施することは業務継続性に影響が出ること
- システム B においては，対策 F を実施することに対する業務継続性への影響はないこと
- システム A においては，攻撃シナリオ E は防御できないものの，対策 G であれば，業務継続性を確保しつつ攻撃シナリオ D を防御可能であること

これらの結果より，「システム B では根本対策である対策 F を適用し，システム A はよりリスクの高い攻撃シナリオ D による攻撃を防ぐために対策 G を今は適用して，今後のメンテナンス時に対策 F の適用を検討する」という対応が可能となる．

表 1 業務継続性評価の例
Table 1 An Example of business continuity.

		システム A	システム B
対策 F	防御成功 (シナリオ D)[*2]	○	○
	防御成功 (シナリオ E)	○	○
	業務継続性影響[*3]	×	○
対策 G	防御成功 (シナリオ D)	○	○
	防御成功 (シナリオ E)	×	×
	業務継続性影響	○	○

[2] 記載の攻撃シナリオと対策の組み合わせにおいて，防御に成功した（○）か否（×）か
[3] 当該対策の適用によって業務継続性に影響が出た（×）か否（○）か

提案手法を用いない場合でも，ここで述べた例のように単純な構成でなおかつすべての情報が揃っている場合は，前記のような対応策を検討することは可能である．但し、現実には多数のシステムが入り混じっており，また複数の対応策があることや，その対策毎の業務継続性への影響などといった情報が揃っていないことが多い．そのため，SDT を用いて，サイバー空間上で自動的かつ迅速に上記の内容が評価されることにより，セキュリティの専門家によるアセスメントや大規模なテスト環境におけるテスト等の一部もしくはすべてを省略して，適切なセキュリティ対策が適用可能となる．

6. まとめと今後の課題

本論では，業務継続性を確保したセキュリティ対策を立案し適用する「セキュリティデジタルツイン」のコンセプトを提案した．このコンセプトでは，セキュリティ対策を行った際の挙動について，システムの状態と時間軸を持つ「ふるまい」を表現するモデルである SDT モデルを提案，これによりセキュリティ対策によるシステム全体への副反応，ひいては業務継続性への影響評価が可能になると考える．

今後の課題としては，上記コンセプトの実装及び評価が挙げられる．特に，モデルの具体的な実装及び生成方法について詳細な検討が必要である．また，モデルによる評価の精度に関する評価も必要である．

参考文献

[1] 独立行政法人情報処理推進機構 (IPA). 情報セキュリティ白書 2021 ˜進むデジタル、広がるリスク：守りの基本を見直そう. 独立行政法人情報処理推進機構 (IPA), Tokyo, 2021. OCLC: 1264648610.

[2] 独立行政法人情報処理推進機構 (IPA). 制御システム関連のサイバーインシデント事例 4 ˜Stuxnet：制御システムを標的とする初めてのマルウェア˜, March 2020.

[3] Cynthia Phillips and Laura Painton Swiler. A graph-based system for network-vulnerability analysis. In *Proceedings of the 1998 workshop on New security paradigms*, NSPW '98, pp. 71–79, New York, NY, USA, January 1998. Association for Computing Machinery.

[4] Xinming Ou, Sudhakar Govindavajhala, and Andrew W Appel. MulVAL: A Logic-based Network Security Analyzer. p. 16.

[5] Ethan Hadar, Dmitry Kravchenko, and Alexander Basovskiy. Cyber Digital Twin Simulator for Automatic Gathering and Prioritization of Security Controls ' Requirements. In *2020 IEEE 28th International Requirements Engineering Conference (RE)*, pp. 250–259, August 2020. ISSN: 2332-6441.

[6] Michael Grieves. *Origins of the Digital Twin Concept*. August 2016.

[7] Jeffrey Voas, Peter Mell, and Vartan Piroumian. Considerations for Digital Twin Technology and Emerging Standards. Technical Report NIST Internal or Interagency Report (NISTIR) 8356 (Draft), National Institute of Standards and Technology, April 2021.

[8] デジタル・ツイン：データを分析して将来を予測する | GE Reports Japan.

[9] ISO. ISO/IEC 27001:2013.

[10] Joint Task Force Transformation Initiative. Security and Privacy Controls for Federal Information Systems and Organizations. Technical Report NIST Special Publication (SP) 800-53 Rev. 4, National Institute of Standards and Technology, January 2015.