サイバー攻撃事案の教訓と社内堅牢化の取り組み

日立グループは，2017年5月にWannaCryと呼ばれるワーム型ウイルスによるサイバー攻撃を受け，社内システムが停止し社内外に影響を与えた。IoT時代を迎え，増加するサイバーセキュリティの脅威に対応すべく，情報セキュリティガバナンスを最も重要な経営課題として取り組むこととした。具体的には2017年10月からCISOを中心としたセキュリティ統括専門組織を設置し，ガバナンス／テクニカル面で社内の堅牢化を推進している。
今後はOAのIT環境だけではなく，IoT/OT系も含む製品・サービスの事業領域，開発・生産などの設備を含めたすべてに対するセキュリティリスクの低減活動を進める。

松川 公 | Matsukawa Toru
西濱 博司 | Nishihama Hiroshi
柴田 大輔 | Shibata Daisuke
川崎 明彦 | Kawasaki Akihiko
野田口 玄 | Nodaguchi Hajime

1. はじめに

日立グループでは，ラピッドサイバー攻撃のような新たな脅威に対し，情報セキュリティを最も重要な経営課題の一つと位置づけ，ガバナンス，テクニカルの両面からグループ全体のさらなる堅牢（ろう）化への取り組みを進めている。

本稿では，日立グループにおけるサイバー攻撃に対する堅牢化の取り組みについて述べる。

2. サイバー攻撃事案の振り返り

2.1 サイバー攻撃の概要

2017年5月12日，WannaCryと呼ばれるワーム型ランサムウェアが欧州から世界中に感染拡大した。本ウイルスはWindows※1)の脆（ぜい）弱性を悪用して，自分自身を他の脆弱なWindowsシステムにネットワークを経由して拡散させる。また，感染したシステムはファイルを暗号化され，その暗号解除の鍵と引き換えに金銭を要求する脅迫文が表示される。日立グループでも欧州の現地法人の検査機器から社内ネットワークのサーバなどに次々と感染し，グローバルで被害が発生した。

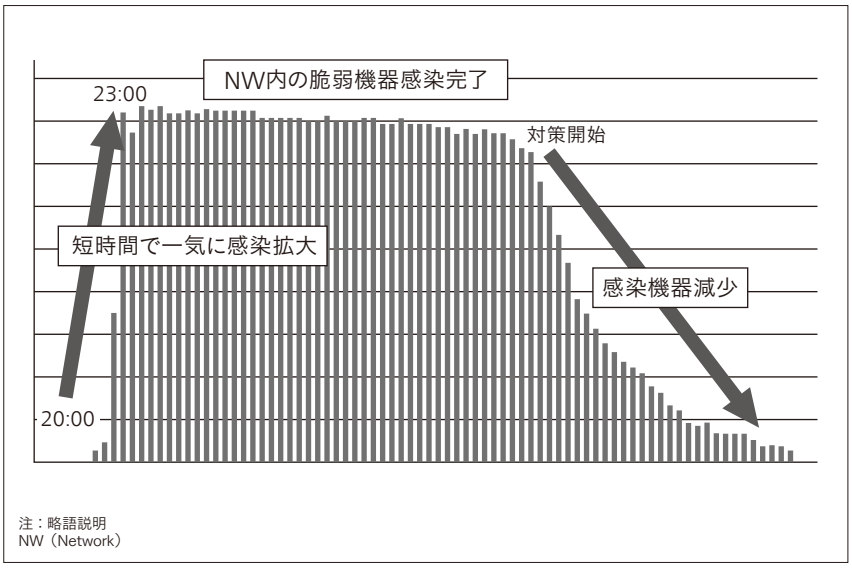
2.2 影響範囲

被害範囲は，社内ネットワークに接続されている機器である業務システムサーバ，OA（Office Automation）用PCなど情報システム部門が管理しているものから，工場にある製造・生産システム，制御や倉庫システム，

※1) Windowsは，米国Microsoft Corporationの米国およびその他の国における登録商標である。

図1｜WannaCryの感染速度

利便性を最優先したフラットネットワークの構成をとっていたため短期間で一気に感染が拡大し，脆弱性が対策されていない機器すべてが感染した。



ファシリティの入退室管理システムまで多岐にわたった。

図1は，5月12日からの社外へのファイアウォールにおけるWannaCryの拡散パケットの廃棄数を表したものである。20:00ごろに感染が始まり，3時間後の23:00にはほぼ飽和状態になり，脆弱性が対策されていない機器すべてに対しての拡散が終わっている。その後，アンチウイルスソフトによる検疫や脆弱性対策によりパケット数は減少していった。

3. サイバー攻撃事案から得た教訓

今回のサイバー攻撃事案から得た教訓は，4つある。

1つ目は，ネットワークの構成の在り方についてである。エンドポイントによるウイルス対策を前提として広域イーサネット※2) によりセグメント化を排除した社内ネットワークは，ワーム型ウイルスの攻撃に対してはエンドポイントが感染した場合，一気に拡散してしまう。また，エンドポイントのセキュリティ状況も把握できていないままネットワークに接続されていることも，ウイルス拡散の原因となった。これらを改善するためには，セキュリティ側面の強化と復旧を前提としたネットワーク監視機能を盛り込むことが重要である。

2つ目は，グローバル化により24時間稼働が必要な各サーバシステムにおいて，セキュリティ対策の不徹底が露呈したことである。ダウンタイムが許容されないことで，脆弱性があっても速やかにパッチを当てられないシステムが被害を受けた。これに対してはパッチ適用を「やらなくても大丈夫」という意識から，「やるのが当然」との意識へ変革し，企業全体で推進することが重要である。

3つ目は，IoT（Internet of Things）機器へのセキュリティ対策の困難さである。今回の事案の感染元である検査機器もそうであったが，組み込みWindowsであるにもかかわらず，パッチ適用がもともと想定されていない機器が大多数であることや，導入する側もシステムをアップデートする意識が薄いことなど，今後の対応の困難さを改めて痛感した。OA機器と異なりパッチを適用できない場合も想定し，ネットワークで防御をすることも考慮した設計が必要である。

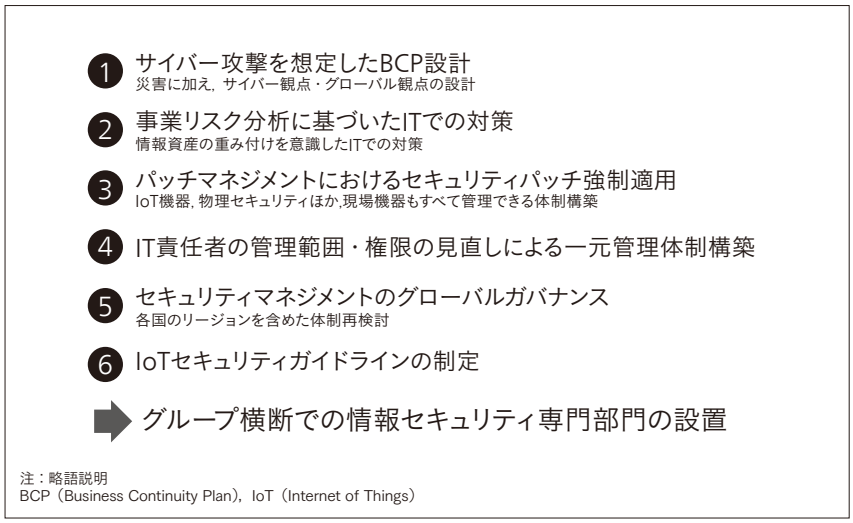
4つ目は，災害対策のIT-BCP（Business Continuity Plan）とサイバーセキュリティのIT-BCPはまったく異なることを再認識したことである。震災をはじめとする災害対策では，速やかに業務を再開することを目的として常に地理的冗長先にデータを同期していたが，暗号化されたファイルも同期してしまったことから，冗長データも破壊されたことで前日ファイルからの復元が必要になり，復旧に長時間を要してしまった。ランサムウェアを想定すると，復旧のために必要なデータバックアップの考え方も見直しが必要である。また，災害時と同様にサイバー攻撃時の事業継続計画（BCP）においても，人命確保・事業復旧を最優先に考えた行動をとる必要性がある。インシデント対応を行う際には，日頃から最悪のシナリオを考え，大規模な被害につながる可能性を常に念頭に置いて対処しなければならない。

これらを実現するためには，攻撃シナリオに沿った手順書整備，トレーニング，現場力向上が重要である。この教訓から社内の堅牢化のため，ガバナンス側面では

※2) イーサネットは，富士ゼロックス株式会社の登録商標である。

図2｜ガバナンス側面の取り組み

今回のサイバー攻撃事案を踏まえたガバナンス側面の取り組みとして，6つの要素に焦点を当て，グループ一体となった情報セキュリティ強化施策を推進している。



注：略語説明
BCP（Business Continuity Plan），IoT（Internet of Things）

図2のとおり，6つの要素に焦点を当てて推進している。これらの要素の実現のために，グループ横断での情報セキュリティ専門部門を設置し，セキュリティガバナンス体制の強化を図った。

4. セキュリティガバナンス体制の強化

IoTの進展やサイバーセキュリティ脅威の増加などから，情報セキュリティガバナンスを最も重要な経営課題の一つと位置づけ，2017年10月から日立グループ全体の情報セキュリティガバナンスを一括して推進するため，CIO（Chief Information Officer）が兼務していた情報セキュリティの責任を分離し，CISO（Chief Information Security Officer）を設置し，CISO配下に日立グループ全体のセキュリティを統括するための専門組織を設置した（**図3**参照）。

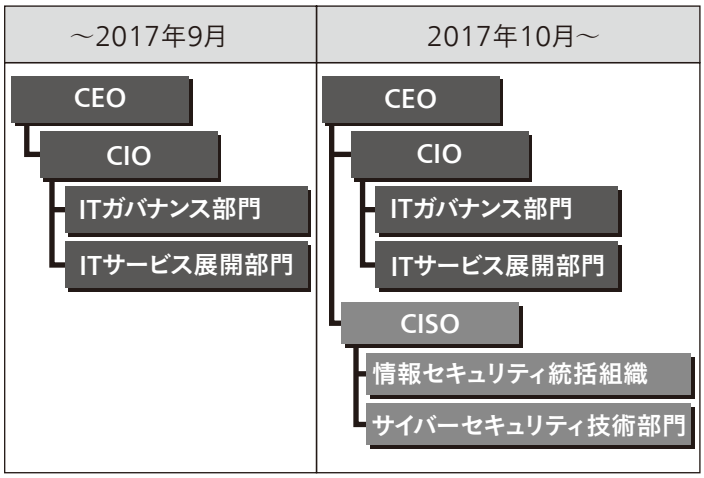
今まではCIOにセキュリティ機能を持たせていたが，IT統制の一部であったセキュリティ統制機能を明確に分離することで，セキュリティファーストに対するグループ全体のガバナンス体制を確立した。

統括組織はサイバー／情報セキュリティマネジメントの継続的実行，日立グループ全体に影響を及ぼす事案へのシステム停止判断と提言，経営インパクト，残存リスク対策の経営会議への定期的な答申および実行を役割としている。

また，専門組織内ではSOC（Security Operation Center）による24時間365日の監視，HIRT（Hitachi Incident Response Team）によるインシデント対応の強化を図っている。**図4**のように全社でサイバー攻撃に対する警報

図3｜CISOの体制と役割

サイバーセキュリティを経営課題と位置づけCISOを設置し，日立グループ全体のセキュリティを統括するための専門組織を新設した。



CISO/セキュリティ統括組織の役割

（1）サイバー／情報セキュリティマネジメントの継続的実行
（2）日立グループ全体に影響を及ぼす事案へのシステム停止判断と提言
（3）経営インパクト，残存リスク対策の日立経営会議への定期的な答申および実行

注：略語説明
CEO（Chief Executive Officer），CIO（Chief Information Officer），CISO（Chief Information Security Officer）

を定め，統一した平時のPDCA（Plan，Do，Check，Act）活動，有事の緊急対策行動が取れる体制を整備した。サイバーBCPの発動が必要となる有事の際はコーポレート全体で緊急対策本部を立ち上げ，BU（Business Unit）／グループ会社のサイバーセキュリティ部門と連携し対応を進める。各コーポレート部門は，緊急対策本部として統括組織と一体となってそれぞれ定められた対応を実施する（警察，マスコミ，省庁などへの社外対応など）。

5. テクニカル面の強化

ガバナンス体制の強化と並行し，攻撃の早期検知と迅速な対処の実現に向け，監視およびインシデント対応についてテクニカル面からの強化も進めている。WannaCryの出現以降，亜種による攻撃にも備える必要があり，強化は複数のフェーズに分けて段階的に，かつ着実に進められるよう計画した。

5.1 堅牢化フェーズ1の取り組み

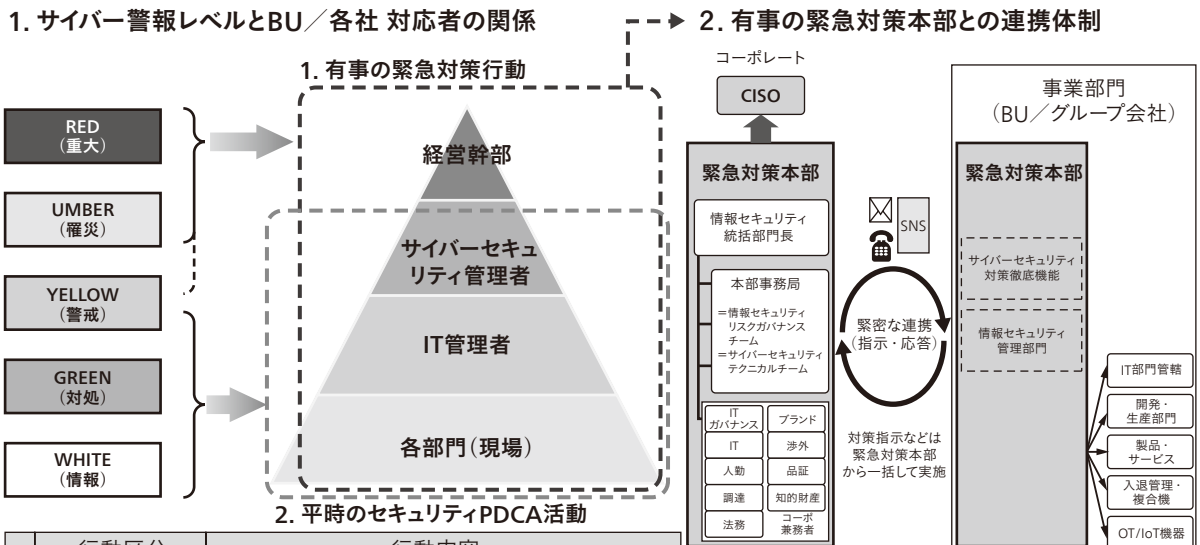
堅牢化フェーズ1では即効性のある施策を優先し，既存の運用をベースとして検知の早期化，判断と対処の迅速化に取り組んだ。

社内ネットワークや業務システムはそれぞれを担当する部署によって自律的に運用管理されてきたため，その構成や詳細について監視側で十分に把握しておらず，運用目的で取得している各種ログについては監視対象外としていた。しかしながら，フラットな構造の社内ネットワークでは監視ポイントを1つでも増やすことが早期検知につながるため，各部署管理の機器やシステムを棚卸しすることでどこに何があるのか整理し，取得可能なログを確認し検知に有用なものは新たに監視対象へと加え，検知の早期化を実現した。

また，近年は脅威の変化が激しく監視業務もそれに合わせて柔軟な対応が求められる。これまで監視側で準備していた運用手順書は確認や対策の共通項目だけを詳細化した断片的なものであったり，対応者の知見を前提と

図4｜サイバー警報と緊急対策本部の連絡体制

グローバルで脅威情報を収集し，緊急度・影響範囲を判断して脅威レベルに分けたサイバー警報を発信する。また，有事の際にはグループ一体となって連携・対応を進める体制を整備した。



	行動区分	行動内容
1	有事の緊急対策行動	・緊急対策本部設置 ・サイバーBCP計画発動（システム保全活動） ・従業員への対策指示
2	平時のセキュリティPDCA活動	・製品・サービス，開発・生産，OT/IoT機器に対するセキュリティマネジメントサイクルPDCAの実行 ・脆弱性対策 ・堅牢化計画推進（堅牢化施策の推進，残存リスク把握，事業インパクトの把握→経営幹部への報告） ・従業員へのセキュリティ向上啓発活動

サイバーBCPの発動が必要となる有事はコーポレート全体で緊急対策本部を立ち上げ，BU／各社のサイバーセキュリティ対策徹底機能と連携し対応を進める。
また各コーポレート部門は緊急対策本部にてそれぞれ定められた対応を実施する。

注：略語説明
PDCA（Plan，Do，Check，Act），BU（Business Unit），OT（Operational Technology），SNS（Social Networking Service）

した抽象的なものとなっていた。そうした知見を持った対応者がたまたま不在の際にWannaCry事案のような緊急事態が発生すると，対処までに時間を要し被害が拡大することが想定された。そこで緊急時の対応手順を見直し，一定の前提知識があれば判断と対処を迷うことなく迅速に進めることのできる手順書の整備を実施した。

また，従来は国内向けの標的型攻撃に監視の重点を置いていたことから，国内外の対応を区別して実施してきた。しかし今回のWannaCry事案は，国外で発生したインシデントが国内に重大な被害を及ぼすという事象であった。そうした深刻な経験から，これまで国内向けに実施してきた対応については国外も想定するものとし，危険度の高い事案については迅速に対応ができるよう24時間365日の受け付けと対応ができる体制を整備した。

5.2
堅牢化フェーズ2の取り組み

堅牢化フェーズ2ではセキュリティ監視の強化に取り組んだ。

まず，さらなる監視強化のため，監視基盤の拡張について検討した。従来からある社内独自の監視基盤拡張も検討したが，国内だけではなくグローバルでの監視強化を早期にかつコスト面も考慮しながら実現させる必要があった。そこで，各社のMSS（Managed Security Service）をベースに選定を行った結果，セキュリティ監視だけではなくインシデント発生時のIR（Incident Response）までサービスとして提供可能な株式会社日立システムズのMSSを採用した。

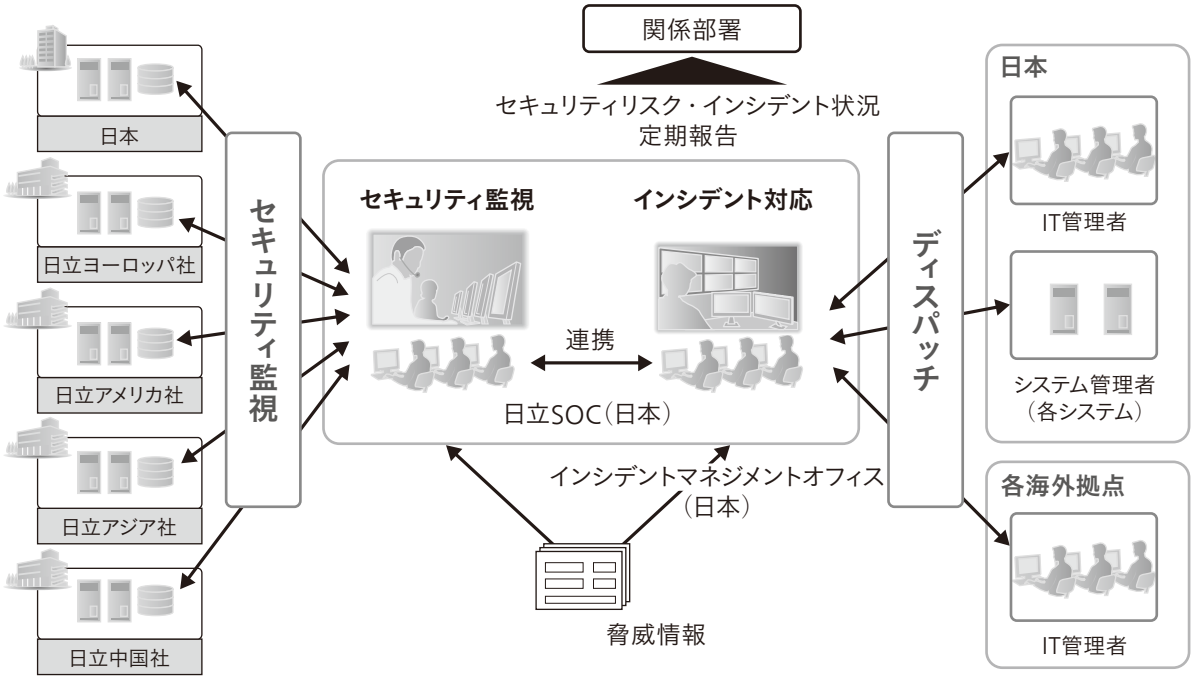
次に，グローバルでの監視強化実現に向け，対象とするシステムおよびネットワークの監視ポイントを定め，グローバルの各システムおよびネットワークデバイスのログの連携・監視を実施するための調整を進めた（**図5**参照）。監視対象拠点としては，日本，日立ヨーロッパ社はもちろん日立アメリカ社，日立アジア社，日立中国社などがある。

監視の仕組みとしては，各監視対象拠点のシステムおよびネットワークデバイスのログを，MSSの監視基盤に集約し相関分析を実施する。欧州のGDPR（General Data Protection Regulation：一般データ保護規則）のように欧州域外に個人情報を含むデータを移転することができないといった規則・法律が拠点ごとにある場合には相関分析を拠点内に限定し実施するが，ログをMSSの監視基盤に集約し分析・監視することで，日立グループへのサイバー攻撃をこれまでよりも早期に検知し，IRによる対策・復旧をより迅速に行うことが可能となる。

今後の取り組みとして，現在SOCでは24時間365日の

図5｜グローバルでのセキュリティ監視強化

日立グループのグローバルでのセキュリティ監視強化に向けて，24時間365日で国内外の社内ネットワーク監視およびインシデント対応を推進する。



注：略語説明
SOC（Security Operation Center）

監視を実施しているが，拠点ごとにIT責任者やIT管理者の運用が異なったり，24時間365日で対応していない拠点もある。また，時差によってもグローバルでの対応に遅れやずれが発生する可能性があるため，インシデント発生時の初動対応から対策までを迅速に実施し，サイバー攻撃に対する被害を最小限に抑えるために取り組んでいく。

6. おわりに

サイバー攻撃事案から教訓を得て推進する社内堅牢化は，現時点ではOAで利用するIT系が中心である。今後，IoT/OT（Operational Technology）系も含むネットワークに直接的／間接的に接続するすべての機器を対象とし，製品・サービスの事業領域，開発・生産などの社内設備を含めた国内・海外すべてに対するセキュリティリスクのマネジメント活動を拡大していく。

執筆者紹介

松川 公
日立製作所 情報セキュリティリスク統括本部
サイバーリスクマネジメント部 所属
現在，日立グループの情報セキュリティリスクマネジメント活動に従事

西濱 博司
日立製作所 情報セキュリティリスク統括本部
サイバーリスクマネジメント部 所属
現在，日立グループの情報セキュリティリスクマネジメント活動に従事

柴田 大輔
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 セキュリティ事業統括本部
サイバーセキュリティ技術本部 所属
現在，日立グループのセキュリティ監視とインシデントレスポンスに従事

川崎 明彦
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 セキュリティ事業統括本部
サイバーセキュリティ技術本部 所属
現在，日立グループのセキュリティ監視とインシデントレスポンスに従事

野田口 玄
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 セキュリティ事業統括本部
サイバーセキュリティ技術本部 所属
現在，日立グループのセキュリティ監視とインシデントレスポンスに従事