REPORT

SCADA / ICS セキュリティリスクが独自調査で明らかに

目次

概要 3

はじめに：SCADA / ICS は格好の標的 4

幅広さと深さが急速に高まる SCADA / ICS 4

SCADA / ICS セキュリティの課題. 6

SCADA と ICS に対する脅威 8

脅威が及ぼす影響 9

リスク軽減に向けた推奨事項 10

これからの道のり：今後の展望. 11

概要

近年、SCADA（監視制御 / データ収集）システムや ICS（産業用制御システム）が多くの民間企業と政府機関に使用されていますが、このようなテクノロジーは重大なセキュリティの課題に直面しています。Forrester Consulting が実施した調査によると、SCADA または ICS を使用する組織の **60% 近く**が、過去 1 年に**セキュリティ侵害を経験**しています。また、その多くは、テクノロジーパートナーなどに高レベルアクセスを許可しているため、システムはさらなるリスクにさらされていることがわかっています。また、ほとんどの組織が**従来の IT システムと SCADA / ICS を接続**していることが明らかになっています。これは、制御システムにハッカーが侵入するリスクになる可能性があります。

このようなリスクがあるにもかかわらず、オペレーターの多くは SCADA / ICS を保護する多数のセキュリティツールのメリットを活用していません。回答者のおよそ**半数**は、SCADA / ICS に **SSH（セキュアシェル）や TLS（トランスポートレイヤーセキュリティ）トラフィック暗号を導入しておらず**、ロールベースのアクセス制御を従業員に適用していないことがわかっています。

SCADA / ICS を使用する組織の多くは、GPS（全地球測位システム）、アクティブ RFID（Radio-Frequency Identification）、Wi-Fi デバイスなどのテクノロジーのホストに自社ネットワークへの接続を許可しており、これがさらなる攻撃経路となっています。また、「IT / OT のコンバージェンスが原因でセキュリティの課題が発生した」という回答は、97% にのぼります。

このように、SCADA / ICS は数々の脅威に直面していますが、セキュリティツールの追加によってシステム保護を強化することが可能です。

SCADA と ICS の違いを理解する

ICS は SCADA システムを介して管理されることが多く、
オペレーターは GUI（グラフィカルユーザーインタフェース）を使用して、
システムステータスの確認、アラートの受信、プロセス管理の調整入力などを行います。

はじめに：SCADA / ICS は格好の標的

近年、電気 / 水道事業者以外にも、多くの組織がデータ収集と機器の自動化を目的に SCADA / ICS を導入しています。事業の妨害、身代金の搾取、あるいはライバル国の重要インフラへの侵入を目的とするハッカーにとって、このようなテクノロジーは価値の高い標的です [1]。Forrester の調査によると、SCADA / ICS を使用する組織の **56%** が過去 1 年間に**セキュリティ侵害を経験**しており、セキュリティ侵害が発生していない組織はわずか 11% に留まっています。

攻撃者は、極めて大きな被害を与えることができます。2015 年 12 月、産業制御システムが攻撃を受け、ウクライナ西部のいくつかの地域で停電が発生しました [2]。このように、被害は米国外に限りません。たとえば、2016 年 3 月、北米の水道事業会社のネットワークがハッカーに侵入され、水処理に使用する有害化学物質のフローを制御する PLC（プログラマブルロジックコントローラ）が短時間乗っ取られました [3]。

ここで大きな問題となるのが、第三者による SCADA / ICS へのアクセスです。多くの組織がテクノロジーベンダーなどの外部組織のセキュリティを信頼し、社内システムへのアクセスを許可しています。Forrester の調査によれば、組織の **60%** が、パートナーや政府機関に**完全なシステムアクセスまたは高度な権限によるアクセス**を許可しています。つまり、SCADA / ICS は深刻なリスクに直面していることを意味し、セキュリティ強化には乗り越えるべき障壁がいくつか存在しているのです。

幅広さと深さが急速に高まる SCADA / ICS

SCADA / ICS 市場は、急速に成長しています。Transparency Market Research によれば、ICS のグローバル市場は 2014 年の 580 億ドルから 2021 年には 810 億ドルへと拡大し、2015 年から 2021 年の間に年平均 4.9% で成長すると予測されています [4]。ICS は、製造施設、港湾、水処理施設、石油パイプライン、エネルギー事業者、建築環境制御システムで幅広く使用されています [5]。また、ICS のグラフィカルユーザーインタフェースを提供する SCADA は、年平均 6.6% で成長しています [6]。

幸運なことに、SCADA / ICS を運用する組織は、自社がリスクに直面しているという事実を認識しています。このような企業は、システム保護を目的にさまざまなテクノロジーとセキュリティ機能を活用しています。たとえば、Forrester の調査によると、組織の **70%** がすべての**ネットワークトラフィックのログ記録と分析**を継続して行っており、24% が現在のセキュリティ分析システムの更なる拡張配備を計画しています。およそ **3 分の 2** の組織が何らかの**ネットワークセキュリティ制御**を使用しており、**62%** は、指紋や顔認識といった**生体認証によるセキュリティ制御**を使用しています。

ICS 市場は、急速に成長しつつあり、
2021 年までに
810 億ドル
に成長すると予測されています。
攻撃対象領域は、毎年拡大を続けています。

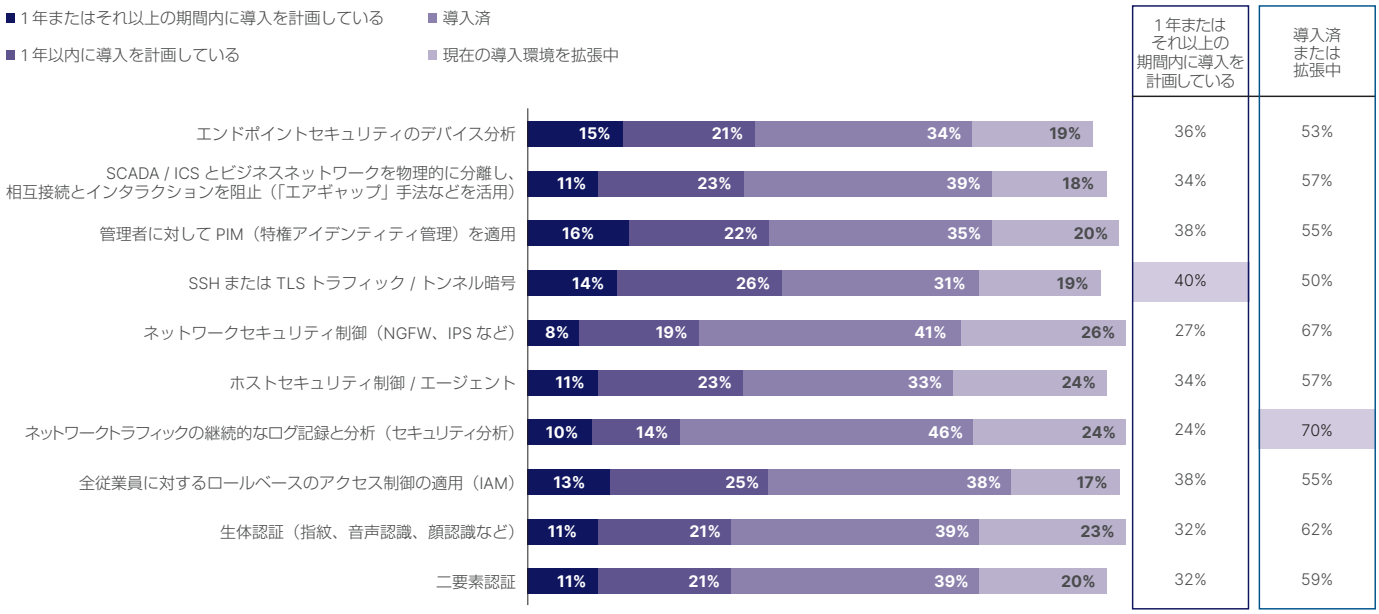
SCADA 市場は前年比 6.6% で成長を続けており、
2022 年までに
134 億千万ドル
に成長すると予測されています。

それにもかかわらず、SCADA / ICS の保護に役立つ他のセキュリティテクノロジーは多くの組織で導入が進んでいません。SSH またはTLS トラフィック暗号を導入していない回答者は半数にのぼります。ただし、その半分以上が1年以内の導入を計画しています。

さらに、管理者に対して PIM（特権アイデンティティ管理）を適用していない組織は **45%** を占めます。PIM は、IT 環境で高い権限を持つアカウントを監視する機能です。そして、**45%** は従業員に対してロールベースのアクセス制御を使用していません。ただし、「このようなテクノロジーを導入する予定はない」と回答した組織はわずかです。

さまざまな SCADA / ICS のセキュリティ保護対策に取り組む多くの組織

設問 1：SCADA / ICS のセキュリティ保護を目的に、導入を計画している対策をお選びください。



対象：重要なインフラストラクチャ、IP レベルの保護、IoT、SCADA のセキュリティを担当する、グローバル組織の意思決定者 429 人
出典：Forrester Consulting がフォーティネットの依頼で実施した調査結果

図 1：SCADA / ICS を運用するほとんどの組織は、ネットワークトラフィックのログ記録と分析を継続的に実行していますが、エンドポイントセキュリティを目的としたデバイス分析を導入している組織は半数超に留まっています。

SCADA / ICS を運用する多くの組織が、基本的なセキュリティツールを無視しています。

45% は、ロールベースのアクセス制御を使用していません。

このため、内部者の脅威に対して脆弱な状態になります。

SCADA / ICS セキュリティの課題

SCADA / ICS テクノロジーを使用する組織は、そのようなシステムのベンダーがクラウドを使用することに対して懸念を持っていると思われます。特に、従業員が私的にテクノロジーやクラウドを使って SCADA / ICS に接続することに対して、不安を感じています。

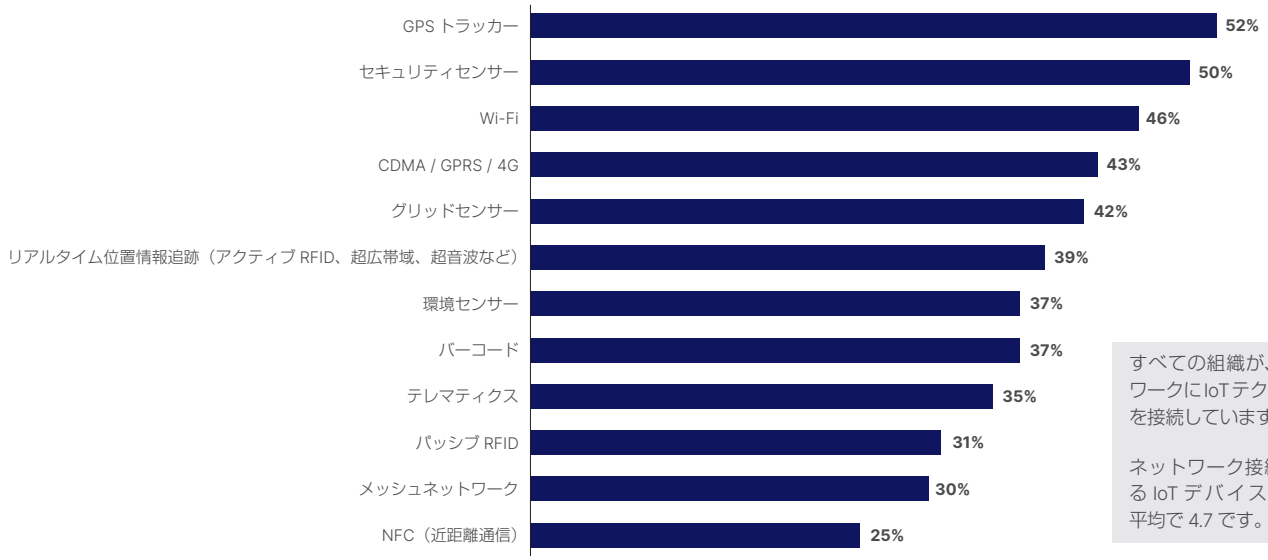
このような行動は、組織が既に抱えているセキュリティリスクをさらに深刻化すると考えられています。現在、実に多くの**無線デバイスや IoT（モノのインターネット）デバイスがネットワークに接続**されており、脆弱性が高まっています。Forrester の調査では、すべての回答者が IoT または無線テクノロジーを使用してネットワークに接続しており、これには SCADA / ICS も含まれます。これに伴うリスクの存在は明らかであり、接続されているテクノロジーの数は平均で 4.7 となっています。

Wi-Fi も大きな問題の 1 つです。**40%** 以上の組織が Wi-Fi デバイス、モバイルデバイス、グリッドセンサーを接続しています。SCADA と ICS を稼働するハードウェアとソフトウェアで構成される OT と IT のコンバージェンスを推進する組織では、このような接続が増加すると、管理が複雑になります。また、IT と OT を基本的な機能で接続している組織が **75% 近く**を占めていることを考えれば、悪意のある脅威への対策はまったく十分とは言えません。

IT / OT のコンバージェンスに関する懸念は、多岐にわたります。およそ **40%** の組織が、自社またはセキュリティパートナーには IT / OT の保護に必要な専門知識が欠けていると感じています。また、**39%** が機密性の高いデータの流出に対する不安を抱えており、**3 分の 1** が接続デバイスのバックドア攻撃を憂慮しています。また、SCADA / ICS を運用する組織にとって、テクノロジーパートナーなどに高レベルアクセスを許可していることも、懸念材料の 1 つになっています。このような権限は、ハッカーの攻撃経路になることがその理由です。

ネットワークに接続されている IoT テクノロジー

設問 2：次の IoT（モノのインターネット）テクノロジーのうち、組織のネットワークに現在接続されているものはどれですか。（該当項目をすべて選択）



すべての組織が、ネットワークに IoT テクノロジーを接続しています。

ネットワーク接続している IoT デバイスの数は、平均で 4.7 です。

対象：重要なインフラストラクチャ、IP レベルの保護、IoT、SCADA のセキュリティを担当する、グローバル組織の意思決定者 429 人
出典：Forrester Consulting がフォーティネットの依頼で実施した調査結果

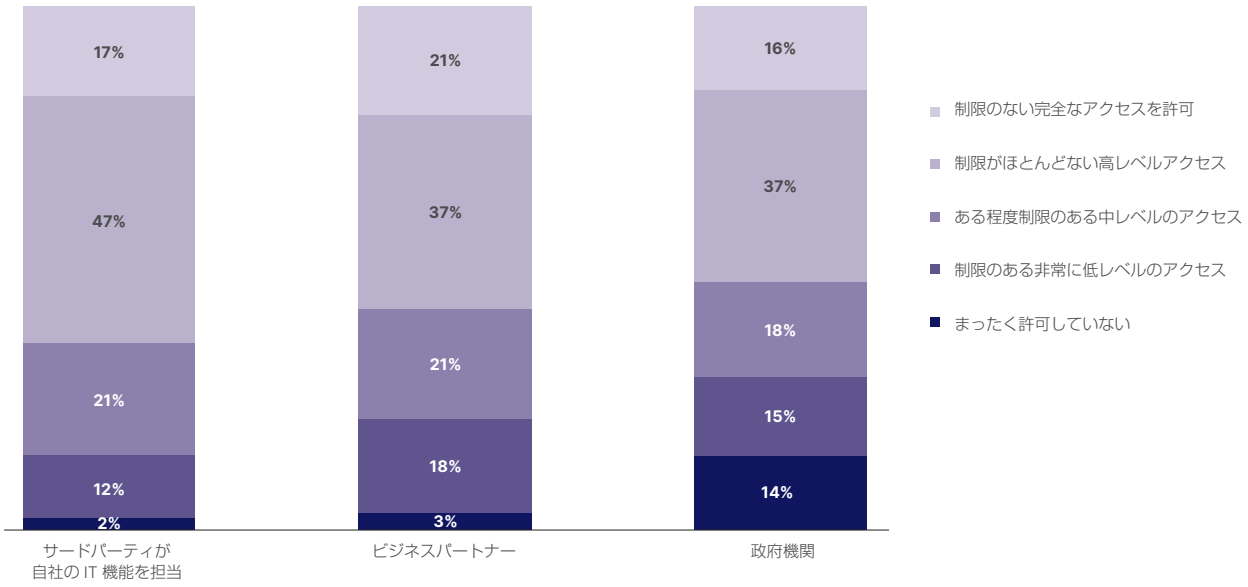
図 2：ほとんどの SCADA / ICS ユーザーは、ネットワークに他のテクノロジーを数多く接続しています。

たとえば、組織の **64%** が、サードパーティ IT ベンダーに SCADA / ICS に対する完全なシステムアクセスまたは高度な権限によるアクセスを許可しています。問題は、直接的な関係から生じるわけではありません。このような権限をビジネスパートナーに与えている組織は 60% 近くにのぼり、政府機関に与えている組織は **50%** を超えています。業界別で言えば、外部に完全なアクセス権限を積極的に付与しているのは、製造業です。

多くの組織が SCADA / ICS セキュリティの一部をアウトソーシングしているという状況も、リスク増大の原因です。IT ベンダーにアウトソーシングされている SCADA / ICS 機能の上位には、無線セキュリティ、侵入検知、ネットワークアクセス制御、IoT セキュリティがありました。このようなアウトソーシングは、分離とはほど遠い状況にあります。調査対象の組織の **56%** は、SCADA セキュリティを複数のベンダーにアウトソーシングしています。その結果、ベンダー間が**うまく連携せず、防御態勢にギャップが生じる**原因になっているケースもあります。

ほとんどの組織が第三者に特権アクセスを提供している

設問 3：SCADA / ICS へのアクセスを、どの程度外部に許可していますか。もっとも当てはまるものを選んでください。



対象：重要なインフラストラクチャ、IP レベルの保護、IoT、SCADA のセキュリティを担当する、グローバル組織の意思決定者 429 人
出典：Forrester Consulting がフォーティネットの依頼で実施した調査結果

図 3：多くの SCADA / ICS ユーザーが、テクノロジーベンダーなどのビジネスパートナーに特権システムアクセスを許可しています。

SCADA / ICS を運用する組織は、パートナーを信頼してシステムの管理を委ねています。

64% が、サードパーティ IT ベンダーに完全なシステムアクセスまたは高レベルアクセスを許可しています。

IT ベンダーの脆弱性により、自社が被害を受ける可能性も否定できません。

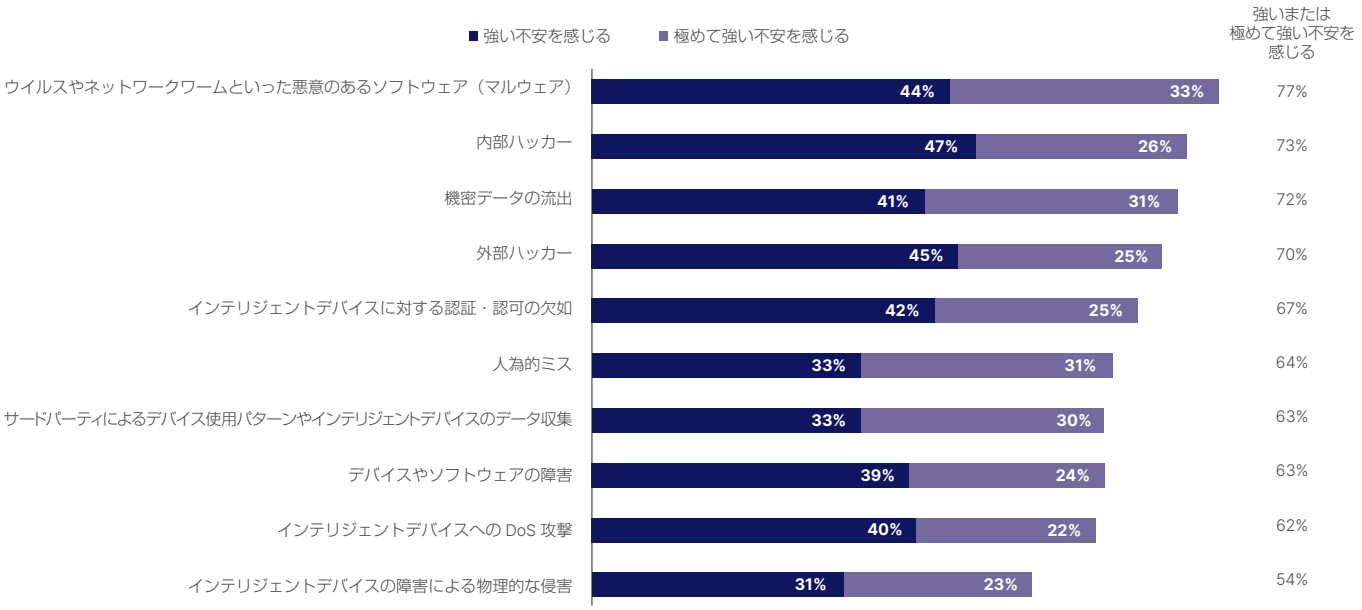
SCADA と ICS に対する脅威

SCADA / ICS を運用している組織を対象に Forrester が実施した調査では、社内ポリシーだけでなく、最も深刻なセキュリティ脅威についても質問しています。調査では、マルウェアや内部のセキュリティ侵害が懸案事項となり、複数のソースから侵入する複数の脅威が認識されていることが明らかになっています。組織の **75%** 以上が、外部のマルウェアに対して、強いまたは非常に強い懸念を示しています。また、**70%** 以上が内部ハッカー、機密データの流出、外部ハッカーに関して、強いまたは非常に強い不安を持っています。**3 分の 2** 以上が、インテリジェントデバイスの認証または承認機能がない点、3 分の 2 近くが人為的ミスを、さらにサードパーティによるデータ / デバイス使用パターンの収集を懸案事項として挙げています。

同様の調査が実施された 2016 年から、マルウェアと内部ハッカーに対する不安が増大しています。この間、脅威のトレンドは大幅に変化し、SCADA / ICS のリスクレベルが高まっているにもかかわらず、SCADA / ICS を運用する組織が認識するリスクレベルは、実際には低下しています。たとえば、人為的ミス、サードパーティによるデータ収集、デバイスやソフトウェアの障害に対する不安は小さくなっています。ただし、これは他のソースからのセキュリティリスクの証拠が認識されているからかもしれません。

セキュリティの課題は、ウイルス、ハッカー、データ流出、認証機能の欠如など、多岐にわたる

設問 4：SCADA / ICS ネットワークのセキュリティについて、次の問題の深刻度をお答えください。



対象：重要なインフラストラクチャ、IP レベルの保護、IoT、SCADA のセキュリティを担当する、グローバル組織の意思決定者 429 人
出典：Forrester Consulting がフォーティネットの依頼で実施した調査結果

図 4：SCADA / ICS を運用する組織は、マルウェアや内部ハッカーといった脅威に不安を感じています。

OT 組織の 70% 以上が、
内部ハッカー、機密データの流出、外部ハッカーに関して、
強いまたは非常に強い不安を感じています。

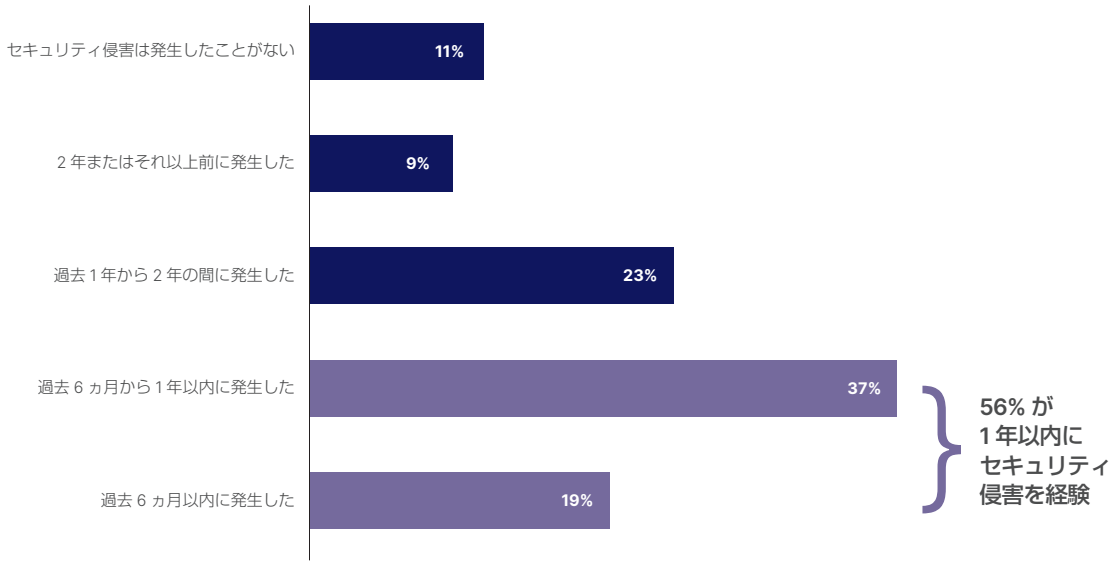
脅威が及ぼす影響

多くの組織が複数のセキュリティプラクティスを採用しているにもかかわらず、SCADA / ICS システムに対する侵害は頻繁に発生しています。たとえば、**回答者の 56% が過去 1 年に SCADA / ICS のセキュリティ侵害を経験**しており、過去にセキュリティ侵害が発生したことのある組織は **32%** を占めています。これまでセキュリティ侵害を経験していない組織は、ほんのわずかです。

SCADA / ICS のセキュリティ侵害は、深刻な影響を及ぼします。組織の **63%** は、SCADA / ICS セキュリティ侵害によって従業員の安全が大きく損なわれると回答しています。また、**58%** は財務的な安定性への大きな影響、**63%** は十分なレベルでシステムを運用する能力に対する深刻な影響を指摘しています。

組織の 56% が過去 1 年に SCADA / ICS セキュリティ侵害を経験

設問 5：過去に組織内の SCADA / ICS でセキュリティ侵害が発生したことがありますか。ご自身の認識の範囲においてお答えください。



対象：重要なインフラストラクチャ、IP レベルの保護、IoT、SCADA のセキュリティを担当する、グローバル組織の意思決定者 429 人
出典：Forrester Consulting がフォーティネットの依頼で実施した調査結果

図 5：SCADA / ICS を使用する組織のほとんどが、過去 1 年間にシステムのセキュリティ侵害を経験しています。

SCADA / ICS システムの侵害は、日常茶飯事です。

SCADA / ICS を運用する組織の 56% が過去 1 年にセキュリティ侵害を経験しています。

セキュリティ侵害は、従業員の安全と組織の財務的安定性を損ないます。

リスク軽減に向けた推奨事項

SCADA / ICS のセキュリティリスクは、さまざま方法で軽減できます。OT / IT システムのコンバージェンスに伴うリスク対応の方法として組織の半数近くが最も重視するのは、完全なビジネス / 運用リスクの評価です。リスク軽減の方法には、一般的な標準の採用、デバイス管理の一元化、ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）をはじめとする政府機関への相談などがあります。

SCADA / ICS セキュリティベンダーの選定については、組織の半数以上が、信頼性の高い情報を提供するテクノロジーコンサルタントに信頼を寄せていることが明らかになっています。たとえば、信頼性という点では、SCADA / ICS ベンダーとパートナーの信頼度は **50%** をわずかに上回る程度です。

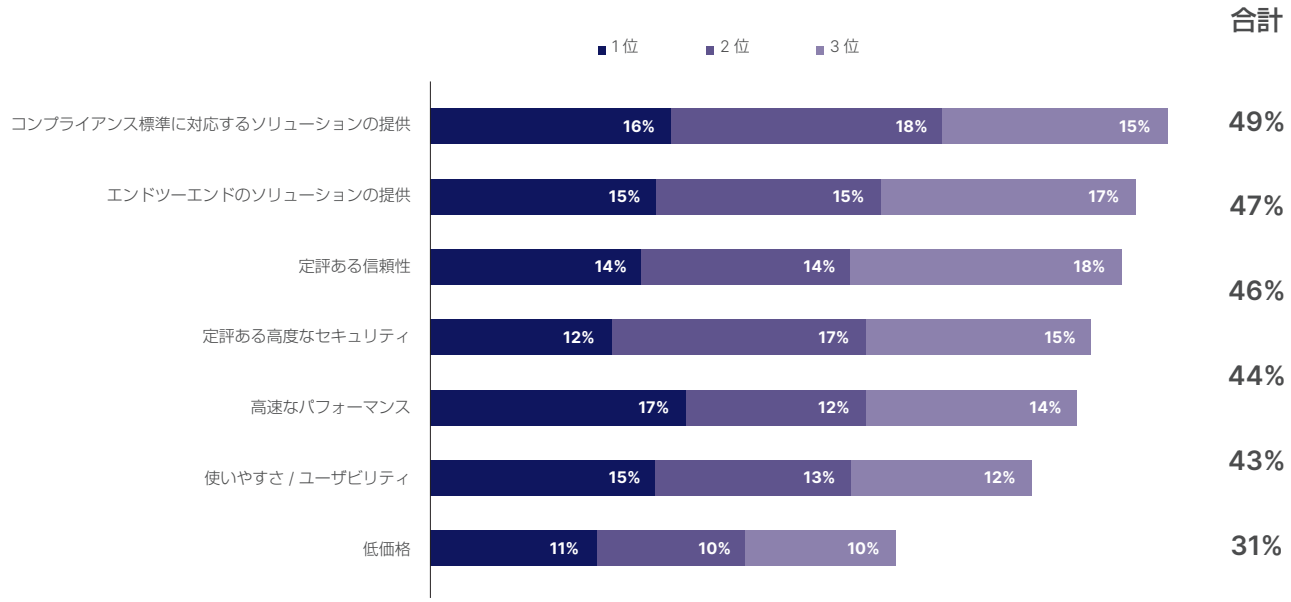
セキュリティプロバイダーとテクノロジーの評価では、次の能力を検討する必要があります。

- 高速なパフォーマンス
- コンプライアンス標準への対応
- 包括的なエンドツーエンドのソリューション

組織では、定評ある信頼性と高レベルのセキュリティの実績がいずれも非常に重視されています。業界 / セキュリティ標準へのコンプライアンスも最優先課題の 1 つです。ほぼ半数が、セキュリティソリューションの選定において最重視する要素として、コンプライアンス標準への準拠を挙げています。エンドツーエンドのソリューションを提供する能力は、重視する要素の第 2 位となっています。興味深いことに、低コストであることを重視する組織は、わずか **30%** に留まっています。

ベンダーの選定基準は、コンプライアンス標準への対応、エンドツーエンドのソリューションの提供、信頼性である

設問 6：SCADA / ICS のセキュリティベンダーの選定において、最も重視する条件は次のどれですか。（上位 3 つを順に挙げてください）



対象：重要なインフラストラクチャ、IP レベルの保護、IoT、SCADA のセキュリティを担当する、グローバル組織の意思決定者 429 人
出典：Forrester Consulting がフォーティネットの依頼で実施した調査結果

図 6：SCADA / ICS ユーザーは、セキュリティベンダーの選定において、コンプライアンス標準への対応やエンドツーエンドソリューションの提供など、複数の優先基準を持っています。

これからの道のり：今後の展望

SCADA / ICS を使用する組織の多くが、今後セキュリティ関連テクノロジーへの投資増を計画しています。セキュリティテクノロジーに予算を割かない組織は、取り残されてしまうことになります。組織の **4 分の 3** 近くが IoT セキュリティへの支出増額を計画しており、その 36% は 5% 以上の増額を予定しています。また、70% が OT セキュリティへの支出増額を計画しており、その 40% は 5% 以上の増額を予定しています。さらに、今後 OT インフラストラクチャへの支出増額を計画している組織は **70%** を占め、その 37% は 5% 以上の増額を予定しています。このような投資増は、システム保護に必要な OT およびセキュリティ標準 / 制御への継続的な取り組みや、さらなる強化の現れです。

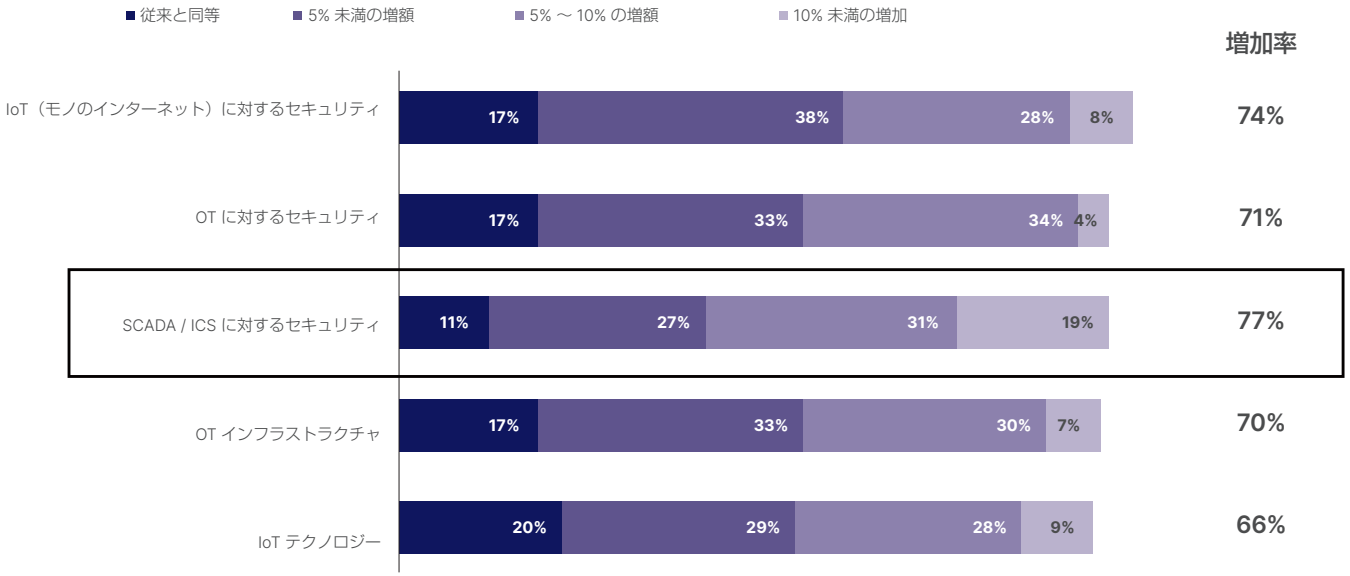
SCADA / ICS を運用する組織がどのようなセキュリティ対策に投資すべきかを検討する際には、資産保護対策を段階的に講じる次のような方法があり、その代表的なものに以下が挙げられます。

- ネットワークセグメンテーションにより、接続された無線と IoT テクノロジーを SCADA / ICS から分離する
- ネットワークインフラストラクチャ（スイッチ、ルーター、無線ネットワークなど）を、重要な資産保護向けに設計されたファイアウォールのようなツールで保護する
- アイデンティティおよびアクセス管理ポリシーを適用することで、外部によるネットワークアクセスや、従業員による不要な領域へのアクセスを禁止する
- WAF（Web アプリケーションファイアウォール）を使用して、パッチが適用されていない Web アプリケーションをスキャンする
- エンドポイント保護を導入し、リアルタイムの実用的なインテリジェンスと脅威の可視化を実現する

従業員や顧客の物理的な安全を損なう可能性を考えれば、従来の IT システムとは異なる方法で SCADA / ICS のセキュリティを検討する必要があることは明らかです。ここで大いに役立つのは多層型アプローチの SCADA / ICS セキュリティで、セキュリティを大幅に強化し、リスクの軽減に効果的です。

SCADA / ICS セキュリティへの投資が他の領域よりも増大

設問 7：次の分野における今後の投資意向をお教えください。



対象：重要なインフラストラクチャ、IP レベルの保護、IoT、SCADA のセキュリティを担当する、グローバル組織の意思決定者 429 人
出典：Forrester Consulting がフォーティネットの依頼で実施した調査結果

図 7：SCADA / ICS を運用する組織の多くが、セキュリティ投資の増額を計画しています。

参考文献

[1] 「Industrial control systems: The holy grail of cyberwar」、Joe Weiss 著、The Christian Science Monitor、2017 年 3 月 24 日（英語）：
https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0324/Industrial-control-systems-The-holy-grail-of-cyberwar

[2] 「Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid」、Kim Zetter 著、WIRED、2016 年 3 月 3 日（英語）：
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[3] 「Water treatment plant hacked, chemical mix changed for tap supplies」、John Leyden 著、The Register、2016 年 3 月 24 日（英語）：
https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

[4] 「Global Industrial Controls System Market to Grow at CAGR of 4.9% from 2015 to 2021」、Transparency Market Research、2015 年 9 月：
https://www.transparencymarketresearch.com/pressrelease/industrial-controls-market.htm

[5] 「Industrial Control Systems Cyber Security」、Mark Fabro 著、Presentation to U.S. Department of Defense、2017 年 6 月 7 日（英語）：
https://www.acq.osd.mil/log/mr/.PSM_workshop.html/2017 Files/Day2/06_Industrial_Control_Systems_CyberSec_Fabro.pdf

[6] 「SCADA Market Worth 13.43 Billion USD by 2022」、MarketsandMarkets、2019 年 4 月 12 日（英語）：
https://www.marketsandmarkets.com/PressReleases/supervisory-control-data-acquisition.asp

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

Report-OT-Forrester-202108-R1