Gartner

セキュリティ／リスク戦略を再考する

サイバーセキュリティの最新プラクティスを取り入れながら、デジタル・ビジネスの実現を支援する

Tom Scholtz
Distinguished VP Analyst, Gartner

はじめに

混乱や破壊的変化が非常に多い年が続いています。新型コロナウイルス感染症 (COVID-19) を乗り超えようとする組織にとって、従業員の健康と安全を優先することが重点課題であったことは言うまでもありません。

多くの組織において、これはデジタル化の導入を加速することを意味していました。できる限り早く、できる限り多くの従業員を在宅勤務に切り替えることも含まれていました。リモートワークへの移行を他社よりも先行して進めている組織もありました。

COVID-19 により、セキュリティ・チームは、クラウドによるセキュリティの価値に改めて注力するようになりました。リモート・アクセスのポリシーやツールを見直し、クラウド・データセンターや SaaS アプリケーションに移行したほか、対面でのやりとりを最小化する新しいデジタル化の取り組みで、セキュリティを確保しました。

Tom Scholtz
Distinguished VP Analyst, Gartner

多くの点で、パンデミックはセキュリティ・チームに対し、ビジネスのためのセキュリティ基盤の大半を再考し、同時に、ビジネスが継続的に進化し成長できるよう支援することを余儀なくさせました。

この eBook では、セキュリティとリスクのリーダーが戦略をどのように考え、取締役会にセキュリティ／リスクについてどのように報告し、チームの要員計画をどのように促進させるかについて学ぶことができます。

セキュリティとリスクに対する見方を新たにする

セキュリティのプロフェッショナルは、米 Equifax 社の情報漏洩事件、SolarWinds 製品の脆弱性、ホテルチェーン Marriott International の顧客情報への不正アクセス、インドの Aadhaar の登録情報漏洩など、新聞の見出しを飾る脅威や情報漏洩に気を取られることが多く、組織にとって最も重要なセキュリティに必ずしも目を向けていません。

根拠のないクラウド・セキュリティへの不安から、セキュリティ・チームがクラウドへの取り組みを躊躇するのは、その典型的な例です。不安が過度になるとビジネス上の機会が失われ、セキュリティへの不相応な支出につながる恐れがあります。

高い注目を集めるこうしたストーリーは、悲観的なシナリオであふれていますが、過去 10 年間のセキュリティ・インシデントにおいてゼロデイ脆弱性が原因となった割合は約 0.4% です。脆弱性の検出に費やされた支出総額と、実際に突き付けられたリスクとの間で、バランスを欠いています。

最高情報セキュリティ責任者 (CISO) は、セキュリティ・プログラムで必須の条件と、ビジネスの前進のために取るべきリスクとの間で、バランスを取る必要があります。これができないと組織は機会を逸し、企業のリーダーにとって CISO は高コストで邪魔な存在になります。

このバランスを取ることは、「言うは易し、行うは難し」かもしれません。デジタル化は加速度的に進んでいますが、染み付いた信念が役に立たないことも多いのです。破壊的変化の真っ只中でも成功を収められるように、今こそマインドセットを変えるときです。状況把握を概念的、感情的に行うのをやめ、「事実」、すなわち未来のデジタル化の現実に適した新たな判断基準を身に付ける必要があります。そうすれば、変化に対応できる新たな環境を生み出すことが可能です。

過去 10 年間のセキュリティ・インシデントにおいてゼロデイ脆弱性が原因となった割合は約 0.4% です。

出典：ガートナー

信頼とレジリエンスを高める

デジタル・ビジネスは新たなエコシステムを生み出しています。このエコシステムでは、パートナーが新たなビジネス機能を付加し、セキュリティを複雑にしています。CISO は信頼とレジリエンスを高めるエコシステムをベースに、リスクとセキュリティへのビジョンを打ち出さなければなりません。

ガートナーのアナリストで、ディスティングイッシュト バイス プレジデントのトム・ショルツ (Tom Scholtz) は、次のように述べています。「目的は、企業保護という火急の課題と、革新的でリスクのある新しいテクノロジ・アプローチで競争力を維持する必要性を両立させた、エコシステムを提供することです」

悪用される脆弱性の大半について、今後も、そのインシデントが発生したタイミングで、セキュリティと IT のプロフェッショナルは知ることになるでしょう。

「成功するかどうかは、CISO が新しい信頼／レジリエンスの原則を意欲的に取り入れるかにかかっています」とトム・ショルツは補足しています。

6 つの信頼／レジリエンスの原則

- チェックボックス型のコンプライアンスから、リスク・ベースの意思決定へとシフトする
- インフラストラクチャの保護だけではなく、ビジネス成果のサポートにも着手する
- ディフェンダーではなく、ファシリテーターになる
- 情報の流れを見極めるが、これを制御しようとはしない
- 人中心の姿勢を持ち、テクノロジの限界を受け入れる
- 検知／対応に投資し、組織を完璧に守ろうとするのをやめる

デジタル・ビジネスのスピードに合わせて動く

この 6 原則を取り入れるために、CISO はこれまでのセキュリティに関する一般的な慣習やベスト・プラクティスからの脱却が必要となります。

「かつてはリスクが大きすぎると考えられていた機会を受け入れるために、あらゆる場所に適応できるセキュリティが必要です」とトム・ショルツは述べています。

同様に重要なのは、CISO がデジタル・ビジネスのスピードに合わせて組織を守ることです。そのために、分散型アーキテクチャによって、拡張性／柔軟性／信頼性の高いサイバーセキュリティ制御を行うサイバーセキュリティ・メッシュを取り入れます。

サイバーセキュリティ・メッシュを実現するテクノロジ

- クラウド・アクセス・セキュリティ・ブローカ (CASB)
- ゼロ・トラスト・ネットワーク・アクセス (ZTNA)
- セキュア・アクセス・サービス・エッジ (SASE)

検出して対応し、報告する

CISO が大規模なサイバー攻撃やランサムウェア攻撃を経験する可能性は低いものの、そうした攻撃に遭った他の CISO から学ぶことは誰もができます。

例えば、規制の厳しい医療業界では、何十万人もの患者のデータを管理および保護し、業界の規制を遵守するという責任を各医療機関が負っています。

しかし、医療機関が標的型フィッシング攻撃の被害に遭うと、病院の従業員や患者が非常に危険な状況に置かれ、とりわけ病院の医療提供能力に影響が及びます。

医療機関の CISO は、その攻撃はどのように起こり、医療施設をどう麻痺させてしまったのかを矢継ぎ早に問われるため、これに回答しなければなりません。

用語

phish•ing (フィッシング)
/'fiSHiNG/

名詞

ソーシャル・エンジニアリングを利用し、個人や企業の資産への不正アクセスを可能にする広範囲で影響力の大きい脅威

smish•ing (スミッシング)
/'smiSHiNG/

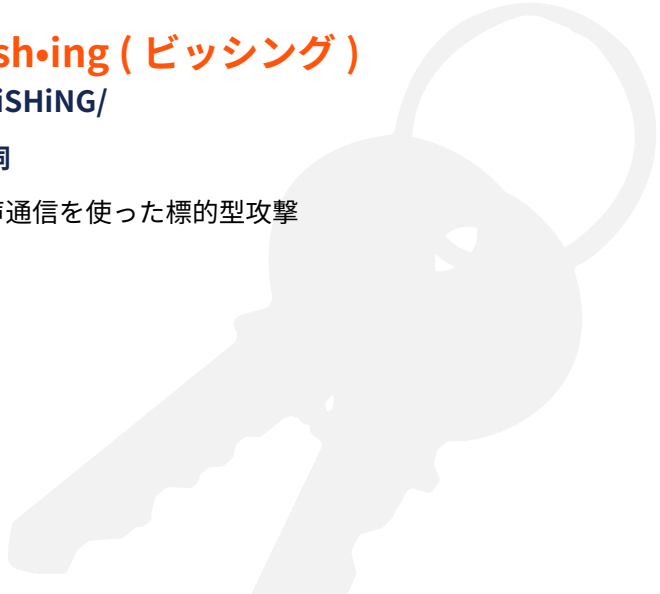
名詞

SMS を使った標的型攻撃

vish•ing (ビッシング)
/'viSHiNG/

名詞

音声通信を使った標的型攻撃



情報セキュリティ・チームが慢性的な人材不足に陥っていて、新規テクノロジを厳しい納期で導入しなければという重圧にもさらされていると回答するCISO もいるでしょう。

セキュリティの熟練者がチームを牽引していたとしても、変化し続ける脅威やトレンドに追い付くための時間やリソースがなく、結果として既知の脆弱性を特定できず、企業を守れない場合があります。既知の脆弱性こそ、組織を最もリスクにさらす可能性が高い脅威です。

組織は、現在の脅威環境に素早く対応しようと四苦八苦しています。手動のプロセスがあまりに多く、さらにセキュリティとリスクの管理者は、リソース／スキル／予算不足に立ち向かわなければなりません。

リソースが不足する中で攻撃の増加に直面したら、CISO は何ができるのでしょうか。

教訓を適用する

- 既知の脆弱性に対処し、パッチを適用する。既存のリソースを評価し、検知と防御のソリューションを均等に組み合わせた投資を行う。
- トレンドを常に把握し、そのインパクトを理解する。 それができずに、脆弱な状態に置かれた医療機関もある。
- 攻撃を受けても、責任の押し付け合いをしない。インシデント対応で最も重要な段階の 1 つは、根本的な原因に焦点を当てることである。責任をなすりつけ合っても、何も解決しない。
- フィッシング対策行動管理 (Anti-Phishing Behavior Management: APBM) を使用する。これは、人中心のセキュリティ戦略において極めて重要な要素となる。
- Email ゲートウェイを保護する。標的型フィッシング手法を導入したセキュア Email ゲートウェイ (Secure Email Gateway: SEG) ベンダーが増えている。最も効果的なのは、プロキシと Time-of-Click の分析フィルタリング技術である。
- 脆弱なシステムを切り離す。まだマルウェアの影響を受けていない脆弱なままのシステムが最も頼りにされていることが多々ある。効果的な暫定対策は、セキュリティ侵害や攻撃が発生した際に、ネットワークの接続を制限することである。
- 静的な個人データへの依存度を下げる。Equifax のようなデータ漏洩リスクを防ぐためにアイデンティティ確認を行う際には、静的ではなく動的なアイデンティティ・データを重視する。

腕を磨き、練習し、実践する

大企業の CISO は、少なくとも年に 1 回、サイバーセキュリティとテクノロジ・リスクについて取締役会に報告することが求められるようになっています。

取締役会での報告は、新たな機会を提供するものですが、困難で思わず立ちすくむような仕事でもあります。プレゼンテーションの際には、各テクノロジの詳細を深堀りする必要はありません。重要なのは、すべてをビジネスに関連付けることです。ここでは、スライド 7 枚で構成された 15 分間のプレゼンテーションについて考えてみましょう。

開始する

最初のスライドには、注目を喚起する概要を示します。取締役会に状況を説明し、以降のスライドで取り上げるトピックを特定するだけにします。詳細は不要ですが、プレゼンテーションには、ビジネス状況、戦略、外部の動向、リスク・ポジションについての情報が明示されている必要があります。以下に例示します。

スライド 1：重要なポイント

ビジネス状況	重大リスク	外部の環境	セキュリティ戦略	推奨事項
明るい兆しも見え始めていますが、いくつかの分野で継続的な改善を行うことで、ビジネス・パフォーマンスを強化します。	最近の企業買収によって、リスク・ポジションには若干の変化がありましたが、それ以外のすべての重大なリスク・ポジションについては安定しています。	社外で発生した事象に対しては、わずかな戦術的対応だけで十分です。	現在のセキュリティ戦略は、概ね目標通りに進んでいます。プロセスの成熟度は継続的に改善しており、ピア・ベンチマークではスコアを上回り、目標に近づいています。	現状を注視し、アクション・プランの承認について検討ください。

ビジネスの実行におけるパフォーマンスと貢献

以降のスライドでは、取締役会が重視するビジネス要素に、セキュリティとリスクを明示的あるいは非明示的に結び付ける必要があります。評価指標に焦点を当て、セキュリティ・チームがプラスの成果にどのように貢献するかを強調します。潜在的な問題点や影響を説明できるよう準備します。取締役から要望があれば、各評価指標の仕組みを詳述したドキュメントを提供します。

2023 年までに、最高情報セキュリティ責任者 (CSO) の評価の 30% は、ビジネスに価値を生み出す能力で評価されるようになる。

出典：ガートナー

スライド 2 ～ 6：明るい兆しも見え始めていますが、いくつかの分野で継続的な改善を行うことで、ビジネス・パフォーマンスを強化します。

財務	顧客	オペレーション	学習と成長
セキュリティによって、ビジネスの成長を支援します。	提供するサービスの可用性と継続性を高めます。	ツールは目的に適合します。	従業員のエンゲージメントは全面的に向上します。
セキュリティ管理を効率化します。	顧客はサービスと設備で当社を信頼します。	変更を効率的かつ確実に実施します。	従業員は正しい意思決定を行います。
納期内かつ予算内でプロジェクトを遂行します。	適用される全規制を遵守します。	プロセスに継続的な改善を組み込みます。	従業員の専門知識を養うために人材育成に投資します。
サプライヤー管理の費用対効果を高めます。	適切な人が適切な情報にアクセスします。	定義した許容リスク内でオペレーショナル・リスクを維持します。	自社のノウハウを競争優位性として保護します。

行動喚起

最後のスライドには、主要なポイントと必要なアクション項目を再掲して、プレゼンテーションを締めくくります。大切なことは、プレゼンテーションを力強く締めくくって、取締役会が、CISO の計画と能力に自信を持てるようにすることです。説明したポイントを要約し、取締役会に求める項目を明確にします。そして質問を受け付け、時間を割いてくれたことに謝意を示します。

スライド 7：アクション・プラン

取締役会に現状を注視するよう求めます：

定常業務 (Business-as-usual: BAU) として行う、ビジネス・パフォーマンスを向上させる作業プログラムについては継続します。	外部の変化に対する小規模なアクションについては、BAU として実行します。	重大なリスク・ポジションへの軽微な変更については、アクションは不要です。	現在のセキュリティ戦略は、概ね目標に向かって進んでいます。プロセス成熟度は継続的に向上し、ピア・ベンチマークでスコアを上回り、目標に近づいています。	現状を注視し、アクション・プランへの承認を検討ください。

次の半期についても、取締役会に対して定期的に更新情報を報告します。

取締役会からのセキュリティ質問への対策は万全ですか？

取締役会は、セキュリティとリスク・マネジメントがいかに重要であるかを理解しているため、リーダーに対してより複雑で含みを持たせた質問をするようになっています。知識拡大にも努め、以前より、企業のプログラムの有効性を問いただせる準備を行っています。

セキュリティに関して取締役会から間違いなく尋ねられる 5 つの質問

トレードオフに関する質問

質問：100% 安全か？それは間違いないか？

質問の意図：このような質問をする取締役は、セキュリティとビジネスへの影響を真に理解していません。100% の安全性や保護を実現することは不可能です。CISO の役割は、リスクが最も高い領域を特定し、ビジネス部門の目標に基づいて、有限のリソースをその管理に割り当てることです。

回答方法：次のように始めます。「脅威は、常に進化するという性質を持ちます。それを考えると、情報リスクの発生源を完全に排除することは不可能です。私の役割は、リスク・コントロールを実装してリスクを管理することです。ビジネスの成長に伴って、適切なリスクの程度を継続的に再評価する必要があります。持続可能なプログラムを構築して、ビジネス運営とビジネス保護の必要性を両立させることを目指します」

脅威環境に関する質問

質問：外部の状況はどれほど悪いのか？ X 社ではどうだったのか？他社と比べて自社はどうか？

質問の意図:取締役はリスクを理解するために、脅威に関するレポート、記事、ブログ、規制当局からのプレッシャーに接するようになります。CISO が常に尋ねられることは、他社、とりわけ同業他社がどのような対策を講じているかです。「空模様」がどのような感じで、自社は他社と比べてどうなのかを知りたいのです。

回答方法：他社のセキュリティ問題の根本原因を推測することは避け、「より多くの情報が得られるまで、XYZ 社での件を憶測で発言するのは差し控えます。詳細が分かり次第、フォローアップいたします」と回答します。「類似の弱点を特定してその修復方法を決める」「事業継続計画を更新する」など、一連の幅広いセキュリティ対策について話し合うことを検討します。

リスクに関する質問

質問：当社にとってのリスクを把握しているか？ CISO を昼夜悩ませ続けている問題は何か？

質問の意図：取締役会は、リスクを受け入れることが 1 つの選択だと理解しています (理解していないとしたら、それは CISO が解決すべき課題です)。取締役会が知りたいのは、自社のリスクが適切に処理されているかどうかです。CISO は、組織のリスク許容度を説明して、リスク・マネジメントに関する意思決定を行うべきです。

回答方法：リスク・マネジメントに関する意思決定がビジネスに及ぼす影響を説明し、自分の見解をエビデンスで裏付けます。取締役会はリスクの許容度に基づいて意思決定を行っているため、エビデンスの部分が極めて重要です。許容範囲を超えるリスクについては、許容範囲に収めるための改善策が必要です。必ずしも短期間で劇的な変更を行う必要はなく、過剰反応には注意が必要です。取締役会は、「重大なリスクを適切に管理していること」、そして「長期的で巧妙なアプローチが場合によっては適切なこと」の保証を求めているのです。

パフォーマンスに関する質問

質問：リソースを適切に割り当てているか？支出は十分か？支出が多い理由は何か？

質問の意図：取締役会は、セキュリティとリスク・マネジメントのリーダーが行き詰まっていないことを確認して、評価指標や ROI について知りたいと考えています。

回答方法：バランス・スコアカードの手法を用いて、「ビジネスの抱負」「これに対する組織のパフォーマンス」をスコアカードの最上部で、シンプルな信号色を用いて表現します。「ビジネスの抱負」は可能な限り、テクノロジではなくビジネス・パフォーマンスの観点から説明します。客観的な基準でセキュリティを評価し、パフォーマンスの裏付けとします。

インシデントに関する質問

質問：どのようにして起こったか？ CISO がコントロールしていると思っていたが？何がうまくいかなかったのか？

質問の意図：インシデントやイベントが発生し、その件について取締役会が既に把握しているのか、CISO が報告をしている場合にこのような質問が投げかけられます。

回答方法：インシデントを避けて通ることは不可能なため、事実を伝えます。知っていること、不足する情報を収集すべく何を行っているのかを共有します。要するに、インシデントを認め、ビジネスへの影響を詳細に説明し、対処が必要な脆弱性とギャップの概要を示し、緩和策を提供します。取締役会の目の前で、ある 1 つのオプションだけを究極的な選択肢として支持しないように注意します。セキュリティとリスクの監督責任は引き続きセキュリティ・リーダーが持ちますが、その説明責任については常に取締役会／経営幹部レベルで定義されなければなりません。

セキュリティ人材へのアプローチを再考する

IT セキュリティ・プロフェッショナルの失業率はほぼゼロです。

セキュリティ・プロフェッショナルに対する需要は引き続き拡大しているものの、このポジションを担えるだけのスキルと経験を有する人材の数が、追い付いていません。スキル不足にさらに追い打ちをかけているのが、IT セキュリティ・チームに期待されている役割の拡大と戦略性の高まりです。つまり、企業成長を後押しし、自社が新しいテクノロジを使ってより賢明にリスクを取れるようにし、全社的に増大している情報セキュリティ・サポート需要に応えることが期待されています。

簡単に言えば、今日のセキュリティ・プロフェッショナルの採用は 3 ～ 4 年前よりも難しくなっています。

CISO の主要なセキュリティ課題

今日の CISO は、以下に示す新しい状況に直面しています。

1. 新しいセキュリティ能力／役割が必要となっています。デジタル化によって、新しいスキルと知識を必要とする幅広い役割がますます求められています。CISO は、今後 24 カ月で、必要となっているセキュリティ能力を 30 以上選び、情報セキュリティ機能に追加することが期待されています。その 1 つが、セキュリティ戦略の設定と企業戦略への情報提供に責任のあるセキュリティ・ストラテジストです。

2. 新しいセキュリティ人材を採用するのは容易ではありません。IT セキュリティ・ポジションの補充には平均 130 日かかります。換言すれば、数カ月の間、ポジションは埋まらず人手不足が続くことになります。その結果、チームは往々にして、離職率が高く採用ペースが遅いという悪循環に陥ってしまいます。

3. セキュリティへの需要が処理能力を超えてしまっています。セキュリティの専門知識に対する需要が増大し、CISO は、チームの業務処理量を飛躍的に増やさなければとの大きなプレッシャーを感じています。需要増加の背景には、デジタル・トランスフォーメーションへの大規模投資、データ侵害やサイバー攻撃に関する報道、アジャイル開発手法の普及があり、CISO は既存の人員数でこなす業務量を増やしながら、将来の人材ニーズのシフトのために計画を立てることが求められています。

データを活用して新たな人材ソースを発掘する

Gartner TalentNeuron ™は、デジタル人材を見つけるためのソースとして活用できます。CISO は、人事部門のリーダーと共に、データを用いて、未開拓の人材ソースをどのように発掘できるかを確かめることができます。

- **人材が逼迫しにくい場所。**需要と供給の両方のデータを分析することで、ターゲットとすべき場所をより明確に把握することができる。
- **隣接する企業や業界。**人材ソースのデータをマイニングして、自社が求める人材を積極的に採用している企業を特定した上で、この情報を自社のソーシング基準に加える。
- **新興の人材プールを持つ都市。**データを活用してデジタル人材プールが出現しつつある都市を特定し、自社のリクルーティング・リソースを拡大できるようにする。

リーン手法でチームにアプローチする

データ侵害の解決策は、より有能で大規模な IT セキュリティ・チームを配置することのように思われています。しかし、リーン手法でスタッフの配置に臨むことで、現状把握力を損なうことなく、リソース不足という課題を軽減することができます。この際に必要なことは、セキュリティ機能の一部を、他の本社機能チーム、ビジネス・チーム、IT チームに委ねることです。

ガートナーは、意図的あるいは状況的にリーン・セキュリティ組織戦略を導入した顧客企業とのインタビューを通じて、希少なセキュリティ・リソースの最適化のためにリーン手法は効果的であることを明らかにしました。まずは、セキュリティ・チームを拡大し続けることがセキュリティ・リスクの増大に対処するための最善策だとの思い込みから脱却することが必要です。

「まずは、セキュリティ・チームを拡大し続けることがセキュリティ・リスクの増大に対処するための最善策だとの思い込みから脱却することが必要です」

Tom Scholtz
Distinguished VP Analyst, Gartner

リーン手法の導入に際しては、以下のアクションを取ることを推奨します。

- **既存のセキュリティ組織の現状に異を唱える。**
  説明責任や、情報セキュリティ・チームが担う役割についての根本的な思い込みを問いただす。こうした思い込みがチームへの要求、ひいては、チームの有効性に重大な影響を与える場合がある。
- **現在のセキュリティ・チームの有効性を評価する。**
  そして、ビジネス部門や IT 部門といった他の領域へと委譲可能な機能や能力 (ユーザー意識向上のためのコミュニケーションなど) を特定する。
- リソースやパフォーマンスが不十分な能力について、**ビジネス部門や IT 部門といった他に見つけられそうな場所を特定する**。
- 自社でリーン手法を採用することの利点と欠点、前提条件を**明確にして、伝える**。

リーンなセキュリティ組織を導入するための前提条件

リーンなセキュリティ組織戦略を正式に導入する上で、リスクがないというわけではなく、いくつかの重要な前提条件があります。

- **経営幹部から明確に支持を得ている。**これが鍵であるため、経営幹部が戦略の理由と目的、そして関連するリスクと複雑性について十分把握できるようにする。
- **セキュリティ・チームに分散チームの管理経験がある。**また、運営委員会や調整／プランニング・フォーラムなど、ガバナンス機能の設置と管理における経験も必要となる。
- **組織文化として学習を奨励する環境がある。**また、個人として成長し、新たな責任を受け入れるよう奨励する組織文化であるべきである。リーン手法でのアプローチは、セキュリティ分野以外の従業員が新たな追加責任を受け入れる能力／対応力／意欲があるかどうかに大きく依存しているためである。
- **従業員教育をサポートできる能力と予算配分がある。**セキュリティ責任を負ったことのない従業員には、速やかにトレーニングを提供する必要がある。セキュリティ・チームまたは新しいライン管理者のいずれが、この教育資金を提供するかを決定する。
- **プロセスの成熟度が高い。**成熟したプロセスであることが極めて重要となる。プロセス･ベースではない機能を開発すると、リスクやセキュリティに精通していないリソースへとシフトした際に、難題に直面することになる。

関連リサーチ

セキュリティとリスクに対する見方を新たにする

顧客企業向けリサーチ

Clouds Are Secure: Are You Using Them Securely? (英語)
Jay Heiser (2019 年 10 月)

Implement an Agile Cybersecurity Program: Lessons Learned From the Covid-19 Pandemic (英語)
(2020 年 9 月)

Smarter With Gartner の記事

The Gartner IT Security Approach for the Digital Age (英語)
Smarter With Gartner、Neil MacDonald (2017 年 6 月)

Reframe Your Core Mindset Beliefs to Meet Digital-Era Demands (英語)
Smarter With Gartner、Graham P. Waller (2016 年 12 月)

検出して対応し、報告する

顧客企業向けリサーチ

How to Use Threat Intelligence for Security Monitoring and Incident Response (英語)
(2020 年 9 月)

The Essential Elements of Effective Vulnerability Management (英語)
(2020 年 10 月)

Smarter With Gartner の記事

10 CIO Resolutions for 2019 (英語)
Mark Raskino (2019 年 1 月)

Learn From the WannaCry Ransomware Attack (英語)
Smarter With Gartner、Jonathan Care (2017 年 5 月)

腕を磨き、練習し、実践する

Smarter With Gartner の記事

The 15-Minute, 7-Slide Security Presentation for Your Board of Directors (英語)
Smarter With Gartner、Rob McMillan (2018 年 8 月)

5 Security Questions Your Board Will Inevitably Ask (英語)
Smarter With Gartner、Sam Olyaei (2019 年 10 月)

セキュリティとリスクのトレンドを理解する

顧客企業向けリサーチ

Top Security and Risk Management Trends (英語)
(2020 年 2 月)

セキュリティ人材へのアプローチを再考する

顧客企業向けリサーチ

IT Quarterly: First Quarter 2018 (英語)
Gartner、CIO Research Team (2018 年 2 月)

Adopt a Lean Digital Security Organization to Mitigate the Skills Shortage (英語)
Tom Scholtz (2019 年 4 月)

Smarter With Gartner の記事

5 Places You Didn’t Think to Look for Digital Talent (英語)
Smarter With Gartner、Dion Love (2019 年 7 月)

Confront the Cybersecurity Talent Shortage (英語)
Smarter With Gartner、Sam Olyaei、Matt Stamper (2017 年 6 月)

Gartner

Learn more.
Dig deep.
Stay ahead.

無料コンテンツ：

ガートナー Special Reports

ガートナーはビジネスと IT を成功に導く、テクノロジの主要な
トレンドについての知見をご提供します。

コンファレンスへの参加

セキュリティ & リスク・マネジメント サミット

セキュリティの確保されたデジタルな未来へと組織を導く方法を、
ガートナーのエキスパートから学ぶことができます。

弊社サービス全般に関する
お問い合わせ先
TEL：03-6430-1850 (営業本部)
E-Mail：japan.sales@gartner.com