

身近に迫るサイバー攻撃や災害への対策はできていますか？



IDCnavi 著・DSK-IDC 編著



Cloud
Data Center
Cyber Security





はじめに

※ 本資料は、株式会社電算システムが提供する事業活動の認知を促進することを目的に、客観的な背景や意義をわかりやすく解説したものです。資料末のPRページには、同社の会社概要やプロモーションが含まれています。

DX 推進のうえで知っておきたい セキュリティ知識

DX にはセキュリティ強化が不可欠

デジタルトランスフォーメーション（DX）を組織内で推進していく中で重要なのが、情報セキュリティの強化です。今日では多くの IT 活用が進められる中、これらの技術を悪用してサイバー犯罪、従業員による不祥事が件数が急激に増えています。

場合によっては DX の推進そのものが、情報セキュリティの強化につながるケースもあるため、新システムの導入の前にはあらかじめ確認しておきたい視点です。

本資料では、情報セキュリティにおけるリスクや、どんな対策が有効なのかについて、詳しくご紹介します。

情報セキュリティ対策が 注目を集める理由 1

今日では、多くの企業が情報セキュリティの強化に注目しています。
次に、その主な理由を 3 つ紹介します。

被害額の増加

1 つ目の理由は、サイバー犯罪被害の増加です。2020 年だけで、世界 10 カ国で推定 3 億 3,000 万人、日本だけで 1,800 万人がサイバー犯罪の被害に遭いました。日本の被害総額は推定 220 億円であり、対策を講じない限り、この数値は増加し続けるでしょう。

また、同調査では、日本人の 74% が個人情報盗まれることを不安視し、73% は対処法を知らないと回答しました。基本的な対策方法が広まっていないことが明らかになり、急いで対策が必要であることが浮き彫りになりました。



参考：INTERNET Watch「被害総額は推定 220 億円、日本では過去 1 年間で 1800 万人以上がサイバー犯罪の被害に」 2021 年 5 月 28 日
<https://internet.watch.impress.co.jp/docs/news/1325582.html>

情報セキュリティ対策が 注目を集める理由 2

DX の推進

DX は、ICT を活用して業務をデジタル化し、生産性の向上や働き方改革を推進することを目的としています。この動きは、歓迎すべきものである一方で、情報セキュリティリスクの増加を促す可能性もあることに注意が必要です。

日本では DX の余地が大きいと言われていますが、数百億円にも上るサイバー犯罪の被害が発生していることから、インターネットやデジタルがさらに普及した DX 環境下では、より深刻なセキュリティ被害が発生するリスクがあることにも留意すべきです。

DX を推進する際には、セキュリティリスクの懸念を念頭に置いて対策を行うことが不可欠です。



情報セキュリティ対策が 注目を集める理由 3

リモートワークの増加

働き方改革の一環として、多くの企業がリモートワークの導入を進めています。リモートワークは、コロナウイルス対策として有効であるだけでなく、従業員のライフスタイルに合わせた柔軟な働き方を実現することができます。しかしながら、リモートワークを実施する際には、セキュリティ上の問題にも十分な注意が必要です。

リモートワーク下では、社内のセキュリティシステムの限界や各個人のモラルに一定の依存が生じるため、業務遂行にセキュリティ上のリスクが存在します。新しい働き方を実現するには、新しいセキュリティシステムの構築にも時間を費やす必要があります。





情報セキュリティにて 想定されている主なリスク 1

ここで、情報セキュリティの分野において脅威とされている主なリスクについて、ご紹介いたします。セキュリティへの脅威は3つの分野に分けることができます。
順に確認していきましょう。

意図的な脅威

一つ目は、意図的な脅威です。これは第三者や社内の人間によって、意図的に引き起こされるもので、組織へ危害を加えることを目的としているため、最も悪質なリスクと言えます。被害を受けた際の社会的影響や事業への影響も大きく、経営が大きく傾いてしまう可能性を有しています。

不正アクセス

意図的に引き起こされる脅威としては、不正アクセスが一般的です。従業員のIDを不正に取得し、社内のデータベースから機密情報や個人情報を流出させたり、それを防ぐために身代金を要求したりといった犯行が実施されます。

企業データや個人情報は闇市場で高値で取引される例も多く、近年のサイバー犯罪において主流となっています。

内部不正

ケースとしては少ないものの、内部の犯行によって情報漏洩が行われるケースもあります。企業のデータを横流しすることで金銭を受け取ったり、産業スパイによって外部へ情報が流出してしまうこともあります。

元従業員が自身のIDを悪用し、企業の機密情報を盗んで競合へ合流することもあり得るため、従業員IDの管理を徹底することも非常に重要です。

情報セキュリティにて 想定されている主なリスク 2

偶発的な脅威

二つ目は、偶発的に発生する脅威です。意図的ではないにせよ、人為的に引き起こされるセキュリティリスクの事例を決して少なくなく、ちょっとした手違いで甚大な被害がもたらされることもあります。

社用デバイスの紛失・盗難

働き方改革の影響で多発しているのが、社用 PC やスマホなどの紛失及び盗難です。リモートワークが普及し、以働く場所が多様化した結果、自宅以外にもカフェや旅行先で働くことも可能になりました。

出先で社用デバイスを紛失したり、盗まれてしまったりするケースも多く、取り扱いには私用デバイス以上に注意が必要となります。

誤操作

あまり使い慣れていないシステムを運用していると、誤った操作で情報漏洩などが起こってしまうこともあります。

社内向けに共有していたファイルが、インターネットを通じて一般公開されてしまったり、セキュリティ設定をオフにしてシステムを利用したりといったケースです。

悪意はないにせよ、企業に大きな損失をもたらす危険があるため、できる限り回避しなければならない事態です。

情報セキュリティにて 想定されている主なリスク 3

環境的な脅威

三つ目は、環境的な脅威です。これまでは人為的にもたらされる脅威ばかりでしたが、必ずしも人間だけがセキュリティを脅かすリスクを孕んでいるとは限りません。

落雷や台風などによる 一時的な自然災害

落雷や台風によってもたらされる被害は、システムに甚大な被害をもたらす可能性があります。

落雷によって電源に接続している全ての機器がショートしてしまったり、停電によってデータが保存されることのないまま喪失してしまったりといったリスクです。

自然災害はいつ起こるかわからないものですが、対策方法は体系化されているので、優先的に取り組むべき事案であるとも言えます。

地震や火災による 長期的な障害の発生

停電や電源のショートはすぐに復旧することも可能ですが、地震や火災による被害は短期間での復旧が難しいケースもあります。

地震によってオフィスが倒壊したり、火事によって全焼した場合、会社の利用はおろか、会社機能を丸ごと失ってしまうこともあります。

オフィス一棟に業務システムを任せすぎてしまうと、オフィスが被害にあった際に業務遂行能力が失われてしまいます。

こういった潜在リスクはあらゆる企業に存在するため、やはりバックアップ体制を整備するなどの基本的な対策は欠かせないでしょう。



情報セキュリティリスクが 大きくなる要因

このような情報セキュリティに対するリスクが大きくなる要因については、企業によってさまざまです。ですが、大抵の場合は以下の三つの理由にまとめることができます。

ソフトウェアの脆弱性

一つ目の要因は、ソフトウェアの脆弱性です。アンチウイルスソフトがインストールされていなかったり、OS のアップデートが長年行われていなかったりなどによって、内部のセキュリティが最新の環境に追いついていないことで発生します。

サイバー犯罪の手口は年々多様化し、ソフトの安定性もアップデートによって保たれます。システムを常に最新の状態で保てるよう、整備しなければなりません。

ハードウェア・建物の脆弱性

ハードウェア本体の老朽化が進んでいると、安定したパフォーマンスを発揮できなかったり、ソフトウェアのアップデートができなかったりという問題が発生します。ソフトウェアほどの頻度でアップデートする必要はありませんが、定期的に本体の買い替えを実施することもセキュリティ対策としては有効です。

また、オフィスそのもののセキュリティ対策はもちろん、電力状況に問題があったり、震災リスクの大きい立地であったりする場合は、移転を検討することも重要です。特に首都圏は直下型地震の到来が近いとされているため、徹底した自然災害への備えを実現することは、情報セキュリティの観点からも不可欠と言えます。

マネジメント体制の不備

三つ目に、マネジメント体制の不備です。導入したICTをどのように活用すればいいのか、あるいは社用デバイスの基本的な取り扱いについて、何らルールが決められていないのは問題です。

ソフトの誤操作や社用端末の紛失、不正アクセスを招き入れることにもなるため、DX の推進に伴い管理体制を整備することが求められます。

DX における主な脅威

現代のサイバーセキュリティに対する脅威の種類

サイバー攻撃には、高度に巧妙なターゲット型攻撃から、無秩序な攻撃まで、多岐にわたるサイバー攻撃が存在します。以下に、そのような脅威の一部を紹介します。

偽装攻撃

今もなお最も広まっているサイバーセキュリティ攻撃の一つです。攻撃者は他人になりすまし、被害者のログイン情報などを盗み取ろうと試みます。

クラウド関連の脅威

近年ますます普及しているクラウドコンピューティングには、企業のネットワークへの侵入や、エンドポイントや SaaS サービスの乗っ取りなどの脅威があります。

ランサムウェア

システムやネットワークを感染させ、ファイルを暗号化し、身代金支払いと引き換えにデータを解放するという犯罪行為です。ランサムウェア攻撃は年々増加しています。

モバイル攻撃

クラウドの脅威と同様に、ユーザーがモバイルデバイスを使用する際にセキュリティが緩くなる傾向があります。マルウェア感染やフィッシング攻撃などが、テキストメッセージや音声通話などを通じて配信されることがあります。

ワイヤレス脅威

Wi-Fi ネットワークのセキュリティが不十分であることは広く知られています。利用が増える一方で、5G などのワイヤレス通信の拡大に伴い、悪用のリスクが高まっています。

IoT に基づく攻撃

スマートホームから産業用センサーや医療技術まで、幅広いデバイスにセキュリティ上の脆弱性が存在します。これらは、ネットワークへの侵入や機密情報への不正アクセスを可能にするリスクがあります。



セキュリティリスクによる 様々な損害

最も一般的で費用のかかるセキュリティリスクによる様々な損害には、以下のようなものがあります。

機密データの漏洩

機密データとは、ネットワーク上に存在し、攻撃者にとって価値のあるあらゆる情報を指します。例えば、企業の秘密情報や知的財産、社内文書、メール、従業員や顧客の個人情報（社会保障番号やクレジットカード番号）、医療データなどがこれに該当します。データ漏洩による直接的な被害だけでなく、コンプライアンスに関する罰金など法的責任の違反による罰則も懸念されます。

システムおよびコンピューティングリソースの侵害

これには、企業のシステムがマルウェアに感染して DDoS 攻撃に利用されるリスクや、暗号通貨マイニングボット、スパムリレーなどの悪意のある脅威に悪用されるリスクも含まれます。こうした事態が発生すると、感染した企業は攻撃者の手先として利用される可能性があります。

金銭的損失

攻撃者がシステムに侵入した場合、企業の金融口座情報が盗まれるリスクが存在します。これは大きな経済的損失や致命的なセキュリティリスクとなり得ます。

情報セキュリティの有効な対策方法

このような要件を満たすための情報セキュリティ対策を推進するためには、どのようなことから始めていくべきなのでしょう。最後に、有効かつ優先的に実施したい対策方法をご紹介します。

管理体制の見直し



業務体制の見直し



基本的なセキュリティ対策の見直し



Step 3

Step 2

Step 1

情報セキュリティの有効な対策方法

Step 1

基本的なセキュリティ対策の見直し

まずは、ソフト面でのセキュリティ対策の見直しです。最新のアンチウイルスソフトを全社に導入し、OS やソフトのアップデートを完了することで、最低限の環境構築を済ませましょう。

対策を進めていく中で、脆弱性を抱えているシステムがあるかどうかチェックできるのが理想です。今できる対策の実施と、今後実行すべき改善点の把握を両立しましょう。

Step 2

業務体制の見直し

二つ目に、業務体制の見直しです。社内システムに依存している業務環境は、災害リスクを抱えるだけでなく、最新の不正アクセス対策環境を整える上で課題となるケースもあります。

クラウドシステムを導入すれば、世界有数のセキュリティ環境で業務を遂行できるだけでなく、バックアップも複数拠点にまたがって確保できるため、BCP 対策にも役立ちます。

Step 3

管理体制の見直し

三つ目に、人為的な被害を抑制するための取り組みです。システム運用前の研修を徹底し、ヒューマンエラーのリスクを小さくしたり、細かく要件を指定したルールブックを作成し、社用端末の運用方針を定めたりすることが大切です。

セキュリティ対策の構築について

組織が採用できる最も効果的なサイバーセキュリティツールや次世代テクノロジーには、以下のような要素が含まれます。これらはすべて、サイバーセキュリティインフラの重要な構成要素と見なされています。

ネットワーク監視ツール

ゼロトラストによる保護

データ暗号化

脆弱性評価と侵入テスト

ファイアウォールによる防御

侵入検知システム

認証技術

マルウェアからの保護



セキュリティ対策の構築について

ファイアウォールによる防御

ファイアウォールは、ネットワークセキュリティの要として、ネットワークトラフィックを監視し、外部との通信を遮断する役割を果たします。攻撃の種類に関わらず、セキュリティの最前線として機能します。

マルウェアからの保護

一般的にアンチウイルスソフトウェアとして知られるセキュリティスイートは、クライアント PC 上で実行され、トロイの木馬などの悪意のあるソフトウェアや高度な持続的脅威からの保護を提供します。メールの添付ファイルや危険なウェブサイトなどを介しての感染を防ぎます。

認証技術

二要素認証や多要素認証などの次世代の認証技術を利用したソフトウェアは、異常なユーザー行動を検出し、正当なユーザーによるネットワークアクセスを保護します。

データ暗号化

場合によっては侵入者がネットワークに侵入した場合に備え、企業データを守るために、データを保管および移動中に暗号化することが推奨されます。

脆弱性評価と侵入テスト

場合によっては侵入者がネットワークに侵入した場合に備え、企業データを守るために、データを保管および移動中に暗号化することが推奨されます。

侵入検知システム

ネットワークの境界セキュリティとして機能し、不正な活動をリアルタイムで監視し、違反が発生した場合にセキュリティ担当者に通知します。

ネットワーク監視ツール

ネットワークの監視はセキュリティ違反だけでなく、デバイスの健全性もテストします。急激なトラフィックの増加やデバイスの障害によるダウンタイムを防止します。

ゼロトラストによる保護

ゼロトラストセキュリティなどの手法においては、ファイアウォールの考え方をさらに進化させ、トラフィックの出どころがネットワークの外部か内部かに関係なく、すべてのトラフィックが潜在的に危険であるという前提に立ち、許可を与える前に検証されるべきと考えられています。

データセンターの安全性

サイバー犯罪のリスクが高まる中、国内企業はセキュリティ強化に努めています。またサイバー攻撃の対策方法の一つとして、データセンターを活用する企業も増えつつあります。ここでは、データセンターのセキュリティ上の利用メリットや、具体的にどれくらい安全なのかについて、解説します。



データセンターの役割

そもそもデータセンターは、サーバーを安全に管理するのに特化した施設を指します。これまで、会社のサーバーは社内のサーバールームなどに設置し管理することが一般的でしたが、最近ではデータ活用の機会増加に伴い、自社で管理することが難しくなりつつあります。

そこで、データセンターというサーバー管理に特化した施設を利用することで、オフィスでのサーバー管理負担を減らし、なおかつ安全性を強化した上で会社のデータやシステムを守る企業が増えています。

データセンターのセキュリティ対策

データセンターはサーバー管理専門の施設ということもあり、そのセキュリティ対策は極めて高度です。データセンターのセキュリティは大きく分けて、物理的セキュリティと仮想的セキュリティという2種類に分類されます。

物理的セキュリティ

Physically

物理的セキュリティは、物理的にサーバーを守るための措置が施されていることを指します。人里離れた場所に施設を設置し、周辺環境がもたらすリスクを避けたり、具体的な施設の位置をわかりにくくして不審者の侵入を遠ざけたりしています。

また、施設内のアクセスには幾重にも施されたロックを解除しなければならず、建物自体も強固であるため、外部の人間が侵入することは簡単ではありません。防火設備や耐震性にも優れており、万が一の災害発生にも対処できるのが特徴です。

また、停電などが発生した際にも予備電源を蓄えているので、すぐにシステムがシャットダウンしてしまうことはありません。

仮想的セキュリティ

Virtual

仮想的セキュリティは、いわゆるインターネットを介したサイバー攻撃を防止したり、被害を最小限に抑えたりするためのセキュリティ対策を指します。サーバーへのアクセス権限が厳重に管理されていたり、脅威検知モニタリングが丁寧に実行され、少しでも不審な動きがあれば迅速に特定し、解決に取り組んでくれたりします。

また、データセンター内のネットワークはゾーンごとに区分けされており、サーバー利用者が一人でもマルウェアに感染したら全滅、といった事態に発展しないよう、もしもの時にはサーバーを遮断し、被害を最小限に抑えます。



データセンターの セキュリティレベル その1

上記のようなデータセンターのセキュリティについては、実際にはデータセンターによってまちまちです。

自社で利用しようとしているデータセンターのセキュリティ強度を確かめる上では「ティア評価」と「データファシリティスタンダード」と呼ばれる、2 種類の評価が役に立ちます。

ティア評価

ティア評価は国内外のデータセンターで採用されている、グローバル標準のセキュリティ指標です。データセンターのティアレベルが高いほど高度なセキュリティが敷かれているということになり、基本的にはティア評価の高いセンターを探すのが良いでしょう。

ティアレベルは、

ティア1

ティア2

ティア3

ティア4

という4つのランクづけが行われており、ティア4クラスのデータセンター利用が理想です。ただ、コストの問題もあることから必ずしも理想のティアを満たしているデータセンターを採用できるとは限りません。

自社である程度のインフラが構築できており、冗長性があるならティア1、高度な機密情報を扱っている、あるいは自社で全く対策が行われていないなどの場合はティア4と、使い分けることが大切です。





データセンターの セキュリティレベル その2

データファシリティスタンダード

データファシリティスタンダードは、日本国内で採用されているデータセンターのセキュリティ基準です。基本的な評価基準はアメリカなどのそれと同じですが、日本の環境に合わせた評価基準も追加で盛り込まれているのが特徴です。

データファシリティスタンダードの評価基準は、

建 物

セキュリティ

電気設備

空調設備

通信設備

設備運用

の6つです。日本は地震や津波などの自然災害リスクが大きい国ということもあり、建物の耐震性や構造に関する評価基準が追加されている点が特徴です。建物自体の耐震性はもちろんですが、大きな揺れがあった際にサーバーラックが倒れてしまったり、サーバーが破損してしまったりしないための対策が施されているかも大事です。

外部からの浸水や水道管破裂時などの対策も評価され、防水・漏水対策を徹底したい際にもこちらの評価基準が活躍します。自然災害のリスクも踏まえたデータセンター選びをする場合、データファシリティスタンダードを参考にするべきでしょう。





セキュリティ強化に データセンター利用が活躍する理由

データセンターを利用する場合、サーバールームを撤廃しサーバーをセンターに移管したり、セットアップの負担が発生したりと手間のかかる作業に対処しなければなりません。しかし、セキュリティ強化を徹底して行いたい場合、多くの企業にとってデータセンターの利用は、優秀な対策方法となるはずです。

高水準のセキュリティ環境をすぐに利用できる

データセンターの利用がセキュリティ対策に活躍する最大の理由は、高水準のセキュリティ環境をすぐに実装できる点にあります。通常、十分なセキュリティ対策を自社で行う場合、システムを一から構築しなければならず、そのためには人も時間もお金もかかってしまいます。セキュリティレベルが高いほどこれらの負担は大きくなるため、十分なリソースを持たない企業には厳しいものがあります。

コストパフォーマンスが高い

データセンターの利用はコストパフォーマンスに優れたセキュリティ強化対策であるだけでなく、システムの保守管理の負担軽減にも役立ちます。データセンターにサーバー管理を任せれば、その保守管理もセンター側で対応してもらうことが可能なので、自社で保守管理にリソースを割く必要がなくなります。また、サーバールームを自社から撤廃できるため、オフィスの省スペース化にも貢献し、賃貸料の圧迫を回避できます。

人件費や家賃といった固定費が一気に解消されるので、経営の見直しが迫られている企業にも嬉しいメリットです。

柔軟なサーバー利用が可能

データセンターを利用する場合、サーバーはデータセンター側で管理してもらうこととなりますが、サーバーのセットアップについては自社で自由に行うこともできます。自社でカスタマイズした専門性の高いサーバーであっても、導入時に環境を適切に構築することで、従来通りの運用が可能です。もちろん、データセンターの高速回線を利用できるので、サーバーが遠隔地に移ったからといって、パフォーマンスに大きな変化が出てしまうこともありません。

サイバーセキュリティは増々重要に


サイバーセキュリティは、現在、世界全体でますます重要性を増し、その規模も広がり続けている分野です。

プライバシー規制の強化に伴い、企業はサイバーセキュリティに対する取り組みをますます重要視する必要があります。万一、セキュリティが侵害された場合、高額の罰金や法的責任が発生する可能性があるため、慎重な対策が求められます。

持続的な警戒態勢がサイバーセキュリティの鍵

報道されるサイバー攻撃による影響やデータへの不正アクセス、財政的な損失についての報告を見ると、サイバーセキュリティの状況は予測不能で驚くべき展開で頻繁に変わっていることが分かります。組織は自身のセキュリティ態勢や直面するリスクを理解し、絶え間なく変化するセキュリティ環境に適応する能力を磨くことが不可欠です。

堅牢なサイバーセキュリティを築くには専門知識が必要であり、ネットワークの安全を保つためには詳細でリアルタイムなセキュリティ監視を通じて変動する状況や新たな脅威に常に対処することが重要です。



DX の推進に伴い、情報セキュリティ対策の価値は年々高まっています。システム面での脆弱性を解消するだけでなく、それを扱う側のリテラシーを強化することで、サイバー犯罪の被害を最小限に抑えたり、ケアレスミスを回避したりすることは十分に可能です。人とモノの両面から対策を進め、DX による恩恵を最大化できるように努めましょう。



PR



データセンターは情報を守る専門機関

電算システムのデータセンター『DSK-IDC』では、ISMS (ISO27001) とプライバシーマークの認証を取得し、24時間専用オペレーターによる万全の監視体制で、大切なデータを守ります。

DX 推進のためのセキュリティ確保、BCP としての災害対策、データ保全など、個々の企業の課題に合った解決方法をワンストップでご提供できるのが、電算システムのデータセンターソリューションです。

セキュリティに関する相談はデータセンターへ

企業内の情報管理・セキュリティが心配など思い当たる場合には、まずは現状の改善・見直し方法を専門家に相談ください。課題の解決方法などは個々の企業・地域・運用状況により様々ですが、データセンターが持つノウハウや対策方法をご活用ください。

DX 推進のためのサイバーセキュリティ対策として、ネットワークセキュリティの見直しやアンチウイルスソフト、バックアップツール導入などのご相談もお受けしております。Web サイトから各種分野の IT コンシェルジュへの無料相談のお申込みができます。まずはお気軽にお問い合わせください。

お問い合わせはこちらから

dsk-idc



<https://www.dsk-idc.jp>





出典

参考

本資料の [10-11,14-15,21] において、以下の出典元を全体的に参考にしています。

Phil Muncaster. “Defending the data center: The time to act is now”. welivesecurity.
<https://www.welivesecurity.com/2022/03/18/defending-the-data-center-the-time-to-act-is-now/>,
(参照 2023-09-28)

Splunk Inc. . “サイバーセキュリティとは？ 戦略やサイバー攻撃の種類を解説”. Splunk.
https://www.splunk.com/ja_jp/data-insider/what-is-cybersecurity.html, (参照 2023-09-28)

Cornerstone Co.,Ltd. . “データセンター事業者の選定で重要な「立地場所」の検討方法”.
IDC 比較・選び方ナビ. <https://idcnavi.com/possibility/location/>, (参照 2023-09-28)

Cornerstone Co.,Ltd. . “BCP 強化の為にデータセンターの選び方とは？利用メリットと共に併せて解説！”.
IDC 比較・選び方ナビ. <https://idcnavi.com/possibility/bcp-data-center/>, (参照 2023-09-28)

Cornerstone Co.,Ltd. . “データセンターの選び方のポイントとは？利用する理由も併せて解説”.
IDC 比較・選び方ナビ. <https://idcnavi.com/possibility/datacenter-select-point/>, (参照 2023-09-28)

転載

本資料は、情報サイト『IDC 比較・選び方ナビ』の内容を、
著作権者である株式会社サン・プランニング・システムの許諾を得て掲載しています。

[2-9,12-13,21] Cornerstone Co.,Ltd. . “情報セキュリティのリスクとは？具体的な対策方法を併せて解説”.
IDC 比較・選び方ナビ. <https://idcnavi.com/knowledge/information-security/>, (参照 2023-09-28)

[16-20] Cornerstone Co.,Ltd. . “データセンターの安全性は大丈夫なの？セキュリティ上のメリットを解説”.
IDC 比較・選び方ナビ. <https://idcnavi.com/knowledge/data-center-security/>, (参照 2023-09-28)



運営企業

会社名

株式会社電算システム

会社案内

1967年に岐阜県で創業して以来、独立系総合型情報処理サービス企業として、情報処理サービス事業と収納代行サービス事業の2つの分野で事業を展開しています。官公庁をはじめ、製造・流通・金融証券などの顧客層に対して、企画から設計・開発・運用管理まで一貫して取り組み、ベストソリューションを提供しています。

お問い合わせ窓口

岐阜本社 ☎501-6196 岐阜県岐阜市日置江1丁目58番地
TEL 058-279-3481 FAX 058-279-3487

東京本社 ☎104-0032 東京都中央区八丁堀2丁目20番8号八丁堀綜通ビル
TEL 03-3206-1780 FAX 03-3206-1774

名古屋支社 ☎460-0003 名古屋市中区錦3丁目1番1号十六銀行名古屋ビル12階
TEL 052-961-3690 FAX 052-961-3631

関連 URL <https://www.densan-s.co.jp>
<https://www.dsk-idc.jp>

※本資料に関するご質問、または株式会社電算システムが提供する関連サービスに関するご質問やご相談は、株式会社電算システムの運営サイト URL よりお気軽にお問い合わせください。