無料資料

今求められる情報漏えい対策とは

企業が抱えるリスクとともに解説

保存版資料

株式会社マキナレコード セミナーレポート
Machina Record Security Seminar

これからセキュリティ対策を始める BtoB 企業必見の
オンラインセミナーを全文書き起こしで無料公開！

情報漏洩を予防する対策を解説

サイバー攻撃や
内部不正による

ONLINE SEMINAR

SECURITY SEMINAR

これからはじめるセキュリティ対策
―情報漏えい対策―

企業の抱える情報漏えいリスクや求められる対策を解説

不正アクセス　　業務委託先管理
クラウドツール利用　　従業員教育

今求められる情報漏えい対策は？企業が抱えるリスクとともに解説

マキナレコードでは、これからセキュリティ対策を始めようとお考えのBtoB企業を対象としたオンラインセミナー「これから始めるセキュリティ対策」を開催しました。第2回のテーマは情報漏えい対策です。サイバー攻撃や内部不正による情報漏洩を予防するための対策を解説しました。

この資料では、同セミナーでお話しした内容をご紹介します。

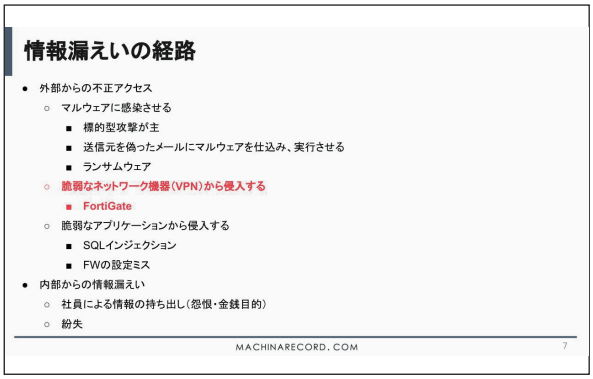
最近のインシデント事例

もうあまりニュースに大きく取り上げられることはなくなってはいますが、1ヶ月に10～20件ぐらい、インシデントが起こっています。大きな会社も含めて被害にあっています。インシデントなので実際の情報漏洩には繋がってないものも一部あるかもしれません。

2022/03/22 森永製菓 164万件（個人情報）
2022/03/01 小島プレス工業（不正アクセス）
2022/02/28 メタップスペイメント 46万件（クレジットカード）
2022/01/22 北海道ガス 3万件（紛失）
2021/05 ネットマーケティング 140万件/免許証等を含む個人情報（個人情報）

こういった事例が日々報告されています。

情報漏洩の経路



情報漏えいの経路は大きく分けると外からか中からかになります。一時期は内部からの漏えいが多いと言われていましたが、最近はかなり攻撃のパターンが複雑化してきており、画一的な攻撃をして奪取するよりは、ターゲットになる端末やデータベース、ファイルサーバーに種を仕込み、長い期間をかけて徐々に情報を入手されていくというケースが増えてきている印象があります。

マルウェアに感染することによる情報漏えい

最近の主流としては手口が2つあります。1つはマルウェアです。これは昔からの手法の一つで、マルウェアに感染することによる情報漏えいです。標的型攻撃メールと言われますが、メールの送信元を偽り、例えば履歴書を送るとか、契約書や請求書の送付メールを装って、ターゲットに対して送られます。その中にマルウェアが仕込まれており、クリックすると感染してしまうというものです。

もともとWindowsはターゲットになっていましたが、最近ではMacでもウイルスに感染するケースが出てきています。昔はMacは大丈夫という神話みたいなものがありましたが、今ではMacも狙われます。実際に数年前に仮想通貨関連で大きな被害があった企業はMacを狙われて侵入されたようです。

VPN 機器からの侵入

もう一つの手口として、最近特に取り上げられるのがVPN機器からの侵入パターンです。一時期、FortiGateの製品が問題になりました。侵入後、アクティブディレクトリなどに上手く権限昇格されてウイルスをばらまかれてしまい、さらにいろんな端末やサーバーに侵入されていくというようなケースです。最近はFortiGate以外のネットワーク機器もターゲットになることがありますので、他のものでも危ないです。

今は数ヶ月程度かけて侵入されることが増えています。なぜそんなに時間がかかるかというと、犯罪者側は中に侵入した後、まずはどこにどんな情報が入っているのかを探索するためです。本当に価値のある情報を取得するため、実際に侵入した端末から社内のネットワークにどんな情報があるのかを調べ、本当に貴重な情報を取得していくというような形でステップを踏んでいきます。リードタイムがあるということを踏まえると、そこに対策の一つの指針が見えてくるかもしれません。

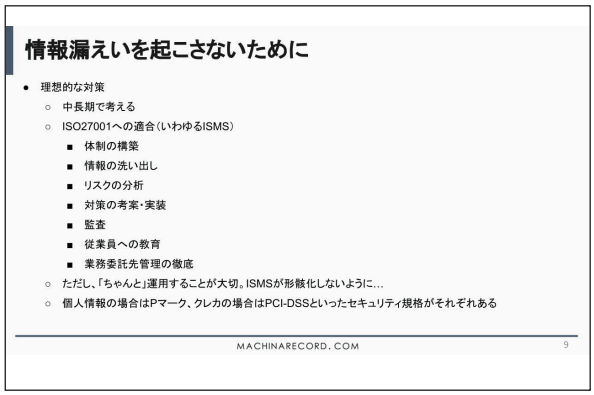
他にも、昔からある手口ですがアプリケーション側の脆弱性から侵入される場合もあります。SQLインジェクションや、ファイアウォール・サーバーの設定ミスなどで中に侵入されるケースがあります。

一方、内部の情報漏えいは、社員から情報を持ち出してしまうケースがあげられます。これには怨恨や金銭目的などがあります。あとは先ほどあげた北海道ガスさんの事例のように紛失するケースもあります。

海外の事例で、攻撃を仕掛ける際に犯罪者側が中の社員にお金を払って、社内情報を取得するケースも多々あります。一例をあげると、携帯電話のキャリア会社の中でカスタマーサポートなどのオペレーションの担当者をリクルーティングして、SIMカードに紐づいている携帯番号を書き換えていたというケースがあります。クレジットカードで決済したり銀行にログインする際、SMSの認証が必要なときにSIMカードの番号を数分だけ切り替えてしまうのです。そうすると本人も気づかないまま、勝手に自分の番号が犯罪者に割り当てられて、SMS認証を実行されてしまいます。

そのような社内での内部犯罪が活発に行われるなど、本当にいろんな形で犯罪者が攻撃を仕掛けてきます。隙があると大きなリスクに繋がっていきます。昔みたいにファイアウォールとか、ネットワークの出入口だけ見ておけばいいという時代は既に終わってしまったといえます。

情報漏えいを起こさないために



理想的な話で言えば、中長期に考えていく必要があります。ISO27001（ISMS）の要求事項にのっとって体制を構築していってセキュリティをしっかりやっていくのが、おそらく一番理想的です。

ISMS に関しては、20 年以上前からこの規格自体はあってオペレーションを回しているところもあって、取得していても事故を起こしてしまった企業もたくさんあります。ただ、ISMS 自体が求めていることは非常に理にかなっています。規定されているセキュリティの要求事項を一つひとつちゃんとこなしていけば、一定レベルのセキュリティは必ず担保される仕組みになっています。

セキュリティ対策をこれから始めていこうと考えているのであれば、ISMS を取得していくことが一番簡単なセキュリティ対策になります。取らないにしても、考え方として必要になってくるので、それに基づいてセキュリティの体制を構築していくことになります。仕組みや体

制の構築、セキュリティ体制をどう運営していくかなど、戦略を立てる組織と責任者が必要になってきます。

ISO27001 への適合

専任の担当者が必要かどうかは、企業の規模にもよりますが、100 人未満の会社であれば、おそらく専任担当者は必要ないでしょう。ただ、300 ～ 400 人ほどの組織になると、間違いなく専任で 1 ～ 2 人は必要になってきます。1000 人を超える企業になれば 5 人ぐらいのチームで回していくことになります。

次に情報の洗い出しやリスクの分析についてです。これらはセキュリティをやっていく上で自社がどんな施策をすべきかの道筋を作るために実施します。

情報の洗い出しは本当に重要で、自社の中に、具体的にどのように情報が保管されているか、どんな情報があるかを把握してパッと言える人がいるのか。ちゃんと集約されているかどうか。顧客情報や契約に関する情報、自分たちのプロダクトに関する情報など、個人情報だけではなく、あらゆる情報に関してちゃんと洗い出しておきましょう。

情報の洗い出しのあとは、その取り扱いに関してどんなリスクが存在するのかを分析する必要があります。これは情報のインとアウト、どのように情報を入手して、それをどこで管理して、どのくらい保存して、誰が使って、どんなアクセス権で使っていて、最後に使い終わったらどのようにそれを削除するのか。「情報のライフサイクル」と呼ばれますけど、どのように行われていくのかっていうのをつぶさに一つひとつステップを追っていく必要があります。

例えば入手する際にどんなリスクがあるのか。管理する際にどんな経営リスクがあるのか。それを保管している情報を誰が見れるのか。情報を見るときにどんなリスクがあってどんな対策をしているのか。情報を削除や移動するときに、どんな対策が打ち出されているのか。それぞれの情報のリスクをきちんと分析して初めて対策・施策を打ち出すことができます。そして実際にそれを実装していくまでの一連の流れをしっかりとやっていく必要があります。

次に監査についてですが、情報を見つけ出して、それを分析して対策を考えて実行する流れがちゃんとできているか、第三者の客観的な視点で監査します。

ここまでがいわゆるマネジメントシステムになるのでこれがちゃんとできると、ISMS もちゃんと回せるよという話になります。

この仕組みについて実際にやってみると確かにその通りだよねと思うことが多々あります。私も以前会社の中でセキュリティ担当をやっていたんですが、ISMS への対応は面倒くさいと肌で感じていました。実際に回すのは嫌だなとも思っていたんですが、あとで冷静に規格を読んでみると、「確かにこれはこの通りだな、これを実際に実装しないとセキュリティ

は担保できなそうだな」とだんだん分かってきたところがありました。皆さんも参考にしていただくといいんじゃないかなと思います。

あとは従業員の教育です。会社の中でセキュリティに関するリテラシーを上げていく必要があります。e ラーニングなどのコンテンツもありますし、座学でもいいと思います。

最後に、抜け穴になりがちなのが、業務委託先の管理の徹底です。過去の内部からの情報漏えいの事例では、私が初めてセキュリティの世界に携わるきっかけになった YahooID 漏洩事件がありました。400 万件ぐらいだったかと思いますが、ヤフーの関連会社の契約社員が情報を盗んで、それを脅迫に使った事件でした。少し前にベネッセで情報漏えいがあったときも、契約社員が情報を取得して、それを他に売却していました。

正社員でも業務委託でも会社に対するロイヤリティの大きさはあまり変わらないかもしれませんが、業務委託の人たちがどんな情報を管理しているのか、どんな情報を渡していて、どのようなセキュリティ対策をしていて、こちらが指し示した通りの意図で情報管理しているのか、ちゃんと把握する必要があります。

また、最近の企業は多かれ少なかれ何か外部サービスを使っているかと思いますが、クラウドサービスの SaaS を使っている場合、そちらも洗い出しておく必要があります。利用先のクラウドサービスが情報漏えいを起こすと、引きずられて自分たちの情報も漏えいしてしまいます。その責任が誰にあるのかというと、そのサービスを使うという決断をした会社が悪いと判断されます。

利用するクラウドサービスが本当に正しいセキュリティ対策を実装しているのかどうか、ちゃんと調べておいたほうがいいです。必要があれば利用するサービスの会社に対して、管理をちゃんとしなさいとプレッシャーをかけたり、セキュリティチェックシートを用いることもしましょう。人的な業務委託だけでなく、サービスの委託先に関しても徹底的に管理する必要があります。

ISMS が形骸化しないよう「ちゃんと」運用することが大切

一連の対策ができたとして、注意しなければいけないのが形骸化です。ISMS は取ってからが始まりといってもいいものです。取ってはいるけど、現在は全然セキュリティ対策をやっていない「名ばかりの ISMS」の企業がたくさんあります。そういう企業が情報漏えいを起こすケースが多いです。責任者が、マインドやモチベーションを常に上げながら、形骸化しないようにしっかり運用していかないといけません。ここが一番大変です。

今回は ISMS を例に挙げましたが、例えば個人情報であれば、国内に限った話ですが、プライバシーマークが規格としてあります。クレジットカードの場合は PCI-DSS という世界標準の規格が別にあります。それぞれフォーカスする部分が違うものの、自社が提供するサービス次第で、プライバシーマークや、PCI-DSS を基準にしてもよいと思います。

今すぐにできる対策としての EDR 導入

ここまで長期の対策についての話をしてきましたが、今すぐできることを知りたいという方もいると思いますので、すぐにできる対策も考えてみました。

対策の 1 つとして、マルウェア対策である EDR（Endpoint Detection and Response）の導入があげられます。すでに何かのマルウェアが入っているかもしれないという不安を払拭できます。

既存のマルウェア対策、いわゆるアンチウイルスソフトでは、今の新しい攻撃に対しては絶対大丈夫とはいえません。肌感的には、防御力は 2 割ぐらいしか上がってないんじゃないかなと思います。最近のサイバー攻撃は本当に誰も知らないセキュリティの脆弱性をついてきます。今までのアンチウイルスソフトは、世の中に一通り周知された攻撃手法に対して、パターン化して保管しておくことで検知する仕組みですので、誰も知らない穴を突かれて入られてしまうケースがあります。

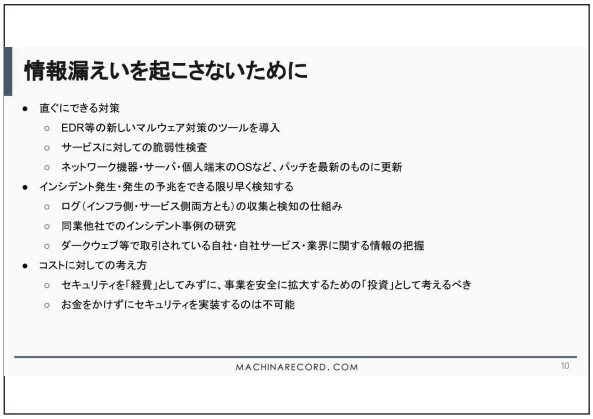
EDR はマルウェアが悪さをする際の特徴的な動きを検知します。社内の端末が潜入されているかは EDR を使うことで一定程度分かります。ただ、EDR も実際に運用すると、偽陽性というか、感染していないのにアクティビティとして怪しいみたいなものもあって、運用が大変だと言われます。ですから実際にセキュリティのアラートを監視していく人やチームが必要になってきます。企業によっては、監視を外部に依頼するケースもあります。当社でも対応しています。ただ、脅威を洗い出して現時点で感染していないとわかるだけでも安心できます。

EDR は最近すごく需要が伸びていて、国内では 3 ～ 4 つの著名な製品があります。当社では CyCraft という台湾の製品を扱っています。なぜ台湾のものかというと台湾は中国からの攻撃が多い。そして日本も中国からの攻撃が非常に多いので、その親和性もあって選んでいます。ほかにもアメリカやイスラエルの製品などがあり、それぞれちょっとずつ特徴が違うので、まだご導入されてない方は、ご検討していただくといいです。

もし情報漏えいが起こったら、必ず EDR を入れることになります。そのときに導入となると高額になってしまうので、今予算があるのであれば、火事が起こる前に導入しておくといいでしょう。

対外的な説明責任としても有効なサービス脆弱性検査

あとは昔からよくあるものとして、サービスに対しての脆弱性検査があります。Web ベースのアプリ系セキュリティ検査や脆弱性検査、ネットワーク周りのセキュリティ検査などがあります。これは実際に安全かどうかを確かめるとともに、対外的な説明責任としてもやっておいたほうがいいです。脆弱性検査をやっていなくてセキュリティ事故が起きたら、なぜ今までやっていなかったのかということになります。外に向けてアピールするためにも、年 1 回でもいいので必ずやっておきたいです。



必須の対策となるセキュリティアップデート

すぐできる対策の最後は、ネットワーク機器・サーバー・個人端末の OS などに最新のパッチをあてることです。これも本当にやったほうがいいです。最低限のことではありますが意外と効果的です。脆弱性が何か見つかったと情報が出てきたら、迅速にパッチをあてましょう。

サーバーのバージョンアップは結構大変ですが、最近サーバー側での脆弱性の話はあまりないです。年 1 回くらいすごく大きいのが出るかくらいです。頻度は高くないので、どちらかというと皆さんの Windows や Mac 端末。そしてネットワーク機器についても、ルーターやファイアウォール、VPN は必ずアップデートしてください。やっていないとほぼ間違いなくやられます。

被害を最小限に抑えるためにすべきこと

次に情報漏えいが起きそうなとき、もしくは起きてしまった際に被害を最小限に抑えるためにすべきこととして、社内のインフラ側もサービス側も、実際にどんな攻撃を受けているのかをいかに迅速に検知できるのかが重要です。実際にサービスをやられてる方なら分かると思いますが、サービス側はほぼ毎日すごい数の攻撃が来ます。インフラ側も VPN などの外側に向いてる口があれば、そこも間違いなくスキャンされてて攻撃の対象として扱われますので、ログをちゃんと追っていく必要があります。

あとは侵入されて何か不正な行動をされているときに、それに気づけないといけないので、見られるログはすべて見て監視できるようにしておきましょう。収集と検知の仕組みが重要になってきます。

また、大企業でセキュリティ対策も既にある程度しているようであれば、同業他社のインシデント事例の研究などもするといいでしょう。さらにダークウェブをモニタリングして、取引されている認証情報や、クレジットカード番号、自分たちの会社や情報資産に対しての攻撃に関する予兆などがないかも見ておきたいです。

世の中のメディア情報も含めて、自社の業界に対してどんな攻撃がされているかのトレンドの把握もセキュリティ対策を考える上で重要になってきます。もし同業他社がやられていれば、自分の会社も同じ形で攻撃される可能性がありますし、犯罪者から価値がある業界だと思われていることが多いので、比較的ターゲットにされやすいと思ったほうがいいでしょう。

あとはセキュリティへのコストに関しての考え方について。こちらはすごく大きな議論になると思います。コストをかけずにセキュリティを実装するのはほぼ不可能で、どうしてもお金がかかります。外部のサービスをある程度使うことになると思いますし、もしすべて自分たちでやろうと思えば大きな人件費がかかってきます。

会社としてそれを経費として考えてしまうと「なぜこんなお金がかかるのか」と思ってしまいがちです。ちょっと考え方を変えて「これは事業を安全に拡大するための投資である」と考えていかないといけません。

「セキュリティ対策はお金がかかるから今はできない」とおろそかにしていると、事故が起こったときに大きな被害が出ます。業務が何カ月も止まって、本来であれば得られていた機会を逸失してしまいかねません。それが起こらないための費用対効果のバランスを見ながら予算をかけて対策をしていく必要があります。

「うちは大丈夫」と思っている企業は、本当に「大丈夫」と言えるのか。もちろん本当にちゃんとセキュリティ対策をやっている企業であればいいのですが、今まで何もやったことがないのに、特に根拠なく大丈夫だと思っている企業はちょっと怪しいです。そんなに自信を持って大丈夫だなんて、今は絶対に言えません。

インシデントハンドリング

実際に事故が起こってしまうケースもあると思います。どんなに対策を打っても、全部機械でできるわけではないので、どうしても人的エラーが出てきます。100% 大丈夫という状態にはできなくて、多分 90% ぐらいまでしか防げません。何かが起こってしまったときには冷静に受け止めて、いかに被害を最小限に抑えるか、仕組みとして考えておいたほうがいいです。

初めてセキュリティ対策をする場合には、セキュリティ対策が実装できるまでの間に事故が起こるかもしれないので、まずはインシデントハンドリング、事故対応のフレームワークを作っておくほうが優先順位として高くなります。

まず公表するか否かの判断です。経営者の方々は本当に頭を悩ませる問題です。個人情報が漏洩している場合は、保有している方にちゃんと告知しなくてはいけないので、有無を言わせず公表せざるを得ません。一方、個人情報ではない部分で漏えいが起こってしまった場合は判断が難しいです。個人的には、ほぼ全ての案件でインシデントが起きたら公表し

たほうがいいと思います。なぜかというと、黙っていてどこかで判明すると、非常に印象が悪いからです。公表して誠実に対応していくほうがいいと思います。

個人のお客様が紐づいてるケースで、かつそれが例えば数十万数百万件とかになると、問い合わせが殺到するのでコールセンターの準備も必要になります。もしそういったたくさんのお客様が影響を受けそうなサービスを運営されているのであれば、事前に何かインシデントが起こったときのために、スムーズにコールセンターを構築できるための下準備をしておくといいです。コールセンターの企業と段取りをつけておくといいでしょう。

次に被害を最速で止めることです。ここも重要な判断になってきます。現場の人たちがどう動くかになりますが、被害をどうやって最速で止めていくか。「なぜそれが起こったのか」という一番根本的な原因究明よりも先に、まず被害を抑えることが重要です。

そのあとに証拠保全や警察との連携になります。もちろん警察に届け出る必要があります。ただ、警察はよほどのことがない限り、あまり積極的に動いてはくれません。犯人を捕まえるなどは、かなり難しいかと思います。サイバー犯罪の場合だと国籍が違うケースも多いので、それが逮捕に至るっていうケースはかなり低くなります。あとは被害者への賠償です。これもよく議論になります。昔は 500 円のクオカードなどを配るなどしていましたが、最近はあまりなくなってきました。

インシデントが起こってしまっても、向き合い方次第で最終的には高評価に繋がるケースも結構あります。その会社が信用に値する会社なのかの評価は、インシデントが起こった後にどれだけ誠実に対応できるかによっても大きく変わります。真摯に「何が起こってどう対応して今こうなっています」というのをちゃんとお客様に報告し進捗を公表していくのが重要になります。

インシデントハンドリングでは CSIRT（Computer Security Incident Response Team）という枠組みがあります。自分もヤフーとかミクシィで CSIRT を構築していました。インシデントに対して、チーム作りをどうするべきか、どう考えればいいかなどのガイドラインがあるので、セキュリティの専門チームがなくても、この CSIRT は作っておいたほうがいいです。

事故が起こると、広報、法務、経営管理など現場以外も含めた様々な部署が絡みます。誰がディレクションして、どう連絡や意識のすり合わせを進めるか、準備しておくことが大事です。事故が起こるとものすごく混乱して情報経路が錯綜するので、最初に一本化しておくことも重要です。

以上、セミナーの内容をお伝えしました。

これからセキュリティ対策を始める BtoB 企業を対象にしたオンラインセミナーシリーズ第 2 回目となる今回は、情報漏えいリスクと求められる対策について。サイバー攻撃や内部不正による情報漏洩を予防するための対策を解説しました。

株式会社マキナレコードでは、この他にも BtoB 企業のセキュリティ対策に関するセミナーを開催しております。ぜひご参加ください。

株式会社マキナレコードについて

サイバー犯罪は非常に多様化しており、犯罪者たちはその形態を単身犯から組織的なものへと移行してきています。犯罪者間での情報交換は、司法機関がその対応策を施行する以上のスピードで行われており、今後はプロアクティブなセキュリティ対策が必須になります。

株式会社マキナレコードでは、日本の市場にあわせたサイバーインテリジェンスを提供し、クライアントにおける既存のセキュリティ体制を強化し、果たしてインターネットのみならず、社会全体をより安全なものにしていくことを目指しています。

登壇者紹介

軍司 祐介

株式会社マキナレコード　代表取締役 CEO

プログラマを経て、セキュリティ専門家として、ヤフー、ミクシィ、楽天などでセキュリティ向上に寄与。
各組織で CSIRT チームの構築や、M&A 時のデューデリを含む各種アセスメント、セキュリティ施策の設計・運用など、セキュリティ分野において 10 年以上の経験を持つ。

本資料は 2022 年 3 月 29 日に開催されたセミナー「これから始めるセキュリティ対策〜情報漏えい対策〜」を元に編集を行い制作しています。株式会社マキナレコードでは、その他にもセキュリティに関するセミナーを開催しております。ご興味をお持ちの方は是非ご参加下さい。
イベント開催情報：https://machinarecord.com/news/

MACHINA RECORD

Cyber Threat Intelligence

お問い合わせ　株式会社マキナレコード　〒105-0001　東京都港区虎ノ門 1-2-15 YS ビル 6F　https://machinarecord.com/