SEMINAR REPORT

スタートアップ、中小企業のセキュリティ入門
これからはじめるセキュリティ対策

登壇者

株式会社マキナレコード
シニアコンサルタント
戎 正人

MACHINA RECORD
Cyber Threat Intelligence

これから始めるセキュリティ対策。優先順位や情報の取り扱い、人員まで一挙解説。

マキナレコードでは、2022年1月18日、セキュリティ対策をこれから始めようとお考えのスタートアップや中小企業向けに「これから始めるセキュリティ対策」をテーマにセミナーを開催しました。 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。

中小企業でも必要なセキュリティ

セキュリティ対策は大企業だけのものではありません。今は中小企業でも、セキュリティ対策が必要になっています。

たとえば大手企業がお客様になるようなBtoBビジネス、特にクラウドサービスで事業を展開する場合は、セキュリティの要求事項が強く求められます。また、エンドユーザー様の個人情報などの金融決済情報を取り扱うようなBtoCビジネスも非常にセキュリティが強く要求されます。

セキュリティ事故が起きると、さまざまな被害につながります。IPOを目指していた企業が上場直前にセキュリティのインシデントによって、IPOできなくなってしまったケースや、事業廃止になるケースなども起きています。

今や「ビジネスにセキュリティは必須」の時代と言ってもいいでしょう。セキュリティ事故は対岸の火事ではありません。不正アクセスの手法（エクスプロイト）は広く公開されていて、何も対策をしなければ簡単に侵入されてしまう時代です。性善説ではなく性悪説で対策をしていく必要があります。

セキュリティ対策へのコストは、信用と安心を得るために必要な投資として考えていかなければなりません。

これからはじめるセキュリティ対策

スタートアップや中小企業でIPOを目標にしている会社は多いでしょう。では、そのような会社はどこまでセキュリティ対策を考えなければならないのでしょうか。

前項で説明した背景などを鑑みて、やっておきたい対策は右記の通りです。

どこまでセキュリティをやるべきか

- セキュリティ事故が発生した場合のエスカレーションフロー
- ルールを守るためのセキュリティ規程の整備
- 社内で取り扱っている情報種別の洗い出し
- できる限り保管場所、削除ポリシーは定めておくべき
- 社内で使っている他社サービス（SaaS等）の洗い出し
- セキュリティを常に念頭に置いたサービス設計
- 委託先の選定は慎重（人や会社、使用しているクラウドサービス）
- 個人情報を取り扱っている場合は経産省のガイドラインは一読する
  - EU圏の個人情報の場合はGDPRマスト
  - 取扱責任者任命、目的に沿った使用、プラポリの公表は必須

セキュリティ規程の整備など社内のルールづくりのほか、社内で使う他社サービスの洗い出し、委託先の選定なども必須といえます。さらにセキュリティを念頭に置いたサービス設計がなされているかもIPOでご支援をする監査をする監査法人から強く要求されます。

また、個人情報を取り扱っている場合には、経済産業省のガイドラインを理解する必要があります。さらにワールドワイドな事業を考えていて、EU圏の個人情報を扱う場合はGDPRへの対応が必要です。

特に昨今、取り扱いが増えている情報に医療ヘルスケア関連情報、GDPRに関連する情報、個人情報があげられます。
自社の事業がどういった情報を扱っているか、どういった業種を狙っていくかによって、IPOを準備する際にこれらの情報に関してのチェックも必要になってくる場合があります。

ISMS や P マークの必要性

セキュリティ対策として、ISMSやPマークなど、第三者認証を取得する企業も増えています。自社内でのチェックではなく第三者にセキュリティ状況を審査してもらって取得するもので、セキュリティが確保されている証明となります。内外に対してセキュリティに関する信頼を得ることができ、非常に大きなメリットがあります。また、継続して認証基準をクリアすることで適切にセキュリティ運用をすることができます。

セキュリティ関連規定について

規格名	認証範囲	対象情報	特徴	取得予算	コンサル	最低工数
Pマーク	国内のみ	個人情報	個人情報保護ガイドライン、運用は難しくない 2年毎更新、信用度中、形骸化多発	50万～ 拠点依	60万～	半年～
ISMS	世界	全企業	ISO27001シリーズ、適用範囲が広いと運用が大変 1年毎レビュー、信用度高、形骸化すると維持が困難	50万～ 拠点依	120万～	9ヶ月～
PCI DSS	世界	クレジットカード	経産省ガイドライン、PCI SSCが定める業界標準 技術的な運用内容が多い、年次監査、信用度高	100万～ 規模依	200万～	1年程度
FISC	国内のみ	金融商品	金融庁ガイドライン、運用度高度、信用度高 通貨を扱う銀行などの金融機関向け	-	N/A	1年～
SOC2	世界	IaaS等	米国公認会計士協会ガイドライン、運用はとても大変 年次監査、信用度最高	1500万～	N/A	1年以上
ISMAP	国内のみ	政府関連情報	選定されたばかり、監査/コンサル可能な会社は僅か 政府～地方自治体案件の入札基準を想定	1000万～	N/A	1年以上

改正個人情報保護法への対処

セキュリティ対策での重要なポイントのひとつが個人情報の取り扱いです。個人情報を取り扱う際の注意点や、2022年4月に施行される改正個人情報保護法のポイントを説明します。

個人情報はどの企業でも取り扱うものです。企業では、従業員の個人情報に始まり、お客様、取引先の情報などを扱います。何らかの形で必ず個人情報保護法を意識する必要があります。法律を守るためにも個人情報保護のガイドラインは必ず読んでおくべきです。さらに、EU圏の個人情報を扱う場合には、EUの個人情報法に相当するGDPRも読まないといけません。

個人情報保護法では、情報の取扱責任者を明確にし、目的を開示して利用に対して同意を得る必要があるなど、厳しい取り決めがなされています。情報の取り扱いについても、どんな個人情報を扱っていくかなど、プライバシーポリシーを決めておかないといけません。

個人情報保護法は3年ごとに見直されることが法律で決まっていて、2022年の4月から改正法が施行されます。4月からのポイントとして、インターネットで閲覧時に広くやりとりされるCookieという仕組みについて、事前に同意を得るなど運用の見直しが必要となる可能性があります。

また、国外に情報を保存する場合のルールなどもあわせて厳格化されるなど、GDPRを意識した改正内容となっています。GDPRを国際的な個人情報保護の一つのベースラインとする動きが進んでいます。

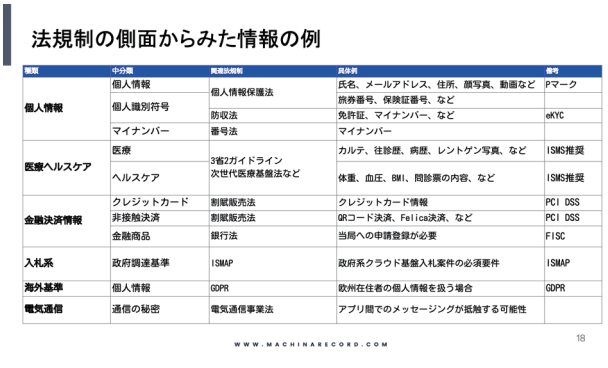
プライバシーポリシーなどを既に自社Webサイトに掲載されている場合には注意が必要です。制定年月日などの日付が古ければ、それだけで法改正に対応していないことがばれてしまいます。ちゃんと2022年4月の改正に合わせて見直しをしていかないといけません。

ISMS や P マークの必要性

セキュリティを考える際、そもそも法律の上で事業やサービスを提供していく必要があります。日本でも特にリスクが高く、影響範囲が大きい事業やサービスに関しては法律でセキュリティに関する規制が定められています。

今の時代、必ず何かしらの法規制が入っていると認識して、どんな法律を守らないといけないかを意識していかなければなりません。

たとえば、金融のサービスを提供する場合には、関係する法律にセキュリティ対策が



法規制の側面からみた情報の例

種類	中分類	関連法規制	具体例	参考
個人情報	個人情報	個人情報保護法	氏名、メールアドレス、住所、顔写真、動画など	Pマーク
	個人識別符号		旅券番号、保険証番号、など	
		防収法	免許証、マイナンバー、など	eKYC
	マイナンバー	番号法	マイナンバー	
医療ヘルスケア	医療	3省2ガイドライン 次世代医療基盤法など	カルテ、往診歴、病歴、レントゲン写真、など	ISMS推奨
	ヘルスケア		体重、血圧、BMI、問診票の内容、など	ISMS推奨
金融決済情報	クレジットカード	割賦販売法	クレジットカード情報	PCI DSS
	非接触決済	割賦販売法	QRコード決済、Felica決済、など	PCI DSS
	金融商品	銀行法	当局への申請登録が必要	FISC
入札系	政府調達基準	ISMAP	政府系クラウド基盤入札案件の必須要件	ISMAP
海外基準	個人情報	GDPR	欧州在住者の個人情報を扱う場合	GDPR
電気通信	通信の秘密	電気通信事業法	アプリ間でのメッセージングが抵触する可能性	

法規制の側面から見た情報の例

定められています。特にクレジットカードなどは漏洩したときのリスクが非常に大きく、悪用されればすぐにお金に換えられてしまいます。そのように金銭価値が高いような情報には非常に厳しい法律の規制がかかっています。ECサイトを運営する場合もそういったところを意識しておかなければいけません。

また、医療ヘルスケア業界についても、電子カルテなどは特にプライバシー性が高く、機微情報です。そういったものを扱う業界なので、当然それに関連する法律などが多くあります。

さらに、昨今は自社以外の事故、いわゆる委託先や使っているクラウドサービスなどの事故でも選定根拠や管理監督責任を問われるようになってきています。便利で低コストなサービスも増えていますが、それを使ってサービスを組み立てて万が一そこから情報が漏れれば、自分たちも選定責任や監督責任を問われることになります。自社の法規制への対応はもちろん必要ですが、自社の中でどうにかできる範囲ではない外部サービスなどについても、本当にそのサービスを使っていいのか、慎重にやっていかないと、非常に大きなインシデントとなる可能性があります。

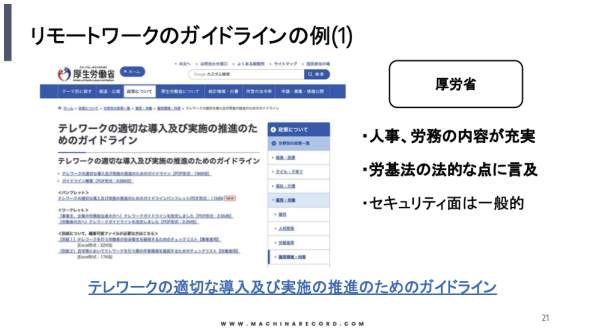
そのため、そのような点も踏まえてサービスを作っていかなければなりません。開発ではセキュリティを意識した標準プロセスを定めていく必要があります。たとえばコードレビューを入れる、リリースするときの基準を定める、自社のシステムのセキュリティ基準を定めておくなどです。

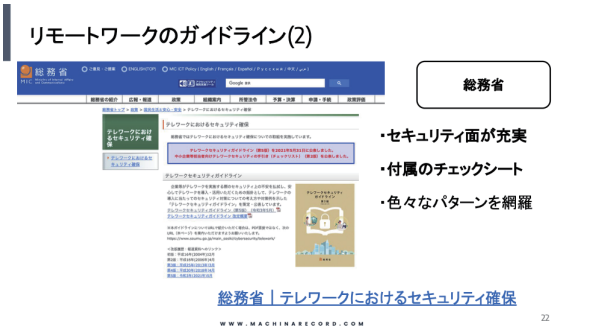
これらのことをしっかり整備しておかないと、未然に防げる事故を防げなかったり、もしくは起きたときに事故対応があまりうまくいかずに、事故の範囲が拡大したりします。会社にとって大きなレピュテーションリスクになりかねません。

リモートワークの併用

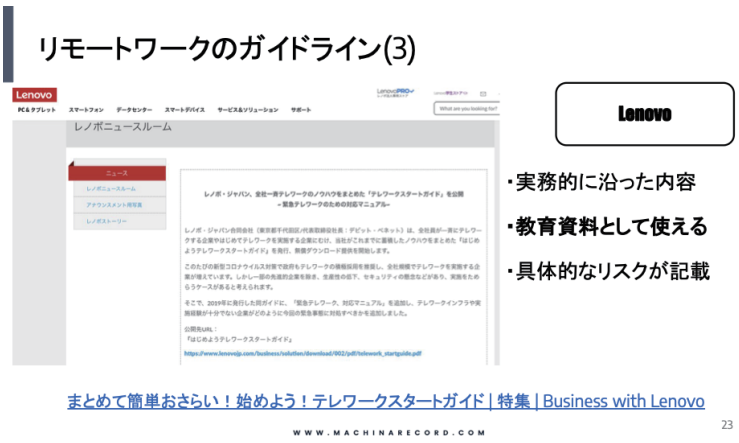
今はリモートワークを実施している会社が非常に多くなっています。コロナ禍の収束が見えず、リモートワークを前提にしている会社も増えています。

リモートワークに関するガイドラインはさまざまなところから出されています。たとえば国、省庁などです。こういったものをしっかり理解して、自社のリモートワークの基準にしたり、参考にできたりするといいでしょう。





他にも、企業が出しているものもあります。たとえばLenovoはマニュアルを公開しています。もともと従業員の方向けの資料で、そのまま使えるような内容になっています。具体的なリスクなども書かれているので、リモートワークを整備する際には参考になります。



当社でもいろんなお客様のセキュリティのところのご相談を受けている中、特にコロナ禍が始まってからは、リモートワークに関連するご相談やお問い合わせが増えています。

リモートワークで気をつけたいポイントとして、VPN接続に関する課題があげられます。VPNは社内のファイルサーバーに自宅のインターネットを介して社外から接続する場合や、グループウェアを使っていく際などに使われるもので、特に外部から狙われます。
このVPNのどこを狙えばいいかの情報は広く出回っていて、対策を行っていないVPN装置のリストも流出しています。VPN装置のファームウェアのアップデートなど、必要なセキュリティ対策がされていなければ、外部から侵入される可能性は高くなります。そうなれば情報漏洩のリスクやランサムウェアの被害、さらに上場企業であれば決算報告の遅延も起こりえます。

また、クラウドサービスを使う際も注意が必要です。誰でも自由にさまざまなクラウドサービスが使えるような時代になり、非常に便利な一方で、利便性とセキュリティは相反しますので、利便性が向上するとセキュリティは低下します。

社員が目に見える範囲にいないリモートワークでは、クラウドサービスの利用についてしっかり管理ができないケースが出ています。そのため、必ず社内で利用に関する基準を作っておく必要があります。無料のクラウドサービスを使ったとき、規約によっては保存しているデータをクラウドサービスの事業者側の都合で第三者に提供しているかもしれません。外部サービスを精査せずに利用すると、このような情報漏洩のリスクを背負うことになります。さらに、利用の基準を会社で定めていない場合は「なぜそんな危ないサービスを使わせているのか」と選定責任を問われることにもなります。

ほかにも、私有PCやスマートフォンを使っての業務に関する基準も作っておかないと、個人で好き放題にやってしまいかねません。そういうことが起きると、IPOを準備する際にITの統制ができていないと評価されてしまいます。

GDPR の扱い方

今後海外展開などを考えている企業、特にEU圏のお客様が利用する場合はGDPRへの対応が必須となります。例として旅行サイトなどがあげられます。EUのユーザーの情報、ビッグデータの分析などを含めて、情報を扱う場合はデータ保護責任者が必要になります。

また、重要な要素のひとつに「移転」という概念があります。GDPRには「十分性認定」といわれるものがあり、EU圏外に情報を移す場合、十分性認定を受けている国、つまりEUがOKを出している国かどうかを厳しく見られます。クラウドサービスを利用する際は、十分性認定を受けていない国を保存場所としていないかまで考えて使わないといけません。

大手のパブリッククラウドベンダーであれば各国に分散して情報を保存していることもあります。どこに保存するかを選べるケースであれば、保存場所をしっかりと考えなければなりません。委託先や利用するクラウドサービスの厳密な管理が要求されます。

日本の個人情報保護法を守っているだけではGDPRの対応までできないのが現状です。例として、GDPRではIPアドレスや携帯電話番号も保護をしないといけない情報になります。そのあたりも考慮しなければなりません。

専任担当者の必要性

セキュリティを会社で整えて守っていくにあたって、専任担当者を置くべきかというご相談を受けるケースが多くあります。

まず、責任者は絶対に置くべきです。社長でも情シスの方でもいいでしょう。委託先の監督責任や選定責任など、会社としてその判断の責任を明確にすることで、ステークホルダーへの説明責任を果たせる状況を作っていくことが非常に大切です。

ただし、専任担当者を雇用するのは現実的に難しい状況です。日本ではエンジニアが慢性的に不足していて、さらにその中でもセキュリティの専門家はとても少なくなっています。スタートアップや中小企業では、なかなかセキュリティを専任で担当する人材というわけにはいかず、開発や情シスと兼務させることが多いです。実際に当社のお客様でもそういったケースが多く見られます。ただ兼務ではどうしても負荷が大きくなり、抜け漏れが起きやすくなります。セキュリティはやるべきことが多く、しっかり手当していく必要がありますので、現実的にはセキュリティに詳しいベンダーなどを入れながらやっていくことになるでしょう。

ケーススタディ紹介

セミナーでは実際に当社がご対応した例もいくつかご紹介しました。
ご予算感や各種セキュリティ規格取得の有無、サービスの脆弱性検査など、様々なご希望に応じて対応が可能です。お気軽にご相談ください。

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

戎 正人
株式会社マキナレコード　シニア・コンサルタント

長年のシステム構築運用を経験した後、監査機関にて PCI DSS QSA（Qualified Security Assessors）として、金融機関やカード会社をはじめ、クラウド利用が多いスタートアップベンチャーなど数十社の PCI DSS 監査及び、準拠に向けた体制 / 業務構築支援を実施。2019 年より現職。

本資料は 2022 年 1 月 18 日に開催されたセミナー「ースタートアップ、中小企業のセキュリティ入門ー これからはじめるセキュリティ対策」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/