NET ASSIST
24/7 Guardian Deity

NEWS LETTER

2022.03
#11

TOPICS

急増するサイバー攻撃と標的型メール攻撃の脅威

3月1日、トヨタ自動車は仕入れ先で自動車の内外装部品を手掛ける小島プレス工業のシステムがサイバー攻撃を受けてダウンしたことを理由に国内のトヨタ全工場の稼働を停止しました。小島プレス工業では2月26日にサーバーの障害を検知し、ウイルス感染と脅迫メッセージの存在も確認しています。具体的な感染経路や脅迫の詳細などは3月7日現在、公表はされていませんが、ウィルス感染と脅迫を受けていることから**ランサムウェア**(※注1)による攻撃とみられています。

サイバー攻撃はオリンピック等の国際イベント開催時だけでなく、コロナ禍のような情勢不安なタイミングに乗じて急増する傾向があります。今回、小島プレス工業でウィルス感染が確認された26日前後もウクライナ情勢による混乱に乗じてサイバー攻撃が急増していることがセキュリティ連盟のデータからも確認が出来ました。

セキュリティ連盟ニュースリリース

https://prtimes.jp/main/html/rd/p/000000003.000095631.html

こういった事態を受けて、同日(1日)には経済産業省や警察庁などの関係省庁は国内の企業などにサイバーセキュリティー対策の強化を求める注意喚起を発表するなど、業界内だけでなく国内外にとても大きなインパクトを与えました。

サイバーセキュリティ対策の強化について(注意喚起)

https://www.meti.go.jp/press/2021/03/20220301007/20220301007-1.pdf

注意喚起の中には「サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。」と記載がありますが、**サプライチェーン攻撃**(※注2)を考慮すると、自社の知名度や事業規模に関わらず、多くの企業が今回の注意喚起の対象になるのではないでしょうか?

(※注1)
ランサムウェア

身代金の要求を含んだウイルスの総称です。遠隔操作やパスワードを盗むなどしてシステムに侵入し、ファイルを暗号化して使用できなくしたうえで、元に戻したければ金銭を要求します。

(※注2)
サプライチェーン攻撃

サプライチェーンとは供給連鎖という意味で、材料や部品の調達から製造、物流、販売など仕入れから供給に至るまでの一連の工程のことを呼びます。この一連の共有連鎖網を悪用したサイバー攻撃がサプライチェーン攻撃です。
前述のトヨタ自動車などの大企業はセキュリティ対策に予算と時間を費やしてシステムは堅牢に要塞化されていますが、その取引先となる数百の企業の中にはセキュリティ対策が不十分な企業もあり、そういった企業が抱えている脆弱性を狙って感染を連鎖的に広げていき、ターゲットとしている大企業へ被害を及ぼします。

よく耳にするEmotet(エモテット)とは

前述のランサムウェアの代表格がEmotetです。2019年11月頃から猛威を振るい、世界的に有名になりました。2021年1月、ヨーロッパでの取り締まり強化によって一旦収束しましたが、2021年11月から活動が再開されIPA(日本情報処理推進機構)からも注意喚起されています。

Emotetは、主にパスワード付きZipファイルとしてメールに添付する形式で配信されます。これまでの標的型メール攻撃と違い、過去実際にあったやり取りの内容や企業名などを利用して、攻撃メールを送るため、誤って開封し感染をしてしまうケースが後を絶ちませんでした。2021年11月、当時の日本政府はパスワード付きのZipファイルをメールで送るPPAPの廃止を発表しましたが、これもEmotetの流行がきっかけと言われています。もし誤ってEmotetに感染してしまった場合、メール情報や連絡先情報を悪用した攻撃メールが社内だけなく取引先などの関係各社にも送信され、サプライチェーン攻撃として被害拡大につながるため、対策と注意が必要です。

ではどのように対策をすればよいのでしょうか？ 答えは「標的型メール訓練」です。

標的型メール訓練

標的型メール攻撃を防ぐためには一人一人の意識向上が必要です。しかし日々巧妙化していく標的型メール攻撃に対して、「怪しいメールは開かない」だけでは対策が不十分です。また“怪しい“の捉え方も十人十色です。そこで、組織全体の意識向上と対策として有効なのが、前回のニュースレター内で「サイバー攻撃からオリンピックを守ったセキュリティ対策とは？」でもご紹介をした「標的型メール訓練」です。

自社の社員を対象に不定期に標的型メールを装った訓練メールを送信し、注意喚起をするとともに実際に開封してしまった社員を確認し、個別に注意をすることで**組織内のセキュリティ意識の向上と均一化**が出来ます。

標的型メール訓練には
一般的に下記のような内容が含まれています。

- 標的型攻撃の基本情報学習
- 危険なメールを模した模擬メールの送付
- 模擬メールを開封してしまった件数の集計・分析

標的型メール訓練サービスの取り扱いを開始！

この度、標的型メール訓練サービスの取り扱いを開始しました。ネットアシストで提供するM&K社の訓練サービスは、メールの文面作成のご相談から実際の配信作業・レポート結果の提出まで、セキュリティベンダーで対応をするため、お客様の作業負担が少なく実施が出来ます。
気になる方はお気軽にご相談ください！

費用イメージ

100名に対して訓練メールを1回送信する場合

基本料金30万円 ＋ 実施費用14万円 ＝44万円

価格表

基本料金 30万円

＋

実施費用	1回実施	2回実施
100アカウントまで	14万円	20万円
500アカウントまで	21万円	30万円
1,000アカウントまで	28万円	40万円
2,000アカウントまで	35万円	50万円

※基本料金＋送信宛先数と配信回数が実施費用です。

情報漏えい、セキュリティインシデントを防ぐ準備はできていますか?

知らなかったでは済まされない「改正個人情報保護法」をおさらい!

昨年12月、弊社主催WEBセミナーのテーマでもありました「改正個人情報保護法」が2022年4月1日に施行されます。(ネットアシストでは毎月テーマを変えてWEBセミナーを開催しておりますので、是非ご参加ください!)今回は改正個人情報保護法をおさらいし、改正後のポイントをお伝えします。そして、いくつかご紹介するセキュリティインシデント事例を基にサイバーセキュリティ対策のポイントも解説します!

そもそも…個人情報保護法とは? ～概要とこれまでの歩み～

情報化社会へ発展が進む2000年代初頭、当時の日本には個人情報を保護する法律はおろか、「個人情報」というワードを具体的に定義する法律もありませんでした。そこで個人情報保護に対する考えがまとめられ、2005年4月に「個人情報保護法」が施行されました。

2017年の改正では個人情報の取扱件数の制限が撤廃され、現在では個人情報を1件でも取り扱うすべての事業者が対象となっています。個人情報保護法とは、「個人の利益・権利の保護」と「個人情報の有用性(利用)」のバランスを図るための法律であり、個人情報を取り扱う事業者が守るべきルールを定めるものです。

守るべきルール

1. 取得・利用に関するルール
2. 保管に関するルール
3. 他人に情報を渡すときのルール
4. 外国にいる第三者に情報を渡すときのルール
5. 本人からの開示や利用停止を求められたときのルール

ここが変わる!「改正個人情報保護法」

本人の権利保護の強化

Point

本人からの請求内容・対象の拡大

事業者の責務の追加

Point

漏えい時の報告・本人通知義務の拡大、
公表・告知事項の追加

企業の特定分野を対象とする団体の認定団体制度が新設される

データの利活用の促進

Point

仮名加工情報制度の新設・提供先で
個人データとなることが想定される場合の
確認義務の新設

法令違反に対するペナルティの強化

Point

法人に対する罰金刑の引き上げ

外国の事業者に対する罰則の強化

セキュリティインシデント事例

事例 1 D株式会社：不正アクセス被害

D社が運営するコンテンツ販売サイトにおいて、サービス異常の調査中に外部からの不正アクセスを確認。顧客のクレジットカード情報56万件以上が流出した可能性。さらに、サーバーが改ざんされ、新たにクレジットカード情報が7千件以上流出した可能性。システムの抜本的な見直しが必要となり、D社は当該サービスを終了。

事例 2 T病院：ランサムウェア感染

ランサムウェアに感染し患者約8万5千人分の電子カルテが閲覧不能。VPNのIDとパスワードの漏洩が侵入経路になった可能性。犯人は電子カルテの復元の為に身代金を要求。T病院は身代金を払わず、約2億円をかけて電子カルテシステムの再構築を発表。

事例 3 株式会社B：情報流出

B社は顧客情報管理をシステム開発・運用を行うグループ会社のS社に委託。ところがシステム保守についてはS社から再委託。再委託先の元従業員が顧客情報約2900万件を不正に取得し、当該情報を名簿業者に売却・流出させていたことが判明。漏えいは業務用PCからMTP対応スマートフォンへのデータの持ち出しによるものと判明。情報を流出された被害者がB社とS社を相手方として、それぞれ損害賠償を求める訴訟を提起。被害者には慰謝料を払い、改善計画を遂行、B社の役員2名及び会長兼社長は辞任。

事例と併せて考える個人情報流出への事前の対応策

個人情報保護法の第20条で「安全管理のために必要かつ適切な措置」を行うことが定められています。昨今の情勢を踏まえるとサイバー攻撃被害に遭うリスクは高まっていると考えられます。セキュリティインシデントは対岸の火事ではありません。

右記6項目について、具体的な準備は出来ていますか？お客様社内で関係部署との連携や社内周知は徹底されていますか？事前の準備がいざというときの助けになりますので、ご確認いただければと思います。

個人情報流出への事前の対応策

1. 基本方針の策定
2. 個人データの取扱いにかかわる規律の整備
3. 組織的安全管理措置
4. 人的安全管理措置
5. 物理的安全管理措置
6. 技術的安全管理措置

インシデントが発生してからでは手遅れ…未然に防ぐセキュリティサービス

前述の対応策⑥に関しましては、

外部からの不正アクセスを防止するセキュリティサービスの導入も有効です。

WAF

不正アクセスや情報漏えいを引き起こすWebアプリケーションレベルの攻撃を防ぎます。

IDS/IPS

WAFで防ぐことができないOS・ミドルウェアレイヤーへの攻撃からサーバーを守ります。

脆弱性診断

情報漏えいを防ぐという観点では、サーバーやネットワーク・プログラムの脆弱性がないか定期的にチェックすることも重要です。

ネットアシストではお客様の環境に合わせた
セキュリティサービスのご提案も可能ですのでお気軽にご相談ください

日本のクラウドが改めて注目を集めています！

政府御用達・安心の国産クラウド

「さくらのクラウドが政府認定クラウドサービスに登録」

昨年末に日本政府が「さくらのクラウド」を、クラウドサービスの認定制度「政府情報システムのためのセキュリティ評価制度」（ISMAP）のリストに登録したと発表しました。そのため「さくらのクラウド」は政府調達の対象サービスになっています。この件について、さくらインターネット社からも次のように発表がありました。

さくらインターネット社からの発表

ISMAPは、日本政府が求めるセキュリティ要求を満たしているクラウドサービスをISMAP運営委員会が評価・登録する制度です。今回さくらのクラウドがISMAPに登録されたことにより、政府機関が情報システムのクラウド基盤として、また、情報システム開発者などが政府機関向けに納入するシステムのクラウド基盤として「さくらのクラウド」を採用することが可能になりました。

どのサーバーが安全かというのは様々な視点があり一概に言えませんが、それでも会社から、あるいはクライアント様から「安全なサーバーを選んで欲しい」という要望は尽きません。そんな時の選択肢として「さくらのクラウド」であれば「日本政府の調達対象になっているサーバーです」と答える事ができますね。

「国家機密の管理は国産クラウドで」

さらに読売新聞の先月の発表によりますと、政府は、行政データをオンラインで共有するため整備を進めている「政府クラウド」で、国家機密にあたるデータに限り日本企業のサービスを採用する方針を固めた、との事です。機密情報の海外流出を防ぐとともに、アメリカの巨大IT企業に先行された日本企業の技術開発を後押しする目的があるようで、2022年度に企業を選定し、2023年度の運用開始を目指すそうです。

実は2021年10月に始まった政府クラウドの先行事業では、Amazon Web ServicesとGoogle Cloud Platformが採用されていました。政府は経済安全保障の観点から、機密性の高い情報の管理では日本企業のサービスを利用する必要があると判断したとの事です。確かに日本の国家機密は日本のサービスに保管すべき、という議論は以前からネットでも散見されていましたね。

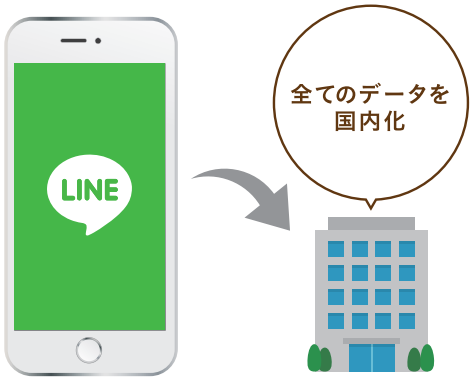
「民間企業の事例」

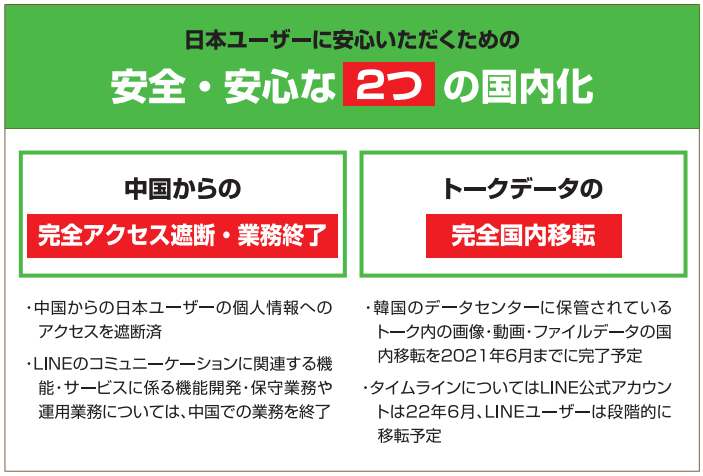
民間サービスでも昨年は、LINE利用者の個人情報を海外に保管していて、中国からアクセスできる状態であった事が問題になりました。このニュースは私の周囲でも話題になり、自分の個人情報が海外に預けられていた事に、不信感を持つ人が多かったですね。LINEの利用を最小限に抑える、と嘆かれる方もいました。

LINEの出沢剛CEOはこの時の問題点について「ユーザーへのわかりやすさ、配慮が欠けていた。ユーザーの感覚でおかしい、気持ち悪いと言うことにセンスや配慮というか気を回すことができなかった」と反省されていました。

その後、LINEは日本のユーザーデータを国内に移転するロードマップを発表し、2024年6月までに全てのデータを国内化する決定がなされています。また出沢剛CEOの反省通り、「ユーザー目線」でのアカウンタビリティ（説明責任）強化のために取り組むことや、安心・安全のための取り組み進捗などの報告も行うとしています。この決定はネットでも好意的に受けとられていました。

このように最近は、ユーザーの個人情報をどこに保管するかという事が重要視されてきている状況です。これからのビジネスは、ユーザーの立場で個人情報がどこに保管されているのが安心されるだろうか、という事も慎重に検討する必要がありそうです。





LINE 株式会社ニュースリリースより引用

お問い合わせはこちらまで！

NET ASSIST 24/7 Guardian Deity 株式会社ネットアシスト

TEL 03-3985-6780 Mail sales@netassist.ne.jp

URL https://www.netassist.ne.jp