報道関係者各位
プレスリリース

2019年9月25日
グローバルセキュリティエキスパート株式会社

GSX、IT セキュリティ e ラーニングの Mina Secure®コンテンツを IPA の発行する「情報セキュリティ 10 大脅威 2019」内容に同期し最新版に刷新へ

グローバルセキュリティエキスパート株式会社（本社：東京都港区海岸1-15-1、代表取締役社長：青柳 史郎、https://www.gsx.co.jp/、以下、GSX）は、GSXオリジナル開発サービスITセキュリティeラーニングであるMina Secure®のコンテンツを刷新リリースしました。具体的にはIPA（独立行政法人情報処理推進機構）の発行する「情報セキュリティ10大脅威 2019」のランキングに同期した内容を新コンテンツとして同日リリースしました。

■ITセキュリティeラーニング「Mina Secure®」のサービスコンセプトについて

- 技術的セキュリティ対策の限界
  標的型攻撃に代表される、情報セキュリティ上のリスクを低減させる為の対策として、昨今では、多層防御をはじめとする技術的なセキュリティ対策が一般的となり、多くの企業で導入が進んでいます。しかしながら、弊社が長年培った情報セキュリティ対策における知見では、これら技術的対策だけでは残念ながら限界があるのが現実です。

- セキュリティ教育という対策手段の意義
  当然ではありますが、最終的に、エンドポイント端末を扱うのも、情報資産を扱うのも、従業員であり一人の人間です。「一人ひとりが、そのエンドポイント端末を、情報資産を、セキュリティ意識をもって扱えるかどうか。」それこそが、技術的な対策を越えて、企業を守ることができる最後のセキュリティ対策ではないかと弊社は考えます。攻撃者という脅威も、不審メールも、減らすことはできません。しかし、従業員の過失や攻撃メールの開封は、減らすことができます。そのために、一人ひとりのセキュリティ意識を向上させうる対策手段が、セキュリティ教育なのです。

- 一人ひとりのセキュリティ意識（アウェアネス）の向上のために
  弊社ではこれまで、標的型メール訓練という攻撃メールのリスク喚起や初動対応の訓練に対する教育サービスのご提供を続けてきた中で、その訓練の補完機能にもなり得る有効なサービスとしてMina Secure®を開発して参りました。近年の外部脅威に企業として対峙すべく、従業員へのセキュリティ教育の醸成（セキュリティアウェアネス）は必要不可欠な要素となっています。従業員に対して、セキュリティ意識をもっと強く向上していただくため、またより広範・多角的なセキュリティ上のリスクに対応していただくため、情報セキュリティ対策全般におけるeラーニングサービスとしてご提案しています。

■IPAの発行する「情報セキュリティ10大脅威 2019」とは

IPA（独立行政法人情報処理推進機構）が毎年発表している「情報セキュリティ10大脅威」の最新版である「2019年版」の詳細が先月発表されました（以下引用文）。

「情報セキュリティ10大脅威 2019」は、2018年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約120名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

■「情報セキュリティ10大脅威 2019」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位 (*1)	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者への被害	3位	ランサムウェアによる被害	2位
NEW	メール等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

（*1）クレジットカード被害の増加とフィッシング手口の多様化に鑑み、2018年個人1位の「インターネットバンキングやクレジットカード情報等の不正利用」を本年から、①インターネットバンキングの不正利用、②クレジットカード情報の不正利用、③仮想通貨交換所を狙った攻撃、④仮想通貨採掘に加担させる手口、⑤フィッシングによる個人情報等の詐取、に分割。

【出典】情報セキュリティ10大脅威 2019｜IPA｜
https://www.ipa.go.jp/security/vuln/10threats2019.html

Mina Secure®の最新版コンテンツ各章の意図・概要（一部）は以下の通りです。

- 第1位：クレジットカード情報の不正利用
  ウイルスや偽のウェブサイトによってクレジットカード情報が盗まれ、不正に利用される被害が多数発生しています。

- 第2位：フィッシングによる個人情報等の詐取
  フィッシング詐欺とは、いかにも信用できそうな送信者を装った偽のメールを送りつけ、偽のウェブサイトに誘導するなどの方法で、クレジットカード番号やユーザID、パスワード等の重要な個人情報を盗み出す行為です。

- 第3位：不正アプリによるスマートフォン利用者への被害
  スマートフォンに不正アプリをインストールさせられることで、スマートフォン内の情報を盗まれたり、スマートフォンの機能を不正に利用される被害が広がっています。

- 第4位：メール等を使った脅迫・詐欺の手口による金銭要求
  被害者のパスワードを提示したり、後ろめたさにつけ込むなどして不安感を煽り、金銭を騙し取ろうとする脅迫・詐欺メールが出回っています。

- 第5位：ネット上の誹謗・中傷・デマ
  インターネットの匿名性を利用して、特定の個人や組織を誹謗・中傷したり、犯罪予告を行う事件が発生しています。

- Mina Secure®「情報セキュリティ10大脅威 2019」対応版、新コンテンツサンプル動画はこちらから
  https://www.gsx.co.jp/informationsecurity/minasecure.html#2019_10MT

■近年の外部脅威の兆候と従業員へのeラーニング実施の必要性

IPAの発足したサイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））の報告によると、依然としてメールをトリガーにしたインシデントが多く、プラント関連事業者を狙う一連の攻撃やビジネスメール詐欺（BEC）の国内組織への攻撃、OLE機能（Windows機能/仕様）を悪用した文書ファイルの手口なども引き続き確認されています。

殊にビジネスメール詐欺（BEC）手法による標的型攻撃では、我々の想定を超えた攻撃者による内偵プロセスが数多くあり、詐欺であることを見破ることが困難になっているケースが見受けられます。

このように、不審メールの本文中のURLのクリックや、添付ファイルを開くことでウイルスに感染に至る可能性も少なくないため、安易な操作を行わないような社内での注意喚起を行うことや、意図的に不審なサイトを閲覧せずとも、通常業務の中でこのようなことは十分に発生しうるため、外部からの攻撃の被害に遭わないよう、OS やブラウザ等のソフトウェアの脆弱性を解消するとともに、不審サイト・詐欺サイト・偽警告等にだまされないようにするといった、従業員への教育を行う必要があります。

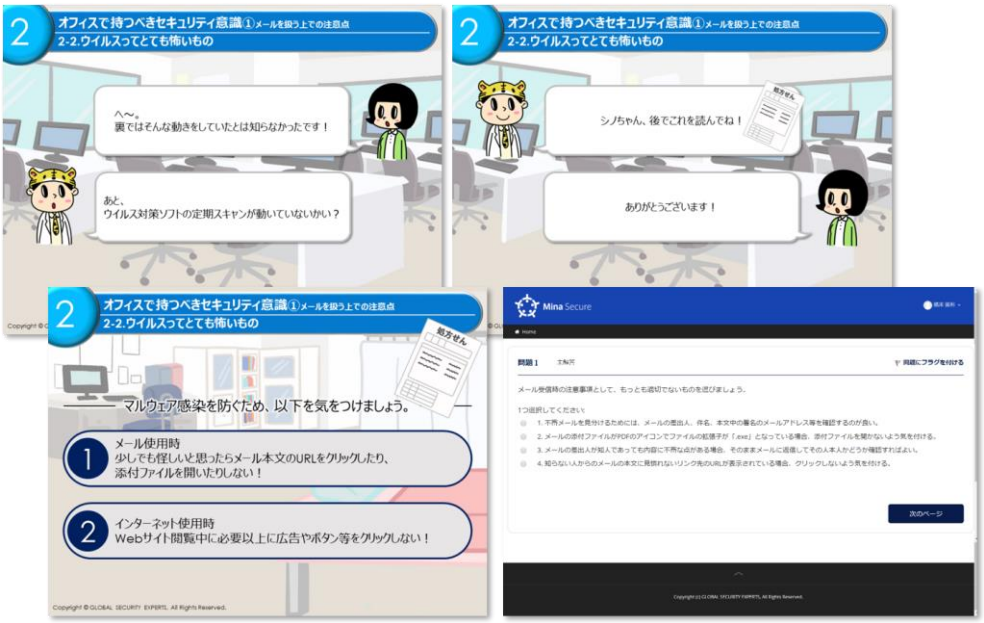
【出典】サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2019年4月～6月]｜IPA｜
https://www.ipa.go.jp/files/000076713.pdf

■ITセキュリティeラーニング Mina Secure® とは

- サイバーセキュリティ教育カンパニーのノウハウと知見
  GSXはサイバーセキュリティ教育カンパニーとして、数多くの企業におけるコンサルティング業務に関わって参りました。これらで得たノウハウと知見をもとに、コンテンツの章立てや編成あるいはコンテンツ細部に渡るまで、専門会社ならではの知見とノウハウを活かして作成した内容になっています。

- 一般ユーザへの分かりやすさと意識づけを徹底したコンテンツ
  一般ユーザの日常業務のなかで、留意いただきたいセキュリティ対策を、分かりやすくご説明しています。可能な限り平易な言葉を用いたうえで、日常業務に自然とセキュリティ意識が溶け込み、根付く様な説明・表現を念頭に作成します。同時に「なぜ駄目なのか」「どんなリスクがあるのか」の理由付けをきちんと説明することで、セキュリティ意識を持つことの意味合いをより深く理解していただける様に考慮しています。

- 管理者向け機能の充実
  管理者様向けのアカウントでは、各種機能をご利用いただけます。受講させたい一般ユーザのアカウント登録はもちろん、その受講状況の確認把握、未受講者へのフォローメール、アンケート結果の確認などの機能を有しています。



■標的型メール訓練サービスやスミッシング訓練サービスとの併用効果について

前述のように依然としてメールをトリガーにしたインシデント事例は多く、eメールの取扱お作法をはじめ、「なぜ標的型メールに注意が必要なのか」「メール受信時に何を注意しなくてはいけないのか」「開封感染時に必要な初動対応が何か」などを分かりやすく従業員に解説する必要があります。

- 開封時コンテンツを未読の【訓練メールの非開封者】にも、あらためて攻撃メール対応の教育ができます
- 攻撃メールの危険性を説明する事で、よりセキュリティアウェアネスを高める事ができ、適切な初動対応についても従業員が理解することができます
- 要注意者である【訓練メールの開封者】に、改めて徹底した攻撃メール対応の教育が可能です
- eメールのみならず会社支給のスマートフォン端末を踏み台に一通のSMSから脅威が迫ることも意識・認識する必要があります

◆グローバルセキュリティエキスパート株式会社について

社名　　：グローバルセキュリティエキスパート株式会社
本社　　：〒105-0022 東京都港区海岸1-15-1 スズエベイディアム4F
西日本支社：〒541-0047 大阪市中央区淡路町3-1-9 淡路町ダイビル7F ※2019年10月1日（火）業務開始
代表者　：代表取締役社長　青柳 史郎
資本金　：592,814,200円（資本準備金含む）
設立　　：2000年4月
コーポレートサイトURL　：https://www.gsx.co.jp/

ー GSX は、サイバーセキュリティ教育カンパニーです ー

わたしたちは、情報セキュリティ・サイバーセキュリティに特化した専門会社であり、セキュリティコンサルティング、脆弱性診断、サイバーセキュリティソリューションをはじめ、日本初のセキュリティ全体像を網羅した教育メニューをご提供しています。

以下のように「教育」という観点を各事業の軸に据え、お客様へセキュリティへの気づきを与え、セキュリティ市場を活性化する事で、日本の情報セキュリティレベル向上に貢献します。

➢　直接的な教育貢献
総合的な教育事業提供社として、EC-Council セキュリティエンジニア養成講座を介してセキュリティエンジニアを輩出し、標的型メール訓練サービスや IT セキュリティ e ラーニングである Mina Secure®及びサイバーセキュリティ演習サービスを介してお客様のセキュリティリテラシーを向上します。

➢　間接的な教育貢献
GSX の既存事業（脆弱性診断サービス、コンサルティングサービス、サイバーセキュリティソリューションサービス）を介して、各サービスに関係するサイバー犯罪やそのリスク、さらにお客様の現状の課題についての"気づき"と、対策の正しい進め方を提供することで、あらゆる事業活動を教育啓蒙の場として活用します。

➢　市場活性化としての教育貢献
お客様の情報セキュリティリテラシー向上のため、共にお客様をサイバー脅威などから守れる業界のプレイヤー（パートナー様）を増やすことを目指します。志を同じくするプレイヤーを増やすことで、さらなる市場の活性化を推進します。

【本リリース内容に関するお問い合わせ先】

グローバルセキュリティエキスパート株式会社　営業本部　マーケティング部
TEL　：03-3578-9001（代）　各種お問い合わせ：https://www.gsx.co.jp/inquiry