

フィッシング攻撃の見極めと 脅威インテリジェンスへの取組 ～インシデント対応を強化するために～

講師の紹介

氏名	星野 樹昭（ほしの しげあき）
業務経歴	26年（セキュリティ経験：20年）
専門分野	ITインフラ設計 / 構築 / テスト 移行設計 セキュリティ製品導入支援 ISMS導入支援
保有資格	情報処理安全確保支援士（登録番号 第002047号） CISSP（Certified Information Systems Security Professional） MCP（Microsoft Certification Professional）
コメント	官公庁や金融機関などの大規模環境から、中小零細企業規模まで、オンプレ/クラウド問わず様々な環境のITインフラ環境導入・移行の経験あり。 セキュリティ製品の導入支援では、DB暗号化ソフトウェアやWeb Application Firewall、クライアントPCのセキュリティ対応など、実績豊富。 現在はISMSコンサルも実施しており、活動は多岐にわたる。



株式会社ワールドスカイ
取締役 星野 樹昭

はじめに

概要

- フィッシング攻撃の現状とその巧妙化
- フィッシング攻撃の検知・見極め方法
- 脅威インテリジェンスの活用法

フィッシング攻撃の現状

1. 攻撃手法の複雑化
 - 多段階攻撃の増加
 - CAPTCHAの悪用
2. AI技術の悪用
 - 生成系AIの悪用
 - ディープフェイクの悪用
3. ターゲットの絞り込み
 - 特定業種や役職者の狙い撃ち
 - 地理的・言語的特性の利用

フィッシング攻撃の事例紹介

カード会社を装ったメール

差出人: MyJCB(サイト・アプリ) <jcb-hoshino@cbel.com> 宛先: hoshino@worldsky.jp.com
件名: お客様のJCBカードがロックされています - 解除手続きの詳細をお知らせします。 日時: Sun, 03 Nov 2024 11:46:34 +0900



このたびは、JCBカードをご利用いただきありがとうございます。

近年、悪意のある利用や高度化した金融サービスの悪用によるマネー・ローンダリングやテロ資金供与の防止対策がますます重要になっています。そのため、当社ではお客様のアカウントに不正利用の可能性が検知されたため、ご本人様確認が完了するまで、カードのご利用を制限させていただきます。

ご本人確認のお願い:

<https://my.jcb.co.jp/Login>

ご本人様確認が完了次第、制限を解除いたします。

ご不便とご心配をおかけしまして誠に申し訳ございませんが、何とぞご理解服りたくお願い申し上げます。

株式会社ジェーシーピー

東京都港区南青山5-1-22

©JCB Co., Ltd. 2024

フィッシング攻撃の見極め方

1. 偽リンクの使用を確認する

このたびは、JCBカードをご利用いただきありがとうございます。

近年、悪意のある利用や高度化した金融サービスの悪用によるマネー・ローンダリングやテロ資金供与の防止策として、不正利用の防止策として不正利用の可能性があるリンクに不正利用の可能性があるリンクを制限させていただき

ご本人確認のお願い

<https://my.jcb.co.jp/Login>

<https://xiaosiqun.com/Logiim>

文面のリンク

<https://my.jcb.co.jp/Login>

にマウスカーソルを乗せると・・・

<https://xiaosiqun.com/Logiim>

という、明らかに文面とは異なるURLが表示される

フィッシング攻撃の見極め方

2. 受信者を慌てさせるような表現を確認する

差出人: MyJCB(サイト・アプリ) <jcb-hoshino@cbel.com> 宛先: hoshino@worldsky.jp
件名: お客様のJCBカードがロックされています - 解除手続きの詳細をお知らせします。 日

ロックされています



このたびは、JCBカードをご利用いただきありがとうございます。

近年、悪意のある利用や高度化した金融サービスの悪用によるマネー・ローンダリングやテロ資金供与の防止対策がますます重要になっています。そのため、当社ではお客様のアカウントに不正利用の可能性が検知されたため、ご本人様確認が完了するまで、カードのご利用を制限させていただきます

制限させていただきます

フィッシング攻撃の見極め方

3. 送信元アドレスを確認する

差出人: MyJOB(サイト・アプリ) <jcb-hoshino@cbel.com> 宛先: hoshino@worldskyjp.com
件名: お客様のJOBカードがロックされています。解除手続きの詳細をお知らせします。 日時: Sun, 03 Nov 2024 11:46:34 +0900

送信元アドレスのドメイン名、

cbel.com

って、誰よ??



アドレス欄に **jcb.co.jp**

カードサイト



世界にひとつ。あなたにひとつ。

オリジナルのドメインは

jcb.co.jp

これとは違うし...

会員向け情報 JCBカードの基本 キャンペーン

フィッシング攻撃の見極め方

4. URLの安全性を確認する



The screenshot displays the Worldsky URL analysis interface for <https://xiaosiqun.com/Logiim>. The main analysis window shows a "ノートン評価" (Norton Rating) of "警告" (Warning) with a red 'X' icon. The text explains that Norton SafeWeb has analyzed the URL and found it to be a phishing site. It also provides a link for "詳細情報" (Detailed Information) and a button for "異議を送信する" (Report a problem). The current category is identified as "フィッシング" (Phishing).

Background details from the main interface:

- Community Score: 10 / 96
- 10/96 security vendors flagged this URL as malicious
- Status: 200
- Content Type: text/html
- Security vendors' analysis table:

Vendor	Category
alphaMountain.ai	Phishing
CRDF	Malicious
G-Data	Malware
Seclookup	Malicious
Trustwave	Phishing
Abusix	Spam
Acronis	Clean
BitDefender	
CyRadar	
Lionic	
Sophos	
VIPRE	Malware
Fortinet	Spam
ADMINUSLabs	Clean

フィッシング攻撃の見極め方

4. URLの安全性を確認する

トレンドマイクロによるWebサイトの安全性の評価

[今すぐ確認 >](#)


http://xiaosiqun.com

トレンドマイクロによるWebサイトの安全性の評価

 **危険**

最新のテストでは、このWebサイトに有害なプログラムが含まれるか、閲覧者にフィッシング詐欺を行う可能性があります。

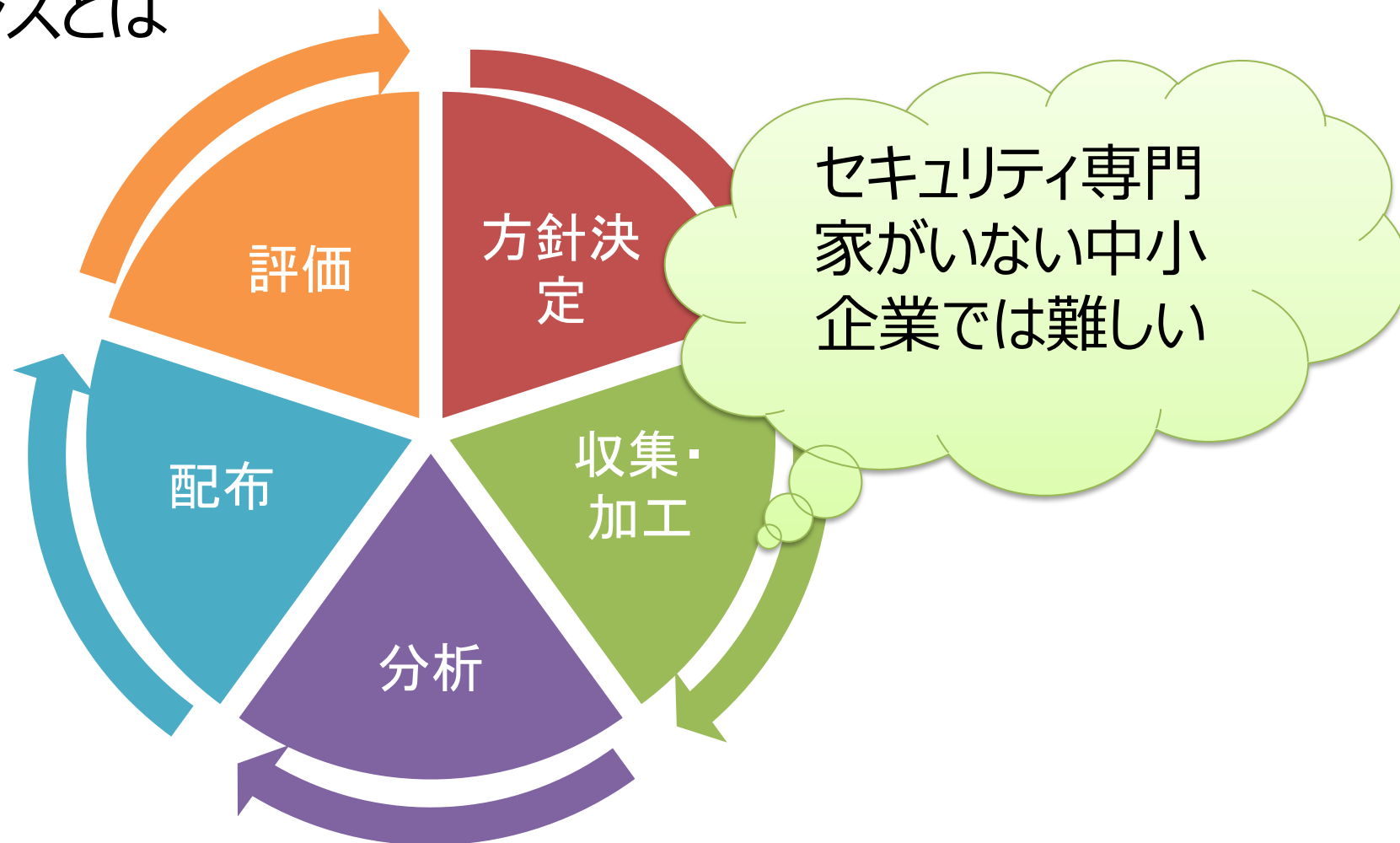
トレンドマイクロによるWebサイトのカテゴリ

 **フィッシング**

正規のWebサイトを偽装してユーザ名やパスワードなどの情報を収集する詐欺サイトです。

脅威インテリジェンスの活用

脅威インテリジェンスとは



【出典】IPA「脅威インテリジェンス導入・運用ガイドライン」から作成

脅威インテリジェンスの活用

ここから始めよう

情報収集

社内への注意喚起

脅威インテリジェンスの情報源

IPA <https://www.ipa.go.jp/>

JPCERT CC <https://www.jpccert.or.jp/>

NISC <https://www.nisc.go.jp/>

警察庁 サイバー警察局

<https://www.npa.go.jp/bureau/cyber/index.html>

Security NEXT

<https://www.security-next.com/>



Worldsky