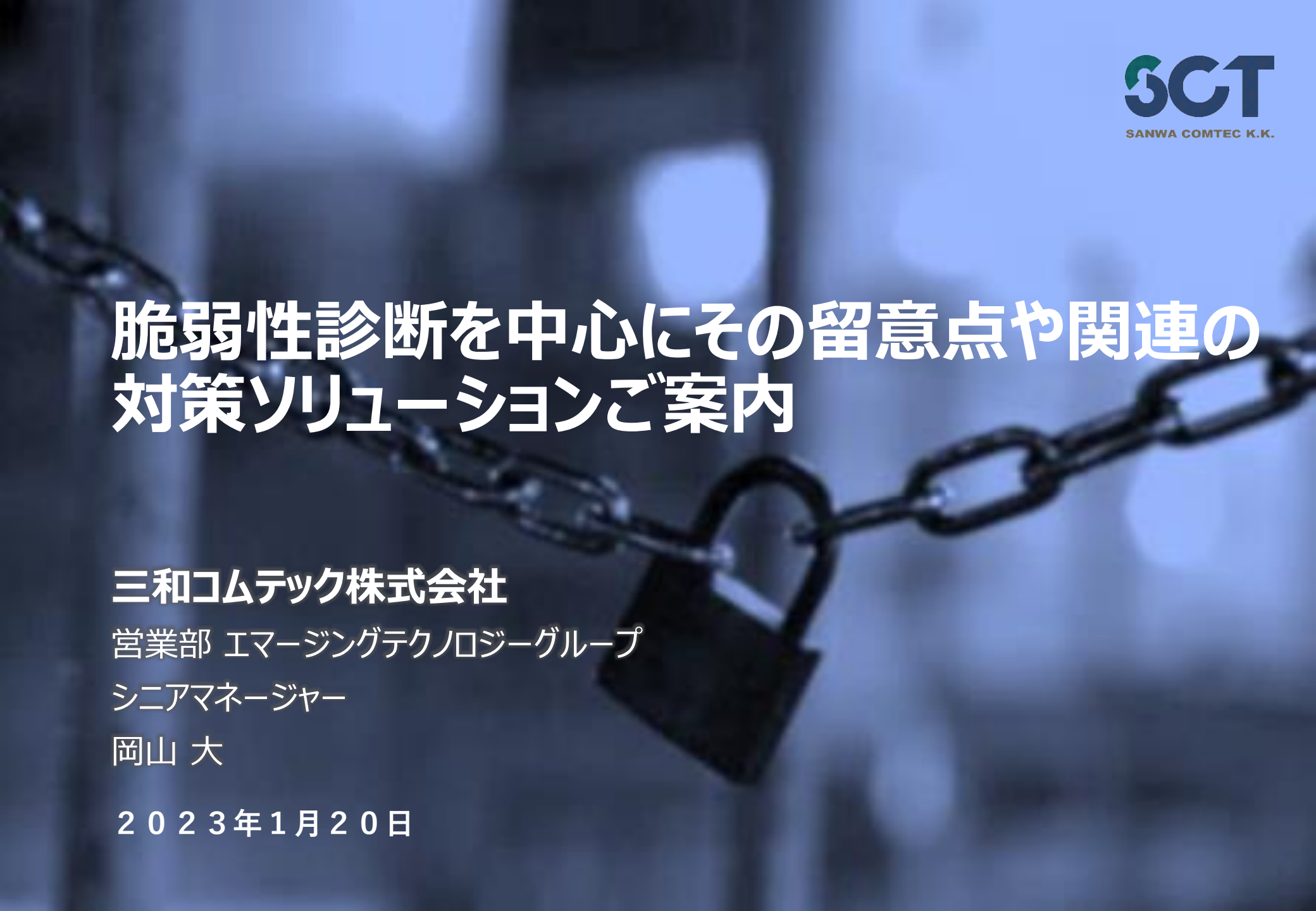


脆弱性診断を中心にその留意点や関連の対策ソリューションご案内

三和コムテック株式会社

営業部 エマージングテクノロジーグループ

シニアマネージャー

岡山 大

２０２３年１月２０日

会社概要

- 社名：三和コムテック株式会社
- 設立：1991 年 8 月
- 本社：東京都港区虎ノ門2-1-1 商船三井ビルディング 4F（2019年11月に に移動）

- 情報セキュリティ分野の取り組み
  - IBMi のセキュリティソリューションの提供
  - 情報システム学会
  - 日本ガイドシェア（JGS）IP部会メンバー2004年より自動脆弱性診断サービスを継続的に提供
  - 手動診断、 Web アプリケーションファイアウォールなど、包括的な脆弱性管理ソリューションを展開
  - **JCDSC(日本カード情報セキュリティ協議会)設立に参画**
  - 2014 年、サイバーセキュリティ診断ブランド「SCT SECURE」を立ち上げ

アジェンダ

1．最近のインシデント状況

2．国内カードセキュリティの流れ

3．診断系 対策ソリューションご紹介

a> V4.0対応

b> EC加盟店（非保持対応）向け

c> 重要インフラ指定会社 など

最近のインシデント状況

インシデント状況　クレレジットカード不正

１）クレジットカード不正被害は激増！　＜前年比: 30%増＞

内訳：　カード偽造は、更に減少傾向（ 割合:　0.65% => 0.2% ）

カード盗用は、大幅増加傾向

（ 155.6億/1H => 206.5億/1H => 同期比: 32%増　）

クレジットカード不正利用被害の発生状況

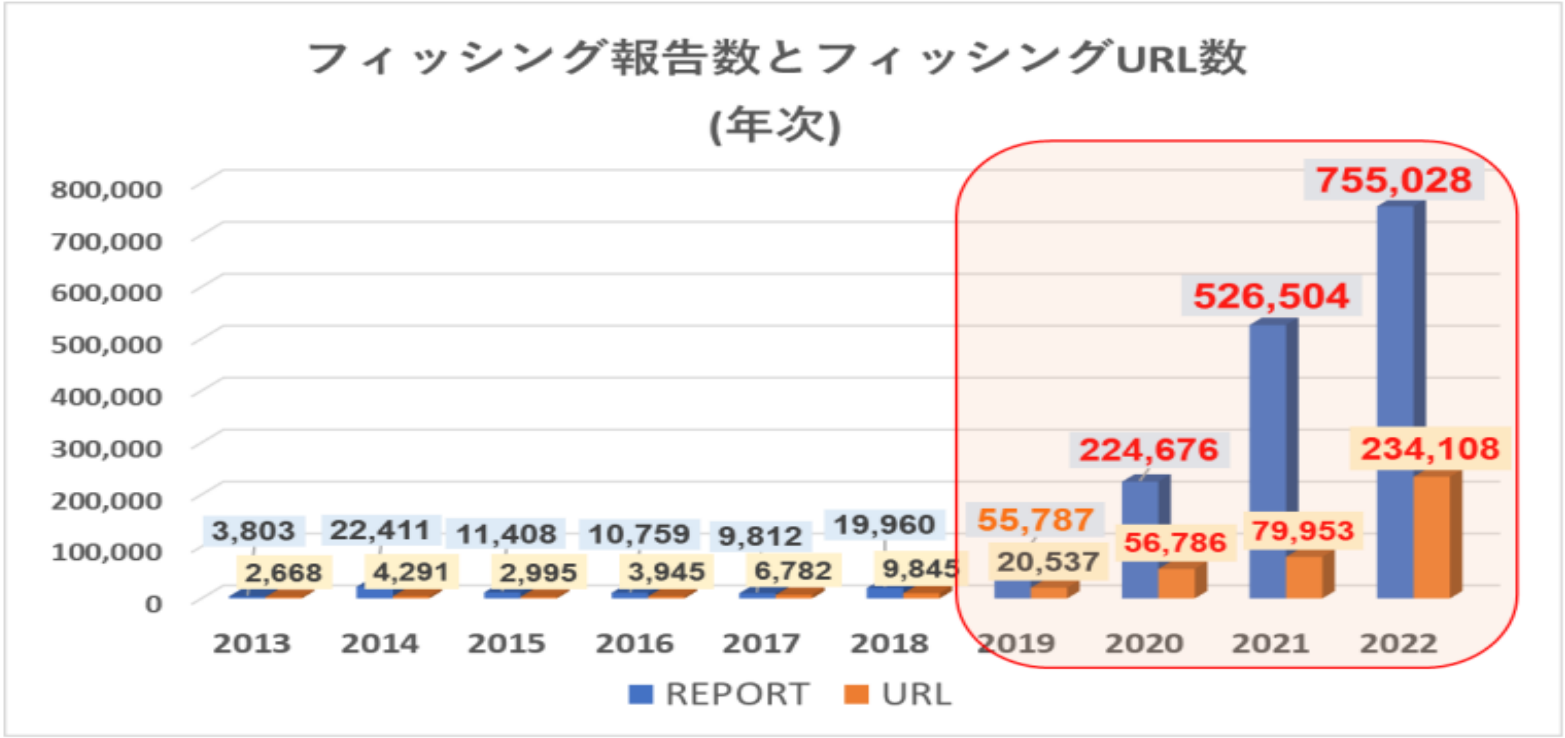
（単位：億円、%）

期　間		クレジットカード不正利用被害額	クレジットカード不正利用被害額の内訳					
			偽造カード被害額		番号盗用被害額		その他不正利用被害額	
			被害額	構成比	被害額	構成比	被害額	構成比
2014年(1月～12月)		114.5	19.5	17.0%	67.3	58.8%	27.7	24.2%
2015年(1月～12月)		120.9	23.1	19.1%	72.2	59.7%	25.6	21.2%
2016年(1月～12月)		142.0	30.6	21.6%	88.9	62.6%	22.5	15.8%
2017年(1月～12月)		236.4	31.7	13.4%	176.7	74.8%	28.0	11.8%
2018年(1月～12月)		235.4	16.0	6.8%	187.6	79.7%	31.8	13.5%
2019年(1月～12月)		274.1	17.8	6.5%	222.9	81.3%	33.4	12.2%
2020年(1月～12月)		253.0	8.0	3.2%	223.6	88.4%	21.4	8.5%
2021年(1月～12月)		330.1	1.5	0.5%	311.7	94.4%	16.9	5.1%
	（1月～3月）	73.7	0.7	0.9%	68.7	93.2%	4.3	5.8%
	（4月～6月）	81.9	0.3	0.4%	78.1	95.4%	3.5	4.2%
	（7月～9月）	81.3	0.2	0.2%	77.1	94.8%	4.0	4.9%
	（10月～12月）	93.2	0.3	0.3%	87.8	94.2%	5.1	5.5%
2022年(1月～6月)		206.5	0.4	0.2%	195.4	94.6%	10.7	5.2%
	（1月～3月）	100.1	0.2	0.2%	94.6	94.5%	5.3	5.3%
	（4月～6月）	106.4	0.2	0.2%	100.8	94.7%	5.4	5.1%

インシデント状況（２）フィッシングサイト

２）フィッシング被害は、2020年から急増

＜報告件数は、13倍以上、URL数も、11倍以上＜2019年比＞



フィッシング対策協議会 HPより

国内のカードセキュリティの流れ

国内カードセキュリティの流れ

1）PCIDSS 準拠 < 2022/04:　V4.0発表 >

2）改正割賦販売法（３度の改正）　準拠

（割賦販売法で義務付けられているカード番号等の適切管理及び不正利用防止措置の実務上の指針）

2016～2020:「実行計画」対応

2021～:　　「クレジットカード・セキュリティガイドライン」へ移行

2022/8～：　**クレジットカード決済システムのセキュリティ対策強化検討会**

対策の強化策の検討 => ガイドラインへ反映

3）その他法規制

改正個人情報保護法　（ 2022/4 罰則強化 ）

犯罪収益移転防止法（2021/11: クレジット分野におけるマネロンガイドライン改定)

サイバーセキュリティ基本法（2021/9 戦略改定　重要インフラ指定 50社向け）

経済安全保障一括推進法（ 2022/5 法案成立）

指定事業者の重要設備導入時等の事前審査の施行

「クレジットカード決済システムの セキュリティ対策強化検討会」

・2022年8月より、５回の検討会を開催

・第5回検討会（2022年12月23日）にて、**クレジットカード決済システムの更なるセキュリティ対策強化に向けた主な取組のポイント（案）**※が開示された。

内容＞ 非対面取引におけるクレジットカード決済の更なるセキュリティ対策強化を図るため、クレジットカード決済網に関わる多様なプレーヤーによる多面的・重層的なセキュリティ対策の取組を整理。

視点＞ １）漏洩防止

ECサイト自体の脆弱性対策を必須化

（システム上の設定不備改善、脆弱性診断、ウイルス対策等）

－例：OSS（オープンソースソフトウェア）を利用したサイト等への対策、WAFの導入）

２）不正利用防止

・本人認証の強化 / EMV3DSの義務化 / リスクベース認証

３）犯罪抑止・広報周知

※ https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/005_02_00.pdf

まとめ

１）２０２０年以降、クレジットカード不正を含め、サイバー攻撃が激化した。

２）コロナ禍の長期化で、リモートワーク化が進む中、我が国でもサイバーリスクが高まっている。

３）サイバーリスクの高まりを受けて、PCIDSS及び様々な国内法により、カードセキュリティ対策の強化が望まれている

＝＞ **高サイバーリスク環境を前提にした、セキュリティ対策が必要**

診断系 対策ソリューションのご案内
＜PCIDSS V4.0新規要件＞

V4.0 新規要件対策ソリューション

1 > 内部診断支援サービス（ 11.3.1.対応 ）

認証スキャン実施計画から、診断実施、実施、対策まで、スムーズな移行、準拠を支援致します。

- 実施計画
  - サンプリング診断支援
  - 結果に基づくGAP分析、実施計画支援
- 実施支援
  - 設定支援 （ サービス / 教育 ）
- 対策支援
  - コンサルティング（優先順位づけ、対策ソリューション案内）

V4.0 新規要件対策ソリューション

2> JavaScript改ざん監視ソリューション<jscrambler>

昨今のカード情報詐取の主な手口となっているWEB（オンライン）スキミング対策。ユーザーのWEBページにて使われているJavaScriptの監視や制御を可能とし、PCIDSS V4.0の新規要件への準拠を可能にします。

- 6.4.3 -消費者のブラウザに読み込まれ、実行されるすべての決済ページスクリプトの管理
- 11.6.1 -消費者ブラウザが受信した決済ページのHTTPヘッダとコンテンツに対する不正な変更を警告する、変更と改ざんの検出メカニズム

なぜ、対策ソリューションなのか？

課題）一般的には、CSP（Content Security Policy）は、マニュアルでの管理・運用が困難

対策）対策ソリューションの利用（jscrambler ）

- JavaScriptエージェント型
- 認可前の新規・変更スクリプトのブロック
- 悪意な動きは、自動防御

ソリューション・デモ動画）

1. V4.0のWEBスキミング防止要件の理解（ウェビナー）
   https://www.youtube.com/watch?v=XVUspnZnJFg&feature=youtu.be
2. ECサイト用（インベントリー管理）- https://youtu.be/IzBNnfFgzo0
3. 機密情報データ - https://youtu.be/F1i9ELo5Dhs

診断系 対策ソリューションのご案内
＜EC加盟店向け＞

加盟店様向け対策ソリューション

１）システム上の設定不備改善 < cloudsec v2 >
クラウド環境を継続的にモニターし、セキュリティ状況を分析
結果は、CISベンチマークなど、セキュリティ基準によって判断

２）脆弱性診断 < SCT SECURE クラウドスキャン など >
ネットワーク（プラットフォーム）診断 < 年間 / ワンタイム >
WEBアプリケーション診断 < 年間 / ワンタイム >
モバイルアプリケーション診断 < 年間 / ワンタイム >
ペネトレーションテスト など

Cloudsec v2とは

クラウド環境の**セキュリティ状況**を解析

クラウド環境を**継続的にモニター**し、セキュリティ状況を分析

結果は**CISベンチマーク**をはじめとするセキュリティ基準に沿って判断

セキュリティリスクを検知した時点で、リスクの内容を**修正方法とともに報告**

AWSやAzureなどのクラウドプラットフォームを**横断的**に解析

Cloudsec v2の特長

自動検知・分析
境界の変化を捕捉
CISベンチマーク準拠/200以上の観点による分析
設定作業は最小限

IaaS、コンテナのための ワークロード分析
DevOpsを支援
Dockerの分析

マルチクラウド、ハイブリッド環境対応
パブリック、ハイブリッド、プライベート環境に対応
同時に複数環境を監視・セキュリティリスクを検知

包括的かつ詳細なレポート
リスクと対策、双方の詳細な情報を提供
PDFフォーマットをサポート

サンプルレポート

Compliance Summary

839912784713/eu-north-1

1.1	Avoid the use of the "root" account	
1.2	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	
1.3	Ensure credentials unused for 90 days or greater are disabled	

1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password

All user accounts with an AWS console password have the multi-factor authentication enabled.

Category
Security & Identity

Description
Multi-Factor Authentication (MFA) adds an extra layer of protection on top of
enabled, when a user signs in to an AWS website, they will be prompted for t
authentication code from their AWS MFA device. It is recommended that MF
console password.

Audit
Perform the following to determine if a MFA device is enabled for all IAM use
Console

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the left pane, select Users
3. If the MFA Device or Password columns are not visible in the table, clic
   the table and ensure a checkmark is next to both, then click Close .
4. Ensure each user having a checkmark in the Password column also ha

1.3 Ensure credentials unused for 90 days or greater are disabled

You should consider REMOVING such user accounts and DISABLING first or second access keys. Let's refer to details in the table below.
Number of faulty user accounts: 0, 2, 1 respectively for PASSWORD, FRIST and SECOND access keys.

Category
Security & Identity

Description
AWS IAM users can access AWS resources using different types of credentials, such as passwords or access keys. It is recommended that all credentials that have been unused in 90 or greater days be removed or deactivated.

Audit
Perform the following to determine if unused credentials exist:**Download Credential Report:**Using Management Console:

1. Login to the AWS Management Console
2. Click Services
3. Click IAM
4. Click on Credential Report
5. This will download an .xls file which contains credential usage for all users within an AWS Account - open this file

Via CLI

1. Run the following commands:
   aws iam generate-credential-report
   aws iam get-credential-report --query 'Content' --output text | base64 -d | cut -d, -f1,4,5,6,9,10,11,14,15,16

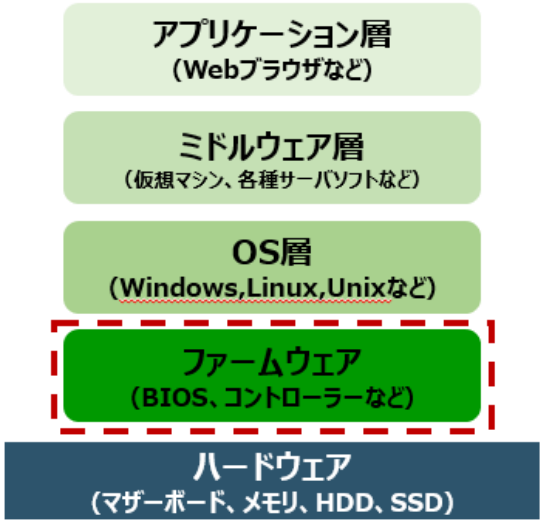
診断系 対策ソリューションのご案内
＜重要インフラ指定会社など＞

重要インフラ対象企業様向け

カード業界関連の国内法・コンプライアンス対策への推奨ソリューション（特に、重要インフラ対象企業）

ファームウェア脆弱性管理ソリューション

従来の脆弱性診断ではカバーできていないOS以下の脆弱性（VBOS：Vulnerability below the OS)の定期診断を実施・対策することで、ファームウェアの脆弱性を突いた攻撃を防ぎます。



ファームウェア脆弱性の怖さ

背景）APT（Advanced Persistent Threat ）や昨今の標的型攻撃、ランサムウェア攻撃、HACTIVISMなどで、ファームウェアの脆弱性を突いたものが増えている。

脆弱性）米国CISA(サイバーセキュリティ・社会基盤安全保障庁）公表の
KEV(実際にサイバー攻撃に利用されたことのある本当に危険な脆弱性)
計856の脆弱性のうち、サーバーソフトやOS、WEBブラウザーなどを抑えて、
ファームウェアの脆弱性がもっとも多く（185以上）リストアップされている。

検出例）

脆弱性名	CVE登録番号	重要度	スコア
Intel ME Out Of Bounds Write	CVE-2020-8752	Critical	9.4
Improper Authentication In Intel ME	CVE-2019-14598 Severity:	High	8.2
Improper Buffer Restrictions In Intel ME Firmware	CVE-2020-0594 C...	Critical	9.8
Heap Overflow In Intel ME Firmware	CVE-2019-0169 C...	Critical	9.6
Insufficient Access Control In Intel ME Firmware	CVE-2019-0089 C...	Critical	9
Insufficient Input Validation In Intel ME Subsystem	CVE-2018-12190 ...	High	8.2

ファームウェア脆弱性の怖さ（実例）

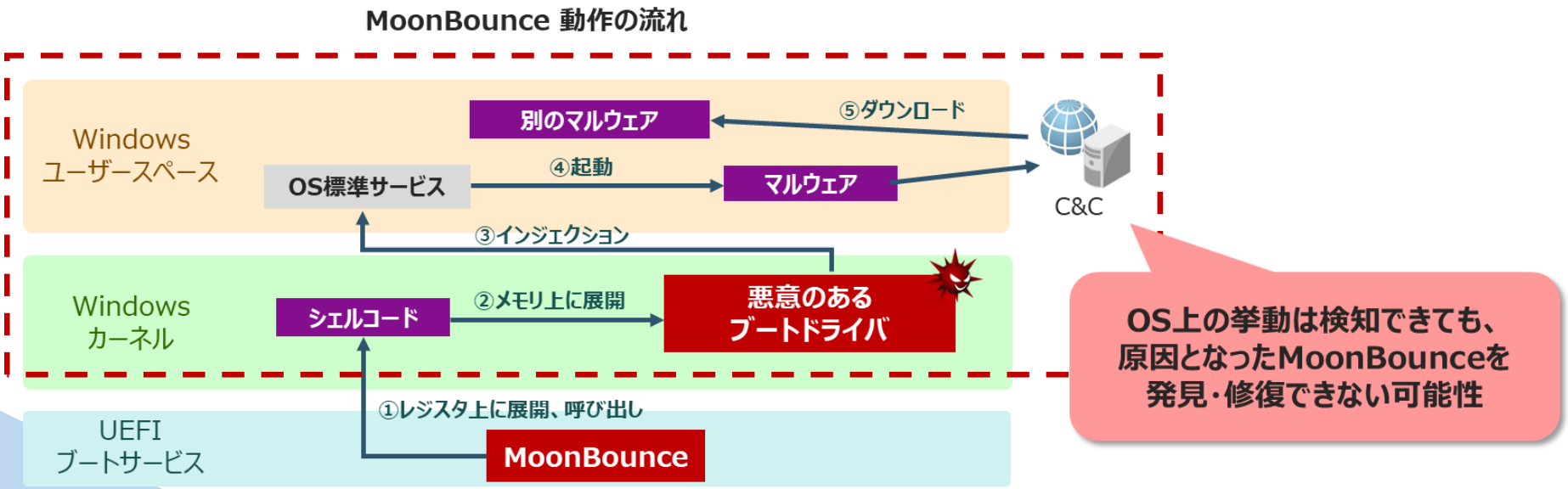
MoonBounce（2021年）

APT41起因とされるUEFI bootkit（ファームウェアに感染するマルウェア）

UEFIブート時の初期段階で実行される既存のコードの内容を変更する

改ざんされたファームウェアにより、OS起動時にメモリ上に直接マルウェアが展開される

→ファイル（感染の痕跡）を残さず、OSより先に起動するため検知が困難



さいごに…

年度末を迎え、下記ソリューションに関して、

・クラウド設定チェック <cloudsec v2>

・各種脆弱性診断

・フォームウェア脆弱性診断＜eclypsium＞

キャンペーンを実施いたします。もちろん、再販もできますのでご活用ください！

ご清聴ありがとうございました！

三和コムテック株式会社

営業部 エマージングテクノロジーグループ

Tel：03-3583-4003

Email：et-sales@sct.co.jp / okayama@sct.co.jp