セキュリティ総論 D レポート No.2

慶應義塾大学 61908697 佐々木良輔

事案

株式会社ヴァンドームヤマダが運営する EC サイト「ヴァンドームジュエリーオンラインストア」が何者かによる不正アクセス攻撃を受け, EC サイト利用者のクレジットカード番号, 有効期限, カード名義人, セキュリティコードなどのクレジットカード情報 2715 点が流出した可能性がある. 攻撃は EC サイトに内在する脆弱性を利用しサーバー内に不正ファイルを設置, アプリケーションを改竄することで行われた. この攻撃により EC サイト利用者の個人情報が格納されたディレクトリが外部からアクセス可能な状態になっていた.[1]

問題点

当事案では EC サイトに内在する脆弱性を利用しサーバーに対して不正な指令を与え攻撃を行ったことから可用性の問題があると言える. 同時に, 本来秘匿されるべきクレジットカード情報を不正に流出したことによる機密性に対する問題があると言える.

法令

不正指令電磁的記録作成等 (刑法 168 条の 2)

不正指令電磁的記録作成等は

1. 正当な理由がないのに
2. 人の電子計算機における実行の用に供する目的で
3. (168 条の 2) 第 1 号又は第 2 号に掲げる電磁的記録その他の記録を
4. 作成, または提供した

場合に成立するものである.[2] ここで EC サイトに内在する脆弱性はシステムのバグに当たるものであり, これは不正指令電磁的記録には当たらない.[2] 一方で攻撃者は脆弱性を利用してサーバー内にスパイウェアのようなものを正当な理由なく挿入, 実行したことから 1, 2, 4 については明らかに成り立っている. また 168 条の 2 第 1 号では「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず, 又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」と

あり, カード情報を不正に流出させることは意図に沿った動作ではないので, 3 も同様に成り立っている. 以上からこの事案では 168 条の 2 が成立すると考えられる.

電子計算機損壊等業務妨害罪 (刑法 234 条の 2)

電子計算機損壊等業務妨害罪の構成要件は

1. 電子計算機に向けた加害行為
2. 電子計算機の動作阻害
3. 業務妨害

の 3 つであり, これらが故意で貫かれていることである.[3] 1 について, これは「電子計算機に虚偽の情報もしくは不正の指令を与える」等が該当する.[3] 等事案ではサーバーにスパイウェアを挿入していることから, 明らかに成り立っている. 2 について「『他人のパスワードを用いて, データベースの情報を不正に入手すること, あるいは他人の電子計算機を無断で使用することなどは, 電子計算機による情報の提供ということ自体は行われており, 業務遂行の外形的妨害は生じていない』として『使用目的に反する動作をさせて業務を妨害したことにはならない』と記述されており, 動作の効率の低下・若干の混乱を『動作阻害』とは, いえないものと考えられる.」[3] とあり, 当事案においても業務遂行の外形的妨害は生じていないと考えられる. したがって当事案においては 234 条の 2 は成立しないと考えられる.

不正アクセス行為の禁止等に関する法律 (不正アクセス禁止法)

不正アクセス禁止法 2 条 4 項では不正アクセス行為は以下のように定義される.[4]

1. 他人の識別符号を悪用することにより, アクセス制御機能により制限された特定電子計算機の機能を利用しうる状態にする行為
2. いわゆるセキュリティホールを攻撃し, アクセス制御機能により制限された特定電子計算機の機能を利用しうる状態にする行為

ここで特定電子計算機とは何らかのネットワークに接続された電子計算機のことであり, アクセス制御機能とは特定電子計算機のある機能の利用を識別符号などを用いて制限する機能である. 当事案において EC サイトに内在する脆弱性を攻撃したことにより, 本来アクセスが制限されているディレクトリやアプリケーションに介入した. したがって 2 条 4 項 2 号の不正アクセスに該当し, 当事案は不正アクセス禁止法に該当すると考えられる.

私法／行政法／刑事法のうちいずれの側面が問題となっているのか

前節で検討した通り, 当事案では刑法 168 条の 2 と不正アクセス行為の禁止等に関する法律に抵触しており, いずれも刑事法であるから刑事法の側面が問題になっていると言える.

参考文献

[1] 株式会社ヴァンドームヤマダ. ヴァンドームジュエリーオンラインストア. https://vendome.jp/news/news_01.html, 11 2021. (Accessed on 11/30/2021).

[2] 法務省. いわゆるコンピュータ・ウイルスに関する罪について. https://www.moj.go.jp/content/001267498.pdf. (Accessed on 11/30/2021).

[3] 独立行政法人情報処理推進機構. わが国における刑事的対応についての示唆. https://www.ipa.go.jp/security/fy11/report/contents/virus/report10.pdf. (Accessed on 11/30/2021).

[4] 警視庁. 不正アクセス行為の禁止等に関する法律の解説. https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf. (Accessed on 11/30/2021).