【Sample】

調査報告書

※一部抜粋

2018 年 7 月 25 日

ネットエージェント株式会社

目次

1. 調査背景

2018 年 6 月 4 日に出向先の UTM が顧客情報.zip のアップロードを検知したため、貴社従業員の不正が発覚し、出向先から情報漏えいに関する調査を要請されました。また、賠償問題に発展する可能性が考えられ、貴社従業員が 6 月末に退職するということもあり、貴社より出向先の情報漏えいに関すること及びその他の不正や情報漏えいの調査依頼を受け、現状の保全および調査を実施しました。

2. 調査実施期間

2018 年 6 月 05 日～ 2018 年 06 月 15 日
※原本の複製及び報告書作成期間を含みます。

3. 調査員

ネットエージェント株式会社	調査員	根戸英二
ネットエージェント株式会社	調査員	熱斗栄治

4. 調査対象期間

貴社指定の以下の期間を、調査対象期間としています。
2018 年 4 月 01 日～ 2018 年 06 月 4 日（端末確保日）

5. 調査対象機器

本調査の調査対象となる記憶媒体が内蔵されている機器は、表 1 の通りです。

表1. 調査対象機器

分類	デスクトップ PC（業務貸与）	貴社管理外 PC
		
メーカー名	Netagent	netagent
型番	abcd-1234	Efgh-5678
S/N	argm813741	jgagr02491jg

調査対象となる記憶媒体は、表 2 の通りです。

表2. 調査対象記憶媒体

分類	原本 1	原本 2	原本 3
	デスクトップ PC 内蔵 HDD 	貴社管理外 PC 内蔵 SSD 	SDXC カード 
メーカー名	netagent	Netagent	netagent
型番	NAHD10000	NAHD320	SD1234
S/N	123456abcd	45678fghi	78912mnopq
LBA（CHS）	—	—	—
容量	500GB	256GB	16GB
HDD サイズ	3.5 インチ	2.5 インチ	—
インターフェイス	SATA	SATA	SD カード

8. 調査結果概要

本件が発覚するより前の 2018 年 6 月 1 日に、SDXC カードに「機密ファイル.zip」がコピーされ、外部に持ち出されていたことが判明しました。

「機密ファイル.zip」は削除ツールにより、完全に消去されていたため、復元不可能な状態でした。

しかし、SDXC カードから復元された「機密ファイル.zip」の中身の全ファイルと同一のファイルが、デスクトップ PC に全て存在することが確認されました。

また、移動やコピーなどの操作状況の調査から、デスクトップ PC 上で「機密ファイル.zip」にまとめられたファイルのファイル名と SDXC カードから復元された「機密ファイル.zip」に含まれているファイルのファイル名が全て一致します。

そのため、SDXC カードから復元された「機密ファイル.zip」は、デスクトップ PC から持ち出されたファイルの可能性があります。

2018 年 6 月 2 日に XXXX ホテルにて、貴社管理外 PC に「機密ファイル.zip」がコピーされ、デスクトップに展開しています。

展開後、「機密ファイル.zip」に含まれている「機密ファイル 1.docx」を更新しています。その直後に、Gmail にアクセスしている記録があります。

なお、貴社管理外 PC に作成された「機密ファイル.zip」は、SDXC カードから復元された「機密ファイル.zip」と同一のものです。

また、各ファイルのタイムスタンプから、SDXC カードから、貴社管理外 PC に「機密ファイル.zip」がコピーされた可能性があると判断しています。

本件の発覚経緯にある「顧客情報.zip」は、貴社による調査対象端末の確保前に削除ツールにより、完全に消去されていたため、復元不可能な状態でした。

しかし、移動やコピーなどの操作状況から「顧客情報.zip」に含まれているファイルと同一の可能性のあるファイルがデスクトップ PC に残っているため、それらのファイルの確認は可能です。

【Sample】

9. タイムライン

本件のタイムラインは、表 5 の通りです。

表5. タイムライン

No.	日時	調査媒体	事象	情報ソース	痕跡抜粋
1	2018/06/01 14:00:00	デスクトップ PC	SDXC カードが接続		
2	2018/06/01 14:10:00	デスクトップ PC	機密ファイル.zip を作成 ※機密ファイル.zip の中身は「機密ファイル.zip 内ファイル一覧.xlsx」を参照		
3	2018/06/01 14:15:00	SDXC カード	SDXC カードに機密ファイル.zip をコピー		
4	2018/06/01 14:20:00	デスクトップ PC	機密ファイル.zip を削除用ツール「delete」により削除		
	2018/06/02 14:50:00	貴社管理外 PC	システム時刻の変更		
5	2018/06/02 15:00:00	貴社管理外 PC	XXXX ホテルで無線 LAN に接続		

【Sample】

10. 調査結果概略図

表 5 のタイムラインから重要事項を抜粋した調査結果の概略図は、図 1. の通りです

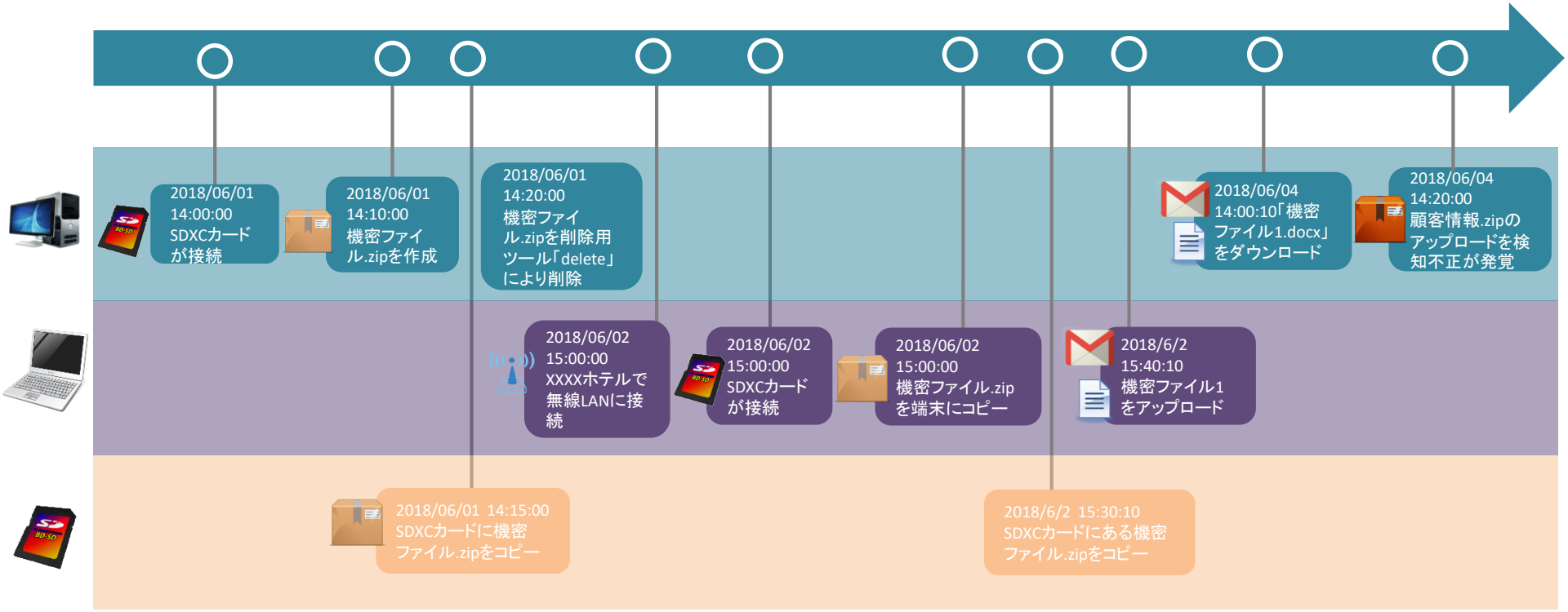

図1. 調査結果概略図

11.4.「機密ファイル.zip」の操作状況調査

「機密ファイル.zip」の操作状況は、表 19 の通りです。

表12.「機密ファイル.zip」操作状況

No.	日時	機密ファイル.zip 保存媒体	操作種別	備考
1	2018/06/01 14:10:00	デスクトップ PC	作成	圧縮ソフト「zipcreate」を使い、デスクトップ PC から機密ファイル.zip を作成しています。詳細は、11.1.章をご参照ください。
2	2018/06/01 14:15:00	SDXC カード	作成（コピー）	ファイルの MD5 ハッシュ値及びタイムスタンプなどにより、SDXC カードへコピーしたと判断しています。詳細は、11.5.章をご参照ください。
3	2018/06/01 14:20:00	デスクトップ PC	削除	削除用ツール「delete」を使い、デスクトップ PC から機密ファイル.zip を削除しています。詳細は、11.1. 章をご参照ください。
4	2016/06/02 14:50:00	貴社管理外 PC	システム時刻の変更	貴社管理外 PC のシステム時刻が変更され、7 年戻されていたことが確認されました。以後、日時には、変更された時間を考慮したものを記載しています。詳細は、11.3.章をご参照ください。
6	2018/06/02 15:20:00	貴社管理外 PC	作成（コピー）	ファイルの MD5 ハッシュ値及びタイムスタンプなどにより、貴社管理外 PC へコピーしたと判断しています。詳細は、11.5.章をご参照ください。
7	2018/06/02 15:30:00	貴社管理外 PC	ー	機密ファイル.zip をデスクトップに展開しています。詳細は 11.6.章をご参照ください。
8	2018/06/02 15:30:10	SDXC カード	削除	SDXC カードから、機密ファイル.zip を削除しています。

なお、情報ソースやファイルパスなどの付加情報を記載した操作履歴の詳細は、「【別紙 3】機密ファイル.zip_操作履歴詳細」をご確認ください。