テックトラップで退職を脅かす日本企業への警鐘

～証拠捏造が可能な日本企業に求められる e-discovery 対策～

多摩大学ルール形成戦略研究所　首席研究員　西尾　素己

I.　本文書の位置づけ

昨今、我々のようなサイバーセキュリティの研究者には「退職後に会社から証拠を捏造された内容証明郵便を送りつけられ、営業秘密の持ち出しや従業員を引き抜く工作をしていたとして訴えるといった脅しとも言える行為に悩まされている」というハニートラップならぬ、テックトラップの相談が増加傾向にある。これは、営業秘密保護法によって日本企業が知財の流出に対して意識が高まったという政策効果が出ている反面、悪徳企業はこの法律を盾に、従業員の職業選択の自由を奪い始めているという別の問題を生み出している。

真の問題は、ほぼ全ての日本企業が従業員の退職後に、元社員が雇用契約違反行為に該当する電子証拠の捏造が可能な情報システム構成になっていることである。これが技術知識のない社員に対して個人対会社という組織力を活用した優越的地位を悪用している状況を生み出しているのだ。

殆どの日本企業は米国では既に導入されている FRCP(Federal Rule of Civil Procedure：連邦民事規則)における e-discovery で定義されている EDRM（The Electronic Discovery Reference Model：電子情報開示参考モデル）に準拠していないため、電子証拠保全能力を有していない。EDRM は米国で過去に電子証拠の偽造や偽装が横行したために米国の司法が導入した電子情報保全のあり方であり、これに準拠しない環境で取得された電子証拠の証拠能力は無いものとみなされている。

以下に示すシナリオは、あくまで一般的な IT 管理者による偽造、偽装を前提としたものであり、以下に示す以外にもデジタル・フォレンジックによりサルベージされるあらゆる電子証拠は偽装が可能である。本書により示される方法論が悪用されないためにも最も一般的で専門的な知識を必要としない方法を示す。

II.　シナリオ

仮想の A 社は元従業員に対して、在籍中に営業秘密に該当する情報の持ち出し、同僚に対する転職の勧誘、これらを裏付けるとするメールのやり取りや関連資料を社内の複合機にて印刷していたとして提訴したとする。その際提示された証拠は電子情報であり、そこに

は元従業員が使用していた貸与コンピュータで作成されたとされる電子メール、電子ファイル、これらの作成日時や最終アクセス日時が表示されているスクリーンショット、Windows イベントビューアの印刷キューログ、複合機のプリントサーバーに残存しているログなどを提出したものとする。

III. 仮定・前提

本文書に記す技術的内容と情報の所有権やアクセス権限などについては以下を仮定・前提とする。これらの仮定・前提は一般的な日本企業の現状を模したものである。

イ）雇用主は在籍中の従業員に貸与したコンピュータに対してメンテナンスなどの IT サポート名目で管理者権限、もしくはそれと同等の権限を有する。このことから雇用主は従業員が使用していた端末を回収後、IT 管理者の協力の下に管理者権限でアクセスすることが可能であると仮定する。

ロ）ログ管理サーバーへのアクセス権と一般的な IT システムのアクセス権などが IT 管理者に集中しており、Audit ログ管理機関が独立した権限を有さない。このことから雇用主が管理する IT 環境では e-discovery もしくはそれと同等の Audit ログ保護や証跡保護を実施していないものと仮定する。

ハ）取引先との NDA などを遵守するため複合機へのキュー（指令）であったとしても社外システムに送信することはあってはならない基本設計である。このことから雇用主が導入する複合機の印刷キューを管理、処理するプリントサーバーは雇用主が管理する社内ネットワーク内に存在し、管理権限も雇用主の IT 管理者が所有すると仮定する。

Ⅳ. 検証（一部机上）

上記の「仮定・前提」に基づき、以下に雇用主が従業員に貸与していたコンピュータを従業員の退職後に使用し、従業員が在籍期間中に特定の文書を従業員の貸与コンピュータにて作成し、雇用主が管理する複合機にて印刷した事実を捏造することに関する実現可能性を検証する。

イ）手順

雇用主は以下の手順により証拠の偽造を実施したものと考えられる。

1. 従業員の貸与コンピュータへの管理者権限でのアクセス
2. 従業員の貸与コンピュータでの文書の作成と作成日時、最終アクセス日時などの偽装
3. 従業員の貸与コンピュータから送付された印刷キューに関するログの偽装
4. 雇用主が管理するプリントサーバーのログの偽装
5. 付随する証拠の偽造

ロ）1.「従業員の貸与コンピュータへの管理者権限でのアクセス」に関する実現可能性検証

仮定・前提に記した通り、雇用主は貸与コンピュータ内に残存する従業員のユーザー名とパスワードを知っている、もしくは貸与コンピュータ内、もしくは当該端末が属する Active Directory（以下 AD）に管理者権限を有している。

従業員が使用していた貸与コンピュータは雇用主が管理する AD に属しており、雇用主は当該 AD の管理者権限を有しており、それゆえにトラブル対処などが可能な状態であるため、この条件を満たすと考えられる。

この場合、図 1 に示す通り雇用主は任意のユーザーのパスワードを任意の値に変更することができる。その際のコマンド例を以下に示す。

```
net user employee ABCD
```

Syntax

Copy

```
net user [<UserName> {<Password> | *} [<Options>]] [/domain]
net user [<UserName> {<Password> | *} /add [<Options>] [/domain]]
net user [<UserName> [/delete] [/domain]]
```

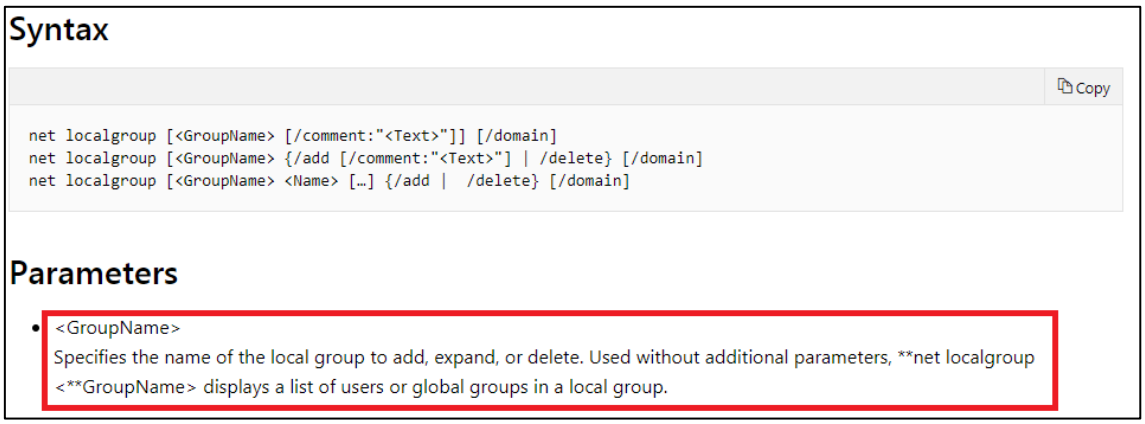
Parameters

Parameter	Description
<UserName>	Specifies the name of the user account to add, delete, modify, or view. The name of the user account can have as many as 20 characters.
<Password>	Assigns or changes a password for the user's account. Type an asterisk (*) to produce a prompt for the password. The password is not displayed when the user types it at the password prompt.
/domain	Performs the operation on the domain controller in the computer's primary domain.
<Options>	Specifies a command-line option. Refer to the next table for descriptions of the command-line option syntax.
net help <Command>	Displays help for the specified **net** command.

図 1　https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc771865(v%3Dws.11)

雇用主は上記に類似するコマンドの実行、もしくはそれと同等の動作をするアプリケーションの実行により従業員の設定したパスワードを知ることなく貸与コンピュータにアクセスすることが可能である。その後管理者権限が必要であれば図 2 に従い、以下のコマンドから管理者権限の付与が可能である。

```
net localgroup administrators employee /add
```



Syntax

Copy

```
net localgroup [<GroupName> [/comment:"<Text>"]] [/domain]
net localgroup [<GroupName> {/add [/comment:"<Text>"] | /delete} [/domain]
net localgroup [<GroupName> <Name> […] {/add |  /delete} [/domain]
```

Parameters

- <GroupName>
  Specifies the name of the local group to add, expand, or delete. Used without additional parameters, **net localgroup <**GroupName> displays a list of users or global groups in a local group.

図　2　https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc725622(v=ws.11)

ハ）2.「従業員の貸与コンピュータでの文書の作成と作成日時、最終アクセス日時などの偽装」に関する実現可能性検証

雇用主は前項の通り従業員の貸与コンピュータに対し、管理者権限でアクセスすることが可能であり、文書は当該端末にインストールされている Microsoft Office を用いて作成可能である。この際、Windows システム上のファイル作成日時が図 3 のようにファイルのプロパティに記録される。

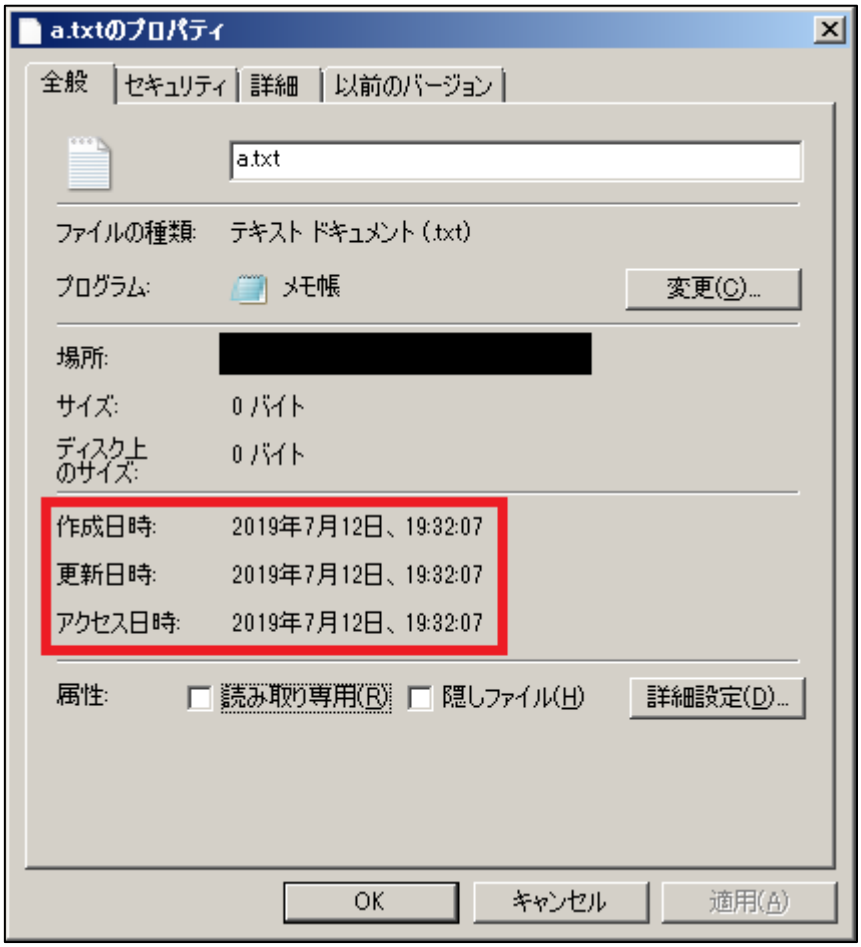


図 3　通常の文書プロパティ

これらのパラメータは従業員が在籍中に作成されたファイルか否かを判断する重要な指標となるが、図 4~6 に示すとおり以下の PowerShell コマンドを実行することで偽装が可能である。

```
Set-ItemProperty a.txt -Name CreationTime -Value "01/01/2099 00:00 AM"
Set-ItemProperty a.txt -Name LastWriteTime -Value "01/01/2099 00:00 AM"
Set-ItemProperty a.txt -Name LastAccessTimeUtc -Value "01/01/2099 00:00 AM"
```

```
Set-ItemProperty a.txt -Name LastWriteTime -Value "01/01/2099 00:00 AM"
Set-ItemProperty a.txt -Name CreationTime -Value "01/01/2099 00:00 AM"
Set-ItemProperty a.txt -Name LastAccessTimeUtc -Value "01/01/2099 00:00 AM"
```

図５　偽装コマンド

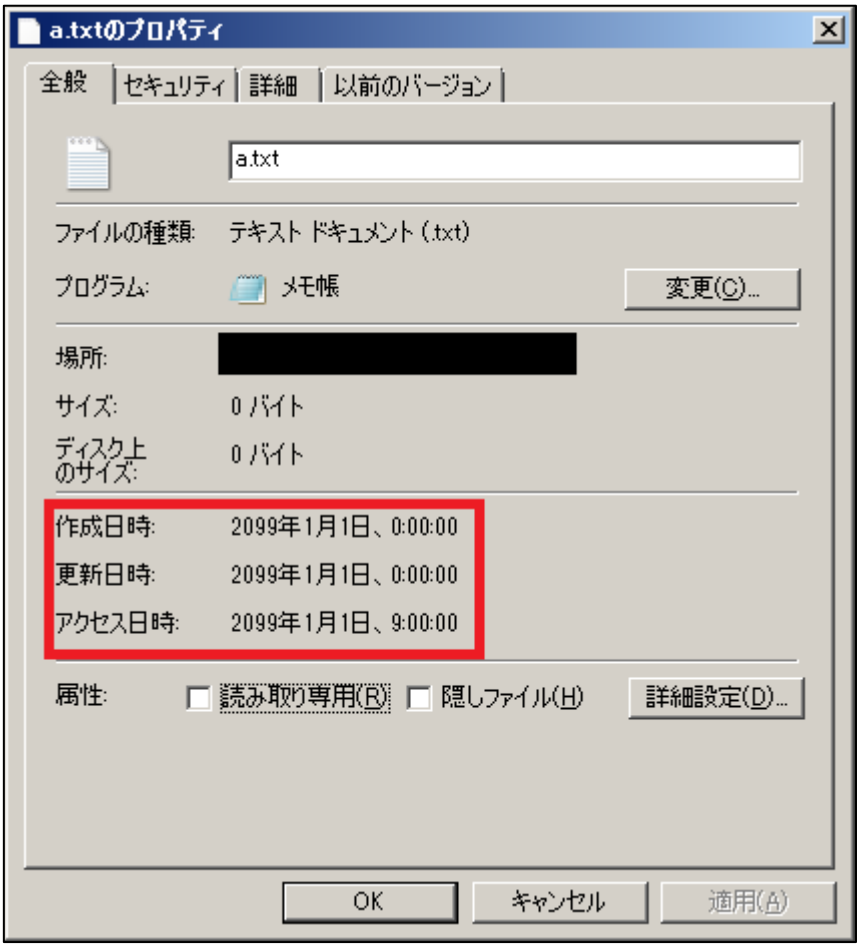


図６　偽装後のファイルプロパティ

ニ）3.「従業員の貸与コンピュータから送付された印刷キューに関するログの偽装」に関する実現可能性検証

従業員の貸与コンピュータのローカルタイムを変更してログを取り直す、もしくは evtx ファイル（Windows のイベントログファイル）をマジックバイト「2A2A」で切り出し、XML を編集することで図 7、8 に示すとおりイベントログの編集が可能である。

図 7　バイナリエディタでの evtx ファイル編集

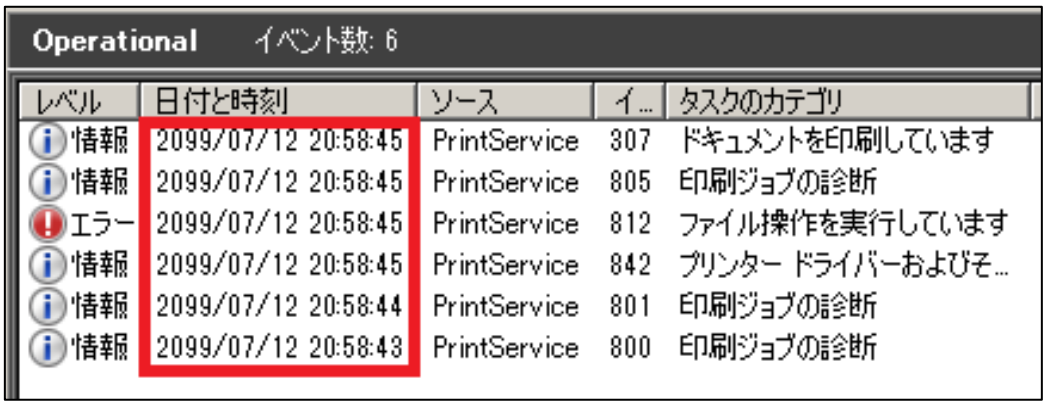


図 8 偽装に成功したアプリケーションとサービスログ以下の印刷ログ
（/Microsoft/Windows/PrintService/Operational）

ホ）4.「雇用主が管理するプリントサーバーのログの偽装」に関する実現可能性検証

従業員が在籍中に雇用主が採用していた複合機のプリントサーバーの処理を示した図を図 9 示す。

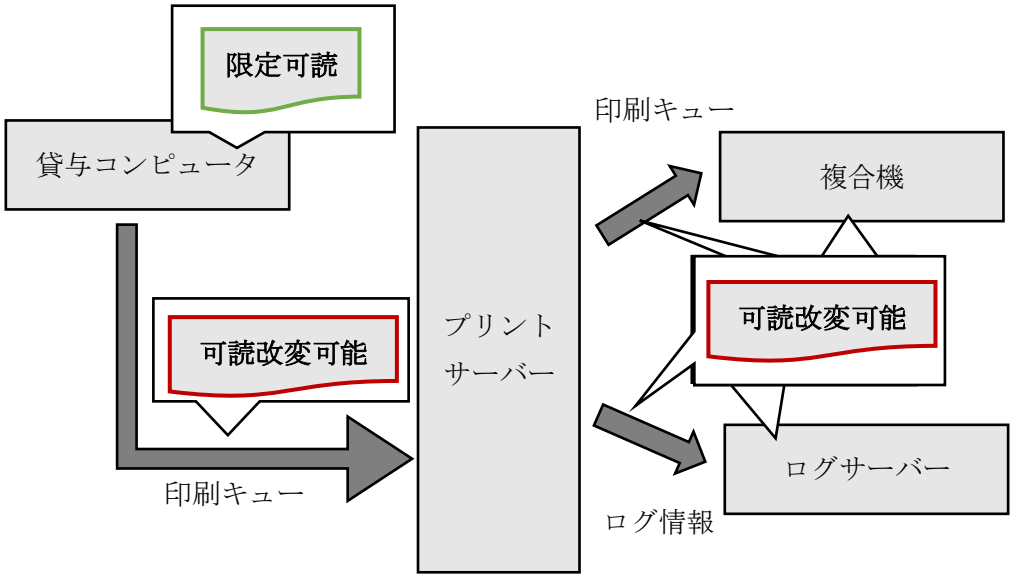


図 9　印刷処理チャート

図 9 示したとおり同社の複合機の情報保護体制では偽装した印刷トラフィックに従ったログ生成が可能であり、かつログサーバー内の情報も IT 管理者に対して可読かつ改変可能な状態で保存される。本書では印刷トラフィックの偽装に関しては割愛する。この実装は雇用主が政府機関等の高い機密性を必要とするプロジェクトを実施する場合には極めて好ましくない実装である。このような実装を取る複合機は数多く存在する。

へ）5.「付随する証拠の偽造」に関する実現可能性検証

前述のような偽装に加え、E メールの偽造や共有ファイルサーバーへのアクセス履歴の改ざんなどが考えられる。以下にそれぞれの可能性について検証する。

Linux ファイルシステムにおけるアクセス履歴の改ざんについて、ファイル実体に対する履歴の改ざんについては以下のコマンドにて実施可能である。

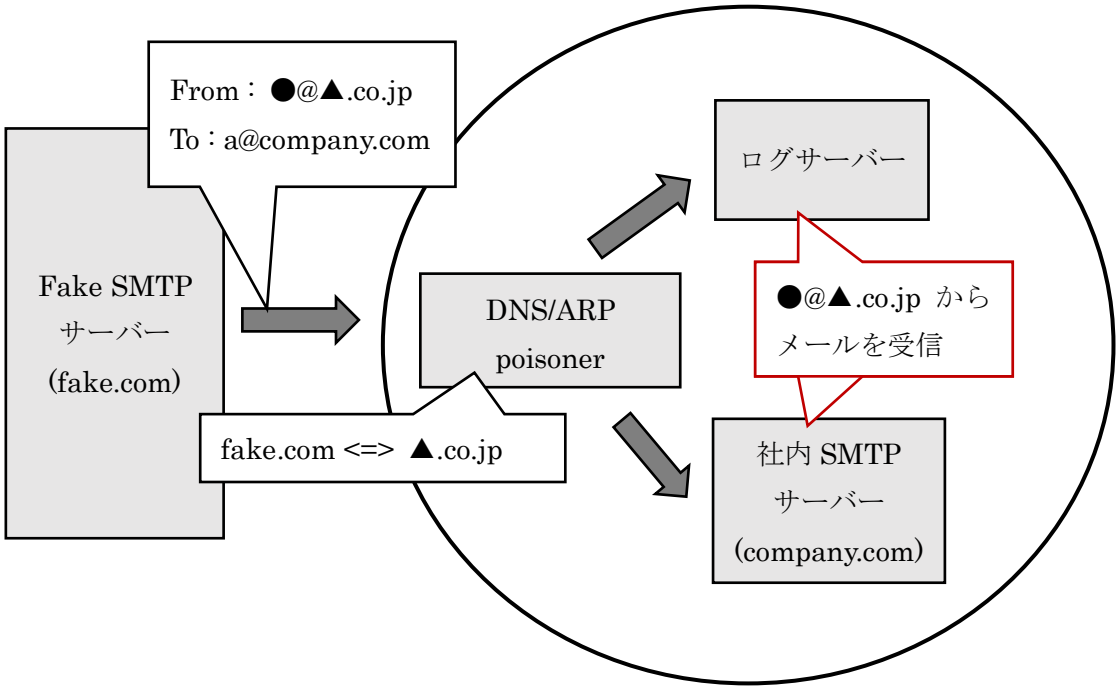
```
touch -a --date="2099-01-01 00:00" a.txt
touch -m --date="2099-01-01 00:00" a.txt
NOW=$(date) && date -s "2099-01-01 00:00" && touch a.txt && date -s "$NOW"
```

```
root@07fe14e24276:/tmp# stat a.txt
  File: 'a.txt'
  Size: 2               Blocks: 8          IO Block: 4096   regular file
Device: 2eh/46d Inode: 86          Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2019-07-07 18:43:50.618588246 +0000
Modify: 2019-07-07 18:43:50.618588246 +0000
Change: 2019-07-07 18:43:50.618588246 +0000
 Birth: -
root@07fe14e24276:/tmp# touch -a --date="2099-01-01 00:00" a.txt
root@07fe14e24276:/tmp# touch -m --date="2099-01-01 00:00" a.txt
root@07fe14e24276:/tmp# NOW=$(date) && date -s "2099-01-01 00:00" && touch a.txt && date -s "$N
OW"
root@07fe14e24276:/tmp# stat a.txt
  File: 'a.txt'
  Size: 2               Blocks: 8          IO Block: 4096   regular file
Device: 2eh/46d Inode: 86          Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2099-01-01 00:00:00.000000000 +0000
Modify: 2099-01-01 00:00:00.000000000 +0000
Change: 2099-01-01 00:00:00.000000000 +0000
 Birth: -
```

図 10　改ざんに成功したファイルサーバー内のファイルアクセス日時

これに加えサーバー側のログ（/var/log 以下）については root 権限により改ざん可能な一般的なファイルフォーマットである。これについてはリモートのログサーバーに転送していたとしても、そもそもログサーバーへの権限を IT 管理者が保有していた場合には同じ手順により改ざんが可能であるため、ブロックチェーン技術やアクセス権限の分離などを徹底する必要がある。また、Windows ベースのファイルシステムであったとしても前項のテクニックを組み合わせることで同等の偽造が可能である。

更に E メールの偽造については以下のような環境を構築することで実現可能である。



受信日時を変更するには上記手順でファイル実体の日時を書き換える、もしくはメール受信時に内部クロックを編集することで偽装が可能である。社内 SMTP サーバーからの偽メール送信は単純に送信ログの送信日時改ざんを行えばよいが、持ち出し先として主張したメールサーバーが e-discovery 耐久だった場合には持ち出しは立証できない。

V. 企業が提出すべき追加証拠

企業は上記のような偽造可能性の否定のため、少なくとも以下のような証拠を追加で提出する必要がある。

1. 従業員に限らず、退職者全員に同じ証拠保全方法を適応しており、そこには全情報のスワイプやファイルシステムへの限定的なアクセス権を持つユーザーの追加など、証拠情報の適切な管理方法が含まれていること。
2. 仮定・前提で挙げた雇用主の管理するシステムの IT 管理者への一極権限集中の否定材料。
3. 複合機システムの設計上の仮説の否定材料。
4. 「3」を提出する場合には、確かに従業員による印刷行為である事を証明する証跡。(従業員のみが知り得るパスワードにより暗号化された実ファイルなど)

VI. 結論

前述の検証の結果から導かれるのは、雇用主は一般的な IT 管理者の知識で十分に証拠の偽造は技術的に可能であるということである。実地検証に耐えられない電子証拠である場合には偽造を疑わざるを得ない。このような現状を見越して米国では e-discovery と呼ばれる電子証拠保全の方法論の適応を電子情報を証拠として裁判所に提出する際には義務付けている。

加えて、今回の検証から図らずも一般的な日本企業における複合機を中心とした情報管理の危険性が浮き彫りになった。政府の CUI（Controlled Unclassified Information）に近い情報を扱う会社であっても、特定プロジェクト関係者以外の目に触れるべきでない情報が複合機を通じてプロジェクト関係者以外にも流出する可能性が高いと言わざるを得ない。

昨年改定された米国国防権限法 NDAA2019 では、電子証拠の保全能力を企業に厳格に求めている。同法では、デュアルユース可能な製品や要素技術、R&D 時に生成される中間生成物、それらの知的財産を有する職員の転職など、米国が規定する情報区分に合致する製品の輸出、再輸出に対して規制をかけている。この中で特に、サイバーセキュリティについては万一の情報漏えいの発生時に過失責任を問うべく、NIST SP800-171 準拠環境での電子情報保護と、e-discovery 耐久な EDRM に準拠した電子証拠保全体制が求められている。NDAA の導入によって電子証拠保全能力（e-discovery を導入した企業）のない企業は技術情報の漏洩の有無すら管理すらできない企業と in して米国のサプライチェーンから排除される可能性が飛躍的に高まるだろう。また、訴訟においても証拠捏造の疑念を抱くリスクを高めることになるだろう。

今後、CRS の Influence Program では証拠捏造のケースを発見した場合は政府や捜査機関、メディアへ速やかに通報し、日本企業が国際的な信用を失わないように意識改革を促し、国内で整備すべきルール形成についても協議を支援していく。