証拠保全ガイドライン 第5版
改定事項の説明

2016年4月26日

サイバーディフェンス研究所
名和 利男

アジェンダ

1. 改定にあたっての状況認識
2. 「高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃」について
3. 「高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃」の事例
4. その他の改定事項
5. 今後の改定について

トピック1

改定にあたっての状況認識

IDFにおける「証拠保全ガイドライン」とは

- 未だに広く認識された標準的な取得手続きのガイドラインが存在しないため、それぞれの運用者及び団体が自主的に作成したガイドラインや、海外のガイドラインを参考にしたものを中心に実運用がなされていた。
- 特に***複数の組織が利害関係者となるような事案***において、***互いの持つ電磁的証拠の相互運用に対して障害***となりかねない。

（デジタル・フォレンジック研究会として、我が国における同関連技術の普及を目指す立場から）
このような状況に対処するため、我が国での**電磁的証拠の保全手続きの参考**として、様々な事案についてその特性を踏まえつつ広く利用して頂けるガイドラインを目指して作成されたもの

前回の「証拠保全ガイドライン」の改定にあたっての状況認識（追加）

- 最近では、サイバー攻撃で利用される技術や手法が急激に高度化及び複雑化しているため、コンピュータ・システムに残存する痕跡やログに依存するデジタル・フォレンジックで***実態解明をすることが困難になる場合が発生***し、更に、インターネットを積極的に利用したサービスやネットワークで繋がることを前提としたアプリケーションサービスを悪用したサイバー攻撃が増加傾向にあるため、***被害の発生する場が広範囲***になってきている。
- 従って、調査すべき対象が管理外のコンピュータ・システムに及ぶことになるため、自組織内で実態解明するには、その境界の内側に位置する装置等に残存する「ネットワーク上のパケット通信の流れの記録として残される様々なログ（以下、***ネットワークログ）等」を集約及び分析して攻撃実態を解明***する　ようになっている。
- また、最近のサイバー犯罪やサイバー攻撃で利用される不正プログラムは、痕跡を残さない回避技術が高度化しているため、コンピュータ・システム内に***残存する痕跡やログが極端な少なく***なってきている。

（デジタル・フォレンジック研究会として、我が国における同関連技術の普及を目指す立場から）
このような状況に対処するため、我が国での**電磁的証拠の保全手続きの参考**として、様々な事案についてその特性を踏まえつつ広く利用して頂けるガイドラインを目指して作成されたもの

今回の「証拠保全ガイドライン」の改定にあたっての状況認識（追加）

- 特に、***高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃が急増***しているが、このような正規プログラムが残すログや証跡のみでは悪意のある挙動を推し量ることは難しい。
- これを本格的に究明するには、電源供給を絶つと消失してしまう特性を持つ（揮発性が高い）メモリ空間に残存するスクリプト等を確保することである。そのため、メモリ上の情報の保全の重要性がさらに高まってきている。

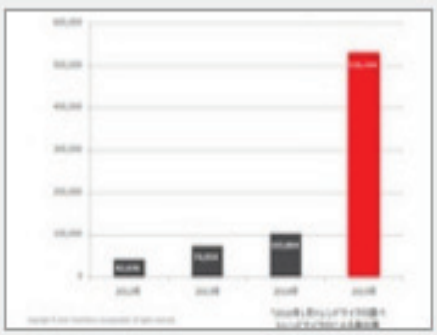
（デジタル・フォレンジック研究会として、我が国における同関連技術の普及を目指す立場から）
このような状況に対処するため、我が国での**電磁的証拠の保全手続きの参考**として、様々な事案についてその特性を踏まえつつ広く利用して頂けるガイドラインを目指して作成されたもの

トピック2

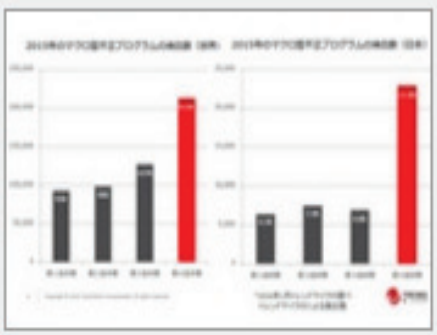
「高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃」について

「高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃」

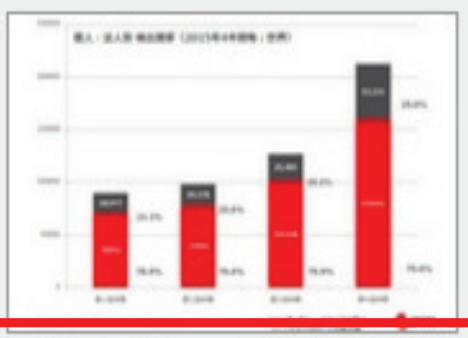
- 2016年1月29日、日本のトレンドマイクロ株式会社は、企業に対してメール添付の**マクロ型不正プログラム**の脅威が急増していると注意喚起した。



2012年～2015年におけるマクロ型不正プログラムの検出数（世界）



日本における第4四半期のマクロ型不正プログラム検出数が急増



検出されているマクロ型不正プログラムの8割弱は常に法人を標的にしたもの

http://scan.netsecurity.ne.jp/article/2016/02/01/38037.html

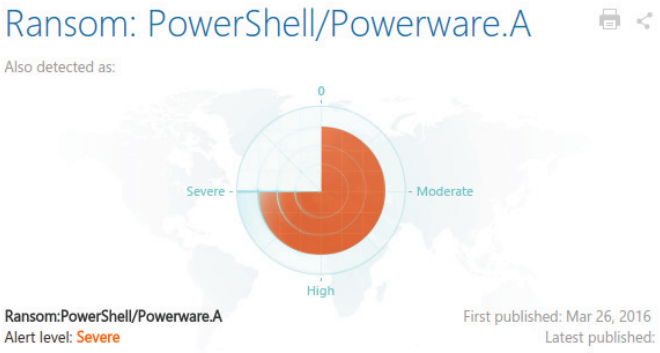
「高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃」

- 2016年3月25日、複数のセキュテリィ会社が PowerWave といわれる**マクロ型不正プログラム**によるランサムウェアの出現と深刻な脅威になり始めたことを警告。

Threat Alert: "PowerWare," New Ransomware Written in PowerShell, Targets Organizations via Microsoft Word

March 25, 2016 / Rico Valdez and Mike Sconzo / Advanced Threat Protection, Detection and Response, Endpoint and Server Security, Prevention, Response

https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/

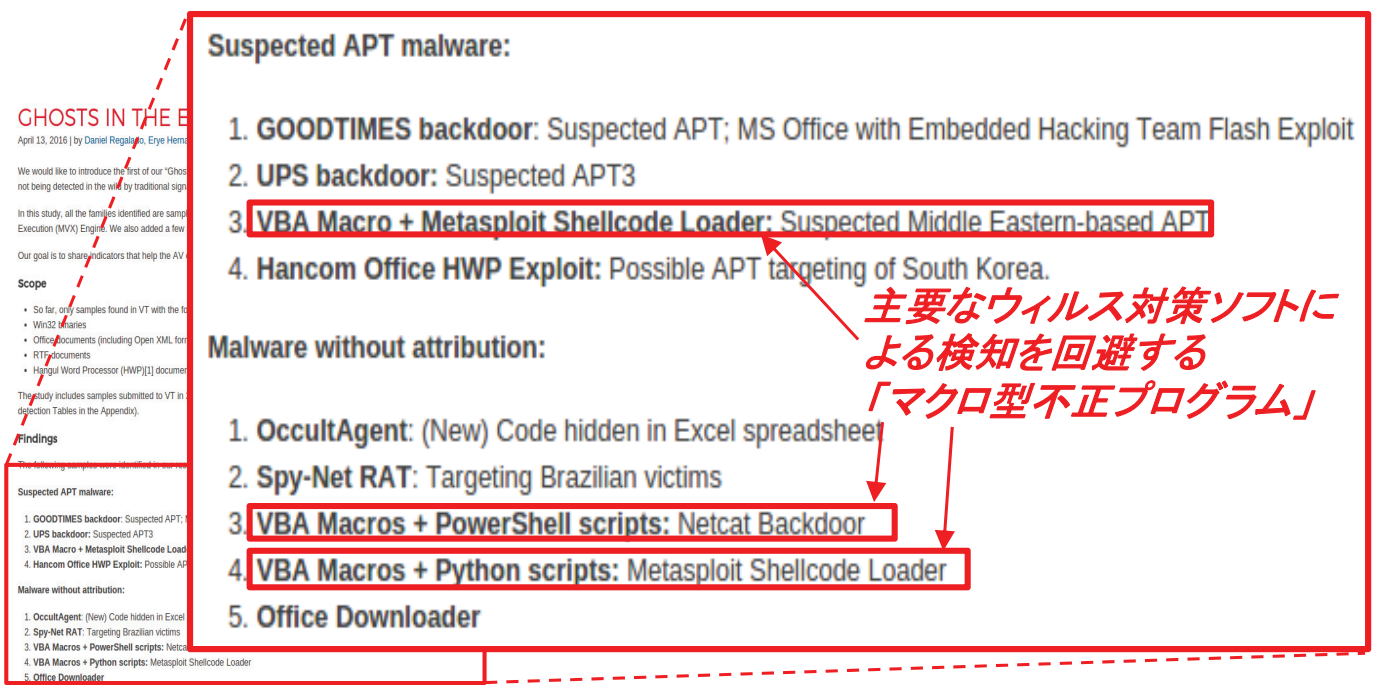


http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=RANSOM:POWERSHELL/POWERWARE.A

Our research found that "PowerWare" is delivered via a macro-enabled Microsoft Word document. The Word document then uses macros to spawn "cmd.exe," which in turn calls PowerShell with options that will download and run the malicious "PowerWare" code. In an interesting twist, "PowerWare" authors initially ask for a $500 ransom, which increases to $1,000 after two weeks.

「高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃」

- 2016年4月11日、FireEyeが**マクロ型不正プログラム**等による潜在脅威を解説。



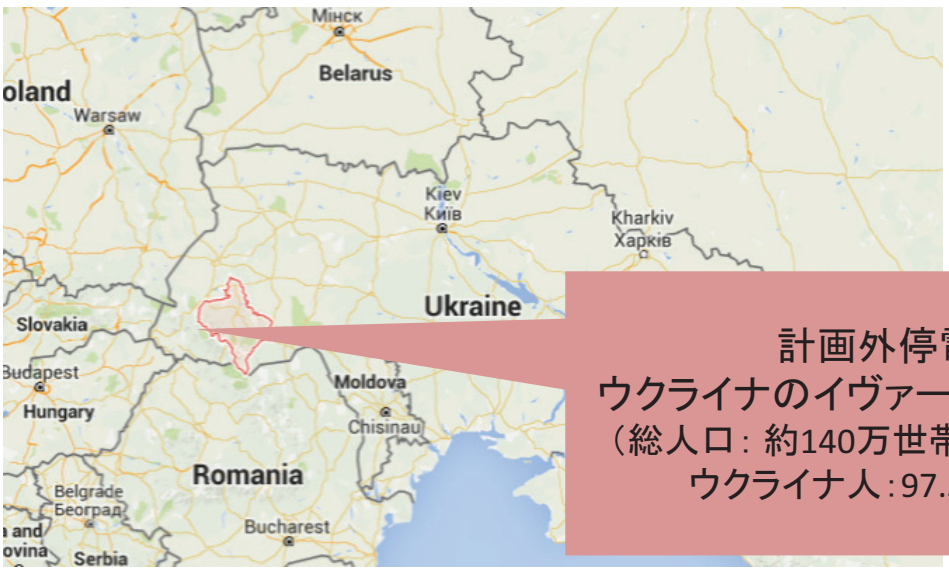
https://www.fireeye.com/blog/threat-research/2016/04/ghosts_in_the_endpoi.html

トピック3

「高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃」の事例

ウクライナの電力供給会社へのサイバー攻撃による計画外停電

- 2015年12月23日、ウクライナの複数の電力供給会社が、同時的なサイバー攻撃を受けて、イヴァーノ＝フランキーウシク州の約8万の顧客への電力供給に障害が発生した。
- ほぼ同時に、電力供給会社の電話回線にも障害が発生し、顧客からの全ての電話を受け付けることが出来なくなった。



計画外停電が発生した
ウクライナのイヴァーノ＝フランキーウシク州
（総人口：約140万世帯、都市人口：約59万世帯
ウクライナ人：97.5%、ロシア人：1.8%）

ウクライナの電力供給会社へのサイバー攻撃による計画外停電

- 最初の攻撃は、ウクライナ・エネルギー省を詐称したスピアフィッシングメールだった。

2015年1月6日に公表されたエネルギー省の情報

Державне підприємство
Національна енергетична компанія
УКРЕНЕРГО

Про компанію | Діяльність | Закупівлі | Розвиток | КСВ

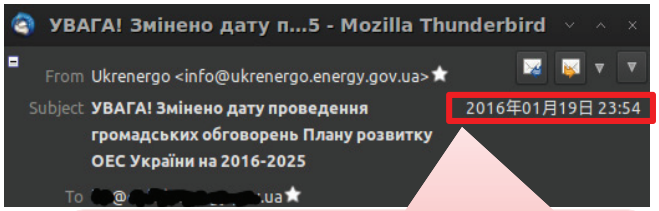
На головну Укренерго > Повна новина

Увага! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025

06 січня 2016 | Розвиток ОЕС України

На численні звернення представників електроенергетичної спільноти, а також з метою залучення ширшого кола учасників, проведення громадських обговорень та консультацій проекту "Плану розвитку ОЕС України на 2016-2025 роки" переноситься на 20 січня 2016 року. Місце та час проведення заходу залишаються без змін (Київська область, Макарівський район, с. Наливайківка, вул. Жовтнева, 112-Б, ПС 750 "Київська") ДП "НЕК "Укренерго" буде забезпечувати трансфер учасників за маршрутом м. Київ (вул. Симона Петлюри, 25) - ПС 750 кВ "Київська" - м. Київ (вул. Симона Петлюри, 25).

2015年1月19日に発生したスピアフィッシングメール



Attention! Changed the date of the public debate ECO Plan of Ukraine for 2016-2025

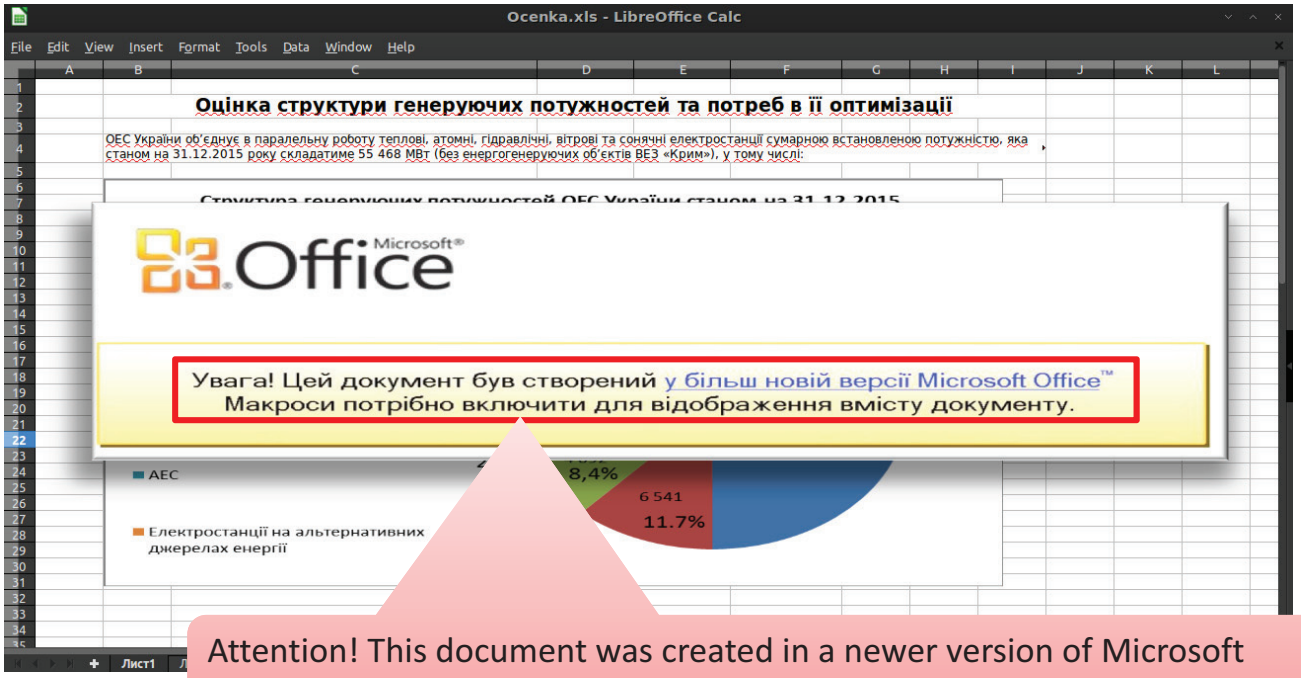
※メッセージソース中に、BlackEnergyグループ特有の攻撃手口が確認できる。

```
<DIV><IMG border=0 hspace=0 alt=""
src="http://62.210.[redacted]/bW[redacted]E=.png"></DIV>
<DIV> </DIV>
```

http://www.ukrenergo.energy.gov.ua/Pages/ua/DetailsNew.aspx?nID=2233

ウクライナの電力供給会社へのサイバー攻撃による計画外停電

- スピアフィッシングメールの添付されていたファイルは、Microsoft 社のオフィス文書（XLSファイル）で、マクロ型不正プログラムが動作する仕組みになっていた。



Attention! This document was created in a newer version of Microsoft Office. Macros are needed to display the contents of the document.

トピック4

その他の改定事項

経験者及び有識者の知見の反映

- 「考慮すべき事項」の大幅追加
  - WGメンバ及び専門的知見を有する関係者からいただいた「それぞれの手続き及び証跡やログ等における適正を確保するために考えていただきたい事項のこと」を各所に追加した。

1　事前に行う準備

インシデントレスポンス（初動対応、証拠保全）では、以下のような事前準備が必要と考えられる。

1.1　インシデントレスポンスを想定した初動対応、証拠保全プロセスの検討及び体制の確立

⑦ インシデントに備えたバックアップ、リストア体制の確立及びテスト

（考慮すべき事項）

・ バックアップやリストアに想定以上に時間がかかる、或いはバックアップデータの真正性が損なわれてしまう場合があるので留意する必要がある。

⑨ インシデントレスポンスを想定した初動対応、証拠保全の手順書の作成

（考慮すべき事項）

・ 初動対応に関わる部署との協力体制が、人事異動等により機能しなくなる場合があるので、留意する必要がある。

経験者及び有識者の知見の反映

1.3　インシデントレスポンス（初動対応、証拠保全）時に必要と考えられる資機材等の選定及び準備

⑦ カメラ、筆記用具等の準備

・ ビデオカメラ、作業確認チェックシート、一貫性追跡記録（ＣｏＣ）、備忘録用紙、ボールペン等

（考慮すべき事項）

・ ボールペンは、記述事項の改ざん防止をすることを期待しているため、消えるボールペンは避けること。

1.4　インシデントレスポンス時に使用する資機材等の熟達

③ 証拠保全作業に関わる技術力の修得や知見の蓄積に必要なトレーニング等の実施

（考慮すべき事項）

・ 熟達のために専門家や経験者のサポートが必要なことがある場合、付録「８　ＩＤＦ団体会員「製品・サービス区分リスト」（全３８社）」で示しているフォレンジック事業者が提供する教育サービスを利用することが考えられる。

経験者及び有識者の知見の反映

- 最新のマルウェア感染手段（ファームウェアへの感染等）の対応

3.2.1　対象物がコンピュータで、電源が OFF の状態の場合

・ ファームウェアのマルウェア感染や意図的な改ざんが行われる可能性がある場合は、電源を ON にするとインシデントが深刻化する場合がある。

「不正競争防止法」改正の反映

<不正競争防止法>

（定義）
第二条第六項
この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

（罰則）
第二十一条　次の各号のいずれかに該当する者は、十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科する。
一　不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。以下この条において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。）その他の保有者の管理を害する行為をいう。以下この条において同じ。）により、営業秘密を取得した者

<不正競争防止法>

（定義）
第二条第六項
この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

（罰則）
第二十一条　次の各号のいずれかに該当する者は、十年以下の懲役若しくは二千万円以下の罰金に処し、又はこれを併科する。
一　不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。以下この条において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。）その他の保有者の管理を害する行為をいう。以下この条において同じ。）により、営業秘密を取得した者
：
［中略］
：
3　次の各号のいずれかに該当する者は、十年以下の懲役若しくは三千万円以下の罰金に処し、又はこれを併科する。
一　日本国外において使用する目的で、第一項第一号又は第三号の罪を犯した者
二　相手方に日本国外において第一項第二号又は第四号から第八号までの罪に当たる使用をする目的があることの情を知って、これらの罪に当たる開示をした者
三　日本国内において事業を行う保有者の営業秘密について、日本国外において第一項第二号又は第四号から第八号までの罪に当たる使用をした者
4　第一項（第三号を除く。）並びに前項第一号（第一項第三号に係る部分を除く。）、第二号及び第三号の罪の未遂は、罰する。

「不正競争防止法」改正の解説（前版）

営業秘密に関する事項は不正競争防止法に定められている。曖昧な概念で使われる「企業秘密」という言葉とは異なり、「営業秘密」は同法の2条6項によってきちんとした定義がなされている。この条文から「秘密管理性」「有用性」「非公知性」が営業秘密成立の三要件となる。

条文自体の記載は省略しているが、不正競争防止法では、その第2条第1項の各号においてどのような行為が不正競争となるかが定められている。そして同4号～9号までが営業秘密に関しての記載であり、ここに不正と見なされる営業秘密の取得や使用、開示等における様々な場合が列挙されている。

そしてそれらを侵害した場合の罰則規定が第21条に記載されている。こちらもすべての条文の記載を省略しているが、第21条第1項の第1号～第7号の各号において刑罰が科される様々な場合を記載している。2009年(平成21年)の改正によって、競合関係にある場合だけでなく、自己の利益の為に営業秘密を不正に取得したり使用したりした場合でも可罰化されたことが特徴である。

2015年（平成27年）3月時点での刑罰の量刑は、最大で10年以下の懲役もしくは1000万円以下の罰金またはこの併科であるが、2014年に起きたベネッセでの営業秘密持ち出し事件を経て、これがさらに重罰化される予定なので注意しておく必要がある。

なお、営業秘密の管理に関する公的な指針としては「営業秘密管理指針」が経済産業省より公表されている(*1)。この指針は2015年（平成27年）1月に全面的な改定がなされ、従来の事例を詳細に記載する形式のものから「不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準の対策を示すもの」に変更された(*2)。

「不正競争防止法」改正の解説（今版）

営業秘密に関する事項は不正競争防止法に定められている。曖昧な概念で使われる「企業秘密」という言葉とは異なり、「営業秘密」は同法の2条6項によってきちんとした定義がなされている。この条文から「秘密管理性」「有用性」「非公知性」が営業秘密成立の三要件となる。**それ故、技術情報だけでなく顧客名簿などのビジネス情報も営業秘密となり得る。**

条文自体の記載は省略しているが、不正競争防止法では、その第2条第1項の各号においてどのような行為が不正競争となるかが定められている。そして同4号～10号までが営業秘密に関しての記載であり、ここに不正と見なされる営業秘密の取得や使用、開示等における様々な場合が列挙されている。**2015年（平成27年）には新たに、営業秘密侵害品の譲渡、引渡し、輸出入、電気通信回線を通じた提供等が不正競争行為として追加された。**

そしてそれらを侵害した場合の罰則規定が第21条に記載されている。こちらも条文のすべてを記載することは紙面都合でしていないが、第21条第1項の第1号～第9号の各号において刑罰が科される様々な場合が規定されている。2009年(平成21年）の改正によって、競合関係にある場合だけでなく、自己の利益の為に営業秘密を不正に取得したり使用したりした場合でも可罰化された。**それ故、金銭目的で営業秘密を持ち出して他人に売却した場合も当然に犯罪となる。**

ベネッセからの顧客名簿の漏洩、そして東芝・サンディスクや新日鉄住金からの技術情報の海外漏洩などといった深刻な流出事件が続いたため、2015年（平成27年）7月の法改正時に、罰則が大幅に強化された。まず、営業秘密漏洩罪の法定刑が「10年以下の懲役若しくは2千万円以下の罰金、又はこれを併科」となった（21条1項）。法人の場合は最大5億円の罰金。さらに海外重罰制度（21条3項）が取り入れられ、国外への漏洩や国外で使用する目的での持出に対しては、罰金額の上限が個人で3千万、法人で10億円となる。

さらに、営業秘密の三次取得者・四次取得者といった転得者も営業秘密を不正取得・不正使用した場合は処罰対象となった（21条1項8号）。**これによって流出した顧客名簿を販売した者などを取り締まることができる。**

「不正競争防止法」改正の解説（今版）

注目すべき点として、今期改正より営業秘密侵害の未遂罪が追加されており（21条4項）、経済産業省の解説資料(*1) によれば、**「取得未遂」として『不正アクセス行為は確認されたが、証拠の隠滅等により営業秘密たる情報の持ち出しの事実を確認できなかった場合。社内メールシステムの管理者の地位を利用し、社内幹部宛のメールが自動で自らにも転送されるようなプログラムを埋め込んでいたが、実際に営業秘密情報が転送される前に明るみに出た場合。』が、「開示未遂」として『営業秘密を電話で売り込み、その後メールで営業秘密を不正に開示するべく、送信しようとしたが、メールソフトの不具合により転職先に到達しなかった場合。』が例示されている。**よってデジタル・フォレンジックの作業としてはこれらの行為の痕跡を探すことになる。

また、営業秘密を蔵置したサーバが海外にあったとしても、**日本国内において事業を行う保有者の情報であれば不正取得となり処罰対象となることも明記された**（21条6項）。さらに、**犯罪収益の没収制度の導入**（21条10項）、**非親告罪化、営業秘密の不正使用に対する差止請求可能期間（除斥期間）の20年への延長**（15条）といった強化等が行われている。

なお、営業秘密の管理に関する公的な指針としては「営業秘密管理指針」が経済産業省より公表されている(*2)。この指針は2015年（平成27年）1月に全面的な改定がなされ、従来の事例を詳細に記載する形式のものから「不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準の対策を示すもの」に変更された(*1)。

「代表的な収集及び分析ツール」の更新

●システム関連の情報取得ツールの例

- **analyzeMF**
  NTFSファイルシステムからMFTのファイルを解析するツール。
  nalyzeMFT
  https://github.com/dkovar/analyzeMFT
- **CDIR Collector**
  Windowsから主要データを保全するためのオープンソース等を活用したツールセット。
  CDIR Collector
  https://github.com/CyberDefenseInstitute/CDIR
- **Event Log Explorer**
  ローカルコンピュータのイベントログの詳細分析や、ネットワーク上の複数のコンピュータのイベントログを集中管理できるツール。
  Event Log Explorer™ for Windows event log management
  http://eventlogxp.com
- **Log Parser**
  さまざまなログの中から必要な情報を検索し、特定の情報を抜き出するツール。並べ直しやExcel用のデータで出力するなど、多様なログ分析を支援する。
  Log Parser 2.2
  http://www.microsoft.com/download/en/details.aspx?id=24659
- **Log Parser Lizard**
  上述のLog Parse をGUI で使えるようにするツール。
  Lizard Labs
  http://www.lizard-labs.net

「代表的な収集及び分析ツール」の更新

●システム関連の情報取得ツールの例（続き）

- **FTK Imager Lite**
  ハードディスクの情報の参照や、メモリダンプの出力、VM などのイメージファイルの読み込みなどを行うツール。
  FTK Imager Lite　http://accessdata.com/product-download/digital-forensics/
- **triage-ir**
  Windowsシステムでマルウェアの攻撃痕跡等の調査に必要となる情報を自動収集するツール。
  triage-ir　https://code.google.com/p/triage-ir/
- **RTIR**
  Request Tracker for Incident Response の略。インシデントハンドリングに係るワークフローを最適化するためのツール。
  RTIR: RT for Incident Response　https://www.bestpractical.com/rtir/

●揮発性メモリの情報取得及び解析ツールの例

- **Belkasoft Live RAM Capturer**
  32/64 bitにそれぞれ対応した無償のメモリダンプツール
  https://belkasoft.com/ram-capturer
- **HBGary Responder Professional**
  HBGary社によって開発・販売されている商用のメモリフォレンジックツール。そのオプション機能として提供されているDigital DNAは、プロセスアドレス空間に含まれるコードを分析して、悪性のコードかどうかをスコアリングする。
  Digital DNA　http://www.countertack.com/countertack-technology-digital-dna

「代表的な収集及び分析ツール」の更新

●揮発性メモリの情報取得及び解析ツールの例（続き）

- **Magnet RAM Capture**
  物理メモリのキャプチャや、データの復旧及び解析ができるフリーツール。
  Acquiring Memory with Magnet RAM Capture
  http://www.magnetforensics.com/acquiring-memory-with-magnet-ram-capture/
- **MoonSols Windows Memory Toolkit**
  メモリの取得や変換を実行するために必要なすべてのユーティリティを含むツール。
  MoonSols Windows Memory Toolkit
  http://www.moonsols.com/windows-memory-toolkit/
- **Redline**
  Mandiant社によって開発・提供されているフリーツール。同社で開発されているMemoryzeという解析ツールのGUIフロントエンドとして使われている。
  Redline ®
  https://www.mandiant.com/resources/download/redline
- **Rekall**
  Googleが提供しているオープンソースのメモリ解析フレームワーク
  http://www.rekall-forensic.com/
- **Volatility Framework**
  オープンソースのメモリフォレンジックツール。プロセス情報の列挙など基本的な機能のほか、有志によって様々なプラグインが提供されている。
  volatility An advanced memory forensics framework
  http://code.google.com/p/volatility/

「代表的な収集及び分析ツール」の更新

●スマートフォンのデータ取得ツールの例

- **Magnet Acquire**
  Magnet Forensics社が開発及び提供しているスマートフォンの論理データの取得をするツール。無料でありながら、Rooting に対応している。
  Magnet Acquire
  https://www.magnetforensics.com/magnet-acquire/

トピック5

今後の改定について

今後の改定について

- 次の領域の知見を反映すべく、WGメンバ及び関係する有識者で議論を重ねていきたい。
  - **ネットワークフォレンジック**
  - **M2M／IoT（スマートメーター等）**
  - **モバイルデバイス**

本資料に関する連絡先

名和 利男（Toshio NAWA）
サイバーディフェンス研究所
専務理事／上級分析官

Email: nawa@cyberdefense.jp
SNS: about.nawa.to
Tel: 03-3242-8700

Office: www.cyberdefense.jp
Response Team: www.cirt.jp