CyberDefense

証拠保全ガイドライン第6版の説明

2017年 6月

サイバーディフェンス研究所
名和 利男

アジェンダ

1. 「証拠保全ガイドライン」とは
2. 改定にあたっての状況認識
3. 第5版から第6版の主な改定事項
4. 関連文書の紹介

トピック 1

「証拠保全ガイドライン」とは

「証拠保全ガイドライン」とは

- 想定読者
  - 主に、インシデントの現場で最初に電磁的証拠の保全にあたる「**ファースト・レスポンダー**」
  - これに限らず、これに限らず、**デジタル・フォレンジック関連技術を運用する全ての者**

- 主な特徴
  - （証拠保全ガイドラインに記述されている）手続きにより収集・取得・保全等された電磁的記録が法廷において証拠として必ず採用されることを**保証するものではない**。
  - 犯罪捜査や金融調査等、それぞれの**特性と法制に基づく手続きが存在することを前提**としたものである。
  - 我が国における電磁的証拠保全の一般的な手続きがどうあるべきか、どの程度まで行えばデータが「法的紛争・訴訟に際し利用可能な（Forensically-soundな）」電磁的証拠となりうるか、という運用現場の悩みに対し、**コンセンサスの形成の一助**になることを意図して作成されたもの。

「デジタル・フォレンジックとは」

インシデントレスポンス（*コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。*）や**法的紛争・訴訟**に際し、電磁的記録の**証拠保全**及び**調査・分析**を行うとともに、電磁的記録の改ざん・毀損等についての**分析・情報収集**等を行う一連の科学的調査手法・技術を言います。
https://digitalforensic.jp/home/what-df/

コンセンサスの例：**「自由心証主義」**

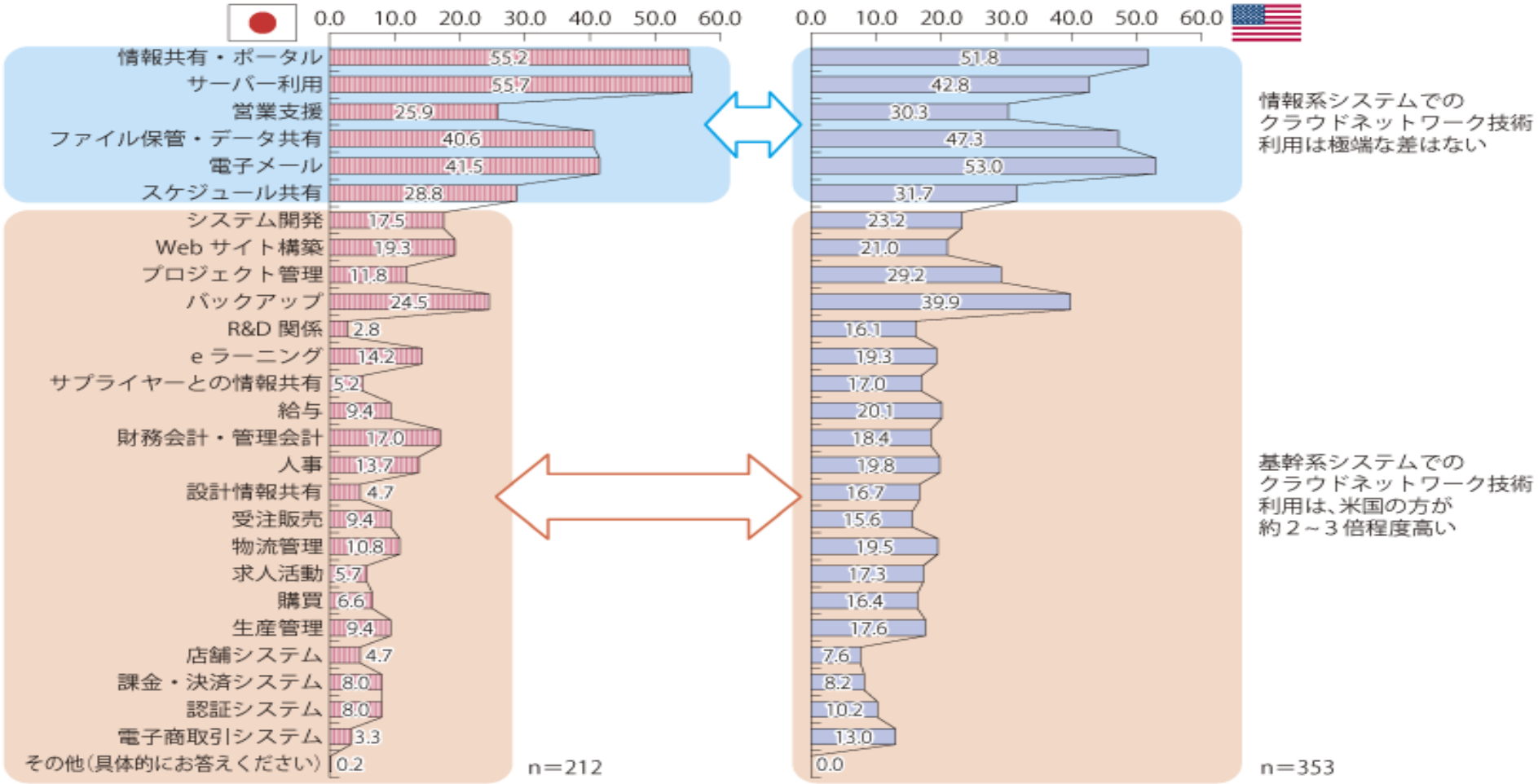
訴訟法上の概念で、事実認定・証拠評価について裁判官の自由な判断に委ねることをいう。裁判官の専門的技術・能力を信頼して、その自由な判断に委ねた方が真実発見に資するという考えに基づく。

トピック 2

改定にあたっての状況認識

改定にあたっての状況認識（1）

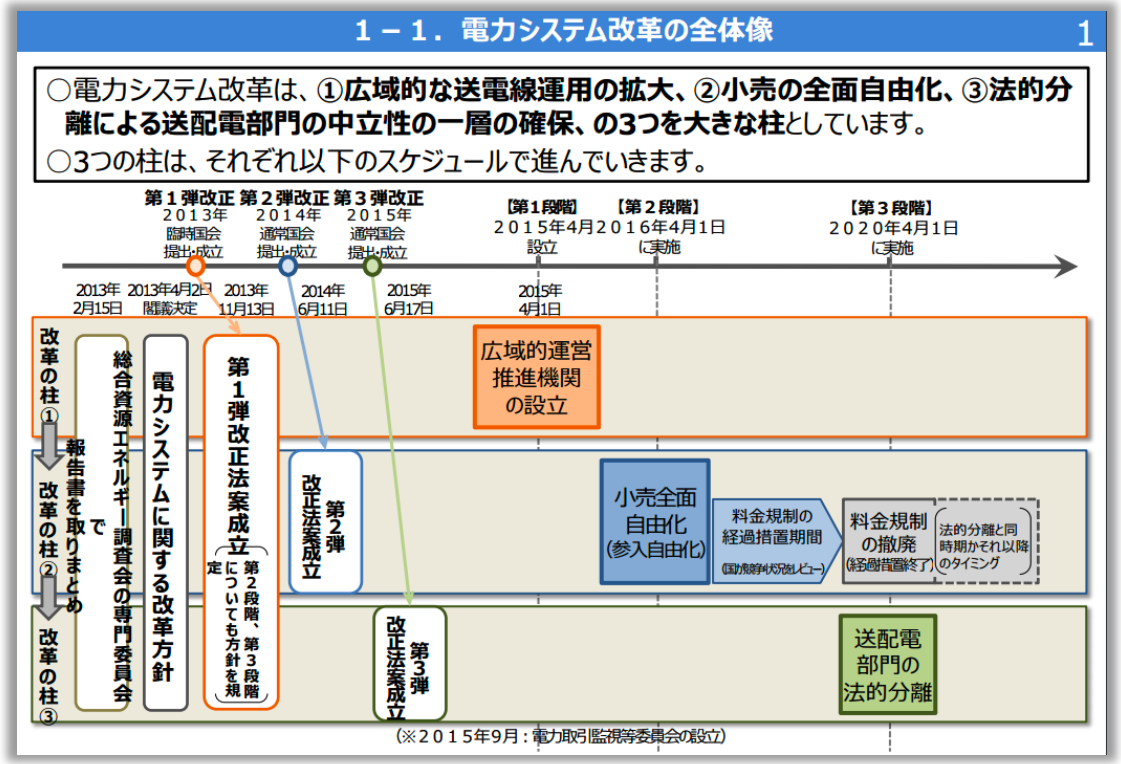
- 民間企業における**基幹業務のクラウド化**が進展。



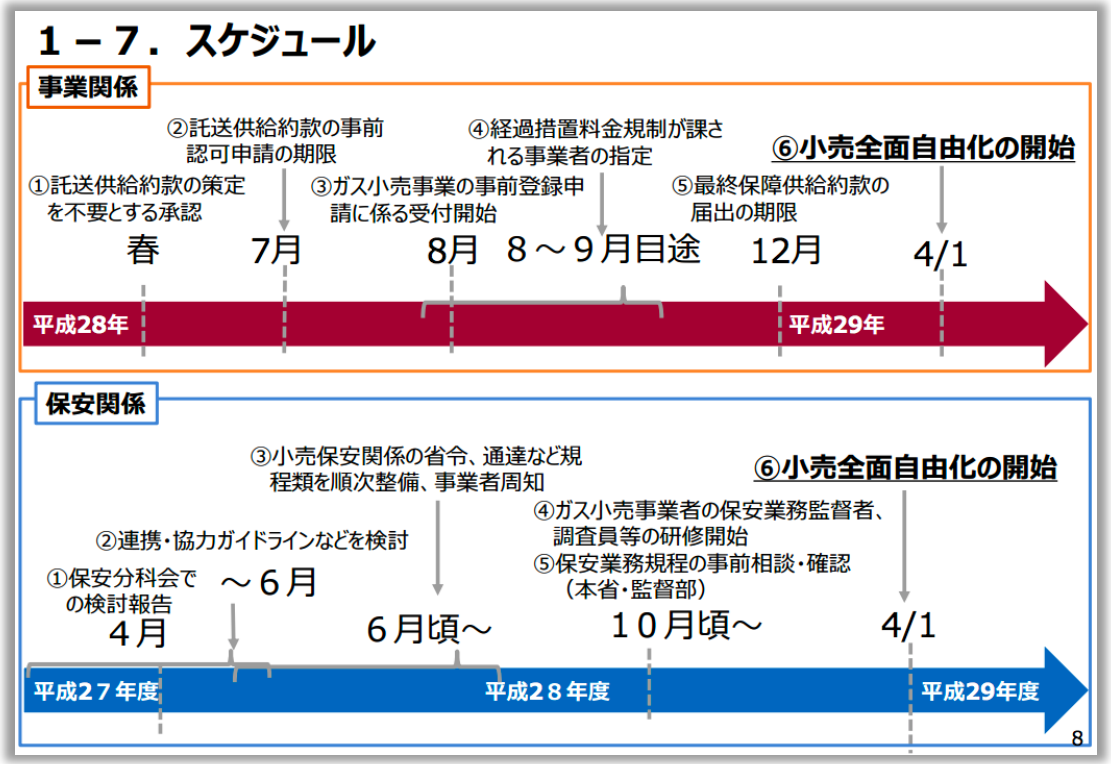
出典：「平成24年版情報通信白書」（総務省）クラウドサービスの利用内訳（日米比較）
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc244220.html

改定にあたっての状況認識(2)

- 様々な**産業領域における規制緩和や自由化**により、付加価値の高いサービス提供、業務効率の向上そしてコストダウン等のために、産業制御システムの領域において汎用技術や汎用製品の導入が積極的に行われている



出典:「電力システム改革について」(経産省)
http://www.enecho.meti.go.jp/category/electricity_and_gas/electric/electricity_liberalization/pdf/system_reform.pdf

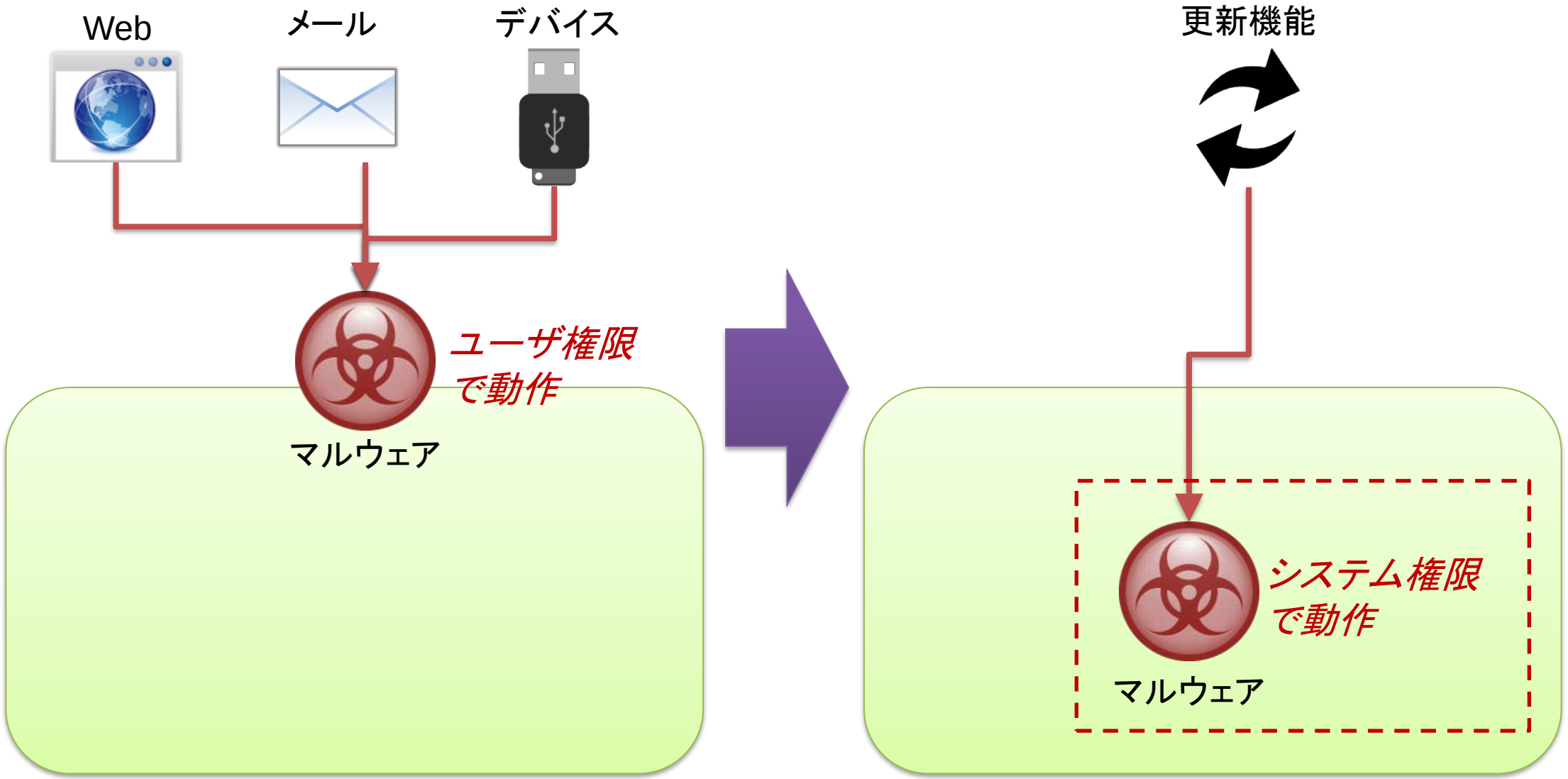


出典:「ガス保安のスマート化の対応状況について」(経産省)
http://www.meti.go.jp/committee/sankoushin/hoan/pdf/006_02_03.pdf

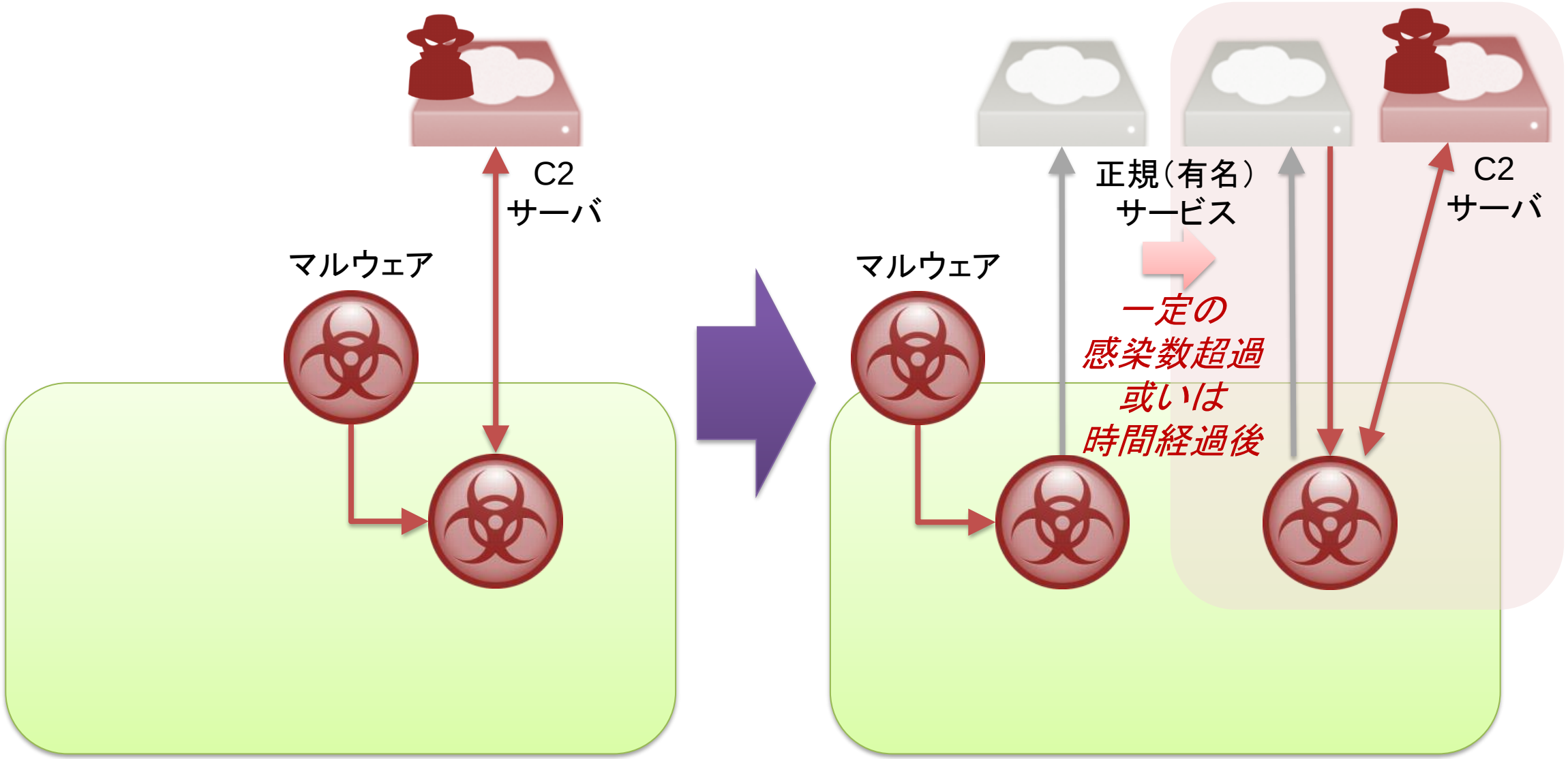
改定にあたっての状況認識(3)

- サイバー攻撃の技術や手法が**急激に高度化及び複雑化**
  - **更新機能を利用するマルウェア感染**
  - **正規(有名)サービスを(時間差で)踏み台にするC2通信**
  - **スクリプト実行環境を利用した正規プログラムによる挙動**
  - **正規(有名)サービスの同期機能を利用するC2通信**

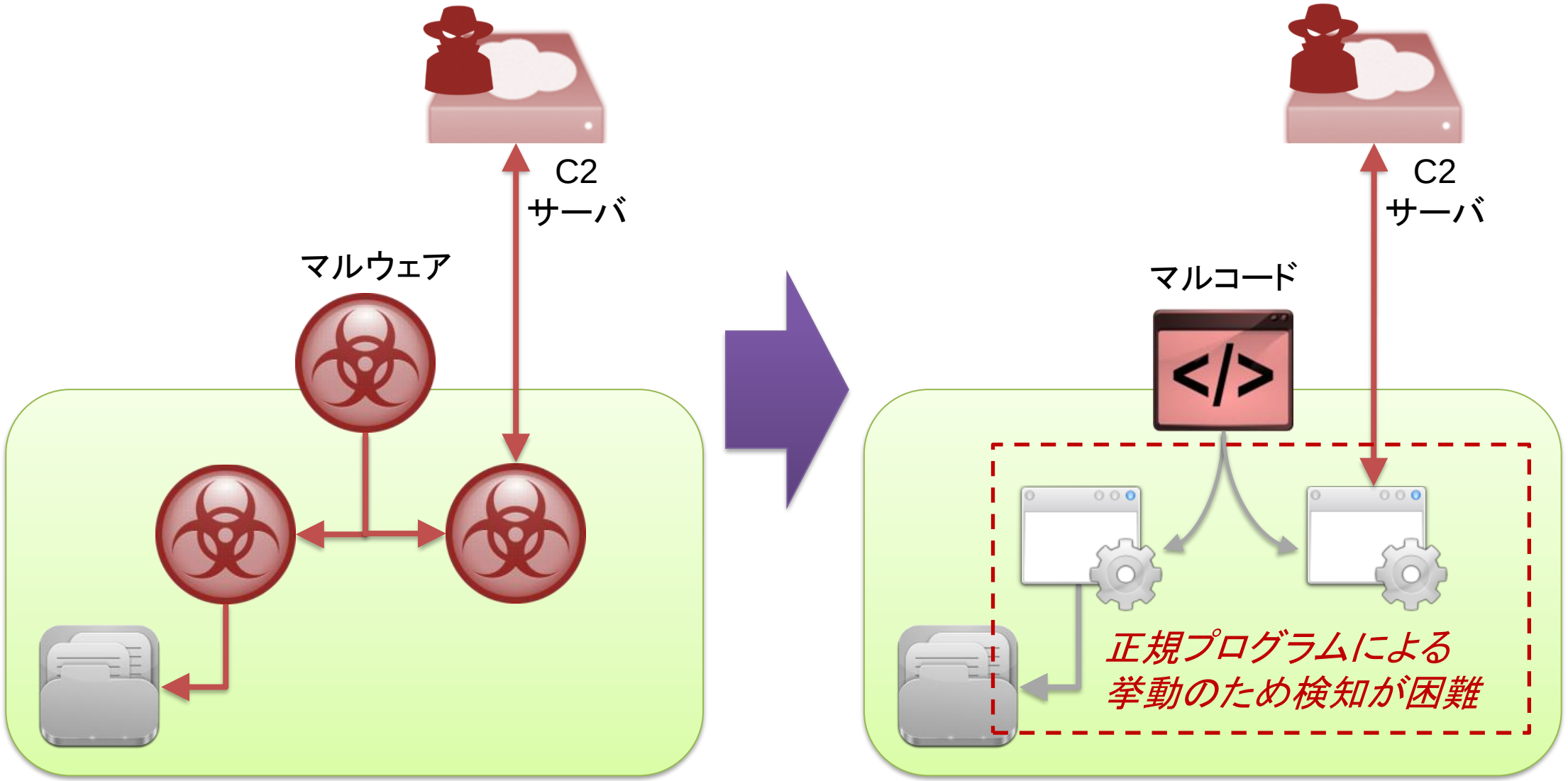
更新機能を利用するマルウェア感染



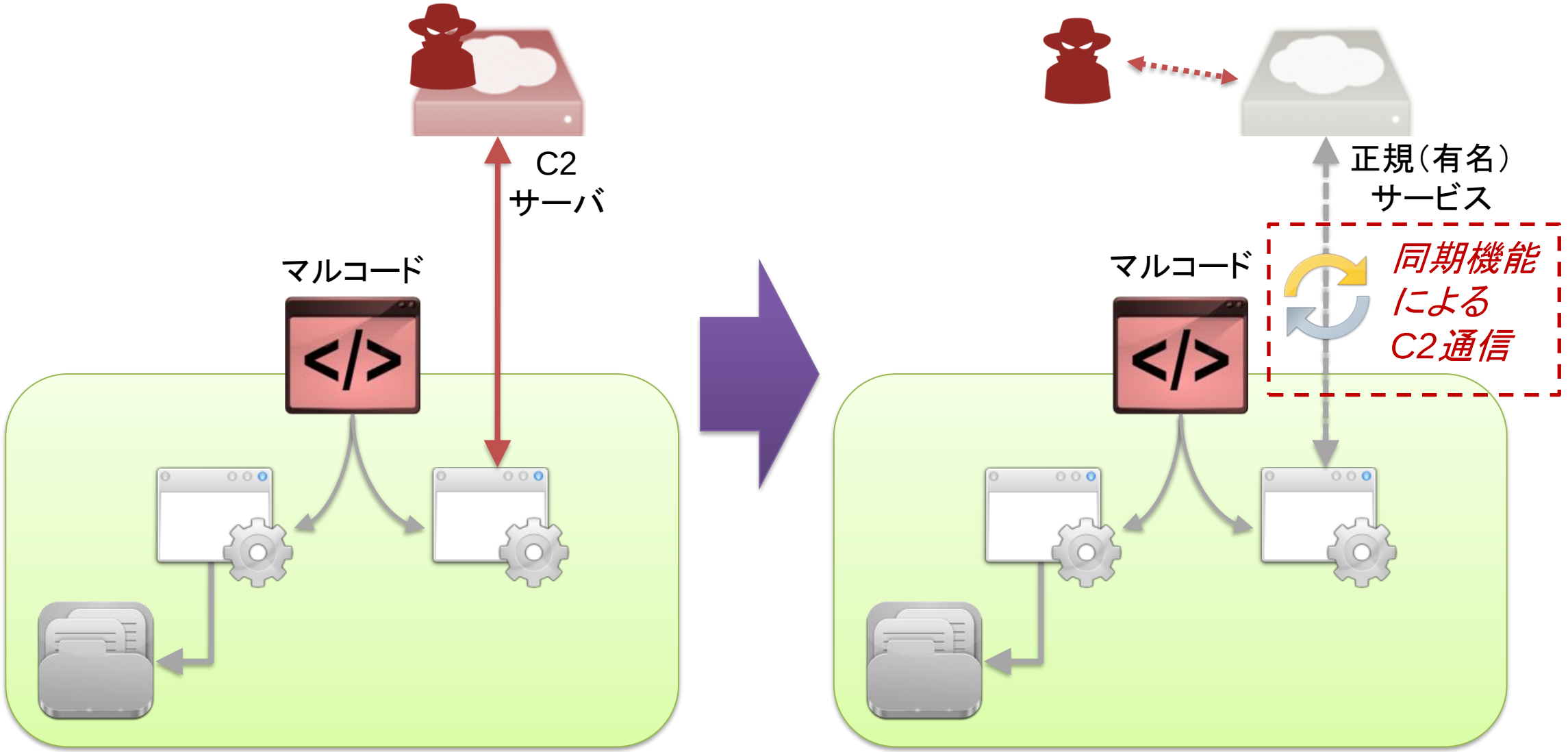
正規(有名)サービスを(時間差で)踏み台にするC2通信



スクリプト実行環境を利用した正規プログラムによる挙動

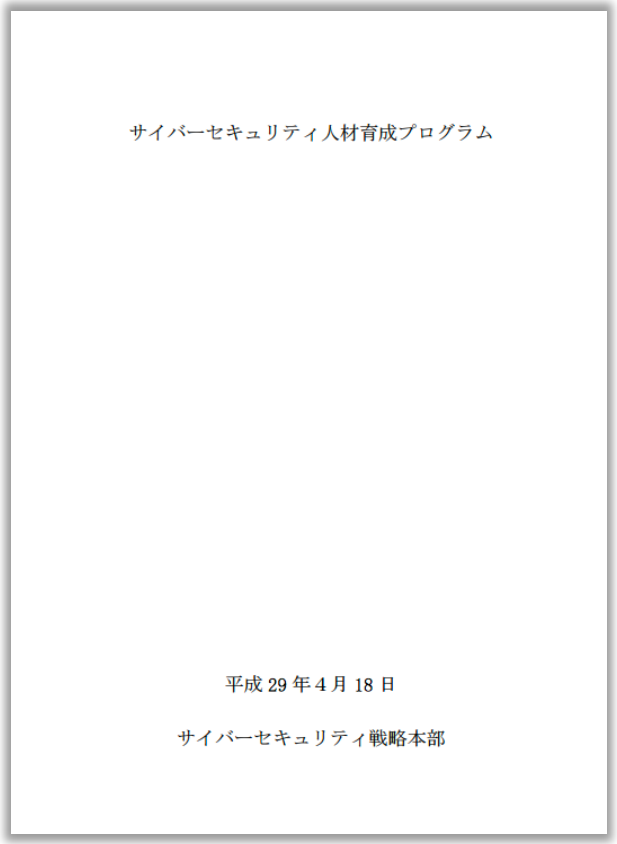


正規(有名)サービスの同期機能を利用するC2通信



改定にあたっての状況認識(4)

- **セキュリティ人材**の育成機運の高まり


サイバーセキュリティ人材育成プログラム

平成 29 年 4 月 18 日

サイバーセキュリティ戦略本部

https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf

http://www.nict.go.jp/nct/

https://www.ipa.go.jp/icscoe/

トピック 2（京都向け特別資料 – Arbor Networks）

改定にあたっての状況認識（追加）※非公開

トピック 3

第5版から第6版の主な改定事項

第5版から第6版の主な改定事項(1)

- 「発生した**インシデントの内容**」の改定

2.1.1.1　発生したインシデントの内容

① 情報流出

② マルウェア感染・発症

③ 不正侵入・持ち出し、コンプライアンス違反

④ 設定ミス、操作ミス、物理的故障・破壊

2.1.1.1　発生したインシデントの内容

① 情報流出・データ破壊

② 不正プログラム（マルウェア、悪意のあるスクリプト等 の実行

③ 不正アクセス・不許可の持ち出し、コンプライアンス違反

④ 設定ミス、操作ミス、物理的故障

⑤ システム悪用、破壊行為 内部犯行

第5版から第6版の主な改定事項(2)

- 「**関係組織**との連携」に “CSIRT担当者” を追加

2.3.2　関係組織との連携

① 法務部門担当者、システム担当者との連携

② システム設計者又は管理者との関係構築

例：構成が複雑な

③ 内部監査・システ

依頼元組織内のセ

④ 関係者の確保及び

インシデントレス

オンサイトで作業

⑤ 解析担当者との連

2.3.2　関係組織との連携

① CSIRT 担当者、法務部門担当者、システム担当者との連携

② システム設計者又は管理者との関係構築

例：構成が複雑なシステム全体ないしその一部の証拠保全を行う際等

③ 内部監査・システム監査担当者との連携

依頼元組織内のセキュリティやプライバシー施策を十分に考慮・遵守

④ 関係者の確保及び無関係者の排除

インシデントレスポンス作業工程において、関係ない第三者が関与できない状況を確保。また、

オンサイトで作業を行う場合は、依頼元の担当者が常駐するように心がける。

⑤ 解析担当者との連携

第5版から第6版の主な改定事項(3)

- 「**インシデント発生の検知**の経緯」の改定

2.1.1.2　インシデント発生の検知の経緯

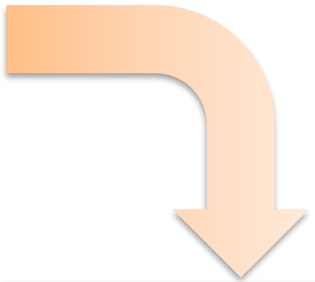
① ログのレビュー

② 不正検知システム

③ 内部告発

④ 自己申告

⑤ 外部からの通報



2.1.1.2　インシデント発生の検知の経緯

① ログのレビュー

② 不正検知システム

③ 内部通報

④ 異常事象の発見・認知

⑤ 外部からの通報

第5版から第6版の主な改定事項(4)

- 「**収集・取得・保全するための対象物の処置**」に ”WiFi等の措置を追加。

⑥ 無為に HDD にデータの書き込み等が発生しないように、ケーブル類は全て筐体から取り外す。

- 電源ケーブル、キーボード・マウス、USB 系のコネクタ類を取り外す。
- 用途不明の接続ケ
  認し、証拠保全作
- 各装置・ケーブル
  帰を可能にするた
  タグ、専用の荷札
  対象となる機器の

⑥ 無為に HDD／SSD にデータの書き込み等が発生しないように、ケーブル類は全て筐体から取り外す。

- 電源ケーブル、キーボード・マウス、USB 系のコネクタ類を取り外す。
- WiFi（無線 LAN）及び Bluethooth の機能を停止する。
- 用途不明の接続ケーブルの場合は、その接続ケーブルについて熟知している人物に用途等を確認し、証拠保全作業の責任者の指揮の下、作業を行う。
- 各装置・ケーブルの取り外しの際は、解析時におけるシステムの正確な再現、作業後の現状復帰を可能にするため、どのケーブルや機器が、どこに取り付けられていたかを、粘着性の低いタグ、専用の荷札タグ等を貼って明確にする（記録シートに明記／写真撮影等）。特に証拠保全対象となる機器の固有情報（製造番号、型式等）は確実に記録する。

第5版から第6版の主な改定事項(5)

- 「**信頼できる機関**による検証」に “IDFの日本語処理解析性能評価” を追加

4.3.2　信頼できる機関による検証

○ CFTT（Computer Forensics Tool Testing[23]）等の信頼できる機関にて検証されたものを利用

4.3.2　信頼できる機関による検証

○ CFTT（Computer Forensics Tool Testing[23]）等の信頼できる機関にて検証されたものや IDF の日本語処理解析性能評価を受けたものを利用

参考：第1回「日本語処理解析性能評価」実施結果報告

https://digitalforensic.jp/wp-content/uploads/2017/03/jpap_report01_20170301-15.pdf

第5版から第6版の主な改定事項(6)

- 「**サービス利用状況**のチェック」に “Cookei情報” を追加

5.6.3　サービスの利用状況のチェック

Web ブラウザ若しくは専用のクライアントツールを用いてサービスにアクセスし、アカウント及びパスワードを入力して、ログインする。正常に対象サービスへのアクセスが確認された後に、対象ユーザの利用状況を確認するために、サービスの基本設定項目及びサービス利用履歴の記録を作成する。

5.6.3　サービスの利用状況のチェック

Web ブラウザ若しくは専用のクライアントツールを用いてサービスにアクセスし、アカウント及びパスワードを入力して、ログインする。正常に対象サービスへのアクセスが確認された後に、対象ユーザの利用状況を確認するために、サービスの基本設定項目、Cookie 情報及びサービス利用履歴の記録を作成する。

トピック 4

関連文書の紹介

Cybercrime Investigation Body Of Knowledge（トレンドマイクロ社がサポート）

Cybercrime Investigation Body Of Knowledge

› English › Japanese

Top ニュース CIBOK について CIBOK編集委員会運営について ダウンロード お問い合わせ ストア

TOP / ニュース / サイバー犯罪捜査のための新標準としてCYBERCRIME INVESTIGATION BODY OF KNOWLEDGEを発表

サイバー犯罪捜査のための新標準としてCybercrime Investigation Body Of Knowledgeを発表

CIBOK編集委員会は、委員会の設立と「CIBOK：Cybercrime Investigation Body of Knowledge」第1版の出版を発表します。CIBOKは全世界の法執行機関や企業向けに、今日の複雑化したサイバー犯罪を解決、予防するための知識、スキル、行動を提供することを目的としています。CIBOKの第1版は英語、日本語で出版されます。

「サイバー犯罪が、注目を集めたい、または能力の誇示を目的とした個人的な活動から、より巧妙で明確な目的を持った組織的な活動へと進化するにつれて、我々にとっては、彼ら犯罪者の目的や動機を理解することに注力することが重要になっていきています」と、CIBOKの主席編集者であり、CIBOK編集員会委員長であるシェーン・シュック博士（Shane Shook , Ph.D.）は述べます。

「我々は、手段、動機、犯罪者を特定する可能性の観点から犯罪を捜査しています。にもかかわらず、サイバー犯罪捜査官はこれまでツールや技術、手順に注目して捜査を行っていました。CIBOKでは、これまでの捜査アプローチとサイバー捜査のアプローチの最適な融合、さらにはサイバー犯罪活動に関する社会、企業の理解を集約した新標準の提供を目的としています。これはグローバルでのサイバー犯罪に対する、官民による連携、協力を実現する1歩となると我々は期待しています。」

CIBOKでは、法執行機関担当者や企業のリスク管理担当者がサイバー犯罪を調査するために必要とされるニーズ、背景、要求事項を記載しており、下記の5つの目的の達成を目的としています。

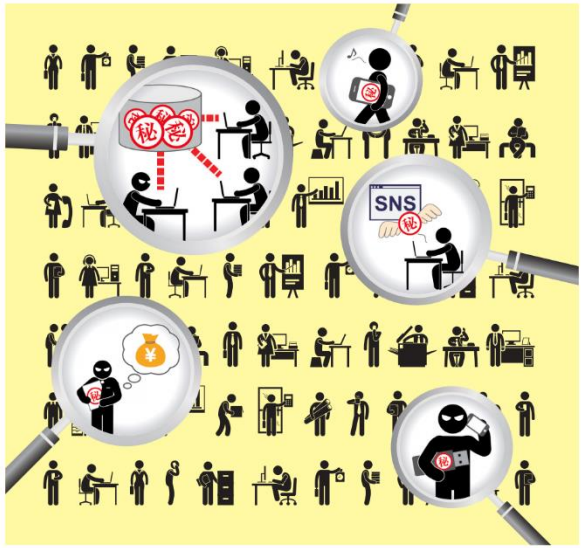
- 全世界で一貫したサイバー犯罪に関する心得（Common Sense Approach）を普及・促進すること
- 他の体系化された実務慣行について、サイバー犯罪捜査の範囲における位置づけを詳細に示すこと
- サイバー犯罪捜査において実践すべき内容を、特徴づけして示すこと
- サイバー犯罪捜査知識体系に対して、トピックスを利用するための手段を提供すること
- トレーニングカリキュラム開発および、業務に携わる個人の知識とスキルが高い水準のレベルであることの保証に必要な基礎を提供すること

https://www.cibok.org/ja/cybercrime-investigation-body-of-knowledge/

組織における内部犯行対策ガイドライン（IPA）

IPA

組織における
内部不正防止ガイドライン



独立行政法人 情報処理推進機構

https://www.ipa.go.jp/files/000057060.pdf

4-9.事後対策

（２７）事後対策に求められる体制の整備

内部不正の影響範囲を特定するために、事象の具体的状況を把握するとともに、被害の最小化策や影響の拡大防止策を実施しなければならない。また、必要に応じて組織内外の関係者との連携体制を確保しなければならない。

■どのようなリスクがあるのか？

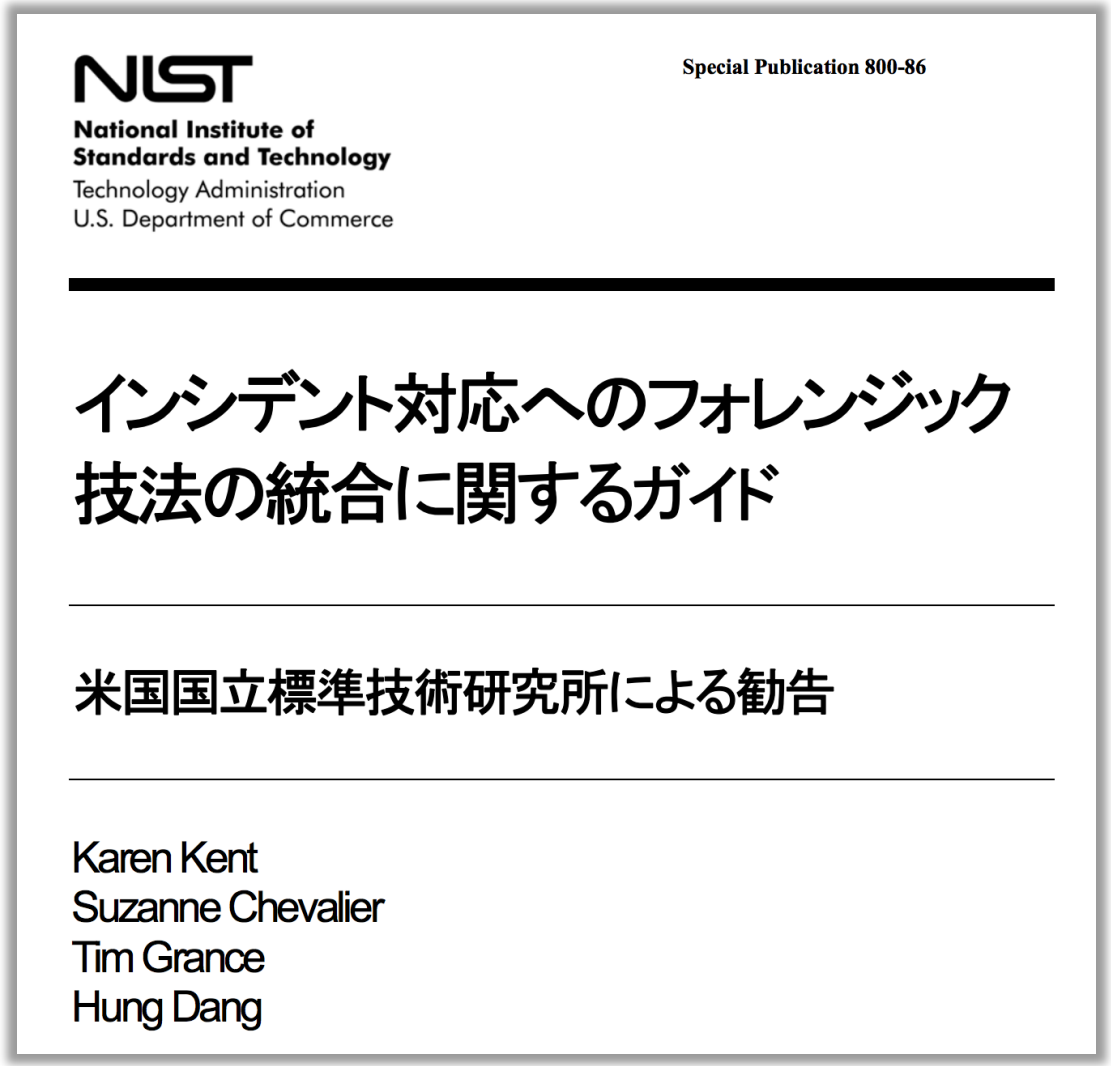
内部不正の影響範囲を特定できないと、迅速な事後対策が施せないだけではなく、法的処置等の対応を検討できなくなる可能性もあります。さらに、内部不正の調査や対処について第三者サービス（デジタル・フォレンジック[49]解析やインシデントレスポンス[50]支援等）を利用する際に必要となる情報や伝達方法を取り決めておかない場合には、適切なサービスを受けられない恐れがあります。

■対策のポイント

事後対策に求められる体制を構築するためには、以下のような内容を整備することが必要です。

1. 内部不正による被害の最小化、及び影響の拡大を防止するために、求められる対応手順や報告手順等を事前に取り決めておくことが必要です。内部不正の具体的な状況を把握し、影響範囲を調査するためには、「いつ、誰が、何をしたのか」に関する検証可能な証拠[51]を保全することが必要です。
2. 内部不正への対応については、システム管理者、インシデントレスポンス担当者（外部のインシデントレスポンス支援担当者を含む）、デジタル・フォレンジック解析担当者（外部支援担当者を含む）、弁護士、内部監査者等と連携することが必要です。

インシデント対応へのフォレンジック技法の統合に関するガイド（米国NIST）



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-86

インシデント対応へのフォレンジック技法の統合に関するガイド

米国国立標準技術研究所による勧告

Karen Kent
Suzanne Chevalier
Tim Grance
Hung Dang

https://www.ipa.go.jp/files/000025351.pdf

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