Internet Week 2015

【S14】CSIRT時代のSOCとのつき合い方 2015

最新のサイバー攻撃に対応するプライベートSOCのご紹介

2015年11月19日

株式会社NTTデータ 品質保証部 情報セキュリティ推進室
NTTDATA-CERT
大谷 尚通

NTT DATA

1.1 もくじ

1. NTTDATA-CERTの紹介

1.2 NTTDATA-CERTのプロフィール

NTT DATA

■名称: NTTDATA-CERT

■所属: NTTデータ 品質保証部 情報セキュリティ推進室

■主な活動:

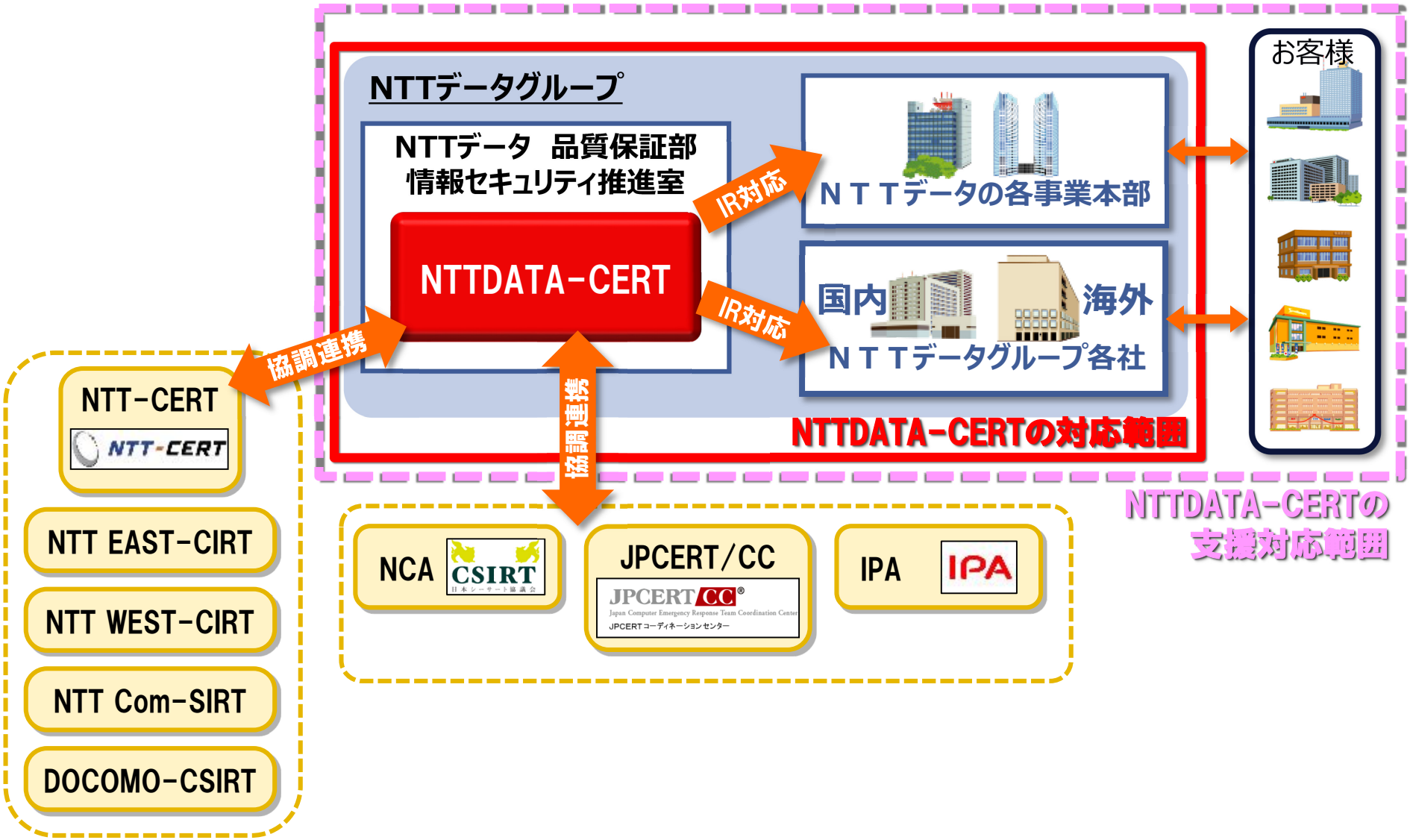
- 情報収集、情報分析、情報発信
- 通信監視
- 緊急対応
- 研究開発、外部連携

■活動範囲:

- NTTデータ、NTTデータグループ 国内/海外各社
- お客様
- NTTグループ (NTTグループ連携)
- 外部セキュリティ組織 (NCA、JPCERT/CC、IPA)

1.3 NTTDATA-CERTの活動範囲

NTTデータグループを中心に各種の情報セキュリティ事案に対応



1.4 情報セキュリティ推進室の体制

NTTデータ

技術革新統括本部

品質保証部

情報セキュリティ推進室

「安心・安全」な情報活用で創造性を育む組織体制の確立に向けて、NTTデータグループの情報セキュリティを推進する

社内・グループセキュリティ推進

社内・グループ会社のセキュリティ推進
グローバルガバナンス強化

商用システムセキュリティ推進

標準類の整備、研修整備
セキュリティ品質基準の普及展開

セキュリティ企画・広報

新規セキュリティ施策、監査、
社内・社外向け広報、申請処理

NTTDATA-CERT

セキュリティ事故の予防に関わる活動
事故発生時の緊急対応・支援
研究開発、対外活動

連携

連携

情報システム部門

社内/グループ会社の
情報システムの開発・運用部門

委託

NTTデータ先端技術（株）

SOC

1.5 NTTDATA-CERTの活動概要

NTTDATA-CERTは、インシデント発生時の緊急対応を迅速かつ正確に行うとともに、平時の活動を通じて、インシデントの発生を未然に防止する。

平時の活動

ベストプラクティスの収集や対応手順の策定　および
啓発活動や訓練等によるセキュリティインシデントの未然防止

未然防止
- 体制、対応手順の整備
- 対応訓練
- セキュリティに関する情報共有
  - 脆弱性情報の配信
  - リスク分析
  - 教育・啓発活動

モニタリング
- ソフトウェア/ハードウェアの弱点情報の収集
- 攻撃情報収集
- Webサイトの巡回監視
- サイバー攻撃の監視
- 最新の技術情報収集

CSIRTメンバのスキル研鑽
- インシデントハンドリング訓練
- コンピュータフォレンジック
- マルウェア解析
- 暗号化技術

活用

フィードバック

セキュリティインシデント発生時の活動

セキュリティ被害の極小化と迅速な復旧および再発防止の徹底

インシデント発生 → 原因分析 → 被害極小化 → 復旧 → 再発防止

平時の活動と**インシデント発生時の活動**を相互に連結し、活動を強化

2. 最新のサイバー攻撃

2.1 最新のサイバー攻撃の特徴

NTT DATA

検知が困難なサイバー攻撃や完全に予防できないサイバー攻撃が増加

- □ 標的型攻撃メール
- □ ウイルス付きばらまきメール
- □ 水飲み場型攻撃（※）
- □ Web待ち伏せ攻撃（※）
- □ マルバタイジング（※）
- □ ブログパーツ攻撃（※）
- □ ランサムウェア
- □ スパイ活動系ウイルス

ユーザが気づかない

完全な予防が困難

ウイルス対策ソフトが検知できない

侵入検知/防止システム(IDS/IPS)が検知/防御できない

（※Drive-By-Download攻撃系。以下、「DBD攻撃」という）

2.2 最新のサイバー攻撃

- 標的型攻撃メール
- ウイルス付きばらまきメール

2.2 標的型攻撃メール/ウイルス付きばらまきメール

NTT DATA

特定の組織や人物を狙って、メールを使ってウイルスを端末へ感染させて侵入する攻撃

標的型攻撃メールは多種多様

【ウイルス付きばらまきメールの種類】

標的型攻撃メールの手法が一般化
特定の組織や人物を狙っていない

~~標的型攻撃メール~~

① **Spamメール型**
不特定多数へ宛て。注文書や儲け話、セールスなどの一般的な内容

② **時事話題型**
不特定多数へ宛て。スポーツイベントや芸能ニュースなど時事内容

教育・訓練で予防可能

【標的型攻撃メールの種類】

③ **特定組織型**
ある組織やプロジェクトの複数関係者、ML宛て。関係者全体宛の連絡等。
送信元は、関係者のメールアドレス乗っ取り、または詐称

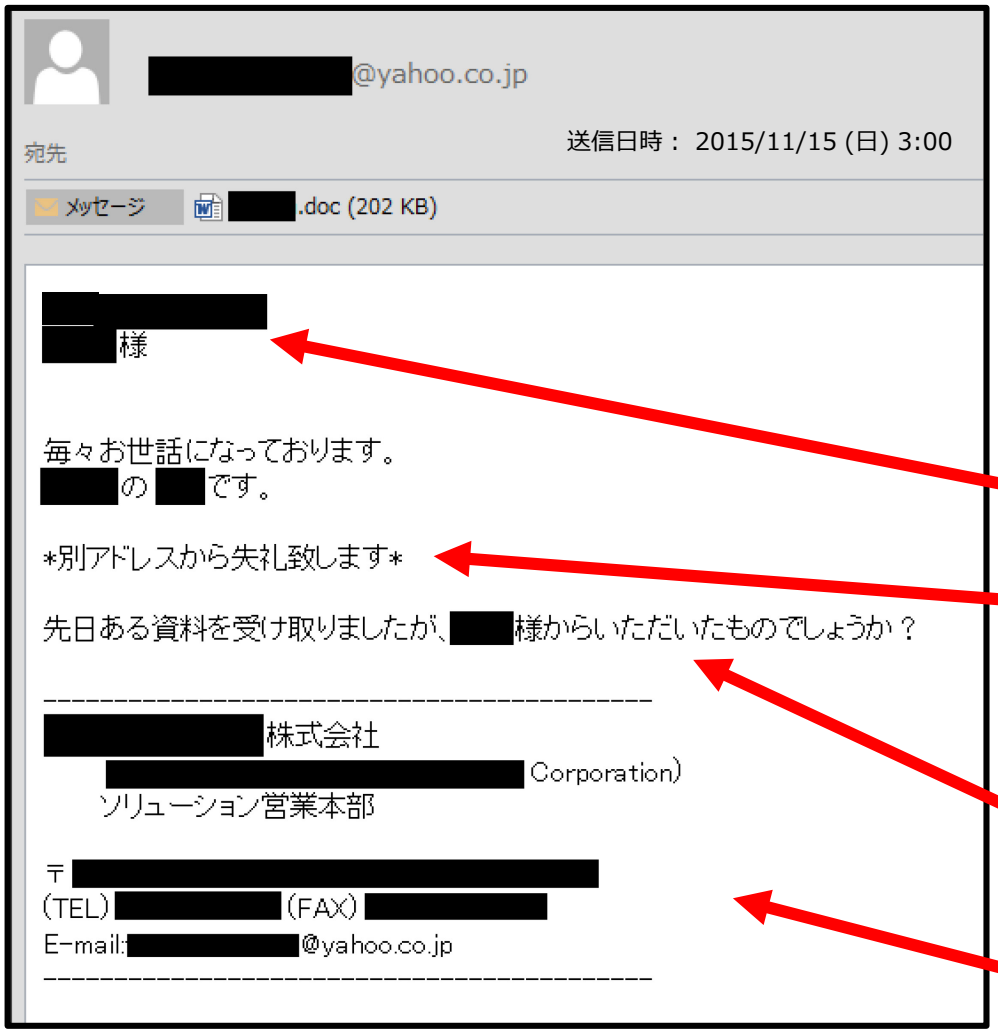
攻撃対象の周辺組織/関係者を攻撃して踏み台にする場合もある

④ **特定ユーザやりとり型**
個人宛て。業務の問合せ。送信元は、関係者のメールアドレスの乗っ取り、または詐称。実在する業務メールを加工/再利用

標的型攻撃メールに気づかない

2.2 標的型攻撃メール（④特定ユーザやりとり型）の実例

実際に届いた標的型攻撃メール（④特定ユーザやりとり型）



④ 特定ユーザやりとり型

個人宛て。業務の問合せ。送信元は、関係者のメールアドレスの乗っ取り、または詐称。実在する業務メールを加工/再利用

騙されポイント！

☆ **実在の人物から個人宛てへ**
標的の個人の知己/取引先を詐称

☆ **会社アドレスから送付できない言い訳**
フリーアドレスでも信用させる

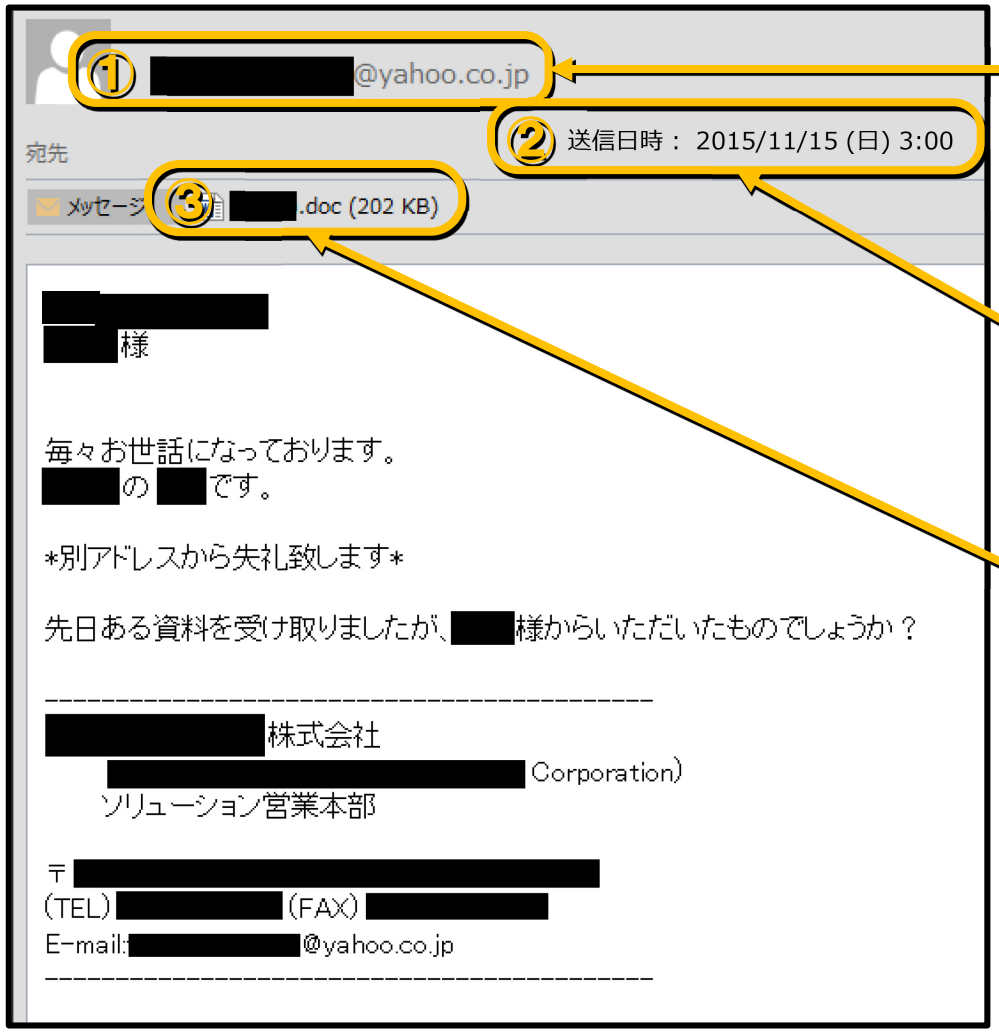
☆ **添付ファイルを開封しなければならない状況**

☆ **本物のシグネチャ**

業務で実際に取引している人になりすまして送付。添付ファイルをパスワード付き圧縮して、パスワードを別メールで送付したり、問い合わせに反応したりする場合もある。

2.2 不審なメールの見分けるポイント④

「フリーメールアドレス」と「送信時刻」に注意



① 送信元がフリーメールアドレス
取引先の会社アドレスではない。フリーメールアドレスの名前が似ていても信用しない

② 送信日時が業務時間外
深夜時刻の場合は怪しい。平日の業務時間中の場合もあるため、判断の一部に使用する

③ 添付ファイルが存在している
ウイルス対策ソフトが検知できない場合が多いので注意

差出人の会社のメールアドレスや電話で、メールの信ぴょう性を確認する

添付ファイルを開いてしまっても
すぐに気づいて対応すれば
間に合う！

2.3 最新のサイバー攻撃

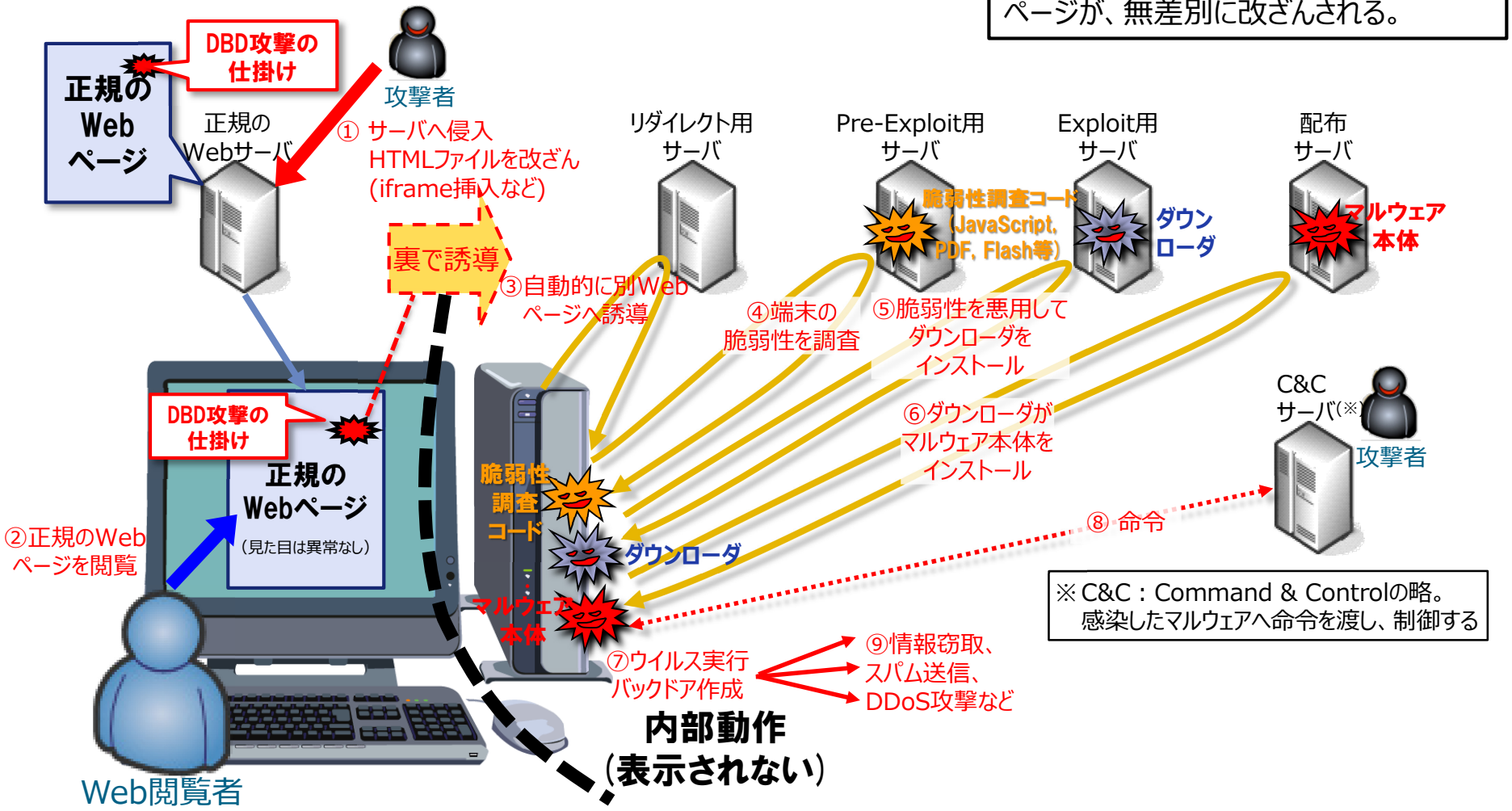
- □ 水飲み場型攻撃
- ○ Web待ち伏せ攻撃
- □ マルバタイジング
- ○ ブログパーツ攻撃

（Drive-By-Download攻撃系）

2.3 Web待ち伏せ攻撃（水飲み場型攻撃の一種）

多くのユーザがアクセスする可能性の高いWebページへDBD攻撃を仕掛ける

NTTDATA-CERTの命名。有名なWebページや有用な情報が掲載されたWebページが、無差別に改ざんされる。



※C&C：Command & Controlの略。
感染したマルウェアへ命令を渡し、制御する

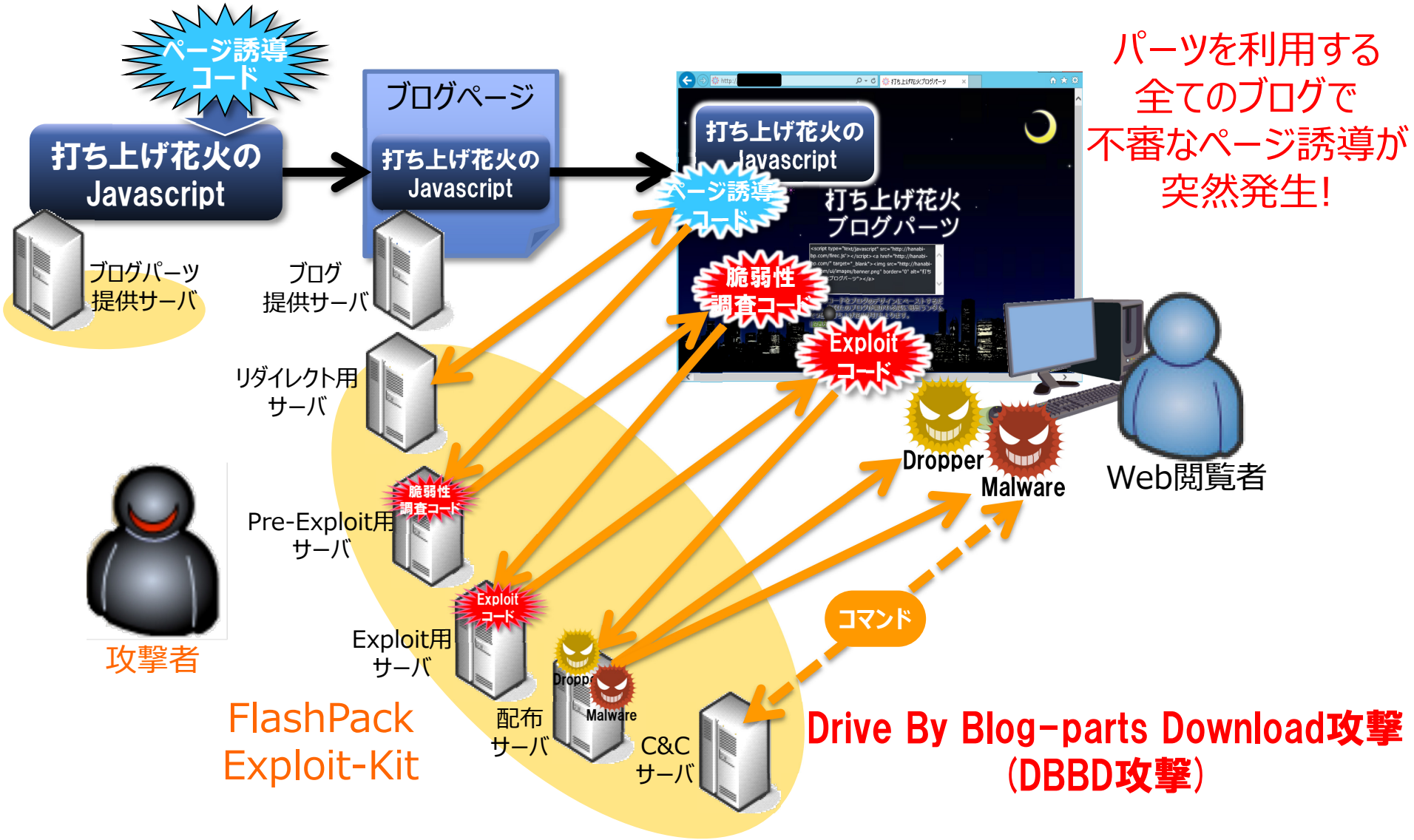
2.3 ブログパーツ攻撃①

ブログパーツを悪用したDrive-By-Download攻撃

【ブログパーツ】
ブログの機能性やデザイン性を向上させるパーツ。ブログサービスが提供するもの以外に、有償または無償で提供している場合もある。提供サイトからHTMLやJavaScript、CSSなどの形式のソースコードをブログに
埋め込んで表示させる。

2.3 ブログパーツ攻撃②

ページ誘導を発生させる不審なコードがブログパーツへ追加される



Web閲覧者は
DBD攻撃に
まったく気づかない！

キーロガーを仕込まれて情報を窃取されたり、
RATで遠隔操作されたり、
ランサムウェアがWordやExcelファイルを暗号化したり・・・

3. いまどきのCSIRTに必要な姿

3.1 CSIRTは受動的な運営

CSIRTは、インシデント・レスポンスだけでいいのか？

- 既知のサイバー攻撃
- 既知のウイルス/マルウェア
- 被害が顕在化したインシデント

インシデント・レスポンス

被害が顕在化するまで気づかないインシデント

- 標的型攻撃メール
- ウイルス付きばらまきメール
- 水飲み場型攻撃
- Web待ち伏せ攻撃
- ブログパーツ攻撃
- マルバタイジング
- ランサムウェア
- スパイ活動系ウイルス

- ユーザが気づかない
- 完全な予防が困難
- ウイルス対策ソフトが検知できない
- 侵入検知/防止システム(IDS/IPS)が検知/防御できない

キーロガーを仕込まれて情報を窃取されたり、RATで遠隔操作されたり、ランサムウェアがWordやExcelファイルを暗号化されたりして、被害が顕在化するまで

連絡をじっと待っているだけでいいのか？

3.2「名ばかりCSIRTで良いのか？」

NTT DATA

第３８３号コラム「名ばかりCSIRTで良いのか？」

投稿日：2015年10月12日 | カテゴリー：コラム, 第12期

第383号コラム：丸山 満彦 監事
（デロイトトーマツ リスクサービス株式会社 代表取締役社長、公認会計士、公認情報システム監査人）
題：「名ばかりCSIRTで良いのか？」

コンピュータ・セキュリティ・インシデント・レスポンス・チーム（CSIRT）を作ろうという話を良く聞くようになりました。この言葉自体は、それほど新しい言葉ではありません。日本シーサート（CSIRT）協議会というCSIRTが実務レベルであつまって情報交換等をするような団体は2007年に設立されていますね。JPCERTコーディネーションセンターというコンピュータ・インシデントに係わる情報共有等をする団体は、１９９６年に「コンピュータ緊急対応センター」として業務を始めています。約20年前ですね。昔からセキュリティをしている人であれば、Code RedやNimdaというウイルスを覚えている方もいると思います。これらのウイルスがはやったのが2001年ですから、それよりも更に5年前の話です。

さて、日本シーサート協議会に加盟しているCSIRTは２０１５年１０月１日現在、ちょうど“１００”チームとなっています。業種でいうとIT業界がやはり多く、全体の3分の1強となっています。しかしここ最近、急に増えているのは金融業界です。主要な総合バンクグループは当然のことですが、保険会社の加盟が相次いでいます。金融庁がCSIRTを構築しているかどうかアンケートをとったりしているものですから、義務付けではないものの、自主的にCSIRTを構築しはじめているのだろうと思います。日本シーサート協議会に加盟をしていないCSIRTがあると想定されるので、実質はもう少しあると思います。

このようなCSIRTを作る動き自体はよいことだと思っていますが、気になることがあります。それは「CSIRTが本当に機能しているのか」ということです。確かに、コンピュータ・インシデントの発生に備えて、チームの組成、役割分担、事故発生時のオペレーションを定義し、インシデントの発生に備えた具体的な訓練や演習をしているチームも多いと思います（それをしていなければ、そもそもCSIRTではありませんから）。しかし、肝心の「インシデントの検知」ができているのでしょうか。「うちの組織は今日もなんのインシデントの発生もなく穏やかだなぁ。うちのセキュリティは万全と言う証拠かな」というようなCSIRTがあれば、「本当にインシデントを検知できているのか」を疑う必要があります。インシデントを検知するためには、セキュリティ監視センターともいうべきセキュリティ・オペレーション・センター（SOC）を持つべきだと思います。社外との通信や社内の通信等を確認し、ウイルス等の侵入がないかどうかを検知できるような機能です。また、サイバー上の脅威に関する情報（たとえば、脆弱性情報や攻撃者に関する情報等）も積極的に収集し、分析できるような機能も必要でしょう。そのような機能が十分にあるのでしょうか？このような機能はCSIRTに含める場合もありますが、別の組織とする場合もあります（弊社の場合は、CSIRTとSOCは別の組織となっています）。

インシデントが発生した場合に対処するCSIRTの構築ばかりに力をいれても仕方がありません。セキュリティ・インシデントを発見する力の向上があわせて必要です。どちらも必要です。そうでなければ意味がありません。

もし、あなたの会社のCSIRTが日々暇にしているようでしたら、それは「名ばかりCSIRT」の可能性があります。本当にインシデントが発見できるような仕組みになっているのか確かめる必要があるかもしれません。予防、発見、対処の３つがそろってできるような組織になることが重要ですね。

【著作権は、丸山氏に属します】

出展：デジタル・フォレンジック研究会第３８３号コラム
https://digitalforensic.jp/2015/10/12/column383/

丸山 満彦　監事
(デロイト トーマツ リスクサービス株式会社　代表取締役社長)

もし、あなたの会社のCSIRTが日々暇にしているようでしたら、それは**「名ばかりCSIRT」の可能性があります。**

「うちの組織は今日もなんのインシデントの発生もなく穏やかだなぁ。うちのセキュリティは万全と言う証拠かな」というようなCSIRTがあれば、「本当にインシデントを検知できているのか」を疑う必要があります。

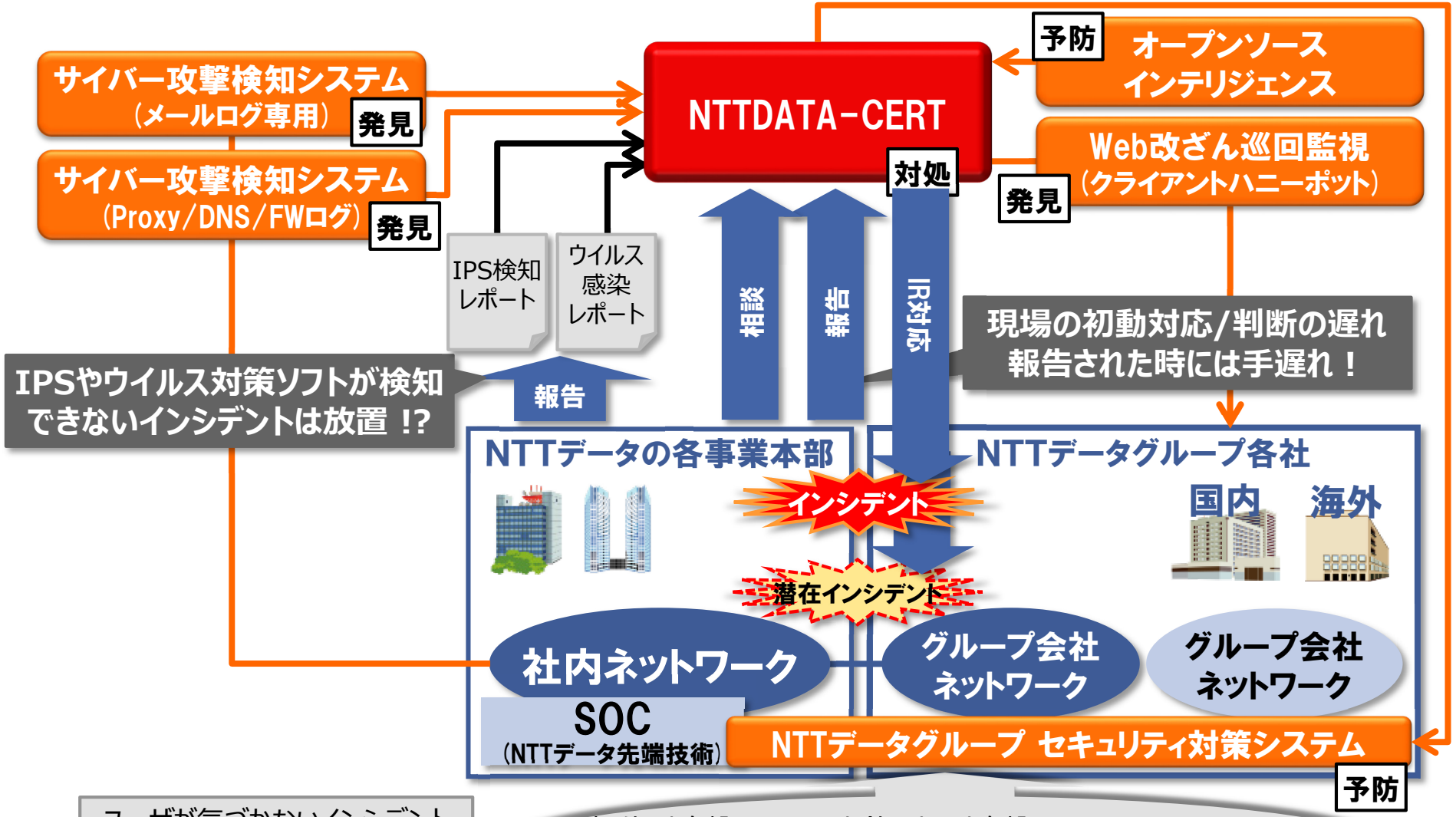
インシデントを検知するためには、セキュリティ監視センターともいうべきセキュリティ・オペレーション・センター(SOC)を持つべきだと思います。

また、サイバー上の脅威に関する情報（たとえば、脆弱性情報や攻撃者に関する情報等）も積極的に収集し、分析できるような機能も必要でしょう。

予防、発見、対処の3つがそろってできるような組織になることが重要ですね。

3.3 NTTDATA-CERTの運営方針の進化

インシデント報告を受けて対応する受動的な体制から能動的な『戦うCSIRT』へ！



ユーザが気づかないインシデント

予防が困難なインシデント

標的型攻撃メール　水飲み場型攻撃　RAT　ランサムウェア
Web待ち伏せ攻撃　マルバタイジング　スパイ活動系ウイルス

3.4 独自のサイバー攻撃検知システム

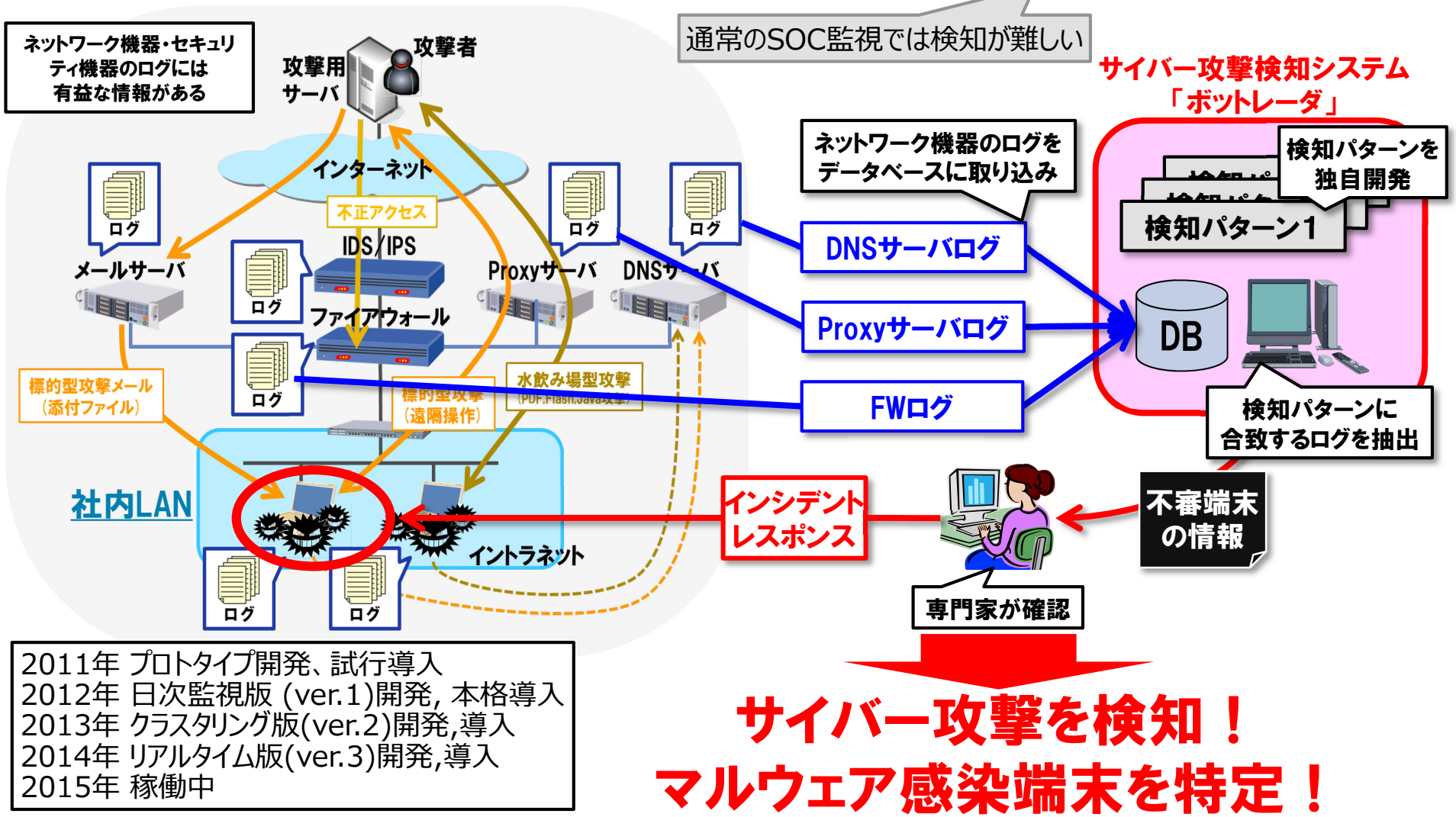
サイバー攻撃検知システム「ボットレーダ」

新しいサイバー攻撃の
早期検知・早期対応を実現

3.4 サイバー攻撃検知システムのコンセプト

NTT DATA

設置済みのセキュリティ機器の通信ログを有効利用してサイバー攻撃を検知



2011年 プロトタイプ開発、試行導入
2012年 日次監視版 (ver.1)開発, 本格導入
2013年 クラスタリング版(ver.2)開発,導入
2014年 リアルタイム版(ver.3)開発,導入
2015年 稼働中

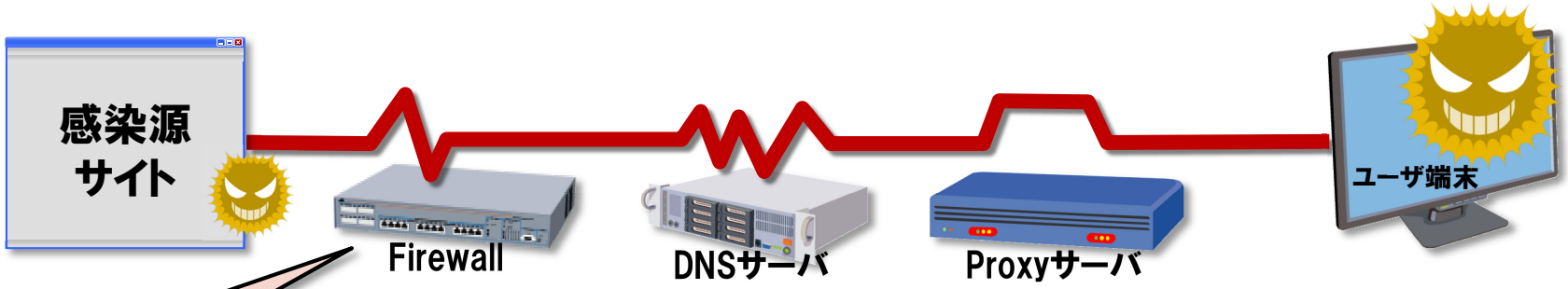
サイバー攻撃を検知！
マルウェア感染端末を特定！

参考： 大谷尚通,北野美紗,重田真義, 企業内ネットワークの通信ログを用いたサイバー攻撃検知システム, MWS2013.
大谷尚通,益子博貴,重田真義, 実環境におけるサイバー攻撃検知システムの有効性評価および検知範囲の拡大に向けた検討, MWS2014.
重田真義,益子博貴,大谷尚通, 企業での実環境を考慮したサイバー攻撃検知システムの有効性評価, MWS2015.

3.4 マルウェア検知のアーキテクチャ

NTT DATA

マルウェア感染時/感染後は、正常な通信とは異なる特徴的な通信が発生



感染時のProxyログ

No	DBD攻撃ステップ	URL	User Agent
1	改ざん元サイト	http://holiday***line.com/	Mozilla/5.0 (compatible; MSIE 10.0; ...
2	Redirectステップ	http://www.com***traer.cl/clik.php?id=6985669	Mozilla/5.0 (compatible; MSIE 10.0; ...
3	pre-Exploitステップ	http://h***j.c***doctor.pw/.../a8e***764(.html	Mozilla/5.0 (compatible; MSIE 10.0; ...
4	Exploitステップ	http://h***j.c***doctor.pw/3487***0/1390***(.jar	Mozilla/4.0 ... Java/1.7.0_15
5	pre-DLステップ	http://h***j.c***doctor.pw/f/1390***/3487***0/2	Mozilla/4.0 ... Java/1.7.0_15
6	Malware-DLステップ	http://receive***t.cc/man.php	Mozilla/4.0

NTTDATA-CERTの分析によると **5段階！**

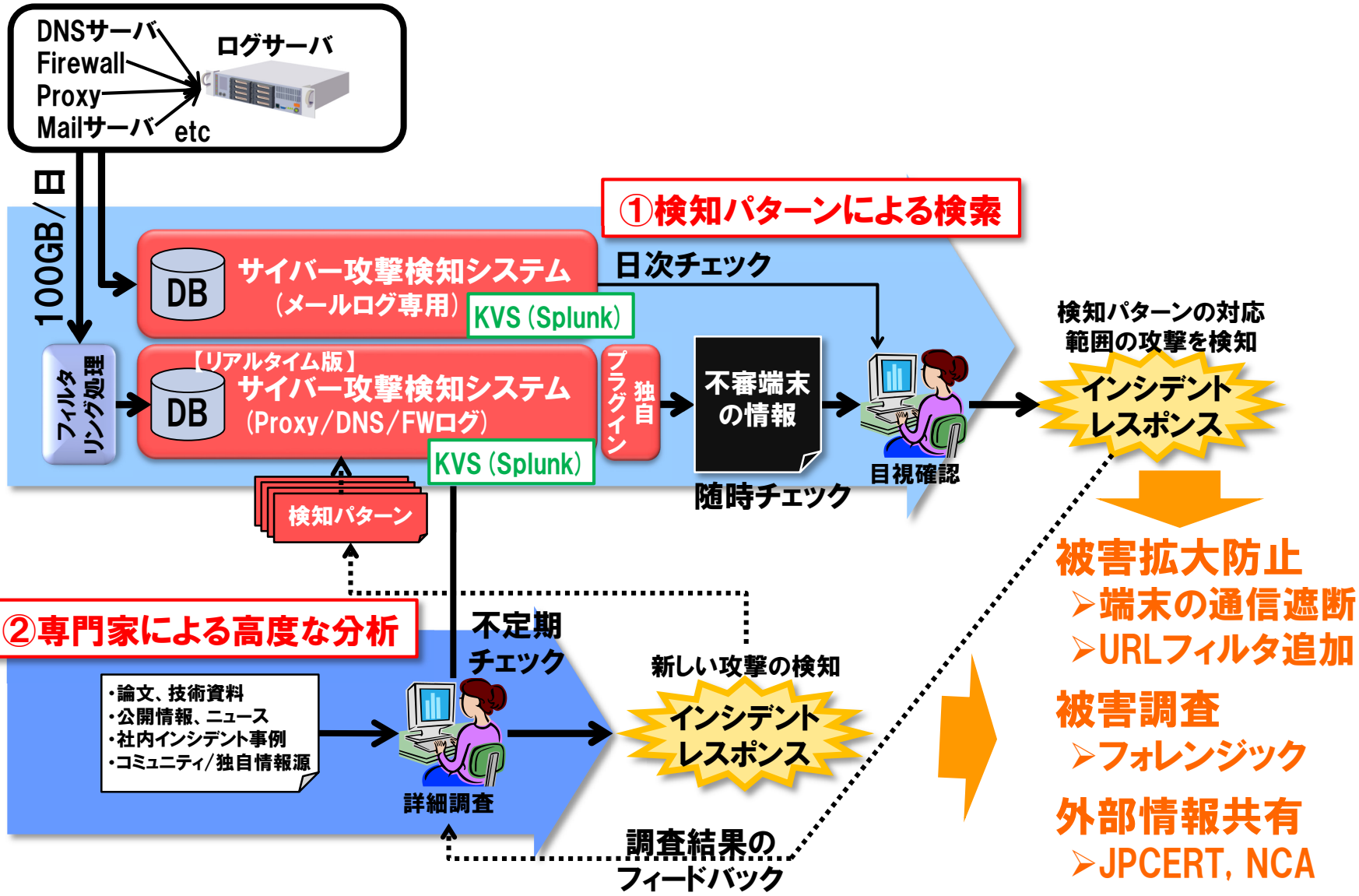
ソフトウェアの起動に伴って生じる必然的な変化(＝定性的特徴)は **攻撃が意図的に偽装しにくい**

通信ログに残った定性的特徴の痕跡からマルウェアに感染した端末を検知

3.4 ボットレーダーの監視運用体制

NTT DATA

「検知パターンによる検索」と「専門家による分析」の二段構成で監視！



新しいサイバー攻撃の
早期検知・早期対応システムの
研究開発、導入には
時間がかかる

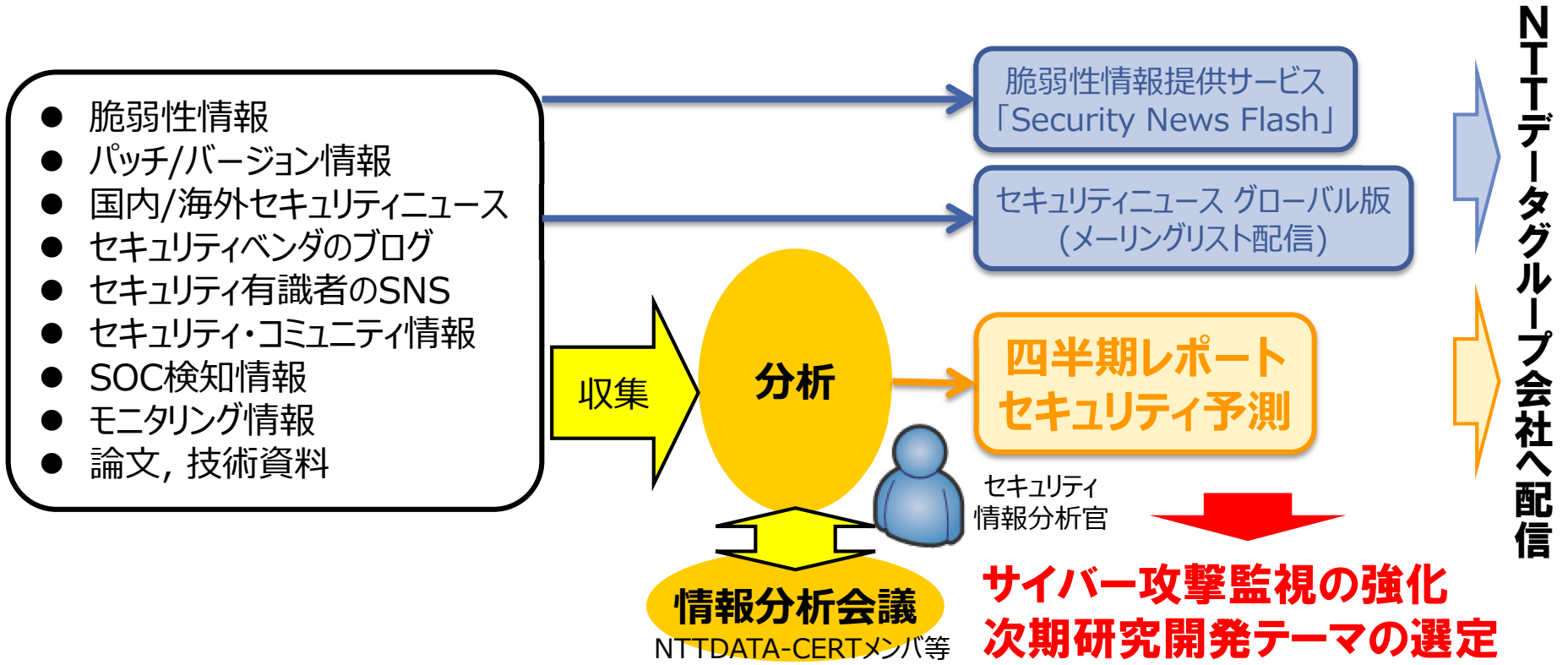
3.5 オープンソース・インテリジェンス

もっと新しいサイバー攻撃に
はやく対応するために！

3.5 OSINTを活用したCSIRT運営

NTT DATA

【オープンソース・インテリジェンス】
公開情報から収集された情報を元にする、情報収集の専門領域を指す。略称は**OSINT**(オシント)。「合法的に入手できる資料」を「合法的に調べ突き合わせる」手法で、情報源は政府の公式発表(プレスリリース)、マスメディアによる報道、インターネット、書籍、電話帳、科学誌その他を含む。具体的には、対象国の方針を割り出すために、対象国の新聞社交欄、ニュースの断片、人事の異動発令などを丹念に集積し、分析するといった手法である。 [Wikipediaより]



引用：Wikipedia
https://ja.wikipedia.org/wiki/オープン・ソース・インテリジェンス

3.5 四半期レポート/セキュリティ予測（例）

NTT DATA

2015年度第2四半期　情報セキュリティ関連の出来事の振り返りと今後の予測

2015年10月15日 に idobatako が投稿 — コメントはありません ↓

NTTDATA-CERTでは、2015年度第2四半期（7～9月期）について情報
した。また、振り返りの結果をもとに、今後の予測を実施しました。
この記事では、その内容を皆様にご紹介します。記事の構成は以下の

- 第2四半期のタイムライン・概要
- 第3四半期以降の予測
- 第2四半期の特筆すべき傾向

第2四半期のタイムライン・概要

2015年度第2四半期の情報セキュリティ関連の出来事のタイムラインを
ドウで開きます）

2015年度以降の予測

前回（2014年度第3四半期の振り返り）に実施した予測の振り返りと、2015年度以降の予測を以下に記載します。

NO.	3Qに実施した予測	4Qの状況の振り返り	FY2015以降の見通し
1	基盤となっているソフトウェアで重大な脆弱性が発見され、広範囲で緊急対応が発生。	以下のように基盤のソフトウェアで脆弱性が発見され	基盤のソフトウェアでの脆弱性発見は今後も発生する。深刻な
2	各国政府、または重要企業（インフラ防衛・基幹産業等）に対するサイバー攻撃がより注目され、政府間での非難・立が激しくなる。ただし、攻撃者が明にはならず、実効性のある取り組みはつながらない。		
3	ランサムウェアの被害がより広がる。にスマートフォン等のモバイル機器染する種類の感染が懸念される。		
4	コンテンツデリバリネットワークやフトウェアのアップデート機能を利用たマルウェア感染の拡大。		
5	米国ではPOSマルウェアの脅威、日本はインターネットバンキングでの被害発生。	日本でのバンキングマルウェアによる被害は、4Qの統計が未公開のため不明。啓発活動は進んでいる。	の業種（交通機関等）がより狙われるか。 バンキングマルウェアの撲滅は困難。ただし啓発等による対策

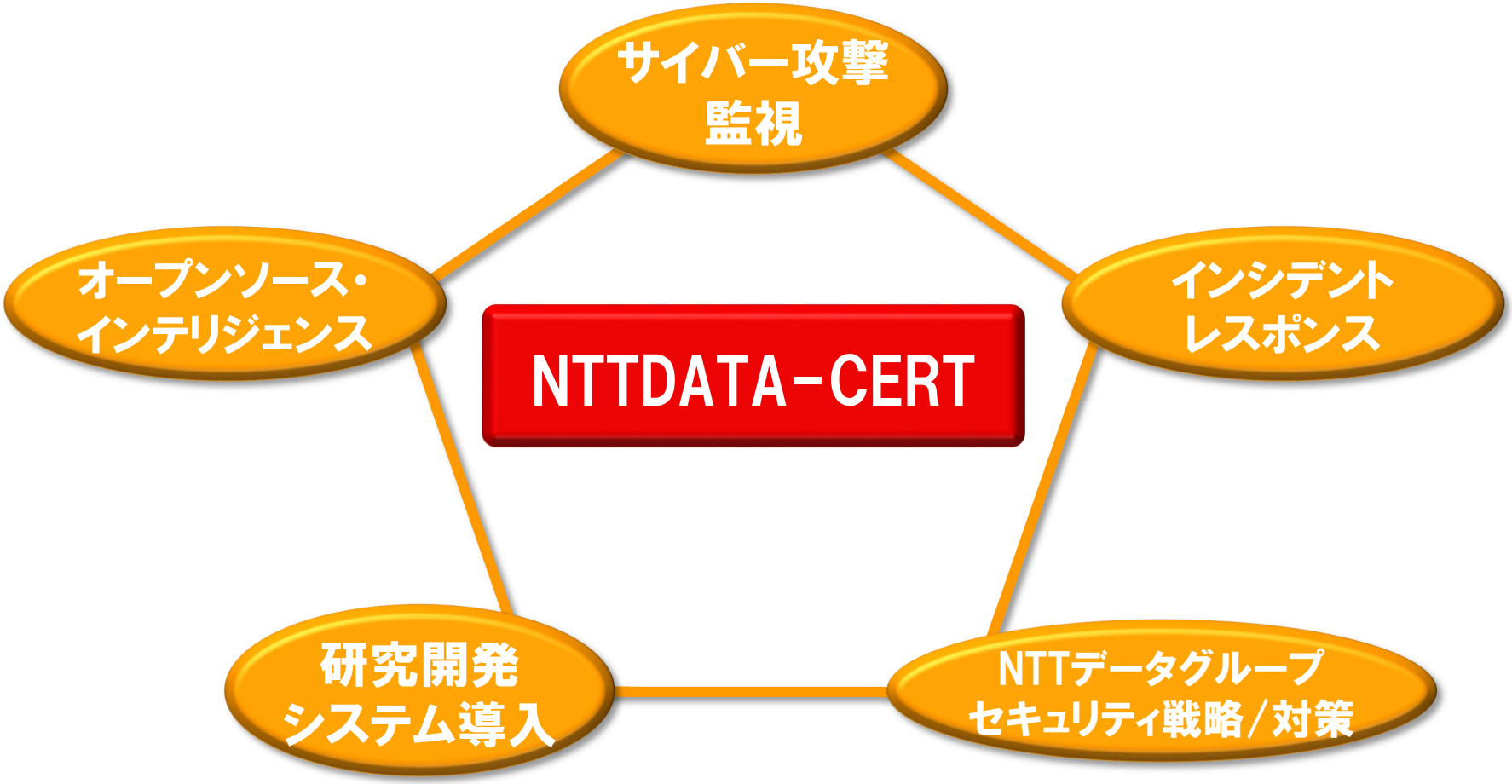
バンキングマルウェアとランサムウェアの融合

感染端末から情報をこっそりと盗み取るバンキングマルウェアと、ファイルを暗号化して身代金を要求するランサムウェアとでは、コソ泥と居直り強盗ほどに性質が異なります。しかし、この二つが融合した新たなマルウェアが登場しないと考える理由はありません。
例えば、一般的にウイルス感染が認められた場合はLANケーブルの抜線が必須ですが、LANケーブルの抜線を検知すると感染端末上のファイルの暗号化を始めるマルウェアが登場したら、どうでしょうか。

4. まとめ

4.1 NTTDATA-CERTのめざす姿

新しいサイバー攻撃の早期検知・早期対応の実現をめざして、
セキュリティ関連情報の収集・分析を起点に、さまざまな業務を有機的に連携



予防、発見、対処の3つが揃ったCSIRTをめざす

NTT DATA

Global IT Innovator