企業に対するサイバー攻撃の実態と対策
～NTTコミュニケーションズの事例紹介～

NTTコミュニケーションズ株式会社
小山　覚
2017年2月3日

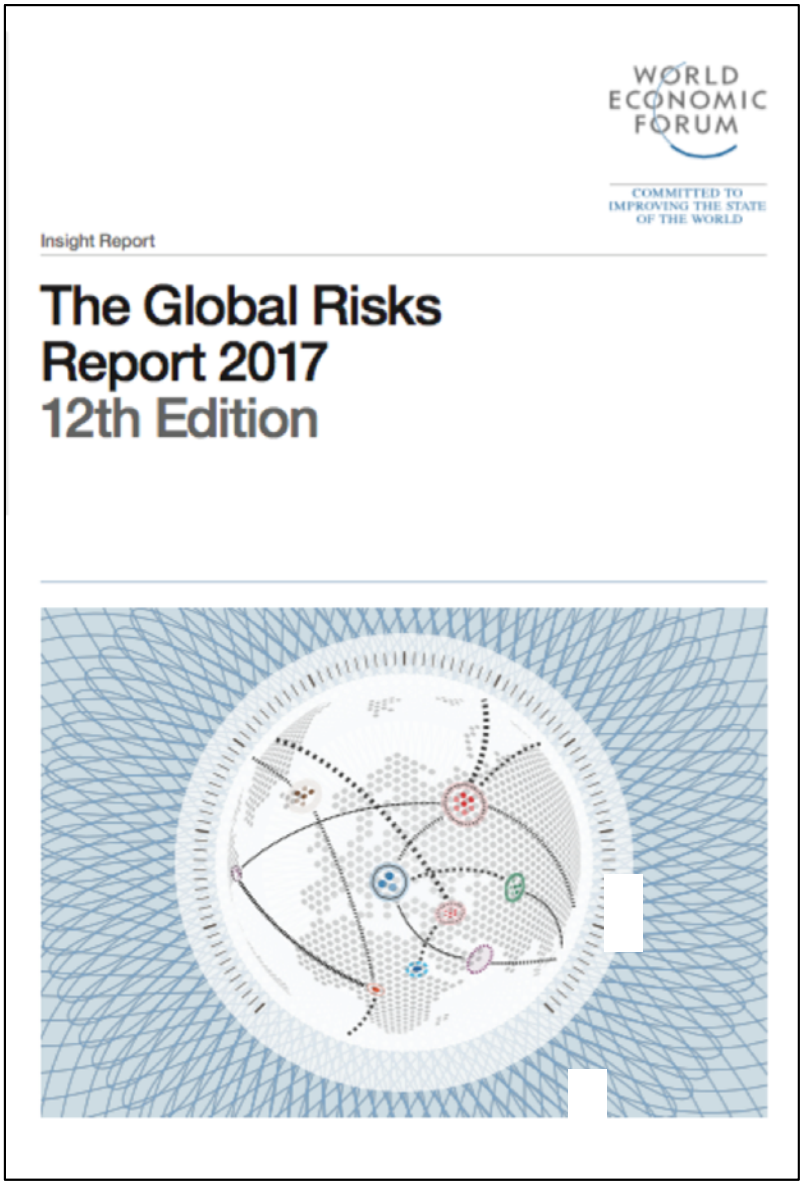
Transform your business, transcend expectations with our technologically advanced solutions.

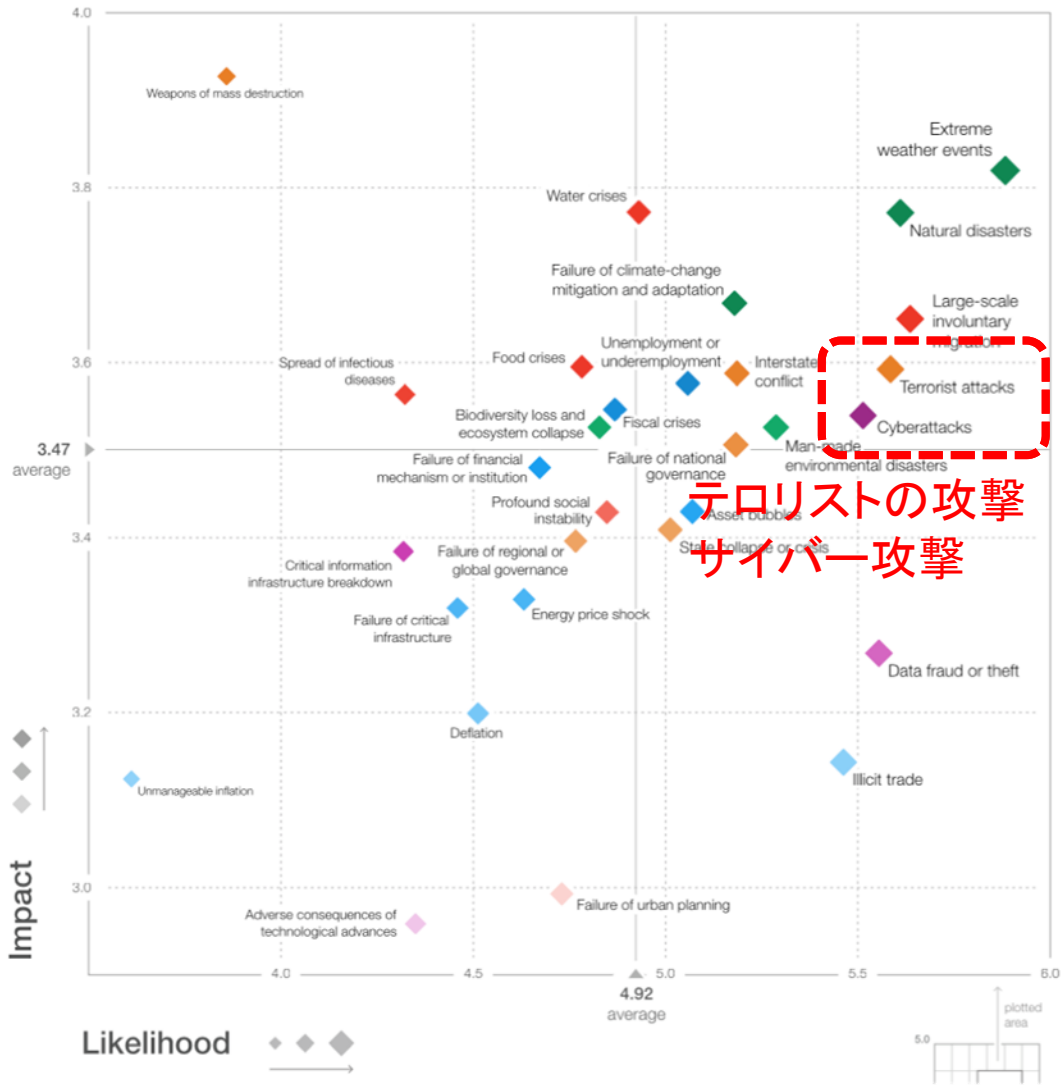
目次

1. セキュリティ脅威の動向
2. 繰り返される情報漏洩事故
3. 当社における標的型攻撃対策の取り組み
4. サイバー攻撃を契機とした、セキュリティ・リスクマネジメントの見直し
5. CSIRT体制強化の取り組み

1. セキュリティ脅威の動向

グローバルリスクレポート2017





米中間のサイバーセキュリティ問題　1/2

2014年5月19日米司法省は中国人民解放軍の将校5人を産業スパイで起訴

人民解放軍の「61398部隊」に所属する将校5人は、原発メーカーのWestinghouse Electricなど米国企業6社のシステムに侵入し、企業秘密などを盗み出したとされる。

自社と顧客の企業秘密を守る為に我々は何をすべきか？

米中間のサイバーセキュリティ問題　2/2

2015年9月米中首脳会談で中国のサイバー攻撃を非難

- オバマ大統領は習近平国家主席に、中国がサイバー攻撃したと考えられる、アトリビューションの根拠を突きつけた
- 両国は知的財産を盗むサイバー攻撃を実行しない、支援しないことで合意

Kevin Lamarque-REUTERS

G7合意はトランプ政権に引き継がれるか？

G7伊勢志摩　首脳宣言　付属文書記載事項
サイバーに関するG7の原則と行動

●目指すべきサイバー空間
オンラインにおける人権と法の支配の原則の堅持

●サイバー空間における安全と安定の促進
国家及びテロリストを含む非国家主体の双方によるサイバー空間の悪意ある利用に対し、密接に協力

一定の場合には、サイバー活動が国連憲章及び国際慣習法にいう武力の行使又は武力攻撃となりうることを確認

G7 JAPAN 2016 Ise-Shima
G７伊勢志摩サミット 2016

http://www.mofa.go.jp/mofaj/files/000160279.pdf

http://www.mofa.go.jp/mofaj/files/000160315.pdf

社会インフラに対するサイバー攻撃のリスク（事例）

交通標識が「ゴジラ襲来」と警告、米国でハッキング被害

2014年 06月 9日 14:38 JST

http://jp.reuters.com/articleoddlyEnoughNewsidJPKBN0EK0A020140609

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

無防備なWebカメラの監視画像を見せるInsecam

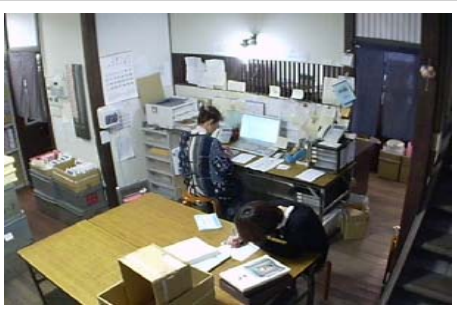
Watch Panasonic camera in
Japan
Shibuya-Ku

Watch Panasonic camera in
Japan
Inazawa

Watch Panasonic camera in
Japan
Osaka

Watch Panasonic camera in
Japan
Numazu

Watch Panasonic camera in
Japan
Obu

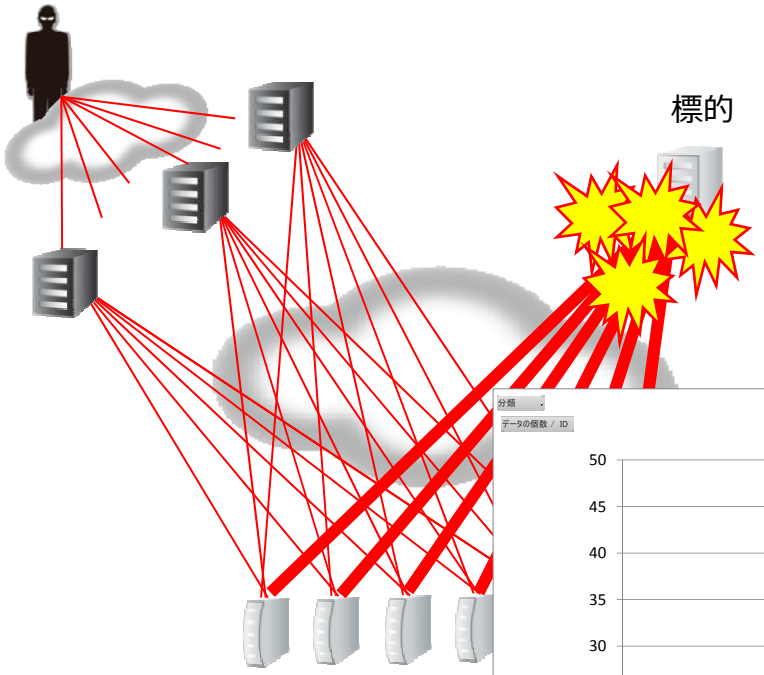


Watch Panasonic camera in
Japan
Takamatsu

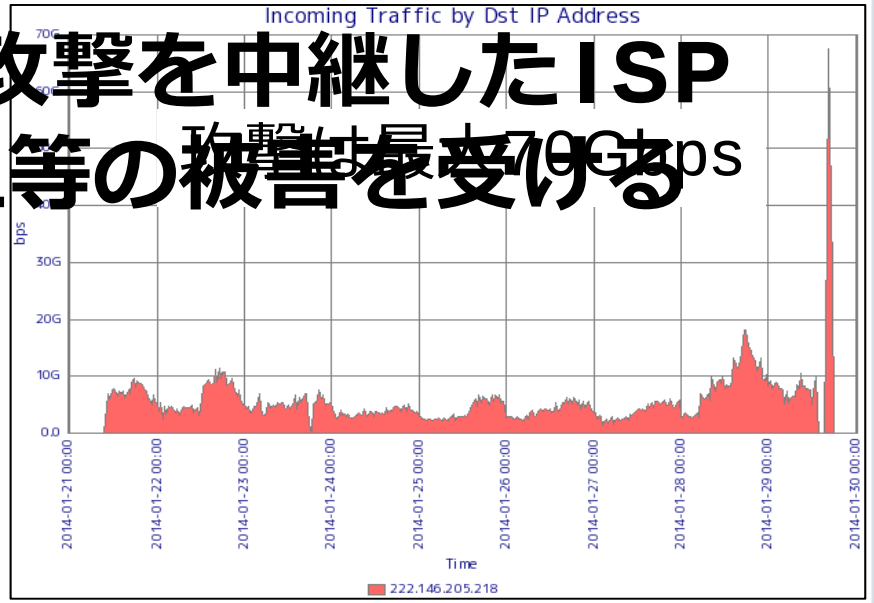
反射・増幅（リフレクション）攻撃事例

標的だけでなく、攻撃を中継したISP
も、システム停止等の被害を受ける

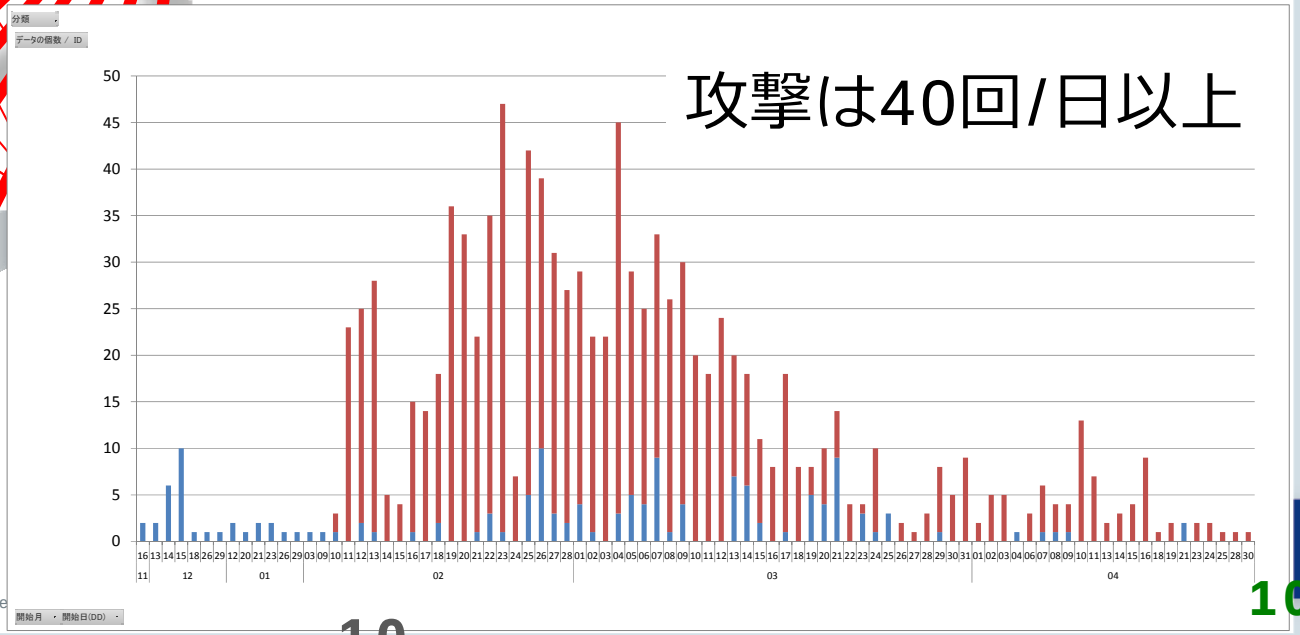
攻撃者



標的



攻撃は最大70Gbps



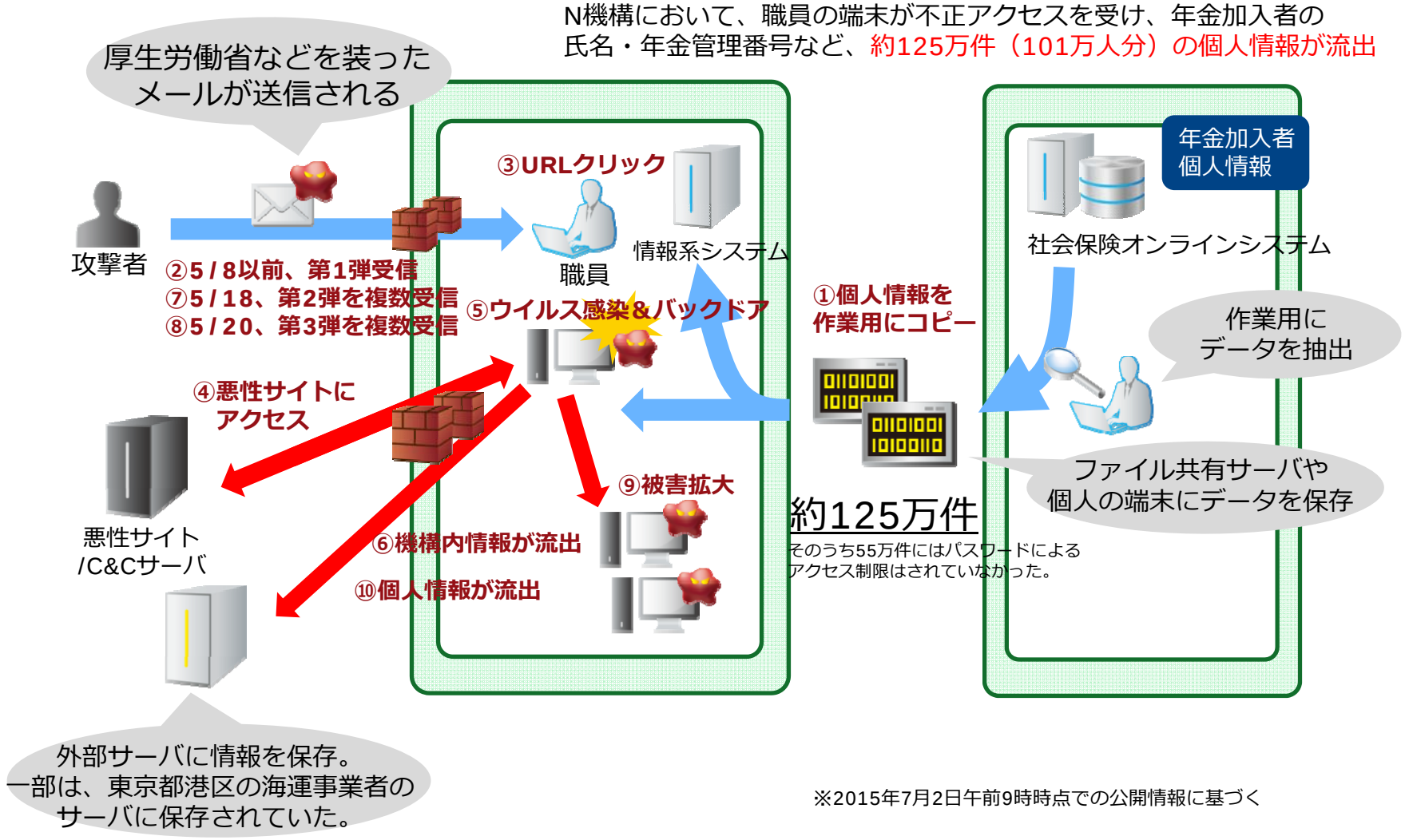
攻撃は40回/日以上

10

2. 繰り返される情報漏洩事故

N機構　個人情報流出までの時系列（概要）

N機構において、職員の端末が不正アクセスを受け、年金加入者の
氏名・年金管理番号など、約125万件（101万人分）の個人情報が流出



※2015年7月2日午前9時時点での公開情報に基づく

標的型攻撃の脅威

日経コンピュータ

核施設や工場までサイバー攻撃の標的に

2012/03/19

浅川 直輝＝日経コンピュータ （筆者執筆記事一覧）

なぜ同じような過ちを繰り返すのか？

マネジメント・普及啓発・技術的対策・監視運用・監査など、何が問題だったのか？

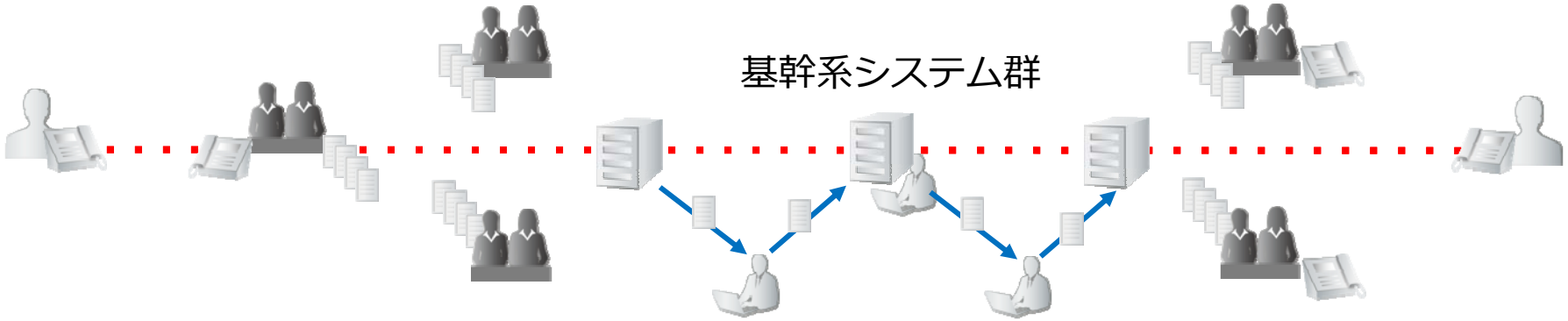
て企業が取るべき対策を考える。

企業の機密情報をおびやかすサイバー攻撃に対し、各国が国を挙げて対策を取り始めた。

出典：http://itpro.nikkeibp.co.jp/article/COLUMN/20120314/386346/?ST=attack

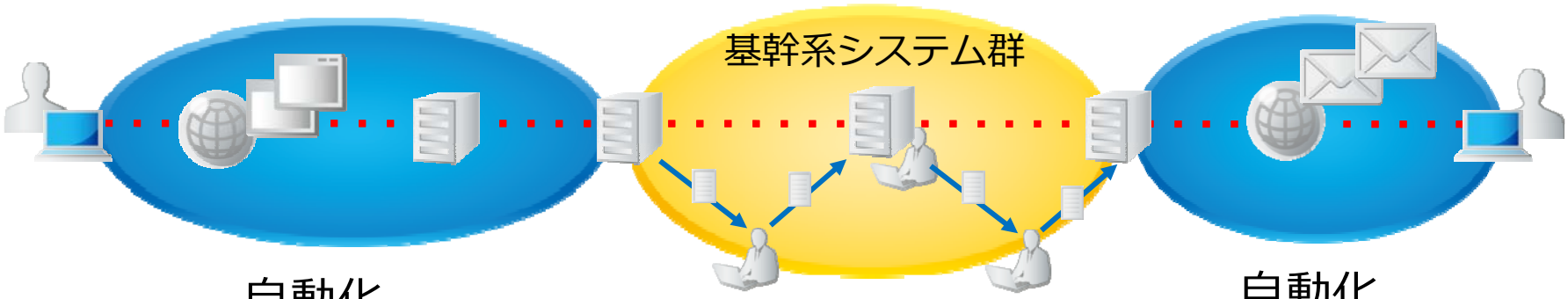
システム化が抱える課題 1/2

手作業中心（IT導入前）



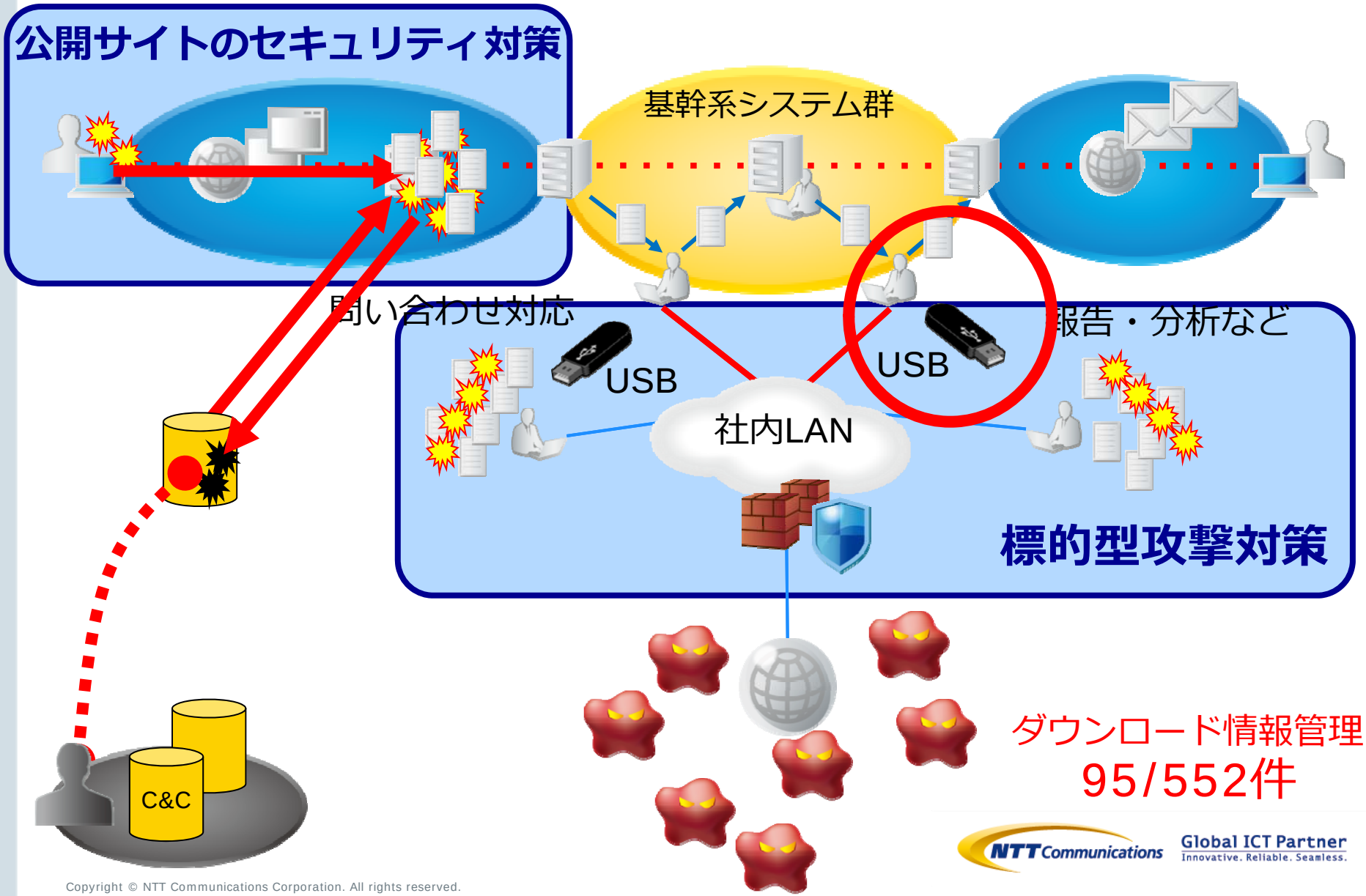
システムは常に変化、移行期や暫定的な業務がリスクを生む

システム化（IT導入後）



自動化　一部手作業　自動化

システム化が抱える課題 2/2



ダウンロード情報管理
95/552件

3.当社における標的型攻撃対策について

標的型攻撃のメールの開封率(弊社訓練結果)

1回目(2012年11月)

・社員・派遣社員10,431名中、

340名(3.3％)が開封

差出人：日本情報推進機構<info@japan-sec.org> ※

宛先：comtaro@ntt.com

件名：【緊急】ソフトウェア製品の複数の脆弱性に対するアップデート

添付　対処マニュアル_Ver01.doc

先般、御社内で使用されているソフトウェア製品において、極めて深刻な脆弱性が複数発見されました。
・・・
現時点で対応可能なパッチをご用意しましたので、添付のマニュアルに沿って、早急に対策を実施願います。
・・・

※架空の団体

社外から緊急メール

2回目(2013年2月)

・社員・派遣社員8,745名中、

1,583名(18.1％)が開封

差出人：佐藤<q-sato@0ntt.com>

宛先：comtaro@ntt.com

件名：【周知】3月定例会のご案内

添付　定例会ご案内（2013年3月）.doc

メンバーの皆様

次回の定例会のご案内をお送りしますので、ご確認のほど、よろしくお願いいたします。
それでは、お会いできるのを楽しみにしています！

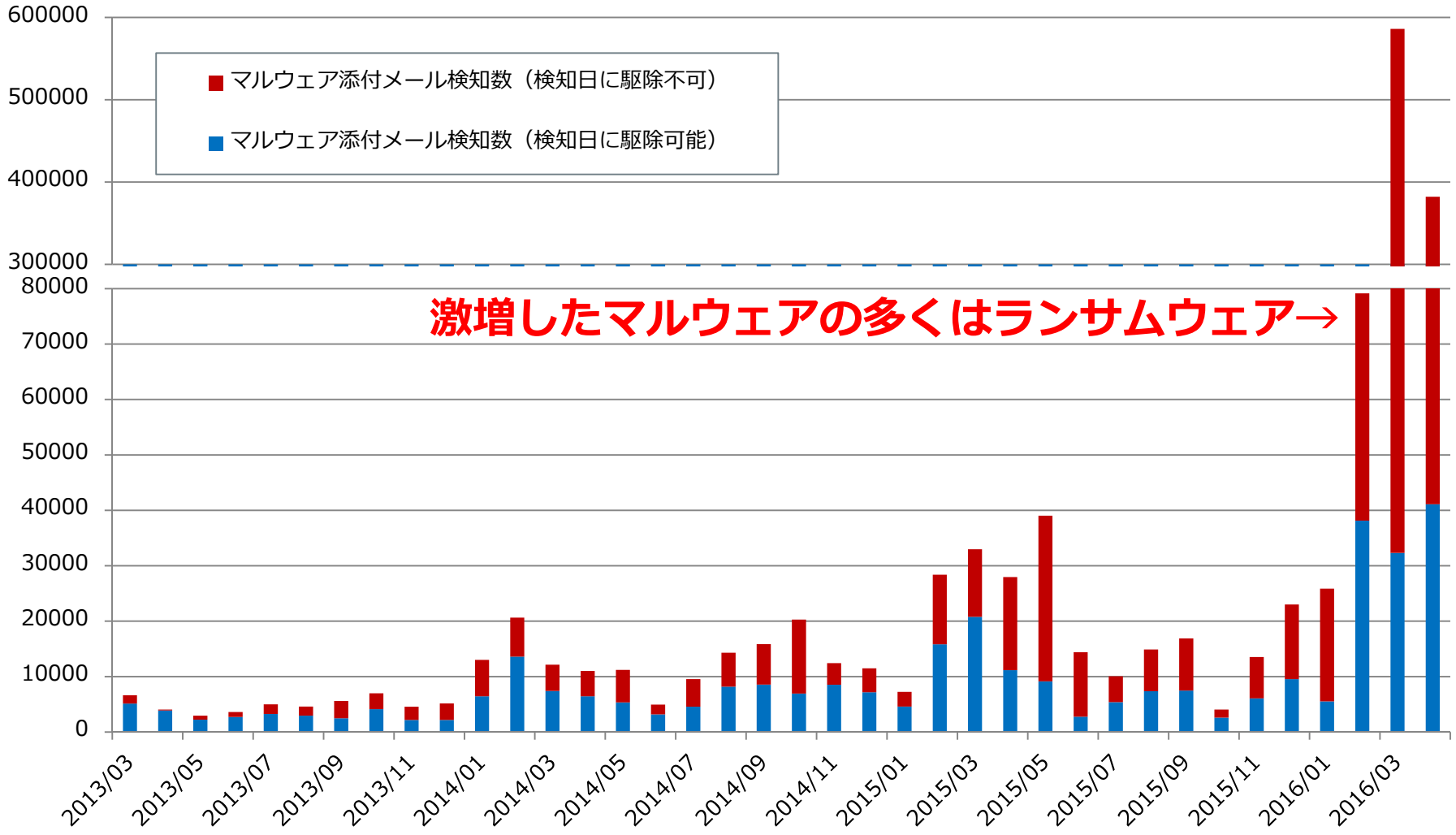
懇親会の案内メール

既にマルウェアが社内に潜伏している前提での対策が必要

NTT Communications　Global ICT Partner Innovative. Reliable. Seamless.

NTTコムに対するマル（ランサム）ウェアの脅威

平均月間メール通数：18,560,624通



組織的攻撃を想定したリスク対策とは

攻撃者のセオリー

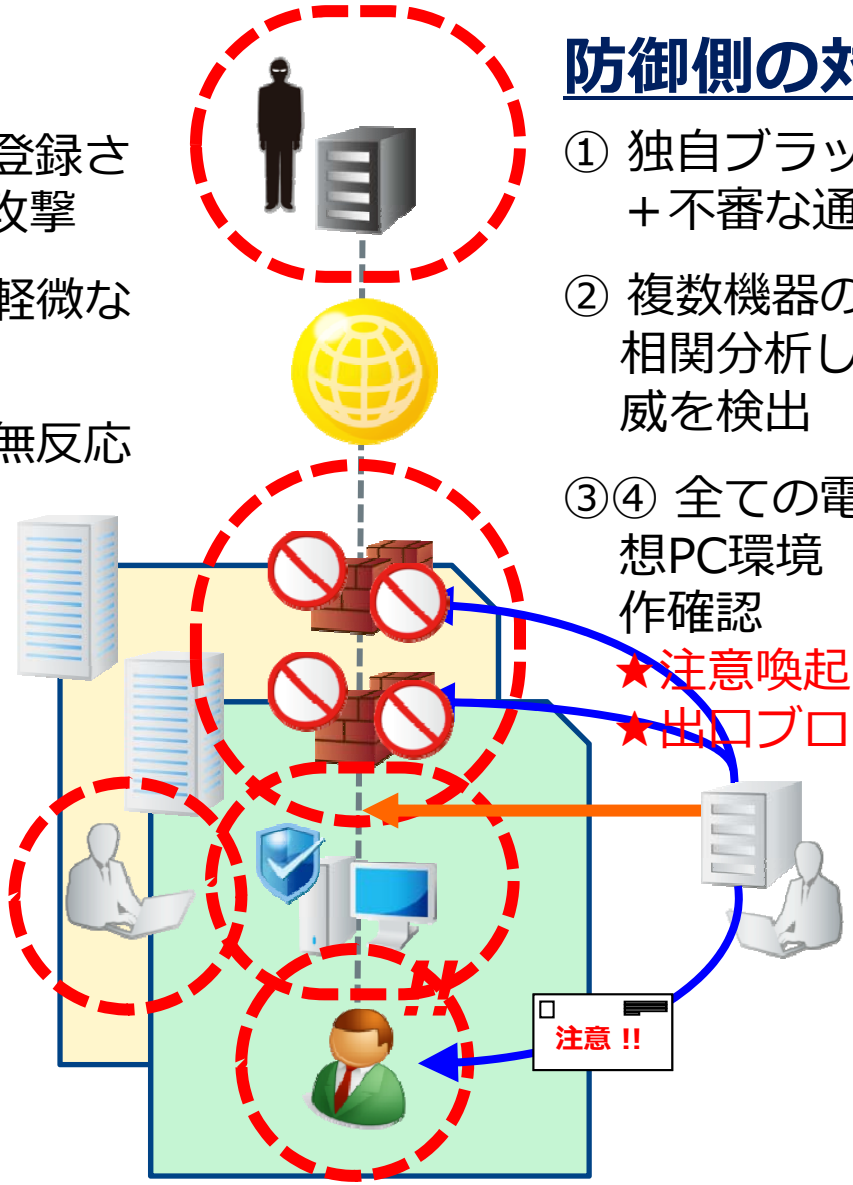
① URLブラックリストに登録されていないサイトから攻撃

② 不正侵入検知装置では軽微な警報

③ ウィルス対策ソフトも無反応

④ 標的（社員）も特定

⑤ システム環境も調査



防御側の対応策

① 独自ブラックリストの導入＋不審な通信先監視

② 複数機器の警報（ログ）を相関分析し、すり抜けた脅威を検出

③④ 全ての電子ファイルを仮想PC環境（Sandbox）で動作確認

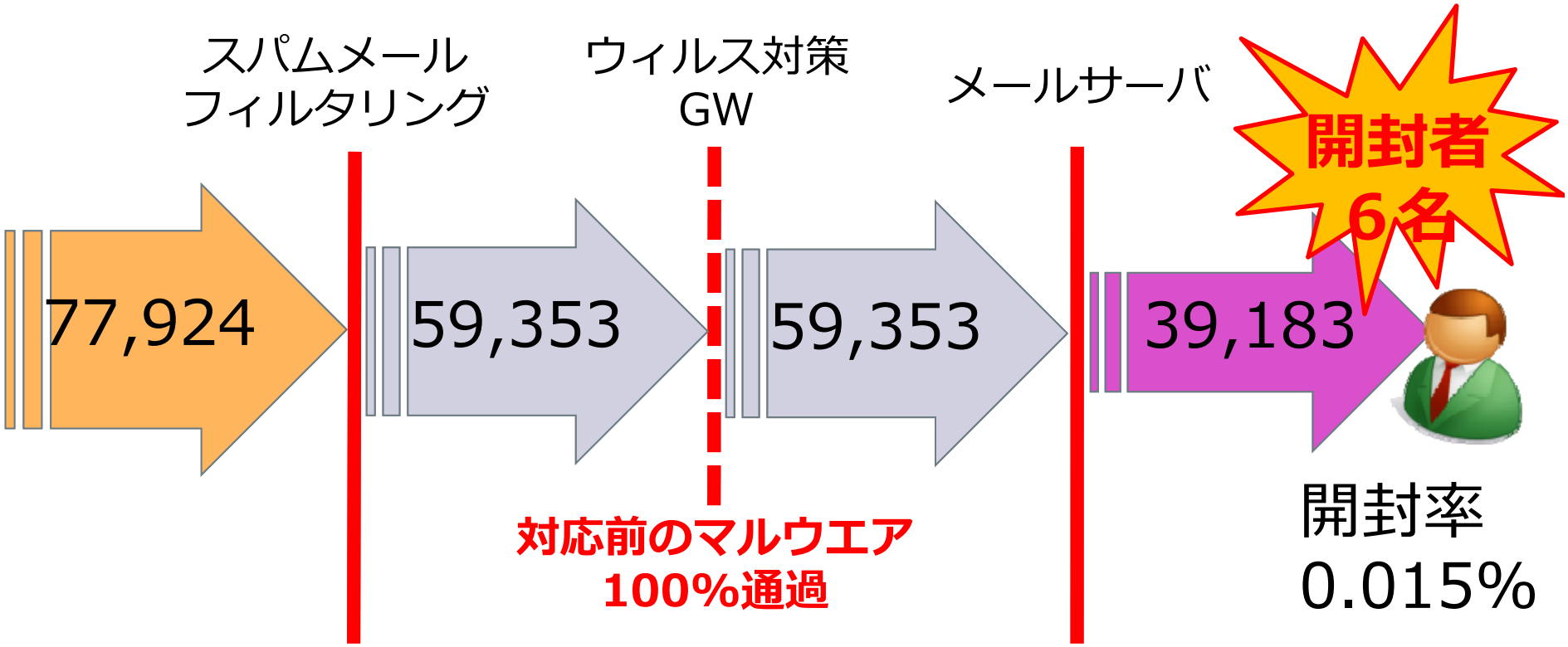
★注意喚起メールの自動送信

★出口ブロック自動設定

Sandbox

未対応ランサムウェアの大量流入経験

ランサムウエア付きメールが短時間に大量着信

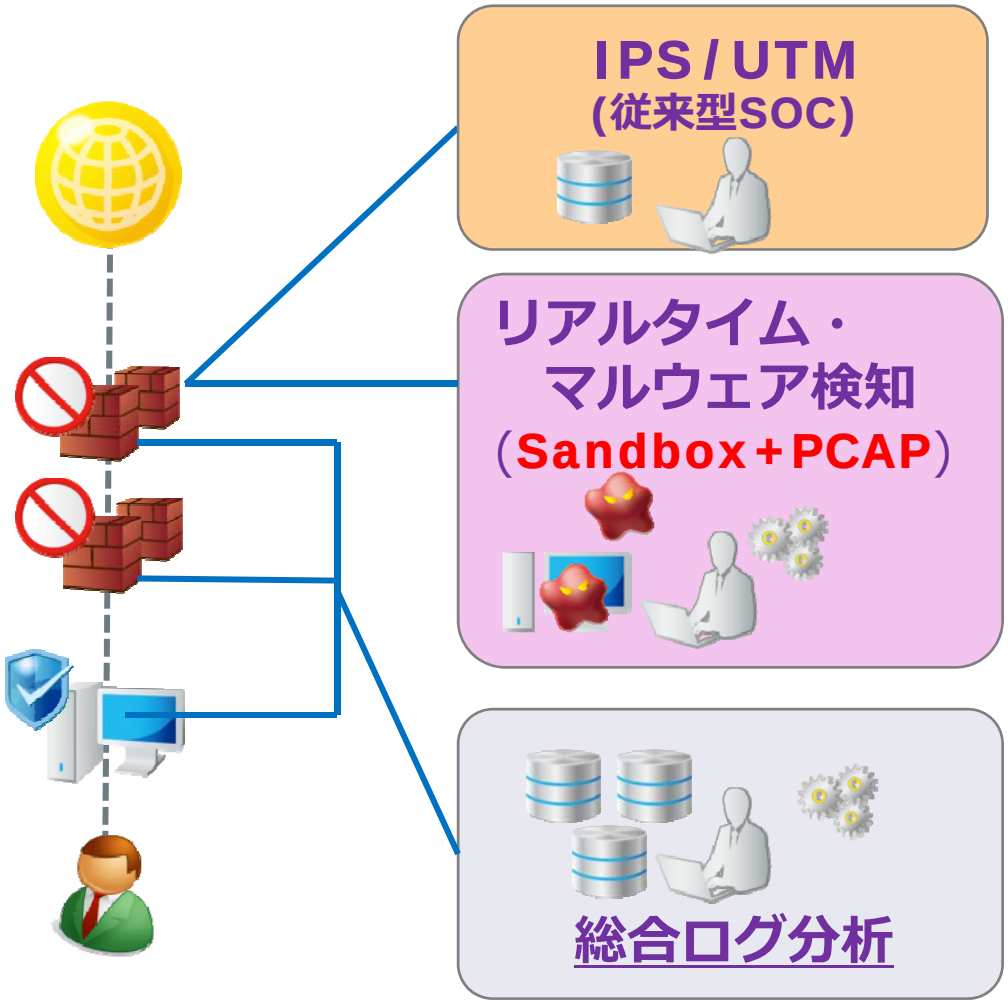


ランサムウエアの本体プログラムのダウンロードを阻止し被害回避

- **プロキシサーバの自動ブロック機能により２名**
- **認証プロキシのID/PW認証により４名**

標的型攻撃対策の実績

NTT Com グループ独自のSIEMエンジンやブラックリストなどにより、
従前の対策で検知困難な未知の重篤なセキュリティ脅威を発見



監視対象：PC約8万台

170億件/53日のログを抽出
(ログソース：IPS/IDS, Sandbox, PROXY)

セキュリティ運用基盤による分析
22万件の疑わしい
ログに絞り込み

リスクアナリストによる重篤度判定

39件の重篤な
セキュリティ脅威を検知

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

4. サイバー攻撃を契機とした、セキュリティ・リスクマネジメントの見直し

2013年7月23日 400万件の顧客情報が流出

News Release

NTT Communications

2013 年 7 月 24 日

OCN IDのサーバーへの不正アクセスについて

NTT コミュニケーションズ(略称：NTT Com)が提供する、メールアドレスを利用して各種 Web サービスにログインできる OCN IDのサーバーにおいて、外部からの不正アクセスが発生していたことが判明しました。現時点では、お客さまの情報などの流出被害は確認されておりませんが、OCN ID 用のメールアドレスと暗号化されたパスワードが外部へ流出した可能性があります。

このような事態が発生し、お客さまに多大なご迷惑をおかけすることになりましたことを、深くお詫び申し上げます。

NTT Com では、今回の事象の発生を厳粛に受け止め再発防止に努めますので、何卒ご理解を賜りますようお願い申し上げます。

1.発生事象

メールアドレスを利用して、OCN メール・OCN マイページ・マイポケットなどにログインできる OCN ID サービスを管理するサーバーにおいて、2013 年 7 月 23 日に 5 つの不審なプログラムファイルを発見しました。当該ファイルや通信ログなどを調査した結果、OCN ID のサーバーが外部から

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

7項目の見直しを実施

★全社ITシステムのセキュリティリスク低減策

1. 全社ITシステム等の調査
2. ITシステムのソフトウェア脆弱性解消の対応策
3. セキュリティ強化策

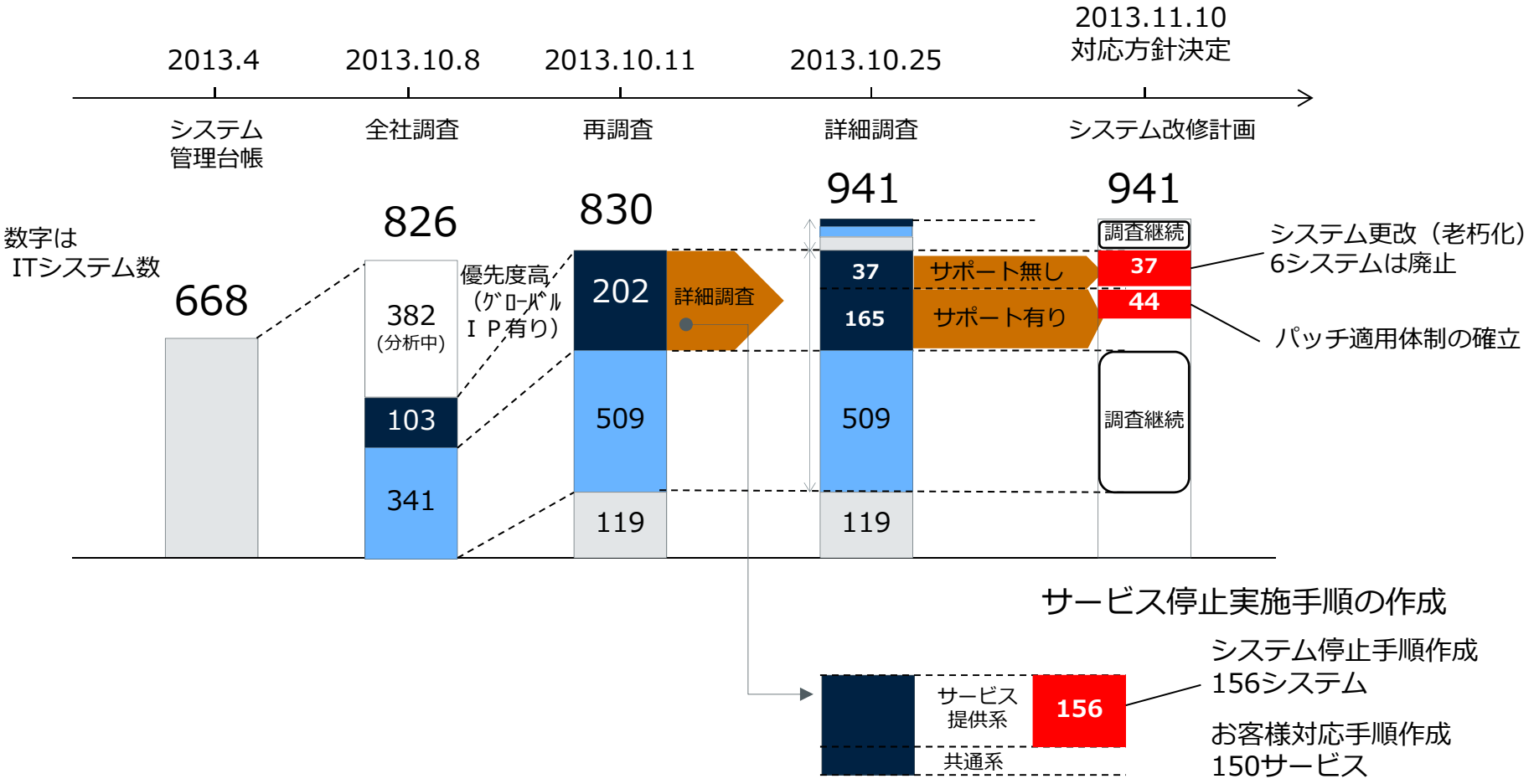
★セキュリティリスクマネジメントの新たな業務運営プロセス

4. 全社ITシステムの管理方針を改めて策定
5. ソフトウェア脆弱性発覚時の対応
6. ソフトウェア脆弱性発覚時の対応訓練
7. 規程/約款の改定

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

1.全社ITシステムを洗い出し、ソフトウェアやハードウェアの構成/運用状態/主管組織等を調査、リスクアセスメントの基礎情報を再整備

2.グローバルIPアドレスを保有するシステムについて「老朽化したシステムの更改」「ソフトウェアパッチの適用」の全体予算を把握し対応策を策定



3．セキュリティ強化策の徹底

■セキュリティ対策の「適用基準」を定め、調査で洗い出されたグローバルIPアドレス保有システムに適用

情報システムの種別		FW	IDS IPS	Email Web ｳｨﾙｽ対策	WAF	VM ｾｷｭﾘﾃｨ	プロファイリング	リアルタイムマルウェア検知	脆弱性診断		リスクアセスメント
									NW	Web	
公開システム	WebAPを保有	●	●	●	●	●	●	●	●	●	●
	上記以外(メール等)	●	●	●		●	●	●	●		●
	インターネットGWを有するシステム	●	●	●			●	●	●		●
社内に閉じたシステム				●			●	●	●		●

４．全社ITシステムの管理方針を改めて策定

●全ITシステムを一元管理する方針を定め、
正確な構成管理とセキュリティレベル担保のためのプロセスを策定

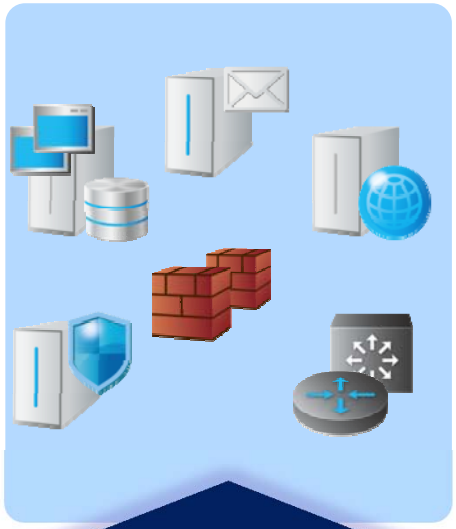
課題	対応方針
システム情報の一元化 タイムリーな情報更新	**ルール化** ➢サービス開発判断・システム投資判断時に情報登録 ➢脆弱性対応状況の登録を義務化
脆弱性情報に対する迅速で確実な対応	**システム化**（情報セキュリティ管理プラットフォー/ISMP） ➢システム構成情報管理の徹底
システムの標準化	**全社のガバナンス強化** ➢ソフトウェア脆弱性への対応はISMPでモニタリング。 ➢ITシステムのハードウェアやOS等を標準化

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

脆弱性マネジメントシステム（ISMP）の利用を徹底

従来のシステム管理台帳を廃止し、脆弱性マネジメントシステムに一本化
より簡易に抜け漏れなく、ガバナンス強化を実現

情報システム



●システム情報登録
・システム名、用途、IP、OS/AP等

●サービス提供
・脆弱性診断（定期、随時）
・当該システムに影響する脆弱性情報を抽出、自動通知

●対策実施
診断結果と脆弱性情報に基づく対策実施

システム管理者

●警報配信（CSIRT）

●脆弱性対応状況管理
・脆弱性対策実施の計画と実績管理

CISO

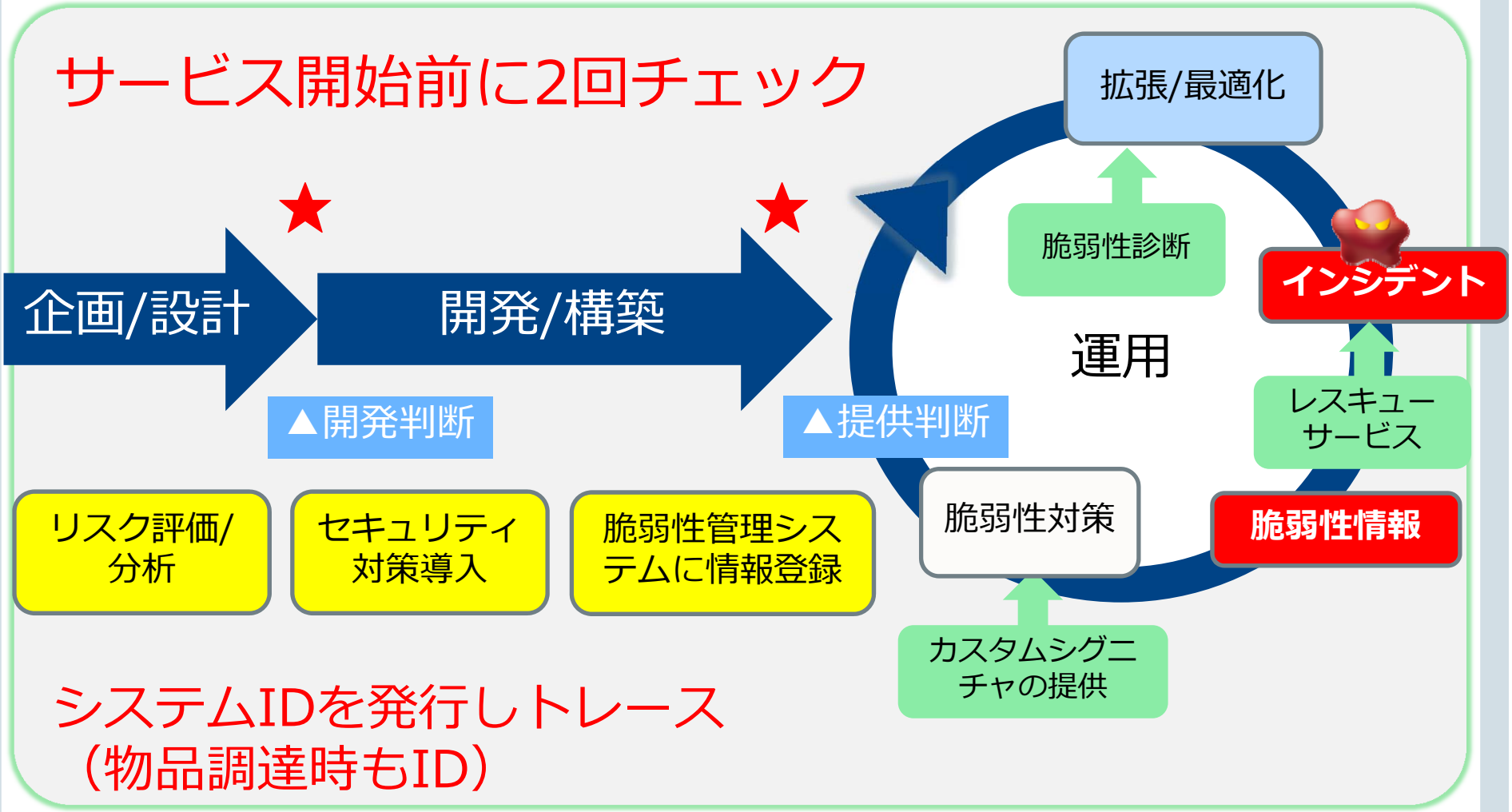
ISMP
Information Security Management Platform

（特徴1）
脆弱性診断結果に基づく対策実施計画と実施状況を一元管理

（特徴2）
登録システム全体の脆弱性対策状況を管理
ボトムラインを可視化

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

当社のリスクマネジメントフレームワーク



5．ソフトウェア脆弱性発覚時の対応

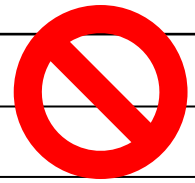
■ 対応緊急度の判定

①リスクレベルと②攻撃可能性（リモート攻撃可否＋攻撃ツール有無）で緊急度を判断

<table>
<tr><td colspan="3" rowspan="2"></td><td colspan="5">①リスクレベル</td></tr>
<tr><td colspan="5">リスク高 ⟶ リスク低</td></tr>
<tr><td colspan="3"></td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td rowspan="3">②攻撃可能性</td><td rowspan="2">リモート攻撃可能</td><td>攻撃ツール有</td><td>S+</td><td rowspan="2">A</td><td colspan="3" rowspan="2">B</td></tr>
<tr><td>攻撃ツール無</td><td>S−</td></tr>
<tr><td colspan="2">リモート攻撃不可能</td><td colspan="4">A</td><td colspan="3">B</td></tr>
</table>

■ 対応実施基準

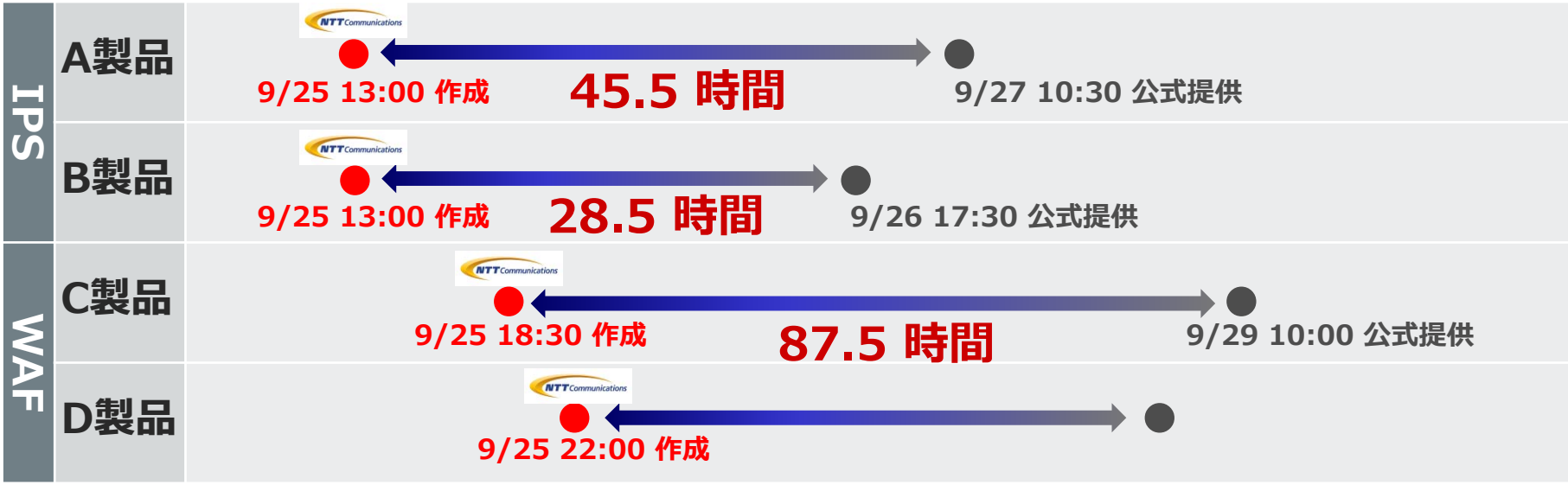
緊急度	対応実施基準
S+	・速やかにサービスを停止し、対処を実施する
S−	・速やかにサービスを停止し、対処を実施することを基本とする ・停止せずに対処可能な場合は、サービス責任者がその根拠を明らかにし、対処を実施する
A	・速やかに手順検討の後、対処を実施する
B	・各組織にて、定期的に対処を実施する



NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

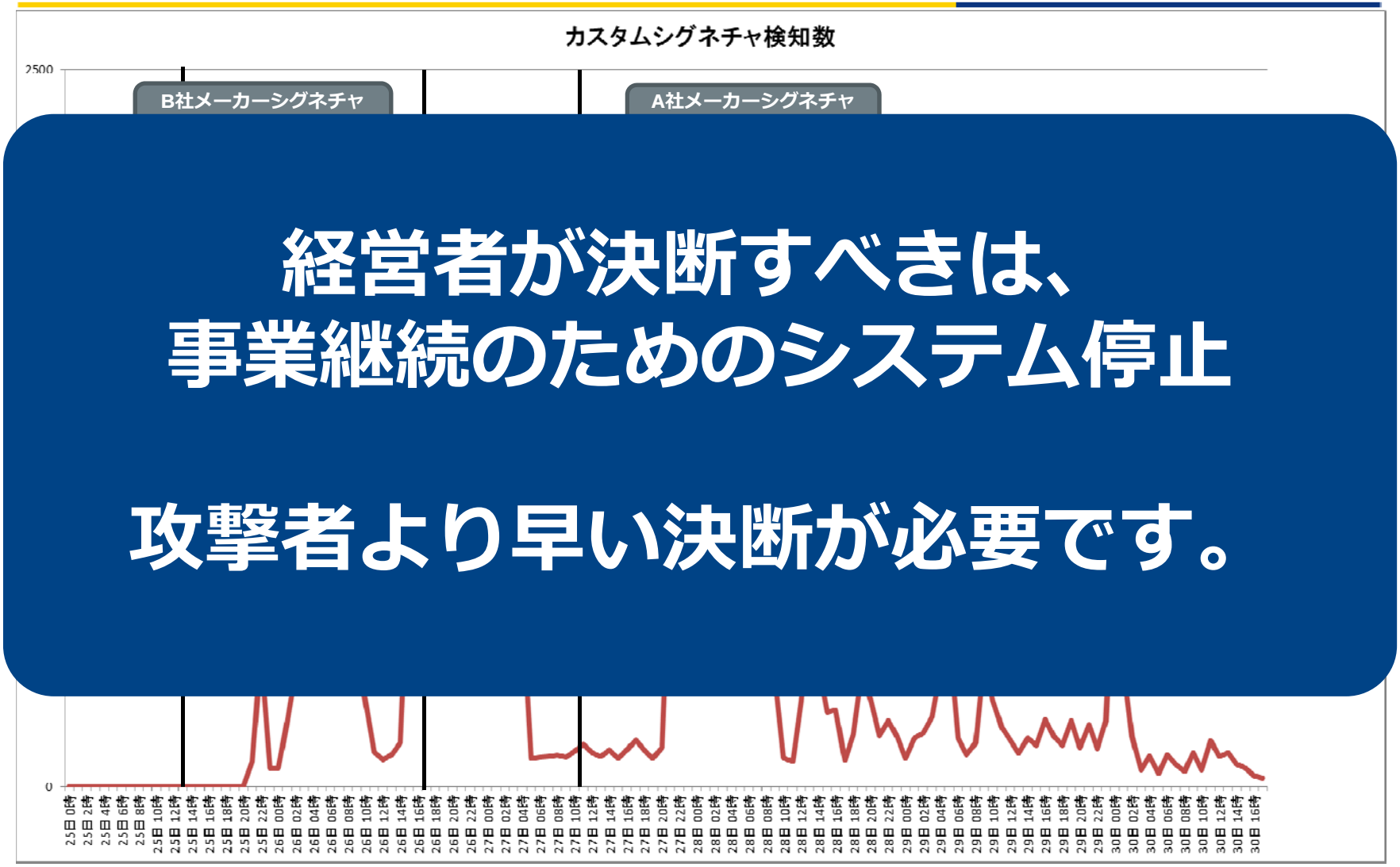
bash脆弱性（ShellShock）対応状況

●独自にカスタムシグニチャを作成し対策実施



NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

bash脆弱性（ShellShock）対応状況



経営者が決断すべきは、
事業継続のためのシステム停止

攻撃者より早い決断が必要です。

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

セキュリティリスクマネジメントの見直し

- セキュリティリスクマネジメントの欠如が露呈
- 全社ITシステム等を徹底調査し、セキュリティリスク低減策を講じるとともに、
- お客様に提供する全サービス・全システムにおける統一したルールや体制を整備
- ITシステムの全社管理とセキュリティリスクマネジメントの新たな業務運営プロセスを確立

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

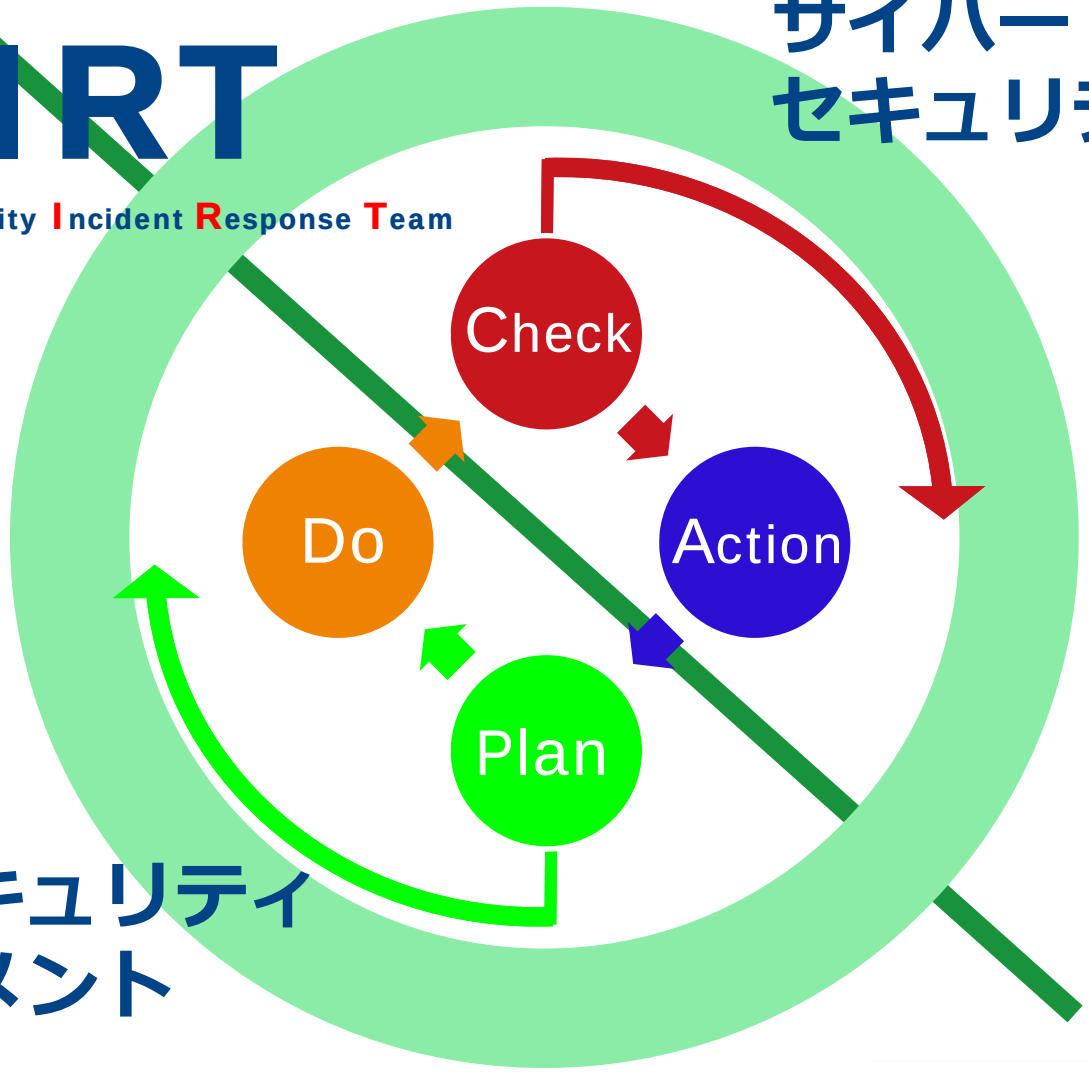
4. CSIRT体制強化の取り組み

情報セキュリティ部（CSIRT）について

CSIRT

Computer **S**ecurity **I**ncident **R**esponse **T**eam

サイバー
セキュリティ対策



情報セキュリティ
マネジメント

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

情報セキュリティの方程式

脆弱性（セキュリティホール）対策の徹底

～人・システム・運用・制度・企業文化～

$$\text{セキュリティレベル} = \frac{\text{①テクノロジー（新技術の導入）} \times \text{②オペレーション（監視・運用・社員教育）}}{\text{③ユーザビリティ（利便性・自由度）}}$$

お客さまや社内外からの、よろず相談や協力要請をお待ちしてます！

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

ご清聴ありがとうございました。