資料安作２４－７

NTT
NTT Secure Platform Laboratories
NTT セキュアプラットフォーム研究所

セキュリティ技術に関する NTT研究所の取り組み

2012年9月4日

NTTセキュアプラットフォーム研究所
大久保　一彦

© 2012 NTT Secure Platform Laboratories

変化する環境とセキュリティ

変化する攻撃

- マルウェアによる攻撃の仕組みが複雑化、新種マルウェア出現ペースの加速
- 攻撃の目的が、犯罪者による「金銭目的」や、組織ぐるみの「組織活動の妨害」に拡大し深刻化

変化するシステム・サービス

- クラウドやスマートフォンなどの新たなシステム・サービスを狙うサイバー攻撃の増加

変化するデータ

- 取り扱うデータ量の爆発的増加だけでなく、守るべき情報資産の割合も増加

© 2012 NTT Secure Platform Laboratories

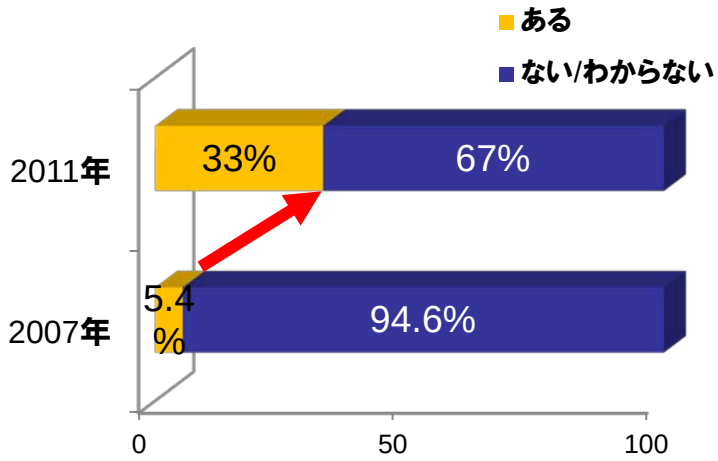
変化するサイバー攻撃の目的

変化する攻撃

攻撃の目的が、従来の個人レベルの「いたずら」や「能力の誇示」から、特定の企業・団体を標的にした、犯罪者による「金銭目的」や、組織ぐるみの「組織活動の妨害」に拡大し深刻化しつつある

新しい攻撃（APT：Advanced Persistent Threat）

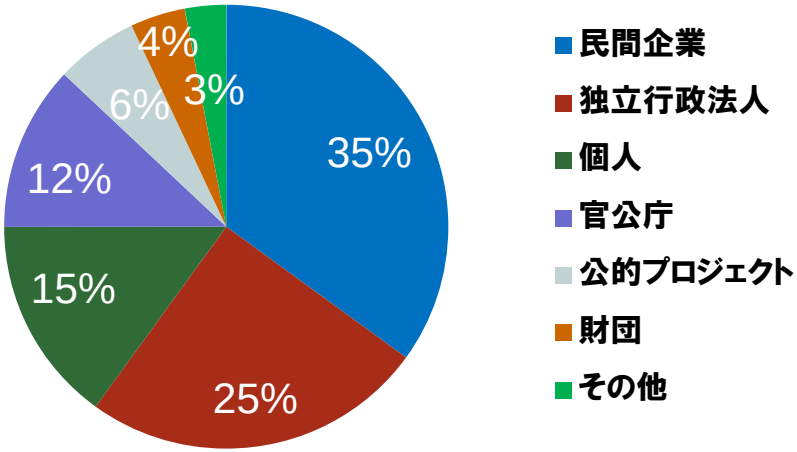
近年、従来からの標的型攻撃を糸口に複数の攻撃手法を組み合わせ、より甚大な被害を与える攻撃事例が報告されている



標的型と思われるサイバー攻撃を受けたことがある企業

2007年の5.4%から2011年の33%に急増

出典：標的型サイバー攻撃への対応について（2011年経済産業省調査）
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/005s_01_00.pdf



標的型攻撃メールのターゲット

民間企業や公共団体の職員を狙った攻撃が多い

出典：IPA テクニカルウォッチ『標的型攻撃メールの分析』に関するレポート
http://www.ipa.go.jp/about/technicalwatch/pdf/111003report.pdf

© 2012 NTT Secure Platform Laboratories

スマートフォンの落とし穴

変化するシステム・サービス

Androidのアプリケーションインストール時に求められるパーミッション解除が悪用されるきっかけとなり、端末内の**電話番号や保存データが漏えい**する危険性がある

電話番号などの個人情報や
SDカード内のデータが漏えい

ネットワーク通信
⇒ パーミッション解除

Android上のアプリケーション⇒マルウェア

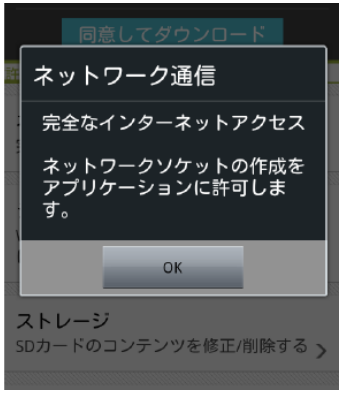
SDカードへのアクセス
⇒ パーミッション解除

電話番号へのアクセス
⇒ パーミッション解除

電話番号

SDカードは、一旦解除すると、
全てのアプリからアクセス可能に

Androidのセキュリティは
パーミッションモデル。
パーミッション解除の表示例（下記）

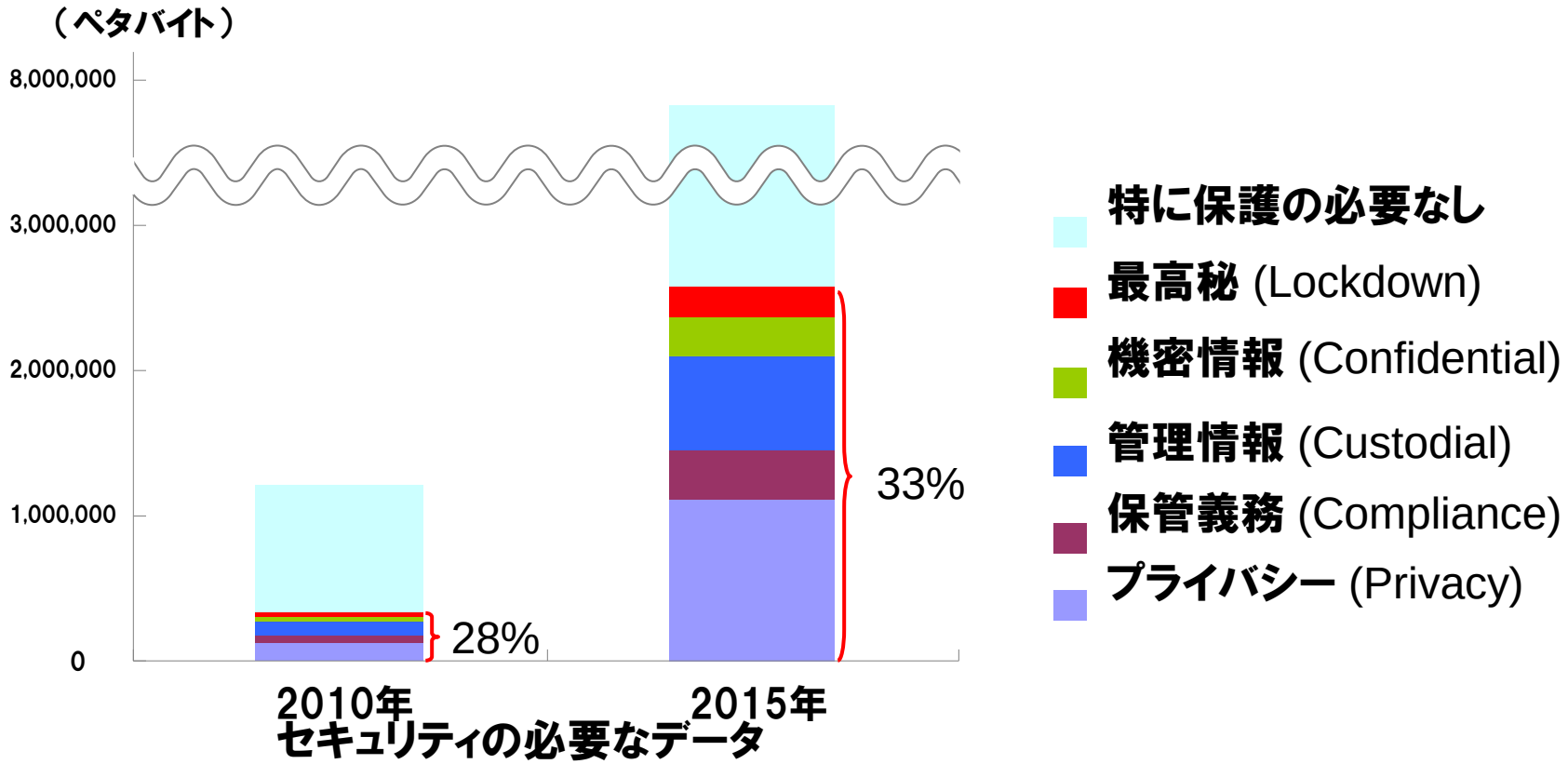


© 2012 NTT Secure Platform Laboratories

セキュリティが必要なデータ

変化するデータ

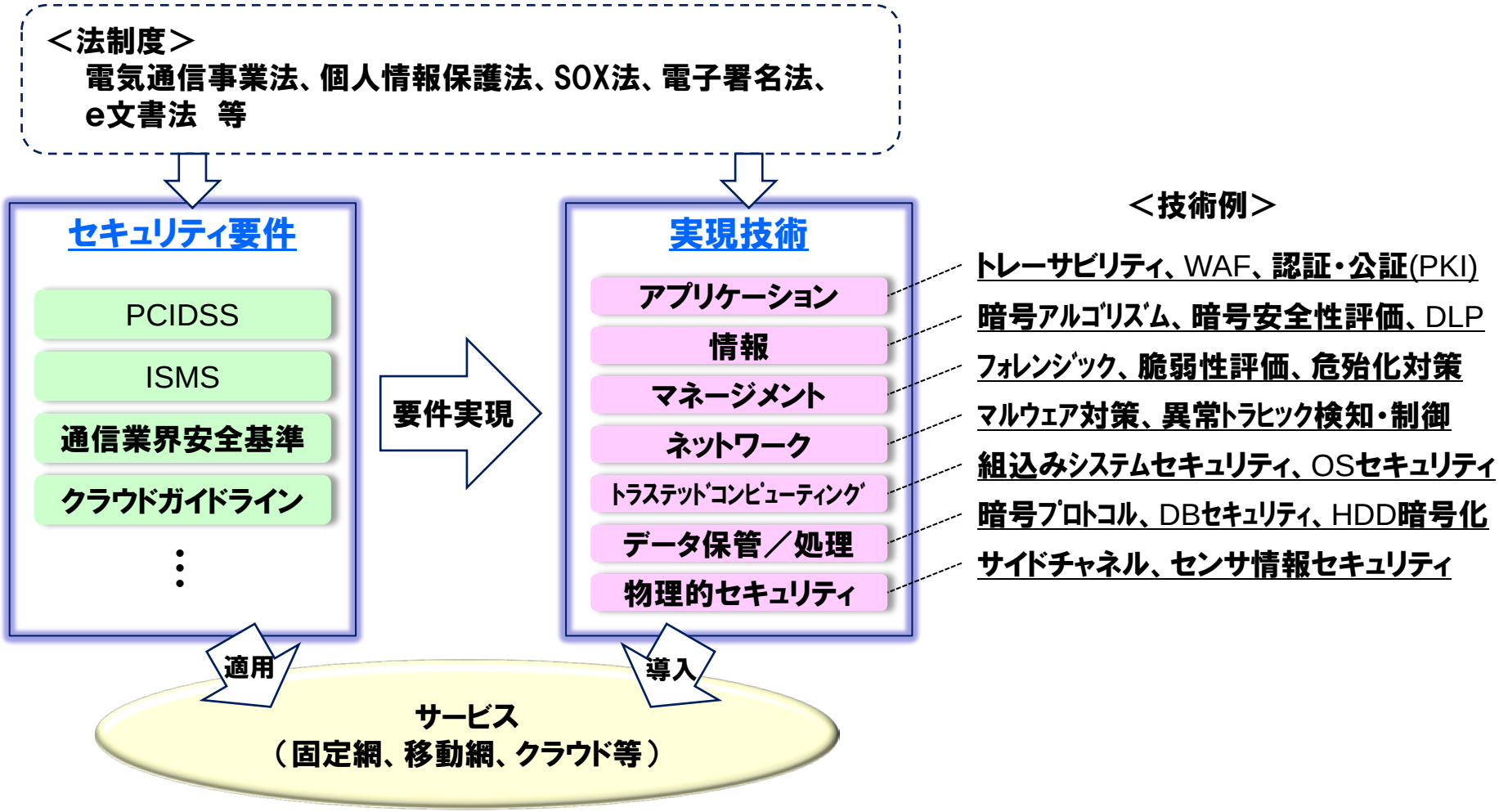
2010年に世界で生成・複製されているデータ量（1.2ゼタバイト）のうち、28%はセキュリティが必要なデータであり、今後この**割合は増加**し、2015年には33%に達する見込み



出典：2011 Digital Universe study, "Extracting Value from Chaos“ by IDC http://idcdocserv.com/1142 を元に作成

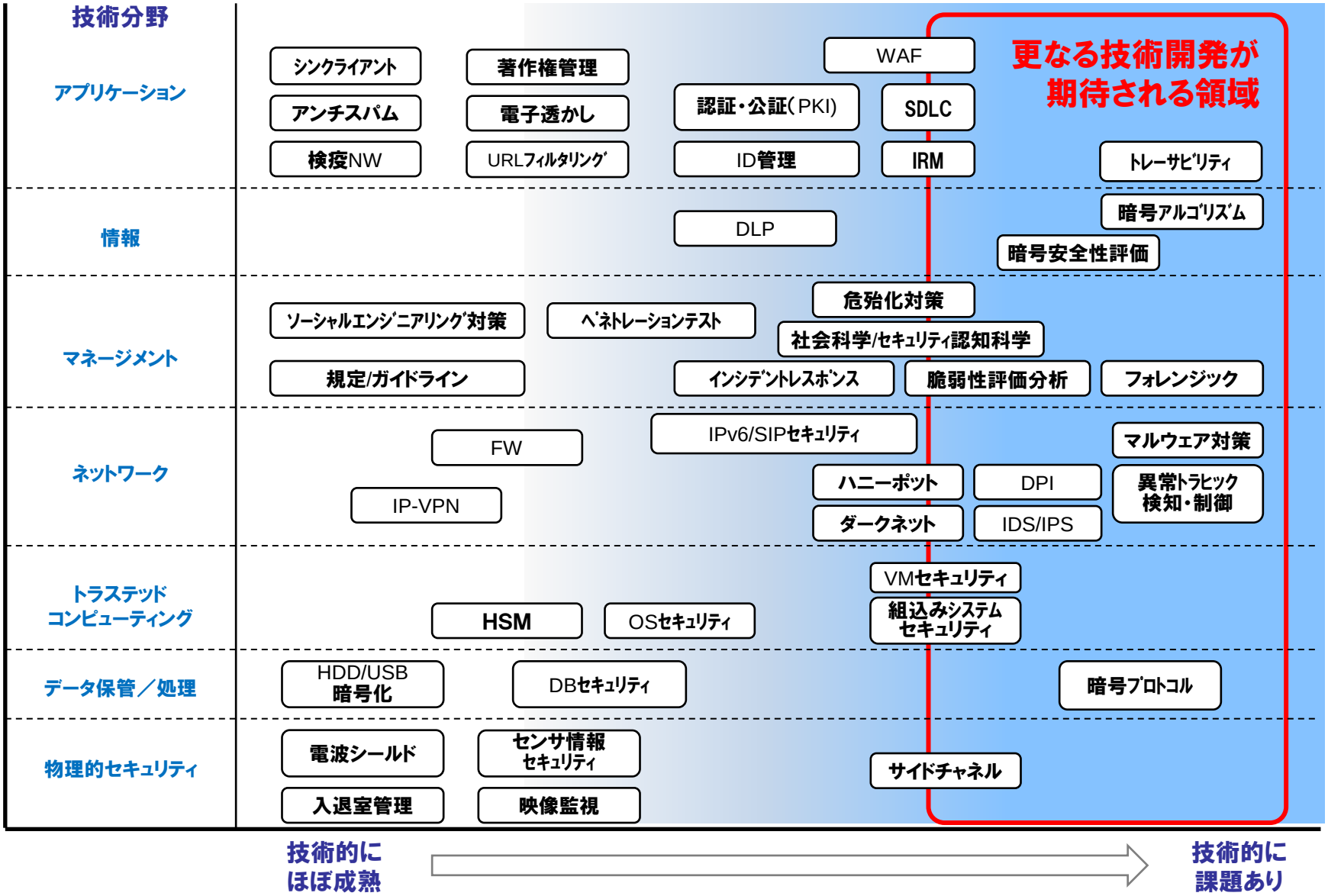
© 2012 NTT Secure Platform Laboratories

電気通信事業者に求められるセキュリティ要件と実現技術



© 2012 NTT Secure Platform Laboratories

セキュリティ技術の成熟度



© 2012 NTT Secure Platform Laboratories

変化する環境に対応するNTT研究所の取り組み

変化する攻撃 ⇒ **脅威の把握が困難**な時代へ

脅威の事前の徹底把握と、発生したインシデントの徹底解析が不可欠

- ◆脅威のプロファイリング・カタログ化
- ◆セキュリティ事象のモニタリング・り障範囲特定
- ◆脅威の予兆検知
- ◆未然防止・被害極小化を図る技術開発と
  セキュリティオペレーション強化

変化するシステム・サービス ⇒ **想定しない脆弱性**が露呈する時代へ

脆弱性の徹底把握と、脆弱性が存在しないシステムの追求

- ◆脆弱性などのセキュリティ情報の共有・分析機能の構築
- ◆安全性が保障されたシステムの構築手法の標準化

変化するデータ ⇒ **大量・重要な情報資産**を扱う時代へ

様々な必要性に応じたセキュリティレベルで情報資産を管理できることが必要

- ◆セキュリティやプライバシーレベルの選べる化

© 2012 NTT Secure Platform Laboratories

マルウェア対策技術

変化する攻撃

世界中に攻撃センサを設置して最新攻撃を監視することにより、ブラックリストをデータベース化し、ネットワークにおけるマルウェア対策やインシデント対応等に活用

- 世界の最新攻撃を監視
- 局所的な攻撃情報も収集
- いち早く最適な対策へ

世界中の攻撃検知、収集

Webアプリの脆弱性
- Webサーバ型ハニーポット

Webブラウザの脆弱性
- Webクライアント型ハニーポット

OSの脆弱性
- Windows型ハニーポット

解析

動的解析

静的解析

攻撃情報のDB化、分析（ブラックリストDB）

- 悪性アプリ情報
- 悪性Web情報
- 攻撃元情報
- Exploitコード情報
- 検体情報

等

活用（NTTグループ会社）

マルウェア対策サービス
- ユーザ保護
- データセンタ保護
- クラウド保護

攻撃監視

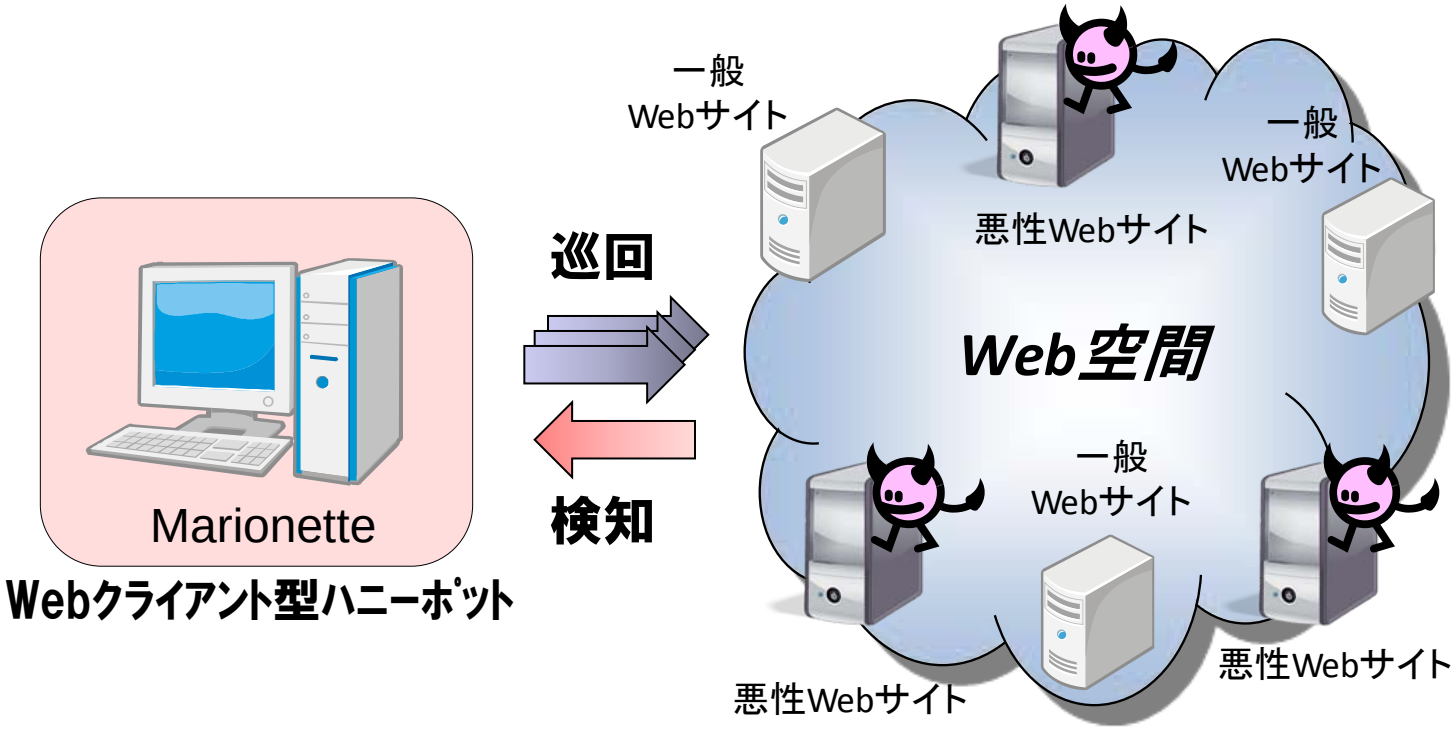
インシデント対応

© 2012 NTT Secure Platform Laboratories

Webクライアント型ハニーポット技術

変化する攻撃

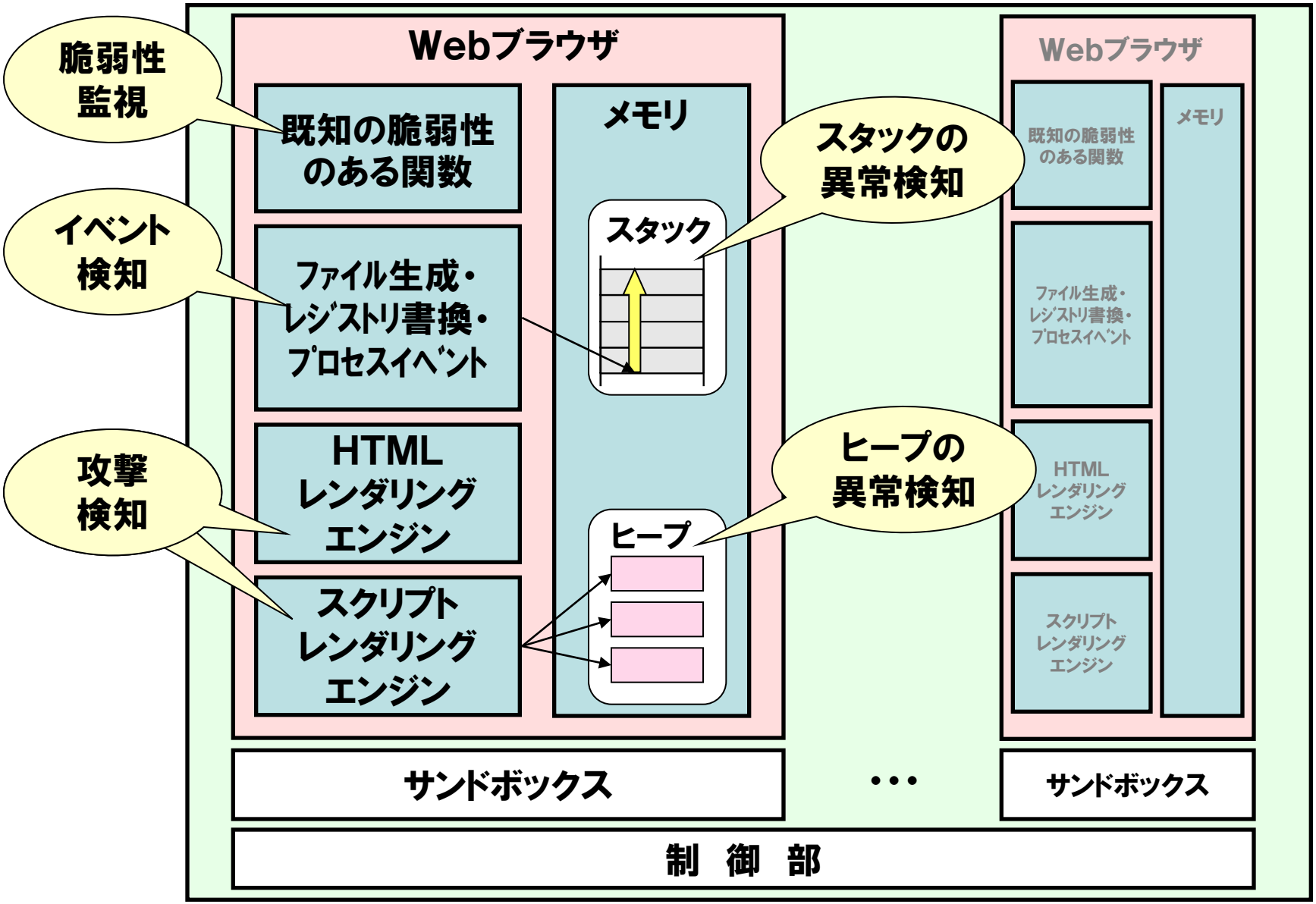
閲覧しただけでマルウェアに感染してしまう悪性Webサイトが急増
【Marionette ～Webクライアント型ハニーポット技術～】
Webサイトを巡回して、Webブラウザへの攻撃を検知、悪性Webサイトを事前に見つけ出し、攻撃情報を収集する技術



© 2012 NTT Secure Platform Laboratories

Marionette： 内部構造

変化する攻撃



© 2012 NTT Secure Platform Laboratories

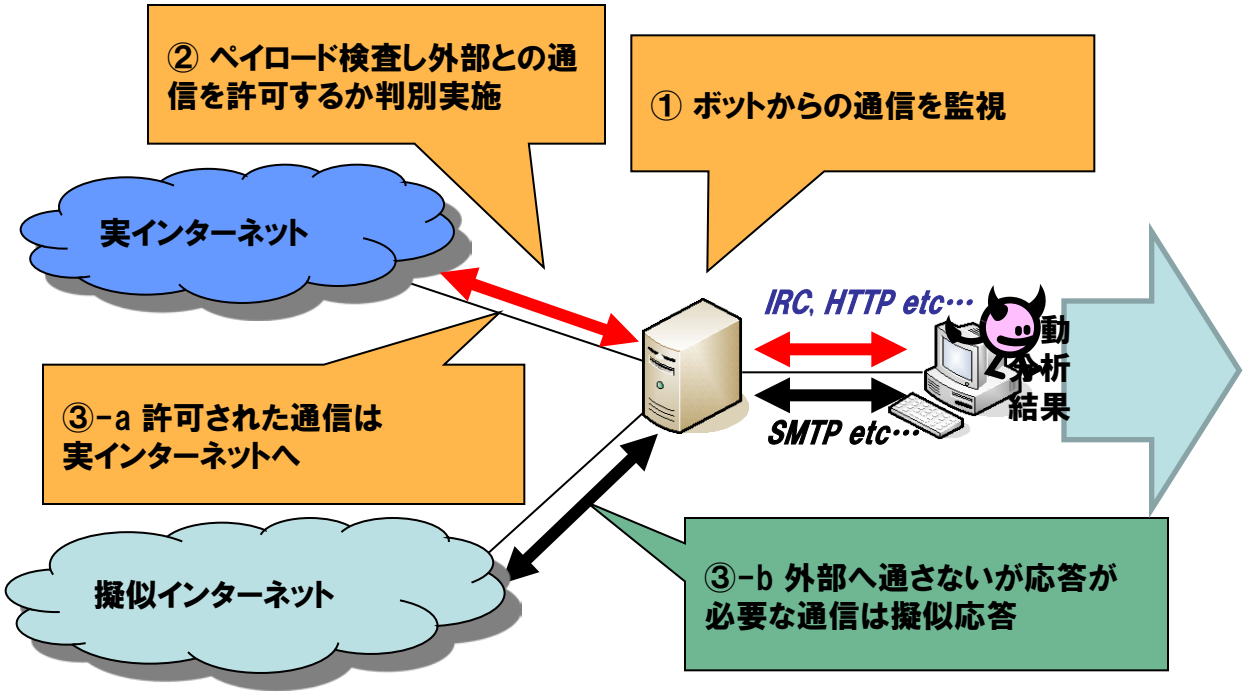
動的解析

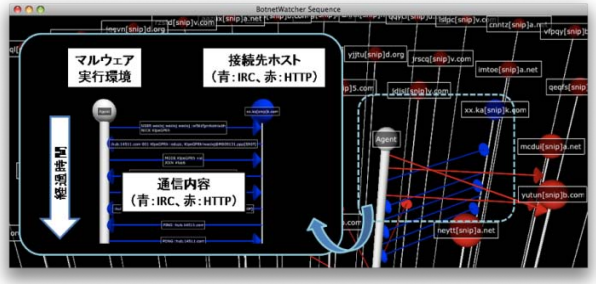
変化する攻撃

マルウェアには、指令サーバからの命令で動作する「ボット」や、別のマルウェアをダウンロードする「ダウンローダ」など、**外部との通信により真の脅威が顕在化**するものも存在。

【Botnet Watcher　～マルウェア通信解析技術～】

指令サーバとの通信や追加プログラムのダウンロードだけをインターネットに通過させ、**マルウェアの安全に動的解析**する技術

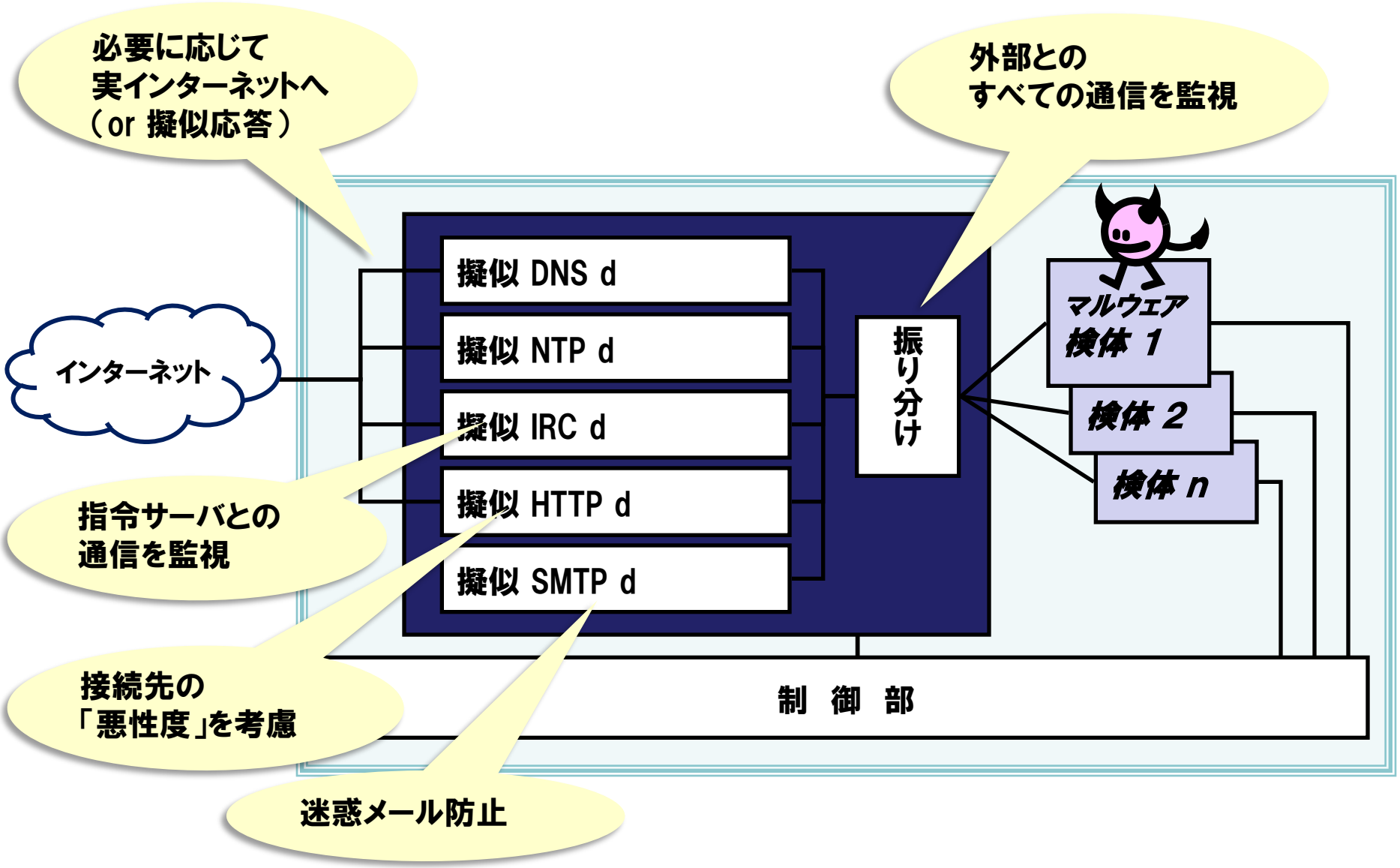




© 2012 NTT Secure Platform Laboratories

Botnet Watcher 詳細

変化する攻撃

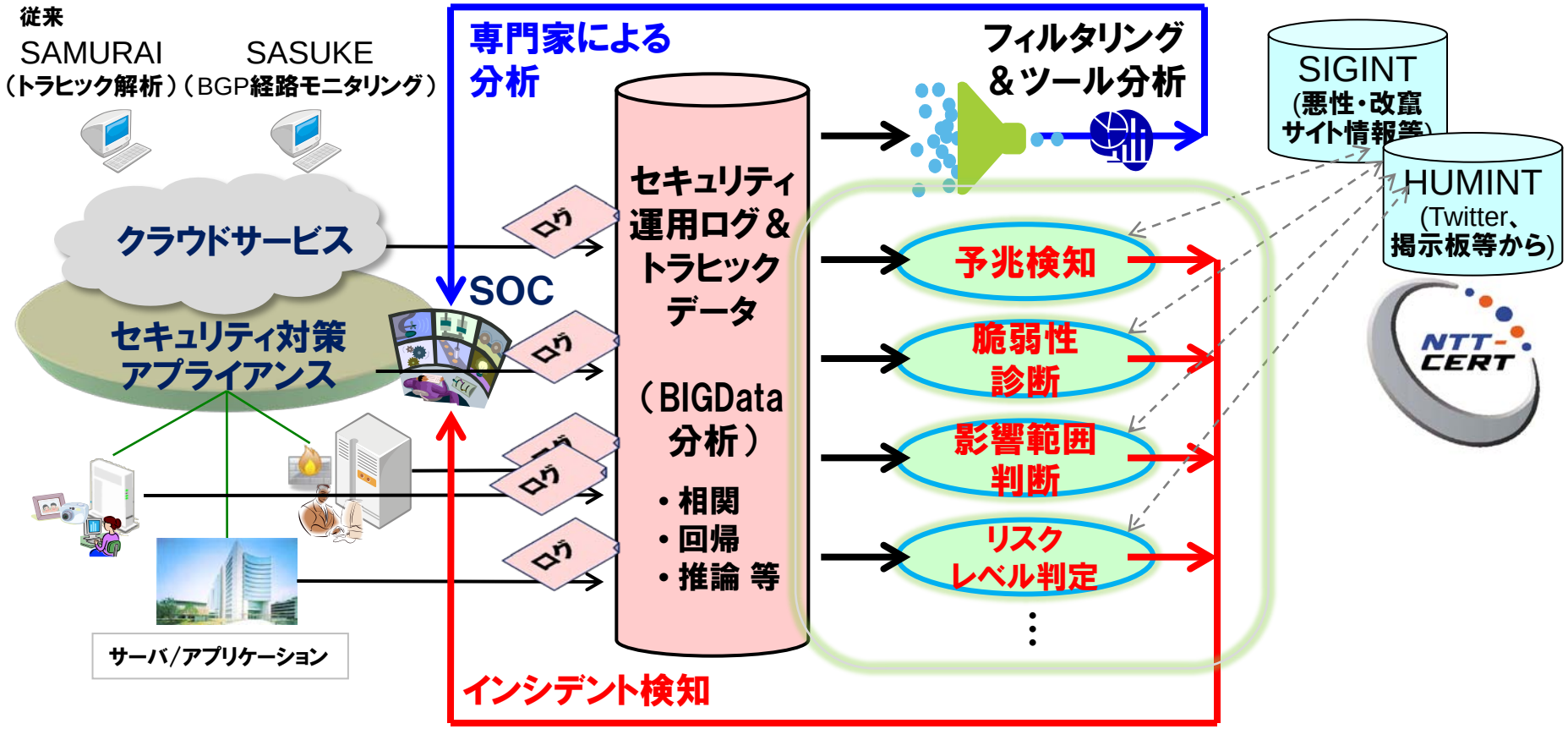


© 2012 NTT Secure Platform Laboratories

新たな脅威へ対応するSIEM開発

変化する攻撃

セキュリティ対策アプライアンス(FW, IPS/IDS, UTM)のログやトラヒック情報を収集・分析し、攻撃の予兆検知やお客様への影響の把握ができる技術を確立 (SIEM: Security Information and Event Management)



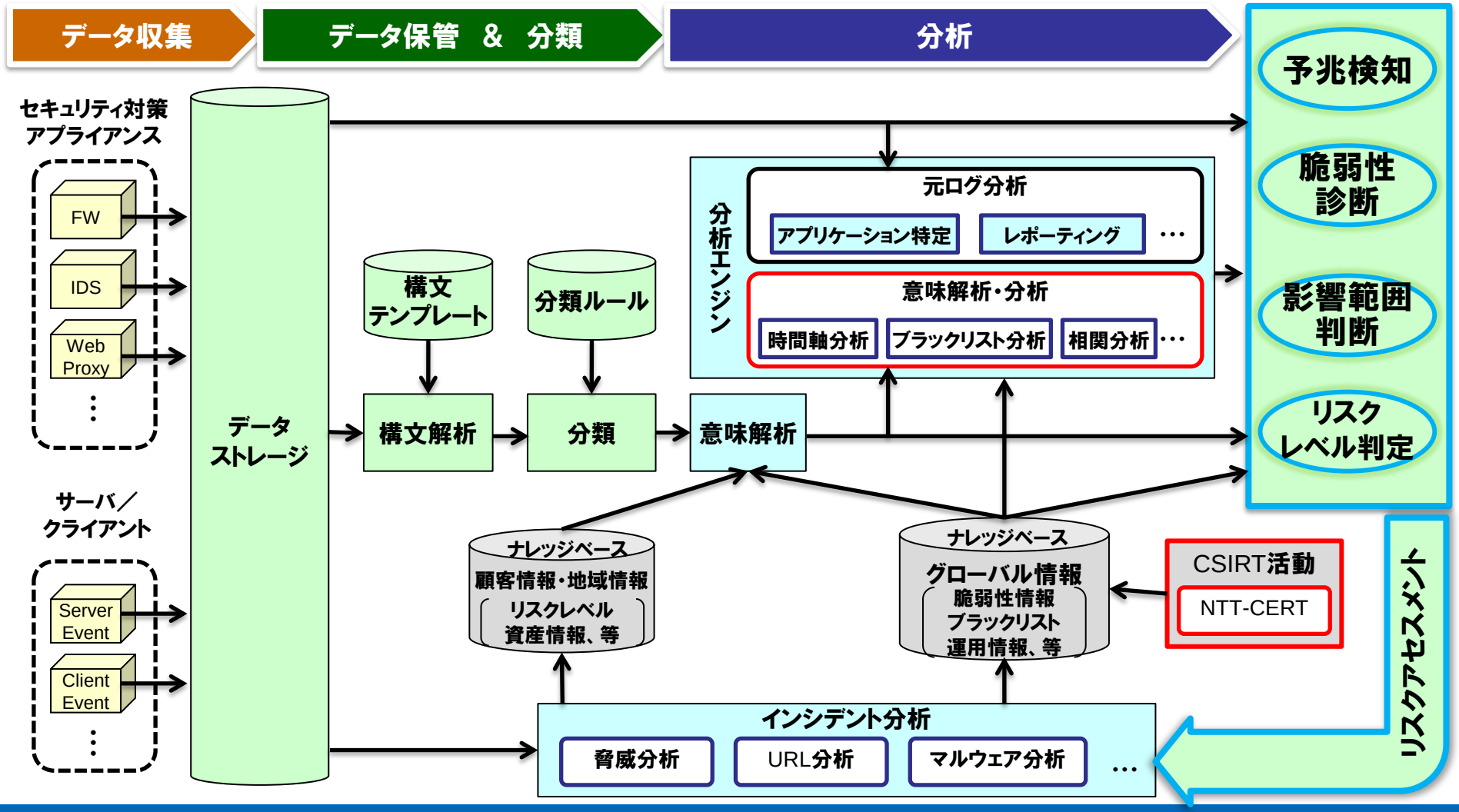
© 2012 NTT Secure Platform Laboratories

ログ分析エンジン技術の開発

変化する攻撃

SIEMの重要機能であるログ分析機能実現に向けて、NTT研究所は分析エンジン技術の開発に取り組む

□：NTT研究所技術

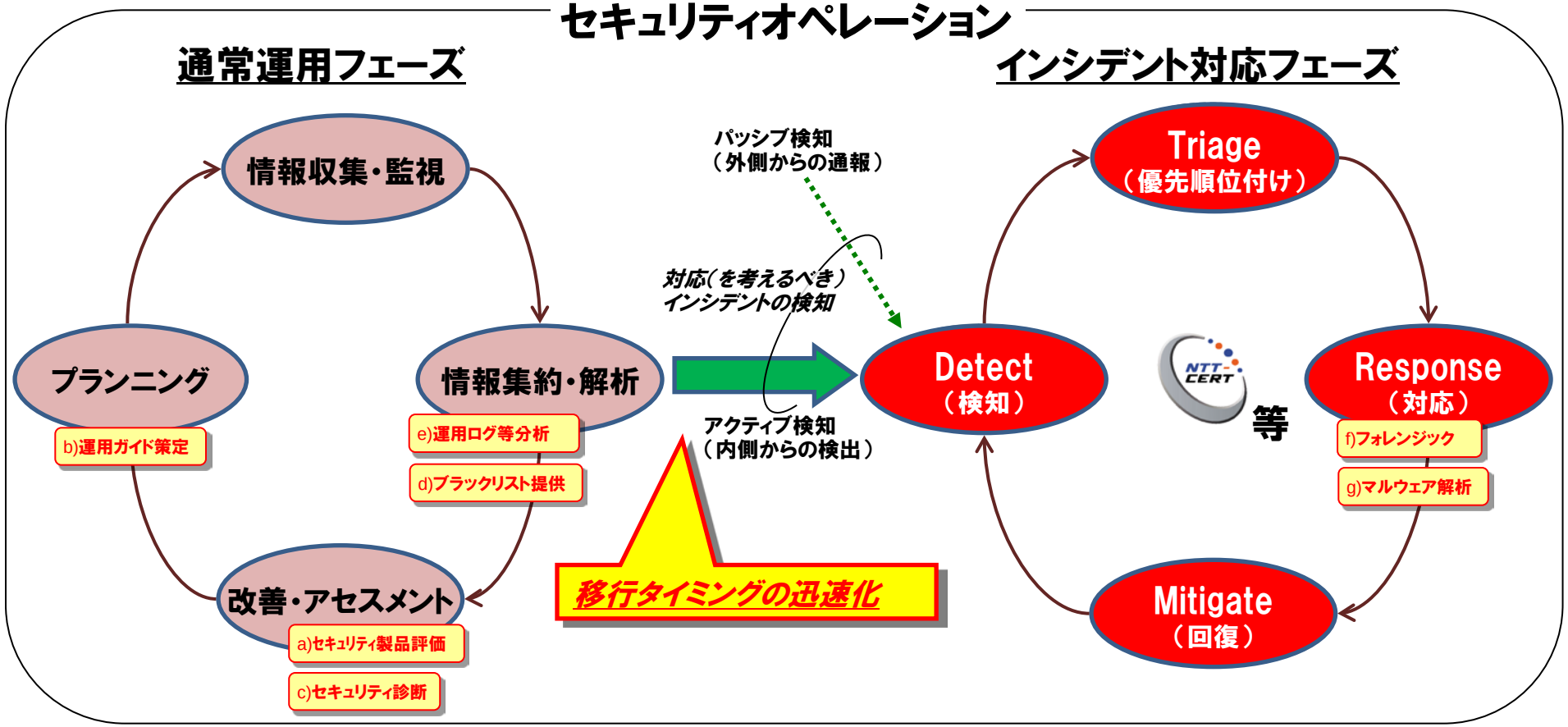


© 2012 NTT Secure Platform Laboratories

セキュリティオペレーションの強化ポイント

変化する攻撃

0-day攻撃や未知のマルウェア等により重大な被害につながる事象が発生した際の
インシデント対応フェーズへの迅速な移行がセキュリティオペレーションの強化ポイント



高度なサイバー攻撃への対応

プロアクティブな対応（予兆検知）

オペレーション効率化・自動化

© 2012 NTT Secure Platform Laboratories

NTT-CERTの業務概要

変化する攻撃

- NTTのCSIRT(Computer Security Incident Response Team)として、2004年に発足。
- セキュリティ情報をいち早くキャッチし、NTTグループ全体の被害の極小化、未然防止を図る。

外部機関
(FIRST,NCA等)

独自センサ等
(例:ハニーポット)

～通常対応～

防止 → 脆弱性等の収集・共有 → 事件 攻撃の検知 → 被害発生時の対応

フィードバック

～警戒・緊急対応～

～ CSIRTがやること ～

- セキュリティ運用 ノウハウ集積・活用
- 脆弱性・攻撃等に関する情報の収集分析と早期検知
- 内外の適材適所への迅速な情報伝達と専門的対応支援

NTT-CERTのNTTグループ支援施策例

- トレーニング等
  - ・セキュリティSE
  - ・セキュリティ教育
- 情報共有
  - ・脆弱性検証情報提供
  - ・公開前脆弱性情報提供
- 分析・調査
  - ・インシデント通知
  - ・情報漏洩検知
- 相談受付
  - ・インシデント対応支援
  - ・事例共有
- 対応支援

各フェーズでNTTグループを支援

リスク管理
被害の未然防止／被害の極小化

事業会社

© 2012 NTT Secure Platform Laboratories

セキュリティオペレーション・リサーチの強化

変化する攻撃

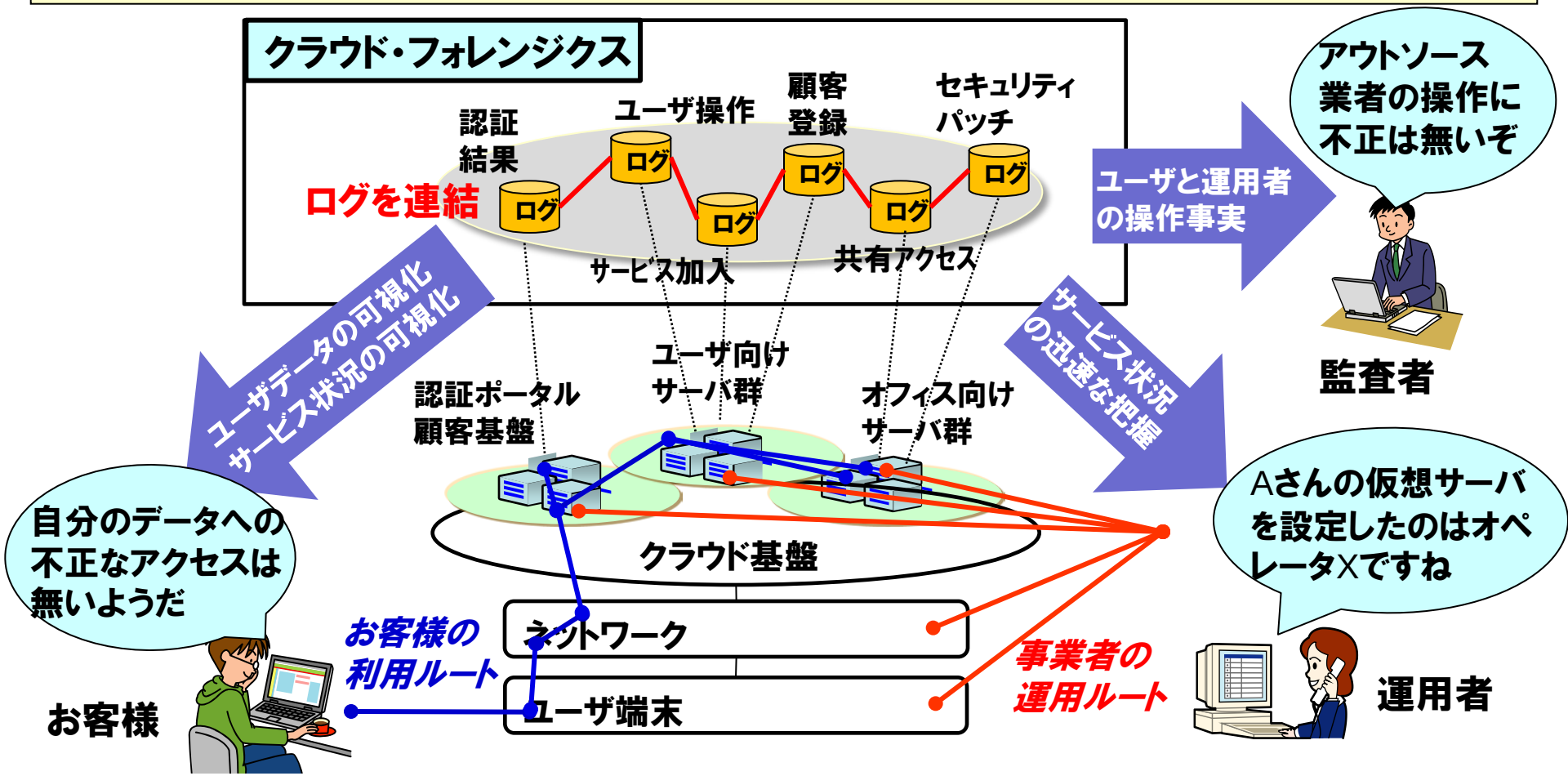
事業会社 セキュリティ運用	未然防止		被害最小化
	予防	検知	事後対応
フィールドサポート	事業環境における検証設備構築や実施手順等に関わる技術支援	セキュリティ診断結果に基づく対応やブラックリスト及びログ分析に関わる技術支援	分析対象取得、技術対策適用における、オンサイトでの技術支援
R&Dミッション	**a）セキュリティ製品評価** 事業導入前に、新たな技術/製品等の機能、性能、脆弱性を評価するとともに、必要な対策等をレポート。 **b）運用ガイド策定** 政府や業界によるガイドライン策定の動向を見据え、グループでの遵守に向けた技術検証や手順書策定を実施。	**c）セキュリティ診断** グループ各社のウェブサイト等について、改竄、脆弱性、要塞化不備を検査/分析し、問題があれば対策等を立案。 **d）ブラックリスト提供** 研究所で構築したブラックリストをグループ会社に情報展開し、攻撃ブロックに寄与。 **e）運用ログ等分析** 関連の先行技術を目利きしつつ、グループにおける運用ログ等の収集・分析手法を確立し、基盤システム化を実施。	**f）フォレンジック** **g）マルウェア解析** アプリケーションログ、システムログ、悪性プログラム等の分析手法の確立及び技術変化に追随する継続的な維持・高度化。

© 2012 NTT Secure Platform Laboratories

クラウド・フォレンジクス技術

変化するシステム・サービス

クラウド上に分散する「人の操作」、「コンテンツの移動・変更」、「プロセスの動作」に関するログ情報などから、
事実証跡のアカウンタビリティを提供し、安心と安全を可視化・証明

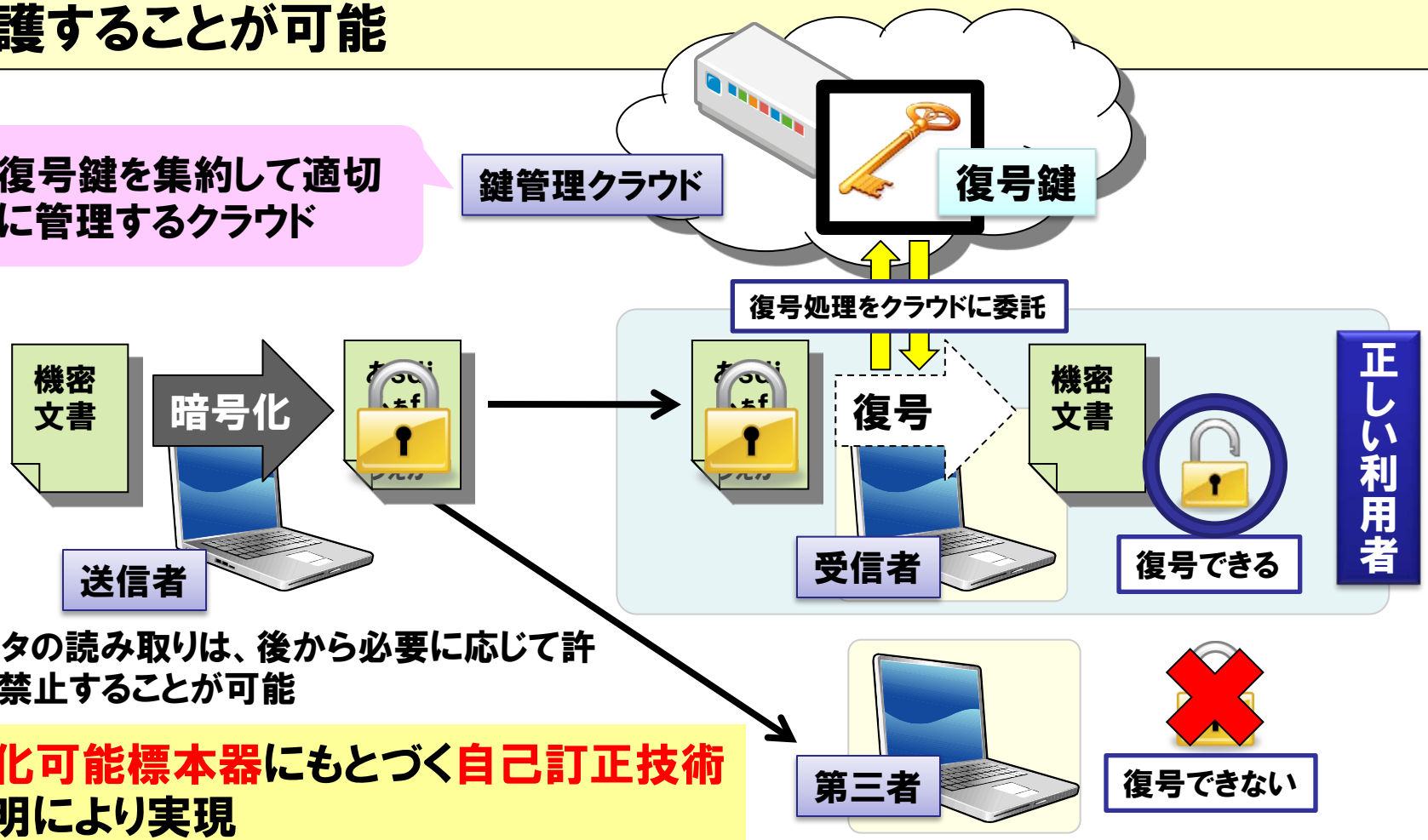


© 2012 NTT Secure Platform Laboratories

クラウド鍵管理型暗号技術

変化するデータ

復号鍵をクラウド内で管理し、**クラウドに復号処理をアウトソース**させる技術であり、利用者は復号鍵を管理することなくデータを保護することが可能



データの読み取りは、後から必要に応じて許可/禁止することが可能

乱数化可能標本器にもとづく**自己訂正技術**の発明により実現

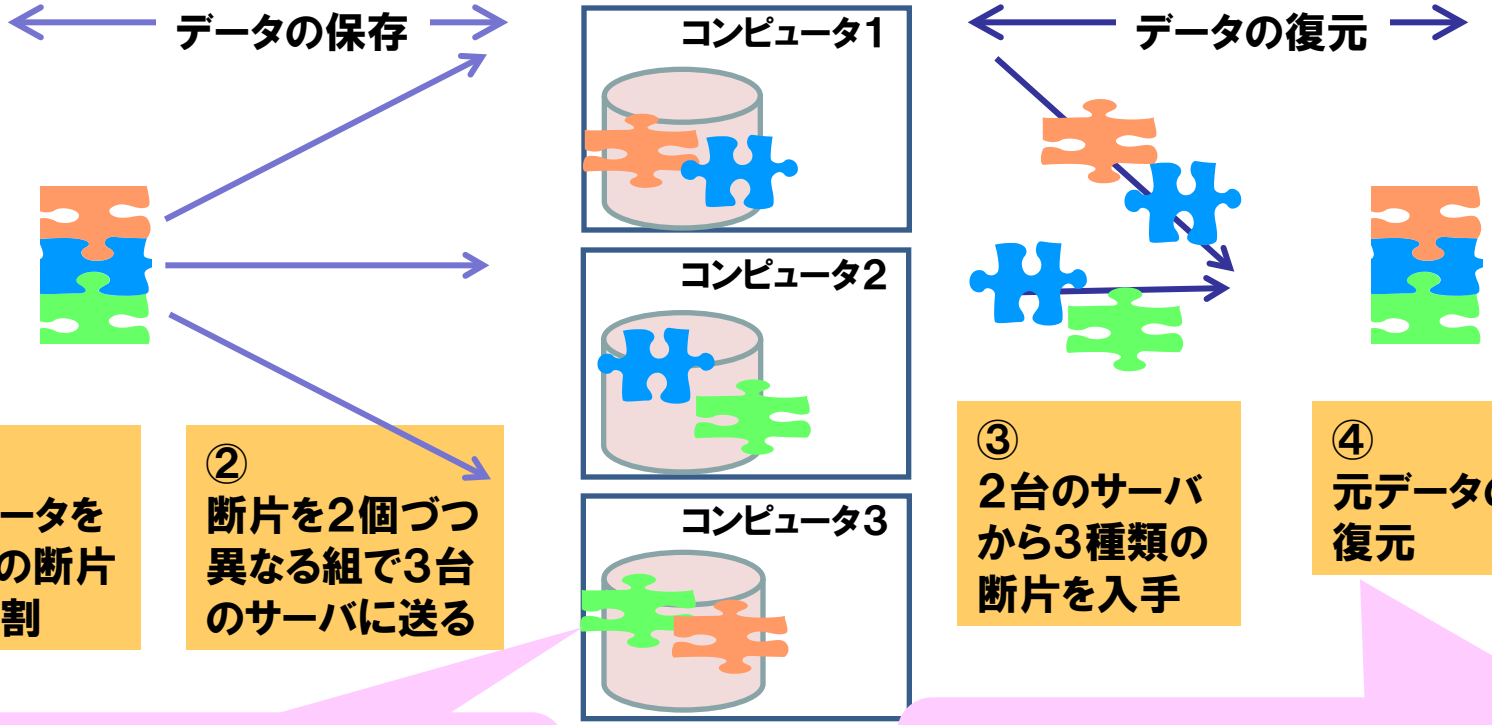
（2012年2月10日報道発表）http://www.ntt.co.jp/news2012/1202/120210b.html

© 2012 NTT Secure Platform Laboratories

秘密分散技術

データの機密性と可用性を高めるために、データを単独では意味のない複数の断片に分割して分散保管する技術

【例】（3個に分割、2個で復元）



① 元データを3個の断片に分割

② 断片を2個づつ異なる組で3台のサーバに送る

③ 2台のサーバから3種類の断片を入手

④ 元データの復元

一定数以上のコンピュータが破られない限り、情報が漏えいしない

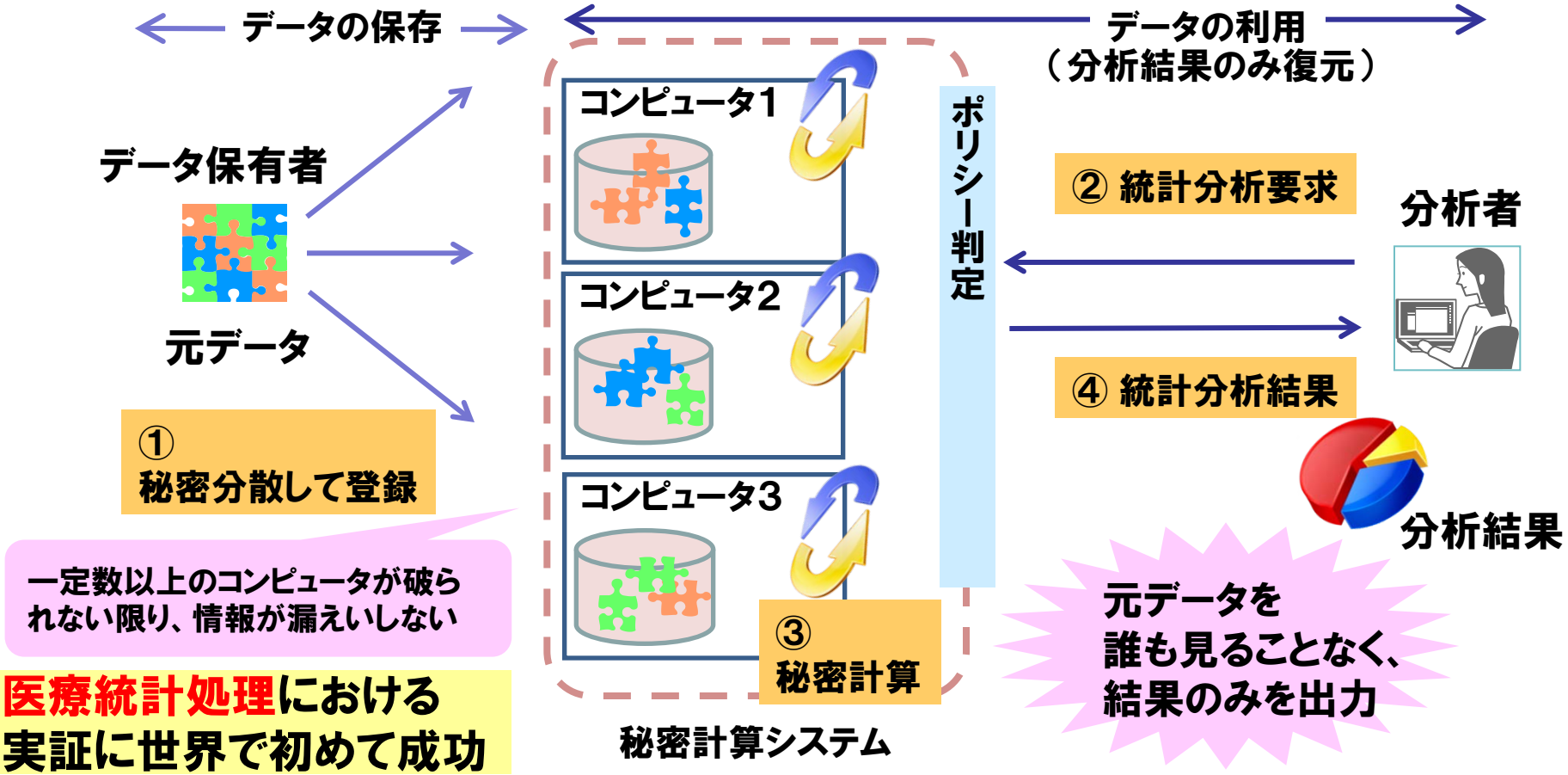
いずれかのコンピュータが災害にあっても、一定数以上のコンピュータが稼動していればデータを復元可能

© 2012 NTT Secure Platform Laboratories

秘密計算技術

変化するデータ

個人情報のようなセンシティブなデータの処理も安心してクラウドへ委託できるようになることを狙う、クラウド運用者に対してもデータを秘匿したまま統計分析などの処理が行える技術



医療統計処理における実証に世界で初めて成功

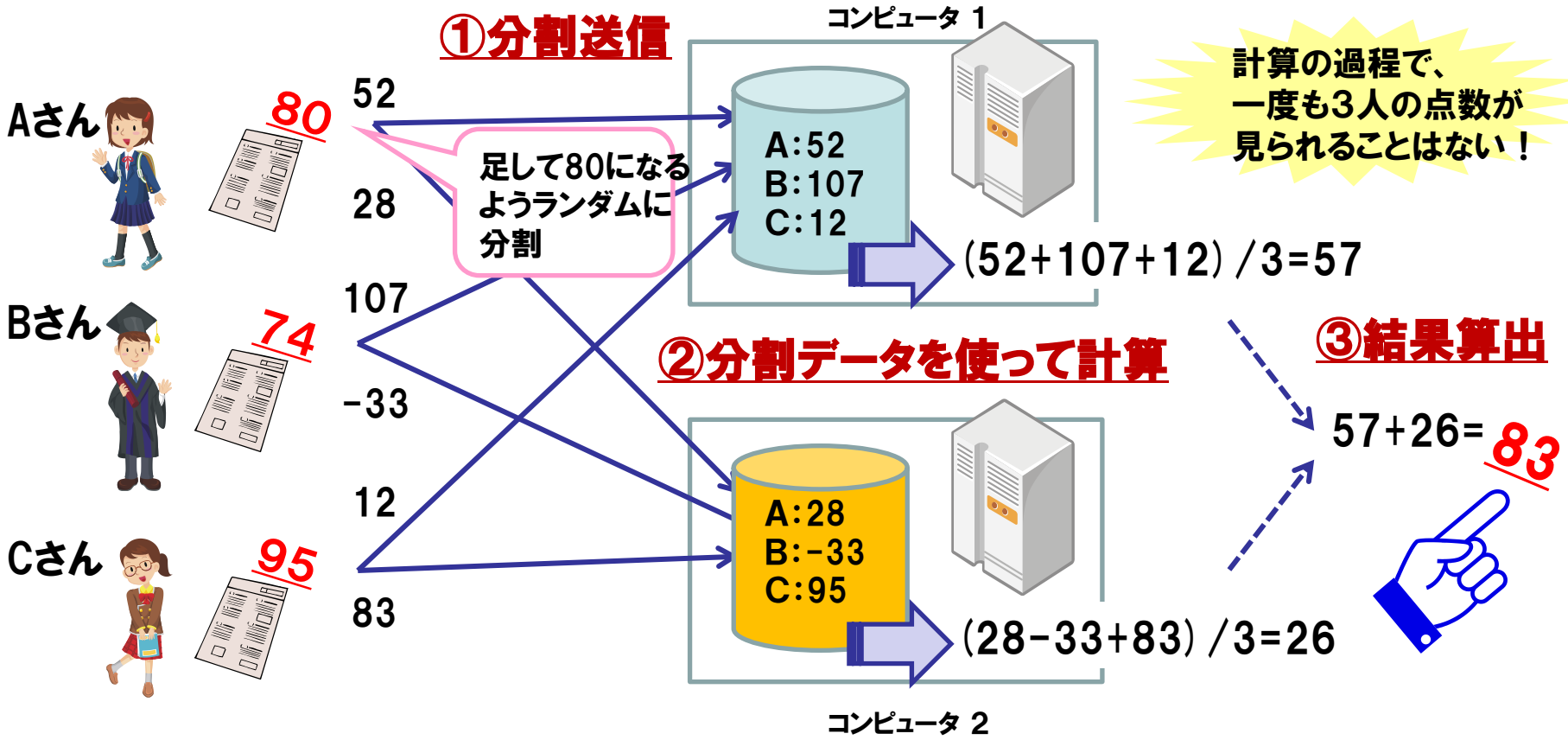
（2012年2月14日報道発表）http://www.ntt.co.jp/news2012/1202/120214a.html

© 2012 NTT Secure Platform Laboratories

秘密計算技術の分かりやすい例

変化するデータ

『3人のテストの点数を誰にも見せないで平均点を求めたい』



より一般的な計算に関しては古くから計算原理は知られていたが、処理コストが高く実用化が困難と考えられていた

© 2012 NTT Secure Platform Laboratories

まとめ：変化する環境に追随するセキュリティ対策

リスク ＝ 脅威 × 脆弱性 × 守るべき資産

変化する攻撃	変化するシステム＆サービス	変化するデータ
攻撃の複雑化・組織化 ↓ ●脅威の把握がより困難に	クラウドやスマートフォン（BYOD）などの普及拡大 ↓ ●想定していなかった脆弱性の露呈	増え続けるデータのセキュリティ担保 ↓ ●守るべき資産が多様かつ大量に

セキュリティ対策（リスク低減）

技術（備え系） ←→ **運用（対応系）**

攻撃検知・防御
（NW&システムを守る）

暗号
（データを守る）

可視化・証跡提供
（継続モニタリング）

オペレーション高度化
（セキュリティ運用強化）

© 2012 NTT Secure Platform Laboratories