ユニシス研究会
JAPAN UNISYS USERS ASSOCIATION

過去と未来を見通すログ分析

～真のウィルス対応は、ウィルスを削除した時から始まる～

東北インフォメーション・システムズ株式会社
本間　淳平

BITS 2015
NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM

会社概要

社名	東北インフォメーション・システムズ株式会社 [略称：TOiNX(トインクス)]
本　社 所 在 地	〒９８０-００２１ 宮城県仙台市青葉区中央二丁目９番１０号 セントレ東北 ＴＥＬ（０２２）７９９－５５５５　ＦＡＸ（０２２）７９９－５５６１
従業員	６８５名(平成２６年７月１日時点)
株　主	東北電力株式会社
主な 事業 内容	○ 東北電力 情報システム企画・開発・運用・ヘルプデスク ○ 東北電力企業グループ 情報システム企画・開発・運用・ヘルプデスク ○ クラウドサービス「彩雲（さいうん）」 ○ セキュリティサービス（標的型攻撃メール対応訓練サービスほか） ○ ｉＤＣ（インターネット・データセンター）　（【丸ごと！バックアップ】サービス） ○ 人事労務業務支援（人事労務総合パッケージ「Ｃｏ.人労（コジロー）」） ○ 電子認証サービス（電子証明書発行サービス） など

目次

１．サービス立ち上げの背景

２．ログ分析を主軸としたサービス

３．ログ分析の手法とその効果 （対応事例）

４．成果と課題

- 1. サービス立ち上げの背景

はじめに

1.1 サービス立ち上げの背景

サイバー攻撃の脅威の増大

ウィルスを利用したサイバー攻撃が年々増加
対策レベルの低い関連企業を踏み台に大企業を狙う手法も

＋

情報を守る義務

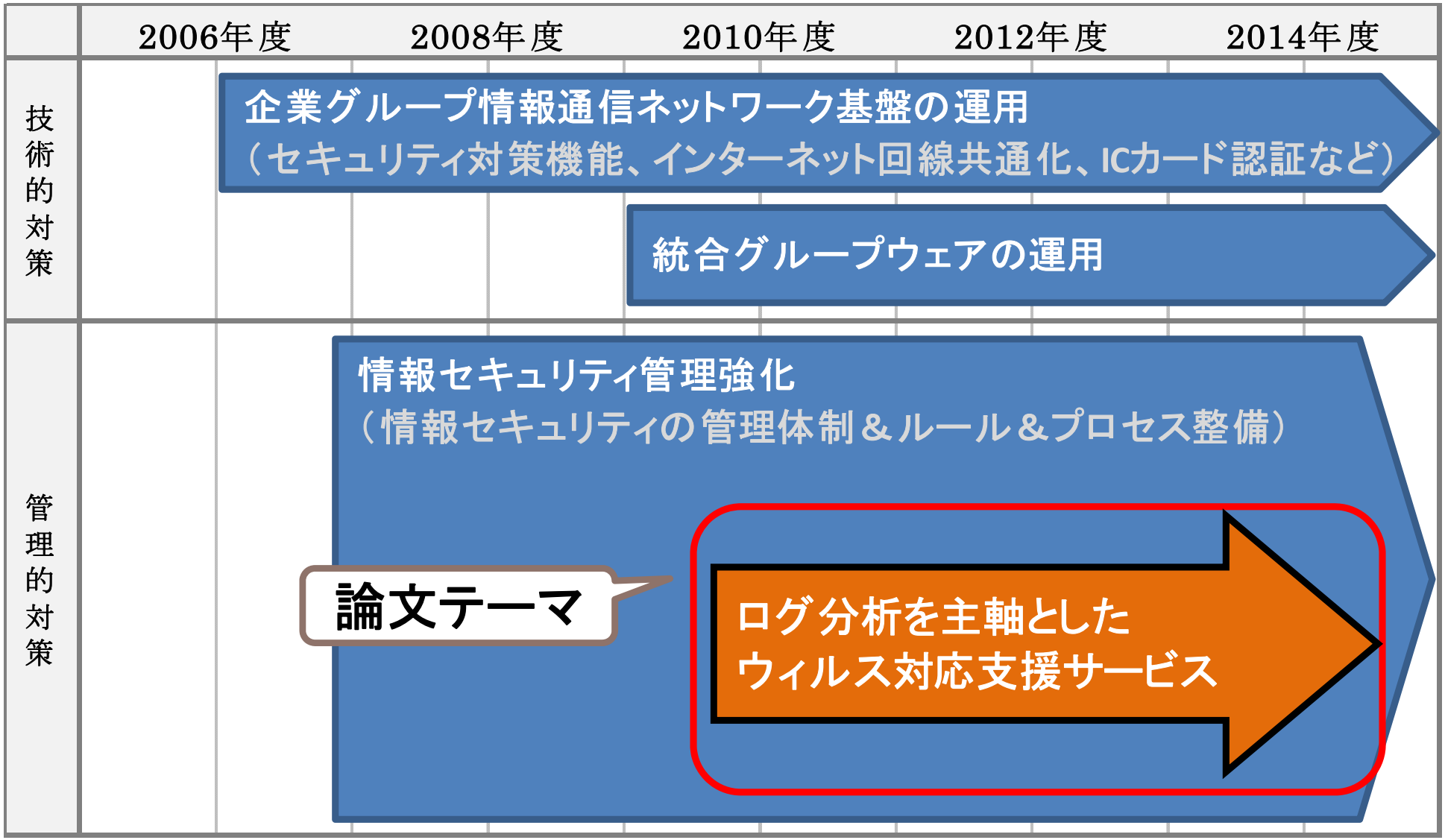
東北電力の業務は企業グループ各社と情報連携
お客様情報や施設情報の安全確保が大前提

＝

東北電力企業グループが一丸となって
情報漏洩対策に取り組む必要がある！

はじめに

1.2 情報セキュリティへの取り組み



※サービス対象…企業グループ32社

- ２．ログ分析を主軸としたサービス

ログ分析を主軸としたサービス

2.1 ウィルス対応は削除したら終わり？

「ウィルス対策ソフトでウィルスを削除すれば、
もう大丈夫、問題ない」

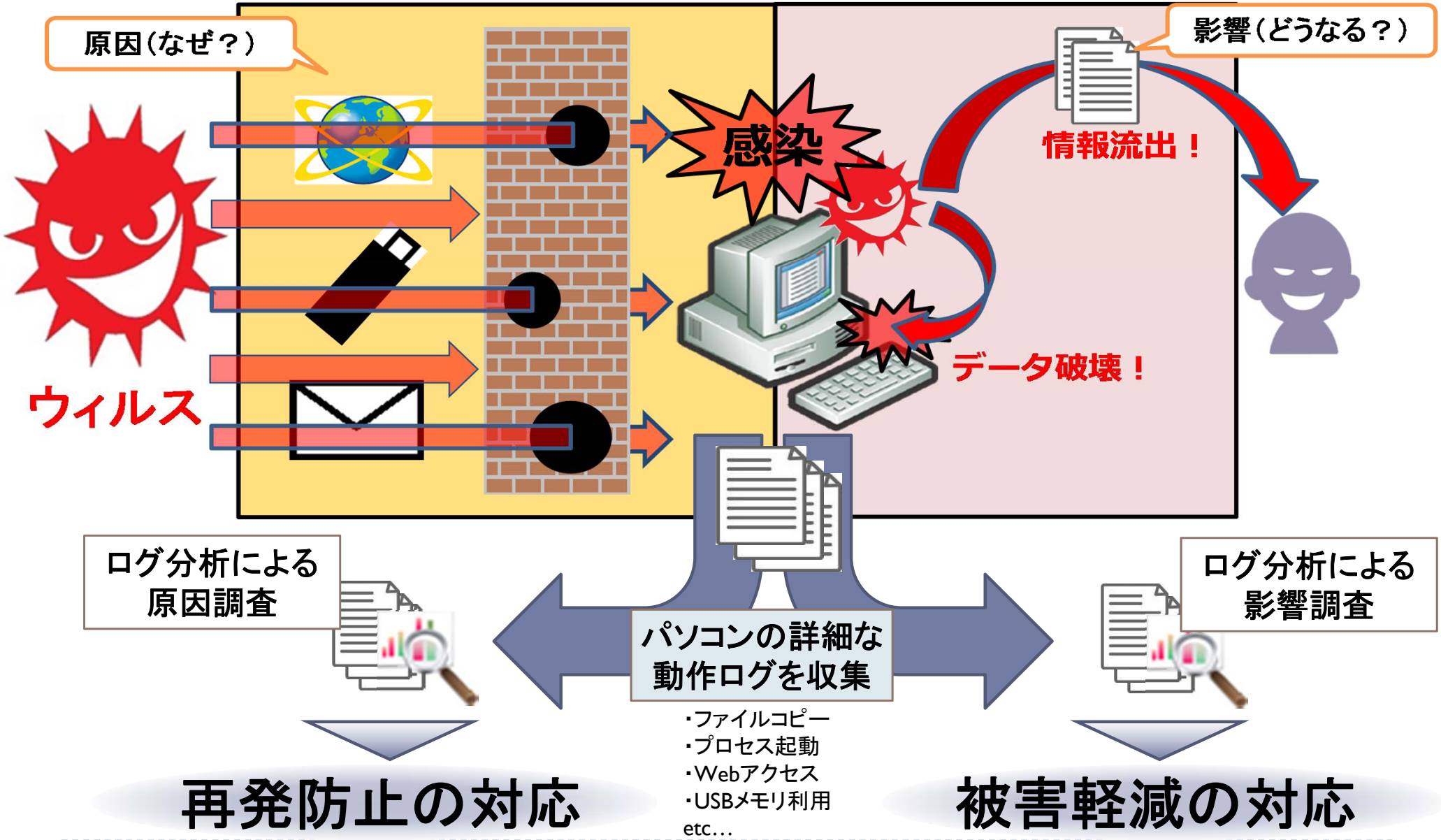
・・・本当に？

家に空き巣が入った場合でも同じことが言えるか？
二度と被害に遭わないよう対策すべきではないか？
何を盗まれたか確認しなくてよいのか？

「**過去**の原因」と「**未来**の影響」を調査して
それぞれのリスクに対応する必要がある！

ログ分析を主軸としたサービス

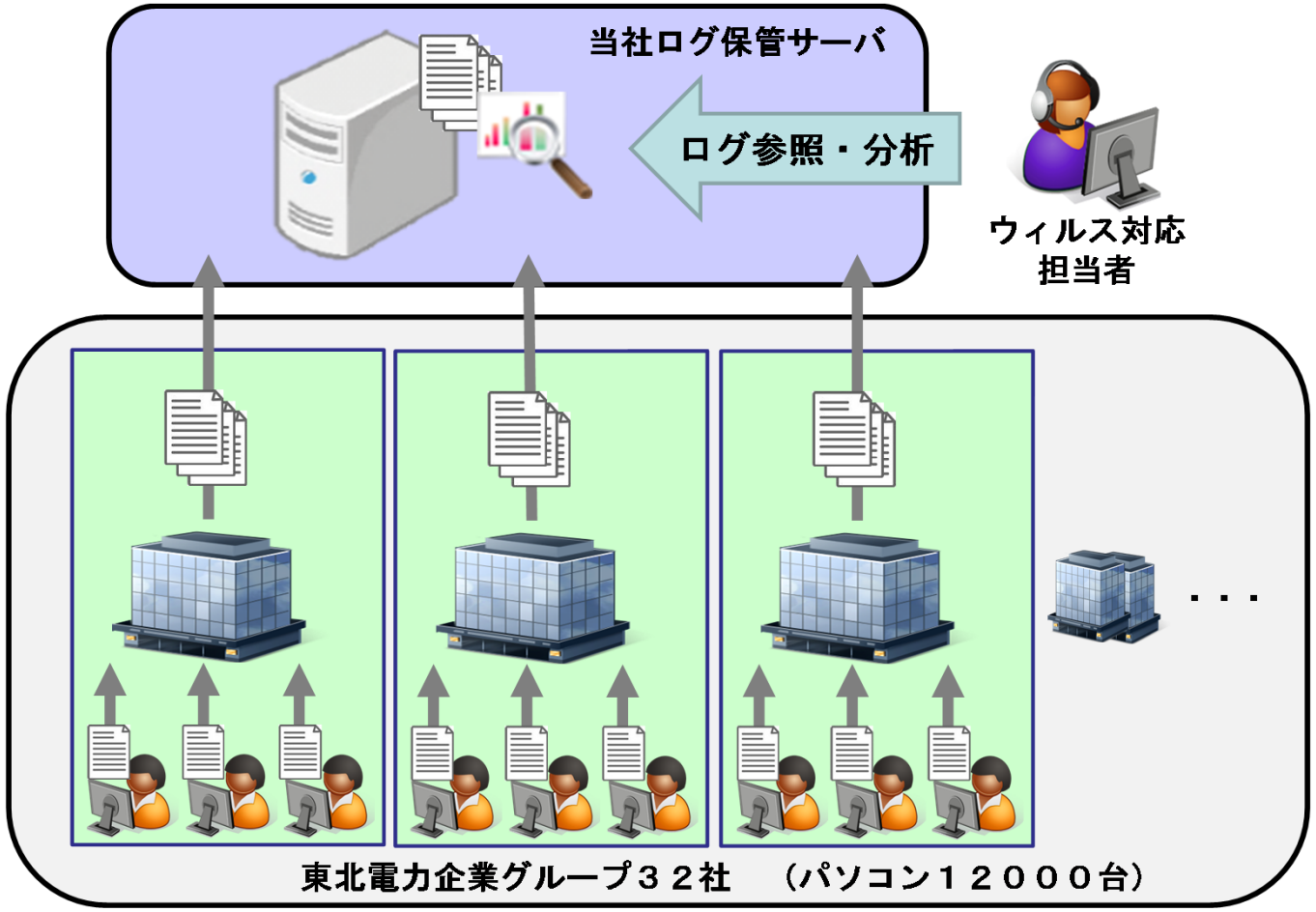
2.2 「過去の原因」と「未来の影響」の調査



ログ分析を主軸としたサービス

2.3 パソコン動作ログ収集の仕組み

1. 企業グループ各社12000台のパソコンにログ収集ツールを導入
2. パソコン動作ログをデータセンターに集約、企業単位で保管
3. ログ検索ツールで必要なログを抽出し、分析



記録可能ログの一部

- パソコン名
- ユーザー名
- ファイル移動元と先
- プロセス起動
- 接続先URL
- 外部媒体接続
- ファイルダウンロード
- ファイルアップロード
- PC起動
- 接続デバイスID
- ウィンドウタイトル

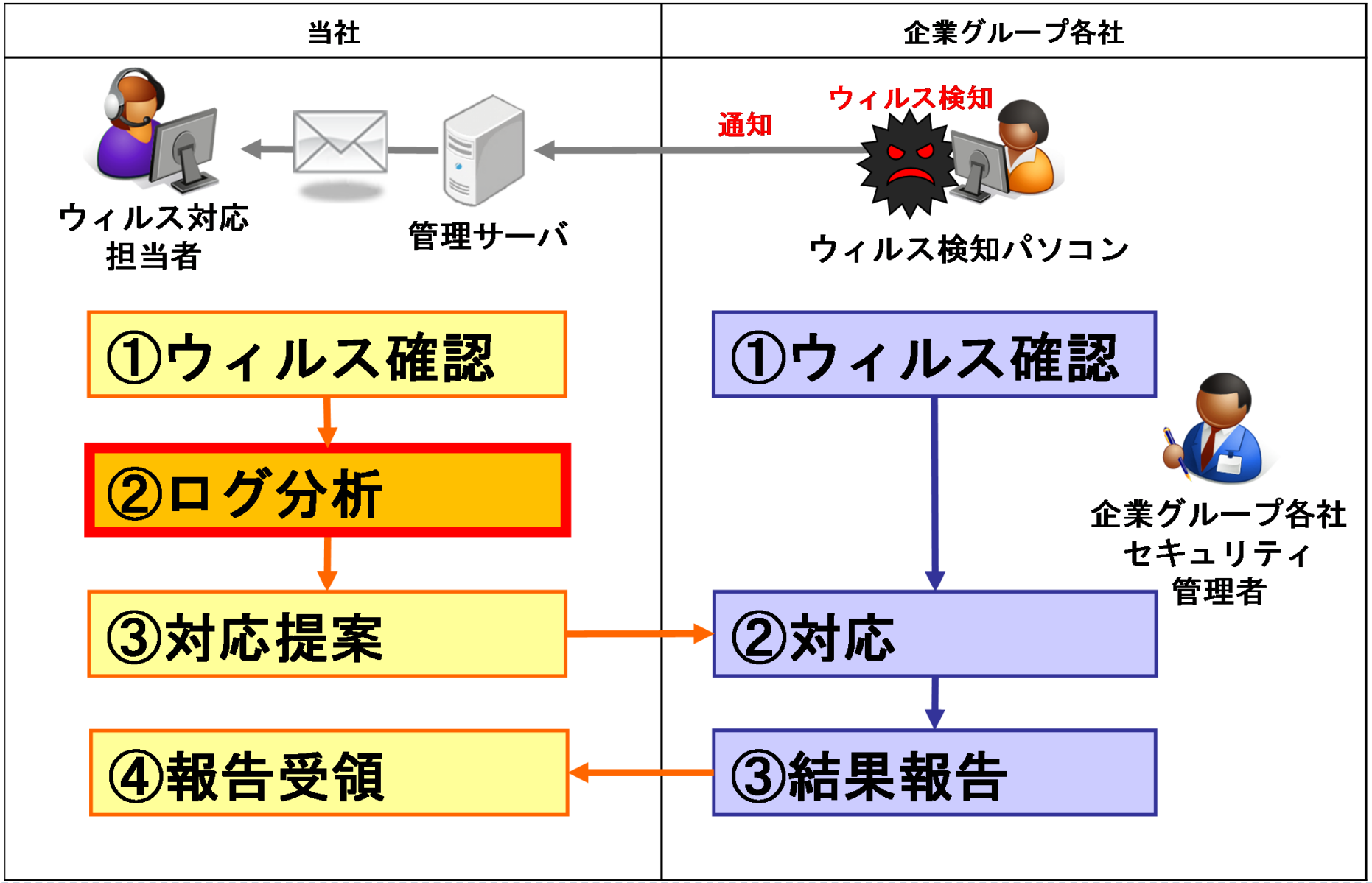
etc…

ログ分析を主軸としたサービス

2.4 パソコン動作ログ収集によるメリット

- **ユーザーが覚えていない情報を記録・調査できる**
  - 詳細な動作内容とその日時、数年前の記録　など
- **ユーザーが認識できない動作を記録・調査できる**
  - 画面表示のない動作、プロセスの起動有無　など
- **企業グループ各社の全パソコンのログを
ユーザーへの負担なく即座に一斉調査できる**
  - 特定の媒体の使用状況、特定プロセスの動作有無　など

ログ分析を主軸としたサービス
2.5 サービスの流れ



- ３．ログ分析の手法とその効果（事例紹介）
  - 事例(1)　Web閲覧で感染するウィルス
  - 事例(2)　有用なツールに偽装するウィルス
  - 事例(3)　外部媒体を経由して感染するウィルス

※事例の中で、WebサイトのURLは加工しています。ご了承ください。

ログ分析の手法とその効果

①状況確認 ▶ ②原因調査 ▶ ③影響調査

3.1 事例(1)Web閲覧で感染するウィルス

- 【第一報】
  - ユーザーがインターネット閲覧中、ウィルス対策ソフトで
    ウィルス「nazzz.exe」を検知した

- 【状況詳細調査】ウィルス検知日時のログ調査
  - [ログ]あるWebサイトに接続した直後にウィルス検知
  - [解析]攻撃者が作成した不正Webサイトと判明
  - [対応]ブラックリスト登録(再発防止)

日時	URL	ファイル名	プロセス	タイトル	操作名
14:41:48	hxxp://nazzz.pw	/index.html	iexplore.exe		接続
14:41:50	C:¥Program Files¥ウィルス	Alert.msg	VirusScan.exe	ウィルス検知	ファイル参照

ログ分析の手法とその効果

3.1 事例(1)Web閲覧で感染するウィルス

- **【原因調査1】検知直前のログ調査**
  - [ログ]不正Webサイト接続の直前、レストランWebサイトに接続
  - [解析]レストランWebサイトから自動再接続の不正コード発見
  - [対応]ブラックリスト登録(再発防止)

原因1

日時	URL	ファイル名	プロセス	タイトル	操作名
14:39:26	hxxp://search.yahoo.co.jp	/search;_ylt=A	iexplore.exe	Yahoo!検索	アクティブウィンドウ
14:41:38	hxxp://karymax.to	/index.html	iexplore.exe	カレー料理レストラン　X市	接続
14:41:48	hxxp://nazzz.pw	/cgi/diarypro	iexplore.exe		接続
14:41:50	C:¥Program Files¥ウィルス	Alert.msg	VirusScan.exe	ウィルス検知	ファイル参照

- **【原因調査2】ユーザーのWeb閲覧目的のヒアリング**
  - [調査]私的な目的でインターネット閲覧していた
  - [対応]私的利用を控えるよう注意指導(再発防止)

原因2

ログ分析の手法とその効果

①状況確認 ▶ ②原因調査 ▶ **③影響調査**

3.1 事例(1)Web閲覧で感染するウィルス

- **【影響調査1】レストランWebサイトのウィルス調査**
  - [解析]不正Webサイトに自動で再接続する機能だけを持つ
  - [判断]動作したが、情報漏洩リスクはない

影響なし

- **【影響調査2】不正Webサイトのウィルス調査**
  - [解析]不正Webサイトに接続するとウィルスが起動する
  - [解析]接続の瞬間に検知、ウィルスプロセス起動なし
  - [判断]動作しておらず、情報漏洩リスクはない

影響なし

日時	URL	ファイル名	プロセス	タイトル	操作名
14:41:48	hxxp://nazzz.pw	/index.html	iexplore.exe		接続
14:41:50	C:¥Program Files¥ウィルス	Alert.msg	VirusScan.exe	ウィルス検知	ファイル参照

ログ分析の手法とその効果

3.2 事例(2)有用なツールに偽装するウィルス

- 【第一報】
  - ユーザーがパソコンを起動した直後、ウィルス対策ソフトでウィルス「pennybee.exe」を検知した

- 【状況詳細調査】ウィルス検知日時のログ調査
  - [ログ]ウイルス対策ソフトの更新直後に検知
  - [推測]過去侵入していたウィルスを、更新で検知可能となった

日時	フォルダ名	ファイル名	プロセス	タイトル	操作名
8:30:56					Windows起動
8:32:15	C:¥Program Files¥ウィルス対策ソフト	ptn.120605	VirusScan.exe	ウィルス対策ソフト	ファイル更新
8:34:18			pennybee.exe		プロセス起動
8:34:19	C:¥Program Files¥ウィルス対策ソフト	Alert.msg	VirusScan.exe	ウィルス検知	ファイル参照

ログ分析の手法とその効果

3.2 事例(2)有用なツールに偽装するウィルス

- **【原因調査1】ウィルスのプロセス名で過去ログ調査**
  - [ログ]「FileOpener」インストール中にウィルス初起動
  - [ログ]同時に「BaiduIME」を自動でインストール
  - [対応]DL元URLをブラックリスト登録（再発防止）

原因1

日時	URL	ファイル名	プロセス	タイトル	操作名
18:52:28	fileopener.com	/file-opener/gb/oc/?adr	iexplore.exe	ダウンロード	アクティブウィンドウ
18:52:55	C:¥Documents and	FileOpenerSetup.exe	iexplore.exe	名前を付けて保存	アクティブウィンドウ
18:53:11	C:¥Documents and	FileOpenerSetup.exe	FileOpenerSetup.exe	fo Installer	プロセス起動
18:53:56			BaiduJP_Setup.exe	Baidu IME Installer	プロセス起動
18:54:12			pennybee.exe		プロセス起動

- **【原因調査2】ツール導入の会社許可有無をヒアリング**
  - [調査]会社が非許可のツールを無断導入したと判明
  - [対応]会社で許可されたソフトを利用するよう指導（再発防止）

原因2

①状況確認 ▶ ②原因調査 ▶ ③影響調査

ログ分析の手法とその効果

3.2 事例(2)有用なツールに偽装するウィルス

- **【影響調査1】pennybeeの調査**
  - [解析]頻繁に広告表示、有償製品の購入を促す　影響なし
  - [判断]動作したが、情報漏洩リスクはない
- **【影響調査2】FileOpenerの調査**
  - [解析]様々な拡張子に対応と偽りインストールさせようとする
  - [解析]pennybeeとBaiduIMEを同時にインストールする　影響なし
  - [解析]頻繁に広告表示、有償製品の購入を促す
  - [判断]動作したが、情報漏洩リスクはない
- **【影響調査3】BaiduIMEの調査**
  - [解析]キー入力を外部サーバに送信する　影響あり
  - [判断]IDやパスワードが漏洩したおそれあり
  - [対応]Webサービス利用有無確認＆パスワード変更

ログ分析の手法とその効果

3.3 事例(3)外部媒体を経由して感染するウィルス

- 【第一報】
  - ユーザーがパソコンを起動した直後、ウィルス対策ソフトでウィルス「DriveVR.exe」を検知した

- 【状況詳細調査】ウィルス検知日時のログ調査
  - [ログ]ウイルス対策ソフトのアップデート後に検知
  - [判断]過去侵入していたウィルスを、更新で検知可能となった

日時	フォルダ名	ファイル名	プロセス	タイトル	操作名
8:19:06					Windows起動
8:20:35	C:¥Program Files¥ウィルス対策ソフト	ptn.111111	VirusScan.exe	ウィルス対策ソフト	ファイル更新
8:24:01			DriveVR.exe		プロセス起動
8:24:02	C:¥Program Files¥ウィルス対策ソフト	Alert.msg	VirusScan.exe	ウィルス検知	ファイル参照

ログ分析の手法とその効果

3.3 事例(3)外部媒体を経由して感染するウィルス

- 【原因調査1】ウィルスのプロセス名で過去ログ調査
  - [ログ]検知日の一ヶ月前、USBメモリ接続でウィルス初起動
  - [対応]USBメモリ初期化（再発防止）

原因1

日時	フォルダ名	ファイル名	プロセス	タイトル	操作名	デバイスID
15:23:12	E:		Explorer.EXE	リムーバブル ディスク (E:)	USB接続	USB¥VID_099D&PID_0123¥1A23456789012[Sony Storage Media USB Device]
15:23:14	E:¥	DriveFix.exe	Explorer.EXE		ファイル参照	
15:23:14	C:¥	DriveFix.exe	Explorer.EXE		ファイル参照	
15:23:14			DriveVR.exe		プロセス起動	

※検知日から一ヶ月前のログ

- 【原因調査2】USBメモリ所有者のヒアリング
  - [調査]取引先から借用したUSBメモリと判明

原因2

  - [対応]取引先への注意喚起（再発防止）

ログ分析の手法とその効果

3.3 事例(3)外部媒体を経由して感染するウィルス

- **【影響調査2】DriveVR.exeのウィルス調査**
  - [解析]外部媒体経由で他パソコンに感染を拡大する
  - [ログ]複数のパソコンと外部媒体で感染の痕跡を発見
  - [対応]感染したパソコンと媒体を初期化

影響あり

感染パソコン名	感染日時
TAKE-PC05	01/0
TAKE-PC04	01/2
TAKE-PC07	01/2
TAKE-PC02	02/0
TAKE-PC18	02/0
MATU-PC03	02/0
TAKE-PC01	02/0

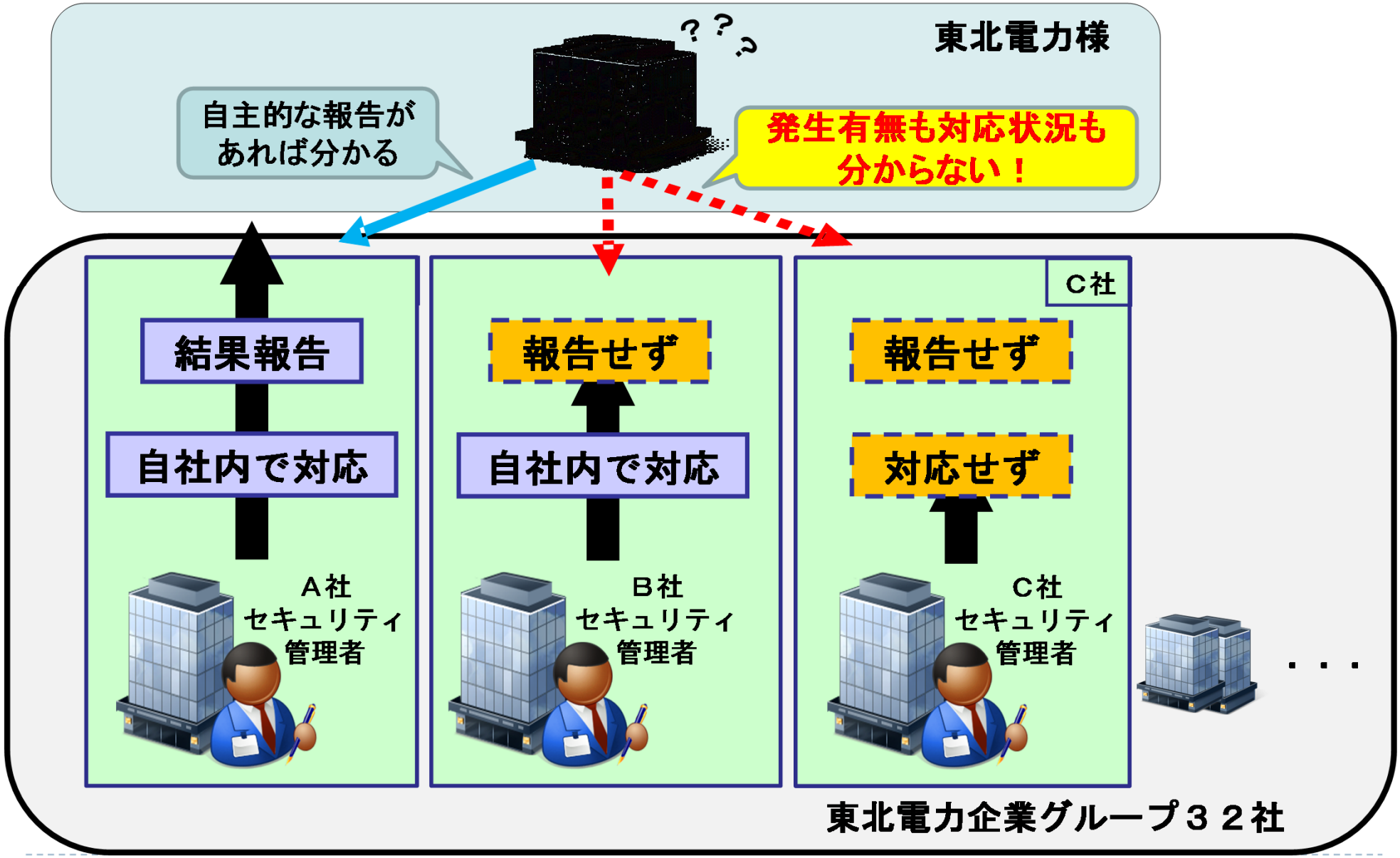
感染媒体種別	デバイスID
[Sony Storage Media USB Device]	VID_099C&PID_0123¥5A12345678901
[Sony Storage Media USB Device]	VID_099C&PID_0123¥5A34567890123
[Sony Storage Media USB Device]	VID_099C&PID_0123¥5A56789012345
[Sony Storage Media USB Device]	VID_099C&PID_0123¥5A78901234567
[Sony Storage Media USB Device]	VID_099C&PID_0123¥5A90123456789
[Sony Storage Media USB Device]	VID_099C&PID_0123¥5A01223344455
[USB2.0 Mobile Disk USB Device]	VID_126F&PID_0163¥3F98877766665

- **【影響調査2】DriveVR.exeのウィルス調査**
  - [解析]ウィルスはオンラインゲームのIDとパスワードを窃取する
  - [判断]動作したが、情報漏洩リスクはない

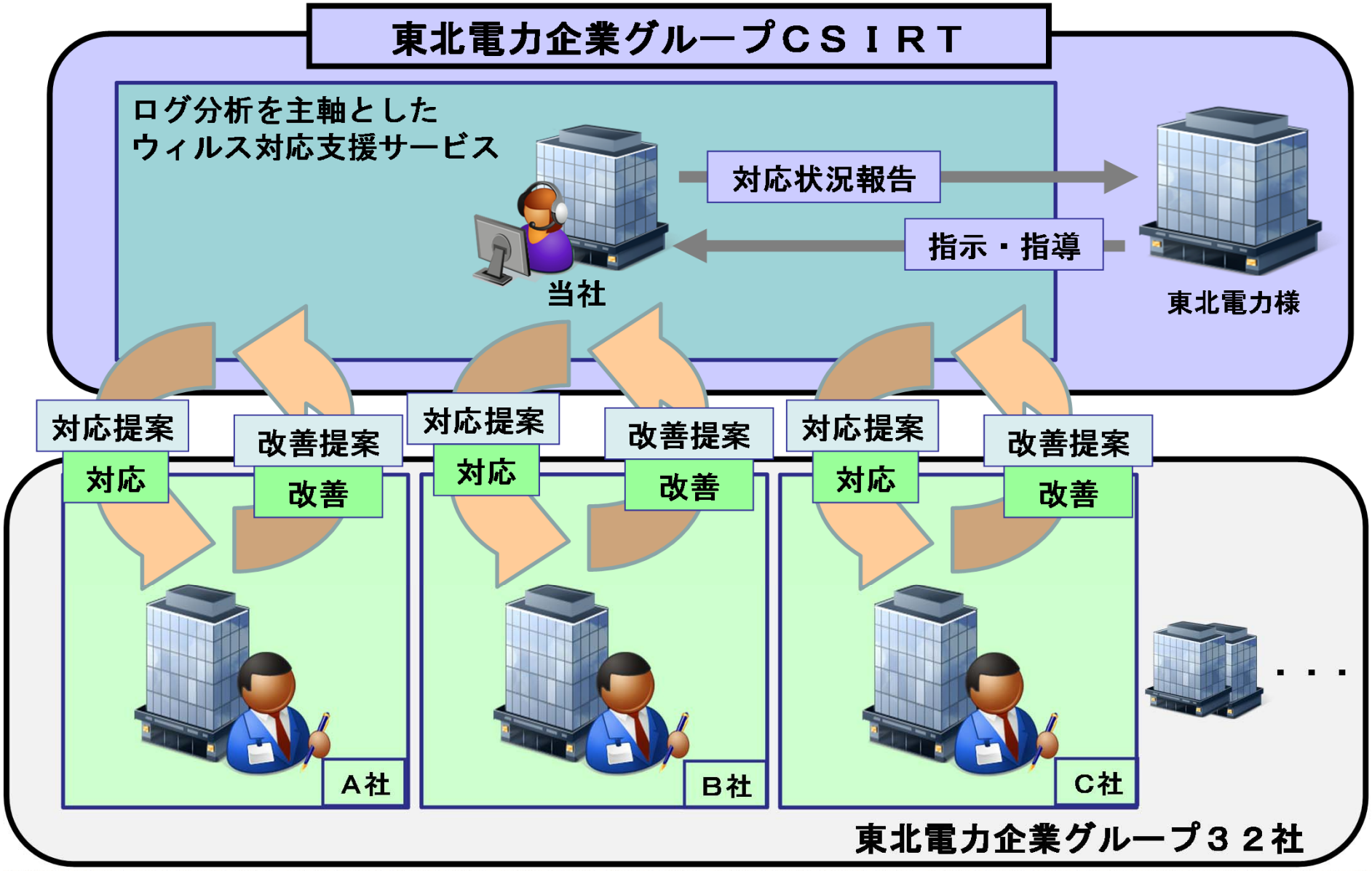
影響なし

４．成果と課題

成果と課題
4.1 サービス提供前の状況



成果と課題
4.2 サービス提供後の状況



※CSIRT…Computer Security Incident Response Team

4.3 成果と課題

成果
1. ウィルス感染の原因解明＆的確な対策で被害を抑制
2. 企業グループ全体で高水準なウィルス対応体制
3. 各社に専門スキルを持つ人材を配置するコストを削減

しかし・・・

なくならない！

- 全文英語のスパムメールを開いてウィルス感染
- 怪しいフリーソフトをインストールしてウィルス感染

課題
ユーザーひとりひとりのセキュリティ意識の向上

おわりに

パソコンに侵入したウィルスは、
検知・削除されるまでの間に様々な悪事を
働いているおそれがあります。

放置し、数年後に発覚して
大きなコストを支払うか？

適切に対応し、被害を
最小限に食い止めるか？

真のウィルス対応は、
ウィルスを削除した時から始まる。