SPAMSNIPER AG

多様化するメールセキュリティのリスクに強固な対策！
標的型攻撃にも有効なメール無害化

基盤・セキュリティソリューション事業本部
基盤・セキュリティソリューション企画センター
企画部　長谷川 隼也

2017年9月22日

Canon
キヤノン ITソリューションズ株式会社

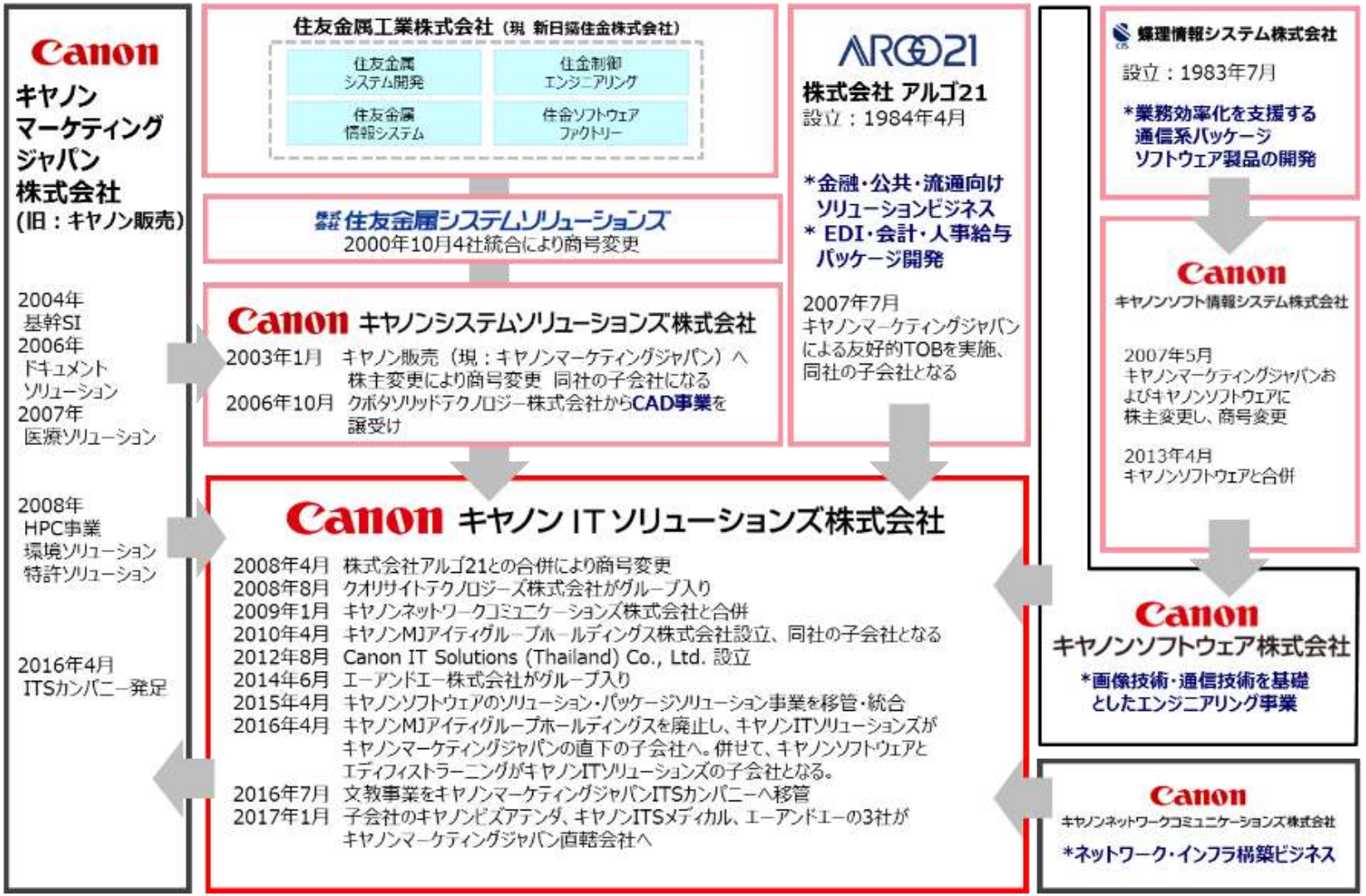
アジェンダ

- キヤノンITソリューションズについて
- 基盤・セキュリティ事業について
- メールセキュリティについて
- メール無害化について
- SPAMSNIPER AGについて
- キャンペーンおよび本日の特典
- 参考（Jiransoft社について）

キヤノンITソリューションズについて

沿革

（2017年1月1日現在）



キヤノングループでの位置づけ

ITソリューションの事業領域

基盤・セキュリティ

EDI

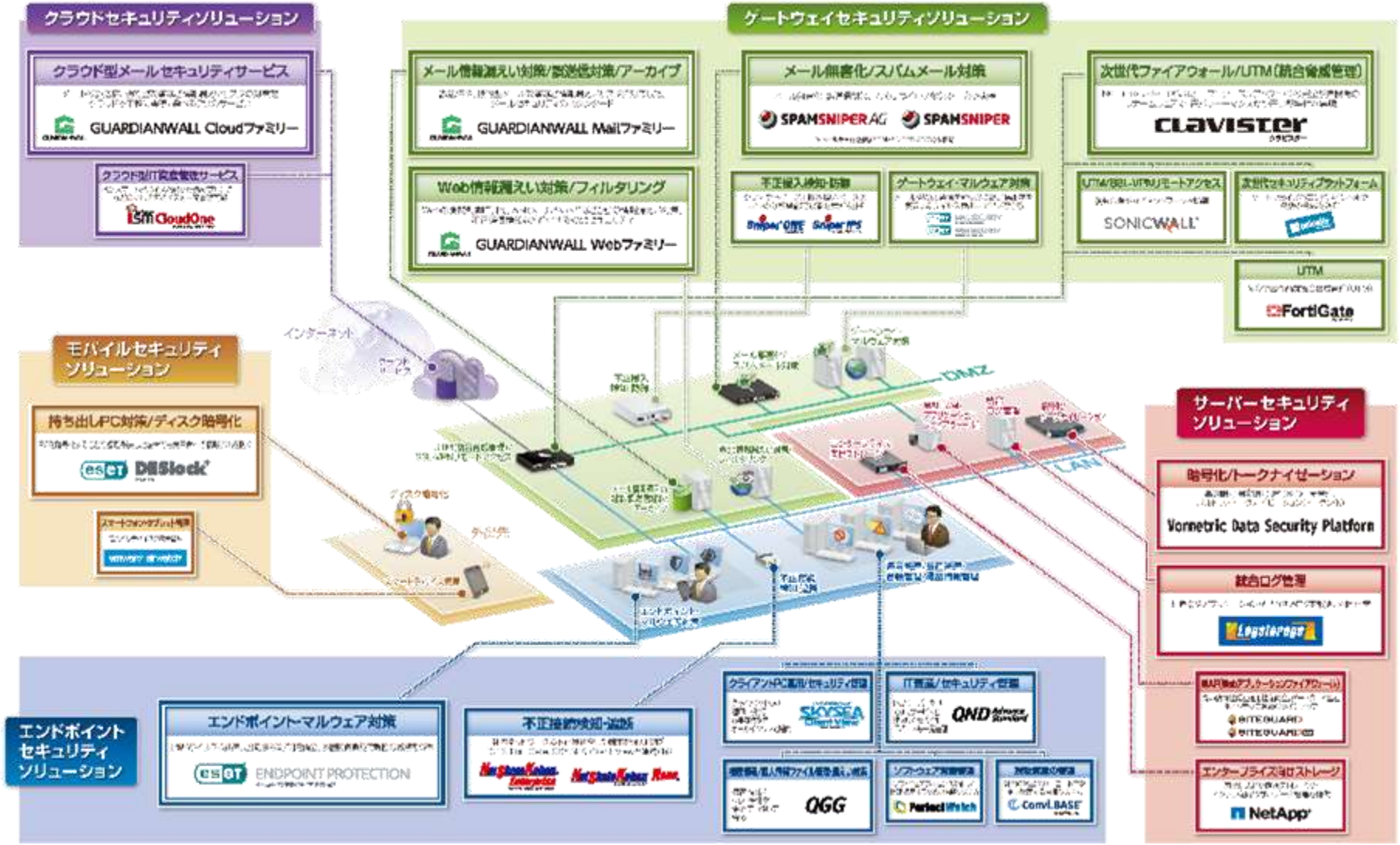
DTP

特許管理

画像処理

基盤・セキュリティ事業について

当社セキュリティソリューションマップ



主なプロダクト・サービス

●セキュリティプロダクト

メール無害化/スパムメール対策

SPAMSNIPER AG

メール誤送信対策/情報漏えい対策/メールアーカイブ

15年連続国内シェアNo1*

GUARDIANWALL

（*） 株式会社富士キメラ総研2016ネットワークセキュリティビジネス調査総覧より

次世代ファイアーウォール/UTM（総合脅威管理）

CLAVISTER

エンドポイント・マルウェア対策

eset ENDPOINT PROTECTION

不正接続検知・遮断

NetSkateKoban

エンタープライズ暗号化ソリューション

Vormetric

●システム基盤構築サービス

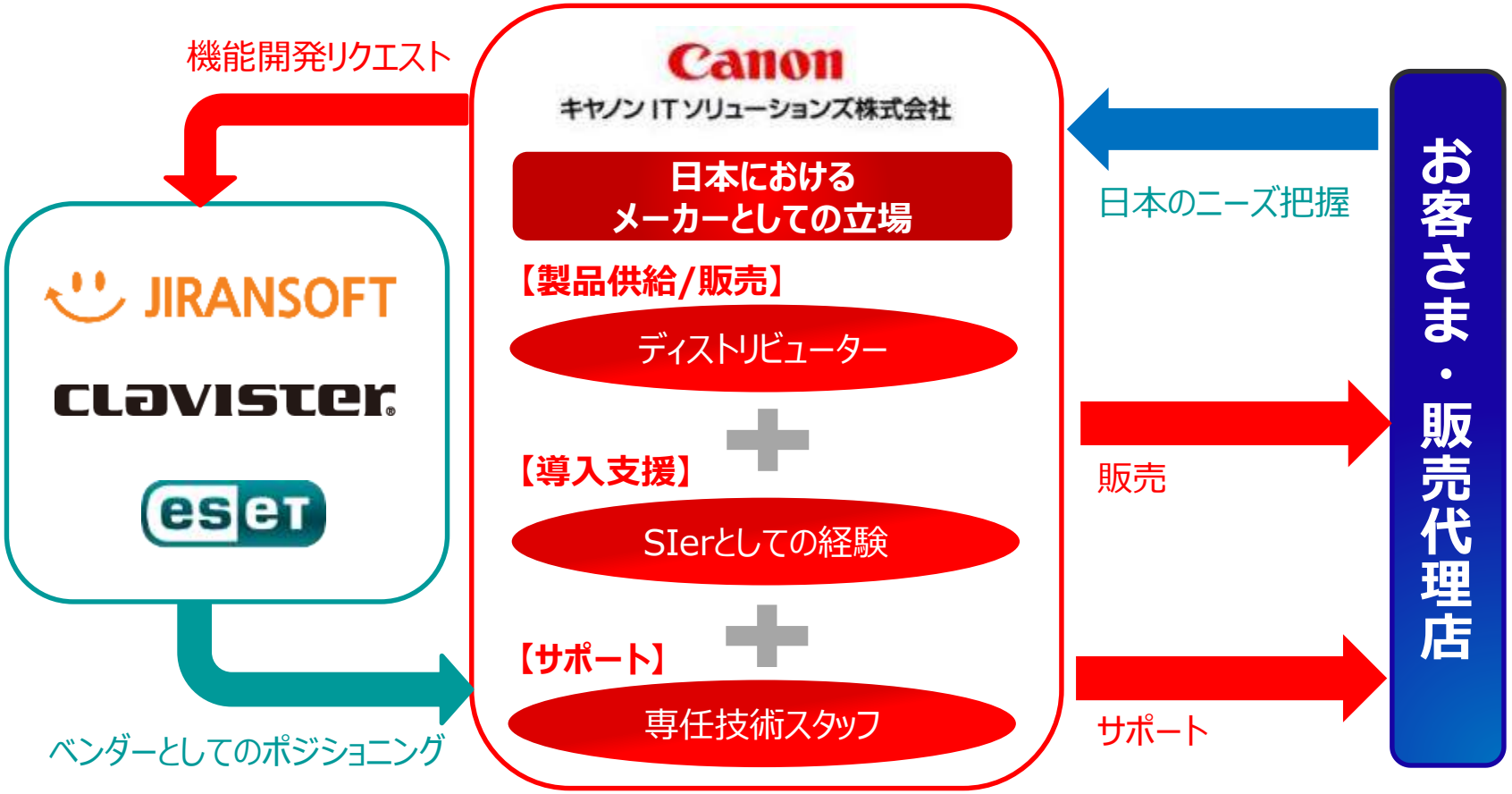
統合プラットフォーム	運用基盤	ネットワーク
仮想化	バックアップ	災害対策

提案 → 要件定義 → 設計 → 開発テスト → 導入 → 運用 → 保守

●プロダクトサポートサービス

- Storage
  EMC
- NW
  F5・PaloAlto・Cisco・FortiGate
- DB
  Oracle・Postgre SQL・SQL Server
- Backup Tools
  NetVault・NetBackup・vRanger
- IT Asset Managment
  QND・SKYSEA

当社の役割り

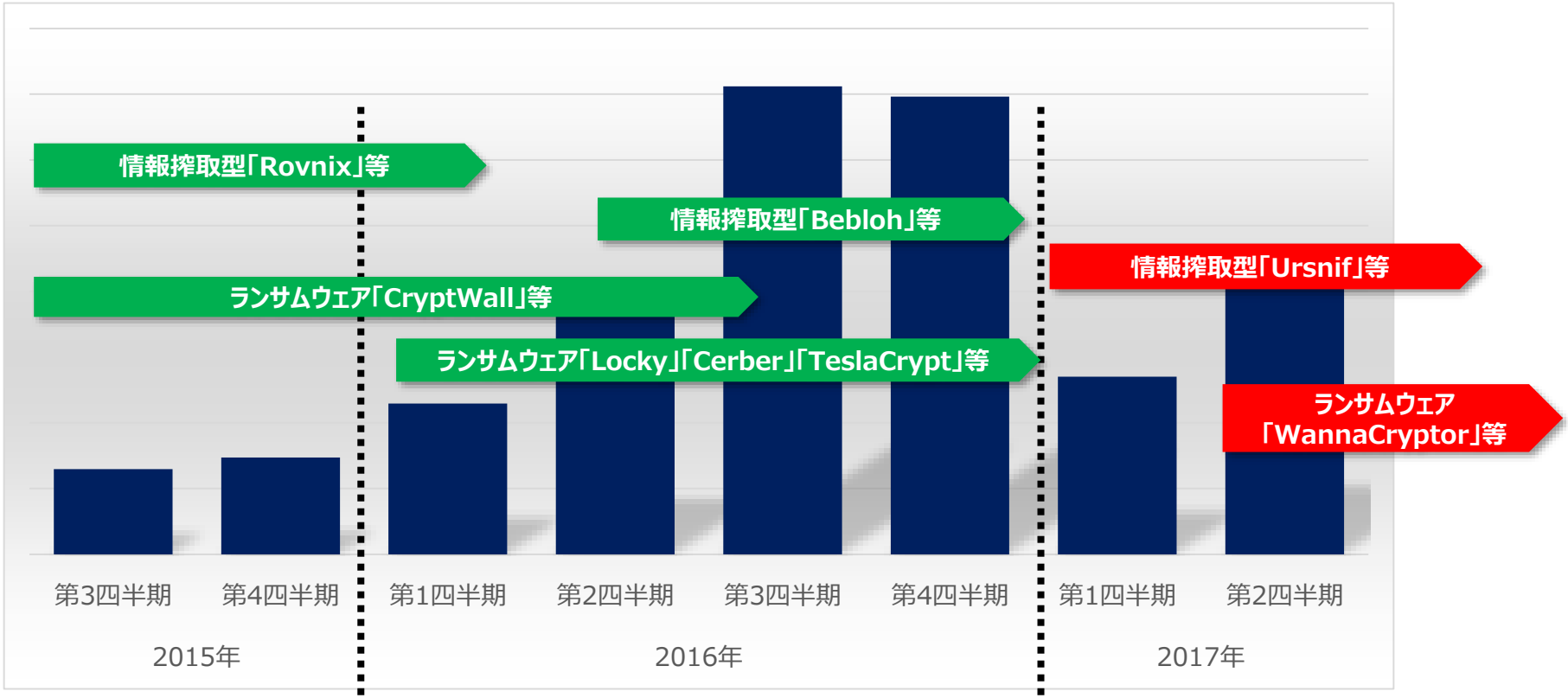


SIerとして培ってきた経験を生かし、国内外のベンダーと連携し、
日本のビジネス環境に合った最適なソリューションを提供する

メールセキュリティについて

2017年上半期　国内検出状況　四半期別

新種の情報搾取型マルウェアやランサムウェアが発生



※本データは、ESET LiveGrid データベースより、全マルウェアより国内で検出した2015年7月～2017年6月までの総検出数を表示したものです。

2017年上半期　国内検出マルウェア上位10種

順位	ESET製品の検出名	マルウェアの役割
1	JS/Danger.ScriptAttachment	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。
2	JS/TrojanDownloader	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。
3	PDF/TrojanDropper.Agent	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。
4	VBA/TrojanDownloader	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。
5	Win32/Kryptik	情報搾取を目的としており、主にインターネットバンキングなどのアカウント情報を狙う
6	Win32/Toolbar	主にブラウザアドインプログラム（ツールバー）に個人情報等送信するプログラムが組み込まれている
7	JS/Danger.DoubleExtension	二重拡張子を施したファイル名が設定されており、このファイルを開くことで主に他のマルウェアをダウンロードする
8	Win32/Spy.Ursnif	情報搾取を目的としており、主にインターネットバンキングなどのアカウント情報を狙う
9	HTML/FakeAlert	ブラウザ上で偽の警告画面を表示し、金銭支払などを行わせる
10	PowerShell/TrojanDownloader	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。

上位は、メール経由による「ダウンローダ」による侵入が多くを占めます。

※本データは、ESET LiveGrid データベースより、全マルウェアより国内で検出した2017年1月～2017年6月までの総検出数から順位付けしたものです。

2017年上半期　国内検出マルウェア上位10種

順位	ESET製品の検出名	マルウェアの役割
1	JS/Danger.ScriptAttachment	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。
2	JS/TrojanDownloader	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。
3	PDF/TrojanDropper.Agent	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。
4	VBA/TrojanDownloader	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。
5	Win32/Kryptik	情報搾取を目的としており、主にインターネットバンキングなどのアカウント情報を狙う
6	Win32/Toolbar	主にブラウザアドインプログラム（ツールバー）に個人情報等送信するプログラムが組み込まれている
7	JS/Danger.DoubleExtension	二重拡張子を施したファイル名が設定されており、このファイルを開くことで主に他のマルウェアをダウンロードする
8	Win32/Spy.Ursnif	情報搾取を目的としており、主にインターネットバンキングなどのアカウント情報を狙う
9	HTML/FakeAlert	ブラウザ上で偽の警告画面を表示し、金銭支払などを行わせる
10	PowerShell/TrojanDownloader	他のマルウェアをダウンロードする。ダウンロードされるマルウェアは主にランサムウェア、情報搾取型マルウェアなど。

背景黄色のマルウェアの侵入手段は、メールの添付ファイルより検出されています。

※本データは、ESET LiveGrid データベースより、全マルウェアより国内で検出した2015年7月～2017年6月までの総検出数を表示したものです。

メール攻撃に係る主流のマルウェア感染の特徴

①ZIPファイルをメールに添付し送り付けます。このZIPファイルには、DOCファイルが圧縮されています。

②ZIPファイルを展開後、DOCファイルに関連付けられたWordが起動すると、画面上ではマクロ機能を有効にするようメッセージが書かれています。

③本命のマルウェアがダウンロードされ発症

※弊社マルウェアラボの調査にて、特に多く確認された特徴を取り上げていますが、すべてのメール攻撃がこれ該当するものを示しているものではありません。

PDFファイルを使ったマルウェア感染の特徴

①PDFファイルを関連付けられたビューアで開くと、添付ファイルも自動的に開く処理が行われます。

②添付ファイルの正体は、DOCファイルに関連付けられたWordが起動すると、画面上ではマクロ機能を有効するようメッセージが書かれています。

③本命のマルウェアがダウンロードされ発症

注：上記の画面では、ランサムウェア「Locky」亜種による感染例をもとに説明しています。
補足：ESET製品で、上記Word形式ファイルの方で検出した場合は、VBA/TrojanDownloaderで検出されます。

※本解析は弊社マルウェアラボにて、該当のファイルを解析した結果をもとに記載しています。

メール利用でこんな経験ございませんか？

外部からの攻撃による被害

- スパム・ウイルス
- ランサムウェア
- 標的型攻撃

うっかりで発生するメールの誤送信

- 宛先 間違え
- 敬称・会社名 間違え
- 書きかけのメールを送信

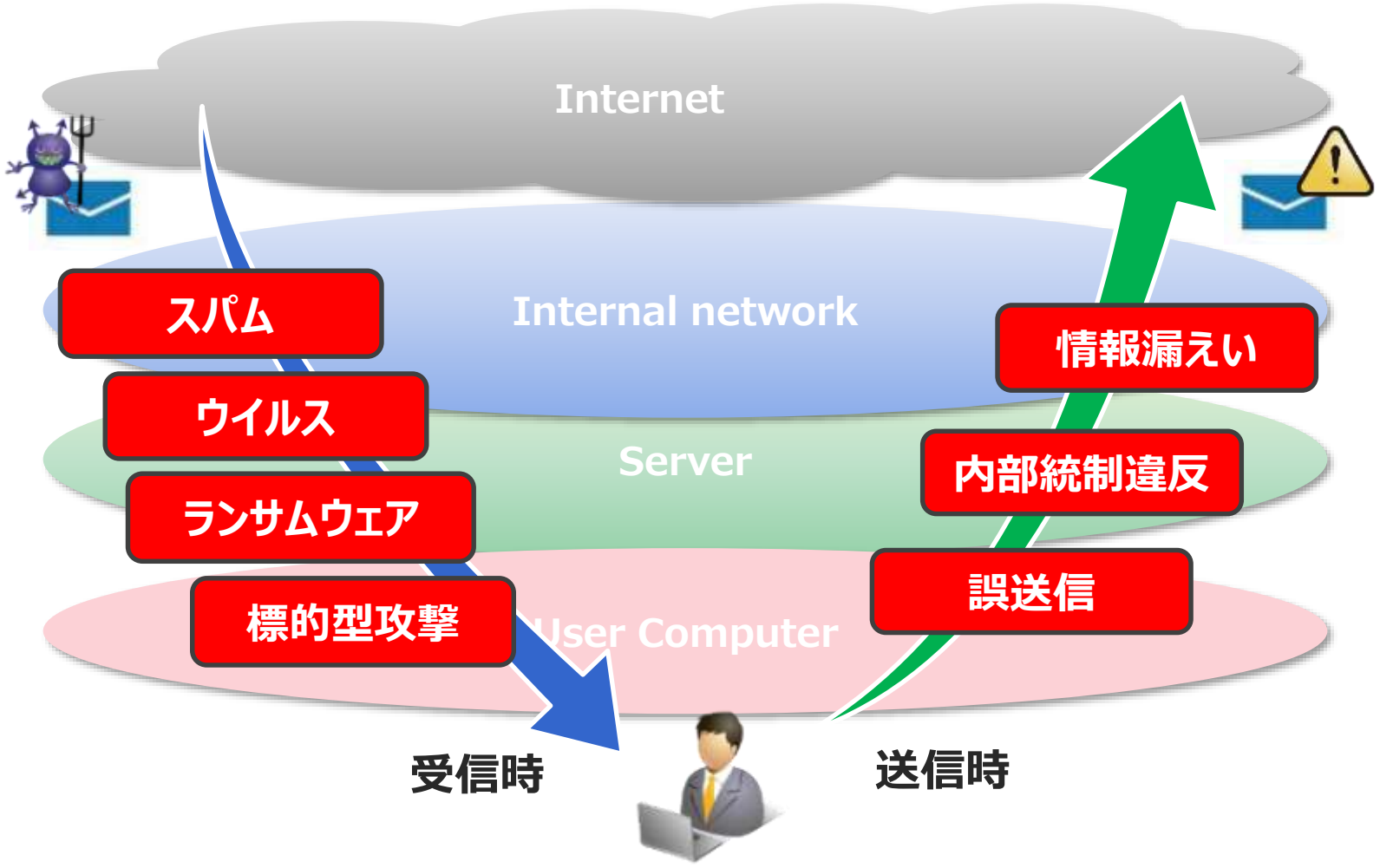
情報漏えいにつながる重大なミス

- BccをToに間違えた
- 添付ファイルを間違えた

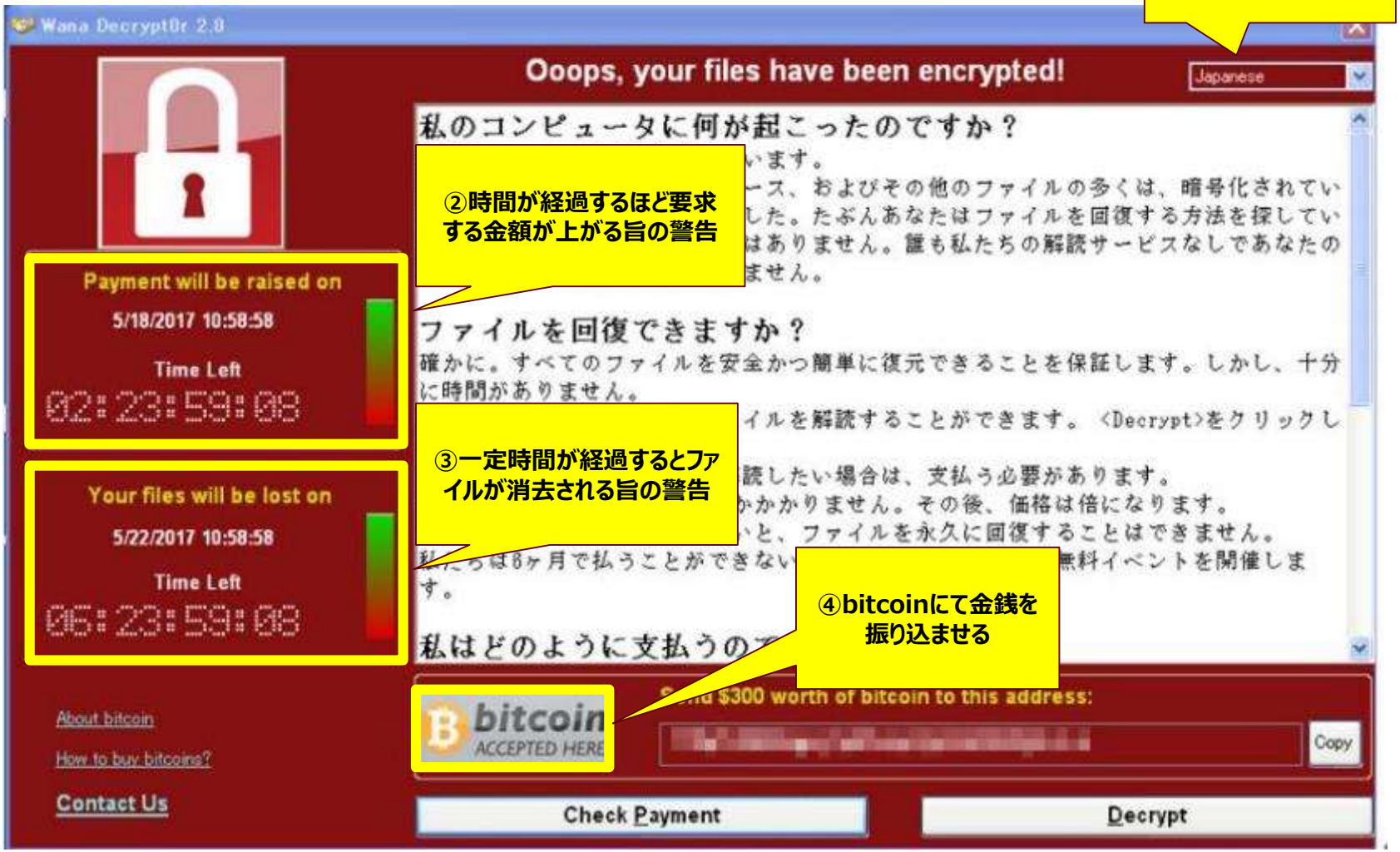
内部統制違反（故意または知らずに）

- 機密情報のメール送信
- 個人情報のメール送信
- 私的メール利用

メールに含まれるセキュリティリスク



ランサムウェア：Wanna Cryptor



図：感染した場合に表示される画面の一例　　出展：https://eset-info.canon-its.jp/malware_info/news/detail/170517.html

どういった対策が必要か

意識改革

情報セキュリティ・ポリシー策定・実践
従業員に対する教育
ITセキュリティ対策室の設置

＋

システム導入

スパム・ウイルス・ランサムウェア
標的型攻撃・誤送信防止
アーカイブ（監査・抑制・有事対応）

当社製品・ソリューションが自信をもって支援します！

メールセキュリティ対策製品・ソリューション

SPAMSNIPER AG

スパム・ウイルス対策　メール無害化　誤送信防止

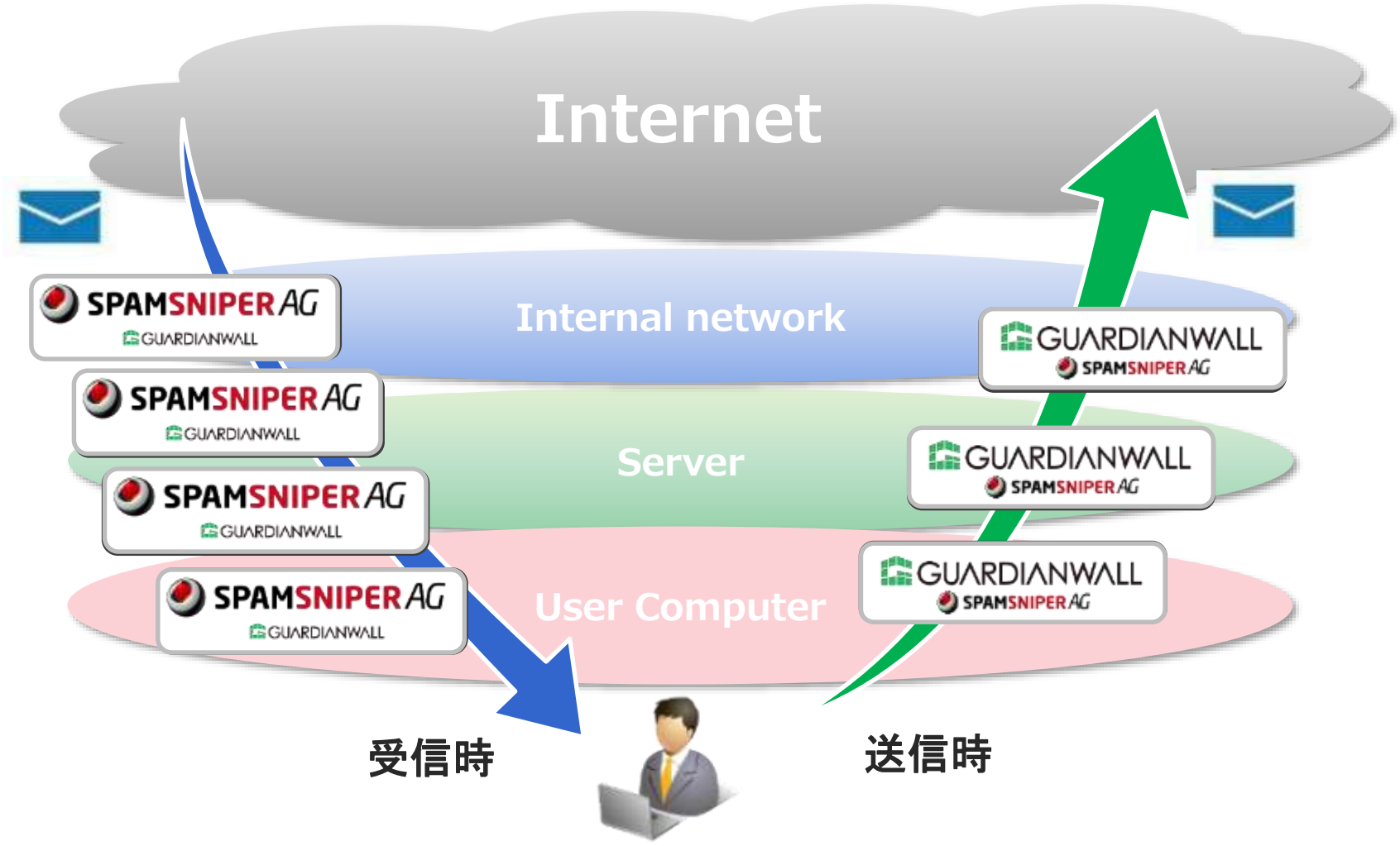
主に**受信時**の対策に有効

GUARDIANWALL

フィルタリング　アーカイブ　誤送信防止

主に**送信時**の対策に有効

メールに含まれるセキュリティリスク（再び）



メール無害化について

メール無害化機能

メール無害化とは、メールの本文および添付ファイルを
安全に扱うよう複数の処理を行うことです。

１．添付ファイル付きメール・HTMLメールの遮断
添付ファイル付きメールやHTMLメールを強制的に遮断

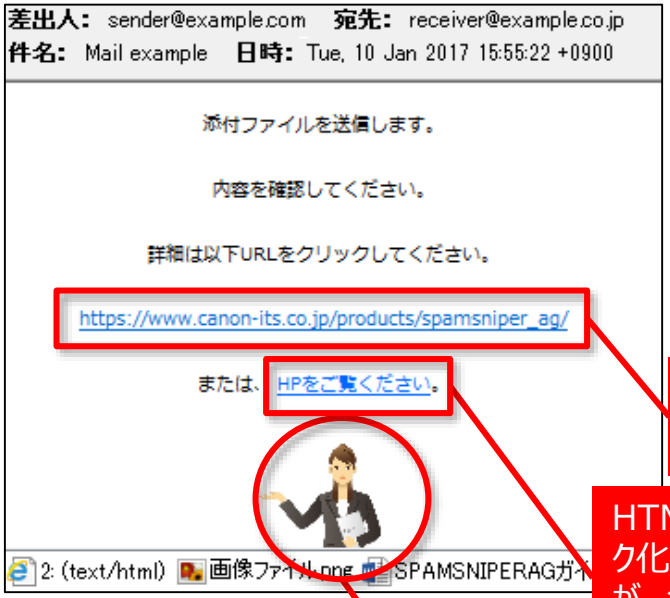
２．添付ファイルの削除
メールの添付ファイルを強制的に削除し、未知のウイルスの侵入を防止する

３．HTML メールのテキスト化
HTMLメールを強制的にテキスト化しURLリンクを除去

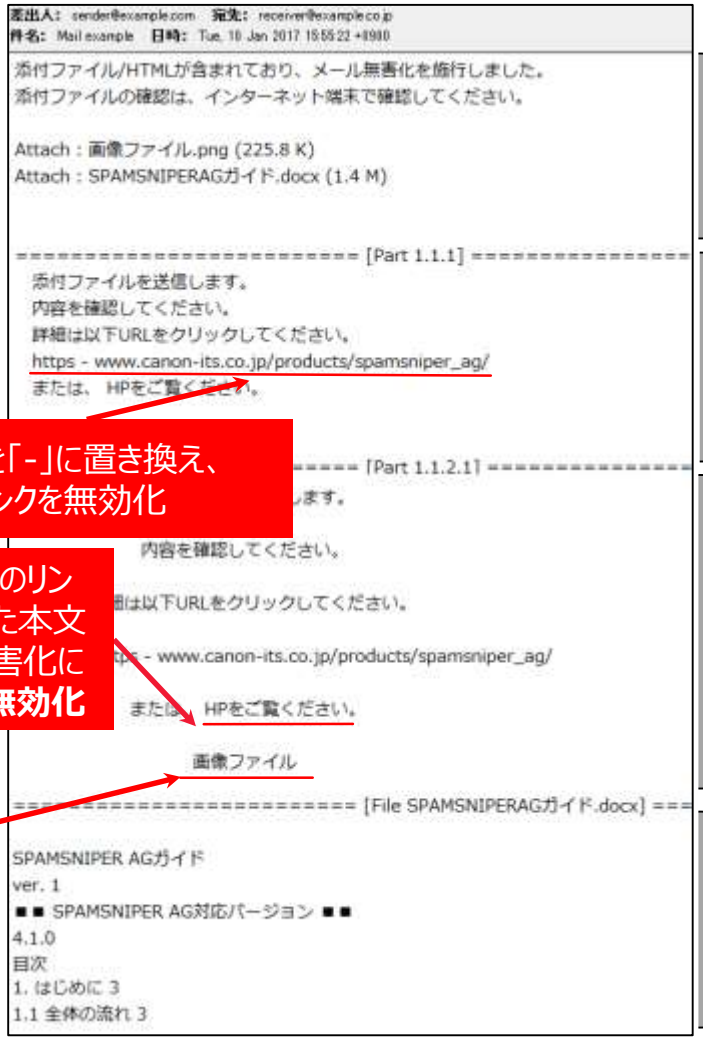
４．原本メールの保管
無害化されていないメール原本を指定のサーバに転送し保管します

無害化されたメールのイメージ

受信メール（無害化前）



受信メール（無害化後）



「://」を「-」に置き換え、URLリンクを無効化

HTMLメールのリンク化されていた本文が、メール無害化により**リンクが無効化**

HTMLメールの本文に挿入されていた画像は、画像につけた名前に置き換わってテキスト化

無害化処理実行の案内文

テキストパート

HTMLパート

削除された添付ファイルの内容

SPAMSNIPER AGについて

SPAMSNIPER AGについて

統合メールセキュリティ

SPAMSNIPER AG

メール無害化　**アンチウイルス・スパム**　**誤送信防止**

アプライアンス版、ソフトウェア版、仮想版で提供

開発元　JIRANSOFT

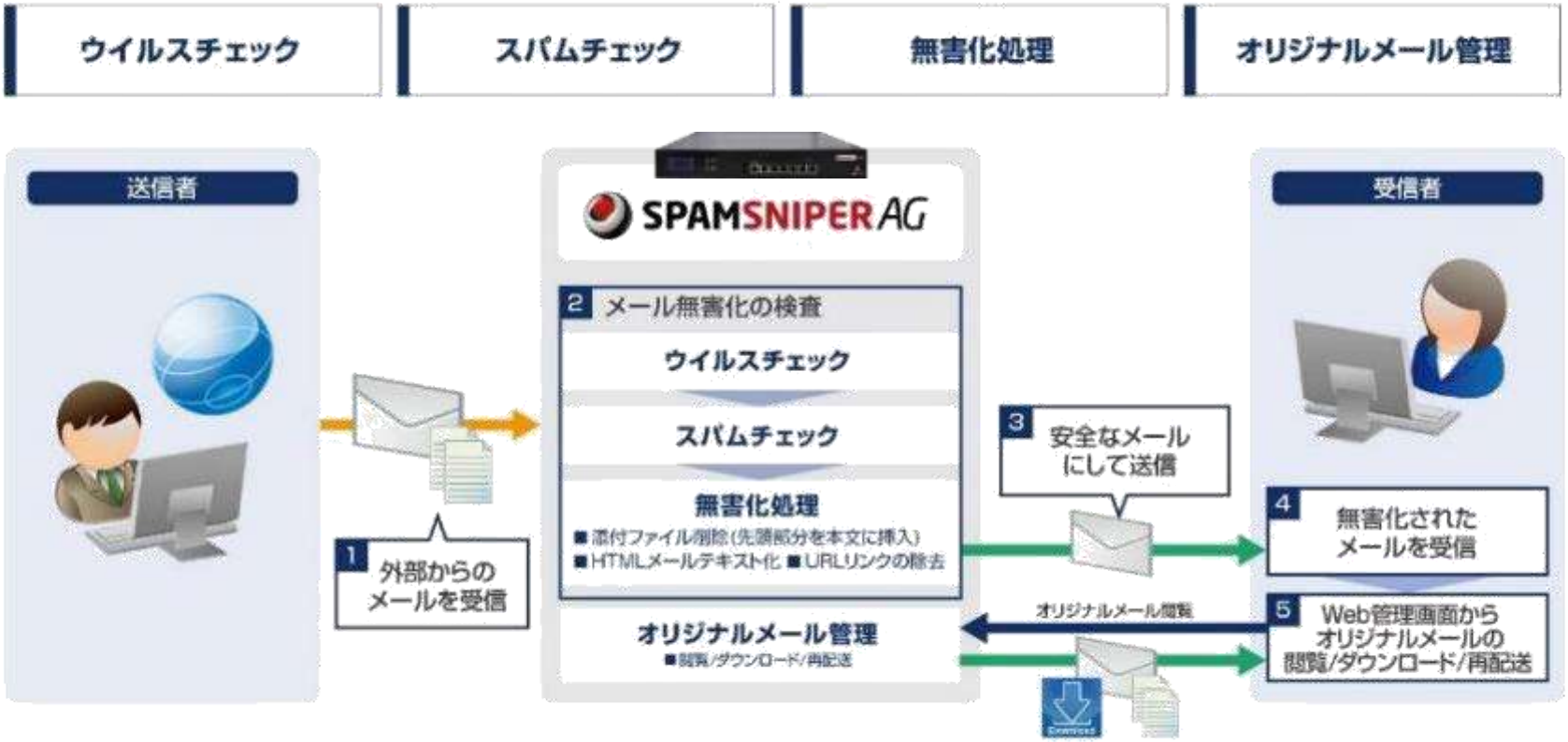
SPAMSNIPER AGの主な特徴

1. メール無害化、アンチウイルス・スパム、誤送信防止を**1台**で実現
2. ブリッジモード、プロキシモードの2つのモードを選択可能
3. 独自OSにより、障害発生時も処理中のメールをロストさせない安全設計
4. ユーザー数無制限（アプライアンス版のみ）、複数ドメイン管理も可能で抜群のコストパフォーマンス
5. アプライアンス版、ソフトウェア版、仮想版の３つの形態で提供可能
6. 日本語に対応した管理画面、マニュアルで操作が容易

検知率96%以上、誤検知率ほぼ0%

受信時の検査イメージ

受信メールのウイルス、スパムチェックに加えて、無害化処理を行うことで、
未知のウイルスの侵入を防ぎ、より安全なメール環境を提供することが可能。



誤送信防止機能

●添付ファイル暗号化

送信メールの添付ファイルをパスワード付きZIPファイルへ自動変換し送信します。

●添付ファイルリンク変換

送信メールの添付ファイルをSPAMSNIPER AGが自動的に剥離しHDD内に保管します。

受信者は、ダウンロード用の添付ファイルリンクからSPAMSNIPER AGに接続し、添付ファイル

をダウンロードする事ができます。

●送信遅延

送信メールをSPAMSNIPER AGが一旦保留し、一定時間経過後に自動送信する事ができます。

●上司（決裁者）承認

送信メールをSPAMSNIPER AGが一旦保留し、上司（決裁者）により承認されたメールのみ

送信する事ができます。

ラインナップ

評価版無償貸し出し中

モデル名	AG1000	AG2000	AG5000	AG10000
筐体イメージ				
利用ユーザー数（ライセンス）	無制限	無制限	無制限	無制限
参考ユーザー数 ※1	1,000	2,000	5,000	1,0000
メール処理件数/日（推奨）※2	70,000	200,000	500,000	1,000,000
メール処理件数/日（最大）※2	120,000	300,000	700,000	1,500,000
メモリ	2GB	8GB	8GB	8GB
HDD	1TB	2TB	2TB	146GB X 4 (RAID5)
NIC	10/100/1000 ×6	10/100/1000 ×6	10/100/1000 ×6	10/100/1000 ×6
バイパスカード	○	○	○	○
サイズ mm（W * D * H）	1U Rack Size 440*249*44	1U Rack Size 443*292*44.5	1U Rack Size 443*292*44。5	2U Rack Size 443*680*86

※1：「参考ユーザー数」はご利用ユーザー数の目安です。メールの処理数やサイズが大きい場合には実際のユーザー数にかかわらず上位機種が必要です。記載のユーザー数はご利用可能なユーザー数を保証するものではございません。

※2：メール処理件数はSPAMSNIPER AG が処理する送受信メールの総計です。（バイパスするメールは件数に含みません。）

キャンペーンのご案内

他社メールセキュリティ製品乗換えキャンペーン実施中!!

※対象となる他社スパムメール、誤送信対策製品（アプライアンス、ソフトウェア）の乗り換え情報の確認が必要となります。
※他社スパムメール、誤送信対策製品からの乗り換えではない場合には適用できません。

キャンペーン期間	2017年 2月 14日（火）～ 2018年 2月 13日（火）

保守５年付パッケージを特別価格にてご提供

■キャンペーン価格

製品名	想定価格（税別）	キャンペーン価格（税別）
SPAMSNIPER AG1000 （先出センドバック保守５年付）	¥2,612,000	¥ 1,900,000
SPAMSNIPER AG2000 （先出センドバック保守５年付）	¥3,564,000	¥ 2,592,000
SPAMSNIPER AG5000 （先出センドバック保守５年付）	¥5,148,000	¥ 3,744,000
SPAMSNIPER AG10000（先出センドバック保守５年付）	¥11,484,000	¥ 8,352,000

メールをクラウド環境でご利用のお客様

GUARDIANWALL Cloudファミリー

組み合わせ自由！選べる7種のメール対策
Office365との連携にも対応

本セッション受講者様向け特典（アンケートご回答者限定）

●特典１．SPAMSNIPER AG 次年度更新費1年間無償

先着10名

内容　　：期間内にAGアプライアンス版を購入のお客様に、次年度保守（1年間分）を無償で提供いたします。

※3年目以降の保守・ライセンス費用は有償となります

対象製品：SPAMSNIPER AGアプライアンス版（AG1000/AG2000/AG5000/AG10000）

対象期間：2017年12月27日当社受注分まで

●特典２．GUARDIANWALL Cloudファミリー 初期費用無償

先着10名

内容　　：期間内に対象サービスを申込いただくと、対象サービスの初期費用を無償にいたします。

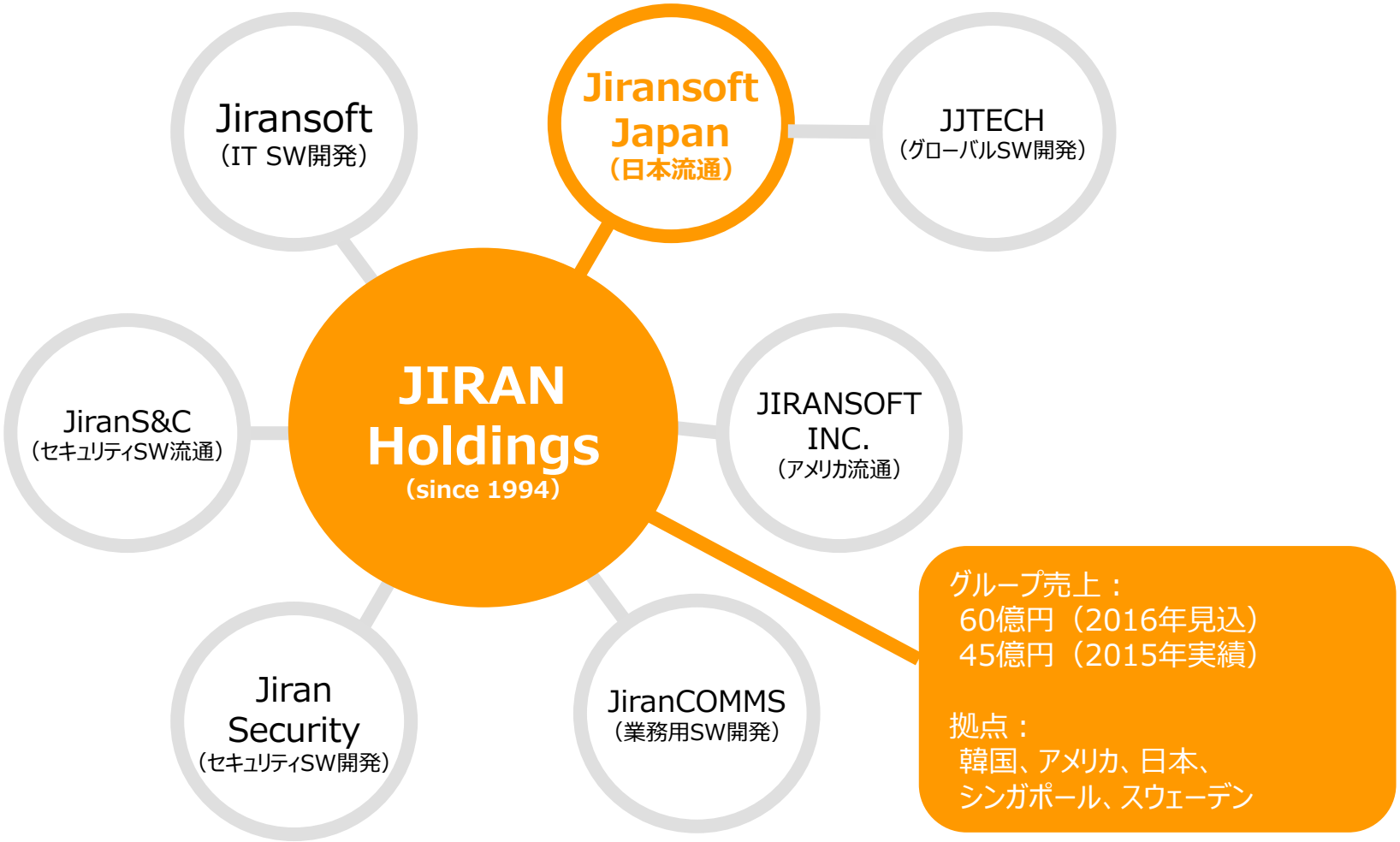
※初期費用以外のサービス利用料金は有償です（月額または年額）

対象サービス：GUARDIANWALL スパム対策サービス（初期費用：30,000円※シルバーサービス）
GUARDIANWALL メール無害化サービス（初期費用：40,000円）

対象期間　　：2017年12月27日当社受注分まで

Jiransoftについて

JIRANSOFT

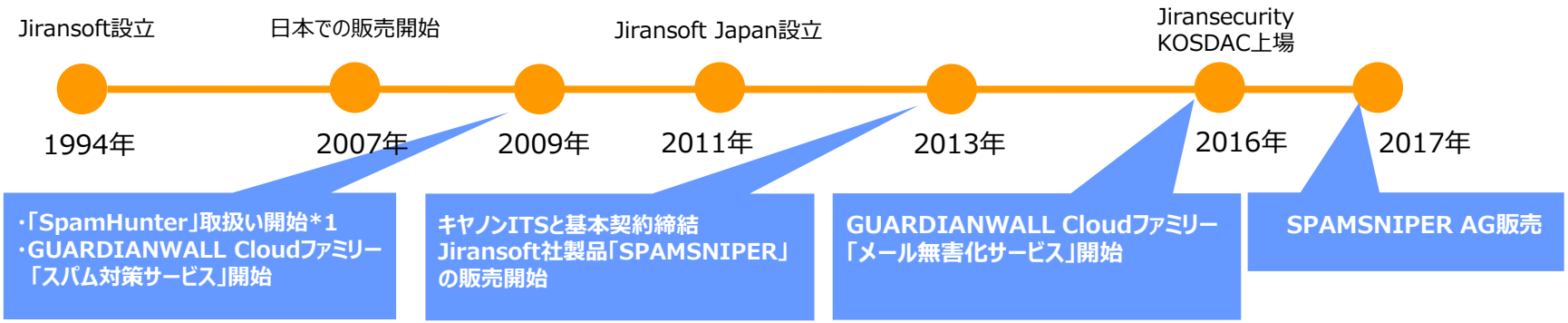


Jiransoft Japanについて

●会社概要

社　名：株式会社Jiransoft Japan
住　所：東京都新宿区新宿6-29-20
設　立：2011年7月
資本金：70,000,000円
代表者：呉 治泳（Oh,Chiyoung）

●沿革



*1 「SpamHunter」はSecuresoft社取扱いのJiransoft社製品「SPAMSNIPER」のOEM製品

メールセキュリティに関する
ご質問・リクエストがございましたら
お気軽にご相談ください。

ご清聴ありがとうございました