



不正端末侵入、メールセキュリティ事故対策に。  
機密データ流出を徹底ガード。



## 情報セキュリティ事故の発生要因

### 情報セキュリティ事故の発生確率（要因別）

電子メールの誤送信

SNSへの不適切な書き込み

携帯電話の紛失盗難

USBメモリの紛失盗難

パソコンの紛失盗難

0.00% 2.00% 4.00% 6.00% 8.00% 10.00% 12.00% 14.00%

最も発生確率が高い情報セキュリティ  
インシデントは電子メールの誤送信！

他要因の約4倍！



(参考) セキュリティ被害調査ワーキンググループ  
情報セキュリティインシデントに関する調査報告書 ~発生確率編~

最も発生確率が高い情報セキュリティインシデントは  
**電子メールの誤送信**で、10%を超えています。  
この値は、他の要因の**約4倍**になります。  
電子メールの誤送信は、**ちょっとしたミスや気の緩み**  
といったことが原因で、最も引き起こしやすいインシ  
デントだといえます。



ミスを防ぐためには個人の心掛けや行動が大切な一  
方、それだけで完全にミスをなくすことは絶対にで  
きません。**企業・組織としては、個人のミスが起こ  
り得るという前提で対策する必要があります。**  
**GE1000を導入すれば、メールの誤送信による情報  
セキュリティ事故を防止できます！**



# GE1000機能アップ! (Ver1.11)

HTMLメールの埋め込み画像をそのまま送信できます！

**New!** メール署名欄のロゴ画像など暗号化不要な埋め込み  
画像を自動で判別！添付ファイルのみ暗号化！

自社のロゴ入り署名

サクサ株式会社  
オフィス営業本部  
〒108-8050 東京都港区白金1-17-3  
NBFプラチナタワー2階  
TEL 03-5791-3932 FAX 03-5791-5564  
E-mail [info\\_saxa@saxa.co.jp](mailto:info_saxa@saxa.co.jp)  
URL <http://www.saxa.co.jp>



添付ファイルは  
今まで通り！

お客様

添付ファイル暗号化時に送信するパスワードメールを  
お客様が自由に編集できる機能を追加しました。

**New!** パスワード通知メールの本文をお客様が自由に編集する  
ことができます！

パスワード通知メール デフォルトメッセージ

送付したメールの添付ファイルはメールシステムにより自動暗号化されました。  
パスワードは下記になります。  
The attachment file of the mail that transmitted a message was automatically encrypted by the mail system.  
The password is as follows.

自由に  
編集  
可能！



メール処理の除外リストをIPアドレス指定できるよう  
になりました！（工率性能UP!!）

**New!** 複合機などのメール暗号化処理が不要な装置を  
IPアドレス指定で除外することができます！

複合機  
IPアドレス：  
192.168.1.250

サーバー  
IPアドレス：  
192.168.1.251

メール処理除外リスト

#	除外IPアドレス
1	192.168.1.250
2	192.168.1.251
3	...

除外リストを  
簡単追加！

受信者

本社/〒108-8050 東京都港区白金1-17-3 NBFプラチナタワー

■オフィス営業本部  
ネットワーク営業部 ☎ (03)5791-3931

●営業拠点

東北支社 ☎ (022)297-5835	札幌営業所 ☎ (011)281-1035
東京支社 ☎ (03)5791-5530	大宮営業所 ☎ (048)650-9311
中部支社 ☎ (052)220-3930	静岡営業所 ☎ (054)653-7711
関西支社 ☎ (06)6367-0393	金沢営業所 ☎ (076)255-0393
九州支社 ☎ (092)473-1511	高松営業所 ☎ (087)861-7450
	広島営業所 ☎ (082)511-7555

●お客様相談室 ☎ 0570-001-393 ☎ (050)5507-8039

URL <http://www.saxa.co.jp/>  
E-mail [customer@saxa-as.co.jp](mailto:customer@saxa-as.co.jp)

HTML本文内画像ファイル  
の自動暗号化除外設定

HTMLメールの本文内埋め込み  
画像を自動暗号化せずに送信す  
る設定を追加しました。

署名欄に自社のロゴ画像を入れて  
いるケースなど、暗号化不要な画像  
を自動で判別し、そのまま送信でき  
ます。

自動暗号化パスワード  
メール編集機能

添付ファイル暗号化時に送信する  
パスワード通知メールの本文を、  
編集できる機能を追加しました。

パスワード通知メールの本文をお客  
様の好みで自由に編集すること  
ができます。

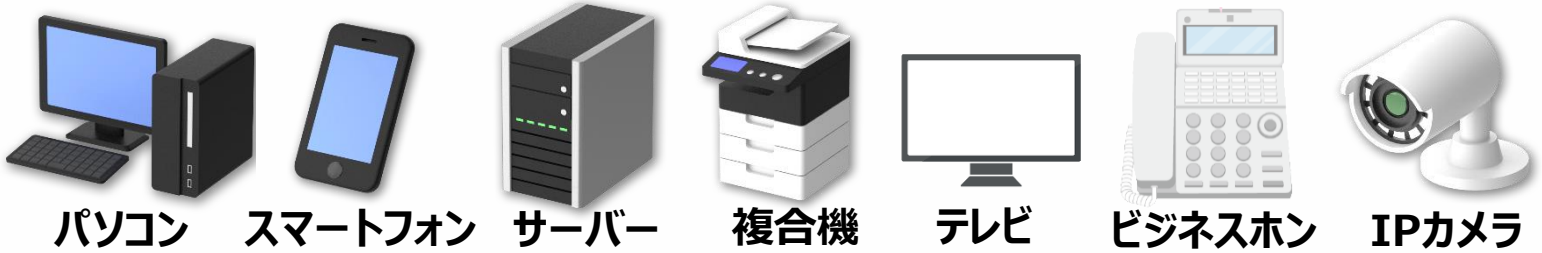
ホワイトリストIP対応

メール処理の除外リストを、メール  
アドレス、ドメイン指定だけでなく、  
**IPアドレスで指定**できるようになり  
ました。  
複合機などをIPアドレスで除外設  
定できるため、機器毎の使用メー  
ルアドレスを調べる必要がありませ  
ん。

GE1000は今後もお客様環境  
のセキュリティ強化、業務効率  
アップに貢献します！

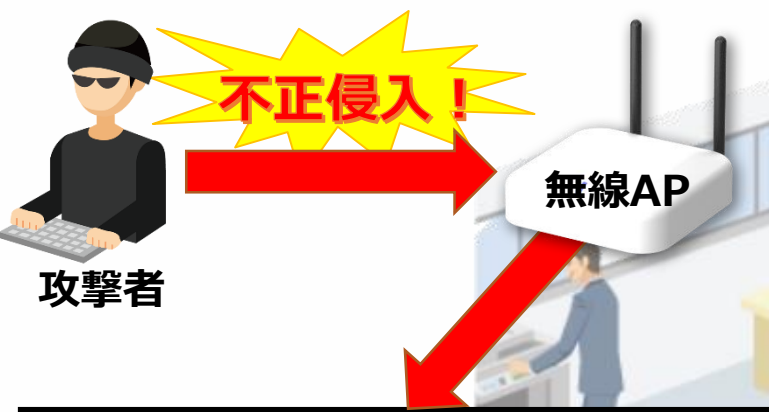


# 無線環境からネットワーク機器が攻撃されることをご存じですか？

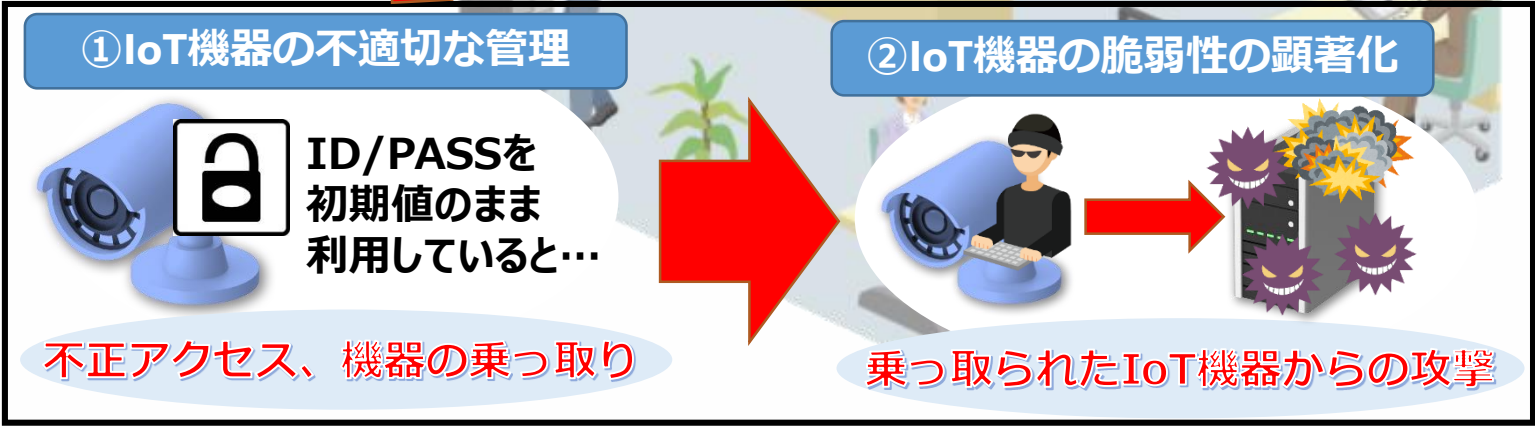


## 社内ネットワークに繋がるすべての機器が、攻撃対象です！

### 無線アクセスポイントが攻撃の入り口となる被害



**「IoT(Internet of Things)機器」**  
 パソコンやスマートフォン以外にも、テレビ・カメラ・冷蔵庫などの家電までインターネットに接続できるようになった。一方、IoT機器利用者はセキュリティに対して特に意識していないため、攻撃のターゲットになりやすい。



①、②の脅威は2018年において社会的に影響が大きかったセキュリティ上の脅威として、IPA独立行政法人情報処理推進機構「情報セキュリティ10大脅威2019」にランクインしています。



## GE1000で不正端末アクセスをブロックしましょう

未許可PCブロックの機能により、不正端末による社内ネットワーク接続をブロックします。内部からのウイルス感染やサーバへの不正アクセスを防止します。



GE1000





# GE1000



※1 サポートセンターへのご連絡にてリモート保守サービスを提供します。

主な仕様	GE1000	GE1000Pro
本体寸法	277mm(W)×178(D)×69mm(H) (突起物を除く)	300mm(W)×180(D)×72(H)mm (突起物を除く)
質量	約1.7kg (電源アダプタを除く)	約3.5kg (電源アダプタを除く)
環境温度	0 ~ 40℃	5 ~ 40℃
相対湿度	20 ~ 80% (結露なきこと)	30 ~ 80% (結露なきこと)
電源周波数	AC100±10V (50 / 60Hz)	AC100±10V (50 / 60Hz)
最大消費電力	24W	12W
EMI / 認証	VCCI-A	VCCI-A
PC同時接続推奨台数	60台	200台
IT機器最大監視端末数 (未許可PCブロック)	最大600台	最大600台
通知メール登録数	最大4メールアドレス (未許可PCブロック通知)	最大4メールアドレス (未許可PCブロック通知)
インターフェース	LAN: 10 / 100 / 1000Mbps 自動認識または手動設定 (AUTO-MDIX 対応)	LAN: 10 / 100 / 1000Mbps 自動認識または手動設定 (AUTO-MDIX 対応)
	ポート数: 5ポート	ポート数: 6ポート (メンテナンス専用ポート×1を含む) ※メンテナンス専用ポートは10 / 100Mbpsのみ対応 ※メンテナンス専用ポートにはお客様のネットワーク機器を接続できません
	接続コネクタ: RJ45 (8ピンモジュラージャック) USB3.0×1	接続コネクタ: RJ45 (8ピンモジュラージャック) USB3.0×1
付属品	電源アダプタ×1、電源ケーブル×1、 LANケーブル×1、取扱説明書×1	電源アダプタ×1、電源コード×1、 LANケーブル×1、取扱説明書×1

## aScanII エンドポイントセキュリティ動作環境

	Windows	Mac
OS	Windows 10/8.1/8/7、 Windows Server2016/ 2012 R2/2012/2008 R2、 Windows Storage Server 2016/ 2012R2/2012/2008 R2(32bit/64bit)	Mojave、 High Sierra、 Sierra、 Catalina
CPU	1.5GHz以上 / 推奨2GHz以上	2GHz以上
メモリ空き容量	2GB以上 / 推奨4GB以上 (※)	4GB以上
ディスク空き容量	インストール時に1GB以上	インストール時に1GB以上
Web環境	Internet Explorer 11以降、 Microsoft Edge	Safari

※インストールには、Microsoft .NET Framework 4.5.2以降がインストールされている必要があります。  
※リアルタイム監視モードの「標準」を選択するには、メモリ4GB以上を推奨します。4GB未満のPCは「軽快」をご利用ください。

管理マネージャ動作環境	
Web環境	Google Chrome (推奨) Internet Explorer 11以降、Microsoft Edge
画面解像度	1024×768以上 (1280×1024推奨)

αPCLog動作環境	
OS	Windows 10 / 8.1 / 8 / 7(32bit / 64bit)
OS言語	日本語 / 英語
CPU	1.5GHz以上 / 推奨2GHz以上
メモリ空き容量	2GB以上 / 推奨4GB以上
ディスク空き容量	インストール時に500MB以上

## システム注意事項

メール機能共通	<ul style="list-style-type: none"> <li>●SMTPサーバ(クラウド/オンプレミス)とクライアント端末(メーラー)の間に本装置を設置してください。</li> <li>●一時的に保留されるメールの合計容量は最大100MBまでとなります。※GE1000Proは最大1GB</li> <li>●SSL/TLS以外の暗号化方式 (STARTTLSなど) が適用されている場合は、利用できません。</li> <li>●501件以上のあて先が指定されたメールは、機能が動作せずそのまま送信します。</li> <li>●IPv6には非対応です。</li> <li>●LAN1を通過する通信に対して本機能が動作します。</li> <li>●Webメールは機能適用外です。</li> </ul>	<ul style="list-style-type: none"> <li>●メール添付ファイル自動暗号化</li> <li>●MacOSで解凍する場合、ファイル名が文字化けする可能性があります。</li> </ul>
送信メールアーカイブ	<ul style="list-style-type: none"> <li>●ストレージの上限に近づいた場合、アーカイブ保存期間の設定内容にかかわらず、残容量を10%確保するまで、古いメールから自動的に削除します。</li> </ul>	<ul style="list-style-type: none"> <li>●送信メールフィルタリング</li> <li>●本機能によるチェックは、件名および本文が対象です。(添付ファイルは対象外)</li> <li>●数字の羅列を、マイナンバー、クレジットカード番号と認識してしまう可能性があります。</li> <li>●未許可PCブロック</li> <li>●IPv6には非対応です。</li> </ul>

**安全に関するご注意**

- 本商品ご購入後は、添付の「取扱説明書」をよくお読みの上、正しくお使いください。「取扱説明書」には、本商品をご購入されたお客様や他の方々への危害や財産の損害を未然に防ぎ、本商品を安全にお使いいただくために守っていただきたい事項を記載しています。
- 水、湿気、湯気、ほこり、油煙などの多い場所には設置しないでください。火災、感電、故障などの原因となることがあります。

[本体について] ●本製品はネットワーク上の脅威に対してそのリスクを低減させるための装置です。本製品を導入することによりその脅威を完全に排除することを保証するものではありません。●本製品はネットワーク機器です。正しい知識を持った方が設置および初期設定を行ってください。●本製品の使用は国内向けとなっておりますので、海外ではご利用できません。●本製品に多くのトラフィック負荷がかかると、通信速度が低下する場合がありますのでご注意ください。●本製品は、外国為替および外国貿易法で定める規制対象貨物・技術に該当する製品です。この商品を輸出する場合または国外に持ち出す場合は、日本政府の輸出許可が必要です。●本製品の補修用性能部品の最低保有期間は、販売終了後7年です。●Windows、Internet Explorer、Microsoft Edgeは米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。●Mac および Safari は、米国およびその他の国々で登録されたApple Inc.の商標です。●Google Chromeは、Google Inc.の商標または登録商標です。●本カタログに記載されている会社名や製品名は各社の商標または商標登録です。●仕様、外観は予告なく変更する場合があります。●カラーは印刷の都合上、実際と異なる場合があります。

## サクサ株式会社

本社 / 〒108-8050 東京都港区白金1-17-3 NBFプラチナタワー

■パートナー営業本部  
ネットワーク営業部 ☎ (03) 5791-3931

■オフィス営業本部

●営業拠点

東北支社 ☎ (022) 297-5835	札幌営業所 ☎ (011) 281-1035
東京支社 ☎ (03) 5791-5530	大宮営業所 ☎ (048) 650-9311
中部支社 ☎ (052) 220-3930	静岡営業所 ☎ (054) 653-7711
関西支社 ☎ (06) 6367-0393	金沢営業所 ☎ (076) 255-0393
九州支社 ☎ (092) 473-1511	高松営業所 ☎ (087) 861-7450
	広島営業所 ☎ (082) 511-7555

●お客様相談室 ☎ 0570-001-393 ☎ (050)5507-8039  
URL <https://www.saxa.co.jp/>  
E-mail [customer@saxa-as.co.jp](mailto:customer@saxa-as.co.jp)

●お問い合わせ・ご用命は

このカタログの記載内容は2020年1月現在のものです。

この印刷物は環境保護のため  
植物油インキを使用しています。

SA-0543





# GE1000シリーズは、社員のメール業務に関わるリスクや業務の負荷を軽減し、効率的な業務をサポートするメールセキュリティ機能を搭載!



重要メールを誤って違うあて先に送信する、社員が意図的にメールで機密情報を送信するなど、企業にはメールが原因の情報漏えいリスクが多数あります。  
GE1000シリーズは、社内の情報漏えいを防ぐ「情報セキュリティゲートウェイ」です。



## Case 1 メール誤送信の経験はありませんか?

あて先を間違える、間違ったデータを送ってしまった、そんな経験ありませんか?



## Case 2 メールの適正利用、出来ていますか?

社員のメール使用履歴、きちんと管理できていますか?



## Case 3 メールでデータを送る際、パスワードを付けていますか?

メールセキュリティの運用を、社員に任せていませんか?

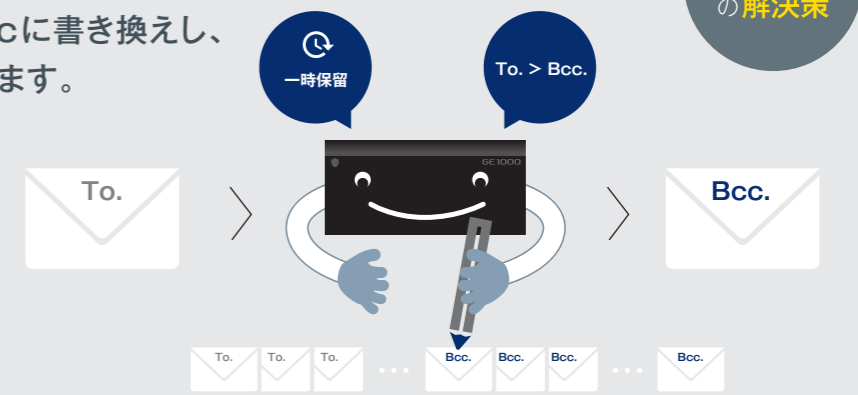


### メール誤送信防止 + あて先Bcc変換 GE1000Pro GE1000 Case 1 の解決策

メールのあて先を自動でBccに書き換えし、メールアドレスの流出を防ぎます。

メールを一時保留しキャンセルする機能と不特定多数のあて先を自動でBccに変換する機能で情報漏えいを防ぎます。

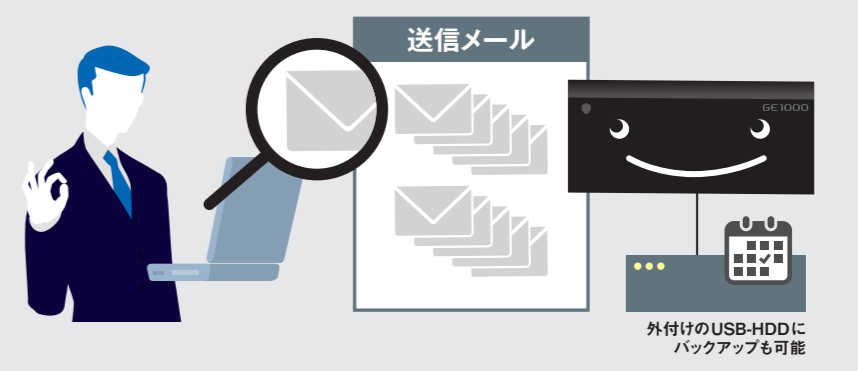
※あて先Bcc変換機能は、GE1000Proのみの機能です



### 送信メールアーカイブ機能 GE1000Pro Case 2 の解決策

社員の送信メールを一括監視。不正利用対策以外に、日々の引継ぎも楽々。

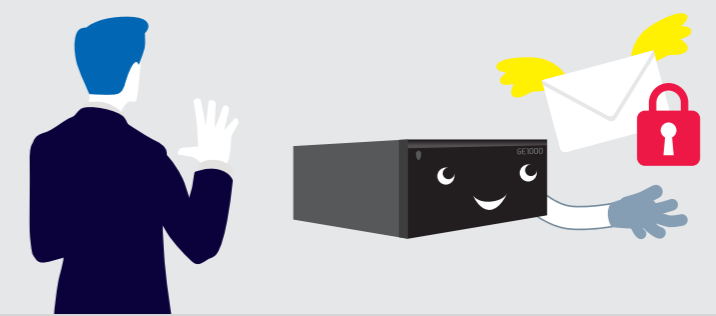
社員の送信メールは、普段お使いのメールソフトから閲覧できるようになります。そのため、情報の共有が容易になります。



### メールセキュリティ事故防止機能 GE1000Pro GE1000 Case 3 の解決策

メール添付ファイル暗号化を自動化して情報漏えい対策!

メールセキュリティを自動化することで、社員が意識することなく、情報漏えい対策が可能です。



# 業務に関係のない端末は通信をブロック！ 未許可PCブロック機能で、クリーンな社内ネットワークを。

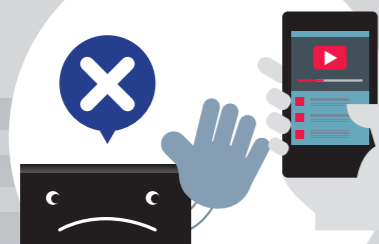
GE1000シリーズは、社内ネットワークに許可されていない端末が接続されることを防ぎます。サクサUTM「SS5000シリーズ」と連携することで、万が一、ウイルス感染した端末が社内ネットワークに接続されたとしても、感染拡大を防ぎます。



Case 1

## 個人のスマートフォン接続、 それって許可されてますか？

業務以外の通信で、社内ネットワークの帯域が圧迫されてしまうことも。



Case 3

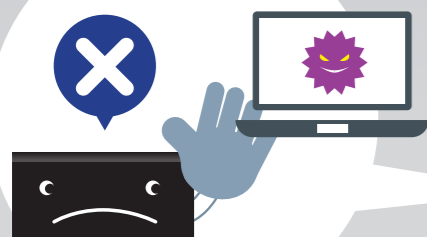
## 業務PCを持ち出し、 万が一ウイルスに感染したら？

外出先で使用しているパソコン、もしかしたらウイルスに感染しているかも…。

Case 2

## 個人のPC接続、万が一 ウイルスに感染したら？

個人PCのセキュリティ対策は、あくまで個人によるもの。適切なセキュリティ対策が取られていないことも。

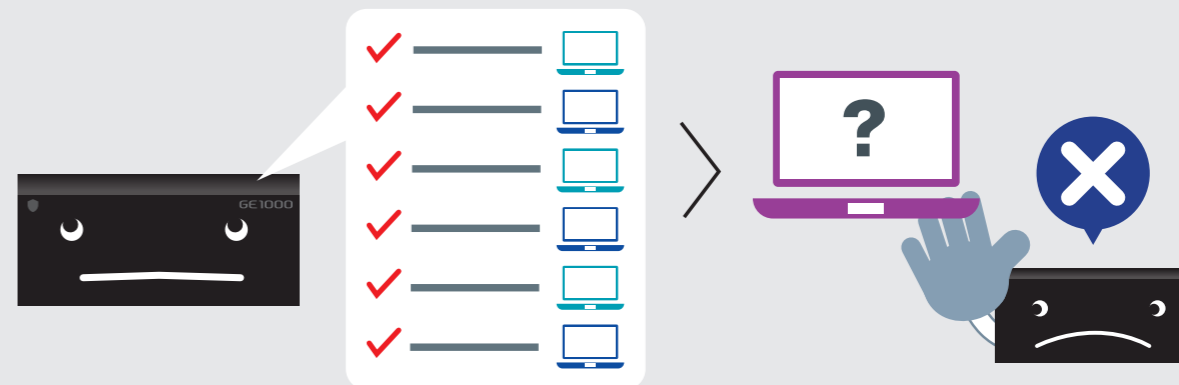


### 未許可PCブロック

GE1000Pro GE1000

Case 1・2  
の解決策

許可されていない端末は、社内ネットワークに接続してもIP通信が出来ないようにする機能です。データの持ち出しなど、情報漏えい等のセキュリティ事故を未然に防ぎます。

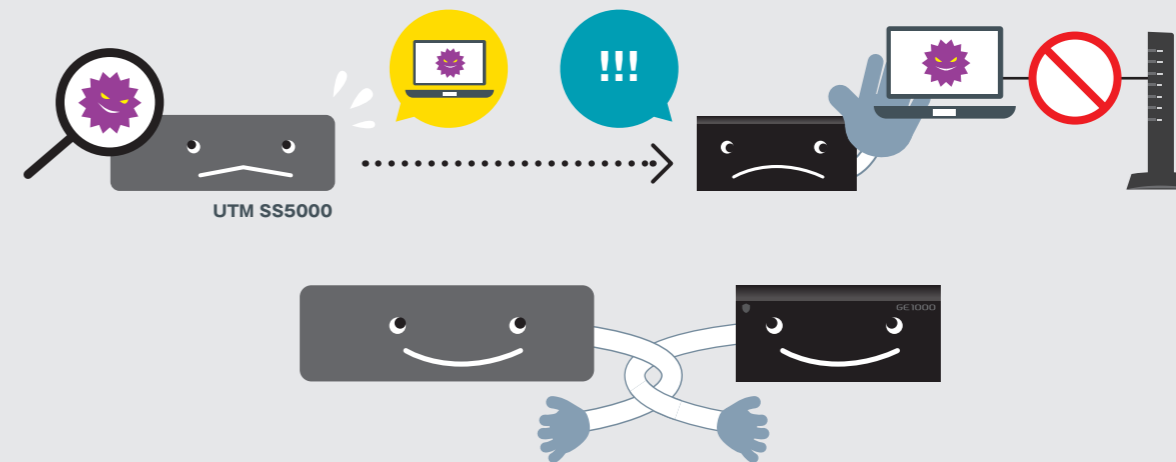


### UTM連携

GE1000Pro GE1000

Case 3  
の解決策

サクサUTM「SS5000シリーズ」と連携することで、より複合的なセキュリティを実現します。万が一、ウイルス感染した場合に「社外へのウイルスばら撒き」をUTMが検知。その後、該当端末の情報を通知することで、GE1000が該当PCを社内ネットワークから隔離します。



### POINT メール報告機能

未許可PCブロックは、許可されていない端末の通信遮断タイミング、UTM連携は、感染した端末の通信を遮断したタイミングで、管理者に対してメールで報告を行います。管理者に自動で報告されるしきみを構築することは、社員の不正行為\*を抑止し、セキュリティ意識の向上につながります。

\*私用端末への業務データ持ち出し、業務に関係のないデータ通信（動画視聴・ゲーム等）



# PRODUCT FEATURES

## 送信メールアーカイブ機能 GE1000Pro

送信メールを、GE1000Proが自動的に保存（アーカイブ）します。

保存されているメールは、普段利用しているメールソフトから簡単に閲覧可能です。メールのやりとりが全て一括で管理できるので、メールからの機密情報漏えいを抑止したり、休暇中の従業員のメール業務を引き継いだりすることが可能になります。もちろん、閲覧者の制限も可能です。

※社外で送信したメールはアーカイブされません。



外付けのUSB-HDDにバックアップも可能。

## メールセキュリティ機能

### 1 メール誤送信防止

GE1000Pro  
GE1000

メールの送信を一定時間保留します。誤送信に気が付いた場合は、GE1000/GE1000Proにアクセスすることで、メールの送信をキャンセルすることが出来ます。



### 2 メール添付ファイル自動暗号化

GE1000Pro  
GE1000

メール送信時に添付ファイルがある場合、自動で暗号化を行います。復号パスワードは自動生成され、送信先に自動でメール通知することもできます。送信者自身で暗号化作業をする手間が無いので、業務効率化に繋がります。



### 3 送信メールフィルタリング

GE1000Pro  
GE1000

個人情報や特定キーワードを含むメール送信を、一時保留します。保留後は、送信者に保留した旨を伝えるメールを通知します。個人情報及び、機密情報の漏えいを防止する機能です。



### 4 あて先Bcc変換



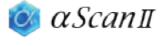





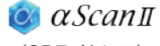

GE1000Pro

あて先数/ドメイン数を条件に、ToやCcを強制的にBccに変換してメール送信する機能です。メールマガジンのように不特定多数のお客様へメールを送信する際に間違っToやCcで送信してしまう「情報漏えい事故」を防ぐことが出来ます。



# Lineup

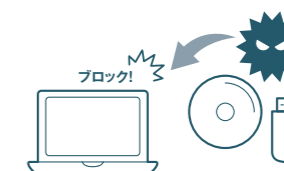
オフィスの環境やネット環境に合わせて、必要なセキュリティをお選びいただけます。

	機能概要		セキュリティソフトウェア (αScanII / αPCLog)	推奨接続台数	サポート 先出しセンドバック (有償サポート/要登録)
	メールセキュリティ	不正端末セキュリティ			
<b>GE1000</b> 	メール添付ファイル自動暗号化 メール誤送信防止 送信メールフィルタリング	未許可PCブロック UTM連携	—	 × 60台	○
<b>GE1000 (α)</b> エンドポイントセキュリティを バンドルした、αシリーズ  +  	メール添付ファイル自動暗号化 メール誤送信防止 送信メールフィルタリング	未許可PCブロック UTM連携	 αScanII (20ライセンス)  αPCLog (20ライセンス)	 × 60台	○
<b>GE1000Pro</b> 	メール添付ファイル自動暗号化 メール誤送信防止 送信メールフィルタリング 送信メールアーカイブ あて先Bcc変換	未許可PCブロック UTM連携	—	 × 200台	○
<b>GE1000Pro (α)</b> エンドポイントセキュリティを バンドルした、αシリーズ  +  	メール添付ファイル自動暗号化 メール誤送信防止 送信メールフィルタリング 送信メールアーカイブ あて先Bcc変換	未許可PCブロック UTM連携	 αScanII (35ライセンス)  αPCLog (35ライセンス)	 × 200台	○

## オプション機能で、ウイルス対策にも備えられます。

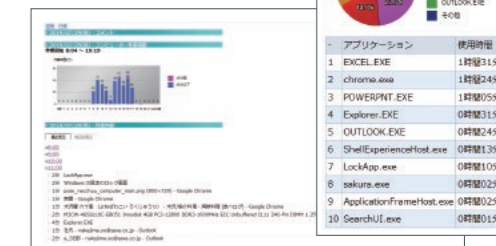
### αScanII(エンドポイントセキュリティ) αScanII

各パソコンにクライアントソフトをインストールすることで、端末に侵入してくるウイルスを駆除することが可能です。USBメモリの自動検疫等、複合的な対策が可能です。



### αPCLog(オフィス管理機能) αPCLog

各パソコンにクライアントソフトをインストールすることで、端末情報が定期的に収集・分析され、作業内容やファイル作業操作履歴の「見える化」が可能になります。



αシリーズ限定